

Fehlerbehebungshandbuch zu NSX

Update 8

Geändert am 21. FEBRUAR 2020

VMware NSX Data Center for vSphere 6.3



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2010–2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Fehlerbehebungshandbuch zu NSX	6
	Allgemeine Richtlinien zur Fehlerbehebung	6
	Verwenden des NSX-Dashboard	7
	Befehlszeilen-Schnellreferenz zu NSX	10
	NSX-Host-Systemdiagnose	22
2	Fehlerbehebung bei der NSX-Infrastruktur	23
	Hostvorbereitung	23
	Erläuterungen zur Hostvorbereitungsarchitektur	29
	Dienstbereitstellung-Workflow für die Hostvorbereitung	33
	Dienstbereitstellungs-Workflow für Drittanbieterdienste	35
	Überprüfen des Kommunikationskanalstatus	37
	Installationsstatus ist „Nicht bereit“	39
	Dienst reagiert nicht	39
	Dienstbereitstellung scheitert mit Fehlermeldung zu nicht verfügbarem OVF/VIB	41
	Problem mit der Option „Auflösen“ nicht behoben	43
	Über vSphere ESX Agent Manager (EAM)	44
	Fehlerbehebung bei NSX Manager-Problemen	45
	Verbinden von NSX Manager mit vCenter Server	47
	Sekundärer NSX Manager hängt im Übergangsmodus fest	50
	Fehlschlagen der Konfiguration des NSX SSO Lookup Service	51
	Vorbereitung des logischen Netzwerks: VXLAN-Transport	54
	VXLAN-VMkernel-NIC ist nicht synchron	56
	Ändern der VXLAN-Gruppierungsrichtlinie und der MTU-Einstellungen	57
	Logische Switch-Portgruppe nicht synchron	59
3	Fehlerbehebung für das NSX-Routing	61
	Grundlegendes zum Distributed Logical Router (DLR)	62
	DLR-Paket-Flow auf oberster Ebene	63
	ARP-Auflösung für DLRs	65
	Grundlegendes zu dem vom Edge Services Gateway bereitgestellten Routing	67
	ECMP-Paket-Flow	67
	NSX-Routing: Voraussetzungen und Hinweise	69
	Benutzeroberflächen von DLR und ESG	72
	Benutzeroberfläche für das NSX-Routing	72
	Benutzeroberfläche von NSX Edges	73
	Neues NSX Edge (DLR)	75
	Unterschiede zwischen ESG und DLR	78

Typische ESG- und DLR-Benutzeroberflächenoperationen	79
Syslog-Konfiguration	79
Statische Routen	80
Route Redistribution	81
Fehlerbehebung für das NSX-Routing	82
Befehlszeilenschnittstelle (CLI) für das NSX-Routing	82
Kurze Zusammenfassung des Routing	85
Überprüfen des DLR-Status mithilfe einer Beispieltopologie für das Routing	86
DLR und seine zugehörigen Hostkomponenten (illustriert)	94
Architektur des Subsystems für verteiltes Routing	96
Komponenten des NSX-Routing-Subsystems	100
Steuerungskomponenten-CLI für das NSX-Routing	103
NSX-Routing-Subsystem: Fehlermodi und -auswirkungen	106
NSX-Protokolle für das Routing	110
Allgemeine Fehlerszenarien und deren Behebung	112
Erfassen von Daten zur Fehlerbehebung	113
4 Fehlerbehebung bei NSX Edge	117
Probleme durch verworfene Edge-Firewall-Pakete	121
Probleme mit der Edge-Routing-Konnektivität	126
NSX Manager- und Edge-Kommunikationsprobleme	128
Debugging für den Nachrichtenbus	129
Edge-Diagnose und -Wiederherstellung	131
5 Fehlerbehebung für Firewall	134
Informationen zur verteilten Firewall	134
CLI-Befehle für DFW (Distributed Firewall, verteilte Firewall)	135
Fehlerbehebung für die verteilte Firewall	138
Identitätsbasierte Firewall	144
6 Fehlerbehebung beim Lastausgleich	148
Szenario: Konfigurieren eines einarmigen Load Balancer	148
Flussdiagramm: Fehlerbehebung für den Load Balancer	154
Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche	155
Fehlerbehebung für Load Balancer mithilfe der Befehlszeilenschnittstelle	166
Allgemeine Probleme mit dem Load Balancer	177
7 Fehlerbehebung für virtuelle private Netzwerke (VPN)	182
L2 VPN	182
L2-VPN – häufig auftretende Konfigurationsprobleme	182
L2VPN-Optionen zum Verringern des Loopings	185

Fehlerbehebung über die Befehlszeile	187
SSL VPN	189
SSL VPN-Webportal wird nicht geöffnet	189
SSL VPN-Plus: Installationsfehler	190
SSL VPN-Plus: Kommunikationsprobleme	193
SSL VPN-Plus: Authentifizierungsprobleme	197
SSL VPN-Plus Client antwortet nicht mehr.	198
Grundlegende Protokollanalyse	198
IPSec-VPN	199
Erfolgreiche Aushandlung (sowohl Phase 1 als auch Phase 2)	199
Phase 1-Richtlinie stimmt nicht überein	200
Phase 2 stimmt nicht überein	201
PFS-Nichtübereinstimmung	202
PSK stimmt nicht überein	203
Paketerfassung für eine erfolgreiche Aushandlung	204
8 Fehlerbehebung für NSX Controller	210
Informationen zur Controller-Clusterarchitektur	210
Bereitstellungsprobleme von NSX Controller	213
Fehlerbehebung bei Festplattenlatenz	218
Festplattenlatenzwarnungen anzeigen	218
Festplattenlatenzprobleme	219
NSX Controller-Cluster-Fehler	221
Ansatz 1: Löschen des beschädigten Controllers und erneutes Bereitstellen eines neuen Controllers	223
Ansatz 2: Erneutes Bereitstellen eines NSX Controller-Clusters	226
Phantom-Controller	227
NSX Controller ist getrennt	229
Probleme mit dem Agenten der Kontrollebene (netcpa)	230
9 Fehlerbehebung bei Guest Introspection	234
Guest Introspection-Architektur	234
Guest Introspection-Protokolle	235
Protokolle des ESX-GI-Moduls (MUX)	236
GI Thin Agent-Protokolle	239
GI-EPSecLib- und SVM-Protokolle	241
Erfassen von Details zur Guest Introspection-Umgebung und -Arbeit	243
Fehlerbehebung beim Thin-Agent unter Linux oder Windows	244
Fehlerbehebung beim ESX-GI-Modul (MUX)	248
Fehlerbehebung bei EPSecLib	249

Fehlerbehebungshandbuch zu NSX

1

Das *Fehlerbehebungshandbuch zu NSX* erläutert die Überwachung und die Fehlerbehebung für das VMware NSX[®] for vSphere[®]-System mithilfe der NSX Manager-Benutzeroberfläche, des vSphere Web Client und anderer NSX-Komponenten, je nach Bedarf.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die NSX in einer VMware vCenter-Umgebung nutzen oder eine Fehlerbehebung dafür durchführen möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datencenter vertraut sind. Dieses Handbuch setzt voraus, mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Web Client vertraut zu sein.

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>.

Dieses Kapitel enthält die folgenden Themen:

- [Allgemeine Richtlinien zur Fehlerbehebung](#)

Allgemeine Richtlinien zur Fehlerbehebung

In diesem Thema werden allgemeine Richtlinien erläutert, denen Sie folgen können, um Probleme mit NSX for vSphere zu beheben.

- 1 Überprüfen Sie im [Verwenden des NSX-Dashboard](#), ob für eine Komponente Fehler oder Warnungen angezeigt werden.
- 2 Überprüfen Sie auf der Registerkarte **Überwachen (Monitor)** des primären NSX Manager, ob Systemereignisse ausgelöst wurden. Weitere Informationen zu Systemereignissen und Alarmen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.
- 3 Mit der GET `api/2.0/services/systemalarms`-API können Sie Alarme für das NSX-Objekt anzeigen. Weitere Informationen zur API finden Sie im Dokument *Handbuch zu NSX-API*.
- 4 Beheben Sie das Problem, wie im *Fehlerbehebungshandbuch zu NSX* beschrieben.

- 5 Wenn Sie das Problem nicht beheben können, laden Sie die Protokolle zum technischen Support herunter und kontaktieren Sie den VMware-Support. Siehe „[How to file a Support Request in My VMware](#)“ (Wie stelle ich in "My VMware" eine Support-Anfrage). Weitere Informationen zum Herunterladen von Protokollen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

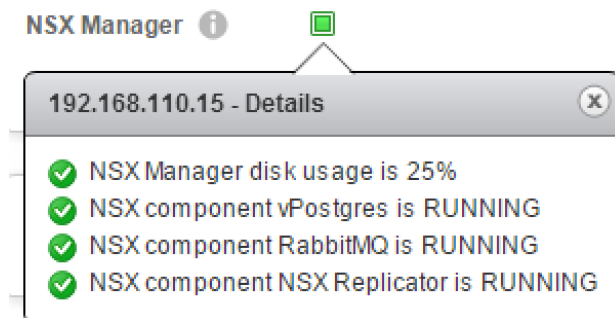
Verwenden des NSX-Dashboard

Das NSX-Dashboard bietet Transparenz des allgemeinen Systemzustands von NSX-Komponenten in einer zentralen Ansicht. Das NSX-Dashboard vereinfacht die Fehlerbehebung, weil es den Status der unterschiedlichen NSX-Komponenten anzeigt, z. B. von NSX Manager-Controllern, logischen Switches, der Hostvorbereitung, Dienstbereitstellung, von Sicherungen und Edge-Benachrichtigungen.

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Dashboard**. Die Dashboard-Seite wird angezeigt.
- 3 Wählen Sie in einer Cross-vCenter NSX-Umgebung NSX Manager mit primärer oder sekundärer Rolle aus.

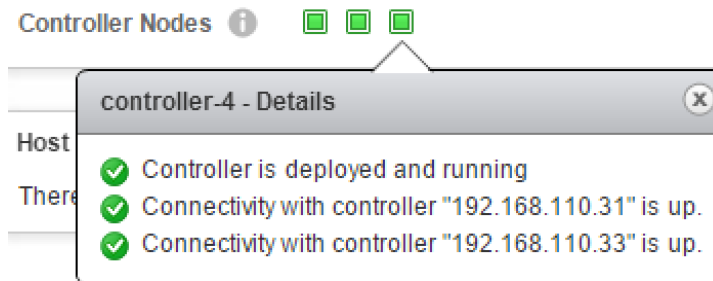
Dashboard stellt folgende Informationen bereit:

- NSX-Infrastruktur – Der NSX Manager-Komponentenstatus für die folgenden Dienste wird überwacht:
 - Datenbank-Dienst (vPostgres).
 - Nachrichtenbus-Dienst (RabbitMQ).
 - Replikator-Dienst – auch für die Überwachung im Hinblick auf Replizierungsfehler zuständig (falls Cross-vCenter NSX aktiviert ist).
 - NSX Manager-Festplattennutzung:
 - Gelb zeigt eine Festplattennutzung von > 80 % an.
 - Rot zeigt eine Festplattennutzung von > 90 % an.

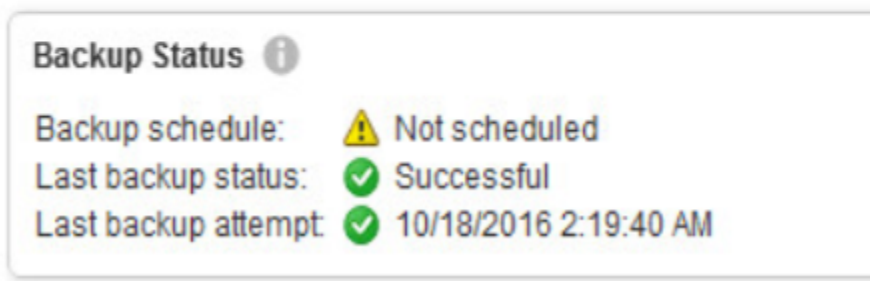
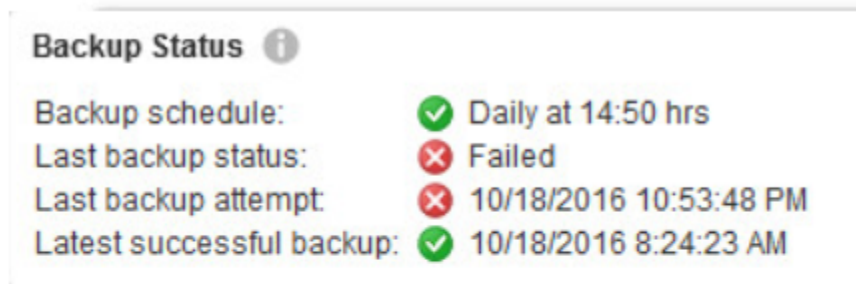


- NSX-Infrastruktur – NSX Controller-Status:
 - Status des Controller-Knotens (verfügbar/nicht verfügbar/wird ausgeführt/wird bereitgestellt/wird entfernt/ausgefallen/unbekannt).
 - Der Konnektivitätsstatus vom Controller-Peer wird angezeigt. Wenn der Controller nicht verfügbar ist und in roter Farbe angezeigt wird, werden die Peer-Controller in gelber Farbe angezeigt.

- Controller-VM-Status: ausgeschaltet/gelöscht.
- Controller-Warnung für Festplattenlatenz.



- NSX Manager-Sicherungsstatus:
 - Sicherungszeitplan.
 - Letzter Sicherungsstatus (fehlgeschlagen/erfolgreich/nicht geplant mit Datum und Uhrzeit).
 - Letzter Sicherungsversuch (Datum und Uhrzeit mit Details).
 - Letzte erfolgreiche Sicherung (Datum und Uhrzeit mit Details).



- NSX-Infrastruktur – Der Hoststatus für die folgenden Dienste wird überwacht:
 - Zugehörige Bereitstellung:
 - Anzahl der Cluster mit gescheiterter Installation.
 - Anzahl der Cluster mit erforderlichem Upgrade.
 - Anzahl der Cluster mit aktuell durchgeführter Installation.

- Anzahl der nicht vorbereiteten Cluster.
- Firewall:
 - Anzahl der Cluster mit deaktivierter Firewall.
 - Anzahl der Cluster, bei denen der Firewallstatus gelb/rot ist:
 - Gelb bedeutet, dass die verteilte Firewall auf allen Clustern deaktiviert ist.
 - Rot bedeutet, dass die verteilte Firewall auf allen Hosts/Clustern nicht installiert werden konnte.
- VXLAN:
 - Anzahl der Cluster mit nicht konfiguriertem VXLAN.
 - Anzahl der Cluster, bei denen der VXLAN-Status grün/gelb/rot ist:
 - Grün bedeutet, dass die Funktion erfolgreich konfiguriert wurde.
 - Gelb steht für beschäftigt, wenn die VXLAN-Konfiguration gerade durchgeführt wird.
 - Rot (Fehler) weist darauf hin, dass die VTEP-Erstellung fehlgeschlagen ist, VTEP die IP-Adresse nicht finden konnte, VTEP eine *LinkLocal*-IP-Adresse zugewiesen bekam usw.
- NSX-Infrastruktur – Status der Dienstbereitstellung
 - Bereitstellungsfehler – Installationsstatus für fehlgeschlagene Bereitstellungen.
 - Dienststatus – für alle fehlgeschlagenen Dienste.
- NSX-Infrastruktur – NSX Edge-Benachrichtigungen:

Das Dashboard für Edge-Benachrichtigungen zeigt aktive Warnungen für bestimmte Dienste an. Es überwacht die Liste der unten aufgeführten kritischen Ereignisse und verfolgt sie nach, bis das Problem behoben ist. Die Warnungen werden automatisch aufgehoben, wenn ein Wiederherstellungsereignis gemeldet wird oder eine erzwungene Edge-Synchronisierung stattfindet oder das Edge erneut bereitgestellt oder aktualisiert wird.

 - Load Balancer (Edge-Load-Balancer-Serverstatus):
 - Der Backend-Server des Edge-Load-Balancers ist nicht verfügbar.
 - Warnstatus des Backend-Servers des Edge-Load-Balancers.
 - VPN (IPsec-Tunnel/IPsec-Kanalstatus):
 - Edge-IPsec-Kanal ist nicht verfügbar.
 - Edge-IPsec-Tunnel ist nicht verfügbar.
 - Appliance (Edge-VM, Edge-Gateway, Edge-Dateisystem, NSX Manager und Berichtsstatus des Edge Services Gateway):
 - Beim Edge-Dienst-Gateway fehlt das Signal für die Prüfung des Systemzustands.
 - Die Edge-VM wurde ausgeschaltet.
 - Bei der Edge-VM fehlt das Signal für die Prüfung des Systemzustands.

- NSX Edge meldet einen fehlerhaften Status.
- NSX Manager meldet einen fehlerhaften Status für dieses Edge Services Gateway.
- Edge-VM ist nicht in VC-Bestand vorhanden.
- Split-Brain-Situation bei Hochverfügbarkeit entdeckt.

Hinweis Load-Balancer- und VPN-Warnungen werden bei Konfigurationsaktualisierungen nicht automatisch aufgehoben. Wenn das Problem behoben ist, müssen Sie die Warnungen manuell aufheben. Nutzen Sie dafür die API mit dem Befehl `alarm-id`. Hier ist das Beispiel der API, die Sie zum Aufheben der Warnungen verwenden können. Genauere Informationen finden Sie unter *Handbuch zu NSX-API*.

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

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

- NSX-Dienste – Firewallveröffentlichungsstatus:
 - Anzahl an Hosts, bei denen der Veröffentlichungsstatus der Firewall „fehlgeschlagen“ lautet. Der Status wird in Rot angezeigt, wenn ein Host die veröffentlichte verteilte Firewallkonfiguration nicht erfolgreich anwendet.
- NSX-Dienste – Status des logischen Netzwerks:
 - Anzahl an logischen Switches mit dem Status Fehler oder Warnung.
 - Wird gekennzeichnet, wenn die gesicherte verteilte virtuelle Portgruppe vom vCenter Server entfernt wird.

Befehlszeilen-Schnellreferenz zu NSX

Sie können die NSX-Befehlszeilenschnittstelle (CLI) verwenden, um Probleme zu beheben.

Tabelle 1-1. Überprüfung der NSX-Installation auf dem ESXi-Host – Befehle für NSX Manager

Beschreibung	Befehle für NSX Manager	Anmerkungen
Listet alle Cluster zur Ermittlung der Cluster-IDs auf	<code>show cluster all</code>	Es werden alle Clusterinformationen angezeigt
Listet alle Hosts im Cluster zur Ermittlung der Host-IDs auf	<code>show cluster clusterID</code>	Es werden die Liste der Hosts im Cluster, die Host-IDs und der Status der Hostvorbereitung für die Installation angezeigt
Listet alle VMs auf einem Host auf	<code>show host hostID</code>	Es werden bestimmte Hostinformationen, VMs, VM-IDs und der Energiestatus angezeigt

Tabelle 1-2. Namen der auf Hosts installierten VIBs und Module zur Verwendung in Befehlen

NSX-Version	ESXi-Version	VIBs	Modul
Alle 6.3.x	5.5	esx-vxlan und esx-vsip	vd12, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.2 und früher	6.0 und höher	esx-vxlan und esx-vsip	vd12, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.3 und höher	6.0 und höher	esx-nsxv	nsx-vd12, nsx-vdrb, nsx-vsip, nsx-dvfilter-switch-security, nsx-core, nsx-bfd, nsx-traceflow

Tabelle 1-3. Überprüfung der NSX-Installation auf dem ESXi-Host - Befehle für den Host

Beschreibung	Befehle für den Host	Anmerkungen
Welche VIBs vorhanden sind, hängt von der NSX- und ESXi-Version ab. In der Tabelle <i>Namen der auf Hosts installierten VIBs und Module</i> finden Sie Informationen darüber, welche Module in Ihrer Installation überprüft werden müssen.	<code>esxcli software vib get -- vibname <name></code>	Sie können damit Version und Datum der installierten VIBs überprüfen. <code>esxcli software vib list</code> übergibt eine Liste aller VIBs auf dem System
Listet alle aktuell im System geladenen Module auf	<code>esxcli system module list</code>	Äquivalenter älterer Befehl: <code>vmkload_mod -l grep -E vd12 vdrb vsip dvfilter-switch-security</code>
Welche Module vorhanden sind, hängt von der NSX- und ESXi-Version ab. In der Tabelle <i>Namen der auf Hosts installierten VIBs und Module</i> finden Sie Informationen darüber, welche Module in Ihrer Installation überprüft werden müssen.	<code>esxcli system module get -m <name></code>	Der Befehl muss für jedes Modul ausgeführt werden
Zwei Benutzerwelt-Agenten (UWAs, User World Agents): Steuerungsebenen-Agent, Firewall-Agent	<code>/etc/init.d/vShield-Stateful-Firewall status</code> <code>/etc/init.d/netcpad status</code>	
Überprüft die Verbindung der UWAs, Port 1234 für Controller und 5671 für NSX Manager	<code>esxcli network ip connection list grep 1234</code> <code>esxcli network ip connection list grep 5671</code>	Controller-TCP-Verbindung Nachrichtenbus-TCP-Verbindung
Überprüft den EAM-Status	vSphere Web Client, Verwaltung > vSphere ESX Agent Manager (Administration > vSphere ESX Agent Manager) überprüfen	

Tabelle 1-4. Überprüfung der NSX-Installation auf dem ESXi-Host – Befehle für das Hostnetzwerk

Beschreibung	Befehle für das Hostnetzwerk	Anmerkungen
Listet die physischen NICs/vmnic auf	<code>esxcli network nic list</code>	Sie können damit NIC-Typ, Treibertyp, Verbindungsstatus und MTU überprüfen
Physische NIC-Details	<code>esxcli network nic get -n vmnic#</code>	Sie können damit den Treiber und die Firmenversionen in Verbindung mit anderen Details überprüfen
Listet die vmk-Netzwerkkarten (NICs) mit IP-Adressen/MAC/MTU etc. auf	<code>esxcli network ip interface ipv4 get</code>	Damit kann sichergestellt werden, dass die VTEPs korrekt instanziiert sind
Listet die Details jeder vmk-Netzwerkkarte (NIC) auf, inklusive der VDS-Informationen	<code>esxcli network ip interface list</code>	Damit kann sichergestellt werden, dass die VTEPs korrekt instanziiert sind
Listet die Details jeder vmk-Netzwerkkarte (NIC) auf, inklusive der VDS-Informationen für VXLAN vmks	<code>esxcli network ip interface list --netstack=vxlan</code>	Damit kann sichergestellt werden, dass die VTEPs korrekt instanziiert sind
Ermittelt den dem VTEP dieses Hosts zugeordneten VDS-Namen	<code>esxcli network vswitch dvs vmware vxlan list</code>	Damit kann sichergestellt werden, dass die VTEPs korrekt instanziiert sind
Sendet einen Ping-Befehl vom VXLAN-dedizierten TCP/IP-Stack	<code>ping ++netstack=vxlan -I vmk1 x.x.x.x</code>	Dieser Befehl dient der Fehlerbehebung bei Problemen der VTEP-Kommunikation: Durch Hinzufügen der Option <code>-d -s 1572</code> können Sie sicherstellen, dass die MTU des Transportnetzwerks für VXLAN korrekt ist
Zeigt die Routing-Tabelle des VXLAN-dedizierten TCP/IP-Stack an	<code>esxcli network ip route ipv4 list -N vxlan</code>	Dieser Befehl dient der Fehlerbehebung bei Problemen der VTEP-Kommunikation
Zeigt die ARP-Tabelle des VXLAN-dedizierten TCP/IP-Stack an	<code>esxcli network ip neighbor list -N vxlan</code>	Dieser Befehl dient der Fehlerbehebung bei Problemen der VTEP-Kommunikation

Tabelle 1-5. Überprüfung der NSX-Installation auf dem ESXi-Host – Protokolldateien für Hosts

Beschreibung	Protokolldatei	Anmerkungen
Für NSX Manager	<code>show manager log follow</code>	Damit werden die NSX Manager-Protokolle maßgeschneidert angepasst. Dient der sofortigen Fehlerbehebung
Installationsprotokolle für einen Host	<code>/var/log/esxupdate.log</code>	
Probleme im Zusammenhang mit Hosts	<code>/var/log/vmkernel.log</code>	
VMkernel-Warnhinweise, Meldungen, Warnungen und Verfügbarkeitsbericht	<code>/var/log/vmksummary.log</code> <code>/var/log/vmkwarning.log</code>	
Erfassung von Fehlern beim Laden von Modulen	<code>/var/log/syslog</code>	IXGBE-Treiberfehler. Abhängigkeitsfehler von NSX-Modulen sind Schlüsselindikatoren
Bei vCenter ist ESX Agent Manager für Updates verantwortlich	In vCenter-Protokollen, <code>eam.log</code>	

Tabelle 1-6. Überprüfung logischer Switches – Befehle für NSX Manager

Beschreibung	Befehl für NSX Manager	Anmerkungen
Listet alle logische Switches auf	<code>show logical-switch list all</code>	Es werden alle logische Switches, ihre in der API verwendeten UUIDs, die Transportzone und vdnscope aufgeführt

Tabelle 1-7. Logische Switches – Befehle für NSX Controller

Beschreibung	Befehle für Controller	Anmerkungen
Ermittelt den Controller, der den VNI besitzt	<code>show control-cluster logical-switches vni 5000</code>	Beachten Sie die Controller-IP-Adresse in der Ausgabe und das zugehörige SSH-Protokoll
Ermittelt alle Hosts, die für diesen VNI mit diesem Controller verbunden sind	<code>show control-cluster logical-switch connection-table 5000</code>	Die Quell-IP-Adresse in der Ausgabe stellt die Verwaltungsschnittstelle des Hosts dar. Die Portnummer ist der Quellport der TCP-Verbindung
Ermittelt die VTEPs, die für das Hosten dieses VNI registriert wurden	<code>show control-cluster logical-switches vtep-table 5002</code>	
Listet die MAC-Adressen auf, die für VMs auf diesem VNI abgerufen wurden	<code>show control-cluster logical-switches mac-table 5002</code>	Stellen Sie sicher, dass sich die MAC-Adresse tatsächlich an dem VTEP, der sie meldet, befindet
Listet den ARP-Cache auf, in dem die VM-IP-Updates enthalten sind	<code>show control-cluster logical-switches arp-table 5002</code>	Der ARP-Cache läuft in 180 Sekunden ab
Ermittelt für ein bestimmtes Host/Controller-Paar welchen VNIs der Host beigetreten ist	<code>show control-cluster logical-switches joined-vnis <host_mgmt_ip></code>	

Tabelle 1-8. Logische Switches – Befehle für den Host

Beschreibung	Befehle für Hosts	Anmerkungen
Überprüft, ob das VXLAN des Hosts synchronisiert ist	<code>esxcli network vswitch dvs vmware vxlan get</code>	Es werden der Synchronisierungsstatus und der für die Kapselung verwendete Port dargestellt
Zeigt die verbundene VM und die Port-ID des logischen Switch für Datenpfaderfassungen an	<code>net-stats -l</code>	Dieser Befehl bietet eine einfachere Möglichkeit zur Erfassung des VM-Switchport für eine bestimmte VM
Überprüft, ob das VXLAN-Kernelmodul vdl2 geladen ist	<code>esxcli system module get -m vdl2</code>	Es werden alle Details zum angegebenen Modul angezeigt und die Version überprüft
Überprüft, ob die korrekte VXLAN-VIB-Version installiert ist In der Tabelle <i>Namen der auf Hosts installierten VIBs und Module</i> finden Sie Informationen darüber, welche VIBs in Ihrer Installation überprüft werden müssen.	<code>esxcli software vib get --vibname esx-vxlan</code> oder <code>esxcli software vib get --vibname esx-nsxv</code>	Es werden alle Details zum angegebenen VIB angezeigt Überprüft Version und Datum

Tabelle 1-8. Logische Switches – Befehle für den Host (Fortsetzung)

Beschreibung	Befehle für Hosts	Anmerkungen
Überprüft, ob der Host andere Hosts im logischen Switch erkennt	<code>esxcli network vswitch dvs vmware vxlan network vtep list --vxlan-id=5001 --vds-name=Compute_VDS</code>	Es wird eine Liste aller VTEPs angezeigt, für die dieser Host über die Information verfügt, dass sie vtep 5001 hosten
Überprüft, ob die Steuerungskomponente aktiviert und für einen logischen Switch aktiv ist	<code>esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS</code>	Damit kann sichergestellt werden, dass die Controller-Verbindung besteht und dass die Anzahl der Ports/MACs den VMs auf dem LS auf diesem Host entspricht
Überprüft, ob der Host die MAC-Adressen aller VMs kennt	<code>esxcli network vswitch dvs vmware vxlan network mac list --vds-name Compute_VDS --vxlan-id=5000</code>	Mit diesem Befehl sollten alle MACs für die VNI 5000-VMs auf diesem Host aufgeführt werden
Überprüft, ob der Host den ARP-Eintrag für Remote-VMs lokal zwischengespeichert hat	<code>esxcli network vswitch dvs vmware vxlan network arp list --vds-name Compute_VDS --vxlan-id=5000</code>	Überprüft, ob der Host den ARP-Eintrag für Remote-VMs lokal zwischengespeichert hat
Überprüft, ob die VM mit LS verbunden und einer lokalen VMKnic-Schnittstelle zugeordnet ist. Es wird auch angezeigt, welcher vmknic-ID ein VM-dvPort zugeordnet ist	<code>esxcli network vswitch dvs vmware vxlan network port list --vds-name Compute_VDS --vxlan-id=5000</code>	Der vdrport wird immer aufgeführt, solange der VNI mit einem Router verbunden ist
Zeigt die vmknic-IDs sowie den Switchport/Uplink an, dem sie zugeordnet sind	<code>esxcli network vswitch dvs vmware vxlan vmknic list --vds-name=DSwitch-Res01</code>	

Tabelle 1-9. Überprüfung logischer Switches – Protokolldateien

Beschreibung	Protokolldatei	Anmerkungen
Hosts werden immer mit Controllern verbunden, auf denen ihre VNIs gehostet werden	<code>/etc/vmware/netcpa/config-by-vsm.xml</code>	Diese Datei muss immer alle in der Umgebung aufgeführten Controller enthalten. Die Datei <code>config-by-vsm.xml</code> wird über den netcpa-Vorgang erstellt.
Die Datei <code>config-by-vsm.xml</code> wird von NSX Manager mithilfe von vsfwd übertragen. Wenn die Datei <code>config-by-vsm.xml</code> nicht korrekt ist, überprüfen Sie das vsfwd-Protokoll	<code>/var/log/vsfwd.log</code>	Untersuchen Sie diese Datei auf mögliche Fehler. Um den Vorgang neu zu starten, verwenden Sie <code>/etc/init.d/vShield-Stateful-Firewall stop start</code>
Die Verbindung zum Controller wird mithilfe von netcpa hergestellt	<code>/var/log/netcpa.log</code>	Untersuchen Sie diese Datei auf mögliche Fehler.
Modulprotokolle zu logischen Switches sind in <code>vmkernel.log</code> enthalten	<code>/var/log/vmkernel.log</code>	Überprüfen Sie die Modulprotokolle zu logischen Switches in <code>/var/log/vmkernel.log</code> „mit dem Präfix VXLAN:“

Tabelle 1-10. Überprüfung des logischen Routings – Befehle für NSX Manager

Beschreibung	Befehle für NSX Manager	Anmerkungen
Befehle für ESG	<code>show edge</code>	CLI-Befehle für das Edge Services Gateway (ESG) beginnen mit ‚show edge‘
Befehle für die DLR-Kontroll-VM	<code>show edge</code>	CLI-Befehle für die Kontroll-VM des Distributed Logical Router (DLR) beginnen mit ‚show edge‘
Befehle für DLR	<code>show logical-router</code>	CLI-Befehle für den Distributed Logical Router (DLR) beginnen mit <code>show logical-router</code>
Listet alle Edges auf	<code>show edge all</code>	Es werden damit alle Edges aufgeführt, die die zentrale Befehlszeilenschnittstelle (CLI) unterstützen
Listet alle Dienste und Bereitstellungsdetails eines Edge auf	<code>show edge edgeID</code>	Es werden damit Informationen zum Edge Service Gateway angezeigt
Listet die Befehlsoptionen für Edge auf	<code>show edge edgeID ?</code>	Mit diesem Befehl werden Informationen wie Version, Protokoll, NAT, Routing-Tabelle, Firewall, Konfiguration, Schnittstelle und Dienste angezeigt
Zeigt Routing-Details an	<code>show edge edgeID ip ?</code>	Mit diesem Befehl werden Routing-Informationen, BGP, OSPF und andere Details dargestellt
Zeigt die Routing-Tabelle an	<code>show edge edgeID ip route</code>	Damit wird die Routing-Tabelle für Edge dargestellt
Zeigt den Routing-Nachbarn an	<code>show edge edgeID ip ospf neighbor</code>	Damit wird die Beziehung zu Routing-Nachbarn dargestellt
Zeigt die Verbindungsinformationen für logische Router an	<code>show logical-router host hostID connection</code>	Damit können Sie überprüfen, ob die Anzahl der verbundenen LIFs sowie die Gruppierungsrichtlinie korrekt sind und ob der erforderliche VDS verwendet wird
Listet alle Instanzen des logischen Routers auf, die auf dem Host ausgeführt werden	<code>show logical-router host hostID dlr all</code>	<p>Damit lässt sich die Anzahl der LIFs und Routen überprüfen.</p> <p>Die Controller-IP muss für einen logischen Router auf allen Hosts identisch sein.</p> <p>Die Steuerungskomponente muss aktiviert sein.</p> <p>Mit <code>--brief</code> wird eine kompakte Antwort übergeben</p>

Tabelle 1-10. Überprüfung des logischen Routings – Befehle für NSX Manager (Fortsetzung)

Beschreibung	Befehle für NSX Manager	Anmerkungen
Überprüft die Routing-Tabelle auf dem Host	<code>show logical-router host hostID dlr dlrID route</code>	Es handelt sich dabei um die Routing-Tabelle, die vom Controller auf alle Hosts in der Transportzone übertragen wird. Diese muss für alle Hosts identisch sein. Wenn verschiedene Routen auf einigen Hosts nicht vorhanden sind, geben Sie den Befehl ‚sync‘ vom oben erwähnten Controller ein. Das Flag E bezieht sich auf Routen, die über ECMP abgerufen wurden
Überprüft die LIFs für einen DLR auf dem Host	<code>show logical-router host hostID dlr dlrID interface (all intName) verbose</code>	Die LIF-Informationen werden vom Controller auf die Hosts übertragen. Mit diesem Befehl können Sie sicherstellen, dass der Host über die notwendigen Informationen über alle LIFs verfügt

Tabelle 1-11. Überprüfung des logischen Routings – Befehle für NSX Controller

Beschreibung	Befehle für NSX Controller	Anmerkungen
Ermittelt alle Instanzen des logischen Routers	<code>show control-cluster logical-routers instance all</code>	Damit werden die Instanz des logischen Routers sowie alle Hosts in der Transportzone aufgeführt, die die Instanz des logischen Routers enthalten müssen. Darüber hinaus wird der Controller angezeigt, der die Dienste für diesen logischen Router bereitstellt
Zeigt Details zu jedem logischen Router an	<code>show control-cluster logical-routers instance 0x570d4555</code>	In der Spalte „IP“ werden die vmk0-IP-Adressen von allen Hosts aufgeführt, auf denen dieser DLR vorhanden ist
Zeigt alle Schnittstellen an, die mit dem logischen Router VERBUNDEN sind	<code>show control-cluster logical-routers interface-summary 0x570d4555</code>	In der Spalte „IP“ werden die vmk0-IP-Adressen von allen Hosts aufgeführt, auf denen dieser DLR vorhanden ist
Zeigt alle Routen an, die von diesem logischen Router abgerufen wurden	<code>show control-cluster logical-routers routes 0x570d4555</code>	Beachten Sie, dass in der Spalte „IP“ die vmk0-IP-Adressen von allen Hosts aufgeführt werden, auf denen dieser DLR vorhanden ist.
Zeigt alle eingerichteten Netzwerkverbindungen wie eine net stat-Ausgabe an	<code>show network connections of-type tcp</code>	Damit können Sie überprüfen, ob der Host, für den Sie eine Fehlerbehebung durchführen, über eine für den Controller eingerichtete netcpa-Verbindung verfügt

Tabelle 1-11. Überprüfung des logischen Routings – Befehle für NSX Controller (Fortsetzung)

Beschreibung	Befehle für NSX Controller	Anmerkungen
Synchronisiert Schnittstellen vom Controller mit dem Host	<code>sync control-cluster logical-routers interface-to-host <logical-router-id> <host-ip></code>	Dieser Befehl ist hilfreich, wenn eine neue Schnittstelle mit einem logischen Router verbunden, aber nicht mit allen Hosts synchronisiert wurde
Synchronisiert Routen vom Controller mit dem Host	<code>sync control-cluster logical-routers route-to-host <logical-router-id> <host-ip></code>	Dieser Befehl ist hilfreich, wenn auf einigen Hosts verschiedene Routen nicht vorhanden, aber für die Mehrheit der Hosts verfügbar sind

Tabelle 1-12. Überprüfung des logischen Routings – Befehle für Edge

Beschreibung	Befehle für Edge oder für die Kontroll-VM logischer Router	Anmerkungen
Zeigt die Konfiguration an	<code>show configuration <global bgp ospf ...></code>	
Zeigt die abgerufenen Routen an	<code>show ip route</code>	Mit diesem Befehl können Sie sicherstellen, dass die Routing- und Weiterleitungstabellen synchronisiert sind
Zeigt die Weiterleitungstabelle an	<code>show ip forwarding</code>	Mit diesem Befehl können Sie sicherstellen, dass die Routing- und Weiterleitungstabellen synchronisiert sind
Zeigt die Distributed Logical Router-Schnittstellen an	<code>show interface</code>	Die erste in der Ausgabe angezeigte Netzwerkkarte (NIC) ist die Distributed Logical Router-Schnittstelle Die Distributed Logical Router-Schnittstelle ist keine echte vNIC auf dieser VM Alle mit dem Distributed Logical Router verbundenen Subnetze sind vom Typ INTERN
Zeigt die anderen Schnittstellen an (Verwaltung)	<code>show interface</code>	Die Verwaltung/HA-Schnittstelle ist eine echte vNIC der Kontroll-VM des logischen Routers. Wenn die HA ohne Angabe einer IP-Adresse aktiviert wurde, wird 169.254.x.x/30 verwendet. Verfügt die Verwaltungsschnittstelle über eine IP-Adresse, wird diese hier dargestellt.
Führt ein Debugging des Protokolls durch	<code>debug ip ospf</code> <code>debug ip bgp</code>	Mit diesem Befehl können Sie Konfigurationsprobleme darstellen (z. B. nicht übereinstimmende OSPF Areas, Timer und falsches ASN). Hinweis: Die Ausgabe wird nur in der Edge-Konsole dargestellt (nicht über eine SSH-Sitzung)

Tabelle 1-12. Überprüfung des logischen Routings – Befehle für Edge (Fortsetzung)

Beschreibung	Befehle für Edge oder für die Kontroll-VM logischer Router	Anmerkungen
OSPF-Befehle	<pre>show configuration ospf show ip ospf interface show ip ospf neighbor show ip route ospf show ip ospf database show tech-support (mit Suche nach den Strings „EXCEPTION“ und „PROBLEM“)</pre>	
BGP-Befehle	<pre>show configuration bgp show ip bgp neighbor show ip bgp show ip route bgp show ip forwarding show tech-support (mit Suche nach den Strings „EXCEPTION“ und „PROBLEM“)</pre>	

Tabelle 1-13. Überprüfung des logischen Routings – Protokolldateien für Hosts

Beschreibung	Protokolldatei	Anmerkungen
Informationen zur Distributed Logical Router-Instanz werden durch vsfwd auf Hosts übertragen und im XML-Format gespeichert	/etc/vmware/netcpa/config-by-vsm.xml	<p>Wenn die Distributed Logical Router-Instanz auf dem Host nicht vorhanden ist, überprüfen Sie zuerst, ob die Instanz in dieser Datei enthalten ist.</p> <p>Ist dies nicht der Fall, starten Sie vsfwd.</p> <p>Darüber hinaus können Sie mit dieser Datei sicherstellen, dass alle Controller vom Host erkannt werden.</p>
Die oben dargestellte Datei wird von NSX Manager mithilfe von vsfwd übertragen. Wenn die Datei config-by-vsm.xml nicht korrekt ist, überprüfen Sie das vsfwd-Protokoll	/var/log/vsfwd.log	<p>Untersuchen Sie diese Datei auf mögliche Fehler.</p> <p>Um den Vorgang neu zu starten, verwenden Sie /etc/init.d/vShield-Stateful-Firewall stop start</p>
Die Verbindung zum Controller wird mithilfe von netcpa hergestellt	/var/log/netcpa.log	Untersuchen Sie diese Datei auf mögliche Fehler.
Modulprotokolle zu logischen Switches sind in vmkernel.log enthalten	/var/log/vmkernel.log	Überprüfen Sie die Modulprotokolle zu logischen Switches in /var/log/vmkernel.log „mit dem Präfix vxlan:“

Tabelle 1-14. Controller-Debugging – Befehle für NSX Manager

Beschreibung	Befehl (für NSX Manager)	Anmerkungen
Listet alle Controller mit dem jeweiligen Status auf	show controller list all	Mit diesem Befehl werden alle Controller und deren Ausführungsstatus dargestellt

Tabelle 1-15. Controller-Debugging – Befehle für NSX Controller

Beschreibung	Befehl (für Controller)	Anmerkungen
Überprüft den Status des Controller-Clusters	<code>show control-cluster status</code>	Die Ausgabe des Befehls sollte immer ‚Join Complete‘ (Beitritt abgeschlossen) und ‚Connected to Cluster Majority‘ (Mit Cluster-Mehrheit verbunden) sein.
Überprüft den Status auf fluktuierende Verbindungen und Meldungen	<code>show control-cluster core stats</code>	Der Zähler für verworfene Elemente darf nicht geändert werden
Zeigt die Aktivität des Knotens in Bezug auf den ursprünglichen Beitritt zum Cluster oder nach einem Neustart an	<code>show control-cluster history</code>	Dies ist ein leistungsfähiges Tool zur Fehlerbehebung bei Problemen im Zusammenhang mit dem Clusterbeitritt
Zeigt eine Liste der Knoten im Cluster an	<code>show control-cluster startup-nodes</code>	Beachten Sie, dass in der Liste nicht nur aktive Clusterknoten enthalten sein können. Die ausgegebene Liste sollte alle aktuell bereitgestellten Controller umfassen. Diese Liste wird vom Start-Controller zur Kontaktaufnahme mit anderen Controllern im Cluster verwendet
Zeigt alle eingerichteten Netzwerkverbindungen wie eine net stat-Ausgabe an	<code>show network connections of-type tcp</code>	Damit können Sie überprüfen, ob der Host, für den Sie eine Fehlerbehebung durchführen, über eine für den Controller eingerichtete netcpa-Verbindung verfügt
Startet den Controller-Vorgang neu	<code>restart controller</code>	Es wird damit nur der Haupt-Controller-Vorgang neu gestartet. Der Befehl erzwingt eine erneute Verbindung mit dem Cluster
Startet den Controller-Knoten neu	<code>restart system</code>	Damit wird die Controller-VM neu gestartet

Tabelle 1-16. Controller-Debugging – Protokolldateien für NSX Controller

Beschreibung	Protokolldatei	Anmerkungen
Zeigt den Controller-Verlauf und kürzliche Beitritte, Neustarts, etc. an	<code>show control-cluster history</code>	Dieser Befehl ist ein leistungsfähiges Tool für Clusterprobleme speziell im Zusammenhang mit dem Clustering
Überprüft Festplatten auf eine zu langsame Geschwindigkeit	<code>show log cloudnet/cloudnet_java-zookeeper<timestamp>.log filtered-by fsync</code>	Eine zuverlässige Möglichkeit zur Überprüfung von Festplatten auf eine zu langsame Geschwindigkeit ist die Prüfung der Datei cloudnet_java-zookeeper.log auf fsync-Meldungen. ZooKeeper gibt diese Meldungen aus, wenn die Synchronisierung länger als eine Sekunde dauert. Dies ist ein deutlicher Hinweis, dass jemand anderes die Festplatte zu diesem Zeitpunkt nutzt

Tabelle 1-16. Controller-Debugging – Protokolldateien für NSX Controller (Fortsetzung)

Beschreibung	Protokolldatei	Anmerkungen
Überprüft Festplatten auf langsame Geschwindigkeit/Ausfall	<code>show log syslog filtered-by collectd</code>	Meldungen wie jene in der umfangreichen Ausgabe zu „collectd“ weisen eventuell auf langsame oder ausgefallene Festplatten hin
Überprüft die Belegung des Festplattenspeicherplatz	<code>show log syslog filtered-by freespace:</code>	Mit einem Hintergrund-Job namens „freespace“ werden regelmäßig alte Protokolle und andere Dateien von der Festplatte gelöscht, wenn der belegte Speicherplatz einen bestimmten Schwellenwert erreicht. In manchen Fällen erhalten Sie eine große Zahl von freespace-Meldungen wenn die Festplatte klein ist und/oder die Belegung rasch zunimmt. Diese Meldungen können ein Hinweis darauf sein, dass der Speicherplatz auf der Festplatte knapp wird
Ermittelt die aktuell aktiven Clustermmitglieder	<code>show log syslog filtered-by Active cluster members</code>	Damit wird die Knoten-ID der aktuell aktiven Clustermmitglieder dargestellt. Da diese Meldung nicht immer ausgegeben wird, ist die Überprüfung älterer Syslog-Protokolle empfehlenswert
Zeigt die zentralen Controller-Protokolle an	<code>show log cloudnet/cloudnet_java-zookeeper.20150703-165223.3702.1og</code>	Wenn mehrere ZooKeeper-Protokolle vorhanden sind, verwenden Sie die Datei mit dem neuesten Zeitstempel. Diese Datei enthält Informationen über die Hauptauswahl der Controller-Cluster sowie weitere Informationen zur Verteilung von Controllern
Zeigt die zentralen Controller-Protokolle an	<code>show log cloudnet/cloudnet.nsx-controller.root.log.INFO.20150703-165223.3668</code>	Hier handelt es sich um die wichtigsten Arbeitsprotokolle des Controllers, etwa zur LIF-Erstellung, zum Verbindungs-Listener auf 1234 oder zum Sharding

Tabelle 1-17. Überprüfung der Verteilten Firewall – Befehle für NSX Manager

Beschreibung	Befehle für NSX Manager	Anmerkungen
Zeigt die Informationen zu einer VM an	<code>show vm vmID</code>	Dazu gehören Informationen wie DC, Cluster, Host, VM-Name, vNICs und installierte dvfilter
Zeigt bestimmte Informationen zur virtuellen Netzwerkkarte an	<code>show vnic icID</code>	Dazu gehören Informationen wie vNIC-Name, MAC-Adresse, PG und angewendete Filter
Es werden alle Clusterinformationen angezeigt	<code>show dfw cluster all</code>	Clustername, Cluster-ID, Datencentername, Firewallstatus
Zeigt bestimmte Clusterinformationen an	<code>show dfw cluster clusterID</code>	Hostname, Host-ID, Installationsstatus
Zeigt Hostinformationen zur DFW an	<code>show dfw host hostID</code>	VM-Name, VM-ID, Energiestatus

Tabelle 1-17. Überprüfung der Verteilten Firewall – Befehle für NSX Manager (Fortsetzung)

Beschreibung	Befehle für NSX Manager	Anmerkungen
Zeigt Details in einem dvfilter an	<code>show dfw host hostID filter filterID <option></code>	Damit werden Regeln, Statistiken, Adress-Sets, etc. für jede vNIC dargestellt
Zeigt DFW-Informationen für eine VM an	<code>show dfw vm vmID</code>	Zeigt den VM-Namen, die vNIC-ID, Filter etc. an
Zeigt vNIC-Details an	<code>show dfw vnic vnicID</code>	Zeigt den vNIC-Namen, die ID, MAC-Adresse, Portgruppe und Filter an
Listet die über die vNIC installierten Filter auf	<code>show dfw host hostID summarize-dvfilter</code>	Damit können Sie die gewünschte VM/vNIC sowie das Namensfeld ermitteln, das in den nächsten Befehlen als Filter verwendet werden soll
Zeigt die Regeln für einen bestimmten Filter bzw. für eine bestimmte vNIC an	<code>show dfw host hostID filter filterID rules</code> <code>show dfw vnic nicID</code>	
Zeigt die Details eines Adress-Sets an	<code>show dfw host hostID filter filterID addrsets</code>	Mit Regeln werden nur Adress-Sets angezeigt. Mit diesem Befehl können darüber hinaus die verschiedenen Elemente eines Adress-Sets dargestellt werden
Zeigt Spoofguard-Details per vNIC an	<code>show dfw host hostID filter filterID spoofguard</code>	Damit wird überprüft, ob SpoofGuard aktiviert ist und wie die/der aktuelle IP/MAC lautet
Zeigt Details der Flow-Datensätze an	<code>show dfw host hostID filter filterID flows</code>	Wenn das Flow Monitoring aktiviert ist, sendet der Host regelmäßig Flow-Informationen zum NSX Manager. Mit diesem Befehl können Sie Flows per vNIC anzeigen
Zeigt Statistiken für jede Regel einer vNIC an	<code>show dfw host hostID filter filterID stats</code>	Mit diesem Befehl können Sie feststellen, ob Regeln angewandt wurden

Tabelle 1-18. Überprüfung der Verteilten Firewall – Befehle für Hosts

Beschreibung	Befehle für den Host	Anmerkungen
Listet die zum Host heruntergeladenen VIBs auf. In der Tabelle <i>Namen der auf Hosts installierten VIBs und Module</i> finden Sie Informationen darüber, welche VIBs in Ihrer Installation überprüft werden müssen.	<code>esxcli software vib list grep esx-vmip</code> oder <code>esxcli software vib list grep esx-nsxv</code>	Damit können Sie feststellen, ob die richtige VIB-Version heruntergeladen wurde
Zeigt Details zu den aktuell geladenen Systemmodulen an In der Tabelle <i>Namen der auf Hosts installierten VIBs und Module</i> finden Sie Informationen darüber, welche Module in Ihrer Installation überprüft werden müssen.	<code>esxcli system module get -m vmip</code> oder <code>esxcli system module get -m nsx-vmip</code>	Damit können Sie feststellen, ob das jeweilige Modul installiert/geladen wurde

Tabelle 1-18. Überprüfung der Verteilten Firewall – Befehle für Hosts (Fortsetzung)

Beschreibung	Befehle für den Host	Anmerkungen
Zeigt eine Vorgangsliste an	<code>ps grep vsfwd</code>	Damit können Sie feststellen, ob der vsfwd-Vorgang mit mehreren Threads ausgeführt wird
Daemon-Befehl	<code>/etc/init.d/vShield-Stateful-Firewall {start stop status restart}</code>	Damit können Sie feststellen, ob der Daemon ausgeführt wird und bei Bedarf neu gestartet werden muss
Zeigt die Netzwerkverbindung an	<code>esxcli network ip connection list grep 5671</code>	Damit können Sie feststellen, ob der Host über eine TCP-Konnektivität mit dem NSX Manager verfügt

Tabelle 1-19. Überprüfung der Verteilten Firewall – Protokolldateien für Hosts

Beschreibung	Protokoll	Anmerkungen
Vorgangsprotokoll	<code>/var/log/vsfwd.log</code>	vsfwd-Deamon-Protokoll für den vsfwd-Vorgang, NSX Manager-Konnektivität und RabbitMQ-Fehlerbehebung
Dedizierte Datei für Paketprotokolle	<code>/var/log/dfwpktlogs.log</code>	Diese Datei stellt die dedizierte Protokolldatei für Paketprotokolle dar
Paketerfassung mit dvfilter	<code>pktcap-uw --dvfilter nic-1413082-eth0-vmware-sfw.2 -- outfile test.pcap</code>	

NSX-Host-Systemdiagnose

Von der zentralen NSX Manager-Befehlszeilenschnittstelle (CLI) aus können Sie den Systemzustand der einzelnen ESXi-Hosts überprüfen.

Für den Systemzustand wird „critical“ (kritisch), „unhealthy“ (instabil) oder „healthy“ (stabil) ausgegeben.

Beispiel:

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

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

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

Der Befehl `host-check` lässt sich auch über die NSX Manager-API aufrufen.

Fehlerbehebung bei der NSX-Infrastruktur

2

Die NSX-Vorbereitung erfolgt in vier Schritten.

- 1 Verbinden Sie NSX Manager mit vCenter Server. Zwischen NSX Manager und vCenter Server besteht eine Eins-zu-Eins-Beziehung.
 - a Registrieren Sie sich bei vCenter Server.
- 2 Stellen Sie die NSX Controller bereit (nur für logisches Switching, verteiltes Routing oder VXLAN im Unicast- oder Hybridmodus erforderlich. Wenn Sie lediglich die verteilte Firewall (Distributed Firewall, DFW) verwenden, werden keine Controller benötigt.)
- 3 Hostvorbereitung: Installieren Sie VIBs für VXLAN, DFW und DLR auf allen Hosts im Cluster. Konfigurieren Sie die RabbitMQ-basierte Messaging-Infrastruktur. Aktivieren Sie die Firewall. Stellen Sie die Controller dar, deren Hosts für NSX bereit sind.
- 4 Konfigurieren Sie die IP-Pool-Einstellungen und VXLAN: Erstellen Sie eine VTEP-Portgruppe und VMKNICs auf allen Hosts im Cluster. In diesem Schritt können Sie die Transport-VLAN-ID, die Gruppierungsrichtlinie und die MTU festlegen.

Weitere Informationen zur Installation und Konfiguration aller Schritte finden Sie im *Installationshandbuch für NSX* und im *Administratorhandbuch für NSX*.

Dieses Kapitel enthält die folgenden Themen:

- [Hostvorbereitung](#)
- [Fehlerbehebung bei NSX Manager-Problemen](#)
- [Vorbereitung des logischen Netzwerks: VXLAN-Transport](#)
- [Logische Switch-Portgruppe nicht synchron](#)

Hostvorbereitung

Der vSphere ESX Agent Manager stellt vSphere-Installationspakete (VIBs) auf ESXi-Hosts bereit.

Für die Bereitstellung auf Hosts muss DNS auf den Hosts, auf vCenter Server und NSX Manager konfiguriert werden. Für die Bereitstellung ist kein Neustart des ESXi-Hosts erforderlich. Dieser muss allerdings bei Aktualisierungen oder nach dem Entfernen von VIBs vorgenommen werden.

VIBs werden auf NSX Manager gehostet und sind auch als ZIP-Datei verfügbar.

Die Datei kann von <https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties> heruntergeladen werden. Die ZIP-Datei zum Herunterladen unterscheidet sich je nach NSX- und ESXi-Version. vSphere 6.0-Hosts verwenden in NSX 6.3.0 z. B. die Datei <https://<NSX-Manager-IP>/bin/vdn/vibs-6.3.0/6.0-buildNumber/vxlan.zip>.

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

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

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

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

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

Welche VIBs auf einem Host installiert sind, hängt von der NSX- und ESXi-Version ab:

ESXi-Version	NSX-Version	Installierte VIBs
5.5	Alle 6.3.x	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	<ul style="list-style-type: none"> ■ esx-nsxv

Sie können die installierten VIBs mit dem Befehl `esxcli software vib list` anzeigen.

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


oder

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

Allgemeine Probleme bei der Hostvorbereitung

Bei der Vorbereitung von Hosts können folgende, typische Probleme auftreten:

- EAM kann keine VIBs bereitstellen.
 - Eine mögliche Ursache ist eine fehlerhafte DNS-Konfiguration auf den Hosts.
 - Eine andere mögliche Ursache ist eine Firewall, die die erforderlichen Ports zwischen ESXi, NSX Manager und vCenter Server blockiert.

Die meisten Probleme werden durch Klicken auf die Option **Auflösen (Resolve)** behoben.

Informationen finden Sie unter [Installationsstatus ist „Nicht bereit“](#).

- Ein früheres VIB einer älteren Version ist bereits installiert. In diesem Fall muss der Benutzer die Hosts neu starten.
- Zwischen NSX Manager und vCenter Server treten Kommunikationsprobleme auf. Die Registerkarte **Hostvorbereitung (Host Preparation)** im Plug-In „Networking and Security“ zeigt einige Hosts nicht korrekt an:
 - Überprüfen Sie, ob mit vCenter Server alle Hosts und Cluster angegeben werden.

Wenn sich das Problem mit der Option **Auflösen (Resolve)** nicht beheben lässt, finden Sie weitere Informationen unter [Problem mit der Option „Auflösen“ nicht behoben](#).

Fehlerbehebung bei der Hostvorbereitung (VIBs)

- Überprüfen Sie den Kommunikationskanalstatus für den Host. Weitere Informationen dazu finden Sie unter [Überprüfen des Kommunikationskanalstatus](#).
- Überprüfen Sie vSphere ESX Agent Manager auf Fehler.

vCenter-Startseite > Verwaltung > vCenter Server-Erweiterungen > vSphere ESX Agent Manager (vCenter home > Administration > vCenter Server Extensions > vSphere ESX Agent Manager)

Überprüfen Sie in vSphere ESX Agent Manager den Status der Agencies mit dem Präfix „VCNS160“. Befindet sich eine Agency in einem ungültigen Status, wählen Sie diese aus und überprüfen Sie die damit verbundenen Probleme.

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

Issues for the selected agencies

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

- Auf dem Host mit einem aufgetretenen Problem führen Sie den Befehl `tail /var/log/esxupdate.log` aus.

```

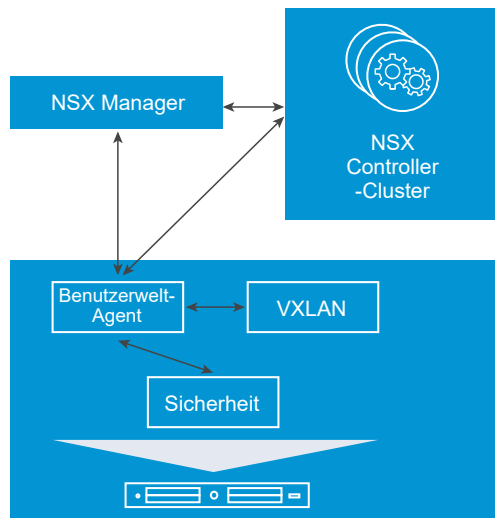
2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vcsa-01a.corp.local/tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exception occurred
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call last):
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate.py", line 106, in <module>
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/online/packages/vmware/esxupdate/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     File "/build/mts/release/online/packages/vmware/esximage/Transaction.py", line 73, in DownloadMetadatas
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-210-fd3f37ad4c', None, "('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-210-fd3f37ad4c', None, 'Temporary failure in name resolution')")')
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<

```

Fehlerbehebung bei der Hostvorbereitung (UWA)

NSX Manager konfiguriert zwei Benutzerwelt-Agenten auf allen Hosts in einem Cluster:

- Nachrichtenbus-UWA (vsfwd)
- Steuerungskomponente-UWA (netcpa)



In seltenen Fällen kann es vorkommen, dass nach einer erfolgreichen Installation der VIBs ein oder beide Benutzerwelt-Agenten nicht korrekt funktionieren. Dies kann folgende Formen annehmen:

- Die Firewall zeigt einen ungültigen Status an.

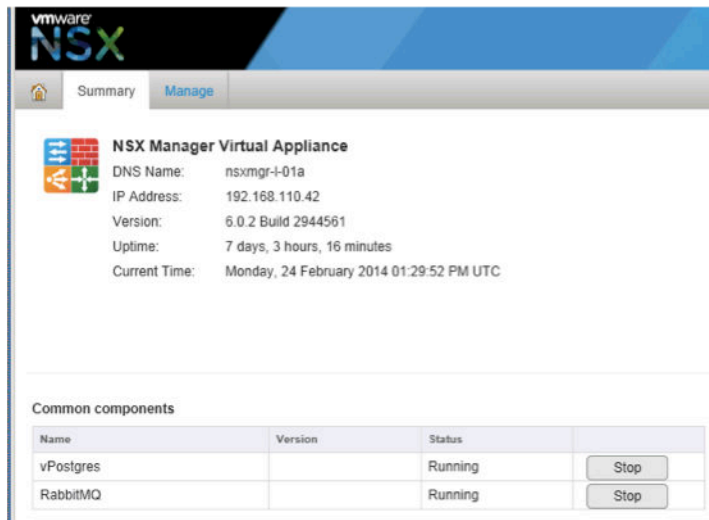
Cluster & Hosts	Installation Status	Firewall
c-1	6.0 Uninstall	Error

- Die Steuerungskomponente zwischen Hypervisoren und den Controllern ist inaktiv. Überprüfen Sie die NSX Manager-Systemereignisse. Informationen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

Getting Started	Summary	Monitor	Manage
Audit Logs	System Events	Tasks	

Timestamp	Severity	Event Source	Code	Event Message
2/26/2014 10:56:38 AM	Critical	Host messaging infrastructure	391002	Messaging infrastructure down on host.
2/26/2014 10:51:56 AM	Critical	host-22	301502	Spoofguard configuration update number 139340752032...
2/26/2014 10:51:56 AM	Critical	host-20	301502	Spoofguard configuration update number 139340752032...

Ist mehr als ein ESXi-Host betroffen, überprüfen Sie den Status des Nachrichtenbusdienstes in der Web UI der NSX Manager-Appliance in der Registerkarte **Übersicht (Summary)**. Wurde RabbitMQ gestoppt, starten Sie diesen Broker neu.



Wenn der Nachrichtenbusdienst für NSX Manager aktiv ist:

- Überprüfen Sie durch Ausführung des Befehls `/etc/init.d/vShield-Stateful-Firewall status` auf den ESXi-Hosts den Status des Benutzerwelt-Agenten des Nachrichtenbusses auf den Hosts.

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

- Überprüfen Sie die Protokolle des Benutzerwelt-Nachrichtenbusses auf den Hosts unter `/var/log/vs fwd.log`.
- Führen Sie auf den ESXi-Hosts den Befehl `esxcfg-advcfg -l | grep Rmq` zur Anzeige aller Rmq-Variablen aus. Es müssen 16 Rmq-Variablen vorhanden sein.

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

- Führen Sie auf den ESXi-Hosts den Befehl `esxcfg-advcfg -g /UserVars/RmqIpAddress` aus. Als Ausgabe sollte die IP-Adresse von NSX Manager angezeigt werden.

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

- Führen Sie auf den ESXi-Hosts den Befehl `esxcli network ip connection list | grep 5671` zur Überprüfung aus, ob die Nachrichtenbusverbindung aktiv ist.

