

验证ACI共享服务 — Shared Service Consumer

PcTag 14

目录

[简介](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置要点](#)

[验证](#)

[场景1 - EPG到EPG：在提供商EPG中定义的共享子网](#)

[EPG-1至EPG-2流量跟踪](#)

[EPG-2至EPG-1流量跟踪](#)

[场景2 - BD到BD：在提供商BD中定义的共享子网。](#)

[EPG-1至EPG-2流量跟踪](#)

[EPG-2至EPG-1流量跟踪](#)

[TCAM使用率突出显示](#)

[结论](#)

[参考资料和有用的链接](#)

简介

本文档介绍在ACI中使用共享BD配置和验证Shared Services配置的步骤。

背景信息

共享服务配置支持在ACI交换矩阵内不同VRF之间的EPG之间进行通信。

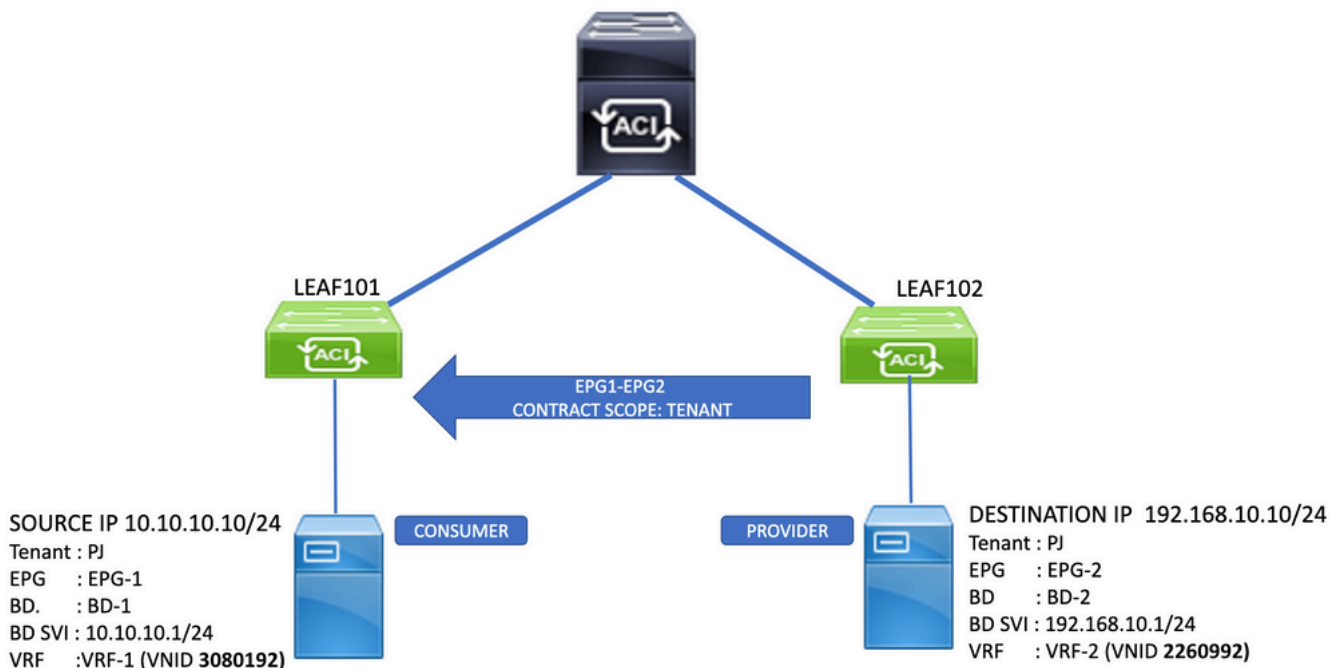
Shared Services充分利用了3个PcTag[类别](#)：

类别名称	PcTag范围
system	1 - 15
全局	16 - 16385
本地	16386 - 65535

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



配置要点

- 子网上的“VRF间共享”子网范围需要泄漏出去,192.168.10.1/24
- 由于EPG在同一个租户中，合同必须至少具有“租户”范围。如果EPG位于不同的租户中，则合同必须具有“全局”范围
- 如果在提供商EPG下定义共享子网，则只需在要共享的EPG上提供合同，并在EPG上使用合同。

