異質平台 Linux 伺服器整合至 Windows NT/AD 網域進行單一簽入之研究：以郵件服務為例

內政部國土測繪中心自行研究報告

中華民國 99 年 10 月

099301000100G2001

異質平台 Linux 伺服器整合至 Windows NT/AD 網域進行單一簽入之研究：以郵件服務為例

研 究 人 員

測繪資訊課 技　士　傅 俊 淇

測繪資訊課 技　正　胡 征 懷

測繪資訊課 課　長　李 旭 志

中　心　主　任　林 燕 山

內政部國土測繪中心自行研究報告

中華民國 99 年 10 月

MINISTRY OF THE INTERIOR

RESEARCH PROJECT REPORT

The Research of Single Sign-On between Different Platforms: Linux Integrated to Windows NT/AD Domain in Mail Service

By

Fu,Chun-Chi

Hu,Cheng-Huai

Lee,Hsu-Chih

Lin,Yen-Shan

October, 2010

異質平台 Linux 伺服器整合至 Windows NT/AD 網域進行單一簽入之研究：以郵件服務為例

摘要

身分識別是諸多應用系統不可或缺的功能，基於資訊環境的多元及複雜出現帳號整合的必要性，而帳號整合具有不同程度的實現。為了優化單一簽入架構，達成高度整合的目標，內政部國土測繪中心(以下簡稱本中心)於 98 年度「綜合行政管理資訊系統增修功能暨維護案」將 LDAP 伺服器自 Sun One Directory 更換為微軟 Active Directory(以下簡稱 AD 網域伺服器)，此項重大系統變更除影響未來系統開發之使用者管理及身分驗證外，亦衝擊部份現行應用系統。

大多數資訊單位選擇運用 Linux 作業系統低成本高穩定性的優點，將其佈署於伺服器端，本中心的 Linux 郵件服務過去由於平台不同，並未整合至單一簽入架構下。當使用者資訊驗證統一改由 AD 網域伺服器執行，於 Linux 作業平台辨識 AD 網域的使用者並完成帳號密碼驗證的問題便無可迴避。本中心的作業環境無異於國內一般辦公機構的資訊配置狀況。故異質平台間進行單一簽入不是個案，而是多數資訊人員會面臨的問題。

本研究將分享本中心單一簽入的作法，並分析採用微軟 AD 網域和其他 LDAP 解決方案在現今資訊作業環境的特點，比較由 AD 網域提供目錄服務在不另行開發程式前提下的 2 種郵件解決方案：微軟 Exchange 伺服器及開放原始碼之差異。結果顯示採用開放原始碼解決方案確可完成異質平台間的單一簽入作業；另廣受採用之 Linux 郵件服務：Postfix(SMTP)、Dovecot(POP)及 OpenWebMail(Web Mail)亦可個別整合單一簽入功能，證明搭配多種開放原始碼解決方案可確保機關在系統規劃時有多元的選擇，並達到經濟實用的目的。

The Research of Single Sign-On between Different Platforms: Linux Integrated to Windows NT/AD Domain in Mail Service

Abstract

Identity authentication is an essential function for various application systems. With the diversity and complication of the information technology environment, there comes the need to integrate different accounts. To optimize the single sign-on infrastructure, National Land Surveying and Mapping Center (hereafter NLSC) replaced the Sun One Directory Server with Microsoft Active Directory Server for LDAP solution in 2009. This significant system change not only affects the user administration and identity authentication of future system development, but also impacts some of the running systems.

Most IT organizations choose to deploy Linux at server side for the advantage of low cost and high stability. However, NLSC's mail service did not integrate into single sign-on framework due to different platform used. Consequently, it is inevitable for Linux platform to identify users from Windows NT/AD Domain and perform identity authentication. As the IT framework of the NLSC is similar to that of other counterparts, single sign-on among different platforms is a common demand of technical staff.

