目录：

[**1、远程连接Linux系统管理** 1](#_Toc418499242)

1.1SSH远程连接介绍 1

1.2SSH服务端介绍 1

1.3SSH客户端介绍 1

1.4SSH的协议介绍 2

1.5ssh远程连接故障排查 3

**2、添加linux普通用户账户** [4](#_Toc418499243)

2.1添加普通用户账户 4

2.2linux系统中三类用户角色 5

**3、安装Linux系统后调优及安全设置** [5](#_Toc418499243)

3.1关闭SELinux功能 6

3.2Linux7种运行级别 7

3.2.1Linux中的7种模式 8

3.2.2设定运行级别为3（文本模式） 8

3.3精简开机系统启动 8

3.3.1重要的开机自启动服务 9

3.3.2设置开机自启动服务的常见方法 10

3.4关闭iptables防火墙 11

3.5 Linux系统安全最小原则说明 11

3.6更改ssh服务端远程登录的配置 12

3.7利用sudo控制用户对系统命令的使用权限 14

3.8Linux中文显示设置 17

3.9设置Linux服务器时间同步 18

3.10历史记录及登录超时环境变量设置 18

3.11加大服务器文件描述符 18

[**4、课前考试题总结** 19](#_Toc418499244)

1. **远程连接linux系统管理**

**1.1 SSH远程连接介绍**

当前，在几乎所有的互联网企业环境中，最常用的Linux提供远程连接服务的工具就是SSH软件，SSH分为客户端和SSH服务端两部分。其中SSH服务端包含的软件程序主要有openssh和openssl，在linux系统中可以按如下方法查询SSH服务端工具的安装情况。

[oldboy@C66-moban ~]$ rpm -q openssh openssl

openssh-5.3p1-104.el6.x86\_64

openssl-1.0.1e-30.el6.x86\_64

提示：openssh是提供SSH服务的程序，openssl是为SSH提供连接加密的程序。

[root@moban ~]# /etc/init.d/sshd status

openssh-daemon (pid 1577) is running...

检查ssh是否运行。

**1.2 SSH服务端介绍**

启动linux系统时，默认情况下，SSH服务端程序就会随系统一起启动，SSH服务是一个守护进程（demon），它在系统后台永久运行并时刻响应来自所有SSH客户端的连接请求。SSH服务端的进程名为sshd，负责实时监听远程SSH客户端的连接请求并进行处理，这些请求一般包括公共密钥认证、密钥交换、对称密钥加密和非安全连接等。SSH服务是系统优化时需要保留开机自启动的服务之一。

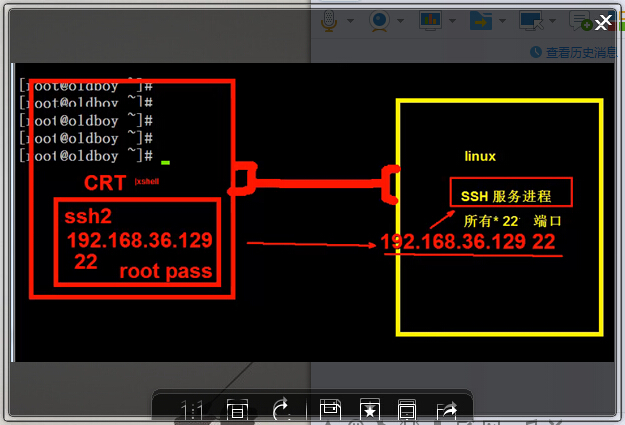
**1.3 SSH客户端介绍**

SSH客户端最常用的工具就是windows平台的secureCRT了，该工具安装很简单，按提示一步步操作即可，运行就可以使用，除CRT软件之外，还有xshell、putty等常用软件以及Linux下的ssh客户端。

**1.4 SSH的协议介绍**

SSH协议是secure shell protocol的简写，由IETF网络工作小组（network working group）制定，在进行数据传输之前，ssh先通过加密技术对联机数据包进行加密处理，然后再进行数据传输，这样就可确保传递数据的安全。SSH是专为远程登录会话和其他网络服务提供的安全性协议，利用SSH协议可以有效地防止远程管理过程中的信息被泄露，在当前的生产环境中，绝大多数企业普遍采用SSH协议服务来代理传统的不安全的远程联机服务软件，如Telnet（23端口，非加密的）等。

SSH的两个不兼容的版本，SSHv1、SSHv2。



查看ssh端口命令：

[root@oldboy ~]# /etc/init.d/sshd status

openssh-daemon (pid 1562) is running...

