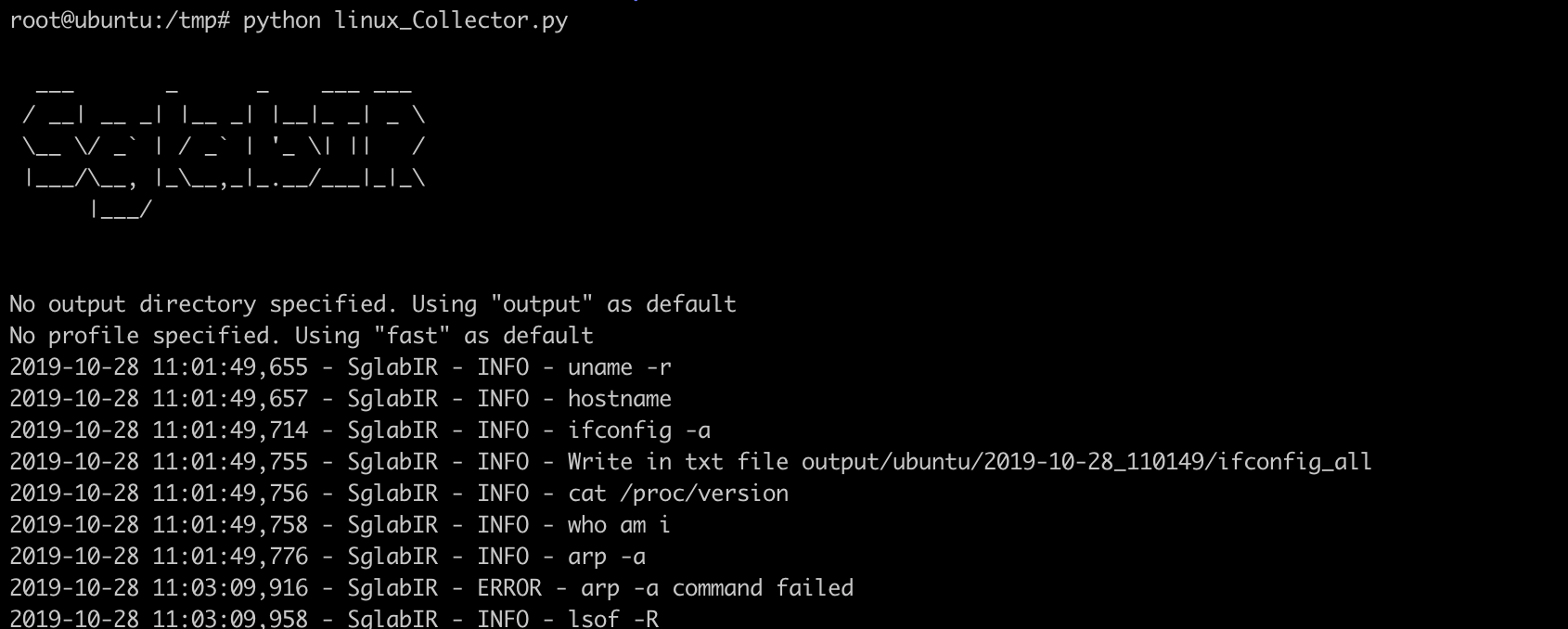
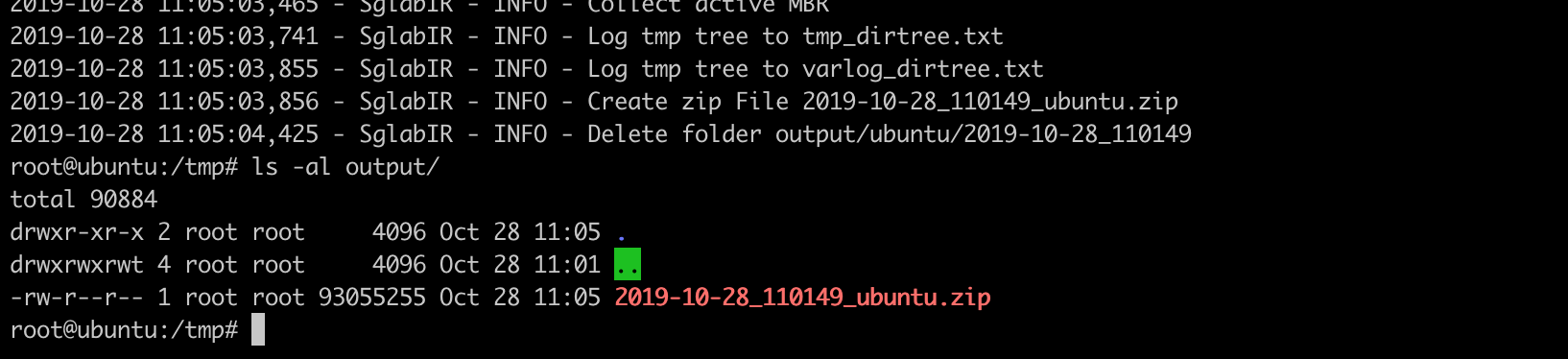
# Linux日志采集工具

采集Linux系统日志、进程、网络、文件等关键信息

1、下载Linux日志采集工具

2、下载完成后使用ROOT权限执行python采集脚本，命令如下：python linux\_Collector.py ,运行之后，会在当前目录生成output目录，进入output目录会看到生成的文件2019-10-28\_110149\_ubuntu.zip，将文件上传到对应的资产后，系统会自动进行分析





# **windows**日志采集工具

采集服务器系统、进程、注册表、网络、关键目录等信息

1、下载Windows日志采集工具

2、下载完成后使用管理员权限执行SgLabIr\_Collector\_x64（x86）.exe程序，运行之后，会在当前目录创建Output文件夹，在Output文件夹内生成<时间>\_<IP>.zip文件，将文件上传到对应的资产后系统会自动进行分析。



