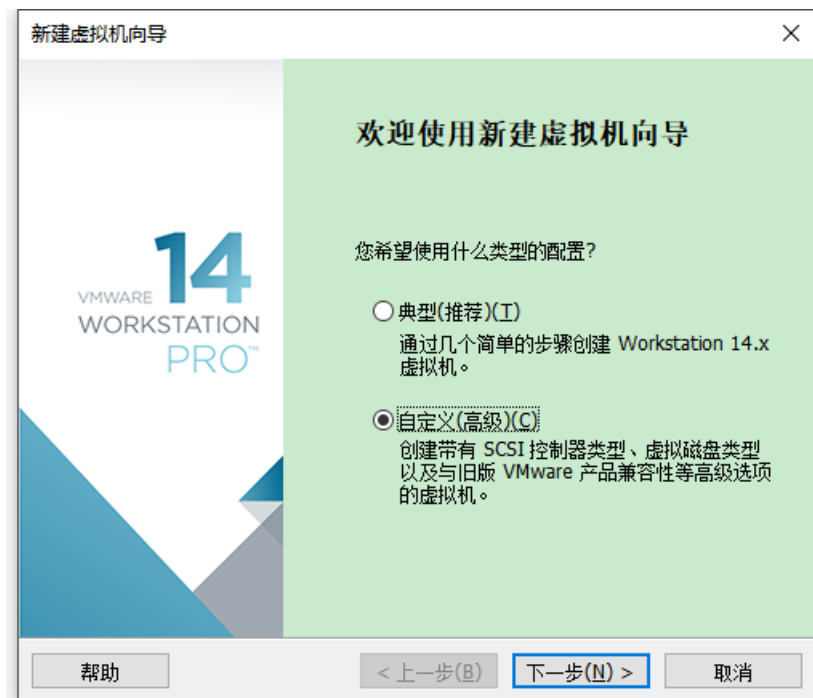


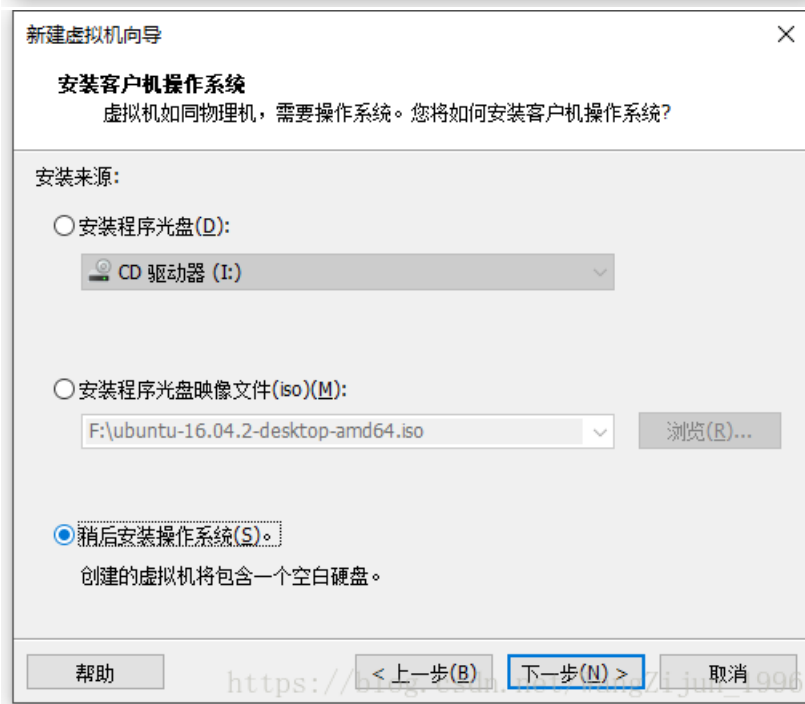
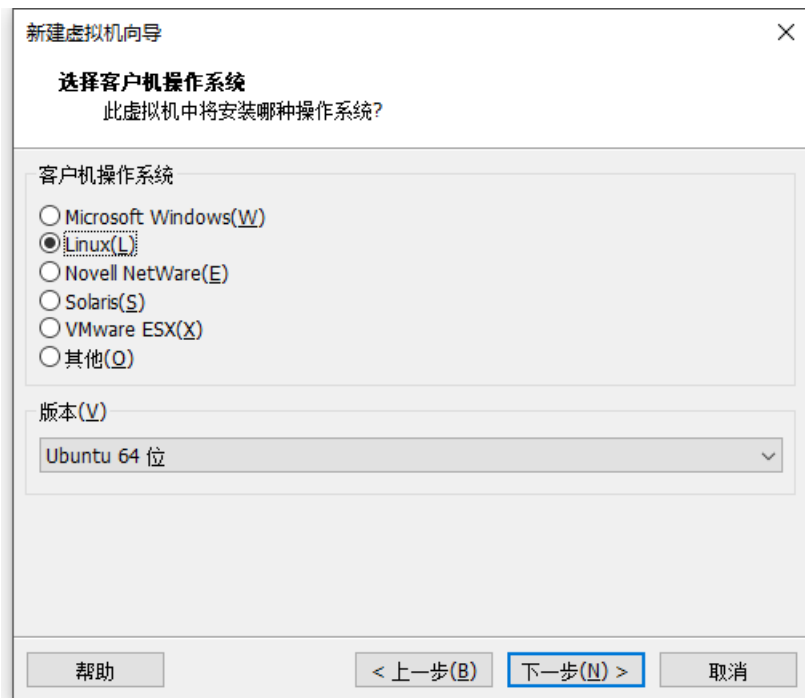
记录下 ubuntu 虚拟机系统环境配置过程

