

在ACI中配置Rogue/COOP例外清單

目錄

[簡介](#)

[為什麼選擇例外清單？](#)

[解決方案](#)

[必備條件](#)

[配置Rogue/COOP例外清單](#)

[驗證](#)

簡介

本文檔介紹有關ACI(以應用為中心的基礎設施)中的惡意/COOP例外清單功能，並介紹配置和驗證。

為什麼選擇例外清單？

ACI中的「惡意EP控制」功能透過將臨時環路的影響隔離到發生環路的特定網橋域中，從而最大程度地減少臨時環路的影響。但是，此功能有時會導致不必要的中斷。例如，在防火牆故障切換期間，兩個防火牆可以使用相同的MAC（介質訪問控制）地址暫時傳輸流量，從而導致網路收斂之前出現問題。在5.2(3)之前，如果ACI檢測到4個EP（終端）在60秒內移動，則會將其設定為靜態，在接下來的30分鐘內不允許移動。在某些部署中，在60秒內進行4次移動可能比較現實。對於預計EP移動的場景，保持時間為30分鐘是比較積極的。

解決方案

要解決此問題，可以配置「惡意/COOP例外清單」。因此，「異常清單」中的MAC地址使用較高的閾值標準來檢測Rogue。在「例外清單」中設定的MAC在10分鐘間隔內移動3000次之後變成無管理。「例外清單」中的MAC位址使用較高的COOP（Oracle通訊協定理事會）抑制臨界值，以避免在COOP中受到抑制。您最多可以在例外清單中新增100個MAC位址。

必備條件

- 此功能自5.2(3)開始提供
- 僅當BD（網橋域）是L2 BD（如同未配置BD進行IP路由一樣）時，才能使用此選項
- 必須啟用Rogue功能才能使Rogue Exception List行為生效。

