SecCenter 无法显示安全设备日志的排错方法

Seccenter A1000 刘思 2013-08-16 发表

SecCenter 无法显示安全设备日志的排错方法

一、问题描述：

安全设备例如防火墙、UTM、ACG等可将系统运行日志以及流量日志等信息保存下来，以便管理员在需要的时候进行查看。但当设备较多的时候，分别登陆到各台设备去查看无疑会增加管理员的工作量，SecCenter可将所有我司安全设备的各类日志信息以图表的形式展现出来，方便管理员进行查看。在某些应用场景中，安全设备相关配置正确，日志信息成功上送到SecCenter服务器，但在SecCenter还是无法查看相关日志信息。针对此种情况，可以按照本文所述的方法进行问题排查。本文主要以防火墙日志（userlog）为例，其他安全设备的日志接收情况与此类似。

三、过程分析：

安全设备将日志上送到SecCenter时，会携带自身时钟信息。SecCenter则打开响应的UDP端口来侦听上送日志报文，并将接收到的报文经由相关进程处理之后写入Mysql数据库。SecCenter前台页面在数据库中调用相关SQL语句并将最终结果通过报表的形式展示出来。

该过程中用到的端口以及进程主要见下图：

二、排错思路

1、查看SecCenter接收器进程是否正常启动。

c:\>netstat -aon | findstr 30010

UDP 0.0.0.0:30010 *:* 4560

从该命令执行结果可得知，进程PID 4560打开了UDP 30010端口。

c:\>tasklist | findstr 4560

receiverv0.exe 4560 Services 0 16,664 K

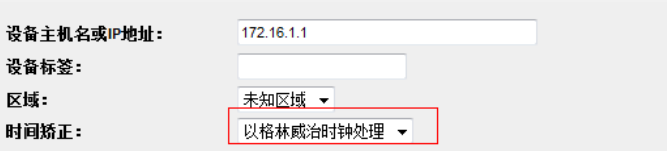
从该命令执行结果可得知，进程PID 4560对应的进程名称为receiverv0.exe，属于正常现象。

若端口被其他进程占用，则关闭占用端口的进程，在..\SecCenter\receiver目录下双击receiverv0.exe，该进程就会启动。若找不到该进程，则可能该进程已经被杀毒软件删除，请将杀毒软件卸载或者在杀毒软件中将该进程设置为信任，并在该目录下执行receiver_install.bat脚本工具，便可重新生成相关接收器可执行文件。

2、确保防火墙的时区与SecCenter的配置一致，若不一致，请修改为一致。

[H3C]display clock

16:06:33 UTC Sat 07/20/2013



3、在上述两步都正确的情况下，请在服务器进行抓包，看是否有udp.dstport==30010的数据包送过来。如未有日志报文过来，请确认设备侧配是否正确。

4、在上述三步都正确的情况下，请查看...\SecCenter\syslog目录下recvNat.log日志，若其中有包含如下字段，则表示发送userlog日志的报文源IP地址非防火墙设备的管理地址，请确保二者一致。需要说明的是，当SecCenter所在服务器防火墙开启的时候，也会有如下报错，请放通相关端口，或者关闭防火墙。

7-20-2013 16:44:33:[INFO] The port is 30017

7-20-2013 16:44:33:[WARNING] The host address inputted is not correct

5、在上述4步都未解决问题的情况下，请收集如下日志、SecCenter版本以及相关抓包以供华三技术支持中心进行分析定位。

日志路径为：

..\SecCenter\syslog

..\SecCenter\server\logs