

NSX-T Data Center 문제 해결 가이드

수정 날짜: 2018년 9월 19일

VMware NSX-T Data Center 2.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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 © 2017, 2018 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

NSX-T Data Center 문제 해결 가이드 5

1 로그 및 서비스 6

- 로그 메시지 6
 - 원격 로깅 구성 7
 - 로그 메시지 ID 8
- Syslog 문제 해결 10
- 서비스 확인 11
- 지원 번들 수집 12

2 계층 2 연결 문제 해결 14

- NSX Manager 및 NSX Controller 클러스터 상태 확인 14
- 논리적 포트 확인 15
- 전송 노드 상태 확인 15
- 논리적 스위치 상태 확인 16
- CCP에서 논리적 스위치 확인 17
- 로컬 제어부 상태 확인 17
- 구성 세션 문제 해결 18
- L2 세션 문제 해결 19
- 오버레이 논리적 스위치에 대한 데이터부 문제 해결 20
- VLAN 논리적 스위치에 대한 데이터부 문제 해결 21
- 오버레이 논리적 스위치에 대한 ARP 문제 해결 22
- VLAN 논리적 스위치 또는 ARP가 해결된 경우 패킷 손실 문제 해결 22

3 설치 문제 해결 24

4 라우팅 문제 해결 28

5 방화벽 문제 해결 30

- ESXi 호스트에 적용되는 방화벽 규칙 결정 30
- KVM 호스트에 적용되는 방화벽 규칙 결정 32
- 방화벽 패킷 로그 34

6 기타 문제 해결 시나리오 36

- 전송 노드 추가 또는 삭제 실패 36
- 전송 노드가 다른 컨트롤러에 연결되는 데 약 5분이 소요됨 37
- NSX Manager VM 성능 저하 38
- NSX 에이전트가 NSX Manager와 통신 시 시간 초과 39

ESXi 호스트 추가 실패 40

잘못된 NSX Controller 상태 40

IPFIX를 사용하도록 설정되어 있으면 KVM VM의 관리 IP에 연결할 수 없음 41

NSX-T Data Center 문제 해결 가이드

“NSX-T Data Center 문제 해결 가이드”는 NSX-T Data Center 환경에서 발생할 수 있는 문제를 해결하는 방법에 대한 정보를 제공합니다.

대상 사용자

이 가이드는 NSX-T Data Center의 시스템 관리자용입니다. 가상화, 네트워킹 및 데이터 센터 작업에 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.

로그 및 서비스

1

로그는 많은 문제 해결 시나리오에서 유용할 수 있습니다. 서비스 상태 확인도 중요합니다.

본 장은 다음 항목을 포함합니다.

- 로그 메시지
- Syslog 문제 해결
- 서비스 확인
- 지원 번들 수집

로그 메시지

ESXi에서 실행되는 항목을 비롯한 모든 NSX-T Data Center 구성 요소의 로그 메시지는 RFC 5424에 명시된 syslog 형식을 준수합니다. KVM 호스트의 로그 메시지는 RFC 3164 형식입니다. 이 로그 파일은 /var/log 디렉토리에 있습니다.

NSX-T Data Center 장치에서 다음 NSX-T Data Center CLI 명령을 실행하여 로그를 확인할 수 있습니다.

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

하이퍼바이저에서 tac, tail, grep 및 more와 같은 Linux 명령을 사용하여 로그를 확인할 수 있습니다. 또한 NSX-T Data Center 장치에서 이러한 명령을 사용할 수 있습니다.

RFC 5424에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc5424>를 참조하십시오. RFC 3164에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc3164>를 참조하십시오.

RFC 5424는 로그 메시지에 대해 다음 형식을 정의합니다.

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

샘플 로그 메시지:

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager" errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'. Marking broker unhealthy.
```

모든 메시지에는 메시지의 소스를 식별하는 데 도움이 되는 구성 요소(comp) 및 하위 구성 요소(subcomp) 정보가 있습니다.

NSX-T Data Center는 일반 로그(숫자 값이 22인 시열 local6) 및 감사 로그(숫자 값이 23인 시열 local7)를 생성합니다. 모든 API 호출은 감사 로그를 트리거합니다.

API 호출에 연결된 감사 로그에는 다음 정보가 있습니다.

- API의 개체를 식별하기 위한 엔티티 ID 매개 변수 `entId`.
- 특정 API 호출을 식별하기 위한 요청 ID 매개 변수 `req-id`.
- API 호출에 `X-NSX-EREQID:<string>` 머리글이 포함된 경우 외부 요청 ID 매개 변수 `ereqId`.
- API 호출에 `X-NSX-EUSER:<string>` 머리글이 포함된 경우 외부 사용자 매개 변수 `euser`.

RFC 5424는 다음과 같은 심각도 수준을 정의합니다.

심각도 수준	설명
0	긴급: 시스템을 사용할 수 없음
1	경고: 작업을 즉시 수행해야 함
2	위험: 위험한 상태
3	오류: 오류 상태
4	경고: 경고 상태
5	알림: 일반적이지만 중요한 상태
6	정보: 정보용 메시지
7	디버그: 디버그 수준 메시지

심각도가 긴급, 경고, 위험 또는 오류인 모든 로그에는 로그 메시지의 구조화된 데이터 부분에 고유한 오류 코드가 포함되어 있습니다. 오류 코드는 문자열과 10진수로 구성됩니다. 문자열은 특정 모듈을 나타냅니다.

MSGID 필드는 메시지 유형을 식별합니다. 메시지 ID 목록은 [로그 메시지 ID](#)의 내용을 참조하십시오.

원격 로깅 구성

원격 로깅 서버로 로그 메시지를 전송하도록 NSX-T Data Center 장치 및 하이퍼바이저를 구성할 수 있습니다.

원격 로깅은 NSX Manager, NSX Controller, NSX Edge 및 하이퍼바이저에서 지원됩니다. 각 노드에서 개별적으로 원격 로깅을 구성해야 합니다.

KVM 호스트에서는 NSX-T Data Center 설치 패키지가 구성 파일을 `/etc/rsyslog.d` 디렉토리에 배치하여 자동으로 rsyslog 데몬을 구성합니다.

사전 요구 사항

- 로그를 수신하도록 로깅 서버를 구성합니다.

절차

1 NSX-T Data Center 장치에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 다음 명령을 실행하여 로그 서버로 전송할 메시지 유형 및 로그 서버를 구성합니다. 여러 시설 또는 메시지 ID는 공백 없이 쉼표로 구분된 목록으로 지정할 수 있습니다.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>]
[messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

이 명령에 대한 자세한 내용은 "NSX-T CLI 참조"를 참조하십시오. 명령을 여러 번 실행하여 여러 로깅 서버 구성을 추가할 수 있습니다. 예:

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b get logging-server 명령으로 로깅 구성을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

2 ESXi 호스트에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 다음 명령을 실행하여 Syslog를 구성하고 테스트 메시지를 전송합니다.

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b 다음 명령을 실행하여 구성을 표시할 수 있습니다.

```
esxcli system syslog config get
```

3 KVM 호스트에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 환경에 대한 /etc/rsyslog.d/10-vmware-remote-logging.conf 파일을 편집합니다.
b 파일에 다음 줄을 추가합니다.

```
*.* @<ip>:514;RFC5424fmt
```

- c 다음 명령을 실행합니다.

```
service rsyslog restart
```

로그 메시지 ID

로그 메시지에서 메시지 ID 필드는 메시지 유형을 식별합니다. set logging-server 명령의 messageid 매개 변수를 사용하여 로깅 서버로 보낼 로그 메시지를 필터링할 수 있습니다.

표 1-1. 로그 메시지 ID

메시지 ID	예
FABRIC	호스트 노드 호스트 준비 Edge 노드 전송 영역 전송 노드 업링크 프로파일 클러스터 프로파일 Edge 클러스터 브리지 클러스터 및 끝점
SWITCHING	논리적 스위치 논리적 스위치 포트 스위칭 프로파일 스위치 보안 기능
ROUTING	논리적 라우터 논리적 라우터 포트 정적 라우팅 동적 라우팅 NAT
FIREWALL	방화벽 규칙 방화벽 규칙 섹션
FIREWALL-PKTLOG	방화벽 연결 로그 방화벽 패킷 로그
GROUPING	IP 집합 MAC 집합 NSGroup NSService NSService 그룹 VNI 풀 IP 풀
DHCP	DHCP 릴레이
SYSTEM	장치 관리(원격 syslog, ntp 등) 클러스터 관리 신뢰 관리 라이선싱 사용자 및 역할 작업 관리 설치(NSX Manager, NSX Controller) 업그레이드(NSX Manager, NSX Controller, NSX Edge 및 호스트 패키지 업그레이드) 인식 태그

표 1-1. 로그 메시지 ID (계속)

메시지 ID	예
MONITORING	SNMP 포트 연결 Traceflow
-	다른 모든 로그 메시지

Syslog 문제 해결

원격 로그 서버에 로그가 수신되지 않을 경우 다음 단계를 수행하십시오.

- 원격 로그 서버의 IP 주소를 확인합니다.
- level 매개 변수가 올바르게 구성되어 있는지 확인합니다.
- facility 매개 변수가 올바르게 구성되어 있는지 확인합니다.
- TLS 프로토콜을 사용하는 경우 프로토콜을 UDP로 설정하여, 인증서 불일치 문제가 있는지 확인합니다.
- TLS 프로토콜을 사용하는 경우 포트 6514가 양쪽 끝에 열려 있는지 확인합니다.
- 메시지 ID 필터를 제거하고, 서버에 로그가 수신되는지 확인합니다.
- `restart service rsyslogd` 명령을 사용하여 rsyslog 서비스를 다시 시작합니다.

샘플 rsyslog 구성 파일(/etc/rsyslog.conf):

