

Configurar a lista de exceções de rogue/COOP na ACI

Contents

[Introdução](#)

[Por que lista de exceções?](#)

[Solução](#)

[Pré-requisito](#)

[Configuração da lista de exceção de Rogue/COOP](#)

[Verificação](#)

Introdução

Este documento descreve sobre o recurso Lista de exceções de invasores/COOP no ACI (Infraestrutura centrada em aplicativos) e aborda a configuração e a verificação.

Por que lista de exceções?

O recurso "Rogue EP Control" na ACI minimiza o impacto de loops temporários colocando em quarentena os endpoints dentro do domínio de bridge específico onde eles ocorrem. No entanto, esse recurso às vezes pode causar interrupções desnecessárias. Por exemplo, durante um failover de firewall, ambos os firewalls podem transmitir momentaneamente o tráfego usando o mesmo endereço MAC (Media Access Control), resultando em falhas até que a rede converja. Antes da versão 5.2(3), se a ACI detectar 4 movimentações de EP (endpoint) em 60 segundos, ela se tornará estática e não poderá se mover nos próximos 30 minutos. 4 mudanças em 60 segundos podem ser realistas em algumas implantações. O tempo de espera de 30 minutos é agressivo para cenários onde se espera mudanças de EP.

Solução

Para resolver esse problema, é possível configurar uma "Lista de exceções de rogue/COOP". MAC endereços na lista de exceções, ele usa um critério de limite mais alto para detectar invasores. O MAC configurado na Lista de Exceções torna-se invasor após 3.000 movimentações em um intervalo de 10 minutos. MAC endereço na Lista de Exceções usa um limite de Redução COOP (Council of Oracle Protocol) mais alto para evitar ser atenuado no COOP. Você pode adicionar até 100 endereços MAC na lista de exceções.

Pré-requisito

- Este recurso está disponível na versão 5.2(3)
- Essa opção pode ser usada apenas se o BD (domínio de ponte) for um BD L2 (como se o

BD não estivesse configurado para roteamento IP)

- O recurso invasor deve ser habilitado para que o comportamento da Lista de exceções invasora funcione.

Configuração da lista de exceção de Rogue/COOP

Esse recurso pode ser utilizado nos domínios de ponte da camada 2 (L2 BD) para evitar que endereços MAC específicos sejam sinalizados como invasores devido a movimentos legítimos.

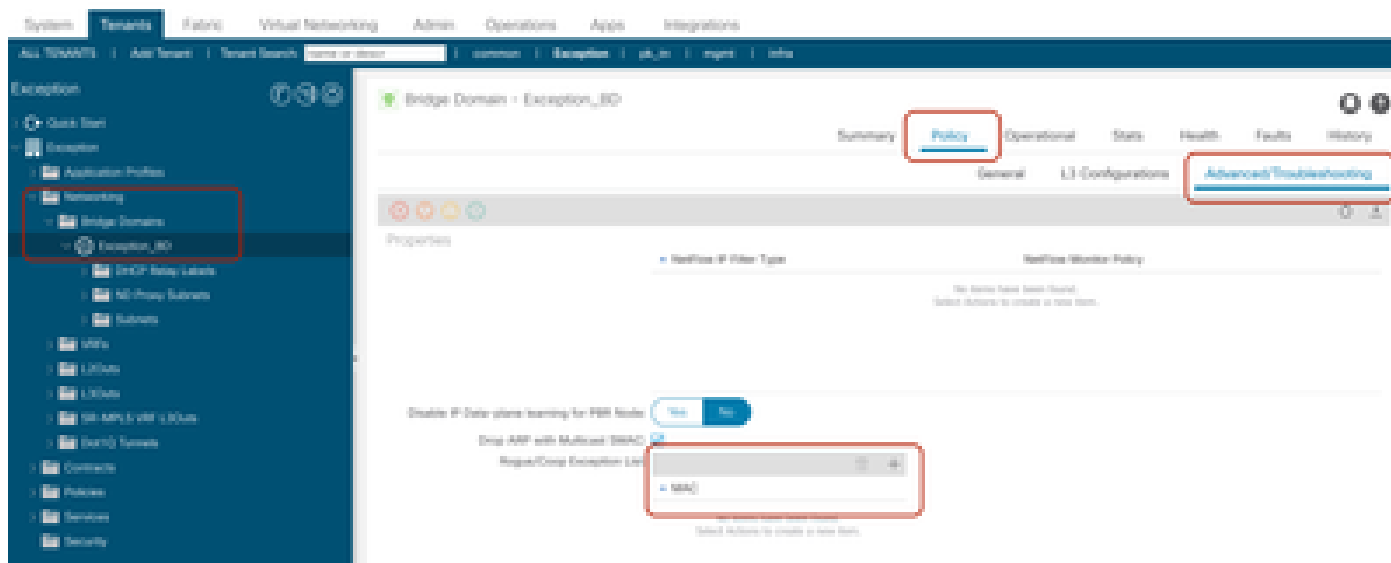
Configuração usando a GUI do APIC (Application Policy Infrastructure Controller)

Para configurar:

Etapa 1. Faça login na GUI do Cisco APIC.

