内核在启动过程中都会产生很多的信息，进行初始化

初始化过程：

探测硬件，初始化硬件

初始化一般信息输出到console中 /dev/console

初始化之后要启动用户进程，

init：最重要 的守护进程(daemon)

进程有三类：守护进程(开机自启) 实时进程 交互式进程

守护进程也需要日志，

内核产生的日志在启动过程中记录，不过内核的记录稍微特殊点，在**/var/log/dmesg** 自己记录，启动完成后再放进去。是一个纯文本文件，从这里也可以看到设备信息（硬件初始化信息），**dmesg命令也可以直接查看硬件信息(dmesg | less)**

各自的服务启动也会记录下来：

早期是各自产生日志，各自软件定义

vsftpd --> /var/log/xfer.log

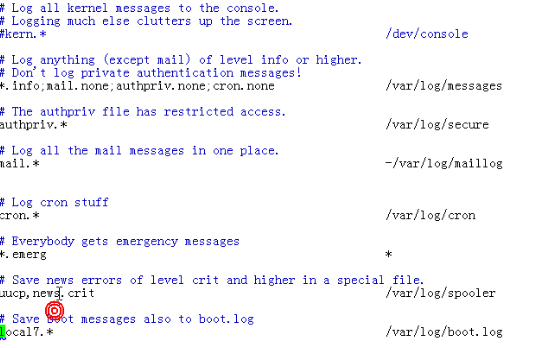
httpd --> /var/log/httpd/access.log

**后期为了统一日志的产生和格式于是产生了**：

**syslog** 是个服务统称(分为syslogd应用软件产生的日志, klogd系统启动之后的内核产生的日志)

以后产生的日志直接给syslog处理就行了，（社会发展，分工越来越明细）

**/etc/syslog.conf**



的内容怎么定义呢：

facility: 定义日志的来源，来识别应用程序

priority(**Log Level**):优先级

常用的**facility**：

The facility is one of the following keywords: **auth**, **authpriv**, **cron**, **daemon**, **kern**, **lpr**打印, mail, mark, news, security (same as auth), syslog, user, uucp and local0 through local7.

不同的facility放在不同的文件中

优先级**priority**

The priority is one of the following keywords, in ascending order: debug, info, notice, warning, warn (same as warning), err, error (same as err), crit, alert, emerg, panic (same as emerg).

操作**action**

facility.priority log\_location(Actions)

Regular File

Named Pipes

Terminal and Console /dev/console

Remote Machine: @HOST

List of Users: root

Everyone logged on: \*

**facility.priority action 谁产生的日志，日志级别 操作**

例子：

mail.info /var/log/maillog

mail.info: 包括此级别和比此级别高的所有级别产生的信息

mail.=info 只此级别的信息

mail.!=info 不包括某个级别

mail.!info 比info等级低的所有信息

mail.\* 所有级别信息

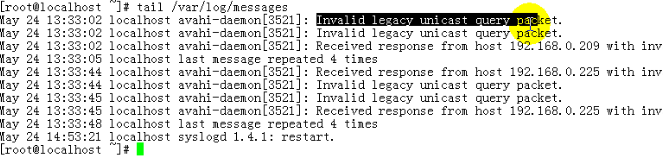
同一个文件可以记录多个**facility的多个级别的**日志信息

cron.info;mail.info /var/log/my.log

cron,mail.info

mail.\*; mail.!=info 除了info级别的所有信息

\*.info



日期和时间 主机名 软件或子系统的名称 信息

**每一个服务在/etc/init.d下都有一个与之对应的脚本：**

**service SERVICE {start|stop|restart|status|reload}**

**/etc/init.d/SERVICE {start|stop|restart|status|reload}**

syslog进程的配置文件

/etc/sysconfig/syslog

-r选项 接受其他机器发来的日志信息

拓展阅读：

1如果日志过大怎么办?涉及到周期性日志切割功能cron

2An asterisk (''\*'') stands for all facilities or all priorities, depending on where it is used (before or after the period). The keyword none stands for no priority of the given facility.

You can specify multiple facilities with the same priority pattern in one statement using the comma ('','') operator. You may specify as much facilities as you want.

Multiple selectors may be specified for a single action using the semicolon ('';'') separator. Remember that each selector in the selector field is capable to overwrite the preceding ones. Using this behavior you can exclude some priorities from the pattern.

将来真正想做一个日志服务器的话syslog还是比较薄弱的，出现了syslog-ng

**syslog-ng** is an open source implementation of the Syslog protocol for Unix and Unix-like systems. It extends the original syslogd model with content-based filtering, rich filtering capabilities, flexible configuration options and adds important features to syslog, like using TCP for transport.

Main features:

High performance

Trusted transfer

Wide range of platforms and architectures

Increased reliability

Big user community

Message filtering and sorting

Event tagging and correlation

Support for the latest IETF standards

It has two editions with a common codebase. The first is called syslog-ng OSE (with the license LGPL) and have additional plugins (modules) under proprietary license. This edition is called Premium Edition (PE)收费 强大.