網路安全的理論與實務

楊中皇 著

第十七章 OpenLDAP目錄服務

http://crypto.nknu.edu.tw/textbook/

伴 您 學 習 成 長 的 每 一 天

第十七章 OpenLDAP目錄服務

- 目錄服務簡介
- LDAP通信協定
- OpenLDAP的安裝方法
- OpenLDAP的使用

目錄服務簡介

- 目錄服務是一種資料儲存的結構與擷取之協定，目錄服務是網路上尋找資料的一種便捷方法
- 就像家中的電話簿或小型資料庫一樣，雖沒有像資料庫擁有許多複雜功能，但透過它可以查詢網路上親朋好友的電子郵件帳號，或是公司行號的電話等

目錄服務簡介(續)

- 目錄服務除了提供查詢個人帳號或是公司資料外，另一個重要應用是，可以結合公開金鑰基礎建設(PKI)，負責維護憑證管理中心目錄內的資訊，作爲核發公開金鑰憑證或憑證廢止清單(CRL)的存放，以提供使用者查詢與下載
- 藉由目錄服務技術方便使用者下載憑證，可簡化憑證管理中心操作流程，此外，透過目錄服務的技術可以更具結構化的爲各式資源進行命名、說明、搜尋、存取及保護等

LDAP通信協定

- X.500是由國際電信標準組織所制定的目錄服務技術標準，由於架構制定過於龐大複雜且耗費系統資源，所以很難實作而不被業界採用
- 後來OSI為了改善上述問題，便針對X.500標準進行精簡，重新規劃一種較簡潔又有效率的通訊協定，即LDAP(Lightweight Directory Access Protocol，輕量型目錄存取協定)
- LDAP最早是被當作X.500的前端通訊協定，後來則逐漸演變成以LDAP伺服器為主

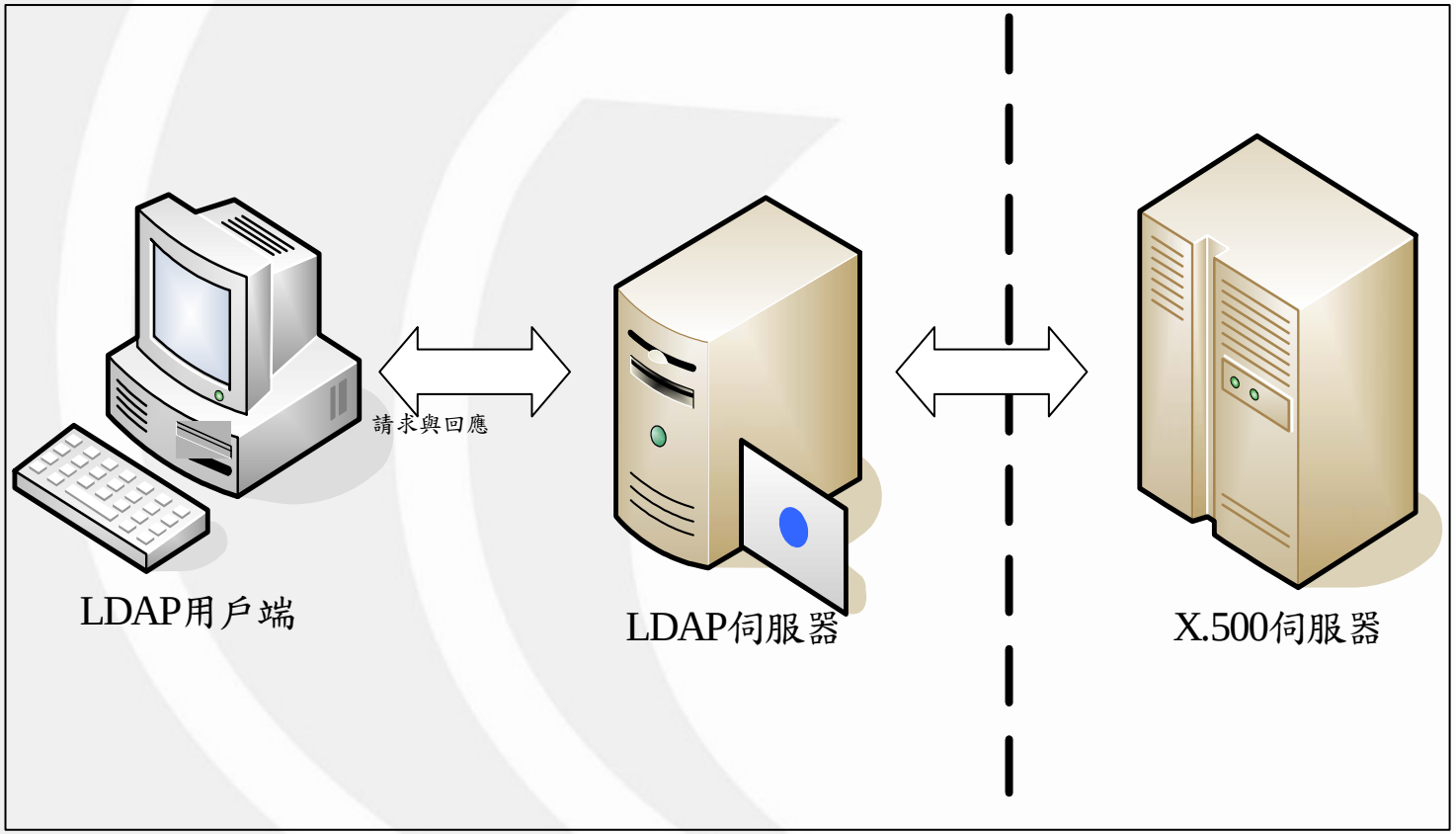
LDAP通信協定(續)

- X.500的使用者與伺服器端之間是以OSI通信協定進行通訊，OSI是個七層堆疊的網路協定，它的複雜與繁重相對於TCP/IP協定，而LDAP相形之下就輕量多了
- LDAP不僅保留X.500標準的優點，還可降低整體管理的成本，讓各個系統存取目錄服務時更簡便
- LDAP涵括了當初X.500所有大部份功能，但卻只有X.500相對極小的資源耗用率，所以被稱爲輕量型目錄存取協定。

LDAP通信協定(續)

- 在設計上，LDAP一開始是作爲X.500伺服器的前端
- 使用者向X.500伺服器進行目錄資訊的存取，而LDAP則被設計爲依據前端的目錄存取需求，向後端的X.500目錄服務伺服器進行各種目錄資訊存取的操作，如：複製(Replica) 、參照(Referral)等
- 使用者透過LDAP將服務請求送到X.500伺服器，LDAP運作在TCP/IP網路上，預設使用port 389進行通訊

