raid (Linux)

* **fdisk** & **mkfs**
* mdadm (raid1)

*mdadm --create /dev/md0 --raid-devices=2 --level=1 /dev/sd{b,c}*

*watch cat /proc/mdstat*

*Personalities : [raid1]*

*md0 : active raid1 sdc[1] sdb[0]*

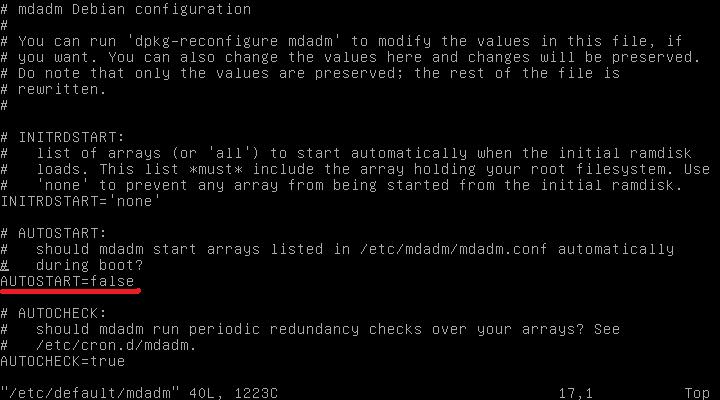
*20970424 blocks super 1.2 [2/2] [UU]*

*mdadm --detail -scan >> /etc/mdadm/mdadm.conf*

* /etc/fstab

*<file system> <mount point> <type> <options> <dump> <pass>*

***/dev/md0 /web ext3 defaults 0 2***

******

***\*特別重要 參考資料都沒提及* (慘痛的教訓)**

資料寫進 *mdadm.conf*

一定要記得確認 */etc/default/mdadm*

***設定* AUTOSTART=true**

**才會開機自動做Raid**

***完成LVM***

fdisk 切割partition

*len@LSF:~$ sudo fdisk /dev/md0*

***t > 8e (id => Linux LVM)***

*Device Boot Start End Blocks Id System*

*/dev/md0p1 1 5242606 20970422 8e Linux LVM*

*apt-get install* ***lvm2***

* ***pv > vg > lv***

***pvcreate*** */dev/md0　　　　　　　#pvcreate /dev/sda{1,2,3,4}*

***vgcreate*** *VG01 /dev/md0　　　　#Volmum name: VG01*

***lvcreate*** *-L 15G -n LVHOME VG01*

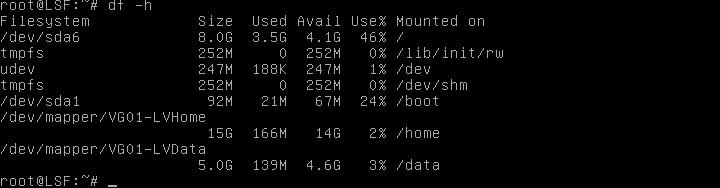
*＊ lvcreate -l 1279 -n LVData VG01*

*Insufficient free extents (0) in volume group VG01: 255975 required*

[tips]

pvdisplay , Free PE用 -l 可以把剩下的空間用PE

塞滿，就不是 -L size 的格式



Dovecot

寫進dovecot.conf的mail\_location

mail\_location = mbox:~/mail:INBOX=/var/mail/%u

使用者家目錄一定要建立，否則mbox沒辦法建立

Samba測試

smb.conf一定要針對share項目寫入 writable = yes & 設定目錄權限

* + 先寫先贏

read only = no

writable = yes

* net use \\lsf\IT twsc2012 /user:it02

ISO *9660* (Linux)

* genisoimage (有些被連結到mkisoimg)
  + genisoimage -o img.iso cd\_dir/
  + mount -t loop img.iso /mnt/cdiso

date (Linux)

* 格式 (--help & man 裡面講的很詳細)
  + yyyy-mm-dd-hhmm

date +%Y-%m-%d-%H%M

Cron

* crontab -e
  + minute hour day month week　　#週 & 月日不可並存
  + \*/15 \* \* \* \* sh /usr/local/etc/webakup.sh　#每15分鐘執行一次

