Dépannage des listes d'accès sur IE3x00

Contenu

Introduction

Ce document décrit comment dépanner et vérifier les entrées des listes de contrôle d'accès (ACL) et les limites matérielles sur la gamme Industrial Ethernet 3x00.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez des connaissances de base sur la configuration des listes de contrôle d’accès.

Components Used

Les informations de ce document sont basées sur IE-3300 avec la version 16.12.4 du logiciel Cisco IOS® XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec les versions matérielles suivantes :

1. IE-3200 (fixe)
2. IE-3300 (modulaire)
3. IE-3400 (modulaire avancé).

Informations générales

Les listes de contrôle d'accès (ACL) d'un commutateur de couche 3 assurent la sécurité de base de votre réseau. Si les listes de contrôle d'accès ne sont pas configurées, tous les paquets qui traversent le commutateur peuvent être autorisés sur toutes les parties du réseau. Les listes de contrôle d'accès contrôlent quels hôtes peuvent accéder à différentes parties d'un réseau ou décident quels types de trafic sont transférés ou bloqués au niveau des interfaces de routeur. Les listes de contrôle d'accès peuvent être configurées pour bloquer le trafic entrant, sortant ou les deux.

Exemple : Vous pouvez autoriser le transfert du trafic de messagerie mais pas le trafic Telnet en dehors du réseau.

Prise en charge et restrictions IE3x00 :

- Les listes d'accès VLAN (VACL) ne sont pas prises en charge sur l'interface virtuelle de commutateur (SVI).
- Lorsque VACL et PACL (Port ACL) sont toutes deux applicables à un paquet, alors PACL a priorité sur VACL et VACL n'est pas appliqué dans un tel cas.
- 255 entrées de contrôle d'accès (ACE) maximum par VACL.
- Aucune limite explicite n'est définie sur le nombre total de VLAN, car TCAM n'est pas découpé en composants, chaque fois qu'un espace suffisant dans TCAM n'est pas disponible pour accepter la nouvelle configuration, une erreur est générée avec un syslog.
- Logging n'est pas pris en charge sur les ACL de sortie.
- Sur la couche 3, les listes de contrôle d'accès non IP ne sont pas prises en charge.
- L4OP (Layer 4 Operator) dans les listes de contrôle d'accès est limité par le matériel à un maximum de 8 L4OP pour UDP et 8 L4OP pour TCP, pour un total de 16 L4OP globales.
- Gardez à l'esprit que l'opérateur **range** consomme 2 L4OP.

  Note: Les L4OP comprennent : gt (supérieur à), lt (inférieur à), neq (différent de), eq (égal), range (plage inclusive)

- Les listes de contrôle d'accès d'entrée sont prises en charge uniquement sur les interfaces physiques, mais pas sur les interfaces logiques telles que VLAN, Port-channel, etc.
- Les listes de contrôle d'accès de port (PACL) sont prises en charge et peuvent être : Non IP, IPv4 et IPv6.
- Les listes de contrôle d'accès non IP et IPv4 ont 1 filtre implicite, tandis que les listes de contrôle d'accès IPv6 en ont 3.
- Les ACL basées sur la plage temporelle sont prises en charge.
- ACL IPv4 avec TTL, correspondance basée sur les options IP non prise en charge.

Dépannage

Étape 1 : identification de la liste de contrôle d'accès suspectée Selon le type de liste de contrôle d'accès, les commandes suivantes sont disponibles :

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
```

L'objectif des résultats de la commande est d'identifier la configuration ACL actuelle sur Cisco IOS.

Étape 2 : vérification de la présence de la même liste de contrôle d'accès dans la table d'entrée matérielle

show platform hardware acl asic 0 tcam { **all** | **index** | **interface** | **static** | **statistics** | **usage** | **vlan-statistics** } - Options de commande disponibles pour vérifier la TCAM du commutateur.

