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、日志服务

- 在CentOS 6.x中日志服务已经由rsyslogd取代了原先的syslogd服务。rsyslogd日志服务更加先进，功能更多。但是不论该服务的使用，还是日志文件的格式其实都是和syslogd服务相兼容的，所以学习起来基本和syslogd服务一致。

- rsyslogd的新特点：
  - 基于TCP网络协议传输日志信息；
  - 更安全的网络传输方式；
  - 有日志消息的及时分析框架；
  - 后台数据库；
  - 配置文件中可以写简单的逻辑判断；
  - 与syslog配置文件相兼容。

确定服务启动

[root@localhost ~]# ps aux | grep rsyslogd

#查看服务是否启动

chkconfig --list | grep rsyslog

#查看服务是否自启动

2、常见日志的作用

日志文件	说　　明
/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	记录了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/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，命令如下： [root@localhost log]# lastb root　　tty1　　Tue Jun 4 22:38 - 22:38 (00:00) *#有人在6月4日22:38使用root用户，在本地终端1登录错误*
/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文件，不能直接vi，而要使用lastlog命令查看。

/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。这个文件会随着用户的登录和注销而不断变化，只记录当前登录用户的信息。同样这个文件不能直接vi，而要使用w，who，users等命令来查询。

- 除了系统默认的日志之外，采用RPM方式安装的系统服务也会默认把日志记录在/var/log/目录中（源码包安装的服务日志是在源码包指定目录中）。不过这些日志不是由rsyslogd服务来记录和管理的，而是各个服务使用自己的日志管理文档来记录自身日志。

日志文件	说　　明
/var/log/httpd/	RPM包安装的apache服务的默认日志目录
/var/log/mail/	RPM包安装的邮件服务的额外日志目录
/var/log/samba/	RPM包安装的samba服务的日志目录
/var/log/sssd/	守护进程安全服务目录

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