```
### rsyslog config file. Customized by VMware.
### Do not edit this file by hand. Use the API to make changes.
$PreserveFQDN on
$ModLoad imklog
$ModLoad immark
module(load="imuxsock" sysSock.useSpecialParser="off")
$RepeatedMsgReduction on
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$ActionFileDefaultTemplate RSYLOG_SyslogProtocol23Format
$IncludeConfig /etc/rsyslog.d/*.conf
$template RFC5424fmt,"%<PRI%>1 %TIMESTAMP:::date-rfc3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID% %STRUCTURED-DATA% %msg%Wn"
$WorkDirectory /var/spool/rsyslog
$ModLoad imudp
$UDPServerAddress 127.0.0.1
$UDPServerRun 514
$PrivDropToUser syslog
$ActionQueueType LinkedList # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
*.info @1.2.3.4:514;RFC5424fmt # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
```

서비스 확인

실행을 중지하거나 시작하지 못하는 서비스는 문제를 일으킬 수 있습니다. 모든 서비스가 정상적으로 실행되고 있는지 확인하는 것이 중요합니다.

NSX Manager 서비스의 상태를 확인하려면 다음을 수행합니다.

```
nsxmgr> get services
Service name:      cm-inventory
Service state:     stopped

Service name:      http
Service state:     stopped
Session timeout:   1800
Connection timeout: 30
Redirect host:     (not configured)

Service name:      install-upgrade
Service state:     stopped
Enabled:           True

Service name:      liagent
Service state:     stopped

Service name:      manager
Service state:     stopped
Logging level:     info

Service name:      mgmt-plane-bus
Service state:     running

Service name:      node-mgmt
Service state:     running

Service name:      nsx-message-bus
Service state:     running

Service name:      nsx-upgrade-agent
Service state:     running

Service name:      ntp
Service state:     running

Service name:      search
Service state:     stopped

Service name:      snmp
Service state:     stopped

Start on boot:     False
Service name:      ssh
Service state:     running
```

```
Start on boot:    True
Service name:     syslog
Service state:    running
```

위의 예에서는 http 서비스가 중지되었습니다. 다음 명령을 사용하여 http 서비스를 시작할 수 있습니다.

```
nsxmgr> start service http
```

SSH 서비스

장치를 배포할 때 SSH 서비스가 사용되도록 설정되지 않은 경우 장치에 관리자로 로그인하고 다음 명령을 사용하여 사용하도록 설정할 수 있습니다.

```
start service ssh
```

호스트가 다음 명령으로 시작될 때 SSH가 시작되도록 구성할 수 있습니다.

```
set service ssh start-on-boot
```

SSH 루트 로그인을 사용하도록 설정하려면 장치에 루트로 로그인하고 /etc/ssh/sshd_config 파일을 편집하고 줄을 바꿉니다.

```
PermitRootLogin prohibit-password
```

또는 장치의 전원을 끄고 vApp 속성을 수정하여 SSH 서비스를 사용하도록 설정하고 SSH 루트 액세스를 사용하도록 설정할 수 있습니다.

다음을 사용하고

```
PermitRootLogin yes
```

다음 명령을 사용하여 sshd 서버를 다시 시작합니다.

```
/etc/init.d/ssh restart
```

지원 번들 수집

등록된 클러스터 및 패브릭 노드의 지원 번들을 수집하고 번들을 시스템에 다운로드하거나 파일 서버에 업로드할 수 있습니다.

번들을 시스템에 다운로드할 경우 각 노드에 대해 매니페스트 파일 및 지원 번들로 구성된 단일 아카이브 파일을 받게 됩니다. 번들을 파일 서버에 업로드할 경우 매니페스트 파일과 개별 번들은 파일 서버에 별도로 업로드됩니다.

NSX Cloud 참고 CSM에 대한 지원 번들을 수집하려면 CSM에 로그인하고 **시스템 > 유틸리티 > 지원 번들**로 이동한 다음 **다운로드**를 클릭하십시오. PCG에 대한 지원 번들은 다음 지침을 사용하여 NSX Manager에서 사용할 수 있습니다. PCG에 대한 지원 번들에는 모든 워크로드 VM에 대한 로그도 포함되어 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.
- 3 **지원 번들** 탭을 클릭합니다.
- 4 대상 노드를 선택합니다.
사용 가능한 노드 유형은 관리 노드, 컨트롤러 노드, Edge, 호스트 및 공용 클라우드 게이트웨이입니다.
- 5 (선택 사항) 로그 수명(일)을 지정하여 지정된 일 수보다 오래된 로그를 제외합니다.
- 6 (선택 사항) 코어 파일 및 감사 로그를 포함 또는 제외할지를 나타내는 스위치를 전환합니다.

참고 코어 파일 및 감사 로그에는 암호 또는 암호화 키와 같은 중요한 정보가 포함될 수 있습니다.

- 7 (선택 사항) 확인란을 선택하여 번들을 파일 서버에 업로드합니다.
- 8 **번들 수집 시작**을 클릭하여 지원 번들 수집을 시작합니다.
존재하는 로그 파일의 개수에 따라 노드마다 몇 분 정도 걸릴 수 있습니다.
- 9 수집 프로세스 상태를 모니터링합니다.
상태 필드에는 지원 번들 수집을 완료한 노드의 백분율이 표시됩니다.
- 10 번들을 파일 서버로 전송하는 옵션이 설정되지 않은 경우 **다운로드**를 클릭하여 번들을 다운로드합니다.

계층 2 연결 문제 해결

2

예를 들어 동일한 논리적 스위치에 연결된 두 개의 VIF(가상 인터페이스) 사이에 통신 오류가 있는 경우(예: 한 VM에서 다른 VM에 ping할 수 없는 경우) 이 섹션의 단계를 수행하여 오류를 해결할 수 있습니다.

시작하기 전에 두 논리적 포트 사이에 트래픽을 차단하는 방화벽 규칙이 없는지 확인합니다. 연결 문제를 해결 하려면 이 섹션에 있는 항목의 순서를 따르는 것이 좋습니다.

본 장은 다음 항목을 포함합니다.

- NSX Manager 및 NSX Controller 클러스터 상태 확인
- 논리적 포트 확인
- 전송 노드 상태 확인
- 논리적 스위치 상태 확인
- CCP에서 논리적 스위치 확인
- 로컬 제어부 상태 확인
- 구성 세션 문제 해결
- L2 세션 문제 해결
- 오버레이 논리적 스위치에 대한 데이터부 문제 해결
- VLAN 논리적 스위치에 대한 데이터부 문제 해결
- 오버레이 논리적 스위치에 대한 ARP 문제 해결
- VLAN 논리적 스위치 또는 ARP가 해결된 경우 패킷 손실 문제 해결

NSX Manager 및 NSX Controller 클러스터 상태 확인

NSX Manager 및 NSX Controller 클러스터의 상태가 정상이고 컨트롤러가 NSX Manager에 연결되어 있는지 확인합니다.

절차

- 1 NSX Manager에서 다음 CLI 명령을 실행하여 상태가 안정적인지 확인합니다.

```
NSX-Manager> get management-cluster status  
Number of nodes in management cluster: 1
```

```
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online
```

```
Management cluster status: STABLE
```

```
Number of nodes in control cluster: 3
```

```
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

- 2 NSX Controller에서 다음 CLI 명령을 실행하여 상태가 활성화인지 확인합니다.

