在发生网页篡改、服务器被植入挖矿木马等安全攻击事件时，日志能协助进行安全事件还原，能尽快找到事件发生的时间、原因等，所以日志收集还是很重要的。本文整理了部分常见中间件、数据库、操作系统的日志收集方法。

# 一、中间件日志

## 1.1 weblogic

weblogic在安装结束后默认开启了日志记录功能，默认配置情况下，weblogic会有3种日志，分别是access log, Server log和domain log，WebLogic 8.x 和 9及以后的版本目录结构有所不同。

WebLogic 9及以后版本：

access log在 $MW\_HOME\user\_projects\domains\<domain\_name>\servers\<server\_name>\logs\access.log

server log在 $MW\_HOME\user\_projects\domains\<domain\_name>\servers\<server\_name>\logs\<server\_name>.log

domain log在 $MW\_HOME\user\_projects\domains\<domain\_name>\servers\<adminserver\_name>\logs\<domain\_name>.log

WebLogic 8.x 版本：

access log路径如下：$MW\_HOME\user\_projects\domains\<domain\_name>\<server\_name>\access.log

server log路径如下：$MW\_HOME\user\_projects\domains\<domain\_name>\<server\_name>\<server\_name>.log

domain log路径如下： $MW\_HOME\user\_projects\domains\<domain\_name>\<domain\_name>.log

其中:

$MW\_HOME是WebLogic的安装目录

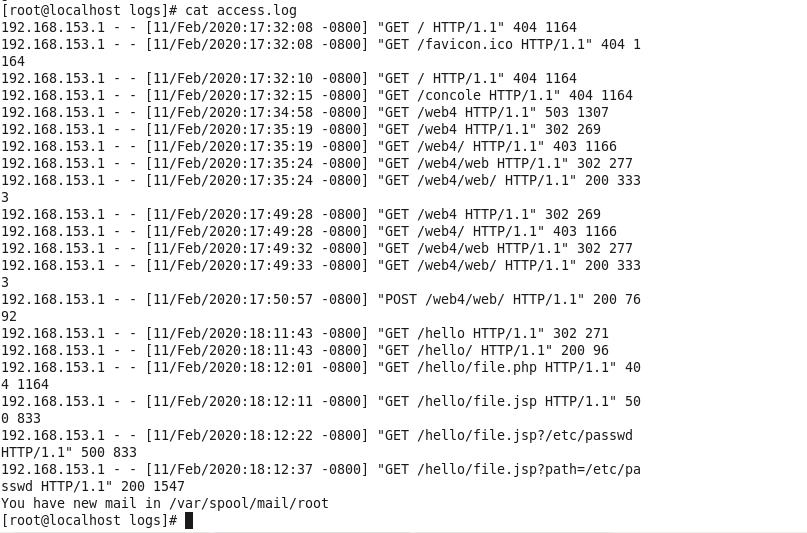
<domain\_name>是域的实际名称，是在创建域的时候指定的

<server\_name>是Server的实际名称，是在创建Server的时候指定的

<adminserver\_name>是Admin Server的实际名称，是在创建Admin Server的时候指定的。

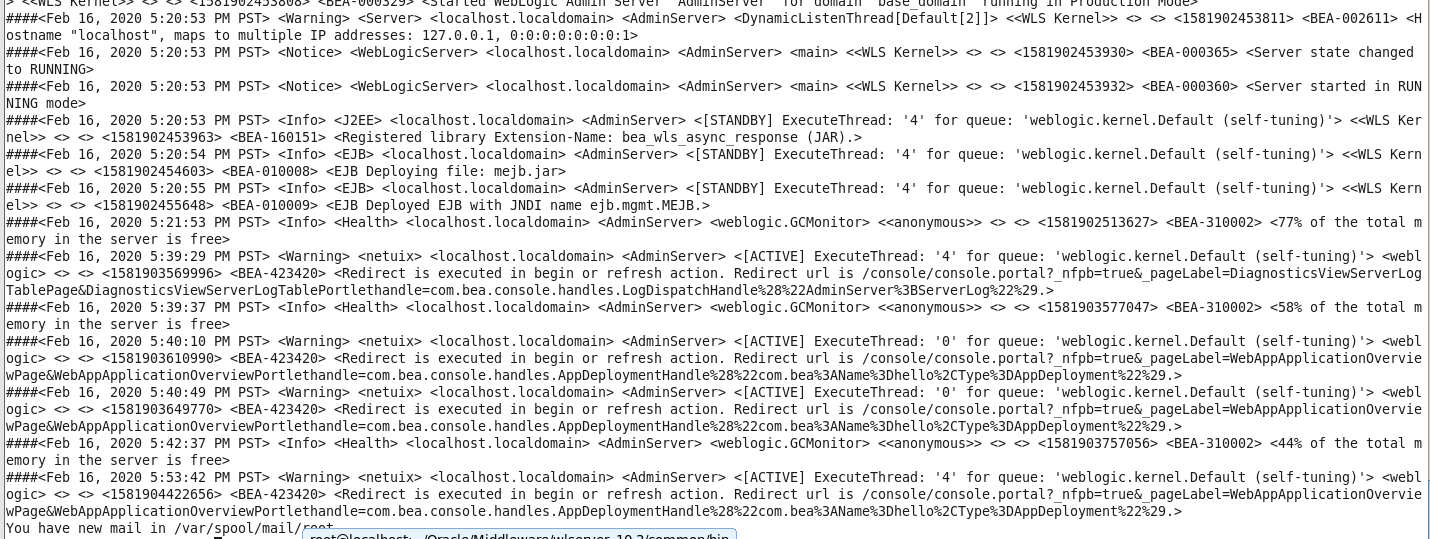
**access.log**

主要记录http请求，默认情况下日志记录处于启用状态，服务器将http请求保存在单独的日志文件中，日志格式如下，主要记录了http请求请求ip地址、请求时间、访问页面、响应状态等信息：



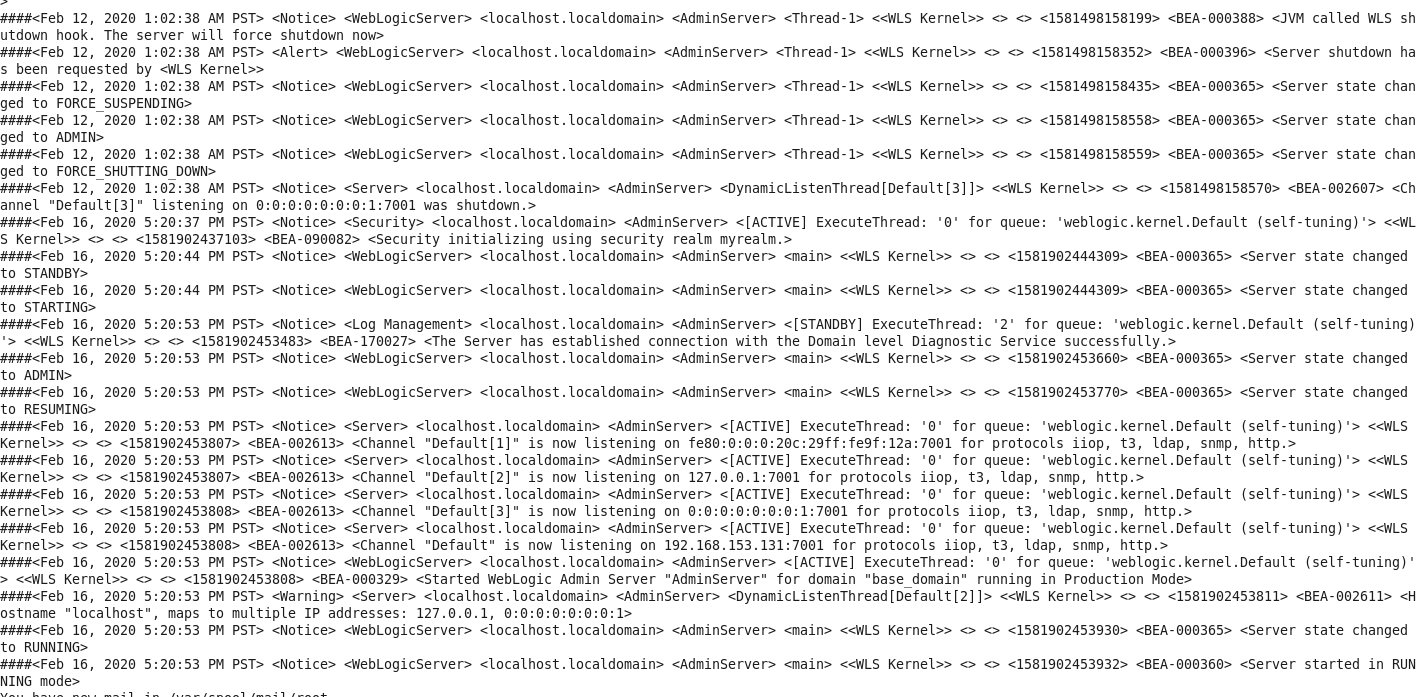
**server log**

主要用于服务器的一般日志记录，比如weblogic的启动、关闭、部署应用等相关记录，日志格式：依次为时间戳，严重程度，子系统，计算机名，服务器名，线程ID。其后消息正文中的行仅表示记录的一次例外并显示该例外的堆栈跟踪式如下：



