==============================================================

**关闭CentOS7防火墙**

# 查看防火墙状态
firewall-cmd --state
# 停止firewall
systemctl stop firewalld.service
# 禁止firewall开机启动
systemctl disable firewalld.service

开启端口

添加端口：firewall-cmd --zone=public --add-port=8081/tcp --permanent

生效：firewall-cmd --reload

firewall-cmd --zone=public --list-ports（查看通过的端口）

重启防火墙：

systemctl restart firewalld.service

关闭防火墙：

systemctl stop firewalld.service

**关闭SELINUX**

# 编辑SELINUX文件
vim /etc/selinux/config
# 将SELINUX=enforcing改为SELINUX=disabled

**清除和关闭iptables**

# 清空iptables规则

iptables -F 清除预设表filter中的所有规则链的规则

iptables -X 清除预设表filter中使用者自定链中的规则

iptables -Z

**iptables**

iptables命令是Linux上常用的防火墙软件，是netfilter项目的一部分。可以直接配置，也可以通过许多前端和图形界面配置。

iptables -t 表名 <-A/I/D/R> 规则链名 [规则号] <-i/o 网卡名> -p 协议名 <-s 源IP/源子网> --sport 源端口 <-d 目标IP/目标子网> --dport 目标端口 -j 动作

--------------------------------

表名包括：

raw：高级功能，如：网址过滤。

mangle：数据包修改（QOS），用于实现服务质量。

net：地址转换，用于网关路由器。

filter：包过滤，用于防火墙规则。

-------------------------------

规则链名包括：

INPUT链：处理输入数据包。

OUTPUT链：处理输出数据包。

PORWARD链：处理转发数据包。

PREROUTING链：用于目标地址转换（DNAT）。

POSTOUTING链：用于源地址转换（SNAT）。

-------------------------------

动作包括：

accept：接收数据包。

DROP：丢弃数据包。

REDIRECT：重定向、映射、透明代理。

SNAT：源地址转换。

DNAT：目标地址转换。

MASQUERADE：IP伪装（NAT），用于ADSL。

LOG：日志记录。

-------------------------------

iptables -A INPUT -p tcp --dport 1801 -j ACCEPT #允许访问22端k

iptables -A OUTPUT -j ACCEPT #允许所有本机向外的访问

iptables -A INPUT -j reject #禁止其他未允许的规则访问

iptables -L -n -v #查看规则

-------------------------------

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

-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：

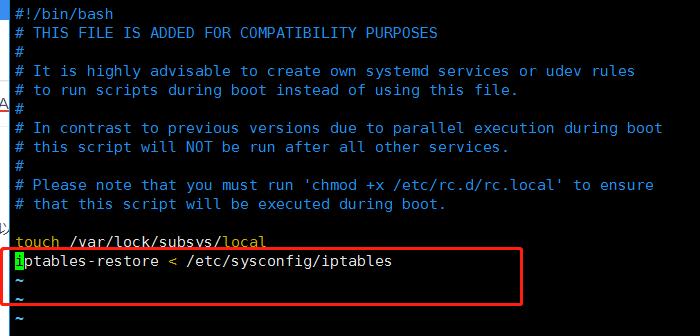
iptables -P INPUT DROP 这就把默认规则给拒绝了。并且没有定义哪个动作，所以关于外界连接的所有规则包括Xshell连接之类的，远程连接都被拒绝了

service iptables save 保存配置文件

iptables-restore < /etc/sysconfig/iptables 读取配置文件

设置开机启动读取配置文件

[root@Docker ~]# vim /etc/rc.local



**2.配置文件说明**

firewalld 存放配置文件有两个目录，/usr/lib/firewalld 和 /etc/firewalld，前者存放了一些默认的文件，后者主要是存放用户自定义的数据，所以我们添加的service或者rule都在后者下面进行。

server 文件夹存储服务数据，就是一组定义好的规则。

zones 存储区域规则

firewalld.conf 默认配置文件，可以设置默认使用的区域，默认区域为 public，对应 zones目录下的 public.xml

**三.命令**

这里需要首先说明的是，在执行命令时，如果没有带 --permanent 参数表示配置立即生效，但是不会对该配置进行存储，相当于重启服务器就会丢失。如果带上则会将配置存储到配置文件，，但是这种仅仅是将配置存储到文件，却并不会实时生效，需要执行 firewall-cmd --reload 命令重载配置才会生效。

