1. 系统健康检查发现服务器IP

问题现象：系统健康检查发现服务器IP不对，通过查询，发现服务器地址不对；

解决方法，登陆数据库：

use dlp;

select server\_ip from sub\_server where id = 0;

update sub\_server set server\_ip = 'xxxx' where server\_ip = '192.168.10.137' and id = 0 ;

1. 终端设备管理中有终端处于离线而且无法卸载

问题现象：终端设备管理中有终端处于离线而且无法卸载；

解决方法，登陆数据库：

use dlp;

select \* from client\_device\G;

select \* from client\_device where id='3332d89cdea74beebbe41734f91dc073'\G;

delete from client\_device where id='3332d89cdea74beebbe41734f91dc073';

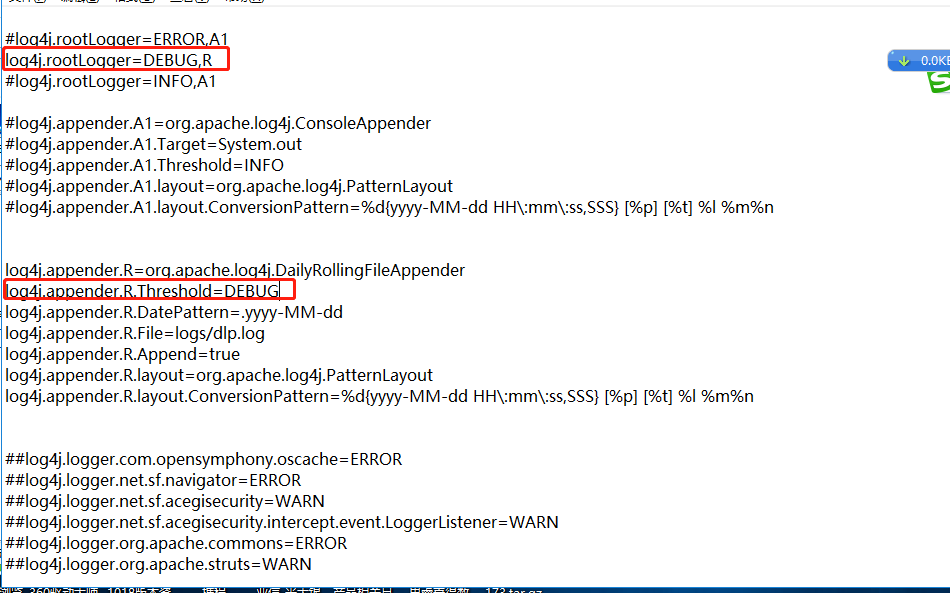
1. 查看服务器数据库中域的配置信息

方法：

select \* from sys\_settinges where kye\_name=’ldap\_flag’\G;

1. 开启dlp.log中配置syslog输出DEBUG字段

方法：在/var/lib/tomcat7/webapps/operationService/WEB-INF/lib/base-0.0.1-SNAPSHOT.jar/ log4j.properties文件的第3行和第14行INFO改成DEBUG,如下图：



扫描syslog输出信息的方法：

在服务器中执行grep write\_syslog dlp.log 查找“write\_syslog”关键字。

1. 5、重置web端sysadmin登陆密码；

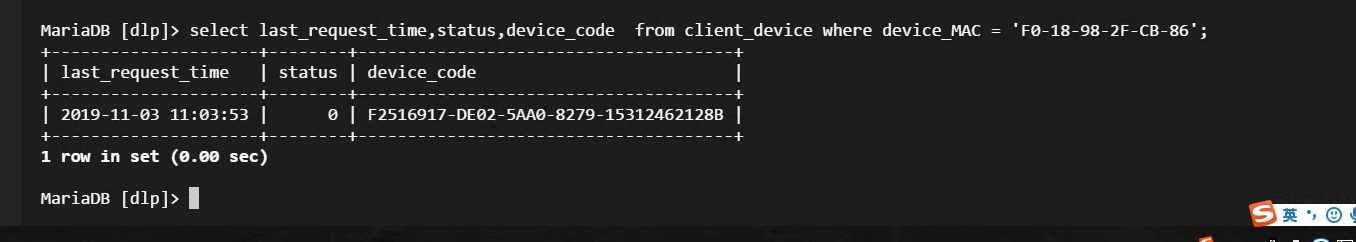
方法：

use dlp;

update sys\_user set `password` = 'd1b71e3b04bd054222bcec9249cbf865' where username ='sysadmin';

