

Handbuch zur Fehlerbehebung von NSX-T Data Center

Geändert am 19. SEP 2018
VMware NSX-T Data Center 2.3



vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Copyright © 2017, 2018 VMware, Inc. Alle Rechte vorbehalten. [Informationen zu Copyright und Marken.](#)

Inhalt

Fehlerbehebungshandbuch zu NSX-T Data Center 5

1 Protokolle und Dienste 6

- Protokollmeldungen 6
- Fehlerbehebung für Probleme mit Syslog 10
- Überprüfen von Diensten 11
- Erfassen von Support-Paketen 13

2 Fehlerbehebung der Layer-2-Konnektivität 15

- Überprüfen des Status von NSX Manager und des NSX Controller -Clusters 15
- Überprüfen der logischen Ports 16
- Überprüfen des Transportknotenstatus 17
- Überprüfen des Status des logischen Switches 17
- Überprüfen der CCP für den logischen Switch 18
- Überprüfen des Status der lokalen Steuerungskomponente 19
- Beheben von Fehlern bei Konfigurationssitzungen 19
- Beheben von Fehlern bei L2-Sitzungen 21
- Beheben von Problemen auf der Datenebene für einen logischen Overlay-Switch 21
- Beheben von Problemen auf der Datenebene für einen logischen VLAN-Switch 23
- Beheben von ARP-Problemen für einen logischen Overlay-Switch 24
- Fehlerbehebung bei Paketverlust für einen logischen VLAN-Switch oder wenn ARP aufgelöst wurde 25

3 Fehlerbehebung: Installation 26

4 Fehlerbehebung: Routing 30

5 Fehlerbehebung für Firewall 33

- Ermitteln der auf einem ESXi-Host angewandten Firewallregeln 33
- Ermitteln der auf einem KVM-Host angewandten Firewallregeln 36
- Protokolle des Firewallpakets 38

6 Andere Szenarien zur Fehlerbehebung 39

- Fehler beim Hinzufügen oder Löschen eines Transportknotens 39
- Verbindungsaufbau des Transportknotens mit einem anderen Controller dauert etwa 5 Minuten 40
- NSX Manager -VM wird herabgestuft 41
- Zeitüberschreitung bei NSX Agent bei der Kommunikation mit NSX Manager 42
- Fehler beim Hinzufügen eines ESXi-Hosts 43

[Falscher NSX Controller-Status](#) 43

[Management-IPs auf KVM-VMs nicht erreichbar bei aktiviertem IPFIX](#) 44

Fehlerbehebungshandbuch zu NSX-T Data Center

Das *Fehlerbehebungshandbuch zu NSX-T Data Center* enthält Informationen zur Fehlerbehebung bei Problemen, die in NSX-T Data Center-Umgebungen auftreten können.

Zielgruppe

Dieses Handbuch ist für Systemadministratoren von NSX-T Data Center vorgesehen. Es wird vorausgesetzt, dass Sie mit Virtualisierung, Netzwerken und Datencentervorgängen vertraut sind.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Protokolle und Dienste

Protokolle können in vielen Fehlerbehebungsszenarien hilfreich sein. Den Status der Dienste zu überprüfen ist ebenso wichtig.

Dieses Kapitel behandelt die folgenden Themen:

- [Protokollmeldungen](#)
- [Fehlerbehebung für Probleme mit Syslog](#)
- [Überprüfen von Diensten](#)
- [Erfassen von Support-Paketen](#)

Protokollmeldungen

Protokollmeldungen aller NSX-T Data Center-Komponenten einschließlich den auf ESXi-Hosts ausgeführten entsprechen dem Syslog-Format gemäß RFC 5424. Protokollmeldungen von KVM-Hosts sind im RFC-3164-Format. Die Protokolldateien befinden sich im Verzeichnis `/var/log`.

Auf NSX-T Data Center-Appliances können Sie den folgenden NSX-T Data Center-CLI-Befehl zum Anzeigen der Protokolle ausführen:

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

Auf Hypervisoren können Sie Linux-Befehle wie z. B. `tail`, `grep` oder `more` verwenden, um die Protokolle anzuzeigen. Diese Befehle können Sie auch auf NSX-T Data Center--Appliances verwenden.

Weitere Informationen zu RFC 5424 finden Sie unter <https://tools.ietf.org/html/rfc5424>. Weitere Informationen zu RFC 3164 finden Sie unter <https://tools.ietf.org/html/rfc3164>.

RFC 5424 legt für Protokollmeldungen das folgende Format fest:

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

Beispiel für eine Protokollmeldung:

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

Jede Nachricht enthält Komponentendetails (comp) und Unterkomponentendetails (subcomp), die es erleichtern, die Quelle der Nachricht zu identifizieren.

NSX-T Data Center erstellt reguläre Protokolle („facility local6“ mit einem numerischen Wert von 22) und Überwachungsprotokolle („facility local7“ mit einem numerischen Wert von 23). Alle API-Aufrufe lösen ein Überwachungsprotokoll aus.

Ein Eintrag im Überwachungsprotokoll, der einem API-Aufruf zugeordnet ist, enthält die folgende Informationen:

- Den Parameter `entId` mit einer Element-ID zur Identifizierung des Objekts der-API.
- Den Parameter `req-id` mit einer Anforderungs-ID zur Identifizierung eines bestimmten API-Aufrufs.
- Den Parameter `reqId` mit einer ID, die auf eine externe Anforderung verweist, wenn der API-Aufruf den Header `X-NSX-EREQID: <string>` enthält.
- Den Parameter `euser` der auf einen externen Benutzer verweist, wenn der API-Aufruf den Header `X-NSX-EUSER: <string>` enthält.

RFC 5424 definiert die folgenden Ebenen für den Schweregrad:

Schweregrad	Beschreibung
0	Notfall: Das System steht nicht zur Verfügung
1	Ernste Warnung: Es muss sofort reagiert werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normale, aber signifikante Bedingung
6	Information: Informationsmeldungen
7	Debug: Meldungen auf Debug-Ebene

Alle Protokolle mit dem Schweregrad „Notfall“, „Ernste Warnung“, „Kritisch“ und „Fehler“ enthalten einen eindeutigen Fehlercode im Abschnitt der strukturierten Daten der Protokollmeldung. Der Fehlercode besteht aus einer Zeichenfolge und einer Dezimalzahl. Die Zeichenfolge steht für ein bestimmtes Modul.

Das MSGID-Feld identifiziert den Meldungstyp. Eine Liste der Meldungs-IDs finden Sie unter [Protokollmeldungs-IDs](#).

Konfigurieren der Remoteprotokollierung

Sie können NSX-T Data Center-Appliances und -Hypervisoren für das Senden von Meldungen zu einem Server für Remoteprotokollierung konfigurieren.

Remoteprotokollierung wird auf NSX Manager-, NSX Controller-, NSX Edge- und Hypervisor-Knoten unterstützt. Sie müssen die Remoteprotokollierung auf jedem Knoten einzeln konfigurieren.