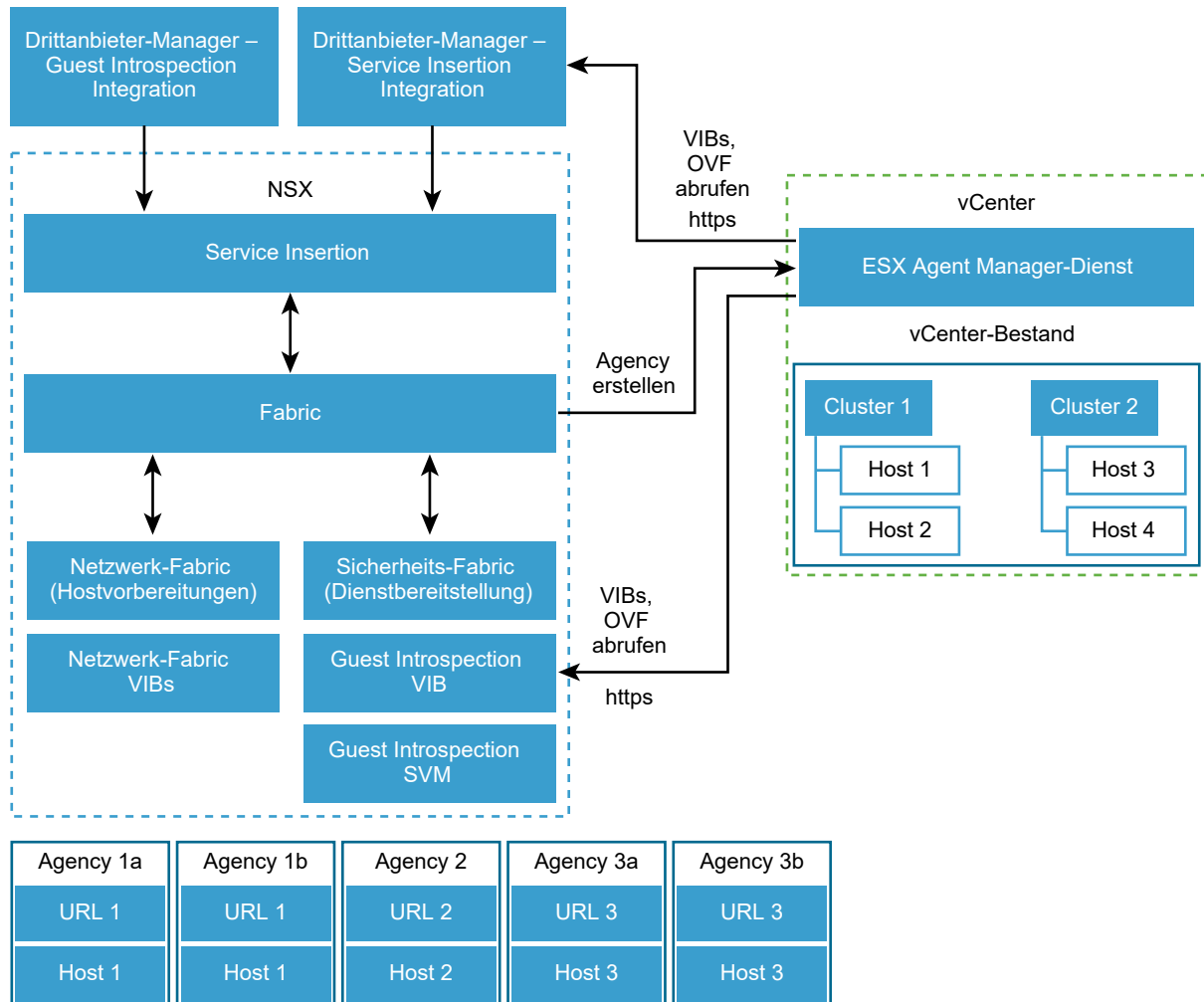
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp          0      0 192.168.110.51:29969      192.168.110.15:5671      ESTABLISHED
35505 newreno vsfwd
tcp          0      0 192.168.110.51:29968      192.168.110.15:5671      ESTABLISHED
35505 newreno vsfwd
```

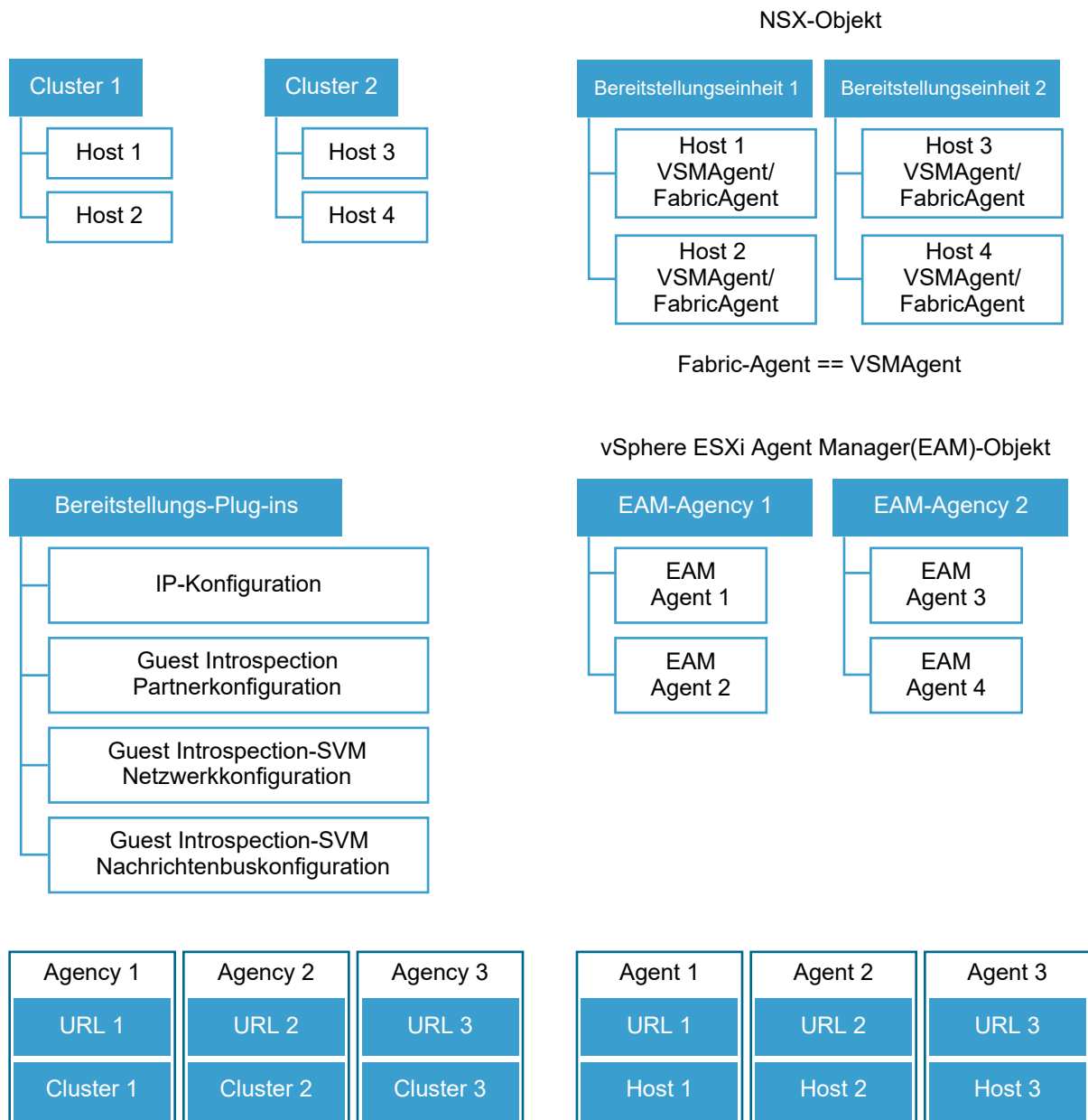
Informationen zu Problemen mit dem Agenten der Steuerungskomponente finden Sie unter [Probleme mit dem Agenten der Kontrollebene \(netcpa\)](#).

Erläuterungen zur Hostvorbereitungsarchitektur

Dieses Thema erläutert die grundlegende Hostvorbereitungsarchitektur.

- Für die Bereitstellung der Netzwerk-Fabric wechseln Sie zur Registerkarte **Hostvorbereitung (Host Preparation)**.
- Für die Bereitstellung der Sicherheits-Fabric wechseln Sie zur Registerkarte **Dienstbereitstellung (Service Deployment)**.





Die folgenden Begriffe helfen Ihnen, die Hostvorbereitungsarchitektur zu verstehen:

Fabric	<p>Fabric ist ein Software-Schicht in NSX Manager, der mit ESX Agent Manager für die Installation von Netzwerk- und Sicherheits-Fabric-Diensten auf Hosts interagiert.</p>
Netzwerk-Fabric	<p>Netzwerk-Fabric-Dienste werden auf einem Cluster bereitgestellt. Zu den Netzwerk-Fabric-Diensten gehören Hostvorbereitung, VXLAN, verteiltes Routing, verteilte Firewall und der Nachrichtenbus.</p>
Sicherheits-Fabric	<p>Sicherheits-Fabric-Dienste werden auf einem Cluster bereitgestellt. Die Sicherheits-Fabric-Dienste umfassen Guest Introspection und Sicherheitslösungen von Partnern.</p>
Fabric-Agent	<p>Ein Fabric-Agent ist eine Kombination aus einem Fabric-Dienst und einem Host in der NSX Manager-Datenbank. Pro Host wird ein Fabric-Agent für einen Cluster erstellt, auf dem ein Netzwerk- oder Sicherheits-Fabric-Dienst bereitgestellt wird.</p> <p>Auch bekannt als: VSM-Agent</p>
Bereitstellungseinheit	<p>Die Kombination aus einem Fabric-Dienst und einem Cluster in der NSX Manager-Datenbank. Eine Bereitstellungseinheit muss vor der Installation von Netzwerk- und Sicherheitsdiensten erstellt werden.</p>
ESX Agent Manager-Agent	<p>Ein ESX Agent Manager-Agent ist eine Kombination aus einer Dienstspezifikation und einem Host in der vCenter Server-Datenbank. Ein ESX Agent Manager-Agent ist einem NSX-Fabric-Agenten zugeordnet.</p>
ESX Agent Manager Agency	<p>Eine ESX Agent Manager Agency ist eine Kombination aus einer Spezifikation und einem Cluster in der vCenter Server-Datenbank. Die Spezifikation beschreibt die verwalteten ESX Agent Manager-Agenten und VIBs, OVFs und deren Konfiguration (z. B. Datenspeicher- und Netzwerkeinstellungen).</p> <p>Der NSX Manager erstellt eine ESX Agent Manager Agency für alle Cluster, die vorbereitet werden.</p> <p>Eine ESX Agent Manager Agency ist einer NSX-Bereitstellungseinheit zugeordnet. Die NSX Manager-Datenbank von Bereitstellungseinheiten und die vCenter ESX Agent Manager-Datenbank von ESX Agent Manager Agencies müssen synchron sein. Sind die beiden Datenbanken nicht synchron, was selten der Fall ist, informiert NSX Sie mit Ereignissen und Alarmen über dieses Problem. NSX Manager erstellt für jede ESX Agent Manager Agency eine Bereitstellungseinheit in seiner Datenbank.</p>

Der NSX Manager erstellt eine ESX Agent Manager Agency für alle Cluster, die vorbereitet werden. NSX Manager erstellt für jede ESX Agent Manager Agency eine Bereitstellungseinheit in seiner Datenbank. Eine ESX Agent Manager Agency = eine Bereitstellungseinheit.

Sie können Agencys auf folgende Arten anzeigen:

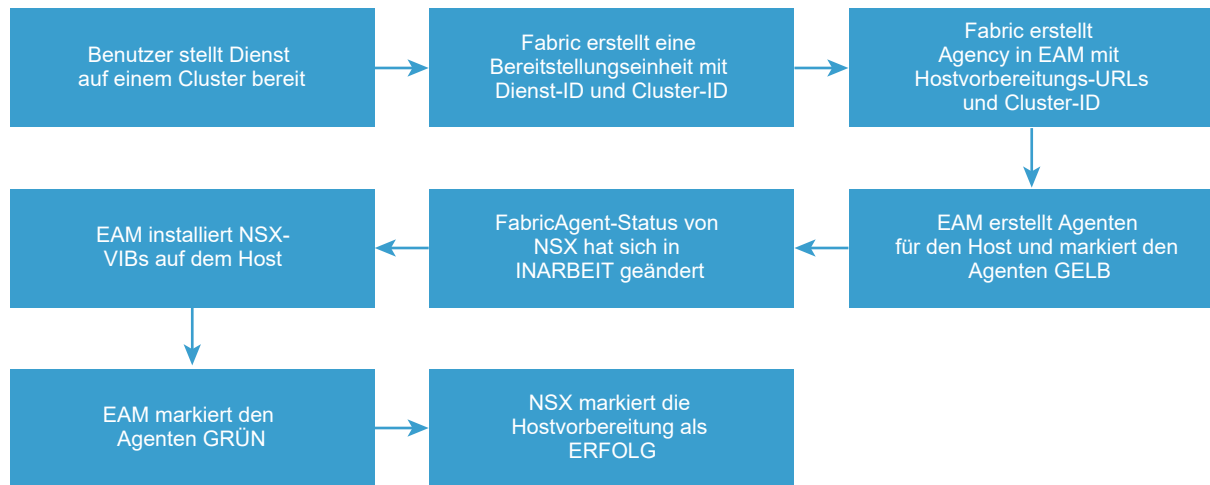
- Über den EAM-MOB *https://<VC-hostname/IP>/eam/mob/*.
- Über den vSphere Web Client:
 - Gehen Sie zu **vCenter Solutions Manager > vSphere ESX Agent Manager > Verwalten (Manage)**.
 - Unter **ESX-Agencys (ESX Agencies)** werden die Agencys angezeigt (eine pro Cluster, der für einen Host vorbereitet wurde).

Der Lebenszyklus einer Bereitstellungseinheit ist an den der Agency gekoppelt. Wird eine Agency von ESX Agent Manager entfernt, so wird auch die zugehörige Bereitstellungseinheit von NSX entfernt.

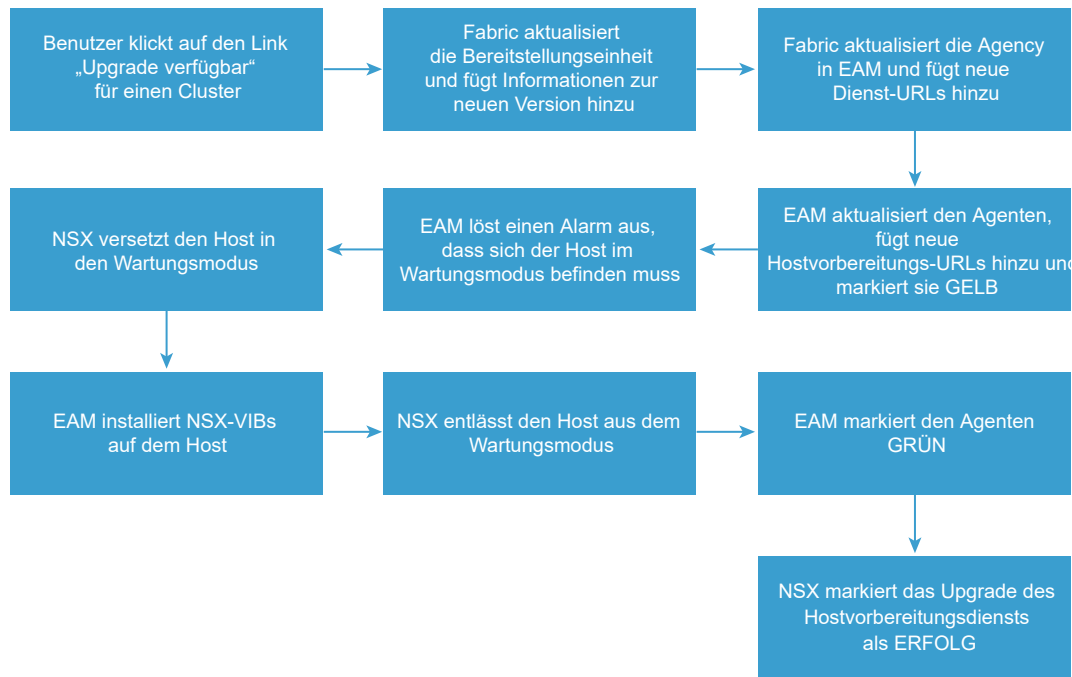
Dienstbereitstellung-Workflow für die Hostvorbereitung

In diesem Abschnitt finden Sie Informationen zum Dienstbereitstellungs-Workflow (Installation und Upgrade) für die Hostvorbereitung.

Workflow der Installation



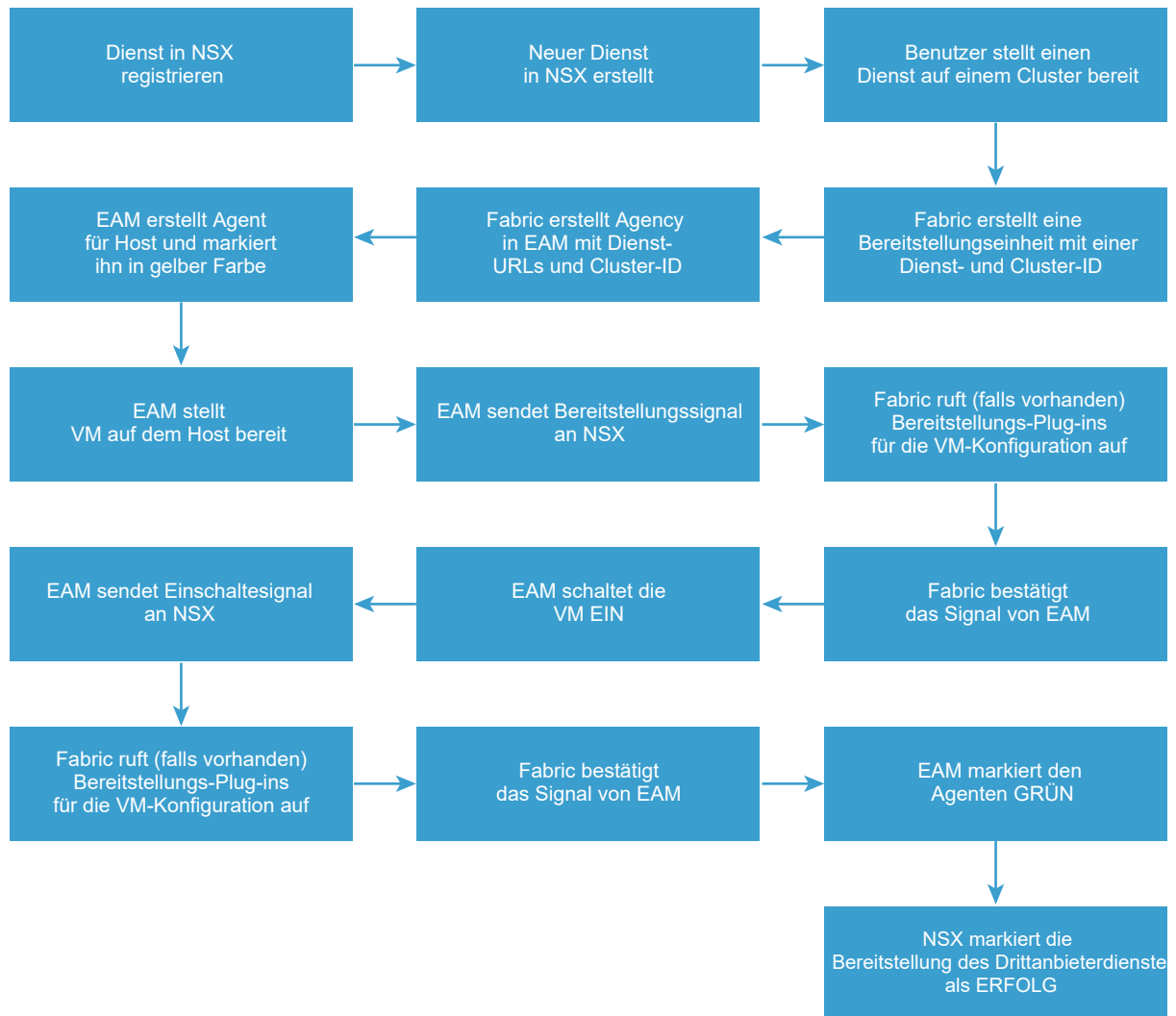
Workflow des Upgrades



Dienstbereitstellungs-Workflow für Drittanbieterdienste

In diesem Abschnitt finden Sie Informationen zum Dienstbereitstellungs-Workflow (Installation und Upgrade) für Drittanbieterdienste.

Workflow der Installation



Workflow des Upgrades



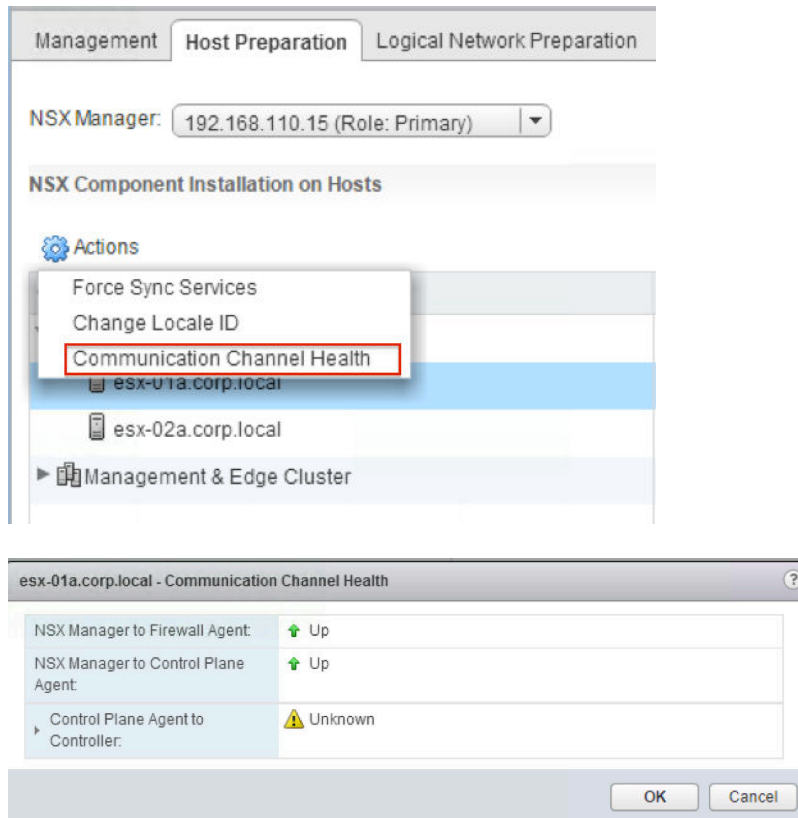
Überprüfen des Kommunikationskanalstatus

In vSphere Web Client können Sie den Status der Kommunikation zwischen einer Vielzahl von Komponenten überprüfen.

Um den Kommunikationskanalstatus zwischen NSX Manager und dem Firewallagenten, NSX Manager und dem Steuerungsebenen-Agenten sowie zwischen dem Steuerungsebenen-Agenten und den Controllern zu überprüfen, führen Sie folgende Schritte durch:

- 1 Navigieren Sie in vSphere Web Client zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.
- 2 Wählen Sie einen Cluster aus oder erweitern Sie einen Cluster und wählen Sie einen Host aus.
Klicken Sie auf **Aktionen (Actions)** (⚙️) und dann auf **Kommunikationskanalstatus (Communication Channel Health)**.

Die Informationen zum Kommunikationskanalstatus werden angezeigt.



Wenn sich der Status einer der drei Verbindungen für einen Host ändert, wird in das NSX Manager-Protokoll eine entsprechende Meldung geschrieben. In dieser Meldung wird der Status einer Verbindung als UP (Aktiv), DOWN (Inaktiv) oder NOT_AVAILABLE (Nicht verfügbar, in vSphere Web Client als „Unbekannt“ angezeigt) angegeben. Ändert sich der Status von UP zu DOWN oder zu NOT_AVAILABLE, wird eine Warnmeldung generiert. Beispiel:

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

Ändert sich der Status von DOWN oder NOT_AVAILABLE zu UP, wird der Warnmeldung vergleichbare INFO-Meldung generiert. Beispiel:

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

Wenn beim Steuerungskomponentenkanal ein Kommunikationsfehler auftritt, wird ein Systemereignis mit einer der folgenden im Detail aufgeführten Fehlerursachen generiert:

- 1255601: Unvollständiges Hostzertifikat
- 1255602: Unvollständiges Controller-Zertifikat
- 1255603: SSL-Handshake-Fehler

- 1255604: Verbindung abgelehnt
- 1255605: Keep-alive-Zeitüberschreitung
- 1255606: SSL-Ausnahme
- 1255607: Ungültige Meldung
- 1255620: Unbekannter Fehler

Von NSX Manager werden außerdem Taktsignalnachrichten für Hosts erstellt. Eine vollständige Konfigurationssynchronisierung wird ausgelöst, wenn das Taktsignal zwischen dem NSX Manager und netcpa abbricht.

Weitere Informationen zum Anzeigen von Warnungen finden Sie im *Administratorhandbuch für NSX*.

Installationsstatus ist „Nicht bereit“

Bei der Hostvorbereitung bemerken Sie möglicherweise, dass der Cluster-Status als `Nicht bereit` angezeigt wird.

Problem

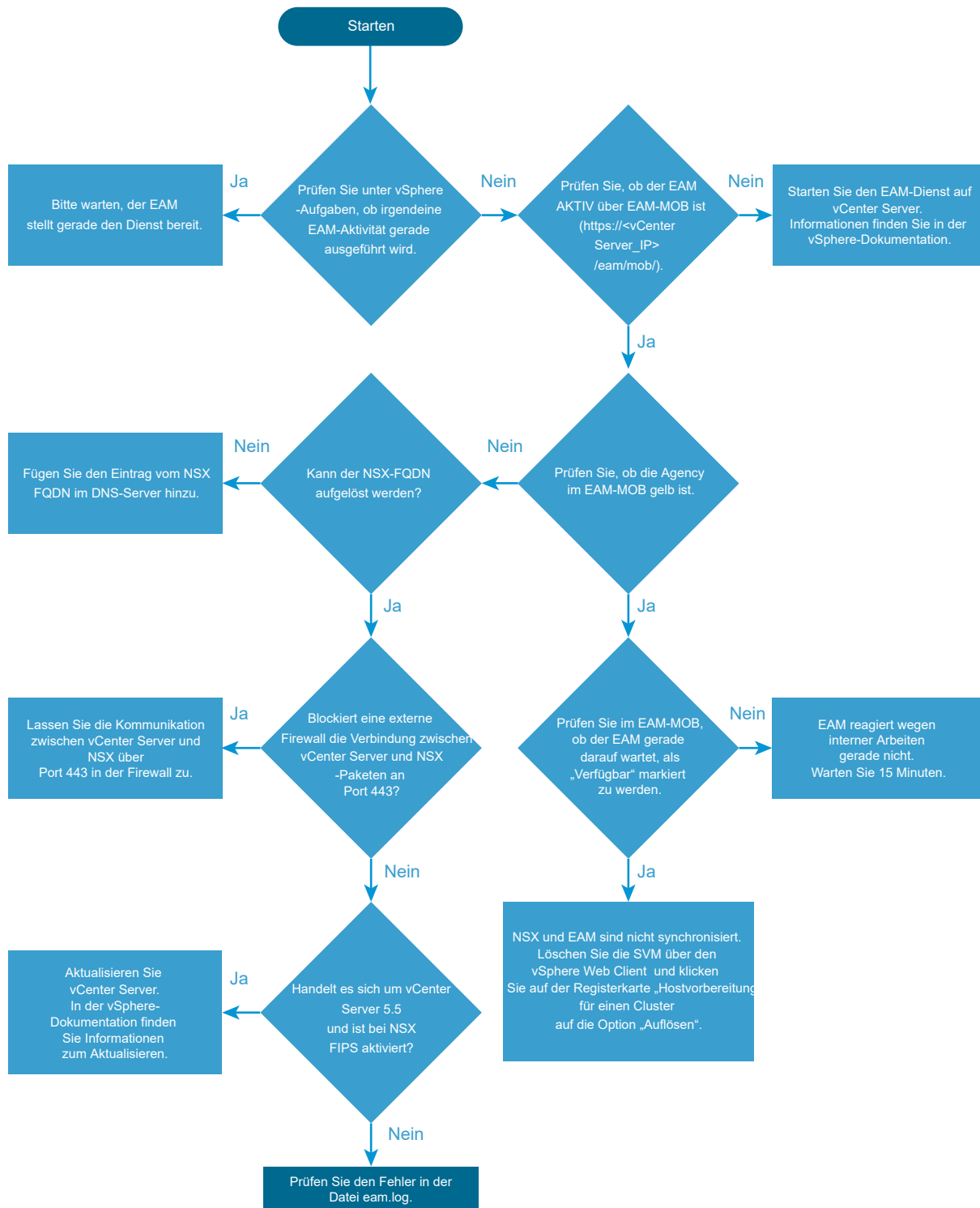
Auf der Registerkarte **Hostvorbereitung (Host Preparation)** oder **Dienstbereitstellung (Service Deployment)** wird der Installationsstatus als `Nicht bereit` angezeigt.

Lösung

- 1 Wechseln Sie zur Registerkarte **Networking & Security (Networking & Security) > Installation > Hostvorbereitung (Host Preparation)** oder **Dienstbereitstellung (Service Deployment)**.
- 2 Klicken Sie auf den Clustern und Hosts auf `Nicht bereit`.
Die Fehlermeldung wird angezeigt.
- 3 Klicken Sie auf die Option **Auflösen (Resolve)**.
Eine Liste aller Probleme, die mit der Option **Auflösen (Resolve)** behoben wurden, finden Sie unter *NSX-Protokollierung und -Systemereignisse*.
- 4 Wenn nach wie vor als Status `Nicht bereit` angezeigt wird und der Fehler noch nicht behoben wurde, finden Sie weitere Informationen unter [Problem mit der Option „Auflösen“ nicht behoben](#).

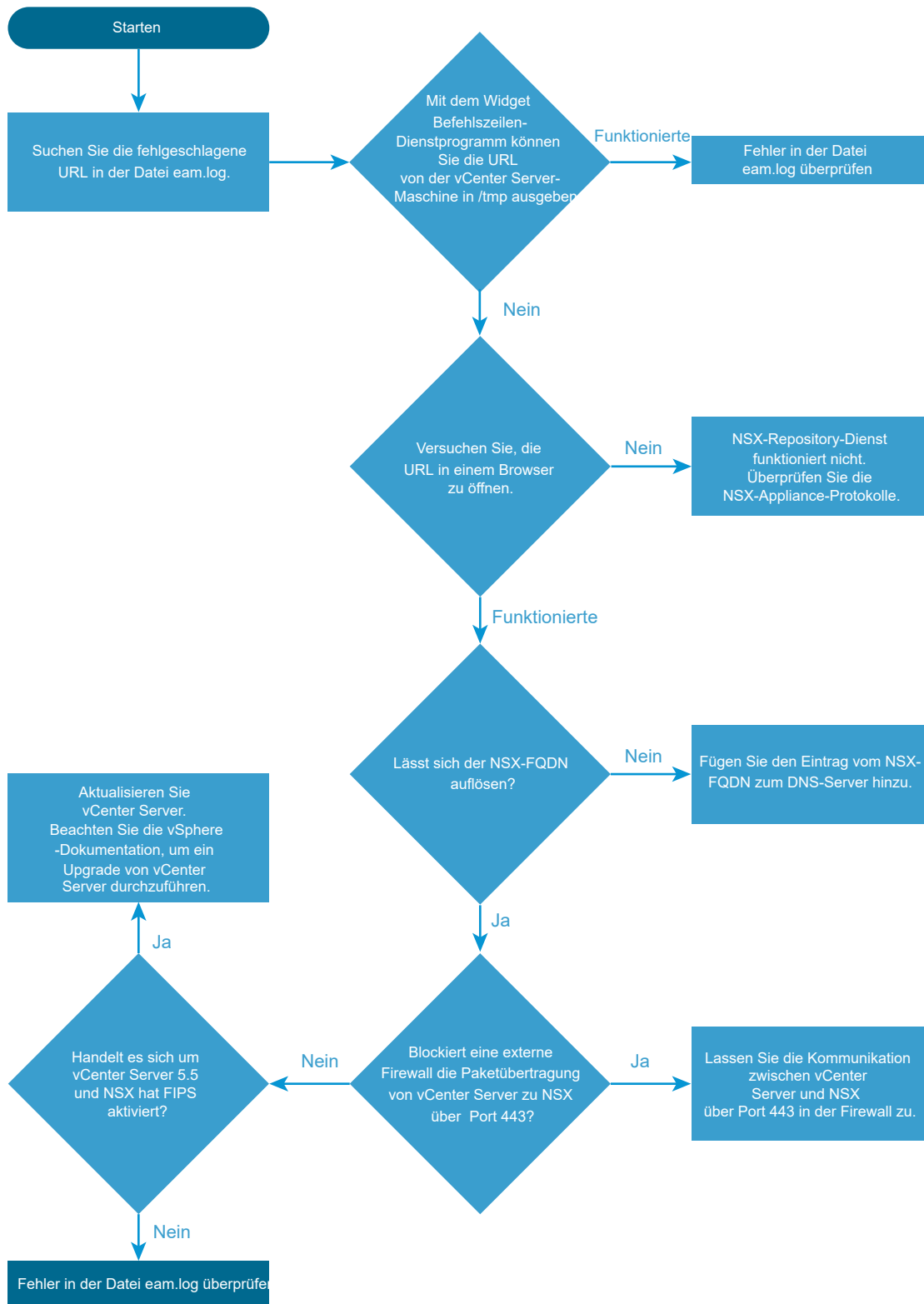
Dienst reagiert nicht

Das Flussdiagramm bietet einen Überblick über den NSX-Hostvorbereitungsvorgang. Außerdem zeigt es, was Sie tun können, wenn der Dienst lange Zeit nicht reagiert oder wenn lange Zeit das sich drehende Symbol angezeigt wird.



Dienstbereitstellung scheitert mit Fehlermeldung zu nicht verfügbarem OVF/VIB

Das Flussdiagramm zeigt, was Sie tun können, wenn die Dienstbereitstellung mit einer Fehlermeldung zu nicht verfügbarem OVF/VIB (OVF/VIB not accessible) scheitert.



Problem mit der Option „Auflösen“ nicht behoben

Auf der Registerkarte **Networking & Security (Networking & Security) > Installation > Hostvorbereitung (Host Preparation)** oder **Dienstbereitstellung (Service Deployment)** wird der Installationsstatus als **Nicht bereit** auf den Clustern und Hosts angezeigt. Durch Klicken auf die Option **Auflösen (Resolve)** lässt sich das Problem nicht beheben.

Problem

- Nach Anklicken des Links **Nicht bereit** wird als Fehlermeldung VIB-Modul für den Agenten ist nicht auf dem Host installiert angezeigt.
- Der ESXi-Host kann über vCenter Server nicht auf VIBs zugreifen.
- Beim Ändern von vShield Endpoint auf NSX Manager wird möglicherweise als Status **Fehlgeschlagen** angezeigt.

Lösung

- 1 Stellen Sie sicher, dass die DNS-Konfiguration auf den vCenter Server ESXi-Hosts und auf NSX Manager korrekt ist. Stellen Sie sicher, dass die Vorwärts- und Rückwärts-DNS-Auflösung von den vCenter Server ESXi-Hosts, von NSX Manager und von vSphere Update Manager funktioniert.
- 2 Um zu ermitteln, ob ein DNS-Problem vorliegt, überprüfen Sie die *esxupdate* -Protokolle und suchen Sie nach der Meldung *esxupdate: ERROR: MetadataDownloadError:IOError: <url>open error [Errno -2] Name= or service not known* in der Datei *esxupdate.log*.

Diese Meldung weist darauf hin, dass der ESXi-Host nicht auf den vollständig qualifizierten Domännennamen (FQDN) von vCenter Server zugreifen kann. Weitere Informationen finden Sie unter [Überprüfen der verwalteten IP-Adresse von VMware vCenter Server \(1008030\)](#).

- 3 Stellen Sie sicher, dass das Network Time Protocol (NTP) korrekt konfiguriert ist. VMware empfiehlt die NTP-Konfiguration. Um festzustellen, ob NTP-Synchronisationsprobleme Ihre Umgebung beeinträchtigen, überprüfen Sie die Datei */etc/ntp.drift* in den NSX Manager-Support-Paketen mit Version 6.2.4 und höher.
- 4 Stellen Sie sicher, dass alle für NSX for vSphere 6.x erforderlichen Ports nicht durch eine Firewall blockiert werden. Weitere Informationen finden Sie unter:
 - [Netzwerk-Portanforderungen für VMware NSX for vSphere \(2079386\)](#).
 - [Für den Zugriff auf VMware vCenter Server, VMware ESXi- und ESX-Hosts und andere Netzwerkkomponenten erforderlichen TCP- und UDP-Ports \(1012382\)](#).

Hinweis VMware vSphere 6.x unterstützt VIB-Downloads über Port 443 (statt Port 80). Dieser Port wird dynamisch geöffnet und geschlossen. Die Zwischengeräte zwischen den ESXi-Hosts und vCenter Server müssen Datenverkehr über diesen Port zulassen.

- 5 Stellen Sie sicher, dass die verwaltete IP-Adresse von vCenter Server korrekt konfiguriert ist. Weitere Informationen finden Sie unter [Überprüfen der verwalteten IP-Adresse von VMware vCenter Server \(1008030\)](#).

- 6 Stellen Sie sicher, dass der vSphere Update Manager ordnungsgemäß funktioniert. Ab vCenter Server 6.0U3 nutzen die Installations- und Upgrade-Vorgänge von NSX nicht mehr vSphere Update Manager mit ESX Agent Manager. VMware empfiehlt dringend, mindestens vCenter Server 6.0U3 oder höher auszuführen. Wenn kein Upgrade möglich ist, stellen Sie sicher, dass der vSphere Update Manager-Dienst ausgeführt wird. Sie können die Umgehungsoption für vSphere Update Manager konfigurieren, wie unter [KB 2053782](#) beschrieben.
- 7 Wenn Sie während der Bereitstellung von vCenter Server nicht standardmäßige Ports festlegen, stellen Sie sicher, dass diese Ports nicht durch die ESXi-Host-Firewall blockiert werden.
- 8 Stellen Sie sicher, dass der *vpxd*-Prozess von vCenter Server den TCP-Port 8089 abhört. NSX Manager unterstützt nur den Standardport 8089.

Über vSphere ESX Agent Manager (EAM)

vSphere ESX Agent Manager automatisiert die Bereitstellung und Verwaltung von Netzwerk- und Sicherheitsdiensten von NSX und erweitert die Funktion eines ESXi-Hosts durch die Bereitstellung zusätzlicher Dienste, die für eine vSphere-Lösung erforderlich sind.

Protokolle und Dienste von ESX Agent Manager

ESX Agent Manager-Protokolle werden in das vCenter-Protokollpaket aufgenommen.

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

Überwachen von ESX Agent Manager

Wichtig Stellen Sie sicher, dass das *bypassVumEnabled*-Flag auf **Wahr** gesetzt ist, bevor Sie mit der NSX-Installation beginnen, und ändern Sie es nach der Installation wieder in **Falsch**. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2053782>.

So prüfen Sie den Status von ESX Agent Manager:

- 1 Navigieren Sie zu vSphere Web Client.
- 2 Klicken Sie auf **Verwaltung > vCenter Server-Erweiterungen (Administration > vCenter Server Extensions)** und dann auf den vSphere ESX Agent Manager.

- a Klicken Sie auf die Registerkarte **Verwalten (Manage)**.

Die Registerkarte **Verwalten (Manage)** enthält Informationen über aktuell ausgeführte Agencys, verwaiste ESX-Agenten und über die ESX-Agenten, die von ESX Agent Manager verwaltet werden.

Weitere Informationen zu Agenten und Agencys finden Sie in der vSphere-Dokumentation.

- b Klicken Sie auf die Registerkarte **Überwachen (Monitor)**.

Auf der Registerkarte **Überwachen (Monitor) > Ereignisse (Events)** werden Informationen zu Ereignissen angezeigt, die ESX Agent Manager zugeordnet sind.

Fehlerbehebung bei NSX Manager-Problemen

Überprüfen Sie, ob die einzelnen Fehlerbehebungsschritte für Ihre Umgebung gelten. Jeder Schritt enthält Anleitungen, mit denen Sie mögliche Ursachen beseitigen und bei Bedarf Korrekturen vornehmen können. Die Schritte werden in der für die Isolierung des Problems und für die Ermittlung der entsprechenden Lösung am geeignetsten erscheinenden Reihenfolge aufgeführt. Sie müssen alle Schritte durchführen.

Problem

- Die Installation von VMware NSX Manager scheitert.
- Das Upgrade von VMware NSX Manager scheitert.
- Die Anmeldung bei VMware NSX Manager scheitert.
- Der Zugriff auf VMware NSX Manager scheitert.

Lösung

- 1 Überprüfen Sie die *NSX-Versionshinweise* zu aktuellen Versionen daraufhin, ob das Problem bereits behoben ist.
- 2 Stellen Sie bei der Installation von VMware NSX Manager sicher, dass die Mindestsystemanforderungen erfüllt sind.
Weitere Informationen finden Sie unter *Installationshandbuch für NSX*.
- 3 Vergewissern Sie sich, dass alle erforderlichen Ports in NSX Manager geöffnet sind.
Weitere Informationen finden Sie unter *Installationshandbuch für NSX*.
- 4 Installationsprobleme:
 - Wenn die Konfiguration von Lookup Service oder vCenter Server scheitert, überprüfen Sie, ob die Uhrzeitangaben von NSX Manager und Lookup Service synchron sind. Verwenden Sie für NSX Manager und Lookup Service die gleiche NTP-Serverkonfiguration. Stellen Sie außerdem sicher, dass DNS ordnungsgemäß konfiguriert ist.
 - Stellen Sie sicher, dass die OVA-Datei korrekt installiert wurde. Wenn eine NSX-OVA-Datei nicht installiert werden kann, wird in einem Fehlerfenster auf dem vSphere-Client angegeben, wo der Fehler aufgetreten ist. Überprüfen Sie auch die MD5-Prüfsumme der heruntergeladenen OVA/OVF-Datei.
 - Stellen Sie sicher, dass die Uhrzeit auf den ESXi-Hosts mit der Uhrzeit von NSX Manager übereinstimmt.
 - VMware empfiehlt, eine Sicherung der NSX Manager-Daten sofort nach der Installation von NSX Manager zu planen.

5 Upgrade-Probleme:

- Lesen Sie vor einem Upgrade die Informationen auf der Seite der Interoperabilitätsmatrix für VMware-Produkte durch.
- VMware empfiehlt, vor dem Upgrade die aktuelle Konfiguration zu sichern und Tech-Support-Protokolle herunterzuladen.
- Nach dem Upgrade von NSX Manager muss unter Umständen eine erneute Synchronisierung mit dem vCenter Server erzwungen werden. Dazu melden Sie sich bei der grafischen Web-Benutzeroberfläche für NSX Manager an. Anschließend wechseln Sie zu **vCenter-Registrierung verwalten > NSX Management Service > Bearbeiten (Manage vCenter Registration > NSX Management Service > Edit)** und geben Sie das Kennwort für den administrativen Benutzer erneut ein.

6 Leistungsprobleme:

- Stellen Sie sicher, dass die Mindestanforderungen für die vCPU erfüllt sind.
- Stellen Sie sicher, dass die Stammpartition (/) über ausreichend Speicherplatz verfügt. Sie können dies überprüfen, indem Sie sich beim ESXi-Host anmelden und den Befehl `df -h` eingeben.

Beispiel:

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

- Überprüfen Sie mit dem Befehl `esxtop`, welche Prozesse sehr viel Kapazität von CPU und Arbeitsspeicher in Anspruch nehmen.
- Wenn in den Protokollen von NSX Manager Fehler wegen unzureichender Speicherkapazität auftreten, überprüfen Sie, ob die Datei `/common/dumps/java.hprof` vorhanden ist. Wenn die Datei vorhanden ist, erstellen Sie eine Kopie dieser Datei und nehmen Sie diese Kopie in das NSX-Tech-Support-Protokollpaket auf.
- Überzeugen Sie sich davon, dass in der Umgebung keine Probleme mit der Speicherlatenz vorliegen.
- Versuchen Sie, NSX Manager auf einen anderen ESXi-Host zu migrieren.

7 Konnektivitätsprobleme:

- Wenn in NSX Manager Verbindungsprobleme mit vCenter Server oder mit dem ESXi-Host auftreten, melden Sie sich bei der NSX Manager-Befehlszeilenschnittstellenkonsole (CLI) an und führen Sie den Befehl `debug connection IP_of_ESXi_or_VC` aus. Überprüfen Sie die Ausgabe.

- Stellen Sie sicher, dass die Virtual Center-Web-Verwaltungsdienste ausgeführt werden und der Browser keinen Fehlerstatus aufweist.
- Wenn die Web-Benutzeroberfläche von NSX Manager nicht aktualisiert wird, können Sie versuchen, das Problem durch Deaktivierung und erneute Aktivierung der Webdienste zu beheben. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2126701>.
- Überprüfen Sie, welche Portgruppe und welche Uplink-NIC von NSX Manager verwendet werden, indem Sie auf dem ESXi-Host den Befehl `esxtop` ausführen. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/1003893>.
- Versuchen Sie, NSX Manager auf einen anderen ESXi-Host zu migrieren.
- Überprüfen Sie die Registerkarte **Aufgaben und Ereignisse (Tasks and Events)** der NSX Manager-VM-Appliance vom vSphere Web Client aus auf der Registerkarte **Überwachen (Monitor)**.
- Wenn für NSX Manager Konnektivitätsprobleme mit vCenter Server auftreten, versuchen Sie, NSX Manager auf den ESXi-Host zu migrieren, auf dem die virtuelle vCenter Server-Maschine ausgeführt wird, um möglicherweise zugrunde liegende physische Netzwerkprobleme zu beheben.

Beachten Sie, dass dies nur möglich ist, wenn sich beide virtuellen Maschinen im selben VLAN bzw. in derselben Portgruppe befinden.

Verbinden von NSX Manager mit vCenter Server

Wenn eine Verbindung zwischen NSX Manager und dem vCenter Server hergestellt ist, kann NSX Manager mithilfe der vSphere API bestimmte Funktionen ausführen, z. B. Dienst-VMs bereitstellen, Hosts vorbereiten und Portgruppen logischer Switches erstellen. Der Verbindungsvorgang installiert ein Web Client-Plug-In für NSX auf dem Web Client Server.

Damit die Verbindung funktioniert, müssen DNS und NTP auf NSX Manager, vCenter Server und auf den ESXi-Hosts konfiguriert sein. Wenn Sie der vSphere-Bestandsliste ESXi-Hosts anhand von Namen hinzugefügt haben, stellen Sie sicher, dass auf NSX Manager DNS-Server konfiguriert wurden und die Namensauflösung funktioniert. Andernfalls kann NSX Manager die IP-Adressen nicht auflösen. Der NTP-Server muss angegeben werden, um sicherzustellen, dass die Zeit des SSO-Servers und die Zeit von NSX Manager synchron sind. Auf NSX Manager ist die Drift-Datei unter `/etc/ntp.drift` im Tech-Support-Paket für den NSX Manager enthalten.

Das Konto, das Sie zur Verbindung von NSX Manager mit vCenter Server verwenden, muss die vCenter-Rolle „Administrator“ besitzen. Die Rolle „Administrator“ ermöglicht es NSX Manager, sich selbst am Sicherheitstoken-Dienstserver zu registrieren. Durch Verwendung eines bestimmten Benutzerkontos für die Verbindung von NSX Manager mit vCenter wird auf NSX Manager auch die Rolle „Enterprise-Administrator“ für den Benutzer erstellt.

Allgemeine Probleme beim Herstellen einer Verbindung von NSX Manager mit vCenter Server

- Falsch konfiguriertes DNS auf NSX Manager, vCenter Server oder einem ESXi-Host.

- Falsch konfiguriertes NTP auf NSX Manager, vCenter Server oder einem ESXi-Host.
- Ein Benutzerkonto ohne die vCenter-Rolle „Administrator“ wurde zur Verbindung von NSX Manager mit vCenter verwendet.
- Probleme mit der Netzwerkkonnektivität zwischen NSX Manager und vCenter Server.
- Benutzeranmeldung bei vCenter mit einem Konto ohne Rolle in NSX Manager.

Sie müssen sich zu Anfang bei vCenter mit dem Konto anmelden, das Sie für die Herstellung einer Verbindung von NSX Manager mit vCenter Server verwendet haben. Dann können Sie mit **Home > Netzwerk und Sicherheit > NSX Manager > {IP von NSX Manager} > Verwalten > Benutzer (Home > Networking & Security > NSX Managers > {IP of NSX Manager} > Manage > Users)** weitere Benutzer mit Rollen in NSX Manager erstellen.

Die erste Anmeldung kann bis zu vier Minuten dauern, da vCenter die NSX Benutzeroberflächenpakete lädt und bereitstellt.

Prüfen der Konnektivität von NSX Manager mit vCenter Server

- Melden Sie sich bei der CLI-Konsole von NSX Manager an.
- Sehen Sie sich die ARP- und Routing-Tabellen an, um die Konnektivität zu überprüfen.

```
nsxmgr# show arp
```

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

```
nsxmgr# show ip route
Codes: K - kernel route, C - connected, S - static,
       > - selected route, * - FIB route
```

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

- Suchen Sie im Protokoll von NSX Manager nach Fehlern, um die Ursache für eine fehlgeschlagene Verbindung mit vCenter Server zu finden. Sie können das Protokoll mit dem Befehl `show log manager follow` anzeigen.


```

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

```

- Führen Sie den Befehl `debug connection IP_of_ESXi_or_VC` aus und überprüfen Sie die Ausgabe.

Durchführen einer Paketerfassung in NSX Manager zur Anzeige der Verbindungen

Verwenden Sie den Debugpaketbefehl: `debug packet [capture|display] interface interface filter`

Der Schnittstellenname in NSX Manager lautet `mgmt`.

Die Filtersyntax folgt dieser Form: „`port_80_or_port_443`“

Der Befehl lässt sich nur im privilegierten Modus ausführen. Sie rufen den privilegierten Modus mit dem Befehl `enable` und mit der Eingabe des Administratorkennworts auf.

Beispiel für die Paketerfassung:

```

nsxmgr# en
nsxmgr# debug packet display interface mgmt port_80_or_port_443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on mgmt, link-type EN10MB (Ethernet), capture size 262144 bytes
23:40:25.321085 IP 192.168.210.15.54688 > 192.168.210.22.443: Flags [P.], seq 2645022162:2645022199,
ack 2668322748, win 244, options [nop,nop,TS val 1447550948 ecr 365097421], length 37
...

```

Prüfen der Netzwerkkonfiguration in NSX Manager

Der Befehl `show running-config` zeigt die grundlegende Konfiguration der Verwaltungsschnittstelle, das NTP und die Standardeinstellungen für Routen an.

```

nsxmgr# show running-config
Building configuration...

Current configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr
!
interface mgmt
ip address 192.168.110.15/24

```

```
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

NSX Manager-Zertifikate

NSX Manager unterstützt zwei Möglichkeiten zum Generieren von Zertifikaten.

- NSX Manager-generierter CSR: Beschränkte Funktionalität aufgrund des Basis-CSR
- PKCS#12: Empfohlen für die Produktion

Es gibt ein bekanntes Problem, bei dem das CMS bei API-Aufrufen unbemerkt fehlschlägt.

Dieses tritt auf, wenn der Zertifikataussteller dem Aufrufer nicht bekannt ist, weil es sich um eine nicht vertrauenswürdige Stammzertifizierungsstelle handelt oder das Zertifikat selbstsigniert ist. Um dieses Problem zu beheben, navigieren Sie in einem Browser zur IP-Adresse oder zum Hostnamen von NSX Manager und akzeptieren Sie das Zertifikat.

Sekundärer NSX Manager hängt im Übergangsmodus fest

Befolgen Sie nachfolgenden Lösungsansatz, wenn der sekundäre NSX Manager im Übergangsmodus festhängt, wie in der Problembeschreibung dargestellt. Dieses Problem tritt auf, wenn Sie das Backup auf dem primären NSX Manager wiederherstellen, während sich der sekundäre NSX Manager im Übergangsmodus befindet.

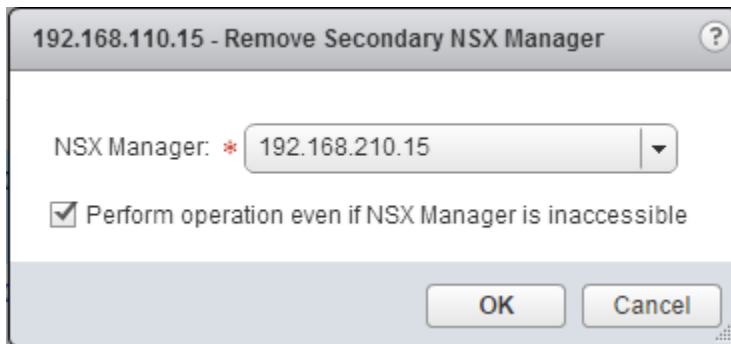
Problem

- 1 Sie haben primäre und sekundäre NSX Manager konfiguriert.
- 2 Sie verwenden das Backup des primären NSX Manager.
- 3 Später entfernen Sie den sekundären NSX Manager. Der sekundäre NSX Manager befindet sich im Übergangsmodus.
- 4 Nun stellen Sie, aus welchen Gründen auch immer, das Backup auf dem primären NSX Manager wieder her.
- 5 In der Datenbank wird der Übergangs-NSX Manager als **Sekundär (Secondary)** aktualisiert, in der Benutzeroberfläche wird er allerdings als **Übergangs- (Transit)** angezeigt und die Synchronisierung schlägt fehl.
- 6 Möglicherweise ist es nicht möglich, den sekundären NSX Manager zu entfernen oder wieder als sekundär einzustellen.
- 7 Beim Versuch, den Übergangs-NSX Manager als sekundär einzustellen, wird die Fehlermeldung NSX Manager-Knoten mit dieser IP-Adresse/diesem Hostnamen bereits vorhanden angezeigt.
- 8 Beim Entfernen des Übergangs-NSX Manager wird die Fehlermeldung Benutzername oder Kennwort ungültig angezeigt.

Lösung

- 1 Melden Sie sich beim vCenter, das mit dem primären NSX Manager verknüpft ist, über den vSphere Web Client an.
- 2 Navigieren Sie zu **Home > Networking & Security> Installation** und klicken Sie auf die Registerkarte **Management**.
- 3 Wählen Sie den sekundären NSX Manager aus, den Sie entfernen möchten, und klicken Sie auf **Aktionen (Actions)** und anschließend auf **Sekundären NSX Manager entfernen (Remove Secondary NSX Manager)**.

Ein Dialogfeld zur Bestätigung wird geöffnet.



- 4 Aktivieren Sie das Kästchen **Vorgang ausführen, auch wenn der Zugriff auf NSX Manager nicht möglich ist (Perform operation even if NSX Manager is inaccessible)**.
- 5 Klicken Sie auf **OK**.

Der sekundäre NSX Manager wird aus der primären Datenbank gelöscht.

- 6 Fügen Sie den sekundären NSX Manager erneut hinzu.

Nächste Schritte

Weitere Informationen zum Hinzufügen des sekundären NSX Manager finden Sie unter *Installationshandbuch für NSX*.

Fehlschlagen der Konfiguration des NSX SSO Lookup Service

Problem

- Registrierung von NSX Manager bei vCenter Server schlägt fehl
- Konfiguration des SSO Lookup Service schlägt fehl
- Es werden möglicherweise folgende Fehler angezeigt:

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

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

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

Lösung

1 Konnektivitätsprobleme:

- Wenn in NSX Manager Verbindungsprobleme mit vCenter Server oder mit dem ESXi-Host auftreten, melden Sie sich bei der NSX Manager-Befehlszeilenschnittstellenkonsole (CLI) an und führen Sie den Befehl `debug connection IP_of_ESXi_or_VC` aus. Überprüfen Sie die Ausgabe.
- Pingen Sie mit der IP-Adresse und dem FQDN von NSX Manager zu vCenter Server, um das Routing oder die statische bzw. die Standardroute in NSX Manager mithilfe des folgenden Befehls zu prüfen:

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

Codes:

K – Kernel-Route,

C – Verbunden,

S – Statisch

> – Ausgewählte Route

* – FIB-Route

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

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

2 DNS-Problem

Pingen Sie mit dem FQDN von NSX Manager zu vCenter Server mithilfe des folgenden Befehls:

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

Es muss dann eine Ausgabe in der folgenden Art angezeigt werden:

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

Wenn dies nicht möglich ist, stellen Sie mit **Verwalten > Netzwerk > DNS-Server (Manage > Network > DNS Servers)** in NSX Manager sicher, dass DNS ordnungsgemäß konfiguriert ist.

3 Firewallproblem

Wenn eine Firewall zwischen NSX Manager und vCenter Server vorhanden ist, stellen Sie sicher, dass SSL auf TCP/443 zulässig ist. Pingen Sie außerdem für die Überprüfung der Konnektivität.

- 4 Vergewissern Sie sich, dass die im Folgenden aufgeführten erforderlichen Ports in NSX Manager geöffnet sind.

Tabelle 2-1. Erforderliche Ports in NSX Manager

Port	Erforderlich für
443/TCP	Herunterladen der OVA-Datei auf den ESXi-Host für die Bereitstellung Mithilfe von REST-APIs Mithilfe der NSX Manager-Benutzeroberfläche
80/TCP	Initiierung der Verbindung mit dem vSphere SDK Messaging zwischen NSX Manager und NSX-Host-Modulen
1234/TCP	Kommunikation zwischen NSX Controller und NSX Manager
5671	Rabbit MQ (Nachrichtenbustechnologie)
22/TCP	Konsolenzugriff (SSH) auf die Befehlszeilenschnittstelle (CLI) Hinweis: Standardmäßig ist dieser Port geschlossen.

5 NTP-Probleme

Stellen Sie sicher, dass die Uhrzeit zwischen vCenter Server und NSX Manager synchronisiert ist. Verwenden Sie zu diesem Zweck identische NTP-Serverkonfigurationen auf NSX Manager und vCenter Server.

Um die Uhrzeit auf NSX Manager zu bestimmen, führen Sie diesen Befehl von der Befehlszeilenschnittstelle (CLI) aus:

```
nsxmgr-l-01a# show clock
Tue Nov 18 06:51:34 UTC 2014
```

Um die Uhrzeit auf vCenter Server zu bestimmen, führen Sie diesen Befehl von der Befehlszeilenschnittstelle (CLI) aus:

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

Es muss dann eine Ausgabe in der folgenden Art angezeigt werden:

```
Tue Nov 18 06:51:31 UTC 2014
```

Hinweis: Starten Sie nach der Konfiguration der Uhrzeiteinstellungen die Appliance erneut.

6 Probleme mit Benutzerberechtigungen

Bestätigen Sie, dass der Benutzer **Admin**-Rechte hat.

Um sich bei vCenter Server oder SSO Lookup Service registrieren zu können, müssen Sie über Administratorrechte verfügen.

Das Standardkonto lautet `administrator` user: `administrator@vsphere.local`.

- 7 Stellen Sie durch Eingabe der Anmeldedaten erneut eine Verbindung mit SSO her.

Vorbereitung des logischen Netzwerks: VXLAN-Transport

NSX bereitet den vSphere Distributed Switch vor, den Sie für VXLAN auswählen, indem eine verteilte virtuelle Portgruppe für die VTEP-VMkernel-NICs erstellt wird.

Die Gruppierungsrichtlinie, die Load-Balancing-Methode, die MTU und die VLAN-ID der VTEPs werden bei der VXLAN-Konfiguration ausgewählt. Die Teaming- und Load-Balancing-Methoden müssen mit der Konfiguration des für VXLAN ausgewählten DVS übereinstimmen.

Für die MTU muss mindestens der Wert 1600 festgelegt werden. Er darf außerdem nicht kleiner sein, als der bereits auf dem DVS konfigurierte Wert.

Wie viele VTEPs erstellt werden, hängt von der ausgewählten Gruppierungsrichtlinie und der DVS-Konfiguration ab.

Allgemeine Probleme bei der VXLAN-Vorbereitung

Die VXLAN-Vorbereitung kann aus verschiedenen Gründen fehlschlagen:

- Die für das VXLAN gewählte Gruppierungsmethode wird vom DVS nicht unterstützt. Informationen zu unterstützten Methoden finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign für VMware NSX for vSphere* unter <https://communities.vmware.com/docs/DOC-27683>.
- Für die VTEPs ist eine falsche VLAN-ID ausgewählt.
- Für die Zuweisung der VTEP-IP-Adressen wurde DHCP ausgewählt, jedoch ist kein DHCP-Server verfügbar.
- Eine VMkernel-NIC fehlt. Beheben Sie den Fehler, wie unter [VXLAN-VMkernel-NIC ist nicht synchron](#) beschrieben.
- Eine VMkernel-NIC verfügt über eine ungültige IP-Adresse. Beheben Sie den Fehler, wie unter <https://kb.vmware.com/kb/2137025> beschrieben.
- Für die VTEPs wurde eine falsche MTU-Einstellung ausgewählt. Sie sollten überprüfen, ob eine MTU-Nichtübereinstimmung vorliegt (wie weiter unten in diesem Abschnitt beschrieben).
- Ein falsches VXLAN-Gateway ist ausgewählt. Sie sollten überprüfen, ob bei der Konfiguration des VXLAN-Gateways ein Fehler vorliegt (wie weiter unten in diesem Abschnitt beschrieben).

Wichtige Portnummern

Der VXLAN-UDP-Port wird für die UDP-Kapselung verwendet. Vor NSX 6.2.3, war die standardmäßige VXLAN-Portnummer 8472. Bei NSX 6.2.3 wurde die standardmäßige VXLAN-Portnummer für neue Installationen in 4789 geändert. Bei NSX 6.2 und neueren Installationen, die ein Hardware-VTEP nutzen, müssen Sie die VXLAN-Portnummer 4789 verwenden. Informationen zum Ändern der VXLAN-Portkonfiguration finden Sie unter „VXLAN-Port ändern“ in *Administratorhandbuch für NSX*.

Für den Status der Steuerungskomponente wird *Deaktiviert* angezeigt, wenn der Host über keine aktiven VMs verfügt, für die eine Controller-Verbindung notwendig ist.

Mit den `show logical-switch`-Befehlen können Sie VXLAN-Details auf dem Host anzeigen. Genauere Informationen finden Sie unter *Befehlszeilenschnittstellen-Referenz zu NSX*.

Der Befehl `show logical-switch host hostID verbose` gibt den Status der Steuerungskomponente als *Deaktiviert* aus, wenn der Host keine VMs enthält, die eine Verbindung mit dem Controller-Cluster zur Weiterleitung von Tabelleninformationen erfordern.

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

Fehler beim Konfigurieren eines VXLAN-Gateways

Wenn VXLAN mithilfe eines statischen IP-Pools unter **Networking & Security > Installation > Hostvorbereitung > VXLAN konfigurieren (Networking & Security > Installation > Host Preparation > Configure VXLAN)** konfiguriert wird und die Konfiguration keinen IP-Pool-Gateway auf VTEP festlegen kann, ändert sich der VXLAN-Konfigurationsstatus für diesen Hostcluster in den Fehlerzustand (ROT). Die Fehlermeldung lautet „VXLAN-Gateway kann auf Host nicht festgelegt werden“ und der Fehlerstatus ist „VXLAN_GATEWAY_SETUP_FAILURE“.

Im REST-API-Aufruf `GET https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>` lautet der Status von VXLAN wie folgt:

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

Problemumgehung: Es gibt zwei Möglichkeiten, den Fehler zu beheben.

- Option 1: Entfernen Sie die VXLAN-Konfiguration für den Hostcluster, beheben Sie das Problem des zugrunde liegenden Gateway-Setups im IP-Pool, indem Sie sicherstellen, dass das Gateway ordnungsgemäß konfiguriert ist, und konfigurieren Sie anschließend VXLAN für den Hostcluster neu.

- Option 2: Führen Sie die nachfolgend aufgeführten Schritte aus.
 - a Korrigieren Sie das zugrunde liegende Gateway-Setup im IP-Pool, indem Sie sicherstellen, dass das Gateway ordnungsgemäß konfiguriert und erreichbar ist.
 - b Versetzen Sie den Host (oder Hosts) in den Wartungsmodus, um sicherzustellen, dass auf dem Host kein VM-Datenverkehr aktiv ist.
 - c Löschen Sie die VXLAN VTEPs aus dem Host.
 - d Deaktivieren Sie den Wartungsmodus für den Host. Durch das Beenden des Wartungsmodus für den Host wird der VXLAN VTEP-Erstellungsvorgang auf NSX Manager ausgelöst. NSX Manager versucht, die erforderlichen VTEPs auf dem Host erneut zu erstellen.

Überprüfen einer MTU-Nichtübereinstimmung

- Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die MTU für 1600 oder höher konfiguriert ist:

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

Dabei ist *vmkx* die ID Ihres VMkernel-Ports und *hostname_or_IP* ist die IP oder der Hostname des VMkernel-Ports.

So können Sie die Gültigkeit aller Uplinks überprüfen. Wenn Sie in einer Multi-VTEP-Umgebung arbeiten, können Sie alle Uplinks validieren, indem Sie den Ping-Befehl von jeder möglichen VTEP-VMkernel-Quelle/Ziel-Schnittstelle ausführen, um alle Pfade zu validieren.

- Überprüfen Sie die physische Infrastruktur. Häufig wird das Problem durch eine Konfigurationsänderung an der physischen Infrastruktur behoben.
- Ermitteln Sie, ob das Problem auf einen einzelnen logischen Switch beschränkt ist oder ob auch andere logische Switches betroffen sind. Überprüfen Sie, ob alle logischen Switches von dem Problem betroffen sind.

Weitere Informationen zur MTU-Überprüfung finden Sie im Dokument *Upgrade-Handbuch für NSX* unter „Überprüfen des NSX-Arbeitszustands“.

VXLAN-VMkernel-NIC ist nicht synchron

Wenn die VMkernel-NIC auf dem Host entfernt wird, aber die VMkernel-NIC-Informationen noch in NSX verfügbar sind, zeigt NSX Manager die entfernte VMkernel-NIC mit einem **Fehler (Error)**-Symbol an.

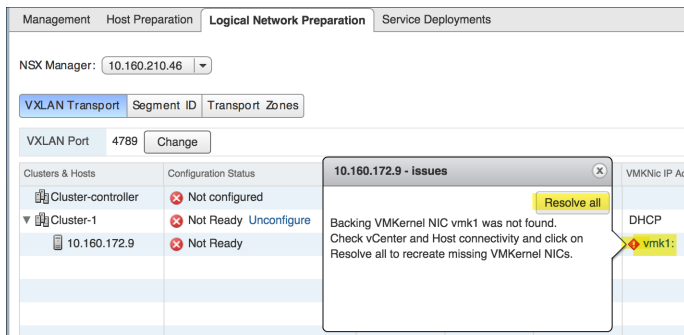
Voraussetzungen

VMkernel-NIC ist auf dem Host gelöscht.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation)**.

- 2 Blenden Sie auf der Registerkarte **VXLAN-Transport (VXLAN Transport)** die Cluster und Hosts ein.



- 3 Klicken Sie auf das **Fehler (Error)**-Symbol, um die Informationen zu der VMkernel-NIC anzuzeigen, die auf dem Host gelöscht wurde.
- 4 Klicken Sie auf die Schaltfläche **Alle auflösen (Resolve All)**, um die gelöschte VMkernel-NIC auf dem Host erneut zu erstellen.

Ergebnisse

Die gelöschte VMkernel-NIC wird auf dem Host erneut erstellt.

Ändern der VXLAN-Gruppierungsrichtlinie und der MTU-Einstellungen

Die VXLAN-Gruppierungsrichtlinie und die MTU-Einstellungen können auf vorbereiteten Hosts und Clustern geändert werden, aber die Änderungen werden nur angewendet, wenn neue Hosts und Cluster für VXLAN vorbereitet werden. Vorhandene virtuelle Portgruppen für VTEP VMkernel können nur geändert werden, wenn die Hosts und Cluster erneut manuell vorbereitet werden. Sie können die Gruppierungsrichtlinie und die MTU-Einstellungen per API ändern.

Problem

Für die VTEPs wurde eine falsche MTU-Einstellung ausgewählt.

Lösung

- Rufen Sie Informationen zu allen für VXLAN vorbereiteten Switches mit der API GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches` ab.
Suchen Sie in der API-Ausgabe nach dem Switch, den Sie ändern möchten, und notieren Sie den Namen. Hier ein Beispiel: *dvs-35*.
- Starten Sie jetzt eine Abfrage für den vSphere Distributed Switch, den Sie zuvor notiert haben.
Tun Sie dies beispielsweise mit der API GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35`.