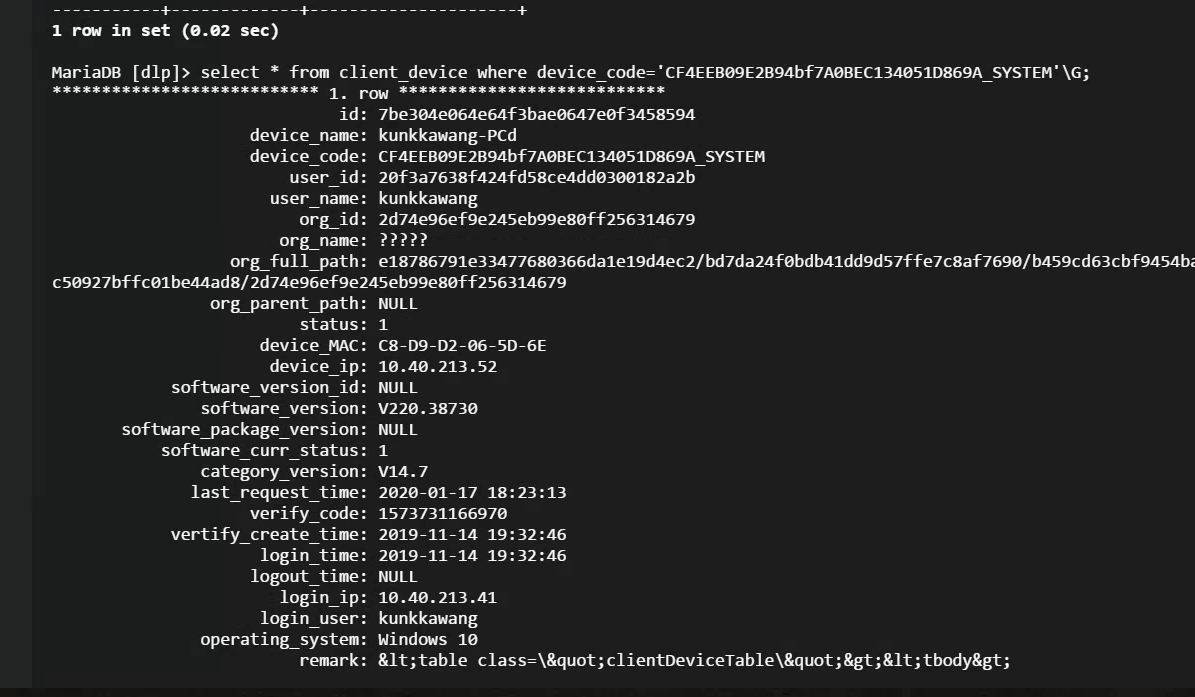
1. 6、在mysql中查询终端状态

select last\_request\_time,status,device\_code from client\_device where device\_MAC ‘f0-18-98-2f-cb-86’;



1. 在数据库中查看终端日志中的hardUuid方法；

方法：



1. 查看linux服务器的sudo权限方法

方法：

vim /etc/sudoers

tomcat7 ALL=NOPASSWD: ALL

1. 导入授权报错

导入服务器授权时报错，首先要看服务器dlp.log、catalina.out日志是否提示有sudo权限，如果没有的话 sudo会不成功，需要修改脚本中含有sudo $\*的

排查license报错方法：

java检验license是否正确

/var/lib/tomcat7/webapps/DLP/WEB-INF/classes/LicenseRequestBuilder -CHECKDIR /var/lib/tomcat7/sysauth/testLic/license.lic

