

NSX 문제 해결 가이드

업데이트 8

수정 날짜: 2020년 2월 21일

VMware NSX Data Center for vSphere 6.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

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

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

목차

1 NSX 문제 해결 가이드 7

일반 문제 해결 지침 7

NSX 대시보드 사용 8

NSX 명령줄 인터페이스 빠른 참조 11

NSX 호스트 상태 점검 21

2 NSX 인프라 문제 해결 23

호스트 준비 23

호스트 준비 아키텍처 이해 28

호스트 준비를 위한 서비스 배포 워크플로 32

타사 서비스에 대한 서비스 배포 워크플로 34

통신 채널 상태 확인 36

설치 상태가 준비되지 않음 38

서비스가 응답하지 않음 38

OVF/VIB 액세스 불가 오류를 나타내며 서비스 배포가 실패함 39

해결 옵션을 사용하여 문제가 해결되지 않음 41

vSphere EAM(ESX Agent Manager) 정보 42

NSX Manager 문제 해결 43

NSX Manager를 vCenter Server에 연결 45

보조 NSX Manager가 전송 모드에서 중단됨 47

NSX SSO Lookup Service 구성 실패 48

논리적 네트워크 준비: VXLAN 전송 51

VXLAN VMkernel NIC가 동기화되지 않음 53

VXLAN 팀 구성 정책 및 MTU 설정 변경 54

논리적 스위치 포트 그룹이 동기화되지 않음 56

3 NSX 라우팅 문제 해결 58

논리적 분산 라우터 이해 59

상위 수준 DLR 패킷 흐름 60

DLR ARP 확인 프로세스 62

Edge Services Gateway에서 제공하는 라우팅 이해 63

ECMP 패킷 흐름 64

NSX 라우팅: 전제 조건 및 고려 사항 66

DLR 및 ESG UI 68

NSX 라우팅 UI 68

NSX Edge UI 69

새 NSX Edge(DLR)	70
ESG 및 DLR 차이점	73
일반적인 ESG 및 DLR UI 작업	74
Syslog 구성	74
정적 경로	76
경로 재배포	77
NSX 라우팅 문제 해결	78
NSX 라우팅 CLI	78
라우팅 요약	81
샘플 라우팅 토폴로지를 사용하여 DLR 상태 확인	82
시각적으로 나타낸 DLR 및 관련 호스트 구성 요소	89
분산 라우팅 하위 시스템 아키텍처	90
NSX 라우팅 하위 시스템 구성 요소	95
NSX 라우팅 제어부 CLI	97
NSX 라우팅 하위 시스템 실패 모드 및 결과	100
라우팅 관련 NSX 로그	104
일반 실패 시나리오 및 수정 사항	106
문제 해결 데이터 수집	106
4 NSX Edge 문제 해결	111
Edge 방화벽 패킷 삭제 문제	115
Edge 라우팅 연결 문제	119
NSX Manager 및 Edge 통신 문제	121
메시지 버스 디버깅	122
Edge 진단 및 복구	124
5 방화벽 문제 해결	127
분산 방화벽 정보	127
DFW에 대한 CLI 명령	128
분산 방화벽 문제 해결	131
ID 방화벽	137
6 로드 밸런싱 문제 해결	140
시나리오: 단일 암 로드 밸런서 구성	140
로드 밸런서에 대한 문제 해결 순서도	146
UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결	147
CLI를 사용하여 로드 밸런서 문제 해결	158
일반 로드 밸런서 문제	169
7 VPN(Virtual Private Network) 문제 해결	174

L2 VPN 174

L2 VPN 일반 구성 문제 174

반복을 완화하기 위한 L2VPN 옵션 176

CLI를 사용하여 문제 해결 179

SSL VPN 181

SSL VPN 웹 포털이 열리지 않음 181

SSL VPN-Plus: 설치 실패 182

SSL VPN-Plus: 통신 문제 185

SSL VPN-Plus: 인증 문제 188

SSL VPN-Plus Client가 응답을 중지함 188

기본 로그 분석 189

IPSec VPN 190

성공적 협상(1단계 및 2단계) 190

1단계 정책 불일치 191

2단계 불일치 192

PFS 불일치 193

PSK 불일치 194

성공적 협상을 위한 패킷 캡처 195

8 NSX Controller 문제 해결 201

컨트롤러 클러스터 아키텍처의 이해 201

NSX Controller 배포 문제 204

디스크 지연 시간 문제 해결 208

디스크 지연 시간 경고 보기 208

디스크 지연 시간 문제 210

NSX Controller 클러스터 오류 211

방법 1: 손상된 컨트롤러 삭제 및 새 컨트롤러 다시 배포 213

방법 2: NSX Controller 클러스터 다시 배포 216

가상 컨트롤러 216

NSX Controller의 연결이 끊김 218

제어부 에이전트(netcpa) 문제 219

9 Guest Introspection 문제 해결 223

Guest Introspection 아키텍처 223

Guest Introspection 로그 224

ESX GI 모듈(MUX) 로그 225

GI Thin Agent 로그 227

GI EPSecLib 및 SVM 로그 230

Guest Introspection 환경 및 작업 세부 정보 수집 232

Linux 또는 Windows의 Thin Agent 문제 해결 233

[ESX GI 모듈\(MUX\) 문제 해결](#) 236

[EPSecLib 문제 해결](#) 237

NSX 문제 해결 가이드

1

NSX 문제 해결 가이드에서는 "" 필요에 따라 NSX Manager 사용자 인터페이스, vSphere Web Client 및 기타 NSX 구성 요소를 사용하여 VMware NSX® for vSphere® 시스템을 모니터링하고 문제를 해결하는 방법을 설명합니다.

대상 사용자

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

VMware 기술 자료 용어집

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

본 장은 다음 항목을 포함합니다.

■ 일반 문제 해결 지침

일반 문제 해결 지침

이 항목에서는 NSX for vSphere 문제를 해결하기 위해 따를 수 있는 일반적인 지침에 대해 설명합니다.

- 1 **NSX 대시보드** 사용로 이동하여 구성 요소에 오류나 경고가 표시되는지 확인합니다.
- 2 기본 NSX Manager의 **모니터(Monitor)** 탭으로 이동한 후 트리거된 시스템 이벤트가 있는지 확인합니다. 시스템 이벤트 및 정보에 대한 자세한 내용은 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.
- 3 NSX API를 사용하여 `GET api/2.0/services/systemalarms` 개체에 대한 경보를 확인합니다. API에 대한 자세한 내용은 "NSX API 가이드"를 참조하십시오.
- 4 "NSX 문제 해결 가이드"에 설명된 대로 문제를 해결합니다.
- 5 문제가 해결되지 않으면 기술 지원 로그를 다운로드하고 VMware 지원팀에 문의합니다. "My VMware에서 지원 요청을 정리하는 방법"을 참조하십시오. 로그를 다운로드하는 방법에 대한 자세한 내용은 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.

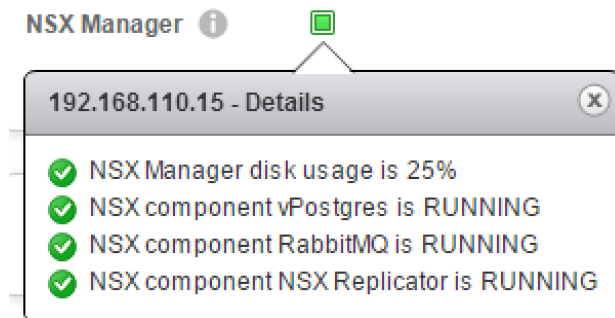
NSX 대시보드 사용

NSX 대시보드는 하나의 중앙 보기에서 NSX 구성 요소의 전반적인 상태에 대한 가시성을 제공합니다. NSX 대시보드는 NSX Manager, 컨트롤러, 논리적 스위치, 호스트 준비, 서비스 배포, 백업뿐만 아니라 Edge 알림과 같은 여러 다른 NSX 구성 요소의 상태를 표시하여 문제 해결을 단순화합니다.

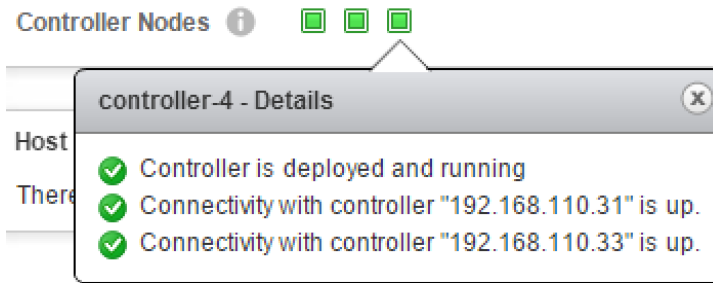
- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭하고 **대시보드(Dashboard)**를 클릭합니다. [대시보드] 페이지가 표시됩니다.
- 3 크로스 vCenter NSX 환경에서 기본 역할 또는 보조 역할을 갖는 NSX Manager를 선택합니다.

대시보드는 다음 정보를 제공합니다.

- NSX 인프라 — 다음 서비스에 대한 NSX Manager 구성 요소 상태가 모니터링됩니다.
 - 데이터베이스 서비스(vPostgres)
 - 메시지 버스 서비스(RabbitMQ)
 - Replicator 서비스 — 복제 오류도 모니터링합니다(크로스 vCenter NSX가 사용되도록 설정된 경우).
 - NSX Manager 디스크 사용량:
 - 노란색은 디스크 사용량이 80%보다 많음을 나타냅니다.
 - 빨간색은 디스크 사용량이 90%보다 많음을 나타냅니다.

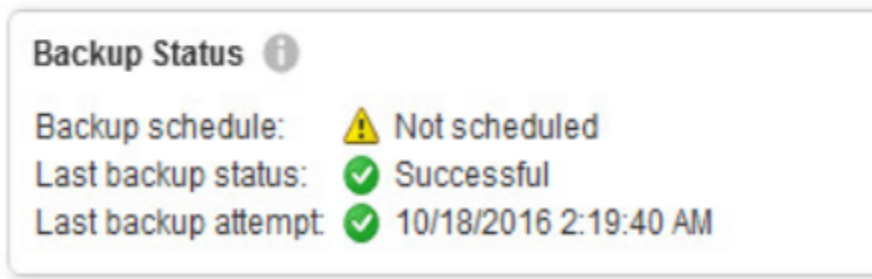
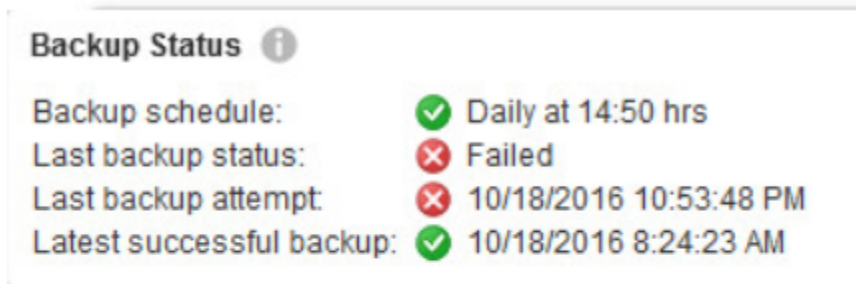


- NSX 인프라—NSX Controller 상태:
 - 컨트롤러 노드 상태(작동/다운/실행 중/배포 중/제거 중/실패/알 수 없음)
 - 컨트롤러 피어 연결 상태가 표시됩니다. 컨트롤러가 다운되어 빨간색으로 표시되면 피어 컨트롤러는 노란색으로 표시됩니다.
 - 컨트롤러 VM 상태(전원 꺼짐/삭제됨)
 - 컨트롤러 디스크 지연 시간 경고



■ NSX Manager 백업 상태:

- 백업 일정
- 마지막 백업 상태(실패/성공/예약되지 않음과 날짜 및 시간)
- 마지막 백업 시도(날짜 및 시간과 세부 정보)
- 마지막 성공 백업(날짜 및 시간과 세부 정보)



■ NSX 인프라 — 다음 서비스에 대한 호스트 상태가 모니터링됩니다.

- 배포 관련:
 - 설치 실패 상태의 클러스터 수
 - 업그레이드가 필요한 클러스터 수
 - 설치가 진행 중인 클러스터 수
 - 준비되지 않은 클러스터 수
- 방화벽:
 - 방화벽이 사용되지 않도록 설정된 클러스터 수

- 방화벽 상태가 노란색/빨간색인 클러스터 수:
 - 노란색은 분산 방화벽이 클러스터에서 사용되지 않도록 설정됨을 나타냅니다.
 - 빨간색은 분산 방화벽이 호스트/클러스터에서 설치될 수 없음을 나타냅니다.
- VXLAN:
 - VXLAN이 구성되지 않은 클라이언트 수
 - VXLAN 상태가 녹색/노란색/빨간색인 클러스터 수:
 - 녹색은 기능이 성공적으로 구성되었음을 나타냅니다.
 - 노란색은 VXLAN 구성이 진행 중임을 의미합니다.
 - 빨간색(오류)은 VTEP 생성이 실패했거나, VTEP에서 IP 주소를 찾을 수 없거나, VTEP에 *LinkLocal* IP 주소가 할당된 경우 등을 나타냅니다.
- NSX 인프라—서비스 배포 상태
 - 배포 실패—실패한 배포에 대한 설치 상태
 - 서비스 상태—실패한 모든 서비스에 해당
- NSX 인프라 —NSX Edge 알림

Edge 알림 대시보드에는 특정 서비스에 대해 활성 상태인 경보를 강조 표시합니다. 아래 나열된 중요 이벤트 목록을 모니터링하고 문제가 해결될 때까지 계속 추적합니다. 경보는 복구 이벤트가 보고되거나, Edge가 강제로 동기화되거나, 재배포되거나, 업그레이드될 때 자동으로 해결됩니다.

 - 로드 밸런서(Edge 로드 밸런서 서버 상태):
 - Edge 로드 밸런서 백엔드 서버가 다운됨
 - Edge 로드 밸런서 백엔드 서버 경고 상태
 - VPN(IPSec 터널/IPSec 채널 상태):
 - Edge IPSec 채널이 다운됨
 - Edge IPSec 터널이 다운됨
 - 장치(Edge VM, Edge Gateway, Edge 파일 시스템, NSX Manager 및 Edge Services Gateway 보고서 상태):
 - Edge Services Gateway에 상태 검사 펄스가 누락됨
 - Edge VM의 전원이 꺼짐
 - Edge VM의 상태 검사 펄스가 누락됨
 - NSX Edge에서 잘못된 상태를 보고함
 - Edge Services Gateway가 잘못된 상태라는 NSX Manager 보고서
 - Edge VM이 VC 인벤토리에 없음

■ HA 분할 브레인 이 감지됨

참고 로드 밸런서 및 VPN 정보가 구성 업데이트 동안 자동으로 지워지지 않습니다. 문제가 해결되면 `alarm-id` 명령을 사용하여 API를 통해 정보를 수동으로 지워야 합니다. 다음은 정보를 지우기 위해 사용할 수 있는 API의 예입니다. 자세한 내용은 "NSX API 가이드"를 참조하십시오.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

■ NSX Services—방화벽 게시 상태:

- 방화벽 게시 상태가 실패인 호스트 수. 호스트가 게시된 분산 방화벽 구성을 성공적으로 적용하지 못할 경우 상태가 빨간색입니다.

■ NSX Services—논리적 네트워킹 상태:

- 상태가 오류 또는 경고인 논리적 스위치 수
- 지원되는 분산 가상 포트 그룹이 vCenter Server에서 삭제될 경우 플래그 지정

NSX 명령줄 인터페이스 빠른 참조

문제를 해결하려면 NSX CLI(명령줄 인터페이스)를 사용할 수 있습니다.

표 1-1. ESXi 호스트의 NSX 설치 확인—NSX Manager에서 실행되는 명령

설명	NSX Manager에 대한 명령	참고
모든 클러스터를 나열하여 클러스터 ID를 가져오기	<code>show cluster all</code>	모든 클러스터 정보 표시
클러스터의 모든 호스트를 나열하여 호스트 ID를 가져오기	<code>show cluster clusterID</code>	클러스터의 호스트 목록, 호스트 ID 및 호스트 준비 설치 상태를 표시합니다.
호스트의 모든 VM 나열	<code>show host hostID</code>	특정 호스트 정보, VM, VM ID 및 전원 상태를 표시합니다.

표 1-2. 명령에서 사용할 수 있게 호스트에 설치된 VIB 및 모듈 이름

NSX 버전	ESXi 버전	VIB	모듈
모든 6.3.x	5.5	esx-vxlan 및 esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.2 및 이전 버전	6.0 이상	esx-vxlan 및 esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.3 이상 버전	6.0 이상	esx-nsxv	nsx-vdl2, nsx-vdrb, nsx-vsip, nsx-dvfilter-switch-security, nsx-core, nsx-bfd, nsx-traceflow

표 1-3. ESXi 호스트의 NSX 설치 확인—호스트에서 실행되는 명령

설명	호스트에 대한 명령	참고
존재하는 VIB는 NSX 및 ESXi 버전에 따라 다릅니다. 설치에서 확인할 모듈에 대한 자세한 내용은 "호스트에 설치된 VIB 및 모듈 이름" 표를 참조하십시오.	<code>esxcli software vib get --vibName <name></code>	설치된 버전/날짜를 확인합니다. <code>esxcli software vib list</code> 는 시스템의 모든 VIB 목록을 나열합니다.
시스템에 현재 로드된 모든 시스템 모듈 나열	<code>esxcli system module list</code>	동급의 이전 명령: <code>vmkload_mod -l grep -E vdl2 vdrb vsip dvfilter-switch-security</code>
존재하는 모듈은 NSX 및 ESXi 버전에 따라 다릅니다. 설치에서 확인할 모듈에 대한 자세한 내용은 "호스트에 설치된 VIB 및 모듈 이름" 표를 참조하십시오.	<code>esxcli system module get -m <name></code>	각 모듈에 대한 명령을 실행합니다.
2개의 UWA(사용자 월드 에이전트): 제어 부 에이전트, 방화벽 에이전트	<code>/etc/init.d/vShield-Stateful-Firewall status</code> <code>/etc/init.d/netcpad status</code>	
컨트롤러에 대한 포트 1234 및 NSX Manager에 대한 포트 5671의 UWA 연결 확인	<code>esxcli network ip connection list grep 1234</code> <code>esxcli network ip connection list grep 5671</code>	컨트롤러 TCP 연결 메시지 버스 TCP 연결
EAM 상태 확인	vSphere Web Client, 관리 > vSphere ESX Agent Manager(Administration > vSphere ESX Agent Manager) 확인	

표 1-4. ESXi 호스트의 NSX 설치 확인—호스트 네트워킹 명령

설명	호스트 네트워킹 명령	참고
물리적 NIC/vmnic 나열	<code>esxcli network nic list</code>	NIC 유형, 드라이버 유형, 링크 상태, MTU를 확인합니다.
물리적 NIC 세부 정보	<code>esxcli network nic get -n vmnic#</code>	드라이버 및 펌웨어 버전과 기타 세부 정보를 확인합니다.

표 1-4. ESXi 호스트의 NSX 설치 확인—호스트 네트워킹 명령 (계속)

설명	호스트 네트워킹 명령	참고
IP 주소/MAC/MTU 등과 함께 vmk NIC 나열	<code>esxcli network ip interface ipv4 get</code>	VTEP가 올바르게 인스턴스화되는지 확인합니다.
각 vmk NIC의 세부 정보(vDS 정보 포함)	<code>esxcli network ip interface list</code>	VTEP가 올바르게 인스턴스화되는지 확인합니다.
각 vmk NIC의 세부 정보(VXLAN vmk에 대한 vDS 정보)	<code>esxcli network ip interface list --netstack=vxlan</code>	VTEP가 올바르게 인스턴스화되는지 확인합니다.
이 호스트의 VTEP와 연관된 VDS 이름 찾기	<code>esxcli network vswitch dvs vmware vxlan list</code>	VTEP가 올바르게 인스턴스화되는지 확인합니다.
VXLAN 전용 TCP/IP 스택에서 Ping	<code>ping ++netstack=vxlan -I vmk1 x.x.x.x</code>	VTEP 통신 문제 해결: 전송 네트워크의 MTU가 VXLAN에 대해 올바른지 확인하기 위한 <code>-d -s 1572</code> 옵션을 추가합니다.
VXLAN 전용 TCP/IP 스택의 라우팅 테이블 보기	<code>esxcli network ip route ipv4 list -N vxlan</code>	VTEP 통신 문제 해결
VXLAN 전용 TCP/IP 스택의 ARP 테이블 보기	<code>esxcli network ip neighbor list -N vxlan</code>	VTEP 통신 문제 해결

표 1-5. ESXi 호스트의 NSX 설치 확인—호스트 로그 파일

설명	로그 파일	참고
NSX Manager에서	<code>show manager log follow</code>	NSX Manager 로그를 추적합니다. 실시간 문제 해결에 적합합니다.
호스트에 대한 모든 설치 관련 로그	<code>/var/log/esxupdate.log</code>	
호스트 관련 문제	<code>/var/log/vmkernel.log</code>	
VMkernel 주의, 메시지, 경고 및 가용성 보고서	<code>/var/log/vmksummary.log</code> <code>/var/log/vmkwarning.log</code>	
모듈 로드 실패가 캡처됨	<code>/var/log/syslog</code>	IXGBE 드라이버 실패. NSX 모듈 종속성 실패가 핵심 지표입니다.
vCenter에서 ESX Agent Manager가 업데이트를 처리	vCenter 로그, <code>eam.log</code>	

표 1-6. 논리적 스위치 확인—NSX Manager에서 실행되는 명령

설명	NSX Manager에 대한 명령	참고
모든 논리적 스위치 나열	<code>show logical-switch list all</code>	모든 논리적 스위치, API에서 사용될 해당 UUID, 전송 영역 및 <code>vdnscope</code> 를 나열합니다.

표 1-7. 논리적 스위치—NSX Controller에서 실행되는 명령

설명	컨트롤러에 대한 명령	참고
VNI의 소유자인 컨트롤러 찾기	<code>show control-cluster logical-switches vni 5000</code>	출력의 컨트롤러 IP 주소 및 해당 SSH를 적어둡니다.
이 VNI에 대한 이 컨트롤러에 연결된 모든 호스트 찾기	<code>show control-cluster logical-switch connection-table 5000</code>	출력의 소스 IP 주소는 호스트의 관리 인터페이스이고 포트 번호는 TCP 연결의 소스 포트입니다.
이 VNI를 호스트하도록 등록된 VTEP 찾기	<code>show control-cluster logical-switches vtep-table 5002</code>	
이 VNI의 VM에 대해 학습된 MAC 주소 나열	<code>show control-cluster logical-switches mac-table 5002</code>	MAC 주소가 실제로 보고하는 VTEP에 있는지 확인합니다.
VM IP 업데이트에 의해 채워진 ARP 캐시 나열	<code>show control-cluster logical-switches arp-table 5002</code>	ARP 캐시는 180초 후에 만료됩니다.
특정 호스트/컨트롤러 쌍에 대해 어떤 VNI 호스트가 가입했는지 찾기	<code>show control-cluster logical-switches joined-vnis <host_mgmt_ip></code>	

표 1-8. 논리적 스위치—호스트에서 실행되는 명령

설명	호스트에 대한 명령	참고
호스트 VXLAN이 동기화 상태인지 여부 확인	<code>esxcli network vswitch dvs vmware vxlan get</code>	동기화 상태 및 캡슐화에 사용된 포트를 표시합니다.
데이터 경로 캡처를 위한 연결된 VM 및 로컬 스위치 포트 ID 보기	<code>net-stats -l</code>	특정 VM에 대한 vm 스위치 포트를 가져오는 더 나은 방법입니다.
VXLAN 커널 모듈 vdl2가 로드되었는지 확인	<code>esxcli system module get -m vdl2</code>	지정된 모듈의 전체 세부 정보를 표시합니다. 버전을 확인합니다.
올바른 VXLAN VIB 버전이 설치되었는지 확인 설치에서 확인할 VIB에 대한 자세한 내용은 "호스트에 설치된 VIB 및 모듈 이름" 표를 참조하십시오.	<code>esxcli software vib get --vibName esx-vxlan</code> or <code>esxcli software vib get --vibName esx-nsxv</code>	지정된 VIB의 전체 세부 정보를 표시합니다. 버전 및 날짜를 확인합니다.
호스트가 논리적 스위치의 다른 호스트에 대해 알고 있는지 확인	<code>esxcli network vswitch dvs vmware vxlan network vtep list --vxlan-id=5001 --vds-name=Compute_VDS</code>	이 호스트에서 알고 있는 vtep 5001을 호스팅하고 있는 모든 VTEP의 목록을 표시합니다.
논리적 스위치에 대해 제어부가 작동되고 활성 상태인지 확인	<code>esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS</code>	컨트롤러 연결이 작동되고 있고 포트/Mac 개수가 이 호스트의 LS에 있는 VM과 일치하는지 확인합니다.
호스트가 모든 VM의 MAC 주소를 학습했는지 확인	<code>esxcli network vswitch dvs vmware vxlan network mac list --vds-name Compute_VDS --vxlan-id=5000</code>	이 호스트에 있는 VNI 5000 VM에 대한 모든 MAC가 나열되어야 합니다.

표 1-8. 논리적 스위치—호스트에서 실행되는 명령 (계속)

설명	호스트에 대한 명령	참고
호스트가 원격 VM에 대한 ARP 항목을 로컬로 캐시했는지 확인	<code>esxcli network vswitch dvs vmware vxlan network arp list --vds-name Compute_VDS --vxlan-id=5000</code>	호스트가 원격 VM에 대한 ARP 항목을 로컬로 캐시했는지 확인
VM이 LS에 연결되고 로컬 VMKnic에 매핑되었는지 확인. VM dvPort가 매핑된 vmknic ID도 표시	<code>esxcli network vswitch dvs vmware vxlan network port list --vds-name Compute_VDS --vxlan-id=5000</code>	vdrport는 VNI가 라우터에 연결된 경우 항상 나열됩니다.
vmknic ID 및 해당 항목이 매핑된 스위치 포트/업링크 표시	<code>esxcli network vswitch dvs vmware vxlan vmknic list --vds-name=DSwitch-Res01</code>	

표 1-9. 논리적 스위치 확인—로그 파일

설명	로그 파일	참고
호스트는 항상 해당 VNI를 호스팅하는 컨트롤러에 연결됨	<code>/etc/vmware/netcpa/config-by-vsm.xml</code>	이 파일에는 항상 환경의 모든 컨트롤러가 나열되어야 합니다. netcpa 프로세스에 의해 config-by-vsm.xml 파일이 생성됩니다.
config-by-vsm.xml 파일이 vsfwd를 사용하는 NSX Manager에 의해 푸시됨 config-by-vsm.xml 파일이 잘못된 경우 vsfwd 로그 확인	<code>/var/log/vsfwd.log</code>	이 파일을 구문 분석하여 오류를 확인합니다. 프로세스를 시작하려면: <code>/etc/init.d/vShield-Stateful-Firewall stop start</code>
컨트롤러에 대한 연결은 netcpa를 사용하여 설정됨	<code>/var/log/netcpa.log</code>	이 파일을 구문 분석하여 오류를 확인합니다.
논리적 스위치 모듈 로그는 vmkernel.log에 있습니다.	<code>/var/log/vmkernel.log</code>	<code>/var/log/vmkernel.log</code> 에서 “VXLAN: 접두사가 붙은” 논리적 스위치 모듈 로그를 확인합니다.

표 1-10. 논리적 라우팅 확인—NSX Manager에서 실행되는 명령

설명	NSX Manager에 대한 명령	참고
ESG에 대한 명령	<code>show edge</code>	ESG(Edge Services Gateway)에 대한 CLI 명령은 'show edge'로 시작합니다.
DLR 제어 VM에 대한 명령	<code>show edge</code>	DLR(논리적 분산 라우터) 제어 VM에 대한 CLI 명령은 'show edge'로 시작합니다.
DLR에 대한 명령	<code>show logical-router</code>	DLR(논리적 분산 라우터)에 대한 CLI 명령은 show logical-router로 시작합니다.
모든 Edge 나열	<code>show edge all</code>	중앙 CLI를 지원하는 모든 Edge를 나열합니다.
Edge에 대한 모든 서비스 및 배포 세부 정보 나열	<code>show edge edgeID</code>	Edge Service Gateway 정보를 표시합니다.

표 1-10. 논리적 라우팅 확인—NSX Manager에서 실행되는 명령 (계속)

설명	NSX Manager에 대한 명령	참고
Edge에 대한 명령 옵션 나열	<code>show edge edgeID ?</code>	세부 정보(예: 버전, 로그, NAT, 라우팅 테이블, 방화벽, 구성, 인터페이스 및 서비스)를 표시합니다.
라우팅 세부 정보 표시	<code>show edge edgeID ip ?</code>	라우팅 정보, BGP, OSPF 및 기타 세부 정보를 표시합니다.
라우팅 테이블 표시	<code>show edge edgeID ip route</code>	Edge의 라우팅 테이블을 표시합니다.
인접 라우팅 표시	<code>show edge edgeID ip ospf neighbor</code>	인접 라우팅 관계를 표시합니다.
논리적 라우터 연결 정보 표시	<code>show logical-router host hostID connection</code>	연결된 LIF의 수가 올바른지, 팀 구성 정책이 올바른지 및 적절한 vDS가 사용되고 있는지 확인합니다.
호스트에서 실행되고 있는 모든 논리적 라우터 인스턴스 나열	<code>show logical-router host hostID dlr all</code>	LIF 및 경로 수를 확인합니다. 컨트롤러 IP는 논리적 라우터에 대한 모든 호스트에서 동일해야 합니다. 제어부 활성 상태는 yes 여야 합니다. --brief 는 간단한 응답을 제공합니다.
호스트의 라우팅 테이블 확인	<code>show logical-router host hostID dlr dlrID route</code>	컨트롤러에서 전송 영역의 모든 호스트로 푸시하는 라우팅 테이블입니다. 모든 호스트에서 동일해야 합니다. 일부 호스트에서 일부 경로가 누락된 경우 위에서 설명한 컨트롤러에서 동기화 명령을 시도합니다. E 플래그는 경로가 ECMP를 통해 학습되었음을 의미합니다.
LIF에서 호스트의 DLR 확인	<code>show logical-router host hostID dlr dlrID interface (all intName) verbose</code>	LIF 정보가 컨트롤러에서 호스트로 푸시됩니다. 이 명령을 사용하여 호스트가 알아야 하는 모든 LIF에 대해 알고 있는지 확인합니다.

표 1-11. 논리적 라우팅 확인—NSX Controller에서 실행되는 명령

설명	NSX Controller에 대한 명령	참고
모든 논리적 라우터 인스턴스 찾기	<code>show control-cluster logical-routers instance all</code>	논리적 라우터 인스턴스 및 논리적 라우터 인스턴스가 있는 전송 영역의 모든 호스트가 나열됩니다. 또한 이 논리적 라우터를 제공하는 컨트롤러를 표시합니다.
각 논리적 라우터의 세부 정보 표시	<code>show control-cluster logical-routers instance 0x570d4555</code>	IP 열에는 이 DLR이 있는 모든 호스트의 vmk0 IP 주소가 표시됩니다.
논리적 라우터에 연결된 모든 인터페이스 표시	<code>show control-cluster logical-routers interface-summary 0x570d4555</code>	IP 열에는 이 DLR이 있는 모든 호스트의 vmk0 IP 주소가 표시됩니다.

표 1-11. 논리적 라우팅 확인—NSX Controller에서 실행되는 명령 (계속)

설명	NSX Controller에 대한 명령	참고
이 논리적 라우터에 의해 학습된 모든 경로 표시	<code>show control-cluster logical-routers routes 0x570d4555</code>	IP 열에는 이 DLR이 있는 모든 호스트의 vmk0 IP 주소가 표시됩니다.
설정된 모든 네트워크 연결 표시(<code>net stat output</code> 과 같음)	<code>show network connections of-type tcp</code>	문제 해결 중인 호스트가 <code>netcpa</code> 를 통해 컨트롤러에 연결되었는지 확인합니다.
컨트롤러에서 호스트로의 인터페이스 동기화	<code>sync control-cluster logical-routers interface-to-host <logical-router-id> <host-ip></code>	새 인터페이스가 논리적 라우터에 연결되었으나 모든 호스트와 동기화되지 않는 경우에 유용합니다.
컨트롤러에서 호스트로의 경로 동기화	<code>sync control-cluster logical-routers route-to-host <logical-router-id> <host-ip></code>	일부 호스트에서 일부 경로가 누락되었으나 대부분의 호스트에서 사용할 수 있는 경우에 유용합니다.

표 1-12. 논리적 라우팅 확인—Edge에서 실행되는 명령

설명	Edge 또는 논리적 라우터 제어 VM에 대한 명령	참고
구성 표시	<code>show configuration <global bgp ospf ...></code>	
학습된 경로 표시	<code>show ip route</code>	라우팅 및 전달 테이블이 동기화되어 있는지 확인합니다.
전달 테이블 표시	<code>show ip forwarding</code>	라우팅 및 전달 테이블이 동기화되어 있는지 확인합니다.
논리적 분산 라우터 인터페이스 표시	<code>show interface</code>	출력에 표시되는 첫 번째 NIC는 논리적 분산 라우터 인터페이스입니다. 논리적 분산 라우터 인터페이스는 해당 VM의 실제 vNIC가 아닙니다. 논리적 분산 라우터에 연결된 모든 서브넷의 유형은 내부입니다.
다른 인터페이스(관리) 표시	<code>show interface</code>	관리/HA 인터페이스가 논리적 라우터 제어 VM의 실제 vNIC입니다. IP 주소를 지정하지 않고 HA가 사용되도록 설정되면 169.254.x.x/30이 사용됩니다. 관리 인터페이스에 IP 주소가 지정되면 여기에 표시됩니다.
프로토콜 디버그	<code>debug ip ospf</code> <code>debug ip bgp</code>	구성 문제(예: 일치하지 않는 OSPF 영역, 타이머 및 잘못된 ASN)를 확인하는 데 유용합니다. 참고: 출력은 Edge의 콘솔(SSH 세션을 통해서가 아님)에만 표시됩니다.

표 1-12. 논리적 라우팅 확인—Edge에서 실행되는 명령 (계속)

설명	Edge 또는 논리적 라우터 제어 VM에 대한 명령	참고
OSPF 명령	<pre>show configuration ospf show ip ospf interface show ip ospf neighbor show ip route ospf show ip ospf database show tech-support(문자열 “EXCEPTION” 및 “PROBLEM” 찾 기)</pre>	
BGP 명령	<pre>show configuration bgp show ip bgp neighbor show ip bgp show ip route bgp show ip forwarding show tech-support (문자열 “EXCEPTION” 및 “PROBLEM” 찾 기)</pre>	

표 1-13. 논리적 라우팅 확인—호스트의 로그 파일

설명	로그 파일	참고
논리적 분산 라우터 인스턴스 정보가 vsfwd에 의해 호스트에 푸시되고 XML 형식으로 저장됩니다.	/etc/vmware/netcpa/config-by-vsm.xml	<p>논리적 분산 라우터 인스턴스가 호스트에 없으면 먼저 이 파일을 확인하여 인스턴스가 나열되는지 검토합니다.</p> <p>인스턴스가 없으면 vsfwd를 다시 시작합니다.</p> <p>또한 이 파일을 사용하여 모든 컨트롤러가 호스트에 알려져 있는지 확인합니다.</p>
위 파일이 vsfwd를 사용하는 NSX Manager에 의해 푸시됨 config-by-vsm.xml 파일이 잘못된 경우 vsfwd 로그 확인	/var/log/vsfwd.log	<p>이 파일을 구문 분석하여 오류를 확인합니다.</p> <p>프로세스를 다시 시작하려면: /etc/init.d/vShield-Stateful-Firewall stop start</p>
컨트롤러에 대한 연결은 netcpa를 사용하여 설정됨	/var/log/netcpa.log	이 파일을 구문 분석하여 오류를 확인합니다.
논리적 스위치 모듈 로그는 vmkernel.log에 있습니다.	/var/log/vmkernel.log	/var/log/vmkernel.log에서 “vxlan: 접두사가 붙은” 논리적 스위치 모듈 로그를 확인합니다.

표 1-14. 컨트롤러 디버깅—NSX Manager에서 실행되는 명령

설명	NSX Manager에 대한 명령	참고
상태가 있는 모든 컨트롤러 나열	show controller list all	모든 컨트롤러 및 해당 실행 상태 목록을 표시합니다.

표 1-15. 컨트롤러 디버깅—NSX Controller에서 실행되는 명령

설명	컨트롤러에 대한 명령	참고
컨트롤러 클러스터 상태 확인	<code>show control-cluster status</code>	항상 '가입 완료' 및 '클러스터 대부분에 연결됨'을 표시해야 합니다.
플래핑 연결 및 메시지에 대한 통계 확인	<code>show control-cluster core stats</code>	삭제된 카운터는 변경되지 않습니다.
초기 또는 다시 시작 이후의 클러스터 가입과 관련된 노드 작업 표시	<code>show control-cluster history</code>	클러스터 가입 문제 해결에 유용합니다.
클러스터의 노드 목록 표시	<code>show control-cluster startup-nodes</code>	목록에 활성 클러스터 노드만 포함되어야 할 필요는 없습니다. 현재 배포된 모든 컨트롤러의 목록이어야 합니다. 이 목록은 시작 컨트롤러가 클러스터의 다른 컨트롤러에 연결하는 데 사용됩니다.
설정된 모든 네트워크 연결 표시(<code>net stat output</code> 과 같음)	<code>show network connections of-type tcp</code>	문제 해결 중인 호스트가 <code>netcpa</code> 를 통해 컨트롤러에 연결되었는지 확인합니다.
컨트롤러 프로세스 다시 시작	<code>restart controller</code>	주 컨트롤러 프로세스만 다시 시작합니다. 클러스터에 강제로 다시 연결합니다.
컨트롤러 노드 재부팅	<code>restart system</code>	컨트롤러 VM을 재부팅합니다.

표 1-16. 컨트롤러 디버깅—NSX Controller에 대한 로그 파일

설명	로그 파일	참고
컨트롤러 기록 및 최근 가입, 다시 시작 등 표시	<code>show control-cluster history</code>	특히 클러스터링과 관련된 컨트롤러 문제를 해결하기에 유용한 도구입니다.
느린 디스크 확인	<code>show log cloudnet/cloudnet_java-zookeeper<timestamp>.log filtered-by fsync</code>	느린 디스크 문제를 확인하는 확실한 방법은 <code>cloudnet_java-zookeeper</code> 로그에서 "fsync" 메시지를 찾는 것입니다. 동기화하는 데 1초가 넘게 걸리면 ZooKeeper가 이 메시지를 인쇄하며, 해당 시간에 해당 디스크가 다른 작업에 사용되고 있음을 나타냅니다.
느리거나 고장난 디스크 확인	<code>show log syslog filtered-by collectd</code>	"collectd"에 대한 자세한 출력에 표시되는 것과 같은 메시지는 느리거나 고장난 디스크와 상호 연관될 수 있습니다.
디스크 공간 사용량 확인	<code>show log syslog filtered-by freespace:</code>	공간 사용량이 임계값에 도달하면 디스크에서 오래된 로그 및 기타 파일을 주기적으로 정리하는 "freespace"라는 백그라운드 작업이 있습니다. 일부 경우에 디스크가 작고 매우 빠르게 채워질 경우 <code>freespace</code> 메시지가 자주 표시됩니다. 이는 디스크가 꽉 찼음을 나타낼 수 있습니다.
현재 활성 상태인 클러스터 멤버 찾기	<code>show log syslog filtered-by Active cluster members</code>	현재 활성 상태인 클러스터 멤버의 노드 ID를 나열합니다. 이 메시지가 항상 출력되는 것은 아니므로 이전 <code>syslog</code> 를 조사해야 할 수 있습니다.

표 1-16. 컨트롤러 디버깅—NSX Controller에 대한 로그 파일 (계속)

설명	로그 파일	참고
핵심 컨트롤러 로그 표시	show log cloudnet/cloudnet_java-zookeeper.20150703-165223.3702.log	여러 zookeeper 로그가 있을 수 있습니다. 최신 타임 스탬프가 지정된 파일을 찾으십시오. 이 파일에는 컨트롤러 클러스터 마스터 선택에 대한 정보와 컨트롤러의 분산 특성과 관련된 기타 정보가 포함되어 있습니다.
핵심 컨트롤러 로그 표시	show log cloudnet/cloudnet_nsx-controller.root.log.INFO.20150703-165223.3668	주 컨트롤러 작동 로그(예: LIF 생성, 1234의 연결 수신기, 샤딩)

표 1-17. 분산 방화벽 확인—NSX Manager에서 실행되는 명령

설명	NSX Manager에 대한 명령	참고
VM 정보 표시	show vm vmID	세부 정보(예: DC, 클러스터, 호스트, VM 이름, vNIC, 설치된 dvfilter)
특정 가상 NIC 정보 표시	show vnic icID	세부 정보(예: vNIC 이름, mac 주소, pg, 적용된 필터)
모든 클러스터 정보 표시	show dfw cluster all	클러스터 이름, 클러스터 ID, 데이터센터 이름, 방화벽 상태
특정 클러스터 정보 표시	show dfw cluster clusterID	호스트 이름, 호스트 ID, 설치 상태
dfw 관련 호스트 정보 표시	show dfw host hostID	VM 이름, VM ID, 전원 상태
dvfilter 내의 세부 정보 표시	show dfw host hostID filter filterID <option>	각 vNIC에 대한 규칙, 통계, 주소 집합 등 나열
VM에 대한 DFW 정보 표시	show dfw vm vmID	VM의 이름, vNIC ID, 필드 등 표시
vNIC 세부 정보 표시	show dfw vnic vnicID	vNIC 이름, ID, MAC 주소, 포트 그룹, 필터 표시
vNIC별 설치된 필터 나열	show dfw host hostID summarize-dvfilter	원하는 VM/vNIC 찾기 및 다음 명령에 필터로 사용할 이름 필터 가져오기
특정 필터/vNIC에 대한 규칙 표시	show dfw host hostID filter filterID rules show dfw vnic nicID	
주소 집합에 대한 세부 정보 표시	show dfw host hostID filter filterID addrsets	규칙에는 주소 집합만 표시되며, 이 명령은 주소 집합에 포함된 내용을 확장하는 데 사용될 수 있습니다.
vNIC별 spoofguard 세부 정보	show dfw host hostID filter filterID spoofguard	SpoofGuard가 사용되도록 설정되어 있는지와 현재 IP/MAC를 확인합니다.

표 1-17. 분산 방화벽 확인—NSX Manager에서 실행되는 명령 (계속)

설명	NSX Manager에 대한 명령	참고
흐름 레코드의 세부 정보 표시	<code>show dfw host hostID filter filterID flows</code>	Flow Monitoring이 사용되도록 설정된 경우 호스트는 흐름 정보를 NSX Manager에 주기적으로 전송합니다. 이 명령을 사용하여 vNIC별 흐름을 확인합니다.
vNIC에 대한 각 규칙의 통계 표시	<code>show dfw host hostID filter filterID stats</code>	규칙을 준수하는지 확인하는 데 유용합니다.

표 1-18. 분산 방화벽 확인—호스트에서 실행되는 명령

설명	호스트에 대한 명령	참고
호스트에 다운로드된 VIB를 나열합니다. 설치에서 확인할 VIB에 대한 자세한 내용은 "호스트에 설치된 VIB 및 모듈 이름" 표를 참조하십시오.	<code>esxcli software vib list grep esx-vmip</code> or <code>esxcli software vib list grep esx-nsxv</code>	올바른 vib 버전이 다운로드되는지 확인합니다.
현재 로드된 시스템 모듈에 대한 세부 정보 설치에서 확인할 모듈에 대한 자세한 내용은 "호스트에 설치된 VIB 및 모듈 이름" 표를 참조하십시오.	<code>esxcli system module get -m vsip</code> or <code>esxcli system module get -m nsx-vmip</code>	모듈이 설치/로드되었는지 확인합니다.
프로세스 목록	<code>ps grep vsfwd</code>	vsfwd 프로세스가 여러 스레드를 사용해서 실행 중인지 확인합니다.
데몬 명령	<code>/etc/init.d/vShield-Stateful-Firewall {start stop status restart}</code>	데몬이 실행 중인지 확인하고 필요한 경우 다시 시작합니다.
네트워크 연결 표시	<code>esxcli network ip connection list grep 5671</code>	호스트가 TCP를 통해 NSX Manager에 연결되어 있는지 확인합니다.

표 1-19. 분산 방화벽 확인—호스트에 대한 로그 파일

설명	로그	참고
프로세스 로그	<code>/var/log/vsfwd.log</code>	vsfwd 데몬 로그, vsfwd 프로세스에 유용, NSX Manager 연결 및 RabbitMQ 문제 해결
패킷 로그 전용 파일	<code>/var/log/dfwpktlogs.log</code>	패킷 로그에 대한 전용 로그 파일
dvfilter에 패킷 캡처	<code>pktcap-uw --dvfilter nic-1413082-eth0-vmware-sfw.2 --outfile test.pcap</code>	

NSX 호스트 상태 점검

NSX Manager 중앙 CLI에서 각 ESXi 호스트의 상태를 확인할 수 있습니다.

상태는 위험, 비정상 또는 정상으로 보고됩니다.

예):

```
nsxmgr> show host host-30 health-status
status: HEALTHY

nsxmgr> show host host-29 health-status
UNHEALTHY, Standard Switch vSwitch1 has no uplinks.
UNHEALTHY, Storage volume datastore1 has no enough free spaces: 19.% free.
status: UNHEALTHY

nsxmgr> show host host-28 health-status
CRITICAL, VXLAN VDS vds-site-a VNI 200000 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 200003 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 5000 multicast addr is not synchronized with VSM: 0.0.0.0.
Status: CRITICAL
```

NSX Manager API를 통해 `host-check` 명령도 호출할 수 있습니다.

NSX 인프라 문제 해결

2

NSX 준비는 4단계로 진행되는 프로세스입니다.

- 1 NSX Manager를 vCenter Server에 연결합니다. NSX Manager와 vCenter Server 간에는 일대일 관계가 있습니다.
 - a vCenter Server에 등록합니다.
- 2 NSX Controller를 배포합니다(유니캐스트 또는 하이브리드 모드의 논리적 스위칭, 분산 라우팅 또는 VXLAN에만 필요합니다. DFW(분산 방화벽)만 사용하는 경우에는 컨트롤러가 필요하지 않습니다.).
- 3 호스트 준비: 클러스터의 모든 호스트에 VXLAN, DFW 및 DLR용 VIB를 설치합니다. Rabbit MQ 기반 메시징 인프라를 구성합니다. 방화벽을 사용하도록 설정합니다. 호스트의 NSX 사용 준비가 되었음을 컨트롤러에 알립니다.
- 4 IP 풀 설정 구성 및 VXLAN 구성: 클러스터의 모든 호스트에 VTEP 포트 그룹 및 VMKNIC를 만듭니다. 이 단계 동안 전송 VLAN ID, 팀 구성 정책 및 MTU를 설정할 수 있습니다.

설치 및 각 단계의 구성에 대한 자세한 내용은 "NSX 설치 가이드" 및 "NSX 관리 가이드"를 참조하십시오. 본 장은 다음 항목을 포함합니다.

- [호스트 준비](#)
- [NSX Manager 문제 해결](#)
- [논리적 네트워크 준비: VXLAN 전송](#)
- [논리적 스위치 포트 그룹이 동기화되지 않음](#)

호스트 준비

vSphere ESX Agent Manager는 ESXi 호스트에 vSphere 설치 번들(VIB)을 배포합니다.

호스트에 배포하려면 DNS가 호스트, vCenter Server 및 NSX Manager에 구성되어 있어야 합니다. 배포를 위해 ESXi 호스트를 재부팅할 필요는 없지만 VIB의 업데이트 또는 제거를 위해서는 ESXi 호스트를 재부팅해야 합니다.

VIB는 NSX Manager에서 호스팅되며 zip 파일로도 제공됩니다.

이 파일은 <https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties>에서 액세스할 수 있습니다. 다운로드할 수 있는 zip 파일은 NSX 및 ESXi 버전에 따라 다릅니다. 예를 들어 NSX 6.3.0에서 vSphere 6.0 호스트는 파일 <https://<NSX-Manager-IP>/bin/vdn/vibs-6.3.0/6.0-buildNumber/vxlan.zip>을 사용합니다.

```
# 5.5 VDN EAM Info
VDN_VIB_PATH.1=/bin/vdn/vibs-6.3.0/5.5-4744075/vxlan.zip
VDN_VIB_VERSION.1=4744075
VDN_HOST_PRODUCT_LINE.1=embeddedEsx
VDN_HOST_VERSION.1=5.5.*

# 6.0 VDN EAM Info
VDN_VIB_PATH.2=/bin/vdn/vibs-6.3.0/6.0-4744062/vxlan.zip
VDN_VIB_VERSION.2=4744062
VDN_HOST_PRODUCT_LINE.2=embeddedEsx
VDN_HOST_VERSION.2=6.0.*

# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.0/6.5-4744074/vxlan.zip
VDN_VIB_VERSION.3=4744074
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*

# Single Version associated with all the VIBs pointed by above VDN_VIB_PATH(s)
VDN_VIB_VERSION=6.3.0.4744320

# Legacy vib location. Used by code to discover available legacy vibs.
LEGACY_VDN_VIB_PATH_FS=/common/em/components/vdn/vibs/legacy/
LEGACY_VDN_VIB_PATH_WEB_ROOT=/bin/vdn/vibs/legacy/
```

호스트에 설치되는 VIB는 NSX 및 ESXi 버전에 따라 다릅니다.

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

esxcli software vib list 명령을 사용하여 설치된 VIB를 볼 수 있습니다.

```
[root@esx-01a:~] esxcli software vib list | grep -e vsip -e vxlan
esx-vsip                6.0.0-0.0.XXXXXXX    VMware  VMwareCertified
2016-04-20
esx-vxlan                6.0.0-0.0.XXXXXXX    VMware  VMwareCertified
2016-04-20
```


or

```
esxcli software vib list | grep nsxv
esx-nsxv                6.0.0-0.0.XXXXXXX      VMware  VMwareCertified
2017-08-11
```

호스트 준비 중에 발생하는 일반적인 문제

호스트 준비 중에 발생할 수 있는 일반적인 문제는 다음과 같습니다.

- EAM이 VIB를 배포하지 못합니다.
 - 호스트에서 DNS가 잘못 구성되어 있기 때문일 수 있습니다.
 - 방화벽이 ESXi, NSX Manager 및 vCenter Server 간의 필수 포트를 차단하고 있을 수 있습니다.

대부분의 문제는 **해결(Resolve)** 옵션을 클릭하여 해결됩니다. **설치 상태가 준비되지 않음** 를 참조하십시오.
- 이전 버전의 이전 VIB가 이미 설치되어 있습니다. 이 경우 사용자가 호스트를 재부팅해야 합니다.
- NSX Manager 및 vCenter Server에서 통신 문제가 발생합니다. **Networking & Security** 플러그인의 **호스트 준비(Host Preparation)** 탭에 일부 호스트가 제대로 표시되지 않습니다.
 - vCenter Server에서 모든 호스트 및 클러스터를 열거할 수 있는지 확인합니다.

문제가 **해결(Resolve)** 옵션을 사용하여 해결되지 않으면 **해결 옵션을 사용하여 문제가 해결되지 않음**을 참조하십시오.

호스트 준비(VIB) 문제 해결

- 호스트에 대한 통신 채널 상태를 확인합니다. **통신 채널 상태 확인**를 참조하십시오.
- vSphere ESX Agent Manager에 오류가 있는지 확인합니다.

vCenter 홈 > 관리 > vCenter Server Extensions > vSphere ESX Agent Manager(vCenter home > Administration > vCenter Server Extensions > vSphere ESX Agent Manager)

vSphere ESX Agent Manager에서 접두사로 “VCNS160”이 붙어 있는 에이전시의 상태를 확인합니다. 에이전시가 불량 상태인 경우 해당 에이전시를 선택하고 문제를 확인합니다.

Agency	State	Status	Optimized Deployment
_VCNS_160_Management & Edge CI...	Enabled	✓ Normal	✓
_VCNS_160_Compute Cluster A_VMwa...	Enabled	⚠ Alert	✓

Trigger Time	Agency	Issue	Host	Agent VM
Thu Apr 28 12:03:12 GMT-0...	_VCNS_160_Compute Clu...	Agent VIB module is not installed	esx-01a.corp.local	

- 문제가 있는 호스트에서 `tail /var/log/esxupdate.log` 명령을 실행합니다.

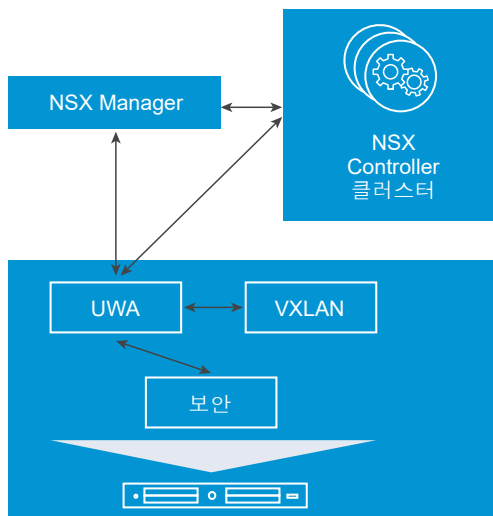
```

2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vc...
o /tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exceptio
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/
site-packages/vmware/esx5update/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/
site-packages/vmware/esximage/Transaction.py", line 73, in DownloadMetadatas
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('h
fd3f37ad4c', None, "('https://vc...:443/eam/vib?id=facdb160-216
rlopen error [Errno -3] Temporary failure in name resolution>')")
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<
  
```

호스트 준비(UWA) 문제 해결

NSX Manager는 클러스터의 모든 호스트에서 2개의 User World Agent를 구성합니다.

- 메시징 버스 UWA(vsfwd)
- 제어부 UWA(netcpa)

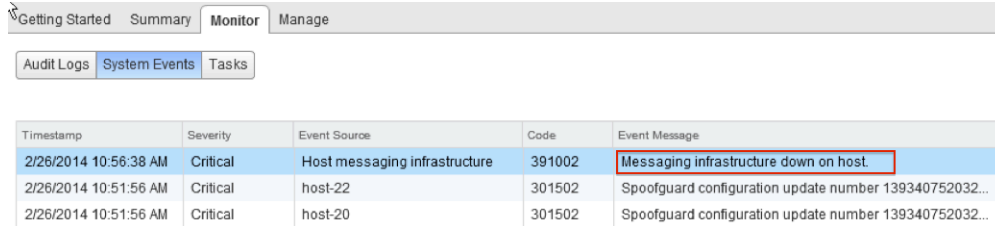


드문 경우 VIB 설치가 성공하지만 일부 이유로 인해 User World Agent 중 하나 또는 둘 다가 제대로 작동하지 않을 수 있습니다. 이 경우 다음과 같은 현상이 나타날 수 있습니다.

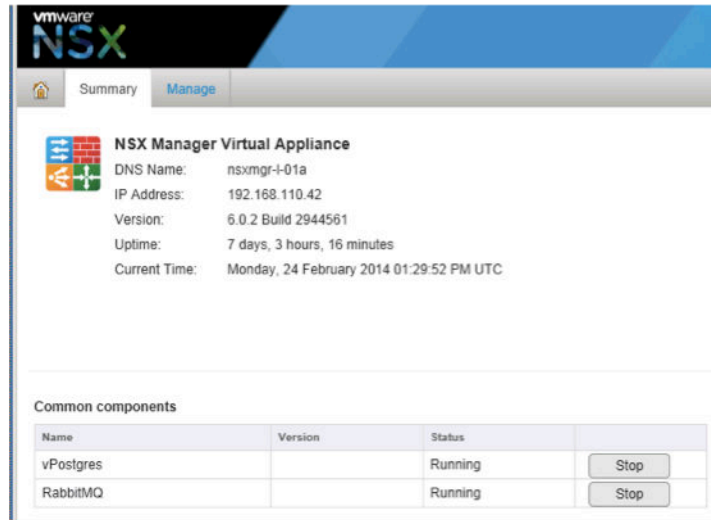
- 방화벽에 잘못된 상태가 표시됩니다.



- 하이퍼바이저 및 컨트롤러 사이의 제어부가 작동 중단됩니다. NSX Manager 시스템 이벤트를 확인합니다. "NSX 로깅 및 시스템 이벤트"를 참조하십시오.



둘 이상의 ESXi 호스트가 영향을 받는 경우 요약(Summary) 탭의 NSX Manager 장치 Web UI에서 메시지 버스 서비스의 상태를 확인하십시오. RabbitMQ가 중지되면 다시 시작하십시오.



메시지 버스 서비스가 NSX Manager에서 활성 상태인 경우:

- ESXi 호스트에서 `/etc/init.d/vShield-Stateful-Firewall status` 명령을 실행하여 호스트의 메시지 버스 User World Agent 상태를 확인합니다.

```
[root@esx-01a:~] /etc/init.d/vShield-Stateful-Firewall status
vShield-Stateful-Firewall is running
```

- `/var/log/vsfwd.log`에서 호스트에 대한 메시지 버스 User World Agent 로그를 확인합니다.

- ESXi 호스트에서 `esxcfg-advcfg -l | grep Rmq` 명령을 실행하여 모든 Rmq 변수를 표시합니다. 16개의 Rmq 변수가 표시되어야 합니다.

```
[root@esx-01a:~] esxcfg-advcfg -l | grep Rmq
/UserVars/RmqIpAddress [String] : Connection info for RMQ Broker
/UserVars/RmqUsername [String] : RMQ Broker Username
/UserVars/RmqPassword [String] : RMQ Broker Password
/UserVars/RmqVHost [String] : RMQ Broker VHost
/UserVars/RmqVsmRequestQueue [String] : RMQ Broker VSM Request Queue
/UserVars/RmqPort [String] : RMQ Broker Port
/UserVars/RmqVsmExchange [String] : RMQ Broker VSM Exchange
/UserVars/RmqClientPeerName [String] : RMQ Broker Client Peer Name
/UserVars/RmqHostId [String] : RMQ Broker Client HostId
/UserVars/RmqHostVer [String] : RMQ Broker Client HostVer
/UserVars/RmqClientId [String] : RMQ Broker Client Id
/UserVars/RmqClientToken [String] : RMQ Broker Client Token
/UserVars/RmqClientRequestQueue [String] : RMQ Broker Client Request Queue
/UserVars/RmqClientResponseQueue [String] : RMQ Broker Client Response Queue
/UserVars/RmqClientExchange [String] : RMQ Broker Client Exchange
/UserVars/RmqSslCertSha1ThumbprintBase64 [String] : RMQ Broker Server Certificate base64 Encoded
Sha1 Hash
```

- ESXi 호스트에서 `esxcfg-advcfg -g /UserVars/RmqIpAddress` 명령을 실행합니다. 출력에는 NSX Manager IP 주소가 표시되어야 합니다.

```
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.15
```

- ESXi 호스트에서 `esxcli network ip connection list | grep 5671` 명령을 실행하여 활성 메시징 버스 연결을 확인합니다.

