

Fehlerbehebung bei IP SLA auf Multipod PBR

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerktopologie](#)

[Hintergrundinformationen](#)

[Szenario](#)

[Schritte zur Fehlerbehebung](#)

[Schritt 1: Identifizieren des IP SLA-Status](#)

[Schritt 2: Knoten-ID mit Integritätsgruppe im Zustand "Down" identifizieren](#)

[Schritt 3: Überprüfung, ob das PBR-Gerät als Endgerät erkannt wurde und über den Service Leaf erreichbar ist](#)

[Schritt 4: Überprüfung der PBR-Integritätsgruppe im lokalen POD und Remote POD](#)

[Schritt 5: Erfassung von IP SLA-Tests mit dem ELAM-Tool](#)

[Schritt 6: Überprüfen Sie, ob das Fabric-System-GIPO \(239.255.255.240 \) auf lokalen und Remote-Spines programmiert ist.](#)

[Schritt 7: Validieren GIPO \(239.255.255.240 \) ist auf dem IPN konfiguriert](#)

[Schritt 8: Bestätigen, dass die IP SLA-Nachverfolgung auf dem Remote-POD aktiviert ist](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zum Identifizieren und Beheben von Problemen mit einem IP SLA-verfolgten Gerät am Remote-POD unter Verwendung einer ACI PBR Multipod-Umgebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Multipod-Lösung
- Servicediagramme mit PBR



Hinweis: Weitere Informationen zur ACI IP SLA-Konfiguration finden Sie im [PBR and Tracking Service Nodes](#) Guide.

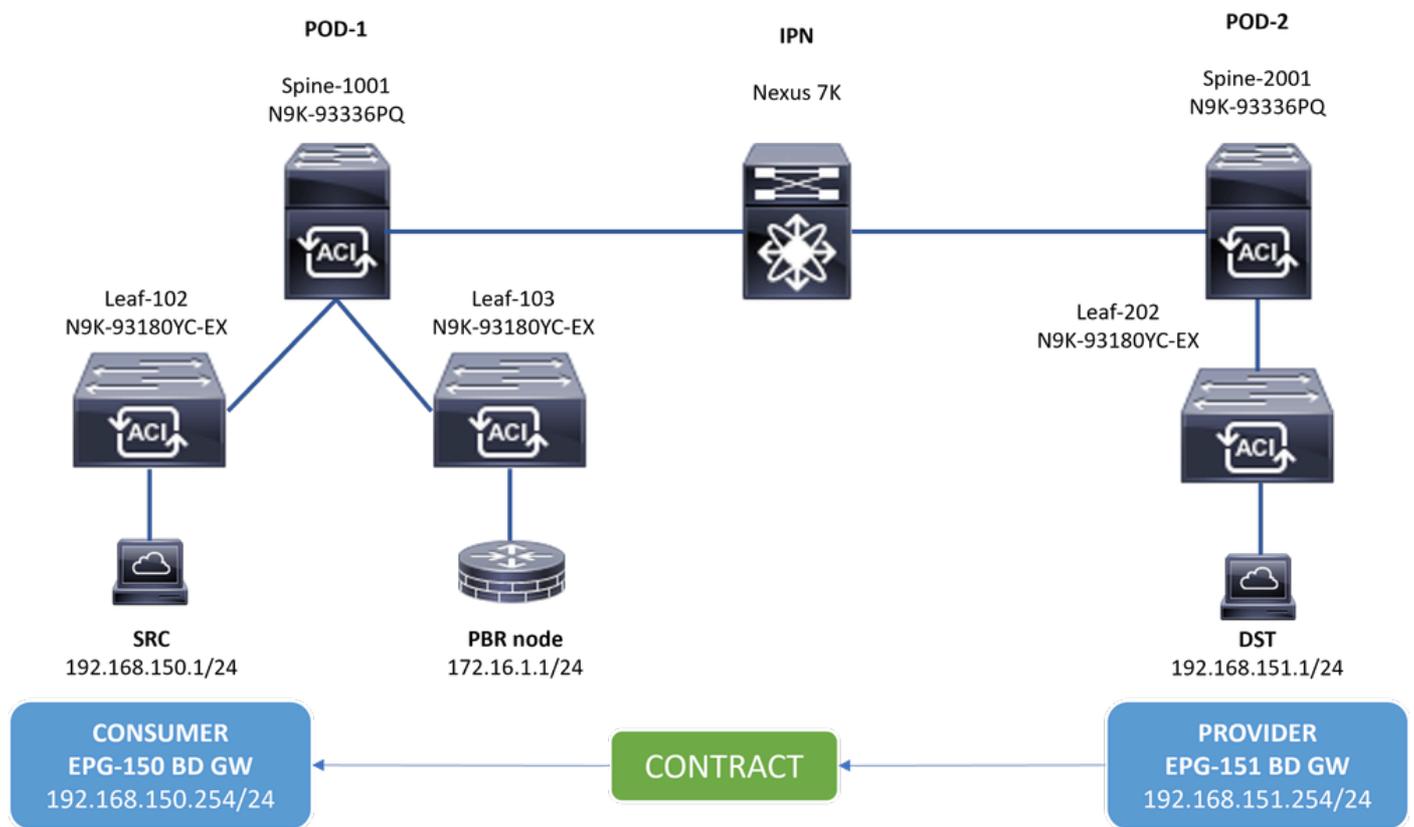
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ACI Version 4.2(7I)
- Cisco Leaf-Switch N9K-C93180YC-EX
- Cisco Spine-Switch N9K-C9336PQ
- Nexus 7000 Version 8.2(2)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerktopologie



