# TODO

# 硬件条件

Ssd：120g 安装系统吧，只放aosp，擦除之前的安装

Hdd：256g，固件归档吧，挂载上去就好了

# 系统简述

1. i386=Intel 80386。其实i386通常被用来作为对Intel（英特尔）32位微处理器的统称。
2. AMD64，又称“x86-64”或“x64”，是一种64位元的电脑处理器架构。它是建基于现有32位元的x86架构，由AMD公司所开发。

## cent os

d

系统版本区别

CentOS-6.3-i386-bin-DVD1.iso

CentOS-6.3-x86\_64-bin-DVD1.iso

CentOS-6.3-x86\_64-netinstall.iso

CentOS-6.3-x86\_64-minimal.iso

CentOS-6.3-x86\_64-bin-DVD2.iso

CentOS-6.3-i386-netinstall.iso

CentOS-6.3-i386-minimal.iso

CentOS-6.3-i386-bin-DVD2.iso

[i386](https://www.baidu.com/s?wd=i386&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y3uAD4Phcvuh7WmvDkP19h0AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtYnWfvrHfdrHfzrjcsrHf1n1c)是32位系统，[x86\_64](https://www.baidu.com/s?wd=x86_64&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y3uAD4Phcvuh7WmvDkP19h0AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtYnWfvrHfdrHfzrjcsrHf1n1c)是64位系统

bin——完整版，netinstall——网络安装盘，启动后需要联网安装

minimal——[小安](https://www.baidu.com/s?wd=%E5%B0%8F%E5%AE%89&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y3uAD4Phcvuh7WmvDkP19h0AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtYnWfvrHfdrHfzrjcsrHf1n1c)装盘，只有基础的软件,系统安装必须的部分,需要其他软件的用yum来安装，一般是做服务器，所以都是minimal，不需要桌面，包自己安装

显示系统版本

#cat  /etc/redhat-release

查询内核版本。

#uname  -r

[[root@iZ94ofdtjo2Z](mailto:root@iZ94ofdtjo2Z) ~]# cat /etc/redhat-release

CentOS release 6.3 (Final)

[[root@iZ94ofdtjo2Z](mailto:root@iZ94ofdtjo2Z) ~]# uname -a

Linux iZ94ofdtjo2Z 2.6.32-358.6.2.el6.x86\_64 #1 SMP Thu May 16 20:59:36 UTC 2013 x86\_64 x86\_64 x86\_64 GNU/Linux

2.安装系统

2.1下载

从<https://wiki.centos.org/Download>   主站找最近最小的镜像文件（做开发700M的那个差不多了）



2.2

参考;

1.CentOS怎样查看系统信息

<http://jingyan.baidu.com/article/e6c8503c062dcee54f1a18d0.html>

2.centos7.0安装教程

<http://jingyan.baidu.com/article/a3aad71aa180e7b1fa009676.html>

3.VM虚拟机下安装Centos7.0图文教程（minimal可以重点参考）

<http://www.centoscn.com/image-text/setup/2014/0723/3341.html>

# U盘安装Ubuntu系统

## Ubuntu镜像源下载地址

1,清华大学镜像源

https://mirrors.tuna.tsinghua.edu.cn/

2,中科大镜像源（推荐）

https://mirrors.ustc.edu.cn/repogen/

## 步骤

1. 首先准备一个U盘，通常CD版2G就够了，而DVD版需要4G，插入U盘后，如果U盘中有文件，先拷贝出去，然后右键选择格式化
2. 文件系统选择FAT32，勾选快速格式化，其它默认
3. 烧录Ubuntu系统，使用UniversalUSBInstaller\_1.9.7.7

<https://universal-usb-installer.en.softonic.com/download?ex=BB-527.1>

4. 开机按F8，选择从U盘载入系统，选择uEIF的U盘的哪一个项目就好了

5.然后按照<https://blog.csdn.net/s634772208/article/details/78573486> 执行

最后

# Linux文件管理

## 有关Linux环境变量

在profile文件添加或修改的内容需要注销系统（或者调用**source**）才能生效。

、常见的环境变量

　　PATH：决定了shell将到哪些目录中寻找命令或程序

　　HOME：当前用户主目录

　　MAIL：是指当前用户的邮件存放目录。

　　SHELL：是指当前用户用的是哪种Shell。

　　HISTSIZE：是指保存历史命令记录的条数。

　　LOGNAME：是指当前用户的登录名。

　　HOSTNAME：是指主机名称，许多应用程序如果要用到主机名的话，通常是从这个环境变量中来取得的。

　　LANG/LANGUGE：是和语言相关的环境变量，使用多种语言的用户可以修改此环境变量。

　　PS1：是基本提示符，对于root用户是#，对于普通用户是$。

　　PS2：是附属提示符，默认是“>”。

**source /etc/profile**是让/etc/profile文件修改后立即生效，

还有一种方法是**：. /etc/profile**

注意：.和/etc/profile有空格

**linux中source命令**

**source命令也称为“点命令”也就是一个符号（.）.source命令通常用于重新执行刚修改的初始或文件，使之立即生效，而不必注销并重新登录。**

**用法： source filename 或. filename**

参考

1.[/etc/profile文件详解](http://blog.chinaunix.net/uid-25749806-id-298287.html)

<http://blog.chinaunix.net/uid-25749806-id-298287.html>

## 02自动启动

D

翻译自：<http://www.thegeekstuff.com/2011/06/chkconfig-examples/>

注意：service的安装目录在/etc/rc.d/init.d下，/etc/init.d 是/etc/rc.d/init.d的链接。

chkconfig命令用来安装，查看或修改 services随系统启动的启动选项的设置。本文章包含了7个实例来解释如何使用chkconfig命令。

1 在shell脚本中检查service的启动选项的设置

当你执行chkconfig加service名字，如果service被配置为自动启动，则它将返回true。下列的代码段显示了如何在脚本中检查一个service是否被配置为自动启动。

# vi check.sh

chkconfig network && echo "Network service is configured"

chkconfig junk && echo "Junk service is configured"

# ./check.sh

Network service is configured

你也可以特别地查看它是否配置为在某个run level自动启动。

# vi check1.sh

chkconfig network --level 3 && echo "Network service is configured for level 3"

chkconfig network --level 1 && echo "Network service is configured for level 1"

# ./check1.sh

Network service is configured for level 3

2 查看所有的services的启动选项的设置

--list选项显示所有的services的启动选项的配置状态。

# chkconfig --list

abrtd 0:off 1:off 2:off 3:on 4:off 5:on 6:off

acpid 0:off 1:off 2:off 3:off 4:off 5:off 6:off

atd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

...

只查看在某个runlevel启动的services，例如查看在runlevel3下自动启动的services。

chkconfig --list | grep 3:on

查看某个service的启动选项的设置，也可以对chkconfig --list 的output使用grep，例如：chkconfig --list | grep network

3 增加一个新的service为自动启动

使用-add选项来增加某个service，使其能够在系统启动的时候自动地启动。

下列的实例显示了如何增加一个新的service iptables，使其能够在系统启动的时候自动地启动。使用‘chkconfig --add’命令将自动地设置在runlevel 2,3,4,5上自动地启动。

# chkconfig --list | grep iptables

# chkconfig --add iptables

# chkconfig --list | grep iptables

iptables 0:off 1:off 2:on 3:on 4:on 5:on 6:off

注意：”chkconfig --add“ 只是设置一个存在的service为自动启动，此service必须已经安装，即已经存在于/etc/rc.d/init.d下。如果service不存在，你需要首先安装service到/etc/rc.d/init.d下，然后再为其设置自动启动选项。这是很多的初学者都容易犯的错误，所以值得在这里强调。

4 删除某个service的自动启动选项的设置

下列的实例显示了ip6tables service被配置为自动启动。

# chkconfig --list | grep ip6tables

ip6tables 0:off 1:off 2:off 3:on 4:off 5:off 6:off

要删除某个service的自动启动的设置，使用--del选项，如下：

# chkconfig --del ip6tables

# chkconfig --list | grep ip6tables

5 设置或取消某个service在某个runlevel的自动启动设置

有时你可能不想取消整个service的自动启动的设置，你只是需要设置或取消service在某个runlevel的自动启动的设置，

下列的实例将取消nfserver service在runlevel5的自动启动设置

# chkconfig --level 5 nfsserver off

你也可以组合多个runlevel，例如你可以取消nfserver在runlevel3和5的自动启动设置

# chkconfig --level 35 nfsserver off

6 chkconfig 与 rc\*.d目录下的脚本 （\*表示runlevel1-6）

当你使用chkconfig来增加或删除某个service的自动启动选项的设置的时候，其实是在rc\*.d目录下做下列的事情：

当chkconfig --add命令执行的时候，其实是在对应的rc\*.d目录下创建相应用来启动和停止service的service的symbollink文件；

当chkconfig --del命令执行的时候，其实是在对应的rc\*.d目录下删除相应用来启动和停止service的service的symbollink文件；

rc\*.d目录下与某个service关联的2个symbollink文件中，以K（kill）开始的表示此文件用来停止service，以S（start）开始的表示此文件用来启动service。

例如service nfsserver没有设置自动启动选项的时候，我们在/rc\*.d下看不到用来启动和停止service的symbollink文件

# chkconfig --list | grep nfsserver

nfsserver 0:off 1:off 2:off 3:off 4:off 5:off 6:off

# ls /etc/rc.d/rc3.d | grep nfsserver

# ls /etc/rc.d/rc5.d | grep nfsserver

当我们为nfsserver service设置自动启动选项后，我们就可以看到相应的symbollink文件了

# chkconfig --add nfsserver

nfsserver 0:off 1:off 2:off 3:on 4:off 5:on 6:off

# cd /etc/rc.d/rc3.d

# ls -l | grep nfsserver

lrwxrwxrwx 1 root root 12 2011-06-18 00:52 K08nfsserver -> ../init.d/nfsserver

lrwxrwxrwx 1 root root 12 2011-06-18 00:52 S14nfsserver -> ../init.d/nfsserver

# cd /etc/rc.d/rc5.d

# ls -l | grep nfsserver

lrwxrwxrwx 1 root root 12 2011-06-18 00:52 K08nfsserver ->../init.d/nfsserver

lrwxrwxrwx 1 root root 12 2011-06-18 00:52 S14nfsserver -> ../init.d/nfsserver

当你取消此service在某个runlevel的自动启动选项的设置的时候，对应的rc\*.d目录下的symbollink文件也将被自动的删除，

# chkconfig --level 5 nfsserver off

# ls /etc/rc.d/rc5.d | grep nfsserver

完！

参考

1.开机自启动

<http://www.cnblogs.com/itech/archive/2011/08/22/2149018.html>

## iptables

d

**一：前言**

防火墙，其实说白了讲，就是用于实现Linux下访问控制的功能的，它分为硬件的或者软件的防火墙两种。无论是在哪个网络中，防火墙工作的地方一定是在网络的边缘。而我们的任务就是需要去定义到底防火墙如何工作，这就是防火墙的策略，规则，以达到让它对出入网络的IP、数据进行检测。

目前市面上比较常见的有3、4层的防火墙，叫网络层的防火墙，还有7层的防火墙，其实是代理层的网关。

对于TCP/IP的七层模型来讲，我们知道第三层是网络层，三层的防火墙会在这层对源地址和目标地址进行检测。但是对于七层的防火墙，不管你源端口或者目标端口，源地址或者目标地址是什么，都将对你所有的东西进行检查。所以，对于设计原理来讲，七层防火墙更加安全，但是这却带来了效率更低。所以市面上通常的防火墙方案，都是两者结合的。而又由于我们都需要从防火墙所控制的这个口来访问，所以防火墙的工作效率就成了用户能够访问数据多少的一个最重要的控制，配置的不好甚至有可能成为流量的瓶颈。

**二：iptables 的历史以及工作原理**

**1.iptables的发展:**

iptables的前身叫ipfirewall （内核1.x时代）,这是一个作者从freeBSD上移植过来的，能够工作在内核当中的，对数据包进行检测的一款简易访问控制工具。但是ipfirewall工作功能极其有限(它需要将所有的规则都放进内核当中，这样规则才能够运行起来，而放进内核，这个做法一般是极其困难的)。当内核发展到2.x系列的时候，软件更名为ipchains，它可以定义多条规则，将他们串起来，共同发挥作用，而现在，它叫做iptables，可以将规则组成一个列表，实现绝对详细的访问控制功能。

他们都是工作在用户空间中，定义规则的工具，本身并不算是防火墙。它们定义的规则，可以让在内核空间当中的netfilter来读取，并且实现让防火墙工作。而放入内核的地方必须要是特定的位置，必须是tcp/ip的协议栈经过的地方。而这个tcp/ip协议栈必须经过的地方，可以实现读取规则的地方就叫做 netfilter.(网络过滤器)

作者一共在内核空间中选择了5个位置，

1.内核空间中：从一个网络接口进来，到另一个网络接口去的

2.数据包从内核流入用户空间的

3.数据包从用户空间流出的

4.进入/离开本机的外网接口

5.进入/离开本机的内网接口

**2.iptables的工作机制**

从上面的发展我们知道了作者选择了5个位置，来作为控制的地方，但是你有没有发现，其实前三个位置已经基本上能将路径彻底封锁了，但是为什么已经在进出的口设置了关卡之后还要在内部卡呢？ 由于数据包尚未进行路由决策，还不知道数据要走向哪里，所以在进出口是没办法实现数据过滤的。所以要在内核空间里设置转发的关卡，进入用户空间的关卡，从用户空间出去的关卡。那么，既然他们没什么用，那我们为什么还要放置他们呢？因为我们在做NAT和DNAT的时候，目标地址转换必须在路由之前转换。所以我们必须在外网而后内网的接口处进行设置关卡。

这五个位置也被称为五个钩子函数（hook functions）,也叫五个规则链。

1.PREROUTING (路由前)

2.INPUT (数据包流入口)

3.FORWARD (转发管卡)

4.OUTPUT(数据包出口)

5.POSTROUTING（路由后）

这是NetFilter规定的五个规则链，任何一个数据包，只要经过本机，必将经过这五个链中的其中一个链。

**3.防火墙的策略**

防火墙策略一般分为两种，一种叫“通”策略，一种叫“堵”策略，通策略，默认门是关着的，必须要定义谁能进。堵策略则是，大门是洞开的，但是你必须有身份认证，否则不能进。所以我们要定义，让进来的进来，让出去的出去，所以通，是要全通，而堵，则是要选择。当我们定义的策略的时候，要分别定义多条功能，其中：定义数据包中允许或者不允许的策略，filter过滤的功能，而定义地址转换的功能的则是nat选项。为了让这些功能交替工作，我们制定出了“表”这个定义，来定义、区分各种不同的工作功能和处理方式。

我们现在用的比较多个功能有3个：

1.filter 定义允许或者不允许的

2.nat 定义地址转换的

3.mangle功能:修改报文原数据

我们修改报文原数据就是来修改TTL的。能够实现将数据包的元数据拆开，在里面做标记/修改内容的。而防火墙标记，其实就是靠mangle来实现的。

小扩展:

对于filter来讲一般只能做在3个链上：INPUT ，FORWARD ，OUTPUT

对于nat来讲一般也只能做在3个链上：PREROUTING ，OUTPUT ，POSTROUTING

而mangle则是5个链都可以做：PREROUTING，INPUT，FORWARD，OUTPUT，POSTROUTING

iptables/netfilter（这款软件）是工作在用户空间的，它可以让规则进行生效的，本身不是一种服务，而且规则是立即生效的。而我们iptables现在被做成了一个服务，可以进行启动，停止的。启动，则将规则直接生效，停止，则将规则撤销。

iptables还支持自己定义链。但是自己定义的链，必须是跟某种特定的链关联起来的。在一个关卡设定，指定当有数据的时候专门去找某个特定的链来处理，当那个链处理完之后，再返回。接着在特定的链中继续检查。

注意：规则的次序非常关键，谁的规则越严格，应该放的越靠前，而检查规则的时候，是按照从上往下的方式进行检查的。

**三．规则的写法:**

iptables定义规则的方式比较复杂:

格式：iptables [-t table] COMMAND chain CRETIRIA -j ACTION

-t table ：3个filter nat mangle

COMMAND：定义如何对规则进行管理

chain：指定你接下来的规则到底是在哪个链上操作的，当定义策略的时候，是可以省略的

CRETIRIA:指定匹配标准

-j ACTION :指定如何进行处理

比如：不允许172.16.0.0/24的进行访问。

iptables -t filter -A INPUT -s 172.16.0.0/16 -p udp --dport 53 -j DROP

当然你如果想拒绝的更彻底：

iptables -t filter -R INPUT 1 -s 172.16.0.0/16 -p udp --dport 53 -j REJECT

iptables -L -n -v #查看定义规则的详细信息

**四：详解COMMAND:**

**1.链管理命令（这都是立即生效的）**

-P :设置默认策略的（设定默认门是关着的还是开着的）

默认策略一般只有两种

iptables -P INPUT (DROP|ACCEPT) 默认是关的/默认是开的

比如：

iptables -P INPUT DROP 这就把默认规则给拒绝了。并且没有定义哪个动作，所以关于外界连接的所有规则包括Xshell连接之类的，远程连接都被拒绝了。

-F: FLASH，清空规则链的(注意每个链的管理权限)

iptables -t nat -F PREROUTING

iptables -t nat -F 清空nat表的所有链

-N:NEW 支持用户新建一个链

iptables -N inbound\_tcp\_web 表示附在tcp表上用于检查web的。

-X: 用于删除用户自定义的空链

使用方法跟-N相同，但是在删除之前必须要将里面的链给清空昂了

-E：用来Rename chain主要是用来给用户自定义的链重命名

-E oldname newname

-Z：清空链，及链中默认规则的计数器的（有两个计数器，被匹配到多少个数据包，多少个字节）

iptables -Z :清空

**2.规则管理命令**

-A：追加，在当前链的最后新增一个规则

-I num : 插入，把当前规则插入为第几条。

-I 3 :插入为第三条

-R num：Replays替换/修改第几条规则

格式：iptables -R 3 …………

-D num：删除，明确指定删除第几条规则

**3.查看管理命令 “-L”**

附加子命令

-n：以数字的方式显示ip，它会将ip直接显示出来，如果不加-n，则会将ip反向解析成主机名。

-v：显示详细信息

-vv

-vvv :越多越详细

-x：在计数器上显示精确值，不做单位换算

--line-numbers : 显示规则的行号

-t nat：显示所有的关卡的信息

**五：详解匹配标准**

**1.通用匹配：源地址目标地址的匹配**

-s：指定作为源地址匹配，这里不能指定主机名称，必须是IP

IP | IP/MASK | 0.0.0.0/0.0.0.0

而且地址可以取反，加一个“!”表示除了哪个IP之外

-d：表示匹配目标地址

-p：用于匹配协议的（这里的协议通常有3种，TCP/UDP/ICMP）

-i eth0：从这块网卡流入的数据

流入一般用在INPUT和PREROUTING上

-o eth0：从这块网卡流出的数据

流出一般在OUTPUT和POSTROUTING上

**2.扩展匹配**

2.1隐含扩展：对协议的扩展

-p tcp :TCP协议的扩展。一般有三种扩展

--dport XX-XX：指定目标端口,不能指定多个非连续端口,只能指定单个端口，比如

--dport 21 或者 --dport 21-23 (此时表示21,22,23)

--sport：指定源端口

--tcp-fiags：TCP的标志位（SYN,ACK，FIN,PSH，RST,URG）

对于它，一般要跟两个参数：

1.检查的标志位

2.必须为1的标志位

--tcpflags syn,ack,fin,rst syn = --syn

表示检查这4个位，这4个位中syn必须为1，其他的必须为0。所以这个意思就是用于检测三次握手的第一次包的。对于这种专门匹配第一包的SYN为1的包，还有一种简写方式，叫做--syn

-p udp：UDP协议的扩展

--dport

--sport

-p icmp：icmp数据报文的扩展

--icmp-type：

echo-request(请求回显)，一般用8 来表示

所以 --icmp-type 8 匹配请求回显数据包

echo-reply （响应的数据包）一般用0来表示

2.2显式扩展（-m）

扩展各种模块

-m multiport：表示启用多端口扩展

之后我们就可以启用比如 --dports 21,23,80

**六：详解-j ACTION**

常用的ACTION：

DROP：悄悄丢弃

一般我们多用DROP来隐藏我们的身份，以及隐藏我们的链表

REJECT：明示拒绝

ACCEPT：接受

custom\_chain：转向一个自定义的链

DNAT

SNAT

MASQUERADE：源地址伪装

REDIRECT：重定向：主要用于实现端口重定向

MARK：打防火墙标记的

RETURN：返回

在自定义链执行完毕后使用返回，来返回原规则链。

**练习题1：**

只要是来自于172.16.0.0/16网段的都允许访问我本机的172.16.100.1的SSHD服务

分析：首先肯定是在允许表中定义的。因为不需要做NAT地址转换之类的，然后查看我们SSHD服务，在22号端口上，处理机制是接受，对于这个表，需要有一来一回两个规则，如果我们允许也好，拒绝也好，对于访问本机服务，我们最好是定义在INPUT链上，而OUTPUT再予以定义就好。(会话的初始端先定义)，所以加规则就是：

定义进来的： iptables -t filter -A INPUT -s 172.16.0.0/16 -d 172.16.100.1 -p tcp --dport 22 -j ACCEPT

定义出去的： iptables -t filter -A OUTPUT -s 172.16.100.1 -d 172.16.0.0/16 -p tcp --dport 22 -j ACCEPT

将默认策略改成DROP:

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

**七：状态检测：**

是一种显式扩展，用于检测会话之间的连接关系的，有了检测我们可以实现会话间功能的扩展

什么是状态检测？对于整个TCP协议来讲，它是一个有连接的协议，三次握手中，第一次握手，我们就叫NEW连接，而从第二次握手以后的，ack都为1，这是正常的数据传输，和tcp的第二次第三次握手，叫做已建立的连接（ESTABLISHED）,还有一种状态，比较诡异的，比如：SYN=1 ACK=1 RST=1,对于这种我们无法识别的，我们都称之为INVALID无法识别的。还有第四种，FTP这种古老的拥有的特征，每个端口都是独立的，21号和20号端口都是一去一回，他们之间是有关系的，这种关系我们称之为RELATED。

所以我们的状态一共有四种：

NEW

ESTABLISHED

RELATED

INVALID

所以我们对于刚才的练习题，可以增加状态检测。比如进来的只允许状态为NEW和ESTABLISHED的进来，出去只允许ESTABLISHED的状态出去，这就可以将比较常见的反弹式木马有很好的控制机制。

对于练习题的扩展：

进来的拒绝出去的允许，进来的只允许ESTABLISHED进来，出去只允许ESTABLISHED出去。默认规则都使用拒绝

iptables -L -n --line-number ：查看之前的规则位于第几行

改写INPUT

iptables -R INPUT 2 -s 172.16.0.0/16 -d 172.16.100.1 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -R OUTPUT 1 -m state --state ESTABLISHED -j ACCEPT

此时如果想再放行一个80端口如何放行呢？

iptables -A INPUT -d 172.16.100.1 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -R INPUT 1 -d 172.16.100.1 -p udp --dport 53 -j ACCEPT

**练习题2：**

假如我们允许自己ping别人，但是别人ping自己ping不通如何实现呢？

分析：对于ping这个协议，进来的为8（ping），出去的为0(响应).我们为了达到目的，需要8出去,允许0进来

在出去的端口上：iptables -A OUTPUT -p icmp --icmp-type 8 -j ACCEPT

在进来的端口上：iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT

小扩展：对于127.0.0.1比较特殊，我们需要明确定义它

iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT

iptables -A OUTPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT

**八：SNAT和DNAT的实现**

由于我们现在IP地址十分紧俏，已经分配完了，这就导致我们必须要进行地址转换，来节约我们仅剩的一点IP资源。那么通过iptables如何实现NAT的地址转换呢？

**1.SNAT基于原地址的转换**

基于原地址的转换一般用在我们的许多内网用户通过一个外网的口上网的时候，这时我们将我们内网的地址转换为一个外网的IP，我们就可以实现连接其他外网IP的功能。

所以我们在iptables中就要定义到底如何转换：

定义的样式：

比如我们现在要将所有192.168.10.0网段的IP在经过的时候全都转换成172.16.100.1这个假设出来的外网地址：

iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -j SNAT --to-source 172.16.100.1

这样，只要是来自本地网络的试图通过网卡访问网络的，都会被统统转换成172.16.100.1这个IP.

