NASA hw9繳交版

Author: B12705014陳泊華

VM setup

註：我的電腦是Mac M1，而本次作業由於qcow2檔案在工作站、本地UTM都嘗試過各種方法（見以下指令）花了不少時間但都沒能架出內網互通（見下圖，少了一張網卡但工作站上也無法使用bridge設定）

```
[nasa@nfs-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic ens3
       valid_lft 84164sec preferred_lft 73364sec
    inet6 fec0::5054:ff:fe12:3456/64 scope site dynamic mngtmpaddr noprefixroute

       valid_lft 86115sec preferred_lft 14115sec
    inet6 fec0::a6e:8474:b074:24af/64 scope site dynamic mngtmpaddr noprefixrout
e
       valid_lft 86115sec preferred_lft 14115sec
    inet6 fe80::e742:54c4:c91c:1704/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe12:3456/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[nasa@nfs-server ~]$
```

後來詢問助教但還是沒有找到適合的解法，最後決定先用Lab的VM把能做的題目先盡力做完，還請見諒

- Server

  ```
  $ qemu-system-x86_64 -cpu host -enable-kvm -m 4096 -vnc
  140.112.30.188:0,to=10000,password=on -monitor stdio -drive file=nfs-
  server.qcow2,format=qcow2,media=disk -vga virtio -nic
  user,hostfwd=tcp::2287-:22,hostfwd=tcp::2289-:2049 -bios
  /usr/share/ovmf/x64/OVMF.fd
  ```

從本機：

```
$ ssh nasa@ws3.csie.ntu.edu.tw -p 2287
```

- Client

  ```
  $ qemu-system-x86_64 -cpu host -enable-kvm -m 4096 -vnc
  ```

```
140.112.30.188:0,to=10000,password=on -monitor stdio -drive file=nfs-client.qcow2,format=qcow2,media=disk -vga virtio -nic user,hostfwd=tcp::2288-:22,hostfwd=tcp::2290-:2049 -bios /usr/share/ovmf/x64/OVMF.fd
```

從本機：

```
$ ssh nasa@ws3.csie.ntu.edu.tw -p 2288
```

1

(a)

1. 按照lab的方法在server的/etc/exports進行設定後 `$ systemctl start nfs-server`
2. 在client端mount： `$ sudo mount -t nfs 192.168.64.9:/srv/nfs/share /mnt/nfs-share`
3. 在client端修改/etc/fstab檔案使其能自動掛載

```
# Static information about the filesystems.
# See fstab(5) for details.

# <file system> <dir> <type> <options> <dump> <pass>
#/swap/swapfile none swap defaults 0 0

192.168.64.9:/srv/nfs/share /mnt/nfs-share nfs defaults 0 0
```

```
$ df -h
```

```
[arch@archlinux ~]$ df -h
Filesystem                  Size  Used Avail Use% Mounted on
dev                         2.0G     0  2.0G   0% /dev
run                         2.0G  712K  2.0G   1% /run
/dev/sda3                    40G  1.4G   38G   4% /
tmpfs                       2.0G     0  2.0G   0% /dev/shm
tmpfs                       2.0G     0  2.0G   0% /tmp
tmpfs                       392M  4.0K  392M   1% /run/user/1000
192.168.64.9:/srv/nfs/share  40G  1.4G   38G   4% /mnt/nfs-share
[arch@archlinux ~]$ cd /mnt/nfs-share
[arch@archlinux nfs-share]$ ls -al
```

(b)

1. client端：/mnt/nfs-share: `$ touch test`

2. server端：ls -al /srv/nfs/share

```
[root@archlinux share]# ls -al
total 0
drwxrwxrwx 1 root root  8 Apr 28 09:10 .
drwxr-xr-x 1 root root 10 Apr 22 03:46 ..
-rw-r--r-- 1 root root  0 Apr 28 01:25 test
[root@archlinux share]#
```

©

*本題由於使用Lab的VM，所以自行adduser進行測試

在server端：

```
$ sudo useradd -m asan
$ sudo passwd asan
$ sudo chown asan:asan /srv/nfs/share/asan
$ sudo chmod 700 /srv/nfs/share/asan
```

