目录：

[1、Linux的定时任务crond 1](#_Toc418499242)

1.1crond是什么？ 1

1.2为什么要使用crond定时任务 2

1.3Linux系统的定时任务 2

1.4 Linux系统crond的定时任务 3

1.5linux系统下定时任务软件种类 4

2、用户管理命令10

2.1用户管理回顾 11

2.2 /etc/skel 目录 13

2.3 /etc/default/useradd 文件 14

2.4 /etc/login.defs文件 15

2.5 useradd命令 15

2.6用户查询相关命令id、finger、users、w、who、last、lastlog、groups 22

3、用户身份切换24

3.1 su命令介绍 24

3.2 sudo命令介绍 25

4、磁盘管理的知识34

4.1磁盘的历史介绍 34

4.2磁盘的外部结构 34

4.3磁盘的内部结构 35

4.4磁盘的类型与区别 36

5、什么是RAID43

6、增加epel源44

# 1、Linux的定时任务服务crond（crontab）服务

* 1. **crond是什么？**

是Linux系统中用来定期执行命令或指定程序任务的服务。crond服务相当于生活中的闹钟，定时任务用来在指定的时间或按一定的频率执行程序或任务。

一般安装完成C5/C6系统的时候，crond就会默认存在了，我们优化开机自启动服务的时候，第一个就是crond。

[root@moban ~]# chkconfig --list crond

crond 0:关闭 1:关闭 2:关闭 3:启用 4:关闭 5:关闭 6:关闭

查看crond配置：

[root@moban ~]# crontab -l

\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1

* 1. **crond的工作原理**

默认情况crond服务，每分钟会检查系统中是否有需要执行的定时任务，如果有，就会根据事先定义好规则来执行这个定时任务。

聪明的同学做个比喻：crond的定时任务就相当于我们生活中的闹钟分钟一样。

crond在不同的服务器上都要部署，分布式定时任务

####秒级别的定时任务需要使用脚本来完成：

[root@moban ~]# while true

> do

> echo "I am oldboy teacher."

> sleep 1

> done

I am oldboy teacher.

I am oldboy teacher.

程序：磁盘上存在的文件。

进程：正在运行的程序，内存里。

守护进程：持续运行的程序，内存里，$SHD

* 1. **为什么需要定时任务？**

互联网的服务器：7\*24小时开机提供服务是网站的基本特征。

服务器有重要数据：至少1天备份一次，5份以上，最近7天的备份。

服务器上的数据一般最低1天备一次全备份

* 1. **Linux系统crond的定时任务**

Linux系统中定时任务调度的工作可以分为以下两种情况：

1. Linux系统自身定期执行的任务工作：系统在周期性自行执行的任务工作，如轮询系统日志、备份系统数据、清理系统缓存等，这些任务无需认为干预，例如：

[root@moban ~]# ls -l /var/log/messages

-rw------- 1 root root 302 10月 26 11:47 /var/log/messages #####系统日志每周一份

[root@moban ~]# ls -l /var/log/secure\*

-rw------- 1 root root 918 10月 26 13:01 /var/log/secure

-rw-------. 1 root root 6462 9月 29 05:59 /var/log/secure-20150929

-rw-------. 1 root root 12601 10月 12 10:11 /var/log/secure-20151012

-rw------- 1 root root 30436 10月 18 12:32 /var/log/secure-20151018

-rw------- 1 root root 3833 10月 26 11:04 /var/log/secure-20151026

Linux系统自身定期执行的任务文件在/etc/logrotate.d中

[root@moban ~]# cd /etc/logrotate.d

[root@moban logrotate.d]# ls

dracut psacct syslog yum

[root@moban logrotate.d]# vi syslog

/var/log/cron

/var/log/maillog

/var/log/messages

/var/log/secure

/var/log/spooler

请不要将定时任务配置命令放到/etc/crontab文件中，这个是不规范的。

系统自身的定期执行的任务

[root@C66-moban new]# ll /etc/|grep cron

-rw-------. 1 root root 541 11月 23 2013 anacrontab

drwxr-xr-x. 2 root root 4096 7月 12 12:18 cron.d

drwxr-xr-x. 2 root root 4096 7月 12 12:20 cron.daily

-rw-------. 1 root root 0 11月 23 2013 cron.deny

drwxr-xr-x. 2 root root 4096 7月 12 12:16 cron.hourly

drwxr-xr-x. 2 root root 4096 7月 12 12:18 cron.monthly

-rw-r--r--. 1 root root 457 9月 27 2011 crontab

drwxr-xr-x. 2 root root 4096 9月 27 2011 cron.weekly

2、用户执行的任务工作：某个用户或系统管理员定期要做的任务工作，例如每个5分钟和互联网上时间服务器进行时间同步，每天晚上0点备份网站站点数据及数据库数据，一般这些工作需要由每个用户自行设置才行。

[root@moban ~]# crontab –l #####查看定时任务的命令#####

\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1

00 \*/2 \* \* \* /bin/sh /server/scripts/tar.sh >/dev/null 2>&1

00 09,14 \* \* 0,6 /bin/sh /server/scripts/oldboy.sh >/dev/null 2>&1

用户执行的任务工作,也就是我们运维管理人员技行的任务工作, 因此,这个用户执行的任务是我们今天讨论的重点。 I

**1.5 linux系统下定时任务软件种类**

严格的说, Linux系统下的定时任务软件还真不少,例如, at,crontab， anacron。

1. at适合仅执行一次就结束的调度任务命令,例如:某天晩上需要处理一个任务, 仅仅是这一天的晚上,属子突发性的工作任务.要执行at命令.还常要启动一个名为atd 的服务才行,在老男孩的工作中从来都不会有需求用这个。因此, 建议大家不要深入研究了,到此我们讲解这里为止即可。

[root@C66-moban new]# chkconfig --list atd

atd 0:关闭 1:关闭 2:关闭 3:关闭 4:关闭 5:关闭 6:关闭

2) anacron为非7\*24小时开机的服务器准备的，每次开机执行的，检测停机期间没有执行的任务，在开机后一次性执行一遍。

3）crond，crond服务默认情况（每分钟），会检查系统中是否有需要执行的定时任务，如果有，就会根据事先定义好的规则来执行这个定时任务。\*\*\*\*\* （crond依赖的服务，crond）

提示：crond是一个定时任务守护进程名字，而crontab是用户用来设置定时任务规则的命令。

crontab指令语法：

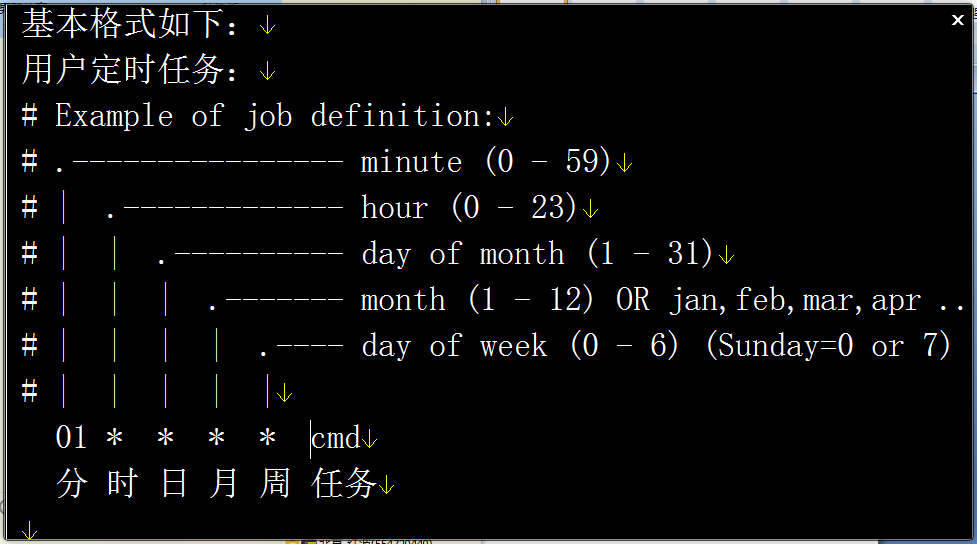
-l ：list  查看有什么定时任务  
-e ：edit 编辑定时任务

crontab –e ==== /var/spool/cron/root

[root@oldboy new]# cat /var/spool/cron/root   
#time sync by oldboy at 2010-2-1  
\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1  
[root@oldboy new]# crontab -l  
#time sync by oldboy at 2010-2-1  
\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1

基本格式如下：

用户定时任务：



特殊符号：

\* 任意时间都，实际就是“每”的意思。

- 取值范围 15-17点，表示15,16,17点。

，列表分隔，15,16,17

/ 例如：分为上的\*/5，表示每隔5分钟。

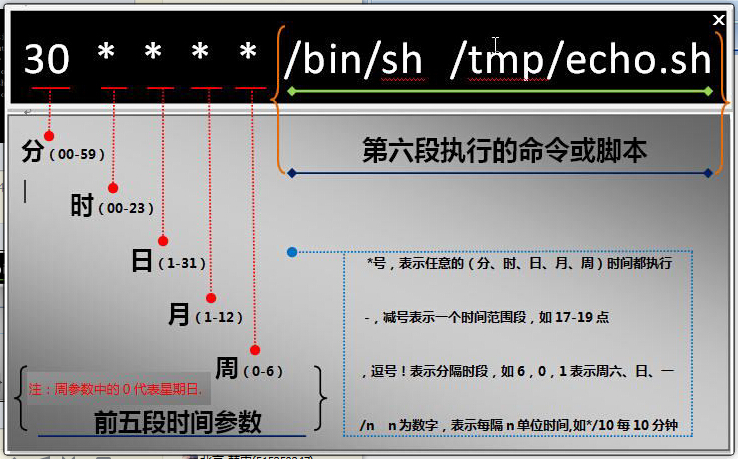
例1: 00 23 \* \* \* cmd

每天23时执行 cmd

例2: 00 17-19 \* \* \* cmd 每天17,18,19整点执行cmd

00 17，18，19 \* \* \* cmd 每天17,18,19整点执行cmd

例3: 30 3-5,17-19 \* \* \* cmd 每天3点半，5点半，17点半，19点半执行cmd



**强调：这是学习态度的体现，这种态度极其重要，不要单纯理解奇数，多结合画图，案例理解原理，记一次很久都忘不掉。**

要学好linux运维请从排版画图开始  
http://oldboy.blog.51cto.com/2561410/1180894

定时任务依赖的服务：

[root@C66-moban new]# chkconfig --list crond

crond 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

[root@oldboy new]# /etc/init.d/crond status  
crond (pid  1008) is running...

