这部分将涉及常用的各类linux命令和一些系统高级管理特性，尤其是shell script的创建，这部分在系统自动化运维时会很有作用。



在进入bash介绍之前，首先需要介绍vim编辑器，虽然现在的编辑器已经非常强大， 比如sublime等，但有些场合还是需要简单的使用vim来进行文件的编辑，由于现在这部分内容已经不是重点，因此通过一个简单的表格介绍其最基本的几个命令。

|  |  |
| --- | --- |
| 命令 | 示例 |
| 编辑w文本 | vi test.txt，默认进入命令模式 |
| 编辑模式 | 通过i字符进入 |
| 命令模式 | 通过[Esc]进入，通过:wq完成编辑并保存，其中w表示保存，q表示退出，:q!表示强制退出不保存 |
| 常见快捷键 | dd删除所在行,yy复制所在行,[ctrl]+r重做上一个操作  u复原前一个操作 |

接下来开始bash常用命令介绍，内容比较多，需要有点耐心。这部分内容推荐把bash脚本当做一个全新的语言进行学习，这个力度将会使你很好的掌握bash。

|  |  |
| --- | --- |
| 命令 | 示例 |
| type name | 查看命令信息 |
| 变量的显示、设置和取消 | echo $PATH, name=xionger, unset name |
| 环境变量 | HOME:用户主文件，SHELL：默认为/bin/bash  HISTSIZE:临时命令条数，PATH：执行文件查找路径，用:分隔 |
| locale | 查看系统语言环境信息，可以通过/etc/sysconfig/i18n |
| 从键盘读取用户输入 | read [-pt] variable  read -p 'please keyin your name： ' -t 30 named |
| 声明变量declare | 默认定义为字符串  declare –a,定义变量为数组  declare –i,定义变量为整数  declare –x,用法与export一样，将之后变量设置为环境变量  declare –r,设置为readonly |
| alias,unalias | 给长命令设置/取消别名 |
| history | 查看已使用命令,history | grep named |
| 相关配置文件 | ~/.bash\_profile, /.bash\_login, /.profile  可以通过source 配置文件，读入环境配置 |
| 数据流重定向 | ll / > ~/temp/llShow.txt,一个>表示方式，2个表示append方式 |
| 命令执行的判断依据 | ; && || |
| Pipe管道命令 | 后续命令依赖于前一个命令的结果，ls –al /etc | less |
| 常用字符串命令 | cut –c 分割字符; **grep** 字符串,查找包含此字符串的行  sort排序命令; uniq去重命令;wc获取行数  其他命令：tr,col,join,paste,expand,split |

Tip:如果命令太长，可以使用\[Enter]方式换行。

**正则表达式在Linux的应用**：正则的概念和使用大家已经非常熟悉，这儿就不做介绍了，可参考博文--[正则表达式](http://www.cnblogs.com/wanliwang01/p/regex_base.html)。这儿主要介绍其在系统中的使用，目的只有一个，为之后的运维脚本提供基础。通常正则会用在grep命令中，比如 grep –n 'the' demo.txt，这儿的the可以用任意正则pattern替换。此外，可以通过sed、awk工具帮助查询脚本，需要时查询相关文档即可。

|  |
| --- |
| #!/bin/bash  # program:用户输入一个文件名，系统检查其目录和权限  # History:2016  PATH=/bin:/sbin:/user/bin:/user/sbin:~/bin  export PATH  #1.输入文件名  echo -e "please input a filename, it will check the filename's type and \  permission \n\n"  read -p "input filename : " filename  test -z $filename && echo "you must input a filename" && exit 0  #2.判断文件是否存在  test ! -e $filename && echo "the filename '$filename' is not existed " &&exit 0  #3.判断文件类型  test -f $filename && filetype='regular file'  test -d $filename && filetype='directory'  test -r $filename && perm='readable'  test -w $filename && perm='$perm writable'  test -x $filename && perm='$perm executable'  #4.输出信息  echo "The filename: $filename is a $filetype"  echo "And the permissions are : $perm" |

常见逻辑结构

|  |  |
| --- | --- |
| 逻辑结构 | 示例 |
| 判断结构 | if ["$yn"=="y"] || ["$yn"=="Y"]; then  echo "OK,continue"  elif ["$yn"=="n"] || ["$yn"=="N"]; then  echo "Fail"  else  echo "Default"  fi |
| 循环结构 | for username in $users  do  id $username  finger $username  done |
| 函数 | function printit(){} |