Es muss dann eine Ausgabe in der folgenden Art angezeigt werden:

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  < name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    < name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>>false</promiscuousMode>
</vdsContext>
```

- 3 Sie können Parameter wie Gruppierungsrichtlinie und/oder MTU auf einem vSphere Distributed Switch per API-Aufruf ändern. Das folgende Beispiel zeigt das Ändern der Gruppierungsrichtlinie für *dvs-35* von *FAILOVER_ORDER* zu *LOADBALANCE_SRCMAC* und der MTU-Einstellung von *1600* zu *9000*.

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

Es muss dann eine Ausgabe in der folgenden Art angezeigt werden:

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

```

<name>Datacenter Site A</name>
</scope>
<clientHandle/>
<extendedAttributes/>
<isUniversal>false</isUniversal>
<universalRevision>0</universalRevision>
</switch>
<mtu>9000</mtu>
<teaming>LOADBALANCE_SRCMAC</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode>
</vdsContext>

```

Hinweis Im Folgenden finden Sie eine Auflistung gültiger Gruppierungsrichtlinieneinträge für den Parameter `<teaming>`:

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

- 4 Stellen Sie sicher, dass die verwendete Syntax korrekt ist und die Änderung für den bearbeiteten vSphere Distributed Switch aktiv ist. Nutzen Sie hierfür den Befehl GET. Beispiel: GET https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35.
- 5 Öffnen Sie vSphere Web Client und überprüfen Sie, ob die Änderungen an der Konfiguration vorgenommen wurden.

Logische Switch-Portgruppe nicht synchron

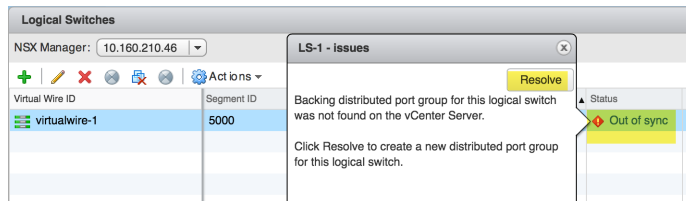
Wenn die virtuelle verteilte Backup-Portgruppe (DVPG) des logischen Switches vom vCenter Server entfernt wird, zeigt die Status-Spalte der Seite **Logische Switches (Logical Switches)** den Status **Out of sync** (nicht synchron) an.

Voraussetzungen

Die DVPG des logischen Switches wird vom vCenter Server entfernt.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Home > Netzwerk und Sicherheit (Networking & Security) > Logische Switches (Logical Switches)**.



- 2 Klicken Sie in der Status-Spalte auf den Link **Nicht synchron (Out of sync)**, um die detaillierte Begründung für diesen Status anzuzeigen.
- 3 Klicken Sie auf die Schaltfläche **Beheben (Resolve)**, um den Fehler zu beheben.

Ergebnisse

Dadurch erstellt die API die Backup-DVPG erneut.

Fehlerbehebung für das NSX-Routing

3

NSX verfügt über zwei verschiedene Arten von Routing-Subsystemen, die für zwei zentrale Anforderungen optimiert sind.

Es handelt sich um folgende NSX-Routing-Subsysteme:

- Das Routing innerhalb eines logischen Raums, auch als „Ost-West“-Routing bezeichnet, wird vom Distributed Logical Router (DLR) bereitgestellt.
- Das Routing zwischen physischem und logischem Raum, auch als „Nord-Süd“-Routing bezeichnet, wird von den Edge Services Gateways (ESG) bereitgestellt.

Beide Subsysteme bieten Optionen für die horizontale Skalierung.

Sie können das verteilte „Ost-West“-Routing über den DLR horizontal skalieren.

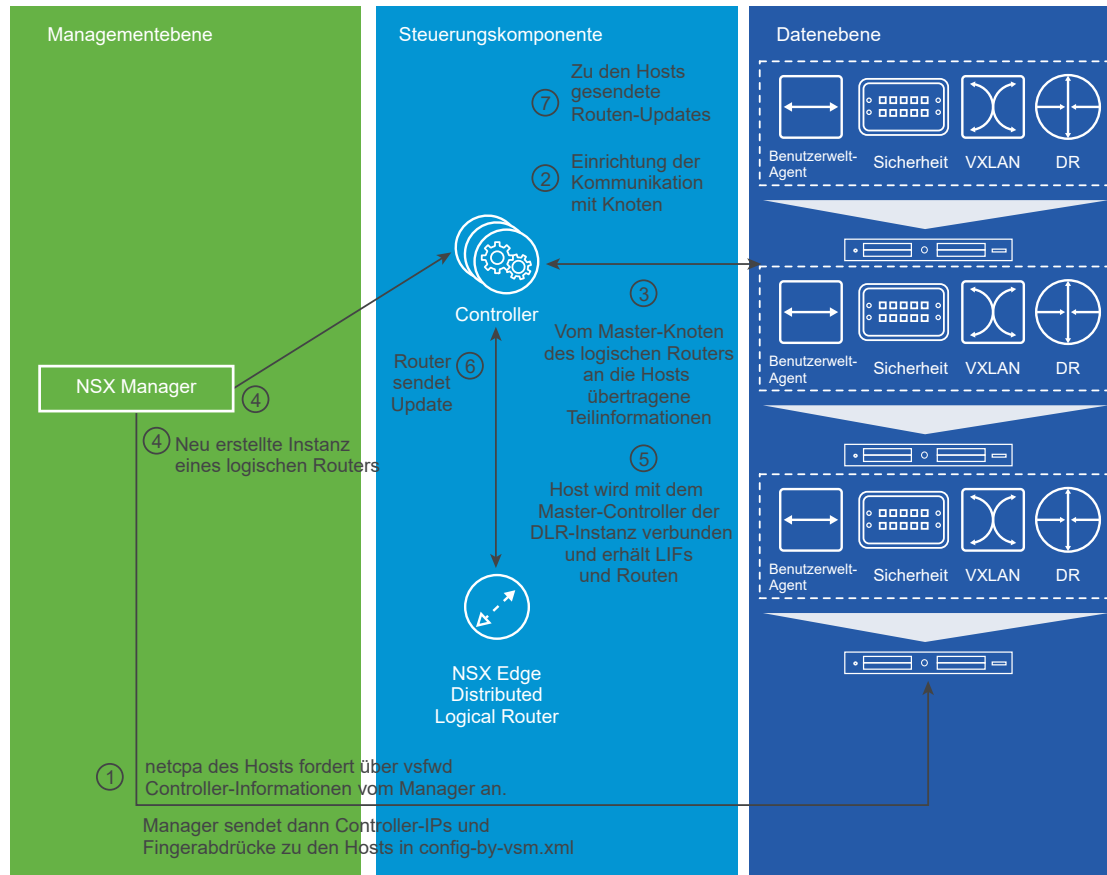
Der DLR unterstützt die Ausführung jeweils eines einzelnen dynamischen Routing-Protokolls (OSPF oder BGP), während das ESG beide Routing-Protokolle zeitgleich ausführen kann. Der Grund liegt darin, dass der DLR als ein „Stub“-Router mit nur einem Ausgangspfad entwickelt wurde, d. h., erweiterte Routing-Konfigurationen sind meist nicht erforderlich.

Sowohl der DLR wie das ESG unterstützen eine Kombination aus statischen und dynamischen Routen.

DLR und ESG unterstützen beide ECMP-Routen.

Beide stellen eine L3-Domänentrennung bereit, d. h., jede Instanz eines Distributed Logical Router oder eines Edge Services Gateway verfügt über seine eigene L3-Konfiguration ähnlich der L3VPN-VRF.

Abbildung 3-1. Erstellen eines DLR



Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zum Distributed Logical Router \(DLR\)](#)
- [Grundlegendes zu dem vom Edge Services Gateway bereitgestellten Routing](#)
- [ECMP-Paket-Flow](#)
- [NSX-Routing: Voraussetzungen und Hinweise](#)
- [Benutzeroberflächen von DLR und ESG](#)
- [Neues NSX Edge \(DLR\)](#)
- [Typische ESG- und DLR-Benutzeroberflächenoperationen](#)
- [Fehlerbehebung für das NSX-Routing](#)

Grundlegendes zum Distributed Logical Router (DLR)

Der DLR ist für die Weiterleitung im logischen Raum zwischen VMs in VXLAN- oder VLAN-gestützten Portgruppen optimiert.

Der DLR verfügt über die folgenden Eigenschaften:

- First-Hop-Routing mit hoher Leistung und geringem Overhead:

- Lineare Skalierung mit der Anzahl von Hosts
- Unterstützung von 8-Wege-ECMP beim Uplink
- Bis zu 1.000 DLR-Instanzen pro Host
- Bis zu 999 logische Schnittstellen (LIFs) bei jedem DLR (8 Uplinks + 991 intern) und 1 Verwaltungsschnittstelle
- Bis zu 10.000 LIFs pro Host verteilt auf alle DLR-Instanzen (wird von NSX Manager nicht erzwungen)

Berücksichtigen Sie folgende Einschränkungen:

- Mit einem bestimmten VLAN oder VXLAN kann jeweils nur ein DLR verbunden werden.
- Auf jedem DLR kann jeweils nur ein Routing-Protokoll ausgeführt werden.
- OSPF kann nicht auf mehreren DLR-Uplinks ausgeführt werden.
- Zum Routing zwischen VXLAN und VLAN muss die Transportzone einen einzelnen DVS umfassen.

Das Design des DLR entspricht auf abstrakter Ebene einem modularen Router-Gehäuse in folgender Hinsicht:

- ESXi-Hosts sind mit Leitungsanschlusskarten vergleichbar:
 - Sie verfügen über Ports mit verbundenen Endstationen (VMs).
 - Hier werden die Weiterleitungsentscheidungen getroffen.
- Die DLR-Steuerungs-VM ist mit einem Routenverarbeitungsmodul vergleichbar:
 - Sie führt dynamische Routing-Protokolle zum Austausch von Routing-Informationen mit den übrigen Netzwerkkomponenten aus.
 - Sie berechnet auf der Konfiguration der Schnittstellen, auf statischen Routen und dynamischen Routing-Informationen basierende Weiterleitungstabellen für „Leitungsanschlusskarten“.
 - Sie programmiert diese Weiterleitungstabellen in die „Leitungsanschlusskarten“ (über Controller-Cluster, um eine Skalierung und Ausfallsicherheit zu ermöglichen).
- Das physische Netzwerk, das die ESXi-Hosts miteinander verbindet, ist mit einer Rückwandplatine vergleichbar:
 - Hier werden VLAN- oder VXLAN-gekapselte Daten zwischen den „Leitungsanschlusskarten“ übertragen.

DLR-Paket-Flow auf oberster Ebene

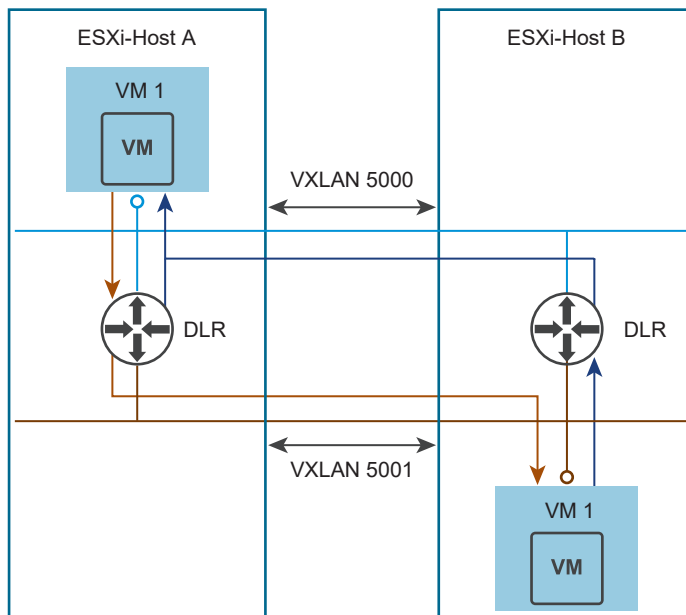
Jeder ESXi-Host verfügt über eine eigene Kopie jeder konfigurierten DLR-Instanz. Für jede DLR-Instanz ist ein spezifisches Set an Tabellen mit den für die Weiterleitung von Paketen erforderlichen Informationen vorhanden. Diese Informationen sind für alle Hosts mit der jeweiligen DLR-Instanz synchronisiert. Die Instanzen eines einzelnen DLR auf verschiedenen Hosts enthalten exakt die gleichen Informationen.

Das Routing wird immer von einer DLR-Instanz auf dem Host gesteuert, auf dem die Quell-VM ausgeführt wird. Wenn sich Quell- und Ziel-VMs auf verschiedenen Hosts befinden, hat dies zur Folge, dass die DLR-Instanz, die das Routing zwischen ihnen bereitstellt, Pakete nur in einer Richtung erkennt, nämlich von der Quell- zur Ziel-VM. Der Datenverkehr in der Gegenrichtung wird nur von der entsprechenden Instanz desselben DLR auf dem Host der Ziel-VM erkannt.

Nach dem Abschluss des Routings durch den DLR obliegt die Übermittlung an das endgültige Ziel dem DVS über L2 – VXLAN oder VLAN, wenn sich Quell- und Ziel-VMs auf unterschiedlichen Hosts befinden, oder dem lokalen DVS, wenn sie auf demselben Host vorhanden sind.

Abbildung 3-2. DLR-Paket-Flow auf oberster Ebene zeigt den Datenfluss zwischen zwei VMs, VM1 und VM2, die auf unterschiedlichen Hosts ausgeführt werden und mit zwei unterschiedlichen logischen Switches, VXLAN 5000 und VXLAN 5001, verbunden sind.

Abbildung 3-2. DLR-Paket-Flow auf oberster Ebene



Paket-Flow (ARP-Auflösung wird übersprungen):

- 1 VM1 sendet ein Paket in Richtung VM2, das dem Gateway von VM1 für das Subnetz von VM2 (oder der Standardeinstellung) zugewiesen ist. Dieses Gateway ist ein VXLAN 5000 LIF auf dem DLR.
- 2 Der DVS auf dem ESXi-Host A übermittelt das Paket an den DLR auf dem Host, auf dem die Suche durchgeführt wird, und die Egress LIF festgelegt ist (in diesem Fall VXLAN 5001 LIF).
- 3 Das Paket wird dann von dieser Ziel-LIF aus gesendet, die im Prinzip das Paket an den DVS zurückgibt, allerdings an einem anderen logischen Switch (5001).
- 4 Der DVS führt dann die L2-Übermittlung dieses Pakets an den Zielhost (ESXi-Host B) durch, auf dem der DVS das Paket an VM2 weiterleitet.

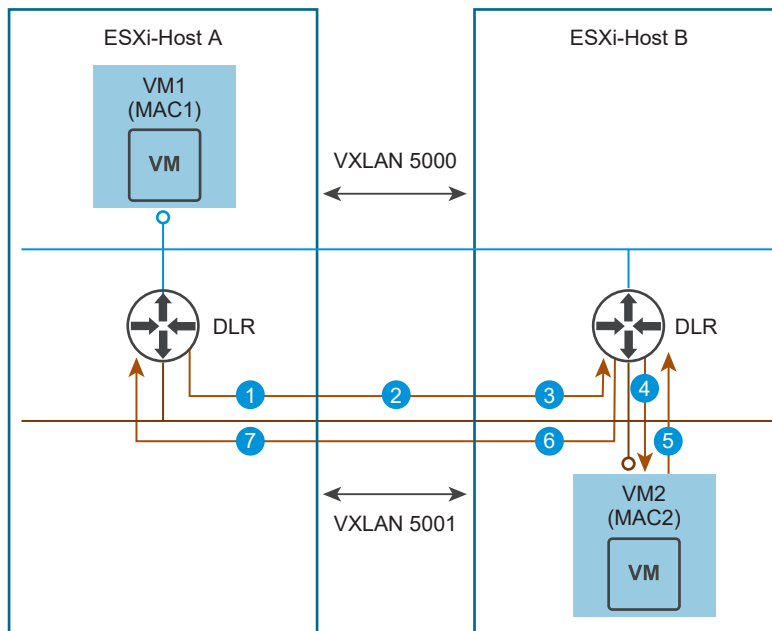
Der Datenverkehr in der Gegenrichtung erfolgt ebenfalls in dieser Reihenfolge. Der Datenverkehr von VM2 wird an die DLR-Instanz auf dem ESXi-Host B weitergeleitet und dann über L2 an VXLAN 5000 übermittelt.

ARP-Auflösung für DLRs

Damit der Datenverkehr von VM1 die virtuelle Maschine VM2 erreichen kann, muss der DLR die MAC-Adresse von VM2 abrufen. Nach dem Abrufen der MAC-Adresse von VM2 ist der DLR in der Lage, die korrekten L2-Kopfzeilen für die ausgehenden Pakete zu erstellen.

Abbildung 3-3. ARP-Vorgang für DLRs stellt den Vorgang der ARP-Auflösung für den DLR dar.

Abbildung 3-3. ARP-Vorgang für DLRs



Um die MAC-Adresse abzurufen, werden vom DLR folgende Schritte durchgeführt:

- 1 Die DLR-Instanz auf Host A generiert ein ARP-Anforderungspaket mit „SRC MAC = vMAC“ und „DST MAC = Broadcast“. Das VXLAN-Modul auf Host A ermittelt alle VTEPs auf dem Egress VXLAN 5001 und sendet jedem eine Kopie dieses Broadcast-Frames.
- 2 Wenn der Frame den Host über den VXLAN-Kapselungsvorgang verlässt, wird der SRC MAC von vMAC zu pMAC A geändert, damit der Datenverkehr in der Gegenrichtung die DLR-Instanz auf Host A finden kann, von der der Datenverkehr ausgeht. Der Frame lautet jetzt „SRC MAC = pMAC A“ und „DST MAC = Broadcast“.
- 3 Wenn der Frame dann auf Host B ankommt und entkapselt wird, wird er ausgewertet und ermittelt, dass er von der IP-Adresse stammt, die dem LIF der lokalen DLR-Instanz auf VXLAN 5001 entspricht. Damit wird der Frame als Anforderung für die Durchführung der Proxy-ARP-Funktion gekennzeichnet. Der DST MAC wird von „Broadcast“ zu „vMAC“ geändert, damit der Frame die lokale DLR-Instanz erreichen kann.

- 4 Die lokale DLR-Instanz auf Host B empfängt den ARP-Anforderungs-Frame, SRC MAC = pMAC A und DST MAC = vMAC, und erfasst die eigene anfordernde LIF-IP-Adresse. Sie speichert den SRC MAC und generiert ein neues ARP-Anforderungspaket mit SRC MAC = vMAC sowie DST MAC = Broadcast. Dieser Frame wird als „DVS Local“ gekennzeichnet, um zu verhindern, dass es für diesen über den dvUplink zu einem Überlauf kommt. Der DVS übermittelt den Frame an VM2.
- 5 VM2 sendet eine ARP-Antwort: SRC MAC = MAC2 und DST MAC = vMAC. Der DVS übermittelt diese an die lokale DLR-Instanz.
- 6 Die DLR-Instanz auf Host B ersetzt DST MAC mit dem pMAC A, der bei Schritt 4 gespeichert wurde, und sendet das Paket zurück zum DVS für eine Rückübermittlung zu Host A.
- 7 Wenn die ARP-Antwort Host A erreicht, wird DST MAC in vMAC geändert und der ARP-Antwort-Frame mit SRC MAC = MAC2 und DST MAC = vMAC erreicht die DLR-Instanz auf Host A.

Die ARP-Auflösung ist damit abgeschlossen und die DLR-Instanz auf Host A kann nun mit dem Senden des Datenverkehrs zu VM2 beginnen.

DLR-ARP-Unterdrückung

Address Resolution Protocol(ARP)-Unterdrückung ist eine Technik, die verwendet wird, um das Ausmaß von ARP-Broadcast-Flutung innerhalb einzelner VXLAN-Segmente zu verringern, d. h. zwischen VMs, die mit demselben logischen Switch verbunden sind.

Wenn die VM1 die MAC-Adresse für die VM2 in Erfahrung bringen möchte, sendet sie eine ARP-Anforderung. Diese ARP-Anforderung wird durch den logischen Switch abgefangen, und wenn der logische Switch bereits über einen ARP-Eintrag für das Ziel verfügt, sendet er die ARP-Antwort an die VM.

Falls dies nicht der Fall ist, sendet er eine ARP-Abfrage an den NSX Controller. Wenn der Controller die VM-IP-zu-MAC-Bindung kennt, antwortet der Controller mit der Bindung, und der logische Switch sendet die ARP-Antwort. Wenn der Controller nicht über den ARP-Eintrag verfügt, wird die ARP-Anforderung erneut auf dem logischen Switch übertragen. NSX Controller ermittelt die MAC-Adresse per Switch-Sicherheitsmodul, das ARP-Anforderungen/DHCP-Pakete überwacht.

Die ARP-Unterdrückung wurde erweitert und umfasst jetzt auch den Distributed Logical Router (DLR).

- ARP-Anforderungen des Distributed Logical Router werden genau wie ARP-Anforderungen von anderen VMs behandelt und unterliegen der Unterdrückung. Wenn der Distributed Logical Router die ARP-Anforderung einer Ziel-IP auflösen muss, wird die ARP-Anforderung durch den logischen Switch unterdrückt, sodass eine Flutung verhindert wird, wenn die IP-zu-MAC-Bindung dem Controller bereits bekannt ist.
- Wenn eine LIF erstellt wird, fügt der Distributed Logical Router den ARP-Eintrag für die LIF-IP im logischen Switch hinzu, sodass ARP-Anforderungen für die LIF-IP auch durch den logischen Switch unterdrückt werden.

Grundlegendes zu dem vom Edge Services Gateway bereitgestellten Routing

Das zweite Subsystem von NSX Routing wird vom Edge Services Gateway (ESG) bereitgestellt.

Das ESG ist im Grunde genommen ein Router in einer virtuellen Maschine. Es wird mit einem Appliance-ähnlichen Formfaktor in vier Größen bereitgestellt, wobei sein kompletter Lebenszyklus von NSX Manager verwaltet wird. Das ESG wird primär als Router im Umgrenzungsbereich eingesetzt. Dort wird es zwischen mehreren DLRs und zwischen der physischen Umgebung und dem virtuellen Netzwerk bereitgestellt.

Das ESG hat die folgenden Eigenschaften:

- Jedes ESG kann über bis zu 10 vNIC-Schnittstellen oder 200 Trunk-Teilschnittstellen verfügen.
- Jedes ESG unterstützt 8-Wege-ECMP für Pfadredundanz und Skalierbarkeit.

ECMP-Paket-Flow

Angenommen, mit zwei ESGs wird eine DLR-Instanz mit 2-Wege-ECMP-Uplinks zur physischen Umgebung bereitgestellt.

Abbildung 3-4. Übersicht über den ESG- und DLR-Paketfluss mit ECMP zeigt den ESG- und DLR-Paketfluss, wie er auftritt, wenn das Equal-Cost-MultiPath-(ECMP)-Routing zwischen den beiden ESGs und der physischen Infrastruktur aktiviert ist.

Daher hat VM1 Zugriff auf einen zweifachen bidirektionalen Durchsatz im Vergleich zu einer Bereitstellung mit einem ESG.

VM1 ist mit einem logischen Switch mit dem VNI 5000 verbunden.

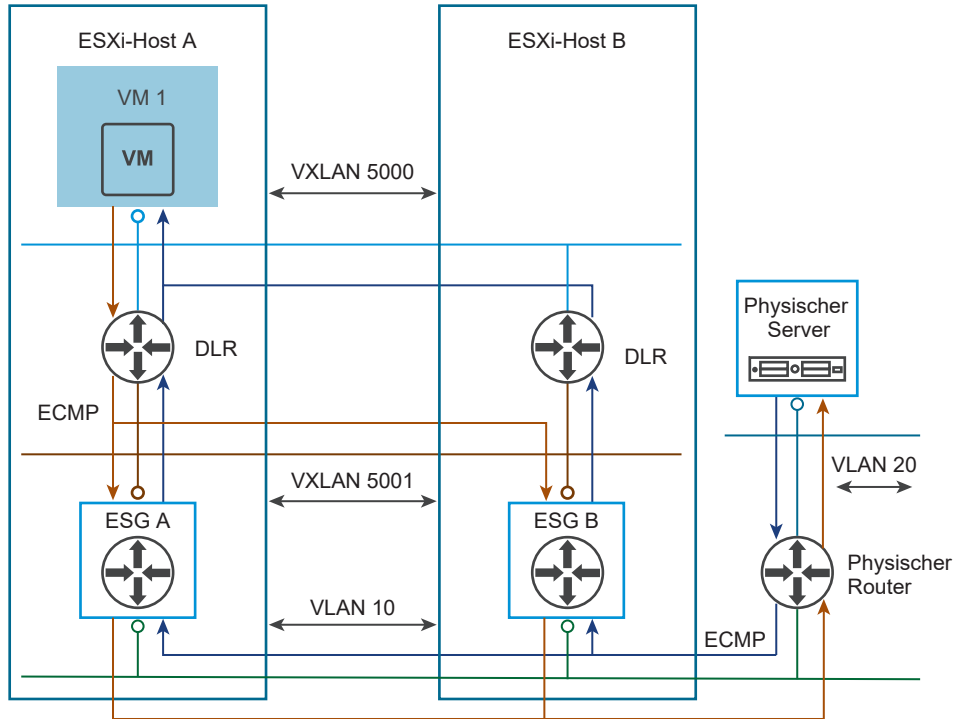
Der DLR verfügt über zwei LIFs: Intern an VNI 5000 und Uplink an VNI 5001.

Auf dem DLR ist ECMP aktiviert. Dieser erhält von den beiden ESGs (ESG A und ESG B) über ein dynamisches Routing-Protokoll (BGP oder OSPF) Equal-Cost-Routen zum IP-Subnetz von VLAN 20.

Die beiden ESGs sind mit einer VLAN-gestützten dvPortgroup verbunden, die mit dem VLAN 10 verknüpft ist, das wiederum mit einem physischen Router, der eine Konnektivität mit VLAN 20 bereitstellt, verbunden ist.

Die ESGs erhalten über ein dynamisches Routing-Protokoll vom physischen Router externe Routen für VLAN 20.

Der physische Router ruft über die beiden ESGs das mit VXLAN 5000 verknüpften IP-Subnetz ab und führt für den an die VMs in diesem Subnetz gerichteten Datenverkehr das ECMP-Load-Balancing durch.

Abbildung 3-4. Übersicht über den ESG- und DLR-Paketfluss mit ECMP

Der DLR kann bis zu acht Equal-Cost-Routen empfangen und ein Load Balancing für den Datenverkehr auf diesen Routen ausführen. Die im Diagramm dargestellten ESG A und ESG B stellen zwei Equal-Cost-Routen bereit.

ESGs können das ECMP-Routing zum physischen Netzwerk durchführen, wobei angenommen wird, dass mehrere physische Router vorhanden sind. Der Einfachheit halber ist im Diagramm nur ein einzelner physischer Router dargestellt.

ECMP muss auf den ESGs nicht für den DLR konfiguriert werden, da sich alle DLR-LIFs „lokal“ auf demselben Host wie die ESGs befinden. Die Konfiguration mehrerer Uplink-Schnittstellen auf einem DLR würde keine zusätzlichen Vorteile bringen.

In Situationen, in denen mehr „Nord-Süd“-Bandbreite benötigt wird, können mehrere ESGs auf verschiedenen ESXi-Hosts platziert werden, sodass bei acht ESGs eine Skalierung auf bis zu ~80 GB/s möglich ist.

Der ECMP-Paketfluss (ohne ARP-Auflösung):

- 1 VM1 sendet ein Paket an den physischen Server. Dieses Paket wird wiederum an das IP-Gateway (eine DLR-LIF) von VM1 auf dem ESXi-Host gesendet.
- 2 Der DLR führt eine Routensuche für die IP-Adresse des physischen Servers durch und stellt fest, dass er nicht direkt mit dem Server verbunden ist, aber von ESG A und ESG B zwei passende ECMP-Routen erhält.
- 3 Der DLR berechnet einen ECMP-Hash, wählt den nächsten Hop aus, bei dem es sich um ESG A oder ESG B handeln kann, und sendet das Paket über die VXLAN 5001-LIF.

- 4 Der DVS stellt das Paket dem gewählten ESG zu.
- 5 Das ESG führt eine Routensuche durch und stellt fest, dass das Subnetz des physischen Servers über die IP-Adresse des physischen Routers im VLAN 10 zugänglich ist, das direkt mit einer Schnittstelle des ESG verbunden ist.
- 6 Das Paket wird über den DVS abgeschickt, der es an das physische Netzwerk weiterleitet, nachdem er es mit dem korrekten 801.Q-Tag mit der VLAN-ID 10 gekennzeichnet hat.
- 7 Das Paket wird durch die physische Switching-Infrastruktur zum physischen Router geleitet, der eine Suche durchführt und feststellt, dass der physische Server direkt mit einer Schnittstelle in VLAN 20 verbunden ist.
- 8 Der physische Router sendet das Paket an den physischen Server.

Rückweg:

- 1 Der physische Server sendet das Paket an VM1, wobei der physische Router den nächsten Hop darstellt.
- 2 Der physische Router führt eine Suche nach dem Subnetz von VM1 durch und erkennt zwei Equal-Cost-Pfade zu diesem Subnetz, wobei die VLAN 10-Schnittstelle von ESG A und ESG B die nächsten Hops sind.
- 3 Der physische Router wählt einen dieser Pfade aus und sendet das Paket an das entsprechende ESG.
- 4 Das physische Netzwerk stellt das Paket dem ESXi-Host zu, auf dem sich das ESG befindet, und liefert es an den DVS, der das Paket entkapselt und über die VLAN 10 zugeordnete dvPortgroup an das ESG weiterleitet.
- 5 Das ESG führt eine Routensuche durch und stellt fest, dass das Subnetz von VM1 über seine Schnittstelle, die VXLAN 5001 zugeordnet ist, zugänglich ist, wobei die IP-Adresse der Uplink-Schnittstelle des DLR der nächste Hop ist.
- 6 Das ESG sendet das Paket an die DLR-Instanz, die sich auf demselben Host wie das ESG befindet.
- 7 Der DLR führt eine Routensuche durch und stellt fest, dass VM1 über seine VXLAN 5000-LIF verfügbar ist.
- 8 Der DLR sendet das Paket über seine VXLAN 5000-LIF an den DVS, der es schließlich zustellt.

NSX-Routing: Voraussetzungen und Hinweise

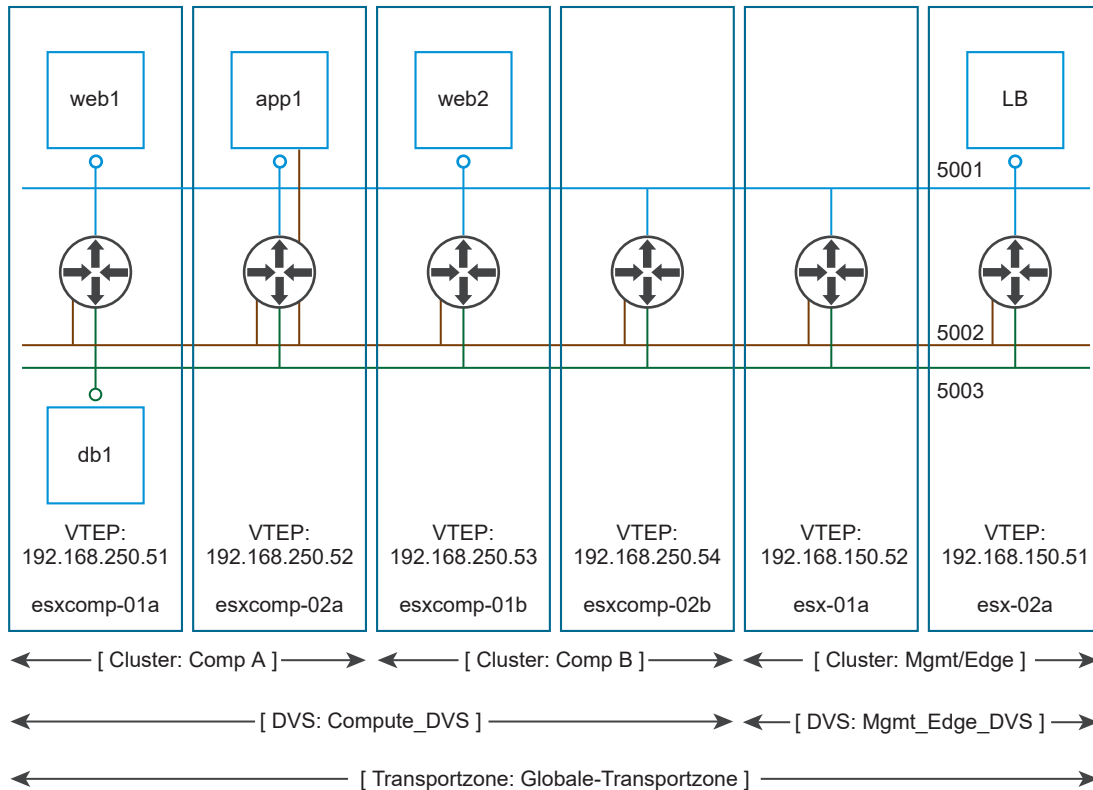
Der DLR und das ESG benötigen für die Bereitstellung von L2-Weiterleitungsdiensten für dvPortgroups (sowohl VXLAN- als auch VLAN-basiert) den DVS für eine funktionierende End-to-End-Konnektivität.

Dies bedeutet, dass L2 für Weiterleitungsdienste, die mit dem DLR und dem ESG verbunden sind, konfiguriert und betriebsbereit sein müssen. Während des NSX-Installationsvorgangs werden diese Dienste durch die „Hostvorbereitung“ und die „Vorbereitung des logischen Netzwerks“ bereitgestellt.

Für das Anlegen von Transportzonen für Multi-Cluster-DVS-Konfigurationen müssen alle Cluster in dem ausgewählten DVS in der Transportzone enthalten sein. Dadurch wird sichergestellt, dass der DLR auf allen Clustern verfügbar ist, in denen auch DVS-dvPortgroups vorhanden sind.

Die DLR-Instanz wurde korrekt erstellt, wenn eine Transportzone an der DVS-Begrenzung ausgerichtet ist.

Abbildung 3-5. Korrekt an der DVS-Begrenzung ausgerichtete Transportzone

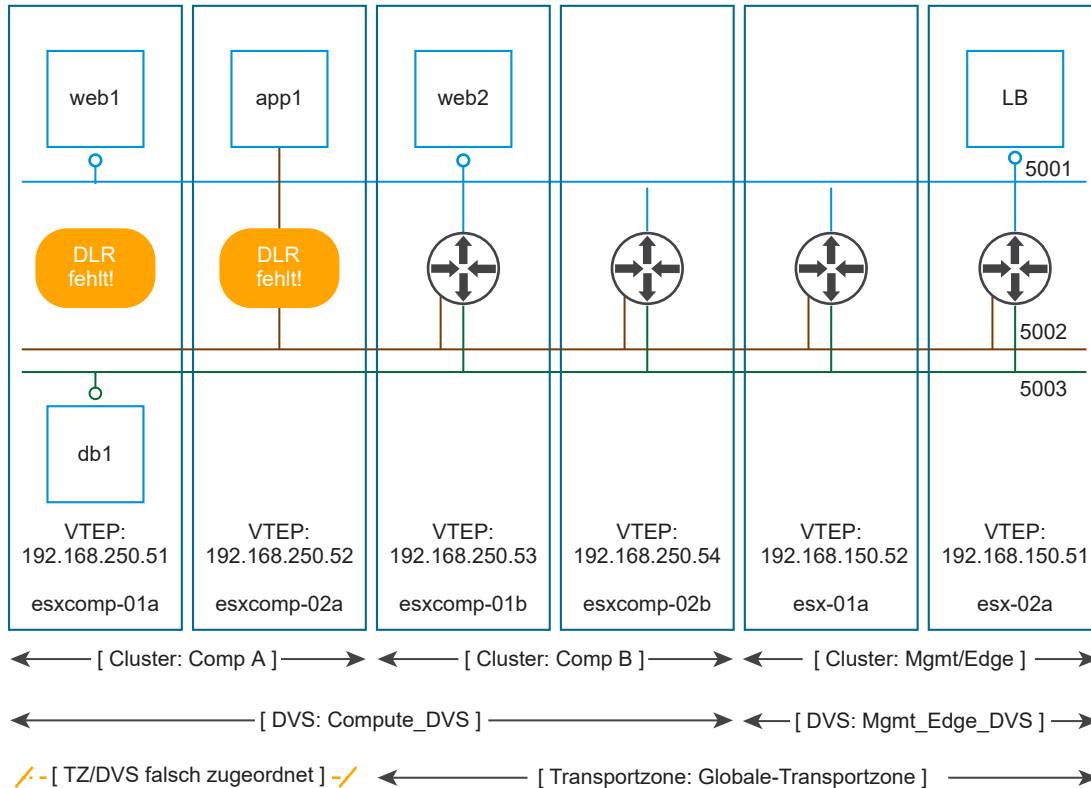


Wenn eine Transportzone nicht an der DVS-Begrenzung ausgerichtet ist, werden der Geltungsbereich der logischen Switches (5001, 5002 und 5003) und die DLR-Instanzen, mit denen diese logischen Switches verbunden sind, getrennt. VMs im Cluster „Comp A“ haben dann keinen Zugriff auf die DLR-LIFs.

Im oben dargestellten Diagramm erstreckt sich der DVS „Compute_DVS“ über die beiden Cluster „Comp A“ und „Comp B“. Die „Globale Transportzone“ enthält sowohl „Comp A“ als auch „Comp B“.

Dies führt zu einer korrekten Ausrichtung zwischen dem Geltungsbereich der logischen Switches (5001, 5002 und 5003) und der DLR-Instanz, die auf allen Hosts in allen Clustern erstellt wurde, in denen diese logischen Switches vorhanden sind.

Wenden wir uns nun einem alternatives Szenario zu, in dem die Konfiguration der Transportzone den Cluster „Comp A“ nicht beinhaltet:

Abbildung 3-6. Nicht korrekt an DVS-Begrenzung ausgerichtete Transportzone

In diesem Fall haben die VMs, die auf Cluster „Comp A“ ausgeführt werden, einen kompletten Zugriff auf alle logischen Switches. Dies ist darauf zurückzuführen, dass die logischen Switches von den dvPortgroups auf Hosts repräsentiert werden und die dvPortgroups ein DVS-weites Konstrukt sind. In unserer Beispielumgebung erstreckt sich „Compute_DVS“ sowohl über „Comp A“ als auch „Comp B“.

Die DLR-Instanzen sind jedoch streng am Geltungsbereich der Transportzone ausgerichtet. Das bedeutet, dass auf den Hosts in „Comp A“ keine DLR-Instanzen erstellt werden.

Im Ergebnis kann die VM „web1“ die VMs „web2“ und „LB“ erreichen, da sie sich auf demselben logischen Switch befinden. Die VMs „app1“ und „db1“ sind dagegen nicht in der Lage, mit anderen zu kommunizieren.

Der DLR benötigt einen funktionsfähigen Controller-Cluster, das ESG hingegen nicht. Stellen Sie sicher, dass der Controller-Cluster eingerichtet und verfügbar ist, ehe Sie eine DLR-Konfiguration erstellen oder ändern.

Wenn der DLR mit VLAN-dvPortgroups verbunden werden soll, stellen Sie sicher, dass die ESXi-Hosts mit konfiguriertem DLR sich gegenseitig auf UDP/6999 erreichen können, damit der DLR-VLAN-basierte ARP-Proxy funktioniert.

Hinweise:

- Eine bestimmte DLR-Instanz kann nicht mit logischen Switches verbunden werden, die sich in verschiedenen Transportzonen befinden. Dadurch wird sichergestellt, dass alle logischen Switches und DLR-Instanzen ausgerichtet sind.

- Der DLR kann nicht mit VLAN-gestützten Portgruppen verbunden werden, wenn dieser mit logischen Switches verbunden ist, die sich über mehr als einen DVS erstrecken. Damit wird wie zuvor die korrekte Ausrichtung der DLR-Instanzen auf die logischen Switches und dvPortgroups für alle Hosts sichergestellt.
- Bei der Auswahl der Position der DLR-Kontroll-VM sollten Sie diese nicht auf demselben Host platzieren, auf dem sich bereits ein oder mehrere ihrer Upstream-ESGs befinden. Dazu verwenden Sie DRS-Anti-Affinitätsregeln, wenn sie sich in demselben Cluster befinden. Dadurch lassen sich die Auswirkungen von Hostfehlern bei DLR-Weiterleitungen verringern.
- OSPF darf nur auf einem einzelnen Uplink aktiviert sein (kann aber mehrere Nachbarschaften unterstützen). BGP hingegen darf auf mehreren Uplink-Schnittstellen aktiviert sein, sofern dies notwendig ist.

Benutzeroberflächen von DLR und ESG

Die DLR- und ESG-Benutzeroberflächen bieten Indikatoren des Systemarbeitszustands.

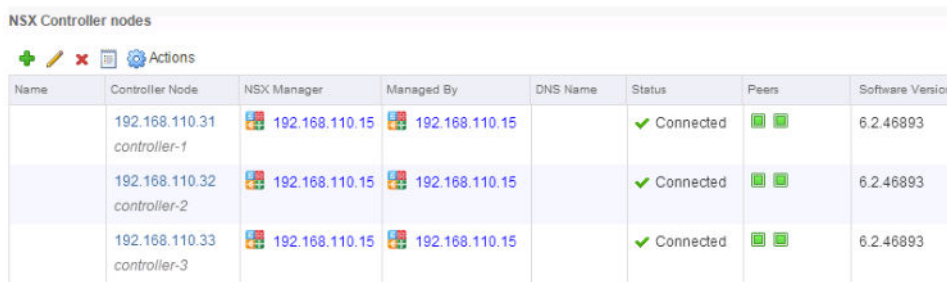
Benutzeroberfläche für das NSX-Routing

Die Benutzeroberfläche des vSphere Web Client enthält zwei große Bereiche, die für das NSX-Routing relevant sind.

Dazu gehören die Infrastrukturabhängigkeiten von L2 und den Steuerungskomponenten sowie die Konfiguration des Routing-Subsystems.

Für das verteilte NSX-Routing werden Funktionen benötigt, die vom Controller-Cluster bereitgestellt werden. Die folgende Abbildung zeigt einen Controller-Cluster in fehlerfreiem Zustand.

NSX Controller nodes



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

Beachten Sie folgende Hinweise:

- Es werden drei Controller bereitgestellt.
- Bei „Status“ gilt für alle Controller „Verbunden“.
- Die Softwareversion ist für alle Controller identisch.
- Jeder Controller-Knoten verfügt über zwei Peers.

Die Hostkernelmodule für das verteilte Routing werden als Bestandteil der VXLAN-Konfiguration auf dem Host installiert und konfiguriert. Das verteilte Routing erfordert demnach, dass die ESXi-Hosts vorbereitet sind und VXLAN darauf konfiguriert ist.

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

Beachten Sie folgende Hinweise:

- Für „Installationsstatus“ gilt „Grün“.
- Für „VXLAN“ gilt „Konfiguriert“.

Stellen Sie sicher, dass die VXLAN-Transportkomponenten korrekt konfiguriert sind.

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

Beachten Sie folgende Hinweise:

- Die VLAN-ID muss dem VTEP-Transport-VLAN entsprechen. Beachten Sie, dass diese in obiger Abbildung „0“ ist. Bei den meisten realen Bereitstellungen ist dies nicht der Fall.
- Die MTU ist für den Wert 1600 oder größer konfiguriert. Stellen Sie sicher, dass für die MTU nicht der Wert 9000 festgelegt wird, in der Annahme, dass die MTU der VMs ebenfalls auf 9000 gesetzt ist. Der maximale MTU-Wert des DVS beträgt 9000. Wenn für die VMs ebenfalls der Wert 9000 festgelegt wurde, ist kein Platz mehr für die VXLAN-Kopfzeile vorhanden.
- Die VMKNics müssen über die korrekten Adressen verfügen. Stellen Sie sicher, dass für sie nicht die Adressen 169.254.x.x festgelegt sind. Diese geben an, dass Knoten keine Adressen aus dem DHCP abrufen konnten.
- Die Gruppierungsrichtlinie muss für alle Cluster-Mitglieder desselben DVS einheitlich sein.
- Die Anzahl der VTEPs muss identisch mit der Anzahl der dvUplinks sein. Stellen Sie sicher, dass die gültigen bzw. vorgesehenen IP-Adressen aufgelistet sind.

Die Transportzonen müssen korrekt an den DVS-Begrenzungen ausgerichtet sein, um zu vermeiden, dass der DLR auf einigen Clustern nicht vorhanden ist.

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

Benutzeroberfläche von NSX Edges

Das NSX-Routing-Subsystem lässt sich im Abschnitt „NSX Edges“ der Benutzeroberfläche konfigurieren und verwalten.

Nach der Auswahl dieses Bereichs der Benutzeroberfläche wird die nachfolgend dargestellte Ansicht eingeblendet.

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

Es werden alle aktuell bereitgestellten DLRs und ESGs mit den folgenden Informationen für jedes Element angezeigt:




- Unter „ID“ ist die ESG- oder DLR-Edge-Appliance ID enthalten, mit der API-Aufrufe für das jeweilige ESG oder den jeweiligen DLR durchgeführt werden können.
- Die Einträge für „Tenant“ (Mandant) und „ID“ bilden den Namen der DLR-Instanz. Dieser wird in der NSX-Befehlszeilenschnittstelle (CLI) dargestellt und verwendet.
- Für einen DLR wird unter „Größe“ immer „Kompakt“ und für das ESG die vom Operator ausgewählte Größe angezeigt.

Zusätzlich zu den Informationen der Tabelle steht Ihnen ein Kontextmenü zur Verfügung, das sich über Schaltflächen oder mit der Option „Aktionen“ aufrufen lässt.

Tabelle 3-1. Kontextmenü von NSX Edge

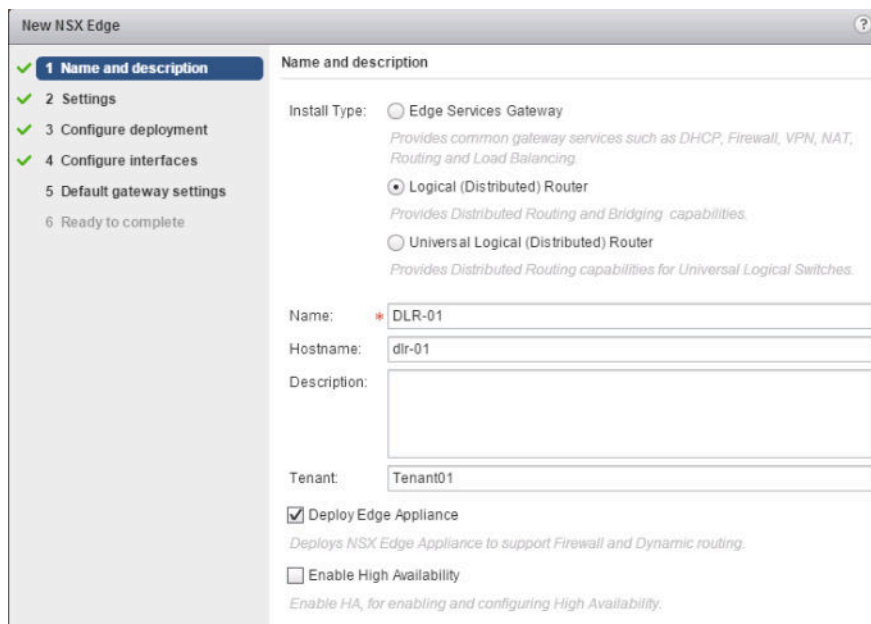
Symbol	Aktion
	Der Vorgang „Synchronisierung erzwingen“ löscht die Konfiguration des ESG oder der DLR-Kontroll-VM, startet diese neu und überträgt die Konfiguration erneut.
	Mit „Erneut bereitstellen“ wird das ESG oder der DLR außer Kraft gesetzt und ein neues ESG oder ein neuer DLR mit der gleichen Konfiguration erstellt. Die vorhandene ID wird beibehalten.
	Die Option „Konfiguration für die automatische Regel ändern“ steht für die integrierten Firewallregeln des ESG zur Verfügung, die bei der Aktivierung von Diensten für das ESG (z. B. BGP mit TCP/179) erstellt werden.
	Mit „Tech-Support-Protokolle herunterladen“ wird ein Protokollpaket vom ESG oder von der DLR-Kontroll-VM erstellt. Für den DLR sind keine Hostprotokolle im Tech-Support-Paket enthalten. Sie müssen gesondert erfasst werden.
	„Appliance-Größe ändern“ steht nur ESGs zur Verfügung. Damit wird eine erneute Bereitstellung mit einer neuen Appliance durchgeführt (die vNIC-MAC-Adressen sind dann geändert).
	Mit „Ändern der CLI-Anmeldedaten“ kann der Operator eine Aktualisierung der CLI-Anmeldedaten erzwingen. Wenn die Befehlszeilenschnittstelle (CLI) für ein ESG oder eine DLR-Kontroll-VM nach fünf gescheiterten Anmeldeversuchen gesperrt ist, kann die Sperre mit dieser Option nicht aufgehoben werden. Sie müssen stattdessen fünf Minuten warten oder Ihr ESG bzw. Ihren DLR mit der entsprechenden Option erneut bereitstellen, um sich mit den korrekten Anmeldedaten anzumelden.
	Mit „Protokollierungsebene ändern“ lässt sich einstellen, wie detailliert Meldungen an das ESG-/DLR-Syslog-Protokoll gesendet werden sollen.
	„Erweitertes Debugging konfigurieren“ stellt das ESG oder den DLR mit aktiviertem Core-Dump und einer zusätzlichen virtuellen Festplatte für das Speichern von Core-Dump-Dateien erneut bereit.

Tabelle 3-1. Kontextmenü von NSX Edge (Fortsetzung)

Symbol	Aktion
	„Bereitstellen“ ist verfügbar, wenn ein ESG ohne Bereitstellung erstellt wurde. Diese Option führt die standardmäßigen Bereitstellungsschritte aus, d. h. sie stellt die OVF-Datei bereit, konfiguriert Schnittstellen und überträgt die Konfiguration auf die erstellte Appliance.
	Wenn die Version des DLR bzw. des ESG älter als der NSX Manager ist, steht die Option „Upgrade-Version“ zur Verfügung.
	Mit „Filter“ können Sie nach ESGs/DLRs per Namen suchen.

Neues NSX Edge (DLR)

Wenn ein Operator einen neuen DLR erstellt, werden die notwendigen Informationen mit dem nachstehend abgebildeten Assistenten eingeholt.



New NSX Edge

1 Name and description

Name and description

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

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

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

Name: *

Hostname:

Description:

Tenant:

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

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

Im Bildschirm „Name und Beschreibung“ werden folgende Informationen erfasst:

- „Name“ wird in der „NSX Edges“-Benutzeroberfläche angezeigt.
- Mit „Hostname“ wird der DNS-Name des ESG oder der DLR-Kontroll-VM festgelegt. Dieser wird in der SSH-/Konsolensitzung, in Syslog-Meldungen und auf der vCenter-Seite „Übersicht“ für das ESG bzw. für die DLR-VM unter „DNS-Name“ dargestellt.
- „Beschreibung“ ist in der Benutzeroberfläche enthalten und zeigt die Liste der NSX Edges an.
- „Mandant“ wird zur Bildung des DLR-Instanznamens eingesetzt, der von der NSX-Befehlszeilenschnittstelle (CLI) verwendet wird. Er kann auch von einer externen Cloud-Managementplattform benutzt werden.

Im Bildschirm „Einstellungen“ werden folgende Informationen erfasst:

- „Benutzername“ und „Kennwort“ legen die Anmeldedaten für die CLI-/VM-Konsole zum Zugriff auf die DLR-Kontroll-VM fest. NSX unterstützt AAA nicht auf ESGs oder DLR-Kontroll-VMs. Dieses Konto verfügt über die kompletten Berechtigungen für das ESG bzw. die DLR-Kontroll-VMs. Die ESG-/DLR-Konfiguration lässt sich allerdings nicht mit der CLI-/VM-Konsole ändern.
- „SSH-Zugriff aktivieren“ aktiviert den Start des SSH-Daemon in der DLR-Kontroll-VM.
 - Die Firewallregeln der Kontroll-VM müssen so angepasst werden, dass ein SSH-Netzwerkzugriff zulässig ist.
 - Der Operator kann mit der DLR-Kontroll-VM von einem Host im Subnetz der Verwaltungsschnittstelle der Kontroll-VM oder von OSPF-/BGP-„Protokolladresse“ eine Verbindung herstellen, sofern eine Protokolladresse konfiguriert ist.

Hinweis Es ist keine Netzwerkkonnektivität zwischen der DLR-Kontroll-VM und einer beliebigen IP-Adresse möglich, die in ein Subnetz fällt, das auf einer „internen“ DLR-Schnittstelle konfiguriert ist. Der Grund liegt darin, dass die Egress-Schnittstelle für diese Subnetze in der DLR-Kontroll-VM auf die Pseudo-Schnittstelle „VDR“ verweist, die nicht mit der Datenebene verbunden ist.

- „HA aktivieren“ stellt die Kontroll-VM als Aktiv/Standby-HA-Paar bereit.
- „Protokollierung der Edge-Steuerungsebene“ legt die Syslog-Ebene in der Edge-Appliance fest.

Im Bildschirm „Bereitstellungskonfiguration“ werden folgende Informationen erfasst:

Resource Pool	Host	Datastore	Folder
Management & E...		ds-site-a-nfs01	

- Unter „Datacenter“ ist das vCenter-Datencenter enthalten, in dem die Kontroll-VM bereitgestellt werden soll.

- „NSX Edge Appliances“ bezieht sich auf die DLR-Kontroll-VM und ermöglicht die Definition von genau einer DLR-Kontroll-VM (wie dargestellt).
 - Wenn „HA“ aktiviert ist, wird das Standby-Edge auf demselben Cluster, Host und Datenspeicher bereitgestellt. Eine DRS-Regel „Separate Virtual Machines“ (Separate virtuelle Maschinen) wird für die aktiven und Standby-DLR-Kontroll-VMs erstellt.

Auf dem Bildschirm „Schnittstellen konfigurieren“ werden folgende Informationen erfasst:

Name	IP Address	Subnet Prefix Length	Connected To
LS A-Uplink	192.168.10.5*	29	vds-mgt_Uplink Network

- „HA-Schnittstelle“
 - Wird nicht als Routing-fähige logische DLR-Schnittstelle erstellt. Es handelt sich lediglich um eine vNIC der Kontroll-VM.
 - Diese Schnittstelle erfordert keine IP-Adresse, da NSX die DLR-Konfiguration über die VMCI verwaltet.
 - Diese Schnittstelle wird für HA-Taktsignale verwendet, wenn die DLR-Option „High Availability aktivieren“ im Bildschirm „Name und Beschreibung“ aktiviert ist.
- „Schnittstellen dieses NSX Edge konfigurieren“ bezieht sich auf logische Schnittstellen des DLR (LIFs)
 - Der DLR stellt L3-Gateway-Dienste für VMs in der dvPortgroup „Verbunden mit“ oder für logische Switches mit IP-Adressen aus den entsprechenden Subnetzen bereit .
 - LIFs vom Typ „Uplink“ werden als vNICs in der Kontroll-VM erstellt und es werden bis zu acht unterstützt. Die letzten beiden verfügbaren vNICs sind der HA-Schnittstelle zugeordnet und eine vNIC wird reserviert.
 - Eine LIF vom Typ „Uplink“ ist für das Funktionieren des dynamischen Routings auf dem DLR erforderlich.
 - Und LIFs vom Typ „Intern“ werden schließlich als Pseudo-vNICs in der Kontroll-VM erstellt. Es können bis zu 991 interne LIFs vorhanden sein.

Im Bildschirm „Standard-Gateway-Einstellungen“ sind folgende Informationen enthalten:

- Durch Auswahl von „Standard-Gateway konfigurieren“ wird eine statische Standardroute auf dem DLR erstellt. Diese Option ist verfügbar, wenn im vorherigen Bildschirm eine LIF vom Typ „Uplink“ erstellt wurde.
- Wird ECMP auf dem Uplink verwendet, sollte diese Option deaktiviert bleiben, um Datenebenenausfälle bei „Nächster-Hop“-Fehlern zu verhindern.

Hinweis Der doppelte Pfeil nach rechts in der oberen rechten Ecke ermöglicht das „Anhalten“ des Assistenten während der Ausführung. Er kann dann später wieder fortgesetzt werden.

Unterschiede zwischen ESG und DLR

Die Assistenten für die ESG- und DLR-Bereitstellung unterscheiden sich in einigen Bereichen.

Der erste Bereich ist der Bildschirm „Bereitstellungskonfiguration“:

Bei einem ESG ermöglicht der Bildschirm „Bereitstellungskonfiguration“ die Auswahl der Edge-Größe. Wird ein ESG nur für das Routing verwendet, ist „Groß“ die typische Größeneinstellung, die für die meisten Szenarien adäquat ist. Durch Auswahl einer höheren Größeneinstellung werden für die Routing-Vorgänge des ESG nicht mehr CPU-Ressourcen bereitgestellt und der Durchsatz wird nicht erhöht.

Es lässt sich auch ein ESG ohne Bereitstellung erstellen, wofür aber dennoch die Konfiguration einer Edge-Appliance erforderlich ist.

Ein „nicht bereitgestelltes“ Edge kann später über einen API-Aufruf oder mit der Option „Bereitstellen“ der Benutzeroberfläche bereitgestellt werden.

Ist die Edge HA ausgewählt, müssen Sie mindestens eine „interne“ Schnittstelle erstellen. Andernfalls fällt die HA (High Availability) ohne Rückmeldung aus und es kommt zu einem „Split-Brain“-Szenario.

Mit der NSX-Benutzeroberfläche und -API kann ein Operator die letzte „interne“ Schnittstelle entfernen, die zum nicht angezeigten Ausfall der HA führt.

Typische ESG- und DLR-Benutzeroberflächenoperationen

Zusätzlich zum Erstellen werden in der Regel weitere Konfigurationsoperationen nach der ersten Bereitstellung ausgeführt.

Hierzu gehören:

- Syslog-Konfiguration
- Verwaltung der statischen Routen
- Konfiguration von Routing-Protokollen und Route Redistribution.

Syslog-Konfiguration

Konfigurieren Sie das ESG oder die DLR-Kontroll-VM so, dass Protokolleinträge an einen Remote-Syslog-Server gesendet werden.

The screenshot shows the configuration page for DLR-01. The 'Manage' tab is active, and the 'Settings' sub-tab is selected. The 'Configuration' sidebar on the left shows 'Interfaces' under 'Configuration'. The main area displays the 'Details' for Syslog configuration:

Details:		Action
Size:	Compact	
Auto generate rules:	Enabled	
Syslog servers:		Change
Server 1:	192.168.110.79	
Server 2:		

Anmerkungen:

- Der Syslog-Server muss als IP-Adresse konfiguriert werden, da das ESG bzw. die DLR-Kontroll-VM nicht mit einem DNS-Server zur Adressauflösung konfiguriert wird.
 - Bei einem ESG kann mit der Option „DNS-Dienst aktivieren“ der DNS-Dienst (DNS-Proxy) aktiviert werden, den das ESG zum Auflösen von DNS-Namen verwenden kann. Im Allgemeinen ist die Angabe des Syslog-Servers über die IP-Adresse jedoch eine zuverlässigere Methode, die mit weniger Abhängigkeiten verbunden ist.
- Es ist nicht möglich, einen Syslog-Port in der Benutzeroberfläche anzugeben (es wird immer 514 verwendet), das Protokoll (UDP/TCP) kann jedoch festgelegt werden.

- Syslog-Meldungen werden von der IP-Adresse der Edge-Schnittstelle gesendet, die in der Weiterleitungstabelle des Edge als Egress-Schnittstelle für die IP-Adresse des Syslog-Servers ausgewählt wurde.
 - Beim DLR darf sich die IP-Adresse des Syslog-Servers in keinem Subnetz befinden, das an einer „internen“ Schnittstelle des DLR konfiguriert ist. Der Grund liegt darin, dass die Egress-Schnittstelle für diese Subnetze in der DLR-Kontroll-VM auf die Pseudo-Schnittstelle „VDR“ verweist, die nicht mit der Datenebene verbunden ist.

Standardmäßig ist die Protokollierung für das ESG/DLR-Routing-Modul deaktiviert. Bei Bedarf aktivieren Sie diese über die Benutzeroberfläche, indem Sie bei „Konfiguration für dynamisches Routing“ auf „Bearbeiten“ klicken.

The screenshot shows the NSX DLR-01 configuration interface. At the top, there's a header with 'DLR-01' and an 'Actions' dropdown. Below this, there are tabs for 'Summary' and 'Manage'. Under 'Manage', there are sub-tabs for 'Settings', 'Firewall', 'Routing' (which is selected), 'Bridging', and 'DHCP Relay'. The 'Routing' tab is active, showing a 'Routing Configuration' section with a 'Reset' button. Below this, there's a section for 'ECMP' with a toggle switch set to 'Enable'. A 'Default Gateway' section has 'Edit' and 'Delete' buttons. Below that, there are input fields for 'Interface', 'Gateway IP', 'MTU', and 'Description'. Further down, the 'Dynamic Routing Configuration' section has an 'Edit' button and input fields for 'Router ID', 'OSPF' (disabled), 'BGP' (disabled), 'Logging' (disabled), and 'Log Level'.

Sie müssen auch die Router-ID konfigurieren. In der Regel handelt es sich dabei um die IP-Adresse der Uplink-Schnittstelle.

Statische Routen

Bei statischen Routen muss der nächste Hop auf eine IP-Adresse in einem Subnetz, das einer LIF- oder ESG-Schnittstelle des DLR zugeordnet ist, festgelegt werden. Andernfalls schlägt die Konfiguration fehl.

Sofern nicht ausgewählt, wird „Interface“ (Schnittstelle) automatisch festgelegt, indem der nächste Hop einem der direkt verbundenen Subnetze zugeordnet wird.

Add Static Route ?

Network: *

10.10.10.0/24

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

Next Hop: *

192.168.10.1

Interface:

▼

i

MTU:

1500

Description:

OK

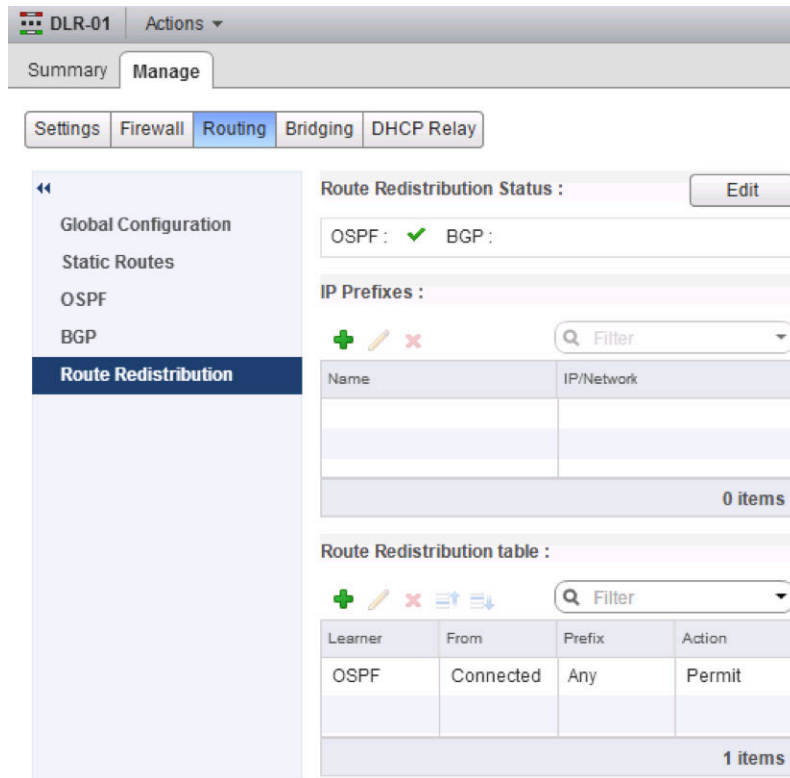
Cancel

Route Redistribution

Wenn Sie der „Tabelle der Route Redistribution“ einen Eintrag hinzufügen, wird dadurch nicht automatisch die Neuverteilung für das ausgewählte „Protokoll für Lernende“ aktiviert. Dies muss explizit mit „Bearbeiten“ für den „Status der Route Redistribution“ vorgenommen werden.

Der DLR ist standardmäßig für die Neuverteilung der verbundenen Routen in OSPF konfiguriert, während dies beim ESG nicht der Fall ist.

Die „Tabelle der Route Redistribution“ wird von oben nach unten verarbeitet; die Verarbeitung wird nach dem ersten Treffer gestoppt. Wenn Sie einige Präfixe von der Neuverteilung ausschließen möchten, fügen Sie im oberen Tabellenbereich spezifischere Einträge ein.



Fehlerbehebung für das NSX-Routing

NSX stellt verschiedene Tools bereit, mit denen Sie sicherstellen können, dass das Routing funktioniert.

Befehlszeilenschnittstelle (CLI) für das NSX-Routing

Mit einer Reihe von CLI-Befehlen kann ein Operator den Ausführungsstatus verschiedener Elemente des NSX-Routing-Subsystems überprüfen.

Aufgrund des verteilten Charakters des NSX-Routing-Subsystems steht eine Vielzahl von CLIs zur Verfügung, auf die von verschiedenen NSX-Komponenten aus zugegriffen werden kann. Seit der Version NSX 6.2 verfügt NSX auch über eine zentrale CLI, mit der sich die erforderliche Zeitspanne für den Zugriff auf verschiedene verteilte Komponenten und für die Anmeldung bei diesen reduzieren lässt. Die CLI bietet einen Zugriff auf die meisten Informationen von einer einzigen Stelle aus: der NSX Manager-Shell.

Überprüfen der Voraussetzungen

Für jeden ESXi-Host müssen zwei grundlegenden Voraussetzungen erfüllt sein:

- Jeder logische Switch, der mit dem DLR verbunden ist, befindet sich in einem fehlerfreien Zustand.
- Der ESXi-Host wurde erfolgreich für VXLAN vorbereitet.

Prüfen des Systemstatus für logische Switches

Das NSX-Routing wird in Verbindung mit logischen NSX-Switches durchgeführt. So überprüfen Sie, ob sich die mit einem DLR verbundenen logischen Switches in einem fehlerfreien Zustand befinden:

- Ermitteln Sie die Segment-ID (VXLAN VNI) für jeden logischen Switch, der mit dem betreffenden DLR verbunden ist (z. B. 5004..5007).

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

- Auf den ESXi-Hosts, auf denen die VMs, die von diesem DLR bedient werden, ausgeführt werden, überprüfen Sie den Status der VXLAN-Steuerungskomponente für die logischen Switches, die mit diesem DLR verbunden sind.

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

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

Überprüfen Sie die folgenden Elemente für jedes infrage kommende VXLAN:

- Für logische Switches im Hybrid- oder Unicast-Modus:
 - Die Steuerungskomponente ist aktiviert (Option „Enabled“).
 - Es sind „multicast proxy“ und „ARP proxy“ aufgelistet. „ARP proxy“ wird auch nach der Deaktivierung von IP Discovery aufgeführt.
 - Eine gültige Controller-IP-Adresse ist unter „Controller“ aufgeführt und die Verbindung ist aktiv (Option „up“ unter „Connection“).
- Die Einstellung für „Port Count“ (Portanzahl) ist korrekt. Sie muss mindestens 1 betragen, auch wenn keine VMs auf diesem Host mit dem betreffenden logischen Switch verbunden sind. Dieser eine Port ist der vdrPort, ein spezieller dvPort, der mit dem Kernelmodul des DLR auf dem ESXi-Host verbunden ist.

- Mit dem im Folgenden aufgeführten Befehl stellen Sie sicher, dass der vdrPort mit jedem infrage kommenden VXLAN verbunden ist.

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

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

- Im obigen Beispiel verfügt VXLAN 5004 über eine VM und eine DLR-Verbindung, während VXLAN 5005 nur eine DLR-Verbindung zur Verfügung steht.
- Überprüfen Sie, ob die erforderlichen VMs korrekt mit ihren entsprechenden VXLANs verbunden sind, z. B. web-sv-01a mit VXLAN 5004

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

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

Überprüfen der VXLAN-Vorbereitung

Das DLR-Kernelmodul wird als Bestandteil einer VXLAN-Konfiguration auf einem ESXi-Host ebenfalls installiert, konfiguriert und mit einem dvPort auf einem DVS verbunden, der für VXLAN vorbereitet wurde.

- 1 Führen Sie `show cluster all` zum Abrufen der Cluster-ID aus.
- 2 Führen Sie `show cluster cluster-id` zum Abrufen der Host-ID aus.
- 3 Führen Sie `show logical-router host hostID connection` zum Abrufen der Statusinformationen aus.

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

Connection Information:
-----

DvsName      VdrPort      NumLifs  VdrVmac
-----
Compute_VDS  vdrPort      4        02:50:56:56:44:52
  Teaming Policy: Default Teaming
```

```
Uplink    : dvUplink1(50331650): 00:50:56:eb:41:d7(Team member)
```

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

- Ein mit VXLAN aktivierter DVS verfügt über einen erstellten vdrPort, der von allen DLR-Instanzen auf diesem ESXi-Host gemeinsam genutzt wird.
- „NumLifs“ (Anzahl der LIFs) bezieht sich auf die Summe der LIFs aller DLR-Instanzen, die auf diesem Host vorhanden sind.
- Bei „VdrVmac“ handelt es sich um den vMAC, den der DLR an allen LIFs für alle Instanzen verwendet. Dieser MAC ist auf allen Hosts identisch. Dieser wird nicht in Frames, die über das physische Netzwerk außerhalb von ESXi-Hosts geleitet werden, dargestellt.
- Für jeden dvUplink eines mit VXLAN aktivierten DVS ist ein entsprechender VTEP vorhanden. Ausgenommen sind Fälle, in denen der LACP/Etherchannel-Teammodus verwendet wird, wenn unabhängig von der Anzahl der dvUplinks nur ein VTEP erstellt wird.
 - Der vom DLR weitergeleitete Datenverkehr (SRC MAC = vMAC) ändert nach dem Verlassen des Hosts den SRC MAC in den pMAC des entsprechenden dvUplink.
 - Beachten Sie, dass der Quellport oder Quell-MAC der ursprünglichen VM zur Bestimmung des dvUplink verwendet wird (dieser wird für jedes Paket in den Metadaten seines DVS beibehalten).
 - Sind mehrere VTEPs auf dem Host vorhanden und ein dvUplink schlägt fehl, wird der dem fehlgeschlagenen dvUplink zugeordnete VTEP zu einem der verbleibenden dvUplinks mit allen VMs verschoben, die mit diesem VTEP verbunden sind. Dadurch werden umfangreiche Änderungen der Steuerungskomponente vermieden, die mit dem Verschieben von VMs zu einem anderen VTEP verbunden wären.
- Die Zahl in „()“ neben jedem „dvUplinkX“ ist die dvPort-Nummer. Dies dient der Paketerfassung auf dem einzelnen Uplink.
- Die für jeden „dvUplinkX“ angezeigte MAC-Adresse ist ein „pMAC“, der diesem dvUplink zugeordnet ist. Diese MAC-Adresse wird für den Datenverkehr vom DLR aus verwendet, wie z. B. für vom DLR generierte ARP-Abfragen sowie für alle Pakete, die vom DLR nach dem Verlassen des ESXi-Hosts weitergeleitet werden. Diese MAC-Adresse wird auf allen physischen Netzwerken dargestellt (direkt, wenn die LIF des DLR vom Typ „VLAN“ ist, oder innerhalb der VXLAN-Pakete für VXLAN-LIFs).
- Pkt Dropped/Replaced/Skipped (Paket verworfen/ersetzt/übersprungen) verweist auf Indikatoren, die sich auf interne Implementierungsdetails des DLR beziehen und in der Regel nicht für die Fehlerbehebung oder die Überwachung verwendet werden.

Kurze Zusammenfassung des Routing

Zur schnellen Behebung von Routing-Problemen ist es hilfreich, die Arbeitsschritte für das Routing und die zugehörigen Informationstabellen zu rekapitulieren.

- 1 Empfangen Sie ein Paket, um es an eine Ziel-IP-Adresse zu senden.

- 2 Überprüfen Sie die Routing-Tabelle und legen Sie die IP-Adresse für den nächsten Hop fest.
- 3 Bestimmen Sie, mit welcher Ihrer Netzwerkschnittstellen dies erreicht werden kann.
- 4 Rufen Sie eine MAC-Adresse für diesen nächsten Hop ab (über ARP).
- 5 Erstellen Sie einen L2 Frame.
- 6 Senden Sie den Frame über die Schnittstelle.

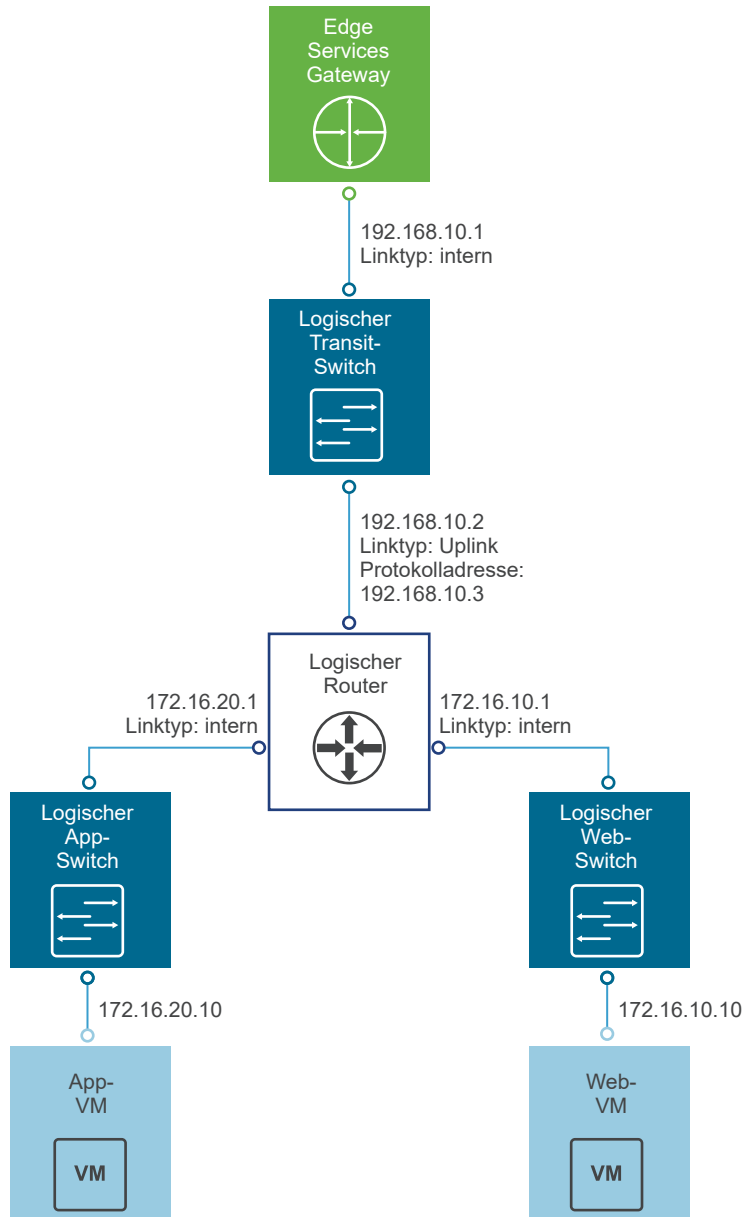
Für das Routing benötigen Sie also:

- Eine Schnittstellentabelle (mit Schnittstellen-IP-Adressen und Netzmasken)
- Eine Routing-Tabelle
- Eine ARP-Tabelle

Überprüfen des DLR-Status mithilfe einer Beispieltopologie für das Routing

In diesem Abschnitt wird beschrieben, wie die Informationen überprüft werden können, die der DLR zum Weiterleiten von Paketen benötigt.

Als Beispiel für eine Routing-Topologie soll eine Gruppe logischer Switches und ein DLR in NSX erstellt werden.

Abbildung 3-7. Beispieltopologie für das Routing

Im Diagramm sind folgende Komponenten dargestellt:

- vier logische Switches, die jeweils über ein eigenes Subnetz verfügen,
- drei VMs, die jeweils mit einem logischen Switch verbunden sind und
 - jeweils eine eigene IP-Adresse und ein IP-Gateway sowie
 - jeweils eine MAC-Adresse (die letzten beiden Oktette werden dargestellt) besitzen.
- Ein DLR ist mit den vier logischen Switches verbunden. Ein logischer Switch ist für die „Uplink“-Verbindung und die übrigen Switches sind für den internen Datenverkehr zuständig.
- Ein externes Gateway, etwa ein ESG, das als Upstream-Gateway für den DLR dient.

Für den obigen DLR wird im Assistenten der Bildschirm „Bereit zum Abschließen“ angezeigt.

New NSX Edge

Ready to complete

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

Management Interface Configuration
 Connected To: Mgmt_Edge_VDS - Mgmt

IP Address	Subnet Prefix Length

NSX Edge Appliances

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

Interfaces

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

Back Next Finish Cancel

Nachdem die Bereitstellung des DLR abgeschlossen ist, kann mit ESXi-CLI-Befehlen der verteilte Status des fraglichen DLR auf den beteiligten Hosts angezeigt und überprüft werden.

Bestätigen der DLR-Instanzen

Als Erstes muss bestätigt werden, dass die DLR-Instanz erstellt wurde und dass seine Steuerungskomponente aktiv ist.

- 1 In der NSX Manager-Shell führen Sie `show cluster all` zum Abrufen der Cluster-ID aus.
- 2 Führen Sie `show cluster cluster-id` zum Abrufen der Host-ID aus.
- 3 Führen Sie `show logical-router host hostID dlr all verbose` zum Abrufen der Statusinformationen aus.

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

```
VDR Instance Information :
```

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


Es muss Folgendes beachtet werden:

- Dieser Befehl stellt alle vorhandenen DLR-Instanzen auf dem jeweiligen ESXi-Host dar.
- „Vdr Name“ (Vdr-Name) besteht aus „Tenant“ + „Edge Id“ (Mandant+Edge-ID). In diesem Beispiel wurde für „Tenant“ (Mandant) keine Angabe gemacht, deshalb ist „default“ (Standard) angegeben. Die „Edge Id“ (Edge-ID) lautet „edge-1“. Diese wird in der NSX-Benutzeroberfläche dargestellt.
 - Befinden sich viele DLR-Instanzen auf einem Host, können Sie zur Ermittlung der gewünschten Instanz die Edge-ID der Benutzeroberfläche „NSX Edges“ entnehmen.
- „Vdr Id“ (Vdr-ID) ist hilfreich für weitere Suchvorgänge, auch nach Protokollen.
- „Number of Lifs“ (Anzahl der LIFs) bezieht sich auf die LIFs dieser speziellen DLR-Instanz.
- Der Wert für „Number of Routes“ (Anzahl der Routen) beträgt in diesem Fall 5. Dabei handelt es sich um vier direkt verbundene Routen (eine für jede LIF) und um eine Standardroute.
- „State“ (Status), „Controller IP“ (Controller IP) und „Control Plane Active“ (Steuerungskomponente aktiv) geben den Status der Steuerungskomponente des DLR an und müssen die korrekte Controller-IP mit der Einstellung „Yes“ (Ja) für „Control Plane Active“ enthalten. Denken Sie daran, dass die DLR-Funktion aktive Controller erfordert. Die oben dargestellte Ausgabe stellt die Voraussetzungen für eine fehlerfreie DLR-Instanz dar.
- „Control Plane IP“ (IP der Steuerungskomponente) verweist auf die IP-Adresse, über die der ESXi-Host mit dem Controller kommuniziert. Bei dieser IP handelt es sich immer um die der Verwaltungs-vmknic des ESXi-Hosts zugeordnete IP. In den meisten Fällen ist dies vmk0.
- „Edge Active“ (Edge aktiv) gibt an, ob es sich bei diesem Host um denjenigen handelt, auf dem die Kontroll-VM für diese DLR-Instanz im aktiven Zustand ausgeführt wird.
 - Die Position der aktiven DLR-Kontroll-VM bestimmt, welcher ESXi-Host für die Ausführung des NSX L2-Bridging (wenn aktiviert) verwendet wird.
- Es ist auch eine „Kurzversion“ des oben dargestellten Befehls verfügbar, die eine komprimierte Variante für einen schnellen Überblick ausgibt. Beachten Sie, dass „Vdr Id“ (Vdr-ID) hier im hexadezimalen Format dargestellt wird:

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

```
VDR Instance Information :
```

```
-----
```

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

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

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

Die Status für „Soft Flush“ geben die kurzlebigen vorübergehenden Statuszustände des LIF-Lebenszyklus an und werden in einem funktionsfähigen DLR in der Regel nicht dargestellt.

Logische Schnittstellen des DLR

Nach der Einrichtung der logischen Schnittstellen, die der DLR erstellt hat, müssen Sie sicherstellen, dass alle logischen Schnittstellen des DRL vorhanden sind und über die erforderliche Konfiguration verfügen.

