# Configurer la liste des exceptions Rogue/COOP dans l'ACI

## Table des matières


Introduction

- Pourquoi une liste d'exceptions ?
- Solution

Prérequis

Configuration de la liste d'exceptions Rogue/COOP

Vérification


## Introduction

Ce document décrit la fonctionnalité Liste des exceptions Rogue/COOP dans l'ACI (Infrastructure axée sur les applications) et couvre la configuration et la vérification.

### Pourquoi une liste d'exceptions ?

La fonctionnalité "Rogue EP Control" de l'ACI minimise l'impact des boucles temporaires en mettant en quarantaine les points d'extrémité dans le domaine de pont spécifique où elles se produisent. Cependant, cette fonctionnalité peut parfois provoquer des interruptions inutiles. Par exemple, lors d'un basculement de pare-feu, les deux pare-feu peuvent transmettre momentanément le trafic en utilisant la même adresse MAC (Media Access Control), ce qui entraîne des problèmes jusqu'à ce que le réseau converge. Avant la version 5.2(3), si l'ACI détecte 4 déplacements d'EP (terminal) en 60 secondes, elle est alors rendue statique et ne peut plus bouger pendant les 30 minutes suivantes. 4 déplacements en 60 secondes peuvent être réalistes dans certains déploiements. Le temps d'attente de 30 minutes est agressif dans les scénarios où des déplacements EP sont attendus.

### Solution

Afin de résoudre ce problème, il est possible de configurer une «Liste d'exceptions Rogue/COOP.» MAC dans la liste des exceptions, il utilise ensuite un seuil plus élevé pour détecter les adresses non autorisées. L'adresse MAC configurée dans la liste d'exceptions devient indésirable après 3 000 déplacements dans un intervalle de 10 minutes.MAC dans la liste d'exceptions utilise un seuil d'amortissement COOP (Council of Oracle Protocol) plus élevé pour éviter d'être amortie dans COOP. Vous pouvez ajouter jusqu'à 100 adresses MAC dans la liste des exceptions.

## Prérequis

- Cette fonctionnalité est disponible à partir de la version 5.2(3)
- Cette option ne peut être utilisée que si le BD (domaine de pont) est un BD de couche 2 (comme si le BD n'était pas configuré pour le routage IP)
- La fonctionnalité des systèmes non fiables doit être activée pour que le comportement Liste des exceptions non fiables fonctionne.

## Configuration de la liste d'exceptions Rogue/COOP

Cette fonctionnalité peut être utilisée dans les domaines de pont de couche 2 (BD de couche 2) pour empêcher des adresses MAC spécifiques d'être marquées comme indésirables en raison de mouvements légitimes.

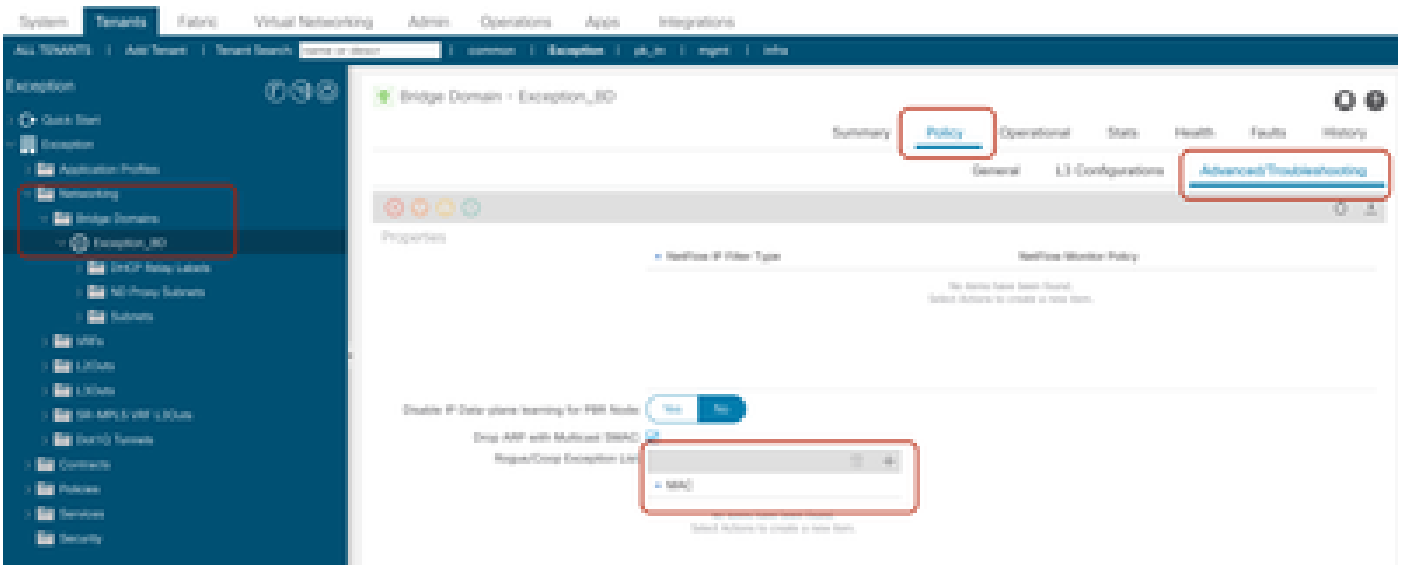
Configuration à l'aide de l'interface utilisateur graphique APIC (Application Policy Infrastructure Controller)

Pour configurer :

Étape 1. Connectez-vous à l'interface graphique Cisco APIC.