**1.重载防火墙配置**

firewall-cmd --reload

**2.查看防火墙运行状态**

firewall-cmd --state

**3.查看默认区域的设置**

firewall-cmd --list-all

**4.应急命令**

firewall-cmd --panic-on # 拒绝所有流量，远程连接会立即断开，只有本地能登陆
firewall-cmd --panic-off # 取消应急模式，但需要重启firewalld后才可以远程ssh
firewall-cmd --query-panic # 查看是否为应急模式

**5.服务**

firewall-cmd --add-service=<service name> #添加服务
firewall-cmd --remove-service=<service name> #移除服务

**6.端口**

firewall-cmd --add-port=<port>/<protocol> #添加端口/协议（TCP/UDP）
firewall-cmd --remove-port=<port>/<protocol> #移除端口/协议（TCP/UDP）
firewall-cmd --list-ports #查看开放的端口

**7.协议**

firewall-cmd --add-protocol=<protocol> # 允许协议 (例：icmp，即允许ping)
firewall-cmd --remove-protocol=<protocol> # 取消协议
firewall-cmd --list-protocols # 查看允许的协议

**8.允许指定ip的所有流量**

firewall-cmd --add-rich-rule="rule family="ipv4" source address="<ip>" accept"

例：

firewall-cmd --add-rich-rule="rule family="ipv4" source address="192.168.2.1" accept" # 表示允许来自192.168.2.1的所有流量

**9.允许指定ip的指定协议**

firewall-cmd --add-rich-rule="rule family="ipv4" source address="<ip>" protocol value="<protocol>" accept"

例：

firewall-cmd --add-rich-rule="rule family="ipv4" source address="192.168.2.208" protocol value="icmp" accept" # 允许192.168.2.208主机的icmp协议，即允许192.168.2.208主机ping

**10.允许指定ip访问指定服务**

firewall-cmd --add-rich-rule="rule family="ipv4" source address="<ip>" service name="<service name>" accept"

例：

firewall-cmd --add-rich-rule="rule family="ipv4" source address="192.168.2.208" service name="ssh" accept" # 允许192.168.2.208主机访问ssh服务

**11.允许指定ip访问指定端口**

firewall-cmd --add-rich-rule="rule family="ipv4" source address="<ip>" port protocol="<port protocol>" port="<port>" accept"

例：

firewall-cmd --add-rich-rule="rule family="ipv4" source address="192.168.2.1" port protocol="tcp" port="22" accept" # 允许192.168.2.1主机访问22端口

**12.将指定ip改为网段**

8-11 的各个命令都支持 source address 设置为网段，即这个网段的ip都是适配这个规则：

例如：

firewall-cmd --zone=drop --add-rich-rule="rule family="ipv4" source address="192.168.2.0/24" port protocol="tcp" port="22" accept"

表示允许192.168.2.0/24网段的主机访问22端口 。

**13.禁止指定ip/网段**

8-12 各个命令中，将 accept 设置为 reject表示拒绝，设置为 drop表示直接丢弃（会返回timeout连接超时）

例如：

firewall-cmd --zone=drop --add-rich-rule="rule family="ipv4" source address="192.168.2.0/24" port protocol="tcp" port="22" reject"