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
  uuid                                address                status
  ---                                -
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.110.201        active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.110.202        active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.110.203        active
```

- 3 NSX Controller에서 다음 CLI 명령을 실행하여 NSX Manager에 연결되어 있는지 확인합니다.

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

논리적 포트 확인

논리적 포트가 동일한 논리적 스위치에 구성되어 있고 작동 상태인지 확인합니다.

절차

- 1 NSX Manager GUI에서 논리적 포트 UUID를 가져옵니다.
- 2 각 논리적 포트에 대해 다음 API 호출을 실행하여 논리적 포트가 동일한 논리적 스위치에 있는지 확인합니다.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 3 각 논리적 포트에 대해 다음 API 호출을 실행하여 작동 상태인지 확인합니다.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>/status
```

전송 노드 상태 확인

전송 노드의 상태를 확인합니다.

절차

- ◆ 다음 API 호출을 실행하여 전송 노드의 상태를 가져옵니다.

```
GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-ID>/state
```

호출이 RPC timeout 오류를 반환하면 다음과 같은 문제 해결 단계를 수행합니다.

- `/etc/init.d/nsx-opsAgent status`를 실행하여 opsAgent가 실행 중인지 확인합니다.
- `/etc/init.d/nsx-mpa status`를 실행하여 nsx-mpa가 실행 중인지 확인합니다.
- nsx-mpa가 NSX Manager에 연결되어 있는지 확인하려면 nsx-mpa 하트비트 로그를 확인합니다.
- opsAgent가 NSX Manager에 연결되어 있는지 확인하려면 nsx-opsAgent 로그를 확인합니다. opsAgent가 NSX Manager에 연결되어 있으면 다음 메시지가 표시됩니다.

```
Connected to mpa, cookie: ...
```

- opsAgent가 HostConfigMsg 처리를 멈추고 있는지 확인하려면 nsx-opsAgent 로그를 확인합니다. 그러한 경우 RMQ 요청 메시지가 표시되지만 응답이 전송되지 않거나 오랫동안 지연된 후에 전송됩니다.
- HostConfigMsg를 실행하는 동안 opsAgent가 충돌했는지 확인합니다.
- RMQ 메시지가 호스트로 전달되는 데 시간이 오래 걸리는지 확인하려면 NSX Manager와 호스트에서 로그 메시지의 타임 스탬프를 비교합니다.

호출이 `partial_success` 오류를 반환하는 경우 여러 가지 원인이 있을 수 있습니다. 먼저 nsx-opsAgent 로그를 확인합니다. ESXi 호스트에서 `hostd.log` 및 `vmkernel.log`를 확인하십시오. KVM에서는 `syslog`에 모든 로그가 유지됩니다.

논리적 스위치 상태 확인

논리적 스위치의 상태를 확인합니다.

절차

- ◆ 다음 API 호출을 실행하여 논리적 스위치의 상태를 가져옵니다.

```
GET https://<nsx-mgr>/api/v1/logical-switches/<logical-switch-ID>/state
```

호출이 `partial_success` 오류를 반환하면 NSX Manager가 논리적 스위치 구성을 푸시하지 못했거나 응답을 받지 못한 전송 노드 목록이 응답에 포함됩니다. 문제 해결 단계는 전송 노드에 대한 문제 해결 단계와 유사합니다. 다음을 확인하십시오.

- 모든 필수 구성 요소가 설치되어 실행 중입니다.
- nsx mpa가 NSX Manager에 연결되어 있습니다.
- nsxa가 세로 스위칭에 연결되어 있습니다.
- nsxa.log 및 nsxaVim.log에서 논리적 스위치 ID를 grep하여 전송 노드에서 논리적 스위치 구성을 수신했는지 확인합니다.
- nsxa 및 nsx-mpa 가동 시간을 확인합니다. Syslog 파일에서 nsxa 로그 메시지를 grep하여 nsxa가 언제 시작 및 중지되었는지 확인합니다.

- 세로 스위칭에 대한 nsxa의 연결 시간을 확인합니다. nsxa가 세로 스위칭에 연결되어 있지 않을 때 논리적 스위치 구성이 호스트로 전송되면 구성이 호스트에 전달되지 않을 수 있습니다.

KVM에서 논리적 스위치 구성이 호스트에 푸시되지 않습니다. 따라서 논리적 스위치 문제의 대부분이 관리부에 있을 가능성이 있습니다.

ESXi에서 불투명 네트워크는 논리적 스위치에 매핑됩니다. 논리적 스위치를 사용하려면 사용자는 vCenter Server 또는 vSphere API를 사용하여 VM을 불투명 네트워크에 연결합니다.

CCP에서 논리적 스위치 확인

논리적 스위치가 CCP(중앙 제어부)에 있는지 확인합니다.

절차

- ◆ NSX Controller에서 다음 CLI 명령을 실행하여 논리적 스위치가 있는지 확인합니다.

```
NSX-Controller1> get logical switches
VNI    UUID                                     Name
52104  feab22ec-94b2-46f4-88f8-f9d44a416272  ls1
```

참고 이 CLI 명령은 VLAN 지원 논리적 스위치를 나열하지 않습니다.

로컬 제어부 상태 확인

오버레이 논리적 스위치에 대해 호스트의 netcpa가 중앙 제어부에 연결되어 있는지 확인합니다.

사전 요구 사항

논리적 스위치가 켜져 있는 컨트롤러를 찾습니다. [CCP에서 논리적 스위치 확인](#)의 내용을 참조하십시오.

절차

- 1 SSH를 사용하여 논리적 스위치가 켜져 있는 컨트롤러에 연결합니다.
- 2 다음 명령을 실행하고 이 VNI에 연결된 하이퍼바이저가 컨트롤러에 표시되는지 확인합니다.

```
get logical-switch 5000 connection-table
```

- 3 하이퍼바이저에서 /bin/nsxcli 명령을 실행하여 NSX CLI를 시작합니다.
- 4 다음 명령을 실행하여 CCP 세션을 가져옵니다.

```
host1> get ccp-session
Session Index State Controller
Config 0      UP    10.33.74.163
L2      5000  UP    10.33.74.163
```

CCP 클러스터의 CCP 노드 중 하나에 구성 세션이 표시되는 것을 볼 수 있습니다. 모든 오버레이 논리적 스위치의 경우, CCP 클러스터의 CCP 노드 중 하나에 대한 L2 세션이 표시됩니다. VLAN 논리적 스위치의 경우 CCP 연결이 없습니다.

구성 세션 문제 해결

CCP 구성 세션이 작동하지 않으면 MPA 및 netcpa의 상태를 확인합니다.

절차

- 1 다음 API 호출을 실행하여 MPA가 NSX Manager에 연결되어 있는지 확인합니다.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 2 하이퍼바이저에서 `/bin/nsxcli` 명령을 실행하여 NSX CLI를 시작합니다.
- 3 다음 명령을 실행하여 `node-uuid`를 가져옵니다.

```
host1> get node-uuid
0c123dd4-8199-11e5-95e2-73cc1cd9b614
```

- 4 다음 명령을 실행하여 NSX Manager가 CCP 정보를 호스트에 푸시했는지 확인합니다.

```
cat /etc/vmware/nsx/config-by-vsm.xml
```

- 5 `config-by-vsm.xml`에 CCP 정보가 있으면 전송 노드가 하이퍼바이저에 구성되어 있는지 확인합니다.

NSX Manager는 전송 노드 생성 단계에서 하이퍼바이저에 대한 호스트 인증서를 전송합니다. 호스트의 연결을 수락하려면 CCP에 호스트 인증서가 있어야 합니다.

- 6 `/etc/vmware/nsx/host-cert.pem`에서 호스트 인증서의 유효성을 확인합니다.

인증서는 NSX Manager가 호스트에 대해 가지고 있는 인증서와 동일해야 합니다.

- 7 다음 명령을 실행하여 `netcpa`의 상태를 확인합니다.

ESXi의 경우:

```
/etc/init.d/netcpad status
```

KVM의 경우:

```
/etc/init.d/nsx-agent status
```

8 netcpa를 시작하거나 다시 시작합니다.

ESXi에서 netcpa가 실행 중이 아니면 netcpa를 시작하거나 실행 중이면 netcpa를 다시 시작합니다.

```
/etc/init.d/netcpad start
```

```
/etc/init.d/netcpad restart
```

KVM에서 netcpa가 실행 중이 아니면 netcpa를 시작하거나 실행 중이면 netcpa를 다시 시작합니다.

```
/etc/init.d/nsx-agent start
```

```
/etc/init.d/nsx-agent restart
```

9 구성 세션이 여전히 작동하지 않으면 기술 지원 번들을 수집하여 VMware 지원팀에 문의하십시오.