Auf einem KVM-Host konfiguriert das NSX-T Data Center-Installationspaket den rsyslog-Daemon automatisch, indem es entsprechende Konfigurationsdateien im Verzeichnis `/etc/rsyslog.d` platziert.

Voraussetzungen

- Konfigurieren Sie einen Protokollierungsserver für den Empfang der Protokolle.

Vorgehensweise

- 1 So konfigurieren Sie die Remoteprotokollierung auf einer NSX-T Data Center-Appliance:

- a Führen Sie den folgenden Befehl aus, um einen Protokollserver zu konfigurieren und festzulegen, welche Arten von Meldungen an den Protokollserver gesendet werden sollen. Mehrere facility- oder messageid-Parameter können, durch Kommas ohne Leerzeichen getrennt, als Liste angegeben werden.

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

Weitere Informationen zu diesem Befehl finden Sie in der *Referenz zur NSX-T-CLI*. Sie haben die Möglichkeit, den Befehl mehrmals zum Hinzufügen mehrerer Konfigurationen für Protokollierungsserver auszuführen. Beispiel:

```
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 Sie können die Protokollierungskonfiguration mit dem Befehl `get logging-server` anzeigen. Beispiel:

```
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 So konfigurieren Sie die Remoteprotokollierung auf einem ESXi-Host:

- a Führen Sie die folgenden Befehle aus, um Syslog zu konfigurieren und eine Testnachricht zu senden:

```
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 Sie können die Konfiguration durch Ausführen des folgenden Befehls anzeigen:

```
esxcli system syslog config get
```

3 So konfigurieren Sie die Remoteprotokollierung auf einem KVM-Host:

- a Bearbeiten Sie die Datei `/etc/rsyslog.d/10-vmware-remote-logging.conf`, um sie an Ihre Umgebung anzupassen.
- b Fügen Sie der Datei die folgende Zeile hinzu:

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

- c Führen Sie den folgenden Befehl aus:

```
service rsyslog restart
```

Protokollmeldungs-IDs

In einer Protokollmeldung identifiziert das Meldungs-ID-Feld den Meldungstyp. Sie können den Parameter `messageid` im Befehl `set logging-server` verwenden, um zu filtern, welche Protokollmeldungen an den Protokollierungsserver gesendet werden.

Tabelle 1-1. Protokollmeldungs-IDs

Meldungs-ID	Beispiele
FABRIC	Hostknoten Hostvorbereitung Edge-Knoten Transportzone Transportknoten Uplink-Profil Clusterprofil Edge-Cluster Bridge-Cluster und -Endpoints
SWITCHING	Logischer Switch Ports für logischen Switch Switching-Profil Funktionen der Switch-Sicherheit
ROUTING	Logischer Router Logische Routerports Statisches Routing Dynamisches Routing NAT
FIREWALL	Firewallregeln Firewallregelabschnitte
FIREWALL-PKTLOG	Protokolle der Firewallverbindung Protokolle des Firewallpakets

Tabelle 1-1. Protokollmeldungs-IDs (Fortsetzung)

Meldungs-ID	Beispiele
GROUPING	IP Sets MAC Sets NS-Gruppen NS-Dienste NS-Dienstgruppen VNI-Pool IP-Pool
DHCP	DHCP-Relay
SYSTEM	Appliance-Verwaltung (remote syslog, ntp, etc.) Clusterverwaltung Vertrauensverwaltung Lizenzierung Benutzer und Rollen Aufgabenverwaltung Installation (NSX Manager, NSX Controller) Upgrade (NSX Manager, NSX Controller, NSX Edge und Upgrades für Hostpakete) Umsetzung Tags
MONITORING	SNMP Portverbindung Traceflow
-	Alle anderen Protokollmeldungen

Fehlerbehebung für Probleme mit Syslog

Wenn der Remote-Protokollserver keine Protokolle empfängt, führen Sie die folgenden Schritte aus:

- Überprüfen Sie die IP-Adresse des Remote-Protokollservers.
- Überprüfen Sie, ob der `level`-Parameter korrekt konfiguriert ist.
- Überprüfen Sie, ob der `facility`-Parameter korrekt konfiguriert ist.
- Wenn das TLS-Protokoll verwendet wird, legen Sie stattdessen das UDP-Protokoll fest, um festzustellen, ob Zertifikate nicht übereinstimmen.
- Wenn das TLS-Protokoll verwendet wird, vergewissern Sie sich, dass Port 6514 an beiden Enden geöffnet ist.
- Entfernen Sie den Meldungs-ID-Filter und stellen Sie fest, ob der Server Protokolle empfängt.
- Starten Sie den rsyslog-Dienst mit dem Befehl `restart service rsyslogd neu`.

Beispiel für eine rsyslog-Konfigurationsdatei (/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%\n"
$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
```

Überprüfen von Diensten

Wenn Dienste nicht mehr ausgeführt werden oder nicht gestartet werden können, kann dies Probleme verursachen. Daher ist es wichtig, sicherzustellen, dass alle Dienste normal ausgeführt werden.

So überprüfen Sie den Status des NSX Manager-Diensts:

```
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

```

Im Beispiel oben wird der HTTP-Dienst beendet. Sie können den HTTP-Dienst mit dem folgenden Befehl starten:

```
nsxmgr> start service http
```

SSH-Dienst

Wenn der SSH-Dienst beim Bereitstellen der Appliance nicht aktiviert wurde, können Sie sich als Administrator bei der Appliance anmelden und sie mit dem folgenden Befehl aktivieren:

```
start service ssh
```

Mit dem folgenden Befehl können Sie SSH so konfigurieren, dass es beim Starten des Hosts gestartet wird:

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

Melden Sie sich zum Aktivieren der SSH-Root-Anmeldung als „root“ bei der Appliance an, bearbeiten Sie die Datei `/etc/ssh/sshd_config` und ersetzen Sie die Zeile

```
PermitRootLogin prohibit-password
```

(Alternativ können Sie den SSH-Dienst und den SSH-Root-Zugriff aktivieren, indem Sie die Appliance ausschalten und ihre vApp-Eigenschaften bearbeiten.)

durch

```
PermitRootLogin yes
```


und starten Sie den sshd-Server mit dem folgenden Befehl:

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

Erfassen von Support-Paketen

Sie können Support-Pakete auf registrierten Clustern und Fabric-Knoten erfassen und die Pakete auf Ihren Computer herunterladen bzw. auf einen Dateiserver hochladen.

Wenn Sie die Pakete auf Ihren Computer herunterladen, erhalten Sie eine einzelne Archivdatei, die aus einer Manifestdatei und Support-Paketen für jeden Knoten besteht. Wenn Sie die Pakete auf einen Dateiserver hochladen, werden die Manifestdatei und die einzelnen Pakete gesondert hochgeladen.

