

Uitzonderingslijst Rogue/COOP in ACI configureren

Inhoud

[Inleiding](#)

[Waarom een uitzonderingslijst?](#)

[Oplossing](#)

[Voorwaarde](#)

[Configuratie van Rogue/COOP Exception List](#)

[Verificatie](#)

Inleiding

Dit document beschrijft informatie over de functie Uitzonderingslijst Rogue/COOP in ACI (Application Centric Infrastructure) en behandelt configuratie en verificatie.

Waarom een uitzonderingslijst?

De functie "Rogue EP Control" in ACI minimaliseert de impact van tijdelijke loops door eindpunten in quarantaine te plaatsen binnen het specifieke brugdomein waar ze voorkomen. Deze functie kan echter in sommige gevallen onnodige verstoringen veroorzaken. Tijdens een firewall-failover kunnen beide firewalls bijvoorbeeld tijdelijk verkeer verzenden met hetzelfde MAC-adres (Media Access Control), wat resulteert in glitches totdat het netwerk convergeert. Vóór 5.2(3) Als ACI 4 EP (Endpoint) in 60 seconden detecteert, wordt het statische tijd en mag het gedurende de volgende 30 minuten niet bewegen. 4 bewegingen in 60 seconden kunnen bij sommige inzet realistisch zijn. De houdtijd van 30 minuten is agressief voor scenario's waarbij EP-bewegingen worden verwacht.

Oplossing

Om dit probleem aan te pakken is het mogelijk om een "Rogue/COOP Exception List" te configureren. MAC-adressen in de Exception List gebruikt het vervolgens een hogere drempelcriteria om Rogue te detecteren. MAC geconfigureerd in Exceptielijst wordt bedrieglijk gemaakt na 3000 bewegingen in 10-minuten interval. MAC adres in Exception List gebruikt een hogere COOP (Council of Oracle Protocol) Damping drempel om te voorkomen dat het wordt gedempt in COOP. U kunt maximaal 100 MAC-adres toevoegen in de uitzonderingenlijst.

Voorwaarde

- Deze optie is beschikbaar vanaf versie 5.2(3)
- Deze optie kan alleen worden gebruikt als de BD (Bridge Domain) een L2 BD is (Alsof de BD

niet is geconfigureerd voor IP-routing)

- De functie Rogue moet worden ingeschakeld om het gedrag Rogue Exception List te laten werken.

Configuratie van Rogue/COOP Exception List

Deze functie kan worden gebruikt in Layer 2 Bridge Domains (L2 BD) om te voorkomen dat specifieke MAC-adressen als schurk worden gemarkeerd als gevolg van legitieme bewegingen.

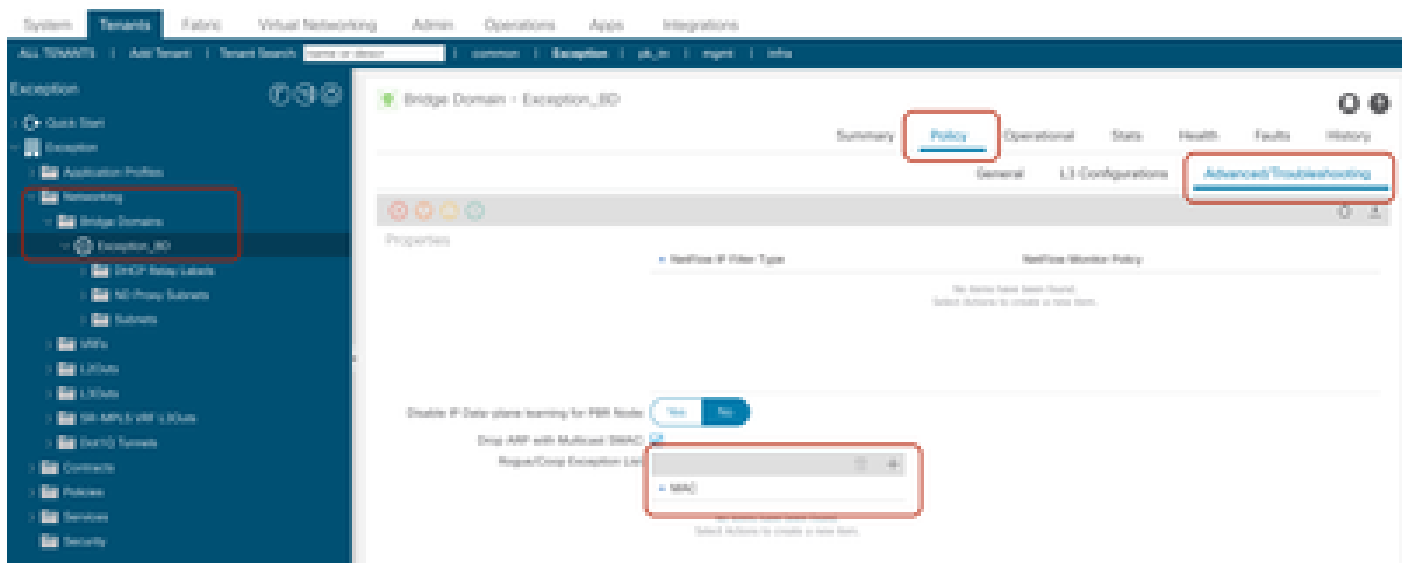
Configuratie met APIC (Application Policy Infrastructure Controller) GUI