张焕银检查license

/var/lib/tomcat7/webapps/openre/WEB-INF/classes/LicenseRequestBuilder -CHECKDIR /var/lib/tomcat7/sysauth/testLic/license.lic

修改配置文件：

/var/lib/tomcat7/webapps/operationService/WEB-INF/classes/command/execProcess.sh

/var/lib/tomcat7/webapps/check/WEB-INF/classes/command/execProcess.sh

/var/lib/tomcat7/webapps/DLP/WEB-INF/classes/comand/execProcess.sh

vim expecProcess.sh

#!/bin/sh

#path

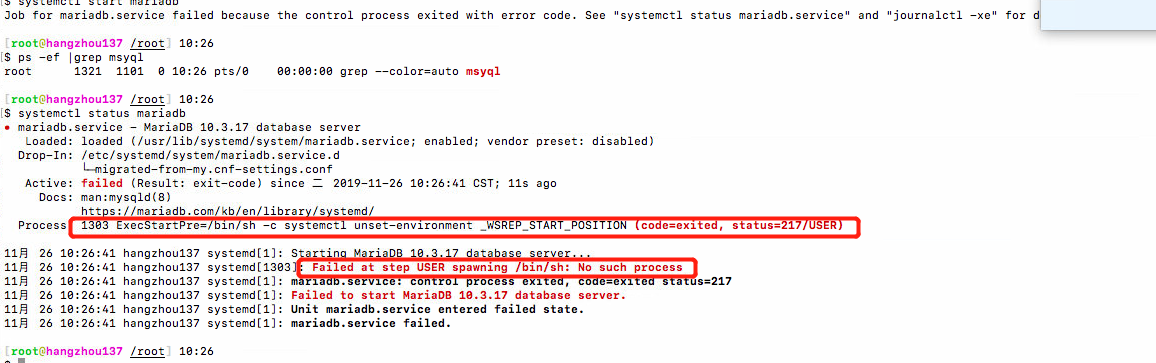
sh -c "$\*"