[root@oldboy ~]# ss -lntup|grep ssh

tcp LISTEN 0 128 :::22 :::\* users:(("sshd",1562,4))

tcp LISTEN 0 128 \*:22 \*:\* users:(("sshd",1562,3))

[root@oldboy ~]# netstat -lntup|grep ssh

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 1562/sshd

tcp 0 0 :::22 :::\* LISTEN 1562/sshd

**1.5 ssh远程连接故障排查**

1. Ping

ping Linux 10.0.0.8 检查路通不通（手机有信号），网络是否通畅。

正确的结果：

Microsoft Windows [版本 6.1.7601]

版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.USER-20150311FQ>ping 10.0.0.8

正在 Ping 10.0.0.8 具有 32 字节的数据:

来自 10.0.0.8 的回复: 字节=32 时间<1ms TTL=64

错误的结果：

C:\Users\Administrator.USER-20150311FQ>ping 10.0.0.7

正在 Ping 10.0.0.7 具有 32 字节的数据:

来自 10.0.0.1 的回复: 无法访问目标主机。

请求超时。

1. telnet与nmap （退出Ctrl+]quit）

Telnet 10.0.0.8 22 （服务功能是否开放）如果是Linux系统也可使用（nmap 10.0.0.7 -p 22）

正确：

connected.....

错误：

connection refused 防火墙iptables或服务功能没开。

NO ROUTE TO HOST 防火墙问题。

关闭防火墙命令：/etc/init.d/iptables stop

1. **添加linux普通用户账户**

**2.1 添加普通用户账户**

Linux是一个多任务、多进程、多CPU、多用户的操作系统，一般情况下，在企业生产环境中应尽量避免直接到root用户下操作，除非有系统维护需求。

可使用如下命令添加一个普通用户账户，并为其设置口令：

添加用户：

[root@moban ~]# useradd oldboy

查看用户是否已添加：

方法1、

[root@moban ~]# id oldboy

uid=500(oldboy) gid=500(oldboy) groups=500(oldboy)

方法2、

[root@moban ~]# tail -l /etc/passwd

给用户添加密码：

[root@moban ~]# passwd oldboy

Changing password for user oldboy.（更改用户 oldboy 的密码 。）

New password: (新的密码)

BAD PASSWORD: it is too simplistic/systematic （无效的密码： 过于简单化/系统化）

BAD PASSWORD: is too simple （无效的密码： 过于简单）

Retype new password: （重新输入新的 密码：）

passwd: all authentication tokens updated successfully. （所有的身份验证令牌已经成功更新。）

####注释：直接修改用户密码的命令：echo 123456|passwd --stdin oldboy

**2.2 linux系统中三类用户角色：**

root超级管理员 ====>皇帝

普通用户 ====>公民（皇帝会任命一部分人管理国家）

虚拟用户 ====>傀儡（没有实际用途，为了程序服务启动要求）

切换用户账户：

[root@moban ~]# su - oldboy 《=====root提示符

[oldboy@moban ~]$ 《=====普通用户

查看当前用户

[oldboy@moban ~]$ whoami

Oldboy

####注释：一般生产场景的工作用户都是使用：普通用户。

说明：

1. 超级用户root切换到普通用户下面，无需输入对应用户密码。
2. 普通用户切换到root或其他普通用户下，需要对应用户的密码。
3. 普通用户的权限比较小，只能进行基本的系统信息查看等操作，无法更改系统配置和管理服务。
4. $符号是普通用户的命令行提示符，#符号是超级管理员的提示符。示例如下：

[root@C66-moban ~]# su – oldboy 🡨超级管理员root对应的提示符。

[oldboy@C66-moban ~]$ 🡨普通用户oldboy对应的提示符。

1. 提示符@前面的字符代表当前用户（whoami），后面的为主机名（hostname），~所在的位置是窗口当前的路径。示例如下：

[oldboy@C66-moban ~]$ 🡨oldboy为当前用户，moban为主机名，~表示当前目录（家目录）。

1. Linux命令提示符由PS1环境变量控制，示例如下：

[root@C66-moban ~]# set|grep PS1 注：PS1为大写。

PS1='[\u@\h \W]\$ '，可以通过全局变量配置/etc/profile文件|调整PS1=’[\u@\h \W\t]$’。

1. **安装Linux系统后调优及安全设置**

**3.1 关闭SELinux功能**

SElinux（security-enhanced-Linux）是美国国家安全局（NSA）对于强制访问控制的实现，这个功能让系统管理员又爱又恨，这里考虑还是把它给关闭了吧，至于安全问题，后面通过其他手段来解决。

关闭方式如下：

1. 修改配置文件，使关闭SELinux永久生效：

[root@moban ~]# cp /etc/selinux/config /etc/selinux/config.ori 🡨操作前切记备份

[root@C66-moban~]#sed -i's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config

修改配置文件可使配置永久生效。

[root@C66-moban ~]# grep SELINUX=disabled /etc/selinux/config

SELINUX=disabled 🡨检查替换结果为disabled就表示编辑成功了。

修改配置文件可使配置永久生效，但必须要重启系统，此步时快速修改方法，也可以通过vi编辑修改此文件。

1. 临时关闭SELINUX，可在命令行执行如下命令:

[root@C66-moban ~]# setenforce

usage: setenforce [ Enforcing | Permissive | 1 | 0 ]

[root@C66-moban ~]# setenforce 0 🡨临时将selinux调成permissive状态。

[root@C66-moban ~]# getenforce 🡨查看selinux当前状态。

Permissive （警告不阻止）

数字0表示permissive，即给出警告提示，但不会阻止操作，相当于disabled。

数字1表示enforcing，即表示selinux 为开启状态。

disabled （关闭selinux）

Enforcing （开启状态）

Permissive （警告不阻止）

**selinux小结：**

selinux是什么？

答：是一个安全的工具，但是控制非常严格，所以生产环境中弃用，使用其他的安全手段。

若要永久关闭selinux的命令（若生效需重启系统）：

/etc/selinux/config

<SELINUX=enforcing改为SELINUX=disabled

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

临时关闭selinux的方法：

setenfore 0 (命令行关闭selinux)

查看命令行是否关闭selinux：

getenfore

**3.2 Linux7种运行级别：**

runlevel Linux运行时的一种状态标识，这个标识用数字表示。

**3.2.1 Linux中的7种模式**

# 0 - halt (Do NOT set initdefault to this) 🡨 (关机模式,Linux系统关机状态时就是0模式)

# 1 - Single user mode 🡨 （单用户模式例root密码丢失若找回请选择1单用户模式）

# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)🡨（多用户模式，但是没有网络文件系统NFS，如果不需要网络的话多用户模式和文本模式是一样的）

# 3 - Full multiuser mode 🡨（文本模式，完整、完全的工作模式）

# 4 – unused 🡨（一般不用，在一些特殊情况下可以用它来做一些事情。例如在笔记本电脑的电池用尽时，可以切换到这个模式来做一些设置。）

# 5 - X11 🡨（桌面模式）

# 6 - reboot (Do NOT set initdefault to this) 🡨（重启模式，运行init 6 机器就会重启）

**3.2.2设定运行级别为3（文本模式）**

设定runlevel为3，即表示使用文本命令行模式管理Linux，检查命令如下：

[root@C66-moban ~]# grep 3:initdefault /etc/inittab

id:3:initdefault: 🡨这里的3就是Linux默认的运行级别，如有需求可以将其修改为其他级别，工作中常用3级别，即文本模式。

[root@C66-moban ~]# runlevel 🡨 查看当前系统运行级别。

N 3

命令说明：7种运行级别0-6，具体：cat /etc/inittab

runlevel： 查看当前系统运行级别。

init ： 切换运行级别，后面接对应级别的数字。

例如：init 6 就表示重启

**3.3 精简开机系统启动**

和Windows系统一样，在Linux服务器运行的过程中，也会有很多无用的软件服务默认就在运行，这些服务占用了很多系统资源，而且也带来了安全隐患，因此要关闭掉，那么，企业生产场景的Linux主机到底需要保留哪些开机启动的服务那？

###注释

为什么要设置开机系统启动？

好处：

1、节省开机时间、加快启动速度。

2、节省资源开销。

3、减少安全隐患。

**3．3.1重要的开机自启动服务**

企业环境新装Linux系统后有必要保留的开机自启动服务有5个，具体如下。

1. sshd

远程连接Linux服务器时需要用到这个服务程序，所以必须要开启，否则将无法远程连接到服务器。

1. rsyslog

是操作系统提供的一种机制，系统的守护程序通常会使用rsyslog将各种信息写到各个系统日志文件中，centos以前此服务的名字为syslog。

1. network

系统启动时，若想激活/关闭各个网络接口，则应（必须）考虑开启。

1. crond

该服务用于周期性地执行系统及用户配置的任务计划，有要周期性执行的任务要开启，此服务几乎是生产场景必须要用的一个软件。

1. sysstat

sysstat是一个软件包，包含检测系统性能及效率的一组工具，这些工具对于系统性能数据很有帮助，比如CPU使用率、硬盘和网络吞吐数据等，这些数据的分析，有利于判断系统运行是否正常，所以它是提高系统运行效率、安全运行服务的助手。

Sysstat软件包集成的主要工具为：

iostat工具提供CPU使用率及硬盘吞吐率的数据。

mpstat工具提供与单个或多个处理器相关的数据。

sar工具负责收集、报告并存储系统活跃的信息。

提示：上述5个服务是安装完系统后建议保留的开机自启动服务，也几乎是一切必须开机保留的自启动服务，将来还可以根据服务器的业务使用场景调整相应的自启动所谓调整，就是增加其他自启动服务。

**3.3．2 设置开机自启动服务的常见方法**

**（1）执行命令然后手动选择处理方法**

方法1：执行ntsysv 命令然后在弹出的窗口中进行设置。

方法2：执行setup->system service，然后在弹出的窗口中进行设置。

方法3：chkconfig 确保3模式下上述指定的服务开启状态就可以了。

**（2）开机自启动处理命令：**

第一种方法：

LANG=en

chkconfig --list|grep "3:on"|awk '{print $1}'|grep -Ev "sshd|rsyslog|network|crond|sysstat"|sed -r 's#(.\*)#chkconfig \1 off#g'|bash

chkconfig --list|grep "3:on"

