Dépannage de l'ACI L3Out - Subnet 0.0.0.0/0 et System PcTag 15

Contenu

Introduction

Ce document décrit la dérivation PcTag du sous-réseau 0.0.0.0/0 lorsqu'il est défini dans un EPG L3Out.

Informations générales

La section **"L3Out EPG with 0.0.0.0/0 subnet"** du Guide de contrat ACI résume 0.0.0.0/0 avec "External Subnets for the External EPG" scope traffic classification as:

- Le trafic provenant d'un L3Out dont le préfixe est le plus long et correspondant à un sous-réseau 0.0.0.0/0 configuré se voit attribuer l'ID de classe source (sclass) du PcTag VRF.
- Le trafic destiné à un EPG L3Out dont le préfixe le plus long correspond à un sous-réseau 0.0.0.0/0 configuré se voit attribuer l'ID de classe de destination (dclass) de 15, un System PcTag.

La section **« Une exception pour 0.0.0.0/0 avec des sous-réseaux externes pour l'EPG externe »** du livre blanc ACI L3Out contient un avertissement :

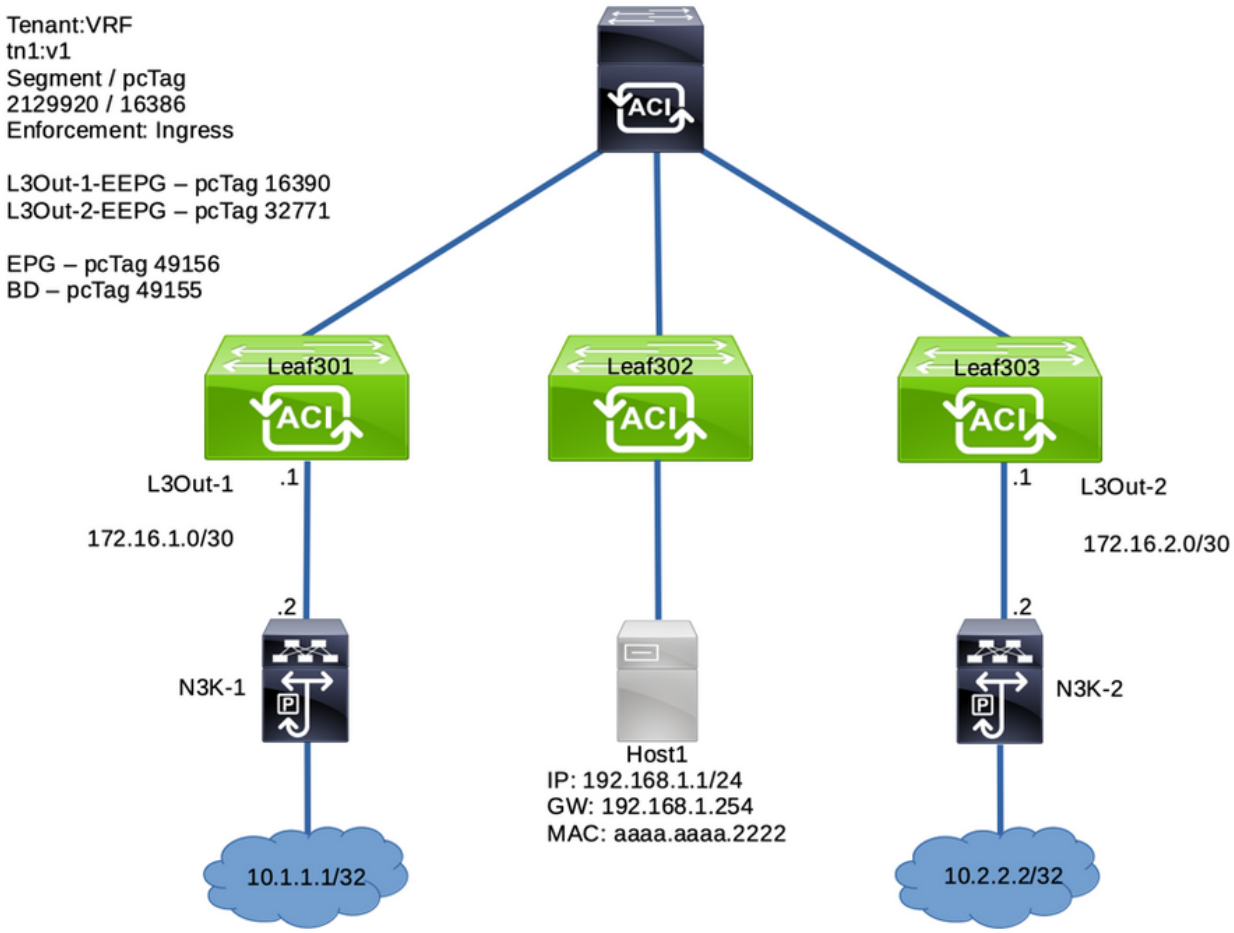
"...Bien que ce ne soit pas recommandé, vous pouvez configurer 0.0.0.0/0 avec 'Sous-réseaux

