实验一

VMware的安装和使用

# 一、实验内容及目的

1. 本次实验需要学生掌握
2. 在计算机上安装VMware Workstation；
3. 建立虚拟机集群，首先要求能上网，掌握如何创建、克隆和管理虚拟机。要求建立三个虚拟机，实现相互发送和接收数据包；
4. 了解SSH的基本使用。要求实现三台机器之间的无密码互访，如master可以无密码远程登录slave1 和slave2。
5. 使用ssh secure file transfer cliet实现Windows主机与Linxu虚拟机文件互传，使用ssh sucure shell client 实现在Windows上远程登录访问服务器。

#### 验收要求

* 两周（即2次实验课）完成
* 第一周实验课完成（1）-（2），验收三台虚拟机互ping通，见p.18实验效果；
* 第二周实验课完成（3）-（4），验收三台虚拟机SSH普通用户下无密码互通，实验效果见p.24； windows 与linux 虚拟机加文件互传， p.26-27。

#### VMware介绍

VMware Workstation是一款著名的桌面虚拟计算机软件，提供了用户在单一的桌面上同时运行不同操作系统，和进行开发、测试、部署新的应用程序的最佳解决方案。VMware可在一台实体机上模拟完整的网络环境，创建便于携带的虚拟机器。对于企业的 IT开发人员和系统管理员而言， VMware在虚拟网路，实时快照，拖曳共享文件夹，支持 PXE 等方面的特点使它成为必不可少的工具。

VMware Workstation允许操作系统和应用程序在一台虚拟机内部运行。虚拟机是独立运行主机操作系统的离散环境。在 VMware Workstation 中，你可以在一个窗口中加载一台虚拟机，它可以运行自己的操作系统和应用程序。你可以在运行于桌面上的多台虚拟机之间切换，通过一个网络共享虚拟机(例如一个公司局域网)，挂起和恢复虚拟机以及退出虚拟机，这一切不会影响你的主机操作和任何操作系统或者其它正在运行的应用程序。

#### 实验环境

1. 硬件环境：计算机一台；
2. 软件环境： Windows、Linux操作系统；
3. 软件：上大网上教学平台

# 二、实验内容

以下实验步骤已在Windows 11+VMware Workstation17+CentOS 7下验证通过

（2023年4月 严昕宇）

#### CentOS 7在VMware下的安装步骤

（1）首先打开虚拟机，点击“创建新的虚拟机”：

图形用户界面, 应用程序

描述已自动生成

（2）默认选择“典型”，点击“下一步”：

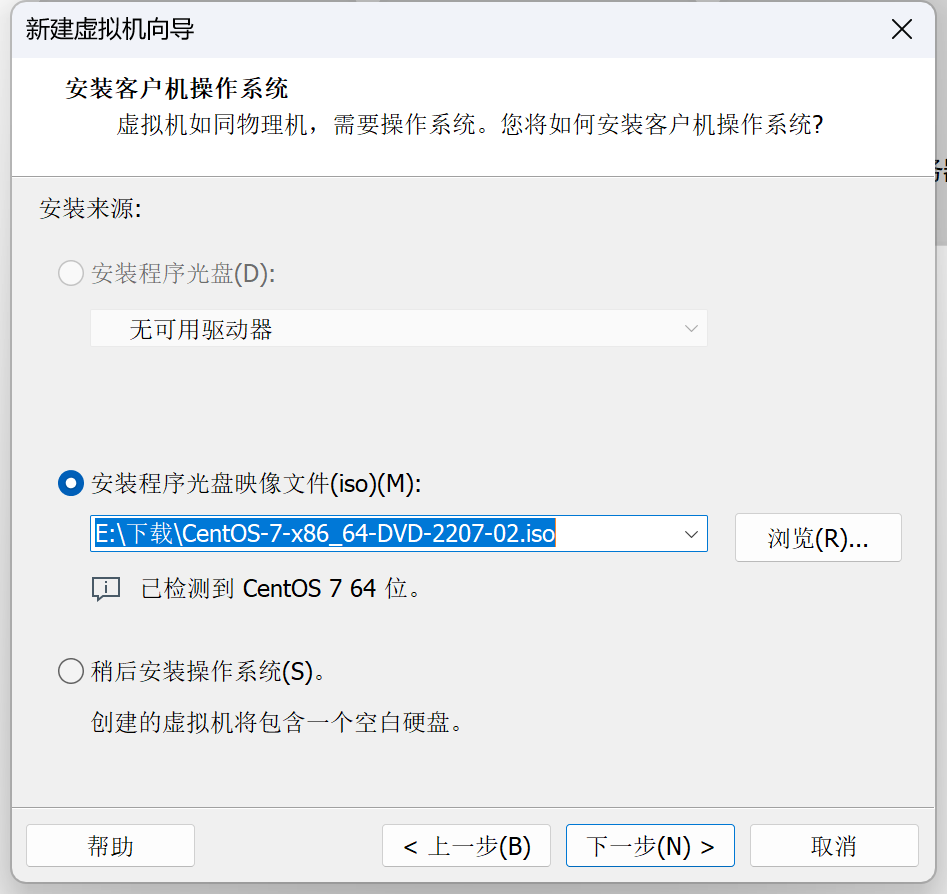
图形用户界面

描述已自动生成

（3）选择CentOS系统镜像文件，然后点击下一步：

CentOS的镜像文件可在通过http://isoredirect.centos.org/centos/7/isos/x86\_64/，选择最近的镜像站下载。

例如上海交通大学镜像站的<http://ftp.sjtu.edu.cn/centos/7.9.2009/isos/x86_64/>选择其中的<http://ftp.sjtu.edu.cn/centos/7.9.2009/isos/x86_64/CentOS-7-x86_64-DVD-2207-02.iso>下载，当然也可以下载其他版本（如最小化版本Minimal）。



（4）选择安装位置：

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

（5）修改磁盘容量（默认即可）：

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

（6）安装完成，开启虚拟机

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

(7) 等待系统安装并初始化（首次运行虚拟机会提示“Install CentOS”，进入CentOS Installer）：

文本

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

（8）按照提示下一步，安装并进入系统：

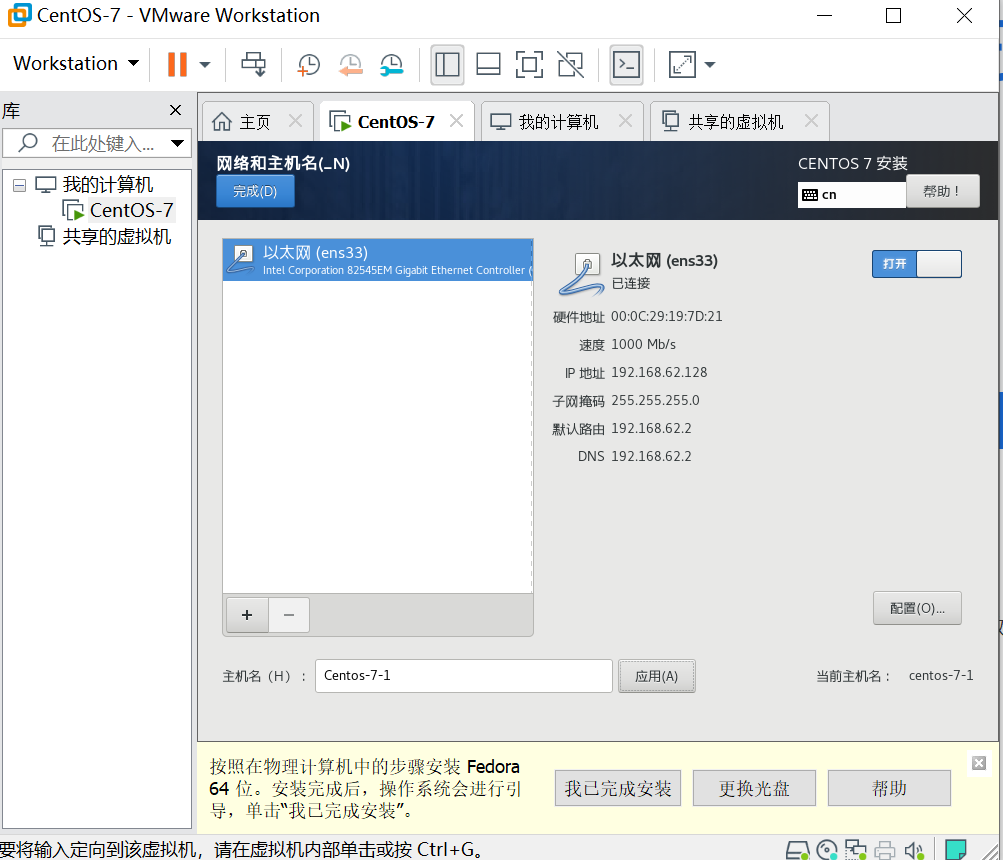
重启后即可进入Linux系统。由于未安装图形界面（或者是Minimal版本），无图形界面，仅有命令行界面。以root用户登录，密码为你刚刚设置的密码。如下：