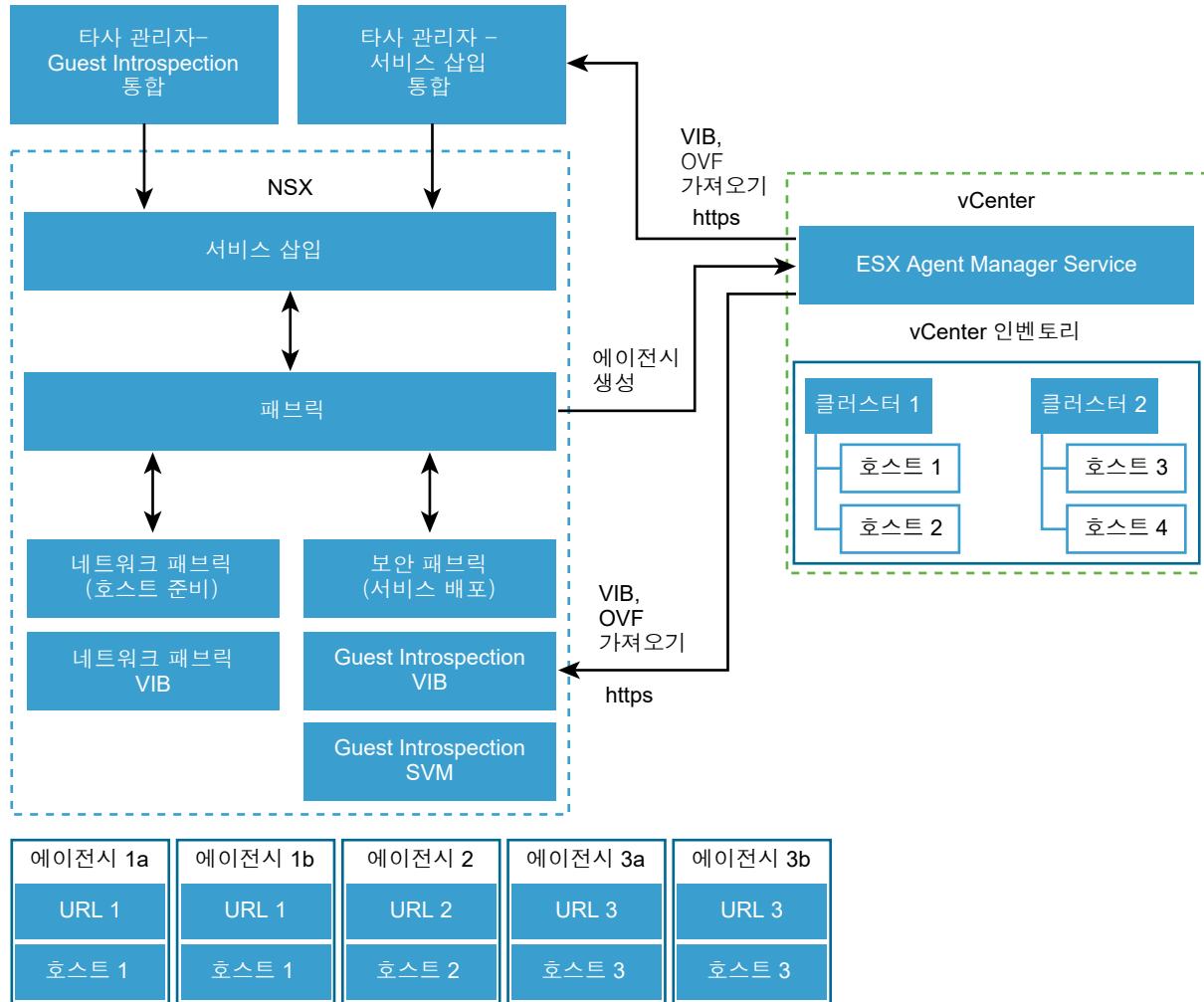
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp          0      0 192.168.110.51:29969      192.168.110.15:5671      ESTABLISHED
35505 newreno  vsfwd
tcp          0      0 192.168.110.51:29968      192.168.110.15:5671      ESTABLISHED
35505 newreno  vsfwd
```

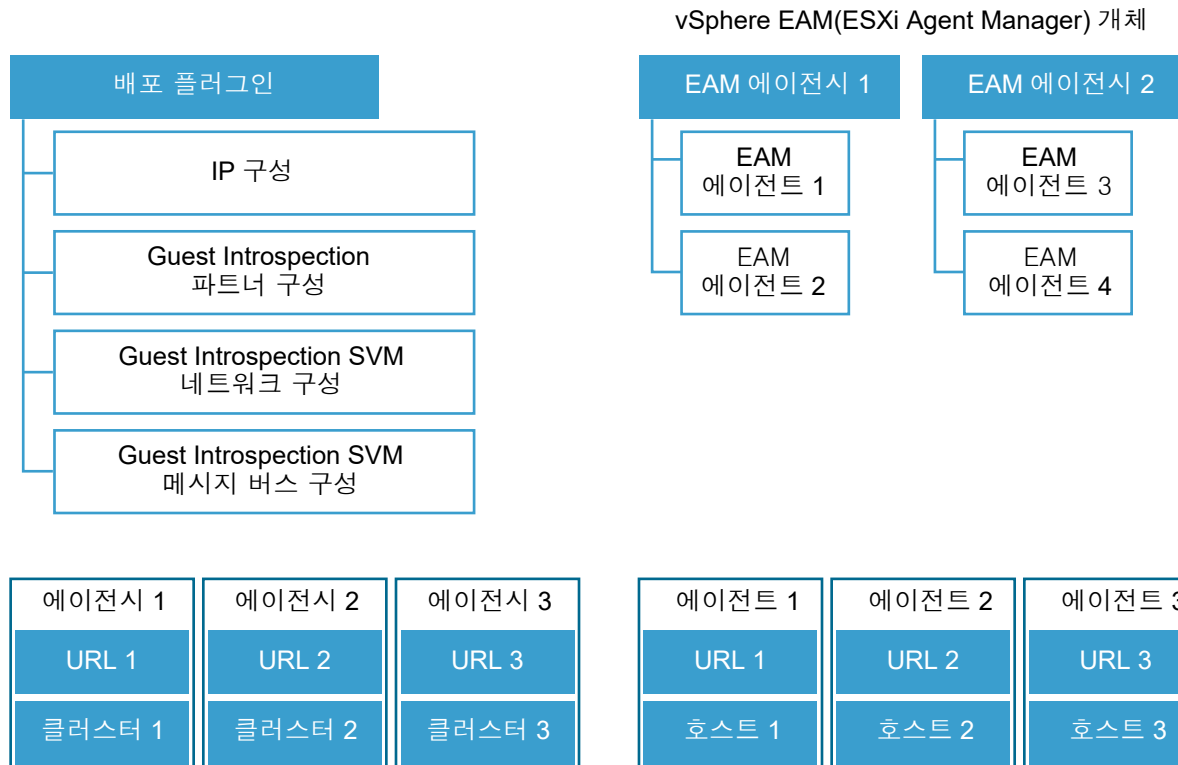
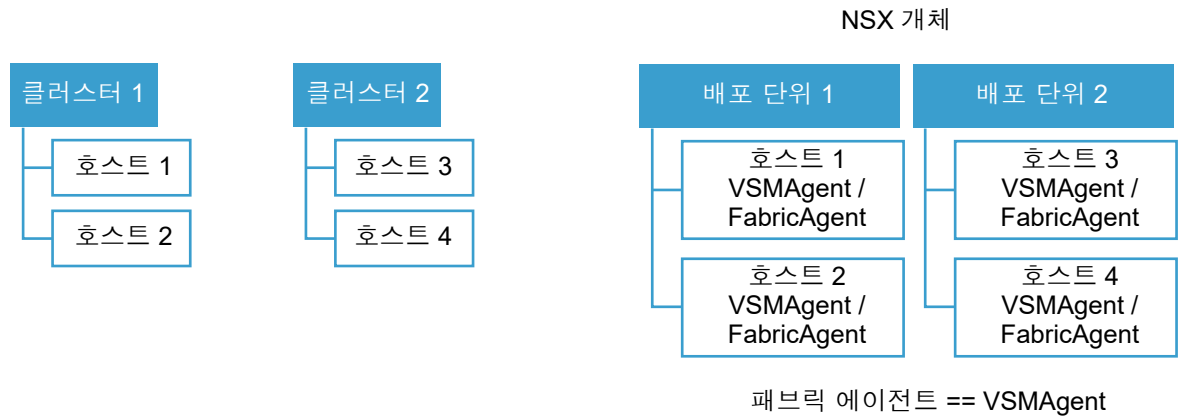
제어부 에이전트와 관련된 문제는 [제어부 에이전트\(netcpa\)](#) 문제를 참조하십시오.

호스트 준비 아키텍처 이해

이 항목에서는 기본 호스트 준비 아키텍처에 대해 설명합니다.

- 네트워크 패브릭을 배포하려면 **호스트 준비(Host Preparation)** 탭으로 이동합니다.
- 보안 패브릭을 배포하려면 **서비스 배포(Service Deployment)** 탭으로 이동합니다.





다음과 같은 용어는 호스트 준비 아키텍처를 이해하는 데 도움이 될 수 있습니다.

패브릭

패브릭은 **NSX Manager**가 호스트에서 네트워크 및 보안 패브릭 서비스를 설치하기 위해 **ESX Agent Manager**와 상호 작용하는 소프트웨어 계층입니다.

네트워크 패브릭

네트워크 패브릭 서비스가 클러스터에 배포됩니다. 네트워크 패브릭 서비스에는 호스트 준비, **VXLAN**, 분산 라우팅, 분산된 방화벽 및 메시지 버스가 포함됩니다.

보안 패브릭

보안 패브릭 서비스가 클러스터에 배포됩니다. 보안 패브릭 서비스에는 **Guest Introspection** 및 파트너 보안 솔루션이 포함됩니다.

패브릭 에이전트

패브릭 에이전트는 **NSX Manager** 데이터베이스에 있는 패브릭 서비스 및 호스트의 조합입니다. 네트워킹 또는 보안 패브릭 서비스가 배포된 클러스터에 대해 호스트당 하나의 패브릭 에이전트가 생성됩니다.

VSM 에이전트라고도 합니다.

배포 단위

NSX Manager 데이터베이스의 패브릭 서비스 및 클러스터 조합입니다. 배포 단위는 네트워킹 및 보안 서비스가 설치되기 전에 생성되어야 합니다.

ESX Agent Manager 에이전트

ESX Agent Manager 에이전트는 **vCenter Server** 데이터베이스의 서비스 사양 및 호스트의 조합입니다. **ESX Agent Manager** 에이전트는 **NSX** 패브릭 에이전트에 매핑됩니다.

ESX Agent Manager 에이전시

ESX Agent Manager 에이전시는 **vCenter Server** 데이터베이스의 사양 및 클러스터 조합입니다. 사양은 **ESX Agent Manager** 에이전트 및 **VIB**, **OVF** 및 관리되는 해당 구성(예: 데이터스토어 및 네트워크 설정)을 설명합니다.

NSX Manager는 준비하려는 각 클러스터에 대해 **ESX Agent Manager** 에이전시를 생성합니다.

ESX Agent Manager 에이전시는 **NSX** 배포 단위에 매핑됩니다. 배포 단위의 **NSX Manager** 데이터베이스와 **ESX Agent Manager** 에이전시의 **vCenter ESX Agent Manager** 데이터베이스는 동기화 상태여야 합니다. 드문 경우에 두 데이터베이스가 동기화되지 않으면 **NSX**는 사용자에게 해당 상태를 알리기 위한 이벤트 및 경보를 트리거합니다. **NSX Manager**는 각 **ESX Agent Manager** 에이전시에 대해 해당 데이터베이스의 배포 단위를 생성합니다.

NSX Manager는 준비하려는 각 클러스터에 대해 **ESX Agent Manager** 에이전시를 생성합니다. **NSX Manager**는 각 **ESX Agent Manager** 에이전시에 대해 해당 데이터베이스의 배포 단위를 생성합니다. **ESX Agent Manager** 에이전시 1개 = 배포 단위 1개

다음과 같은 방식으로 에이전시를 확인할 수 있습니다.

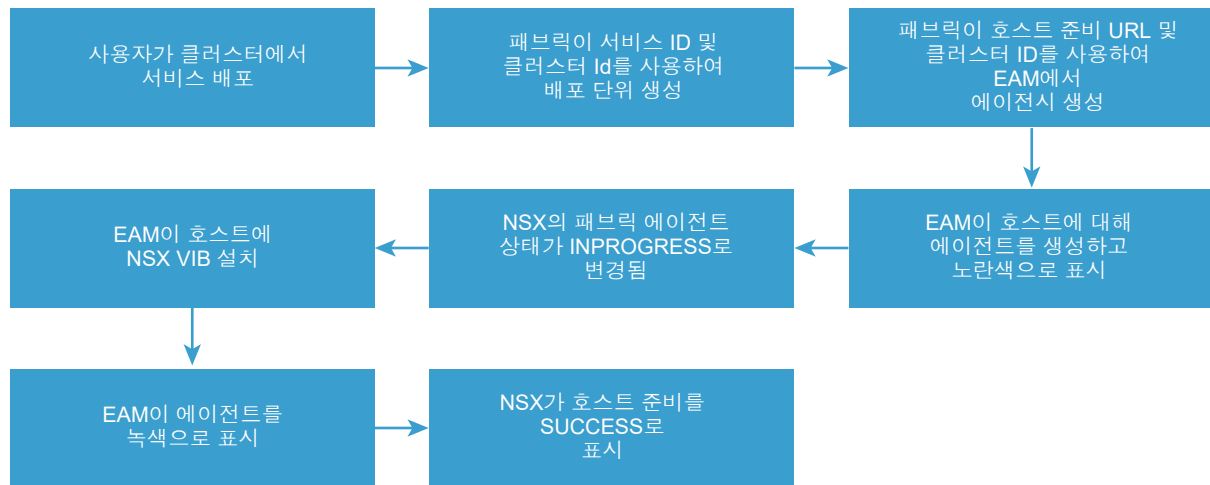
- EAM MOB <https://<VC-hostname/IP>/eam/mob/>에서
- vSphere Web Client에서:
 - **VCenter Solutions Manager > vSphere ESX Agent Manager > 관리(Manage)**로 이동합니다.
 - **ESX 에이전시(ESX Agencies)**에서 에이전시를 볼 수 있습니다(호스트에 대해 준비된 클러스터당 1개).

배포 단위의 수명 주기는 에이전시의 수명 주기와 관련되어 있으며 **ESX Agent Manager**에서 에이전시를 제거하면 **NSX**에서 해당 배포 단위가 제거됩니다.

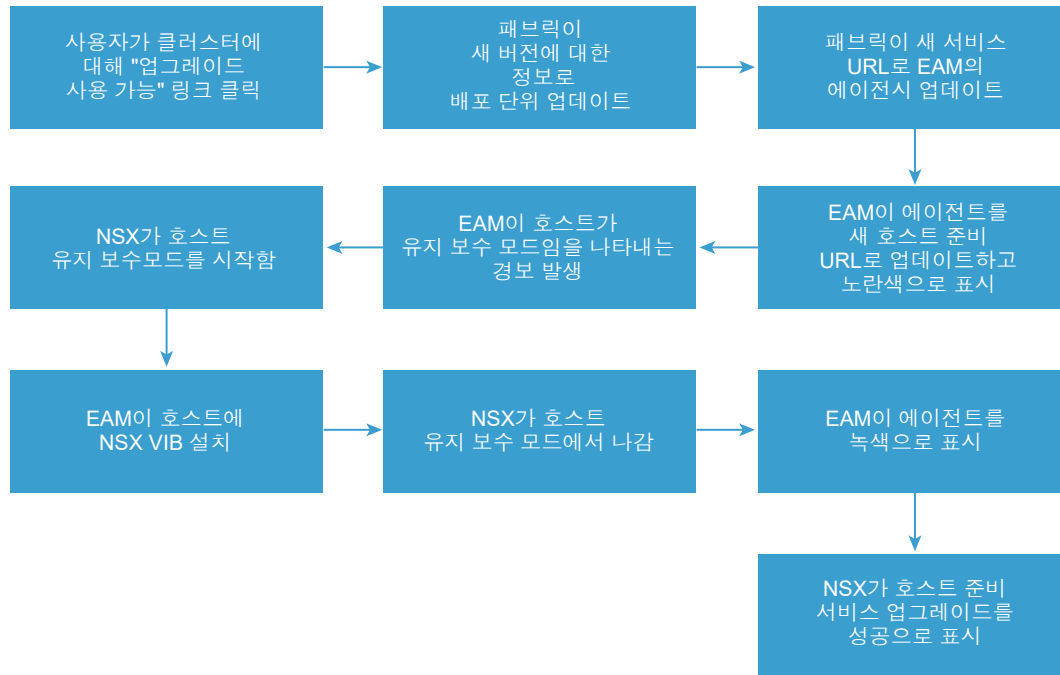
호스트 준비를 위한 서비스 배포 워크플로

이 항목에서는 호스트 준비에 대한 서비스 배포 워크플로(설치 및 업그레이드)를 제공합니다.

설치 워크플로



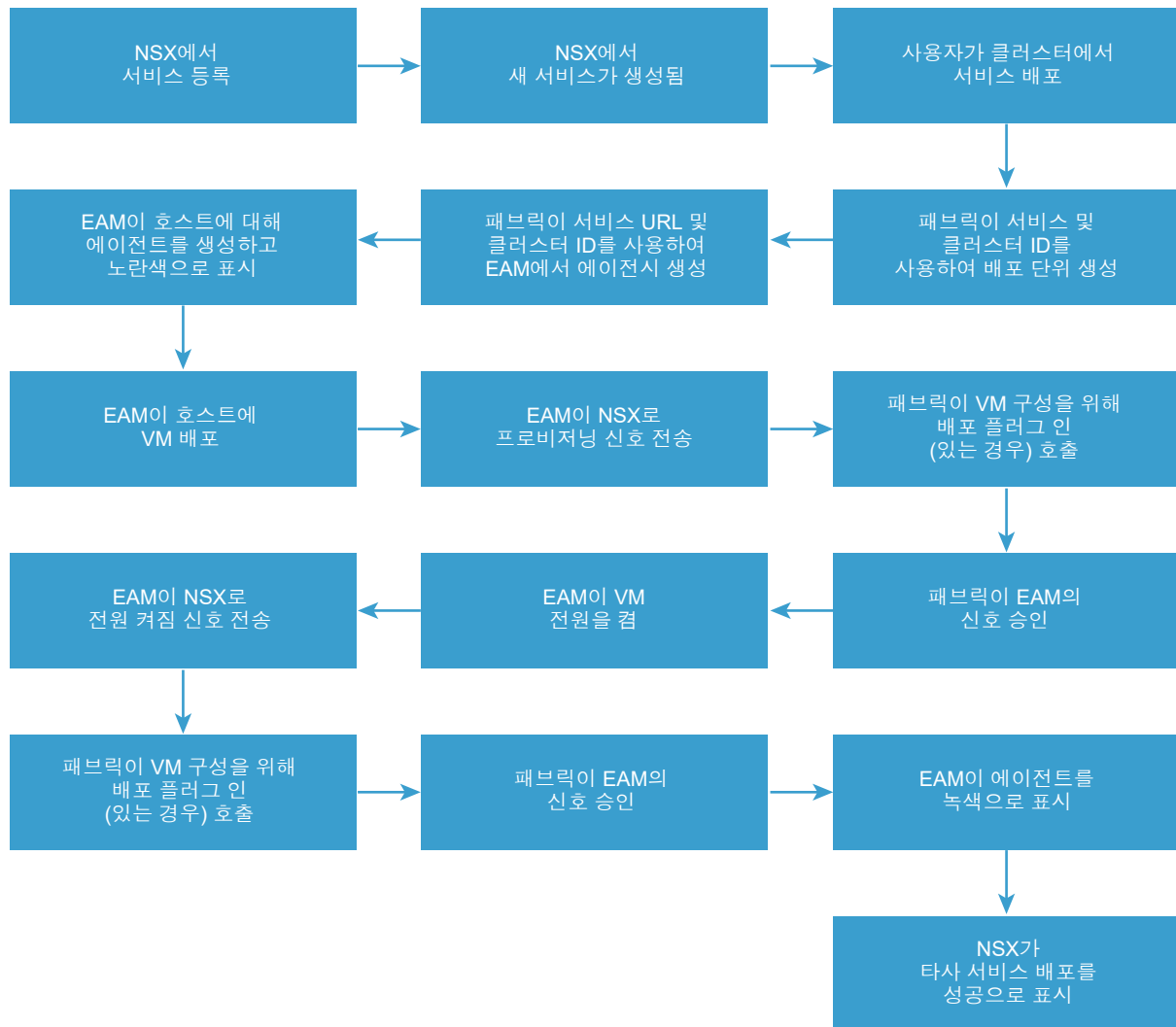
업그레이드 워크플로



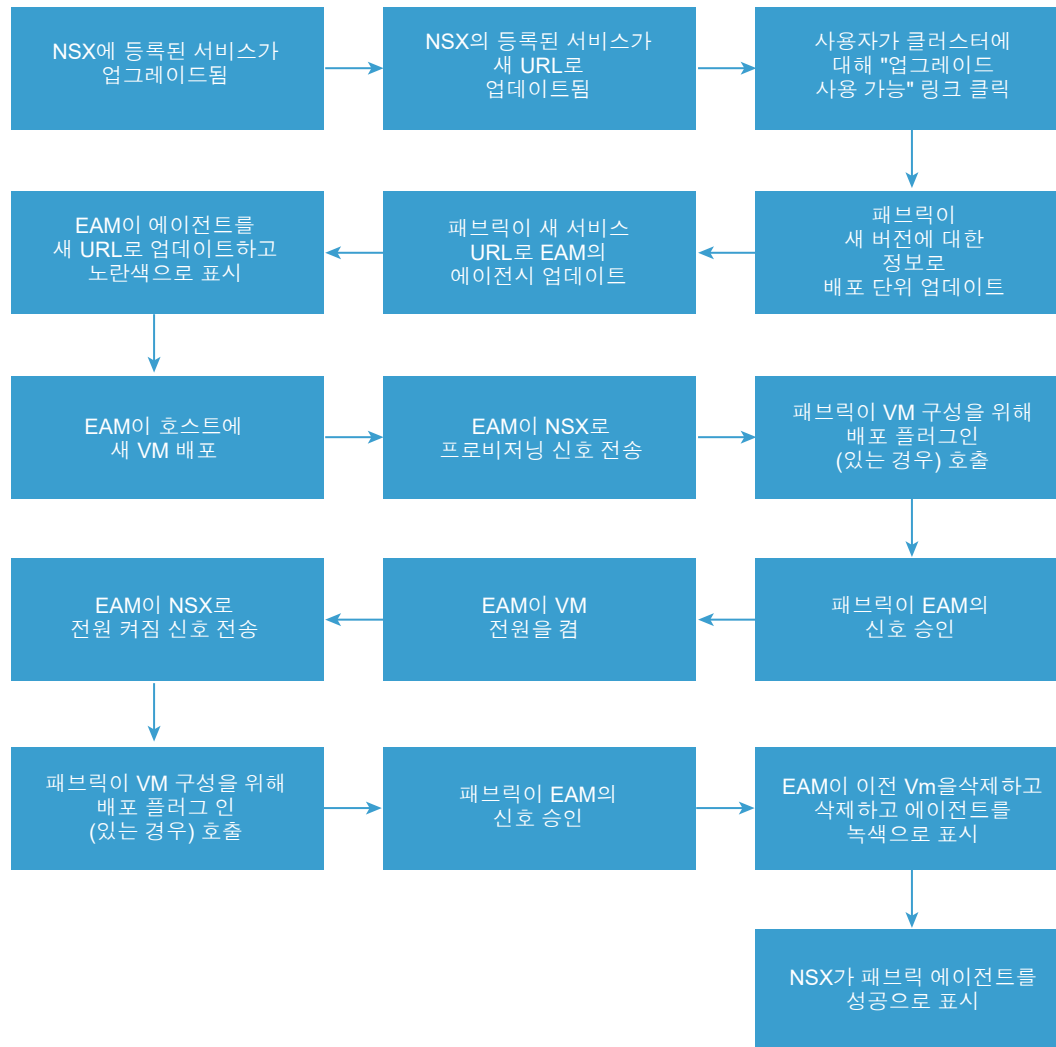
타사 서비스에 대한 서비스 배포 워크플로

이 항목에서는 타사 서비스에 대한 서비스 배포 워크플로(설치 및 업그레이드)를 제공합니다.

설치 워크플로




업그레이드 워크플로



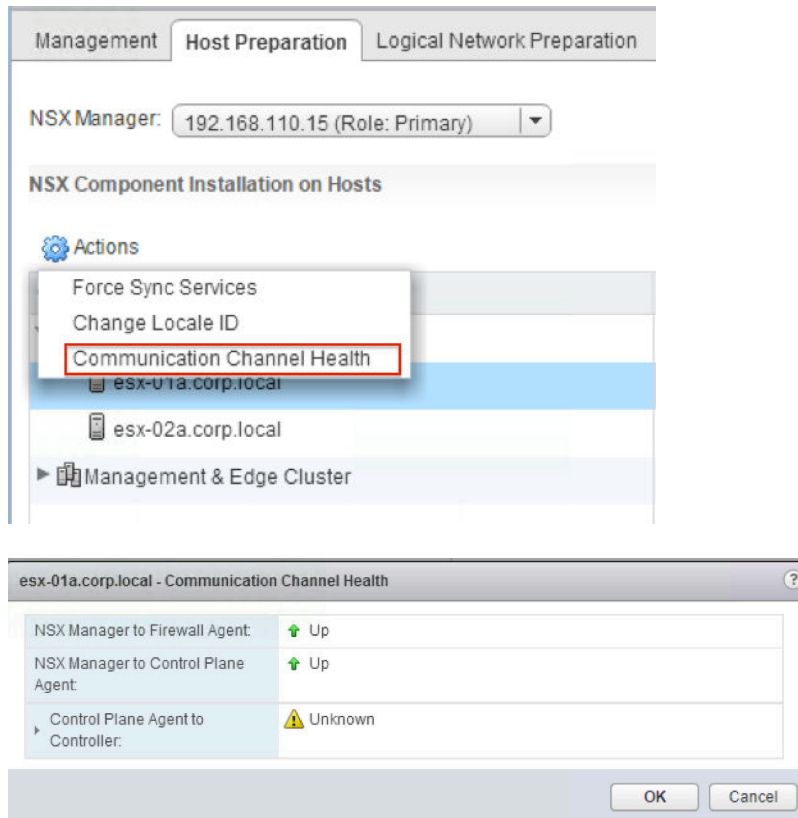
통신 채널 상태 확인

vSphere Web Client에서 다양한 구성 요소 간 통신 상태를 확인할 수 있습니다.

NSX Manager와 방화벽 에이전트, NSX Manager와 제어부 에이전트, 제어부 에이전트와 컨트롤러 간 통신 채널 상태를 확인하려면 다음 단계를 수행합니다.

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 호스트 준비(Host Preparation)**로 이동합니다.
- 2 클러스터를 선택하거나 클러스터를 확장하고 호스트를 선택합니다. **작업(Actions)**()을 클릭한 후 **통신 채널 상태(Communication Channel Health)**를 클릭합니다.

통신 채널 상태 정보가 표시됩니다.



호스트에 대한 세 연결 중 하나의 상태가 변경되면 NSX Manager 로그에 메시지가 기록됩니다. 로그 메시지에서 연결 상태는 UP, DOWN 또는 NOT_AVAILABLE(vSphere Web Client에서 Unknown으로 표시)일 수 있습니다. 상태가 UP에서 DOWN 또는 NOT_AVAILABLE로 변경되면 주의 메시지가 생성됩니다. 예:

```
2016-05-23 23:36:34.736 GMT+00:00 WARN TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1941, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: DOWN.
```

상태가 DOWN 또는 NOT_AVAILABLE에서 UP으로 변경되면 주의 메시지와 비슷한 INFO 메시지가 생성됩니다. 예:

```
2016-05-23 23:55:12.736 GMT+00:00 INFO TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1938, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: UP.
```

제어부 채널에 통신 장애가 발생하면 다음의 자세한 장애 이유 중 하나를 포함하는 시스템 이벤트가 생성됩니다.

- 1255601: 잘못된 호스트 인증서
- 1255602: 잘못된 컨트롤러 인증서
- 1255603: SSL 핸드셰이크 오류
- 1255604: 연결이 거부됨

- 1255605: 연결 유지 시간 초과
- 1255606: SSL 예외
- 1255607: 잘못된 메시지
- 1255620: 알 수 없는 오류

또한 NSX Manager에서 호스트로 하트비트 메시지가 생성됩니다. NSX Manager와 netcpa 간에 하트비트가 손실되면 구성 전체 동기화가 트리거됩니다.

로그를 다운로드하는 방법에 대한 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

설치 상태가 준비되지 않음

호스트 준비 중에 클러스터 상태가 준비 안 됨으로 표시되는 것을 확인할 수 있습니다.

문제

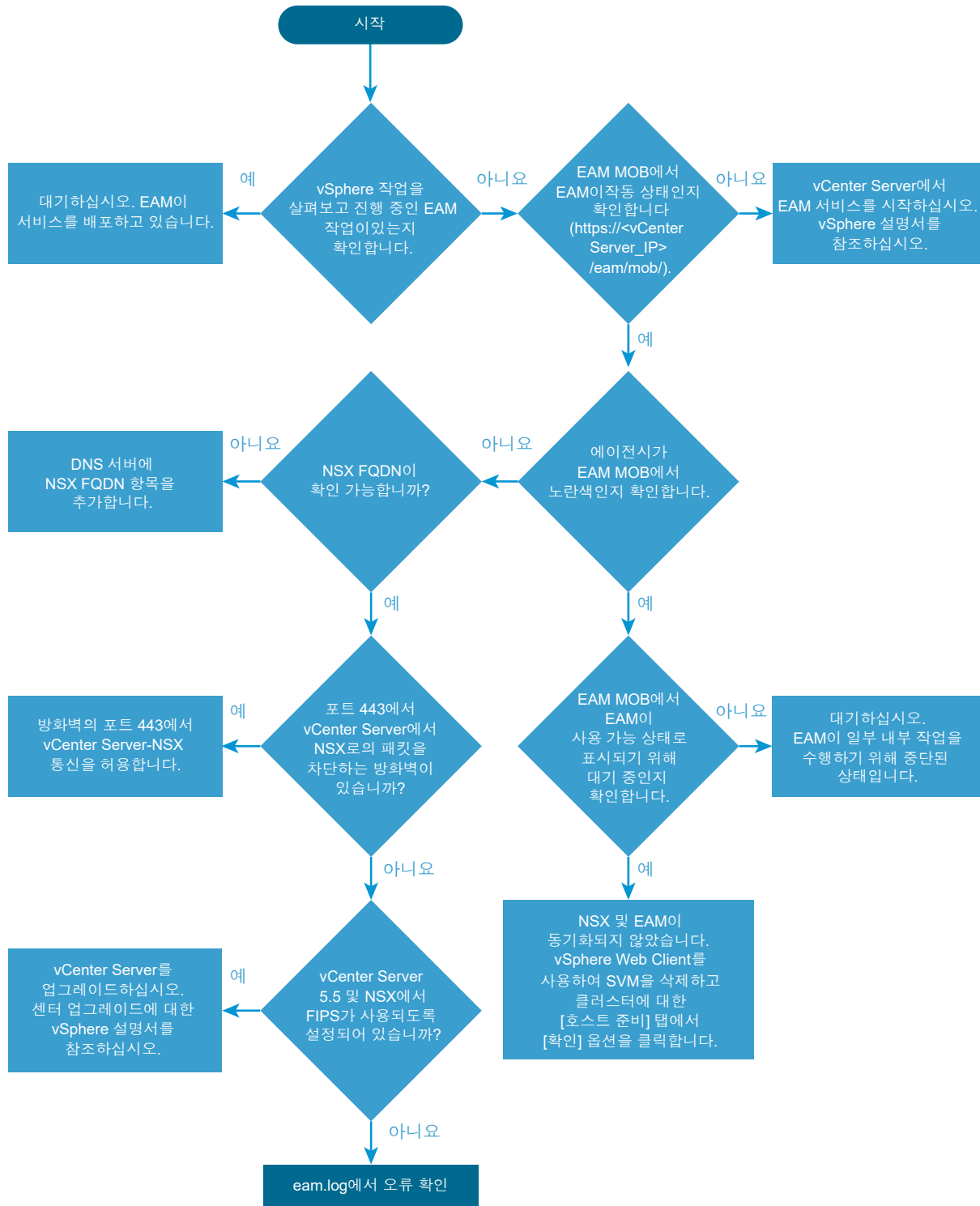
호스트 준비(Host Preparation) 탭 또는 **서비스 배포(Service Deployment)** 탭에서 설치 상태가 준비 안 됨으로 나타납니다.

해결책

- 1 **Networking & Security > 설치(Installation)>호스트 준비(Host Preparation)** 탭 또는 **서비스 배포(Service Deployment)** 탭으로 이동합니다.
- 2 클러스터 및 호스트에서 준비 안 됨을 클릭합니다.
오류 메시지가 표시됩니다.
- 3 **해결(Resolve)** 옵션을 클릭합니다.
해결(Resolve) 옵션을 통해 해결된 문제 목록을 보려면 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.
- 4 준비 안 됨이 계속 표시되고 오류가 해결되지 않으면 **해결 옵션을 사용하여 문제가 해결되지 않음**을 참조하십시오.

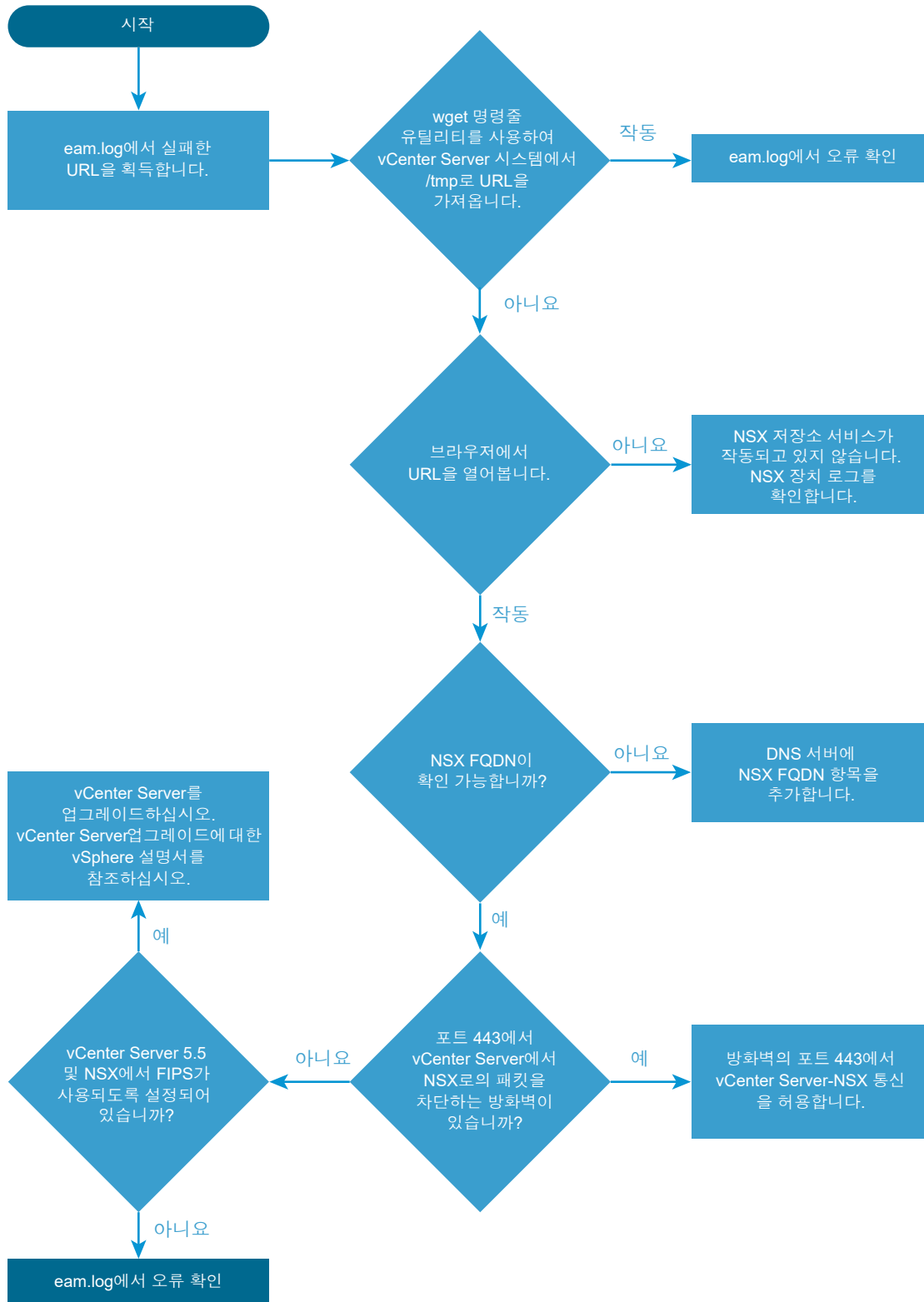
서비스가 응답하지 않음

이 순서도는 NSX 호스트 준비 프로세스 및 서비스가 오랫동안 응답하지 않거나 오랫동안 회전하는 아이콘을 표시하는 경우 수행할 작업을 대략적으로 설명합니다.



OVF/VIB 액세스 불가 오류를 나타내며 서비스 배포가 실패함

이 순서도는 OVF/VIB 액세스 불가 오류를 나타내며 서비스 배포가 실패할 때 수행할 작업을 제공합니다.



해결 옵션을 사용하여 문제가 해결되지 않음

Networking & Security > 설치(Installation) > 호스트 준비(Host Preparation) 탭 또는 **서비스 배포(Service Deployment)** 탭에서 설치 상태가 클러스터 및 호스트에서 준비 안 됨으로 나타납니다. **해결(Resolve)** 옵션을 클릭해도 문제가 해결되지 않습니다.

문제

- 준비 안 됨 링크를 클릭하면 에이전트에 대한 VIB 모듈이 호스트에 설치되지 않음으로 오류가 표시됩니다.
- ESXi 호스트가 vCenter Server에서 VIB에 액세스하지 못합니다.
- vShield Endpoint에서 NSX Manager로 변경하는 동안 상태가 실패로 표시될 수 있습니다.

해결책

- 1 DNS가 vCenter Server, ESXi 호스트 및 NSX Manager에서 올바르게 구성되어 있는지 확인하십시오. vCenter Server, ESXi 호스트, NSX Manager 및 vSphere Update Manager의 정방향 및 역방향 DNS 확인이 작동하는지 확인합니다.
- 2 문제가 DNS와 관련이 있는지 확인하려면 `esxupdate` 로그를 검토하고 `esxupdate.log` 파일에서 “`esxupdate: ERROR: MetadataDownloadError: IOError: <urlopen error [Errno -2] Name= or service not known`” 메시지를 찾습니다.

이 메시지는 ESXi 호스트에서 vCenter Server의 FQDN(정규화된 도메인 이름)에 액세스할 수 없음을 나타냅니다. 자세한 내용은 [VMware vCenter Server 관리 IP 주소 확인\(1008030\)](#)을 참조하십시오.
- 3 NTP(네트워크 타임 프로토콜)가 올바르게 구성되어 있는지 확인합니다. NTP를 구성하는 것이 좋습니다. NTP가 동기화되지 않는 문제가 작업 환경에 영향을 미치는지 확인하려면 버전 6.2.4 이상의 NSX Manager 지원 번들에서 `/etc/ntp.drift` 파일을 확인하십시오.
- 4 NSX for vSphere 6.x에 필요한 모든 포트가 방화벽에 의해 차단되지 않는지 확인하십시오. 자세한 내용은 다음을 참조하십시오.
 - [VMware NSX for vSphere에 대한 네트워크 포트 요구 사항\(2079386\)](#)
 - [VMware vCenter Server, VMware ESXi 및 ESX 호스트, 기타 네트워크 구성 요소에 액세스하는 데 필요한 TCP 및 UDP 포트\(1012382\)](#)

참고 VMware vSphere 6.x에서는 포트 443(포트 80 대신)을 통한 VIB 다운로드를 지원합니다. 이 포트는 동적으로 열리고 닫힙니다. ESXi 호스트와 vCenter Server 간의 중간 디바이스는 이 포트를 사용하여 트래픽을 허용해야 합니다.

- 5 vCenter Server 관리 IP 주소가 올바르게 구성되어 있는지 확인합니다. 자세한 내용은 [VMware vCenter Server 관리 IP 주소 확인\(1008030\)](#)을 참조하십시오.

- 6 vSphere Update Manager가 올바르게 작동되고 있는지 확인합니다. vCenter Server 6.0U3부터는 NSX 설치 및 업그레이드 절차의 경우 더 이상 ESX Agent Manager에서 vSphere Update Manager를 사용하지 않습니다. vCenter Server 6.0U3 이상을 실행할 것을 강력히 권장합니다. 업그레이드할 수 없는 경우 vSphere Update Manager 서비스가 실행되고 있는지 확인합니다. [KB 2053782](#)에 따라 vSphere Update Manager 바이패스 옵션을 구성할 수 있습니다.
- 7 vCenter Server를 배포하는 동안 비기본 포트를 지정하는 경우 이러한 포트가 ESXi 호스트 방화벽에 의해 차단되지 않는지 확인합니다.
- 8 `vpzd` 프로세스가 vCenter Server TCP 포트 8089에서 수신하는지 확인합니다. NSX Manager는 기본 포트 8089만 지원합니다.

vSphere EAM(ESX Agent Manager) 정보

vSphere ESX Agent Manager가 vSphere 솔루션에 필요한 추가 서비스를 제공하도록 ESXi 호스트의 기능을 확장하면서 NSX 네트워킹 및 보안 서비스를 배포 및 관리하는 프로세스를 자동화합니다.

ESX Agent Manager의 로그 및 서비스

ESX Agent Manager 로그는 vCenter 로그 번들의 일부로 포함되어 있습니다.

- Windows—C:\ProgramData\VMware\vCenterServer\logs\eam\eam.log
- VCSA—/var/log/vmware/vpx/eam.log
- ESXi—/var/log/esxupdate.log

ESX Agent Manager 모니터링

중요 NSX 설치를 시작하기 전에 `bypassVumEnabled` 플래그를 **True**로 변경하고 설치 이후에 다시 **False**로 변경해야 합니다. <https://kb.vmware.com/kb/2053782>를 참조하십시오.

ESX Agent Manager의 상태를 확인하려면:

- 1 vSphere Web Client로 이동합니다.
- 2 **관리 > vCenter Server 확장(Administration > vCenter Server Extensions)**을 클릭하고 vSphere ESX Agent Manager를 클릭합니다.
 - a **관리(Manage)** 탭을 클릭합니다.

관리(Manage) 탭에서는 실행 중인 에이전시에 대한 정보가 표시되고, 분리된 ESX 에이전트가 나열되고, ESX Agent Manager가 관리하는 ESX 에이전트에 대한 정보가 로깅됩니다.

에이전트 및 에이전시에 대한 자세한 내용은 vSphere 설명서를 참조하십시오.
 - b **모니터(Monitor)** 탭을 클릭합니다.

모니터(Monitor) > 이벤트(Events) 탭에는 ESX Agent Manager와 연결된 이벤트에 대한 정보가 표시됩니다.

NSX Manager 문제 해결

각 문제 해결 단계가 작업 환경에 맞는지 확인하십시오. 각 단계에서는 가능한 원인을 해결하고 필요한 경우 수정 조치를 취하기 위한 지침을 제공합니다. 이러한 단계는 문제를 분리하고 적절한 해결책을 찾아내는 데 가장 적합한 순서대로 진행됩니다. 단계를 건너뛰지 마십시오.

문제

- VMware NSX Manager 설치가 실패합니다.
- VMware NSX Manager 업그레이드가 실패합니다.
- VMware NSX Manager로의 로그인에 실패합니다.
- VMware NSX Manager 액세스가 실패합니다.

해결책

- 1 현재 릴리스의 "NSX 릴리스 정보"를 확인하여 버그가 해결되었는지 알아봅니다.
- 2 VMware NSX Manager를 설치할 때 최소 시스템 요구 사항이 충족되었는지 확인합니다.
"NSX 설치 가이드"를 참조하십시오.
- 3 NSX Manager에서 모든 필수 포트가 열려 있는지 확인하십시오.
"NSX 설치 가이드"를 참조하십시오.
- 4 설치 문제:
 - Lookup Service 또는 vCenter Server 구성이 실패하면 NSX Manager 및 Lookup Service 장치의 시간이 동기화되어 있는지 확인합니다. NSX Manager 및 Lookup Service에서 동일한 NTP 서버 구성을 사용합니다. 또한 DNS가 제대로 구성되어 있는지 확인하십시오.
 - OVA 파일이 올바르게 설치되어 있는지 확인하십시오. NSX OVA 파일을 설치할 수 없을 경우 vSphere Client의 오류 창에 실패한 부분이 표시됩니다. 또한 다운로드한 OVA/OVF 파일의 MD5 체크섬을 확인하고 유효한지 검사하십시오.
 - ESXi 호스트의 시간이 NSX Manager와 동기화되어 있는지 확인합니다.
 - VMware에서는 NSX Manager를 설치한 직후에 NSX Manager 데이터의 백업을 예약하는 것을 권장합니다.
- 5 업그레이드 문제:
 - 업그레이드하기 전에 [제품 상호 운용성 매트릭스] 페이지에서 최신 상호 운용성 정보를 참조하십시오.
 - 업그레이드하기 전에 현재 구성을 백업하고 기술 지원 로그를 다운로드하는 것이 좋습니다.

- NSX Manager 업그레이드 후에 vCenter Server와의 강제 다시 동기화가 필요할 수 있습니다. 이렇게 하려면 NSX Manager 웹 인터페이스 GUI에 로그인합니다. 그런 다음 **vCenter 등록 관리 > NSX 관리 서비스 > 편집(Manage vCenter Registration > NSX Management Service > Edit)**으로 이동하고 관리자 암호를 다시 입력합니다.

6 성능 문제:

- 최소 vCPU 요구 사항이 충족되었는지 확인합니다.
- 루트(/) 파티션에 적절한 공간이 있는지 확인합니다. ESXi 호스트에 로그인하고 `df -h` 명령을 입력하여 이를 확인할 수 있습니다.

예:

```
[root@esx-01a:~] df -h
Filesystem      Size  Used Available Use% Mounted on
NFS              111.4G  80.8G   30.5G   73% /vmfs/volumes/ds-site-a-nfs01
vfat             249.7M 172.2M   77.5M   69% /vmfs/volumes/68cb5875-d887b9c6-a805-65901f83f3d4
vfat             249.7M 167.7M   82.0M   67% /vmfs/volumes/fe84b77a-b2a8860f-38cf-168d5dfe66a5
vfat             285.8M 206.3M   79.6M   72% /vmfs/volumes/54de790f-05f8a633-2ad8-00505603302a
```

- `esxtop` 명령을 사용하여 대량의 CPU 및 메모리를 사용하고 있는 프로세스를 확인합니다.
- NSX Manager의 로그에 메모리 부족 오류가 있는 경우 `/common/dumps/java.hprof` 파일이 있는지 확인합니다. 이 파일이 있는 경우 이 파일의 복사본을 생성하여 이를 NSX 기술 지원 로그 번들에 포함합니다.
- 작업 환경에 스토리지 지연 시간 문제가 없는지 확인합니다.
- NSX Manager를 다른 ESXi 호스트로 마이그레이션합니다.

7 연결 문제:

- NSX Manager와 vCenter Server 또는 ESXi 호스트 간에 연결 문제가 있는 경우 NSX Manager CLI 콘솔에 로그인하여 `debug connection IP_of_ESXi_or_VC` 명령을 실행하고 출력을 확인합니다.
- Virtual Center 웹 관리 서비스가 시작되고 브라우저가 오류 상태가 아닌지 확인하십시오.
- NSX Manager 웹 UI(사용자 인터페이스)가 업데이트되고 있지 않으면 웹 서비스를 사용하지 않도록 설정한 후 다시 사용하도록 설정하여 문제 해결을 시도해 볼 수 있습니다. <https://kb.vmware.com/kb/2126701>를 참조하십시오.
- ESXi 호스트에서 `esxtop` 명령을 사용하여 NSX Manager에서 사용되는 포트 그룹 및 업링크 NIC를 확인합니다. 자세한 내용은 <https://kb.vmware.com/kb/1003893> 항목을 참조하십시오.
- NSX Manager를 다른 ESXi 호스트로 마이그레이션합니다.
- **모니터(Monitor)** 탭의 vSphere Web Client에서 NSX Manager 가상 시스템 장치의 **태스크 및 이벤트(Tasks and Events)** 탭을 선택합니다.

- NSX Manager와 vCenter Server 간에 연결 문제가 있는 경우 NSX Manager를 vCenter Server 가상 시스템이 실행되고 있는 동일한 ESXi 호스트로 마이그레이션을 시도하여 가능한 기본 물리적 네트워크 문제를 제거합니다.

이 작업은 두 가상 시스템이 같은 VLAN/포트 그룹에 있는 경우에만 작동합니다.

NSX Manager를 vCenter Server에 연결

NSX Manager와 vCenter Server 간 연결을 통해 NSX Manager는 vSphere API를 사용하여 서비스 VM 배포, 호스트 준비 및 논리적 스위치 포트 그룹 생성과 같은 기능을 수행할 수 있습니다. 연결 프로세스가 진행되면 Web Client Server에 NSX용 웹 클라이언트 플러그인이 설치됩니다.

연결이 작동하려면 NSX Manager, vCenter Server 및 ESXi 호스트에 DNS 및 NTP가 구성되어야 합니다. 이름을 사용하여 ESXi 호스트를 vSphere 인벤토리에 추가한 경우 NSX Manager에서 DNS 서버가 구성되어 있고 이름 확인이 작동하고 있는지 확인합니다. 그렇지 않으면 NSX Manager에서 IP 주소를 확인할 수 없습니다. SSO 서버 시간과 NSX Manager 시간이 동기화되도록 NTP 서버를 지정해야 합니다. NSX Manager에서 `/etc/ntp.drift`의 드리프트 파일은 NSX Manager에 대한 기술 지원 번들에 포함되어 있습니다.

NSX Manager를 vCenter Server에 연결하는 데 사용하는 계정은 vCenter 역할 "관리자"여야 합니다. "관리자" 역할이 있으면 NSX Manager는 자체적으로 보안 토큰 서비스 서버에 등록될 수 있습니다. 특정 사용자 계정이 NSX Manager를 vCenter에 연결하는 데 사용되면 해당 사용자의 "엔터프라이즈 관리자" 역할도 NSX Manager에서 생성됩니다.

NSX Manager를 vCenter Server로 연결하는 작업과 관련된 일반적인 문제

- DNS가 NSX Manager, vCenter Server 또는 ESXi 호스트에서 잘못 구성되었습니다.
- NTP가 NSX Manager, vCenter Server 또는 ESXi 호스트에서 잘못 구성되었습니다.
- vCenter 관리자 역할이 없는 사용자 계정이 NSX Manager를 vCenter에 연결하는 데 사용되었습니다.
- NSX Manager와 vCenter Server 간에 네트워크 연결 문제가 있습니다.
- 사용자가 NSX Manager에서 역할이 없는 계정을 사용하여 vCenter에 로그인하려 합니다.

처음에는 NSX Manager를 vCenter Server에 연결하는 데 사용한 계정으로 vCenter에 로그인해야 합니다. 그런 다음 **홈 > Networking & Security > NSX Manager > {NSX Manager의 IP} > 관리 > 사용자(Home > Networking & Security > NSX Managers > {IP of NSX Manager} > Manage > Users)**를 사용하여 NSX Manager에서 역할이 있는 추가 사용자를 생성할 수 있습니다.

vCenter가 NSX UI 번들을 로드하고 배포하는 동안 첫 번째 로그인이 진행되는 데 4분까지 소요될 수 있습니다.

NSX Manager에서 vCenter Server로의 연결 확인

- NSX Manager CLI 콘솔에 로그인합니다.

- 연결을 확인하려면 **ARP** 및 라우팅 테이블을 봅니다.

```
nsxmgr# show arp
```

IP address	HW type	Flags	HW address	Mask	Device
192.168.110.31	0x1	0x2	00:50:56:ae:ab:01	*	mgmt
192.168.110.2	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.1	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.33	0x1	0x2	00:50:56:ae:4f:7c	*	mgmt
192.168.110.32	0x1	0x2	00:50:56:ae:50:bf	*	mgmt
192.168.110.10	0x1	0x2	00:50:56:03:19:4e	*	mgmt
192.168.110.51	0x1	0x2	00:50:56:03:30:2a	*	mgmt
192.168.110.22	0x1	0x2	00:50:56:01:21:f9	*	mgmt
192.168.110.55	0x1	0x2	00:50:56:01:23:21	*	mgmt
192.168.110.26	0x1	0x2	00:50:56:01:21:ef	*	mgmt
192.168.110.54	0x1	0x2	00:50:56:01:22:ef	*	mgmt
192.168.110.52	0x1	0x2	00:50:56:03:30:16	*	mgmt

```
nsxmgr# show ip route
```

Codes: K - kernel route, C - connected, S - static,
> - selected route, * - FIB route

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

- NSX Manager 로그에서 오류를 조회하여 vCenter Server로 연결되지 않는 이유를 확인합니다. 로그를 보기 위한 명령은 `show log manager follow`입니다.

```
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:491 - I/O exception (org.apache.http.NoHttpResponseException: The target server failed to respond)
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:498 - Retrying request
2014-02-26 12:53:23.815 GMT WARN ViInventoryThread ViInventory:1482 - We received error from VC, probably lost connection.
2014-02-26 12:53:23.817 GMT INFO VcEventsReaderThread VcEventsReader$VcEventsReaderThread:347 - Caught exception:com.vmware.vim.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to https://vc-1-01a.corp.local refused
2014-02-26 12:53:23.821 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:348 - Caught exception during p
com.vmware.vim.vimomi.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to ht
```

- `debug connection IP_of_ESXi_or_VC` 명령을 실행하고 출력을 검토합니다.

NSX Manager에서 패킷 캡처를 수행하여 연결 확인

다음 디버그 패킷 명령을 사용합니다. `debug packet [capture|display] interface interface filter`

NSX Manager의 인터페이스 이름은 `mgmt`입니다.

필터 구문은 `"port_80_or_port_443"` 형식을 따릅니다.

이 명령은 권한이 있는 모드에서만 실행됩니다. 권한이 있는 모드를 시작하려면 `enable` 명령을 실행하고 관리자 암호를 제공하십시오.

패킷 캡처 예제:

```
nsxmgr# en
nsxmgr# debug packet display interface mgmt port_80_or_port_443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on mgmt, link-type EN10MB (Ethernet), capture size 262144 bytes
23:40:25.321085 IP 192.168.210.15.54688 > 192.168.210.22.443: Flags [P.], seq 2645022162:2645022199,
ack 2668322748, win 244, options [nop,nop,TS val 1447550948 ecr 365097421], length 37
...
```

NSX Manager에서 네트워크 구성 확인

show running-config 명령은 관리 인터페이스, NTP 및 기본 경로 설정에 대한 기본 구성을 표시합니다.

```
nsxmgr# show running-config
Building configuration...

Current configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr
!
interface mgmt
 ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

NSX Manager 인증서

NSX Manager는 인증서를 생성하는 2가지 방법을 지원합니다.

- NSX Manager에서 CSR 생성: 기본 CSR 때문에 기능이 제한됨
- PKCS#12: 운영 환경에서 사용 권장

CMS가 자동으로 API 호출을 수행하는 데 실패하는 알려진 문제가 있습니다.

인증서 발급자가 신뢰할 수 없는 루트 CA(인증 기관)이거나 인증서가 자체 서명되었으므로 호출자에게 알려지지 않은 경우에 이러한 문제가 발생합니다. 이 문제를 해결하려면 브라우저를 사용하여 NSX Manager IP 주소 또는 호스트 이름으로 이동한 후 인증서를 수락합니다.

보조 NSX Manager가 전송 모드에서 중단됨

문제에 설명된 대로 보조 NSX Manager가 전송 모드에서 중단되면 아래에 설명된 해결 방법을 사용합니다. 보조 NSX Manager가 전송 모드일 때 기본 NSX Manager에서 백업을 복원하는 경우 이 문제가 발생합니다.

문제

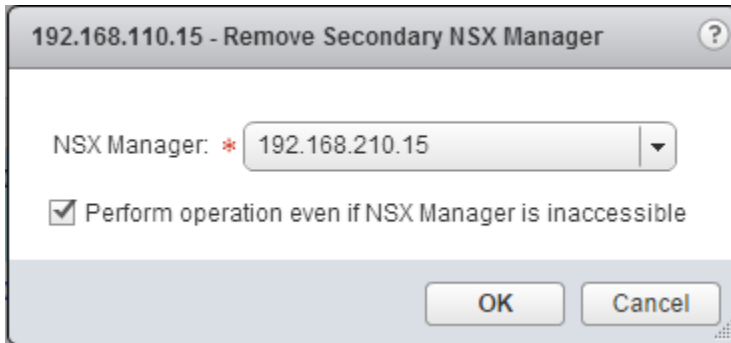
- 1 기본 및 보조 NSX Manager를 구성했습니다.
- 2 기본 NSX Manager의 백업을 작성합니다.

- 3 나중에 보조 NSX Manager를 제거합니다. 보조 NSX Manager가 전송 모드에 있습니다.
- 4 이제 몇 가지 이유로 인해 기본 NSX Manager에서 백업을 복원합니다.
- 5 데이터베이스에서 전송 NSX Manager가 **보조(Secondary)**로 업데이트되지만 UI에서 **전송(Transit)**으로 표시되고 동기화는 실패합니다.
- 6 보조 NSX Manager를 제거하거나 다시 보조로 승격시키지 못할 수 있습니다.
- 7 전송 NSX Manager를 승격하는 경우 IP 주소/호스트 이름을 갖는 NSX Manager 노드가 이미 있습니다. 라는 오류 메시지가 표시됩니다.
- 8 전송 NSX Manager를 제거하는 경우 잘못된 사용자 이름 또는 암호라는 오류 메시지가 표시됩니다.

해결책

- 1 vSphere Web Client를 사용하여 기본 NSX Manager에 연결된 vCenter에 로그인합니다.
- 2 **홈(Home) > Networking & Security> 설치(Installation)**로 이동한 다음 **관리(Management)** 탭을 선택합니다.
- 3 삭제하려는 보조 NSX Manager를 선택하고 **작업(Actions)**을 클릭한 다음 **보조 NSX Manager 제거(Remove Secondary NSX Manager)**를 클릭합니다.

확인 대화상자가 나타납니다.



- 4 NSX Manager에 액세스할 수 없는 경우에도 작업 수행(Perform operation even if NSX Manager is inaccessible) 확인란을 선택합니다.
- 5 **확인(OK)**을 클릭합니다.

보조 NSX Manager가 기본 데이터베이스에서 삭제됩니다.

- 6 보조 NSX Manager를 다시 추가합니다.

다음에 수행할 작업

보조 NSX Manager 추가에 대한 자세한 내용은 "NSX 설치 가이드"를 참조하십시오.

NSX SSO Lookup Service 구성 실패

문제

- vCenter Server에 NSX Manager 등록 실패
- SSO Lookup Service 구성 실패
- 다음 오류가 표시될 수 있습니다.

```
nested exception is java.net.UnknownHostException: vc.local( vc.corp.local )
```

```
NSX Management Service operation failed.( Initialization of Admin Registration Service
Provider failed. Root Cause: Error occurred while registration of lookup service,
com.vmware.vim.sso.admin.exception.InternalError: General failure.
```

```
com.vmware.vshield.vsm.security.service.impl.SamlTokenSSOAuthenticator : SSO is not
configured or initialized properly so cannot authenticate user.
```

해결책

1 연결 문제:

- NSX Manager와 vCenter Server 또는 ESXi 호스트 간에 연결 문제가 있는 경우 NSX Manager CLI 콘솔에 로그인하여 `debug connection IP_of_ESXi_or_VC` 명령을 실행하고 출력을 확인합니다.
- 다음 명령을 사용하여 IP 주소 및 FQDN을 통해 NSX Manager에서 vCenter Server로 Ping하여 NSX Manager의 라우팅, 정적 또는 기본 경로를 확인합니다.

```
nsxmgr-l-01a# show ip route
```

코드:

K - 커널 경로,

C - 연결됨,

S - 정적

> - 선택된 경로,

* - FIB 경로

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.2, mgmt
```

```
C>* 192.168.110.0/24 is directly connected, mgmt
```

2 DNS 문제

다음 명령을 사용하여 FQDN으로 NSX Manager에서 vCenter Server로 Ping을 수행합니다.

```
nsx-mgr> ping vc-l-01a.corp.local
```

다음 예와 비슷한 출력이 표시됩니다.

```

nsx-mgr> ping vc-l-01a.corp.local
PING vc-l-01a.corp.local (192.168.110.51): 56 data bytes
64 bytes from 192.168.110.51: icmp_seq=0 ttl=64 time=1.749 ms
64 bytes from 192.168.110.51: icmp_seq=1 ttl=64 time=2.111 ms
64 bytes from 192.168.110.51: icmp_seq=2 ttl=64 time=8.082 ms
64 bytes from 192.168.110.51: icmp_seq=3 ttl=64 time=2.010 ms
64 bytes from 192.168.110.51: icmp_seq=4 ttl=64 time=0.857 ms

```

이러한 출력이 표시되지 않으면 NSX Manager에서 **관리 > 네트워크 > DNS 서버(Manage > Network > DNS Servers)**로 이동한 후 DNS가 제대로 구성되어 있는지 확인합니다.

3 방화벽 문제

NSX Manager와 vCenter Server 간에 방화벽이 있는 경우 TCP/443에서 SSL이 허용되는지 확인합니다. 또한 ping을 수행하여 연결을 확인합니다.

4 NSX Manager에서 다음 필수 포트가 열려 있는지 확인합니다.

표 2-1. NSX Manager 열린 포트

포트	다음에 필요함
443/TCP	배포를 위해 ESXI 호스트에서 OVA 파일 다운로드 REST API 사용 NSX Manager 사용자 인터페이스 사용
80/TCP	vSphere SDK에 대한 연결 시작 NSX Manager와 NSX 호스트 모듈 간 메시징
1234/TCP	NSX Controller와 NSX Manager 간 통신
5671	Rabbit MQ(메시징 버스 기술)
22/TCP	CLI에 대한 콘솔 액세스(SSH) 참고: 기본적으로 이 포트는 닫혀 있습니다.

5 NTP 문제

vCenter Server와 NSX Manager 간에 시간이 동기화되었는지 확인합니다. 이를 위해서는 NSX Manager 및 vCenter Server에서 동일한 NTP 서버 구성을 사용합니다.

NSX Manager에서 시간을 확인하려면 CLI에서 다음 명령을 실행합니다.

```
nsxmgr-l-01a# show clock
```

```
Tue Nov 18 06:51:34 UTC 2014
```

vCenter Server에서 시간을 확인하려면 CLI에서 다음 명령을 실행합니다.

```
vc-l-01a:~ # date
```

다음과 비슷한 출력이 표시됩니다.

Tue Nov 18 06:51:31 UTC 2014

참고: 시간 설정을 구성한 후에 장치를 다시 시작합니다.

6 사용자 사용 권한 문제

사용자에게 **관리자** 권한이 있는지 확인합니다.

vCenter Server 또는 SSO Lookup Service에 등록하려면 관리 권한이 있어야 합니다.

기본 계정은 `administrator user: administrator@vsphere.local`입니다.

7 자격 증명을 입력하여 SSO에 다시 연결합니다.

논리적 네트워크 준비: VXLAN 전송

NSX는 VTEP VMkernel NIC에 대한 분산 가상 포트 그룹을 생성하여 VXLAN에 대해 사용자가 선택한 vSphere Distributed Switch를 준비합니다.

VXLAN 구성 중에 VTEP의 팀 구성 정책, 로드 밸런싱 메서드, MTU 및 VLAN ID가 선택됩니다. 팀 구성 및 로드 밸런싱 메서드는 VXLAN에 대해 선택된 DVS의 구성과 일치해야 합니다.

MTU는 DVS에 이미 구성된 수준으로 최소 1600 이상으로 설정되어야 합니다.

생성되는 VTEP 수는 선택된 팀 구성 정책과 DVS 구성에 따라 다릅니다.

VXLAN 준비 중에 발생하는 일반적인 문제

VXLAN 준비는 다음과 같은 몇 가지 이유로 실패할 수 있습니다.

- VXLAN에 대해 선택된 팀 구성 방법이 DVS에서 지원되는 방법과 일치하지 않습니다. 지원되는 방법을 검토하려면 <https://communities.vmware.com/docs/DOC-27683>에서 "VMware NSX for vSphere 네트워크 가상화 설계 가이드"를 참조하십시오.
- VTEP에 대해 잘못된 VLAN ID를 선택했습니다.
- VTEP IP 주소를 할당하기 위해 DHCP를 선택했으나 DHCP 서버를 사용할 수 없습니다.
- VMkernel NIC가 없습니다. [VXLAN VMkernel NIC가 동기화되지 않음](#)에 설명된 대로 오류를 해결합니다.
- VMkernel NIC의 IP 주소가 잘못되었습니다. <https://kb.vmware.com/kb/2137025>에 설명된 대로 오류를 해결합니다.
- VTEP에 대해 잘못된 MTU 설정을 선택했습니다. 이 항목의 뒷부분에 설명된 대로 MTU 불일치가 있는지 조사해야 합니다.
- 잘못된 VXLAN 게이트웨이를 선택했습니다. 이 항목의 뒷부분에 설명된 대로 VXLAN 게이트웨이를 구성하는 동안 오류가 발생하는지 조사해야 합니다.

중요한 포트 번호

VXLAN UDP 포트는 UDP 캡슐화에 사용됩니다. NSX 6.2.3 이전에는 기본 VXLAN 포트 번호가 8472였습니다. NSX 6.2.3에서는 새 설치의 경우 기본 VXLAN 포트 번호가 4789로 변경되었습니다. 하드웨어 VTEP를 사용하는 NSX 6.2 이상 설치에서는 VXLAN 포트 번호 4789를 사용해야 합니다. VXLAN 포트 구성 변경에 대한 자세한 내용은 "NSX 관리 가이드"에서 "VXLAN 포트 변경"을 참조하십시오.

호스트에 컨트롤러 연결이 필요한 활성 VM이 없는 경우 제어부 상태는 **사용 안 함**으로 표시됩니다.

호스트에서 VXLAN 세부 정보를 보려면 `show logical-switch` 명령을 사용합니다. 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오.

`show logical-switch host hostID verbose` 명령은 호스트가 테이블 정보를 전달하기 위해 컨트롤러 클러스터에 연결해야 하는 VM으로 채워지지 않은 경우 제어부 상태를 **사용 안 함**으로 표시합니다.

```
Network count: 18
VXLAN network: 32003
Multicast IP: 0.0.0.0
Control plane: Disabled <<=====
MAC entry count: 0
ARP entry count: 0
Port count: 1
```

VXLAN 게이트웨이 구성 중 오류

정적 IP 풀을 사용하여 VXLAN을 구성할 때(**Networking & Security > 설치 > 호스트 준비 > VXLAN 구성 (Networking & Security > Installation > Host Preparation > Configure VXLAN)**에서) 구성이 VTEP에서 IP 풀 게이트웨이의 설정에 실패하면, VXLAN 구성 상태가 호스트 클러스터에 대해 오류(빨간색) 상태에 진입합니다. 오류 메시지는 “호스트에서 VXLAN 게이트웨이를 설정할 수 없음”이며 오류 상태는 “VXLAN_GATEWAY_SETUP_FAILURE”입니다.

REST API 호출 GET `https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>`에서 VXLAN의 상태는 다음과 같습니다.

```
<nwFabricFeatureStatus>
<featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

해결 방법: 오류를 수정하는 옵션에는 두 가지가 있습니다.

- **Option 1:** 호스트 클러스터에 대한 **VXLAN** 구성을 제거하고, 게이트웨이가 제대로 구성되고 연결 가능한지 확인하여 IP 풀에서 기본 게이트웨이 설정을 수정한 다음 호스트 클러스터에 대한 **VXLAN**을 재구성합니다.
- **Option 2:** 다음 단계를 수행하십시오.
 - a 게이트웨이가 제대로 구성되고 연결 가능한지 확인하여 IP 풀에서 기본 게이트웨이 설정을 수정합니다.
 - b 호스트에 활성화된 VM 트래픽이 없도록 호스트를 유지 보수 모드로 전환합니다.
 - c 호스트에서 **VXLAN VTEP**를 삭제합니다.
 - d 호스트의 유지 보수 모드 설정을 해제합니다. 호스트의 유지 보수 모드 설정을 해제하면 **NSX Manager**에서 **VXLAN VTEP** 생성 프로세스가 트리거됩니다. **NSX Manager**는 호스트에서 필요한 **VTEP**의 재생성을 시도합니다.

MTU 불일치 조사

- 다음 명령을 실행하여 MTU가 1600 이상으로 구성되었는지 확인합니다.

```
ping ++netstack=vxlan -d -s 1572 -I <vmkx hostname_or_IP>
```

여기서 **vmkx**는 VMkernel 포트의 ID이고 **hostname_or_IP**는 VMkernel 포트의 IP 또는 호스트 이름입니다.

이 명령을 사용하면 모든 업링크의 유효성을 확인할 수 있습니다. 다중 VTEP 환경에서 작업하는 경우 가능한 각 VTEP VMkernel 소스/대상 인터페이스에서 ping 명령을 통해 모든 업링크를 확인하여 모든 경로가 유효한지 확인할 수 있습니다.

- 물리적 인프라를 확인합니다. 대부분의 경우 물리적 인프라의 구성을 변경하면 문제가 해결됩니다.
- 문제가 단일 논리적 스위치로 국한되는지 또는 다른 논리적 스위치에도 영향이 미치는지를 확인합니다. 이 문제가 모든 논리적 스위치에 영향을 주는지 확인합니다.

MTU 확인 방법에 대한 자세한 내용은 "NSX 업그레이드 가이드"에서 "NSX 작동 상태 확인"을 참조하십시오.

VXLAN VMkernel NIC가 동기화되지 않음

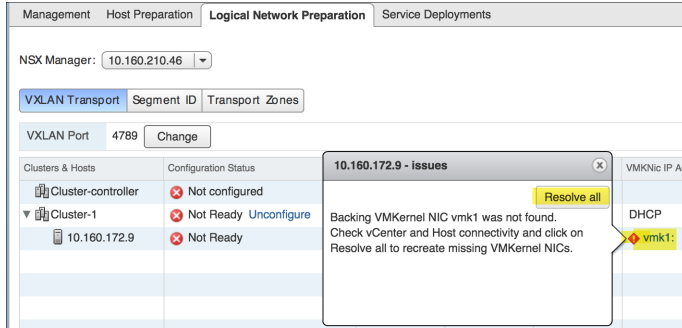
호스트에서 VMkernel NIC가 삭제되지만 VMkernel NIC 정보를 NSX에서 여전히 사용할 수 있으면 NSX Manager는 **오류(Error)** 아이콘을 사용하여 삭제된 VMkernel NIC를 나타냅니다.

사전 요구 사항

VMkernel NIC는 호스트에서 삭제됩니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 논리적 네트워크 준비(Logical Network Preparation)**로 이동합니다.
- 2 **VXLAN 전송(VXLAN Transport)** 탭에서 [클러스터 및 호스트]를 확장합니다.



- 3 **오류(Error)** 아이콘을 클릭하여 호스트에서 삭제된 VMkernel NIC의 정보를 확인합니다.
- 4 **모두 해결(Resolve All)** 버튼을 클릭하여 호스트에서 삭제된 VMkernel NIC를 다시 생성합니다.

결과

삭제된 VMkernel NIC가 호스트에서 다시 생성됩니다.

VXLAN 팀 구성 정책 및 MTU 설정 변경

VXLAN 팀 구성 정책 및 MTU 설정은 준비된 호스트 및 클러스터에서 변경될 수 있지만 변경 사항은 VXLAN에 대한 새 호스트 및 클러스터를 준비하는 경우에만 적용됩니다. 수동으로 호스트 및 클러스터를 다시 준비해야만 VTEP VMkernel에 대한 기존 가상 포트 그룹을 변경할 수 있습니다. API를 사용하여 팀 구성 정책 및 MTU 설정을 변경할 수 있습니다.

문제

VTEP에 대해 잘못된 MTU 설정을 선택했습니다.

해결책

- 1 GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches` API를 사용하여 모든 VXLAN 준비 스위치에 대한 정보를 검색합니다.

API의 출력에서 수정하려는 스위치를 찾아 이름을 적어둡니다. 예를 들면 **dvs-35**와 같습니다.

- 2 이제 이전에 적어둔 특정 vSphere Distributed Switch를 사용하여 쿼리합니다.

예를 들면 GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35` API와 같습니다.

다음 예와 비슷한 출력이 표시됩니다.

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
```

```

<objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
<vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
<nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
<revision>6</revision>
<type>
  <typeName>VmwareDistributedVirtualSwitch</typeName>
</type>
< name>vds-site-a</name>
<scope>
  <id>datacenter-21</id>
  <objectTypeName>Datacenter</objectTypeName>
  < name>Datacenter Site A</name>
</scope>
<clientHandle/>
<extendedAttributes/>
<isUniversal>false</isUniversal>
<universalRevision>0</universalRevision>
</switch>
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode>
</vdsContext>

```

- 3 API 호출을 사용하여 vSphere Distributed Switch에서 팀 구성 및/또는 MTU같은 매개 변수를 수정할 수 있습니다. 다음 예제에서는 팀 구성 정책 *dvs-35*를 *FAILOVER_ORDER*에서 *LOADBALANCE_SRCMAC*로, MTU를 1600에서 9000으로 바꾸는 방법을 보여줍니다.

■ NSX: PUT <https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches>

다음 예와 비슷한 출력이 표시됩니다.

