谁动了设备配置——利用日志信息判断设备配置发生变更的原因

金山 2016-04-13 发表

客户反馈SecBladeII（Comware V5）防火墙单板内联口被Shutdown，但从命令行配置命令操作记录看不到有人操作的日志，希望办事处分析确认故障原因。

由于SecBladeII防火墙单板内联口被Shutdown，造成主用和备用防火墙VRRP状态切换，出现VRRP切换告警。

从设备的日志记录看，目前判断是人为手工关闭Ten0/0内联接口造成的相关问题。

交换机侧只有内联口Down一条日志，无其它问题，是正常的。

防火墙侧的过程如下（以下时间均为防火墙卡本地时钟）：

1、首先，用户登录设备Web管理页面，用户名为linjw（第一次登录时密码验证错误，reason 3为即密码错）

```
#Apr  6 18:48:47:074 2016 ZMY-FW-1 SHELL/4/LOGINAUTHFAIL:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.3:linjw failed to login from Web, reason is 3
#Apr  6 18:49:04:570 2016 ZMY-FW-1 SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:linjw login from Web
#Apr  6 18:54:53:611 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
```

2、然后，用户登录后，在接口管理页面中，将设备内联Ten0/0通过Web页面的“关闭”按钮Down掉。

下面的日志中ifAdminStatus is 2表示的是接口的当前管理状态为Down，也就是Administratively Down；而ifOperStatus is 2 表明的是当前的接口实际状态为Down。

其中，索引号为2511920384的接口是Ten0/0主接口，ifAdminStatus is 2、ifOperStatus is 2表示这个接口当前是管理Down，实际状态也是Down。

其它索引号代表的是主接口派生出来的三层子接口，ifAdminStatus is 1、ifOperStatus is 2表示这些接口当前的管理Up的，但由于主接口Down了，所以实际状态也Down了。

```
#Apr  6 18:54:53:611 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920384 is Down, ifAdminStatus is 2, ifOperStatus is 2
#Apr  6 18:54:53:611 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920484 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:612 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920486 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:612 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920487 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:612 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920584 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:612 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920586 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:613 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920588 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:613 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920589 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:613 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920590 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:613 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920591 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:614 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251920592 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:730 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251921272 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:730 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251921294 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:730 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251921486 is Down, ifAdminStatus is 1, ifOperStatus is 2
#Apr  6 18:54:53:731 2016 ZMY-FW-1 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3: Interface 251921487 is Down, ifAdminStatus is 1, ifOperStatus is 2
```

3、接下来，防火墙软件检测到设备配置发生了变化，打印了Trap告警，CommandSource=2, COnfigSource=4, COnfigDestination=2表示配置变化的来源是通过Web管理页面

修改了设备当前运行配置信息。

```
#Apr  6 18:57:17:475 2016 ZMY-FW-1 CFGMAN/4/TRAP:
Trap 1.3.6.1.4.1.25506.2.4.2.1: configure changed, EventIndex=1014, CommandSource=2, COnfigSource=4, COnfigDestination=2.
```

4、最后，由于防火墙配置了Web登录用户空闲推出时间，该用户登录约一小时后退出Web登录。

```
#
web idle-timeout 60
#
```

```
#Apr  6 19:55:00:427 2016 ZMY-FW-1 SHELL/4/LOGOUT:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.2:linjw logout from Web
```