[root@moban oldboy]# ps -ef|grep crond|grep -v grep

root 1275 1 0 Oct27 ? 00:00:01 crond

|  |  |  |
| --- | --- | --- |
| crontab –e | /var/spool/cron/root | crontab –e编辑会检查语法，而直接echo,vi编辑配置不会 |
| visudo | /etc/sudoers | visudo编辑会检查语法，而直接echo,vi编辑配置不会。 |

生产环境crontab专业实例：

例1：每分钟打印一次自己的名字拼音到“/server/log自己的名字命名的文件”

[root@moban ~]# mkdir -p /server/log/ 首先创建这个目录和文件（echo不会自动生产文件的）

[root@moban log]# touch lidongkai.txt

[root@moban log]# crontab –e

\* \* \* \* \* echo "li dong kai" >> /server/log/lidongkai.txt

~

[root@moban ~]# crontab -l

\* \* \* \* \* echo "li dong kai" >> /server/log/lidongkai.txt

[root@moban log]# tailf /server/log/lidongkai.txt

li dong kai

**解答小结：**

1、定时任务要加注释。

2、结尾不要有 >dev/null 2>&1

3、/server/log 目录必须要存在才能出结果，echo是不会创建文件的，首先要touch这个文件。

4、定时任务中的路径一定要绝对路径。

5、crond服务必须要开启运行。

6、查看定时任务日志命令： tail /var/log/cron

**属于定时任务的规范步骤：**

1、尽量使用脚本，但要提前在命令行测试好。

2、把操作成功的命令复制到脚本里。

3、脚本放到指定目录

4、/bin/sh /server/scripts/tar.sh 全路径侧四脚本命令行测试。

5、复制目录行测试的脚本名字到定时任务里。

6、crontab -e

\*/3 \* \* \* \* /bin/sh 全路径测试脚本 >/dev/null 2>&1

7、crontab -l 检查定时任务。

8、最新的任务放在最上面。

crontab –e ====/var/spool/cron/root

例2：每周六、日上午9:00和下午14:00来老男孩Linux培训学习（执行/server/scripts/date.sh）。

要求：/server/scripts/oldboy.sh脚本的功能是打印当天的日期：格式为2015-10-28，可以随意。

最佳到一个文件里或者干脆在屏幕输出。

1、定时任务一定尽量用脚本来实现。

2、命令行操作成功，然后放入脚本执行成功，最后在配置任务。

3、复制操作成功的命令行脚本，再定时任务里配置。

解答：细心，听话（专业，规范）

1. 步骤1创建目录/server/scripts和编写date.sh脚本

[root@moban ~]# mkdir /server/scripts/ -p

[root@moban ~]# echo "date +%F" > /server/scripts/date.sh

[root@moban ~]# cat /server/scripts/date.sh

date +%F

[root@moban ~]# sh /server/scripts/date.sh

2015-10-28

1. 书写定时任务

[root@moban ~]# echo "#study to oldboy linux" >> /var/spool/cron/root

[root@moban ~]# echo "00 09 14 \* \* 6,7 /bin/sh/server/scripts/date.sh" >> /var/spool/cron/root

[root@moban ~]# crontab -l|tail -2

#study to oldboy linux

00 09 14 \* \* 6,7 /bin/sh/server/scripts/date.sh

也可以输入crontab –e 然后放入如下内容保存：

#study to oldboy linux

00 09 14 \* \* 6,7 /bin/sh/server/scripts/date.sh 经验🡨脚本最好是复制命令行执行过的命令。

根据以上两个例题，做一个定时任务的总结：

**#######书写定时任务的若干要领方法：########**

1、为定时任务规范加必要的注释。

2、执行shell脚本任务前加/bin/sh

3、定时任务命令或脚本结尾加>/dev/nu11 2>&1

定时任务的结尾要加上>/dev/null 2>&1 == 1>/dev/null 2>/dev/null ==&>/dev/null

4、定时任务命令或程序最好写到脚本里执行

5、 在指定用户下执行相关的定时任务

6、 生产任务程序不要随意打印输出信息

tar zcvf echo123 >a.1og

7、定时任务执行的脚本要规范路径(/server/scripts)

8、配置定时任务规范操作过程

9、配置定时任务规范操作过程，防止出错。

1)首先要在命令行操作成功,然后复制成功的命令到脚本里,在细小环节减少出错的机会

2)然后测试脚本,测试成功后,复制脚本的规范路径到定时任务配置里,不要手敲。

3)先在测試环境下测试, 然后正式环境规法部署

**工作中调试定时任务的方法：**

1、增加执行任务频率调试任务（某些任务不能用于生产环境没有测试机会）

每分钟或者系统时间之后5分钟执行，看看结果是否正确。

代码、配置变更发布流程：个人开发环境--办公测试环境-->IDC机房测试环境--->IDC正式环境（分组，灰度发布）

2、调整系统时间调试任务（不能直接用于生产环境），保持5分钟。

3、通过脚本日志输出调试定时任务。

4、注意一些任务命令带来的问题：

例如：

\*/1 \* \* \* \* echo "==" >>/tmp/oldboy.log >/dev/null 2>1

\*/1 \* \* \* \* tar zcf /tmp/oldboy\_$(date +%F).tar.gz /etc/hosts >dev/null 2>&1

5、注意：环境变量导致定时任务故障（Java）

6、通过crond定时任务服务日志调试定时任务。

7、其他稀奇古怪的问题调试的办法。

**crontab定时任务生产应用问题10箴言**

1、系统环境变量问题

http://oldboy.blog.51cto.com/2561410/1541515

2、定时任务里的命令要用绝对路径。

3、脚本权限问题加/bin/sh

4、时间变量问题用反斜线\%转义，最好用脚本。

5、>/dev/null 2>&1问题（1>/dev/null 2>dev/null，&>dev/null）

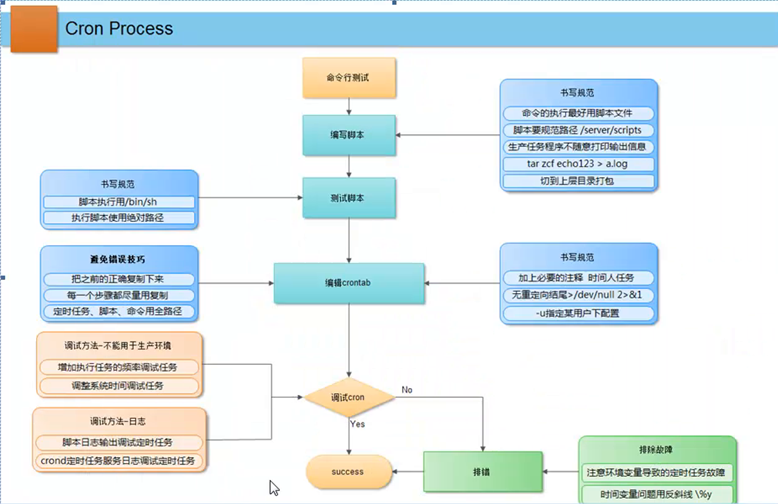
6、定时任务规则之前加注释

7、使用脚本程序替代命令行定时任务。

8、避免不必要的程序及命令输出。

9、切到目录的上一级打包目录

10、定时任务脚本中的程序命令尽量用全路径（和环境变量的识别有关）



# 2、用户管理命令

**2.1 用户管理回顾**

用户管理：

三种用户角色：

超级

普通

虚拟

对应的UID范围：0、1-499、500-65535

1、/etc/passwd的权限是644

[root@moban /]# cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin



UID与GID取值范围全部是0-65535

[root@moban /]# cat /etc/shells

/bin/sh

/bin/bash

/sbin/nologin

/bin/dash

/bin/tcsh

/bin/csh

Linux支持shell的脚本。

1. 密码文件 /etc/shadow

[root@moban /]# tail /etc/shadow

haldaemon:!!:16702::::::

ntp:!!:16702::::::

saslauth:!!:16702::::::

postfix:!!:16702::::::

sshd:!!:16702::::::

tcpdump:!!:16702::::::

oldboy:$6$StRpSOha$Uo9.xDb35.CgTolw6xaLa9v30UIdtT81DQnroKDbH1K4XqcW8BiAWaPu8tVI3UbLj4WBhsBf5/jOf/u1una/p/:16709:0:99999:7:::

fff:!!:16709:0:99999:7:::

111:!!:16709:0:99999:7:::

msn:!!:16709:0:99999:7:::

3、 /etc/group

[root@moban /]# tail /etc/group

saslauth:x:76:

postdrop:x:90:

postfix:x:89:

sshd:x:74:

tcpdump:x:72:

slocate:x:21:

oldboy:x:500:

fff:x:501:

111:x:502:

msn:x:503:

**小结论：**

groupadd 添加用户组会更改 /etc/group、/etc/gshadow

/etc/passwd 账号

/etc/shadow 密码

/etc/group 组

/etc/gshadow 组密码

Useradd更改上述4个

Passwd 更改第二个

Groupadd 更改后两个

账户管理的命令：

和用户相关的命令：

useradd 增加

userdel 删除

usermod 修改

id 查

和密码相关的命令：

passwd 修改密码

chage 修改用户密码有效期限

角色：

su

sudo

visudo

组的命令：

groupadd 添加用户组

groupdel 删除用户组

小结论：  
1、 useradd添加用户会更改/etc/passwd、/etc/shadow、/etc/group、/etc/gshadow。

2、 passwd为用户设置密码会更改/etc/shadow。

与用户组相关的配置文件

/etc/group 用户组配置文件

/etc/gshadow 用户组的影子文件



**2.2** **/etc/skel 目录**

作用：用来存放新用户配置文件的目录，当我们添加新用户时，这个目录下的所有文件会自动被复制到新添加的用户的家目录下；默认情况下，/etc/skel目录下的所有文件都是隐藏文件（以.点开头的文件）；通过修改、添加、删除/etc/skel目录小的文件，我们可以为新创建的用户提供统一的、标准的、初始化用户环境。

[root@moban ~]# ls -la /home/oldboy/

总用量 28

drwx------. 2 oldboy oldboy 4096 10月 20 09:53 .

drwxr-xr-x. 7 root root 4096 10月 27 16:59 ..

