#### 养成良好的习惯

##### 备份

备份的好处:

◆ 可以还原

建议备份的格式: 文件名.用户名.日期

◆ 可以用来对比,修改了哪些地方

# diff  文件名   备份文件名    //查看文件和备份文件的差别

# vimdiff    文件名  备份文件名        //在vim中显示两个文件的差异之处

tree命令

# tree a   //查看目录结构

-a 显示所有文件(包括隐藏文件)

-d 只显示目录

-L #, 显示#层级,默认显示所有的

-f 为显示完整的路径

-i 不显示树枝(目录结构的横线)

-F 在目录基名后面加上/

往一个txt文件里追加内容

    1) # echo "内容" >> txt文件

    2) # cat >> 文件绝对路径 << EOF 内容 内容 内容 内容 内容 内容 内容 内容 内容 EOF //就是把两个EOF之间的内容追加到txt文件内的内容尾,优势:可以同时追加多行.

    # for f in `seq 1000`;do touch $f.txt;done    //按序列创建1.txt ~ 1000.txt

移动命令:

# mv [-ifu] [源文件/源目录] [目标目录]

    -i 如果目标文件已经存在,询问是否覆盖

    -f 强制执行,不会询问

    -u 若目标文件已经存在,则比较文件新旧,才会移动

# rmdir 目录名    //删除空目录

###### 让test里显示除了oldboy外的其他内容.

awk sed grep

这三个命令都可以直接接文件, 不是必须接在管道符后面

grep

# grep -v oldboy test.txt    //从test.txt里过滤掉oldboy(oldboy不显示,其他内容正常显示)

sed

# sed '/oldboy/d' /tmp/test.txt    //从/tmp/test.txt里过滤掉oldboy(不显示,但其他内容正常显示)

# sed -n /oldboy/p /tmp/test.txt        //取消默认输出,打印包含oldboy的语句,相当于 grep oldboy /tmp/test.txt

# sed -n /[^oldboy]/p test.txt        //正则表达式,从/tmp/test.txt 里过滤掉oldboy, 显示其他内容

awk

# awk /[^oldboy]/ test.txt    //从/tmp/test.txt 里过滤掉oldboy, 显示其他内容

用/mnt/test.txt 覆盖掉/tmp/test,且不提示覆盖(mv 和cp 都可以)

1) # \cp -f /mnt/test.txt /tmp/test.txt    //在命令前面加上反斜线'\'

2) # /bin/cp -f /mnt/test.txt /tmp/test.txt    //用命令的全路径

只查看 ett.txt 文件内第20行到第30行的内容

# seq 100     //生成序列数字1-100

# seq -s " " 5 //-s seperator 指定分隔符,{a..z}是横着排列

➜ ~ seq -s " " 5

1 2 3 4 5

# seq 100 >ett.txt    // 在ett.txt内写入1-100的数字

方法1). # head -30 ett.txt|tail -11

方法2). # sed  -n '20,30p' ett.txt    //取消默认输出(默认输出1-100),显示20-30行,p是print

方法3). # awk '{if(NR>19 && NR<31) print $1}' ett.txt    //打印20-30行, NR是行号

find 并删除

[[root@localhost](mailto:root@localhost) tmp]# find /tmp -inum 524313 -ok rm {} \;    //-ok 可换成 -exec,-ok会在执行前询问

< rm ... /tmp/test > ? n

[[root@localhost](mailto:root@localhost) tmp]# find /tmp -inum 524313 |xargs rm    //xargs 功能和-exec一样

[[root@localhost](mailto:root@localhost) tmp]# ls

a.txt    services                                  yum\_save\_tx-2016-07-05-02-16QQh1jE.yumtx

ett.txt  yum\_save\_tx-2016-07-05-02-16nylnZA.yumtx

[[root@localhost](mailto:root@localhost) tmp]# seq -s " " 20 30      //打印,序列20-30.数字之间用" " 中间部分间隔,-s 'SEPERATOR'

