Cisco 设备日志转储的故障排除

许杨春 诺基亚西门子网络

由于 Cisco 设备的 flash 有限，将日志转储到 Unix pc 一种有效的方式。这方面的资料非常多，最权威当然是 Cisco 的产品说明书. 但是在实践发现光按“Catalyst 3750 Switch Software Configuration Guide”中的说明配置后还不一定成功，尤其是 Unix pc 端的配置需要调整。

在 Switch 操作如下：
3750#configure terminal
3750#logging <host>　　这里<host>是 Unix pc 的 ip 地址，本例中为 10.68.173.253.
其他的配置都使用缺省值,这样一个最简单的日志转储到 Unix pc 的配置已经完成。

在 Unix pc 操作如下：
[root@localhost ~]# vi /etc/syslog.conf
加入一行，
local7.debug　/var/log/cisco.log
注意 Cisco 文档在 IOS Release 12.2(55)SE 的描述中有文件名不一致的问题。
[root@localhost ~]# touch /var/log/cisco.log　　建立或刷新文件 cisco.log
[root@localhost ~]# chmod 666 /var/log/cisco.log　修改文件权限
再重新启动 sylog 进程
[root@localhost ~]# kill -HUP `cat /etc/syslog.pid`
cat: /etc/syslog.pid: No such file or directory
kill: usage: kill [-s sigspec | -n signum | -sigspec] pid | jobspec ... or kill -l [sigspec]
这里碰到了第一个问题，syslog 原来没有启动，所以用以下命令启动。
[root@localhost ~]# service syslog start
Starting system logger:
Starting kernel logger:
[root@localhost ~]#

但是过一段时间后，检查/var/log/cisco.log 文件，发现文件大小依然为 0。
再回到 Switch 检查，用以下命令检查日志的设置是否正确：
3750#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes,
 0 overruns, xml disabled, filtering disabled)
<略去无关显示>
　　Trap logging: level informational, 52 message lines logged
　　　　Logging to 10.68.173.253　(udp port 514,　audit disabled,
　　　　　　authentication disabled, encryption disabled, link up),
　　　　　　2 message lines logged,
　　　　　　0 message lines rate-limited,
　　　　　　0 message lines dropped-by-MD,

xml disabled, sequence number disabled
filtering disabled
<略去无关显示>
3750#
黑体部分显示说明 Switch 确实在向 Unix pc 发包，那么 udp 数据包是否到了 Unix pc 呢。Unix PC 上执行 tcpdump 可以看到类似 syslog 包（用 Wireshark 分析得）

1 0.000000 10.68.173.130 10.68.173.253 Syslog 241 LOCAL7.DEBUG: 804745574: 4024597424: *Mar 22 15:57:12.929: IP: s=10.68.173.130 (local), d=10.68.173.253, len 215, local feature, Local Clustering(8), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

这说明从 Switch 到 Unix pc 的通路是通畅的，可以排除防火墙之类的影响。由于 udp 无连接特性，还需要检查接收方是否运行正常，Unix pc 上用 netstat 命令察看 udp 监听端口：
[root@localhost ~]# netstat -l -u
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 0 0 localhost.localdomain:58766 *:*
udp 0 0 10.68.173.253:31001 *:*
udp 0 0 10.68.173.253:31002 *:*
<略去无关显示>

没有看到对应 udp 端口（514）在监听。
检查后发现，原来该 Linux 版本的 syslog 缺省设置是丢弃外来的数据，修改 syslog 配置如
[root@localhost ~]# vi /etc/sysconfig/syslog
Options to syslogd
-m 0 disables 'MARK' messages.
#-r enables logging from remote machines
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
SYSLOGD_OPTIONS="-m 0 -r " 在引号内加入-r
再重启 syslog，netstat 就可以看 syslog udp 监听端口
[root@localhost ~]# /etc/init.d/syslog restart
Shutting down kernel logger: [OK]
Shutting down system logger: [OK]
Starting system logger: [OK]
Starting kernel logger: [OK]
[root@localhost ~]# netstat -l -u
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 110400 0 *:**syslog** *:*
<略去无关显示>
再检查检查/var/log/cisco.log 文件大量数据包。最后本次实验结束用
LTE_3750(config)#no logging on
关闭 Switch 的日志输出。