打包后示例如下：

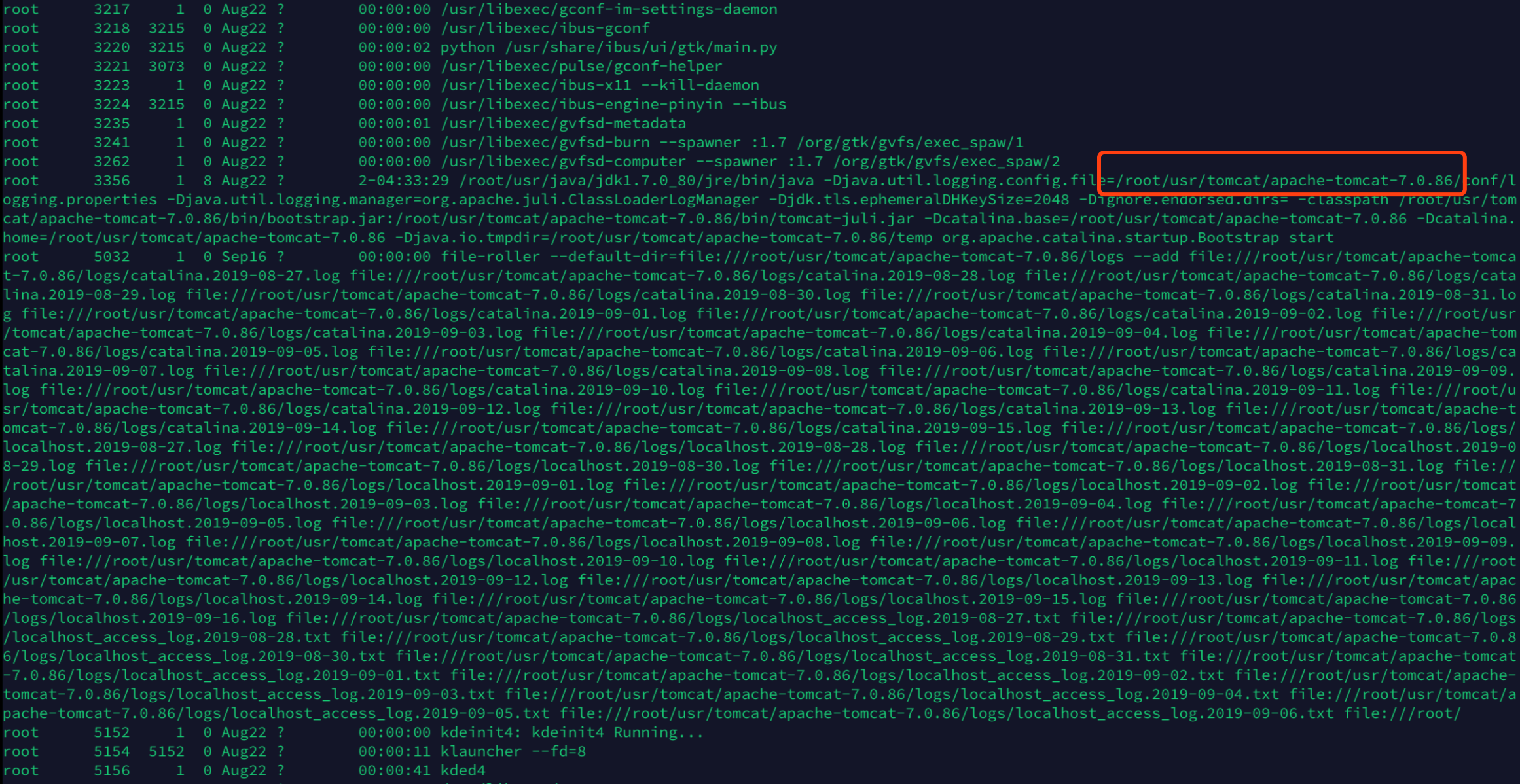


# web日志采集工具

## Linux服务器

#### Tomcat

1、Tomcat日志一般可以通过ps -ef命令寻找进程中存在的TOMCAT路径，例如下图：

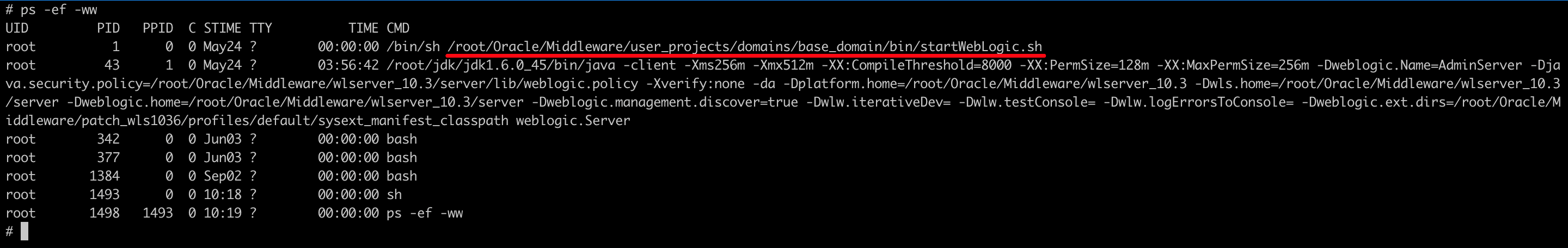


2、使用cd命令进入到目标目录后找到logs目录，然后执行tar -cvf wwwlog\_20190918.tar.gz WEB目录

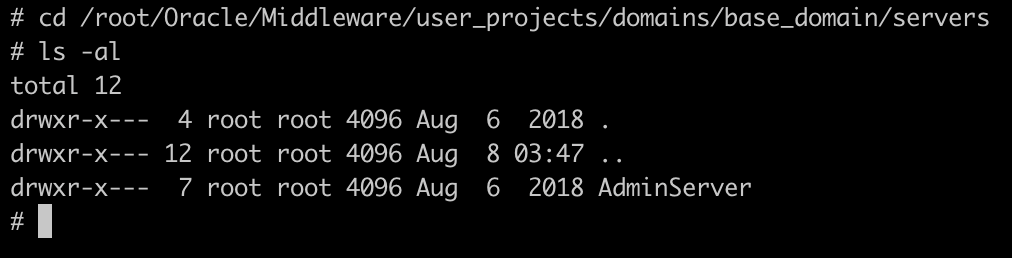