-rw-------. 1 oldboy oldboy 39 10月 27 22:10 .bash\_history

-rw-r--r--. 1 oldboy oldboy 18 7月 24 02:55 .bash\_logout

-rw-r--r--. 1 oldboy oldboy 176 7月 24 02:55 .bash\_profile

-rw-r--r--. 1 oldboy oldboy 124 7月 24 02:55 .bashrc

-rw------- 1 oldboy oldboy 1605 10月 20 09:53 .viminfo

/home/xiaowan下的隐藏环境文件就是从/etc/skel拷贝的。

[root@moban /]# ls -a /home/xiaowan/

. .. .bash\_logout .bash\_profile .bashrc

企业面试题：

老男孩教育企业面试案例：请问如下登录环境故障的原理及解决办法？  
-bash-4.1$   
-bash-4.1$

[root@oldboy ~]# rm -f /home/xiaowan/.bash\*  
[root@oldboy ~]# su - xiaowan  
Welcome to oldboy training,26..  
-bash-4.1$   
-bash-4.1$

如何恢复：

法1：

-bash-4.1$ cp /etc/skel/.bash\* ~/.  
-bash-4.1$ ls -a  
.  ..  .bash\_logout  .bash\_profile  .bashrc  
-bash-4.1$ logout  
[root@oldboy ~]# su - xiaowan  
Welcome to oldboy training,26..  
[xiaowan@oldboy ~]$

法2：

[root@oldboy ~]# set|grep -i ps1  
PS1='[\u@\h \W]\$ '  
[root@oldboy ~]#   
[root@oldboy ~]#   
[root@oldboy ~]# rm -f /home/xiaowan/.bash\*  
[root@oldboy ~]# su - xiaowan  
Welcome to oldboy training,26..  
-bash-4.1$ PS1='[\u@\h \W]\$ '  
[xiaowan@oldboy ~]$ ls -a  
.  ..  
[xiaowan@oldboy ~]$ cp /etc/skel/.bash\* ~/

**2.3 /****etc/default/useradd 文件（useradd的老婆）**

/etc/default/useradd文件是在使用useradd添加用户是的一个需要调用的一个默认的配置文件，可以使用“useradd –D参数”，这样的命令格式来修改文件里面的内容。

useradd在添加用户的时候会优先读取 /etc/default/useradd文件，根据设置创建用户。

此文件可以用vim编辑，也可使用 useradd –D命令。

[root@moban /]# cat /etc/default/useradd

# useradd defaults file

GROUP=100 #-->依赖于/etc/login.defs的USERGROUPS\_ENAB参数，如果为no，则此处控制。

HOME=/home #-->把用户的家目录建在/home中。

INACTIVE=-1 #-->是否启用账号 停权，-1表示不启用。

EXPIRE= #-->账号终止日期，不设置表示不启用。

SHELL=/bin/bash #-->新用户默认所用的shell类型。

SKEL=/etc/skel #-->配置新用户家目录的默认文件存放路径。当我们用useradd添加用户是，用户家目录下的文件，都是从这里配置的目录中复制过去的。

CREATE\_MAIL\_SPOOL=yes #-->创建mail文件。

是useradd的默认配置文件。

如果useradd指定了参数，就会覆盖 /etc/default/useradd默认的配置。（参数是优先的）

**2.4 /etc/login.defs文件**

小结：

/etc/skel 的作用

/etc/default/useradd的作用

**2.5 useradd 添加用户命令**

**修改的文件：**

/etc/passwd

/etc/shadow

/etc/group

/etc/gshadow

**默认行为：**

/etc/default/useradd

/etc/login.defs

**常用参数：**

|  |  |
| --- | --- |
| **useradd参数选项** | **注释说明** |
| -e expire\_date | 账号终止日期。 |
| -g initial\_group | group名称或以数字来做为用户登入起始用户组（group）。用户组名须为系统现有存在的名称 |
| -G group[…] | 定义此用户为多个不同的groups成员。每个用户组使用“，”分隔，用户组名同-g选项的限制。默认值为用户的起始用户组。 |
| -M | 不建立用户家目录，优先于/etc/login.defs文件的设定。一般创建虚拟用户时不建立家目录，部署服务时需要创建虚拟用户。 |
| -s shell | 指定登录的shell名称。默认值为不填写，这样系统会帮你指定预设的登入shell（根据/etc/default/useradd预设的值） |
| -u uid | 用户的ID值，这个值必须是唯一的，除非用-o选项。数字不可为负数。 |
| -d home\_dir | 新账号每次登入时所使用的home\_dir。修改新用户的家目录。 |

**实例7：useradd  -c、-u、-G、-s、-d多个参数组合例子**  
自定义用户的家目录、shell类型、所归属的用户组等；  
添加用户oldboy6，并设置其用户注释信息为HandsomeBoy，UID指定为806，  
归属为用户组 root、oldboy、sa成员，其shell类型为/bin/sh，设置家目录为/oldboy6。  
实操结果为：

[root@moban ~]# useradd -c "HandsomeBoy" -u 806 -G root,oldboy,sa -s /bin/sh -d /oldboy6 oldboy6

[root@moban ~]# id oldboy6

uid=806(oldboy6) gid=806(oldboy6) 组=806(oldboy6),0(root),500(oldboy),507(sa)

**useradd –D 的用法**

说明：useradd加-D参数后，其实际效果就是改变配置文件/etc/default/useradd文件的默认值；当然，这样的修改操作也可以通过命令列编辑的方式直接修改/etc/default/useradd更新预设值。

|  |  |
| --- | --- |
| **useradd –D 参数选项** | **注释说明** |
| -b default\_home | 定义用户所属目录的前一个目录。用户名称会附加在default\_home后面用来建立新用户的目录。使用-d后则此选项无效。 |
| -e default\_expire\_date | 用户账户停止日期 |
| -f default\_inactive | 账号过期几天后停权。 |
| -g default\_group | 新账号起始用户组名或ID。用户组名须为现有存在的名称。用户组ID也须为现有存在的用户组。 |

**实例：useradd –g –M –e 多个参数组合例子**

添加一个用户oldboy7，属于sa组，不创建家目录，2015/10/31用户过期。

[root@oldboy ~]# groupadd sa  
[root@oldboy ~]# useradd oldboy7 -g sa -M -e "2015/10/31"  
[root@oldboy ~]# ls /home/oldboy7  
ls: 无法访问/home/oldboy7: 没有那个文件或目录  
[root@oldboy ~]# id oldboy7  
uid=807(oldboy7) gid=807(sa) 组=807(sa)  
[root@oldboy ~]# chage -l oldboy7  
Last password change                                    : Oct 27, 2015  
Password expires                                        : never  
Password inactive                                       : never  
Account expires                                         : Oct 31, 2015  
Minimum number of days between password change          : 0  
Maximum number of days between password change          : 99999  
Number of days of warning before password expires       : 7  
  
测试过期-e：  
Your account has expired; please contact your system administrator

Chage –l 查看用户时间信息

[root@oldboy ~]# useradd -D -s /bin/bash  
[root@oldboy ~]# cat /etc/default/useradd   
# useradd defaults file  
GROUP=100  
HOME=/home  
INACTIVE=-1  
EXPIRE=  
SHELL=/bin/bash  
SKEL=/etc/skel  
CREATE\_MAIL\_SPOOL=yes

Useradd默认配置文件 /etc/default/useradd

-u 指定uid

-s 指定登录shell

-M 不创建家目录

-g 指定所属组

-e 指定过期时间

-D 修改/etc/default/useradd文件

Usermod用户信息修改相关命令

参数：

|  |  |
| --- | --- |
| **Usermod参数选项** | **注释说明** |
| -c comment | 注释（第五栏） |
| -d home\_dir | 更改家目录 |
| -e expire\_date | 修改时间 （账户过期） |
| -f inactive\_days | 设置停权时间 |
| -g initial\_group | 修改所属的组 |
| -G group[..] | 修改多个组 |
| -s shell | 修改shell |
| -u uid | 修改uid |
| -L | 冻结用户的密码 |
| -U | 取消冻结用户的密码 |

useradd oldboy6 -c "Handsomeboy" -u 806 -s /bin/sh -d /oldboy6 -G root,oldboy  
   
  
[root@oldboy ~]# usermod -c "boy" -u 888 -s /sbin/nologin -d /home/oldboy8 -G oldboy oldboy6   
  
[root@oldboy ~]# grep oldboy6 /etc/passwd   
oldboy6:x:888:806:boy:/home/oldboy8:/sbin/nologin

[root@oldboy ~]# usermod oldboy7 -g oldboy -d /tmp -e "2015/12/31"  
usermod: user '2015/12/31' does not exist  
[root@oldboy ~]# usermod -g oldboy -d /tmp -e "2015/12/31" oldboy7  
[root@oldboy ~]# id oldboy7  
uid=807(oldboy7) gid=500(oldboy) 组=500(oldboy)  
[root@oldboy ~]# grep oldboy7 /etc/passwd  
oldboy7:x:807:500::/tmp:/bin/tcsh  
[root@oldboy ~]# chage -l oldboy7  
Last password change                                    : Oct 27, 2015  
Password expires                                        : never  
Password inactive                                       : never  
Account expires                                         : Dec 31, 2015  
Minimum number of days between password change          : 0  
Maximum number of days between password change          : 99999  
Number of days of warning before password expires       : 7

Userdel 删除用户

参数：-r 删除家目录

删除用户的两种方法：

#a3:x:510:511::/home/a3:/bin/tcsh  
a4:x:511:512::/home/a4:/bin/bash  
"/etc/passwd" 35L, 1472C 已写入                             
[root@oldboy ~]#   
[root@oldboy ~]# su - a3  
su: 用户a3 不存在  
[root@oldboy ~]# usermod a4 -s /sbin/nologin   
usermod: user '/sbin/nologin' does not exist  
[root@oldboy ~]# usermod -s /sbin/nologin a4   
[root@oldboy ~]# su - a4  
This account is currently not available.

删除用户的经验：

1. 不要带-r
2. 修改/etc/passwd注释。
3. 使用usermod –s /sbin/nologin

集中用户管理：

活动目录AD，LADP服务。

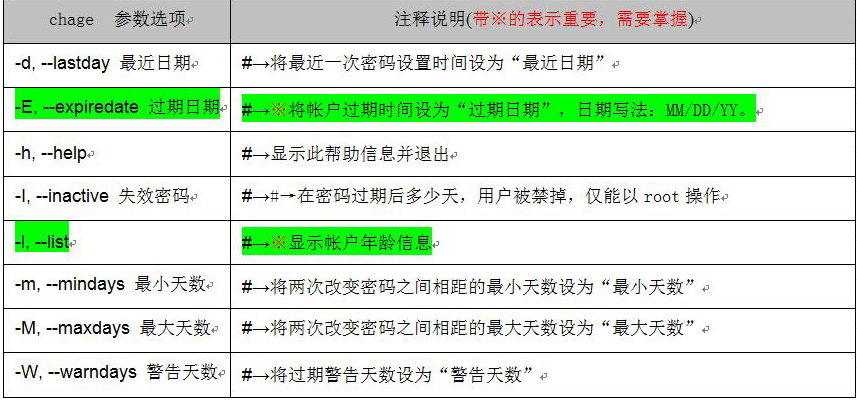
密码：动态密码。

ID 打印真实的用户的组uid和gid

[root@oldboy ~]# id -g  
0  
[root@oldboy ~]# id –u 查看uid  
0  
[root@oldboy ~]# id -u oldboy  
500  
[root@oldboy ~]# id -g oldboy 查看gid  
506  
[root@oldboy ~]# id -gn oldboy 查看组名  
incahome  
[root@oldboy ~]# id -un oldboy 查看用户名  
oldboy  
[root@oldboy ~]# id oldboy  
uid=500(oldboy) gid=506(incahome) 组=506(incahome)

chage 修改用户密码有效期限（针对密码的）

-E 过期日期，将账户过期时间设为



Usermod –e 修改用户密码时间期限。

[root@oldboy ~]# usermod -e "2015/11/11" oldboy7 修改用户密码时间期限  
[root@oldboy ~]# chage -l oldboy7         查看用户时间期限      
Last password change                                    : Oct 31, 2015  
Password expires                                        : never  
Password inactive                                       : never  
Account expires                                         : Nov 11, 2015  
Minimum number of days between password change          : 0  
Maximum number of days between password change          : 99999  
Number of days of warning before password expires       : 7  
[root@oldboy ~]# chage -E "2015/12/31" oldboy7 修改用户密码时间期限  
[root@oldboy ~]# chage -l oldboy7               
Last password change                                    : Oct 31, 2015  
Password expires                                        : never  
Password inactive                                       : never  
Account expires                                         : Dec 31, 2015  
Minimum number of days between password change          : 0  
Maximum number of days between password change          : 99999  
Number of days of warning before password expires       : 7