文本

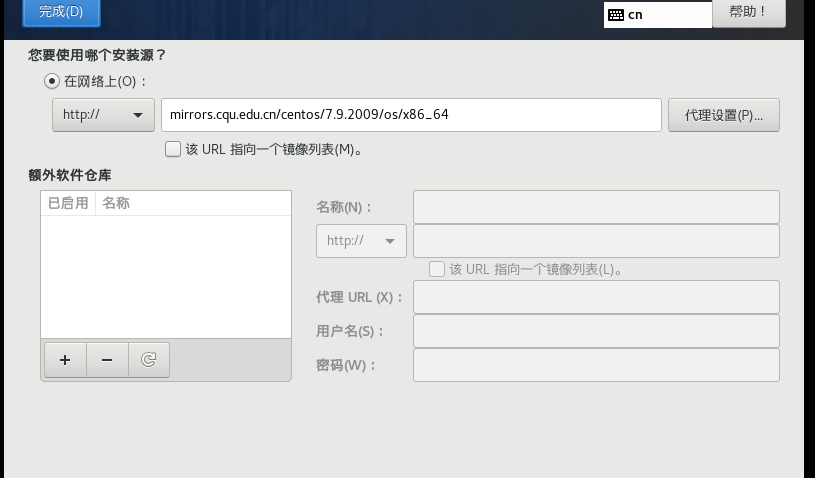
描述已自动生成

注：若安装过程中，出现软件安装源错误的提示，则要先配置，使得安装程序能访问网络，步骤如下：





然后设置安装源位：在网络上填入：http://mirrors.cqu.edu.cn/centos/7.9.2009/os/x86\_64/（其他亦可）



（9）打开网络：

1. 首先确保宿主机已联网，利用命令“ping”连接一个网站，例如：

文本

描述已自动生成

返回结果表示目前该系统未联网。

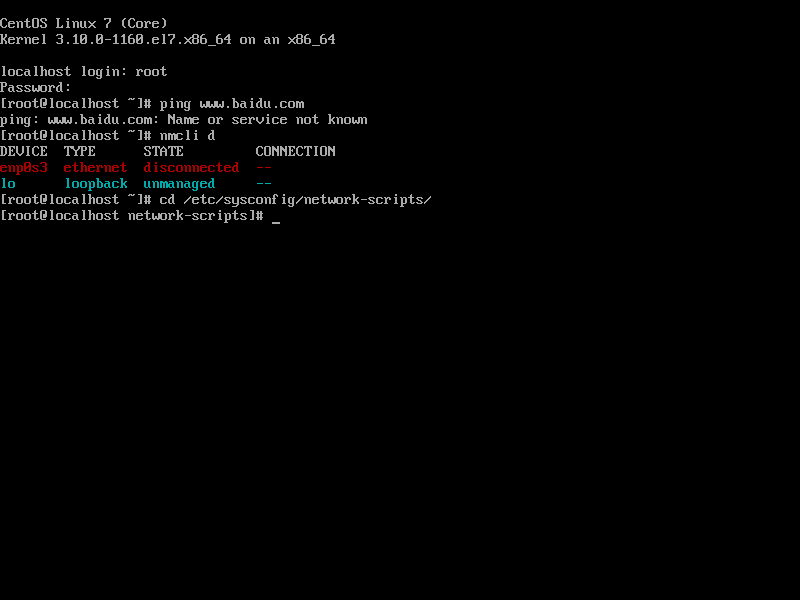
1. 在命令行输入以下命令，查看该虚拟机的网卡名称：

文本

描述已自动生成

本例中网卡为enp0s3（你的电脑网卡名称可能与本例中的不同，例如可能是ens33）

1. 利用命令“cd”进入如下文件夹：



1. 利用命令“ls”显示当前文件夹下所有文件及文件夹名：

图形用户界面, 文本

描述已自动生成

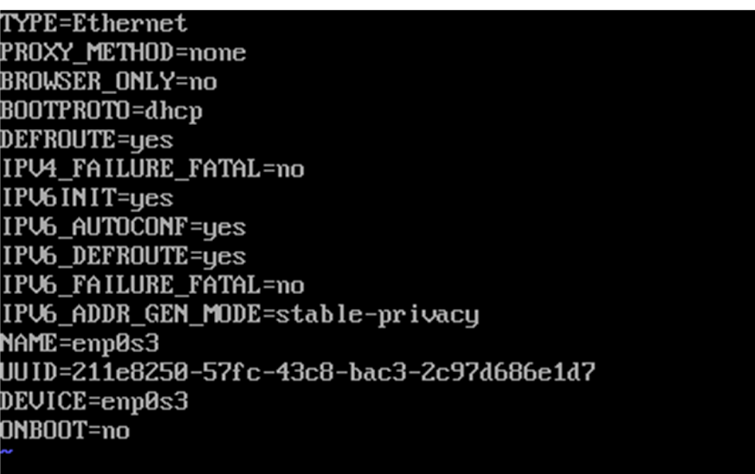
可以看到，有一个文件名包含刚刚所看到的网卡名称，即ifcfg-enp0s3

1. 利用Linux文本编辑器vi或者vim，查看文件内容，命令如下：

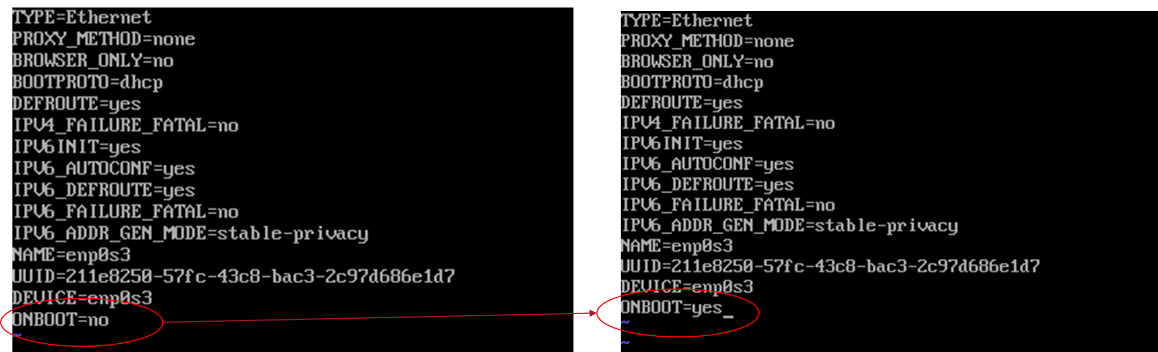
文本

描述已自动生成

1. 上述命令显示该文件内容：



1. 利用vi修改刚刚打开的网卡配置文件：



1. 利用如下命令重新启动网络服务，再连接一个网站，看看是否有返回结果？

文本

描述已自动生成

返回结果如上图所示，表示该虚拟机已联网

（10）安装图形界面：

本教程安装过程中未安装图形界面（或当使用CentOS Minimal版本），仅有命令行界面。安装图形界面并非该实验要求，可根据需要自行决定是否安装图形界面。

1. 利用如下命令下载并安装图形界面：

文本

描述已自动生成

1. 完成后，利用命令“init 5”进入图形界面：

屏幕上写着字

描述已自动生成

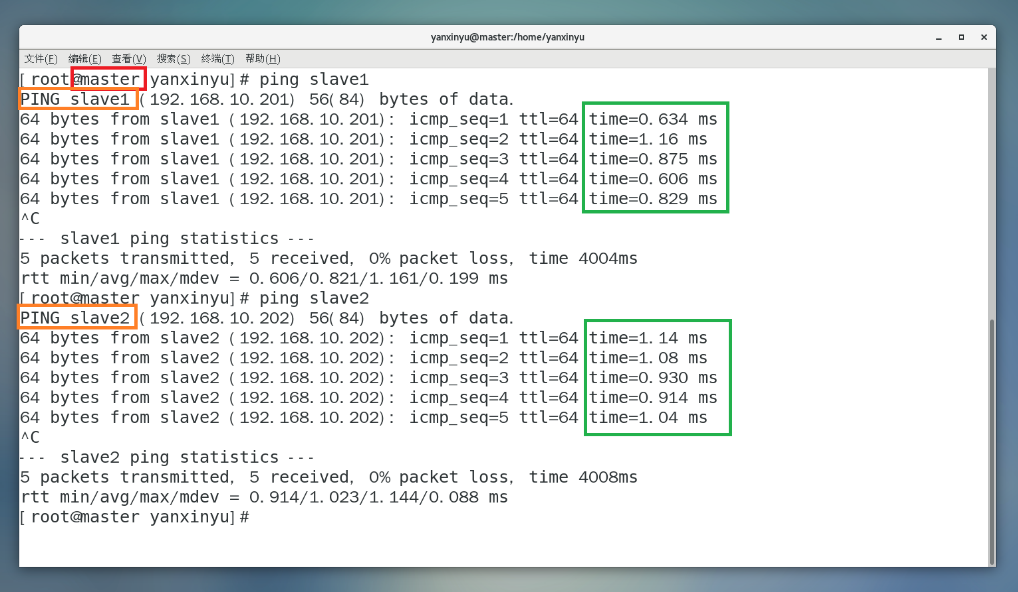
1. 如果需要启动时默认打开图形化界面，右键点击打开一个终端，输入：

|  |
| --- |
| systemctl set-default multi-user.target |

（11）CentOS 7的安装过程到此结束

#### 建立三个虚拟机之间的虚拟网络

**目标：**建立三个虚拟机，按照下方表格分配静态并设置host name，当三台虚拟机同时运行时，使得相互之间可以ping通。如：



**（注意：具体实验时采取的网段需要根据具体情况，需要参考安装主机的NAT配置情况）**

|  |  |
| --- | --- |
| host name | ip address |
| master | 192.168.13.130 |