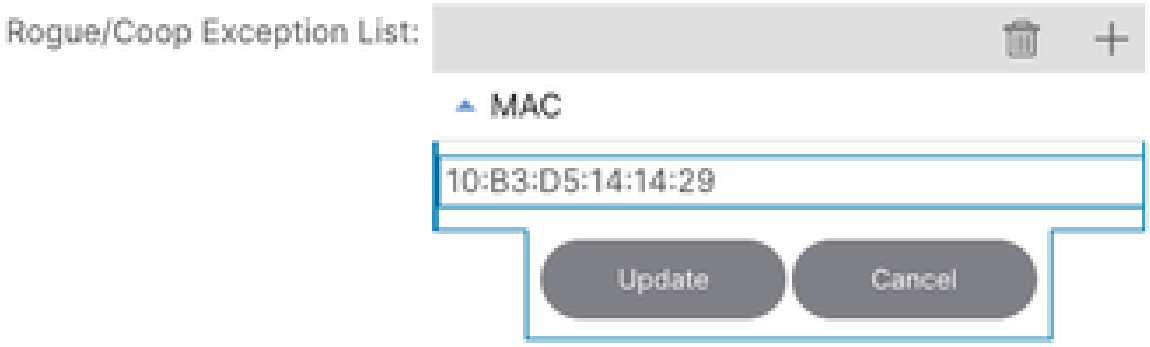
Étape 2. Accédez à Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting Tab

Sur cette page, vous pouvez ajouter des adresses MAC dans la liste des exceptions.




Étape 3. Cliquez sur l'icône + pour ajouter une adresse MAC dans la liste des exceptions Rogue/COOP.

Étape 4. Ajoutez une adresse MAC et mettez à jour.




## Vérification

Pour illustrer cette fonctionnalité, un point de terminaison dont l'adresse MAC est 10:B3:D5:14:14:29 est connecté à notre fabric ACI dans l'exception de locataire et le domaine de pont BD-Exception.

Après avoir ajouté l'adresse MAC à la liste d'exceptions dans la section « Configuration of Rogue/COOP Exception List » de ce document, la configuration peut être vérifiée à l'aide de la requête d'objet géré : moquery -c fvRogueExceptionMac

CLI APIC :

<#root>

```
bgl-aci04-apic1#
moquery -c fvRogueExceptionMac

Total Objects shown: 1

# fv.RogueExceptionMac
mac : 10:B3:D5:14:14:29
annotation :
childAction :
descr :
dn : uni/tn-Exception/BD-Exception_BD/rgexpmac-10:B3:D5:14:14:29
extMngdBy :
lcOwn : local
modTs : 2024-07-17T04:57:04.923+00:00
name :
nameAlias :
rn : rgexpmac-10:B3:D5:14:14:29
status :
uid : 16222
userdom : :all:

bgl-aci04-apic1#
```

CLI leaf :

Cette moquery fournit les compteurs appliqués sur la liste des exceptions indésirables.

<#root>

```
bgl-aci04-leaf1#
```

**moquery -c "topoctrlRogueExpP"**

```
Total Objects shown: 1

# topoctrl.RogueExpP
childAction :
descr :
dn : sys/topoctrl/rogueexpp
lcOwn : local
modTs : 2024-07-13T15:51:57.921+00:00
name :
nameAlias :
rn : rogueexpp
rogueExpEpDetectIntvl : 600   <<< Detection Interval in second
rogueExpEpDetectMult : 3000   <<< Detection Multiple (No of moves)
rogueExpEpHoldIntvl : 30      <<< Hold Interval in second
status :
```

Avec moquery, vous pouvez vérifier que n'importe quel mac particulier est ajouté à la liste des exceptions.

<#root>

```
bgl-aci04-leaf1#
```

**moquery -c "l2RogueExpMac" -f 'l2.RogueExpMac.mac=="10:B3:D5:14:14:29"'**

```
Total Objects shown: 1
# l2.RogueExpMac
mac : 10:B3:D5:14:14:29
childAction :
dn : sys/ctx-[vxlan-2293760]/bd-[vxlan-15957970]/rogueexpmac-10:B3:D5:14:14:29
lcOwn : local
modTs : 2024-07-17T04:57:04.939+00:00
name :
operSt : up
rn : rogueexpmac-10:B3:D5:14:14:29
status :
bgl-aci04-leaf1#
```

Pour confirmer les paramètres de la liste des exceptions à partir de Leaf CLI :

<#root>

```
module-1#
```

**show system internal epmc global-info | grep "Rogue Exception List"**

```
Rogue Exception List Endpoint Detection Interval : 600
Rogue Exception List Endpoint Detection Multiple : 3000
Rogue Exception List Endpoint Hold Interval : 30
module-1#
module-1#
module-1#
```

Vérifier le terminal dans les connaissances acquises dans EPMC et vérifier également le nombre de déplacements pour ce terminal.

