** Section 1 **

NFS(Network File system)

- port:
  - NFSv3: 111 使用 portmapper
  - NFSv4: 2049 (TCP only)
- 設定檔: /etc/exports
  - /etc/exports 設定檔語法
    分享目錄 對象(選項)

可以使用 rpcinfo 指令觀察 RPC(遠端程序呼叫)相關資訊
Daemon

- rpcbind 預設就會啟動
- nfsserver 預設沒有啟動(可確認 nfs-kernel-server 套件是否有安裝)

NFSv4:

- 固定使用 TCP port 2049
- 可以支援加密 / 可以使用 Kerberos (Per-User basis not only based on IP or DNS)
- 是否啟用 NFSv4 支援 /etc/sysconfig/nfs 內的 NFS4_SUPPORT="yes" 來決定
- 使用 fsid=0 定義一個根目錄, 只有該目錄下的子目錄才能被掛載
- option
  - fsid=0 指定掛載虛擬根目錄, 只能有一個
  - crossmnt 應該被加到 fsid=0 的選項後, 讓遠端的 filesystem 可以掛載
  - no_subtree_check 不檢查父目錄權限, 可以增加 NFS 效率 (預設值)
  - bind=路徑 將資料夾指定到虛擬根目錄下
  - nohide 不用一一明確指定掛載就會直接掛載到虛擬的根目錄
  - hide 掛載 NFSv4 虛擬根目錄的時候, 其他子目錄不會掛載(預設值)

Notes:

- 用戶端可以使用 showmount 來觀察 Server 分享的 NFS 資源
- 用戶端可以使用 mount -o nfsvers=n 來指定 NFS 的版本 3 或是 2, 但是 NFSv4 要使用 -t nfs4 的方式來指定, /etc/fstab 內也是 nfs (for v2 and v3), nfs4
- 可以 man nfs 取得更多的說明

因為 NFS 預設有設定 root_squash,

- 如果使用 root 身份寫入擁有人會被轉換成 nobody, 如果要以 root 身份寫入, 可以於/etc/exports 內加入 no_root_squash 的選項

使用 NFS 必須注意檔案擁有人的問題,

- 以 NFS 方式分享, 其檔案的擁有人取決於該檔案的 UID, 故應避免 Server 端與 client 端 UID 不一致的現象

NFS 分享也可以透過 autofs 的方式來達成自動掛載 nfs.

automounter

目的: 有掛載需求的時候,
自動 mount, 沒有掛載需求的時候(Timeout)自動 umount

Daemon: autofs (於用戶端使用, 自動掛載 NFS Server 上的分享資料夾)
設定檔: /etc/auto.master

設定檔語法
監控目錄 該目錄設定檔 選項

時區相關設定 /etc/sysconfig/clock

ntpdate 透過網際網路來執行對時的指令

可以使用以下來對時
#sntp -P no -r time.stdtime.gov.tw

FTP: Pure-ftpd

- Port: 21(ftp-cmd)/20(ftp-data)
- 設定檔: /etc/pure-ftpd/pure-ftpd.conf
- Type: 主動式/被動式
- 預設使用 匿名使用者(ftp)來連線,並針對所有使用者進行 chroot
- 藉由修改 AnonymousCantUpload no 讓匿名使用者可以上傳資料
- 預設使用 AutoRename yes 如果上傳檔案重複, 會自動更改檔案名稱

主動連線模式: 由 FTP 提出 SYN 的要求, 來進行資料的傳輸
被動連線模式: 由 FTP 告知連線的 Port, 讓 client 來進行連線要求進行資料的傳輸