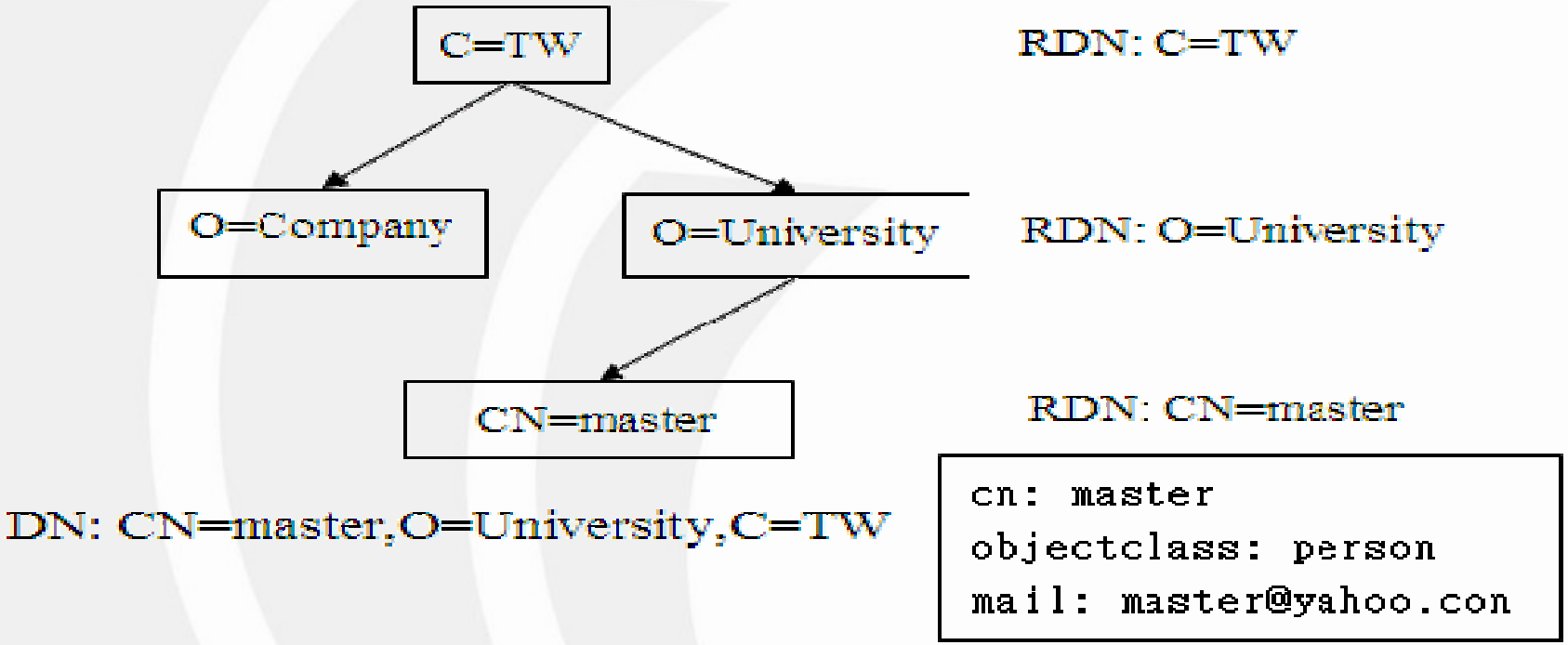
LDAP用戶端/伺服器與X.500伺服器之間的關係



命名空間

- 在X.500定義中，目錄服務內部所儲存的資訊都有一個很清楚的命名與定址機制，這個機制稱之爲命名空間(Namespace)
  - 命名空間所對應的資訊儲存空間稱爲DIT(Directory Information Tree)
  - 在DIT中每個節點(Node)被稱爲Entry或Object
  - 每個Entry是由一些屬性(Attribute)所構成
  - 其每個屬性都有自己隸屬的屬性種類(Attribute Type)
  - 而每個Entry也都有自己隸屬的物件類別(Object Class)
  - 每一個Entry都有一個唯一的識別名稱(DN，Distinguished Name)
  - 而DN是由多個RDN (Relative Distinguished Name)依序構成的字串

master的命名空間



- 如上圖，有個Entry稱爲master，它的完整識別名稱(DN)，DN=CN=master,O=university,C=TW，是由其上鄰接節點的RDN串接而成，而其物件類別爲person，其中的mail屬性其值是master@yahoo.com

LDAP四個模型

- 資訊模型：資訊模型提供了LDAP建立結構和資料類型，而Entry就是構成LDAP目錄的基本單元。
  - 一筆Entry所包含的資訊和一個或多個objectclass物件類別有關
  - 這些objectclass具有必要的或選用的屬性
  - 屬性類型所定義的編號或規則可用來管理屬性特有的資料類型和搜尋時如何比對的規則
- 命名模型：其定義在於目錄資訊樹的物件及資料具有唯一性，這個命名爲相對識別名稱(RDN)，由鄰接物件節點RDN往上串接直到根節點(root)的路徑，所形成的名稱爲識別名稱(DN)
- 功能模型：LDAP的功能模型就是協定，是提供目錄樹中的資料存取方法，包含認證、詢問和更新操作
- 安全模型：提供使用者可以證明自己身份的方法

LDAP的目錄樹

- LDAP的目錄樹是一層層分支出去的樹狀結構，而整個目錄分佈在許多伺服器中，每個伺服器都複製了一個整體分支圖，定期同步化複製資料
- 在資料庫裡，每一筆紀錄稱之爲Entry，Entry並不限定只儲存使用者相關的資料，也可以是一個部門或是一台電腦或一台伺服器的相關資料
- 在將Entry資料存入到資料庫之前，必須先以LDIF語法定義每一項Entry。

LDIF

- LDAP交換格式(LDAP Interchange Format，簡稱LDIF)定義於RFC2849，係用來儲存LDAP組態資訊和目錄內容的標準文字檔格式
- LDIF通常用來將新的資料匯入目錄或是變更既有資料
- LDIF檔中的資料需要按照LDAP目錄的schema綱要規則，而綱要檔可以當作是目錄的資料類型定義，目錄中每一筆資料的新增或修改，依照綱要檔規則來檢查其正確性，如果匯入資料違反綱要檔，會造成違反綱要(schema violation)的結果，將無法順利建立此資料

LDIF語法

- LDIF檔中，#符號表示註解

- LDIF內含了屬性名稱和值的對應，屬性列在冒號(：)的左邊，而值出現在右邊，冒號與值之間以一個空格隔開

- LDIF檔匯集了多筆項目，每筆項目以空白列隔開

LDAP目錄服務優點

- 使用標準的協定：LDAP是由IETF所訂的標準協定，就像TCP/IP、SMTP、SNMP等，可以與世界知名的目錄服務主機互通資料
- 有多種存取權限：LDAP能將使用者分類，並且賦予個別存取權限，可以限制使用者在網路上的資源，提供既開放又保密的功能
- 具有安全編碼功能：LDAP支援資料加密，使得一般使用者不能輕易從LDAP伺服器得到資料，以保障使用者隱私
- 提供快速且進階的搜尋功能：LDAP的搜尋功能讓使用者找尋帳號或是個人資料時，可以關鍵字查詢，讓使用者能快速查到想要的資料

LDAP之普及

- LDAP目前已有40多家公司採用
  - 如Netscape已將之包含在最新版的Communicator套裝產品中
  - 微軟Windows NT內附「Active Directory」產品
  - Novell NetWare Directory Services 與LDAP相容
  - Cisco 的網路產品也支援
  - 目前在Unix-like系統下免費且功能強大的LDAP Server莫過於OpenLDAP，其在Red Hat Linux Distribution皆有提供。

LDAP發展歷史

- LDAP第一版(LDAPv1)是由密西根大學發表
  - 當初LDAP設計是爲了作X.500目錄伺服器的前端存取方法，當作與X.500目錄伺服器對話的輕量型協定
  - 逐漸發展成以LDAP爲主體的伺服器設計
  - 設計來提供存取目錄能力，並提供簡單管理與瀏覽應用，作爲與目錄溝通的介面
  - LDAPv1文件在1994年3月發表，但並未成爲IETF正式文件
- LDAP第二版(LDAPv2)
  - 發表於1995年3月RFC 1777
  - 在1996年4月，40多家廠商，包含Microsoft，Netscape，Novell宣佈旗下目錄服務產品可以支援LDAP
  - 可以整合應用在網路上，因此LDAP得到極大重視

LDAP第三版

- LDAP第三版(LDAPv3)發表於1997年12月RFC 2251，主要用來取代LDAPv2，而LDAPv3與LDAPv2及LDAPv1相比新增以下幾項功能：
  - 智慧性參照：本地伺服器根據詢問可以參照其他伺服器目錄，即使用者可運用遍及網路的通訊錄做查詢，透過單一伺服器查到其他網路的資料
  - 支援萬國碼UTF-8編碼：使用者可使用當地語言佈署目錄伺服器，應用程式可以在單一視窗顯示多重語言，像Netscape Directory Server 4.0就支援38種語言，並且允許使用者加入新的分類功能
  - 加強安全認證：支援SSL與SASL，加強認證與加密保護目錄資料
  - 動態延伸綱要檔：透過綱要檔管理操作LDAP，使用者可按需求自行制定綱要檔，設定使用者喜愛組態，或其他共享資料。
  - 通信協定延伸：不需重寫就可以加入新的協定操作，所以使用者可依自己需求擴充新的協定

LDAP各版本差異性

	LDAPv1	LDAPv2	LDAPv3
適用網路	TCP/IP	TCP/IP	TCP/IP
安全性	Password/ Kerberos	Password/ Kerberos	Password/Kerberos /SSL/TLS/SASL
綱要檔	固定	固定	動態

LDAP各版本差異性說明

- 就安全性來說，LDAPv1和LDAPv2提供兩種身分認證方法—明文密碼和Kerberos 4，但在LDAPv3則另外提出SASL(Simple Authentication Socket Layer)與X.509強健型的身份認證方法
- 所謂簡單身分認證方式就是輸入帳號或密碼，這種認證方式的安全性令人擔憂，而SASL提供使用者與伺服器之間一個安全協調的對話機制，用以決定雙方將來通話時所使用的安全協定。
- SASL定義在RFC 2222，是提供連線導向通信協定支援認證的方法，用來建立使用者與伺服器在連線初期之間安全層次的協議。
  - 如果伺服器支援SASL，在連線初期就會做認證協定交換，認證過程中會有一系列伺服器的挑戰(challenges)和使用者的回應(responses)
  - 交換過程皆用編碼方式傳送，認證方法是使用者傳送一個授權識別碼(authorization identity)到伺服器端，協商彼此之間使用的安全層次
  - 如果雙方都接受，接下來要定義或協商的就是每一次接收時安全層接收緩衝的最大容量
  - SASL支援幾種認證方法，包括GSSAPI for Kerberos V，DIGEST-MD5和TLS等。
- LDAPv2與LDAPv3差異極大，應儘量避免兩者佈署在一起，基本上LDAPv2已面臨被淘汰邊緣