| slave1 | 192.168.13.201 |
| slave2 | 192.168.13.202 |

注：（1）此处的IP地址可以根据自己的电脑自行规划，此处为示例

（2）为实现虚拟机间的网络互通，我们将使用NAT方式连接网络

网络地址转换（NAT, Network Address Translation）属接入广域网（WAN）技术，是一种将私有（保留）地址转化为合法IP地址的转换技术，它被广泛应用于各种类型Internet接入方式和各种类型的网络中。原因很简单，NAT不仅完美地解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

（1）配置VMware网络，选择VMware菜单：编辑->虚拟网络编辑器

图形用户界面, 文本, 应用程序

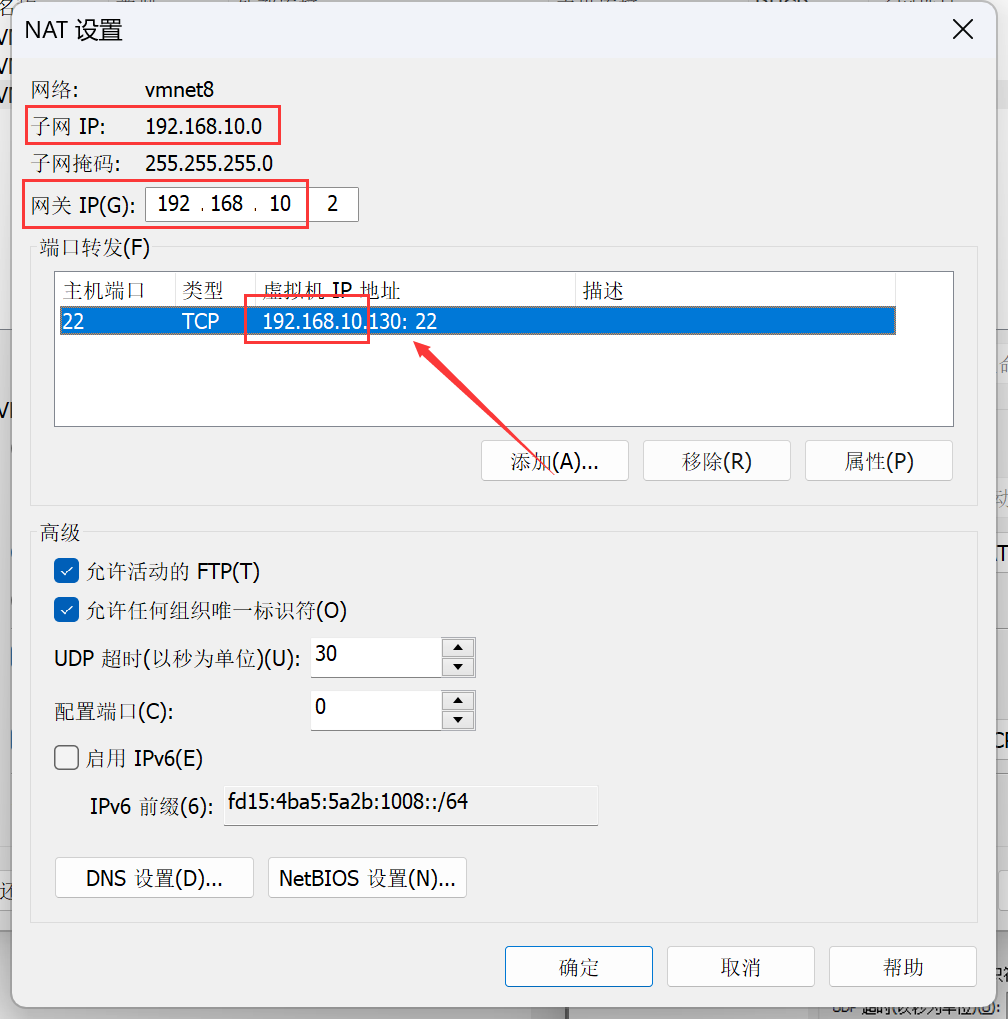
描述已自动生成

1. 需要关注此处的子网IP和子网掩码，之后设置中需要用到！

图形用户界面, 应用程序

描述已自动生成

1. 点击VMnet8 NAT一行，点击“NAT设置“，根据下图设置，注意要确保网关与子网在同一网段（此处意为“192.168.**10**前三个数字相同”），此外为了避免和其它网络冲突，虚拟机网关（192.168.**10**.2）设置没有采用习惯的1或者254网址。此处网址设置请同学自己查找资料学习关于网络IP设置、网关等方面的知识。



1. Windows开始菜单->运行->services.msc或打开控制面板的“服务”，找到以VMware开头的服务，确保都启用。

（2）打开虚拟机，配置第一台虚拟机

1. 打开虚拟机，由于之前配置了图形化界面，故启动进入runlevel 5模式，即GUI界面模式
2. 虚拟机里操作： 应用程序->系统工具->终端（或右键桌面，选择打开终端），在终端中输入命令“su”切换到超级用户，并输入对应的密码，如下所示：

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

**注意：**

* 其中“yanxinyu”是之前建立系统所创建的普通用户，切换为超级用户时，根据提示输入之前设定的密码，密码输入时不可见，输入完回车即可，成功超级用户的标志为$变为#，输入exit即可退出）
* 从超级用户切换到普通用户的命令为“su 普通用户名”即可，如下所示：

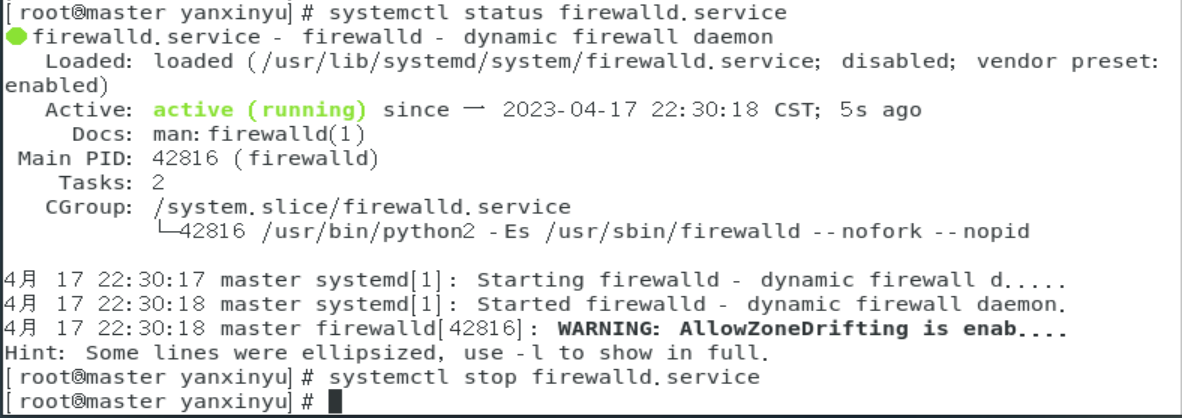
示意图

低可信度描述已自动生成

1. 关闭防火墙（可以不关，但要注意不要拦截后续实验中使用到的网络通信）

|  |
| --- |
| # 暂停防火墙命令  **systemctl status firewalld.service**  **systemctl stop firewalld.service**  # 永久关闭防火墙命令  **systemctl disable firewalld.service** |

