Contents

[hide]

- 1 目標
- 2 FTP
  - 2.1 File Transfer Protocol(FTP)
  - 2.2 man 5 vsftpd.conf
  - 2.3 vsftp LAB 1:vsftpd啟動及使用
  - 2.4 vsftp LAB2:設定一般使用者可以登入
  - 2.5 vsftp LAB 3:設定chroot
  - 2.6 vsftp LAB 4:連線限制
- 3 NFS
  - 3.1 網路檔案服務 (NFS)
  - 3.2 伺服器檔案：NFS
  - 3.3 NFS Server
  - 3.4 和防火牆相關的 port
  - 3.5 NFS 工具
  - 3.6 客戶端的 NFS
  - 3.7 NFS LAB1: NFS export and AUTOFS 自動掛載目錄
    - 3.7.1 題目(a):Export /share 目錄
    - 3.7.2 NFS 客戶端測試及掛載
    - 3.7.3 題目(b):AUTOFS 自動掛載目錄
  - 3.8 NFS:LAB2依下列設定設定NFS
- 4 目標檢核
- 5 實作

目標

- Configure Network File System (NFS) file sharing
- Describe the NFS service
- Configure a network mountable directory
- Secure your new NFS share for use in an internal network only

FTP

File Transfer Protocol(FTP)

- vsftpd ：在此Linux中預設安裝的 FTP server

- vsftpd - 在此Linux 中預設安裝的 FTP server

1. vsftpd is a secure and fast FTP server for UNIX-like systems that is used on many large and critical Internet sites. Its rich feature set includes SSL encryption, IPv6, bandwidth throttling, PAM integration, virtual users, virtual IPs and per-user / per-IP configuration.
2. 官方網站：http://vsftpd.beasts.org/

- 不用修改 xinetd ，就具有 stand alone daemon 和 super daemon 兩種方式可以供使用
- 允許系統、匿名或是虛擬使用者登入
- The anonymous directory hierarchy is provided by the vsftpd RPM
- /etc/vsftpd/vsftpd.conf 為主要的設定檔
- 型態: SystemV-managed service
- 套件: vsftpd
- 服務程式: /usr/sbin/vsftpd
- 啟動程序: /etc/init.d/vsftpd
- Ports: 21 (ftp), 20 (ftp-data)
- 設定: /etc/vsftpd/vsftpd.conf /etc/vsftpd.ftpusers /etc/pam.d/vsftpd
- 紀錄檔(Log): /var/log/xferlog
- 相關設定選項: tcp_wrappers, ip_conntrack_ftp, ip_nat_ftp
- 關於 vsftpd 的存取權限設定

存取控制	相關檔案及設定
Application	/etc/vsftpd/vsftpd.conf
PAM	/etc/pam.d/vsftpd
xinetd	N/A
tcp_wrappers	有連結，且被vsftpd的服務使用
SELinux	ensure correct file contexts; change on boolean
Netfilter,IPv4	tcp and upd port 21 and ip_conntrack_ftp.ko

- 關於 ftp 的 selinux 文件可以使用 man -k ftp | grep selinux 找尋， 手冊為 man 8 ftpd_selinux
- 通常可以使用 semanage fcontext -l | grep ftp 來檢查 selinux 的 policy file
- 可以使用 getsebool -a | grep ftp 找尋相關的 booleans 值
- 允許匿名使用者上傳的 selinux 設定為：