第二种方法：

chkconfig --list|grep "3:on"|awk '{print $1}'|grep -Ev "sshd|rsyslog|network|crond|sysstat"|awk '{print "chkconfig " $1 " off"}'|bash

第二种方法的简化：

chkconfig --list|grep "3:on"|grep -Ev "sshd|rsyslog|network|crond|sysstat"|awk '{print "chkconfig " $1 " off"}'|bash

第三种方法：

LANG=en

for oldboy in `chkconfig --list|grep 3:on|awk '{print $1}'`;do chkconfig --level 3 $oldboy off;done

for oldboy in crond network rsyslog sshd sysstat ;do chkconfig --level 3 $oldboy on;done

**3.4 关闭iptables防火墙**

关闭防火墙的目的是为了让初学者学习更方便，将来在学了iptables技术后可以开启，在企业环境中，一般只有外网IP的服务器才需要开启防火墙。关闭防火墙命令：

[root@C66-moban ~]# /etc/init.d/iptables stop （service iptables stop等价命令，但这种命令很烂）

iptables: Setting chains to policy ACCEPT: filter [ OK ]

iptables: Flushing firewall rules: [ OK ]

iptables: Unloading modules: [ OK ]

[root@C66-moban ~]# /etc/init.d/iptables status

iptables: Firewall is not running.

**3.5 Linux系统安全最小原则说明**

最小化原则对Linux系统安全来说极其重要：即多一事不如少一事。具体包括如下几个方面：

（1）安装Linux系统最小化，即选包最小化，yum安装软件包也要最小化，无用的包不装。

（2）开机自动启动服务最小化，既无用的服务不开启。

（3）操作命令最小化，例如：用rm –f test.txt 而不用rm –fr test.txt

（4）登录Linux用户最小化，平时没有需求不用root登录，用普通用户登录即可。

（5）普通用户授权权限最小化，即只给必须的管理系统的命令，不能啥都可以干。

（6）Linux系统文件及目录的权限设置最小化，禁止随意创建、更改、删除文件。

**3.6更改****ssh服务端远程登录的配置**

Windows服务器的默认远程管理端口是3389，管理员用户是administrator，普通用户是guest。Linux的管理用户是root，普通用户默认有多个，远程连接默认端口是22，这些通常搞IT的人都知道，那么黑客是否也知道呢？所以，为了系统安全要隐藏或更改默认的配置才行。更改配置的命令如下：

方法1，比较繁琐：

[root@moban ~]# cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.ori

#-🡪更改配置前进行备份，是系统管理员的一个良好的习惯。

[root@moban ~]# vi /etc/ssh/sshd\_config #-🡪编辑 sshd\_config

####by oldboy#2011-11-24##

Port 52113 #-🡪修改端口号

PermitRootLogin no #-🡪是否允许root登录

PermitEmptyPasswords no #-🡪是否允许密码为空的用户远程登录。

UseDNS no #-🡪指定sshd是否应该对远程主机名进行反向解析

GSSAPIAuthentication no #-🡪解决Linux之间使用SSH远程连接慢的问题。

####by oldboy#2011-11-24##

方法2，最简易版优化命令：

sed -ir '13 iPort 52113\nPermitRootLogin no\nPermitEmptyPasswords no\nUseDNS no\nGSSAPIAuthentication no' sshd\_config

如果想使上面的命令生效的话需要重启sshd服务，命令为：

[root@www ~]# /etc/init.d/sshd reload （平滑重启）

重新载入 sshd： [确定]

或者

[root@www ~]# /etc/init.d/sshd restart （强制重启）

Stopping sshd: [ OK ]

Starting sshd: [ OK ]

ListenAddress 10.0.0.8:52113 只监听内网的IP和端口

####在vi编辑器中使用：set nu即可以显示行号。

[root@moban ~]# netstat -lntup|grep sshd

tcp 0 0 0.0.0.0:52113 0.0.0.0:\* LISTEN 1956/sshd

tcp 0 0 :::52113 :::\* LISTEN 1956/sshd

####查看端口信息的命令

其中，sshd\_config修改的相关参数说明见下表

|  |  |
| --- | --- |
| 参数 | 说明 |
| Port | 指定sshd守护进程监听的端口号，默认为22，默认在本机的所有网络接口上监听，也可以通过listenAddress指定只在某个特定的接口上监听。  端口范围：0～65535，不能喝已有的服务端口冲突。  一般建议为比1024大的端口 |
| PermitRootLogin | 是否允许root登录。可用值如下：“yes”（默认）表示允许；“no”表示禁止；“without-password”表示禁止使用密码认证登录；“forced-only”表示只有在指定了command选项的情况下才允许使用公钥认证登录，同时其他认证方法全部被禁止，这个值常用于做远程备份之类的事情。 |
| PermitEmptyPasswords | 是否允许密码为空的用户远程登录。默认为“no” |
| UseDNS | 指定sshd是否应该对远程主机名进行反向解析，以检查此主机名是否与其IP地址真实对应。默认值为“yes”。  建议改成“no”，否则可能会导致SSH链接很慢。 |
| GSSAPIAuthentication | 解决Linux之间使用SSH远程连接慢的问题。 |