Section 2

Open Printing 網站
http://www.linuxprinting.org

新增印表機
#yast printer
#yast2 printer

CUPS 網頁管理介面
http://127.0.0.1:631

停用印表機
cupsdisable 印表機名稱

啟用印表機
cupsenable 印表機名稱

拒絕新的工作要求
reject 印表機名稱

接受新的工作要求
accept 印表機名稱

Printq
/etc/cups/printers.conf

Section 3

LDAP (Lightweight Directory Access Protocol) 輕量級目錄存取服務

- ldap port 389 / ldaps port 636
- Server 設定檔 YaST 預設不使用 /etc/openldap/slapd.conf (openldap 2.3 以後都採用此方式)
  - 可以使用 ldapsearch -Y external -H ldapi:/// -b cn=config 觀察設定檔
  - YaST uses OpenLDAP's dynamic configuration database (back-config) to store the LDAP server's configuration. For details about the dynamic configuration backend please see the slapd-config(5) manpage or the OpenLDAP Software 2.4 Administrator's Guide
  - 設定檔分散在 /etc/openldap/slapd.d 目錄下 可以參考 http://www.openldap.org/doc/admin24/slapdconf2.html
- Client
  - 可以觀察/etc/nsswitch.conf 內的相關設定是否有 ldap
  - 觀察相關伺服器設定 /etc/ldap.conf /etc/sysconf/ldap
- Binding (結合) LDAP 的認証行為說法
- 資料庫 /var/lib/ldap
  - bdb: Berkeley Data Base
  - hdb: Hierarchical Berkeley Data Base, 使用 hierachical database layout
- 簡化 X.500 的目錄存取協定
- 一般使用 openldap 套件可同時支援 version 2 and version3 http://www.openldap.org/
  - 文件 http://www.openldap.org/doc/admin24/
- 目錄與資料庫的差異在於是否會經常性的大量讀寫. (例如通訊錄)
- 可以集中或是分散存放(Support for replications – prevent the creation of a single point of failure)
- 可以表現出階層架構特性 (依照組織架構, 或是地區架構)
- 驗證集中管理,降低維護成本(與 local file 比較)(亦可使用 NIS Service, 但是 Unix/Linux Only)(heterogeneous 異質系統整合).

X.500 Directory standard

- Directory Information Databse (DIB)
  - 由物件(Object)(也被稱為 entry)所組成, 可以反應實體架構與資源
  - 每一物件都有一個唯一的識別名稱(distinguished name),透過屬性(attribute)來紀錄物件的資料
- Directory Information Tree (DIT)
  - 以樹狀的架構呈現 DIB 內的資訊.
  - 透過綱要(schema)來檢查語法是否符合定義.
- Directory User Agent (DUA)
  - X.500 使用 client / Server 架構來存取.
  - Client side.
- Directory System Agent (DSA)
  - DSA 會接受 / 回覆 / 轉介(如果該 DSA 沒有資訊) DUA 的要求.
  - Server side.
- Directory Access Protocol (DAP)
  - DUA 用來與 DSA 溝通的協定.
- Directory System Protocol (DSP)
  - 如果 DSA 不能提供 DUA 的資訊, DSA 會使用 DSP 將要求轉給另外一個 DSA.
  - 用於 DSA 的溝通.

- Directory Information Shadowing Protocol (DISP)
  - X.500 稱為 Shadowing, DAP 稱為 replication.
  - DSAs 用 DISP 來覆寫(replicaion)彼此的 DIB,用於分散式架構(改善效能, 防止 single point failure)

LDAP Object (LDAP 物件)

  - 物件(Object)(也被稱為 entry)所組成, 可以反應實體架構與資源
  - 每一物件都有一個唯一的識別名稱(distinguished name),透過屬性(attribute)來紀錄物件的資料

LDAP Class (LDAP 類別)

- 由屬性所組成的集合(Collection),用來定義/建立屬性.

LDAP Schema

  - 綱要(schema)來檢查語法是否符合定義, 是否可以建立該物件.是否可以包含某個物件.

LDAP 目錄結構組成

DN (Distinguished Name)

- 識別名稱，LDAP 中記錄的唯一位置.

RDN (Relative Distinguished Name)

- 相對識別名稱.

CN (Common Name of)

- 顯示名稱,一筆 LDAP 記錄名稱

OU (Organizational Unit)

- 組織,一筆 LDAP 記錄所屬組織

使用 逗號(comma)來分隔與紀錄物件, 例如 cn=BJohnson,ou=SLC,o=DA

** Section 4 **

Samba
Samba is an Open Source/Free Software suite that has, since 1992, provided file and print services to all manner of SMB/CIFS clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License.

smbd: 管理 samba 分享
nmbd: 管理 NetBIOS 相關

Samba
- Port: 137/138/139/445
- 設定檔: /etc/samba/smb.conf
  - global 區段: 套用到全部
  - share 區段: 該分享的資料夾/印表機