測試：使用arch身份嘗試進入資料夾

```
$ ls /srv/nfs/share/asan
```

```
[arch@archlinux ~]$ ls /srv/nfs/share/asan
ls: cannot open directory '/srv/nfs/share/asan': Permission denied
```

```
[asan@archlinux asan]$ ls -al
total 0
drwx------ 1 asan asan  0 Apr 28 09:11 .
drwxrwxrwx 1 root root 16 Apr 28 09:11 ..
[asan@archlinux asan]$
```

reference:
NFS Lab slides

2

(a)
AUTH_SYS標準認證機制是一種基於主機的身份驗證方法，它使用主機上的用戶和群組ID來識別用戶；當Asan嘗試訪問NFS伺服器上的共享目錄時，NFS 伺服器會檢查Asan的用戶ID和群組ID是否具有適當的許可權來訪問目錄。如果Asan在伺服器上沒有相應的用戶或群組ID，或者權限設置不正確，就有可能無法正確訪問目錄。

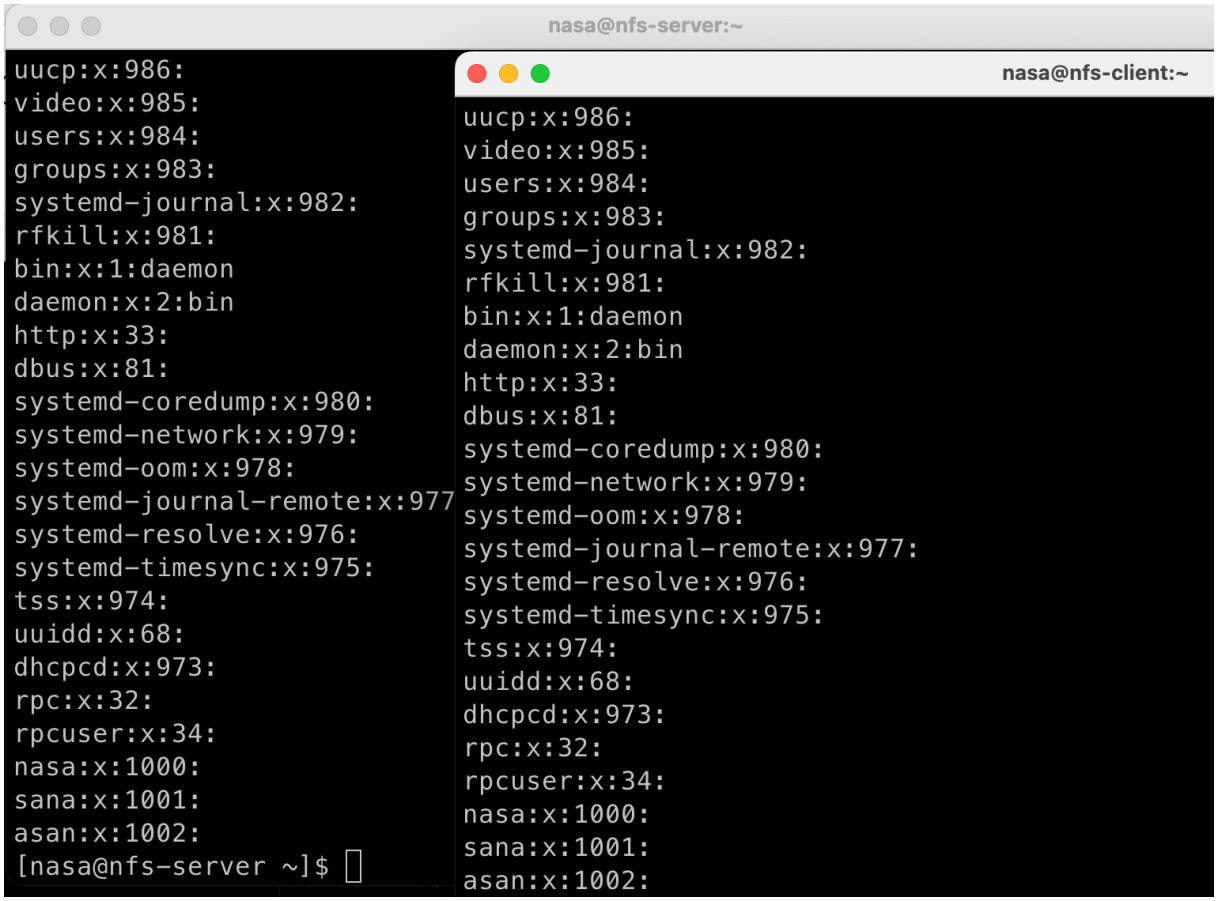
(b)
*本題由於使用Lab的VM，所以自行adduser進行測試

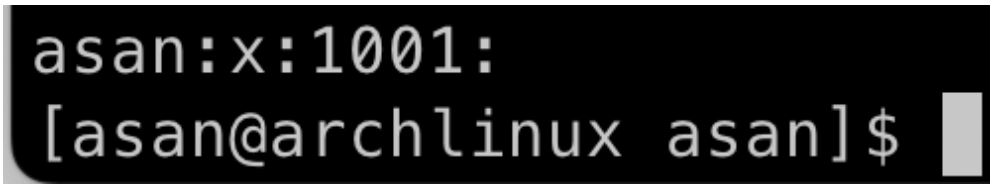
在client端：

```
$ sudo useradd -m asan
$ sudo passwd asan
```

1. 檢查server與client端兩邊的UID、GID是否一致

```
$ cat /etc/group
```





2. 在server端/etc/exports裡新增Asan的目錄共享

```
# /etc/exports - exports(5) - directories exported to NFS clients
#
# Example for NFSv3:
#  /srv/home        hostname1(rw,sync) hostname2(ro,sync)
# Example for NFSv4:
#  /srv/nfs4        hostname1(rw,sync,fsid=0)
#  /srv/nfs4/home   hostname1(rw,sync,nohide)
# Using Kerberos and integrity checking:
#  /srv/nfs4        *(rw,sync,sec=krb5i,fsid=0)
#  /srv/nfs4/home   *(rw,sync,sec=krb5i,nohide)
#
# Use `exportfs -arv` to reload.
/srv/nfs 192.168.64.10(rw,sync,fsid=0)
