关于H3C VCFC产品同步防火墙以及负载均衡部分手动配置导致业务中断的问题公告

刘洪彬 2016-11-28 发表

在VCFC与硬件以及NFV安全、负载均衡设备配合实现安全纳管或者服务链组网时。在某些特殊场景，需要对相关设备手动添加配置，例如：租户需要使用两个外部网段，或者需要额外手动配置安全策略等情况。当出现openflow断开重新连接，或者安全、负载均衡设备对应Context、VNF重启时，VCFC会对设备中的配置进行同步，手动添加的配置会被VCFC删除，导致业务出现中断。

VCFC控制器中对于同步设备配置的设置分为默认、开启、关闭、保留增量数据四种。

1、默认：表示控制器与指定物理网元进行数据同步时采取的策略与缺省配置对话框的数据同步策略相同。本取值只在配置指定物理网元的数据同步参数时显示。

2、开启：表示控制器自动将内存中可下发的数据同步到物理网元，并对物理网元上存在但控制器上不存在的数据进行删除，使物理网元上数据与控制器上数据保持一致。

3、关闭：表示控制器不自动将内存中可下发的数据同步到物理网元。

4、保留设备增量数据：表示控制器自动将内存中可下发的数据同步到物理网元，不删除物理网元上存在但控制器上不存在的数据。

在VCFC E2180P03及其之前版本没有上述配置同步功能，默认所有设备的手工添加配置均会被删除。

在VCFC E2180P04版本中，上述配置同步功能仅对物理网元生效（包括网关设备和接入设备），对VCFC纳管的硬件安全设备Context以及NFV VFW、VLB产品不生效,手动添加的配置都会被删除。

在VCFC E2180P05和E2180P06版本中，上述配置同步功能对物理网元、VCFC纳管的硬件安全设备Context以及NFV VFW和VLB产品部分配置实现了同步控制，受控配置列表如下，其他手动添加的配置均会被删除：

1、VFW：

1) VRF

2) 子网对应的静态路由

3) ACL（其中num 为3499的ACL 由ssl vpn下发，num为ACL 3500由 IPSEC 下发，不受同步开关控制；）

4) 安全外网对应的静态路由

5) SNAT

6) 浮动IP

7) 外网IP（loopBack2 口）

8) MQC限速

9) 安全外网，租户承载网，安全内网（虚拟路由器绑定FW和LB服务资源）

10)NAT server

2、VLB：

1) VRF

2) 安全内网，租户承载网

3) ACL

4) PBR

5) 静态路由

当业务流量中断时，通过日志可以发现安全设备对应手动增加的配置被删除，且从以下VCFC netconf_operation模块诊断日志可以看出，手动增加的配置被控制器删除。VCFC netconf模块诊断日志路径为：**\logs\netconf\netconf_operation\log.log**

Security zone配置被删除日志记录：

[2016-11-04 12:18:28.124] INFO pool-128-thread-18 DE0005I App:com.h3c.sdn.fw.fwapp, Device ip: 10.254.1.1, Operate ip:10.254.0.135, Detail:<top xmlns="**http://www.h3c.com/netconf/config:1.0**">

```
 <SecurityZone>
   <IPv4Members xc:operation="remove">
     <IPv4Member>
       <ZoneName>SNPFBVXPDTTVAWZLGJJIJT2MVU</ZoneName>
       <Ipv4Address>10.254.7.0</Ipv4Address>
       <Ipv4Mask>24</Ipv4Mask>
       <VRF>2r5cp5516f9imp6nigqrnhppqg</VRF>
     </IPv4Member>
   </IPv4Members>
 </SecurityZone>
```

1、对于需要手动增加相关业务配置的局点，如该配置在受控配置列表中，可以升级到E2180P06版本，并将默认同步策略设置成“保留设备增量数据”。

2、对于需要手动增加相关业务配置的局点，但该配置不在受控配置列表中，需要保证管理网和设备的稳定，避免VCFC与设备Openflow连接的断开与重连。
3、对于已经发生故障的局点可以手动重新配置被误删除的相关配置，恢复业务。
解决方案：
该问题在E2180P07版本最终解决，预计2016年12月底左右发布。