Topologie

Hintergrundinformationen

Mithilfe eines Servicediagramms kann die Cisco ACI den Datenverkehr zwischen Sicherheitszonen an eine Firewall oder einen Load Balancer umleiten, ohne dass die Firewall oder der Load Balancer als Standard-Gateway für die Server fungieren müssen.

Mit der IP SLA-Funktion in der PBR-Einrichtung kann die ACI-Fabric diesen Serviceknoten (L4-L7-Gerät) in Ihrer Umgebung überwachen und die Fabric kann Datenverkehr zwischen Quelle und Ziel nicht an einen ausgefallenen Serviceknoten umleiten, wenn er nicht erreichbar ist.



Hinweis: ACI IPSLA benötigt die GIPO-Adresse des Fabric-Systems (Multicast-Adresse **239.255.255.240/28**), um die Tests zu senden und den Trackingstatus zu verteilen.

Szenario

In diesem Beispiel kann keine Ost-West-Verbindung zwischen dem Quellendpunkt 192.168.150.1 am POD-1 und dem Zielserver 192.168.151.1 am POD-2 hergestellt werden. Der Datenverkehr wird vom Service-Leaf 103 am POD-1 an den PBR-Knoten 172.16.1.1 umgeleitet. PBR verwendet IP SLA-Überwachung und Richtlinien für Umleitungsintegritätsgruppen.

Schritte zur Fehlerbehebung

Schritt 1: Identifizieren des IP SLA-Status

- Navigieren Sie auf der APIC-Benutzeroberfläche zu **Tenants > Your_Tenant > Faults (Tenants > Ihr_Tenant > Fehler)**.
- Suchen Sie die Fehler **F2911, F2833, F2992**.