20 21 22 23 24 25 26 27 28 29 30

[[root@localhost](mailto:root@localhost) tmp]#  seq -s "$" 20 30    //-s " "表示指明序列之间的间隔符号

20$21$22$23$24$25$26$27$28$29$30

[[root@localhost](mailto:root@localhost) tmp]# touch `seq -s " " 20 30`        //创建20 -30 序列文件,` `(反引号,键盘上的~键)中间可以插入命令

[[root@localhost](mailto:root@localhost) tmp]# ls

20  22  24  26  28  30     ett.txt   yum\_save\_tx-2016-07-05-02-16nylnZA.yumtx

21  23  25  27  29  a.txt  services  yum\_save\_tx-2016-07-05-02-16QQh1jE.yumtx

反选查找,就是排除a.log

[[root@localhost](mailto:root@localhost) ~]# find /tmp -type f ! -name 'a.log' -exec ls -l {} \;

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/24

-rw-------. 1 root root 209 7月   5 02:16 /tmp/yum\_save\_tx-2016-07-05-02-16nylnZA.yumtx

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/21

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/28

-rw-r--r--. 1 root root 641020 7月   5 08:46 /tmp/services

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/20

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/23

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/29

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/27

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/26

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/30

-rw-r--r--. 1 root root 12288 7月   1 12:59 /tmp/.test.swp

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/22

-rw-r--r--. 1 root root 0 7月   6 08:00 /tmp/25

-rw-r--r--. 1 root root 24576 7月   5 08:46 /tmp/.services.swp

-rw-------. 1 root root 209 7月   5 02:16 /tmp/yum\_save\_tx-2016-07-05-02-16QQh1jE.yumtx