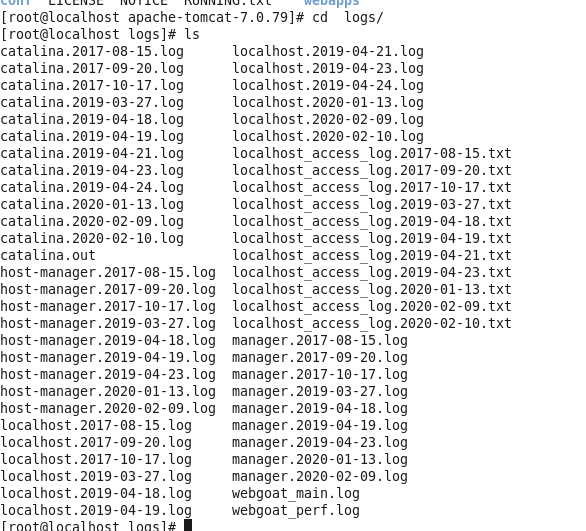
**domain log**

主要记录了一个domain的运行情况，一个domain中的各个weblogic server 可以把它们的一些信息（如：严重错误）发送到AdminServer上，AdminServer把这些信息传递到domain.log上

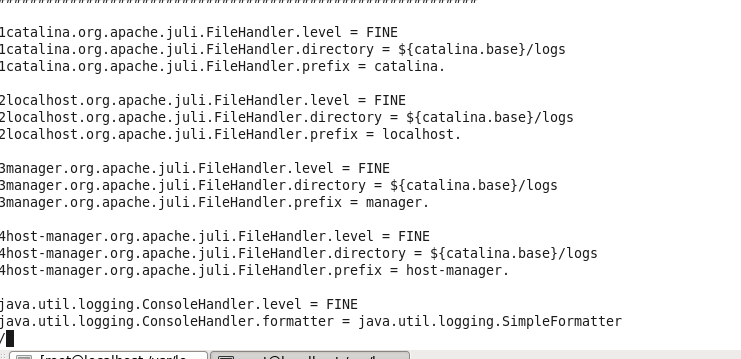


## 1.2 tomcat

tomcat日志默认路径：在安装目录下的logs文件夹下：



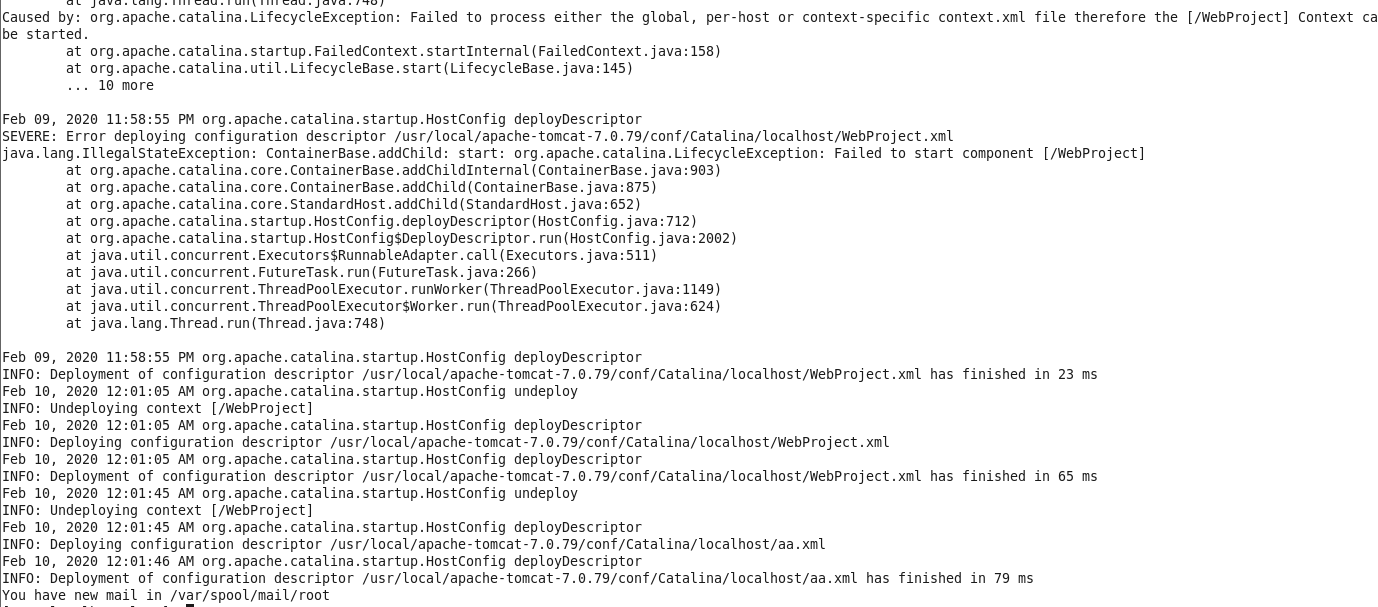
如果在安装中默认修改了日志存储位置，可在 conf/logging.properties文件中查看



tomcat日志一般分为catalina.out、localhost、manager、localhost\_access\_log4种格式日志。

**catalina.out**

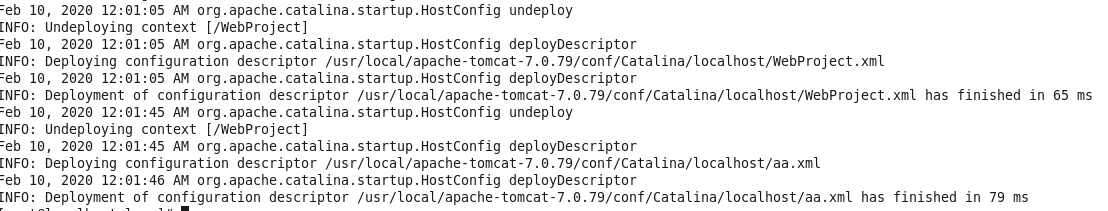
运行中的日志，主要记录运行中产生的一些信息，尤其是一些异常错误日志信息，内容如下：



**catalina.Y-M-D.log**

是tomcat自己运行的一些日志，这些日志还会输出到catalina.out，

但是应用向console输出的日志不会输出到catalina.{yyyy-MM-dd}.log



**localhost.Y-M-D.log**

程序异常没有被捕获的时候抛出的地方，

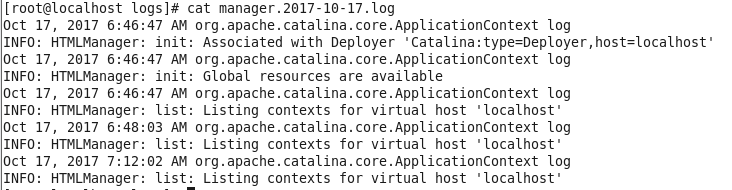
Tomcat下内部代码丢出的日志（jsp页面内部错误的异常，org.apache.jasper.runtime.HttpJspBase.service类丢出的，日志信息就在该文件！）

应用初始化(listener, filter, servlet)未处理的异常最后被tomcat捕获而输出的日志，而这些未处理异常最终会导致应用无法启动。



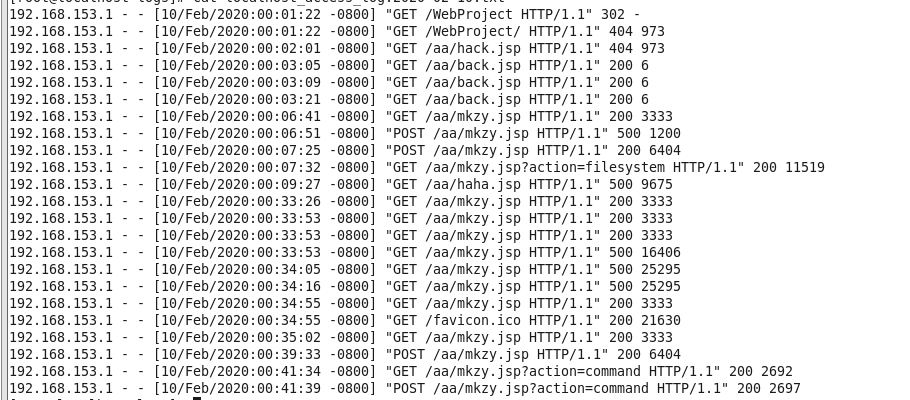
**manager.Y-M-D.log**

管理日志

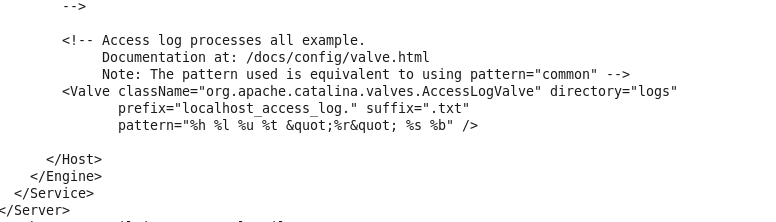


**localhost\_access\_log**

主要记录访问日志信息，记录访问的的时间、ip地址等信息，也是应急中经常用到的日志信息



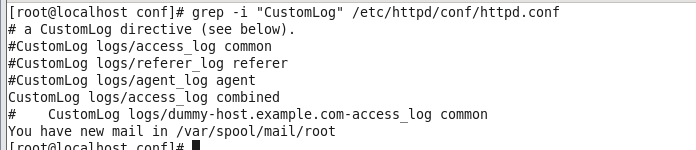
此部分日志可通过查看server.xml文件的如下内容，来确定是否启用了访问日志记录