- 1 In der NSX Manager-Shell führen Sie `show cluster all` zum Abrufen der Cluster-ID aus.
- 2 Führen Sie `show cluster cluster-id` zum Abrufen der Host-ID aus.
- 3 Führen Sie `show logical-router host hostID dlr all brief` zum Abrufen der dlrID (Vdr-Name) aus.
- 4 Führen Sie `show logical-router host hostID dlr dlrID interface all brief` zum Abrufen zusammengefasster Statusinformationen für alle Schnittstellen aus.
- 5 Führen Sie `show logical-router host hostID dlr dlrID interface (all | intName) verbose` zum Abrufen der Statusinformationen für alle Schnittstellen oder für eine bestimmte Schnittstelle aus.

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

```
VDR default+edge-1:1460487509 LIF Information :
```

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

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

```
Name:          570d45550000000b
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5001
Ip(Mask):      172.16.20.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:        Enabled
```

```

Flags:                0x2388
DHCP Relay:           Not enabled

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

```

Es muss Folgendes beachtet werden:

- Der LIF-Name ist für alle DLR-Instanzen auf dem Host einheitlich. Er ist auf den Hosts und auf dem Master-Controller-Knoten des DLR identisch.
- Unter „Mode“ (Modus) wird angezeigt, ob für die LIF das Routing oder das Bridging gültig ist und ob diese vom Typ „Internal“ (Intern) oder „Uplink“ ist.
- „ID“ zeigt den LIF-Typ und die entsprechende Dienst-ID an (VXLAN und VNI, oder VLAN und VID).
- „Ip(Mask)“ (IP-Maske) wird für Routing-LIFs dargestellt.
- Wenn eine LIF mit einem VXLAN im Hybrid- oder Unicast-Modus verbunden ist, wird für „VXLAN Control Plane“ (VXLAN-Steuerungskomponente) „Enabled“ (Aktiviert) angezeigt.
- Für VXLAN-LIFs mit VXLAN im Unicast-Modus ist unter „VXLAN Multicast IP“ (VXLAN-Multicast-IP) „0.0.0.1“ angegeben. Ansonsten wird die tatsächliche Multicast-IP-Adresse dargestellt.
- Unter „State“ (Status) muss für Routing-LIFs „Enabled“ (Aktiviert) angezeigt sein. Für Bridging-LIFs gilt „Enabled“ (Aktiviert) für den Host, der das Bridging ausführt, und „Init“ (Initialisieren) für alle anderen Hosts.
- „Flags“ bietet eine zusammenfassende Darstellung des LIF-Status. Es werden folgende Informationen für die LIF angezeigt:
 - Routing- oder Bridging-Modus
 - Ob es sich bei der VLAN-LIF um eine DI (designierte Instanz) handelt
 - Ob dafür das DHCP-Relay aktiviert ist
 - Beachten Sie das Flag 0x0100, das gesetzt wird, wenn ein VXLAN-VNI-Beitritt durch den DLR veranlasst wurde (im Gegensatz zu einem Host mit einer VM auf diesem VXLAN)
 - Flags werden zur besseren Lesbarkeit in einer „Kurzfassung“ dargestellt.

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

```
VDR default+edge-1 LIF Information :
```

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

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

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

Lif Name	Id	Mode	State	Ip(Mask)
-----	--	-----	-----	-----
570d455500000000a	Vxlan:5001	R,D,In	A	172.16.10.1(255.255.255.0)
570d455500000000c	Vxlan:5003	R,D,In	A	172.16.30.1(255.255.255.0)
570d455500000000b	Vxlan:5002	R,D,In	A	172.16.20.1(255.255.255.0)
570d4555000000002	Vxlan:5000	R,D,Up	A	192.168.10.5(255.255.255.248)

DLR-Routen

Nachdem Sie sichergestellt haben, dass ein DLR vorhanden ist, sich in einem fehlerfreien Zustand befindet und über alle LIFs verfügt, müssen Sie als Nächstes die Routing-Tabelle überprüfen.

- 1 In der NSX Manager-Shell führen Sie `show cluster all` zum Abrufen der Cluster-ID aus.
- 2 Führen Sie `show cluster cluster-id` zum Abrufen der Host-ID aus.
- 3 Führen Sie `show logical-router host hostID dlr all brief` zum Abrufen der dlrID (Vdr-Name) aus.
- 4 Führen Sie `show logical-router host hostID dlr dlrID route` zum Abrufen der Statusinformationen für alle Schnittstellen aus.

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

VDR default+edge-1:1460487509 Route Table

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

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

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
-----	-----	-----	-----	---	-----	-----	-----
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	10068944	570d4555000000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000a
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000b
172.16.30.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000000c
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10068944	570d4555000000002

Es muss Folgendes beachtet werden:

- „Interface“ (Schnittstelle) zeigt die Egress-LIF an, die für das entsprechende unter „Destination“ (Ziel) dargestellte Ziel ausgewählt wird. Dafür wird der Name einer LIF des DLR verwendet.
- Für ECMP-Routen sind mehrere Routen mit demselben Ziel, mit derselben GenMask und Schnittstelle, aber mit einem anderen Gateway verfügbar. Zu den Flags gehört auch das Flag „E“, das für den ECMP-Typ dieser Routen steht.

ARP-Tabelle des DLR

Für die vom DLR weitergeleiteten Pakete muss der DLR ARP-Anforderungen für die IP-Adresse des nächsten Hop auflösen können. Die Ergebnisse dieses Auflösungs Vorgangs werden lokal auf den DLR-Instanzen der einzelnen Hosts gespeichert.

Controller spielen für diesen Vorgang keine Rolle. Sie werden nicht zur Verteilung der Ergebnisse von ARP-Einträgen auf andere Hosts benötigt.

Inaktive zwischengespeicherte Einträge werden nach 600 Sekunden entfernt. Weitere Informationen zur ARP-Auflösung für DLRs finden Sie unter [ARP-Auflösung für DLRs](#).

- 1 In der NSX Manager-Shell führen Sie `show cluster all` zum Abrufen der Cluster-ID aus.
- 2 Führen Sie `show cluster cluster-id` zum Abrufen der Host-ID aus.
- 3 Führen Sie `show logical-router host hostID dlr all brief` zum Abrufen der dlrID (Vdr-Name) aus.
- 4 Führen Sie `show logical-router host hostID dlr dlrID arp` zum Abrufen der Statusinformationen für alle Schnittstellen aus.

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

VDR default+edge-1:1460487509 ARP Information :

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

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

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

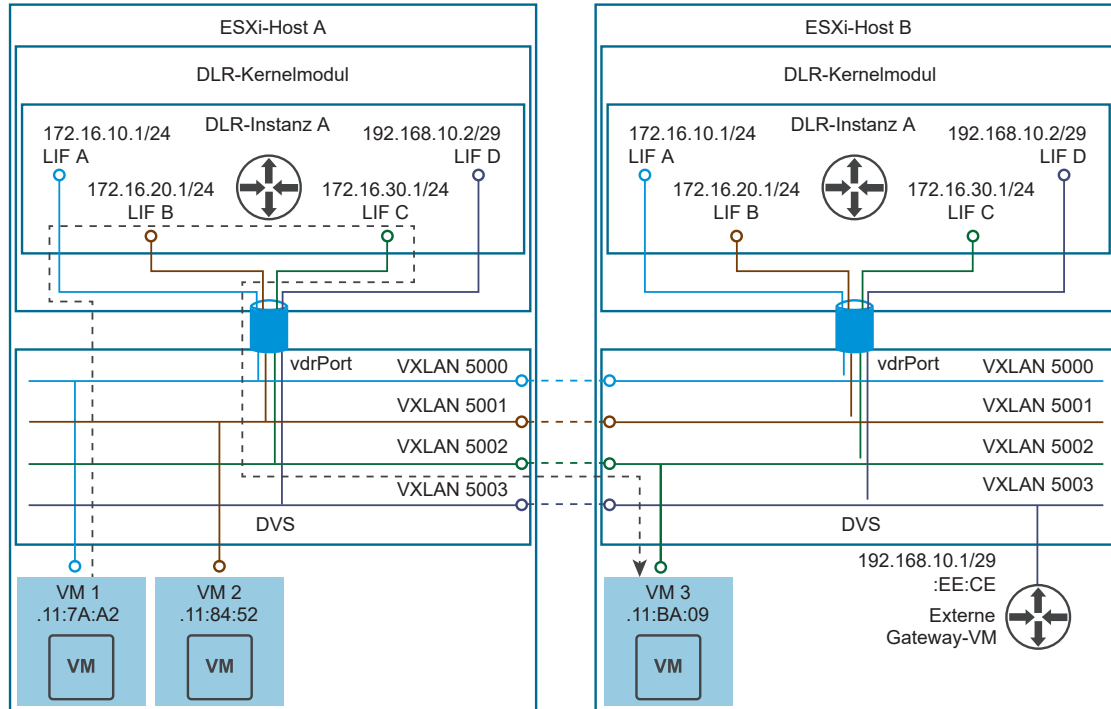
Beachten Sie folgende Hinweise:

- Alle ARP-Einträge für die eigenen LIFs (Flag „I“) des DLR sind identisch und enthalten denselben vMAC, der in [Überprüfen der VXLAN-Vorbereitung](#) erläutert wurde.
- ARP-Einträge mit dem Flag „L“ entsprechen den VMs, die auf dem Host ausgeführt werden, auf dem auch der CLI-Befehl ausgeführt wird.
- „SrcPort“ zeigt die ID des dvPort an, an dem der ARP-Eintrag ursprünglich erstellt wurde. Wenn der ARP-Eintrag von einem anderen Host stammt, wird die dvPort-ID des dvUplink angezeigt. Auf diese dvPort-ID kann mit der dvPort-ID des dvUplink, die in [Überprüfen der VXLAN-Vorbereitung](#) erläutert wurde, verwiesen werden.
- Das Flag „Nascent“ (Im Entstehen begriffen) wird in der Regel nicht ausgewertet. Es wird gesetzt, während der DLR auf die Ankunft der ARP-Antwort wartet. Alle Einträge mit diesem Flag sind eventuell ein Hinweis auf ein Problem mit der ARP-Auflösung.

DLR und seine zugehörigen Hostkomponenten (illustriert)

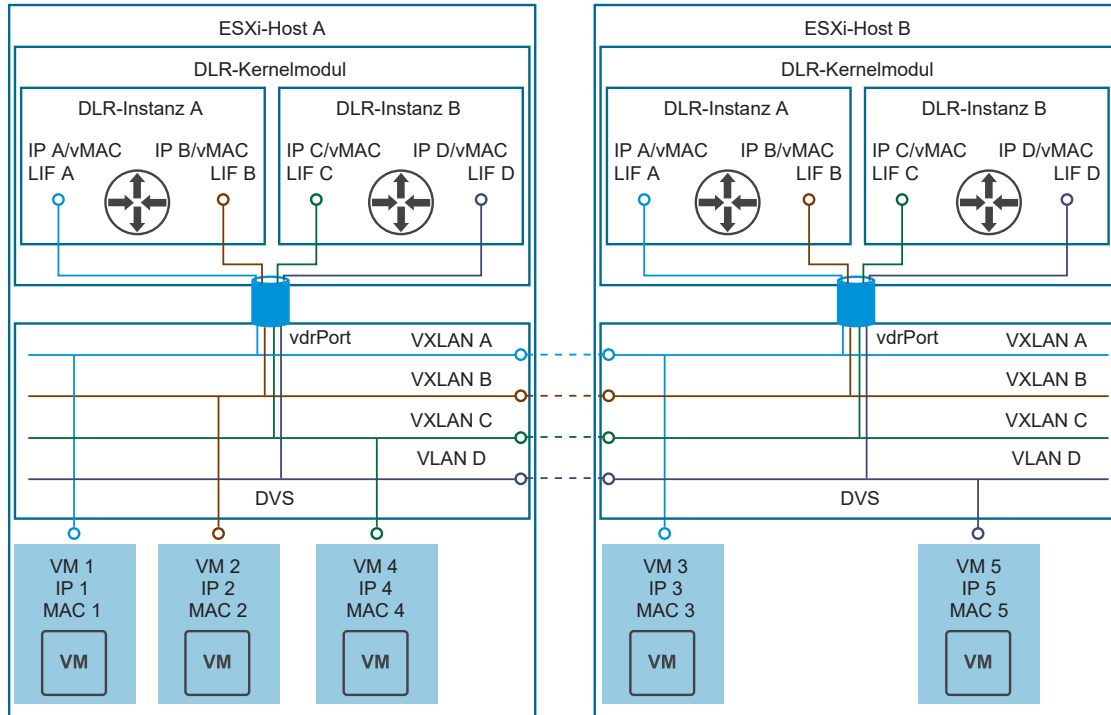
Das nachfolgende Diagramm stellt zwei Hosts dar, ESXi-Host A und ESXi-Host B, auf denen die „DLR-Instanz A“ des Beispiels konfiguriert und mit den vier VXLAN-LIFs verbunden ist.

Abbildung 3-8. Zwei Hosts mit einer einzigen DLR-Instanz

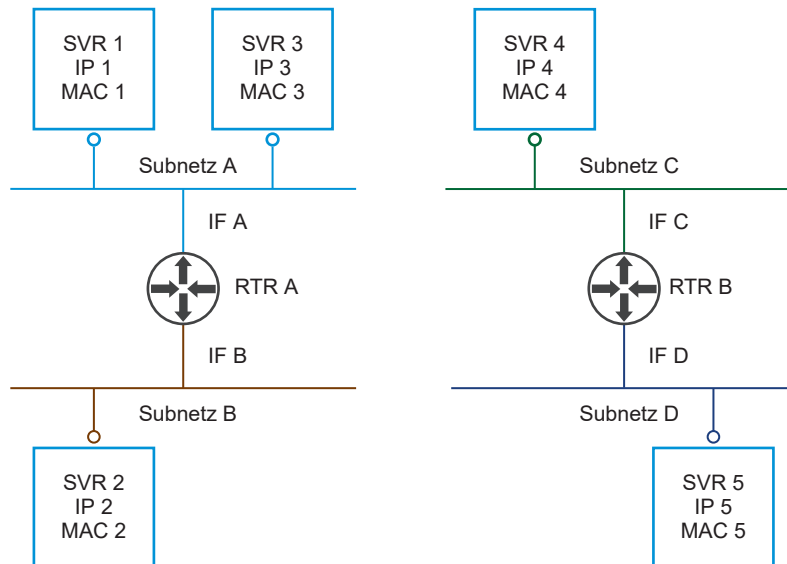


- Jeder Host verfügt über einen „L2 Switch“ (DVS) und einen „Router-on-a-Stick“ (DLR-Kernelmodul), der mit diesem „Switch“ über eine „Trunk“-Schnittstelle verbunden ist (vdrPort).
 - Beachten Sie, dass dieser „Trunk“ Übertragungen sowohl für VLANs wie auch für VXLANs durchführen kann. Allerdings sind in den Paketen, die den vdrPort durchlaufen, keine 801.Q- oder UDP/VXLAN-Kopfzeilen vorhanden. Stattdessen verwendet der DVS eine interne Methode zur Kennzeichnung von Metadaten, um diese Informationen an das DLR-Kernelmodul weiterzugeben.
- Wenn der DVS einen Frame mit „Ziel-MAC = vMAC“ erkennt, geht er davon aus, dass dieser Frame für den DLR bestimmt ist, und leitet ihn an den vdrPort weiter.
- Nachdem die Pakete über den vdrPort im DLR-Kernelmodul angekommen sind, wird aus deren Metadaten der VXLAN-VNI oder die VLAN-ID ermittelt, zu dem bzw. zu der sie gehören. Mit diesen Informationen wird dann festgestellt, zu welcher LIF welcher DLR-Instanz dieses Paket gehört.
 - Als Nebeneffekt dieses Systems kann nur eine DLR-Instanz mit einem bestimmten VLAN oder VXLAN verbunden werden.

Sind mehrere DLR-Instanzen vorhanden, hat das Diagramm folgendes Aussehen:

Abbildung 3-9. Zwei Hosts mit zwei DLR-Instanzen

Dies entspricht einer Netzwerktopologie mit zwei unabhängigen Routing-Domänen, die komplett getrennt voneinander betrieben werden, wobei sich die IP-Adressen potenziell überlappen.

Abbildung 3-10. Netzwerktopologie, die zwei Hosts und zwei DLR-Instanzen entspricht

Architektur des Subsystems für verteiltes Routing

DLR-Instanzen auf ESXi-Hosts haben Zugriff auf alle Informationen, die für die Ausführung des L3-Routings benötigt werden.

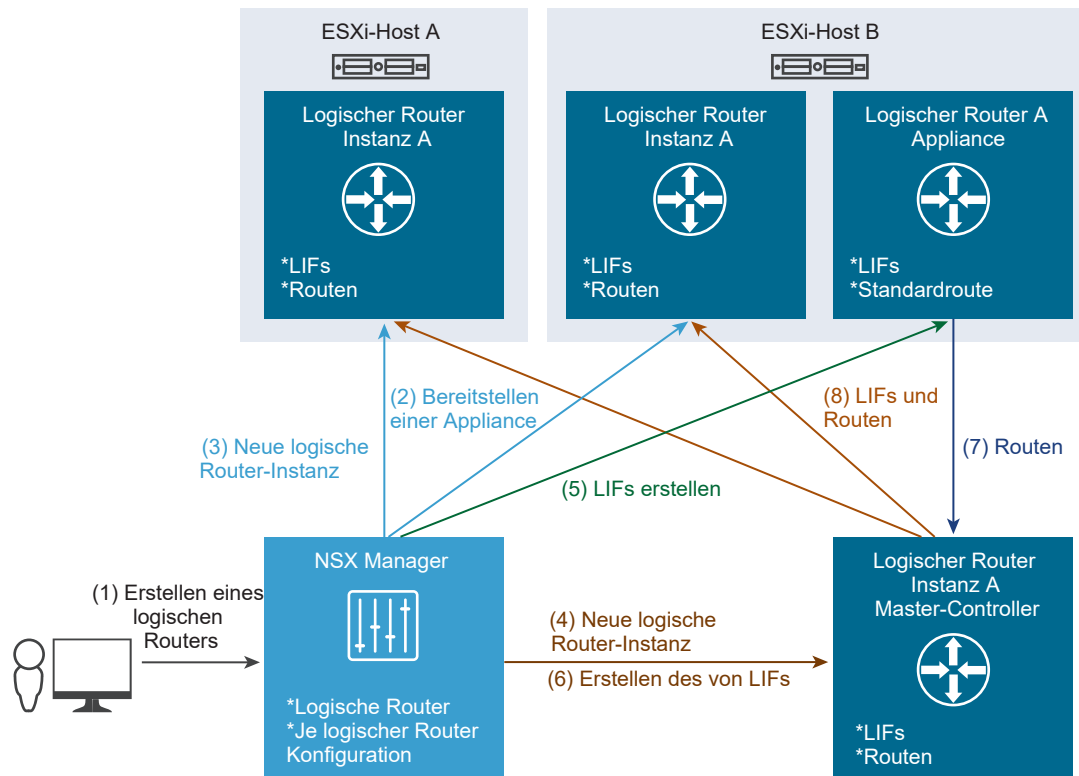
- Netzwerke werden direkt verbunden (auf der Basis der Schnittstellenkonfiguration)
- Nächste Hops für jedes Subnetz (in der Routing-Tabelle ermittelt)
- MAC-Adresse zum Einfügen in Egress-Frames zum Erreichen der nächsten Hops (ARP-Tabelle)

Diese Informationen werden den Instanzen übermittelt, die über mehrere ESXi-Hosts verteilt sind.

Erstellen eines DLR

Das nachfolgende Diagramm stellt den Vorgang für das Erstellen eines neuen DLR mit NSX auf oberster Ebene grafisch dar.

Abbildung 3-11. Erstellen eines DLR



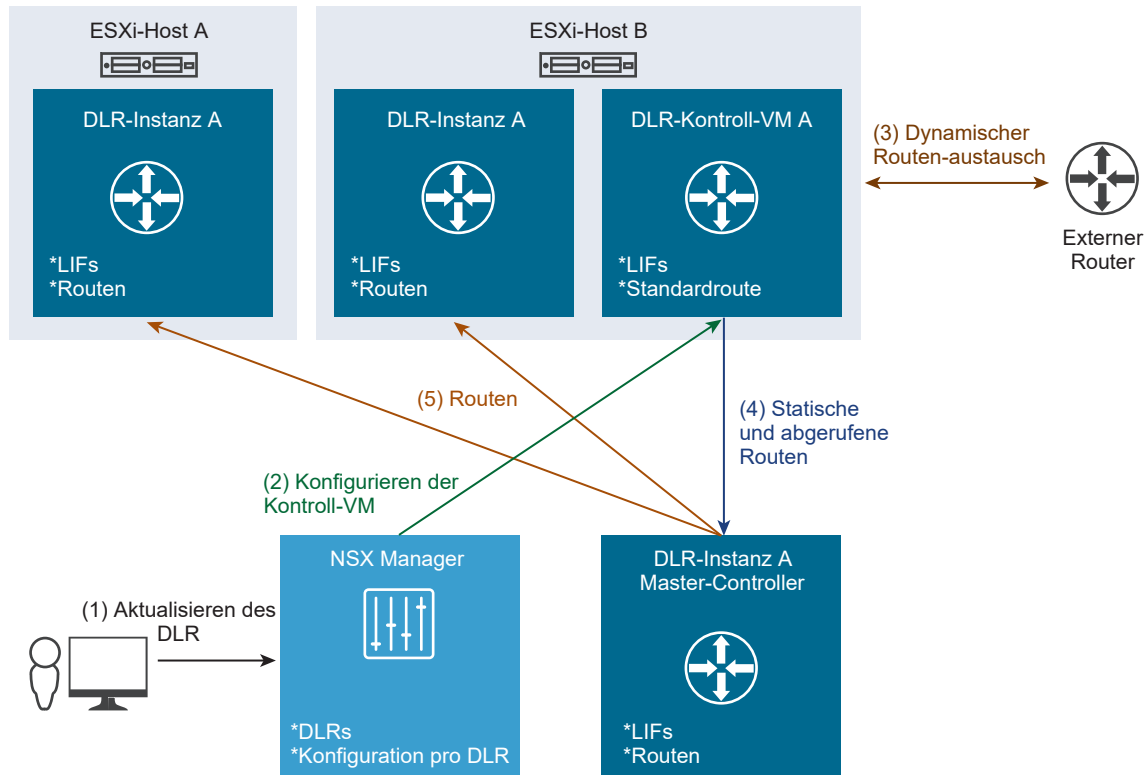
Wenn ein Assistent der Benutzeroberfläche mit der Schaltfläche „Beenden“ abgeschlossen oder ein API-Aufruf zum Bereitstellen eines neuen DLR durchgeführt wurde, werden vom System folgende Schritte ausgeführt:

- 1 NSX Manager erhält einen API-Aufruf zum Bereitstellen eines neuen DLR (direkt oder vom durch den Assistenten der Benutzeroberfläche aufgerufenen vSphere Web Client).

- 2 NSX Manager ruft den mit ihm verbundenen vCenter Server zum Bereitstellen einer DLR-Kontroll-VM auf (oder ein HA-Paar, wenn HA angefordert wurde).
 - a Die DLR-Kontroll-VM wird eingeschaltet und mit dem NSX Manager zurück verbunden. Sie kann dann die Konfiguration empfangen.
 - b Wenn ein HA-Paar bereitgestellt wurde, konfiguriert NSX Manager eine Anti-Affinitätsregel, mit der die Ausführung des HA-Paars auf verschiedenen Hosts gewährleistet ist. Der DRS trennt diese dann.
- 3 NSX Manager erstellt eine DLR-Instanz auf den Hosts:
 - a NSX Manager sucht nach den logischen Switches, die mit dem neuen DLR verbunden werden sollen, um deren Transportzone festzustellen.
 - b Anschließend wird nach einer Liste von Clustern gesucht, die in dieser Transportzone konfiguriert wurden, und der neue DLR wird auf jedem Host in diesen Clustern erstellt.
 - c An dieser Stelle kennen die Hosts nur die neue DLR-ID. Sie verfügen über keine zugehörigen Informationen (LIFs oder Routen).
- 4 NSX Manager erstellt eine neue DLR-Instanz auf dem Controller-Cluster.
 - a Der Controller-Cluster bestimmt einen der Controller-Knoten als Master für diese DLR-Instanz.
- 5 NSX Manager sendet die Konfiguration inklusive der LIFs zur DLR-Kontroll-VM.
 - a Die ESXi-Hosts (inklusive jener, auf denen die DLR-Kontroll-VM ausgeführt wird) erhalten in Teilschritten Informationen vom Controller-Cluster, ermitteln, welcher Controller-Knoten für die neue DLR-Instanz zuständig ist, und stellen eine Verbindung mit dem Controller-Knoten her (wenn keine Verbindung vorhanden ist).
- 6 Nach dem Erstellen der LIF in der DLR-Kontroll-VM legt der NSX Manager die LIFs des neuen DLR auf dem Controller-Cluster an.
- 7 Die DLR-Kontroll-VM stellt eine Verbindung mit dem Controller-Knoten der neuen DLR-Instanz her und sendet die Routen zum Controller-Knoten:
 - a Als Erstes übersetzt der DLR seine Routing-Tabelle in die Weiterleitungstabelle (durch Auflösung der Präfixe für die LIFs).
 - b Anschließend sendet der DLR die sich daraus ergebende Tabelle zum Controller-Knoten.
- 8 Der Controller-Knoten überträgt die LIFs und Routen über die in Schritt 5a eingerichtete Verbindung zu den anderen Hosts, auf denen die neue DLR-Instanz vorhanden ist.

Hinzufügen des dynamischen Routings zu einem DLR

Wenn der DLR über einen „direkten“ API-Aufruf erstellt wird (und nicht mit der Benutzeroberfläche des vSphere Web Client), kann er mit einer vollständigen Konfiguration ausgestattet werden, die auch das dynamische Routing umfasst(1).

Abbildung 3-12. Dynamisches Routing auf dem DLR

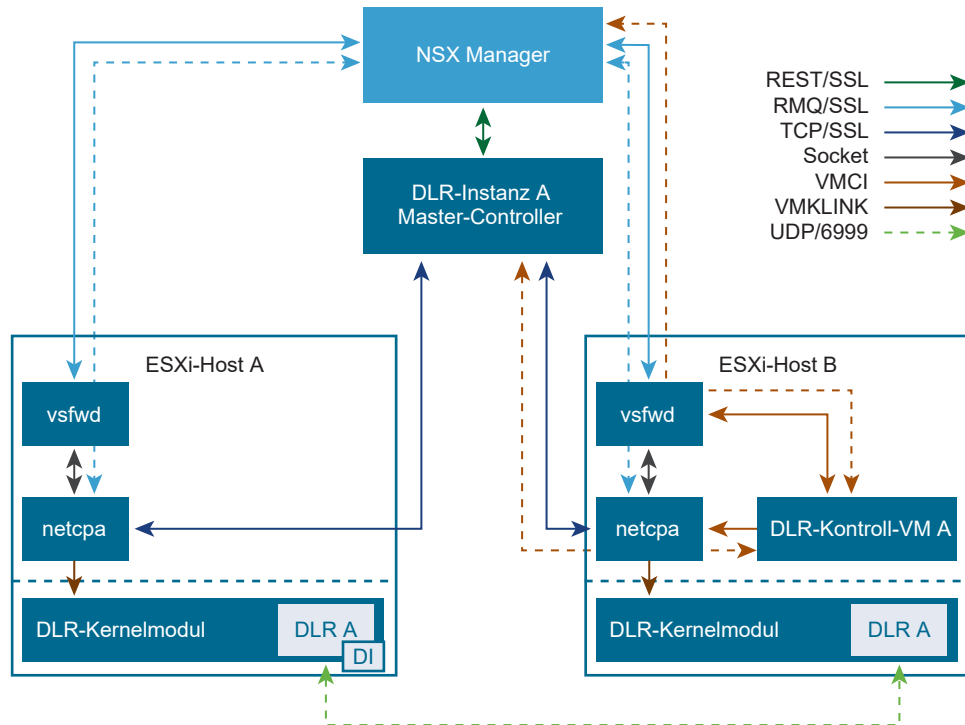
- 1 Der NSX Manager erhält einen API-Aufruf zum Ändern der vorhandenen DLR-Konfiguration, in diesem Fall durch Hinzufügen des dynamischen Routings.
- 2 Der NSX Manager sendet die neue Konfiguration an die DLR-Kontroll-VM.
- 3 Die DLR-Kontroll-VM wendet die Konfiguration an und durchläuft den Vorgang zum Einrichten von Routing-Nachbarschaften, zum Austausch von Routing-Informationen, etc.
- 4 Nach dem Austausch von Routing-Informationen berechnet die DLR-Kontroll-VM die Weiterleitungstabelle und sendet diese an den Master-Controller-Knoten des DLR.
- 5 Der Master-Controller-Knoten des DLR verteilt die aktualisierten Routen dann auf die ESXi-Hosts, auf denen sich die DLR-Instanz befindet.

Beachten Sie, dass die DLR-Instanz auf dem ESXi-Host, auf dem die DLR-Kontroll-VM ausgeführt wird, ihre LIFs und Routen nur vom Master-Controller-Knoten des DLR erhält, also nicht direkt von der DLR-Kontroll-VM oder vom NSX Manager.

Elemente und Kommunikationskanäle der DRL-Steuerungs- und Verwaltungskomponenten

Dieser Abschnitt bietet einen kurzen Überblick über die Elemente der DRL-Steuerungs- und Verwaltungskomponenten.

Die Abbildung stellt die Elemente und die entsprechenden Kommunikationskanäle zwischen ihnen dar.

Abbildung 3-13. Elemente der DRL-Steuerungs- und Verwaltungskomponenten

- **NSX Manager:**
 - Verfügt über direkte Kommunikationskanäle mit dem Controller-Cluster
 - Verfügt über eine direkte ständige Verbindung mit dem Nachrichtenbus-Client-Vorgang (vsfwd), der auf jedem für NSX vorbereiteten Host ausgeführt wird
- Für jede DLR-Instanz ist ein Controller-Knoten (von drei verfügbaren) als Master ausgewählt
 - Die Master-Funktion kann einem anderen Controller-Knoten übertragen werden, wenn der ursprüngliche Controller-Knoten fehlschlägt
- Auf jedem ESXi-Host werden zwei Benutzerwelt-Agenten (UWAs, User World Agents) ausgeführt: der Nachrichtenbus-Client (vsfwd) und der Steuerungskomponenten-Agent (netcpa)
 - Der netcpa-Agent benötigt für die Ausführung Informationen vom NSX Manager (z. B. wo die Controller zu finden sind und wie er für diese authentifiziert wird); auf diese Informationen wird über die von vsfwd zur Verfügung gestellte Nachrichtenbusverbindung zugegriffen
 - netcpa kommuniziert auch mit dem DLR-Kernelmodul für dessen Programmierung mit den erforderlichen Informationen, die es von den Controllern erhält
- Für jede DLR-Instanz ist eine DLR-Kontroll-VM vorhanden, die auf einem der ESXi-Hosts ausgeführt wird. Die DLR-Kontroll-VM verfügt über zwei Kommunikationskanäle:
 - Ein VMCi-Kanal zum NSX Manager über vsfwd, der für die Konfiguration der Kontroll-VM verwendet wird

- Ein VMCI-Kanal zum DLR-Master-Controller über netcpa, der zum Versenden der Routing-Tabelle des DLR zum Controller verwendet wird
- Verfügt der DLR über eine VLAN-LIF, wird einer der beteiligten ESXi-Hosts vom Controller als DI (designierte Instanz) ausgewählt. Das DLR-Kernelmodul auf den anderen ESXi-Hosts erfordert eine Durchführung von Proxy-ARP-Abfragen durch die DI auf dem zugeordneten VLAN.

Komponenten des NSX-Routing-Subsystems

Das NSX-Routing-Subsystem wird durch mehrere Komponenten aktiviert.

- NSX Manager
- Controller-Cluster
- ESXi-Hostmodule (Kernel und UWA)
- DLR-Kontroll-VMs
- ESGs

NSX Manager

NSX Manager stellt folgende Funktionen für das NSX-Routing bereit:

- Zentrale Verwaltungskomponente mit einem einheitlichen API-Zugriffspunkt für alle NSX-Verwaltungsvorgänge
- Installation des Kernelmoduls für das verteilte Routing und die Benutzerwelt-Agenten (UWAs, User World Agents) auf den Hosts zu deren Vorbereitung für die NSX-Funktionen
- Erstellen/Löschen von DLRs und DLR-LIFs
- Bereitstellen/Löschen der DLR-Kontroll-VM sowie des ESG über vCenter
- Konfiguration des Controller-Clusters über eine REST API und der Hosts über einen Nachrichtenbus:
 - Ausstattung des Steuerungskomponenten-Agenten für den Host mit den IP-Adressen von Controllern
 - Generierung der Zertifikate zum Schutz der Kommunikation der Steuerungskomponente und deren Verteilung an Hosts und Controller
- Konfiguration von ESGs und DLR-Kontroll-VMs über den Nachrichtenbus
 - Beachten Sie, dass ESGs auf nicht vorbereiteten Hosts bereitgestellt werden können; in diesem Fall wird VIX anstelle des Nachrichtenbus verwendet

Controller-Cluster

Das verteilte NSX-Routing erfordert Controller, die nach Skalierung und Verfügbarkeit gruppiert sind und die folgenden Funktionen bereitstellen:

- Unterstützung von VXLAN und einer Steuerungskomponente für das verteilte Routing
- CLI-Schnittstelle für Statistiken und Laufzeitstatus

- Auswahl eines Master-Controller-Knotens für jede DLR-Instanz
 - Master-Controller erhalten Routing-Informationen von der DLR-Kontroll-VM und verteilen diese an die Hosts
 - Senden der LIF-Tabelle an die Hosts
 - Permanente Erfassung des Hosts, auf dem sich die DLR-Kontroll-VM befindet
 - Auswahl der designierten Instanz für VLAN-LIFs und Übergabe dieser Informationen an die Hosts, Überwachung des DI-Hosts über „Keep-alives“ der Steuerungskomponente (der Zeitüberschreitungswert beträgt 30 Sekunden, die Nachweiszeit zwischen 20-40 Sekunden), Senden eines Updates an Hosts, wenn der ausgewählte DI-Host nicht mehr vorhanden ist

ESXi-Hostmodule

Das NSX-Routing nutzt direkt zwei Benutzerwelt-Agenten (UWAs, User World Agents) sowie ein Routing-Kernelmodul und benötigt das VXLAN-Kernelmodul für die VXLAN-Konnektivität.

Im Folgenden finden Sie eine Zusammenfassung der Funktion der einzelnen Komponenten:

- Der Steuerungskomponenten-Agent (netcpa) ist ein TCP-Client (SSL), der mit dem Controller mithilfe des Steuerungskomponentenprotokolls kommuniziert. Damit lässt sich eine Verbindung mit mehreren Controllern herstellen. netcpa kommuniziert mit dem Nachrichtenbus-Client (vsfwd), um vom NSX Manager Informationen zur Steuerungskomponente abzurufen.
- netcpa-Packaging und -Bereitstellung:
 - Der Agent ist Bestandteil des VXLAN-VIB (vSphere-Installationspaket)
 - Wird vom NSX Manager im Rahmen der Hostvorbereitung über EAM (ESX Agency Manager) installiert
 - Wird als Dienst-Daemon auf ESXi-netcpa ausgeführt
 - Kann über sein Startskript /etc/init.d/netcpad gestartet/angehalten/abgefragt werden
 - Kann remote über „Networking and Security“ > „UI-Installation“ -> „Hostvorbereitung“ -> „Installationsstatus“ auf einzelnen Hosts oder in einem kompletten Cluster neu gestartet werden
- Das DLR-Kernelmodul (vdrb) ist in DVS zur Aktivierung der L3-Weiterleitung integriert
 - Mit netcpa konfiguriert
 - Als Bestandteil der VXLAN-VIB-Bereitstellung installiert
 - Wird mit dem DVS über einen speziellen Trunk namens „vdrPort“ verbunden, der sowohl VLANs als auch VXLANs unterstützt
 - Verfügt über Informationen zu DLR-Instanzen (pro Instanz):
 - LIF und Routentabellen
 - Lokaler ARP-Cache auf Host

- Der Nachrichtenbus-Client (vsfwd) wird von netcpa, ESGs und DLR-Kontroll-VMs zur Kommunikation mit dem NSX Manager verwendet
 - vsfwd ruft die IP-Adresse des NSX Manager, die von vCenter über vpxa/hosd festgelegt wurde, von /UserVars/RmqIpAddress ab und meldet sich beim Nachrichtenbusserver mithilfe der Host-spezifischen Anmeldedaten, die in anderen /UserVars/Rmq*-Variablen gespeichert sind, an
- Der auf einem ESXi-Host ausgeführte netcpa-Agent benötigt vsfwd für folgende Aufgaben:
 - Abrufen des privaten SSL-Schlüssels der Steuerungskomponente für den Host und des Zertifikats vom NSX Manager. Diese sind in /etc/vmware/ssl/rui-for-netcpa gespeichert*
 - Abrufen der IP-Adressen und SSL-Fingerabdrücke von Controllern vom NSX Manager. Diese sind in /etc/vmware/netcpa/config-by-vsm.xml gespeichert
 - Erstellen und Löschen von DLR-Instanzen auf seinem Host nach Anweisungen vom NSX Manager
- Packaging und Bereitstellung
 - Wie bei netcpa, Teil des VXLAN-VIB
 - Wird als Dienst-Daemon auf ESXi- vsfwd ausgeführt
 - Kann über sein Startskript /etc/init.d/ vShield-Stateful-Firewall gestartet/angehalten/abgefragt werden
- ESGs und DLR-Kontroll-VMs verwenden den VMCI-Kanal für vsfwd zum Empfang der Konfiguration vom NSX Manager

DLR-Kontroll-VMs und ESGs

- Die DLR-Kontroll-VM ist ein „Routenverarbeitungsmodul“ für seine DLR-Instanz
 - Verfügt über einen „Platzhalter“ oder über „echte“ vNIC-Schnittstellen für jede DLR-LIF zusammen mit der IP-Konfiguration
 - Kann eines von zwei verfügbaren dynamischen Routing-Protokollen (BGP oder OSPF) ausführen und/oder statische Routen verwenden
 - Erfordert mindestens eine „Uplink“-LIF, um OSPF oder BGP ausführen zu können
 - Berechnet die Weiterleitungstabelle von direkt verbundenen (LIF-) Subnetzen, statischen sowie dynamischen Routen und sendet diese über seinen VMCI-Link an netcpa zum Master-Controller der DLR-Instanz
 - Unterstützt die HA in der Aktiv/Standby-VM-Paarkonfiguration
- Das ESG ist ein eigenständiger Router in einer VM
 - Vollständig unabhängig vom NSX-DLR-Routing-Subsystem (keine Integration der NSX-Steuerungskomponente)
 - Wird in der Regel als Upstream-Gateway für einen oder mehrere DLRs verwendet
 - Unterstützt mehrere gleichzeitig ausgeführte dynamische Routing-Protokolle

Steuerungskomponenten-CLI für das NSX-Routing

Zusätzlich zu den Hostkomponenten verwendet das NSX-Routing Dienste des Controller-Clusters und der DLR-Kontroll-VMs, die jeweils Informationen für die DLR-Steuerungskomponente liefern und über eine eigene CLI zu deren Auswertung verfügen.

Master-Controller der DLR-Instanz

Jede DLR-Instanz wird durch einen der Controller-Knoten bedient. Mit den folgenden CLI-Befehlen können Sie Informationen dieses Controller-Knotens für die DLR-Instanz anzeigen lassen, als deren Master er fungiert.

```
nsx-controller # show control-cluster logical-routers instance 1460487509
LR-Id      LR-Name      Hosts[]      Edge-Connection Service-Controller
1460487509 default+edge-1 192.168.210.57      192.168.110.201
              192.168.210.51
              192.168.210.52
              192.168.210.56
              192.168.110.51
              192.168.110.52

nsx-controller # show control-cluster logical-routers interface-summary 1460487509
Interface      Type  Id      IP[]
570d455500000002  vxlan  5003    192.168.10.2/29
570d45550000000b  vxlan  5001    172.16.20.1/24
570d45550000000c  vxlan  5002    172.16.30.1/24
570d45550000000a  vxlan  5000    172.16.10.1/24

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

- Der Unterbefehl „instance“ des Befehls „show control-cluster logical-routers“ stellt eine Liste der Hosts dar, die mit diesem Controller für diese DLR-Instanz verbunden sind. In einer ordnungsgemäß funktionierenden Umgebung enthält diese Liste alle Hosts von allen Clustern, in denen der DLR vorhanden ist.
- Der Unterbefehl „interface-summary“ zeigt die LIFs an, die der Controller vom NSX Manager abgerufen hat. Diese Informationen werden an die Hosts gesendet.
- Der Unterbefehl „routes“ zeigt die Routing-Tabelle an, die zu diesem Controller durch diese DLR-Kontroll-VM gesendet wird. Beachten Sie, dass diese Tabelle mit Ausnahme des ESXi-Hosts keine direkt verbundenen Subnetze enthält, da diese Informationen von der LIF-Konfiguration bereitgestellt werden.

DLR-Kontroll-VM

Die DLR-Kontroll-VM verfügt über LIFs und Routing-/Weiterleitungstabellen. Die wesentliche Ausgabe im Lebenszyklus der DLR-Kontroll-VM ist die DLR-Routing-Tabelle, die aus Schnittstellen und Routen besteht.

```
edge-1-0> show ip route

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

Total number of routes: 5

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

edge-1-0> show ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route
R>* 0.0.0.0/0 via 192.168.10.1, vNic_2
C>* 172.16.10.0/24 is directly connected, VDR
C>* 172.16.20.0/24 is directly connected, VDR
C>* 172.16.30.0/24 is directly connected, VDR
C>* 192.168.10.0/29 is directly connected, vNic_2
```

- In der Weiterleitungstabelle wird angezeigt, welche DLR-Schnittstelle als Egress für ein bestimmtes Zielsubnetz gewählt wurde.
 - Die „VDR“-Schnittstelle wird für alle LIFs vom Typ „Intern“ dargestellt. Die „VDR“-Schnittstelle ist eine „Pseudo-Schnittstelle“, die keiner vNIC entspricht.

Die Schnittstellen der DLR-Kontroll-VM können wie folgt dargestellt werden:

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



```

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

Interface vNic_2 is up, line protocol is up
  index 9 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:ae:08
  inet 192.168.10.2/29
  inet6 fe80::250:56ff:fe8e:ae08/64
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 361446, bytes 30167226, dropped 0, multicast packets 361168
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 361413, bytes 30287912, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

```

Wichtige Hinweise:

- Der „VDR“-Schnittstelle ist keine VM-NIC (vNIC) zugeordnet. Es handelt sich um eine einzelne „Pseudo-Schnittstelle“, die mit allen IP-Adressen für alle „internen“ LIFs des DLR konfiguriert wurde.
- Die Schnittstelle vNic_0 in diesem Beispiel ist die HA-Schnittstelle.
 - Die Ausgabe oben ist das Ergebnis eines mit aktivierter HA bereitgestellten DLR. Der HA-Schnittstelle wurde eine IP-Adresse zugewiesen. Diese wird in Form von zwei IP-Adressen dargestellt: 169.254.1.1/30 (automatisch für die HA zugewiesen) und 10.10.10.1/24 (manuell der HA-Schnittstelle zugewiesen).
 - Bei einem ESG kann der Operator manuell eine seiner vNICs als HA zuweisen oder standardmäßig das System automatisch aus verfügbaren „internen“ Schnittstellen auswählen lassen. Ohne Schnittstellen des Typs „Intern“ ist keine HA möglich.
- Die Schnittstelle vNic_2 ist vom Typ „Uplink“, deshalb wird sie als eine „echte“ vNIC behandelt.
 - Beachten Sie, dass die an dieser Schnittstelle angezeigte IP-Adresse mit jener der LIF des DLR übereinstimmt. Allerdings antwortet die DLR-Kontroll-VM nicht auf ARP-Abfragen für die IP-Adresse der LIF (in diesem Fall 192.168.10.2/29). Dies ist die Folge eines ARP-Filters, der für die MAC-Adresse dieser vNIC gültig ist.

- Der oben genannte Status gilt solange, bis ein dynamisches Routing-Protokoll für den DLR konfiguriert wird, bei dem die IP-Adresse zusammen mit dem ARP-Filter entfernt und mit der Adresse „Protocol IP“ ersetzt wird, die bei der Konfiguration des dynamisches Routing-Protokolls angegeben wurde.
- Diese vNIC wird vom dynamischen Routing-Protokoll, das in der DLR-Kontroll-VM ausgeführt wird, für die Kommunikation mit den anderen Routern zum Ankündigen und Abrufen von Routen verwendet.
- Nach der Trennung des Edge und dem HA-Failover wird die IP-Adresse der getrennten Edge-Schnittstelle aus der Routing Information Base (RIB) bzw. der Forwarding Information Base (FIB) des aktiven Edge entfernt. Die IP wird jedoch nicht aus der FIB-Tabelle des Standby-Edge entfernt und wird immer noch mit dem Befehl `show ip forwarding` angezeigt. Dies ist das erwartete Verhalten.

NSX-Routing-Subsystem: Fehlermodi und -auswirkungen

In diesem Kapitel werden typische Fehlerszenarien und deren Auswirkungen auf die Komponenten des NSX-Routing-Subsystems beschrieben.

NSX Manager

Tabelle 3-2. NSX Manager: Fehlermodi und -auswirkungen

Fehlermodus	Fehlerauswirkungen
Verlust der Netzwerkkonnektivität mit der NSX Manager-VM	<ul style="list-style-type: none"> ■ Kompletter Ausfall aller NSX Manager-Funktionen, einschließlich der CRUD-Vorgänge für das NSX-Routing/-Bridging ■ Kein Verlust von Konfigurationsdaten ■ Kein Ausfall der Datenebene oder Steuerungskomponenten
Verlust der Netzwerkkonnektivität zwischen NSX Manager und ESXi-Hosts oder RabbitMQ-Serverfehler	<ul style="list-style-type: none"> ■ Wenn eine DLR-Kontroll-VM oder ein ESG auf den betroffenen Hosts ausgeführt wird, scheitern die CRUD-Vorgänge ■ Das Erstellen und Löschen von DLR-Instanzen auf betroffenen Hosts scheitert ■ Kein Verlust von Konfigurationsdaten ■ Kein Ausfall der Datenebene oder Steuerungskomponenten ■ Alle dynamischen Routing-Updates werden weiterhin durchgeführt

Tabelle 3-2. NSX Manager: Fehlermodi und -auswirkungen (Fortsetzung)

Fehlermodus	Fehlerauswirkungen
Verlust der Netzwerkkonnektivität zwischen NSX Manager und den Controllern	<ul style="list-style-type: none"> ■ Das Erstellen, Aktualisieren und Löschen für verteiltes NSX-Routing und Bridging scheitert ■ Kein Verlust von Konfigurationsdaten ■ Kein Ausfall der Datenebene oder Steuerungskomponenten
NSX Manager-VM wurde entfernt (Datenspeicherfehler)	<ul style="list-style-type: none"> ■ Kompletter Ausfall aller NSX Manager-Funktionen, einschließlich der CRUD-Vorgänge für das NSX-Routing/-Bridging ■ Gefahr, dass eine Teilmenge von Routing/Bridging-Instanzen verwaist, wenn NSX Manager auf einer älteren Konfiguration wiederhergestellt wird und eventuell eine manuelle Bereinigung bzw. eine manueller Abgleich erforderlich ist ■ Kein Ausfall der Datenebene oder Steuerungskomponenten, sofern kein Abgleich erforderlich ist

Controller-Cluster

Tabelle 3-3. NSX Controller: Fehlermodi und -auswirkungen

Fehlermodus	Fehlerauswirkungen
Controller-Cluster verliert Netzwerkkonnektivität mit ESXi-Hosts	<ul style="list-style-type: none"> ■ Kompletter Ausfall der Funktionen der DLR-Steuerungskomponente (Erstellen, Aktualisieren und Löschen von Routen, einschließlich dynamischer Routen) ■ Ausfall der Funktionen der DLR-Verwaltungskomponente (Erstellen, Aktualisieren und Löschen von LIFs auf Hosts) ■ Die VXLAN-Weiterleitung wird beeinträchtigt, wodurch der End-to-End-Weiterleitungsvorgang (L2+L3) scheitern kann ■ Die Datenebene funktioniert weiterhin auf der Basis des letzten bekannten Status
Ein oder zwei Controller verlieren die Konnektivität mit den ESXi-Hosts	<ul style="list-style-type: none"> ■ Wenn der betroffene Controller nach wie vor andere Controller in diesem Cluster erreicht, treten für alle DLR-Instanzen, die von diesem Controller gesteuert werden, die oben beschriebenen Auswirkungen auf. Andere Controller übernehmen die Aufgaben nicht automatisch
Ein Controller verliert die Netzwerkkonnektivität mit anderen Controllern (oder vollständig)	<ul style="list-style-type: none"> ■ Zwei noch vorhandene Controller übernehmen die VXLANs und DLRs, die vom isolierten Controller gesteuert wurden ■ Der betroffene Controller wechselt in den schreibgeschützten Modus, verwirft seine Sitzungen auf den Hosts und verweigert die Annahme neuer Sitzungen

Tabelle 3-3. NSX Controller: Fehlermodi und -auswirkungen (Fortsetzung)

Fehlermodus	Fehlerauswirkungen
Controller verlieren die gegenseitige Konnektivität	<ul style="list-style-type: none"> ■ Alle Controller wechseln in den schreibgeschützten Modus, trennen ihre Verbindungen mit den Hosts und verweigern die Herstellung neuer Verbindungen ■ Das Erstellen, Aktualisieren und Löschen für alle DLR-LIFs und Routen (einschließlich dynamischer Routen) scheitert ■ Die NSX-Routing-Konfiguration (LIFs) kann eventuell zwischen NSX Manager und Controller-Cluster nicht mehr synchronisiert werden, sodass ein manueller Eingriff zur Neusynchronisierung erforderlich wird ■ Hosts werden weiterhin auf der Basis des letzten bekannten Status der Steuerungskomponenten betrieben
Eine Controller-VM ist verloren gegangen	<ul style="list-style-type: none"> ■ Controller-Cluster verliert Redundanz ■ Verwaltungs-/Steuerungskomponenten funktionieren weiterhin normal
Zwei Controller-VMs sind verloren gegangen	<ul style="list-style-type: none"> ■ Die übrigen Controller wechseln in den schreibgeschützten Modus. Die Auswirkungen sind identisch mit jenen beim Verlust der gegenseitigen Konnektivität von Controllern (siehe weiter oben). Es ist vermutlich eine manuelle Cluster-Wiederherstellung erforderlich

Hostmodule

netcpa benötigt den SSL-Schlüssel und das Zertifikat des Hosts sowie die SSL-Fingerabdrücke, um eine sichere Kommunikation mit den Controllern einzurichten. Diese werden vom NSX Manager über den Nachrichtenbus (von vsfwd bereitgestellt).

Wenn der Zertifikataustausch scheitert, kann netcpa keine Verbindung mit den Controllern herstellen.

Hinweis: Dieser Abschnitt enthält keine Erläuterungen zu Fehlern von Kernelmodulen. Bei diesen handelt es sich um schwerwiegende PSOD-Fehler, die selten auftreten.

Tabelle 3-4. Hostmodule: Fehlermodi und -auswirkungen

Fehlermodus	Fehlerauswirkungen
vsfwd verwendet die Benutzername/Kennwort-Authentifizierung für den Zugriff auf den Nachrichtenbusserver, die zeitlich begrenzt sein kann	<ul style="list-style-type: none"> ■ Wenn ein vsfwd-Vorgang auf einem neu vorbereiteten ESXi-Host den NSX Manager nicht innerhalb von zwei Stunden erreichen kann, laufen die temporären, bei der Installation vergebenen Anmeldedaten ab und der Nachrichtenbus ist auf diesem Host nicht mehr funktionsfähig
Die Auswirkungen von Fehlern des Nachrichtenbus-Client (vsfwd) sind vom entsprechenden Zeitpunkt abhängig	

Tabelle 3-4. Hostmodule: Fehlermodi und -auswirkungen (Fortsetzung)

Fehlermodus	Fehlerauswirkungen
Bei einem Scheitern, bevor andere Elemente der NSX-Steuerungskomponente einen stabilen Ausführungsstatus erreicht haben	<ul style="list-style-type: none"> ■ Das verteilte Routing auf dem Host wird angehalten, da der Host nicht mehr mit den Controllern kommunizieren kann ■ Der Host ruft keine DLR-Instanzen vom NSX Manager ab
Bei einem Scheitern, nachdem der Host einen stabilen Status erreicht hat	<ul style="list-style-type: none"> ■ ESGs und DLR-Kontroll-VMs, die auf dem Host ausgeführt werden, können keine Konfigurations-Updates empfangen ■ Der Host ruft neue DLRs nicht ab und kann vorhandene DLRs nicht löschen ■ Der Datenpfad des Hosts wird weiterhin auf der Basis der Konfiguration des Hosts zum Zeitpunkt des Fehlers verwendet

Tabelle 3-5. netcpa: Fehlermodi und -auswirkungen

Fehlermodus	Fehlerauswirkungen
Die Auswirkungen von Fehlern des Steuerungskomponenten-Agenten (netcpa) sind vom entsprechenden Zeitpunkt abhängig	
Bei einem Scheitern, bevor die NSX-Datenpfad-Kernelmodule einen stabilen Ausführungsstatus erreicht haben	<ul style="list-style-type: none"> ■ Das verteilte Routing auf dem Host wird angehalten
Bei einem Scheitern, nachdem der Host einen stabilen Status erreicht hat	<ul style="list-style-type: none"> ■ Die DLR-Kontroll-VMs, die auf dem Host ausgeführt werden, können die Updates ihrer Weiterleitungstabellen nicht an die Controller senden ■ Der Datenpfad für das verteilte Routing empfängt keine LIF- oder Routen-Updates von Controllern, wird aber auf der Basis des Status vor dem Fehlerzeitpunkt weiterhin verwendet

DLR-Kontroll-VM

Tabelle 3-6. DLR-Kontroll-VM: Fehlermodi und -auswirkungen

Fehlermodus	Fehlerauswirkungen
DLR-Kontroll-VM ist verloren gegangen oder ausgeschaltet	<ul style="list-style-type: none"> ■ Das Erstellen, Aktualisieren und Löschen für diese DLR-LIFs und Routen scheitert ■ Dynamische Routen-Updates werden nicht an die Hosts gesendet (einschließlich Entnahme von Präfixen, die über eine jetzt aufgehobene Nachbarschaft empfangen wurden)
DLR-Kontroll-VM verliert die Konnektivität mit NSX Manager und Controllern	<ul style="list-style-type: none"> ■ Es hat die gleichen Auswirkungen, mit einer Ausnahme: Wenn die DLR-Kontroll-VM und ihre Routing-Nachbarschaften noch aktiv sind, ist der Datenverkehr zu und von zuvor abgerufenen Präfixen nicht betroffen
DLR-Kontroll-VM verliert die Konnektivität mit NSX Manager	<ul style="list-style-type: none"> ■ Die NSX Manager-Vorgänge zum Erstellen, Aktualisieren und Löschen dieser DLR-LIFs und Routen scheitern und werden nicht erneut vorgenommen ■ Dynamische Routing-Updates werden weiterhin übermittelt
DLR-Kontroll-VM verliert die Konnektivität mit den Controllern	<ul style="list-style-type: none"> ■ Alle Routing-Änderungen (statische oder dynamische) für diesen DLR werden nicht an die Hosts übermittelt

NSX-Protokolle für das Routing

Es wird empfohlen, alle NSX-Komponenten so zu konfigurieren, dass deren Protokolle an einen zentralen Collector gesendet werden, damit sie an einer Stelle ausgewertet werden können.

Bei Bedarf können Sie die Protokollierungsebene der NSX-Komponenten ändern. Weitere Informationen finden Sie im Thema „Protokollierungsebene von NSX-Komponenten festlegen“ unter *NSX-Protokollierung und -Systemereignisse*.

NSX Manager-Protokolle

- `show log` in der NSX Manager-Befehlszeilenschnittstelle (CLI)
- Tech-Support-Protokollpaket, das über die NSX Manager-Benutzeroberfläche zusammengestellt werden kann

NSX Manager Virtual Appliance Management



Das NSX Manager-Protokoll enthält Informationen zur Verwaltungskomponente, die die CRUD-Vorgänge betreffen (Create/Read/Update/Delete, Erstellen/Lesen/Aktualisieren/Löschen).

Controller-Protokolle

Controller enthalten mehrere Module, von denen viele eigene Protokolldateien generieren. Auf Controller-Protokolle kann mit dem Befehl `show log <log file> [filtered-by <string>]` zugegriffen werden. Die folgenden Protokolldateien betreffen das Routing:

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: Dieses Protokoll verwaltet die Konfiguration und den internen API-Server.
- `cloudnet/cloudnet_nsx-controller.log`: Dies ist das Protokoll für den zentralen Controller-Prozess.
- `cloudnet/cloudnet_cpp.log_nsx-controller.log`: Dieses Protokoll verwaltet das Clustering und Bootstrap.
- `cloudnet/cloudnet_cpp.log.ERROR`: Diese Datei ist vorhanden, wenn ein Fehler auftritt.

Controller-Protokolle sind umfangreich und in den meisten Fällen nur erforderlich, wenn das VMware-Technikteam zur Fehlerbehebung in schwierigeren Fällen hinzugezogen wird.

Zusätzlich zum Aufruf über die `show log`-CLI können einzelne Protokolldateien mithilfe des Befehls `watch log <logfile> [filtered-by <string>]` in Echtzeit, d. h. zum Zeitpunkt der Aktualisierung, eingesehen werden.

Die Protokolle sind im Controller-Support-Paket enthalten, das durch Auswahl des Controller-Knotens in der NSX-Benutzeroberfläche und durch Klicken auf das Symbol **Tech-Support-Protokolle herunterladen (Download tech support logs)** generiert und heruntergeladen werden kann.

ESXi Host-Protokolle

Durch auf ESXi-Hosts ausgeführten NSX-Komponenten werden folgende Protokolldateien erstellt:

- VMkernel-Protokolle: `/var/log/vmkernel.log`
- Protokolle des Steuerungskomponenten-Agenten: `/var/log/netcpa.log`
- Protokolle des Nachrichtenbus-Client: `/var/log/vsfwd.log`

Die Protokolle können auch als Bestandteil des VM-Support-Pakets zusammengestellt werden, das von vCenter Server generiert wird. Diese Datei ist nur für den Benutzer bzw. die Benutzergruppen mit *root*-Rechten zugänglich.

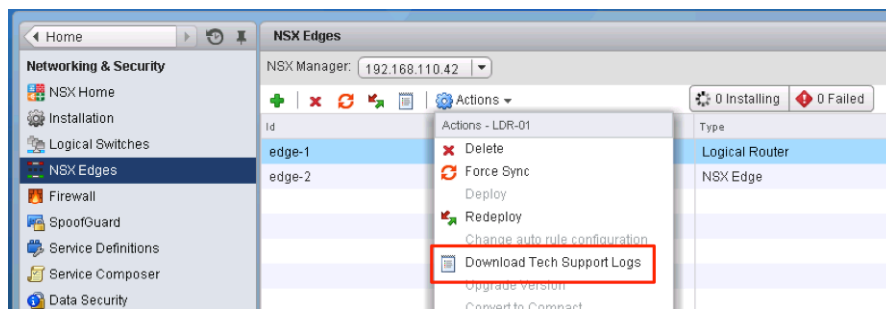
ESG-/DLR-Kontroll-VM-Protokolle

Für den Zugriff auf die Protokolldateien des ESG und der DLR-Kontroll-VM haben Sie zwei Möglichkeiten: Sie können diese mithilfe einer CLI darstellen oder das Tech-Support-Paket mithilfe der Befehlszeilenschnittstelle (CLI) oder der Benutzeroberfläche herunterladen.

Zur Darstellung der Protokolle verwenden Sie den CLI-Befehl `show log [follow | reverse]`.

So laden Sie das Tech-Support-Paket herunter:

- An der CLI wechseln Sie in den `enable`-Modus und führen Sie dann den Befehl `export tech-support <[scp | ftp]> <URI>` aus.
- Im vSphere Web Client wählen Sie die Option **Tech-Support-Protokolle herunterladen (Download Tech Support Logs)** im Menü **Aktionen (Actions)** aus.



Andere nützliche Dateien und deren Speicherorte

Auch wenn es sich dabei im engeren Sinn nicht um Protokolle handelt, gibt es eine Vielzahl von Dateien, die für das Verständnis und die Fehlerbehebung des NSX-Routings eine Unterstützung bieten.

- Die Datei `/etc/vmware/netcpa/config-by-vsm.xml` zur Konfiguration des Steuerungskomponenten-Agenten enthält Informationen über die folgenden Komponenten:
 - Controller, IP-Adressen, TCP-Ports, Zertifikat-Fingerabdrücke, Aktivierung/Deaktivierung von SSL
 - dvUplinks am DVS, mit VXLAN aktiviert (Gruppierungsrichtlinie, Namen, UUID)

- DLR-Instanzen, die der Host erkennt (DLR-ID und -Name)
- Die Datei `/etc/vmware/netcpa/netcpa.xml` zur Konfiguration des Steuerungskomponenten-Agenten enthält verschiedene Konfigurationsoptionen für netcpa, inklusive der Protokollierungsebene (diese ist standardmäßig **info**).
- Zertifikatdateien der Steuerungskomponente: `/etc/vmware/ssl/rui-for-netcpa.*`
 - Zwei Dateien: Hostzertifikat und privater Schlüssel des Host
 - Verwendet für die Authentifizierung von Hostverbindungen mit Controllern

Alle diese Dateien werden vom Agenten der Steuerungskomponente mithilfe von Informationen des NSX Manager erstellt, die über die von vsfwd bereitgestellte Nachrichtenbusverbindung übertragen werden.

Allgemeine Fehlerszenarien und deren Behebung

Die häufigsten Fehlerszenarien lassen sich in zwei Kategorien einteilen.

Probleme mit der Konfiguration und Probleme mit der Steuerungskomponente. Probleme mit der Verwaltungskomponente treten selten auf.

Konfigurationsprobleme und deren Behebung

Die allgemeinen Konfigurationsprobleme und ihre Auswirkungen werden in [Tabelle 3-7. Allgemeine Konfigurationsprobleme und ihre Auswirkungen](#) beschrieben.

Tabelle 3-7. Allgemeine Konfigurationsprobleme und ihre Auswirkungen

Probleme	Auswirkungen
Protokoll und weitergeleitete IP-Adressen werden beim dynamischen Routing umgekehrt	Die dynamische Protokollnachbarschaft kommen nicht zum Einsatz
Die Transportzone ist nicht an der DVS-Grenze ausgerichtet	Das verteilte Routing funktioniert nicht mit einer Teilmenge der ESXi-Hosts (wenn sich welche nicht in der Transportzone befinden)
Die Protokollkonfiguration für das dynamische Routing stimmt nicht überein (Timer, MTU, BGP ASN, Kennwörter, der OSPF-Area zugeordnete Schnittstelle)	Die dynamische Protokollnachbarschaft kommt nicht zum Einsatz
Die DLR-HA-Schnittstelle ist einer IP-Adresse zugewiesen und die Neuverteilung der verbundenen Routen ist aktiviert	Die DLR-Kontroll-VM übernimmt Datenverkehr für das HA-Schnittstellen-Subnetz und verursacht Blackholes für den Datenverkehr

Zur Behebung dieser Probleme überprüfen Sie die Konfiguration und korrigieren Sie diese, falls notwendig.

Mit dem CLI-Befehl `debug ip ospf` oder `debug ip bgp` können Sie, wenn erforderlich, Protokolle auf der DLR-Kontroll-VM oder der ESG-Konsole (nicht über eine SSH-Sitzung) anzeigen und Probleme der Protokollkonfiguration ermitteln.

Probleme mit Steuerungskomponenten und deren Behebung

Die Probleme mit Steuerungskomponenten treten häufig aufgrund folgender Ursachen auf:

- Der Host Control Plane Agent (netcpa) kann keine Verbindung zu NSX Manager über den von vsfwd bereitgestellten Nachrichtenbuskanal herstellen
- Die Controller-Cluster haben Probleme mit der Handhabung der Master-Rolle für die DLR/VXLAN-Instanzen

Probleme mit dem Controller-Cluster, die sich auf die Handhabung der Master-Rolle beziehen, lassen sich häufig durch einen Neustart eines NSX Controller beheben (`restart controller` in der CLI des Controllers).

Weitere Informationen zur Fehlerhebung bei Problemen von Steuerungskomponenten finden Sie unter <http://kb.vmware.com/kb/2125767>.

Erfassen von Daten zur Fehlerbehebung

Dieser Abschnitt bietet einen Überblick über die CLI-Befehle, die im Allgemeinen für die Behebung von Fehlern beim NSX-Routing verwendet werden.

NSX Manager

Ab der Version NSX 6.2 werden Befehle, die bisher vom NSX Controller und von anderen NSX-Komponenten aus zur Fehlerbehebung für das NSX-Routing ausgeführt wurden, direkt aus dem NSX Manager aufgerufen.

- Liste von DLR-Instanzen
- Liste von LIFs für jede DLR-Instanz
- Liste von Routen für jede DLR-Instanz
- List von MAC-Adressen für jede DLR-Bridging-Instanz
- Schnittstellen
- Routing-und Weiterleitungstabellen
- Zustand dynamischer Routing-Protokolle (OSPF oder BGP)
- Vom NSX Manager zur DLR-Kontroll-VM oder zum ESG gesendete Konfiguration

DLR-Kontroll-VM und ESG

Die DLR-Kontroll-VM und das ESG bieten eine Funktionalität zur Erfassung von Paketen an ihren Schnittstellen. Die Paketerfassung bietet eine Unterstützung durch die Fehlerbehebung bei Problemen der Routing-Protokolle im Bedarfsfall.

- 1 Führen Sie `show interfaces` für die Auflistung der Namen der Schnittstellen aus.
- 2 Führen Sie `debug packet [display | capture] interface <interface name>` aus.
 - Bei der Erfassung werden die Pakete in einer `.pcap`-Datei gespeichert.

- 3 Führen Sie `debug show files` für die Auflistung der gespeicherten Erfassungsdateien aus.
- 4 Führen Sie `debug copy [scp | ftp] ...` für das Herunterladen von Erfassungen für eine Offline-Analyse aus.

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

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

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

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

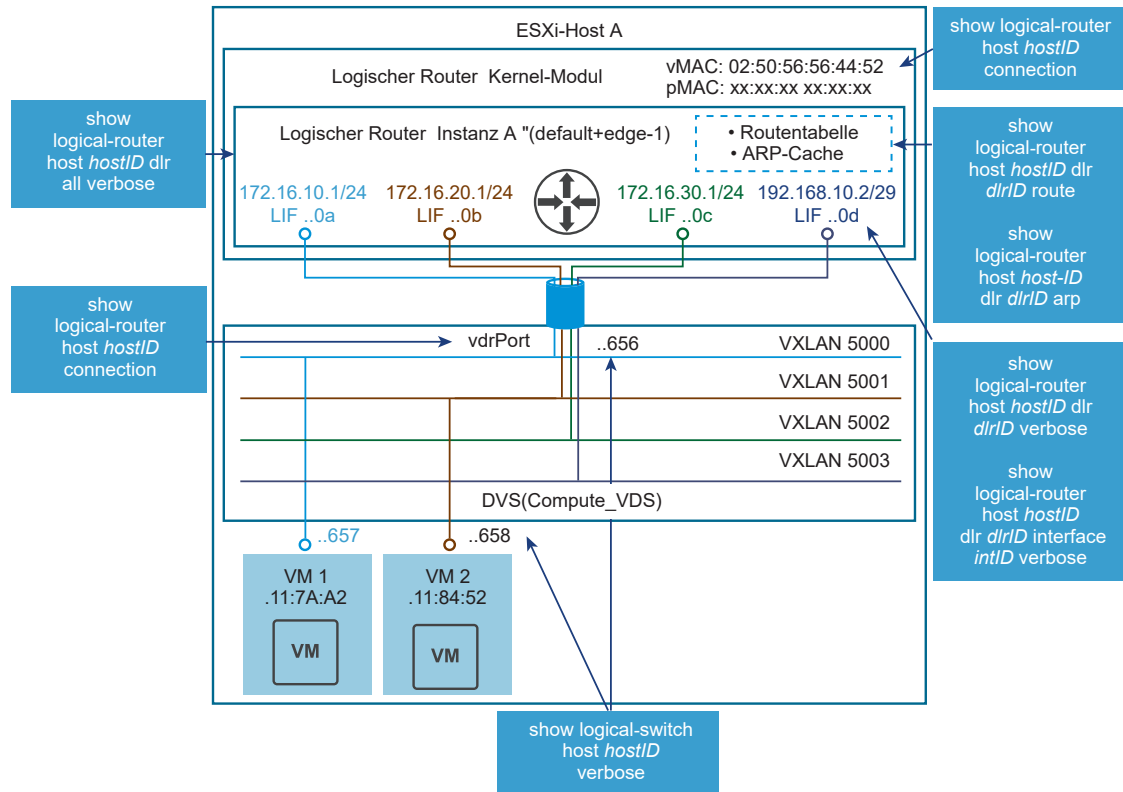
Der Befehl `debug packet` verwendet `tcpdump` im Hintergrund und akzeptiert Filtermodifikatoren, die wie `tcpdump`-Filtermodifikatoren unter UNIX formatiert sind. Es müssen lediglich im Filterausdruck die Leerzeichen durch Unterstriche („_“) ersetzt werden.

Der nachfolgend dargestellte Befehl stellt beispielsweise den gesamten Datenverkehr über `vNic_0` außer SSH dar, um nicht den Datenverkehr der interaktiven Sitzung selbst anzeigen zu müssen.

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

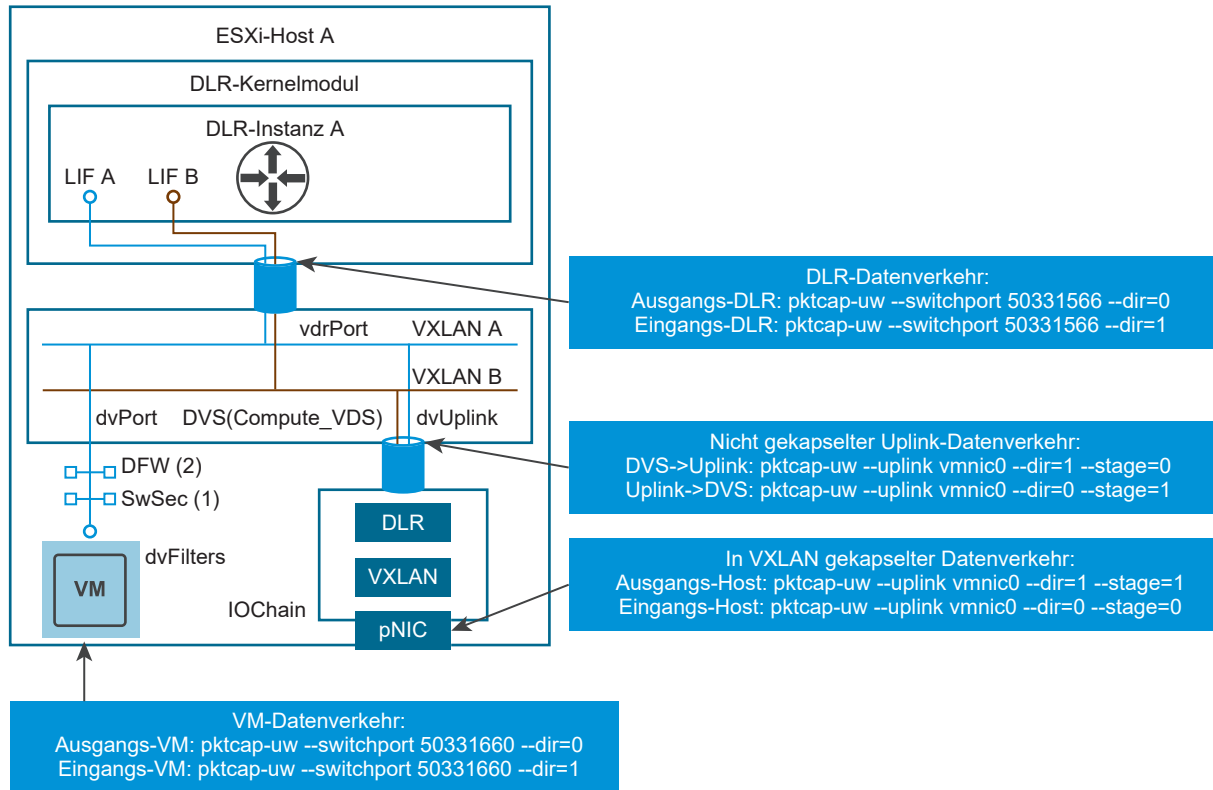
ESXi-Hosts

Hosts sind eng mit dem NSX-Routing verknüpft. [Abbildung 3-14. Hostkomponenten für die Fehlerbehebung beim NSX-Routing](#) stellt visuell die Komponenten im Routing-Subsystem und die NSX Manager-CLI-Befehle dar, mit denen Informationen über die Komponenten angezeigt werden können:

Abbildung 3-14. Hostkomponenten für die Fehlerbehebung beim NSX-Routing

Die im Datenpfad erfassten Pakete bieten eine Unterstützung durch Ermittlung von Problemen auf verschiedenen Ebenen der Paketweiterleitung im Bedarfsfall. [Abbildung 3-15. Erfassungspunkte und zugehörige CLI-Befehle](#) zeigt die wichtigsten Erfassungspunkte und die entsprechenden erforderlichen CLI-Befehle.

Abbildung 3-15. Erfassungspunkte und zugehörige CLI-Befehle



Fehlerbehebung bei NSX Edge

4

Dieser Abschnitt erläutert VMware NSX Edge und bietet Informationen zur Fehlerbehebung.

Um mit der NSX Edge-Appliance auftretende Probleme zu beheben, müssen Sie zunächst prüfen, ob die im Folgenden aufgeführten Schritte zur Fehlerbehebung für Ihre Umgebung relevant sind. Jeder Schritt enthält Anleitungen oder einen Link zu einem Dokument, mit denen Sie mögliche Ursachen beseitigen und korrigierende Maßnahmen wie erforderlich vornehmen können. Die Schritte werden in der für die Isolierung des Problems und für die Ermittlung der entsprechenden Lösung am geeignetsten erscheinenden Reihenfolge aufgeführt. Sie müssen alle Schritte durchführen.

Überprüfen Sie die Versionshinweise für aktuelle Versionen, ob das Problem bereits behoben ist.

Stellen Sie bei der Installation von VMware NSX Edge sicher, dass die Mindestsystemanforderungen erfüllt sind. Weitere Informationen finden Sie unter *Installationshandbuch für NSX*.

Installations- und Upgrade-Probleme

- Stellen Sie sicher, dass das aufgetretene Problem kein „Würde blockieren“-Fehler ist. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/2107951>.
- Wenn der Upgrade-Vorgang oder die erneute Bereitstellung erfolgreich durchgeführt wurde, aber keine Konnektivität mit der Edge-Schnittstelle besteht, müssen Sie die Konnektivität auf dem Backend-Schicht 2-Switch überprüfen. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2135285>.
- Wenn die Bereitstellung oder das Upgrade von Edge mit folgender Fehlermeldung scheitert:

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

ODER

- Wenn die Bereitstellung oder das Upgrade erfolgreich ist, aber keine Konnektivität mit den Edge-Schnittstellen vorhanden ist:

- Die Ausführung des Befehls `show interface` sowie die Edge-Support-Protokolle stellen Meldungen folgender Art dar:

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

In beiden Fällen ist der Host-Switch nicht bereit oder weist Probleme auf. Zur Behebung des Problems müssen Sie den Host-Switch überprüfen.

Konfigurationsprobleme

- Erfassen Sie die Diagnoseinformationen zu NSX Edge. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2079380>.

Filtern Sie die NSX Edge-Protokolle durch eine Suche nach dem String `vse_die`. Die Protokollinformationen in der Nähe dieses String enthalten eventuell Informationen über den Konfigurationsfehler.

Hohe CPU-Nutzung

Wenn Sie eine hohe CPU-Nutzung auf dem NSX Edge feststellen, überprüfen Sie mit dem Befehl `esxtop` die Leistung der Appliance auf dem ESXi-Host. Zusätzliche Informationen dazu finden Sie in folgenden Knowledgebase-Artikeln:

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

Weitere Erläuterungen erhalten Sie unter <https://communities.vmware.com/docs/DOC-9279>.

Ein hoher Wert für den `ksoftirqd`-Vorgang signalisiert eine hohe Rate eingehender Pakete. Stellen Sie sicher, dass die Protokollierung auf dem Datenpfad, z. B. für Firewallregeln, aktiviert ist. Ermitteln Sie mit dem Befehl `show log follow`, ob eine große Anzahl an Protokolltreffern ermittelt wurde.

Darstellen der Statistiken für verworfene Pakete

Ab der Version NSX for vSphere 6.2.3 können Sie mit dem Befehl `show packet drops` die Statistiken für verworfene Pakete mit folgenden Elementen anzeigen:

- Schnittstelle
- Treiber

- L2
- L3
- Firewall

Zur Ausführung des Befehls melden Sie sich bei der NSX Edge-CLI an und wechseln Sie in den Basismodus. Weitere Informationen dazu finden Sie in der *Befehlszeilenschnittstellen-Referenz zu NSX*.
Beispiel:

```
show packet drops
```

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

```
Driver Errors
```

```
=====
```

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

```
Interface Drops
```

```
=====
```

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

```
L2 RX Errors
```

```
=====
```

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

```
L2 TX Errors
```

```
=====
```

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

L3 Errors

=====

IP:

ReasmFails : 0
 InHdrErrors : 0
 InDiscards : 0
 FragFails : 0
 InAddrErrors : 0
 OutDiscards : 0
 OutNoRoutes : 0
 ReasmTimeout : 0

ICMP:

InTimeExcds : 0
 InErrors : 227
 OutTimeExcds : 0
 OutDestUnreachs : 152
 OutParmProbs : 0
 InSrcQuenchs : 0
 InRedirects : 0
 OutSrcQuenchs : 0
 InDestUnreachs : 151
 OutErrors : 0
 InParmProbs : 0

Firewall Drop Counters

=====

Ipv4 Rules

=====

Chain - INPUT

rid	pkts	bytes	target	prot	opt	in	out	source	destination	state
0	119	30517	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	INVALID
0	0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain - POSTROUTING

rid	pkts	bytes	target	prot	opt	in	out	source	destination	state
0	101	4040	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	INVALID
0	0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Ipv6 Rules

=====

Chain - INPUT

rid	pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	0	DROP	all		*	*	::/0	::/0	INVALID
0	0	0	DROP	all		*	*	::/0	::/0	

Chain - POSTROUTING

rid	pkts	bytes	target	prot	opt	in	out	source	destination	state
0	0	0	DROP	all		*	*	::/0	::/0	INVALID
0	0	0	DROP	all		*	*	::/0	::/0	

Erwartetes Verhalten beim Verwalten von NSX Edge

- Wenn Sie in vSphere Web Client L2 VPN auf einem NSX Edge konfigurieren und **Site-Konfigurationsdetails: (Site Configuration Details)** hinzufügen, entfernen oder verändern, werden alle vorhandenen Verbindungen getrennt und erneut wiederhergestellt. Dies ist ein erwartetes Verhalten.
- NSX Edge ist eine virtuelle Maschine (VM) und besteht aus mehreren Dateien, die auf einem Speichergerät gespeichert werden. Schlüsseldateien sind die Konfigurationsdatei, die Datei(en) der virtuellen Festplatte, die Datei mit den NVRAM-Einstellungen, die Auslagerungsdatei und die Protokolldatei. Basierend auf dem angewendeten VM-Speicherprofil oder der manuellen Platzierung können die Konfigurationsdateien der virtuellen Maschine, die Datei der virtuellen Festplatte oder die Auslagerungsdatei am selben Speicherort oder an verschiedenen Speicherorten auf verschiedenen Datenspeichern platziert werden. Falls sich Dateien der virtuellen Maschine an unterschiedlichen Speicherorten befinden, zeigt NSX Manager den Datenspeicher an, der die VMX-Datei für die VM-Bereitstellung enthält und verwendet ihn. Bei einer erneuten Bereitstellung oder bei Upgrade-Vorgängen stellt NSX Manager die NSX Edge-VM(s) im konfigurierten Datenspeicher oder dem Live-Datenspeicher bereit, der die VMX-Dateien hostet. Der *Name des Datenspeichers* und die *ID des Datenspeichers* (der die VMX-Datei auf der VM hostet) werden als Teil des Parameters *Appliance* zurückgegeben und auf der Benutzeroberfläche angezeigt oder als Antwort auf die REST API bereitgestellt. Über den vCenter Server finden Sie Einzelheiten zum genauen Layout jeder NSX Manager-VM-Datei und zu einem oder mehreren der Datenspeicher, in dem die Dateien platziert werden. Weitere Informationen finden Sie in der folgenden Dokumentation:
 - *vSphere-Administratorhandbuch für virtuelle Maschinen*
 - *vSphere-Ressourcenverwaltung*
 - *vCenter Server und Hostverwaltung*

Dieses Kapitel enthält die folgenden Themen:

- [Probleme durch verworfene Edge-Firewall-Pakete](#)
- [Probleme mit der Edge-Routing-Konnektivität](#)
- [NSX Manager- und Edge-Kommunikationsprobleme](#)
- [Debugging für den Nachrichtenbus](#)
- [Edge-Diagnose und -Wiederherstellung](#)

Probleme durch verworfene Edge-Firewall-Pakete

Anzeigen von Statistiken für verworfene Firewall-Pakete

Ab der Version NSX for vSphere 6.2.3 können Sie mit dem Befehl `show packet drops` die Statistiken für verworfene Pakete für die Firewall anzeigen.

Zur Ausführung des Befehls melden Sie sich bei der NSX Edge-CLI an und wechseln Sie in den Basismodus. Weitere Informationen dazu finden Sie in der *Befehlszeilenschnittstellen-Referenz zu NSX*.
Beispiel:

```
show packet drops

vShield Edge Packet Drop Stats:

Firewall Drop Counters
=====

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

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

Firewallprobleme von Edge-Paketen

Zur Ausführung eines Befehls melden Sie sich bei der NSX Edge-Befehlszeilenschnittstelle an und wechseln Sie in den Basismodus. Weitere Informationen dazu finden Sie in der *Befehlszeilenschnittstellen-Referenz zu NSX*.

- 1 Überprüfen Sie mit dem Befehl `show firewall` die Tabelle der Firewallregeln. Die Tabelle `usr_rules` stellt die konfigurierten Regeln dar.

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

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

```

0      23789 1184K ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
state RELATED,ESTABLISHED
0      116K 8374K usr_rules  all  --  *    *    0.0.0.0/0    0.0.0.0/0
0          0    0 DROP      all  --  *    *    0.0.0.0/0    0.0.0.0/0

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

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

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target    prot opt in     out     source        destination
0     78903  16M ACCEPT    all  --  *    lo    0.0.0.0/0    0.0.0.0/0
0     679K  41M DROP      all  --  *    *    0.0.0.0/0    0.0.0.0/0
state INVALID
0     3146M 4098G block_out all  --  *    *    0.0.0.0/0    0.0.0.0/0
0          0    0 ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
PHYSDEV match --physdev-in tap0 --physdev-out vNic_+
0          0    0 ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out tap0
0          0    0 ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
PHYSDEV match --physdev-in na+ --physdev-out vNic_+
0          0    0 ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out na+
0     3145M 4098G ACCEPT    all  --  *    *    0.0.0.0/0    0.0.0.0/0
state RELATED,ESTABLISHED
0     221K  13M usr_rules all  --  *    *    0.0.0.0/0    0.0.0.0/0
0          0    0 DROP      all  --  *    *    0.0.0.0/0    0.0.0.0/0

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

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

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

```

Prüfen Sie, ob ein inkrementeller Wert einer DROP Invalid-Regel im Abschnitt POST_ROUTING des Befehls `show firewall` vorhanden ist. Typische Ursachen sind u. a.:

- Probleme durch asymmetrisches Routing
- TCP-basierte Anwendungen, die mehr als eine Stunde inaktiv waren. Treten Zeitüberschreitungsprobleme aufgrund von Inaktivität auf und befinden sich die Anwendungen ungewöhnlich lange im Leerlauf, erhöhen Sie mithilfe der REST-API den Wert für die Zeitüberschreitung durch Inaktivität in den Einstellungen. Siehe <https://kb.vmware.com/kb/2101275>.

2 Erfassen Sie die Ausgabe des Befehls `show ipset`.

```

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

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

Name: 1_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=6, DestPort=179, SrcPort=Any    (encoded: 0.6.0.179,0.6.0.0/16)
Proto=89, DestPort=Any, SrcPort=Any   (encoded: 0.89.0.0/16,0.89.0.0/16)

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

```

3 Aktivieren Sie mit der REST-API oder mit der Edge-Benutzeroberfläche die Protokollierung für eine bestimmte Firewall und überwachen Sie die Protokolle mit dem Befehl `show log follow`.

Wenn keine Protokolle angezeigt werden, aktivieren Sie mithilfe der nachfolgend aufgeführten REST-API die Protokollierung in der DROP Invalid-Regel.

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

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

Suchen Sie mit dem Befehl `show log follow` nach Protokollen folgender Art:

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

- 4 Prüfen Sie mit dem Befehl `show flowtable rule_id`, ob in der Statustabelle der Edge-Firewall einander entsprechende Verbindungen vorhanden sind:

```
nsxedge> show flowtable
1: tcp 6 21554 ESTABLISHED src=192.168.110.10 dst=192.168.5.3 sport=25981
d port=22 pkts=52 bytes=5432 src=192.168.5.3 dst=192.168.110.10 sport=22 dport=259
81 pkts=44 bytes=7201 [ASSURED] mark=0 rid=131073 use=1
2: tcp 6 21595 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=53194
dport=10 001 pkts=33334 bytes=11284650 src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=5319
4 pkts=33324 bytes=1394146 [ASSURED] mark=0 rid=0 use=1
```

Vergleichen Sie mit dem Befehl `show flowstats` die Anzahl der aktiven Verbindungen und die maximal zulässige Anzahl:

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

- 5 Überprüfen Sie mit dem Befehl `show log follow` die Edge-Protokolle und suchen Sie nach verworfenen ALGs. Suchen Sie nach Strings in der Art von `tftp_alg`, `msrpc_alg` oder `oracle_tns`. Weitere Informationen dazu finden Sie unter:

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

Probleme mit der Edge-Routing-Konnektivität

- 1 Starten Sie mithilfe des Befehls `ping <destination_IP_address>` einen gesteuerten Datenverkehr von einem Client.
- 2 Erfassen Sie den Datenverkehr gleichzeitig an beiden Schnittstellen, schreiben Sie die Ausgabe in eine Datei und exportieren Sie diese mithilfe von SCP.

Beispiel:

Erfassen Sie mit folgendem Befehl den Datenverkehr an der Ingress-Schnittstelle:

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

Erfassen Sie mit folgendem Befehl den Datenverkehr an der Egress-Schnittstelle:

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

Für eine gleichzeitige Paketerfassung verwenden Sie das ESXi-Dienstprogramm `pktcap-uw` zur Paketerfassung in ESXi. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2051814>.

Tritt das Verwerfen von Paketen dauerhaft auf, prüfen Sie, ob Konfigurationsfehler in folgenden Bereichen aufgetreten sind:

- IP-Adressen und -Routen
- Firewallregeln oder NAT-Regeln
- Asymmetrisches Routing
- RP-Filterüberprüfungen
 - a Überprüfen Sie mit dem Befehl `show interface IP/-Subnetze` für Schnittstellen.

- b Wenn keine Routen auf der Datenebene vorhanden sind, führen Sie folgende Befehle aus:
 - `show ip route`
 - `show ip route static`
 - `show ip route bgp`
 - `show ip route ospf`
- c Überprüfen Sie mit dem Befehl `show ip forwarding` die Routing-Tabelle auf erforderliche Routen.
- d Wenn Sie über mehrere Pfade verfügen, führen Sie den Befehl `show rpfilter` aus.

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

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

Zur Überprüfung der RPF-Statistiken führen Sie den Befehl `show rpfstats` aus.

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

Tritt das Verwerfen von Paketen zufällig auf, prüfen Sie, ob Beschränkungen von Ressourcen vorhanden sind:

- a Für die Nutzung von CPU und Arbeitsspeicher führen Sie folgende Befehle aus:
 - `show system cpu`
 - `show system memory`
 - `show system storage`
 - `show process monitor`
 - `top`

Für ESXi führen Sie den Befehl `esxtop n` aus.

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

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

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

NSX Manager- und Edge-Kommunikationsprobleme

NSX Manager kommuniziert mit NSX Edge über den VIX- oder den Nachrichtenbus. Dieser wird von NSX Manager bei der Edge-Bereitstellung ausgewählt und ändert sich nicht mehr.

Hinweis VIX wird in NSX 6.3.0 und höher nicht unterstützt.

VIX

- VIX wird für NSX Edge verwendet, wenn der ESXi-Host nicht vorbereitet wurde.
- Der NSX Manager erhält die Hostanmeldedaten von vCenter Server, um zuerst eine Verbindung mit dem ESXi-Host herzustellen.
- Der NSX Manager verwendet die Edge-Anmeldedaten für die Anmeldung bei der Edge-Appliance.
- Der `vmtoolsd`-Vorgang auf dem Edge steuert die VIX-Kommunikation.

VIX-Fehler können aus folgenden Gründen auftreten:

- Der NSX Manager kann keine Kommunikation mit dem vCenter Server herstellen.
- Der NSX Manager kann keine Kommunikation mit den ESXi-Hosts herstellen.
- NSX Manager weist interne Probleme auf.
- Edge weist interne Probleme auf.

VIX-Debugging

Überprüfen Sie in den NSX Manager-Protokollen die VIX-Fehler VIX_E_<Fehler>, um die Fehlerursache einzugrenzen. Suchen Sie nach Fehlern folgender Art:

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

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

Tritt der Fehler zur selben Zeit für verschiedene Edges auf, liegt er im Allgemeinen nicht auf der Seite von Edge.

Debugging für den Nachrichtenbus

Der Nachrichtenbus wird für die NSX Edge-Kommunikation verwendet, wenn ESXi-Hosts vorbereitet sind.

Beim Auftreten von Problemen können die NSX Manager-Protokolle Einträge folgender Art enthalten:

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

Dieses Problem tritt in folgenden Fällen auf:

- Edge befindet sich in einem ungültigen Zustand
- Die Verbindung des Nachrichtebusses ist unterbrochen

Zur Beurteilung des Problems auf dem Edge führen Sie Folgendes aus:

- Zur Prüfung der rmq-Konnektivität führen Sie folgenden Befehl aus:

```
nsxedge> show messagebus messages
-----
Message bus is enabled
cmd conn state : listening
init_req      : 1
init_resp     : 1
init_req_err  : 0
...
```

- Zur Prüfung der vmci-Konnektivität führen Sie folgenden Befehl aus:

```
nsxedge> show messagebus forwarder
-----
Forwarder Command Channel
vmci_conn      : up
app_client_conn : up
vmci_rx        : 3649
```

```

vmci_tx          : 3648
vmci_rx_err      : 0
vmci_tx_err      : 0
vmci_closed_by_peer: 8
vmci_tx_no_socket : 0
app_rx          : 3648
app_tx          : 3649
app_rx_err       : 0
app_tx_err       : 0
app_conn_req     : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
Forwarder Event Channel
vmci_conn        : up
app_client_conn  : up
vmci_rx          : 1143
vmci_tx          : 13924
vmci_rx_err      : 0
vmci_tx_err      : 0
vmci_closed_by_peer: 0
vmci_tx_no_socket : 0
app_rx          : 13924
app_tx          : 1143
app_rx_err       : 0
app_tx_err       : 0
app_conn_req     : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
cli_rx          : 1
cli_tx          : 1
cli_tx_err       : 0
counters_reset   : 0

```

In diesem Beispiel zeigt die Ausgabe `vmci_closed_by_peer: 8` an, wie oft die Verbindung durch den Hostagenten getrennt wurde. Nimmt diese Anzahl zu und ist `vmci_conn` inaktiv, kann der Hostagent keine Verbindung mit dem RMQ-Broker herstellen. In `show log follow` suchen Sie nach wiederholt auftretenden Fehlern in den Edge-Protokollen: `VmciProxy: [daemon.debug] VMCI Socket is closed by peer` (VMCI-Socket wurde durch den Peer getrennt)

Zur Beurteilung des Problems auf dem ESXi-Host führen Sie Folgendes aus:

- Zur Überprüfung, ob der ESXi-Host eine Verbindung mit dem RMQ-Broker herstellen kann, führen Sie folgenden Befehl aus:

```

esxcli network ip connection list | grep 5671

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

```

```
vsfwd
tcp    0    0  10.32.43.4:20808  10.32.43.230:5671  ESTABLISHED    35847  newreno
vsfwd
tcp    0    0  10.32.43.4:12486  10.32.43.230:5671  ESTABLISHED    35847  newreno  vsfwd
```

Edge-Diagnose und -Wiederherstellung

Edge-Diagnose

- Überprüfen Sie mit folgendem Befehl, ob `vmtoolsd` ausgeführt wird:

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

- Überprüfen Sie mit folgendem Befehl, ob sich Edge in einem gültigen Zustand befindet:

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

Mit dem Befehl `show eventmgr` können Sie prüfen, ob der Abfragebefehl empfangen und verarbeitet wurde.

```
nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
profiling       : 0
cfg_rx          : 1
cfg_rx_msgbus   : 0
cfg_rx_err      : 0
cfg_exec_err    : 0
cfg_resp        : 0
cfg_resp_err    : 0
cfg_resp_ln_err : 0
fastquery_rx    : 0 fastquery_err : 0
clearcmd_rx     : 0
clearcmd_err    : 0
```

```

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

```

Edge-Wiederherstellung

Wenn `vmtoolsd` nicht ausgeführt wird oder sich NSX Edge in einem ungültigen Zustand befindet, starten Sie Edge neu.

Ein Neustart sollte ausreichend sein, um das Edge nach einem Absturz wiederherzustellen. Eine erneute Bereitstellung ist nicht erforderlich.

Hinweis Notieren Sie alle Protokollinformationen aus dem alten Edge, wenn die erneute Bereitstellung abgeschlossen ist.

Für das Debugging eines Kernel-Absturzes ist Folgendes erforderlich:

- Entweder die vmss-Datei (VM-Anhaltevorgänge) oder die vmsn-Datei (VM-Snapshot) für die Edge-VM im abgestürzten Zustand. Wenn eine vmem-Datei vorhanden ist, ist diese ebenfalls erforderlich. Mit diesen Dateien lässt sich eine Kernel-Core-Dump-Datei extrahieren, die der VMware-Support analysieren kann.
- Das Edge-Support-Protokoll, das unmittelbar nach dem Neustart des abgestürzten Edge (ohne erneute Bereitstellung) generiert wird. Sie können darüber hinaus die Edge-Protokolle prüfen. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2079380>.
- Ein Screenshot der Edge-Konsole ist ebenfalls hilfreich, auch wenn dieser in der Regel nicht den vollständigen Absturzbericht enthält.

Fehlerbehebung für Firewall

5

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

Dieses Kapitel enthält die folgenden Themen:

- [Informationen zur verteilten Firewall](#)
- [Identitätsbasierte Firewall](#)

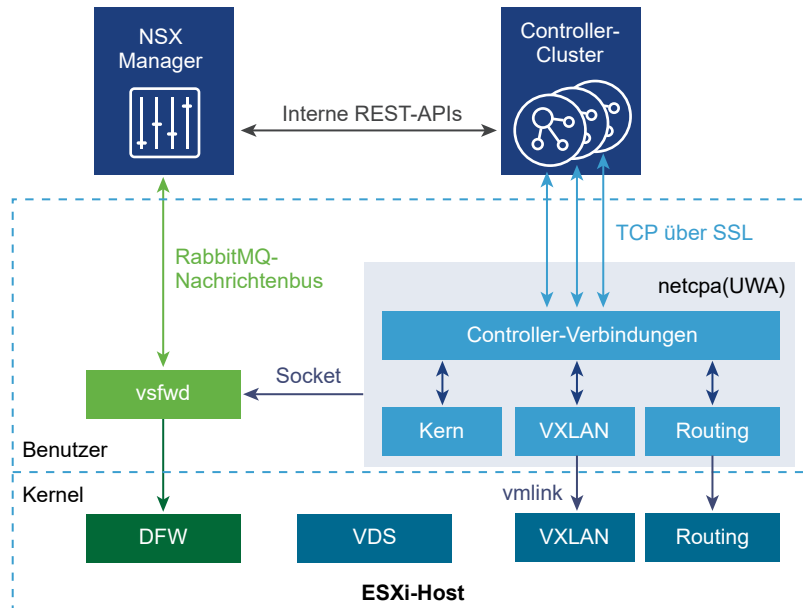
Informationen zur verteilten Firewall

Ein RabbitMQ-Nachrichtenbus wird für die Kommunikation zwischen dem vsfwd- (RMQ-Client) und dem RMQ-Server-Prozess verwendet, der auf dem NSX Manager gehostet wird. Mit dem Nachrichtenbus sendet der NSX Manager verschiedene Informationen an die ESXi-Hosts, darunter auch Richtlinienregeln, die auf der verteilten Firewall im Kernel programmiert werden müssen.

Die verteilte Firewall von NSX ist eine im Hypervisor-Kernel eingebettete Firewall, die eine Anzeige und Steuerung für virtualisierte Arbeitslasten und Netzwerke bietet. Sie können Zugriffssteuerungsrichtlinien auf der Grundlage von VMware vCenter-Objekten wie Datacenter und Cluster, Namen und Tags virtueller Maschinen, Netzwerkstrukturen wie IP/VLAN/VXLAN-Adressen sowie der Benutzergruppenidentität aus Active Directory erstellen. Es wird jetzt eine konsistente Zugriffssteuerungsrichtlinie erzwungen, wenn eine virtuelle Maschine mithilfe von vMotion über physische Hosts hinweg verschoben wird, ohne dass Firewallregeln neu erstellt werden müssen. Da die verteilte Firewall im Hypervisor eingebettet ist, liefert sie einen Durchsatz, der nahezu der Verbindungsgeschwindigkeit entspricht und so eine größere Konsolidierung der Arbeitslast auf physischen Servern ermöglicht. Die verteilte Eigenschaft der Firewall liefert eine Architektur mit horizontaler Skalierung, die automatisch die Firewall-Kapazitäten erweitert, wenn zusätzliche Hosts zu einem Datacenter hinzugefügt werden.

Die NSX Manager-Web-Anwendung und die NSX-Komponenten auf den ESXi-Hosts kommunizieren über den RabbitMQ-Broker-Vorgang miteinander, der auf derselben virtuellen Maschine wie die NSX Manager-Web-Anwendung ausgeführt wird. Hierzu wird das Kommunikationsprotokoll AMQP (Advanced Message Queueing Protocol) verwendet. Der Kanal wird durch SSL geschützt. Auf einem ESXi-Host richtet der VSFWD-Vorgang (vShield Firewall Daemon) die SSL-Verbindung mit dem Broker ein, verwaltet diese SSL-Verbindung und sendet bzw. empfängt Nachrichten im Namen anderer Komponenten, die über IPC mit diesem Vorgang kommunizieren.

Abbildung 5-1. Diagramm zu ESXi-Host-Benutzer und Kernel-Speicher



CLI-Befehle für DFW (Distributed Firewall, verteilte Firewall)

Sie können mit der zentralen Befehlszeilenschnittstelle (CLI) von NSX Manager umfangreiche Informationen über verteilte Firewalls abrufen.

Verwenden der Befehle der zentralen Befehlszeilenschnittstelle (CLI) von Show dfw

Die gewünschten Informationen lassen sich in der folgenden Reihenfolge darstellen:

- 1 Melden Sie sich bei der zentralen Befehlszeilenschnittstelle (CLI) von NSX Manager mit den *Admin*-Anmeldedaten an.
- 2 Führen Sie die folgenden Befehle aus:
 - a Führen Sie den Befehl `show cluster all` aus, um alle Cluster anzuzeigen.

```
nsxmgr>show cluster all
```

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

- b Führen Sie den Befehl `show cluster <clusterID>` aus, um Hosts in einem bestimmten Cluster anzuzeigen.

```
nsxmgr> show cluster domain-c33
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
No.  Host Name           Host Id      Installation Status
1    esx-02a.corp.local     host-32      Enabled
2    esx-01a.corp.local     host-28      Enabled
```

- c Führen Sie `show host <hostID>` aus, um alle VMs auf einem Host anzuzeigen.

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

- d Führen Sie den Befehl `show vm <vmID>` aus, um Informationen für eine VM anzuzeigen, einschließlich Filternamen und vNIC-IDs:

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

- e Notieren Sie die vNIC-ID und führen Sie weitere Befehle wie `show dfw vnic <vnicID>` und `show dfw host <hostID> filter <filter ID> rules` aus:

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



```

nsxmgr> show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules
ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmp type 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmp type 8 from addrset ip-securitygroup-10 to addrset
ip-securitygroup-11 accept;
  rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
  rule 1009 at 8 inout protocol icmp icmp type 8 from addrset ip-securitygroup-11 to addrset
ip-securitygroup-12 accept;
  rule 1003 at 9 inout protocol ipv6-icmp icmp type 136 from any to any accept;
  rule 1003 at 10 inout protocol ipv6-icmp icmp type 135 from any to any accept;
  rule 1002 at 11 inout protocol udp from any to any port 67 accept;
  rule 1002 at 12 inout protocol udp from any to any port 68 accept;
  rule 1001 at 13 inout protocol any from any to any accept;
}

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

```

Verwenden des Befehls `export host-tech-support` der zentralen Befehlszeilenschnittstelle (CLI)

Der Befehl `export host-tech-support` ermöglicht es Ihnen, ein ESXi-Host-Support-Paket auf einen festgelegten Server zu exportieren. Zudem erfasst dieser Befehl mit NSX in Zusammenhang stehende Ausgaben und Dateien auf festgelegten Hosts. Hierzu zählen unter anderem die folgenden Elemente:

- VMKernel- und vsfwd-Protokolldateien
- Liste mit Filtern
- Liste mit DFW-Regeln
- Liste mit Containern
- SpoofGuard-Details
- Mit dem Host in Zusammenhang stehende Informationen
- Mit IP-Erkennung in Zusammenhang stehende Informationen
- RMQ-Befehlsausgaben
- Details zu Sicherheitsgruppe, Dienstprofil und Instanz
- Mit der ESX-CLI in Zusammenhang stehende Ausgaben

Dieser Befehl entfernt auch alle temporären Dateien auf NSX Manager.

So erfassen Sie mit NSX in Zusammenhang stehende Ausgaben und Dateien:

- 1 Melden Sie sich bei der zentralen Befehlszeilenschnittstelle (CLI) von NSX Manager mit den *Admin*-Anmeldedaten an.
- 2 Führen Sie die folgenden Befehle aus:
 - a `show cluster all` – Mit diesem Befehl können Sie die erforderliche Host-ID ermitteln.
 - b `export host-tech-support host-id scp uid@ip:/path` – Mit diesem Befehl können Sie das technische Support-Paket für NSX generieren und auf einen festgelegten Server kopieren.

Weitere Informationen finden Sie hier:

- [Befehlszeilen-Schnellreferenz zu NSX.](#)
- [Befehlszeilenschnittstellen-Referenz zu NSX.](#)

Fehlerbehebung für die verteilte Firewall

Dieser Abschnitt enthält Informationen zum Verständnis und zur Fehlerbehebung für die verteilte Firewall von VMware NSX 6.x.

Problem

- Die Veröffentlichung von Regeln für die verteilte Firewall scheitert.
- Die Aktualisierung von Regeln für die verteilte Firewall scheitert.

Ursache

Überprüfen Sie, ob die einzelnen unten angegebenen Fehlerbehebungsschritte für Ihre Umgebung gelten. Jeder Schritt enthält Anleitungen oder einen Link zu einem Dokument, mit denen Sie mögliche Ursachen beseitigen und korrigierende Maßnahmen wie erforderlich vornehmen können. Die Schritte werden in der für die Isolierung des Problems und für die Ermittlung der entsprechenden Lösung am geeignetsten erscheinenden Reihenfolge aufgeführt. Versuchen Sie nach jedem Schritt erneut, die Regeln für die verteilte Firewall zu aktualisieren bzw. zu veröffentlichen.

Lösung

- 1 Stellen Sie sicher, dass die NSX-VIBs auf jedem ESXi-Host im Cluster erfolgreich installiert worden sind. Dazu führen Sie auf jedem ESXi-Host im Cluster die nachfolgend aufgeführten Befehle aus.

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

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

NSX-Versionen vor NSX 6.2 verfügen über ein zusätzliches VIB:

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

Ab NSX 6.3.3 mit ESXi 6.0 oder höher werden die VIBs „esx-vxlan“ und „esx-vsip“ durch „esx-nsxv“ ersetzt.

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

- 2 Überprüfen Sie, ob auf den ESXi-Hosts der vShield-Stateful-Firewall-Dienst ausgeführt wird.

Beispiel:

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

vShield-Stateful-Firewall is running
```

- 3 Überprüfen Sie, ob der Nachrichtenbus ordnungsgemäß mit dem NSX Manager kommuniziert.

Dieser Vorgang wird automatisch vom Watchdog-Skript gestartet, das den Vorgang auch neu startet, wenn er aus einem unbekannten Grund beendet wird. Führen Sie diesen Befehl auf jedem ESXi-Host im Cluster aus.

Beispiel:

```
# ps | grep vsfwd

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

Es sollten mindestens 12 ausgeführte vsfwd-Vorgänge in der Befehlsausgabe vorhanden sein. Wenn weniger ausgeführte Vorgänge vorhanden sind (wahrscheinlich nur 2), wird vsfwd nicht ordnungsgemäß ausgeführt.

- 4 Überprüfen Sie, ob Port 5671 in der Firewallkonfiguration für die Kommunikation geöffnet ist.

Dieser Befehl stellt die VSFWD-Konnektivität zum RabbitMQ-Broker dar. Führen Sie diesen Befehl auf den ESXi-Hosts aus, um eine Liste der Verbindungen zwischen dem vsfwd-Vorgang auf dem ESXi-Host und dem NSX Manager anzuzeigen. Stellen Sie sicher, dass der Port 5671 in jeder externen Firewall der Umgebung für die Kommunikation geöffnet ist. Zudem sollten mindestens zwei Verbindungen an Port 5671 vorhanden sein. An Port 5671 können mehr Verbindungen bestehen, da auf dem ESXi-Host virtuelle NSX Edge-Maschinen bereitgestellt sind, die auch Verbindungen mit dem RMQ-Broker herstellen.

Beispiel:

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

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

5 Stellen Sie sicher, dass VSFWD konfiguriert ist.

Dieser Befehl sollte die IP-Adresse des NSX Manager anzeigen.

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

6 Wenn Sie für diesen ESXi-Host ein Hostprofil verwenden, stellen Sie sicher, dass die RabbitMQ-Konfiguration nicht im Hostprofil festgelegt ist.

Siehe:

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

7 Überprüfen Sie, ob die RabbitMQ-Anmeldedaten des ESXi-Hosts nicht mit denen von NSX Manager synchronisiert sind. Laden Sie die Tech-Support-Protokolle für NSX Manager herunter. Nachdem Sie alle Tech-Support-Protokolle für NSX Manager erfasst haben, suchen Sie in den Protokollen nach Einträgen folgender Art:

Replace host-420 with the host-id of the suspect host (Host-420 durch Host-ID des verdächtigen Hosts ersetzen).

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

8 Wenn Sie solche Einträge in den Protokollen für den verdächtigen ESXi-Host finden, synchronisieren Sie den Nachrichtenbus erneut.

Verwenden Sie zum erneuten Synchronisieren des Nachrichtenbus die REST-API. Erfassen Sie die Protokolle unmittelbar nach der erneuten Synchronisierung des Nachrichtenbus, um das Problem besser verstehen zu können.

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

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

Request Body:

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

- 9 Verwenden Sie den Befehl `export host-tech-support <host-id> scp <uid@ip:/path>` zum Erfassen hostspezifischer Firewallprotokolle.

Beispiel:

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

- 10 Überprüfen Sie mit dem Befehl `show dfw host host-id summarize-dvfilter`, ob die Firewallregeln auf einem Host bereitgestellt sind und auf die virtuellen Maschinen angewendet werden.

In der Ausgabe zeigt der Eintrag `module: vsip` an, dass das Modul „verteilte Firewall“ geladen wurde und ausgeführt wird. Der Eintrag `name` gibt die Firewall an, die auf jeder vNIC ausgeführt wird.

Zur Ermittlung der Host-IDs können Sie mit dem Befehl `show dfw cluster all` die IDs der Cluster-Domäne und anschließend mit dem Befehl `show dfw cluster domain-id` die Host-IDs abrufen.

Beispiel:

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

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

Slowpaths:

Filters:
world 342296 vmm0:2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979 vcUuid:'3f
43 54 76 8f 54 4e 5a-8d 01 59 65 4a 4e 99 79'
port 50331660 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979.eth1
vNic slot 2
  name: nic-342296-eth1-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 1
  name: nic-342296-eth1-dvfilter-generic-vmware-swsec.1
  agentName: dvfilter-generic-vmware-swsec
  state: IOChain Attached
  vmState: Detached
```

```

failurePolicy: failClosed
slowPathID: none
filter source: Alternate Opaque Channel
port 50331661 (disconnected)
vNic slot 2
name: nic-342296-eth2-vmware-sfw.2 <===== DFW filter
agentName: vmware-sfw
state: IOChain Detached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation
port 33554441 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979
vNic slot 2
name: nic-342296-eth0-vmware-sfw.2<===== DFW filter
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation

```

11 Führen Sie den Befehl `show dfw host hostID filter filterID rules` aus.

Beispiel:

```

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

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

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

```

12 Führen Sie den Befehl `show dfw host hostID filter filterID addrsets` aus.

Beispiel:

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

addrset dst1011 {
ip 172.16.10.10,
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-10 {
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-11 {
ip 172.16.20.11,
ip fe80::250:56ff:feae:23b9,
}
addrset ip-securitygroup-12 {
ip 172.16.30.11,
ip fe80::250:56ff:feae:d42b,
}
addrset src1013 {
ip 172.16.10.12,
ip 172.17.10.11,
ip fe80::250:56ff:feae:cf88,
ip fe80::250:56ff:feae:f86b,
}
```

13 Wenn Sie die obigen Schritte zur Fehlerbehebung durchgeführt haben und dennoch keine Firewallregeln auf den virtuellen Hostmaschinen veröffentlichen können, erzwingen Sie über die Benutzeroberfläche von NSX Manager oder über den nachfolgend aufgeführten REST-API-Aufruf eine Synchronisierung auf Hostebene.

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

Lösung

Anmerkungen:

- Stellen Sie sicher, dass VMware Tools auf den virtuellen Maschinen ausgeführt wird, wenn in den Firewallregeln keine IP-Adressen verwendet werden. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/2084048>.

In VMware NSX 6.2.0 wurde die Option zur Erkennung der IP-Adresse der VM mithilfe von DHCP-Snooping oder ARP-Snooping eingeführt. Mit diesen neuen Erkennungsmechanismen kann NSX die auf IP-Adressen basierten Sicherheitsregeln auf virtuellen Maschinen erzwingen, auf denen VMware Tools nicht installiert ist. Weitere Informationen finden Sie in den Versionshinweisen zu NSX 6.2.0.

Die verteilte Firewall wird aktiviert, sobald der Hostvorbereitungsvorgang abgeschlossen ist. Wenn eine virtuelle Maschine grundsätzlich keine verteilte Firewall benötigt, kann sie der Ausschlussliste hinzugefügt werden (standardmäßig werden NSX Manager, NSX Controller und Edge Services Gateways automatisch von der Funktion der Verteilten Firewall ausgeschlossen). Es besteht die Möglichkeit, dass der Zugriff auf vCenter Server nach dem Erstellen einer Deny-All-Regel (Alles-Verweigern-Regel) in der Verteilten Firewall blockiert wird. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/2079620>.

- Wenn Sie für die Fehlerbehebung der Verteilten Firewall von NSX 6.x von VMware Unterstützung vom technischen Support von VMware benötigen, ist Folgendes erforderlich:
 - Ausgabe des Befehls `show dfw host hostID summarize-dvfilter` auf jedem ESXi-Host im Cluster.
 - verteilte Firewall-Konfiguration der Registerkarte **Networking and Security > Firewall > Allgemein (Networking and Security > Firewall > General)** durch Klicken auf **Konfiguration exportieren (Export Configuration)**. Damit wird die verteilte Firewall-Konfiguration in ein XML-Format exportiert.
 - NSX Manager-Protokolle. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/2074678>.
 - vCenter Server-Protokolle. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/1011641>.

Identitätsbasierte Firewall

Problem

Die Veröffentlichung oder die Aktualisierung der Regeln einer identitätsbasierten Firewall schlägt fehl.

Ursache

Die identitätsbasierte Firewall (IDFW) ermöglicht die Verwendung von benutzerbasierten Regeln für die verteilte Firewall (Distributed Firewall, DFW).

Benutzerbasierte Regeln für die verteilte Firewall werden von der Mitgliedschaft in einer Active Directory-Gruppe bestimmt. IDFW prüft, wo Active Directory-Benutzer angemeldet sind, und ordnet die Anmeldungen jeweils einer IP-Adresse zu, die von der Verteilten Firewall zur Anwendung der Firewallregeln verwendet wird. Die identitätsbasierte Firewall erfordert entweder ein Guest Introspection-Framework und/oder Active Directory Event Log Scraper.

Lösung

- 1 Stellen Sie sicher, dass die vollständige oder inkrementelle Synchronisierung des Active Directory-Servers bei NSX Manager funktioniert.
 - a Melden Sie sich in vSphere Web Client bei dem vCenter an, das mit NSX Manager verknüpft ist.
 - b Wechseln Sie zu **Start > Networking & Security > NSX Manager (Home > Networking & Security > NSX Managers)** und wählen Sie Ihren NSX-Manager aus der Liste aus.
 - c Wählen Sie die Registerkarte **Verwalten (Manage)** und dann die Registerkarte **Domänen (Domains)** aus. Wählen Sie Ihre Domäne aus der Liste aus. Stellen Sie sicher, dass in der Spalte **Letzter Synchronisierungsstatus (Last Synchronization Status)** der Eintrag SUCCESS (ERFOLG) angezeigt wird und unter **Letzte Synchronisierungszeit (Last Synchronization Time)** die entsprechende Uhrzeit enthalten ist.
- 2 Wenn Ihre Firewallumgebung die Methode des Ereignisprotokoll-Scraping für die Erkennung der Anmeldung verwendet, führen Sie die folgenden Schritte durch, um sicherzustellen, dass für Ihre Domäne ein Ereignisprotokoll-Server konfiguriert ist:
 - a Melden Sie sich in vSphere Web Client bei dem vCenter an, das mit NSX Manager verknüpft ist.
 - b Wechseln Sie zu **Start > Networking & Security > NSX Manager (Home > Networking & Security > NSX Managers)** und wählen Sie Ihren NSX-Manager aus der Liste aus.
 - c Wählen Sie die Registerkarte **Verwalten (Manage)** und dann die Registerkarte **Domänen (Domains)** aus. Wählen Sie Ihre Domäne aus der Liste aus. Hier können Sie die Domänenkonfiguration im Detail überprüfen und bearbeiten.
 - d Wählen Sie **Ereignisprotokoll-Server (Event Log Servers)** aus den Domänendetails aus und prüfen Sie, ob Ihr Ereignisprotokoll-Server hinzugefügt wurde.
 - e Wählen Sie Ihren Ereignisprotokoll-Server aus und stellen Sie sicher, dass in der Spalte **Letzter Synchronisierungsstatus (Last Sync Status)** der Eintrag SUCCESS (ERFOLG) angezeigt wird und unter **Uhrzeit der letzten Synchronisierung (Last Sync Time)** die entsprechende Uhrzeit.
- 3 Wenn Ihre Firewallumgebung Guest Introspection verwendet, muss das Framework auf den Computerclustern bereitgestellt werden, auf denen sich Ihre IDFW-geschützten virtuellen Maschinen befinden. Der Systemzustand des Dienstes muss in der Benutzeroberfläche als grün angezeigt werden. Diagnoseinformationen zu Guest Introspection finden Sie in den Knowledgebase-Artikeln „Troubleshooting vShield Endpoint/NSX Guest Introspection“ (Fehlerbehebung für vShield Endpoint/NSX Guest Introspection; siehe <https://kb.vmware.com/kb/2094261>) und „Collecting logs in VMware NSX for vSphere 6.x Guest Introspection Universal Service Virtual Machine“ (Erfassen von Protokollen in der globalen Dienst-VM von VMware NSX for vSphere 6.x Guest Introspection; siehe <https://kb.vmware.com/kb/2144624>).

- 4 Nach der Prüfung der Konfiguration Ihrer Methode zur Erkennung der Anmeldung stellen Sie sicher, dass NSX Manager Anmeldeereignisse empfängt.
 - a Melden Sie sich als Active Directory-Benutzer an.
 - b Führen Sie den im Folgenden aufgeführten Befehl zur Abfrage von Anmeldeereignissen aus. Stellen Sie sicher, dass Ihr Benutzer in den Ergebnissen zurückgegeben wird. GET `https://<nsxmgr-ip>/1.0/identity/userIpMapping`.

Example output:

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

- 5 Stellen Sie sicher, dass Ihre Sicherheitsgruppe in einer Firewallregel verwendet wird oder über eine zugewiesene Sicherheitsrichtlinie verfügt. Die Sicherheitsgruppe wird in IDFW erst verarbeitet, wenn eine der im Folgenden aufgeführten Bedingungen zutrifft.
- 6 Nach der Prüfung, ob IDFW Anmeldungen korrekt erkennt, stellen Sie sicher, dass der ESXi-Host mit Ihrer Desktop-VM die korrekte Konfiguration erhält. Für diese Schritte wird die zentrale NSX Manager-CLI verwendet. Um die IP-Adresse der Desktop-VM in der Liste **ip-securitygroup** zu prüfen, führen Sie folgende Schritte durch:
 - a Unter [CLI-Befehle für DFW \(Distributed Firewall, verteilte Firewall\)](#) finden Sie Erläuterungen zum Abrufen des für die Desktop-VM angewendeten Filternamens.
 - b Führen Sie den Befehl `show dfw host hostID filter filterID rules` aus, um die Elemente der ermittelten Regeln für die verteilte Firewall anzuzeigen.
 - c Führen Sie den Befehl `show dfw host hostID filter filterID addrsets` aus, um die IP-Adressen in der Liste `ip-securitygroup` anzuzeigen. Stellen Sie sicher, dass Ihre IP-Adresse in der Liste enthalten ist.

Lösung

Hinweis: Für die Fehlerbehebung bei einer identitätsbasierten Firewall mithilfe des technischen Supports von VMware sind folgende Daten hilfreich:

- Bei Verwendung des Ereignisprotokoll-Scraping Angaben zum Umfang in Active Directory:
 - Anzahl der Domänen für einen einzelnen NSX Manager
 - Anzahl der Gesamtstrukturen

Anzahl der Benutzer pro Gesamtstruktur

Anzahl der Benutzer pro Domäne

Anzahl der Active Directory-Gruppen pro Domäne

Anzahl der Benutzer pro Active Directory-Gruppe

Anzahl von Active Directory pro Benutzer

Anzahl der Domänen-Controller

Anzahl der Active Directory-Protokollserver

- Angaben zum Umfang der Benutzeranmeldung:
 - Durchschnittliche Anzahl der Benutzer pro Minute
- Bereitstellungsdetails mithilfe von IDFW mit VDI:
 - Anzahl der VDI-Desktops pro VC
 - Anzahl der Hosts pro VC
 - Anzahl der VDI-Desktops pro Host
- Bei Verwendung von Guest Introspection:
 - Version von VMware Tools (Guest Introspection-Treiber)
 - Version des Windows-Gastbetriebssystems

Fehlerbehebung beim Lastausgleich

6

Der Load Balancer von NSX Edge aktiviert den Netzwerkdatenverkehr, um mehreren Pfaden zu einem bestimmten Ziel zu folgen. Er verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Es stehen zwei Typen von Load-Balancing-Diensten zur Konfiguration in NSX zur Verfügung: ein „Einarmiger“-Modus, auch „Proxy-Modus“ genannt, und der Inline-Modus, auch als „Transparenter Modus“ bezeichnet. Weitere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Bevor Sie mit der Fehlerbehebung und der Überprüfung der Konfiguration beginnen, verfassen Sie eine präzise Beschreibung des Fehlers, erstellen Sie eine Topologie-Zuordnung für den Client, virtuellen Server und Backend-Server und informieren Sie sich über die Anwendungsanforderungen.

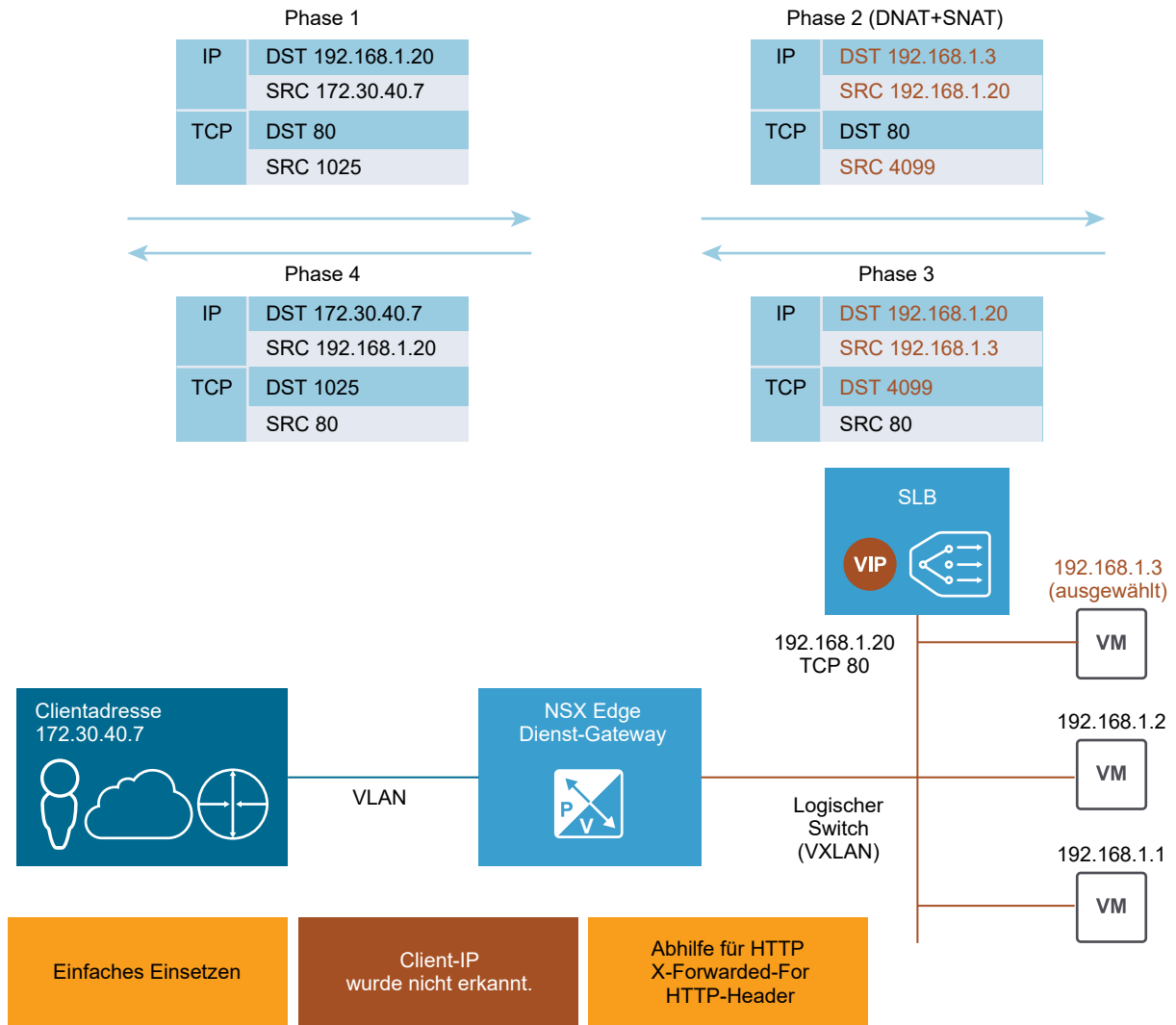
Beispielsweise besteht ein Unterschied, ob ein Client keine Verbindung herstellen kann oder ob nach dem Verbindungsaufbau zufällige Sitzungsfehler auftreten. Die Fehlerbehebung beim Load Balancer beginnt immer mit der Überprüfung von Verbindungsfehlern.

Dieses Kapitel enthält die folgenden Themen:

- [Konfiguration eines einarmigen Load Balancer](#)
- [Flussdiagramm: Fehlerbehebung für den Load Balancer](#)
- [Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche](#)
- [Fehlerbehebung für Load Balancer mithilfe der Befehlszeilenschnittstelle](#)
- [Allgemeine Probleme mit dem Load Balancer](#)

Konfiguration eines einarmigen Load Balancer

Das Edge Services Gateway (ESG) kann als Proxy für den eingehenden Benutzerdatenverkehr angesehen werden.



Im Proxymodus verwendet der Load Balancer seine eigene IP-Adresse als Quelladresse, um Anforderungen an einen Backend-Server zu senden. Der Backend-Server interpretiert jeden Datenverkehr so, als würde er vom Load Balancer gesendet und antwortet dem Load Balancer direkt. Dieser Modus wird auch als SNAT-Modus oder nicht-transparenter Modus bezeichnet. Weitere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Ein typischer einarmiger NSX-Load-Balancer wird in demselben Subnetz wie seine Backend-Server bereitgestellt, getrennt vom logischen Router. Der virtuelle Server des NSX-Load-Balancer hört eine virtuelle IP auf eingehende Anforderungen ab und verteilt die Anforderungen an die Backend-Server. Für den Datenverkehr in der Gegenrichtung ist eine umgekehrte NAT erforderlich, um die Quell-IP-Adresse vom Backend-Server in eine virtuelle IP- (VIP-)Adresse umzuwandeln und dann die VIP-Adresse an den Client zu senden. Ohne diesen Vorgang wird die Verbindung zum Client unterbrochen.

Nachdem das ESG den Datenverkehr empfangen hat, werden zwei Operationen durchgeführt: Mit der „Destination Network Address Translation“ (DNAT) wird die VIP-Adresse in die IP-Adresse einer Load-Balancer-Maschine umgewandelt. Mit der „Source Network Address Translation“ (SNAT) wird die Client-IP-Adresse durch die ESG-IP-Adresse ersetzt.

Dann sendet der ESG-Server den Datenverkehr an den Load-Balancer-Server und der Load-Balancer-Server sendet die Antwort zurück an das ESG und weiter an den Client. Diese Option ist sehr viel einfacher zu konfigurieren als der Inline-Modus. Es sind aber zwei potenzielle Einschränkungen vorhanden. Erstens erfordert dieser Modus einen dedizierten ESG-Server, zweitens kennen die Load-Balancer-Server die Original-IP-Adresse des Client nicht. Eine Problemumgehung für HTTP/HTTPS-Anwendungen besteht in der Aktivierung von „X-Forwarded-For“ einfügen“ im HTTP-Anwendungsprofil, damit die Client-IP-Adresse in den X-Forwarded-For-HTTP-Header der Anforderung übertragen wird, die zum Backend-Server gesendet wird.

Wenn der Backend-Server die Client-IP-Adresse für andere Anwendungen als HTTP/HTTPS kennen muss, können Sie den IP-Pool so konfigurieren, dass er transparent ist. Wenn sich die Clients nicht in demselben Subnetz befinden wie die Backend-Server, sollte der Inline-Modus verwendet werden. Andernfalls müssen Sie die IP-Adresse des Load Balancer als Standard-Gateway des Backend-Servers verwenden.

Hinweis In der Regel gibt es drei Methoden, um die Verbindungsintegrität zu gewährleisten:

- Inline-/Transparent-Modus
- SNAT-/Proxy-/nicht-transparenter Modus (siehe Erläuterungen weiter oben)
- Direct Server Return (SDR) – derzeit nicht unterstützt

Im DSR-Modus sendet der Backend-Server die Antwort direkt an den Client. Aktuell unterstützt der NSX-Load-Balancer DSR nicht.

Verfahren

- 1 Lassen Sie uns als Beispiel einen einarmigen virtuellen Server mit SSL-Offloading konfigurieren. Erstellen Sie ein Zertifikat durch Doppelklicken auf das Edge und durch anschließende Auswahl von **Verwalten > Einstellungen > Zertifikat (Manage > Settings > Certificate)**.

- 2 Aktivieren Sie den Dienst des Load Balancer durch Auswahl von **Verwalten > Load Balancer > Globale Konfiguration > Bearbeiten (Manage > Load Balancer > Global Configuration > Edit)**.

Edit Load balancer global configuration

☒ Enable Load Balancer

☐ Enable Acceleration

☐ Logging

Log Level: **Info** ▼

☐ Enable Service Insertion

Service Definition:

Service Configuration:

Deployment Specification:

- 3 Erstellen Sie ein HTTPS-Anwendungsprofil durch Auswahl von **Verwalten > Load Balancer > Anwendungsprofile (Manage > Load Balancer > Application Profiles)**.

New Profile ?

Name:

Type: **HTTPS** ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: **None** ▼

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica... **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

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

Hinweis Die in der obigen Abbildung verwendeten selbstsignierten Zertifikate dienen nur der Veranschaulichung.

- 4 Optional klicken Sie auf **Verwalten > Load Balancer > Dienstüberwachung (Manage > Load Balancer > Service Monitoring)** und ändern Sie die Standarddienstüberwachung vom Basis-HTTP/HTTPS-Protokoll in spezifische URL/URIs je nach Anforderung.

- 5 Erstellen Sie Serverpools durch Auswahl von **Verwalten > Load Balancer > Pools (Manage > Load Balancer > Pools)**.

Wenn Sie den SNAT-Modus verwenden möchten, lassen Sie das Kontrollkästchen **Transparent** in der Poolkonfiguration deaktiviert.

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

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

☒ Transparent

OK Cancel

Stellen Sie sicher, dass die VMs aufgelistet und aktiviert sind.

- 6 Optional klicken Sie auf **Verwalten > Load Balancer > Pools > Poolstatistik anzeigen (Manage > Load Balancer > Pools > Show Pool Statistics)**, um den Status zu überprüfen.

Stellen Sie sicher, dass der Mitgliedsstatus „UP“ ist.

- 7 Erstellen Sie einen virtuellen Server durch Auswahl von **Verwalten > Load Balancer > Virtueller Server (Manage > Load Balancer > Virtual Servers)**.

Wenn Sie den L4-Load-Balancer für UDP oder ein leistungsstärkeres TCP verwenden möchten, aktivieren Sie **Beschleunigung aktivieren (Enable Acceleration)**. Wenn Sie **Beschleunigung aktivieren (Enable Acceleration)** aktiviert haben, stellen Sie sicher, dass der Firewallstatus auf dem Load-Balancer-NSX Edge auf **Aktiviert (Enabled)** festgelegt ist, da für L4 SNAT eine Firewall erforderlich ist.

General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

Application Profile: * OneArmWeb-01 ▼

Name: * Web-Tier-VIP-01

Description:

IP Address: * 172.16.10.10 [X] Select IP Address

Protocol: HTTPS ▼

Port: * 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

Stellen Sie sicher, dass die IP-Adresse an den Serverpool gebunden ist.

- 8 Optional können Sie, wenn Sie eine Anwendungsregel verwenden, die Konfiguration unter **Verwalten > Load Balancer > Anwendungsregeln (Manage > Load Balancer > Application Rules)** überprüfen.

Add Application Rule ?

Name: App-Rule-1

Script: # A sample application rule to log the name of the virtual server
capture request header Host len 32

- 9 Bei der Verwendung einer Anwendungsregel müssen Sie sicherstellen, dass die Anwendungsregel mit dem virtuellen Server verbunden ist. Dies können Sie unter **Verwalten > Load Balancer > Virtueller Server > Erweitert (Manage > Load Balancer > Virtual Servers > Advanced)**überprüfen.

Weitere unterstützte Beispiele finden Sie unter <https://communities.vmware.com/docs/DOC-31772>.

Edit Virtual Server ?

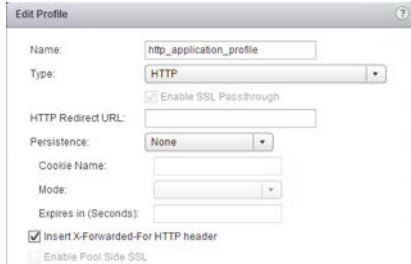
General | **Advanced**

Application Rules:

+ X [Icons] Filter ▼

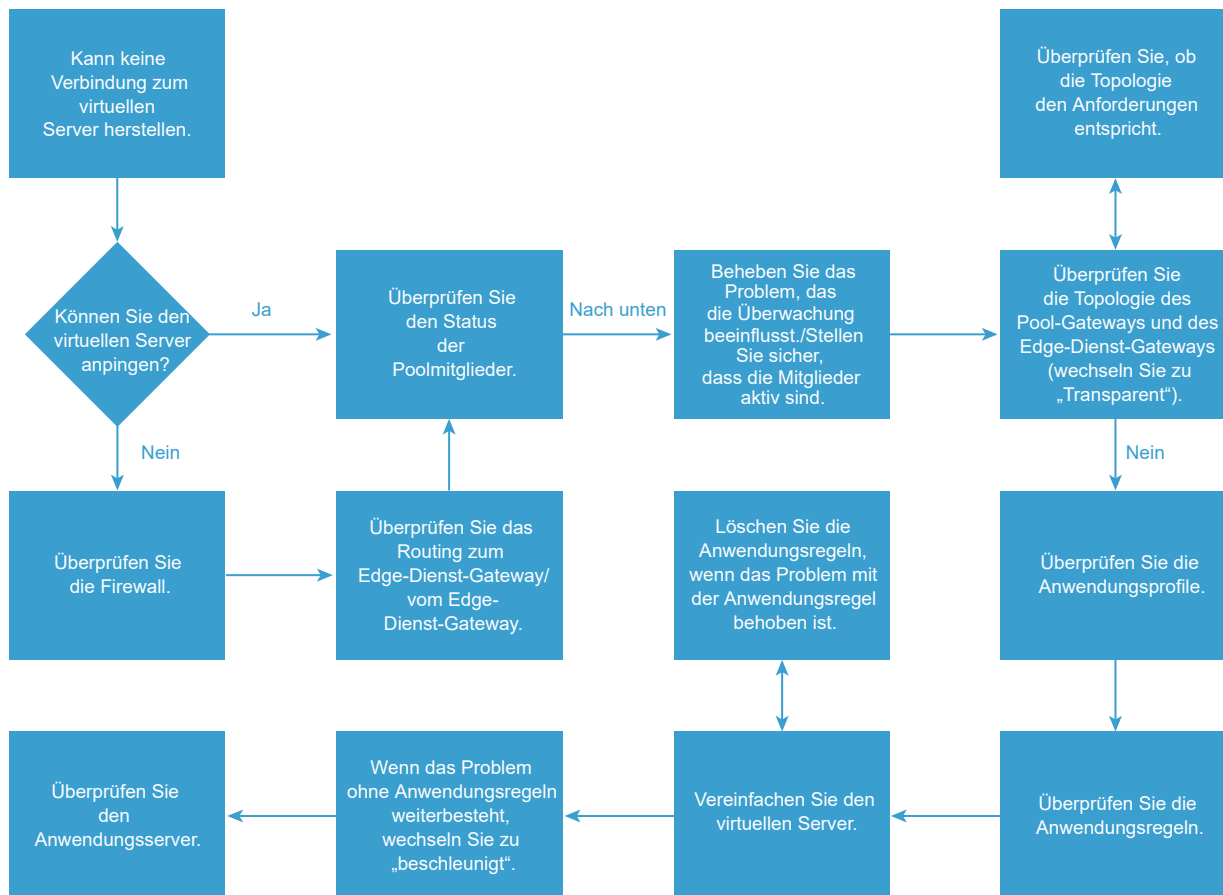
Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

Im nicht-transparenten Modus kann der Backend-Server nicht die Client-IP, aber die interne IP-Adresse des Load Balancer erkennen. Als Problemumgehung für den HTTP/HTTPS-Datenverkehr aktivieren Sie **HTTP-Header 'X-Forwarded-For' einfügen (Insert X-Forwarded-For HTTP header)**. Wenn diese Option aktiviert ist, fügt der Edge Load Balancer den Header „X-Forwarded-For“ mit dem Wert der Client-Quell-IP-Adresse hinzu.



Flussdiagramm: Fehlerbehebung für den Load Balancer

Das folgende Flussdiagramm bietet einen Überblick über die Fehlerbehebung bei Load-Balancer-Problemen.



Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche

Sie können die Load-Balancer-Konfiguration über den vSphere Web Client überprüfen. Sie können mit der Benutzeroberfläche verschiedene Load-Balancer-Fehler beheben.

Nachdem klar ist, was funktionieren sollte, und nach dem Definieren des Problems überprüfen Sie die Konfiguration über die Benutzeroberfläche wie folgt:

Voraussetzungen

Notieren Sie sich folgende Daten:

- IP-Adresse, Protokoll und Port des virtuellen Servers
- IP-Adresse und Port der Backend-Anwendungsserver
- Die gewünschte Topologie: Inline oder einarmig Weitere Informationen finden Sie im Abschnitt zum logischen Load Balancer im *Administratorhandbuch für NSX*.
- Überprüfen Sie die Traceroute und ermitteln Sie mit anderen Netzwerkverbindungstools, ob die Pakete an das richtige Ziel übertragen werden (Edge-Dienst-Gateway).
- Überprüfen Sie, ob alle Upstream-Firewalls den Datenverkehr korrekt zulassen.
- Definieren Sie das aufgetretene Problem. Beispiel: Die DNS-Einträge für den virtuellen Server sind korrekt, man erhält aber keine korrekten Inhalte oder falsche Inhalte zurück, usw.

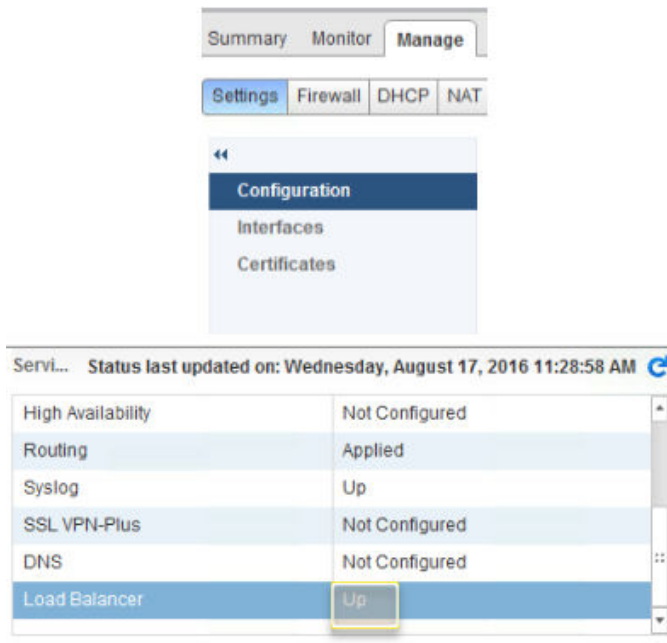
Problem

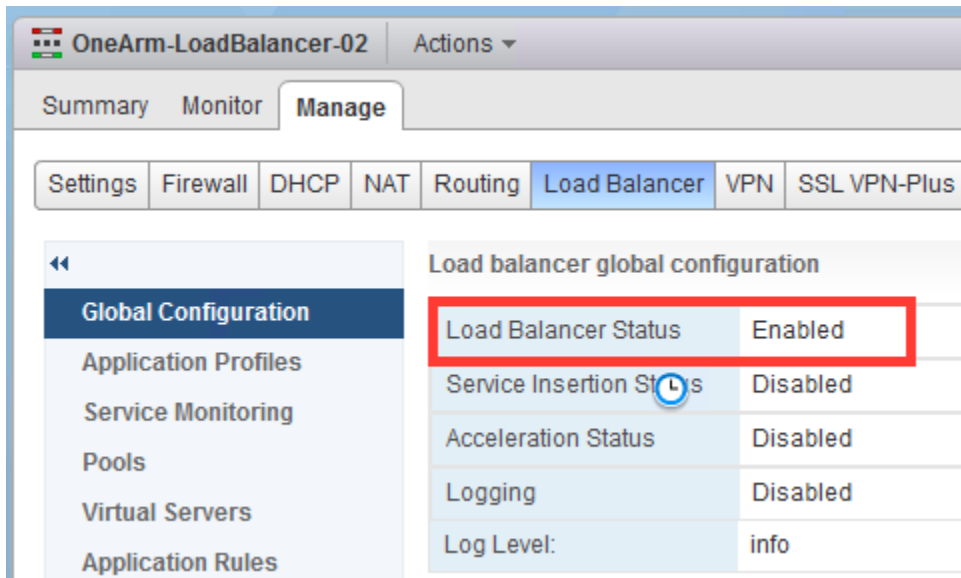
Der Load Balancer funktioniert nicht ordnungsgemäß.

