Lec 18 认识与分析日志文件

什么是日志文件

何时、何地(来源IP)、何人(什么服务名称)、做了什么

记录系统在什么时候由哪个程序做了什么样的行为,发生了何种事件等等。

说明

importance { 解决系统方面的错误 / 解决网络服务的问题 / 记录过往事件

常见的日志文件:

△ /var/log/boot.log　只有在本次开机启动的信息

△ /var/log/cron　crontab 的记录

△ /var/log/lastlog　系统上所有的帐号最近一次登入系统时的相关信息 `/lastlog`

△ /var/log/maillog 或 /var/log/mail/*

★△ /var/log/messages　几乎系统发生的错误信息(或是重要信息)都会被记录在这个文件中

一般格式

① 事件发生的日期与时间

② 发生此事件的主机名

③ 启动此事件的服务名称(如 systemd, crond 等)或指令与函数名称(如 su, login 等)

④ 该讯息的实际数据内容

记录日志文件的服务: rsyslog.service

(暂时看不懂...)

日志文件的轮转: logrotate

rsyslogd 利用的是 daemon 的方式来启动时,当有需求时立刻会被执行;

但 logrotate 却是在规定的时间到了之后才会进行日志文件的轮转,所以这个 logrotate 是挂在 cron 下的。/etc/cron.daily/

logrotate 的配置文件

'在什么状态下进行轮转?'

include /etc/logrotate.d

- /etc/logrotate.conf ← 主要的参数文件　/etc/logrotate.conf
- /etc/logrotate.d/ ← 目录,所有文件都会被读入,可覆盖 /etc/logrotate.conf 中的默认设定

(相当于 /opt/imal/etc/joschyd.conf 与 /opt/imal/etc/joschyd-sections/)

logrotate 的主要功能,将旧的日志文件移动为旧文件,并且重新建立一个新的、空的文件来记录。

一般要定义: ① 频率 ② 保留几个日志文件 ③ 被轮转的文件名加上日期作为文件名(dateext) ④ 是否压缩

(写法详见原书)

实际测试 logrotate 的动作

logrotate [-vf] <logfile>

[-v] 显示 logrotate 的运作

[-f] 强制让所有日志文件都进行轮转

自定义日志文件的轮转功能

修改 /etc/logrotate.d/* 文件的实例见原书

systemd-journald.service 简介

systemd-journald：内存，开机前的日志文件信息便消失了

rsyslogd：以前的信息，磁盘

使用 journalctl 观察日志信息

略

logger 指令的应用

略

保存 journal 的方式

略

分析日志文件

略