1. setsebool allow_ftpd_full_access on

man 5 vsftpd.conf

- 官方手冊中的節錄

```
AME
       vsftpd.conf - config file for vsftpd

DESCRIPTION
       vsftpd.conf may be used to control vari-
       ous aspects of  vsftpd's  behaviour.  By
       default,  vsftpd  looks for this file at
       the  location   /etc/vsftpd/vsftpd.conf.
       However, you may override this by speci-
       fying a command line argument to vsftpd.
       The  command  line argument is the path-
       name  of  the  configuration  file  for
       vsftpd. This behaviour is useful because
       you may wish to use  an  advanced  inetd
```

```
          such  as  xinetd  to  launch vsftpd with
          different configuration files on  a  per
          virtual host basis.

        anonymous_enable
               Controls whether anonymous logins
               are permitted or not. If enabled,
               both the usernames ftp and anony-
               mous  are recognised as anonymous
               logins.

               Default: YES
         chroot_list_enable
               If  activated,  you may provide a
               list  of  local  users  who   are
               placed  in  a  chroot()  jail  in
               their home directory upon  login.
               The meaning is slightly different
               if chroot_local_user  is  set  to
               YES.   In  this  case,  the  list
               becomes a list of users which are
               NOT  to  be  placed in a chroot()
               jail.  By default, the file  con-
               taining      this      list      is
               /etc/vsftpd/chroot_list, but  you
               may   override   this   with   the
               chroot_list_file setting.

               Default: NO

         chroot_local_user
               If set to YES, local  users  will
               be   (by  default)  placed  in  a
               chroot()  jail  in   their   home
               directory  after login.  Warning:
               This option has security implica-
               tions,  especially  if  the users
               have upload permission, or  shell
               access.  Only  enable if you know
               what you are  doing.   Note  that
               these  security  implications are
               not vsftpd specific.  They  apply
               to all FTP daemons which offer to
               put  local  users   in   chroot()
               jails.

               Default: NO
```

vsftp LAB 1:vsftpd啟動及使用

- 啟動 vsftpd

```
[root@localhost ~]# service vsftpd restart
```

- 用最原始的模式 ftp client 登入系統

```
[root@localhost ~]# ftp localhost
Connected to localhost.localdomain.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (localhost:root): ftp
```

```
Name (localhost:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,232,103)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jan 17  2007 pub
226 Directory send OK.
ftp> bye
221 Goodbye.
```

vsftp LAB2:設定一般使用者可以登入

- 修改設定檔案 vsftpd.conf

```
[root@localhost ~]# gedit /etc/vsftpd/vsftpd.conf
local_enable=YES
write_enable=YES
```

- 設定完成後需要重新啟動讀入設定檔

```
[root@localhost ~]# service vsftpd restart
正在關閉 vsftpd:                                          [  確定  ]
正在啟動 vsftpd 中的 vsftpd:                               [  確定  ]
```

- 登入測試,請使用任一各本地端使用者帳戶登入 ftp server 這時候會產生 selinux 的警告訊息,內容大致如下

```
SummarySELinux is preventing the ftp daemon from reading
users home directories (home).
Detailed DescriptionSELinux has denied the ftp daemon
access to users home directories (home).
Someone is attempting to login via your ftp daemon to
a user account.
If you only setup ftp to allow anonymous ftp, this
could signal a intrusion attempt.
Allowing AccessIf you want ftp to allow users access to
their home directories you need to turn on the
ftp_home_dir boolean: "setsebool -P ftp_home_dir=1"
The following command will allow this access:
setsebool -P ftp_home_dir=1
Additional Information
```

- 只需要一警示說明,執行指令 "setsebool -P ftp_home_dir=1" 即可取消取消 SELINUX 針對使用者不能讀取 user_home_dir 的限制取消.

```
[root@localhost ~]# setsebool -P ftp_home_dir=1
```

vsftp LAB 3:設定chroot

- 把登入系統的使用者限定他只能在自己的 home 內活動

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
# users to NOT chroot().
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
```

- 要建立 chroot_list 這個檔案，並把所有在 /etc/passwd 的所有帳號，都寫入此檔案。使用

要建立 chroot_list 這個檔案，並把所有在 /etc/passwd 的所有帳號，都寫入此檔案，使用者只要在此檔案內，都是 chroot 的範圍。

