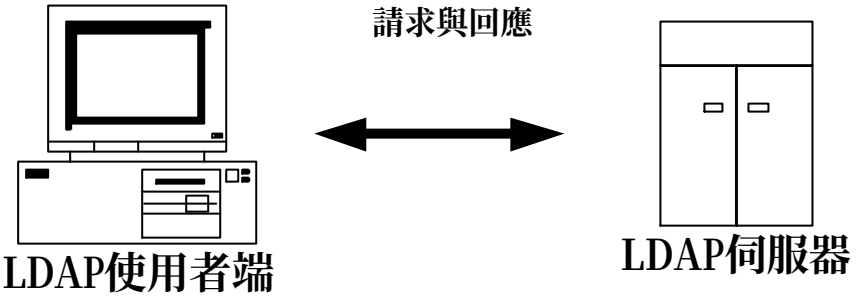
LDAP 目錄伺服器

1-1LDAP 簡介

LDAP 為輕量級名錄存取協定(Lightweight Directory Access Protocol)。LDAP 的前身為 X.500 目錄服務。LDAP 一開始是作為供桌上型電腦的輕型協定，將服務請求送到 X.500 伺服器的閘道。DNS 名稱伺服器也是 LDAP 的一種。LDAP 名錄服務與資料庫有幾個相伺的地方，資料快取和可延伸的綱要 schema。LDAP 的 directory 目錄可用來儲存二元資訊。LDAP 為以一個訊息為基礎且採用主從式架構定義於 RFC2251 的協定。我們可以到 http://en.tldp.org/HOWTO/LDAP-HOWTO/index.html 查詢所有 LDAP 目錄伺服器的說明文件。

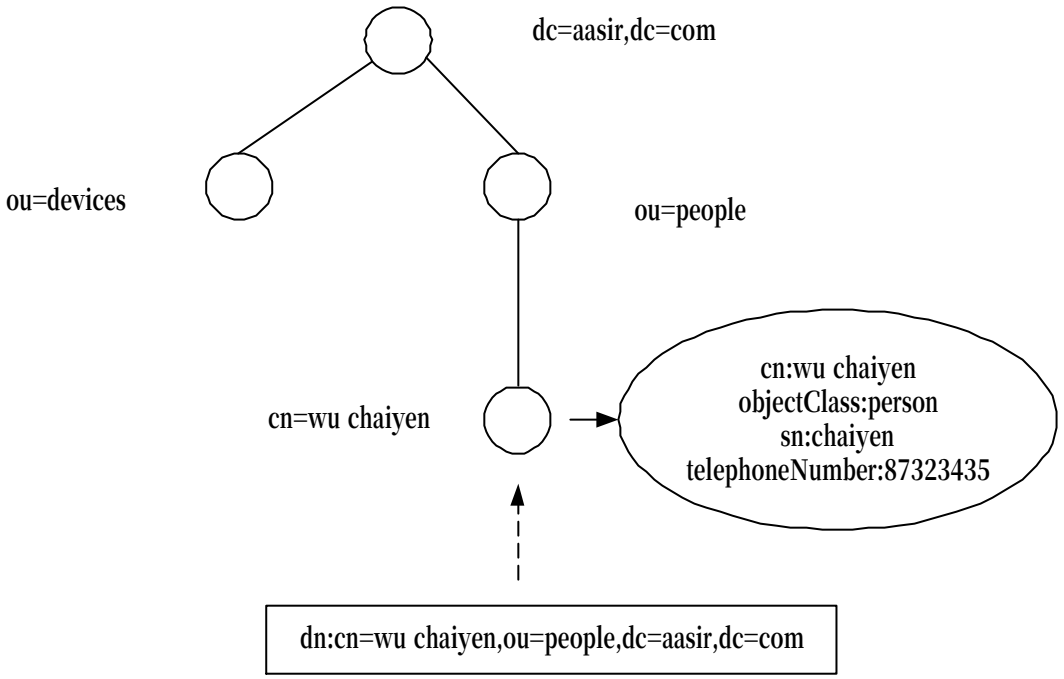


LDAP使用者端與伺服器端的關係

LDAP 模型是以使用者端的觀點來看 LDAP 伺服器所提供的服務。LDAP 定義了四個模型。

資訊模型：資訊模型提供 LDAP 建立結構和資料類型。而 entry 項目就是構成 LDAP 目錄的基本單元。名錄資訊樹 DIT(Directory Information Tree)。一筆 entry 項目所包含的資訊和一個或多個 objectClass 物件類別的實體有關。這些 objectClass 具有某些必要或選用的屬性。屬性類型所定義的編碼和規則可用來管理屬性持有的資料類型和搜詢時如何比對該資料。

命名模型：命名模型定義目錄資訊樹的項目及資料具有唯一性。這個稱為相對識別名稱 RDN(Relative Distinguished Name)。DN **就是由所在的項目節點往上直到根節點** root **的路徑，也稱為識別名稱**(Distingushed name)。**在圖中最底下的節點目錄項目有一個** cn=wu chaiyen **的** RDN。**此節點包含** RDN **的屬性和數值。最下面一個節點的** DN **是** cn=wu chaiyen,ou=opeople,dc=aasir,dc=com。



LDAP的目錄資訊樹

功能模型：LDAP **的功能模型就是協定。**LDAP **協定提供目錄樹中的存取資料方法。功能包含認證、詢問操作和更新操作。**

安全模型：安全模型提供使用者端可以證明自己的身份。

1-2LDAP 概念

LDAP 交換格式是用來儲存 LDAP 組態資訊和目錄內容的標準文字檔格式。LDIF 檔匯集了多筆項目，每筆項目以空白隔開；LDIF 包含了屬性名稱和值的對應關係；LDIF 匯集了多道指令，用來指示解析器處理資訊的方法。

LDIF 被用來將新的資料匯入名錄或者是變更資料。LDIF 檔中的資料需要按照 LDAP 目錄的 schema 綱要規則。我們可以將 schema 綱要當作是目錄的資料定義。目錄中每一筆資料的新增或變更，要按照 schema 綱要來檢查其正確性，如果資料違反 schema，則會出現違反綱要(schema violation)。

這是 LDIF 檔中的資料。

在 LDIF 語法中，#(井符號)是表示註解。

屬性在冒號(：)左邊，數值在冒號右邊。

dn 屬性可以用來辨視項目的 DN。

```
# 建立根節點
dn: dc=aasir,dc=com
dc: aasir
objectClass: dcObject
objectClass: organizationalUnit
ou: aasir dot com

## 建立'people' ou
dn: ou=people,dc=aasir,dc=com
ou: people
objectClass: organizationalUnit
```

1-2-1 屬性

屬性可以持有數值，就像一般程式設計的變數一樣，但是 LDAP 的屬性可以保有多個數值。我們可以看到 LDIF 的項目 wu chaiyen，它的 mail 屬性有兩個數值，分別是 wu.chaiyen@msa.hinet.net 和 wu.chaiyen@hotmail.com。

```
# LDIF 的項目wu chaiyen
dn: cn=wu chaiyen,ou=people,dc=aasir,dc=com
cn: wu chaiyen
sn: chaiyen
mail: wu.chaiyen@msa.hinet.net
mail: wu.chaiyen@hotmail.com
telephoneNumber: 02-87323435
objectClass: inetorgperson
```

而電話號碼可以是 a-z、A-Z、0-9 或是各種的標點符號像是連字號。屬性類型定義所包含的比對規則會告訴 LDAP 伺服器進行比對。一般在 core.schema 中定義 telephoneNumber 屬性有兩項比對規則。telephoneNumberMatch 規則用來進行是否相等的比較，telehoneNumberSubstringsMatch 規則用來處理內容的電話號碼比較。