 **Hinweis zu NSX Cloud** Wenn Sie das Support-Paket für CSM erfassen möchten, melden Sie sich bei CSM an, wechseln Sie zu **System > Dienstprogramme > Support-Paket** und klicken Sie auf **Herunterladen**. Das Support-Paket für PCG ist in NSX Manager verfügbar. Gehen Sie anhand der folgenden Anweisungen vor. Das Support-Paket für PCG enthält auch Protokolle für alle Arbeitslast-VMs.

Vorgehensweise

- 1 Navigieren Sie im Browser zu <https://nsx-manager-ip-address> und melden Sie sich mit Administratorrechten bei NSX Manager an.
- 2 Wählen Sie im Navigationsbereich die Option **System > Dienstprogramme** aus.
- 3 Klicken Sie auf die Registerkarte **Support-Paket**.
- 4 Wählen Sie die Zielknoten aus.

Bei den verfügbaren Knotentypen handelt es sich um Verwaltungsknoten, Controller-Knoten, Edges, Hosts und Public Cloud-Gateways (PCGs).
- 5 (Optional) Geben Sie den Protokollierungszeitraum in Tagen an, um Protokolle auszuschließen, die vor der festgelegten Anzahl an Tagen erstellt wurden.

- 6 (Optional) Schalten Sie den Switch um, der angibt, ob Core-Dateien und Überwachungsprotokolle einbezogen werden sollen.

Hinweis Core-Dateien und Überwachungsprotokolle können vertrauliche Informationen wie etwa Kennwörter oder Verschlüsselungsschlüssel enthalten.

- 7 (Optional) Aktivieren Sie das entsprechende Kontrollkästchen, um die Pakete auf einen Dateiserver hochzuladen.
- 8 Klicken Sie auf **Paketerfassung starten**, um mit der Erfassung der Support-Pakete zu beginnen.
Je nach der Anzahl der Protokolldateien kann die Erfassung für jeden Knoten mehrere Minuten dauern.
- 9 Überwachen Sie den Status des Erfassungsvorgangs.
Das Statusfeld zeigt in Prozenten an, für wie viele Knoten die Erfassung des Support-Pakets durchgeführt wurde.
- 10 Wenn die Option für das Senden des Pakets an einen Dateiserver nicht aktiviert ist, klicken Sie auf **Herunterladen**, um das Paket herunterzuladen.

Fehlerbehebung der Layer-2-Konnektivität

2

Wenn ein Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) auftritt, die mit dem gleichen logischen Switch verbunden sind, können Sie beispielsweise keine VM von einer anderen VM aus anpingen. Folgen Sie den Schritten in diesem Abschnitt, um den Fehler zu beheben.

Bevor Sie beginnen, stellen Sie sicher, dass keine Firewallregel vorhanden ist, die den Datenverkehr zwischen den beiden logischen Ports blockiert. Es wird empfohlen, die Reihenfolge der Themen in diesem Abschnitt einzuhalten, um das Konnektivitätsproblem zu beheben.

Dieses Kapitel behandelt die folgenden Themen:

- [Überprüfen des Status von NSX Manager und des NSX Controller-Clusters](#)
- [Überprüfen der logischen Ports](#)
- [Überprüfen des Transportknotenstatus](#)
- [Überprüfen des Status des logischen Switches](#)
- [Überprüfen der CCP für den logischen Switch](#)
- [Überprüfen des Status der lokalen Steuerungskomponente](#)
- [Beheben von Fehlern bei Konfigurationssitzungen](#)
- [Beheben von Fehlern bei L2-Sitzungen](#)
- [Beheben von Problemen auf der Datenebene für einen logischen Overlay-Switch](#)
- [Beheben von Problemen auf der Datenebene für einen logischen VLAN-Switch](#)
- [Beheben von ARP-Problemen für einen logischen Overlay-Switch](#)
- [Fehlerbehebung bei Paketverlust für einen logischen VLAN-Switch oder wenn ARP aufgelöst wurde](#)

Überprüfen des Status von NSX Manager und des NSX Controller -Clusters

Stellen Sie sicher, dass der Status von NSX Manager und des NSX Controller-Clusters normal ist und die Controller mit dem NSX Managerverbunden sind.

Vorgehensweise

- 1 Führen Sie den folgenden CLI-Befehl auf dem NSX Manager aus, um sicherzustellen, dass er einen stabilen Status aufweist.

```
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 Führen Sie den folgenden CLI-Befehl auf einem NSX Controller aus, um sicherzustellen, dass er einen aktiven Status aufweist.

```
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 Führen Sie den folgenden CLI-Befehl auf einem NSX Controller aus, um sicherzustellen, dass er mit dem NSX Manager verbunden ist.

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

Überprüfen der logischen Ports

Vergewissern Sie sich, dass die logischen Ports auf dem gleichen logischen Switch konfiguriert sind und einen aktiven Status aufweisen.

Vorgehensweise

- 1 Rufen Sie über die NSX Manager-GUI die UUIDs der logischen Ports ab.
- 2 Führen Sie für jeden logischen Port den folgenden API-Aufruf durch, um sicherzustellen, dass sich die logischen Ports auf demselben logischen Switch befinden.

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

- 3 Führen Sie für jeden logischen Port den folgenden API-Aufruf durch, um sicherzustellen, dass er einen aktiven Status aufweist.

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

Überprüfen des Transportknotenstatus

Überprüfen Sie den Status des Transportknotens.

Vorgehensweise

- ◆ Führen Sie den folgenden API-Aufruf durch, um den Status des Transportknotens abzurufen:

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

Wenn der Aufruf den Fehler `RPC timeout` (RPC-Zeitüberschreitung) zurückgibt, führen Sie folgende Schritte zur Fehlerbehebung durch:

- Führen Sie `/etc/init.d/nsx-opsAgent status` aus, um zu prüfen, ob `opsAgent` ausgeführt wird.
- Führen Sie `/etc/init.d/nsx-mpa status` aus, um zu prüfen, ob `nsx-mpa` ausgeführt wird.
- Um festzustellen, ob `nsx-mpa` mit dem NSX Manager verbunden ist, überprüfen Sie die `nsx-mpa`-Taktsignalprotokolle.
- Um festzustellen, ob `opsAgent` mit NSX Manager verbunden ist, überprüfen Sie das `nsx-ops-Agent`-Protokoll. Wenn `opsAgent` mit NSX Manager verbunden ist, wird folgende Meldung angezeigt:

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

- Um festzustellen, ob `opsAgent` beim Verarbeiten von `HostConfigMsg` hängen geblieben ist, überprüfen Sie das `nsx-opsAgent`-Protokoll. Ist dies der Fall, wird eine RMQ-Anforderungsmeldung angezeigt, aber die Antwort wird nicht oder erst nach einer langen Verzögerung gesendet.
- Überprüfen Sie, ob `opsAgent` abgestürzt ist, während `HostConfigMsg` ausgeführt wurde.
- Um festzustellen, ob das Senden von RMQ-Meldungen an den Host lange dauert, vergleichen Sie die Zeitstempel der Protokollmeldungen auf dem NSX Manager und auf dem Host.