那么，如果172.16.100.1不是固定的怎么办？

我们都知道当我们使用联通或者电信上网的时候，一般它都会在每次你开机的时候随机生成一个外网的IP，意思就是外网地址是动态变换的。这时我们就要将外网地址换成 MASQUERADE(动态伪装):它可以实现自动寻找到外网地址，而自动将其改为正确的外网地址。所以，我们就需要这样设置：

iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -j MASQUERADE

这里要注意：地址伪装并不适用于所有的地方。

**2.DNAT目标地址转换**

对于目标地址转换，数据流向是从外向内的，外面的是客户端，里面的是服务器端通过目标地址转换，我们可以让外面的ip通过我们对外的外网ip来访问我们服务器不同的服务器，而我们的服务却放在内网服务器的不同的服务器上。

如何做目标地址转换呢？：

iptables -t nat -A PREROUTING -d 192.168.10.18 -p tcp --dport 80 -j DNAT --todestination 172.16.100.2

目标地址转换要做在到达网卡之前进行转换,所以要做在PREROUTING这个位置上

九：控制规则的存放以及开启

注意：你所定义的所有内容，当你重启的时候都会失效，要想我们能够生效，需要使用一个命令将它保存起来

1.service iptables save 命令

它会保存在/etc/sysconfig/iptables这个文件中

2.iptables-save 命令

iptables-save > /etc/sysconfig/iptables

3.iptables-restore 命令

开机的时候，它会自动加载/etc/sysconfig/iptabels

如果开机不能加载或者没有加载，而你想让一个自己写的配置文件（假设为iptables.2）手动生效的话：

iptables-restore < /etc/sysconfig/iptables.2

则完成了将iptables中定义的规则手动生效

**十：总结**

Iptables是一个非常重要的工具，它是每一个防火墙上几乎必备的设置，也是我们在做大型网络的时候，为了很多原因而必须要设置的。学好Iptables,可以让我们对整个网络的结构有一个比较深刻的了解，同时，我们还能够将内核空间中数据的走向以及linux的安全给掌握的非常透彻。我们在学习的时候，尽量能结合着各种各样的项目，实验来完成，这样对你加深iptables的配置，以及各种技巧有非常大的帮助

小结:

<http://www.360doc.com/content/11/0506/09/706976_114731108.shtml>

[iptables详解](http://blog.csdn.net/comchen/article/details/7772630)

<http://blog.csdn.net/comchen/article/details/7772630>

## Selinux

几乎可以肯定每个人都听说过 SELinux (更准确的说，尝试关闭过)，甚至某些过往的经验让您对 SELinux 产生了偏见。不过随着日益增长的 0-day 安全漏洞，或许现在是时候去了解下这个在 Linux 内核中已经有8年历史的强制性访问控制系统(MAC)了。

**SELinux 与强制访问控制系统**

SELinux 全称 Security Enhanced Linux (安全强化 Linux)，是 MAC (Mandatory Access Control，强制访问控制系统)的一个实现，目的在于明确的指明某个进程可以访问哪些资源(文件、网络端口等)。

强制访问控制系统的用途在于增强系统抵御 0-Day 攻击(利用尚未公开的漏洞实现的攻击行为)的能力。所以它不是网络防火墙或 ACL 的替代品，在用途上也不重复。

举例来说，系统上的 Apache 被发现存在一个漏洞，使得某远程用户可以访问系统上的敏感文件(比如 /etc/passwd 来获得系统已存在用户)，而修复该安全漏洞的 Apache 更新补丁尚未释出。此时 SELinux 可以起到弥补该漏洞的缓和方案。因为 /etc/passwd 不具有 Apache 的访问标签，所以 Apache 对于 /etc/passwd 的访问会被 SELinux 阻止。

相比其他强制性访问控制系统，**SELinux 有如下优势：**

●控制策略是可查询而非程序不可见的。

●可以热更改策略而无需重启或者停止服务。

●可以从进程初始化、继承和程序执行三个方面通过策略进行控制。

●控制范围覆盖文件系统、目录、文件、文件启动描述符、端口、消息接口和网络接口。

那么 SELinux 对于系统性能有什么样的影响呢?根据 Phoronix 在 2009 年使用 Fedora 11 所做的横向比较来看，开启 SELinux 仅在少数情况下导致系统性能约 5% 的降低。

SELinux 是不是会十分影响一般桌面应用及程序开发呢?原先是，因为 SELinux 的策略主要针对服务器环境。但随着 SELinux 8年来的广泛应用，目前 SELinux 策略在一般桌面及程序开发环境下依然可以同时满足安全性及便利性的要求。以刚刚发布的 Fedora 15 为例，笔者在搭建完整的娱乐(包含多款第三方原生 Linux 游戏及 Wine 游戏)及开发环境(Android SDK + Eclipse)过程中，只有 Wine 程序的首次运行时受到 SELinux 默认策略的阻拦，在图形化的“SELinux 故障排除程序”帮助下，点击一下按钮就解决了。

**了解和配置 SELinux**

**1. 获取当前 SELinux 运行状态**

getenforce

可能返回结果有三种：Enforcing、Permissive 和 Disabled。Disabled 代表 SELinux 被禁用，Permissive 代表仅记录安全警告但不阻止可疑行为，Enforcing 代表记录警告且阻止可疑行为。

目前常见发行版中，RHEL 和 Fedora 默认设置为 Enforcing，其余的如 openSUSE 等为 Permissive。

**2. 改变 SELinux 运行状态**

setenforce [ Enforcing | Permissive | 1 | 0 ]

该命令可以立刻改变 SELinux 运行状态，在 Enforcing 和 Permissive 之间切换，结果保持至关机。一个典型的用途是看看到底是不是 SELinux 导致某个服务或者程序无法运行。若是在 setenforce 0 之后服务或者程序依然无法运行，那么就可以肯定不是 SELinux 导致的。

若是想要永久变更系统 SELinux 运行环境，可以通过更改配置文件 /etc/sysconfig/selinux 实现。注意当从 Disabled 切换到 Permissive 或者 Enforcing 模式后需要重启计算机并为整个文件系统重新创建安全标签(touch /.autorelabel && reboot)。

**3. SELinux 运行策略**

配置文件 /etc/sysconfig/selinux 还包含了 SELinux 运行策略的信息，通过改变变量 SELINUXTYPE 的值实现，该值有两种可能：targeted 代表仅针对预制的几种网络服务和访问请求使用 SELinux 保护，strict 代表所有网络服务和访问请求都要经过 SELinux。

RHEL 和 Fedora 默认设置为 targeted，包含了对几乎所有常见网络服务的 SELinux 策略配置，已经默认安装并且可以无需修改直接使用。

若是想自己编辑 SELinux 策略，也提供了命令行下的策略编辑器 seedit 以及 Eclipse 下的编辑插件 eclipse-slide 。

**4. coreutils 工具的 SELinux 模式**

常见的属于 coreutils 的工具如 ps、ls 等等，可以通过增加 Z 选项的方式获知 SELinux 方面的信息。

如

ps auxZ | grep lldpad system\_u:system\_r:initrc\_t:s0 root 1000 8.9 0.0 3040 668 ? Ss 21:01 6:08 /usr/sbin/lldpad -d

如

ls -Z /usr/lib/xulrunner-2/libmozjs.so -rwxr-xr-x. root root system\_u:object\_r:lib\_t:s0 /usr/lib/xulrunner-2/libmozjs.so

以此类推，Z 选项可以应用在几乎全部 coreutils 工具里。

**Apache SELinux 配置实例**

**1. 让 Apache 可以访问位于非默认目录下的网站文件**

首先，用 semanage fcontext -l | grep '/var/www' 获知默认 /var/www 目录的 SELinux 上下文：

/var/www(/.\*)? all files system\_u:object\_r:httpd\_sys\_content\_t:s0

从中可以看到 Apache 只能访问包含 httpdsyscontent\_t 标签的文件。

假设希望 Apache 使用 /srv/www 作为网站文件目录，那么就需要给这个目录下的文件增加 httpdsyscontent\_t 标签，分两步实现。

首先为 /srv/www 这个目录下的文件添加默认标签类型：semanage fcontext -a -t httpd\_sys\_content\_t '/srv/www(/.\*)?' 然后用新的标签类型标注已有文件：restorecon -Rv /srv/www 之后 Apache 就可以使用该目录下的文件构建网站了。

其中 restorecon 在 SELinux 管理中很常见，起到恢复文件默认标签的作用。比如当从用户主目录下将某个文件复制到 Apache 网站目录下时，Apache 默认是无法访问，因为用户主目录的下的文件标签是 userhomet。此时就需要 restorecon 将其恢复为可被 Apache 访问的httpdsyscontent\_t 类型：

restorecon reset /srv/www/foo.com/html/file.html context unconfined\_u:object\_r:user\_home\_t:s0->system\_u:object\_r:httpd\_sys\_content\_t:s0

**2. 让 Apache 侦听非标准端口**

默认情况下 Apache 只侦听 80 和 443 两个端口，若是直接指定其侦听 888 端口的话，会在 service httpd restart 的时候报错：

Starting httpd: (13)Permission denied: make\_sock: could not bind to address [::]:888 (13)Permission denied: make\_sock: could not bind to address 0.0.0.0:888 no listening sockets available, shutting down Unable to open logs

这个时候，若是在桌面环境下 SELinux 故障排除工具应该已经弹出来报错了。若是在终端下，可以通过查看 /var/log/messages 日志然后用sealert -l 加编号的方式查看，或者直接使用 sealert -b 浏览。无论哪种方式，内容和以下会比较类似：

SELinux is preventing /usr/sbin/httpd from name\_bind access on the tcp\_socket port 888. \*\*\*\*\* Plugin bind\_ports (92.2 confidence) suggests \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* If you want to allow /usr/sbin/httpd to bind to network port 888 Then you need to modify the port type. Do # semanage port -a -t PORT\_TYPE -p tcp 888 `where PORT\_TYPE is one of the following: ntop\_port\_t, http\_cache\_port\_t, http\_port\_t.` \*\*\*\*\* Plugin catchall\_boolean (7.83 confidence) suggests \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* If you want to allow system to run with NIS Then you must tell SELinux about this by enabling the 'allow\_ypbind' boolean. Do setsebool -P allow\_ypbind 1 \*\*\*\*\* Plugin catchall (1.41 confidence) suggests \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* If you believe that httpd should be allowed name\_bind access on the port 888 tcp\_socket by default. Then you should report this as a bug. You can generate a local policy module to allow this access. Do allow this access for now by executing: # grep httpd /var/log/audit/audit.log | audit2allow -M mypol # semodule -i mypol.pp

可以看出 SELinux 根据三种不同情况分别给出了对应的解决方法。在这里，第一种情况是我们想要的，于是按照其建议输入：

semanage port -a -t http\_port\_t -p tcp 888

之后再次启动 Apache 服务就不会有问题了。

这里又可以见到 semanage 这个 SELinux 管理配置工具。它第一个选项代表要更改的类型，然后紧跟所要进行操作。详细内容参考 Man 手册

**3. 允许 Apache 访问创建私人网站**

若是希望用户可以通过在 ~/public\_html/ 放置文件的方式创建自己的个人网站的话，那么需要在 Apache 策略中允许该操作执行。使用：

setsebool httpd\_enable\_homedirs 1

setsebool 是用来切换由布尔值控制的 SELinux 策略的，当前布尔值策略的状态可以通过 getsebool 来获知。

默认情况下 setsebool 的设置只保留到下一次重启之前，若是想永久生效的话，需要添加 -P 参数，比如：

setsebool -P httpd\_enable\_homedirs 1

**总结**

1.selinux类似于防火墙，主要是保护自己的，而不是阻止别人的 。

2.如果希望您的服务器能有效抵挡 0-day 攻击时（），那么 SELinux 或许就是一个值得考虑的缓和方案。

原文：http://linuxtoy.org/archives/selinux-introduction.html

# 常用命令

在线命令详解：<http://man.linuxde.net/>

不同Linux发行版的命令数量不一样，但Linux发行版本最少的命令也有200多个。系统中的作用分成下面六个部分一一介绍。

◆ 安装和登录命令：login、shutdown、halt、reboot、install、mount、umount、chsh、exit、last；

◆ 文件处理命令：file、mkdir、grep、dd、find、mv、ls、diff、cat、ln；

◆ 系统管理相关命令：df、top、free、quota、at、lp、adduser、groupadd、kill、crontab；

◆ 网络操作命令：ifconfig、ip、ping、netstat、telnet、ftp、route、rlogin、rcp、finger、mail、 nslookup；

◆ 系统安全相关命令：passwd、su、umask、chgrp、chmod、chown、chattr、sudo ps、who；

◆ 其它命令：tar、unzip、gunzip、unarj、mtools、man、unendcode、uudecode。

## 安装与登陆命令

Df

login

1.作用

login的作用是登录系统，它的使用权限是所有用户。

2.格式

login [name][－p ][－h 主机名称]

3.主要参数

－p:通知login保持现在的环境参数。

－h:用来向远程登录的之间传输用户名。

如果选择用命令行模式登录Linux的话，那么看到的第一个Linux命令就是login：。

一般界面是这样的：

Manddrake Linux release 9.1(Bamboo) for i586

renrel 2.4.21－0.13mdk on i686 / tty1

localhost login:root

password:

上面代码中，第一行是Linux发行版本号，第二行是内核版本号和登录的虚拟控制台，我们在第三行输入登录名，按“Enter”键在Password后输入账户密码，即可登录系统。出于安全考虑，输入账户密码时字符不会在屏幕上回显，光标也不移动。

登录后会看到下面这个界面（以超级用户为例）：

[root@localhost root]#

last login:Tue ,Nov 18 10:00:55 on vc/1

上面显示的是登录星期、月、日、时间和使用的虚拟控制台。

4.应用技巧

Linux

是一个真正的多用户操作系统，可以同时接受多个用户登录，还允许一个用户进行多次登录。这是因为Linux和许多版本的Unix一样，提供了虚拟控制台的

访问方式，允许用户在同一时间从控制台（系统的控制台是与系统直接相连的监视器和键盘）进行多次登录。每个虚拟控制台可以看作是一个独立的工作站，工作台

之间可以切换。虚拟控制台的切换可以通过按下Alt键和一个功能键来实现，通常使用F1-F6 。

例如，用户登录后，按一下“Alt+

F2”键，用户就可以看到上面出现的“login:”提示符，说明用户看到了第二个虚拟控制台。然后只需按“Alt+

F1”键，就可以回到第一个虚拟控制台。一个新安装的Linux系统允许用户使用“Alt+F1”到“Alt+F6”键来访问前六个虚拟控制台。虚拟控制

台最有用的是，当一个程序出错造成系统死锁时，可以切换到其它虚拟控制台工作，关闭这个程序。

shutdown

1.作用

shutdown命令的作用是关闭计算机，它的使用权限是超级用户。

2.格式

shutdown [－h][－i][－k][－m][－t]

3.重要参数

－t：在改变到其它运行级别之前，告诉init程序多久以后关机。

－k：并不真正关机，只是送警告信号给每位登录者。

－h：关机后关闭电源。

－c：cancel current process取消目前正在执行的关机程序。所以这个选项当然没有时间参数，但是可以输入一个用来解释的讯息，而这信息将会送到每位使用者。

－F：在重启计算机时强迫fsck。

－time：设定关机前的时间。

－m: 将系统改为单用户模式。

－i：关机时显示系统信息。

4.命令说明

shutdown

命令可以安全地将系统关机。有些用户会使用直接断掉电源的方式来关闭Linux系统，这是十分危险的。因为Linux与Windows不同，其后台运行着

许多进程，所以强制关机可能会导致进程的数据丢失，使系统处于不稳定的状态，甚至在有的系统中会损坏硬件设备（硬盘）。在系统关机前使用

shutdown命令，系统管理员会通知所有登录的用户系统将要关闭，并且login指令会被冻结，即新的用户不能再登录。

halt

1.作用

halt命令的作用是关闭系统，它的使用权限是超级用户。

2.格式

halt [－n] [－w] [－d] [－f] [－i] [－p]

3.主要参数说明

－n：防止sync系统调用，它用在用fsck修补根分区之后，以阻止内核用老版本的超级块覆盖修补过的超级块。

－w：并不是真正的重启或关机,只是写wtmp（/var/log/wtmp）纪录。

－f：没有调用shutdown，而强制关机或重启。

－i：关机（或重启）前，关掉所有的网络接口。

－f：强迫关机，不呼叫shutdown这个指令。

－p: 当关机的时候顺便做关闭电源的动作。

－d：关闭系统，但不留下纪录。

4.命令说明

halt

就是调用shutdown

－h。halt执行时，杀死应用进程，执行sync(将存于buffer中的资料强制写入硬盘中)系统调用，文件系统写操作完成后就会停止内核。若系统的

运行级别为0或6，则关闭系统；否则以shutdown指令（加上－h参数）来取代。

reboot

1.作用

reboot命令的作用是重新启动计算机，它的使用权限是系统管理者。

2.格式

reboot [－n] [－w] [－d] [－f] [－i]

3.主要参数

－n: 在重开机前不做将记忆体资料写回硬盘的动作。

－w: 并不会真的重开机，只是把记录写到/var/log/wtmp文件里。

－d: 不把记录写到/var/log/wtmp文件里（－n这个参数包含了－d）。

－i: 在重开机之前先把所有与网络相关的装置停止。

install

1.作用

install命令的作用是安装或升级软件或备份数据，它的使用权限是所有用户。

2.格式

(1)install [选项]... 来源 目的地

(2)install [选项]... 来源... 目录

(3)install －d [选项]... 目录...

在

前两种格式中，会将复制至或将多个文件复制至已存在的，同时设定权

限模式及所有者/所属组。在第三种格式中，会创建所有指定的目录及它们的主目录。长选项必须用的参数在使用短选项时也是必须的。

3.主要参数

－－backup[=CONTROL]：为每个已存在的目的地文件进行备份。

－b：类似 －－backup，但不接受任何参数。

－c：(此选项不作处理)。

－d，－－directory：所有参数都作为目录处理，而且会创建指定目录的所有主目录。

－D：创建前的所有主目录，然后将复制至 ；在第一种使用格式中有用。

－g，－－group=组：自行设定所属组，而不是进程目前的所属组。

－m，－－mode=模式：自行设定权限模式 (像chmod)，而不是rwxr－xr－x。

－o，－－owner=所有者：自行设定所有者 (只适用于超级用户)。

－p，－－preserve－timestamps：以文件的访问/修改时间作为相应的目的地文件的时间属性。

－s，－－strip：用strip命令删除symbol table，只适用于第一及第二种使用格式。

－S，－－suffix=后缀：自行指定备份文件的。

－v，－－verbose：处理每个文件/目录时印出名称。

－－help：显示此帮助信息并离开。

－－version：显示版本信息并离开。

mount

1.作用

mount命令的作用是加载文件系统，它的用权限是超级用户或/etc/fstab中允许的使用者。

2.格式

mount －a [－fv] [－t vfstype] [－n] [－rw] [－F] device dir

3.主要参数

－h：显示辅助信息。

－v：显示信息，通常和－f用来除错。

－a：将/etc/fstab中定义的所有文件系统挂上。

－F：这个命令通常和－a一起使用，它会为每一个mount的动作产生一个行程负责执行。在系统需要挂上大量NFS文件系统时可以加快加载的速度。

－f：通常用于除错。它会使mount不执行实际挂上的动作，而是模拟整个挂上的过程，通常会和－v一起使用。

－t vfstype：显示被加载文件系统的类型。

－n：一般而言，mount挂上后会在/etc/mtab中写入一笔资料，在系统中没有可写入文件系统的情况下，可以用这个选项取消这个动作。

4.应用技巧

在Linux

和Unix系统上，所有文件都是作为一个大型树（以/为根）的一部分访问的。要访问CD-ROM上的文件，需要将CD-ROM设备挂装在文件树中的某个挂

装点。如果发行版安装了自动挂装包，那么这个步骤可自动进行。在Linux中，如果要使用硬盘、光驱等储存设备，就得先将它加载，当储存设备挂上了之后，

就可以把它当成一个目录来访问。挂上一个设备使用mount命令。在使用mount这个指令时，至少要先知道下列三种信息：要加载对象的文件系统类型、要

加载对象的设备名称及要将设备加载到哪个目录下。

（1）Linux可以识别的文件系统

◆ Windows 95/98常用的FAT 32文件系统：vfat ；

◆ Win NT/2000 的文件系统：ntfs ；

◆ OS/2用的文件系统：hpfs；

◆ Linux用的文件系统：ext2、ext3；

◆ CD-ROM光盘用的文件系统：iso9660。

虽然vfat是指FAT 32系统，但事实上它也兼容FAT 16的文件系统类型。

（2）确定设备的名称

在Linux

中，设备名称通常都存在/dev里。这些设备名称的命名都是有规则的，可以用“推理”的方式把设备名称找出来。例如，/dev/hda1这个

IDE设备，hd是Hard Disk(硬盘)的，sd是SCSI Device，fd是Floppy Device(或是Floppy

Disk?)。a代表第一个设备，通常IDE接口可以接上4个IDE设备(比如4块硬盘)。所以要识别IDE硬盘的方法分别就是hda、hdb、hdc、

hdd。hda1中的“1”代表hda的第一个硬盘分区

(partition)，hda2代表hda的第二主分区，第一个逻辑分区从hda5开始，依此类推。此外，可以直接检查

/var/log/messages文件，在该文件中可以找到计算机开机后系统已辨认出来的设备代号。

（3）查找挂接点

在决

定将设备挂接之前，先要查看一下计算机是不是有个/mnt的空目录，该目录就是专门用来当作挂载点(Mount

Point)的目录。建议在/mnt里建几个/mnt/cdrom、/mnt/floppy、/mnt/mo等目录，当作目录的专用挂载点。举例而言，如

要挂载下列5个设备，其执行指令可能如下 (假设都是Linux的ext2系统，如果是Windows XX请将ext2改成vfat)：

软盘 ===>mount －t ext2 /dev/fd0 /mnt/floppy

cdrom ===>mount －t iso9660 /dev/hdc /mnt/cdrom

SCSI cdrom ===>mount －t iso9660 /dev/sdb /mnt/scdrom

SCSI cdr ===>mount －t iso9660 /dev/sdc /mnt/scdr

不过目前大多数较新的Linux发行版本（包括红旗 Linux、中软Linux、Mandrake Linux等）都可以自动挂装文件系统，但Red Hat Linux除外。

umount

1.作用

umount命令的作用是卸载一个文件系统，它的使用权限是超级用户或/etc/fstab中允许的使用者。

2.格式

unmount －a [－fFnrsvw] [－t vfstype] [－n] [－rw] [－F] device dir

3.使用说明

umount

命令是mount命令的逆操作，它的参数和使用方法和mount命令是一样的。Linux挂装CD-ROM后，会锁定CD—ROM，这样就不能用CD-

ROM面板上的Eject按钮弹出它。但是，当不再需要光盘时，如果已将/cdrom作为符号链接，请使用umount/cdrom来卸装它。仅当无用户

正在使用光盘时，该命令才会成功。该命令包括了将带有当前工作目录当作该光盘中的目录的终端窗口。

chsh

1.作用

chsh命令的作用是更改使用者shell设定，它的使用权限是所有使用者。

2.格式

chsh [ －s ] [ －list] [ －－help ] [ －v ] [ username ]

3.主要参数

－l：显示系统所有Shell类型。

－v：显示Shell版本号。

4.应用技巧

前面介绍了Linux下有多种Shell，一般缺省的是Bash，如果想更换Shell类型可以使用chsh命令。先输入账户密码，然后输入新Shell类型，如果操作正确系统会显示“Shell change”。其界面一般如下：

Changing fihanging shell for cao

Password:

New shell [/bin/bash]: /bin/tcsh

上面代码中，[ ]内是目前使用的Shell。普通用户只能修改自己的Shell，超级用户可以修改全体用户的Shell。要想查询系统提供哪些Shell，可以使用chsh -l 命令，见图1所示。

图1 系统可以使用的Shell类型

从图1中可以看到，笔者系统中可以使用的Shell有bash（缺省）、csh、sh、tcsh四种。

exit

1.作用

exit命令的作用是退出系统，它的使用权限是所有用户。

2.格式

exit

3.参数

exit命令没有参数，运行后退出系统进入登录界面。

last

1.作用

last命令的作用是显示近期用户或终端的登录情况，它的使用权限是所有用户。通过last命令查看该程序的log，管理员可以获知谁曾经或企图连接系统。

2.格式

1ast[—n][－f file][－t tty] [—h 节点][－I —IP][—1][－y][1D]

