# Konfigurieren einer Liste nicht autorisierter bzw. COOP-Ausnahmen in der ACI

## Inhalt



## Einleitung

Dieses Dokument beschreibt die Funktion für nicht autorisierte/COOP-Ausnahmelisten in der ACI (Application Centric Infrastructure) und behandelt Konfiguration und Verifizierung.

### Warum eine Ausnahmeliste?

Die Funktion "Rogue EP Control" der ACI minimiert die Auswirkungen temporärer Schleifen, indem Endpunkte innerhalb der Bridge-Domäne, in der sie auftreten, unter Quarantäne gestellt werden. Diese Funktion kann jedoch manchmal zu unnötigen Unterbrechungen führen. Während eines Firewall-Failovers können beispielsweise beide Firewalls vorübergehend Datenverkehr mit derselben MAC-Adresse (Media Access Control) übertragen, was zu Störungen führt, bis das Netzwerk konvergiert. Vor 5.2(3) Wenn die ACI erkennt, dass 4 EPs (Endpunkte) innerhalb von 60 Sekunden verschoben werden, wird sie statisch und kann nicht innerhalb der nächsten 30 Minuten verschoben werden. 4 Züge in 60 Sekunden können in einigen Bereitstellungen realistisch sein. Eine Haltezeit von 30 Minuten ist für Szenarien, in denen EP-Schritte erwartet werden, sehr aggressiv.

### Lösung

Um dieses Problem zu beheben, kann eine "Rogue/COOP Exception List" konfiguriert werden. MAC Adressen in der Ausnahmeliste verwendet dann ein höheres Schwellenwertkriterium, um nicht autorisierte Zugriffe zu erkennen. Die in der Ausnahmeliste konfigurierte MAC wird nach 3000 Verschiebungen im 10-Minuten-Intervall deaktiviert.MAC-Adresse in der Ausnahmeliste verwendet einen höheren COOP (Council of Oracle Protocol)-Dämpfungsschwellenwert, um eine Dämpfung in COOP zu vermeiden. Sie können bis zu 100 MAC-Adressen in der Ausnahmeliste hinzufügen.

## Voraussetzung

- Diese Funktion ist ab Version 5.2(3) verfügbar.
- Diese Option kann nur verwendet werden, wenn es sich bei dem BD (Bridge-Domäne) um einen L2-BD handelt (als wäre der BD nicht für IP-Routing konfiguriert).
- Die Funktion für nicht autorisierte Ausnahmen muss aktiviert sein, damit das Verhalten der Liste nicht autorisierter Ausnahmen funktioniert.

## Konfiguration der Liste nicht autorisierter bzw. COOP-Ausnahmen

Diese Funktion kann in Layer-2-Bridge-Domänen (L2 BD) verwendet werden, um zu verhindern, dass bestimmte MAC-Adressen aufgrund legitimer Bewegungen als nicht autorisiert gekennzeichnet werden.

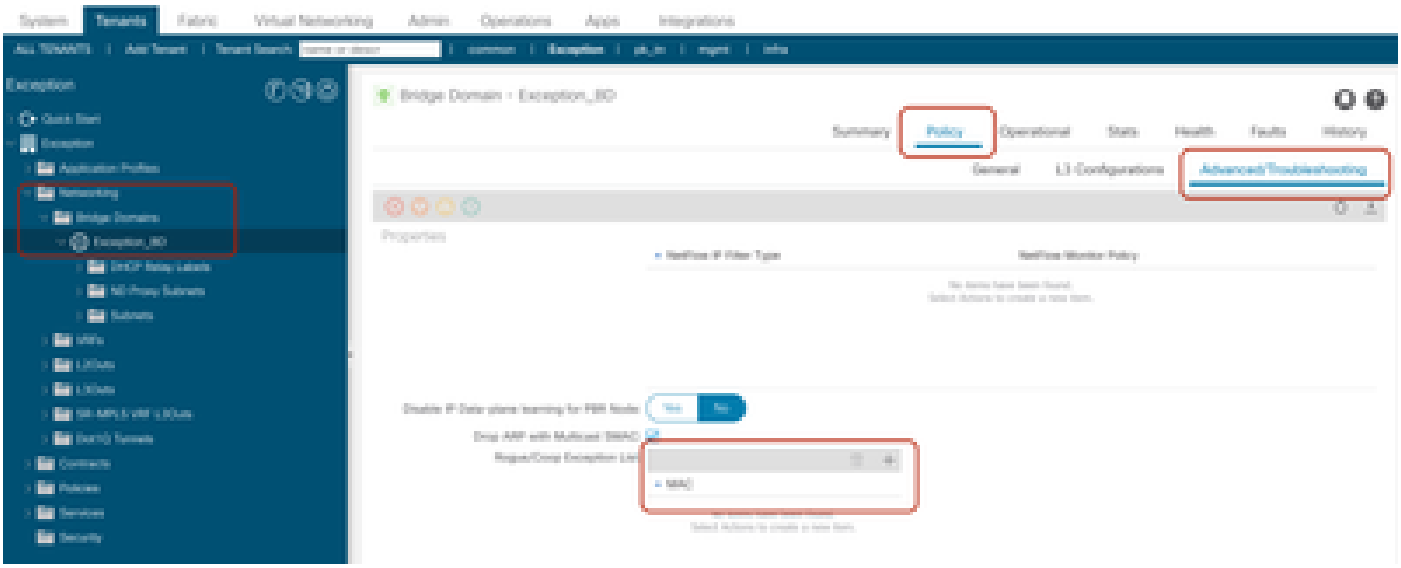
Konfiguration über die grafische Benutzeroberfläche des APIC (Application Policy Infrastructure Controller)

Konfiguration:

Schritt 1: Melden Sie sich bei der Cisco APIC-Benutzeroberfläche an.