Wenn der Aufruf den Fehler `partial_success` zurückgibt, kann es hierfür viele Gründe geben. Sehen Sie sich als Erstes die `nsx-opsAgent`-Protokolle an. Überprüfen Sie auf dem ESXi-Host die Protokolle `hostd.log` und `vmkernel.log`. Auf KVM sind alle Protokolle im `syslog` enthalten.

Überprüfen des Status des logischen Switches

Überprüfen Sie den Status des logischen Switches.

Vorgehensweise

- ◆ Führen Sie den folgenden API-Aufruf durch, um den Status des logischen Switches abzurufen.

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

Wenn der Aufruf den Fehler `partial_success` zurückgibt, enthält die Antwort eine Liste der Transportknoten, bei denen NSX Manager die Konfiguration des logischen Switches nicht weitergeben konnte oder keine Antwort erhalten hat. Die Schritte zur Fehlerbehebung ähneln denen für den Transportknoten. Überprüfen Sie Folgendes:

- Alle erforderlichen Komponenten sind installiert und werden ausgeführt.
- `nsx-mpa` ist mit NSX Manager verbunden.
- `nsxa` ist mit dem Switching Vertical verbunden.
- Ermitteln Sie mit `grep` die ID des logischen Switches in `nsxa.log` und `nsxaVim.log`, um festzustellen, ob die Konfiguration des logischen Switches vom Transportknoten empfangen wurde.
- Überprüfen Sie die Betriebszeit von `nsxa` und `nsx-mpa`. Ermitteln Sie, wann `nsxa` gestartet und gestoppt wurde, und durchsuchen Sie dazu mit `grep` die `nsxa`-Protokollmeldungen in der Datei `Syslog`.
- Ermitteln Sie die Verbindungszeit von `nsxa` mit dem Switching Vertical. Wenn die Konfiguration des logischen Switches an den Host gesendet wird, während `nsxa` nicht mit dem Switching Vertical verbunden ist, wird die Konfiguration möglicherweise nicht an den Host übermittelt.

Bei KVM wird keine Konfiguration für logische Switches an den Host gesendet. Daher treten die meisten Probleme im Zusammenhang mit logischen Switches wahrscheinlich auf der Managementebene auf.

Unter ESXi wird ein opakes Netzwerk dem logischen Switch zugeordnet. Um den logischen Switch zu verwenden, verbinden Benutzer VMs mit dem opaken Netzwerk unter Verwendung von vCenter Server oder vSphere API.

Überprüfen der CCP für den logischen Switch

Stellen Sie sicher, dass der logische Switch sich in der zentralen Steuerungskomponente (CCP) befindet.

Vorgehensweise

- ◆ Führen Sie den folgenden CLI-Befehl auf einem NSX Controller aus, um sicherzustellen, dass der logische Switch vorhanden ist.

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

Hinweis Mit diesem CLI-Befehl werden keine VLAN-basierten logischen Switches aufgelistet.

Überprüfen des Status der lokalen Steuerungskomponente

Vergewissern Sie sich bei einem logischen Overlay-Switch, dass netcpa auf dem Host mit der zentralen Steuerungskomponente verbunden ist.

Voraussetzungen

Ermitteln Sie den Controller, auf dem sich der logische Switch befindet. Siehe [Überprüfen der CCP für den logischen Switch](#).

Vorgehensweise

- 1 Stellen Sie eine SSH-Verbindung mit dem Controller her, auf dem sich der logische Switch befindet.
- 2 Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass der Controller die Hypervisoren anzeigt, die mit dieser VNI verbunden sind.

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

- 3 Führen Sie auf den Hypervisoren den Befehl `/bin/nsxcli` aus, um die NSX-Befehlszeilenschnittstelle zu starten.
- 4 Führen Sie den folgenden Befehl aus, um die CCP-Sitzungen abzurufen.

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

Es sollte eine Config-Sitzung auf einem der CCP-Knoten im CCP-Cluster angezeigt werden. Für jeden logischen Overlay-Switch sollte eine L2-Sitzung zu einem der CCP-Knoten im CCP-Cluster angezeigt werden. Für logische VLAN-Switches gibt es keine CCP-Verbindungen.

Beheben von Fehlern bei Konfigurationssitzungen

Wenn die CCP-Konfigurationssitzung nicht aktiv ist, überprüfen Sie den Status von MPA und netcpa.

Vorgehensweise

- 1 Führen Sie den folgenden API-Aufruf durch, um festzustellen, ob MPA mit dem NSX Manager verbunden ist.

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

- 2 Führen Sie auf dem Hypervisor den Befehl `/bin/nsxcli` aus, um die NSX-Befehlszeilenschnittstelle (CLI) zu starten.

- 3 Führen Sie den folgenden Befehl aus, um die Knoten-UUID abzurufen.

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

- 4 Führen Sie den folgenden Befehl aus, um zu prüfen, ob der NSX Manager die CCP-Informationen an den Host weitergegeben hat.

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

- 5 Wenn config-by-vsm.xml CCP-Informationen aufweist, prüfen Sie, ob auf dem Hypervisor ein Transportknoten konfiguriert ist.

Der NSX Manager sendet das Hostzertifikat für den Hypervisor innerhalb des Schritts zur Transportknotenerstellung. Die CCP muss über das Hostzertifikat verfügen, damit er Verbindungen vom Host akzeptiert.

- 6 Überprüfen Sie die Gültigkeit des Hostzertifikats in /etc/vmware/nsx/host-cert.pem.

Das Zertifikat muss mit demjenigen, das der NSX Manager für den Host hat, übereinstimmen.

- 7 Führen Sie den folgenden Befehl aus, um den Status von netcpa zu überprüfen.

Auf ESXi:

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

Auf KVM:

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

- 8 Starten Sie netcpa bzw. starten Sie es neu.

Starten Sie auf ESXi netcpa, wenn es nicht ausgeführt wird, oder starten Sie es neu, wenn es ausgeführt wird.

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

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

Starten Sie auf KVM netcpa, wenn es nicht ausgeführt wird, oder starten Sie es neu, wenn es ausgeführt wird.

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

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

- 9 Wenn die Konfigurationssitzung immer noch nicht aktiv ist, erfassen Sie die technischen Support-Pakete und wenden Sie sich an den VMware Support.

Beheben von Fehlern bei L2-Sitzungen

Dies gilt nur für logische Overlay-Switches.

Vorgehensweise

- 1 Führen Sie auf dem Hypervisor den Befehl `/bin/nsxcli` aus, um die NSX-Befehlszeilenschnittstelle (CLI) zu starten.
- 2 Führen Sie den folgenden Befehl aus, um festzustellen, ob der logische Switch auf dem Host vorhanden ist.

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

- 3 Vergewissern Sie sich, dass der Zustand des Ports nicht `admin down` ist.