```

<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  <name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    <name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>

```

```
<mtu>9000</mtu>
<teaming>LOADBALANCE_SRCMAC</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode>
</vdsContext>
```

참고 다음은 <teaming> 매개 변수의 올바른 팀 구성 정책 항목 목록입니다.

- FAILOVER_ORDER
- ETHER_CHANNEL
- LACP_ACTIVE
- LACP_PASSIVE
- LOADBALANCE_LOADBASED
- LOADBALANCE_SRCID
- LOADBALANCE_SRCMAC LACP_V2

- 4 GET 명령을 사용하여 사용한 구문이 올바른지와 작동 중인 vSphere Distributed Switch에 대해 변경 사항이 활성화되었는지를 확인하십시오. 예를 들면 GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35`와 같습니다.
- 5 vSphere Web Client를 열고 구성 변경 사항이 반영되었는지 확인합니다.

논리적 스위치 포트 그룹이 동기화되지 않음

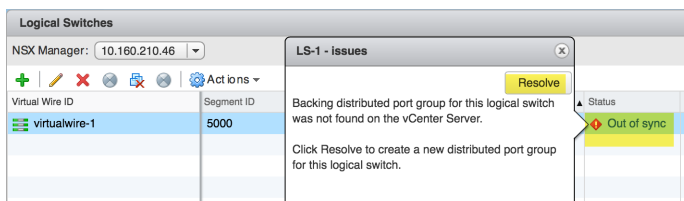
논리적 스위치의 백업 DVPG(분산 가상 포트 그룹)가 vCenter Server에서 삭제되면 **논리적 스위치(Logical Switches)** 페이지의 [상태] 열에 **동기화되지 않음(Out of sync)** 상태가 표시됩니다.

사전 요구 사항

논리적 스위치의 DVPG가 vCenter Server에서 삭제되었습니다.

절차

- 1 vSphere Web Client에서 **홈(Home) > 네트워킹 및 보안(Networking & Security) > 논리적 스위치(Logical Switches)**로 이동합니다.



- 2 [상태] 열에서 **동기화되지 않음(Out of sync)** 링크를 클릭하여 이 동기화되지 않음 상태에 대한 자세한 원인을 확인하십시오.
- 3 **해결(Resolve)** 버튼을 클릭하여 문제를 해결하십시오.

결과

백업 DVPG를 다시 생성하기 위한 API가 호출됩니다.

NSX 라우팅 문제 해결

3

NSX에는 2가지 핵심 요구에 맞게 최적화된 2가지 유형의 라우팅 하위 시스템이 있습니다.

NSX 라우팅 하위 시스템은 다음과 같습니다.

- DLR(논리적 분산 라우터)에서 제공하는 “동쪽-서쪽” 라우팅으로도 알려져 있는 논리적 공간 내 라우팅
- ESG(Edge Services Gateway)가 제공하는 “북쪽 - 남쪽” 라우팅으로도 알려져 있는 물리적 및 논리적 공간 사이의 라우팅

둘 다 수평 크기 조절을 위한 옵션을 제공합니다.

DLR을 통해 분산 E-W 라우팅을 확장할 수 있습니다.

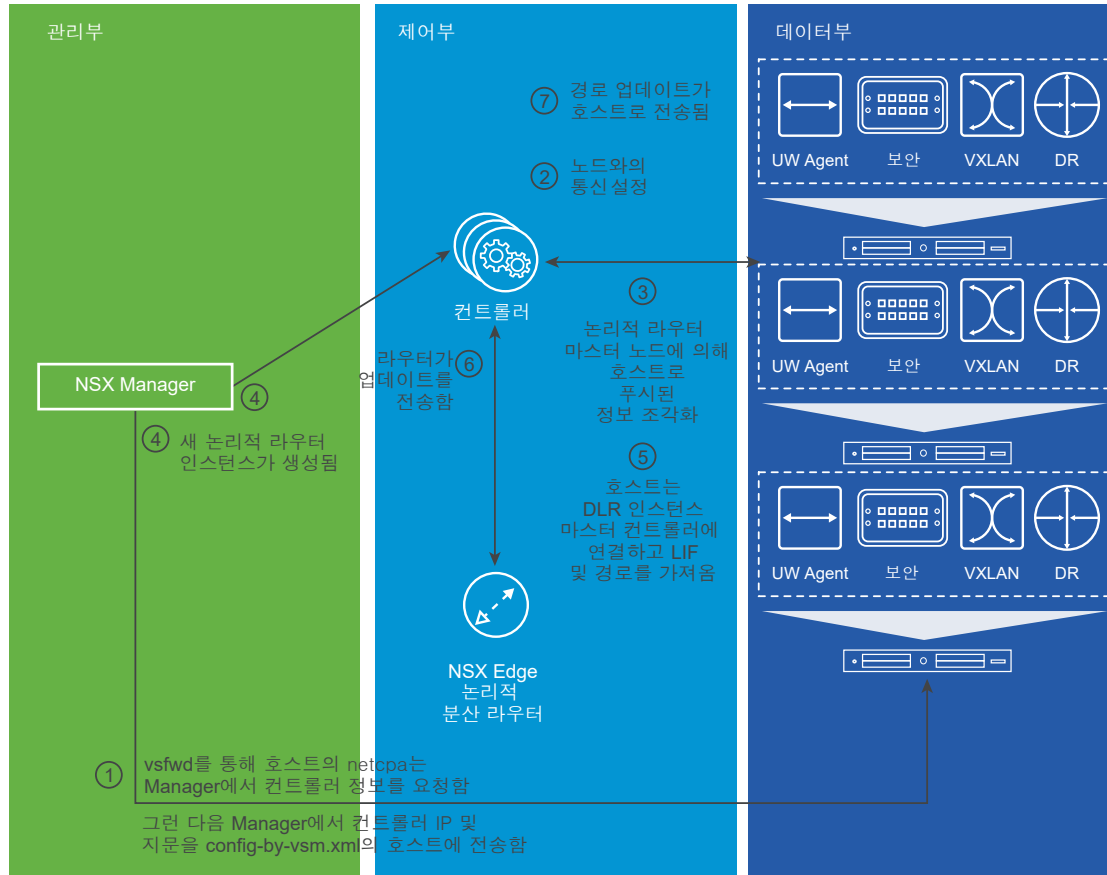
DLR은 한 번에 단일 동적 라우팅 프로토콜(OSPF 또는 BGP)의 실행을 지원하지만 ESG는 두 라우팅 프로토콜의 동시 실행을 지원합니다. 이는 DLR이 단일 출력 경로가 있는 “스텝” 라우터로 설계되었기 때문입니다. 즉, 좀 더 고급 수준의 라우팅 구성이 필요하지 않습니다.

DLR 및 ESG 둘 다 정적 및 동적 경로 조합을 지원합니다.

DLR 및 ESG 둘 다 ECMP 경로를 지원합니다.

둘 다 L3 도메인 분리를 제공합니다. 즉, 논리적 분산 라우터 또는 Edge Services Gateway의 각 인스턴스에는 L3VPN VRF와 비슷하게 자체 L3 구성이 있습니다.

그림 3-1. DLR 생성



본 장은 다음 항목을 포함합니다.

- 논리적 분산 라우터 이해
- Edge Services Gateway에서 제공하는 라우팅 이해
- ECMP 패킷 흐름
- NSX 라우팅: 전제 조건 및 고려 사항
- DLR 및 ESG UI
- 새 NSX Edge(DLR)
- 일반적인 ESG 및 DLR UI 작업
- NSX 라우팅 문제 해결

논리적 분산 라우터 이해

DLR은 VM 간의 논리적 공간, VXLAN 지원 또는 VLAN 지원 포트 그룹에서 전달을 수행하도록 최적화되어 있습니다.

DLR은 다음 속성을 갖습니다.

- 고성능, 낮은 오버헤드 첫 번째 홉 라우팅:
- 호스트 수를 선형으로 확장
- 업링크에서 8방향 ECMP 지원
- 호스트별 최대 1,000개의 DLR 인스턴스
- 각 DLR(업링크 8개 + 내부 991개)에 대해 최대 999개의 LIF(논리적 인터페이스) + 관리 1개
- 모든 DLR 인스턴스 간에 분산된 호스트별 최대 10,000개의 LIF(NSX Manager에 의해 적용되지 않는)

다음과 같은 사항에 유의하십시오.

- 둘 이상의 DLR을 지정된 VLAN 또는 VXLAN에 연결할 수 없습니다.
- 각 DLR에서 둘 이상의 라우팅 프로토콜을 실행할 수 없습니다.
- OSPF가 사용될 경우, 둘 이상의 DLR 업링크에서 실행할 수 없습니다.
- VXLAN 및 VLAN 간에 경로를 지정하려면 전송 영역이 단일 DVS를 포함해야 합니다.

DLR의 설계를 자세히 들여다보면 다음과 같은 방식에서 모듈식 라우터 새시와 유사합니다.

- ESXi 호스트는 다음과 같은 측면에서 라인 카드와 같습니다.
 - 연결된 엔드 스테이션(VM)을 포함하는 포트가 있습니다.
 - 여기에서 전달 결정이 수행됩니다.
- DLR 제어 VM은 다음과 같은 측면에서 경로 프로세서 엔진과 같습니다.
 - 동적 라우팅 프로토콜을 실행하여 나머지 네트워크와 라우팅 정보를 교환합니다.
 - 인터페이스 구성, 정적 경로 및 동적 라우팅 정보를 토대로 "라인 카드"에 대한 전달 테이블을 계산합니다.
 - 이러한 전달 테이블을 "라인 카드"로 프로그래밍합니다(컨트롤러 클러스터를 통해 확장성 및 복원력 설정).
- ESXi 호스트를 함께 연결하는 물리적 네트워크는 다음과 같은 측면에서 백플레인과 같습니다.
 - "라인 카드" 사이에 VLAN 캡슐화 또는 VXLAN 캡슐화 데이터를 전달합니다.

상위 수준 DLR 패킷 흐름

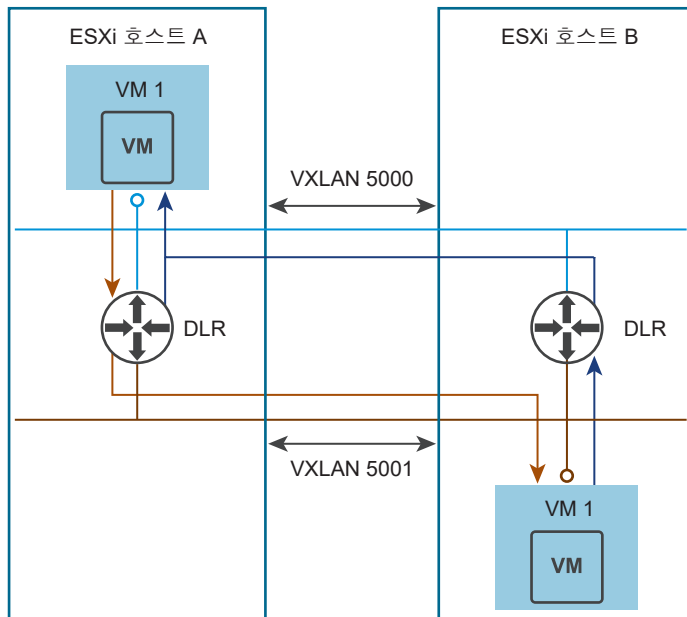
각 ESXi 호스트에는 구성된 각 DLR 인스턴스의 자체 복사본이 있습니다. 각 DLR 인스턴스에는 패킷 전달에 필요한 정보가 들어 있는 고유한 테이블 세트가 있습니다. 이 정보는 이 DLR 인스턴스가 있는 모든 호스트에서 동기화됩니다. 여러 다른 호스트에 있는 개별 DLR의 인스턴스는 정확히 동일한 정보를 갖고 있습니다.

라우팅은 항상 소스 VM이 실행되는 동일한 호스트의 DLR 인스턴스에 의해 처리됩니다. 즉, 소스 및 대상 VM이 다른 호스트에 있을 때 이들 사이에 라우팅을 제공하는 DLR 인스턴스는 한 방향(소스 VM에서 대상으로)으로만 패킷을 확인합니다. 반환 트래픽은 대상 VM 호스트에서 동일한 DLR의 해당 인스턴스에서 확인됩니다.

DLR이 라우팅을 완료하면 최종 대상으로의 전달은 소스 및 대상 VM이 다른 호스트에 있는 경우 L2 - VXLAN 또는 VLAN을 통해 DVS가 처리하고, 같은 호스트에 있는 경우 DVS가 직접 처리합니다.

그림 3-2. 상위 수준 DLR 패킷 흐름에서는 다른 호스트에서 실행되고 2개의 다른 논리적 스위치 VXLAN 5000 및 VXLAN 5001에 연결된 2개의 VM인 VM1 및 VM2 사이의 데이터 흐름을 보여줍니다.

그림 3-2. 상위 수준 DLR 패킷 흐름



패킷 흐름(ARP 확인은 건너뛸):

- 1 VM1은 VM2로 패킷을 전송하며 해당 주소는 VM2 서브넷에 대한 VM1 게이트웨이(또는 기본값)로 지정되어 있습니다. 이 게이트웨이는 DLR의 VXLAN 5000 LIF입니다.
- 2 ESXi 호스트 A의 DVS는 패킷을 해당 호스트의 DLR로 전달합니다. 여기서 조화가 수행되고 송신 LIF가 확인됩니다(이 경우 VXLAN 5001 LIF).
- 3 그런 다음 패킷이 해당 LIF에서 전송됩니다. 이 LIF는 기본적으로 이러한 패킷을 다른 논리적 스위치(5001)의 DVS로 반환합니다.
- 4 그러면 DVS는 L2를 통해 해당 패킷을 대상 호스트(ESXi 호스트 B)로 전달합니다. 여기서 DVS는 패킷을 VM2로 전달합니다.

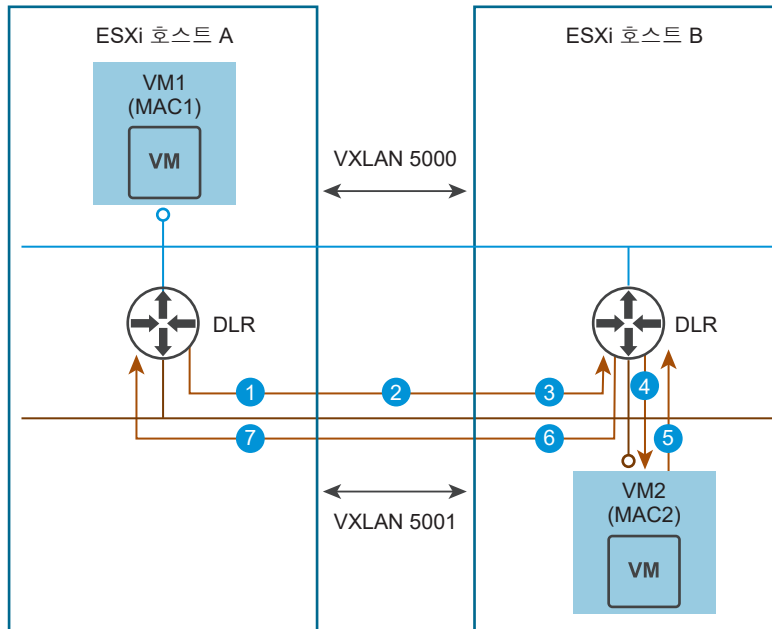
반환 트래픽은 동일한 순서를 따릅니다. 즉, VM2의 트래픽이 ESXi 호스트 B의 DLR 인스턴스로 전달된 후 VXLAN 5000의 L2를 통해 전달됩니다.

DLR ARP 확인 프로세스

VM1의 트래픽이 VM2에 도달하려면 먼저 DLR이 VM2의 MAC 주소를 인식해야 합니다. VM2의 MAC 주소를 인식한 후에 DLR은 아웃바운드 패킷에 대해 올바른 L2 헤더를 생성할 수 있습니다.

그림 3-3. DLR ARP 프로세스에는 DLR의 ARP 확인 프로세스가 나와 있습니다.

그림 3-3. DLR ARP 프로세스



MAC 주소를 인식하기 위해 DLR은 다음 단계를 따릅니다.

- 1 호스트 A의 DLR 인스턴스는 SRC MAC = vMAC 및 DST MAC = Broadcast인 ARP 요청 패킷을 생성합니다. 호스트 A의 VXLAN 모듈은 송신 VXLAN 5001에서 모든 VTEP를 찾은 후 각각에 해당 브로드캐스트 프레임 사본을 전송합니다.
- 2 프레임이 VXLAN 캡슐화 프로세스를 통해 호스트를 나가면 SRC MAC은 vMAC에서 pMAC A로 변경되므로 반환 트래픽은 호스트 A에서 원래 DLR 인스턴스를 찾을 수 있습니다. 이제 프레임은 SRC MAC = pMAC A 및 DST MAC = Broadcast입니다.
- 3 프레임이 호스트 B에서 수신되고 캡슐화가 해제되면 검사가 진행된 후 VXLAN 5001의 로컬 DLR 인스턴스 LIF와 일치하는 IP 주소에서 소싱되는지 확인됩니다. 이 경우 프레임은 프록시 ARP 기능을 수행하기 위한 요청으로 태그가 지정됩니다. 해당 프레임이 로컬 DLR 인스턴스에 도달할 수 있도록 DST MAC이 Broadcast에서 vMAC으로 변경됩니다.
- 4 호스트 B의 로컬 DLR 인스턴스는 ARP 요청 프레임, SRC MAC = pMAC A, DST MAC = vMAC을 수신하며, 이를 요청하는 자체 LIF IP 주소를 확인합니다. 그런 다음 SRC MAC을 저장하고 새로운 ARP 요청 패킷, SRC MAC = vMAC, DST MAC = Broadcast를 생성합니다. 이 프레임은 dvUplink를 통해 폭발적으로 증가하지 않도록 하기 위해 “DVS 로컬”로 태그가 지정됩니다. DVS는 프레임을 VM2에 전달합니다.

- 5 VM2는 ARP 응답, SRC MAC = MAC2, DST MAC = vMAC을 전송합니다. DVS는 이를 로컬 DLR 인스턴스로 전송합니다.
- 6 호스트 B의 DLR 인스턴스는 DST MAC을 4단계에서 저장된 pMAC A로 바꾼 후 호스트 A로 다시 전송하기 위해 패킷을 DVS로 보냅니다.
- 7 ARP 응답이 호스트 A에 도달하면 DST MAC은 vMAC으로 변경되고 SRC MAC = MAC2 및 DST MAC = vMAC이 지정된 ARP 응답 프레임은 호스트 A의 DLR 인스턴스에 도달합니다.

ARP 확인 프로세스가 완료되고 이제 호스트 A의 DLR 인스턴스는 VM2로 트래픽을 전송할 수 있습니다.

DLR ARP 억제

ARP(주소 확인 프로토콜) 억제는 동일한 논리적 스위치에 연결된 VM 사이에서 개별 VXLAN 세그먼트 내의 ARP 브로드캐스트 플러딩 양을 줄이는 데 사용되는 기술입니다.

VM1이 VM2의 MAC 주소를 알려고 할 경우 ARP 요청을 전송합니다. 이 ARP 요청이 논리적 스위치에 의해 인터셉트되고 논리적 스위치에 대상에 대한 ARP 항목이 이미 있으면 논리적 스위치는 VM으로 ARP 응답을 전송합니다.

그렇지 않은 경우 NSX Controller에 ARP 쿼리를 전송합니다. 컨트롤러가 VM IP - MAC 바인딩을 알고 있는 경우 컨트롤러는 해당 바인딩을 통해 응답하고 논리적 스위치는 ARP 응답을 전송합니다. 컨트롤러에 ARP 항목이 없는 경우 논리적 스위치에서 ARP 요청이 다시 브로드캐스트됩니다. NSX Controller는 ARP 요청/DHCP 패킷에서 스누핑하는 스위치 보안 모듈을 통해 MAC 주소를 학습합니다.

ARP 억제는 DLR(논리적 분산 라우터)도 포함하도록 확장되었습니다.

- 논리적 분산 라우터의 ARP 요청은 다른 VM의 ARP 요청과 동일한 방식으로 취급되며 억제됩니다. 논리적 분산 라우터가 대상 IP의 ARP 요청을 해결해야 할 경우 ARP 요청이 논리적 스위치에 의해 억제되어 컨트롤러에서 IP - MAC 바인딩을 이미 알고 있는 경우 플러딩이 방지됩니다.
- LIF가 생성되면 논리적 분산 라우터는 논리적 스위치에 LIF IP에 대한 ARP 항목을 추가하므로 LIF IP에 대한 ARP 요청도 논리적 스위치에 의해 억제됩니다.

Edge Services Gateway에서 제공하는 라우팅 이해

NSX 라우팅의 두 번째 하위 시스템은 Edge Services Gateway에서 제공됩니다.

ESG는 기본적으로 가상 시스템의 라우터입니다. 이 기능은 4가지 크기의 장치형 폼 팩터로 제공되며 전체 수명 주기가 NSX Manager를 통해 관리됩니다. ESG의 기본 사용 사례는 주변 라우터로서 사용되는 방식입니다. 이 경우 여러 DLR 간 및 물리적 환경과 가상화된 네트워크 간에 배포됩니다.

ESG는 다음과 같은 속성을 갖습니다.

- 각 ESG에는 최대 10개의 vNIC 인터페이스 또는 200개의 트렁크 하위 인터페이스가 있습니다.
- 각 ESG는 경로 이중화 및 확장성을 위해 8방향 ECMP를 지원합니다.

ECMP 패킷 흐름

물리적 환경이 있는 양방향 ECMP 업링크를 DLR 인스턴스에 제공하기 위해 2개의 ESG가 배포된다고 가정해보겠습니다.

그림 3-4. ECMP를 사용하는 고급 ESG 및 DLR 패킷 흐름에서는 두 ESG 및 물리적 인프라 간에 ECMP(동일 비용 다중 경로) 라우팅이 사용되도록 설정된 경우의 ESG 및 DLR 패킷 흐름을 보여줍니다.

따라서 VM1은 단일 ESG가 있는 배포와 비교할 때 2배의 양방향 처리량을 보여 줍니다.

VM1은 VNI 5000을 사용하여 논리적 스위치에 연결됩니다.

DLR에는 2개의 LIF가 있습니다. 하나는 VNI 5000의 내부용이고, 다른 하나는 VNI 5001의 업링크용입니다.

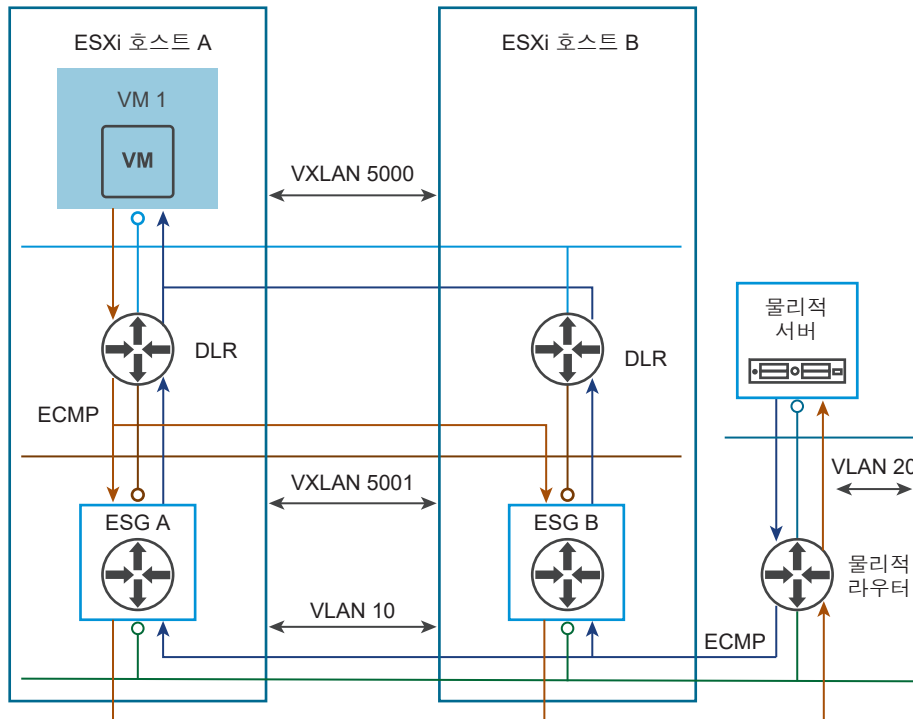
DLR에는 ECMP가 사용되도록 설정되어 있으며, 동적 라우팅 프로토콜(BGP 또는 OSPF)을 통해 ESG 쌍인 ESG A 및 ESG B에서 VLAN 20의 IP 서브넷으로 이동되는 동일 비용 경로가 수신됩니다.

두 ESG가 VLAN 10에 연결된 VLAN 지원 dvPortgroup에 연결됩니다. 여기서 VLAN 20에 대한 연결을 제공하는 물리적 라우터도 연결됩니다.

ESG는 물리적 라우터에서 동적 라우팅 프로토콜을 통해 VLAN 20에 대한 외부 경로를 수신합니다.

대신, 물리적 라우터는 두 ESG의 VXLAN 5000과 연결된 IP 서브넷에 대해 학습하고 해당 서브넷의 VM으로 전달되는 트래픽에 대해 ECMP 로드 밸런싱을 수행합니다.

그림 3-4. ECMP를 사용하는 고급 ESG 및 DLR 패킷 흐름



DLR은 최대 8개의 동일 비용 경로를 수신하고 경로 간에 트래픽 밸런스를 유지할 수 있습니다. 다이어그램의 ESG A 및 ESG B는 2개의 동일 비용 경로를 제공합니다.

ESG는 물리적 네트워크로의 ECMP 라우팅을 수행할 수 있으며 여러 물리적 경로가 존재한다고 가정합니다. 단순화를 위해 이 다이어그램에서는 단일 물리적 라우터를 표시합니다.

모든 DLR LIF가 ESG가 상주하는 동일한 호스트에서 “로컬” 이므로 ECMP를 DLR에 대한 ESG에 구성할 필요가 없습니다. DLR에 여러 업링크 인터페이스를 구성함으로써 제공되는 추가적인 이점은 없습니다.

추가 북쪽-남쪽 대역폭이 필요한 상황에서는 여러 ESG를 다른 ESXi 호스트에 배치하여 8개의 ESG로 80Gbps까지 확장할 수 있습니다.

ECMP 패킷 흐름(ARP 확인 포함 안 함):

- 1 VM1은 물리적 서버로 패킷을 전송하며, 이 패킷은 ESXi 호스트 A의 VM1 IP 게이트웨이(DLR LIF)로 전송됩니다.
- 2 DLR은 물리적 서버 IP의 경로를 조회하고, 직접 연결되지 않았지만 ESG A 및 ESG B에서 수신된 두 ECMP 경로에 일치하는지 확인합니다.
- 3 DLR은 ECMP 해시를 계산하고, ESG A 또는 ESG B 중에서 다음 홉이 될 수 있는 항목을 결정한 다음 패킷을 VXLAN 5001 LIF로 전송합니다.
- 4 DVS는 선택된 ESG로 패킷을 전달합니다.
- 5 ESG는 라우팅 조회를 수행하고, 물리적 서버의 서브넷을 ESG의 인터페이스 중 하나에 직접 연결된 VLAN 10의 물리적 라우터 IP 주소를 통해 액세스할 수 있는지 확인합니다.
- 6 패킷은 DVS를 통해 전송되며 DVS는 VLAN ID 10을 사용하여 해당 패킷에 올바른 801.Q 태그를 지정한 후 물리적 네트워크로 전달합니다.
- 7 패킷은 물리적 스위칭 인프라를 통해 이동하여 물리적 라우터에 도달합니다. 그러면 물리적 라우터는 조회를 통해 물리적 서버가 VLAN 20의 인터페이스에 직접 연결되었는지 확인합니다.
- 8 물리적 라우터는 물리적 서버에 패킷을 전송합니다.

역방향 전송:

- 1 물리적 서버는 물리적 라우터를 다음 홉으로 사용하여 VM1으로 패킷을 전송합니다.
- 2 물리적 라우터는 VM1의 서브넷을 조회하고, 다음 홉인 ESG A 및 ESG B의 VLAN 10 인터페이스 각각의 해당 서브넷에 대한 두 동일 비용 경로를 확인합니다.
- 3 물리적 라우터는 경로 중 하나를 선택하고 해당 ESG로 패킷을 전송합니다.
- 4 물리적 네트워크는 ESG가 상주하는 ESXi 호스트로 패킷을 전달한 다음 패킷 캡슐화를 해제하는 DVS로 전달하고 VLAN 10에 연결된 dvPortgroup의 패킷을 ESG로 전달합니다.
- 5 ESG는 라우팅 조회를 수행하고 다음 홉인 DLR의 업링크 인터페이스 IP 주소의 VXLAN 5001과 연결된 해당 인터페이스를 통해 VM1 서브넷에 액세스할 수 있는지 확인합니다.
- 6 ESG는 ESG와 동일한 호스트의 DLR 인스턴스로 패킷을 전송합니다.
- 7 DLR은 라우팅 조회를 수행하여 VM1을 해당 VXLAN 5000 LIF를 통해 사용할 수 있는지 확인합니다.

8 DLR은 VXLAN 5000 LIF에서 DVS로 패킷을 전송하며, DVS에서 최종 전달을 수행합니다.

NSX 라우팅: 전제 조건 및 고려 사항

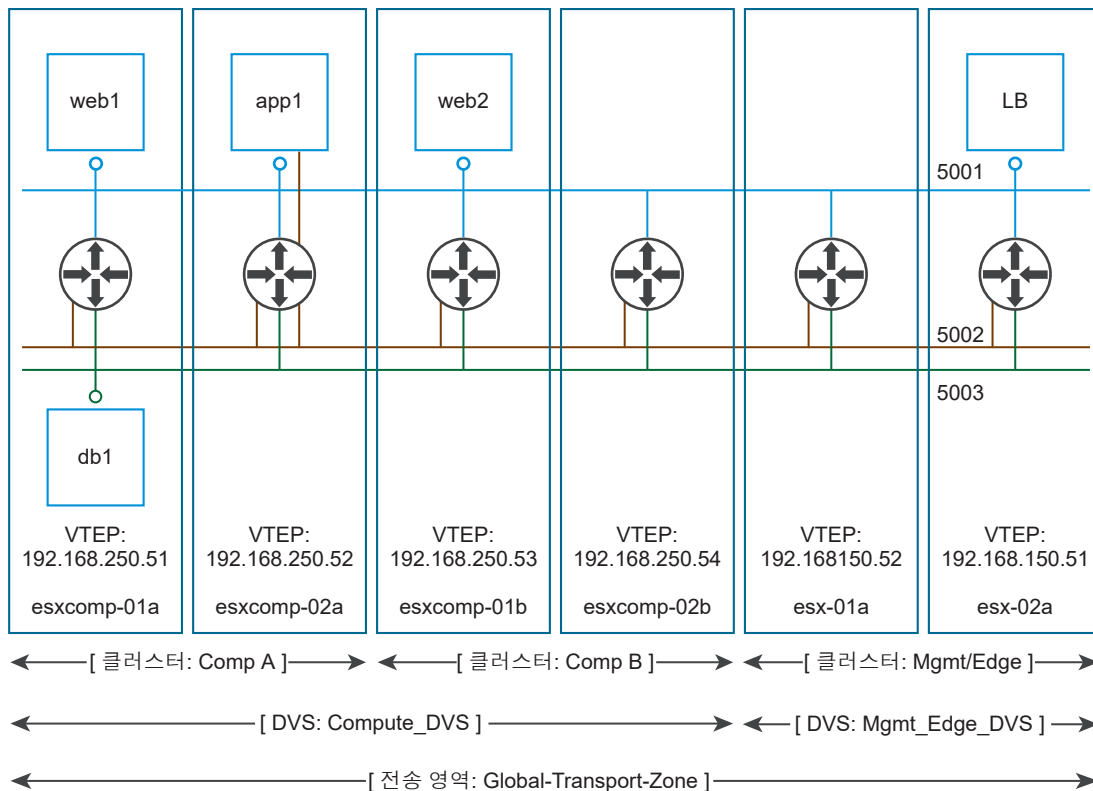
DLR 및 ESG는 dvPortgroup(VXLAN 및 VLAN 기반)에 L2 전달 서비스를 제공하여 중단 간 연결을 작동하기 위해 DVS에 의존합니다.

즉, DLR 또는 ESG에 연결된 서비스를 전달하는 L2가 구성되고 작동되어야 함을 의미합니다. NSX 설치 프로세스에서 이러한 서비스는 “호스트 준비” 및 “논리적 네트워크 준비”를 통해 제공됩니다.

다중 클러스터 DVS 구성에서 전송 영역을 생성할 경우 선택된 DVS의 모든 클러스터가 전송 영역에 포함되어 있는지 확인하십시오. 이를 통해 DVS dvPortgroup을 사용할 수 있는 모든 클러스터에서 DLR을 사용할 수 있도록 합니다.

전송 영역이 DVS 경계에 맞춰 설정되면 DLR 인스턴스가 올바르게 생성됩니다.

그림 3-5. 전송 영역이 DVS 경계에 맞춰 설정된 경우



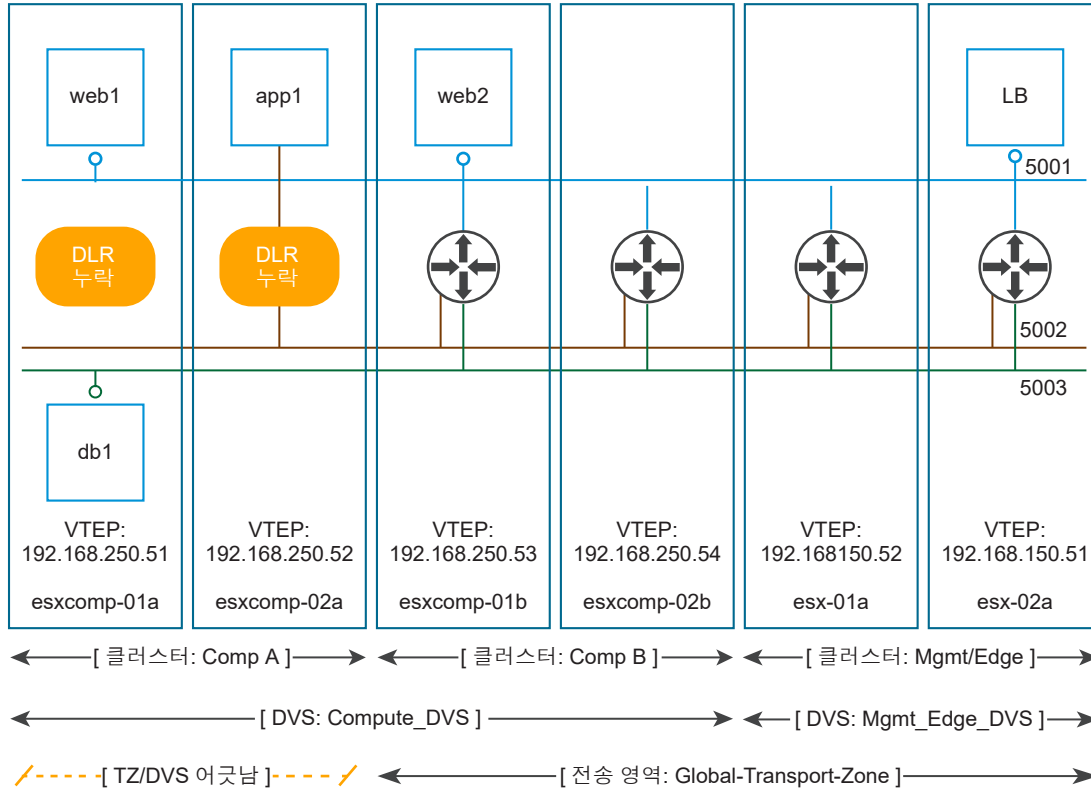
전송 영역이 DVS 경계에 맞춰지지 않은 경우 논리적 스위치의 범위(5001, 5002 및 5003) 및 이 논리적 스위치가 연결된 DLR 인스턴스가 연결 해제되기 때문에 Comp A 클러스터의 VM이 DLR LIF에 액세스할 수 없게 됩니다.

위 다이어그램에서 DVS “Compute_DVS”는 2개의 클러스터, 즉 “Comp A” 및 “Comp B”를 포함합니다. “Global-Transport-Zone”에는 “Comp A”와 “Comp B”가 둘 다 포함됩니다.

결과적으로 논리적 스위치의 범위(5001, 5002, 5003)와 이러한 논리적 스위치가 있는 모든 클러스터의 모든 호스트에서 생성된 DLR 인스턴스가 올바르게 정렬됩니다.

이제 전송 영역이 클러스터 “Comp A”를 포함하지 않도록 구성된 다른 경우를 살펴보겠습니다.

그림 3-6. 전송 영역이 DVS 경계에 맞춰 설정되지 않은 경우



이 경우 클러스터 “Comp A”에서 실행되는 VM은 모든 논리적 스위치에 대해 모든 액세스 권한을 갖습니다. 논리적 스위치가 호스트의 dvPortgroup으로 표현되고 dvPortgroup이 DVS 전체 구성이기 때문입니다. 샘플 환경에서 “Compute_DVS”는 “Comp A”와 “Comp B”를 둘 다 포함합니다.

그렇지만 DLR 인스턴스는 전송 영역 범위에 딱 맞게 생성됩니다. 즉, DLR 인스턴스는 “Comp A”의 호스트에 생성되지 않습니다.

결과적으로 VM “web2” 및 “LB”가 같은 논리적 스위치에 있기 때문에 VM “web1”에서 이러한 항목에 연결할 수 있지만 VM “app1” 및 “db1”은 어떤 대상과도 통신할 수 없습니다.

DLR은 작동을 위해 컨트롤러 클러스터가 필요하지만 ESG는 그렇지 않습니다. DLR 구성을 생성하거나 변경하기 전에 컨트롤러 클러스터가 최신 상태이고 사용 가능한지 확인하십시오.

DLR을 VLAN dvPortgroup에 연결해야 할 경우 DLR VLAN 기반 ARP 프록시가 작동하려면 DLR이 구성된 ESXi 호스트가 UDP/6999에서 서로 연결할 수 있어야 합니다.

고려 사항:

- 지정된 DLR 인스턴스는 다른 전송 영역에 있는 논리적 스위치에 연결할 수 없습니다. 이를 통해 모든 논리적 스위치와 DLR 인스턴스가 서로 맞춰 정렬될 수 있게 됩니다.

- DLR이 둘 이상의 DVS에 걸쳐 있는 논리적 스위치에 연결된 경우 해당 DLR을 VLAN 지원 포트 그룹에 연결할 수 없습니다. 위와 같이 이를 통해 DLR 인스턴스가 호스트 간의 논리적 스위치 및 dvPortgroup에 맞춰 올바르게 정렬될 수 있게 됩니다.
- DLR 제어 VM을 배치할 때 동일한 클러스터에 있는 경우 DRS 반선회도 규칙을 사용하여 하나 이상의 업스트림 ESG와 동일한 호스트에 배치하지 않도록 하십시오. 이렇게 하면 호스트 장애가 DLR 전달에 미치는 영향을 줄일 수 있습니다.
- OSPF는 단일 업링크에서만 사용하도록 설정할 수 있습니다(그렇지만 다중 인접성을 지원함). 그렇지만 BGP는 필요한 경우 여러 업링크 인터페이스에서 사용되도록 설정할 수 있습니다.

DLR 및 ESG UI

DLR 및 ESG UI는 시스템 작동 상태 표시기를 제공합니다.

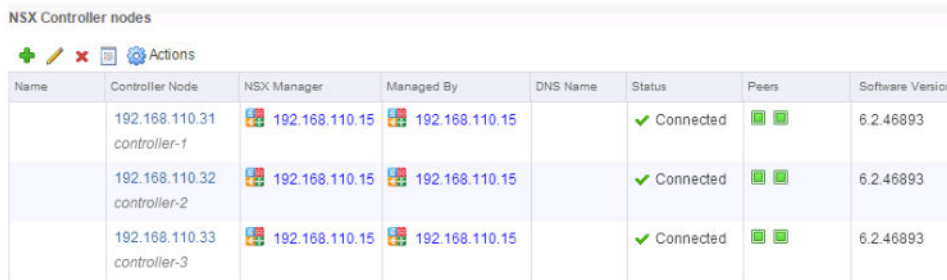
NSX 라우팅 UI

vSphere Web Client UI는 NSX 라우팅과 관련된 2가지 주요 섹션을 제공합니다.

여기에는 L2 및 제어부 인프라 종속성과 라우팅 하위 시스템 구성이 포함됩니다.

NSX 분산 라우팅에는 컨트롤러 클러스터에서 제공하는 기능이 필요합니다. 다음 스크린샷은 정상 상태의 컨트롤러 클러스터를 보여줍니다.

NSX Controller nodes



Name	Controller Node	NSX Manager	Managed By	DNS Name	Status	Peers	Software Version
	192.168.110.31 controller-1	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893
	192.168.110.32 controller-2	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893
	192.168.110.33 controller-3	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893

유의 사항:

- 배포된 3개의 컨트롤러가 있습니다.
- 모든 컨트롤러의 “실행 상태”는 “연결됨”입니다.
- 모든 컨트롤러에 대한 소프트웨어 버전이 같습니다.
- 각 컨트롤러 노드에는 2개의 피어가 있습니다.

분산 라우팅에 대한 호스트 커널 모듈이 호스트에 설치되고 VXLAN 구성의 일부로 구성됩니다. 즉, 분산 라우팅에서는 ESXi 호스트가 준비되고 이 위에 VXLAN이 구성되어야 합니다.

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶ Compute Cluster A	✓ 6.2.3.3771501	✓ Enabled	✓ Configured
▶ Management & Edge Cluster	✓ 6.2.3.3771501	✓ Enabled	✓ Configured

유의 사항:

- “설치 상태”가 녹색입니다.
- “VXLAN”은 “구성됨”입니다.

VXLAN 전송 구성 요소가 올바르게 구성되어 있는지 확인하십시오.

VXLAN Transport		Segment ID	Transport Zones				
Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing	Teaming Policy	VTEP
▼ Compute Cluster A	Unconfigure	vds-site-a	0	1600	IP Pool	Fail Over	1
esx-02a.corp.local	Ready				vmk3: 192.168.130.51		
esx-01a.corp.local	Ready				vmk3: 192.168.130.52		
▼ Management & Edge	Unconfigure	vds-mgt-edge	0	1600	IP Pool	Fail Over	1
esxmgmt-02a.corp.l	Ready				vmk3: 192.168.120.52		
esxmgmt-01a.corp.l	Ready				vmk3: 192.168.120.51		

유의 사항:

- VTEP 전송 VLAN의 VLAN ID가 올바른 것이어야 합니다. 위 스크린샷에서는 "0"으로 나와 있지만 대부분의 실제 배포에서는 그렇지 않습니다.
- MTU는 1600 이상으로 구성됩니다. VM의 MTU도 9000으로 설정될 것이라는 가정 하에 MTU를 9000으로 설정하지 않았는지 확인하십시오. DVS 최대 MTU가 9000이고, VM도 9000에 있는 경우 VXLAN 헤더에 대한 공간이 없습니다.
- VMKNic가 올바른 주소를 가져야 합니다. 169.254.x.x 주소로 설정되어 있지 않은지 확인하십시오. 이 주소로 설정되어 있으면 노드가 DHCP에서 주소를 가져오지 못한 것입니다.
- 동일한 DVS의 모든 클러스터 멤버에 대해 팀 구성 정책이 일관되어야 합니다.
- VTEP의 수가 dvUplink의 수와 같아야 합니다. 유효한/예상된 IP 주소가 나열되는지 확인하십시오.

일부 클러스터에서 DLR이 누락되는 상황을 피하려면 전송 영역이 DVS 경계에 맞춰 올바르게 정렬되어야 합니다.

Name	NSX vSwitch	Status
Compute Cluster A	vds-site-a	Normal
Management & Edge ...	vds-mgt-edge	Normal

NSX Edge UI

NSX 라우팅 하위 시스템은 UI의 “NSX Edge” 섹션에서 구성되고 관리됩니다.

이 UI 부분을 선택하면 다음 보기가 나타납니다.

Home

Networking & Security

NSX Home

Dashboard

Installation

Logical Switches

NSX Edges

Firewall

SpooGuard

NSX Manager: 192.168.110.15 (Role: Primary)

0 Installing 0 Failed










Id	Name	Type	Version	Status	Tenant	Interfaces	Size
edge-2	Local-Distributed-Router	Logical Router	6.2.3	Deployed	Default	4	Compact
edge-3	Perimeter-Gateway-01	NSX Edge	6.2.3	Deployed	Default	2	Compact
edge-4	OneArm-LoadBalancer-01	NSX Edge	6.2.3	Deployed	Default	1	Compact
edge-5	Perimeter-Gateway-02	NSX Edge	6.2.3	Deployed	Default	2	Compact
edge-6	OneArm-LoadBalancer-02	NSX Edge	6.2.3	Deployed	Default	1	Compact
edge-9178...	Universal-Distributed-Router	Universal Distributed Router	6.2.3	Deployed	Default	4	Compact

현재 배포된 모든 DLR 및 ESG가 표시되고 각각에 대해 다음 정보가 표시됩니다.

- “Id” 는 해당 ESG 또는 DLR을 나타내는 모든 API 호출에 사용할 수 있는 ESG 또는 DLR Edge 장치 ID를 표시합니다.
- “Tenant” + “Id” 가 DLR 인스턴스 이름을 만듭니다. 이 이름은 NSX CLI에서 표시되고 사용됩니다.
- “Size” 는 DLR에 대해 항상 “소형” 이며 ESG의 작업자가 선택한 크기가 됩니다.

테이블에 표시된 정보 외에 버튼이나 "작업"을 통해 액세스할 수 있는 컨텍스트 메뉴가 있습니다.

표 3-1. NSX Edge 컨텍스트 메뉴

아이콘	작업
	“강제 동기화” 작업은 ESG 또는 DLR의 제어 VM 구성을 지우고 재부팅하고 구성을 다시 푸시합니다.
	“다시 배포” 는 ESG 또는 DLR을 분해하고 동일한 구성의 새 ESG 또는 DLR을 만듭니다. 기존 ID는 보존됩니다.
	“자동 규칙 구성 변경” 은 ESG에서 서비스가 사용되도록 설정될 때 생성된 ESG의 내장 방화벽 규칙에 적용됩니다(예: TCP/179가 필요한 BGP).
	“기술 지원 로그 다운로드” 는 ESG 또는 DLR 제어 VM에서 로그 번들을 만듭니다. DLR의 경우 호스트 로그는 기술 지원 번들에 포함되지 않으며 별도로 수집해야 합니다.
	“장치 크기 변경” 은 ESG에만 적용됩니다. 새 장치에 “다시 배포” 가 수행됩니다(vNIC MAC 주소가 변경됨).
	“CLI 자격 증명 변경” 은 작업자가 CLI 자격 증명을 강제로 업데이트할 수 있도록 합니다. 5번의 로그인 시도가 실패한 후에 ESG 또는 DLR 제어 VM에서 CLI가 잠겨진 경우 이 옵션을 선택하면 잠금이 해제됩니다. 5분 동안 기다리거나 ESG/DLR을 “다시 배포” 하여 올바른 자격 증명으로 되돌아가야 합니다.
	“로그 수준 변경” 은 ESG/DLR Syslog로 전송할 세부 정보의 수준을 변경합니다.
	“고급 디버깅 구성” 은 사용하도록 설정된 코어 덤프와 코어 덤프 파일을 저장하기 위해 연결된 추가 가상 디스크를 포함한 ESG 또는 DLR을 다시 배포합니다.
	“배포” 는 ESG가 생성되기만 하고 배포되지 않았을 때 사용할 수 있습니다. 이 옵션은 배포 단계(OVF 배포, 인터페이스 구성, 생성한 장치에 구성 푸시)를 실행합니다.
	DLR/ESG의 버전이 NSX Manager보다 오래된 경우 “버전 업그레이드” 옵션을 사용할 수 있게 됩니다.
	“필터” 는 “이름” 으로 ESG/DLR을 검색할 수 있도록 합니다.

새 NSX Edge(DLR)

작업자가 새 DLR을 만들면 다음 마법사에서 필요한 정보를 수집합니다.

New NSX Edge

1 Name and description

Name and description

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

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

☐ Universal Logical (Distributed) Router
Provides Distributed Routing capabilities for Universal Logical Switches.

Name:

Hostname:

Description:

Tenant:

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

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

“이름 및 설명” 화면에서 다음 정보가 수집됩니다.

- “이름” 이 “NSX Edge” UI에 나타납니다.
- “호스트 이름” 은 SSH/콘솔 세션, syslog 메시지 및 ESG/DLR VM에 대한 vCenter “요약” 페이지에 있는 “DNS 이름” 에 표시되는 ESG 또는 DLR 제어 VM의 DNS 이름을 설정하는 데 사용됩니다.
- “설명” 은 NSX Edge의 목록을 표시하는 UI에 있습니다.
- “테넌트” 는 NSX CLI에 사용되는 DLR 인스턴스 이름을 만드는 데 사용됩니다. 외부 클라우드 관리 플랫폼에서도 사용될 수 있습니다.

“설정” 화면:

New NSX Edge

2 Settings

Settings

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

User Name:

Password:

Confirm password:

☒ Enable SSH access

Edge Control Level Logging:

Set the Edge Control Level Logging

- “사용자 이름” 및 “암호” 는 DLR 제어 VM에 액세스하기 위한 CLI/VM 콘솔 자격 증명을 설정합니다. NSX는 ESG 또는 DLR 제어 VM에서 AAA를 지원하지 않습니다. 이 계정은 ESG/DLR 제어 VM에 대해 모든 권한을 가지지만 CLI/VMconsole을 통해 ESG/DLR 구성을 변경할 수 없습니다.
- “SSH 액세스 사용” 을 선택하면 DLR 제어 VM의 SSH 데몬을 시작할 수 있습니다.
 - SSH 네트워크 액세스를 허용하려면 제어 VM 방화벽 규칙을 조정해야 합니다.

- 작업자는 제어 VM 관리 인터페이스의 서브넷에 있는 호스트에서 또는 프로토콜 주소가 구성된 경우 OSPF/BGP “프로토콜 주소”에 대한 이러한 제한 없이 DLR 제어 VM에 연결할 수 있습니다.

참고 DLR 제어 VM과 해당 DLR의 “내부” 인터페이스에 구성된 임의의 서브넷에 속하는 임의의 IP 주소 간에 네트워크 연결을 할 수 없습니다. DLR 제어 VM의 이러한 서브넷에 대한 송신 인터페이스가 데이터부에 연결되지 않은 유사 인터페이스 “VDR”을 가리키기 때문입니다.

- “HA 사용” 을 선택하면 제어 VM이 활성/대기 HA 쌍으로 배포됩니다.
- “Edge 제어 수준 로깅” 을 선택하면 Edge 장치에 대해 syslog 수준이 설정됩니다.

“배포 구성” 화면:

- “데이터센터” 를 선택하면 제어 VM을 배포할 vCenter 데이터센터가 선택됩니다.
- “NSX Edge Appliance” 는 DLR 제어 VM을 나타내며, 정확히 1개를 정의할 수 있도록 합니다(그림 참조).
- “HA” 를 사용하도록 설정하면 동일한 클러스터, 호스트 및 데이터스토어에 대기 Edge가 배포됩니다. 활성 및 대기 DLR 제어 VM에 대해 DRS “별도의 가상 시스템” 규칙이 생성됩니다.

“인터페이스 구성” 화면:

- “HA 인터페이스”
 - 라우팅할 수 있는 DLR 논리적 인터페이스로 생성되지 않습니다. 제어 VM의 유일한 vNIC입니다.
 - NSX는 VMCI를 통해 DLR 구성을 관리하므로 이 인터페이스에는 IP 주소가 필요하지 않습니다.

- "이름 및 설명" 화면에서 **DLR "고가용성 사용"** 을 선택한 경우 **HA** 하트비트에 이 인터페이스가 사용됩니다.
- "이 NSX Edge의 인터페이스" 는 **DLR LIF**(논리적 인터페이스)를 나타냅니다.
 - DLR은 해당 서브넷의 **IP** 주소가 있는 "연결 대상" **dvPortgroup** 또는 논리적 스위치의 **VM**에 **L3** 게이트웨이 서비스를 제공합니다.
 - "업링크" 유형 **LIF**는 제어 **VM**에서 **vNIC**로 생성되므로 최대 **8**개가 지원됩니다. 사용 가능한 마지막 두 **vNIC**는 **HA** 인터페이스와 예약된 **1**개의 **vNIC**에 할당됩니다.
 - DLR에 대해 동적 라우팅이 작동하려면 "업링크" 유형 **LIF**가 필요합니다.
 - 또한 "내부" 유형 **LIF**가 제어 **VM**에서 유사 **vNIC**로 생성되며 최대 **991**개가 가능합니다.

"기본 게이트웨이 설정" 화면:

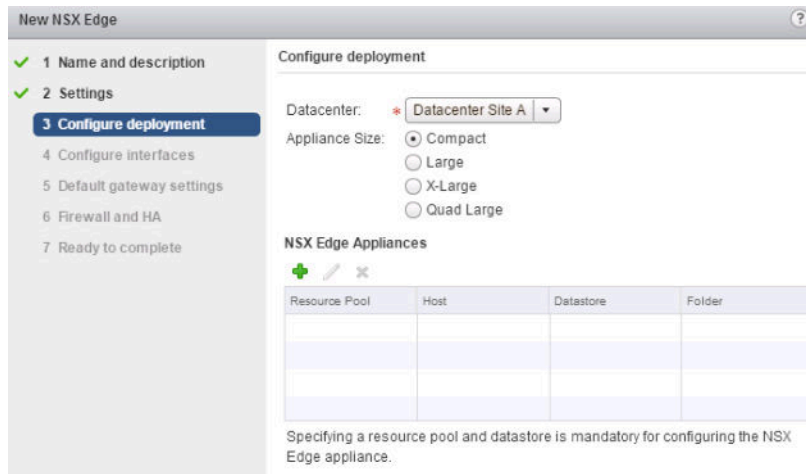
- [기본 게이트웨이 구성]을 선택하면 **DLR**에 대한 정적 기본 경로가 생성됩니다. 이 옵션은 "업링크" 유형의 **LIF**가 이전 화면에서 만들어지는 경우에 사용할 수 있습니다.
- 업링크에서 **ECMP**가 사용될 경우 다음 홉 실패 시 데이터부 중단을 방지하기 위해 이 옵션을 사용하지 않도록 설정하는 것이 좋습니다.

참고 상단 오른쪽 모서리에 있는 이중 오른쪽 화살표는 진행 중인 마법사를 "일시 중단" 하는 데 사용됩니다. 일시 중단한 마법사는 나중에 다시 시작할 수 있습니다.

ESG 및 DLR 차이점

ESG가 배포될 때의 마법사 화면은 **DLR**의 경우와 비교할 때 약간 다릅니다.

첫 번째 차이는 "배포 구성" 화면에서 나타납니다.



ESG의 경우 “배포 구성”에서 Edge 크기를 선택할 수 있습니다. ESG가 라우팅에만 사용되는 경우 “중형”이 대부분의 시나리오에 적합한 크기입니다. 더 큰 크기를 선택한다고 해서 ESG 라우팅 프로세스에 더 많은 CPU 리소스가 제공되는 것은 아니며 처리량이 늘어나지도 않습니다.

또한 배포하지 않고 ESG를 생성할 수도 있습니다. 이 경우에도 Edge Appliance를 구성해야 합니다.

“배포되지 않은” Edge는 나중에 API 호출 또는 “배포” UI 작업을 통해 배포할 수 있습니다.

Edge HA를 선택한 경우 하나 이상의 “내부” 인터페이스를 생성해야 합니다. 그렇지 않으면 HA가 자동으로 실패하여 “분할 브레인” 시나리오가 발생합니다.

NSX UI 및 API를 사용하여 작업자는 마지막 “내부” 인터페이스를 제거하여 HA가 자동으로 실패하도록 할 수 있습니다.

일반적인 ESG 및 DLR UI 작업

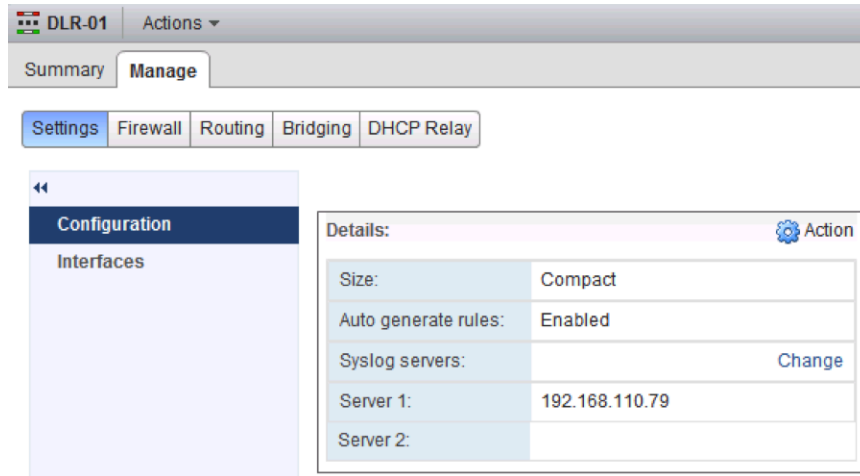
생성 외에 초기 배포 이후에 실행되는 몇 가지 구성 작업이 있습니다.

여기에는 다음이 포함됩니다.

- Syslog 구성
- 정적 경로 관리
- 라우팅 프로토콜 및 경로 재배포 구성

Syslog 구성

원격 Syslog 서버로 로그 항목을 보내도록 ESG 또는 DLR 제어 VM을 구성합니다.



참고:

- ESG/DLR 제어 VM은 DNS 확인자로 구성되지 않으므로 Syslog 서버는 IP 주소로 구성해야 합니다.
 - ESG의 경우 ESG 자체가 DNS 이름을 확인하는 데 사용할 수 있는 “DNS 서비스 사용” (DNS 프록시)을 설정할 수 있지만 일반적으로 좀 더 안정적이면서 종속성을 줄이는 방법은 Syslog 서버를 IP 주소로 지정하는 것입니다.
- UI에서는 Syslog 포트(항상 514)를 지정할 수 없지만 프로토콜(UDP/TCP)을 지정할 수 있습니다.
- Syslog 메시지는 Edge 전달 테이블에 의해 Syslog 서버 IP에 대한 송신으로 선택된 Edge 인터페이스의 IP 주소에서 생성됩니다.
 - DLR의 경우 Syslog 서버의 IP 주소는 DLR “내부” 인터페이스에 구성된 서브넷에 있을 수 없습니다. DLR 제어 VM의 이러한 서브넷에 대한 송신 인터페이스가 데이터부에 연결되지 않은 유사 인터페이스 “VDR” 을 가리키기 때문입니다.

기본적으로 ESG/DLR 라우팅 엔진에 대한 로깅은 사용되지 않도록 설정됩니다. 필요한 경우 “동적 라우팅 구성”에 대해 “편집” 을 클릭하여 UI에서 이 기능을 사용하도록 설정하십시오.

DLR-01 Actions ▾

Summary Manage

Settings Firewall Routing Bridging DHCP Relay

Global Configuration
Static Routes
OSPF
BGP
Route Redistribution

Routing Configuration : Reset

ECMP : Disabled Enable

Default Gateway : Edit Delete

Interface :
Gateway IP :
MTU :
Description :

Dynamic Routing Configuration : Edit

Router ID :
OSPF : Disabled
BGP : Disabled
Logging : Disabled
Log Level :

일반적으로 업링크 인터페이스의 IP 주소가 되는 라우터 ID도 구성해야 합니다.

정적 경로

정적 경로에서는 다음 홉이 DLR의 LIF 또는 ESG의 인터페이스 중 하나와 연결된 서브넷의 IP 주소로 설정되어야 합니다. 그렇지 않으면 구성이 실패합니다.

“인터페이스”를 선택하지 않으면 다음 홉을 직접 연결된 서브넷 중 하나와 일치시키는 방식으로 인터페이스가 자동으로 설정됩니다.

Add Static Route

Network: * 10.10.10.0/24
*Network should be entered in CIDR format
e.g. 192.169.1.0/24*

Next Hop: * 192.168.10.1

Interface:
MTU: 1500

Description:

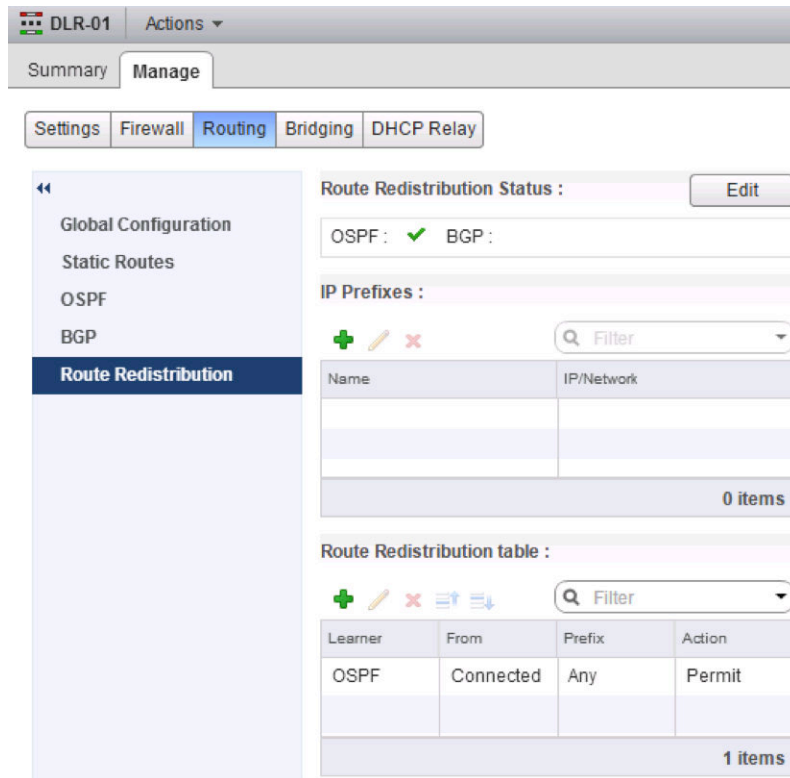
OK Cancel

경로 재배포

“경로 재배포 테이블”에 항목을 추가해도 선택한 “학습자 프로토콜”에 대한 재배포가 자동으로 사용되도록 설정되지 않습니다. 이 작업은 “경로 재배포 상태”의 “편집”에서 명시적으로 수행되어야 합니다.

DLR은 기본적으로 OSPF로 연결된 경로를 재배포하도록 구성되어 있으나 ESG는 그렇지 않습니다.

“경로 재배포 테이블”은 위에서 아래로 처리되며 첫 번째 일치 항목이 나타나면 처리가 중지됩니다. 재배포에서 일부 접두사를 제외하려면 맨 위에 좀 더 구체적인 항목을 포함하십시오.



NSX 라우팅 문제 해결

NSX는 라우팅이 작동되는지 확인하기 위한 여러 도구를 제공합니다.

NSX 라우팅 CLI

작업자가 NSX 라우팅 하위 시스템의 다양한 부분에 대한 실행 상태를 검사할 수 있는 CLI 명령 모음이 있습니다.

NSX 라우팅 하위 시스템의 분산 특성 때문에 NSX의 다양한 구성 요소에서 액세스할 수 있는 여러 CLI가 있습니다. NSX 버전 6.2부터 NSX는 다양한 분산 구성 요소에 액세스하고 로그인하는 데 필요한 "이동 시간"을 줄이는 데 도움이 되는 중앙 CLI도 제공합니다. 또한 단일 위치인 NSX Manager 셸에서 대부분의 정보에 액세스할 수 있도록 합니다.

전제 조건 확인

각 ESXi 호스트에 대해 다음 2가지 주요 전제 조건이 충족되어야 합니다.

- DLR에 연결되는 모든 논리적 스위치는 정상 상태여야 합니다.
- ESXi 호스트는 VXLAN에 대해 준비 완료 상태여야 합니다.

논리적 스위치 상태 점검

NSX 라우팅은 NSX 논리적 스위치와 함께 작동합니다. DLR에 연결된 논리적 스위치가 정상 상태인지 확인하려면:

- 문제의 DLR에 연결된 각 논리적 스위치의 세그먼트 ID(VXLAN VNI)를 찾습니다(예: 5004..5007).

Logical Switches						
NSX Manager: 192.168.110.42						
Name	1 ▲	Status	Transport Zone	Segment ID	Control Plane Mode	Description
LS A		✓ Normal	Global-Transport-Zone	5004	Unicast	
LS B		✓ Normal	Global-Transport-Zone	5005	Unicast	
LS C		✓ Normal	Global-Transport-Zone	5006	Unicast	
LS D		✓ Normal	Global-Transport-Zone	5007	Unicast	

- 이 DLR에서 제공하는 VM이 실행 중인 ESXi 호스트에서 이 DLR에 연결된 논리적 스위치에 대한 VXLAN 제어부의 상태를 확인합니다.

```
# esxcli network vswitch dvs vmware vxlan network list --vds-name=Compute_VDS
```

VXLAN ID	Multicast IP	Control Plane	Controller Connection	Port
Count	MAC Entry Count	ARP Entry Count		
5004	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.201	
(up)	2	2	0	
5005	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0	0	
5006	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203	
(up)	1	1	0	
5007	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0	0	

각 관련 VXLAN에 대해 다음을 확인합니다.

- 하이브리드 또는 유니캐스트 모드인 논리적 스위치의 경우:
 - 제어부가 "사용"으로 설정되어 있습니다.
 - “멀티캐스트 프록시” 및 “ARP 프록시”가 나열됩니다. “ARP 프록시”는 IP 검색을 사용하지 않도록 설정한 경우에도 표시됩니다.
 - 유효한 컨트롤러 IP 주소가 "컨트롤러" 아래에 나열되고 "연결"은 "실행" 상태입니다.
- “포트 수”는 맞는 것처럼 보입니다. 문제의 논리적 스위치에 연결된 해당 호스트에 VM이 없더라도 포트 수는 1 이상입니다. 이 포트는 ESXi 호스트의 DLR 커널 모듈에 연결된 특수한 dvPort인 vdrPort입니다.

- 다음 명령을 실행하여 vdrPort가 관련 VXLAN 각각에 연결되어 있는지 확인합니다.

```
~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5004
Switch Port ID   VDS Port ID   VMKNIC ID
-----
50331656        53            0
50331650        vdrPort       0

~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5005
Switch Port ID   VDS Port ID   VMKNIC ID
-----
50331650        vdrPort       0
```

- 위 예에서 VXLAN 5004에는 하나의 VM 및 하나의 DLR 연결이 있지만 VXLAN 5005에는 DLR 연결만 있습니다.
- 해당 VM이 해당 VXLAN에 제대로 연결되어 있는지 확인합니다(예: VXLAN 5004의 web-sv-01a).

```
~ # esxcfg-vswitch -l
DVS Name      Num Ports  Used Ports  Configured Ports  MTU      Uplinks
Compute_VDS   1536       10          512               1600     vmnic0

  DVPort ID      In Use      Client
[.skipped..]
  53             1           web-sv-01a.eth0
```

VXLAN 준비 점검

ESXi 호스트에 대한 VXLAN 구성의 일부로 DLR 커널 모듈도 VXLAN용으로 준비된 DVS의 dvPort에 설치되고, 구성되고, 연결됩니다.

- 1 show cluster all을 실행하여 클러스터 ID를 가져옵니다.
- 2 show cluster cluster-id를 실행하여 호스트 ID를 가져옵니다.
- 3 show logical-router host hostID connection를 실행하여 상태 정보를 가져옵니다.

```
nsxmgr-01a# show logical-router host <hostID> connection

Connection Information:
-----

DvsName      VdrPort      NumLifs  VdrVmac
-----
Compute_VDS  vdrPort      4        02:50:56:56:44:52
  Teaming Policy: Default Teaming
  Uplink   : dvUplink1(50331650): 00:50:56:eb:41:d7(Team member)
```


Stats : Pkt Dropped	Pkt Replaced	Pkt Skipped
Input : 0	0	1968734458
Output : 303	7799	31891126

- VXLAN이 사용하도록 설정된 DVS에 하나의 vdrPort가 생성되며 해당 ESXi 호스트의 모든 DLR 인스턴스에서 공유됩니다.
- “NumLifs” 는 이 호스트에 존재하는 모든 DLR 인스턴스의 LIF 합계를 나타냅니다.
- “VdrVmac” 는 DLR이 모든 인스턴스의 모든 LIF에서 사용하는 vMAC입니다. 이 MAC는 모든 호스트에서 동일합니다. ESXi 호스트 외부의 물리적 네트워크를 이동하는 프레임에서는 확인되지 않습니다.
- LACP/Etherchannel 팀 구성 모드가 사용되어, dvUplink 수와 관계없이 VTEP가 1개만 생성되는 경우를 제외하고, VXLAN이 사용하도록 설정된 DVS의 각 dvUplink에 대해 일치하는 VTEP가 있습니다.
 - 호스트를 나갈 때 DLR이 전송하는 트래픽(SRC MAC = vMAC)의 경우 SRC MAC가 해당 dvUplink의 pMAC로 변경됩니다.
 - 원래 VM의 소스 포트 또는 소스 MAC는 dvUplink를 확인하는 데 사용됩니다(DVS의 메타데이터에 있는 각 패킷에 대해 보존됨).
 - 호스트에 여러 VTEP가 있고 dvUplink 중 하나가 실패할 경우 실패한 dvUplink와 연결된 VTEP는 해당 VTEP에 고정된 모든 VM과 함께 남은 dvUplink 중 하나로 이동됩니다. 이 작업은 다른 VTEP로 VM을 이동할 때 발생하는 제어부 변경 내용이 너무 많아지지 않도록 하기 위해 수행됩니다.
- 각 “dvUplinkX” 옆의 “()” 에 있는 숫자는 dvPort 번호입니다. 개별 업링크의 패킷 캡처에 유용합니다.
- 각 “dvUplinkX” 에 대해 표시되는 MAC 주소는 해당 dvUplink와 연결된 “pMAC” 입니다. 이 MAC 주소는 DLR에서 시작된 트래픽(예: DLR에서 생성된 ARP 쿼리 및 이러한 패킷이 ESXi 호스트를 나갈 때 DLR에서 라우팅한 모든 패킷)에 사용됩니다. 이 MAC 주소는 물리적 네트워크에서 볼 수 있습니다(DLR LIF가 VLAN 유형인 경우 직접 또는 VXLAN LIF의 경우 VXLAN 패킷 내부에서).
- [Pkt Dropped], [Replaced], [Skipped]는 DLR의 내부 구현 세부 정보와 관련된 카운터를 나타내며, 일반적으로 문제 해결이나 모니터링에는 사용되지 않습니다.

라우팅 요약

라우팅 문제를 효과적으로 해결하려면 라우팅이 작동하는 방식과 관련 정보 테이블을 검토하는 것이 도움이 됩니다.

- 1 대상 IP 주소로 전송할 패킷을 수신합니다.
- 2 라우팅 테이블을 확인하고 다음 홉의 IP 주소를 파악합니다.
- 3 여기에 연결될 수 있는 네트워크 인터페이스를 확인합니다.
- 4 다음 홉의 MAC 주소를 가져옵니다(ARP를 통해).
- 5 L2 프레임을 구축합니다.
- 6 인터페이스 외부로 프레임을 전송합니다.

라우팅을 수행하려면 다음이 필요합니다.

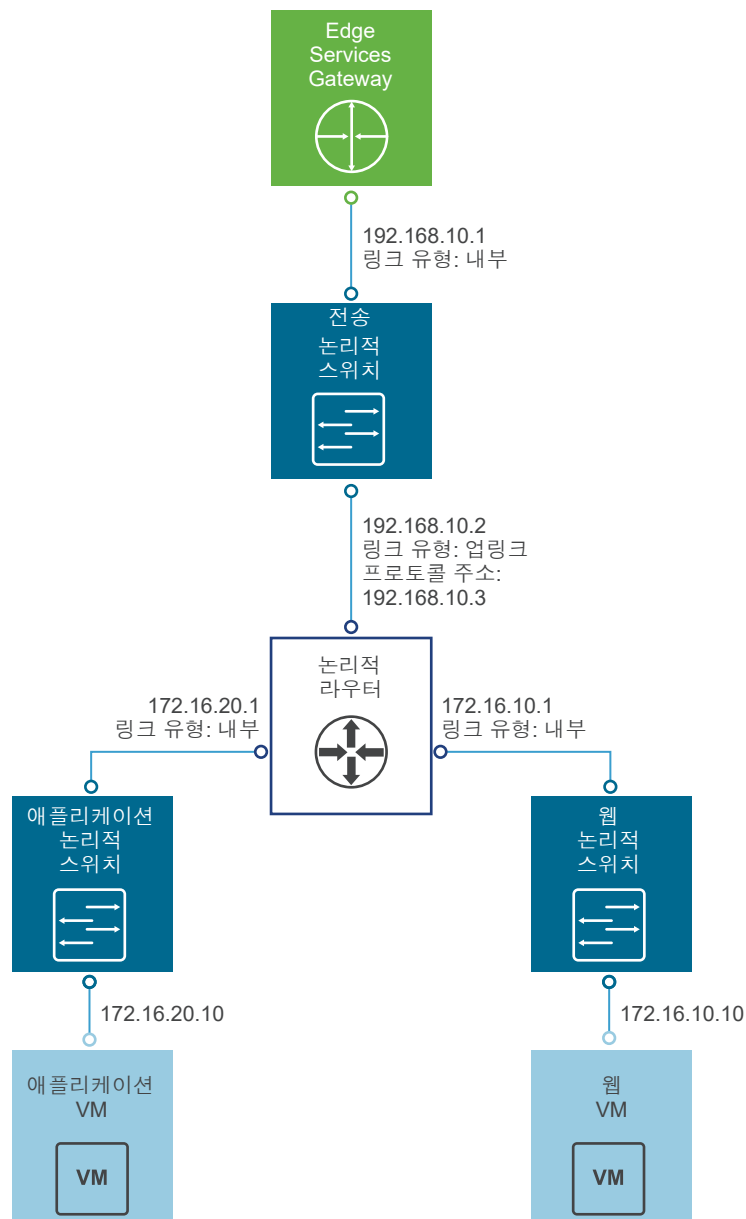
- 인터페이스 테이블(인터페이스 IP 주소 및 넷마스크 포함)
- 라우팅 테이블
- ARP 테이블

샘플 라우팅 토폴로지를 사용하여 DLR 상태 확인

이 섹션에서는 DLR이 패킷을 라우팅하기 위해 필요로 하는 정보를 확인하는 방법을 설명합니다.

샘플 라우팅 토폴로지를 살펴보고 NSX에서 생성하기 위한 논리적 스위치 및 DLR 집합을 생성해보겠습니다.

그림 3-7. 샘플 라우팅 토폴로지



이 다이어그램에는 다음이 표시됩니다.

- 각각 자체 서브넷이 있는 논리적 스위치 4개
- 논리적 스위치별 하나씩 연결된 VM 3개
 - 각각 자체 IP 주소 및 IP 게이트웨이 포함
 - 각각 MAC 주소(마지막 2개의 8진수가 표시됨) 포함
- 4개의 논리적 스위치에 연결된 DLR 1개, 논리적 스위치 1개는 “업링크” 용이고 나머지는 내부용임
- ESG일 수 있으며 DLR에 대한 업스트림 게이트웨이로 작동하는 외부 게이트웨이

위의 DLR에 대해 “완료 준비” 마법사 화면이 표시됩니다.

New NSX Edge

Ready to complete

Name and description

Name: DLR1
 Install Type: Logical (Distributed) Router
 Tenant:
 HA: Disabled

Management Interface Configuration

Connected To: Mgmt_Edge_VDS - Mgmt

IP Address	Subnet Prefix Length

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
Management and Edge Cluster		ds-site-a-nfs01	

Interfaces

Name	IP Address	Subnet Prefix Length	Connected To
LS A	172.16.10.1*	24	LS A
LS B	172.16.20.1*	24	LS B
LS C	172.16.30.1*	24	LS C
LS D	192.168.10.2*	29	LS D

Buttons: Back, Next, Finish, Cancel

DLR 배포가 완료되면 ESXi CLI 명령을 사용하여 참여 호스트에서 문제가 있는 DLR의 분산 상태를 확인하고 유효한지 검사할 수 있습니다.

DLR 인스턴스 확인

확인할 첫 번째 항목은 DLR 인스턴스가 생성되었는지 여부 및 해당 제어부가 활성 상태인지 여부입니다.

- 1 NSX Manager 셸에서 `show cluster all`을 실행하여 클러스터 ID를 가져옵니다.
- 2 `show cluster cluster-id`를 실행하여 호스트 ID를 가져옵니다.
- 3 `show logical-router host hostID dlr all verbose`를 실행하여 상태 정보를 가져옵니다.

