東北大學秦皇島分校
Northeastern University at Qinhuangdao

Linux操作系统与内核分析

-- Linux基本命令

于七龙

目录

Part 1 Linux基础命令

Linux命令格式

- 常见Linux命令格式如下

命令名称 [命令参数] [命令对象]

- 命令名称、命令参数、命令对象间**以空格间隔**
- 命令参数普遍以“-”或“--”作为前缀
- 命令对象一般指需要处理的文件、目录、用户等资源
- 命令参数分为长格式与短格式
  - 长格式：ls --all
  - 短格式：ls -a

tips

长格式不能合并，短格式参数可合并，如：ls -al

man命令

- 功能：查看命令帮助信息
- 格式：man [参数] [命令名]，如：man man
- 常用快捷键

快捷键	功能
空格、Page down / Page up	后一页 /上一页
Home / End	首页 / 尾页
/ 或 ?	从上往下搜索 / 从下往上搜索
n / N	下一个搜索结果 / 上一个搜索结果
q	退出帮助文档

- 其它帮助命令：info、 -h / --help

cd命令

- 功能：切换工作路径
- 格式：cd [目录路径]，如：cd /
- 常用参数

命令	功能
cd ..	进入上级目录
cd -	返回上次所在目录
cd ~	进入当前用户的home目录
cd ~用户名	进入指定用户的home目录

pwd命令

- 功能：显示当前所在工作目录
- 格式：pwd

ls命令

- 功能：查看目录内容
- 格式：ls [参数]... [目录名称]...
  - 如：ls -ls /etc
- 常用参数

命令	功能
ls -a	查看所有文件（包含隐藏文件）
ls -l	列出详细信息
ls -d	列出目录信息

Linux目录结构

- Linux是典型的树形文件结构

目录	说明	目录	说明
/	根目录，一切路径的起点	/etc	配置文件
/bin	可执行文件，如用户命令	/var	可变文件
/dev	设备文件	/home	普通用户home目录
/lib	库文件，内核模块文件	/root	root用户home目录
/proc	虚拟文件系统，内核映射文件	/opt	第三方软件
/sys	虚拟文件系统，设备相关映射文件	/sbin	重要的系统执行文件
/usr	继承于UNIX，存放程序与相关数据		
/boot	系统启动相关文件		

Part 2 Linux文件管理

mkdir命令

- 功能：新建目录
- 格式：mkdir [参数]… 目录名…
  - 如：mkdir /test
- 常用参数

参数	功能	示例
–p	递归创建目录	mkdir –p /a/b/c

touch命令

- 功能：修改文件时间戳，**但常用于新建空白文本文件**
- 创建文本文件格式：touch 文件名
- 设置文件时间格式：touch 参数 时间 文件名
- 常见参数

参数	功能
-a	修改“最近读取时间（atime）”
-m	修改“修改时间（mtime）”
-d	同时修改“读取时间”和“修改时间”

rm命令

- 功能：删除文件或目录
- 格式：rm [参数]... [文件]...
- 常用参数

参数	功能
-f	忽略提示，强制删除
-r	递归删除目录及目录内内容

cat命令

- 功能：查看文本文件内容
- 格式：cat [参数]... [文件]...
- 常用参数

参数	功能	示例
-n	**显示行号**	**cat -n /etc/ssh/ssh_config：查看/etc/ssh/ssh_config文件内容**
-b	显示行号（跳过无内容行）	cat -b /etc/ssh/ssh_config：查看/etc/ssh/ssh_config文件内容

more命令

- 功能：按窗口大小分页查看文本文件内容
- 格式：more [参数] 文件...