表示禁止192.168.2.0/24网段的主机访问22端口 。

====================================================================================================================================================

liunx命令大全：http://man.linuxde.net/

常用命令：

ls：列出当前目录的文件

pwd：显示当前目录

hash：缓存记录

cd：切换目录

cd - 在当前目录和前一次所在的目录进行切换

printenv:显示环境变量

查看内核：uname -a

查看历史命令：history

清屏：reset

查看连服务器：who

ps #查看当前终端活跃进程

ps -aux | aux #查看所有进程, -a 所有进程, -u 进程拥有者, -x 守护进程

top #实时查看系统进程资源占用情况

netstat -anp 查看网络统计信息

===============================================================

**crond系统定时任务**

crontab 参数 -e：编辑crontab 定时任务

-l :查询crontab 任务

-r:删除当前用户所有的crontab任务

\* \* \* \* \*

第一个\*:表示分，第二个\*:表示时，第三个:表示天，第一个\*:表示月，第五个\*:表示周

重启crond服务管理器：service crond restart

========================================================================

rpm -qa 查询系统安装的软件

rpm -e 卸载软件

rpm -ivh 安装软件

查看监听(Listen)的端口

netstat -lntp

查看端口使用的进程

lsof -i:端口号

检查端口被哪个进程占用

netstat -lnp|grep 8080

查看进程占用那个端口

netstat -nap | grep 9836

命令类型：

内置命令（shell内置）

外部命令：在文件系统的某个路径下有一个与命令名称相应的可执行文件

环境变量：命名的内存空间

PATH：使用冒号分开的路径

文件类型：

文件权限：9位，没3位一组，每组：rwx（读，写，执行），r--

文件硬连接的次数

文件的属主(owner)

文件的属组（group）

文件大小（size），单位是字节

时间数（timeatamp）：最近一次被修改的时间

访问：access

修改：modify 文件内容发生了改变

改变：change，metadata 元数据

yum -y install lrzsz 安装rz命令上传。

yum install net-tools 安装ifconfig命令

yum install tree 安装tree命令

yum install wget 安装wget 命令

yum install vim\* 安装vim命令

时间同步

1.  安装ntpdate工具

# yum -y install ntp ntpdate

2.  设置系统时间与网络时间同步

# ntpdate cn.pool.ntp.org

3.  将系统时间写入硬件时间

# hwclock --systohc

文件格式转换

set ff=unix

将数据由内存同步到磁盘:sync

关机：halt

重启：reboot

定时关机：shutdown -r 时间 " 1 minute reboot "

找回root密码：

远程登入：

修改用户权限

修改 /etc/sudoers

**查看文件内容**

cat :第一行开始显示 -n 显示行号。-A显示特殊符号

tac：从最后一行开始显示

more：一页一页显示

less：/ 子串，向下搜寻的功能；n：向下查找，N：向上查找

head：只看头几行

tail：只看尾几行

**日志**

/var/log/messages 大多数系统日志消息记录在此处.例外是与身份验证, 电子邮件处理相关的定期运行作业的消息以及纯粹与调试相关的消息

/var/log/secure 安全和身份验证相关的消息和错误的日志文件

/var/log/maillog 与邮件服务器相关的日志文件

/var/log/cron 与定期执行任务相关的日志文件

/var/log/boot.log 与系统启动相关的消息记录在此处

**liunx 目录结构**

辅助命令: tree -df -L 1 /

/ -根

├── /bin -存放系统执行文件

├── /boot -存放启动引导程序

├── /cdrom -光驱

├── /dev -计算机设备

├── /etc -存放系统相关服务的配置文件, 默认

├── /home -普通用户家目录

├── /lib -存放系统库文件

├── /lost+found -存放意外丢失的文件

├── /media -挂载目录

├── /mnt -早期的挂载目录

├── /opt -一些rpm安装后的文件的存放目录

├── /proc -进程

├── /root -root家目录

├── /run -运行时的文件例如程序的pid文件

├── /sbin -存放仅管理员能够使用的命令

├── /srv -服务

├── /sys -系统

├── /tmp -临时文件夹

├── /usr -存放用户安装程序

└── /var -存放log、数据库数据文件、网站的默认位置

**最小安装**

**修改网络信息**

**1、先把我们的ip地址设置为静态ip地址。**

TYPE="Ethernet"

PROXY\_METHOD="none"

BROWSER\_ONLY="no"