```
nsxmgr# show logical-router host host-id dlr all verbose
```

```
VDR Instance Information :
```

```

Vdr Name:          default+edge-1
Vdr Id:            1460487509
Number of Lifs:    4
Number of Routes:  5
State:            Enabled
Controller IP:     192.168.110.201
Control Plane Active: Yes
Control Plane IP:  192.168.210.51
Edge Active:      No

```

유의 사항:

- 이 명령은 지정된 ESXi 호스트에 있는 모든 DLR 인스턴스를 표시합니다.
- “Vdr Name” 은 “테넌트” + “Edge ID” 로 구성됩니다. 이 예에서 “테넌트” 는 지정되지 않았으므로 단어 “default” 가 사용됩니다. “Edge ID” 는 NSX UI에서 볼 수 있는 “edge-1” 입니다.
 - 호스트에 많은 DLR 인스턴스가 있는 경우 적절한 인스턴스를 찾는 방법은 UI “NSX Edge” 에 표시된 “Edge ID” 를 찾는 것입니다.
- “Vdr Id” 는 로그를 포함하는 추가 조회에 유용합니다.
- “Number of Lifs” 는 이 개별 DLR 인스턴스에 있는 LIF를 나타냅니다.
- 이 경우 “Number of Routes” 는 직접 연결된 경로 4개(각 LIF에 대해 하나씩)와 기본 경로 1개를 합한 5개입니다.
- “State” , “Controller IP” 및 “Control Plane Active” 는 DLR 제어부의 상태를 나타내며 Control Plane Active: Yes인 올바른 컨트롤러 IP를 나열해야 합니다. DLR 기능에는 작업 컨트롤러가 필요합니다. 위 출력에는 정상 상태의 DLR 인스턴스에 필요한 컨트롤러를 보여줍니다.
- “Control Plane IP” 는 ESXi 호스트가 컨트롤러에 연결하는 데 사용하는 IP 주소를 나타냅니다. 이 IP 는 항상 ESXi 호스트의 관리 vmknic(대부분의 경우 vmk0)와 연결된 IP입니다.
- “Edge Active” 는 이 호스트가 이 DLR 인스턴스의 제어 VM이 실행되고 있는 호스트인지 여부와 활성 상태 여부를 나타냅니다.
 - 활성 DLR 제어 VM의 배치에 따라 NSX L2 브리징(사용하도록 설정된 경우)을 수행하는 데 사용되는 ESXi 호스트가 결정됩니다.
- 위 명령의 경우 빠르게 살펴보는 데 유용한 압축된 출력을 생성하는 “간단” 버전도 있습니다. “Vdr Id” 는 여기에서 16진수 형식으로 표시됩니다.

```
nsxmgr# show logical-router host host-id dlr all brief
```

```
VDR Instance Information :
```

```
-----
```

```
State Legend: [A: Active], [D: Deleting], [X: Deleted], [I: Init]
```

```
State Legend: [SF-R: Soft Flush Route], [SF-L: Soft Flush LIF]
```

Vdr Name	Vdr Id	#Lifs	#Routes	State	Controller Ip	CP Ip
-----	-----	-----	-----	-----	-----	-----
default+edge-1	0x570d4555	4	5	A	192.168.110.201	192.168.210.51

“Soft Flush” 상태는 LIF 수명 주기의 단기 일시적 상태를 나타내며 정상 상태의 DLR에서는 일반적으로 확인되지 않습니다.

DLR의 논리적 인터페이스

DLR이 생성되면 모든 DLR의 논리적 인터페이스가 존재하는지와 구성이 올바른지 확인하십시오.

- 1 NSX Manager 셸에서 `show cluster all`을 실행하여 클러스터 ID를 가져옵니다.
- 2 `show cluster cluster-id`를 실행하여 호스트 ID를 가져옵니다.
- 3 `show logical-router host hostID dlr all brief`를 실행하여 dlrID(Vdr 이름)를 가져옵니다.
- 4 `show logical-router host hostID dlr dlrID interface all brief`를 실행하여 모든 인터페이스에 대한 상태 정보 요약을 가져옵니다.
- 5 `show logical-router host hostID dlr dlrID interface (all | intName) verbose`를 실행하여 모든 인터페이스 또는 특정 인터페이스에 대한 상태 정보를 가져옵니다.

```
nsxmgr# show logical-router host hostID dlr dlrID interface all verbose
```

VDR default+edge-1:1460487509 LIF Information :

```
Name:          570d45550000000a
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5000
Ip(Mask):      172.16.10.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2388
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000c
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5002
Ip(Mask):      172.16.30.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2288
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000b
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5001
```

```

Ip(Mask):          172.16.20.1(255.255.255.0)
Connected Dvs:     Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:             Enabled
Flags:             0x2388
DHCP Relay:        Not enabled

Name:              570d455500000002
Mode:              Routing, Distributed, Uplink
Id:                Vxlan:5003
Ip(Mask):          192.168.10.2(255.255.255.248)
Connected Dvs:     Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:             Enabled
Flags:             0x2208
DHCP Relay:        Not enabled

```

유의 사항:

- LIF "Name"은 호스트의 모든 DLR 인스턴스에서 고유합니다. 호스트 및 DLR의 마스터 컨트롤러 노드에서 동일합니다.
- LIF의 "Mode"는 LIF가 라우팅하는지 또는 브리징하는지와 내부인지 또는 업링크인지를 나타냅니다.
- "Id"는 LIF 유형 및 해당 서비스 ID(VXLAN 및 VNI 또는 VLAN 및 VID)를 나타냅니다.
- "Ip(Mask)"는 "라우팅" LIF에 대해 표시됩니다.
- LIF가 하이브리드 또는 유니캐스트 모드로 VXLAN에 연결되어 있으면 "VXLAN Control Plane"이 "Enabled"입니다.
- VXLAN이 유니캐스트 모드인 VXLAN LIF의 경우 "VXLAN Multicast IP"는 "0.0.0.1"로 표시되고, 그렇지 않은 경우 실제 멀티캐스트 IP 주소가 표시됩니다.
- "State"는 라우팅된 LIF에 대해 "Enabled"여야 합니다. 브리징 LIF의 경우 브리징을 수행하는 호스트에서는 "Enabled"이고, 다른 모든 호스트에서는 "Init"입니다.
- "Flags"는 LIF 상태의 요약 표현이고 LIF가 다음 중 어떤 상태인지를 나타냅니다.
 - 라우팅 또는 브리징되었는지 여부
 - VLAN LIF가 DI인지 여부
 - DHCP 릴레이가 사용되도록 설정되어 있는지 여부
 - 중요한 사항은 플래그 0x0100입니다. 이 플래그는 VXLAN VNI 연결이 DLR(해당 VXLAN에 VM이 있는 호스트가 아님)에 의해 발생했을 때 설정됩니다.

- 플래그는 "간단" 모드에서 좀 더 읽기 쉬운 형식으로 표시됩니다.

```
nsxmgr# show logical-router host hostID dlr dlrID interface all brief
```

VDR default+edge-1 LIF Information :

State Legend: [A:Active], [d:Deleting], [X:Deleted], [I:Init],[SF-L:Soft Flush LIF]

Modes Legend: [B:Bridging],[E: Empty], [R:Routing],[S:Sedimented],[D:Distributed]

Modes Legend: [In:Internal],[Up:Uplink]

Lif Name	Id	Mode	State	Ip(Mask)
-----	--	----	-----	-----
570d45550000000a	Vxlan:5001	R,D,In	A	172.16.10.1(255.255.255.0)
570d45550000000c	Vxlan:5003	R,D,In	A	172.16.30.1(255.255.255.0)
570d45550000000b	Vxlan:5002	R,D,In	A	172.16.20.1(255.255.255.0)
570d455500000002	Vxlan:5000	R,D,Up	A	192.168.10.5(255.255.255.248)

DLR 경로

DLR이 존재하고 정상 상태이며 모든 LIF가 있는지 확인한 후에는 라우팅 테이블을 확인해야 합니다.

- 1 NSX Manager 셸에서 `show cluster all`을 실행하여 클러스터 ID를 가져옵니다.
- 2 `show cluster cluster-id`를 실행하여 호스트 ID를 가져옵니다.
- 3 `show logical-router host hostID dlr all brief`를 실행하여 dlrID(Vdr 이름)를 가져옵니다.
- 4 `show logical-router host hostID dlr dlrID route`를 실행하여 모든 인터페이스에 대한 상태 정보를 가져옵니다.

```
nsxmgr# show logical-router host hostID dlr dlrID route
```

VDR default+edge-1:1460487509 Route Table

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

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

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
-----	-----	-----	-----	---	-----	-----	-----
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	10068944	570d455500000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000a
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000b
172.16.30.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000c
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000002

유의 사항:

- “Interface” 는 해당 “Destination” 에 대해 선택할 송신 LIF를 나타냅니다. DLR LIF 중 하나의 “Lif Name” 으로 설정됩니다.
- ECMP 경로의 경우 [Destination], [GenMask] 및 [Interface]는 동일하지만 [Gateway]는 다른 둘 이상의 경로가 존재합니다. [Flags]에는 해당 경로의 ECMP 특성을 반영하기 위해 "E"가 포함됩니다.

DLR의 ARP 테이블

DLR을 전달하는 패킷에 대해 다음 홉의 IP 주소에 대한 ARP 요청을 확인할 수 있어야 합니다. 이러한 확인 프로세스의 결과는 개별 호스트의 DLR 인스턴스에 로컬로 저장됩니다.

컨트롤러는 이 프로세스에서 아무런 역할도 하지 않으며 결과 ARP 항목을 다른 호스트에 분산하는 데 사용되지 않습니다.

비활성 캐시 항목은 600초 동안 보존되었다가 제거됩니다. DLR ARP 확인 프로세스에 대한 자세한 내용은 [DLR ARP 확인 프로세스](#)를 참조하십시오.

- 1 NSX Manager 셸에서 `show cluster all`을 실행하여 클러스터 ID를 가져옵니다.
- 2 `show cluster cluster-id`를 실행하여 호스트 ID를 가져옵니다.
- 3 `show logical-router host hostID dlr all brief`를 실행하여 dlrID(Vdr 이름)를 가져옵니다.
- 4 `show logical-router host hostID dlr dlrID arp`를 실행하여 모든 인터페이스에 대한 상태 정보를 가져옵니다.

```
nsxmgr# show logical-router host hostID dlr dlrID arp
```

VDR default+edge-1:1460487509 ARP Information :

Legend: [S: Static], [V: Valid], [P: Proxy], [I: Interface]

Legend: [N: Nascent], [L: Local], [D: Deleted]

Network	Mac	Flags	Expiry	SrcPort	Interface	Refcnt
-----	----	-----	-----	-----	-----	-----
172.16.10.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000a	1
172.16.10.11	00:50:56:a6:7a:a2	VL	147	50331657	570d45550000000a	2
172.16.30.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000c	1
172.16.30.11	00:50:56:a6:ba:09	V	583	50331650	570d45550000000c	2
172.16.20.11	00:50:56:a6:84:52	VL	568	50331658	570d45550000000b	2
172.16.20.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000b	1
192.168.10.2	02:50:56:56:44:52	VI	permanent	0	570d455500000002	1
192.168.10.1	00:50:56:8e:ee:ce	V	147	50331650	570d455500000002	1

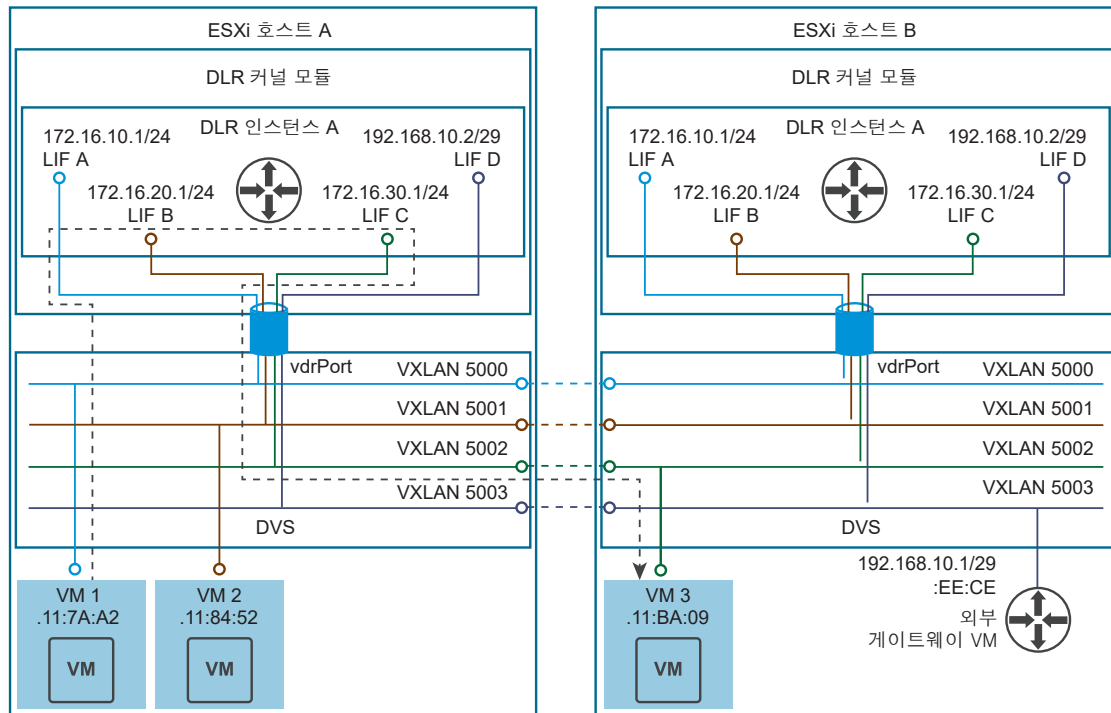
유의 사항:

- DLR의 자체 LIF에 대한 모든 ARP 항목(“I” 플래그)은 동일하며 [VXLAN 준비 점검](#)에 언급된 동일한 vMAC을 나타냅니다.
- “L” 플래그가 있는 ARP 항목은 CLI 명령이 실행된 호스트에서 실행되는 VM에 해당합니다.
- “SrcPort”는 ARP 항목이 시작된 dvPort ID를 나타냅니다. ARP 항목이 다른 호스트에서 시작된 경우 dvUplink의 dvPort ID가 표시됩니다. 이 dvPort ID는 [VXLAN 준비 점검](#)에 설명된 dvUplink dvPort ID와 상호 참조될 수 있습니다.
- “Nascent” 플래그는 일반적으로 확인되지 않습니다. DLR이 ARP 응답이 도착되기를 기다리는 동안 설정됩니다. 이 플래그가 설정된 모든 항목은 ARP 확인에 문제가 있음을 나타낼 수 있습니다.

시각적으로 나타낸 DLR 및 관련 호스트 구성 요소

다음 다이어그램은 2개의 호스트 즉 ESXi 호스트 A와 ESXi 호스트 B를 나타냅니다. 여기서는 예제 “DLR 인스턴스 A”가 구성되고 4개의 VXLAN LIF에 연결되어 있습니다.

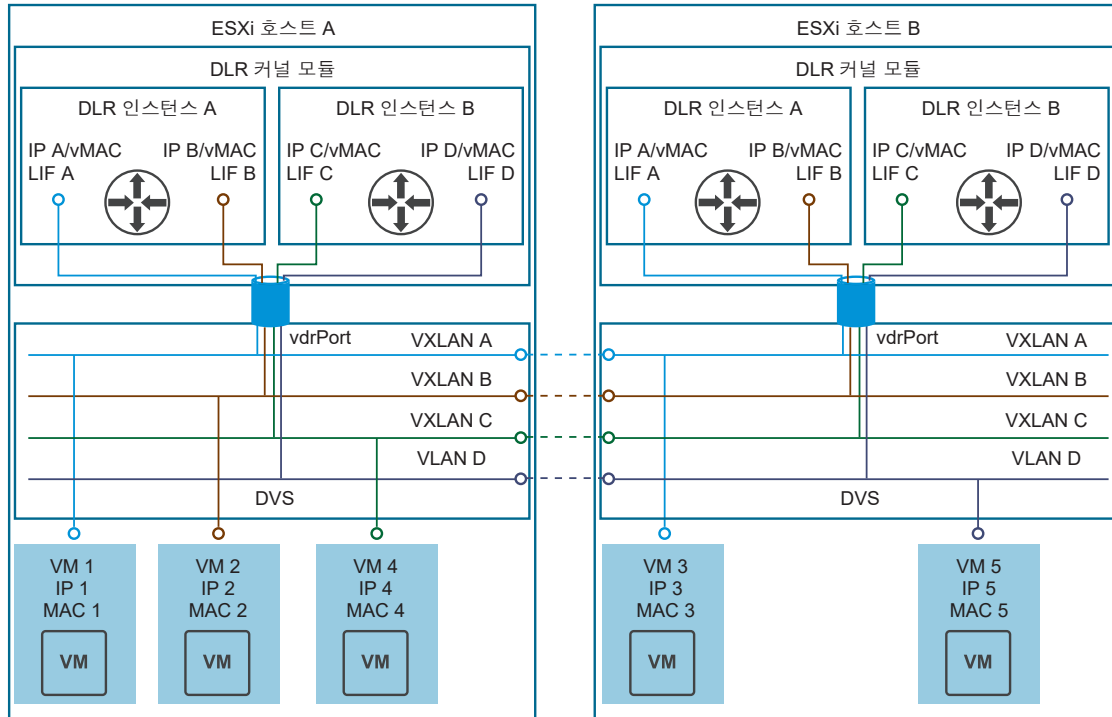
그림 3-8. 단일 DLR 인스턴스가 있는 2개의 호스트



- 각 호스트에는 “L2 스위치” (DVS)와 “트렁크” 인터페이스(vdrPort)를 통해 해당 “스위치”에 연결된 “스틱 위의 라우터” (DLR 커널 모듈)가 있습니다.
- 이 “트렁크”는 VLAN과 VXLAN을 둘 다 전송할 수 있지만 vdrPort를 탐색하는 패킷에 801.Q 또는 UDP/VXLAN 헤더가 없습니다. 대신 DVS는 내부 메타데이터 태그 지정 방법을 사용하여 해당 정보를 DLR 커널 모듈에 전달합니다.
- DVS는 Destination MAC = vMAC의 프레임을 만나면 DLR에 대한 것임을 알고 해당 프레임을 vdrPort로 전달합니다.
- 패킷이 vdrPort를 통해 DLR 커널 모듈에 도착하면 해당 메타데이터가 속하는 VXLAN VNI 또는 VLAN ID가 확인됩니다. 그런 후에 이 정보는 패킷이 속하는 DLR 인스턴스의 LIF를 확인하는 데 사용됩니다.
- 이 시스템의 단점은 둘 이상의 DLR 인스턴스가 지정된 VLAN 또는 VXLAN에 연결될 수 없다는 것입니다.

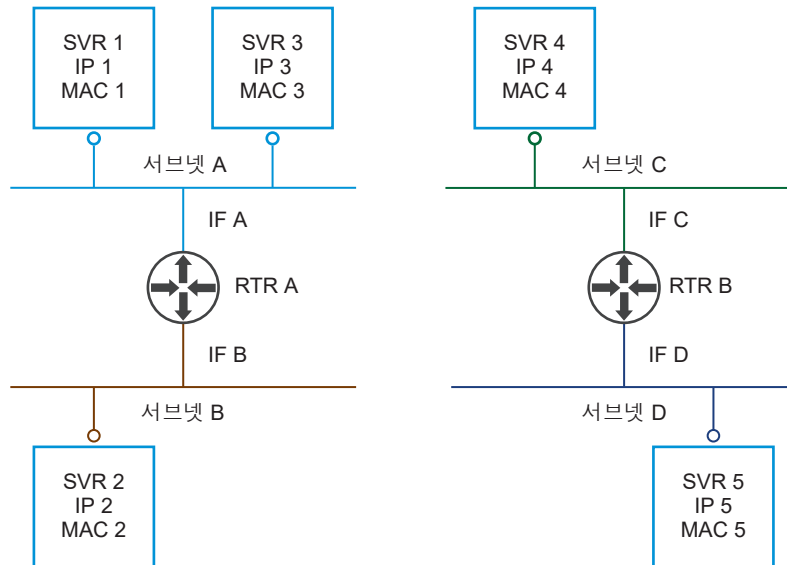
둘 이상의 DLR 인스턴스가 있으면 위 다이어그램은 다음과 같아집니다.

그림 3-9. 2개의 DLR 인스턴스가 있는 2개의 호스트



이것은 2개의 독립적인 라우팅 도메인이 서로 완전하게 분리되어 작동하고 IP 주소가 겹칠 수 있는 네트워크 토폴로지에 해당합니다.

그림 3-10. 2개의 호스트 및 2개의 DLR 인스턴스가 있는 네트워크 토폴로지



분산 라우팅 하위 시스템 아키텍처

ESXi 호스트의 DLR 인스턴스는 L3 라우팅을 수행하는 데 필요한 모든 정보에 액세스할 수 있어야 합니다.

- 네트워크가 직접 연결됨(인터페이스의 구성에서 학습)

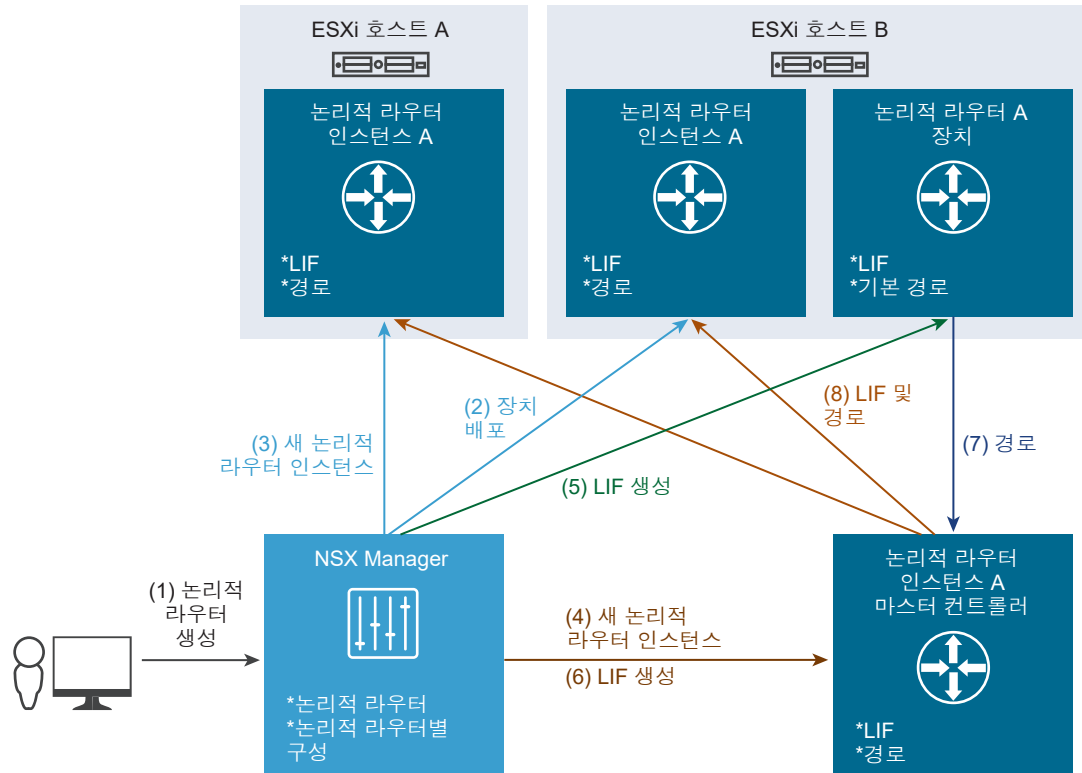
- 각 서브넷의 다음 홉(라우팅 테이블에서 조회)
- 다음 홉에 도달하기 위해 송신 프레임에 삽입할 MAC 주소(ARP 테이블)

이 정보는 여러 ESXi 호스트 간에 분산된 인스턴스로 전달됩니다.

DLR 생성 프로세스

다음 다이어그램은 NSX가 새 DLR을 생성하기 위해 진행하는 프로세스를 자세히 나타낸 그림입니다.

그림 3-11. DLR 생성 프로세스



UI 마법사가 “완료” 버튼으로 제출되거나 새 DLR 배포에 대한 API 호출이 수행되면 시스템은 다음 단계를 진행합니다.

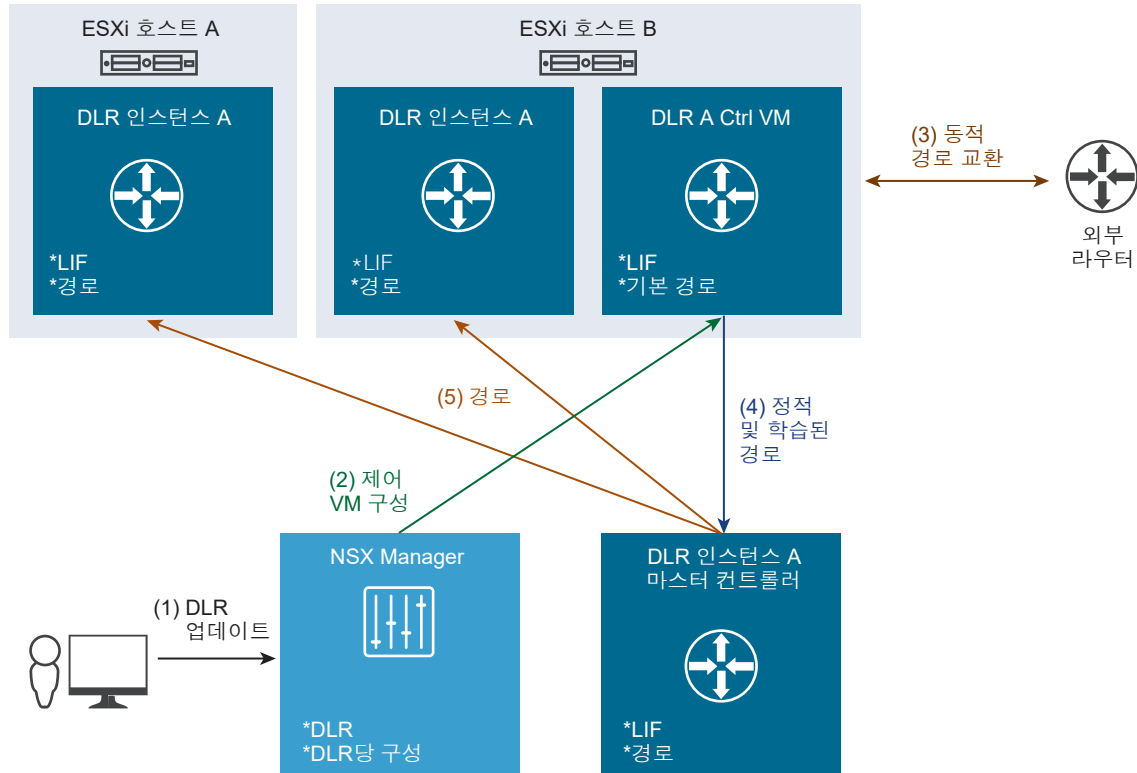
- 1 NSX Manager는 새 DLR을 배포하기 위한 API 호출을 수신합니다(직접 또는 UI 마법사에 의해 호출된 vSphere Web Client를 통해).
- 2 NSX Manager는 연결된 vCenter Server를 호출하여 DLR 제어 VM(또는 HA가 요청된 경우 한 쌍)을 배포합니다.
 - a DLR 제어 VM이 켜지고 NSX Manager에 다시 연결되어 구성을 수신할 준비가 완료됩니다.
 - b HA 쌍이 배포된 경우 NSX Manager는 HA 쌍을 다른 호스트에서 계속 실행하게 하는 반선호도 규칙을 구성합니다. 그러면 DRS는 이들을 분리하는 작업을 수행합니다.

- 3 NSX Manager는 호스트에서 DLR 인스턴스를 생성합니다.
 - a NSX Manager는 새 DLR에 연결될 논리적 스위치를 조회하여 논리적 스위치가 속할 전송 영역을 확인합니다.
 - b 그런 다음 이 전송 영역에 구성된 클러스터 목록을 조회한 후 이러한 클러스터의 각 호스트에 새 DLR을 생성합니다.
 - c 이때 호스트는 새 DLR ID만 알고 있으며 해당 정보(LIF 또는 경로)는 보유하고 있지 않습니다.
- 4 NSX Manager는 컨트롤러 클러스터에 새 DLR 인스턴스를 생성합니다.
 - a 컨트롤러 클러스터는 컨트롤러 노드 중 하나를 이 DLR 인스턴스의 마스터로 할당합니다.
- 5 NSX Manager는 LIF를 포함하는 구성을 DLR 제어 VM으로 전송합니다.
 - a ESXi 호스트(DLR 제어 VM이 실행되는 호스트 포함)는 컨트롤러 클러스터에서 조각화 정보를 수신하고, 새 DLR 인스턴스를 담당할 컨트롤러 노드를 결정하고, 해당 컨트롤러 노드에 연결합니다(기존 연결이 없는 경우).
- 6 DLR 제어 VM에서 LIF가 생성된 후에 NSX Manager는 컨트롤러 클러스터에서 새 DLR의 LIF를 생성합니다.
- 7 DLR 제어 VM은 새 DLR 인스턴스의 컨트롤러 노드에 연결한 후 해당 컨트롤러 노드에 경로를 전송합니다.
 - a 먼저 DLR은 라우팅 테이블을 전달 테이블로 변환합니다(LIF의 접두사로 확인).
 - b 그런 다음 DLR은 결과 테이블을 컨트롤러 노드로 전송합니다.
- 8 컨트롤러 노드는 5.a 단계에서 설정된 연결을 통해 새 DLR 인스턴스가 있는 다른 호스트로 LIF 및 경로를 푸시합니다.

DLR에 동적 라우팅 추가

DLR이 “직접” API 호출을 통해 생성되면(vSphere Web Client UI를 사용하는 경우와 다름) 동적 라우팅을 포함하는 완전한 구성을 제공할 수 있습니다(1).

그림 3-12. DLR의 동적 라우팅



- 1 NSX Manager는 기존 DLR의 구성을 변경(이 경우 동적 라우팅 추가)하기 위한 API 호출을 수신합니다.
- 2 NSX Manager는 DLR 제어 VM으로 새 구성을 보냅니다.
- 3 DLR 제어 VM은 구성을 적용하고, 라우팅 인접성을 설정하고, 라우팅 정보를 교환하는 등의 프로세스를 진행합니다.
- 4 라우팅 교환 후에 DLR 제어 VM은 전달 테이블을 계산한 후 DLR의 마스터 컨트롤러 노드로 전송합니다.
- 5 DLR의 마스터 컨트롤러 노드는 업데이트된 경로를 DLR 인스턴스가 있는 ESXi 호스트로 분산합니다.

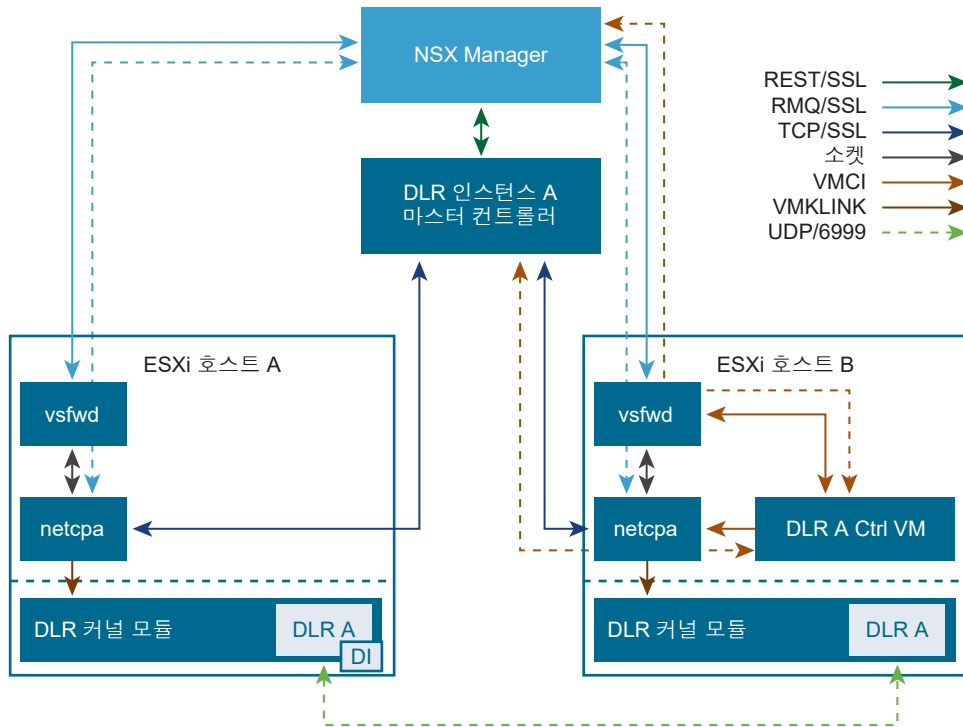
DLR 제어 VM이 실행되는 ESXi 호스트의 DLR 인스턴스는 LIF를 수신하고, DLR 제어 VM 또는 NSX Manager로부터 직접 라우팅되지 않고 DLR의 마스터 컨트롤러 노드로부터만 라우팅됩니다.

DLR 제어부 및 관리부 구성 요소 및 통신

이 섹션에서는 DLR 제어부 및 관리부의 구성 요소에 대해 간단히 설명합니다.

그림에서는 구성 요소와 해당 구성 요소 간의 통신 채널을 보여줍니다.

그림 3-13. DLR 제어부 및 관리부 구성 요소



■ NSX Manager:

- 컨트롤러 클러스터와 직접 통신이 설정되어 있습니다.
- NSX용으로 준비된 각 호스트에서 실행되는 메시지 버스 클라이언트(**vsfwd**) 프로세스와의 직접 영구 연결이 설정되어 있습니다.
- 각 DLR 인스턴스에 대해 하나의 컨트롤러 노드(사용 가능한 3개 중 하나)가 마스터로 선택됩니다.
 - 마스터 기능은 원래 컨트롤러 노드에 장애가 발생할 경우 다른 컨트롤러 노드로 이동될 수 있습니다.
- 각 ESXi 호스트에서 2개의 UWA(User World Agents), 즉 메시지 버스 클라이언트(**vsfwd**)와 제어부 에이전트(**netcpa**)를 실행합니다.
 - **netcpa**가 작동하려면 **NSX Manager**의 정보가 필요합니다(예: 컨트롤러를 찾는 위치, 컨트롤러 인증 방법). 이 정보는 **vsfwd**에서 제공하는 메시지 버스 연결을 통해 액세스할 수 있습니다.
 - 또한 **netcpa**는 DLR 커널 모듈과 통신하여 컨트롤러에서 받은 관련 정보로 프로그래밍합니다.
- 각 DLR 인스턴스에 대해 ESXi 호스트 중 하나에서 실행되는 DLR 제어 VM이 있습니다. DLR 제어 VM에는 다음과 같은 2개의 통신 채널이 있습니다.
 - **vsfwd**를 통한 VMCi 채널과 **NSX Manager** 연결은 제어 VM을 구성하는 데 사용됩니다.
 - **netcpa**를 통한 VMCi 채널과 DLR 마스터 컨트롤러 간 연결은 DLR의 라우팅 테이블을 컨트롤러로 전송하는 데 사용됩니다.

- DLR에 VLAN LIF가 있는 경우 포함되는 ESXi 호스트 중 하나가 컨트롤러에 의해 DI(지정된 인스턴스)로 지명됩니다. 다른 ESXi 호스트의 DLR 커널 모듈은 DI가 연결된 VLAN에 대해 프록시 ARP 쿼리를 수행하도록 요청합니다.

NSX 라우팅 하위 시스템 구성 요소

NSX 라우팅 하위 시스템은 여러 구성 요소에 의해 사용되도록 설정됩니다.

- NSX Manager
- 컨트롤러 클러스터
- ESXi 호스트 모듈(커널 및 UWA)
- DLR 제어 VM
- ESG

NSX Manager

NSX Manager는 NSX 라우팅과 관련해서 다음 기능을 제공합니다.

- 중앙 집중 관리부로 작동하여 모든 NSX 관리 작업을 위한 통합 API 액세스 지점을 제공합니다.
- 호스트에 분산 라우팅 커널 모듈 및 User World Agent를 설치하여 NSX 작동 준비를 진행합니다.
- DLR 및 DLR LIF를 생성/소멸시킵니다.
- vCenter를 통해 DLR 제어 VM 및 ESG를 배포/삭제합니다.
- REST API를 통해 컨트롤러 클러스터를 구성하고 메시지 버스를 통해 호스트를 구성합니다.
 - 호스트 제어부 에이전트에 컨트롤러의 IP 주소를 제공합니다.
 - 인증서를 생성한 후 호스트 및 컨트롤러에 배포하여 제어부 통신의 보안을 유지합니다.
- 메시지 버스를 통해 ESG 및 DLR 제어 VM을 구성합니다.
 - ESG를 준비되지 않은 호스트에 배포할 수 있습니다. 이 경우 VIX가 메시지 버스 대신 사용됩니다.

컨트롤러 클러스터

NSX 분산 라우팅에는 확장 및 가용성을 위해 클러스터링된 컨트롤러가 필요합니다. 이러한 컨트롤러는 다음 기능을 제공합니다.

- VXLAN 및 분산 라우팅 제어부를 지원합니다.
- 통계 및 런타임 상태에 대한 CLI 인터페이스를 제공합니다.
- 각 DLR 인스턴스에 대한 마스터 컨트롤러 노드를 선택합니다.
 - 마스터 노드는 DLR 제어 VM에서 라우팅 정보를 수신한 후 호스트에 배포합니다.
 - 호스트에 LIF 테이블을 전송합니다.
 - DLR 제어 VM이 위치하는 호스트를 추적합니다.

- VLAN LIF에 대해 지정된 인스턴스를 선택하고 이 정보를 호스트에 전달합니다. 제어부 KeepAlive를 통해 DI 호스트를 모니터링합니다(시간 초과는 30초, 감지 시간은 20~40초일 수 있음). 그리고 선택한 DI 호스트가 사라질 경우 호스트에 업데이트 내용을 전송합니다.

ESXi 호스트 모듈

NSX 라우팅은 2개의 UWA(User World Agent)와 라우팅 커널 모듈을 직접 활용하고 VXLAN 커널 모듈을 통해 VXLAN에 연결합니다.

다음은 이러한 각 구성 요소가 수행하는 작업에 대한 요약입니다.

- 제어부 에이전트(**netcpa**)는 제어부 프로토콜을 사용하여 컨트롤러와 통신하는 TCP(SSL) 클라이언트입니다. 여러 컨트롤러에 연결될 수 있습니다. **netcpa**는 메시지 버스 클라이언트(**vsfwd**)와 통신하여 NSX Manager에서 제어부 관련 정보를 검색합니다.
- **netcpa** 패키징 및 배포:
 - 에이전트는 VXLAN VIB(vSphere 설치 번들)에 패키징됩니다.
 - 호스트 준비 동안 EAM(ESX Agency Manager)을 통해 NSX Manager에 의해 설치됩니다.
 - ESXi **netcpa**에 대한 서비스 데몬으로 실행됩니다.
 - 시작 스크립트 `/etc/init.d/netcpad`를 통해 시작/중지/쿼리될 수 있습니다.
 - 개별 호스트 또는 전체 클러스터의 [네트워킹 및 보안 UI 설치] -> [호스트 준비] -> [설치 상태]를 통해 원격으로 다시 시작할 수 있습니다.
- DLR 커널 모듈(**vdrb**)은 L3 전달을 사용하기 위해 DVS와 통합됩니다.
 - **netcpa**에 의해 구성됩니다.
 - VXLAN VIB 배포의 일부로 설치됩니다.
 - VLAN 및 VXLAN을 둘 다 지원하는 “vdrPort”라는 특수 트렁크를 통해 DVS에 연결됩니다.
 - DLR 인스턴스에 대한 정보를 인스턴스별로 포함합니다.
 - LIF 및 경로 테이블
 - host-local ARP 캐시
- 메시지 버스 클라이언트(**vsfwd**)는 **netcpa**, ESG 및 DLR 제어 VM에서 NSX Manager와 통신하는 데 사용됩니다.
 - **vsfwd**는 vCenter가 `vpax/hosd`를 통해 설정한 `/UserVars/RmqIpAddress`에서 NSX Manager의 IP 주소를 가져오고 다른 `/UserVars/Rmq*` 변수에 저장된 호스트별 자격 증명을 사용하여 메시지 버스 서버에 로그인합니다.
- ESXi 호스트에서 실행되는 **netcpa**는 **vsfwd**를 활용하여 다음을 수행합니다.
 - NSX Manager에서 호스트의 제어부 SSL 개인 키 및 인증서를 가져옵니다. 이러한 항목은 `/etc/vmware/ssl/rui-for-netcpa`에 저장됩니다.*

- NSX Manager에서 컨트롤러의 IP 주소 및 SSL 지문을 가져옵니다. 이러한 항목은 `/etc/vmware/netcpa/config-by-vsm.xml`에 저장됩니다.
- NSX Manager의 지침에 따라 해당 호스트에서 DLR 인스턴스를 만들고 삭제합니다.
- 패키징 및 배포
 - netcpa와 같이 VXLAN VIB의 일부입니다.
 - ESXi vsfwd에 대한 서비스 데몬으로 실행됩니다.
 - 시작 스크립트 `/etc/init.d/vShield-Stateful-Firewall`을 통해 시작/중지/쿼리될 수 있습니다.
- ESG 및 DLR 제어 VM은 vsfwd에 대한 VMCI 채널을 사용하여 NSX Manager에서 구성을 수신합니다.

DLR 제어 VM 및 ESG

- DLR 제어 VM은 DLR 인스턴스에 대한 “경로 프로세서”입니다.
 - 각 DLR LIF에 대한 “위치 지정자” 또는 “실제 vNIC” 인터페이스와 IP 구성을 포함합니다.
 - 사용 가능한 두 동적 라우팅 프로토콜(BGP 또는 OSPF) 중 하나를 실행하거나 정적 경로를 사용할 수 있습니다.
 - OSPF 또는 BGP를 실행하기 위해 하나 이상의 "업링크" LIF가 필요합니다.
 - 직접 연결된(LIF) 서브넷, 정적 및 동적 경로에서 전달 테이블을 계산한 후 netcpa에 대한 VMCI 링크를 통해 DLR 인스턴스의 마스터 컨트롤러로 보냅니다.
 - 활성/대기 VM 쌍 구성에서 HA를 지원합니다.
- ESG는 VM의 자체 포함 라우터입니다.
 - NSX DLR 라우팅 하위 시스템에서 완전히 독립됩니다(NSX 제어부 통합 없음).
 - 일반적으로 하나 이상의 DLR에 대한 업스트림 게이트웨이로 사용됩니다.
 - 동시에 실행되는 둘 이상의 동적 라우팅 프로토콜을 지원합니다.

NSX 라우팅 제어부 CLI

호스트 구성 요소 외에 NSX 라우팅은 DLR 제어부의 정보 출처이며 검사를 위한 자체 CLI가 있는 컨트롤러 클러스터 및 DLR 제어 VM의 서비스를 사용합니다.

DLR 인스턴스 마스터 컨트롤러

각 DLR 인스턴스는 컨트롤러 노드 중 하나에서 제공됩니다. 다음 CLI 명령을 사용하여 이 컨트롤러 노드가 마스터로 작용하는 DLR 인스턴스에 대해 제공하는 정보를 볼 수 있습니다.

```
nsx-controller # show control-cluster logical-routers instance 1460487509
LR-Id      LR-Name      Hosts[]      Edge-Connection Service-Controller
1460487509 default+edge-1 192.168.210.57 192.168.110.201
           192.168.210.51
           192.168.210.52
```

```

192.168.210.56
192.168.110.51
192.168.110.52

nsx-controller # show control-cluster logical-routers interface-summary 1460487509
Interface                               Type  Id      IP[]
570d4555000000002                      vxlan 5003    192.168.10.2/29
570d455500000000b                      vxlan 5001    172.16.20.1/24
570d455500000000c                      vxlan 5002    172.16.30.1/24
570d455500000000a                      vxlan 5000    172.16.10.1/24

nsx-controller # show control-cluster logical-routers routes 1460487509
LR-Id      Destination      Next-Hop
1460487509 0.0.0.0/0        192.168.10.1

```

- “show control-cluster logical-routers” 명령의 “instance” 하위 명령은 이 DLR 인스턴스에 대해 이 컨트롤러에 연결된 호스트 목록을 표시합니다. 올바르게 작동하는 환경에서 이 목록에는 DLR이 존재하는 모든 클러스터의 모든 호스트가 포함됩니다.
- “interface-summary” 를 실행하면 컨트롤러가 NSX Manager에서 확인한 LIF가 표시됩니다. 이 정보는 호스트로 전송됩니다.
- “routes” 를 실행하면 이 DLR 제어 VM에서 이 컨트롤러로 보낸 라우팅 테이블이 표시됩니다. ESXi 호스트에서와 달리 이 테이블에는 직접 연결된 서브넷은 포함되지 않습니다. 이 정보는 LIF 구성에서 제공하기 때문입니다.

DLR 제어 VM

DLR 제어 VM에는 LIF 및 라우팅/전달 테이블이 있습니다. DLR 제어 VM 수명 주기의 주요 출력은 인터페이스 및 경로로 이루어진 DLR 라우팅 테이블입니다.

```

edge-1-0> show ip route

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

Total number of routes: 5

S      0.0.0.0/0          [1/1]          via 192.168.10.1
C      172.16.10.0/24   [0/0]          via 172.16.10.1
C      172.16.20.0/24   [0/0]          via 172.16.20.1
C      172.16.30.0/24   [0/0]          via 172.16.30.1
C      192.168.10.0/29   [0/0]          via 192.168.10.2

edge-1-0> show ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route
R>* 0.0.0.0/0 via 192.168.10.1, vNic_2

```

```
C>* 172.16.10.0/24 is directly connected, VDR
C>* 172.16.20.0/24 is directly connected, VDR
C>* 172.16.30.0/24 is directly connected, VDR
C>* 192.168.10.0/29 is directly connected, vNic_2
```

- 전달 테이블은 지정된 대상 서브넷에 대한 송신으로 선택된 DLR 인터페이스를 표시하는 데 사용됩니다.
 - “VDR” 인터페이스는 “내부” 유형의 모든 LIF에 대해 표시됩니다. “VDR” 인터페이스는 vNIC에 해당되지 않는 유사 인터페이스입니다.

DLR 제어 VM의 인터페이스는 다음과 같이 표시될 수 있습니다.

```
edge-1-0> show interface
Interface VDR is up, line protocol is up
  index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,NOARP>
  HWaddr: be:3d:a1:52:90:f4
  inet6 fe80::bc3d:a1ff:fe52:90f4/64
  inet 172.16.10.1/24
  inet 172.16.20.1/24
  inet 172.16.30.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

Interface vNic_0 is up, line protocol is up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:1c:fb
  inet6 fe80::250:56ff:fe8e:1cfb/64
  inet 169.254.1.1/30
  inet 10.10.10.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 582249, bytes 37339072, dropped 49, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 4726382, bytes 461202852, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

Interface vNic_2 is up, line protocol is up
  index 9 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:ae:08
  inet 192.168.10.2/29
  inet6 fe80::250:56ff:fe8e:ae08/64
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 361446, bytes 30167226, dropped 0, multicast packets 361168
```

```
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 361413, bytes 30287912, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

주요 참고:

- 인터페이스 “VDR”에는 연결된 vNIC(VM NIC)가 없습니다. 모든 DLR의 “내부” LIF에 대한 모든 IP 주소로 구성된 단일 “유사 인터페이스”입니다.
- 이 예에서 인터페이스 vNic_0은 HA 인터페이스입니다.
 - 위 출력은 HA가 설정된 상태로 배포된 DLR에서 가져온 것이며 HA 인터페이스에는 IP 주소가 할당되어 있습니다. 이것은 2개의 IP 주소, 즉 169.254.1.1/30(HA에 대해 자동으로 할당됨) 및 10.10.10.1/24(HA 인터페이스에 수동으로 할당됨)로 나타납니다.
 - ESG에서 작업자는 수동으로 해당 vNIC 중 하나를 HA로 할당하거나, 시스템이 사용 가능한 “내부” 인터페이스 중에서 자동으로 선택할 수 있게 기본값 상태로 둘 수 있습니다. “내부” 유형을 반드시 지정해야 합니다. 그렇지 않으면 HA가 실패합니다.
- 인터페이스 vNic_2는 업링크 유형이므로 “실제” vNIC로 표시됩니다.
 - 이 인터페이스에 표시된 IP 주소는 DLR의 LIF와 같지만 DLR 제어 VM은 LIF IP 주소에 대한 ARP 쿼리에 답변하지 않습니다(이 경우 192.168.10.2/29). 이를 가능하게 하는 이 vNIC의 MAC 주소에 적용된 ARP 필터가 있습니다.
 - 동적 라우팅 프로토콜이 DLR에 대해 구성되고, IP 주소가 ARP 필터에 따라 제거된 후, 동적 라우팅 프로토콜 구성 동안 지정된 “프로토콜 IP” 주소로 대체될 때까지 위의 사항이 적용됩니다.
 - 이 vNIC는 DLR 제어 VM에서 실행되는 동적 라우팅 프로토콜이 경로를 알리고 확인하기 위해 다른 라우터와 통신하는 데 사용됩니다.
- Edge의 연결이 끊기고 HA 페일오버가 수행된 후, 연결이 끊긴 Edge 인터페이스 IP 주소가 활성 Edge RIB(라우팅 정보 기반)/FIB(전달 정보 기반)에서 제거됩니다. 하지만 대기 Edge FIB 테이블 또는 show ip forwarding 명령은 해당 IP를 계속 표시하며 IP는 FIB 테이블에서 제거되지 않습니다. 이는 예상된 동작입니다.

NSX 라우팅 하위 시스템 실패 모드 및 결과

이 장에서는 NSX 라우팅 하위 시스템의 구성 요소에 영향을 미칠 수 있는 일반적인 실패 시나리오를 검토하고 이러한 실패의 결과를 대략적으로 설명합니다.

NSX Manager

표 3-2. NSX Manager 실패 모드 및 결과

실패 모드	실패 결과
NSX Manager VM에 대한 네트워크 연결 해제	<ul style="list-style-type: none"> ■ 모든 NSX Manager 기능(NSX 라우팅/브리징의 CRUD 포함) 완전 중단 ■ 구성 데이터 손실 없음 ■ 데이터 또는 제어부 중단 없음
NSX Manager와 ESXi 호스트 간 네트워크 연결 해제 또는 RabbitMQ 서버가 실패합니다.	<ul style="list-style-type: none"> ■ 영향 받는 호스트에서 DLR 제어 VM 또는 ESG가 실행되고 있는 경우 해당 CRUD 작업이 실패합니다. ■ 영향 받는 호스트의 DLR 인스턴스 생성 및 삭제가 실패합니다. ■ 구성 데이터 손실 없음 ■ 데이터 또는 제어부 중단 없음 ■ 동적 라우팅 업데이트는 계속 작동합니다.
NSX Manager 및 컨트롤러 간 네트워크 연결 해제	<ul style="list-style-type: none"> ■ NSX 분산 라우팅 및 브리징에 대한 생성, 업데이트 및 삭제 작업이 실패합니다. ■ 구성 데이터 손실 없음 ■ 데이터 또는 제어부 중단 없음
NSX Manager VM이 소멸됩니다(데이터스토어 실패).	<ul style="list-style-type: none"> ■ 모든 NSX Manager 기능(NSX 라우팅/브리징의 CRUD 포함) 완전 중단 ■ NSX Manager가 이전 구성으로 복원되는 경우 라우팅/브리징 인스턴스의 일부가 분리될 수 있으며 수동 정리 및 조정이 필요합니다. ■ 조정이 필요하지 않는 한 데이터 또는 제어부는 중단되지 않습니다.

컨트롤러 클러스터

표 3-3. NSX Controller 실패 모드 및 결과

실패 모드	실패 결과
컨트롤러 클러스터와 ESXi 호스트 간 네트워크 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ DLR 제어부 기능(동적인 경우를 포함하여 경로 생성, 업데이트 및 삭제) 완전 중단 ■ DLR 관리부 기능(호스트의 LIF 생성, 업데이트 및 삭제) 중단 ■ VXLAN 전달에 영향을 미쳐 종단 간(L2+L3) 전달 프로세스도 실패할 수 있습니다. ■ 데이터부는 마지막으로 알려진 상태를 기준으로 계속 작동합니다.
하나 이상의 컨트롤러와 ESXi 호스트 간 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ 영향 받은 컨트롤러가 클러스터의 다른 컨트롤러에 여전히 연결할 수 있으면 이 컨트롤러가 통제하는 모든 DLR 인스턴스에는 위에 설명된 것과 동일한 결과가 나타납니다. 다른 컨트롤러가 자동으로 인계 받지 않습니다.

표 3-3. NSX Controller 실패 모드 및 결과 (계속)

실패 모드	실패 결과
한 컨트롤러와 다른 컨트롤러 간의 네트워크 연결이 끊어집니다 (또는 완전히).	<ul style="list-style-type: none"> ■ 나머지 두 컨트롤러가 격리된 컨트롤러에서 처리하던 VXLAN 및 DLR을 인계 받습니다. ■ 영향 받는 컨트롤러는 읽기 전용 모드로 전환되고, 호스트와의 세션을 삭제하고, 새 세션을 거부합니다.
컨트롤러 간 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ 모든 컨트롤러가 읽기 전용 모드로 전환되고, 호스트와의 연결이 끊어지고, 새 연결을 거부합니다. ■ 모든 DLR LIF 및 경로(동적 포함)에 대한 생성, 업데이트 및 삭제 작업이 실패합니다. ■ NSX Manager와 컨트롤러 클러스터 간에 동기화되지 않아 NSX 라우팅 구성(LIF)을 수동으로 다시 동기화해야 할 수 있습니다. ■ 호스트는 마지막에 알려진 제어부 상태에서 계속 작동합니다.
하나의 컨트롤러 VM이 유실됩니다.	<ul style="list-style-type: none"> ■ 컨트롤러 클러스터가 중복성을 유실합니다. ■ 관리/제어부는 평소처럼 계속 작동합니다.
두 컨트롤러 VM이 유실됩니다.	<ul style="list-style-type: none"> ■ 나머지 컨트롤러는 읽기 전용 모드로 전환되고, 컨트롤러 간 연결이 끊어진 경우(위 참조)와 동일한 영향을 미칩니다. 수동 클러스터 복구가 필요할 수 있습니다.

호스트 모듈

netcpa는 컨트롤러와의 보안 통신을 설정하기 위해 호스트 SSL 키 및 인증서와 SSL 지문을 사용합니다. 이러한 항목은 메시지 버스를 통해 NSX Manager에서 가져옵니다(vsfwd에 의해 제공됨).

인증서 교환 프로세스가 실패하면 netcpa는 컨트롤러에 제대로 연결하지 못할 수 있습니다.

참고: 이 섹션에서는 커널 모듈이 실패하는 경우에 대해서는 다루지 않습니다. 그 결과가 심각하고(PSOD) 드물게 발생하기 때문입니다.

표 3-4. 호스트 모듈 실패 모드 및 결과

실패 모드	실패 결과
vsfwd는 사용자 이름/암호 인증을 사용하여 메시지 버스 서버에 액세스하며, 이러한 인증은 만료될 수 있습니다.	<ul style="list-style-type: none"> ■ 새로 준비한 ESXi 호스트의 vsfwd가 2시간 이내에 NSX Manager에 연결할 수 없으면 설치 중에 제공된 임시 로그인/암호가 만료되고 이 호스트의 메시지 버스가 작동되지 않게 됩니다.
메시지 버스 클라이언트(vsfwd)의 실패 결과는 타이밍에 따라 다릅니다.	

표 3-4. 호스트 모듈 실패 모드 및 결과 (계속)

실패 모드	실패 결과
NSX 제어부의 다른 부분이 안정적인 실행 상태에 도달할 수 있게 되기 전에 실패하는 경우	<ul style="list-style-type: none"> ■ 호스트가 컨트롤러와 통신할 수 없기 때문에 호스트의 분산 라우팅이 작동을 중지합니다. ■ 호스트가 NSX Manager에서 DLR 인스턴스를 확인하지 않습니다.
호스트가 안정적인 상태에 도달한 후에 실패하는 경우	<ul style="list-style-type: none"> ■ 호스트에서 실행되는 ESG 및 DLR 제어 VM이 구성 업데이트를 수신할 수 없게 됩니다. ■ 호스트가 새 DLR을 확인하지 않아 기존 DLR을 삭제할 수 없습니다. ■ 호스트 데이터 경로는 실패 시에 호스트에 지정되었던 구성을 기준으로 계속 작동합니다.

표 3-5. netcpa 실패 모드 및 결과

실패 모드	실패 결과
제어부 에이전트(netcpa)의 실패 결과는 타이밍에 따라 다릅니다.	
NSX 데이터 경로 커널 모듈이 안정적인 실행 상태에 도달할 수 있게 되기 전에 실패하는 경우	<ul style="list-style-type: none"> ■ 호스트의 분산 라우팅이 작동을 중지합니다.
호스트가 안정적인 상태에 도달한 후에 실패하는 경우	<ul style="list-style-type: none"> ■ 호스트에서 실행되는 DLR 제어 VM이 전달 테이블 업데이트를 컨트롤러에 전송할 수 없게 됩니다. ■ 분산 라우팅 데이터 경로는 컨트롤러에서 LIF 또는 경로 업데이트를 수신하지 않지만 실패 이전 상태를 기준으로 계속 작동합니다.

DLR 제어 VM

표 3-6. DLR 제어 VM 실패 모드 및 결과

실패 모드	실패 결과
DLR 제어 VM이 유실되거나 전원이 꺼졌습니다.	<ul style="list-style-type: none"> ■ 이 DLR LIF 및 경로에 대한 생성, 업데이트 및 삭제 작업이 실패합니다. ■ 동적 경로 업데이트가 호스트로 전송되지 않습니다(현재 끊어진 인접성을 통해 수신된 접두사의 철회 포함).
DLR 제어 VM과 NSX Manager 및 컨트롤러와의 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ DLR 제어 VM 및 해당 라우팅 인접성이 여전히 작동되는 경우를 제외하고 이전에 확인된 접두사와의 트래픽은 영향을 받지 않으며 동일한 결과가 나타납니다.
DLR 제어 VM과 NSX Manager과의 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ 이 DLR의 LIF 및 경로에 대한 NSX Manager의 생성, 업데이트 및 삭제 작업이 실패하고 다시 시도되지 않습니다. ■ 동적 라우팅 업데이트가 계속 전파됩니다.
DLR 제어 VM과 컨트롤러와의 연결이 끊어집니다.	<ul style="list-style-type: none"> ■ 이 DLR에 대한 라우팅 변경 내용(정적 또는 동적)이 호스트로 전파되지 않습니다.

라우팅 관련 NSX 로그

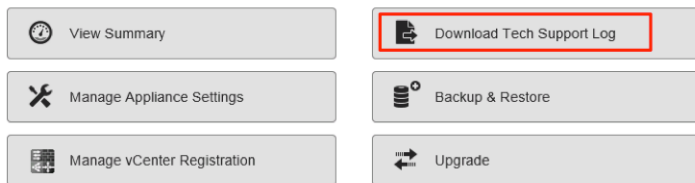
모범 사례는 로그를 중앙 수집기로 보내도록 NSX의 모든 구성 요소를 구성하는 것입니다. 그러면 중앙 수집기에서 이러한 구성 요소가 검사될 수 있습니다.

필요한 경우 NSX 구성 요소의 로그 수준을 변경할 수 있습니다. 자세한 내용은 "NSX 로깅 및 시스템 이벤트"에서 "NSX 구성 요소의 로깅 수준 설정" 항목을 참조하십시오.

NSX Manager 로그

- NSX Manager CLI에서 `show log`
- NSX Manager UI를 통해 수집된 기술 지원 로그 번들

NSX Manager Virtual Appliance Management



NSX Manager 로그에는 CRUD(생성, 읽기, 업데이트 및 삭제) 작업을 포함하는 관리부 관련 정보가 포함됩니다.

컨트롤러 로그

컨트롤러에는 여러 모듈이 포함되어 있으며 많은 경우에 자체 로그 파일이 있습니다. 컨트롤러 로그는 `show log <log file> [filtered-by <string>]` 명령을 사용하여 액세스할 수 있습니다. 라우팅과 관련된 로그 파일은 다음과 같습니다.

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: 이 로그는 구성 및 내부 API 서버를 관리합니다.
- `cloudnet/cloudnet.nsx-controller.log`: 컨트롤러 주 프로세스 로그입니다.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: 이 로그는 클러스터링 및 부트스트랩을 관리합니다.
- `cloudnet/cloudnet_cpp.log.ERROR`: 이 파일은 오류가 발생하는 경우에 생깁니다.

컨트롤러 로그는 상세 로그로 대부분의 경우 까다로운 문제 상황에서 문제 해결을 지원하기 위해 VMware 엔지니어링 팀이 수집될 때만 필요합니다.

`show log` CLI 외에 `watch log <logfile> [filtered-by <string>]` 명령을 사용하여 개별 로그 파일이 업데이트될 때 실시간으로 로그 파일을 확인할 수 있습니다.

로그는 NSX UI에서 컨트롤러 노드를 선택하고 **기술 지원 로그 다운로드(Download tech support logs)** 아이콘을 클릭하여 생성 및 다운로드할 수 있는 컨트롤러 지원 번들에 포함되어 있습니다.

ESXi 호스트 로그

ESXi 호스트에서 실행되는 NSX 구성 요소는 다음과 같은 몇 가지 로그 파일을 작성합니다.

- VMkernel 로그: `/var/log/vmkernel.log`
- 제어부 에이전트 로그: `/var/log/netcpa.log`
- 메시지 버스 클라이언트 로그: `/var/log/vsfwd.log`

또한 vCenter Server에서 생성된 VM 지원 번들의 일부로 로그를 수집할 수도 있습니다. 로그 파일은 루트 권한이 있는 사용자 또는 사용자 그룹에서만 액세스할 수 있습니다.

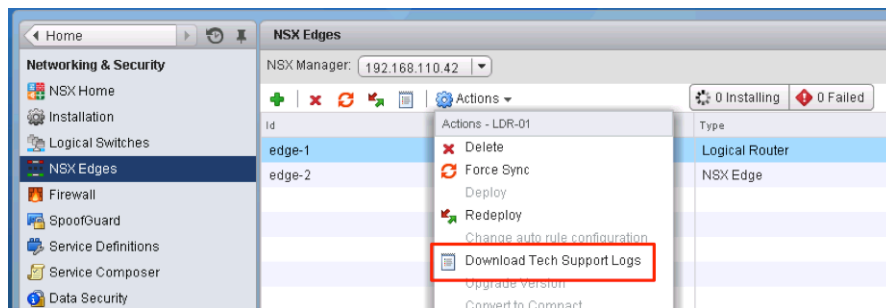
ESG/DLR 제어 VM 로그

ESG 및 DLR 제어 VM의 로그 파일에 액세스하는 방법에는 두 가지가 있습니다. 하나는 CLI를 사용하여 표시하는 것이고 다른 하나는 CLI 또는 UI를 사용하여 기술 지원 번들을 다운로드하는 것입니다.

로그를 표시하기 위한 CLI 명령은 `show log [follow | reverse]`입니다.

기술 지원 번들을 다운로드하려면:

- CLI에서 `enable` 모드를 입력하고 `export tech-support <[scp | ftp]> <URI>` 명령을 실행합니다.
- vSphere Web Client의 **작업(Actions)** 메뉴에서 **기술 지원 로그 다운로드(Download Tech Support Logs)** 옵션을 선택합니다.



기타 유용한 파일 및 해당 위치

엄격히 말해서 로그는 아니지만 NSX 라우팅을 이해하고 관련 문제를 해결하는 데 도움이 될 수 있는 많은 파일이 있습니다.

- 제어부 에이전트 구성(`/etc/vmware/netcpa/config-by-vsm.xml`)에는 다음 구성 요소에 대한 정보가 포함되어 있습니다.
 - 컨트롤러 IP 주소, TCP 포트, 인증서 지문, SSL 사용/사용 안 함
 - VXLAN을 사용하여 DVS가 사용되도록 설정된 dvUplink(팀 구성 정책, 이름, UUID)
 - 호스트가 알고 있는 DLR 인스턴스(DLR ID, 이름)
- 제어부 에이전트 구성(`/etc/vmware/netcpa/netcpa.xml`)에는 로깅 수준(기본적으로 **정보(info)**)을 비롯하여 netcpa에 대한 다양한 구성 옵션이 포함되어 있습니다.

■ 제어부 인증서 파일: /etc/vmware/ssl/rui-for-netcpa.*

- 2개의 파일: 호스트 인증서 및 호스트 개인 키
- 컨트롤러에 대한 호스트 연결을 인증하는 데 사용

이러한 모든 파일은 vsfwd에서 제공하는 메시지 버스 연결을 통해 NSX Manager에서 수신된 정보를 사용하여 제어부 에이전트에서 만듭니다.

일반 실패 시나리오 및 수정 사항

가장 일반적인 실패 시나리오는 두 범주로 나뉩니다.

즉 구성 및 제어부 문제입니다. 관리부 문제도 발생하기는 하지만 일반적이지 않습니다.

구성 문제 및 수정 사항

일반 구성 문제 및 해당 결과는 표 3-7. 일반 구성 문제 및 결과에 설명되어 있습니다.

표 3-7. 일반 구성 문제 및 결과

문제	결과
프로토콜 및 전달 IP 주소가 동적 라우팅에 대해 뒤바뀜	동적 프로토콜 인접성이 발생하지 않음
전송 영역이 DVS 경계에 맞춰 조정되지 않음	분산 라우팅이 ESXi 호스트 일부에서 작동하지 않음(전송 영역에서 누락된 호스트)
동적 라우팅 프로토콜 구성 불일치(타이머, MTU, BGP ASN, 암호, 인터페이스-OSPF 영역 매핑)	동적 프로토콜 인접성이 발생하지 않음
DLR HA 인터페이스에 IP 주소가 할당되고 연결된 경로의 재분산이 사용되도록 설정됨	DLR 제어 VM이 HA 인터페이스 서브넷의 트래픽을 끌어들인 후 해당 트래픽을 흡수함

이러한 문제를 해결하려면 구성을 검토하고 필요한 경우 수정하십시오.

필요한 경우 `debug ip ospf` 또는 `debug ip bgp` CLI 명령을 사용하고 DLR 제어 VM 또는 ESG 콘솔(SSH 세션 아님)의 로그를 확인하여 프로토콜 구성 문제가 있는지 감지합니다.

제어부 문제 및 수정 사항

확인되는 제어부 문제는 다음 문제로 인해 발생하는 경우가 많습니다.

- 호스트 제어부 에이전트(netcpa)가 vsfwd에서 제공하는 메시지 버스 채널을 통해 NSX Manager에 연결할 수 없음
 - 컨트롤러 클러스터에서 DLR/VXLAN 인스턴스에 대한 마스터 역할 처리를 수행하는 데 문제가 있음
- 마스터 역할 처리와 관련된 컨트롤러 클러스터 문제는 종종 NSX Controller 중 하나를 다시 시작하여 해결할 수 있습니다(컨트롤러의 CLI에서 `restart controller`).

제어부 문제 해결에 대한 자세한 내용은 <http://kb.vmware.com/kb/2125767>을 참조하십시오.

문제 해결 데이터 수집

이 섹션에서는 NSX 라우팅 문제 해결에 일반적으로 사용되는 CLI 명령을 요약해서 설명합니다.

NSX Manager

NSX 6.2부터 NSX 라우팅 문제 해결을 위해 NSX Controller 및 기타 NSX 구성 요소에서 실행되던 명령이 NSX Manager에서 직접 실행됩니다.

- DLR 인스턴스 목록
- 각 DLR 인스턴스에 대한 LIF 목록
- 각 DLR 인스턴스에 대한 경로 목록
- 각 DLR 브리징 인스턴스에 대한 MAC 주소 목록
- 인터페이스
- 라우팅 및 전달 테이블
- 동적 라우팅 프로토콜 상태(OSPF 또는 BGP)
- NSX Manager에서 DLR 제어 VM 또는 ESG로 전송하는 구성

DLR 제어 VM 및 ESG

DLR 제어 VM 및 ESG는 해당 인터페이스에서 패킷을 캡처하기 위한 기능을 제공합니다. 패킷 캡처는 라우팅 프로토콜 문제 해결에 도움이 될 수 있습니다.

- 1 `show interfaces`를 실행하여 인터페이스 이름을 나열합니다.
- 2 `debug packet [display | capture] interface <interface name>`을 실행합니다.
 - 캡처를 사용하는 경우 패킷이 `.pcap` 파일에 저장됩니다.
- 3 `debug show files`를 실행하여 저장된 캡처 파일을 나열합니다.

4 `debug copy [scp | ftp] ...`를 실행하여 오프라인 분석을 위해 캡처를 다운로드합니다.

```
d1r-01-0> debug packet capture interface vNic_2
tcpdump: listening on vNic_2, link-type EN10MB (Ethernet), capture size 65535 bytes
43 packets captured
48 packets received by filter
0 packets dropped by kernel
```

```
d1r-01-0> debug show files
total 4.0K
-rw----- 1 3.6K Mar 30 23:49 tcpdump_vNic_2.0
```

```
d1r-01-0> debug copy
  scp  use scp to copy
  ftp  use ftp to copy
```

```
d1r-01-0> debug copy scp
  URL  user@<remote-host>:<path-to>
```

`debug packet` 명령은 백그라운드에서 `tcpdump`를 사용하고 UNIX의 `tcpdump` 필터링 수정자 같은 형식의 필터링 수정자를 수락할 수 있습니다. 필터 표현식의 공백을 밑줄("_")로 바꾸어야 하는지만 고려하면 됩니다.