LDAP相關RFC文件-LDAPv2

- LDAPv2(草案)
  - RFC1487，X.500 Lightweight Directory Access Protocol，1993年7月發表
  - RFC 1488，The X.500 String Representation of Standard Attribute Syntaxes，1993年7月發表
  - RFC 1558，A String Representation of LDAP Search Filter，1993年發表
- LDAPv2(草案標準)
  - RFC 1777，Lightweight Directory Access Protocol，1995年3月發表
  - RFC 1778，The String Representation of Standard Attribute Syntaxes，1995年3月發表
  - RFC 1798，Connection-less Lightweight Directory Access Protocol，1995年7月發表
  - RFC 1823，The LDAP Application Program Interface，1995年8月發表

LDAP相關RFC文件-LDAPv3

- RFC 2251，Lightweight Directory Access Protocol(v3)，1997年12月發表
- RFC 2252，Lightweight Directory Access Protocol(v3)-Attribute Syntax Definitions， 1997年12月發表
- RFC 2253，Lightweight Directory Access Protocol(v3)-UTF-8 String Representation of Distinguished Named，1997年12月發表
- RFC 2254，The String Representation of LDAP Search Filter，1997年12月發表
- RFC 2255，The LDAP URL Format，1997年12月發表
- RFC 2256，A Summary of the X.500 User Schema for use with LDAPV3，1997年12月發表
- RFC 2829，Authentication Methods for LDAP
- RFC 2830，Lightweight Directory Access Protocol(v3)：Extension for Transport Layer Security
- RFC 3377，Lightweight Directory Access Protocol(v3)：Technical Specification

操作平台

- OpenLDAP適用在Unix-like系統下
  - RedHat Linux
  - SuSE Linux
  - Mandrake Linux
  - Debian GNU/Linux
  - OpenBSD，NetBSD，FreeBSD
- 亦支援Windows

OpenLDAP安裝-Linux

- 預先安裝SSL/TLS程式庫(建議OpenSSL 0.9.7+)
- SSL/TLS可讓LDAP的用戶端與伺服端在交談期間，甚至在認證用戶端之前，可以進行SSL/TLS session的安全會談
- 相關軟體請至OpenSSL Project (http://www.openssl.org/)下載。安裝步驟如下：
  - 先將openssl安裝套件解壓縮
  - #tar zxvf openssl-0.9.7e.tar.gz
  - 切換到openssl目錄下執行安裝
  - #cd openssl-0.9.7e
  - # ./config
  - # make
  - # make install

安裝Berkeley DB 4程式庫

- 先將BerkerlyDB套件解壓縮
  - # tar zxvf db-4.3.28.tar.gz
- 切換到BerkeleyDB目錄下執行安裝
  - # cd db-4.3.28/build_unix
  - # ../dist/configure
  - # make ; make install
- 將BerkeleyDB的lib路徑加到/etc/ld.so.conf中並執行ldconfig，使OpenLDAP能找到對應的library位置
  - # vi /etc/ld.so.conf
- 在檔案末端加入 /usr/local/BerkeleyDB.4.3/lib
  - # ldconfig

安裝Cyrus SASL 2.1.18+

- LDAP需要SASL的最常見理由是整合Kerberos認證，如果您只想以簡易(明文)繫結來存取目錄，可以不需安裝SASL，但是要識別可以變更資料的管理者身分，就必須經由SASL來認證
- SASL程式庫是由卡內基美濃大學製作，可至 ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/下載，而安裝步驟如下：
- 先將cyrus-sasl安裝套件解壓縮
  - # tar zxvf cyrus-sasl-2.1.19.tar.gz
- 切換到cyrus-sasl目錄下執行安裝
  - # cd cyrus-sasl-2.1.19
  - # ./configure
  - # make
  - # make install
  - # ln –s /usr/local/lib/sasl2 /usr/lib/sasl2
- 最後需要使用到連結符號，是因爲SASL程式庫將會在/usr/lib/sasl2/目錄中尋找已安裝的機制。

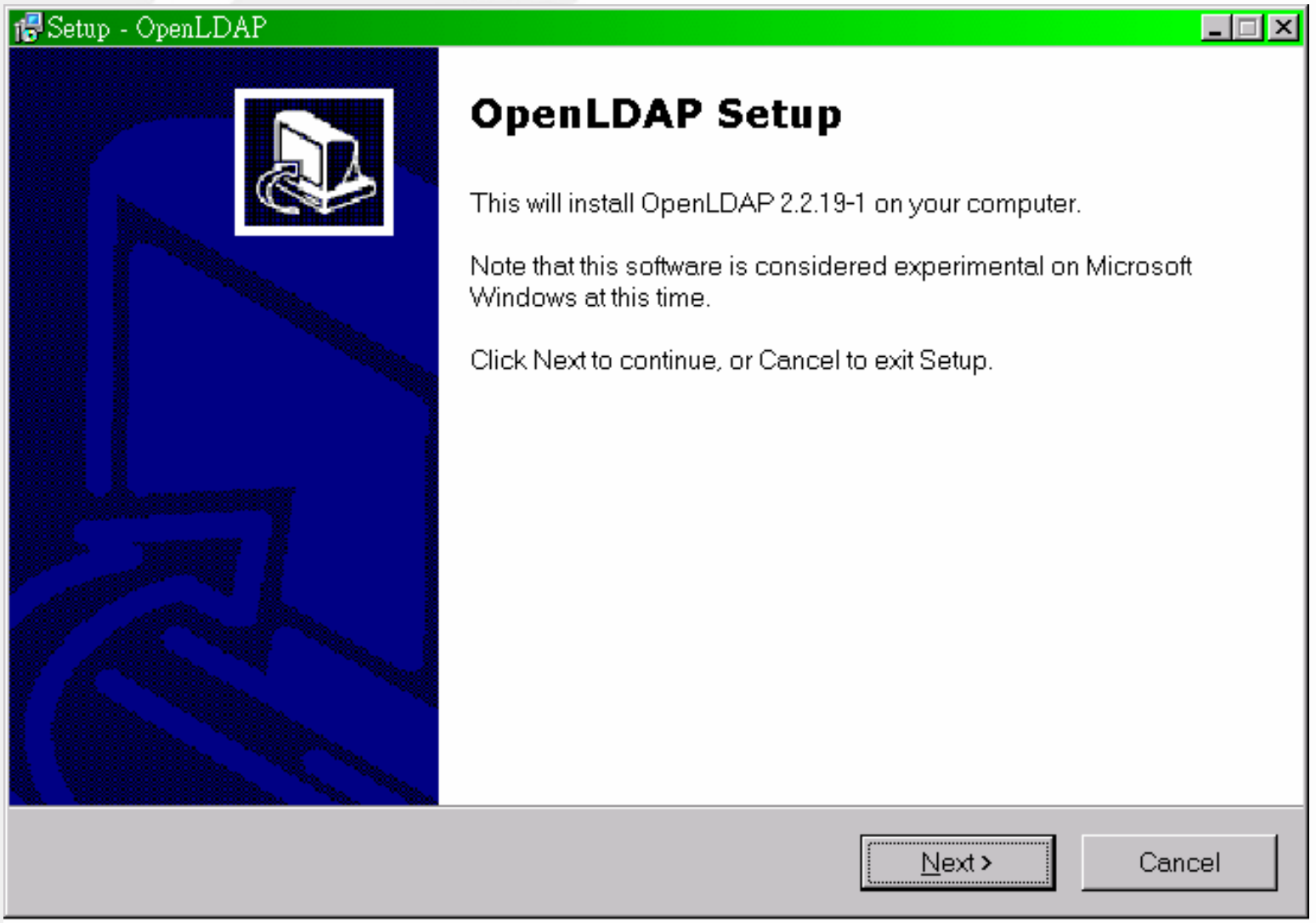
編譯且安裝OpenLDAP

- 先將OpenLDAP安裝套件解壓縮並切換到openldap目錄下
  - # tar zxvf openldap-2.2.24.tar.gz
  - # cd openldap-2.2.24
- 將OpenLDAP資料庫位置設定到安裝好的BerkeleyDB
  - # env CPPFLAGS="-I/usr/local/BerkeleyDB.4.3/include "LDFLAGS="-L/usr/local/BerkeleyDB.4.3/lib"
- configure script支援許多選項，可以使用./configure --help命令，列出完整參數選項：
  - # ./configure
- 建立軟體，這一步有兩個部份，第一部份是構連相依套件，然後再編譯
  - # make depend
  - # make
- 爲確認是否編譯正確，這一個測試步驟不要省(可能會花幾分鐘)。
  - # make test
- 安裝軟體
  - # make install

