

Linux 查看日志文件

日志文件

查看日志文件

使用 `cat` 查看日志文件

使用 `less` 进行分页查看

使用 `tail` 查看日志文件

使用 `grep` 过滤日志文件

查看用户最后登录的记录

日志文件

- 1、**messages**：另一个常见的系统日志文件，记录了系统级事件，通常位于 `/var/log/messages`。
- 2、**boot.log**：记录了系统启动过程中的事件和消息。通常位于 `/var/log/boot.log`。
- 3、**secure**：安全日志，用于记录与系统和网络安全相关的事件，如入侵尝试、漏洞扫描等。通常位于 `/var/log/secure`。
- 4、**cron**：定时任务日志，记录了定时任务（cron任务）的执行情况，包括任务的启动和完成时间。通常位于 `/var/log/cron`。
- 5、**httpd（或apache2）**：Apache HTTP服务器的访问日志和错误日志，记录了HTTP请求和服务器错误信息。通常位于 `/var/log/httpd/` 或 `/var/log/apache2/` 目录中。
- 6、**nginx**：Nginx Web服务器的访问日志和错误日志，用于记录HTTP请求和服务器错误。通常位于 `/var/log/nginx/` 目录中。

查看日志文件

使用 `cat` 查看日志文件

▼

Plain Text

```
1 cat /var/log/messages
```

这将简单地显示整个日志文件的内容。如果日志文件很长，可能需要滚动浏览。

使用 less 进行分页查看

▼	Plain Text
1	<code>less /var/log/messages</code>

less 允许你以一页一页的方式查看日志文件，使用箭头键和其他命令来导航和搜索文件内容。按下 q 键退出 less，可以按空格实现翻页。

使用 tail 查看日志文件

▼	ABAP
1	<code>tail /var/log/messages</code>

更适合查看和监视日志文件的最新信息，尤其是在故障排除、监视应用程序或系统状态时。

▼	ABAP
1	<code>tail -f /var/log/messages</code>

-f 选项表示"follow"，它使 tail 命令持续刷新并显示新添加到文件的内容。这对于实时监视日志文件非常有用，因为你可以看到日志的更新，以便迅速响应事件或问题。

使用 grep 过滤日志文件

如果你要查找特定关键字或筛选日志文件的内容，你可以结合使用 grep 命令，比如：

▼	ABAP
1	<code>cat /var/log/messages grep "关键词"</code>

▼	ABAP
1	<code>less /var/log/messages grep "关键词"</code>

▼	ABAP
1	<code>tail /var/log/messages grep "关键词"</code>

关键字：日期和时间范围、IP地址或主机名、IP地址或主机名

查看用户最后登录的记录

▼	ABAP
1	last

这将显示最近登录会话的列表，显示用户名、终端、远程主机（如果适用）、登录时间和注销时间。信息按顶部的最新登录进行排序。

▼	ABAP
1	lastlog

此命令将显示系统上所有用户的上次登录时间。它显示用户名、端口和用户上次登录的时间。它可以成为检查所有用户的最后登录记录的有用工具。