Creating
CentOS7.4 Virtual Machine

Csci E63 Big Data Analytics

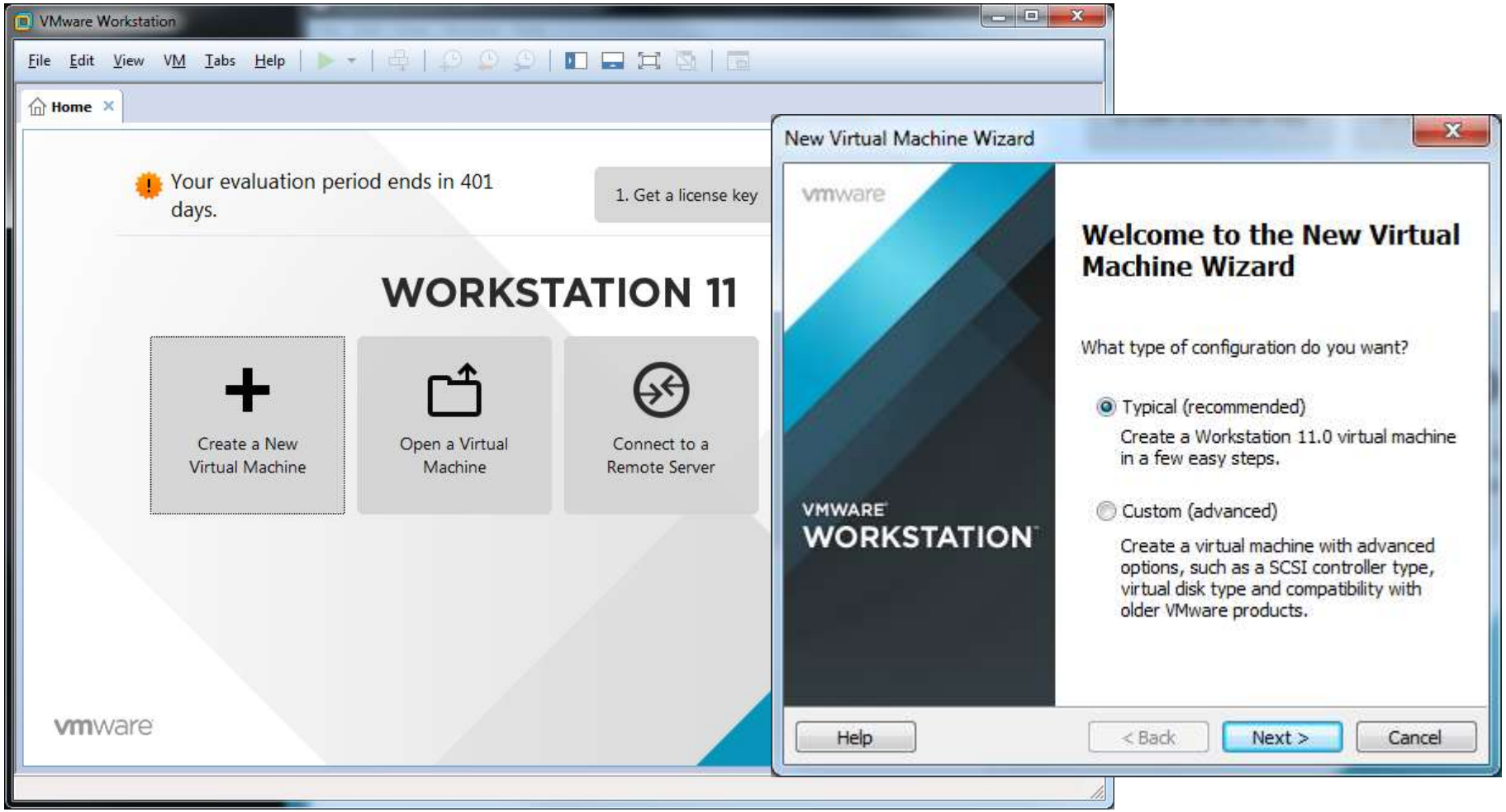
Zoran B. Djordjević

Download CentOS 7.4, Select a mirror near you

- Go to https://www.centos.org, select the button: GetCentOS Now.
- On the next screen select DVD ISO. This will give you a 4.5 GB download.
- If you know what you are doing you can work with either of other two distributions.
- With some downloads I got an impression that I have to burn the DVD and that CentOS would not install from an `iso` image. That might not be true on your machine.
- Normally, VMWare Workstation installs a Linux OS-s from an `iso` image.

Start VMware Workstation

- Select "`Create a New Virtual Machine`".
- Accept Custom, Next >

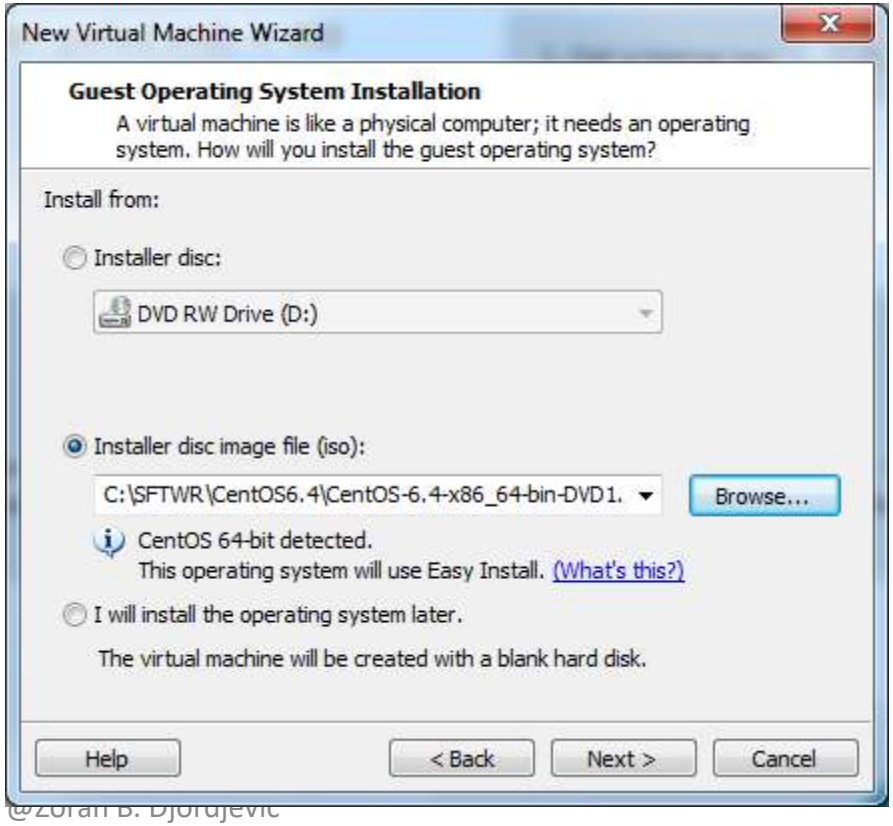


Guest Operating System Installation

- Check “Installer disc image file (iso):” and
- Select download CentOS 7.4 ISO file. In my case the file is:

`E:\Zoran\Software\CentOS\CentOS-7-x86_64-DVD-1708.iso`

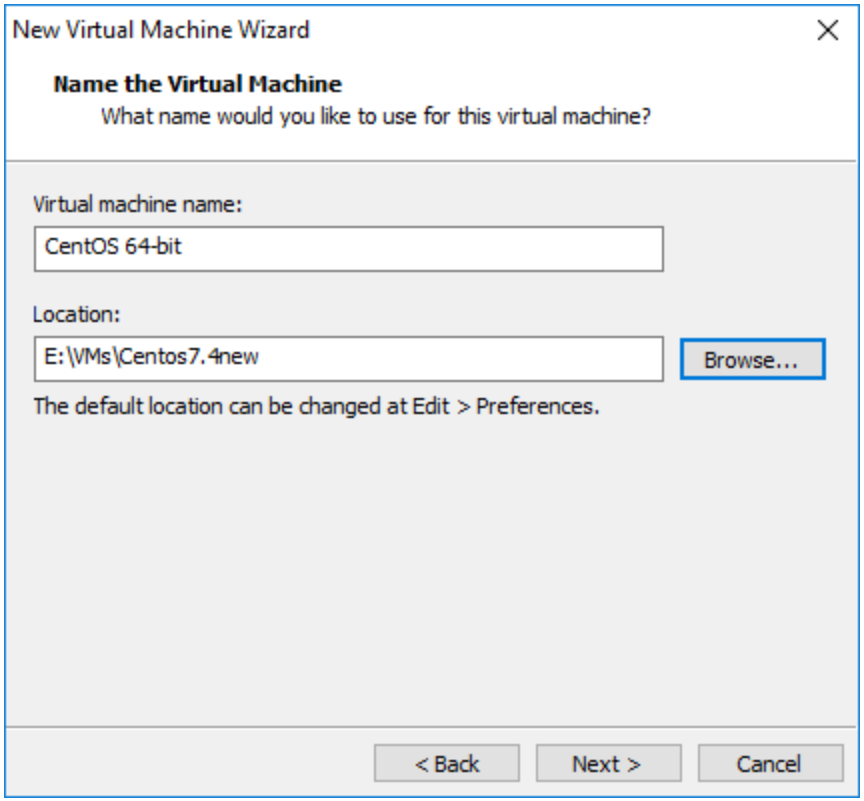
- Select `Next >`
- If VMWare Workstation accepts to read your `iso` file, it is faster and safer to use that `iso` file, as depicted on in the image on the below, than to burn the DVD first.



Name your VM, create a folder

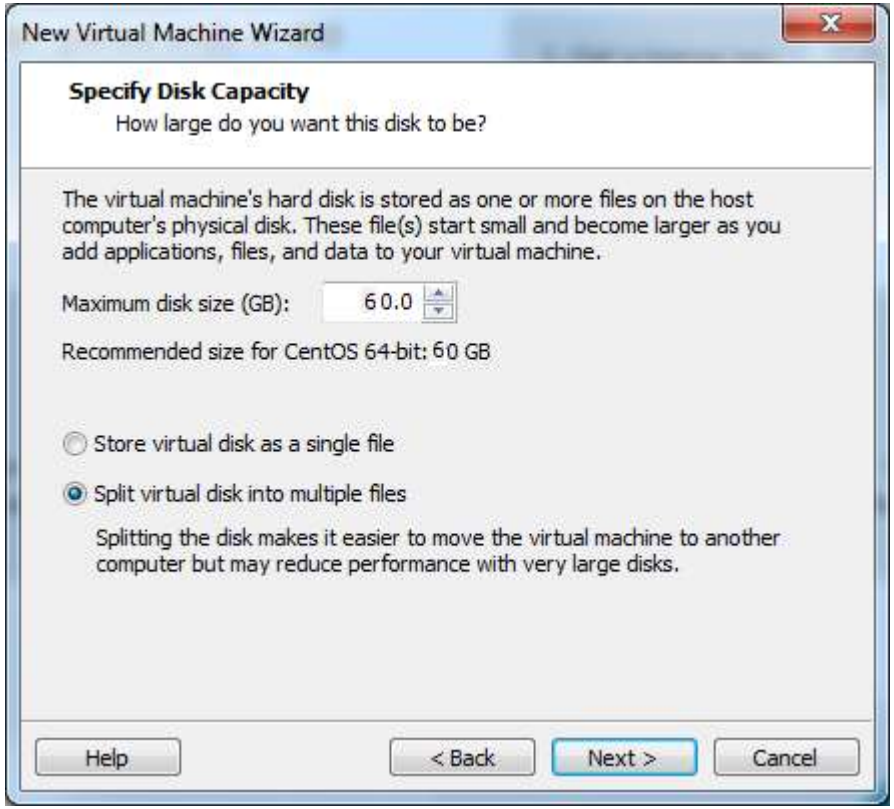
- Name you VM and create a folder where to store its component files.
- You can place you VM anywhere, including a thumb drive or a USB external drive.

