# التحقق من صحة قوائم التحكم في الوصول الأمنية على محولات Catalyst 9000 Switches

## المحتويات

# المقدمة

يصف هذا المستند كيفية التحقق من قوائم التحكم في الوصول (ACL) واستكشاف أخطائها وإصلاحها (قوائم التحكم في الوصول) على محولات Catalyst 9000 Series Switches.

# المتطلبات الأساسية

## المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية التالية:

- C9200
- C9300
- C9400
- C9500
- C9600

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

---

ملاحظة: راجع دليل التكوين المناسب للأوامر المستخدمة لتمكين هذه الميزات على منصات Cisco الأخرى.

---

# معلومات أساسية

تقوم قوائم التحكم في الوصول (ACLs) بتصفية حركة المرور عند مرورها عبر موجه أو محول والسماح للحزم التي تعبر الواجهات المحددة أو رفضها. قائمة التحكم في الوصول (ACL) هي مجموعة متسلسلة من شروط الترخيص والرفض التي تنطبق على الحزم. عندما يتم إستلام حزمة على واجهة، يقوم المحول بمقارنة الحقول في الحزمة مقابل أي قوائم التحكم في الوصول (ACL) مطبقة للتحقق من أن الحزمة لديها الأذونات المطلوبة لإعادة التوجيه، استنادا إلى المعايير المحددة في قوائم الوصول. يقوم هذا البرنامج، واحدا تلو الآخر، باختبار الحزم حسب الشروط الواردة في قائمة الوصول. تقرر التطابق الأول ما إذا كان المحول يقبل الحزم أو يرفضها. لأن المحول يتوقف عن الاختبار بعد المطابقة الأولى، فإن ترتيب الأوضاع في القائمة أمر بالغ الأهمية. إذا لم تكن هناك شروط مطابقة، فإن المحول يرفض الحزمة. إذا لم توجد قيود، سيقوم المحول بإعادة توجيه الحزمة؛ وإلا، سيقوم المحول بإسقاط الحزمة. يمكن أن يستخدم المحول قوائم التحكم في الوصول (ACL) على جميع الحزم التي يقوم بإعادة توجيهها.

يمكنك تكوين قوائم الوصول لتوفير الأمان الأساسي لشبكتك. إذا لم تقم بتكوين قوائم التحكم في الوصول (ACL)، يمكن السماح بجميع الحزم التي تمر عبر المحول على جميع أجزاء الشبكة. يمكنك إستخدام قوائم التحكم في الوصول (ACL) للتحكم في عناوين أو تحديد وأ الشبكة من مختلفة المضيفة التي يمكنها الوصول إلى أجزاء البيئات. على سبيل المثال، يمكنك حركة المرور التي يتم إعادة توجيهها أو حظرها في واجهات المحول. إعادة توجيه حركة مرور برنامج Telnet.

## المصطلح

| | |
|---|---|
| إيس | إدخال التحكم في الوصول (ACE) - قاعدة/خط واحد داخل قائمة التحكم في الوصول (ACL) |
| ACL | قائمة التحكم في الوصول (ACL) - مجموعة من وحدات ACE المطبقة على منفذ ما |
| DACL | قائمة التحكم في الوصول (DACL) القابلة للتنزيل - قائمة تحكم في الوصول (ACL) يتم دفعها بشكل ديناميكي من خادم سياسة أمان ISE |
| PACL | قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) - قائمة تحكم في الوصول (ACL) يتم تطبيقها على واجهة الطبقة 2 |
| RACL | قائمة التحكم في الوصول (RACL) الموجهة - قائمة تحكم في الوصول (ACL) يتم تطبيقها على واجهة الطبقة 3 |
| VACL | VLAN ACL (VACL) - قائمة تحكم في الوصول (ACL) مطبقة على شبكة VLAN |
| GACL | قائمة التحكم في الوصول الخاصة بالمجموعة (GACL) - قائمة تحكم في الوصول (ACL) يتم تعيينها ديناميكيا لمجموعة مستخدمين أو عميل استناد إلى هويتهم |
| IP ACL | حزم IPv4/IPv6. تحتوي هذه القواعد على حقول وسمات حزم يستخدم لتصنيف الحزم. على سبيل المثال في ذلك الطبقة الثالثة والطبقة الرابعة بما في ذلك مجموعة متنوعة من الطبقة 4 بما TCP/UDP مصدر ومنفذ والوجهة لـ IPv4 عناوين الحصر والوجهة وعلامات TCP و DSCP وما إلى ذلك. |
| MACL | قائمة التحكم في الوصول (ACL) لعنوان MAC (MAC) - حزم تستخدم لتصنيف الحزم باستخدام 2 الطبقة. تحتوي القواعد على حقول وسمات مختلفة من IP. التي ليس لها IP، كتابة ether، وهذا. في ذلك عنوان MAC المصدر/الطبقة الدنيا |
| L4OP | منفذ مشغل الطبقة 4 (L4OP) - يطابق مطابق آخر غير EQ (مساو ل). GT (أكبر من)، LT (أقل من)، NE (يساوي ال)، والنطاق (من إلى) |

| | |
|---|---|
| VCU | وحدة مقارنة القيمة (VCU) - تتم ترجمة نقاط الوصول من المستوى الرابع إلى وحدة التحكم في الوصول للقيم (VCU) إلجراء التصنيف على رؤوس الطبقة الرابعة |
| VMR | نتيجة قناع القيمة (VMR) - تتم برمجة إدخال ACE داخلياً في TCAM ك VMR. |
| CGD | قاعدة بيانات مجموعة الفئة (CGD) - حيث يقوم FMAN-FP بتخزين محتوى قائمة التحكم في الوصول (ACL) |
| الطبقات | كيف يتم تحديد وحدات ACE في CGD |
| سي جي | مجموعة الفئة (CGD) - مجموعة من الفئات حول كيفية تحديد قوائم التحكم في الوصول في CGD |
| CGE | إدخال مجموعة الفئة (CGE) - إدخال ACE مخزن داخل مجموعة الفئة |
| فمان | مدير إعادة التوجيه (FMAN) - طبقة البرمجة بين Cisco IOS® XE والأجزة |
| أطعمتما | برنامج تشغيل محرك إعادة التوجيه (FED) - المكون الذي يعمل على برمجة أجزة الجاز |

# أمثلة إستخدام موارد ACL

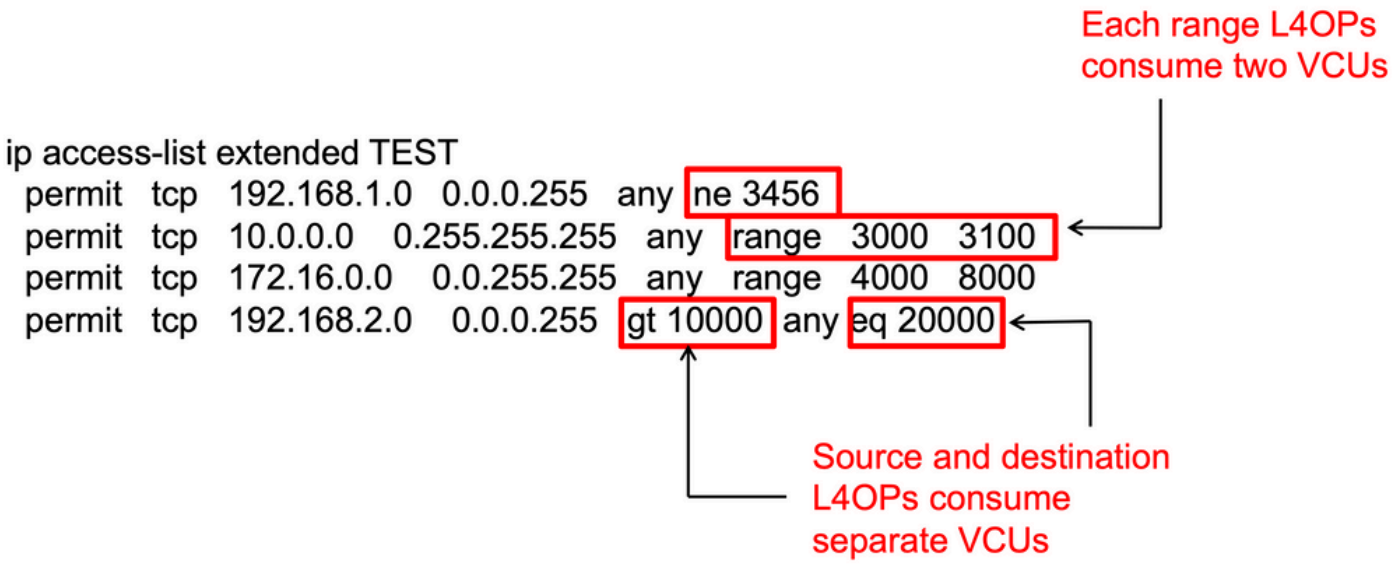
تم تقديم ثلاثة أمثلة هنا لتوضيح كيفية إستهلاك قوائم التحكم في الوصول (ACL) لـ VCUs و L4OP و TCAM.

## مثال 1. بروتوكول IPv4 TCAM

```
access-list 101 permit ip any 10.1.1.0 0.0.0.255
access-list 101 permit ip any 10.1.2.0 0.0.0.255
access-list 101 permit ip any 10.1.3.0 0.0.0.255
access-list 101 permit ip any 10.1.4.0 0.0.0.255
access-list 101 permit ip any 10.1.5.0 0.0.0.255
```

| | إدخالات TCAM | L4OPs | VCUs |
|---|---|---|---|
| إستهلاك | 5 | 0 | 0 |

مثال 2. IPv4 TCAM/L4OP/VCU




<#root>

```
ip access-list extended TEST
10 permit tcp 192.168.1.0 0.0.0.255 any
neq 3456


<-- 1 L4OP, 1 VCU


20 permit tcp 10.0.0.0 0.255.255.255 any
range 3000 3100  <-- 1 L4OP, 2 VCU


30 permit tcp 172.16.0.0 0.0.255.255 any
range 4000 8000  <-- 1 L4OP, 2 VCU


40 permit tcp 192.168.2.0 0.0.0.255
gt 10000
 any
eq 20000 <-- 2 L4OP, 2 VCU
```

| | إدخالات TCAM | L4OPs | VCUs |
|---|---|---|---|
| إستهلاك | 4 | 5 | 7 |

مثال 3. بروتوكول IPv6 TCAM/L4OP/VCU

يستخدم إدخالات التحكم في الوصول (ACEs) إلى IPv6 إدخالات TCAM مقابل إدخال واحد ل IPv4. في هذا المثال، تستهلك أربع وحدات إدخال وإخراج (ACE) ثمانية وحدات TCAM بدلا من أربعة.