3.主要参数

－n：指定输出记录的条数。

－f file：指定用文件file作为查询用的log文件。

－t tty：只显示指定的虚拟控制台上登录情况。

－h 节点：只显示指定的节点上的登录情况。

－i IP：只显示指定的IP上登录的情况。

－1：用IP来显示远端地址。

－y：显示记录的年、月、日。

－ID：知道查询的用户名。

－x:显示系统关闭、用户登录和退出的历史。

动手练习

上面介绍了Linux安装和登录命令，下面介绍几个实例，动手练习一下刚才讲过的命令。

1.一次运行多个命令

在一个命令行中可以执行多个命令，用分号将各个命令隔开即可，例如：

＃last －x；halt

上面代码表示在显示系统关闭、用户登录和退出的历史后关闭计算机。

2.利用mount挂装文件系统访问Windows系统

许多Linux发行版本现在都可以自动加载Vfat分区来访问Windows系统，而Red Hat各个版本都没有自动加载Vfat分区，因此还需要进行手工操作。

mount

可以将Windows分区作为Linux的一个“文件”挂接到Linux的一个空文件夹下，从而将Windows的分区和/mnt这个目录联系起来。因

此，只要访问这个文件夹就相当于访问该分区了。首先要在/mnt下建立winc文件夹，在命令提示符下输入下面命令：

＃mount -t vfat /dev/hda1 /mnt/winc

即

表示将Windows的C分区挂到Liunx的/mnt/winc目录下。这时，在/mnt/winc目录下就可以看到Windows中C盘的内容了。使

用类似的方法可以访问Windows系统的D、E盘。在Linux系统显示Windows的分区一般顺序这样的：hda1为C盘、hda5为D盘、

hda6为E盘……以此类推。上述方法可以查看Windows系统有一个很大的问题，就是Windows中的所有中文文件名或文件夹名全部显示为问号

“？”，而英文却可以正常显示。我们可以通过加入一些参数让它显示中文。还以上面的操作为例，此时输入命令：

＃mount -t vfat -o iocharset=cp936 /dev/hda1 /mnt/winc

现在它就可以正常显示中文了。

3.使用mount加挂闪盘上的文件系统

在Linux下使用闪盘非常简单。Linux对USB设备有很好的支持，当插入闪盘后，闪盘被识别为一个SCSI盘，通常输入以下命令：

＃ mount /dev/sda1 /usb

就能够加挂闪盘上的文件系统。

小知识

Linux命令与Shell

所

谓Shell，就是命令解释程序，它提供了程序设计接口，可以使用程序来编程。学习Shell对于Linux初学者理解Linux系统是非常重要的。

Linux系统的Shell作为操作系统的外壳，为用户提供了使用操作系统的接口。Shell是命令语言、命令解释程序及程序设计语言的统称，是用户和

Linux内核之间的接口程序。如果把Linux内核想象成一个球体的中心，Shell就是围绕内核的外层。当从Shell或其它程序向Linux传递命

令时，内核会做出相应的反应。Shell在Linux系统的作用和MS DOS下的COMMAND.COM和Windows 95/98 的

explorer.exe相似。Shell虽然不是系统核心的一部分，只是系统核心的一个外延，但它能够调用系统内核的大部分功能。因此，可以说

Shell是Unux/Linux最重要的实用程序。

Linux中的Shell有多种类型，其中最常用的是Bourne

Shell(sh)、C Shell(csh)和Korn Shell(ksh)。大多数Linux发行版本缺省的Shell是Bourne

Again Shell，它是Bourne Shell的扩展，简称bash，与Bourne Shell完全向后兼容，并且在Bourne

Shell的基础上增加了很多特性。bash放在/bin/bash中，可以提供如命令补全、命令编辑和命令历史表等功能。它还包含了很多C

Shell和Korn

Shell中的优点，有灵活和强大的编程接口，同时又有很友好的用户界面。Linux系统中200多个命令中有40个是bash的内部命令，主要包括

exit、less、lp、kill、 cd、pwd、fc、fg等。

## 文件处理命令

D

Linux

系统信息存放在文件里，文件与普通的公务文件类似。每个文件都有自己的名字、内容、存放地址及其它一些管理信息，如文件的用户、文件的大小等。文件可以是

一封信、一个通讯录，或者是程序的源语句、程序的数据，甚至可以包括可执行的程序和其它非正文内容。

Linux文件系统具有良好的结构，系统提供了很多文件处理程序。这里主要介绍常用的文件处理命令。

file

1.作用 件内容判断文件类型，使用权限是所有用户。

2.格式

file通过探测文

file [options] 文件名

3.[options]主要参数

-v：在标准输出后显示版本信息，并且退出。

-z：探测压缩过的文件类型。

-L：允许符合连接。

-f name：从文件namefile中读取要分析的文件名列表。

4.简单说明

使用file命令可以知道某个文件究竟是二进制（ELF格式）的可执行文件, 还是Shell Script文件，或者是其它的什么格式。file能识别的文件类型有目录、Shell脚本、英文文本、二进制可执行文件、C语言源文件、文本文件、DOS的可执行文件。

5.应用实例

如果我们看到一个没有后缀的文件grap，可以使用下面命令：

$ file grap

grap： English text

此时系统显示这是一个英文文本文件。需要说明的是，file命令不能探测包括图形、音频、视频等多媒体文件类型。

mkdir

1.作用

mkdir命令的作用是建立名称为dirname的子目录，与MS DOS下的md命令类似，它的使用权限是所有用户。

2.格式

mkdir [options] 目录名

3.[options]主要参数

－m, －－mode=模式：设定权限，与chmod类似。

－p, －－parents：需要时创建上层目录；如果目录早已存在，则不当作错误。

－v, －－verbose：每次创建新目录都显示信息。

－－version：显示版本信息后离开。

rm

1. rm -rf /var/log/httpd/access

将会删除文件夹 /var/log/httpd/access目录以及其下所有文件、文件夹

1. 2

删除文件使用实例：

rm -f /var/log/httpd/access.log

将会强制删除/var/log/httpd/access.log这个文件

4.应用实例

在进行目录创建时可以设置目录的权限，此时使用的参数是“－m”。假设要创建的目录名是“tsk”，让所有用户都有rwx(即读、写、执行的权限)，那么可以使用以下命令：

$ mkdir －m 777 tsk

grep

1.作用

grep命令可以指定文件中搜索特定的内容，并将含有这些内容的行标准输出。grep全称是Global Regular Expression Print，表示全局正则表达式版本，它的使用权限是所有用户。

2.格式

grep [options]

3.主要参数

[options]主要参数：

－c：只输出匹配行的计数。

－I：不区分大小写（只适用于单字符）。

－h：查询多文件时不显示文件名。

－l：查询多文件时只输出包含匹配字符的文件名。

－n：显示匹配行及行号。

－s：不显示不存在或无匹配文本的错误信息。

－v：显示不包含匹配文本的所有行。

pattern正则表达式主要参数：

\：忽略正则表达式中特殊字符的原有含义。

^：匹配正则表达式的开始行。

$: 匹配正则表达式的结束行。

\：到匹配正则表达式的行结束。

[ ]：单个字符，如[A]即A符合要求 。

[ - ]：范围，如[A-Z]，即A、B、C一直到Z都符合要求 。

。：所有的单个字符。

\* ：有字符，长度可以为0。

正

则表达式是Linux/Unix系统中非常重要的概念。正则表达式（也称为“regex”或“regexp”）是一个可以描述一类字符串的模式

（Pattern）。如果一个字符串可以用某个正则表达式来描述，我们就说这个字符和该正则表达式匹配（Match）。这和DOS中用户可以使用通配符

“\*”代表任意字符类似。在Linux系统上，正则表达式通常被用来查找文本的模式，以及对文本执行“搜索－替换”操作和其它功能。

4.应用实例

查

询DNS服务是日常工作之一，这意味着要维护覆盖不同网络的大量IP地址。有时IP地址会超过2000个。如果要查看nnn.nnn网络地址，但是却忘了

第二部分中的其余部分，只知到有两个句点，例如nnn nn..。要抽取其中所有nnn.nnn IP地址，使用[0－9 ]\{3

\}\.[0－0\{3\}\。含义是任意数字出现3次，后跟句点，接着是任意数字出现3次，后跟句点。

$grep '[0－9 ]\{3 \}\.[0－0\{3\}\' ipfile

补充说明，grep家族还包括fgrep和egrep。fgrep是fix grep，允许查找字符串而不是一个模式；egrep是扩展grep，支持基本及扩展的正则表达式，但不支持\q模式范围的应用及与之相对应的一些更加规范的模式。

dd

1.作用

dd命令用来复制文件，并根据参数将数据转换和格式化。

2.格式

dd [options]

3.[opitions]主要参数

bs=字节：强迫 ibs=及obs=。

cbs=字节：每次转换指定的。

conv=关键字：根据以逗号分隔的关键字表示的方式来转换文件。

count=块数目：只复制指定的输入数据。

ibs=字节：每次读取指定的。

if=文件：读取内容，而非标准输入的数据。

obs=字节：每次写入指定的。

of=文件：将数据写入，而不在标准输出显示。

seek=块数目：先略过以obs为单位的指定的输出数据。

skip=块数目：先略过以ibs为单位的指定的输入数据。

4.应用实例

dd命令常常用来制作Linux启动盘。先找一个可引导内核，令它的根设备指向正确的根分区，然后使用dd命令将其写入软盘：

$ rdev vmlinuz /dev/hda

$dd if＝vmlinuz of＝/dev/fd0

上面代码说明，使用rdev命令将可引导内核vmlinuz中的根设备指向/dev/hda，请把“hda”换成自己的根分区，接下来用dd命令将该内核写入软盘。

find

1.作用

find命令的作用是在目录中搜索文件，它的使用权限是所有用户。

2.格式

find [path][options][expression]

path指定目录路径，系统从这里开始沿着目录树向下查找文件。它是一个路径列表，相互用空格分离，如果不写path，那么默认为当前目录。

3.主要参数

[options]参数：

－depth：使用深度级别的查找过程方式，在某层指定目录中优先查找文件内容。

－maxdepth levels：表示至多查找到开始目录的第level层子目录。level是一个非负数，如果level是0的话表示仅在当前目录中查找。

－mindepth levels：表示至少查找到开始目录的第level层子目录。

－mount：不在其它文件系统（如Msdos、Vfat等）的目录和文件中查找。

－version：打印版本。

[expression]是匹配表达式，是find命令接受的表达式，find命令的所有操作都是针对表达式的。它的参数非常多，这里只介绍一些常用的参数。

—name：支持统配符\*和?。

－atime n：搜索在过去n天读取过的文件。

－ctime n：搜索在过去n天修改过的文件。

－group grpoupname：搜索所有组为grpoupname的文件。

－user 用户名：搜索所有文件属主为用户名（ID或名称）的文件。

－size n：搜索文件大小是n个block的文件。

－print：输出搜索结果，并且打印。

4.应用技巧

find命令查找文件的几种方法：

（1）根据文件名查找

例如，我们想要查找一个文件名是lilo.conf的文件，可以使用如下命令：

find / －name lilo.conf

find命令后的“/”表示搜索整个硬盘。

（2）快速查找文件

根

据文件名查找文件会遇到一个实际问题，就是要花费相当长的一段时间，特别是大型Linux文件系统和大容量硬盘文件放在很深的子目录中时。如果我们知道了

这个文件存放在某个目录中，那么只要在这个目录中往下寻找就能节省很多时间。比如smb.conf文件，从它的文件后缀“.conf”可以判断这是一个配

置文件，那么它应该在/etc目录内，此时可以使用下面命令：

find /etc －name smb.conf

这样，使用“快速查找文件”方式可以缩短时间。

（3）根据部分文件名查找方法

有时我们知道只某个文件包含有abvd这4个字，那么要查找系统中所有包含有这4个字符的文件可以输入下面命令：

find / －name '\*abvd\*'

输入这个命令以后，Linux系统会将在/目录中查找所有的包含有abvd这4个字符的文件（其中\*是通配符），比如abvdrmyz等符合条件的文件都能显示出来。

(4) 使用混合查找方式查找文件

find命令可以使用混合查找的方法，例如，我们想在/etc目录中查找大于500000字节，并且在24小时内修改的某个文件，则可以使用-and (与)把两个查找参数链接起来组合成一个混合的查找方式。

find /etc -size +500000c -and -mtime +1

find / -name "police" -type d

mv

1.作用

mv命令用来为文件或目录改名，或者将文件由一个目录移入另一个目录中，它的使用权限是所有用户。该命令如同DOS命令中的ren和move的组合。

2.格式

mv[options] 源文件或目录 目标文件或目录

3.[options]主要参数

－i：交互方式操作。如果mv操作将导致对已存在的目标文件的覆盖，此时系统询问是否重写，要求用户回答“y”或“n”，这样可以避免误覆盖文件。

－f：禁止交互操作。mv操作要覆盖某个已有的目标文件时不给任何指示，指定此参数后i参数将不再起作用。

4.应用实例

（1）将/usr/cbu中的所有文件移到当前目录（用“.”表示）中：

$ mv /usr/cbu/ \* .

（2）将文件cjh.txt重命名为wjz.txt：

$ mv cjh.txt wjz.txt

ls

linux下重命名文件或文件夹的命令mv既可以重命名，又可以移动文件或文件夹.

例子：将目录A重命名为B

mv A B

例子：将/a目录移动到/b下，并重命名为c

mv /a /b/c

1.作用

ls命令用于显示目录内容，类似DOS下的dir命令，它的使用权限是所有用户。

2.格式

ls [options][filename]

3.options主要参数

－a, －－all：不隐藏任何以“.” 字符开始的项目。

－A, －－almost－all：列出除了“ . ”及 “.. ”以外的任何项目。

－－author：印出每个文件著作者。

－b, －－escape：以八进制溢出序列表示不可打印的字符。

－－block－size=大小：块以指定的字节为单位。

－B, －－ignore－backups：不列出任何以 ~ 字符结束的项目。

－f：不进行排序，－aU参数生效，－lst参数失效。

－F, －－classify：加上文件类型的指示符号 (\*/=@| 其中一个)。

－g：like －l, but do not list owner。

－G, －－no－group：inhibit display of group information。

－i, －－inode：列出每个文件的inode号。

－I, －－ignore=样式：不印出任何符合Shell万用字符的项目。

－k：即－－block－size=1K。

－l：使用较长格式列出信息。

－L, －－dereference：当显示符号链接的文件信息时，显示符号链接所指示的对象，而并非符号链接本身的信息。

－m：所有项目以逗号分隔，并填满整行行宽。

－n, －－numeric－uid－gid：类似－l，但列出UID及GID号。

－N, －－literal：列出未经处理的项目名称，例如不特别处理控制字符。

－p, －－file－type：加上文件类型的指示符号 (/=@| 其中一个)。

－Q, －－quote－name：将项目名称括上双引号。

－r, －－reverse：依相反次序排列。

－R, －－recursive：同时列出所有子目录层。

－s, －－size：以块大小为序。

4.应用举例

ls

命令是Linux系统使用频率最多的命令，它的参数也是Linux命令中最多的。使用ls命令时会有几种不同的颜色，其中蓝色表示是目录，绿色表示是可执

行文件，红色表示是压缩文件，浅蓝色表示是链接文件，加粗的黑色表示符号链接，灰色表示是其它格式文件。ls最常使用的是ls- l，见图1所示。

图1 使用ls-l命令

文

件类型开头是由10个字符构成的字符串。其中第一个字符表示文件类型，它可以是下述类型之一：－（普通文件）、d（目录）、l（符号链接）、b（块设备文

件）、c（字符设备文件）。后面的9个字符表示文件的访问权限，分为3组，每组3位。第一组表示文件属主的权限，第二组表示同组用户的权限，第三组表示其

他用户的权限。每一组的三个字符分别表示对文件的读（r）、写（w）和执行权限（x）。对于目录，表示进入权限。s表示当文件被执行时，把该文件的UID

或GID赋予执行进程的UID（用户ID）或GID（组

ID）。t表示设置标志位（留在内存，不被换出）。如果该文件是目录，那么在该目录中的文件只能被超级用户、目录拥有者或文件属主删除。如果它是可执行文

件，那么在该文件执行后，指向其正文段的指针仍留在内存。这样再次执行它时，系统就能更快地装入该文件。接着显示的是文件大小、生成时间、文件或命令名

称。

diff

1.作用

diff命令用于两个文件之间的比较，并指出两者的不同，它的使用权限是所有用户。

2.格式

diff [options] 源文件 目标文件

3.[options]主要参数

-a：将所有文件当作文本文件来处理。

-b：忽略空格造成的不同。

-B：忽略空行造成的不同。

-c：使用纲要输出格式。

-H：利用试探法加速对大文件的搜索。

-I：忽略大小写的变化。

-n --rcs：输出RCS格式。

cmp

1.作用

cmp（“compare”的缩写）命令用来简要指出两个文件是否存在差异，它的使用权限是所有用户。

2.格式

cmp[options] 文件名

3.[options]主要参数

-l: 将字节以十进制的方式输出，并方便将两个文件中不同的以八进制的方式输出。

cat

1.作用

cat（“concatenate”的缩写）命令用于连接并显示指定的一个和多个文件的有关信息，它的使用权限是所有用户。

2.格式

cat [options] 文件1 文件2……

3.[options]主要参数

－n：由第一行开始对所有输出的行数编号。

－b：和－n相似，只不过对于空白行不编号。

－s：当遇到有连续两行以上的空白行时，就代换为一行的空白行。

4.应用举例

（1）cat命令一个最简单的用处是显示文本文件的内容。例如，我们想在命令行看一下README文件的内容，可以使用命令：

$ cat README

（2）

有时需要将几个文件处理成一个文件，并将这种处理的结果保存到一个单独的输出文件。cat命令在其输入上接受一个或多个文件，并将它们作为一个单独的文件

打印到它的输出。例如，把README和INSTALL的文件内容加上行号（空白行不加）之后，将内容附加到一个新文本文件File1 中：

$ cat README INSTALL File1

（3）cat还有一个重要的功能就是可以对行进行编号，见图2所示。这种功能对于程序文档的编制，以及法律和科学文档的编制很方便，打印在左边的行号使得参考文档的某一部分变得容易，这些在编程、科学研究、业务报告甚至是立法工作中都是非常重要的。

图2 使用cat命令/etc/named.conf文件进行编号

对行进行编号功能有-b（只能对非空白行进行编号）和-n（可以对所有行进行编号）两个参数：

$ cat -b /etc/named.conf

（4）产寻

ln

1.作用

ln命令用来在文件之间创建链接，它的使用权限是所有用户。

2.格式

ln [options] 源文件 [链接名]

3.参数

－f：链结时先将源文件删除。

－d：允许系统管理者硬链结自己的目录。

－s：进行软链结(Symbolic Link)。

－b：将在链结时会被覆盖或删除的文件进行备份。

链接有两种，一种被称为硬链接（Hard Link），另一种被称为符号链接（Symbolic Link）。默认情况下，ln命令产生硬链接。

硬

连接指通过索引节点来进行的连接。在Linux的文件系统中，保存在磁盘分区中的文件不管是什么类型都给它分配一个编号，称为索引节点号(Inode

Index)。在Linux中，多个文件名指向同一索引节点是存在的。一般这种连接就是硬连接。硬连接的作用是允许一个文件拥有多个有效路径名，这样用户

就可以建立硬连接到重要文件，以防止“误删”的功能。其原因如上所述，因为对应该目录的索引节点有一个以上的连接。只删除一个连接并不影响索引节点本身和

其它的连接，只有当最后一个连接被删除后，文件的数据块及目录的连接才会被释放。也就是说，文件才会被真正删除。

与硬连接相对应，Lnux系统中还存在另一种连接，称为符号连接（Symbilc Link），也叫软连接。软链接文件有点类似于Windows的快捷方式。它实际上是特殊文件的一种。在符号连接中，文件实际上是一个文本文件，其中包含的有另一文件的位置信息。

动手练习

上面我们介绍了Linux文件处理命令，下面介绍几个实例，大家可以动手练习一下刚才讲过的命令。

1.利用符号链接快速访问关键目录

符

号链接是一个非常实用的功能。假设有一些目录或文件需要频繁使用，但由于Linux的文件和目录结构等原因，这个文件或目录在很深的子目录中。比如，

Apache

Web服务器文档位于系统的/usr/local/httpd/htdocs中，并且不想每次都要从主目录进入这样一个长的路径之中(实际上，这个路径也

非常不容易记忆)。

为了解决这个问题，可以在主目录中创建一个符号链接，这样在需要进入该目录时，只需进入这个链接即可。

为了能方便地进入Web服务器(/usr/local/httpd/htdocs)文档所在的目录，在主目录下可以使用以下命令：

$ ln -s /usr/local/httpd/htdocs gg

这样每次进入gg目录就可访问Web服务器的文档，以后如果不再访问Web服务器的文档时，删除gg即可，而真正的Web服务器的文档并没有删除。

2.使用dd命令将init.rd格式的root.ram内容导入内存

dd if=/dev/fd0 of=floppy.fd

dd if=root.ram of=/dev/ram0 #

3.grep命令系统调用

grep是Linux/Unix中使用最广泛的命令之一，许多Linux系统内部都可以调用它。

(1)如果要查询目录列表中的目录，方法如下：

$ ls -l | grep '∧d'

(2)如果在一个目录中查询不包含目录的所有文件，方法如下：

$ ls -l | grep '∧[∧d]'

(3)用find命令调用grep，如所有C源代码中的“Chinput”，方法如下：

$find /ZhXwin -name \*.c -exec grep -q -s Chinput {} \;-print

Linux必学的60个命令(3)-系统管理命令

Linux必学的系统管理命令

对于Linux系统来说，无论是中央处理器、内存、磁盘驱动器、键盘、鼠标，还是用户等都是文件，Linux系统管理的命令是它正常运行的核心。熟悉了Linux常用的文件处理命令以后，这一讲介绍对系统和用户进行管理的命令。

df

1.作用

df命令用来检查文件系统的磁盘空间占用情况，使用权限是所有用户。

2.格式

df [options]

3.主要参数

－s：对每个Names参数只给出占用的数据块总数。

－a：递归地显示指定目录中各文件及子目录中各文件占用的数据块数。若既不指定－s，也不指定－a，则只显示Names中的每一个目录及其中的各子目录所占的磁盘块数。

－k：以1024字节为单位列出磁盘空间使用情况。

－x：跳过在不同文件系统上的目录不予统计。

－l：计算所有的文件大小，对硬链接文件则计算多次。

－i：显示inode信息而非块使用量。

－h：以容易理解的格式印出文件系统大小，例如136KB、254MB、21GB。

－P：使用POSIX输出格式。

－T：显示文件系统类型。

4.说明

df命令被广泛地用来生成文件系统的使用统计数据，它能显示系统中所有的文件系统的信息，包括总容量、可用的空闲空间、目前的安装点等。

超

级权限用户使用df命令时会发现这样的情况：某个分区的容量超过了100％。这是因为Linux系统为超级用户保留了10％的空间，由其单独支配。也就是

说，对于超级用户而言，他所见到的硬盘容量将是110％。这样的安排对于系统管理而言是有好处的，当硬盘被使用的容量接近100％时系统管理员还可以正常

工作。

5.应用实例

Linux支持的文件系统非常多，包括JFS、ReiserFS、ext、ext2、ext3、ISO9660、XFS、Minx、vfat、MSDOS等。使用df -T命令查看磁盘空间时还可以得到文件系统的信息：

＃df －T

文件系统 类型 容量 已用 可用 已用% 挂载点

/dev/hda7 reiserfs 5.2G 1.6G 3.7G 30% /

/dev/hda1 vfat 2.4G 1.6G 827M 66% /windows/C

/dev/hda5 vfat 3.0G 1.7G 1.3G 57% /windows/D

/dev/hda9 vfat 3.0G 2.4G 566M 82% /windows/E

/dev/hda10 NTFS 3.2G 573M 2.6G 18% /windows/F

/dev/hda11 vfat 1.6G 1.5G 23M 99% /windows/G

从上面除了可以看到磁盘空间的容量、使用情况外，分区的文件系统类型、挂载点等信息也一览无遗。

top

1.作用

top命令用来显示执行中的程序进程，使用权限是所有用户。

2.格式

top [－] [d delay] [q] [c] [S] [s] [n]

