Risoluzione dei problemi relativi agli elenchi degli accessi su IE3x00

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi e verificare le voci degli Access Control Lists (ACL) e i limiti hardware su Industrial Ethernet serie 3x00.

Prerequisiti

Requisiti

Cisco consiglia di avere una conoscenza base della configurazione degli ACL.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è IE-3300 con software Cisco IOS® XE versione 16.12.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questo documento può essere utilizzato anche con queste versioni hardware:

1. IE-3200 (fissa)
2. IE-3300 (modulare)
3. IE-3400 (modulare avanzato).

Premesse

Gli elenchi degli accessi (ACL) su uno switch di layer 3 forniscono la sicurezza di base per la rete. Se gli ACL non sono configurati, tutti i pacchetti che attraversano lo switch possono essere autorizzati su tutte le parti della rete. Gli ACL controllano gli host che possono accedere alle diverse parti della rete o decidere i tipi di traffico da inoltrare o bloccare sulle interfacce del router. È possibile configurare gli ACL in modo da bloccare il traffico in entrata, in uscita o entrambi.

Esempio: È possibile consentire l'inoltro del traffico di posta elettronica ma non il traffico Telnet all'esterno della rete.

Supporto e limitazioni di IE3x00:

- Gli elenchi degli accessi VLAN (VACL) non sono supportati sull'interfaccia virtuale dello switch (SVI).
- Quando VACL e Port ACL (PACL) sono entrambi applicabili per un pacchetto, il PACL ha la precedenza sul VACL e il VACL non viene applicato in questo caso.
- Massimo 255 voci di controllo di accesso (ACE) per VACL.
- Non è stato definito alcun limite esplicito sul totale delle VLAN in quanto il TCAM non viene scolpito nei componenti e ogni volta che non è disponibile spazio sufficiente per accettare la nuova configurazione, viene generato un errore con un syslog.
- Logging non è supportato negli ACL in uscita.
- Sugli ACL di layer 3, gli ACL non IP non sono supportati.
- L'operatore di layer 4 (L4OP) negli ACL è limitato dall'hardware a un massimo di 8 L4OP per UDP e 8 L4OP per TCP, per un totale di 16 L4OP globali.
- Tenere presente che l'operatore **range** utilizza 2 L4OP.

  Nota: I PO L4E comprendono: gt (maggiore di), lt (minore di), neq (diverso da), eq (uguale a), range (intervallo inclusivo)

- Gli ACL in ingresso sono supportati solo sulle interfacce fisiche, non su interfacce logiche come VLAN, Port-channel e così via.
- Gli ACL (PACL) delle porte sono supportati e possono essere: Non IP, IPv4 e IPv6.
- Gli ACL non IP e IPv4 dispongono di 1 filtro implicito, mentre gli ACL IPv6 dispongono di 3 filtri impliciti.
- Sono supportati gli ACL con limiti di tempo.
- L'ACL IPv4 con TTL e opzioni IP basate sulla corrispondenza non è supportato.

Risoluzione dei problemi

Passaggio 1. **Identificare** l'ACL con cui si sospettano problemi. A seconda del tipo di ACL, sono disponibili i seguenti comandi:

show access-list { *acl-no* | *acl-name* } **show mac access-group interface** *interface_name* show ipv6 access-list *acl_name* show ip access-list { *acl-no* | *acl-name* } show ipv6 access-list *acl_name*

```
IE3300#show access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
IE3300#show ip access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
```

Lo scopo degli output del comando è quello di identificare la configurazione ACL corrente su Cisco IOS.

Passaggio 2. **Verificare che** lo stesso ACL sia presente nella tabella delle voci hardware.

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Opzioni dei comandi disponibili per controllare la TCAM dello switch.

```
IE3300#show platform hardware acl asic 0 tcam interface GigabitEthernet 1/4 ipv4 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]
```

Nell'output della tabella hardware sono presenti tre coppie di regole dalle quali:

P: Stands for pattern = indica gli indirizzi IP o le subnet della voce ACE.

M: Stands for mask = questi sono i bit jolly della voce ACE.