externes pour l'EPG externe' dans plusieurs EPG L3Out dans le même VRF... Bien que cette configuration soit autorisée, un déploiement de contrat imprévu se produit..."

Cet article traite de ce déploiement de contrat imprévu.

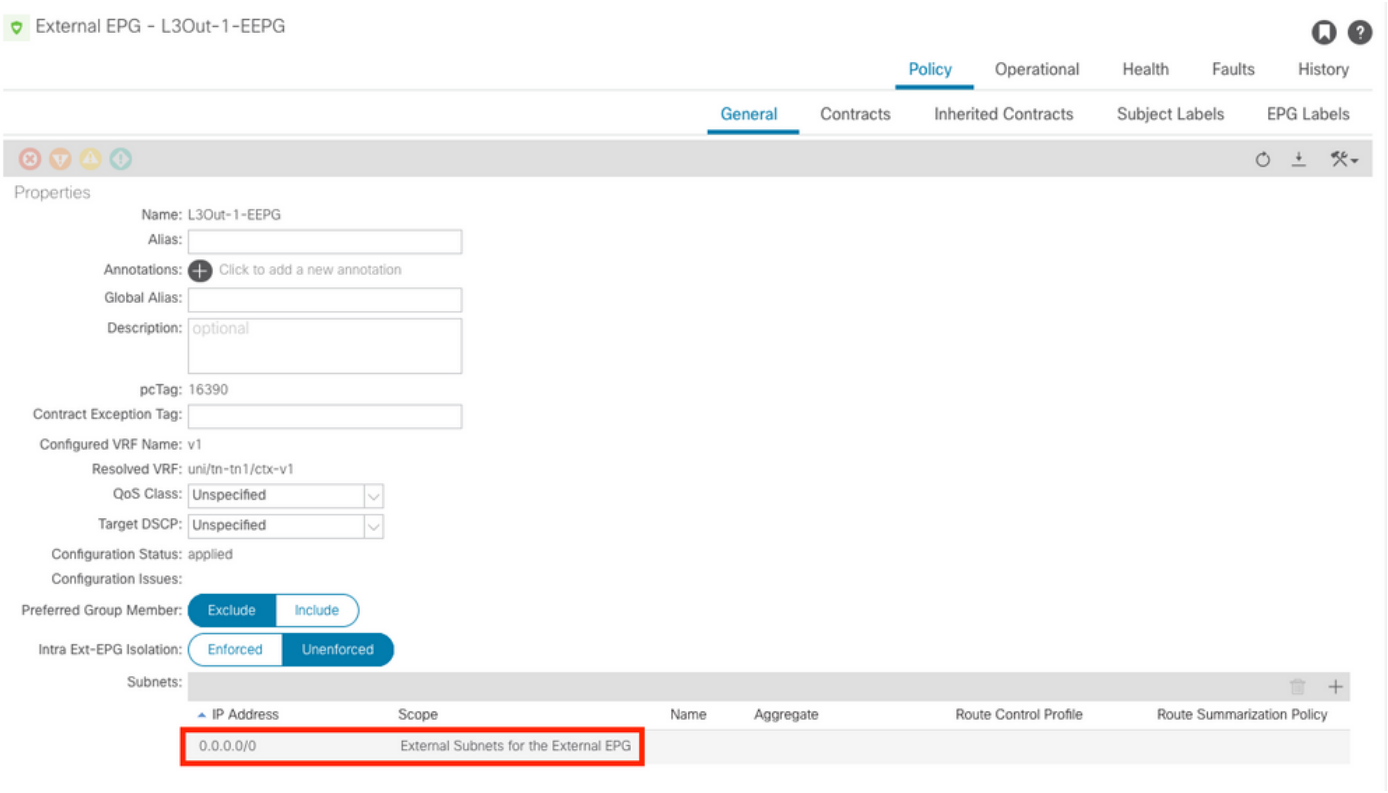
Configuration

Schéma de topologie



Points forts de configuration

- Les noeuds leaf 301 et 303 sont des noeuds leaf en limite
- Le noeud leaf 302 est un leaf non en limite
- L3Out-1-EEPG, sur le leaf en limite 301, a un sous-réseau 0.0.0.0/0 avec « Sous-réseaux externes pour l'EPG externe »
- L3Out-1-EEPG fournit un contrat
- EPG, sur Non-Border Leaf 302, utilise le même contrat



Vérification

VRF avec application de la stratégie « en entrée »

Zonage de feuille non-frontalier-Règles

Comme indiqué dans la section Informations d'arrière-plan, le trafic destiné aux réseaux derrière cette L3Out dont le préfixe correspond le plus longtemps sur le sous-réseau 0.0.0.0/0 configuré obtient une classe de destination (pcTag) de 15.

Voici la table des règles de zonage sur le leaf 302 non frontalier pour VRF "v1" (ID de segment 2129920) :

```
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)    |
```

```
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

Deux règles sont installées suite au contrat conclu entre L3Out-1-EEPG et EPG (49156) :

- La règle 4112 s'applique au trafic externe provenant de l'EPG L3Out avec 0.0.0.0/0 LPM destiné à l'EPG. Le flux de trafic est classifié avec la classe de la balise VRF PcTag (16386) et la dclass de l'EPG (49156) .
