NASA HW3

NA

Short Answers

1. Pass: 直接通過，Block: 過來直接丟掉，不會回覆 Reject: 過來丟棄，並回覆給sender
2. interface match到所有穿過這個interface的流量，interface ip只match到這台pfsense機器在interface上面的ip。
3. stateful firewall代表可以檢追蹤紀錄封包狀態，規則上只要設定單向，反向會由於防火牆上的紀錄自動放行，pfSense屬於這種。
   stateless firewall代表所有封包全部都只能靠規則表，不會狀態紀錄，因此規則設計上較為複雜，需要雙向設定。

pfSense

> all add operation are add to bottom

1. Interfaces/vlan 5 IPv4 Configuration Type = Static IPv4
   IPv4 Address = 10.5.0.1/24

   Interfaces/vlan 8 IPv4 Configuration Type = Static IPv4
   IPv4 Address = 10.8.0.1/24

   Interfaces/vlan 99 IPv4 Configuration Type = Static IPv4
   IPv4 Address = 10.99.0.1/24

   Service/DHCP Server/vlan 5 Enable DHCP server on VLAN5 interface
   Range From = 10.5.0.1 To = 10.5.0.254
   DNS servers = 8.8.8.8
   DNS servers = 8.8.4.4

   Service/DHCP Server/vlan 8 Enable DHCP server on VLAN8 interface
   Range From = 10.8.0.1 To = 10.8.0.254
   DNS servers = 8.8.8.8
   DNS servers = 8.8.4.4

   Service/DHCP Server/vlan 99 Enable DHCP server on VLAN99 interface
   Range From = 10.99.0.1 To = 10.99.0.254
   DNS servers = 8.8.8.8
   DNS servers = 8.8.4.4

2. Firewall/Alias/IP/Add Name = GOOGLD_DNS
   IP or FQDN = 8.8.8.8
   Add Host
   IP or FQDN = 8.8.4.4

   Firewall/Alias/Ports/Add Name = ADMIN_PORTS
   Port = 22
   Add Port
   Port = 80
   Add Port
   Port = 443

Firewall/Alias/IP/Add Name = CSIE_WORKSTATIONS
IP or FQDN = linux1.csie.org
Add Host
IP or FQDN = linux2.csie.org
Add Host
IP or FQDN = linux3.csie.org

3. Firewall/Rules/vlan99/Add Source = VLAN99 net
Destination This firewall(self)
Destination Port Range FROM = ADMIN_PORTS TO = ADMIN_PORTS

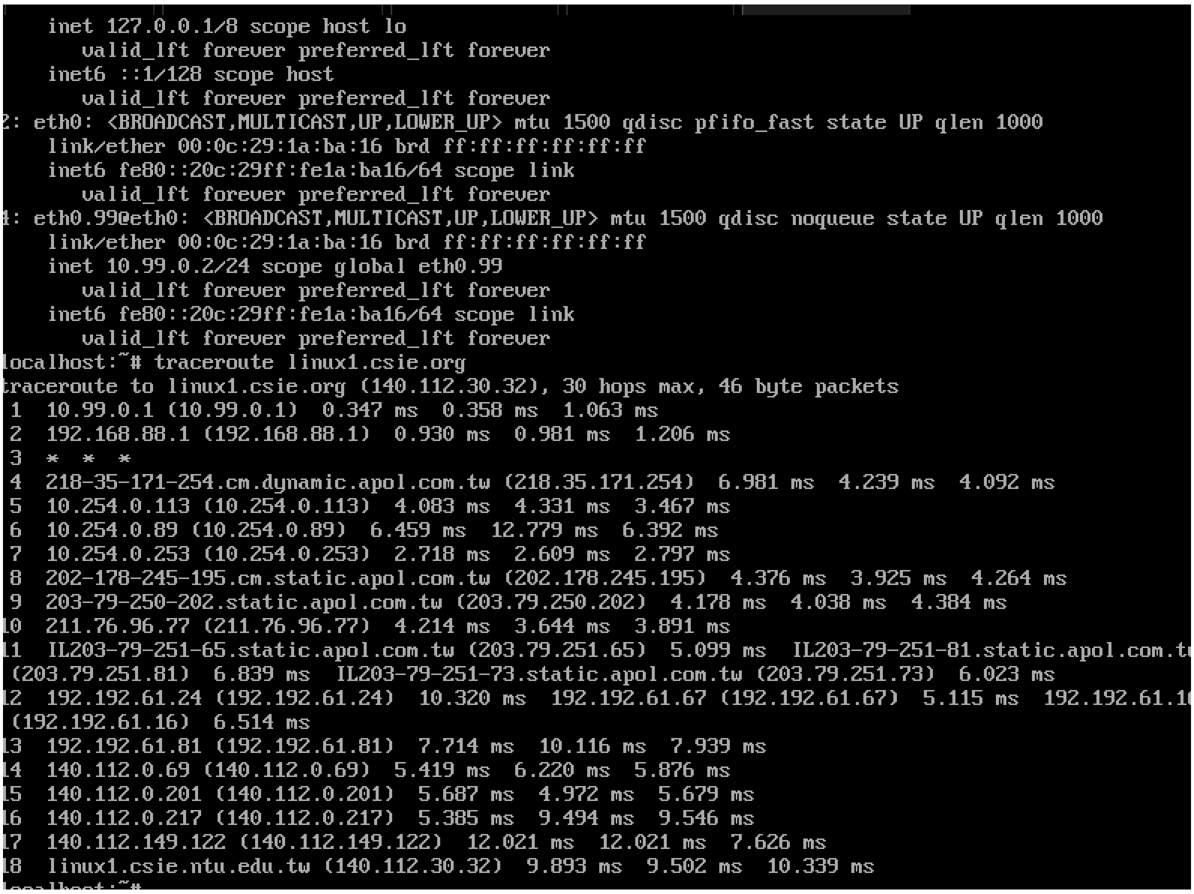
Firewall/Rules/vlan5/Add Action = Block
Source = VLAN5 net
Destination This firewall(self)
Destination Port Range FROM = ADMIN_PORTS TO = ADMIN_PORTS