```
[root@localhost ~]# cut -d: -f1 /etc/passwd > /etc/vsftpd/chroot_list
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

- 以上 chroot 的設定也可以使用 chroot_local_user=YES 這各參數，這樣這各 chroot_list 就會成為非 chroot() 的列表清單，請使用者自行決定方便使用的方式。底下為 chroot any user 的設定。

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
```

vsftp LAB 4:連線限制

- 設定：example.com(192.168.0.0/24) 可以匿名登入，其他網域則終止連線
- 先檢查 vsftpd 有無支援 tcp wrapper ， ldd 指令可以列出該檔案關聯的函式庫

```
[root@server1 ~]# ldd /usr/sbin/vsftpd | grep libwrap
        libwrap.so.0 => /usr/lib/libwrap.so.0 (0x00a5c000)
```

- 設定 Netfilter 確定保沒有 iptable 的限制在，ftp 跑的是 tcp 21 port 網段為 192.168.0.0/24

```
[root@server1 ~]# iptables -I INPUT 1 -s 192.168.0.0/24 -p tcp --dport 21 -j ACCEPT
[root@server1 ~]# iptables -A INPUT -i eth0 -p tcp --dport 21 -j REJECT
[root@server1 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT  tcp  --  192.168.0.0/24 0.0.0.0/0  tcp dpt:21

REJECT  tcp  --  0.0.0.0/0      0.0.0.0/0  tcp dpt:21
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- 記得要儲存 service iptables save ，並且要設定 iptables service 有預設啟動
- example.com 網段為 192.168.0.0/24 所以設定為

```
[root@server1 ~]# vi /etc/hosts.allow
vsftpd: 192.168.0.
[root@server1 ~]# vi /etc/hosts.deny
vsftpd:  ALL
```

- 請使用 ftp 192.168.0.XX 驗證ftp的存取

NFS

網路檔案服務 (NFS)

- 在這裡的 NFS 和 BSD 或 UNIX 系統的 nfs 式幾乎一樣的....

1. 輸出的設定檔在 /etc/exports
2. 伺服器可以使用 exportfs -r or service nfs reload 重新載入輸出的目錄設定檔案
3. 分享的目錄能夠被 mount command
4. 這各 NFS server 是一個 RPC service 所以需要 portmap 程式

- 驗證這些服務是否執行可以使用列命令：

1. rpcinfo -p
2. service portmap status
3. service nfs status

- 驗證這些服務是否在遠端主機執行，可以用：

1. showmount -e station250.example.com
2. rpcinfo -p station250.example.com

- 還有哪些？

1. exportfs -r
2. exportfs -v
3. exportfs -a
4. exportfs -u

- portmap, rpc.nfsd and rpc.mountd 這三個套件都會被 nfs Server 所需要

伺服器檔案：NFS

- 類別: Standalone service
- 套件: nfs-utils
- 服務: rpc.nfsd, rpc.lockd, rpciod, rpc.mountd, rpc.rquotad, rpc.statd
- 啟動腳本: /etc/init.d/nfs, /etc/init.d/nfslock
- Ports: 2049(nfsd), Others assigned by portmap (111)
- 設定檔: /etc/exports
- 相關設定: portmap (mandatory), tcp_wrappers
  - tcp_wrappers 需要兩個服務名稱：mountd and portmap 這兩個
  - 例如 hosts.allow 設定 mountd, portmap:192.168.0. 這樣可以允許 192.168.0.的 mountd, portmap服務通過

NFS Server

- Exported directories are defined in /etc/exports
- 輸出目錄被定義在 /etc/exports
- Each entry specifies the directory to share and the hosts allowed to access the share plus associated permissions and options
  - options should be specified
  - default options: (ro,sync,root_squash)
  - root mapped to nfsnobody
- default options: (ro,sync,root_squash)