效果如下所示：



1. 修改hostname（主机名）

|  |
| --- |
| # 方法1：修改hostname文件，重启后生效  **vi /etc/hostname**  使用vi，输入i进入编辑模式，按键Esc进入命令模式  插入内容：**master**（机器名，后续slave1、2同理）  # 方法2：不用重启机器，使用命令  **hostnamectl set-hostname master** |

效果如下所示：

图片包含 形状

描述已自动生成

（3）配置CentOS网络（需要root权限）

1. 输入以下指令

|  |
| --- |
| **ip addr** |

1. 找到需要配置的网卡名ens33

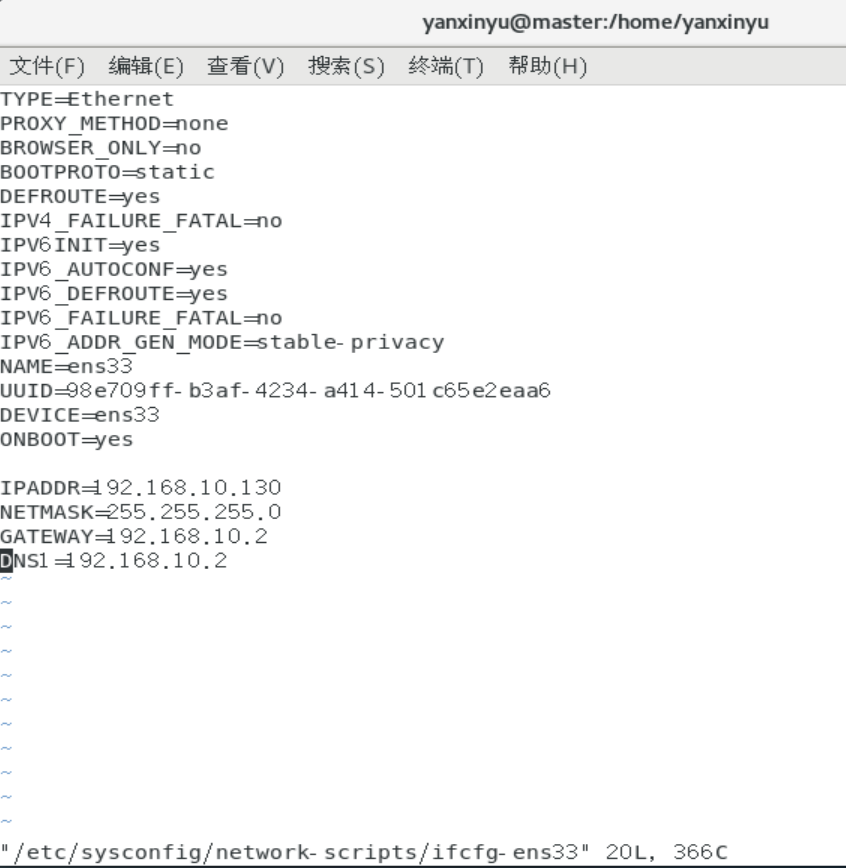
文本, 信件

描述已自动生成

1. 再到 /etc/sysconfig/network-scripts/找到与网卡名对应的配置文件ifcfg-ens33，有关内容修改为：

|  |
| --- |
| # 备注：退出保存操作，先按Esc,进入命令模式，在命令模式中输入“:wq”保存并退出  **BOOTPROTO=static**  # IP地址需要参考之前NAT处的配置情况  **IPADDR=192.168.10.130**  **NETMASK=255.255.255.0**  **GATEWAY=192.168.10.2**  **DNS1=192.168.10.2** |

注意：如果此机器源自克隆，请将此处的UUID和HWADDR两行删掉，并重新修改。配置后如下图所示：

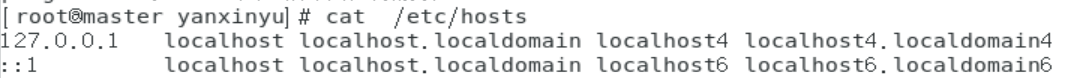


1. 修改hosts映射

首先可以使用cat命令查看hosts文件内容

|  |
| --- |
| **cat /etc/hosts** |

结果如下所示：



在root用户下使用vim编辑hosts文件，根据实际情况（之前规划的网络）将以下代码修改后，加入hosts文件末尾：

|  |
| --- |
| **vim /etc/hosts**  # 插入内容：  **192.168.10.130 master**  **192.168.10.201 slave1**  **192.168.10.202 slave2** |

效果如下所示：

文本

中度可信度描述已自动生成

1. 重启网络功能（必须操作，不能用重启代替）：

|  |
| --- |
| **systemctl restart network** |

试试能否ping通过主机、网关？能否访问外网？如果主机能访问，虚拟机也应能访问。

一些文字和图片的手机截图

描述已自动生成

（3）复制两台虚拟机

注意：为了提高实验效率，克隆两台上面已经建立好的主机，（此外可以根据上面的实验重新安装两台主机，并且请保持新建立的两台新主机和上面的master主机拥有相同的用户名和密码密码）。如果使用克隆，则从可以从步骤1）开始克隆虚拟机。

1. 克隆slave1（参考：https://blog.csdn.net/wangmx1993328/article/details/108036920）

**图形用户界面, 应用程序

描述已自动生成**

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

1. 开启复制来的虚拟机，修改ip和host name（由于是复制的虚拟机，此时ip和host name仍然是先前master的，因此要修改为我们所希望的slave1或2的ip和host name）
2. 修改网卡配置文件ifcfg-XXX，将IPADDR=后的ip改为192.168.10.222（之前规划的）
3. 由于各设备网卡的UUID和MAC地址各不相同，因此需要修改，首先修改UUID

|  |
| --- |
| # 查看网卡UUID  **nmcli con show**  # 生成UUID  **uuidgen 网卡名**  # 修改网卡UUID  **# 将生成的UUID复制到配置文件中** |

1. 再修改MAC地址，即HWADDR值。打开虚拟机设置：



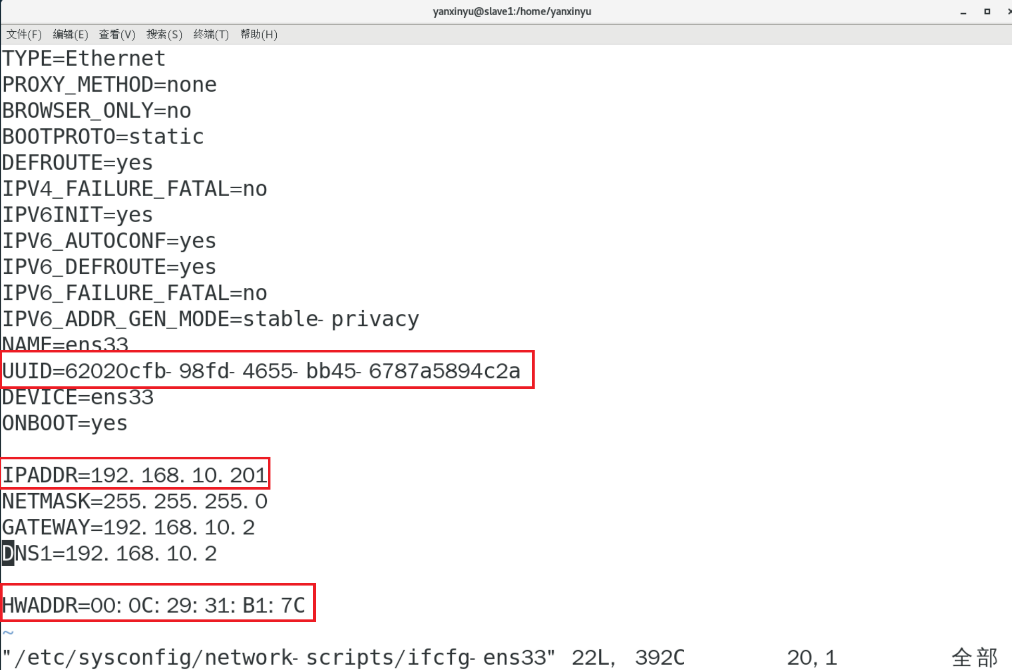
图形用户界面

中度可信度描述已自动生成

图形用户界面

描述已自动生成

将对应的MAC地址写入配置文件中，最终如下所示：



1. 重启网络功能

|  |
| --- |
| **systemctl restart network** |

1. 修改hostname（主机名），即修改/etc/hostname中内容为slave1，重启
2. 至此slave1设置完毕

（4）同理克隆slave2，并参考slave1类似的修改，步骤省略。

（5）这些设置完成后，同时开启这些虚拟机时可以相互ping通。

1. 使用master ping master、 slave1、slave2，正常情况下会受到来自master、slave1、slave2的数据包，成功如下所示：