3、等待命令执行完成之后，将日志上传到对应的资产里面，系统会自动进行分析。

#### WebLogic

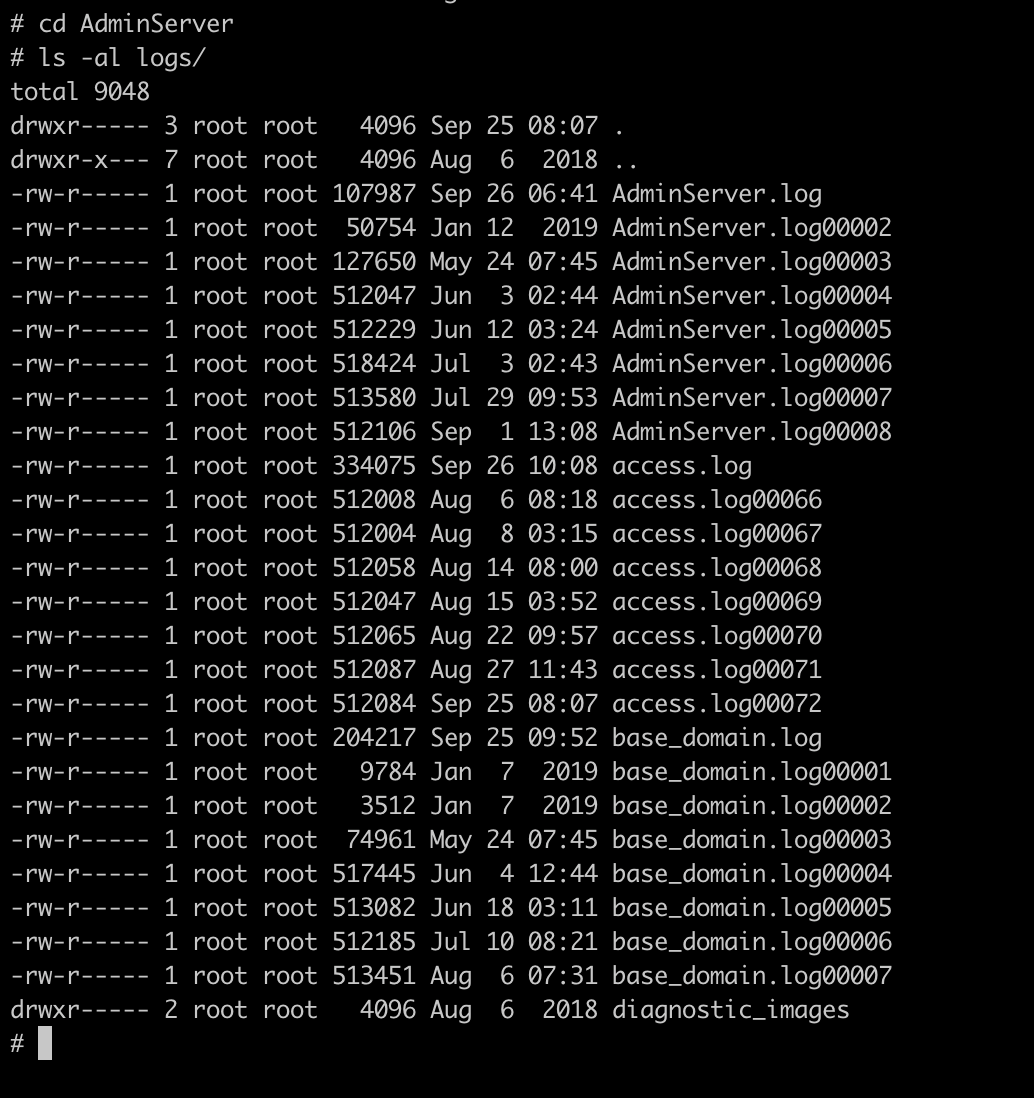
1、使用ps -ef -ww命令寻找weblogic启动脚本路径



2、进入相应域的servers目录，如/root/Oracle/Middleware/user\_projects/domains/base\_domain

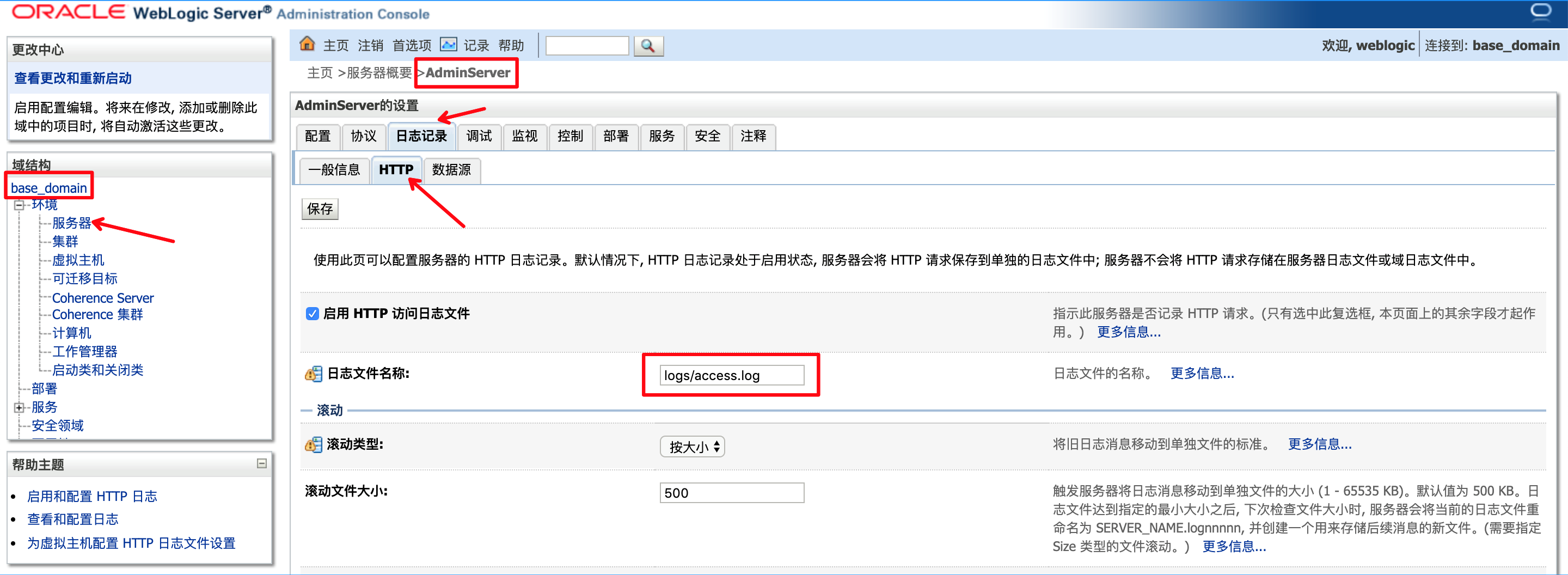


3、进入对应的Server目录，并在logs目录下寻找日志



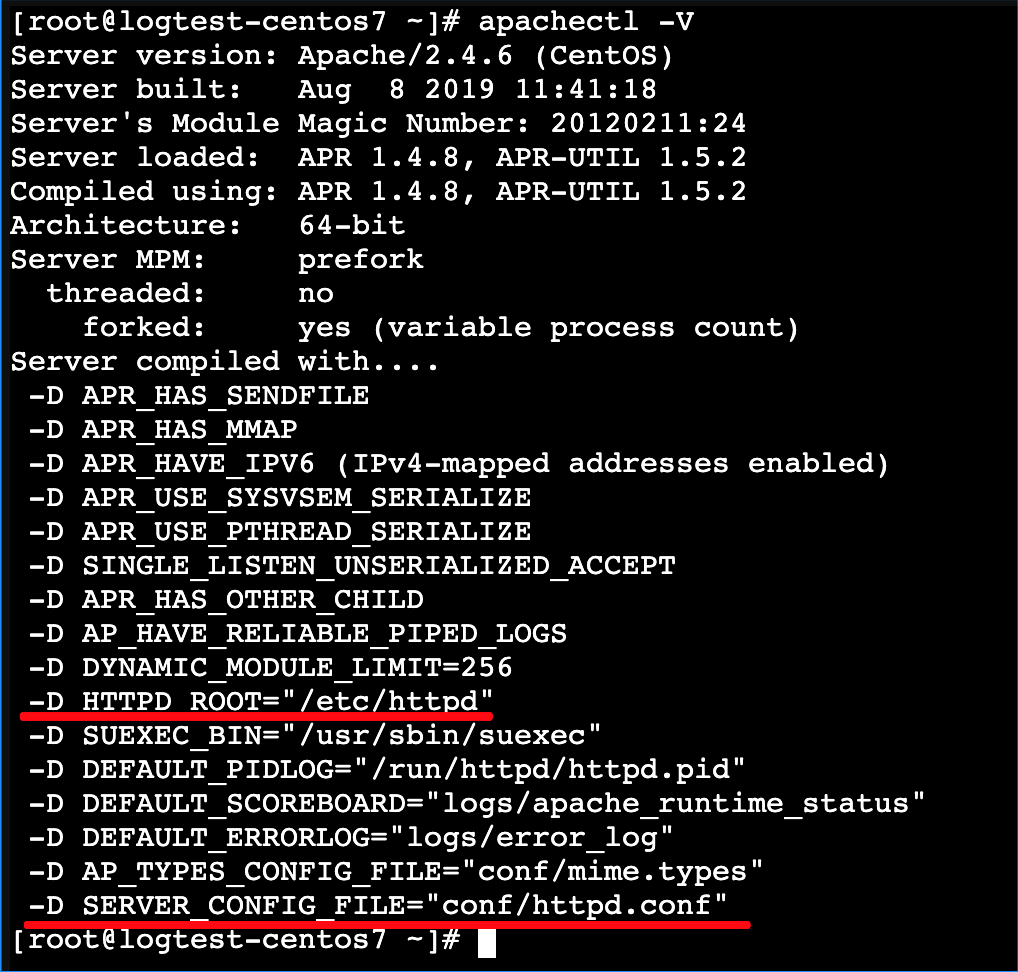
4、使用命令tar cvzf /tmp/weblog2019.tar.gz logs/\*即可打包logs/目录下的所有文件，最后将/tmp/weblog2019.tar.gz上传到对应的资产里面，系统会自动进行分析。

5、或者直接通过web登录weblogic控制台确定域（base\_doamin）、服务器名（AdminServer）以及日志文件名称（logs/access.log），然后进入相应的目录（如/root/Oracle/Middleware/user\_projects/domains/域/servers/服务器名/日志路径）下进行打包