或者

- 如果共享子网在提供商BD下定义，则合同必须由EPG提供，且仅由BD上的EPG和子网使用。随着更多分区规则的编程，这将占用更多TCAM空间。

注意： VZany不支持作为共享服务提供商。

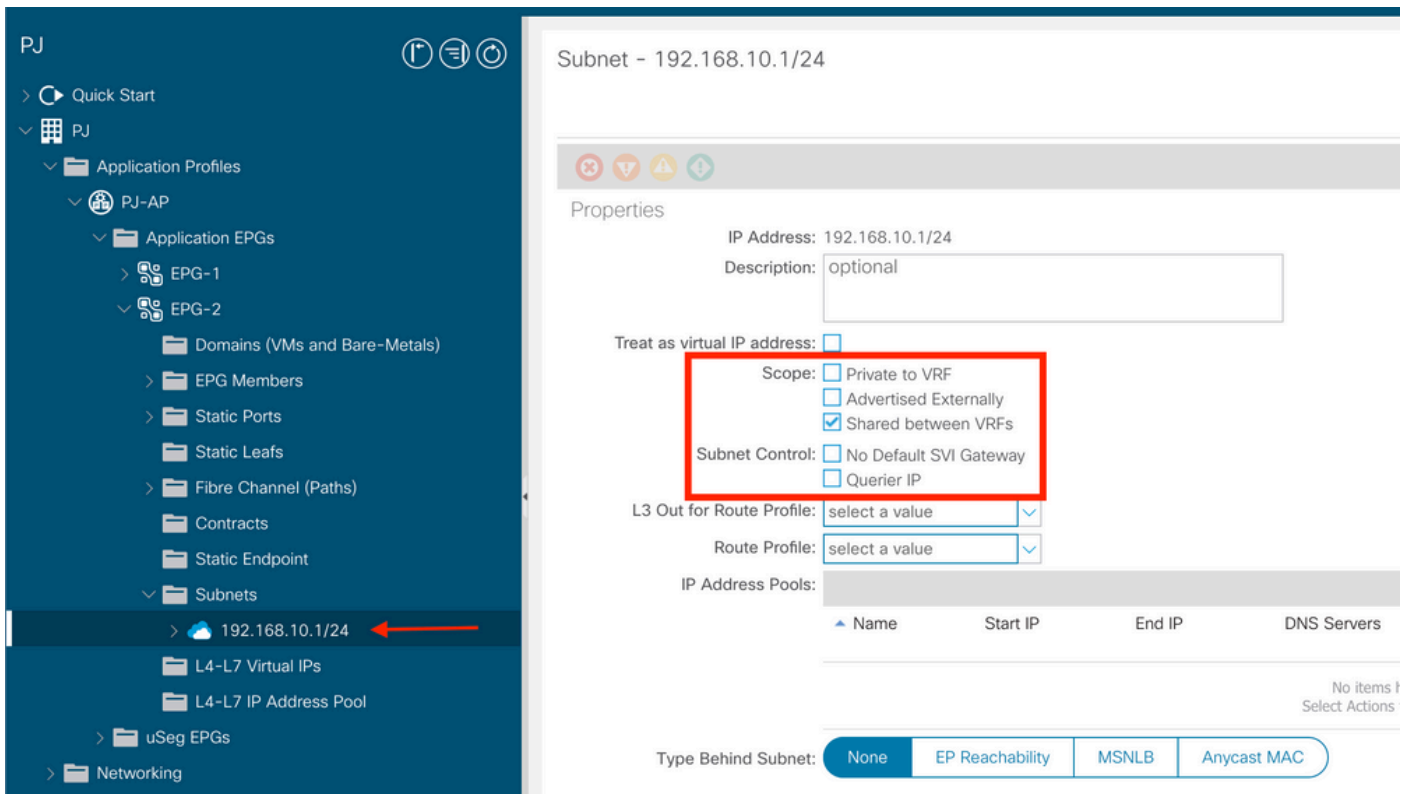
验证

场景1 - EPG到EPG：在提供商EPG中定义的共享子网

在本示例场景中，共享子网在EPG-2下配置。

注意： 如果在EPG及其关联的BD下定义相同的子网，则两个定义必须设置相同的Scope值。

此选项可优化TCAM利用率并完成Shared Services配置。TCAM已优化，因为分区规则只需在使用者VRF中进行编程。在此场景中，消费者VRF仅位于枝叶101上。