3.主要参数

d：指定更新的间隔，以秒计算。

q：没有任何延迟的更新。如果使用者有超级用户，则top命令将会以最高的优先序执行。

c：显示进程完整的路径与名称。

S：累积模式，会将己完成或消失的子行程的CPU时间累积起来。

s：安全模式。

i：不显示任何闲置(Idle)或无用(Zombie)的行程。

n：显示更新的次数，完成后将会退出top。

4.说明

top命令是Linux系统管理的一个主要命令，通过它可以获得许多信息。这里我们结合图1来说明它给出的信息。

图1 top命令的显示

在

图1中，第一行表示的项目依次为当前时间、系统启动时间、当前系统登录用户数目、平均负载。第二行显示的是所有启动的进程、目前运行的、挂起

(Sleeping)的和无用(Zombie)的进程。第三行显示的是目前CPU的使用情况，包括系统占用的比例、用户使用比例、闲置(Idle)比例。

第四行显示物理内存的使用情况，包括总的可以使用的内存、已用内存、空闲内存、缓冲区占用的内存。第五行显示交换分区使用情况，包括总的交换分区、使用

的、空闲的和用于高速缓存的大小。第六行显示的项目最多，下面列出了详细解释。

PID（Process ID）：进程标示号。

USER：进程所有者的用户名。

PR：进程的优先级别。

NI：进程的优先级别数值。

VIRT：进程占用的虚拟内存值。

RES：进程占用的物理内存值。

SHR：进程使用的共享内存值。

S：进程的状态，其中S表示休眠，R表示正在运行，Z表示僵死状态，N表示该进程优先值是负数。

%CPU：该进程占用的CPU使用率。

%MEM：该进程占用的物理内存和总内存的百分比。

TIME＋：该进程启动后占用的总的CPU时间。

Command：进程启动的启动命令名称，如果这一行显示不下，进程会有一个完整的命令行。

top命令使用过程中，还可以使用一些交互的命令来完成其它参数的功能。这些命令是通过快捷键启动的。

：立刻刷新。

P：根据CPU使用大小进行排序。

T：根据时间、累计时间排序。

q：退出top命令。

m：切换显示内存信息。

t：切换显示进程和CPU状态信息。

c：切换显示命令名称和完整命令行。

M：根据使用内存大小进行排序。

W：将当前设置写入~/.toprc文件中。这是写top配置文件的推荐方法。

可以看到，top命令是一个功能十分强大的监控系统的工具，对于系统管理员而言尤其重要。但是，它的缺点是会消耗很多系统资源。

5.应用实例

使用top命令可以监视指定用户，缺省情况是监视所有用户的进程。如果想查看指定用户的情况，在终端中按“U”键，然后输入用户名，系统就会切换为指定用户的进程运行界面，见图2所示。

图2 使用top命令监视指定用户

free

1.作用

free命令用来显示内存的使用情况，使用权限是所有用户。

2.格式

free [－b|－k|－m] [－o] [－s delay] [－t] [－V]

3.主要参数

－b －k －m：分别以字节（KB、MB）为单位显示内存使用情况。

－s delay：显示每隔多少秒数来显示一次内存使用情况。

－t：显示内存总和列。

－o：不显示缓冲区调节列。

4.应用实例

free命令是用来查看内存使用情况的主要命令。和top命令相比，它的优点是使用简单，并且只占用很少的系统资源。通过－S参数可以使用free命令不间断地监视有多少内存在使用，这样可以把它当作一个方便实时监控器。

＃free －b －s5

使用这个命令后终端会连续不断地报告内存使用情况（以字节为单位），每5秒更新一次。

quota

1.作用

quota命令用来显示磁盘使用情况和限制情况，使用权限超级用户。

2.格式

quota [－g][－u][－v][－p] 用户名 组名

3.参数

－g：显示用户所在组的磁盘使用限制。

－u：显示用户的磁盘使用限制。

－v：显示没有分配空间的文件系统的分配情况。

－p：显示简化信息。

4.应用实例

在企业应用中磁盘配额非常重要，普通用户要学会看懂自己的磁盘使用情况。要查询自己的磁盘配额可以使用下面命令（下例中用户账号是caojh)：

＃quota caojh

Disk quotas for user caojh(uid 502):

Filesystem blocks quota limit grace files quota limit grace

/dev/hda3 58 200000 400000 41 500 1000

以上显示ID号为502的caojh账号，文件个数设置为500～1000个，硬盘空间限制设置为200MB～400MB。一旦磁盘配额要用完时，就需要删除一些垃圾文件或向系统管理员请求追加配额。

at

1.作用

at命令用来在指定时刻执行指定的命令序列。

2.格式

at [－V] [－q x] [－f file] [－m] time

3.主要参数

－V：显示标准错误输出。

－q：许多队列输出。

－f：从文件中读取作业。

－m：执行完作业后发送电子邮件到用户。

time：设定作业执行的时间。time格式有严格的要求，由小时、分钟、日期和时间的偏移量组成，其中日期的格式为MM.DD.YY，MM是分钟，DD是日期，YY是指年份。偏移量的格式为时间＋偏移量，单位是minutes、hours和days。

4.应用实例

＃at －f data 15:30 +2 days

上面命令表示让系统在两天后的17：30执行文件data中指明的作业。

lp

1.作用

lp是打印文件的命令，使用权限是所有用户。

2.格式

lp [－c][－d][－m][－number][－title][-p]

3.主要参数

－c：先拷贝文件再打印。

－d：打印队列文件。

－m：打印结束后发送电子邮件到用户。

－number：打印份数。

－title：打印标题。

－p：设定打印的优先级别，最高为100。

4.应用实例

（1）使用lp命令打印多个文件

＃lp 2 3 4

request id is 11 (3 file(s))

其中2、3、4分别是文件名；“request id is 11 (3 file(s)) ”表示这是第11个打印命令，依次打印这三个文件。

（2）设定打印优先级别

＃lp lp -d LaserJet -p 90 /etc/aliases

通过添加“-p 90”，规定了打印作业的优先级为90。它将在优先级低于90的打印作业之前打印，包括没有设置优先级的作业，缺省优先级是50

useradd

1.作用

useradd命令用来建立用户帐号和创建用户的起始目录，使用权限是超级用户。

2.格式

useradd [－d home] [－s shell] [－c comment] [－m [－k template]] [－f inactive] [－e expire ] [－p passwd] [－r] name

3.主要参数

－c：加上备注文字，备注文字保存在passwd的备注栏中。

－d：指定用户登入时的启始目录。

－D：变更预设值。

－e：指定账号的有效期限，缺省表示永久有效。

－f：指定在密码过期后多少天即关闭该账号。

－g：指定用户所属的群组。

－G：指定用户所属的附加群组。

－m：自动建立用户的登入目录。

－M：不要自动建立用户的登入目录。

－n：取消建立以用户名称为名的群组。

－r：建立系统账号。

－s：指定用户登入后所使用的shell。

－u：指定用户ID号。

4.说明

useradd可用来建立用户账号，它和adduser命令是相同的。账号建好之后，再用passwd设定账号的密码。使用useradd命令所建立的账号，实际上是保存在/etc/passwd文本文件中。

5.应用实例

建立一个新用户账户，并设置ID：

＃useradd caojh －u 544

需要说明的是，设定ID值时尽量要大于500，以免冲突。因为Linux安装后会建立一些特殊用户，一般0到499之间的值留给bin、mail这样的系统账号。

groupadd

1.作用

groupadd命令用于将新组加入系统。

2.格式

groupadd [－g gid] [－o]] [－r] [－f] groupname

3.主要参数

－g gid：指定组ID号。

－o：允许组ID号，不必惟一。

－r：加入组ID号，低于499系统账号。

－f：加入已经有的组时，发展程序退出。

4.应用实例

建立一个新组，并设置组ID加入系统：

＃groupadd －g 344 cjh

此时在/etc/passwd文件中产生一个组ID（GID）是344的项目。

kill

1.作用

kill命令用来中止一个进程。

2.格式

kill [ －s signal | －p ] [ －a ] pid ...

kill －l [ signal ]

3.参数

－s：指定发送的信号。

－p：模拟发送信号。

－l：指定信号的名称列表。

pid：要中止进程的ID号。

Signal：表示信号。

4.说明

进程是Linux系统中一个非常重要的概念。Linux是一个多任务的操作系统，系统上经常同时运行着多个进程。我们不关心这些进程究竟是如何分配的，或者是内核如何管理分配时间片的，所关心的是如何去控制这些进程，让它们能够很好地为用户服务。

Linux

操作系统包括三种不同类型的进程，每种进程都有自己的特点和属性。交互进程是由一个Shell启动的进程。交互进程既可以在前台运行，也可以在后台运行。

批处理进程和终端没有联系，是一个进程序列。监控进程（也称系统守护进程）时Linux系统启动时启动的进程，并在后台运行。例如，httpd是著名的

Apache服务器的监控进程。

kill命令的工作原理是，向Linux系统的内核发送一个系统操作信号

和某个程序的进程标识号，然后系统内核就可以对进程标识号指定的进程进行操作。比如在top命令中，我们看到系统运行许多进程，有时就需要使用kill中

止某些进程来提高系统资源。在讲解安装和登陆命令时，曾提到系统多个虚拟控制台的作用是当一个程序出错造成系统死锁时，可以切换到其它虚拟控制台工作关闭

这个程序。此时使用的命令就是kill，因为kill是大多数Shell内部命令可以直接调用的。

5.应用实例

（1）强行中止（经常使用杀掉）一个进程标识号为324的进程：

＃kill －9 324

（2）解除Linux系统的死锁

在Linux

中有时会发生这样一种情况：一个程序崩溃，并且处于死锁的状态。此时一般不用重新启动计算机，只需要中止(或者说是关闭)这个有问题的程序即可。当

kill处于X-Window界面时，主要的程序(除了崩溃的程序之外)一般都已经正常启动了。此时打开一个终端，在那里中止有问题的程序。比如，如果

Mozilla浏览器程序出现了锁死的情况，可以使用kill命令来中止所有包含有Mozolla浏览器的程序。首先用top命令查处该程序的PID，然

后使用kill命令停止这个程序：

＃kill －SIGKILL XXX

其中，XXX是包含有Mozolla浏览器的程序的进程标识号。

（3）使用命令回收内存

我们知道内存对于系统是非常重要的，回收内存可以提高系统资源。kill命令可以及时地中止一些“越轨”的程序或很长时间没有相应的程序。例如，使用top命令发现一个无用 (Zombie) 的进程，此时可以使用下面命令：

＃kill －9 XXX

其中，XXX是无用的进程标识号。

然后使用下面命令：

＃free

此时会发现可用内存容量增加了。

（4）killall命令

Linux下还提供了一个killall命令，可以直接使用进程的名字而不是进程标识号，例如：

＃ killall -HUP inetd

crontab

1.作用

使用crontab命令可以修改crontab配置文件，然后该配置由cron公用程序在适当的时间执行，该命令使用权限是所有用户。

2.格式

crontab [ －u user ] 文件

crontab [ －u user ] { －l | －r | －e }

3.主要参数

－e：执行文字编辑器来设定时程表，内定的文字编辑器是vi。

－r：删除目前的时程表。

－l：列出目前的时程表。

crontab

文件的格式为“M H D m d

cmd”。其中，M代表分钟（0～59），H代表小时（0～23），D代表天（1～31），m代表月（1～12），d代表一星期内的天（0～6，0为星期

天）。cmd表示要运行的程序，它被送入sh执行，这个Shell只有USER、HOME、SHELL三个环境变量。

4.说明

和at命令相比，crontab命令适合完成固定周期的任务。

5.应用实例

设置一个定时、定期的系统提示：

[cao @www cao]#crontab －e

此时系统会打开一个vi编辑器。

如果输入以下内容：35 17 \* \* 5 wall "Tomorrow is Saturday I will go CS"，然后存盘退出。这时在/var/spool/cron/目录下会生产一个cao的文件，内容如下：

# DO NOT EDIT THIS FILE － edit the master and reinstall.

# (/tmp/crontab.2707 installed on Thu Jan 1 22:01:51 2004)

# (Cron version －－ $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)

35 17 \* \* 5 wall "Tomorrow is Saturday I will play CS "

这样每个星期五17：35系统就会弹出一个终端，提醒星期六可以打打CS了！显示结果见图3所示。

图3 一个定时、定期的系统提示

动手练习

1.联合使用kill和top命令观察系统性能的变化

首先启动一个终端运行top命令，然后再启动一个终端使用kill命令，见图4所示。

图4 观察kill命令对top终端的影响

这时利用上面介绍的kill命令来中止一些程序：

＃kill SIGKILL XXX

然后再看top命令终端的变化，包括内存容量、CPU使用率、系统负载等。注意，有些进程是不能中止的，不过学习Linux命令时可以试试，看看系统有什么反应。

2.使用at和halt命令定时关机

首先设定关机时间是17:35，输入下面代码：

＃at 17:35

warning: commands will be executed using (in order) a) $SHELL b) login shell c) /bin/sh

at>halt `-i －p

at>

job 6 at 2004－01－01 17:35

此

时实际上就已经进入Linux系统的Shell，并且编写一个最简单程序：halt －i

－p。上面Shell中的文本结束符号表示按“Ctrl＋D”组合键关闭命令，提交任务退出Shell。“Job 6 at 2004－01－01

17:35”表示系统接受第6个at命令，在“2004－01－01 17:35”时执行命令：先把所有网络相关的装置停止，关闭系统后关闭电源。

3.用crontab命令实现每天定时的病毒扫描

前面已经介绍了一个简单的crontab命令操作，这里看一些更重要的操作。

（1）建立一个文件，文件名称自己设定，假设为caoproject：

＃crontab －e

（2）文件内容如下：

05 09 \* \* \* antivir

用vi编辑后存盘退出。antivir是一个查杀Linux病毒的软件，当然需要时先安装在系统中。

（3）使用crontab命令添加到任务列表中：

＃crontab caoproject

这样系统内所有用户在每天的9点05分会自动进行病毒扫描。

4.用kill使修改的配置文件马上生效

Windows用户一般都知道，重要配置文件修改后往往都要重新启动计算机才能使修改生效。而Linux由于采用了模块化设计，可以自己根据需要实时设定服务。这里以网络服务inetd为例介绍一些操作技巧。

inetd

是一个监听守护进程，监听与提供互联网服务进程（如rlogin、telnet、ftp、rsh）进行连接的要求，并扩展所需的服务进程。默认情况下，

inetd监听的这些daemon均列于/etc

/inetd.conf文件中。编辑/etc/inetd.conf文件，可以改变inetd启动服务器守护进程的选项，然后驱使inetd以

SIGHUP（signal 1）向当前的inetd进程发送信号，使inetd重读该文件。这一过程由kill命令来实现。

用vi或其它编辑器修改inetd.conf后，首先使用下面命令：

＃ps -ef |grep inetd

上面代码表明查询inetd.conf的进程号(PID)，这里假设是1426，然后使用下面命令：

＃ kill -1426 inetd

这样配置文件就生效了。

这一讲介绍的系统管理命令都是比较重要的，特别是crontab命令和quota命令使用起来会有一定难度，需要多做一些练习。另外，使用kill命令要注意“－9“这个参数，练习时最好不要运行一些重要的程序。

## 网络操作命令

因

为Linux系统是在Internet上起源和发展的，它与生俱来拥有强大的网络功能和丰富的网络应用软件，尤其是TCP/IP网络协议的实现尤为成熟。

Linux的网络命令比较多，其中一些命令像ping、

ftp、telnet、route、netstat等在其它操作系统上也能看到，但也有一些Unix/Linux系统独有的命令，如ifconfig、

finger、mail等。Linux网络操作命令的一个特点是，命令参数选项和功能很多，一个命令往往还可以实现其它命令的功能。

ifconfig

1.作用

ifconfig用于查看和更改网络接口的地址和参数，包括IP地址、网络掩码、广播地址，使用权限是超级用户。

2.格式

ifconfig -interface [options] address

3.主要参数

-interface：指定的网络接口名，如eth0和eth1。

up：激活指定的网络接口卡。

down：关闭指定的网络接口。

broadcast address：设置接口的广播地址。

pointopoint：启用点对点方式。

address：设置指定接口设备的IP地址。

netmask address：设置接口的子网掩码。

4.应用说明

ifconfig是用来设置和配置网卡的命令行工具。为了手工配置网络，这是一个必须掌握的命令。使用该命令的好处是无须重新启动机器。要赋给eth0接口IP地址207.164.186.2，并且马上激活它，使用下面命令：

#fconfig eth0 210.34.6.89 netmask 255.255.255.128 broadcast 210.34.6.127

该

命令的作用是设置网卡eth0的IP地址、网络掩码和网络的本地广播地址。若运行不带任何参数的ifconfig命令，这个命令将显示机器所有激活接口的

信息。带有“-a”参数的命令则显示所有接口的信息，包括没有激活的接口。注意，用ifconfig命令配置的网络设备参数，机器重新启动以后将会丢失。

如果要暂停某个网络接口的工作，可以使用down参数：

#ifconfig eth0 down

ip

1.作用

ip是iproute2软件包里面的一个强大的网络配置工具，它能够替代一些传统的网络管理工具，例如ifconfig、route等，使用权限为超级用户。几乎所有的Linux发行版本都支持该命令。

2.格式

ip [OPTIONS] OBJECT [COMMAND [ARGUMENTS]]

3.主要参数

OPTIONS是修改ip行为或改变其输出的选项。所有的选项都是以-字符开头，分为长、短两种形式。目前，ip支持如表1所示选项。

OBJECT是要管理者获取信息的对象。目前ip认识的对象见表2所示。

表1 ip支持的选项

-V,-Version 打印ip的版本并退出。

-s,-stats,-statistics 输出更为详尽的信息。如果这个选项出现两次或多次，则输出的信息将更为详尽。

-f,-family 这个选项后面接协议种类，包括inet、inet6或link，强调使用的协议种类。如果没有足够的信息告诉ip使用的协议种类，ip就会使用默认值inet或any。link比较特殊，它表示不涉及任何网络协议。

-4 是-family inet的简写。

-6 是-family inet6的简写。

-0 是-family link的简写。

-o,-oneline 对每行记录都使用单行输出，回行用字符代替。如果需要使用wc、grep等工具处理ip的输出，则会用到这个选项。

-r,-resolve 查询域名解析系统，用获得的主机名代替主机IP地址

COMMAND

设置针对指定对象执行的操作，它和对象的类型有关。一般情况下，ip支持对象的增加(add)、删除(delete)和展示(show或list)。有些

对象不支持这些操作，或者有其它的一些命令。对于所有的对象，用户可以使用help命令获得帮助。这个命令会列出这个对象支持的命令和参数的语法。如果没

有指定对象的操作命令，ip会使用默认的命令。一般情况下，默认命令是list，如果对象不能列出，就会执行help命令。

ARGUMENTS

是命令的一些参数，它们倚赖于对象和命令。ip支持两种类型的参数：flag和parameter。flag由一个关键词组成；parameter由一个

关键词加一个数值组成。为了方便，每个命令都有一个可以忽略的默认参数。例如，参数dev是ip link命令的默认参数，因此ip link ls

eth0等于ip link ls dev eth0。我们将在后面的详细介绍每个命令的使用，命令的默认参数将使用default标出。

4.应用实例

添加IP地址192.168.2.2/24到eth0网卡上：

#ip addr add 192.168.1.1/24 dev eth0

丢弃源地址属于192.168.2.0/24网络的所有数据报：

#ip rule add from 192.168.2.0/24 prio 32777 reject

ping

1.作用

ping检测主机网络接口状态，使用权限是所有用户。

2.格式

ping [-dfnqrRv][-c][-i][-I][-l][-p][-s][-t] IP地址

3.主要参数

-d：使用Socket的SO\_DEBUG功能。

-c：设置完成要求回应的次数。

-f：极限检测。

-i：指定收发信息的间隔秒数。

-I：网络界面使用指定的网络界面送出数据包。

-l：前置载入，设置在送出要求信息之前，先行发出的数据包。

-n：只输出数值。

-p：设置填满数据包的范本样式。

-q：不显示指令执行过程，开头和结尾的相关信息除外。

-r：忽略普通的Routing Table，直接将数据包送到远端主机上。

-R：记录路由过程。

-s：设置数据包的大小。

-t：设置存活数值TTL的大小。

-v：详细显示指令的执行过程。

ping

命令是使用最多的网络指令，通常我们使用它检测网络是否连通，它使用ICMP协议。但是有时会有这样的情况，我们可以浏览器查看一个网页，但是却无法

ping通，这是因为一些网站处于安全考虑安装了防火墙。另外，也可以在自己计算机上试一试，通过下面的方法使系统对ping没有反应：

# echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

netstat

1.作用

检查整个Linux网络状态。

2.格式

netstat [-acCeFghilMnNoprstuvVwx][-A][--ip]

3.主要参数

-a--all：显示所有连线中的Socket。

-A：列出该网络类型连线中的IP相关地址和网络类型。

-c--continuous：持续列出网络状态。

-C--cache：显示路由器配置的快取信息。

-e--extend：显示网络其它相关信息。

-F--fib：显示FIB。

-g--groups：显示多重广播功能群组组员名单。

-h--help：在线帮助。

-i--interfaces：显示网络界面信息表单。

-l--listening：显示监控中的服务器的Socket。

-M--masquerade：显示伪装的网络连线。

-n--numeric：直接使用IP地址，而不通过域名服务器。

-N--netlink--symbolic：显示网络硬件外围设备的符号连接名称。

-o--timers：显示计时器。

-p--programs：显示正在使用Socket的程序识别码和程序名称。

-r--route：显示Routing Table。

-s--statistice：显示网络工作信息统计表。

-t--tcp：显示TCP传输协议的连线状况。

-u--udp：显示UDP传输协议的连线状况。

-v--verbose：显示指令执行过程。

-V--version：显示版本信息。

-w--raw：显示RAW传输协议的连线状况。

-x--unix：和指定“-A unix”参数相同。

--ip--inet：和指定“-A inet”参数相同。

4.应用实例

**netstat**

主要用于Linux察看自身的网络状况，如开启的端口、在为哪些用户服务，以及服务的状态等。此外，它还显示系统路由表、网络接口状态等。可以说，它是一

个综合性的网络状态的察看工具。在默认情况下，netstat只显示已建立连接的端口。如果要显示处于监听状态的所有端口，使用-a参数即可：

#netstat -a

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 \*:32768 \*:\* LISTEN

tcp 0 0 \*:32769 \*:\* LISTEN

tcp 0 0 \*:nfs \*:\* LISTEN

tcp 0 0 \*:32770 \*:\* LISTEN

tcp 0 0 \*:868 \*:\* LISTEN

tcp 0 0 \*:617 \*:\* LISTEN

tcp 0 0 \*:mysql \*:\* LISTEN

tcp 0 0 \*:netbios-ssn \*:\* LISTEN

tcp 0 0 \*:sunrpc \*:\* LISTEN

tcp 0 0 \*:10000 \*:\* LISTEN

tcp 0 0 \*:http \*:\* LISTEN

......