下载 iso 镜像（不建议官网下载，速度慢，并且新版不好用）

之后在 VMware 中创建一个虚拟机

下图





新建虚拟机向导

命名虚拟机

您希望该虚拟机使用什么名称?

虚拟机名称(V):

Ubuntu 64 位

位置(L):

C:\Users\Administrator\Documents\Virtual Machines\Ubuntu 64 位

浏览(B)...

在“编辑”>“首选项”中可更改默认位置。

< 上一步(B)

下一步(N) >

取消

新建虚拟机向导

处理器配置

为此虚拟机指定处理器数量。

处理器

处理器数量(P):

1

每个处理器的内核数(C):

1

处理器内核总数:

1

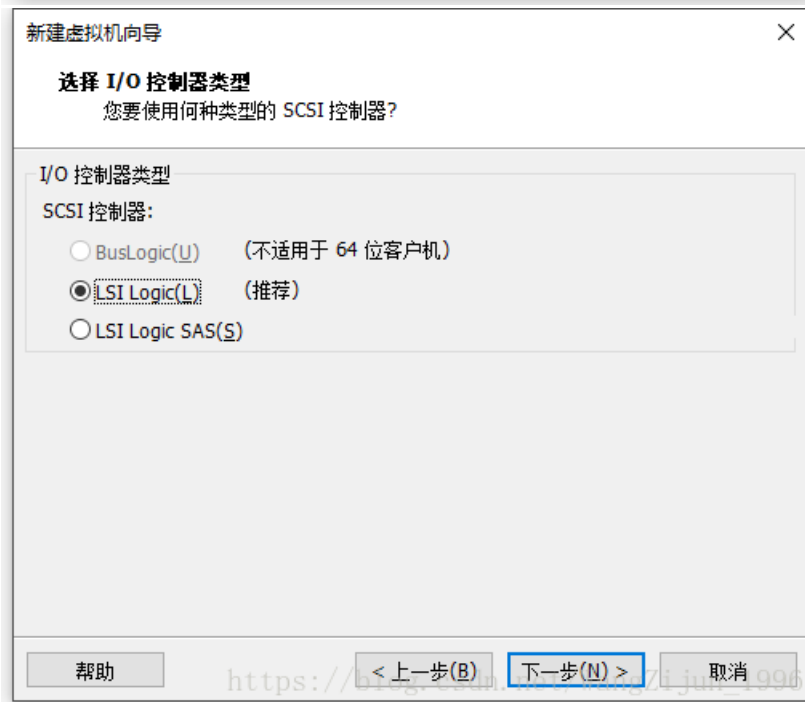
帮助

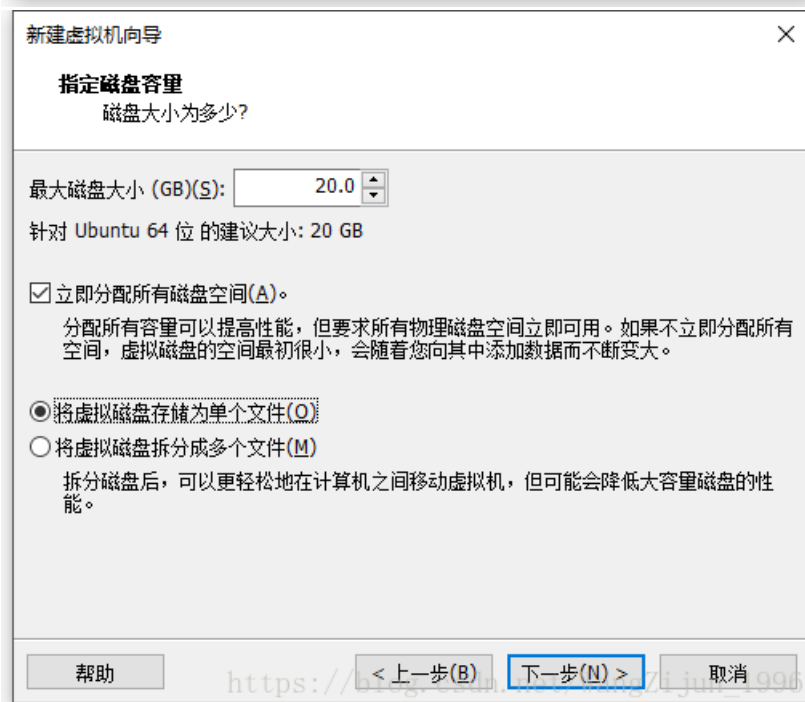
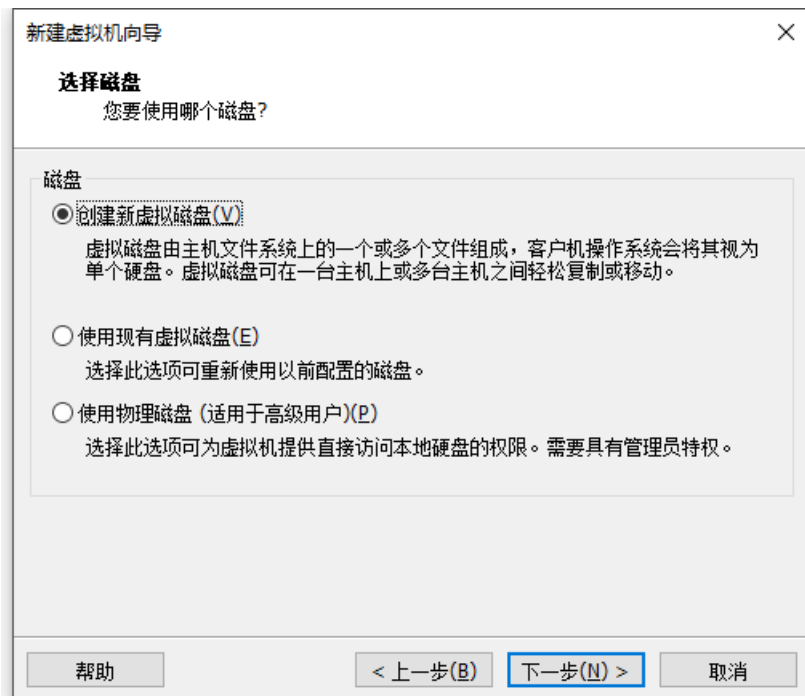
< 上一步(B)