- Hit Next>



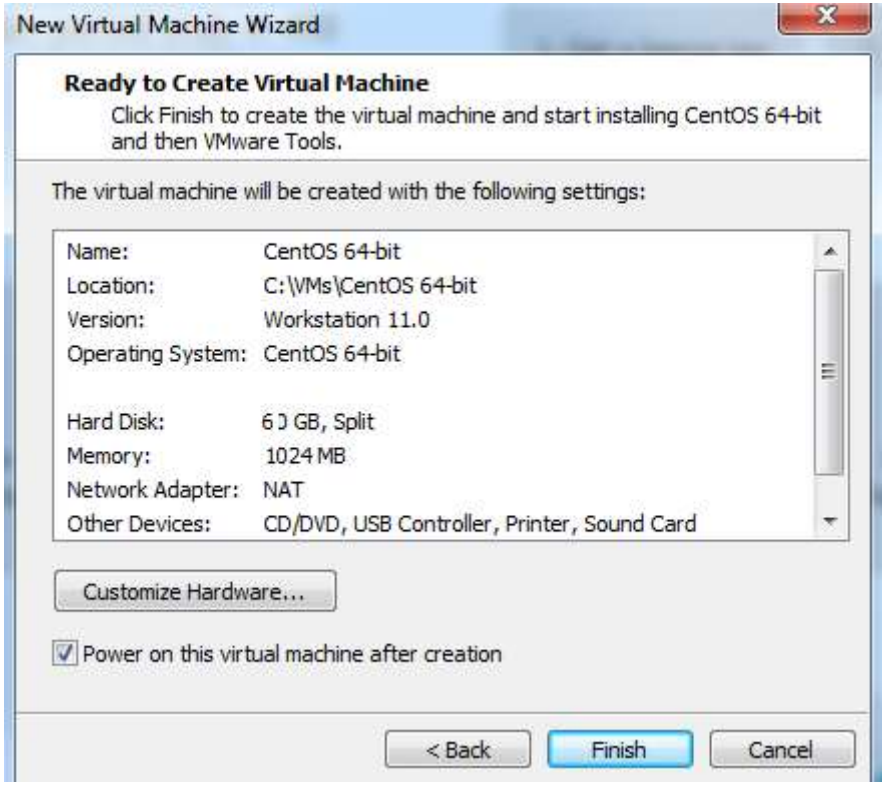
Select size of your VM

- Select Maximum disk size (60 GB) and most importantly “Split virtual disk into multiple files”.
- Click “Next >”



Customize Hardware, Select Memory, Network

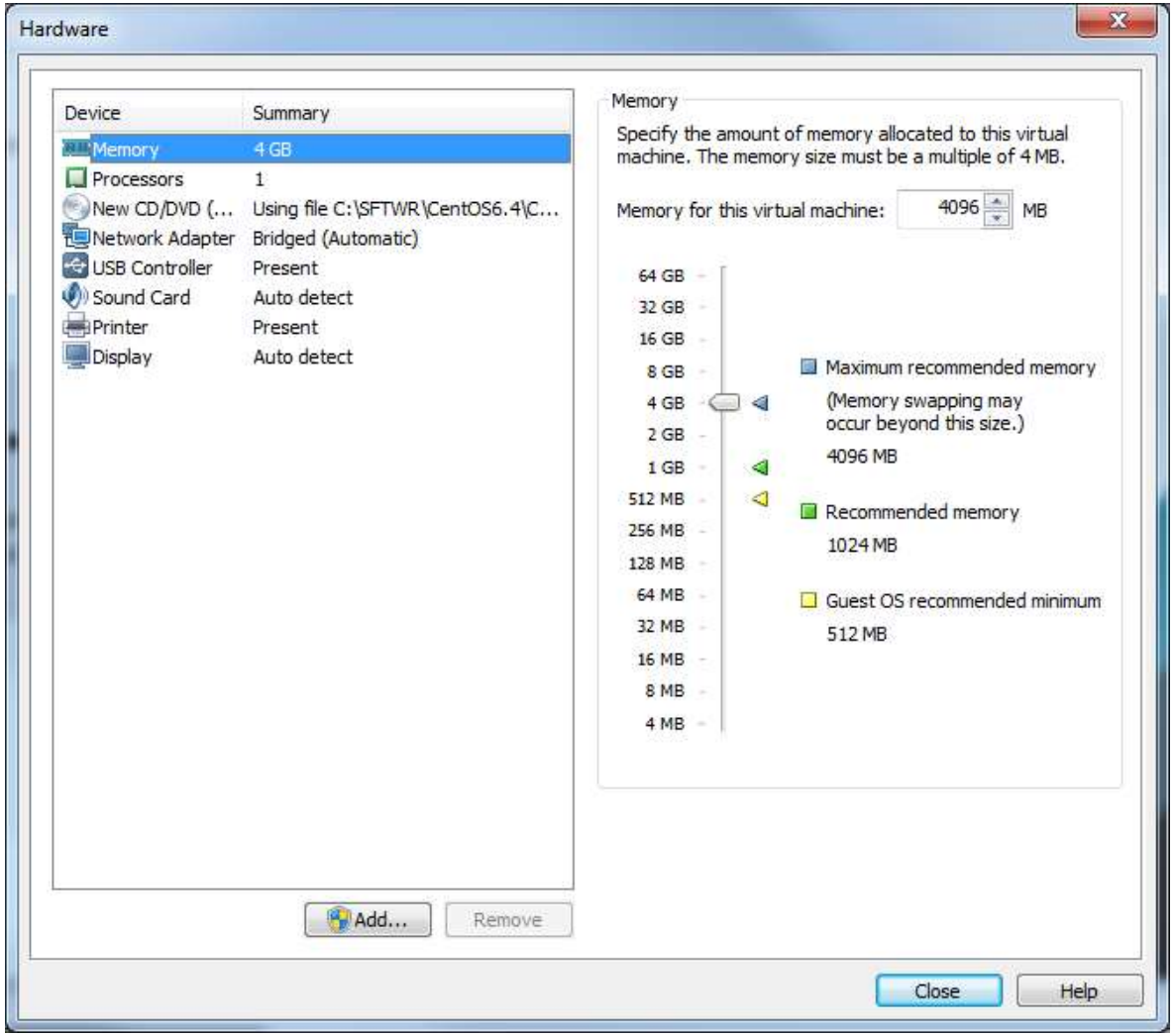
- Select “Customize Hardware” in order to assign memory to your VM and select network arrangement.



Select Memory

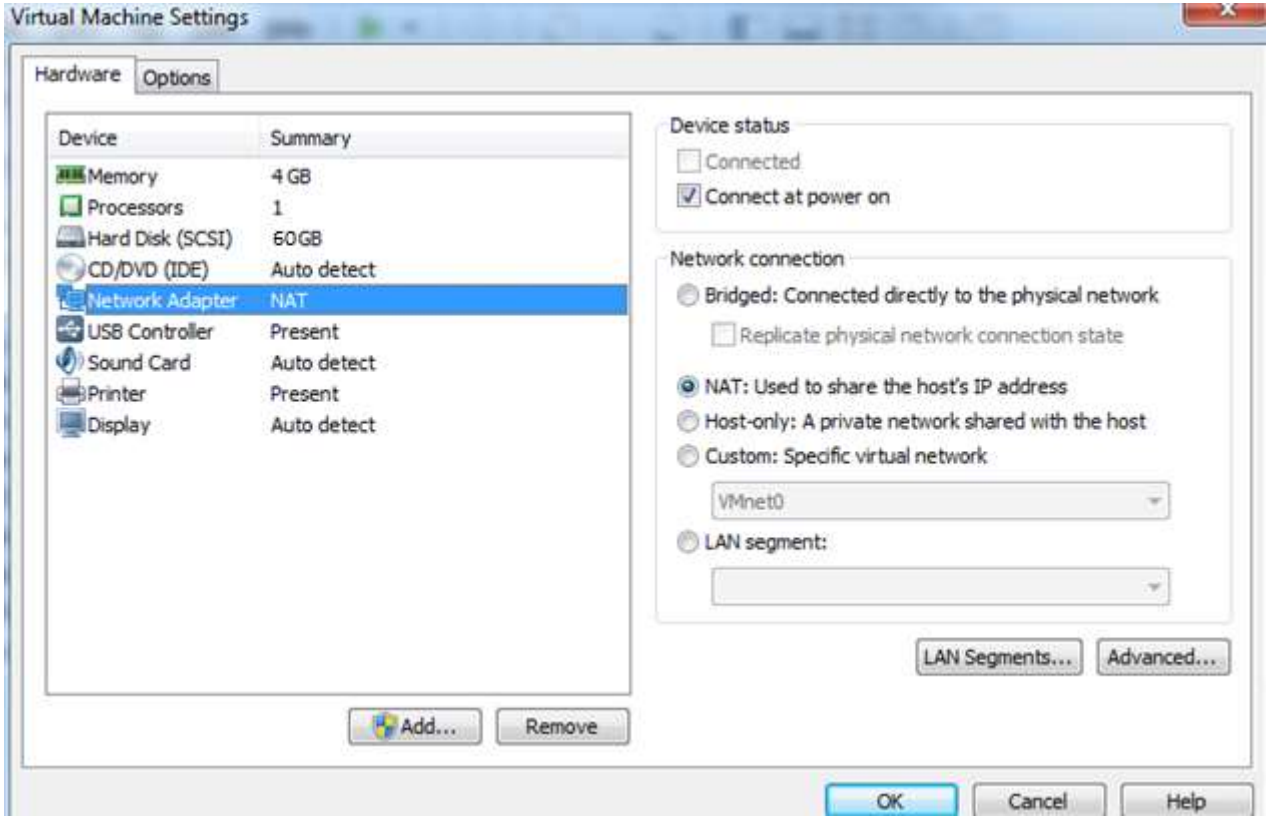
- More memory, faster the performance.
- Your VM will behave as a standalone machine with that much RAM.

- Some basic Hadoop processes could run on 2GB.
- Many processes require 4GB; some 8 or 10 GB.
- You could change (adjust) the size of memory later as you need it.
- I chose 4GB for now
- You might want to go buy new laptop, first. ☺



Network Setup

- Default network configuration contains one NAT (Natural Address Translation) adapter which has the same IP address as the host machine.
- That adapter is quite useful and we will leave it alone. We want another.
- On the Virtual Machine Settings select `Network Adapter` and then click `Add` button