Voce ACE	Indice	SIP	DIP	Protocollo	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (qualsiasi)	0.0.0.0 (qualsiasi)	0x11	0x00 (massimo sforzo)
permit udp any eq 2222 any	1P, 1M, 1	0.0.0.0 (qualsiasi)	0.0.0.0 (qualsiasi)	0x11	0x00 (massimo sforzo)
deny ip any any (implicit)	2 P, 2 M, 2	0.0.0.0 (qualsiasi)	0.0.0.0 (qualsiasi)	0x00	0x00 (massimo sforzo)

Voce ACE	Src OP	Porta Src 1	Porta Src 2	OP destinazione	Porta Dst1	Porta Dst2
permit udp any any eq 2222	—	—	—	EQ	2222	—
permit udp any eq 2222 any	EQ	2222	—	—	—	—
deny ip any any (implicit)	—	—	—	—	—	—

> **Nota:** Esempi di voci di maschera: parola chiave host = ff.ff.ff.ff, carattere jolly 0.0.0.255 = ff.ff.ff.00, qualsiasi parola chiave = 00.00.00.00

Indice: numero della regola. Nell'esempio sono presenti 0, 1 e 2 indici.

SIP: indica l'indirizzo IP di origine in formato ESADECIMALE. Poiché le regole contengono la parola chiave 'any', l'indirizzo IP di origine è composto da tutti zero.

DIP - Indica l'indirizzo IP di destinazione in formato ESADECIMALE. La parola chiave 'any' nella regola viene convertita in tutti gli zeri.

Protocol: indica il protocollo delle ACE. 0x11 per UDP.

> **Nota:** Elenco dei protocolli noti: 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP - DSCP (Differentiated Services Code Point) presente nella regola. Se non specificato, il valore è 0x00 (massimo sforzo).

Tipo IGMP: per specificare se la voce ACE contiene tipi IGMP.

Tipo ICMP: per specificare se la voce ACE contiene tipi ICMP.

Codice ICMP: per specificare se la voce ACE contiene tipi di codice ICMP.

Contrassegni TCP - Specifica se la voce ACE ha contrassegni TCP.

Src OP - Indica l'origine L4OP utilizzata nella regola. Nessuna voce nella prima voce ACE. Alla seconda voce ACE è associato EQ come operatore.

Src port1: indica la prima porta di origine se la voce ACE è basata su UDP o TCP.

Src port2: indica la seconda porta di origine se la voce ACE è basata su UDP o TCP.

Dst OP - Indica la destinazione L4OP utilizzata nella regola. Per la prima voce ACE l'operatore è EQ, mentre per la seconda voce ACE non è presente alcun operatore.

Porta destinazione1: indica la prima porta di destinazione se la ACE è basata su UDP o TCP.

Porta Dst2: indica la seconda porta di destinazione se la ACE è basata su UDP o TCP.

Le regole sono associate alla porta **ACL:<0,x>** in cui 0 indica ASIC = 0 e X corrisponde a ASIC port number = 1.

Nella tabella è inoltre possibile visualizzare l'azione eseguita per ogni istruzione ACE.

Indice ACE	Azione
0	ASIC_ACL_PERMIT [1]
1	ASIC_ACL_PERMIT [1]
2	ASIC_ACL_DENY[0]

Passaggio 3. **Verificare** le stesse voci ACL con comandi diversi:

Voci ACL in un dato indice

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - Questo comando mostra l'elenco di regole in un ID ACL specifico.

```
IE3300#show platform hardware acl asic 0 tcam index 45 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
```

```
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]
```

Qui index è lo scostamento con cui la regola viene programmata nel TCAM.

Per controllare quale indice ACL viene usato, è necessario identificare la porta a cui è applicato l'ACL e usare il comando show platform hardware acl asic 0 tcam interface *nome_interfaccia* ipv4 detailper ottenere il numero ID dell'ACL.

> **Nota:** Tenere presente che questo comando non visualizza il mapping ASIC/porta. Inoltre, se si applica lo stesso ACL a interfacce diverse, la TCAM crea una voce ACL ID diversa. Ciò significa che non vi è riutilizzo dell'indice per lo stesso ACL applicato a interfacce diverse nello spazio TCAM.

Voci ACL programmate nell'hardware

show platform hardware acl asic 0 tcam all [detail] - Visualizza tutte le informazioni sul TCAM.

```
IE3300#show platform hardware acl asic 0 tcam all
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[0]

ACL_KEY_TYPE_v4 - ACL Id 46

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
```

```
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  EQ.     2222       ---------  0     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------   0xFF     0xFFFF   ---------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x11      0x00  0/00    ---------  ---------  ---------  ------
---
EQ.     2222       ---------  ------  ---------  ---------  0     0
  1M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  ------
---
 0xFF     0xFFFF   ---------  ------  ---------  ---------- 3f   3ff
  1 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  2P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  0     0
  2M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------- 3f   3ff
  2 Action: ASIC_ACL_DENY[0], Match Counter[12244]
```