#sudo $\*

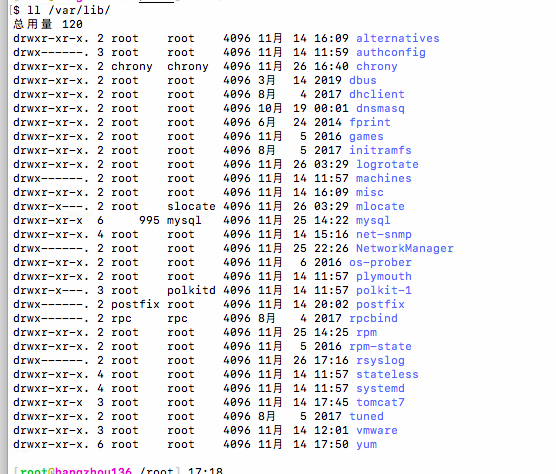
注：如果没有sudo权限也可能出现资源监控图不显示。

1. mariadb无法启动

报如下错误



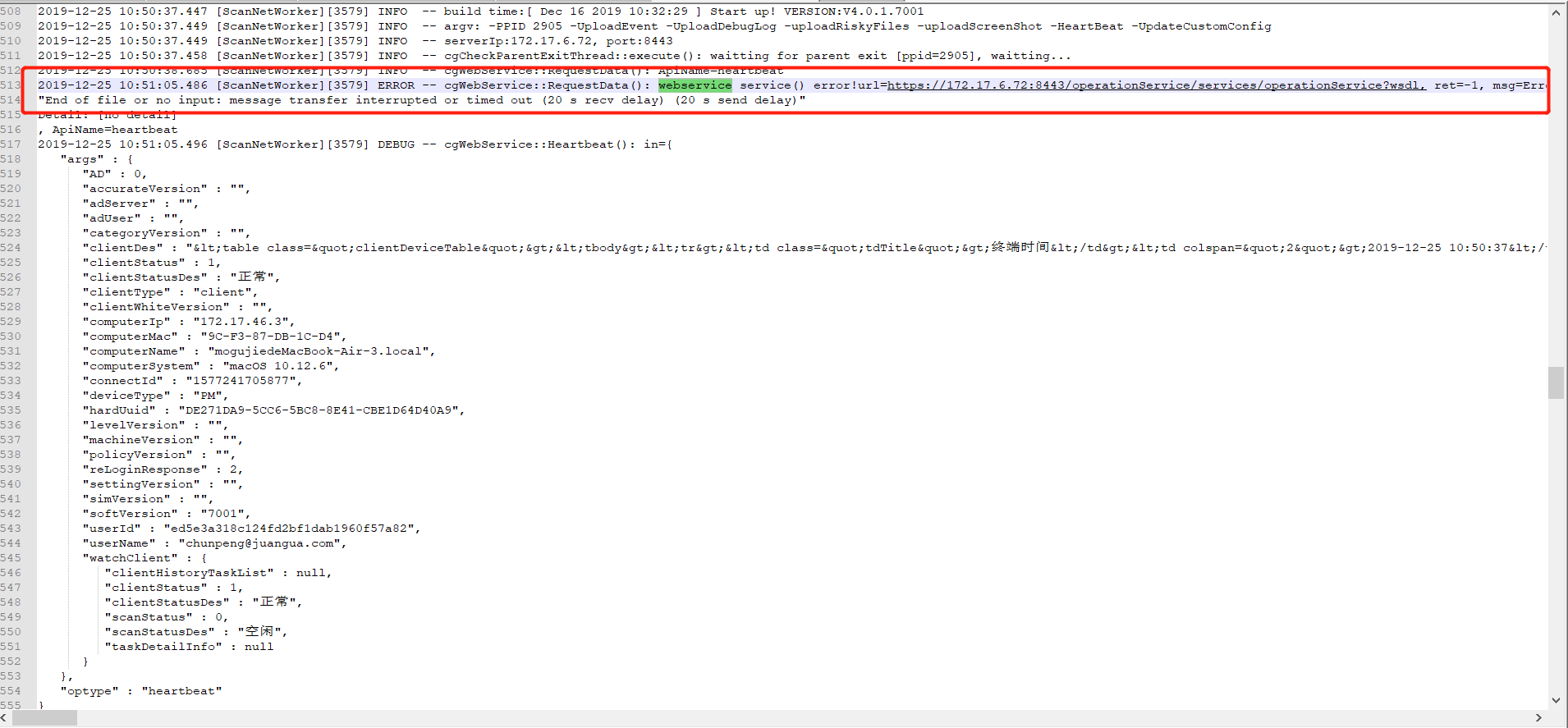
需要查看mysql安装目录的属主和属组权限是否发生变化，如下 ：

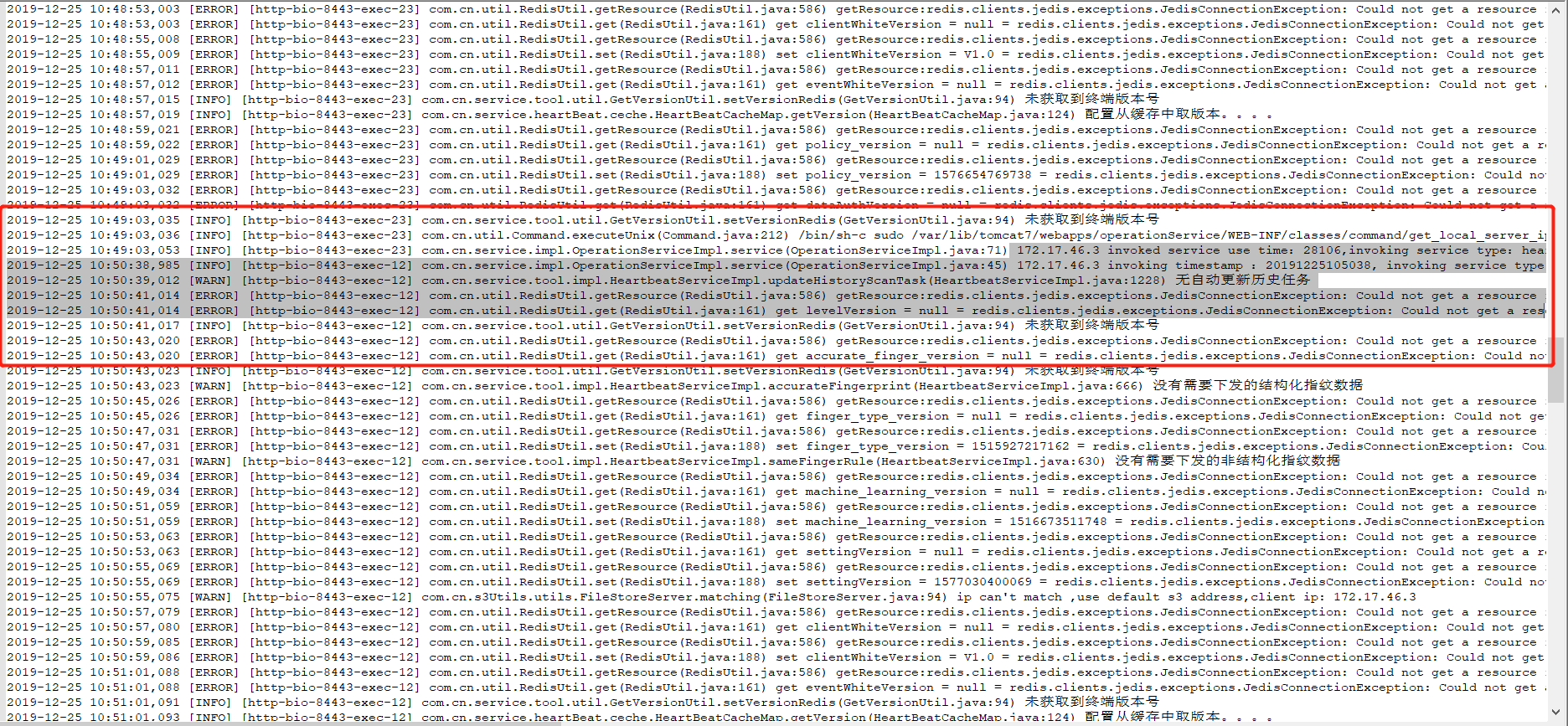


如果发生变化通过chown修改过来即可。