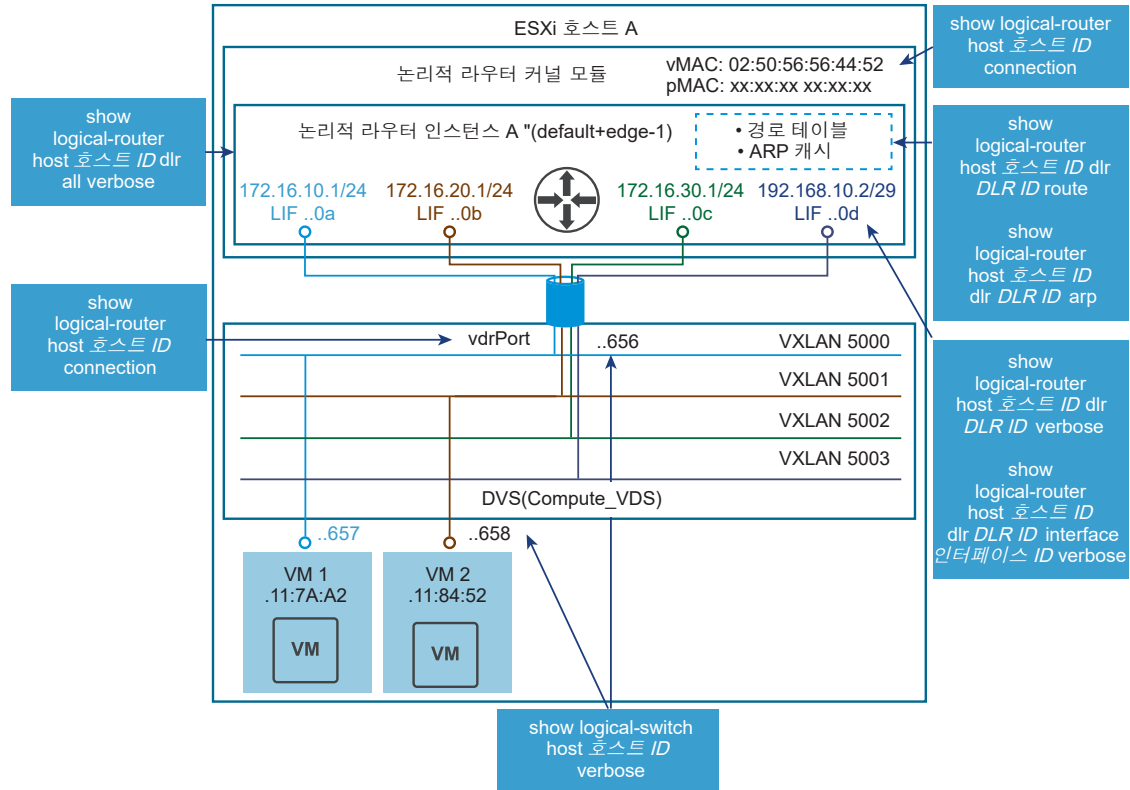
예를 들어 다음 명령은 대화형 세션 자체에 속하는 트래픽을 검토하지 않기 위해 **SSH**를 제외하고 `vNic_0`을 통과하는 모든 트래픽을 표시합니다.

```
plr-02-0> debug packet display interface vNic_0 port_not_22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vNic_0, link-type EN10MB (Ethernet), capture size 65535 bytes
04:10:48.197768 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 4191398894:4191398913,
ack 2824012766, win 913, length 19: BGP, length: 19
04:10:48.199230 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [.] , ack 19, win 2623, length 0
04:10:48.299804 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [P.], seq 1:20, ack 19, win 2623,
length 19: BGP, length: 19
04:10:48.299849 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [.] , ack 20, win 913, length 0
04:10:49.205347 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 19:38, ack 20, win 913,
length 19: BGP, length: 19
```

ESXi 호스트

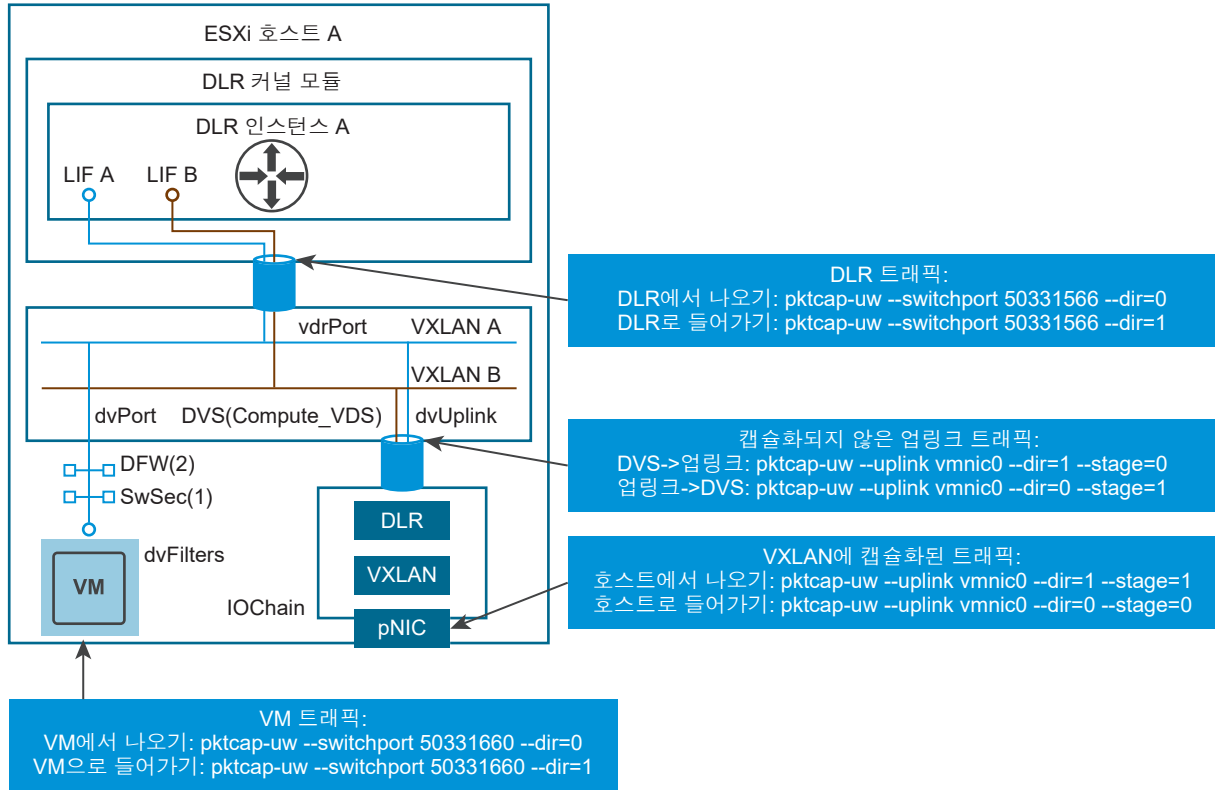
호스트는 **NSX** 라우팅과 긴밀히 연결되어 있습니다. [그림 3-14. NSX 라우팅 문제 해결과 관련된 호스트 구성 요소](#)에서는 라우팅 하위 시스템에 포함되는 구성 요소와 관련 정보를 표시하는 데 사용되는 **NSX Manager CLI** 명령을 시각적으로 보여줍니다.

그림 3-14. NSX 라우팅 문제 해결과 관련된 호스트 구성 요소



데이터 경로에 캡처된 패킷은 패킷 전달의 다양한 단계에서 발생하는 문제를 식별하는 데 도움이 될 수 있습니다. 그림 3-15. 캡처 지점 및 관련 CLI 명령에서는 사용할 주요 캡처 지점 및 각 CLI 명령에 대해 설명합니다.

그림 3-15. 캡처 지점 및 관련 CLI 명령



NSX Edge 문제 해결

4

이 항목에서는 VMware NSX Edge를 이해하고 문제를 해결하기 위한 정보를 제공합니다.

NSX Edge Appliance 문제를 해결하려면 아래의 각 문제 해결 단계가 작업 환경에 맞는지 확인하십시오. 각 단계에서는 가능한 원인을 해결하고 필요한 경우 수정 조치를 취하기 위한 지침 또는 문서에 대한 링크를 제공합니다. 이러한 단계는 문제를 분리하고 적절한 해결책을 찾아내는 데 가장 적합한 순서대로 진행됩니다. 단계를 건너뛰지 마십시오.

현재 릴리스의 릴리스 정보를 확인하여 문제가 해결되었는지 알아봅니다.

VMware NSX Edge를 설치할 때 최소 시스템 요구 사항이 충족되었는지 확인합니다. "NSX 설치 가이드"를 참조하십시오.

설치 및 업그레이드 문제

- 발생하는 문제가 "Would Block(차단)" 문제와 관련되지 않았는지 확인합니다. 자세한 내용은 <https://kb.vmware.com/kb/2107951> 항목을 참조하십시오.
- 업그레이드 또는 재배포가 성공적으로 수행되었으나 Edge 인터페이스에 연결되지 않으면 백엔드 계층 2 스위치의 연결을 확인하십시오. <https://kb.vmware.com/kb/2135285>를 참조하십시오.
- Edge 배포 또는 업그레이드가 오류를 발생하며 실패하는 경우:

```
/sbin/ifconfig vNic_1 up failed : SIOCSIFFLAGS: Invalid argument
```

또는

- 배포 또는 업그레이드가 성공적으로 수행되었으나 Edge 인터페이스에 연결되지 않는 경우:
- `show interface` 명령과 Edge 지원 로그를 실행하면 다음과 비슷한 항목이 표시됩니다.

```
vNic_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
link/ether 00:50:56:32:05:03 brd ff:ff:ff:ff:ff:ff
inet 21.12.227.244/23 scope global vNic_0
inet6 fe80::250:56ff:fe32:503/64 scope link tentative dadfailed
valid_lft forever preferred_lft forever
```

두 경우 모두 호스트 스위치가 준비되지 않았거나 문제가 있습니다. 이러한 상황을 해결하려면 호스트 스위치를 조사하십시오.

구성 문제

- NSX Edge 진단 정보를 수집합니다. <https://kb.vmware.com/kb/2079380>를 참조하십시오.

문자열 `vse_die`를 검색하여 NSX Edge 로그를 필터링합니다. 이 문자열 가까이에 있는 로그는 구성 오류에 대한 정보를 제공합니다.

높은 CPU 활용도

NSX Edge에서 CPU 활용도가 높은 경우 ESXi 호스트에서 `esxtop` 명령을 사용하여 장치의 성능을 확인하십시오. 다음 기술 자료 문서를 검토하십시오.

- <https://kb.vmware.com/kb/1008205>
- <https://kb.vmware.com/kb/1008014>
- <https://kb.vmware.com/kb/1010071>
- <https://kb.vmware.com/kb/2096171>

<https://communities.vmware.com/docs/DOC-9279>도 참조하십시오.

`ksoftirqd` 프로세스의 값이 높으면 수신 패킷 속도가 높은 것을 나타냅니다. 방화벽 규칙의 경우처럼 데이터 경로에 대해 로깅이 사용되도록 설정되어 있는지 확인하십시오. `show log follow` 명령을 실행하여 많은 수의 로그 적중 수가 기록되고 있는지 확인합니다.

패킷 삭제 통계 표시

NSX for vSphere 6.2.3부터 `show packet drops` 명령을 사용하여 다음에 대한 패킷 삭제 통계를 표시할 수 있습니다.

- 인터페이스
- 드라이버
- L2
- L3
- 방화벽

이 명령을 실행하려면 NSX Edge CLI에 로그인하고 기본 모드로 전환합니다. 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오. 예:

```
show packet drops
```

```
vShield Edge Packet Drop Stats:
```

```
Driver Errors
```



```
=====
              TX      TX      TX      RX      RX      RX
Interface Dropped Error Ring Full Dropped Error Out Of Buf
vNic_0      0        0        0        0        0        0
vNic_1      0        0        0        0        0        0
vNic_2      0        0        0        0        0        2
vNic_3      0        0        0        0        0        0
vNic_4      0        0        0        0        0        0
vNic_5      0        0        0        0        0        0
```

Interface Drops

```
=====
Interface RX Dropped TX Dropped
vNic_0              4          0
vNic_1             2710          0
vNic_2              0          0
vNic_3              2          0
vNic_4              2          0
vNic_5              2          0
```

L2 RX Errors

```
=====
Interface length crc frame fifo missed
vNic_0          0  0      0  0      0
vNic_1          0  0      0  0      0
vNic_2          0  0      0  0      0
vNic_3          0  0      0  0      0
vNic_4          0  0      0  0      0
vNic_5          0  0      0  0      0
```

L2 TX Errors

```
=====
Interface aborted fifo window heartbeat
vNic_0          0  0      0          0
vNic_1          0  0      0          0
vNic_2          0  0      0          0
vNic_3          0  0      0          0
vNic_4          0  0      0          0
vNic_5          0  0      0          0
```

L3 Errors

```
=====
IP:
  ReasmFails : 0
  InHdrErrors : 0
  InDiscards : 0
  FragFails : 0
  InAddrErrors : 0
  OutDiscards : 0
  OutNoRoutes : 0
  ReasmTimeout : 0
ICMP:
  InTimeExcds : 0
  InErrors : 227
  OutTimeExcds : 0
```

```

OutDestUnreachs : 152
OutParmProbs : 0
InSrcQuenchs : 0
InRedirects : 0
OutSrcQuenchs : 0
InDestUnreachs : 151
OutErrors : 0
InParmProbs : 0

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0

```

NSX Edge 관리 시 예상 동작

- vSphere Web Client에서 NSX Edge의 L2 VPN을 구성하고 **사이트 구성 세부 정보(Site Configuration Details)**를 추가, 제거 또는 수정할 때 기존 연결이 끊어졌다가 다시 연결됩니다. 이는 예상된 동작입니다.
- NSX Edge는 VM(가상 시스템)으로, 스토리지 디바이스에 저장된 여러 파일로 구성됩니다. 키 파일은 구성 파일, 가상 디스크 파일, NVRAM 설정 파일, 스왑 파일 및 로그 파일입니다. 적용된 VM 스토리지 프로파일 또는 수동 배치에 따라, 가상 시스템 구성 파일, 가상 디스크 파일, 스왑 파일은 같은 위치 또는 다른 데이터스토어의 별도 위치에 배치될 수 있습니다. 서로 다른 위치에 가상 시스템 파일이 있는 경우, NSX Manager는 VM 배포에 대한 VMX 파일이 있는 데이터스토어를 표시하고 사용합니다. 재배포 또는 업그레이드 작업 동안 NSX Manager는 구성된 데이터스토어 또는 VMX 파일을 호스트하는 라이브 데이터스토어에 NSX Edge VM을 배포합니다. 데이터스토어 이름 및 데이터스토어 ID (VM의

VMX 파일 호스트)는 Appliance 매개 변수의 일부로 반환되고, UI에 표시되거나 REST API에 대한 응답으로 제공됩니다. 정확한 각 NSX Manager VM 파일 및 파일에 배치되는 하나 이상의 데이터스토어의 정확한 배치에 대한 자세한 내용은 vCenter Server를 참조해야 합니다. 자세한 내용은 다음 문서를 참조하십시오.

- *vSphere 가상 시스템 관리자.*
- *vSphere 리소스 관리.*
- *vCenter Server 및 호스트 관리*

본 장은 다음 항목을 포함합니다.

- [Edge 방화벽 패킷 삭제 문제](#)
- [Edge 라우팅 연결 문제](#)
- [NSX Manager 및 Edge 통신 문제](#)
- [메시지 버스 디버깅](#)
- [Edge 진단 및 복구](#)

Edge 방화벽 패킷 삭제 문제

방화벽 패킷 삭제 통계 표시

NSX for vSphere 6.2.3부터 `show packet drops` 명령을 사용하여 방화벽에 대한 패킷 삭제 통계를 표시할 수 있습니다.

이 명령을 실행하려면 NSX Edge CLI에 로그인하고 기본 모드로 전환합니다. 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오. 예:

```
show packet drops

vShield Edge Packet Drop Stats:

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
```

```

=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0

```

Edge 패킷 방화벽 문제

명령을 실행하려면 **NSX Edge CLI**에 로그인하고 기본 모드로 전환합니다. 자세한 내용은 "**NSX 명령줄 인터페이스 참조**"를 참조하십시오.

- 1 **show firewall** 명령을 사용하여 방화벽 규칙 테이블을 확인합니다. **usr_rules** 테이블에 구성된 규칙이 표시됩니다.

```

nsxedge> show firewall
Chain PREROUTING (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in  out  source  destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target  prot opt in  out  source  destination
0    78903 16M ACCEPT  all  --  lo   *    0.0.0.0/0  0.0.0.0/0
0    0 0 DROP    all  --  *    *    0.0.0.0/0  0.0.0.0/0
state INVALID
0    140K 9558K block_in all  --  *    *    0.0.0.0/0  0.0.0.0/0
0    23789 1184K ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0
state RELATED,ESTABLISHED
0    116K 8374K usr_rules all  --  *    *    0.0.0.0/0  0.0.0.0/0
0    0 0 DROP    all  --  *    *    0.0.0.0/0  0.0.0.0/0

Chain FORWARD (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in  out  source  destination

Chain OUTPUT (policy ACCEPT 173K packets, 22M bytes)
rid  pkts bytes target  prot opt in  out  source  destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target  prot opt in  out  source  destination
0    78903 16M ACCEPT  all  --  *    lo   0.0.0.0/0  0.0.0.0/0
0    679K 41M DROP    all  --  *    *    0.0.0.0/0  0.0.0.0/0
state INVALID
0    3146M 4098G block_out all  --  *    *    0.0.0.0/0  0.0.0.0/0
0    0 0 ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in tap0 --physdev-out vNic_+
0    0 0 ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out tap0
0    0 0 ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in na+ --physdev-out vNic_+
0    0 0 ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out na+
0    3145M 4098G ACCEPT  all  --  *    *    0.0.0.0/0  0.0.0.0/0

```

```

state RELATED,ESTABLISHED
0      221K   13M usr_rules all -- *      *      0.0.0.0/0      0.0.0.0/0
0      0      0 DROP      all -- *      *      0.0.0.0/0      0.0.0.0/0

Chain block_in (1 references)
rid  pkts bytes target    prot opt in     out     source      destination

Chain block_out (1 references)
rid  pkts bytes target    prot opt in     out     source      destination

Chain usr_rules (2 references)
rid  pkts bytes target    prot opt in     out     source      destination
131074 70104 5086K ACCEPT    all -- *      *      0.0.0.0/0      0.0.0.0/0
match-set 0_131074-os-v4-1 src
131075 116K 8370K ACCEPT    all -- *      *      0.0.0.0/0      0.0.0.0/0
match-set 1_131075-ov-v4-1 dst
131073 151K 7844K ACCEPT    all -- *      *      0.0.0.0/0      0.0.0.0/0

```

`show firewall` 명령의 `POST_ROUTING` 섹션에서 `DROP invalid` 규칙의 증분 값을 확인합니다. 일반적인 원인은 다음과 같습니다.

- 비대칭 라우팅 문제
- 1시간 넘게 비활성 상태였던 TCP 기반 애플리케이션. 비활성 시간 초과 문제가 있으며 애플리케이션이 장시간 유휴 상태인 경우 REST API를 사용하여 비활성 시간 초과 설정을 늘리십시오. <https://kb.vmware.com/kb/2101275> 항목을 참조하십시오.

2 `show ipset` 명령 출력을 수집합니다.

```

nsxedge> show ipset
Name: 0_131074-os-v4-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 0_131074-os-v6-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 1_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2

```

```

Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=6, DestPort=179, SrcPort=Any      (encoded: 0.6.0.179,0.6.0.0/16)
Proto=89, DestPort=Any, SrcPort=Any      (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 1_131075-ov-v6-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=89, DestPort=Any, SrcPort=Any      (encoded: 0.89.0.0/16,0.89.0.0/16)
Proto=6, DestPort=179, SrcPort=Any      (encoded: 0.6.0.179,0.6.0.0/16)

```

- 3 REST API 또는 Edge 사용자 인터페이스를 사용하여 특정 방화벽 규칙에 대해 로깅을 사용하도록 설정하고 `show log follow` 명령을 사용하여 로그를 모니터링합니다.

로그가 보이지 않으면 다음 REST API를 사용하여 DROP Invalid 규칙에 대해 로깅을 사용하도록 설정합니다.

```

URL : https://NSX_Manager_IP/api/4.0/edges/{edgeId}/firewall/config/global

PUT Method
Input representation
<globalConfig>    <!-- Optional -->
<tcpPickOngoingConnections>false</tcpPickOngoingConnections>    <!-- Optional. Defaults to false -->
>
<tcpAllowOutOfWindowPackets>false</tcpAllowOutOfWindowPackets>    <!-- Optional. Defaults to false -->
<tcpSendResetForClosedVsePorts>true</tcpSendResetForClosedVsePorts>    <!-- Optional. Defaults to true -->
<dropInvalidTraffic>true</dropInvalidTraffic>    <!-- Optional. Defaults to true -->
<logInvalidTraffic>true</logInvalidTraffic>    <!-- Optional. Defaults to false -->
<tcpTimeoutOpen>30</tcpTimeoutOpen>    <!-- Optional. Defaults to 30 -->
<tcpTimeoutEstablished>3600</tcpTimeoutEstablished>    <!-- Optional. Defaults to 3600 -->
<tcpTimeoutClose>30</tcpTimeoutClose>    <!-- Optional. Defaults to 30 -->
<udpTimeout>60</udpTimeout>    <!-- Optional. Defaults to 60 -->
<icmpTimeout>10</icmpTimeout>    <!-- Optional. Defaults to 10 -->
<icmp6Timeout>10</icmp6Timeout>    <!-- Optional. Defaults to 10 -->
<ipGenericTimeout>120</ipGenericTimeout>    <!-- Optional. Defaults to 120 -->
</globalConfig>
Output representation
No payload

```

show log follow 명령을 사용하여 다음과 비슷한 로그를 찾습니다.

```
2016-04-18T20:53:31+00:00 edge-0 kernel: nf_ct_tcp: invalid TCP flag combination IN= OUT=
SRC=172.16.1.4 DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=43343 PROTO=TCP
SPT=5050 DPT=80 SEQ=0 ACK=1572141176 WINDOW=512 RES=0x00 URG PSH FIN URGP=0
2016-04-18T20:53:31+00:00 edge-0 kernel: INVALID IN= OUT=vNic_1 SRC=172.16.1.4
DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=43343 PROTO=TCP SPT=5050 DPT=80
WINDOW=512 RES=0x00 URG PSH FIN URGP=0
```

- 4 show flowtable rule_id 명령을 사용하여 Edge 방화벽 상태 테이블에서 일치하는 연결을 확인합니다.

```
nsxedge> show flowtable
1: tcp 6 21554 ESTABLISHED src=192.168.110.10 dst=192.168.5.3 sport=25981
dport=22 pkts=52 bytes=5432 src=192.168.5.3 dst=192.168.110.10 sport=22 dport=259
81 pkts=44 bytes=7201 [ASSURED] mark=0 rid=131073 use=1
2: tcp 6 21595 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=53194
dport=1001 pkts=33334 bytes=11284650 src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=5319
4 pkts=33324 bytes=1394146 [ASSURED] mark=0 rid=0 use=1
```

show flowstats 명령을 사용하여 활성 연결 개수 및 허용되는 최대 연결 개수를 비교합니다.

```
nsxedge> show flowstats
Total Flow Capacity: 65536
Current Statistics :
cpu=0 searched=3280373 found=3034890571 new=52678 invalid=659946 ignore=77605
delete=52667 delete_list=49778 insert=49789 insert_failed=0 drop=0 early_drop=0
error=0 search_restart=0
```

- 5 show log follow 명령을 사용하여 Edge 로그를 확인하고 ALG 삭제물을 찾습니다. tftp_alg, msrpc_alg 또는 oracle_tns와 비슷한 문자열을 검색합니다. 자세한 내용은 다음을 참조하십시오.

- <https://kb.vmware.com/kb/2126674>
- <https://kb.vmware.com/kb/2137751>

Edge 라우팅 연결 문제

- 1 ping <destination_IP_address> 명령을 사용하여 클라이언트에서 제어되는 트래픽을 시작합니다.
- 2 두 인터페이스에서 동시에 트래픽을 캡처하고, 출력을 파일에 쓰고, SCP를 사용하여 내보냅니다.

예:

다음 명령을 사용하여 수신 인터페이스의 트래픽을 캡처합니다.

```
debug packet display interface vNic_0 -n_src_host_1.1.1.1
```

다음 명령을 사용하여 송신 인터페이스의 트래픽을 캡처합니다.

```
debug packet display interface vNic_1 -n_src_host_1.1.1.1
```

동시 패킷 캡처의 경우 ESXi의 ESXi 패킷 캡처 유틸리티 `pktcap-uw` 도구를 사용하십시오. <https://kb.vmware.com/kb/2051814>를 참조하십시오.

패킷 삭제가 일관되게 나타나면 다음과 관련된 구성 오류를 확인하십시오.

- IP 주소 및 경로
- 방화벽 규칙 또는 NAT 규칙
- 비대칭 라우팅
- RP 필터 확인

a `show interface` 명령을 사용하여 인터페이스 IP/서브넷을 확인합니다.

b 데이터부에 누락된 경로가 있으면 다음 명령을 실행합니다.

- `show ip route`
- `show ip route static`
- `show ip route bgp`
- `show ip route ospf`

c `show ip forwarding` 명령을 실행하여 라우팅 테이블에서 필요한 경로를 확인합니다.

d 여러 개의 경로가 있으면 `show rpfilter` 명령을 실행합니다.

```
nsxedge> show rpfilter
net.ipv4.conf.VDR.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.br-sub.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.vNic_0.rp_filter = 1
net.ipv4.conf.vNic_1.rp_filter = 1
net.ipv4.conf.vNic_2.rp_filter = 1
net.ipv4.conf.vNic_3.rp_filter = 1
net.ipv4.conf.vNic_4.rp_filter = 1
net.ipv4.conf.vNic_5.rp_filter = 1
net.ipv4.conf.vNic_6.rp_filter = 1
net.ipv4.conf.vNic_7.rp_filter = 1
net.ipv4.conf.vNic_8.rp_filter = 1
net.ipv4.conf.vNic_9.rp_filter = 1
```

```
nsxedge> show rpfstats
RPF drop packet count: 484
```


RPF 통계를 확인하려면 `show rpfstats` 명령을 실행합니다.

```
nsxedge> show rpfstats
RPF drop packet count: 484
```

패킷 삭제가 무작위로 나타나면 리소스 제한을 확인하십시오.

a CPU 또는 메모리 사용량의 경우 다음 명령을 실행합니다.

- `show system cpu`
- `show system memory`
- `show system storage`
- `show process monitor`
- `top`

ESXi의 경우 `esxtop n` 명령을 실행합니다.

```
PCPU USED(%): 2.5 5.0 3.7 77 AVG: 22
PCPU UTIL(%): 0.5 2.7 3.3 92 AVG: 24
```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT
98255269	98255269	esxtop.11224149	1	67.04	69.86	0.00	6.26
2	2	system	139	3.03	4.61	0.00	12053.58
86329	86329	app-01a	6	0.69	0.57	0.00	466.09
78730	78730	db-01a	6	0.48	0.67	0.00	441.44
90486	90486	app-02a	6	0.38	0.32	0.00	463.42

%VMWAIT	%RDY	%IDLE	%OVRLP	%CSTP	%MLMTD	%SWPWT
11.01	-	0.39	0.00	0.09	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
13900.00	-	28.68	0.00	2.69	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
600.00	0.00	0.19	151.92	0.00	0.00	0.00

NSX Manager 및 Edge 통신 문제

NSX Manager는 VIX 또는 메시지 버스를 통해 NSX Edge와 통신합니다. 해당 Edge가 배포된 후 변경되지 않으면 NSX Manager에서 선택됩니다.

참고 VIX는 NSX 6.3.0 이상에서 지원되지 않습니다.

VIX

- VIX는 ESXi 호스트가 준비되지 않은 경우 NSX Edge에 사용됩니다.
- NSX Manager는 vCenter Server에서 호스트 자격 증명을 가져와 ESXi 호스트에 먼저 연결합니다.

- NSX Manager는 Edge 자격 증명을 사용하여 Edge 장치에 로그인합니다.
- Edge의 `vmtoolsd` 프로세스는 VIX 통신을 처리합니다.

다음과 같은 이유로 VIX 장애가 발생합니다.

- NSX Manager가 vCenter Server와 통신할 수 없습니다.
- NSX Manager가 ESXi 호스트와 통신할 수 없습니다.
- NSX Manager 내부 문제가 있습니다.
- Edge 내부 문제가 있습니다.

VIX 디버깅

NSX Manager 로그에서 VIX 오류 `VIX_E_<error>`를 확인하여 원인을 좁히십시오. 다음과 비슷한 오류를 찾습니다.

```
Vix Command 1126400 failed, reason com.vmware.vshield.edge.exception.VixException: vShield
Edge:10013:Error code 'VIX_E_FILE_NOT_FOUND' was returned by VIX API.:null
```

```
Health check failed for edge edge-13 VM vm-5025 reason:
com.vmware.vshield.edge.exception.VixException: vShield Edge:10013:Error code
'VIX_E_VM_NOT_RUNNING' was returned by VIX API.:null
```

일반적으로 많은 Edge에 대해 동일한 오류가 동시에 발생하면 Edge 측 문제가 아닙니다.

메시지 버스 디버깅

ESXi 호스트가 준비되어 있을 때 NSX Edge 통신에 메시지 버스가 사용됩니다.

문제가 발생하면 NSX Manager 로그에 다음과 비슷한 항목이 포함되어 있을 수 있습니다.

```
GMT ERROR taskScheduler-6 PublishTask:963 - Failed to configure VSE-vm index 0, vm-id vm-117,
edge edge-5. Error: RPC request timed out
```

이 문제는 다음 경우에 발생합니다.

- Edge가 잘못된 상태입니다.
- 메시지 버스 연결이 끊어졌습니다.

Edge의 문제를 진단하려면:

- `rmq` 연결을 확인하려면 다음 명령을 실행합니다.

```
nsxedge> show messagebus messages
-----
Message bus is enabled
cmd conn state : listening
```

```
init_req      : 1
init_resp     : 1
init_req_err   : 0
...
```

- vmci 연결을 확인하려면 다음 명령을 실행합니다.

```
nsxedge> show messagebus forwarder
```

```
-----
Forwarder Command Channel
```

```
vmci_conn      : up
app_client_conn : up
vmci_rx        : 3649
vmci_tx        : 3648
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 8
vmci_tx_no_socket : 0
app_rx        : 3648
app_tx        : 3649
app_rx_err    : 0
app_tx_err    : 0
app_conn_req   : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
```

```
Forwarder Event Channel
```

```
vmci_conn      : up
app_client_conn : up
vmci_rx        : 1143
vmci_tx        : 13924
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 0
vmci_tx_no_socket : 0
app_rx        : 13924
app_tx        : 1143
app_rx_err    : 0
app_tx_err    : 0
app_conn_req   : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
```

```
cli_rx        : 1
cli_tx        : 1
cli_tx_err    : 0
counters_reset : 0
```

이 예에서 출력 **vmci_closed_by_peer: 8**은 호스트 에이전트에서 연결을 닫은 횟수를 나타냅니다. 이 횟수가 늘어나고 있으며 **vmci conn**이 다운되면 호스트 에이전트는 **RMQ** 브로커에 연결할 수 없습니다. **show log follow**의 **Edge** 로그에서 다음 오류가 반복적으로 나타나는지 확인합니다.

VmciProxy: [daemon.debug] VMCi Socket is closed by peer(소켓이 피어에 의해 닫힘)

ESXi 호스트의 문제를 진단하려면:

- ESXi 호스트가 RMQ 브로커에 연결되어 있는지 확인하려면 다음 명령을 실행합니다.

```
esxcli network ip connection list | grep 5671
```

tcp	0	0	10.32.43.4:43329	10.32.43.230:5671	ESTABLISHED	35854	newreno	
vsfwd								
tcp	0	0	10.32.43.4:52667	10.32.43.230:5671	ESTABLISHED	35854	newreno	
vsfwd								
tcp	0	0	10.32.43.4:20808	10.32.43.230:5671	ESTABLISHED	35847	newreno	
vsfwd								
tcp	0	0	10.32.43.4:12486	10.32.43.230:5671	ESTABLISHED	35847	newreno	vsfwd

Edge 진단 및 복구

Edge 진단

- 다음 명령을 사용하여 `vmtoolsd`가 실행되고 있는지 확인합니다.

```
nsxedge> show process list
Perimeter-Gateway-01-0> show process list
%CPU %MEM    VSZ   RSZ STAT  STARTED    TIME COMMAND
 0.0  0.1   4244   720 Ss      May 16 00:00:15 init [3]
...
 0.0  0.1   4240   640 S       May 16 00:00:00 logger -p daemon debug -t vserrdd
 0.2  0.9  57192  4668 S       May 16 00:23:07 /usr/local/bin/vmtoolsd --plugin-pa
 0.0  0.4   4304  2260 SLs     May 16 00:01:54 /usr/sbin/watchdog
...
```

- 다음 명령을 실행하여 Edge가 정상 상태인지 확인합니다.

```
nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
profiling       : 0
cfg_rx          : 1
cfg_rx_msgbus   : 0
...
```

`show eventmgr` 명령을 사용하여 쿼리 명령이 수신되고 처리되는지 확인하십시오.

```
nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
profiling       : 0
cfg_rx          : 1
cfg_rx_msgbus   : 0
```

```

cfg_rx_err      : 0
cfg_exec_err    : 0
cfg_resp        : 0
cfg_resp_err    : 0
cfg_resp_ln_err : 0
fastquery_rx    : 0 fastquery_err : 0
clearcmd_rx     : 0
clearcmd_err    : 0
ha_rx           : 0
ha_rx_err       : 0
ha_exec_err     : 0
status_rx       : 16
status_rx_err   : 0
status_svr      : 10
status_evt      : 0
status_evt_push : 0
status_ha       : 0
status_ver      : 1
status_sys      : 5
status_cmd      : 0
status_svr_err  : 0
status_evt_err  : 0
status_sys_err  : 0
status_ha_err   : 0
status_ver_err  : 0
status_cmd_err  : 0
evt_report      : 1
evt_report_err  : 0
hc_report       : 10962
hc_report_err   : 0
cli_rx          : 2
cli_resp        : 1
cli_resp_err    : 0
counter_reset   : 0
----- Health Status -----
system status   : good
ha state        : active
cfg version     : 7
generation      : 0
server status   : 1
syslog-ng       : 1
haproxy         : 0
ipsec           : 0
sslvpn         : 0
l2vpn          : 0
dns             : 0
dhcp            : 0
heartbeat       : 0
monitor         : 0
gslb            : 0
----- System Events -----

```

Edge 복구

vmtoolsd가 실행되고 있지 않거나 NSX Edge가 잘못된 상태이면 Edge를 재부팅하십시오.

충돌에서 복구하려는 경우 재부팅만으로 충분합니다. 다시 배포할 필요는 없습니다.

참고 다시 배포가 완료되면 이전 Edge의 모든 로깅 정보를 적어둡니다.

커널 충돌을 디버깅하려면 다음이 필요합니다.

- 충돌 상태에 있는 동안 Edge VM에 대한 vmss(VM 일시 중단) 또는 vmsn(VM 스냅샷) 파일. vmem 파일이 있는 경우에도 필요합니다. 이러한 파일은 VMware 지원이 분석할 수 있는 커널 코어 덤프 파일을 추출하는 데 사용할 수 있습니다.
- 충돌한 Edge가 재부팅(다시 배포는 아님)된 직후에 생성된 Edge 지원 로그. Edge 로그를 확인할 수도 있습니다. <https://kb.vmware.com/kb/2079380>를 참조하십시오.
- Edge 콘솔의 스크린샷은 항상 전체 충돌 보고서를 포함하는 것은 아니지만 도움이 될 수 있습니다.

방화벽 문제 해결

5

이 섹션에서는 방화벽 문제 해결에 대한 정보를 제공합니다.

본 장은 다음 항목을 포함합니다.

- 분산 방화벽 정보
- ID 방화벽

분산 방화벽 정보

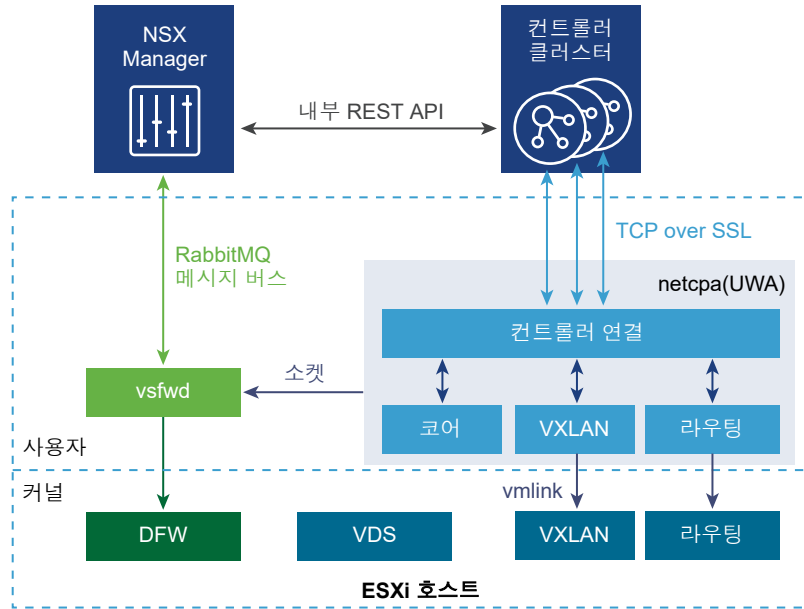
RabbitMQ 메시지 버스는 vsfwd(RMQ 클라이언트) 및 NSX Manager에 호스팅된 RMQ 서버 프로세스 간 통신에 사용됩니다. 이 메시지 버스는 NSX Manager가 커널의 분산 방화벽에서 프로그래밍되어야 하는 정책 규칙을 비롯한 다양한 정보를 ESXi 호스트에 보내는 데 사용됩니다.

NSX 분산 방화벽은 가상 워크로드와 네트워크에 대한 가시성 및 제어 기능을 제공하는 하이퍼바이저 커널이 포함된 방화벽입니다. 데이터센터 및 클러스터, 가상 시스템 이름 및 태그, IP/VLAN/VXLAN 주소와 같은 네트워크 구성 요소, Active Directory의 사용자 그룹 ID와 같은 VMware vCenter 개체를 기반으로 액세스 제어 정책을 생성할 수 있습니다. 이제 가상 시스템이 물리적 호스트에서 vMotion을 통해 이동될 때 일관된 액세스 제어 정책이 강제로 적용되므로 방화벽 규칙을 다시 작성할 필요가 없습니다. 분산 방화벽은 하이퍼바이저에 포함되어 있기 때문에 회선에 가까운 속도의 처리량을 제공함으로써 물리적 서버에서 더 높은 수준의 워크로드 통합을 가능하게 합니다. 이 방화벽이 지닌 분산 특성은 데이터센터에 호스트가 추가될 때마다 방화벽 용량을 자동 확장하는 확장 아키텍처를 제공합니다.

ESXi 호스트의 NSX Manager 웹 애플리케이션 및 NSX 구성 요소는 NSX Manager 웹 애플리케이션과 동일한 가상 시스템에서 실행되는 RabbitMQ 브로커 프로세스를 통해 서로 통신합니다. 사용되는 통신 프로토콜은 AMQP(Advanced Message Queueing Protocol)이고 해당 채널은 SSL을 사용하여 보호됩니다.

ESXi 호스트에서 VSFWD(vShield 방화벽 데몬) 프로세스는 브로커에 대한 SSL 연결을 설정 및 유지 보수하고 다른 구성 요소 대신 메시지를 송수신하며 IPC를 통해 통신합니다.

그림 5-1. ESXi 호스트 사용자 및 커널 공간 다이어그램



DFW에 대한 CLI 명령

NSX Manager 중앙 CLI에서 분산 방화벽에 대한 대부분의 정보를 가져올 수 있습니다.

Show dfw 중앙 CLI 명령 사용

원하는 정보로 드릴다운하는 경로는 다음과 같습니다.

- 1 관리자 자격 증명을 사용하여 NSX Manager 중앙 CLI에 로그인합니다.
- 2 다음 명령을 실행합니다.
 - a 모든 클러스터를 표시하려면 `show cluster all` 명령을 실행합니다.

```
nsxmgr>show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	Compute Cluster A	domain-c33	Datacenter Site A	Enabled
2	Management & Edge Cluster	domain-c41	Datacenter Site A	Enabled

- b 특정 클러스터에 호스트를 표시하려면 `show cluster <clusterID>` 명령을 실행합니다.

```
nsxmgr> show cluster domain-c33
```

Datacenter: Datacenter Site A
Cluster: Compute Cluster A

No.	Host Name	Host Id	Installation Status
1	esx-02a.corp.local	host-32	Enabled
2	esx-01a.corp.local	host-28	Enabled

- c 호스트의 모든 VM을 표시하려면 `show host <hostID>`를 실행합니다.

```
nsxmgr> show host host-28
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
No.  VM Name    VM Id    Power Status
1    web-02a     vm-219   on
2    web-01a     vm-216   on
3    win8-01a    vm-206   off
4    app-02a     vm-264   on
```

- d 필터 이름 및 vNIC ID를 포함하는 VM에 대한 정보를 표시하려면 `show vm <vmID>` 명령을 실행합니다.

```
nsxmgr> show vm vm-264
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
Host-ID: host-28
VM: app-02a
Virtual Nics List:
1.
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Filters        nic-79396-eth0-vmware-sfw.2
```

- e vNIC ID를 기록하고 `show dfw vnic <vnicID>` 및 `show dfw host <hostID> filter <filter ID> rules`와 같은 추가 명령을 실행합니다.

```
nsxmgr> show dfw vnic 502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Mac Address    00:50:56:ae:6c:6b
Port Group Id  dvportgroup-385
Filters        nic-79396-eth0-vmware-sfw.2

nsxmgr> show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules
ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmp type 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-securitygroup-11 port 8443 accept;
```

```

rule 1010 at 6 inout protocol icmp icmptype 8 from addrset ip-securitygroup-10 to addrset
ip-securitygroup-11 accept;
rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
rule 1009 at 8 inout protocol icmp icmptype 8 from addrset ip-securitygroup-11 to addrset
ip-securitygroup-12 accept;
rule 1003 at 9 inout protocol ipv6-icmp icmptype 136 from any to any accept;
rule 1003 at 10 inout protocol ipv6-icmp icmptype 135 from any to any accept;
rule 1002 at 11 inout protocol udp from any to any port 67 accept;
rule 1002 at 12 inout protocol udp from any to any port 68 accept;
rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
# Filter rules
rule 1004 at 1 inout ethertype any from any to any accept;
}

```

export host-tech-support 중량 CLI 명령 사용

export host-tech-support 명령을 사용하면 ESXi 호스트 지원 번들을 지정된 서버로 내보낼 수 있습니다. 또한 이 명령은 지정된 호스트에 대해 다음과 같은 NSX 관련 출력 및 파일(다음으로 제한되지 않음)을 수집합니다.

- VMKernel 및 vsfwd 로그 파일
- 필터 목록
- DFW 규칙 목록
- 컨테이너 목록
- SpoofGuard 세부 정보
- 호스트 관련 정보
- IP 검색 관련 정보
- RMQ 명령 출력
- 보안 그룹, 서비스 프로파일 및 인스턴스 세부 정보
- ESX CLI 관련 출력

또한 이 명령은 NSX Manager에 대한 모든 임시 파일을 제거합니다.

NSX 관련 출력 및 파일을 수집하려면:

- 1 관리자 자격 증명을 사용하여 NSX Manager 중량 CLI에 로그인합니다.
- 2 다음 명령을 실행합니다.
 - a show cluster all - 필요한 호스트 ID 찾기.
 - b export host-tech-support host-id scp uid@ip:/path - NSX 기술 지원 번들을 생성하고 지정된 서버에 복사.

자세한 내용은 다음을 참조하십시오.

- [NSX 명령줄 인터페이스 빠른 참조](#).
- ["NSX 명령줄 인터페이스 참조"](#).

분산 방화벽 문제 해결

이 항목에서는 VMware NSX 6.x DFW(분산 방화벽)를 이해하고 관련 문제를 해결하기 위한 정보를 제공합니다.

문제

- 분산 방화벽 규칙 게시가 실패합니다.
- 분산 방화벽 규칙 업데이트가 실패합니다.

원인

아래의 각 문제 해결 단계가 작업 환경에 맞는지 확인하십시오. 각 단계에서는 가능한 원인을 해결하고 필요한 경우 수정 조치를 취하기 위한 지침 또는 문서에 대한 링크를 제공합니다. 이러한 단계는 문제를 분리하고 적절한 해결책을 찾아내는 데 가장 적합한 순서대로 진행됩니다. 각 단계를 수행한 후에 분산 방화벽 규칙 업데이트/게시를 다시 시도하십시오.

해결책

- 1 NSX VIB가 클러스터의 각 ESXi 호스트에 성공적으로 설치되었는지 확인합니다. 이렇게 하려면 클러스터의 각 ESXi 호스트에 대해 다음 명령을 실행합니다.

```
# esxcli software vib list | grep vsip
esx-vsip                6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04

# esxcli software vib list | grep vxlan
esx-vxlan               6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04
```

NSX 6.2 이전 버전에는 다음과 같은 추가 VIB가 있습니다.

```
# esxcli software vib list | grep dvfilter
esx-dvfilter-switch-security  5.5.0-0.0.2318233  VMware  VMwareCertified  2015-01-24
```

ESXi 6.0 이상이 있는 NSX 6.3.3부터 esx-vxlan 및 esx-vsip VIB가 esx-nsxv로 대체됩니다.

```
# esxcli software vib list | grep nsxv
esx-nsxv                 6.0.0-0.0.6216823  VMware  VMwareCertified  2017-08-10
```

2 ESXi 호스트에서 vShield-Stateful-Firewall 서비스가 실행 상태인지 확인합니다.

예:

```
# /etc/init.d/vShield-Stateful-Firewall status

vShield-Stateful-Firewall is running
```

3 메시지 버스가 NSX Manager와 제대로 통신하고 있는지 확인합니다.

이 프로세스는 감시 스크립트에 의해 자동으로 시작되며, 알 수 없는 이유로 프로세스가 종료되는 경우 프로세스가 다시 시작됩니다. 클러스터의 각 ESXi 호스트에 대해 다음 명령을 실행합니다.

예:

```
# ps | grep vsfwd

107557 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
```

명령 출력에서 12개 이상의 vsfwd 프로세스가 실행되고 있어야 합니다. 더 적은(주로 2개만) 프로세스가 실행 중인 경우 vsfwd가 제대로 실행되지 않는 것입니다.

4 방화벽 구성에서 통신을 위해 포트 5671이 열려 있는지 확인합니다.

이 명령은 RabbitMQ 브로커와의 VSFWD 연결을 보여줍니다. ESXi 호스트에 대해 다음 명령을 실행하여 ESXi 호스트의 vsfwd 프로세스에서 NSX Manager로의 연결 목록을 확인합니다. 통신이 가능하도록 환경의 외부 방화벽에서 포트 5671이 열려 있는지 확인합니다. 또한 포트 5671에 둘 이상의 연결이 있어야 합니다. ESXi 호스트에는 RMQ 브로커와도 연결되는 NSX Edge 가상 시스템이 배포되어 있으므로 포트 5671에 더 많은 연결이 있을 수 있습니다.

예:

```
# esxccli network ip connection list |grep 5671

tcp          0      0 192.168.110.51:30133      192.168.110.15:5671    ESTABLISHED
10949155 newreno vsfwd
tcp          0      0 192.168.110.51:39156      192.168.110.15:5671    ESTABLISHED
10949155 newreno vsfwd
```

5 VSFWD가 구성되어 있는지 확인합니다.

다음 명령은 NSX Manager IP 주소를 표시합니다.

```
# esxcfg-advcfg -g /UserVars/RmqIpAddress
```

- 6 이 ESXi 호스트에 대해 호스트 파일을 사용하는 경우 호스트 프로파일에 RabbitMQ 구성이 설정되지 않아야 합니다.

참조할 사항:

- <https://kb.vmware.com/kb/2092871>
- <https://kb.vmware.com/kb/2125901>

- 7 ESXi 호스트의 RabbitMQ 자격 증명이 NSX Manager와 동기화되지 않았는지 확인합니다. NSX Manager 기술 지원 로그를 다운로드합니다. 모든 NSX Manager 기술 지원 로그를 수집한 후에 모든 로그에서 다음과 같은 항목을 검색합니다.

host-420을 문제가 의심되는 호스트의 호스트 ID로 바꿉니다.

```
PLAIN login refused: user 'uw-host-420' - invalid credentials.
```

- 8 이러한 항목을 의심되는 ESXi 호스트에 대한 로그에서 찾으면 메시지 버스를 다시 동기화하십시오.

메시지 버스를 다시 동기화하려면 REST API를 사용하십시오. 문제를 보다 잘 이해하려면 메시지 버스가 다시 동기화된 직후에 로그를 수집하십시오.

```
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
Request:

POST https://NSX_Manager_IP/api/2.0/nwfabric/configure?action=synchronize

Request Body:

<nwFabricFeatureConfig>
<featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
<resourceConfig>
<resourceId>{HOST/CLUSTER MOID}</resourceId>
</resourceConfig>
</nwFabricFeatureConfig>
```

- 9 export host-tech-support <host-id> scp <uid@ip:/path> 명령을 사용하여 호스트별 방화벽 로그를 수집합니다.

예:

```
nsxmgr# export host-tech-support host-28 scp Administrator@192.168.110.10
Generating logs for Host: host-28...
```

- 10** `show dfw host host-id summarize-dvfilter` 명령을 사용하여 방화벽 규칙이 호스트에 배포되었는지와 가상 시스템에 적용되었는지 확인합니다.

출력에서 `module: vsip`는 DFW 모듈이 로드되어 실행 중임을 나타냅니다. `name`은 각 `vNic`에서 실행 중인 방화벽을 표시합니다.

클러스터 도메인 ID를 가져오는 `show dfw cluster all` 명령을 실행한 다음 호스트 ID를 가져오는 `show dfw cluster domain-id`를 실행하여 호스트 ID를 가져올 수 있습니다.

예:

```
# show dfw host host-28 summarize-dvfilter

Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: ESXi-Firewall, refCount: 5, rev: 0x1010000, apiRev: 0x1010000, module: esxfw
agent: dvfilter-generic-vmware, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-generic-fastpath
agent: dvfilter-generic-vmware-swsec, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-switch-security
agent: bridgelearningfilter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vdrb
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: vmware-sfw, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: vsip

Slowpaths:

Filters:
world 342296 vmm0:2-vm-RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979 vcUuid:'3f
43 54 76 8f 54 4e 5a-8d 01 59 65 4a 4e 99 79'
port 50331660 2-vm-RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979.eth1
vNic slot 2
  name: nic-342296-eth1-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 1
  name: nic-342296-eth1-dvfilter-generic-vmware-swsec.1
  agentName: dvfilter-generic-vmware-swsec
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Alternate Opaque Channel
port 50331661 (disconnected)
vNic slot 2
  name: nic-342296-eth2-vmware-sfw.2 <===== DFW filter
  agentName: vmware-sfw
  state: IOChain Detached
  vmState: Detached
  failurePolicy: failClosed
```

```

slowPathID: none
filter source: Dynamic Filter Creation
port 33554441 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979
vNic slot 2
name: nic-342296-eth0-vmware-sfw.2<===== DFW filter
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation

```

11 show dfw host hostID filter filterID rules 명령을 실행합니다.

예):

```

# show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules

ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmptype 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmptype 8 from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 accept;
  rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
  rule 1009 at 8 inout protocol icmp icmptype 8 from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 accept;
  rule 1003 at 9 inout protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 1003 at 10 inout protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 1002 at 11 inout protocol udp from any to any port 67 accept;
  rule 1002 at 12 inout protocol udp from any to any port 68 accept;
  rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
  # Filter rules
  rule 1004 at 1 inout ethertype any from any to any accept;
}

```

12 show dfw host hostID filter filterID addrsets 명령을 실행합니다.

예):

```

# show dfw host host-28 filter nic-342296-eth2-vmware-sfw.2 addrsets

addrset dst1011 {
ip 172.16.10.10,
ip 172.16.10.11,
}

```

```

ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-10 {
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-11 {
ip 172.16.20.11,
ip fe80::250:56ff:feae:23b9,
}
addrset ip-securitygroup-12 {
ip 172.16.30.11,
ip fe80::250:56ff:feae:d42b,
}
addrset src1013 {
ip 172.16.10.12,
ip 172.17.10.11,
ip fe80::250:56ff:feae:cf88,
ip fe80::250:56ff:feae:f86b,
}

```

- 13** 위의 각 문제 해결 단계가 유효한지 확인했으나 호스트 가상 시스템에 방화벽 규칙을 게시할 수 없는 경우 NSX Manager UI 또는 다음 REST API 호출을 통해 호스트 수준 강제 동기화를 실행하십시오.

```

URL : [https:]https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml

```

해결책

참고:

- 방화벽 규칙이 IP 주소를 사용하지 않는 경우 가상 시스템에서 VMware Tools가 실행되고 있는지 확인하십시오. 자세한 내용은 <https://kb.vmware.com/kb/2084048> 항목을 참조하십시오.

VMware NSX 6.2.0에는 DHCP 스누핑 또는 ARP 스누핑을 사용하여 가상 시스템의 IP 주소를 검색하는 옵션이 추가되었습니다. NSX는 이 새로운 검색 메커니즘을 통해 VMware Tools가 설치되지 않은 가상 시스템에서 IP 주소 기반 보안 규칙을 적용할 수 있습니다. 자세한 내용은 NSX 6.2.0 릴리스 정보를 참조하십시오.

DFW는 호스트 준비 프로세스가 완료되는 즉시 활성화됩니다. 가상 시스템에 DFW 서비스가 전혀 필요하지 않을 경우 제외 목록 기능에 추가될 수 있습니다(기본적으로 NSX Manager, NSX Controller 및 Edge Services Gateway는 DFW 기능에서 자동으로 제외됨). DFW에서 [모두 거부] 규칙을 생성한 후에 vCenter Server 액세스가 차단될 수 있습니다. 자세한 내용은 <https://kb.vmware.com/kb/2079620> 항목을 참조하십시오.

- VMware 기술 지원을 통해 VMware NSX 6.x DFW(분산 방화벽) 문제를 해결할 경우 다음이 필요합니다.
 - 클러스터의 각 ESXi 호스트에 대한 `show dfw host hostID summarize-dvfilter` 명령의 출력
 - **Networking & Security > 방화벽 > 일반(Networking and Security > Firewall > General)** 탭에서 분산 방화벽 구성을 누르고 **구성 내보내기(Export Configuration)**를 클릭합니다. 이렇게 하면 분산 방화벽 구성이 XML 형식으로 내보내집니다.
 - NSX Manager 로그 자세한 내용은 <https://kb.vmware.com/kb/2074678> 항목을 참조하십시오.
 - vCenter Server 로그 자세한 내용은 <https://kb.vmware.com/kb/1011641> 항목을 참조하십시오.

ID 방화벽

문제

ID 방화벽 규칙의 게시 또는 업데이트가 실패합니다.

원인

IDFW(ID 방화벽)는 사용자 기반 DFW(분산 방화벽 규칙)를 허용합니다.

사용자 기반 분산 방화벽 규칙은 AD(Active Directory) 그룹 멤버 자격의 자격에 따라 결정됩니다. IDFW는 Active Directory 사용자가 로그인된 위치를 모니터링하고 DFW에서 방화벽 규칙을 적용하는 데 사용하는 IP 주소에 로그인을 매핑합니다. IDFW에는 Guest Introspection 프레임워크 및/또는 Active Directory 이벤트 로그 스크랩이 필요합니다.

해결책

- 1 Active Directory 서버 전체/델타 동기화가 NSX Manager에서 작동하는지 확인합니다.
 - a vSphere Web Client에서 NSX Manager에 연결된 vCenter에 로그인합니다.
 - b **홈 > Networking & Security > NSX Manager(Home > Networking & Security> NSX Managers)**로 이동한 후 목록에서 NSX Manager를 선택합니다.
 - c **관리(Manage)** 탭을 선택한 후 **도메인(Domains)** 탭을 선택합니다. 목록에서 도메인을 선택합니다. **마지막 동기화 상태(Last Synchronization Status)** 열에 [성공]이 표시되고 **마지막 동기화 시간(Last Synchronization Time)**은 현재인지 확인합니다.

- 2 방화벽 환경이 로그인 감지에 이벤트 로그 스크랩 방법을 사용하는 경우 다음 단계에 따라 도메인에 대해 이벤트 로그 서버를 구성했는지 확인합니다.
 - a vSphere Web Client에서 NSX Manager에 연결된 vCenter에 로그인합니다.
 - b **홈 > Networking & Security > NSX Manager(Home > Networking & Security> NSX Managers)**로 이동한 후 목록에서 NSX Manager를 선택합니다.
 - c **관리(Manage)** 탭을 선택한 후 **도메인(Domains)** 탭을 선택합니다. 목록에서 도메인을 선택합니다. 여기서 자세한 도메인 구성을 보고 편집할 수 있습니다.
 - d 도메인 세부 정보에서 **이벤트 로그 서버(Event Log Servers)**를 선택하고 이벤트 로그 서버가 추가되었는지 확인합니다.
 - e 이벤트 로그 서버를 선택하고 **마지막 동기화 상태(Last Sync Status)** 열에 [성공]이 표시되고 **마지막 동기화 시간(Last Sync Time)**이 현재인지 확인합니다.
- 3 방화벽 환경이 Guest Introspection을 사용하는 경우 해당 프레임워크를 IDFW 보호 VM이 상주할 계산 클러스터에 배포해야 합니다. UI의 서비스 상태는 녹색입니다. Guest Introspection 진단 정보는 기술 자료 문서, vShield Endpoint/NSX Guest Introspection 문제 해결 <https://kb.vmware.com/kb/2094261> 및 VMware NSX for vSphere 6.x Guest Introspection Universal Service Virtual Machine에서 로그 수집 <https://kb.vmware.com/kb/2144624>에서 찾을 수 있습니다.
- 4 로그인 감지 방법의 구성이 올바른지 확인한 후에 NSX Manager가 로그인 이벤트를 수신하는지 확인합니다.
 - a Active Directory 사용자로 로그인합니다.
 - b 다음 명령을 실행하여 로그인 이벤트를 쿼리합니다. 사용자가 결과에 반환되는지 확인합니다. GET <https://<nsxmgr-ip>/1.0/identity/userIpMapping>.