配置Rogue/COOP例外清單

此功能可用於第2層網橋域(L2 BD)，以防止特定MAC地址由於合法移動而被標籤為非法。

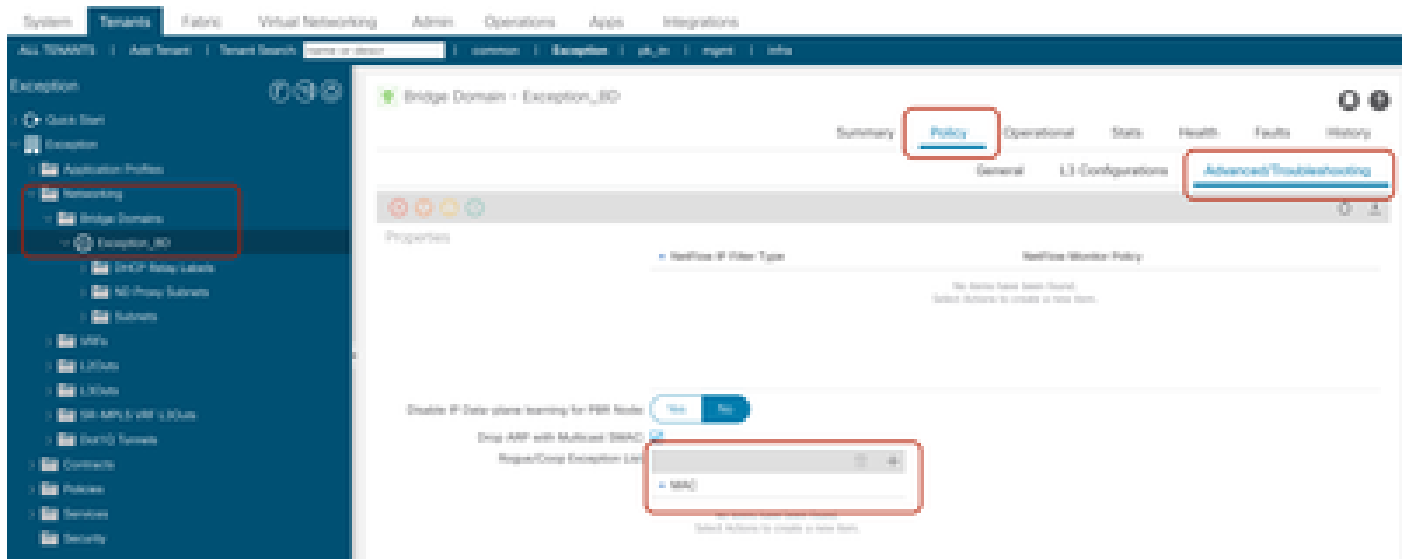
使用APIC（應用策略基礎設施控制器）GUI進行配置

若要設定：

步驟 1.登入到Cisco APIC GUI。

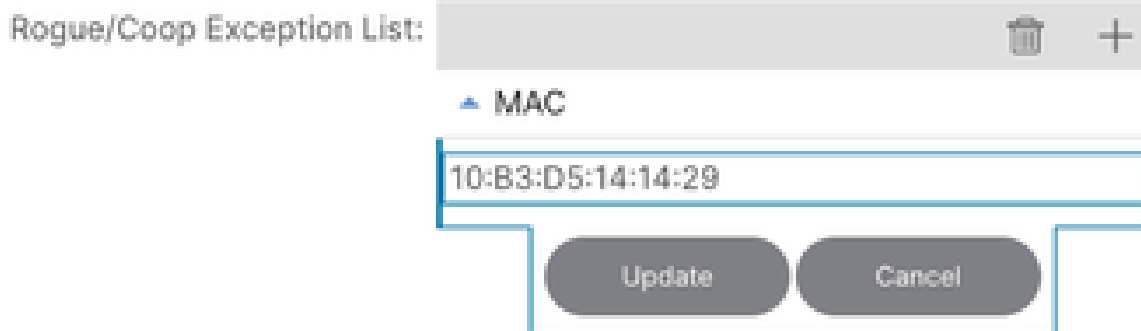
步驟 2.轉至Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting頁籤

您可以在此頁面的「例外」清單中新增MAC位址。



步驟 3.選擇+圖示在惡意/COOP例外清單中增加MAC地址。

步驟 4.增加MAC地址並更新。



驗證

為了演示此功能，有一個終端的MAC地址為10：B3：D5:14:14:29，連線到租戶例外和網橋域(BD) BD-例外內的ACI交換矩陣。

在將MAC地址增加到本文檔的「惡意/COOP例外清單配置」部分的例外清單後，可以使用託管對象(MO)查詢驗證配置：moquery -c fvRogueExceptionMac

APIC CLI：

<#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#

枝葉CLI :

此moquery提供套用至無管理「例外」清單的計時器。

<#root>

bgl-aci04-leaf1#

moquery -c "topoctrlRogueExpP"

Total Objects shown: 1

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

使用moquery，您可以驗證是否已將任何特定MAC增加到「例外」清單中。

<#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#
```

要從枝葉CLI確認例外清單引數，請執行以下操作：

<#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#
```

在EPMC中驗證已學習終端並檢查該終端的移動計數。

枝葉CLI：

<#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: Ha1
EP Flags : local|MAC|sc|class|timer|
Aging: Timer-type : HT ::: Timeout-left : 784 ::: Hit-bit : Yes ::: Timer-reset count : 0

PD handles:
[L2]: Hd1 : 0x18c1e ::: Hit: Yes
:::
```

module-1#

若要檢查例外清單組態，請執行下列步驟：

枝葉CLI：

<#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#

您可以在Operations > EP tracker處檢查APIC GUI中的終端移動，並在此處搜尋MAC地址。

End Point Search

10b3d5141429	<button>Search</button>			
Learned At	Tenant	Application	EPG	IP
Pod-1, Leaf-104, Port eth1/21 (learned)	Exception	Exception_AP	Exception_EPG	

State Transitions

Date	IP	MAC	EPG	Action	Node	Interface	Encap
2024/06/28 04:34:19	0.0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-104	eth1/22	vlan-241
2024/06/28 04:34:08	0.0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-105	eth1/21	vlan-241
2024/06/28 04:33:19	0.0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-104	eth1/22	vlan-241
2024/06/28 04:33:08	0.0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-105	eth1/21	vlan-241

因為仍有此MAC地址的移動，但是此終端現在沒有惡意標籤。

這可以透過命令來驗證。

枝葉CLI：

若要檢查是否已將惡意旗標新增至枝葉epm（端點管理員）中獲知的端點

<#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#

APIC CLI :

檢查是否存在欺詐端點故障。

<#root>

bgl-aci04-apic1#

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

No Mos found

bgl-aci04-apic1#

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）。