*webakup.sh*

#!/bin/sh

genisoimage -o /backup/`date +%Y-%m-%d-%H%M.iso` /web

Apache

* 自訂log位置

*/etc/apache2/sites-enabled/000-default*

*CustomLog ${APACHE\_LOG\_DIR}/myaccess.log mylogtype*

自訂log格式

*apache2.conf*

*LogFormat "%h %l %u %t \"%r\"" mylogtype*

*(100.0.77.3 - - [25/Jul/2013:19:44:25 +0800] "GET /favicon.ico HTTP/1.1")*

* mod\_rewrite *(http 轉 https)*

RewriteEngine on

RewriteCond %{HTTPS} off

RewriteRule /?(.\*) https://%{SERVER\_NAME}/$1 [L,R]

登入訊息

* /etc/motd、/etc/issue
* ssh

*sshd\_config*

Banner /etc/issue.net

*(Cron)* #每分鐘更新訊息時間

\*/1 \* \* \* \* sh /usr/local/etc/bannerup.sh

*bannerup.sh*

#!/bin/sh

echo "Time：`date +%H:%M` – This Workstation is Monitored. Any Unauthorized Usage Will Be prosecuted." > /etc/issue.net

SSH

**＊＊＊空密碼登入＊＊＊**

除了修改　*shadow*　或　*passwd -d*把密碼清空外

還必須修改pam的驗證方式

* **pam.d**
* **/etc/pam.d/sshd**

# Standard Un\*x authentication.

@include common-auth #可以知道sshd預設引用common-auth的設定

* **/etc/pam.d/common-auth**

預設為　nullok\_secure　修改或註解掉即可

auth [success=2 default=ignore] pam\_unix.so nullok\_secure

auth [success=2 default=ignore] pam\_unix.so nullok

這樣直接su就可以空密碼登入　再來修改 sshd\_config 的設定允許空密碼ssh

# To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords yes

openssl genrsa -out /etc/ssl/private/ssl.key 1024

openssl req -new -key /etc/ssl/private/ssl.key -out /etc/ssl/private/ssl.csr

openssl x509 -req -days 365 -in private/ssl.csr -signkey private/ssl.key -out priva

te/ssl.crt

len@LSF:~$ sudo locate CA.pl

*/usr/lib/ssl/misc/CA.pl*

*usage: CA -newcert|-newreq|-newreq-nodes|-newca|-sign|-verify*

*usage: CA -signcert certfile keyfile|-newcert|-newreq|-newca|-sign|-verify*

*apt-get install krb5-clients krb5-config winbind*

/etc/krb5.conf

[libdefaults]

default\_realm = NETWORK.TW

[realms]

NETWORK.TW = {

kdc = network.tw

admin\_server = network.tw

}

[domain\_realm]

.network.tw = network.tw

network.tw = network.tw

net ads join network.tw -U administrator #加入網域

*sudo sudo wbinfo -t*

could not obtain winbind interface details!

could not obtain winbind domain name!

checking the trust secret for domain (null) via RPC calls failed

Could not check secret

[重啟Winbind]

*sudo wbinfo -t*

checking the trust secret for domain NETWORK via RPC calls succeeded

**＊＊＊新增系統資料庫對應設定檔到Winbind的驗證方式＊＊＊**

# /etc/nsswitch.conf [標準C函式庫ex.getpwent() & NSS的對應檔案]

passwd: compat winbind #passwd: files winbind

group: compat winbind #group: files winbind

realm = host.com

security = ads

password server = 172.16.1.2

***template homedir = /home/%u***

|  |  |
| --- | --- |
| wbinfo -u | getent passwd　正確讀取到AD資料 |
|  |  |

*/etc/pam.d/samba*

@include common-auth

@include common-account

@include common-session-noninteractive

auth sufficient pam\_winbind.so

account sufficient pam\_winbind.so

session required pam\_mkhomedir.so umask=0022 skel=/etc/skel

註：實際試驗結果, 上述寫法getent能正確讀取到passwd database內AD的帳戶訊息在pam\_unix.so就能傳回success, sufficient旗標的影響不太大

*分別追回三個共用驗證include files*

Debian預設就在 common-auth & common-account 分別寫入有關Winbind的驗證規則

* *[common-account]*

auth [success=1 default=ignore] pam\_winbind.so krb5\_auth krb5\_ccache\_type=FILE cached\_login try\_first\_pass

* *[common-passwd]*

password [success=1 default=ignore] pam\_winbind.so use\_authtok try\_first\_pass

workgroup = NETWORK

realm = network.tw

security = domain

password server = ws.network.tw

# Some defaults for winbind (make sure you're not using the ranges

# for something else.)

idmap uid = 10000-20000

idmap gid = 10000-20000

template shell = /bin/bash

winbind enum groups = yes

winbind enum users = yes

[Pam.d allow specific accounts login]