tips

与more命令相似有less命令，坊间常云：less is more

head命令

- 功能：查看文本文件的前N行（默认N=10）
- 格式：head [参数]... [文件]...
- 常用参数

参数	功能	示例
-n N	显示前N行	head -n 5 /etc/ssh/ssh_config : 查看/etc/ssh/ssh_config文件前5行内容

tail命令

- 功能：查看文本文件的最后N行（默认N=10）
- 格式：head [参数]... [文件] ...
- 常用参数

参数	功能	示例
-n X	显示后X行	tail -n 5 /etc/ssh/ssh_config : 查看/etc/ssh/ssh_config文件最后5行内容
-f	持续刷新文件内容	tail –f tail -f /var/log/kern.log: 持续查看/var/log/kern.log文件后10行内容

cut命令

- 功能：查看文件的指定列
- 格式：cut 参数... [文件]...
- 常用参数

参数	功能	示例
-b	选择指定字节	cut –b 1 /etc/passwd: 查看passwd文件每行第1字节
-c	选择指定字符	cut –c 1-3 /etc/passwd: 查看passwd文件每行第1-3字符
-d	指定分界符	cut -d: -f 1 /etc/passwd: 以：为分界符，查看passwd文件每行第1列
-f	选择指定区域，常与-d连用	cut -d: -f 5- /etc/passwd: 以：为分界符，查看passwd文件每行第5至最后列

wc命令

- 功能：查看文件行数、字数、字节数等信息
- 格式：wc [参数]… [文件]…
- 常用参数

参数	功能	示例
-c	显示字节数	wc –c /etc/ssh/ssh_config: 查看ssh_config文件字节数
-m	显示字符数	
-l	显示行数	wc –l /etc/passwd: 查看passwd文件行数
-w	显示字数	

diff命令

- 功能：按行比较文件间的差异
- 格式：diff [参数]... 文件
- 常用参数

参数	功能	示例
-q(--brief)	查看文件是否相同	diff /etc/passwd /etc/passwd-：查看文件是否相同
-c	查看具体不同的内容	diff –c /etc/passwd /etc/passwd-: 差异的内容(感叹号表示差异行)

stat命令

- 功能：查看文件或文件系统状态
- 格式：stat [参数]… 文件…

- **stat命令实际是以文字格式显示文件的inode内容**
  - Access：Atime，文件内容修改后最近一次访问时间
  - Change：Ctime，最近一次更改文件属性信息时间
  - Modify：Mtime，最近一次修改文件内容时间

file命令

- 功能：查看文件类型
- 格式：file 文件名

find命令

- 功能：在目录层次结构中查找文件
- 格式：find [查找路径] 条件 操作
- 常用参数

参数	功能	示例
-name	**按名称查找**	**find / -name passwd:在所有目录中查找名为passwd的文件**
-user	按所有者查找	find / -user yql:在所有目录中查找所有者为yql的文件
-type b/d/c/p/l/f	按文件类型查找	find /home/yql -type f:在/home/yql目录中查找文本文件
-size	按文件大小查找	find / -size +50KB:在所有目录中查找大于50K的文件

- find命令使用过程中，常配合通配符“*”使用

grep命令

- 功能：搜索文件中的内容
- 格式：grep [参数] 模式 [文件]
- 常用参数

参数	功能	示例
-n	显示行号	grep –n yql /etc/passwd:在passwd文件中查找yql关键字
-v	反向匹配：显示没有关键字的行	grep –nv yql /etc/passwd:在passwd文件中查找yql关键字

tar命令

- 功能：打包（压缩）、解包（解压）文件
- 格式：tar [参数...] [文件...]
- 常用参数

参数	功能	示例
-c	创建打包文件	tar -czvf test.tar.gz /test：将/test目录压缩为test.tar.gz tar -xzvf test.tar.gz –C /test2：将压缩文件解压至/test2目录
-x	解开打包文件	
-z	以gzip格式打包或解包	
-j	以bzip2格式打包或解包	
-v	显示打包或解包过程	
-f	目标文件名	

zip/ unzip命令

- 功能：压缩文件为zip格式 / 解压zip压缩包
- 格式：zip [参数...] [文件...]
- 常用参数

参数	功能	示例
-r	递归操作	zip -r test.zip /test：将/test目录及其子目录压缩为test.zip unzip test.zip –d /test2：将压缩文件解压test2目录
-l	查看压缩文件内容	unzip –l test.zip