Firewall/Rules/vlan8/Add Action = Block
Source = VLAN8 net
Destination This firewall(self)
Destination Port Range FROM = ADMIN_PORTS TO = ADMIN_PORTS

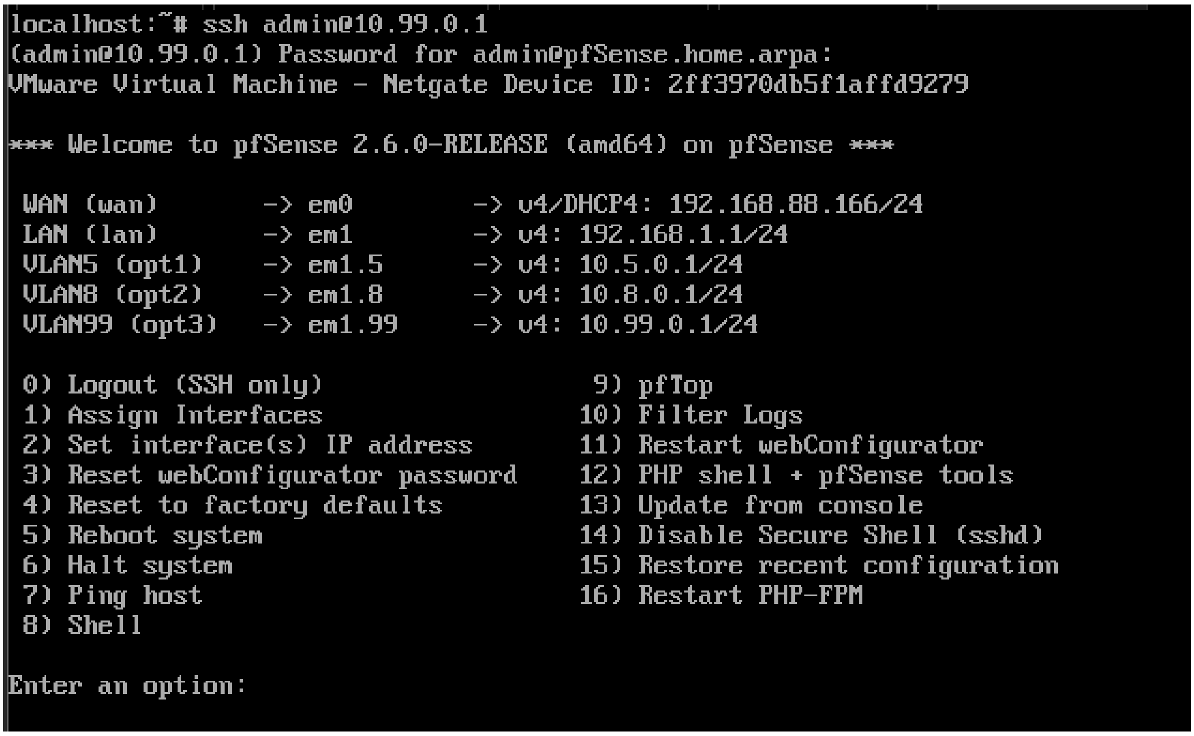
4. 這題我認為條件二就是第三題 不用額外開規則給ANY，因為如果不是的話第三題就會很沒有意義，而會在這題出現只是為了彌補題目的"只能"。

Firewall/Rules/vlan99/Add Protocol = UDP
Source = VLAN99 net
Destination = Single host or alias GOOGLE_DNS
Destination Port Range FROM = 53 TO = 53