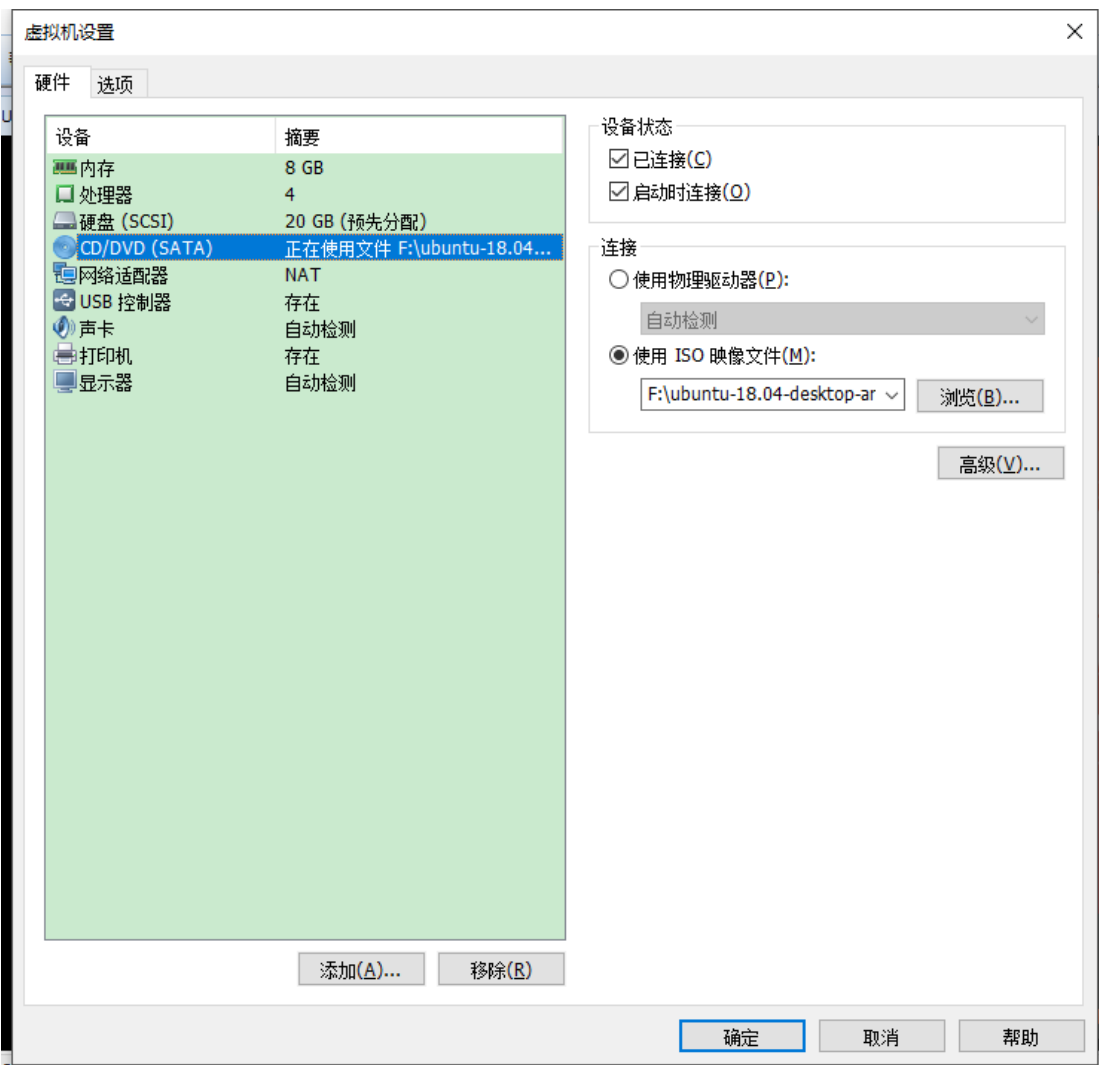
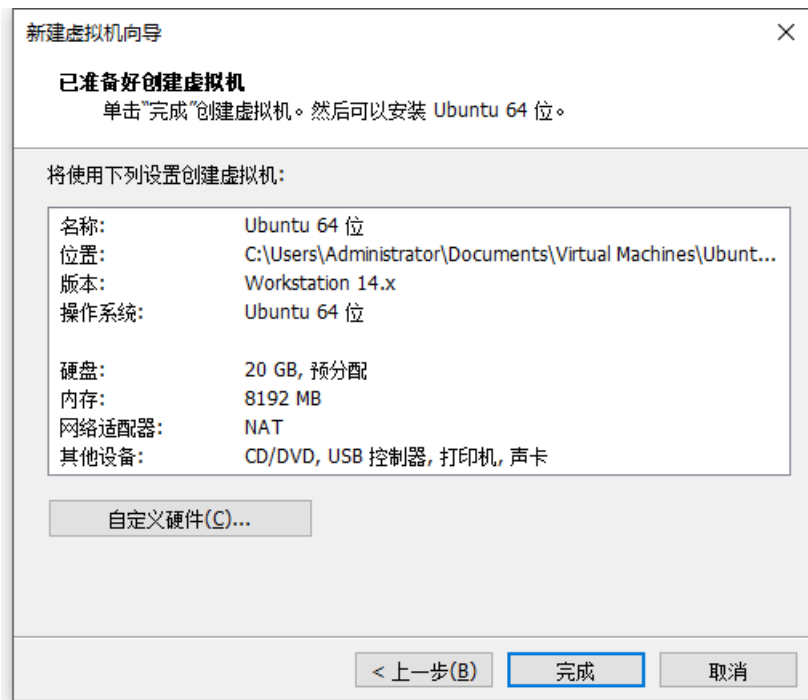
下一步(N) >