- La règle 4111 concerne le trafic provenant de l'EPG destiné à l'EPG L3Out avec 0.0.0.0/0 LPM. Le flux de trafic est classé avec la classe de l'EPG (49156) et la dclass de System PcTag 15

Zonage des leafs en limite - Règles

Le noeud leaf en limite 301 n'a pas les mêmes règles de zonage que le noeud leaf non en limite 302 en raison de l'application de la stratégie VRF définie sur « Ingress » (Entrée) (valeur par défaut). La politique relative à ces types de flux devrait être appliquée aux noeuds leaf non frontaliers.

```
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 vers L3Out ELAM

Une requête ping du point d'extrémité EPG 192.168.1.1 vers l'IP derrière L3Out-1-EEPG a abouti :

```
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
```

Un ELAM pour le trafic EPG vers L3Out sur le Leaf 302 non frontalier (passerelle EPG) confirme :

1. Le paquet a les adresses IP source et de destination attendues : IP source : 192.168.1.1, IP

de destination : 10.1.1.1

2. La classe source (sclass) est l'EPG PcTag **49156**
3. La classe de destination (dclass) est System PcTag **15**, car le préfixe 10.1.1.0/24 le plus long correspond au sous-réseau 0.0.0.0/0 sur L3Out-1-EEPG
4. La stratégie a été appliquée à ce noeud 302, le noeud leaf non périphérique.

```
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" )
```

La commande donnée par ereport peut être entrée pour une validation supplémentaire de la règle de zonage qui a été atteinte :

```
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 vers EPG ELAM

Le flux de retour obtient une stratégie appliquée sur le noeud leaf non frontalier 302. Ceci est attendu lorsque l'application de la stratégie VRF est définie sur « Entrée ».