案例：

oldgirl用户7天内不能更改密码，60天以后必须修改密码，过期前提前10天通知oldgirl用户，过期后30天后禁止用户登陆。

chage  -m7 -M60 -W10 -I30 oldgirl  
passwd -n7 -x60 -w10 -i30 oldgirl  
  
[root@oldboy ~]# chage  -m7 -M60 -W10 -I30 oldgirl  
[root@oldboy ~]# chage -l oldgirl  
Last password change                                    : Oct 23, 2015  
Password expires                                        : Dec 22, 2015  
Password inactive                                       : Jan 21, 2016  
Account expires                                         : never  
Minimum number of days between password change          : 7  
Maximum number of days between password change          : 60  
Number of days of warning before password expires       : 10  
  
[root@oldboy ~]# passwd -n8 -x61 -w11 -i31 oldgirl    
调整用户密码老化数据oldgirl。  
passwd: 操作成功  
[root@oldboy ~]# chage -l oldgirl                   
Last password change                                    : Oct 23, 2015  
Password expires                                        : Dec 23, 2015  
Password inactive                                       : Jan 23, 2016  
Account expires                                         : never  
Minimum number of days between password change          : 8  
Maximum number of days between password change          : 61  
Number of days of warning before password expires       : 11

passwd的参数：



groupadd 添加用户组命令

与groupadd命令有关的文件有：

/etc/group -用户组相关文件

/etc/gshadow -用户组加密相关文件

默认行为：

/etc/login.defs

实用参数： -g ，指定用户组GID值。

[root@moban oldboy]# groupadd sa2 -g 888 创建一个组，这个组的GID值为888

[root@moban oldboy]# grep sa2 /etc/group 查看相应的信息

sa2:x:888:

groupdel 删除

当组里面还有组员的时候，使用groupdel是无法删除这个组的。

**用户管理命令小结：**

1、和用户相关的配置文件知识点：

/etc/passwd账号文件及不同列内容

/etc/shadow账号密码文件及不同列内容

/etc/group组的文件及不同列内容

/etc/gshadow组密码文件及不同列内容

2、用户管理命令

Useradd –u –G –s –M –e –c –d

对应/etc/skel，/etc/default/useradd，/etc/login.defs

userdel –r

usermod –u –g –G –s –M –e –c –d –L –U –I

id

change –l –E –M –W –m –I

passwd –stdin –n –i –w –x (suid为重点)

su

sudo

visudo

3、组管理命令

groupadd –g

groupdel

groupmod

**2.6** **用户查询相关命令id、finger、users、w、who、last、lastlog、groups**

w ：查看谁登录了系统。（显示谁已经登录了，并且他在干什么）

[root@moban ~]# w

21:36:08 up 1 day, 14:43, 1 user, load average: 0.00, 0.00, 0.00

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

oldboy pts/0 10.0.0.1 21:31 0.00s 0.04s 0.05s sshd: oldboy [priv]

用户 终端 IP地址 登录时间 空闲时间

who 只是看谁登录了系统。（who被w包含了）

[root@moban ~]# who

oldboy pts/0 2015-10-28 21:31 (10.0.0.1)

users 只显示谁登录了。（users被who包含了。。只显示用户名）

[root@moban ~]# users

oldboy

last 显示已登录的用户列表及登录时间等。查看的信息和/var/log/wtmp及/var/log/btmp两个文件有关

[root@moban ~]# last

oldboy pts/0 10.0.0.1 Wed Oct 28 21:31 still logged in

oldboy pts/0 10.0.0.1 Wed Oct 28 19:34 - 21:31 (01:56)

oldboy pts/1 10.0.0.1 Wed Oct 28 15:26 - 16:27 (01:01)

oldboy pts/0 10.0.0.1 Wed Oct 28 12:54 - 15:27 (02:32)

oldboy pts/0 10.0.0.1 Tue Oct 27 23:01 - 12:45 (13:44)

oldboy pts/1 10.0.0.1 Tue Oct 27 21:55 - 22:10 (00:15)

oldboy pts/0 10.0.0.1 Tue Oct 27 21:37 - 23:00 (01:23)

oldboy pts/0 10.0.0.1 Tue Oct 27 19:39 - 21:37 (01:58)

lastlog 报告最近的所有系统用户的登录信息。查看的信息和/var/log/lastlog日志有关。

[root@moban ~]# lastlog

用户名 端口 来自 最后登陆时间

root tty1 一 10月 12 20:31:58 +0800 2015

oldboy pts/0 10.0.0.1 三 10月 28 21:31:49 +0800 2015

bin \*\*从未登录过\*\*

daemon \*\*从未登录过\*\*

adm \*\*从未登录过\*\*

lp \*\*从未登录过\*\*

sync \*\*从未登录过\*\*

shutdown \*\*从未登录过\*\*

halt \*\*从未登录过\*\*

mail \*\*从未登录过\*\*

uucp \*\*从未登录过\*\*

operator \*\*从未登录过\*\*

games \*\*从未登录过\*\*

查看文件为何格式的命令如下：

[root@moban ~]# file /var/log/lastlog

/var/log/lastlog: data 为普通文件中的数据文件，特殊格式的数据文件

[root@moban ~]# file /var/lib/mlocate/mlocate.db

/var/lib/mlocate/mlocate.db: data 为普通文件中的数据文件，特殊格式的数据文件

groups 查询所归属的用户组

[root@moban ~]# groups oldboy

oldboy : oldboy

[root@moban ~]# groups

root

newgrp 用户更改自己的有效用户组（只能在当前用户下做更改，只是临时生效。）

[root@moban ~]# id oldboy

uid=500(oldboy) gid=500(oldboy) 组=500(oldboy),504(sa)

[root@moban ~]# su - oldboy

[oldboy@moban ~]$ newgrp sa

[oldboy@moban ~]$ groups

sa oldboy

**3、用户身份切换**

**3.1 su命令介绍**

su命令就是切换用户身份的命令。

常用参数：

|  |  |
| --- | --- |
| **su参数选项** | **注释说明** |
| * -l --login | 是一个shell称为登录的shell，如执行su – oldboy时，表示该用户想改变身份为oldboy，并且使用oldboy用户的环境变量配置，如：  /home/oldboy/.bash\_profile等。 |
| -c –command=COMMAND | 切换到一个shell下，执行后一个命令，然后退出所切换的用户环境。 |
| -m –preserve-environment | 切换用户是，不重置用户环境变量。 |
| -s –shell=SHELL | 如果/etc/shells允许，则运行指定的shell |

su – c （以其他用户身份直接创建文件或执行程序）

[root@oldboy ~]# su - oldboy -c " touch a1"   
[root@oldboy ~]# ls -l /home/oldboy/a1  
-rw-rw-r--. 1 oldboy oldboy 0 Oct 29 10:11 /home/oldboy/a1

[root@moban ~]# su - oldboy -c pwd

/home/oldboy

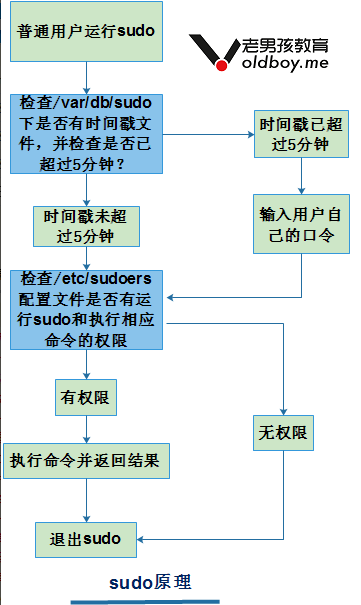
########分用户方案启动服务命令########  
su - tddoc  -c '/bin/sh /home/tddoc/bin/deploy.sh'

su的优点：任意普通用户切换到root用户下（需要root的密码）。

su的缺点：权限太大（拥有root权限），可以随意删除修改文件目录等。

**3.2 sudo命令介绍**

1. 普通用户必须知道root密码才可以切换到root，这样root密码具泄露了。相当于把“刀把”给了别人。
2. 使用su命令切换身份，无法对切换后的身份做精细的控制，拿到超级权限



如果在普通用户oldboy下想创建或删除用户如何做：

[root@moban ~]# useradd a1

[root@moban ~]# su - oldboy

[oldboy@moban ~]$ useradd old

-bash: /usr/sbin/useradd: 权限不够

[oldboy@moban ~]$ userdel a1

-bash: /usr/sbin/userdel: 权限不够

[oldboy@moban ~]$ su -

密码：

[root@moban ~]# visudo 切记加命令时需要全路径，两条命令后要加”，”逗号，后面还要有空格。

root ALL=(ALL) ALL

oldboy ALL=(ALL) /usr/sbin/useradd, /usr/sbin/userdel

[root@moban ~]# su - oldboy

[oldboy@moban ~]$ sudo useradd old 切换到普通用户是想要执行命令需加sudo带兵符

[sudo] password for oldboy:

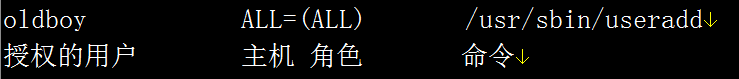
[oldboy@moban ~]$ tail -l /etc/passwd

old:x:502:502::/home/old:/bin/bash

|  |  |
| --- | --- |
| **sudo参数选项** | **注释说明** |
| -l | 列出用户在主机上可用的和被禁止的命令；当配置好sudo授权规则后，可用这个参数来查看授权情况。 |
| -v | 验证用户的时间戳；当用户运行sudo，输入用户的密码后，在短时间内可以不用输入口令直接进行sudo操作；用-v可以跟踪最新的时间戳 |
| -u | 指定以某个用户身份执行特定的命令操作。Oldboy ALL=(ALL) /bin/cp |
| -k | 同-K，删除时间戳，下一个sudo命令要求提供密码。前提是该用户授权中不能有NOPASSWD：参数。时间戳默认5分钟也会失效。 |

sudo总结：

1. sudo –l 检查被授予的权限。
2. 第二次执行命令时（没有超过五分钟，时间戳问题）即可不用输入密码。
3. sudo –K 清除时间戳（普通用户执行命令时需输入普通用户密码）；授权NOPASSWD执行命令时就不用输入密码了。
4. 编辑sudo时尽量不要使用echo，要使用visudo，可以帮助检查语法是否支持。