Part 3 Linux系统管理

uname命令

- 功能：查看系统信息
- 格式：uname [参数]...
- 常用参数

参数	功能	示例
-a	查看系统所有信息	uname -a

date命令

- 功能：查看、设置系统日期、时间
- 格式：date [参数]… +格式
- 常用参数

参数	功能	参数	功能
-s	设置时间		
%H	小时，24小时制	%j	本年的第几天
%i	小时，12小时制	%Y	年
%M	分钟	%m	月
%S	秒	%d	日
示例	date -s “20210301 8:30:00“ ： 设置指定时间 date “+%Y-%m-%d %H:%M:%S” ： 按指定格式显示时间		

ps命令

- 功能：查看进程状态
- 格式：ps [参数]
- 常用参数

参数	功能	示例
-a	查看所有进程（所有用户）	ps –aux：显示所有用户进程及信息 ps –ef：同上 ps –auxw –-sort=rss：按内存占用情况对进程排序（升序） ps –auxw –-sort=-rss：按内存占用情况对进程排序（降序）
-u	显示用户ID	
-x	除了终端的进程	

ps命令查看进程信息

```
[root@localhost ~]# ps aux | more
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.0 193952  7036 ?        Ss   Mar08   4:12 /usr/lib/systemd/systemd
root          2  0.0  0.0      0     0 ?        S    Mar08   0:02 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    Mar08   2:21 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   Mar08   0:00 [kworker/0:0H]
root          7  0.0  0.0      0     0 ?        S    Mar08   6:54 [migration/0]
```

- 进程信息

USER:启动进程用户　　PID：进程号　　%CPU：CPU占用率　　%MEM：内存占用率

VSZ：占用虚拟内存大小（KB）　　RSS：占用物理内存大小（KB）

TTY：进程建立时所对应的终端（？：不占用终端）

STAT：进程状态（R：运行或在运行队列；S：可中断睡眠；T：被跟踪或停止；Z：僵尸进程；W：无足够内存分页可分配；<：高优先级进程；N：低优先级进程；s：领导进程（有子进程）；D：不可中断（通常是IO）；L：有页在内存中被锁定；l：多线程；+：位于后台的进程组）

START：进程开始时间　　TIME：占用CPU时间　　COMMAND：进程对应命令名

top命令

- 功能：查看系统进程
- 格式：top [参数]...
- 常用参数

参数	功能	示例
-d	指定监控间隔	top –d 5：每5秒刷新
-u | U	指定用户	top -u yql -d 3 -n 5：监控yql用户进程，每3秒刷新，刷新5次后退出
-p	指定pid	
-n	设定监控间隔次数，然后退出	

top命令查看进程信息

```
top - 16:33:21 up  5:29,  3 users,  load average: 0.93, 0.30, 0.14
Tasks: 330 total,   3 running, 327 sleeping,   0 stopped,   0 zombie
%Cpu(s): 32.3 us, 65.5 sy,  0.0 ni,  0.0 id,  0.6 wa,  0.0 hi,  1.6 si,  0.0 st
MiB Mem :   1958.4 total,     67.1 free,    919.3 used,    972.0 buff/cache
MiB Swap:    923.3 total,    908.4 free,     14.8 used.    856.3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  87814 yql       20   0 3046048 177996  82056 R  26.8   8.9   0:05.17 gnome-shell
  87908 yql       20   0  708144  29884  26044 S   8.0   1.5   0:00.34 evolution-calen
     84 root      20   0       0      0      0 S   5.5   0.0   0:01.92 kswapd0
  87931 yql       20   0  682064  29100  25648 S   5.5   1.5   0:00.18 evolution-addre
  87913 geoclue   20   0  362344  12472  10976 S   5.2   0.6   0:00.17 geoclue
```