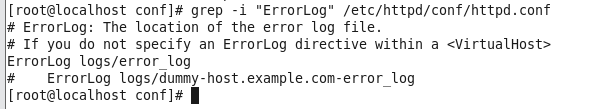
## 1.3apache

apache日志一般分为access\_log和error\_log两种，通过查看httpd.conf文件查看apache日志路径：

grep -i "CustomLog" /etc/httpd/conf/httpd.conf

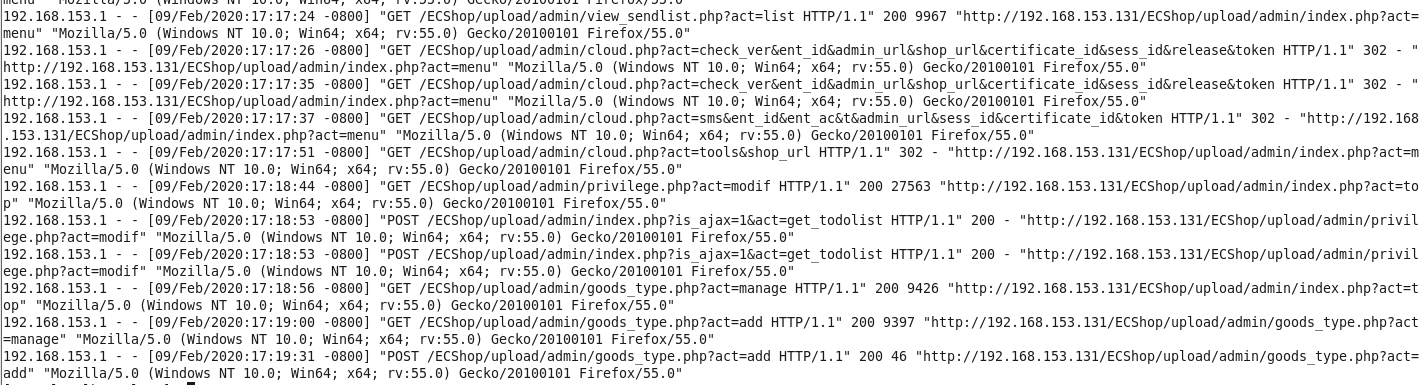


grep -i "ErrorLog" /etc/httpd/conf/httpd.conf



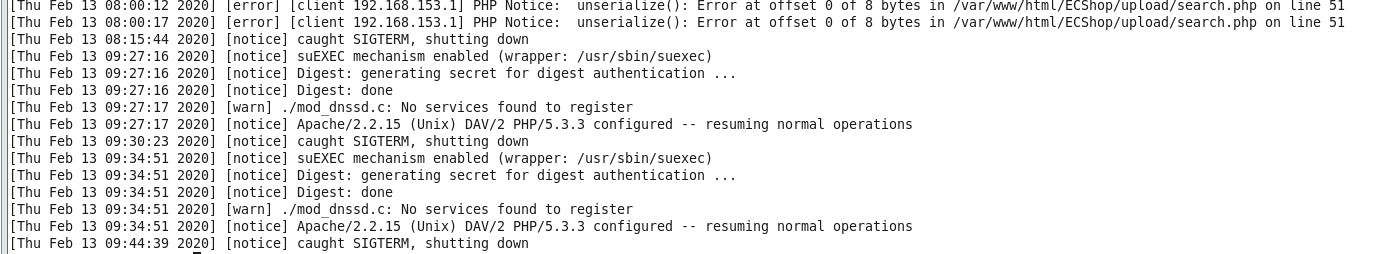
**access\_log**

访问日志,记录所有对apache服务器进行请求的访问



**error\_log**

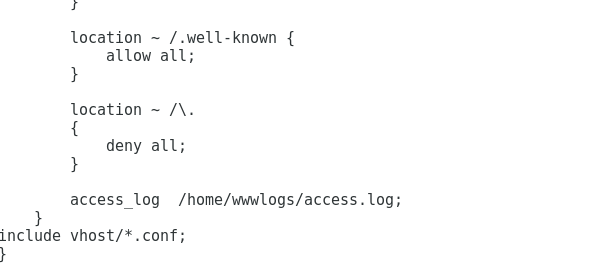
错误日志,记录下任何错误的处理请求，通常服务器出现什么错误，可对该日志进行查看



## 1.4nginx

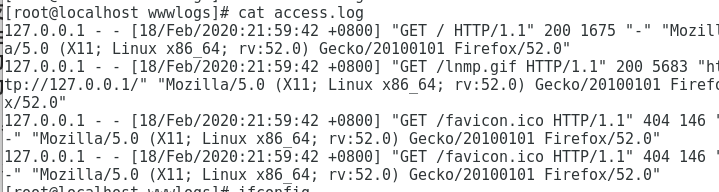
nginx的日志主要分为access.log、error.log两种，可通过查看nginx.conf文件来查找相关日志路径，如下图