CLI leaf :

<#root>

```
module-1#
```

**show system internal epmc endpoint mac 10:B3:D5:14:14:29**

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: BD vnid : 15957970
Encap vlan : 802.1Q/101
VRF name : Exception:Exception_vrf ::: VRF vnid : 2293760
phy if : 0x1a015000 ::: tunnel if : 0 ::: Interface : Ethernet1/22
Ref count : 5 ::: sclass : 16386
Timestamp : 07/17/2024 05:20:20.523019
::: last mv ts: 07/17/2024 05:19:17.424213 ::: ep move cnt: 9   <<<< Shows how many times endpoint move
::: Learns Src: Hal
EP Flags : local|MAC|sclass|timer|
Aging: Timer-type : HT ::: Timeout-left : 784 ::: Hit-bit : Yes ::: Timer-reset count : 0

PD handles:
[L2]: Hdl : 0x18c1e ::: Hit: Yes
::::


module-1#
```

Pour vérifier la configuration de la liste des exceptions :

CLI leaf :

<#root>

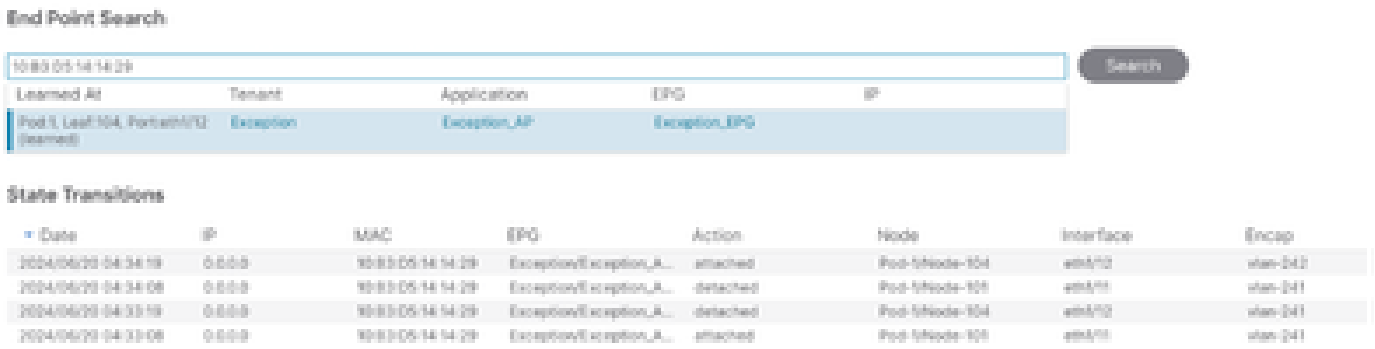
```
module-1#
```

**show system internal epmc rogue-exp-ep**

```
BD: 15957970 MAC:10b3.d514.1429
[01/01/1970 00:00:00.000000] : 0 Moves in 60 sec

module-1#
```

Vous pouvez vérifier les mouvements des terminaux dans l'interface graphique du contrôleur APIC à l'adresse Operations > EP tracker, Search MAC address here.




Comme toujours, il y a des mouvements pour cette adresse MAC, mais maintenant il n'y a pas d'indicateur de non-fiabilité pour ce terminal.

Ceci peut être vérifié à l'aide de commandes.

CLI LEAF :

Pour vérifier si un indicateur non autorisé est ajouté au point de terminaison appris dans leaf epm (gestionnaire de points de terminaison)

<#root>

```
bgl-aci04-leaf1#
```

**show system internal epm endpoint mac 10:B3:D5:14:14:29**

```
MAC : 10b3.d514.1429 ::: Num IPs : 0
Vlan id : 9 ::: Vlan vnid : 8193 ::: VRF name : Exception:Exception_vrf
BD vnid : 15957970 ::: VRF vnid : 2293760
Phy If : 0x1a015000 ::: Tunnel If : 0
Interface : Ethernet1/22
Flags : 0x80004804 ::: sclass : 16386 ::: Ref count : 4
EP Create Timestamp : 07/17/2024 05:19:10.424033
EP Update Timestamp : 07/17/2024 05:22:03.674624
EP Flags : local|MAC|sclass|timer|                <<<< Once if endpoint is rogue a Rogue flag is added

::::

bgl-aci04-leaf1#
```

CLI APIC :

Pour vérifier si une erreur est déclenchée pour le point de terminaison non autorisé.

<#root>

```
bgl-aci04-apic1#
```

```
moquery -c faultInst -f 'fault.Inst.code=="F3014"'
```

```
No Mos found
bgl-aci04-apic1#
```

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.