某局点SecCenter CSAP-SA 态势感知综合日志审计平台(硬件主机) agent管理添加自定义文件时，报错“新增失败”问题排查

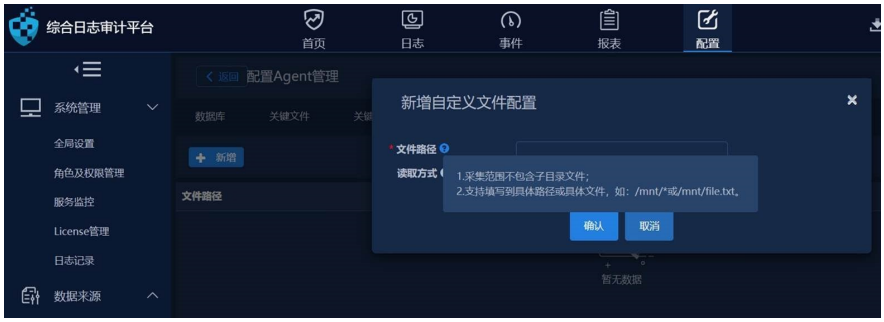
Syslog日志 日志采集器 徐猛 2021-01-14 发表

组网及说明

不涉及

问题描述

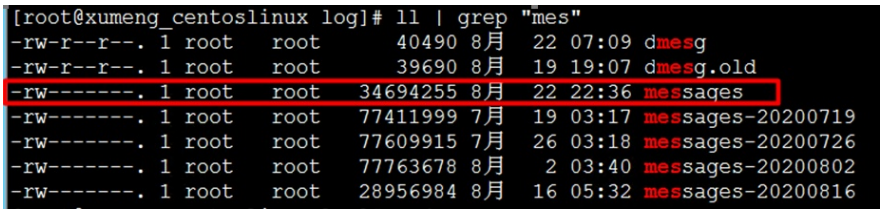
现场使用 E1707P03 版本的综合日志审计平台管理网络设备，以及服务器的日志等信息，目前网络服务器安装agent后，基本日志等信息，已经能正常的被日志审计平台接收和识别，但是客户在新增自定义文件配置中，添加一些应用日志进行上传，在添加文件路径后，直接报错新增失败。



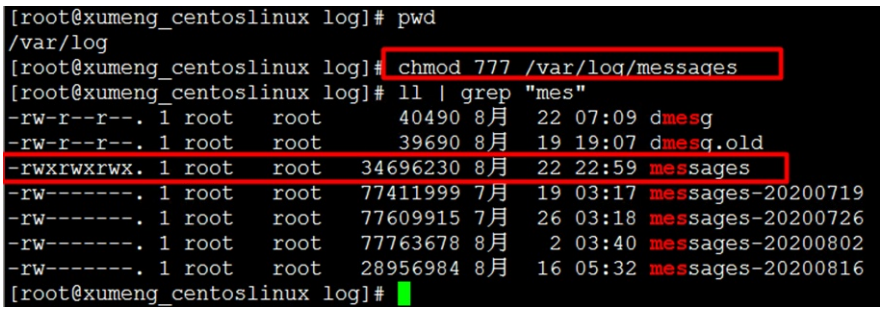
过程分析

1、经过和渠道了解，添加的目录是linux系统的一个服务器日志文件，且客户在设备上，通过cat /var/log/messages可以正常查看。

2、了解到linux操作系统具有丰富的权限控制功能，怀疑是日志审计设备不具有读取该日志文件的权限导致的。后来在linux系统中，通过ll命令查看文件列表，发现messages文件在默认情况下，针对组成员和其他成员不具备读写执行权限。



3、指导现场使用linux的chmod命令将该文件的权限设置为chmod 777 /var/log/messages，即让所有用户对该文件都具有读写执行的权限。客户修改后，在日志审计设备上即可新增自定义文件配置处，即可成功添加配置。



解决方法

默认情况linux上的日志文件/var/log/messages,针对组成员和其他成员不具备读权限。

现场情况允许的话，可以在linux上执行chmod 777 /var/log/messages将文件权限放开，该方法同样适用于其他linux系统的文件读写场景。