EPG-1至EPG-2流量跟踪

消费者枝叶101

枝叶101消费者VRF PJ:VRF-1上的路由信息显示通过VNID 226092 (即提供商VRF PJ:VRF-2) 到达192.168.10.10的路由：

```
leaf101# show ip route 192.168.10.10 vrf PJ:VRF-1
```

```
IP Route Table for VRF "PJ:VRF-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'% ' in via output denotes VRF
```

```
192.168.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.240.33%overlay-1, [1/0], 23:06:11, static, tag 4294967294, rwVnid: vxlan-2260992
    recursive next hop: 10.0.240.33/32%overlay-1
```

可以根据从源10.10.10.10到目标192.168.10.1的ICMP请求，使用消费者枝叶101上的ELAM验证流量

```
leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 10.10.10.10 dst_ip 192.168.10.10
module-1# start
```

```
module-1# ereport
```

```
...
```

```
-----
-----
Outer L3 Header
```

```

-----
...
IP Protocol Number          : ICMP
IP CheckSum                 : 37262( 0x918E )
Destination IP           : 192.168.10.10
Source IP                : 10.10.10.10
-----

Contract Lookup Key
-----

IP Protocol                 : ICMP( 0x1 )
L4 Src Port                 : 2048( 0x800 )
L4 Dst Port                 : 16568( 0x40B8 )
sclass (src pcTag)       : 16388( 0x4004 )
dclass (dst pcTag)       : 10930( 0x2AB2 )
src pcTag is from local table : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded
-----

Contract Result
-----

Contract Drop               : no
Contract Logging            : no
Contract Applied         : yes
Contract Hit                : yes
Contract Aclqos Stats Index : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )

```

报告显示，该合同应用于消费者枝叶101，且分配了Src pcTag 16388(EPG-1)和Dst PcTAG 10930(EPG-2)。

这些值可以与Consumer VRF PJ:VRF-1(VNID 3080192)中的已编程Zoning-Rules进行比较，以识别哪个规则ID被命中：

```

leaf101# show zoning-rule scope 3080192
+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4117 | 10930 | 0 | implicit | uni-dir | enabled | 3080192 |
deny,log | shsrc_any_any_deny(12) |
| 4108 | 10930 | 16388 | 8 | uni-dir-ignore | enabled | 3080192 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
| 4118 | 16388 | 10930 | 8 | bi-dir | enabled | 3080192 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

注意：隐式拒绝规则从提供商EPG-2(PcTag 10930)自动创建到任何(PcTag 0)。这是为了防止从提供商VRF到消费者VRF的通信，而无需在EPG之间签订其他合同。

EPG-2至EPG-1流量跟踪

提供程序枝叶102

提供商VRF PJ:VRF-2的枝叶102上的路由信息显示通过VNID 3080192的10.10.10.10的路由，此为Consumer VRF PJ:VRF-1:

```
leaf102# show ip route 10.10.10.10 vrf PJ:VRF-2
IP Route Table for VRF "PJ:VRF-2"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%' in via output denotes VRF

10.10.10.0/24, ubest/mbest: 1/0, attached, direct, pervasive
   *via 10.0.240.33%overlay-1, [1/0], 1d22h, static, tag 4294967294, rwVnid: vxlan-3080192
       recursive next hop: 10.0.240.33/32%overlay-1
```

可以根据从源192.168.10.10到目标10.10.10.10的ICMP请求，使用提供商枝叶101上的ELAM验证流量：

```
leaf102# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start
```

```
module-1# ereport
```

```
... -----
----- Outer L3 Header -----
----- ...
IP Protocol Number : ICMP IP CheckSum : 37262( 0x918E ) Destination IP      :
10.10.10.10
Source IP           : 192.168.10.10

-----
-----
Contract Lookup Key
-----
-----
IP Protocol           : ICMP( 0x1 )
L4 Src Port          : 0( 0x0 )
L4 Dst Port          : 18616( 0x48B8 )
sclass (src pcTag)   : 10930( 0x2AB2 )
dclass (dst pcTag)   : 14( 0xE )
src pcTag is from local table      : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet     : no
If yes, Contract is not applied here because it is flooded

-----
-----
Contract Result
-----
-----
Contract Drop         : no
Contract Logging      : no
Contract Applied      : no
```

```
Contract Hit : yes
Contract Aclqos Stats Index : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