<#root>

```
ipv6 access-list v6TEST
sequence 10 deny ipv6 any 2001:DB8:C18::/48 fragments
sequence 20 deny ipv6 2001:DB8::/32 any
sequence 30 permit tcp host 2001:DB8:C19:2:1::F host 2001:DB8:C18:2:1::1
```

**eq bgp  <-- One L4OP & VCU**

```
sequence 40 permit tcp host 2001:DB8:C19:2:1::F
```

**eq bgp**

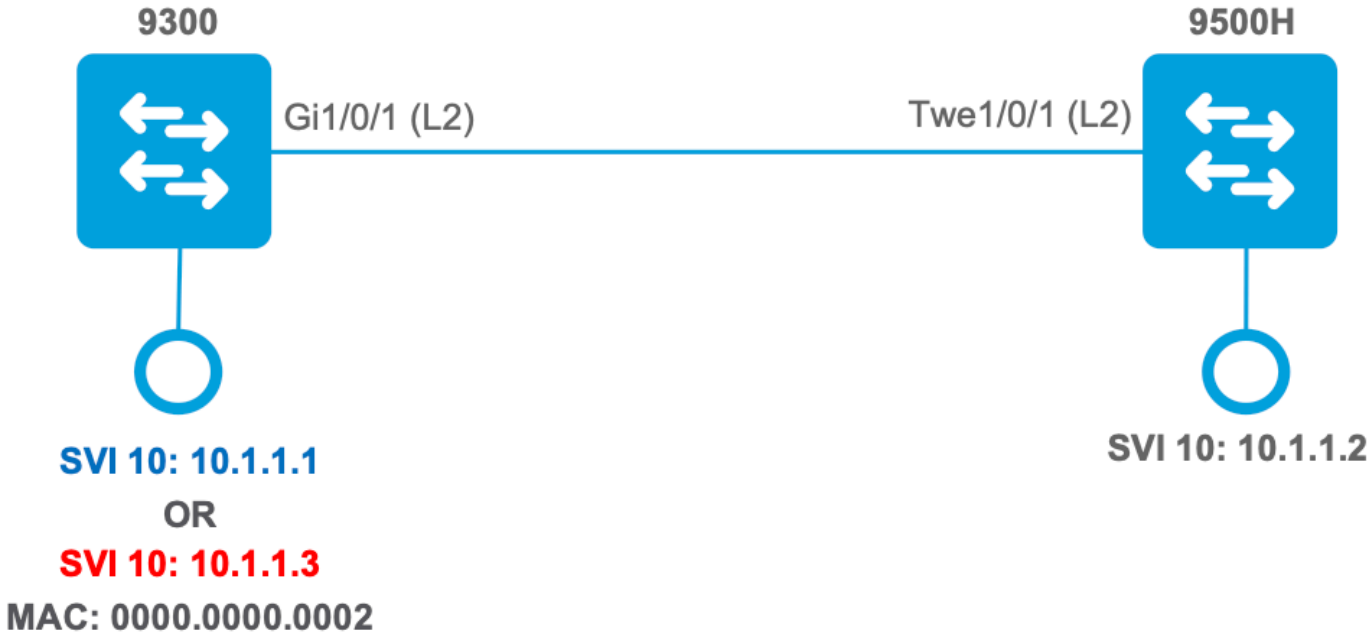
```
 host 2001:DB8:C18:2:1::1
```

**<-- One L4OP & VCU**

| | إدخالات TCAM | L4OPs | VCUs |
|---|---|---|---|
| إستهلاك | 8 | 2 | 2 |

## المخطط

يستخدم ال 9300 VLAN 10 SVI أحد عناوين IP المبينين في هذه الصورة، بناء على ما إذا كانت نتيجة إعادة توجيه أو إسقاط مبينة في المثال.



# التكوين والتحقق

يغطي هذا القسم كيفية التحقق من برمجة قائمة التحكم في الوصول (ACL) واستكشاف أخطائها وإصلاحها في البرامج والأجهزة.

## 1. PACL (IP ACL) السيناريو

تم تعيين قوائم التحكم في الوصول الخاصة بالمنفذ (PACL) إلى واجهة الطبقة 2.

- حد الأمان: المنافذ أو شبكات VLAN
- المرفق: واجهة الطبقة 2
- الإتجاه: مدخل أو مخرج (واحد في كل مرة)
- أنواع قوائم التحكم في الوصول (ACL) المدعومة: قوائم التحكم في الوصول إلى MAC وقوائم التحكم في الوصول إلى IP (قياسية أو موسعة)

تكوين PACL باستخدام قائمة التحكم في الوصول إلى IP

```
<#root>

9500H(config)#

ip access-list extended TEST          <-- Create a named extended ACL


9500H(config-ext-nacl)#

permit ip host 10.1.1.1 any

9500H(config-ext-nacl)#

permit udp host 10.1.1.1 eq 1000 host 10.1.1.2


9500H#

show access-lists TEST                        <-- Display the ACL configured


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2

9500H(config)#

interface twentyFiveGigE 1/0/1        <-- Apply ACL to Layer 2 interface


9500H(config-if)#

ip access-group TEST in


9500H#

show running-config interface twentyFiveGigE 1/0/1
```

```
Building configuration...

Current configuration : 63 bytes
!
interface TwentyFiveGigE1/0/1
 ip access-group TEST in                              <-- Display the ACL applied to the interface

end
```

التحقق من PACL

إسترداد IF_ID المقترن بالواجهة.

```
<#root>

9500H#

show platform software fed active ifm interfaces ethernet

Interface
 IF_ID
               State
----------------------------------------------------------------

TwentyFiveGigE1/0/1


0x00000008
          READY
<-- IF_ID value for Tw1/0/1
```

تحقق من ربط معرف مجموعة الفئات (CG ID) ب IF_ID.

```
<#root>

9500H#

show platform software fed active acl interface 0x8       <-- IF_ID with leading zeros omitted


##########################################################
########                              ##################
#######   Printing Interface Infos     #################
########                              ##################
##########################################################

INTERFACE:
```

**TwentyFiveGigE1/0/1** **<-- Confirms the interface matches the IF_ID**

MAC 0000.0000.0000
##########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028

**Interface Type: Port** **<-- Type: Port indicates Layer 2 interface**

**if-id: 0x0000000000000008** **<-- IF_ID 0x8 is correct**

    Input IPv4: Policy Handle: 0x5b000093

**Policy Name: TEST** **<-- The named ACL bound to this interface**

**CG ID: 9** **<-- Class Group ID for this entry**

**CGM Feature: [0] acl** **<-- Feature is ACL**

        Bind Order: 0

معلومات قائمة التحكم في الوصول (ACL) المقترنة بمعرف CG.

<#root>

9500H#

**show platform software fed active acl info acl-cgid 9 <-- The CG ID associated to the ACL TEST**

##########################################################
#########                            ##################
########      Printing CG Entries      #################
#########                            ##################
##########################################################
==================================

**ACL CG (acl/9): TEST type: IPv4 <-- feature ACL/CG ID 9: ACl name TEST : ACL type IPv4**

Total Ref count 1
---------------------------------

**1 Interface**

**<-- ACL is applied to one interface**

```
---------------------------------
  region reg_id: 10
    subregion subr_id: 0
      GCE#:1
#flds: 2


l4:N
 matchall:N deny:N
<-- #flds: 2 = two fields in entry | l4:N (no Layer 4 port match)

        Result: 0x01010000

ipv4_src: value
 =
0x0a010101
,
mask = 0xffffffff

<-- src 0x0a010101 hex = 10.1.1.1 | mask 0xffffffff = exact host match


ipv4_dst: value
 =
0x00000000, mask = 0x00000000

<--

dst & mask = 0x00000000 = match any
       GCE#:1 #flds: 4
l4:Y
 matchall:N deny:N
<-- #flds: 4 = four fields in entry | l4:Y (ACE uses UDP port L4 match)

        Result: 0x01010000

ipv4_src: value = 0x0a010101, mask = 0xffffffff  <-- Exact match (host) 10.1.1.1


ipv4_dst: value = 0x0a010102, mask = 0xffffffff  <-- Exact match (host) 10.1.1.2
```

**ip_prot: start = 17, end = 17** **<-- protocol 17 is UDP**

**l4_src: start = 1000, end = 1000** **<-- matches eq 1000 (equal UDP port 1000)**

معلومات النهج الخاصة بمعرف CG، وكذلك الواجهات التي تستخدم معرف CG.

<#root>

9500H#

**show platform software fed active acl policy 9** **<-- Use the CG ID value**

```
##########################################################
#########                                ##################
########     Printing Policy Infos      #################
#########                                ##################
##########################################################
```

**INTERFACE: TwentyFiveGigE1/0/1** **<-- Interface with ACL applied**

MAC 0000.0000.0000

```
##########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028
    Interface Type: Port
```

**if-id: 0x0000000000000008** **<-- The Interface IF_ID 0x8**

---

**Direction: Input** **<-- ACl is applied in the ingress direction**

**Protocol Type:IPv4** **<-- Type is IPv4**

```
    Policy Intface Handle: 0x880000c1
    Policy Handle: 0x5b000093

##########################################################
#########                                ##################
########      Policy information        #################
#########                                ##################
##########################################################
```

Policy handle : 0x5b000093

**Policy name : TEST** **<-- ACL Name TEST**

**ID : 9** **<-- CG ID for this ACL entry**

```
Protocol           : [3] IPV4
Feature            : [1] AAL_FEATURE_PACL                <-- ASIC feature is PACL

Number of ACLs     : 1

##########################################################
## Complete policy ACL information
##########################################################
Acl number    : 1
====================================
Acl handle      : 0x320000d2
Acl flags       : 0x00000001
Number of ACEs

  : 3

<-- 3 ACEs: two explicit and the implicit deny entry


  Ace handle [1] : 0xb700010a
  Ace handle [2] : 0x5800010b


Interface(s):


        TwentyFiveGigE1/0/1                             <-- The interface ACL is applied


##########################################################
#########                                  ##################
########  Policy instance information  ##################
#########                                  ##################
##########################################################
Policy intf handle    : 0x880000c1
Policy handle         : 0x5b000093
ID                    : 9
Protocol              : [3] IPV4
Feature               : [1] AAL_FEATURE_PACL
Direction             : [1] Ingress
Number of ACLs        : 1
Number of VMRs        : 3------------
```

تأكيد عمل PACL.

---

ملاحظة: عندما تدخل show ip access-lists privileged EXEC الأمر، الي يمثل عدد التطابقات المعروض الحزم التي يتم التحكم في الوصول إليها في الجهاز. أستخدم أمر EXEC show platform software الذي تم تغذيته للمحول {switch_num|active|standby} قائمة التحكم في الوصول إلى عدادات الأجهزة ذات الامتيازات للحصول على بعض إحصائيات قوائم التحكم في الوصول الخاصة بالأجهزة الأساسية للحزم المحولة والموجهة.

---

<#root>

```
### Ping originated from neighbor device with source 10.1.1.1 ###

C9300#
ping 10.1.1.2 source g 1/0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1                    <--- Ping source is permitted and p

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms <-- 100% ping success


### Ping originated from neighbor device with source 10.1.1.3 ###
C9300#
ping 10.1.1.2 source g 1/0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.3                    <-- Ping source is denied (implicit

.....
Success rate is 0 percent (0/5)                                  <-- 0% ping success

### Confirm PACL drop ###
9500H#
show access-lists TEST

Extended IP access list TEST

    10 permit ip host 10.1.1.1 any                               <-- Counters in this command do not
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2

9500H#
show platform software fed active acl counters hardware | i PACL Drop
Ingress IPv4 PACL Drop            (0x77000005):         11 frames    <-- Hardware level command displays
Ingress IPv6 PACL Drop            (0x12000012):          0 frames

<...snip...>
```

## السيناريو 2. PACL (قائمة التحكم في الوصول لـ Mac)

يتم تعيين قوائم التحكم في الوصول الخاصة بالمنفذ (PACL) إلى واجهة الطبقة 2.

