

Solucionar problemas de SLA IP em PBR de vários pods

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia de rede](#)

[Informações de Apoio](#)

[Cenário](#)

[Passos de Troubleshooting](#)

[Etapa 1. Identificar o status do SLA IP](#)

[Etapa 2. Identificar ID do Nó com Grupo de Integridade no estado Inativo](#)

[Etapa 3. Validar que o dispositivo PBR é reconhecido como um endpoint e pode ser acessado a partir da folha de serviço](#)

[Etapa 4. Verificar o grupo de integridade do PBR no POD local e no POD remoto](#)

[Etapa 5. Capturar sondas IP SLA com a ferramenta ELAM](#)

[Etapa 6. Verifique se o GIPO do sistema de estrutura \(239.255.255.240 \) está programado em espinhas locais e remotas](#)

[Passo 7. Validar que o GIPO \(239.255.255.240 \) está configurado no IPN](#)

[Etapa 8. Confirme se o rastreamento IP SLA está ATIVADO no POD remoto](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para identificar e solucionar problemas de um dispositivo rastreado IP SLA no POD remoto usando o ambiente ACI PBR Multipod.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Solução de vários pods
- Gráficos de serviço com PBR



Observação: para obter mais informações sobre a configuração do SLA IP da ACI, consulte o [guia PBR and Tracking Service Nodes](#).

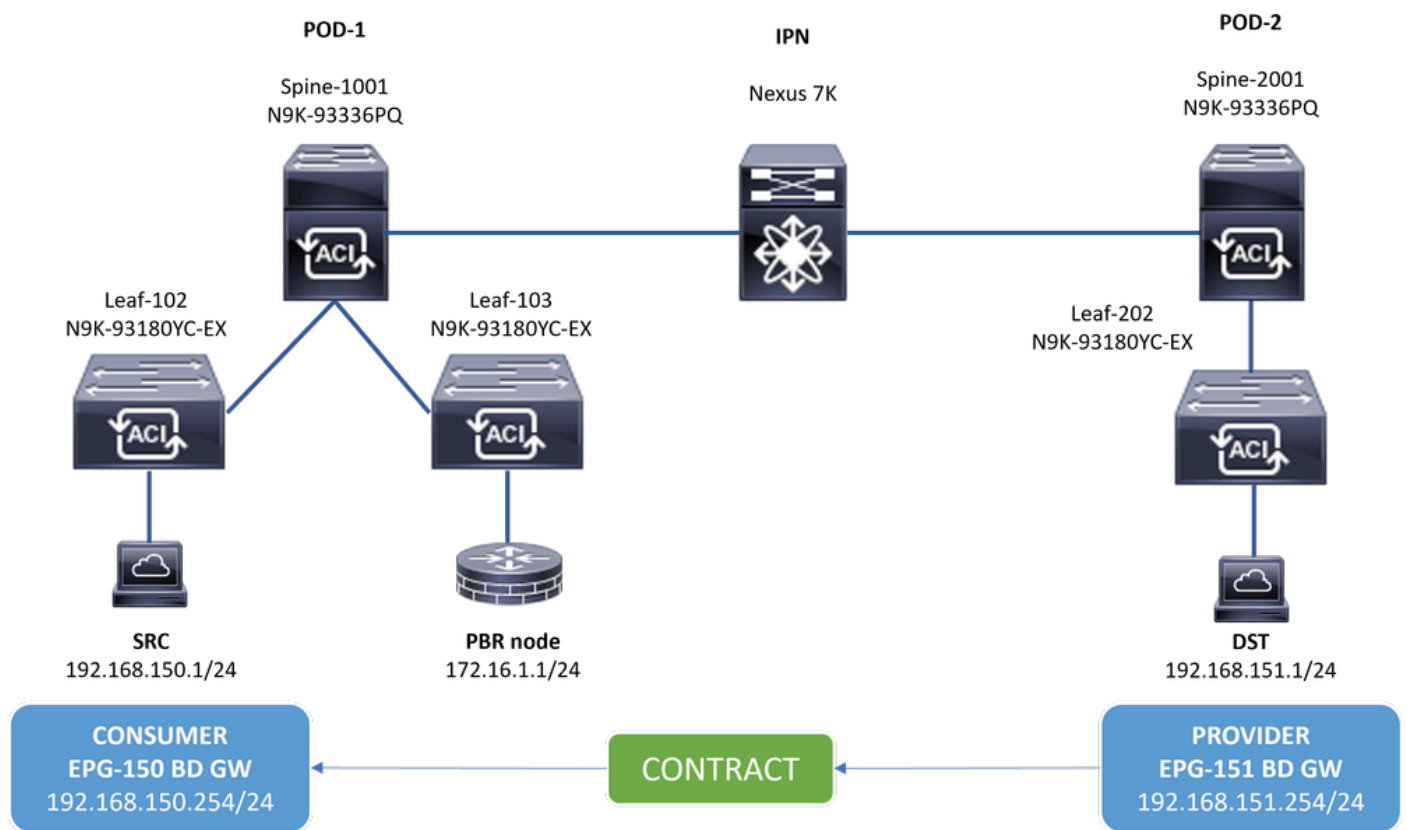
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia de rede