1. rw：read-write，可讀寫的權限；
2. ro：read-only，唯讀的權限；
3. sync：資料同步寫入到記憶體與硬碟當中
4. async：資料會先暫存於記憶體當中
5. no_root_squash：登入 NFS 主機使用分享目錄的使用者，如果是 root 的話，那麼對於這個分享的目錄來說，他就具有 root 的權限
6. root_squash：在登入 NFS 主機使用分享之目錄的使用者如果是 root 時，那這個使用者的權限將被壓縮成為匿名使用者，通常他的 UID 與 GID 都會變成 nobody 帳號權限
7. all_squash：不論登入 NFS 的使用者身份為何， 他的身份都會被壓縮成為匿名使用者 nobody

和防火牆相關的 **port**

- Port Options for the Firewall
- mountd, statd, lockd and rquotad can be forced to use a static port
- Configuration variables in /etc/sysconfig/nfs
    - MOUNTD_PORT="4002"
    - STATD_PORT="4003"
    - LOCKD_TCPPORT="4004"
    - LOCKD_UDPPORT="4004"
    - RQUOTAD_PORT="4005"
    - STATD_OUTGOING_PORT="4006"
- 關於 nfs 的存取權限設定

存取控制	相關檔案及設定
Application	/etc/exports
PAM	N/A
xinetd	N/A
tcp_wrappers	/sbin/portmap有被連結到libwrap.a
SELinux	ensure correct file contexts; no change on boolean
Netfilter,IPv4	tcp and upd port 111 and 2049 are constant;see other port values in configuration

NFS 工具

- exportfs -v 輸出 NFS 的目錄
- showmount -e hostname 觀看 NFS 分享的資訊
- rpcinfo -p hostname 觀看RPC狀況

客戶端的 **NFS**

- NFS 被實作為一個 kernel module，也就是開機時就有載入
- 可以使用/etc/fstab 掛載
- NFS 可以在開機時透過 /etc/init.d/nfs 程式啟動
- 可以使用 autofs 安裝NFS的服務的需求和卸載時
- nfs 用戶端可供處理掛載的參數： man nfs 中關於 nfs 的部份

```
Options for the nfs file system type
```

rsize=n The number of bytes NFS uses when reading files from an NFS server. The rsize is negotiated between the server and client to determine the largest block size that both can support. The value specified by this option is the maximum size that could be used; however, the actual size used may be smaller. Note: Setting this size to a value less than the largest supported block size will adversely affect performance.

wsize=n The number of bytes NFS uses when writing files to an NFS server. The wsize is negotiated between the server and client to determine the largest block size that both can support. The value specified by this option is the maximum size that could be used; however, the actual size used may be smaller. Note: Setting this size to a value less than the largest supported block size will adversely affect performance.

intr This will allow NFS operations (on hard mounts) to be interrupted while waiting for a response from the server.

nolock Do not use locking. Do not start lockd.

noexec Do not allow direct execution of any binaries on the mounted file system. (Until recently it was possible to run binaries anyway using a command like /lib/ld*.so /mnt/binary. This trick fails since Linux 2.4.25 / 2.6.0.)

sync All I/O to the file system should be done synchronously. In case of media with limited number of write cycles (e.g. some flash drives) "sync" may cause life-cycle shortening.

soft If an NFS file operation has a major timeout then report an I/O error to the calling program. The default is to continue retrying NFS file operations indefinitely.

hard If an NFS file operation has a major timeout then report "server not responding" on the console and continue retrying indefinitely. This is the default.

intr If an NFS file operation has a major timeout and it is hard mounted, then allow signals to interupt the file operation and cause it to return EINTR to the calling program. The default is to not allow file operations to be interrupted.

NFS LAB1: NFS export and AUTOFS 自動掛載目錄

- 題目(a)：
  - Export 你的 /share 目錄通過 NFS Server 只(Only)給這個 example.com(192.168.3.0/24) 的網域使用，分享權限請設定為 read only,root_squash 。
  - 使用 mount 掛載 nfs 分享的目錄
  - The size of the buffer for read and write access is 8 KB.
  - The execution of binaries or shell scripts residing on the NFS filesystems is not allowed.
  - All I/O to the filesystem should be done synchronously

- All I/O to the filesystem should be done synchronously.