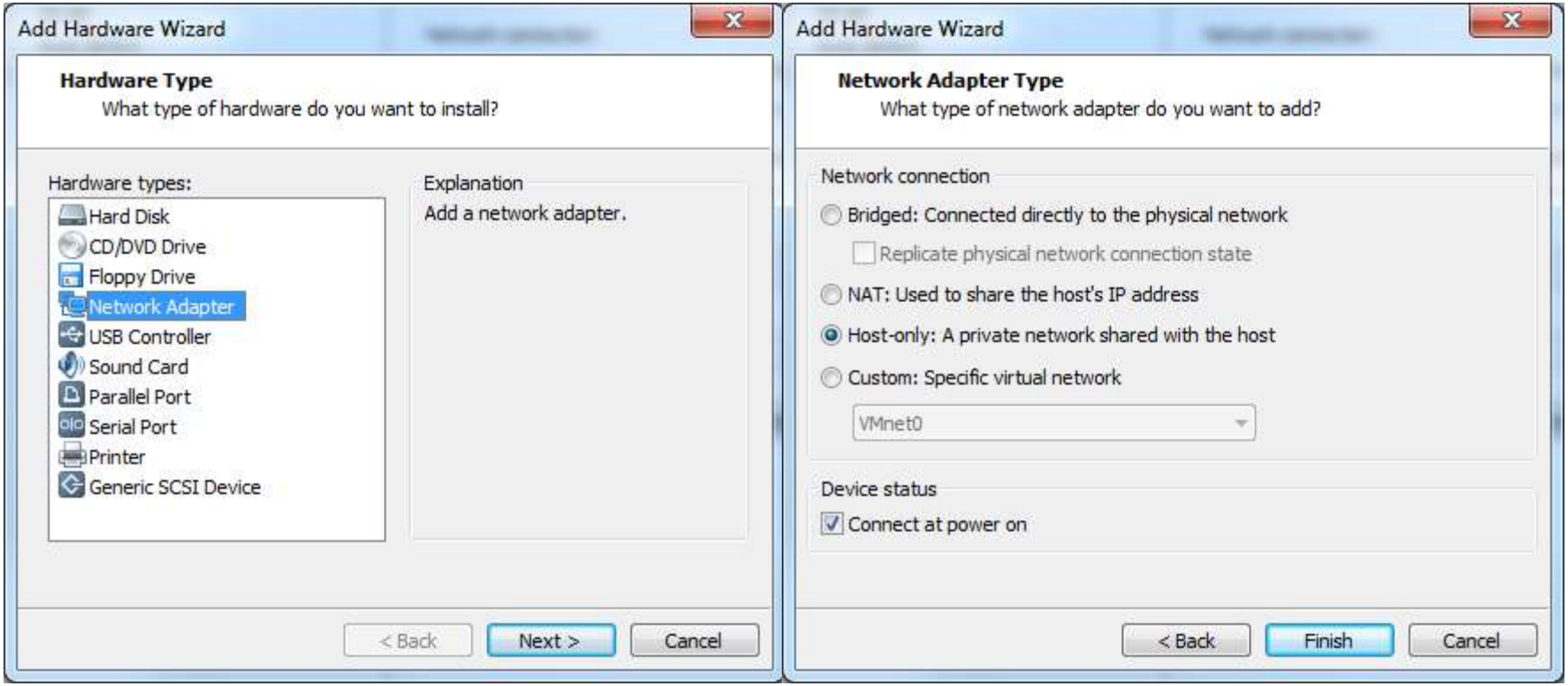


Adding Host-only Adapter

On the `Add Hardware Wizard` select `Network Adapter` again and hit `Next>`

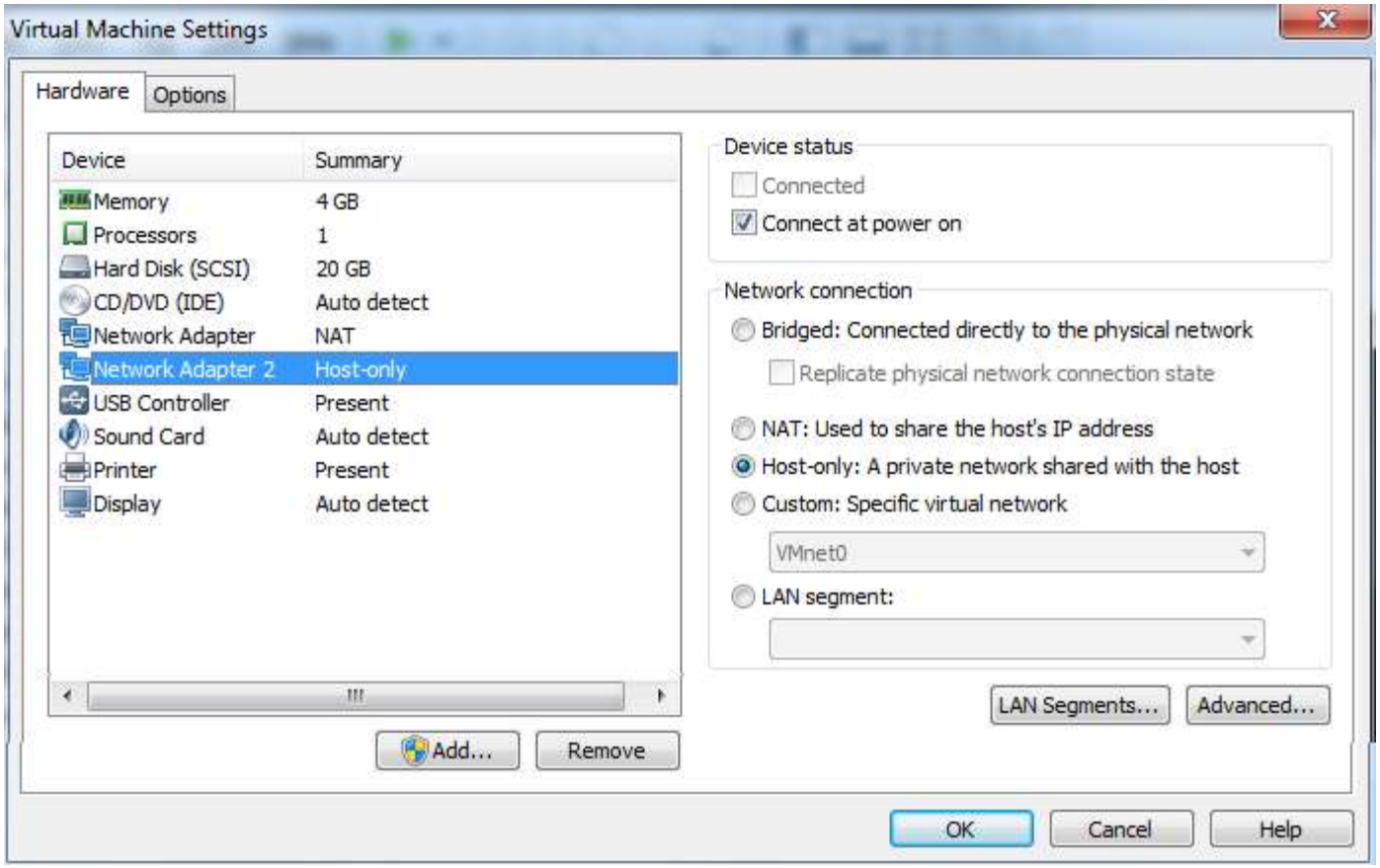
On the `Network Adapter Type` wizard select `Host-only: A private network shared with the host.`

Select `Finish` and then `Close`



Two Network Adapters

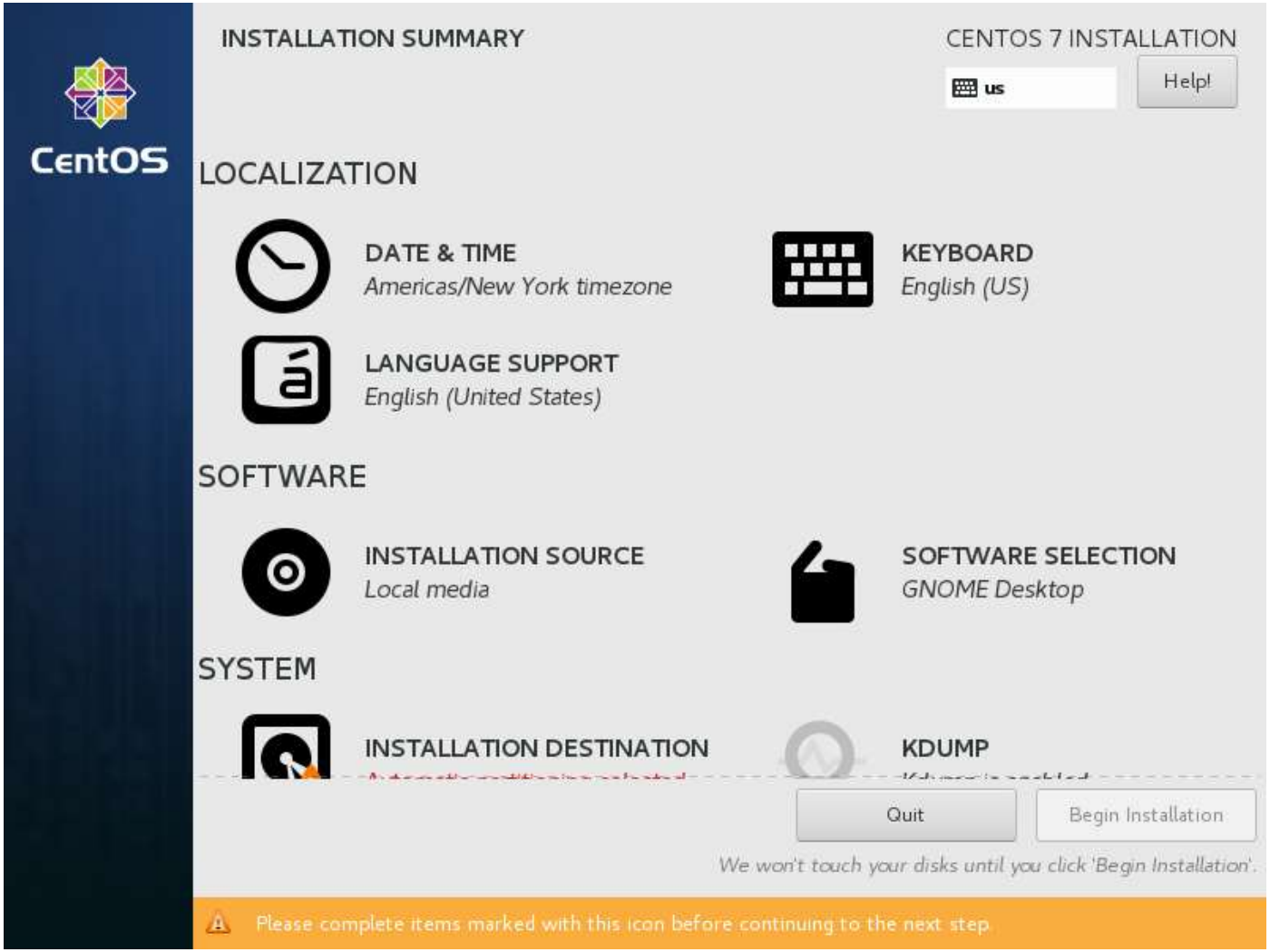
- On the `Virtual Machine Settings` we now see two Network Adapters.
- One adapter is of type `NAT` and the other is of type `Host-only`.
- Hit `OK` and `Finish`



- When you get the screen bellow with up-down arrow navigate to Install CetnOS 7 and then hit the Tab.

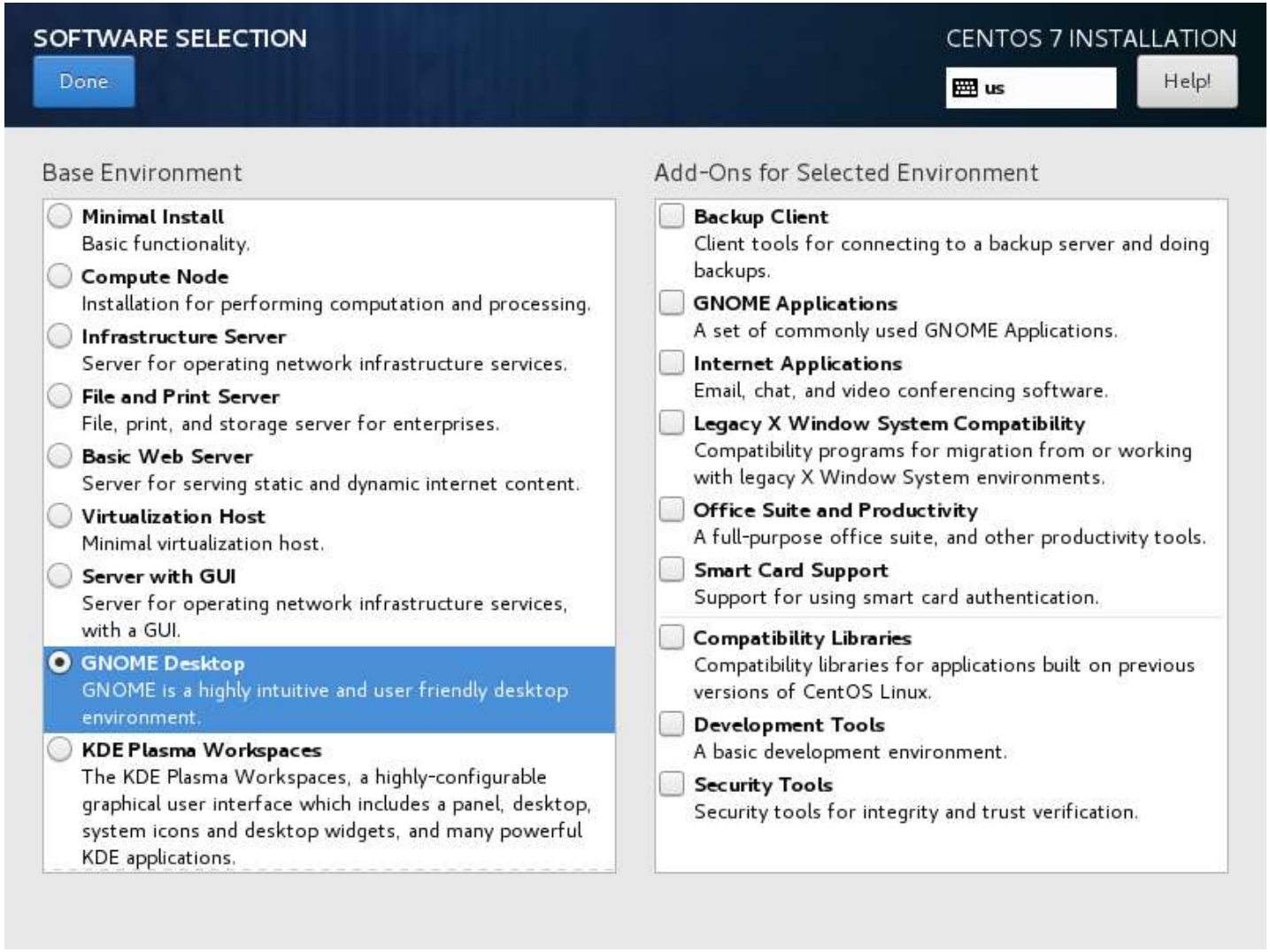
Scroll up or down and hit Software Selection

- On the screen that follows (INSTALLATION SUMMARY) make sure you find SOFTWARE SELECTION and click on it.