Topologia

Informações de Apoio

Usando um gráfico de serviço, a Cisco ACI pode redirecionar o tráfego entre zonas de segurança para um firewall ou balanceador de carga, sem a necessidade de o firewall ou balanceador de carga ser o gateway padrão para os servidores.

O recurso IP SLA na configuração do PBR permite que a estrutura da ACI monitore esse nó de serviço (dispositivo L4-L7) em seu ambiente e permite que a estrutura não redirecione o tráfego entre a origem e o destino para um nó de serviço que esteja inativo se estiver inacessível.



Observação: o IPSLA da ACI depende do GIPO (endereço multicast **239.255.255.240/28**) do sistema de estrutura para enviar as sondas e distribuir o status de rastreamento.

Cenário

Neste exemplo, a conectividade leste-oeste não pode ser concluída entre o ponto final de origem 192.168.150.1 no POD-1 para o servidor de destino 192.168.151.1 no POD-2. O tráfego está sendo redirecionado para o nó PBR 172.16.1.1 a partir da folha de serviço 103 no POD-1. O PBR está usando o monitoramento de SLA de IP e as políticas de Redirect Health Group.

Passos de Troubleshooting

Etapa 1. Identificar o status do SLA IP

- Na interface do APIC, navegue para **Locatários > Seu_Locatário > Falhas**.
- Procure falhas **F2911, F2833, F2992**.

The screenshot shows the Cisco APIC interface for tenant 'lb1'. The 'Faults' tab is active, displaying a table of faults. The table has the following 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/rsdesAfr-[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

Falhas de SLA IP

Etapa 2. Identificar ID do Nó com Grupo de Integridade no estado Inativo

- No APIC CLI, execute o comando **moquery** usando **F2911, F2833, F2992 com falha**.
- Você pode ver que o grupo de funcionamento **lb1::lb-healthGrp** está inoperante para a folha 202 no POD-2.

<#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
```

Etapa 3. Validar que o dispositivo PBR é reconhecido como um endpoint e pode ser acessado a partir da folha de serviço

<#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|
```