- 題目(b),接續上題：
  - Note: 因為你將不會有 root 存取, 你將不能夠把目錄掛載輸出到 /shared 目錄,使用你的 guest account 對於這系統服務測試.
  - 無論如何, the auto-mounter on the system has been configured such that it will automount your /shared directory under /home/guestx/nfs/stationx, where x is your station number.
  - 於是, successful execution of 「ls /home/guestx/nfs/stationx」 指示 that the automounter was able to automount your NFS share.

題目(a):Export /share 目錄

- Export 你的 /share 目錄通過 NFS Server 只(Only)給這個 example.com(192.168.3.0/24) 的網域使用，分享權限請設定為 read only,root_squash 。

```
# 如果沒有 /share 目錄請自行建立
[root@localhost ~]# mkdir /share
# 設定分享目錄及權限
[root@localhost ~]# vim /etc/exports
/share 192.168.3.0/24(ro,root_squash)
# 重新啟動 nfs server
[root@localhost ~]# /etc/init.d/nfs restart
Shutting down NFS mountd:                                  [  OK  ]
Shutting down NFS daemon:                                  [  OK  ]
Shutting down NFS quotas:                                  [  OK  ]
Shutting down NFS services:                                [  OK  ]
Starting NFS services:                                     [  OK  ]
Starting NFS quotas:                                       [  OK  ]

Starting NFS daemon:                                       [  OK  ]
Starting NFS mountd:                                       [  OK  ]

# 還要啟動這一個
[root@localhost ~]# /etc/init.d/nfslock restart
Stopping NFS locking:                                      [  OK  ]
Stopping NFS statd:                                        [  OK  ]
Starting NFS statd:                                        [  OK  ]
```

- 測試本機的 export 及 NFS Client 驗證
- 測試設定檔輸出

```
# 驗證設定檔的設定輸出
[root@localhost ~]# exportfs -v
/share          192.168.3.0/24(ro,wdelay,root_squash,no_subtree_check,anonuid=65534
,anongid=65534)
# 使用 showmount 在本機測試是否可工作
[root@localhost ~]# showmount -e 192.168.3.208
Export list for 192.168.3.208:
/share  192.168.3.0/24
```

NFS 客戶端測試及掛載

- 使用 mount 掛載 nfs 分享的目錄

1. The size of the buffer for read and write access is 8 KB.
2. The execution of binaries or shell scripts residing on the NFS filesystems is not allowed.

3. All I/O to the filesystem should be done synchronously.

- 切換到另一台主機，使用showmount 測試

```
[root@server153 ~]# showmount -e 192.168.3.208
Export list for 192.168.3.208:
/share  192.168.3.0/24
# 建立一個準備掛載的目錄
[root@server153 ~]# mkdir /mnt/share
```

- 使用 mount -t nfs 來掛載

```
# mount /mnt/share
[root@server153 ~]# mount -t nfs \
-o rsize=8192,wsize=8192,noexec,sync 192.168.3.208:/share /mnt/share/
# check mount infomation
[root@server153 /]# mount
192.168.3.208:/share on /mnt/share type nfs
(rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.3.208)
# list files to check
[root@server153 ~]# ls /mnt/share/
aaa
```

題目(b):AUTOFS 自動掛載目錄

- 題目(b),接續上題題目(a):
- Note: 因為你將不會有 root 的存取權限, 你將不能夠把目錄掛載輸出到 /share 目錄,所以要請你使用你的 guest account 對於這系統服務測試.
- 無論如何, the auto-mounter on the system has been configured such that it will automount your /share directory under /home/guest1/nfs/station1
- 於是完成執行「ls /home/guestx/nfs/station1」指示這個 automounter 是能夠自動掛載你分享出來的 NFS share.