上面显示出，这台主机同时提供HTTP、FTP、NFS、MySQL等服务。

telnet

1.作用

telnet表示开启终端机阶段作业，并登入远端主机。telnet是一个Linux命令，同时也是一个协议（远程登陆协议）。

2.格式

telnet [-8acdEfFKLrx][-b][-e][-k][-l][-n][-S][-X][主机名称IP地址]

3.主要参数

-8：允许使用8位字符资料，包括输入与输出。

-a：尝试自动登入远端系统。

-b：使用别名指定远端主机名称。

-c：不读取用户专属目录里的.telnetrc文件。

-d：启动排错模式。

-e：设置脱离字符。

-E：滤除脱离字符。

-f：此参数的效果和指定“-F”参数相同。

-F：使用Kerberos V5认证时，加上此参数可把本地主机的认证数据上传到远端主机。

-k：使用Kerberos认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名。

-K：不自动登入远端主机。

-l：指定要登入远端主机的用户名称。

-L：允许输出8位字符资料。

-n：指定文件记录相关信息。

-r：使用类似rlogin指令的用户界面。

-S：服务类型，设置telnet连线所需的IP TOS信息。

-x：假设主机有支持数据加密的功能，就使用它。

-X：关闭指定的认证形态。

4.应用说明

用

户使用telnet命令可以进行远程登录，并在远程计算机之间进行通信。用户通过网络在远程计算机上登录，就像登录到本地机上执行命令一样。为了通过

telnet登录到远程计算机上，必须知道远程机上的合法用户名和口令。虽然有些系统确实为远程用户提供登录功能，但出于对安全的考虑，要限制来宾的操作

权限，因此，这种情况下能使用的功能是很少的。

telnet只为普通终端提供终端仿真，而不支持X-

Window等图形环境。当允许远程用户登录时，系统通常把这些用户放在一个受限制的Shell中，以防系统被怀有恶意的或不小心的用户破坏。用户还可以

使用telnet从远程站点登录到自己的计算机上，检查电子邮件、编辑文件和运行程序，就像在本地登录一样。

ftp

1.作用

ftp命令进行远程文件传输。FTP是ARPANet的标准文件传输协议，该网络就是现今Internet的前身，所以ftp既是协议又是一个命令。

2.格式

ftp [-dignv][主机名称IP地址]

3.主要参数

-d：详细显示指令执行过程，便于排错分析程序执行的情形。

-i：关闭互动模式，不询问任何问题。

-g：关闭本地主机文件名称支持特殊字符的扩充特性。

-n：不使用自动登陆。

-v：显示指令执行过程。

4.应用说明

ftp

命令是标准的文件传输协议的用户接口，是在TCP/IP网络计算机之间传输文件简单有效的方法，它允许用户传输ASCⅡ文件和二进制文件。为了使用ftp

来传输文件，用户必须知道远程计算机上的合法用户名和口令。这个用户名/口令的组合用来确认ftp会话，并用来确定用户对要传输的文件进行什么样的访问。

另外，用户需要知道对其进行ftp会话的计算机名字的IP地址。

用户可以通过使用ftp客户程序，连接到另一台计算机上；可以在目录中上下移动、列出目录内容；可以把文件从远程计算机机拷贝到本地机上；还可以把文件从本地机传输到远程系统中。ftp内部命令有72个，下面列出主要几个内部命令：

ls：列出远程机的当前目录。

cd：在远程机上改变工作目录。

lcd：在本地机上改变工作目录。

close：终止当前的ftp会话。

hash：每次传输完数据缓冲区中的数据后就显示一个#号。

get（mget）：从远程机传送指定文件到本地机。

put（mput）：从本地机传送指定文件到远程机。

quit：断开与远程机的连接，并退出ftp。

route

1.作用

route表示手工产生、修改和查看路由表。

2.格式

#route [-add][-net|-host] targetaddress [-netmask Nm][dev]If]

#route [－delete][-net|-host] targetaddress [gw Gw] [-netmask Nm] [dev]If]

3.主要参数

-add：增加路由。

-delete：删除路由。

-net：路由到达的是一个网络，而不是一台主机。

-host：路由到达的是一台主机。

-netmask Nm：指定路由的子网掩码。

gw：指定路由的网关。

[dev]If：强迫路由链指定接口。

4.应用实例

route命令是用来查看和设置Linux系统的路由信息，以实现与其它网络的通信。要实现两个不同的子网之间的通信，需要一台连接两个网络的路由器，或者同时位于两个网络的网关来实现。

在Linux系统中，设置路由通常是为了解决以下问题：该Linux系统在一个局域网中，局域网中有一个网关，能够让机器访问Internet，那么就需要将这台机器的IP地址设置为Linux机器的默认路由。使用下面命令可以增加一个默认路由：

route add 0.0.0.0 192.168.1.1

rlogin

1.作用

rlogin用来进行远程注册。

2.格式

rlogin [ -8EKLdx ] [ -e char ] [-k realm ] [ - l username ] host

3.主要参数

-8：此选项始终允许8位输入数据通道。该选项允许发送格式化的ANSI字符和其它的特殊代码。如果不用这个选项，除非远端的不是终止和启动字符，否则就去掉奇偶校验位。

-E：停止把任何字符当作转义字符。当和-8选项一起使用时，它提供一个完全的透明连接。

-K：关闭所有的Kerberos确认。只有与使用Kerberos 确认协议的主机连接时才使用这个选项。

-L：允许rlogin会话在litout模式中运行。要了解更多信息，请查阅tty联机帮助。

-d：打开与远程主机进行通信的TCP sockets的socket调试。要了解更多信息，请查阅setsockopt的联机帮助。

-e：为rlogin会话设置转义字符，默认的转义字符是“～”。

-k：请求rlogin获得在指定区域内远程主机的Kerberos许可，而不是获得由krb\_realmofhost(3)确定的远程主机区域内的远程主机的Kerberos许可。

-x：为所有通过rlogin会话传送的数据打开DES加密。这会影响响应时间和CPU利用率，但是可以提高安全性。

4.使用说明

如果在网络中的不同系统上都有账号，或者可以访问别人在另一个系统上的账号，那么要访问别的系统中的账号，首先就要注册到系统中，接着通过网络远程注册到账号所在的系统中。rlogin可以远程注册到别的系统中，它的参数应是一个系统名。

rcp

1.作用

rcp代表远程文件拷贝，用于计算机之间文件拷贝，使用权限是所有用户。

2.格式

rcp [-px] [-k realm] file1 file2 rcp [-px] [-r] [-k realm] file

3.主要参数

-r：递归地把源目录中的所有内容拷贝到目的目录中。要使用这个选项，目的必须是一个目录。

-p：试图保留源文件的修改时间和模式，忽略umask。

-k：请求rcp获得在指定区域内的远程主机的Kerberos许可，而不是获得由krb\_relmofhost(3)确定的远程主机区域内的远程主机的Kerberos许可。

-x：为传送的所有数据打开DES加密。

finger

1.作用

finger用来查询一台主机上的登录账号的信息，通常会显示用户名、主目录、停滞时间、登录时间、登录Shell等信息，使用权限为所有用户。

2.格式

finger [选项] [使用者] [用户@主机]

3.主要参数

-s：显示用户注册名、实际姓名、终端名称、写状态、停滞时间、登录时间等信息。

-l：除了用-s选项显示的信息外，还显示用户主目录、登录Shell、邮件状态等信息，以及用户主目录下的.plan、.project和.forward文件的内容。

-p：除了不显示.plan文件和.project文件以外，与-l选项相同。

4.应用实例

在计算机上使用finger：

[root@localhost root]# Finger

Login Name Tty Idle Login Time Office Office Phone

root root tty1 2 Dec 15 11

root root pts/0 1 Dec 15 11

root root \*pts/1 Dec 15 11

5.应用说明

如果要查询远程机上的用户信息，需要在用户名后面接“@主机名”，采用[用户名@主机名]的格式，不过要查询的网络主机需要运行finger守护进程的支持。

mail

1.作用

mail作用是发送电子邮件，使用权限是所有用户。此外，mail还是一个电子邮件程序。

2.格式

mail [-s subject] [-c address] [-b address]

mail -f [mailbox]mail [-u user]

3.主要参数

-b address：表示输出信息的匿名收信人地址清单。

-c address：表示输出信息的抄送（）收信人地址清单。

-f [mailbox]：从收件箱者指定邮箱读取邮件。

-s subject：指定输出信息的主体行。

[-u user]：端口指定优化的收件箱读取邮件。

nslookup

1.作用

nslookup命令的功能是查询一台机器的IP地址和其对应的域名。使用权限所有用户。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的IP地址对应的域名。

2.格式

nslookup ［IP地址/域名］

3.应用实例

（1）在本地计算机上使用nslookup命令

$ nslookup

Default Server: name.cao.com.cn

Address: 192.168.1.9

>

在符号“>”后面输入要查询的IP地址域名，并回车即可。如果要退出该命令，输入“exit”，并回车即可。

（2）使用nslookup命令测试named

输入下面命令：

nslookup

然后就进入交换式nslookup环境。如果named正常启动，则nslookup会显示当前DNS服务器的地址和域名，否则表示named没能正常启动。

下面简单介绍一些基本的DNS诊断。

◆

检查正向DNS解析，在nslookup提示符下输入带域名的主机名，如hp712.my.com，nslookup应能显示该主机名对应的IP地址。如

果只输入hp712，nslookup会根据/etc/resolv.conf的定义，自动添加my.com域名，并回答对应的IP地址。

◆检查反向DNS解析，在nslookup提示符下输入某个IP地址，如192.22.33.20，nslookup应能回答该IP地址所对应的主机名。

◆检查MX邮件地址记录在nslookup提示符下输入：

set q=mx

然后输入某个域名，输入my.com和mail.my.com，nslookup应能够回答对应的邮件服务器地址，即support.my.com和support2.my.com。

动手练习

1.危险的网络命令

互

联网的发展使安全成为一个不能忽视的问题，finger、ftp、rcp和telnet在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，嗅

探器可以非常容易地截获这些口令和数据。而且，这些服务程序的安全验证方式也是有弱点的，很容易受到“中间服务器”方式的攻击。这里笔者把一些不安全的命

令根据危险等级列出，见表3所示。

现在ftp、telnet可以被SSH命令代替绑定在端口22上，其连

接采用协商方式，使用RSA加密。身份鉴别完成之后，后面的所有流量都使用IDEA

进行加密。SSH（Secure　Shell）程序可以通过网络登录到远程主机，并执行命令。rcp、rlogin等远程调用命令也逐渐被VNC软件代

替。

2.在一张网卡上绑定多个IP地址

在Linux下，可以使用ifconfig方便地绑定多个IP地址到一张网卡。例如，eth0接口的原有IP地址为192.168.0 .254，可以执行下面命令：

ifconfig eth0:0 192.168.0.253 netmask 255.255.255.0

ifconfig eth0:1 192.168.0.252 netmask 255.255.255.0

......

3.修改网卡MAC地址

首先必须关闭网卡设备，命令如下：

/sbin/ifconfig eth0 down

修改MAC地址，命令如下：

/sbin/ifconfig eth0 hw ether 00:AA:BB:CC:DD:EE

重新启用网卡：

/sbin/ifconfig eht0 up

这样网卡的MAC地址就更改完成了。每张网卡的MAC地址是惟一，但不是不能修改的，只要保证在网络中的MAC地址的惟一性就可以了。

4.初步部署IPv6

IPv4

技术在网络发展中起到了巨大的作用，不过随着时间的流逝它无论在网络地址的提供、服务质量、安全性等方面都越来越力不从心，IPv6呼之欲出。Linux

是所有操作系统中最先支持IPv6的，一般Linux基于2.4内核的Linux发行版本都可以直接使用IPv6，不过主要发行版本没有加载IPv6模

块，可以使用命令手工加载，需要超级用户的权限。

(1)加载IPv6模块

使用命令检测，其中inet6 addr: fe80::5054:abff:fe34:5b09/64，就是eth0网卡的IPv6地址。

# modprobe IPv6

＃ifconfig

eth0 Link encap:Ethernet HWaddr 52:54:AB:34:5B:09

inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0

inet6 addr: fe80::5054:abff:fe34:5b09/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:21 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:100

RX bytes:0 (0.0 b) TX bytes:1360 (1.3 Kb)

Interrupt:5 Base address:0xec00

(2)使用ping命令检测网卡的IPv6地址是否有效

#ping6 -I eth0 -c 2 fe80::200:e8ff:fea0:2586

和IPv4不一样，使用ping6命令时必须指定一个网卡界面，否则系统不知道将数据包发送到哪个网络设备。I表示Interface、eth0是第一个网卡，－c表示回路，2表示ping6操作两次。结果见图1所示。

图1 IPv6网络下的ping6命令

(3)使用ip命令在IPv6下为eth0增加一个IP地址

#ip -6 addr add 3ffe:ffff:0:f101::1/64 dev eth0

使用ifconfig命令，查看网卡是否出现第二个IPv6地址。

Linux网络的主要优点是能够实现资源和信息的共享，并且用户可以远程访问信息。Linux提供了一组强有力的网络命令来为用户服务，这些工具能够帮助用户进行网络设定、检查网络状况、登录到远程计算机上、传输文件和执行远程命令等。

上面介绍了Linux中比较重要的网络命令，其实Linux还有许多命令需要学习。Linux网络操作命令的一个特点就是命令参数选项很多，并不要求全部记住，关键在于理解命令的主要用途和学会使用帮助信息。

## 网络安全命令

F

虽然Linux和Windows NT/2000系统一样是一个多用户的系统，但是它们之间有不少重要的差别。对于很多习惯了Windows系统的管理员来讲，如何保证Linux操作系统安全、可靠将会面临许多新的挑战。本文将重点介绍Linux系统安全的命令。

passwd

1.作用

passwd命令原来修改账户的登陆密码，使用权限是所有用户。

2.格式

passwd [选项] 账户名称

3.主要参数

-l：锁定已经命名的账户名称，只有具备超级用户权限的使用者方可使用。

-u：解开账户锁定状态，只有具备超级用户权限的使用者方可使用。

-x, --maximum=DAYS：最大密码使用时间（天），只有具备超级用户权限的使用者方可使用。

-n, --minimum=DAYS：最小密码使用时间（天），只有具备超级用户权限的使用者方可使用。

-d：删除使用者的密码, 只有具备超级用户权限的使用者方可使用。

-S：检查指定使用者的密码认证种类, 只有具备超级用户权限的使用者方可使用。

4.应用实例

$ passwd

Changing password for user cao.

Changing password for cao

(current) UNIX password:

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

从上面可以看到，使用passwd命令需要输入旧的密码，然后再输入两次新密码。

su

1.作用

su的作用是变更为其它使用者的身份，超级用户除外，需要键入该使用者的密码。

2.格式

su [选项]... [-] [USER [ARG]...]

3.主要参数

-f ， --fast：不必读启动文件（如 csh.cshrc 等），仅用于csh或tcsh两种Shell。

-l ， --login：加了这个参数之后，就好像是重新登陆为该使用者一样，大部分环境变量（例如HOME、SHELL和USER等）都是以该使用者（USER）为主，并且工作目录也会改变。如果没有指定USER，缺省情况是root。

-m， -p ，--preserve-environment：执行su时不改变环境变数。

-c command：变更账号为USER的使用者，并执行指令（command）后再变回原来使用者。

USER：欲变更的使用者账号，ARG传入新的Shell参数。

4.应用实例

变更账号为超级用户，并在执行df命令后还原使用者。 su -c df root

umask

1.作用

umask设置用户文件和目录的文件创建缺省屏蔽值，若将此命令放入profile文件，就可控制该用户后续所建文件的存取许可。它告诉系统在创建文件时不给谁存取许可。使用权限是所有用户。

2.格式

umask [-p] [-S] [mode]

3.参数

－S：确定当前的umask设置。

－p：修改umask 设置。

[mode]：修改数值。

4.说明

传

统Unix的umask值是022，这样就可以防止同属于该组的其它用户及别的组的用户修改该用户的文件。既然每个用户都拥有并属于一个自己的私有组，那

么这种“组保护模式”就不在需要了。严密的权限设定构成了Linux安全的基础，在权限上犯错误是致命的。需要注意的是，umask命令用来设置进程所创

建的文件的读写权限，最保险的值是0077，即关闭创建文件的进程以外的所有进程的读写权限，表示为-rw-------。在

～/.bash\_profile中，加上一行命令umask 0077可以保证每次启动Shell后, 进程的umask权限都可以被正确设定。

5.应用实例

umask -S

u=rwx,g=rx,o=rx

umask -p 177

umask -S

u=rw,g=,o=

上述5行命令，首先显示当前状态，然后把umask值改为177，结果只有文件所有者具有读写文件的权限，其它用户不能访问该文件。这显然是一种非常安全的设置。

chgrp

1.作用

chgrp表示修改一个或多个文件或目录所属的组。使用权限是超级用户。

2.格式

chgrp [选项]... 组 文件...

或

chgrp [选项]... --reference=参考文件 文件...

将每个的所属组设定为。

3.参数

-c, --changes ：像 --verbose，但只在有更改时才显示结果。

--dereference：会影响符号链接所指示的对象，而非符号链接本身。

-h, --no-dereference：会影响符号链接本身，而非符号链接所指示的目的地(当系统支持更改符号链接的所有者，此选项才有效)。

-f, --silent, --quiet：去除大部分的错误信息。

--reference=参考文件：使用的所属组，而非指定的。

-R, --recursive：递归处理所有的文件及子目录。

-v, --verbose：处理任何文件都会显示信息。

4.应用说明

该命令改变指定指定文件所属的用户组。其中group可以是用户组ID，也可以是/etc/group文件中用户组的组名。文件名是以空格分开的要改变属组的文件列表，支持通配符。如果用户不是该文件的属主或超级用户，则不能改变该文件的组。

5.应用实例

改变/opt/local /book/及其子目录下的所有文件的属组为book，命令如下：

$ chgrp - R book /opt/local /book

chmod

1.作用

chmod命令是非常重要的，用于改变文件或目录的访问权限，用户可以用它控制文件或目录的访问权限，使用权限是超级用户。

2.格式

chmod命令有两种用法。一种是包含字母和操作符表达式的字符设定法（相对权限设定）；另一种是包含数字的数字设定法（绝对权限设定）。

（1）字符设定法

chmod [who] [+ | - | =] [mode] 文件名

◆操作对象who可以是下述字母中的任一个或它们的组合

u：表示用户，即文件或目录的所有者。

g：表示同组用户，即与文件属主有相同组ID的所有用户。

o：表示其它用户。

a：表示所有用户，它是系统默认值。

◆操作符号

+：添加某个权限。

-：取消某个权限。

=：赋予给定权限，并取消其它所有权限（如果有的话）。

◆设置mode的权限可用下述字母的任意组合

r：可读。

w：可写。

x：可执行。

X：只有目标文件对某些用户是可执行的或该目标文件是目录时才追加x属性。

s：文件执行时把进程的属主或组ID置为该文件的文件属主。方式“u＋s”设置文件的用户ID位，“g＋s”设置组ID位。

t：保存程序的文本到交换设备上。

u：与文件属主拥有一样的权限。

g：与和文件属主同组的用户拥有一样的权限。

o：与其它用户拥有一样的权限。

文件名：以空格分开的要改变权限的文件列表，支持通配符。

一个命令行中可以给出多个权限方式，其间用逗号隔开。

（2） 数字设定法

数字设定法的一般形式为： chmod [mode] 文件名

数字属性的格式应为3个0到7的八进制数，其顺序是(u)(g)(o)文件名，以空格分开的要改变权限的文件列表，支持通配符。

数

字表示的权限的含义如下：**0001=2^0为所有者的执行权限；0002=2^1为所有者的写权限；0004=2^2为所有者的读权限**；0010为组的执行权限；0020为组的写

权限；0040为组的读权限；0100为其他人的执行权限；0200为其他人的写权限；0400为其他人的读权限；1000为粘贴位置位；2000表示假

如这个文件是可执行文件，则为组ID为位置位，否则其中文件锁定位置位；4000表示假如这个文件是可执行文件，则为用户ID为位置位。

总结 ：chmode ugo：user，group，other，范围由小到大，权限数字越小，代表权限越大。

u=**2^0+2^1+2^2**

3.实例

如果一个系统管理员写了一个表格(tem)让所有用户填写，那么必须授权用户对这个文件有读写权限，可以使用命令：＃chmod 666 tem

上

面代码中，这个666数字是如何计算出来的呢？0002为所有者的写权限，0004为所有者的读权限，0020为组的写权限，0040为组的读权限，

0200为其他人的写权限，0400为其他人的读权限，这6个数字相加就是666（注以上数字都是八进制数），结果见图1所示。

图1 用chmod数字方法设定文件权限

从图1可以看出，tem文件的权限是-rw-rw-rw-，即用户对这个文件有读写权限。

如果用字符权限设定使用下面命令：

＃chmod a =wx tem

chown

1.作用

更改一个或多个文件或目录的属主和属组。使用权限是超级用户。

2.格式

chown [选项] 用户或组 文件

3.主要参数

--dereference：受影响的是符号链接所指示的对象，而非符号链接本身。

-h, --no-dereference：会影响符号链接本身，而非符号链接所指示的目的地(当系统支持更改符号链接的所有者，此选项才有效)。

--from=目前所有者:目前组只当每个文件的所有者和组符合选项所指定的，才会更改所有者和组。其中一个可以省略，这已省略的属性就不需要符合原有的属性。

-f, --silent, --quiet：去除大部分的错误信息。

-R, --recursive：递归处理所有的文件及子目录。

-v, --verbose：处理任何文件都会显示信息。

4.说明

chown 将指定文件的拥有者改为指定的用户或组，用户可以是用户名或用户ID；组可以是组名或组ID；文件是以空格分开的要改变权限的文件列表，支持通配符。系统管理员经常使用chown命令，在将文件拷贝到另一个用户的目录下以后，让用户拥有使用该文件的权限。

5.应用实例

1.把文件shiyan.c的所有者改为wan

$ chown wan shiyan.c

2.把目录/hi及其下的所有文件和子目录的属主改成wan，属组改成users。

$ chown - R wan.users /hi

chattr

1.作用

修改ext2和ext3文件系统属性(attribute)，使用权限超级用户。

2.格式

chattr [-RV] [-+=AacDdijsSu] [-v version] 文件或目录

3.主要参数

－R：递归处理所有的文件及子目录。

－V：详细显示修改内容，并打印输出。

－：失效属性。

＋：激活属性。

= ：指定属性。

A：Atime，告诉系统不要修改对这个文件的最后访问时间。

S：Sync，一旦应用程序对这个文件执行了写操作，使系统立刻把修改的结果写到磁盘。

a：Append Only，系统只允许在这个文件之后追加数据，不允许任何进程覆盖或截断这个文件。如果目录具有这个属性，系统将只允许在这个目录下建立和修改文件，而不允许删除任何文件。

i：Immutable，系统不允许对这个文件进行任何的修改。如果目录具有这个属性，那么任何的进程只能修改目录之下的文件，不允许建立和删除文件。

D：检查压缩文件中的错误。

d：No dump，在进行文件系统备份时，dump程序将忽略这个文件。

C：Compress，系统以透明的方式压缩这个文件。从这个文件读取时，返回的是解压之后的数据；而向这个文件中写入数据时，数据首先被压缩之后才写入磁盘。

s：Secure Delete，让系统在删除这个文件时，使用0填充文件所在的区域。

u：Undelete，当一个应用程序请求删除这个文件，系统会保留其数据块以便以后能够恢复删除这个文件。

4.说明

chattr

命令的作用很大，其中一些功能是由Linux内核版本来支持的，如果Linux内核版本低于2.2，那么许多功能不能实现。同样－D检查压缩文件中的错误

的功能，需要2.5.19以上内核才能支持。另外，通过chattr命令修改属性能够提高系统的安全性，但是它并不适合所有的目录。chattr命令不能

保护/、/dev、/tmp、/var目录。

5.应用实例

1.恢复/root目录,即子目录的所有文件

# chattr -R +u/root

2.用chattr命令防止系统中某个关键文件被修改

在Linux下，有些配置文件(passwd ,fatab)是不允许任何人修改的，为了防止被误删除或修改，可以设定该文件的“不可修改位(immutable)”，命令如下：

# chattr +i /etc/fstab

sudo

1.作用

sudo是一种以限制配置文件中的命令为基础，在有限时间内给用户使用，并且记录到日志中的命令，权限是所有用户。

2.格式

sudo [-bhHpV] [-s ] [-u ] [指令]

sudo [-klv]

3.主要参数

－b：在后台执行命令。

-h：显示帮助。

-H：将HOME环境变量设为新身份的HOME环境变量。

-k：结束密码的有效期，即下次将需要输入密码。

-l：列出当前用户可以使用的命令。

-p：改变询问密码的提示符号。

-s ：执行指定的Shell。

-u ：以指定的用户为新身份，不使用时默认为root。

-v：延长密码有效期5分钟。

4.说明

sudo

命令的配置在/etc/sudoers文件中。当用户使用sudo时，需要输入口令以验证使用者身份。随后的一段时间内可以使用定义好的命令，当使用配置

文件中没有的命令时，将会有报警的记录。sudo是系统管理员用来允许某些用户以root身份运行部分/全部系统命令的程序。一个明显的用途是增强了站点

的安全性，如果需要每天以超级用户的身份做一些日常工作，经常执行一些固定的几个只有超级用户身份才能执行的命令，那么用sudo是非常适合的。

ps

1.作用

ps显示瞬间进程 (process) 的动态，使用权限是所有使用者。

2.格式

ps [options] [--help]

3.主要参数

ps的参数非常多, 此出仅列出几个常用的参数。

-A：列出所有的进程。

-l：显示长列表。

-m：显示内存信息。

-w：显示加宽可以显示较多的信息。

-e：显示所有进程。

a：显示终端上的所有进程,包括其它用户的进程。

-au：显示较详细的信息。

-aux：显示所有包含其它使用者的进程。

4.说明

要

对进程进行监测和控制，首先要了解当前进程的情况，也就是需要查看当前进程。ps命令就是最基本、也是非常强大的进程查看命令。使用该命令可以确定有哪些

进程正在运行、运行的状态、进程是否结束、进程有没有僵尸、哪些进程占用了过多的资源等。图2给出了ps-aux命令详解。大部分信息都可以通过执行该命

令得到。最常用的三个参数是u、a、x。下面就结合这三个参数详细说明ps命令的作用：ps aux

图2 ps-aux命令详解

图2第2行代码中，USER表示进程拥有者；PID表示进程标示符；%CPU表示占用的CPU使用率；%MEM占用的物理内存使用率；VSZ表示占用的虚拟内存大小；RSS为进程占用的物理内存值；TTY为终端的次要装置号码。

STAT

表示进程的状态，其中D为不可中断的静止（I/O动作）；R正在执行中；S静止状态；T暂停执行；Z不存在，但暂时无法消除；W没有足够的内存分页可分

配；高优先序的进程；N低优先序的进程；L有内存分页分配并锁在内存体内 (实时系统或

I/O)。START为进程开始时间。TIME为执行的时间。COMMAND是所执行的指令。

4.应用实例

在进行系统维护时，经常会出现内存使用量惊人，而又不知道是哪一个进程占用了大量进程的情况。除了可以使用top命令查看内存使用情况之外，还可以使用下面的命令：

ps aux | sort +5n

who

1.作用

who显示系统中有哪些用户登陆系统，显示的资料包含了使用者ID、使用的登陆终端、上线时间、呆滞时间、CPU占用，以及做了些什么。 使用权限为所有用户。

2.格式

who - [husfV] [user]

3.主要参数

-h：不要显示标题列。

-u：不要显示使用者的动作/工作。

-s：使用简短的格式来显示。

-f：不要显示使用者的上线位置。

-V：显示程序版本。

4.说明

该

命令主要用于查看当前在线上的用户情况。如果用户想和其它用户建立即时通信，比如使用talk命令，那么首先要确定的就是该用户确实在线上,不然

talk进程就无法建立起来。又如，系统管理员希望监视每个登录的用户此时此刻的所作所为，也要使用who命令。who命令应用起来非常简单，可以比较准

确地掌握用户的情况,所以使用非常广泛。

动手练习

1.使用Linux命令检测系统入侵者

安

装过Mandrake Linux和Red Hat

Linux的用户都会知道，Linux系统会内置三种不同级别（标准、高、更高）的防火墙，当进行了Linux服务器的安装和一些基本的设置后，服务器应

该说是比较安全的，但是也会有黑客通过各种方法利用系统管理员的疏忽侵入系统。如何快速查找黑客非常重要。一般来说，可以使用命令查询黑客是否入侵，见表

1。

表1 查询黑客入侵现象的命令对应表

举例说明，如果黑客嗅探网络，那么它必须使网卡接口处于混杂模式，使用下面命令进行查询：

＃ifconfig -a

eth0 Link encap:Ethernet HWaddr 00:00:E8:A0:25:86

inet addr:192.168.1.7 Bcast:192.168.1.255 Mask:255.255.255.0

UP BROADCAST RUNNING PROMISCUOUS MTU:1500 Metric:1

......