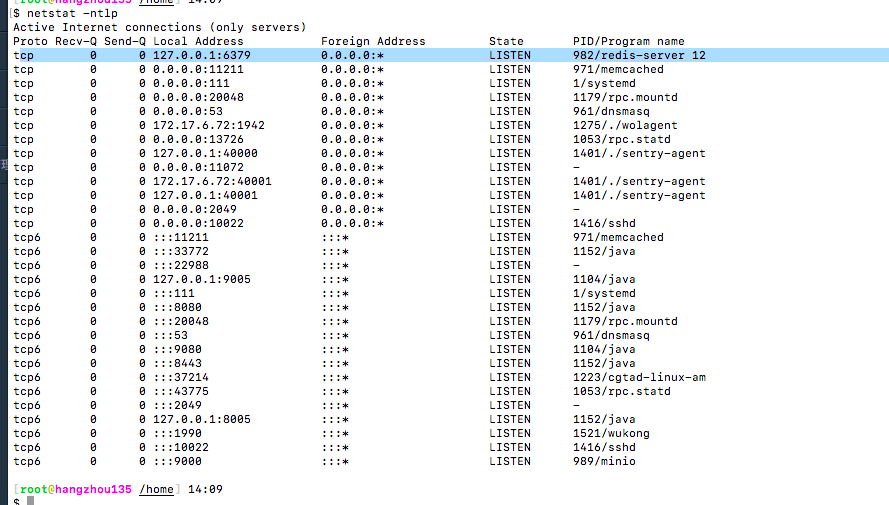
1. 终端在线，管理平台显示是离线

P9终端，有人反馈Mac终端，明明在线，但是管理平台显示就是离线，查看dlp.log日志报如下错误：





且redis正常运行



终端获取不了分类及策略：



解决方法：

将redis注释重启tomcat7即可。

1. 扩展memdata分区
2. 在/cirrus/bin/falco.sh文件中

init\_mem\_filesys()