- 建立目錄及確定沒有東西

```
[root@server153 ~]# mkdir -p /home/guest1/nfs/
[root@server153 ~]# ls /home/guest1/nfs/station1
ls: /home/guest1/nfs/station1: 沒有此一檔案或目錄
```

- 設定 autofs.master 監控目錄及 auto.home(自訂檔名)監控的字串

```
[root@server153 ~]# vim /etc/auto.master
/home/guest1/nfs        /etc/auto.home
[root@server153 ~]# vim /etc/auto.home
station1        -ro,soft,intr   192.168.3.208:/share
[root@server153 ~]# /etc/init.d/autofs restart
正在停止 automount:                                        [  確定  ]
正在啟動 automount:                                        [  確定  ]
```

- 啟動 automount 指令後系統會產生 selinux 的錯誤警示訊息,請使用 setroubleshootd 觀看類似下面的訊息:

```
# SummarySELinux is preventing the /usr/sbin/automount from using potentially
 mislabeled files (/home/guest1/nfs).Detailed DescriptionSELinux has denied
/usr/sbin/automount access to potentially mislabeled file(s) (/home/guest1/nfs).
# This means that SELinux will not allow /usr/sbin/automount to use these files.
 It is common for users to edit files in their home directory or tmp directories
 and then move (mv) them to system directories.
# The problem is that the files end up with the wrong file context which
confined applications are not allowed to access.Allowing AccessIf you want
 /usr/sbin/automount to access this files, you need to relabel them using
```

```
 restorecon -v /home/guest1/nfs.
# You might want to relabel the entire directory using restorecon -R -v
/home/guest1.Additional InformationSource
## Context:  system_u:system_r:automount_tTarget
## Context:  root:object_r:user_home_tTarget
## Objects:  /home/guest1/nfs [ dir ]Affected
## RPM Packages:  autofs-5.0.1-0.rc2.55 [application]
## Policy RPM:  selinux-policy-2.4.6-104.el5Selinux
## Enabled:  TruePolicy
## Type:  targetedMLS
## Enabled:  TrueEnforcing
## Mode:  EnforcingPlugin
## Name:  plugins.home_tmp_bad_labelsHost
## Name:  server153.example.com
## Platform: Linux server153.example.com 2.6.18-128.el5xen #1 SMP
## Wed Dec 17 12:22:24 EST 2008 i686 i686
## Alert Count:  1Line Numbers:
```

- 這大意是說 automount 的執行權限和目錄的權限不一樣，所以你必須修正這個問題。這串訊息有提供修正的方法，但是實際測試後沒有發揮效果。所以我使用另一個方式完成修正讓 automount 可以工作。
- 測試及修正 selinux

```
[root@server153 ~]# ls /home/guest1 -lZ
drwxr-xr-x  root root root:object_r:user_home_t        nfs
# 使用 chcon 引用 /mnt 套用到 /home/guest1/nfs
[root@server153 ~]# chcon --reference=/mnt /home/guest1/nfs
[root@server153 ~]# ls /home/guest1 -lZ
drwxr-xr-x  root root system_u:object_r:autofs_t       nfs
# try again
[root@server153 ~]# /etc/init.d/autofs restart
正在停止 automount:                                        [  確定  ]
正在啟動 automount:                                        [  確定  ]
[root@server153 ~]# ls /home/guest1/nfs/station1
aaa
[root@server153 ~]# mount
192.168.3.208:/share on /home/guest1/nfs/station1 type nfs
 (ro,soft,intr,addr=192.168.3.208)
```