The screenshot shows the APIC interface for Tenant - lb1. The 'Faults' tab is active, displaying a table of faults. The table has columns: Severity, Acked, Cause, Creation Time, Affected Object, Description, Code, Last Transition, and Lifecycle. Three faults are listed:

Severity	Acked	Cause	Creation Time	Affected Object	Description	Code	Last Transition	Lifecycle
Warning	Yes	svcredir-provision-failed	2024-01-31T19:14:43...	topology/pod-2/node-202/sys/svcredir/inst/destgrp-2/rdesA8-[topology/pod-2/node-202/sys/svcredir/inst/dest-[172.16.1.1]-	Fault delegate: PBR service source on nodeid 202 fabric hostname MXS2-LF202 is in failed state, reason tracked as down.	F2992	2024-01-31T19:16:48...	Raised
Warning	Yes	svcredir-threshold-violated	2024-01-31T19:14:43...	topology/pod-2/node-202/sys/svcredir/inst/destgrp-2	Fault delegate: PBR service redir grp id 2 on nodeid 202 fabric hostname MXS2-LF202 is in failed state, reason tracked as down.	F2833	2024-01-31T19:16:48...	Raised
Warning	Yes	svcredir-healthgrp-down	2024-01-31T19:07:31...	topology/pod-2/node-202/sys/svcredir/inst/healthgrp-lb1:lb-healthGrp	Fault delegate: PBR service health grp lb1:lb-healthGrp on nodeid 202 fabric hostname MXS2-LF202 is in failed state, reason Health grp service is down.	F2911	2024-01-31T19:16:48...	Raised

IP SLA-Fehler

Schritt 2: Knoten-ID mit Integritätsgruppe im Zustand "Down" identifizieren

- Führen Sie auf der APIC-CLI den Befehl **moquery** mit den Fehlern **F2911, F2833 und F2992** aus.
- Sie können sehen, dass die Integritätsgruppe **lb1:lb-healthGrp** für Leaf 202 im POD-2 deaktiviert ist.

<#root>

```
MXS2-AP002# moquery -c faultInst -f 'fault.Inst.code == "F2911"'
```

```
# fault.Inst
code : F2911
ack : no
alert : no
annotation :
cause : svcredir-healthgrp-down
changeSet : operSt (New: disabled), operStQual (New: healthgrp-service-down)
childAction :
created : 2024-01-31T19:07:31.505-06:00
delegated : yes
descr : PBR service health grp
```

```
lb1:lb-healthGrp
```

```
on nodeid 202 fabric hostname MXS2-LF202 is in failed state, reason Health grp service is down.
```

```
dn : topology/pod-2/node-202/sys/svcredir/inst/healthgrp-lb1:lb-healthGrp/fault-F2911 <<<
```

```
domain : infra
extMngdBy : undefined
highestSeverity : major
```

Schritt 3: Überprüfung, ob das PBR-Gerät als Endgerät erkannt wurde und über den Service Leaf erreichbar ist

```
<#root>
```

```
MXS2-LF103# show system internal epm endpoint ip 172.16.1.1
```

```
MAC : 40ce.2490.5743 ::: Num IPs : 1
IP# 0 : 172.16.1.1 ::: IP# 0 flags : ::: 13-sw-hit: No
Vlan id : 22 ::: Vlan vnid : 13192 ::: VRF name : lb1:vrf1
BD vnid : 15958043 ::: VRF vnid : 2162693
Phy If : 0x1a00b000 ::: Tunnel If : 0
Interface :
```

```
Ethernet1/12
```

```
Flags : 0x80004c04 ::: sclass : 16391 ::: Ref count : 5
EP Create Timestamp : 02/01/2024 00:36:23.229262
EP Update Timestamp : 02/02/2024 01:43:38.767306
EP Flags :
```

```
local
```

```
|IP|MAC|sclass|timer|
```

```
MXS2-LF103# iping 172.16.1.1 -v lb1:vrf1
```

```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.254: 56 data bytes
64 bytes from 172.16.1.1: icmp_seq=0 ttl=255 time=1.046 ms
64 bytes from 172.16.1.1: icmp_seq=1 ttl=255 time=1.074 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=255 time=1.024 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=255 time=0.842 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=255 time=1.189 ms
```

```
--- 172.16.1.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.842/1.034/1.189 ms
```

Schritt 4: Überprüfung der PBR-Integrationsgruppe im lokalen POD und Remote POD



Hinweis: Berücksichtigen Sie den lokalen POD als den POD, für den das PBR-Gerät konfiguriert wird.