Firewall/Rules/vlan99/Add Protocol = ANY
Address Family = IPv4+IPv6
Source = VLAN99 net
Destination = Single host or alias => CSIE_WORKSTATIONS



```
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:1a:ba:16 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:fe1a:ba16/64 scope link
       valid_lft forever preferred_lft forever
4: eth0.99@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP qlen 1000
    link/ether 00:0c:29:1a:ba:16 brd ff:ff:ff:ff:ff:ff
    inet 10.99.0.2/24 scope global eth0.99
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe1a:ba16/64 scope link
       valid_lft forever preferred_lft forever
localhost:~# traceroute linux1.csie.org
traceroute to linux1.csie.org (140.112.30.32), 30 hops max, 46 byte packets
 1  10.99.0.1 (10.99.0.1)  0.347 ms  0.358 ms  1.063 ms
 2  192.168.88.1 (192.168.88.1)  0.930 ms  0.981 ms  1.206 ms
 3  *  *  *
 4  218-35-171-254.cm.dynamic.apol.com.tw (218.35.171.254)  6.981 ms  4.239 ms  4.092 ms
 5  10.254.0.113 (10.254.0.113)  4.083 ms  4.331 ms  3.467 ms
 6  10.254.0.89 (10.254.0.89)  6.459 ms  12.779 ms  6.392 ms
 7  10.254.0.253 (10.254.0.253)  2.718 ms  2.609 ms  2.797 ms
 8  202-178-245-195.cm.static.apol.com.tw (202.178.245.195)  4.376 ms  3.925 ms  4.264 ms
 9  203-79-250-202.static.apol.com.tw (203.79.250.202)  4.178 ms  4.038 ms  4.384 ms
10  211.76.96.77 (211.76.96.77)  4.214 ms  3.644 ms  3.891 ms
11  IL203-79-251-65.static.apol.com.tw (203.79.251.65)  5.099 ms  IL203-79-251-81.static.apol.com.t
 (203.79.251.81)  6.839 ms  IL203-79-251-73.static.apol.com.tw (203.79.251.73)  6.023 ms
12  192.192.61.24 (192.192.61.24)  10.320 ms  192.192.61.67 (192.192.61.67)  5.115 ms  192.192.61.1
 (192.192.61.16)  6.514 ms
13  192.192.61.81 (192.192.61.81)  7.714 ms  10.116 ms  7.939 ms