這是定義 telephoneNumber 的屬性。EQUALITY 和 SUBSTR 為比對規則，SYNTAX 為語法規則。{32}表示屬性的最大常度。

#vi /etc/openldap/schema/core.schema

```
attributetype ( 2.5.4.20 NAME 'telephoneNumber'
        EQUALITY telephoneNumberMatch
        SUBSTR telephoneNumberSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

在 LDAP 目錄中所有項目都要有一個 objectClass 屬性。每個 objectClass 的數值就像項目中所存放資料的樣版。它會定義在項目中出現的屬性。

ObjectClass 的定義就像屬性類型、語法和比對規則，一個 objectClass 擁有一個物件識別碼 OID；關鍵字 MUST 用來表示在此物件中一定出現的任何屬性；關鍵字 MAY 用來定義不一定要在物件之實例中出現的屬性；關鍵字 SUP 指出此物件衍伸自哪個父物件，一個子物件會繼承父物件的屬性、語法和比對規則；有可能兩個物件類別擁有共同的屬性成員，整個綱要之屬性類型的命名空間是扁平的結構。

#vi /etc/openldap/schema/core.schema

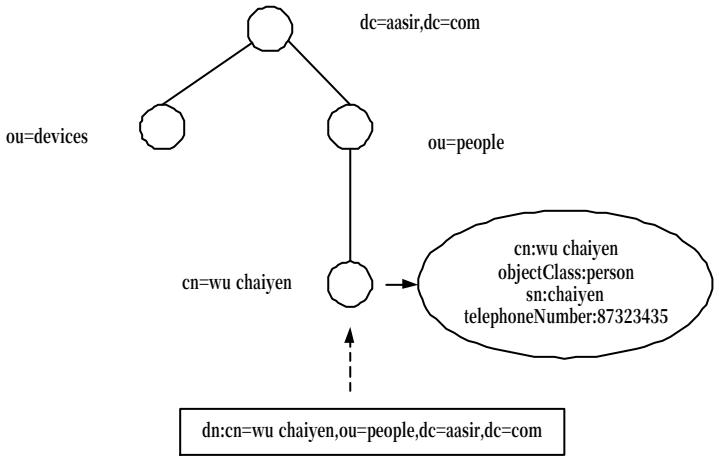
```
objectclass ( 2.5.6.5 NAME 'organizationalUnit' SUP top STRUCTURAL
        MUST ou
        MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
                x121Address $ registeredAddress $ destinationIndicator $
                preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
                telephoneNumber $ internationaliSDNNumber $
                facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
                postalAddress $ physicalDeliveryOfficeName $ st $ l $ description ) )
```

在 LDAP 伺服器中有結構性類別(structural object class)、輔助物件類別(auxiliary object class)和抽象物件類別(abstract object class)。

1-2-2dc 屬性

在根節點，我們可以解釋 domain 物件類別和 dc 屬性的意義。dcobject 是個輔助類別，可用來增加既有項目所包含的組織資訊如 organizationalUnit。domain 物件類別為一個獨立容器，可用來存放組織資訊和網域名稱元件。

```
# LDIF所列舉的內容
dn: dc=aasir,dc=com
objectClass: domain
dc:aasir
```



LDAP的目錄資訊樹

目錄的命名其根節點為 DN。LDAP 伺服器會以命名環境 dc=aasir,dc=com 來判段是否要回應使用者的請求。如果使用者端透過 Outlook 或 Netscape 來查詢 cn=wu chaiyen,ou=people,dc=false,dc=com 的資訊，我們 aasir.com 網站的 LDAP 伺服器將會回應錯誤的資訊，因為它所查詢的資訊是在我們 dc=aasir,dc=com 的命名環境外。這是將 LDAP DN 對應到 DNS 網域名稱。

schema 綱要的內容很多，我們可以在 http://docs.sun.com 來查詢其相關的文件，我們也可以由 http://www.rfc-editor.org 來查詢相關內容。

1-2-3 認證與分散式目錄

因為 LDAP 可以分為使用者端和伺服器端，因此需要連線。所有的搜詢和詢問將會受到認證之使用者授權等級控制。編碼或加密類型有{CRYPT}、{MD5}、{SHA}和{SSHA}這幾種。LDAP 目錄的認證稱為連繫 binding。一般使用者進入 LDAP 伺服器時需要提供使用者名稱和密碼。

在分散式目錄中，不同的主機有不同的目錄。主目錄伺服器 aasir.com 和次目錄伺服器 flash.aasir.com，我們使用上層連結 superiror knowledge link 和下層連結 subordinate knowledge link 來將這兩台伺服器作連結。

Superior knowledge link 也稱為 referral 也就是從次伺服器 flash.aasir.com 指回主目錄 aasir.com 。因此我們將 flash.aasir.com 伺服器設定 ldap://aasir.com/dc=aasir,dc=com。

Subordinate knowledge link 稱為 reference，也將是將目錄伺服器的某個節點連接到次伺服器的命名環境。也就是在 aasir.com 上設定 ref:ldap://flash.aasir.com/ou=people,dc=aasir,dc=org。

這是在 aasir.com 伺服器上設定的 LDIF 項目。

```
# LDIF 的項目wu chaiyen
dn: cn=wu chaiyen,ou=people,dc=aasir,dc=com
objectClass: referral
ref:ldap://flash.aasir.com/ou=people,dc=aasir,dc=com
```

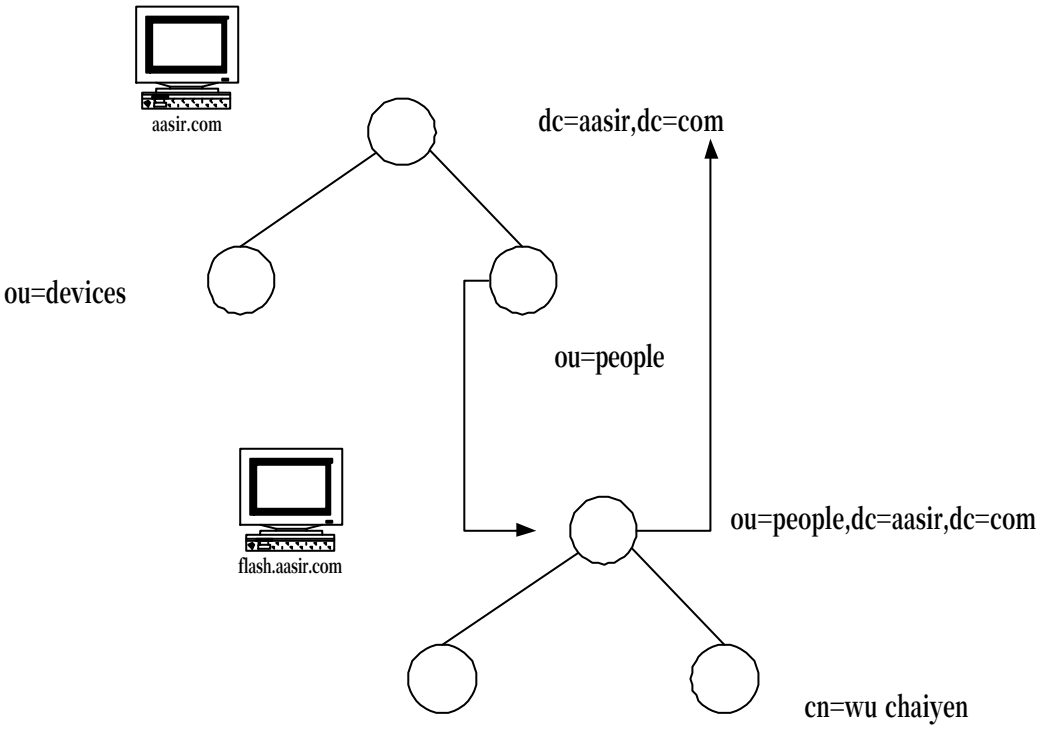
這是在 core.schema **中所設定的** referral **物件類別，其必要屬性為** ref。

vi /etc/openldap/schema/core.schema

