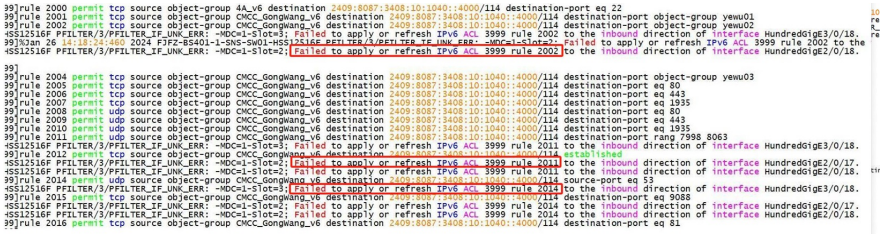
acl出方向调用对象组不生效

ACL　叶红兵　2024-02-23 发表

问题描述

配置基于对象组的acl后会产生告警：

rule 2000 permit tcp source object-group 4A_v6 destination 2409:8087:3408:10:1040::4000/114 destination-port eq 22



过程分析

正常这样配置可以配进去：

```
acl ipv6 advanced 3999
 rule 2001 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port object-group yewu01
 rule 2002 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port object-group yewu02
 rule 2003 permit udp destination 2409:8087:3408:10:1040::4000/114 destination-port object-group yewu02
 rule 2004 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port object-group yewu03
 rule 2005 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port eq www
 rule 2006 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 443
 rule 2007 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 1935
 rule 2008 permit udp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 80
 rule 2009 permit udp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 443
 rule 2010 permit udp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 1935
 rule 2011 permit udp destination 2409:8087:3408:10:1040::4000/114 destination-port range 7998 8063
 rule 2012 permit tcp destination 2409:8087:3408:10:1040::4000/114 established
 rule 2014 permit udp destination 2409:8087:3408:10:1040::4000/114 source-port eq dns
 rule 2015 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 9088
 rule 2016 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port eq 81
```

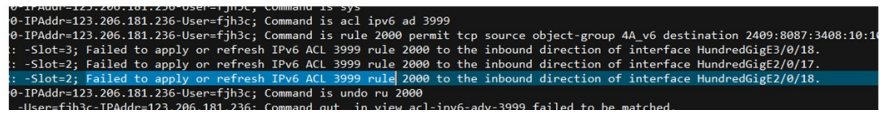
对象组信息

```
Ipv6 address object group 4A_v6: 6 objects(out of use)
 0 network host address 2409:8089:1020:5010:6004::1115
 5 network host address 2409:8089:1020:5010:6004::1116
 10 network host address 2409:8089:1020:5010:6004::1117
 15 network host address 2409:8089:1020:5010:6004::1118
 20 network host address 2409:8089:1020:6010:3001::10
 25 network host address 2409:8089:1020:6010:3001::11
```

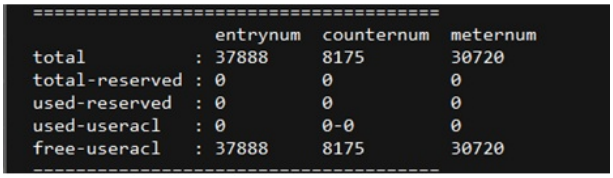
若单独配置，也可以配置进去

官网手册未发现有相关配置限制。官网链接： **https://www.h3c.com/cn/d_202308/1905616_30005_0.htm**

日志里报错后也没有写acl不支持



资源足够



解决方法

在acl 3999 ru2000 的CMCC对象组里面是空的，可以成功调用，但是在对象组里加地址后也会报错，怀疑是因为ipv6的地址问题。

采集下这个命令，**probe**视图下**bcm slot 2 chip 2 diag/field/res**

是Acl超位宽了，最大支持320bit的匹配项，当前超过了320下发失败

Chassis00 slot02 2024/01/26 13:28:27:879979 [LINE:2911-TASK:aclmgrd-FUNC:_bcm_dpp_field_group_verify_qset]:specified qset is too wide 324 for unit 2 stage 0, max 320

超过64位的地址要占128bit，低于64位的地址只占64bit，再上端口、端口号段、TCP关键字等超过了320bit的位宽

rule 2000 permit tcp source object-group 4A_v6 destination 2409:8087:3408:10:1040::4000/114 destination-port eq 22

rule 2001 permit tcp destination 2409:8087:3408:10:1040::4000/114 destination-port object-group yewu01

建议把源地址或者目的地址的匹配掩码不要超过64位，可以减少位宽占用

Resource DB 7 [Group 7]

Type = TCAM, Stage = ingress_pmf, Priority = 74, Key Size = 320, NOF CEs = 14

Key:

Second	Key msb	Key lsb	Lost Bits	Qual msb	Qual lsb	Qual Type	
No	31	0	0	31	0	ipv6_sip_high	//ipv6源地址，32bit
No	63	32	0	31	0	ipv6_sip_low	//ipv6源地址，32bit
No	79	64	0	15	0	user_def_4	//目的端口号，16bit
No	111	80	0	63	32	ipv6_sip_low	//ipv6源地址，32bit
No	143	112	0	63	32	ipv6_sip_high	//ipv6源地址，32bit
No	159	144	0	15	0	user_def_3	//源端口号，16bit
Yes	31	0	0	31	0	ipv6_dip_high	//ipv6目的地址，32bit
Yes	39	32	0	7	0	ipv6_next_prtcl	//TCP，8bit
Yes	63	40	0	23	0	ipv6_l4ops	//range，24bit
Yes	69	64	0	5	0	ipv4_tcp_ctl	//TCP关键字，6bit
Yes	88	80	0	8	0	src_pp_port	//ipv6报文默认下发，9bit
Yes	92	89	0	3	0	eth_tag_format	//ipv6报文默认下发，4bit
Yes	124	93	0	63	32	ipv6_dip_high	//ipv6目的地址，，32bit
Yes	131	125	3	3	0	pfq1_next_protocol	//ipv6报文默认下发，4bit