给组授权：

##Allows people in group sa to run all commands

%sa ALL=（ALL） ALL

批量管理的时候：

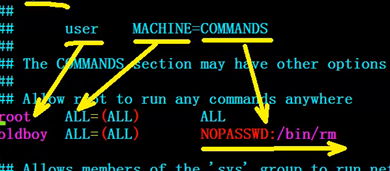
echo “%sa ALL=(ALL) ALL” >>/etc/sudoers

visudo –c

改好/etc/sudoers推送所有服务器

[root@moban ~]# ll /etc/sudoers

-r--r-----. 1 root root 4057 9月 25 04:09 /etc/sudoers

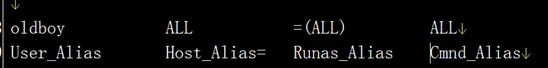


User代表用户。MACHINE代表机器 COMMANDS代表可执行的命令。

oldboy ALL =(ALL) ALL

User\_Alias host\_Alias Runas\_Alias Cmnd\_Alias

用户 主机名 获得谁的权限 使用什么命令

****

1、User\_Alias定义用户别名 （对应的用户位置）

19 ## rather than USERALIAS

20 ## User\_Alias ADMINS = jsmith, mikem

2、 Host\_Alias 定义主机别名 （对应的第一个ALL）

13 ## Host\_Alias FILESERVERS = fs1, fs2 #---请注意定义规范：

14 ## Host\_Alias MAILSERVERS = smtp1, smtp2 #---请注意定义规范：

1. Runas\_Alias 定义runas角色别名

Runas\_Alias OP=root,oldboy

4、Cmnd\_Alias 定义命令别名（对应最后边的ALL此处可以写入多个命令）

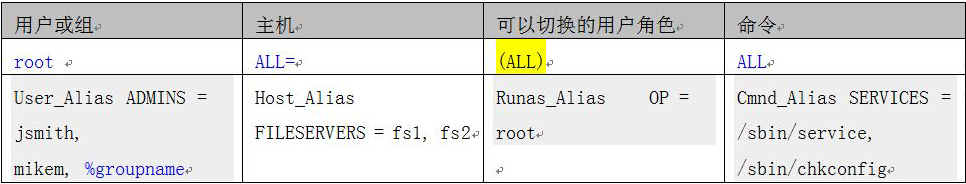
27 # Cmnd\_Alias NETWORKING = /sbin/route, /sbin/ifconfig,

/bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptabl

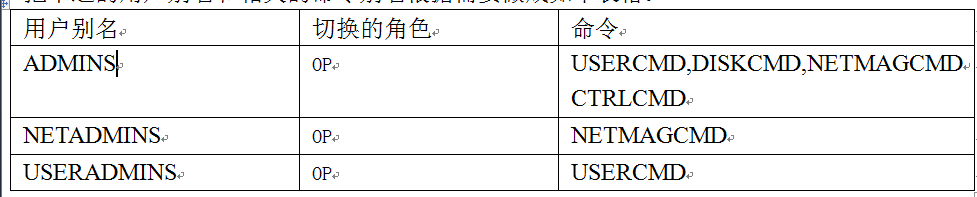
es, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig,

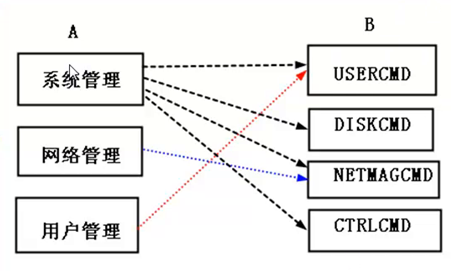
/sbin/mii-tool

**人生中第一个项目：**



实例：现有一些数据，根据如下的数据，测试结果是否正确。





User\_Alias ADMINS = oldboy, ett, %sa  
User\_Alias NETADMINS = leo, maya  
User\_Alias USERADMINS = zuma  
  
Cmnd\_Alias  USERCMD = /usr/sbin/useradd, /usr/sbin/userdel, \  
/usr/bin/passwd [A-Za-z]\*, /bin/chown, /bin/chmod  
Cmnd\_Alias   DISKCMD = /sbin/fdisk, /sbin/parted  
Cmnd\_Alias   NETMAGCMD = /sbin/ifconfig, /etc/init.d/network  
Cmnd\_Alias   CTRLCMD = /usr/sbin/reboot, /usr/sbin/halt   
  
Runas\_Alias  OP = root, oldboy  
  
## The COMMANDS section may have other options added to it.  
ADMINS       ALL=(ALL)   USERCMD, NETMAGCMD, CTRLCMD, DISKCMD  
NETADMINS     ALL=(OP)   NOPASSWD: NETMAGCMD  
USERADMINS    ALL=(OP)   NOPASSWD: USERCMD

首先将测试数据放入到visudo最末行中

[root@moban ~]# su - oldboy

[oldboy@moban ~]$ sudo -l

[sudo] password for oldboy:

匹配此主机上 oldboy 的默认条目：

requiretty, !visiblepw, always\_set\_home, env\_reset,

env\_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC

KDEDIR LS\_COLORS", env\_keep+="MAIL PS1 PS2 QTDIR

USERNAME LANG LC\_ADDRESS LC\_CTYPE",

env\_keep+="LC\_COLLATE LC\_IDENTIFICATION

LC\_MEASUREMENT LC\_MESSAGES", env\_keep+="LC\_MONETARY

LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE",

env\_keep+="LC\_TIME LC\_ALL LANGUAGE LINGUAS

\_XKB\_CHARSET XAUTHORITY",

secure\_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 oldboy 可以在该主机上运行以下命令：

(ALL) /usr/sbin/useradd, /usr/sbin/userdel,

/usr/bin/passwd [A-Za-z]\*, /bin/chown, /bin/chmod,

(ALL) /sbin/ifconfig, /etc/init.d/network, (ALL)

/usr/sbin/reboot, /usr/sbin/halt, (ALL) /sbin/fdisk,

/sbin/parted

[oldboy@moban ~]$ su -

密码：

[root@moban ~]# useradd maya

[root@moban ~]# passwd maya

更改用户 maya 的密码 。

新的 密码：

无效的密码： WAY 过短

无效的密码： 是回文

重新输入新的 密码：

passwd： 所有的身份验证令牌已经成功更新。

[root@moban ~]# su - maya

[maya@moban ~]$ sudo -l

匹配此主机上 maya 的默认条目：

requiretty, !visiblepw, always\_set\_home, env\_reset,

env\_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC

KDEDIR LS\_COLORS", env\_keep+="MAIL PS1 PS2 QTDIR

USERNAME LANG LC\_ADDRESS LC\_CTYPE",

env\_keep+="LC\_COLLATE LC\_IDENTIFICATION

LC\_MEASUREMENT LC\_MESSAGES", env\_keep+="LC\_MONETARY

LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE",

env\_keep+="LC\_TIME LC\_ALL LANGUAGE LINGUAS

\_XKB\_CHARSET XAUTHORITY",

secure\_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 maya 可以在该主机上运行以下命令：

(root, oldboy) NOPASSWD: /sbin/ifconfig,

/etc/init.d/network

[maya@moban ~]$ su -

密码：

[root@moban ~]# groupadd sa

[root@moban ~]# useradd lifen -g sa

[root@moban ~]# passwd lifen

更改用户 lifen 的密码 。

新的 密码：

无效的密码： WAY 过短

无效的密码： 过于简单

重新输入新的 密码：

passwd： 所有的身份验证令牌已经成功更新。

[root@moban ~]# su - lifen

[lifen@moban ~]$ sudo -l

We trust you have received the usual lecture from the local System

Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.

#2) Think before you type.

#3) With great power comes great responsibility.

[sudo] password for lifen:

匹配此主机上 lifen 的默认条目：

requiretty, !visiblepw, always\_set\_home, env\_reset,

env\_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC

KDEDIR LS\_COLORS", env\_keep+="MAIL PS1 PS2 QTDIR

USERNAME LANG LC\_ADDRESS LC\_CTYPE",

env\_keep+="LC\_COLLATE LC\_IDENTIFICATION

LC\_MEASUREMENT LC\_MESSAGES", env\_keep+="LC\_MONETARY

LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE",

env\_keep+="LC\_TIME LC\_ALL LANGUAGE LINGUAS

\_XKB\_CHARSET XAUTHORITY",

secure\_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 lifen 可以在该主机上运行以下命令：

(ALL) /usr/sbin/useradd, /usr/sbin/userdel,

/usr/bin/passwd [A-Za-z]\*, /bin/chown, /bin/chmod,

(ALL) /sbin/ifconfig, /etc/init.d/network, (ALL)

/usr/sbin/reboot, /usr/sbin/halt, (ALL) /sbin/fdisk,

/sbin/parted

[lifen@moban ~]$ su -

密码：

[root@moban ~]# useradd zuma

[root@moban ~]# su - zuma

[zuma@moban ~]$ sudo -l

匹配此主机上 zuma 的默认条目：

requiretty, !visiblepw, always\_set\_home, env\_reset,

env\_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC

KDEDIR LS\_COLORS", env\_keep+="MAIL PS1 PS2 QTDIR

USERNAME LANG LC\_ADDRESS LC\_CTYPE",

env\_keep+="LC\_COLLATE LC\_IDENTIFICATION

LC\_MEASUREMENT LC\_MESSAGES", env\_keep+="LC\_MONETARY

LC\_NAME LC\_NUMERIC LC\_PAPER LC\_TELEPHONE",

env\_keep+="LC\_TIME LC\_ALL LANGUAGE LINGUAS

\_XKB\_CHARSET XAUTHORITY",

secure\_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 zuma 可以在该主机上运行以下命令：

(root, oldboy) NOPASSWD: /usr/sbin/useradd,

/usr/sbin/userdel, /usr/bin/passwd [A-Za-z]\*,

/bin/chown, /bin/chmod

**sudo配置文件/etc/sudoers授权规则注意事项总结：**

1. 授权规则中的所有ALL字符串必须为大写字母
2. 禁止的命令要放在后面。例：/usr/sbin/\*，/sbin/\*，!/usr/sbin/visudo，!/sbin/fdisk
3. 一行内容超长可以用“\”斜线换行。