Führen Sie unter ESXi `net-dvs` aus und sehen Sie sich die Antwort an. Beispiel:

```
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.
```

Wenn der logische Port im blockierten Zustand beendet wird, erfassen Sie die technischen Support-Pakete und wenden Sie sich an den VMware Support. In der Zwischenzeit führen Sie den folgenden Befehl zum Abrufen des DVS-Namens aus:

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

Führen Sie den folgenden Befehl aus, um die Blockierung des Ports aufzuheben:

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

Führen Sie bei KVM `ovs-vsctl list interface` aus und stellen Sie sicher, dass die Schnittstelle mit der entsprechenden VIF-UUID vorhanden ist und `admin_state „up“` lautet. Sie können die VIF-UUID in OVSDb in `external-ids:iface-id` sehen.

Beheben von Problemen auf der Datenebene für einen logischen Overlay-Switch

Die Schritte in diesem Abschnitt dienen zur Behebung von Konnektivitätsproblemen zwischen VMs auf verschiedenen Hypervisoren über den Overlay-Switch, wenn die Konfigurations- und Laufzeitzustände normal sind.

Wenn die virtuellen Maschinen sich auf demselben Hypervisor befinden, wechseln Sie zu [Beheben von ARP-Problemen für einen logischen Overlay-Switch](#).

Vorgehensweise

- 1 Führen Sie den folgenden Befehl auf dem Controller mit dem logischen Switch aus, um festzustellen, ob die CCP über die richtige VTEP-Liste verfügt:

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

- 2 Führen Sie den folgenden NSX-CLI-Befehl auf jedem Hypervisor aus, um festzustellen, ob er über die richtige VTEP-Liste verfügt.

Auf ESXi:

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

Alternativ dazu können Sie für die VTEP-Informationen den folgenden Shell-Befehl ausführen:

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

Auf KVM:

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

- 3 Überprüfen Sie, ob die VTEPs auf den Hypervisoren sich gegenseitig anpingen können.

An der ESXi Shell-Eingabeaufforderung:

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

An der KVM-Shell-Eingabeaufforderung:

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

Wenn die VTEPs sich nicht gegenseitig anpingen können:

- a Stellen Sie sicher, dass das Transport-VLAN, das beim Erstellen des Transportknotens angegeben wurde, dem vom Underlay erwarteten VLAN entspricht. Wenn Sie Zugriffsports im Underlay verwenden, sollte das Transport-VLAN auf 0 festgelegt werden. Wenn Sie ein Transport-VLAN angeben, sollten die Underlay-Switch-Ports, mit denen sich die Hypervisoren verbinden, so konfiguriert sein, dass sie dieses VLAN im Trunk-Modus akzeptieren.
- b Überprüfen Sie die Underlay-Konnektivität.

4 Überprüfen Sie, ob die BFD-Sitzungen zwischen den VTEPs ausgeführt werden.

Führen Sie unter ESXi `net-vd12 -M bfd` aus und sehen Sie sich die Antwort an. Beispiel:

```
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
```

Ermitteln Sie bei KVM die GENEVE-Schnittstelle für die Remote-IP-Adresse.

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

Wenn Sie den Namen der Schnittstelle nicht kennen, führen Sie `ovs-vsctl find Interface type=geneve` aus, um alle Tunnelschnittstellen zurückzugeben. Suchen Sie nach BFD-Informationen.

Wenn Sie keine GENEVE-Schnittstelle zum Remote-VTEP finden können, überprüfen Sie, ob `nsx-agent` ausgeführt wird und die OVS-Integrations-Bridge mit `nsx-agent` verbunden ist.

```
[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
```

Beheben von Problemen auf der Datenebene für einen logischen VLAN-Switch

Die Schritte in diesem Abschnitt dienen zur Behebung von Konnektivitätsproblemen zwischen VMs auf verschiedenen Hypervisoren über das konfigurierte VLAN auf dem Underlay, wenn die Konfigurations- und Laufzeitzustände normal sind.

Wenn die VMs sich auf demselben Hypervisor befinden und alle Konfigurations- und Laufzeitzustände normal sind, wechseln Sie zu [Beheben von ARP-Problemen für einen logischen Overlay-Switch](#).

Vorgehensweise

- ◆ Vergewissern Sie sich, dass das Underlay für das VLAN für den logischen Switch im Trunk-Modus konfiguriert ist.

Stellen Sie unter ESXi sicher, dass das VLAN auf dem logischen Port konfiguriert ist. Führen Sie dazu `net-dvs` aus und suchen Sie nach dem logischen Port. Beispiel:

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

Bei KVM wird der logische VLAN-Switch als Openflow-Regel auf der Integrations-Bridge konfiguriert. Mit anderen Worten: Von der VIF empfangener Datenverkehr wird mit VLAN X gekennzeichnet und auf dem Patch-Port zur PIF-Bridge weitergeleitet. Führen Sie `ovs-vsctl list interface` aus und überprüfen Sie das Vorhandensein des Patch-Ports zwischen der von NSX verwalteten Bridge und der NSX-Switch-Bridge.

Beheben von ARP-Problemen für einen logischen Overlay-Switch

Die Schritte in diesem Abschnitt sind für die Fehlerbehebung gedacht, wenn Pakete für einen Overlay-Switch verloren gegangen sind.

Wechseln Sie bei einem VLAN-gestützten logischen Switch zu [Fehlerbehebung bei Paketverlust für einen logischen VLAN-Switch oder wenn ARP aufgelöst wurde](#).

Führen Sie vor den folgenden Schritten zur Fehlerbehebung auf jeder VM den Befehl `arp -n` aus. Wenn ARP auf beiden VMs erfolgreich aufgelöst wird, müssen Sie die Schritte in diesem Abschnitt nicht ausführen. Fahren Sie stattdessen mit dem nächsten Abschnitt [Fehlerbehebung bei Paketverlust für einen logischen VLAN-Switch oder wenn ARP aufgelöst wurde](#) fort.

Vorgehensweise

- ◆ Wenn beide Endpoints ESXi sind und ARP-Proxy auf dem logischen Switch aktiviert ist (nur für logische Overlay-Switches unterstützt), überprüfen Sie die ARP-Tabelle auf der CCP und dem Hypervisor.

Auf der CCP:

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

Starten Sie auf dem Hypervisor die NSX-CLI und führen Sie den folgenden Befehl aus:

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

Durch Abrufen der ARP-Tabelle werden wir nur darüber in Kenntnis gesetzt, ob wir den richtigen ARP-Proxy-Zustand haben. Wenn die ARP-Antwort von keinem Proxyserver empfangen wird oder der Host KVM ist und keine Unterstützung für ARP-Proxy bietet, sollte der Datenpfad die ARP-Anforderung übermitteln. Möglicherweise tritt ein Problem mit der Weiterleitung des BUM-Datenverkehrs auf. Führen Sie die folgenden Schritte aus:

- Wenn der Replikationsmodus für den logischen Switch MTEP ist, ändern Sie über die Benutzeroberfläche von NSX Manager den Replikationsmodus für den logischen Switch in SOURCE. Dadurch wird das Problem möglicherweise behoben, und der Ping-Befehl wird dann ausgeführt.
- Fügen Sie statische ARP-Einträge hinzu und testen Sie, ob der Rest des Datenpfads funktioniert.

