日志管理

日志管理

日志文件：系统中各个运行消息的文件，不同的日志文件记录了不同类型的信息，如内核消息、错误消息等

syslog服务：
syslogd: 系统，非内核产生的信息
klogd：内核，专门负责记录内核产生的日志信息

一.分析日志文件
通过浏览日志查找关键信息，对系统服务进行调试
判断故障发生的原因
1.分类
1）内核及系统日志：数据由系统服务rsyslog统一管理
可以根据主配文件/etc/rsyslog.conf中的设置决定内核消息
及其各种系统消息的记录位置

2）用户日志：数据用于记录系统用户登录及其退出系统的相关信息
，包括用户名、登录终端、登录时间、来源、使用的进程等等

3）程序日志：应用程序自己独立管理的一个日志，记录程序本身运行过程中的各种事件信息
2.内核和系统日志
/etc/rsyslog.conf
#grep -v "^$" /etc/rsyslog.conf
主配文件使用
mail.notice（举例）
服务 级别
/var/log/messages 内核和大多数系统消息日志位置
每一行的消息内容
时间：消息发出的时间和日期
主机名：生成消息的计算机的名称

子系统的名称：发出消息的应用程序的名称

消息内容：消息的具体内容

3.用户日志和程序日志

查询当前登录的用户情况：users，who，w

查询用户登录的历史记录：last,lastb

查看安全日志文件：/var/log/secure

程序日志：

例如：httpd 服务的日志文件access_log和error_log

分别记录客户访问事件和错误信息

4.常见日志文件：

/var/log/boot.log：记录了系统在引导过程中发生的事件，就是Linux系统开机自检过程显示的信息

/var/log/messages ： 记录Linux操作系统常见的系统和服务错误信息

/var/log/cron crond 计划任务产生的事件信息

/var/log/dmesg 引导过程中产生的信息

/var/log/maillog 记录电子邮件活动信息

/var/log/lastlog 记录最后一次用户成功登陆的时间、登陆IP等信息

/var/log/secure Linux系统安全日志，记录用户和工作组变化情况、用户登陆认证情况

/var/log/syslog：只记录警告信息，常常是系统出问题的信息，使用lastlog查看

/var/log/wtmp 记录用户登录、注销、系统启动、关键等信息，使用last命令查看

/var/log/btmp 记录失败或者是错误的登录信息和验证 lastb命令查看

/var/run/utmp： 该日志文件记录有关当前登录的每个用户的信息。如 who、w、users、finger等就需要访问这个文件

5.日志消息的级别

0 emerg 会导致主机系统不可用的情况

1 alert 必须马上采取措施解决的问题

2 crit 比较严重的情况

3 err 运行出现问题

4 warning 可能影响系统功能，需要提醒用户的重要事件

5 notice 不会影响正常功能，但是需要注意的事件

6 info 一般信息

7 debug 程序或系统调试信息等

8 none 不记录任何日志

6.服务名称

1）服务名称

auth	# 认证相关的
authpriv	# 权限,授权相关的
cron	# 任务计划相关的
daemon	# 守护进程相关的
kern	# 内核相关的
lpr	# 打印相关的
mail	# 邮件相关的
mark	# 标记相关的
news	# 新闻相关的
security	# 安全相关的,与auth 类似
syslog	# syslog自己的
user	# 用户相关的
uucp	# unix to unix cp 相关的
local0 到 local7	# 用户自定义使用
*	# *表示所有的facility

7.action(动作)日志记录的位置

系统上的绝对路径 # 普通文件 如： /var/log/xxx

| # 管道 通过管道送给其他的命令处理

终端 # 终端 如：/dev/console

@HOST # 远程主机 如： @10.0.0.1

用户 # 系统用户 如： root

* # 登录到系统上的所有用户，一般emerg级别的日志是这样定义的

日志需要滚动(日志切割)：

messages messages.1 messages.2 messages.3

/sbin/init

/var/log/messages: 系统标准错误日志信息；非内核产生引导信息；各子系统产生的信息；

/var/log/maillog: 邮件系统产生的日志信息；

/var/log/secure:

定义格式例子：

mail.info /var/log/mail.log # 表示将mail相关的,级别为info及

info以上级别的信息记录到/var/log/mail.log文件中

auth.=info @10.0.0.1 # 表示将auth相关的,级别为info的信息记录到10.0.0.1主机上去

前提是10.0.0.1要能接收其他主机发来的日志信息

user.!=error # 表示记录user相关的,不包括error级别的信息

user.!error # 与user.error相反

*.info # 表示记录所有的日志信息的info级别

mail.* # 表示记录mail相关的所有级别的信息

. # 你懂的.

cron.info;mail.info # 多个日志来源可以用";" 隔开

cron,mail.info # 与cron.info;mail.info 是一个意思

mail.*;mail.!=info # 表示记录mail相关的所有级别的信息,但是不包括info级别的