**如果想远程连接使用sudo命令的话，需要使用ssh –t 命令**

[root@oldboy ~]# su - oldboy  
[oldboy@oldboy ~]$ ssh 10.0.0.7 sudo /sbin/parted /dev/sda  
The authenticity of host '10.0.0.7 (10.0.0.7)' can't be established.  
RSA key fingerprint is 23:f8:a2:36:96:9f:bf:ab:57:db:c8:44:fd:6b:e0:97.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.0.7' (RSA) to the list of known hosts.  
oldboy@10.0.0.7's password:   
sudo: sorry, you must have a tty to run sudo  
[oldboy@oldboy ~]$ ssh -t 10.0.0.7 sudo /sbin/parted /dev/sda  
oldboy@10.0.0.7's password:   
GNU Parted 2.1  
Using /dev/sda  
Welcome to GNU Parted! Type 'help' to view a list of commands.  
(parted) p                                                                  
Model: VMware, VMware Virtual S (scsi)  
Disk /dev/sda: 8590MB  
Sector size (logical/physical): 512B/512B  
Partition Table: msdos  
  
Number  Start   End     Size    Type     File system     Flags  
 1      1049kB  211MB   210MB   primary  ext4            boot  
 2      211MB   1016MB  805MB   primary  linux-swap(v1)  
 3      1016MB  8590MB  7574MB  primary  ext4  
  
(parted)

有关sudo参考资料：  
1)/etc/sudoers  
2)man sudoers  
3)man sudo

sudo 控制用户能干什么，不能干什么

用户审计 日志审计 任何用户执行的任何操作都记录（可以录像和回放）

法1）通过环境变量命令及rsyslog服务进行全部日志审计（信息太大，不推荐）

法2）sudo配合rsyslog服务，进行日志审计（审计信息较少，效果不佳）

法3）在bash解释器程序里嵌入一个监视器，让所有被审计的系统用户使用修改过的增加了

配置/etc/sudoers

增加一行sudo的日志

Defaults logfile=/var/log/sudo.log 增加日志到visudo最后一行中。

[root@moban ~]# su - oldboy

[oldboy@moban ~]$ sudo rm -fr /root/data

[sudo] password for oldboy:

对不起，用户 oldboy 无权以 root 的身份在 moban 上执行 /bin/rm -fr /root/data。

[oldboy@moban ~]$ logout

[root@moban ~]# cat /var/log/sudo.log

Sep 25 06:06:39 : oldboy : 命令禁止使用 ; TTY=pts/1 ; PWD=/home/oldboy ;

USER=root ; COMMAND=/bin/rm -fr /root/data

收集日志的好博文

日志相关：rsyslog,Awstats,flume logstash scribe kafka,storm，ELK(Elasticsearch+Logstash+Kibana)

http://oldboy.blog.51cto.com/2561410/775056

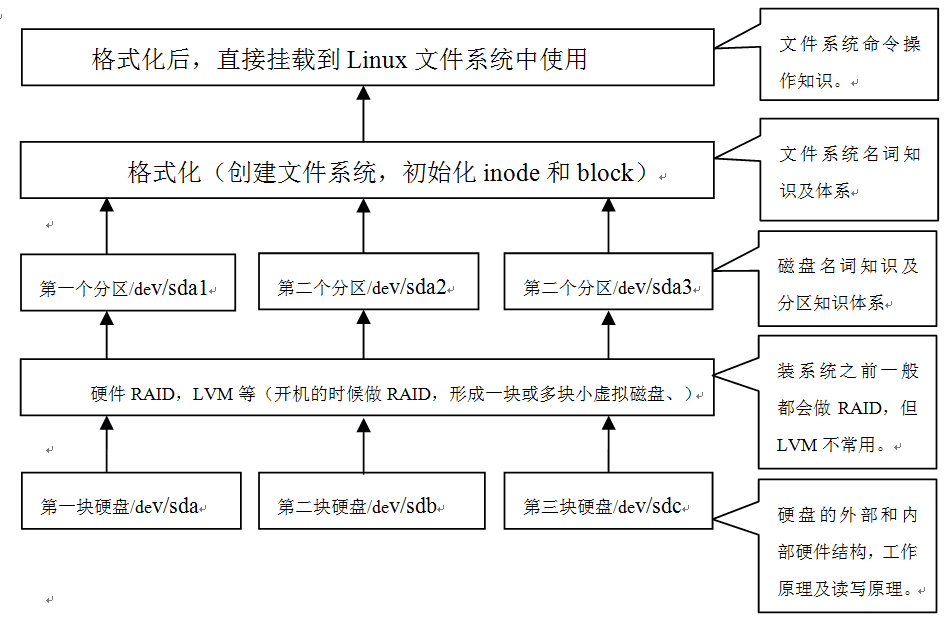
4、有关磁盘管理的知识

**4.1磁盘的历史介绍：**

1956年9月IBM想世界展示了第一台磁盘存储西乡塘IBM 350 RAMAC至今，磁盘存储系统已经历了近半个世纪的发展。最早的RAMAC容量只有5MB，然后却需要使用50个直径为24英寸的磁盘。而现在的一块容量高达100GB的磁盘，仅仅只需3张磁盘片（3.5寸盘）即可。

IBM 350 RAMAC可以说是磁盘的鼻祖，现代磁盘的真正原型是1973年IBM公司推出的Winchester（温氏）磁盘，它的特点：磁盘在工作时，磁头悬浮在告诉转动的磁盘盘片上方，而不是与盘片直接接触。磁盘在工作时，磁头沿高速旋转的盘片上方做径向移动。这便是当今所有磁盘的雏形。现代的磁盘容量虽然更大了，但是依然在沿用“温彻斯特”的动作模式，称这种磁盘为机械式磁盘。

|  |  |
| --- | --- |
| **发展趋势：** | **实现措施：** |
| 体积更小 | 存储密度更高 |
| 速度更快 | 读写更灵敏的磁头，主轴转数更快，接口更先进了 |
| 容量更大 | 存储密度更高 |
| 使用更安全 | 数据保持技术 |



**4.2磁盘的外部结构**

磁盘的作用：

磁盘的最主要用途就是用来存储日常工作、学习、生活中的数据的，例如：照片、视频、工作文档等。

[root@moban ~]# free –m 查看内存信息的命令

total used free shared buffers cached

Mem: 992 736 255 0 53 446

-/+ buffers/cache: 236 756 剩余内存

Swap: 767 0 767

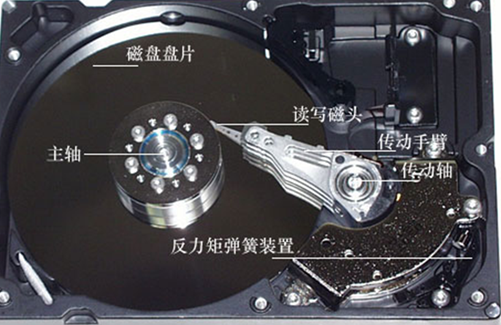
#####缓存无处不在#####

提示：

1. Linux系统的特性是将系统不用的物理内存缓存起来，因此255不是系统的真实内存。
2. 系统真正可用内存是756M。
3. buffers为写入缓冲区，sync将缓冲区数据写入磁盘。
4. cache为读取数据的缓存区。
5. 硬盘是机械的，无论是写入还是读取都很慢，所以读取和写入都是用了缓存技术。
6. 门户架构网站都会用缓存技术，来让用户写入读取尽可能不接触磁盘。

**4.3 磁盘的内部结构**

磁盘的内部结构主要包括：盘片、磁头、盘片主轴、控制电机、磁头控制器、数据转换器、接口、缓存等几个部分。所有的盘片都有固定在一个旋转轴上，这个轴即盘片主轴。而所有的盘片之间是平行的，在每个盘片（一个盘片两个盘面）的每个存储面上都有一个磁头，磁头与盘片之间的距离比头发丝的直径还小很多倍。所有的磁头（一个有效盘面就有一个磁头）连载一个磁头控制器上，由磁头控制器负责各个磁头的运动。磁头可沿盘片的半径方向做径向运动（就是沿着半径由圆心到圆周线做直线运动）。



1. 磁头组件：它是由读写磁头、传动手臂、传动轴三部分组成。磁头是磁盘技术中最重要和关键的一环。实际上是集成工艺制成的多个磁头的组合，它采用了非接触式头、盘结构，加电后在高速旋转的磁盘表面移动，与盘片之间的间隙只有0.1~0.3um(微米)，这样可以获得很好的数据传输率。现在转速为7200RPM的磁盘飞高一般都低于0.3um，以利于读取较大的高信噪比信号，确保数据传输可靠性。

磁盘读取数据的工作原理是利用特定的磁粒子的极性来记录数据。磁头在读取数据时，将磁粒子的不同极性转成不同的电脉冲信号，在利用数据转换器将这些原始信号变成电脑可以使用的数据，写的操作正好与此相反。

2）磁头驱动装置。磁盘的寻道是靠移动磁头，而移动磁头则需要该装置驱动才能实现（机械操作）。磁头驱动装置由电磁线圈电机、磁头驱动小车、防震动装置构成，高精度的轻型磁头驱动装置能够对磁头进行正确的驱动和定位，并能在很短的时间内精确定位系统指令指定的磁道。

磁盘接口分为IDE、SATA、SCSI和光纤FC通道四种

3） 磁盘片，盘片是磁盘存储数据的真正载体，磁盘盘片大多采用金属薄膜材料。（也有玻璃材料），这种金属薄膜较软盘的不连续颗粒载体具有更高的存储密度、高剩磁及高矫顽力等优点。

4）主轴组件。主轴组件包括如轴承和驱动电机等。随着磁盘容量的扩大和速度的提高，主轴电机的速度也在不断提升，有厂商开始采用精密机械工业的液态轴承电机技术。例如希捷公司的酷鱼ATAIV就是采用此电机技术。这样也有利于降低磁盘工作噪音。

**4.4 磁盘的类型与区别**

**IDE磁盘与IDE接口**

IDE英文全称为“integrated drive electronics”，即电子集成驱动器，本意是指把“磁盘控制器”与“盘体”集成在一起的磁盘驱动器。

主板IDE接口



磁盘IDE接口



**SATA磁盘与SATA接口**

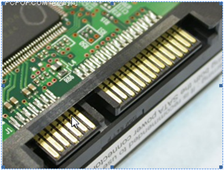
使用SATA（serial ATA）口的磁盘又叫串口磁盘，当前PC机磁盘的主流。2001年由Intel、apt、Dell、IBM、希捷、迈拓这几大厂商徐成的serial ATA委员会正式确立了serial ATA 1.0规范。