/etc/pam.d/sshd

auth required pam\_listfile.so item=user sense=allow file=/etc/ssh/allow\_list onerr=fail

/etc/ssh/allow\_list

root

[telnet]

apt-get install telnetd

telnetd統一交由inted (Internet Daemon) 管理

修改其設定檔 */etc/inetd.conf*

telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetd

為了修改telnet的port　依照manual敘述

The service name entry is the name of a valid service in the file /etc/services or a port number. For “internal” services (discussed below), the service name must be the official name of the service (that is, the first entry in /etc/services).

服務名稱與*/etc/service*內一致

*/etc/service*

telnet 10023/tcp

*直接修改port number再重新啟動系統使inted初始化即可*

*netstat -ntlp*

*tcp 0 0 0.0.0.0:10023 0.0.0.0:\* LISTEN 2530/inetd*

visudo [/etc/sudoers]

(sudo 免密碼)

*username All=(All) NOPASSWD: All*

\*MRTG Tips

@man snmpd.examples

/etc/snmp/snmpd.conf

# Listen for connections from the local system only

agentAddress udp:127.0.0.1:161

#對所有介面啟用

view all included .1

rocommunity public localhost

/etc/init.d/snmpd restart

snmpwalk -v 1 -c public localhost

(-v version, -c community[ID])

cfgmaker --output=/etc/mrtg.cfg public@localohst

(cfgmaker public@localohst > /etc/mrtg.cfg)

env LANG=C mrtg /etc/mrtg.cfg #until no error in 3 times

indexmaker --output=/var/www/mrtg/index.htm /etc/mrtg.cfg

crontab

\*/5 \* \* \* \* env LANG=C /usr/sbin/mrtg /etc/mrtg.cfg

(BUT mrtg have cron job by DEFAULT @/etc/cron.d/mrtg)

重建Active Directory DNS record

dcpromo /forceremoval #刪除AD

C:\Windows\System32\config\netlogon.dns > backup

C:\Windows\SYSVOL > SYSVOL.bak

remove DNS role && reboot

dcpromo with DNS

[mod\_rewrite]

RewriteCond %{HTTP\_HOST} !^www.web.com [NC] #請求的主機中URL不是www.web.com ,[NC]的意思是忽略大小寫

RewriteCond %{HTTP\_HOST} !^$ #求的主機中URL不為空

RewriteRule ^/(.\*) http://www.web.com/ [L]

#含義是如果Client請求的主機中的URL符合上述條件，則直接進行跳轉到http://www.web.com/,[L]意味著立即停止重寫操作，並不再應用其他重寫規則。這裡的.\*是指匹配所有URL中不包含換行字符，()括號的功能是把所​​有的字符做一個標記，以便於後面的應用.就是引用前面裡的(.\*)字符。

1) R[=code](force redirect) 強制外部重定向[r=301]

2) F(force URL to be forbidden)禁用URL,返回403HTTP狀態碼。

3) G(force URL to be gone) 強制URL為GONE，返回410HTTP狀態碼。

4) P(force proxy) 強制使用代理轉發。

5) L(last rule) 表明當前規則是最後一條規則，停止分析以後規則的重寫。

6) N(next round) 重新從第一條規則開始運行重寫過程。

7) C(chained with next rule) 與下一條規則關聯

8) T=MIME-type(force MIME type) 強制MIME類型

9) NS (used only if no internal sub-request) 只用於不是內部子請求

10) NC(no case) 不區分大小寫

11) QSA(query string append) 追加請求字符串

12) NE(no URI escaping of output) 不在輸出轉義特殊字符

例如：RewriteRule /foo/(.\*) /bar?arg=P1\%3d$1 [R,NE] 將能正確的將/foo/zoo轉換成/bar?arg=P1=zoo