/etc/samba/smb.conf
- workgroup 工作群組/網域名稱
- netbios name 設定網芳名稱
- security 驗證方式(share --> 不驗證, user --> 提供驗證)
- read only=yes 唯讀
- writable=yes 可寫入
- [ ] 分享名稱
- path 實際上在 linux 路徑
- browseable 可瀏覽
- create mask 建立檔案預設產生的權限
- directory mask 建立資料夾預設產生的權限
- printable 如果設定為 yes, 則為印表機分享
- valid users 設定特定使用者(username)/群組(@groupname) 才能使用這個分享
- write list 設定特定使用者(username)/群組(@groupname) 才有寫入權限
- public 可以匿名存取

mount 掛載 samba 的檔案系統,
- 請使用 -t cifs 的類型, 目前已經沒有 smbfs 類型
- 可以使用 -o iocharset= 的選項指定編碼, 例如 -o iocharset=utf8
- 如果不希望 username and password 放在 /etc/fstab 被看到, 可以將 cifs 掛載寫入於/etc/samba/smbfstab 檔案內 這個檔案只有 root 可以讀寫, 於開機的時候會掛載

可以使用 smbpasswd 建立使用者的 samba 密碼(該使用者必須存在於 Unix 系統上)

可以在 window 上面的命令提示字元
使用 net use * /delete
清除已經連線的網芳資源

** Section 5 **

DNS
Domain Name Service

- 正解: 名稱轉換成 IP
- 反解: IP 轉換成名稱

www.pchome.com.tw

www --> hostname/simple name
- pchome --> 該網站名稱
- .com --> TLDs(Top Level Domains)
- .tw --> ccTLDs(country-code Top Level Domains)

pchome.com.tw --> Domain suffix
www.pchome.com.tw --> FQDN

Resource Record

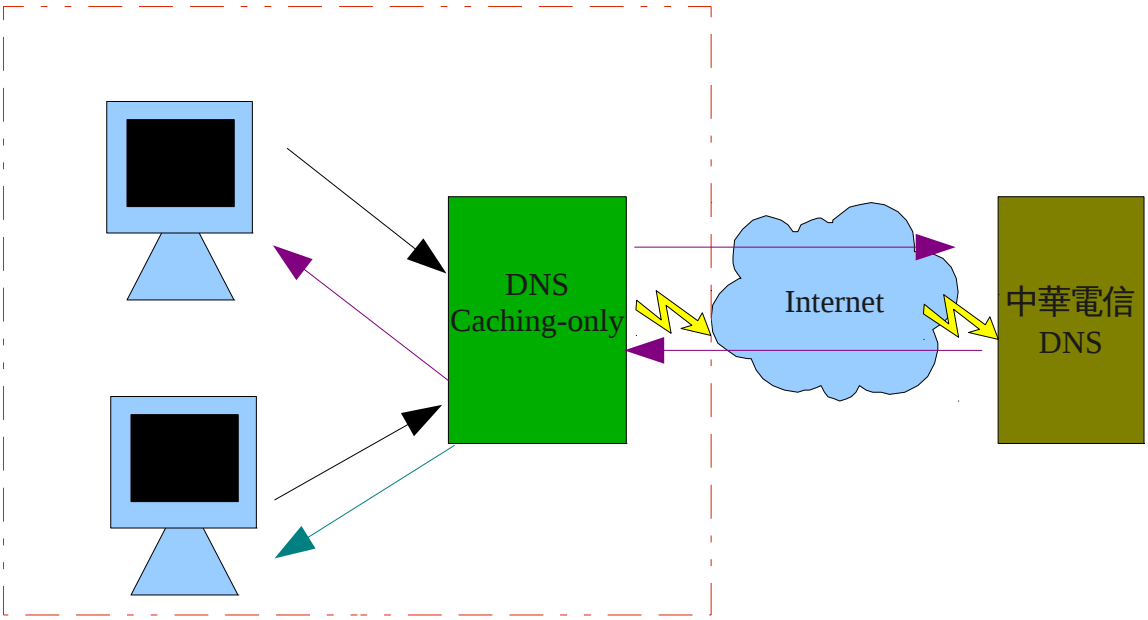
針對主機
- A Record: IP 位址
- PTR Record: FQDN
- CNAME Record: 別名