BOOTPROTO="static" # 使用静态IP地址，默认为dhcp【修改】

IPADDR="192.168.14.18" # 设置的静态IP地址【修改】

NETMASK="255.255.255.0" # 子网掩码【修改】

GATEWAY="192.168.14.1" # 网关地址【修改】

DNS1="114.114.114.114" # DNS服务器【修改】

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="ens33"

UUID="7ce8dd59-cbaa-4b0f-bfe4-b3d938bfc148"

DEVICE="ens33"

ONBOOT="yes"

**4.重启网络服务**

　　执行命令：

　　service network restart 　或 　 systemctl restart network

**5、启用ifconfig 命令**

依赖于 net-tools 软件

# yum install -y net-tools

输入#ifconfig ，

**6、CentOS自带vi编辑器，功能没有vim强大，我么再安装一个vim编辑器**

# yum install -y vim-enhanced

**7、CentOS7最小化安装后没有wget软件，但是以后我们会经常用到这个组件，所以我们安装一下**

# yum install -y wget

**8、CentOS自带的国外源有时候会很慢，替换成国内的阿里源**

先进入源的目录

#cd /etc/yum.repos.d

备份一下官方源

#mv CentOS-Base.repo CentOS-Base.repo.bak

将阿里源文件下载下来

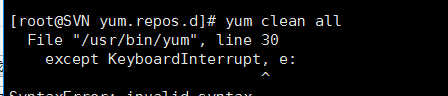
#wget -O /etc/yum.repos.d/CentOS-Base.repo <http://mirrors.aliyun.com/repo/Centos-7.repo>

重建源数据缓存

# yum clean all

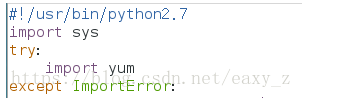
#yum makecache

错误提示

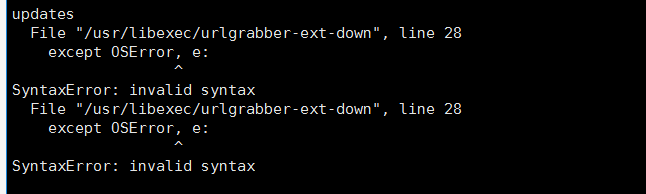


解决办法

修改/usr/bin/yum文件中的第一行为#!/usr/bin/python2.7



错误提示



# vi /usr/libexec/urlgrabber-ext-down

将第一行"#!/usr/bin/python" 改为 "#!/usr/bin/python2.7"即可。

5.内存情况

[root@localhost ~]# cat /proc/meminfo | head -4

4.查看cpu信息

[root@localhost ~]# cat /proc/cpuinfo | grep name

2.查看系统版本

[root@localhost ~]# rpm -q centos-release

3.磁盘分区和使用情况  #注意默认分区情况下，大分区会被分在/home目录下，装软件的时候要注意装在/home目录下

[root@localhost ~]# df -h

1.查看系统位数、内核版本

[root@localhost ~]# uname -a

========================================================================================

[**CentOS7 监控网络流量**](https://www.cnblogs.com/heqiuyong/p/11123646.html)

首先，以下介绍的流量监控工具安装之前均需要安装epel源，

安装epel源：

[root@bogon ~]# yum -y install epel-release

安装 iftop 工具，查看各个连接的流量情况

[root@bogon ~]# yum -y install iftop

[root@bogon ~]# iftop -i ens33 -n -P

或安装 tcptrack 工具，查看各个连接的流量情况

[root@bogon ~]# yum install -y libpcap-devel libpcap

[root@bogon ~]# wget http://packages.psychotic.ninja/6/base/x86\_64/RPMS/tcptrack-1.4.2-9.el6.psychotic.x86\_64.rpm

[root@bogon ~]# rpm -ivh tcptrack-1.4.2-9.el6.psychotic.x86\_64.rpm

[root@bogon ~]# tcptrack -i ens33

或安装 nethogs 工具，查看各个进程的流量情况

[root@bogon ~]# yum -y install nethogs

[root@bogon ~]# nethogs

 或安装 nload 工具，查看总体流量趋势情况

[root@bogon ~]# yum -y install nload

[root@bogon ~]# nload