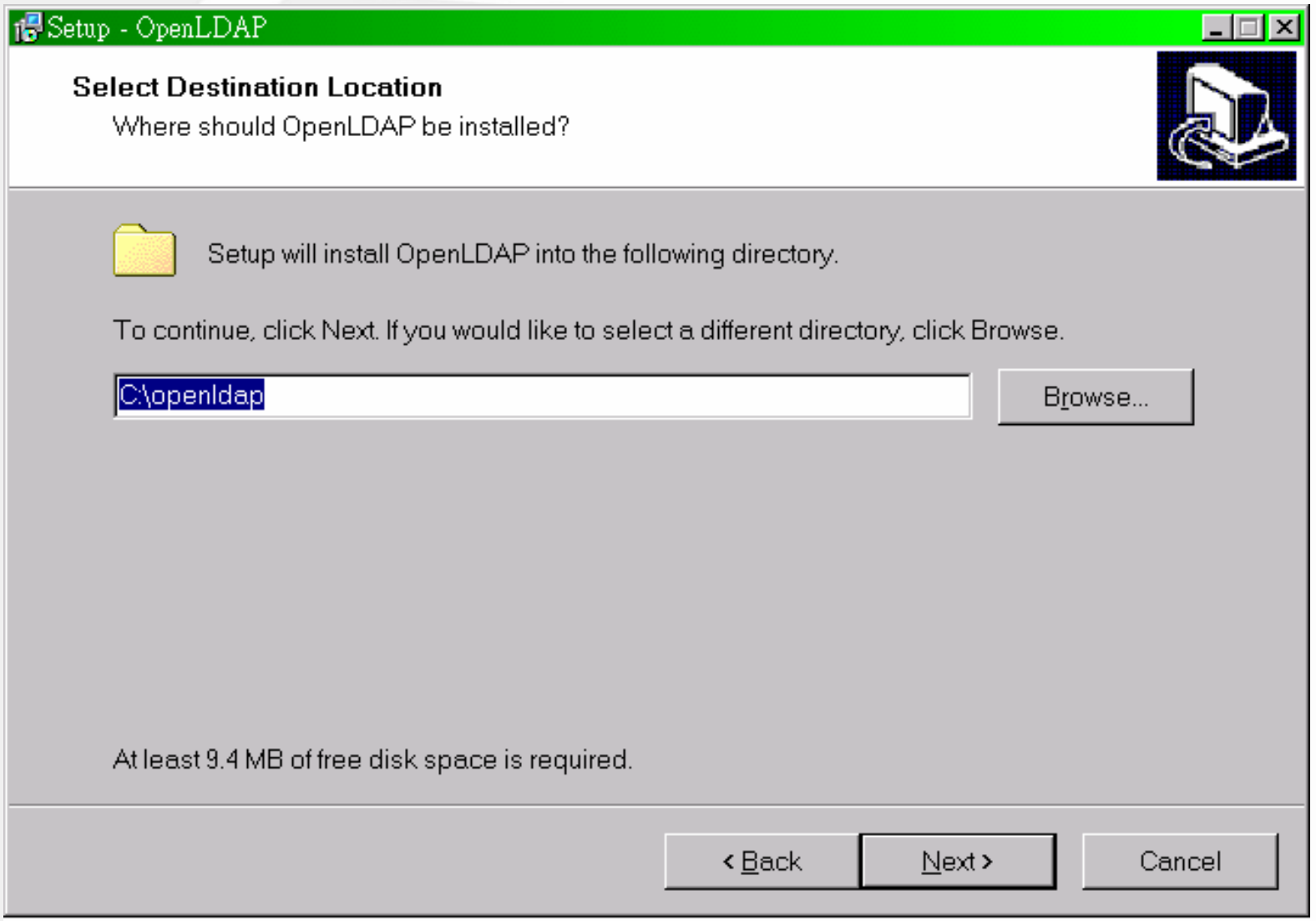
OpenLDAP安裝-Windows

- 在Windows上安裝OpenLDAP
- 只需從
  - http://lucas.bergmans.us/hacks/openldap/download 下載安裝檔
- 依安裝精靈指示一步步執行，就可以完成安裝步驟

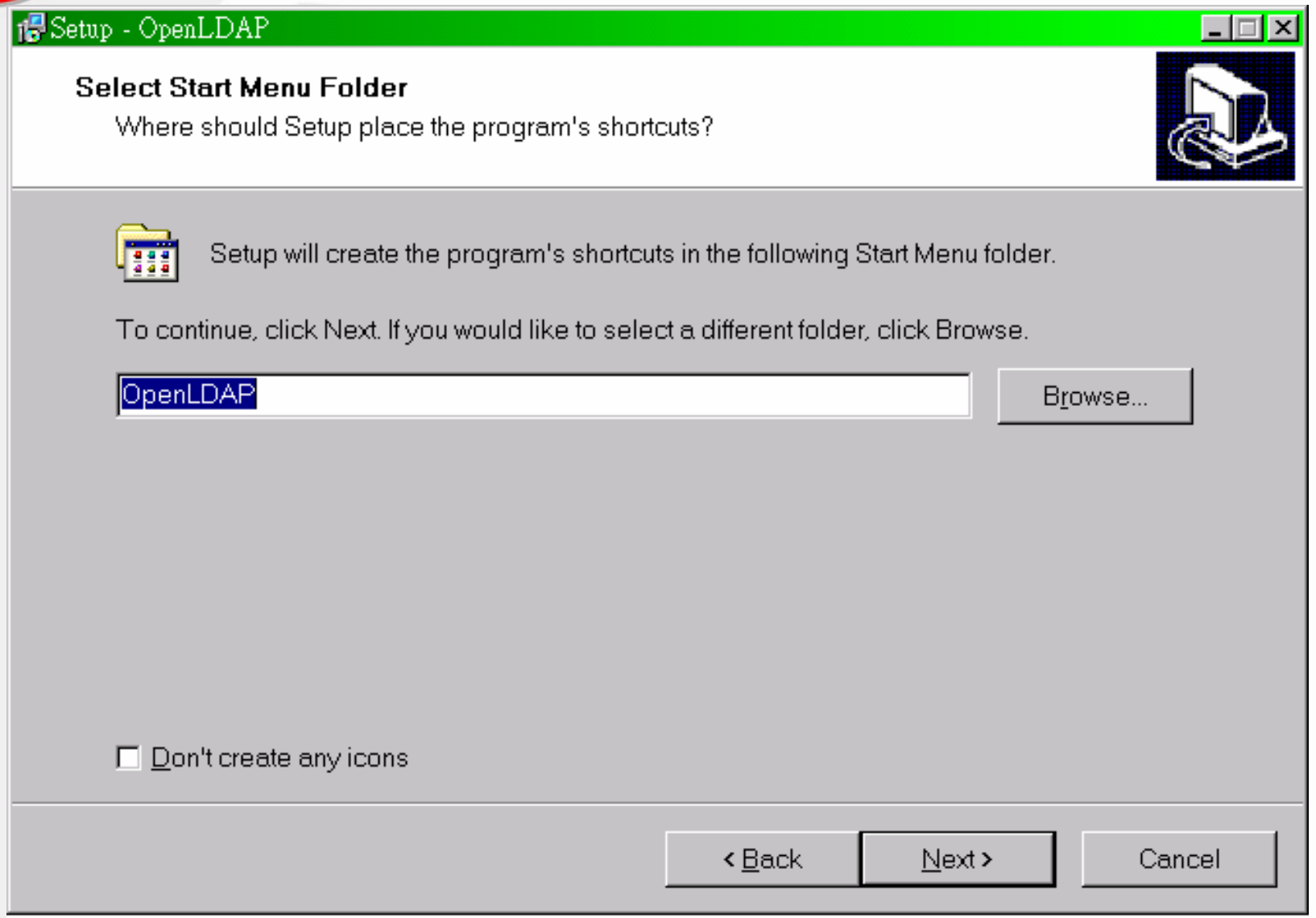
OpenLDAP for win32 啓始安裝畫面



安裝路徑採用預設值即在C:\openldap



OpenLDAP for win32 執行安裝



OpenLDAP的使用

- OpenLDAP套件中包含slapd（OpenLDAP獨立伺服器）、slurpd（OpenLDAP複製伺服器）及用戶端、伺服器與發展程式庫
- 在OpenLDAP安裝成功後，在啓動之前，第一步要先設定slapd.conf組態檔，而在編譯slapd.conf 時，要遵循以下規則：
  - #字號開頭或是空白列忽略不執行。
  - 參數與相對應的值用空白符號（空格[space]或跳格[tab]）隔開。
  - 若第一行爲空格，則視爲前一列的延續，無須使用延續符號，例如倒斜線（＼）。
- slapd.conf分成兩個區段
  - 第一個區段爲全域區段（global section），裡面參數的設定關係到OpenLDAP伺服器的整體行爲
  - 第二區段爲資料庫區端（database section），其設定與slapd所使用的資料庫有關
- 一個slapd可以佈署一個以上的後端資料庫，而他們與相對應資料是分開存放的，資料庫間不會相互影響