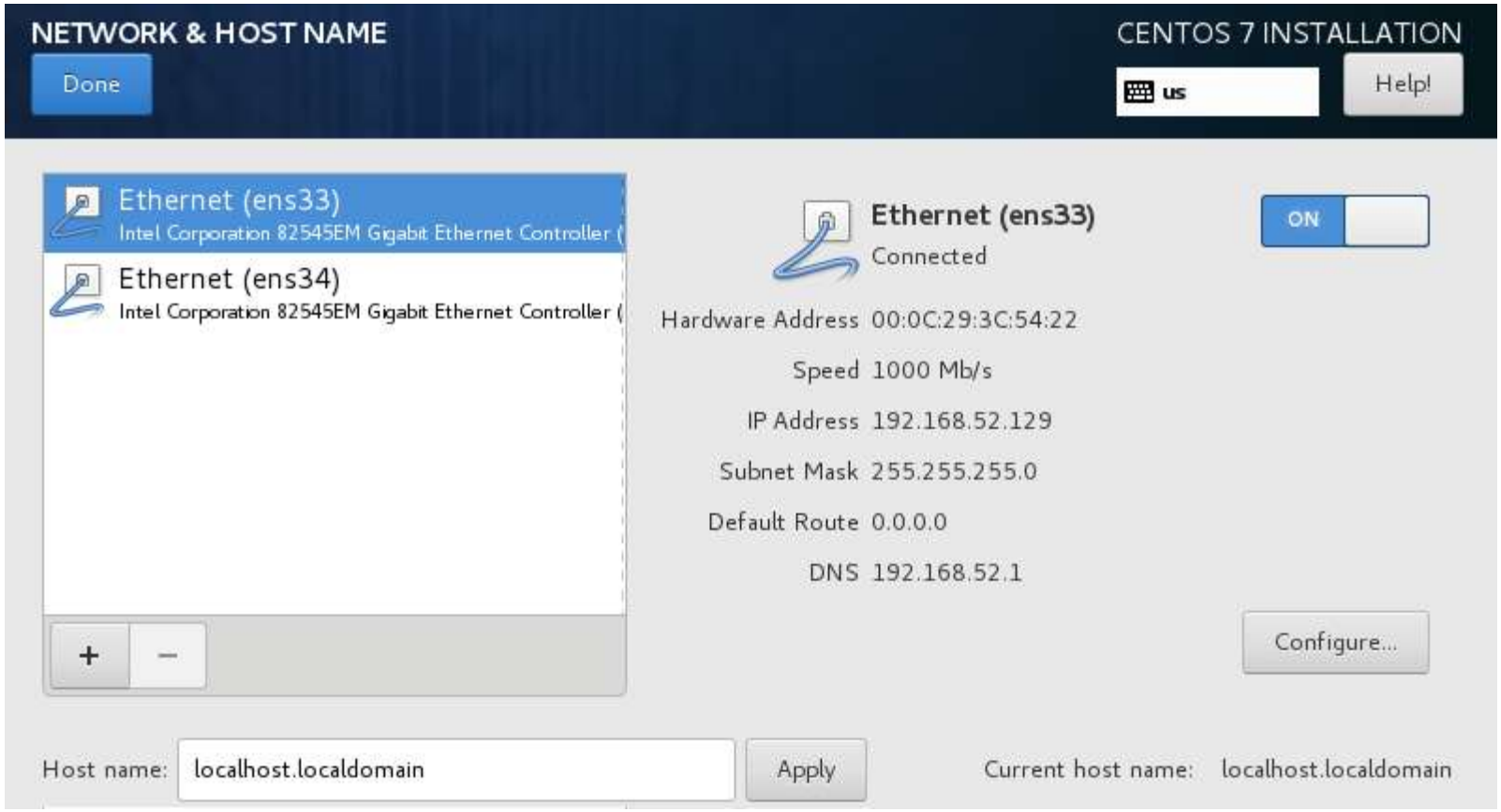
Select GNOME Desktop

On the SOFTWARE SELECTION screen, select GNOME Desktop. Done



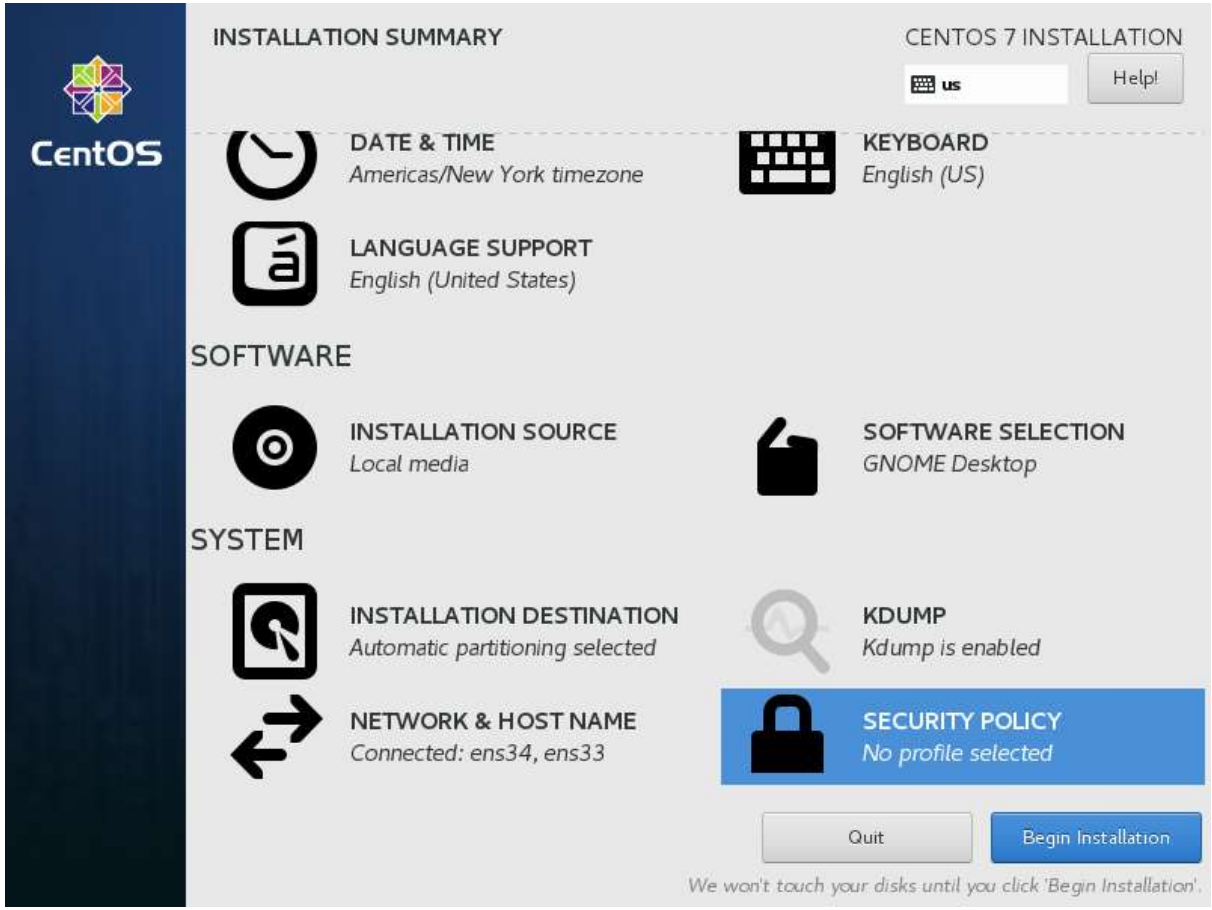
Select other options

- Once you are back on INSTALLATION SUMMARY screen you can adjust your timezone, keyboard and other options.
- Select Network & Hostname. On the next screen toggle both network card to ON. Leave Host name as is, unless you have a preference. Hit Done



Toggle Installation Destination

- Enter Installation Destination screen but do not change anything. Just hit Done.
- Leave Security Policy as is unless you know what you are doing.
- Hit Begin Installation at the bottom of the Installation Summary Screen

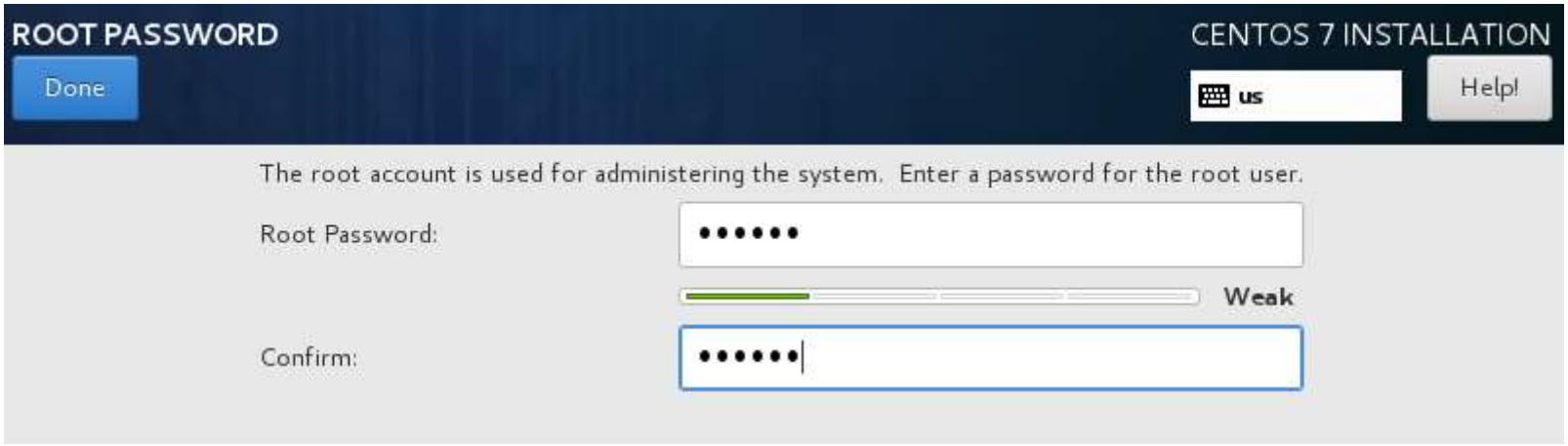


User Creation Screen

- On CONFIGURATION Screen select first Root Password and then User Creation option:

ROOT PASSWORD

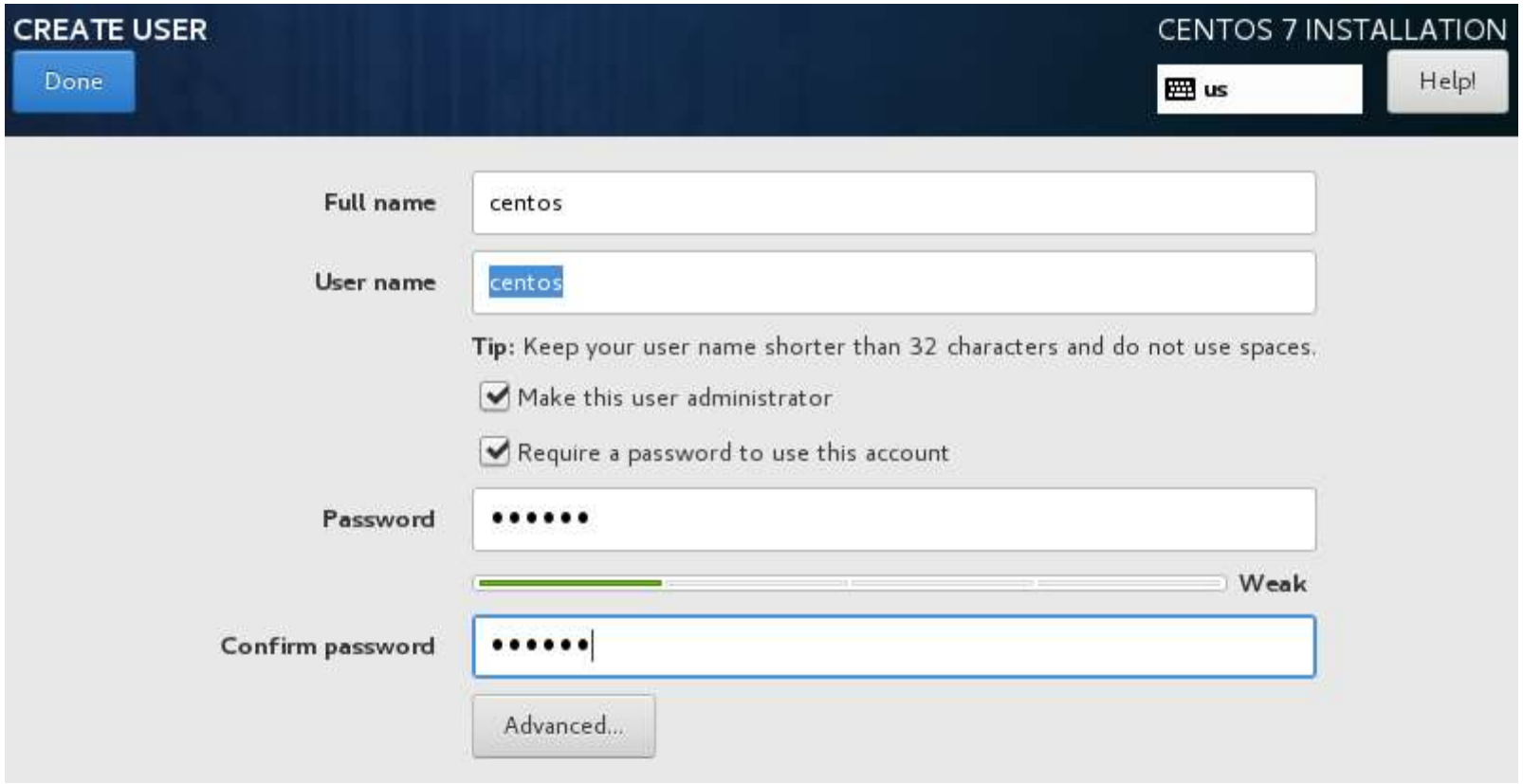
- Enter a password that you can remember. Hit Done



- Please note that VM swallows your cursor. To release the cursor do: Ctrl and Alt keys at the same time.

Create new user

- Make sure you check “Make this user administrator”. This new user will have “sudo” privileges. Hit Done

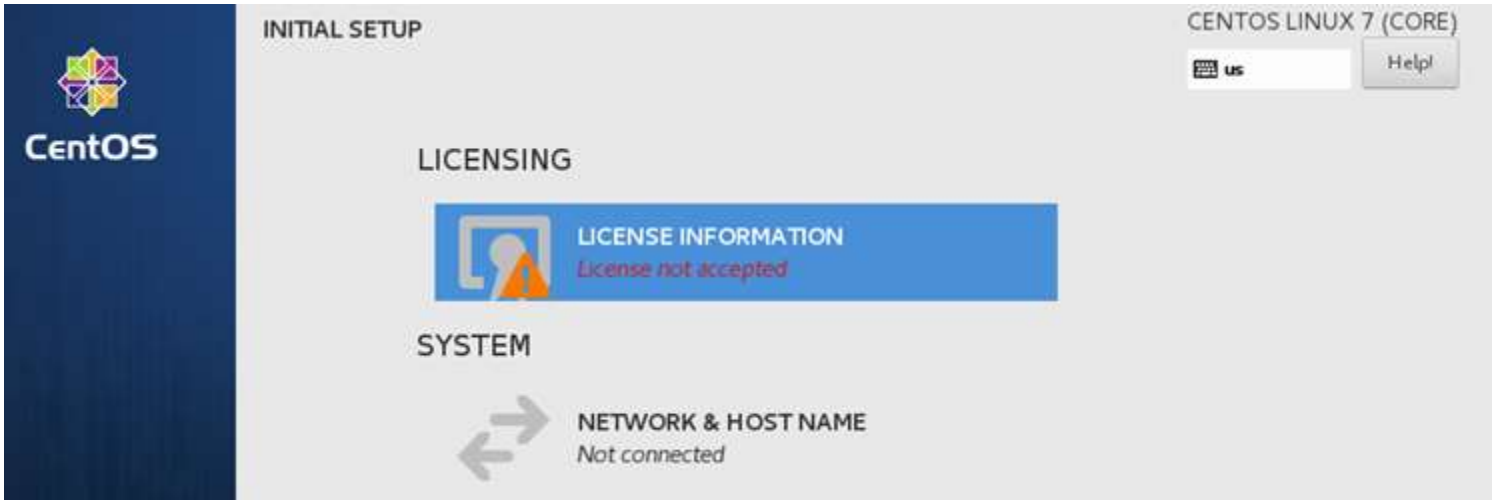


Wait on CONFIGURATION Screen

- The installation will proceed another 10-20 minutes. Wait. On the bottom of the configuration screen you can see names of various Linux modules that are being installed. After a while you will be asked to Reboot. Do it.

Accept License

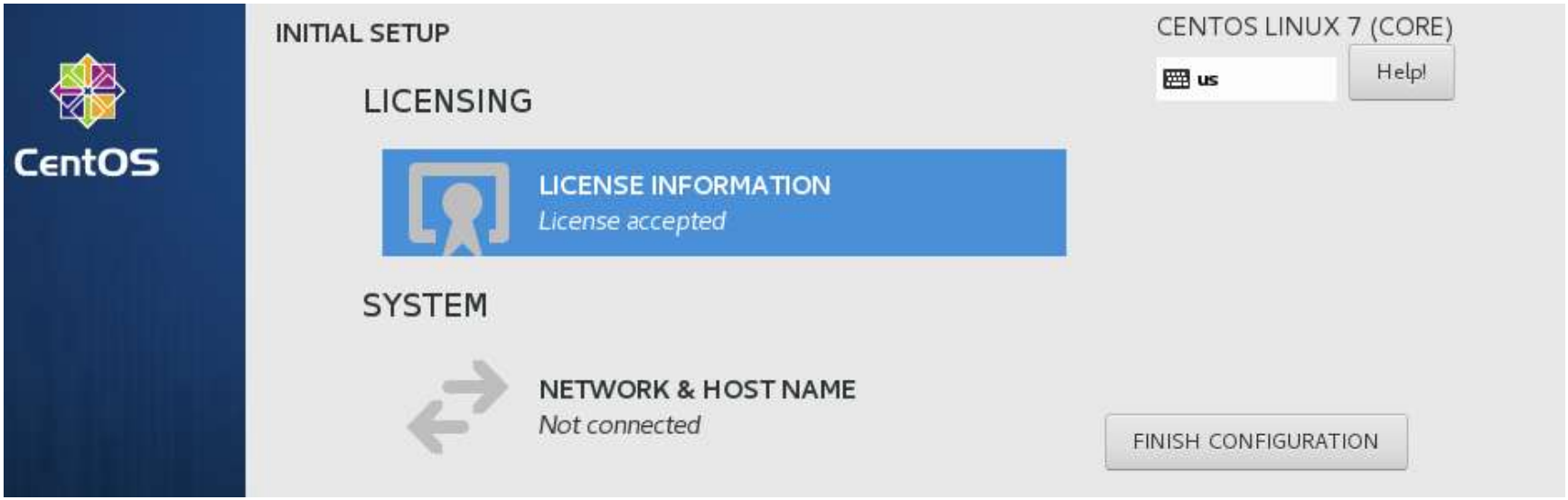
- On the next screen hit Licensing Prompt



- and then on the next screen accept license Agreement. Hit Done

- On the bottom of the same screen you will see QUIT. Hit it.

