syslog组件端口手动修改后未同步修改info-center主机端口号导致没有syslog日志的经验案例

统一数字底盘 SeerAnalyzer AD-NET解决方案 **很好网络使我CPU火热** 4天前 发表

问题描述

先部署分析器后部署syslog导致端口冲突，syslog组件端口冲突手动修改后未同步修改info-center主机端口号导致没有syslog日志

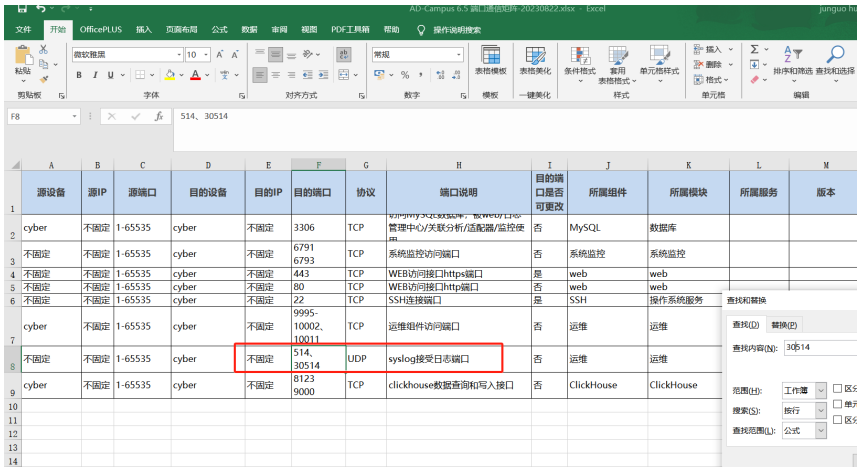
过程分析

首先在服务器后台用tcpdump抓包看到有syslog日志，说明设备发送了syslog日志到服务器主机后台。进一步观察后发现同时部署了分析器和syslog组件，并且进一步反馈存在部署时端口冲突报错，然后修改端口的操作，所以确认是info-center没有对应修改端口号，未发送日志到syslog组件。

1、首先部署syslog组件和分析器有顺序要求，可以参照对应底盘手册

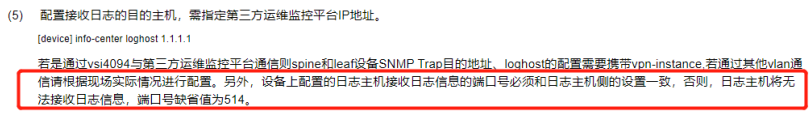
- 若分析组件（Analyzer-Collector）和 Syslog 组件需同时安装，请安装 Syslog 组件后，再安装分析组件，否则 Syslog 组件将部署异常。

情况如下：
若先部署syslog组件，再部署分析器，无异常提示
若先部署分析器，再部署syslog组件，此时分析器占用syslog组件默认的514端口，会导致syslog组件部署失败。
2、若出现了先部署分析器，再部署syslog组件的情况下，底盘除了默认的514端口还可以使用其他端口号接受设备发送的日志，具体可以根据方案版本参考端口通信矩阵，以ADCampus6.5版本为例，除了514还可以用30514端口



源设备	源IP	源端口	目的设备	目的IP	目的端口	协议	端口说明	目的端口是否可更改	所属组件	所属模块	所属服务	版本
cyber	不固定	1-65535	cyber	不固定	3306	TCP	管理中心/关联分析/适配器/监控使用	否	MySQL	数据库		
不固定	不固定	1-65535	cyber	不固定	6791 6793	TCP	系统监控访问端口	否	系统监控	系统监控		
不固定	不固定	1-65535	cyber	不固定	443	TCP	WEB访问接口https端口	是	web	web		
不固定	不固定	1-65535	cyber	不固定	80	TCP	WEB访问接口http端口	否	web	web		
不固定	不固定	1-65535	cyber	不固定	22	TCP	SSH连接端口	是	SSH	操作系统服务		
cyber	不固定	1-65535	cyber	不固定	9995-10002、10011	TCP	运维组件访问端口	否	运维	运维		
不固定	不固定	1-65535	cyber	不固定	514、30514	UDP	syslog接受日志端口	否	运维	运维		
cyber	不固定	1-65535	cyber	不固定	8123 9000	TCP	clickhouse数据查询和写入接口	否	ClickHouse	ClickHouse		

所以如果先部署分析器，后部署了syslog组件，可以选择卸载分析器或者修改syslog组件的端口号。
3、如果修改了syslog组件的端口号后，那么对应的开局部署指导里的info-center配置也要修改，因为此时默认端口还是514端口
可以具体参考方案的运维监控指导书



(5) 配置接收日志的目的主机，需指定第三方运维监控平台IP地址。

```
[device] info-center loghost 1.1.1.1
```

若是通过vsi4094与第三方运维监控平台通信则spine和leaf设备SNMP Trap目的地址、loghost的配置需要携带vpn-instance,若通过其他vlan通信请根据现场实际情况进行配置。另外，设备上配置的日志主机接收日志信息的端口号必须和日志主机侧的设置一致，否则，日志主机将无法接收日志信息，端口号缺省值为514。

修改端口号之后可以正常接受syslog日志。

解决方法

手动修改info-center配置

info-center loghost 1.1.1.1 port +修改后的端口号
规避问题