Lösung

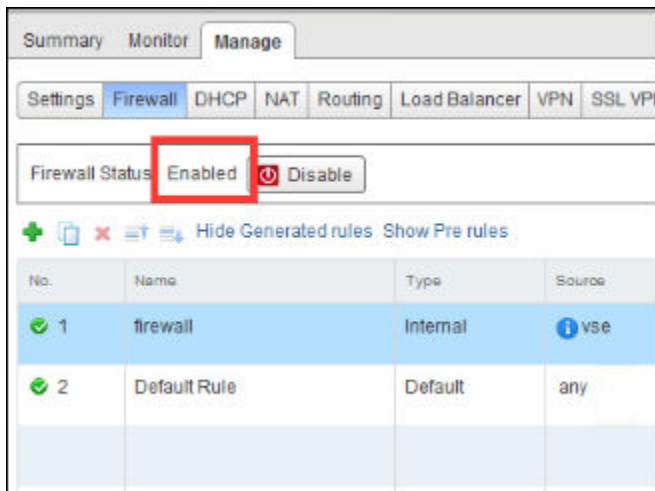
- 1 Überprüfen Sie die folgenden Anwendungsvoraussetzungen: Protokolle, die vom Load Balancer unterstützt werden müssen (TCP, UDP, HTTP, HTTPS), Ports, Persistenzanforderungen und Poolmitglieder.
 - Sind der Load Balancer und die Firewall aktiviert? Verfügt das Edge-Dienst-Gateway über die korrekten Routen?
 - Welche IP-Adresse, welchen Port und welches Protokoll sollte der virtuelle Server überwachen?
 - Wird SSL-Offloading verwendet? Benötigen Sie für die Kommunikation mit Backend-Servern SSL?
 - Verwenden Sie Anwendungsregeln?
 - Welche Topologie liegt vor? Der NSX-Load Balancer muss den gesamten Datenverkehr vom Client und vom Server analysieren.
 - Ist der NSX-Load Balancer inline oder wird die Clientquelladresse übersetzt, um sicherzustellen, dass der Rückdatenverkehr zurück zum Load Balancer fließt?

- 2 Navigieren Sie zum NSX Edge und überprüfen Sie die Konfigurationen, die erforderlich sind, um das Load-Balancing zu aktivieren und den Datenverkehr wie folgt fließen zu lassen:
 - a Überprüfen Sie, ob der Load Balancer als **Hochgefahren (Up)** aufgeführt wird.





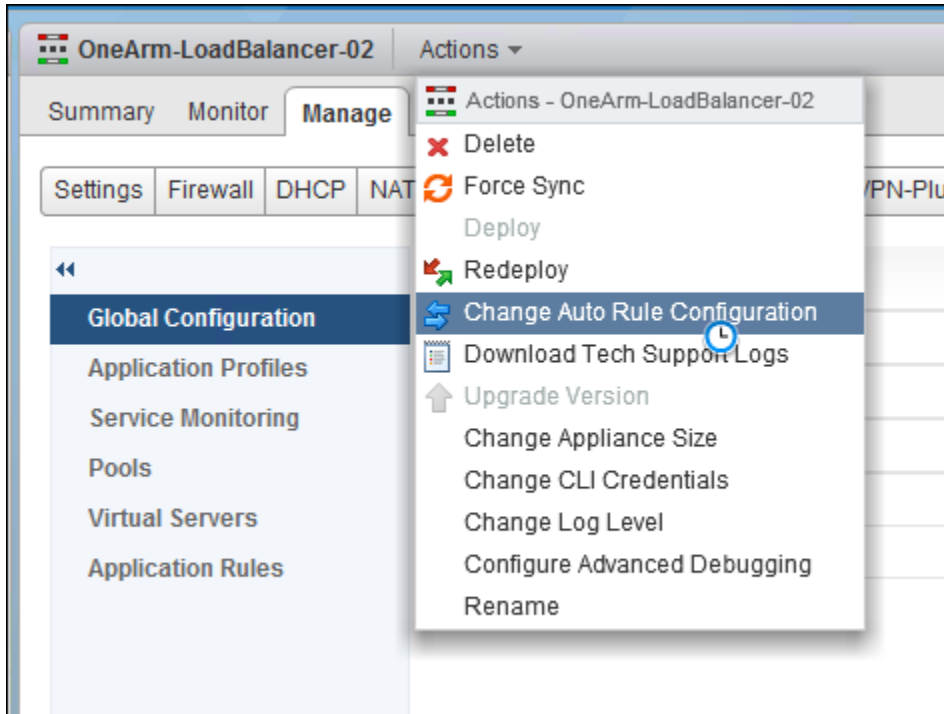
- b Überprüfen Sie, ob die Firewall **Aktiviert (Enabled)** ist. Für beschleunigte virtuelle Server MUSS die Firewall aktiviert sein. Nicht beschleunigte TCP- und L7-HTTP/HTTPS-VIPs müssen über eine Richtlinie verfügen, die Datenverkehr zulässt. Beachten Sie, dass sich Firewallfilter nicht auf beschleunigte virtuelle Server auswirken.



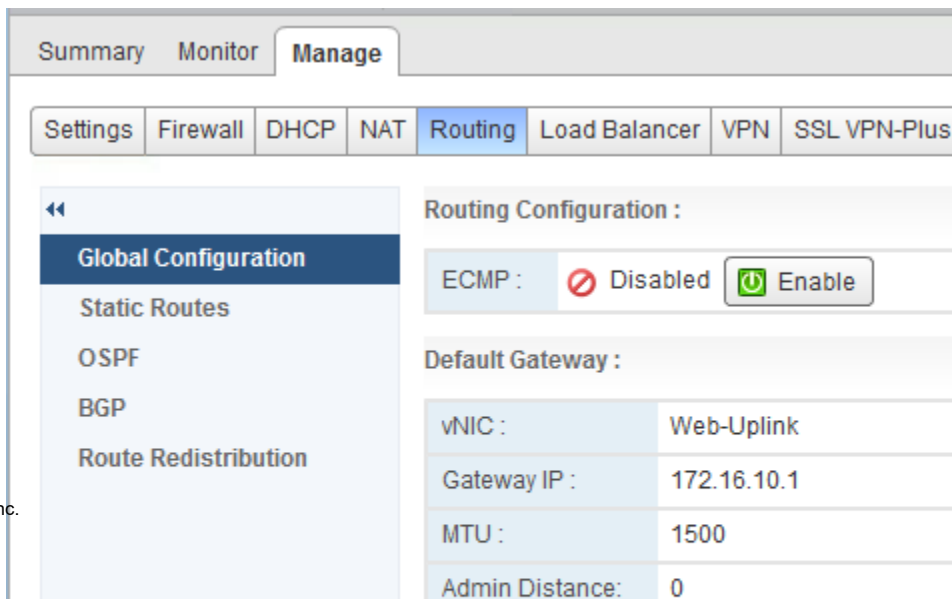
- c Stellen Sie sicher, dass die NAT-Regeln für den virtuellen Server erstellt werden. Klicken Sie auf der Registerkarte **NAT** auf den Link **Interne Regeln ausblenden (Hide internal rules)** oder **Interne Regeln einblenden (Unhide internal rules)**, um die Überprüfung zu beginnen.

Hinweis Wenn Sie das Load-Balancing aktiviert und die Dienste konfiguriert haben, aber keine NAT-Regeln festgelegt haben, bedeutet dies, dass die automatische Regelkonfiguration nicht aktiviert wurde.

- d Sie können die automatischen Regelkonfigurationen ändern. Weitere Informationen finden Sie im Abschnitt „Automatische Regelkonfiguration ändern“ im *Administratorhandbuch für NSX*. Wenn ein NSX-Edge-Dienst-Gateway bereitgestellt wird, haben Sie die Möglichkeit, die automatische Regelkonfiguration einzurichten. Wenn diese Option bei der Bereitstellung des Edge-Dienst-Gateways nicht ausgewählt wurde, müssen Sie sie aktivieren, damit der Load Balancer ordnungsgemäß funktioniert. Überprüfen Sie den Mitgliedsstatus des Pools mithilfe der Benutzeroberfläche.



- e Überprüfen Sie das Routing und stellen Sie sicher, dass das Edge-Dienst-Gateway über eine Standardroute oder eine statische Route zu Ihren Clientsystemen und den Backend-Servern verfügt. Wenn keine Route zu den Servern vorliegt, schlägt die Prüfung des Systemzustands fehl. Wenn Sie ein dynamisches Routing-Protokoll verwenden, müssen Sie möglicherweise die Befehlszeile nutzen. Weitere Informationen finden Sie unter [Befehlszeilenschnittstelle \(CLI\) für das NSX-Routing](#).
- a Überprüfen Sie die Standardroute.



Gateway über eine Schnittstelle im Subnetz verfügt. Häufig sind die Anwendungsserver mit diesen Servern verbunden.

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

aces of this NSX Edge.

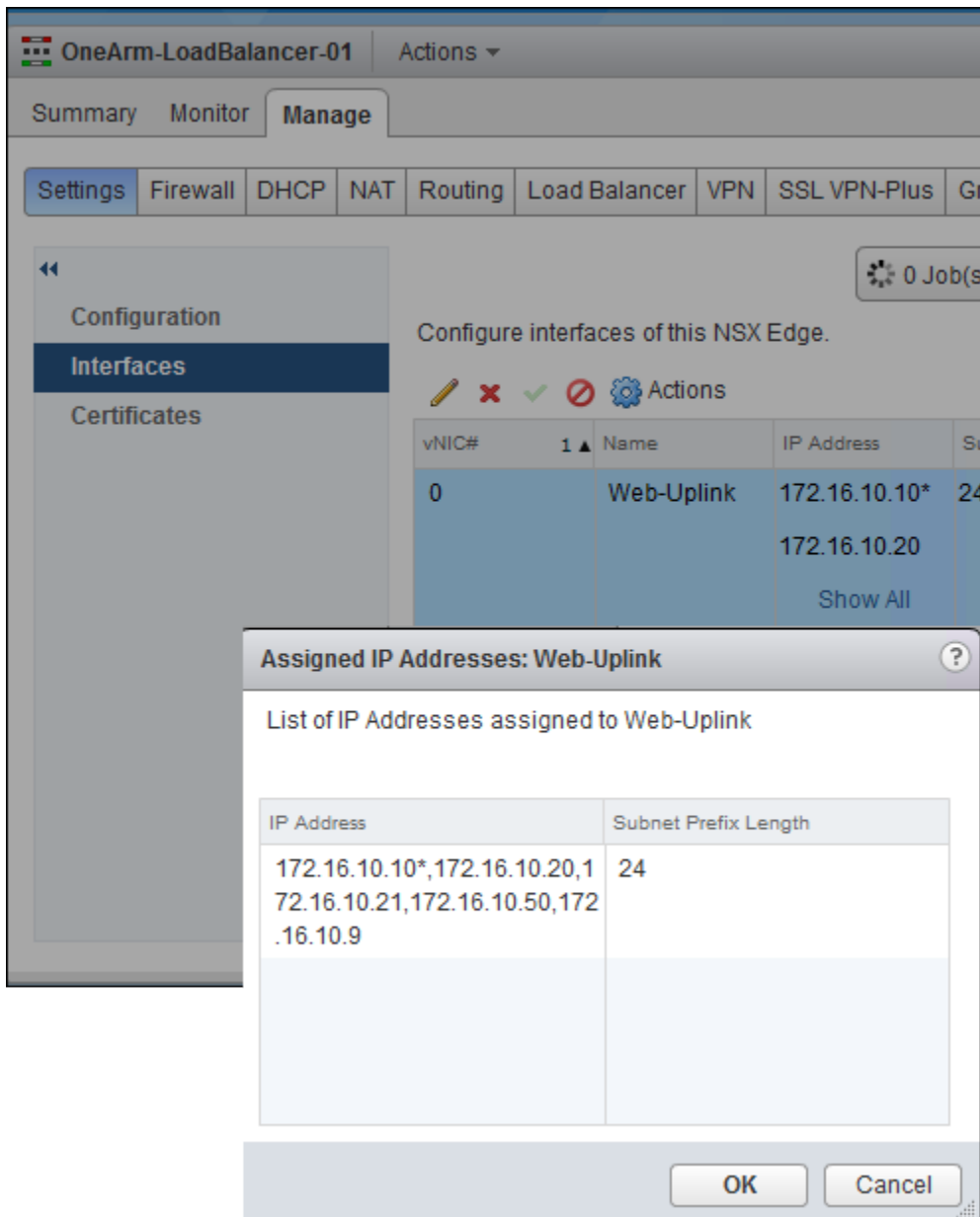
Actions

Filter

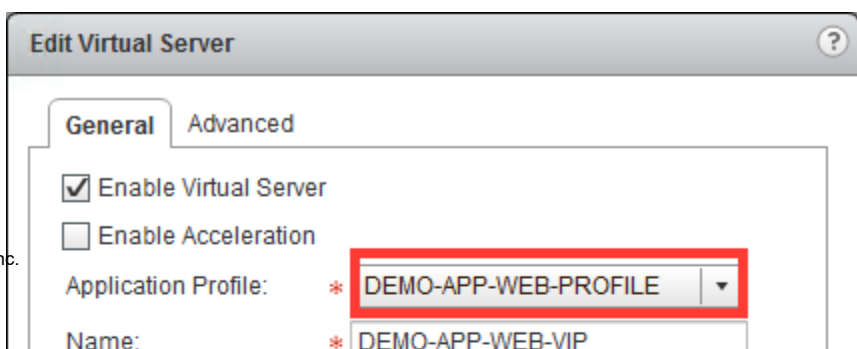
Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
Web-Uplink	172.16.10.10*	24	Web-Tier-01	Uplink	✓
	172.16.10.20				
	Show All				
INLINE_SUBNI	172.16.100.1*	24	INLINE_SUBNI	Internal	✓
vnic2				Internal	✗
vnic3				Internal	✗
vnic4				Internal	✗
vnic5				Internal	✗

- c Überprüfen Sie auf der Registerkarte **Routing > Statische Routen (Static Routes)** die statischen Routen.

- 3 Überprüfen Sie die IP-Adresse, den Port und das Protokoll des virtuellen Servers.
 - a Doppelklicken Sie auf einen NSX Edge und navigieren Sie zu **Verwalten (Manage) > Einstellungen (Settings) > Schnittstellen (Interfaces)**. Überprüfen Sie, ob die IP-Adresse des virtuellen Servers zu einer Schnittstelle hinzugefügt wurde.



- b Überprüfen Sie, ob für den virtuellen Server die korrekte IP-Adresse, Port(s) und Protokolle konfiguriert wurden, um die Anwendung zu unterstützen.
 - a Überprüfen Sie das vom virtuellen Server verwendete Anwendungsprofil.



das Protokoll (HTTP oder HTTPS) des virtuellen Servers.

Edit Virtual Server

General | Advanced

☒ Enable Virtual Server
☐ Enable Acceleration

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

Name: * DEMO-APP-WEB-VIP

Description:

IP Address: * 172.16.10.20 × [Select IP Address](#)

Protocol: HTTPS ▼

Port: * 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

OK Cancel

- c Überprüfen Sie, ob das Anwendungsprofil die unterstützte Persistenzmethode, den Typ (Protokoll) und SSL (wenn benötigt) einhält bzw. aufweist. Wenn Sie SSL nutzen, stellen Sie sicher, dass ein Zertifikat mit dem korrekten Namen und Ablaufdatum verwendet wird.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

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

Cipher: Default

Client Authentication: Ignore

OK Cancel

- d Überprüfen Sie, ob für die Verbindungen der Clients das korrekte Zertifikat genutzt wird.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☒ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

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

Cipher: Default

Client Authentication: Ignore

OK Cancel

- e Überprüfen Sie, ob ein Clientzertifikat benötigt wird, die Clients aber nicht konfiguriert sind. Überprüfen Sie außerdem, ob Sie eine begrenzte Chiffrenliste ausgewählt haben, die zu stark begrenzt ist (z. B. Clients, die ältere Browser verwenden).

Edit Profile

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificates Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

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

Cipher: Default

Client Authentication: Ignore

OK Cancel

- f Überprüfen Sie, ob Sie SSL für die Backend-Server benötigen.

Edit Profile

Name: DEMO-APP-WEB-PROFILE

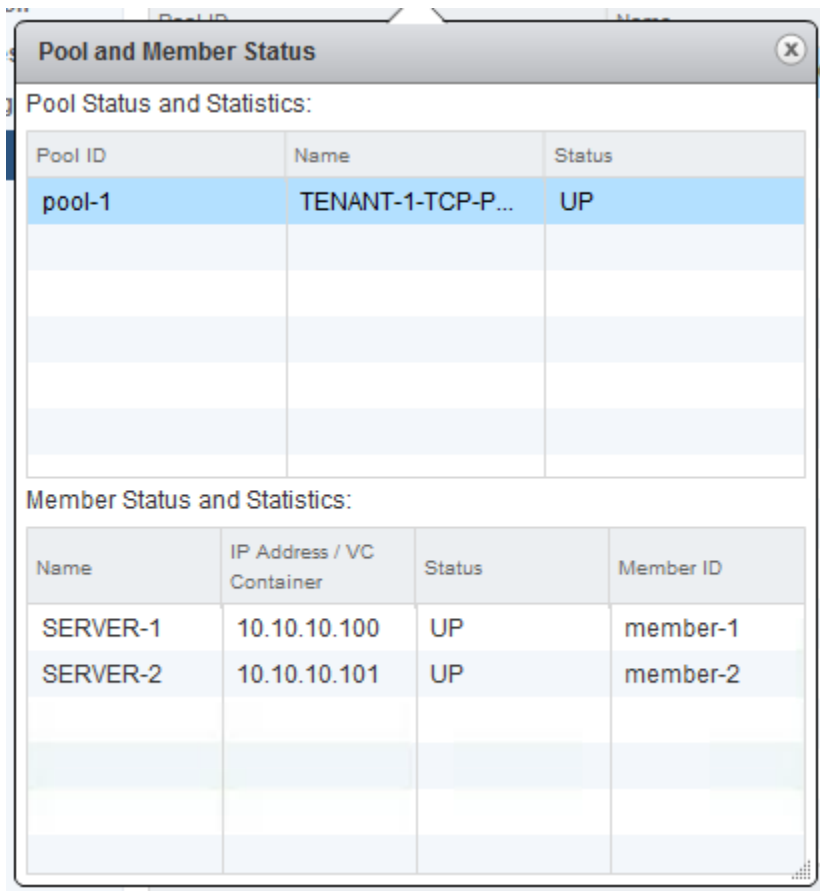
Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

4 Überprüfen Sie den Poolstatus und die -konfiguration wie folgt:

- a Überprüfen Sie den Poolstatus: Mindestens ein Mitglied muss aktiv sein, um den Datenverkehr zu verarbeiten, ein Mitglied ist jedoch möglicherweise nicht ausreichend, um den gesamten Datenverkehr zu verarbeiten. Wenn kein Poolmitglied oder nur eine geringe Anzahl an Poolmitgliedern aktiv ist, versuchen Sie, das Problem wie nachfolgend beschrieben zu beheben.



Pool and Member Status

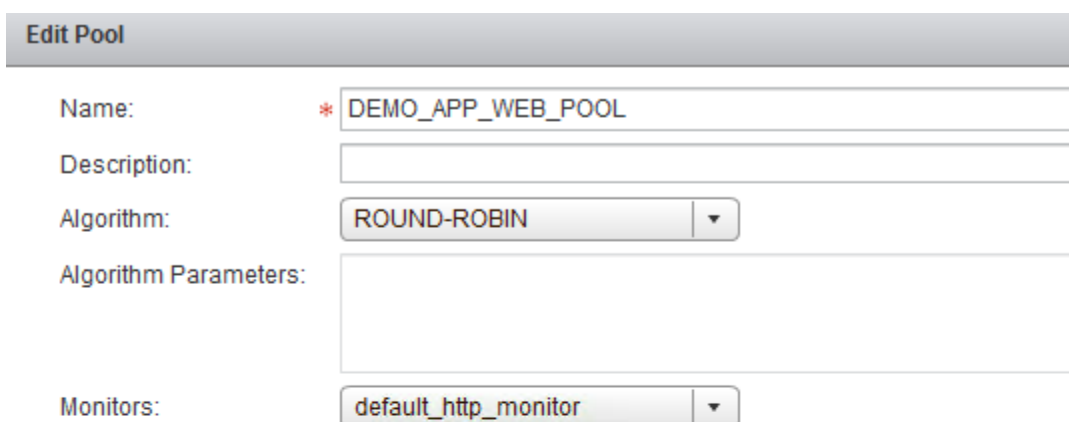
Pool Status and Statistics:

Pool ID	Name	Status
pool-1	TENANT-1-TCP-P...	UP

Member Status and Statistics:

Name	IP Address / VC Container	Status	Member ID
SERVER-1	10.10.10.100	UP	member-1
SERVER-2	10.10.10.101	UP	member-2

- b Überprüfen Sie, ob die Topologie korrekt ist. Der SNAT-Clientdatenverkehr wird über die Poolkonfiguration gesteuert. Ist das Edge-Dienst-Gateway, das die Load-Balancing-Funktion hostet, nicht inline, um den gesamten Datenverkehr zu sehen, schlägt es fehl. Um die IP-Adresse der Clientquelle beizubehalten, wählen Sie den Modus **Transparent** aus. Weitere Informationen finden Sie im *Administratorhandbuch für NSX*.



Edit Pool

Name: * DEMO_APP_WEB_POOL

Description:

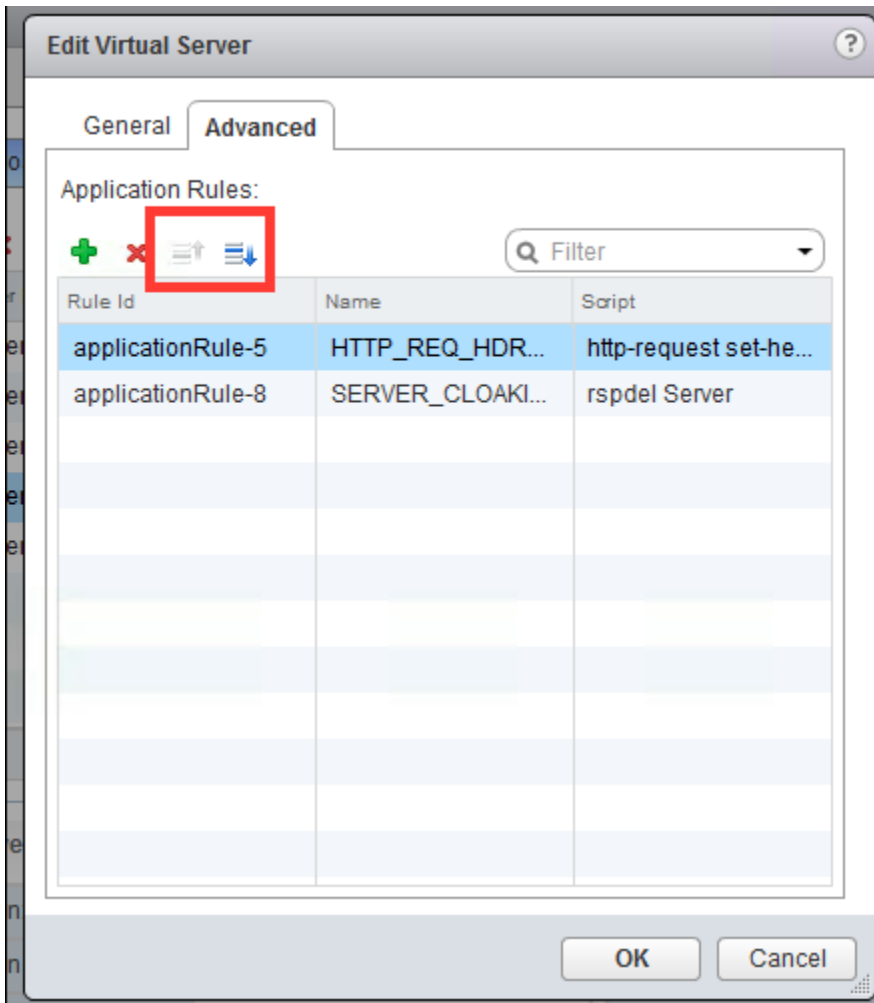
Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_http_monitor

Members:

- 5 Wenn Sie Anwendungsregeln verwenden, überprüfen Sie die Regeln. Löschen Sie ggf. die Regeln, um zu prüfen, ob der Datenverkehr fließt.
 - a Ordnen Sie die Regeln neu, um zu prüfen, ob die Reihenfolge der Regeln für eine Unterbrechung des Datenflusses verantwortlich ist. Informationen zum Hinzufügen einer Anwendungsregel und Beispiele für Anwendungsregeln finden Sie im Abschnitt zu Anwendungsregeln im *Administratorhandbuch für NSX*.



Nächste Schritte

Wenn Sie das Problem nicht finden konnten, müssen Sie möglicherweise versuchen, über die Befehlszeile herauszufinden, was passiert. Weitere Informationen finden Sie unter [Fehlerbehebung für Load Balancer mithilfe der Befehlszeilenschnittstelle](#).

Fehlerbehebung für Load Balancer mithilfe der Befehlszeilenschnittstelle

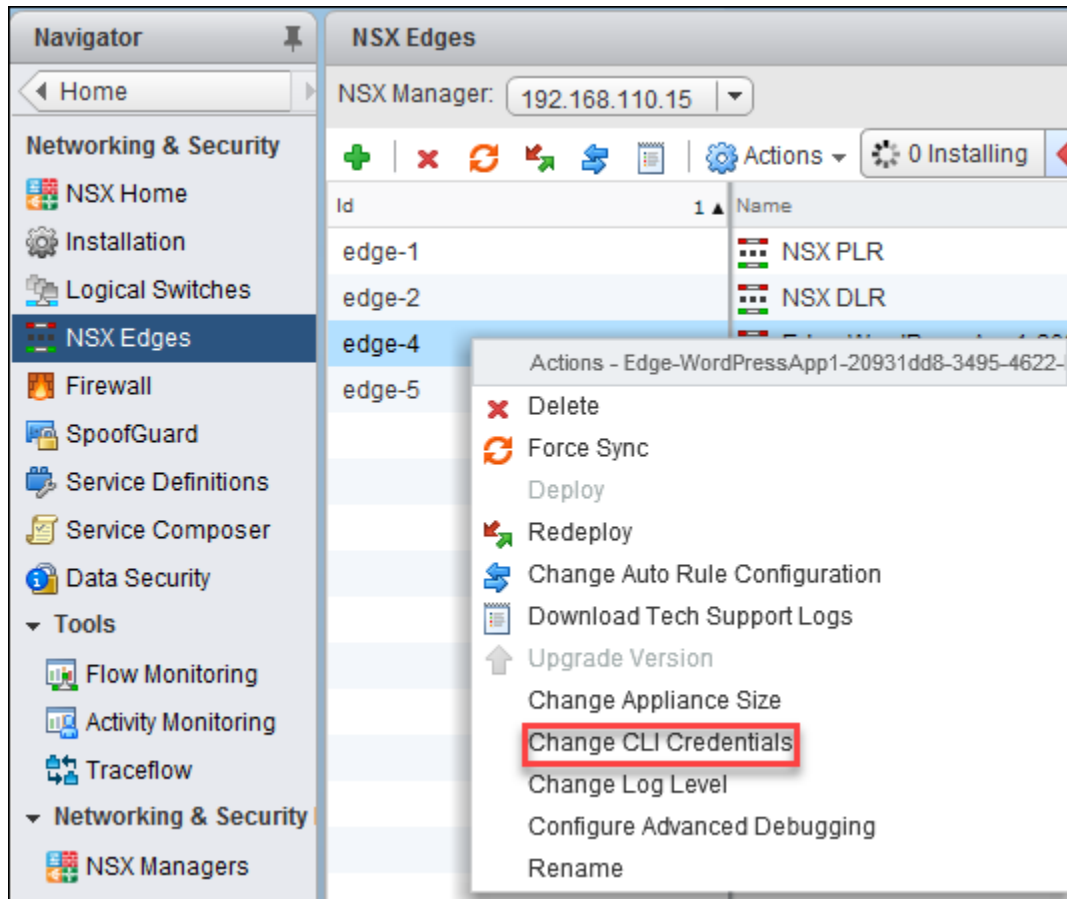
Die NSX-Befehlszeilenschnittstelle kann detaillierte Verfolgungsprotokolle bieten, Pakete erfassen und die Metriken für die Fehlerbehebung des Lastausgleichsdiensts überprüfen.

Problem

Das Load Balancing lässt sich nicht wie gewünscht durchführen.

Lösung

- 1 Aktivieren Sie SSH für die virtuelle Appliance oder prüfen Sie, ob dies möglich ist. Beim Edge-Dienst-Gateway handelt es sich um eine virtuelle Appliance, bei der während der Bereitstellung die Option zur Aktivierung von SSH besteht. Wenn Sie SSH aktivieren müssen, wählen Sie die gewünschte Appliance aus. Klicken Sie dann im Menü **Aktionen (Actions)** auf **Ändern der CLI-Anmeldedaten (Change CLI Credentials)**.



- 2 Das Edge-Dienst-Gateway bietet mehrere Anzeigebefehle, mit denen Sie den Laufzeit- und den Konfigurationsstatus einsehen können. Mit diesen Befehlen können Sie Informationen zur Konfiguration und zu Statistiken anzeigen.

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

- 3 Damit das Load-Balancing und NAT ordnungsgemäß funktionieren, müssen Sie die Firewall aktivieren. Führen Sie den Befehl `#show firewall` aus. Wenn dieser Befehl keine hilfreiche Ausgabe bewirkt, finden Sie weitere Informationen im Abschnitt [Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche](#).

```

NSX-edge-8-0> show firewall
Chain PREROUTING (policy ACCEPT 21947 packets, 7809K bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
)      348 67915 ACCEPT      all  --  lo      *        0.0.0.0/0    0.0.0.0/0
)      134  5360 DROP        all  --  *        *        0.0.0.0/0    0.0.0.0/0    state INVALID
)     21482 7736K block_in  all  --  *        *        0.0.0.0/0    0.0.0.0/0
)     20545 7671K ACCEPT    all  --  *        *        0.0.0.0/0    0.0.0.0/0    state RELATED
)       937 65139 usr_rules  all  --  *        *        0.0.0.0/0    0.0.0.0/0
)         0 0 DROP        all  --  *        *        0.0.0.0/0    0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain OUTPUT (policy ACCEPT 20673 packets, 1248K bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
)      348 67915 ACCEPT      all  --  *        lo      0.0.0.0/0    0.0.0.0/0
)       34  1360 DROP        all  --  *        *        0.0.0.0/0    0.0.0.0/0    state INVALID
)     20295 1179K block_out  all  --  *        *        0.0.0.0/0    0.0.0.0/0
)         0 0 ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)     14599 802K ACCEPT    all  --  *        *        0.0.0.0/0    0.0.0.0/0    state RELATED
)      5696  377K usr_rules  all  --  *        *        0.0.0.0/0    0.0.0.0/0
)         0 0 DROP        all  --  *        *        0.0.0.0/0    0.0.0.0/0
Chain block_in (1 references)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain block_out (1 references)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain usr_rules (2 references)
:cid  pkts bytes target      prot opt in      out     source      destination
133137 4861  333K ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    match-set 0_
133138 0 0 ACCEPT      all  --  *        *        0.0.0.0/0    0.0.0.0/0    match-set 1_
133139 936 65099 ACCEPT    all  --  *        *        0.0.0.0/0    0.0.0.0/0    match-set 2_
133141 835 43459 ACCEPT    all  --  *        *        0.0.0.0/0    0.0.0.0/0    match-set 3_
133131 1 40 LOG        all  --  *        *        0.0.0.0/0    0.0.0.0/0    LOG flags 0
133131 1 40 ACCEPT    all  --  *        *        0.0.0.0/0    0.0.0.0/0

```


- 4 Damit der Load Balancer ordnungsgemäß funktioniert, ist NAT erforderlich. Führen Sie den Befehl `show nat` aus. Wenn dieser Befehl keine hilfreiche Ausgabe bewirkt, finden Sie weitere Informationen im Abschnitt [Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche](#).

```

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

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

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

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

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

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

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

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

```

- 5 Die Firewall sollte also aktiviert sein und für den Load Balancer sollten NAT-Regeln vorliegen. Außerdem sollten Sie sicherstellen, dass der Load-Balancing-Prozess aktiviert ist. Mit dem Befehl `show service loadbalancer` können Sie den Status der Load-Balancer-Engine überprüfen (L4/L7).

```

nsxedge> show service loadbalancer
haIndex:          0

```

```

-----
Loadbalancer Services Status:

```

```

L7 Loadbalancer   : running

```

```

-----
L7 Loadbalancer Statistics:

```

```

STATUS      PID      MAX_MEM_MB MAX SOCK   MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running     1580      0          2081      1024      0         0         0
0           0

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

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

```

- a Verwenden Sie den `show service loadbalancer session`-Befehl, um die Sitzungstabelle des Lastausgleichsdiensts anzuzeigen. Wenn im System Datenverkehr vorhanden ist, werden Sitzungen angezeigt.

```

nsxedge> show service loadbalancer session

-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB MAX SOCK   MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running     1580      0          2081      1024      0         0         0
0           0

-----L7 Loadbalancer Current Sessions:

0x2192df1f300: proto=unix_stream src=unix:1 fe=GLOBAL be=<NONE> srv=<none> ts=09 age=0s
calls=2  rq[f=c08200h,
i=0,an=00h,rx=20s,wx=,ax=] rp[f=008000h,i=0,an=00h,rx=,wx=,ax=] s0=[7,8h,fd=1,ex=]
s1=[7,0h,fd=-1,ex=] exp=19s

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

L4 Loadbalancer Current Sessions:

pro expire state      source      virtual      destination

```

- b Überprüfen Sie den `show service loadbalancer table`-Befehl, um Schicht-7-Status verfügbarer Tabellen des Lastausgleichsdiensts anzuzeigen. Beachten Sie, dass in dieser Tabelle keine Informationen zu beschleunigten virtuellen Servern angezeigt werden.

```

nsxedge> show service loadbalancer table

-----
L7 Loadbalancer Sticky Table Status:

TABLE      TYPE      SIZE(BYTE)  USED(BYTE)

```

- 6 Wenn alle erforderlichen Dienste ordnungsgemäß ausgeführt werden, prüfen Sie die Routing-Tabelle. Es muss eine Route zum Client und zu den Servern vorliegen. Mit den Befehlen `show ip route` und `show ip forwarding` können Sie anzeigen, welche Routen zu den Schnittstellen vorliegen.

```

NSX-edge-8-0> sh ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 4

S      0.0.0.0/0          [1/1]          via 192.168.8.2
C      10.10.10.0/24      [0/0]          via 10.10.10.1
C      169.254.1.4/30     [0/0]          via 169.254.1.5
C      192.168.8.0/24     [0/0]          via 192.168.8.3
NSX-edge-8-0> sh ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route

R>* 0.0.0.0/0 via 192.168.8.2, vNic_2
C>* 10.10.10.0/24 is directly connected, vNic_0
C>* 169.254.1.4/30 is directly connected, vNic_0
C>* 192.168.8.0/24 is directly connected, vNic_2
NSX-edge-8-0>

```

- 7 Stellen Sie sicher, dass es einen ARP-Eintrag für die Systeme, z. B. das Gateway oder den nächsten Hop, und die Backend-Server gibt. Prüfen können Sie dies mit dem Befehl `show arp`.

```

OneArm-LoadBalancer-01-0> show arp
-----
vShield Edge ARP Cache:
IP Address                Interface  MAC Address      State
fe80::250:56ff:feae:f86b  vNic_0    00:50:56:ae:f8:6b STALE
fe80::250:56ff:feae:5066  vNic_1    00:50:56:ae:50:66 STALE
fe80::250:56ff:feae:3e3d  vNic_0    00:50:56:ae:3e:3d STALE
172.16.100.11             vNic_1    00:50:56:ae:50:66 REACHABLE
172.16.10.1               vNic_0    02:50:56:56:44:52 REACHABLE
172.16.10.11             vNic_0    00:50:56:ae:3e:3d REACHABLE
OneArm-LoadBalancer-01-0>

```

- 8 Anhand der Informationen aus den Protokollen lässt sich Datenverkehr identifizieren, der bei der Diagnostizierung von Problemen hilfreich sein kann. Mit den Befehlen `show log` oder `show log follow` können Sie das Protokoll verfolgen, mit dem Sie den Datenverkehr identifizieren können. Beachten Sie, dass für die Ausführung des Load Balancers **Protokollierung (Logging)** aktiviert und auf **Info** oder **Debug** festgelegt werden muss.

```

nsxedge> show log
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuacct
...

```

- 9 Nachdem sichergestellt wurde, dass die grundlegenden Dienste mit den korrekten Pfaden zu den Clients ausgeführt werden, sehen wir uns an, was in der Anwendungsschicht abläuft. Mit dem Befehl `show service loadbalancer pool` können Sie die Poolstatus des Lastausgleichsdiensts (L4/L7) anzeigen. Ein Poolmitglied muss aktiv sein, um die Inhalte zu unterstützen. Für gewöhnlich sind mehrere Mitglieder vonnöten, da das Anforderungsvolumen die Kapazität einer einzelnen Arbeitslast überschreitet. Wenn die Zustandsüberwachung durch eine interne Prüfung des Systemzustands erfolgt, zeigen die Ausgabe `last state change time` (Zeitpunkt der letzten Statusänderung) und `failure reason` (Grund für Fehler) an, wenn die Prüfung des Systemzustands fehlschlägt. Wenn die Zustandsüberwachung durch einen Überwachungsdienst erfolgt, wird neben den oben genannten zwei Ausgaben auch `last check time` (Zeitpunkt der letzten Prüfung) angezeigt.

```
nsxedge> show service loadbalancer pool
-----
Loadbalancer Pool Statistics:

POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
```

- 10 Überprüfen Sie den Status der Dienstüberwachung (OK, WARNUNG, KRITISCH), um den Zustand aller konfigurierten Backend-Server einzusehen.

```
nsxedge> show service loadbalancer monitor
-----
Loadbalancer Health Check Statistics:

MONITOR PROVIDER    POOL            MEMBER          HEALTH STATUS
built-in            Web-Tier-Pool-01 web-01a         default_https_monitor:L7OK
built-in            Web-Tier-Pool-01 web-02a         default_https_monitor:L7OK
```

Für den Befehl `show service load balancer monitor` werden drei Arten von Zustandsüberwachungswerten in der Ausgabe der Befehlszeilenschnittstelle angezeigt:

- Integrated (integriert): Die Zustandsprüfung ist aktiviert und wird von der L7-Engine (HA-Proxy) ausgeführt.

- **Monitor Service (Überwachungsdienst):** Die Zustandsprüfung ist aktiviert und wird von der Überwachungsdienst-Engine (NAGIOS) ausgeführt. Den Ausführungsstatus des Überwachungsdienstes können Sie mit den Befehlen `show service monitor` und `show service monitor service` in der Befehlszeilenschnittstelle überprüfen. Das Feld **Status** sollte den Wert OK, WARNUNG oder KRITISCH enthalten.
- **Not Defined (nicht definiert):** Die Zustandsprüfung ist deaktiviert.

In der letzten Spalte der Ausgabe wird der Systemzustand des Poolmitglieds angezeigt. Die folgenden Status werden angezeigt:

Tabelle 6-1. Systemzustand mit Beschreibung

Systemzustand	Beschreibung
Built-in	<ul style="list-style-type: none"> ■ UNK: Unbekannt ■ INI: Wird initialisiert ■ SOCKERR: Socket-Fehler ■ L4OK: Prüfung auf Schicht 4 bestanden, Prüfungen für höhere Schicht nicht aktiviert ■ L4TOUT: Zeitüberschreitung bei Schicht 1–4 ■ L4CON: Verbindungsproblem bei Schicht 1–4. Beispiel: „Verbindung abgelehnt“ (tcp rst) oder „Keine Route zum Host“ (icmp) ■ L6OK: Prüfung auf Schicht 6 bestanden ■ L6TOUT: Zeitüberschreitung bei Schicht 6 (SSL) ■ L6RSP: Ungültige Antwort auf Schicht 6 – Protokollfehler. Dies kann folgende Ursachen haben: <ul style="list-style-type: none"> ■ Der Backend-Server unterstützt nur „SSLv3“ oder „TLSv1.0“ oder ■ das Zertifikat des Backend-Servers ist ungültig oder ■ die Verschlüsselungsverhandlung ist fehlgeschlagen, etc. ■ L7OK: Prüfung auf Schicht 7 bestanden ■ L7OKC: Prüfung auf Schicht 7 bedingt bestanden. Beispiel: 404 mit disable-on-404 ■ L7TOUT: Zeitüberschreitung bei Schicht 7 (HTTP/SMTP) ■ L7RSP: Ungültige Antwort auf Schicht 7 – Protokollfehler ■ L7STS: Antwortfehler bei Schicht 7. Beispiel: HTTP 5xx
KRITISCH	<ul style="list-style-type: none"> ■ SSL-Protokoll Version 2 wird von Ihrer SSL-Bibliothek nicht unterstützt. ■ Nicht unterstützte Version des SSL-Protokolls ■ SSL-Kontext kann nicht erstellt werden. ■ SSL-Verbindung kann nicht hergestellt werden. ■ SSL-Handshake kann nicht initiiert werden. ■ Serverzertifikat kann nicht abgerufen werden. ■ Zertifikatsbetreff konnten nicht abgerufen werden. ■ Falsches Zeitformat im Zertifikat ■ Zertifikat „<cn>“ am <expire time of certificate> abgelaufen ■ Zertifikat „<cn>“ heute <expire time of certificate> abgelaufen
WARNUNG/ KRITISCH	Zertifikat „<cn>“ läuft in <days_left/expire time of certificate> Tag(en) ab

Tabelle 6-1. Systemzustand mit Beschreibung (Fortsetzung)

Systemzustand	Beschreibung
ICMP	<ul style="list-style-type: none"> ■ Netz nicht erreichbar ■ Host nicht erreichbar ■ Protokoll nicht erreichbar ■ Port nicht erreichbar ■ Quellroute fehlgeschlagen ■ Quellhost isoliert ■ Unbekanntes Netzwerk ■ Unbekannter Host ■ Netzwerk verweigert ■ Host verweigert ■ Ungültiger Dienstyp für das Netzwerk ■ Ungültiger Dienstyp für den Host ■ Durch Filter verboten ■ Verstoß gegen Hostvorrang ■ Vorranggrenze. Für den Vorgang erforderlicher Mindestvorrang ■ Ungültiger Code
UDP/TCP	<ul style="list-style-type: none"> ■ Fehler bei Socket-Erstellung ■ Verbindung mit Adresse xxxx und Port xxx: [Weitere Informationen finden Sie unter Linux-Fehlercode.] ■ Keine Daten vom Host empfangen ■ Unerwartete Antwort vom Host/Socket
HTTP/HTTPS	<ul style="list-style-type: none"> ■ HTTP UNBEKANNT: Fehler bei Arbeitsspeicherzuteilung ■ HTTP KRITISCH: TCP-Socket kann nicht geöffnet werden (Socket-Erstellung oder Verbindung mit Server ist fehlgeschlagen). ■ HTTP KRITISCH: Fehler beim Empfang von Daten ■ HTTP KRITISCH: Keine Daten vom Host empfangen ■ HTTP KRITISCH: Ungültige HTTP-Antwort von Host empfangen: <status line> (falsches Format der erwarteten Statuszeile) ■ HTTP KRITISCH: Ungültige Statuszeile <status line=> (Statuscode besteht nicht aus 3 Ziffern: XXX) ■ HTTP KRITISCH: Ungültiger Status <status line> (Statuscode >= 600 oder < 100) ■ HTTP KRITISCH: Zeichenfolge nicht gefunden ■ HTTP KRITISCH: Muster nicht gefunden ■ HTTP WARNUNG: Seitengröße <page_length> zu groß ■ HTTP WARNUNG: Seitengröße <page_length> zu klein

- 11** Beim Fehlercode „L4TOUT/L4CON“ bestehen in der Regel Verbindungsprobleme im zugrunde liegenden Netzwerk. Duplicate IP tritt häufig als Hauptursache mit diesem Grund auf. Führen Sie bei diesem Problem folgende Fehlerbehebung durch:
- Überprüfen Sie den Hochverfügbarkeitsstatus von Edges, wenn die Hochverfügbarkeit mit dem Befehl `show service highavailability` auf beiden Edges aktiviert wurde. Überprüfen Sie, ob der Hochverfügbarkeits-Link DOWN (nicht verfügbar) und alle Edges Active sind, damit es keine doppelte Edge-IP im Netzwerk gibt.
 - Überprüfen Sie mit dem Befehl `show arp` die Edge-ARP-Tabelle und prüfen Sie, ob der ARP-Eintrag des Backend-Servers zwischen den beiden MAC-Adressen geändert wird.
 - Überprüfen Sie die Backend-Server-ARP-Tabelle oder überprüfen Sie mit dem Befehl `arp-ping`, ob ein anderer Rechner dieselbe IP-Adresse aufweist wie der Edge.
- 12** Überprüfen Sie die Statistiken der Load-Balancer-Objekte (VIPs, Pools, Mitglieder). Überprüfen Sie, ob alle Mitglieder des spezifischen Pools aktiv sind und ausgeführt werden. Überprüfen Sie, ob der Transparent-Modus aktiviert ist. Wenn dies der Fall ist, sollte sich das Edge-Dienst-Gateway inline zwischen Client und Server befinden. Überprüfen Sie, ob sich die Sitzungsanzahl der Server erhöht.

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01
```

TIMESTAMP	SESSIONS	BYTESIN	BYTESOUT	SESSIONRATE	HTTPREQS
2016-04-27 19:56:40	00	00	00	00	00
2016-04-27 19:55:00	00	32	100	00	00

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01 | MEMBER
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-1, STATUS: UP
+--> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-2, STATUS: UP
```

- 13** Überprüfen Sie, ob beim virtuellen Server ein Standardpool vorhanden und dieser an den Server gebunden ist. Wenn Sie Pools über Anwendungsregeln verwenden, müssen Sie sich die einzelnen Pools wie im Befehl `#show service loadbalancer pool` gezeigt ansehen. Geben Sie den Namen des virtuellen Servers an.

```
nsxedge> show service loadbalancer virtual Web-Tier-VIP-01
```

```
-----
Loadbalancer VirtualServer Statistics:
```

```
VIRTUAL Web-Tier-VIP-01
| ADDRESS [172.16.10.10]:443
| SESSION (cur, max, total) = (0, 0, 0)
| RATE (cur, max, limit) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
```

```

+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)

```

- 14** Wenn alle Konfigurationen in Ordnung zu sein scheinen und der Fehler dennoch fortbesteht, müssen Sie Datenverkehr erfassen, um herauszufinden, wo das Problem liegt. Es gibt zwei Verbindungen: vom Client zum virtuellen Server und vom Edge-Dienst-Gateway zum Backend-Pool (mit oder ohne Transparent-Konfiguration auf der Poolebene). Der Befehl `#show ip forwarding` führt die vNIC-Schnittstellen auf. Diese Daten können Sie nutzen.

Nehmen wir beispielsweise an, der Clientcomputer befindet sich auf `vNic_0` und der Server auf `vNic_1`. Sie verwenden die Client-IP-Adresse `192.168.1.2`, die VIP-IP-Adresse `192.168.2.2`, ausgeführt auf Port 80. Die IP-Adresse für die Load-Balancer-Schnittstelle ist `192.168.3.1` und die IP-Adresse des Backend-Servers `192.168.3.3`. Es gibt zwei unterschiedliche Befehle für die Paketerfassung. Einer davon zeigt die Pakete an, der andere erfasst die Pakete in einer Datei, die Sie herunterladen können. Erfassen Sie die Pakete, um den abnormalen Fehler des Load Balancers zu erkennen. Sie können Pakete aus zwei Richtungen erfassen:

- Erfassen Sie die Pakete vom Client.
- Erfassen Sie die zum Backend-Server gesendeten Pakete.

```

#debug packet capture interface interface-name [filter using _ for space]- creates a packet
capture file that you can download
#debug packet display interface interface-name [filter using _ for space]- outputs packet data to
the console
#debug show files - to see a list of packet capture
#debug copy scp user@url:path file-name/all - to download the packet capture

```

Beispiel:

- Erfassung auf vNIC_0: `debug packet display interface vNic_0`
- Erfassung auf allen Schnittstellen: `debug packet display interface any`
- Erfassung auf vNIC_0 mit einem Filter: `debug packet display interface vNic_0 host_192.168.11.3_and_host_192.168.11.41`
- Eine Paketerfassung aus dem Datenverkehr vom Client zum virtuellen Server: `#debug packet display|capture interface vNic_0 host_192.168.1.2_and_host_192.168.2.2_and_port_80`
- Eine Paketerfassung aus dem Datenverkehr zwischen dem Edge-Dienst-Gateway und dem Server, auf dem sich der Pool im Transparent-Modus befindet: `#debug packet display|capture interface vNic_1 host 192.168.1.2_and_host_192.168.3.3_and_port_80`

- Eine Paketerfassung aus dem Datenverkehr zwischen dem Edge-Dienst-Gateway und dem Server, auf dem sich der Pool nicht im Transparent-Modus befindet: `#debug packet display| capture interface vNic_1 host 192.168.3.1_and_host_192.168.3.3_and_port_80`

Allgemeine Probleme mit dem Load Balancer

In diesem Abschnitt werden verschiedene Probleme und deren Behebung erläutert.

Die folgenden Probleme treten beim NSX-Load-Balancing häufiger auf:

- Das Load-Balancing auf dem TCP-Port (z. B. Port 443) funktioniert nicht.
 - Überprüfen Sie die Topologie. Genauere Informationen finden Sie unter *Administratorhandbuch für NSX*.
 - Überprüfen Sie, ob die IP-Adresse des virtuellen Servers per Ping erreichbar ist oder prüfen Sie am Upstream-Router, ob die ARP-Tabelle ausgefüllt ist.
 - [Überprüfung der Load-Balancer-Konfiguration und Fehlerbehebung über die Benutzeroberfläche](#).
 - [Fehlerbehebung für Load Balancer mithilfe der Befehlszeilenschnittstelle](#).
 - Erfassen Sie Pakete.
- Ein Mitglied des Load-Balancer-Pools wird nicht verwendet.
 - Überprüfen Sie, ob sich der Server im Pool befindet, und überwachen Sie den Systemzustand.
- Lasten des Edge-Datenverkehrs werden nicht verteilt.
 - Überprüfen Sie die Pool- und die Persistenzkonfiguration. Wenn Sie Persistenz konfiguriert haben und eine geringe Anzahl an Clients verwenden, werden die Verbindungen möglicherweise nicht gleichmäßig auf Mitglieder des Backend-Pools verteilt.
- Die Schicht 7-Load-Balancer-Engine wurde gestoppt.
- Die Systemzustandsüberwachungs-Engine wurde gestoppt.
 - Aktivieren Sie den Load-Balancing-Dienst. Weitere Informationen finden Sie im *Administratorhandbuch für NSX*.
- Der Überwachungsstatus eines Poolmitglieds ist WARNUNG/KRITISCH.
 - Überprüfen Sie, ob der Anwendungsserver über den Load Balancer erreichbar ist.
 - Überprüfen Sie, ob die Firewall des Anwendungsservers oder die verteilte Firewall Datenverkehr zulässt.
 - Stellen Sie sicher, dass der Anwendungsserver auf die festgelegte Prüfung des Systemzustands reagieren kann.
- Ein Poolmitglied befindet sich im Status INAKTIV.
 - Überprüfen Sie, ob das Poolmitglied in der Poolkonfiguration aktiviert ist.

- Die Schicht 7-Stickiness-Tabelle ist nicht mit dem Standby-Edge synchronisiert.
 - Stellen Sie sicher, dass hohe Verfügbarkeit konfiguriert ist.
- Es bestehen Clientverbindungen, aber eine Anwendungstransaktion lässt sich nicht abschließen.
 - Überprüfen Sie, ob im Anwendungsprofil die richtige Persistenz konfiguriert ist.
 - Wenn die Anwendung mit nur einem Server im Pool funktioniert (nicht mit zwei Servern), handelt es sich mit hoher Wahrscheinlichkeit um ein Persistenzproblem.

Grundlegende Fehlerbehebung

- 1 Überprüfen Sie den Konfigurationsstatus des Load Balancers im vSphere Web Client:
 - a Klicken Sie auf **Netzwerk und Sicherheit > NSX Edges (Networking & Security > NSX Edges)**.
 - b Doppelklicken Sie auf eine NSX Edge-Instanz.
 - c Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
 - d Überprüfen Sie den Zustand des Load Balancer und die konfigurierte Protokollierungsstufe.
- 2 Bevor Sie mit der Fehlerbehebung des Load-Balancing-Dienstes beginnen, führen Sie folgenden Befehl auf dem NSX Manager aus, um sicherzustellen, dass der Dienst funktioniert:

```
nsxmgr> show edge edge-4 service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer      : running
-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB  MAX SOCK   MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE
CONN_RATE_LIMIT  MAX_CONN_RATE
running     1580      0           2081      1024      0         0         0
0           0
-----
L4 Loadbalancer Statistics:
MAX_CONN  ACT_CONN  INACT_CONN  TOTAL_CONN
0         0         0           0
-----
Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn
```

Hinweis Mit dem Befehl `show edge all` können Sie die Namen der NSX Edges nachschlagen.

Beheben von Konfigurationsproblemen

Wenn der Konfigurationsvorgang für den Load Balancer von der NSX-Benutzeroberfläche oder dem REST API-Aufruf abgelehnt wird, gilt dies als Konfigurationsproblem.

Beheben von Problemen auf der Datenebene

Die Load-Balancer-Konfiguration wird vom NSX Manager akzeptiert, aber beim Load-Balancing-Server des Client-Edges treten Verbindungs- oder Leistungsprobleme auf. Zu den Problemen auf der Datenebene gehören auch CLI-Probleme mit dem Load Balancer zur Laufzeit sowie Systemereignisprobleme des Load Balancer.

- 1 Ändern Sie mit diesem REST API-Aufruf die Edge-Protokollierungsstufe bei NSX Manager von INFO in TRACE oder DEBUG.

```
URL: https://NSX_Manager_IP/api/1.0/services/debug/loglevel/com.vmware.vshield.edge?level=TRACE
Method: POST
```

- 2 Überprüfen Sie den Status des Poolmitglieds im vSphere Web Client.
 - a Klicken Sie auf **Netzwerk und Sicherheit > NSX Edges (Networking & Security > NSX Edges)**.
 - b Doppelklicken Sie auf eine NSX Edge-Instanz.
 - c Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
 - d Klicken Sie auf **Pools**, um eine Zusammenfassung der konfigurierten Load-Balancer-Pools anzuzeigen.
 - e Wählen Sie Ihren Load-Balancer-Pool aus. Klicken Sie auf **Poolstatistik anzeigen (Show Pool Statistics)** und überprüfen Sie, ob der Poolzustand „UP“ ist.
- 3 Ausführlichere Statistiken zur Konfiguration des Load-Balancer-Pools können Sie bei NSX Manager mit dem folgenden REST API-Aufruf abrufen:

```
URL: https://NSX_Manager_IP/api/4.0/edges/{edgeId}/loadbalancer/statistics
Method: GET
```

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
  <timeStamp>1463507779</timeStamp>
  <pool>
    <poolId>pool-1</poolId>
    <name>Web-Tier-Pool-01</name>
    <member>
      <memberId>member-1</memberId>
      <name>web-01a</name>
      <ipAddress>172.16.10.11</ipAddress>
      <status>UP</status>
      <lastStateChangeTime>2016-05-16 07:02:00</lastStateChangeTime>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <httpReqTotal>0</httpReqTotal>
      <httpReqRate>0</httpReqRate>
      <httpReqRateMax>0</httpReqRateMax>
```

```

        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <member>
        <memberId>member-2</memberId>
        <name>web-02a</name>
        <ipAddress>172.16.10.12</ipAddress>
        <status>UP</status>
        <lastStateChangeTime>2016-05-16 07:02:01</lastStateChangeTime>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <status>UP</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</pool>
<virtualServer>
    <virtualServerId>virtualServer-1</virtualServerId>
    <name>Web-Tier-VIP-01</name>
    <ipAddress>172.16.10.10</ipAddress>
    <status>OPEN</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</virtualServer>
</loadBalancerStatusAndStats>

```

- 4 Um Load-Balancer-Statistiken über die Befehlszeile abzurufen, führen Sie die folgenden Befehle auf dem NSX Edge aus.

Für einen bestimmten virtuellen Server: Führen Sie zunächst den Befehl `show service loadbalancer virtual` aus, um den Namen des virtuellen Servers zu erhalten. Anschließend führen Sie `show statistics loadbalancer virtual <virtual-server-name>` aus.

Für einen bestimmten TCP-Pool führen Sie zuerst `show service loadbalancer pool` aus, um den Poolnamen abzurufen. Anschließend führen Sie `show statistics loadbalancer pool <pool-name>` aus.

- 5 Überprüfen Sie die Statistiken des Load Balancer auf eventuelle Hinweise auf Fehler.

Fehlerbehebung für virtuelle private Netzwerke (VPN)

7

NSX Edge unterstützt diverse Arten von VPNs. In diesem Abschnitt wird die Fehlerbehebung bei L2 VPN- und SSL VPN-Problemen beschrieben.

Dieses Kapitel enthält die folgenden Themen:

- [L2 VPN](#)
- [SSL VPN](#)
- [IPSec-VPN](#)

L2 VPN

Mit L2 VPN können Sie mehrere logische L2-Netzwerksysteme (sowohl VLAN als auch VXLAN) über L3-Grenzen hinaus erweitern und in einem SSL VPN tunneln. Darüber hinaus können Sie mehrere Sites auf einem L2 VPN-Server konfigurieren. Virtuelle Maschinen verbleiben auf demselben Subnetz, auch wenn sie zwischen diesen Sites verschoben wurden, und ihre IP-Adressen ändern sich nicht. Sie haben auch die Möglichkeit, einen eigenständigen Edge an einen Remote-Standort bereitzustellen, ohne dass dieser Standort NSX unterstützt. Dank der Egress-Optimierung kann der Edge alle Pakete, die lokal an die Egress-optimierte IP-Adresse gesendet werden, routen und alles andere überbrücken.

Dadurch ermöglicht L2 VPN Unternehmen eine reibungslose und durch VXLAN oder VLAN gesicherte Migration von Arbeitslasten zwischen physisch getrennten Speicherorten. Für Cloud-Anbieter stellt L2 VPN einen Mechanismus zur Verfügung, mit dem Sie Mandanten aufnehmen können, ohne die bestehenden IP-Adressen für Arbeitslasten und Anwendungen ändern zu müssen.

L2-VPN - häufig auftretende Konfigurationsprobleme

In diesem Abschnitt werden häufig auftretende Konfigurationsprobleme im Zusammenhang mit L2-VPN erläutert.

Problem

Nachfolgend sind häufig auftretende Konfigurationsprobleme beschrieben:

- Der L2-VPN-Client wurde konfiguriert, aber die mit dem Internet verbundene Firewall lässt über den Ziel-Port 443 keinen Datenverkehr im Tunnel zu.

- Der L2-VPN-Client wurde für die Validierung von Serverzertifikaten konfiguriert, jedoch nicht mit dem korrekten CA-Zertifikat oder FQDN.
- Der L2-VPN-Server wurde konfiguriert, aber die NAT-/Firewallregel wurde nicht auf der Internetfirewall erstellt.
- Die Trunk-Schnittstelle wird nicht von einer verteilten bzw. standardmäßigen Portgruppe gestützt.

Hinweis Der L2-VPN-Server überwacht standardmäßig Port 443. Dieser Port ist über die L2-VPN-Servereinstellungen konfigurierbar.

Der L2-VPN-Client stellt standardmäßig eine ausgehende Verbindung zu Port 443 her. Dieser Port ist über die L2-VPN-Client-Einstellungen konfigurierbar.

Lösung

- 1 Überprüfen Sie, ob der L2-VPN-Serverprozess ausgeführt wird.
 - a Melden Sie sich bei der NSX Edge-VM an.
 - b Führen Sie den Befehl `show process monitor` aus und prüfen Sie, ob ein Prozess mit dem Namen `l2vpn` vorhanden ist.
 - c Führen Sie den Befehl `show service network-connections` aus und prüfen Sie, ob der Prozess `l2vpn` Port 443 überwacht.
- 2 Überprüfen Sie, ob der L2-VPN-Clientprozess ausgeführt wird.
 - a Melden Sie sich bei der NSX Edge-VM an.
 - b Führen Sie den Befehl `show process monitor` aus und prüfen Sie, ob ein Prozess mit dem Namen `naclientd` vorhanden ist.
 - c Führen Sie den Befehl `show service network-connections` aus und prüfen Sie, ob der Prozess `naclientd` Port 443 überwacht.
- 3 Prüfen Sie, ob man über das Internet auf den L2-VPN-Server zugreifen kann.
 - a Öffnen Sie einen Browser und rufen Sie **`https://<l2vpn-public-ip>`** auf.
 - b Es sollte eine Portalanmeldeseite angezeigt werden. Wird die Portalseite angezeigt, ist der L2-VPN-Server über das Internet erreichbar.
- 4 Überprüfen Sie, ob die Trunk-Schnittstelle durch eine verteilte oder standardmäßige Portgruppe gestützt wird.
 - a Wenn die Trunk-Schnittstelle von einer verteilten Portgruppe gestützt wird, wird automatisch ein Sink-Port eingerichtet.
 - b Wird die Trunk-Schnittstelle von einer standardmäßigen Portgruppe gestützt, sollten Sie den vSphere Distributed Switch manuell wie folgt konfigurieren:
 - Legen Sie für den Port den **promiskuitiven (promiscuous)** Modus fest.
 - Legen Sie **Gefälschte Übertragungen (Forged Transmits)** auf **Akzeptieren (Accept)** fest.

5 L2-VPN-Schleifenprobleme abmildern

- a Zwei größere Probleme treten auf, wenn die NIC-Gruppierung nicht korrekt konfiguriert ist: MAC-Flapping und duplizierte Pakete. Überprüfen Sie die Konfiguration, wie unter [L2VPN-Optionen zum Verringern des Loopings](#) beschrieben.

6 Prüfen Sie, ob VMs im L2-VPN miteinander kommunizieren können.

- a Melden Sie sich bei der L2-VPN-Serverbefehlszeile an und erfassen Sie das Paket auf der entsprechenden TAP-Schnittstelle `debug packet capture interface name`.
- b Melden Sie sich beim L2-VPN-Client an und erfassen Sie das Paket auf der entsprechenden TAP-Schnittstelle `debug packet capture interface name`.
- c Analysieren Sie diese Erfassungen, um zu prüfen, ob ARP aufgelöst wird, und den Datenverkehrsfluss.
- d Prüfen Sie, ob die Eigenschaft `Allow Forged Transmits`: dvSwitch auf *L2 VPN trunk port* (L2-VPN-Trunk-Port) festgelegt ist.
- e Prüfen Sie, ob der Sink-Port auf *L2 VPN trunk port* (L2-VPN-Trunk-Port) festgelegt ist. Melden Sie sich dazu beim Host an und führen Sie den Befehl `net-dvs -l` aus. Prüfen Sie, ob die Sink-Eigenschaft für den internen L2-VPN-Edge-Port eingestellt ist (`com.vmware.etherswitch.port.extraEthFRP = SINK`). „Interner Port“ bezieht sich auf den *dvPort*, über den der NSX Edge-Trunk verbunden ist.

net-dvs -l

ESXi

```
port 939:
com.vmware.common.port.alias = , propType = CONFIG
com.vmware.common.port.connectid = 323234212 , propType = CONFIG
com.vmware.common.port.portgroupid = dvportgroup-181 , propType = CONFIG
com.vmware.common.port.block = false , propType = CONFIG
com.vmware.common.port.dvfilter = filters (num = 0):
    propType = CONFIG
com.vmware.common.port.ptAllowed = 0x 0. 0. 0. 0
    propType = CONFIG
com.vmware.etherswitch.port.txUplink = normal , propType = CONFIG
com.vmware.common.port.volatile.persist = /vmfs/volumes/9ec6ae8b-38b8e621/.dvsData/1e ec 0e 50 02 9c a9 21-b6 d8
fc 73 e5 79 69/939 , propType = CONFIG
com.vmware.common.port.ptAllowedRT = 0x 0. 0. 0. 0
    propType = RUNTIME
com.vmware.net.vxlan.trunkcfg = 0x63.6f.6e.66.69.67.56.65.72.73.69.6f.6e.3d.30.2e.31.3b.61.6c.6c.6f.77.47.75.65.7
74.56.6c.61.6e.3d.30.3b.6e.75.6d.54.72.75.6e.6b.4d.65.6d.62.65.72.73.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.43.70.45.6e.61.62.
.65.64.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.56.6e.69.3d.35.30.30.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.4d.63.61.73.74.49.70
d.30.2e.30.2e.30.2e.31.3b
    propType = CONFIG POLICY
com.vmware.etherswitch.port.extraEthFRP = SINK
    propType = CONFIG POLICY
com.vmware.etherswitch.port.teaming:
    load balancing = first uplink (i.e. explicit)
    link selection = link state up;
    link behavior = notify switch; best effort on failure; shotgun on failure;
    active = dvUplink1;
    standby =
    propType = CONFIG
com.vmware.etherswitch.port.security = deny promiscuous; deny mac change; allow forged frames
    propType = CONFIG
com.vmware.etherswitch.port.vlan = Guest VLAN tagging
    ranges = 0
    propType = CONFIG
com.vmware.common.port.statistics:
    pktsInUnicast = 0
    bytesInUnicast = 0
    pktsInMulticast = 6
    bytesInMulticast = 620
```

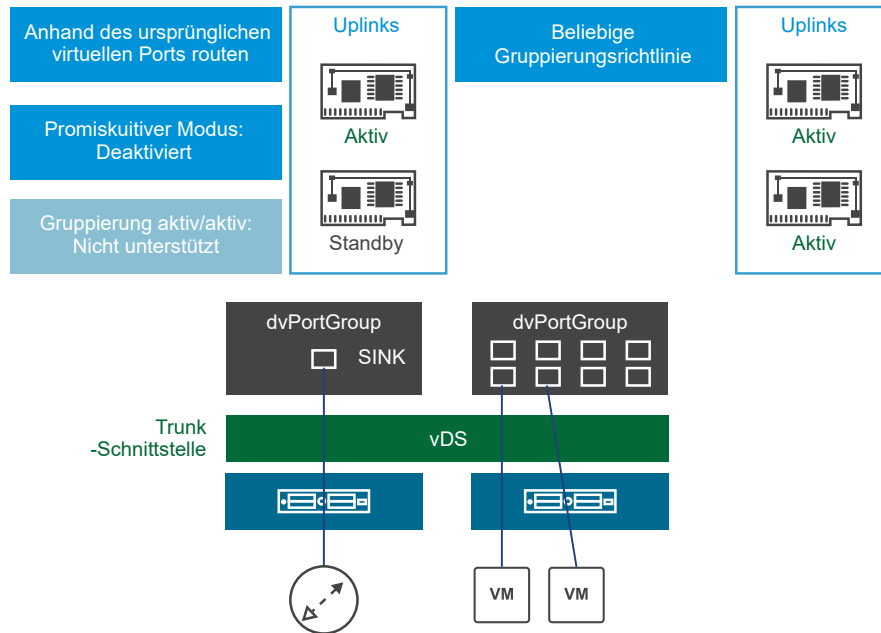
Sink port should be enabled for the dvPort where the Edge trunk is connected to

L2VPN-Optionen zum Verringern des Loopings

Es gibt zwei Optionen, um das Looping zu verringern. Die NSX Edges und virtuellen Maschinen können sich auf unterschiedlichen oder auf demselben ESXi-Host befinden.

Option 1: Unterschiedliche ESXi-Hosts für die L2VPN Edges und die virtuellen Maschinen

1. Bereitstellen von L2VPN Edges und VMs auf separaten ESXi-Hosts



- 1 Stellen Sie die Edges und die virtuellen Maschinen auf getrennten ESXi-Hosts bereit.
- 2 Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die der TRUNK vNic des Edges zugeordnete verteilte Portgruppe wie folgt:
 - a Load Balancing: „Anhand des ursprünglichen virtuellen Ports routen“.
 - b Konfigurieren Sie nur einen Uplink als „Aktiv“ und den anderen Uplink als „Standby“.
- 3 Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die den virtuellen Maschinen zugeordnete verteilte Portgruppe wie folgt:
 - a Jede Gruppierungsrichtlinie kann verwendet werden.
 - b Mehrere aktive Uplinks können konfiguriert werden.

- 4 Konfigurieren Sie Edges für die Verwendung des SINK-Portmodus und deaktivieren Sie den Promiscuous-Modus auf der TRUNK vNic.

Hinweis

- Promiskuitiven Modus deaktivieren: Wenn Sie einen vSphere Distributed Switch verwenden.
- Promiskuitiven Modus aktivieren: Wenn Sie den virtuellen Switch verwenden, um die Trunk-Schnittstelle zu konfigurieren.

Wenn für einen virtuellen Switch der promiskuitive Modus aktiviert ist, werden einige Pakete nicht verworfen, die von den Uplinks eingehen, die derzeit nicht vom promiskuitiven Port verwendet werden. Sie sollten ReversePathFwdCheckPromisc aktivieren und dann deaktivieren. Für den promiskuitiven Port werden dann explizit alle Pakete, die von den derzeit nicht verwendeten Uplinks eingehen, verworfen.

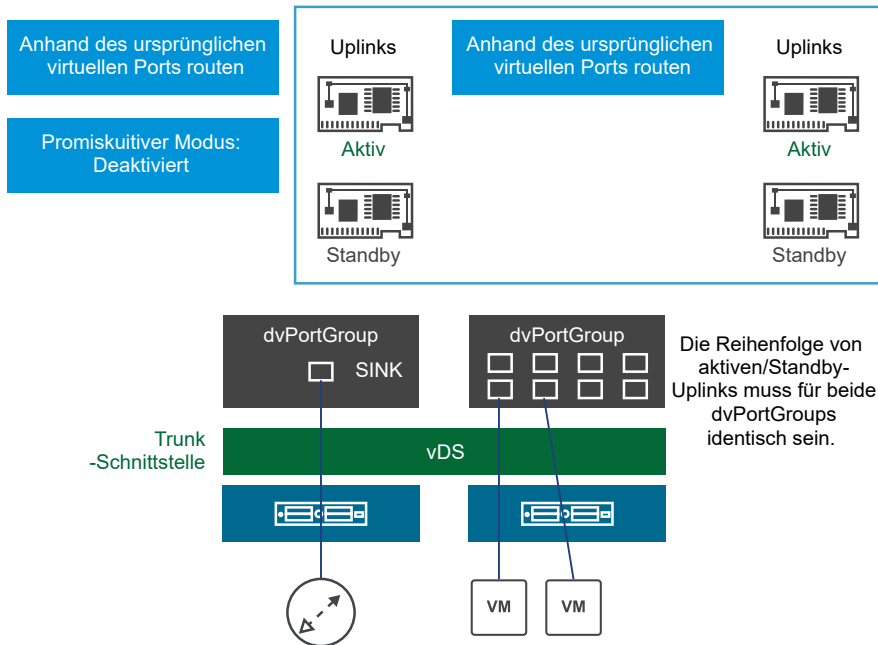
Um die duplizierten Pakete zu blockieren, aktivieren Sie die RPF-Überprüfung für den promiskuitiven Modus in der ESXi-CLI, in der NSX Edge vorhanden ist:

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

Ändern Sie in der Sicherheitsrichtlinie **PortGroup** für **PromiscuousMode** den Wert von **Akzeptieren (Accept)** zu **Ablehnen (Reject)** und wieder zu **Akzeptieren (Accept)**, um die konfigurierte Änderung zu aktivieren.

- Option 2: Edges und virtuelle Maschinen auf demselben ESXi-Host

2. Bereitstellen von L2VPN Edges und VMs auf demselben Host



- a Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die der TRUNK vNic des Edges zugeordnete verteilte Portgruppe wie folgt:
 - 1 Load Balancing: „Anhand des ursprünglichen virtuellen Ports routen“.
 - 2 Konfigurieren Sie einen Uplink als „Aktiv“ und den anderen Uplink als „Standby“.
- b Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die den virtuellen Maschinen zugeordnete verteilte Portgruppe wie folgt:
 - 1 Jede Gruppierungsrichtlinie kann verwendet werden.
 - 2 Nur ein Uplink kann aktiv sein.
 - 3 Die Reihenfolge der aktiven/Standby-Uplinks muss für die verteilte Portgruppe der virtuellen Maschine und die verteilte Portgruppe der TRUNK vNic des Edges identisch sein.
- c Konfigurieren Sie das clientseitige eigenständige Edge für die Verwendung des SINK-Portmodus und deaktivieren Sie den Promiscuous-Modus auf der TRUNK vNic.

Fehlerbehebung über die Befehlszeile

In vielen Fällen können Sie für die L2-VPN-Fehlerbehebung die NSX-Befehlszeile verwenden.

Problem

Das L2-VPN funktioniert nicht ordnungsgemäß.

Lösung

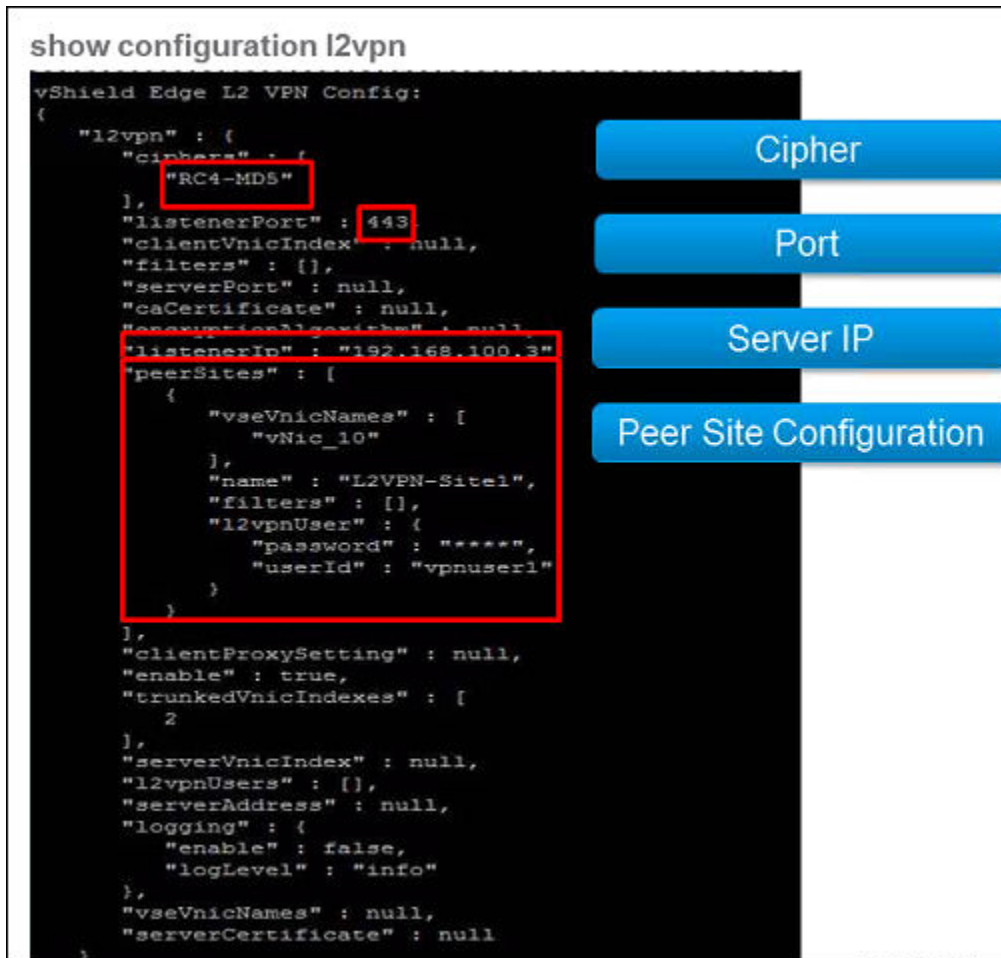
- 1 Mit den folgenden zentralen Befehlen können Sie das VPN auf Konfigurationsprobleme untersuchen:


```
show edge <edgeID> configuration l2vpn.
```

Beispiel: `show edge edge-1 configuration l2vpn`.

2 Verwenden Sie die folgenden Befehle sowohl auf dem Client- als auch auf dem Server-Edge:

- `show configuration l2vpn` – Überprüft die folgenden vier zentralen Werte, um den Server zu prüfen.



- `show service l2vpn bridge` – Die Anzahl der Schnittstellen hängt von der Anzahl der L2-VPN-Clients ab. Bei der nachfolgenden Ausgabe wird ein einzelner L2-VPN-Client (na1) konfiguriert. Port1 bezieht sich auf `vNic_2`. Die MAC-Adresse 02:50:56:56:44:52 wurde auf der `vNic_2`-Schnittstelle abgerufen und gehört nicht lokal zum Edge (L2-VPN-Server). Zeile 3 im folgenden Beispiel bezieht sich auf die Schnittstelle `na1`.

