今日学习心得

1. kill命令

当一个进程结束的时候或者要异常结束的时候，会向其父进程返回一个或者接收一个 SIGHUP 信号而做出的结束进程或者其他的操作，这个 SIGHUP 信号不仅可以由系统发送，我们可以使用 kill 来发送这个信号来操作进程的结束或者重启等等。

命令：kill -9 [uid]

2. 进程的执行顺序

我们在使用 ps 命令的时候可以看到大部分的进程都是处于休眠的状态，如果这些进程都被唤醒，那么该谁最先享受 CPU 的服务，后面的进程又该是一个什么样的顺序呢？进程调度的队列又该如何去排列呢？就是靠该进程的优先级值来判定进程调度的优先级。

而 nice 的值我们是可以通过 nice 命令来修改的，而需要注意的是 nice 值可以调整的范围是 -20 ~ 19，其中 root 有着至高无上的权力，既可以调整自己的进程也可以调整其他用户的程序，并且是所有的值都可以用，而普通用户只可以调制属于自己的进程，并且其使用的范围只能是 0 ~ 19，因为系统为了避免一般用户抢占系统资源而设置的一个限制。

3. 日志

日志是一个系统管理员，一个运维人员，甚至是开发人员不可或缺的东西，系统用久了偶尔也会出现一些错误，我们需要日志来给系统排错，在一些网络应用服务不能正常工作的时候，我们需要用日志来做问题定位，日志还是过往时间的记录本，我们可以通过它知道我们是否被不明用户登录过等等。

在 Linux 中大部分的发行版都内置使用 syslog 系统日志。

根据服务对象粗略的将日志分为两类：系统日志、应用日志

系统日志主要是存放系统内置程序或系统内核之类的日志信息如 alternatives.log 、btmp 等等，应用日志主要是我们装的第三方应用所产生的日志如 tomcat7 、apache2 等等。



4. 日志的产生

日志可以通过两种方式产生：

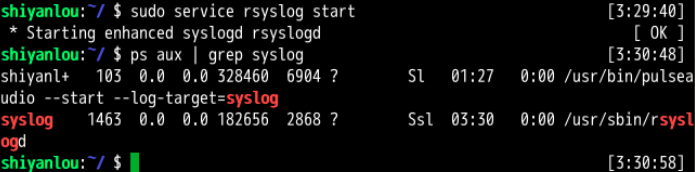
一种是由软件开发商自己来自定义日志格式然后指定输出日志位置；

一种方式就是 Linux 提供的日志服务程序，而我们这里系统日志是通过 syslog 来实现，提供日志管理服务。

配置日志：

syslog 是一个系统日志记录程序，在早期的大部分 Linux 发行版都是内置 syslog，让其作为系统的默认日志收集工具，虽然随着时代的进步与发展，syslog 已经年老体衰跟不上时代的需求，所以他被 rsyslog 所代替了，较新的 Ubuntu、Fedora 等等都是默认使用 rsyslog 作为系统的日志收集工具

rsyslog的全称是 rocket-fast system for log，它提供了高性能，高安全功能和模块化设计。rsyslog 能够接受各种各样的来源，将其输入，输出的结果到不同的目的地。rsyslog 可以提供超过每秒一百万条消息给目标文件。



rsyslog 主要是由 Input、Output、Parser 这样三个模块构成的，并且了解到数据的简单走向，首先通过 Input module 来收集消息，然后将得到的消息传给 Parser module，通过分析模块的层层处理，将真正需要的消息传给 Output module，然后便输出至日志文件中。

5. 转储日志

在本地的机器中每天都有成百上千条日志被写入文件中，更别说是我们的服务器，每天都会有数十兆甚至更多的日志信息被写入文件中，如果是这样的话，每天看着我们的日志文件不断的膨胀，要占用许多的空间，所以有个叫 logrotate 的东西诞生了。

logrotate 程序是一个日志文件管理工具。用来把旧的日志文件删除，并创建新的日志文件。我们可以根据日志文件的大小，也可以根据其天数来切割日志、管理日志，这个过程又叫做“转储”。

大多数 Linux 发行版使用 logrotate 或 newsyslog 对日志进行管理。logrotate 程序不但可以压缩日志文件，减少存储空间，还可以将日志发送到指定 E-mail，方便管理员及时查看日志。

显而易见，logrotate 是基于 CRON 来运行的，其脚本是 /etc/cron.daily/logrotate；同时我们可以在 /etc/logrotate 中找到其配置文件