L2 세션 문제 해결

이 항목은 오버레이 논리적 스위치에만 적용됩니다.

절차

- 1 하이퍼바이저에서 `/bin/nsxcli` 명령을 실행하여 NSX CLI를 시작합니다.
- 2 다음 명령을 실행하여 논리적 스위치가 호스트에 있는지 확인합니다.

```
host1> get logical-switches
```

- 3 포트의 상태가 `admin down`이 아닌지 확인합니다.

ESXi에서 `net-dvs`를 실행하고 응답을 살펴봅니다. 예를 들면 다음과 같습니다.

```
port 63eadf53-ff92-4a0e-9496-4200e99709ff:
com.vmware.port.extraConfig.opaqueNetwork.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.type = nsx.LogicalSwitch , propType = RUNTIME
com.vmware.common.port.block = false, ... <- Make sure the value is false.
com.vmware.vswitch.port.vxlan = ...
com.vmware.common.port.volatile.status = inUse ... <- make sure the value is inUse.
```

논리적 포트가 차단된 상태로 끝나면 기술 지원 번들을 수집하여 VMware 지원팀에 문의하십시오. 그 사이, 다음 명령을 실행하여 DVS 이름을 가져옵니다.

```
[root@host1:~] net-dvs | grep nsx-switch
com.vmware.common.alias = nsx-switch , propType = CONFIG
```

다음 명령을 실행하여 포트 차단을 해제합니다.

```
[root@host1:~] net-dvs -s com.vmware.common.port.block=false <DVS-NAME> -p <logical-port-ID>
```

KVM에서 `ovs-vsctl list interface`를 실행하여 해당 VIF UUID가 있는 인터페이스가 있고 `admin_state`가 작동하는지 확인합니다. OVSDDB의 VIF UUID는 `external-ids:iface-id`에서 볼 수 있습니다.

오버레이 논리적 스위치에 대한 데이터부 문제 해결

이 섹션의 단계는 구성 및 런타임 상태가 정상일 때 오버레이 스위치를 통해 서로 다른 하이퍼바이저에 있는 VM 사이의 연결 문제를 해결하기 위한 단계입니다.

VM이 동일한 하이퍼바이저에 있으면 [오버레이 논리적 스위치에 대한 ARP 문제 해결](#)로 이동하십시오.

절차

- 1 논리적 스위치가 있는 컨트롤러에서 다음 명령을 실행하여 CCP에 올바른 VTEP 목록이 있는지 확인합니다.

```
controller1> get logical-switch 5000 vtep
```

- 2 각 하이퍼바이저에서 다음 NSX CLI 명령을 실행하여 올바른 VTEP 목록이 있는지 확인합니다.
ESXi의 경우:

```
host1> get logical-switch <logical-switch-UUID> tep-table
```

또는 다음 셸 명령을 실행하여 VTEP 정보를 확인할 수 있습니다.

```
[root@host1:~] net-vd12 -M vtep -s vds -n VNI
```

KVM의 경우:

```
host1> get logical-switch <logical-switch-UUID or VNI> tep-table
```

- 3 하이퍼바이저의 VTEP가 서로 ping할 수 있는지 확인합니다.

ESXi shell prompt:

```
host1> ping ++netstack=vxlan <remote-VTEP-IP>
```

KVM shell prompt:

```
host1> ping <remote-VTEP-IP>
```

VTEP가 서로 ping할 수 없는 경우에는 다음을 수행합니다.

- a 전송 노드를 생성할 때 지정된 전송 VLAN이 언더레이에 필요한 VLAN과 일치하는지 확인합니다. 언더레이의 액세스 포트를 사용하는 경우 전송 VLAN을 0으로 설정해야 합니다. 전송 VLAN을 지정하는 경우 하이퍼바이저가 연결하는 언더레이 스위치 포트는 트렁크 모드에서 이 VLAN을 허용하도록 구성되어야 합니다.
- b 언더레이 연결을 확인합니다.

4 VTEP 사이의 BFD 세션이 작동하는지 확인합니다.

ESXi에서 `net-vd12 -M bfd`를 실행하고 응답을 살펴봅니다. 예를 들면 다음과 같습니다.

```
BFD count: 1
=====
Local IP: 192.168.48.35, Remote IP: 192.168.197.243, Local State: up, Remote State: up, Local
Diag: No Diagnostic, Remote Diag: No Diagnostic, minRx: 1000000, isDisabled: 0
```

KVM의 경우 원격 IP에 대한 GENEVE 인터페이스를 찾습니다.

```
ovs-vsctl list interface <GENEVE-interface-name>
```

인터페이스 이름을 모르면 `ovs-vsctl find Interface type=geneve`를 실행하여 모든 터널 인터페이스를 반환합니다. BFD 정보를 찾습니다.

원격 VTEP에 대한 GENEVE 인터페이스를 찾을 수 없는 경우 `nsx-agent`가 실행 중이고 OVS 통합 브리지가 `nsx-agent`에 연결되어 있는지 확인합니다.

```
[root@host1 ~]# ovs-vsctl show
96c9e543-fc68-448a-9882-6e161c313a5b
  Manager "tcp:127.0.0.1:6632"
    is_connected: true
  Bridge nsx-managed
    Controller "tcp:127.0.0.1:6633"
      is_connected: true
    Controller "unix:ovs-l3d.mgmt"
      is_connected: true
    fail_mode: secure
```

VLAN 논리적 스위치에 대한 데이터부 문제 해결

이 섹션의 단계는 구성 및 런타임 상태가 정상일 때 언더레이에 구성된 VLAN을 통해 서로 다른 하이퍼바이저에 있는 VM 사이의 연결 문제를 해결하기 위한 단계입니다.

VM이 동일한 하이퍼바이저에 있고 모든 구성 및 런타임 상태가 정상적인 경우에는 [오버레이 논리적 스위치에 대한 ARP 문제 해결](#)로 이동하십시오.

절차

- ◆ 언더레이가 트렁크 모드에서 논리적 스위치에 대한 VLAN에 대해 구성되어 있는지 확인합니다.

ESXi에서 `net-dvs`를 실행하고 논리적 포트를 찾아서 논리적 포트에 VLAN이 구성되어 있는지 확인합니다. 예:

```
port 63eadf53-ff92-4a0e-9496-4200e99709ff:
  com.vmware.common.port.volatile.vlan = VLAN 1000 propType = RUNTIME VOLATILE
```

KVM에서 VLAN 논리적 스위치는 통합 브리지의 개방형 흐름 규칙으로 구성됩니다. 즉, VIF에서 수신된 트래픽의 경우 VLAN X로 태그를 지정하고 패치 포트에서 PIF 브리지로 전달합니다. `ovs-vsctl list interface`를 실행하고 NSX 관리 브리지와 NSX 스위치 브리지 사이에 패치 포트가 있는지 확인합니다.

오버레이 논리적 스위치에 대한 ARP 문제 해결

이 섹션의 단계는 오버레이 스위치에서 패킷이 손실되는 문제를 해결하기 위한 단계입니다.

VLAN 지원 논리적 스위치를 보려면 [VLAN 논리적 스위치 또는 ARP가 해결된 경우 패킷 손실 문제 해결](#)로 이동하십시오.

다음 문제 해결 단계를 수행하기 전에 각 VM에 `arp -n` 명령을 실행합니다. 두 VM에서 ARP가 성공적으로 해결되면 이 섹션의 단계를 수행할 필요가 없습니다. 대신 다음 섹션 [VLAN 논리적 스위치 또는 ARP가 해결된 경우 패킷 손실 문제 해결](#)로 이동하십시오.

절차

- ◆ 두 끝점이 모두 ESXi이고 ARP 프록시가 논리적 스위치에서 사용되도록 설정된 경우(오버레이 논리적 스위치에서만 지원됨) CCP 및 하이퍼바이저에서 ARP 테이블을 확인합니다.

CCP의 경우:

```
controller1> get logical-switch 5000 arp-table
```

하이퍼바이저에서 NSX CLI를 시작하고 다음 명령을 실행합니다.

```
host1> get logical-switch <logical-switch-UUID> arp-table
```

ARP 테이블을 가져오면 올바른 ARP 프록시 상태인지 여부만 알 수 있습니다. 프록시를 통해 ARP 응답이 수신되지 않거나 호스트가 KVM이고 ARP 프록시를 지원하지 않는 경우 데이터 경로는 ARP 요청을 브로드캐스트해야 합니다. BUM 트래픽 전달에 문제가 있을 수 있습니다. 다음 단계를 시도합니다.