14  140.112.0.69 (140.112.0.69)  5.419 ms  6.220 ms  5.876 ms
15  140.112.0.201 (140.112.0.201)  5.687 ms  4.972 ms  5.679 ms
16  140.112.0.217 (140.112.0.217)  5.385 ms  9.494 ms  9.546 ms
17  140.112.149.122 (140.112.149.122)  12.021 ms  12.021 ms  7.626 ms
18  linux1.csie.ntu.edu.tw (140.112.30.32)  9.893 ms  9.502 ms  10.339 ms
localhost:~#
```



```
localhost:~# ssh admin@10.99.0.1
(admin@10.99.0.1) Password for admin@pfSense.home.arpa:
VMware Virtual Machine - Netgate Device ID: 2ff3970db5f1affd9279

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.88.166/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 VLAN5 (opt1)    -> em1.5      -> v4: 10.5.0.1/24
 VLAN8 (opt2)    -> em1.8      -> v4: 10.8.0.1/24
 VLAN99 (opt3)   -> em1.99     -> v4: 10.99.0.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

5. Firewall/Rules/vlan5/Add   Protocol = ICMP
                                  ICMP Subtypes = Echo request
                                  Source = VLAN5 net
                                  Destination = VLAN8 net

Firewall/Rules/vlan8/Add   Protocol = ICMP
Action = Block
ICMP Subtypes = Echo request
Source = VLAN8 net
Destination = VLAN5 net

6. Firewall/Schedules/Add Schedule Name = V5
Month = May_22
Date 10
Add Time

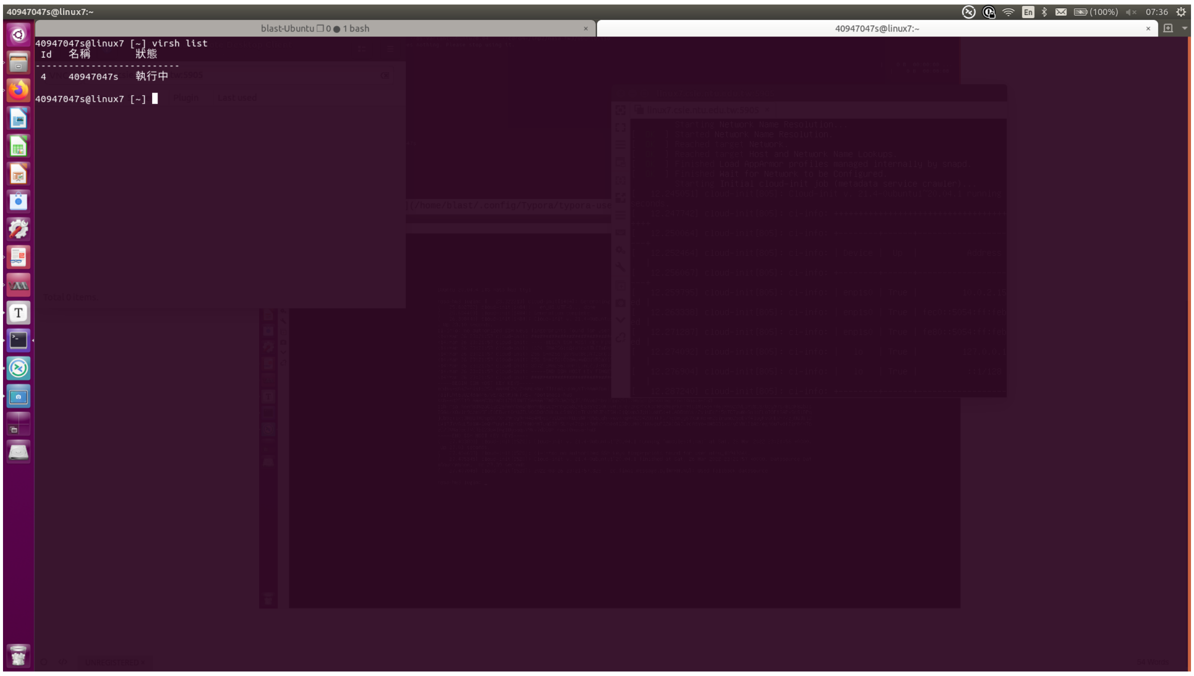
Firewall/Rules/vlan5/Add to Top Action = Block
Address Family = IPv4+IPv6
Protocal = Any
Source = VLAN5 net
Destination = any
Display Advanced
Schedule = V5

SA

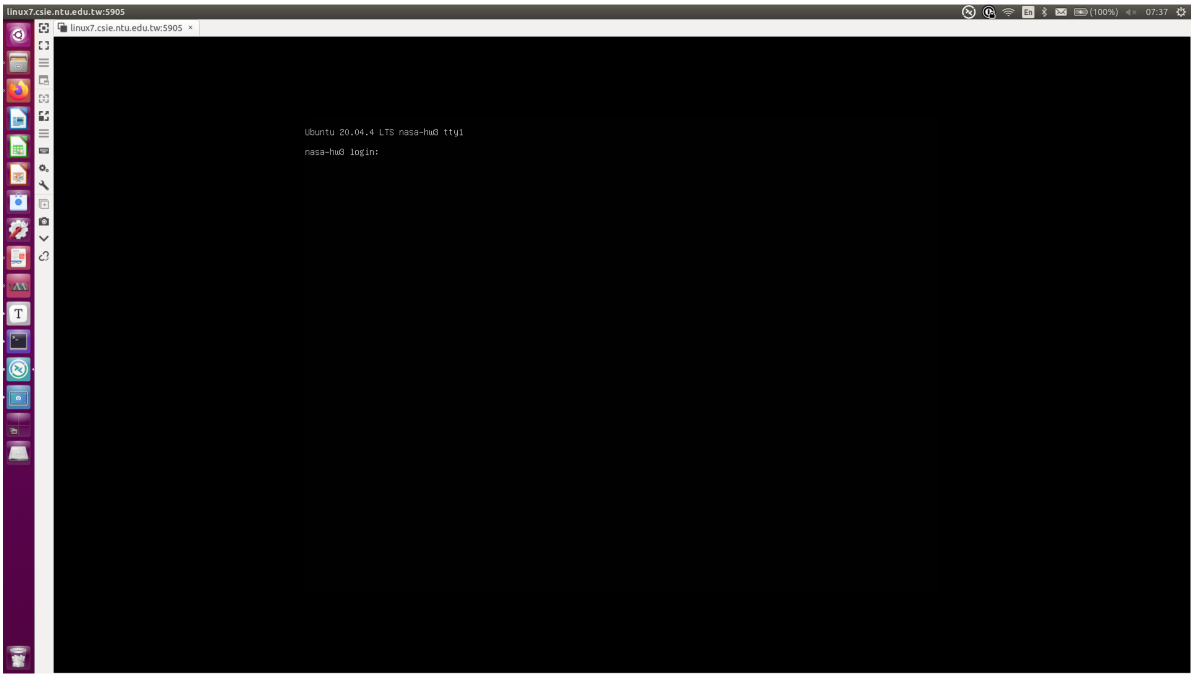
> Install ubuntu on vish: https://notes.wadeism.net/post/kvm-create-vm-in-terminal/
> Enable Vish on Linux: https://www.cyberciti.biz/faq/how-to-enable-kvm-virsh-console-access-for-ubuntu-linux-vm/

1. KVM & Virsh

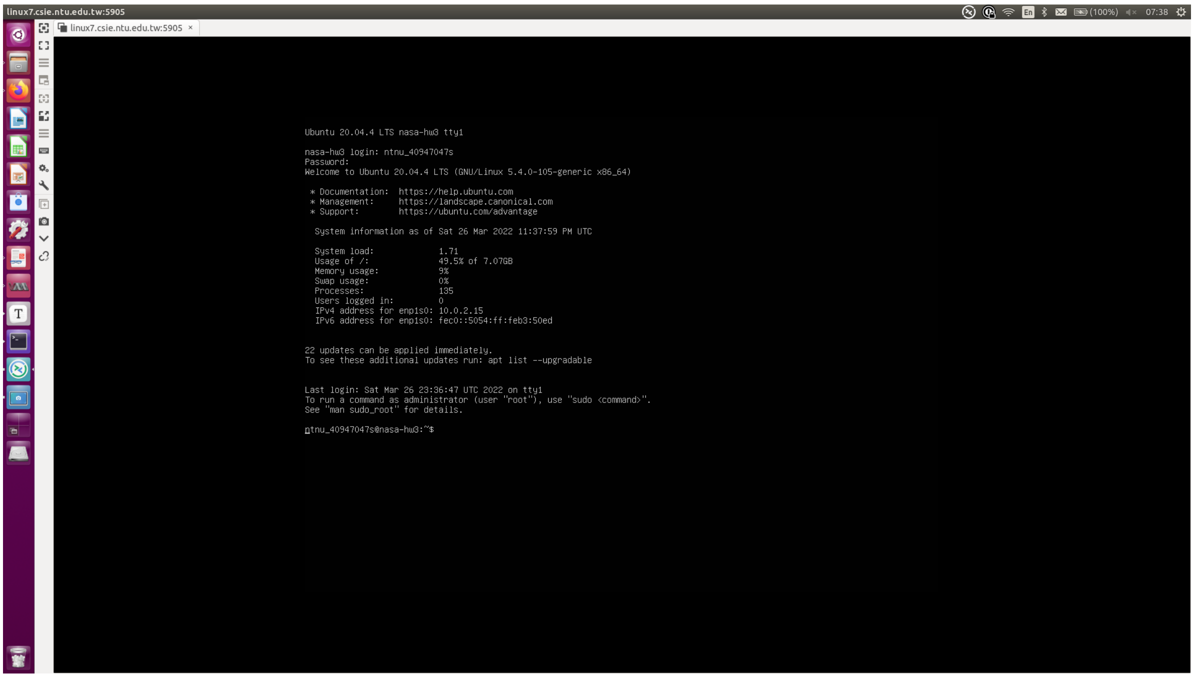
1.



