CSAP-SA-M综合日志审计平台无法正常接收日志

info-center Syslog日志 王奎银 2020-02-25 发表

组网及说明

不涉及

问题描述

现场安装完CSAP-SA-M综合日志审计平台也配置好日志源、同时日志采集器也处于在线状态。但是仍然没有日志发送过来，已经确认综合日志审计平台到日志源设备可以通的

过程分析

当时怀疑有两个有两个原因：

1. 综合日志审计平台到日志源有安全设备阻断udp协议；
2. 日志源侧有特殊配置未输出到日志主机，比如info-center闭环，或者没有配置日志

排查发现：

1. 中间设备没有安全设备阻断UDP协议；
2. 确认现场的设备，相关配置都是正常的，而且在设备抓包我们都是正常可以将报文发送出来（抓取目的地址为日志服务器的UDP514报文）

在综合日志审计平台侧抓包发现抓不到报文。

后来我们确认到综合日志审计平台的日志源要与设备发送日志的源接口要一致。

解决方法

设备侧配置日志要发送日志到日志服务器的时候需要配置源接口与CSAP-SA-M综合日志审计平台的日志源相同，虽然设备侧日志发送的源接口是可选的，但是在这里必须要填写。

配置命令：

[H3C] info-center loghost source LoopBack 0

不管安全设备、交换机和路由器都是需要这样的配置，综合日志审计平台对日志源接口进行检查。