-rw-r--r--. 1 root root 134 7月   6 02:03 /tmp/a.txt

-rw-r--r--. 1 root root 292 7月   5 06:52 /tmp/ett.txt

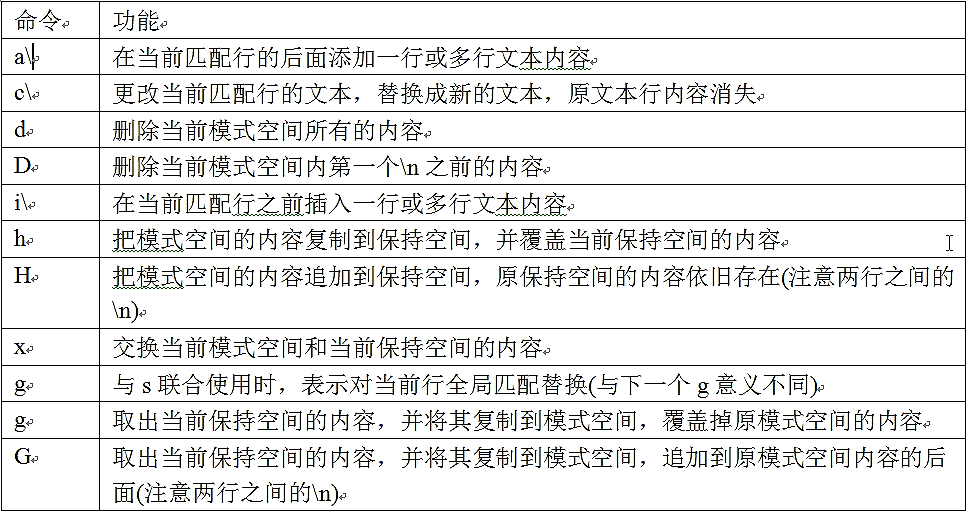
其他命令

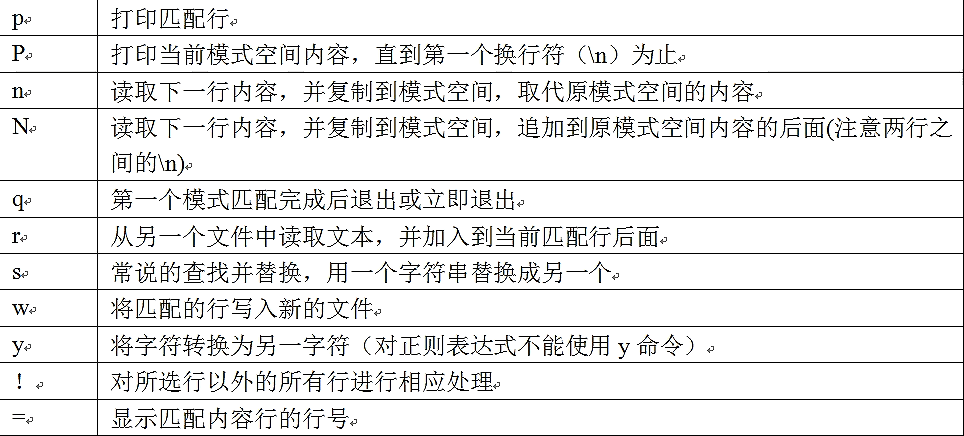
# echo "123456"|passwd --stdin aphey && history -c    // 把aphey用户密码更改为123456,一般用于批量创建用户.

# LANG=zh\_CN.UTF-8            //可以在操作界面切换语言, 中文为 zh\_CN.UTF-8; 英文为EN

# yum grouplist     //可以查看安装的软件组

###### sed 命令







###### 优化 Selinux

* 关闭Selinux

⑴ # sed -i 's/SELINUX=enforcing/SELINUX=disabled' /etc/selinux/config

也可以用 sed -i 's#SELINUX=enforcing#SELINUX=disabled#g' /etc/selinux/config

⑵ # vi /etc/selinux/config    //手动修改

    SELINUX=disabled

⑶ # setenforce=0    //临时生效,一般在配置文件里先改了,然后再用此命令

  # getenforce        //查看selinux当前状态

* 设定运行级别runlevel

    # runlevel    //查看运行级别

    # init 0-6 //重启系统并更换到对应的运行级别

# telinit 0-6 //不重启系统并更换到对应的运行级别

* Linux中文显示设置

[root@localhost]~# cat /etc/sysconfig/i18n

LANG="en\_US.UTF-8"

SYSFONT="latarcyrheb-sun16"

[root@localhost]~# cp /etc/sysconfig/i18n /etc/sysconfig.ori //备份一下

[root@localhost]~# echo 'LANG="zh\_CN.UTF-8"' > /etc/sysconfig/i18n //通过输出冲定向来修改

[root@localhost]~# source /etc/sysconfig/i18n //让它生效

* 设定账号闲置超时时间

[root@localhost]~# export TMOUT=10 //超时时间为10秒,追加到/etc/profile永久生效

* 更改ssh登录标准

windows user : administrator    guest    Port:3389

Linux user; root 很多普通用户    port:22

所以我们要改掉默认的用户和端口.

# cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak    //先备份sshd配置文件

# vi sshd\_config    //编辑sshd\_config,常规我们纸修改下面四项

######by oldboy#2016-07-11####

Port 52113    //→ssh连接默认的端口,所有人都知道,必须要改

PermitRootLogin no    //→root用户黑客都知道,禁止它远程登录,但是可以先用普通用户登录后再换root用户

PermitEmptyPasswords no    //→禁止空密码登录

UseDNS no    //→不使用DNS

######by oldboy#2016-07-11####

# /etc/init.d/sshd restart    //→ 修改完配置文件后需要重启相关服务

# lsof -i :52113    //只知道端口,可以反查相关服务

然后从windows上用远程工具连接linux,发现连接不上

我们在windowsn上ping linuxIP, 发现可以ping通,说明网络线路是通的

然后我们用 telnet linuxIp 52113 不通, 说明sshd服务是不通的.

那我们就要到linux那去确认

1) sshd服务是否启动,用lsof -i :52113 查询即可

2) 确认防火墙是否开启 /etc/init.d/iptables status

修改/etc/ssh/sshd\_config修改端口,禁止root登录.