```
40947047s@linux7 [~] virsh list
 Id   名稱         狀態
---------------------------
 4    40947047s    執行中

40947047s@linux7 [~] █
```

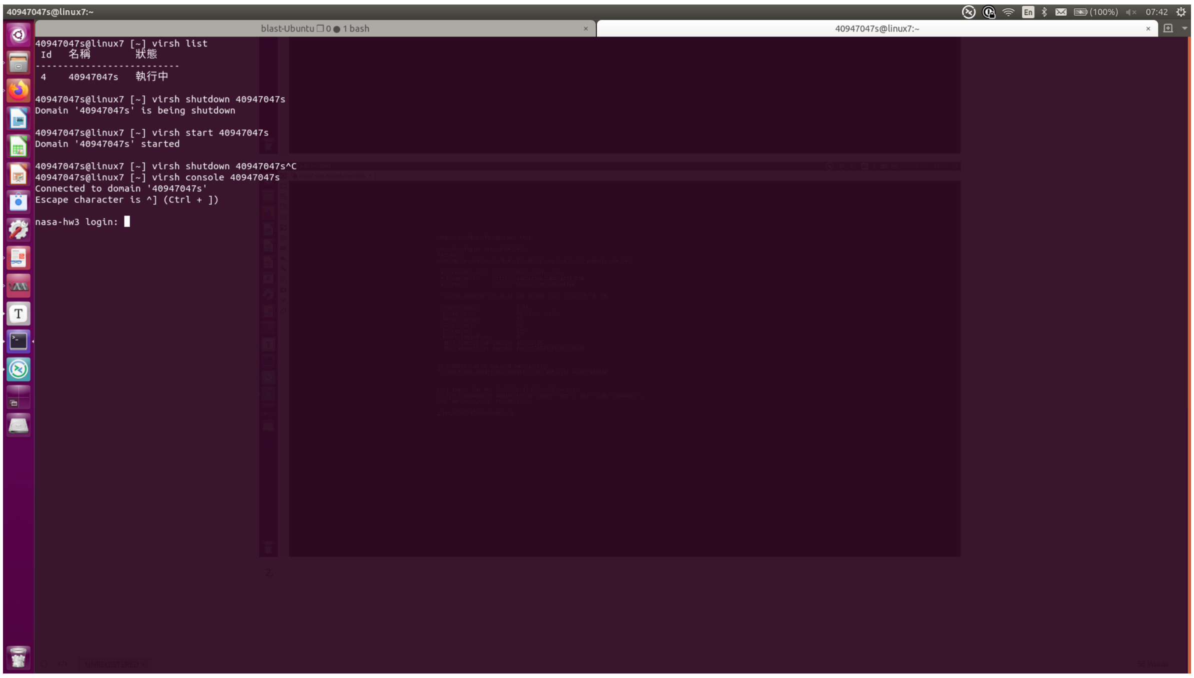


```
Ubuntu 20.04.4 LTS nasa-hw3 tty1

nasa-hw3 login:
```



```
Ubuntu 20.04.4 LTS nasa-hw3 tty1

nasa-hw3 login: ntnu_40947047s
Password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-105-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 26 Mar 2022 11:37:59 PM UTC

  System load:             1.71
  Usage of /:              49.5% of 7.07GB
  Memory usage:            9%
  Swap usage:              0%
  Processes:               135
  Users logged in:         0
  IPv4 address for enp1s0: 10.0.2.15
  IPv6 address for enp1s0: fec0::5054:ff:feb3:50ed


22 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Sat Mar 26 23:36:47 UTC 2022 on tty1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ntnu_40947047s@nasa-hw3:~$
```

2.

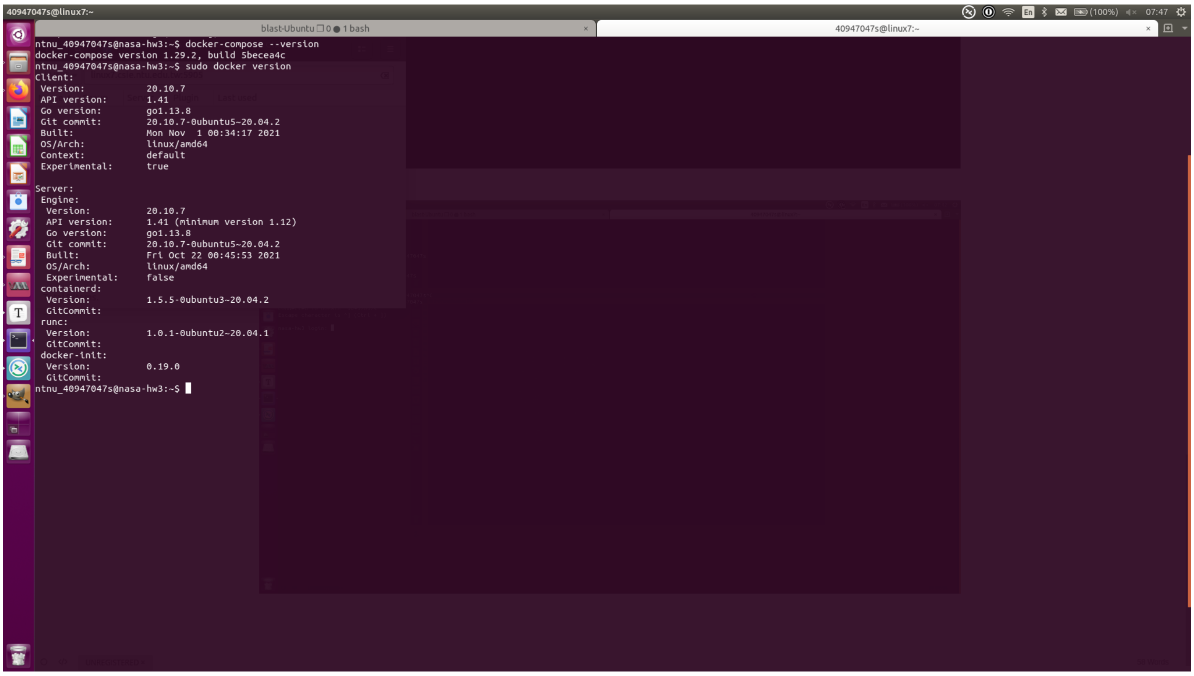