Etapa 2. Vá para Localizador > Rede > Domínios de Bridge > BD > Política > Guia Avançado/Solução de Problemas

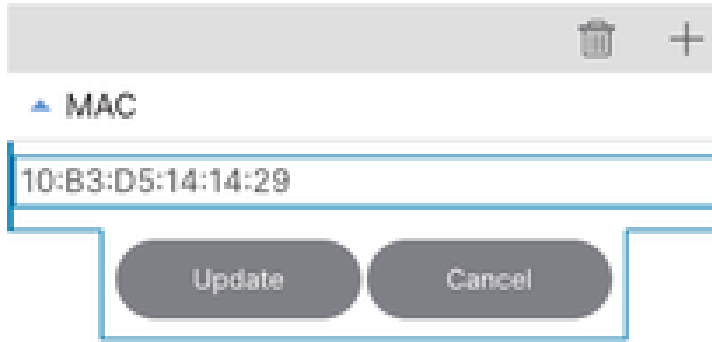
Nesta página, você pode adicionar endereços MAC na lista Exceção.



Etapa 3. Selecione o ícone + para adicionar o endereço MAC na lista de exceções de Rogue/COOP.

Etapa 4. Adicione o endereço MAC e atualize.

Rogue/Coop Exception List:



Verificação

Para demonstrar esse recurso, há um endpoint com o endereço MAC 10:B3:D5:14:14:29 conectado à estrutura da ACI dentro da exceção de usuário e do domínio de ponte (BD) BD-Exception.

Depois de adicionar o endereço MAC à lista de exceções na seção "Configuração da lista de exceções de Rogue/COOP" deste documento, a configuração pode ser verificada usando a consulta de Objeto Gerenciado (MO): `moquery -c fvRogueExceptionMac`

CLI DO APIC:

<#root>

`bg1-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:
```

`bg1-aci04-apic1#`

Folha CLI:

Este moquery fornece os temporizadores aplicados na lista de Exceções não autorizadas.

<#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 :

Com o moquery, você pode verificar se um mac específico foi adicionado à lista de exceções.

<#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#

Para confirmar os parâmetros da lista de Exceções do 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#
```

Para verificar o endpoint no aprendido no EPMC e verificar as contagens de movimentação também para esse endpoint.

Folha 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#
```

Para verificar a Configuração da lista de Exceções:

Folha 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#

Você pode verificar os movimentos do endpoint na GUI do APIC em Operations > EP tracker, Search MAC address aqui.

End Point Search

10B3D5141429

Learned_Alt

Tenant

Application

EPG

IP

Pod 1, Leaf 104, Port 10/22 (learned)

Exception

Exception_AP

Exception_EPG

Search

State Transitions

Date

IP

MAC

EPG

Action

Node

Interface

Encap

2024/04/29 04:34:19

0.0.0.0

10B3D5141429

Exception/Exception_A...

attached

Pod-1/Node-104

eth4/22

vlan-241

2024/04/29 04:34:08

0.0.0.0

10B3D5141429

Exception/Exception_A...

detached

Pod-1/Node-104

eth4/22

vlan-241

2024/04/29 04:33:59

0.0.0.0

10B3D5141429

Exception/Exception_A...

detached

Pod-1/Node-104

eth4/22

vlan-241

2024/04/29 04:33:08

0.0.0.0

10B3D5141429

Exception/Exception_A...

attached

Pod-1/Node-104

eth4/22

vlan-241

Como ainda há movimentos para esse endereço MAC, agora não há nenhum flag invasor para esse ponto final.

Isso pode ser verificado com comandos.

CLI LEAF:

Para verificar se o sinalizador invasor é adicionado ao ponto final aprendido no epm folha (gerenciador de ponto final)

<#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#
```

CLI DO APIC:

Para verificar se alguma falha foi gerada para o ponto final do ponto final invasor.

<#root>

bgl-aci04-apic1#

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

No Mos found

bgl-aci04-apic1#

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.