- حد الأمان: المنافذ أو شبكات VLAN
- المرفق: واجهة الطبقة 2
- الإتجاه: مدخل أو مخرج (واحد في كل مرة)
- أنواع قوائم التحكم في الوصول (ACL) المدعومة: قوائم التحكم في الوصول إلى MAC (قياسية أو موسعة) وقوائم التحكم في الوصول إلى IP

تكوين PACL باستخدام قائمة التحكم في الوصول إلى MAC

```
<#root>

9500H#

show run | sec mac access-list


mac access-list extended

MAC-TEST           <-- MAC ACL named MAC-TEST



permit host 0001.aaaa.aaaa any             <-- permit host MAC to any dest MAC



9500H#

show access-lists MAC-TEST


Extended MAC access list MAC-TEST
    permit host 0001.aaaa.aaaa any

9500H#

show running-config interface twentyFiveGigE 1/0/1


Building configuration...

interface TwentyFiveGigE1/0/1
switchport access vlan 10
switchport mode access

mac access-group MAC-TEST in               <-- Applied MACL to layer 2 interface
```

التحقق من PACL

إسترداد IF_ID المقترن بالواجهة.

```
<#root>

9500H#
```

**show platform software fed active ifm interfaces ethernet**

Interface

**IF_ID**

State

---

**TwentyFiveGigE1/0/1**

**0x00000008**

READY

**<-- IF_ID value for Tw1/0/1**

تحقق من ربط معرف مجموعة الفئات (CG ID) بـ IF_ID.

<#root>

9500H#

**show platform software fed active acl interface 0x8 <-- IF_ID with leading zeros omitted**

```
##########################################################
########                                ##################
#######   Printing Interface Infos     #################
########                                ##################
##########################################################
```

**INTERFACE: TwentyFiveGigE1/0/1 <-- Confirms the interface matches the IF**

MAC 0000.0000.0000

```
##########################################################
    intfinfo: 0x7f489404e408
    Interface handle: 0x7e000028
```

**Interface Type: Port <-- Type: Port indicates Layer 2 interface**

**if-id: 0x0000000000000008 <-- IF_ID 0x8 is correct**

Input MAC: Policy Handle: 0xde000098

**Policy Name: MAC-TEST <-- The named ACL bound to this interface**

**CG ID: 20 <-- Class Group ID for this entry**

```
CGM Feature: [0] acl                                    <-- Feature is ACL

        Bind Order: 0
```

معلومات قائمة التحكم في الوصول (ACL) المقترنة بمعرف CG.

```
<#root>

9500H#

show platform software fed active acl info acl-cgid 20  <-- The CG ID associated to the ACl MAC-TEST


##########################################################
#########                                 ##################
########      Printing CG Entries        #################
#########                                 ##################
##########################################################
==================================

ACL CG (acl/20): MAC-TEST type: MAC                          <-- feature ACL/CG ID 20: ACL name MAC-TES


Total Ref count 1
---------------------------------

1 Interface                                                  <-- Applied to one interface


---------------------------------
  region reg_id: 3
    subregion subr_id: 0
       GCE#:1 #flds: 2 l4:N matchall:N deny:N
         Result: 0x01010000

 mac_dest: value = 0x00, mask = 0x00                  <-- Mac dest: hex 0x00 mask 0x00 is "any destinati



mac_src: value = 0x1aaaaaaaa

,

mask = 0xffffffffffff


<-- Mac source: 0x1aaaaaaaa | hex with leading zeros omitted (0001.aaaa.aaaa) & mask 0xffffffffffff is h
```

معلومات النهج الخاصة بمعرف CG، وكذلك الواجهات التي تستخدم معرف CG.

```
<#root>
```

```
9500H#
show platform software fed active acl policy 20      <-- Use the CG ID value

##########################################################
#########                                  ##################
########     Printing Policy Infos     ##################
#########                                  ##################
##########################################################

INTERFACE: TwentyFiveGigE1/0/1                                  <-- Interface with ACL applied

MAC 0000.0000.0000
##########################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x7e000028
    Interface Type: Port

if-id: 0x0000000000000008                                 <-- The Interface IF_ID 0x8

------------
Direction:  Input                                               <-- ACl is applied in the ingress direction


Protocol Type:MAC                                               <-- Type is MAC


    Policy Intface Handle: 0x30000c6
    Policy Handle: 0xde000098

##########################################################
#########                                  ##################
########         Policy information    ##################
#########                                  ##################
##########################################################
Policy handle         : 0xde000098
Policy name           : MAC-TEST                                <-- ACL name is MAC-TEST


ID                    : 20                                      <-- CG ID for this ACL entry


Protocol              : [1] MAC
Feature               : [1] AAL_FEATURE_PACL                    <-- ASIC Feature is PACL


Number of ACLs        : 1

##########################################################
## Complete policy ACL information
##########################################################
Acl number : 1
====================================
Acl handle : 0xd60000dc
Acl flags : 0x00000001
Number of ACEs : 2                                              <-- 2 ACEs: one permit, and one implicit deny
```

```
  Ace handle [1] : 0x38000120
  Ace handle [2] : 0x31000121
```

**Interface(s):**

**TwentyFiveGigE1/0/1 <-- Interface the ACL is applied**

```
##########################################################
#########                                ##################
########  Policy instance information  ##################
#########                                ##################
##########################################################
Policy intf handle    : 0x030000c6
Policy handle         : 0xde000098
ID                    : 20
Protocol              : [1] MAC
Feature               : [1] AAL_FEATURE_PACL
Direction             : [1] Ingress
Number of ACLs        : 1
Number of VMRs        : 3------------
```

تأكيد عمل PACL:

- يسمح MAC فقط بعنوان المصدر 0001.aaa.aaa.
- ونظرا لأن هذه قائمة تحكم في الوصول (MAC)، يتم إسقاط حزمة ARP غير الخاصة ب IP، مما يؤدي إلى فشل إختبار الاتصال.

<#root>

**### Ping originated from neighbor device with Source MAC 0000.0000.0002 ###**

C9300#

**ping 10.1.1.2 source vlan 10**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.....
```

**Success rate is 0 percent (0/5)**

C9300#

**show ip arp**

```
Protocol  Address          Age (min)  Hardware Addr    Type    Interface
Internet  10.1.1.2                0
```

**Incomplete**

```
       ARPA

<-- ARP is unable to complete on Source device

### Monitor capture configured on Tw 1/0/1 ingress ###

9500H#

monitor capture 1 interface TwentyFiveGigE 1/0/1 in match any


9500H#

show monitor cap

Status Information for Capture 1
  Target Type:


 Interface: TwentyFiveGigE1/0/1, Direction: IN


9500H#sh monitor capture 1 buffer brief | inc ARP

    5   4.767385 00:00:00:00:00:02 b^F^R

ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1


    8   8.767085 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1
   11  10.767452 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1
   13  12.768125 00:00:00:00:00:02 b^F^R ff:ff:ff:ff:ff:ff ARP 60 Who has 10.1.1.2? Tell 10.1.1.1


<-- 9300 (10.1.1.1) sends ARP request, but since there is no reply 4 more ARP requests are sent



9500H#

show platform software fed active acl counters hardware | inc MAC PACL Drop
Ingress MAC PACL Drop                       (0x73000021): 937 frames         <-- Confirmed that ARP requ

Egress MAC PACL Drop                        (0x0200004c): 0 frames

<...snip...>
```

## السيناريو 3. RACL

يتم تعيين قائمة التحكم في الوصول للاستقبال (RACL) لواجهة الطبقة 3 مثل الواجهة SVI أو المجمعة.

- حدود الأمان: شبكات فرعية مختلفة
- المرفق: واجهة الطبقة 3
- الإتجاه: مدخل أو مخرج
- أنواع قوائم التحكم في الوصول (ACL) المدعومة: قوائم التحكم في الوصول إلى IP (قياسية أو موسعة)

تكوين RACL

```
<#root>

9500H(config)#

ip access-list extended TEST          <-- Create a named extended ACL


9500H(config-ext-nacl)#

permit ip host 10.1.1.1 any

9500H(config-ext-nacl)#

permit udp host 10.1.1.1 eq 1000 host 10.1.1.2



9500H#

show access-lists TEST                        <-- Display the ACL configured


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2

9500H(config)#

interface Vlan 10                     <-- Apply ACL to Layer 3 SVI interface


9500H(config-if)#

ip access-group TEST in



9500H#

show running-config interface Vlan 10


Building configuration...

Current configuration : 84 bytes
!
interface Vlan10

 ip access-group TEST in                              <-- Display the ACL applied to the interface


end
```

التحقق من RACL

إسترداد IF_ID المقترن بالواجهة.

```
<#root>

9500H#
```

```
show platform software fed active ifm mappings l3if-le  <-- Retrieve the IF_ID for a Layer 3 SVI type po

Mappings Table

L3IF_LE                    Interface                               IF_ID             Type
------------------------------------------------------------------------------------------------------
0x00007f8d04983958

Vlan10


0x00000026

        SVI_L3_LE

<-- IF_ID value for SVI 10
```

تحقق من ربط معرف مجموعة الفئات (CG ID) ب IF_ID.

```
<#root>

9500H#

show platform software fed active acl interface 0x26  <-- IF_ID for SVI Vlan 10 with leading zeros omitt

############################################################
########                                ##################
#######     Printing Interface Infos    #################
########                                ##################
############################################################

INTERFACE: Vlan10                                          <-- Confirms the interface matches the IF_ID


MAC 0000.0000.0000
############################################################
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x6e000047

Interface Type: L3                                         <-- Type: L3 indicates Layer 3 type interface



if-id: 0x0000000000000026                                  <-- IF_ID 0x26 is correct

    Input IPv4: Policy Handle: 0x2e000095

Policy Name: TEST                                      <-- The named ACL bound to this interface


  CG ID: 9                                           <-- Class Group ID for this entry
```

```
CGM Feature: [0] acl                                    <-- Feature is ACL

        Bind Order: 0
```

معلومات قائمة التحكم في الوصول (ACL) المقترنة بمعرف CG.

```
<#root>

9500H#

show platform software fed active acl info acl-cgid 9  <-- The CG ID associated to the ACL TEST

########################################################
#########                              ##################
########      Printing CG Entries      #################
#########                              ##################
########################################################
==================================

ACL CG (acl/9): TEST type: IPv4


<-- feature ACL/CG ID 9: ACl name TEST : ACl type IPv4


Total Ref count 2
---------------------------------

2 Interface                             <-- Interface count is 2. Applied to SVI 10 and as PACL to Tw1/0/


---------------------------------
region reg_id: 10
  subregion subr_id: 0
    GCE#:1

#flds: 2


l4:N

 matchall:N deny:N

<-- #flds: 2 = two fields in entry | l4:N (no Layer 4 port match)


      Result: 0x01010000

      ipv4_src: value

 =

0x0a010101

,

mask = 0xffffffff
```

**<-- src 0x0a010101 hex = 10.1.1.1 | mask 0xffffffff = exact host match**

**ipv4_dst: value**

**=**

**0x00000000, mask = 0x00000000**

**<--**

**dst & mask = 0x00000000 = match any**

GCE#:1 #flds: 4

**l4:Y**

matchall:N deny:N

**<-- #flds: 4 = four fields in entry | l4:Y (ACE uses UDP port L4 match)**

Result: 0x01010000

**ipv4_src: value = 0x0a010101, mask = 0xffffffff <-- Exact match (host) 10.1.1.1**

**ipv4_dst: value = 0x0a010102, mask = 0xffffffff <-- Exact match (host) 10.1.1.2**

**ip_prot: start = 17, end = 17 <-- protocol 17 is UDP**

**l4_src: start = 1000, end = 1000 <-- matches eq 1000 (equal UDP port 1000)**

معلومات النهج الخاصة بمعرف CG، وكذلك الواجهات التي تستخدم معرف CG.

<#root>

9500H#

**show platform software fed active acl policy 9 <-- Use the CG ID Value**

```
##########################################################
#########                              ##################
########     Printing Policy Infos     ##################
#########                              ##################
##########################################################
```

**INTERFACE: Vlan10 <-- Interface with ACL applied**

MAC 0000.0000.0000

```
##########################################################
```

```
    intfinfo: 0x7f8cfc02de98
    Interface handle: 0x6e000047
    Interface Type: L3
    if-id: 0x0000000000000026                          <-- Interface IF_ID 0x26


------------

Direction:  Input                                      <-- ACL applied in the ingress direction


Protocol Type:IPv4                                     <-- Type is IPv4


    Policy Intface Handle: 0x1c0000c2
    Policy Handle: 0x2e000095


############################################################
#########                                  ##################
########        Policy information          #################
#########                                  ##################
############################################################
Policy handle        : 0x2e000095
Policy name          : TEST                            <-- ACL name TEST


ID                   : 9


<-- CG ID for this ACL entry


Protocol             : [3] IPV4
Feature              : [27] AAL_FEATURE_RACL           <-- ASIC feature is RACL


Number of ACLs       : 1

############################################################
## Complete policy ACL information
############################################################
Acl number       : 1
====================================
Acl handle         : 0x7c0000d4
Acl flags          : 0x00000001
Number of ACEs     : 5                                 <-- 5 Aces: 2 explicit, 1 implicit deny, 2 ???