top命令查看进程信息

- load average：系统负载（3个数值分别为1、5、15 分钟内的平均值，数值越小意味着负载越低）
- %cpu：us:用户空间百分比；sy：内核空间：ni:通过nice值修改过权限的用户空间；id：空闲；wa：IO队列等待时间；hi：硬中断消耗时间；si：软中断消耗时间；st：虚拟机偷取时间。其中，us+sy+ni+id+wa+hi+si+st=100%

pidof命令

- 功能：查看服务对应的进程号
- 格式：pidof [参数]... [服务名]
- 示例
  - pidof sshd

kill命令

- 功能：杀死进程
- 格式：kill [参数]... 进程号...
- 示例：
  - kill 123:杀死123进程
  - kill 123 456 789：杀死123、456、789三个进程
  - kill -9 123：强制删除123进程
  - kill -9 -1：强制删除能删除的所有进程

killall命令

- 功能：通过服务名杀死所有进程
- 格式：killall [参数]... 进程号...
- 示例：
  - killall sshd：杀死sshd服务的所有进程

free命令

- 功能：查看内存使用信息
- 格式：free [参数]
- 示例：
  - free
  - free –k ： 设定单位为Kb
  - free –m
  - free –g
  - free –h：人性化显示

tips

不同参数可能会显示不太准确，平时使用中应根据实际情况注意单位的选择

uptime命令

- 功能：查看系统运行信息
- 格式：uptime [参数]
- 示例
  - uptime：查看系统运行信息

who、whoami、last命令

- 功能：查看登录主机的用户、查看当前用户、查看登录记录
- 格式：who、whoami、last

history命令

- 功能：查看当前用户执行过的命令
- 格式：history [参数]...
- 示例
  - history : 查看历史命令
  - history –c : 删除历史记录

tips

- 历史命令保存于用户home目录中的.bash_history文件中
- “！编码数字” 可用于执行历史命令

ifconfig命令

- 功能：查看网卡信息、设置网卡
- 格式：ifconfig [参数]... [内容]
- 示例
  - ifconfig : 查看网卡信息
  - ifconfig -v ens33 192.168.254.188/24 : 设置IP地址
  - ifconfig ens33 down/up：禁用网卡/激活网卡

tips

ifconfig命令设置IP为临时有效，网卡重启后恢复

网卡配置

- 功能：配置IP获取方式、IP等网络参数
- 方法
  - 修改配置文件（不同发行版配置文件有差异）
    - Ubuntu: /etc/netplan/***.yaml
    - RHEL: /etc/sysconfig/network-scripts/ifcfg-***
  - 图形化界面配置
    - nmtui
    - setup