Fehlerbehebung bei Paketverlust für einen logischen VLAN-Switch oder wenn ARP aufgelöst wurde

Sie können das automatisierte Traceflow-Tool verwenden oder die Pakete manuell verfolgen, um einen Paketverlust zu beheben.

Um das Traceflow-Tool über die Benutzeroberfläche von NSX Manager auszuführen, navigieren Sie zu **Tools > Traceflow**. Weitere Informationen finden Sie im *NSX-T-Administratorhandbuch*.

Vorgehensweise

- ◆ Um die Pakete manuell zu verfolgen,

Führen Sie unter ESXi `net-stats -l` aus, um die Switch-Port-ID von den VIFs zu erhalten. Wenn sich die Quell- und Ziel-VIFs auf demselben Hypervisor befinden, führen Sie die folgenden Befehle aus:

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

Wenn sich die Quell- und Ziel-VIFs auf unterschiedlichen Hypervisoren befinden, führen Sie auf dem Hypervisor, der die Quell-VIF hostet, folgende Befehle aus:

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

Führen Sie auf dem Hypervisor, der die Ziel-VIF hostet, die folgenden Befehle aus:

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

Wenn sich auf KVM die Quell- und Ziel-VIFs auf demselben Hypervisor befinden, führen Sie den folgenden Befehl aus:

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

Fehlerbehebung: Installation

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Problemen mit der Installation.

Grundlegende Infrastrukturdienste

Die folgenden Dienste müssen auf den Appliances und Hypervisoren ausgeführt werden. Das gilt auch für vCenter Server, wenn es als Berechnungsmanager verwendet wird.

- NTP
- DNS

Achten Sie darauf, dass die Firewall nicht den Datenverkehr zwischen NSX-T-Komponenten und -Hypervisoren blockiert. Achten Sie darauf, dass die erforderlichen Ports zwischen den Komponenten geöffnet sind.

Melden Sie sich zum Leeren des DNS-Cache im NSX Manager über die SSH als Root beim Manager an und führen Sie den folgenden Befehl aus:

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

Daraufhin können Sie die DNS-Konfigurationsdatei überprüfen.

```
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
```

Überprüfen der Kommunikation vom Host zum Controller und Manager

Auf einem ESXi-Host mit NSX-T-CLI-Befehlen:

```
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
```

Auf einem KVM-Host mit NSX-T-CLI-Befehlen:

```
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
```

Auf einem ESXi-Host mit Host-CLI-Befehlen:

```
[root@esxi-01:~] esxcli network ip connection list | grep 1235
tcp          0      0 192.168.110.53:42271      192.168.110.16:1235  ESTABLIS-
HED        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
```

Auf einem KVM-Host mit Host-CLI-Befehlen:

```
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>

```

Host-Registrierungsfehler

Wenn NSX-T die falsche IP-Adresse verwendet, schlägt die Hostregistrierung fehl. Dies kann geschehen, wenn ein Host über mehrere IP-Adressen verfügt. Beim Versuch, die Transportknoten zu löschen, verbleiben diese im verwaisten Zustand. So lässt sich das Problem beheben:

- Klicken Sie auf **Fabric > Knoten > Hosts**, bearbeiten Sie den Host und entfernen Sie alle IP-Adressen außer der Management-IP-Adresse.
- Klicken Sie auf die Fehler und wählen Sie **Beheben**.

Probleme beim KVM-Host

Probleme beim KVM-Host werden manchmal durch unzureichenden Festplattenspeicher verursacht. Das /boot-Verzeichnis kann sich schnell füllen und Fehler verursachen, wie zum Beispiel:

- Softwareinstallation auf Host fehlgeschlagen
- Kein Speicherplatz frei auf Gerät

Sie können den Befehl **df -h** ausführen, um zu überprüfen, wie viel Speicher verfügbar ist. Wenn das /boot-Verzeichnis bei 100 % angekommen ist, können Sie Folgendes tun:

- `sudo dpkg --get-selections | grep ^ii` ausführen, um alle installierten Kerneln anzuzeigen.
- `uname -r` ausführen, um Ihren derzeit ausgeführten Kernel anzuzeigen. Entfernen Sie diesen Kernel nicht (linux-image).
- Mithilfe von `apt-get purge` nicht mehr benötigte Images entfernen. Führen Sie zum Beispiel `sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic` aus.
- Den Host neu starten.
- In NSX Manager die Fehler überprüfen und **Beheben** auswählen.
- Überprüfen, ob die VMs eingeschaltet sind.

Konfigurationsfehler bei der Bereitstellung einer Edge-VM

Nach der Bereitstellung einer Edge-VM zeigt NSX Manager als Status der VM **Konfigurationsfehler** an. Das Manager-Protokoll weist sinngemäß die folgende Meldung auf:

```
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'].
```

Mit einem Neustart des Edge-Datenpfaddienstes und anschließendem Neustart der VM sollte das Problem behoben werden.

Erzwingen des Entfernens eines Transportknotens

Mit dem folgenden API-Aufruf können Sie einen Transportknoten entfernen, der im verwaisten Zustand steckengeblieben ist:

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

NSX Manager führt keine Validierungen im Hinblick darauf durch, ob aktive VMs auf dem Host ausgeführt werden. Sie sind für die Löschung von N-VDS und VIBs verantwortlich. Wenn Sie den Knoten über den Berechnungsmanager hinzugefügt haben, löschen Sie den Berechnungsmanager zuerst und löschen Sie dann den Knoten. Der Transportknoten wird ebenfalls gelöscht.

Fehlerbehebung: Routing

NSX-T verfügt über integrierte Tools für die Behebung von Routingfehlern.

Traceflow

Mit Traceflow können Sie den Flow von Datenpaketen überprüfen. Sie können zugestellte, verlorengelassene, empfangene und weitergeleitete Pakete anzeigen. Wenn ein Paket verloren geht, wird ein Grund angezeigt. Zum Beispiel kann ein Paket wegen einer Firewallregel verloren gehen.

Überprüfung der Routingtabellen

Führen Sie die folgenden Befehle aus, um die Routingtabelle auf einem Dienstrouter anzuzeigen:

```
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

```

Führen Sie den folgenden Befehl aus, um die IP-Adresse von Schnittstellen abzurufen:

```

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

```

Ankündigung für T1-Routen

Sie müssen T1 Routen ankündigen, damit sie auf T0-Routern und aufwärts sichtbar sind. Es gibt verschiedene Arten von Routen, die Sie ankündigen können: NSX Connected, NAT, Static, LB VIP und LB SNAT.

Fehlerbehebung für Firewall

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Problemen mit der Firewall.