- 논리적 스위치에 대한 복제 모드가 MTEP인 경우 NSX Manager GUI에서 논리적 스위치의 복제 모드를 SOURCE로 변경합니다. 이렇게 하면 문제가 해결되고 ping이 작동하기 시작합니다.
- 정적 ARP 항목을 추가하고 나머지 데이터 경로가 작동하는지 확인합니다.

VLAN 논리적 스위치 또는 ARP가 해결된 경우 패킷 손실 문제 해결

자동화된 Traceflow 도구를 사용하거나 수동으로 패킷을 추적하여 패킷 손실 문제를 해결할 수 있습니다.

Traceflow 도구를 실행하려면 NSX Manager GUI에서 **도구 > Traceflow**로 이동합니다. 자세한 내용은 "NSX-T 관리 가이드"를 참조하십시오.

절차

- ◆ 수동으로 패킷을 추적하려면 다음을 수행하십시오.

ESXi에서 `net-stats -l`을 실행하여 VIF의 스위치 포트 ID를 가져옵니다. 소스 및 대상 VIF가 동일한 하이퍼바이저에 있으면 다음 명령을 실행합니다.

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --switchport <dst-switch-port-ID> --dir=1
```

소스 및 대상 VIF가 서로 다른 하이퍼바이저에 있는 경우 소스 VIF를 호스팅하는 하이퍼바이저에서 다음 명령을 실행합니다.

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --uplink <uplink-name> --dir=1
```

대상 VIF를 호스팅하는 하이퍼바이저에서 다음 명령을 실행합니다.

```
pktcap-uw --uplink <uplink-name> --dir=0
pktcap-uw --switchport <dest-switch-port-ID> --dir=1
```

KVM에서 소스 및 대상 VIF가 동일한 하이퍼바이저에 있는 경우 다음 명령을 실행합니다.

```
ovs-dpctl dump-flows
```

설치 문제 해결

3

이 섹션에서는 설치 문제 해결에 대한 정보를 제공합니다.

기본 인프라 서비스

다음 서비스는 장치와 하이퍼바이저를 비롯해 vCenter Server가 계산 관리자로 사용되는 경우 vCenter Server에서도 실행 중이어야 합니다.

- NTP
- DNS

방화벽이 NSX-T 구성 요소와 하이퍼바이저 간의 트래픽을 차단하지 않아야 합니다. 필수 포트가 구성 요소 간에 열려 있어야 합니다.

NSX Manager에서 DNS 캐시를 플러시하려면 SSH를 사용하여 NSX Manager에 루트로 로그인하고 다음 명령을 실행합니다.

```
root@nsx-mgr-01:~# /etc/init.d/resolvconf restart
[ ok ] Restarting resolvconf (via systemctl): resolvconf.service.
```

그런 다음 DNS 구성 파일을 확인할 수 있습니다.

```
root@nsx-mgr-01:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.253.1
search mgt.sg.lab
```

호스트와 컨트롤러 및 관리자 간의 통신 확인

NSX-T CLI 명령을 사용하여 ESXi 호스트에서:

```
esxi-01.corp.local> get managers
- 192.168.110.19 Connected

esxi-01.corp.local> get controllers
```

Controller IP	Port	SSL	Status	Is Physical Master	Session State	Controller FQDN
192.168.110.16	1235	enabled	connected	true	up	NA

NSX-T CLI 명령을 사용하여 KVM 호스트에서:

```
kvm-01> get managers
- 192.168.110.19 Connected

kvm-01> get controllers
```

Controller IP	Port	SSL	Status	Is Physical	Master	Session State	Controller FQDN
192.168.110.16	1235	enabled	connected	true		up	NA

호스트 CLI 명령을 사용하여 ESXi 호스트에서:

```
[root@esxi-01:~] esxcli network ip connection list | grep 1235
tcp          0      0 192.168.110.53:42271          192.168.110.16:1235 ESTABLISHED    67702
newreno netcpa
[root@esxi-01:~]
[root@esxi-01:~] esxcli network ip connection list | grep 5671
tcp          0      0 192.168.110.253:11721        192.168.110.19:5671 ESTABLISHED    2103688 newreno mpa
tcp          0      0 192.168.110.253:30977        192.168.110.19:5671 ESTABLISHED    2103688 newreno mpa
```

호스트 CLI 명령을 사용하여 KVM 호스트에서:

```
root@kvm-01:/home/vmware# netstat -nap | grep 1235
tcp          0      0 192.168.110.55:53686        192.168.110.16:1235 ESTABLISHED    2554/netcpa
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware# netstat -nap | grep 5671
tcp          0      0 192.168.110.55:50108        192.168.110.19:5671 ESTABLISHED    2870/mpa
tcp          0      0 192.168.110.55:50110        192.168.110.19:5671 ESTABLISHED    2870/mpa

root@kvm-01:/home/vmware# tcpdump -i ens32 port 1235 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
<truncated output>
03:46:27.040461 IP nsxcontroller01.corp.local.1235 > kvm-01.corp.local.38754: Flags [P.], seq
3315301231:3315301275, ack 2671171555, win 323, length 44
03:46:27.040509 IP kvm-01.corp.local.38754 > nsxcontroller01.corp.local.1235: Flags [.], ack 44, win 1002, length
0
^C
<truncated output>
root@kvm-01:/home/vmware#

root@kvm-01:/home/vmware# tcpdump -i ens32 port 5671 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
03:51:16.802934 IP kvm-01.corp.local.58954 > nsxmgr01.corp.local.amqs: Flags [P.], seq 1153:1222, ack 1790, win
259, length 69
03:51:16.823328 IP nsxmgr01.corp.local.amqs > kvm-01.corp.local.58954: Flags [P.], seq 1790:1891, ack 1222, win
254, length 101
^C
<truncated output>
```

호스트 등록 실패

NSX-T가 잘못된 IP 주소를 사용하는 경우 호스트 등록이 실패합니다. 이 문제는 호스트에 여러 IP 주소가 있는 경우에 발생할 수 있습니다. 전송 노드를 삭제하려고 하면 링크가 끊어진 상태로 남습니다. 문제를 해결하려면 다음을 수행합니다.

- **패브릭 > 노드 > 호스트**로 이동하고 호스트를 편집하고 관리를 제외한 모든 IP 주소를 제거합니다.
- 오류를 클릭하고 **해결**을 선택합니다.

KVM 호스트 문제

KVM 호스트 문제는 때때로 충분하지 않은 디스크 공간으로 인해 발생합니다. /boot 디렉토리는 빨리 찼 수 있으며 다음과 같은 오류를 초래할 수 있습니다.

- 호스트에 소프트웨어를 설치하지 못했습니다.
- 디바이스에 남아 있는 공간이 없습니다.

df -h 명령을 실행하여 사용 가능한 스토리지를 확인할 수 있습니다. /boot 디렉토리가 100%에 도달한 경우 다음을 수행할 수 있습니다.

- `sudo dpkg --get-selections | grep ^ii`를 실행하여 모든 커널이 설치되었는지 확인합니다.
- `uname -r`를 실행하여 현재 실행 중인 커널을 확인합니다. 이 커널을 제거하지 마십시오(linux-image).
- `apt-get purge`를 사용하여 더 이상 필요하지 않은 이미지를 제거합니다. 예를 들어 `sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic`를 실행합니다.
- 호스트를 재부팅합니다.
- NSX Manager에서 오류를 확인하고 **해결**을 선택합니다.
- VM의 전원이 켜져 있는지 확인합니다.

Edge VM을 배포할 때 구성 오류 발생

Edge VM을 배포한 후 NSX Manager가 VM의 상태를 **구성 오류**로 표시합니다. 관리자 로그에는 다음과 유사한 메시지가 있습니다.

```
nsx-manager NSX - FABRIC [nsx@6876 comp="nsx-manager" errorCode="MP16027" subcomp="manager"] Edge
758ad396-0754-11e8-877e-005056abf715 is not ready for configuration error occurred, error detail is NSX Edge
configuration has failed. The host does not support required cpu features: ['aes'].
```

Edge 데이터 경로 서비스를 다시 시작하면 VM이 해당 문제를 해결합니다.

전송 노드 강제 제거

다음 API 호출을 수행하여 링크가 끊어진 상태에 멈춰 있는 전송 노드를 제거할 수 있습니다.

```
DELETE https://<NSX Manager>/api/v1/transport-nodes/<TN ID>?force=true
```

NSX Manager는 호스트에서 실행 중인 활성 VM이 있는지 여부를 검증하지 않습니다. N-VDS 및 VIB를 삭제해야 합니다. 계산 관리자를 통해 추가된 노드가 있는 경우 먼저 계산 관리자를 삭제한 다음 노드를 삭제합니다. 전송 노드도 삭제됩니다.