文本

描述已自动生成

1. slave1 ping master、slave2和slave2 ping master、slave1结果同理：

文本

描述已自动生成

文本

中度可信度描述已自动生成

#### 实现SSH和RSH互通

（1）相关知识介绍

**SSH** 为 Secure SHell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定，它是建立在应用层和传输层基础上的一种安全通信协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

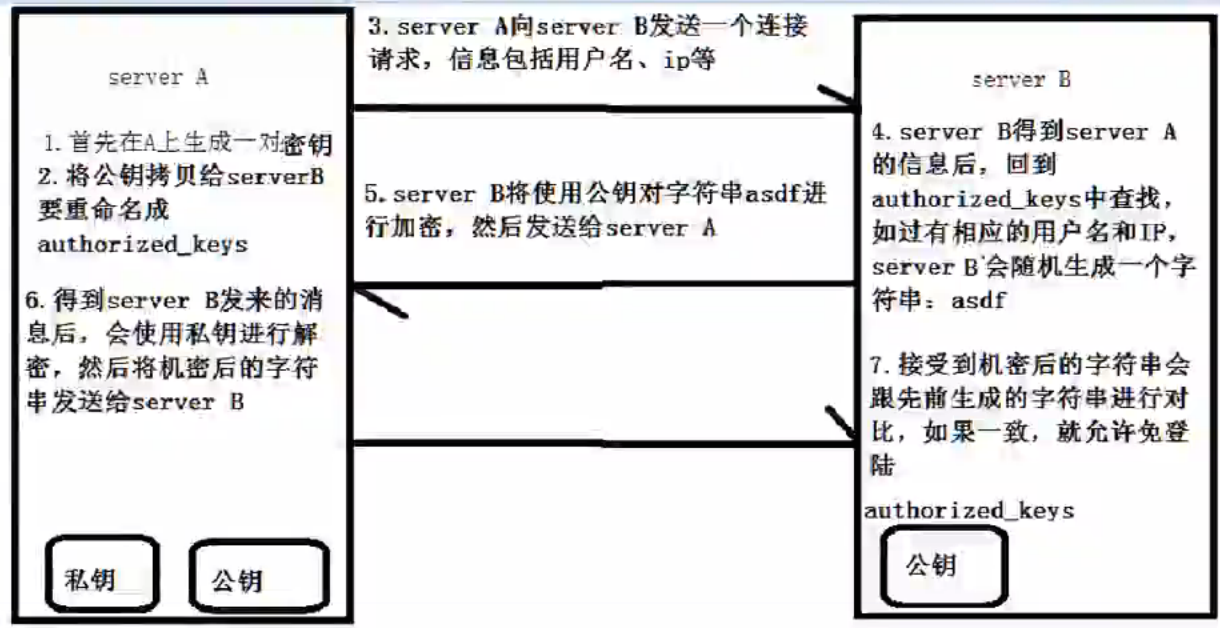
**RSH**是Remote SHell的缩写，该命令在指定的远程主机上启动一个shell并执行用户在rsh命令行中指定的命令；如果用户没有给出要执行的命令，rsh就用rlogin命令使用户登录到远程机上。

（2）SSH无密码互访配置

**知识预备：**

ssh无密码验证原理：节点A要实现无密码公钥认证连接到节点B上时，节点A是客户端，节点B是服务端，需要在客户端A上生成一个密钥对，包括一个公钥和一个私钥，而后将公钥复制到服务端B上。当客户端A通过ssh连接服务端B时，服务端B就会生成一个随机数并用客户端A的公钥对随机数进行加密，并发送给客户端A。客户端A收到加密数之后再用私钥进行解密，并将解密数回传给B，B确认解密数无误之后就允许A进行连接了。这就是一个公钥认证过程，其间不需要用户手工输入密码。重要过程是将客户端A公钥复制到B上。

总之：A要免密码登录到B，B首先要拥有A的公钥，然后B要做一次加密验证。对于非对称加密，公钥加密的密文不能公钥解开，只能私钥解开。



（3）配置步骤（该实验需要root权限）

1. 检查是否安装了SSH软件包：

|  |
| --- |
| **yum list installed | grep ssh** |

1. 当然，一般情况下CentOS会默认安装OpenSSH，再检查ssh服务是否启用：

|  |
| --- |
| **systemctl list-units --type=service | grep network** |

若显示不是running，启动：

|  |
| --- |
| **systemctl start sshd** |

开机自启动：

|  |
| --- |
| **systemctl enable sshd** |

1. 令每台虚拟机各自生成密钥对，将各自的公钥传到同一台虚拟机中合并生成key，具体步骤如下：
2. 同时打开虚拟机，修改每台虚拟机的ssh配置文件：

|  |
| --- |
| **vi /etc/ssh/sshd\_config** |

1. 找到下列行 去掉注释符号#：

|  |
| --- |
| **PubkeyAuthentication yes （允许公钥认证）**  **AuthorizedKeysFile .ssh/authorized\_keys（公钥存放在.ssh/** **authorized\_keys文件中）** |

1. 修改后需要重启ssh：

|  |
| --- |
| **systemctl restart sshd** |

1. 分别在每台虚拟机上生成密码对，以下所有操作都在root用户下进行(可根据自己实际情况选择非root用户)，运行命令：

|  |
| --- |
| **ssh-keygen -t rsa** |

此命令可在默认路径~/.ssh/下生成私钥id\_rsa公钥id\_rsa.pub，用ls -a 可以查看.ssh目录

1. 使用

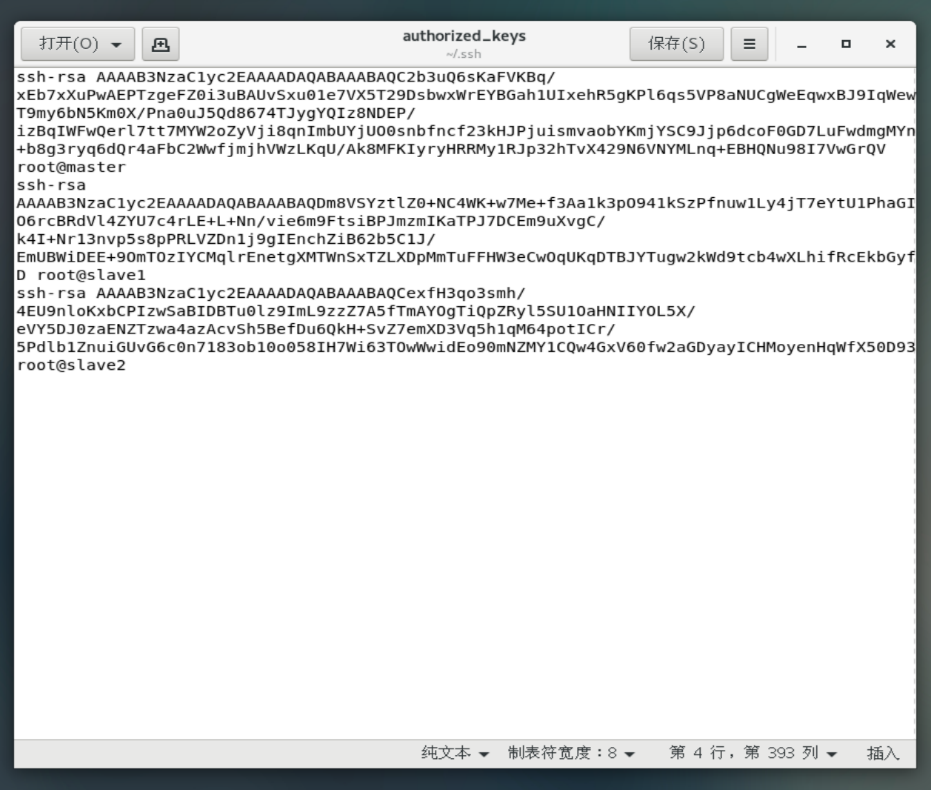
|  |
| --- |
| **scp id\_rsa.pub root@master:/root/.ssh/ id\_rsa.pub.slave1** |

来实现将公钥传至主机（在slave1上操作时，向master发送公钥，为了不与master的公钥重复，因此在最后加上.slave1作为标识，slave2同理）将其都传入主机是为了生成authorized\_keys文件，包含所有机器的公钥。

1. 生成authorized\_keys：此时在master的/root/.ssh/ 至少应该有id\_rsa.pub.slave1 id\_rsa.pub.slave2和id\_rsa.pub三个文件，将三个公钥内容添加到同一文件authorized\_keys中具体执行以下命令：

|  |
| --- |
| **cd ~/.ssh/**  **cat id\_rsa.pub >> authorized\_keys**  **cat id\_rsa.pub.slave1 >> authorized\_keys**  **cat id\_rsa.pub.slave2 >> authorized\_keys** |

