Ps aux | grep rsyslogd #查看服务器是否启动

Chkconfig --list | grep rsyslog #查看服务器是否自启动（我电脑不行）

/var/log/btmp:记录错误登录的日志。这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看。

/var/log/lastlog:记录系统中所有用户最后一次的登录时间的日志。这个文件也是二进制我文件，不能直接vi，而要使用lastlog命令查看。

/var/log/cron：记录了系统定时任务相关的日志。

/var/log/cups:记录打印信息的日志。

/var/log/dmesg:记录系统在开机时内核自检的信息。也可以使用dmesg命令直接查看内核自检信息。

/var/log/mailog：记录邮件信息。

/var/log/message：记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就是应该是这个日志文件。

/var/log/secure：记录验证和授权方面的信息，只要涉及账户和密码的程序都会记录。比如说系统的登录，ssh的登录，su切换用户，sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中。

/var/log/wtmp：永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看。

/var/run/utmp：记录当前已经登录的用户的信息。这个玩家会随着用户的登录和注销而不断变化，只记录当前登录哦那过户的信息。同样这个文件不能直接vi，而要使用w，who，users等命令来查询。

基本日志格式包含以下四列：

1. 事件产生的时间；
2. 发生事件的服务器的主机名；
3. 产生事件的服务名或程序名；
4. 事件的具体信息。