从

这个命令的输出中，可以看到上面讲到的这些概念。第一行的00:00:E8:A0:25:86是mac地址，第二行的192.168.1.7是IP地址，

第四行讲的是接收数据状态，这时正在被黑客嗅探。一般而言，网卡有几种接收数据帧的状态，如Broadcast、Multicast、

Promiscuous等。Broadcast是指接收所有类型为广播报文的数据帧；Multicast是指接收特定的组播报文；Promiscuous

则是通常说的混杂模式，是指对报文中的目的硬件地址不加任何检查、全部接收的工作模式。

2.限制su命令的滥用

我

们知道，超级用户在Linux中有最大的权利，几乎所有黑客都想得到这个目标。Linux可以增加对切换到超级用户的限制。使用PAM

（Pluggable Authentication

Modules）可以禁止除在wheel组以外的任何人su成root，修改/etc/pam.d/su文件，除去屏蔽标识#。使用

/usr/sbin/usermod G10 bjecadm将bjecadm这个账号加入gid为10的组，就是wheel组。命令如下：

/etc/pam.d/su # 使用密码验证＃

auth sufficient /lib/security/pam\_wheel.so debug

# 限制只有wheel组用户才可以切换到root＃

auth required /lib/security/pam\_wheel.so use\_uid

chmod -G10 bjecadm

另外，每当用户试图使用su命令进入系统用户时,命令将在/usr/adm/sulog文件中写一条信息,若该文件记录了大量试图用su进入root的无效操作信息,则表明了可能有人企图破译root口令。

Linux命令有着强大的功能。对于Linux系统管理员来说，往往只需要通过各种安全命令技巧，组合构成安全防线。从计算机安全的角度看，世界上没有绝对安全的计算机系统，Linux系统也不例外。

Linux必学的60个命令(6)-其他命令

在前面几讲中，我们把Linux命令按照在系统中的作用分成几个部分分别予以介绍。但是，还有一些命令不好划分，然而学习它们同样是比较重要的。

tar

1.作用

tar命令是Unix/Linux系统中备份文件的可靠方法，几乎可以工作于任何环境中，它的使用权限是所有用户，压缩解压文件。

2.格式

tar [主选项+辅选项] 文件或目录

3.主要参数

使用该命令时，主选项是必须要有的，它告诉tar要做什么事情，辅选项是辅助使用的，可以选用。

主选项：

-c 创建新的档案文件。如果用户想备份一个目录或是一些文件，就要选择这个选项。

-r 把要存档的文件追加到档案文件的未尾。例如用户已经做好备份文件，又发现还有一个目录或是一些文件忘记备份了，这时可以使用该选项，将忘记的目录或文件追加到备份文件中。

-t 列出档案文件的内容，查看已经备份了哪些文件。

-u 更新文件。就是说，用新增的文件取代原备份文件，如果在备份文件中找不到要更新的文件，则把它追加到备份文件的最后。

-x 从档案文件中释放文件。

辅助选项：

-b 该选项是为磁带机设定的，其后跟一数字，用来说明区块的大小，系统预设值为20（20×512 bytes）。

-f 使用档案文件或设备，这个选项通常是必选的。

-k 保存已经存在的文件。例如把某个文件还原，在还原的过程中遇到相同的文件，不会进行覆盖。

-m 在还原文件时，把所有文件的修改时间设定为现在。

-M 创建多卷的档案文件，以便在几个磁盘中存放。

-v 详细报告tar处理的文件信息。如无此选项，tar不报告文件信息。

-w 每一步都要求确认。

-z 用gzip来压缩/解压缩文件，加上该选项后可以将档案文件进行压缩，但还原时也一定要使用该选项进行解压缩。

4.应用说明

tar 是Tape Archive（磁带归档）的缩写，最初设计用于将文件打包到磁带上。如果下载过Linux的源代码，或许已经碰到过tar文件

请注意，不要忘了Linux是区分大小写的。例如，tar命令应该总是以小写的形式执行。命令行开关可以是大写、小写或大小写的混合。例如，-t和-T执行不同的功能。文件或目录名称可以混合使用大小写，而且就像命令和命令行开关一样是区分大小写的。

5.应用实例

tar是一个命令行的工具，没有图形界面。使用Konsole打开一个终端窗口，接下来是一个简单的备份命令（在/temp目录中创建一个back.tar的文件，/usr目录中所有内容都包含在其中。）：

$tar cvf - /usr > /temp/back.tar

另

外，tar命令支持前面第三讲中讲过的crontab命令，可以用crontab工具设置成基于时间的有规律地运行。例如，每晚6点把/usr目录备份到

hda—第一个IDE接口的主驱动器 (总是位于第一个硬盘)中，只要将下面语句添加到root的crontab中即可：

$00 06 \* \* \* tar cvf /dev/hda1/usrfiles.tar - /usr

一般情况下，以下这些目录是需要备份的：

◆/etc 包含所有核心配置文件，其中包括网络配置、系统名称、防火墙规则、用户、组，以及其它全局系统项。

◆ /var 包含系统守护进程（服务）所使用的信息，包括DNS配置、DHCP租期、邮件缓冲文件、HTTP服务器文件、dB2实例配置等。

◆/home 包含所有默认用户的主目录，包括个人设置、已下载的文件和用户不希望失去的其它信息。

◆/root 根（root）用户的主目录。

◆/opt 是安装许多非系统文件的地方。IBM软件就安装在这里。OpenOffice、JDK和其它软件在默认情况下也安装在这里。

有些目录是可以不备份的：

◆ /proc 应该永远不要备份这个目录。它不是一个真实的文件系统，而是运行内核和环境的虚拟化视图，包括诸如/proc/kcore这样的文件，这个文件是整个运行内存的虚拟视图。备份这些文件只是在浪费资源。

◆/dev 包含硬件设备的文件表示。如果计划还原到一个空白的系统，就可以备份/dev。然而，如果计划还原到一个已安装的Linux 系统，那么备份/dev是没有必要的。

unzip

1.作用

unzip

命令位于/usr/bin目录中，它们和MS DOS下的pkzip、pkunzip及MS

Windows中的Winzip软件功能一样，将文件压缩成.zip文件，以节省硬盘空间，当需要的时候再将压缩文件用unzip命令解开。该命令使用权

限是所有用户。

2.格式

unzip [-cflptuvz][-agCjLMnoqsVX][-P ][.zip文件][文件][-d ][-x ]

3.主要参数

-c：将解压缩的结果显示到屏幕上，并对字符做适当的转换。

-f：更新现有的文件。

-l：显示压缩文件内所包含的文件。

-p：与-c参数类似，会将解压缩的结果显示到屏幕上，但不会执行任何的转换。

-t：检查压缩文件是否正确。

-u：与-f参数类似，但是除了更新现有的文件外，也会将压缩文件中的其它文件解压缩到目录中。

-v：执行是时显示详细的信息。

-z：仅显示压缩文件的备注文字。

-a：对文本文件进行必要的字符转换。

-b：不要对文本文件进行字符转换。

-C：压缩文件中的文件名称区分大小写。

-j：不处理压缩文件中原有的目录路径。

-L：将压缩文件中的全部文件名改为小写。

-M：将输出结果送到more程序处理。

-n：解压缩时不要覆盖原有的文件。

-o：不必先询问用户，unzip执行后覆盖原有文件。

-P：使用zip的密码选项。

-q：执行时不显示任何信息。

-s：将文件名中的空白字符转换为底线字符。

-V：保留VMS的文件版本信息。

-X：解压缩时同时回存文件原来的UID/GID。

[.zip文件]：指定.zip压缩文件。

[文件]：指定要处理.zip压缩文件中的哪些文件。

-d：指定文件解压缩后所要存储的目录。

-x：指定不要处理.zip压缩文件中的哪些文件。

-Z unzip：-Z等于执行zipinfo指令。在Linux中，还提供了一个叫zipinfo的工具，能够察看zip压缩文件的详细信息。unzip最新版本是5.50。

gunzip

1.作用

gunzip命令作用是解压文件，使用权限是所有用户。

2.格式

gunzip [-acfhlLnNqrtvV][-s ][文件...]

或者

gunzip [-acfhlLnNqrtvV][-s ][目录]

3.主要参数

-a或--ascii：使用ASCII文字模式。

-c或--stdout或--to-stdout：把解压后的文件输出到标准输出设备。

-f或-force：强行解开压缩文件，不理会文件名称或硬连接是否存在，以及该文件是否为符号连接。

-h或--help：在线帮助。

-l或--list：列出压缩文件的相关信息。

-L或--license：显示版本与版权信息。

-n或--no-name：解压缩时，若压缩文件内含有原来的文件名称及时间戳记，则将其忽略不予处理。

-N或--name：解压缩时，若压缩文件内含有原来的文件名称及时间戳记，则将其回存到解开的文件上。

-q或--quiet：不显示警告信息。

-r或--recursive：递归处理，将指定目录下的所有文件及子目录一并处理。

-S或--suffix：更改压缩字尾字符串。

-t或--test：测试压缩文件是否正确无误。

-v或--verbose：显示指令执行过程。

-V或--version：显示版本信息。

4.说明

gunzip是个使用广泛的解压缩程序，它用于解开被gzip压缩过的文件，这些压缩文件预设最后的扩展名为“.gz”。事实上，gunzip就是gzip的硬连接，因此不论是压缩或解压缩，都可通过gzip指令单独完成。gunzip最新版本是1.3.3 。

unarj

1.作用

unarj解压缩格式为.arj格式的文件，使用权限是所有用户。

2.格式

unarj [eltx][.arj压缩文件]

3.主要参数

e：解压缩.arj文件。

l：显示压缩文件内所包含的文件。

t：检查压缩文件是否正确。

x：解压缩时保留原有的路径。

4.说明

带有.arj扩展名的文件是由用于MS DOS和Windows的ARJ实用程序创建的。因为ARJ是一种不能免费获得源代码的共享件程序，所以在

mtools

1.作用

mtools

实际上是一个命令集合，是DOS文件系统的工具程序，它可以模拟许多DOS命令，使用起来非常方便。使用权限是所有用户。Linux系统提供了一组称为

mtools的可移植工具，可以让用户轻松地从标准的DOS软盘上读、写文件和目录。它们对DOS和Linux环境之间交换文件非常有用。mtools的

使用非常简单，如果想把软盘里所有的文件都拷贝到硬盘上，那么就可以执行以下命令：

mcopy a:\*.\*

也就是说，只需要在相应的DOS命令之前加上一个字母“m”，就可以完成对应的功能了。一般Linux发行版本中都有这个软件，可以使用下面命令检查一下。

rpm -qa|grep mtools

如果没有安装，也没有关系，可以从网上下载(<http://mtools.linux.lu/>)一个最新版本来安装。目前可供下载的最新mtools版本是

2.包括的命令

mcd 目录名：改变MS DOS下的目录。

mcopy 源文件 目标文件：在MS DOS和Unix之间复制文件。

mdel 文件名：删除MS DOS下的文件。

mdir 目录名：显示MS DOS下的目录。

mformat 驱动器号：在低级格式化的软盘上创建MS DOS文件系统。

rnlabel 驱动器号：产生MS DOS下的卷标。

mmd 目录名：建立MS DOS下的目录。

mrd 目录名：删除MS DOS下的目录。

mren 源文件 目标文件：重新命名已存在的MS DOS文件。

mtype 文件名：显示MS DOS文件的内容。

请注意，这些命令和对应的MS DOS命令非常相似。在mtools命令中，“/”和“\”是可以混用的。因为文件列表的是DOS系统下的文档，对大小写并不敏感，所以“CDE”和“cde”在这里是一样的。

3.应用实例

(1)如果把软盘进行快速格式化，可以使用命令mformat：

mformat A：

mtools

当初发展的目的是用来处理DOS文件系统的，所以只能用在FAT文件格式的分区上。需要注意的是，如果用mount命令来挂载了FAT16/32分区，那

么就不能使用mtools的指令来处理这些分区上的文件。这是因为一旦FAT16/32分区挂到了Linux文件目录下，Linux就会将其视为文件系统

本身的一部分，这时如果要对其操作就必须使用Linux本身所附带的指令集。

(2)将DOS盘上的文件htca.c复制到当前目录下，并用ls命令进行验证。

$ mcopy a:\htca.c

$ ls -l htca.c

-rw-r- -r- - 1 xxq xxq 27136 Jan 1 01:80 htca.c

man

1.作用

man命令用来提供在线帮助，使用权限是所有用户。在Linux系统中存储着一部联机使用的手册，以供用户在终端上查找。使用man命令可以调阅其中的帮助信息，非常方便和实用。

2.格式

man 命令名称

man [-acdfhkKtwW] [-m system] [-p string] [-C config\_file] [-M path] [-P pager] [-S section\_list] [section] name ...

3.参数

-C config\_file：指定设定文件man.conf，缺省值是/etc/man.conf。

-M path：指定了联机手册的搜寻路径, 如果没有指定则使用环境变数MANPATH的设定；如果没有使用MANPATH， 则会使用/usr/lib/man.conf内的设定；如果MANPATH是空字串，则表示使用缺省值。

-P pager：指定使用何种pager.man会优先使用此选项设定，然后是依环境变数MANPAGER设定，然后是环境变数PAGER；man缺省使用/usr/bin/less -is。

-S section\_list man：所搜寻的章节列表(以冒号分隔)，此选项会覆盖环境变数MANSECT的设定。

-a man：缺省情况是在显示第一个找到的手册之后，就会停止搜寻，使用此选项会强迫man继续显示所有符合name的联机手册。

-c：即使有最新的cat page，也继续对联机手册重新作排版，本选项在屏幕的行列数改变时或已排版的联机手册损坏时特别有意义。

-d：不要真的显示联机手册，只显示除错讯息。

-D：同时显示联机手册与除错讯息。

-h：显示求助讯息然后结束程式 。

-K：对所有的联机手册搜寻所指定的字串。请注意，本功能回应速度可能很慢，如果指定section（区域）会对速度有帮助。

-m system：依所指定的system名称而指定另一组的联机手册。

man：是manual（手册）的缩写。在输入命令有困难时，可以立刻得到这个文档。例如, 如果使用ps命令时遇到困难，可以输入man ps得到帮助信息，此时会显示出ps的手册页（man page）。

由于手册页man page是用less程序来看的(可以方便地使屏幕上翻和下翻), 所以在man page里可以使用less的所有选项。

less中比较重要的功能键有:

[q] 退出；

[Enter] 一行行地下翻；

[Space] 一页页地下翻；

上翻一页；

[/] 后跟一个字符串和[Enter]来查找字符串；

[n] 发现上一次查找的下一个匹配。

4.阅读手册页

手册页在很少的空间里提供了很多的信息， 这里简单介绍一下大多数手册页中都有的部分内容。Linux手册页主要有九个部分：用户指令、系统调用、程序库、设备说明、文件格式、游戏、杂项、系统指令、内核，手册页快照见图1所示。

图1 ps命令手册页快照

Linux手册页布局见表1。

5.应用实例

Linux

命令中有一些基础的、重要的命令，例如ps、find、cat和ls等。下面来举一个综合应用的例子，由此可以看出man的地位在Linux中可谓至关重

要。但是，man所显示的信息却不是普通的文本，如果直接将这些文字重定向到一个文本文件，就会发现在man中高亮显示的文字就变成了两个，而且有不计其

数的制表符，使打印、编辑都变得非常不便。不过，使用下面这样一条语句就能得到ps命令打印。

# man ps | col -b | lpr

这条命令同时运用了输出重定向和管道两种技巧，作用是将ps命令的帮助信息可以直接打印出来。更多的Man文件可以查看Linux Man

unencode

1.作用

unencode命令可以把一个二进制文件表编码为一个文本文件，使用权限是所有用户。

2.格式

uuencode [-hv] [源文件] 目标文件

3.主要参数

－h：列出指令使用格式(help) 。

－v：列出版本信息。

4.应用说明

uuencode指令可以将二进制文件转化成可使用电子邮件发送的ASCII编码形式。uuencode编码后的资料都以 begin开始，以end作为结束，且通常其中的每一行的开始均为“M”，中间部分是编码过的文件，编码后的文件比源文件要大一些。

uudecode

1.作用

uudecode命令用来将uuencode编码后的档案还原，uudecode只会将begin与end标记之间的编码资料还原，程序会跳过标记以外的资料。它的使用权限为所有用户。

2.格式

uuencode [-hv] [file1 ...]

3.主要参数

－h：列出指令使用格式(help)。

－v：列出版本信息。

4.应用实例

使用下面命令一次还原几个文件：

uuencode file1.uud file2.uud file3.uud

动手练习

1.在Linux命令行下发送邮件

虽然Linux桌面应用发展很快，但是命令行（Shell）在Linux中依然有很强的生命力。如果能确认电子邮件服务器支持8bit的字节，就可以直接使用下面命令：

cat ＜附件文件名＞ | mail ＜邮件地址＞

cat（cat是concatenate的缩写）命令是将几个文件处理成一个文件，并将这种处理的结果保存到一个单独的输出文件，这里我们用它来合并邮件的文本。

写好邮件名称，比如叫cjkmail，然后使用下面命令：

$uuencode ＜附件文件名＞ ＜附件文件名＞ >>cjkmail

这样就可以用vi编辑器写cjkmail文件，并在前面写上信的正文，然后寄出。

对方收到信后，把信中属于cjkmail中的内容拷贝出来，存为themail.uue。如果对方是在Windows下，就可以用WinRAR或WinZip解压，这样就可以看到附件。

如果对方也使用Linux，可以用undecode命令还原：

$ uudencode -o＜附件文件名＞ themail.uue

2.实现tar的分卷

笔者想把一个378MB的文件压缩成多个63MB的文件（笔者的USB为64MB），使用下面命令：

$tar czvf - dir | split -d -b 63m

然后合并命令：

$cat x\* > dir.tgz

以上例子实际是由三个命令组合完成的，即用tar打包，用split分割，用cat合并。“tar czvf - dir”的意思是把dir目录打包，并输出到标准输出（argv），这样就可以直接用管道输出给split。

3.连续执行一个命令

使用watch命令，可以反复执行命令。如果和ls配合，可以达到观察某文件大小变化的效果。

$watch ls －l file.name

4.用tar命令导出一个文件

有一个tar格式的DVD文件GLvPro6.4\_linux.tar，因为该文件非常大（4.7GB），如果全部解压比较麻烦，可以用下面命令先导出readme.txt看看。

tar xvf GLvPro6.4\_linux.tar readme.txt

这样readme.txt就单独被导出了。

5.用tar打包一个目录时只备份其中的几个子目录

tar cf --exclude home/cjh home/cao

这样home目录下只有cjh和cao两个子目录备份。

到此为止，Linux必学的60个命令已经全部介绍完了。Linux的命令行方式功能强大，如果熟练掌握了Linux的常用命令，往往只需要通过各种技巧就

可以组合构成一条复杂的命令，从而完成用户任务。Linux系统中的命令实在是太多了，不可能像在MS

DOS中把所有的命令及参数都记住。Linux系统提供了一些方法，比如可以通过“help”和“man”来查询名令。

高级命令

1.rpm

RMP 是 LINUX 下的一种软件的可执行程序，你只要安装它就可以了。这种软件安装包通常是一个RPM包（Redhat Linux Packet Manager，就是Redhat的包管理器），后缀是.rpm。

RPM是Red Hat公司随Redhat Linux推出了一个软件包管理器，通过它能够更加轻松容易地实现软件的安装。

1.安装软件：执行rpm -ivh rpm包名（,ivh是以verbose模式安装,可显示进度条的.），如：

#rpm -ivh apache-1.3.6.i386.rpm

2.升级软件：执行rpm -Uvh rpm包名。

3.反安装：执行rpm -e rpm包名。

4.查询软件包的详细信息：执行rpm -qpi rpm包名

5.查询某个文件是属于那个rpm包的：执行rpm -qf rpm包名

6.查该软件包会向系统里面写入哪些文件：执行 rpm -qpl rpm包名

2.update-alternatives

update-alternatives --install /usr/bin/java java /wrroy/bin/jdk1.8.0\_65/bin/java 60

update-alternatives --remove java /wrroy/bin/jdk1.8.0\_65/bin/java

返回上一次目录

返回上一次目录

有时候千辛万苦进入了一个很深层的目录，一不小心输入了cd并回车，有什么办法快速回到刚才所在的目录呢？对于bash来说，只需要很管理的一个命令：

## cd -

该命令等同于cd $OLDPWD，关于这一点在bash的手册页(可使用命令man bash访问其手册页)中有介绍：

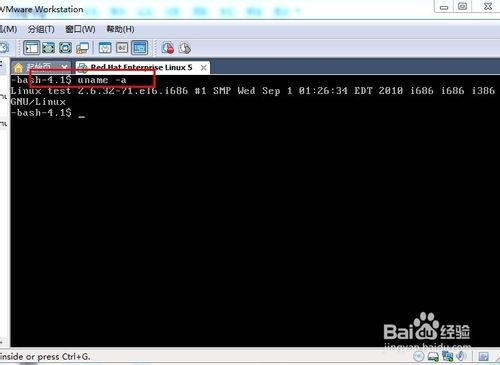
An argument of - is equivalent to $OLDPWD.

并且它还会返回上一次目录的物理路径。

## 系统信息

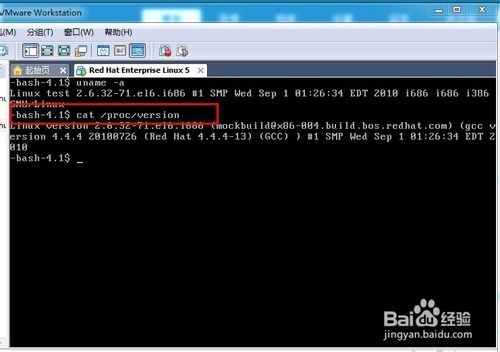
J

输入"uname -a ",可显示电脑以及操作系统的相关信息。



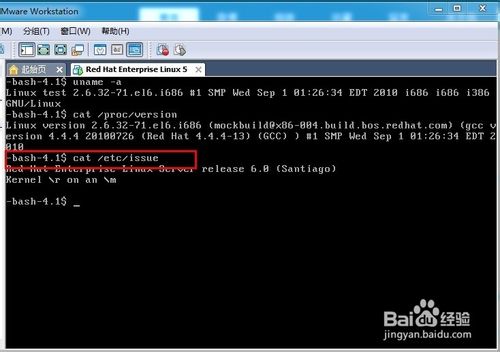
1. 2

输入"cat /proc/version",说明正在运行的内核版本。



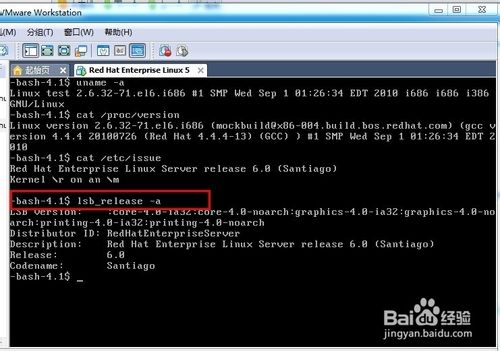
1. 3

输入"cat /etc/issue", 显示的是发行版本信息



1. 4

lsb\_release -a (适用于所有的linux，包括Redhat、SuSE、Debian等发行版，但是在debian下要安装lsb)



END

注意事项

* 如果不知道命令的意思.可以通过 "man 命令"可以查看它的使用方式.及详细信息.