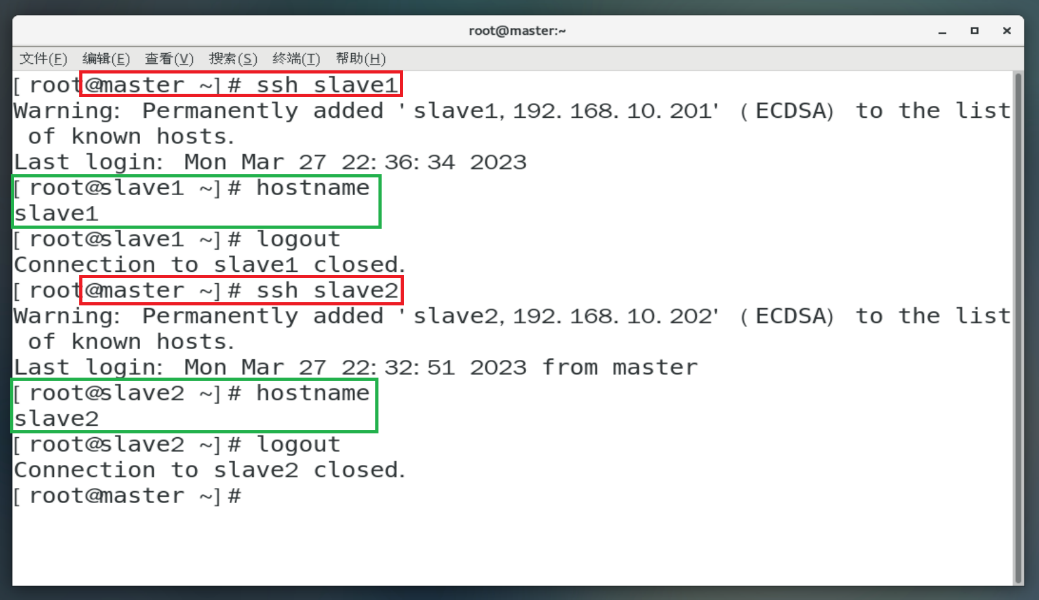
效果如下图所示：



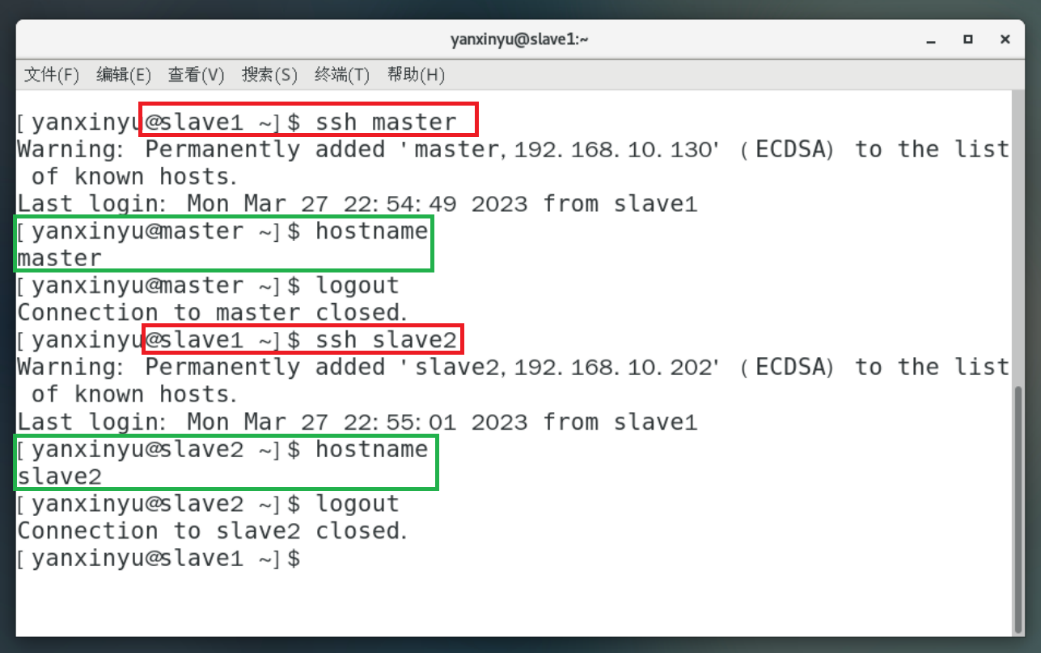
1. 此时，拥有该文件的虚拟机可以被另两台虚拟机直接登录，实现了ssh无密码验证互通，将此文件发送给slave1和slave2的/root/.ssh后，使三台虚拟机用root用户可以相互直接登录：

|  |
| --- |
| **scp authorized\_keys slave1:/root/.ssh/authorized\_keys**  **scp authorized\_keys slave2:/root/.ssh/authorized\_keys** |

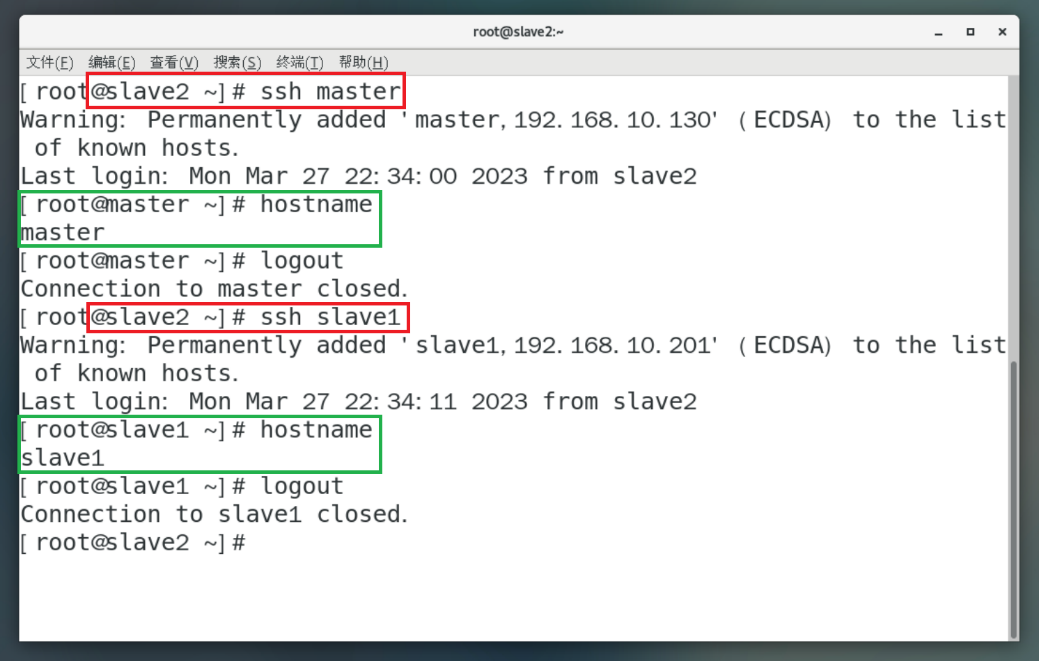
1. 此时在master或slave2的terminal中输入ssh slave1，便可登录slave1，以此类推。展示如下：



master ssh slave1、slave2



slave1 ssh master、slave2



slave2 ssh master、slave1

1. 当然，步骤8-11可以用Linux的ssh-copy-id命令快速实现，个人在实验中也首先使用了此方法。可参考：https://zhuanlan.zhihu.com/p/493460491



注意：由于之前已配置过hosts，因此user@server处只要填写master、slave1、slave2即可

#### 使用SSH实现Windows主机与Linux虚拟机文件互传

**注意：**

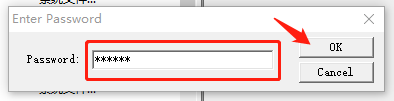
* 下载安装SSH Secure Shell Client 3.2.9 <http://xiazai.zol.com.cn/detail/38/372685.shtml>
* 在实现互传文件之前先要令主机（此处使用windows 10）和虚拟机ping通
* 在cmd中输入ipconfig查看本机ip，在terminal中输入ifconfig查看虚拟机ip

1. 关闭Windows防火墙
2. 更改虚拟网卡设置 在NAT的连接方式下，要使主机能够ping通虚拟机，需要保证VMnet8虚拟网卡的ip地址和虚拟机的ip地址在同一网段中。打开网络与共享中心，更改适配器设置，找到VMnet8（对应NAT）设置其ipv4属性，将其修改至于虚拟机ip属于同一网段
3. 此时主机与虚拟机应当能够相互ping通，打开SSH Secure Shell Client，点击Quick Connect，在Host name中输入虚拟机ip，在User name中输入用户名（注意：不是主机名），点击connect，输入密码，成功登录的标志为显示类似terminal中的输入提示符