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens32"
UUID="4e30d98a-5e85-4619-90d4-6feaea91c9e3"
DEVICE="ens32"
ONBOOT="yes"
IPADDR="202.206.20.12"
PREFIX="24"
GATEWAY="202.206.20.1"
DNS1="202.206.16.2"
IPV6_PRIVACY="no"
```

修改网卡配置文件

systemctl命令

- 功能：控制系统服务
- 格式：systemctl [参数...] 命令 [单元...]

命令	功能
systemctl status sshd	查看sshd服务状态
systemctl start sshd	启动sshd服务
systemctl stop sshd	停止sshd服务
systemctl restart sshd	重启sshd服务
systemctl enable sshd	设置sshd服务开机启动
systemctl disable sshd	设置sshd服务开机不启动
systemctl list-unit-files	查看开机启动项

tips

如果不知道服务名，可通过“/etc/init.d/服务名 命令”方式控制

reboot、halt、shutdown、powoff命令

- 功能：重启、关闭系统
- 示例

命令	功能
reboot	重启系统
halt	关闭系统（不关闭电源）
halt -p	关闭系统，并关闭电源
halt --reboot	重启系统
shutdown –h 5	5五分钟后关机，并关闭电源
poweroff	关闭系统与电源

tips

Reboot用于重启，halt用于挂起；shutdown用于计划任务；poweroff用于关机

crontab命令

- 功能：计划任务
- 格式：crontab [参数]
- 常用参数

参数	功能	示例
-l	查看计划任务	crontab –l: 查看计划任务
-e	编辑计划任务	0 0 * * * /sbin/service httpd restart：每天0点重启httpd服务
-r	删除计划任务	

- 编辑任务通过vi编辑器编辑文件；
- 任务格式：分、时、日、月、星期命令，空字段以“*”占位；

crontab命令

- crontab调用了vi编辑器，控制crond服务
- 格式：分(0-59)、时(0-23)、日(1-31)、月(1-12)、星期(0-6) 命令，空字段以“*”占位，表示“每一单位”

命令	功能
* * * * * /usr/bin/date >> /test/every1min.txt	每分钟执行查询日期并写入文件
*/2 * * * * /usr/bin/date >> /test/every2min.txt	每2分钟执行
30 14 * * * /usr/bin/date >> /test/1430.txt	每天14:30执行
10,20 * * * * /usr/bin/date >> /test/10and20.txt	每小时的第10、20分执行
1-10/2 * * * * /usr/bin/date >> /test/1to10.txt	每小时的第1-10分钟每2分钟执行

tips

- 命令需用绝对路径方式填写
- 使用whereis命令查询绝对路径，如：whereis date

Linux软件安装

- Linux终端中可通过多种方式安装软件

	在线安装		离线安装				
	yum	apt	rpm安装包	源码安装	deb安装包	run安装包	bin安装包
备注	RHEL、CentOS等	Ubuntu等	RHEL、CentOS等	通用	Debian等	通用	根据实际情况

yum、apt命令

- 功能：软件管理
  - yum常用于RHEL系列系统，apt命令常用于Ubuntu等系统
- 格式：yum / apt [参数] [命令] [软件包...]

示例(yum)	示例(apt)	功能
yum install <package_name>	apt install <package_name>	安装软件
yum remove <package_name>	apt remove <package_name>	卸载软件