```
objectclass ( 2.16.840.1.113730.3.2.6 NAME 'referral'
        DESC 'Named referral object'
        SUP top STRUCTURAL MUST ref )
```

這是 ref **屬性的定義**。

```
attributetype ( 2.16.840.1.113730.3.1.34 NAME 'ref'
        DESC 'Named referral'
        EQUALITY caseExactMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
        USAGE distributedOperation )
```



建立分散式目錄

1-3 安裝 LDAP 伺服器

我們可以從 http://www.openldap.org/中下載 LDAP 的軟體。我們也可以從密西根大學的伺服器下載 ftp://terminator.rs.itd.umich.edu/ldap。一般 RedHat Linux Fadora 1 或 Linux 中已經內建 LDAP 伺服器軟體，但是我們也可以下載最新版來安裝。

我們使用 tar 來解開 openldap 的原始檔。

#tar xvzf openldap-2.1.16.tgz

我們也可以使用下列 gunzip 指令來解開原始檔。

#gunzip openldap-2.1.16.tgz | tar xvf -

在組態前，我們可以觀看組態檔的設定選項。

#./configure --help

開始組態 LDAP 伺服器。

#./configure

在組態後，我們可以開始編譯，首先我們開始建立相依關係。

#make depend

開始編譯

#make

我們可以使用 make test 指令來測試編譯的情況。

#make test

現在我們可以安裝好已經編譯好的軟體。

#su root -c 'make install'

1-4 組態 LDAP 伺服器

我們在這裏以 RedHat Linux Fadora 1 所設定安裝的 LDAP 組態為主。

OPENLDAP 的元件或指令	說明
/usr/sbin/slapd	這是 slapd 執行檔所在位置，也是啟動 LDAP 伺服器的主程式。
/etc/rc.d/init.d/ldap start	這是系統啟動 ldap 的執行檔，也可以使用此程式來啟動 LDAP 伺服器。
/usr/sbin/slurpd	提供 LDAP 伺服器提供複製服務。
/usr/bin/ldapadd	在 LDAP 伺服器新增項目。
/usr/bin/ldapdelete	在 LDAP 伺服器刪除項目。
/usr/bin/ldapsearch	在 LDAP 伺服器搜詢項目。
/usr/bin/ldapmodify	在 LDAP 伺服器修改項目。
/usr/bin/ldappasswd	用來變更 LDAP 項目中的密碼屬性。

我們可以編輯 OpenLDAP 的組態檔 slapd.conf。

vi /etc/openldap/slapd.conf

這是全域區段 global section。全域區段從 slapd.conf 的第一行開始到 database 指令為止。

```
# global section

## include the minimum schema required
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
## added logging parameters
loglevel        296
pidfile         /var/slapd.pid
argsfile        /var/slapd.args

## TLS options for slapd
#TLSCipherSuite         HIGH
#TLSCertificateFile     /etc/local/slapd-cert.pem
#TLSCertificateKeyFile  /etc/local/slapd-key.pem

## misc security settings
password-hash   {SSHA}
```

1-4-1 綱要 schema

我們 LDAP 伺服器第一步就是設定決定目錄要支援哪一些綱要 schema，基本的綱要如 objectClass 和 attributeType 都是定義在 core.schema 綱要中。我們使用 include 指令來將綱要包含進來。

```
## include the minimum schema required
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
```

綱要	說明
core.schema	用來存放 LDAP 主要的核心物件和屬性。
inetorgperson.schema	用來描述 inetorgperson 物件類別和相對應的屬性，如果使用人們的聯絡資訊，則要包含此綱要。需同時引用 cosin.schema 綱要。
cosine.schema	支援 COSINE 和 X.500 目錄的計劃。
misc.schema	定義雜項物件和屬性，包含 Sendmail 以 LDAP 為基礎的郵件路徑實作。
nis.schema	定義以 LDAP 代替 NIS 伺服器所需的物件與屬性。

1-4-2 記錄檔

log 記錄可以將執行期間的資訊記錄下來。Loglevel 為登錄等級，對應的設定值是一個整數，該整數用來表示哪些類型的資訊應該記錄在系統記錄檔中。這個數值是由二的倍數的數值所組成，例如 8+32+256=296(loglevel 所指定的數值)，這表示將連線管理(8)、搜尋過濾器的處理過程和連線的統計記錄。

pidfile 此參數所指定的檔案，會包含 LDAP 的伺服器的行程編號。

argsfile 此參數所指定的檔案會包含正在執行的指令參數。

```
## added logging parameters
loglevel        296
pidfile         /var/slapd.pid
argsfile        /var/slapd.args
```

我們可以使用/etc/rc.d/init.d/ldap stauts 來觀看目前 ldap 的行程編號。

```
[root@flash chaiyen]# /etc/rc.d/init.d/ldap status
slapd (pid 2690) 正在執行中...
```

我們編輯 pidfile 所指定的/var/slapd.pid 可以看到 2690 的 ldap 行程編號。

#vi /var/slapd.pid

2690

我們編輯/var/slapd.args 來觀看目前執行 ldap 的指令。

#vi /var/slapd.args

/usr/sbin/slapd

所有的資訊可以使用 suslog 的 LOG_LEVEL4 進行登錄，我們可以在/etc/syslog.conf 系統記錄檔下增加下列，將記錄放到/var/log/slapd.log。

Local4.debug　　/var/log/slapd.log

loglevel 的數值	記錄資訊
-1	記錄所有的記錄資訊
0	不記錄
1	追蹤函式呼叫
2	封包處理
4	大量追蹤
8	連線管理
16	封包的收送
32	搜尋過濾器
64	處理組態檔
128	存取控制清單的記錄
256	操作和結果的統計
512	用戶端的統計
1024	SHELL 的通訊

1-4-3SSL/TLS 選項

TLSCERtificateFile 是設定 LDAP 伺服器的私有金鑰檔案。

TLSCERtificateKeyFile 是設定 LDAP 伺服器的公開憑証。

```
## TLS options for slapd
#TLSCipherSuite         HIGH
#TLSCertificateFile     /etc/local/slapd-cert.pem
#TLSCertificateKeyFile  /etc/local/slapd-key.pem
```

我們使用 CA.pl 來產生憑證檔 newreq.pem, 下面是產生的過程。

```
[root@flash log]# /usr/share/ssl/misc/CA.pl -newcert
Generating a 1024 bit RSA private key
.....................++++++
.++++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:tw
State or Province Name (full name) [Berkshire]:taipei
Locality Name (eg, city) [Newbury]:taipei
Organization Name (eg, company) [My Company Ltd]:aasir.com
Organizational Unit Name (eg, section) []:aasir
Common Name (eg, your name or your server's hostname) []:chaiyen
Email Address []:wu.chaiyen@msa.hinet.net
Certificate (and private key) is in newreq.pem
```

我們使用 openssl 指令來移除私鑰的密碼, 並且將私有金鑰改為 slapd-key.pem 的名子。我們將 newreq.pem 改成 slapd-cert.pem 的公開憑證, 這樣在 TLSCertificateFile 和 TLSCertificateKeyFile 再指定路徑就可以了。

```
# /usr/bin/openssl rsa -in /var/log/newreq.pem -out slapd-key.pem
Enter pass phrase for /var/log/newreq.pem:
writing RSA key
```

1-4-4 其它安全設定

password-hash 參數是用來定義作為使用者密碼屬性值的預定密碼加密，預設是{SSHA}。其它的選項包括{SHA}、{SMD5}、{MD5}、{CRYPT}和{CLEARTEXT}這幾個選項。