Configureren:

Stap 1. Log in op de Cisco APIC GUI.

Stap 2. Ga naar huurder > Netwerken > Bridge Domains > BD > Beleid > Geavanceerd/tabblad Problemen oplossen

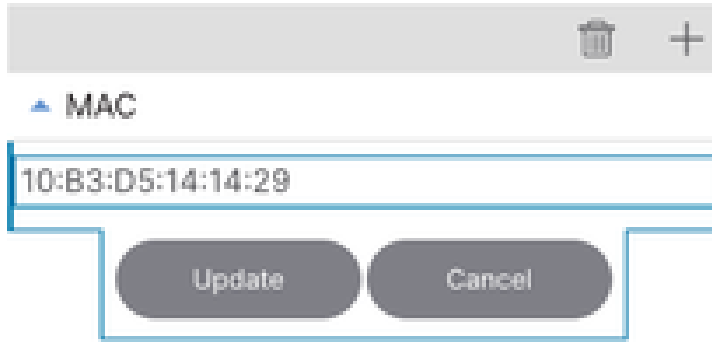
Op deze pagina kunt u MAC-adressen toevoegen in de lijst Uitzondering.



Stap 3. Selecteer + pictogram om MAC-adres toe te voegen in de uitzonderingenlijst Rogue/COOP.

Stap 4. Voeg MAC-adres en update toe.

Rogue/Coop Exception List:



Verificatie

Om deze functie te demonstreren, is er een eindpunt met het MAC-adres 10:B3:D5:14:14:29 verbonden met onze ACI-stof binnen de Tenant Exception en Bridge Domain (BD) BD-Exception.

Na het toevoegen van het MAC-adres aan de uitzonderingenlijst in de sectie "Configuration of Rogue/COOP Exception List" van dit document, kan de configuratie worden geverifieerd met behulp van de Managed Object (MO) query: `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#
```

Blad-CLI:

Deze moquery biedt de timers die worden toegepast op frauduleuze uitzonderingslijst.

```
<#root>
```

```
bg1-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 :
```

Met moquery kunt u controleren of een bepaalde mac is toegevoegd in de Exception lijst.

```
<#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#
```

Zo bevestigt u de parameters van de Exception list van 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#
```

Om te controleren of het eindpunt in EPMC is geleerd en om ook de verplaatsingen voor dat eindpunt te controleren.

Blad-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#
```

U kunt de configuratie van de uitzonderingslijst als volgt controleren:

Blad-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#

U kunt de endpointbewegingen in APIC GUI controleren op Operations > EP tracker, Search MAC-adres hier.

End Point Search

10b3d5141429					Search
Learned At	Tenant	Application	EPG	IP	
Pod1, Leaf104, Port10/10 (learned)	Exception	Exception_AP	Exception_EPG		

State Transitions

Date	IP	MAC	EPG	Action	Node	Interface	Encap
2024/06/20 04:34:18	0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-104	eth4/22	vlan-241
2024/06/20 04:34:08	0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-105	eth4/21	vlan-241
2024/06/20 04:33:58	0.0.0	10b3d5141429	Exception/Exception_A...	detached	Pod-1/Node-104	eth4/22	vlan-241
2024/06/20 04:33:08	0.0.0	10b3d5141429	Exception/Exception_A...	attached	Pod-1/Node-105	eth4/21	vlan-241

Zoals nog steeds zijn er bewegingen voor dit MAC-adres, maar nu is er geen Rogue Flag voor dit Endpoint.

Dit kan worden geverifieerd met opdrachten.

BLADCLI:

Om te controleren of schurkenvlag is toegevoegd aan aangeleerd eindpunt in blad epm (endpoint manager)

```
<#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 CLI:

Om te controleren of een fout is veroorzaakt door een foutief eindpunt.

```
<#root>
```

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

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

```
No Mos found
```

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.