```
plr01-0> show service l2vpn bridge
```

bridge name	bridge id	STP enabled	interfaces
br-sub	8000.0050568e19fb	no	vNic_2 na1

List of learned MAC addresses for L2 VPN bridge br-sub

port no	mac addr	is local?	vlanid	ageing timer
1	00:50:56:8e:19:fb	yes	0	0.00
1	02:50:56:56:44:52	no	1	0.87
2	2a:56:30:31:7e:3b	yes	0	0.00

- show service l2vpn trunk table
- show service l2vpn conversion table – Im folgenden Beispiel wird die VLAN-ID Nr. 1 eines Ethernet-Frames, der auf Tunnel Nr. 1 ankommt, in VXLAN mit der VLAN-Nummer 5001 umgewandelt, bevor das Paket an den VDS weitergeleitet wird.

```
plr01-0> show service l2vpn conversion-table
```

TunnelId	VLAN/VNI	Type
1	5001	VXLAN

vNIC#	Name	Network	VLAN / VNI	Tunnel ID	Status
10	Subint-to-W...	Web-Tier-01	5001	1	✓

- show process monitor – Stellt fest, ob die Prozesse „l2vpn“ (Server) und „naclientd“ (Client) ausgeführt werden.
- show service network-connections – Stellt fest, ob die Prozesse „l2vpn“ (Server) und „naclientd“ (Client) Port 443 überwachen.

SSL VPN

Sie können diese Informationen zur Fehlerbehebung bei Problemen mit Ihrem Setup verwenden.

SSL VPN-Webportal wird nicht geöffnet

SSL VPN-Benutzer können die Anmeldeseite des SSL VPN-Webportals zum Herunterladen und Installieren des SSL VPN-Plus Client-Installationspakets nicht öffnen.

Problem

Die Anmeldeseite des SSL VPN-Webportals öffnet sich nicht bzw. die Seite rendert nicht ordnungsgemäß in Ihrem Systembrowser.

Ursache

Dieses Problem kann folgende Ursachen haben:

- Ihr System verwendet eine nicht unterstützte Browserversion.
- Cookies und JavaScript sind in Ihrem Browser nicht aktiviert.

Lösung

- 1 Stellen Sie sicher, dass Sie die Anmeldeseite des SSL VPN-Webportals über einen der folgenden unterstützten Browser öffnen.

Browser	Unterstützte Mindestversionen
Internet Explorer	9.0.8112.16421
Chrome	67.03396
Safari	10.x

- 2 Öffnen Sie Ihre Browsereinstellungen und stellen Sie sicher, dass Cookies und JavaScript aktiviert sind.
- 3 Wenn beim Browser Englisch nicht als Sprache festgelegt ist, wählen Sie für die Sprache Englisch aus und überprüfen Sie, ob das Problem damit behoben ist.
- 4 Überprüfen Sie, ob Sie die AES-Verschlüsselung auf dem SSL VPN-Server ausgewählt haben. Einige Browser unterstützen die AES-Verschlüsselung nicht.

SSL VPN-Plus: Installationsfehler

In diesem Thema finden Sie Informationen zu möglichen Problemen im Zusammenhang mit der Installation des SSL VPN-Plus Clients sowie zu deren Behebung.

Problem

Allgemeine Probleme im Zusammenhang mit der Installation des SSL VPN-Plus Clients:

- SSL VPN-Plus Client wurde erfolgreich installiert, doch der Client funktioniert nicht.
- Auf Mac-Computern werden Warnmeldungen im Zusammenhang mit Kernel-Extensions angezeigt.
- Unter macOS High Sierra werden nach der Installation die folgenden Fehlermeldungen angezeigt:

```
/opt/sslvpn-plus/naclient/signed_kext/tap.kext failed to load - (libkern/kext)system policy prevents loading; check the system/kernel logs for errors or try kextutil(8).
Error: Could not load /opt/sslvpn-plus/naclient/signed_kext/tap.kext
```

```
installer[4571] <Debug>: install:didFailWithError:Error Domain=
PKInstallErrorDomain Code=112 "An error occurred while running scripts from the
package "naclient.pkg".
" UserInfo={NSFilePath=./postinstall,NSURL=file:///<pathtofile>/
naclient.pkg,PKInstallPackageIdentifier=
com.vmware.sslvpn,NSLocalizedString=An error occurred while running scripts from the
```

```
package "naclient.pkg".}

installer[4571] <Error>: Install failed: The Installer encountered an error that caused the
installation to fail. Contact the software manufacturer for assistance.
installer: The install failed (The Installer encountered an error that caused the installation to
fail.
Contact the software manufacturer for assistance.)
```

- Auf Windows-Computern wird die folgende Fehlermeldung angezeigt: Treiberinstallation mit Grund E000024B fehlgeschlagen: Bitte versuchen Sie, den Computer neu zu starten.

Ursache

Der SSL VPN-Plus Client kann durch einen der folgenden Gründe fehlschlagen, auch wenn Sie ihn erfolgreich auf Ihrem Computer installiert haben:

- Konfigurationsdatei (naclient.cfg) fehlt oder ist ungültig.
- Verzeichnisberechtigungen oder Benutzerberechtigungen sind falsch.
- SSL VPN-Server ist nicht erreichbar.
- Auf Mac- und Linux-Computern ist der Tap-Treiber nicht geladen.

Auf Mac-Computern werden Warnmeldungen im Zusammenhang mit Kernel-Extensions angezeigt, da Ihr System das Laden der Kernel-Extensions blockiert.

Unter macOS High Sierra werden Fehler bei der Installation angezeigt, wenn Ihr Mac-Computer keine Kext zulässt und Sie auch nicht zum Laden der Kext auffordert.

Auf Windows-Computern wird ein Fehler bei der Treiberinstallation (E000024B) angezeigt, da Sie die Option **SSL-Clientnetzwerkadapter ausblenden (Hide SSL client network adapter)** im Edge SSL VPN-Plus Client-Installationsprogramm aktiviert haben.

Lösung

- 1 Stellen Sie sicher, dass Sie den SSL VPN-Plus Client auf unterstützten Betriebssystemen installieren. Informationen zu unterstützten Betriebssystemen finden Sie im Thema „Übersicht über SSL VPN-Plus“ im *Administratorhandbuch für NSX*.
- 2 Stellen Sie auf Windows-Maschinen sicher, dass Benutzer, die den SSL VPN-Plus Client installieren, über **Administratorrechte** verfügen. Auf Mac- und Linux-Computern benötigen Benutzer **Rootberechtigungen** zum Installieren des SSL VPN-Plus Clients. Damit der SSL VPN-Plus Client auf Mac-Computern gestartet und erfolgreich ausgeführt werden kann, benötigen Benutzer außerdem **Ausführberechtigungen** für das Verzeichnis `usr/local/lib`.
- 3 Stellen Sie auf Linux-Computern sicher, dass die folgenden Bibliotheken installiert sind. Diese Bibliotheken sind für eine ordnungsgemäße Funktion der Benutzeroberfläche erforderlich.
 - TCL
 - TK
 - NSS

- 4 Wenn der Tap-Treiber auf Mac- und Linux-Computern nicht geladen wird, führen Sie das Shell-Skript aus, um den Treiber zu laden.

Betriebssystem	Beschreibung
Mac	Führen Sie das Shell-Skript <code>NaClient.sh</code> über das Verzeichnis <code>/opt/sslvpn-plus/naclient/</code> mit Sudo -Rechten aus.
Linux	Führen Sie das Shell-Skript <code>naclient.sh</code> mit Sudo -Rechten aus. Sie finden dieses Skript im Verzeichnis <code>linux_phat_client/linux_phat_client</code> .

- 5 Um die Warnmeldungen im Zusammenhang mit Kernel-Extensions unter macOS High Sierra oder höher aufzulösen, müssen Sie eine explizite Benutzergenehmigung zum Laden einer Kernel-Extension (Kext) erteilen. Führen Sie die folgenden Schritte aus:
- Öffnen Sie auf Ihrem Mac-Computer das Fenster **Systemeinstellungen (System Preferences) > Sicherheit & Datenschutz (Security & Privacy)**.
 - Am unteren Fensterrand sehen Sie eine Meldung ähnlich der folgenden: Das Laden einer Systemsoftware wurde blockiert. Klicken Sie auf die Schaltfläche „Zulassen“.
 - Um mit der Installation fortzufahren, klicken Sie auf **Zulassen (Allow)**.

Detaillierte Informationen zur Erteilung von Benutzergenehmigungen zum Laden einer Kernel-Extension finden Sie unter https://developer.apple.com/library/content/technotes/tn2459/_index.html.
 - Während die Kernel-Extension geladen wird, wird der SSL VPN-Plus Client-Installationsvorgang weiterhin im Hintergrund ausgeführt. Der SSL VPN-Plus Client wird installiert, doch Sie erhalten die folgende Fehlermeldung: Die Installation ist fehlgeschlagen. Beim Installationsprogramm ist ein Fehler aufgetreten, sodass die Installation nicht durchgeführt werden kann. Wenden Sie sich an den Hersteller der Software, um Unterstützung zu erhalten.
 - Um diesen Fehler zu beheben, deinstallieren Sie den SSL VPN-Plus Client und installieren Sie ihn erneut.

- 6 Um unter macOS High Sierra Fehlermeldungen im Zusammenhang mit der Installation zu beheben, führen Sie diese Schritte aus.

- a Stellen Sie sicher, dass Benachrichtigungen aktiviert sind. Gehen Sie zu **Systemeinstellungen (System Preferences) > Sicherheit & Datenschutz (Security & Privacy) > Benachrichtigungen zulassen (Allow Notifications)**.

Hinweis Wenn Sie den SSL VPN-Plus Client erstmals unter macOS High Sierra installieren, werden Sie in einem Benachrichtigungsfenster aufgefordert, die Installation zuzulassen. Diese Benachrichtigung wird in der Regel nur 30 Minuten lang angezeigt. Wenn die Benachrichtigung ausgeblendet wird, bevor Sie auf **Zulassen (Allow)** geklickt haben, starten Sie Ihren Computer neu und installieren Sie den SSL VPN-Plus Client erneut.

Wenn die Installation weiterhin fehlschlägt, bedeutet es, dass Ihr System Kernel-Extensions (Kexts) nicht zulässt und Sie auch nicht zum Laden der Kext auffordert. Führen Sie die verbleibenden Teilschritte zum Hinzufügen von tuntap kext team id zur vorab genehmigten Kext-Liste aus.

- b Starten Sie Ihren Mac-Computer im Wiederherstellungsmodus erneut.
- 1 Klicken Sie oben links auf Ihrem Bildschirm auf das Apple-Logo.
 - 2 Klicken Sie auf **Neustart (Restart)**.
 - 3 Drücken Sie sofort die Tasten „Befehl“ und „R“, bis ein Apple-Logo oder ein sich drehender Globus angezeigt wird. Ein sich drehender Globus wird angezeigt, wenn Ihr Mac-Computer versucht, die macOS-Wiederherstellung durch den Zugriff auf das Internet zu starten, da er nicht über das integrierte Wiederherstellungssystem gestartet werden kann. Mac ist nun im Wiederherstellungsmodus gestartet.
- c Klicken Sie in der Leiste ganz oben auf **Dienstprogramme (Utilities) > Terminal**.
- d Um tuntap kext team id zur Liste der vorab genehmigten Kexts hinzuzufügen, führen Sie den Befehl – `spctl kext-consent add KS8XL6T9FZ` aus.
- e Starten Sie Ihre Mac-Maschine im normalen Modus neu.
- f Um zu überprüfen, ob die „team-id“ in der Liste der vorab genehmigten Kexts angezeigt wird, führen Sie den Befehl – `spctl kext-consent list` aus.
- g Installieren Sie das SSL VPN-Plus Client-Paket.
- 7 Wenn Ihnen auf Windows-Computern ein Fehler bei der Treiberinstallation (E00024B) angezeigt wird, deaktivieren Sie die Option **SSL-Clientnetzwerkadapter ausblenden (Hide SSL client network adapter)** im Edge SSL VPN-Plus Client-Installationsprogramm. Anweisungen zum Deaktivieren dieser Option finden Sie im VMware-Knowledgebase-Artikel unter <https://kb.vmware.com/s/article/2108766>.

SSL VPN-Plus: Kommunikationsprobleme

In diesem Thema finden Sie Informationen zu möglichen Problemen im Zusammenhang mit der SSL VPN-Konnektivität und dem Datenpfad sowie zu deren Behebung.

Problem

Allgemeine Probleme im Zusammenhang mit der SSL VPN-Konnektivität und dem Datenpfad:

- SSL VPN-Plus Client kann keine Verbindung mit dem SSL VPN-Server herstellen.
- SSL VPN-Plus Client ist installiert, doch die SSL VPN-Plus-Dienste werden nicht ausgeführt.
- Die maximale Anzahl der angemeldeten Benutzer ist erreicht. Das SSL VPN-Webportal bzw. der SSL VPN-Plus Client zeigt die folgende Meldung an:

Die maximale Anzahl der Benutzer erreicht./Die maximale Anzahl der angemeldeten Benutzer ist gemäß SSL VPN-Lizenz erreicht. Versuchen Sie es später erneut oder Lesen von SSL ist fehlgeschlagen.

- SSL VPN-Dienste werden ausgeführt, doch der Datenpfad funktioniert nicht.
- SSL VPN-Verbindung ist hergestellt, doch es kann nicht auf Anwendungen im privaten Netzwerk zugegriffen werden.

Lösung

- 1 Wenn der SSL VPN-Plus Client keine Verbindung mit dem SSL VPN-Server herstellen kann, führen Sie folgende Schritte durch:
 - Stellen Sie sicher, dass sich der SSL VPN-Benutzer mit dem richtigen Benutzernamen und Kennwort anmeldet.
 - Überprüfen Sie, ob der SSL VPN-Benutzer gültig ist.
 - Überprüfen Sie, ob der SSL VPN-Benutzer den SSL VPN-Server über das Webportal erreichen kann.
- 2 Führen Sie auf dem NSX Edge die folgenden Schritte aus, um zu überprüfen, ob der SSL VPN-Prozess ausgeführt wird.
 - a Melden Sie sich beim NSX Edge über die CLI an. Weitere Informationen zur Anmeldung bei der Edge-CLI finden Sie in der *Befehlszeilenschnittstellen-Referenz zu NSX*.
 - b Führen Sie den Befehl `show process monitor` aus und suchen Sie den Prozess `sslvpn`.
 - c Führen Sie den Befehl `show service network-connections` aus und prüfen Sie, ob der Prozess `sslvpn` auf Port 443 aufgelistet ist.

Hinweis Standardmäßig verwendet das System Port 443 für SSL-Datenverkehr. Wenn Sie einen anderen TCP-Port für den SSL-Datenverkehr konfiguriert haben, stellen Sie jedoch sicher, dass der Prozess `sslvpn` auf dieser TCP-Portnummer aufgeführt ist.

3 Überprüfen Sie auf dem SSL VPN-Plus Client, ob die SSL VPN-Plus-Dienste ausgeführt werden.

Betriebssystem	Beschreibung
Windows	Öffnen Sie den Task-Manager und überprüfen Sie, ob der SSL VPN-Plus Client-Dienst gestartet wurde.
Mac	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass der Prozess <code>naclientd</code> für den Daemon gestartet wurde. ■ Stellen Sie sicher, dass der Prozess <code>naclient</code> für die GUI gestartet wurde. Führen Sie den Befehl <code>ps -ef grep "naclient"</code> aus, um zu überprüfen, ob die Prozesse ausgeführt werden.
Linux	<ul style="list-style-type: none"> ■ Stellen Sie sicher, dass die Prozesse <code>naclientd</code> und <code>naclient_poll</code> gestartet wurden. ■ Führen Sie den Befehl <code>ps -ef grep "naclient"</code> aus, um zu überprüfen, ob die Prozesse ausgeführt werden.

Wenn die Dienste nicht ausgeführt werden, führen Sie die folgenden Befehle zum Starten der Dienste aus.

Betriebssystem	Befehl
Mac	Führen Sie den Befehl <code>sudo launchctl load -w /Library/LaunchDaemons/com.vmware.naclientd.plist</code> aus.
Linux	Führen Sie den Befehl <code>sudo service naclient start</code> aus.

4 Wenn die maximale Anzahl der angemeldeten SSL VPN-Benutzer erreicht ist, erhöhen Sie die Anzahl gleichzeitiger Benutzer (CCU), indem Sie den NSX Edge-Formfaktor erhöhen.

Weitere Informationen finden Sie im Dokument *Administratorhandbuch für NSX*. Beachten Sie, dass die verbundenen Benutzer vom VPN getrennt werden, wenn Sie diesen Vorgang durchführen.

- 5 Wenn die SSL VPN-Dienste ausgeführt werden, doch der Datenpfad nicht funktioniert, führen Sie die folgenden Schritte aus:
 - a Überprüfen Sie, ob eine virtuelle IP-Adresse nach dem erfolgreichen Herstellen einer Verbindung zugewiesen wurde.
 - b Überprüfen Sie, ob die Routen hinzugefügt wurden.

- 6 Wenn auf Anwendungen im privaten Netzwerk (Back-End) nicht zugegriffen werden kann, führen Sie die folgenden Schritte aus, um das Problem zu beheben:
- a Stellen Sie sicher, dass sich das private Netzwerk und der IP-Pool nicht im selben Subnetz befinden.
 - b Wenn der Administrator keinen IP-Pool definiert hat bzw. wenn der IP-Pool ausgeschöpft ist, führen Sie diese Schritte aus.
 - 1 Melden Sie sich bei vSphere Web Client an.
 - 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
 - 3 Doppelklicken Sie auf ein NSX Edge und klicken Sie anschließend auf die Registerkarte **SSL VPN-Plus**.
 - 4 Fügen Sie einen statischen IP-Pool wie unter dem Thema „Hinzufügen eines IP-Pools“ im Dokument *Administratorhandbuch für NSX* erläutert hinzu. Stellen Sie sicher, dass Sie die IP-Adresse im Textfeld **Gateway** hinzugefügt haben. Die Gateway-IP-Adresse ist der Schnittstelle `na0` zugewiesen. Der gesamte Nicht-TCP-Datenverkehr durchläuft den virtuellen Adapter, der als Schnittstelle `na0` benannt ist. Sie können mehrere IP-Pools mit unterschiedlichen Gateway-IP-Adressen erstellen, die aber derselben Schnittstelle `na0` zugewiesen sind.
 - 5 Überprüfen Sie mit dem Befehl `show interface na0` die angegebene IP-Adresse und prüfen Sie, ob alle IP-Pools derselben Schnittstelle `na0` zugewiesen sind.
 - 6 Melden Sie sich beim Clientcomputer an, wechseln Sie zum Bildschirm **SSL VPN-Plus Client – Statistiken (SSL VPN-Plus Client - Statistics)** und überprüfen Sie die zugewiesene virtuelle IP-Adresse.
 - c Melden Sie sich bei der NSX Edge-Befehlszeilenschnittstelle (CLI) an und führen Sie für die Schnittstelle „na0“ eine Paketerfassung durch Ausführung des Befehls `debug packet capture interface na0` durch. Sie können Pakete auch mit der **Paketerfassungsfunktion (Packet Capture)** erfassen. Details hierzu finden Sie im *Administratorhandbuch für NSX*.

Hinweis Die Paketerfassung wird weiter im Hintergrund ausgeführt, bis Sie die Erfassung durch Ausführung des Befehls `no debug packet capture interface na0` beenden.

 - d Wenn die TCP-Optimierung nicht aktiviert ist, überprüfen Sie die Firewallregeln.
 - e Für den Nicht-TCP-Datenverkehr stellen Sie sicher, dass für das Back-End-Netzwerk das Standard-Gateway als interne Schnittstelle des Edge festgelegt ist.
 - f Melden Sie sich bei Mac- und Linux-Clients bei dem System an, auf dem der SSL VPN-Client installiert ist, und führen Sie die Paketerfassung für die Schnittstelle „tap0“ oder für den virtuellen Adapter durch Ausführung des Befehls `tcpdump -i tap0 -s 1500 -w filepath` durch. Verwenden Sie bei Windows-Clients ein Paketanalysetool wie Wireshark und erfassen Sie Pakete auf dem SSL VPN-Plus Client-Adapter.

- 7 Wenn das Problem mit den oben stehenden Schritten nicht behoben werden kann, verwenden Sie die folgenden NSX Edge-CLI-Befehle, um die Fehlerbehebung fortzuführen.

Zweck	Befehl
Überprüfen Sie den SSL VPN-Status.	<code>show service sslvpn-plus</code>
Überprüfen Sie die SSL VPN-Statistiken.	<code>show service sslvpn-plus stats</code>
Überprüfen Sie die VPN-Clients, die verbunden sind.	<code>show service sslvpn-plus tunnels</code>
Aktivieren Sie SSL VPN-Plus-Sitzungen.	<code>show service sslvpn-plus sessions</code>

SSL VPN-Plus: Authentifizierungsprobleme

Bei der SSL VPN-Plus-Authentifizierung treten Probleme auf.

Problem

SSL VPN-Plus-Authentifizierung schlägt fehl.

Lösung

- ◆ Überprüfen Sie bei Authentifizierungsproblemen die folgenden Einstellungen:
 - a Stellen Sie sicher, dass der externe Authentifizierungsserver von NSX Edge aus erreichbar ist. Pingt Sie in NSX Edge den Authentifizierungsserver an und überprüfen Sie, ob der Server erreichbar ist.
 - b Überprüfen Sie die Konfiguration des externen Authentifizierungsservers mithilfe von Tools wie LDAP-Browser und stellen Sie fest, ob die Konfiguration funktioniert. Es können mithilfe des LDAP-Browsers nur LDAP- und AD-Authentifizierungsserver überprüft werden.
 - c Stellen Sie sicher, dass für den lokalen Authentifizierungsserver die niedrigste Priorität festgelegt ist, wenn diese im Authentifizierungsprozess konfiguriert wird.
 - d Wenn Sie Active Directory (AD) verwenden, legen Sie dafür den `no-ssl`-Modus fest und führen Sie die Paketerfassung für die Schnittstelle durch, von der der Active Directory-Server erreichbar ist.
 - e Wenn die Authentifizierung erfolgreich im Syslog-Server durchgeführt wurde, wird eine Meldung folgender Art angezeigt:


```
Log Output - SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09:28:39,-,-,,,,,,,,-,-,
```
 - f Wenn die Authentifizierung im Syslog-Server fehlschlägt, wird eine Meldung folgender Art angezeigt:


```
Log Output - SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09:28:39,-,-,,,,,,,,-,-,
```

SSL VPN-Plus Client antwortet nicht mehr.

SSL VPN-Plus Client antwortet nicht mehr, wenn die TCP-Optimierung aktiviert ist.

Problem

Sie haben den SSL VPN-Plus-Dienst zur Ausführung auf einem NSX Edge konfiguriert und die TCP-Optimierung für das Senden von Datenverkehr über den Tunnel aktiviert. Der SSL VPN-Plus-Client antwortet nicht mehr, wenn Sie Messungen zur Netzwerkleistung und Abstimmungstools (z. B. iperf3) auf dem SSL VPN-Plus Client ausführen.

Ursache

Eines der beiden nachfolgend aufgeführten Szenarien kann dazu führen, dass der Tunnel-Lesefehler auftritt, wenn Daten vom SSL VPN-Plus Client gesendet werden:

- Back-End-Server beendet die TCP-Verbindung mit dem SSL VPN-Server durch das Senden einer TCP-FIN-Sequenz.
- Der Tunnel-Schreibvorgang schlägt beim Weiterleiten von Daten an den Back-End-Server fehl.

Der Tunnel-Lesefehler ist Unbekannte Protokoll-ID. Durch diesen Fehler wird der Tunnel zwischen dem SSL VPN-Server und dem SSL VPN-Plus Client gelöscht, wodurch wiederum SSL-Lese-/Schreibvorgänge auf dem Client fehlschlagen und der SSL VPN-Plus-Client nicht mehr antwortet.

Lösung

- ◆ Gehen Sie zur Behebung dieses Problems wie folgt im vSphere Web Client vor, um die TCP-Optimierung für den privaten Netzwerkdatenverkehr über den SSL VPN-Tunnel zu deaktivieren.
 - a Doppelklicken Sie auf die NSX Edge-VM, auf der Sie den SSL VPN-Plus-Dienst konfiguriert haben.
 - b Klicken Sie auf die Registerkarte **SSL VPN-Plus**, und wählen Sie dann das private Netzwerk.
 - c Deaktivieren Sie das Kontrollkästchen **TCP-Optimierung aktivieren (Enable TCP Optimization)**.

Grundlegende Protokollanalyse

SSL VPN-Plus-Gateway-Protokolle werden an den auf der NSX Edge-Appliance konfigurierten Syslog-Server gesendet. SSL VPN-Plus Client-Protokolle werden im folgenden Verzeichnis auf dem Computer des Remotebenutzers gespeichert: `C:\Users\Benutzername\AppData\Local\VMware\vpn\svp_client.log`.

Grundlegende Protokollanalyse – Authentifizierung

Erfolgreiche Authentifizierung

- Die folgende Protokollausgabe zeigt, dass der Benutzer *a* am 28. Oktober 2016 um 09:28 erfolgreich beim Netzwerkzugriffsclient authentifiziert wurde.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCE
S,,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

Fehler bei Authentifizierung

- Die folgende Protokollausgabe zeigt, dass der Benutzer *a* am 28. Oktober 2016 um 09:28 Uhr nicht beim Netzwerkzugriffsscient authentifiziert werden konnte.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILUR
E,,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

Informationen zur Behebung von Problemen bei der Authentifizierung finden Sie unter [SSL VPN-Plus: Installationsfehler](#).

Grundlegende Protokollanalyse – Datenpfad

Erfolgreicher Datenpfad

- Die folgende Protokollausgabe zeigt, dass der Benutzer *a* am 28. Oktober 2016 um 09:41 mit dem Netzwerkzugriffsscient über TCP erfolgreich eine Verbindung mit dem Back-End-Webserver 192.168.10.8 hergestellt hat.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,,10-28-2013,09:41:03,-,-,192.168.10.8,8
0,,,,,,,,,-,-,-
```

Fehler beim Datenpfad

- Die folgende Protokollausgabe zeigt, dass der Benutzer *a* am 28. Oktober 2016 um 09:41 mit dem Netzwerkzugriffsscient über TCP keine Verbindung mit dem Back-End-Webserver 192.168.10.8 herstellen konnte.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,,10-28-2013,09:41:03,-,-,192.168.10.8,8
0,,,,,,,,,-,-,-
```

IPSec-VPN

Anhand dieser Informationen können Sie konfigurationsbedingte Aushandlungsprobleme beheben.

Erfolgreiche Aushandlung (sowohl Phase 1 als auch Phase 2)

Die folgenden Beispiele zeigen das Ergebnis einer erfolgreichen Aushandlung zwischen NSX Edge und einem Cisco-Gerät.

NSX Edge

Von der NSX Edge-Befehlszeilenschnittstelle aus (ipsec auto -status, Teil des Befehls „show service ipsec“):

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
```

```

import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
import:admin initiate

```

Cisco

```

ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L      Role   : responder
Rekey : no      State  : MM_ACTIVE
Encrypt : 3des  Hash   : SHA
Auth : preshared Lifetime: 28800
Lifetime Remaining: 28379

```

Phase 1-Richtlinie stimmt nicht überein

Im Folgenden sind Protokolleinträge für Fehler aufgrund der Nichtübereinstimmung der Phase-1-Richtlinie aufgeführt.

NSX Edge

NSX Edge hängt im Zustand „STATE_MAIN_I1“. Suchen Sie unter „/var/log/messages“ nach Informationen, die zeigen, dass der Peer eine IKE-Meldung zurückgesendet hat, bei der „NO_PROPOSAL_CHOSEN“ festgelegt ist.

```

000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:

```



```
"s1-c1" #1: ignoring informational payload,
type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

Wenn „debug crypto“ aktiviert ist, wird eine Fehlermeldung ausgegeben, die angibt, dass keine Vorschläge akzeptiert wurden.

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
  IP = 10.20.129.80, IKE_DECODE RECEIVED
  Message (msgid=0) with payloads : HDR + SA (1)
  + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
  processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
  types for class Group Description: Rcv'd: Group 5
  Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
  types for class Group Description: Rcv'd: Group 5
  Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
  Message (msgid=0) with payloads : HDR + NOTIFY (11)
  + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
  All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
  payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
  FSM error history (struct &0xd8355a60) <state>, <event>:
  MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
  EV_START_MM-->MM_START, EV_START_MM-->MM_START,
  EV_START_MM-->MM_START, EV_START_MM-->MM_START,
  EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
  MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
  tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
  delete/delete with reason message
```

Phase 2 stimmt nicht überein

Im Folgenden sind Protokolleinträge für Fehler aufgrund der Nichtübereinstimmung der Phase-2-Richtlinie aufgeführt.

NSX Edge

NSX Edge hängt im Status „STATE_QUICK_I1“. Ein Protokollmeldung zeigt, dass der Peer eine NO_PROPOSAL_CHOSEN-Meldung gesendet hat.

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
  QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
  idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
```

```

0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     next payload
type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
|     DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |     Notify Message
Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
ignoring informational payload, type NO_PROPOSAL_CHOSEN
msgid=00000000

```

Cisco

Die Debug-Meldungen zeigen, dass Phase 1 abgeschlossen wurde, Phase 2 jedoch fehlschlug, weil das Aushandeln der Richtlinien gescheitert ist.

```

Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
+ SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
Session is being torn down. Reason: Phase 2 Mismatch

```

PFS-Nichtübereinstimmung

Im Folgenden sind Protokolleinträge für Fehler aufgrund von PFS-Nichtübereinstimmung aufgeführt.

NSX Edge

PFS wird als Teil der Phase 2 ausgehandelt. Bei Nichtübereinstimmung von PFS ähnelt das Verhalten dem unter [Phase 2 stimmt nicht überein](#) beschriebenen Fehlerfall.

```

000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |
| ***parse ISAKMP Notification Payload:

```

```

Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   next payload
           type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |   Notify Message
           Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
           informational payload, type NO_PROPOSAL_CHOSEN
           msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
           91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |
           | processing informational NO_PROPOSAL_CHOSEN (14)

```

Cisco

```

<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
           IP = 10.20.129.80, sending delete/delete with
           reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
           IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
           IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
           IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
           IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
           Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
           + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
           Session is being torn down. Reason: Phase 2 Mismatch

```

PSK stimmt nicht überein

Im Folgenden sind Protokolleinträge für Fehler aufgrund von PSK-Nichtübereinstimmung aufgeführt.

NSX Edge

Der PSK wird in der letzten Runde der Phase 1 ausgehandelt. Wenn die PSK-Aushandlung fehlschlägt, ist der Status von NSX Edge „STATE_MAIN_I4“. Der Peer sendet eine INVALID_ID_INFORMATION-Meldung.

```

Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
           "s1-c1" #1: transition from state STATE_MAIN_I3 to
           state STATE_MAIN_I4

```

```

Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
STATE_MAIN_I4: ISAKMP SA established
{auth=OAKLEY_PRESHARED_KEY
cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
ignoring informational payload, type INVALID_ID_INFORMATION
msgid=00000000

```

Cisco

```

Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
+ NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, Received encrypted Oakley Main Mode
packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
Message (msgid=0) with payloads : HDR + NOTIFY (11)
+ NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, ERROR, had problems decrypting
packet, probably due to mismatched pre-shared key.
Aborting

```

Paketerfassung für eine erfolgreiche Aushandlung

Die folgende Liste zeigt eine Paketerfassungssitzung für eine erfolgreiche Aushandlung zwischen NSX Edge und einem Cisco-Gerät.

No.	Time	Source	Destination	Protocol	Info
9203	768.394800	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)
Frame 9203 (190 bytes on wire, 190 bytes captured)					
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd), Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)					
Internet Protocol, Src: 10.20.129.80 (10.20.129.80), Dst: 10.20.131.62 (10.20.131.62)					
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)					
Internet Security Association and Key Management Protocol					
Initiator cookie: 92585D2D797E9C52					
Responder cookie: 0000000000000000					
Next payload: Security Association (1)					
Version: 1.0					
Exchange type: Identity Protection (Main Mode) (2)					
Flags: 0x00					

```

Message ID: 0x00000000
Length: 148
Security Association payload
  Next payload: Vendor ID (13)
  Payload length: 84
  Domain of interpretation: IPSEC (1)
  Situation: IDENTITY (1)
  Proposal payload # 0
    Next payload: NONE (0)
    Payload length: 72
    Proposal number: 0
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 2
    Transform payload # 0
      Next payload: Transform (3)
      Payload length: 32
      Transform number: 0
      Transform ID: KEY_IKE (1)
      Life-Type (11): Seconds (1)
      Life-Duration (12): Duration-Value (28800)
      Encryption-Algorithm (1): 3DES-CBC (5)
      Hash-Algorithm (2): SHA (2)
      Authentication-Method (3): PSK (1)
      Group-Description (4): 1536 bit MODP group (5)
    Transform payload # 1
      Next payload: NONE (0)
      Payload length: 32
      Transform number: 1
      Transform ID: KEY_IKE (1)
      Life-Type (11): Seconds (1)
      Life-Duration (12): Duration-Value (28800)
      Encryption-Algorithm (1): 3DES-CBC (5)
      Hash-Algorithm (2): SHA (2)
      Authentication-Method (3): PSK (1)
      Group-Description (4): Alternate 1024-bit MODP group (2)
  Vendor ID: 4F456C6A405D72544D42754D
  Next payload: Vendor ID (13)
  Payload length: 16
  Vendor ID: 4F456C6A405D72544D42754D
Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
  Next payload: NONE (0)
  Payload length: 20
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

```

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
  Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)

```

Internet Security Association and Key Management Protocol

```

Initiator cookie: 92585D2D797E9C52
Responder cookie: 34704CFC8C8DBD09
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
Message ID: 0x00000000
Length: 104
Security Association payload
  Next payload: Vendor ID (13)
  Payload length: 52
  Domain of interpretation: IPSEC (1)
  Situation: IDENTITY (1)
  Proposal payload # 1
    Next payload: NONE (0)
    Payload length: 40
    Proposal number: 1
    Protocol ID: ISAKMP (1)
    SPI Size: 0
    Proposal transforms: 1
    Transform payload # 1
      Next payload: NONE (0)
      Payload length: 32
      Transform number: 1
      Transform ID: KEY_IKE (1)
      Encryption-Algorithm (1): 3DES-CBC (5)
      Hash-Algorithm (2): SHA (2)
      Group-Description (4): Alternate 1024-bit MODP group (2)
      Authentication-Method (3): PSK (1)
      Life-Type (11): Seconds (1)
      Life-Duration (12): Duration-Value (28800)
  Vendor ID: Microsoft L2TP/IPSec VPN Client
  Next payload: NONE (0)
  Payload length: 24
  Vendor ID: Microsoft L2TP/IPSec VPN Client

```

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

```

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
  Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
  Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000

```

```

Length: 180
Key Exchange payload
  Next payload: Nonce (10)
  Payload length: 132
  Key Exchange Data (128 bytes / 1024 bits)
Nonce payload
  Next payload: NONE (0)
  Payload length: 20
  Nonce Data

```

No.	Time	Source	Destination	Protocol Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
  Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
  Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: Vendor ID (13)
    Payload length: 24
    Nonce Data
  Vendor ID: CISCO-UNITY-1.0
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: CISCO-UNITY-1.0
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
    Next payload: Vendor ID (13)
    Payload length: 12
    Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Vendor ID: CISCO-CONCENTRATOR
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: CISCO-CONCENTRATOR

```

No.	Time	Source	Destination	Protocol Info
-----	------	--------	-------------	---------------

9207 768.404990 10.20.129.80 10.20.131.62 ISAKMP Identity Protection
(Main Mode)

Frame 9207 (110 bytes on wire, 110 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 68
 Encrypted payload (40 bytes)

No.	Time	Source	Destination	Protocol	Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

Frame 9208 (126 bytes on wire, 126 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 84
 Encrypted payload (56 bytes)

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)

Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
 Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

Frame 9211 (94 bytes on wire, 94 bytes captured)
 Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 52
 Encrypted payload (24 bytes)

Fehlerbehebung für NSX Controller

8

Dieses Thema bietet Informationen zur Erkennung von Ursachen für NSX Controller-Fehler und zur Fehlerbehebung bei Controllern.

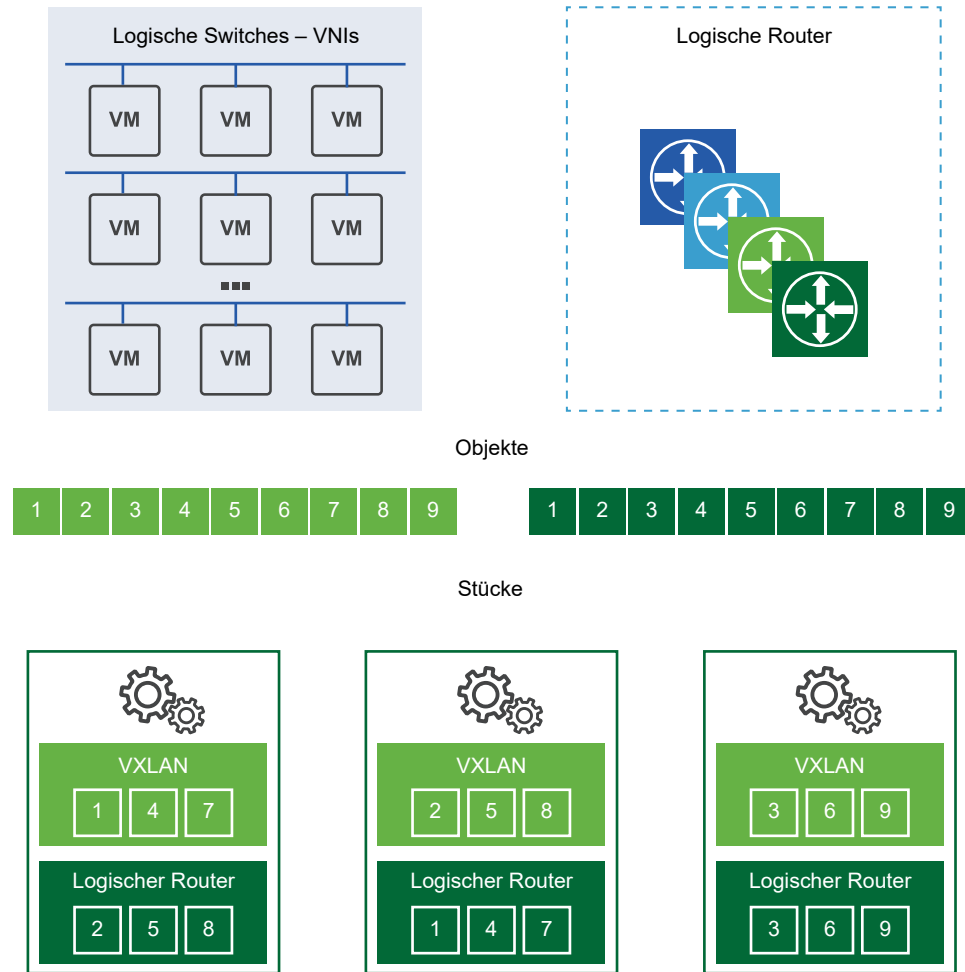
Dieses Kapitel enthält die folgenden Themen:

- [Informationen zur Controller-Clusterarchitektur](#)
- [Bereitstellungsprobleme von NSX Controller](#)
- [Fehlerbehebung bei Festplattenlatenz](#)
- [NSX Controller-Cluster-Fehler](#)
- [NSX Controller ist getrennt](#)
- [Probleme mit dem Agenten der Kontrollebene \(netcpa\)](#)

Informationen zur Controller-Clusterarchitektur

Beim NSX Controller-Cluster handelt es sich um ein verteiltes Scale-Out-System, bei dem jedem Controller-Knoten ein Satz an Rollen zugewiesen ist. Diese Rollen legen die Art von Aufgaben fest, die der Knoten implementieren kann. Um die Ausfallsicherheit und die Leistung zu erhöhen, sollte die Bereitstellung der Controller-VMs auf drei unterschiedlichen Hosts erfolgen.

Mithilfe der horizontalen Fragmentierung („Sharding“) werden Arbeitslasten auf alle NSX Controller-Clusterknoten verteilt. Beim Sharding werden NSX Controller-Arbeitslasten in kleine Datensätze aufgeteilt, damit jede NSX Controller-Instanz dieselbe Arbeitslast verarbeiten muss.



Dies zeigt, dass einzelne Controller-Knoten als Master für bestimmte Instanzen wie logisches Switching, logisches Routing und andere Dienste auftreten können. Nachdem eine Master-NSX Controller-Instanz für eine Rolle ausgewählt wurde, teilt dieser NSX Controller die unterschiedlichen logischen Switches und Router unter allen verfügbaren NSX Controller-Instanzen in einem Cluster auf.

Jedes nummerierte Kästchen in einem Shard steht für die Datensätze, die der Master zum Aufteilen der Arbeitslasten verwendet. Der logische Master-Switch teilt die logischen Switches in Shards auf und weist diese Datensätze den unterschiedlichen NSX Controller-Instanzen zu. Der logische Master-Router teilt die logischen Router ebenfalls in Shards auf und weist diese Datensätze den unterschiedlichen NSX Controller-Instanzen zu.

Diese Datensätze werden den unterschiedlichen NSX Controller-Instanzen in diesem Cluster zugewiesen. Der Master für eine Rolle legt fest, welche NSX Controller-Instanzen welchem Datensatz zugewiesen werden. Wenn Router-Shard 3 eine Anforderung erhält, bekommt dieser Datensatz den Befehl, eine Verbindung zur dritten NSX Controller-Instanz herzustellen. Wenn der Shard 2 der logischen Switches eine Anforderung erhält, wird diese von der zweiten NSX Controller-Instanz verarbeitet.

Wenn eine der NSX Controller-Instanzen in einem Cluster ausfällt, verteilen die Master für die Rollen die Datensätze auf den verbleibenden verfügbaren Clustern. Einer der Controller-Knoten wird als Master für jede Rolle ausgewählt. Dieser Master ist für die Zuteilung der Datensätze zu den einzelnen Controller-Knoten zuständig. Er kann feststellen, ob ein Knoten ausgefallen ist, und teilt die Datensätze auf die verbleibenden Knoten auf. Der Master informiert außerdem die ESXi-Hosts über den Ausfall des Clusterknotens.

Für die Auswahl des Masters für jede Rolle ist eine Mehrheitswahl aller aktiven und inaktiven Knoten im Cluster erforderlich. Das ist der hauptsächliche Grund dafür, dass ein Controller-Cluster immer eine ungerade Anzahl an Knoten enthalten muss.

ZooKeeper

ZooKeeper ist eine Clientserverarchitektur, die für den NSX Controller-Clustermechanismus verantwortlich ist. Der Controller-Cluster wird mit ZooKeeper erkannt und erstellt. Wenn ein Cluster gestartet wird, bedeutet das, dass ZooKeeper auf allen Knoten gestartet wird. Die ZooKeeper-Knoten durchlaufen den Wahlvorgang, um den Controller-Cluster zu bilden. Im Cluster muss ein ZooKeeper-Master-Knoten vorhanden sein. Dieser wird unter den Knoten ausgewählt.

Wenn ein neuer Controller-Knoten erstellt wird, schlägt NSX Manager dem aktuellen Cluster die Knoteninformationen, einschließlich Knoten-IP und -ID, vor. Daher kennt jeder Knoten die Gesamtzahl an Knoten, die für das Clustering zur Verfügung stehen. Bei der Wahl des ZooKeeper-Masters gibt jeder Knoten eine Stimme für die Wahl des Master-Knotens ab. Die Wahl wird erneut ausgelöst, bis ein Knoten die Mehrheit aller Stimmen erhalten hat. In einem Cluster aus drei Knoten muss der Master beispielsweise mindestens zwei Stimmen erhalten.

Hinweis Um zu verhindern, dass kein ZooKeeper-Master gewählt werden kann, MUSS die Anzahl an Knoten im Cluster drei sein.

- Wenn der erste Controller bereitgestellt wird, handelt es sich um einen Sonderfall und der erste Controller wird Master. Daher muss bei der Controller-Bereitstellung auch erst die Bereitstellung des ersten Knotens abgeschlossen sein, bevor weitere Knoten hinzugefügt werden.
- Wenn der zweite Controller hinzugefügt wird, handelt es sich ebenfalls um einen Sonderfall, da die Anzahl an Knoten zu diesem Zeitpunkt gerade ist.
- Wenn der dritte Knoten hinzugefügt wird, erreicht der Cluster einen unterstützten stabilen Status.

ZooKeeper unterstützt jeweils nur einen Ausfall. Das heißt, dass bei Ausfall eines Controller-Knotens der Knoten wiederhergestellt werden muss, bevor ein weiterer Ausfall auftritt. Andernfalls kann es zu Problemen mit der Funktionstüchtigkeit des Clusters geben.

Domänenmanager der zentralen Kontrollebene (Central Control Plane, CCP)

Dabei handelt es sich um die Ebene über ZooKeeper, die die Konfiguration für den Start von ZooKeeper auf allen Knoten bereitstellt. Der Domänenmanager aktualisiert die Konfiguration zwischen allen Knoten im Cluster und fordert dann remote den Start des ZooKeeper-Prozesses an.

Der Domänenmanager ist für das Starten aller Domänen verantwortlich. Um dem Cluster beizutreten, muss die CCP-Domäne mit den CCP-Domänen auf anderen Rechnern kommunizieren. Die Komponente der CCP-Domäne, die die Clusterinitialisierung unterstützt, ist *zk-cluster-bootstrap*.

Controller-Beziehung zu anderen Komponenten

Der Controller-Cluster ist für die Verwaltung und Bereitstellung von Informationen zu logischen Switches, logischen Routern und VTEPs für die ESXi-Hosts verantwortlich.

Wenn ein logischer Switch erstellt wird, legen die Controller-Knoten im Cluster fest, welcher Knoten im Cluster *Master* oder *Besitzer* für diesen logischen Switch wird. Dasselbe gilt, wenn ein logischer Router hinzugefügt wird.

Sobald der Besitzer für einen logischen Switch bzw. Router festgelegt wurde, sendet der Knoten diese Besitzinformationen an die ESXi-Hosts, die zur Transportzone dieses Switches bzw. Routers gehören. Die gesamte Auswahl des Besitzes und das Vorschlagen der Besitzinformationen für die Hosts wird als „Sharding“ bezeichnet. Beachten Sie: Besitz bedeutet, dass der Knoten für alle NSX-Vorgänge für diesen logischen Switch bzw. Router verantwortlich ist. Die anderen Knoten führen keine Vorgänge für diesen logischen Switch aus.

Es darf nur ein Besitzer die Informationsquelle für einen logischen Switch und Router sein. Wenn in einem Controller-Cluster zwei oder mehr Knoten als Besitzer für einen logischen Switch bzw. Router gewählt werden, hat möglicherweise jeder Host im Netzwerk unterschiedliche Informationen zur Informationsquelle für diesen logischen Switch bzw. Router. In diesem Fall kommt es zu einem Netzwerkausfall, da Vorgänge auf der Kontroll- und Datenebene nur eine Informationsquelle aufweisen können.

Wenn ein Controller-Knoten ausfällt, führen die verbleibenden Knoten im Cluster ein Resharding durch, um die Zuständigkeit für den logischen Switch und das logische Routing zu ermitteln.

Bereitstellungsprobleme von NSX Controller

NSX Controller werden von NSX Manager im OVA-Format bereitgestellt. Ein Controller-Cluster bietet die Möglichkeit einer Hochverfügbarkeit (HA, High Availability). Für die Bereitstellung von Controllern müssen NSX Manager, vCenter Server und ESXi-Hosts über ein konfiguriertes DNS und NTP verfügen. Zur Zuweisung der IP-Adresse an jeden Controller muss ein Pool von statischen IP-Adressen verwendet werden.

Es wird empfohlen, DRS-Anti-Affinitätsregeln zu implementieren, um die NSX Controller auf getrennten Hosts zu halten. Sie müssen DREI NSX Controller bereitstellen.

Allgemeine Probleme mit Controllern

Bei der Bereitstellung von NSX Controllern können folgende, typische Probleme auftreten:

- Fehler bei der Bereitstellung von NSX Controller(n).
- Beitritt des NSX Controller zum Cluster schlägt fehl.

- Mit dem Befehl `show control-cluster status` wird das Majority status-Flapping zwischen Connected to cluster majority und Interrupted connection to cluster majority angezeigt.
- Probleme bei der Anzeige des Verbindungsstatus auf dem NSX-Dashboard.
- Wir empfehlen den Befehl `show control-cluster status`, um anzuzeigen, ob ein Controller einem Controller-Cluster beigetreten ist. Sie müssen diesen Befehl auf jedem Controller ausführen, um den allgemeinen Clusterstatus herauszufinden.

```

controller # show control-cluster status
Type                Status                                     Since
-----
Join status:         Join complete                               10/17 18:16:58
Majority status:     Connected to cluster majority                         10/17 18:16:46
Restart status:      This controller can be safely restarted             10/17 18:16:51
Cluster ID:          af2e9dec-19b9-4530-8e68-944188584268
Node UUID:           af2e9dec-19b9-4530-8e68-944188584268
Role                 Configured status  Active status
-----
api_provider         enabled           activated
persistence_server   enabled           activated
switch_manager       enabled           activated
logical_manager       enabled           activated
dht_node             enabled           activated

```

Hinweis Wenn Sie sehen, dass ein Controller-Knoten nicht verbunden ist, verwenden Sie NICHT den Befehl `join cluster` oder `force join`. Dieser Befehl ist nicht für den Beitritt eines Knotens zum Cluster gedacht. Die Verwendung des Befehls könnte zu einem völlig unsicheren Clusterstatus führen.

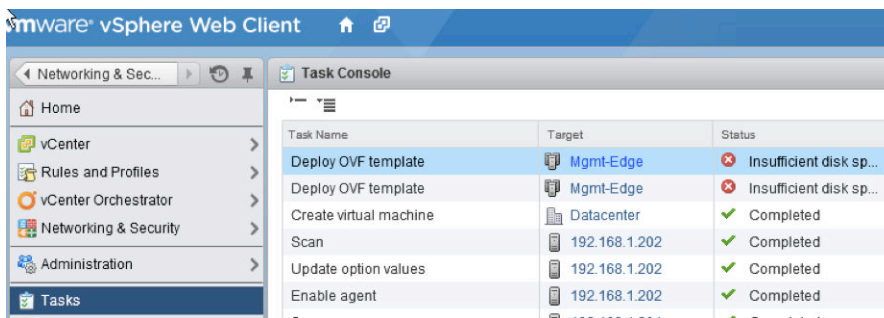
Clusterstartknoten geben den Clustermitgliedern lediglich einen Hinweis, wo gesucht werden muss, wenn die Mitglieder starten. Machen Sie sich keine Sorgen, wenn diese Liste Clustermitglieder enthält, die nicht länger genutzt werden. Die Clusterfunktionalität wird dadurch nicht beeinträchtigt.

Alle Clustermitglieder sollten dieselbe Cluster-ID aufweisen. Wenn dies nicht der Fall ist, befindet sich der Cluster in einem fehlerhaften Status. Kümmern Sie sich in diesem Fall zusammen mit dem technischen Support von VMware um die Fehlerbehebung.

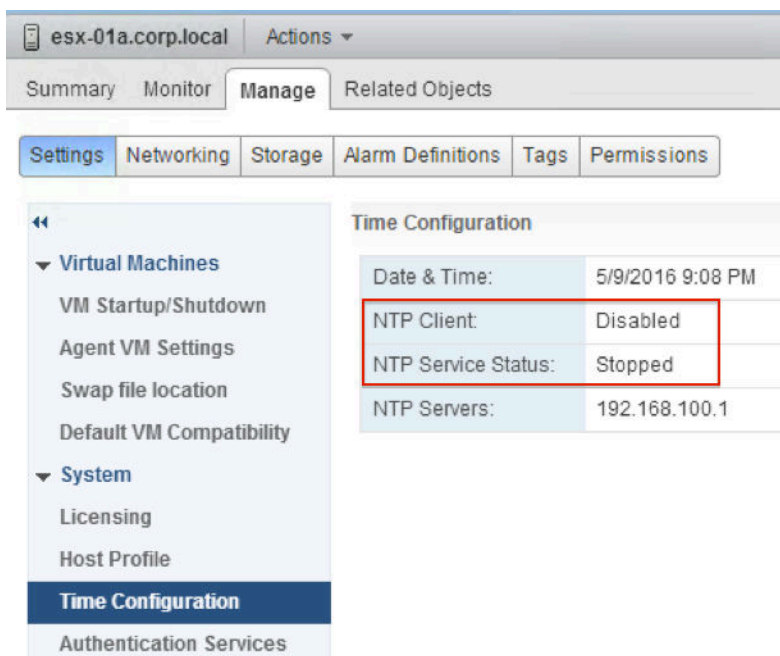
- Der Befehl `show control-cluster startup-nodes` dient nicht dazu, alle aktuell im Cluster vorhandenen Knoten anzuzeigen. Stattdessen zeigt der Befehl, welche anderen Controller-Knoten von diesem Knoten genutzt werden, um die Mitgliedschaft im Cluster zu laden, wenn der Controller-Prozess erneut startet. Dementsprechend zeigt die Befehlsausgabe möglicherweise einige Knoten, die ausgeschaltet sind oder auf andere Weise vom Cluster entfernt wurden.
- Des Weiteren können Sie mit dem Befehl `show control-cluster network ipsec status` den IPsec-Status (Internet Protocol Security) anzeigen. Wenn Sie bemerken, dass Controller einige Minuten oder Stunden lang nicht untereinander kommunizieren können, führen Sie den Befehl `cat /var/log/syslog | egrep "sending DPD request|IKE_SA"` aus, um zu prüfen,

ob die Protokollnachrichten fehlenden Datenverkehr angeben. Sie können auch mit dem Befehl `ipsec statusall | egrep "bytes_i|bytes_o"` überprüfen, dass keine zwei IPsec-Tunnel eingerichtet wurden. Wenn Sie ein mutmaßliches Controller-Cluster-Problem an einen Mitarbeiter des technischen Supports von VMware melden, legen Sie die Ausgabe dieser Befehle sowie die Controller-Protokolle vor.

- Probleme der IP-Konnektivität zwischen NSX Manager und den NSX Controllern. Diese werden meist durch Konnektivitätsprobleme der physischen Netzwerke verursacht oder durch Blockierung der Kommunikation aufgrund einer Firewall.
- Unzureichende Ressourcen wie ein zu geringer verfügbarer Speicher auf vSphere zum Hosten der Controller. Solche Probleme lassen sich durch die Anzeige des vCenter-Ereignis- und Aufgabenprotokolls während der Bereitstellung der Controller ermitteln.



- Ein „defekter“ Controller verhält sich falsch oder aktualisierte Controller befinden sich im Status **Getrennt (Disconnected)**.
- DNS auf ESXi-Hosts und NSX Manager sind nicht korrekt konfiguriert.
- NTPs auf ESXi-Hosts und NSX Manager sind nicht synchronisiert.



- Wenn neu verbundene VMs über keinen Netzwerkzugriff verfügen, liegt die Ursache vermutlich in einem Problem der Steuerungskomponente. Überprüfen Sie den Status des Controllers.

Führen Sie auch den Befehl `esxcli network vswitch dvs vmware vxlan network list --vds-name <name>` auf ESXi-Hosts aus, um den Status der Steuerungskomponente zu prüfen.

Beachten Sie, die Controller-Verbindung getrennt sein muss.

```
/etc/vmware/netcpa # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane Controller Connection
-----
5000 N/A (headend replication) Enabled (multicast proxy, ARP proxy) 192.168.110.203 (down)
```

- Mit dem CLI-Befehl `show log manager follow` von NSX Manager können Sie weitere Ursachen von Fehlern beim Bereitstellen von Controllern ermitteln.