```
## misc security settings
password-hash   {SSHA}
```

1-4-5 資料庫區段

一個 slapd.conf 組態檔有一個全域區段 global section 和多個資料庫區段，每個資料庫區段是用來定義其目錄分割區。每一個目錄分割區開始於 database 指令，直到下一個分割區段 database 開始。

```
#######################################################
## define the beginning of example database
database        ldbm

## define the root suffix we serve
suffix          "dc=aasir,dc=com"

## define a root DN for super-user privileges
rootdn          "cn=Manager,dc=aasir,dc=com"

## define the password used with rootdn
## This is the Base64 encoded MD5 hash of 'secret'
rootpw          {SSHA}qnsN8rXUkgfAaI4mKVlhBaTctD8idm8E

## directory containing the database files
directory       /var/lib/ldap

## files should be created 'rw' for the owner **only**
mode            0600

## indexes to maintain
index           objectClass     eq
index           cn,sn,mail              pres,eq
index           departmentNumber        eq
## db tuning parameters
## cache 2,000 entries in memory
cachesize       2000
```

資料庫的參數可以是 ldbm、bdb、passwd 和 shell。

database ldbm

資料庫參數	說明
bdb	使用 Berkley DB 資料庫管理
ldbm	使用 GNU 資料庫管理
passwd	使用系統密碼檔
shell	使用外部的資料庫

suffix 是定義目錄分割區的命名環境。

suffix “dc=aasir,dc=com”

每個 LDAP 目錄要有一個 rootdn 帳號，rootdn 不會受到存取的控制。rootpw 是 rootdn 帳號的密碼。我們使用 slappasswd 指令將密碼使用 SSHA 加密，加密後會得到一大串字串，再將它放到 rootpw 中，這就是加密的密碼字串。

rootdn "cn=Manager,dc=aasir,dc=com"

rootpw {SSHA}qnsN8rXUkgfAaI4mKVlhBaTctD8idm8E

使用 slappasswd 產生 SSHA 加密的密碼，這是 secret 密碼使用 SSHA 加密的結果。

```
[root@flash chaiyen]# /usr/sbin/slappasswd -h {SSHA}
New password:
Re-enter new password:
{SSHA}qnsN8rXUkgfAaI4mKVlhBaTctD8idm8E
```

directory 是包含資料庫檔案的目錄，我們預設是放在/var/lib/ldap 中。

directory /var/lib/ldap

在/var/lib/ldap 是我們 LDAP 資料庫所產生的檔案所放置的目錄，其權限為 600。

```
[root@flash chaiyen]# cd /var/lib/ldap
[root@flash ldap]# ls
cn.dbb  dn2id.dbb  id2entry.dbb  mail.dbb  nextid.dbb  objectClass.dbb  sn.dbb
```

我們在 mode 中定義所產生檔案的權限為 600。

mode 0600

這是 LDAP 所產生的資料庫檔案，其權限為 600。

```
[root@flash ldap]# ls -l
總計 56
-rw-------    1 root     root         8192 10月 14 19:24 cn.dbb
-rw-------    1 root     root         8192 10月 14 19:24 dn2id.dbb
-rw-------    1 root     root         8192 10月 14 19:24 id2entry.dbb
-rw-------    1 root     root         8192 10月 14 19:24 mail.dbb
-rw-------    1 root     root         8192 10月 14 19:24 nextid.dbb
-rw-------    1 root     root         8192 10月 14 19:24 objectClass.dbb
-rw-------    1 root     root         8192 10月 14 19:24 sn.dbb
```

index 參數用來指定 slapd 應該為哪些屬性唯護索引。這些索引可讓搜尋操作最佳化，這就像是關聯式資料庫所用的索引。每個索引類型都會對應目錄綱要所定義的其中一個比對規則。

索引類型	說明
approx(approximate)	為屬性值的類似(approximate)或音形一致的比對索引資訊。
eq(equality)	為屬性值的相等索引比對。
pres(presence)	為判段是否存在於屬性的索引資訊。
sub(substring)	為屬性值的簡易子字串比對索引資訊。

同一個資料庫可以有多筆索引的定義，每一筆定義可以包含多個屬性或多個索引類型。各屬性或各所引類型之間用逗號隔開，屬性與索引類型之間則以空白隔開。

這是 objectClass 屬性定義相等 eq 索引。

```
index                   objectClass         eq
```

這是 cn、sn 和 mail 屬性定義存在(presence)索引和相等 equality 索引。

```
index                   cn,sn,mail                      pres,eq
```

這是 departmentNumber 屬性定義相等 eq 索引。

```
index                   departmentNumber            eq
```

cachesize 參數用來定義應該在記憶體中快取的數量項目。如果我們的目錄包含 1,000,000 筆項目，則可以設定 100,000 的快取空間，預設是 1000 筆。

```
cachesize               2000
```

1-4-6ACL 存取控制清單

使用*星號代表全部的存取對項。下面的 ACL 將會授予全部的人存取的權限，第二列的空隔表示它是前面一行的延續。

```
access to *
        by * read
```

這個允許使用者變更自己在名錄中的密碼，限製 userPassword 只能用於認證。

```
access to attrs=userPassword
       by self write
       by * auth
```

限制只能存取 userPassword 屬性，任何人都可以存取該屬性，但只能基於認證。

```
access to attrs=userPassword
       by * auth
```

有管理權限的使用者帳號放在 ou=admins,ou=eng,dc=aasir,dc=com 這個 DN 節點，一般的使用者帳號放在 ou=eng,dc=aasir,dc=com，一般使用者不應該看到其它使用者的密碼，使用者可以變更自己的密碼，具管理權限的使用者可變更任何使用者的密碼。

```
access to dn=".*,ou=eng,dc=aasir,dc=com"
       attrs=userPassword
       by self write
       by * auth
       by dn=".*,ou=admins,ou=eng,dc=aasir,dc=com" write
```

1-4-7 執行 LDAP 伺服器

啟動 LDAP 伺服器。

#/etc/rc.d/init.d/ldap start

重新啟動 LDAP 伺服器。

```
[root@flash chaiyen]# /etc/rc.d/init.d/ldap restart
停止 slapd:[失敗]
啓動 slapd:[  確定  ]
```

我們也可以使用 slapd 指令來啟動 LDAP 伺服器

#/usr/sbin/slapd

1-5 實作 LDAP 伺服器

我們在 aasir.com 伺服器上使用 LDAP 目錄伺服器，在遠端的使用用者運用 OUTLOOK 來搜尋觀看遠端的 LDAP 目錄伺服器資料。因此在這裏我們會實作 LDAP 伺服器，並且運用 Outlook 來觀看 LDAP 的內容。我們將所有員工的資料，使用 schema 綱要來定義，並且將它輸入到資料庫。當要查尋員工資料時，就可以使用 LDAP 伺服器來查詢。

1-5-1LDAP 組態設定

我們編輯 LDAP 目錄伺服器的組態檔 slapd.conf。這些相關的設定我們在前面已經有說明。這是 aasir.com 的網站，所以在 suffix 上我們定義 dc=aasir,dc=com。

vi /etc/openldap/slapd.conf

```
# global section
## include the minimum schema required
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
## added logging parameters
loglevel        296
pidfile         /var/slapd.pid
argsfile        /var/slapd.args
## misc security settings
password-hash   {SSHA}
#######################################################
## define the beginning of example database
database        ldbm
## define the root suffix we serve
suffix          "dc=aasir,dc=com"
## define a root DN for super-user privileges
rootdn          "cn=Manager,dc=aasir,dc=com"
## define the password used with rootdn
## This is the Base64 encoded MD5 hash of 'secret'
rootpw          {SSHA}2aksIaicAvwc+DhCrXUFlhgWsbBJPLxy
## directory containing the database files
directory       /var/lib/ldap
## files should be created 'rw' for the owner **only**
mode            0600
## indexes to maintain
index           objectClass     eq
index           cn,sn,mail              pres,eq
index           departmentNumber        eq
## db tuning parameters
## cache 2,000 entries in memory
cachesize       2000