**access.log**

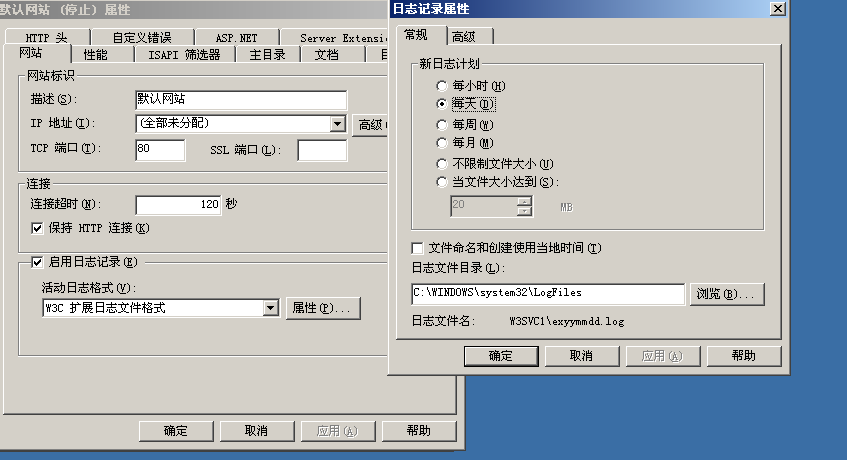
主要记录访问日志，记录访问客户端ip地址、访问时间、访问页面等信息



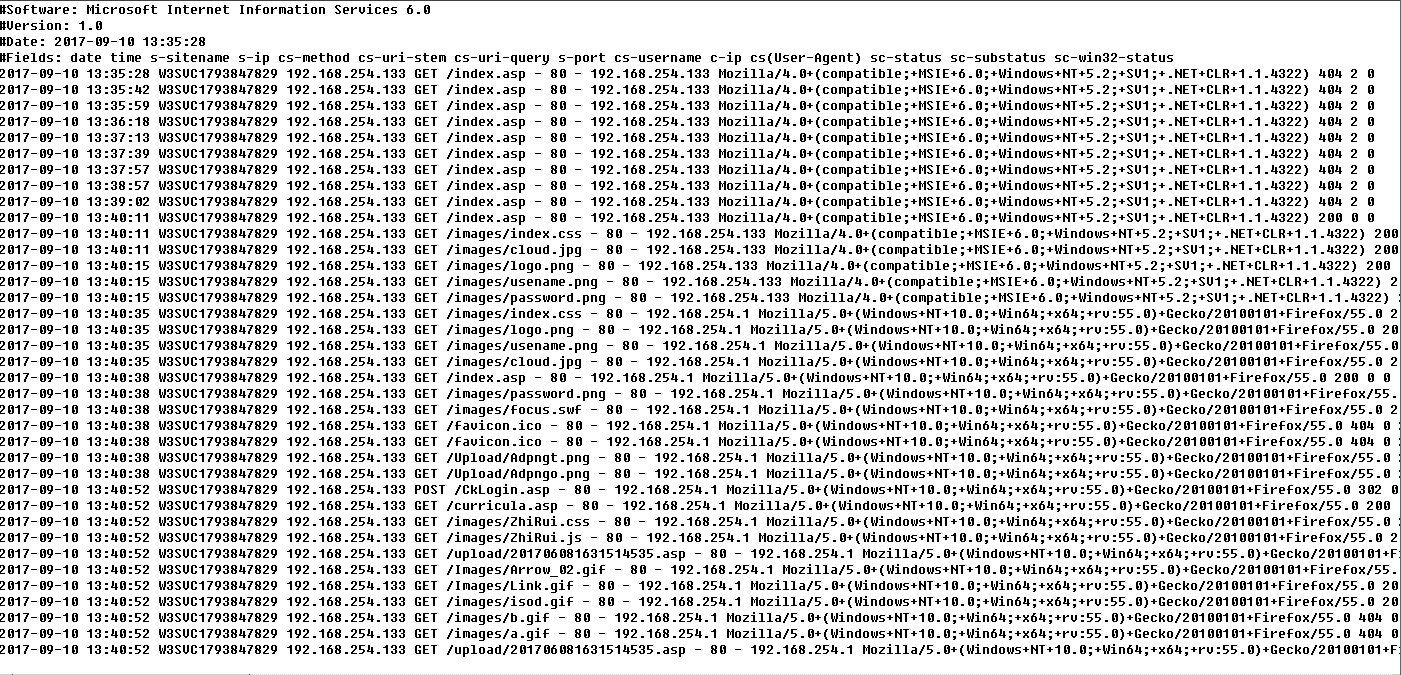
error.log,主要记录一些错误信息。

## 1.5 iis

查看日志文件位置：



打开文件夹下其中一个名为ex170910.log，日志内容具体如下，包括访问域名时间、ip、访问url等信息。

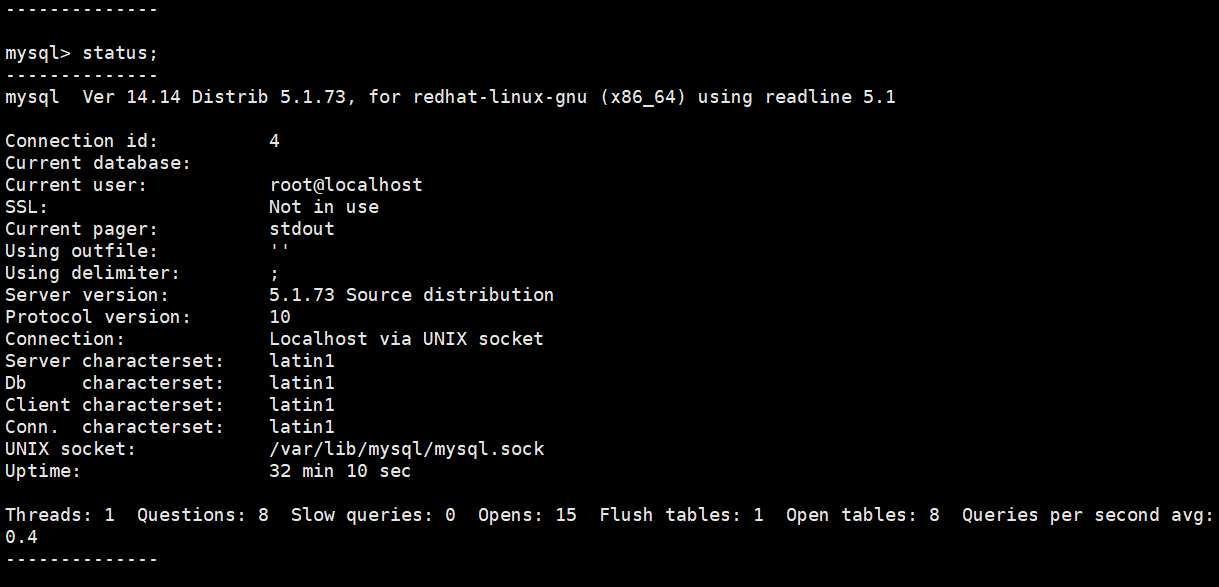


# 二、数据库日志

本次主要介绍关于mysql、sqlserver、oracle的一些日志信息。

## 2.1 mysql：

status：查看当前数据库状态



mysql的日志主要分为以下几种：

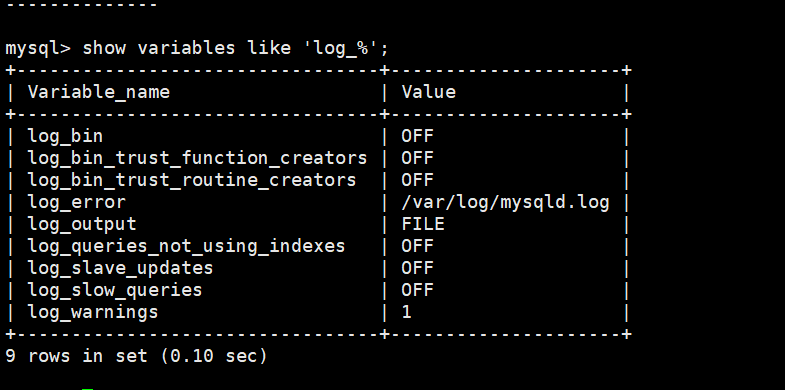
 Error Log：记录Mysql运行过程中的Error、Warning、Note等信息，系统出错或者某条记录出问题可以查看Error日志；

Genaral Query Log：记录mysql的日常日志，包括查询、修改、更新等的每条sql；

Binary Log ：二进制日志，包含一些事件，这些事件描述了数据库的改动，如建表、数据改动等，主要用于备份恢复、回滚操作等；

Slow Query Log\*：记录Mysql 慢查询的日志；

show variables like 'log\_%';



可见mysql默认只是开启了错误日志，错误日志内容如下：

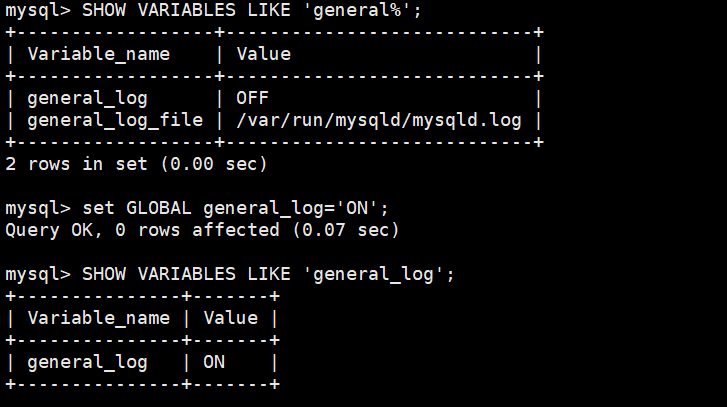


此处重点分析Genaral Query Log，也是应急中经常会查看到的，其他日志类型可查看大牛已经整理好的详细笔记，链接如下：<https://www.jianshu.com/p/db19a1d384bc>

通过开启日志，来记录所有查询和执行的sql语句：

GLOBAL general\_log='ON'；

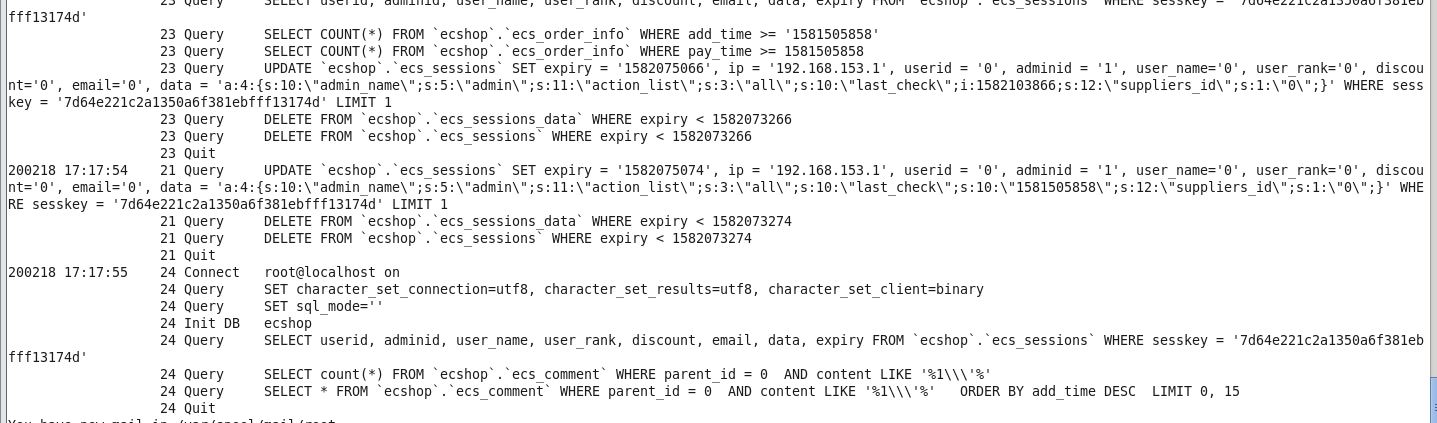
SHOW VARIABLES LIKE 'general%';