取消

https://blog.csdn.net/qq_34447966





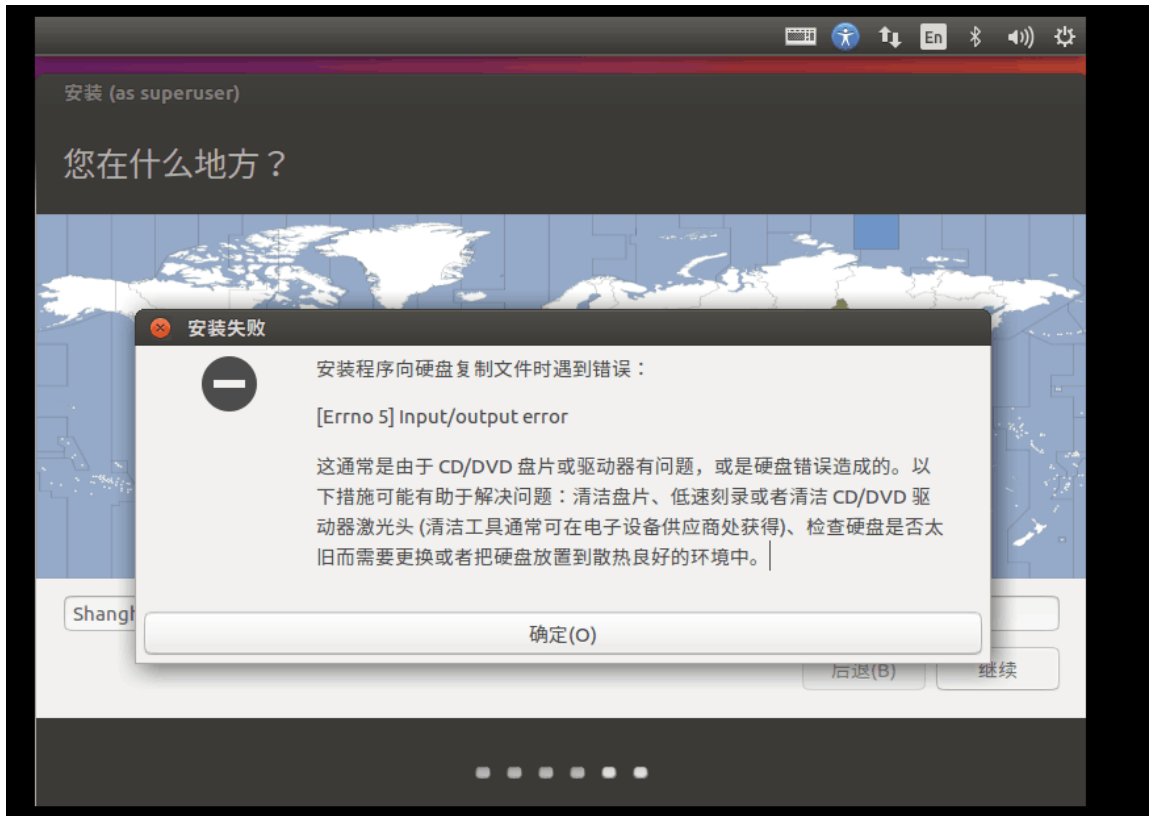


记得添加一下镜像文件