yum search <keyword>	apt search <keyword>	搜索软件
yum list installed	apt list --installed	查看已安装软件
yum check-update	apt update	列出所有可更新的软件清单命令
yum update	apt upgrade	更新所有软件命令

rpm命令

- 功能：软件管理
  - 由RedHat创立的文件格式(redhat package manager)，现已成为Linux安装包标准之一
- 格式：rpm [参数] [软件包…]

命令	功能
rpm –ivh xxx.rpm	安装软件
rpm –e xxx.rpm	卸载软件
rpm -qa | grep xxx	查询是否安装软件

源码安装

- 功能：利用源代码安装程序
- 安装分为三个步骤
  - 配置(设置安装路径等)：./configure
  - 编译：make
  - 安装：install

tips

- 安装从开源平台下载的源码程序时，常用本安装方式

run安装包、bin安装包

- 功能：利用run或bin安装包安装程序
- run与bin安装包在源码安装基础上简化了安装流程
  - run和bin安装包是将shell脚本和zip、rpm等软件包打包，实际安装过程是脚本解压安装包并安装

Part 4 管道、vi编辑器

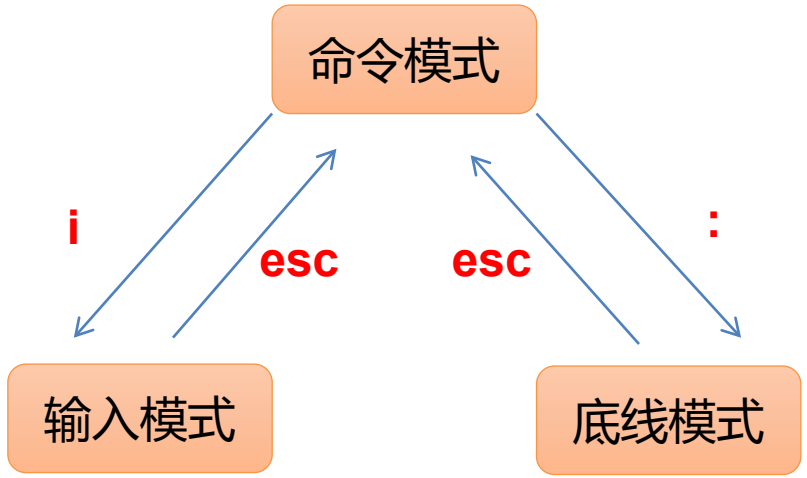
管道

- 功能：将上一个命令的输出作为后一个命令的输入
- 格式：命令1 | 命令2 ...

命令	功能
cat /etc/passwd | more	分页查看文件
systemctl list-unit-files | grep enabled	查看开机启动的服务

vi命令

- 功能：编辑文本文件
- 格式：vi 文件
- vi编辑器有3中模式



  - 命令模式(Command mode)：可查看、复制、粘贴、搜索，但不能编辑文本
  - 输入模式(Insert mode)：编辑文本
  - 底线模式(Last line mode)：保存或退出

vi命令

- 命令模式常用快捷键

快捷键	功能
yy	复制光标所在行
2yy	复制光标所在行开始2行
dd	剪切（删除）光标所在行
2dd	剪切（删除）光标所在行开始2行
p	粘贴yy或dd的内容
/关键字	从 上往下搜索
？关键字	从下往上搜索
n	定位搜索到的下一个内容
N	定位搜索到的上一个内容

vi命令

- 底线模式常用快捷键

快捷键	功能
:wq!	保存并退出
:w	保存
:q!	强制退出(不保存)
:set nu	显示行号
:set nonu	不显示行号
:行号	跳转到指定行

Part 5 Linux用户与权限

useradd命令

- 功能：新建用户
- 格式：useradd [参数] 用户名

示例	功能
useradd yql	创建yql用户
useradd –m yql	创建yql用户并新建home目录

tips

- 新建用户另外有adduser命令

passwd命令

- 功能：设置用户密码
- 格式：passwd [参数] [用户名]

示例	功能
passwd	修改当前用户密码
passwd yql	设置/修改yql用户的密码

tips

- Linux中，输入密码不显示，输入结束直接Enter

userdel命令

- 功能：删除用户
- 格式：useradd [参数] 用户名

示例	功能
userdel yql	删除yql用户
userdel –r yql	删除yql及用户home目录

tips

- 实际使用中，建议删除用户时，用户数据手动删除

id命令

- 功能：查看用户ID等信息
- 格式：id [参数] [用户名]
- id命令显示内容分为3部分
  - uid：用户ID
  - gid/groups：用户组
  - 其它：扩展组

tips

- uid一般有默认范围，如uid=0为**root用户**，1-999为**系统用户**，1000+为**普通用户**

示例	功能
id	查看当前用户信息
Id yql	查看yql用户信息

groupadd命令

- 功能：添加用户组
- 格式：groupadd [参数] 组名

示例	功能
groupadd yu	添加用户组yu

Linux文件权限

- 查看文件权限：ls –l [文件名]