注意：具体ip地址按照实际情况输入。

图形用户界面, 文本, 应用程序

描述已自动生成





1. 点击window->SSH Secure File Transfer进入文件传输界面，左边为本机文件目录，右边为虚拟机的文件目录，可直接拖拽复制

图形用户界面, 应用程序

描述已自动生成图形用户界面, 文本, 应用程序

描述已自动生成

#### RSH互通（选做）

RSH配置参考文献：

<https://blog.csdn.net/weixin_45450312/article/details/119888383>

<https://blog.csdn.net/qq_51401253/article/details/123465029>

1. 安装相关服务

​rsh是需要先安装的，使用yum -y install rsh rsh-server安装相关服务，使用rpm -qa | grep rsh检查是否安装成功，使用service xinetd restart启动rsh服务。而在这里如果报错提示不知道什么是xinetd，则说明你没有安装xinetd，使用yum install -y xinetd命令进行安装即可。

1. 添加相关配置文件：在目录/etc/xinetd.d/下分别添加rsh,rlogin,rexec文件，其中文件内容为(重点在于保证disable = no)：

|  |
| --- |
| **#rsh**  **service shell {**  **disable = no**  **socket\_type = stream**  **wait = no**  **user = root**  **log\_on\_success += USERID**  **log\_on\_failure += USERID**  **server = /usr/sbin/in.rshd**  **}**  **#rlogin**  **service login {**  **disable = no**  **socket\_type = stream**  **wait = no**  **user = root**  **log\_on\_success += USERID**  **log\_on\_failure += USERID**  **server = /usr/sbin/in.rlogind**  **}**  **#rexec**  **service exec {**  **disable = no**  **socket\_type = stream**  **wait = no**  **user = root**  **log\_on\_success += USERID**  **log\_on\_failure += USERID**  **server = /usr/sbin/in.rexecd**  **}** |

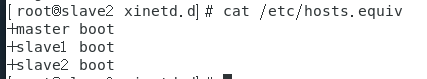
1. 然后在目录/etc/securetty中添加rexec,rsh,rlogin，可以直接打开添加，也可以通过命令

|  |
| --- |
| **echo "rsh" >> /etc/securetty**  **echo "rlogin" >> /etc/securetty**  **echo "rexec" >> /etc/securetty** |

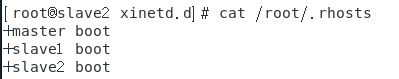
具体效果如下所示：



1. 在目录/etc/hosts.equiv下添加其余虚拟机信息



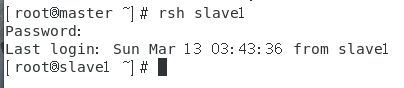
1. 在/root/下创建.rhosts文件，文件内容和/etc/hosts.equiv相同

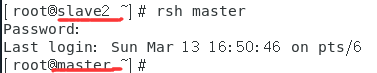


1. 执行下列命令启动服务

|  |
| --- |
| **systemctl restart rsh.socket**  **systemctl restart rlogin.socket**  **systemctl restart rexec.socket**  **systemctl enable rsh.socket**  **systemctl enable rlogin.socket**  **systemctl enable rexec.socket** |

1. 启动xinetd,使用命令systemctl restart xinetd，然后通过rsh命令就可以实现接入其他的虚拟机了





# 三、附件（VIM简介）

参考：<https://www.runoob.com/linux/linux-vim.html>

要求：要求熟悉使用vim及使用VIM编写一个c程序并输出“hello Word”；

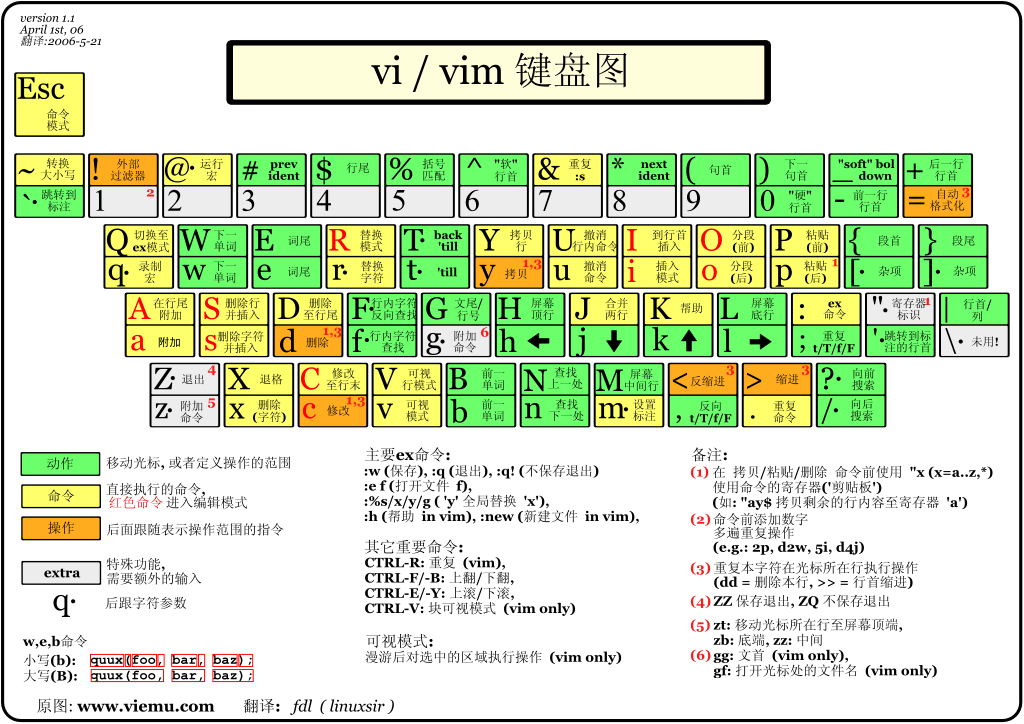
#### 什么是 vim？

Vim是从vi发展出来的一个文本编辑器。代码补完、编译及错误跳转等方便编程的功能特别丰富，在程序员中被广泛使用。

简单的来说，vi是老式的字处理器，不过功能已经很齐全了，但是还是有可以进步的地方。vim则可以说是程序开发者的一项很好用的工具。

连vim的官方网站([http://www.vim.org](http://www.vim.org/))自己也说vim是一个程序开发工具而不是文字处理软件。

vim键盘图：



#### vi/vim 的使用

基本上 vi/vim 共分为三种模式，分别是**命令模式（Command mode）**，**输入模式（Insert mode）**和**底线命令模式（Last line mode）**。 这三种模式的作用分别是：

【命令模式】

用户刚刚启动 vi/vim，便进入了命令模式。

此状态下敲击键盘动作会被Vim识别为命令，而非输入字符。比如我们此时按下i，并不会输入一个字符，i被当作了一个命令。

以下是常用的几个命令：

* **i** 切换到输入模式，以输入字符。
* **x** 删除当前光标所在处的字符。
* **:** 切换到底线命令模式，以在最底一行输入命令。

若想要编辑文本：启动Vim，进入了命令模式，按下i，切换到输入模式。

命令模式只有一些最基本的命令，因此仍要依靠底线命令模式输入更多命令。

【输入模式】

在命令模式下按下i就进入了输入模式。

在输入模式中，可以使用以下按键：

* 字符按键以及Shift组合，输入字符
* ENTER，回车键，换行
* BACK SPACE，退格键，删除光标前一个字符
* DEL，删除键，删除光标后一个字符
* 方向键，在文本中移动光标
* HOME/END，移动光标到行首/行尾
* Page Up/Page Down，上/下翻页
* Insert，切换光标为输入/替换模式，光标将变成竖线/下划线
* ESC，退出输入模式，切换到命令模式