OpenLDAP所安裝的元件

名稱	說明
libexec/slapd	LDAP伺服器
libexec/slurpd	協助LDAP伺服器提供複製服務
Bin/ldapadd	這些命令列工具程式可用來在LDAP伺服器上新增、變更及刪除項目。這些命令同時支援LDAPv2和LDAPv3。
Bin/ldapmodify	
Bin/ldapdelete	
Bin/ldapmodrdn	
Bin/ldapsearch	這些命令列公用程式可用來搜尋LDAP名錄，或是針對某項目(entry)所持有的特定屬性(attribute)進行比較操作的測試。
Bin/ldapcompare	
Bin/ldappasswd	這個工具程式可用來變更LDAP項目的密碼屬性。
sbin/slapadd	這些工具程式可用來操作slapd在當地所使用的後端資料庫。
sbin/slapcat	
sbin/slapindex	
sbin/slappasswd	這個簡單的公用程式可用來產生適合用來在slapd.conf檔中的密碼雜湊值。
lib/libldap*	OpenLDAP用戶端軟體發展工具箱。
lib/liblber*	
include/ldap*.h	
include/lber*.h	

LDAP schema

- 設定slapd.conf 第一步就是決定目錄支援那種schema(綱要檔)
- 所謂schema ，簡單來說就是支援何種資料類型，其綱要檔預定存放路徑在/usr/local/etc/openldap/schema
- 在slapd.conf組態檔中，用include來指定伺服器所要引用的綱要檔，下面是設定最基本組態的方式：
  - #
  - # See slapd.conf(5) for details on configuration options.
  - # This file should NOT be world readable.
  - #
  - include /usr/local/etc/openldap/schema/core.schema
  - include /usr/local/etc/openldap/schema/cosine.schema
  - include /usr/local/etc/openldap/schema/inetorgperson.schema

LDAP schema(續)

- core.schema
  - 存放OpenLDAP必要的核心綱要，此綱要定義了RFCs 2251-2256所描述的、基本的LDAPv3屬性與物件。
- cosine.schema
  - 支援COSINE與X.500目錄的實驗計畫，參見RFC 1274。
- inetorgperson.schema
  - 定義了RFC 2798所描述的inetOrgPerson物件類別及其相對應的屬性，此物件常被拿來存放人們的聯絡資訊。
- nis.schema
  - 定義了RFC 2307所描述的、以LDAP替代NIS時所必需的屬性與物件。
- 要引用綱要檔時，除了要瞭解儲存物件所支援的資料型態而慎選綱要檔外，尚須注意綱要檔之間的相依關係

登錄（loglevel）

- slapd.conf的全域區段會看到一段登錄參數
  - # Do not enable referrals until AFTER you have a working directory
  - # service AND an understanding of referrals.
  - # referral ldap://root.openldap.org
  - loglevel 296
  - pidfile /usr/local/var/run/slapd.pid
  - argsfile /usr/local/var/run/slapd.args
- 可用來控制slapd將資訊登錄於何處，及實際寫入日誌檔的資訊量
- loglevel爲登錄等級，可將執行期間的資訊記錄下來，其設定值爲整數，該整數用來表示那些類型的資訊，應該紀錄在系統紀錄檔中
- pidfile filename 此參數所指定的檔案，將會儲存目前正在執行的slapd的行程識別碼(process ID)
- argsfile filename 此參數所指定的檔案，將會包含目前正在執行slapd行程所使用的命令列參數

OpenLDAP登錄等級

-1	所有的登錄資訊
0	不登錄任何資訊
1	追縱函式呼叫
2	封包處理除錯資訊
4	大量追蹤除錯資訊
8	連線管理
16	列出封包的送收
32	搜尋過濾器(Search filter)的處理
64	組態檔的處理
128	存取控制清單的處理
256	連線、操作及結果的統計
512	結果傳回用戶端的統計
1024	與shell後端的通訊
2048	印出物件剖析除錯資訊

SASL選項

- 全域區段有包含三個與SASL有關的選項：
  - sasl-host（hostname）：提供SASL認證主機的完整網域名稱(FQDN)；hostname是slapd伺服器的網域名稱
  - sasl-realm（string）：用來認證的SASL網域
  - sasl-secprops（properties）：是定義各種會對SASL影響的安全特性
- 如果不想易受主動攻擊或匿名攻擊機制，可使用DES加密法，其設定爲
  - sasl-secprops　noactive,noanonymous,minssf=56

sasl-secprops的參數值

none	清除預定的安全特性(noplain、noanonymous)
noplain	停用易受被動攻擊的機制
noactive	停用易受主動攻擊的機制
nodict	停用易受字典檔攻擊的機制
noanonymous	停用支援匿名攻擊的機制
forwardsec	需要在會談中交換秘密
passcred	需要傳遞憑證的機制
minssf=factor	定義要實施最小安全強度設定值。其值包含：0(不防護)、1(僅有完整性防護)、56(允許DES加密)、112(允許Triple DES或其他串流加密法)以及128(允許RC4、Blowfis或同類的其他加密法)。
maxssf=factor	定義要實施最大安全強度設定值
maxbufsize=size	定義安全層接收緩衝的最大容量。

資料庫區段

- 一個slapd.conf組態檔有一個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

```
########################################################################
# ldbm database definitions
########################################################################
database    bdb
suffix      “dc=example,dc=com”
rootdn      “cn=Manager,dc=example,dc=com”
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw      secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory    /usr/local/var/openldap-data
mode       0600
# Indices to maintain
index   objectclass       eq
index   cn,sn,mail        eq,sub
index   departmentNumber  eq
# ACL
access to *
      by * read
```

資料庫區段(續)

- 撰寫資料庫區段第一步就是定義資料庫的類型，本章是使用Berkley DB 4資料庫管理程式，定義是bdb，OpenLDAP建議使用此後端資料庫。另外一種是ldbm，係實作自GNU Database Manager或Sleepycat的Berkeley DB，相較於bdb是較舊的
- # 定義資料庫後端類型
  - database bdb
  - # 定義根物件(root entry)的命名環境
  - suffix “dc=example,dc=com”

資料庫區段(續)

- 每個LDAP目錄都須有個root DN(rootdn)帳號，相似於Unix系統的超級使用者(root)帳號，還有個相對應的root password(rootpw)，其預設值是secret
- 可用slappasswd指令將密碼用{CRYPT}、{MD5}、{SMD5}、{SSHA}和{SHA}來加密，加密後可得到一大串字串，再將它放在rootpw中，就是加密後的密碼字串：
  - rootdn “cn=Manager,dc=example,dc=com”
  - rootpw {SSHA}2aksloiqpcAvwc+DhCrXuFiHihsWbJpLxyG
- directory是包含資料庫檔案的目錄，預設存放在/usr/local/var/openldap-data
- 在mode中定義資料庫檔案只讓擁有者有讀寫權限(0600)
  - directory /usr/local/var/openldap-data
  - mode 0600

比對規則

- Index參數通常是指定slapd應該用哪些屬性當作維護索引，這些索引可讓搜尋速度最佳化，就像是關聯式資料庫所用的索引
- 每個索引類型都會對應到目錄綱要所定義的比對規則
- 同個資料庫可有多筆索引比對的規則，其每筆定義可以包含多個屬性或多個索引類型，各屬性或各索引類型之間用逗號隔開，屬性與索引類型之間則用空白隔開：
  - # Indices to maintain
  - index objectclass eq
  - index cn,sn,mail eq,sub
  - index departmentNumber eq

比對規則表

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類型
eq(equality)	為屬性值相等的索引比對
pres(presence)	為判斷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

存取控制清單(ACL)

- OpenLDAP所提供的目錄存取控制清單，儘管語法簡單但非常有彈性而且功能強大；基本上是用來定義誰(who)有權力(right)存取什麼(what)?
- 下面的ACL將會授予全部的人都有存取的權限，第二列的空格表示是前一列的延續
  - # ACL
  - access to *
  - by * read
- 以下則是只允許使用者變更自己目錄中的密碼，限制userPassword只能用於認證
  - access to attrs=userPassword
  - by self write
  - by * auth