```
40947047s@linux7 [~] virsh list
 Id   名稱          狀態
---------------------------
 4    40947047s   執行中

40947047s@linux7 [~] virsh shutdown 40947047s
Domain '40947047s' is being shutdown

40947047s@linux7 [~] virsh start 40947047s
Domain '40947047s' started

40947047s@linux7 [~] virsh shutdown 40947047s^C
40947047s@linux7 [~] virsh console 40947047s
Connected to domain '40947047s'
Escape character is ^] (Ctrl + ])

nasa-hw3 login: 
```

2. Docker

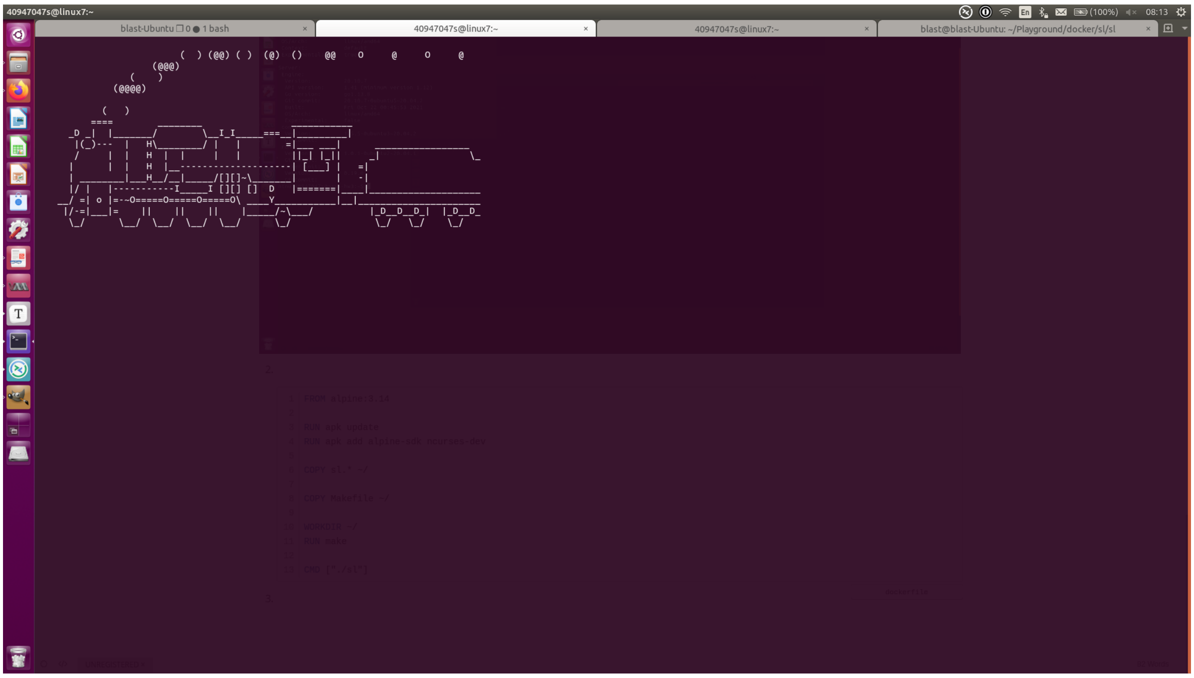
> Install docker-compose: https://docs.docker.com/compose/install/
>
> How to use docker alpine: https://hub.docker.com/_/alpine
>
> Build-essential on alpine package manager: https://github.com/gliderlabs/docker-alpine/issues/24
>
> Send POST request by curl: https://gist.github.com/subfuzion/08c5d85437d5d4f00e58

1.



```
ntnu_40947047s@nasa-hw3:~$ docker-compose --version
docker-compose version 1.29.2, build 5becea4c
ntnu_40947047s@nasa-hw3:~$ sudo docker version
Client:
 Version:           20.10.7
 API version:       1.41
 Go version:        go1.13.8
 Git commit:        20.10.7-0ubuntu5~20.04.2
 Built:             Mon Nov  1 00:34:17 2021
 OS/Arch:           linux/amd64
 Context:           default
 Experimental:      true