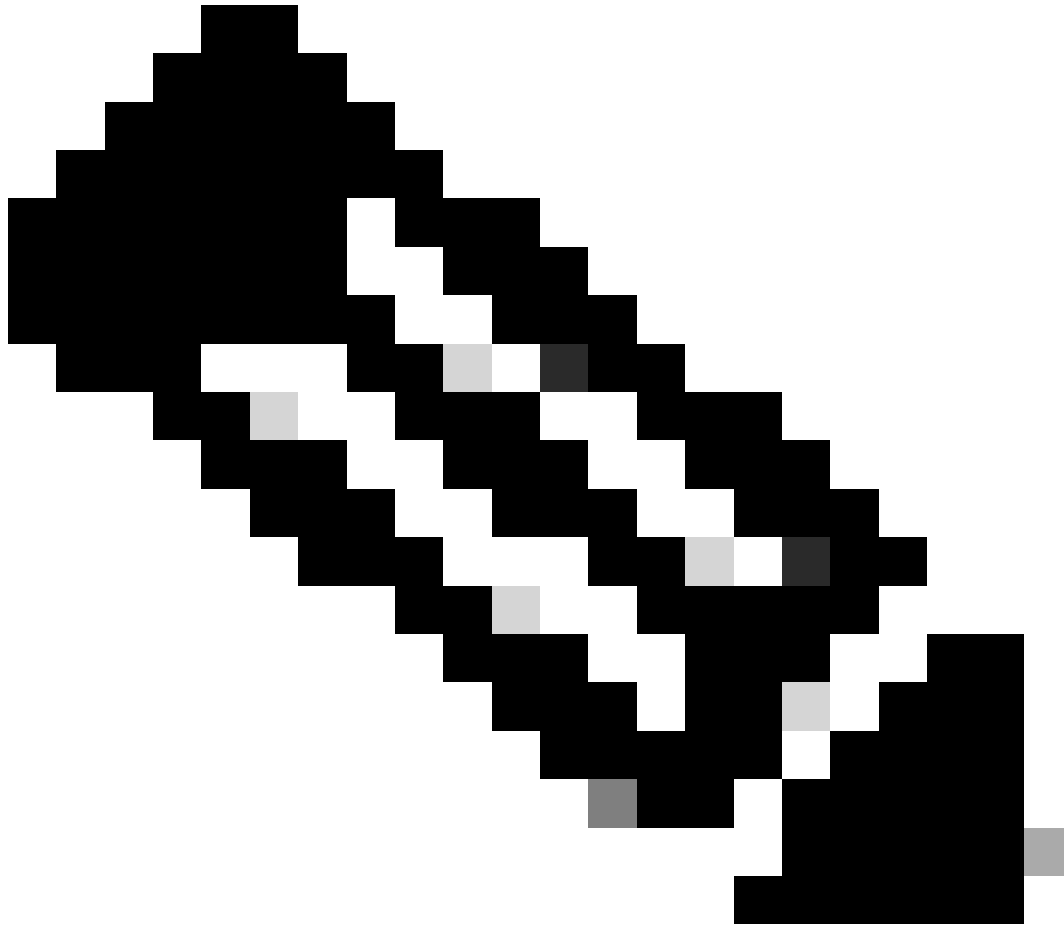
```
MXS2-LF103# iping 172.16.1.1 -v lb1:vrf1
```

```
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
```

Etapa 4. Verificar o grupo de integridade do PBR no POD local e no POD remoto



Observação: considere o POD local aquele que configura o dispositivo PBR.

A folha 103 é a folha de serviço no POD-1. Portanto, consideramos o POD-1 como o POD local e o POD-2 como o POD remoto.

O grupo de integridade é programado apenas em switches leaf nos quais os EPGs de origem e destino exigem sua implantação.

1. O EPG de origem está localizado no nó de folha 102 POD-1. Você pode ver que o dispositivo PBR é rastreado como UP do Service Leaf 103 POD-1.

<#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]-[vxlan-2162693]]
```

```
up
```

2. EPG de destino está localizado no nó de folha 202 POD-2. Você pode ver que o dispositivo PBR é rastreado como INATIVO a partir do Service Leaf 103 POD-1.

<#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]-[vxlan-2162693]]
```

```
down <<<<< Health Group is down.
```

Etapa 5. Capturar sondas IP SLA com a ferramenta ELAM



Observação: você pode usar o Embedded Logic Analyzer Module (ELAM), uma ferramenta de captura incorporada, para capturar o pacote recebido. A sintaxe do ELAM depende do tipo de hardware. Outra abordagem é usar o aplicativo [ELAM Assistant](#).

Para capturar os testes SLA IP, você deve usar esses valores na sintaxe ELAM para entender onde o pacote alcança ou está sendo descartado.

Cabeçalho L2 interno ELAM

MAC origem = **00-00-00-00-00-01**

MAC de destino = **01-00-00-00-00-00**



Observação: o MAC de origem e o Mac de destino (mostrado anteriormente) são valores fixos no cabeçalho interno para pacotes SLA IP.