# simple ACL granting read access to the world
access to *
        by * read
```

1-5-2 定義 schema 綱要

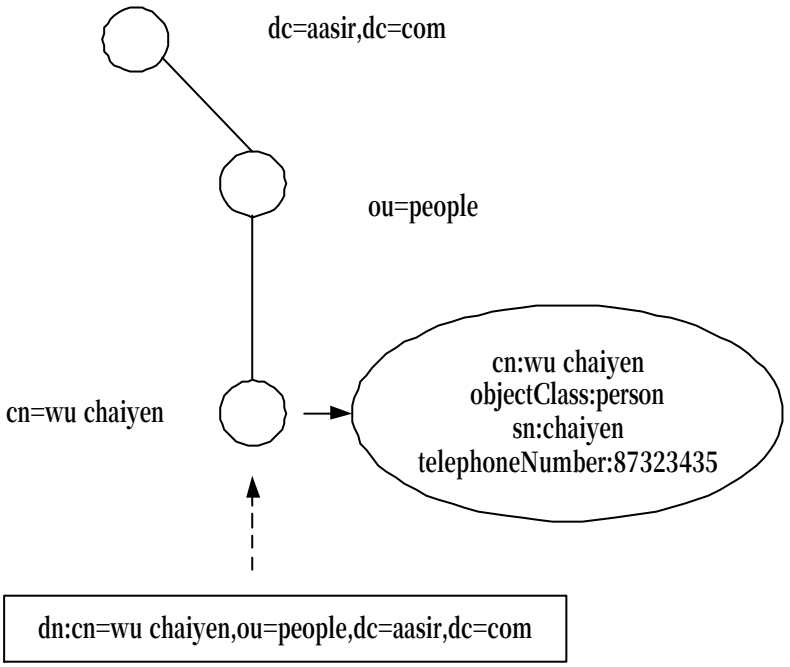
我們先定義綱要，也就是目錄儲存資訊的格式，我們的命名環境已經被定義成下面的情況。

"dc=aasir,dc=com"

員工的聯絡資訊被存放在 people 這個組織單位。

ou=people,dc=aasir,dc=com

這是 aasir.com 公司的目錄命名空間。



員工聯絡資訊

這是我們目錄中員工項目所需要包含的屬性，這包含必要的屬性 cn 和 sn。

```
dn: cn=wu chaiyen,ou=people,dc=aasir,dc=com
cn: wu chaiyen
sn: chaiyen
mail: root@aasir.com
mail: wu.chaiyen@msa.hinet.net
telephoneNumber: 02-87323435
objectClass: inetorgperson
```

1-5-3 設定儲存資料的目錄

當我們設定好 aasir.com 的綱要後，我們要在 slapd.conf 組態檔中加入支援我們所選定的屬性和物件類別。為了能夠支援 inetOrgPerson 物件類別，我們需包含 include core.schema 綱要、cosine.schema 綱要、inetorgperson.schema 綱要。

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
```

如果我們要搜尋員工的資訊，我們應該修改索引的部份，來包含完整的屬性。我們建立 cn 作索引、sn(姓氏)和 mail 電子郵件來作索引。

```
index           objectClass     eq
index           cn,sn,mail              pres,eq
index           departmentNumber        eq
```

我們也可以加入 sub(子字串)索引，這樣就可以支援子字串的索引機制。

```
index           cn,sn,amil      eq,sub
```

我們設定資料所存放的目錄位置。

```
directory       /var/lib/ldap
```

這是我們建立/var/lib/ldap 目錄，以及設定該目錄的存取權限來確保檔案系統已經可以儲存資料的目錄。

```
#mkdir –p /var/lib/ldap
#chmod 700 /var/lib/ldap
```

1-5-4 啟動 slapd

我們可以使用 SysV 來啟動 ldap。

```
/etc/rc.d/init.d/ldap restart
```

我們可以觀看 LDAP 目錄伺服器的狀態。

```
/etc/rc.d/init.d/ldap status
```

我們可以停止 LDAP 目錄伺服器。

```
/etc/rc.d/init.d/ldap stop
```

我們也可以直接啟動 LDAP 目錄伺服器，使用 LDAP 伺服器的指令。

```
#/usr/sbin/slapd
```

我們可以使用 chkconfig 指令來指定服務和希望服務執行的層級。我們可以使用 on 選項來指定服務的執行層級，也可以使用 off 選項來關閉。我們可以使用—level 選項來執行。

這 chkconfig 執行可以有/sbin/chkconfig 或者是輸入 chkconfig 來執行。這是我們啟動 LDAP 目錄網站伺服器，並且執行層級為 5。

/sbin/chkconfig --level 5 ldap on

我們使用 off 選項，當 runlevel 為 3 時，則 LDAP 目錄伺服器會關閉。

/sbin/chkconfig --level 3 ldap off

這 reset 選項將儲存服務到 chkconfig 預設選項。

/sbin/chkconfig ldap reset

我們可以觀看服務的啟動資訊使用—list 選項。

/sbin/chkconfig --list ldap

```
[root@aasir chaiyen]# /sbin/chkconfig --list ldap
ldap            0:關閉  1:關閉  2:關閉  3:關閉  4:關閉  5:開啓  6:關閉
```

執行層級 runlevel	rc.d 目錄	說明
0	rc0.d	關閉
1	rc1.d	單一使用者模式 (無網路、限制容量)
2	rc2.d	多人使用者模式(沒有支援 NFS 網路檔案系統)
3	rc3.d	多人使用者模式(全工能模式)
4	rc4.d	沒有使用到
5	rc5.d	多人使用者模式，支援圖型化界面登錄。
6	rc6.d	重新啟動系統。

1-5-5 加入目錄項目

目錄操作的工具有 slapadd、slapcat、slapindex 和 slappasswd。我們可以使用 slapadd 來將資訊加入目錄。這些命令可以讓管理者將各項目匯入資料庫檔案，並將整個目錄匯出成 LDIF 檔案。我們可以使用 man slapadd 來觀看該指令使用的方法。

我們將項目存入目錄，並建立一個 good.ldif 的檔案。這個檔案包含根節點的 LDIF 項目，並且建立 people ou 節點，節點為組織單位 organizationalUnit。

vi good.ldif

```
# Build the root node
dn: dc=aasir,dc=com
dc: aasir
objectClass: dcObject
objectClass: organizationalUnit
ou: aasir Dot com

## Build the 'people' ou
dn: ou=people,dc=aasir,dc=com
ou: people
objectClass: organizationalUnit
```

我們使用 slapadd 將 good.ldif 檔案加入到 LDAP 伺服器的目錄中。

#/usr/sbin/slapadd　-v –l　good.ldif

如果顯示這些，表示輸入到 LDAP 伺服器成功。

```
[root@aasir chaiyen]# /usr/sbin/slapadd -v -l good.ldif
added: "dc=aasir,dc=com" (00000001)
added: "ou=people,dc=aasir,dc=com" (00000002)
```

slapadd 指令選項	說明
-f 檔案	指定 slapd.conf 組態檔
-l 檔案	從指定檔案讀取 LDIF。
-v	啟動詳細訊息模式。
-c	啟動連續模式(關閉 error)
-b suffix	使用指定的 suffix 來決定加入項目到哪個資料庫。

