ACI L3Out — 子網0.0.0.0/0和系統PcTag 15故障排除

目錄

簡介

本文檔介紹在L3Out EPG中定義0.0.0.0/0子網的PcTag派生。

背景資訊

ACI Contract Guide的「L3Out EPG with 0.0.0.0/0 subnet」部分將0.0.0.0/0與「External Subnets for the External EPG」範圍流量分類總結為：

- 源自L3Out且是匹配到已配置0.0.0.0/0子網的最長字首的流量將分配給VRF PcTag的源類ID（類）。
- 目的地為與已配置的0.0.0.0/0子網匹配的最長字首的L3Out EPG的流量將目標類ID(dclass)分配為15，即系統PcTag。

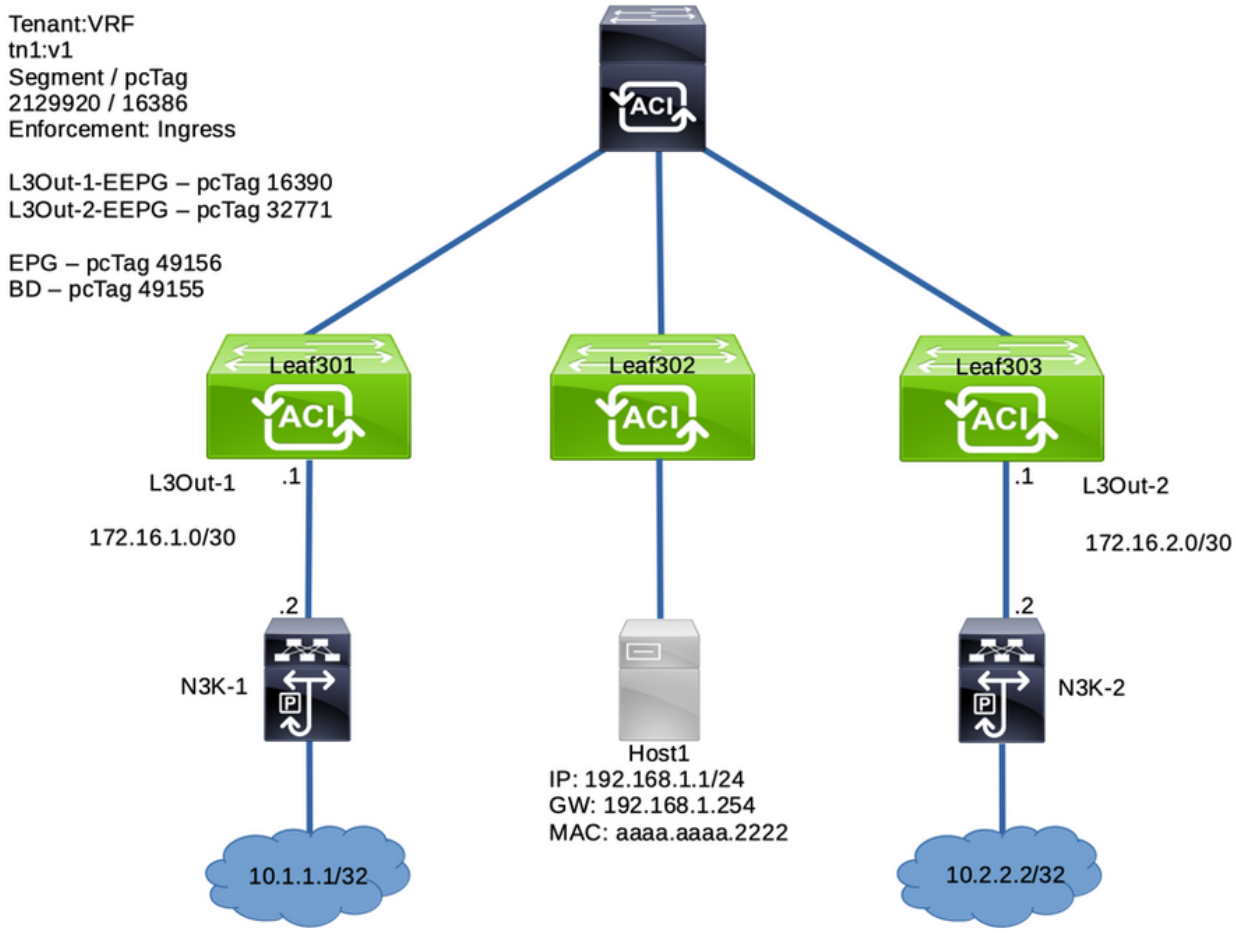
ACI L3Out白皮書的「**An exception for 0.0.0.0/0 with External Subnets for the External EPG**」部分包含一條警告：