  Ace handle [1] : 0x0600010f
  Ace handle [2] : 0x8e000110
  Ace handle [3] : 0x3b000111
  Ace handle [4] : 0xeb000112
  Ace handle [5] : 0x79000113


Interface(s):
```

```
        Vlan10                                          <-- The interface the ACL is applied

#########################################################
#########                              ##################
########  Policy instance information  #################
#########                              ##################
#########################################################
Policy intf handle     : 0x1c0000c2
Policy handle          : 0x2e000095
ID                     : 9
Protocol               : [3] IPV4
Feature                : [27] AAL_FEATURE_RACL
Direction              : [1] Ingress
Number of ACLs         : 1
Number of VMRs         : 4------------
```

تأكيد أن RACL يعمل.

---

ملاحظة: عندما تدخل show ip access-lists privileged EXEC الأمر، الا يمثل عدد التطابقات المعروض الحزم التي يتم التحكم في الوصول إليها في الجهاز. أستخدم show platform software fed switch{switch_num|active|standby}أجهزة عدادات قائمة التحكم في الوصول الأمر EXEC ذي الامتيازات للحصول على بعض إحصائيات قائمة التحكم في الوصول (ACL) الخاصة بالأجهزة الأساسية للحزم المحولة والموجهة.

---

<#root>

```
### Ping originated from neighbor device with source 10.1.1.1 ###


C9300#

ping 10.1.1.2 source g 1/0/1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.1                    <--- Ping source is permitted and p


!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms <-- 100% ping success



### Ping originated from neighbor device with source 10.1.1.3 ###

C9300#

ping 10.1.1.2 source g 1/0/1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

Packet sent with a source address of 10.1.1.3                    <-- Ping source is denied (implicit
```

```
.....
Success rate is 0 percent (0/5)                                    <-- 0% ping success


### Confirm RACL drop ###

9500H#

show access-lists TEST


Extended IP access list TEST


    10 permit ip host 10.1.1.1 any                                 <-- Counters in this command do not
    20 permit udp host 10.1.1.1 eq 1000 host 10.1.1.2


9500H#

show platform software fed active acl counters hardware | i RACL Drop
Ingress IPv4 RACL Drop              (0xed000007):         100 frames  <-- Hardware level command display


<...snip...>
```

## السيناريو 4. VACL

عينت VLANs إلى طبقة 2 VLAN.

- حدود الأمان: داخل شبكة VLAN أو عبرها
- المرفق: خريطة VLAN/VLAN
- الإتجاه: الدخول والخروج في آن واحد
- أنواع قوائم التحكم في الوصول (ACL) المدعومة: قوائم التحكم في الوصول إلى MAC وقوائم التحكم في الوصول إلى IP (قياسية أو موسعة)

تكوين VACL

<#root>

```
ip access-list extended TEST


 10 permit ip host 10.1.1.1 any
 20 permit ip any host 10.1.1.1


ip access-list extended ELSE


 10 permit ip any any


vlan access-map VACL 10
```

```
 match ip address TEST
 action forward
```

**vlan access-map VACL 20**

```
 match ip address ELSE
 action drop
```

**vlan filter VACL vlan-list 10**

9500H#

**sh vlan access-map VACL**

```
Vlan access-map "VACL" 10
  Match clauses:
    ip address: TEST
```

**Action:**

**forward**

```
Vlan access-map "VACL" 20
  Match clauses:
    ip address: ELSE
```

**Action:**

**drop**

9500H#

**sh vlan filter access-map VACL**

VLAN Map VACL is filtering VLANs:

**10**

## التحقق من VACL

إسترداد IF_ID المقترن بالواجهة.

<#root>

9500H#

**show platform software fed active ifm interfaces vlan**

```
Interface
IF_ID
               State
--------------------------------------------------------------------
Vlan10                           0x00420010
        READY
```

تحقق من ربط معرف مجموعة الفئات (CG ID) ب IF_ID.

```
<#root>
9500H#
show platform software fed active acl interface 0x420010  <-- IF_ID for the Vlan


#########################################################
########                               ##################
#######   Printing Interface Infos     ##################
########                               ##################
#########################################################

INTERFACE: Vlan10                                          <-- Can be L2 only, with no vlan interfa


MAC 0000.0000.0000
#########################################################
    intfinfo: 0x7fc8cc7c7f48
    Interface handle: 0xf1000024
    Interface Type: Vlan
    if-id: 0x0000000000420010

Input IPv4:

 Policy Handle: 0xd10000a3
<-- VACL has both Ingress and Egress actions



Policy Name: VACL                                    <-- Name of the VACL used



CG ID: 530                                         <-- Class Group ID for entry



 CGM Feature: [35] acl-grp                           <-- Feature is ACL group, versus ACl

        Bind Order: 0
```

**Output IPv4:**

```
 Policy Handle: 0xc80000a4
```

**<-- VACL has both Ingress and Egress actions**

```
         Policy Name: VACL
              CG ID: 530
         CGM Feature: [35] acl-grp
    Bind Order: 0
```

معلومات قائمة التحكم في الوصول (ACL) المقترنة بمعرف مجموعة CG.

هناك قوائم التحكم في الوصول (ACL) مستخدمة في سياسة قائمة التحكم في الوصول في هذه المجموعة، مجمعة في مجموعة قائمة التحكم في الوصول إلى شبكة VACL المسماة نفسها

<#root>

```
9500H#
```

**show platform software fed active acl info acl-grp-cgid 530  <-- use the group-id command versus gc ID**

```
##########################################################
#########                                ##################
########    Printing CG Entries          #################
#########                                ##################
##########################################################
==================================
```

**ACL CG (acl-grp/530): VACL type: IPv4                                  <-- feature acl/group ID 530: name VA**

```
Total Ref count 2
---------------------------------
```

**2 VACL                                                                 <-- Ingress and egress ACL direction**

```
---------------------------------
  region reg_id: 12
    subregion subr_id: 0
      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x06000000
```

**ipv4_src: value = 0x0a010101, mask = 0xffffffff           <-- permit from host 10.1.1.1 (see PACL exampl**

**ipv4_dst: value = 0x00000000, mask = 0x00000000           <-- to any other host**

```
      GCE#:20 #flds: 2 l4:N matchall:N deny:N
        Result: 0x06000000
```

**ipv4_src: value = 0x00000000, mask = 0x00000000           <-- permit from any host**

```
ipv4_dst: value = 0x0a010101, mask = 0xffffffff          <-- to host 10.1.1.1

      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x05000000

 ipv4_src: value = 0x00000000, mask = 0x00000000          <-- This is the ACL named 'ELSE' which is per

        ipv4_dst: value = 0x00000000, mask = 0x00000000          <-- with VACL, the logic used was "per
```

معلومات النهج الخاصة بمعرف CG، وكذلك الواجهات التي تستخدم معرف CG.

```
<#root>

9500H#

show platform software fed active acl policy 530     <-- use the acl-grp ID


##########################################################
#########                                ##################
########     Printing Policy Infos      #################
#########                                ##################
##########################################################

INTERFACE: Vlan10
MAC 0000.0000.0000
##########################################################
    intfinfo: 0x7fa15802a5d8
    Interface handle: 0xf1000024

Interface Type: Vlan                                    <-- Interface type is the Vlan, not a specific in



if-id: 0x0000000000420010                               <-- the Vlan IF_ID matches Vlan 10


------------

Direction: Input                                            <-- VACL in the input direction


Protocol Type:IPv4
    Policy Intface Handle: 0x44000001
    Policy Handle: 0x29000090

##########################################################
#########                                ##################
########       Policy information       #################
#########                                ##################
##########################################################
Policy handle       : 0x29000090

Policy name         : VACL                                  <-- the VACL policy is named 'VACL'
```

```
ID                  : 530
Protocol            : [3] IPV4
Feature             : [23] AAL_FEATURE_VACL              <-- ASIC feature is VACL


Number of ACLs      : 2                                  <-- 2 ACL used in the VACL: "TEST & ELSE"


############################################################
## Complete policy ACL information
############################################################
Acl number : 1
====================================
Acl handle : 0xa6000090
Acl flags : 0x00000001
Number of ACEs : 4
  Ace handle [1] : 0x87000107
  Ace handle [2] : 0x30000108
  Ace handle [3] : 0x73000109
  Ace handle [4] : 0xb700010a

Acl number : 2
====================================
Acl handle : 0x0f000091
Acl flags : 0x00000001
Number of ACEs : 1
  Ace handle [1] : 0x5800010b

Interface(s):
        Vlan10
############################################################
#########                                  ##################
########  Policy instance information  ##################
#########                                  ##################
############################################################
Policy intf handle    : 0x44000001
Policy handle         : 0x29000090
ID                    : 530                            <-- 530 is the acl group ID


Protocol              : [3] IPV4
Feature               : [23] AAL_FEATURE_VACL
Direction             : [1] Ingress                    <-- Ingress VACL direction


Number of ACLs        : 2
Number of VMRs        : 4------------
Direction:  Output
Protocol Type:IPv4
    Policy Intface Handle: 0xac000002
    Policy Handle: 0x31000091

############################################################
#########                                  ##################
########        Policy information     ##################
#########                                  ##################
############################################################
Policy handle        : 0x31000091
```

```
Policy name          : VACL
ID                   : 530
Protocol             : [3] IPV4
Feature              : [23] AAL_FEATURE_VACL
Number of ACLs       : 2

#########################################################
## Complete policy ACL information
#########################################################
Acl number    : 1
=====================================
Acl handle      : 0xe0000092
Acl flags       : 0x00000001
Number of ACEs  : 4
  Ace handle [1] : 0xf500010c
  Ace handle [2] : 0xd800010d
  Ace handle [3] : 0x4c00010e
  Ace handle [4] : 0x0600010f

Acl number    : 2
=====================================
Acl handle      : 0x14000093
Acl flags       : 0x00000001
Number of ACEs : 1
  Ace handle [1] : 0x8e000110

Interface(s):
        Vlan10
#########################################################
#########                              ##################
########  Policy instance information  #################
#########                              ##################
#########################################################
Policy intf handle    : 0xac000002
Policy handle         : 0x31000091

ID                    : 530                             <-- 530 is the acl group ID


Protocol              : [3] IPV4
Feature               : [23] AAL_FEATURE_VACL

Direction             : [2] Egress                      <-- Egress VACL direction


Number of ACLs        : 2
Number of VMRs        : 4------------
```

تأكيد أن VACL يعمل.

- أستكشاف الأخطاء وإصلاحها وه نفس السيناريو الخاص بأقسام PACL و RACl. راجع هذه الأقسام للحصول على تفاصيل حول إختبار الاتصال.
- تم رفض إختبار الاتصال من 10.1.1.3 إلى 10.1.1.2 بواسطة سياسة قائمة التحكم في الوصول (ACL) المطبقة.
- تحقق من أمر إسقاط النظام الأساسي.

<#root>

```
9500H#
show platform software fed active acl counters hardware | inc VACL Drop


Ingress IPv4 VACL Drop
              (0x23000006):
1011 frames      <-- Hardware level command displays drops against VACL


<...snip...>
```

## السيناريو 5. قائمة التحكم في الوصول الخاصة بالمجموعة/العميل (DACL)

يتم تطبيق قوائم التحكم في الوصول (ACL) الخاصة بالمجموعة/العميل بشكل ديناميكي على مجموعة مستخدمين أو عميل استنادا إلى هويتهم. ويسمى هذا أحيانا أيضا DACL.

- حدود الأمان: العميل (مستوى واجهة العميل)
- المرفق: كل واجهة زبون
- الإتجاه: مدخل فقط
- أنواع قوائم التحكم في الوصول (ACL) المدعومة: قوائم التحكم في الوصول إلى MAC وقوائم التحكم في الوصول (ACL) إلى IP (قياسية أو موسعة)

تكوين GACL

<#root>

```
Cat9400#
show run interface gigabitEthernet 2/0/1

Building configuration...