接下来直接开启虚拟机会自动进入安装

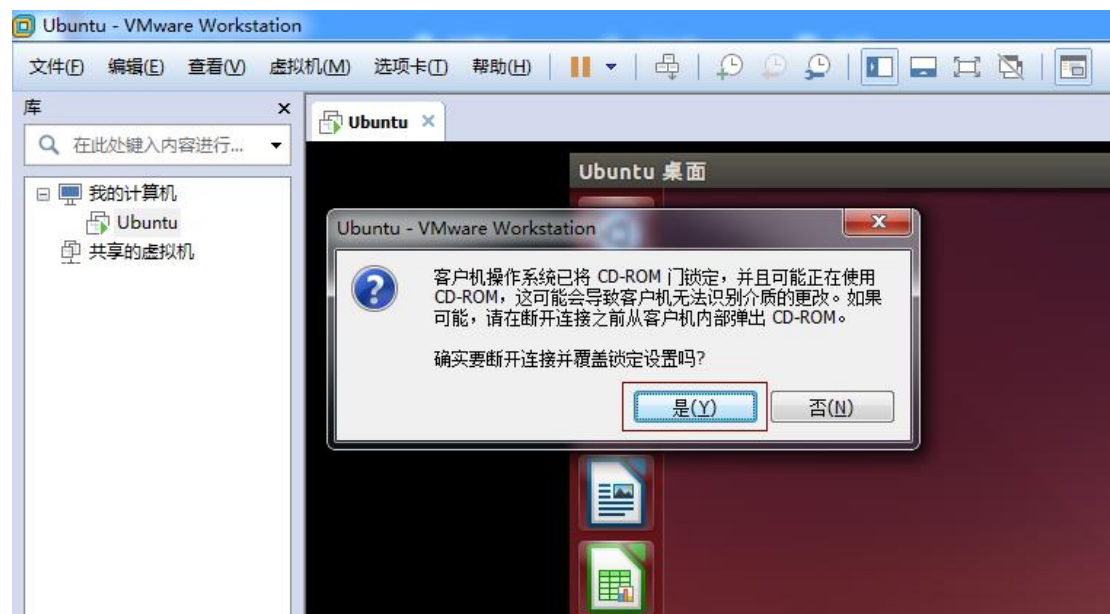
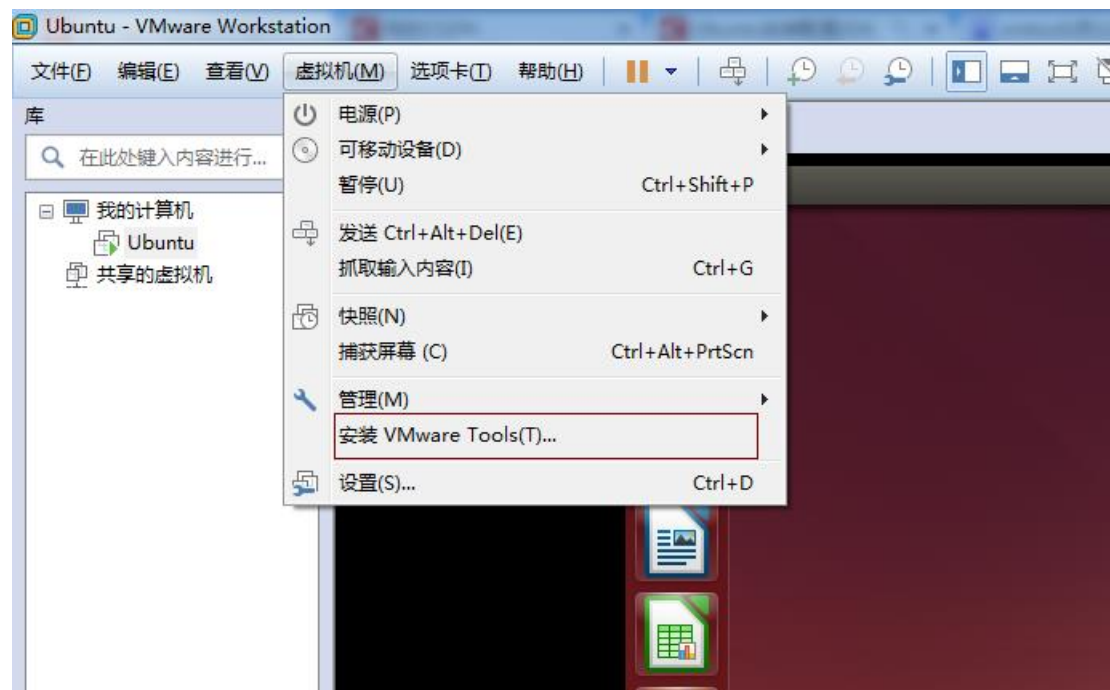