**3.7 利用sudo控制用户对系统命令的使用权限**

为了安全及管理的方便，可将需要有root权限的用户加入sudo管理，这样用普通用户通过自己的普通账户登录，用root的权限来管理系统了，当然也就不需要有root登录密码了。

执行如下visudo命令，即可打开sudo的配置文件进行编辑。

[oldboy@moban ~]$ visudo #--🡪相当于直接编辑/etc/sudoers，但用visudo命令方式更安全。

[root@moban ~]# visudo

user（想要分配的用户） MACHINE（希望用户管理的机器）=COMMANDS（希望用户拥有哪些权限）

oldboy（用户） ALL（在所有机器上）=(ALL)（以所有的角色） /bin/touch, /usr/sbin/useradd（可以创建文本、创建用户）

root ALL=(ALL)（允许以哪个角色去执行命令） ALL

在/etc/sudoers文件的第98行下面添加需要提升为root权限的普通用户名

#####vi快捷键YY为复制；P为粘贴；：set nu为显示行号；行号+GG=切换到指定的行；

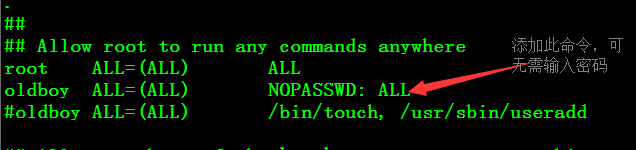
使用which命令查看命令所在路径

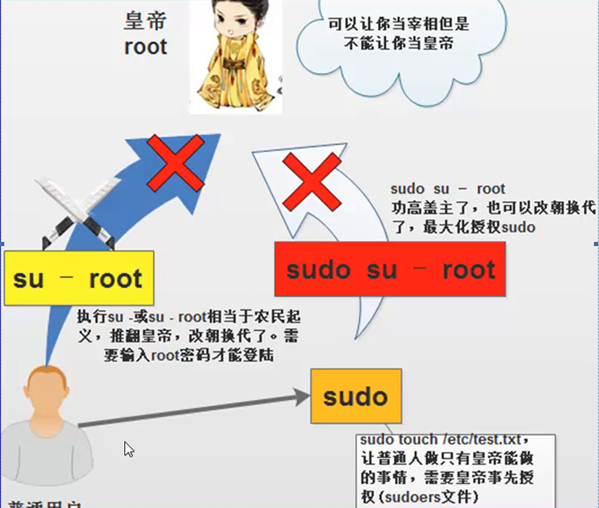
例如：

[root@moban ~]# which useradd

/usr/sbin/useradd

修改此命令后，oldboy用户的权限与root一样高。可以修改root的权限。





查找命令所在路径共四种方法：

法1：

[root@moban ~]# which useradd

/usr/sbin/useradd

法2：

[root@moban ~]# find / -type f -name "useradd"

/etc/default/useradd

/usr/sbin/useradd

法3：

[root@moban ~]# whereis -b useradd

useradd: /usr/sbin/useradd

法4：

[root@moban ~]# locate useradd

/etc/default/useradd

/usr/sbin/luseradd

/usr/sbin/useradd

###which原理：搜索范围来自全局环境PATH变量对应的路径。

[root@moban ~]# echo $PATH

/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin

###PATH的路径为以上，不同的路径以“：”分隔，使用which查找命令时在上面路径查找。

变量所在的位置：

[root@moban ~]# grep PATH /etc/profile

case ":${PATH}:" in

PATH=$PATH:$1

PATH=$1:$PATH

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

**PATH变量的内容：**

[root@moban ~]# export PATH="/tmp:$PATH" #--🡪临时添加PATH路径（$PATH要写全，不然除内置命令外其他命令都将无法使用）

[root@moban ~]# echo $PATH

/tmp:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin

[root@moban ~]# which oldboy #-🡪先查找看是否有oldboy命令。

/usr/bin/which: no oldboy in (/tmp:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)

[root@moban ~]# touch /tmp/oldboy

[root@moban ~]# chmod +x /tmp/oldboy #-🡪 将/tmp/oldboy变成命令

[root@moban ~]# which oldboy

/tmp/oldboy

[root@moban ~]# chmod -x /tmp/oldboy

[root@moban ~]# which oldboy

/usr/bin/which: no oldboy in (/tmp:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)