general\_log：日志功能是否开启，默认关闭OFF

general\_log\_file：日志文件保存位置

到对应路径下查看日志内容如下，会记录当前针对数据库所做的所有操作



## 2.2 sqlserver：

SQL Server日志记录了完整的SQL Server数据库运行的状态信息，并以消息的形式记录系统级、应用级操作。

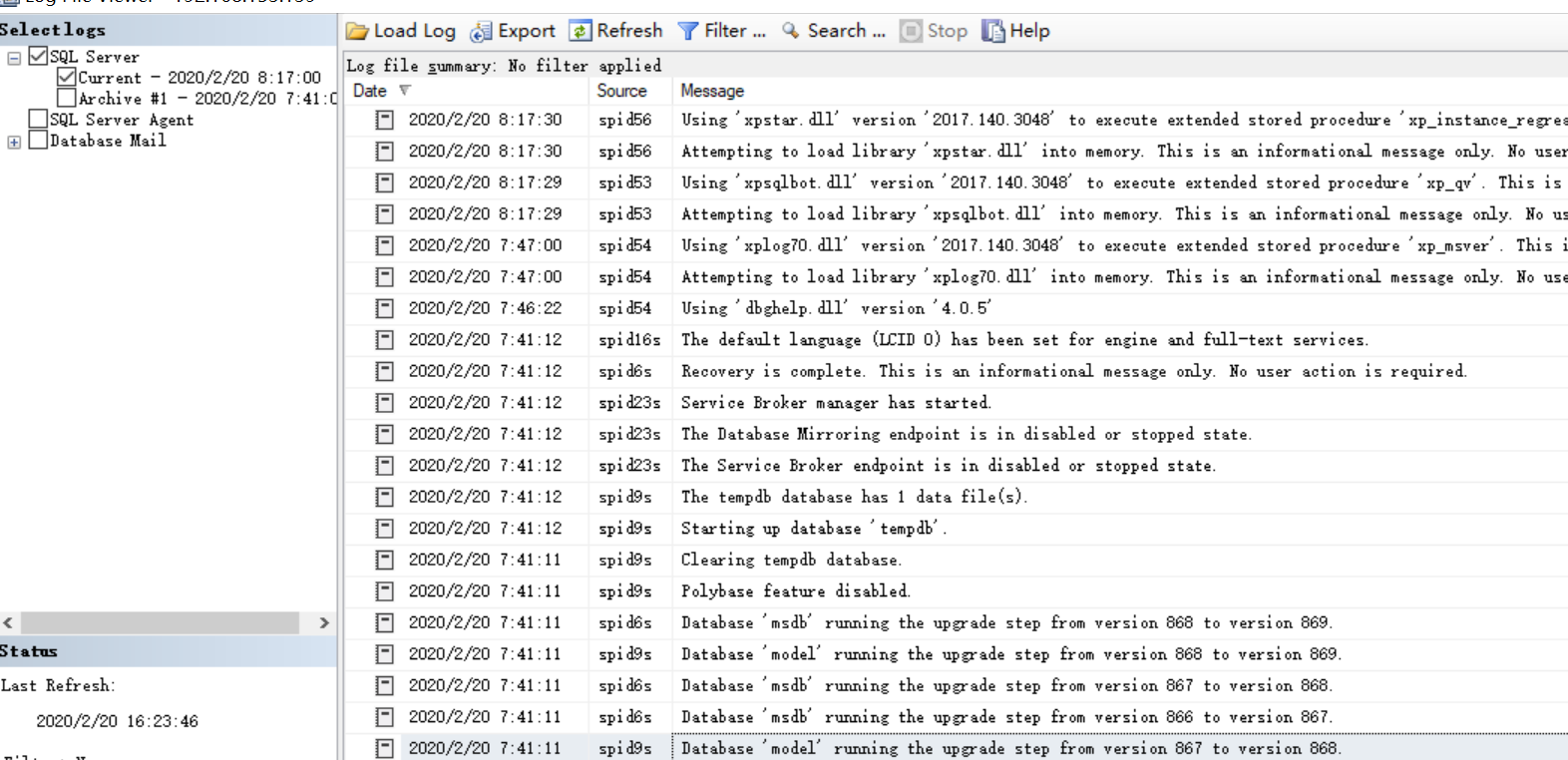
可以使用 SQL Server Management Studio 中的日志文件查看器来访问有关在以下日志中捕获的错误和事件的信息：

SQL Server Management Studio连接sqlserver数据库，查看与常规 SQL Server 活动相关的日志。

1. 在对象资源管理器中，展开 **“管理”** 。
2. 执行下列任一操作：

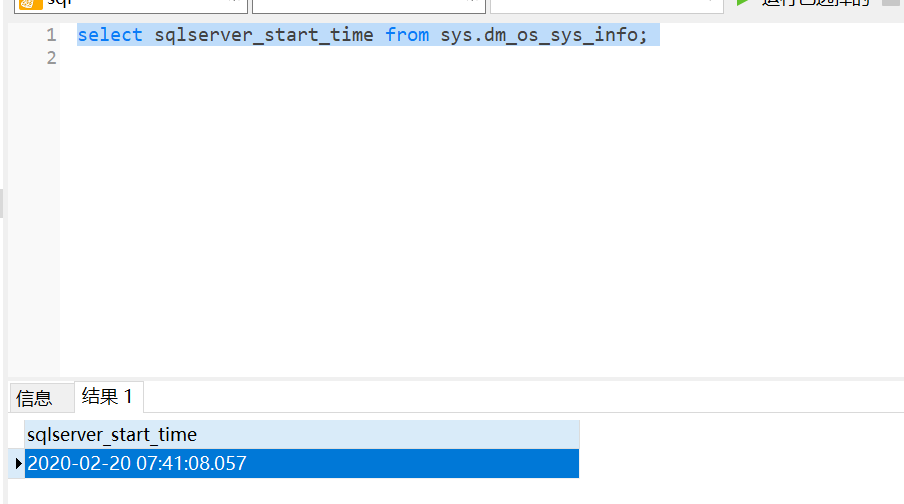
1.右键单击“SQL Server 日志” ，指向“查看” ，然后单击“SQL Server 日志” 或“SQL Server 和 Windows 日志” 。

2.展开“SQL Server 日志” ，右键单击任何日志文件，然后单击“查看 SQL Server 日志” 。 还可以双击任何日志文件，日志格式如下：



查询最近一次启动sqlserver时间：

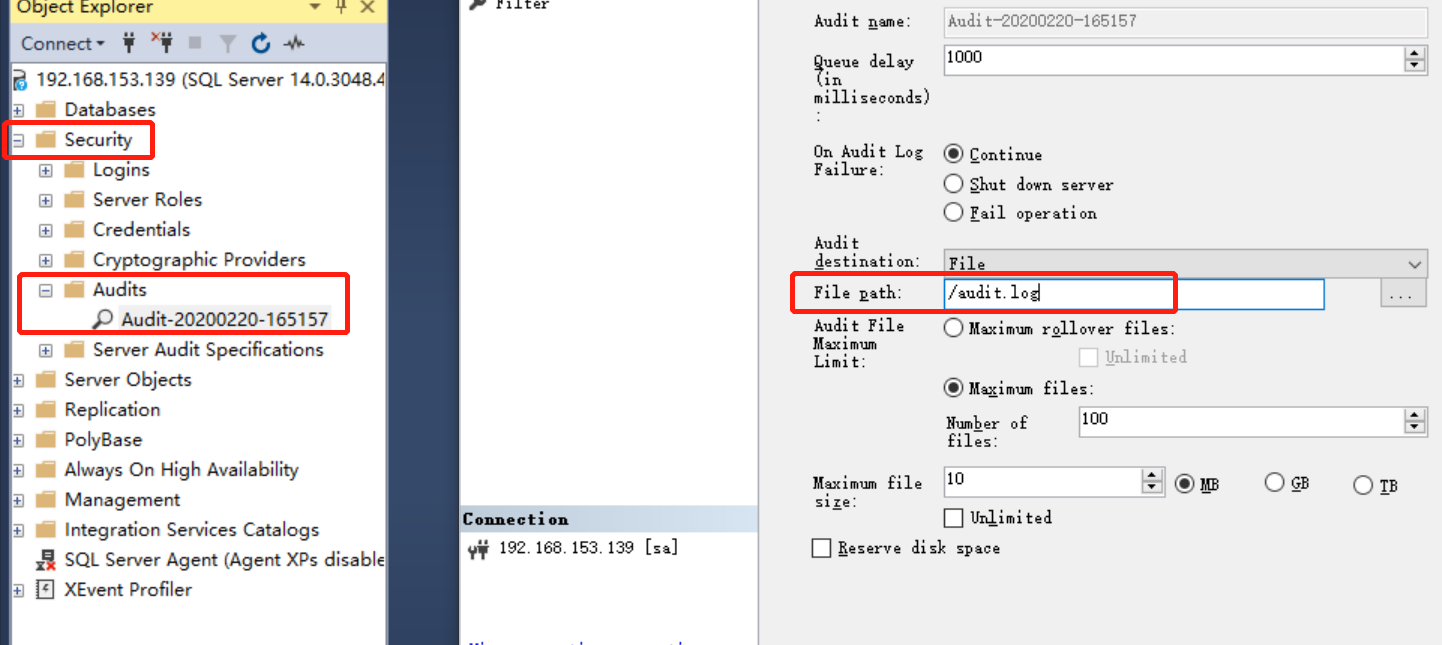
select sqlserver\_start\_time from sys.dm\_os\_sys\_info;



历史sql记录查询：SQL Server并没有这样的实现，只有sys.dm\_exec\_query\_stats缓存了一部分 (sql server服务开启后执行的语句，某些不被缓存执行计划的语句并不记录)。

这个视图主要是对执行计划的统计，包含消耗成本，运行次数等等，并没有session，user，每次被执行的时间等信息：

启动sql server 审计功能，会记录所有的操作记录，可以通过查看 Audits来查看日志的存储路径

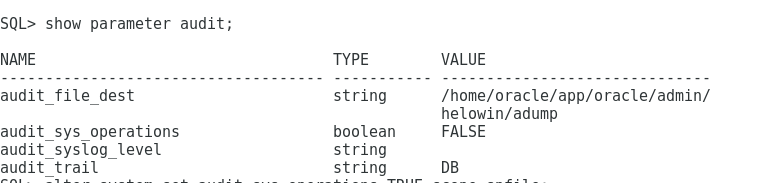


Sqlserver开启日志审计功能可参考：https://blog.51cto.com/gaowenlong/1908381

## 2.3 oracle：

Oracle日志文件分为两种：重做日志文件（redo log file）、归档日志文件，其中重做日志文件主要记录了数据库的操作过程，可以在进行数据库恢复时，将重做日志文件在还原的数据库上进行执行，以达到数据库的最新状态。