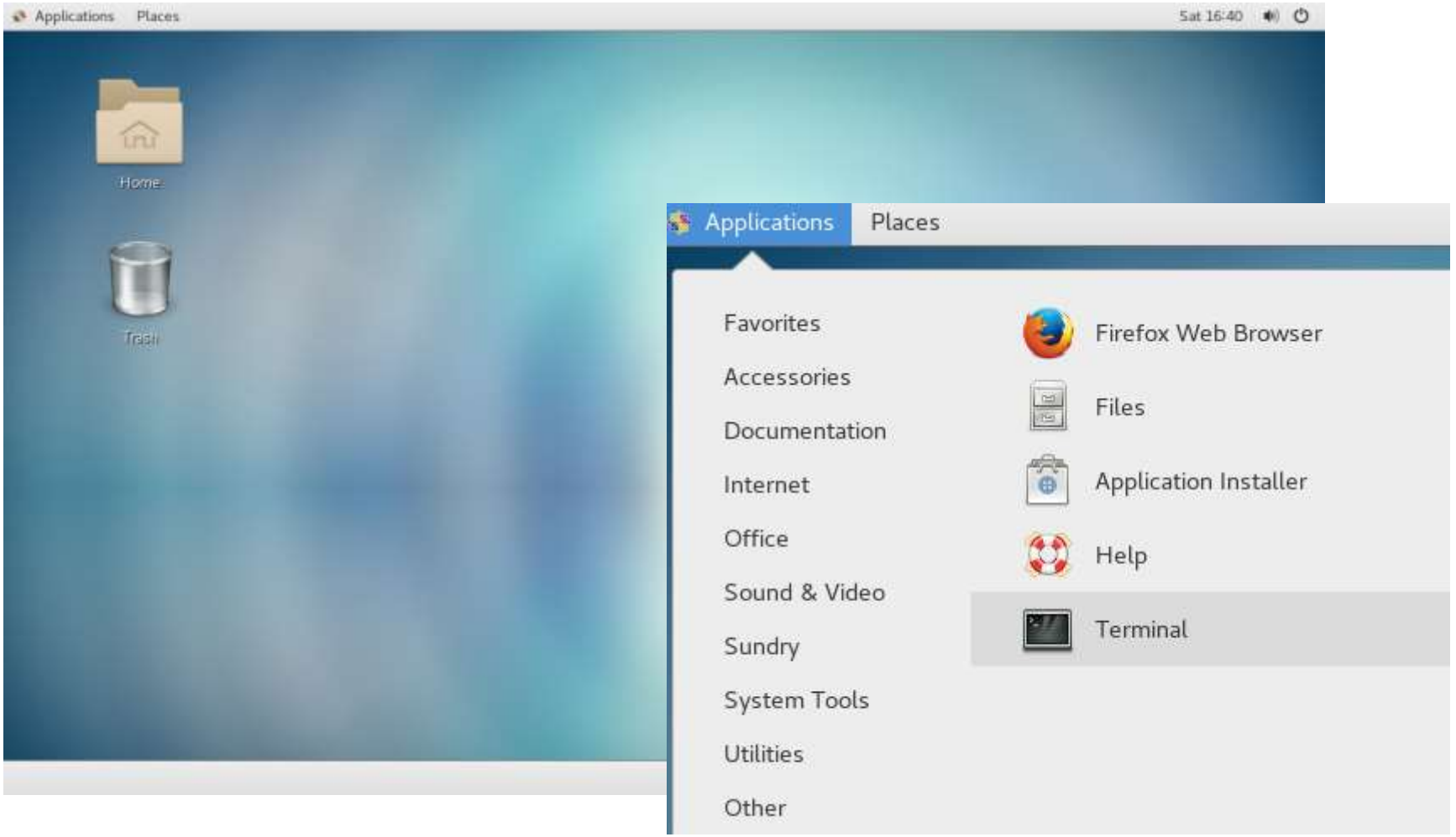
Finish Configuration



Login as user `centos` or `root`

You Are in

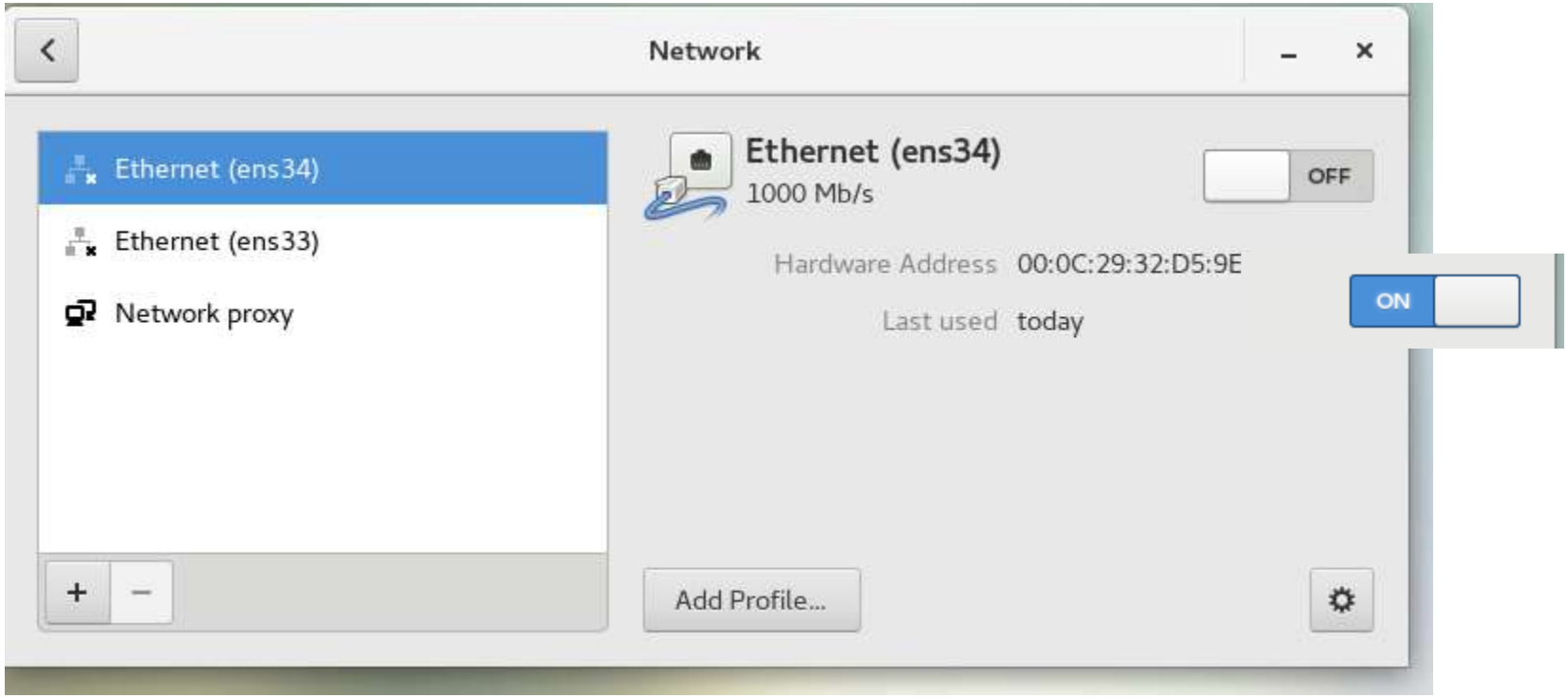
- You might be asked to configure a few more things. Just do it.



- Command terminal is at Applications > Favorites > Terminal

Enable Network Cards

- If you failed to enable network cards during the installation, you can do that now. Select Application > System Tools > Settings and then on the next screen: Network. You will get a screen that looks like this



- Toggle OFF button into ON. That card (ens34) is now open for network traffic. Do the same with the other card (ens33).
- To keep card working on every reboot apply procedure on the next slide.

Making Network Card come on with Every Reboot

- Rather than enabling network cards after every reboot we could edit the configuration file for the network interface.
- On CentOS 7 that file is normally called

```
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- eth0 or eth1, ..2, etc. are the traditional designation for the network cards.
- In our case, those cards are called ens33 and ens34, so file name are:

```
ifcfg-ens33 and ifcfg-ens34
```

- As user root or a sudo user vi those files and change:

```
ONBOOT=no to ONBOOT=yes
```

- Some setups seem to also require the addition of a line:

```
BOOTPROTO=dhcp
```

where a DHCP setup is in play;

- Static IP setups would take:

```
BOOTPROTO=static
```

- of course

Open Port 22

- On you VM prompt do the following:

```
$ sudo firewall-cmd --zone=public --add-port=22/tcp –permanent
$ sudo firewall-cmd –reload
```

- You can check whether port 22 is added using iptables command:

```
$ sudo iptables -vnL | grep 22
[sudo] password for centos:
    0     0 ACCEPT     all  --  *      virbr0  0.0.0.0/0
192.168.122.0/24     ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  virbr0 * 192.168.122.0/24  0.0.0.0/0
    3   156 ACCEPT     tcp  --  *      * 0.0.0.0/0         0.0.0.0/0
tcp dpt:22 ctstate NEW
    0     0 ACCEPT     tcp  --  *      * 0.0.0.0/0         0.0.0.0/0
tcp dpt:22 ctstate NEW
```

- Subsequently, you will have to reboot your system:

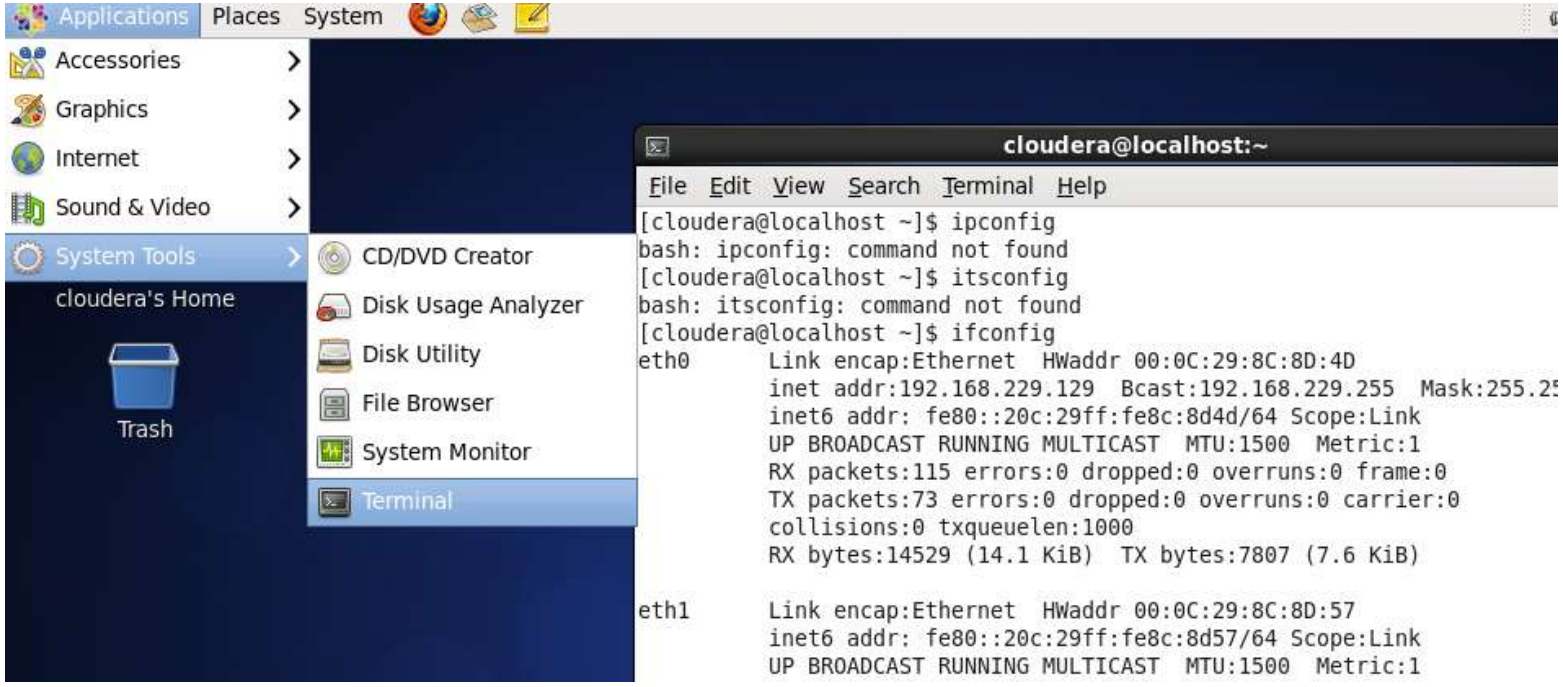
```
$ su
Password: xxxxxxx
[root]$ reboot
```

Open Terminal Window and find IP Address

- In the screen that opens we can go to

  `Applications > System Tools > Terminal`

- White (not Black) terminal window will open. If we type `ifconfig`, the system will produce the IP Address of the Host-only adapter we created. As we can see the IP address is `192.168.229.129`.
- We could use that IP address to connect to our VM as if it were a server.



Connect to VM as a Server, Transfer Files

- If we open a Cygwin window on our PC, we could issue `ssh` command:

```
$ ssh centos@192.168.229.129
centos@192.168.229.129's password:
[centos@localhost ~]$ pwd
/home/centos
[centos@localhost ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[centos@localhost ~]$ exit
logout
Connection to 192.168.229.129 closed.
```

- Similarly, we could use scp command to transfer files to VM. For example:

```
$ scp JDBCSample.java centos@192.168.229.129:~
centos@192.168.229.129's password:
JDBCSample.java                                   100%  771
0.8KB/s   00:00
zdjordje@FDCE-ZDJORDJ-2 /cygdrive/c/CLASSES/code
$ ssh centos@192.168.229.129
centos@192.168.229.129's password:
Last login: Tue Feb 24 15:15:38 2015 from 192.168.229.1
[centos@localhost ~]$ ls
Desktop  Documents  Downloads  JDBCSample.java  Music  Pictures  Public
Templates  Videos
```

- We transferred file `JDBCSample.java` from my PC to the home directory (~) of user `centos` on the VM.

Fix `known-host` file

- If you try to ssh or scp into your VM, you might get the following output:

```
$ scp ulysses10.txt centos@192.168.135.128:/home/centos
@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:piRMa8YWGodtJuabFdQAflBLWCcyzL+S5IlBSu+MUg8.
Please contact your system administrator.
Add correct host key in /home/zdjor/.ssh/known_hosts to get rid of this
message.
Offending RSA key in /home/zdjor/.ssh/known_hosts:34
RSA host key for 192.168.135.128 has changed and you have requested strict
checking.
Host key verification failed.
lost connection
```

Fix known-host file

- Open file `known_hosts` and remove the line with offending server.
- In my case:

```
$ vi /home/zdjor/.ssh/known_hosts
```

- I found the line with server `192.168.135.128` and deleted that one line.
- When I try scp-ing again, I get a normal dialog:

```
$ scp ulysses10.txt centos@192.168.135.128:/home/centos
The authenticity of host '192.168.135.128 (192.168.135.128)'
can't be established.
ECDSA key fingerprint is
SHA256:xYRJJ53vbe9ouRMAuPq2m4ZZZPk2FcVbwHIOAyvOFSo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.135.128' (ECDSA) to the list
of known hosts.
centos@192.168.135.128's password:
ulysses10.txt
100% 1529KB  44.6MB/s   00:00
```

passphraseless `ssh`

- Various Hadoop processes have to navigate to different machines in the cluster and it would be a nuisance if they would have to submit a password on every entry. For example if you type

```
[centos@localhost Downloads]$ ssh localhost
```

- The system will ask you for centos's password

```
The authenticity of host 'localhost (::1)' can't be established.
RSA key fingerprint is
88:87:fc:e8:24:d0:c9:81:0e:f4:9c:9e:7a:24:b3:46.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known
hosts.
centos@localhost's password:xxxxxxxxx
Last login: Fri Feb 27 15:29:59 2015 from 192.168.72.1
[centos@localhost ~]$
```

- If you do `ls -la` in your home directory you will see directory `.ssh`
- Initially, the directory contains a file `known_hosts`

passphraseless `ssh`

- In the home directory of the user whom you want to equip with passphraseless `ssh` run the following commands:

```
[centos@localhost ~]$ ssh-keygen -t dsa -P '' -f ~/.ssh/id_dsa
Generating public/private dsa key pair.
Your identification has been saved in /home/centos/.ssh/id_dsa.
Your public key has been saved in /home/centos/.ssh/id_dsa.pub.
The key fingerprint is:
a6:f6:6b:1f:3b:77:0b:24:e1:b5:c0:c1:89:19:29:aa
centos@localhost.localdomain
The key's randomart image is:
+--[ DSA 1024]----+
|        .*..     |
|       . +.o.    |
|      . .  + .   |
|     .     . + . |
|    .     S o o  |
|   E     o   o   |
|       o   . .   |
|      . .. .o... |
|        .oooo ... |
+-----------------+
[centos@localhost ~]$
```

passphraseless ssh

```
[centos@localhost ~]$ cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys
[centos@localhost ~]$ cd .ssh
[centos@localhost .ssh]$ ls
authorized_keys  id_dsa  id_dsa.pub  known_hosts
```

- The above `cat` command has copied the public key to the `authorized_keys` file of the .ssh directory

```
[centos@localhost .ssh]$ cat authorized_keys
ssh-dss
AAAAB3NzaC1kc3MAAACBAI5Jsfv/wSHLNpC/KS8CPDR60zVUGzvc8K9L71igZeyd0xI8iN
KGKM53+MMbgaIUHWxBWxdixFMkcOyIIee7ljZuBUPe6H6/AEY0MMnLetFLQt/DyYf6VpT0
mpVUpjspOOtbmqZrL+GRaQ0l3ApbPcucgYIavT0oHdW2ba5b07G9AAAAFQDb9BTZ81YbkQ
lUvxGaI+PbTMak/QAAAIBb6mAcrdiHl+96/JwybKfMXaHhZZEzJjbki5S3UhUOiAoJXi4g
LOtS2kr7NSKCh/J+TYVvc5rxnyHiBZYGTARSFSw2nsQ+rJi9v70PoQ8Ij69+QhlPb0ugW/
f4Pmn9fpFaMaSeQMRCfvYV11tFh1YjWrvYagnbzgiSk0YvE7BwAAAIATMX1giXJwglwnxN
KalcH+krRAA7Xy38nnGYR4KJdGaQ/0Z1zIObYb3T1EPFkQoWYlu2FR76eMFocCtK1f1sEL
E7afq/OVmkaF8Nu09ED086PiF24ZJp2p3VJIIwueLOz7EoSUItqumVoIJQVyMltpoPh+dy
Dtc5uLWOfVY2fISw== centos@localhost.localdomain
```

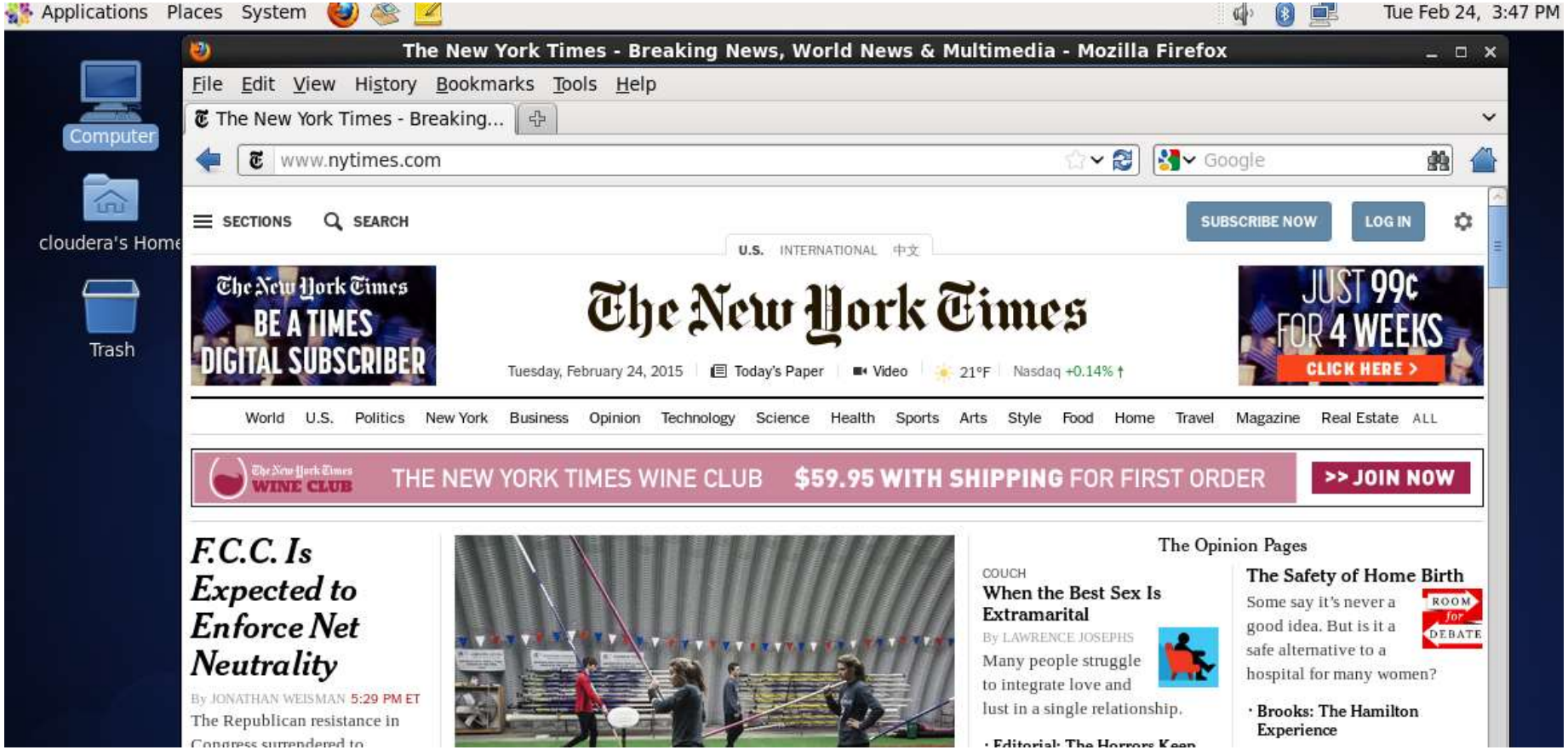
- You can transfer the private key (`.shh/id_dsa`) you just generated to any machine and then login to your VM using the `ssh` command