[root@moban ~]# chmod +x /tmp/oldboy

[root@moban ~]# which oldboy

/tmp/oldboy

**3.8 Linux中文显示设置**

字符集就是一套文字符号及其编码，最常见的字符集UTF-8：非定长的字符集，一个汉字用UTF-8格式会占用3个字符集，广泛支持，MYSQL也使用UTF-8；GBK：定长，双字节，不是国际标准，支持的系统不少。字符集的配置文件是：

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

LANG="en\_US.UTF-8" -🡪变量

SYSFONT="latarcyrheb-sun16"

[root@moban ~]# cp /etc/sysconfig/i18n /etc/sysconfig/i18n.ori -🡪备份

[root@moban ~]# sed -i 's#LANG="en\_US.UTF-8"#LANG="zh\_CN.UTF-8"#g' /etc/sysconfig/i18n

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

LANG="zh\_CN.UTF-8"

SYSFONT="latarcyrheb-sun16"

#####此时字符集已修改完成，若要使其生效的话，请使用下面的命令。

[root@moban ~]# source /etc/sysconfig/i18n -🡪使其生效。

[root@moban ~]# echo $LANG

zh\_CN.UTF-8

使Linux系统支持中文字符集的步骤如下：

1. 将服务器端字符集（/etc/sysconfig/i18n）改为LANG=LANG="zh\_CN.UTF-8"。
2. 将客服端字符集（CRT）调整为UTF-8

**3.9设置Linux服务器时间同步**

使用date命令查看当前系统时间：

[root@moban ~]# date

2015年 10月 12日 星期一 09:45:17 CST

修改年月日的命令：

[root@moban ~]# date -s "2015/10/12 9:46"

2015年 10月 12日 星期一 09:46:00 CST

同步互联网时间命令：

/usr/sbin/ntpdate.nist.gov

每隔5分钟和时间服务器同步的命令：

echo "\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/"

将时间同步的命令保存

[root@moban ~]# echo "\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1" >>/var/spool/cron/root

查看：

[root@moban ~]# crontab -l

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

**3.10 历史记录及登录超时环境变量设置**

1.设置闲置账号超时时间

设置闲置账号超时时间的示例命令如下，注意此处的配置仅临时生效。

为CRT终端设置超时（过多少秒之后系统自动退出）

[root@moban data]# export TMOUT=10

[root@moban data]# timed out waiting for input: auto-logout 🡨10秒提示超时

设置永久生效命令：

[root@moban ~]# echo "export TMOUT=10" >>/etc/profile

[root@moban ~]# tail -1 /etc/profile

export TMOUT=10

使其生效的命令：

[root@moban ~]# source /etc/profile

设置Linux默认的历史记录数

设置Linux默认的历史记录数时，示例命令如下，注意此处的配置仅临时生效。

[root@moban ~]# export HISTSIZE=5

[root@moban ~]# history

871 history --help

872 history

873 history

874 HISTSIZE=5

875 history

使其永久生效的命令与配置文件

[root@moban ~]# cat ~/.bash\_history --🡪此时还是显示全部命令

[root@moban ~]#HISTFILESIZE=5 ---🡪使配置文件也变为5条记录

把配置参数放入配置文件，使得可是永久生效：

[root@moban ~]# echo 'HISTFILESIZE=5' >>/etc/profile -🡪在历史记录文件中只显示5条命令（~/.bash\_history）