性能：可靠、简单、热插拔、性能高。

主板SATA接口



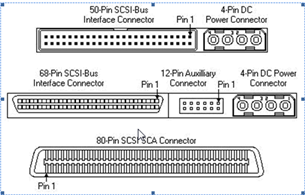
磁盘上的SATA接口



**SCSI磁盘与SCSI接口**

全称“small computer system interface”（小型计算机系统接口），和IDE（ATA）是完全不同的接口，IDE接口是早起普通PC的标准接口，而SCSI并不是专门为磁盘设计的接口，是一种广泛应用于小型机上的高速数据传输技术。SCSI接口具有应用范围广、多任务、带宽大、CPU占用率低，以及热插拔等优点，因较高的价格使得它很难如IDE磁盘般普及，因此，早几年的SCSI磁盘主要应用于中、高端服务器和高档工作站中。

SCSI接口模拟图：



说明：我们在使用VMWARE做虚拟化时发现选择的就是SCSI接口模式。

SAS 骡子

SATA 马

SCSI 驴

**SAS磁盘与SAS接口**

是新一代的SCSI技术，和现在流行的serial ATA（SATA）磁盘相同，都是采用串口技术以获得更高的传输速度，并通过缩短连线改善内部空间等。此接口的设计是为了改善存储系统的效能、可用性和扩张性。

SAS技术的优势：

SAS技术与SAS磁盘是在人们希望SATA与SCSI接口共同优势基础上诞生的。

1. SAS技术降低了磁盘阵列的成本。
2. 串行接口让传输性能提高。
3. 更好的扩展性能

SCSI接口的扩展性能一般，最多只能连接15个（单通道）或者30个（双通道）设备。而SAS接口结构有非常好的扩展能力，最多可以连接16384个磁盘设备。

1. 安装更简单
2. 更好的兼容性

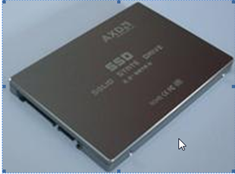
总体来说SAS技术是结合了SATA与SCSI两者的优点而诞生的，同时串行SCSI（SAS）是点到点的结构，因此除了提高性能之外，每个设备连接到指定的数据通路上提高了带宽，从而为数据传输与存取提供了必要保障。

serial-Attached SCSI（SAS）

企业生产环境主流磁盘的相关信息对比：  
企业生产场景普及程度：SAS>SATA>SSD  
单位容量对比性能和价格：SSD>SAS>SATA（一块SSD，和一块SATA）  
单位价格购买磁盘容量：SATA>SAS>SSD

SSD磁盘

固态磁盘（Solid State Drive、IDE FLASH DISK）



新一代的固态磁盘普遍采用SATA-2接口及SATA-3接口。

SLC（Single Layer Cell 单层单元）和MLC（Multi-Level Cell多层单元）

固态盘的优点：速度快

缺点：成本高，容量低，写入数量有限



重要优势：随机存取速度，功耗，防震，重量方面优势很大，特别是存取性能。  
重要缺点：容量低、价格高、写寿命有限，数据恢复难。

**生产环境磁盘的选型和应用案例**

服务器的选型

DELL，HP，IBM等，其中DELL，HP是互联网公司的主流服务器，这两个品牌的服务器综合的性价比较高。

磁盘选型：

主流磁盘为SAS、SATA、SSD等。

1. 企业级SAS磁盘

企业里常见的SAS硬盘是15000转/分

用途：用于提供生产线上的普通对外提供服务的业务服务器。

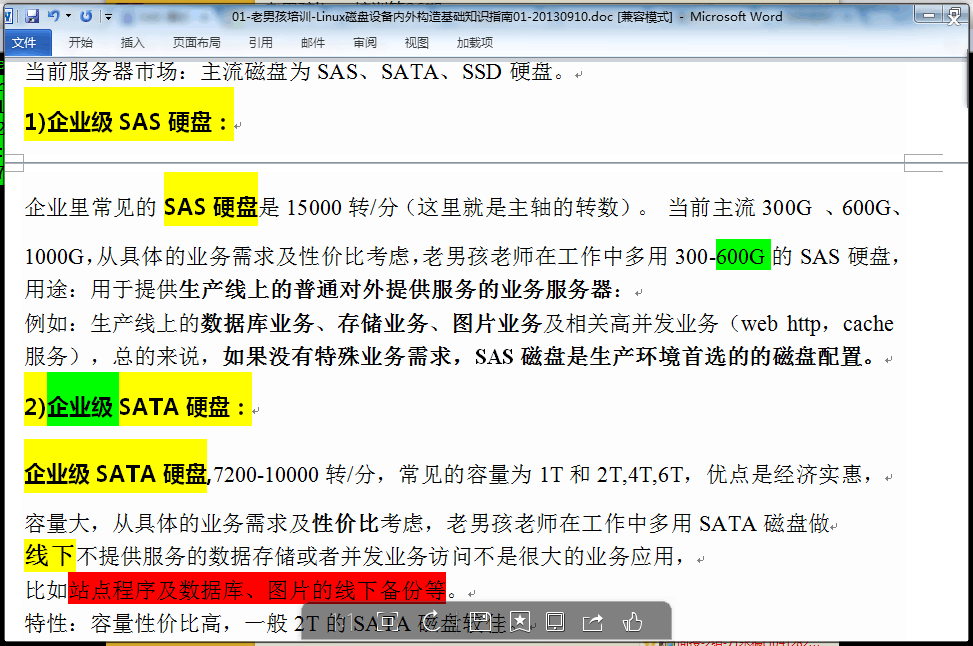
例如：数据库业务、存储业务、图片业务及相关高并发业务。总的来说，如果没有特殊业务需求，SAS磁盘是生产环境首选的磁盘配置。

1. 企业级SATA硬盘：

企业级SATA硬盘，7200-10000转/分，常见的容量为1T和2T，4T，6T，优点是经济实惠，容量大，从具体的业务需求及性价比考虑，在工作中多用SATA磁盘做。

磁盘选购小结：

1. 线上的业务，用SAS磁盘。
2. 线下的业务，用SATA磁盘，磁带库备份。
3. 线上高并发，小容量的业务，SSD磁盘。
4. 思想：根据数据的访问热度，只能分析分层存储。SATA+SSD。



磁盘的知识及读写原理：

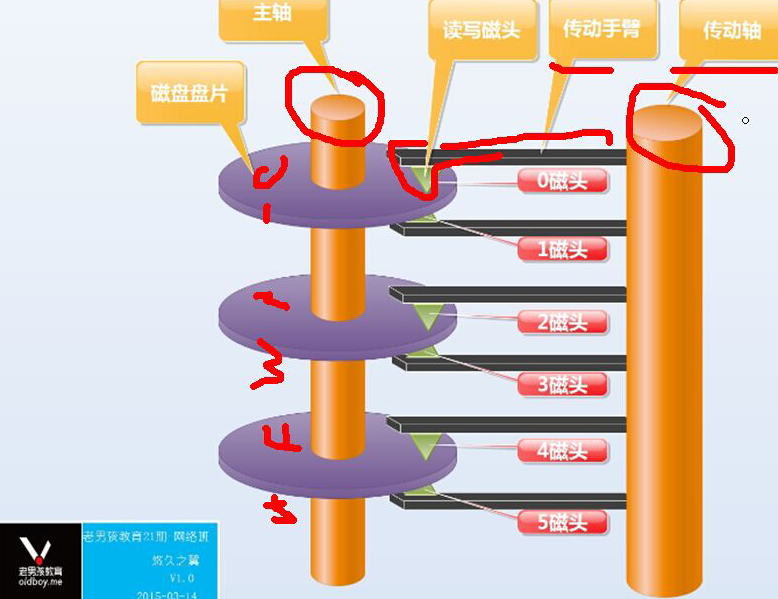
|  |  |
| --- | --- |
| **英文** | **汉语** |
| Disk | 磁盘 |
| Head | 磁头 |
| Sector | 扇区 |
| Track | 磁道 |
| Cylinder | 柱面 |
| Units | 单元块（一个柱面的大小） |
| Block | 数据块 |
| inode | 索引节点 |

一般来说，一块磁盘有一个到数个盘片，一般为2-14片。

磁盘的每一个盘面一般有300-1024个磁道。

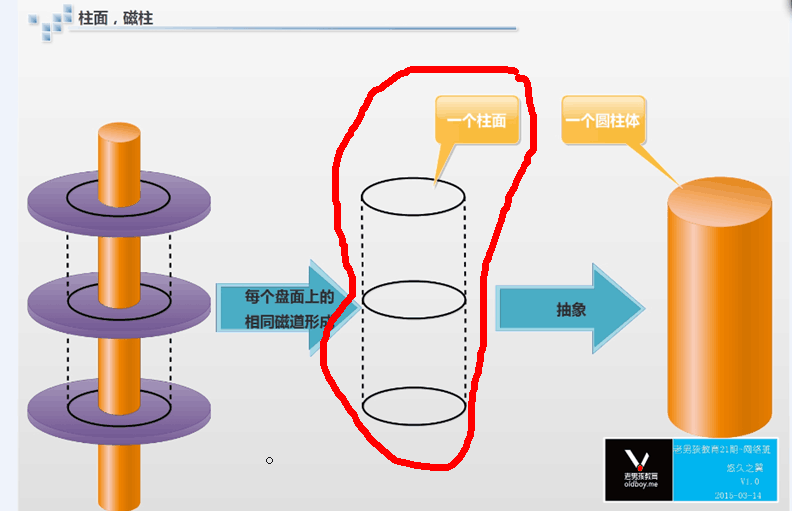
磁道的定义：

磁盘在格式化时被划分成许多同心圆，这些同心圆的轨迹叫做磁道（Track）。磁道由盘面从外向内依次从0开始顺序编号。



柱面的特点：

柱面是所有盘面相同半径的所有半径的集合。  
柱面数==一个盘面的磁道数。



磁盘的扇区：

每个扇区的大小是512个字节

扇区就是磁道的圆弧，是磁盘的一部分；一个扇区主要有两部分内容：存储数据地点的标识符和存储数据的数据段。 （扇区包括数据的位置和内容）

**磁道柱面扇区总结：**

1） 一块磁盘有2-14个盘片，每个盘片有两个面，每个面对应一个读写磁头，用磁头号来区分盘面，即盘面数就是磁盘数，盘面数\*2=磁头数（盘面数）

2) 不同盘面数的磁道被划分为多个扇形区域，每个区域就是一个扇区sector

3) 同一个盘面以盘片为圆心，每个不同半径的圆形轨迹就是一个磁道track

4) 不同盘面相同半径的磁道组成一个圆柱面就是柱面。cylinder

5) 一个柱面包含多个磁道（这些磁道半径相同），一个磁道包含多个扇区

6) 数据信息记录可表示为：某磁头，某磁道（柱面），某扇区.