針對網域
- SOA Record: 網域 DNS 的相關資訊
- NS Record: DNS 伺服器
- MX Record: 郵件伺服器

DNS 特性
- 階層式架構: 會先詢問 ROOT DNS SERVER 再往下詢問
- 分散式架構: 每個 DNS 伺服器只負責自己的 Zone

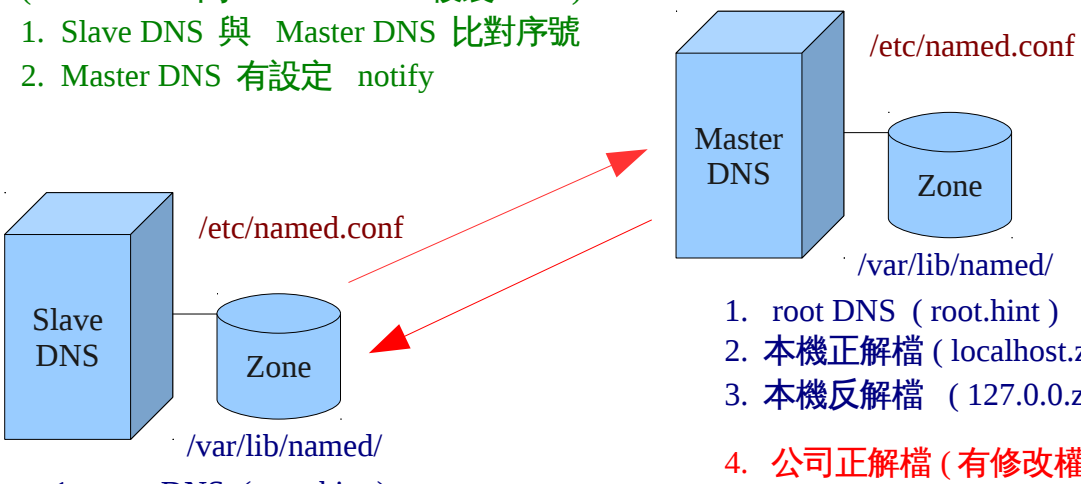
DNS 伺服器
- Port: 53
- 套件: bind*
- 設定檔: /etc/named.conf
- Zone 位置: /var/lib/named 因為有使用 bind-chrootenv 套件, 故 zone 會在/var/lib/named/var/lib/named (可透過 /etc/sysconfig/named 內的 NAMED_RUN_CHROOTED="yes"來觀察)

DNS Type



Caching Name Server

Zone transfer
(Slave DNS 向 Master DNS 複製 zone)
1. Slave DNS 與 Master DNS 比對序號
2. Master DNS 有設定 notify



1. root DNS (root.hint)
2. 本機正解檔 (localhost.zone)
3. 本機反解檔 (127.0.0.zone)

4. 公司正解檔 (無修改權利)
5. 公司反解檔 (無修改權利)

因為有了 bind-chrootenv, 故 zone 會在
/var/lib/named/var/lib/named
因為 /etc/sysconfig/named 有設定

NAMED_RUN_CHROOTED="yes"

1. root DNS (root.hint)
2. 本機正解檔 (localhost.zone)
3. 本機反解檔 (127.0.0.zone)

4. 公司正解檔 (有修改權利)
5. 公司反解檔 (有修改權利)

因為有了 bind-chrootenv, 故 zone 會在
/var/lib/named/var/lib/named
因為 /etc/sysconfig/named 有設定

NAMED_RUN_CHROOTED="yes"

在 zone 檔案內

- 使用 ; 來註解
- 網域名稱（FQDN）部份 一定要使用 . 為結束
  - **www.pchome.com.tw.** 正確寫法
  - www.example.com 忘記附加 . --> 自動幫你附加網域名稱尾碼 --> **www.example.com.example.com.**
- 使用@ 來代替網域名稱, @ --> example.com.

DNS Trouble shotting

- /etc/resolv.conf 是否指向正確的 DNS Server? (serverx 的 IP 而非 168.95.1.1)
- /etc/named.conf 是否有設定正確的 zone 設定?
- 做完設定檔的修改 是否有#rcnamed reload 或是 #rcnamed restart 使其生效?
- Zone 檔案內的序號 是否超過十位數? 2008112101
- 每次的修改 是否有更新序號?