"。..儘管不建議這樣做，但您可以在同一VRF中的多個L3Out EPG中使用「外部EPG的子網」配置0.0.0.0/0。 允許此配置時，會發生意外的合約部署……」

本文深入探討這種意想不到的合約部署。

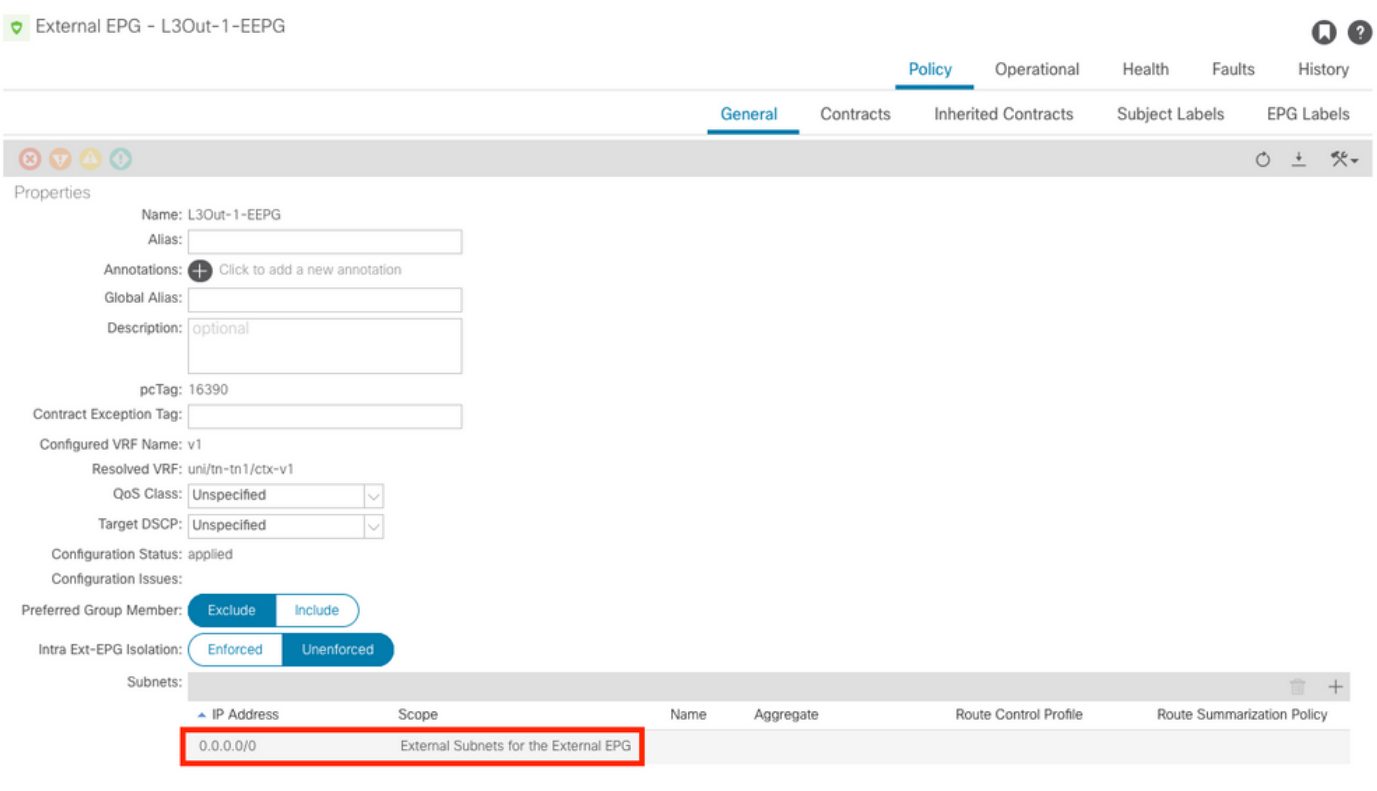
設定

拓撲圖



配置要點

- 枝葉節點301和303是邊界枝葉節點
- 枝葉節點302是非邊界枝葉
- 邊界枝葉301上的L3Out-1-EEPG有一個0.0.0.0/0子網，其中包含「外部EPG的外部子網」
- L3Out-1-EEPG提供合約
- 非邊界枝葉302上的EPG使用相同的合約