```
Example output:
<UserIpMappings>
  <UserIpMapping>
    <ip>50.1.111.192</ip>
    <userName>user1_group20</userName>
    <displayName>user1_group20</displayName>
    <domainName>cd.ad1.db.com</domainName>
    <startTime class="sql-timestamp">2017-05-11 22:30:51.0</startTime>
    <startType>EVENTLOG</startType>
    <lastSeenTime class="sql-timestamp">2017-05-11 22:30:52.0</lastSeenTime>
    <lastSeenType>EVENTLOG</lastSeenType>
  </UserIpMapping>
</UserIpMappings>
```

- 5 Security Group이 방화벽 규칙에서 사용되는지 또는 할당된 보안 정책이 있는지 확인합니다. 다음 조건 중 하나가 충족되지 않으면 IDFW의 Security Group 처리는 진행되지 않습니다.

- 6 IDFW가 로그인을 올바르게 감지한 후에 데스크톱 VM이 상주하는 ESXi 호스트가 올바른 구성을 수신하는지 확인합니다. 이러한 단계는 NSX Manager 중앙 CLI를 사용합니다. **ip-securitygroup** 목록에 채워진 데스크톱 VM IP 주소를 확인하려면
- a DFW에 대한 CLI 명령을 참조하여 데스크톱 VM에 적용된 필터 이름을 검색하십시오.
 - b DFW 찾기 규칙 항목을 확인하려면 `show dfw host hostID filter filterID rules` 명령을 실행합니다.
 - c ip-securitygroup 목록에 채워진 IP 주소를 보려면 `show dfw host hostID filter filterID addrsets` 명령을 실행합니다. 목록에 IP가 표시되는지 확인합니다.

해결책

참고: VMware 기술 지원을 통해 ID IDFW 문제를 해결할 때는 다음 데이터가 유용합니다.

- 이벤트 로그 스크랩을 사용하는 경우 다음 Active Directory 크기 데이터:
 - 단일 NSX Manager의 도메인 수
 - 포리스트 수
 - 사용자/포리스트 수
 - 사용자/도메인 수
 - 도메인당 Active Directory 그룹 수
 - 사용자/Active Directory 그룹 수
 - Active Directory/사용자 수
 - 도메인 컨트롤러 수
 - Active Directory 로그 서버 수
- 다음 사용자 로그인 크기 데이터:
 - 분당 평균 사용자 수
- VDI와 IDFW를 사용하는 배포 세부 정보:
 - VDI 데스크톱/VC 수
 - 호스트/VC 수
 - VDI 데스크톱/호스트 수
- Guest Introspection을 사용하는 경우:
 - VMTools 버전(Guest Introspection 드라이버)
 - Windows Guest OS 버전

로드 밸런싱 문제 해결

6

NSX Edge 로드 밸런스를 사용하면 특정 대상으로 이어지는 여러 경로로 네트워크 트래픽을 보낼 수 있습니다. 즉, 로드 분산이 사용자에게 투명하게 진행되도록 들어오는 서비스 요청을 여러 서버 간에 균일하게 분산합니다. NSX에서 구성하는 로드 밸런싱 서비스에는 2가지 유형이 있습니다. 하나는 프록시 모드로도 알려져 있는 단일 암 모드이고, 다른 하나는 투명 모드로도 알려져 있는 인라인 모드입니다. 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

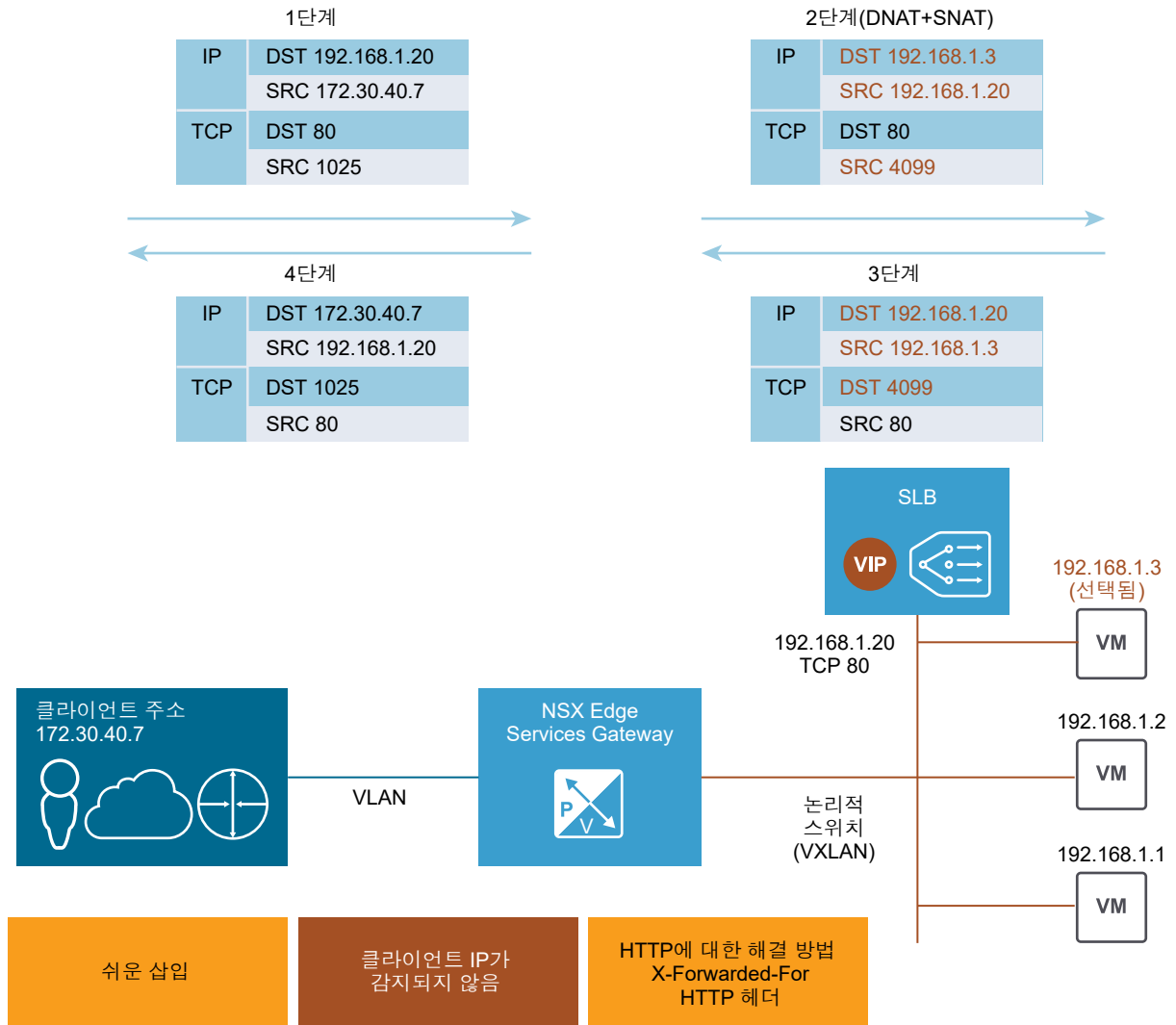
문제 해결 및 구성 확인을 시작하기 전에 오류에 대한 정확한 설명을 가져오고, 클라이언트, 가상 서버 및 백엔드 서버와 관련된 토폴로지 맵을 생성하고, 애플리케이션 요구 사항을 이해합니다. 예를 들어 클라이언트가 연결할 수 없거나 연결 후에 임의의 세션 오류와 다른 오류가 표시될 수 있습니다. 로드 밸런서 문제를 해결할 때 항상 맨 먼저 연결 오류를 확인합니다.

본 장은 다음 항목을 포함합니다.

- 단일 암 로드 밸런서 구성
- 로드 밸런서에 대한 문제 해결 순서도
- UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결
- CLI를 사용하여 로드 밸런서 문제 해결
- 일반 로드 밸런서 문제

단일 암 로드 밸런서 구성

ESG(Edge Services Gateway)는 수신 클라이언트 트래픽에 대한 프록시로 간주될 수 있습니다.



프록시 모드에서 로드 밸런서는 자체 IP 주소를 소스 주소로 사용하여 백엔드 서버로 요청을 전송합니다. 백엔드 서버는 로드 밸런서에서 전송되는 모든 트래픽을 확인하고 응답을 로드 밸런서로 직접 보냅니다. 이 모드는 **SNAT** 모드 또는 비투명 모드라고도 합니다. 자세한 내용은 "**NSX 관리 가이드**"를 참조하십시오.

일반적인 **NSX** 단일 암 로드 밸런서는 논리적 라우터와는 별도로 해당 백엔드 서버가 있는 동일한 서브넷에 배포됩니다. **NSX** 로드 밸런서 가상 서버는 클라이언트의 수신 요청을 가상 IP에서 수신하고 해당 요청을 백엔드 서버로 발송합니다. 반환 트래픽의 경우 소스 IP 주소를 백엔드 서버에서 **VIP(가상 IP)** 주소로 변경한 다음 가상 IP 주소를 클라이언트로 보내기 위해 역방향 **NAT**가 필요합니다. 이 작업이 없으면 클라이언트의 연결이 끊어질 수 있습니다.

ESG는 트래픽을 수신하면 두 가지 작업을 수행합니다. 하나는 **VIP** 주소를 로드 밸런싱된 시스템 중 하나의 IP 주소로 변경하기 위한 **DNAT**(대상 네트워크 주소 변환)이고 다른 하나는 클라이언트 IP 주소를 **ESG** IP 주소와 교환하기 위한 **SNAT**(소스 네트워크 주소 변환)입니다.

그런 다음 **ESG** 서버는 로드 밸런싱된 서버로 트래픽을 전송하며, 로드 밸런싱된 서버는 응답을 **ESG**로 보낸 후 클라이언트로 다시 보냅니다. 이 옵션은 인라인 모드보다 구성하기가 훨씬 더 쉽지만 두 가지 잠재적인 문제가 있습니다. 첫째는 이 모드에는 전용 **ESG** 서버가 필요하다는 것이고 둘째는 로드 밸런서 서버가 원래 클라이언트 IP 주소를 알지 못한다는 것입니다. **HTTP/HTTPS** 애플리케이션에 대한 한 가지 해결 방법은 클라이언트 IP 주소가 요청의 **X-Forwarded-For** HTTP 헤더를 통해 백엔드 서버로 전달되도록 **HTTP** 애플리케이션 프로파일에서 **[X-Forwarded-Forheader 삽입]**을 사용하도록 설정하는 것입니다.

HTTP/HTTPS 이외의 애플리케이션에 대한 백엔드 서버에 클라이언트 IP 주소 가시성이 필요한 경우 IP 풀을 투명하게 구성할 수 있습니다. 클라이언트가 백엔드 서버와 동일한 서브넷에 있지 않은 경우 인라인 모드가 권장됩니다. 그렇지 않은 경우 백엔드 서버의 기본 게이트웨이로 로드 밸런서 IP 주소를 사용해야 합니다.

참고 일반적으로 연결 무결성을 보장하는 방법에는 다음 세 가지가 있습니다.

- 인라인/투명 모드
- **SNAT/프록시/비투명 모드**(위에 설명됨)
- **DSR(직접 서버 반환)** - 현재 지원되지 않습니다.

DSR 모드에서 백엔드 서버는 클라이언트에 직접 응답합니다. 현재 **NSX** 로드 밸런서는 **DSR**을 지원하지 않습니다.

절차

- 1 예를 들어 **SSL** 오프로드를 사용하여 단일 암 가상 서버를 구성해보겠습니다. **Edge**를 두 번 클릭한 다음 **관리 > 설정 > 인증서(Manage > Settings > Certificate)**를 선택하여 인증서를 생성합니다.

2 관리 > 로드 밸런서 > 글로벌 구성 > 편집(Manage > Load Balancer > Global Configuration > Edit)

을 선택하여 로드 밸런서 서비스를 사용하도록 설정합니다.

Edit Load balancer global configuration

☒ Enable Load Balancer

☐ Enable Acceleration

☐ Logging

Log Level: **Info** ▼

☐ Enable Service Insertion

Service Definition:

Service Configuration:

Deployment Specification:

3 관리 > 로드 밸런서 > 애플리케이션 프로파일(Manage > Load Balancer > Application Profiles)

을 선택하여 HTTPS 애플리케이션 프로파일을 생성합니다.

New Profile ?

Name:

Type: **HTTPS** ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: **None** ▼

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica... Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

참고 위의 스크린샷은 문서 용도로만 자체 서명된 인증서를 사용합니다.

4 필요한 경우 관리 > 로드 밸런서 > 서비스 모니터링(Manage > Load Balancer > Service Monitoring)

을 클릭하고 기본 서비스 모니터링을 편집하여 기본 HTTP/HTTPS에서 특정 URL/URI로 변경합니다.

5 관리 > 로드 밸런서 > 풀(Manage > Load Balancer > Pools)을 선택하여 서버 풀을 생성합니다.

SNAT 모드를 사용하려면 풀 구성에서 **투명(Transparent)** 확인란을 선택 취소된 상태로 둡니다.

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☐ Transparent

OK Cancel

VM이 나열되고 사용되도록 설정되어 있는지 확인합니다.

6 필요한 경우 관리 > 로드 밸런서 > 풀 > 풀 통계 표시(Manage > Load Balancer > Pools > Show Pool Statistics)를 클릭하여 상태를 확인합니다.

멤버 상태가 [UP]인지 확인합니다.

7 관리 > 로드 밸런서 > 가상 서버(Manage > Load Balancer > Virtual Servers)를 선택하여 가상 서버를 생성합니다.

UDP 또는 고성능 TCP에 대해 L4 로드 밸런서를 사용하려면 **가속 사용(Enable Acceleration)**을 선택합니다. **가속 사용(Enable Acceleration)**을 선택하는 경우 L4 SNAT에서 방화벽이 필요하므로 로드 밸런서 NSX Edge에서 방화벽 상태가 **사용(Enabled)**인지 확인합니다.

The screenshot shows the 'General' tab of the 'Virtual Server' configuration window. The 'Enable Virtual Server' checkbox is checked. Other settings include: Application Profile: OneArmWeb-01, Name: Web-Tier-VIP-01, IP Address: 172.16.10.10, Protocol: HTTPS, Port: 443, Default Pool: Web-Tier-Pool-01, Connection Limit: 0, and Connection Rate Limit: 0 (CPS).

IP 주소가 서버 풀에 연결되어 있는지 확인합니다.

- 8 필요한 경우 애플리케이션 규칙을 사용하고 있으면 **관리 > 로드 밸런서 > 애플리케이션 규칙(Manage > Load Balancer > Application Rules)**에서 구성을 확인합니다.

The screenshot shows the 'Add Application Rule' dialog box. The 'Name' field is 'App-Rule-1'. The 'Script' field contains the following text: '# A sample application rule to log the name of the virtual server' and 'capture request header Host len 32'.

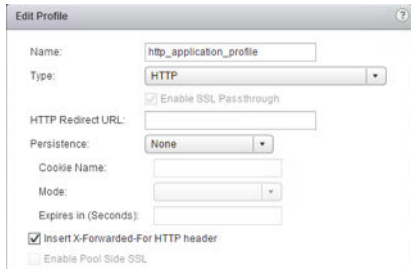
- 9 애플리케이션 규칙을 사용하는 경우 **관리 > 로드 밸런서 > 가상 서버 > 고급(Manage > Load Balancer > Virtual Servers > Advanced)**에서 애플리케이션 규칙이 가상 서버에 연결되어 있는지 확인합니다.

지원되는 예제를 보려면 <https://communities.vmware.com/docs/DOC-31772>를 참조하십시오.

The screenshot shows the 'Advanced' tab of the 'Edit Virtual Server' dialog box. The 'Application Rules' section displays a table with one rule:

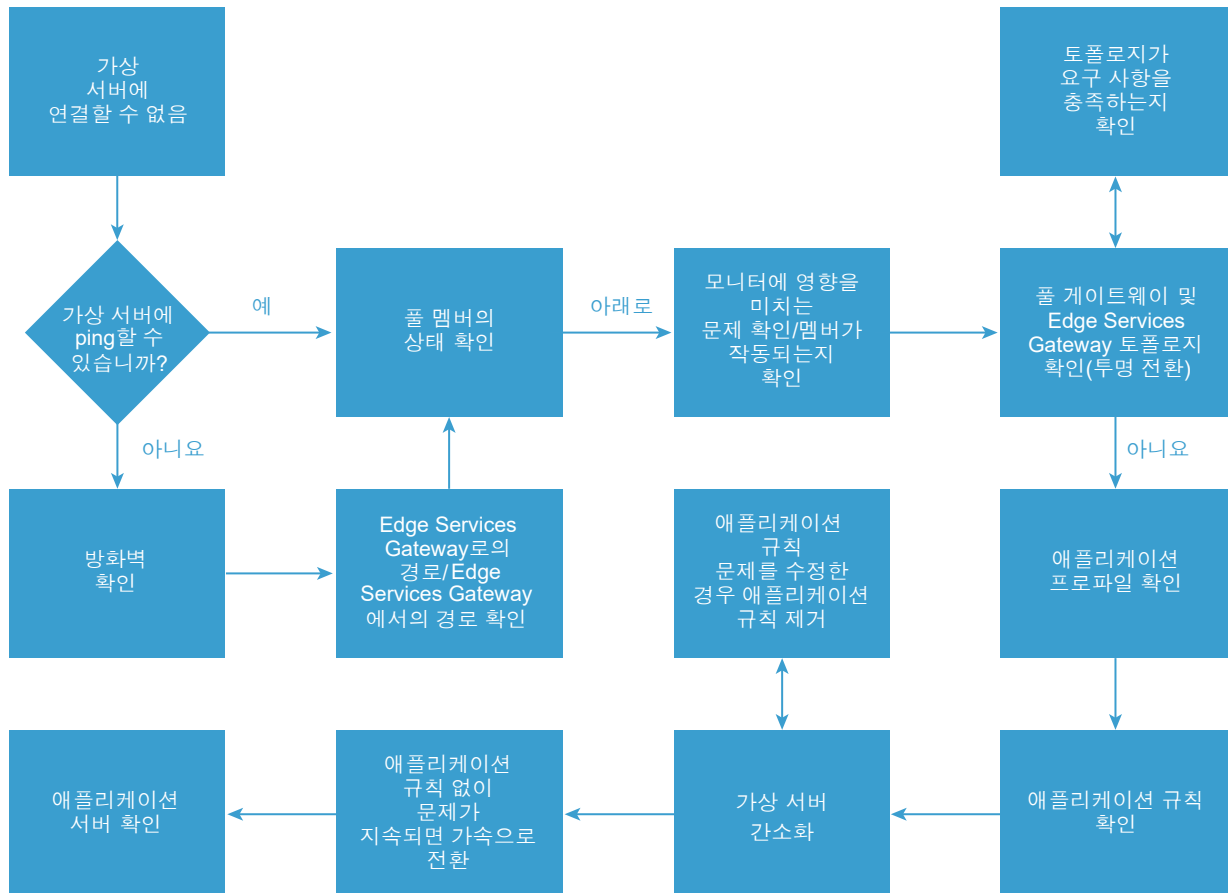
Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

비투명 모드에서 백엔드 서버는 클라이언트 IP를 볼 수 없으나 로드 밸런서 내부 IP 주소를 볼 수 있습니다. HTTP/HTTPS 트래픽에 대한 해결 방법으로 **X-Forwarded-For HTTP 헤더 삽입(Insert X-Forwarded-For HTTP header)**을 선택합니다. 이 옵션을 선택하면 Edge 로드 밸런서는 클라이언트 소스 IP 주소 값과 함께 "X-Forwarded-For" 헤더를 추가합니다.



로드 밸런서에 대한 문제 해결 순서도

다음 순서도는 로드 밸런서 문제 해결 방법에 대한 개요를 보여줍니다.



UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결

vSphere Web Client를 통해 로드 밸런서 구성을 확인할 수 있습니다. UI를 사용하여 일부 로드 밸런서 문제를 해결할 수 있습니다.

작동하는 기능을 이해하고 문제를 정의한 후에 다음과 같이 UI를 통해 구성을 확인합니다.

사전 요구 사항

다음 세부 정보를 적어 두십시오.

- 가상 서버의 IP, 프로토콜 및 포트.
- 백엔드 애플리케이션 서버의 IP 및 포트.
- 의도한 토폴로지(인라인 또는 단일 암). 자세한 내용은 "NSX 관리 가이드"에서 논리적 로드 밸런서 항목을 참조하십시오.
- 추적 경로를 확인하고 다른 네트워크 연결 도구를 사용하여 패킷이 올바른 위치(Edge Services Gateway)로 이동되는지 확인합니다.
- 업스트림 방화벽이 트래픽을 올바르게 허용하는지 확인합니다.
- 발생한 문제를 정의합니다. 예를 들어 가상 서버에 대한 DNS 레코드는 올바르지만 콘텐츠가 반환되지 않거나 잘못된 콘텐츠가 반환됩니다.

문제

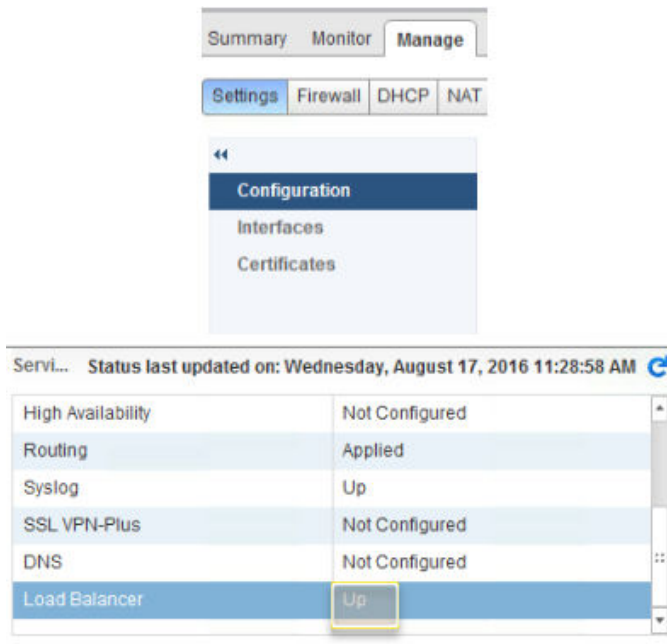
로드 밸런서가 예상대로 작동하지 않습니다.

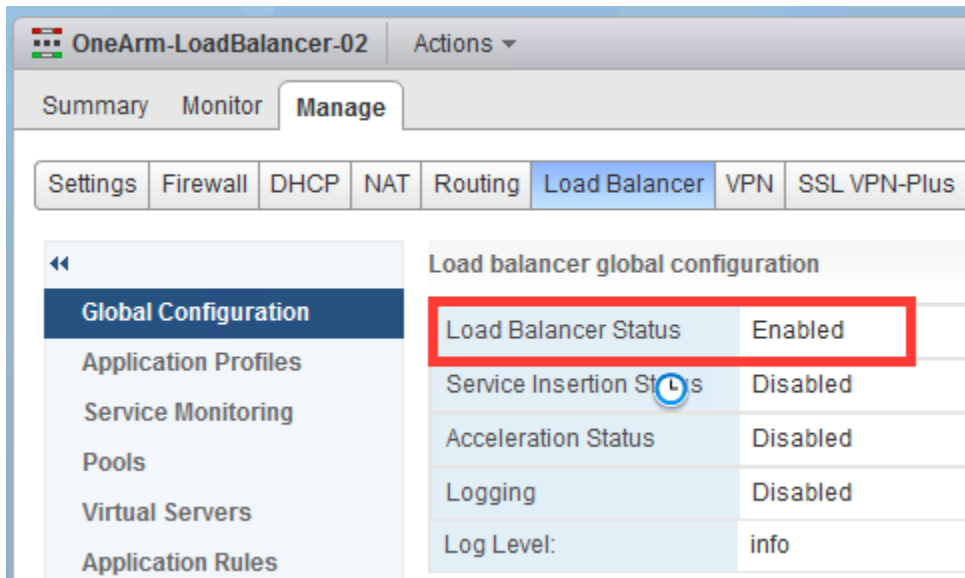
해결책

- 1 다음 애플리케이션 요구 사항을 확인합니다. 즉, 로드 밸런서에서 지원되어야 하는 프로토콜(TCP, UDP, HTTP, HTTPS), 포트, 지속성 요구 사항 및 풀 멤버를 확인해야 합니다.
 - 로드 밸런서 및 방화벽이 사용되도록 설정되어 있고 Edge Services Gateway에 적절한 경로가 있습니까?
 - 가상 서버가 수신하는 IP 주소, 포트 및 프로토콜은 무엇입니까?
 - SSL 오프로드가 사용되고 있습니까? 백엔드 서버와 통신할 때 SSL을 사용해야 합니까?
 - 애플리케이션 규칙을 사용하고 있습니까?
 - 토폴로지란 무엇입니까? NSX 로드 밸런서는 클라이언트 및 서버의 모든 트래픽을 구문 분석해야 합니다.
 - NSX 로드 밸런서가 인라인이거나 반환 트래픽이 로드 밸런서로 다시 이동하도록 클라이언트 소스 주소가 변환됩니까?

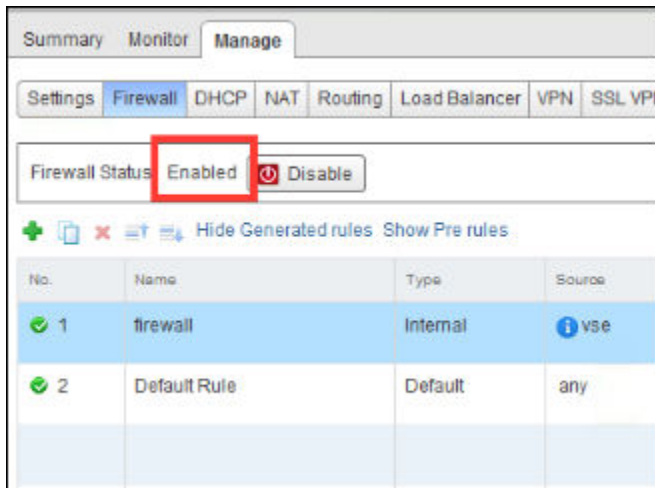
2 NSX Edge로 이동하고 로드 밸런싱을 사용하도록 설정하는 데 필요한 구성을 확인한 후 다음과 같이 트래픽이 흐르도록 합니다.

a 로드 밸런서가 **작동(Up)**으로 표시되는지 확인합니다.





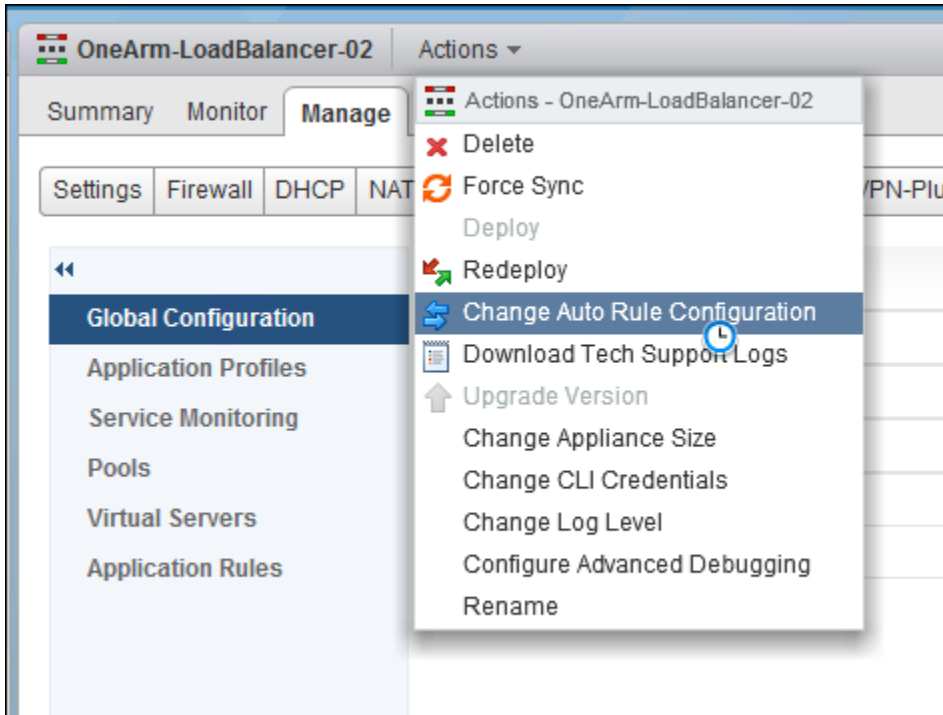
- b 방화벽이 **사용(Enabled)**인지 확인합니다. 가속 가상 서버를 위해서는 방화벽을 사용하도록 설정해야 합니다. 비가속 TCP 및 L7 HTTP/HTTPS VIP에는 트래픽을 허용하는 정책이 있어야 합니다. 방화벽 필터는 가속 가상 서버에 영향을 미치지 않습니다.



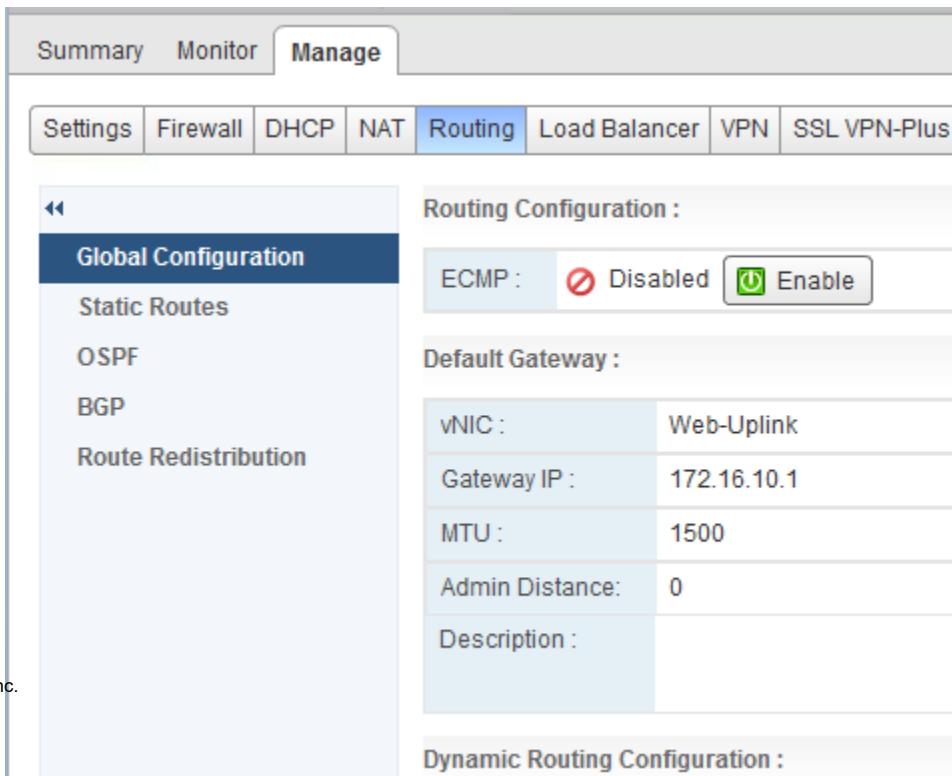
- c 가상 서버에 대해 NAT 규칙이 생성되는지 확인합니다. NAT 탭에서 **내부 규칙 숨기기(Hide internal rules)** 또는 **내부 규칙 숨기기 취소(Unhide internal rules)** 링크를 클릭하여 확인합니다.

참고 로드 밸런싱을 사용하도록 설정하고 서비스를 구성했으나 NAT 규칙을 구성하지 않은 경우 자동 규칙 구성이 사용되도록 설정되지 않은 것입니다.

- d 자동 규칙 구성을 변경할 수 있습니다. 자세한 내용은 "NSX 관리 가이드"에서 "자동 규칙 구성 변경" 항목을 참조하십시오. NSX Edge Services Gateway가 배포되면 자동 규칙 구성을 구성하는 옵션이 제공됩니다. Edge Services Gateway를 배포하는 동안 이 옵션을 선택하지 않은 경우 사용하도록 설정해야 로드 밸런서가 제대로 작동합니다. UI를 통해 풀 멤버 상태를 확인합니다.



- e 라우팅을 확인하고, Edge Service Gateway에 클라이언트 시스템 및 백엔드 서버에 대한 기본 경로 또는 정적 경로가 있는지 확인합니다. 서버에 대한 경로가 없으면 상태 검사가 실패합니다. 동적 라우팅 프로토콜을 사용하는 경우 CLI를 사용해야 할 수 있습니다. 자세한 내용은 [NSX 라우팅 CLI](#)를 참조하십시오.
- a 기본 경로를 확인합니다.



는 경로입니다. 대부분 애플리케이션 서버는 이러한 서버에 연결됩니다.

⚙️ 0 Job(s) In Progress
❗ 0 Job(s) Failed

aces of this NSX Edge.

⚙️ Actions

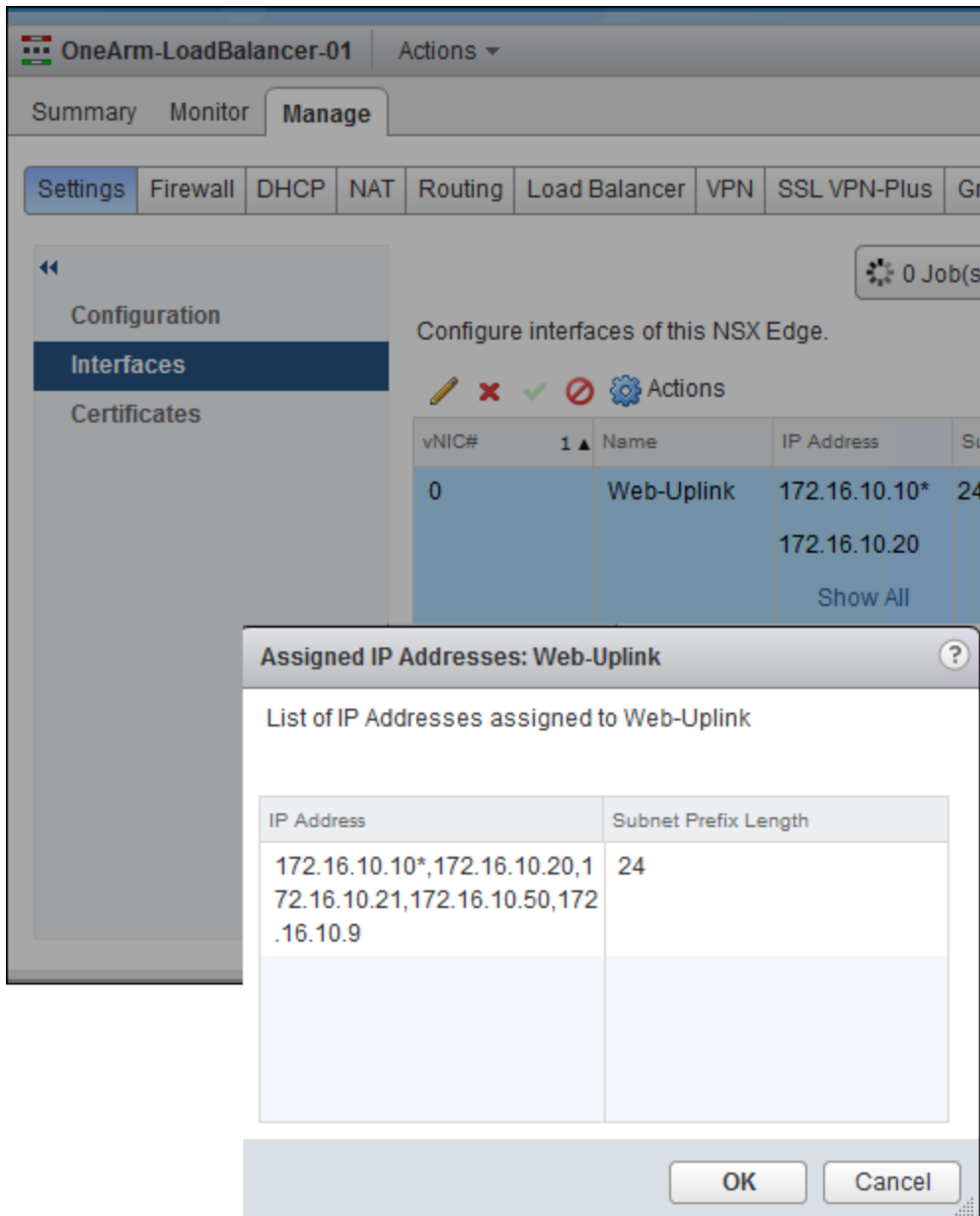
🔍 Filter

Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
Web-Uplink	172.16.10.10*	24	Web-Tier-01	Uplink	✓
	172.16.10.20				
	Show All				
INLINE_SUBNI	172.16.100.1*	24	INLINE_SUBNI	Internal	✓
vnic2				Internal	❌
vnic3				Internal	❌
vnic4				Internal	❌
vnic5				Internal	❌

- c 라우팅(Routing) 탭 > 정적 경로(Static Routes)에서 정적 경로를 확인합니다.

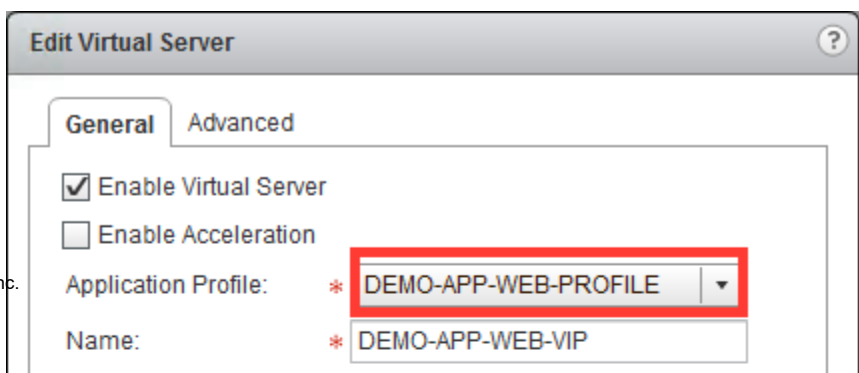
3 가상 서버의 IP 주소, 포트 및 프로토콜을 확인합니다.

- a NSX Edge를 두 번 클릭하고 **관리(Manage) > 설정(Settings)> 인터페이스(Interfaces)**로 이동합니다. 가상 서버의 IP 주소가 인터페이스에 추가되었는지 확인합니다.



- b 가상 서버에 애플리케이션을 지원하도록 구성된 적절한 IP 주소, 포트 및 프로토콜이 있는지 확인합니다.

- a 가상 서버에 사용되는 애플리케이션 프로파일을 확인합니다.



을 확인합니다.

Edit Virtual Server

General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * DEMO-APP-WEB-PROFILE ▼

Name: * DEMO-APP-WEB-VIP

Description:

IP Address: * 172.16.10.20 ✕ Select IP Address

Protocol: HTTPS ▼

Port: * 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

OK Cancel

- c 애플리케이션 프로파일에서 지원되는 지속성 방법, 유형(프로토콜) 및 SSL(필요한 경우)을 충족하는지 확인합니다. SSL을 사용하는 경우 올바른 이름 및 만료 날짜의 인증서를 사용하고 있는지 확인합니다.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- d 클라이언트가 연결하기 위한 올바른 인증서가 사용되는지 확인합니다.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☒ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.COF	DEMO.WEB.APP.COF	Wed Apr 27 2016 - Sa
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Th
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- e 클라이언트 인증서가 필요하지만 클라이언트가 구성되어 있지 않은지 확인합니다. 또한 좁은 암호 목록을 선택한 경우 암호 목록이 너무 좁은지 확인합니다(예: 이전 브라우저를 사용하는 클라이언트).

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- f 백엔드 서버에 대한 SSL이 필요한지 확인합니다.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

4 다음과 같이 풀 상태 및 구성을 확인합니다.

- a 풀 상태를 확인합니다. 하나 이상의 멤버가 트래픽을 제공할 수 있도록 작동 상태여야 하지만 한 멤버가 모든 트래픽을 제공하는 데 충분하지 않을 수 있습니다. 0개 또는 제한된 수의 풀 멤버가 작동 상태인 경우 다음 단계에 설명된 대로 문제를 수정해보십시오.

Pool ID

Name

Status

pool-1

TENANT-1-TCP-P...

UP

</

- b 토폴로지가 올바른지 확인합니다. SNAT 클라이언트 트래픽은 풀 구성에서 제어됩니다. 로드 밸런서 함수를 호스팅하는 Edge Services Gateway가 인라인이 아니어서 모든 트래픽을 볼 수는 없는 경우 실패합니다. 클라이언트 소스의 IP를 유지하려면 **투명(Transparent)** 모드를 선택합니다. 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

Edit Pool

Name:

* DEMO_APP_WEB_POOL

Description:

Algorithm:

ROUND-ROBIN ▼

Algorithm Parameters:

Monitors:

default_http_monitor ▼

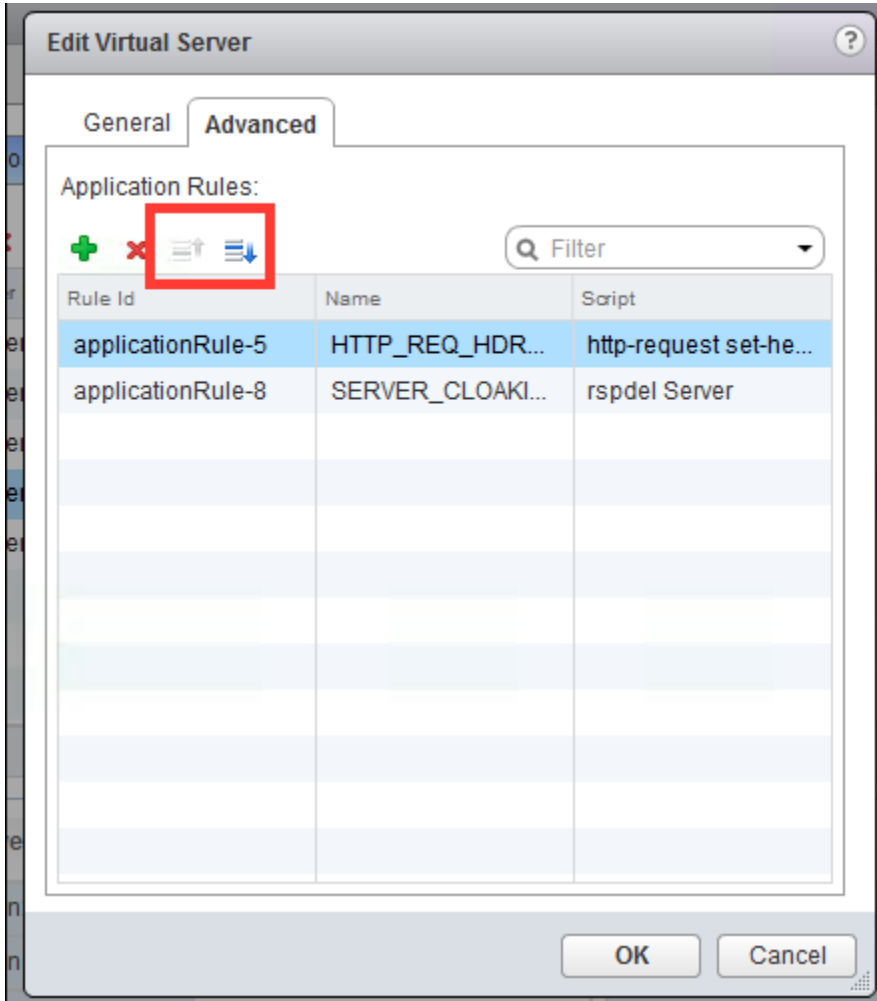
Members:

+

×

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	M C

- 5 애플리케이션 규칙을 사용하는 경우 규칙을 확인합니다. 필요한 경우 규칙을 제거하여 트래픽이 흐르는지 확인합니다.
- a 규칙 순서를 바꾸어 규칙 순서로 인해 논리가 트래픽 흐름을 중단시키는지 확인합니다. 애플리케이션 규칙을 추가하고 애플리케이션 규칙 예를 보는 방법에 대한 자세한 내용은 "NSX 관리 가이드"의 "애플리케이션 규칙 추가" 항목을 참조하십시오.



다음에 수행할 작업

문제를 찾을 수 없으면 CLI(명령줄 인터페이스)를 사용하여 발생하는 현상을 확인할 수 있습니다. 자세한 내용은 [CLI를 사용하여 로드 밸런서 문제 해결](#)를 참조하십시오.

CLI를 사용하여 로드 밸런서 문제 해결

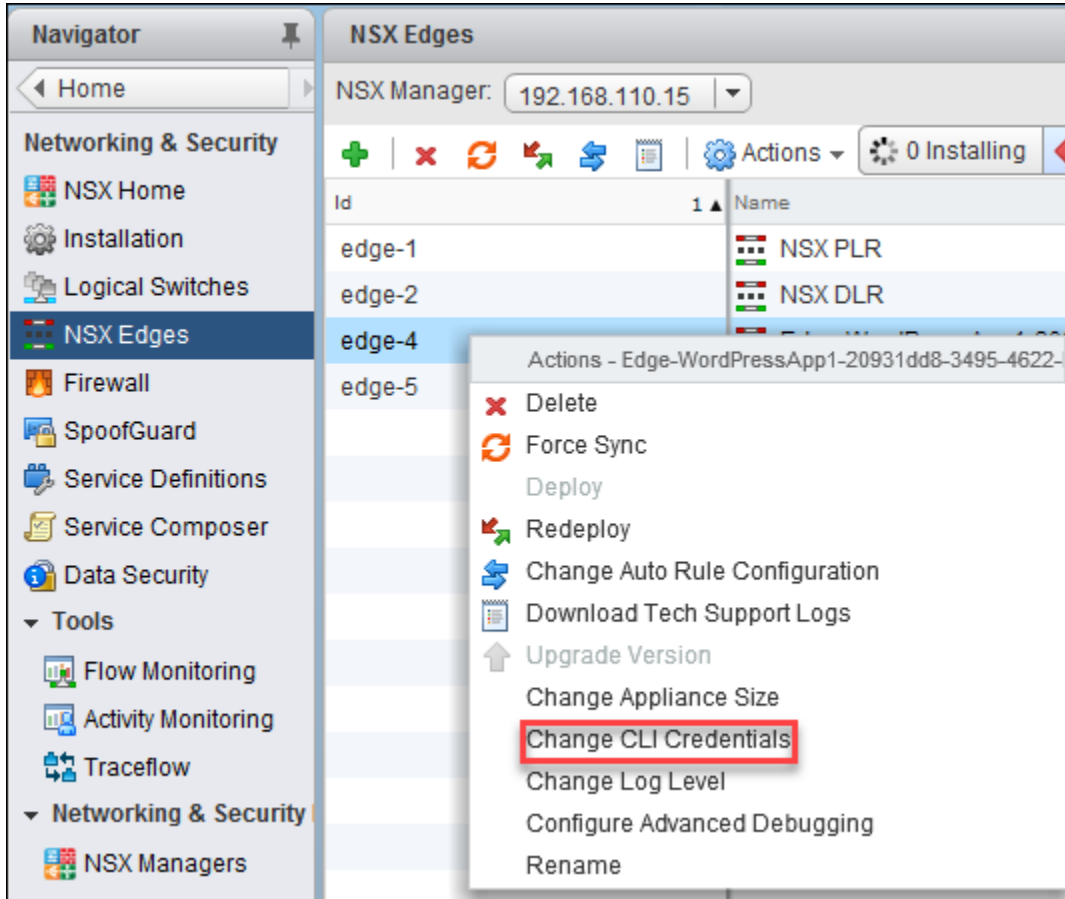
NSX CLI를 사용하여 자세한 비상 로그를 가져오고, 패킷 캡처를 수행하고, 로드 밸런서 문제 해결을 위한 메트릭을 확인할 수 있습니다.

문제

로드 밸런싱이 예상대로 진행되지 않습니다.

해결책

- 1 사용하도록 설정하거나 가상 장치에 대해 SSH를 수행할 수 있는지 확인합니다. Edge Services Gateway는 배포 중에 SSH를 사용하도록 설정하기 위한 옵션이 있는 가상 장치입니다. SSH를 사용하도록 설정해야 하는 경우 필요한 장치를 선택하고 **작업(Actions)** 메뉴에서 **CLI 자격 증명 변경(Change CLI Credentials)**을 클릭합니다.



- 2 Edge Services Gateway에는 런타임 상태 및 구성 상태를 확인하기 위한 몇 가지 **show** 명령이 있습니다. 명령을 사용하여 구성 및 통계 정보를 표시합니다.

```
nsxedge> show configuration loadbalancer
nsxedge> show configuration loadbalancer virtual [virtual-server-name]
nsxedge> show configuration loadbalancer pool [pool-name]
nsxedge> show configuration loadbalancer monitor [monitor-name]
nsxedge> show configuration loadbalancer profile [profile-name]
nsxedge> show configuration loadbalancer rule [rule-name]
```

- 3 로드 밸런싱 및 NAT가 제대로 작동하려면 방화벽을 사용하도록 설정해야 합니다. #show firewall 명령을 사용합니다. 명령을 사용하여 의미 있는 출력을 얻지 못할 경우 [UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결](#) 섹션을 참조하십시오.

```

NSX-edge-8-0> show firewall
Chain PREROUTING (policy ACCEPT 21947 packets, 7809K bytes)
:~id      pkts bytes target     prot opt in     out     source      destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
:~id      pkts bytes target     prot opt in     out     source      destination
)        348 67915 ACCEPT     all  --  lo      *        0.0.0.0/0    0.0.0.0/0
)        134  5360 DROP       all  --  *      *        0.0.0.0/0    0.0.0.0/0    state INVALID
)        21482 7736K block_in all  --  *      *        0.0.0.0/0    0.0.0.0/0
)        20545 7671K ACCEPT   all  --  *      *        0.0.0.0/0    0.0.0.0/0    state RELATED
)         937 65139 usr_rules all  --  *      *        0.0.0.0/0    0.0.0.0/0
)          0      0 DROP      all  --  *      *        0.0.0.0/0    0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
:~id      pkts bytes target     prot opt in     out     source      destination

Chain OUTPUT (policy ACCEPT 20673 packets, 1248K bytes)
:~id      pkts bytes target     prot opt in     out     source      destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
:~id      pkts bytes target     prot opt in     out     source      destination
)        348 67915 ACCEPT     all  --  *      lo      0.0.0.0/0    0.0.0.0/0
)         34  1360 DROP       all  --  *      *        0.0.0.0/0    0.0.0.0/0    state INVALID
)        20295 1179K block_out all  --  *      *        0.0.0.0/0    0.0.0.0/0
)          0      0 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)          0      0 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)          0      0 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)          0      0 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)        14599 802K ACCEPT   all  --  *      *        0.0.0.0/0    0.0.0.0/0    state RELATED
)         5696 377K usr_rules all  --  *      *        0.0.0.0/0    0.0.0.0/0
)          0      0 DROP      all  --  *      *        0.0.0.0/0    0.0.0.0/0

Chain block_in (1 references)
:~id      pkts bytes target     prot opt in     out     source      destination

Chain block_out (1 references)
:~id      pkts bytes target     prot opt in     out     source      destination

Chain usr_rules (2 references)
:~id      pkts bytes target     prot opt in     out     source      destination
l33137  4861  333K ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    match-set 0_
l33138      0      0 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    match-set 1_
l33139   936 65099 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    match-set 2_
l33141   835 43459 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0    match-set 3_
l33131      1      40 LOG        all  --  *      *        0.0.0.0/0    0.0.0.0/0    LOG flags 0
l33131      1      40 ACCEPT     all  --  *      *        0.0.0.0/0    0.0.0.0/0

```


- 4 로드 밸런서가 제대로 작동하려면 NAT가 필요합니다. `show nat` 명령을 사용합니다. 명령을 사용하여 의미 있는 출력을 얻지 못할 경우 [UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결](#) 섹션을 참조하십시오.

```

NSX-edge-8-0> show nat
Chain PREROUTING (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target     prot opt in     out     source      destination
0      568 40044 int_dnat  all  --  *      *       0.0.0.0/0    0.0.0.0/0
0      568 40044 usr_dnat  all  --  *      *       0.0.0.0/0    0.0.0.0/0

Chain INPUT (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target     prot opt in     out     source      destination

Chain OUTPUT (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target     prot opt in     out     source      destination
0      896 46706 int_dnat  all  --  *      *       0.0.0.0/0    0.0.0.0/0
0      896 46706 usr_dnat  all  --  *      *       0.0.0.0/0    0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target     prot opt in     out     source      destination
0      896 46706 int_snat  all  --  *      *       0.0.0.0/0    0.0.0.0/0
0      896 46706 usr_snat  all  --  *      *       0.0.0.0/0    0.0.0.0/0

Chain int_dnat (2 references)
rid  pkts bytes target     prot opt in     out     source      destination

Chain int_snat (1 references)
rid  pkts bytes target     prot opt in     out     source      destination
0      0      0 ACCEPT    all  --  *      *       0.0.0.0/0    0.0.0.0/0

Chain usr_dnat (2 references)
rid  pkts bytes target     prot opt in     out     source      destination
0      0      0 DNAT      tcp  --  vNic_2 *       0.0.0.0/0    192.168.8.20
0      0      0 LOG       all  --  vNic_2 *       0.0.0.0/0    192.168.8.11
0      0      0 DNAT      all  --  vNic_2 *       0.0.0.0/0    192.168.8.11

Chain usr_snat (1 references)
rid  pkts bytes target     prot opt in     out     source      destination
0      0      0 LOG       all  --  *      vNic_2 10.10.10.101 0.0.0.0/0
0      0      0 SNAT      all  --  *      vNic_2 10.10.10.101 0.0.0.0/0
0      0      0 LOG       all  --  *      vNic_2 10.10.10.0/24 0.0.0.0/0
0      0      0 SNAT      all  --  *      vNic_2 10.10.10.0/24 0.0.0.0/0
NSX-edge-8-0>

```

- 5 방화벽이 사용되도록 설정되고 로드 밸런서에 NAT 규칙이 지정되는 것 외에도, 로드 밸런싱 프로세스를 사용하도록 설정해야 합니다. `show service loadbalancer` 명령을 사용하여 로드 밸런서 엔진 상태(L4/L7)를 확인합니다.

```

nsxedge> show service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer    : running
-----
L7 Loadbalancer Statistics:
STATUS    PID      MAX_MEM_MB  MAX SOCK  MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE
CONN_RATE_LIMIT  MAX_CONN_RATE

```

```

running    1580      0      2081    1024      0      0      0
0          0

-----
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0

Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn

```

- a `show service loadbalancer session` 명령을 사용하여 로드 밸런서 세션 테이블을 확인합니다. 시스템에 트래픽이 있으면 세션이 표시됩니다.

```

nsxedge> show service loadbalancer session

-----
L7 Loadbalancer Statistics:
STATUS     PID      MAX_MEM_MB MAX SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running    1580      0      2081    1024      0          0          0
0          0

-----L7 Loadbalancer Current Sessions:

0x2192df1f300: proto=unix_stream src=unix:1 fe=GLOBAL be=<NONE> srv=<none> ts=09 age=0s
calls=2 rq[f=c08200h,
i=0,an=00h,rx=20s,wx=,ax=] rp[f=008000h,i=0,an=00h,rx=,wx=,ax=] s0=[7,8h,fd=1,ex=]
s1=[7,0h,fd=-1,ex=] exp=19s

-----
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0

L4 Loadbalancer Current Sessions:

pro expire state      source      virtual      destination

```

- b `show service loadbalancer` 명령을 사용하여 로드 밸런서 계층 7 고정 테이블 상태를 확인합니다. 이 테이블에는 가속 가상 서버에 대한 정보는 표시되지 않습니다.

```

nsxedge> show service loadbalancer table

-----
L7 Loadbalancer Sticky Table Status:

TABLE     TYPE     SIZE(BYTE)  USED(BYTE)

```

- 6 모든 필수 서비스가 제대로 실행되는 경우 라우팅 테이블을 확인하고 클라이언트 및 서버에 대한 경로가 있어야 합니다. 경로를 인터페이스에 매핑하는 `show ip route` 및 `show ip forwarding` 명령을 사용합니다.

```

NSX-edge-8-0> sh ip route

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

Total number of routes: 4

S      0.0.0.0/0          [1/1]          via 192.168.8.2
C      10.10.10.0/24      [0/0]          via 10.10.10.1
C      169.254.1.4/30     [0/0]          via 169.254.1.5
C      192.168.8.0/24     [0/0]          via 192.168.8.3
NSX-edge-8-0> sh ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route

R>* 0.0.0.0/0 via 192.168.8.2, vNic_2
C>* 10.10.10.0/24 is directly connected, vNic_0
C>* 169.254.1.4/30 is directly connected, vNic_0
C>* 192.168.8.0/24 is directly connected, vNic_2
NSX-edge-8-0>

```

- 7 `show arp` 명령을 사용하여 시스템에 대한 ARP 항목(예: 게이트웨이 또는 다음 홉)과 백엔드 서버가 있는지 확인합니다.

```

OneArm-LoadBalancer-01-0> show arp
-----
vShield Edge ARP Cache:
IP Address                Interface  MAC Address  State
fe80::250:56ff:feae:f86b  vNic_0    00:50:56:ae:f8:6b  STALE
fe80::250:56ff:feae:5066  vNic_1    00:50:56:ae:50:66  STALE
fe80::250:56ff:feae:3e3d  vNic_0    00:50:56:ae:3e:3d  STALE
172.16.100.11             vNic_1    00:50:56:ae:50:66  REACHABLE
172.16.10.1               vNic_0    02:50:56:56:44:52  REACHABLE
172.16.10.11             vNic_0    00:50:56:ae:3e:3d  REACHABLE
OneArm-LoadBalancer-01-0>

```

- 8 로그에는 문제를 진단하는 데 도움이 될 수 있는 트래픽을 찾기 위한 정보가 제공됩니다. `show log` 또는 `show log follow` 명령을 사용하여 트래픽을 찾는 데 도움이 되는 로그에 태그를 지정합니다. **로깅(Logging)**을 사용하도록 설정하고 **정보(Info)** 또는 **디버그(Debug)**로 설정한 상태로 로드 밸런서를 실행하고 있는지 확인합니다.

```

nsxedge> show log
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuacct
...

```

- 9 기본 서비스가 클라이언트에 대한 적절한 경로로 실행되고 있음을 확인했으므로 애플리케이션 계층에서 진행되는 상황을 살펴보겠습니다. **show service loadbalancer pool** 명령을 사용하여 로드 밸런서 풀 상태(L4/L7)를 확인합니다. 하나 이상의 멤버가 콘텐츠를 제공할 수 있도록 작동 상태여야 합니다. 일반적으로 요청 볼륨이 단일 워크로드의 용량을 초과하므로 둘 이상의 멤버가 필요합니다. 기본 제공 상태 검사가 상태 모니터를 제공하는 경우 상태 검사가 실패할 때 출력에 마지막 상태 변경 시간 및 실패 원인도 표시됩니다. 모니터 서비스에서 상태 모니터를 제공하는 경우 위의 두 가지 출력 외에 마지막 확인 시간도 표시됩니다.

```
nsxedge> show service loadbalancer pool

-----
Loadbalancer Pool Statistics:

POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
```

- 10 서비스 모니터 상태(정상, 경고, 주의)를 확인하여 구성된 모든 백엔드 서버의 상태를 알아봅니다.

```
nsxedge> show service loadbalancer monitor

-----
Loadbalancer Health Check Statistics:

MONITOR PROVIDER    POOL          MEMBER        HEALTH STATUS
built-in            Web-Tier-Pool-01  web-01a      default_https_monitor:L7OK
built-in            Web-Tier-Pool-01  web-02a      default_https_monitor:L7OK
```

show service load balancer monitor 명령의 경우 다음 세 가지 유형의 상태 모니터 값이 CLI 출력에 표시됩니다.

- 기본 제공: 상태 점검이 사용되도록 설정되고 L7 엔진(HA 프록시)에 의해 수행됩니다.
- 모니터 서비스: 상태 점검이 사용되도록 설정되고 모니터 서비스 엔진(NAGIOS)에 의해 수행됩니다. 모니터 서비스 실행 상태는 **show service monitor** 및 **show service monitor service** CLI 명령을 사용하여 확인할 수 있습니다. **상태(Status)** 필드는 정상, 주의 또는 위험일 수 있습니다.
- 정의되지 않음: 상태 점검이 사용되지 않도록 설정됩니다.

출력의 마지막 열은 폴 멤버의 상태입니다. 다음 상태가 표시됩니다.

표 6-1. 상태 및 설명

상태	설명
기본 제공	<ul style="list-style-type: none"> ■ UNK: 알 수 없음 ■ INI: 초기화 중 ■ SOCKERR: 소켓 오류 ■ L4OK: 계층 4에서 검사 통과. 상위 계층 테스트를 사용하도록 설정되지 않음 ■ L4TOUT: 계층 1~4 시간 초과 ■ L4CON: 계층 1~4 연결 문제. 예: "연결이 거부됨"(tcp rst) 또는 "호스트에 대한 경로 없음"(icmp) ■ L6OK: 계층 6에서 검사 통과 ■ L6TOUT: 계층 6(SSL) 시간 초과 ■ L6RSP: 계층 6 잘못된 응답 - 프로토콜 오류. 발생 가능한 원인은 다음과 같습니다. <ul style="list-style-type: none"> ■ 백엔드 서버가 "SSLv3" 또는 "TLSv1.0"만 지원하는 경우 ■ 백엔드 서버의 인증서가 올바르지 않은 경우 ■ 암호 협상에 실패하는 경우 ■ L7OK: 계층 7에서 검사 통과 ■ L7OKC: 계층 7에서 조건부로 검사 통과. 예: disable-on-404 상태의 404 ■ L7TOUT: 계층 7(HTTP/SMTP) 시간 초과 ■ L7RSP: 계층 7 잘못된 응답 - 프로토콜 오류 ■ L7STS: 계층 7 응답 오류. 예: HTTP 5xx
위험	<ul style="list-style-type: none"> ■ SSL 프로토콜 버전 2가 SSL 라이브러리에서 지원되지 않음 ■ 지원되지 않는 SSL 프로토콜 버전 ■ SSL 컨텍스트를 만들 수 없음 ■ SSL 연결을 만들 수 없음 ■ SSL 핸드셰이크를 시작할 수 없음 ■ 서버 인증서를 검색할 수 없음 ■ 인증서 주체를 검색할 수 없음 ■ 인증서의 잘못된 시간 형식 ■ 인증서 '<cn>'이(가) <expire time of certificate>에 만료됨 ■ 인증서 '<cn>'이(가) 오늘 <expire time of certificate>에 만료됨
주의/위험	인증서 '<cn>'이(가) <days_left/expire time of certificate>일 후에 만료됨

표 6-1. 상태 및 설명 (계속)

상태	설명
ICMP	<ul style="list-style-type: none"> ■ 네트워크에 연결할 수 없음 ■ 호스트에 연결할 수 없음 ■ 프로토콜에 연결할 수 없음 ■ 포트에 연결할 수 없음 ■ 소스 경로 실패 ■ 소스 호스트가 분리됨 ■ 알 수 없는 네트워크 ■ 알 수 없는 호스트 ■ 네트워크가 거부됨 ■ 호스트가 거부됨 ■ 네트워크에 대한 잘못된 ToS(서비스 유형) ■ 호스트에 대한 잘못된 ToS(서비스 유형) ■ 필터로 금지됨 ■ 호스트 우선 순위 위반 ■ 우선 순위 구분. 작업에 필요한 최소 우선 순위 수준 ■ 잘못된 코드
UDP/TCP	<ul style="list-style-type: none"> ■ 소켓 생성 실패 ■ 주소 xxxx 및 포트 xxx에 연결: [Linux 오류 코드 참조] ■ 호스트에서 데이터가 수신되지 않음 ■ 호스트/소켓의 예기치 않은 응답
HTTP/HTTPS	<ul style="list-style-type: none"> ■ HTTP 알 수 없음: 메모리 할당 오류 ■ HTTP 위험: TCP 소켓을 열 수 없음(소켓 생성 또는 서버 연결 실패) ■ HTTP 위험: 데이터를 수신하는 동안 오류 발생 ■ HTTP 위험: 호스트에서 데이터가 수신되지 않음 ■ HTTP 위험: 호스트에서 잘못된 HTTP 응답을 수신함: <status line>(잘못된 예상 상태 줄 형식) ■ HTTP 위험: 잘못된 상태 줄 <status line>(상태 코드가 3자리 숫자: XXX가 아님) ■ HTTP 위험: 잘못된 상태 <status line>(상태 코드 >= 600 또는 < 100) ■ HTTP 위험: 문자열을 찾을 수 없음 ■ HTTP 위험: 패턴을 찾을 수 없음 ■ HTTP 주의: 페이지 크기 <page_length>이(가) 너무 큼 ■ HTTP 주의: 페이지 크기 <page_length>이(가) 너무 작음

- 11** 오류 코드가 L4TOUT/L4CON인 경우 일반적으로 기본 네트워킹에 연결 문제가 있는 것입니다.

Duplicate IP는 다음 이유가 근본 원인인 경우가 많습니다. 이 오류가 발생하면 다음과 같이 문제를 해결합니다.

- a 두 Edge에서 **show service highavailability** 명령을 사용하여 HA가 사용되도록 설정될 때 Edge의 HA(고가용성) 상태를 확인합니다. HA 링크가 **DOWN** 상태인지와 모든 Edge가 **Active** 상태인지 그리고 결과적으로 네트워크에 중복된 **Edge IP**가 없는지 확인합니다.
- b **show arp** 명령으로 Edge ARP 테이블을 확인하고, 두 MAC 주소 간에 백엔드 서버의 **ARP** 항목이 변경되는지도 확인합니다.
- c 백엔드 서버 **ARP** 테이블을 확인하거나 **arp-ping** 명령을 사용하고 다른 시스템이 **Edge IP**와 동일한 IP를 갖는지 여부를 확인합니다.

- 12** 로드 밸런서 개체 통계(VIP, 풀, 멤버)를 확인합니다. 특정 풀을 확인하고 멤버가 작동 및 실행되고 있는지 확인합니다. 투명 모드가 사용되도록 설정되어 있는지 확인합니다. 이렇게 설정된 경우 **Edge Services Gateway**가 클라이언트와 서버 간에 인라인 상태여야 합니다. 서버가 세션 카운터 증분을 표시하는지 확인합니다.

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01
```

TIMESTAMP	SESSIONS	BYTESIN	BYTESOUT	SESSIONRATE	HTTPREQS
2016-04-27 19:56:40	00	00	00	00	00
2016-04-27 19:55:00	00	32	100	00	00

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01 | MEMBER
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-1, STATUS: UP
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-2, STATUS: UP
```

- 13** 이제 가상 서버를 확인하고 기본 풀이 있는지와 풀이 바인딩되어 있는지 확인합니다. 애플리케이션 규칙을 통해 풀을 사용하는 경우 **#show service loadbalancer pool** 명령에 표시되는 것처럼 특정 풀을 확인해야 합니다. 가상 서버의 이름을 지정합니다.

```
nsxedge> show service loadbalancer virtual Web-Tier-VIP-01
```

Loadbalancer VirtualServer Statistics:

```
VIRTUAL Web-Tier-VIP-01
| ADDRESS [172.16.10.10]:443
| SESSION (cur, max, total) = (0, 0, 0)
| RATE (cur, max, limit) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
```

```

| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)

```

- 14** 모든 항목이 제대로 구성된 것처럼 보이는데도 여전히 오류가 발생하면 상황을 이해하기 위해 트래픽을 캡처해야 합니다. 두 가지 연결, 즉 클라이언트에서 가상 서버로의 연결과 Edge Services Gateway에서 백엔드 풀로의 연결이 있습니다(풀 수준에서 투명 구성 포함 또는 미포함). **#show ip forwarding** 명령은 vNic 인터페이스를 나열하며 해당 데이터를 사용할 수 있습니다.

예를 들어 클라이언트 컴퓨터가 vNic_0에 있고 서버가 vNic_1에 있다고 가정하고 포트 80에서 실행되는 클라이언트 IP 주소 192.168.1.2와 VIP IP 192.168.2.2를 사용합니다. 로드 밸런서 인터페이스 IP는 192.168.3.1이고 백엔드 서버 IP는 192.168.3.3입니다. 두 개의 다른 패킷 캡처 명령이 있습니다. 하나는 패킷을 표시하지만, 다른 하나는 다운로드할 수 있는 파일에 패킷을 캡처합니다. 패킷을 캡처하여 로드 밸런서 비정상 오류를 감지합니다. 다음 두 방향에서 패킷을 캡처할 수 있습니다.

- 클라이언트에서 패킷을 캡처합니다.
- 백엔드 서버로 전송된 패킷을 캡처합니다.

```

#debug packet capture interface interface-name [filter using _ for space]- creates a packet
capture file that you can download
#debug packet display interface interface-name [filter using _ for space]- outputs packet data to
the console
#debug show files - to see a list of packet capture
#debug copy scp user@url:path file-name/all - to download the packet capture

```

예:

- vNIC_0에 캡처: `debug packet display interface vNic_0`
- 모든 인터페이스에 캡처: `debug packet display interface any`
- 필터를 사용하여 vNIC_0에 캡처: `debug packet display interface vNic_0 host_192.168.11.3_and_host_192.168.11.41`
- 클라이언트에서 가상 서버로의 트래픽 패킷 캡처: `#debug packet display|capture interface vNic_0 host_192.168.1.2_and_host_192.168.2.2_and_port_80`
- 풀이 투명 모드인 경우 Edge Services Gateway와 서버 간 패킷 캡처: `#debug packet display|capture interface vNic_1 host 192.168.1.2_and_host_192.168.3.3_and_port_80`
- 풀이 투명 모드가 아닌 경우 Edge Services Gateway와 서버 간 패킷 캡처: `#debug packet display|capture interface vNic_1 host 192.168.3.1_and_host_192.168.3.3_and_port_80`

일반 로드 밸런서 문제

이 항목에서는 몇 가지 문제와 해결 방법을 살펴봅니다.

다음 문제는 **NSX** 로드 밸런싱을 사용할 때 일반적으로 나타납니다.

- **TCP 포트(예: 포트 443)의 로드 밸런싱은 작동하지 않습니다.**
 - 토폴로지를 확인합니다. 자세한 내용은 "**NSX 관리 가이드**"를 참조하십시오.
 - **Ping**을 사용하여 가상 서버 **IP** 주소에 연결할 수 있는지 확인하거나 업스트림 라우터를 확인하여 **ARP** 테이블이 채워져 있도록 합니다.
 - **UI를 사용하여 로드 밸런서 구성 확인 및 문제 해결.**
 - **CLI를 사용하여 로드 밸런서 문제 해결.**
 - 패킷을 캡처합니다.
- 로드 밸런싱 풀의 멤버가 활용되지 않습니다.
 - 서버가 풀에 있는지, 사용되도록 설정되어 있는지 확인하고 상태를 모니터링합니다.
- **Edge** 트래픽이 로드 밸런싱되지 않습니다.
 - 풀 및 지속성 구성을 확인합니다. 지속성이 구성되어 있고 소수의 클라이언트를 사용하는 경우 연결이 백엔드 풀 멤버로 동등하게 분산되지 않을 수 있습니다.
- 계층 **7** 로드 밸런싱 엔진이 중지되었습니다.
- 상태 모니터 엔진이 중지되었습니다.
 - 로드 밸런서 서비스를 사용하도록 설정합니다. "**NSX 관리 가이드**"를 참조하십시오.
- 풀 멤버 모니터 상태가 주의/위험입니다.
 - 로드 밸런서에서 애플리케이션 서버에 연결할 수 있는지 확인합니다.
 - 애플리케이션 서버 방화벽 또는 **DFW**가 트래픽을 허용하는지 확인합니다.
 - 애플리케이션 서버가 지정된 상태 탐색에 응답할 수 있는지 확인합니다.
- 풀 멤버가 비활성 상태입니다.
 - 풀 구성에서 풀 멤버가 사용되도록 설정되어 있는지 확인합니다.
- 계층 **7** 고정 테이블이 대기 **Edge**와 동기화되지 않습니다.
 - **HA**가 구성되어 있는지 확인합니다.
- 클라이언트 연결이 구성되어 있으나 애플리케이션 트랜잭션을 완료할 수 없습니다.
 - 애플리케이션 프로파일에서 적절한 지속성이 구성되어 있는지 확인합니다.
 - 애플리케이션이 풀의 (둘이 아니고) 한 서버에서만 작동할 경우 지속성 문제일 가능성이 높습니다.

기본 문제 해결

- 1 vSphere Web Client에서 로드 밸런서 구성 상태를 확인합니다.
 - a 네트워킹 및 보안 > NSX Edge(Networking & Security > NSX Edges)를 클릭합니다.
 - b NSX Edge를 두 번 클릭합니다.
 - c 관리(Manage)를 클릭한 다음 로드 밸런서(Load Balancer) 탭을 클릭합니다.
 - d 로드 밸런서 상태 및 로깅 수준이 구성되어 있는지 확인합니다.
- 2 로드 밸런서 서비스 문제를 해결하기 전에 NSX Manager에서 다음 명령을 실행하여 서비스가 작동 및 실행되고 있는지 확인합니다.

```
nsxmgr> show edge edge-4 service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer      : running
-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB  MAX SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT  MAX_CONN_RATE
running    1580      0          2081      1024       0          0          0
0          0
-----
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN  TOTAL_CONN
0          0          0          0
-----
Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn
```

참고 show edge all을 실행하여 NSX Edge의 이름을 조회할 수 있습니다.

구성 문제 해결

로드 밸런서 구성 작업이 NSX 사용자 인터페이스 또는 REST API 호출에 의해 거부되면 구성 문제로 분류됩니다.

데이터부 문제 해결

로드 밸런서 구성이 NSX Manager에서 수락되지만 클라이언트-Edge 로드 밸런서 서버 간에 연결 또는 성능 문제가 있습니다. 데이터부 문제에는 로드 밸런서 런타임 CLI 문제 및 로드 밸런서 시스템 이벤트 문제도 포함됩니다.

- 1 다음 REST API 호출을 사용하여 NSX Manager의 Edge 로깅 수준을 INFO에서 TRACE 또는 DEBUG로 변경합니다.

```
URL: https://NSX_Manager_IP/api/1.0/services/debug/loglevel/com.vmware.vshield.edge?level=TRACE
Method: POST
```

- 2 vSphere Web Client에서 풀 멤버 상태를 확인합니다.

- a 네트워킹 및 보안 > NSX Edge(Networking & Security > NSX Edges)를 클릭합니다.
- b NSX Edge를 두 번 클릭합니다.
- c 관리(Manage)를 클릭한 다음 로드 밸런서(Load Balancer) 탭을 클릭합니다.
- d 풀(Pools)을 클릭하여 구성된 로드 밸런서 풀의 요약을 확인하십시오.
- e 로드 밸런서 풀을 선택합니다. 풀 통계 표시(Show Pool Statistics)를 클릭하여 풀 상태가 UP인지 확인하십시오.

- 3 다음 REST API 호출을 사용하여 NSX Manager에서 보다 자세한 로드 밸런서 풀 구성 통계를 얻을 수 있습니다.

```
URL: https://NSX_Manager_IP/api/4.0/edges/{edgeId}/loadbalancer/statistics
Method: GET
```

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
  <timeStamp>1463507779</timeStamp>
  <pool>
    <poolId>pool-1</poolId>
    <name>Web-Tier-Pool-01</name>
    <member>
      <memberId>member-1</memberId>
      <name>web-01a</name>
      <ipAddress>172.16.10.11</ipAddress>
      <status>UP</status>
      <lastStateChangeTime>2016-05-16 07:02:00</lastStateChangeTime>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <httpReqTotal>0</httpReqTotal>
      <httpReqRate>0</httpReqRate>
      <httpReqRateMax>0</httpReqRateMax>
      <maxSessions>0</maxSessions>
      <rate>0</rate>
      <rateLimit>0</rateLimit>
```

```

        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <member>
        <memberId>member-2</memberId>
        <name>web-02a</name>
        <ipAddress>172.16.10.12</ipAddress>
        <status>UP</status>
        <lastStateChangeTime>2016-05-16 07:02:01</lastStateChangeTime>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <status>UP</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</pool>
<virtualServer>
    <virtualServerId>virtualServer-1</virtualServerId>
    <name>Web-Tier-VIP-01</name>
    <ipAddress>172.16.10.10</ipAddress>
    <status>OPEN</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</virtualServer>
</loadBalancerStatusAndStats>

```

4 명령줄에서 로드 밸런서 통계를 확인하려면 NSX Edge에서 다음 명령을 실행합니다.

특정 가상 서버: 먼저 `show service loadbalancer virtual`을 실행하여 가상 서버 이름을 가져옵니다. 그런 다음 `show statistics loadbalancer virtual <virtual-server-name>`을 실행합니다.

특정 TCP 풀: 먼저 `show service loadbalancer pool`을 실행하여 풀 이름을 가져옵니다. 그런 다음 `show statistics loadbalancer pool <pool-name>`을 실행합니다.

5 로드 밸런서 통계에서 실패 표시를 확인하십시오.

VPN(Virtual Private Network) 문제 해결

7

NSX Edge는 여러 가지 유형의 VPN을 지원합니다. 이 문제 해결 섹션에서는 L2 VPN 및 SSL VPN 문제 해결 방법을 설명합니다.

본 장은 다음 항목을 포함합니다.

- L2 VPN
- SSL VPN
- IPSec VPN

L2 VPN

L2 VPN을 사용할 경우 SSL VPN 내에서 터널링하여 여러 논리적 L2 네트워크(VLAN 및 VXLAN)를 L3 경계 간에 확장할 수 있습니다. 또한 L2 VPN 서버에서 여러 사이트를 구성할 수 있습니다. 가상 시스템은 사이트 간에 이동할 때 동일한 서브넷에 남아 있으며 해당 IP 주소는 바뀌지 않습니다. 또한 원격 사이트에서 "NSX를 사용"하도록 설정하지 않고도 독립형 Edge를 배포할 수도 있습니다. 송신 최적화를 통해 Edge는 모든 패킷을 송신 최적화 IP 주소에 로컬로 전송하고 다른 모든 것을 브리지할 수 있습니다.

따라서 L2 VPN을 사용하는 엔터프라이즈는 VXLAN 또는 VLAN으로 지원되는 워크로드를 물리적으로 분리된 위치 간에 원활하게 마이그레이션할 수 있습니다. 클라우드 제공자의 경우 L2 VPN은 워크로드 및 애플리케이션에 대한 기존 IP 주소를 수정하지 않고 온보드 테넌트를 수용하는 메커니즘을 제공합니다.

L2 VPN 일반 구성 문제

이 항목에서는 L2 VPN에 관련된 일반 구성 문제를 설명합니다.

문제

일반적인 구성 문제는 다음과 같습니다.

- L2 VPN 클라이언트가 구성되어 있으나 인터넷 연결 방화벽에서 트래픽이 대상 포트 443을 통해 터널을 통과해서 흐르도록 허용하지 않습니다.
- L2 VPN 클라이언트가 서버 인증서의 유효성을 검사하도록 구성되어 있으나 올바른 CA 인증서 또는 FQDN으로 구성되지 않았습니다.

- L2 VPN 서버가 구성되었으나 인터넷 연결 방화벽에서 NAT/방화벽 규칙이 생성되지 않았습니다.
- 트렁크 인터페이스가 분산 포트 그룹 또는 표준 포트 그룹을 통해 지원되지 않습니다.

참고 L2 VPN 서버는 기본적으로 포트 443에서 수신됩니다. 이 포트는 L2 VPN 서버 설정에서 구성할 수 있습니다.

L2 VPN 클라이언트는 기본적으로 포트 443에 대해 송신 연결을 설정합니다. 이 포트는 L2 VPN 클라이언트 설정에서 구성할 수 있습니다.

해결책

- 1 L2 VPN 서버 프로세스가 실행되고 있는지 확인합니다.
 - a NSX Edge VM에 로그인합니다.
 - b `show process monitor` 명령을 실행하고 이름이 `l2vpn`인 프로세스를 찾을 수 있는지 확인합니다.
 - c `show service network-connections` 명령을 실행하고 `l2vpn` 프로세스가 포트 443에서 수신하는지 확인합니다.
- 2 L2 VPN 클라이언트 프로세스가 실행되고 있는지 확인합니다.
 - a NSX Edge VM에 로그인합니다.
 - b `show process monitor` 명령을 실행하고 이름이 `naclientd`인 프로세스를 찾을 수 있는지 확인합니다.
 - c `show service network-connections` 명령을 실행하고 `naclientd` 프로세스가 포트 443에서 수신하는지 확인합니다.
- 3 인터넷에서 L2 VPN 서버에 액세스할 수 있는지 확인합니다.
 - a 브라우저를 열고 `https://<L2 VPN 공용 IP>`로 이동합니다.
 - b 포털 로그인 페이지가 표시되어야 합니다. 포털 페이지가 표시되면 인터넷을 통해 L2 VPN 서버에 연결할 수 있는 것입니다.
- 4 트렁크 인터페이스가 분산 포트 그룹 또는 표준 포트 그룹을 통해 지원되는지 확인합니다.
 - a 트렁크 인터페이스가 분산 포트 그룹을 통해 지원되면 싱크 포트가 자동으로 설정됩니다.
 - b 트렁크 인터페이스가 표준 포트 그룹을 통해 지원되면 다음과 같이 vSphere Distributed Switch를 수동으로 구성해야 합니다.
 - 포트를 비규칙(promiscuous) 모드로 설정합니다.
 - 위조 전송(Forged Transmits)을 수락(Accept)으로 설정합니다.
- 5 L2 VPN 루핑 문제를 완화합니다.
 - a NIC 팀 구성이 제대로 구성되지 않으면 MAC 플래핑과 중복된 패킷의 두 가지 주요 문제가 관찰됩니다. 반복을 완화하기 위한 L2VPN 옵션에 설명된 구성을 확인합니다.