Leaf 103 ist der Service Leaf am POD-1. Aus diesem Grund wird POD-1 als lokaler POD und POD-2 als Remote-POD betrachtet.

Die Integritätsgruppe ist nur auf Leaf-Switches programmiert, bei denen die Bereitstellung aufgrund von Quell- und Ziel-EPGs erforderlich ist.

1. Die Quell-EPG befindet sich auf Leaf Node 102 POD-1. Wie Sie sehen, wird das PBR-Gerät vom Service Leaf 103 POD-1 als UP verfolgt.

<#root>

```
MXS2-LF102# show service redir info health-group lb1::lb-healthGrp
```

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr

=====

HG-Name HG-OperSt HG-Dest HG-Dest-OperSt

=====

lb1::lb-healthGrp

enabled

dest-[172.16.1.1]-[vlan-2162693]]

up

2. Die Ziel-EPG befindet sich auf Leaf Node 202 POD-2. Wie Sie sehen, wird das PBR-Gerät vom Service Leaf 103 POD-1 nach "DOWN" sortiert.

<#root>

MXS2-LF202# show service redir info health-group lb1::lb-healthGrp

=====

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr

=====

HG-Name HG-OperSt HG-Dest HG-Dest-OperSt

=====

lb1::lb-healthGrp

disabled

dest-[172.16.1.1]-[vlan-2162693]]

down <<<<< Health Group is down.

Schritt 5: Erfassung von IP SLA-Tests mit dem ELAM-Tool



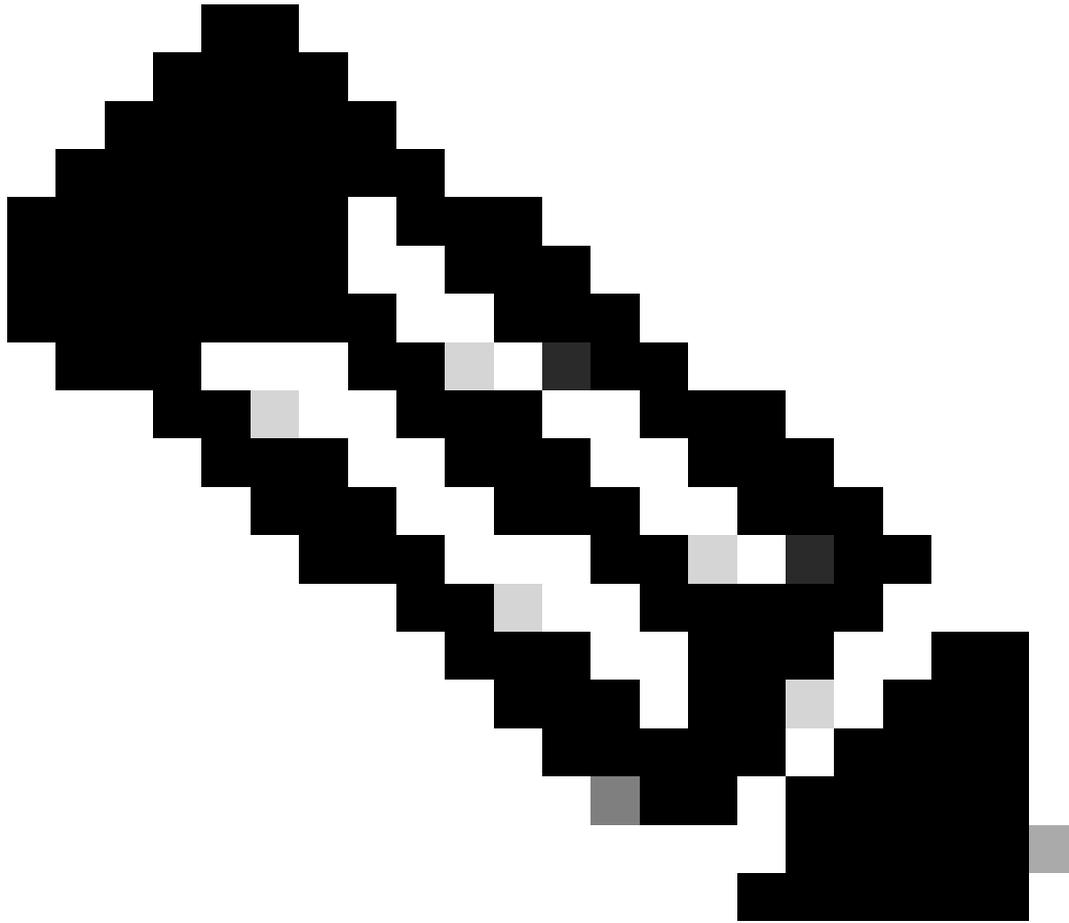
Hinweis: Sie können das Embedded Logic Analyzer Module (ELAM), ein integriertes Erfassungstool, verwenden, um das eingehende Paket zu erfassen. Die ELAM-Syntax hängt vom Hardwaretyp ab. Ein weiterer Ansatz besteht in der Verwendung der [ELAM Assistant-App](#).