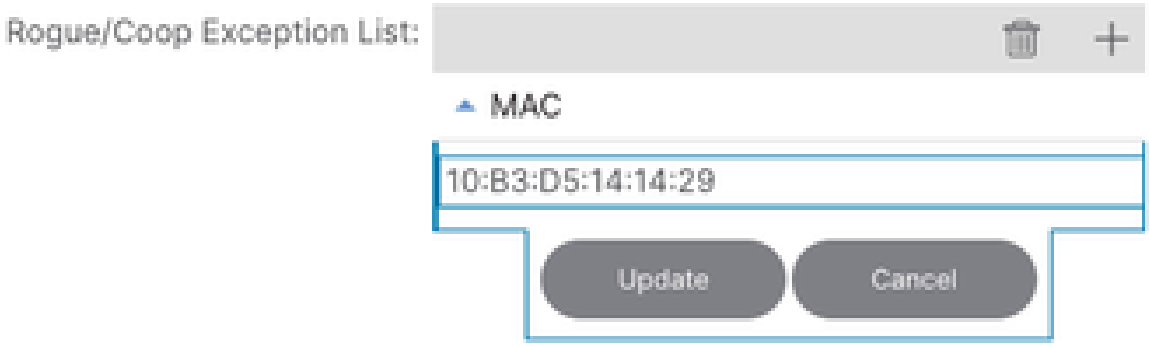
Schritt 2: Gehen Sie zu Tenant > Networking > Bridge Domains > BD > Policy > Advanced/Troubleshooting Tab

Auf dieser Seite können Sie MAC-Adressen in der Ausnahmeliste hinzufügen.




Schritt 3: Klicken Sie auf das Symbol +, um die MAC-Adresse zur Liste nicht autorisierter/COOP-Ausnahmen hinzuzufügen.

Schritt 4: MAC-Adresse hinzufügen und aktualisieren.




# Verifizierung

Zur Demonstration dieser Funktion muss ein Endpunkt mit der MAC-Adresse 10:B3:D5:14:14:29 mit unserer ACI-Fabric verbunden sein, und zwar innerhalb der Tenant Exception- und Bridge Domain (BD)-BD-Exception.

Nachdem die MAC-Adresse der Ausnahmeliste im Abschnitt "Konfiguration der Liste nicht autorisierter bzw. COOP-Ausnahmen" dieses Dokuments hinzugefügt wurde, kann die Konfiguration mithilfe der Abfrage für verwaltete Objekte (MO) überprüft werden: 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#
```

Leaf-CLI:

Diese Moquery stellt die Timer bereit, die auf die Liste nicht autorisierter Ausnahmen angewendet werden.

<#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 :
```

Mit moquery können Sie überprüfen, ob eine bestimmte MAC in der Ausnahmeliste hinzugefügt wurde.

<#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#
```

So bestätigen Sie Ausnahmelistenparameter von 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#

Überprüfen Sie den Endpunkt in "Gelernt" im EPMC und überprüfen Sie die Anzahl der Verschiebungen für diesen Endpunkt.

Leaf-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: 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#

So überprüfen Sie die Konfiguration der Ausnahmeliste:

Leaf-CLI:

<#root>

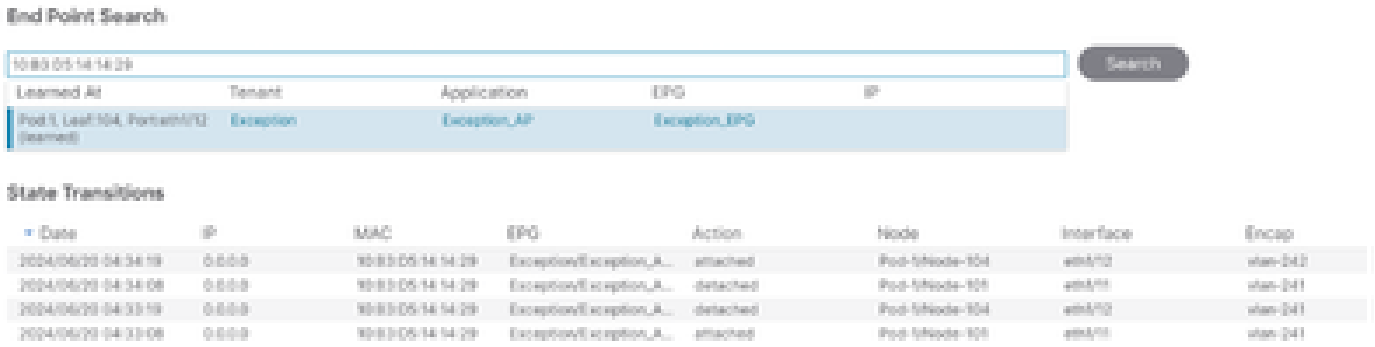
module-1#

```
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#
```

Sie können die Bewegungen der Endpunkte in der APIC-GUI unter Operations > EP tracker, Search MAC address hier überprüfen.




Wie immer gibt es Bewegungen für diese MAC-Adresse, aber jetzt gibt es keine Rogue Flag für diesen Endpunkt.

Dies kann mit Befehlen überprüft werden.

LEAF-CLI:

Überprüft, ob dem erkannten Endpunkt im Endpunkt-EPM (Endpunkt-Manager) eine Rogue-Markierung hinzugefügt wird.

<#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:

Überprüft, ob ein Fehler für einen Endpunkt mit nicht autorisierten Endpunkten aufgetreten ist.

<#root>

```
bgl-aci04-apic1#

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


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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.