```
2014-02-26 10:09:44.931 GMT INFO taskScheduler-25 VCConnection$VimClient:1219 - Create stub for com.vmware.vim.binding
28c5157-abf3-718e-88c5-42209f389211
2014-02-26 10:09:44.932 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:301 - got prop collector up
ctReference: type = PropertyFilter, value = session[d46b86a2-7a10-c17e-6ebe-8ab252ee4efd]527420f2-bdd7-529b-8ab6-17d16
6E3-4A64-96D7-5833C287588F
2014-02-26 10:09:44.937 GMT ERROR taskScheduler-25 VCUtils:184 - Error while waiting for property collector updates.
com.vmware.vim.binding.vim.fault.NoDiskSpace:
datastore = datastore1 (1)
inherited from com.vmware.vim.binding.vim.fault.FileFault:
file = [datastore1 (1)] NSX_Controller_1c3dd18d-0cd3-4d7d-896b-51247176ae77/NSX_Controller_1c3dd18d-0cd3-4d7d-896b-512
inherited from com.vmware.vim.binding.vim.fault.VimFault:
inherited from com.vmware.vim.binding.vim.fault.NoDiskSpace: Insufficient disk space on datastore 'datastore1 (1)'.
```

Host-Verbindungsprobleme

Mit den folgenden Befehlen können Sie Host-Verbindungsprobleme erkennen. Führen Sie diese Befehle auf jedem Controller-Knoten durch.

- Prüfen Sie mit dem Befehl `show log cloudnet/cloudnet_java-vnet-controller*.log` `filtered-by host_IP`, ob abnormale Fehlerstatistiken vorliegen.
- Überprüfen Sie mit den folgenden Befehlen die Nachrichtenstatistiken des logischen Switches/Routers oder die hohe Nachrichtenrate:
 - `show control-cluster core stats`: allgemeine Statistiken
 - `show control-cluster core stats-sample`: neueste Statistiken (Auszüge)
 - `show control-cluster core connection-stats ip`: Statistiken je Verbindung
 - `show control-cluster logical-switches stats`
 - `show control-cluster logical-routers stats`
 - `show control-cluster logical-switches stats-sample`
 - `show control-cluster logical-routers stats-sample`
 - `show control-cluster logical-switches vni-stats vni`
 - `show control-cluster logical-switches vni-stats-sample vni`
 - `show control-cluster logical-switches connection-stats ip`
 - `show control-cluster logical-routers connection-stats ip`

- Mit dem Befehl `show host hostID health-status` können Sie den Systemzustand von Hosts in Ihren vorbereiteten Clustern überprüfen. Für die Controller-Fehlerbehebung werden folgende Systemzustandsprüfungen unterstützt:
 - Überprüfung, ob die `net-config-by-vsm.xml` mit der Controller-Liste synchronisiert ist.
 - Überprüfung, ob eine Socket-Verbindung zum Controller besteht.
 - Überprüfung, ob die VXLAN-Netzwerkennung (VNI) erstellt wurde und die Konfiguration korrekt ist.
 - Überprüfung, ob die VNI eine Verbindung zu den Master-Controllern herstellt (falls die Kontrollebene aktiviert ist).

Installations- und Bereitstellungsprobleme

- Stellen Sie sicher, dass mindestens drei Controller-Knoten in einem Cluster bereitgestellt werden. VMware empfiehlt, mit Hilfe der nativen Anti-Affinitätsregeln von vSphere die Bereitstellung von mehr als einem Controller-Knoten auf demselben ESXi-Host zu verhindern.
- Überprüfen Sie, dass alle NSX Controllers den Status `Connected` aufweisen. Wenn einer der Controller-Knoten den Status `Disconnected` aufweist, stellen Sie sicher, dass die nachfolgenden Informationen konsistent sind. Führen Sie dazu den Befehl `show control-cluster status` auf allen Controller-Knoten aus:

Typ	Status
Join status (Beitrittsstatus)	Join complete (Beitritt abgeschlossen)
Majority status (Mehrheitsstatus)	Connected to cluster majority (Mit Clustermehrheit verbunden)
Cluster-ID	Dieselben Informationen auf allen Controller-Knoten

- Stellen Sie sicher, dass alle Rollen auf allen Controller-Knoten konsistent sind:

Rolle	Konfigurierter Status	Aktiver Status
<code>api_provider</code>	aktiviert	aktiviert
<code>persistence_server</code>	aktiviert	aktiviert
<code>switch_manager</code>	aktiviert	aktiviert
<code>logical_manager</code>	aktiviert	aktiviert
<code>directory_server</code>	aktiviert	aktiviert

- Überprüfen Sie, ob der `vnet-controller`-Vorgang ausgeführt wird. Führen Sie den Befehl `show process` auf allen Controller-Knoten durch, um sicherzustellen, dass der Dienst `java-dir-server` ausgeführt wird.
- Überprüfen Sie den Clusterverlauf, und stellen Sie sicher, dass es keine Anzeichen für Host-Verbindungs-Flapping, VNI-Beitrittsfehler und abnormale Änderungen bei den

Clustermemberschaften gibt. Um dies zu überprüfen, führen Sie den Befehl `show control-cluster history` aus. Dieser Befehl zeigt auch an, ob der Knoten häufig neu gestartet wird. Stellen Sie sicher, dass es nur wenige Protokolldateien mit einer Dateigröße von null (0) und mit unterschiedlichen Prozess-IDs gibt.

- Überprüfen Sie, ob die VXLAN-Netzwerk-ID (VNI) konfiguriert ist. Weitere Informationen finden Sie im Abschnitt Schritte zur VXLAN-Vorbereitung im VMware VXLAN Deployment Guide.
- Überprüfen Sie, ob auf dem Controller-Cluster SSL aktiviert ist. Führen Sie den Befehl `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by sslEnabled` auf jedem Controller-Knoten durch.

Fehlerbehebung bei Festplattenlatenz

Sie können Festplattenlatenzwarnungen auf der Registerkarte **Management** anzeigen. NSX Controller müssen auf Festplatten mit geringer Latenz betrieben werden.

Festplattenlatenzwarnungen anzeigen

Mit Festplattenlatenzwarnungen werden die Festplattenverfügbarkeit und Latenzprobleme überwacht und gemeldet. Sie können die Details zur Festplattenlatenz für jeden NSX Controller anzeigen. Die Berechnungen der Lese- und Schreiblatenz werden in einen gleitenden 5-Sekunden-Durchschnitt (standardmäßig) eingegeben, was wiederum eine Warnung auslöst, wenn der Latenzhöchstwert überschritten wird. Die Warnung wird abgeschaltet, wenn der Durchschnitt sich dem unteren Grenzwert nähert. Standardmäßig ist der Höchstwert auf 200 ms, der untere Grenzwert auf 100 ms eingestellt. Hohe Latenzen beeinträchtigen den Betrieb der verteilten Clusteranwendungen auf jedem Controller-Knoten.

Um die Festplattenlatenzwarnungen für NSX Controller anzuzeigen, führen Sie folgenden Vorgang durch:

Voraussetzungen







Latenzhöchstwert ist erreicht.



Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.

- 3 Navigieren Sie unter **Management** zum gewünschten Controller und klicken Sie auf den Link **Datenträgerwarnung (Disk Alert)**.

Das Fenster für Festplattenlatenzwarnungen wird angezeigt.

192.168.110.33 - Disk Latency Alerts				
Device Name	Latency Type	Refresh Time	Last Latency (ms)	Average Latency (ms)
 sda	Write	9/26/2016 2:15 PM	3.2	7.906
 sda	Read	9/26/2016 1:08 PM	0.0	0.0
 dm-1	Write	9/16/2016 5:11 PM	0.0	0.0
 dm-1	Read	9/22/2016 4:31 PM	0.0	0.0
 dm-0	Write	9/26/2016 2:15 PM	3.64	9.822
 dm-0	Read	9/26/2016 10:05 AM	0.0	33.334
6 items				

5	 Disk Alert	 Disk Alert
---	--	--

Ergebnisse

Sie können die Latenzinformationen für den ausgewählten Controller anzeigen. Die Warnberichte werden sieben Tage lang in der Protokolldatei `cloudnet/run/iostat/iostat_alert.log` gespeichert. Mit dem Befehl `show log cloudnet/run/iostat/iostat_alert.log` können Sie die Protokolldatei anzeigen.

Nächste Schritte

Weitere Informationen zur Fehlerbehebung bei Festplattenlatenz finden Sie unter [Festplattenlatenzprobleme](#).

Weitere Informationen zu Protokollmeldungen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

Festplattenlatenzprobleme

Die Controller müssen auf Festplatten mit geringer Latenz betrieben werden. Für den Cluster ist erforderlich, dass das Festplattenspeichersystem für jeden Knoten eine Spitzenschreiblatenz von weniger als 300 ms und eine durchschnittliche Schreiblatenz von weniger als 100 ms aufweist.

Problem

- Ein bereitgestellter NSX Controller wird von einem Controller-Cluster getrennt.
- Es können keine Controller-Protokolle gesammelt werden, weil die Festplattenpartition voll ist.
- Erfüllt das Speichersystem diesen Anforderungen nicht, kann der Cluster instabil werden und zu einem Systemausfall führen.
- TCP-Listeners für einen funktionierenden NSX Controller erscheinen nicht mehr in der Ausgabe des Befehls `show network connections of-type tcp`.
- Der abgetrennte Controller versucht, dem Cluster mit einer UUID aus lauter Nullen beizutreten, was nicht gültig ist.

- Der Befehl "show control-cluster history" zeigt eine ähnliche Nachricht an wie:

```
INFO.20150530-000550.1774:D0530 13:25:29.452639 1983 zookeeper_client.cc:774] Zookeeper
client disconnected!
```

- Das Ausführen des Befehls `show log cloudnet/cloudnet_java-zookeeper*.log` in der NSX Controller-Konsole enthält ähnliche Einträge wie:

```
cloudnet_java-zookeeper.20150530-000550.1806.log-2015-05-30
13:25:07,382 47956539 [SyncThread:1] WARN
org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead
log in SyncThread:1 took 3219ms which will adversely effect operation latency.
See the ZooKeeper troubleshooting guide
```

- Das NSX Controller-Protokoll enthält ähnliche Einträge wie:

```
D0525 13:46:07.185200 31975
rpc-broker.cc:369] Registering address resolution for: 20.5.1.11:7777
D0525 13:46:07.185246 31975
rpc-tcp.cc:548] Handshake complete, both peers support the same
protocol
D0525 13:46:07.197654 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
D0525 13:46:07.222869 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
```

Ursache

Dieses Problem ist auf eine langsame Festplattenleistung zurückzuführen, die sich negativ auf den NSX Controller-Cluster auswirkt.

- Um langsame Festplatten zu ermitteln, suchen Sie nach *fsync*-Nachrichten in der `/var/log/cloudnet/cloudnet_java-zookeeper-Protokoll`datei. Wenn *fsync* länger als eine Sekunde

dauert, zeigt Zookeeper eine *fsync*-Warnmeldung an und es deutet darauf hin, dass die Festplatte zu langsam ist. VMware empfiehlt, speziell für den Controller-Cluster eine LUN (Logical Unit Number) zuzuweisen und/oder den Speicher-Array hinsichtlich der Latenzen näher an den Controller-Cluster zu verschieben.

- Sie können die Berechnungen der Lese- und Schreiblatenz anzeigen, die in einen gleitenden 5-Sekunden-Durchschnitt (standardmäßig) eingegeben werden, was wiederum eine Warnung auslöst, wenn der Latenzhöchstwert überschritten wird. Die Warnung wird abgeschaltet, wenn der Durchschnitt sich dem unteren Grenzwert nähert. Standardmäßig ist der Höchstwert auf 200 ms, der untere Grenzwert auf 100 ms eingestellt. Sie können den Befehl `show disk-latency-alert config` verwenden. Die Ausgabe wird wie folgt angezeigt:

```
enabled=True   low-wm=51       high-wm=150
nsx-controller # set disk-latency-alert enabled yes
nsx-controller # set disk-latency-alert low-wm 100
nsx-controller # set disk-latency-alert high-wm 200
```

- Mit der GET `/api/2.0/vdn/controller/<controller-id>/systemStats` REST API können Sie den Latenzwarnstatus der Controller-Knoten abrufen.
- Mit der GET `/api/2.0/vdn/controller` REST API können Sie anzeigen, ob eine Festplattenlatenz-Warnung auf einem Controller-Knoten erkannt wurde.

Lösung

- 1 Stellen Sie NSX Controller auf Festplatten mit geringer Latenz bereit.
- 2 Jeder Controller sollte einen eigenen Festplattenspeicher-Server nutzen. Verwenden Sie einen Festplattenspeicher-Server nicht für zwei Controller gleichzeitig.

Nächste Schritte

Weitere Informationen zum Anzeigen von Warnungen finden Sie unter [Festplattenlatenzwarnungen anzeigen](#).

NSX Controller-Cluster-Fehler

Wenn einer der NSX Controller-Knoten im Cluster ausfällt, verfügen Sie weiterhin über zwei Controller, die funktionieren. Die Clustermehrheit bleibt erhalten und die Steuerungskomponente funktioniert weiterhin.

Problem

Der NSX Controller-Cluster ist ausgefallen.

Lösung

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie unter **Networking & Security** auf **Installation > Verwaltung (Installation > Management)**.

- 3 Beobachten Sie im Bereich für die NSX Controller-Knoten die Spalte „Peers“. Werden in dieser Spalte grüne Kästchen angezeigt, liegt kein Fehler bei der Peer-Controller-Verbindung im Cluster vor. Ein rotes Kästchen weist auf einen Peer-Fehler hin. Klicken Sie auf das Kästchen, um detaillierte Informationen anzuzeigen.
- 4 Wenn die Spalte „Peers“ ein Problem im Controller-Cluster anzeigt, melden Sie sich bei der CLI jedes NSX Controller an, um eine genaue Diagnose durchzuführen. Führen Sie den Anzeigebefehl `control-cluster status` aus, um den Status jedes Controllers zu diagnostizieren. Alle Controller im Cluster müssen über dieselbe Cluster-UUID verfügen. Die Cluster-UUID entspricht möglicherweise jedoch nicht der UUID des Master-Controllers. Informationen zu Bereitstellungsproblemen finden Sie in der Beschreibung unter [Bereitstellungsprobleme von NSX Controller](#).
- 5 Sie können folgende Schritte zur Fehlerbehebung ausprobieren, bevor Sie den Controller-Knoten oder Controller-Cluster erneut bereitstellen:
 - a Überprüfen Sie, ob der Controller eingeschaltet ist.
 - b Versuchen Sie, zwischen dem betroffenen Controller und anderen Knoten sowie dem Manager Ping-Befehle zu senden, um die Netzwerkpfade zu überprüfen. Wenn Sie Netzwerkprobleme erkennen, beheben Sie sie wie unter [Bereitstellungsprobleme von NSX Controller](#) beschrieben.
 - c Überprüfen Sie den IPsec-Status (Internet Protocol Security) mit den folgenden Befehlen.
 - Überprüfen Sie mit dem Befehl `show control-cluster network ipsec status`, ob IPsec aktiviert ist.
 - Überprüfen Sie den Status der IPsec-Tunnel mit dem Befehl `show control-cluster network ipsec tunnels`.

Sie können auch die IPSec-Statusinformationen verwenden, um ein Ticket beim technischen Support von VMware zu öffnen.
 - d Wenn es sich bei dem Fehler nicht um ein Netzwerkproblem handelt, können Sie auswählen, ob Sie den Knoten neu starten oder erneut bereitstellen möchten.

Wenn Sie einen Knoten neu starten möchten, stellen Sie sicher, dass nur jeweils ein Controller neu gestartet wird. Wenn jedoch in einem Controller-Cluster bei mehr als einem Controller-Knoten ein Fehler auftritt, starten Sie alle Knoten gleichzeitig neu. Wenn Sie einen Knoten von einem fehlerfreien Cluster neu starten, überprüfen Sie anschließend immer, ob der Cluster neu formiert wird und die erneute Partitionierung („Resharding“) korrekt durchgeführt wurde.

- 6 Wenn Sie Controller erneut bereitstellen möchten, verwenden Sie einen der folgenden beiden Ansätze:
 - Ansatz 1: Löschen Sie den beschädigten Controller-Knoten und stellen Sie erneut einen neuen Controller-Knoten bereit.
 - Ansatz 2: Löschen Sie den Controller-Cluster und stellen Sie erneut einen neuen Controller-Cluster bereit.

VMware empfiehlt den zweiten Ansatz.

Nächste Schritte

Wählen Sie einen beliebigen Ansatz:

- [Ansatz 1: Löschen des beschädigten Controllers und erneutes Bereitstellen eines neuen Controllers](#)
- [Ansatz 2: Erneutes Bereitstellen eines NSX Controller-Clusters](#)

Ansatz 1: Löschen des beschädigten Controllers und erneutes Bereitstellen eines neuen Controllers

Sie können zunächst versuchen, das Problem zu beheben, ohne einen neuen NSX Controller-Cluster bereitzustellen. Bei diesem Ansatz löschen Sie zuerst den beschädigten NSX Controller-Knoten und stellen dann einen neuen NSX Controller-Knoten bereit.

Verfahren

1 [Einen NSX-Controller löschen](#)

Sie können einen NSX Controller gewaltsam oder vorsichtig löschen. Der Vorgang zum vorsichtigen Löschen überprüft die folgenden Bedingungen, bevor der Knoten entfernt wird:

2 [Einen NSX-Controller erneut bereitstellen](#)

Stellen Sie nach dem Löschen des beschädigten Controller-Knotens einen neuen Controller-Knoten bereit.

Einen NSX-Controller löschen

Sie können einen NSX Controller gewaltsam oder vorsichtig löschen. Der Vorgang zum vorsichtigen Löschen überprüft die folgenden Bedingungen, bevor der Knoten entfernt wird:

- Es liegt kein aktueller Upgrade-Vorgang für den NSX Controller-Knoten vor.
- Der Systemzustand des Controller-Clusters ist in Ordnung, und eine Controller-Cluster-API-Anforderung kann verarbeitet werden.
- Der Host-Status, wie er vom vCenter Server-Bestand entnommen wird, zeigt, dass der Host verbunden und eingeschaltet ist.
- Es handelt sich nicht um den letzten Controller-Knoten.

Bei der erzwungenen Löschung werden die oben genannten Bedingungen vor dem Entfernen des Controller-Knotens nicht überprüft.

- Wichtige Punkte beim Löschen von Controllern:
 - Versuchen Sie nicht, die Controller-VM zu löschen, bevor Sie den Controller über die Benutzeroberfläche oder die API von vSphere Web Client löschen. Wenn die Benutzeroberfläche nicht zielführend ist, löschen Sie den Controller mit der DELETE /2.0/vdn/controller/{controllerId}-API.
 - Stellen Sie nach dem Löschen eines Knotens sicher, dass der vorhandene Cluster stabil bleibt.

- Wenn alle Knoten eines Clusters gelöscht werden, müssen Sie den letzten vorhandenen Knoten mit der Option **Entfernen des Controllers erzwingen (Forcefully remove the controller)** löschen. Überprüfen Sie immer, ob die Controller-VM erfolgreich gelöscht wurde. Fahren Sie andernfalls die VM herunter, und löschen Sie die Controller-VM mithilfe der Benutzeroberfläche.
- Ein fehlgeschlagener Löschvorgang bedeutet, dass die VM nicht gelöscht werden konnte. Rufen Sie in diesem Fall das Löschen des Controllers über die Benutzeroberfläche auf. Verwenden Sie dazu die Option **Entfernen des Controllers erzwingen (Forcefully remove the controller)**. Setzen Sie den `forceRemoval`-Parameter für die API auf *wahr*. Fahren Sie die VM nach dem erzwungenen Entfernen herunter, und löschen Sie die Controller-VM mithilfe der Benutzeroberfläche.
- Da ein Cluster mit mehreren Knoten nur einen Fehler unterstützt, gilt das Löschen als Fehler. Der gelöschte Knoten muss erneut bereitgestellt werden, bevor ein weiterer Fehler auftritt.
- Bei einer Cross-vCenter NSX-Umgebung:
 - Das direkte Löschen oder Ausschalten der Controller-VM in vCenter Server wird nicht unterstützt. In der Spalte **Status** wird **Out of sync** (nicht synchron) angezeigt.
 - Wenn die Controller-Löschung nur zum Teil erfolgreich abgeschlossen wurde und in der NSX Manager-Datenbank in einer Cross-vCenter NSX-Umgebung ein Eintrag zurückbleibt, verwenden Sie die `DELETE api/2.0/vdn/controller/external-API`.
 - Wenn der Controller über die NSX Manager-API importiert wurde, nutzen Sie die `removeExternalControllerReference`-API mit der `forceRemoval`-Option.
 - Beim Löschen eines Controllers fordert NSX das Löschen einer Controller-VM über vCenter Server mithilfe der ID für ein verwaltetes Objekt (Managed Object ID, MOID) der virtuellen Maschine an. Wenn vCenter Server die VM nicht über die MOID ermitteln kann, meldet NSX einen Fehler für die Anforderung zum Löschen eines Controllers und bricht den Vorgang ab.

Wenn die Option **Löschen erzwingen (Forcefully Delete)** aktiviert ist, wird das Löschen des Controllers von NSX nicht abgebrochen und die Controller-Informationen werden gelöscht. NSX aktualisiert auch alle Hosts, um die Vertrauensstellung des gelöschten Controllers gegenüber den Hosts aufzuheben. Wenn allerdings die Controller-VM nach wie vor aktiv ist und mit einer anderen MOID ausgeführt wird, verfügt sie immer noch über Anmeldedaten, mit denen sie als Mitglied im Controller-Cluster agieren kann. In diesem Fall funktionieren alle logischen Switches oder Router, die diesem Controller-Knoten zugewiesen sind, nicht mehr ordnungsgemäß, da die ESXi-Hosts den gelöschten Controller nicht mehr als vertrauenswürdig behandeln.

Um den NSX Controller zu löschen, führen Sie den folgenden Vorgang durch:

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
- 3 Wählen Sie unter **Management** den Controller aus, den Sie löschen möchten.
- 4 Klicken Sie auf das Symbol **(x) löschen (Delete (x))**.

5 Wählen Sie **Löschen (Delete)** oder **Löschen erzwingen (Forcefully Delete)** aus.

- ◆ Wenn Sie die Option **Löschen erzwingen (Forcefully Delete)** auswählen, wird das Löschen des Controllers erzwungen, und die Löschung erfolgt nicht ordnungsgemäß. Bei dieser Option werden also alle Fehler ignoriert und sämtliche Daten von der Datenbank entfernt. Daher sollten Sie sicherstellen, dass alle etwaigen Fehler manuell behoben werden. Sie müssen bestätigen, dass die Controller-VM erfolgreich gelöscht wurde. Falls dies nicht der Fall ist, müssen Sie sie über vCenter Server löschen.

Hinweis Wenn Sie den letzten Controller im Cluster löschen, müssen Sie die Option **Löschen erzwingen (Forcefully Delete)** aktivieren, um den letzten Controller-Knoten zu entfernen. Wenn sich keine Controller im System befinden, werden die Hosts im „Headless“-Modus betrieben. Bei neuen VMs oder VMs mit vMotion treten Netzwerkprobleme auf, es sei denn, neue Controller werden bereitgestellt und die Synchronisierung ist abgeschlossen.

- ◆ Wenn Sie diese nicht aktivieren, wird der Controller vorsichtig gelöscht.

6 Klicken Sie auf **Ja (Yes)**. Die vorsichtige Controller-Löschung nutzt die folgende Sequenz:

- a Der Knoten wird ausgeschaltet.
- b Der Systemzustand des Clusters wird überprüft.
- c Wenn der Zustand des Clusters nicht in Ordnung ist, wird der Controller eingeschaltet und die Löschanforderung abgelehnt.
- d Wenn der Zustand des Clusters in Ordnung ist, wird die Controller-VM entfernt und die IP-Adresse des Knotens freigegeben.
- e Die ID der Controller-VM wird aus dem Cluster entfernt.

Der ausgewählte Controller wird gelöscht.

7 Führen Sie eine Neusynchronisierung des Controller-Zustands durch, indem Sie auf **Aktionen > Controllerstatus aktualisieren (Actions > Update Controller State)** klicken.

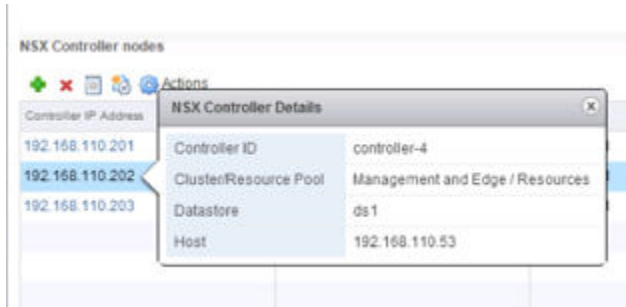
Einen NSX-Controller erneut bereitstellen

Stellen Sie nach dem Löschen des beschädigten Controller-Knotens einen neuen Controller-Knoten bereit.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie unter **Networking & Security** auf **Installation > Verwaltung (Installation > Management)**.
- 3 Klicken Sie im Abschnitt **NSX Controller-Knoten** auf den betroffenen Controller. Erstellen Sie Screenshots oder notieren Sie sich die Konfigurationsinformationen auf dem Bildschirm **Details zum NSX Controller** zur späteren Referenz.

Beispiel:



- 4 Um einen neuen NSX Controller-Knoten bereitzustellen, klicken Sie auf das Symbol **Knoten hinzufügen (+) (Add Node (+))**.
- 5 Wählen Sie im Dialogfeld „Controller hinzufügen“ das Datacenter aus, zu dem Sie den Knoten hinzufügen, und konfigurieren Sie die Controller-Einstellungen.
 - a Wählen Sie den entsprechenden Cluster aus.
 - b Wählen Sie einen Host im Cluster und Speicher aus.
 - c Wählen Sie die verteilte Portgruppe aus.
 - d Wählen Sie den IP-Pool aus, aus dem IP-Adressen dem Knoten zugewiesen werden sollen.
 - e Klicken Sie auf **OK**, warten Sie, bis die Installation abgeschlossen ist, und stellen Sie sicher, dass der Knoten über den Status **Normal** verfügt.

Detaillierte Informationen zum Hinzufügen eines Controller-Knotens finden Sie unter „Bereitstellen des NSX Controller-Clusters“ im *Installationshandbuch für NSX*.

- 6 Führen Sie eine Neusynchronisierung des Controller-Zustands durch, indem Sie auf **Aktionen > Controllerstatus aktualisieren** klicken.

Die Option „Controller-Zustand aktualisieren“ schiebt die Konfiguration von VXLAN und dem Distributed Logical Router (einschließlich der Universalobjekte in einer Cross-vCenter NSX-Bereitstellung) vom NSX Manager zum Controller-Cluster.

Ansatz 2: Erneutes Bereitstellen eines NSX Controller-Clusters

Löschen Sie bei diesem Ansatz alle drei Controller-Knoten und fügen Sie neue Controller-Knoten hinzu, um einen voll funktionsfähigen Cluster mit drei Knoten beizubehalten.

VMware empfiehlt, den NSX Controller-Cluster zu löschen, wenn eine der folgenden Bedingungen zutrifft:

- Auf mindestens einem Controller-Knoten ist ein schwerwiegender oder nicht behebbarer Fehler aufgetreten.
- Auf die Controller-VMs kann nicht zugegriffen werden und sie können nicht repariert werden.

In solchen Fällen sollten Sie vorzugsweise alle Controller-Knoten löschen, selbst wenn einige Controller-Knoten fehlerfrei erscheinen.

Stellen Sie erneut einen neuen Controller-Cluster bereit und aktualisieren Sie dann den Controller-Zustandsmechanismus im NSX Manager. Das Aktualisieren des Controller-Zustands hat eine Neusynchronisierung von VXLAN und eine erneute Bereitstellung der Distributed Logical Routers zur Folge.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Navigieren Sie zu **Netzwerk und Sicherheit > Installation > Management**.
- 3 Löschen Sie im Abschnitt **NSX Controller-Knoten** alle drei Controller-Knoten. Wählen Sie jeden Knoten einzeln aus und klicken Sie auf das Symbol **Löschen** (✖).

Wenn im System keine Controller vorhanden sind, werden die Hosts im Modus „Monitorlos“ ausgeführt. Bei neuen oder migrierten virtuellen Maschinen treten Netzwerkprobleme auf, bis neue Controller bereitgestellt sind und die Synchronisierung abgeschlossen ist.

- 4 Stellen Sie drei neue Controller-Knoten bereit, um einen voll funktionsfähigen NSX Controller-Cluster zu erstellen.

Detaillierte Informationen zum Hinzufügen eines Controller-Clusters finden Sie unter „Bereitstellen des NSX Controller-Clusters“ im *Installationshandbuch für NSX*.

- 5 Führen Sie eine Neusynchronisierung des Controller-Zustands durch, indem Sie auf **Aktionen > Controllerstatus aktualisieren** klicken.

Phantom-Controller

Bei einem Phantom-Controller kann es sich um eine Live-Controller-VM oder eine nicht vorhandene VM handeln, die am Cluster beteiligt ist oder nicht. NSX Manager synchronisiert die Liste aller VMs aus der vCenter Server-Bestandsliste. Ein Phantom-Controller wird erstellt, wenn vCenter Server oder der Host eine Controller-VM ohne Anforderung von NSX Manager löscht oder wenn die vCenter Server-Bestandsliste die Referenz-MOID der Controller-VMs ändert.

Wenn ein Controller von NSX erstellt wird, werden die Konfigurationsinformationen in NSX Manager gespeichert. NSX Manager stellt die neue Controller-VM über vCenter Server bereit.

Der NSX-Administrator stellt die Konfiguration, darunter auch den IP-Adressenpool, für NSX Manager bereit, um einen Controller zu erstellen. NSX Manager entfernt eine IP-Adresse aus dem Pool und überträgt diese IP mit dem Rest der Controller-Konfiguration als VM-Erstellungsanforderung an vCenter Server. NSX Manager wartet darauf, dass vCenter Server den Status der Anforderung bestätigt.

- The controller creation process was successful: Wenn die Controller-VM erfolgreich erstellt wurde, startet vCenter Server die Controller-VM. NSX Manager speichert die Managed Object ID (ID für ein verwaltetes Objekt, MOID) der virtuellen Maschine mit dem Rest der Konfigurationsinformationen des Controllers. Bei der MOID (oder MO-REF) handelt es sich um einen eindeutigen Bezeichner, den vCenter allen Objekten seiner Bestandsliste zuweist. vCenter Server verwendet diese MOID auch, um die VM zu überwachen, wenn sie Teil der vCenter Server-Bestandsliste bleibt.

- The controller creation process was not successful: Wenn IP- und Netzwerkverbindungskonfigurationen fehlerhaft waren, kann NSX ManagervCenter Server möglicherweise nicht kontaktieren. NSX Manager wartet für einen vordefinierten Zeitraum, um einen Einzelknoten-Controller-Cluster (für den ersten) oder einen neuen Controller für einen Beitritt zum aktiven Cluster zu erstellen. Wenn der Timer abläuft, übermittelt NSX Manager eine Anforderung an vCenter Server, die VM zu löschen. Die IP-Adresse wird an den Pool zurückgegeben, und NSX erklärt die Erstellung des Controllers für gescheitert.

Entstehung von Phantom-Controllern

Wenn NSX Manager die Löschung eines Controllers anfordert, ermittelt vCenter Server die Controller-VM für die Löschung mithilfe der MOID.

Doch wenn beliebige vCenter-Aktivitäten die Entfernung der Controller-VM aus der vCenter Server-Bestandsliste zur Folge haben, entfernt vCenter die MOID aus seiner Datenbank. Beachten Sie, dass die Controller-VM nach wie vor auf NSX Manager vorhanden und aktiv sein kann, auch wenn sie aus der vCenter-Bestandsliste entfernt wurde. Doch für vCenter Server ist die Controller-VM nicht mehr vorhanden. Obwohl die VM aus der Bestandsliste von vCenter Server entfernt wurde, wurde die VM möglicherweise nicht gelöscht. Wenn die VM noch aktiv ist, ist sie noch am Controller-Cluster von NSX beteiligt oder versucht, sich daran zu beteiligen.

In den folgenden Fällen kommt es besonders häufig zur Entstehung von Phantom-Controllern:

- Der Administrator von vCenter Server entfernt den Host, der die Controller-VM aus der Bestandsliste enthält. Später fügt er den Host wieder hinzu. Wenn der Host entfernt wird, löscht vCenter Server alle dem Host und den darin enthaltenen VMs zugeordneten MOIDs. Wenn der Host später wieder hinzugefügt wird, weist vCenter Server dem Host und den VMs eine ganz neue MOID zu. Für die Benutzer von NSX erscheinen Host und VMs unverändert, doch für vCenter Server sind Host und VMs ganz neue Objekte. In der Praxis können Host und VMs jedoch unverändert genutzt werden. Die Anwendungen, die auf Host und VMs ausgeführt werden, ändern sich nicht.
- Der Administrator von vCenter Server löscht die Controller-VM über vCenter Server oder unter Verwendung der Hostverwaltung. Die Löschung wurde nicht von NSX Manager initiiert.
- *Löschen* umfasst in diesem Fall auch alle Host-/Speicherfehler, die zum Verlust der VM führen. In diesem Fall geht die VM für vCenter Server und auch für den Cluster und NSX Manager verloren. Doch weil die Löschung nicht von NSX Manager initiiert wurde, gehen sowohl NSX Manager und der Controller-Cluster davon aus, dass der Controller nach wie vor gültig ist. Der an NSX Manager zurückgegebene Controller-Status besagt, dass dieser Controller-Knoten ausgefallen ist und nicht Teil des Clusters ist. Es erfolgt keine Anzeige in der Benutzeroberfläche. NSX Manager verfügt auch über Protokolle, denen entnommen werden kann, dass der Controller nicht mehr erreichbar ist.

Vorgehen bei Ermitteln eines Phantom-Controllers

- 1 Führen Sie eine Synchronisierung durch, wie unter [NSX Controller ist getrennt](#) beschrieben.

- 2 Sehen Sie sich die Protokolleinträge an. Wenn die Controller-VM versehentlich gelöscht oder beschädigt wurde, müssen Sie die Option **Löschen erzwingen (Forcefully Delete)** verwenden, um den Eintrag aus der Datenbank von NSX Manager zu löschen. Einzelheiten dazu finden Sie unter [Einen NSX-Controller löschen](#).
- 3 Stellen Sie nach dem Löschen des Controllers Folgendes sicher:
 - Die Controller-VM ist tatsächlich gelöscht.
 - Der Befehl `show controller-cluster startup-nodes` zeigt nur gültige Controller.
 - Die syslog-Einträge für NSX Manager zeigen keinen zusätzlichen Controller mehr.

Ab NSX 6.2.7 oder höher überprüft NSX Manager die vCenter-Bestandsliste, um sicherzustellen, dass die Controller-VM noch in der Bestandsliste vorhanden ist. Dies geschieht auf Basis der ursprünglichen MOID. Wenn NSX Manager die Controller-VM nicht in der Bestandsliste finden kann, sucht NSX Manager die VM mithilfe der Instanz-UUID der VM. Die Instanz-UUID ist in der VM gespeichert. Sie ändert sich also auch dann nicht, wenn die VM wieder zur vCenter-Bestandsliste hinzugefügt wird. Wenn NSX Manager die VM mit der Instanz-UUID finden kann, nimmt NSX Manager die neue MOID in seine Datenbank auf.

Wenn Sie die Controller-VM klonen, hat die geklonte VM jedoch dieselben Eigenschaften wie die ursprüngliche VM, sowie eine neue Instanz-UUID. NSX Manager kann die MOID für die geklonte VM nicht erkennen.

Protokolleinträge für Phantom-Controller

Der folgende Protokolleintrag auf Fehlerstufe wird angezeigt, wenn ein Phantom-Controller erkannt wird:

- 2017-07-31 22:15:05.844 UTC ERROR NVPStatusCheck ControllerServiceImpl:2146 – Controller <#> does not exist, might be deleted already. Skip saving its connectivity info.
- 2017-07-31 22:15:05.769 UTC ERROR NVPStatusCheck ControllerServiceImpl:2580 – the node is created by this NSX Manager <#>, but database has no record and delete might be in progress.

NSX Controller ist getrennt

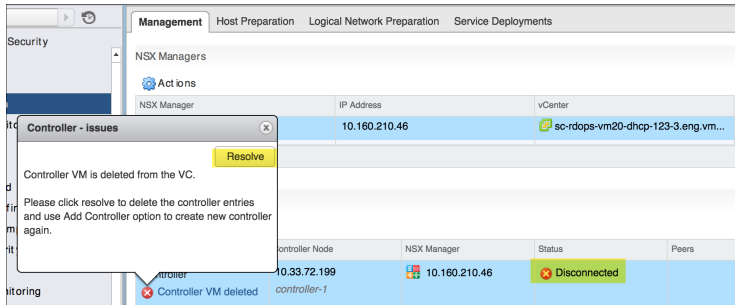
Wenn die NSX Controller-VM über einen vCenter Server ausgeschaltet oder eine Controller-VM vom vCenter Server gelöscht wurde, zeigt die Spalte **Status** der Seite **Installation > Management** den Status **Out of sync** (nicht synchron) an.

Voraussetzungen

Controller-VM ausgeschaltet oder Controller-VM vom vCenter Server gelöscht.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Installation > Management**.



- 2 Klicken Sie auf den Link **Fehler (Error)**, um detaillierte Angaben zu der fehlenden Synchronisierung einzusehen.
- 3 Klicken Sie auf die Schaltfläche **Beheben (Resolve)**, um den Fehler zu beheben.

Ergebnisse

Wenn die Controller-VM ausgeschaltet wird, löst die Managementebene einen power on-Befehl für den Controller aus.

Wenn eine Controller-VM gelöscht wird, werden die Einträge des Controllers von der Managementebene gelöscht und die Managementebene meldet die Controller-Löschung an die zentrale Kontrollebene.

Nächste Schritte

Erstellen Sie mit der Option **Knoten hinzufügen (Add Node)** einen neuen Controller. Genauere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Probleme mit dem Agenten der Kontrollebene (netcpa)

Bei NSX für vSphere dient die Kontrollebene (netcpa) als lokaler Agentendaemon, der mit NSX Manager und dem Controller-Cluster kommuniziert. Die Funktion **Kommunikationskanalstatus (Communication Channel Health)** ist eine proaktive Überprüfung des Systemzustands, die in regelmäßigen Abständen den Zustand der zentralen bis zur lokalen Kontrollebene an den NSX Manager meldet und die in der Benutzeroberfläche von NSX Manager angezeigt wird. Dieser Bericht dient auch als Taktsignal, um den Betriebszustand des NSX Manager zum ESXi-Host-netcpa-Kanal zu erkennen. Er bietet Fehlerdetails bei Kommunikationsfehlern, generiert ein Ereignis, wenn ein Kanal in den falschen Status verfällt, und erstellt außerdem Taktsignalnachrichten vom NSX Manager zu Hosts.

Problem

Konnektivitätsprobleme zwischen Steuerungsebenen-Agent und Controller.

Ursache

Wenn eine Verbindung ausfällt, funktioniert der Steuerungsebenen-Agent möglicherweise nicht korrekt.

Lösung

- 1 Wenn der Kanal in einen fehlerhaften Status wechselt, überprüfen Sie den Verbindungsstatus mit folgendem Befehl:

```
GET https://<NSX_Manager_IP>/api/2.0/vdn/inventory/host/{hostId}/connection/status
```

Nachfolgend finden Sie ein Beispiel für den zurückgegebenen Code:

```
<?xml version="1.0" encoding="UTF-8"?>
<hostConnStatus>
<hostName>10.161.246.20</hostName>
<hostId>host-21</hostId>
<nsxMgrToFirewallAgentConn>UP</nsxMgrToFirewallAgentConn>
<nsxMgrToControlPlaneAgentConn>UP</nsxMgrToControlPlaneAgentConn>
<hostToControllerConn>DOWN</hostToControllerConn>
<fullSyncCount>-1</fullSyncCount>
<hostToControllerConnectionErrors>
<hostToControllerConnectionError>
<controllerIp>10.160.203.236</controllerIp>
<errorCode>1255604</errorCode>
<errorMessage>Connection Refused</errorMessage>
</hostToControllerConnectionError>
<hostToControllerConnectionError>
<controllerIp>10.160.203.237</controllerIp>
<errorCode>1255603</errorCode>
<errorMessage>SSL Handshake Failure</errorMessage>
</hostToControllerConnectionError>
</hostToControllerConnectionErrors>
</hostConnStatus>
```

Die folgenden Fehlercodes werden unterstützt:

1255602: Unvollständiges Controller-Zertifikat 1255603: SSL-Handshake-Fehler 1255604: Verbindung abgelehnt. 1255605: Keep-alive-Zeitüberschreitung 1255606: SSL-Ausnahme 1255607: Ungültige Meldung 1255620: Unbekannter Fehler

- 2 Ermitteln Sie den Grund für den Ausfall des Steuerungsebenen-Agenten wie folgt:
 - a Überprüfen Sie durch Ausführung des Befehls `/etc/init.d/netcpad status` auf den ESXi-Hosts den Status des Steuerungsebenen-Agenten auf den Hosts.

```
[root@esx-01a:~] /etc/init.d/netcpad status
netCP agent service is running
```

- b Überprüfen Sie die Konfigurationen des Steuerungsebenen-Agenten mithilfe des Befehls `more /etc/vmware/netcpa/config-by-vsm.xml`. Es müssen die IP-Adressen der NSX Controller aufgeführt sein.

```
[root@esx-01a:~] more /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
```

```

<connection id="0000">
  <port>1234</port>
  <server>192.168.110.31</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>A5:C6:A2:B2:57:97:36:F0:7C:13:DB:64:9B:86:E6:EF:1A:7E:5C:36</thumbprint>
</connection>
<connection id="0001">
  <port>1234</port>
  <server>192.168.110.32</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>12:E0:25:B2:E0:35:D7:84:90:71:CF:C7:53:97:FD:96:EE:ED:7C:DD</thumbprint>
</connection>
<connection id="0002">
  <port>1234</port>
  <server>192.168.110.33</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>BD:DB:BA:B0:DC:61:AD:94:C6:0F:7E:F5:80:19:44:51:BA:90:2C:8D</thumbprint>
</connection>
</connectionList>
...

```

- 3 Überprüfen Sie mit folgendem Befehl die Verbindungen zwischen den Controllern und dem Steuerungsebenen-Agenten. Die Ausgabe ist eine Verbindung für jeden Controller.

```

>[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp      0  0  192.168.110.51:16594      192.168.110.31:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:46917      192.168.110.33:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0  0  192.168.110.51:47891      192.168.110.32:1234      ESTABLISHED      36752  newreno
netcpa-worker

```

- 4 Überprüfen Sie mit folgendem Befehl, ob die Verbindungen zwischen den Controllern und dem Steuerungsebenen-Agenten den Status CLOSED oder CLOSE_WAIT aufweisen:

```

esxcli network ip
  connection list |grep "1234.*netcpa*" | egrep "CLOSED|CLOSE_WAIT"

```

- 5 Falls der Steuerungsebenen-Agent bereits länger ausgefallen war, sind die Verbindungen möglicherweise gar nicht vorhanden. Um dies zu überprüfen, führen Sie folgenden Befehl aus. Die Ausgabe ist eine Verbindung für jeden Controller.

```

esxcli network ip
  connection list |grep "1234.*netcpa*" |grep ESTABLISHED

```


- 6** Mechanismus zur automatischen Wiederherstellung des Steuerungsebenen-Agenten (netcpa): Der Prozess zur automatischen Überwachung des Steuerebenen-Agenten erkennt, dass der Steuerungsebenen-Agent einen fehlerhaften Status aufweist. Wenn der Steuerungsebenen-Agent einen fehlerhaften Status aufweist, reagiert er nicht mehr und versucht dann automatisch, eine Wiederherstellung durchzuführen.

- a Wenn der Steuerungsebenen-Agent nicht mehr reagiert, wird eine Live-Core-Datei generiert. Sie finden die Core-Datei wie folgt:

```
ls /var/core
netcpa-worker-zdump.000
```

- b Syslog-Fehler werden in der Datei *vmkwarning.log* gemeldet.

```
cat /var/run/log/vmkwarning.log | grep NETCPA
2017-08-11T06:32:17.994Z cpu1:1000044539)ALERT: Critical - NETCPA is hanged
Taking live-dump & restarting netcpa process!
```

Hinweis Wenn bei der Überwachung des Steuerungsebenen-Agenten aufgrund einer verspäteten Antwort auf die Statusüberprüfung ein temporärer Fehler auftritt, wird in den VMKernel-Protokollen möglicherweise eine Warnmeldung wie unten angezeigt.

```
Warning - NETCPA getting netcpa status failed!
```

Sie können diese Warnung ignorieren.

- 7** Wenn keine automatische Wiederherstellung erfolgt, starten Sie den Steuerungsebenen-Agenten wie folgt neu:
- a Melden Sie sich über SSH oder die Konsole als Root beim ESXi-Host an.
 - b Führen Sie den Befehl `/etc/init.d/netcpad restart` aus, um den Steuerungsebenen-Agenten auf dem ESXi-Host neu zu starten.

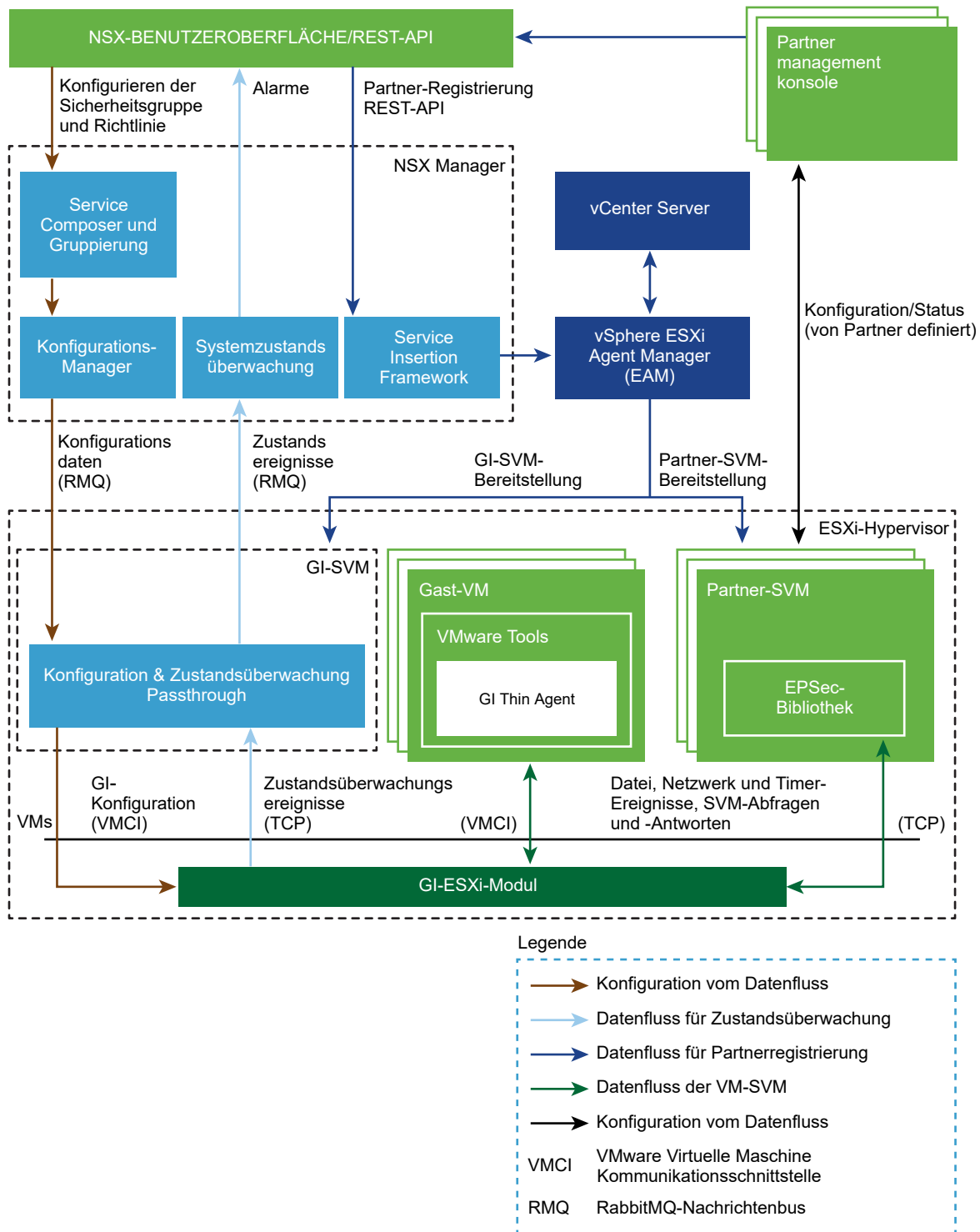
Fehlerbehebung bei Guest Introspection

9

Dieses Kapitel enthält die folgenden Themen:

- [Guest Introspection-Architektur](#)
- [Guest Introspection-Protokolle](#)
- [Erfassen von Details zur Guest Introspection-Umgebung und -Arbeit](#)
- [Fehlerbehebung beim Thin-Agent unter Linux oder Windows](#)
- [Fehlerbehebung beim ESX-GI-Modul \(MUX\)](#)
- [Fehlerbehebung bei EPSecLib](#)

Guest Introspection-Architektur



Guest Introspection-Protokolle

Es gibt verschiedene Protokolle, die Sie erfassen können, um sie bei der Fehlerbehebung für Guest Introspection zu verwenden.

Protokolle des ESX-GI-Moduls (MUX)

Wenn virtuelle Maschinen auf einem ESXi-Host nicht mit Guest Introspection funktionieren oder wenn auf einem Host hinsichtlich der Kommunikation mit der SVA Alarme ausgelöst werden, liegt möglicherweise ein Problem beim ESX-GI-Modul auf dem ESXi-Host vor.

Protokollpfad und Beispielmeldung

MUX-Protokollpfad

/var/log/syslog

var/run/syslog.log

Meldungen des ESX-GI-Moduls (MUX) weisen das Format <Zeitstempel>EPSecMUX<[ThreadID]>: <Meldung> auf.

Beispiel:

```
2017-07-16T05:44:49Z EPSecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

Im obigen Beispiel:

- [ERROR] ist die Art der Benachrichtigung. Andere mögliche Typen sind [DEBUG] oder [INFO].
- (EPSEC) gibt an, dass die Nachrichten zur Endpoint-Sicherheit gehören.

Protokolldateien aktivieren und anzeigen

Um die auf dem Host installierte Version des ESX-GI-Modul-VIBs anzuzeigen, führen Sie den Befehl `#esxcli software vib list | grep epsec-mux` aus.

Um die vollständige Protokollierung zu aktivieren, führen Sie diese Schritte in der Eingabeaufforderung des ESXi-Hosts aus.

- 1 Führen Sie den Befehl „`ps -c | grep Mux`“ aus, um die ESX-GI-Modulprozesse anzuzeigen, die gerade ausgeführt werden.

Beispiel:

```
~ # ps -c | grep Mux
192223 192223 sh /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

- 2 Wenn der Dienst nicht ausgeführt wird, können Sie ihn mit diesen Befehlen erneut starten: `/etc/init.d/vShield-Endpoint-Mux start` oder `/etc//init.d/vShield-Endpoint-Mux restart`.
- 3 Um die ESX-GI-Modulprozesse, die gerade ausgeführt werden, anzuhalten, darunter auch den `watchdog.sh`-Prozess, führen Sie den Befehl `~ # kill -9 192223 192233 192236` aus.

Beachten Sie, dass zwei ESX-GI-Modulprozesse erzeugt werden.

- 4 Starten Sie ein ESX-GI-Modul mit einer neuen Option -d. Beachten Sie, dass die Option „-d“ für die EPSec-MUX-Builds 5.1.0-01255202 und 5.1.0-01814505 ~ # /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910 nicht vorhanden ist.
- 5 Zeigen Sie die Protokollnachrichten des ESX GI-Moduls in der Datei /var/log/syslog.log auf dem ESXi-Host an. Überprüfen Sie, ob die Einträge zu globalen Lösungen, zur Lösungs-ID und zur Portnummer korrekt sind.

Beispiel: Muxconfig.xml-Beispieldatei

```
<?xml version="1.0" encoding="UTF-8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService (216).vmx</
vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-alpha-01.vmx</
vmxPath>

    </Solution>

    <Solution>

      <id>6341068275337723904</id>
```

```

    <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

    <listenOn>ip</listenOn>

    <port>48655</port>

    <uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>

    <vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>

  </Solution>
</InstalledSolutions>

<DefaultSolutions/>

<GlobalSolutions>

  <solution>

    <id>100</id>

    <tag></tag>

    <order>0</order>

  </solution>

  <solution>

    <id>102</id>

    <tag></tag>

    <order>10000</order>

  </solution>

  <solution>

    <id>6341068275337723904</id>

    <tag></tag>

    <order>10001</order>

  </solution>
</GlobalSolutions>

</EndpointConfig>

```

GI Thin Agent-Protokolle

Der Thin Agent ist auf dem VM-Gastbetriebssystem installiert und erkennt Anmeldedetails von Benutzern.

Protokollpfad und Beispielmeldung

Der Thin Agent besteht aus GI-Treibern – vsepflt.sys, vnetflt.sys und vnetwfp.sys (Windows 10 und höher).

Die Thin Agent-Protokolle befinden sich als Teil des vCenter-Protokollpakets auf dem ESXi-Host. Der Protokollpfad lautet `/vmfs/volumes/<datastore>/<vmname>/vmware.log`. Zum Beispiel: `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Thin Agent-Meldungen weisen folgendes Format auf: `<Zeitstempel> <VM name=""><Process name=""><[PID]>: <Meldung>.</[PID]>`

Im Beispielprotokoll unter `Guest: vnet` oder `Guest:vsep` werden Protokollmeldungen für die jeweiligen GI-Treiber angegeben, gefolgt von Debugging-Meldungen.

Beispiel:

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

Beispiel: Aktivieren der vShield Guest Introspection Thin Agent-Treiber-Protokollierung

Weil die Debugging-Einstellung die Datei `vmware.log` so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Für dieses Verfahren müssen Sie die Windows-Registry ändern. Bevor Sie die Registry ändern, erstellen Sie eine Sicherungskopie. Weitere Informationen zum Sichern und Wiederherstellen der Registry finden Sie im Microsoft Knowledgebase-Artikel [136393](#).

So aktivieren Sie die Debugging-Protokollierung für den Thin Agent-Treiber:

- 1 Klicken Sie auf **Start > Ausführen (Start > Run)**. Geben Sie „regedit“ ein und klicken Sie auf **OK**. Die Registry-Editor-Fenster wird geöffnet. Weitere Informationen finden Sie im Microsoft Knowledgebase-Artikel [256986](#).

- 2 Erstellen Sie mit dem Registry-Editor diesen Schlüssel: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt\parameters.
- 3 Erstellen Sie unter dem neu erstellten Parameterschlüssel diese DWORDs. Stellen Sie sicher, dass hexadezimal ausgewählt ist, wenn Sie diese Werten eingeben:

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

Andere Werte für den log_level-Parameterschlüssel:

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

- 4 Öffnen Sie eine Eingabeaufforderung als Administrator. Führen Sie diese Befehle aus, um das Laden Minitreiber des vShield Endpoint-Dateisystems zu beenden und ihn dann erneut zu laden:

- fltmc unload vsepflt
- fltmc load vsepflt

Sie finden die Protokolleinträge in der vmware.log-Datei, die sich auf der virtuellen Maschine befindet.

Aktivieren der vShield GI Netzwerktreiber-Protokollierung

Weil die Debugging-Einstellung die Datei vmware.log so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Für dieses Verfahren müssen Sie die Windows-Registry ändern. Bevor Sie die Registry ändern, erstellen Sie eine Sicherungskopie. Weitere Informationen zum Sichern und Wiederherstellen der Registry finden Sie im Microsoft Knowledgebase-Artikel [136393](#).

- 1 Klicken Sie auf **Start > Ausführen (Start > Run)**. Geben Sie „regedit“ ein und klicken Sie auf **OK**. Die Registry-Editor-Fenster wird geöffnet. Weitere Informationen finden Sie im Microsoft Knowledgebase-Artikel [256986](#).
- 2 So bearbeiten Sie die Registry:

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest" = DWORD: 0x00000001
```

- 3 Starten Sie die virtuelle Maschine neu.

Speicherort der Protokolldateien vsepflt.sys und vnetflt.sys

Mit den log_dest-Registry-Einstellungen DWORD: 0x00000001 meldet sich der Endpoint Thin Agent-Treiber beim Debugger an. Führen Sie den Debugger (DbgView von SysInternals oder windbg) aus, um die Debugging-Ausgabe zu erfassen.

Alternativ können Sie die log_dest-Registry-Einstellung auf DWORD:0x000000002 festlegen. Dann werden die Treiberprotokolle in der Datei vmware.log ausgegeben, die sich im entsprechenden VM-Ordner auf dem ESXi-Host befindet.

Aktivieren der UMC-Protokollierung

Die Benutzermodus-Komponente (UMC) von Guest Introspection wird im VMware Tools-Dienst in der geschützten virtuellen Maschine ausgeführt.

- 1 Erstellen Sie unter Windows XP und Windows Server 2003 eine Tools-Config-Datei, wenn unter folgendem Pfad keine vorhanden ist: C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware Tools\tools.conf.
- 2 Erstellen Sie unter Windows Vista, Windows 7 und Windows Server 2008 eine Tools-Config-Datei, wenn unter folgendem Pfad keine vorhanden ist: C:\ProgramData\VMware\VMware Tools\tools.conf
- 3 Fügen Sie diese Zeilen in der Datei tools.conf, um die UMC-Komponentenprotokollierung zu aktivieren.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

Mit der Einstellung vsep.handler = vmx werden die Protokolle der UMC-Komponente in der Datei vmware.log ausgegeben, die sich im entsprechenden VM-Ordner auf dem ESXi-Host befindet.

Mit den folgenden Einstellungsprotokollen werden die Protokolle der UMC-Komponente in der angegebenen Protokolldatei ausgegeben.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

GI-EPSecLib- und SVM-Protokolle

Die EPSecLib empfängt Ereignisse vom ESX-GI-Modul (MUX) des ESXi-Hosts.

Protokollpfad und Beispielmeldung

EPSecLib-Protokollpfad

/var/log/syslog

var/run/syslog

EPSecLib-Nachrichten weisen folgendes Format auf: <Zeitstempel> <VM Name><Process Name><[PID]>: <Meldung>

Im folgenden Beispiel ist [ERROR] der Nachrichtentyp und (EPSEC) steht für die Nachrichten, die sich auf Guest Introspection beziehen.

Beispiel:

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
[7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

Erfassen von Protokollen

So aktivieren Sie die Debugging-Protokollierung für die EPSec-Bibliothek, die eine Komponente der GI-SVM ist:

- 1 Melden Sie sich bei der GI-SVM mit dem Konsolenkennwort von NSX Manager an.
- 2 Erstellen Sie die Datei `/etc/epsec.lib.conf` und fügen Sie Folgendes hinzu:


```
ENABLE_DEBUG=TRUE

ENABLE_SUPPORT=TRUE
```
- 3 Ändern Sie die Berechtigungen, indem Sie den Befehl `chmod 644 /etc/epsec.lib.conf` ausführen.
- 4 Starten Sie den GI-SVM-Prozess neu, indem Sie den Befehl `/usr/local/sbin/rcusvm restart` ausführen.

Dies aktiviert die Debugging-Protokollierung für EPSecLib auf der GI-SVM. Die Debugging-Protokolle finden Sie im Verzeichnis `/var/log/messages` (gilt für NSX for vSphere 6.2.x und 6.3.x). Weil die Debugging-Einstellung die Datei `vmware.log` so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

GI-SVM-Protokolle

Bevor Sie Protokolle erfassen, legen Sie die Host-ID oder Host-MOID fest:

- Führen Sie die Befehle `show cluster all` und `show cluster <cluster ID>` in NSX Manager aus.

Beispiel:

```
nsxmgr-01a> show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	RegionA01-COMP01	domain-c26	RegionA01	Enabled
2	RegionA01-MGMT01	domain-c71	RegionA01	Enabled

```
nsxmgr-01a> show cluster domain-c26
```

```

Datacenter: RegionA01
Cluster: RegionA01-COMP01
No.  Host Name                Host Id                Installation Status
1     esx-01a.corp.local         host-29                Ready
2     esx-02a.corp.local         host-31                Ready

```

- 1 Um den aktuellen Protokollierungsstatus zu ermitteln, führen Sie diesen Befehl aus:

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm
```

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/root
```

- 2 Um den aktuellen Protokollierungsstatus zu ändern, führen Sie diesen Befehl aus:

```
POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel
```

```

## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>

```

- 3 Um Protokolle zu generieren, führen Sie diesen Befehl aus:

```
GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs
```

Wählen Sie Send und Download.

Beachten Sie, dass dieser Befehl GI-SVM-Protokolle generiert und die Datei als `techsupportlogs.log.gz`-Datei speichert. Weil die Debugging-Einstellung die Datei `vmware.log` so sehr überfüllen kann, dass es zu einer Drosselung kommt, empfehlen wir, den Debugging-Modus wieder zu deaktivieren, sobald Sie alle benötigten Daten erfasst haben.

Erfassen von Details zur Guest Introspection-Umgebung und -Arbeit

Das Erfassen von Umgebungsdetails ist für die Überprüfung der Kompatibilität von Komponenten hilfreich.

- 1 Ermitteln Sie, ob NSX Guest Introspection in der Kundenumgebung verwendet wird. Wenn dies nicht der Fall ist, entfernen Sie den Guest Introspection-Dienst von der virtuellen Maschine und bestätigen Sie, dass das Problem behoben wurde.

2 So erfassen Sie Umgebungsdetails:

- a ESXi-Build-Version – Führen Sie den Befehl `uname -a` auf dem ESXi-Host aus oder klicken Sie im vSphere Web Client auf einen Host und suchen Sie oben im rechten Bereich nach der Build-Nummer.
- b Linux-Produktversion und -Build-Nummer
- c Mit `/usr/sbin/vsep -v` können Sie die Produktversion abrufen.

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

3 VMware NSX® for vSphere® -Version und Folgendes:

- Name und Versionsnummer der Partnerlösung
 - Von der Partnerlösung genutzte Versionsnummer der EPsec-Bibliothek: Melden Sie sich bei der GI-SVM an und führen Sie `#strings path to EPsec library/libEPsec.so | grep BUILD` aus.
 - Gastbetriebssystem in der virtuellen Maschine
 - Jegliche anderen Anwendungen oder Dateisystemtreiber von Drittanbietern
- 4 Version des ESX GI-Moduls (MUX) – Führen Sie den Befehl `esxcli software vib list | grep epsec-mux` aus.
 - 5 Erfassen Sie Arbeitslastdetails, beispielsweise den Servertyp.
 - 6 Erfassen Sie ESXi-Hostprotokolle. Weitere Informationen finden Sie unter [Erfassen von Diagnosedaten für VMware ESX/ESXi \(653\)](#).
 - 7 Erfassen Sie Protokolle der virtuellen Dienst-Maschine (GI-SVM) von der Partnerlösung. Weitere Informationen zur Protokollerfassung für die GI-SVM erhalten Sie bei Ihrem Partner.
 - 8 Erfassen Sie eine Anhaltestatusdatei, während das Problem auftritt. Informationen zum Erfassen von Diagnosedaten finden Sie unter [Anhalten einer virtuelle Maschine auf ESX/ESXi \(2005831\)](#).
 - 9 Vergleichen Sie nach dem Erfassen der Daten die Kompatibilität der vSphere-Komponenten. Weitere Informationen finden Sie unter [VMware-Produktkompatibilitätsmatrix](#).

Fehlerbehebung beim Thin-Agent unter Linux oder Windows

Der Guest Introspection Thin Agent wird zusammen mit VMware Tools™ auf jeder Gast-VM installiert.

Fehlerbehebung beim Thin-Agent unter Linux

Wenn eine virtuelle Maschine bei Lese- oder Schreibvorgängen und beim Entpacken oder Speichern von Dateien langsam ist, liegen möglicherweise Probleme mit dem Thin Agent vor.

- 1 Überprüfen Sie die Kompatibilität der beteiligten Komponenten. Die Kompatibilität ist eines der größten Probleme bei Endpoint. Sie benötigen die Build-Nummern für ESXi, vCenter Server, NSX Manager und die von Ihnen verwendete Sicherheitslösung (Trend Micro, McAfee, Kaspersky, Symantec usw.). Wenn Ihnen diese Daten vorliegen, vergleichen Sie die Kompatibilität der vSphere-Komponenten. Weitere Informationen finden Sie unter [VMware-Produktkompatibilitätsmatrix](#).
- 2 Stellen Sie sicher, dass File Introspection auf dem System installiert ist.
- 3 Überprüfen Sie mit dem Befehl `service vsep status`, ob der Thin Agent ausgeführt wird. Nach Ausführung dieses Befehls sollten Sie sehen, dass der vsep-Dienst ausgeführt wird.
- 4 Wenn Sie der Meinung sind, dass der Thin Agent ein Leistungsproblem im System verursacht, halten Sie den Dienst mit dem Befehl `service vsep stop` an.
- 5 Führen Sie anschließend einen Test durch, um eine Baseline zu erhalten. Anschließend können Sie mit dem Befehl `service vsep start` den vsep-Dienst starten und einen weiteren Test durchführen.
- 6 So aktivieren Sie Debugging für den Thin Agent unter Linux:
 - a Öffnen Sie die Datei `/etc/vsep/vsep.conf`.
 - b Ändern Sie bei allen Protokollen `DEBUG_LEVEL=4` in `DEBUG_LEVEL=7` um.
 - c Bei moderaten Protokollen kann dieser Wert auf `DEBUG_LEVEL=6` festgelegt werden.
 - d Das standardmäßige Protokollziel (`DEBUG_DEST=2`) ist `vmware.log` (auf dem Host). Um es in „Gast“ zu ändern (i.e `/var/log/message` or `/var/log/syslog`), legen Sie `DEBUG_DEST=1` fest.

Hinweis Das Aktivieren der vollständigen Protokollierung kann dazu führen, dass die Datei `vmware.log` überfüllt und möglicherweise extrem groß wird. Deaktivieren Sie die vollständige Protokollierung so bald wie möglich.

Fehlerbehebung beim Thin-Agent unter Windows

- 1 Überprüfen Sie die Kompatibilität der beteiligten Komponenten. Sie benötigen die Build-Nummern für ESXi, vCenter Server, NSX Manager und die von Ihnen verwendete Sicherheitslösung (Trend Micro, McAfee, Kaspersky, Symantec usw.). Wenn Ihnen diese Daten vorliegen, vergleichen Sie die Kompatibilität der vSphere-Komponenten. Weitere Informationen finden Sie unter [VMware-Produktkompatibilitätsmatrix](#).
- 2 Stellen Sie sicher, dass VMware Tools [™] auf dem neuesten Stand ist. Wenn Sie feststellen, dass nur eine bestimmte virtuelle Maschine betroffen ist, finden Sie weitere Informationen unter [Installieren und Aktualisieren von VMware Tools in vSphere \(2004754\)](#).
- 3 Überprüfen Sie mit dem Powershell-Befehl `fl tmc`, dass der Thin Agent geladen wurde.

Nach Ausführung dieses Befehls sollten Sie den Namen „vsepflt“ in der Treiberliste finden. Wenn der Treiber nicht geladen wird, sollten Sie den Treiber mit dem Befehl `fltmc load vsepflt` laden können.

- 4 Wenn der Thin Agent ein Leistungsproblem im System verursacht, halten Sie das Laden des Treibers mit diesem Befehl an: `fltmc unload vsepflt`.

Führen Sie anschließend einen Test durch, um eine Baseline zu erhalten. Anschließend können Sie den Treiber laden und einen weiteren Test mit folgendem Befehl ausführen:

```
fltmc load vsepflt.
```

Wenn Sie feststellen, dass ein Leistungsproblem beim Thin Agent vorliegt, finden Sie weitere Informationen unter [Langsame VMs nach dem Upgrade von VMware-Tools in NSX und vCloud Networking and Security \(2144236\)](#).

- 5 Wenn Sie Network Introspection nicht verwenden, entfernen oder deaktivieren Sie diesen Treiber.

Sie können Network Introspection auch über das Installationsprogramm „Modify VMware Tools“ entfernen:

- a Stellen Sie das VMware Tools-Installationsprogramm bereit.
- b Navigieren Sie zu **Steuerungsbereich > Programme und Funktionen (Control Panel > Programs and Features)**.
- c Klicken Sie mit der rechten Maustaste auf **VMware Tools > Ändern (VMware Tools > Modify)**.
- d Wählen Sie **Vollständige Installation (Complete install)** aus.
- e Suchen Sie NSX File Introspection. Es sollte ein Unterordner nur für Network Introspection vorhanden sein.
- f Deaktivieren Sie **Network Introspection**.
- g Starten Sie die VM neu, um die Deinstallation des Treibers abzuschließen.

- 6 Aktivieren Sie die Debugging-Protokollierung für den Thin Agent. Weitere Informationen finden Sie unter [Guest Introspection-Protokolle](#). Alle Debugging-Informationen werden in der Datei `vmware.log` für diese virtuelle Maschine protokolliert.

- 7 Anhand der Procmon-Protokolle können Sie die Dateiprüfungen des Thin Agent überprüfen. Weitere Informationen finden Sie unter [Fehlerbehebung bei vShield Endpoint-Leistungsproblemen mit Antivirus-Software \(2094239\)](#).

Erfassen von Umgebungs- und Arbeitslastdetails

- 1 Ermitteln Sie, ob NSX Guest Introspection in der Kundenumgebung verwendet wird. Wenn dies nicht der Fall ist, entfernen Sie den Guest Introspection-Dienst von der virtuellen Maschine und bestätigen Sie, dass das Problem behoben wurde. Beheben Sie Guest Introspection-Probleme nur, wenn Guest Introspection benötigt wird.

2 So erfassen Sie Umgebungsdetails:

- a ESXi-Build-Version – Führen Sie den Befehl `uname -a` auf dem ESXi-Host aus oder klicken Sie im vSphere Web Client auf einen Host und suchen Sie oben im rechten Bereich nach der Build-Nummer.
- b Linux-Produktversion und -Build-Nummer
- c Mit `/usr/sbin/vsep -v` können Sie die Produktversion abrufen.

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

3 VMware NSX® for vSphere® -Version und Folgendes:

- Name und Versionsnummer der Partnerlösung
 - Von der Partnerlösung genutzte Versionsnummer der EPsec-Bibliothek: Melden Sie sich bei der SVM an und führen Sie `#strings path to EPsec library/libEPsec.so | grep BUILD` aus.
 - Gastbetriebssystem in der virtuellen Maschine
 - Jegliche anderen Anwendungen oder Dateisystemtreiber von Drittanbietern
- 4 ESX GI-Modul-(MUX)-Version – Führen Sie den Befehl `esxcli software vib list | grep epsec-mux` aus.
 - 5 Erfassen Sie Arbeitslastdetails, beispielsweise den Servertyp.
 - 6 Erfassen Sie ESXi-Hostprotokolle. Weitere Informationen finden Sie unter [Erfassen von Diagnosedaten für VMware ESX/ESXi \(653\)](#).
 - 7 Erfassen Sie Protokolle der virtuellen Dienst-Maschine (SVM) von der Partnerlösung. Weitere Informationen zur Protokollerfassung für die SVM erhalten Sie bei Ihrem Partner.
 - 8 Erfassen Sie eine Anhaltestatusdatei, während das Problem auftritt. Informationen zum Erfassen von Diagnosedaten finden Sie unter [Anhalten einer virtuellen Maschine auf ESX/ESXi \(2005831\)](#).

Fehlerbehebung bei einem Thin Agent-Absturz

Wenn der Thin Agent abstürzt, wird die Core-Datei im `/Verzeichnis` erstellt. Rufen Sie die Core-Dump-Datei (Core) vom Speicherort/Verzeichnis ab. Prüfen Sie mit dem Befehl `file`, ob der Core von vsep generiert wird. Beispiel:

```
# file core
core: ELF 64-bit LSB core file x86-64, version 1 (SYSV), SVR4-style, from '/usr/sbin/vsep'
```

Virtuelle Maschine bleibt hängen oder friert ein

Erfassen Sie die VMware-vmss-Datei im Anhaltetestatus. Informationen dazu finden Sie unter [Anhalten einer virtuellen Maschine auf ESX/ESXi zum Erfassen von Diagnosedaten \(2005831\)](#) oder lassen Sie die VM abstürzen und erfassen Sie die vollständige Speicher-Dump-Datei. VMware bietet ein Dienstprogramm für die Konvertierung von ESXi-vmss-Dateien in Core-Dump-Dateien. Weitere Informationen finden Sie unter [Verwerfen von Vmss2core](#).

Fehlerbehebung beim ESX-GI-Modul (MUX)

ESX-GI-Modul (MUX)

Wenn alle virtuellen Maschinen auf einem ESXi-Host nicht mit Guest Introspection funktionieren oder auf einem bestimmten Host Alarme bezüglich der GI-SVA-Kommunikation ausgelöst werden, könnte ein Problem mit dem ESX-GI-Modul-Modul auf dem ESXi-Host vorliegen.

- 1 Um zu prüfen, ob der Dienst auf dem ESXi-Host ausgeführt wird, führen Sie den Befehl `# /etc/init.d/vShield-Endpoint-Mux status` aus:

Beispiel:

```
# /etc/init.d/vShield-Endpoint-Mux status
vShield-Endpoint-Mux is running
```

- 2 Wenn Sie feststellen, dass der Dienst nicht ausgeführt wird, starten Sie ihn neu oder starten Sie ihn mit folgendem Befehl:

```
/etc/init.d/vShield-Endpoint-Mux start
```

oder

```
/etc/init.d/vShield-Endpoint-Mux restart
```

Hinweis: Sie können diesen Dienst gefahrlos während der Produktionszeit neu starten, da dieser Vorgang keine wesentlichen Auswirkungen hat und der Neustart innerhalb weniger Sekunden erfolgt.

- 3 Um einen besseren Einblick darin zu gewinnen, was das ESX-GI-Modul tut, oder um den Kommunikationsstatus zu überprüfen, können Sie die Protokolle auf dem ESXi-Host überprüfen. ESX-GI-Modulprotokolle werden in die Host-Datei `/var/log/syslog` geschrieben. Dies ist auch in den ESXi-Host-Support-Protokollen enthalten.

Weitere Informationen finden Sie unter [Sammeln von Diagnosedaten für ESX/ESXi-Hosts und vCenter Server mit dem vSphere Web Client \(2032892\)](#)

- 4 Die Standardoption für die ESX-GI-Modulprotokollierung Standard ist „Info“ und kann zum Debugging erhöht werden, um weitere Daten zu erfassen:

Weitere Informationen finden Sie unter [Guest Introspection-Protokolle](#).

- 5 Die erneute Installation des ESX-GI-Moduls kann ebenfalls viele Probleme beheben, besonders dann, wenn die falsche Version installiert wurde oder der ESXi-Host in einer Umgebung eingesetzt wird, in der zuvor Endpoints installiert waren. Dies muss entfernt und neu installiert werden.

Um das VIB zu entfernen, führen Sie diesen Befehl aus: `esxcli software vib remove -n epsec-mux`

- 6 Wenn bei der VIB-Installation ein Problem auftritt, prüfen Sie die Datei `/var/log/esxupdate.log` auf dem ESXi-Host. In diesem Protokoll sind die aussagekräftigsten Informationen dazu, weshalb der Treiber nicht erfolgreich installiert wurde. Dieses Problem kommt häufig bei der Installation von ESX-GI-Modulen vor. Weitere Informationen finden Sie unter [Installation von NSX Guest Introspection-Diensten \(ESX-GI-Modul-VIB\) auf dem ESXi-Host schlägt bei VMware NSX for vSphere 6.x fehl \(2135278\)](#).

- 7 Um zu ermitteln, ob ein beschädigtes ESXi-Image vorliegt, suchen Sie eine Meldung, die folgender ähnelt:

```
esxupdate: esxupdate: ERROR: Installation Error:
(None, 'No image profile is found on the host or image profile is empty.
An image profile is required to install or remove VIBs. To install an image profile,
use the esxcli image profile install command.')
```

- 8 Führen Sie den Befehl `cd /vmfs/volumes` auf dem ESXi-Host aus, um zu prüfen, ob das Image beschädigt ist.

- a Um die Datei `imgdb.tgz` zu suchen, führen Sie folgenden Befehl aus: `find * | grep imgdb.tgz`.

Dieser Befehl führt normalerweise zu zwei Übereinstimmungen. Beispiel:

`0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz` oder `edbf587b-da2add08-3185-3113649d5262/imgdb.tgz`

- b Führen Sie für jeden Treffer diesen Befehl aus: `ls -l match_result`.

Beispiel:

```
> ls -l 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz -rwx-----
1 root root 26393 Jul 20 19:28 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz
> ls -l edbf587b-da2add08-3185-3113649d5262/imgdb.tgz -rwx-----
1 root root 93 Jul 19 17:32 edbf587b-da2add08-3185-3113649d5262/imgdb.tgz
```

Die Standardgröße für die Datei `imgdb.tgz` ist wesentlich größer als die der anderen Datei. Und wenn eine der Dateien nur wenige Bytes umfasst, weist dies auf eine Beschädigung hin. Die einzige unterstützte Möglichkeit, dies zu beheben, ist die erneute Installation von ESXi für diesen bestimmten ESXi-Host.

Fehlerbehebung bei EPSecLib

NSX Manager ist für die Bereitstellung dieser virtuellen Maschine zuständig.

EPSecLib

In der Vergangenheit (mit vShield) war die Drittanbieter-SVA-Lösung für die Bereitstellung zuständig. Diese Lösung stellt jetzt eine Verbindung mit NSX Manager her. Der NSX Manager ist für die Bereitstellung dieser SVA zuständig. Wenn in der Umgebung Alarme auf den SVAs ausgelöst werden, stellen Sie sie erneut über den NSX Manager bereit.

- Jegliche Konfigurationen gehen verloren, da sie alle in NSX Manager gespeichert sind.
- Es ist besser, die virtuellen SVA-Maschinen erneut bereitzustellen statt sie neu zu starten.
- NSX nutzt EAM für die Bereitstellung und Überwachung der VIBs und SVMs auf dem Host, beispielsweise der SVA.
- Anhand des EAMs wird der Installationsstatus ermittelt.
- Dem Installationsstatus in der NSX-Benutzeroberfläche lässt sich nur entnehmen, ob die VIBs installiert sind oder ob die SVM eingeschaltet ist.
- Der Dienststatus in der NSX-Benutzeroberfläche gibt an, ob die Dienste der virtuellen Maschine ordnungsgemäß funktionieren.

SVA-Bereitstellung und Beziehung zwischen NSX und vCenter Server-Prozess

- 1 Wenn der Cluster für die Vorbereitung auf den Endpoint ausgewählt wird, wird eine Agency auf EAM zum Bereitstellen der SVA erstellt.
- 2 EAM stellt dann die ovf-Datei zusammen mit den generierten Agency-Informationen dem ESXi-Host bereit.
- 3 NSX Manager überprüft, ob die ovf-Datei von EAM bereitgestellt wurde.
- 4 NSX Manager überprüft, ob die virtuelle Maschine von EAM eingeschaltet wurde.
- 5 NSX Manager informiert den Manager der SVA-Partnerlösung, dass die virtuelle Maschine eingeschaltet und registriert wurde.
- 6 EAM sendet ein Ereignis zu NSX, um zu melden, dass die Installation abgeschlossen wurde.
- 7 Der Manager der SVA-Partnerlösung sendet ein Ereignis zu NSX, um zu melden, dass der Dienst in der virtuellen SVA-Maschine ausgeführt wird.
- 8 Falls ein Problem mit der SVA auftritt, finden Sie an zwei Stellen Protokolle, die Sie sich ansehen können. Sie können die EAM-Protokolle prüfen, da EAM für die Bereitstellung dieser virtuellen Maschinen zuständig ist. Weitere Informationen finden Sie unter [Sammeln von Diagnosedaten für VMware vCenter Server 4.x, 5.x und 6.0 \(1011641\)](#). Alternativ können Sie auch die SVA-Protokolle überprüfen.

Weitere Informationen finden Sie unter [Guest Introspection-Protokolle](#).

- 9 Wenn ein Problem mit der SVA-Bereitstellung auftritt, besteht möglicherweise ein Problem bei der Kommunikation zwischen EAM und NSX Manager. Sie können die EAM-Protokolle prüfen. Am einfachsten geht dies, indem Sie den EAM-Dienst neu starten. Weitere Informationen finden Sie unter [Hostvorbereitung](#).

10 Wenn alles Vorgenannte zu funktionieren scheint, Sie aber die Endpoint-Funktionalität testen möchten, können Sie dies mit einer Eicar-Testdatei tun:

- Erstellen Sie eine neue Textdatei mit einer beliebigen Kennzeichnung, beispielsweise: eicar.test.
- Die Datei sollte nur folgende Zeichenfolge enthalten:
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
- Speichern Sie die Datei. Beim Speichern sollten Sie sehen, dass die Datei gelöscht wird. Dies bestätigt, dass die Endpoint-Lösung funktioniert.