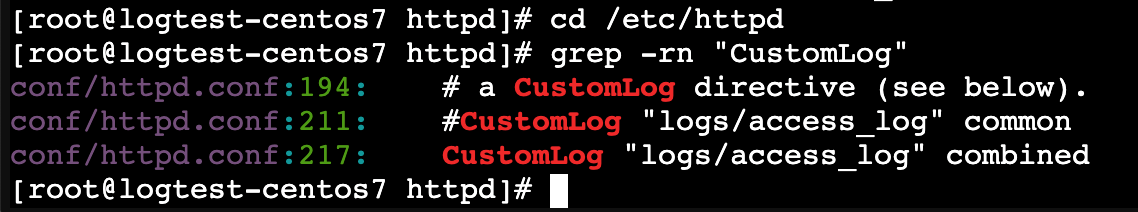


#### Apache

1、使用命令apachectl -V或httpd -V确定HTTPD\_ROOT与SERVER\_CONFIG\_FILE的值



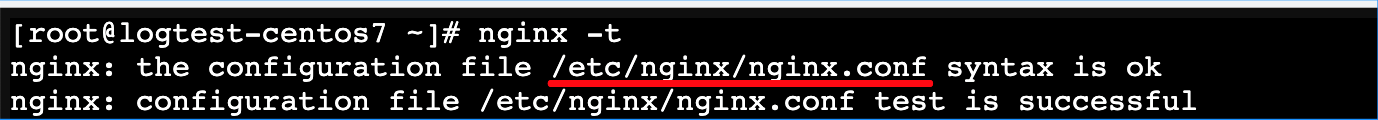
2、简单获取日志配置，进入HTTPD\_ROOT目录 （如/etc/httpd）后使用命令grep -rn "CustomLog"即可列出所有CustomLog配置项，将生效的日志文件（非注释符#开头的行）打包：使用命令tar cvzf /tmp/weblog2019.tar.gz logs/\*即可打包logs/目录下的所有文件，最后将/tmp/weblog2019.tar.gz上传到对应的资产里面，系统会自动进行分析。



3、手动查看配置文件。先查看/etc/httpd/conf.d/httpd.conf，检查所有Include、IncludeOptional指令所包含的文件、目录，查看是否有步骤2中没有搜索到的CustomLog路径，再次打包上传。

#### Nginx

1、使用命令nginx -t命令确定主配置文件路径



2、进入主配置目录/etc/nginx，并使用命令grep -rn "\_log"搜索所有日志配置行

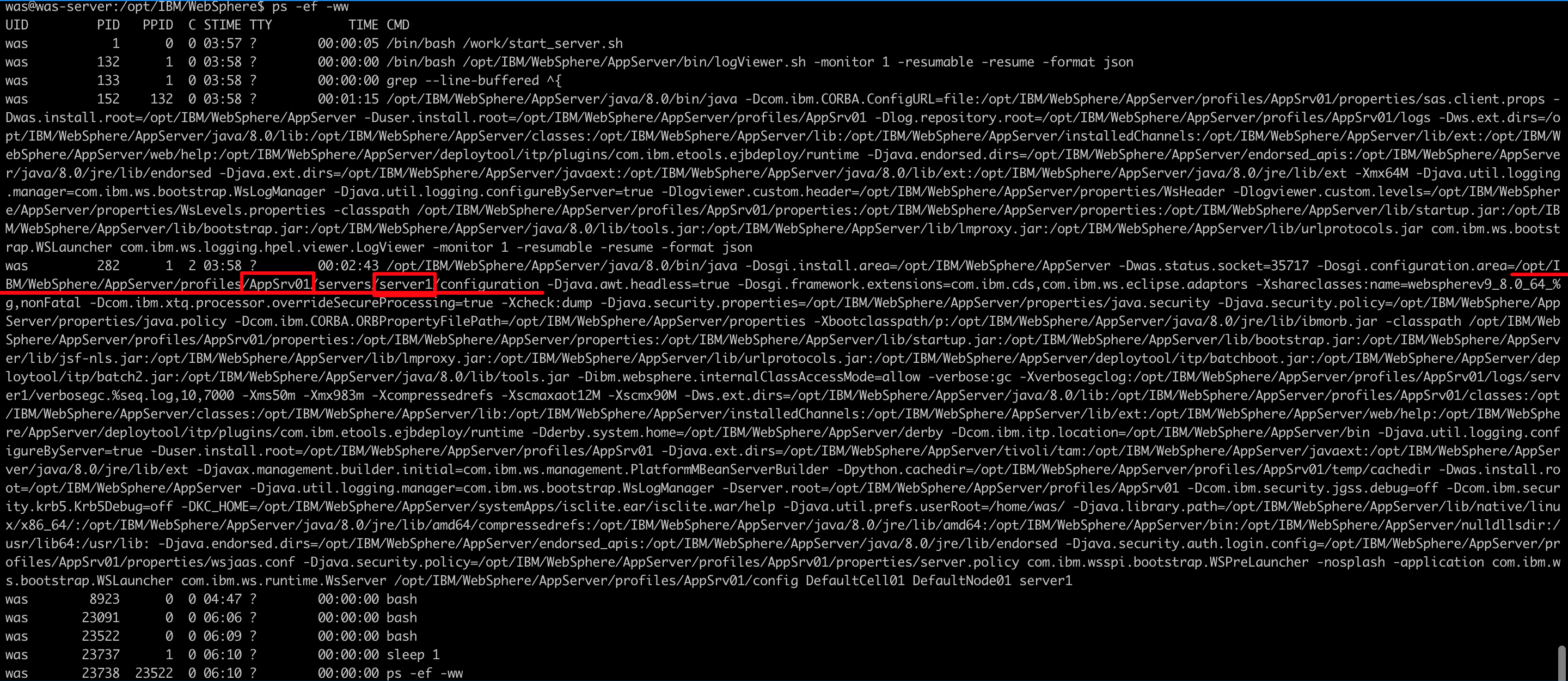


3、将生效的日志文件（非注释符#开头的行）打包：使用命令tar cvzf /tmp/weblog2019.tar.gz /var/log/nginx/\*即可打包/var/log/nginx/目录下的所有文件，最后将/tmp/weblog2019.tar.gz上传到对应的资产里面，系统会自动进行分析。