```
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" )
```

Validation supplémentaire :

```
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)#
```

VRF avec application de la stratégie de sortie

Zonage de feuille non-frontalier-Règles

Lorsque l'application de la stratégie VRF est définie sur « Egress » (Sortie), les règles de contrat d'une L3Out sont déployées sur les noeuds leaf en limite et non en limite. Par conséquent, cette configuration consomme de l'espace TCAM supplémentaire par rapport à l'application « en entrée ». Cette configuration n'est pas la valeur par défaut et, si elle est utilisée, elle doit être étudiée attentivement.

Le noeud leaf non frontalier 302 a deux règles de zonage, une par directionnalité de flux :

```
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)    |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
```

Zonage des leafs en limite - Règles

Avec l'application de la politique de « sortie », le noeud de périphérie 301 dispose également de deux règles de zonage supplémentaires :

```
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 vers L3Out ELAM

Une requête ping du point d'extrémité 192.168.1.1 vers le réseau derrière L3Out aboutit :

```
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
```

Le module ELAM sur le noeud leaf non frontalier 302 indique que la **politique n'a pas été appliquée** sur ce noeud leaf. En outre, il a pris une dclass de **System PcTag 1** pour permettre au flux d'atteindre le noeud leaf suivant dans le flux :

```
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" )
```

L'ELAM sur le noeud leaf en limite 301 indique que la **stratégie a été appliquée sur ce noeud**. Il a également récupéré une dclass de **System PcTag 15.** Cela signifie qu'il correspond au préfixe le plus long sur l'entrée de sous-réseau 0.0.0.0/0 L3Out :

```
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 vers EPG ELAM

Il y a un avertissement avec le flux de retour dans cette configuration :

- Le noeud leaf en limite 301 n'a pas de point de terminaison d'apprentissage pour 192.168.1.1.

```
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...
```

Par conséquent, la politique n'est pas appliquée au noeud leaf en limite 301 pour ce flux et il doit être implicitement autorisé à atteindre le leaf suivant :

```
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" )
```

Au lieu de cela, la stratégie est appliquée au noeud leaf non frontalier 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
```

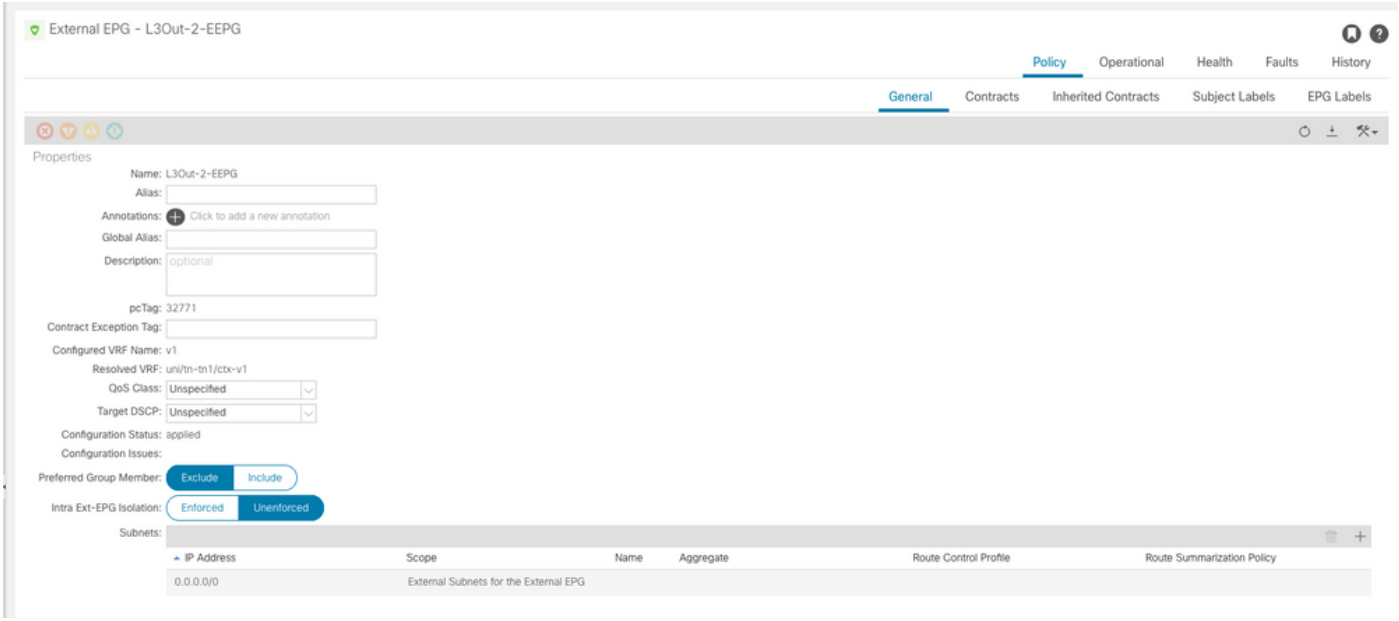
Si le noeud leaf en limite 301 avait un point de terminaison apprendre 192.168.1.1, la politique aurait été appliquée sur ce noeud.