* history相关

1) history -c: 清空所有历史命令 -d 删除指定条目的命令 -w 保存历史命令到 ~/.bash\_history中

2) 调短历史命令的存储数量 #export HISTSIZE=5 //只保存5条命令,默认为1000

3) 控制历史记录文件(~/.bash\_history)中保存命令的长度 #export HISTFILESIZE=5

上述命令只是临时生效,要想永久生效,就把他们放到/etc/profile中,并source一下

* 克隆虚拟机网络问题处理:

1) [root@localhost]~# vi /etc/sysconfig/network-scripts/ifcfg-eth0

2) 删除掉 HWADDR行和UUID行 再清空/etc/udev/rules.d/70-persistent-net.rules来内容就可以了.

3) #reboot 重启即可

* buffer 和cache的区别?

buffer: 缓冲,从内存慢慢过渡到硬盘

cache: 缓存,从硬盘过渡到内存,别人从内存访问

* 过滤出已知当前目录下oldboy中的所有一级目录(提示:不包含oldboy目录下面目录的子目录及隐藏目录,即只能是一级目录),附上文件.

[root@localhost ~]# mkdir oldboy

[root@localhost ~]# cd oldboy

[root@localhost oldboy]# mkdir ext test xiaodong xiaofan xingfujie -p

[root@localhost oldboy]# touch ext/oldboy jeacen wodi.gz yingsui.gz

[root@localhost oldboy]# cd ..

[root@localhost ~]# tree

.

├── anaconda-ks.cfg

├── install.log

├── install.log.syslog

└── oldboy

├── ext

│   └── oldboy

├── jeacen

├── test

├── wodi.gz

├── xiaodong

├── xiaofan

├── xingfujie

└── yingsui.gz

解题思想方法:

1. 根据颜色区分文件和目录(目录的字体是浅蓝色)
2. ls -l结果中,以d开头的就是目录

[root@localhost oldboy]# ls -l | grep "^d"

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 ext

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 test

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xiaodong

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xiaofan

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xingfujie

1. 通过给目录加表示,然后通过过滤标识,就可以过滤出目录[ls -F(flags不同的文件加不同的标识) 或ls -p(path,只针对目录),这两个选项就是在目录文件名后面加”/”]

[root@localhost oldboy]# ls -p | grep "/"

ext/

test/

xiaodong/

xiaofan/

xingfujie/

1. 通过find 直接查找指定类型的文件(-d 就是目录)

[root@localhost oldboy]# find ./ -maxdepth 1 -type d ! -name "."

./xingfujie

./xiaofan

./test

./xiaodong

./ext

1. ls -l输出结果中第二列数字大于1(要求文件没被硬链接)

[root@localhost oldboy]# ls -l|awk '{if($2>1)print$0}'

total 20

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 ext

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 test

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xiaodong

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xiaofan

drwxr-xr-x. 2 root root 4096 Jun 18 09:51 xingfujie

* 只保留7天的安全日志

//模拟环境

makedir /app/logs -p

for n in $(seq 14);

do

date -s “2016/01/$n”;

touch access\_www\_$(date +%F).log;

done

date -s “2016/01/15”

//删除7天前的文件

1. # find /app/logs -type f -mtime +7|xargs rm -r
2. # find /app/logs -type f -mtime +7-exec rm {} \;
3. # rm `find /app/logs -type f -mtime +7`

* 显示/etc/inittab文件行号的方法

1. cat -n /etc/inittab
2. nl /etc/inittab
3. awk ‘{print NR,$0}’ /etc/inittab
4. vi /etc/inittab，然后用set设置
5. grep -n “.” /etc/inittab //，是任意一个字符，前面加上行号

* 显示/proc/meminfo文件中以大小S开头的行(要求两种方式)

方法一) [root@localhost tmp]# grep "^[Ss]" /proc/meminfo

SwapCached: 0 kB

SwapTotal: 8167416 kB

SwapFree: 8167416 kB

Shmem: 3716 kB

Slab: 293272 kB

SReclaimable: 226360 kB

SUnreclaim: 66912 kB

方法二) [root@localhost tmp]# grep -i "^s" /proc/meminfo

SwapCached: 0 kB

SwapTotal: 8167416 kB

SwapFree: 8167416 kB

Shmem: 3716 kB

Slab: 293292 kB

SReclaimable: 226364 kB

SUnreclaim: 66928 kB

* 显示/etc/passwd文件中不以/bin/bash结尾的行

[root@localhost tmp]# grep -v "/bin/bash$" /etc/passwd

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

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin

saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin

postfix:x:89:89::/var/spool/postfix:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