Questo output visualizza tutti gli ID ACL memorizzati nella tabella hardware. Sono disponibili due ACL ID distinti (45, 46), ma la struttura di ciascun blocco è esattamente la stessa. Ciò indica che entrambi gli ID ACL appartengono allo stesso ACL configurato nel software:

```
IE3300#show ip access-list 103
Extended IP access list 103
    10 permit udp any any eq 2222
    20 permit udp any eq 2222 any
```

Applicato a interfacce diverse.

```
IE3300#show run interface GigabitEthernet 1/4
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet1/4
 ip access-group 103 in
end

IE3300#show run interface GigabitEthernet 1/5
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet1/5
 ip access-group 103 in
end
```

Utilizzo TCAM

show platform hardware acl asic 0 tcam usage - Questo comando visualizza l'uso degli ACL nell'ASIC. IE3x00 dispone di un solo ASIC (0)

```
IE3300#show platform hardware acl asic 0 tcam usage
        TCAM Usage For ASIC Num : 0

                Static ACEs      : 18   (0   %)
                Extended ACEs    : 0    (0   %)
                ULTRA ACEs        : 0    (0   %)
                STANDARD ACEs    : 6    (0   %)
                Free  Entries     : 3048 (100 %)
                Total Entries   : 3072
```

La voce ACE standard ha una larghezza di 24 byte. ACE esteso è largo 48 byte; Ultra ACE ha una larghezza di 72 byte.

Voci statiche ACL

show platform hardware acl asic 0 tcam static [detail]- Visualizza le configurazioni ACL statiche (specifiche del protocollo di controllo).

```
IE3300-Petra#show platform hardware acl asic 0 tcam static detail
Switch MAC Global Entry:
MAC DA: 01:00:0c:00:00:00/ff:ff:ff:00:00:00
  4 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[6908]
Dot1x EAP Global Entry:
Ethertype: 0x888e/0xffff
  1 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[2], Match Counter[0]
CISP Global Entry:
Ethertype: 0x0130/0xffff
  0 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[2], Match Counter[0]
REP Beacon Global Entry:
Ethertype: 0x0131/0xffff
  2 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[0]
REP Preferred Global Entry:
MAC DA: 00:00:00:00:00:00/00:00:00:00:00:00
 14 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
REP Preferred Global Entry:
Ethertype: 0x0000/0x0000
 16 Action: ASIC_ACL_DENY_AND_LOG[2], CPU queue[1], Match Counter[25702]
REP Preferred Global Entry:
Ethertype: 0x0129/0xffff
 15 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
DHCP related entries:
None.
MLD related entries:
None.
```

Questo output di comando visualizza le voci ACL programmate dal sistema per i diversi protocolli di controllo dello switch.

Statistiche ACL

show platform hardware acl asic 0 tcam statistics *interface_name* - Visualizza le statistiche ACL in tempo reale. Il contatore non è cumulativo. Dopo aver visualizzato il comando per la prima volta, i contatori vengono ripristinati se il traffico che raggiunge l'ACL si arresta.

```
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 2
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 1
IE3300#show platform hardware acl asic 0 tcam statistics GigabitEthernet 1/4
         TCAM STATISTICS OF ASIC NUM  :0
         Number Of IPv4 Permits   : 0
         Number Of IPv4 Drops     : 0
```

Questo comando indica quanti accessi riusciti ai permessi si sono verificati per l'ACL sull'interfaccia specificata e quante cadute sono state effettuate mentre il traffico è attivamente accodato sulla porta. I contatori vengono reimpostati dopo la prima visualizzazione del comando.

> **Suggerimento**: Poiché i contatori vengono reimpostati dopo ogni esecuzione del comando, è consigliabile eseguire il comando più volte e tenere traccia degli output precedenti per un contatore cumulativo di autorizzazione/rilascio.