ACL使用者定義規則

*	任何使用者連線
Self	現行使用者連線
anonymous	未經過認證的使用者連線
Users	經過認證的使用者連線

執行LDAP伺服器

- 啓動LDAP伺服器
  - # /usr/local/libexec/slapd
- 以ps 命令驗證slapd是否正在執行
  - # ps –ef | grep slapd
- 執行上述指令後，應該會看到如下輸出：
  - root 3443 1 0 20:39 ? 00:00:00 /usr/ local/libexec/slapd
  - root 3458 3399 0 20:42 tty1 00:00:00 grep slapd
- 停止LDAP伺服器
  - # kill –INT <process id of slapd listed by ps aux>
- 或
  - #cat /usr/local/var/run/slapd.pid
  - #3443 (系統回應)
  - #kill –INT 3443

加入目錄項目

- 目錄操作工具有slapadd、slapcat、slapindex和slappasswd
- slapadd 是利用來將資訊加入目錄，讓管理者能將各項目匯入資料庫檔案，並將整個目錄匯出成LDIF檔案
- 查看該指令使用方式請使用man slapadd指令

加入目錄項目(續)

- 首先，建立一個root.ldif檔案，這個檔案須包含根節點的LDIF項目，並且建立people ou節點，而節點爲組織單位OrganizationalUnit。操作指令如下：
  - # vi root.ldif
  - ## Build the root node
  - dn: dc=example,dc=com
  - dc: example
  - objectClass: dcObject
  - objectClass: organizationalUnit
  - ou: Example Dot Com
  - ## Build the ‘people’ ou
  - dn: ou=people,dc=example,dc=com
  - ou: people
  - objectClass: organizationalUnit
- 接著使用slapadd 將root.ldif檔案加入到LDPA伺服器的目錄中，如表17.7所示。
  - # /usr/local/sbin/slapadd –v –l root.ldif
- 如果顯示以下這些文字，則表示成功加入到LDAP伺服器的目錄中。
  - add: “dc=example,dc=com”(00000001)
  - add: “ou=people,dc=example,dc=com”(00000002)

slapadd指令選項

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來決定加入項目到那個資料庫

查詢目錄的內容

- 要查詢LDAP伺服器的目錄資料和存取控制的情況及所有objectClass屬性的項目
- 利用ldapsearch指令
  - # /usr/local/bin/ldapsearch –x –b “dc=example,dc=com” “(objectclass=*)”

新增、修改項目到目錄伺服器

- 例如要編輯Tiger Wang和Jerry Carter等人員的項目，其指令及操作方式如下
  - # vi users.ldif
  - ## LDIF entry for ‘Tiger Wang’
  - dn: cn=Tiger Wang,ou=people,dc=example,dc=com
  - cn: Tiger Wang
  - sn: Wang
  - mail: wang@yahoo.com
  - mail: wang2005@hotmail.com
  - roomNumber: 822 David Hall
  - departmentNumber: Engineering
  - telephoneNumber: 0836-478234
  - mobile: 0935239872
  - objectClass: inetorgperson
  - ## LDIF entry for ‘Jerry Carter’
  - dn: cn=Jerry Carter,ou=people,dc=example,dc=com
  - cn: Jerry Carter
  - sn: Carter
  - mail: carter@nowhere.net
  - telephoneNumber: 555-123-1234
  - objectClass: inetorgperson

新增、修改項目到目錄伺服器(續)

- 編輯完後，再使用ldapmodify將項目資料加入目錄伺服器LDAP：
  - # /usr/local/bin/ldapmodify –D “cn=Manager,dc=example,dc=com” –w secret –x –a –f users.ldif
- 假設需在 Tiger Wang新增URL的欄位，可以使用labeledURI的屬性，並使用changetype關鍵字來變更項目的關鍵所在；Changetype屬性值是修改(modify)，而add屬性是增加labeledURI屬性
  - # vi update.ldif
  - ## add a web page location to Tiger Wang
  - dn: cn= Tiger Wang,ou=people,dc=example,dc=com
  - changetype: modify
  - add: labeledURI
  - labeledURI: http://www.yahoo.com/tigerwang
- ldapmodify是修改原有項目的指令，如下：
  - # /usr/local/bin/ldapmodify –D “cn=Manager,dc=example,dc=com” –w secret –x –a –f update.ldif
- 這時Tiger Wang就會增加labeledURI屬性

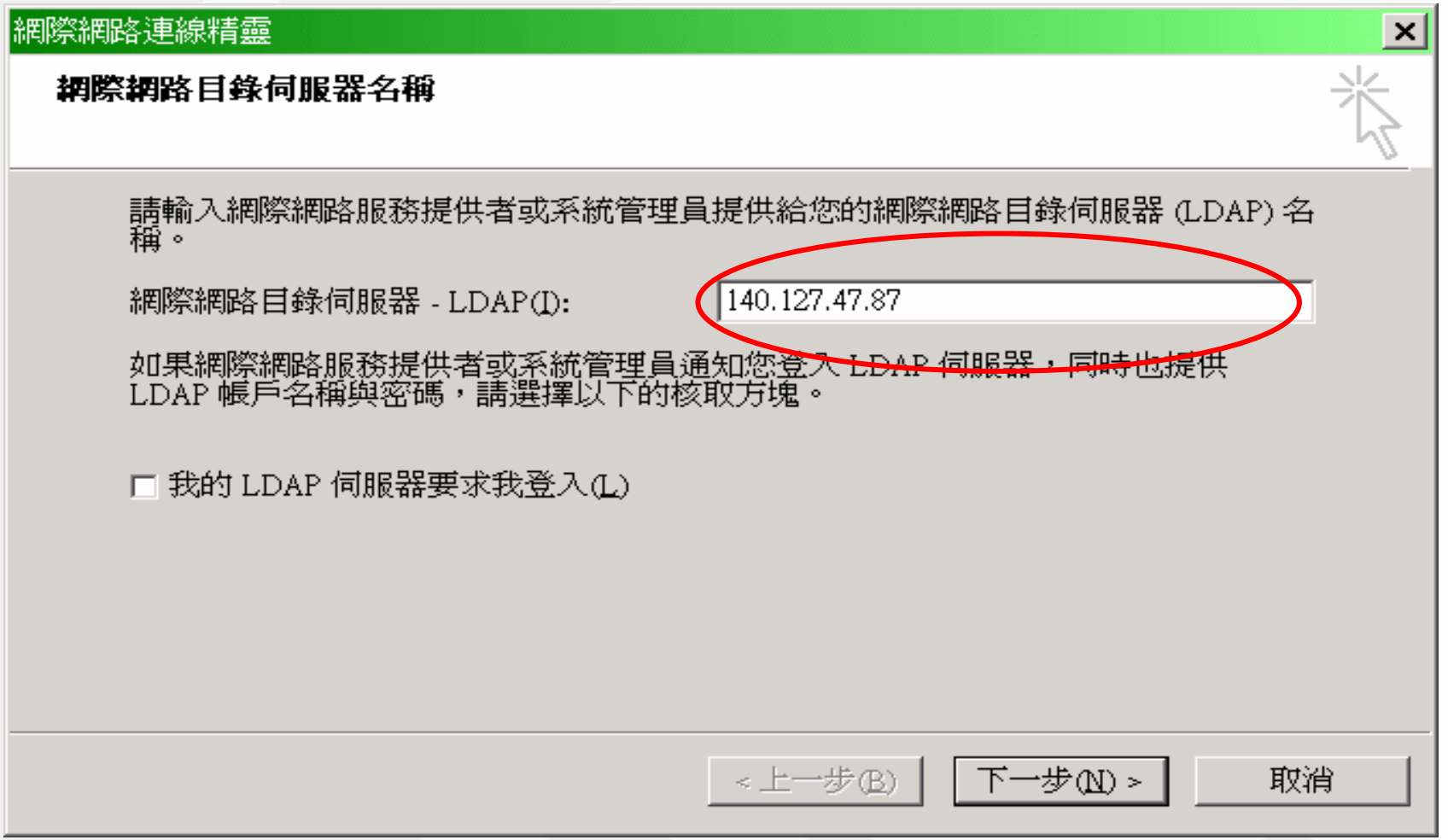
LDAP 用戶端應用實例

- Microsoft Outlook Express支援LDAP協定，可利用Outlook Express觀看遠端LDAP目錄伺服器的各項資訊；例如搜尋個人資料時，只須打開outlook就可以查詢該人員的資料
- 開啓Outlook Express，「工具」==>「帳號」(如上圖)