* 显示/etc/passwd文件中ID号最大的用户的用户名

[root@localhost tmp]# sort -n -t: -k3 /etc/passwd| tail -1 | cut -d: -f1

aphey

[root@localhost tmp]# cat /etc/passwd //查看认证一下

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

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin

saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin

postfix:x:89:89::/var/spool/postfix:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

aphey:x:500:500::/home/aphey:/bin/bash

* 找出/etc/passwd中的两位或三位数

//解题思路: 需要锚定数字的位数,不锚定的话,4位数字也会被匹配进来

[root@localhost tmp]# grep "\<[[:digit:]]\{2,3\}" /etc/passwd

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin

saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin

postfix:x:89:89::/var/spool/postfix:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

aphey:x:500:500::/home/aphey:/bin/bash

* 显示/etc/rc.d/rc.sysinit文件中,至少以一个空白字符开头,且后面存在非空白字符的行

[root@localhost tmp]# grep "^[[:space:]]\+" /etc/rc.d/rc.sysinit |grep "[^[:space:]]"

. /etc/sysconfig/network

HOSTNAME=localhost

mount -n -t proc /proc /proc

...

* 找出netstat -tan的结果中以"LISTEN"后跟0、1或多个空白字符结尾的行

[root@localhost tmp]# netstat -tan|grep "LISTEN[[:space:]]\*$"

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:7777 0.0.0.0:\* LISTEN

tcp 0 0 :::23 :::\* LISTEN

tcp 0 0 ::1:25 :::\* LISTEN

tcp 0 0 :::7777 :::\* LISTEN

* 找出/etc/passwd文件中用户名同shell名的行;**锚定单词的方法!**\_

[root@mail ~]# grep "^\([[:alnum:]]\+\>\).\*\1$" /etc/passwd

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

* 如果root用户存在,就显示其默认的shell程序

[root@localhost tmp]# id root &>/dev/null && grep "^root" /etc/passwd|cut -d: -f7

/bin/bash

* 显示当前系统root、centos或user1的默认shell和uid

[root@mail sh]# egrep "^(root|centos|user1)\>" /etc/passwd| cut -d: -f 3,7

0:/bin/bash

* 找出/etc/rc.d/init.d/functions文件中连字符\_或者某单词后面跟一个小括号的行

[root@localhost tmp]# egrep "^[\_[:alpha:]]+\(\)" /etc/rc.d/init.d/functions

fstab\_decode\_str() {

checkpid() {

\_\_readlink() {

\_\_fgrep() {

\_\_kill\_pids\_term\_kill\_checkpids() {

\_\_kill\_pids\_term\_kill() {

\_\_umount\_loop() {

\_\_source\_netdevs\_fstab() {

\_\_source\_netdevs\_mtab() {

\_\_umount\_loopback\_loop() {

* 使用echo输出一个绝对路径，使用egrep取出其基名

[root@localhost tmp]# echo "/mnt/cdrom/images"|egrep "[^/]+/?$"

/mnt/cdrom/images

[root@localhost tmp]# echo "/mnt/cdrom/images/"|egrep "[^/]+/?$"

/mnt/cdrom/images/

// 上面两个命令的grep用-o 选项就可以显示基名

[root@localhost tmp]# echo "/mnt/cdrom/images/"|grep -E -o "[^/]+/?$"

images/

[root@localhost tmp]# echo "/mnt/cdrom/images"|grep -E -o "[^/]+/?$"

images

* 找出ifconfig命令结果中的ip地址

[root@localhost tmp]# ifconfig| awk 'NR==2{print}'| awk -F "[ :]+" '{print $4}'

192.168.88.123