

1.

1. Has hardware virtualization support. Explain how you verify it.

因為是使用這裡是使用Windows的Hyper-V所以要開啟巢狀虛擬化技術
因此需要在系統管理員權限下的PowerShell下執行

```
Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
```

來開啟巢狀虛擬化技術(是虛擬機的名稱)
接下來的操作在VM Host，以使用者root的身分執行

```
#檢查是否有虛擬化支援
grep vmx /proc/cpuinfo
#當確定有虛擬化支援之後
#安裝虛擬化套件
yum install -y virt-install qemu-kvm libvirt
#啟動虛擬化套件
systemctl start libvirtd
systemctl enable libvirtd
```

然後為了方便，在192.168.179.1這題機器上開個http server把CentOS的映像放上去，然後把映像檔放到磁碟中方便之後作業

```
curl http://192.168.179.1/CentOS-7-x86_64-Minimal-1611.iso -o CentOS.iso
mv CentOS.iso /var/lib/libvirt/images/Centos-7.iso
```

2. Allow non-root user to create a VM without sudo. 3. But only a certain user.

加入一個名為joe的使用者

```
adduser joe
passwd joe
```

為了開放權限，在/etc/polkit-1/localauthority/50-local.d/50-org.libvirt-remote.pkla這個檔案中加入以下資訊

```
vim /etc/polkit-1/localauthority/50-local.d/50-org.libvirt-remote.pkla
```

```
[Remote libvirt SSH access]
Identity=unix-user:joe
Action=org.libvirt.unix.manage
ResultAny=yes
ResultInactive=yes
ResultActive=yes
```

4. Show that how to use virsh to connect to the VM host without root permission.

這個操作在Client端執行，然後VM Host的IP為192.168.179.87

```
ssh-copy-id joe@192.168.179.87
virsh --connect qemu+ssh://joe@192.168.179.87/system
```

5. Follow the principle of least privilege.

如上

2.

接下來的操作在VM Host，以使用者root的身分執行

```
#使用fdisk弄出一個新的分割區
fdisk /dev/sda
n
p
3
<default>
<default>
t
3
8e
w
q
#重啟來使磁碟分割表生效
reboot
#把剛剛建出的磁區加入c1這個卷組中
vgextend c1 /dev/sda3
#建一個名為vm的lvm磁區
lvcreate -L 8G c1 -n vm
```

kickstart檔的來源為/root/anaconda-ks.cfg，做一些簡單修改後(如把sda換成vda、加入zerombr、reboot等等)

找一台http server把kickstart檔案放上去，然後http server的IP為192.168.179.1

```
#把檔案複製上去
scp /root/anaconda-ks.cfg root@192.168.179.1:/var/www/html
```

然後執行安裝指令

```
virt-install \
-n "AAA" \
--description "A VM" \
--os-type=Linux \
--os-variant=centos7.0 \
--ram=2048 \
--vcpus=4 \
--disk path=/dev/cl/vm,bus=virtio,format=raw \
--location=/var/lib/libvirt/images/Centos-7.iso \
--network bridge:br1 \
--graphics vnc,password=magic \
-x "ks=http://192.168.179.1/anaconda-ks.cfg" \
--noautoconsole
```

指令的參數意思為

```
virt-install
名字為 "AAA"
簡介 "A VM"
作業系統的種類是 Linux
作業系統是 centos7.0
使用 2048MB 的記憶體
使用 4 顆CPU
硬碟的位置是 /dev/cl/vm，使用 virtio 模式，然後使用 raw 格式
安裝程式的 iso 位置是 /var/lib/libvirt/images/Centos-7.iso
網路設定為橋接到 br1 這個介面上
使用vnc當作圖形的連接方式，然後使用magic當作密碼
額外參數，參數內容是代表kickstart檔的位置
這樣裝的時候可以不用連到console上
```

3.