라우팅 문제 해결

4

NSX-T에는 라우팅 문제를 해결하기 위한 기본 제공 도구가 있습니다.

Traceflow

Traceflow를 사용하여 패킷 흐름을 검사할 수 있습니다. 전송, 삭제, 수신 및 전달된 패킷을 확인할 수 있습니다. 패킷이 삭제된 경우 이유가 표시됩니다. 예를 들어 패킷은 방화벽 규칙 때문에 삭제될 수 있습니다.

라우팅 테이블 확인

서비스 라우터의 라우팅 테이블을 확인하려면 다음 명령을 실행합니다.

```
edge01> get logical-router
Logical Route
UUID                                VRF  LR-ID  Name                                Type                                Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666 0     0      SR-t0-router                        TUNNEL                             3
c9393d0c-1fcf-4c34-889d-2da1eeee25b8 1     10     SR-t0-router                        SERVICE_ROUTER_TIER0               5
9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5 2     8      DR-t1-router01                     DISTRIBUTED_ROUTER_TIER1            6
c91eb7c5-0297-4fed-9c22-b96df1c9b80f 3     9      DR-t0-router                        DISTRIBUTED_ROUTER_TIER0            4

edge01> vrf 1
edge01(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
t1l: Tier1-LB VIP, t1s: Tier1-LB SNAT

Total number of routes: 25

b  10.10.20.0/24      [20/0]      via 192.168.140.1
b  10.10.30.0/24      [20/0]      via 192.168.140.1
b  10.20.20.0/24      [20/0]      via 192.168.140.1
b  10.20.30.0/24      [20/0]      via 192.168.140.1
b  30.0.0.0/8         [20/0]      via 192.168.140.1
rl 100.64.80.0/31     [0/0]       via 169.254.0.1
rl 100.64.80.2/31    [0/0]       via 169.254.0.1
rl 100.64.80.4/31    [0/0]       via 169.254.0.1
<TRUNCATED OUTPUT>
b  192.168.200.0/24   [20/0]      via 192.168.140.1
```

```

b    192.168.210.0/24    [20/0]    via 192.168.140.1
b    192.168.220.0/24    [20/0]    via 192.168.140.1
b    192.168.230.0/24    [20/0]    via 192.168.140.1
b    192.168.240.0/24    [20/0]    via 192.168.140.1

```

인터페이스의 IP 주소를 가져오려면 다음 명령을 실행합니다.

```

edge01(tier0_sr)> get interfaces
Logical Router
UUID                                VRF  LR-ID  Name                Type
c9393d0c-1fcf-4c34-889d-2da1eeee25b8  1    10     SR-t0-router        SERVICE_ROUTER_TIER0
interfaces
  interface    : 977ac2eb-8ab7-40e9-8abe-782a438c749a
  ifuid        : 285
  name         : uplink01
  mode         : lif
  IP/Mask      : 192.168.140.3/24
  MAC         : 00:50:56:b5:d5:64
  LS port      : 14391f86-efef-4e3d-98c3-f291c17d13f8
  urpf-mode    : STRICT_MODE
  admin        : up
  MTU          : 1600

  interface    : 6af81d72-4d32-5f66-b7ae-403e617290e5
  ifuid        : 270
  mode         : blackhole

  interface    : 015e709d-6079-5c19-9556-8be2e956f775
  ifuid        : 269
  mode         : cpu

  interface    : 3f40f838-eb8a-4f35-854c-ea8bb872dc47
  ifuid        : 272
  name         : bp-sr0-port
  mode         : lif
  IP/Mask      : 169.254.0.2/28
  MAC         : 02:50:56:56:53:00
  VNI         : 25489
  LS port      : 770a208d-27fa-4f8d-afad-a9c41ca6295b
  urpf-mode    : NONE
  admin        : up
  MTU          : 1500

  interface    : 00003300-0000-0000-0000-00000000000a
  ifuid        : 263
  mode         : loopback
  IP/Mask      : 127.0.0.1/8

```

T1 경로 보급

T0 라우터 이상에서 표시되도록 T1 경로를 보급해야 합니다. NSX Connected, NAT, Static, LB VIP 및 LB SNAT와 같이 보급할 수 있는 서로 다른 유형의 경로가 있습니다.

방화벽 문제 해결

5

이 섹션에서는 방화벽 문제 해결에 대한 정보를 제공합니다.

본 장은 다음 항목을 포함합니다.

- ESXi 호스트에 적용되는 방화벽 규칙 결정
- KVM 호스트에 적용되는 방화벽 규칙 결정
- 방화벽 패킷 로그

ESXi 호스트에 적용되는 방화벽 규칙 결정

ESXi 호스트의 방화벽 문제를 해결하기 위해 호스트에 적용되는 방화벽 규칙을 살펴볼 수 있습니다.

ESXi 호스트의 dvfilter 목록을 가져옵니다.

```
[root@esxi-01:~] summarize-dvfilter
<TRUNCATED OUTPUT>
world 70181 vmm0:app-01a vcluid: '50 35 9c 70 18 8e 99 1d-3c f9 8e cc 6b 27 4c 6f'
port 50331655 app-01a.eth0
vNic slot 2
name: nic-70181-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation
world 70179 vmm0:web-02a vcluid: '50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
vNic slot 2
name: nic-70179-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation
```

특정 VM에 대한 dvfilter를 찾습니다.

```
[root@esxi-01:~] summarize-dvfilter | less -p web

world 70179 vmm0:web-02a vcUuid:'50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
  vNic slot 2
  name: nic-70179-eth0-vmware-sfw.2
agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
.
.
.
```

특정 dvfilter(이 예에서는 nic-70227-eth0-vmware-sfw.2가 dvfilter 이름임)에 적용되는 방화벽 규칙을 결정합니다.

```
[root@esxi-02:~] vsipioctl getrules -f nic-70227-eth0-vmware-sfw.2
ruleset mainrs {
rule 3072 at 1 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443 accept with log;
rule 3072 at 2 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80 accept with log;
rule 3074 at 3 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
rule 3074 at 4 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 22 accept with log;
rule 3075 at 5 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
rule 3076 at 6 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 443 accept with log;
rule 3076 at 7 inout protocol icmp typecode 8:0 from ip 192.168.110.10 to addrset rdst3076 accept with log;
rule 3076 at 8 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 22 accept with log;
rule 3076 at 9 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 80 accept with log;
rule 2 at 10 inout protocol any from any to any accept with log;
}

ruleset mainrs_L2 {
rule 1 at 1 inout ethertype any stateless from any to any accept;
}
```

특정 dvfilter에서 사용되는 주소 집합의 목록을 가져옵니다.

```
[root@esxi-02:~] vsipioctl getaddrsets -f nic-70227-eth0-vmware-sfw.2
addrset 48822ec3-2670-497b-82f9-524618c16877 {
ip 172.16.10.13,
mac 52:54:00:42:4d:38,
}
addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}
addrset b695c8df-9894-4068-a5e7-5504fe48d459 {
```

```
ip 172.16.30.11,
mac 52:54:00:64:0e:4f,
}
addrset rdst3076 {
ip 172.16.10.13,
ip 172.16.30.11,
mac 52:54:00:42:4d:38,
mac 52:54:00:64:0e:4f,
}
```

특정 dvfilter를 통해 흐름을 확인합니다.

```
[root@esxi-02:~] vsipioctl getflows -f nic-75360-eth0-vmware-sfw.2
Count retrieved from kernel active(L3,L4)=20, active(L2)+inactive(L3,L4)=0, drop(L2,L3,L4)=0
a5d914f7a5b85fe5 Active tcp 0800 IN 3076 0 0 192.168.110.10:Unknown(51281) -> 172.16.10.11:ssh(22) 513
FINWAIT2:FINWAIT2 4304 5177 34 33
a5d914f7a5b86001 Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60006) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b86006 Active igmp 0800 IN 2 0 0 0.0.0.0 -> 224.0.0.1 36 0 1 0
a5d914f7a5b86011 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60098) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5411 9 6
a5d914f7a5b86012 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46001) -> 172.16.20.11:Unknown(8443) 815
FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86013 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(40080) -> 192.168.110.10:domain(53) 268 140 2 2
a5d914f7a5b86014 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(59251) -> 192.168.110.10:domain(53) 268 140 2 2
a5d914f7a5b86015 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0 0 72 0 1
a5d914f7a5b86016 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0 0 72 0 1
a5d914f7a5b86017 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60104) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5451 9 7
a5d914f7a5b86018 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46002) -> 172.16.20.11:Unknown(8443) 815
TIMEWAIT:TIMEWAIT 7314 1230 8 9
a5d914f7a5b86019 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60110) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 373 5451 8 7
a5d914f7a5b8601a Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46003) -> 172.16.20.11:Unknown(8443) 815
FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b8601b Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60114) -> 172.16.10.11:http(80) 328
TIMEWAIT:TIMEWAIT 413 5451 9 7
a5d914f7a5b8601c Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46004) -> 172.16.20.11:Unknown(8443) 815
TIMEWAIT:TIMEWAIT 7262 1218 7 9
a5d914f7a5b8601d Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60060) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b8601e Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60120) -> 172.16.10.11:http(80) 320
TIMEWAIT:TIMEWAIT 373 5411 8 6
a5d914f7a5b8601f Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46005) -> 172.16.20.11:Unknown(8443) 815
FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86020 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60126) -> 172.16.10.11:http(80) 229 EST:EST
173 5371 3 5
a5d914f7a5b86021 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46006) -> 172.16.20.11:Unknown(8443) 815
FINWAIT2:FINWAIT2 7418 1230 10 9
```