The research shares NLSC's approach to single sign-on and analyzes the features of adopting Windows NT/AD Domain and other LDAP solutions respectively. In addition, the research compares the differences between the two mail solutions, Microsoft Exchange Server and Open Source software, on the premise that AD Domain provides directory services without extra programming.The result shows that Open Source solution can perform single sign-on between different platforms, and that the widely distributed Linux mail services: Postfix (SMTP), Dovecot (POP3) and Open Web Mail (Web Mail), can plug in the single sign-on function individually, which proves that Open Source solutions can ensure institutions not only having multiple choices when developing systems but also saving cost.

目　　次

圖　　目　　次

第一章、前言

第一節、研究動機與目的

鑑於資訊環境的多元化，多系統並存已是常態，特別是人數、單位眾多的辦公環境。依不同單位、使用者與用途，發展建置不同的應用系統或作業平台更是習以為常。多人多系統的電腦環境中，身分識別是相當重要的機制，目前最為通用的機制是帳號加密碼的認證方式。隨著環境的複雜化，便出現帳號整合的必要性。

帳號整合具有以下優點：(施威銘,2002)

- 使用者單一簽入(Single Sign On)：最完美的帳號整合為使用者登入後，除非使用者登出，否則存取其他資源時，系統將自動認證，不會再跳出視窗要求輸入帳號密碼，這樣的整合對於使用者來說最為方便。
- 使用者單一帳號密碼(Single Account/Password)：如果實現單一簽入有困難，退而求其次的目標應是單一帳號與密碼，讓使用者不必記憶太多密碼。而且在某一台電腦上，更改某服務的密碼後，所有其他的電腦與服務皆全部適用新密碼。
- 中央控管所有使用者的資料與設定：除了方便使用者外，管理者也能從帳號整合中得利。因為帳號不是分散在各個電腦或各個服務上，所以新增帳號或更改使用者的帳號資料時，只要在主控電腦上作業即可，不需要四處設定，大大地增進管理上的效率。

以上述特點為目標執行起來可能會有程度上的差異，如：使用者單一簽入是從電腦開機登入開始即納入，或是自使用者登入一入口網才開始；單一帳號密碼是否納入所有應用系統；所有帳號的管理操作是否能由同一中控台進行。由此可見帳號整合具有不同程度的實現。然而在系統架構之初，因為功能和複雜度都未臻一定規模，在有限的開發能量下，通常不會直接採用帳號整合的方式，而是建立各自系統

所需的基本人員資料庫；等到系統眾多、規模漸大，帳號整合的需求相對明確才會著手進行，因此帳號整合多以循序漸進的方式施行。

目前實現單一簽入的選項有 Microsoft Active Dictionary、Sun One Directory Server、OpenLDAP、NIS、Novell eDirectory、IBM Tivoli Directory Server 等，微軟 Active Dictionary 挾 Windows 作業系統的高占有率被廣泛採用，而 OpenLDAP 則由於開放原始碼免費穩定的特性亦佔有一席之地。然而現實中的資訊作業環境絕不似 Linux+OpenLDAP 或者 Windows+Active Directory 如此單調，正因為多元環境的存在，在單一簽入的實現上仍有或多或少的問題點等待克服，使得資訊人員在處理異質平台間的帳號整合時多採取程度不一的折衷作法，如：所有應用系統透過一 LDAP 入口網進行單一簽入，Windows 個人電腦由 AD 網域管理使用者登入，Linux 主機單一帳號密碼、NIS…等。

本研究針對異質平台間的單一簽入為主題，完成所有主機納入集中式管理，自人員新增至人事系統開始，從電腦開機登入到存取各項應用系統及資源的高度整合，並使商業套裝軟體及開放原始碼解決方案達到兼容並蓄的效果，提供資訊人員在委外開發或自行程式設計以外的一個新選項。鑑於國內提供自由軟體或開放原始碼解決方案的服務業並不發達，故以自行研究方式使用開放原始碼解決方案，除可節省公帑購買商用套裝軟體授權、響應行政院研考會推廣使用開放原始碼外，尚能確保機關進行系統架構規劃時可有多元的選擇，避免基於未來相容性及擴充性考量而在當下把即將採購建置的系統向特定產品傾斜。

