在VMware workstation中网络适配器可以修改网络连接，常用的网络连接：

桥接：虚拟机网络物理化，直接将虚拟机的网卡接入到真实物理网络下，两台不同主机中的虚机如果需要访问必须设置为桥接模式，如果想修改桥接到的网络（有线，无线或蓝牙等）选择编辑菜单，选择虚拟网络编辑器，然后设置桥接即可（其中有网络连接中看到的所有网卡信息）

NAT：主要用于共享上网，只要外面主机可以上网，虚拟机自动可以上网，不用管外面上网方式（有线、无线、4G上网卡等），外面（其他主机或者其他主机中虚机）是无法访问该虚机，本主机可以访问NAT的虚拟机，是通过本地主机的vmnet8网卡通信

仅主机：不能上网，只能和自己本主机的vmnet1网卡通信

自定义中vmnet0就是桥接，vmnet1就是仅主机，vmnet8就是nat

设置NAT连接方式

网络配置：IP地址、子网掩码、默认网关、DNS

IP地址和子网掩码必须配置，网关和DNS是可选

网关主要用于访问不同网络（上网必须用到网关）

DNS主要是通过域名访问来访问网络中服务（IP地址不好记，域名好记）

系统中网卡的命名一般以eth开头后面数字，eth0第一张网卡，eth1第二张网卡......

7之前系统都是采用eth的方式进行命名的，但是在7的系统下（RHEL7或CentOS7中）网卡命名一般以en0（有线）开头或wl（无线WIFI）开头或ww（上网卡）开头，便于区分不同类型的网卡，有的时候如果网卡类型无法识别也会采用eth命名方式

NetworkManager服务是从6的系统开始增加的一个服务，6之前的系统如果修改网卡配置文件需要重启网络服务才能生效，该服务可以不需要手动重启，修改完配置文件后自动应用新配置信息，如果禁用该服务，那么修改配置文件后就需要手动重启

6系统中配置IP地址

setup集成管理工具包，内中含有大量集中工具（7中不支持配置网络，nmcli管理网络）

网络信息查看命令：

ifconfig

ip addr show

默认情况下如果安装过程中没有配置网络信息，网络是被禁用的需要手动启用

vim /etc/sysconfig/network-scripts/ifcfg-eth0 修改下面一行的信息

ONBOOT=yes 默认是no代表禁用，改为yes即可

service network restart 如果没有开启NetworkManager服务的话需要使用该命令重启网络服务以读取修改过的配置文件

ping 8.8.8.8 测试网络连接，如果ping通证明互联网连接是OK的

ip route 查看本机路由表以及网关

host 测试名称解析，测试DNS服务器是否正常

traceroute 探测路由，探测到达目标网络经过每个路由器的IP地址

mtr 既能探测路由也能测试网络连通

修改主机名：

hostname 查看主机名也能在后面添加主机名进行修改，但是一旦重启恢复到之前配置

vim /etc/sysconfig/network 将第二行改成自己的主机名即可，这个主机名一般都是采用FQDN（完全合格域名）格式，一般含有主机而且有后缀，主要用于标记当前服务器所起的功能服务用，建议都是按照提供的服务进行命名，不建议一个网络内有重名

DNS是提供名称解析，本地可以使用hosts文件(/etc/hosts)，hosts只能用于本地，只做本地解析，适用于局域网环境，DNS适用于互联网或者网络比较大型，hosts文件优先级高于DNS服务器