KVM 호스트에 적용되는 방화벽 규칙 결정

KVM 호스트의 방화벽 문제를 해결하기 위해 호스트에 적용되는 방화벽 규칙을 살펴볼 수 있습니다.

KVM 호스트의 방화벽 규칙에 따르는 VIF의 목록을 가져옵니다.

```
# ovs-appctl -t /var/run/openvswitch/nsxa-ctl dfw/vif
Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
Port name   : db-01a-eth0
Port number : 2
```

출력이 비어 있는 경우 노드와 컨트롤러 간의 연결 문제를 확인합니다.

특정 VIF(이 예에서는 da95fc1e-65fd-461f-814d-d92970029bf0이 VIF ID임)에 적용되는 규칙의 목록을 가져옵니다.

```
# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules da95fc1e-65fd-461f-814d-d92970029bf0
Distributed firewall status: enabled

Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
ruleset d035308b-cb0d-4e7e-aae5-a428b461db46 {
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443 accept with log;
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80 accept with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 22 accept with log;
  rule 3075 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
}

ruleset 3027fed3-60b1-483e-aa17-c28719275704 {
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459 port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459 port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459 port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877 port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80 accept with log;
}
```

```
ruleset 5e9bdc3-adba-4f67-a680-5e6ed5b8f40a {
  rule 2 inout protocol any from any to any accept with log;
}

ruleset ddf93011-4078-4006-b8f8-73f979d7a717 {
  rule 1 inout ethertype any stateless from any to any accept;
}
```

특정 VIF에서 사용되는 주소 집합의 목록을 가져옵니다.

```
# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/addrsets da95fc1e-65fd-461f-814d-d92970029bf0
48822ec3-2670-497b-82f9-524618c16877 {
  mac 52:54:00:42:4d:38,
  ip 172.16.10.13,
}

8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}

b695c8df-9894-4068-a5e7-5504fe48d459 {
  mac 52:54:00:64:0e:4f,
  ip 172.16.30.11,
}
```

Linux Conntrack 모듈을 통해 연결을 확인합니다. 이 예에서는 2개의 특정 IP 주소 간의 흐름을 확인합니다.

```
# ovs-appctl -t ovs-l3d conntrack/show | grep 192.168.110.10 | grep 172.16.10.13
ACTIVE
icmp,orig=(src=192.168.110.10,dst=172.16.10.13,id=1,type=8,code=0),reply=(src=172.16.10.13,dst=192.168.110.10,id=1,type=0,code=0),start=2018-03-26T04:43:28.325,id=3122159040,zone=23119,status=SEEN_REPLY|
CONFIRMED,timeout=29,mark=3076,labels=0x1f
```

방화벽 패킷 로그

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

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

```
# tail -f /var/log/dfwpktlogs.log
2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP FIN 100.64.80.1/60688->172.16.10.11/80 8/7 373/5451
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP FIN 172.16.10.11/46108->172.16.20.11/8443 8/9 1178/7366
2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP RST 100.64.80.1/60692->172.16.10.11/80 9/6 413/5411
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7 1218/7262
2018-03-27T10:23:37.442Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35770->172.16.20.11/8443 S
2018-03-27T10:23:38.492Z INET match PASS 2 OUT 1500 TCP 172.16.10.11/80->100.64.80.1/60660 A
2018-03-27T10:23:39.934Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60720->172.16.10.11/80 S
2018-03-27T10:23:39.944Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46114->172.16.20.11/8443 S
2018-03-27T10:23:39.944Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46114->172.16.20.11/8443 S
2018-03-27T10:23:42.449Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35771->172.16.20.11/8443 S
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7 1218/7262
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35766->172.16.20.11/8443 9/10 1233/7418
```

```

2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.11/46110->172.16.20.11/8443 9/9 1230/7366
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35767->172.16.20.11/8443 9/10 1233/7418
2018-03-27T10:23:44.939Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60726->172.16.10.11/80 S
2018-03-27T10:23:44.957Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46115->172.16.20.11/8443 S
2018-03-27T10:23:44.957Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46115->172.16.20.11/8443 S
2018-03-27T10:23:45.480Z INET TERM 2 OUT TCP TIMEOUT 172.16.10.11/80->100.64.80.1/60528 1/1 1500/56
    
```

기타 문제 해결 시나리오

6

이 섹션에서는 다양한 오류 시나리오를 해결하는 방법을 설명합니다.

본 장은 다음 항목을 포함합니다.

- 전송 노드 추가 또는 삭제 실패
- 전송 노드가 다른 컨트롤러에 연결되는 데 약 5분이 소요됨
- NSX Manager VM 성능 저하
- NSX 에이전트가 NSX Manager와 통신 시 시간 초과
- ESXi 호스트 추가 실패
- 잘못된 NSX Controller 상태
- IPFIX를 사용하도록 설정되어 있으면 KVM VM의 관리 IP에 연결할 수 없음

전송 노드 추가 또는 삭제 실패

전송 노드를 삭제 또는 추가할 수 없습니다.

문제

다음과 같은 시나리오에서 오류가 발생합니다.

- 1 ESXi 호스트가 패브릭 노드이며 전송 노드입니다.
- 2 호스트가 전송 노드로 제거됩니다. 하지만 전송 노드 삭제가 실패합니다. 전송 노드 상태가 분리됨입니다.
- 3 호스트가 패브릭 노드로 즉시 제거됩니다.
- 4 호스트가 패브릭 노드로 다시 추가됩니다.
- 5 호스트가 새로운 전송 영역과 스위치가 있는 전송 노드로 추가됩니다. 이 단계에서 실패/일부 성공 오류가 발생합니다.

원인

2단계에서 몇 분 정도 기다리면 NSX Manager가 삭제를 다시 시도하기 때문에 전송 노드 삭제가 성공합니다. 패브릭 노드를 즉시 삭제하면 NSX-T Data Center에서 호스트가 제거되기 때문에 NSX Manager가 재시도할 수 없습니다. 이로 인해 호스트가 불완전하게 정리되어 스위치 구성이 여전히 존재하기 때문에 5단계가 실패합니다.

해결책

- 1 호스트의 vCenter Server에서 NSX-T Data Center 스위치에 연결된 모든 vmknics를 삭제합니다.
- 2 `esxcfg-vswitch -l` CLI 명령을 사용하여 스위치 이름을 가져옵니다. 예:

```
esxcfg-vswitch -l
```

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
vSwitch0	1536	4	128	1500	vmnic0

PortGroup Name	VLAN ID	Used Ports	Uplinks
VM Network	0	0	vmnic0
Management Network	0	1	vmnic0

Switch Name	Num Ports	Used Ports	Uplinks
nsxvswitch	1536	4	

- 3 `esxcfg-vswitch -d <switch-name> --dvswitch` CLI 명령을 사용하여 스위치 이름을 삭제합니다. 예:

```
esxcfg-vswitch -d nsxvswitch --dvswitch
```

전송 노드가 다른 컨트롤러에 연결되는 데 약 5분이 소요됨

ESXi 전송 노드의 연결된 컨트롤러가 작동 중지되는 경우 전송 노드가 다른 컨트롤러에 연결되는 데 약 5분이 소요됩니다.

문제

ESXi 전송 노드는 일반적으로 컨트롤러 클러스터의 특정 컨트롤러에 연결됩니다. CLI 명령 `get controllers`를 사용하여 연결된 컨트롤러를 찾을 수 있습니다. 연결된 컨트롤러가 작동 중지되는 경우 전송 노드가 다른 컨트롤러에 연결되는 데 약 5분이 소요됩니다.

