

ACIでの不正/COOP例外リストの設定

内容

[はじめに](#)

[例外リストを使用する理由](#)

[解決方法](#)

[前提条件](#)

[不正/COOP例外リストの設定](#)

[検証](#)

はじめに

このドキュメントでは、ACI(アプリケーションセントリックインフラストラクチャ)の不正/COOP例外リスト(ROGUE/COOP Exception List)機能について説明し、設定と検証について説明します。

例外リストを使用する理由

ACIの「不正EP制御」機能は、発生した特定のブリッジドメイン内のエンドポイントを隔離することによって、一時的なループの影響を最小限に抑えます。ただし、この機能によって不要な中断が発生する場合があります。たとえば、ファイアウォールのフェールオーバー中に、両方のファイアウォールが同じMAC (メディアアクセス制御) アドレスを使用して一時的にトラフィックを送信し、ネットワークが収束するまでエラーが発生する可能性があります。5.2(3)より前のリリースでは、ACIが4つのEP (エンドポイント) が60秒以内に移動したことを検出すると、その後はスタティックに設定され、次の30分間は移動できなくなります。60秒で4回移動する方法は、一部の導入では現実的です。30分のホールドタイムは、EPの移動が予想されるシナリオではアグレッシブです。

解決方法

この問題に対処するために、「Rogue/COOP Exception List」を設定できます。MACアドレスは、例外リスト内で、より高いしきい値の基準を使用して不正を検出します。例外リストで設定されたMACは、10分間隔で3000回移動した後に不正になります。例外リストのMACアドレスは、COOP(Council of Oracle Protocol)の減衰しきい値を高くすることで、COOPで減衰するのを防ぎます。例外リストには最大100個のMACアドレスを追加できます。

前提条件

- この機能は、5.2(3)以降のバージョンで利用可能です
- このオプションは、BD (ブリッジドメイン) がL2 BDである場合 (BDがIPルーティング用に設定されていない場合) にのみ使用できます。
- Rogue Exception Listの動作が動作するためには、不正機能を有効にする必要があります。

不正/COOP例外リストの設定

この機能をレイヤ2ブリッジドメイン(L2 BD)で使用すると、正当な移動によって特定のMACアドレスが不正としてフラグ付けされるのを防ぐことができます。

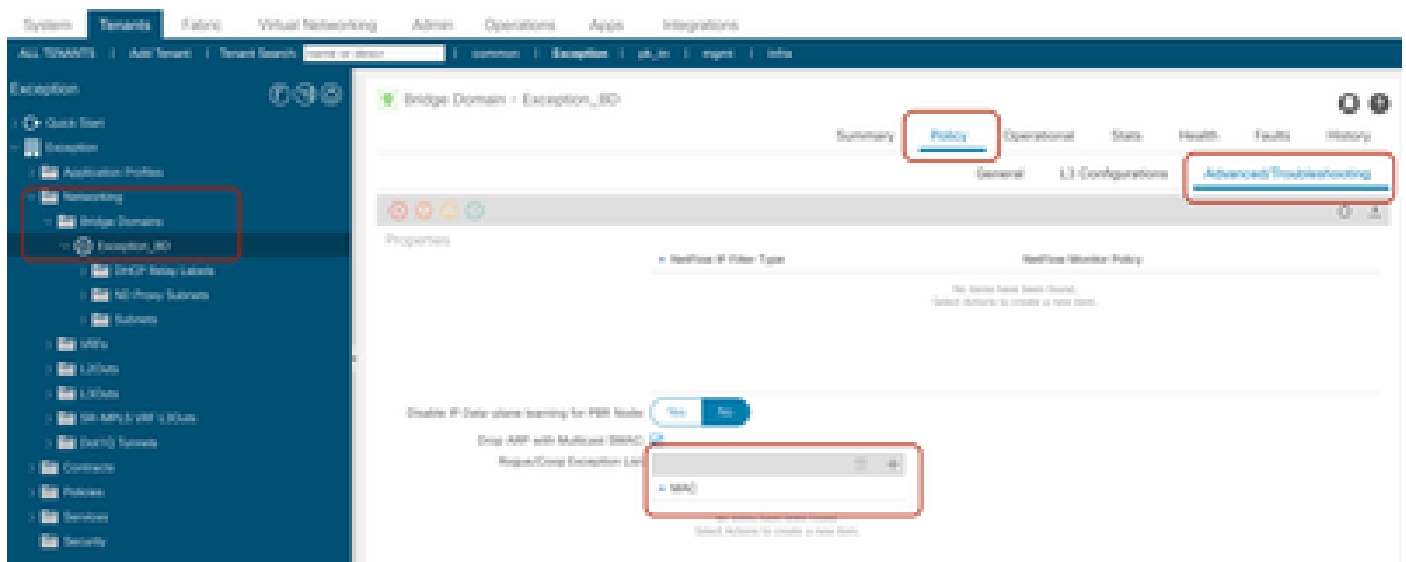
APIC(Application Policy Infrastructure Controller)GUIを使用した設定