驗證

實施「輸入」策略的VRF

非邊界枝葉分割槽規則

如「背景資訊」一節中突出顯示的，發往此L3Out後網路(已配置0.0.0.0/0子網中最長字首匹配項為15的流量將獲得目標類(pcTag)。

這是VRF "v1"(網段ID 2129920)的非邊界枝葉302上的分割槽規則表：

```
Leaf-302#  show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

由於L3Out-1-EEPG和EPG(49156)之間的合約，安裝了兩個規則：

- 規則4112適用於來源為L3Out EPG且目的地為0.0.0.0/0 LPM的外部流量。 流量使用VRF PcTag(16386)和EPG(49156)的類別進行分類。
- 規則4111適用於來源為EPG且目的地為0.0.0.0/0 LPM的L3Out EPG的流量。 流量使用EPG類(49156)和System PcTag 15類分類

邊界枝葉分割槽 — 規則

由於VRF策略實施設定為「輸入」（預設值），邊界枝葉節點301沒有與非邊界枝葉節點302相同的分割槽規則。 這些型別的流的策略應應用於非邊界枝葉節點。

```
Leaf-301# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |  Action  |
Priority       |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
|   4105  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |      |  permit  |
any_any_filter(17)  |
|   4107  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |      | deny,log |
any_any_any(21)     |
|   4106  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |      | deny,log |
any_vrf_any_deny(22) |
|   4108  |   0    | 16387  | implicit | uni-dir | enabled | 2129920 |      |  permit  |
any_dest_any(16)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+

*No entry for 16386 to 49156 , or 49156 to 15*
```

EPG到L3Out ELAM

從EPG端點192.168.1.1 ping L3Out-1-EEPG之後的IP成功：

```
Host# ping 10.1.1.1 count 10000 int 1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=252 time=1.063 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=252 time=0.92 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=252 time=0.963 ms
```

非邊界枝葉302（EPG網關）上的EPG到L3Out流量的ELAM確認：

1. 封包具有預期的來源和目的地IP:源IP:192.168.1.1，目的IP:10.1.1.1
2. 源類（類）是EPG PcTag類**49156**
3. 目的地類別(dclass)為系統PcTag **15**，因為10.1.1.0/24最長字首匹配L3Out-1-EEPG上的0.0.0.0/0子網
4. 在此節點302（非邊界枝葉節點）上應用了策略。

```
Leaf-302# ereport
================================================================================================================
============================================================
                                                                    Captured Packet
================================================================================================================
============================================================
...snip...
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Outer L2 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Destination MAC               : 0022.BDF8.19FF
Source MAC                    : AAAA.AAAA.2222
802.1Q tag is valid           : yes( 0x1 )
CoS                           : 0( 0x0 )
Access Encap VLAN             : 192( 0xC0 )

----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
L3 Type                       : IPv4
...
IP Protocol Number            : ICMP
IP CheckSum                   : 63781( 0xF925 )
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1
...
================================================================================================================
============================================================
                                                                Contract Lookup ( FPC )
================================================================================================================
============================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 2048( 0x800 )
L4 Dst Port                           : 43014( 0xA806 )
sclass (src pcTag)                    : 49156( 0xC004 )
dclass (dst pcTag)                    : 15( 0xF )
src pcTag is from local table         : yes
...

----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Drop                         : no
Contract Logging                      : no
Contract Applied                      : yes
Contract Hit                          : yes
Contract Aclqos Stats Index           : 81875
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875" )
```

可以輸入ereport提供的命令，以便進一步驗證所命中的Zoning-Rule:

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875"
========================================
Rule ID: 4111 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 46 | hw_index = 45 | stats_idx = 81875

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81875
```

L3Out到EPG ELAM

返回流將策略應用於非邊界枝葉節點302。當VRF策略實施設定為「輸入」時，這是預期情況。

```
Leaf-302# ereport
...
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
Inner L3 Header
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                      : IPv4
DSCP                         : 0
Don't Fragment Bit           : 0x0
TTL                          : 254
IP Protocol Number           : ICMP
Destination IP               : 192.168.1.1
Source IP                    : 10.1.1.1

=================================================================================================
=====================================================
                                                                    Contract Lookup ( FPC )
=================================================================================================
=====================================================

-------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                             : ICMP( 0x1 )
L4 Src Port                             : 0( 0x0 )
L4 Dst Port                             : 60691( 0xED13 )
sclass (src pcTag)                      : 16386( 0x4002 )
dclass (dst pcTag)                      : 49156( 0xC004 )
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" )
```