第二節、研究架構

本論文的第一章在闡述研究的目的與動機，並提出本研究的構想。第二章說明本中心進行帳號整合的演進及分析，如何從多應用系統多主機多使用者走向 AD 網域主機集中式管理，使用者存取應用系統單一帳號密碼，再發展為使用者單一簽入，以及當大多數主機為 Windows 作業系統時，將 LDAP 方案轉換為 Active Directory 具有哪些優點。第三章說明異質平台導入 LDAP 的可能問題，並以 Linux 廣受採用的郵件服務為例，點出：當機關使用開放原始碼的郵件服務(sendmail、postfix 或 dovecot…等套件)時，多是透過一 LDAP 入口網對 Linux 伺服器上的帳號進行密碼同步，無法達到完全單一簽入可能具有的問題。第四章針對以 AD 網域作 LDAP 服務時，可能採用的郵件服務解決方案及成本探討，以及為何不再沿用過去慣用的程式開發方式解決本次需求。在確定採用的技術後，第五章說明透過對 Linux 系統架構的掌握，如何完成異質平台的整合以及使用者帳號密碼認證的原理。並於第六章則詳述實作方式及本研究所使用的套件，如何將 Linux 主機加入 AD 網域並進行帳號整合、如何使郵件服務及 OpenWebMail 整合 AD 認證，以及在機關的 LDAP 入口網將使用者帳號密碼自動帶入 OpenWebMail，省卻使用者自行輸入的程式設計技巧。最後於第六章為本研究作結論並提出幾點建議。

第二章、本中心進行帳號整合的演進及分析

內政部國土測繪中心(以下簡稱本中心)之個人電腦為微軟視窗(Windows)作業系統，伺服器多數為 Windows Server 再搭配少數的 Linux 主機和儲存設備，配置情形無異於國內一般辦公機構。以下介紹本中心進行使用者帳號整合和主機集中化管理的架構及沿革。

第一節、系統沿革

1、AD(Active Directory)網域管理

本中心曾依據93年資訊使用管理稽核改進建議事項於94年辦理架設 AD 網域管理伺服器。當時建立 AD 網域主要目的在於將中心本部及駐外單位為數龐大的個人電腦納入網域以利控管，工作內容計有：將 NLSC(本中心之英文縮寫)網域內之個人電腦及伺服器之 Windows Update 藉由 WSUS 伺服器自動派送安裝系統修補檔，中心之防毒軟體 Trend Micro 結合至網域管理功能統一監控病毒碼、防毒引擎更新狀況及病毒事件通報。除了將電腦納入網域統一控管外，該案亦將本中心組織之單位及人員建立一符合 LDAP 規格之目錄樹，使用者在登入電腦的時候能選擇是否由 AD 網域登入。

2、員工園地：

舊版員工園地當時作為一辦公入口網，使用者可統一以一組帳號密碼由員工園地登入內部各線上系統，各線上系統不自行管理使用者帳號密碼資訊，而是由員工園地維護一組自用的使用者帳號密碼資訊與其他系統共用，透過在員工園地指向各線上系統之網路連結中攜入加密編碼後之使用者資訊以供識別和傳遞(網址;jsessionid=加密編碼參數)，達成偽單一簽入的效果。此架構存在的問題是系統關聯性過高，當員工園地無法正常提供服務，各應用系統無法自行辨識使用者，使用者無法越過它進入由它連結出去的應用系統。另外此架構並不易將已自行發展帳號管理功能的系統納入。

圖 1、舊版員工園地

3、工作儀表板：

於 96 年綜合行政管理系統開發乙案中除開發現行網際差勤、電子表單功能外，尚初步完成單一簽入入口網(工作儀表板)，該案建置一基於 Sun One Directory Server 之 LDAP 伺服器及一對應至本中心組織及人員現況之目錄樹，以期將來作為本中心各線上系統單一簽入之用，使各線上系統不須個別建立並維護使用者帳號密碼資料及登入認證問題。但在人員目錄樹維護方面限制必須使用廠商自行設計之「電子目錄服務管理系統」；舊有員工園地內之各線上系統要與該目錄服務介接進行帳號密碼認證前必須配合修改程式之登入功能，雖然 Sun One Directory Server 亦符合 LDAP 規格，但該案不允許各系統直接連結到 LDAP 伺服器，僅可由廠商提供自行封裝之 JAVA 程式介面透過「電子目錄服務管理系統」進行存取，諸多線上系統的委外廠商反映不易與其採用的開發方式(ASP.NET、PHP)相容；加上 Sun One Directory Server 由於先天限制，無法整合本中心原有之 AD 網域使用者，造成 2 種不同步之目錄樹並存的現象，當人事單位於人事系統上進行人員管理(因應組織再造部門合併、人員調動、新進、退休…