1-5-6 查詢目錄的內容

我們先將 ldap 目錄伺服器暫停，然後再啟動。

#/etc/rc.d/init.d/ldap stop

我們使用/usr/sbin/slapd 來啟動目錄伺服器。

#/usr/sbin/slapd

我們可以使用 ldapsearch 來查詢 LDAP 伺服器。Ldapsearch 可以讓我們查詢目錄資料和存取控制的情況。我們使用 ldapsearch 指令來查詢所有 objectClass 屬性的項目。

/usr/bin/ldapsearch -x -b "dc=aasir,dc=com" "(objectclass=*)"

```
version: 2

#
# filter: (objectclass=*)
# requesting: ALL
#

# aasir, com
dn: dc=aasir,dc=com
dc: aasir
objectClass: dcObject
objectClass: organizationalUnit
ou: aasir Dot com

# people, aasir, com
dn: ou=people,dc=aasir,dc=com
ou: people
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 3
```

Ldapsearch 、 ldapadd 、 ldapdelete 、 ldapmodfy 和 ldapmodrdn 的選項	說明
-d integer	指定要記錄何種除錯資訊。
-D binddn	指定用來連結 LDAP 伺服器的 DN。
-f 檔案名稱	從指定檔案讀取 LDIF。
-H URI	指定 URI 參考到 LDAP 的伺服器。
-l	啟用 SASL 交談模式。
-k	使用 kerberos IV 授權。
-v	以詳細模式執行。
-x	用簡單的授權模式來代替 SASL。
-Y 機制	指定 SASL 機制來用於授權。
-w 密碼	指定用於認證的密碼。

1-5-7 更新目錄的資訊

我們可以新增、修改項目到目錄伺服器，我們先寫好 LDIF 項目，然後使用 ldapmodify 指令將項目加入到目錄伺服器。我們編輯員工 wu chaiyen 和 goddess tsen 的項目。

#vi users.ldif

```
## LDIF entry for 'wu chaiyen'
dn: cn=wu chaiyen,ou=people,dc=aasir,dc=com
cn: wu chaiyen
sn: chaiyen
mail: root@aasir.com
mail: wu.chaiyen@msa.hinet.net
telephoneNumber: 02-87323435
objectClass: inetorgperson

## LDIF entry for 'goddess tsen'
dn: cn=goddess Tsen,ou=people,dc=aasir,dc=com
cn: goddess
sn: goddess
mail: goddess@ddm.org.tw
telephoneNumber: 02-27360841
objectClass: inetorgperson
```

我們使用 ldapmodify 來將項目資料加入目錄伺服器 LDAP。

```
# /usr/bin/ldapmodify -D "cn=Manager,dc=aasir,dc=com" -w secret -x -a -f users.ldif
adding new entry "cn=wu chaiyen,ou=people,dc=aasir,dc=com"

adding new entry "cn=goddess Tsen,ou=people,dc=aasir,dc=com"
```

這是兩個項目的資料，chiang Ming-Feng 和 Lewis Liu，我們也使用 ldapmodify 指令將這兩筆資料再加入到 LDAP 伺服器。

```
## LDIF entry for 'chiang Ming-Feng'
dn: cn=chiang Ming-Feng,ou=people,dc=aasir,dc=com
cn: Chiang
sn: Ming-Feng
mail: jmf@sinotech.org.tw
telephoneNumber: 02-87322010
objectClass: inetorgperson

## LDIF entry for 'Lewis Liu'
dn: cn=Lewis Liu,ou=people,dc=aasir,dc=com
cn: Lewis
sn: Liu
mail: lewis@ourlinx.ocm
telephoneNumber: 02-23218617
objectClass: inetorgperson
```

這是我們使用 ldapmodify 來將這兩筆資料加入到目錄伺服器。

```
[root@aasir chaiyen]# ldapmodify -D "cn=Manager,dc=aasir,dc=com" -w secret -x -a
 -f users_1.ldif
adding new entry "cn=chiang Ming-Feng,ou=people,dc=aasir,dc=com"

adding new entry "cn=Lewis Liu,ou=people,dc=aasir,dc=com"
```

假如我們要在員工 goddess Tsen 新增 URL 的位址，我們可以使用 labeledURI 的屬性。我們使用 changetype 關鍵字來變更項目的關鍵所在。Changetype 屬性值是修改 modify，我們 add 屬性是增加 labeledURi 屬性。

#vi update.ldif

```
## add a web page location to wu chaiyen
dn: cn=goddess Tsen,ou=people,dc=aasir,dc=com
changetype: modify
add: labeledURI
labeledURI: http://www.ddm.org.tw
```

我們將原有項目使用 ldapmodify 來修改該項目。

```
[root@aasir chaiyen]# /usr/bin/ldapmodify -D "cn=Manager,dc=aasir,dc=com" -w sec
ret -x -a -f update.ldif
modifying entry "cn=goddess Tsen,ou=people,dc=aasir,dc=com"
```

這時 goddess Tsen 就會新增了 labeledURI 的屬性。

```
# goddess Tsen, people, aasir, com
dn: cn=goddess Tsen,ou=people,dc=aasir,dc=com
cn: goddess
sn: goddess
mail: goddess@ddm.org.tw
telephoneNumber: 02-27360841
objectClass: inetorgperson
labeledURI: http://www.ddm.org.tw
```

在 LDIF 檔中的 changetype 屬性, 可以接受 add、delete、modify、modrdn 和 moddn

數值	說明
add	新增項目到目錄。
delete	從目錄刪除項目。
modify	修改某項目的屬性。可以新增也可以刪除屬性值。
modrdn	變更某項目的 RDN。
moddn	變更某項目的 DN。

我們可以將項目的屬性刪除。我們將 goddess Tsen 屬性的 labeledURI 屬性刪除。

```
## delete a web page location to goddess Tsen
dn: cn=goddess Tsen,ou=people,dc=aasir,dc=com
changetype: modify
delete: labeledURI
labeledURI: http://www.ddm.org.tw
```

我們執行 ldapmodify **指令**。

```
[root@aasir chaiyen]# /usr/bin/ldapmodify -D "cn=Manager,dc=aasir,dc=com" -w sec
ret -x -a -f update_1.ldif
modifying entry "cn=goddess Tsen,ou=people,dc=aasir,dc=com"
```

這時 goddess Tsen**的** URI **就已經被刪除了**。

```
# goddess Tsen, people, aasir, com
dn: cn=goddess Tsen,ou=people,dc=aasir,dc=com
cn: goddess
sn: goddess
mail: goddess@ddm.org.tw
telephoneNumber: 02-27360841
objectClass: inetorgperson
```