Server:
 Engine:
  Version:          20.10.7
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.13.8
  Git commit:       20.10.7-0ubuntu5~20.04.2
  Built:            Fri Oct 22 00:45:53 2021
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.5.5-0ubuntu3~20.04.2
  GitCommit:
 runc:
  Version:          1.0.1-0ubuntu2~20.04.1
  GitCommit:
 docker-init:
  Version:          0.19.0
  GitCommit:
ntnu_40947047s@nasa-hw3:~$ 
```

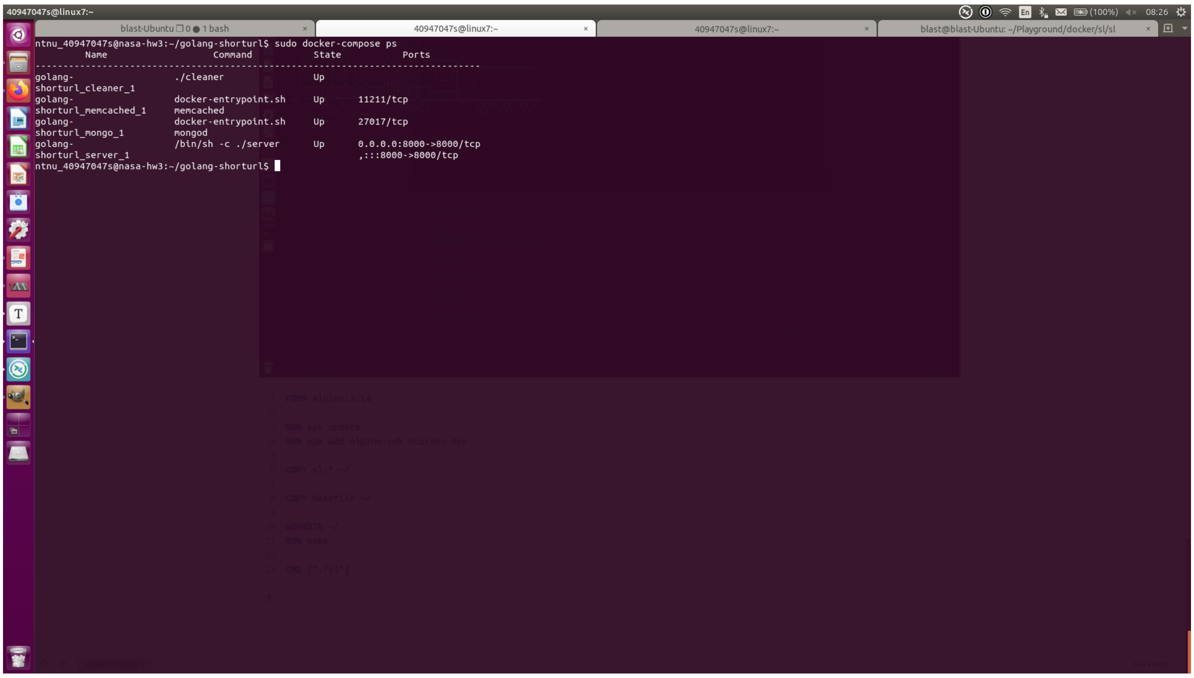
2.



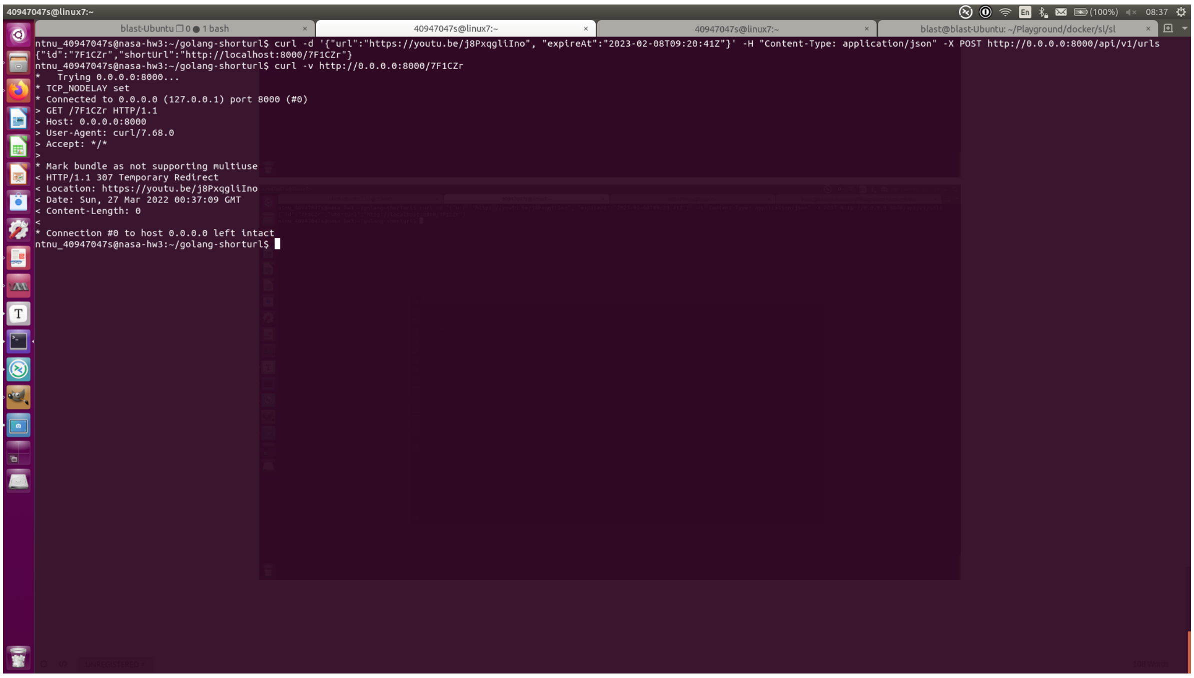
```
                    (  ) (@@) ( )  (@)  ()    @@    O     @     O     @
                 (@@@)
              (    )
          (@@@@)

        (   )
      ====        ________                ___________
  _D _|  |_______/        \__I_I_____===__|_________|
   |(_)---  |   H\________/ |   |        =|___ ___|      ________________
   /     |  |   H  |  |     |   |         ||_| |_||     _|                \_
  |      |  |   H  |__--------------------| [___] |   =|
  | ________|___H__/__|_____/[][]~\_______|       |   -|
  |/ |   |-----------I_____I [][] []  D   |=======|____|_____________________
__/ =| o |=-~O=====O=====O=====O\ ____Y___________|__|________________________
 |/-=|___|=    ||    ||    ||    |_____/~\___/          |_D__D__D_|  |_D__D_
  \_/      \__/  \__/  \__/  \__/      \_/               \_/   \_/    \_/
```