在此报告中，请注意class和dclass都是非本地值。

共享服务提供商EPG-2现在驱动的全局PcTag为10930。

分配给此数据包的dclass是**Shared Service Consumer PcTag 14**。PcTag 14是为VRF间流量保留的系统PcTag。

观察在Provider EPG2 PcTag 10930和Shared Service Consumer System PcTag 14之间的Provider Leaf 102上编程了一个特殊的Zoning-Rule，其“操作”设置为“**permit_override**”。此规则允许匹配的流转发到消费者枝叶以进行最终策略查找：

```
leaf102# show zoning-rule
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action |
Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 4113 | 10930 | 14 | implicit | uni-dir | enabled | 2260992 | | permit_override |
src_dst_any(9) |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
```

场景2 - BD到BD：在提供商BD中定义的共享子网。

在本示例场景中，共享子网仅在BD-2中配置。

要完成Shared Services配置，合同必须在两个EPG（EPG-1和EPG-2）上同时使用和提供。

PJ



> Quick Start

▼ PJ

▼ Application Profiles

▼ PJ-AP

▼ Application EPGs

> EPG-1

> EPG-2

> uSeg EPGs

▼ Networking

▼ Bridge Domains

▼ BD-1

> DHCP Relay Labels

▼ Subnets

10.10.10.1/24



> ND Proxy Subnets

▼ BD-2

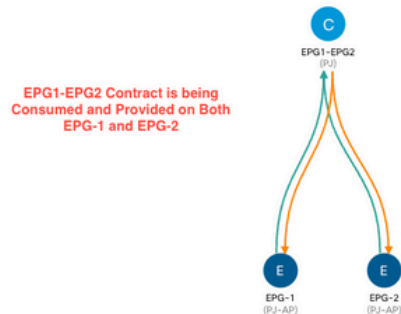
> DHCP Relay Labels

▼ Subnets

192.168.10.1/24



> ND Proxy Subnets



Provider
Consumer
Intra EPG/ESG
Provider (from Master)
Consumer (From Master)
Intra EPG/ESG (from Master)
Master EPG/ESG

EPG-1至EPG-2流量跟踪

当共享服务合同在两个EPG上提供和消耗时，EPG-1（枝叶101）和EPG-2（枝叶102）之间的数据包流观察到以下属性：

- EPG-1被视为提供商
- EPG-2被视为消费者
- 枝叶102是消费者枝叶，因此在此处应用最终策略。

路由信息与场景1相同。

“提供商”枝叶101:

```

Leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 10.10.10.10 dst_ip 192.168.10.10
module-1# start
module-1# status
  
```

```

module-1# ereport
  
```

```

... -----
----- Outer L3 Header -----
----- ...
IP Protocol Number : ICMP IP CheckSum : 23304( 0x5B08 ) Destination IP      :
192.168.10.10
Source IP           : 10.10.10.10
-----
Contract Lookup Key
-----
IP Protocol          : ICMP( 0x1 )
L4 Src Port         : 2048( 0x800 )
L4 Dst Port         : 59074( 0xE6C2 )
sclass (src pCtag)  : 18( 0x12 )
  
```



```
dclass (dst pcTag) : 14( 0xE )
src pcTag is from local table : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded
```

```
-----
-----
Contract Result
-----
-----
Contract Drop : no
Contract Logging : no
Contract Applied : no
Contract Hit : yes
Contract Aclqos Stats Index : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

观察到dclass 14已分配。这意味着允许流量通过“permit_override”规则继续，以便消费者枝叶可以驱动最终策略查找。

“消费者”枝叶102

```
Leaf102# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 14 out-select 1
module-1# set inner ipv4 src_ip 10.10.10.10 dst_ip 192.168.10.10
module-1# start
```

```
module-1# ereport
...
```

```
-----
----- Inner L3 Header -----
----- ... IP -----
Protocol Number : ICMP Destination IP : 192.168.10.10
Source IP : 10.10.10.10
```

```
-----
-----
Contract Lookup Key
-----
-----
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 26203( 0x665B )
sclass (src pcTag) : 18( 0x12 )
dclass (dst pcTag) : 10930( 0x2AB2 )
src pcTag is from local table : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded
```

```
-----
-----
Contract Result
-----
-----
Contract Drop : no
Contract Logging : no
Contract Applied : yes
```

```
Contract Hit : yes
Contract Aclqos Stats Index : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