在Linux中，用户的账号信息都保存在/etc/passwd文件中，常见的账号管理命令如下所示。

|  |  |
| --- | --- |
| 命令 | 示例 |
| 组命令 | groups查看当前组，newgrp创建新组 |
| 用户命令 | useradd创建用户，passwd修改密码，chage显示密码详细信息  usermod修改用户信息, userdel删除用户 |
| Acl权限 | Getfacl, setfacl |
| 用户身份切换 | su切换用户, sudo模拟root进行操作，非常有用，比如安装软件  **sudo apt install xxx** |
| pam模块 | Pluggable Authentication Modules用于用户认证 |
| 信息查询 | w, who获取账号登录信息，last,lastlog |

接下来，介绍linux关于文件系统的一些高级概念。

磁盘配额Quota：用于管理每个用户可用的磁盘大小，包括一个hard阀值和一个soft阀值。

软件磁盘阵列Software RAID：比如RAID-0性能最佳，RAID-1完整备份，RAID-0+1兼顾性能和备份，RAID-5通过同位检查码parity来均衡性能和安全，任何一个盘损坏，均可恢复，通过/etc/madadm.conf配置。

逻辑卷管理器LVM（Logical Volume Manager）:涉及5个主要概念，PV表示物理卷，VG表示卷用户组，PE表示物理扩展块，LV表示逻辑卷。

Tip:现在流行的docker就是建立在LXC上的容器引擎，这部分内容还需要加强。

我们常见的Job类型工作在Linux中被称为crontab例行性任务，系统中常见的例行性工作包括：进行日志文件的轮替，日志文件分析Logwatch任务，新建locate数据库，whatis数据库的建立,RPM软件日志文件的新建，删除临时文件，与网络服务有关的分析行为。

仅执行一次的工作：/etc/init.d/atd restart, chkconfig atd on, at now + 5 minutes

循环性的例行工作：59 23 1 5 \* mail tete < /home/xionger/lover.txt 每年给女友发邮件，系统配置文件/etc/crontab

之后介绍Linux的进程管理，Linux的进程也包括进程控制块PCB和数据部分，前者包含PID和权限相关信息，数据部分包含了程序所需的代码和相关资料，对其管理的相关命令如下所示。

|  |  |
| --- | --- |
| 命令 | 示例 |
| 工作管理 | Jobs查看当前工作，kill –pid关闭后台进程 |
| 进程查看 | ps aux, ps aux | egrep '(cron|syslog)'  top动态查看进程变化  pstree查看进程树  ps aux | grep 'syslog' | grep -v 'grep' | awk '{print $2}'  killall -9 httpd终止所有以httpd启动的进程 |
| 进程优先级 | ps -l, nice, renice [number] PID |
| 系统资源的查看 | free查看内存信息;uname查看内核信息;  uptime查看系统启动时间和工作负载  netstat:跟踪网路  其他命令：dmesg, vmstat  cat /etc/services |

最后介绍，个人觉得比较重要的系统服务和日志分析部分。在Linux中，daemon后台进程(也就是服务)包含两类，一种是stand\_alone的，一种是由super daemon统一管理的。通常来说，每一个服务都具有一个指定的端口，比如http服务的80端口，ftp服务的21端口。服务的启动脚本将放置在/etc/init.d/\*中，其相关初始化配置文件放在/etc/sysconfig/\*中，super daemon的配置文件在/etc/xinetd.conf,/etc/xinetd.d/\*中，服务自身的配置文件放在/etc/\*中，服务产生的数据放在/var/lib/\*中，服务的PID则记录在/var/run/\*中。可以通过service xxx restart启动服务，通过service --status-all查看服务状态。

Tip:可以通过修改/etc/hosts.allow和/etc/hosts.deny来设置白/黑名单。

在Linux中，常见的日志文件通常在/var/log/目录, cron为工作调度日志，dmesg为内核检测信息，lastlog所有账号最近一次登录信息，maillog邮件相关信息(SMTP, POP3)，messages系统错误信息，secure登录相关安全信息，httpd网络服务信息。

那么记录日志文件的服务是什么呢？syslogd,可以通过如下命令查看：ps aux | grep syslog, chkconfig --list syslog，为了保护日志文件，我们可以通过chattr –a来实现。此外，日志的轮替是通过logroate服务来实现的，其配置文件为/etc/logrotate,conf,/etc/logrotate.d目录中文件均会被读入配置。（注意在**阿里云中，所有的syslog均变为rsyslog**）.

此外，linux常见的日志分析工具包括logwatch，可以定期将分析报告发送到你的邮箱，如果需要更进一步的自定义分析，到时参阅资料即可。

“人活着就要实现自己吹过的’牛逼’”--佚名

参考资料：

1. 鸟哥. 鸟哥的Linux私房菜 基础学习篇(第三版)[M]. 北京:人民邮电出版社, 2010.