Mapping porta-ASIC

show platform pm port-map - Visualizza la mappatura ASIC/porta per tutte le interfacce dello switch.

```
IE3300#show platform pm port-map

interface gid  gpn  asic slot unit gpn-idb
-----------------------------------------
Gi1/1     1    1    0/24 1    1    Yes
Gi1/2     2    2    0/26 1    2    Yes
Gi1/3     3    3    0/0  1    3    Yes
Gi1/4     4    4    0/1  1    4    Yes
Gi1/5     5    5    0/2  1    5    Yes
Gi1/6     6    6    0/3  1    6    Yes
Gi1/7     7    7    0/4  1    7    Yes
Gi1/8     8    8    0/5  1    8    Yes
Gi1/9     9    9    0/6  1    9    Yes
Gi1/10    10   10   0/7  1    10   Yes
```

0/**x** under asic column indicates = asic/**asic_port_number**

Comandi debug

debug platform acl all - Questo comando abilita tutti gli eventi di gestione ACL.

```
IE3300#debug platform acl all
ACL Manager debugging is on
ACL MAC debugging is on
ACL IPV4 debugging is on
ACL Interface debugging is on
ACL ODM debugging is on
ACL HAL debugging is on
ACL IPV6 debugging is on
ACL ERR debugging is on
ACL VMR debugging is on
ACL Limits debugging is on
ACL VLAN debugging is on
```

debug platform acl hal - Visualizza gli eventi correlati a Hardware Abstraction Layer (HAL).

Per un evento di rimozione/applicazione di ACL su un'interfaccia, viene visualizzato se la regola è stata programmata nell'hardware e le informazioni vengono stampate nella console.

```
[IMSP-ACL-HAL] : Direction 0
[IMSP-ACL-HAL] : TCAM: region_type = 1, lookup_stage = 0, key_type = 1, packet_type = 1,
acl_type = 1, pcl_id = 0, priority = 1
[IMSP-ACL-HAL] : asic_acl_add_port_access_list programmed rule for asic_num=0, region_type=1,
acl_type=1,
port_num=1, lookup stage=0 packet_type=1, key_type=1, pcl_id=0, priority=32, num_aces=3,
acl_handle=0x7F8EA6DC58, acl_dir=0, cpu_log_queue=7 with acl_err=0
[IMSP-ACL-HAL] : Dump acl, acl_handle:0x0x7F8EA6DC58
```

Direzione 0 = In entrata (ACL applicato in entrata)

Direzione 1 = In uscita (ACL applicato in uscita)

debug platform acl ipv4 - Visualizza gli eventi correlati all'IPv4 degli ACL.

debug platform acl ipv6- Visualizza gli eventi correlati all'ACL IPv6.

debug platform acl mac - Visualizza gli eventi correlati agli ACL MAC.

debug platform acl error - Visualizza gli eventi correlati agli errori ACL.

```
[IMSP-ACL-ERROR] : asic_acl_delete_access_list successfully deleted rule for asic_num=0,
region_type=1 acl_handle=0x7F8EA6DC58, acl_dir=0 atomic_update=0 with acl_err=0
```

debug platform acl odm - Visualizza gli eventi correlati a ODM (Order Dependant Merge) ACL.

```
[IMSP-ACL-ODM] : ODM: Num. ACEs before collapse - 2
[IMSP-ACL-ODM] : ODM: Num. ACEs after collapse - 2
[IMSP-ACL-ODM] : Number of Aces after ODM Pre Optimization- 2
[IMSP-ACL-ODM] : ODM: ACEs post collapse = 2
[IMSP-ACL-ODM] : Number of Aces after Final ODM Merge- 2
[IMSP-ACL-ODM] : ODM: Num. ACEs before collapse - 2
[IMSP-ACL-ODM] : ODM: Num. ACEs after collapse - 2
<snip>
```

debug platform acl port-acl - Visualizza gli eventi correlati agli ACL delle porte.

```
[IMSP-ACL-PORT] : PACL attach common
[IMSP-ACL-PORT] : Dumping List of ACL-Handle pairs...
```

```
[IMSP-ACL-PORT] : ACL:103, Handle: 0x7F8EA6DC64, Asic Num: 0,Use Count: 1, Is overloaded: 0
[IMSP-ACL-PORT] : ACL:103, Handle: 0x7F8EA6DC58, Asic Num: 0,Use Count: 1, Is overloaded: 0
[IMSP-ACL-PORT] : ACL Detached from the port
[IMSP-ACL-PORT] : Acl-port handle info, Idb Entry Found
[IMSP-ACL-PORT] : ACL handle=0x7F8EA6DC58 found for port=Gi1/4
[IMSP-ACL-PORT] : Calling HAL asic_acl_remove_port
[IMSP-ACL-PORT] : asic_acl_remove_port successful for asic_num=0, acl_handle=0x7F8EA6DC58,
port_num=1
[IMSP-ACL-PORT] : acl_type: 1, handle: 0x0, dir: 0, acl_name: 0x0, idb: 0x7F4D0AF288
[IMSP-ACL-PORT] : List of HW Programmed Port-ACLs...
[IMSP-ACL-PORT] : Port: Gi1/3
[IMSP-ACL-PORT] : Ingress IPV4: handle = 0x7F8EA6DC64, acl_name = 103, is_acl_overloaded = 0,
auth_proxy_vmr = 0x0, overload_vmr_entries = 0
[IMSP-ACL-PORT] : Port: Gi1/4
[IMSP-ACL-PORT] : Ingress IPV4: handle = 0x7F8EA6DC58, acl_name = 103, is_acl_overloaded = 0,
auth_proxy_vmr = 0x0, overload_vmr_entries = 0
[IMSP-ACL-PORT] : rc = 1
[IMSP-ACL-PORT] : No more acl on this port!!
[IMSP-ACL-PORT] : Free stored_acl_name=0x0
[IMSP-ACL-PORT] : Update_Pacl_info, Updated entries for idb=0x0
<snip>
```