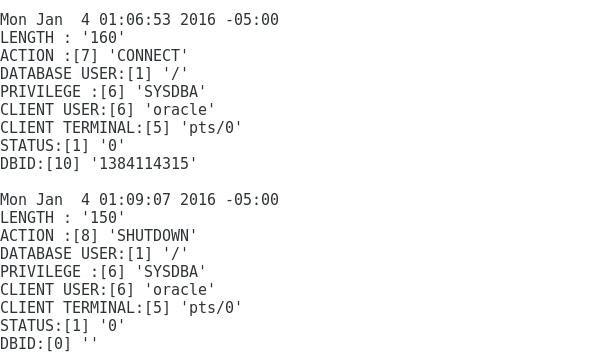
Oracle数据库默认只是对数据库的登录情况记录，但是不对数据库的查询记录统计，可通过show parameter audit，查看审计功能是否开启，若audit\_sys\_operations值为DB。



None：是默认值，不做审计；

DB：将audit trail 记录在数据库的审计相关表中，如aud$，审计的结果只有连接信息；

audit\_file\_dest为存放的日志路径，可查看adump下相关文件，内容如下：



DB,Extended：这样审计结果里面除了连接信息还包含了当时执行的具体语句；

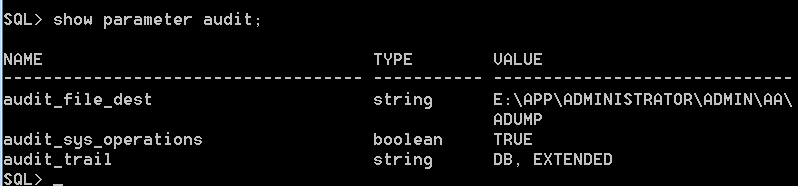
OS：将audit trail 记录在操作系统文件中，文件名由audit\_file\_dest参数指定；

开启审计功能：

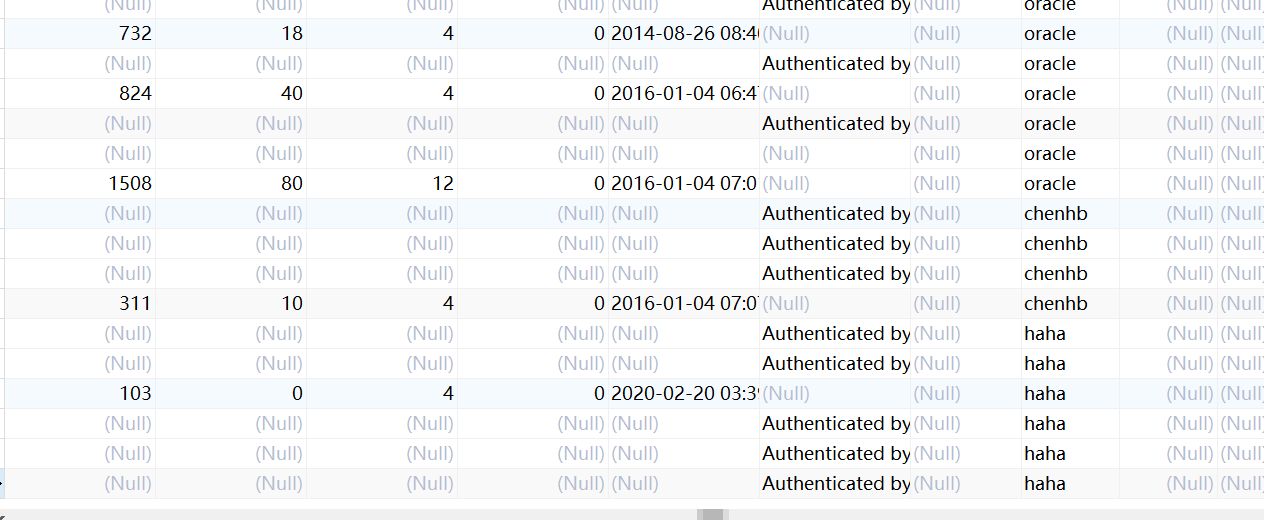
alter system set audit\_sys\_operations=TRUE scope=spfile;

alter system set audit\_trail=db,extended scope=spfile;

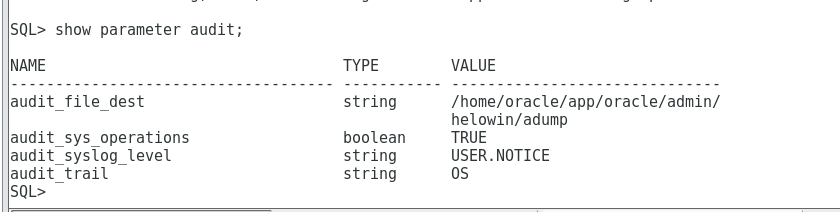
重启实例即可



开启后会把审计内容记录到sys 库的AUD$表中



修改将日志文件记录在操作系统中:alter system set audit\_trail='OS' scope=spfile;