{

....

if [ $memfs\_load = 0 ]; then

mount -t tmpfs -o size=2048m tmpfs /cirrus/memdata

fi

}

修改上面的size=2048m（2G）为 8192 （8G),即改为：

mount -t tmpfs -o size=2048m tmpfs /cirrus/memdata

1. 使得memdata新的8G内存生效

#cd /cirrus/bin

#./fslco.sh -stop

#df 可以看到memdata占用2G

#umount /cirrus/memdata

#df 这时，可以看到memdata的tmpfs已经不存在了

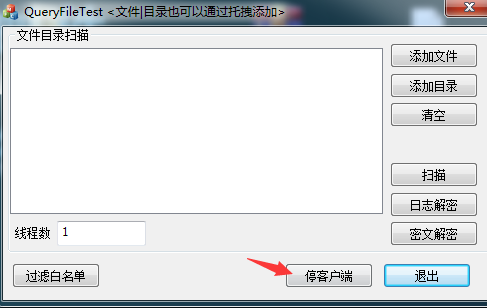
按照上面1所示更改falco.sh文件

#./falco.sh -start

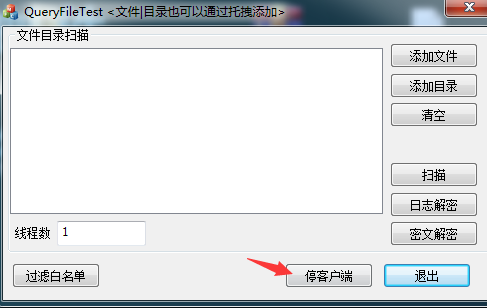
#df 这时，可以看到memdata的tmpfs已经占用8G了。

以后，重新启动服务器，8G也会自动生效的。

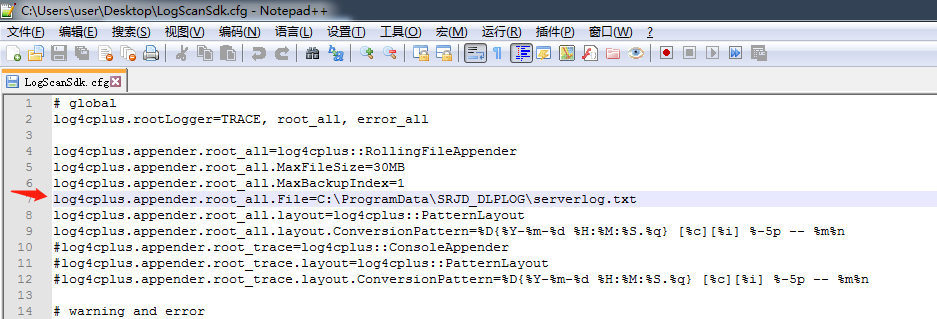
1. Windows终端开启引擎扫描日志
2. 使用工具停客户端



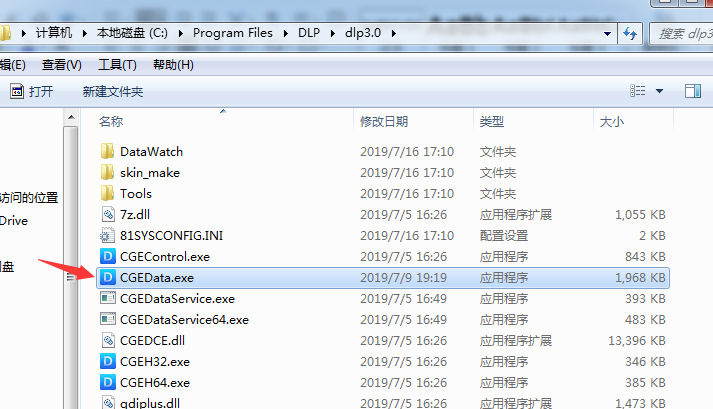
1. 在C:\Program Files\DLP\dlp3.0 目录下找到 LogScanSdk.cfg 文件