6 L2 VPN의 VM이 서로 통신할 수 있는지 확인합니다.

- L2 VPN 서버 CLI에 로그인하고 해당 탭 인터페이스 `debug packet capture interface name`에서 패킷을 캡처합니다.
- L2 VPN 클라이언트에 로그인하고 해당 탭 인터페이스 `debug packet capture interface name`에서 패킷 캡처를 캡처합니다.
- 이러한 캡처를 분석하여 ARP가 해결되고 있는지와 데이터 트래픽 흐름을 확인합니다.
- Allow Forged Transmits: dvSwitch 속성이 **L2 VPN 트렁크 포트**로 설정되어 있는지 확인합니다.
- 싱크 포트가 **L2 VPN 트렁크 포트**로 설정되어 있는지 확인합니다. 이렇게 하려면 호스트에 로그인하고 `net-dvs -l` 명령을 실행합니다. L2 VPN Edge 내부 포트에 대해 설정된 SINK 속성 (`com.vmware.etherSwitch.port.extraEthFRP = SINK`)을 확인합니다. 내부 포트는 NSX Edge 트렁크가 연결되는 `dvPort`를 나타냅니다.

net-dvs -l

ESXi

```
port 939:
  com.vmware.common.port.alias = , propType = CONFIG
  com.vmware.common.port.connectid = 323234212 , propType = CONFIG
  com.vmware.common.port.portgroupid = dvportgroup-181 , propType = CONFIG
  com.vmware.common.port.block = false , propType = CONFIG
  com.vmware.common.port.dvfilter = filters (num = 0):
    propType = CONFIG
  com.vmware.common.port.ptAllowed = 0x 0. 0. 0. 0
    propType = CONFIG
  com.vmware.etherSwitch.port.txUplink = normal , propType = CONFIG
  com.vmware.common.port.volatile.persist = /vmfs/volumes/9ec6ae8b-38b8e621/.dvsData/1c ec 0e 50 02 9c a9 21-b6 d8
  fc 73 e5 79 69/939 , propType = CONFIG
  com.vmware.common.port.ptAllowedRT = 0x 0. 0. 0. 0
    propType = RUNTIME
  com.vmware.net.vxlan.trunkcfg = 0x63.6f.6e.66.69.67.56.65.72.73.69.6f.6e.3d.30.2e.31.3b.61.6c.6c.6f.77.47.75.65.7
  74.56.6c.61.6e.3d.30.3b.6e.75.6d.54.72.75.6e.6b.4d.65.6d.62.65.72.73.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.43.70.45.6e.61.62.
  .65.64.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.56.6e.69.3d.35.30.30.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.4d.63.61.73.74.49.70
  d.30.2e.30.2e.30.2e.31.3b
    propType = CONFIG POLICY
  com.vmware.etherSwitch.port.extraEthFRP = SINK
    propType = CONFIG POLICY
  com.vmware.etherSwitch.port.teaming:
    load balancing = first uplink (i.e. explicit)
    link selection = link state up;
    link behavior = notify switch; best effort on failure; shotgun on failure;
    active = dvUplink1;
    standby =
    propType = CONFIG
  com.vmware.etherSwitch.port.security = deny promiscuous; deny mac change; allow forged frames
    propType = CONFIG
  com.vmware.etherSwitch.port.vlan = Guest VLAN tagging
    ranges = 0
    propType = CONFIG
  com.vmware.common.port.statistics:
    pktsInUnicast = 0
    bytesInUnicast = 0
    pktsInMulticast = 6
    bytesInMulticast = 620
```

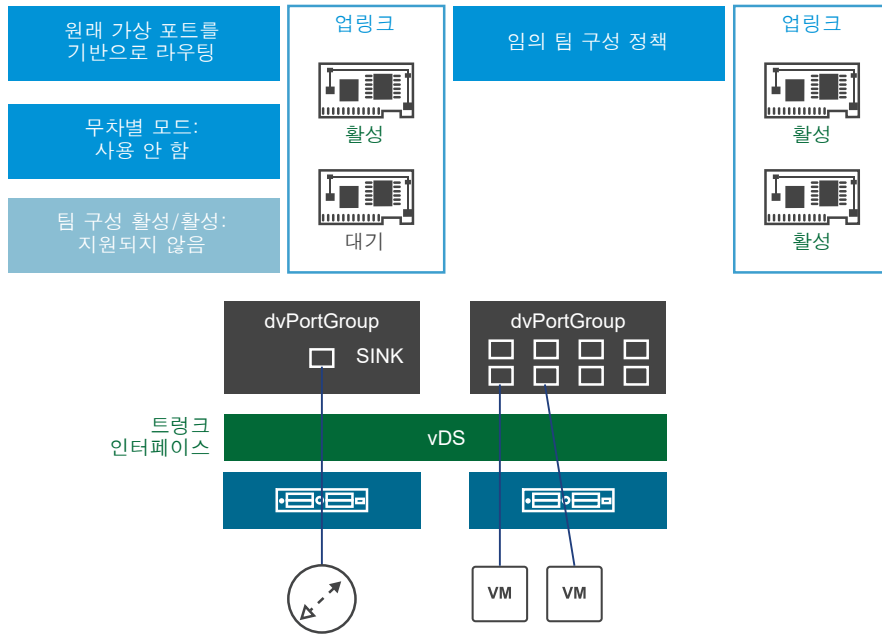
Sink port should be enabled for the dvPort where the Edge trunk is connected to

반복을 완화하기 위한 L2VPN 옵션

반복을 완화하기 위한 두 가지 옵션이 있습니다. NSX Edge와 VM을 서로 다른 ESXi 호스트에 배치할 수도 있고 또는 동일한 ESXi 호스트에 배치할 수도 있습니다.

옵션 1: L2VPN Edge용 ESXi 호스트와 VM용 ESXi 호스트 구분

1. 별도 ESXi 호스트에 L2VPN Edge 및 VM 배포



- 1 Edge와 VM을 별도의 ESXi 호스트에 배포합니다.
- 2 다음과 같이 Edge의 트렁크 vNic에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - a 로드 밸런싱을 "원래 가상 포트를 기반으로 라우팅"으로 설정합니다.
 - b 업링크 하나만 활성화로 설정하고 나머지 업링크는 대기로 설정합니다.
- 3 다음과 같이 VM에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - a 모든 팀 구성 정책이 허용됩니다.
 - b 활성화 업링크를 여러 개 구성할 수 있습니다.

- 4 SINK 포트 모드를 사용하도록 Edge를 구성하고 트렁크 vNic에서 비규칙 모드를 사용하지 않도록 설정합니다.

참고

- 비규칙 모드 사용 안 함: vSphere Distributed Switch를 사용하는 경우
- 비규칙 모드 사용: 가상 스위치를 사용하여 트렁크 인터페이스를 구성하는 경우

가상 스위치의 비규칙 모드가 사용으로 설정된 경우 현재 비규칙 포트에서 사용되지 않는 업링크의 패킷 일부가 삭제되지 않습니다. ReversePathFwdCheckPromisc를 사용하도록 설정했다가 사용하지 않도록 설정하면 비규칙 포트에 대해 현재 사용되지 않은 업링크에서 들어오는 모든 패킷이 명시적으로 삭제됩니다.

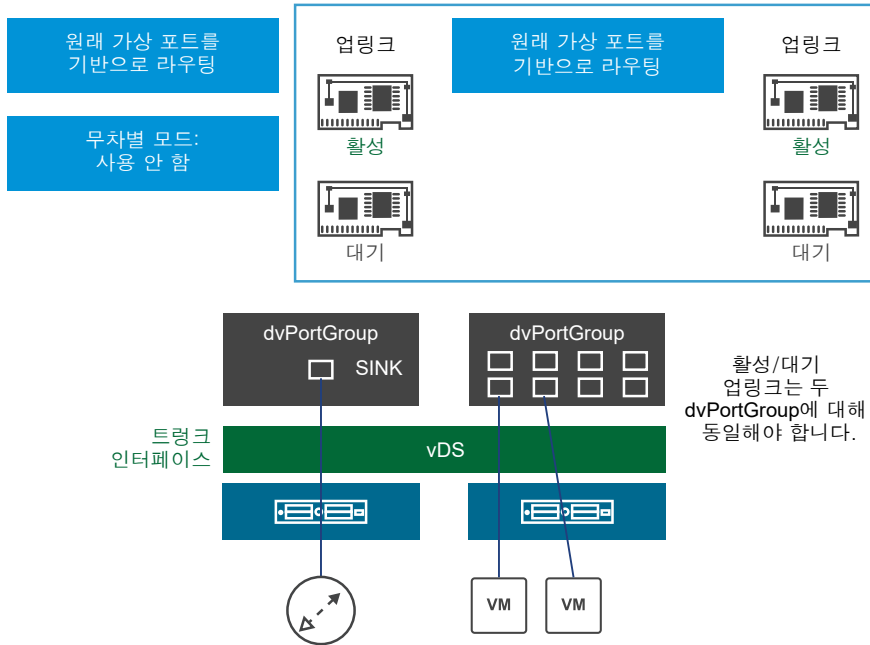
중복된 패킷을 차단하려면 NSX Edge가 있는 ESXi CLI에서 비규칙 모드에 대한 RPF 확인을 활성화합니다.

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to Promiscuous mode.
```

포트 그룹(PortGroup) 보안 정책에서 비규칙 모드(PromiscuousMode)를 수락(Accept)에서 거부(Reject)로 설정했다가 다시 수락(Accept)으로 설정하여 구성된 변경 사항을 활성화합니다.

- 옵션 2: 동일한 ESXi 호스트의 Edge 및 VM

2. 동일한 호스트에 L2VPN Edge 및 VM 배포



- a 다음과 같이 **Edge**의 트렁크 vNic에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - 1 로드 밸런싱을 "원래 가상 포트를 기반으로 라우팅"으로 설정합니다.
 - 2 업링크 하나만 활성으로 설정하고 나머지 업링크는 대기로 설정합니다.
- b 다음과 같이 **VM**에 연결된 분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성합니다.
 - 1 모든 팀 구성 정책이 허용됩니다.
 - 2 업링크 중 하나만 활성 상태일 수 있습니다.
 - 3 VM의 분산 포트 그룹과 **Edge**의 트렁크 vNic 분산 포트 그룹에 대해 활성/대기 업링크의 순서가 동일해야 합니다.
- c SINK 포트 모드를 사용하도록 클라이언트 측 독립형 **Edge**를 구성하고 트렁크 vNic에서 비규칙 모드를 사용하지 않도록 설정합니다.

CLI를 사용하여 문제 해결

NSX CLI(명령줄 인터페이스)를 사용하여 일부 L2 VPN 문제 해결을 수행할 수 있습니다.

문제

L2 VPN이 예상대로 작동하지 않습니다.

해결책

- 1 다음 중앙 CLI 명령을 사용하여 구성 문제를 확인합니다.

```
show edge <edgeID> configuration l2vpn.
```

예: show edge edge-1 configuration l2vpn.

2 클라이언트 및 서버 Edge 둘 다에서 다음 명령을 사용합니다.

- show configuration l2vpn - 다음 4가지 키 값을 통해 서버를 확인합니다.

show configuration l2vpn

```
vShield Edge L2 VPN Config:
{
  "l2vpn" : {
    "cipher" : {
      "RC4-MD5"
    },
    "listenerPort" : 443,
    "clientVnicIndex" : null,
    "filters" : [],
    "serverPort" : null,
    "caCertificate" : null,
    "peerSiteAlgorithm" : null,
    "listenerIp" : "192.168.100.3",
    "peerSites" : [
      {
        "vseVnicNames" : [
          "vNic_10"
        ],
        "name" : "L2VPN-Site1",
        "filters" : [],
        "l2vpnUser" : {
          "password" : "*****",
          "userId" : "vpnuser1"
        }
      }
    ],
    "clientProxySetting" : null,
    "enable" : true,
    "trunkedVnicIndexes" : [
      2
    ],
    "serverVnicIndex" : null,
    "l2vpnUsers" : [],
    "serverAddress" : null,
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "vseVnicNames" : null,
    "serverCertificate" : null
  }
}
```

Cipher

Port

Server IP

Peer Site Configuration

- show service l2vpn bridge - 인터페이스 수는 L2 VPN 클라이언트의 수에 따라 다릅니다. 아래 출력에서는 단일 L2 VPN 클라이언트(na1)가 구성됩니다. Port1은 vNic_2를 나타냅니다. MAC 주소 02:50:56:56:44:52는 vNic_2 인터페이스에서 학습되었으며 Edge의 로컬이 아닙니다(L2 VPN 서버). 다음 예의 세 번째 행은 na1 인터페이스를 나타냅니다.

```
plr01-0> show service l2vpn bridge
```

bridge name	bridge id	STP enabled	interfaces
br-sub	8000.0050568e19fb	no	vNic_2 na1

List of learned MAC addresses for L2 VPN bridge br-sub

port	no	mac addr	is local?	vlanid	ageing timer
1		00:50:56:8e:19:fb	yes	0	0.00
1		02:50:56:56:44:52	no	1	0.87
2		2a:56:30:31:7e:3b	yes	0	0.00

- `show service l2vpn trunk table`
- `show service l2vpn conversion table` - 다음 예에서 1번 터널에 도달하는 이더넷 프레임은 패킷이 VDS에 전달되기 전에 해당 1번 VLAN ID가 VLAN 번호 5001을 갖는 VXLAN으로 변환됩니다.



- `show process monitor - l2vpn`(서버) 및 `naclntd`(클라이언트) 프로세스가 실행되고 있는지를 식별합니다.
- `show service network-connections - l2vpn`(서버) 및 `naclntd`(클라이언트) 프로세스가 포트 443에서 수신하고 있는지를 식별합니다.

SSL VPN

다음 정보를 사용하여 설정 문제를 해결할 수 있습니다.

SSL VPN 웹 포털이 열리지 않음

SSL VPN 사용자는 [SSL VPN 웹 포털 로그인] 페이지를 열어 SSL VPN-Plus Client 설치 패키지를 다운로드한 후 설치할 수 없습니다.

문제

[SSL VPN 웹 포털 로그인] 페이지가 열리지 않거나 페이지가 시스템 브라우저에서 올바르게 렌더링되지 않습니다.

원인

다음과 같은 이유 중 하나로 이 문제가 발생할 수 있습니다.

- 시스템이 지원되지 않는 브라우저 버전을 사용합니다.
- 브라우저에서 쿠키 및 JavaScript가 사용하도록 설정되어 있지 않습니다.

해결책

- 1 다음과 같은 지원되는 브라우저 중 하나에서 [SSL VPN 웹 포털 로그인] 페이지를 열어야 합니다.

브라우저	지원되는 최소 버전
Internet Explorer	9.0.8112.16421
Chrome	67.03396
Safari	10.x

- 2 브라우저 설정을 열고 쿠키 및 JavaScript가 사용하도록 설정되어 있는지 확인합니다.
- 3 브라우저 언어가 영어로 설정되지 않은 경우 언어를 영어로 설정하고 문제가 지속되는지 확인합니다.
- 4 SSL VPN 서버에서 AES 암호를 선택했는지 확인합니다. 일부 브라우저는 AES 암호화를 지원하지 않습니다.

SSL VPN-Plus: 설치 실패

발생 가능한 SSL VPN-Plus Client 관련 설치 문제 및 해결 방법을 이해하려면 이 항목을 사용하십시오.

문제

SSL VPN-Plus Client 설치와 관련된 일반적인 문제는 다음과 같습니다.

- SSL VPN-Plus Client가 성공적으로 설치되었지만 클라이언트가 작동하지 않습니다.
- Mac 시스템에서 커널 확장 주의 메시지가 표시됩니다.
- Mac OS High Sierra에서 다음과 같은 설치 오류 메시지가 표시됩니다.

```
/opt/sslvpn-plus/naclient/signed_kext/tap.kext failed to load - (libkern/kext)system policy prevents loading; check the system/kernel logs for errors or try kextutil(8).
Error: Could not load /opt/sslvpn-plus/naclient/signed_kext/tap.kext
```

```
installer[4571] <Debug>: install:didFailWithError:Error Domain=
PKInstallErrorDomain Code=112 "An error occurred while running scripts from the package
"naclient.pkg" .
" UserInfo={NSFilePath=./postinstall,NSURL=file:///<pathtofile>/
naclient.pkg,PKInstallPackageIdentifier=
com.vmware.sslvpn,NSLocalizedString=An error occurred while running scripts from the
package "naclient.pkg" .}
```

```
installer[4571] <Error>: Install failed: The Installer encountered an error that caused the
installation to fail. Contact the software manufacturer for assistance.
installer: The install failed (The Installer encountered an error that caused the installation to
fail.
Contact the software manufacturer for assistance.)
```

- Windows 시스템에서 다음과 같은 오류 메시지가 표시됩니다. 다음과 같은 이유 때문에 드라이버를 설치하지 못했습니다. E000024B. 시스템을 재부팅해 보십시오.

원인

다음과 같은 이유 중 하나로 인해 **SSL VPN-Plus Client**를 컴퓨터에 성공적으로 설치한 후에 이 프로그램이 실패할 수 있습니다.

- 구성 파일(**naclient.cfg**)이 누락되었거나 구성 파일이 잘못되었습니다.
- 디렉토리 사용 권한 또는 사용자 사용 권한이 올바르지 않습니다.
- **SSL VPN** 서버에 연결할 수 없습니다.
- **Mac** 및 **Linux** 시스템에서 탭 드라이버가 로드되지 않았습니다.

Mac 시스템에서는 커널 확장 로드가 차단되므로 커널 확장 주의 메시지가 표시됩니다.

Mac OS High Sierra에서는 **Mac** 시스템에서 **kext**를 허용하지 않고 **kext**를 로드하도록 요구하지도 않을 경우 설치 오류가 표시됩니다.

Windows 시스템에서는 **Edge SSL VPN-Plus Client** 설치 관리자에서 **SSL 클라이언트 네트워크 어댑터 숨기기(Hide SSL client network adapter)** 옵션을 사용하도록 설정했으므로 드라이버 설치 실패(**E000024B**)가 표시됩니다.

해결책

- 1 지원되는 운영 체제에서 **SSL VPN-Plus Client**를 설치해야 합니다. 지원되는 운영 체제에 대한 자세한 내용은 "**NSX 관리 가이드**"에서 **SSL VPN-Plus** 개요 항목을 참조하십시오.
- 2 **Windows** 시스템에서 **SSL VPN-Plus Client**를 설치하는 사용자에게 **관리자** 권한이 있는지 확인합니다. **Mac** 및 **Linux** 시스템에서 **SSL VPN-Plus Client**를 설치하려면 사용자에게 **루트** 권한이 있어야 합니다. 또한 **Mac** 시스템에서 **SSL VPN-Plus Client**가 성공적으로 시작 및 실행되려면 **usr/local/lib** 디렉토리에 대해 **실행** 권한이 있어야 합니다.
- 3 **Linux** 시스템에서 다음과 같은 라이브러리가 설치되어 있는지 확인합니다. UI가 작동하려면 다음 라이브러리가 필요합니다.
 - **TCL**
 - **TK**
 - **NSS**
- 4 탭 드라이버가 **Mac** 및 **Linux** 시스템에서 로드되지 않으면 **shell script**를 실행하여 드라이버를 로드합니다.

운영 체제	설명
Mac	sudo 권한을 사용하여 /opt/sslvpn-plus/naclient/ 디렉토리에서 Naclient.sh shell script 를 실행합니다.
Linux	sudo 권한을 사용하여 naclient.sh shell script 를 실행합니다. 이 스크립트는 linux_phat_client/linux_phat_client 디렉토리에서 찾을 수 있습니다.

- 5 macOS High Sierra 이상이 있는 시스템에서 커널 확장 주의 메시지를 해결하려면 커널 확장(kext)을 로드하기 위한 명시적 사용자 승인을 제공해야 합니다. 다음 단계를 수행합니다.
 - a Mac 시스템에서 **시스템 환경 설정(System Preferences) > 보안 및 개인 정보(Security & Privacy)** 창을 엽니다.
 - b 창 아래쪽에서 "일부 시스템 소프트웨어의 로드가 차단되었습니다."와 유사한 메시지가 표시될 수 있습니다. "허용" 버튼을 클릭합니다.
 - c 설치를 계속하려면 **허용(Allow)**을 클릭합니다.
 커널 확장 로드와 관련한 사용자 승인을 제공하는 방법에 대한 자세한 내용은 https://developer.apple.com/library/content/technotes/tn2459/_index.html을 참조하십시오.
 - d 커널 확장을 로드하는 동안 **SSL VPN-Plus Client** 설치 프로세스가 백그라운드에서 계속 실행됩니다. **SSL VPN-Plus Client**가 설치되지만 다음 오류 메시지가 표시됩니다. 설치가 실패했습니다. 설치 관리자에서 설치 실패를 야기하는 오류가 발생했습니다. 소프트웨어 제조업체에 도움을 요청하십시오.
 - e 이 오류를 해결하려면 **SSL VPN-Plus Client**를 제거했다가 다시 설치합니다.
- 6 Mac OS High Sierra에서 설치 오류 메시지를 해결하려면 다음 단계를 수행합니다.
 - a 알림이 사용하도록 설정되어 있는지 확인합니다. **시스템 환경 설정(System Preferences) > 보안 및 개인 정보(Security & Privacy) > 알림 허용(Allow Notifications)**으로 이동합니다.

참고 Mac OS High Sierra에서 **SSL VPN-Plus Client**를 처음 설치하는 경우 알림 창에 설치를 허용할지 묻는 메시지가 표시됩니다. 이 알림은 일반적으로 30분 동안 지속됩니다. 이 알림이 **허용(Allow)**을 클릭하기 전에 사라지면 시스템을 다시 시작하고 **SSL VPN-Plus Client**를 다시 설치합니다.

설치가 계속 실패하면 커널 확장(kext)이 허용되지 않고 kext를 로드하라는 메시지도 표시되지 않습니다. 나머지 하위 단계를 완료하여 미리 승인된 kext 목록에 `tuntap kext team id`를 추가합니다.

 - b 복구 모드에서 Mac 시스템을 다시 시작합니다.
 - 1 화면 왼쪽 상단에서 **Apple** 로고를 클릭합니다.
 - 2 **다시 시작(Restart)**을 클릭합니다.
 - 3 **Apple** 로고 또는 회전하는 지구본이 보일 때까지 **Command**와 **R** 키를 즉시 누릅니다. 회전하는 지구본은 Mac 시스템이 기본 제공 복구 시스템을 통해 시작할 수 없어 인터넷에 연결하여 macOS 복구를 시작하려고 하면 나타납니다. 이제 Mac이 복구 모드에서 시작됩니다.
 - c 맨 위 막대에서 **유틸리티(Utilties) > 터미널(Terminal)**을 클릭합니다.
 - d 사전 승인된 kext 목록에 `tuntap kext team id`를 추가하려면 `- spctl kext-consent add KS8XL6T9FZ` 명령을 실행합니다.
 - e 표준 모드에서 Mac 시스템을 다시 시작합니다.

f 사전 승인된 **kext** 목록에 **team-id**가 표시되는지 여부를 확인하려면 – **spctl kext-consent list** 명령을 실행합니다.

g SSL VPN-Plus Client 패키지를 설치합니다.

- 7 Windows 시스템에서 드라이버 설치 실패 오류(E00024B)가 표시되면 Edge SSL VPN-Plus Client 설치 관리자에서 **SSL 클라이언트 네트워크 어댑터 숨기기(Hide SSL client network adapter)** 옵션을 사용하지 않도록 설정합니다. 이 옵션을 사용하지 않도록 설정하기 위한 지침을 보려면 <https://kb.vmware.com/s/article/2108766>에서 VMware 기술 자료 문서를 참조하십시오.

SSL VPN-Plus: 통신 문제

발생 가능한 SSL VPN 연결 및 데이터 경로 문제와 해결 방법을 이해하려면 이 항목을 사용하십시오.

문제

SSL VPN 연결 및 데이터 경로와 관련된 일반적인 문제는 다음과 같습니다.

- SSL VPN-Plus Client가 SSL VPN 서버에 연결할 수 없습니다.
- SSL VPN-Plus Client가 설치되어 있지만 SSL VPN-Plus 서비스가 실행되고 있지 않습니다.
- 로그인한 사용자의 최대 수에 도달했습니다. SSL VPN 웹 포털 또는 SSL VPN-Plus Client에 다음과 같은 메시지가 표시됩니다.

최대 사용자 수에 도달했습니다/SSL VPN-Plus 라이선스에 따라 로그인한 사용자의 최대 수에 도달했습니다. 잠시 후 다시 시도하십시오. 또는 SSL 읽기에 실패했습니다.가 표시됩니다.

- SSL VPN 서비스가 실행되고 있지만 데이터 경로가 작동하지 않습니다.
- SSL VPN 연결이 설정되었지만 전용 네트워크의 애플리케이션에 액세스할 수 없습니다.

해결책

- 1 SSL VPN-Plus Client가 SSL VPN 서버에 연결할 수 없으면 다음을 수행합니다.
 - SSL VPN 사용자가 올바른 사용자 이름 및 암호를 사용하여 로그인되어 있는지 확인합니다.
 - SSL VPN 사용자가 유효한지 여부를 확인합니다.
 - SSL VPN 사용자가 웹 포털을 사용하여 SSL VPN 서버에 연결할 수 있는지 여부를 확인합니다.

2 NSX Edge에서 다음 단계를 수행하여 SSL VPN 프로세스가 실행 중인지 여부를 확인합니다.

- a CLI에서 NSX Edge에 로그인합니다. Edge CLI에 로그인하는 방법에 대한 자세한 내용은 "NSX 명령줄 인터페이스 참조"를 참조하십시오.
- b `show process monitor` 명령을 실행하고 `sslvpn` 프로세스를 찾습니다.
- c `show service network-connections` 명령을 실행하고 `sslvpn` 프로세스가 포트 443에서 수신 대기하는지 확인합니다.

참고 기본적으로 SSL 트래픽에 대해 포트 443이 사용됩니다. 그러나 SSL 트래픽에 대해 다른 TCP 포트를 구성한 경우 `sslvpn` 프로세스가 해당 TCP 포트 번호에서 수신 대기하는지 확인합니다.

3 SSL VPN-Plus Client에서 SSL VPN-Plus 서비스가 실행 중인지 여부를 확인합니다.

운영 체제	설명
Windows	작업 관리자를 열고 SSL VPN-Plus Client 서비스가 시작되었는지 여부를 확인합니다.
Mac	<ul style="list-style-type: none"> ■ <code>naclientd</code> 프로세스가 데몬에 대해 시작되었는지 확인합니다. ■ <code>naclient</code> 프로세스가 GUI에 대해 시작되었는지 확인합니다. 프로세스가 실행 중인지 여부를 확인하려면 <code>ps -ef grep "naclient"</code> 명령을 실행합니다.
Linux	<ul style="list-style-type: none"> ■ <code>naclientd</code> 및 <code>naclient_poll</code> 프로세스가 시작되었는지 확인합니다. ■ 프로세스가 실행 중인지 여부를 확인하려면 <code>ps -ef grep "naclient"</code> 명령을 실행합니다.

서비스가 실행되고 있지 않으면 다음 명령을 실행하여 서비스를 시작합니다.

운영 체제	명령
Mac	<code>sudo launchctl load -w /Library/LaunchDaemons/com.vmware.naclientd.plist</code> 명령을 실행합니다.
Linux	<code>sudo service naclient start</code> 명령을 실행합니다.

4 로그인한 SSL VPN 사용자가 최대 수에 도달한 경우 NSX Edge 폼 팩터를 늘려 CCU(동시 사용자 수)를 늘립니다.

자세한 내용은 "NSX 관리 가이드"를 참조하십시오. 이 작업을 수행하면 연결된 사용자가 VPN에서 연결이 끊어집니다.

5 SSL VPN 서비스가 실행되고 있지만 데이터 경로가 작동하지 않는 경우 다음 단계를 수행합니다.

- a 연결에 성공한 후 가상 IP가 지정되었는지 여부를 확인합니다.
- b 경로가 추가되었는지 여부를 확인합니다.

6 전용(백엔드) 네트워크의 애플리케이션에 액세스할 수 없는 경우 다음 단계를 수행하여 문제를 해결합니다.

- a 전용 네트워크 및 IP 풀이 동일한 서브넷에 있지 않은지 확인합니다.
- b 관리자가 IP 풀을 정의하지 않았거나 IP 풀이 모두 사용된 경우 다음 단계를 수행합니다.
 - 1 vSphere Web Client에 로그인합니다.
 - 2 **네트워킹 및 보안(Networking & Security)**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
 - 3 NSX Edge를 두 번 클릭하고 **SSL VPN-Plus** 탭을 클릭합니다.
 - 4 "NSX 관리 가이드"의 "IP 풀 추가" 항목에 설명된 대로 정적 IP 풀을 추가합니다. **게이트웨이(Gateway)** 텍스트 상자에서 IP 주소를 추가해야 합니다. 게이트웨이 IP 주소가 **na0** 인터페이스에 할당됩니다. 모든 TCP 이외 트래픽은 **na0** 인터페이스라는 가상 어댑터를 통해 흐릅니다. 동일한 **na0** 인터페이스에 할당된 다른 게이트웨이 IP 주소로 여러 IP 풀을 생성할 수 있습니다.
 - 5 `show interface na0` 명령을 사용하여 제공된 IP 주소를 확인하고 모든 IP 풀이 동일한 **na0** 인터페이스에 할당되었는지 확인합니다.
 - 6 클라이언트 시스템에 로그인하고 **SSL VPN-Plus Client - 통계(SSL VPN-Plus Client - Statistics)** 화면으로 이동한 후 할당된 가상 IP 주소를 확인합니다.
- c NSX Edge CLI(명령줄 인터페이스)에 로그인하고 `debug packet capture interface na0` 명령을 실행하여 na0 인터페이스에 대해 패킷 캡처를 수행합니다. 또한 **패킷 캡처(Packet Capture)** 도구를 사용하여 패킷을 캡처할 수도 있습니다. 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

참고 `no debug packet capture interface na0` 명령을 실행하여 캡처를 중지할 때까지 패킷 캡처는 백그라운드에서 계속 실행됩니다.

- d TCP 최적화가 사용되도록 설정되면 방화벽 규칙을 확인합니다.
 - e TCP 이외 트래픽의 경우 백엔드 네트워크의 기본 게이트웨이가 Edge의 내부 인터페이스로 설정되어 있는지 확인합니다.
 - f Mac 및 Linux 클라이언트의 경우 SSL VPN Client가 설치된 시스템으로 로그인한 후 `tcpdump -i tap0 -s 1500 -w filepath` 명령을 실행하여 tap0 인터페이스 또는 가상 어댑터에 대해 패킷 캡처를 수행합니다. Windows 클라이언트에서는 Wireshark와 같은 패킷 분석기 도구를 사용하여 SSL VPN-Plus Client 어댑터에서 패킷을 캡처합니다.
- 7** 위의 모든 단계로 문제가 해결되지 않으면 다음 NSX Edge CLI 명령을 사용하여 문제를 추가적으로 해결합니다.

용도	명령
SSL VPN 상태를 확인합니다.	<code>show service sslvpn-plus</code>
SSL VPN 통계를 확인합니다.	<code>show service sslvpn-plus stats</code>

용도	명령
연결된 VPN 클라이언트를 확인합니다.	<code>show service sslvpn-plus tunnels</code>
SSL VPN-Plus 세션을 확인합니다.	<code>show service sslvpn-plus sessions</code>

SSL VPN-Plus: 인증 문제

SSL VPN-Plus 인증 문제가 발생했습니다.

문제

SSL VPN-Plus 인증에 실패합니다.

해결책

- ◆ 인증 문제가 발생하면 다음 설정을 확인하십시오.
 - a NSX Edge에서 외부 인증 서버에 연결할 수 있는지 확인합니다. NSX Edge에서 인증 서버를 ping 하고 해당 서버에 연결할 수 있는지 확인합니다.
 - b LDAP 브라우저와 같은 도구를 사용하여 외부 인증 서버 구성을 확인하고 구성이 작동하는지 검토 하십시오. LDAP 및 AD 인증 서버만 LDAP 브라우저를 통해 확인할 수 있습니다.
 - c 로컬 인증 서버가 인증 프로세스에서 구성된 경우 가장 낮은 우선 순위로 설정되어 있는지 확인합 니다.
 - d AD(Active Directory)를 사용하는 경우 `no-ssl` 모드로 설정하고 AD 서버에 연결할 수 있는 인터페 이스에서 패킷 캡처를 수행합니다.
 - e syslog 서버에서 인증이 성공하면 다음과 비슷한 메시지가 표시됩니다. Log Output -
`SVP_LOG_NOTICE,`
`10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09`
`:28:39,-,-,,,,,,,,,-,-,`
 - f syslog 서버에서 인증이 실패하면 다음과 비슷한 메시지가 표시됩니다. Log Output -
`SVP_LOG_NOTICE,`
`10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09`
`:28:39,-,-,,,,,,,,,-,-,`

SSL VPN-Plus Client가 응답을 중지함

TCP 최적화를 사용하도록 설정할 경우 SSL VPN-Plus Client가 응답을 중지합니다.

문제

터널을 통해 트래픽을 전송하기 위해 SSL VPN-Plus 서비스를 NSX Edge에서 실행되도록 구성하고 TCP 최적화를 사용하도록 설정했습니다. SSL VPN-Plus Client에서 네트워크 성능 측정 및 조정 도구(예: iperf3)를 실행할 때 SSL VPN-Plus Client가 응답을 중지합니다.

원인

다음 두 시나리오 중 하나는 **SSL VPN-Plus Client**에서 데이터를 전송할 때 터널 읽기 오류를 일으킬 수 있습니다.

- 백엔드 서버는 **TCP FIN** 시퀀스를 전송하여 **SSL VPN** 서버와의 **TCP** 연결을 닫습니다.
- 백엔드 서버에 데이터를 전달하는 동안 터널 쓰기 작업이 실패합니다.

터널 읽기 오류는 알 수 없는 프로토콜 ID입니다. 이 오류는 **SSL VPN** 서버와 **SSL VPN-Plus Client** 간에 터널을 지우며, 이로 인해 클라이언트에서 **SSL** 읽기/쓰기 작업이 실패하고 **SSL VPN-Plus Client**가 응답을 중지합니다.

해결책

- ◆ 이 문제를 해결하려면 **vSphere Web Client**에서 다음 단계를 수행하여 **SSL VPN** 터널을 통한 전용 네트워크 트래픽에 대해 **TCP** 최적화를 사용하지 않도록 설정합니다.
 - a **SSL VPN-Plus** 서비스를 구성한 **NSX Edge VM**을 두 번 클릭합니다.
 - b **SSL VPN-Plus** 탭을 클릭하고 개인 네트워크를 선택합니다.
 - c **TCP 최적화 사용(Enable TCP Optimization)** 확인란을 선택 취소합니다.

기본 로그 분석

SSL VPN-Plus Gateway 로그는 **NSX Edge Appliance**에 구성된 **Syslog** 서버로 전송됩니다. **SSL VPN-Plus Client** 로그는 원격 사용자 컴퓨터 **C:\Users\username\AppData\Local\VMware\vpn\svp_client.log** 디렉토리에 저장됩니다.

기본 로그 분석 - 인증

인증 성공

- 다음 로그 출력은 사용자 **a**가 **2016년 10월 28일, 0928**시에 네트워크 액세스 클라이언트에서 성공적으로 인증되었음을 보여 줍니다.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

인증 실패

- 다음 로그 출력은 사용자 **a**가 **2016년 10월 28일, 0928**시에 네트워크 액세스 클라이언트에서 인증되지 못했음을 보여줍니다.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

인증 문제를 해결하려면 [SSL VPN-Plus: 설치 실패](#)를 참조하십시오.

기본 로그 분석 - 데이터 경로

데이터 경로 성공

- 다음 로그 출력은 사용자 **a**가 2016년 10월 28일, 0941시에 TCP를 통한 네트워크 액세스 클라이언트로 백엔드 웹 서버 192.168.10.8에 성공적으로 연결되었음을 보여 줍니다.

SVP_LOG_INFO,10-28-2016,09:41:03,TCP

Connect,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,-,-

데이터 경로 실패

- 다음 로그 출력은 사용자 **a**가 2016년 10월 28일, 0941시에 TCP를 통한 네트워크 액세스 클라이언트로 백엔드 웹 서버 192.168.10.8에 연결되지 못했음을 보여 줍니다.

SVP_LOG_INFO,10-28-2016,09:41:03,TCP

Connect,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,-,-

IPSec VPN

다음은 설치 과정에서 발생한 협상 문제를 해결하는 데 유용한 정보입니다.

성공적 협상(1단계 및 2단계)

다음 예에는 NSX Edge와 Cisco 디바이스 간에 성공한 협상 결과가 나와 있습니다.

NSX Edge

NSX Edge 명령줄 인터페이스에서 발췌(ipsec auto -status, part of show service ipsec command):

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L           Role      : responder
Rekey : no           State    : MM_ACTIVE
```

```

Encrypt : 3des      Hash      : SHA
Auth : preshared  Lifetime: 28800
Lifetime Remaining: 28379

```

1단계 정책 불일치

다음은 1단계 정책 불일치 오류 로그를 나타냅니다.

NSX Edge

NSX Edge가 STATE_MAIN_I1 상태에서 작동이 중단되었습니다. `/var/log/messages`를 확인하여 피어가 "NO_PROPOSAL_CHOSEN"이 설정된 IKE 메시지를 다시 전송했음을 나타내는 정보가 있는지 찾습니다.

```

000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
      import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      "s1-c1" #1: ignoring informational payload,
      type NO_PROPOSAL_CHOSEN msgid=00000000

```

Cisco

debug crypto를 사용하도록 설정한 경우 제안이 수락되지 않았음을 보여 주는 오류 메시지가 표시됩니다.

```

ciscoasa# Aug 26 18:17:27 [IKEv1]:
      IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=0) with payloads : HDR + SA (1)
      + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
      types for class Group Description: Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
      types for class Group Description: Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 124

```

```

Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
    All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
    payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
    FSM error history (struct &0xd8355a60) <state>, <event>:
    MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM-->MM_START,
    EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
    MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
    tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
    delete/delete with reason message

```

2단계 불일치

다음은 2단계 정책 불일치 오류 로그를 나타냅니다.

NSX Edge

NSX Edge가 STATE_QUICK_I1 상태에서 작동이 중단되었습니다. 로그 메시지에는 피어가 NO_PROPOSAL_CHOSEN 메시지를 전송했음이 나타납니다.

```

000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
    QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
    idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
    0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
    ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     next payload
    type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
    |     DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     Notify Message
    Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
    ignoring informational payload, type NO_PROPOSAL_CHOSEN
    msgid=00000000

```

Cisco

디버그 메시지에는 1단계가 완료되었지만 정책 협상에 실패하여 2단계가 실패했음이 나타납니다.

```

Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
    IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
    for this connection: DPD

```



```

Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
    Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
    + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
    total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
    Session is being torn down. Reason: Phase 2 Mismatch

```

PFS 불일치

다음은 PFS 불일치 오류 로그를 나타냅니다.

NSX Edge

PFS가 2단계의 일부로 협상되었습니다. PFS가 일치하지 않으면 [2단계 불일치](#)에 설명된 실패 사례와 유사한 동작이 발생합니다.

```

000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
    QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
    idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
    (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      next payload
    type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    |      DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      Notify Message
    Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
    informational payload, type NO_PROPOSAL_CHOSEN
    msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
    91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
    | processing informational NO_PROPOSAL_CHOSEN (14)

```

Cisco

```

<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
    IP = 10.20.129.80, sending delete/delete with
    reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,

```

```

      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
      + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch

```

PSK 불일치

다음은 PSK 불일치 오류 로그를 나타냅니다.

NSX Edge

PSK는 1단계의 마지막 라운드에서 협상됩니다. PSK 협상이 실패할 경우 NSX Edge 상태는 STATE_MAIN_I4가 됩니다. 피어는 INVALID_ID_INFORMATION이 포함된 메시지를 전송합니다.

```

Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
      "s1-c1" #1: transition from state STATE_MAIN_I3 to
      state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      STATE_MAIN_I4: ISAKMP SA established
      {auth=OAKLEY_PRESHARED_KEY
      cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
      Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
      initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
      {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
      pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      ignoring informational payload, type INVALID_ID_INFORMATION
      msgid=00000000

```

Cisco

```

Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
      IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
      + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
      + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
      + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, Received encrypted Oakley Main Mode
      packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)

```

```
+ NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, ERROR, had problems decrypting
packet, probably due to mismatched pre-shared key.
Aborting
```

성공적 협상을 위한 패킷 캡처

아래에는 NSX Edge와 Cisco 디바이스 간의 성공적 협상을 위한 패킷 캡처 세션이 나와 있습니다.

No.	Time	Source	Destination	Protocol	Info
9203	768.394800	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

```
Frame 9203 (190 bytes on wire, 190 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 148
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
  Proposal payload # 0
    Next payload: NONE (0)
    Payload length: 72
    Proposal number: 0
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 2
  Transform payload # 0
    Next payload: Transform (3)
    Payload length: 32
    Transform number: 0
    Transform ID: KEY_IKE (1)
    Life-Type (11): Seconds (1)
    Life-Duration (12): Duration-Value (28800)
    Encryption-Algorithm (1): 3DES-CBC (5)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): 1536 bit MODP group (5)
  Transform payload # 1
    Next payload: NONE (0)
    Payload length: 32
```

```

    Transform number: 1
    Transform ID: KEY_IKE (1)
    Life-Type (11): Seconds (1)
    Life-Duration (12): Duration-Value (28800)
    Encryption-Algorithm (1): 3DES-CBC (5)
    Hash-Algorithm (2): SHA (2)
    Authentication-Method (3): PSK (1)
    Group-Description (4): Alternate 1024-bit MODP group (2)
Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

```

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
    Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
    Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
    Initiator cookie: 92585D2D797E9C52
    Responder cookie: 34704CFC8C8DBD09
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
    Flags: 0x00
    Message ID: 0x00000000
    Length: 104
    Security Association payload
        Next payload: Vendor ID (13)
        Payload length: 52
        Domain of interpretation: IPSEC (1)
        Situation: IDENTITY (1)
        Proposal payload # 1
            Next payload: NONE (0)
            Payload length: 40
            Proposal number: 1
            Protocol ID: ISAKMP (1)
            SPI Size: 0
            Proposal transforms: 1
            Transform payload # 1
                Next payload: NONE (0)
                Payload length: 32
                Transform number: 1
                Transform ID: KEY_IKE (1)
                Encryption-Algorithm (1): 3DES-CBC (5)
                Hash-Algorithm (2): SHA (2)

```

```

Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): PSK (1)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-Value (28800)
Vendor ID: Microsoft L2TP/IPSec VPN Client
Next payload: NONE (0)
Payload length: 24
Vendor ID: Microsoft L2TP/IPSec VPN Client

```

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

```

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data

```

No.	Time	Source	Destination	Protocol Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000

```

```

Length: 256
Key Exchange payload
  Next payload: Nonce (10)
  Payload length: 132
  Key Exchange Data (128 bytes / 1024 bits)
Nonce payload
  Next payload: Vendor ID (13)
  Payload length: 24
  Nonce Data
Vendor ID: CISCO-UNITY-1.0
  Next payload: Vendor ID (13)
  Payload length: 20
  Vendor ID: CISCO-UNITY-1.0
Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Next payload: Vendor ID (13)
  Payload length: 12
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Next payload: Vendor ID (13)
  Payload length: 20
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
Vendor ID: CISCO-CONCENTRATOR
  Next payload: NONE (0)
  Payload length: 20
  Vendor ID: CISCO-CONCENTRATOR

```

No.	Time	Source	Destination	Protocol Info
9207	768.404990	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

```

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted payload (40 bytes)

```

No.	Time	Source	Destination	Protocol Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
  Dst: 10.20.129.80 (10.20.129.80)

```

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 84
  Encrypted payload (56 bytes)
```

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```
Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)
```

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

```
Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
  Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)
```

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```
Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 52
  Encrypted payload (24 bytes)
```


NSX Controller 문제 해결

8

이 섹션에서는 **NSX Controller** 실패의 원인을 식별하고 컨트롤러 문제를 해결하는 방법에 대한 정보를 제공합니다.

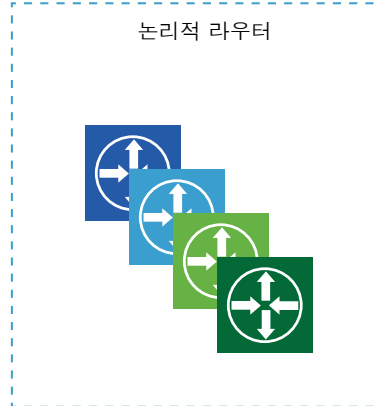
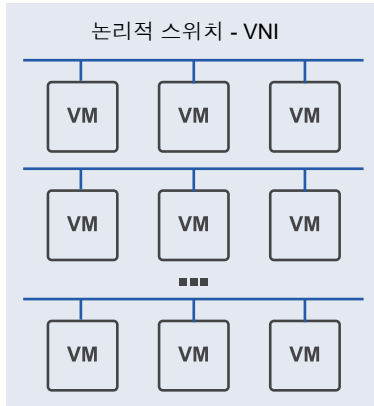
본 장은 다음 항목을 포함합니다.

- 컨트롤러 클러스터 아키텍처의 이해
- **NSX Controller** 배포 문제
- 디스크 지연 시간 문제 해결
- **NSX Controller** 클러스터 오류
- **NSX Controller**의 연결이 끊김
- 제어부 에이전트(**netcpa**) 문제

컨트롤러 클러스터 아키텍처의 이해

NSX Controller 클러스터는 각 컨트롤러 노드에 노드가 구현할 수 있는 작업 유형을 정의하는 역할 집합이 할당되는 스케일아웃 분산 시스템을 나타냅니다. 복원력 및 성능을 위해 컨트롤러 **VM**의 배포는 **3**개의 고유 호스트에서 진행해야 합니다.

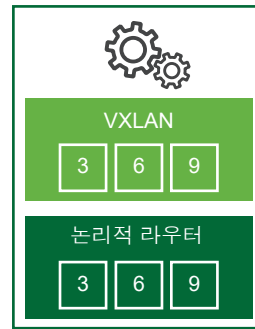
NSX Controller 클러스터 노드 간에 워크로드를 분산하기 위해 샤딩이 사용됩니다. 샤딩은 각 **NSX Controller** 인스턴스가 동일한 작업 부분을 포함하도록 **NSX Controller** 워크로드를 여러 다른 샤드로 나누는 작업입니다.



개체



샤드



여기서는 고유한 컨트롤러 노드가 논리적 스위칭, 논리적 라우팅 및 기타 서비스 등의 지정된 엔티티에 대한 마스터로 작동하는 방식을 보여줍니다. 역할에 대해 마스터 **NSX Controller** 인스턴스가 선택되면 해당 **NSX Controller**는 여러 다른 논리적 스위치 및 라우터를 클러스터의 사용 가능한 모든 **NSX Controller** 인스턴스 간에 나눕니다.

샤드에서 번호가 매겨진 각 상자는 마스터가 워크로드를 나누는 데 사용하는 샤드를 나타냅니다. 논리적 스위치 마스터는 논리적 스위치를 샤드로 나눈 후 이러한 샤드를 여러 다른 **NSX Controller** 인스턴스에 할당합니다. 또한 논리적 라우터에 대한 마스터는 논리적 라우터를 샤드로 나눈 후 이러한 샤드를 여러 다른 **NSX Controller** 인스턴스에 할당합니다.

이러한 샤드는 해당 클러스터의 여러 다른 **NSX Controller** 인스턴스에 할당됩니다. 역할에 대한 마스터는 어떤 샤드에 어떤 **NSX Controller** 인스턴스가 할당되는지를 결정합니다. 요청이 라우터 샤드 3에서 발생하면 샤드는 세 번째 **NSX Controller** 인스턴스에 연결하라는 지시를 받습니다. 요청이 논리적 스위치 샤드 2에서 발생하면 해당 요청은 두 번째 **NSX Controller** 인스턴스에 의해 처리됩니다.

클러스터에서 **NSX Controller** 인스턴스 중 하나가 실패하면 역할에 대한 마스터는 샤드를 사용 가능한 나머지 클러스터로 재분산합니다. 컨트롤러 노드 중 하나가 각 역할에 대한 마스터로 선택됩니다. 마스터는 개별 컨트롤러 노드에 샤드를 할당하는 일을 담당하고 한 노드가 실패할 경우 샤드를 다른 노드로 재배치하는 일을 담당합니다. 또한 마스터는 클러스터 노드의 실패 사실을 **ESXi** 호스트에 알립니다.

각 역할에 대한 마스터를 선택하려면 클러스터의 모든 활성 및 비활성 노드에서 과반수 투표 수를 얻어야 합니다. 주로 이로 인해 컨트롤러 클러스터는 항상 홀수 개수의 노드로 배포되어야 합니다.

ZooKeeper

ZooKeeper는 NSX Controller 클러스터 메커니즘을 담당하는 클라이언트 서버 아키텍처입니다.

ZooKeeper를 사용하여 컨트롤러 클러스터가 검색되고 생성됩니다. 클러스터가 작동된다는 것은 모든 노드에서 ZooKeeper가 작동된다는 것을 의미합니다. ZooKeeper 노드는 선택 프로세스를 거쳐 제어 클러스터를 형성합니다. 클러스터에는 1개의 ZooKeeper 마스터 노드가 있어야 합니다. 이는 노드 간 선택을 통해 수행됩니다.

새 컨트롤러 노드가 생성되면 NSX Manager는 노드 IP 및 ID를 포함하는 노드 정보를 현재 클러스터에 전파합니다. 이와 같이 각 노드는 클러스터링에 사용할 수 있는 전체 노드 수를 알게 됩니다. ZooKeeper 마스터 선택 동안 각 노드는 마스터 노드를 선택하기 위해 한 번씩 투표합니다. 한 노드가 과반수 투표 수를 얻을 때까지 선택이 다시 트리거됩니다. 예를 들어 3개의 노드 클러스터에서 마스터는 2표 이상을 받아야 합니다.

참고 ZooKeeper 마스터를 선택할 수 없는 시나리오를 방지하려면 클러스터의 노드 수가 3개여야 합니다.

- 첫 번째 컨트롤러가 배포될 때는 특수한 경우로, 첫 번째 컨트롤러가 마스터가 됩니다. 이와 같이 컨트롤러를 배포할 때 첫 번째 노드의 배포가 완료되어야만 다른 노드가 추가될 수 있습니다.
- 두 번째 컨트롤러를 추가할 때도 이번에는 노드 수가 짝수이므로 특수한 경우가 됩니다.
- 세 번째 노드가 추가될 경우 클러스터는 지원되는 안정적인 상태에 도달합니다.

ZooKeeper는 한 번에 하나의 실패만 허용할 수 있습니다. 즉, 한 컨트롤러 노드가 다운될 경우 다른 실패가 발생하기 전에 복구해야 합니다. 그렇지 않으면 클러스터 중단과 관련된 문제가 발생할 수 있습니다.

CCP(중앙 제어부) 도메인 관리자

이는 ZooKeeper 위 계층으로, 모든 노드의 ZooKeeper가 시작되기 위한 구성을 제공합니다. 도메인 관리자는 클러스터의 모든 노드 간에 구성을 업데이트한 다음 ZooKeeper 프로세스가 시작되도록 원격 프로시저 호출을 수행합니다.

도메인 관리자는 모든 도메인을 시작하는 일을 담당합니다. 클러스터에 연결하기 위해 CCP 도메인은 다른 시스템의 CCP 도메인과 소통합니다. 클러스터 초기화에 도움이 되는 CCP 도메인의 구성 요소는 **ZK 클러스터 부트스트랩**입니다.

다른 구성 요소와의 컨트롤러 관계

컨트롤러 클러스터는 논리적 스위치, 논리적 라우터 및 VTEP에 대한 정보를 유지하고 ESXi 호스트에 제공하는 역할을 합니다.

논리적 스위치가 생성되면 컨트롤러 노드는 클러스터 내에서 어떤 노드가 해당 논리적 스위치에 대해 *마스터*인지 또는 *소유자*인지를 결정합니다. 논리적 라우터가 추가될 때도 마찬가지입니다.

논리적 스위치 또는 논리적 라우터에 대해 소유권이 설정되면 노드는 해당 스위치 또는 라우터의 전송 영역에 속하는 ESXi 호스트로 해당 소유권을 전송합니다. 소유권의 선택과 호스트로의 소유권 정보 전파 전체를 ‘샤딩’이라고 합니다. 소유권은 노드가 해당 논리적 스위치 또는 논리적 라우터에 대한 모든 NSX 관련 작업을 담당함을 의미합니다. 다른 노드는 해당 논리적 스위치에 대해 어떤 작업도 수행하지 않습니다.

하나의 소유자만 논리적 스위치 및 논리적 라우터의 소스여야 하므로, 둘 이상의 노드가 논리적 스위치 또는 논리적 라우터에 대한 소유자로 선택되면 네트워크의 각 호스트가 논리적 스위치 또는 논리적 라우터의 소스와 관련해서 다른 정보를 가질 수 있으므로 컨트롤러 클러스터가 중단됩니다. 이러한 경우 네트워크 제어부 및 데이터부 작업은 하나의 소스만 가질 수 있으므로 네트워크 중단이 발생합니다.

컨트롤러 노드가 다운되면 클러스터의 나머지 노드는 샤딩을 다시 실행하여 논리적 스위치 및 논리적 라우팅의 소유권을 결정합니다.

NSX Controller 배포 문제

NSX Controller는 NSX Manager에 의해 OVA 형식으로 배포됩니다. 컨트롤러 클러스터가 있으면고가용성이 보장됩니다. 컨트롤러를 배포하려면 NSX Manager, vCenter Server 및 ESXi 호스트에 DNS 및 NTP가 구성되어 있어야 합니다. 정적 IP 풀을 사용하여 각 컨트롤러에 IP 주소를 할당해야 합니다.

별도의 호스트에 NSX Controller를 유지하려면 DRS 선호도 방지 규칙을 구현하는 것이 좋습니다. 3개의 NSX Controller를 배포해야 합니다.

컨트롤러의 일반적인 문제

NSX Controller 배포 중에 발생할 수 있는 일반적인 문제는 다음과 같습니다.

- NSX Controller 배포가 실패합니다.
- NSX Controller에서 클러스터에 연결하지 못합니다.
- `show control-cluster status` 명령을 실행하면 클러스터 대부분에 연결됨과 클러스터 대부분에 대해 연결이 중단된 간의 과반수 상태 플래핑이 표시됩니다.
- NSX 대시보드에 표시되는 연결 상태 문제.
 - `show control-cluster status` 명령은 컨트롤러가 제어 클러스터에 연결되었는지 여부를 확인하기 위한 권장 명령입니다. 각 컨트롤러에 대해 이 명령을 실행하여 전체 클러스터 상태를 확인해야 합니다.

```
controller # show control-cluster status
```

Type	Status	Since
Join status:	Join complete	10/17 18:16:58
Majority status:	Connected to cluster majority	10/17 18:16:46
Restart status:	This controller can be safely restarted	10/17 18:16:51
Cluster ID:	af2e9dec-19b9-4530-8e68-944188584268	
Node UUID:	af2e9dec-19b9-4530-8e68-944188584268	
Role	Configured status Active status	

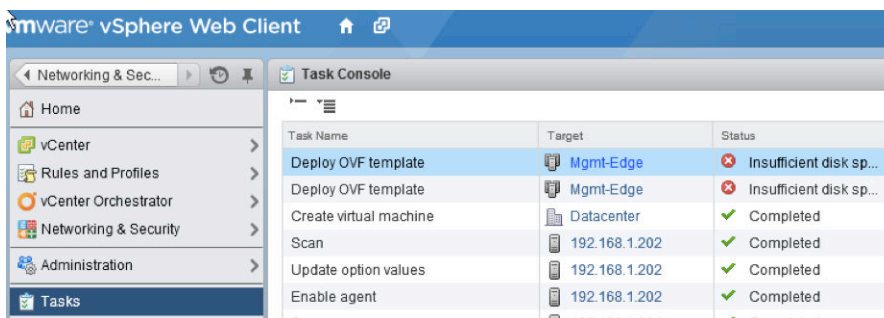
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
dht_node	enabled	activated

참고 컨트롤러 노드의 연결이 끊어지면 **join cluster** 또는 **force join** 명령을 사용하지 마십시오. 이 명령은 클러스터에 노드를 연결하기 위한 것이 아닙니다. 이 명령을 수행하면 클러스터는 완전히 불확실한 상태가 될 수 있습니다.

클러스터 시작 노드는 클러스터 멤버에게 멤버가 시작될 때 확인할 위치에 대한 정보를 제공하는 힌트일 뿐입니다. 이 목록에 더 이상 서비스되지 않는 클러스터 멤버가 포함되어 있더라도 안심하십시오. 이는 클러스터 기능에 영향을 미치지 않습니다.

모든 클러스터 멤버는 동일한 클러스터 ID를 가져야 합니다. 그러지 않으면 클러스터가 중단된 상태가 되므로 VMware 기술 지원 팀을 통해 복구해야 합니다.

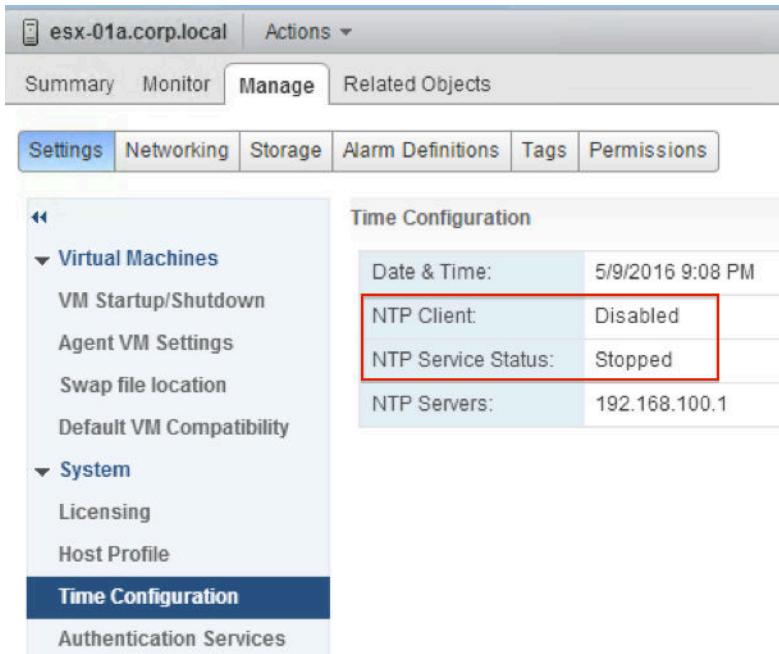
- **show control-cluster startup-nodes** 명령은 클러스터에 현재 있는 모든 노드를 표시하기 위한 것이 아닙니다. 대신, 이 명령은 컨트롤러 프로세스가 다시 시작될 때 이 노드에서 멤버 자격을 클러스터에 부트스트랩하는 데 사용하는 다른 컨트롤러 노드를 표시합니다. 따라서 명령 출력에는 종료되었거나 클러스터에서 삭제된 일부 노드가 표시될 수 있습니다.
- 또한 **show control-cluster network ipsec status** 명령을 사용하여 IPsec(인터넷 프로토콜 보안) 상태를 조사할 수 있습니다. 컨트롤러가 몇 분에서 몇 시간 동안 서로 통신할 수 없으면 **cat /var/log/syslog | egrep "sending DPD request|IKE_SA"** 명령을 실행하고 로그 메시지가 트래픽이 없음을 나타내는지 확인합니다. **ipsec statusall | egrep "bytes_i|bytes_o"** 명령을 실행하고 설정된 2개의 IPsec 터널이 없는지 확인할 수도 있습니다. VMware 기술 지원 담당자에게 의심되는 제어 클러스터 문제를 보고할 때 이러한 명령의 출력과 컨트롤러 로그를 제공합니다.
- NSX Manager와 NSX Controller 간 IP 연결 문제. 이 문제는 일반적으로 물리적 네트워크 연결 문제 또는 방화벽의 통신 차단으로 인해 발생합니다.
- vSphere에서 사용 가능한 스토리지와 같이 컨트롤러를 호스팅하기 위한 리소스 부족. 컨트롤러 배포 중에 vCenter 이벤트 및 작업 로그를 확인하면 이러한 문제를 식별할 수 있습니다.



Task Name	Target	Status
Deploy OVF template	Mgmt-Edge	✗ Insufficient disk sp...
Deploy OVF template	Mgmt-Edge	✗ Insufficient disk sp...
Create virtual machine	Datacenter	✓ Completed
Scan	192.168.1.202	✓ Completed
Update option values	192.168.1.202	✓ Completed
Enable agent	192.168.1.202	✓ Completed

- "rogue" 컨트롤러가 잘못 동작하거나 업그레이드된 컨트롤러가 **연결 해제됨(Disconnected)** 상태입니다.

- ESXi 호스트 및 NSX Manager의 DNS가 제대로 구성되지 않았습니다.
- ESXi 호스트의 NTP와 NSX Manager가 동기화되지 않았습니다.



- 새로 연결된 VM이 네트워크에 액세스할 수 없으면 제어부 문제일 수 있습니다. 컨트롤러 상태를 확인합니다.

또한 ESXi 호스트에서 `esxcli network vswitch dvs vmware vxlan network list --vds-name <name>` 명령을 실행하여 제어부 상태를 확인하십시오. 컨트롤러 연결이 끊어져 있는지 확인하십시오.

```
/etc/vmware/netcpa # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane Controller Connection
ARP Entry Count MTEP Count
-----
5000 N/A (headend replication) Enabled (multicast proxy, ARP proxy) 192.168.110.203 (down)
```

- `show log manager follow NSX Manager CLI` 명령을 실행하면 컨트롤러 배포 실패에 대한 다른 원인을 파악할 수 있습니다.

```
2014-02-26 10:09:44.931 GMT INFO taskScheduler-25 VcConnection$VimClient:1219 - Create stub for com.vmware.vim.binding
28c5157-abf3-718e-88c5-42209f389211
2014-02-26 10:09:44.932 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:301 - got prop collector up
ctReference: type = PropertyFilter, value = session[d46b86a2-7a10-c17e-6ebe-8ab252ee4efd]527420f2-bdd7-529b-8ab6-17d16
6E3-4A64-96D7-5833C287588F
2014-02-26 10:09:44.937 GMT ERROR taskScheduler-25 VcUtils:184 - Error while waiting for property collector updates.
com.vmware.vim.binding.vim.fault.NoDiskSpace:
datastore = datastore1 (1)
inherited from com.vmware.vim.binding.vim.fault.FileFault:
file = [datastore1 (1)] NSX_Controller_1c3dd18d-0cd3-4d7d-896b-51247176ae77/NSX_Controller_1c3dd18d-0cd3-4d7d-896b-512
inherited from com.vmware.vim.binding.vim.fault.VimFault:
inherited from com.vmware.vim.binding.vim.fault.NoDiskSpace: Insufficient disk space on datastore 'datastore1 (1)'.
```

호스트 연결 문제

다음 명령을 사용하여 호스트 연결 오류를 확인합니다. 각 컨트롤러 노드에 대해 다음 명령을 실행합니다.

- `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by host_IP` 명령을 사용하여 비정상 오류 통계를 확인합니다.
- 다음 명령을 사용하여 논리적 스위치/라우터 메시지 통계 또는 높은 메시지 속도를 확인합니다.
 - `show control-cluster core stats`: 전체 통계
 - `show control-cluster core stats-sample`: 최신 통계 샘플
 - `show control-cluster core connection-stats ip`: 연결별 통계
 - `show control-cluster logical-switches stats`
 - `show control-cluster logical-routers stats`
 - `show control-cluster logical-switches stats-sample`
 - `show control-cluster logical-routers stats-sample`
 - `show control-cluster logical-switches vni-stats vni`
 - `show control-cluster logical-switches vni-stats-sample vni`
 - `show control-cluster logical-switches connection-stats ip`
 - `show control-cluster logical-routers connection-stats ip`
- `show host hostID health-status` 명령을 사용하여 준비된 클러스터에 있는 호스트의 상태를 확인할 수 있습니다. 컨트롤러 문제 해결을 위해 다음 상태 검사가 지원됩니다.
 - `net-config-by-vsm.xml`이 컨트롤러 목록과 동기화되는지 확인합니다.
 - 컨트롤러에 대한 소켓 연결이 있는지 확인합니다.
 - VNI(VXLAN 네트워크 식별자)가 생성되었는지와 구성이 올바른지 확인합니다.
 - VNI가 마스터 컨트롤러에 연결되는지 확인합니다(제어부가 사용되도록 설정된 경우).

설치 및 배포 문제

- 클러스터에 3개 이상의 컨트롤러 노드가 배포되었는지 확인합니다. VMware에서는 네이티브 vSphere 반선호도 규칙을 활용하여 동일한 ESXi 호스트에 둘 이상의 컨트롤러 노드가 배포되지 않도록 하는 것을 권장합니다.
- 모든 NSX Controller에 연결된 상태가 표시되는지 확인합니다. 컨트롤러 노드에 연결 해제된 상태가 표시되면 모든 컨트롤러 노드에 대해 `show control-cluster status` 명령을 실행하여 다음 정보가 일관적인지 확인합니다.

유형	상태
연결 상태	연결 완료
과반수 상태	클러스터 대부분에 연결됨
클러스터 ID	모든 컨트롤러 노드에 대한 동일한 정보

- 모든 컨트롤러 노드에서 모든 역할이 일관되는지 확인합니다.

역할	구성된 상태	활성 상태
api_provider	사용	활성화됨
persistence_server	사용	활성화됨
switch_manager	사용	활성화됨
logical_manager	사용	활성화됨
directory_server	사용	활성화됨

- `vnet-controller` 프로세스가 실행 중인지 확인합니다. 모든 컨트롤러 노드에서 `show process` 명령을 실행하고 `java-dir-server` 서비스가 실행되고 있는지 확인합니다.
- 클러스터 기록을 확인하고 호스트 연결 플래핑 또는 VNI 연결 실패 및 비정상 클러스터 멤버 자격 변경 표시가 없는지 확인합니다. 이를 확인하려면 `show control-cluster history` 명령을 실행합니다. 또한 이 명령은 노드가 자주 다시 시작되는지 여부도 표시합니다. 크기가 0이고 다른 프로세스 ID를 갖는 많은 로그 파일이 없는지 확인합니다.
- VNI(VXLAN 네트워크 식별자)가 구성되어 있는지 확인합니다. 자세한 내용은 VMware VXLAN Deployment Guide의 VXLAN 준비 단계 섹션을 참조하십시오.
- 컨트롤러 클러스터에서 SSL이 사용되도록 설정되어 있는지 확인합니다. 각 컨트롤러 노드에 대해 `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by sslEnabled` 명령을 실행합니다.

디스크 지연 시간 문제 해결

관리(Management) 탭에서 디스크 지연 시간 경고를 볼 수 있습니다. NSX Controller는 낮은 지연 시간을 가진 디스크에서 작동해야 합니다.

디스크 지연 시간 경고 보기

디스크 지연 시간 경고는 디스크 가용성 또는 지연 시간 문제를 모니터링하고 보고합니다. 각 NSX Controller에 대해 디스크 지연 시간 세부 정보를 볼 수 있습니다. 읽기 지연 시간 및 쓰기 지연 시간 계산 결과는 5초(기본값) 이동 평균에 입력됩니다. 이 값은 지연 시간 제한을 위반할 때 경고를 트리거하는 데 사용됩니다. 평균 시간이 낮은 워터마크에 도달하면 경고가 해제됩니다. 기본적으로 높은 워터마크는 200ms로, 낮은 워터마크는 100ms로 설정됩니다. 높은 지연 시간은 각 컨트롤러 노드에서 분산 클러스터링 애플리케이션 작업에 영향을 미칩니다.







NSX Controller에 대한 디스크 지연 시간 경고를 보려면 다음 절차를 수행합니다.



사전 요구 사항

지연 시간 제한에 도달했습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **설치(Installation)**를 클릭합니다.
- 3 **관리(Management)**에서 필요한 컨트롤러로 이동한 후 **디스크 경고(Disk Alert)** 링크를 클릭합니다.
디스크 지연 시간 경고 창이 나타납니다.

192.168.110.33 - Disk Latency Alerts				
Device Name	Latency Type	Refresh Time	Last Latency (ms)	Average Latency (ms)
 sda	Write	9/26/2016 2:15 PM	3.2	7.906
 sda	Read	9/26/2016 1:08 PM	0.0	0.0
 dm-1	Write	9/16/2016 5:11 PM	0.0	0.0
 dm-1	Read	9/22/2016 4:31 PM	0.0	0.0
 dm-0	Write	9/26/2016 2:15 PM	3.64	9.822
 dm-0	Read	9/26/2016 10:05 AM	0.0	33.334
6 items				

5	 Disk Alert	192.168.110.15	✓ Connected	 Disk Alert
---	--	----------------	-------------	--

결과

선택한 컨트롤러에 대한 지연 시간 세부 정보를 볼 수 있습니다. `cloudnet/run/iostat/iostat_alert.log` 파일에 7일 동안 경고 로그가 저장됩니다. `show log cloudnet/run/iostat/iostat_alert.log` 명령을 사용하여 로그 파일을 표시할 수 있습니다.