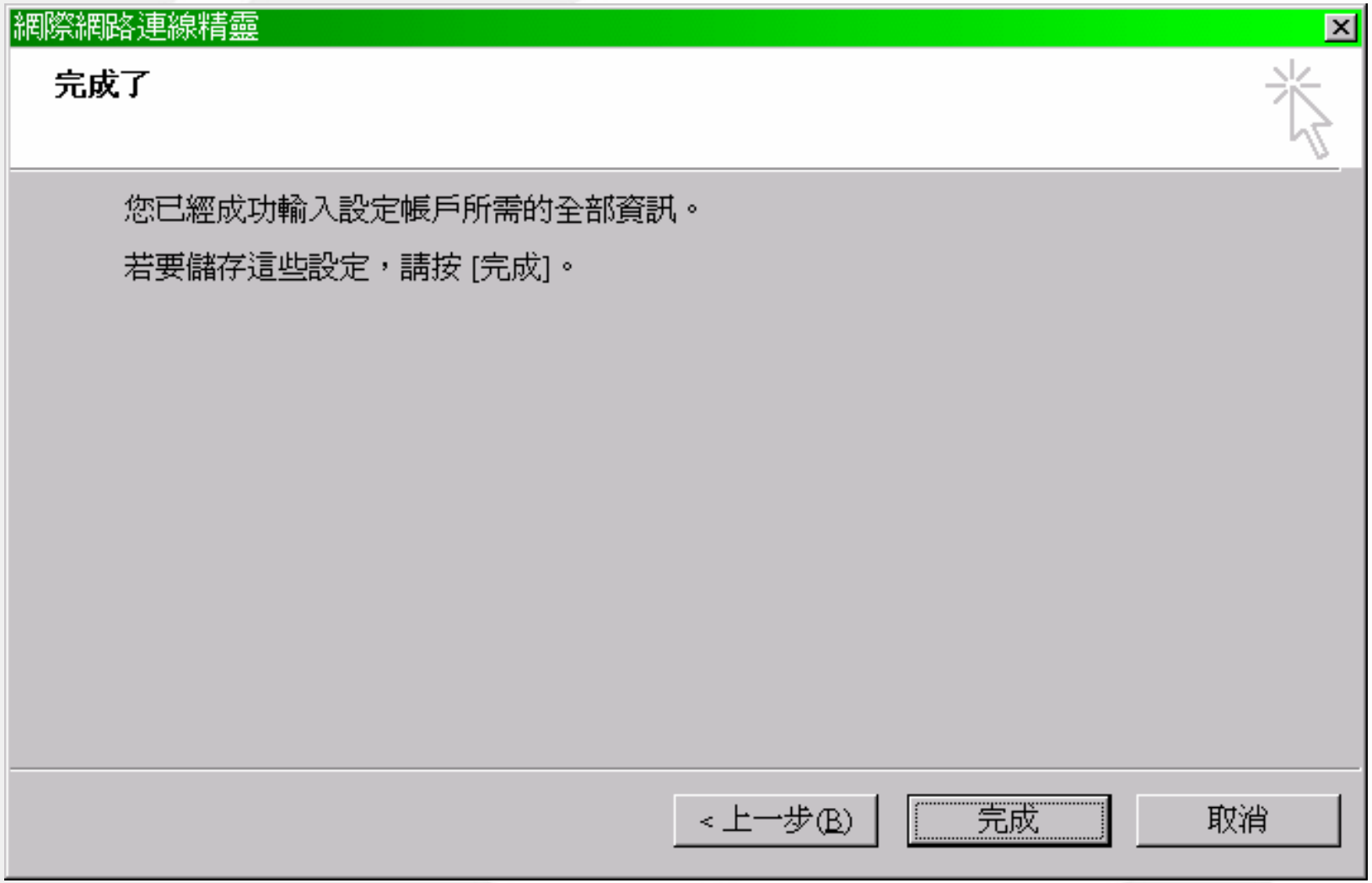
新增新的目錄服務


網際網路帳戶
全部
郵件
新聞
目錄服務
帳戶
類型
連線
140.127.47.87 目錄服務 任何可使用的
Active Directory 目錄服務 區域網路
Bigfoot Internet Dire... 目錄服務 區域網路
InfoSpace Business ... 目錄服務 區域網路
InfoSpace Internet D... 目錄服務 區域網路
VeriSign Internet Di... 目錄服務 區域網路
WhoWhere Internet ... 目錄服務 區域網路
新增(A)
移除(R)
內容(P)
設成預設值(D)
匯入(I)...
匯出(E)...
設定順序(S)...
關閉
郵件(M)...
新聞(N)...
目錄服務(D)...

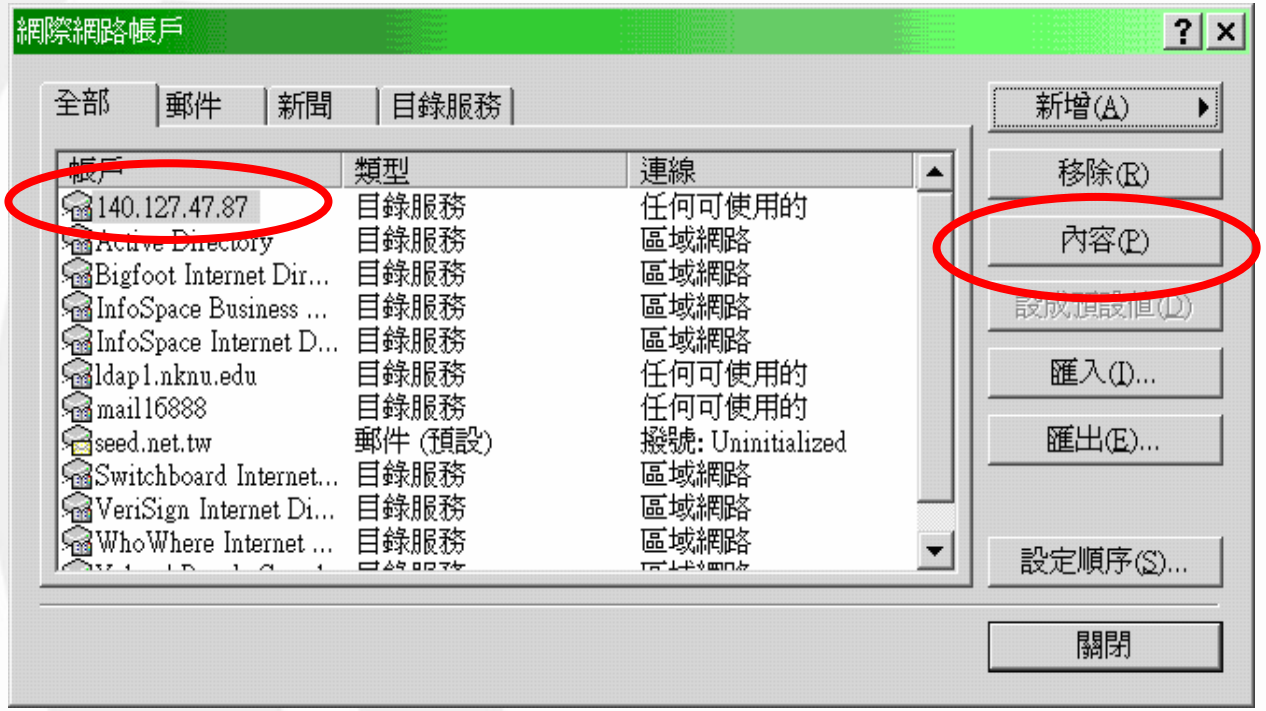
輸入目錄伺服器位址


網際網路連線精靈
網際網路目錄伺服器名稱
請輸入網際網路服務提供者或系統管理員提供給您的網際網路目錄伺服器 (LDAP) 名稱。
網際網路目錄伺服器 - LDAP(I):
140.127.47.87
如果網際網路服務提供者或系統管理員通知您登入 LDAP 伺服器，同時也提供 LDAP 帳戶名稱與密碼，請選擇以下的核取方塊。
我的 LDAP 伺服器要求我登入(L)
< 上一步(B)
下一步(N) >
取消