之后一个点继续，应该就没有问题
安装时我遇到一个问题

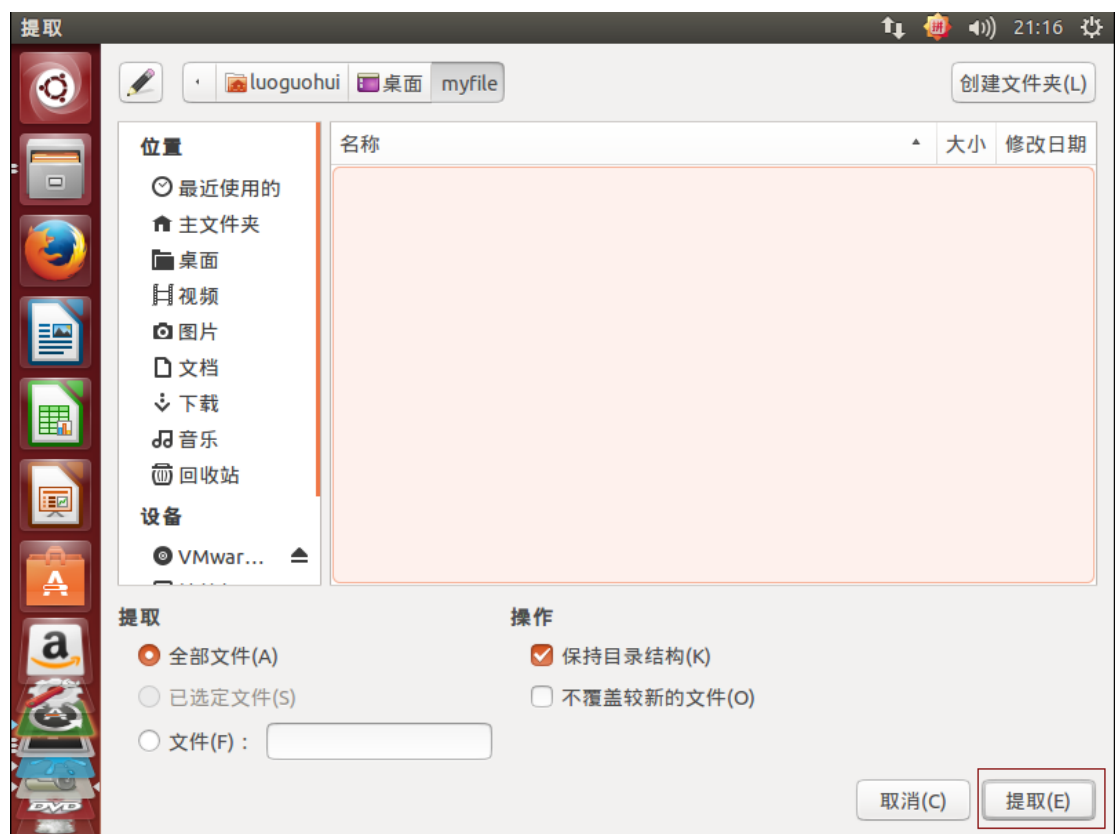
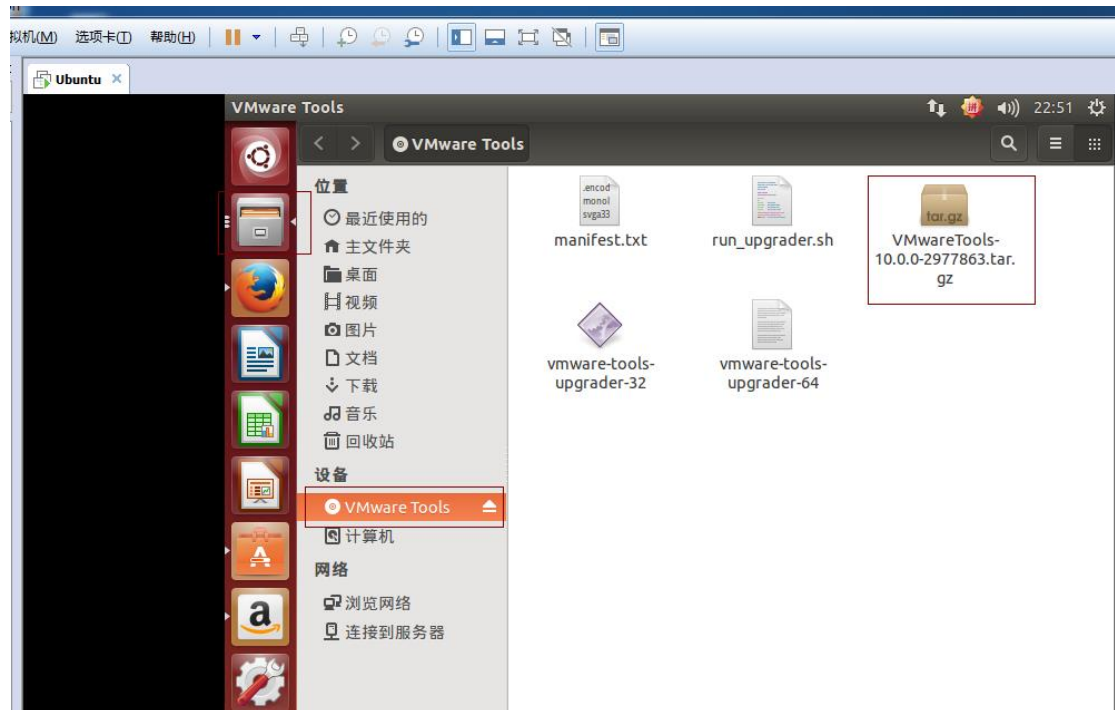