設定するには次の操作をします。

ステップ 1 : Cisco APIC GUIにログインします。

ステップ 2 : テナント>ネットワーキング>ブリッジドメイン> BD >ポリシー>詳細/トラブルシューティングタブに移動します

このページでは、例外リストにMACアドレスを追加できます。



ステップ 3 : +アイコンを選択して、Rogue/COOP例外リストにMACアドレスを追加します。

ステップ 4 : MACアドレスを追加して更新します。

Rogue/Coop Exception List:  

 MAC

検証

この機能をデモンストレーションするため、テナント例外およびブリッジドメイン(BD)BD例外内に、MACアドレスが10:B3:D5:14:14:29のエンドポイントがACIファブリックに接続されています。

このドキュメントの「Rogue/COOP例外リストの設定」セクションの例外リストにMACアドレスを追加すると、管理対象オブジェクト(MO)クエリmoquery -c fvRogueExceptionMacを使用して設定を確認できます。

APICの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#

リーフCLI:

このクエリーは、不正例外リストに適用されるタイマーを提供します。

<#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 :
```

moqueryを使用すると、特定のMACが例外リストに追加されたことを確認できます。

<#root>

bg1-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 :
bg1-aci04-leaf1#
```

リーフCLIから例外リストのパラメータを確認するには、次の手順を実行します。

<#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#
```

EPMCで学習されたエンドポイントを確認し、そのエンドポイントの移動数も確認します。

リーフ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 moved
::: 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]: Hd1 : 0x18c1e ::: Hit: Yes
:::
```

module-1#

例外リストの構成を確認するには、次の手順に従います。

リーフ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#

APIC GUIのOperations > EP tracker、Search MAC addressでエンドポイントの移動を確認できます。

End Point Search

10b3d5141429					Search
Learned At	Tenant	Application	EPG	IP	
Pod-1, Leaf-104, Fortian/12 (learned)	Exception	Exception_APP	Exception_EPG		

State Transitions

Date	IP	MAC	EPG	Action	Node	Interface	Vlan
2024/04/29 04:34:19	0.0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-104	ethA/12	vlan-241
2024/04/29 04:34:09	0.0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-105	ethA/11	vlan-241
2024/04/29 04:33:19	0.0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-104	ethA/12	vlan-241
2024/04/29 04:33:09	0.0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-105	ethA/11	vlan-241

このMACアドレスに対する移動は引き続き存在しますが、このエンドポイントに対する不正フラグは存在しません。

これはコマンドで確認できます。

リーフCLI:

リーフepm（エンドポイントマネージャ）の学習エンドポイントに不正フラグが追加されているかどうかを確認するには

<#root>

bg1-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

::::

bg1-aci04-leaf1#

APICのCLI:

不正エンドポイントエンドポイントでエラーが発生したかどうかを確認します。

<#root>

bg1-aci04-apic1#

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

No Mos found

bgl-aci04-apic1#

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。