다음에 수행할 작업

디스크 지연 시간 문제 해결에 대한 자세한 내용은 [디스크 지연 시간 문제](#)를 참조하십시오.

로그 메시지에 대한 자세한 내용은 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.

디스크 지연 시간 문제

컨트롤러는 낮은 지연 시간을 가진 디스크에서 작동해야 합니다. 클러스터는 각 노드에 대한 디스크 스토리지 시스템이 **300ms**보다 작은 최대 쓰기 지연 시간과 **100ms**보다 작은 평균 쓰기 지연 시간을 갖도록 요구합니다.

문제

- 배포된 **NSX Controller**의 연결이 컨트롤러 클러스터에서 끊깁니다.
- 디스크 파티션이 꽉 차 있으므로 컨트롤러 로그를 수집할 수 없습니다.
- 스토리지 시스템이 이러한 요구 사항을 충족하지 못하면 클러스터가 불안정해지며 시스템 다운타임이 발생할 수 있습니다.
- 작동하는 **NSX Controller**에 적용되는 TCP 수신기는 더 이상 **show network connections of-type tcp** 명령의 출력에 나타나지 않습니다.
- 연결이 끊긴 컨트롤러는 유효하지 않은, 모두 0으로 구성된 **UUID**를 사용하여 클러스터에 연결하려고 합니다.
- **show control-cluster history** 명령을 실행하면 다음과 비슷한 메시지가 표시됩니다.

```
INFO.20150530-000550.1774:D0530 13:25:29.452639 1983 zookeeper_client.cc:774] Zookeeper client disconnected!
```

- **NSX Controller** 콘솔에서 **show log cloudnet/cloudnet_java-zookeeper*.log** 명령을 실행하면 다음과 비슷한 항목이 포함됩니다.

```
cloudnet_java-zookeeper.20150530-000550.1806.log-2015-05-30
13:25:07,382 47956539 [SyncThread:1] WARN
org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead
log in SyncThread:1 took 3219ms which will adversely effect operation latency.
See the ZooKeeper troubleshooting guide
```

- **NSX Controller** 로그에는 다음과 비슷한 항목이 포함됩니다.

```
D0525 13:46:07.185200 31975
rpc-broker.cc:369] Registering address resolution for: 20.5.1.11:7777
D0525 13:46:07.185246 31975
rpc-tcp.cc:548] Handshake complete, both peers support the same
protocol
D0525 13:46:07.197654 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
D0525 13:46:07.222869 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
```

원인

이 문제는 디스크 성능 저하로 인해 발생할 수 있으며 NSX Controller 클러스터에 좋지 않은 영향을 미칩니다.

- `/var/log/cloudnet/cloudnet_java-zookeeper log` 파일에서 **fsync** 메시지를 찾아 느린 디스크를 확인합니다. **fsync**가 1초보다 오래 걸리면 ZooKeeper는 **fsync** 경고 메시지를 표시하며, 이는 디스크가 너무 느리다는 의미입니다. VMware에서는 제어 클러스터용으로 LUN(논리적 단위 번호)을 특별히 지정하고, 지연 시간 측면에서 제어 클러스터에 더 가깝게 스토리지 어레이를 이동하는 것을 권장합니다.
- 5초(기본값) 이동 평균에 입력된 읽기 지연 시간 및 쓰기 지연 시간 계산을 볼 수 있습니다. 이 값은 지연 시간 제한을 위반할 때 경고를 트리거하는 데 사용됩니다. 평균 시간이 낮은 워터마크에 도달하면 경고가 해제됩니다. 기본적으로 높은 워터마크는 200ms로, 낮은 워터마크는 100ms로 설정됩니다. `show disk-latency-alert config` 명령을 사용할 수 있습니다. 출력은 다음과 같이 표시됩니다.

```
enabled=True    low-wm=51      high-wm=150
nsx-controller # set disk-latency-alert enabled yes
nsx-controller # set disk-latency-alert low-wm 100
nsx-controller # set disk-latency-alert high-wm 200
```

- GET `/api/2.0/vdn/controller/<controller-id>/systemStats` REST API를 사용하여 컨트롤러 노드의 지연 시간 경고 상태를 가져옵니다.
- GET `/api/2.0/vdn/controller` REST API를 사용하여 디스크 지연 시간 경고가 컨트롤러 노드에서 감지되는지 여부를 나타냅니다.

해결책

- 1 지연 시간이 낮은 디스크에 NSX Controller를 배포합니다.
- 2 각 컨트롤러는 자체 디스크 스토리지 서버를 사용해야 합니다. 두 컨트롤러 간에 동일한 디스크 스토리지 서버를 공유하지 마십시오.

다음에 수행할 작업

경고를 보는 방법에 대한 자세한 내용은 [디스크 지연 시간 경고 보기](#)를 참조하십시오.

NSX Controller 클러스터 오류

클러스터의 NSX Controller 노드 중 하나가 실패해도 두 개의 컨트롤러는 계속 작동합니다. 클러스터 과반수가 유지되고 제어부가 계속 작동합니다.

문제

NSX Controller 클러스터가 실패했습니다.

해결책

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**에서 **설치 > 관리(Installation > Management)**를 클릭합니다.

- 3 NSX Controller 노드 섹션에서 [피어] 열을 확인합니다. [피어] 열에 녹색 상자가 표시되면 클러스터의 피어 컨트롤러 연결에 오류가 없는 것입니다. 빨간색 상자는 피어에 오류가 있는 것을 나타냅니다. 세부 정보를 보려면 이 상자를 클릭합니다.
- 4 컨트롤러 클러스터에서 [피어] 열에 문제가 표시되면 각 NSX Controller CLI로 로그인하여 자세한 진단을 수행합니다. `show control-cluster status` 명령을 실행하여 각 컨트롤러의 상태를 진단합니다. 클러스터의 모든 컨트롤러는 동일한 클러스터 UUID를 갖지만 클러스터 UUID가 마스터 컨트롤러의 UUID와 같지 않을 수 있습니다. [NSX Controller 배포 문제](#)에 설명된 대로 배포 문제에 대한 정보를 확인할 수 있습니다.
- 5 컨트롤러 노드 또는 컨트롤러 클러스터를 다시 배포하기 전에 다음 단계를 사용하여 문제를 해결할 수 있습니다.
 - a 컨트롤러의 전원이 켜져 있는지 확인합니다.
 - b 영향받은 컨트롤러에서 다른 노드 및 관리자로 또는 영향받은 컨트롤러로 ping을 수행합니다. 네트워크 문제가 발견되면 [NSX Controller 배포 문제](#)의 설명대로 해결하십시오.
 - c 다음 CLI 명령을 사용하여 IPsec(인터넷 프로토콜 보안) 상태를 확인합니다.
 - `show control-cluster network ipsec status` 명령을 사용하여 IPsec가 사용되도록 설정되었는지 확인합니다.
 - `show control-cluster network ipsec tunnels` 명령을 사용하여 IPsec 터널의 상태를 확인합니다.

IPsec 상태 정보를 사용하여 VMware 기술 지원 팀의 티켓을 열 수도 있습니다.
 - d 문제가 네트워크 문제가 아닌 경우 재부팅할지 또는 다시 배포할지를 선택할 수 있습니다.

노드를 재부팅하려는 경우 한번에 한 컨트롤러만 재부팅해야 합니다. 하지만 컨트롤러 클러스터가 둘 이상의 컨트롤러 노드가 실패한 상태이면 모든 컨트롤러 클러스터를 동시에 재부팅합니다. 정상 클러스터에서 노드를 재부팅할 때는 항상 그 이후에 클러스터가 재구성되는지 확인한 다음, 클러스터 리사딩이 제대로 수행되었는지 확인합니다.
- 6 컨트롤러를 다시 배포하기로 결정한 경우 다음 두 가지 방법 중 하나를 사용합니다.
 - 방법 1: 손상된 컨트롤러 노드를 삭제하고 새 컨트롤러 노드를 다시 배포합니다.
 - 방법 2: 컨트롤러 클러스터를 삭제하고 새 컨트롤러 클러스터를 다시 배포합니다.

VMware에서는 두 번째 방법을 권장합니다.

다음에 수행할 작업

다음 방법 중 하나를 선택합니다.

- 방법 1: 손상된 컨트롤러 삭제 및 새 컨트롤러 다시 배포
- 방법 2: NSX Controller 클러스터 다시 배포

방법 1: 손상된 컨트롤러 삭제 및 새 컨트롤러 다시 배포

먼저 새 **NSX Controller** 클러스터를 다시 배포하지 않고 문제 해결을 시도할 수 있습니다. 이 방법에서는 먼저 손상된 **NSX Controller** 노드를 삭제한 다음, 새 **NSX Controller** 노드를 배포합니다.

절차

1 NSX Controller 삭제

NSX Controller를 강제로 또는 정상적으로 삭제할 수 있습니다. 정상적인 제거 절차에서는 노드를 제거하기 전에 다음 조건을 확인합니다.

2 NSX Controller 다시 배포

손상된 컨트롤러 노드를 삭제한 후에는 새 컨트롤러 노드를 배포합니다.

NSX Controller 삭제

NSX Controller를 강제로 또는 정상적으로 삭제할 수 있습니다. 정상적인 제거 절차에서는 노드를 제거하기 전에 다음 조건을 확인합니다.

- 현재 **NSX Controller** 노드 업그레이드 작업이 없습니다.
- 컨트롤러 클러스터가 정상 상태이고 컨트롤러 클러스터 **API** 요청을 처리할 수 있습니다.
- **vCenter Server** 인벤토리에서 가져온 호스트 상태가 연결됨 및 전원 켜짐을 표시합니다.
- 마지막 컨트롤러 노드가 아닙니다.

강제 제거 절차에서는 컨트롤러 노드를 제거하기 전에 위에 언급된 조건을 확인하지 않습니다.

- 컨트롤러를 삭제할 때 기억해 둘 사항:
 - **vSphere Web Client UI** 또는 **API**를 통해 삭제하기 전에 컨트롤러 **VM**을 삭제하려고 시도하지 마십시오. **UI**를 사용할 수 없으면 **DELETE /2.0/vdn/controller/{controllerId}** **API**를 사용하여 컨트롤러를 삭제하십시오.
 - 노드 삭제 후에 기존 클러스터가 안정적인 상태인지 확인합니다.
 - 클러스터의 모든 노드를 삭제할 경우 마지막으로 남은 노드는 **컨트롤러 강제 제거(Forcely remove the controller)** 옵션을 사용하여 삭제해야 합니다. 항상 컨트롤러 **VM**이 성공적으로 삭제되었는지 확인합니다. 삭제되지 않은 경우 수동으로 **VM** 전원을 끄고 **UI**를 사용하여 컨트롤러 **VM**을 삭제하십시오.
 - 삭제 작업이 실패하는 경우 **VM**을 삭제할 수 없습니다. 이러한 경우 **컨트롤러 강제 제거(Forcely remove the controller)** 옵션을 사용하여 **UI**를 통해 컨트롤러 삭제를 호출하십시오. **API**의 경우 **forceRemoval** 매개 변수를 **true**로 설정하십시오. 강제 제거 후에 수동으로 **VM** 전원을 끄고 **UI**를 사용하여 컨트롤러 **VM**을 삭제하십시오.
 - 다중 노드 클러스터는 1번의 실패만 허용할 수 있으므로 삭제는 실패 횟수로 계산됩니다. 다른 실패가 발생하기 전에 삭제된 노드를 재배포해야 합니다.

■ 크로스 vCenter NSX 환경:

- vCenter Server에서 직접 컨트롤러 VM을 삭제하거나 전원을 끄는 작업은 지원되지 않습니다. **상태(Status)** 열에 **동기화되지 않음(Out of sync)** 상태가 표시됩니다.
- 컨트롤러 삭제가 부분적으로만 성공하고 항목이 크로스 vCenter NSX 환경의 NSX Manager 데이터베이스에 남아 있으면 DELETE api/2.0/vdn/controller/external API를 사용합니다.
- 컨트롤러를 NSX Manager API를 통해 가져온 경우 removeExternalControllerReference API와 forceRemoval 옵션을 함께 사용합니다.
- 컨트롤러가 삭제되면 NSX는 VM의 MOID(관리 개체 ID)를 사용하여 vCenter Server를 통해 컨트롤러 VM을 삭제할 것을 요청합니다. vCenter Server가 해당 MOID로 VM을 찾을 수 없으면 NSX는 컨트롤러 삭제 요청에 대해 실패를 보고하고 작업을 중단합니다.

강제 삭제(Forcefully Delete) 옵션이 선택되면 NSX는 컨트롤러 삭제 작업을 중단하지 않고 컨트롤러의 정보를 지웁니다. 또한 NSX는 삭제된 컨트롤러를 더 이상 신뢰하지 않도록 모든 호스트를 업데이트합니다. 그렇지만 컨트롤러 VM이 여전히 활성 상태이고 다른 MOID를 사용하여 실행되는 경우에는 컨트롤러 클러스터의 멤버로 참여하기 위한 자격 증명이 여전히 있는 것입니다. 이 시나리오에서 ESXi 호스트는 더 이상 삭제된 컨트롤러를 신뢰하지 않으므로 이 컨트롤러 노드에 할당된 논리적 스위치 또는 라우터는 제대로 작동하지 않습니다.

NSX Controller를 삭제하려면 다음 절차를 수행합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **설치(Installation)**를 클릭합니다.
- 3 **관리(Management)**에서 삭제하려는 컨트롤러를 선택합니다.
- 4 **삭제(x)(Delete (x))** 아이콘을 클릭합니다.
- 5 **삭제(Delete)** 또는 **강제 삭제(Forcefully Delete)**를 선택합니다.
 - ◆ **강제 삭제(Forcefully Delete)** 옵션을 선택하는 경우 컨트롤러는 정상적이지 않게 강제로 삭제됩니다. 이 옵션은 모든 실패를 무시하고 데이터베이스에서 데이터를 지웁니다. 가능한 실패가 수동으로 처리되도록 해야 합니다. 컨트롤러 VM이 삭제되었는지 확인해야 합니다. 그렇지 않은 경우 vCenter Server를 통해 삭제해야 합니다.

참고 클러스터의 마지막 컨트롤러를 삭제하는 경우 **강제 삭제(Forcefully Delete)** 옵션을 선택하여 마지막 컨트롤러 노드를 제거해야 합니다. 시스템에 컨트롤러가 없는 경우 호스트가 "헤드리스" 모드로 작동 중인 것입니다. 새 컨트롤러가 배포되고 동기화가 완료될 때까지는 새 VM 또는 vMotion으로 이동한 VM에서 네트워킹 문제가 발생합니다.

- ◆ 이 옵션을 선택하지 않을 경우 컨트롤러가 정상적으로 삭제됩니다.

- 6 예(Yes)**를 클릭합니다. 정상적인 컨트롤러 삭제에서는 다음 순서대로 작업이 진행됩니다.
- 노드의 전원을 끕니다.
 - 클러스터 상태를 확인합니다.
 - 클러스터가 정상 상태가 아니면 컨트롤러의 전원을 켜고 제거 요청을 삭제합니다.
 - 클러스터가 정상 상태인 경우 컨트롤러의 VM을 제거하고 노드의 IP 주소를 해제합니다.
 - 클러스터에서 컨트롤러 VM의 ID를 제거합니다.
- 선택된 컨트롤러가 삭제됩니다.
- 7 작업 > 컨트롤러 상태 업데이트(Actions > Update Controller State)**를 클릭하여 컨트롤러 상태를 재 동기화합니다.

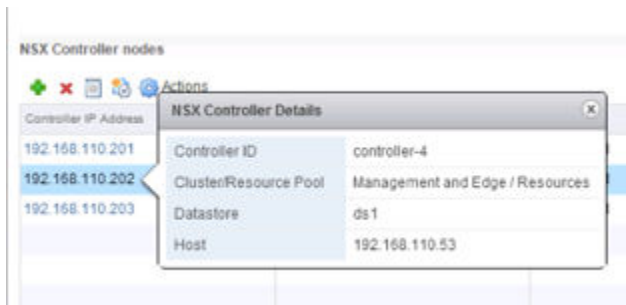
NSX Controller 다시 배포

손상된 컨트롤러 노드를 삭제한 후에는 새 컨트롤러 노드를 배포합니다.

절차

- vSphere Web Client에 로그인합니다.
- Networking & Security**에서 **설치 > 관리(Installation > Management)**를 클릭합니다.
- NSX Controller 노드** 섹션에서 영향을 받는 컨트롤러를 클릭합니다. 나중에 참조하기 위해 스크린샷을 생성하거나 **NSX Controller 세부 정보** 화면의 구성 정보를 기록해 둡니다.

예:



- 노드 추가(+)(Add Node (+))** 아이콘을 클릭하여 새 NSX Controller 노드를 배포합니다.
- [컨트롤러 추가] 대화상자에서 노드를 추가할 데이터 센터를 선택하고 컨트롤러 설정을 구성합니다.
 - 적절한 클러스터를 선택합니다.
 - 클러스터 및 스토리지에서 [호스트]를 선택합니다.
 - 분산 포트 그룹을 선택합니다.
 - 노드에 할당할 IP 주소가 포함된 IP 풀을 선택합니다.
 - 확인(OK)**을 클릭하고 설치가 완료될 때까지 기다린 후 노드가 **정상** 상태인지 확인합니다.

컨트롤러 노드 추가에 대한 자세한 내용은 "NSX 설치 가이드"의 "NSX Controller 클러스터 배포"를 참조하십시오.

6 작업 > 컨트롤러 상태 업데이트를 클릭하여 컨트롤러 상태를 재동기화합니다.

[컨트롤러 상태 업데이트]는 NSX Manager의 현재 VXLAN 및 논리적 분산 라우터 구성(크로스 vCenter NSX 배포의 범용 개체 포함)을 컨트롤러 클러스터로 푸시합니다.

방법 2: NSX Controller 클러스터 다시 배포

이 방법에서는 세 개의 컨트롤러 노드를 모두 삭제하고 새 컨트롤러 노드를 추가하여 전기능 3노드 클러스터를 유지합니다.

다음 조건 중 하나라도 해당하는 경우 NSX Controller 클러스터를 삭제하는 것이 좋습니다.

- 하나 이상의 컨트롤러 노드에 치명적이거나 복구할 수 없는 오류가 발생합니다.
- 컨트롤러 가상 시스템을 액세스할 수 없으며 수정할 수도 없습니다.

이러한 경우 일부 컨트롤러 노드가 정상 상태로 보이더라도 모든 컨트롤러 노드를 삭제하는 것이 좋습니다.

새 컨트롤러 클러스터를 다시 배포한 다음, NSX Manager에서 컨트롤러 상태 메커니즘을 업데이트합니다. 컨트롤러 상태를 업데이트하면 VXLAN이 재동기화되고 논리적 분산 라우터가 다시 배포됩니다.

절차

1 vSphere Web Client에 로그인합니다.

2 네트워킹 및 보안 > 설치 > 관리로 이동합니다.

3 NSX Controller 노드 섹션에서 세 개의 컨트롤러 노드를 모두 삭제합니다. 한번에 하나의 노드를 선택하고 삭제(✖) 아이콘을 클릭합니다.

시스템에 컨트롤러가 없으면 호스트가 "헤드리스" 모드에서 작동합니다. 새 컨트롤러가 배포되고 동기화가 완료될 때까지는 새 가상 시스템 또는 마이그레이션 가상 시스템에서 네트워킹 문제가 발생합니다.

4 새 컨트롤러 노드 3개를 배포하여 전기능 NSX Controller 클러스터를 생성합니다.

컨트롤러 클러스터 추가에 대한 자세한 내용은 "NSX 설치 가이드"의 "NSX Controller 클러스터 배포"를 참조하십시오.

5 작업 > 컨트롤러 상태 업데이트를 클릭하여 컨트롤러 상태를 재동기화합니다.

가상 컨트롤러

가상 컨트롤러는 클러스터에 참여하거나 참여하지 않을 수 있는 라이브 컨트롤러 VM(가상 시스템) 또는 존재하지 않는 VM일 수 있습니다. NSX Manager는 vCenter Server 인벤토리의 모든 VM 목록을 동기화합니다. 가상 컨트롤러는 vCenter Server 또는 호스트가 NSX Manager의 요청 없이 컨트롤러 VM을 삭제하거나 vCenter Server 인벤토리가 컨트롤러 VM의 참조 MOID를 변경할 때 생성됩니다.

컨트롤러가 NSX에서 생성되면 구성 정보가 NSX Manager 내부에 저장됩니다. NSX Manager는 vCenter Server를 통해 새 컨트롤러 VM을 배포합니다.

NSX 관리자는 컨트롤러를 생성하기 위해 NSX Manager에 대한 IP 주소 풀을 포함하는 구성을 제공합니다. NSX Manager는 풀에서 IP 주소를 제거하고, 컨트롤러 구성의 나머지와 해당 IP를 vCenter Server에 대한 VM 생성 요청으로서 푸시합니다. NSX Manager는 vCenter Server에서 요청의 상태를 확인할 때까지 기다립니다.

- **The controller creation process was successful:** 컨트롤러 VM이 성공적으로 생성되면 vCenter Server는 컨트롤러 VM을 시작합니다. NSX Manager는 나머지 컨트롤러 구성 정보와 함께 VM의 MOID(관리 개체 ID)를 저장합니다. MOID(또는 MO-REF)는 vCenter가 해당 인벤토리의 모든 개체에 할당하는 고유한 식별자입니다. 또한 vCenter Server는 이 MOID를 통해 VM을 추적하여 VM이 vCenter Server 인벤토리의 일부로 남아 있는지 확인합니다.
- **The controller creation process was not successful:** IP 및 네트워크 연결 구성이 잘못된 경우 NSX Manager에서 vCenter Server에 연결하지 못할 수 있습니다. NSX Manager는 미리 설정된 시간 동안 대기했다가 활성 클러스터에 참여할 단일 노드 컨트롤러 클러스터(첫 번째의 경우) 또는 새 컨트롤러를 생성합니다. 타이머가 만료되면 NSX Manager는 vCenter Server에 VM을 삭제하도록 요청합니다. IP 주소가 풀로 다시 반환되고 NSX는 컨트롤러 생성 실패를 선언합니다.

가상 컨트롤러가 생성되는 방식

NSX Manager가 컨트롤러 삭제를 요청하는 경우 vCenter Server는 MOID를 사용하여 삭제할 컨트롤러를 VM을 찾습니다.

그러나 vCenter 작업으로 인해 vCenter Server 인벤토리에서 컨트롤러 VM이 제거되면 vCenter는 해당 데이터베이스에서 MOID를 제거합니다. 컨트롤러 VM은 vCenter 인벤토리에서 제거된 후에도 NSX Manager에서 여전히 작동되며 활성 상태를 유지할 수 있습니다. 하지만 vCenter Server의 입장에서는 컨트롤러 VM이 더 이상 존재하지 않게 됩니다. vCenter Server가 해당 인벤토리에서 VM을 제거하더라도 VM이 삭제되지 않을 수 있습니다. VM이 여전히 활성 상태인 경우 NSX 컨트롤러 클러스터에 참여하고 있거나 참여하려고 시도하게 됩니다.

다음은 가상 컨트롤러가 생성되는 방법의 가장 일반적인 예입니다.

- vCenter Server 관리자가 인벤토리에서 컨트롤러 VM을 포함하는 호스트를 제거합니다. 나중에 호스트를 다시 추가합니다. 호스트가 제거될 때 vCenter Server가 호스트와 연결된 MOID 및 포함된 VM을 모두 삭제합니다. 호스트가 나중에 다시 추가되면 vCenter Server가 호스트 및 VM에 새로운 MOID를 할당합니다. NSX 사용자에게는 호스트와 VM이 여전히 동일하지만 vCenter Server의 관점에서는 호스트와 VM이 완전히 새로운 개체입니다. 그러나 실질적으로 해당 호스트와 VM은 여전히 같다고 볼 수 있습니다. 호스트 및 VM 내에서 실행되는 애플리케이션은 달라지지 않습니다.
- vCenter Server 관리자가 vCenter Server 또는 호스트 관리를 사용하여 컨트롤러 VM을 삭제합니다. 이 삭제는 NSX Manager에서 시작되지 않았습니다.
- 또한 이 경우에서의 삭제에는 VM 손실로 이어지는 모든 호스트/스토리지 오류도 포함됩니다. 이 경우 해당 VM은 vCenter Server에서 손실될 뿐만 아니라 클러스터 및 NSX Manager에서도 손실됩니다. 하

지만 이 삭제가 NSX Manager에서 시작되지 않았으므로 NSX Manager 및 컨트롤러 클러스터 둘 다 해당 컨트롤러가 여전히 유효하다고 봅니다. NSX Manager로 반환된 컨트롤러 상태는 이 컨트롤러 노드가 다운되었으며 클러스터의 일부가 아니며 UI에 표시됨을 나타냅니다. 또한 NSX Manager에는 해당 컨트롤러에 더 이상 연결할 수 없음을 나타내는 로그도 있습니다.

가상 컨트롤러가 표시될 때 수행할 작업

- 1 NSX Controller의 연결이 끊김에 설명된 대로 컨트롤러를 동기화합니다.
- 2 로그 항목을 참조하십시오. 컨트롤러 VM이 실수로 삭제되었거나 손상된 경우 **강제 삭제(Forcefully Delete)** 옵션을 사용하여 NSX Manager 데이터베이스에서 항목을 지워야 합니다. 자세한 내용은 [NSX Controller 삭제](#)를 참조하십시오.
- 3 컨트롤러를 삭제한 후 다음을 확인하십시오.
 - 컨트롤러 VM이 실제로 삭제되었는지 확인합니다.
 - `show controller-cluster startup-nodes` 명령이 올바른 컨트롤러만 표시하는지 확인합니다.
 - NSX Manager에 대한 syslog 항목이 더 이상 추가 컨트롤러를 표시하지 않는지 확인합니다.

NSX 6.2.7 이상에서 NSX Manager는 vCenter 인벤토리를 확인하여 컨트롤러 VM이 원래 MOID를 기준으로 하는 인벤토리에 여전히 존재하는지 검토합니다. NSX Manager가 인벤토리에서 컨트롤러 VM을 찾을 수 없는 경우 NSX Manager는 VM의 인스턴스 UUID를 사용하여 VM을 검색합니다. 인스턴스 UUID는 VM 내에 저장되므로 VM이 vCenter 인벤토리에 다시 추가되어도 변경되지 않습니다. NSX Manager에서 인스턴스 UUID를 사용하여 VM을 찾을 수 있는 경우 NSX Manager는 새 MOID로 해당 데이터베이스를 업데이트합니다.

그렇지만 컨트롤러 VM을 복제하는 경우 복제된 VM은 새 인스턴스 UUID는 물론, 원래 VM과 동일한 속성을 갖습니다. NSX Manager는 복제된 VM에 대한 MOID를 검색할 수 없습니다.

가상 컨트롤러에 대한 로그 항목

가상 컨트롤러가 감지되면 다음 오류 수준 로그 항목이 표시됩니다.

- 2017-07-31 22:15:05.844 UTC ERROR NVPStatusCheck ControllerServiceImpl:2146 - Controller <#> does not exist, might be deleted already. Skip saving its connectivity info.
- 2017-07-31 22:15:05.769 UTC ERROR NVPStatusCheck ControllerServiceImpl:2580 - the node is created by this NSX Manager <#>, but database has no record and delete might be in progress.

NSX Controller의 연결이 끊김

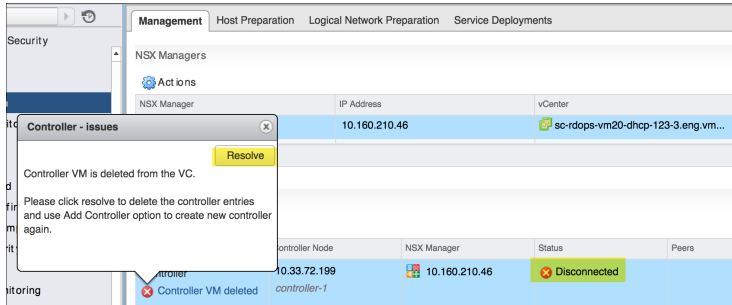
vCenter Server에서 NSX Controller VM 전원이 꺼졌거나 컨트롤러 VM이 vCenter Server에서 삭제되면 **설치(Installation) > 관리(Management)** 페이지의 **상태(Status)** 열에 **동기화되지 않음(Out of sync)** 상태가 표시됩니다.

사전 요구 사항

vCenter Server에서 컨트롤러 VM 전원이 꺼졌거나 컨트롤러 VM이 삭제되었습니다.

절차

- 1 vSphere Web Client에서 **Networking & Security > 설치(Installation) > 관리(Management)**로 이동합니다.



- 2 **오류(Error)** 링크를 클릭하여 이러한 동기화되지 않음 상태에 대한 자세한 원인을 확인하십시오.

- 3 **해결(Resolve)** 버튼을 클릭하여 문제를 해결하십시오.

결과

컨트롤러 VM의 전원이 꺼지면 관리부는 컨트롤러에 대해 **power on** 명령을 트리거합니다.

컨트롤러 VM이 삭제되면 컨트롤러 항목이 관리부에서 삭제되고 관리부는 컨트롤러 삭제 사실을 중앙 제어부에 전달합니다.

다음에 수행할 작업

노드 추가(Add Node) 옵션을 사용하여 새 컨트롤러를 생성합니다. 자세한 내용은 "NSX 관리 가이드"를 참조하십시오.

제어부 에이전트(netcpa) 문제

vSphere용 NSX에서 제어부(netcpa)는 로컬 에이전트 데몬으로 작동하고 NSX Manager 및 컨트롤러 클러스터와 통신합니다. **통신 채널 상태(Communication Channel Health)** 기능은 중앙 제어부-로컬 제어부 상태를 NSX Manager에 주기적으로 보고하고 NSX Manager UI에 표시되는 사전 예방적 상태 검사입니다. 이 보고서는 ESXi 호스트 netcpa 채널에 대한 NSX Manager의 작동 상태를 감지하기 위한 하트비트로도 사용됩니다. 통신 장애 동안 오류 세부 정보를 제공하고, 채널이 잘못된 상태가 될 때 이벤트를 생성하고, NSX Manager에서 호스트로의 하트비트 메시지를 생성합니다.

문제

제어부 에이전트와 컨트롤러 간에 연결 문제가 있습니다.

원인

누락된 연결이 있으면 제어부 에이전트가 제대로 작동하지 않는 것일 수 있습니다.

해결책

- 1 다음 명령을 사용하여 채널이 잘못된 상태가 될 때의 연결 상태를 확인합니다.

GET https://<NSX_Manager_IP>/api/2.0/vdn/inventory/host/{hostId}/connection/status

다음은 반환 값의 예입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<hostConnStatus>
<hostName>10.161.246.20</hostName>
<hostId>host-21</hostId>
<nsxMgrToFirewallAgentConn>UP</nsxMgrToFirewallAgentConn>
<nsxMgrToControlPlaneAgentConn>UP</nsxMgrToControlPlaneAgentConn>
<hostToControllerConn>DOWN</hostToControllerConn>
<fullSyncCount>-1</fullSyncCount>
<hostToControllerConnectionErrors>
<hostToControllerConnectionError>
<controllerIp>10.160.203.236</controllerIp>
<errorCode>1255604</errorCode>
<errorMessage>Connection Refused</errorMessage>
</hostToControllerConnectionError>
<hostToControllerConnectionError>
<controllerIp>10.160.203.237</controllerIp>
<errorCode>1255603</errorCode>
<errorMessage>SSL Handshake Failure</errorMessage>
</hostToControllerConnectionError>
</hostToControllerConnectionErrors>
</hostConnStatus>
```

다음 오류 코드가 지원됩니다.

1255602: 불완전한 컨트롤러 인증서 1255603: SSL 핸드셰이크 실패 1255604: 연결이 거부됨 1255605: 연결 유지 시간 초과 1255606: SSL 예외 1255607: 잘못된 메시지 1255620: 알 수 없는 오류

- 2 다음과 같이 제어부 에이전트가 다운된 이유를 확인하십시오.

- a ESXi 호스트에서 `/etc/init.d/netcpad status` 명령을 실행하여 호스트의 제어부 에이전트 상태를 확인합니다.

```
[root@esx-01a:~] /etc/init.d/netcpad status
netCP agent service is running
```

- b `more /etc/vmware/netcpa/config-by-vsm.xml` 명령을 사용하여 제어부 에이전트 구성을 확인합니다. NSX Controller의 IP 주소가 나열되어야 합니다.

```
[root@esx-01a:~] more /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
    <connection id="0000">
      <port>1234</port>
      <server>192.168.110.31</server>
```

```

    <sslEnabled>true</sslEnabled>
    <thumbprint>A5:C6:A2:B2:57:97:36:F0:7C:13:DB:64:9B:86:E6:EF:1A:7E:5C:36</thumbprint>
  </connection>
  <connection id="0001">
    <port>1234</port>
    <server>192.168.110.32</server>
    <sslEnabled>true</sslEnabled>
    <thumbprint>12:E0:25:B2:E0:35:D7:84:90:71:CF:C7:53:97:FD:96:EE:ED:7C:DD</thumbprint>
  </connection>
  <connection id="0002">
    <port>1234</port>
    <server>192.168.110.33</server>
    <sslEnabled>true</sslEnabled>
    <thumbprint>BD:DB:BA:B0:DC:61:AD:94:C6:0F:7E:F5:80:19:44:51:BA:90:2C:8D</thumbprint>
  </connection>
</connectionList>
...

```

- 3 다음 명령을 사용하여 제어부 에이전트에서 컨트롤러에 대한 연결을 확인합니다. 출력은 각 컨트롤러에 대한 단일 연결입니다.

```

>[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp      0  0  192.168.110.51:16594      192.168.110.31:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:46917      192.168.110.33:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:47891      192.168.110.32:1234      ESTABLISHED      36752  newreno
netcpa-worker

```

- 4 다음 명령을 실행하여 제어부 에이전트에서 컨트롤러에 대한 연결이 CLOSED 또는 CLOSE_WAIT 상태로 표시되는지 확인합니다.

```

esxcli network ip
  connection list |grep "1234.*netcpa*" | egrep "CLOSED|CLOSE_WAIT"

```

- 5 제어부 에이전트가 꽤 오랫동안 다운된 경우 연결이 전혀 없을 수 있습니다. 이를 확인하려면 다음 명령을 실행합니다. 출력은 각 컨트롤러에 대한 단일 연결입니다.

```

esxcli network ip
  connection list |grep "1234.*netcpa*" |grep ESTABLISHED

```

- 6** 제어부 에이전트(**netcpa**) 자동 복구 메커니즘: 자동 제어부 에이전트 모니터링 프로세스는 잘못된 상태인 제어부 에이전트를 감지합니다. 제어부 에이전트가 잘못된 상태인 경우 응답을 중지한 후 자동으로 복구를 시도합니다.

- a** 제어부 에이전트가 응답을 중지하는 경우 라이브 코어 파일이 생성됩니다. 코어 파일을 찾는 방법은 다음과 같습니다.

```
ls /var/core
netcpa-worker-zdump.000
```

- b** **vmkwarning.log** 파일에 Syslog 오류가 보고됩니다.

```
cat /var/run/log/vmkwarning.log | grep NETCPA
2017-08-11T06:32:17.994Z cpu1:1000044539)ALERT: Critical - NETCPA is hanged
Taking live-dump & restarting netcpa process!
```

참고 제어부 에이전트 모니터에서 상태 검사에 대한 응답 지연으로 인해 일시적 오류가 발생할 경우 다음과 비슷한 경고 메시지가 **VMKernel** 로그에 보고될 수 있습니다.

경고 - NETCPA에서 netcpa 상태를 가져오지 못했습니다.

이 경고는 무시해도 됩니다.

- 7** 이 문제가 자동으로 복구되지 않을 경우 다음과 같이 제어부 에이전트를 다시 시작합니다.
- a** SSH 또는 콘솔을 통해 **ESXi** 호스트에 루트 권한으로 로그인합니다.
- b** **/etc/init.d/netcpad restart** 명령을 실행하여 **ESXi** 호스트에서 제어부 에이전트를 다시 시작합니다.

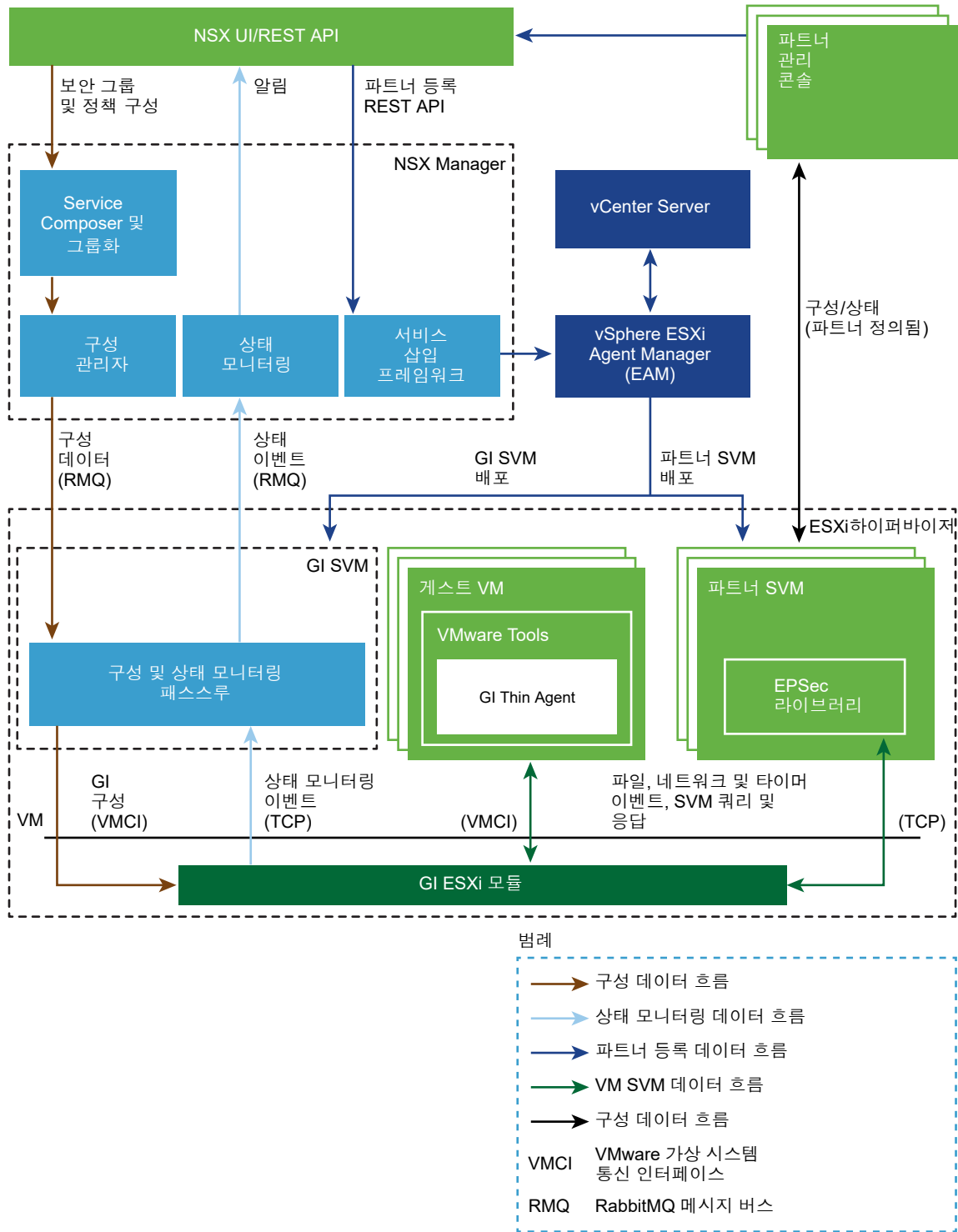
Guest Introspection 문제 해결

9

본 장은 다음 항목을 포함합니다.

- [Guest Introspection 아키텍처](#)
- [Guest Introspection 로그](#)
- [Guest Introspection 환경 및 작업 세부 정보 수집](#)
- [Linux 또는 Windows의 Thin Agent 문제 해결](#)
- [ESX GI 모듈\(MUX\) 문제 해결](#)
- [EPSecLib 문제 해결](#)

Guest Introspection 아키텍처



Guest Intropection 로그

Guest Intropection 문제를 해결하는 동안 사용할 수 있는 여러 가지 로그를 캡처할 수 있습니다.

ESX GI 모듈(MUX) 로그

ESXi 호스트의 가상 시스템에서 Guest Introspection이 작동하지 않거나 호스트에 SVA와의 통신과 관련된 정보가 발생하는 경우 ESXi 호스트의 ESX GI 모듈에 문제가 있는 것일 수 있습니다.

로그 경로 및 샘플 메시지

MUX 로그 경로

/var/log/syslog

var/run/syslog.log

ESX GI 모듈(MUX) 메시지는 <timestamp>EPsecMUX<[ThreadID]>: <message> 형식을 따릅니다.

예:

```
2017-07-16T05:44:49Z EPsecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

위 예에서 각각의 의미는 다음과 같습니다.

- [ERROR]는 메시지의 유형입니다. 다른 유형으로 [DEBUG], [INFO]가 있습니다.
- (EPSEC)는 메시지가 끝점 보안과 관련되어 있음을 나타냅니다.

로그 파일 사용 및 보기

호스트에 설치된 ESX GI 모듈 VIB의 버전을 확인하려면 `#esxcli software vib list | grep epsec-mux` 명령을 실행합니다.

전체 로깅을 설정하려면 ESXi 호스트 명령 셸에서 다음 단계를 수행합니다.

- 1 `ps -c | grep Mux` 명령을 실행하여 현재 실행 중인 ESX GI 모듈 프로세스를 찾습니다.

예:

```
~ # ps -c | grep Mux
192223 192223 sh /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

- 2 서비스가 실행되지 않는 경우 `/etc/init.d/vShield-Endpoint-Mux start` 또는 `/etc//init.d/vShield-Endpoint-Mux restart` 명령을 사용하여 다시 시작할 수 있습니다.
- 3 `watchdog.sh` 프로세스를 포함하여 실행 중인 ESX GI 모듈 프로세스를 중지하려면 `~ # kill -9 192223 192233 192236` 명령을 실행합니다.
두 ESX GI 모듈 프로세스가 생성됩니다.
- 4 새 `-d` 옵션을 사용하여 ESX GI 모듈을 시작합니다. `epsec-mux` 빌드 5.1.0-01255202 및 5.1.0-01814505 ~ `# /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910`의 경우 옵션 `-d`가 없습니다.

- 5 ESXi 호스트에서 `/var/log/syslog.log` 파일의 ESX GI 모듈 로그 메시지를 확인합니다. 글로벌 솔루션, 솔루션 ID, 포트 번호에 해당하는 항목이 올바르게 지정되었는지 확인합니다.

예제: 샘플 **muxconfig.xml** 파일

```
<?xml version="1.0" encoding="UTF-8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService (216).vmx</vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-alpha-01.vmx</vmxPath>

    </Solution>

    <Solution>

      <id>6341068275337723904</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>
```

```

<uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>

<vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>

</Solution>
</InstalledSolutions>
<DefaultSolutions/>
<GlobalSolutions>
  <solution>
    <id>100</id>
    <tag></tag>
    <order>0</order>
  </solution>
  <solution>
    <id>102</id>
    <tag></tag>
    <order>10000</order>
  </solution>
  <solution>
    <id>6341068275337723904</id>
    <tag></tag>
    <order>10001</order>
  </solution>
</GlobalSolutions>
</EndpointConfig>

```

GI Thin Agent 로그

Thin Agent는 VM 게스트 OS에 설치되고 사용자 로그인 세부 정보를 감지합니다.

로그 경로 및 샘플 메시지

Thin Agent는 GI 드라이버인 vsepflt.sys, vnetflt.sys, vnetwfp.sys(Windows 10 이상)로 구성되어 있습니다.

Thin Agent 로그는 VCenter 로그 번들의 일부로 ESXi 호스트에 있습니다. 로그 경로는 `/vmfs/volumes/<datastore>/<vmname>/vmware.log`입니다. 예: `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Thin Agent 메시지는 `<timestamp> <VM Name><Process Name><[PID]>: <message>` 형식을 따릅니다.

Guest: vnet or Guest:vsep 아래의 로그 예제에서는 해당 GI 드라이버와 관련된 로그 메시지와 디버그 메시지를 차례로 표시합니다.

예:

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

예제: vShield Guest Introspection Thin Agent 드라이버 로깅 사용

디버그 설정은 `vmware.log` 파일을 조절하는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

이 절차에서는 Windows 레지스트리를 수정해야 합니다. 레지스트리를 수정하기 전에 레지스트리 백업을 생성해야 합니다. 레지스트리 백업 및 복원에 대한 자세한 내용은 Microsoft 기술 자료 문서 [136393](#)을 참조하십시오.

Thin Agent 드라이버에 대한 디버그 로깅을 사용하도록 설정하려면:

- 1 시작 > 실행(Start > Run)을 클릭합니다. `regedit`를 입력하고 확인(OK)을 클릭합니다. 레지스트리 편집기 창이 열립니다. 자세한 내용은 Microsoft 기술 자료 문서 [256986](#)을 참조하십시오.
- 2 레지스트리 편집기를 사용하여 다음 키를 생성합니다. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepfilt\parameters`
- 3 새로 생성된 매개 변수 키 아래에 이러한 DWORD를 생성합니다. 이러한 값을 입력할 때는 16진수를 선택해야 합니다.

```
Name: log_dest
Type: DWORD
Value: 0x2
```

```
Name: log_level
Type: DWORD
Value: 0x10
```

log_level 매개 변수 키의 다른 값:

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

- 관리자 권한으로 명령 프롬프트를 엽니다. 다음 명령을 실행하여 vShield Endpoint 파일 시스템 미니 드라이버를 언로드했다가 다시 로드합니다.

- fltmc unload vsepflt
- fltmc load vsepflt

가상 시스템에 있는 vmware.log 파일에서 로그 항목을 찾을 수 있습니다.

vShield GI 네트워크 검사 드라이버 로깅 사용

디버그 설정은 vmware.log 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

이 절차에서는 Windows 레지스트리를 수정해야 합니다. 레지스트리를 수정하기 전에 레지스트리 백업을 생성해야 합니다. 레지스트리 백업 및 복원에 대한 자세한 내용은 Microsoft 기술 자료 문서 [136393](#)을 참조하십시오.

- 1 시작 > 실행(Start > Run)을 클릭합니다. regedit를 입력하고 확인(OK)을 클릭합니다. 레지스트리 편집기 창이 열립니다. 자세한 내용은 Microsoft 기술 자료 문서 [256986](#)을 참조하십시오.
- 2 레지스트리를 편집합니다.

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest" = DWORD: 0x00000001
```

- 3 가상 시스템을 재부팅합니다.

vsepflt.sys 및 vnetflt.sys 로그 파일 위치

log_dest 레지스트리 설정 DWORD: 0x00000001을 사용하여 Endpoint Thin Agent 드라이버가 디버거에 로깅합니다. 디버거(SysInternals 또는 windbg의 DbgView)를 실행하여 디버그 출력을 캡처합니다.

또는 log_dest 레지스트리 설정 DWORD: 0x00000002를 설정할 수 있습니다. 이 경우 드라이버 로그는 ESXi 호스트의 해당 가상 시스템 폴더에 있는 vmware.log 파일에 인쇄됩니다.

UMC 로깅 사용

Guest Introspection UMC(사용자 모드 구성 요소)는 보호된 가상 시스템의 VMware Tools 서비스 내에서 실행됩니다.

- 1 Windows XP 및 Windows Server 2003에서는 경로 C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf에 존재하지 않을 경우 tools config 파일을 생성합니다.
- 2 Windows Vista, Windows 7 및 Windows Server 2008에서는 경로 C:\ProgramData\VMware\VMware Tools\tools.conf에 존재하지 않을 경우 tools config 파일을 생성합니다.
- 3 tools.conf 파일에 다음 줄을 추가하여 UMC 구성 요소 로깅을 사용하도록 설정합니다.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

vsep.handler = vmx 설정에서 UMC 구성 요소는 ESXi 호스트의 해당 가상 시스템 폴더에 있는 vmware.log 파일에 로그인합니다.

다음 설정 로그를 사용하면 UMC 구성 요소 로그가 지정한 로그 파일에 인쇄됩니다.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

GI EPSecLib 및 SVM 로그

EPSecLib는 ESXi 호스트 ESX GI 모듈(MUX)에서 이벤트를 수신합니다.

로그 경로 및 샘플 메시지

EPSecLib 로그 경로

/var/log/syslog

var/run/syslog

EPSecLib 메시지는 <timestamp> <VM Name><Process Name><[PID]>: <message> 형식을 따릅니다.

[ERROR] 아래의 예제는 메시지의 유형이고 (EPSEC)는 Guest Introspection에만 관련되는 메시지를 나타냅니다.

예:

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
[7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

로그 수집

GI SVM 내 구성 요소인 EPSec 라이브러리에 대한 디버그 로깅을 사용하도록 설정하려면:

- 1 NSX Manager에서 콘솔 암호를 가져와 GI SVM에 로그인합니다.
- 2 `/etc/epseclib.conf` 파일을 생성하고 다음을 추가합니다.

```
ENABLE_DEBUG=TRUE
ENABLE_SUPPORT=TRUE
```
- 3 `chmod 644 /etc/epseclib.conf` 명령을 실행하여 사용 권한을 변경합니다.
- 4 `/usr/local/sbin/rcusvm restart` 명령을 실행하여 GI-SVM 프로세스를 다시 시작합니다.

이렇게 하면 GI SVM에서 EPSecLib에 대해 디버그 로깅을 사용하도록 설정되고, NSX for vSphere 6.2.x 및 6.3.x에 적용할 수 있는 `/var/log/messages`에서 디버그 로그를 찾을 수 있습니다. 디버그 설정은 `vmware.log` 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

GI SVM 로그

로그를 캡처하기 전에 호스트 ID 또는 호스트 MOID를 확인합니다.

- NSX Manager에서 `show cluster all` 및 `show cluster <cluster ID>` 명령을 실행합니다.

예:

```
nsxmgr-01a> show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	RegionA01-COMP01	domain-c26	RegionA01	Enabled
2	RegionA01-MGMT01	domain-c71	RegionA01	Enabled

```
nsxmgr-01a> show cluster domain-c26
```

```
Datacenter: RegionA01
Cluster: RegionA01-COMP01
```

No.	Host Name	Host Id	Installation Status
1	esx-01a.corp.local	host-29	Ready
2	esx-02a.corp.local	host-31	Ready

- 1 현재 로깅 상태를 확인하려면 다음 명령을 실행합니다.

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm
```

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/root
```
- 2 현재 로깅 상태를 변경하려면 다음 명령을 실행합니다.

POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

- 3 로그를 생성하려면 다음 명령을 실행합니다.

GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs

Send 및 Download를 선택합니다.

이 명령은 GI SVM 로그를 생성하고 파일을 **techsupportlogs.log.gz** 파일로 저장합니다. 디버그 설정은 **vmware.log** 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

Guest Introspection 환경 및 작업 세부 정보 수집

환경 세부 정보를 수집하면 구성 요소의 호환성을 확인하는 데 도움이 됩니다.

- 1 NSX Guest Introspection이 고객 환경에서 사용되고 있는지 확인합니다. 사용되고 있지 않은 경우 가상 시스템에 대한 Guest Introspection 서비스를 제거하고 이 문제가 해결되었는지 확인합니다.
- 2 환경 세부 정보 수집:
 - a ESXi 빌드 버전 - ESXi 호스트에서 **uname -a** 명령을 실행하거나 vSphere Web Client에서 호스트를 클릭하고 오른쪽 창 위쪽에서 빌드 번호를 찾습니다.
 - b Linux 제품 버전 및 빌드 번호
 - c **/usr/sbin/vsep -v**를 입력하면 프로덕션 버전이 표시됩니다.

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```


3 VMware NSX® for vSphere® 버전 및 다음 내용:

- 파트너 솔루션 이름 및 버전 번호
- 파트너 솔루션에서 사용되는 EPSec 라이브러리 버전 번호: GI SVM에 로그인하고 EPSec library/libEPSec.so | grep BUILD에 대해 #strings 경로 실행
- 가상 시스템의 게스트 운영 체제
- 다른 모든 타사 애플리케이션 또는 파일 시스템 드라이버

4 ESX GI 모듈(MUX) 버전 - esxcli software vib list | grep epsec-mux 명령을 실행합니다.

5 서버 유형 등의 워크로드 세부 정보를 수집합니다.

6 ESXi 호스트 로그를 수집합니다. 자세한 내용은 [VMware ESX/ESXi에 대한 진단 정보 수집\(653\)](#)을 참조하십시오.

7 파트너 솔루션에서 GI SVM(서비스 가상 시스템) 로그를 수집합니다. GI SVM 로그 수집에 대한 자세한 내용은 파트너에게 문의하십시오.

8 문제가 발생하는 동안 일시 중단 상태를 수집합니다. 진단 정보를 수집하려면 [ESX/ESXi에서 가상 시스템 일시 중단\(2005831\)](#)을 참조하십시오.

9 날짜를 수집한 후 vSphere 구성 요소의 호환성을 비교합니다. 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

Linux 또는 Windows의 Thin Agent 문제 해결

Guest Introspection Thin Agent는 각 게스트 가상 시스템에 VMware Tools™와 함께 설치됩니다.

Linux의 Thin Agent 문제 해결

가상 시스템의 읽기 및 쓰기 작업, 파일 압축 해제 또는 저장이 느려지는 경우 Thin Agent에 문제가 있을 수 있습니다.

- 1 관련된 모든 구성 요소의 호환성을 확인합니다. 호환성은 끝점의 주요 문제 중 하나입니다. ESXi, vCenter Server, NSX Manager 및 사용자가 선택한 보안 솔루션(예: Trend Micro, McAfee, Kaspersky, Symantec 등)의 빌드 번호가 필요합니다. 이 데이터를 수집한 후 vSphere 구성 요소의 호환성을 비교합니다. 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.
- 2 파일 자체 검사가 시스템에 설치되어 있는지 확인합니다.
- 3 **service vsep status** 명령을 사용하여 Thin Agent가 실행되고 있는지 확인합니다. 이 명령이 실행되면 vsep 서비스가 실행 중 상태로 표시됩니다.
- 4 Thin Agent가 시스템에 성능 문제를 야기하는 것으로 판단되면 **service vsep stop** 명령을 실행하여 서비스를 중지합니다.
- 5 그런 다음 테스트를 수행하여 기준선을 얻습니다. **service vsep start** 명령을 실행하여 vsep 서비스를 시작하고 다른 테스트를 수행할 수 있습니다.

6 Linux Thin Agent에 대해 디버깅을 사용하도록 설정:

- a `/etc/vsep/vsep.conf` 파일을 엽니다.
- b 모든 로그에 대해 `DEBUG_LEVEL=4`를 `DEBUG_LEVEL=7`로 변경합니다.
- c 보통 로그에 대해서는 `DEBUG_LEVEL=6`으로 설정할 수 있습니다.
- d 기본 로그 대상(`DEBUG_DEST=2`)은 `vmware.log`(호스트)입니다. 게스트(예: `/var/log/message` 또는 `/var/log/syslog`)로 변경하려면 `DEBUG_DEST=1`을 설정하십시오.

참고 전체 로깅을 사용하도록 설정하면 `vmware.log` 파일에서 과도한 로그 작업 플러딩이 발생하여 파일이 매우 커질 수 있습니다. 가능한 한 빨리 전체 로깅을 사용하지 않도록 설정합니다.

Windows의 Thin Agent 문제 해결

- 1 관련된 모든 구성 요소의 호환성을 확인합니다. ESXi, vCenter Server, NSX Manager 및 사용자가 선택한 보안 솔루션(예: Trend Micro, McAfee, Kaspersky, Symantec 등)의 빌드 번호가 필요합니다. 모든 데이터를 수집한 후 vSphere 구성 요소의 호환성을 비교할 수 있습니다. 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

- 2 VMware Tools TM가 최신 상태인지 확인합니다. 특정 가상 시스템이 영향을 받는다는 것이 확인되면 [vSphere에서 VMware Tools 설치 및 업그레이드\(2004754\)](#)를 참조하십시오.

- 3 Powershell 명령 `fltmc`를 실행하여 Thin Agent가 로드되었는지 확인합니다.

이 명령이 실행되면 `vsepflt` 드라이버 목록에 이름 `vsepflt`가 표시됩니다. 드라이버가 로드되지 않으면 `fltmc load vsepflt` 명령을 사용하여 드라이버를 로드할 수 있습니다.

- 4 Thin Agent가 시스템에 성능 문제를 야기하는 경우 `fltmc unload vsepflt` 명령을 실행하여 드라이버를 언로드합니다.

다음으로, 테스트를 수행하여 기준선을 얻습니다. 다음 명령을 실행하여 드라이버를 로드하고 다른 테스트를 수행할 수 있습니다.

```
fltmc load vsepflt.
```

Thin Agent에 성능 문제가 있음을 확인한 경우 [NSX/vCloud Networking & Security에서 VMware Tools를 업그레이드한 후에 VM이 느려짐\(2144236\)](#)을 참조하십시오.

- 5 네트워크 검사를 사용하지 않는 경우 이 드라이버를 제거하거나 사용하지 않도록 설정합니다.

VMware Tools 설치 관리자를 수정하여 네트워크 검사를 제거할 수도 있습니다.

- a VMware Tools 설치 관리자를 마운트합니다.
- b **제어판 > 프로그램 및 기능(Control Panel > Programs and Features)**으로 이동합니다.
- c 마우스 오른쪽 버튼으로 **VMware Tools > 수정(VMware Tools > Modify)**을 클릭합니다.
- d **설치 완료(Complete install)**를 선택합니다.
- e NSX 파일 자체 검사를 찾습니다. 네트워크 검사에만 해당하는 하위 폴더가 있습니다.

- f **네트워크 검사(Network Introspection)**를 사용하지 않도록 설정합니다.
 - g VM을 재부팅하여 드라이버 제거를 완료합니다.
- 6 Thin Agent에 대해 디버그 로깅을 사용하도록 설정합니다. 자세한 내용은 [Guest Introspection 로그](#) 항목을 참조하십시오. 모든 디버깅 정보는 해당 가상 시스템에 대한 `vmware.log` 파일에 기록되도록 구성됩니다.
 - 7 `procmon` 로그를 검토하여 Thin Agent의 파일 검사를 검토합니다. 자세한 내용은 [바이러스 백신 소프트웨어로 인한 vShield Endpoint 성능 문제 해결\(2094239\)](#)을 참조하십시오.

환경 및 워크로드 세부 정보 수집

- 1 NSX Guest Introspection이 고객 환경에서 사용되고 있는지 확인합니다. 사용되고 있지 않은 경우 가상 시스템에 대한 Guest Introspection 서비스를 제거하고 이 문제가 해결되었는지 확인합니다. Guest Introspection이 필요한 경우에만 게스트 검사 문제를 해결하십시오.
- 2 환경 세부 정보 수집:
 - a ESXi 빌드 버전 - ESXi 호스트에서 `uname -a` 명령을 실행하거나 vSphere Web Client에서 호스트를 클릭하고 오른쪽 창 위쪽에서 빌드 번호를 찾습니다.
 - b Linux 제품 버전 및 빌드 번호
 - c `/usr/sbin/vsep -v`를 입력하면 프로덕션 버전이 표시됩니다.

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

- 3 VMware NSX® for vSphere® 버전 및 다음 내용:
 - 파트너 솔루션 이름 및 버전 번호
 - 파트너 솔루션에서 사용되는 EPsec 라이브러리 버전 번호: SVM에 로그인하고 `EPsec library/libEPsec.so | grep BUILD`에 대해 `#strings` 경로 실행
 - 가상 시스템의 게스트 운영 체제
 - 다른 모든 타사 애플리케이션 또는 파일 시스템 드라이버
- 4 ESX GI 모듈(MUX) 버전 - `esxcli software vib list | grep epsec-mux` 명령을 실행합니다.
- 5 서버 유형 등의 워크로드 세부 정보를 수집합니다.
- 6 ESXi 호스트 로그를 수집합니다. 자세한 내용은 [VMware ESX/ESXi에 대한 진단 정보 수집\(653\)](#)을 참조하십시오.
- 7 파트너 솔루션에서 SVM(서비스 가상 시스템) 로그를 수집합니다. 파트너에게 SVM 로그 수집에 대한 자세한 정보를 문의하십시오.

- 8 문제가 발생하는 동안 일시 중단 상태를 수집합니다. 진단 정보를 수집하려면 [ESX/ESX에서 가상 시스템 일시 중단\(2005831\)](#)을 참조하십시오.

Thin Agent 충돌 문제 해결

Thin Agent가 충돌하는 경우 `/directory`에 코어 파일이 생성됩니다. `location / directory`에서 코어 덤프 파일(코어)을 수집합니다. `file` 명령을 사용하여 코어가 `vsep`에서 생성되었는지 확인합니다. 예:

```
# file core
core: ELF 64-bit LSB core file x86-64, version 1 (SYSV), SVR4-style, from '/usr/sbin/vsep'
```

가상 시스템이 응답하지 않거나 작동 중지됨

일시 중단된 상태의 가상 시스템 VMware vmss 파일을 수집한 후 [ESX/ESXi에서 가상 시스템을 일시 중단하여 진단 정보 수집\(2005831\)](#)을 참조하거나 가상 시스템 충돌을 야기한 후 전체 메모리 덤프 파일을 수집합니다. VMware는 ESXi vmss 파일을 코어 덤프 파일로 변환하는 유틸리티를 제공합니다. 자세한 내용은 [Vmss2core Fling](#)을 참조하십시오.

ESX GI 모듈(MUX) 문제 해결

ESX GI 모듈(MUX)

ESXi 호스트의 일부 가상 시스템에서 Guest Introspection이 작동하지 않거나 특정 호스트에서 GI SVA와 통신과 관련된 경보가 발생하는 경우 ESXi 호스트의 ESX GI 모듈에 문제가 있을 수 있습니다.

- 1 `# /etc/init.d/vShield-Endpoint-Mux status` 명령을 실행하여 ESXi 호스트에서 서비스가 실행되고 있는지 확인합니다.

예:

```
# /etc/init.d/vShield-Endpoint-Mux status
vShield-Endpoint-Mux is running
```

- 2 서비스가 실행되고 있지 않다고 표시되면 다시 시작하거나 다음 명령을 사용하여 시작합니다.

```
/etc/init.d/vShield-Endpoint-Mux start
```

또는

```
/etc/init.d/vShield-Endpoint-Mux restart
```

이 서비스를 다시 시작해도 큰 영향을 미치지 않으며 몇 초 안에 다시 시작되므로, 프로덕션 시간 동안 이 서비스를 다시 시작해도 무방합니다.

- 3 ESX GI 모듈이 수행하는 작업을 보다 잘 이해하거나 통신 상태를 확인하려면 ESXi 호스트에서 로그를 확인할 수 있습니다. ESX GI 모듈 로그는 호스트 `/var/log/syslog` 파일에 기록됩니다. ESXi 호스트 지원 로그에도 포함됩니다.

자세한 내용은 [vSphere Web Client](#)를 사용하여 [ESX/ESXi 호스트 및 vCenter Server](#)에 대한 진단 정보 수집(2032892)을 참조하십시오.

- 4 ESX GI 모듈에 대한 기본 로깅 옵션은 [정보]이며, [디버그]로 승격하여 추가 정보를 수집할 수 있습니다.

자세한 내용은 [Guest Introspection 로그](#) 항목을 참조하십시오.

- 5 ESX GI 모듈을 다시 설치하는 것으로도 많은 문제를 해결할 수 있습니다. 특히 잘못된 버전이 설치되어 있거나 ESXi 호스트를 이전에 끝점이 설치되어 있던 환경으로 가져온 경우에는 다시 설치하는 것이 유용할 수 있습니다. 이러한 경우 제거했다가 다시 설치해야 합니다.

VIB를 제거하려면 `esxcli software vib remove -n epsec-mux` 명령을 실행합니다.

- 6 VIB 설치 문제가 발생하는 경우 ESXi 호스트의 `/var/log/esxupdate.log` 파일을 확인하십시오. 이 로그는 드라이버가 성공적으로 설치되지 않는 이유에 대한 가장 명확한 정보를 보여줍니다. 이것은 ESX GI 모듈 설치에 대한 일반적인 문제입니다. 자세한 내용은 [VMware NSX for vSphere 6.x의 ESXi 호스트에서 NSX Guest Introspection 서비스\(ESX GI 모듈 VIB\)를 설치하지 못함\(2135278\)](#)을 참조하십시오.

- 7 손상된 ESXi 이미지를 확인하려면 다음과 비슷한 메시지를 찾아보십시오.

```
esxupdate: esxupdate: ERROR: Installation Error:
(None, 'No image profile is found on the host or image profile is empty.
An image profile is required to install or remove VIBs. To install an image profile,
use the esxcli image profile install command.')
```

- 8 이미지가 손상되었는지 확인하려면 ESXi 호스트에서 `cd /vmfs/volumes` 명령을 실행합니다.

- a `find * | grep imgdb.tgz` 명령을 실행하여 `imgdb.tgz` 파일을 검색합니다.

이 명령을 실행하면 일반적으로 2개의 일치 항목이 검색됩니다. 예:

```
0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz 또는 edbf587b-
da2add08-3185-3113649d5262/imgdb.tgz
```

- b 각 일치 항목에 대해 `ls -l match_result` 명령을 실행합니다.

예:

```
> ls -l 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz -rwx-----
1 root root 26393 Jul 20 19:28 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz
> ls -l edbf587b-da2add08-3185-3113649d5262/imgdb.tgz -rwx-----
1 root root 93 Jul 19 17:32 edbf587b-da2add08-3185-3113649d5262/imgdb.tgz
```

`imgdb.tgz` 파일의 기본 크기가 다른 파일보다 훨씬 더 크거나 파일 중 하나가 2~3바이트에 불과할 경우 파일이 손상된 것을 나타냅니다. 이 문제를 해결하기 위해 지원되는 유일한 방법은 해당 특정 ESXi 호스트에 대해 ESXi를 다시 설치하는 것입니다.

EPSecLib 문제 해결

NSX Manager가 이 가상 시스템 배포를 처리합니다.

EPSecLib

과거에는(vShield 사용) 타사 SVA 솔루션으로 배포를 처리했습니다. 이제 해당 솔루션은 NSX Manager에 연결됩니다. NSX Manager는 이 SVA의 배포를 처리합니다. 환경의 SVA에서 경보가 발생하는 경우 NSX Manager를 통해 다시 배포합니다.

- 모든 구성이 NSX Manager 내에 저장되어 있으므로 모든 구성이 손실됩니다.
- 재부팅하는 대신 SVA 가상 시스템을 다시 배포하는 것이 좋습니다.
- NSX는 호스트에서 SVA와 같은 VIB 및 SVM을 배포 및 모니터링하기 위해 EAM에 의존합니다.
- EAM은 설치 상태를 확인할 수 있는 믿을 수 있는 소스입니다.
- NSX UI(사용자 인터페이스)의 설치 상태는 VIB가 설치되어 있는지 여부 또는 SVM의 전원이 켜져 있는지 여부만 알려줄 수 있습니다.
- NSX UI의 서비스 상태는 가상 시스템의 기능이 작동하는지 여부를 나타냅니다.

SVA 배포와 NSX 및 vCenter Server 프로세스 간 관계

- 1 클러스터를 끝점으로 준비하도록 선택하면 EAM에서 SVA를 배포하기 위한 에이전시가 생성됩니다.
- 2 그런 다음 EAM은 생성한 에이전시 정보를 사용하여 ESXi 호스트에 ovf를 배포합니다.
- 3 NSX Manager는 EAM에 의해 ovf가 배포되었는지 확인합니다.
- 4 NSX Manager는 EAM에 의해 가상 시스템 전원이 켜졌는지 확인합니다.
- 5 NSX Manager는 가상 시스템의 전원이 켜져 있고 등록되었음을 파트너 SVA Solution Manager에게 알립니다.
- 6 EAM은 설치가 완료되었음을 나타내기 위해 NSX로 이벤트를 전송합니다.
- 7 파트너 SVA Solution Manager는 SVA 가상 시스템 내의 서비스가 작동되고 있으며 실행 중임을 나타내기 위해 NSX로 이벤트를 전송합니다.
- 8 SVA에 문제가 발생하는 경우 다음 두 위치에서 로그를 확인할 수 있습니다. EAM은 이러한 가상 시스템의 배포를 처리하므로 EAM 로그를 확인할 수 있습니다. 자세한 내용은 [VMware vCenter Server 4.x, 5.x 및 6.0에 대한 진단 정보 수집\(1011641\)](#)을 참조하십시오. 또는 SVA 로그를 확인하십시오. 자세한 내용은 [Guest Introspection 로그](#) 항목을 참조하십시오.
- 9 SVA 배포에 문제가 있는 경우 EAM 및 NSX Manager와의 통신에 문제가 있을 수 있습니다. EAM 로그를 확인할 수 있으며, 가장 간단한 방법은 EAM 서비스를 다시 시작하는 것입니다. 자세한 내용은 [호스트 준비](#) 항목을 참조하십시오.
- 10 위의 모든 방법이 제대로 수행되지만 끝점 기능을 테스트하고 싶은 경우 Eicar Test 파일을 사용하여 테스트할 수 있습니다.
 - 임의 레이블을 사용하여 텍스트 파일을 생성합니다. 예: eicar.test.
 - 파일 콘텐츠는 다음 문자열만 포함해야 합니다.

X50!P%AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

- 파일을 저장합니다. 저장할 때 해당 파일이 삭제되는 것을 볼 수 있습니다. 이 경우 끝점 솔루션이 작동하는 것입니다.