```
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]
```

La sortie de la table matérielle contient trois paires de règles à partir desquelles :

P : Signifie pattern = il s'agit des IP ou des sous-réseaux dans l'ACE.

M : Signifie masque = ce sont les bits génériques dans l'ACE.

Entrée ACE	Indice	SIP	TREMPER	Protocol	DSCP
permit udp any any eq 2222	0P, 0M, 0	0.0.0.0 (tout)	0.0.0.0 (tout)	0x11	0x00 (au mieux)
permit udp any eq 2222 any	1P, 1M, 1	0.0.0.0 (tout)	0.0.0.0 (tout)	0x11	0x00 (au mieux)
deny ip any any (implicit)	2P, 2M, 2	0.0.0.0 (tout)	0.0.0.0 (tout)	0x00	0x00 (au mieux)

Entrée ACE	OP Src	Port1 Src	Src port2	OP POST	Dst port1	Dst port2
permit udp any any eq 2222	------	---------	---------	EQ.	2222	---------
permit udp any eq 2222 any	QE	2222	---------	---------	---------	---------
deny ip any any (implicit)	------	---------	---------	---------	---------	---------

> **Note**: Exemples d'entrées de masque : mot-clé host = ff.ff.ff.ff, masque générique 0.0.0.255 = ff.ff.ff.00, mot-clé any = 00.00.00.00

Index - Numéro de la règle. Nous avons 0, 1 et 2 index dans l'exemple.

SIP : indique l'adresse IP source au format HEX. Puisque les règles ont le mot clé « any », l'IP source est composée uniquement de zéros.

DIP : indique l'adresse IP de destination au format HEX. Le mot clé « any » de la règle se traduit par des zéros.

Protocol : indique le protocole des ACE. 0x11 correspond à UDP.

> **Note**: Liste des protocoles connus : 0x01 - ICMP, 0x06 - TCP, 0x11 - UDP, 0x29 - IPv6.

DSCP : DSCP (Differentiated Services Code Point) présent dans la règle. La valeur non spécifiée est 0x00 (au mieux).

IGMP Type : indique si l'ACE contient des types IGMP.

ICMP Type : indique si l'ACE contient des types ICMP.

Code ICMP - Spécifie si l'ACE contient des types de code ICMP.

Indicateurs TCP : indique si l'ACE possède des indicateurs TCP.

OP Src : indique la L4OP source utilisée dans la règle. Il n'y en a pas dans la première entrée ACE. La deuxième entrée ACE a EQ comme opérateur.

Src port1 : indique le premier port source si l'ACE est basé sur UDP ou TCP.

Src port2 : indique le deuxième port source si l'ACE est basé sur UDP ou TCP.

Dst OP : indique la destination L4OP utilisée dans la règle. La première entrée ACE a EQ comme opérateur, il n'y en a pas dans la seconde entrée ACE.

Dst port1 : indique le premier port de destination si l'ACE est basé sur UDP ou TCP.

Dst port2 : indique le deuxième port de destination si l'ACE est basé sur UDP ou TCP.

Les règles sont liées au port **ACL:<0,x>** où 0 signifie ASIC = 0 et X correspond au numéro de port ASIC = 1.

Vous pouvez également voir l'action entreprise par instruction ACE dans le tableau.

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

Étape 3. **Vérifiez** les mêmes entrées de liste de contrôle d'accès avec les commandes suivantes :

Entrées ACL à un index donné

show platform hardware acl asic 0 tcam index *acl_id* **[detail]** - Cette commande affiche la liste des règles sous un ID ACL spécifique.

```
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]
```

Ici index est le décalage auquel la règle est programmée dans la TCAM.

Pour vérifier quel index de liste de contrôle d'accès est utilisé, vous devez identifier le port où la liste de contrôle d'accès est appliquée et utiliser la commande show platform hardware acl asic 0 tcam interface *nom_interface* ipv4 detailpour obtenir l'ID de la liste de contrôle d'accès.

> **Note**: Gardez à l'esprit que cette commande n'affiche pas le mappage ASIC/Port. En outre, si vous appliquez la même liste de contrôle d'accès à différentes interfaces, la TCAM crée une entrée d'ID de liste de contrôle d'accès différente. Cela signifie qu'il n'y a pas de réutilisation d'index pour la même ACL appliquée à différentes interfaces dans l'espace TCAM.

Entrées ACL programmées dans le matériel

show platform hardware acl asic 0 tcam all [detail] - Affiche toutes les informations sur la 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]
```

Cette sortie affiche tous les ID ACL stockés dans la table matérielle. Il existe deux ID de liste de contrôle d'accès distincts (45, 46), mais la structure de chaque bloc est exactement la même. Cela indique que les deux ID ACL appartiennent à la même ACL configurée dans le logiciel :

```
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
```

qui est appliqué à différentes interfaces.

```
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
```

Utilisation de TCAM

show platform hardware acl asic 0 tcam usage - Cette commande affiche l'utilisation des ACL dans l'ASIC. IE3x00 n'a qu'un 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
```

L'ACE standard a une largeur de 24 octets ; L'ACE étendue fait 48 octets ; Ultra ACE a une largeur de 72 octets.

Entrées statiques ACL

show platform hardware acl asic 0 tcam static [detail]- Affiche les configurations des listes de contrôle d'accès statiques (spécifiques au protocole de contrôle).

```
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.
```

Cette sortie de commande affiche les entrées ACL programmées par le système pour différents protocoles de contrôle du commutateur.

Statistiques ACL

show platform hardware acl asic 0 tcam statistics *interface_name* - Affiche les statistiques ACL en temps réel, le compteur n'est pas cumulatif. Après avoir affiché la commande la première fois, les compteurs sont réinitialisés si le trafic qui atteint la liste de contrôle d'accès s'arrête.