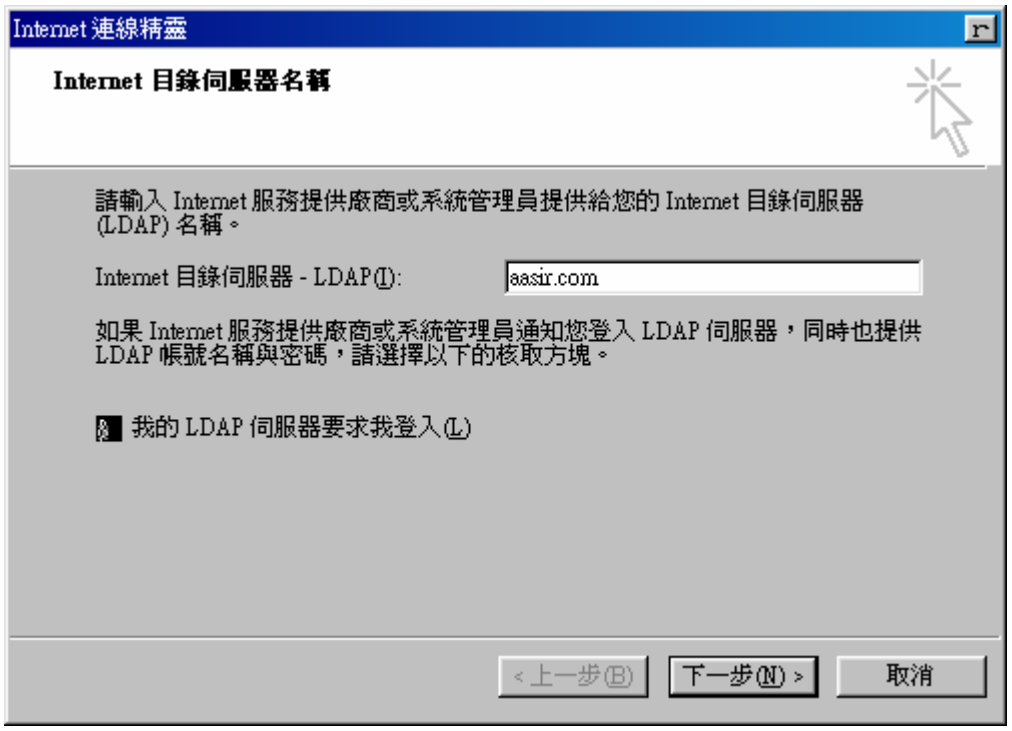
1-5-8 使用者端 LDAP

我們可以使用 Outlook 來觀看遠端 LDAP 目錄伺服器的各項資訊。例如我們要搜尋某個員工的資料時，我們只要打開我們的 Outlook 就可以查詢該員工的資料了。