Current configuration : 419 bytes
!
interface GigabitEthernet2/0/1
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 5


ip access-group ACL-ALLOW in                    <-- This is the pre-authenticated ACL (deny ip any any)

 authentication periodic
 authentication timer reauthenticate server
 access-session control-direction in
 access-session port-control auto
 no snmp trap link-status
 mab
 dot1x pae authenticator
 spanning-tree portfast
```

```
service-policy type control subscriber ISE_Gi2/0/1

end

Cat9400#

show access-session interface gigabitEthernet 2/0/1 details

            Interface:  GigabitEthernet2/0/1

 IIF-ID:  0x1765EB2C               <-- The IF_ID used in this example is dynamic


 MAC Address:  000a.aaaa.aaaa            <-- The client MAC

         IPv6 Address:  Unknown
         IPv4 Address:  10.10.10.10
            User-Name:  00-0A-AA-AA-AA-AA


Status:  Authorized               <-- Authorized client

               Domain:  VOICE
       Oper host mode:  multi-auth
     Oper control dir:  in
      Session timeout:  300s (server), Remaining: 182s
       Timeout action:  Reauthenticate
    Common Session ID:  27B17A0A000003F499620261
      Acct Session ID:  0x000003e7
               Handle:  0x590003ea
       Current Policy:  ISE_Gi2/0/1


Server Policies:

              ACS ACL:

xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

  <-- The ACL pushed from ISE server


Method status list:
       Method           State
        dot1x           Stopped

 mab           Authc Success                                    <-- Authenticated via MAB (Mac authent


Cat9400#

show ip access-lists xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

Extended IP access list xACSACLx-IP-MAB-FULL-ACCESS-GOOD-59fb6e5e

 1 permit ip any any                                                <-- ISE pushed a permit ip any ar
```

## التحقق من GACL

معرف CG للمجموعة المرتبط بمعرف iif.

```
<#root>

Cat9400#

show platform software fed active acl interface 0x1765EB2C                <-- The IF_ID from the access

##########################################################
########                                ##################
#######    Printing Interface Infos    #################
########                                ##################
##########################################################

INTERFACE: Client MAC

000a.aaaa.aaaa

                                                <-- Client MAC matches the access-session output

MAC

000a.aaaa.aaaa

##########################################################
    intfinfo: 0x7f104820cae8
    Interface handle: 0x5a000110

Interface Type: Group                                                     <-- This is a group ident


IIF ID: 0x1765eb2c

    Input IPv4: Policy Handle: 0x9d00011e


  Policy Name: ACL-ALLOW:xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

:

<-- DACL name matches



CG ID: 127760                                                          <-- The ACL group ID

       CGM Feature: [35]

acl-grp

        Bind Order: 0
```

معلومات قائمة التحكم في الوصول (ACL) المقترنة بمعرف GC الخاص بالمجموعة.

```
<#root>

Cat9400#

show platform software fed active acl info acl-grp-cgid 127760                          <-- the CG ID
```

```
#########################################################
#########                                ################
########      Printing CG Entries       ################
#########                                ################
#########################################################
==================================
ACL CG (

acl-grp/127760

):

ACL-ALLOW:xACSACLx-IP-MAB-FULL-ACCESS-59fb6e5e

: type: IPv4

<-- Group ID & ACL name are correct


Total Ref count 1
---------------------------------

1 CGACL                                                                                                    <-- 1

---------------------------------
  region reg_id: 1
    subregion subr_id: 0
      GCE#:1 #flds: 2 l4:N matchall:N deny:N
        Result: 0x04000000


 ipv4_src: value = 0x00000000, mask = 0x00000000                                                           <-- Permits I
        ipv4_dst: value = 0x00000000, mask = 0x00000000

      GCE#:10 #flds: 2 l4:N matchall:N deny:N
        Result: 0x04000000
        ipv4_src: value = 0x00000000, mask = 0x00000000
        ipv4_dst: value = 0x00000000, mask = 0x00000000
```

## السيناريو 6. تسجيل قائمة التحكم في الوصول (ACL)

يمكن أن يوفر برنامج الجهاز رسائل syslog حول الحزم المسموح بها أو المرفوضة بواسطة قائمة وصول IP القياسية. تتسبب أي حزمة تطابق قائمة التحكم في الوصول (ACL) في إرسال رسالة سجل معلومات حول الحزمة إلى وحدة التحكم. يتم التحكم في مستوى الرسائل التي تم تسجيلها إلى وحدة التحكم بواسطةوحدة تحكم التسجيلأوامر التحكم في رسائل syslog.

- رسائل سجل قائمة التحكم في الوصول غير مدعومة لقوائم التحكم في الوصول (ACL) المستخدمة لإعادة توجيه المسار العكسي للبث الأحادي (uRPF). وهو مدعوم فقط لـ RACL.
- سجل قائمة التحكم في الوصول في إتجاه المخرج غير مدعوم للحزم التي يتم إنشاؤها من مستوى التحكم بالجهاز.
- يتم التوجيه في الأجهزة وتسجيل الدخول إلى البرنامج، لذلك إذا تطابق عدد كبير من الحزم مع ACE التصريحي أو الرفض الذي يحتوي على كلمة أساسية log، فلن يكون البرنامج قادرا على مطابقة معدل معالجة الجهاز، ولا يمكن تسجيل جميع الحزم.

- تتسبب الحزمة الأولى التي تشغل قائمة التحكم في الوصول في ظهور رسالة سجل مباشرة، ويتم تجميع الحزم التالية على أول 5 دقائق قبل أن يظهر أو يتم تسجيلها. تتضمن رسالة السجل رقم قائمة الوصول، ما إذا كان قد تم السماح للحزمة أو رفضها، وعنوان IP للمصدر للحزمة، وعدد الحزم من ذلك المصدر المسموح بها أو المرفوضة في فترة الخمس دقائق السابقة.
- راجع دليل تكوين الأمان المناسب، Cisco IOS XE كما هو موضح في قسم المعلومات ذات الصلة للحصول على تفاصيل كاملة حول سلوك سجل قائمة التحكم في الوصول وقيوده.

سجل مثال PACL:

يوضح هذا المثال حالة سلبية، حيث لا يعمل نوع قائمة التحكم في الوصول والكلمة الأساسية log.

```
<#root>

9500H#

show access-lists TEST


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any

log             <-- Log keyword applied to ACE entry


    20 deny ip host 10.1.1.3 any

log


9500H(config)#

interface twentyFiveGigE 1/0/1

9500H(config-if)#

ip access-group TEST in           <-- apply logged ACL
Switch Port ACLs are not supported for LOG!        <-- message indicates this is an unsupported combinat
```

سجل مثال RACL (رفض):

```
<#root>

9500H#

show access-lists TEST


Extended IP access list TEST
    10 permit ip host 10.1.1.1 any

log            <-- Log keyword applied to ACE entry
```

```
    20 deny ip host 10.1.1.3 any
log


9500H(config)#
interface vlan 10

9500H(config-if)#
ip access-group TEST in          <-- ACL applied to SVI

### Orginate ICMP from 10.1.1.3 to 10.1.1.2 (denied by ACE) ###
C9300#
ping 10.1.1.2 source vlan 10 repeat 110
Type escape sequence to abort.


Sending 10, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.3
..........

Success rate is 0 percent (0/110)

9500H#
show access-list TEST

Extended IP access list TEST
    10 permit ip host 10.1.1.1 any log

 20 deny ip host 10.1.1.3 any log (110 matches)  <-- Matches increment in show access-list command

9500H#
show platform software fed active acl counters hardware | inc RACL
Ingress IPv4 RACL Drop          (0xed000007):            0 frames
Ingress IPv4 RACL Drop and Log  (0x93000009):          110 frames   <-- Aggregate command shows hits on

%SEC-6-IPACCESSLOGDP: list TEST denied icmp 10.1.1.3 -> 10.1.1.2 (8/0), 10 packets  <-- Syslog message i
```

تسجيل مثال RACL (السماح):
عند إستخدام عبارة سجل لبيان السماح، تظهر مرات وصول عداد البرامج ضعف عدد الحزم المرسلة.