参考链接：<http://jingyan.baidu.com/article/7908e85c725159af481ad2f7.html>

1.查看硬盘

[mushme@investide ~]$ df -ah

文件系统              容量  已用 可用 已用% 挂载点

/dev/cciss/c0d0p1     123G   63G   55G  54% /

proc                     0     0     0   -  /proc

sysfs                    0     0     0   -  /sys

devpts                   0     0     0   -  /dev/pts

tmpfs                 2.0G     0  2.0G   0% /dev/shm

none                     0     0     0   -  /proc/sys/fs/binfmt\_misc

sunrpc                   0     0     0   -  /var/lib/nfs/rpc\_pipefs

nfsd                     0     0     0   -  /proc/fs/nfsd

查看目录大小

du -sh /project

2.查看内存

[mushme@investide ~]$ free -m

             total       used       free     shared    buffers     cached

Mem:          3916       3281        634          0        135       1858

-/+ buffers/cache:       1287       2628

Swap:        10000        235       9765

或者用下面这个命令

cat /proc/meminfo

3.查看cpu

[mushme@investide ~]$ cat /proc/cpuinfo | grep name | cut -f2 -d: | uniq -c

      8  Intel(R) Xeon(R) CPU           E5506  @ 2.13GHz

说明是8个逻辑cpu

[mushme@investide ~]$ cat /proc/cpuinfo | grep physical | uniq -c

      4 physical id     : 0

      4 physical id     : 1

实际是2个cpu

[mushme@investide ~]$ getconf LONG\_BIT

32

当前cpu运行在32位下

[mushme@investide ~]$ cat /proc/cpuinfo | grep flags | grep ' lm ' | wc -l

8

(结果大于0, 说明支持64bit计算. lm指long mode, 支持lm则是64bit)

再完整看cpu详细信息, 不过大部分我们都不关心而已.

# dmidecode | grep 'Processor Information'

4.查看当前操作系统内核信息

[mushme@investide ~]$ uname -a

Linux investide.cn 2.6.18-238.9.1.el5PAE #1 SMP Tue Apr 12 18:52:55 EDT 2011 i686 i686 i386 GNU/Linux

5.查看网卡信息

# dmesg | grep -i eth

6.查看系统

cat /etc/issue

原文链接：<http://www.oschina.net/question/12_30886?sort=time>

# Ssh

## Xshell

### Xshell实现Windows上传文件到Linux主机

<http://www.linuxidc.com/Linux/2015-05/117975.htm>

经常有这样的需求，我们在Windows下载的软件包，如何上传到远程Linux主机上？还有如何从Linux主机下载软件包到Windows下；之前我的做法现在看来好笨好繁琐，不过也达到了目的，笨人有本方法嘛；

我是怎么操作的：

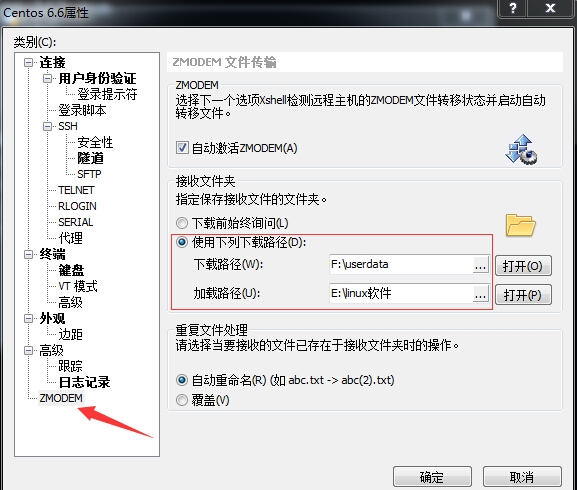
1、打开一台本地Linux虚拟机，使用mount 挂载Windows的共享文件夹到Linux上，然后拷贝数据到Linux虚拟机里面；（经常第一步都不顺利，无法挂载Windows的文件夹）

2、在本地Linux虚拟机使用rsync同步拷贝的数据到远程Linux主机上，需要双方都要安装rsync包、openssh-clients包；遇到大一点的文件拷贝很费时间；

3、还有一种方法就是直接使用wget直接下载，提前是有下载的网址；大部分都是下载到Windows本地然后上传到远程Linux主机；

下面介绍一个简单的方法，方便上传Windows的文件到Linux上，也可以从Linux下载到Windows本地；

1、使用我们常用的Xshell登录工具，新建立一个远程会话，填写ip地址及用户名密码后，选择最下面的ZMODEM，填写下载的路径，加载的路径；2个路径可以一样也可以不一样；



2、在Linux主机上，安装上传下载工具包rz及sz

如果不知道你要安装包的具体名称，可以使用yum provides \*/name 进行查找系统自带软件包的信息；

[root@localhost src]# yum provides \*/rz

lrzsz-0.12.20-27.1.el6.i686 : The lrz and lsz modem communications programs

Repo        : base

Filename    : /usr/bin/rz

一般会列出软件包的名称及版本，还有安装路径；查询到软件包名后，使用yum install -y 包名 进行安装。

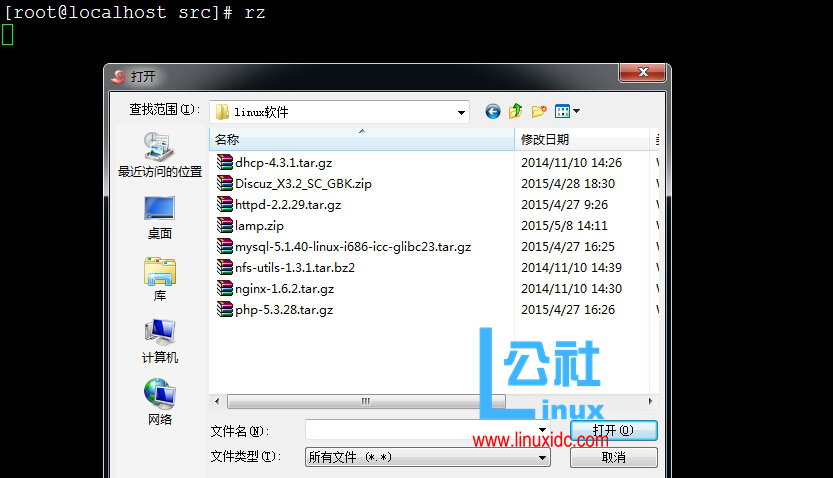
lrzsz包安装完成后包括上传rz、下载sz命令；只需要安装这个包即可。

[root@localhost src]# yum install -y lrzsz

3、从Windows上传文件，上传命令为rz；在Linux命令行下输入rz，上传的文件在当前命令行的目录下；

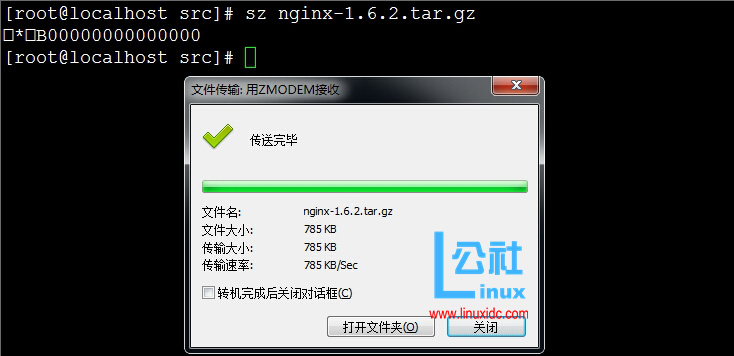
[root@localhost src]# rz

输入rz命令后，会弹出对话框，选择你要上传的文件，选择打开就上传到Linux主机。上传完可以使用ls 查看；



4、从Linux主机下载文件，下载命令为sz ，后面跟要下载的文件名；可以选择下载的保存文件夹；

[root@localhost src]# sz nginx-1.6.2.tar.gz



此方法相对来说比较简单快捷，可以满足日常需要，有更好的方法欢迎大家互相交流。

Xshell 登录 [CentOS](http://www.linuxidc.com/topicnews.aspx?tid=14) 6.3 中文乱码的解决 <http://www.linuxidc.com/Linux/2013-06/86600.htm>

VirtualBox4.12文本安装CentOS 5.4以及Xshell连接教程 PDF <http://www.linuxidc.com/Linux/2013-06/85575.htm>

Xshell连接CentOS6.5 iptables或ls 输出乱码 <http://www.linuxidc.com/Linux/2014-06/103725.htm>

VMware Linux使用Xshell登陆 <http://www.linuxidc.com/Linux/2012-06/62546.htm>

使用Xshell密钥认证机制远程登录Linux <http://www.linuxidc.com/Linux/2015-03/114947.htm>

**本文永久更新链接地址**：<http://www.linuxidc.com/Linux/2015-05/117975.htm>

# 分区管理

1. **使用Ext4 without journaling文件系统**

Sdfa

选择了Ext4系统,接下来需要关闭日志功能。

首先,系统挂载时无法停用日志功能,所以需要进入刚才的U盘系统,利用root权限执行:

tune2fs -O ^has\_journal /dev/sda1

即关闭/dev/sda1上的日志功能。

然后,运行操作系统检测:

e2fsck -f /dev/sda1

不这样,文件系统可能会出错。

最后,重启,进入SSD中的系统,检查是否设置成功:

dmesg | grep EXT4

如果出现:

EXT4-fs (sda1): mounted filesystem without journal

说明设置成功。

原来是:mounted filesystem with ordered data mode

如果需要再次开启日志功能,只要运行tune2fs -O has\_journal /dev/sda1即可

内核版本cat /proc/version

先查看下是否有磁盘没有分区

fdisk -l

<https://www.cnblogs.com/visec479/p/4072754.html>

格式化分区

格式化命令：mkfs.ext3 /dev/sdb1 是格式化成 ext3

自动挂载新分区到指定目录下

起因：ubuntu系统使用固态硬盘120G不够使用，如今已无法满足日常需要，于是增加了一枚机械硬盘，分别分了两个空闲分区，依次使系统自启时挂在到/home/和/usr/指定目录下

安装过程：

查看硬盘所有分区并记录下待挂在分区（主要以硬盘，分区大小和格式确定）

fdisk -l

格式化分区为ext4

mkfs.ext4 /dev/sda7

查看分区UUID

sudo blkid

编辑系统挂载配置文件/etc/fstab

vim /etc/fstab

增加：

# new /dev/sda6

UUID=fdccb3ee-1efb-4822-b947-9ad28a4c4243 /home/zhoudazhuang/dev\_sda\_6 ext4 defaults 0 0

# new /dev/sda7

UUID=f3ff6a9b-71d6-4daa-bfc2-805d50a03c50 /usr/dev\_sda\_7 ext4 defaults 0 0

注：格式为 设备名称 挂载点 分区类型 挂载选项 dump选项 fsck选项

dump选项–这一项为0，就表示从不备份。如果上次用dump备份，将显示备份至今的天数。

fsck选项 –启动时fsck检查的顺序。为0就表示不检查，（/）分区永远都是1，其它的分区只能从2开始，当数字相同就同时检查（但不能有两1）

修改文件所属权限

sudo chown -R zhoudazhuang:zhoudazhuang /home/zhoudazhuang/dev\_sda\_6

sudo chmod -R 4755 /home/zhoudazhuang/dev\_sda\_6

在注：chmod使用的数字的意思： 读（r=4），写（w=2），执行（x=1）可读可写为4+2=6 依次内存 755表示的是文件所有者权限7（三者权限之和），与所有者同组用户5（读+执行），其他用户同前一个5，这里的4的意思是（其他）用户执行拥有所有者相同的文件权限（对于其他要使用的文件）

重启

sudo reboot now

apt-get install xxx时出错

<https://blog.csdn.net/sela0708/article/details/72905044>

通过终端安装程序sudo apt-get install xxx时出错：

出现这个问题可能是有另外一个程序正在运行，导致资源被锁不可用。而导致资源被锁的原因可能是上次运行安装或更新时没有正常完成，进而出现此状况，解决的办法其实很简单：

在终端中敲入以下两句

sudo rm /var/cache/apt/archives/lock

sudo rm /var/lib/dpkg/lock

还是会卡住：重启按住shift，修复一下安装包就好了！！！！

**Ubuntu系统SSD硬盘优化**

https://www.aliyun.com/jiaocheng/157810.html

# 账户管理

## 切换到root身份

1. sudo+命令，输入当前用户密码后以root权限执行命令，有时间限制且仅限当前命令。
2. sudo -i，输入当前用户密码后以root权限登录shell，无时间限制。使用exit或logout退出。
3. su，输入root账户的密码后切换到root身份，无时间限制。su 用户名切换回其它用户。
4. sudo su，效果同su，只是不需要root的密码，而需要当前用户的密码。
5. 一、Ubuntu的
6. 默认root密码是随机的，即每次开机都有一个新的root密码。我们可以在终端输入命令 sudo passwd，然后输入当前用户的密码，
7. enter，
8. 二、终端会提示我们输入新的密码并确认，此时的密码就是root新密码。修改成功后，输入命令 su root，再输入新的密码就ok了。

# 常用软件包

F

软件中心：谷歌浏览器，

下载安装:搜狗<https://jingyan.baidu.com/article/ad310e80ae6d971849f49ed3.html>

重启就好。

安装无线驱动：<http://blog.csdn.net/zx3517288/article/details/51580063>

<http://cdn-cw.mediatek.com/Downloads/linux/DPO_MT7601U_LinuxSTA_3.0.0.4_20130913.tar.bz2>

[e](http://wifi.tenda.com.cn/)

vi /etc/modprobe.d/blacklist.conf

安装搬瓦工翻墙：

软件使用

 1. 在终端下：

          复制命令：Ctrl + Shift + C  组合键.

          粘贴命令：Ctrl + Shift + V  组合键.

## Apt管理

<code style="font-family:Consolas, 'Liberation Mono', Menlo, Courier, monospace;font-size:.85em;border:none;color:rgb(4,4,224);background:0px 0px;line-height:inherit;">sudo apt-get update 更新源

  sudo apt-get install package 安装包

  sudo apt-get remove package 删除包

  sudo apt-cache search package 搜索软件包

  sudo apt-cache show package 获取包的相关信息，如说明、大小、版本等

  sudo apt-get install package --reinstall 重新安装包

  sudo apt-get -f install 修复安装

  sudo apt-get remove package --purge 删除包，包括配置文件等

  sudo apt-get build-dep package 安装相关的编译环境

  sudo apt-get upgrade 更新已安装的包

  sudo apt-get dist-upgrade 升级系统

  sudo apt-cache depends package 了解使用该包依赖那些包

  sudo apt-cache rdepends package 查看该包被哪些包依赖

  sudo apt-get source package 下载该包的源代码

  sudo apt-get clean && sudo apt-get autoclean 清理无用的包

 

Ubuntu

## 如何添加快速启动方式

**Ubuntu12.10添加matlab启动器**

首先我们要了解，Ubuntu 的 Dash 里所有程序都是在 /usr/share/applications 中的，所以我们的思路很简单——建一个类似于“快捷方式”一样的东西扔进去就好了。

1. 终端运行gedit matlab.desktop & #创建一个eclipse.desktop文件

在该文件中编辑如下：

[Desktop Entry]

Name=matlab

Name[zh\_CN]=matlab

Comment=matlab

Exec=/usr/local/matlab/bin/matlab -desktop

Icon=/usr/local/matlab/toolbox/nnet/nnresource/icons/matlab.png

Terminal=false

Type=Application

Categories=Application;

Encoding=UTF-8

StartupNotify=true

注意：上述执行目录Exec设置中必须加上“空格-desktop”否则，matlab只会闪一下

2. 保存文件，修改权限

chmod 777 eclipse.desktop #该方式比较暴力

3.然后将该文件复制到/usr/share/applications/

sudo cp matlab.desktop /usr/share/applications

4. 点击Dash会发现matlab图标，点击即可打开，为方便也可将图标拖拽至启动器

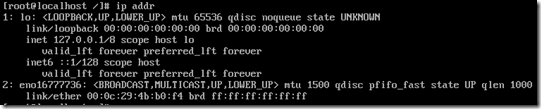
<http://www.csdn123.com/html/itweb/20130907/105358_105356_105336.htm>

# 虚拟机

G

**3. 配置网络**

输入：ip addr，显示网络并未连接

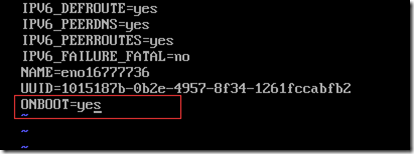


查看“虚拟机->设置->网络适配器”选择连接模式为“NAT模式”

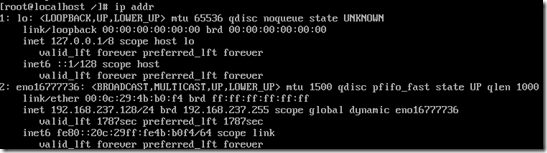
终端打开"/etc/sysconfig/network-script/ifcfg-eno16777736"

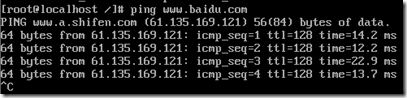
技术分享

修改ONBOOT=yes



输入"service network restart"重启网络服务，再次检查ip，以及ping





ctrl+c

ctrl+d

可以停止评

**4. 更新及安装软件**

yum inatall [perl](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=perl&k0=perl&kdi0=0&luki=2&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)        //后面安装MVwareTools必装软件

yum install net-[tools](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=tools&k0=tools&kdi0=0&luki=6&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)  //ifconfig命令,MVwareTools也需要使用

yum install gcc //一套由GNU工程开发的支持多种[编程语言](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%B1%E0%B3%CC%D3%EF%D1%D4&k0=%B1%E0%B3%CC%D3%EF%D1%D4&kdi0=0&luki=8&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)的[编译器](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%B1%E0%D2%EB%C6%F7&k0=%B1%E0%D2%EB%C6%F7&kdi0=0&luki=4&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)，MVwareTools也需要使用

yum install kernel-devel //MVwareTools也需要使用，内核开发需要的头文件，用于代码编译

yum install make //MVwareTools也需要使用，makefile，安装完后，重启os

yum -y update  //更新系统，需要5分钟左右

yum install vim        //强大的Vi编辑器，minial7自带了

yum install wget    //从网络上自动下载文件的工具

yum install cpp

yum install gcc-c++

yum install gdb   //调试[工具](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%B9%A4%BE%DF&k0=%B9%A4%BE%DF&kdi0=0&luki=1&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)

yum groupinstall "Development Tools"

说明：

    查询本地是否[安装](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%B0%B2%D7%B0&k0=%B0%B2%D7%B0&kdi0=0&luki=9&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)某个软件

    输入： rpm –qa xxx

    返回：版本号 or 无

**5. 修改默认分辨率**

查看：<http://www.centoscn.com/CentOS/config/2014/1031/4029.html>

修改文件"/boot/grub2/grub.cfg"，找到

linux16 /vmlinuz-3.10.0-123.el7.x86\_64 root=UUID=881ac4e6-4a55-47b1-b864-555de7051763 ro rd.lvm.lv=centos/swap vconsole.font=latarcyrheb-sun16 rd.lvm.lv=centos/root crashkernel=auto  vconsole.keymap=us rhgb quiet LANG=en\_US.UTF-8

在后面添加vga=0x???(问号代表分辨率代码)，在这里贴一张对应表，方便查看



修改后如下：



然后修改运行级别，打开"/etc/inittab"



在后面添加

# ln -sf /lib/systemd/system/runlevel?.target /etc/systemd/system/default.target

保存后，快来重启试试吧！

**6. 安装VMwareTools**

1).点击“[虚拟机](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%D0%E9%C4%E2%BB%FA&k0=%D0%E9%C4%E2%BB%FA&kdi0=0&luki=10&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)->安装VMware Tools”加载镜像

    mkdir /mnt/cdrom

    mount /dev/cdrom /mnt/cdrom         #挂载设备

    cd /mnt/cdrom

    cp vmware-tools-xxxxxx.tar.gz /root

    umount /mnt/cdrom                         #关闭设备

    cd /root

    tar zxvf vmware-tools-xxxxxx.tar.gz #解压文件

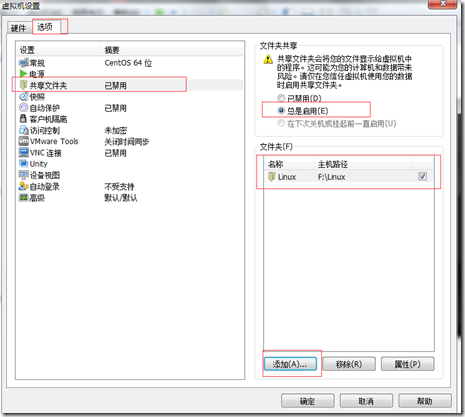
2).安装vmware-tools

    cd vmware-tools-distrib                    #进入文件目录

    ./vmware-install.pl                            #[安装](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%B0%B2%D7%B0&k0=%B0%B2%D7%B0&kdi0=0&luki=9&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)

**7. 配置共享文件夹**

点击“设置”，添加共享文件夹



在终端下"/mnt/hgfs/"下可以看到刚才添加的文件夹

技术分享

现在可以无缝连接windows和linux世界了

说明：

    我在系统update后曾经找不到共享[文件夹](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%CE%C4%BC%FE%BC%D0&k0=%CE%C4%BC%FE%BC%D0&kdi0=0&luki=5&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)了，后来上网查找发现需要重新配置Tools

    运行/usr/bin/vmware-config-[tools](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=tools&k0=tools&kdi0=0&luki=6&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0).pl即可

**无法更新运行时文件夹共享状态：在客户机操作系统内装载共享文件夹文件系统时出错--解决办法**

**8. HelloWorld**

让我们来编译运行一下程序

在windows下编写一个HelloWorl原文件，到[虚拟机](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1001&ch=0&di=128&fv=18&is_app=0&jk=2781b7566dfc8918&k=%D0%E9%C4%E2%BB%FA&k0=%D0%E9%C4%E2%BB%FA&kdi0=0&luki=10&mcpm=0&n=10&p=baidu&q=65035100_cpr&rb=0&rs=1&seller_id=1&sid=1889fc6d56b78127&ssp2=1&stid=0&t=tpclicked3_hc&td=1836545&tu=u1836545&u=http%3A%2F%2Fwww%2Ebubuko%2Ecom%2Finfodetail%2D824041%2Ehtml&urlid=0)中编译运行，快看

技术分享

9.