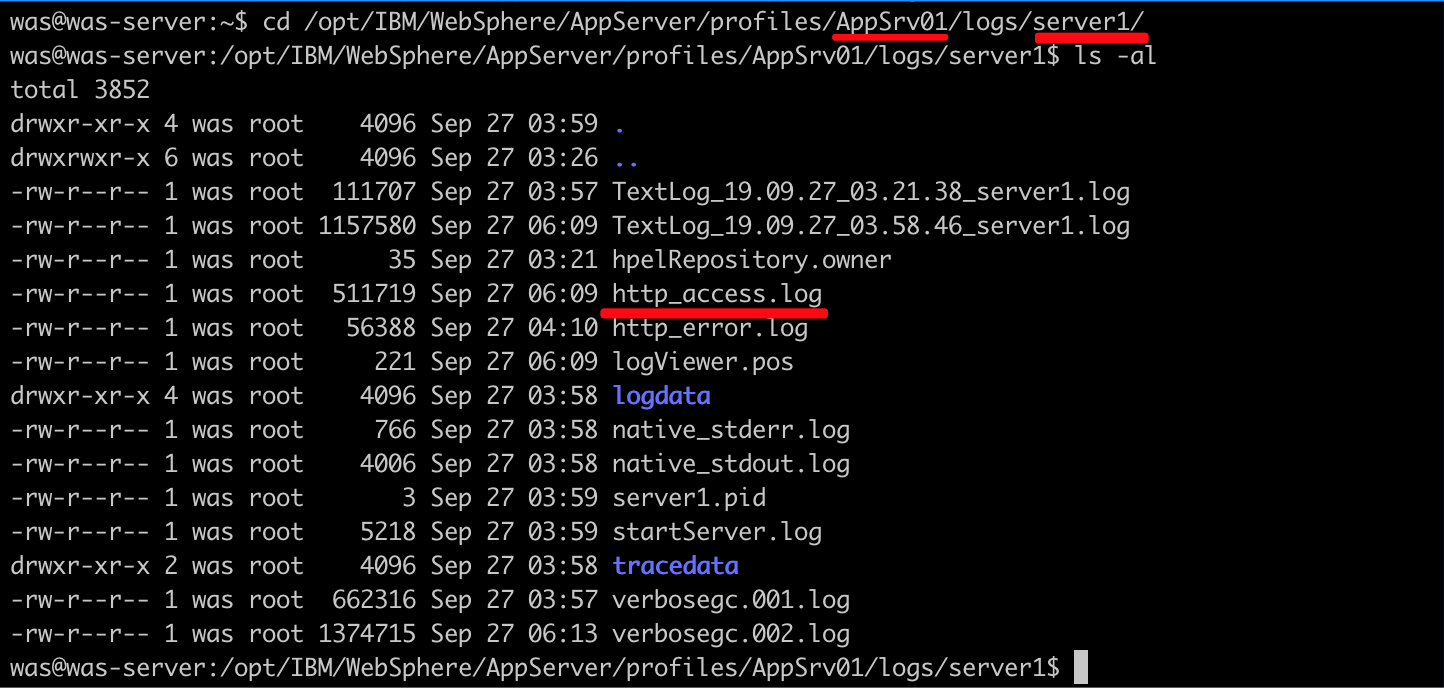
4、手动查看配置文件。从/etc/nginx/nginx.conf开始，递归检查所有include指令所包含的文件、目录，查看是否有步骤3中没有搜索到的log配置，再次打包上传。

#### Websphere

1、使用命令ps -ef -ww确定websphere的profiles路径以及server名



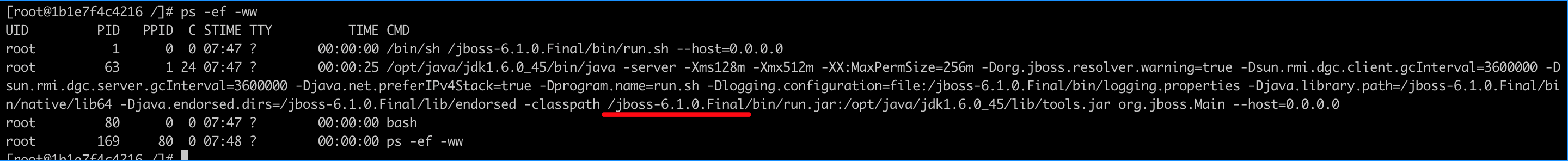
2、从profiles目录下的logs子目录中打包响应server名的日志



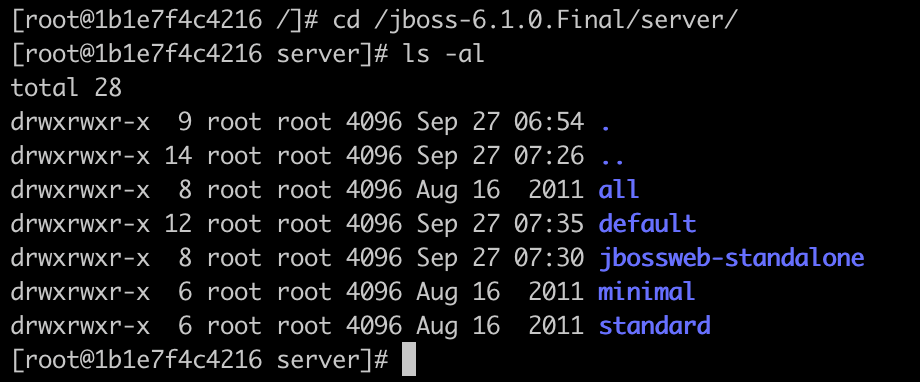
3、使用命令tar cvzf /tmp/weblog2019.tar.gz /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/\*即可打包该目录下的所有文件，最后将/tmp/weblog2019.tar.gz上传到对应的资产里面，系统会自动进行分析。