debug platform acl vmr - Visualizza gli eventi correlati al risultato della maschera di valore ACL (VMR). Se si verificano problemi con VMR, è possibile visualizzarli qui.

```
[IMSP-ACL-VMR] : DstIP Mask=00.00.00.00
[IMSP-ACL-VMR] : Protocol Value/Mask=0011/FFFF
[IMSP-ACL-VMR] : Fragment field set to FALSE
[IMSP-ACL-VMR] : SrcPort1 Value/Mask=D908/FFFF
[IMSP-ACL-VMR] : SrcPort2 Value/Mask=D90F/FFFF
[IMSP-ACL-VMR] : SrcL4Op Value is Range
[IMSP-ACL-VMR] : SrcL4Op Mask is FFFFFFFF
[IMSP-ACL-VMR] : Action is PERMIT
[IMSP-ACL-VMR] : ACE number => 30
[IMSP-ACL-VMR] : vmr_ptr 0x7F51D973B0
[IMSP-ACL-VMR] : vmr_ptr->entry 0x7F51D973B0
<snip>
```

Problemi comuni

Esaurimento L4OP

L'esaurimento del comparatore L4OPs può essere identificato dopo aver abilitato i seguenti debug:

debug platform port-asic hal acl errors debug platform port-asic hal tcam errors

> **Nota:** I comandi di debug non visualizzano informazioni nel buffer di registro dello switch. Le informazioni vengono invece visualizzate nella show platform software trace message ios R0

Eseguire il comando **show platform software trace message ios R0** per visualizzare le informazioni sui debug.

show platform software trace message ios R0:

```
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (ERR): *Aug 17 21:04:47.244:
%IMSP_ACLMGR-3-INVALIDACL: Add access-list failed
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): Unable to add access-list
[IMSP-ACL-ERROR]:imsp_acl_program_tcam,2026:
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
asic_acl_add_port_access_list failed for asic_num=0, region_type=1, acl_type=1,
port_num=1, lookup stage=0, packet_type=1, key_type=1, pcl_id=0, priority=32, num_aces=99
acl_handle=0x0, acl_dir=0, cpu_log_queue=7 with acl_err=2
[IMSP-ACL-ERROR]:imsp_acl_add_port_access_list,211:
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
ACL ERR:[pc3_add_port_access_list:5471] - not enough available port comparators,asic_num[0],
acl_type[1], num_aces[99]
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [IOSRP] [6472]: (note):

ACL ERR:[prv_check_for_available_port_comparators:5282] - Not enough TCP port comparators
available: Required[20] > Available[8]
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [IOSRP] [6472]: (note):

2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): TCAM: region_type = 1,
lookup_stage = 0, key_type = 1,
packet_type = 1, acl_type = 1, pcl_id = 0, priority = 1
[IMSP-ACL-HAL] :
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note):
2022/08/17 21:04:47.244 {IOSRP_R0-0}{1}: [iosrp] [8748]: (note): Direction 0
[IMSP-ACL-HAL] :
```

Per il modello IE3x00, è previsto un limite di 8 L4OP per UDP e di 8 L4OP per TCP, per un totale massimo di 16 L4OP in tutti gli ACL implementati nello switch. (La restrizione è globale, non per ACL).

> **Nota:** Al momento non è disponibile alcun comando per controllare la quantità di comparatori usati/liberi nella CLI.