 Searching for a valid kernel header path.....The path " " is not a valid path to the 2.4.20-8 kernel headers.Would you like to change it

参考:

1.VM11+CentOS7mini安装及配置

http://www.bubuko.com/infodetail-824041.html

2.在VMware上安装CentOS-6.5 minimal - 安装VMware Tools

http://www.cnblogs.com/xyq/p/4068018.html

3.无法更新运行时文件夹共享状态：在客户机操作系统内装载共享文件夹文件系统时出错--解决办法

http://www.bubuko.com/infodetail-1025108.html

# vi编辑器

df

[*vi*](http://www.eepw.com.cn/news/listbylabel/label/vi)[*编辑器*](http://www.eepw.com.cn/news/listbylabel/label/%E7%BC%96%E8%BE%91%E5%99%A8)是所有Unix及Linux系统下标准的[*编辑器*](http://www.eepw.com.cn/news/listbylabel/label/%E7%BC%96%E8%BE%91%E5%99%A8)，它的强大不逊色于任何最新的文本[*编辑器*](http://www.eepw.com.cn/news/listbylabel/label/%E7%BC%96%E8%BE%91%E5%99%A8)，这里只是简单地介绍一下它的用法和一小部分指令。由于对Unix及Linux系统的任何版本，[*vi*](http://www.eepw.com.cn/news/listbylabel/label/vi)编辑器是完全相同的，因此您可以在其他任何介绍[*vi*](http://www.eepw.com.cn/news/listbylabel/label/vi)的地方进一步了解它。Vi也是Linux中最基本的文本编辑器，学会它后，您将在Linux的世界里畅行无阻。

1、vi的基本概念

　　基本上vi可以分为三种状态，分别是命令模式（command mode）、插入模式（Insert mode）和底行模式（last line mode），各模式的功能区分如下：

    1) 命令行模式command mode）

　　控制屏幕光标的移动，字符、字或行的删除，移动复制某区段及进入Insert mode下，或者到 last line mode。

    2) 插入模式（Insert mode）

　　只有在Insert mode下，才可以做文字输入，按「ESC」键可回到命令行模式。

    3) 底行模式（last line mode）

　　将文件保存或退出vi，也可以设置编辑环境，如寻找字符串、列出行号……等。

    不过一般我们在使用时把vi简化成两个模式，就是将底行模式（last line mode）也算入命令行模式command mode）。

2、vi的基本操作

a) 进入vi

   　在系统提示符号输入vi及文件名称后，就进入vi全屏幕编辑画面：

　　$ vi myfile

　　不过有一点要特别注意，就是您进入vi之后，是处于「命令行模式（command mode）」，您要切换到「插入模式（Insert mode）」才能够输入文字。初次使用vi的人都会想先用上下左右键移动光标，结果电脑一直哔哔叫，把自己气个半死，所以进入vi后，先不要乱动，转换到「插入模式（Insert mode）」再说吧！

b) 切换至插入模式（Insert mode）编辑文件

　　在「命令行模式（command mode）」下按一下字母「i」就可以进入「插入模式（Insert mode）」，这时候你就可以开始输入文字了。

c) Insert 的切换

　　您目前处于「插入模式（Insert mode）」，您就只能一直输入文字，如果您发现输错了字！想用光标键往回移动，将该字删除，就要先按一下「ESC」键转到「命令行模式（command mode）」再删除文字。

d) 退出vi及保存文件

　　在「命令行模式（command mode）」下，按一下「：」冒号键进入「Last line mode」，例如：

: w filename （输入 「w filename」将文章以指定的文件名filename保存）

: wq (输入「wq」，存盘并退出vi)

: q! (输入q!， 不存盘强制退出vi)

3、命令行模式（command mode）功能键

1）. 插入模式

       按「i」切换进入插入模式「insert mode」，按"i"进入插入模式后是从光标当前位置开始输入文件；

　　按「a」进入插入模式后，是从目前光标所在位置的下一个位置开始输入文字；

　　按「o」进入插入模式后，是插入新的一行，从行首开始输入文字。

2）. 从插入模式切换为命令行模式

      按「ESC」键。

3）. 移动光标

　　vi可以直接用键盘上的光标来上下左右移动，但正规的vi是用小写英文字母「h」、「j」、「k」、「l」，分别控制光标左、下、上、右移一格。

　　按「ctrl」+「b」：屏幕往"后"移动一页。

　　按「ctrl」+「f」：屏幕往"前"移动一页。

　　按「ctrl」+「u」：屏幕往"后"移动半页。

　　按「ctrl」+「d」：屏幕往"前"移动半页。

　　按数字「0」：移到文章的开头。

　　按「G」：移动到文章的最后。

　　按「$」：移动到光标所在行的"行尾"。

　　按「^」：移动到光标所在行的"行首"

　　按「w」：光标跳到下个字的开头

　　按「e」：光标跳到下个字的字尾

　　按「b」：光标回到上个字的开头

　　按「#l」：光标移到该行的第#个位置，如：5l,56l。

4）. 删除文字

　　「x」：每按一次，删除光标所在位置的"后面"一个字符。

　　「#x」：例如，「6x」表示删除光标所在位置的"后面"6个字符。

　　「X」：大写的X，每按一次，删除光标所在位置的"前面"一个字符。

　　「#X」：例如，「20X」表示删除光标所在位置的"前面"20个字符。

　　「dd」：删除光标所在行。

　　「#dd」：从光标所在行开始删除#行

5）. 复制

　　「yw」：将光标所在之处到字尾的字符复制到缓冲区中。

　　「#yw」：复制#个字到缓冲区

　　「yy」：复制光标所在行到缓冲区。

　　「#yy」：例如，「6yy」表示拷贝从光标所在的该行"往下数"6行文字。

　　「p」：将缓冲区内的字符贴到光标所在位置。注意：所有与"y"有关的复制命令都必须与"p"配合才能完成复制与粘贴功能。

6）. 替换

　　「r」：替换光标所在处的字符。

　　「R」：替换光标所到之处的字符，直到按下「ESC」键为止。

7）. 回复上一次操作

　　「u」：如果您误执行一个命令，可以马上按下「u」，回到上一个操作。按多次"u"可以执行多次回复。

8）. 更改

　　「cw」：更改光标所在处的字到字尾处

　　「c#w」：例如，「c3w」表示更改3个字

9）. 跳至指定的行

　　「ctrl」+「g」列出光标所在行的行号。

　　「#G」：例如，「15G」，表示移动光标至文章的第15行行首。

4、Last line mode下命令简介

　　在使用「last line mode」之前，请记住先按「ESC」键确定您已经处于「command mode」下后，再按「：」冒号即可进入「last line mode」。

A) 列出行号

　「set nu」：输入「set nu」后，会在文件中的每一行前面列出行号。

B) 跳到文件中的某一行

　「#」：「#」号表示一个数字，在冒号后输入一个数字，再按回车键就会跳到该行了，如输入数字15，再回车，就会跳到文章的第15行。

C) 查找字符

　「/关键字」：先按「/」键，再输入您想寻找的字符，如果第一次找的关键字不是您想要的，可以一直按「n」会往后寻找到您要的关键字为止。

　「?关键字」：先按「?」键，再输入您想寻找的字符，如果第一次找的关键字不是您想要的，可以一直按「n」会往前寻找到您要的关键字为止。

D) 保存文件

　「w」：在冒号输入字母「w」就可以将文件保存起来。

E) 离开vi

　「q」：按「q」就是退出，如果无法离开vi，可以在「q」后跟一个「!」强制离开vi。

　「qw」：一般建议离开时，搭配「w」一起使用，这样在退出的时候还可以保存文件。

5、vi命令列表

1、下表列出命令模式下的一些键的功能：

h

左移光标一个字符

l

右移光标一个字符

k

光标上移一行

j

光标下移一行

^

光标移动至行首

0

数字"0"，光标移至文章的开头

G

光标移至文章的最后

$

光标移动至行尾

Ctrl+f

向前翻屏

Ctrl+b

向后翻屏

Ctrl+d

向前翻半屏

Ctrl+u

向后翻半屏

i

在光标位置前插入字符

a

在光标所在位置的后一个字符开始增加

o

插入新的一行，从行首开始输入

ESC

从输入状态退至命令状态

x

删除光标后面的字符

#x

删除光标后的＃个字符

X

(大写X)，删除光标前面的字符

#X

删除光标前面的#个字符

dd

删除光标所在的行

#dd

删除从光标所在行数的#行

yw

复制光标所在位置的一个字

#yw

复制光标所在位置的#个字

yy

复制光标所在位置的一行

#yy

复制从光标所在行数的#行

p

粘贴

u

取消操作

cw

更改光标所在位置的一个字

#cw

更改光标所在位置的#个字

2、下表列出行命令模式下的一些指令

w filename

储存正在编辑的文件为filename

wq filename

储存正在编辑的文件为filename，并退出vi

q!

放弃所有修改，退出vi

set nu

显示行号

/或?

查找，在/后输入要查找的内容

n

与/或?一起使用，如果查找的内容不是想要找的关键字，按n或向后（与/联用）或向前（与?联用）继续查找，直到找到为止。

对于第一次用vi，有几点注意要提醒一下：

1、用vi打开文件后，是处于「命令行模式（command mode）」，您要切换到「插入模式（Insert mode）」才能够输入文字。切换方法：在「命令行模式（command mode）」下按一下字母「i」就可以进入「插入模式（Insert mode）」，这时候你就可以开始输入文字了。

2、编辑好后，需从插入模式切换为命令行模式才能对文件进行保存，切换方法：按「ESC」键。

3、保存并退出文件：在命令模式下输入:wq即可！（别忘了wq前面的）

**vi使用手册**

|  |
| --- |
|  |
|  |

|  |
| --- |
| VI是unix上最常用的文本编辑工具，作为unix软件测试人员，有必要熟练掌握它。  进入vi的命令  vi filename :打开或新建文件，并将光标置于第一行首  vi +n filename ：打开文件，并将光标置于第n行首  vi + filename ：打开文件，并将光标置于最后一行首  vi +/pattern filename：打开文件，并将光标置于第一个与pattern匹配的串处  vi -r filename ：在上次正用vi编辑时发生系统崩溃，恢复filename  vi filename....filename ：打开多个文件，依次编辑  移动光标类命令  h ：光标左移一个字符  l ：光标右移一个字符  space：光标右移一个字符  Backspace：光标左移一个字符  k或Ctrl+p：光标上移一行  j或Ctrl+n ：光标下移一行  Enter ：光标下移一行  w或W ：光标右移一个字至字首  b或B ：光标左移一个字至字首  e或E ：光标右移一个字j至字尾  ) ：光标移至句尾  ( ：光标移至句首  }：光标移至段落开头  {：光标移至段落结尾  nG：光标移至第n行首  n+：光标下移n行  n-：光标上移n行  n$：光标移至第n行尾  H ：光标移至屏幕顶行  M ：光标移至屏幕中间行  L ：光标移至屏幕最后行  0：（注意是数字零）光标移至当前行首  $：光标移至当前行尾  屏幕翻滚类命令  Ctrl+u：向文件首翻半屏  Ctrl+d：向文件尾翻半屏  Ctrl+f：向文件尾翻一屏  Ctrl＋b；向文件首翻一屏  nz：将第n行滚至屏幕顶部，不指定n时将当前行滚至屏幕顶部。  插入文本类命令  i ：在光标前  I ：在当前行首  a：光标后  A：在当前行尾  o：在当前行之下新开一行  O：在当前行之上新开一行  r：替换当前字符  R：替换当前字符及其后的字符，直至按ESC键  s：从当前光标位置处开始，以输入的文本替代指定数目的字符  S：删除指定数目的行，并以所输入文本代替之  ncw或nCW：修改指定数目的字  nCC：修改指定数目的行  删除命令  ndw或ndW：删除光标处开始及其后的n-1个字  do：删至行首  d$：删至行尾  ndd：删除当前行及其后n-1行  x或X：删除一个字符，x删除光标后的，而X删除光标前的  Ctrl+u：删除输入方式下所输入的文本  搜索及替换命令 :  /pattern：从光标开始处向文件尾搜索pattern  ?pattern：从光标开始处向文件首搜索pattern  n：在同一方向重复上一次搜索命令  N：在反方向上重复上一次搜索命令  ：s/p1/p2/g：将当前行中所有p1均用p2替代  ：n1,n2s/p1/p2/g：将第n1至n2行中所有p1均用p2替代  ：g/p1/s//p2/g：将文件中所有p1均用p2替换  选项设置  all：列出所有选项设置情况  term：设置终端类型  ignorance：在搜索中忽略大小写  list：显示制表位(Ctrl+I)和行尾标志（$)  number：显示行号  report：显示由面向行的命令修改过的数目  terse：显示简短的警告信息  warn：在转到别的文件时若没保存当前文件则显示NO write信息  nomagic：允许在搜索模式中，使用前面不带“\”的特殊字符  nowrapscan：禁止vi在搜索到达文件两端时，又从另一端开始  mesg：允许vi显示其他用户用write写到自己终端上的信息  最后行方式命令  ：n1,n2 co n3：将n1行到n2行之间的内容拷贝到第n3行下  ：n1,n2 m n3：将n1行到n2行之间的内容移至到第n3行下  ：n1,n2 d ：将n1行到n2行之间的内容删除  ：w ：保存当前文件  ：e filename：打开文件filename进行编辑  ：x：保存当前文件并退出  ：q：退出vi  ：q!：不保存文件并退出vi  ：!command：执行shell命令command  ：n1,n2 w!command：将文件中n1行至n2行的内容作为command的输入并执行之，若不指  定n1，n2，则表示将整个文件内容作为command的输入 |

参考地址:<http://www.eepw.com.cn/article/48018.htm>

# Wget

Linux wget是一个下载文件的工具，它用在命令行下。对于Linux用户是必不可少的工具，尤其对于网络管理员，经常要下载一些软件或从远程服务器恢复备份到本地服务器

Linux wget是一个下载文件的工具，它用在命令行下。对于Linux用户是必不可少的工具，尤其对于网络管理员，经常要下载一些软件或从远程服务器恢复备份到本地服务器。如果我们使用虚拟主机，处理这样的事务我们只能先从远程服务器下载到我们电脑磁盘，然后再用ftp工具上传到服务器。这样既浪费时间又浪费精力，那不没办法的事。而到了Linux VPS，它则可以直接下载到服务器而不用经过上传这一步。wget工具体积小但功能完善，它支持断点下载功能，同时支持FTP和HTTP下载方式，支持代理服务器和设置起来方便简单。下面我们以实例的形式说明怎么使用wget。

**1、使用wget下载单个文件**

以下的例子是从网络下载一个文件并保存在当前目录

wget http://cn.wordpress.org/wordpress-3.1-zh\_CN.zip

在下载的过程中会显示进度条，包含（下载完成百分比，已经下载的字节，当前下载速度，剩余下载时间）。

**2、使用wget -O下载并以不同的文件名保存**

wget默认会以最后一个符合”/”的后面的字符来命令，对于动态链接的下载通常文件名会不正确。

错误：下面的例子会下载一个文件并以名称download.php?id=1080保存

wget http://www.centos.bz/download?id=1

即使下载的文件是zip格式，它仍然以download.php?id=1080命令。

正确：为了解决这个问题，我们可以使用参数-O来指定一个文件名：

wget -O wordpress.zip http://www.centos.bz/download.php?id=1080

**3、使用wget –limit -rate限速下载**

当你执行wget的时候，它默认会占用全部可能的宽带下载。但是当你准备下载一个大文件，而你还需要下载其它文件时就有必要限速了。

wget –limit-rate=300k http://cn.wordpress.org/wordpress-3.1-zh\_CN.zip

**4、使用wget -c断点续传**

使用wget -c重新启动下载中断的文件:

wget -c http://cn.wordpress.org/wordpress-3.1-zh\_CN.zip

对于我们下载大文件时突然由于网络等原因中断非常有帮助，我们可以继续接着下载而不是重新下载一个文件。需要继续中断的下载时可以使用-c参数。

**5、使用wget -b后台下载**

对于下载非常大的文件的时候，我们可以使用参数-b进行后台下载。

wget -b http://cn.wordpress.org/wordpress-3.1-zh\_CN.zip

Continuing in background, pid 1840.

Output will be written to `wget-log’.

你可以使用以下命令来察看下载进度

tail -f wget-log

**6、伪装代理名称下载**

有些网站能通过根据判断代理名称不是浏览器而拒绝你的下载请求。不过你可以通过–user-agent参数伪装。

wget –user-agent=”Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/534.16 (KHTML, like Gecko) Chrome/10.0.648.204 Safari/534.16″ 下载链接

**7、使用wget –spider测试下载链接**

当你打算进行定时下载，你应该在预定时间测试下载链接是否有效。我们可以增加–spider参数进行检查。

wget –spider URL

如果下载链接正确，将会显示

wget –spider URL

Spider mode enabled. Check if remote file exists.

HTTP request sent, awaiting response… 200 OK

Length: unspecified [text/html]

Remote file exists and could contain further links,

but recursion is disabled — not retrieving.

这保证了下载能在预定的时间进行，但当你给错了一个链接，将会显示如下错误

wget –spider url

Spider mode enabled. Check if remote file exists.

HTTP request sent, awaiting response… 404 Not Found

Remote file does not exist — broken link!!!

你可以在以下几种情况下使用spider参数：

定时下载之前进行检查

间隔检测网站是否可用

检查网站页面的死链接

**8、使用wget –tries增加重试次数**

如果网络有问题或下载一个大文件也有可能失败。wget默认重试20次连接下载文件。如果需要，你可以使用–tries增加重试次数。

wget –tries=40 URL

**9、使用wget -i下载多个文件**

首先，保存一份下载链接文件

cat > filelist.txt

url1

url2

url3

url4

接着使用这个文件和参数-i下载

wget -i filelist.txt

**10、使用wget –mirror镜像网站**

下面的例子是下载整个网站到本地。

wget –mirror -p –convert-links -P ./LOCAL URL

–miror:开户镜像下载

-p:下载所有为了html页面显示正常的文件

–convert-links:下载后，转换成本地的链接

-P ./LOCAL：保存所有文件和目录到本地指定目录

**11、使用wget –reject过滤指定格式下载**

你想下载一个网站，但你不希望下载图片，你可以使用以下命令。

wget –reject=gif url

**12、使用wget -o把下载信息存入日志文件**

你不希望下载信息直接显示在终端而是在一个日志文件，可以使用以下命令：

wget -o download.log URL

**13、使用wget -Q限制总下载文件大小**

当你想要下载的文件超过5M而退出下载，你可以使用以下命令:

wget -Q5m -i filelist.txt

注意：这个参数对单个文件下载不起作用，只能递归下载时才有效。

**14、使用wget -r -A下载指定格式文件**

可以在以下情况使用该功能

下载一个网站的所有图片

下载一个网站的所有视频

下载一个网站的所有PDF文件

wget -r -A.pdf url

**15、使用wget FTP下载**

你可以使用wget来完成ftp链接的下载。

使用wget匿名ftp下载

wget ftp-url

使用wget用户名和密码认证的ftp下载

wget –ftp-user=USERNAME –ftp-password=PASSWORD url

**wget是在Linux下开发的开放源代码的软件，作者是Hrvoje Niksic，后来被移植到包括Windows在内的各个平台上。它有以下功能和特点：**

（1）支持断点下传功能；这一点，也是网络蚂蚁和FlashGet当年最大的卖点，现在，Wget也可以使用此功能，那些网络不是太好的用户可以放心了；

（2）同时支持FTP和HTTP下载方式；尽管现在大部分软件可以使用HTTP方式下载，但是，有些时候，仍然需要使用FTP方式下载软件；

（3）支持代理服务器；对安全强度很高的系统而言，一般不会将自己的系统直接暴露在互联网上，所以，支持代理是下载软件必须有的功能；

（4）设置方便简单；可能，习惯图形界面的用户已经不是太习惯命令行了，但是，命令行在设置上其实有更多的优点，最少，鼠标可以少点很多次，也不要担心是否错点鼠标；

（5）程序小，完全免费；程序小可以考虑不计，因为现在的硬盘实在太大了；完全免费就不得不考虑了，即使网络上有很多所谓的免费软件，但是，这些软件的广告却不是我们喜欢的；

wget虽然功能强大，但是使用起来还是比较简单的，基本的语法是：wget [参数列表] URL。下面就结合具体的例子来说明一下wget的用法。

**1、下载整个http或者ftp站点。**

wget http://place.your.url/here

这个命令可以将http://place.your.url/here 首页下载下来。使用-x会强制建立服务器上一模一样的目录，如果使用-nd参数，那么服务器上下载的所有内容都会加到本地当前目录。

wget -r http://place.your.url/here

这 个命令会按照递归的方法，下载服务器上所有的目录和文件，实质就是下载整个网站。这个命令一定要小心使用，因为在下载的时候，被下载网站指向的所有地址同 样会被下载，因此，如果这个网站引用了其他网站，那么被引用的网站也会被下载下来！基于这个原因，这个参数不常用。可以用-l number参数来指定下载的层次。例如只下载两层，那么使用-l 2。

要是您想制作镜像站点，那么可以使用－m参数，例如：wget -m http://place.your.url/here

这时wget会自动判断合适的参数来制作镜像站点。此时，wget会登录到服务器上，读入robots.txt并按robots.txt的规定来执行。

**2、断点续传。**

当文件特别大或者网络特别慢的时候，往往一个文件还没有下载完，连接就已经被切断，此时就需要断点续传。wget的断点续传是自动的，只需要使用-c参数，例如：

wget -c http://the.url.of/incomplete/file

使用断点续传要求服务器支持断点续传。-t参数表示重试次数，例如需要重试100次，那么就写-t 100，如果设成-t 0，那么表示无穷次重试，直到连接成功。-T参数表示超时等待时间，例如-T 120，表示等待120秒连接不上就算超时。

**3、批量下载。**

如果有多个文件需要下载，那么可以生成一个文件，把每个文件的URL写一行，例如生成文件download.txt，然后用命令：wget -i download.txt

这样就会把download.txt里面列出的每个URL都下载下来。（如果列的是文件就下载文件，如果列的是网站，那么下载首页）

**4、选择性的下载。**

可以指定让wget只下载一类文件，或者不下载什么文件。例如：

wget -m –reject=gif http://target.web.site/subdirectory

表示下载http://target.web.site/subdirectory，但是忽略gif文件。–accept=LIST 可以接受的文件类型，–reject=LIST拒绝接受的文件类型。

**5、密码和认证。**

wget只能处理利用用户名/密码方式限制访问的网站，可以利用两个参数：

–http-user=USER设置HTTP用户

–http-passwd=PASS设置HTTP密码

对于需要证书做认证的网站，就只能利用其他下载工具了，例如curl。

**6、利用代理服务器进行下载。**

如果用户的网络需要经过代理服务器，那么可以让wget通过代理服务器进行文件的下载。此时需要在当前用户的目录下创建一个.wgetrc文件。文件中可以设置代理服务器：

http-proxy = 111.111.111.111:8080

ftp-proxy = 111.111.111.111:8080

分别表示http的代理服务器和ftp的代理服务器。如果代理服务器需要密码则使用：

–proxy-user=USER设置代理用户

–proxy-passwd=PASS设置代理密码

这两个参数。

使用参数–proxy=on/off 使用或者关闭代理。

wget还有很多有用的功能，需要用户去挖掘。

附录：

命令格式：

wget [参数列表] [目标软件、网页的网址]

-V,–version 显示软件版本号然后退出；

-h,–help显示软件帮助信息；

-e,–execute=COMMAND 执行一个 “.wgetrc”命令

-o,–output-file=FILE 将软件输出信息保存到文件；

-a,–append-output=FILE将软件输出信息追加到文件；

-d,–debug显示输出信息；

-q,–quiet 不显示输出信息；

-i,–input-file=FILE 从文件中取得URL；

-t,–tries=NUMBER 是否下载次数（0表示无穷次）

-O –output-document=FILE下载文件保存为别的文件名

-nc, –no-clobber 不要覆盖已经存在的文件

-N,–timestamping只下载比本地新的文件

-T,–timeout=SECONDS 设置超时时间

-Y,–proxy=on/off 关闭代理

-nd,–no-directories 不建立目录

-x,–force-directories 强制建立目录

–http-user=USER设置HTTP用户

–http-passwd=PASS设置HTTP密码

–proxy-user=USER设置代理用户

–proxy-passwd=PASS设置代理密码

-r,–recursive 下载整个网站、目录（小心使用）

-l,–level=NUMBER 下载层次

-A,–accept=LIST 可以接受的文件类型

-R,–reject=LIST拒绝接受的文件类型

-D,–domains=LIST可以接受的域名

–exclude-domains=LIST拒绝的域名

-L,–relative 下载关联链接

–follow-ftp 只下载FTP链接

-H,–span-hosts 可以下载外面的主机

-I,–include-directories=LIST允许的目录

-X,–exclude-directories=LIST 拒绝的目录

中文文档名在平常的情况下会被编码， 但是在 –cut-dirs 时又是正常的，

wget -r -np -nH –cut-dirs=3 ftp://host/test/

测试.txt

wget -r -np -nH -nd ftp://host/test/

%B4%FA%B8%D5.txt

wget “ftp://host/test/\*”

%B4%FA%B8%D5.txt

由 於不知名的原因，可能是为了避开特殊档名， wget 会自动将抓取档名的部分用 encode\_string 处理过， 所以该 patch 就把被 encode\_string 处理成 “%3A” 这种东西， 用 decode\_string 还原成 “:”，并套用在目录与档案名称的部分，decode\_string 是 wget 内建的函式。

wget -t0 -c -nH -x -np -b -m -P /home/sunny/NOD32view/ http://downloads1.kaspersky-labs.com/bases/ -o wget.log

参考：<http://www.jb51.net/LINUXjishu/86326.html>