進一步驗證：

```
module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
========================================
Rule ID: 4112 Scope 6 Src EPG: 16386 Dst EPG: 49156 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
module-1(DBG-elam-insel14)#
```

實施「出口」策略的VRF

非邊界枝葉分割槽規則

當VRF策略實施設定為「輸出」時，L3Out的合約規則將部署在邊界枝葉節點和非邊界枝葉節點上。因此，與「輸入」實施相比，此配置會消耗額外的TCAM空間。此組態不是預設值，若使用，必須慎重考慮。

非邊界枝葉節點302有兩個分割槽規則，每個流方向性一個：

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name      |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                 |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                 |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                 |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                 |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

邊界枝葉分割槽 — 規則

通過「出口」策略實施，Border Leaf Node 301還有另外兩個分割槽規則：

```
Leaf-301# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name      |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
|   4105  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                 |
permit  |  any_any_filter(17)  |
|   4107  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                 |
deny,log |   any_any_any(21)    |
|   4106  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                 |
deny,log | any_vrf_any_deny(22) |
|   4108  |   0    | 16387  | implicit | uni-dir | enabled | 2129920 |                 |
permit  |   any_dest_any(16)   |
|   4109  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4110  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

EPG到L3Out ELAM

從終端192.168.1.1 ping L3Out背後的網路成功：

```
Host# ping 10.1.1.1 count 10000 int 1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=252 time=1.319 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=252 time=0.962 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=252 time=0.958 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=252 time=1.093 ms
```

非邊界枝葉節點302上的ELAM表示未在**此枝葉上應**用策略。此外，它還選擇了System PcTag 1類，以允許流命中流中的下一個葉節點：

```
Leaf-302# ereport
================================================================================================
=================================================
                                                                    Captured Packet

------------------------------------------------------------------------------------------------
-------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------
-------------------------------------------------
...
IP Protocol Number            : ICMP
IP CheckSum                   : 26943( 0x693F )
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1

================================================================================================
=================================================
                                                                      Contract Lookup ( FPC )
================================================================================================
=================================================
```

```
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 27360( 0x6AE0 )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 1( 0x1 )
...

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Drop                            : no
Contract Logging                         : no
Contract Applied                         : no
Contract Hit                             : yes
Contract Aclqos Stats Index              : 81903
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81903" )
```

邊界枝葉節點301上的ELAM指示該**節點上應用了策略**。它還選擇了**系統PcTag 15類。這表示0.0.0.0/0 L3Out子網條目上匹配的最長字首：**

```
Leaf-301# ereport
================================================================================================
================================================
                                                                  Captured Packet
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------
...
IP Protocol Number            : ICMP
Destination IP                : 10.1.1.1
Source IP                     : 192.168.1.1

================================================================================================
================================================
                                                                      Contract Lookup ( FPC )
================================================================================================
================================================

------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 40498( 0x9E32 )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 15( 0xF )
```

```
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" )
...

module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
=========================================
Rule ID: 4110 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
```

L3Out到EPG ELAM

此設定中的返回流存在警告：

- 邊界枝葉節點301沒有針對192.168.1.1的終端學習。

```
Leaf-301# show endpoint ip 192.168.1.1
Legend:
S - static s - arp L - local O - peer-attached
V - vpc-attached a - local-aged p - peer-aged M - span
B - bounce H - vtep R - peer-attached-rl D - bounce-to-proxy
E - shared-service m - svc-mgr
+-----------------------------------+---------------+-----------------+--------------+----------
---+
VLAN/ Encap MAC Address MAC Info/ Interface
Domain VLAN IP Address IP Info
+-----------------------------------+---------------+-----------------+--------------+----------
---+
...empty...
```

因此，未針對此流在邊界枝葉節點301上應用策略，必須隱式允許它到達下一個枝葉：

```
Leaf-301# ereport
=================================================================================================
=====================================================
                                                                  Captured Packet
=================================================================================================
=====================================================
-------------------------------------------------------------------------------------------------
-----------------------------------------------------
```