Um die IP SLA-Tests zu erfassen, müssen Sie diese Werte in der ELAM-Syntax verwenden, um zu ermitteln, wo das Paket ankommt oder verworfen wird.

ELAM: Innerer L2-Header

Quell-MAC = **00-00-00-00-00-01**

Ziel-MAC = **01-00-00-00-00-00**



Hinweis: Quell-MAC und Ziel-Mac (weiter oben abgebildet) sind feste Werte im inneren Header für IP SLA-Pakete.

ELAM Äußerer L3-Header

Quell-IP = TEP von Ihrem Service Leaf (Leaf 103 TEP in LAB = 172.30.200.64)

Ziel-IP = **239.255.255.240** (Die GIPO des Fabric-Systems muss immer die gleiche sein.)

<#root>

```
trigger reset
trigger init in-select 14 out-select 0
set inner 12 dst_mac
```

01-00-00-00-00-00

src_mac

00-00-00-00-00-01

```
set outer ipv4 src_ip
```

172.30.200.64

dst_ip

239.255.255.240

```
start
stat
ereport
```

...

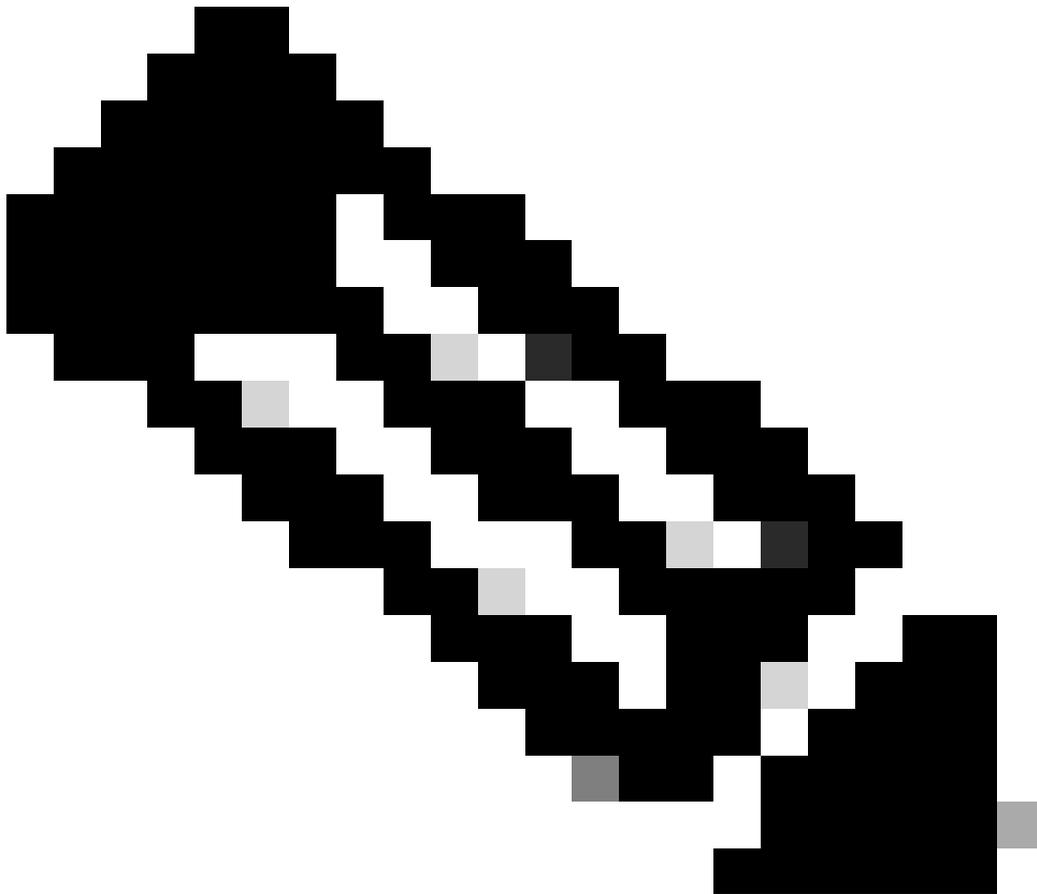
Inner L2 Header

Inner Destination MAC : 0100.0000.0000
Source MAC : 0000.0000.0001
802.1Q tag is valid : no
CoS : 0
Access Encap VLAN : 0

Outer L3 Header

L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 27
IP Protocol Number : UDP
Destination IP : 239.255.255.240
Source IP : 172.30.200.64

Schritt 6: Überprüfen Sie, ob das Fabric-System-GIPO (239.255.255.240) auf lokalen und Remote-Spines programmiert ist.



