CSAP-SA综合日志审计平台 agent管理添加自定义文件失败经验案例

日志采集器 葛松炜 2021-02-23 发表

组网及说明

不涉及

问题描述

现场反馈使用CSAP-SA综合日志审计平台接收Linux服务器的日志信息，目前网络服务器安装agent后，基本日志信息已经能正常被综合日志审计平台接收并识别，但是客户现场想在自定义文件中手动添加一些Linux服务器上的日志进行上传，在添加文件路径后，直接报错新增失败。

过程分析

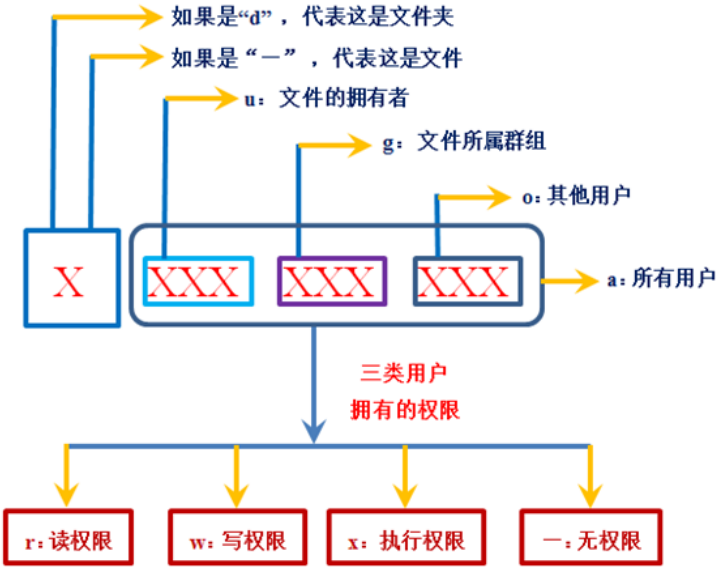
起初以为是新增自定义文件的文件路径格式写的有误，搜索后发现/var/log/messages确实是Linux服务器存放日志的地方，路径没有问题。测试后发现是/var/log/messages日志文件的权限不足导致。

解决方法

让现场在Linux服务器上，执行chmod 777 /var/log/messages修改目录权限后解决。下图为在服务器上查看日志文件的权限，可以看到只有该文件的拥有者有日志文件的读写权限，其余用户均无权限。使用chmod 777 /var/log/messages命令后，使文件拥有者，文件所属群组用户及其他用户均有对该文件的读、写、执行权限，有了足够的权限后，CSAP-SA综合日志审计平台就可以成功读取Linux服务器上该文件内的日志信息了。

```
[root@xumeng_centoslinux log]# ll | grep "mes"
-rw-r--r--. 1 root    root       40490 8月  22 07:09 dmesg
-rw-r--r--. 1 root    root       39690 8月  19 19:07 dmesg.old
-rw-------. 1 root    root    34694255 8月  22 22:36 messages
-rw-------. 1 root    root    77411999 7月  19 03:17 messages-20200719
-rw-------. 1 root    root    77609915 7月  26 03:18 messages-20200726
-rw-------. 1 root    root    77763678 8月   2 03:40 messages-20200802
-rw-------. 1 root    root    28956984 8月  16 05:32 messages-20200816
[root@xumeng_centoslinux log]# pwd
/var/log
[root@xumeng_centoslinux log]# chmod 777 /var/log/messages
[root@xumeng_centoslinux log]# ll | grep "mes"
-rw-r--r--. 1 root    root       40490 8月  22 07:09 dmesg
-rw-r--r--. 1 root    root       39690 8月  19 19:07 dmesg.old
-rwxrwxrwx. 1 root    root    34696230 8月  22 22:59 messages
-rw-------. 1 root    root    77411999 7月  19 03:17 messages-20200719
-rw-------. 1 root    root    77609915 7月  26 03:18 messages-20200726
-rw-------. 1 root    root    77763678 8月   2 03:40 messages-20200802
-rw-------. 1 root    root    28956984 8月  16 05:32 messages-20200816
[root@xumeng_centoslinux log]#
```

通过上图可以看出，在Linux系统内查看文件时，文件最前端有文件的权限说明。以本案例中的messages文件为例，起初文件的权限为-rw-------，共十个字符，对比下图说明，第一个字符可以知道是文件夹还是文件，后面九个字符分为三组，每组分别对应了不同用户所拥有的权限。因为messages文件后九个字符仅有前两个是rw，其余都是-，所以该文件只有文件拥有者有读写权限，无执行权限，其余用户均无任何权限。



这三种权限可以依次通过二进制数字表示，有对应权限为1，无对应权限为0。举个例子，如果文件的拥有者拥有读权限和写权限，没有执行权限，则对应二进制为110，转换为十进制后就是数字6。根据之前问题的解决方案，执行chmod 777 /var/log/messages修改目录权限后解决，可以看到将三种用户的权限都修改为了7，而7对应的二进制数为111，所以执行该命令实际就是让三类用户都拥有了读、写、执行三种权限，修改后可以看到文件权限由原先的-rw-------变为了-rwxrwxrwx。