上述便是现场的情况还原，由于是Web页面上的操作，所以在设备的history command中是没有这条记录的。

经过问题分析，现场反馈的问题确认为用户自行操作导致，不是H3C设备自身原因。

通过实验室模拟操作，我们可以观察到分别通过CLI、Web、SNMP操作修改设备配置后，设备上会产生的记录信息，希望对大家分析此类问题有帮助。

CLI命令行方式操作

```
Jul 18 09:16:18 10.255.255.91 Jul 18 09:14:39 2012 F5000A5_1 %%10IFNET/4/INTERFACE UPDOWN(t):   Trap 1.3.6.1.6.3.1.1.5.3: Interface 486539273 is Down, ifAdminStatus is 2, ifOperStatus is 2
Jul 18 09:16:18 10.255.255.91 Jul 18 09:14:39 2012 F5000A5_1 %%10SHELL/6/SHELL_CMD(l): -Task=vt0-IPAddr=10.255.255.129-User=**; Command is shutdown
Jul 18 09:16:18 10.255.255.91 Jul 18 09:14:39 2012 F5000A5_1 %%10IFNET/3/LINK_UPDOWN(l): Vlan-interface10 link status is DOWN.
Jul 18 09:16:18 10.255.255.91 Jul 18 09:14:39 2012 F5000A5_1 %%10IFNET/5/LINEPROTO_UPDOWN(l): Line protocol on the interface Vlan-interface10 is DOWN.
Jul 18 09:16:20 10.255.255.91 Jul 18 09:14:41 2012 F5000A5_1 %%10IFNET/4/INTERFACE UPDOWN(t):   Trap 1.3.6.1.6.3.1.1.5.4: Interface 486539273 is Up, ifAdminStatus is 1, ifOperStatus is 1
```

WEB方式操作

```
Jul 18 09:16:45 10.255.255.91 Jul 18 09:15:06 2012 F5000A5_1 %%10SHELL/4/LOGIN(t):   Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:h3c login from Web
Jul 18 09:16:45 10.255.255.91 Jul 18 09:15:06 2012 F5000A5_1 %%10WEB/4/WEBOPT_LOGIN_SUC(l): h3c logged in from 10.255.255.129
Jul 18 09:17:07 10.255.255.91 Jul 18 09:15:28 2012 F5000A5_1 %%10IFNET/4/INTERFACE UPDOWN(t):   Trap 1.3.6.1.6.3.1.1.5.3: Interface 486539273 is Down, ifAdminStatus is 2, ifOperStatus is 2
Jul 18 09:17:07 10.255.255.91 Jul 18 09:15:28 2012 F5000A5_1 %%10IFNET/3/LINK_UPDOWN(l): Vlan-interface10 link status is DOWN.
Jul 18 09:17:07 10.255.255.91 Jul 18 09:15:28 2012 F5000A5_1 %%10IFNET/5/LINEPROTO_UPDOWN(l): Line protocol on the interface Vlan-interface10 is DOWN.
Jul 18 09:17:11 10.255.255.91 Jul 18 09:15:32 2012 F5000A5_1 %%10IFNET/4/INTERFACE UPDOWN(t):   Trap 1.3.6.1.6.3.1.1.5.4: Interface 486539273 is Up, ifAdminStatus is 1, ifOperStatus is 1
Jul 18 09:22:10 10.255.255.91 Jul 18 09:20:31 2012 F5000A5_1 %%10CFGMAN/4/TRAP(t):  Trap 1.3.6.1.4.1.25506.2.4.2.1: configure changed, EventIndex=10, CommandSource=2, COnfigSource=4, COnfigDestination=2.
```

SNMP方式操作

```
Jul 18 09:38:39 10.255.255.91 Jul 18 09:37:01 2012 F5000A5_1 %%10IFNET/3/LINK_UPDOWN(l): Vlan-interface10 link status is DOWN.
Jul 18 09:38:39 10.255.255.91 Jul 18 09:37:01 2012 F5000A5_1 %%10IFNET/5/LINEPROTO_UPDOWN(l): Line protocol on the interface Vlan-interface10 is DOWN.
Jul 18 09:38:39 10.255.255.91 Jul 18 09:37:01 2012 F5000A5_1 %%10CFGMAN/5/CFGMAN_CFGCHANGED(l): -EventIndex=11-CommandSource=2-COnfigSource=3-COnfigDestination=2; Configuration is changed.
Jul 18 09:38:42 10.255.255.91 Jul 18 09:37:04 2012 F5000A5_1 %%10IFNET/4/INTERFACE UPDOWN(t):   Trap 1.3.6.1.6.3.1.1.5.4: Interface 486539273 is Up, ifAdminStatus is 1, ifOperStatus is 1
Jul 18 09:38:42 10.255.255.91 Jul 18 09:37:04 2012 F5000A5_1 %%10CFGMAN/4/TRAP(t):  Trap 1.3.6.1.4.1.25506.2.4.2.1: configure changed, EventIndex=12, CommandSource=2, COnfigSource=3, COnfigDestination=2.
```