Hinweis: Für jedes GIPO wird nur ein Spine-Knoten von jedem POD als autoritäres Gerät für die Weiterleitung von Multicast-

Frames und das Senden von IGMP-Joins an das IPN ausgewählt.

1. Spine 1001 POD-1 ist der maßgebliche Switch für die Weiterleitung von Multicast-Frames und das Senden von IGMP-Joins an das IPN.

Die Schnittstelle Eth1/3 weist zum N7K IPN.

<#root>

```
MXS2-SP1001# show isis internal mcast routes gipo | more
```

```
IS-IS process: isis_infra  
VRF : default
```

```
GIPo Routes
```

```
=====  
System GIPo - Configured: 0.0.0.0  
Operational: 239.255.255.240  
=====
```

```
<OUTPUT CUT> ...
```

```
GIPo: 239.255.255.240 [LOCAL]
```

```
OIF List:  
Ethernet1/35.36
```

```
Ethernet1/3.3(External) <<< Interface must point out to IPN on elected Spine
```

```
Ethernet1/16.40  
Ethernet1/17.45
```

Ethernet1/2.37
Ethernet1/36.42
Ethernet1/1.43

```
MXS2-SP1001# show ip igmp gipo joins | grep 239.255.255.240
```

```
239.255.255.240 0.0.0.0 Join Eth1/3.3 43 Enabled
```

2. Spine 2001 POD-2 ist der maßgebliche Switch für die Weiterleitung von Multicast-Frames und das Senden von IGMP-Joins an das IPN.

Die Schnittstelle Eth1/36 weist zum N7K IPN.