修改DNS服务器地址：

setup工具可以

vim /etc/resolv.conf 通过nameserver来定义DNS服务器，最多可以定义三个

进程管理

ps 可以查看进程，列出的是某个时刻进程（就是执行ps的时候）

ps aux 查看所有进程以用户为单位显示，包括图形化下进程

top 可以实时显示进程信息，每隔3s刷新一次，按照CPU使用情况由高到低排序

进程结束

kill PID编号 可以结束某个进程，需要提前知道进程的编号

查找进程PID方法：

ps aux | grep firefox 列出系统中所有进程信息只显示含有firefox的

pgrep -l firefox 就是ps和grep命令的结合，显示PID和进程名

killall firefox 不需要查询PID编号，直接结束所有名称为firefox的进程

任务计划：

crontab Linux中周期性执行的任务计划

crontab命令选项

-e 以vi方式编辑任务计划

-l 查看任务计划

-r 清空任务计划

-u 指定用户，root专用，比如crontab -l -u test查询test用户的任务计划

crontab如果不指定选项，默认是新建任务计划，会清空之前所有的配置信息

vim /etc/crontab 查看crontab任务计划的配置文件，里面记录格式信息

crontab -e 编辑当前用户的任务计划，格式前面是时间字段，后面是具体命令

1 \* \* \* \* ls \*通配符代表任何时间，该时间字段代表每个小时的第一分钟执行ls命令，由于ls会直接在屏幕输出结果，系统会默认以电子邮件的方式发送给root用户，建议所有会在屏幕输出结果的命令都重定向至某个文件中，文件要写绝对路径

\*/1 \* \* \* \* date >> /tmp/date.txt 每隔一分钟将date命令的结果追加到/tmp/date.txt文件中

Linux远程管理：

telnet：明文传输，不加密，安全性差，默认情况下Linux中不启用，可以手动启用，但是root用户不能远程连接，root连接永远都是密码错误，可以先用普通用户接入，然后再使用su命令切换至root

ssh：加密传输，安全性高，默认情况下Linux采用的远程管理方式，默认已经开启的。

VNC是图形化下远程连接

SSH采用的通用的公钥和私钥加密和解密方式，服务器生成密钥对（公钥和私钥），客户端下载服务器的公钥，使用服务器的公钥进行加密，服务器收到加密的数据利用自己的私钥来解密，私钥服务器不会给其他任何人，所以可以保证数据其他用户获取也无法解密

ssh是C/S模式，需要有服务器有客户端，客户端连接服务器（也可以一台主机既是服务器也是客户端，正常情况下不会出现该方式，测试环境可以使用）

ssh 对方IP地址 测试环境可以使用本机IP地址连接自己，第一次连接对方主机需要使用yes下载对方的公钥，以后将不会再需要下载（除非服务器换公钥，或者连接其他服务器）

vim ~/.ssh/know\_hosts 该文件记录的所有下载的服务器的公钥信息，每行一个公钥

在服务器端执行

ls /etc/ssh 可以看到该目录有\_key结尾和\_key.pub结尾的若干文件，名称都是成对的，服务器可以自行选择采用哪对公钥和私钥进行加密和解密，以.pub结尾的是公钥，文件可以公开，另一个名称一样但是没有.pub结尾的就是私钥文件，这个文件不能给任何人，自己妥善保管

ssh 对方IP 本地登录用户名和对方用户一致可以直接连接对方

ssh -l 对方用户名 对方IP地址 指定用户连接远程服务器

ssh服务器认证

密码认证：默认就是密码认证，要求客户端输入用户密码才能连接

密钥认证：默认也是开启，用户生成自己的公钥和私钥（客户自行选择是否生成和服务器的密钥对不同），如果客户生成了密钥对，将公钥上传至服务器，以后连接服务器将不再需要密码

客户端执行：生成密钥对

ssh-keygen 客户端的密钥对是每个用户独立的，位置建议默认值，否则调用私钥需要定义，密码如果是免密登录不需要填写，如果为了安全建议加上密码

ls ~/.ssh/ 可以看到id\_rsa私钥文件，id\_rsa.pub公钥文件

上传公钥文件至服务器

ssh-copy-id -i /root/.ssh/id\_rsa.pub root@对方IP 上传指定用户的公钥文件至服务器的root用户下，如果是当前用户公钥可以不需要-i选项

scp 借助于SSH协议进行远程的安全的复制

scp /etc/passwd root@对方IP:/tmp 将本地/etc/passwd文件上传至服务器的/tmp目录

scp root@对方IP:/etc/passwd ./ 将对方服务器的文件下载至本地当前目录

如果能够免密登录，就不需要密码，也可以写入crontab中周期性执行

rsync 同步文件夹，和上面用法相同，只做增量复制

Windows连接Linux主机

putty 绿色小软件可以使用ssh协议连接服务器

winscp 可以使用scp和Linux主机进行文件上传下载

禁用SSH密码认证：

服务器执行

vim /etc/ssh/sshd\_config

搜索Password开头的那行，将yes改为no，注意是没有#开头的

service sshd restart即可