磁道：看起来就像一个平面圆周形  
  
扇区： 盘面由圆心像四周画直线，不同的磁道被直线分为许多扇形（弧形）的区域，每个弧形的区域就叫做扇区。每个扇区的大小一般为512字节，扇区看起来就是圆弧或扇形  
  
柱面：磁盘中，不同盘片（或盘面）相同半径的磁道轨迹从上至下组成的圆柱形区域就称之为柱面，柱面看起来就是一个圆柱形。

磁盘容量的算法：

法1：

磁盘的容量=磁盘的容量=磁头数\*磁道数\*扇区数\*512bytes  
 一个磁道的容量=扇区数\*512bytes  
 一个盘面的容量=磁道数\*扇区数\*512bytes  
 磁盘的容量=盘面数\*一个盘面的容量  
法2：

磁盘容量=柱面数（磁盘数）\*柱面大小（磁道大小\*磁头数）

[root@moban ~]# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes

255 heads, 63 sectors/track, 1044 cylinders

Units = cylinders of 16065 \* 512 = 8225280 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk identifier: 0x000bc2cc

[root@moban ~]# echo "255\*63\*1044\*512"|bc

8587192320

总结：

1. 盘片的旋转是靠马达带动主轴，带动盘片旋转。
2. 磁头的径向移动也是靠步进电机来完成的。
3. 所有的刺头同时同向移动的。

磁盘再读写数据时，应尽可能让磁头不动（磁头移动叫寻道），或者少移动

磁盘读数据按照柱面进行的

**机械磁盘读写磁盘数据的原理小结**

1. 磁盘是按照柱面为单位读写数据的，即先读取同一个盘面的某一个磁道,读完之后, 如果数据没有读完,磁头也不会切换真他的磁道,而是选择切换磁头,读取下一个盘面的相同半径的磁道, 直到所有盘面的相同半径的磁道读取完成之后, 如果数据还没有读写完成,才会切換其他不同半径的磁道,这个切換磁道的过程称为寻道。
2. 不同磁头间的切换是电子切换,而不同磁道间的切换需要磁头做径向运动,这个径向运动需要步进电机调节,这个动作是机械的切换。

寻道：机械的

本部分重点小结：  
1、名词：磁道，柱面，扇区。  
2、数据在磁盘的位置，三维地址，0磁头0磁道1扇区。  
3、磁盘的容量计算。  
4、磁盘读写数据的原理。

什么是扇区：

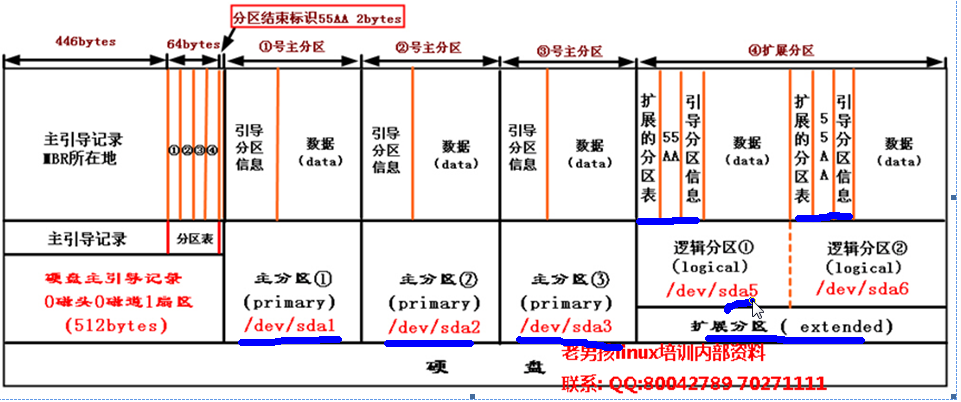
磁道上的一个弧形区域（盘面由圆心向四周画直线，不同的磁道被直线分成许多扇形（弧形）的区域，每个弧形的区域叫扇区，每个扇区大小一般为512字节，扇区看起来就是圆弧或扇形。）

什么是磁道：

以盘面的圆心为中心不同半径的同心圆。（每个盘片有两个面，都可记录信息，盘片表面以盘片中心为圆心，用于记录数据的不同半径的圆形磁化轨迹就称为磁道）

什么是柱面：

不同盘片相同半径的磁道轨迹从上至下组成的圆柱形区域就称之为柱面，柱面看起来就是一个圆柱形。



5、什么是RAID

是廉价冗余磁盘阵列（redundant array of inexpensive disk）的简称。

Raid的好处：容量更大了，性能更高了，有冗余了。

Raid级别介绍

把多个物理磁盘通过不同的技术组成磁盘阵列，这个不同的技术方式就被称之为raid级别。

0、1、2、3、4、5、6、7、10、53等。

|  |  |  |  |
| --- | --- | --- | --- |
| **RAID级别** | **关键优点** | **关键缺点** | **实际应用场景** |
| RAID 0 | 读写速度最快 | 没有任何冗余 | MySQL slave集群的节点RS |
| RAID 1 | 100%冗余，镜像。 | 读写性能一般，成本高 | 单独的，数据重要，且不能宕机的业务。监控，系统盘。 |
| RAID 5 | 具备一定性能和冗余，可以坏一块盘，读性能不错。 | 写入性能不高。 | 一般的业务都可以用 |
| RAID 10  RAID 0+1 | 读写速度很快，100%冗余 | 成本高 | 性能和冗余要求都很好的业务。数据库和存储的主节点。 |

下表提供了7级raid的简单定义。

|  |  |  |  |
| --- | --- | --- | --- |
| R级别 | 描述 | 速度 | 容错性能 |
| 0 | 磁盘分段 | 磁盘并行输入/出 | 无 |
| 1 | 磁盘镜像 | 没有提高 | 有（允许） |
|  |  |  |  |
|  |  |  |  |

Raid技术分类

常见raid技术分为两种

1、软raid技术：

在Linux下载安装系统过程中或者安装系统后通过自带的软件就能实现软raid功能，使用软raid可省去购买昂贵的硬件raid控制器和附件就能极大的增强磁盘的IO性能和可靠性。由于是用软件去实现的raid功能，所以它配置灵活、管理方便。跟同事使用软件raid，还可以实现将几个物理磁盘合并成一个更大的虚拟设备，从而达到性能改进和数据冗余的目的。

2、硬RAID技术：

基于硬件的raid解决方案比基于软raid技术在使用性能和服务性能上回更胜一筹，具体表现在检测和修复多为错误的能力、错误磁盘自动检测和阵列重建等方面。从安全性能考虑，基于硬件的raid解决方案也是更安全的，因此，在实际的生产场景工作中，基于硬件的raid

什么是lvm

LVM全称（logic volume management）逻辑卷管理

可以管理磁盘的容量，让磁盘分区可以随意放大或缩小，便于更好的应用磁盘的剩余空间，如果过于强调性能与备份，那么还是应该使用raid功能，而不是LVM

LVM是在硬盘的分区之上，创建一个逻辑层，以方便系统管理整个硬盘分区系统，LVM最先有IBM开发，在AIX系统上实现，OS/2操作系统与HP-UX也支持这个功能。在1998年，Heinz Mauelshagen根据在HP-UX上的LVM管理器，写作出第一个Linux版本。

Raid和LVM的区别

LVM：灵活的调整分区的容量，有一定的冗余和性能功能，但很弱。

RAID：更侧重性能和数据安全。

为什么需要raid？

磁盘阵列可以把多个磁盘驱动器通过不同的链接方式链接在一起协同工作，大大提高了读取速度，同时把磁盘协同的可靠性提高到接近无错的境界。

1. 提升数据安全性
2. 提升数据读写性能
3. 提供更大的单一逻辑盘数据容量存储。

RAID0

又称为stripe（条带化）或striping（条带模式），它在所有raid级别中具有最高的存储性能。

RAID 0提高存储性能的原理是把连续的数据分散到多个磁盘上存取。这样，协同有数据读写请求就尅在多个磁盘并行的执行，每个磁盘读写属于它自己的那部分数据请求。这种数据上的并行操作可以充分利用总线的带宽，显著提高磁盘整体存取性能。

生产场景：

1. 负载均衡集群下面的多个相同RS节点服务器。
2. 分区时文件存储下面的主节点或CHUNK SERVER.
3. Mysql 主从复制的多个slave服务器。
4. 对性能要求很高，对冗余要求很低的相关业务。

|  |  |
| --- | --- |
| **关注点** | **描述** |
| 容量 | 是4块盘加在一起的容量，在raid级别中具备最高的存储性能，原理是把连续的数据分散到多个磁盘上存取。 |
| 性能 | 理论上磁盘读写速度比单盘提升4倍，磁盘越多倍数会越小。 |
| 冗余 | 无任何冗余，坏1块盘，整个raid都不能使用。 |
| 场合 | 适合于大规模并发读写，但对数据安全性要求不高的情况。如：集群中的RS，做虚拟机的实体机、负载均衡集群下面的多个相同RS节点服务器，如分布式文件存储下面的CHUNK SERVER，以及MySQL主从复制的多个slave服务器。 |
| 特点 | 速度快，无冗余，容量无损失。 |

Raid1

又称为mirror或mirroring（镜像），它的宗旨是最大消毒的保证用户数据的可用性和可修复性。Raid1的操作方式是把用户写入一个磁盘的数据百分之百地自动复制到另一个磁盘上，从而实现存储双份

|  |  |
| --- | --- |
| **关注点** | **描述** |
| 容量 | 损失50%的磁盘容量。例如：2块1T的盘，做raid1后，容量为1T |
| 性能 | Mirror不能提高存储性能,理论上写性能和单盘相差不大有人说读取效率是2 倍,到底如何呢?请有测试环境的同学帮忙测试?暂且按照只读单盘说明, |
| 冗余 | 在所有RAID级别中, RAID1提供最高的数据安全保障冗余度50%。 |
| 场合 | 适用子存放重要数据, 如服务器系统分区和对性能要求不高的数据库存储等领域, |
| 特点 | 100%冗余,容量损失一半 |

RAID 5是一种存储性能、数据安全和存储成本兼顾的存储解决方案。  
RAID 5是把数据和相对应的奇偶校验信息存储到组成RAID5的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当RAID5的一个磁盘数据发生损坏后，利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。

|  |  |
| --- | --- |
| **关注点** | **描述** |
| 容量 | 损失一块盘的数据容量 |
| 性能 | Raid5具有和raid0相近似的数据读取速度，知识多了一个奇偶校验信息，写入数据的速度比对单个磁盘进行写入操作稍慢。 |
| 冗余 | 可损失一块盘。Raid5数据安全保障程度比raid1低而磁盘空间利用率要比raid1高。 |
| 场合 | Raid5可以理解为是raid0和raid1的折衷方案。适合对性能和冗余都有一定要求，又都不是十分高的情况。MySQL的主从库都可以，存储也可以。普通的服务器为了减少维护成本，又保持一定冗余和读性能都可以做raid5. |
| 特点 | 容量损失一块盘，写数据通过奇偶校验，raid0和raid1的折衷方案。 |

6、增加epel源

rpm -ivh <http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm>

wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-6.repo