请注意，EPG-1和EPG-2现在都具有Global PcTags;EPG-1为PcTag 18,EPG-2为PcTag 10938。

EPG-2至EPG-1流量跟踪

当共享服务合同在两个EPG上提供和消耗时，EPG-2（枝叶102）和EPG-1（枝叶101）之间的数据包流观察到以下属性：

- EPG-2被视为提供商
- EPG-1被视为消费者
- 枝叶101是消费者枝叶，因此在此处应用最终策略。

路由信息与场景1相同。

“提供商”枝叶102

```
Leaf102# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start
```

```
module-1# ereport
```

```
... -----
----- Outer L3 Header -----
----- ...
IP Protocol Number : ICMP IP CheckSum : 23308( 0x5B0C ) Destination IP :
10.10.10.10
Source IP : 192.168.10.10
```

```
-----
Contract Lookup Key
-----
```

```
-----
IP Protocol : ICMP( 0x1 )
L4 Src Port : 0( 0x0 )
L4 Dst Port : 56682( 0xDD6A )
sclass (src pcTag) : 10930( 0x2AB2 )
dclass (dst pcTag) : 14( 0xE )
src pcTag is from local table : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet : no
If yes, Contract is not applied here because it is flooded
```

```
-----
Contract Result
-----
```

```
-----
Contract Drop : no
Contract Logging : no
Contract Applied : no
Contract Hit : yes
```

```
Contract Aclqos Stats Index          : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
```

观察到dclass 14已分配。这意味着允许流量通过“permit_override”规则继续，以便消费者枝叶可以驱动最终策略查找。

“消费者”枝叶101

```
Leaf101# vsh_lc
module-1# trigger reset
module-1# trigger init in-select 6 out-select 1
module-1# set outer ipv4 src_ip 192.168.10.10 dst_ip 10.10.10.10
module-1# start
```

```
module-1# ereport
```

```
-----
----- Inner L3 Header -----
----- L3 Type
: IPv4 DSCP : 0 Don't Fragment Bit : 0x0 TTL : 254 IP Protocol Number : ICMP Destination IP
: 10.10.10.10
Source IP          : 192.168.10.10
```

```
Contract Lookup Key
```

```
-----
IP Protocol          : ICMP( 0x1 )
L4 Src Port         : 0( 0x0 )
L4 Dst Port         : 22874( 0x595A )
sclass (src pcTag)  : 10930( 0x2AB2 )
dclass (dst pcTag)  : 18( 0x12 )
src pcTag is from local table      : no
derived from group-id in iVxLAN header of incoming packet
Unknown Unicast / Flood Packet     : no
If yes, Contract is not applied here because it is flooded
```

```
Contract Result
```

```
-----
Contract Drop          : no
Contract Logging       : no
Contract Applied       : yes
Contract Hit           : yes
Contract Aclqos Stats Index : 81874
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874" )
```

TCAM使用率突出显示

在BD到BD方案中，观察到Zoning-Rules增加了一倍，因为EPG-1和EPG-2都是共享服务合同消费者：

```
Leaf101# show zoning-rule scope 3080192
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4117 | 10930 | 0 | implicit | uni-dir | enabled | 3080192 |
deny,log | shsrc_any_any_deny(12) |
| 4129 | 18 | 14 | implicit | uni-dir | enabled | 3080192 |
permit_override | src_dst_any(9) |
| 4128 | 10930 | 18 | 8 | bi-dir | enabled | 3080192 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
| 4127 | 18 | 10930 | 8 | uni-dir-ignore | enabled | 3080192 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Leaf102# **show zoning-rule scope 2260992**

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name |
Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 4113 | 10930 | 14 | implicit | uni-dir | enabled | 2260992 |
permit_override | src_dst_any(9) |
| 4123 | 18 | 10930 | 8 | bi-dir | enabled | 2260992 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
| 4124 | 18 | 0 | implicit | uni-dir | enabled | 2260992 |
deny,log | shsrc_any_any_deny(12) |
| 4122 | 10930 | 18 | 8 | uni-dir-ignore | enabled | 2260992 | PJ:EPG1-EPG2 |
permit | fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

注意：请注意，由于此配置，隐式“shsrc_any_any_deny”和“permit_override” Zoning-Rules的数量也增加了一倍。

结论

这两种配置方案都实现了共享服务功能，但是BD到BD方法需要额外的TCAM消耗。

参考资料和有用的链接

[思科ACI合同指南](#)

[了解ACI Shared Services并对其进行故障排除 — DGTL-TSCDCN-305](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。