```
<#root>
C9300#
```

```
ping 10.1.1.2 source vlan 10 repeat 5          <-- 5 ICMP Requests are sent


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 1/1/1 ms

9500H#

show access-lists TEST


Extended IP access list TEST


 10 permit ip host 10.1.1.1 any log (10 matches)  <-- Hit counter shows 10


    20 deny ip host 10.1.1.3 any log (115 matches)
```

# استكشاف الأخطاء وإصلاحها

## إحصائيات قائمة التحكم في الوصول (ACL)

عند أستكشاف أخطاء قائمة التحكم في الوصول (ACL) وإصلاحها، فمن الضروري فهم كيفية قياس إحصائيات قائمة التحكم في الوصول (ACL) بواسطة الجهاز ومكان قياسها.

- يتم تجميع إحصائيات قائمة التحكم في الوصول (ACL) على مستوى إجمالي وليس على مستوى ACE.
- لا تتوفر لدى الأجهزة إمكانية السماح لكل ACE أو لكل حالة من حالات قائمة التحكم في الوصول (ACL).
- يتم تجميع إحصائيات مثل الرفض والسجل والحزم المعاد توجيهها لوحدة المعالجة المركزية.
- يتم تجميع إحصائيات حزم IPv6 و IPv4 و MAC بشكل منفصل.
- يمكن إستخدام show platform software fed switch active acl counters hardware لعرض إحصائيات التجميع.

## مسح إحصائيات قوائم التحكم في الوصول (ACL)

عند أستكشاف أخطاء قائمة التحكم في الوصول (ACL) وإصلاحها، قد يكون من المفيد مسح عدادات قائمة التحكم في الوصول (ACL) المختلفة للحصول على أعداد أساسية جديدة.

- تتيح لك هذه الأوامر مسح إحصائيات عداد قائمة التحكم في الوصول (ACL) للبرامج والأجهزة.
- عندما تقوم باستكشاف أخطاء أحداث مطابقة/إصابة قائمة التحكم في الوصول (ACL) وإصلاحها، يوصى بمسح قائمة التحكم في الوصول (ACL) ذات الصلة إلى تطابقات الخط الأساسي الحديثة أو ذات الصلة.

<#root>

**clear platform software fed active acl counters hardware**

 (clears the hardware matched counters)

**clear ip access-list counters**

 (clears the software matched counters - IPv4)

**clear ipv6 access-list counters**

 (clears the software matched counters - IPv6)

## ماذا يحدث عندما يكون ACL TCAM ممتلئا؟

- يتم تطبيق قوائم التحكم في الوصول (ACL) دائما في TCAM الخاص بالأجهزة. إذا كان TCAM مستخدما بالفعل من قبل قوائم التحكم في الوصول (ACL) التي تم تكوينها مسبقا، فإن قوائم التحكم في الوصول (ACL) الجديدة لا تحصل على موارد قائمة التحكم في الوصول (ACL) المطلوبة المطلوبة للبرمجة.
- إذا تمت إضافة قائمة التحكم في الوصول (ACL) بعد استنفاد TCAM، يتم إسقاط جميع الحزم للقارن الذي يتم إرفاقه.
- يسمى إجراء الاحتفاظ بقوائم التحكم في الوصول (ACL) في البرنامج إلغاء التحميل.
- عند توفر الموارد، يحاول المحول تلقائيا برمجة قوائم التحكم في الوصول (ACL) في الجهاز. في حال نجاح هذه الخطوة، يتم دفع قوائم التحكم في الوصول إلى الأجهزة وتبدأ الحزم في إعادة التوجيه.
- إن عملية برمجة قائمة التحكم بالوصول (ACL) التي يتم حملها بواسطة البرنامج إلى TCAM تسمى إعادة التحميل.
- يمكن إلغاء تحميل/إعادة تحميل PACL و VACL و RACL و GACL بشكل مستقل عن بعضها البعض.

## معدل إستهلاك ACL TCAM

- تبدأ الواجهة التي يتم تطبيق قائمة التحكم في الوصول (ACL) التي تمت إضافتها حديثا في إسقاط الحزم حتى تصبح موارد الأجهزة متوفرة.
- يتم وضع عملاء قائمة التحكم في الوصول للبنية الأساسية (GACL) في والية UnAuth.

## إستهلاك وحدة معالجة الرسومات (VCU)

- وبمجرد تجاوز حد L4OPs أو من وحدات VCU، يقوم البرنامج بتنفيذ توسعة قائمة التحكم بالوصول (ACL) وينشئ إدخالات ACE جديدة لتنفيذ إجراء مكافئ دون إستخدام وحدات VCU.
- بمجرد حدوث ذلك، يمكن أن تصبح TCAM مرهقة من هذه الإدخالات المضافة.

## أخطاء ACL Syslog

إذا نفدت من مكان موارد قائمة تحكم في الوصول (ACL) أمان معين، فسيتم إنشاء رسائل syslog بواسطة النظام (الواجهة، وشبكة VLAN، والتسمية، وما إلى ذلك، ويمكن أن تختلف القيم).

| رسالة سجل ACL | التعريف | إجراء الاسترداد |
|---|---|---|
| %ACL_ERRMSG-4-unload: تم تفريغ الحمولة 1: الإدخال <ACL> على الواجهة <interface> غير مبرمج في الأجهزة وتم إسقاط حركة مرور إلى البيانات. | تم إلغاء تحميل قائمة التحكم في الوصول (ACL) (تحتفظ بها في البرنامج) | تحقق من مقياس TCAM. إذا كانت أكبر من النطاق، قم بإعادة تصميم قوائم التحكم في الوصول (ACL). |
| %ACL_ERRMSG-6-Remove: تم تفريغ 1%: تمت إزالة التكوين غير المحمل للإدخال <ACL> على الواجهة <interface> للتسمية <label>asic<number>. | تمت إزالة تكوين قائمة التحكم في الوصول (ACL) غير المحملة من الواجهة | تمت إزالة قائمة التحكم في الوصول (ACL) بالفعل، لا يوجد إجراء يجب إتخاذه |
| %ACL_ERRMSG-6-RELOAD: تم تحميل الآن إدخال <ACL> على الواجهة <interface> إلى الجهاز للتسمية <label> على asic<number>. | تم تثبيت قائمة التحكم في الوصول (ACL) الآن في الأجهزة | تم حل المشكلة مع قائمة التحكم في الوصول (ACL) الآن في الجهاز، ولم يتم إتخاذ أي إجراء |
| %ACL_ERRMSG-3-ERROR: لم يتم تطبيق تكوين <ACL> IP ACL للإدخال <number> في أمر التطبيق على <interface>. | أنواع أخرى من أخطاء قائمة التحكم في الوصول (مثل dot1x ACL لفشل التثبيت) | تأكد من دعم تكوين قائمة التحكم في الوصول (ACL)، والمقياس TCAM لا يتعدى |
| %ACL_ERRMSG-6-GACL_INFO: الحمولة 1 لـ GACL غير مدعومة: fed: R0/0: | تحتوي GACL على خيار سجل | إزالة سجلات GACL. لا يدعم GACL عبارات السجل من GACL. |

| | | |
|---|---|---|
| | تم تكوينه | |
| ٪ACL_ERRMSG-6-PACL_INFO: المجال 1 R0/0: fed: التسجيل غير مدعوم لـ PACL. | تحتوي قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) على خيار سجل تم تكوينه | لا تدعم قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) عبارات السجلات. إزالة السجل من PACL. |
| ٪ACL_ERRMSG-3-ERROR: المجال 1 R0/0: مقبض: إدخال IPv4 مجموعة ACL implicit_deny:<name>: لا يتم تطبيق التكوين على Client MAC 0000.0000. | فشل (dot1x) قائمة التحكم في الوصول (ACL) في التطبيق على المنفذ الهدف | تأكد من دعم تكوين قائمة التحكم في الوصول (ACL)، والسعة المتاحة لـ TCAM |

## سيناريوهات خارج المواردوإجراءات الاسترداد

| السيناريو 1. ربط قائمة التحكم في الوصول (ACL) | إجراء الاسترداد |
|---|---|
| • يتم إنشاء قائمة التحكم في الوصول (ACL) وتطبيقها على واجهة أو شبكة VLAN.<br>• فشل الربط بسبب شروط "خارج الموارد"، مثل استهلاك TCAM.<br>• لا يمكن برمجة أي من إدخالات ACE لقائمة التحكم في الوصول (ACL) في TCAM. تظل قائمة التحكم في الوصول (ACL) في حالة إلغاء التحميل.<br>• في حالة إلغاء التحميل، تسقط كل حركة المرور (بما في ذلك حزم التحكم) على الواجهة حتى يتم إصلاح المشكلة. | قم بإعادة تصميم قائمة التحكم في الوصول (ACL) لتقليل استخدام TCAM. |
| السيناريو 2. تحرير قائمة التحكم في الوصول (ACL) | إجراء الاسترداد |
| • يتم إنشاء قائمة تحكم في الوصول (ACL) وتطبيقها على واجهة، كما تتم إضافة المزيد من إدخالات ACE إلى قائمة | قم بإعادة تصميم قائمة التحكم في الوصول (ACL) لتقليل استخدام TCAM. |

| | |
|---|---|
| | التحكم في الوصول هذه لأنها تنطبق على الواجهة (الواجهات).<br>• إذا لم يكن TCAM يحتوي على موارد، فإن عملية التحرير تفشل.<br>• لا يمكن برمجة أي وحدات ACE داخل قائمة التحكم في الوصول (ACL) في TCAM. تبقى قائمة التحكم في الوصول (ACL) في حالة الإغلاق التحميلي.<br>• في حالة الإغلاق التحميلي، تسقط كل حركات المرور (بما في ذلك حزم التحكم) على الواجهة حتى يتم إصلاح المشكلة.<br>• تفشل إدخالات قائمة التحكم في الوصول (ACL) الموجودة في حالة الإغلاق التحميلي حتى يتم إصلاح هذه الحالة. |
| السيناريو 3. ACL Re-Bind | الاسترداد |
| • إعادة تطبيق قائمة التحكم في الوصول (ACL) على الواجهة، ثم إزالة قائمة التحكم في الوصول (ACL) الخاصة بالإخراج وهي بنفس الواجهة دون فصل قائمة التحكم في الوصول (ACL) الأولى.<br>• يتم إنشاء قائمة التحكم في الوصول (ACL) الأولى وإرفاقها بنجاح.<br>• يتم إنشاء قائمة تحكم في الوصول (ACL) أكبر باسم مختلف وبنفس البروتوكول (IPv4/IPv6) وتتصل بنفس الواجهة.<br>• يقوم الجهاز بفصل قائمة التحكم في الوصول (ACL) الأولى بنجاح وإرفاق قائمة التحكم في الوصول (ACL) الجديدة بهذه الواجهة.<br>• إذا لم يكن TCAM يحتوي على موارد فإن عملية إعادة الربط تفشل.<br>• لا يمكن برمجة أي وحدات ACE داخل قائمة التحكم في الوصول (ACL) في TCAM. تظل قائمة التحكم في الوصول (ACL) في حالة الإغلاق التحميلي.<br>• في حالة الإغلاق التحميلي، تسقط كل حركة مرور (بما في ذلك حزم التحكم) على الواجهة حتى يتم إصلاح المشكلة. | تقييم إعادة تصميم قائمة التحكم في الوصول (ACL) لتقليل استخدام TCAM. |
| السيناريو 4. ربط قائمة التحكم في الوصول | الاسترداد |

| | |
|---|---|
| (ACL) القائمة الفارغة (الخالية) | |
| • يتم إنشاء قائمة تحكم بالوصول (ACL) ليس لها إدخالات ACE وترتبط بواجهة.<br>• يقوم النظام بإنشاء قائمة التحكم في الوصول (ACL) هذه داخليا باستخدام تصريح "أي ACE"، ويرتبط بالواجهة في الجهاز (يتم السماح بجميع حركات المرور في هذه الحالة).<br>• ثم تتم إضافة إدخالات ACE إلى قائمة التحكم بالوصول (ACL) بنفس الاسم أو الرقم. يقوم النظام بوضع TCAM عند إضافة كل ACE.<br>• إذا نفدت موارد TCAM عند إضافة إدخالات ACE، يتم نقل قائمة التحكم في الوصول (ACL) إلى حالة الإغاء التحميل.<br>• في حالة الإغاء التحميل، تسقط كل حركة مرور (بما في ذلك حزم التحكم) على الواجهة حتى يتم إصلاح المشكلة.<br>• كما تفشل إدخالات قائمة التحكم في الوصول (ACL) الموجودة في حالة الإغاء التحميل حتى يتم إصلاح هذه الحالة. | يقوم بإعادة تصميم قائمة التحكم في الوصول (ACL) لتقليل استخدام TCAM. |

## التحقق من قياس قائمة التحكم في الوصول (ACL)

يغطي هذا القسم الأوامر لتحديد قياس قائمة التحكم في الوصول واستخدام TCAM.

ملخص قائمة الوصول إلى FMAN:

تحديد قوائم التحكم في الوصول (ACL) التي تم تكوينها وإجمالي عدد ACE لكل قائمة تحكم في الوصول (ACL).