```
[root@localhost /]# ll
total 32
lrwxrwxrwx.   1 root root    7 Mar  8 10:56 bin -> usr/bin
dr-xr-xr-x.   5 root root 4096 Mar  8 11:17 boot
drwxr-xr-x.   2 root root   59 May  3 22:17 code
```

文件权限

- **关键字段解读（以上图中code目录为例）**
  - d：文件类型，l(链接文件)、d(目录)、-(文本文件)
  - **rwxr-xr-x：文件权限**
  - 1：硬链接数
  - root：文件所有者
  - root：文件所有者所在组
  - 59：文件大小

文件权限解读：

rwxr-xr-x分为3部分：

1，rwx：文件所有者权限，可读，可写，可执行；

2，r-x：文件所有者同组用户权限，可读，可执行，不可写；

3，r-x：其它用户权限，可读，可执行，不可写；

chmod命令

- 功能：修改文件权限
- 格式：chmod [参数] 模式 文件名
- **权限表示方法**
  - **r：4**
  - **w：2**
  - **x：1**

示例	功能
chmod 755 /test/haha.txt	设置/test/haha.txt文件除文件所有者以外其它所有用户均不可写
chmod 777 /test/haha.txt	设置所有用户可读、可写、可执行
chmod -R 770 /test/	设置其它用户不可访问，所有者及同组用户所有权限

chown命令

- 功能：修改文件所有者或组
- 格式：chown [参数] [所有者]:[组] 文件名...

示例	功能
chown yql:yql /test/haha.txt	设置/test/haha.txt文件所有者和组名均为yql
chown -R root:yql /test/	设置/test目录及其子文件文件所有者为root，组为yql

usermod命令

- 功能：修改用户账户属性
- 格式：usermod [参数] 用户

示例	功能
usermod –g yql yql2	设置yql2用户组名为yql组
usermod –aG sudo yql	将yql用户追加至sudo组

su命令

- 功能：切换用户
- 格式：su [参数] 用户

示例	功能
su root	从当前用户切换至root用户
su – root	彻底切换到root用户，即把环境变量等信息也进行变更

Part 6 iptables

Linux防火墙

- 系统防火墙是系统与网络间的屏障，用于保护系统与数据的安全
- 不同Linux发行版有不同的防火墙服务
  - RHEL/CentOS：Firewalld
  - Ubuntu：UFW
- 不同Linux发行版虽具有不同的防火墙服务程序，但普遍基于iptables实现

iptables

- iptables是Linux系统中定义防火墙策略的管理工具，定义的规则由内核中的netfilter网络过滤器实现
- iptables具有以下功能
  - 处理路由选择前的数据包（PREROUTING）
  - **处理流入的数据包（INPUT）**
  - 处理流出的数据包（OUTPUT）
  - 处理转发的数据包（FORWARD）
  - 处理路由选择后的数据包（POSTROUTING）

iptables

- iptables可通过 源IP、目的IP、协议、端口、服务类型等进行匹配

参数	功能	示例
-L	查看规则	iptables -L
-F	清空规则	iptables -F
-P	恢复默认规则	iptables -P
-A	在规则末尾追加规则	
-I [num]	在第num条规则前插入规则	
-D num	删除第num条规则	
-s / -d	匹配源IP / 目的IP，！表示排除	
-p 协议	匹配协议	
-i / -o 网卡	匹配指定网卡 下行 / 上行数据	
--sport / --dport num	匹配 源端口 / 目的端口	

iptables

- iptables可通过 源IP、目的IP、协议、端口、服务类型等进行匹配

示例	功能
iptables -A INPUT -p icmp -j REJECT	拒绝流入ICMP包
iptables -A INPUT -p icmp -j DROP	丢弃流入ICMP包
iptables -I INPUT -s 192.168.10.0/24 -p tcp --dport 22 –j ACCEPT	只允许指定网段的主机访问本机的22 端口
iptables -A INPUT -p tcp --dport 10:100 -j REJECT	拒绝所有主机访问10-100端口

- **编辑iptables后需保存，否则重启系统后失效**
  - **iptables-save**

iptables

- 防火墙策略按照从上往下顺序匹配
  - 允许动作在前，拒绝动作在后
  - 允许动作用“-I”，拒绝动作用“-A”

```
iptables -I INPUT DROP
iptables -A INPUT -p icmp -j ACCEPT
```

```
iptables -A INPUT DROP
iptables -I INPUT -p icmp -j ACCEPT
```