- 完成掛載，但記得此服務需要於啟動後自動啟用，所以 nfs server 及 automount 服務都需要設定開機後自動啟用。
- 最後再把剛剛的 nfs options 補上

```
[root@server153 ~]# vim /etc/auto.home
station1        -rsize=8192,wsize=8192,noexec,sync,intr,soft 192.168.3.208:/share
[root@server153 ~]# /etc/init.d/autofs restart
正在停止 automount:                                        [  確定  ]
正在啟動 automount:                                        [  確定  ]
[root@server153 ~]# ls /home/guest1/nfs/station1
aaa
[root@server153 ~]# mount
192.168.3.208:/share on /home/guest1/nfs/station1 type nfs
(rw,noexec,sync,rsize=8192,wsize=8192,intr,soft,addr=192.168.3.208)
```

- ***最後請記得設定***
  - 程式預設要啟動 autofs ,nfs , portmap 都要設定為開機後啟動.
  - example.com 的存取控制需要測試
  - ls /home/guest1/nfs/station1 重開機後還可以使用正常
  - mount 的顯示權限屬性要對

mount的檔案權限要對

NFS:LAB2依下列設定設定NFS

- Export directories via NFS
- a) Configure the NFS server on server1(自己的機器ex:192.168.3.1) to export the directories /home and /nishome. Use the following parameters:

1. All machines in the networks 192.168.3.0/24 have access to /home.
2. All machines in the networks 192.168.3.0/24 and 192.168.2.0/24 have access to /nishome.
3. Both exported directories allow read/write access (subject to correct permissions).
4. No access with root permissions is allowed.
5. All I/O to the filesystems is done synchronously.
6. Make sure the NFS server will be started automatically after a reboot.

- b) Configure the client machine server2(使用192.168.3.249測試) to mount /home and /nishome from server1 automatically during startup. The mount points are /mnt/home and /mnt/nishome respectively. Use the following parameters:

1. The size of the buffer for read and write access is 8 KB.
2. The execution of binaries or shell scripts residing on the NFS filesystems is not allowed.
3. All I/O to the filesystem should be done synchronously.

- 設定(a)NFS server部份 on server 1

```
[root@localhost /]# vi /etc/exports
/home 192.168.3.0/24(rw,root_squash,sync)
/nishome 192.168.3.0/24(rw,root_squash,sync) 192.168.2.0/24(rw,root_squash,sync)
# 啟動 portmap (RPC程式)
[root@localhost /]# /etc/init.d/portmap restart
Stopping portmap:                                          [  OK  ]
Starting portmap:                                          [  OK  ]
# 啟動 NFS server
[root@localhost /]# /etc/init.d/nfs restart
Shutting down NFS mountd:                                  [FAILED]
Shutting down NFS daemon:                                  [FAILED]
Shutting down NFS quotas:                                  [FAILED]
Shutting down NFS services:                                [  OK  ]
Starting NFS services:                                     [  OK  ]
Starting NFS quotas:                                       [  OK  ]
Starting NFS daemon:                                       [  OK  ]
Starting NFS mountd:                                       [  OK  ]
# 檢查設定檔
[root@localhost /]# exportfs  -v
/nishome        192.168.3.0/24(rw,wdelay,root_squash,no_subtree_check,
anonuid=65534,anongid=65534)
/nishome        192.168.2.0/24(rw,wdelay,root_squash,no_subtree_check,
anonuid=65534,anongid=65534)
/home           192.168.3.0/24(rw,wdelay,root_squash,no_subtree_check,
anonuid=65534,anongid=65534)
# 檢查掛載資訊
[root@localhost /]# showmount -e localhost
Export list for localhost:
/home    192.168.3.0/24
/nishome 192.168.2.0/24,192.168.3.0/24
# 預設開機啟動
[root@localhost /]# chkconfig portmap on
[root@localhost /]# chkconfig nfs on
# 檢查 port
[root@localhost ~]# rpcinfo -p
```

```
    program vers proto   port
     100000    2   tcp    111  portmapper
     100000    2   udp    111  portmapper
     100024    1   udp    623  status
     100024    1   tcp    626  status
     100011    1   udp    757  rquotad
     100011    2   udp    757  rquotad
     100011    1   tcp    760  rquotad
     100011    2   tcp    760  rquotad
     100003    2   udp   2049  nfs
     100003    3   udp   2049  nfs
     100003    4   udp   2049  nfs
     100003    2   tcp   2049  nfs
     100003    3   tcp   2049  nfs
     100003    4   tcp   2049  nfs
     100021    1   udp   1028  nlockmgr
     100021    3   udp   1028  nlockmgr
     100021    4   udp   1028  nlockmgr
     100021    1   tcp   2562  nlockmgr
     100021    3   tcp   2562  nlockmgr
     100021    4   tcp   2562  nlockmgr
     100005    1   udp    772  mountd
     100005    1   tcp    775  mountd
     100005    2   udp    772  mountd
     100005    2   tcp    775  mountd
     100005    3   udp    772  mountd
     100005    3   tcp    775  mountd
```