Dépannage

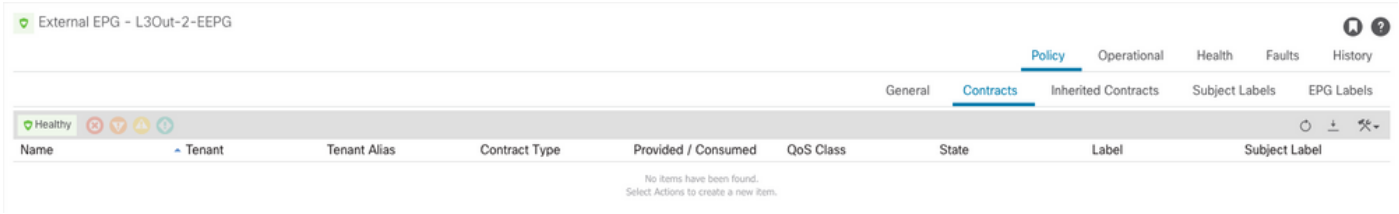
Scénario - Autorisations non intentionnelles

Un déploiement avec plusieurs sorties L3 dans le même VRF configuré avec le sous-réseau 0.0.0.0/0 avec « Sous-réseaux externes pour l'EPG externe » peut permettre au trafic de passer à des destinations externes de manière inattendue.

Pour ce faire, ajoutez le sous-réseau 0.0.0.0/0 sous L3Out-2-EEPG qui se trouve dans le même VRF que L3Out-1-EEPG.



Il n'y a aucun contrat sur L3Out-2-EEPG, nous nous attendons donc à ce que tout le trafic soit abandonné par défaut :



Cependant, une requête ping du point de terminaison EPG 192.168.1.1 vers la destination 10.2.2.2 derrière L3Out-2-EEPG aboutit. C'est inattendu !

```
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
```

La route de transfert et le préfixe policy-mgr indiquent que le trafic destiné à 10.2.2.2 dans ce VRF est affecté à System 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#
```

Un ELAM sur le noeud leaf non frontalier 302 valide que le trafic est classé avec une dclass de System PcTag 15.

```
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
```

Les règles de zonage pour VRF "v1" n'affichent aucune nouvelle entrée pour EPG et L3Out-2 :