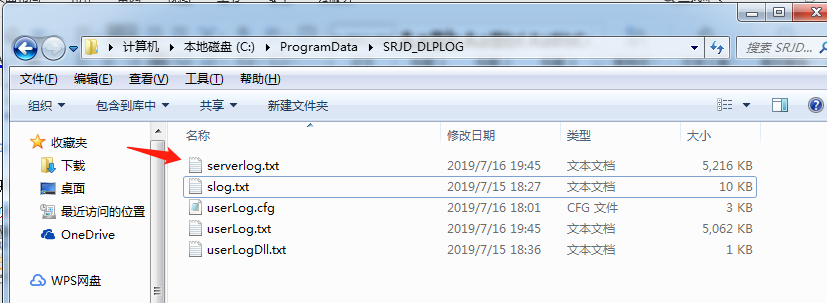
1. 打开LogScanSdk.cfg，在其中log4cplus.appender.root\_all.File=后面添加 C:\ProgramData\SRJD\_DLPLOG\serverlog.txt，保存文件



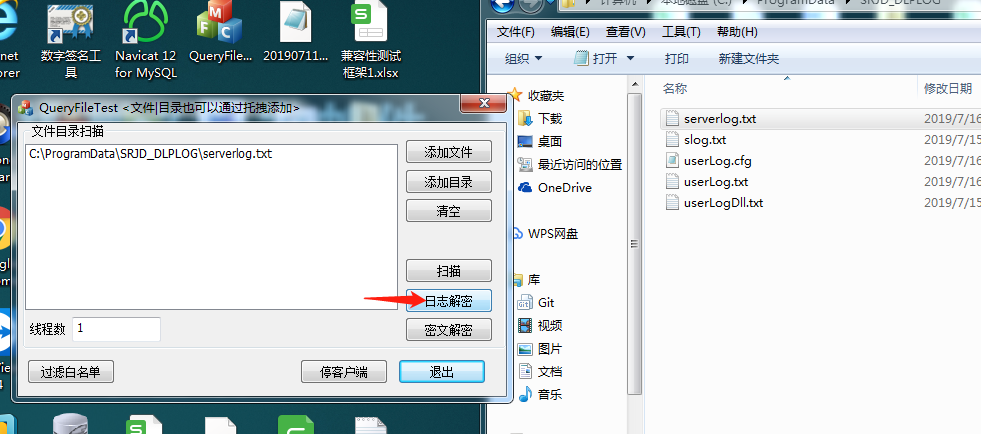
1. 在 C:\Program Files\DLP\dlp3.0 目录中双击CGEDaTa.exe，启动DLP



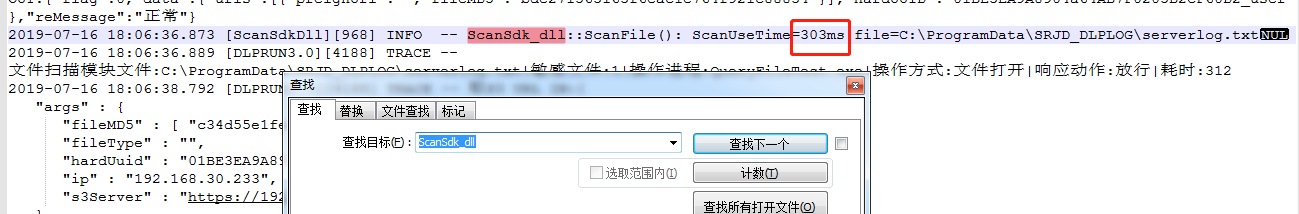
1. 在 C:\ProgramData\SRJD\_DLPLOG 目录下会出现serverlog.txt



1. 使用工具解密



1. 打开解密后文件，搜索 “ScanSdk\_dll”，该行中的时间即为扫描时间。



示例：2019-07-16 18:06:36.873 [ScanSdkDll][968] INFO -- ScanSdk\_dll::ScanFile(): ScanUseTime=303ms file=C:\ProgramData\SRJD\_DLPLOG\serverlog.txt