- 設定(b) on server 2 , NFS client部份

```
# 建立目的掛載點
[root@localhost ~]# mkdir /mnt/home
[root@localhost ~]# mkdir /mnt/nishome
# 掛載
[root@localhost ~]# mount -t nfs \
-o rsize=8192,wsize=8192,noexec,sync 192.168.3.119:/home /mnt/home
[root@localhost ~]# mount -t nfs \
-o rsize=8192,wsize=8192,noexec,sync 192.168.3.119:/nishome /mnt/nishome
# 看掛載是否成功，選項設定是否正確
[root@localhost ~]# mount
/dev/sda2 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sda1 on /boot type ext3 (rw)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda11 on /home type ext3 (rw)
/dev/md0 on /raiddata type ext3 (rw)
/dev/sda3 on /usr type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
nfsd on /proc/fs/nfsd type nfsd (rw)
192.168.3.119:/home on /mnt/home type nfs
(rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.3.119)
192.168.3.119:/nishome on /mnt/nishome type nfs
(rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.3.119)

# 參考 mtab 內容
[root@localhost ~]# more /etc/mtab
/dev/sda2 / ext3 rw 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
devpts /dev/pts devpts rw,gid=5,mode=620 0 0
```

```
/dev/sda1 /boot ext3 rw 0 0
tmpfs /dev/shm tmpfs rw 0 0
/dev/sda11 /home ext3 rw 0 0
/dev/md0 /raiddata ext3 rw 0 0
/dev/sda3 /usr ext3 rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
sunrpc /var/lib/nfs/rpc_pipefs rpc_pipefs rw 0 0
nfsd /proc/fs/nfsd nfsd rw 0 0
192.168.3.119:/home /mnt/home nfs
rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.0.119 0 0
192.168.3.119:/nishome /mnt/nishome nfs
rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.0.119 0 0
# 設定開機啟動，寫入fstab
[root@localhost ~]# vi /etc/fstab
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
LABEL=/home             /home                   ext3    defaults        1 2
proc                    /proc                   proc    defaults        0 0
/dev/md0                /raiddata               ext3    defaults        1 2
sysfs                   /sys                    sysfs   defaults        0 0
LABEL=/usr              /usr                    ext3    defaults        1 2
LABEL=SWAP-sda5         swap                    swap    defaults        0 0
192.168.3.119:/home     /mnt/home     nfs
rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.3.119  0 0
192.168.3.119:/nishome  /mnt/nishome  nfs
rw,noexec,sync,rsize=8192,wsize=8192,addr=192.168.3.119  0 0
# 把剛剛掛載的卸載
[root@localhost ~]# umount /mnt/home
[root@localhost ~]# umount /mnt/nishome
# from /etc/fstab 自動掛載進入，如無問題開機後即可自行掛載
[root@localhost ~]# mount /mnt/home
[root@localhost ~]# mount /mnt/nishome
```

目標檢核

實作

回到索引頁 or 回到首頁