<#root>

```
MXS2-SP2001# show isis internal mcast routes gipo | more
```

```
IS-IS process: isis_infra  
VRF : default
```

GIPo Routes

```
=====  
System GIPo - Configured: 0.0.0.0  
Operational: 239.255.255.240  
=====
```

<OUTPUT CUT> ...

```
GIPo: 239.255.255.240 [LOCAL]
```

```
OIF List:  
Ethernet1/2.40
```

Ethernet1/1.44

Ethernet1/36.36(External) <<< Interface must point out to IPN on elected Spine

```
MXS2-SP2001# show ip igmp gipo joins | grep 239.255.255.240
```

```
239.255.255.240 0.0.0.0 Join Eth1/36.36 76 Enabled
```

3. Achten Sie darauf, dass die Liste der ausgehenden Schnittstellen für beide Spines nicht leer von VSH ist.

<#root>

```
MXS2-SP1001# vsh
```

```
MXS2-SP1001# show forwarding distribution multicast outgoing-interface-list gipo | more
```

```
....  
Outgoing Interface List Index: 1  
Reference Count: 1  
Number of Outgoing Interfaces: 5  
Ethernet1/35.36  
Ethernet1/3.3  
Ethernet1/2.37  
Ethernet1/36.42
```

```
Ethernet1/1.43
External GIPO OIFList
Ext OIFL: 8001
Ref Count: 393
No OIFs: 1
Ethernet1/3.3
```

Schritt 7. Validate GIPO (239.255.255.240) ist auf dem IPN konfiguriert

1. Bei der IPN-Konfiguration fehlt GIPO 239.255.255.240.

```
<#root>
```

```
N7K-ACI_ADMIN-VDC-ACI-IPN-MPOD# show run pim
```

```
...
ip pim rp-address 192.168.100.2 group-list 225.0.0.0/15 bidir
ip pim ssm range 232.0.0.0/8
```

```
N7K-ACI_ADMIN-VDC-ACI-IPN-MPOD# show ip mroute 239.255.255.240
```

```
IP Multicast Routing Table for VRF "default"
```

```
(* , 239.255.255.240/32), uptime: 1d01h, igmp ip pim
```

```
Incoming interface: Null, RPF nbr: 0.0.0.0 <<< Incoming interface and RPF are MISSING
```

```
Outgoing interface list: (count: 2)
Ethernet3/3.4, uptime: 1d01h, igmp
Ethernet3/1.4, uptime: 1d01h, igmp
```

2. GIPO 239.255.255.240 ist jetzt auf IPN konfiguriert.

<#root>

```
N7K-ACI_ADMIN-VDC-ACI-IPN-MPOD# show run pim
```

```
...
```

```
ip pim rp-address 192.168.100.2 group-list 225.0.0.0/15 bidir
```

```
ip pim rp-address 192.168.100.2 group-list 239.255.255.240/28 bidir <<< GIPO is configured
```

```
ip pim ssm range 232.0.0.0/8
```

```
N7K-ACI_ADMIN-VDC-ACI-IPN-MPOD# show ip mroute 225.0.42.16
```

```
IP Multicast Routing Table for VRF "default"
```

```
(*, 225.0.42.16/32), bidir, uptime: 1w6d, ip pim igmp
```

```
Incoming interface: loopback1, RPF nbr: 192.168.100.2
```

```
Outgoing interface list: (count: 2)
```

```
Ethernet3/1.4, uptime: 1d02h, igmp
```

```
loopback1, uptime: 1d03h, pim, (RPF)
```

Schritt 8: Bestätigen, dass die IP SLA-Nachverfolgung auf dem Remote-POD aktiviert ist

<#root>

```
MXS2-LF202# show service redir info health-group lb1:lb-healthGrp
```

```
=====
```

LEGEND

TL: Threshold(Low) | TH: Threshold(High) | HP: HashProfile | HG: HealthGrp | BAC: Backup-Dest | TRA: Tr

```
=====
```

HG-Name HG-OperSt HG-Dest HG-Dest-OperSt

```
=====
```

lb1:lb-healthGrp

enabled

dest-[172.16.1.1]-[vlan-2162693]]

up

Zugehörige Informationen

Cisco Bug-ID	Bug-Titel	Version reparieren
Cisco Bug-ID CSCwi75331	Das wiederholte Laden von FM und LC im Chassis kann zu einer Fehlprogrammierung der GIPO IP OIFlist führen.	Keine feste Version. Problemumgehung verwenden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.