設定完成



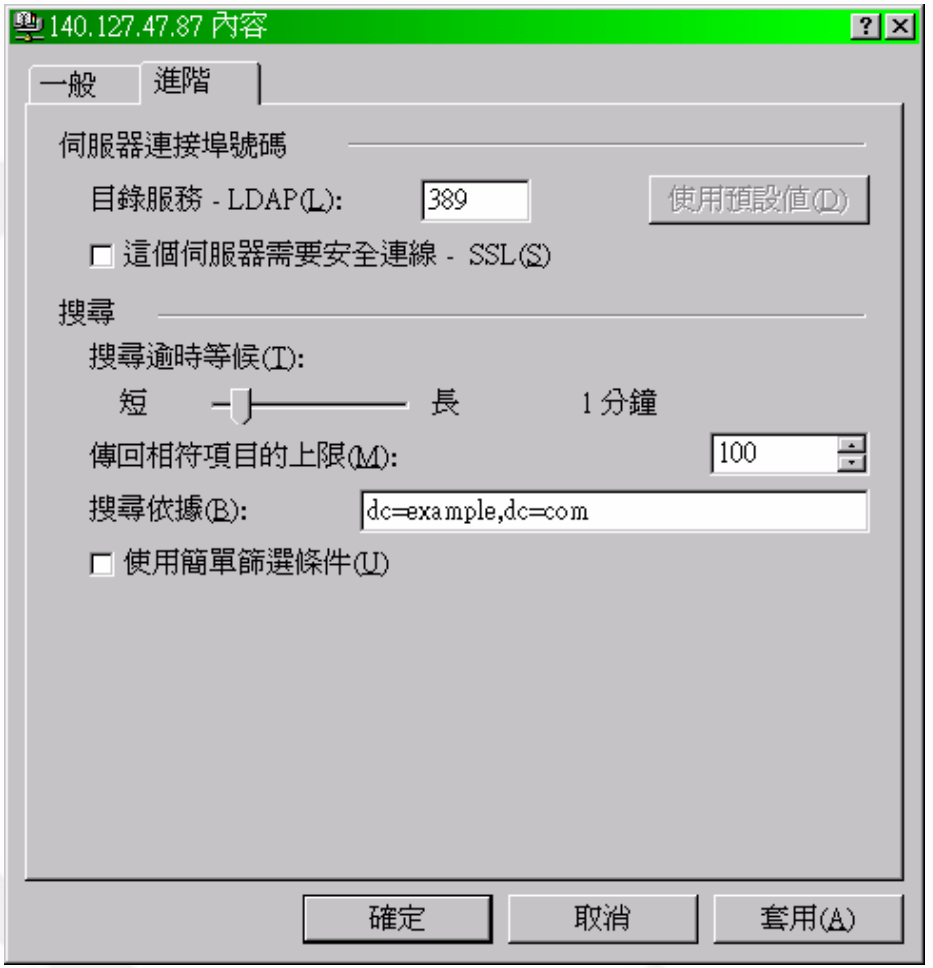
設定目錄服務內容



- 開啓Outlook Express，「工具」==>「帳號」==>「全部」書籤==>點選「140.127.47.87」這個目錄服務==>在點選「內容」，如上圖

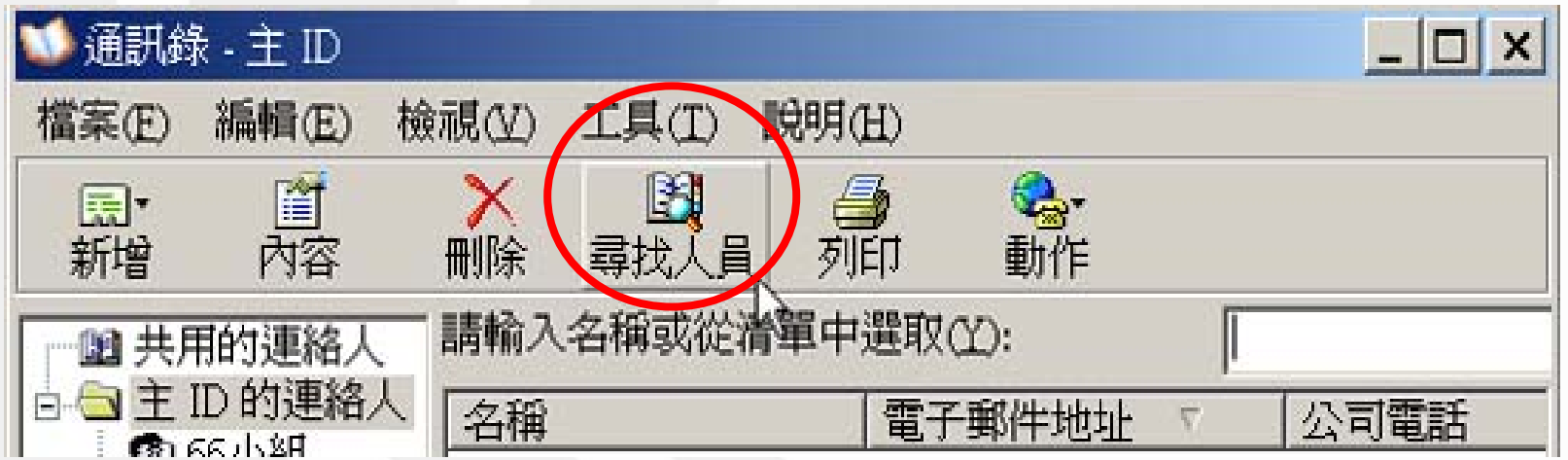
設定搜尋依據

- 點選「內容」後如右圖
- 接著再點選「進階」，於「搜尋依據」的欄位填入「dc=example,dc=com」，最後點選「確定」
- 即完成並可以藉由Outlook來查詢LDAP



以Outlook Express查詢LDAP

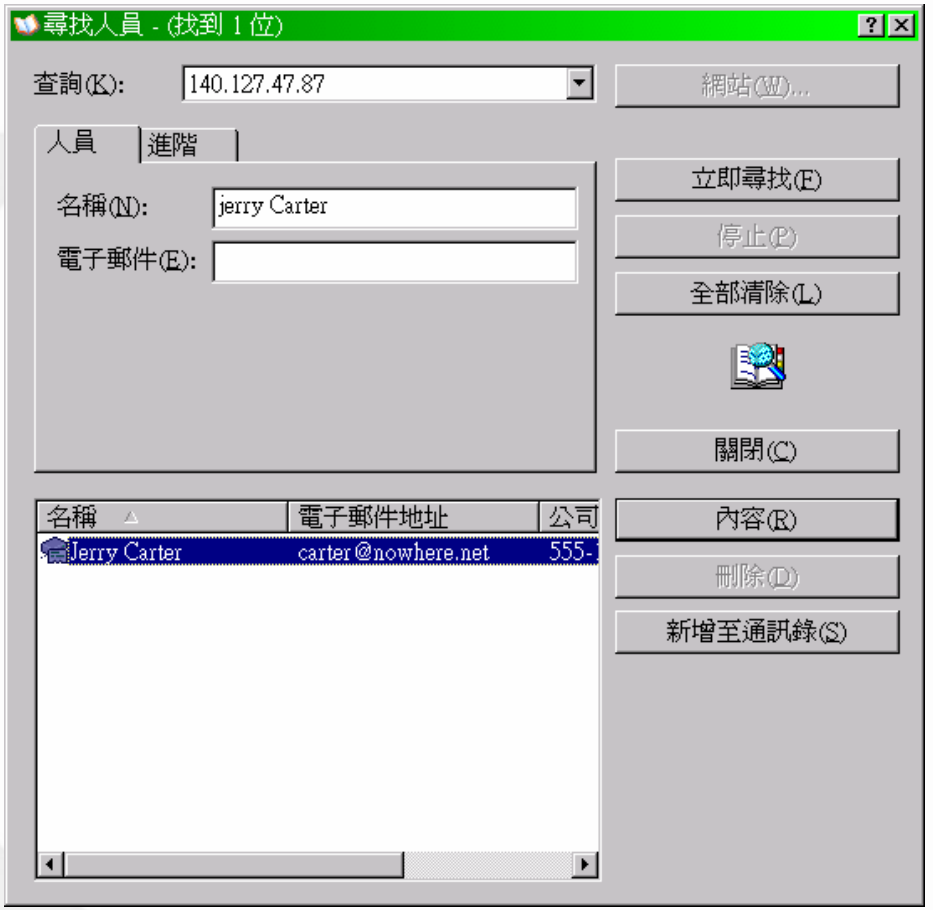
點選通訊錄圖示



點選尋找人員圖示

以Outlook Express查詢LDAP(續)

- 於『查詢(K)』這個地方選取【140.127.47.87】，並且於上方標籤點取【進階】
- 接著於定義條件框中選擇『名稱』、『包含』、且於右方欄位處填入所要查詢的姓名
- 而後先點選下方的「新增」，再點選「立即尋找」，即可以進行搜尋，其點選所搜尋的結果
- 最後點選「內容」即可以進行查看資訊，如右圖



LDAP Browser工具

- Java SDK or Runtime
  - http://java.sun.com/
- LDAP Browser
  - http://www.iit.com/~gawojar/ldap/
- GQ LDAP Client
  - http://biot.com/gq/
- KLDAP
  - http://www.mountpoint.ch/oliver/kldap

參考資料

- Tom Jackiewicz，*Deploying OpenLDAP*，Apress，2004
- Gerald Carter，*LDAP System Administration*，O'Reilly，2003
- OpenLDAP Project，*OpenLDAP 2.2 Administrator's Guide*，http://www.openldap.org
- Softerra，LDAP Browser 2.6，http://www.ldapbrowser.com/