```
Outer L3 Header
------------------------------------------------------------------------------------------------------
------------------------------------------------------
...
IP Protocol Number            : ICMP
IP CheckSum                   : 25157( 0x6245 )
Destination IP                : 192.168.1.1
Source IP                     : 10.1.1.1

======================================================================================================
======================================================
                                                                    Contract Lookup ( FPC )
======================================================================================================
======================================================

------------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------------
------------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 0( 0x0 )
L4 Dst Port                           : 33570( 0x8322 )
sclass (src pcTag)                    : 16386( 0x4002 )
dclass (dst pcTag)                    : 1( 0x1 )
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           : 81903
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81903" )
```

相反，策略應用於非邊界枝葉節點302:

```
Leaf-302# ereport
======================================================================================================
======================================================
                                                                    Captured Packet
======================================================================================================
======================================================

------------------------------------------------------------------------------------------------------
------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------------
------------------------------------------------------
...
IP Protocol Number            : ICMP
Destination IP                : 192.168.1.1
Source IP                     : 10.1.1.1

======================================================================================================
```

```
=====================================================
                                                                    Contract Lookup ( FPC )
=========================================================================================================
=====================================================

---------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
---------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                           : ICMP( 0x1 )
L4 Src Port                           : 0( 0x0 )
L4 Dst Port                           : 61057( 0xEE81 )
sclass (src pcTag)                    : 16386( 0x4002 )
dclass (dst pcTag)                    : 49156( 0xC004 )
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" )
...

module-1(DBG-elam-insel14)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81874"
=========================================
Rule ID: 4112 Scope 6 Src EPG: 16386 Dst EPG: 49156 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 47 | hw_index = 46 | stats_idx = 81874

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81874
```

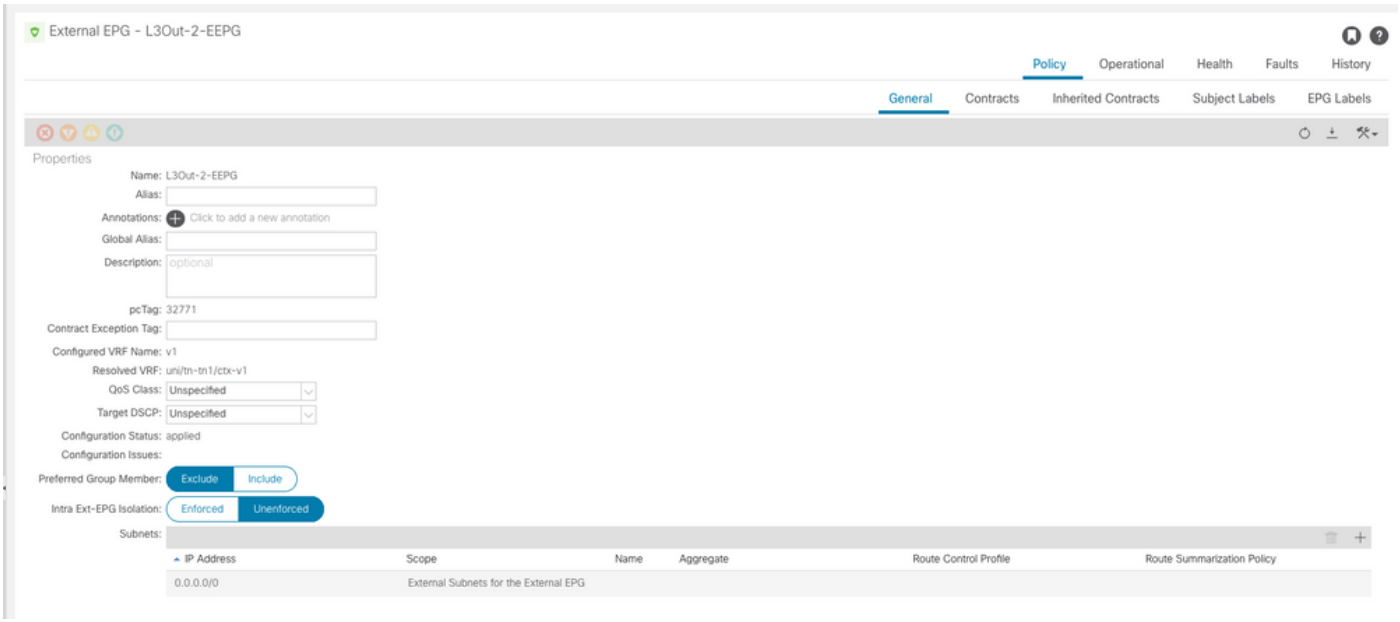
如果邊界枝葉節點301具有終端獲知192.168.1.1，則在該節點上應用策略。

疑難排解

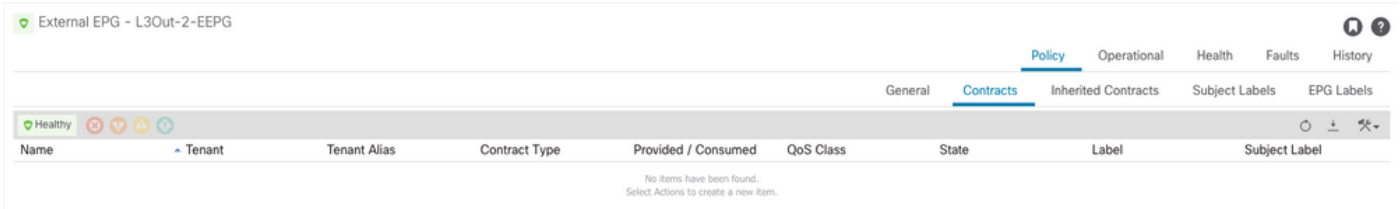
場景 — 意外允許

0.0.0/0如果部署在同一VRF中配置了多個L3Outs，且子網中配置了「外部EPG的外部子網」，則會允許流量意外傳遞到外部目標。

為此，請在L3Out-2-EEPG下新增0.0.0.0/0子網，該子網與L3Out-1-EEPG位於同一VRF中。



在L3Out-2-EEPG上沒有合約，因此我們預計預設情況下所有流量都會被丟棄：



但是，從EPG端點192.168.1.1 ping L3Out-2-EEPG後的目的地10.2.2.2成功。這是意外的！