```dockerfile
FROM alpine:3.14

RUN apk update
RUN apk add alpine-sdk ncurses-dev

COPY sl.* ~/

COPY Makefile ~/

WORKDIR ~/
RUN make

CMD ["./sl"]
```

3.



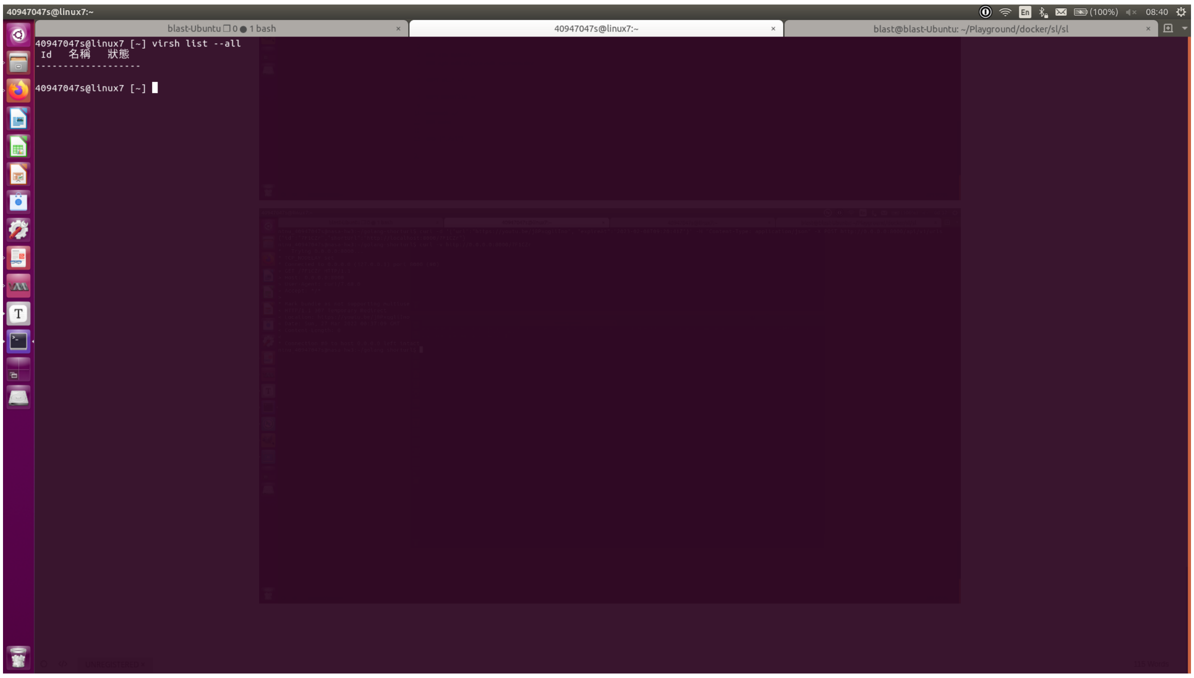
```
ntnu_40947047s@nasa-hw3:~/golang-shorturl$ sudo docker-compose ps
         Name                    Command            State             Ports
--------------------------------------------------------------------------------
golang-                   ./cleaner                 Up
shorturl_cleaner_1
golang-                   docker-entrypoint.sh      Up      11211/tcp
shorturl_memcached_1      memcached
golang-                   docker-entrypoint.sh      Up      27017/tcp
shorturl_mongo_1          mongod
golang-                   /bin/sh -c ./server       Up      0.0.0.0:8000->8000/tcp
shorturl_server_1                                           ,:::8000->8000/tcp
ntnu_40947047s@nasa-hw3:~/golang-shorturl$ █
```



40947047s@linux7:~
08:37
blast-Ubuntu ☐ 0 ● 1 bash
40947047s@linux7:~
40947047s@linux7:~
blast@blast-Ubuntu: ~/Playground/docker/sl/sl

```
ntnu_40947047s@nasa-hw3:~/golang-shorturl$ curl -d '{"url":"https://youtu.be/j8PxqgliIno", "expireAt":"2023-02-08T09:20:41Z"}' -H "Content-Type: application/json" -X POST http://0.0.0.0:8000/api/v1/urls
{"id":"7F1CZr","shortUrl":"http://localhost:8000/7F1CZr"}
ntnu_40947047s@nasa-hw3:~/golang-shorturl$ curl -v http://0.0.0.0:8000/7F1CZr
*   Trying 0.0.0.0:8000...
* TCP_NODELAY set
* Connected to 0.0.0.0 (127.0.0.1) port 8000 (#0)
> GET /7F1CZr HTTP/1.1
> Host: 0.0.0.0:8000
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 307 Temporary Redirect
< Location: https://youtu.be/j8PxqgliIno
< Date: Sun, 27 Mar 2022 00:37:09 GMT
< Content-Length: 0
<
* Connection #0 to host 0.0.0.0 left intact
ntnu_40947047s@nasa-hw3:~/golang-shorturl$ 
```

4.



40947047s@linux7:~
08:40
blast-Ubuntu ☐ 0 ● 1 bash
40947047s@linux7:~
blast@blast-Ubuntu: ~/Playground/docker/sl/sl

```
40947047s@linux7 [~] virsh list --all
 Id   名稱   狀態
--------------------

40947047s@linux7 [~] 
```