兄弟连教育

www.lampbrother.net

第十四讲 日志管理

主讲人：沈超（http://weibo.com/lampsc)

交流论坛：http://bbs.lampbrother.net

课程大纲

14.1 日志管理简介

14.2 rsyslogd日志服务

14.3 日志轮替

1、日志文件格式

- 基本日志格式包含以下四列：
  - 事件产生的时间；
  - 发生事件的服务器的主机名；
  - 产生事件的服务名或程序名；
  - 事件的具体信息。

2、/etc/rsyslog.conf配置文件

authpriv.* /var/log/secure

#服务名称[连接符号]日志等级 日志记录位置

#认证相关服务.所有日志等级 记录在

/var/log/secure日志中

服务名称

服务名称	说　明
auth	安全和认证相关消息（不推荐使用authpriv替代）
authpriv	安全和认证相关消息（私有的）
cron	系统定时任务cront和at产生的日志
daemon	和各个守护进程相关的日志
ftp	ftp守护进程产生的日志
kern	内核产生的日志（不是用户进程产生的）
local0-local7	为本地使用预留的服务
lpr	打印产生的日志

mail	邮件收发信息
news	与新闻服务器相关的日志
syslog	有syslogd服务产生的日志信息（虽然服务名称已经改为rsyslogd，但是很多配置都还是沿用了syslogd的，这里并没有修改服务名）。
user	用户等级类别的日志信息
uucp	uucp子系统的日志信息，uucp是早期linux系统进行数据传递的协议，后来也常用在新闻组服务中。

连接符号

- 连接符号可以识别为：
  - “*”代表所有日志等级，比如：“authpriv.*”代表authpriv认证信息服务产生的日志，所有的日志等级都记录
  - “.”代表只要比后面的等级高的（包含该等级）日志都记录下来。比如：“cron.info”代表cron服务产生的日志，只要日志等级大于等于info级别，就记录
  - “.=”代表只记录所需等级的日志，其他等级的都不记录。比如：“*.=emerg”代表人和日志服务产生的日志，只要等级是emerg等级就记录。这种用法及少见，了解就好
  - “.!”代表不等于，也就是除了该等级的日志外，其他等级的日志都记录。

日志等级

等级名称	说　　明
debug	一般的调试信息说明
info	基本的通知信息
notice	普通信息，但是有一定的重要性
warning	警告信息，但是还不回影响到服务或系统的运行
err	错误信息，一般达到err等级的信息以及可以影响到服务或系统的运行了。
crit	临界状况信息，比err等级还要严重
alert	警告状态信息，比crit还要严重。必须立即采取行动
emerg	疼痛等级信息，系统已经无法使用了

日志记录位置

- 日志文件的绝对路径，如“/var/log/secure”
- 系统设备文件，如“/dev/lp0”
- 转发给远程主机，如“@192.168.0.210:514”
- 用户名，如“root”
- 忽略或丢弃日志，如“~”

扫描上面的二维码

关注兄弟连官方微信账号

兄弟连官方网址：www.lampbrother.net