[root@moban ~]# echo 'TMOUT=300' >>/etc/profile -🡪5分钟自动退出（连接的超时时间控制变量）

[root@moban ~]# echo 'HISTSIZE=5' >>/etc/profile -🡪只显示5条命令

[root@moban ~]# tail -3 /etc/profile

export TMOUT=300

HISTSIZE=5

HISTFILESIZE=5

[root@moban ~]# source /etc/profile ###-🡪使得配置文件生效。

**3.11 加大服务器文件描述符**

文件描述符概念：

1. 表示形式为整数数字，一般使用（0-65535）范围。
2. 进程使用的时候会占用文件描述符（标示打开的文件）
3. 查看文件描述符：ulimit -n

[root@moban ~]# ulimit -n

1024

1. 调整文件描述符：

法1：

[root@moban ~]# ulimit -SHn 65535

[root@moban ~]# ulimit -n

65535

#####--🡪此法为临时生效。

法2：

[root@moban ~]# echo '\* - nofile 65535 ' >>/etc/security/limits.conf

[root@moban ~]# tail -1 /etc/security/limits.conf

\* - nofile 65535

####--🡪此法为永久生效（配置完成后需重新登录CRT）

调整的文件为

[root@moban security]# cat -n limits.conf

#<domain> (域) <type> （类型） <item> （项） <value>（配置的值）

\* - nofile 65535

域：可能是一个用户名，一个组名，是一个通配符\*，还可以是%等等。

类型：1）软限制 2)应限制

项：要对哪项优化，nofile就是最大的打开文件描述符的数量。

**3.12 调整内核参数文件/etc/sysctl.conf**

[root@moban ~]# vim /etc/sysctl.conf

net.ipv4.tcp\_fin\_timeout = 2

net.ipv4.tcp\_tw\_reuse = 1

net.ipv4.tcp\_tw\_recycle = 1

net.ipv4.tcp\_syncookies = 1

net.ipv4.tcp\_keepalive\_time = 600

net.ipv4.ip\_local\_port\_range = 4000 65000

net.ipv4.tcp\_max\_syn\_backlog = 16384

net.ipv4.tcp\_max\_tw\_buckets = 36000

net.ipv4.route.gc\_timeout = 100

net.ipv4.tcp\_syn\_retries = 1

net.ipv4.tcp\_synack\_retries = 1

net.core.somaxconn = 16384

net.core.netdev\_max\_backlog = 16384

net.ipv4.tcp\_max\_orphans = 16384

#以下参数是对iptables防火墙的优化，防火墙不开会提示，可以忽略不理。

net.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_max = 25000000

net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180

net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120

net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60

net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

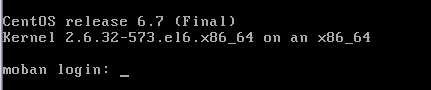
[root@moban ~]# sysctl –p ####--🡪使其生效

Shift+g切换到文件结尾，按0在下一行处于编辑模式

以上优化参数的描述在<http://yangrong.blog.51cto.com/6945369/1321594> 中可查询到。

**3.13 隐藏Linux版本信息显示**

在登录Linux主机本地（非CRT连接）前，会显示系统的版本和内核，如下图所示。

****

登录Linux前的终端显示图，查看上图的命令为：

[root@moban ~]# cat /etc/issue

CentOS release 6.7 (Final)

Kernel \r on an \m

[root@moban ~]# cat /etc/issue.net

CentOS release 6.7 (Final)

Kernel \r on an \m

为了保护系统安全不让其他人知道你的系统信息，需将上图消息清空，清空命令为：

1、

[root@moban ~]# > /etc/issue

2、

[root@moban ~]# cat /dev/null >/etc/issue

编辑上图中的文字路径

[root@moban ~]# vi /etc/motd ######---🡪退出在进入就生效。

**3.14 锁定关键系统文件，防止提权被篡改**

要锁定关键系统文件，必须对账号密码文件及启动文件加锁，防止被篡改。

[root@moban ~]# chattr +i /etc/shadow /etc/group /etc/gshadow /etc/inittab

提示：上锁后，如需临时操作，可以解锁后对文件进行修改，之后再上锁。

想要更为安全，可以把chattr改名转移，防止被黑客利用。命令如下：

[root@moban ~]# mv /usr/bin/chattr /usr/bin/oldboy1

将chattr命令路径更改即可。

**3.15清除多余的系统虚拟账号**

[root@moban ~]# grep -v "nologin$" /etc/passwd

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

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

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

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

oldboy:x:500:500::/home/oldboy:/bin/bash

fff:x:501:501::/home/fff:/bin/bash

111:x:502:502::/home/111:/bin/bash

msn:x:503:503::/home/msn:/bin/bash

**3.16 为grub菜单加密码**

为grub菜单加密码的目的是防止他人修改grub做内核启动等设置

[root@moban ~]# /sbin/grub-md5-crypt

Password:

Retype password:

$1$SgF8T$qppcvgWeR7276.ry5kUWr/

###--🡪此时密码已生成，需将密码放到下面的配置文件第14行内。

[root@moban ~]# vi /etc/grub.conf

14 password --md5 $1$SgF8T$qppcvgWeR7276.ry5kUWr/

**3.17 禁止Linux系统被ping**

[root@moban ~]# echo "net.ipv4.icmp\_echo\_ignore\_all=1" >> /etc/sysctl.conf

[root@moban ~]# sysctl -p ---🡪使其生效

**优化小结：**

1）不用root管理,以普通用户的名义通过sudo授权管理。

2) 更改默认的远程连接SSH服务端口，禁止root用户远程连接，甚至要更改为只监听内网IP。

3）定时自动更新服务器时间，使其和互联网时间同步。

4）配置yum更新源,从国内更新源下载安装软件包。

5）关闭seLinux及iptables（在工作场景中，如果有外部IP一般要打开iptables，高并发除外）。

6）调整文件描述符的数量，进程及文件的打开都会消耗文件描述符。

7）定时自动清理邮件目录垃圾文件，防止inodes节点被占满

（注意Centos6和Centos5的目录不同）。

8）精简并保留必要的开机自启动服务（如crond、sshd、network、rsyslog、sysstat）。

9）Linux内核参数优化/etc/sysctl.conf，执行sysctl -p生效。

10）更改字符集，使其支持中文，但建议还是用英文字符集，防止出现乱码问题。

11）锁定关键系统文件如（/etc/passwd /etc/shadow /etc/group /etc/gshadow /etc/inittab）

处理以上内容后把chattr、lsattr改名为oldboy，这样就安全多了。

12）清空/etc/issue、/etc/issue.net，去除系统及内核版本登录前的屏幕显示。

13）清除多余的系统虚拟账号。

14）为grub菜单加密码。

15)禁止被PING

16）升级漏洞软件

**4、课前考试题**

1、创建目录/data/oldboy ，并且在该目录下创建文件oldboy.txt，然后在文件oldboy.txt里写入内容"inet addr:10.0.0.8 Bcast:10.0.0.255 Mask:255.255.255.0"（不包含引号）。