```
<#root>

9500H#

show platform software access-list f0 summary


Access-list

                         Index        Num Ref

 Num ACEs

--------------------------------------------------------------------------

TEST
```

```
                                    1           1             2

<-- ACL TEST contains 2 ACE entries


ELSE                                2           1             1
DENY                                3           0             1
```

إستخدام قائمة التحكم في الوصول (ACL:

```
<#root>

9500H#

show platform software fed active acl usage

##########################################################
########                                  ##################
#######      Printing Usage Infos         #################
########                                  ##################
##########################################################
#####

ACE Software VMR max:196608 used:283                    <-- Value/Mask/Result entry usage


##########################################################
==========================================================================================================

Feature Type


ACL Type


Dir


Name


 Entries Used


VACL                    IPV4            Ingress          VACL                    4

<-- Type of ACL Feature, type of ACL, Direction ACL applied, name of ACL, and number of TCAM entries cor

==========================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries Used
RACL                    IPV4            Ingress         TEST                    5
```

إستخدام TCAM (17.x):

يحتوي أمر إستخدام TCAM على إختلافات كبيرة بين قطارات 16.x و 17.x.

<#root>

9500H#

**show platform hardware fed active fwd-asic resource tcam utilization**

Codes: EM - Exact_Match,

**I - Input**

,

**O - Output**

, IO - Input & Output, NA - Not Applicable

**CAM Utilization for ASIC [0]**

Table Subtype

**Dir**

**Max**

Used

**%Used**

V4 V6 MPLS Other

---

**Security ACL Ipv4**

TCAM

**I**

**7168**

16

**0.22%**

16 0 0 0

Security ACL Non Ipv4 TCAM I 5120 76 1.48% 0 36 0 40

Security ACL Ipv4 TCAM

**O**

7168 18 0.25% 18 0 0 0

Security ACL Non Ipv4 TCAM O 8192 27 0.33% 0 22 0 5

**<...snip...>**

**<-- Percentage used and other counters about ACL consumption**
**<-- Dir = ACL direction (Input/Output ACl)**

إستخدام TCAM (16.x):

يحتوي أمر إستخدام TCAM على إختلافات كبيرة بين قطارات 16.x و 17.x.

```
<#root>

C9300#

show platform hardware fed switch active fwd-asic resource tcam utilization

CAM Utilization for ASIC [0]
 Table                                              Max Values

Used Values

----------------------------------------------------------------------------


 Security Access Control Entries                        5120

 126         <-- Total used of the Maximum
<...snip...>
```

قالب إدارة قاعدة بيانات المحول (SDM) المخصص (إعادة تخصيص TCAM)

باستخدام Cisco IOS XE Bengaluru 17.4.1، يمكنك تكوين قالب إدارة قاعدة بيانات المحول (SDM) مخصص لميزات قائمة التحكم في الوصول باستخدام sdm prefer custom acl erasecat4000_flash:.

تتم تغطية تفاصيل حول كيفية تكوين هذه الميزة والتحقق من صحتها في دليل تكوين إدارة النظام، Cisco IOS XE Bengaluru 17.4.x (محولات Catalyst 9500 Switches).

تمت مالحظة بعض عمليات التكوين والتحقق الأساسية في هذا القسم.

التحقق من قالب إدارة قاعدة بيانات المحول (SDM) الحالي:

```
<#root>

9500H#

show sdm prefer

Showing SDM Template Info

This is the Core template.                                                    <-- Core SD

  Security Ingress IPv4 Access Control Entries*:         7168  (current) - 7168  (proposed)  <-- IPv4 AC

  Security Ingress Non-IPv4 Access Control Entries*:     5120  (current) - 5120  (proposed)
```

```
  Security Egress IPv4 Access Control Entries*:          7168  (current) - 7168  (proposed)
  Security Egress Non-IPv4 Access Control Entries*:      8192  (current) - 8192  (proposed)