如果要 Master DNS 自動通知 Slave DNS 紀錄有變動

- /etc/named.conf 內設定 notify yes;
- 該 Slave DNS 在 zone 有 NS 及 A Record

如果要限制 zone transfer 的主機
可以在/etc/named.conf
加入 allow-transfer { 主機; };
來限定特定主機才能進行 zone transfer

apache2

/etc/apache2/ 存放 web 伺服器設定檔的目錄

- httpd.conf 主要設定檔
- default-server.conf 預設網站設定檔
- vhost.d 虛擬主機相關設定
- uid.conf apache2 執行的 uid / gid 設定
- listen.conf 指定 apache2 IP 及 port

/etc/apache2/default-server.conf 預設的網站設定檔

- DocumentRoot 網站的根目錄

/etc/apache2/httpd.conf apache2 主要設定檔

- 使用 include 的方式匯入設定
- DirectoryIndex 首頁的設定

Virtual Host

- Name Base Virtual Host: 以 Server Name 為判定的虛擬主機
- IP Base Virtual Host: 以 IP 為判定的虛擬主機
- 設定檔 /etc/apache2/vhosts.d/*.conf

限制使用者需驗證才能進入該目錄

```
<Directory /srv/www/htdocs/security>
#驗證方式
AuthType Basic
#驗證標題
Authname "Security Area"
#驗證相關檔案位置
AuthUserFile  /etc/apache2/htpasswd
#條件--合法使用者
Require valid-user
</Directory>
```

可以利用 htpasswd2 建立該驗證檔案

語法

- #htpasswd2 檔案位置 使用者名稱
- 第一次建立檔案才使用 -c 選項
- 如果要新增第二個使用者, 請不要加上 -c 選項
- -c Create the passwdfile. If passwdfile already exists, it is rewritten and truncated. This option cannot be combined with the -n option.

** Section 6 **

IPv6

- 增強定址能力及自動設定機制
  - 增加 IP 位址 IPv6 為 2^{128} 次方, Ipv4 為 2^{32} 次方
- 簡化標頭格式 / 提升路由效率
  - IPv6 的 header 為 40 bytes 固定長度
    - 8 bytes Header
    - 2 組 16 bytes 的 IP 位置(分別代表來源及目的地位址)
    - 可以用較低的成本來進行更快的處理
- IPv6 的表示法
  - 由 128 bits 組成, 使用 16 進位來表示.
  - 通常以 8 組 16 進位數字, 每組 4 個 16 進位來表示,以冒號來分隔
    - 例如 fe80:0000:0000:0000:0211:11ff:fec2:35f4 就是一個 IPv6 位址
    - 為了簡單表示 連續的 0 可以省略, 以上面的例子, 可以省略為 fe80::211:11ff:fec2:35f4, 但是省略只能有一個, 前導的 0 也可以被省略
- 保密性更佳
- IPv6 類型
  - Unicast 單點廣播
  - Multicast 多點廣播(IPv6 已經不再使用 廣播位址, 而由多點廣播取代之)
  - Anycast 任一廣播
- IPv6
  - Localhost
    - 0000:0000:0000:0000:0000:0000:0000:0001
    - 可以表示為 ::1
  - Unspecified Address
    - 0000:0000:0000:0000:0000:0000:0000:0000
    - 可以表示為 ::
  - Link Local Address
    - 不可以通過路由器, 在同一個介面上使用, 相當於 APIPA 位址(169.254.xx.xx)
    - fe8x (目前正在使用, x 通常為 0)
    - fe9x
    - feax
    - febx
  - Site Local Address
    - 等於 IPv4 私人位址空間 (10.0.0.0/8、172.16.0.0/12 及 192.168.0.0/16)
    - fec0
  - Interface ID
    - 可以使用 EUI-64 演算法 來產生, 產生方式為
    - 將 fffe 插入網卡 MAC 位址的 第 3 與第 4 組位址之間,
      - 例如 00:16:EA:E5:68:90 插入 fffe 就是 00:16:ea:ff:fe:e5:68:90
    - 將網卡廠商 ID 的轉成 2 進位第 7 個 bit 設定為 1
      - 例如 00:16:EA 轉成 2 進位 000000000001011011101010, 將第 7 個 bit 設定為 1, 就是 000000100001011011101010, 換成 16 進位就是 02:16:ea
      - 接上剛剛的位址就是 02:16:ea:ff:fe:e5:68:90