其中303ms为扫描时间，C:\ProgramData\SRJD\_DLPLOG\serverlog.txt为文件路径。

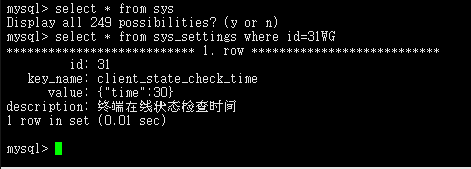
1. 终端心跳设置

打开tomcat配置文件，/var/lib/tomcat7/webapps/operationService/WEB-INF/classes/application.properties，修改heart.beat.time.out选项，默认配置100，可以根据现场情况修改。



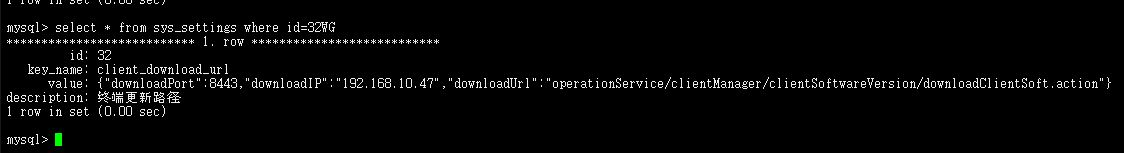
1. 终端健康性检查

进入数据库，修改id=31的value项，默认为30分钟，根据现场情况修改，如图



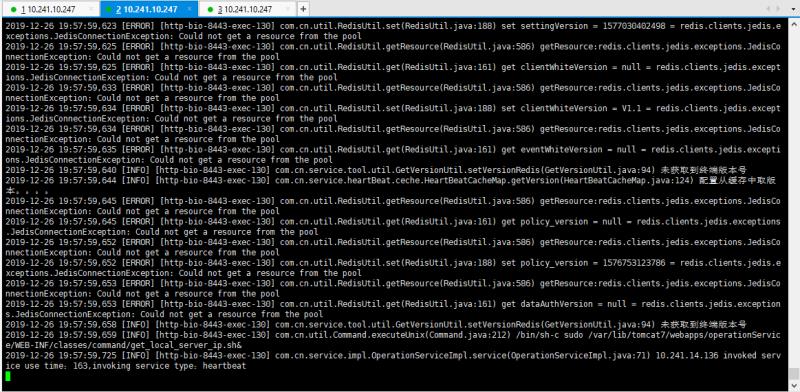
1. 终端升级包下载路径

进入数据库，修改id=32的value项.



1. 二级服务器无法访问一级服务器的redis

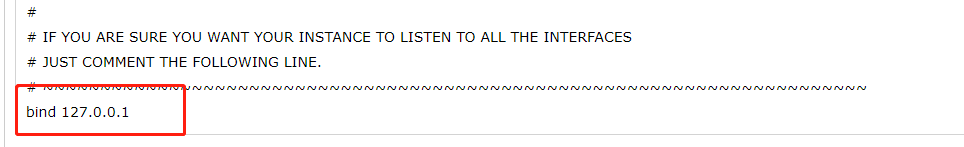
服务器端口没有限制，但是二级服务器telent一级服务器的redis端口，无法通讯，二级服务器dlp.log中，报错如下：



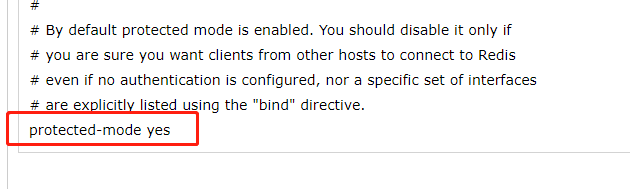
解决方法如下：

redis默认只允许本地访问，要使redis可以远程访问可以修改redis.conf

打开redis.conf文件在NETWORK部分有说明，注释掉bind 127.0.0.1可以使所有的ip访问redis



修改protected-mode no



1. 清除探针上的ocr返回结果缓存

删除探针服务器的/tmp/cirrusgate/日期，或搜索ScanSDK。在POC测试中可能会用到。