#### JBOSS

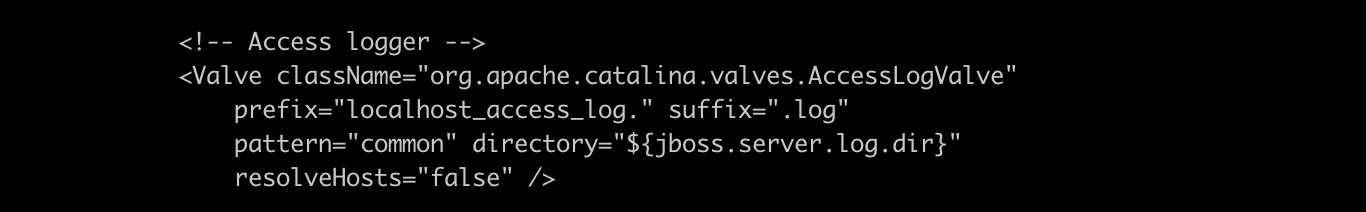
1、使用命令ps -ef -ww确定jboss根目录



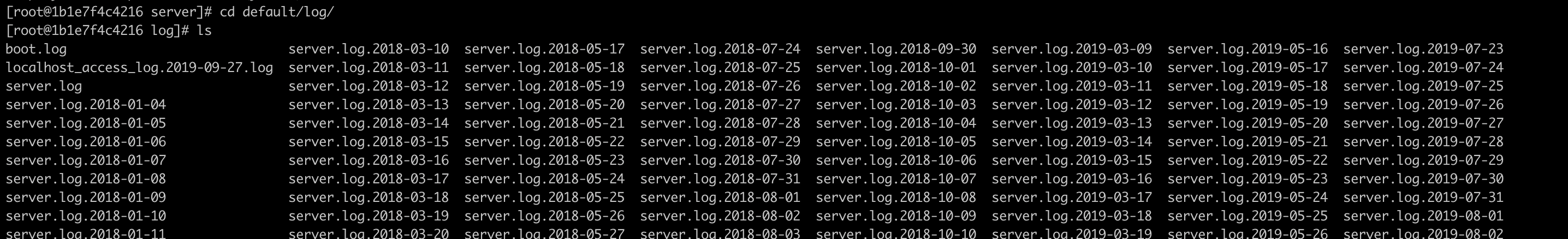
2、进入jboss的server目录，查看server配置。默认情况下运行的为default配置



3、使用命令cat default/deploy/jbossweb.sar/server.xml查看default的配置文件，如果Access logger配置项没有被注释，则说明存在访问日志



4、进入default/log目录即可找到对应日志



5、使用命令tar cvzf /tmp/weblog2019.tar.gz default/log/\*即可打包该目录下的所有文件，最后将/tmp/weblog2019.tar.gz上传到对应的资产里面，系统会自动进行分析。

## Windows服务器

#### IIS

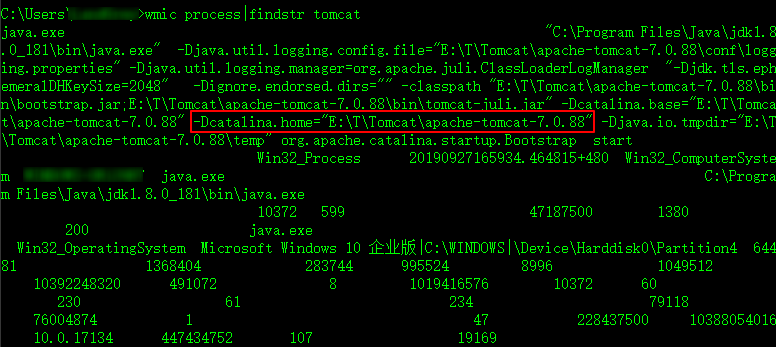
1、打开IIS管理区，右键xxx，如下图所示，查找日志文件路径



2、进入目录后利用压缩软件进行压缩，然后将文件传到对应的资产，系统进行自动分析

#### Tomcat

1、Tomcat日志一般可以通过wmic process|findstr tomcat命令寻找进程中存在的TOMCAT catalina.home路径

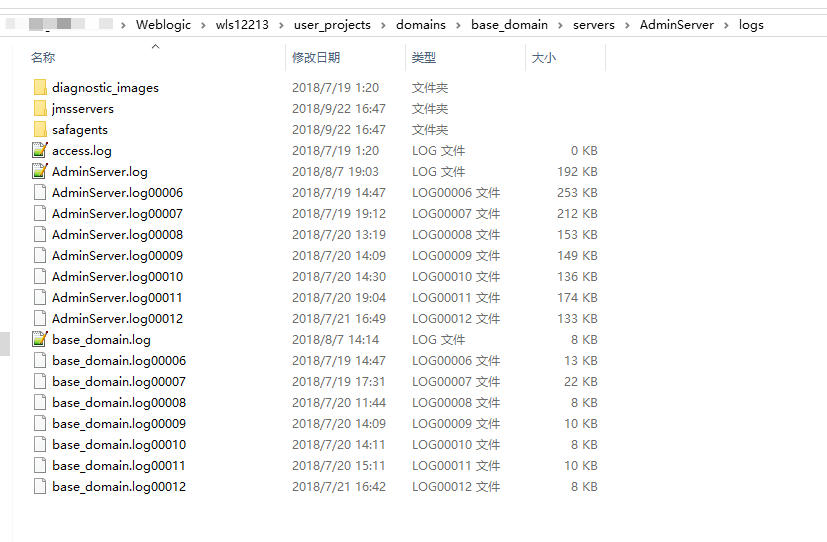


2、日志目录在catalina.home 下的 logs 目录，如 Tomcat\apache-tomcat-7.0.88\logs

以下web中间件寻找方式类似，先找到各中间件安装的Home路径后按描述寻找对应Logs位置

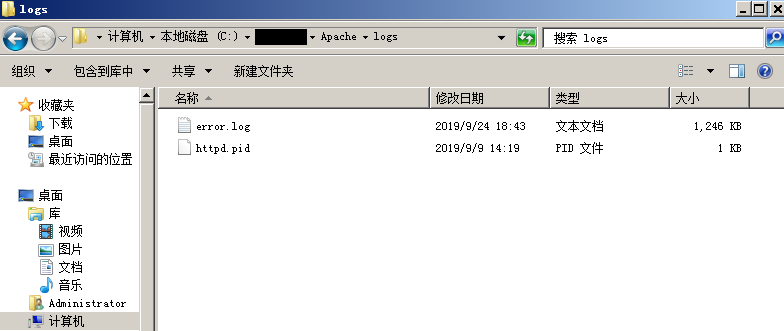
#### WebLogic

路径在 Weblogic\<wls12213>\user\_projects\domains\base\_domain\servers\AdminServer\logs