```
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
```

Cette commande vous indique le nombre d'occurrences dans les autorisations pour la liste de contrôle d'accès sur l'interface spécifiée, et le nombre d'abandons qui ont été également atteints alors que le trafic est activement mis en file d'attente dans le port. Les compteurs sont réinitialisés une fois la commande affichée pour la première fois.

> **Astuce** : Étant donné que les compteurs sont réinitialisés après chaque exécution de la commande, il est recommandé d'exécuter la commande plusieurs fois et de conserver un enregistrement des résultats précédents pour un compteur d'autorisation/abandon cumulatif.

Mappage de port à ASIC

show platform pm port-map - Affiche le mappage ASIC/Port pour toutes les interfaces du commutateur.

```
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**

Commandes de débogage

debug platform acl all - Cette commande active tous les événements du gestionnaire 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 - Affiche les événements liés à la couche d'abstraction matérielle (HAL).

Pour un événement de suppression/application de liste de contrôle d'accès sur une interface, il indique si la règle a été programmée dans le matériel et affiche les informations dans la 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
```

Direction 0 = entrante (ACL appliquée en entrée)

Direction 1 = Sortante (ACL appliquée en sortie)

debug platform acl ipv4 - Affiche les événements associés à ACL IPv4.

debug platform acl ipv6- Affiche les événements associés à ACL IPv6.

debug platform acl mac - Affiche les événements MAC ACL.

debug platform acl error - Affiche les événements liés aux erreurs 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 - Affiche les événements associés à la fusion dépendante de l'ordre (ODM) 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 - Affiche les événements liés aux ACL de port.

```
[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 - Affiche les événements associés au masque de valeur ACL (VMR). Si vous rencontrez des problèmes avec VMR, vous pouvez les voir ici.

```
[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>
```

Problèmes courants

Épuisement L4OP

L'épuisement du comparateur L4OPs peut être identifié après avoir activé ces débogages :

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

> **Note**: Les commandes debug n'affichent pas d'informations dans la mémoire tampon du journal du commutateur. Au lieu de cela, les informations sont affichées dans la show platform software trace message ios R0erasecat4000_flash:.

Exécutez la commande **show platform software trace message ios R0** pour afficher les informations sur les débogages.

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] :
```

Pour IE3x00, il y a une limite de 8 L4OP pour UDP et 8 L4OP pour TCP, pour un total maximal de 16 L4OP dans toutes les listes de contrôle d'accès implémentées dans le commutateur. (La restriction est globale, pas par ACL).

> **Note**: Actuellement, aucune commande n'est disponible pour vérifier la quantité de comparateurs consommés/libres dans la CLI.

Si vous rencontrez ce problème :

- Vérifiez avec les commandes debug si les erreurs sont liées à la limitation L4OP.
- Vous devez réduire le nombre de L4OP utilisés dans la liste de contrôle d'accès. Chaque commande range utilise 2 comparateurs de ports.
- Si vous pouvez utiliser des ACE avec la commande **range**, ceux-ci peuvent être convertis pour utiliser le mot clé **eq** à la place, de sorte qu'il ne consommera pas le L4OP disponible pour UDP et TCP, c'est-à-dire :

Ligne :
permit tcp any any range 55560 55567

Peut se transformer en :
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

Référez-vous à l'ID de bogue Cisco CSCv0745. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue internes.

Les ACL de couche 4 ne sont pas récapitulées dans TCAM

Lorsque des listes de contrôle d'accès de couche 4 avec des adresses IP et/ou des numéros de port consécutifs sont entrées, elles sont automatiquement récapitulées par le système avant d'être

écrites dans TCAM pour économiser de l'espace. Le système fait de son mieux en se basant sur les entrées de la liste de contrôle d'accès pour résumer avec le MVR approprié afin de couvrir une plage d'entrées où il peut. Cela peut être vérifié lorsque vous vérifiez la TCAM et le nombre de lignes programmées pour la liste de contrôle d'accès. C'est-à-dire :

```
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>
```

Le problème est que la valeur du masque n'est pas lue correctement, donc la seule entrée qui est réellement programmée (avec la liste de contrôle d'accès dans l'exemple) est **permit tcp any any eq 8**,car il s'agit de la liste de contrôle d'accès de résumé de niveau supérieur. Les entrées pour les numéros de port 9-11 ne sont pas visibles car le masque de 0.0.0.3 n'est pas lu correctement.

Référez-vous à l'ID de bogue Cisco CSCvx6354 . Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue internes.

Commandes à collecter pour le TAC

Les problèmes les plus courants liés aux listes d'accès sur IE3x00 sont traités dans ce guide, avec les étapes de correction appropriées. Toutefois, si ce guide ne résout pas votre problème, collectez la liste de commandes affichée et joignez-la à votre demande de service 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
```

Copiez le fichier hors du commutateur et téléchargez-le dans le dossier du centre d'assistance technique.

Le résultat de la liste de contrôle d'accès de support technique est requis comme point de départ lorsque vous dépannez des problèmes liés à la liste de contrôle d'accès dans les plates-formes IE3x00.

Informations connexes

- Notes de version des commutateurs Cisco Catalyst IE3x00 Rugged, IE3400 Rugged, IE3400 Heavy Duty et ESS3300, Cisco IOS XE Gibraltar 16.12.x
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.