Dieses Kapitel behandelt die folgenden Themen:

- [Ermitteln der auf einem ESXi-Host angewandten Firewallregeln](#)
- [Ermitteln der auf einem KVM-Host angewandten Firewallregeln](#)
- [Protokolle des Firewallpakets](#)

Ermitteln der auf einem ESXi-Host angewandten Firewallregeln

Zur Behebung von Problemen mit der Firewall bei einem ESXi-Host können Sie die Firewallregeln überprüfen, die für den Host gelten.

So rufen Sie die Liste der DvFilter auf dem ESXi-Host ab:

```
[root@esxi-01:~] summarize-dvfilter
<TRUNCATED OUTPUT>
world 70181 vmm0:app-01a vcUuid:'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 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
```

Suchen Sie einen DvFilter für eine spezifische VM:

```
[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
.
.
.
```

Ermitteln Sie die Firewallregeln, die für einen bestimmten DvFilter gelten (in diesem Beispiel ist nic-70227-eth0-vmware-sfw.2 der Name des DvFilters).

```
[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;
}
}
```

So rufen Sie die Liste der Adressensätze ab, die in einem bestimmten DvFilter verwendet werden:

```
[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,
}

```

Überprüfen Sie die Flows über einen bestimmten DvFilter:

```

[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:Un-
known(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:Un-
known(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:Un-
known(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:Un-
known(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:Un-
known(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:Un-
known(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
```

Ermitteln der auf einem KVM-Host angewandten Firewallregeln

Zur Behebung von Problemen mit der Firewall bei einem KVM-Host können Sie die Firewallregeln überprüfen, die für den Host gelten.

So rufen Sie die Liste der VIFs ab, für die die Firewallregeln auf dem KVM-Host gelten:

```
# 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
```

Wenn die Ausgabe leer ist, suchen Sie nach Konnektivitätsproblemen zwischen dem Knoten und den Controllern.

So rufen Sie die Liste der Regeln ab, die auf eine bestimmte VIF angewandt werden (in diesem Beispiel ist da95fc1e-65fd-461f-814d-d92970029bf0 die VIF-ID):

```
# 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;
}

```

So rufen Sie die Liste der Adressensätze ab, die in einer bestimmten VIF verwendet werden:

```

# 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,
}

```

Überprüfen Sie die Verbindungen über das Linux Conntrack-Modul. In diesem Beispiel suchen wir nach Flows zwischen zwei bestimmten IP-Adressen.

```

# 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=8,code=0),start=2018-03-26T04:43:28.325,id=3122159040,zone=23119,status=SEEN_REPLY|CONFIRMED,time-out=29,mark=3076,labels=0x1f

```

Protokolle des Firewallpakets

Wenn die Protokollierung für Firewallregeln aktiviert ist, können Sie zur Fehlerbehebung die Protokolle der Firewallpakete durchsehen.

Die Protokolldatei für ESXi- und KVM-Hosts lautet jeweils `/var/log/dfwpktlogs.log`.

```
# 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
```

Andere Szenarien zur Fehlerbehebung

6

Dieser Abschnitt beschreibt, wie Sie eine Fehlerbehebung für verschiedene Szenarien durchführen.

Dieses Kapitel behandelt die folgenden Themen:

- Fehler beim Hinzufügen oder Löschen eines Transportknotens
- Verbindungsaufbau des Transportknotens mit einem anderen Controller dauert etwa 5 Minuten
- NSX Manager-VM wird herabgestuft
- Zeitüberschreitung bei NSX Agent bei der Kommunikation mit NSX Manager
- Fehler beim Hinzufügen eines ESXi-Hosts
- Falscher NSX Controller-Status
- Management-IPs auf KVM-VMs nicht erreichbar bei aktiviertem IPFIX

Fehler beim Hinzufügen oder Löschen eines Transportknotens

Ein Transportknoten kann nicht gelöscht oder hinzugefügt werden.

Problem

Der Fehler tritt im folgenden Szenario auf:

- 1 Ein ESXi-Host ist ein Fabric-Knoten und ein Transportknoten.
- 2 Der Host wird als Transportknoten entfernt. Die Löschung des Transportknotens schlägt jedoch fehl. Der Zustand des Transportknotens lautet `Verwaist`.
- 3 Der Host wird als Fabric-Knoten sofort entfernt.
- 4 Der Host wird als Fabric-Knoten erneut hinzugefügt.
- 5 Der Host wird als Transportknoten mit einer neuen Transportzone und einem neuen Switch hinzugefügt. Dieser Schritt führt zu dem Fehler `Fehlgeschlagen/Teilweise erfolgreich`.

Ursache

Wenn Sie in Schritt 2 einige Minuten warten, wird die Löschung des Transportknotens erfolgreich abgeschlossen, weil NSX Manager die Löschung erneut versucht. Wenn Sie den Fabric-Knoten sofort löschen, kann NSX Manager keinen erneuten Versuch unternehmen, da der Host aus NSX-T Data Center entfernt wird. Dies führt zu einer unvollständigen Bereinigung des Hosts, bei der die Switch-Konfiguration noch vorhanden ist, und dies führt wiederum dazu, dass Schritt 5 fehlschlägt.

Lösung

- 1 Löschen Sie alle mit dem NSX-T Data Center-Switch verbundenen vmknics vom vCenter Server auf dem Host.
- 2 Rufen Sie mithilfe des CLI-Befehls `esxcfg-vswitch -l` den Switch-Namen ab. Beispiel:

```
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 Löschen Sie mithilfe des CLI-Befehls `esxcfg-vswitch -d <switch-name> --dvswitch` den Switch-Namen. Beispiel:

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

Verbindungsaufbau des Transportknotens mit einem anderen Controller dauert etwa 5 Minuten

Wenn die Verbindung zwischen einem ESXi-Transportknoten und seinem angeschlossenen Controller unterbrochen wird, dauert es etwa 5 Minuten, bis sich der Transportknoten mit einem anderen Controller verbindet.

Problem

Ein ESXi-Transportknoten ist normalerweise mit einem spezifischen Controller in einem Controller-Cluster verbunden. Sie können den verbundenen Controller mit dem CLI-Befehl `get controllers` finden. Wenn die Verbindung zum angeschlossenen Controller unterbrochen wird, dauert es etwa 5 Minuten, bis sich der Transportknoten mit einem anderen Controller verbindet.

Ursache

Der Transportknoten versucht zunächst über einen bestimmten Zeitraum hinweg, sich erneut mit dem ausgefallenen Controller zu verbinden. Gelingt dies nicht, stellt er stattdessen eine Verbindung zu einem anderen Controller her. Der gesamte Vorgang dauert ca. 5 Minuten. Dies ist das erwartete Verhalten.

NSX Manager -VM wird herabgestuft

NSX Manager, der auf einem KVM-Host bereitgestellt ist, gibt einen Fehler zurück, wenn CLI-Befehle wie `get service` und `get interface` ausgeführt werden.

Problem

Der CLI-Befehl „`get service`“ gibt einen Fehler zurück. Beispiel:

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

Andere CLI-Befehle geben möglicherweise ebenfalls einen Fehler zurück. Der Befehl `get support-bundle` gibt an, dass das Verzeichnis `/tmp` zu einem schreibgeschützten Verzeichnis geworden ist. Beispiel:

```
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'
```

Das Protokoll `/var/log/messages-<timestamp>` enthält Meldungen wie die Folgende:

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

Ursache

Eines oder mehrere Dateisysteme auf der NSX Manager-Appliance waren beschädigt. Mögliche Gründe sind in <https://access.redhat.com/solutions/22621> dokumentiert.

Zur Lösung des Problems können Sie die beschädigten Dateisysteme reparieren oder eine Wiederherstellung aus einer Sicherung durchführen.

Lösung

- 1 Option 1: Sie reparieren die beschädigten Dateisysteme. Die folgenden Schritte gelten spezifisch für NSX Manager bei Ausführung auf einem KVM-Host.
 - a Führen Sie den Befehl `virsh destroy` aus, um die NSX Manager-VM anzuhalten.
 - b Führen Sie den Befehl `virt-rescue` im Schreibmodus auf dem QCOW2-Image aus. Beispiel:

```
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 Führen Sie in der Eingabeaufforderung `virt-rescue` den Befehl `e2fsck` aus, um das Dateisystem `tmp` zu reparieren. Beispiel:

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

- d Führen Sie bei Bedarf `e2fsck /dev/nsx/tmp` erneut aus, bis keine Fehler mehr vorhanden sind.
- e Starten Sie NSX Manager mit dem Befehl `virsh start neu`.

2 Option 2: Sie führen eine Wiederherstellung aus einer Sicherung durch.

Anweisungen hierzu finden Sie im *NSX-T-Administratorhandbuch*.

Zeitüberschreitung bei NSX Agent bei der Kommunikation mit NSX Manager

In großen Umgebungen mit vielen Transportknoten und VMs auf ESXi-Hosts tritt bei der Kommunikation von auf ESXi-Hosts ausgeführten NSX Agents mit NSX Manager möglicherweise eine Zeitüberschreitung auf.

Problem

Manche Vorgänge, wie beispielsweise der Versuch des Anhängens einer VM-vnic an einen logischen Switch, schlagen fehl. `/var/run/log/nsx-opsagent.log` enthält sinngemäß folgende Meldung:

```
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
```

Ursache

In großen Umgebungen dauern manche Vorgänge möglicherweise länger als normal und schlagen fehl, weil die Standardwerte für die Zeitüberschreitung überschritten werden.

Lösung

1 Erhöhen Sie den Zeitüberschreitungswert für den NSX Agent.

- a Halten Sie auf dem ESXi-Host mit dem folgenden Befehl den NSX opsAgent an:

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

- b Bearbeiten Sie die Datei `/etc/vmware/nsx-opsagent/nsxa.json` und ändern Sie den Wert für `vifOperationTimeout` von 25 beispielsweise auf 55.

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

Hinweis Dieser Zeitüberschreitungswert muss kleiner als der von Ihnen in Schritt 2 festgelegte Wert für die `hostd`-Zeitüberschreitung sein.

- c Starten Sie den NSX opsAgent mit dem folgenden Befehl:

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

2 Erhöhen Sie den Wert für die hostd-Zeitüberschreitung.

- a Halten Sie auf dem ESXi-Host den hostd-Agent mit dem folgenden Befehl an:

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

- b Bearbeiten Sie die Datei `/etc/vmware/hostd/config.xml`. Heben Sie unter `<opaqueNetwork>` die Auskommentierung des Eintrags für `<taskTimeout>` auf und ändern Sie den Wert von 30 auf beispielsweise 60.

```
<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 Starten Sie den hostd-Agent mit dem folgenden Befehl:

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

Fehler beim Hinzufügen eines ESXi-Hosts

Sie können dem NSX-T Data Center-Fabric keinen ESXi-Host hinzufügen.

Problem

In der grafischen Benutzeroberfläche von NSX Manager schlägt das Hinzufügen eines ESXi-Hosts mit einem Fehler ähnlich dem Folgenden fehl: Dateipfad von ... wird von mehreren Nicht-Overlay-VIBs beansprucht. Die Protokolldatei zeigt Meldungen ähnlich der Folgenden an:

```
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/vmkmmod/nsx-vsip' is claimed by multiple non-overlay VIBs
```

Ursache

Einige VIBs von einer vorherigen Installation befinden sich noch auf dem Host, möglicherweise weil keine vollständige Deinstallation stattgefunden hat.

Lösung

- 1 Ermitteln Sie die Namen der VIBs, die diesen Fehler verursachen, aus der Fehlermeldung.
- 2 Verwenden Sie ESXi-Befehle zum Deinstallieren der VIBs.

Falscher NSX Controller-Status

Manche Controller in einem NSX Controller-Clusterbericht weisen einen falschen Status für einen der Controller auf.

Problem

Nachdem ein Controller einige Male aus- und eingeschaltet wurde, melden die anderen Controller, dass er inaktiv ist, obwohl er aktiv ist und ausgeführt wird.

Ursache

Ein interner Fehler, der das ZooKeeper-Modul betrifft, tritt manchmal auf, wenn ein Controller aus- und eingeschaltet wird, und führt zu einem Kommunikationsfehler zwischen diesem Controller und den anderen Controllern im Cluster.

Lösung

- ◆ Entfernen Sie den als inaktiv gemeldeten Controller-Knoten aus dem Cluster, entfernen Sie die Clusterkonfiguration aus dem Knoten und fügen Sie den Knoten erneut dem Cluster hinzu. Weitere Informationen finden Sie im Abschnitt „Ersetzen eines Mitglieds des NSX Controller-Clusters“ im *NSX-T Administratorhandbuch*.

Management-IPs auf KVM-VMs nicht erreichbar bei aktiviertem IPFIX

Wenn IPFIX auf mehreren VMs auf einem KVM-Host aktiviert ist und die Sampling-Rate 100 % beträgt, sind die Management-IPs auf manchen der VMs möglicherweise zwischenzeitlich nicht erreichbar.

Problem

Wenn Sie IPFIX für mehrere VMs auf demselben Host aktivieren und die Sampling-Rate auf 100 % einstellen, kann es zu einem großen Aufkommen an IPFIX-Datenverkehr kommen. Dies kann sich auf den Managementdatenverkehr auswirken und dazu führen, dass die Management-IPs zwischenzeitlich nicht erreichbar sind, selbst wenn der Produktions- und der Managementdatenverkehr über verschiedene OVS erfolgen.

Ursache

Die Arbeitslast ist zu belastend für den Host und die VMs.

Lösung

- ◆ Verringern Sie die Last auf dem Host, indem Sie die Anzahl der VMs mit aktiviertem IPFIX oder die Sampling-Rate verringern.