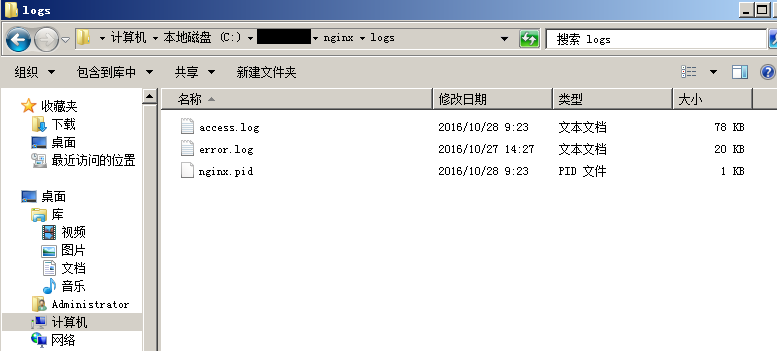
#### Apache

路径在 /Apache/logs



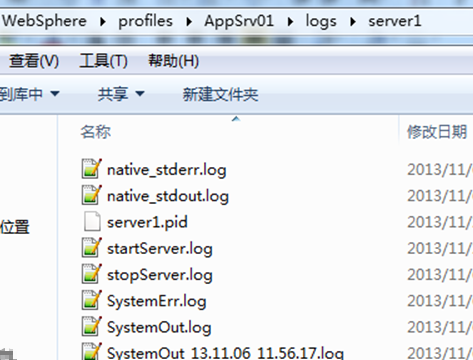
#### Nginx

路径在 /nginx/logs



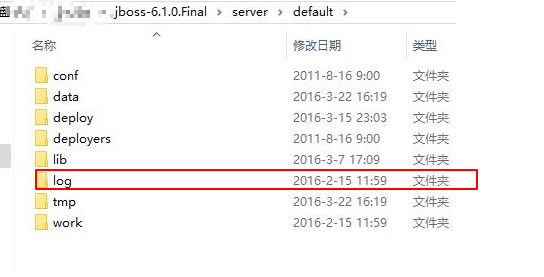
#### Websphere

日志路径如下WebSphere\<AppServer>\profiles\AppSrv01\logs\server1\



#### JBOSS

日志路径位置在JBOSS安装Home目录下的\server\default\log目录，其中目录所在位置也可在配置文件conf/log4j.xml实现修改



#### 总结

以上Logs文件找到后同Linux类似操作，用Winrar或7zip等压缩软件压缩成zip包后上传到对应资产进行分析。

# WebShell及暗链查杀工具

对网站所存在的WEBSHELL、暗链进程检查

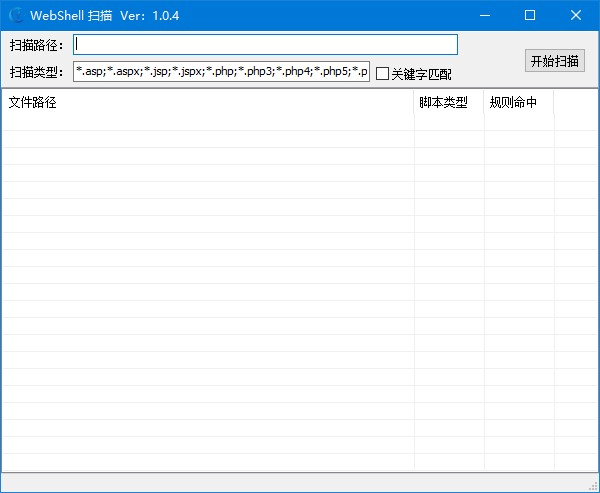
下载

### 操作指南

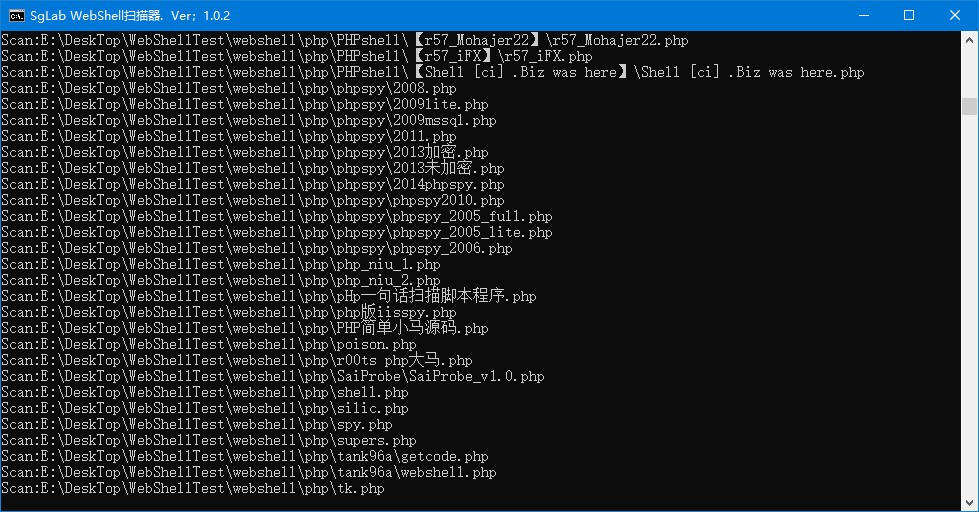
1、下载Webshell及暗链查杀工具

2、使用扫描

A．界面版（WebShell\_Scaner\_Gui.exe），点击扫描路径输入框，进行扫描路径选择，在确认要扫描的文件类型（文件扩展名，每个以; 英文分号隔开）及是否启用关键词匹配算法后，点击开始扫描即可。



B．命令行版（WebShell\_Scaner.exe），在Cmd命令行下运行（需管理员权限），使用参数-p C:WebHtml 来指定扫描目录，-e \*.asp;\*.php;\*.jsp来指定扫描的文件类型（文件扩展名，每个以; 英文分号隔开），加入-m 参数可开启字符串匹配算法。



3．扫描完成后结果会保存至程序同目录一个 数字时间戳.zip名字的压缩包。