【底线命令模式】

在命令模式下按下:（英文冒号）就进入了底线命令模式。

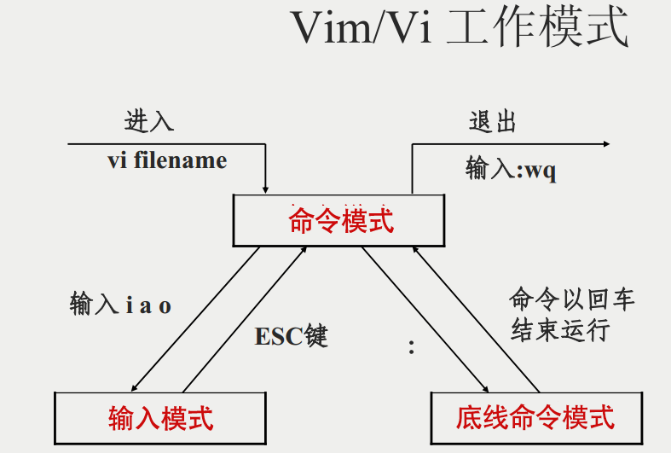
底线命令模式可以输入单个或多个字符的命令，可用的命令非常多。

在底线命令模式中，基本的命令有（已经省略了冒号）：

* q 不保存退出程序
* w 保存文件
* wq 保存并退出
* q! 不保存修改并推出

按ESC键可随时退出底线命令模式。

简单的说，我们可以将这三个模式想成底下的图标来表示：

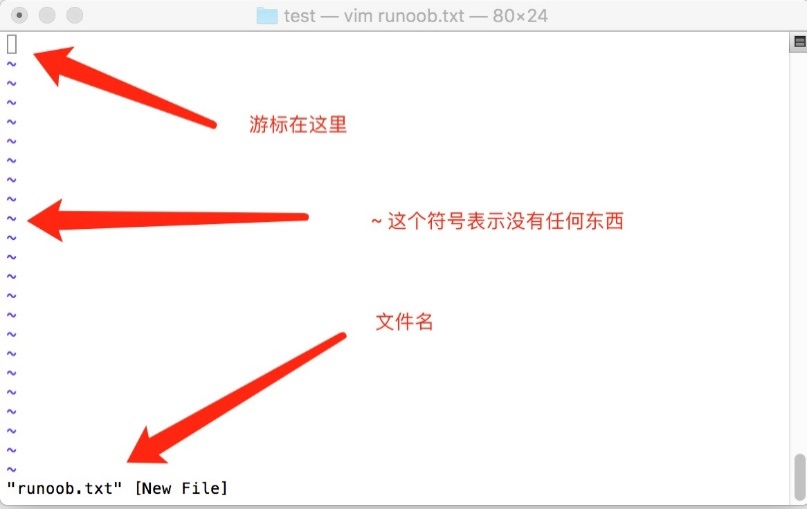


#### vi/vim 使用实例

【使用 vi/vim 进入一般模式】

如果你想要使用vi来建立一个名为test.txt的文件时，你可以这样做：

直接输入**vi 文件名，**就能够进入vi的一般模式了。请注意，记得vi后面一定要加文件名，不管该文件存在与否！



【按下i进入输入模式(也称为编辑模式)，开始编辑文字】

在一般模式之中，只要按下 i, o, a 等字符就可以进入输入模式了！

在编辑模式当中，你可以发现在左下角状态栏中会出现 –INSERT- 的字样，那就是可以输入任意字符的提示。

这个时候，键盘上除了 **Esc** 这个按键之外，其他的按键都可以视作为一般的输入按钮了，所以你可以进行任何的编辑。

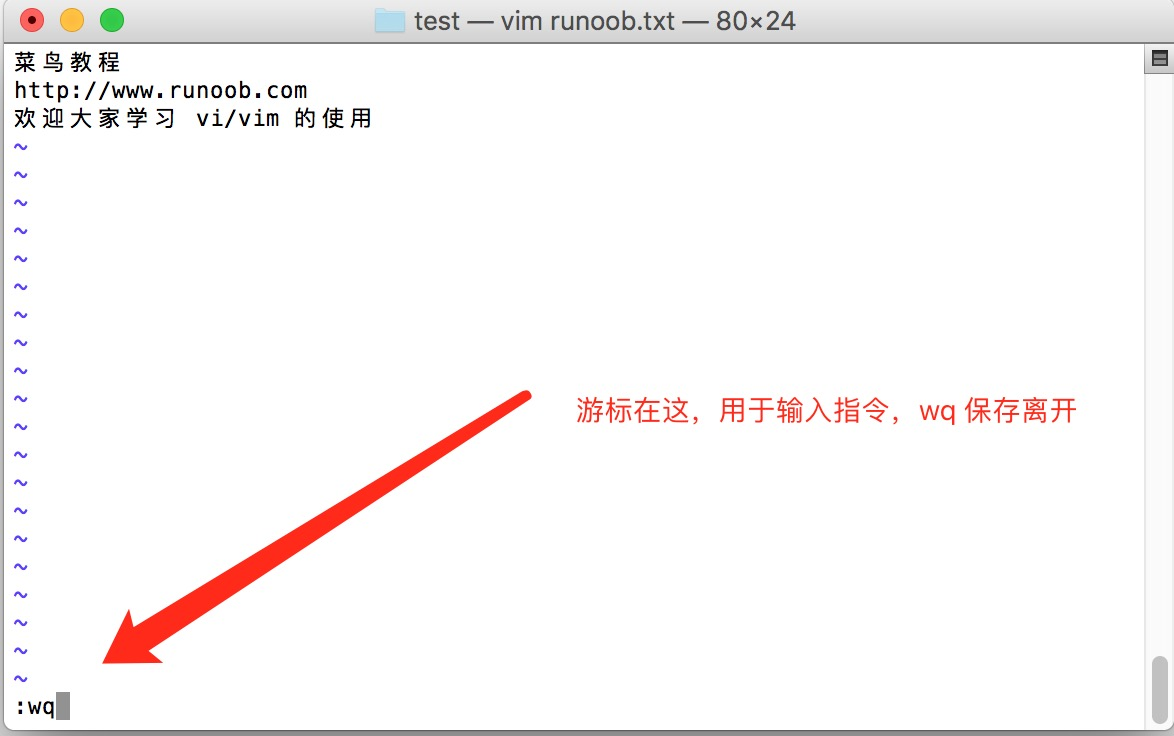


【按下ESC按钮回到一般模式】

好了，假设我已经按照上面的样式给他编辑完毕了，那么应该要如何退出呢？是的！没错！就是给他按下 **Esc** 这个按钮即可！马上你就会发现画面左下角的 – INSERT – 不见了！

【在一般模式中按下 :wq 储存后离开 vi】

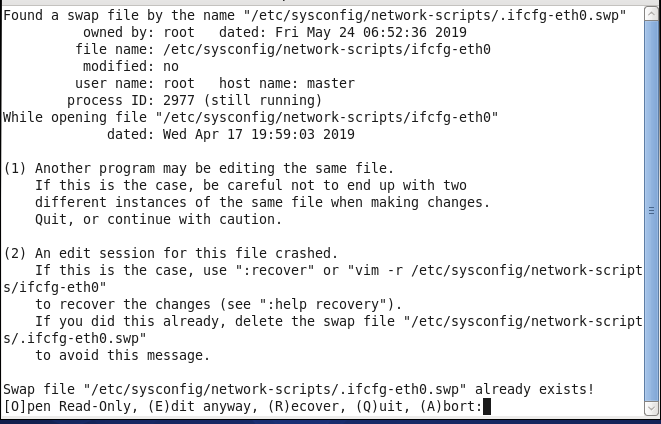
OK，我们要存档了，存盘并离开的指令很简单，输入 **:wq** 即可保存离开！



OK! 这样我们就成功创建了一个 runoob.txt 的文件。

#### 注意

* 如果当该文件在指定目录下存在，则会直接打开该文件，如果不存在则会先创建该文件并打开
* 在Linux系统中，使用vim的时候如果是非正常关闭，则会有一份以“.”开头且以“.swp”结尾的隐藏文件，当再次使用vim 打开该文件的时候，会出现下图z1所示的提示，可以输入“o”代表只读模式打开，输入“e“则表示直接编译，”q”表示退出当前界面，“r”表示恢复，此外更加直接的解决方式是，直接删除该交换文件，重新打开编辑即可。



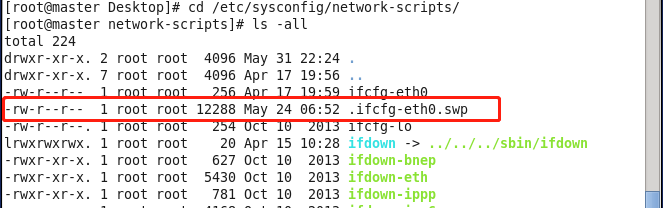
下面介绍删除对应的交换文件方式：

1. 首先进入对应的文件夹目录下下面

[root@master Desktop]# cd /etc/sysconfig/network-scripts/

1. 找到对应的交换文件：

[root@master Desktop]# ls -all



1. 然后使用root 用户删除对应的交换文件：

[root@master network-scripts]# rm -r .ifcfg-eth0.swp

文本

描述已自动生成

在删除的时候会询问是否要删除该文件，输入“y”表示确认删除，“n”表示取消删除