/srv/nfs/share 192.168.64.10(rw,sync,no_root_squash)
/srv/nfs/share/asan 192.168.64.10(rw,sync)
```

reference:
https://blog.csdn.net/fangyinchun/article/details/84599471
(https://blog.csdn.net/fangyinchun/article/details/84599471)

3

(a)
RPCSEC_GSS認證模式使用Kerberos 5票據加密來提供安全性。透過 RPCSEC_GSS，NFS客戶端和伺服器可以使用Kerberos來進行身份驗證和加密通信，從而保護NFS數據的安全性。因為使用了加密和身份驗證，RPCSEC_GSS不容易受到中間人攻擊等安全威脅的影響。

(b)
*本題所架設的KDC一樣複製至lab的nfs-server（因為hw的qcow檔在本地尚無法順利boot起來）

1. ssh後ip a查看基本設定

```
[arch@archlinux ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether b6:87:02:88:19:51 brd ff:ff:ff:ff:ff:ff
    altname enp0s1
    inet 192.168.64.11/24 metric 1024 brd 192.168.64.255 scope global dynamic et
h0
       valid_lft 85736sec preferred_lft 85736sec
    inet6 fd70:70a3:a6a8:38c8:b487:2ff:fe88:1951/64 scope global dynamic mngtmpa
ddr noprefixroute
       valid_lft 2591981sec preferred_lft 604781sec
    inet6 fe80::b487:2ff:fe88:1951/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[arch@archlinux ~]$
```

2. 利用date檢查三台VM的時間一致

配置KDC伺服器的/etc/krb5.conf文件，指定Kerberos領域和KDC訊息

reference:
(i) https://linux.vbird.org/events/kerberos.php (https://linux.vbird.org/events/kerberos.php)
(ii) https://wiki.archlinux.org/title/Kerberos (https://wiki.archlinux.org/title/Kerberos)