```
Host# ping 10.2.2.2
PING 10.2.2.2 (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=252 time=0.881 ms
64 bytes from 10.2.2.2: icmp_seq=1 ttl=252 time=0.801 ms
64 bytes from 10.2.2.2: icmp_seq=2 ttl=252 time=0.877 ms
64 bytes from 10.2.2.2: icmp_seq=3 ttl=252 time=0.827 ms
```

轉發路由和policy-mgr字首都顯示此VRF中目的地為10.2.2.2的流量被分配系統PcTag 15

```
Leaf-302# vsh_lc -c "show forward route 10.2.2.2 platform vrf tn1:v1"
...
Policy Prefix 0.0.0.0/0

SDK Information:
vrf: 7(0x7), routed_if: 0x0 epc_class: 15(0xf)
...


Leaf-302# vsh -c "show system internal policy-mgr prefix"
Requested prefix data

Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                        Addr
Class Shared Remote Complete Svc_ena
======= ======  ===========  =======  ============================
================================ ====== ====== ====== ======== ========
...
2129920 7      0x7           Up     tn1:v1
0.0.0.0/0    15       False  False  False    False
```

```
2129920 7      0x80000007    Up     tn1:v1
::/0   15      False  False  False    False

Leaf-302#
```

非邊界枝葉節點302上的ELAM驗證使用系統PcTag 15類對流量進行分類。

```
Leaf-302# ereport
================================================================================================================
========================================================= Captured Packet
================================================================================================================
========================================================= ----------------------------------------
----------------------------------------------------------------------------------------------------------------
------------- Outer L3 Header ------------------------------------------------------------------
---------------------------------------------------------------------------------- ... IP
Protocol Number : ICMP IP CheckSum : 14444( 0x386C ) Destination IP                : 10.2.2.2
Source IP                      : 192.168.1.1

================================================================================================================
================================================================
                                                                          Contract Lookup ( FPC )
================================================================================================================
================================================================

----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 33134( 0x816E )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 15( 0xF )
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              : 81875
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875" )
...

module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81875"
========================================
Rule ID: 4111 Scope 6 Src EPG: 49156 Dst EPG: 15 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 46 | hw_index = 45 | stats_idx = 81875

  Curr TCAM resource:
  ============================
    === SDK Info ===
```

```
        Result/Stats Idx: 81875
```

VRF "v1"的分割槽規則未顯示EPG和L3Out-2的任何新條目：

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name      |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
|   4107  |   0    |   0    | implarp  | uni-dir | enabled | 2129920 |                 |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit | uni-dir | enabled | 2129920 |                 |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit | uni-dir | enabled | 2129920 |                 |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit | uni-dir | enabled | 2129920 |                 |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  | uni-dir | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
Leaf-302#
```