[root@moban ~]# mkdir /data/oldboy -p;cd /data/oldboy;touch oldboy.txt

[root@moban oldboy]# ls

oldboy.txt

[root@moban oldboy]# echo "inet addr:10.0.0.8 Bcast:10.0.0.255 Mask:255.255.255.0" >oldboy.txt

[root@moban oldboy]# cat oldboy.txt

inet addr:10.0.0.8 Bcast:10.0.0.255 Mask:255.255.255.0

2、将题1中的oldboy.txt文件内容通过命令在屏幕上输出：

10.0.0.8 10.0.0.255 255.255.255.0

[root@moban oldboy]# awk -F "[ :]" '{print $3,$5,$7}' oldboy.txt

10.0.0.8 10.0.0.255 255.255.255.0

3、将题1中的oldboy目录移动到/tmp目录下，并将/etc/passwd文件复制到/tmp/oldboy下。

[root@moban ~]# mv /data/oldboy /tmp

[root@moban ~]# ls /tmp

a oldboy ssh-jmzZwC2456 ssh-xyGxkT2270 yum.log

[root@moban oldboy]# cp /etc/passwd /tmp/oldboy/

[root@moban oldboy]# ls

oldboy.txt passwd

4、在题3的基础上使用awk取passwd文件的第10行到20行的第三列重定向到/tmp/oldboy/test.txt文件里。

[root@moban oldboy]# awk -F '[:]' 'NR>9 && NR<21 {print $3}' /tmp/oldboy/passwd >/tmp/oldboy/test.txt

[root@moban oldboy]# ls

oldboy.txt passwd test.txt

[root@moban oldboy]# cat test.txt

10

11

12

13

14

99

81

69

173

68

38

5、在题3的基础上用命令rm删除文件时会出现如下禁止使用rm的提示，并使该效果永久生效。

[root@oldboy oldboy]# rm -f passwd

Do not use rm command.

[root@moban oldboy]# alias rm='echo "Do not use rm command."'

[root@moban oldboy]# rm -f passwd

Do not use rm command. -f passwd

[root@moban oldboy]# echo alias rm='echo "Do not use rm command."' >>/root/.bashrc

[root@moban oldboy]# source /etc/profile

6、在题3的基础上,删除/tmp/oldboy/下的除passwd外其他文件

[root@moban oldboy]# ls

oldboy.txt passwd test.txt

[root@moban oldboy]# find ./ -type f ! -name "passwd"

./test.txt

./oldboy.txt

[root@moban oldboy]# find ./ -type f ! -name "passwd"|xargs rm -f

[root@moban oldboy]# ls

passwd

7、在题3的基础上,请用awk,grep,sed,head,tail分别取出passwd文件中的第2-5行

[root@moban oldboy]# sed -n '2,5p' passwd

[root@moban oldboy]# head -5 passwd|tail -4

[root@moban oldboy]# awk 'NR>1 && NR<6' passwd

[root@moban oldboy]# grep "bin:x" -A 3 passwd

8、在题3的基础上,使用命令调换passwd文件里root位置和/bin/bash位置？即调换所有的第一列和最后一列位置调换？

例：

默认：root:x:0:0:root:/root:/bin/bash

修改后：/bin/bash:x:0:0:root:/root:root

[root@moban oldboy]# awk -F "[:]" '{print $7":"$2":"$3":"$4":"$5":"$6":"$1}' passwd

9、把/data目录及其子目录下所有以扩展名.txt结尾的文件中包含oldgirl的字符串全部替换为oldboy。

[root@moban oldboy]# find /data -type f -name "\*.txt"|xargs sed -i 's#oldgirl#oldboy#g'

10、什么是linux的运行级别，请描述linux的运行级别不同数字的含义?

0 关机模式

1 单用户模式

2 多用户模式，没有NFS

3 文字模式

4 一般不用，在一些特殊情况下可以用它来做一些事情。例如在笔记本电脑的电池用尽时，可以切换到这个模式来做一些设置

5 桌面模式

6 重启模式

11、请说出下列字符代表的意义(附加题)。

~ - . .. | > >> < << ！

~ 用户家目录

- 返回上一次目录

. 当前目录

.. 上一级目录

| 管道

> 重定向

>> 追加重定向

< 输入重定向

<< 追加输入重定向

！取反