원인

전송 노드는 기존 컨트롤러 연결을 포기하고 다른 컨트롤러에 연결되기 전에 특정 시간 동안 작동 중지된 컨트롤러에 다시 연결하려고 시도합니다. 전체 프로세스에는 약 5분이 소요됩니다. 이는 예상된 동작입니다.

NSX Manager VM 성능 저하

get service 및 get interface 등의 CLI 명령을 실행하면 KVM 호스트에 배포된 NSX Manager에서 오류를 반환합니다.

문제

CLI 명령 get service가 오류를 반환합니다. 예를 들면 다음과 같습니다.

```
nsx-manager-1> get service
% An error occurred while processing the service command
```

다른 CLI 명령도 오류를 반환할 수 있습니다. get support-bundle 명령은 /tmp 디렉토리가 읽기 전용이 되었음을 나타냅니다. 예를 들면 다음과 같습니다.

```
nsx-manager-1> get support-bundle file failed-to-get-service.tgz
% An error occurred while retrieving the support bundle: [Errno 30] Read-only file system: '/tmp/tmpHzXF1u'
```

/var/log/messages-<timestamp> 로그에는 다음과 같은 메시지가 있습니다.

```
Nov 17 07:26:48 no kernel: NMI watchdog: BUG: soft lockup - CPU#5 stuck for 23s! [qemu-kvm:4386]
```

원인

NSX Manager 장치에서 하나 이상의 파일 시스템이 손상되었습니다. 몇 가지 가능한 원인이 <https://access.redhat.com/solutions/22621>에 문서화되어 있습니다.

이 문제를 해결하려면 손상된 파일 시스템을 복구하거나 백업에서 복원을 수행할 수 있습니다.

해결책

- 1 옵션 1: 손상된 파일 시스템을 복구합니다. 다음 단계는 KVM 호스트에서 실행되는 NSX Manager에만 사용됩니다.
 - a virsh destroy 명령을 실행하여 NSX Manager VM을 중지합니다.
 - b qcow2 이미지에서 쓰기 모드로 virt-rescue 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
virt-rescue --rw -a nsx-unified-appliance-2.0.0.0.6522097.phadniss-p0-DK-to-DGo-on-rhel-
prod_nsx_manager_1.qcow2
```

- c virt-rescue 명령 프롬프트에서 e2fsck 명령을 실행하여 tmp 파일 시스템을 수정합니다. 예를 들면 다음과 같습니다.

```
<rescue> e2fsck /dev/nsx/tmp
```

- d 필요한 경우 오류가 없어질 때까지 e2fsck /dev/nsx/tmp를 다시 실행합니다.
 - e virsh start를 사용하여 NSX Manager를 다시 시작합니다.
- 2 옵션 2: 백업에서 복원을 수행합니다.

지침을 보려면 "NSX-T 관리 가이드"를 참조하십시오.

NSX 에이전트가 NSX Manager와 통신 시 시간 초과

ESXi 호스트에 다수의 전송 노드와 VM이 있는 대규모 환경에서, ESXi 호스트에서 실행되는 NSX 에이전트는 NSX Manager와 통신할 때 시간이 초과될 수 있습니다.

문제

VM vnic이 논리적 스위치에 연결하려는 경우와 같은 일부 작업이 실패합니다. `/var/run/log/nsx-opsagent.log`에 다음과 같은 메시지가 있습니다.

```
level="ERROR" errorCode="MPA41542"] [MP_AddVnicAttachment] RPC call [0e316296-13-14] to NSX management plane
timeout
2017-05-15T05:32:13Z nsxa: [nsx@6876 comp="nsx-esx" subcomp="NSXA[VifHandlerThread:-2282640]" tid="1000017079"
level="ERROR" errorCode="MPA42003"] [DoMpVifAttachRpc] MP_AddVnicAttachment() failed: RPC call to NSX management
plane timeout
```

원인

대규모 환경에서는 일부 작업이 평소보다 오래 걸리므로 기본 시간 초과 값이 초과되어 실패할 수 있습니다.

해결책

1 NSX 에이전트 시간 초과 값을 늘립니다.

- a ESXi 호스트에서 다음 명령을 사용하여 NSX opsAgent를 중지합니다.

```
/etc/init.d/nsx-opsagent stop
```

- b `/etc/vmware/nsx-opsagent/nsxa.json` 파일을 편집하고 `vifOperationTimeout` 값을 25에서 예를 들어, 55로 변경합니다.

```
"mp" : {
  /* timeout for VIF operation */
  "vifOperationTimeout" : 25,
```

참고 이 시간 초과 값은 2단계에서 설정하는 `hostd` 시간 초과 값보다 작아야 합니다.

- c 다음 명령을 사용하여 NSX opsAgent를 시작합니다.

```
/etc/init.d/nsx-opsagent start
```

2 hostd 시간 초과 값을 늘립니다.

- a ESXi 호스트에서 다음 명령을 사용하여 hostd 에이전트를 중지합니다.

```
/etc/init.d/hostd stop
```

- b /etc/vmware/hostd/config.xml 파일을 편집합니다. <opaqueNetwork>아래에서 <taskTimeout>에 대한 항목의 주석 처리를 제거하고 값을 30에서 예를 들어, 60으로 변경합니다.

```
<opaqueNetwork>
  <!-- maximum message size allowed in opaque network manager IPC, in bytes. -->
  <!-- <maxMsgSize> 65536 </maxMsgSize> -->
  <!-- maximum wait time for opaque network response -->
  <!-- <taskTimeout> 30 </taskTimeout> -->
```

- c 다음 명령을 사용하여 hostd 에이전트를 시작합니다.

```
/etc/init.d/hostd start
```

ESXi 호스트 추가 실패

NSX-T Data Center 패브릭에 ESXi 호스트를 추가할 수 없습니다.

문제

NSX Manager GUI에서 ESXi 호스트를 추가할 때 파일 경로 ...이(가) 여러 비오버레이 VIB에 의해 할당되었습니다." 오류로 인해 실패합니다. 로그 파일에 다음과 같은 메시지가 표시됩니다.

```
Failed to install software on host. Failed to install software on host. 10.172.120.60 : java.rmi.RemoteException:
[DependencyError] File path of '/usr/lib/vmware/vmkmod/nsx-vsip' is claimed by multiple non-overlay VIBs
```

원인

이전 설치의 VIB 일부가 호스트에 여전히 남아 있으며 완전 제거가 발생하지 않았기 때문일 수 있습니다.

해결책

- 오류 메시지에서 오류를 유발하는 VIB의 이름을 가져옵니다.
- ESXi 명령을 사용하여 VIB를 제거합니다.

잘못된 NSX Controller 상태

NSX Controller 클러스터의 일부 컨트롤러가 컨트롤러 중 하나에 대해 잘못된 상태를 보고합니다.

문제

컨트롤러의 전원을 여러 번 껐다가 켜면, 해당 컨트롤러가 작동 중일 때 다른 컨트롤러가 이를 비활성 상태라고 보고합니다.

원인

컨트롤러를 켜다가 켜 때 ZooKeeper 모듈 관련 내부 오류가 발생하는 경우가 있으며 이로 인해 컨트롤러와 클러스터의 다른 컨트롤러 사이에 통신 오류가 발생합니다.

해결책

- ◆ 클러스터에서 비활성으로 보고된 컨트롤러 노드를 제거하고 노드에서 클러스터 구성을 제거한 다음 노드를 클러스터에 다시 가입시킵니다. 자세한 내용은 "NSX-T 관리 가이드"의 "NSX Controller 클러스터의 멤버 교체" 섹션을 참조하십시오.

IPFIX를 사용하도록 설정되어 있으면 KVM VM의 관리 IP에 연결할 수 없음

KVM 호스트의 여러 VM에 IPFIX를 사용하도록 설정되어 있고 샘플링 비율이 100%이면 일부 VM의 관리 IP에 간헐적으로 연결할 수 없습니다.

문제

동일한 호스트의 여러 VM에 대해 IPFIX를 사용하도록 설정하고 샘플링 비율을 100%로 설정하면 대량의 IPFIX 트래픽이 발생할 수 있습니다. 이것이 관리 트래픽에 영향을 미쳐서 프로덕션 트래픽 및 관리 트래픽이 다른 OVS를 통과하더라도 관리 IP에 간헐적으로 연결할 수 없게 됩니다.

원인

워크로드가 호스트와 VM에 대해 과도하게 폭증합니다.

해결책

- ◆ IPFIX를 사용하도록 설정된 VM 수를 줄이거나 샘플링 비율을 줄여서 호스트의 로드를 줄입니다.