这里还没找到很好的方法解决，建议重新找个镜像下载，然后问题完美解决

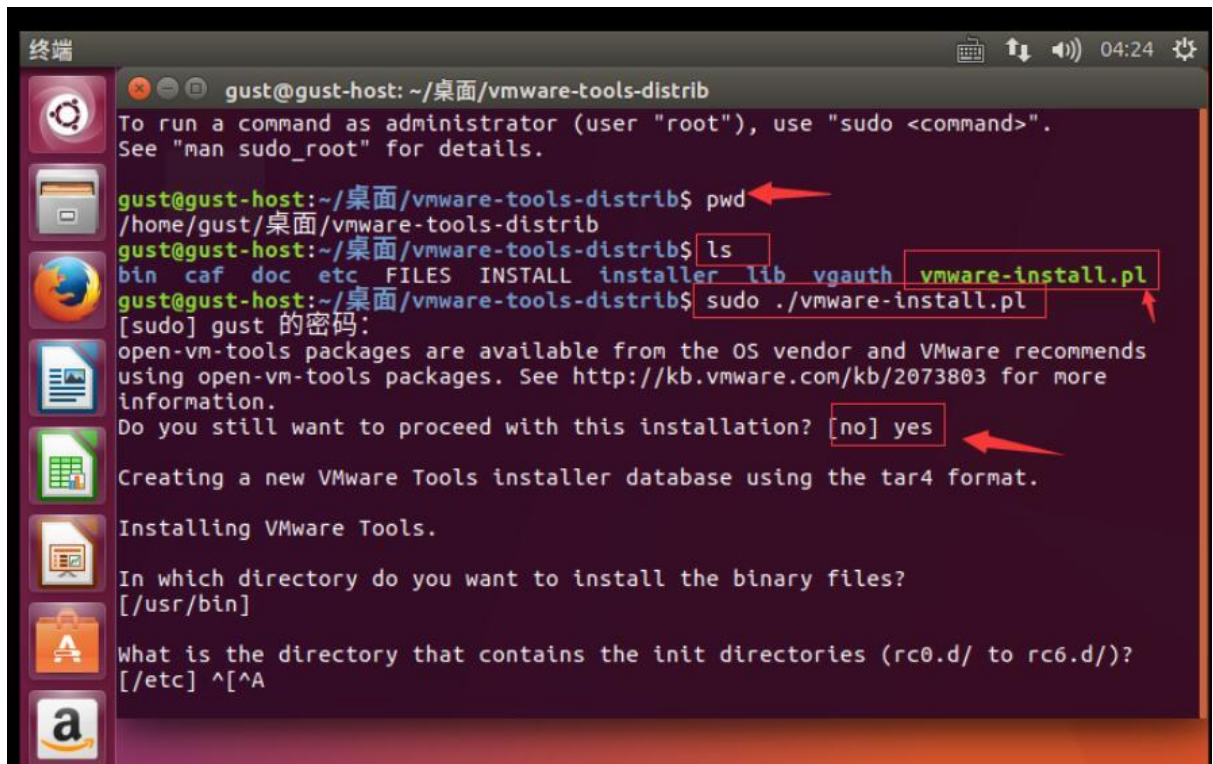
接下来是安装 VMware tools，主要是方便以后使用



在这里我又出了问题,我打开 VMware tools 时发现没有这个包,解决方法是将之前的 CD/DVD 移除之后,问题也得到解决



之后桌面上就多了这个文件，下面将文件在终端里打开
输入 ls 可以看见文件回车，然后 `sudo ./vmware-install.pl`
登陆，在第一个 NO 之后输入 yes，接下来一直回车直到出现 enjoy，安装成功，重启系统。