1. Explain what is the interface that virsh console simulates.

virsh console 模擬的是 serial port 連接到虛擬機上後的輸出。

2. Explain how to do the thing like virsh console on a physical machine.

如常見的RS-232串列埠，我們可以用RS-232 to USB的轉接線來接到個人使用的電腦上，

Windows上使用putty連接到COM上(或是使用WSL+Linux的cu)。

Linux上的cu使用方法(假設電腦上的device name為ttySX)

```
cu -l /dev/ttySX -s <baud-rate-speed>
```

3. Find pictures of the interface or the special tool you need to use.



RS-232接頭



RS-232 to USB轉接器

4.

以下指令在 VM Guest 內的執行

```
# 將"ttyS0"加到/etc/securetty的尾端
echo "ttyS0" >> /etc/securetty
```

然後在/etc/default/grub內加入以下內容

```
vi /etc/default/grub
```

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --
stop=1"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=cl/root rd.lvm.lv=cl/swap rhgb"
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

然後重新config一次grub2

```
grub2-mkconfig -o /boot/grub2/grub.cfg
#重起來確認是否成功
reboot
```

接下來只要在virsh中使用

```
console (domain name)
```

就可以成功看到grub和登入畫面了

5.

使用nmtui建立bridge (ens33)，然後bridge到ens33上

```
nmtui
Edit a connection
<Add>
Bridge
Device 欄位輸入 br1
Slaves 欄位中選 <Add>
Ethernet
Device 欄位輸入 ens33
<OK>
<OK>
#然後把ens33這個profile刪掉
選取ens33
<Delete>
Delete
<Back>
<OK>
#重起使bridge生效
reboot
```

之前做第二題的時候，因為使用了

```
--network bridge:br1
```

這個參數，因此VM Guest的網卡會自動的bridge到VM Host的br1
然後接下來在VM Guest中要連上網路就直接使用

```
dhclient
```

自動獲得IP後就能上網了。

6.

1. List VMs on a VM host.

```
list
```

2. Remove a VM.

```
destroy <VM Name>
undefine <VM Name>
```

3. List interfaces of a VM.

```
domiflist <VM Name>
```

4. Delete an interface of a VM.

```
detach-interface <VM Name> <Interface Type>
```

5. "Edit" config of a VM directly.

```
edit <VM Name>
```

7.

NAT

使用NAT的方式連到網路，相當於會有一台虛擬的router處理兩個不同網段的IP，然後虛擬機連外時會使用那台虛擬的router當作Gateway，但是當外面的機器要連到虛擬機時，就需要在router上開port forwarding才能連到內部的機器，然後那些虛擬機可以共用同樣的Public IP。

macvtap

macvtap是一個混和了macvlan和tap兩個特性的一種連線方式，他的作法是當網卡連線進來的時候會先通過macvlan把不同連線目標(mac)的流量分道不同的vlan上(除了目標是原始網卡的流量)，然後那些穿過vlan的流量再接到不同的/dev/tapX檔案，然後用虛擬機就是透過檔案去跟外界溝通，然後出去的流量就相當於是把剛剛的過程反向。而使用這個方法的限制是外面的網卡必須要可以要多個IP，但是目前的Linux實現有個缺陷，在Bridge模式下的macvtap子設備不能和Host通訊，也就是虛擬機無法和Host通訊。

routed mode

就是使用一個虛擬的switch(in routed mode)當作那些虛擬機的路由器(第三層)，但是這個switch要設定一個靜態的路由表來決定每個傳進來的流量要傳到哪個IP去，然後不使用NAT來處理回來的流量，因此如果要連到Public IP上的話，有幾台虛擬機就需要幾個Public IP。

Linux bridge

這個方式是使用Linux內建的Bridge裝置去橋接實體(也有可能是虛擬)的網路卡和虛擬機中的網卡，讓兩張網卡可以直接互相連通。然後虛擬機中通常會要到一個跟Host網卡相同網段的IP，讓外部的人可以直接使用那個IP直接連到虛擬機中而不需要透過NAT或是router。