13) PT(pass through to next handler) 傳遞給下一個處理

例如：

RewriteRule ^/abc(.\*) /def$1 [PT] # 將會交給/def規則處理

Alias​​ /def /ghi

14) S=num(skip next rule(s)) 跳過​​num條規則

15) E=VAR:VAL(set environment variable) 設置環境變量

*RewriteEngine on*

*RewriteCond %{HTTPS} !^on$ [NC]*

*RewriteRule . https://%{HTTP\_HOST}%{REQUEST\_URI} [L]*

**mount --bind /var/ftp/public2 /home/B/public2**

[ntp]

net time \\ip /set /y

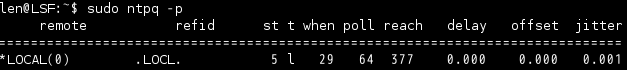
w32tm

NTP

設定本機為最上層伺服器

*ntp.conf*

*server 127.127.1.0　　　　#127.127.0.0/16*

**

*synctime.sh*

#!/bin/sh

ntpdate 100.0.77.1

hwclock -w

SOA record

@ IN SOA network.tw admin.network.tw (  
 1 ; serial number *#序號*  
 3600 ; refresh [1h] *#slave更新間隔(檢查Serial number)*  
 600 ; retry [10m] *#slave連結失敗每隔幾秒retry*  
 86400 ; expire [1d] *#超過時間slave便刪除這份record*  
 3600 ) ; min TTL [1h]

#代表這個 zone file 中所有 record 的內定的 TTL 值，也就是其它的 DNS server cache 這筆 record 時，最長不應該超過這個時間。

**SUID, SGID, Sticky bit 的設定方法：**

前面介紹過 SUID 與 SGID 的功能，那麼如何開啟檔案使成為具有 SUID 與 SGID 的權限呢？！這就需要剛剛的數字更改權限的方法了！現在你應該已經知道數字型態個更改權限方式為『三個數字』的組合，那麼如果在這三個數字之前再加上一個數字的話，那最前的面數字就代表這幾個屬性了！ ( **註：通常我們使用 chmod xyz filename 的方式來設定 filename 的屬性時，則是假設沒有 SUID, SGID 及 Sticky bit 啦！** )

* + 4 為 SUID
  + 2 為 SGID
  + 1 為 Sticky bit

假設要將一個檔案屬性改為『-rwsr-xr-x』時，由於 s 在使用者權限中，所以是 SUID ，因此，在原先的 755 之前還要加上 4 ，也就是：『 chmod 4755 filename 』來設定！此外，還有大 S 與大 T 的產生喔！參考底下的範例啦！

|  |
| --- |
| [root@test tmp]# touch test  [root@test tmp]# ll  total 0  -rw-r--r-- 1 root root 0 Feb 6 23:08 test  [root@test tmp]# chmod 4755 test  [root@vbird tmp]# ll  total 0  -rwsr-xr-x 1 root root 0 Feb 6 23:08 test\*  [root@test tmp]# chmod 6755 test  [root@test tmp]# ll  total 0  -rwsr-sr-x 1 root root 0 Feb 6 23:08 test\*  [root@test tmp]# chmod 1755 test  [root@test tmp]# ll  total 0  -rwxr-xr-t 1 root root 0 Feb 6 23:08 test\*  上面的三個例子應該都很好說明啊！就是直接將 x 以 s 或者是 t 來取代就是了！也就是分別為 SUID, SGID 及 sticky bit 的設定方法啦！  [root@test tmp]# chmod 7666 test  [root@test tmp]# ll  total 0  -rwSrwSrwT 1 root root 0 Feb 6 23:08 test  這個例子就要特別小心啦！怎麼會出現大寫的 S 與 T 呢？不都是小寫的嗎？因為 s 與 t 都是取代 x 這個參數的，但是你有沒有發現阿，我們是下達 7666 喔！也就是說， user, group 以及 others 都沒有 x 這個可執行的標誌 ( 因為 666 嘛！ )，所以，這個 S, T 代表的就是『空的』啦！怎麼說？ SUID 是表示『該檔案在執行的時候，具有檔案擁有者的權限』，但是檔案擁有者都無法執行了，哪裡來的權限給其他人使用？當然就是空的啦！ ^\_^ |

-A INPUT -i eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT

-A INPUT -d 163.60.30.1/32 -i eth2 -p tcp -m multiport --ports 80,443,25,143 -j ACCEPT

-A INPUT -s 120.10.20.0/24 -j DROP

iptables -A INPUT -s 120.10.20.0/24 -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A INPUT -s 120.10.20.0/24 -d 163.60.30.1/32 -p tcp -m multiport --ports 80,443,25,143 -j ACCEPT

iptables -A INPUT -s 120.10.20.0/24 -j DROP