A terminal window titled '终端' (Terminal) showing the installation of VMware Tools. The user is 'gust' on a host named 'gust-host'. The current directory is '~/桌面/vmware-tools-distrib'. The terminal shows the following commands and outputs:
1. `pwd` returns `/home/gust/桌面/vmware-tools-distrib`.
2. `ls` lists the contents: `bin caf doc etc FILES INSTALL installer lib vgauth vmware-install.pl`.
3. `sudo ./vmware-install.pl` is executed. A password prompt is shown, and the user enters their password.
4. A message states: 'open-vm-tools packages are available from the OS vendor and VMware recommends using open-vm-tools packages. See http://kb.vmware.com/kb/2073803 for more information.'
5. A prompt asks: 'Do you still want to proceed with this installation?' with '[no] yes' as options. The user selects 'yes'.
6. A message says: 'Creating a new VMware Tools installer database using the tar4 format.'
7. A message says: 'Installing VMware Tools.'
8. A prompt asks: 'In which directory do you want to install the binary files?' with `[/usr/bin]` as the default.
9. A prompt asks: 'What is the directory that contains the init directories (rc0.d/ to rc6.d/)?' with `[/etc] ^[^A` as the default.
The terminal window has a sidebar with icons for various applications like a file manager, web browser, and terminal.

接下来就是配置 pwntools 环境，配置时我都快哭了，配置问题太多了。

首先是安装 git

这是命令 **`sudo apt-get install git`**

接着是安装 capston

命令 **`git clone https://github.com/aquynh/capstone`**

切换到其目录 `cd capstone`

安装

`make`

`sudo make install`

还需要安装 pip

`sudo apt-get install python-pip`(当然如果你版本在 16.04 之上可以省略 get)

配置 python 环境

`sudo apt-get install python-pip python-dev build-essential`

之后在这里我就遇见一个问题输入命令

`sudo pip install --upgrade pip` 时会显示我 pip 的版本不够（虽然这条语句就是来升级 pip 的）如果有同样问题，可以更新 ubuntu 系统，之前我下的时候用的是 ubuntu16.04，现在更新到 18.04 这样 pip 也就可以升级了

系统更新操作如下

`sudo apt-get update` 更新资源

`sudo apt-get upgrade` 对软件进行升级

`sudo apt-get dist-upgrade` 对系统的升级

输入命令

`sudo reboot` 重启系统

`sudo apt-get update`

`sudo update-manager -c -d` 检测更新

这时我出现的是软件升级

如果不行的话可以换个命令将前面的-d 去掉

应该就可以了

系统更新有点长，差不多两小时

然后我们回到之前一步

```
sudo pip install --upgrade pip
```

应该可以升级成功了

```
sudo pip install --upgrade virtualenv
```

最后就是

```
pip install pwntools
```

这里可能还会出现权限不够的问题

```
s ropgadget filelock pycparser
Installing collected packages: capstone, sortedcontainers, intervaltree, Markup
Safe, mako, pyparsing, packaging, pycparser, cffi, pynacl, pyasn1, bcrypt, para
miko, psutil, pyelftools, pygments, pypandoc, pyserial, pysocks, python-dateuti
l, urllib3, certifi, chardet, requests, ropgadget, filelock, pluggy, py, toml,
tox, unicorn, pwntools
Could not install packages due to an EnvironmentError: [Errno 13] 权限不够: '/u
sr/local/lib/python2.7/dist-packages/capstone'
Consider using the '--user' option or check the permissions.
```

现在就需要获得 root 权限

```
rooter@rooter-virtual-machine:~$ sudo passwd root
输入新的 UNIX 密码:
重新输入新的 UNIX 密码:
passwd: 已成功更新密码
rooter@rooter-virtual-machine:~$ su
密码:
```

图中命令我们可以拥有命令权限

```
rooter@rooter-virtual-machine:~$ su
密码:
root@rooter-virtual-machine:/home/rooter# pip install pwntools
Collecting pwntools
  Downloading https://files.pythonhosted.org/packages/f2/d6/465061352e03a31b846
4fcbdb5a8d2240850a20d96c7727f274a80fe48d16/pwntools-3.12.1.tar.gz (2.0MB)
    100% |████████████████████████████████████████| 2.0MB 841kB/s
Collecting capstone>=3.0.5rc2 (from pwntools)
  Downloading https://files.pythonhosted.org/packages/8f/73/d763ec77f1a5b501b86
b654a940e7c08721f6382ba50618d6d21dac3e2dc/capstone-3.0.5.post1-py2.py3-none-man
ylinux1_x86_64.whl (1.6MB)
    100% |████████████████████████████████████████| 1.6MB 956kB/s
Collecting intervaltree (from pwntools)
  Downloading https://files.pythonhosted.org/packages/ca/c1/450d109b70fa58ca9d7
7972b02f69222412f9175ccf99fdeaf167be9583c/intervaltree-2.1.0.tar.gz
Collecting mako>=1.0.0 (from pwntools)
  Downloading https://files.pythonhosted.org/packages/eb/f3/67579bb486517c0d495
47f9697e36582cd19dafb5df9e687ed8e22de57fa/Mako-1.0.7.tar.gz (564kB)
    100% |████████████████████████████████████████| 573kB 10.3MB/s
```

重新输入刚才命令，环境配置成功，最后测试 import pwn，没有报错，然后测

试 asm 功能打开 python shell

直接在命令行输入 python 即可

```
>>> pwn.asm("xor eax,eax")
```

显示'1\x0'时成功