由於L3Out-2-EEPG僅配置了0.0.0.0/0子網，因此所有發往它的流量都使用System PcTag 15分類進行分類。

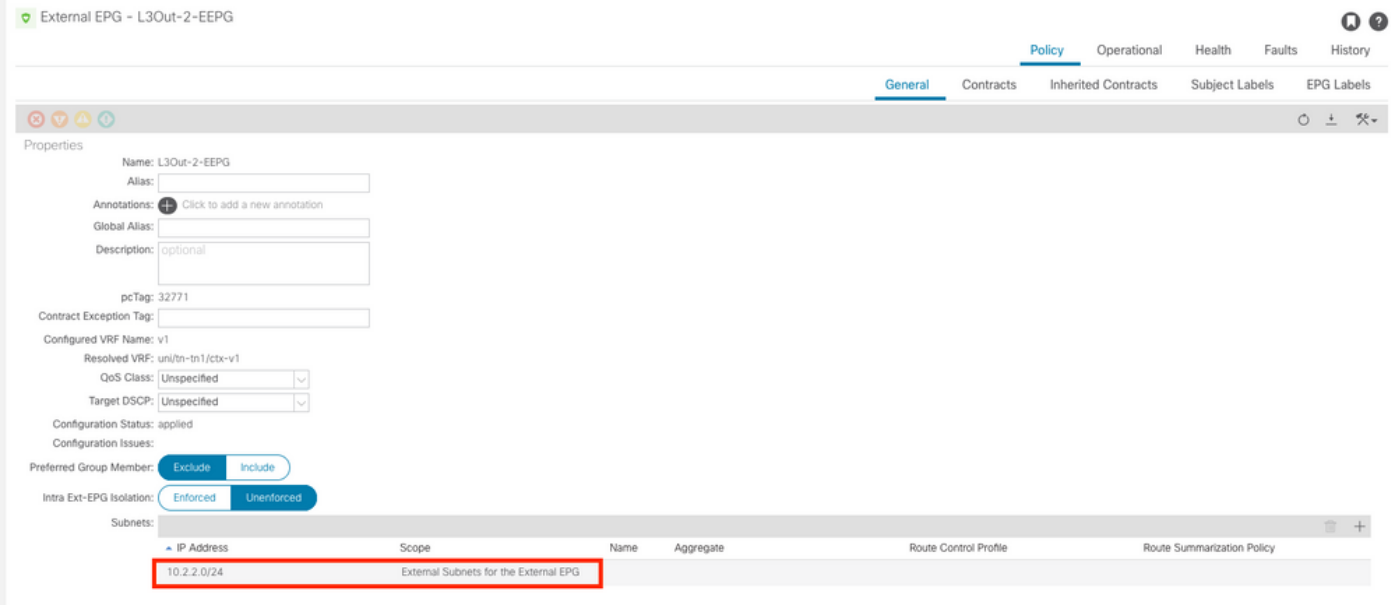
Zoning-Rules ID 4111和4112被程式設計為L3Out-1-EEPG具有0.0.0.0/0子網並提供EPG使用的合約。

由於此配置，意外地允許到L3Out-2-EEPG的流！

解決方案 — 無意允許

要防止此行為，請執行以下操作：

1. 強烈建議每個VRF僅對一個L3Out EPG使用0.0.0.0/0子網
2. 如有可能，在同一VRF中的其他L3Out使用特定子網。這允許流量將唯一的L3Out PcTag值提取為其類。



應用這些更改以緩解意外允許：

1. 在L3Out-2-EEPG上，將0.0.0.0/0子網替換為10.2.2.0/24子網
2. 在L3Out-2-EEPG上，提供合約
3. 在EPG上，使用相同的合約

完成後，在非邊界枝葉節點302上觀察這些更改：

- 對於10.2.2.0/24，有一個更具體的policy-mgr字首與L3Out-2-EEPG PcTag連線關32771
- 有一個Zoning-Rules ID 4109條目 此條目允許從EPG PcTag到491563Out-2-EEPG PcTag的流32771
- 有一個Zoning-Rules ID 4110條目 此條目允許從L3Out-2-EEPG PcTag到EPG 32771的流49156