** Section 8 **

shell script:

- 將指令寫入到檔案執行
- 一般會命名為 *.sh 提醒管理者這是個 shell script
- 會於第一行 利用 #! 宣告 Shell 種類
- 需注意執行的方式是
  - 直接執行（在 subshell 執行)
  - 使用 . 或是 source 的方式（在 current shell 執行)
- 給予適當的權限（#chmod a+x *.sh)
- 指令的描述需考慮 路徑變數 $PATH

source 指令/ . :　　目前的 shell 執行

直接執行:　　在 subshell 執行

在 scripts 內可以使用　#! 宣告 shell 種類

有關於引數(arg)

$0　shell 本身

$1　第一個引數

$2　第二個引數

$@　集合 'dog' 'fish' 'cat'

$*　合併 'dog fish cat'

$#　顯示引數的總數

可以使用 test 指令或是 [ ] 來測試有沒有滿足條件

- -f　檢查是否為檔案
- -d　檢查是否為資料夾
- -e　檢查是否有存在(不論是檔案或是資料夾)
- -n　字串長度不得為零
- -a　AND 條件

&&　邏輯 AND

||　邏輯 OR

$?　Return Value(回覆值, 通常 0 代表成功)

```
if　條件式; then
    XXXXX(條件成真要執行的指令)
    else
    XXXXX(條件不成真要執行的指令)
fi
```

Lab:請建立一個 shell script
名稱為 work1.sh
目的:檢查 apache2 是否有在運作

- 如果 apache2 正常運作, 則在螢幕前面顯示 The web service is running
- 如果 apache2 非正常運作, 則在螢幕前面顯示 The web service is down 並請重新啟動 apache2

參考 work1.sh

```
#!/bin/bash
# netstat -tupln | grep :80
rcapache2 status | grep running > /dev/null
a=$?
if [ $a = 0 ]; then
   echo "The Web server is running"
  else
   echo "The Web server is down"
   rcapache2 start
fi
```

參考 work1var.sh

```
#!/bin/bash
if [ -f /var/run/httpd2.pid ]; then
      echo "the web service is running"
      else
      echo "the web service is down"
      rcapache2 restart
fi
```

Lab 建立一個 shell script 監控 apache 程序

名稱:work1-2.sh

- 此 script 執行時需加一個數字參數作為 top 的 iterations 參數,例如 apachemon 5

- 此 script 呼叫 top 並使用 batch 模式監控 apache 程序 wwwrun
- top 的輸出儲存至/home/max 目錄.儲存檔名格式為 apachemon-YYYY-MM-DD-HH:MM,例如 apachemon-2007-05-02-13:02
- 此 script 至少執行一次並產生一個紀錄檔.

參考 work1-2.sh

```
#!/bin/bash
/usr/bin/top -b -n $1 -u wwwrun > /home/max/apachemon-$(date +%F-%R)
```

for 變數名稱 in xxxx
do
XXXXX
done

read 互動式的指令, 會停下來等使用者輸入值, 定義為所定義的變數值

while 當條件為真的時,就執行

while 條件式;
do
XXXXX
done

shift 會把第一個引數刪除, 把最後一個引數往前推

until 直到條件為真才停止

until 條件式;
do
XXXXX
done

Lab:寫一個 script 來作 disk monitor
名稱 work2.sh
請先設定 使用者 max 在/home 可以使用空間為 4MB ~ 5MB
要求:

- 將目前 quota 使用狀況，寫到一個記錄檔/var/log/quotareport，要將此紀錄檔自動寫信給 root，並指定信件主旨 Report Quota
- 當呼叫此 script 執行時，之前的記錄檔必須刪除
- 為了確保紀錄檔存在，請至少執行一次此 script

參考 work2.sh

```
#!/bin/bash
[ -f /var/log/quotareport ] && /bin/rm  /var/log/quotareport
/usr/sbin/repquota -a | /usr/bin/tee  /var/log/quotareport | /usr/bin/mail -s "Report Quota" root
```