```
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#
```

Comme le sous-réseau 0.0.0.0/0 est configuré pour L3Out-2-EEPG uniquement, tout le trafic qui lui est destiné est classé avec dclass de System PcTag 15.

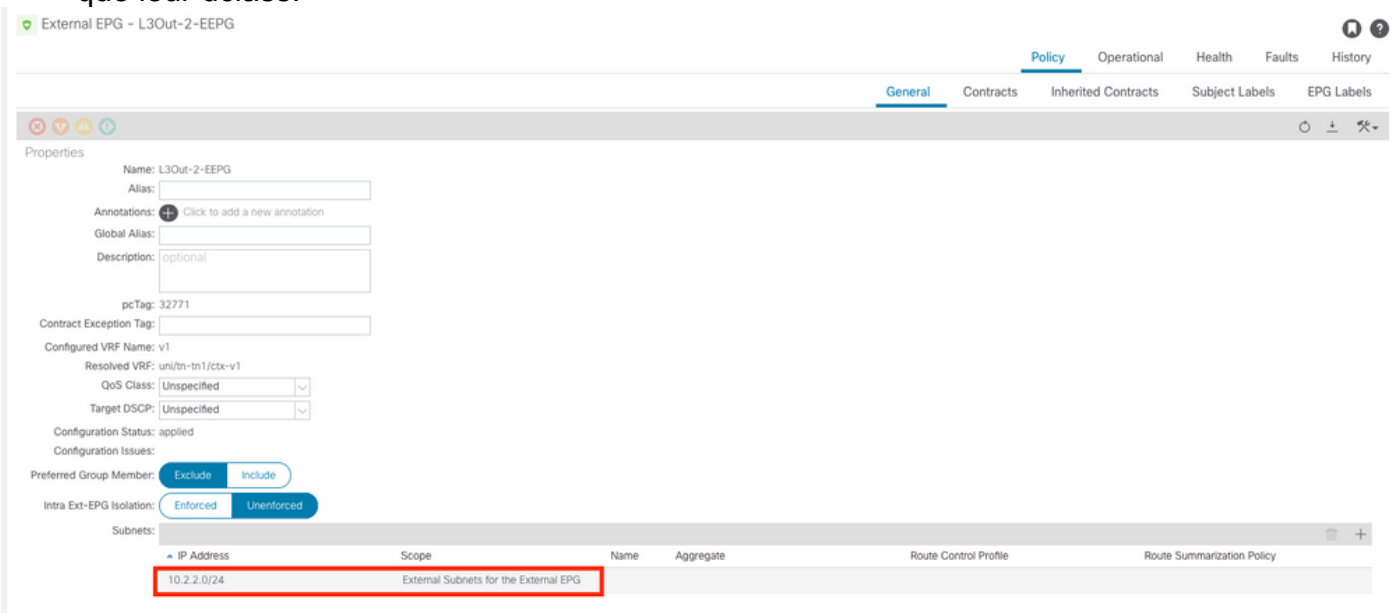
Les ID de règles de zonage 4111 et 4112 sont programmés car L3Out-1-EEPG possède le sous-réseau 0.0.0.0/0 et fournit un contrat qui est utilisé par EPG.

Les flux vers L3Out-2-EEPG sont inopinément autorisés en raison de cette configuration !

Solution - Autorisations imprévues

Pour empêcher ce comportement :

1. Il est fortement recommandé d'utiliser uniquement le sous-réseau 0.0.0.0/0 sur un EPG L3Out par VRF
2. Dans la mesure du possible, utilisez des sous-réseaux spécifiques pour d'autres sorties L3 dans le même VRF. Cela permet au trafic d'extraire les valeurs uniques L3Out PcTag en tant que leur dclass.



Appliquez ces modifications pour atténuer les imprévus autoriser :

1. Sur L3Out-2-EEPG, remplacez le sous-réseau 0.0.0.0/0 par un sous-réseau 10.2.2.0/24
2. Sur L3Out-2-EEPG, fournissez un contrat
3. Sur EPG, utilisez le même contrat

Une fois terminé, observez ces modifications sur le noeud leaf non frontalier 302 :

- Il existe un préfixe policy-mgr plus spécifique pour 10.2.2.0/24 lié à L3Out-2-EEPG PcTag 32771
- Il existe une entrée Zoning-Rules ID 4109 Cette entrée autorise un flux de EPG PcTag 49156 vers L3Out-2-EEPG PcTag 32771
- Il existe une entrée Zoning-Rules ID 4110 Cette entrée autorise un flux de L3Out-2-EEPG PcTag 32771 vers EPG PcTag 49156

La route de transfert mise à jour et le préfixe policy-mgr qui montrent que 10.2.2.2 se voit attribuer la balise PgTag L3Out-2-EEPG de 32771 :

```
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
```

Note: Les ID de règles de zonage 4111 et 4112 existent toujours sur le noeud leaf non frontalier 302, car L3Out-1-EEPG possède toujours le sous-réseau 0.0.0.0/0 et entretient également une relation contractuelle avec EPG. Cependant, le trafic L3Out-2-EEPG n'utilise plus ces règles par inadvertance, car son trafic est maintenant classé avec l'étiquette de PC L3Out, et non avec l'étiquette de PC système 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)    |
+---------+--------+--------+----------+----------------+---------+---------+------------------
+----------+----------------------+
```

La commande ping de l'hôte EPG vers la destination externe derrière L3Out-2-EEPG a réussi :

```
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
```

L'ELAM de la requête ICMP sur le noeud leaf non-Border 302 indique que dclass est maintenant 32771 - le PcTag de L3Out-2-EEPG.

```
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" )
...
```

La commande ereport provided aclqos montre que ce flux atteint l'une des nouvelles règles de zonage, en particulier l'ID de règle 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.