```
ssh -i id_dsa centos@192.168.255.129
```

- Without being asked for the password

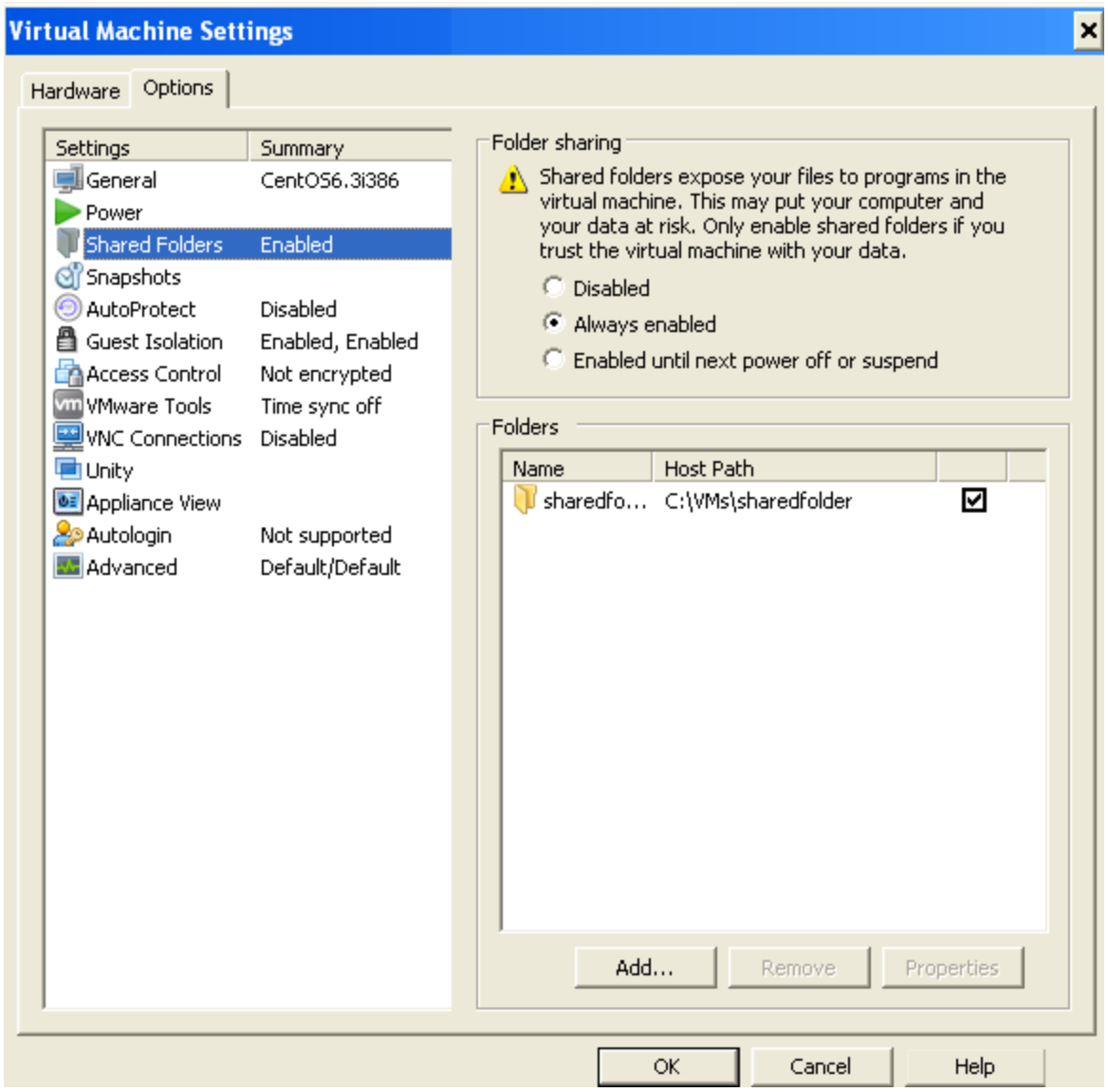
NET Adapter and connection to the Web

- We have another Network adapter (NAT) that uses IP address of the host machine and enables us to connect to the Internet from inside our VM.
- Open a browser and type the URL of the Ministry of Truth. You will see the truth. All you have to do is believe. All courtesy of NAT adapter.



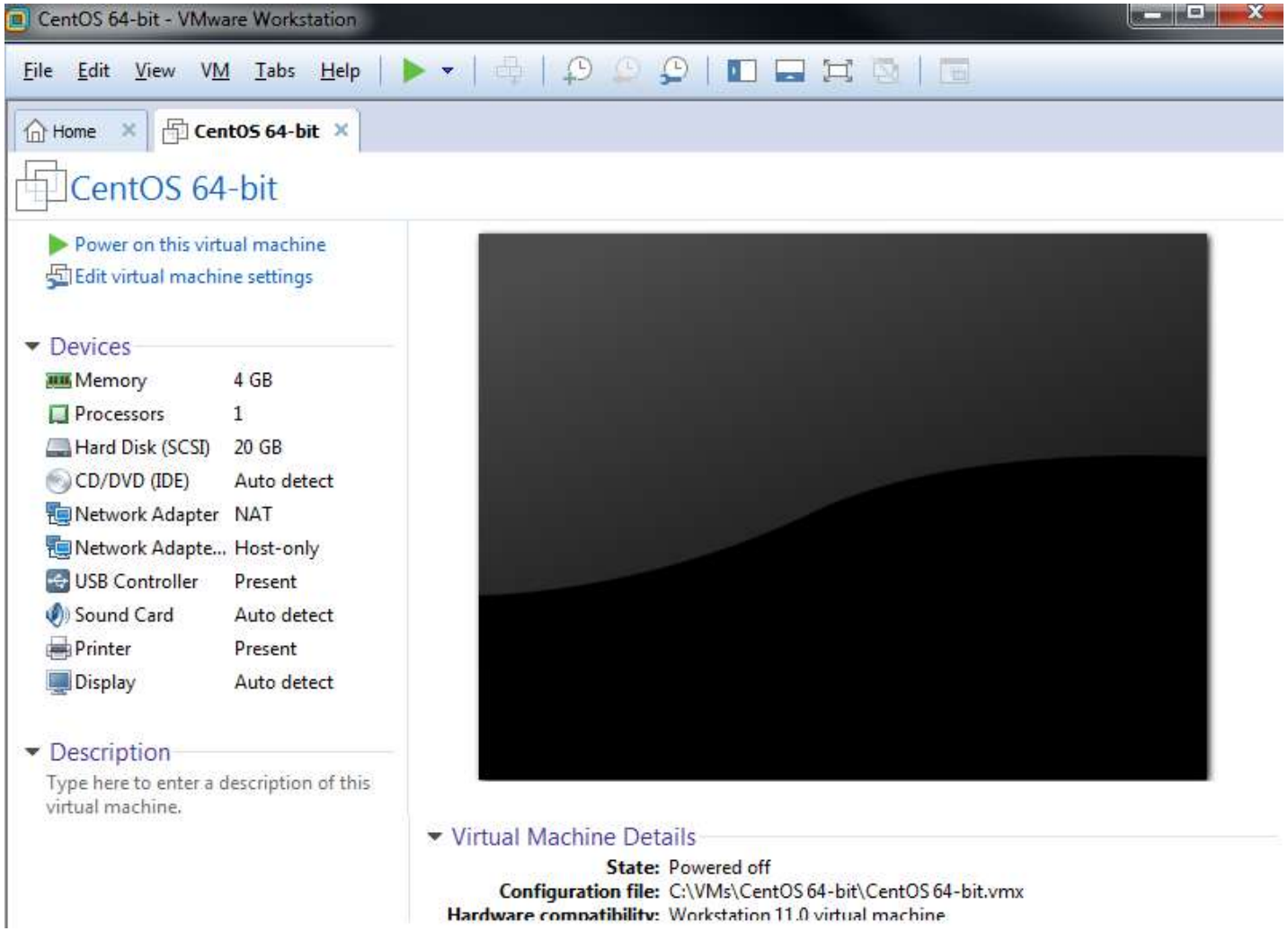
Enable Shared Folders

- Another way to share files with the host OS is to enable `Shared Folders`.
- Power down VM. Right click on the VM, select `Edit virtual machine settings` > `Options`
- Select `Shared Folders` > `Add`
- Add folder `c:\VMs\sharedfolder`
- Check `Always enable` > `Finish` > `OK`
- Power up VM
- Login as `centos`.
- Shared folder will shows as `/mnt/hgfs/sharefolder`



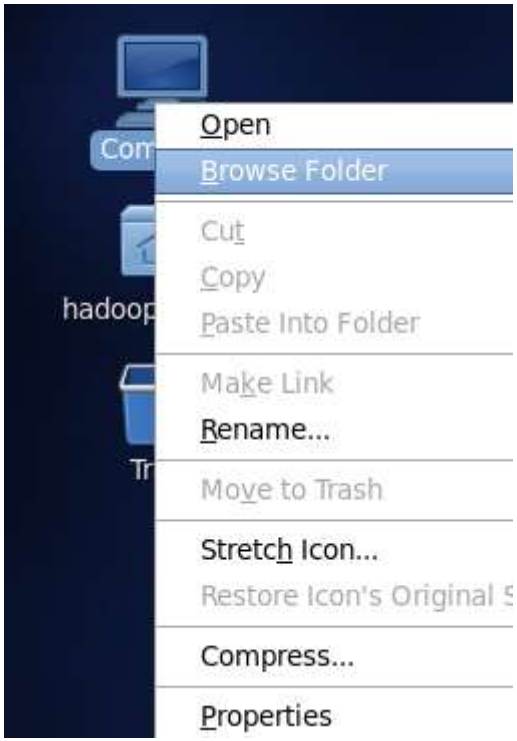
Open a Virtual Machine

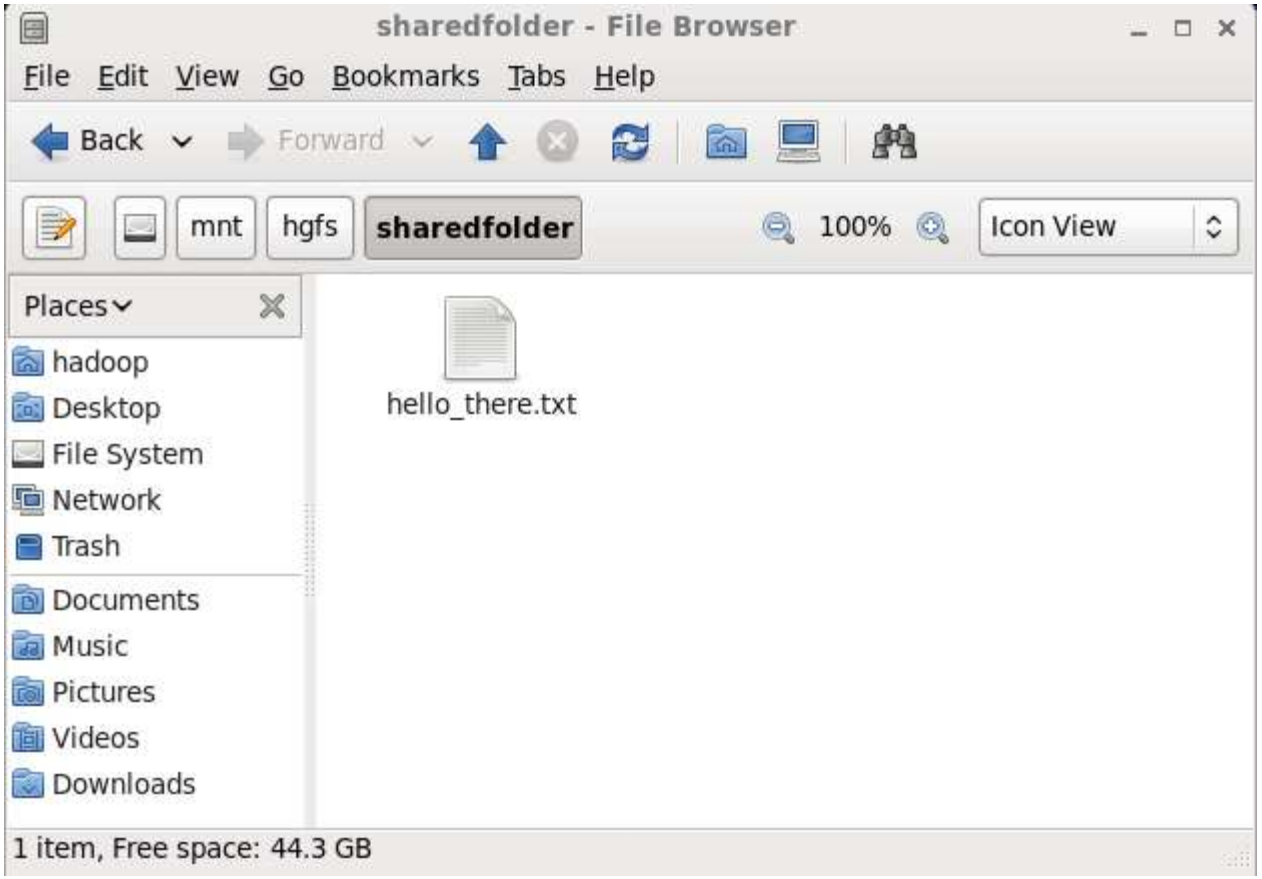
- Open the Workstation, select Open a Virtual Machine icon and select the VM file you want to run from your OS. To power the VM hit the green triangle. If you have enough memory, could run several VMs simultaneously.



Locate Shared Folder, `Browse Folder`

- Right click on `Computer` icon
  - `Browse Folder > File System > mnt > hgfs > sharefolder`





- We can use the `sharefolder`
- to share files back and forth between the operating system of your host machine and the operating system of your new VM.
- On some VMs sharefolder has to be mounted. Do not despair. You have seen it in recitation.

Select Terminal, `whoami`, Shell

- Select

`Applications > System Tools > Terminal.`

- Find out who you are,

```
$ whoami
```

- Examine `/etc/passwd` file
- Examine `/etc/group` file
- User `centos` belongs to group `centos` and has `bash` shell.

```
[centos@localhost ~]$ whoami
centos
[centos@localhost ~]$ cat /etc/passwd | grep centos
centos:x:500:500:CentOS6.4:/home/centos:/bin/bash
[centos@localhost ~]$ cat /etc/group | grep centos
centos:x:500
[centos@localhost ~]$ pwd
/home/centos
```

`mount`-ing sharedfolder

- Sometimes your will move (copy) your VM to another machine or your would download a VM and the above procedure for creating shared folder would simply not work. You will select the shard folder through VM Options but once you are in VM, the content of the shared folder will not be visible.
- At point you need to manually "`mount`" that folder. VM for whatever reasons failed to do it for you.
- Open Linux command prompt and issue the following command:

```
$ sudo mount -t vmhgfs .host:/ /mnt/hgfs
```

- The `sahredfolder` will appear under `/mnt/hgfs/sharedfolder`

sudo privileges of user centos

- We need centos to be very powerful user. This is enabled by user root who grants "sudo" privilege to user centos. We want centos to issue sudo commands without the password.
- On the command prompt of user centos, type:

```
$ su        # Then provide the password of that user (or root??).
```

- root's password is the same as the password of user centos.
- As user root open the terminal window and change permissions on file /etc/sudores

```
$chmod a+w /etc/sudoers
```

- As root, use tool visudo to add the following line to /etc/sudoers file:

```
# NEVER use plain vi for changes to /etc/sudoers file
$ visudo /etc/sudoers          # add a line that reads:
   centos  ALL=(ALL) NOPASSWD: ALL
```

- User centos will not be asked for password after every sudo command.
- Exit and save modifications by typing Hold [shift]+press "X"
- Change permission back on file: /etc/sudoers:

```
root$ chmod –w /etc/sudoers
```

Giving `sudo` privileges to user `centos`

Allowing user `centos` to run commands without checking its password, is a security issue but is a great convenience. Interestingly, CDH installation does ask for a user with sudo privileges and no password.

- On some Linux systems, CentOS included, `sudo` command clears the environmental variables.
- In order to preserve some of those, you need to add lines to `/etc/sudoers` that read like :

```
Defaults env_keep+= "JAVA_HOME"
```

- Then change permissions of `/etc/sudoers` back to read only (440 mode). Note, if you do not do this your sudoers will not function properly.

```
$chmod 440 /etc/sudoers          # must do it as root
$ls –ls /etc/sudoers
-r—r----- . 1 root root 4035 Mar 8 06:56 /etc/sudoers
```

- Once you install Java JDK, you will be able to verify that `sudo` command does not remove `JAVA_HOME` environmental variable by typing:

```
$sudo env | grep JAVA_HOME
```