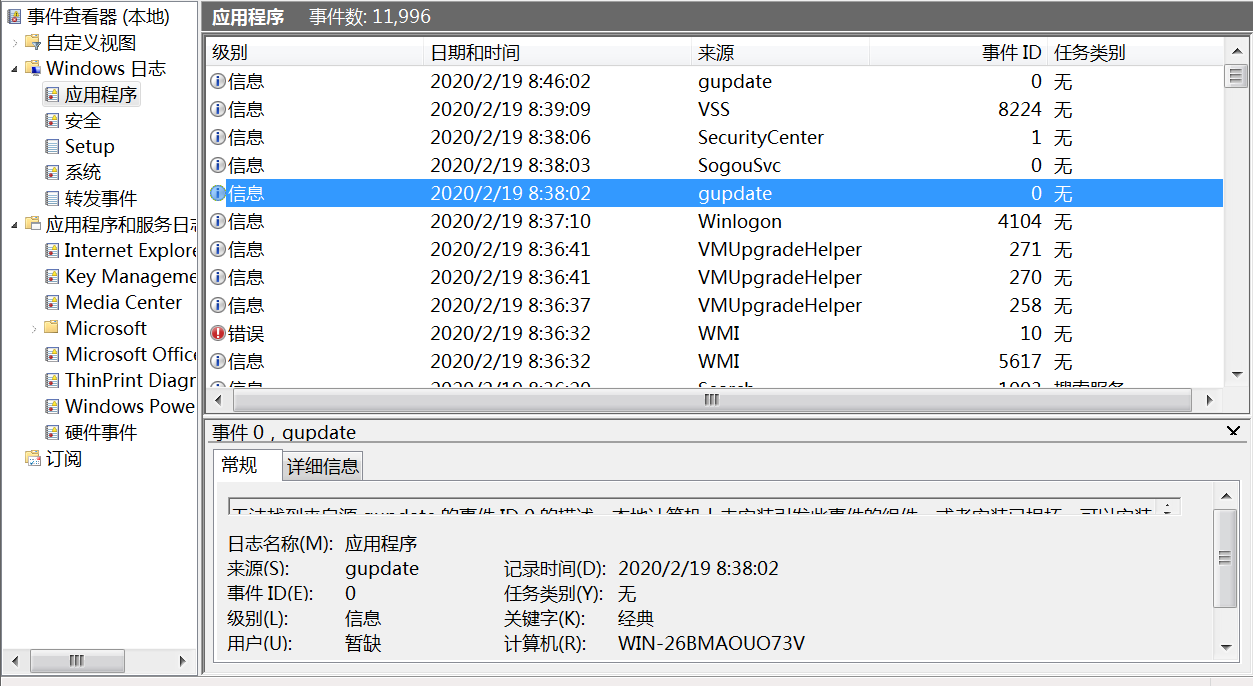
Audit\_file\_dest即为日志保存的具体路径。

关于日志的详细配置可以参考：<http://blog.itpub.net/31397003/viewspace-2145164/>

# 三、操作系统日志

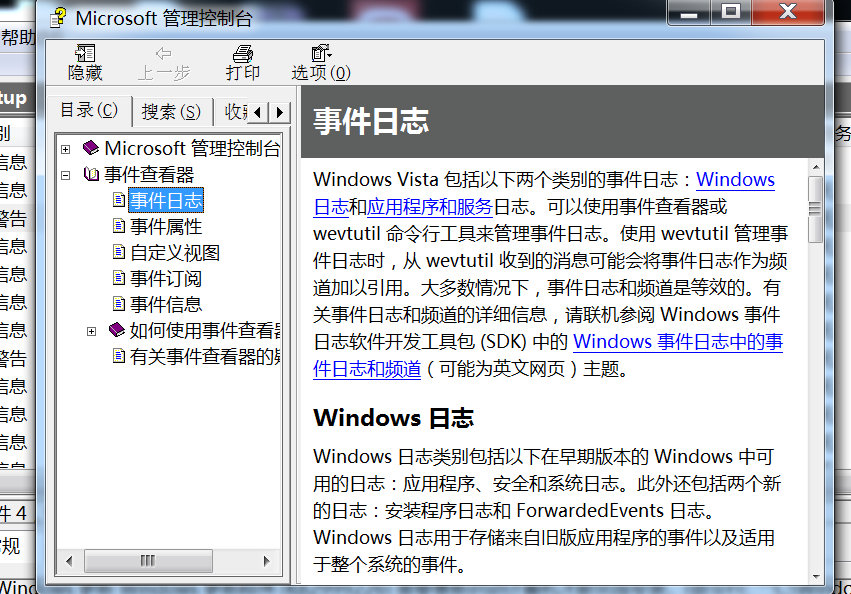
## 3.1 windows日志

查看windows日志方法：开始->运行->输入eventvwr



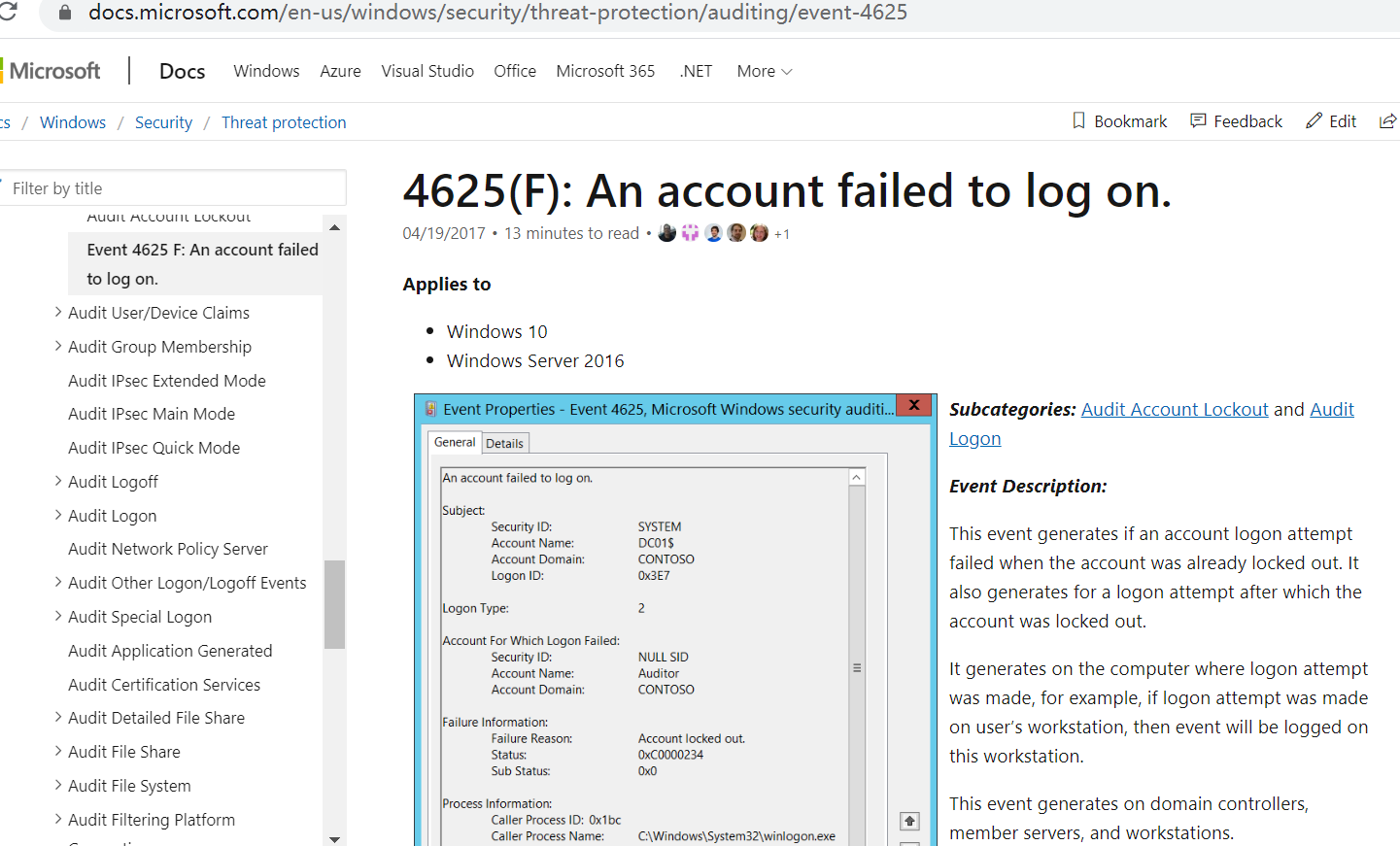
|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 事件类型 | 描述 | 文件名 |
| Windows日志 | 系统 | 系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。系统组件所记录的事件类型由 Windows 预先确定。 | %SystemRoot%\System32\Winevt\Logs\System.evtx |
| 安全 | 安全日志包含诸如有效和无效的登录尝试等事件，以及与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理员可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，则对系统的登录尝试将记录在安全日志中。 | %SystemRoot%\System32\Winevt\Logs\Security.evtx |
| 应用程序 | 应用程序日志包含由应用程序或程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。程序开发人员决定记录哪些事件。 | %SystemRoot%\System32\Winevt\Logs\Application.evtx |
| 转发事件 | ForwardedEvents 日志用于存储从远程计算机收集的事件。若要从远程计算机收集事件，必须创建事件订阅。 | %SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx |

可通过查看帮助手册进一步获取日志信息：

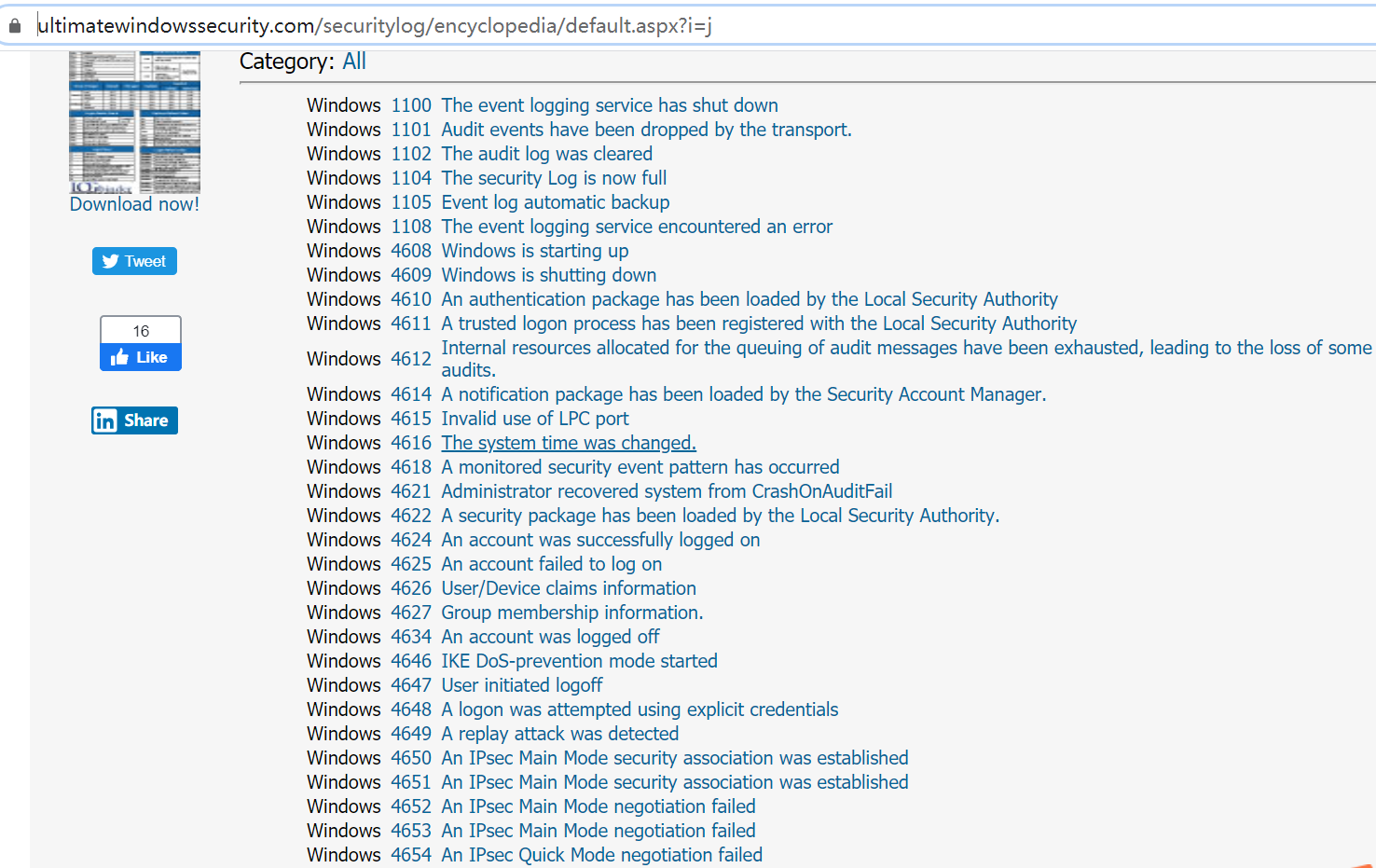


Windows的日志以事件id来标识具体发生的动作行为，可通过微软查询具体id对应的操作：

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625>



也可访问如下网站查看：<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j>



之前也已经有大牛写过关于windows日志查看内容，可参考如下链接：

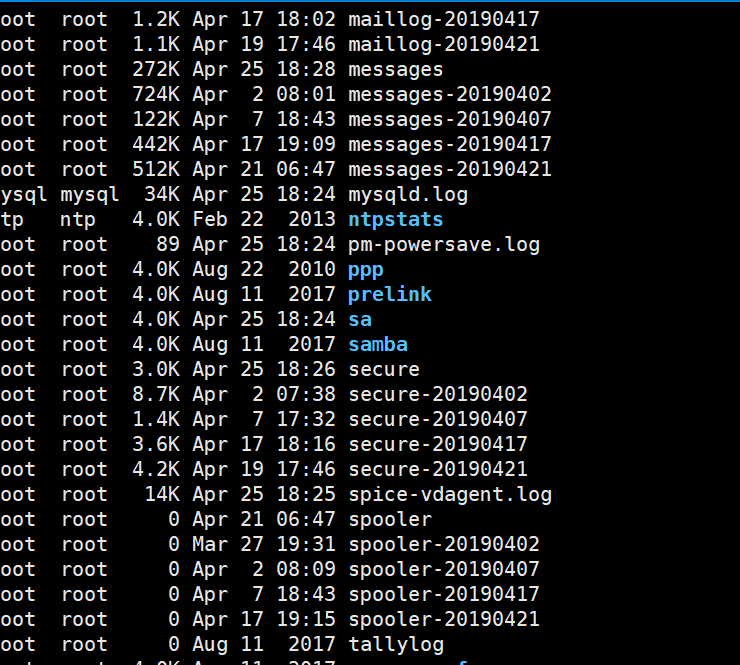
https://www.freebuf.com/vuls/175560.html

## 3.2 linux日志

通过查看 /etc/rsyslog.conf ，可查看相关系统日志配置情况。



linux系统日志一般存放在/var/log/目录下。



/var/log/messages：记录Linux内核消息及各种应用程序的公共日志信息，包括启动、IO错误、网络错误、程序故障等。对于未使用独立日志文件的应用程序或服务，一般都可以从该文件获得相关的事件记录信息。

/var/log/cron：记录crond计划任务产生的事件消息。

/varlog/dmesg：记录Linux系统在引导过程中的各种事件信息。

/var/log/maillog：记录进入或发出系统的电子邮件活动。

/var/log/lastlog：最近几次成功登录事件和最后一次不成功登录事件。

/var/log/rpmpkgs：记录系统中安装各rpm包列表信息。

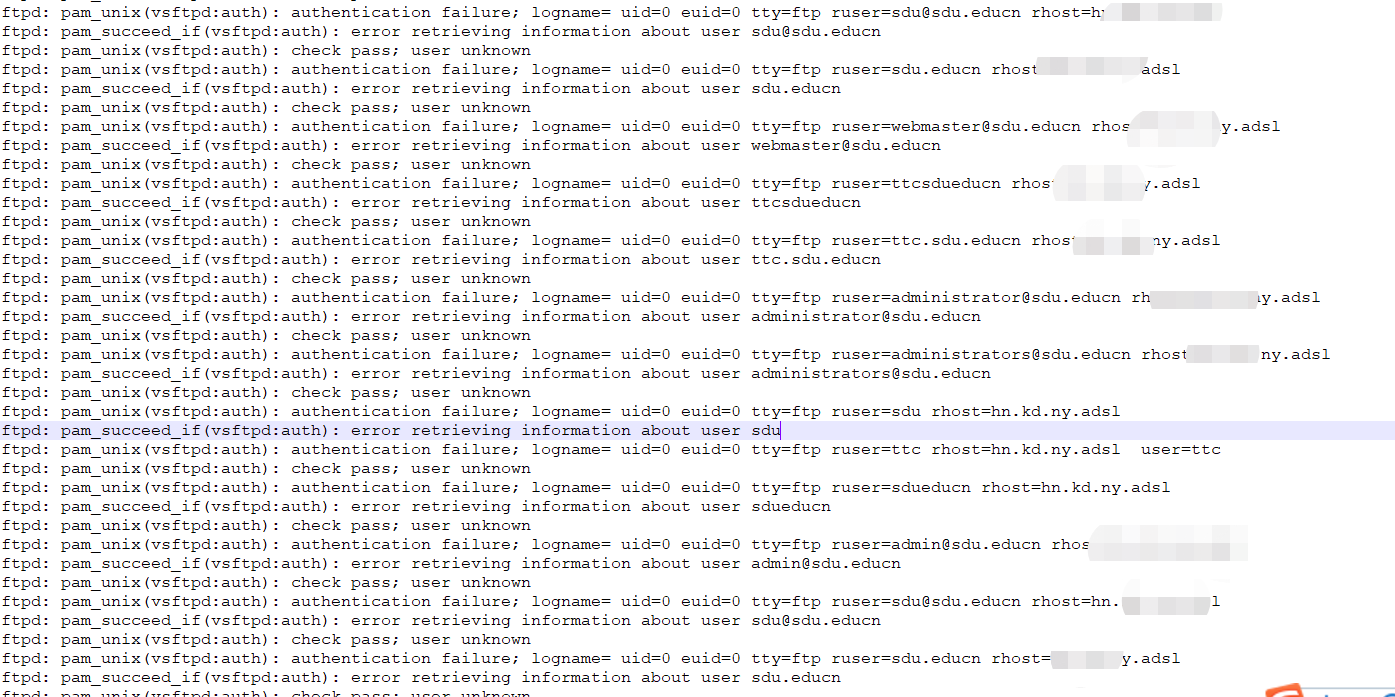
/var/log/secure：记录用户登录认证过程中的事件信息。

/var/log/wtmp：记录每个用户登录、注销及系统启动和停机事件。

/var/log/utmp：记录当前登录的每个用户的详细信息

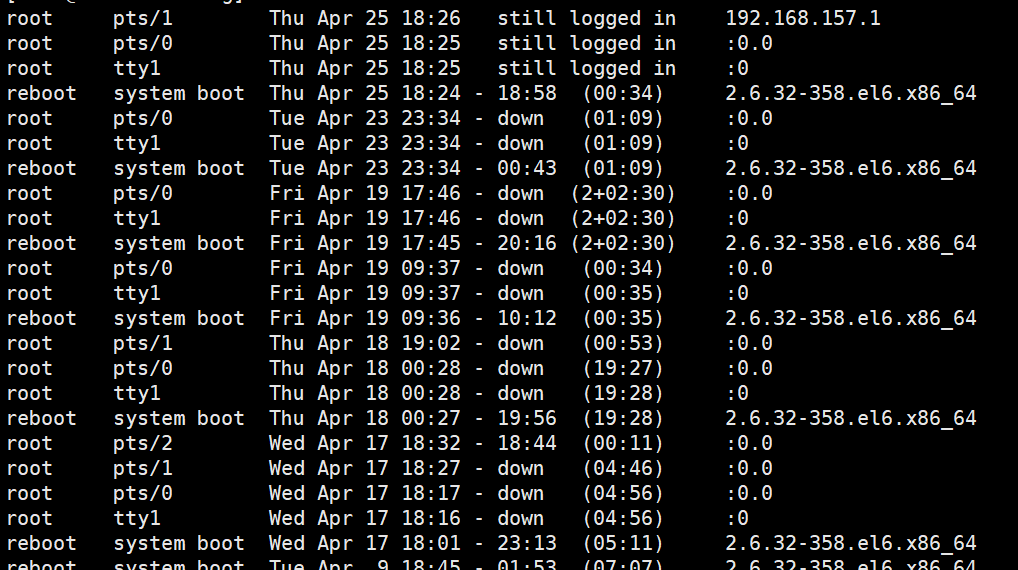
**secure**

是应急中最常用的文件，主要记录系统存取数据的文件，如POP3、ssh、telnet、ftp等相关记录，从日志中可看出系统服务是否遭受到安全威胁，从如下日志中可看到ftp服务一直在被破解。

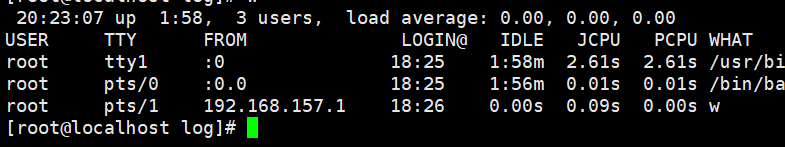


**用户日志**

wtmp日志记录了用户的登录、退出、重启等情况，可以查看系统是否存在异常用户登录，判断攻击者是否已经登录服务器，由于wtmp日志为二进制文件，所以利用用last命令查看，last -t 20190426120950 ,可查看这个时间之前的日志。



utmp日志记录当前用户的一些信息，由于utmp日志文件同样为二进制文件，可通过w、who命令查看



lastlog命令，用于显示系统中所有用户最近一次登录信息。lastlog文件在每次有用户登录时被查询。可以使用lastlog命令检查某特定用户上次登录的时间，并格式化输出上次登录日志/var/log/lastlog的内容。它根据UID排序显示登录名、端口号（tty）和上次登录时间。如果一个用户从未登录过，lastlog显示Never logged。注意需要以root身份运行该命令。