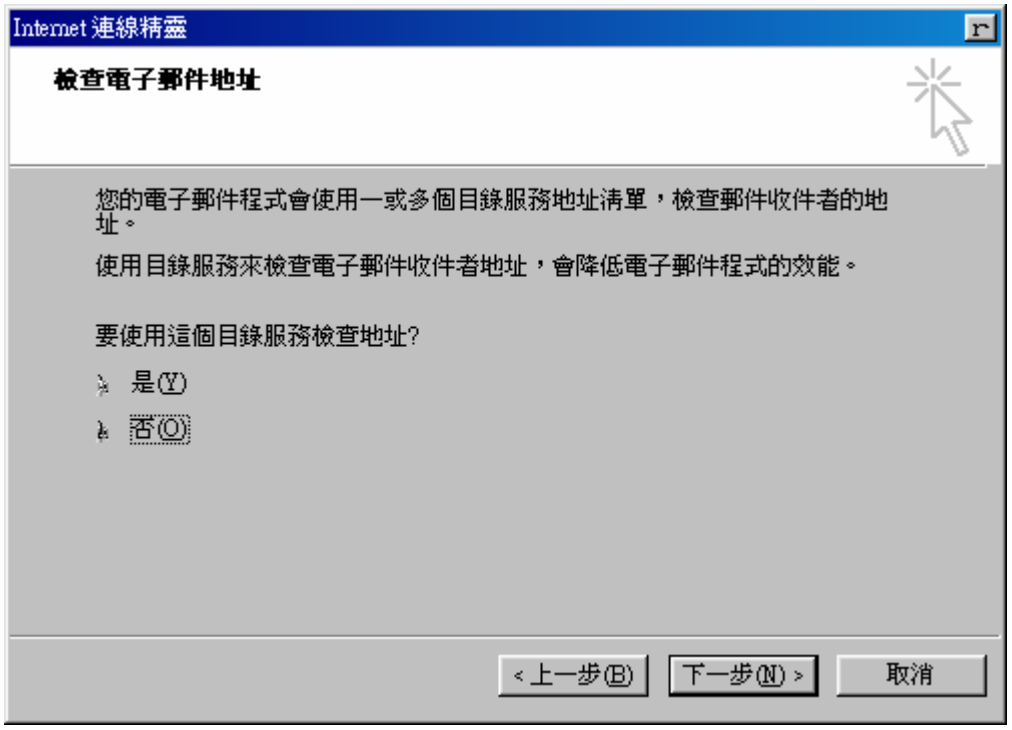
我們開啟 outlook，選取工具→帳號。

我們選取新增→目錄服務。

我們輸入我們 LDAP **目錄伺服器的位置** aasir.com。

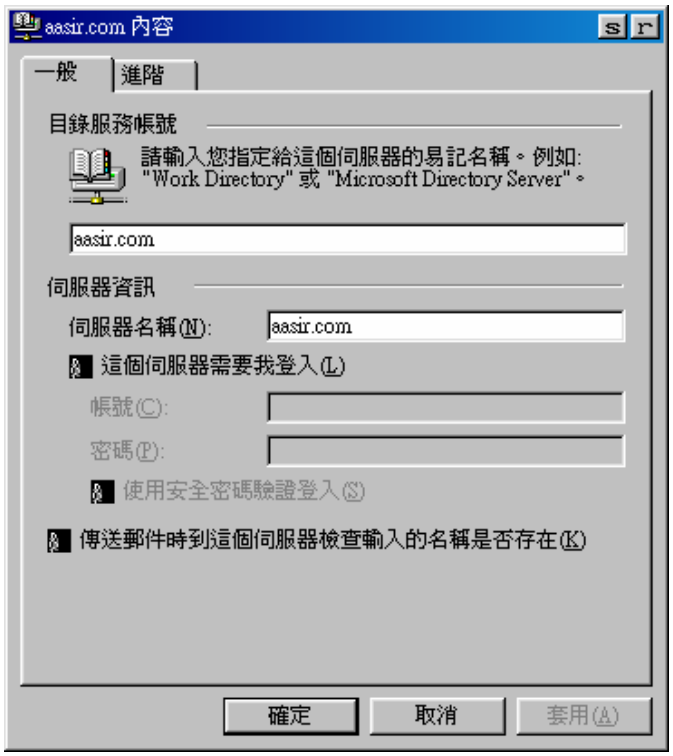


我們選取下一步。

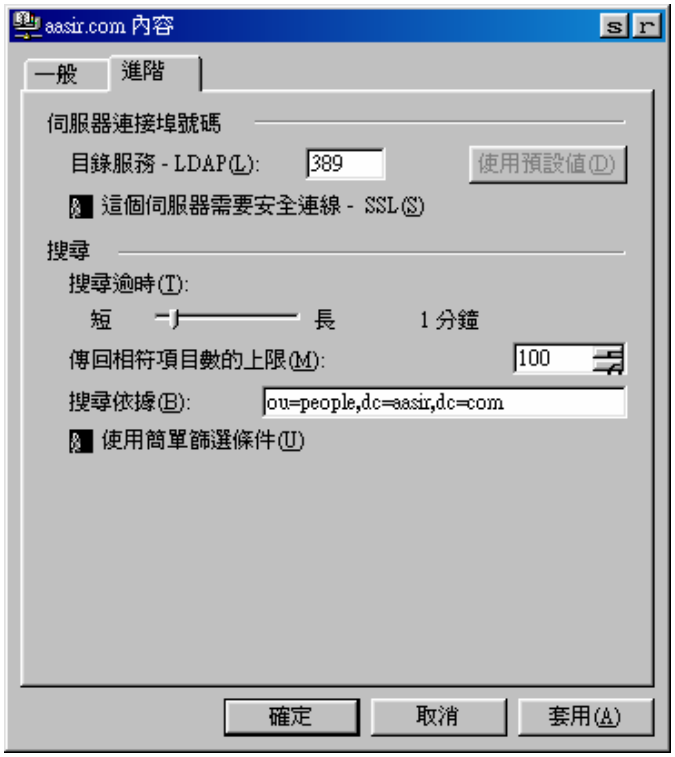


選取 aasir.com **目錄服務，並且選取內容。**

我們輸入目錄伺服器的名稱 aasir.com。

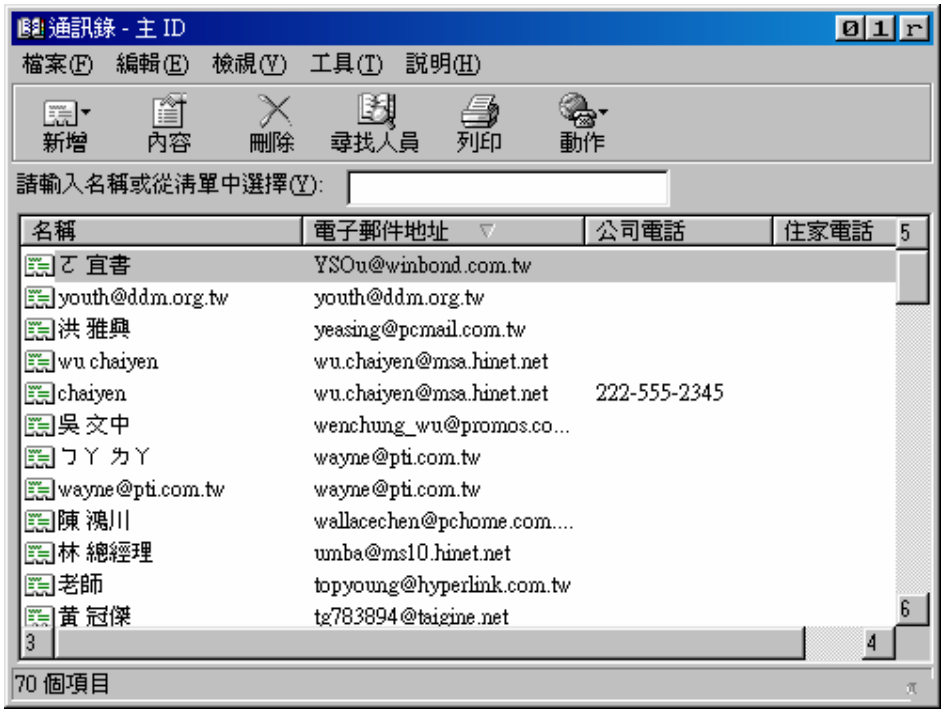


我們選取進階，一般目錄服務的連接埠是 389。我們的搜尋依據是 ou=people,dc=aasir,dc=com。

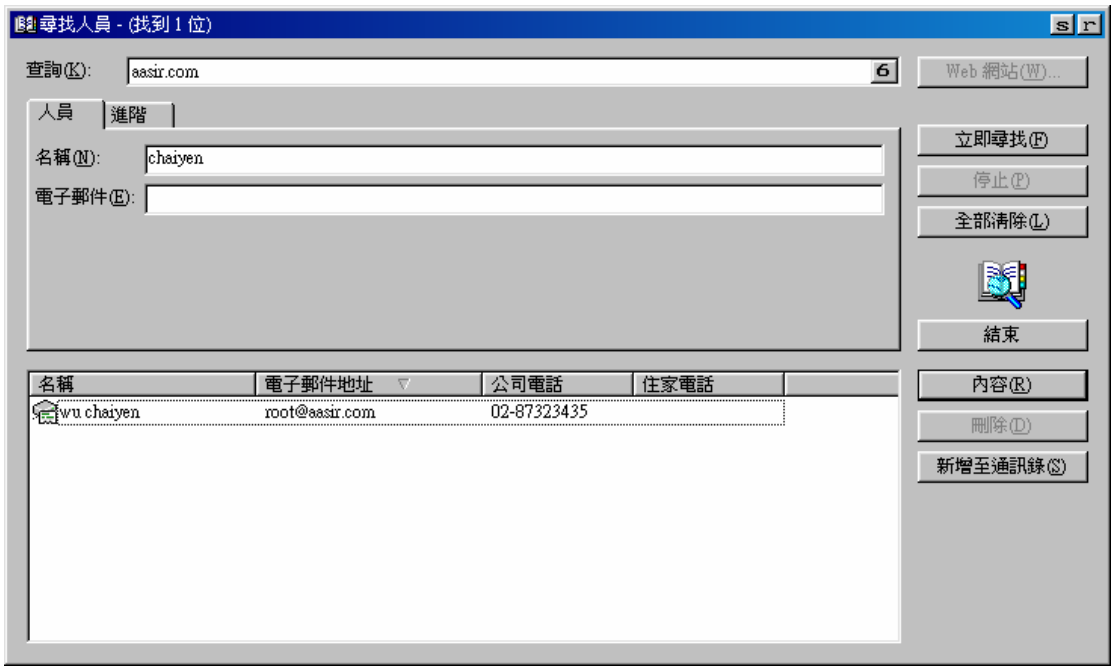


我們設定好之後可以開始搜尋遠端的 LDAP 目錄伺服器，我們選取工具→通訊錄。

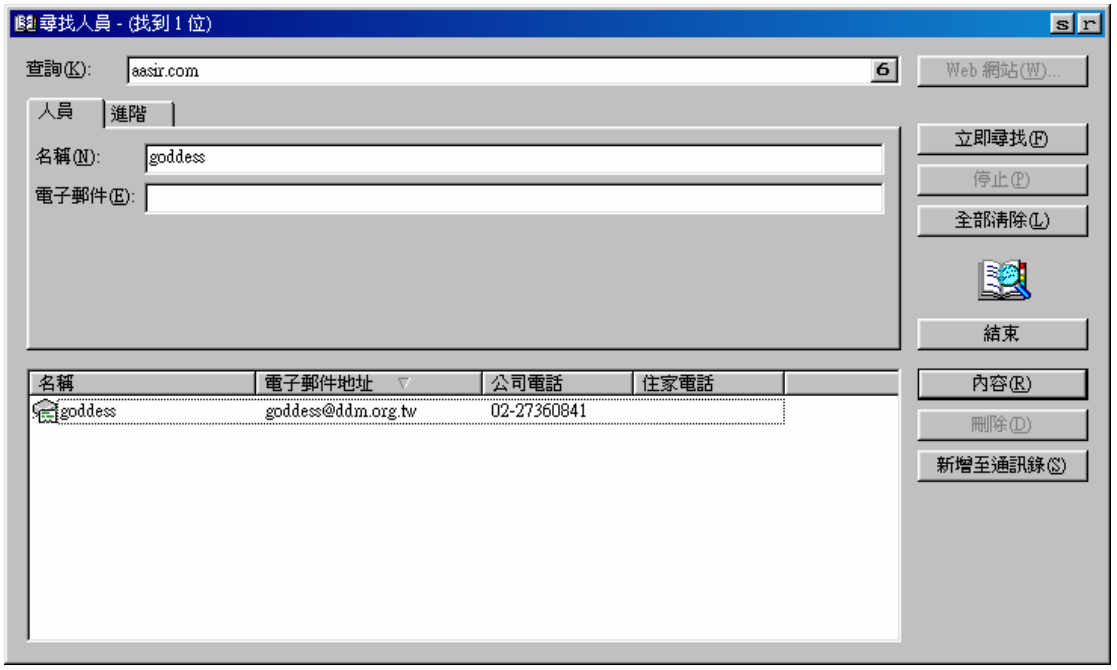
我們選取尋找人員。



我們查詢的是 aasir.com **的目錄伺服器** LDAP。**我們輸入** chaiyen **名稱，並且按下立即尋找，這樣就可以找到遠端** aasir.com **的** LDAP **目錄伺服器資料。**



我們也可以搜尋特定員工的資料，並且按下內容。



我們可以在內容觀看 goddess **的詳細資料。**