  <...snip...>


9500H#

show sdm prefer custom user-input

Custom Template Feature Values are not modified

<-- No customization to SDM
```

تعديل قالب إدارة قاعدة بيانات المحول (SDM) الحالي:

- 9500H(config)#يفضل مدير قاعدة بيانات المحول (SDM) قائمة التحكم في الوصول (ACL) المخصصة
  9500H(config-sdm-acl)#إدخال ACL 26 أولوية 1 <— تطبيق قيمة 26K جديدة. (الأولوية التي تمت مناقشتها في دليل التكوين)
  9500H(config-sdm-acl)#ACL-egress 20 priority 2
  9500H(config-sdm-acl)#خرج
  إستخدام show sdm prefer custom لرؤية القيم المقترحة و sdm prefer custom commit من أجل تطبيق هذه التغييرات عبر واجهة سطر الأوامر "عرض التغييرات".
- تحقق من التغييرات التي أجريت على ملف تعريف إدارة قاعدة بيانات المحول (SDM).
- 9500H#إظهار sdm أفضل مخصص

عرض معلومات قالب إدارة قاعدة بيانات المحول (SDM):

هذا هو القالب المخصص مع تفاصيله.
إدخالات التحكم في الوصول إلى الأمام عند المدخل*: 12288 (حالي) - 26624 (مقترح) <—
الاستخدام الحالي والمقترح (مقترح 26 كيلوبايت)
إدخالات التحكم في الوصول لأمام الخروج*: 15360 (حالي) - 20480 (مقترح)

9500H#يفضل show sdm إدخال المستخدم المخصص

إدخال مستخدم ميزة قائمة التحكم في الوصول (ACL)
قيم إدخال المستخدم
==========

أولوية اسم الميزة مقياس
—
إدخالات التحكم في الوصول إلى الأمام للمدخل: 1 26*1024 <— تم التعديل حسب إدخال المستخدم إلى 26 × 1024 (26 ك)
إدخالات التحكم في الوصول إلى أمام الخروج: 20*1024 <— تم تعديلها حسب إدخال المستخدم إلى 20 × 1024 (20 كيلو)

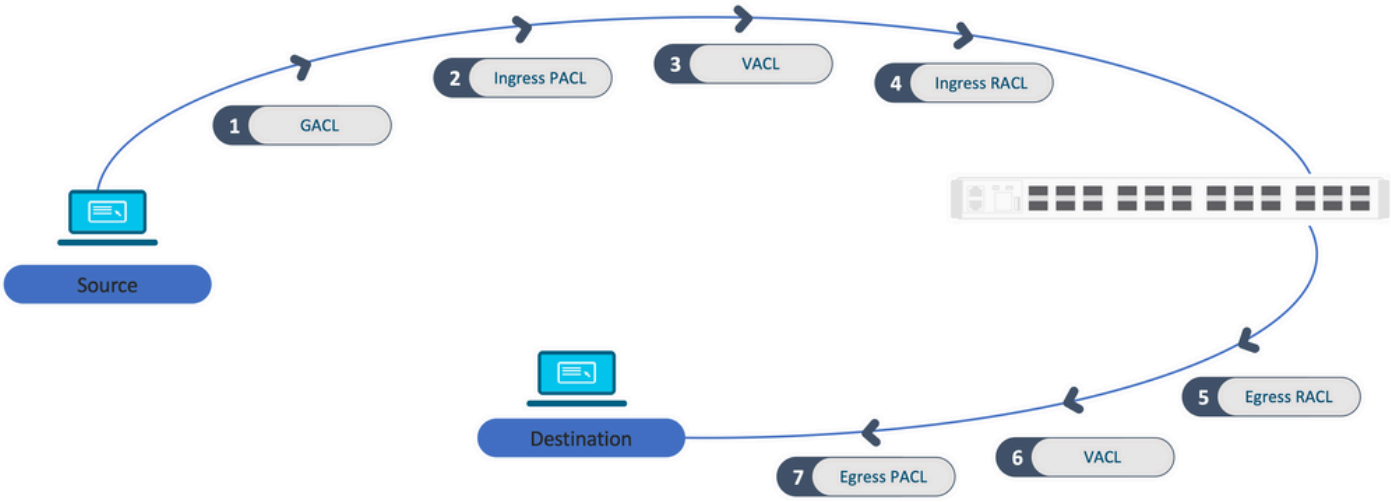
- تطبيق التغييرات على ملف تعريف إدارة قاعدة بيانات المحول (SDM).
- 9500H(config)#إدارة قاعدة بيانات المحول (SDM) تفضل الالتزام المخصص

يتم تخزين التغييرات التي يتم إجراؤها على تفضيلات إدارة قاعدة بيانات المحول (SDM) الجاري تشغيلها وتصبح سارية المفعول على عملية إعادة التحميل التالية.
<— بمجرد إعادة التحميل، تم تخصيص ACL TCAM للقيمة المخصصة.

قراءة اضافية:

أمر معالجة قائمة التحكم في الوصول (ACL):

تتم معالجة قوائم التحكم في الوصول (ACL) بهذا الترتيب من المصدر إلى الوجهة.




قوائم التحكم في الوصول (ACL) المبرمجة في مكدس:

- يتم تطبيق قوائم التحكم في الوصول (ACL) غير المستندة إلى المنفذ (على سبيل المثال، VACL و RACL) على حركة المرور على أي محول وتتم برمجتها على جميع المحولات في المكدس.
- يتم تطبيق قوائم التحكم في الوصول (ACL) المستندة إلى المنفذ فقط على حركة المرور على المنفذ ويتم برمجتها فقط على المحول الذي يملك الواجهة.
- تتم برمجة قوائم التحكم في الوصول (ACL) بواسطة المحول النشط ثم يتم تطبيقها على محولات الأعضاء.
- تنطبق القواعد نفسها على خيارات التكرار الأخرى، مثل ISSU/SVL.

توسيع قائمة التحكم في الوصول (ACL):

- يحدث توسيع قائمة التحكم في الوصول (ACL) عندما ينفذ الجهاز من L4OPs أو Lables أو VCUs. يجب أن يقوم الجهاز بإنشاء وحدات ACE متعددة مكافئة من أجل تحقيق نفس المنطق، ومن أجل إستنزاف TCAM بسرعة.
- #### عمليات النشر (OPs) من L4قيد التطوير وتم إنشاء قائمة التحكم في الوصول (ACL) هذه ##
  9500H(config)#ip access-list extended TEST
  9500H(config-ext-nacl)#السماح ل TCP 10.0.0.0.255.255.255 أي gt 150 <— يطابق المنافذ 151 وأعلى

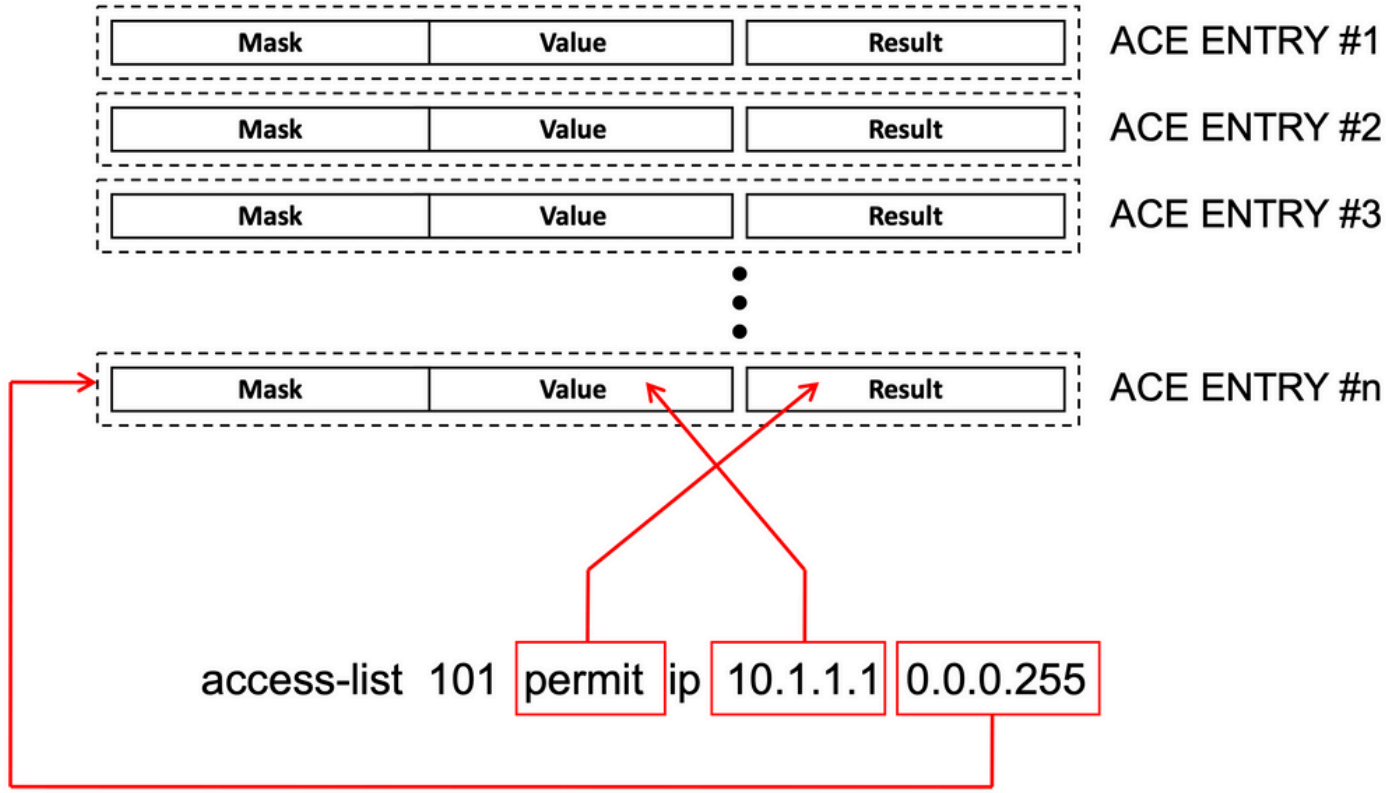
### يجب توسيع هذا المحول إلى وحدات تحكم في الوصول (ACE) متعددة الأطراف ال
### L4OP سلسلة من الوصول إلى قطعة تستخدم
9500H(config-ext-nacl)#allow tcp 10.0.0.255.255.255 أي eq 151
9500H(config-ext-nacl)#allow tcp 10.0.0.255.255.255 أي eq 152
9500H(config-ext-nacl)#allow tcp 10.0.0.255.255.255 أي eq 153
9500H(config-ext-nacl)#allowed tcp 10.0.0.0.255.255.255 أي eq 154
... وهكذا ...

إستهلاك TCAM ومشاركة الملصقات:

- تتم الإشارة إلى كل سياسة قائمة تحكم في الوصول (ACL) داخليا بواسطة تسمية.
- عندما يتم تطبيق سياسة قائمة التحكم في الوصول (قائمة التحكم في الوصول RACL) على واجهات متعددة أو شبكة VLAN، فإنها للأمان مثل GACL أو PACL أو VACL تستخدم نفس التسمية.
- تستخدم قائمة التحكم بالوصول (ACL) إلى المدخل/المخرج مساحات تسمية مختلفة.
- تستخدم قوائم التحكم بالوصول الخاصة ببروتوكول IPv4 و IPv6 و MAC مساحات تسميات أخرى.
- يتم تطبيق قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) نفسها على مدخل الواجهة A ومخرج الواجهة A. هناك إثنان مثال من ال pacl في ال TCAM، كل واحد مع عنوان فريد لمدخل ومخرج.
- إذا تم تطبيق قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) نفسها مع نقطة وصول من السلسلة L4OP على واجهات المدخل المتعددة الموجودة على كل مركز، فسيكون هناك مثالان لنفس قائمة التحكم في الوصول الخاصة بالمنفذ (PACL) تمت برمجتها في TCAM، واحد لكل مركز.

الوصف:

تتم برمجة ACE داخليا في TCAM كـ "VMR" - المعروفة أيضا باسم القيمة، القناع، النتيجة. يمكن لكل إدخال ACE إستهلاك VMRs ويمكنه إستهلاك وحدات VCUs.




قابلية توسع قائمة التحكم في الوصول (ACL):

يتم تخصيص موارد قائمة التحكم في الوصول (ACL) الأمنية لقوائم التحكم في الوصول (ACL) الأمنية. لا تتم مشاركتها مع ميزات أخرى.

| موارد ACL TCAM | Cisco Catalyst 9600 | Cisco Catalyst 9500 | Cisco Catalyst 9400 | Cisco Catalyst 9300 | Cisco Catalyst 9200 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| إدخالات بروتوكول IPv4 | المدخل: 12000* | الخروج: 15000* | الطراز C9500: 18000* | أداء فائق للطراز C9500<br>المدخل: 12000*<br>المخرج: 15000* | 18000* | الطراز C9300:<br>5000 | الطراز C9300B:<br>18000 | الطراز C9300X:8000 | 1000 |
| إدخالات IPv6 | نصف إدخالات IPv4 | | نصف إدخالات IPv4 | | نصف إدخالات IPv4 | نصف إدخالات IPv4 | | | نصف إدخالات IPv4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| الحد الأقصى لعدد إدخالات قوائم التحكم في الوصول إلى IPv4 | 12000 | المسار C9500: 18000 | أداء فائق للمسار C9500: 15000 | 18000 | المسار C9300: 5000 | المسار C9300B: 18000 | المسار C9300X: 8000 | 1000 |
| الحد الأقصى لعدد إدخالات قوائم التحكم في الوصول إلى IPv6 | 6000 | المسار C9500: 9000 | أداء فائق للمسار C9500: 7500 | 9000 | 2500/9000/4000 | | | 500 |
| L4OPs/Label | 8 | 8 | | 8 | 8 | | | 8 |
| نطاق وصول Ingress VCUs | 192 | 192 | | 192 | 192 | | | 192 |
| نطاق وصول Egress | 96 | 96 | | 96 | 96 | | | 96 |

## معلومات ذات صلة

- دليل تكوين الأمان، Cisco IOS XE Amsterdam، الإصدار 17.3.x (محولات Catalyst 9200 Switches)
- دليل تكوين الأمان، Cisco IOS XE Amsterdam، الإصدار 17.3.x (محولات Catalyst 9300 Switches)
- دليل تكوين الأمان، Cisco IOS XE Amsterdam، الإصدار 17.3.x (محولات Catalyst 9400 Switches)
- دليل تكوين الأمان، Cisco IOS XE Amsterdam، الإصدار 17.3.x (محولات Catalyst 9500 Switches)
- دليل تكوين الأمان، Cisco IOS XE Amsterdam، الإصدار 17.3.x (محولات Catalyst 9600 Switches)
- دليل تكوين إدارة النظام، Cisco IOS XE Bengaluru 17.4.x (محولات Catalyst 9500 Switches)
- الدعم التقني والتنزيلات من Cisco

## أوامر التتبع والتصحيح

| num | | ةظحالم |
|---|---|---|
| 1 | show platform hardware fed [switch] active fwd-asic drops exceptions asic <0> | قم بتفريغ عدادات الاستثناء على ASIC #N. |
| 2 | show platform software fed [switch] active acl | يطبع هذا الأمر المعلومات حول جميع قوائم التحكم في الوصول (ACL) التي تم تكوينها على المربع مع معلومات الواجهة والنهج. |
| 3 | show platform software fed [switch] active acl policy 18 | يقوم هذا الأمر بطباعة المعلومات حول النهج 18 فقط. يمكنك الحصول على معرف النهج هذا من الأمر 2. |
| 4 | show platform software fed [switch] active acl interface intftype pacl | يطبع هذا الأمر المعلومات حول قائمة التحكم في الوصول (ACL) استنادا إلى نوع الواجهة (pacl/vacl/racl/gacl/sgacl وما إلى ذلك). |
| 5 | show platform software fed [switch] active acl interface intftype pacl acltype ipv4 | يطبع هذا الأمر المعلومات حول قائمة التحكم في الوصول (ACL) استنادا إلى نوع الواجهة (PACL/VACL/RACL/GACL/SGACL وما إلى ذلك) ويقوم أيضا بتصفية البروتوكول على النحو (IPv4/IPv6/Mac وما إلى ذلك). |
| 6 | show platform software fed [switch] active acl interface intftype pacl acltype ipv4 | يطبع هذا الأمر المعلومات حول الواجهات. |
| 7 | show platform software fed [switch] active acl interface 0x9 | يطبع هذا الأمر المعلومات القصيرة لقائمة التحكم في الوصول (ACL) المطبقة على الواجهة، استنادا إلى أمر IIF-ID (من 6). |
| 8 | show platform software fed [switch] active acl definition | يطبع هذا الأمر المعلومات حول قوائم التحكم في الوصول (ACL) التي تم تكوينها على المربع والتي يتواجد وجودها في CGD. |
| 9 | show platform software fed [switch] active acl iifid 0x9 | يطبع هذا الأمر المعلومات التفصيلية لقائمة التحكم في الوصول (ACL) المطبقة على الواجهة، استنادا إلى معرف IIF. |

| | | |
|---|---|---|
| 10 | show platform software fed [switch] active acl usage | يطبع هذا الأمر عدد VMRs التي تستخدمها قائمة تحكم الوصول (ACL) استنادا إلى نوع الميزة. |
| 11 | show platform software fed [switch] active acl policy intftype pacl vcu | يمنحك هذا الأمر معلومات السياسة ومعلومات وحدة VCU أيضا استنادا إلى نوع الواجهة (pacl/vacl/racl/gacl/sgacl وما إلى ذلك). |
| 12 | show platform software fed [switch] active acl policy intftype pacl cam | يمنحك هذا الأمر معلومات السياسة والتفاصيل حول الواجهة على عنان، CAM في VMRs (pacl/valc/racl/gacl/sgacl وما إلى ذلك). |
| 13 | show platform software interface [switch] [active] R0 brief | يمنحك هذا الأمر تفاصيل حول الواجهة الموجودة على الرعب. |
| 14 | show platform software fed [switch] active port if_id 9 | يطبع هذا أمر التفاصيل حول الميانع بناء على IIF-ID. |
| 15 | show platform software fed [switch] active vlan 30 | يطبع هذا أمر التفاصيل حول VLAN 30. |
| 16 | show platform software fed [switch] active acl cam asic 0 | يوقوم هذا الأمر بطباعة كاميرا قائمة التحكم في الوصول (ACL) الكاملة على ASIC 0 التي تم إستخدامها. |
| 17 | show platform software fed [switch] active acl counters hardware | يوقوم هذا الأمر بطباعة جميع عدادات قائمة التحكم في الوصول من الأجهزة. |
| 18 | show platform hardware fed [switch] active fwd-asic resource tcam table pbr record 0 format 0 | طباعة الإدخالات لقسم PBR، مما يمكنك إعطاء أقسام لثم مختلفة ACL و CPP من الدب PBR. |
| 19 | show platform software fed [switch] active punt cpuq [1\|2\|3 …] | للتحقق من النشاط في إحدى قوائم انتظار وحدة المعالجة المركزية، لديك أيضا خيارات لمسح إحصائيات قائمة الانتظار للتصحيح. |
| 20 | show platform software fed [switch] active ifm mappings gpn | طباعة تخطيط الواجهة باستخدام IIF-ID و GPNs |
| 21 | show platform software fed [switch active ifm if-id | عم يقالتالي، واجهة المعلومات حول تكوين الواجهة التي يكون قم بطباعة من التحقق للأمر هذا في ASIC. |

| | | |
|---|---|---|
| | | عليها ASIC و CORE. |
| 22 | set platform software trace fed [switch] active acl/asic_vmr/asic_vcu/cgacl/sgacl [debug\|error …] | تعيين التتبع لميزة معينة في FED. |
| 23 | request platform software trace rotate all | مسح مخزن التتبع المؤقت. |
| 24 | show platform software trace message fed [switch] active | طباعة مخزن التتبع المؤقت ل FED. |
| 25 | set platform  software trace forwarding-manager [switch] [active] f0 fman [debug\|error …] | تمكين المسارات ل FMAN. |
| 26 | show platform software trace message forwarding-manager [switch] [active] f0 | طباعة مخزن التتبع المؤقت ل FMAN. |
| 27 | debug platform software infrastructure punt detail | قم بتعيين تصحيح الأخطاء على PUNT. |
| 28 | debug ip cef packet all input rate 100 | تصحيح حزم CEF قيد التشغيل. |

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).