更新的轉發路由和policy-mgr字首，其中顯示10.2.2.2分配了32771的L3Out-2-EEPG PgTag:

```
Leaf-302# vsh_lc -c "show forward route 10.2.2.2 platform vrf tn1:v1"
...
Policy Prefix 10.2.2.0/24
...
SDK Information:
vrf: 7(0x7), routed_if: 0x0 epc_class: 32771(0x8003)
attributes: SUP_CP DST_POL_IC SRC_POL_IC

Leaf-302# vsh -c "show system internal policy-mgr prefix"
Requested prefix data

Vrf-Vni VRF-Id Table-Id Table-State  VRF-Name                        Addr
Class Shared Remote Complete Svc_ena
======= ======  =========== =======  ============================
================================= ====== ====== ====== ======== ========
...
2129920 7      0x7           Up     tn1:v1
0.0.0.0/0   15      False  False  False    False
2129920 7      0x80000007    Up     tn1:v1
::/0   15      False  False  False    False
2129920 7      0x7           Up     tn1:v1
10.2.2.0/24  32771   False  True   False    False
```

附註：Zoning-Rules ID 4111和4112仍然存在於非邊界枝葉節點302上，因為L3Out-1-EEPG仍然具有0.0.0.0/0子網，並且與EPG存在合約關係。但是，L3Out-2-EEPG流量不再在不經意間使用這些規則，因為其流量現在使用L3Out PcTag進行分類，而不是使用System PcTag 15:

```
Leaf-302# show zoning-rule scope 2129920
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
|   4107  |   0    |   0    | implarp  |    uni-dir     | enabled | 2129920 |                  |
permit  |  any_any_filter(17)  |
|   4106  |   0    |   0    | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log |   any_any_any(21)    |
|   4105  |   0    | 49155  | implicit |    uni-dir     | enabled | 2129920 |                  |
permit  |   any_dest_any(16)   |
|   4108  |   0    |   15   | implicit |    uni-dir     | enabled | 2129920 |                  |
deny,log | any_vrf_any_deny(22) |
|   4112  | 16386  | 49156  | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4111  | 49156  |   15   | default  |    uni-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4109  | 49156  | 32771  | default  |     bi-dir     | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
|   4110  | 32771  | 49156  | default  | uni-dir-ignore | enabled | 2129920 | tn1:EPG_to_L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

從EPG主機ping L3Out-2-EEPG後的外部目標成功：

```
Host# ping 10.2.2.2
PING 10.2.2.2 (10.2.2.2): 56 data bytes
64 bytes from 10.2.2.2: icmp_seq=0 ttl=252 time=0.854 ms
64 bytes from 10.2.2.2: icmp_seq=1 ttl=252 time=0.669 ms
64 bytes from 10.2.2.2: icmp_seq=2 ttl=252 time=0.716 ms
64 bytes from 10.2.2.2: icmp_seq=3 ttl=252 time=0.669 ms
64 bytes from 10.2.2.2: icmp_seq=4 ttl=252 time=0.666 ms
```

非邊界枝葉節點302上icmp請求的ELAM指示該類現在為32771 - L3Out-2-EEPG的PcTag。

```
Leaf-302# ereport
================================================================================================
=====================================================
                                                          Captured Packet
================================================================================================
=====================================================
------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
------------------------------------------------------------------------------------------------
-----------------------------------------------------
...
IP Protocol Number : ICMP
IP CheckSum : 4095( 0xFFF )
Destination IP : 10.2.2.2
```

```
Source IP : 192.168.1.1

================================================================================================================
================================================
                                                                        Contract Lookup ( FPC )
================================================================================================================
================================================
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 49837( 0xC2AD )
sclass (src pcTag)                       : 49156( 0xC004 )
dclass (dst pcTag)                       : 32771( 0x8003 )
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              : 81873
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873" )
...
```

ereport提供的aclqos命令顯示此流命中了一個新的分割槽規則，特別是規則ID 4109:

```
module-1(DBG-elam-insel6)# show sys int aclqos zoning-rules | grep -B 9 "Idx: 81873"
========================================
Rule ID: 4109 Scope 6 Src EPG: 49156 Dst EPG: 32771 Filter 65535
    unit_id: 0
    === Region priority: 2462 (rule prio: 9 entry: 158)===
        sw_index = 48 | hw_index = 47 | stats_idx = 81873

  Curr TCAM resource:
  ============================
    === SDK Info ===
        Result/Stats Idx: 81873
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。