某局点 S7600 PBR新增acl提示资源不足问题

ACL 策略路由 张文宁 2021-12-14 发表

组网及说明

不涉及

问题描述

客户对一台S7610设备新增一条acl rule规则时，设备日志提醒资源不足，没有处理。

在acl 3330中新增一条rule 257，设备打印资源不足日志：

%Nov 10 00:10:03:360 2021 HKG_2F_K04-KY-S7610-IN SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.9.9.1-User=zzgqidc; Command is acl adv 3330

%Nov 10 00:10:05:191 2021 HKG_2F_K04-KY-S7610-IN SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.9.9.1-User=zzgqidc; Command is dis this

%Nov 10 00:10:40:558 2021 HKG_2F_K04-KY-S7610-IN SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.9.9.1-User=zzgqidc; Command is rule 257 permit tcp source 59.227.152.213 0 destination 172.24.130.224 0 destination-port range 9920 9929

%Nov 10 00:10:46:275 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=2-Slot=7; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:47:203 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=1-Slot=0; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:603 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=2-Slot=0; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:064 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=1-Slot=7; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:886 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=1-Slot=1; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:675 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=2-Slot=1; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:842 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=2-Slot=2; Failed to update the policy wj because of insufficient hardware resources.

%Nov 10 00:10:46:807 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=1-Slot=2; Failed to update the policy wj because of insufficient hardware resources.

过程分析

从反馈的诊断信息看，Acl资源还有很多，才使用49%：

```
==== display qos-acl resource ====
Interfaces: GE1/0/0/1 to GE1/0/0/48 (chassis 1 slot 0)
------------------------------------------------------------------------
Type          Total     Reserved  Configured Remaining  Usage
------------------------------------------------------------------------
VFP ACL       2048      1024      0          1024       50%
IFP ACL       8192      2048      1989       4155       49%
IFP Meter     4096      1024      0          3072       25%
IFP Counter   4096      1024      9          3063       25%
EFP ACL       1024      0         10         1014       0%
EFP Meter     512       0         0          512        0%
EFP Counter   512       0         10         502        1%
```

但是Range资源不足了，这个资源每芯片可用30个（30个不同范围，range范围重复的只算一个），当前配置里面如下端口号范围每个都不一样，都会单独占用range资源，已经有30个：

```
destination-port range 20000 20050
destination-port range 28081 28082
destination-port range 3000 3006
destination-port range 30010 30014
destination-port range 3128 3132
destination-port range 61616 61618
destination-port range 8000 8001
destination-port range 8000 8004
destination-port range 8000 8005
destination-port range 8000 8020
destination-port range 8002 8003
destination-port range 8004 8005
destination-port range 8006 8007
destination-port range 8080 8081
destination-port range 8080 8082
destination-port range 8080 8087
destination-port range 8080 8099
destination-port range 8081 8083
destination-port range 8086 8087
destination-port range 8088 8091
destination-port range 8170 8172
destination-port range 8291 8293
destination-port range 8514 8515
destination-port range 8920 8922
destination-port range 9001 9003
destination-port range 9091 9095
destination-port range 9200 9201
destination-port range 9900 9909
destination-port range 9990 9991
destination-port range snmp snmptrap
```

而新配置的这条rule是destination-port range 9920 9929，又是一个新的范围，也会再申请占用这个资源，因为此时已经没有空余资源，因此超出规格，设备打印日志资源不足告警：

```
%Nov 10 00:10:40:558 2021 HKG_2F_K04-KY-S7610-IN SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.9.9.1-User=zzgqidc; Command is rule 257 permit tcp source 59.227.152.213 0 destination 172.24.130.224 0 destination-port range 9920 9929
%Nov 10 00:10:46:275 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=2-Slot=7; Failed to update the policy wj because of insufficient hardware resources.
%Nov 10 00:10:47:203 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Chassis=1-Slot=0; Failed to update the policy wj because of insufficient hardware resources.
%Nov 10 00:10:46:603 2021 HKG_2F_K04-KY-S7610-IN PBR4/4/PBR_HARDWARE_ERROR: -Cha
```

ssis=2-Slot=0; Failed to update the policy wj because of insufficient hardware resources.

解决方法

综上，是由于range资源不足导致的acl下发失败。

从配置可以看到，很多端口号范围很小，建议通过eq（eq没有规格，但这样改写会增加rule条目数）的方式写成等价的多条下发，减少range资源的使用：

destination-port range 20000 20050
destination-port range 28081 28082
destination-port range 3000 3006
destination-port range 30010 30014
destination-port range 3128 3132
destination-port range 61616 61618
destination-port range 8000 8001
destination-port range 8000 8004
destination-port range 8000 8005
destination-port range 8000 8020
destination-port range 8002 8003
destination-port range 8004 8005
destination-port range 8006 8007
destination-port range 8080 8081
destination-port range 8080 8082
destination-port range 8080 8087
destination-port range 8080 8099
destination-port range 8081 8083
destination-port range 8086 8087

整改举例：

整改前：

rule permit tcp source 172.20.30.166 0 destination 172.24.130.8 0 destination-port range 28081 28082

整改后：

rule permit tcp source 172.20.30.166 0 destination 172.24.130.8 0 destination-port eq 28081
rule permit tcp source 172.20.30.166 0 destination 172.24.130.8 0 destination-port eq 28082

整改效果是range资源减一，相应的acl资源加一。

关于现场下发失败提示资源不足后，业务受影响问题，undo rule才恢复的原因说明：

当PBR中某个rule规则变动时，所有相关接口的PBR规则都会重刷，重刷时前面的规则成功了，但到后面由于资源不足，下发动作会停止并打印日志，后面的acl就无法下发完全，导致业务受影响。

在现网中，虽然Rule 257是acl 3330最后一条rule，但只是node 40，因为变化时整个PBR都会重刷，所以下发动作在node 40最后一条rule时因为资源不足而停止了，那么node 60之后的业务无法继续下发成功，导致业务异常。

#
policy-based-route wj permit node 10
if-match acl 3001
apply next-hop 172.20.15.130
#
policy-based-route wj permit node 20
if-match acl 3334
apply next-hop 172.20.15.194
#
policy-based-route wj permit node 30
if-match acl 3820
apply next-hop 172.20.15.194
#
policy-based-route wj permit node 40
if-match acl 3330
apply next-hop 172.20.15.162

#
policy-based-route wj permit node 60