Cabeçalho L3 externo ELAM

IP de origem = TEP da folha de serviço (Folha 103 TEP no LAB = 172.30.200.64)

IP de destino = 239.255.255.240 (O GIPO do sistema de estrutura deve ser sempre o mesmo)

<#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
```

...

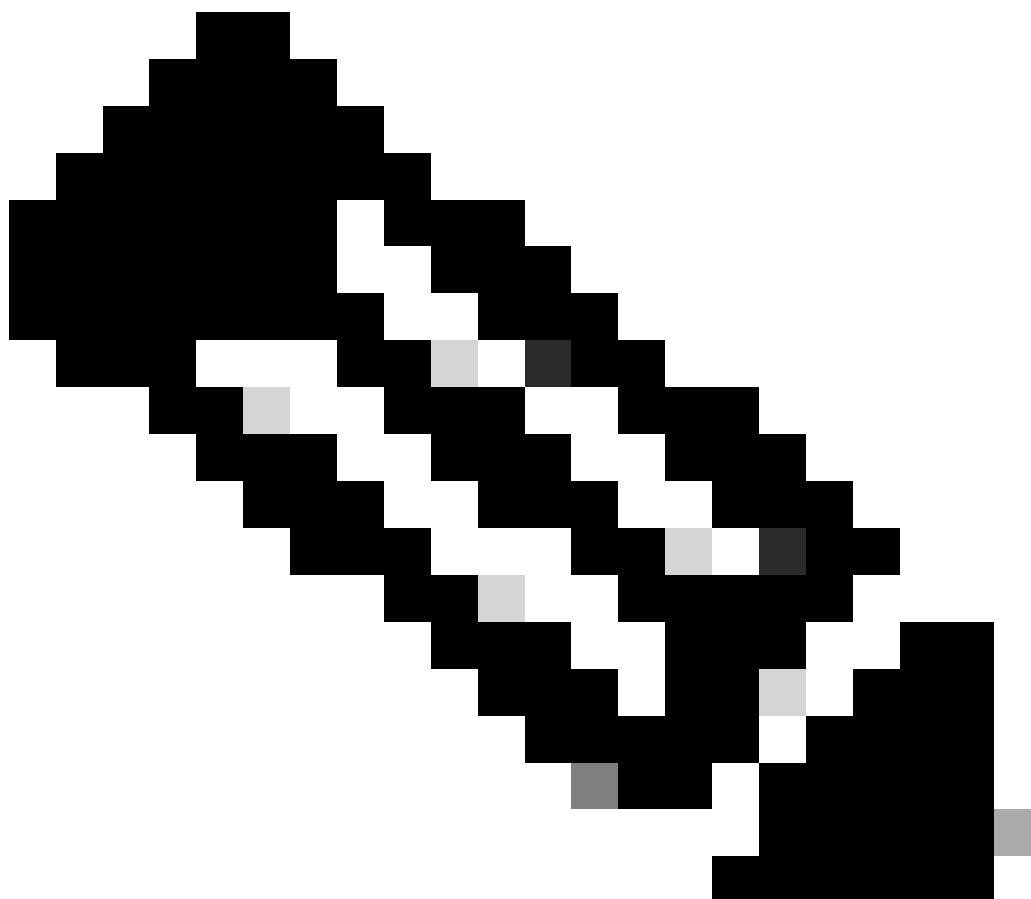
Inner L2 Header

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

Etapa 6. Verifique se o GIPO do sistema de estrutura (239.255.255.240) está programado em espinhas locais e remotas



Observação: para cada GIPO, apenas um nó spine de cada POD é eleito como o dispositivo autorizado para encaminhar quadros

multicast e enviar junções IGMP para o IPN.

1. Spine 1001 POD-1 é o switch com autoridade para encaminhar quadros multicast e enviar junções IGMP para o IPN.

A interface Eth1/3 está voltada para o IPN N7K.

<#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 O POD-2 é o switch com autoridade para encaminhar quadros multicast e enviar junções IGMP para o IPN.

A interface Eth1/36 está voltada para o IPN N7K.

<#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. Certifique-se de que o gipo outgoing-interface-list não esteja vazio do VSH para ambos os spines.

```
<#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
```

Passo 7. Validar que o GIPO (239.255.255.240) está configurado no IPN

1. O GIPO 239.255.255.240 está ausente na configuração do IPN.

```
<#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. O GIPO 239.255.255.240 agora está configurado no IPN.

<#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)
```

Etapa 8. Confirme se o rastreamento IP SLA está ATIVADO no POD remoto

<#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

Informações Relacionadas

ID de bug da Cisco	Título do erro	Corrigir versão
ID de bug da Cisco CSCwi75331	Repetidamente, recarregar o FM e o LC no chassi pode levar a uma programação incorreta da lista OIF IP do GIPO.	Nenhuma versão fixa. Use uma solução alternativa.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.