Se si verifica questo problema:

- Verificare con i comandi di debug se gli errori sono correlati alla limitazione L4OP.
- Ènecessario ridurre il numero di L4OP in uso nell'ACL. Ogni comando range utilizza 2 comparatori di porte.
- Se si possono usare le voci ACE con il comando **range**, è possibile convertirle in modo da usare la parola chiave **eq**, in modo che non utilizzi l'L4OP disponibile per UDP e TCP, ossia:

Riga:
permit tcp any any range 55560 55567

Può trasformarsi in:
permit tcp any any eq 55560 permit tcp any any eq 55561 permit tcp any any eq 55562 permit tcp any any eq 55563 permit tcp any any eq 55564 permit tcp any any eq 55565 permit tcp any any eq 55566 permit tcp any any eq 55567

Fare riferimento all'ID bug Cisco CSCv07745. Solo gli utenti Cisco registrati possono accedere alle informazioni interne sul bug.

Gli ACL di layer 4 non vengono riepilogati in TCAM

Quando si immettono ACL L4 con indirizzi IP e/o numeri di porta consecutivi, questi vengono riepilogati automaticamente dal sistema prima di essere scritti in TCAM per preservare spazio. Il sistema fa del suo meglio basandosi sulle voci ACL da riepilogare con il MVR appropriato per

coprire una serie di voci dove può. È possibile verificare questa condizione quando si controlla il TCAM e il numero di righe programmate per l'ACL. Cioè:

```
IE3300#show ip access-list TEST
Extended IP access list TEST
    10 permit tcp any any eq 8
    20 permit tcp any any eq 9
    30 permit tcp any any eq 10
    40 permit tcp any any eq 11
```

```
IE3300#show platform hardware acl asic 0 tcam interface GigabitEthernet 1/4 ipv4 detail
ACL_KEY_TYPE_v4 - ACL Id 45

Ingress ACL_KEY_TYPE_v4 -
Index  SIP          DIP          Protocol  DSCP  Frag/Tiny  IGMP type  ICMP type  ICMP code  TCP
flags
Src OP  Src port1  Src port2  Dst OP  Dst port1  Dst port2  Src Port   PCLId
=====  ===========  ===========  ========  ====  ==========  =========  =========  =========
=========
======  =========  =========  ======  =========  =========  ========   ====
  0P   00.00.00.00  00.00.00.00  0x06      0x00  0/00    ---------  ---------  ---------  0x00
------  ---------  ---------  EQ.     8          ---------  1     0
  0M   00.00.00.00  00.00.00.00  0xff      0x00  0/00    ---------  ---------  ---------  0x00
------  ---------  ---------   0xFF     0xFFFF   --------- 3f   3ff
  0 Action: ASIC_ACL_PERMIT[1], Match Counter[0]
  1P   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  ---------  1     0
  1M   00.00.00.00  00.00.00.00  0x00      0x00  0/00    ---------  ---------  ---------  ------
---
------  ---------  ---------  ------  ---------  --------- 3f   3ff
  1 Action: ASIC_ACL_DENY[0], Match Counter[0]

<asic,port> pair bind to this ACL:< 0, 1>
```

Il problema è che il valore della maschera non viene letto correttamente, quindi l'unica voce che viene effettivamente programmata (con l'ACL nell'esempio) è **permit tcp any any eq 8,**poiché questo è l'ACL di riepilogo di primo livello. Le voci per i numeri di porta 9-11 non vengono visualizzate perché la maschera 0.0.0.3 non viene letta correttamente.

Fare riferimento all'ID bug Cisco CSCvx6354. Solo gli utenti Cisco registrati possono accedere alle informazioni interne sul bug.

Comandi da raccogliere per TAC

I problemi più comuni relativi agli elenchi degli accessi su IE3x00 sono illustrati in questa guida, con le procedure di risoluzione appropriate. Tuttavia, se la presente guida non risolve il problema, raccogliere l'elenco di comandi visualizzato e allegarlo alla richiesta di servizio TAC.

Show tech-support acl

```
IE3300#show tech-support acl | redir flash:tech-acl.txt
IE3300#dir flash: | i .txt
89249  -rw-           56287  Aug 18 2022 00:50:32 +00:00  tech-acl.txt
```

Copiare il file dallo switch e caricarlo nella richiesta TAC.

L'output ACL del supporto tecnico è necessario come punto di partenza quando si risolvono i problemi relativi agli ACL nelle piattaforme IE3x00.

Informazioni correlate

- Note di rilascio per gli switch Cisco Catalyst serie IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty e ESS3300, Cisco IOS XE Gibraltar 16.12.x
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).