等)，資訊人員必須手動於 AD 網域進行相關設定，否則會因資訊不同步出現組織人員錯置的情形。此作法亦無法解決舊有員工園地系統關聯性過高的問題，反而更加複雜。因為與 LDAP 伺服器介接不易，使舊有的應用系統不易改寫，對於舊有系統只好妥協維持原來員工園地運作的方式，再由員工園地與工作儀表板連結；新系統只能透過 LDAP 廠商提供的程式介面介接，亦非標準的單一簽入作法。當工作儀表板無法正常提供服務，使用者還是無法正常存取應用系統，且與員工園地產生連帶影響不易維護及偵錯；在系統管理、建立備援機制等方面，本中心現有網管及駐點人員所受訓練及技術背景對此較不熟悉，必須協同應用系統負責人及廠商共同維護。

圖 2、LDAP 入口網：工作儀表板

4、工作儀表板 v.2(AD 網域)

鑑於工作儀表板先前運作並不完美，於是著手改善系統架構，加上考量本中心已建置 AD 網域管理伺服器及 AD 目錄樹，且以 AD 作為 LDAP 伺服器相較於其他解決方案，如：OpenLDAP 而言，AD 網域管理伺服器具有容易安裝設定，且提供實作和管理目錄工具的優點，簡化管理及自行設計備份、復原機制的工作；由於本中心現有駐點人員具

有微軟 MCSE 認證，針對以上工作內容足以勝任。故於 98 年度「綜合行政管理資訊系統增修功能暨維護案」將 LDAP 伺服器由 Sun One Directory Server 轉移至 AD 網域管理伺服器，逐步朝目錄樹單一化及降低各系統間關聯性發展。

由於各線上系統要透過 AD 網域管理伺服器進行帳號密碼認證，需依 LDAP 規範修改程式的身分識別功能，另外缺少登入頁面的線上系統必須製作登入頁面供使用者輸入帳號密碼，使系統不必經由工作儀表板或員工園地亦能自行連結 AD 進行認證，降低關聯性。此作法因大部分程式語言皆支援直接呼叫其自有的 LDAP API(如：ASP.NET、PHP、Perl、Java 等)，因此各系統開發廠商可自行規劃完成單一簽入功能，至本年度(99)為止，行政系統已盡數開發完畢。

由於本中心並非所有同仁都配有個人電腦，所以具有 2 種方式(如圖 3)：

1、當使用者以網域帳號登入個人電腦，仍不可直接以該登入身分存取應用系統，必須在 LDAP 入口網輸入 1 次帳號密碼，然後可自由存取其他應用系統；

2、當使用者以本機帳號登入個人電腦或輸入之網域帳號密碼與登入個人電腦之使用者不同，則各系統都會出現帳號密碼登入框供使用者輸入網域帳號密碼再次確認身分，一來確保使用者無誤，二來鼓勵使用者盡量使用 AD 網域登入。

就人事單位使用的人事系統來說，除了內部使用之外，還與人事行政局人事資料庫連接，進行必要的資料交換作業。當中心的 LDAP 目錄樹與內部人事系統連結，完成行政和資訊作業同步，無論是人員的到職、離職、部門調動，欄位內容經人事單位確認再由人事系統同步而來的資訊最具即時性和正確性。雖然 LDAP 支援自訂欄位，但本中心並未在 AD 內擴充額外欄位，一來 AD 預設的個人資訊欄位以足夠

使用，二來不額外擴充欄位確保 AD 的資料庫不致過大影響效率。部份應用系統(如：薪資系統、請假)需要更詳盡的人事資料時，再連結人事系統查詢即可。基本上，經由這次系統架構調整，大致奠定本中心未來系統開發的方向。

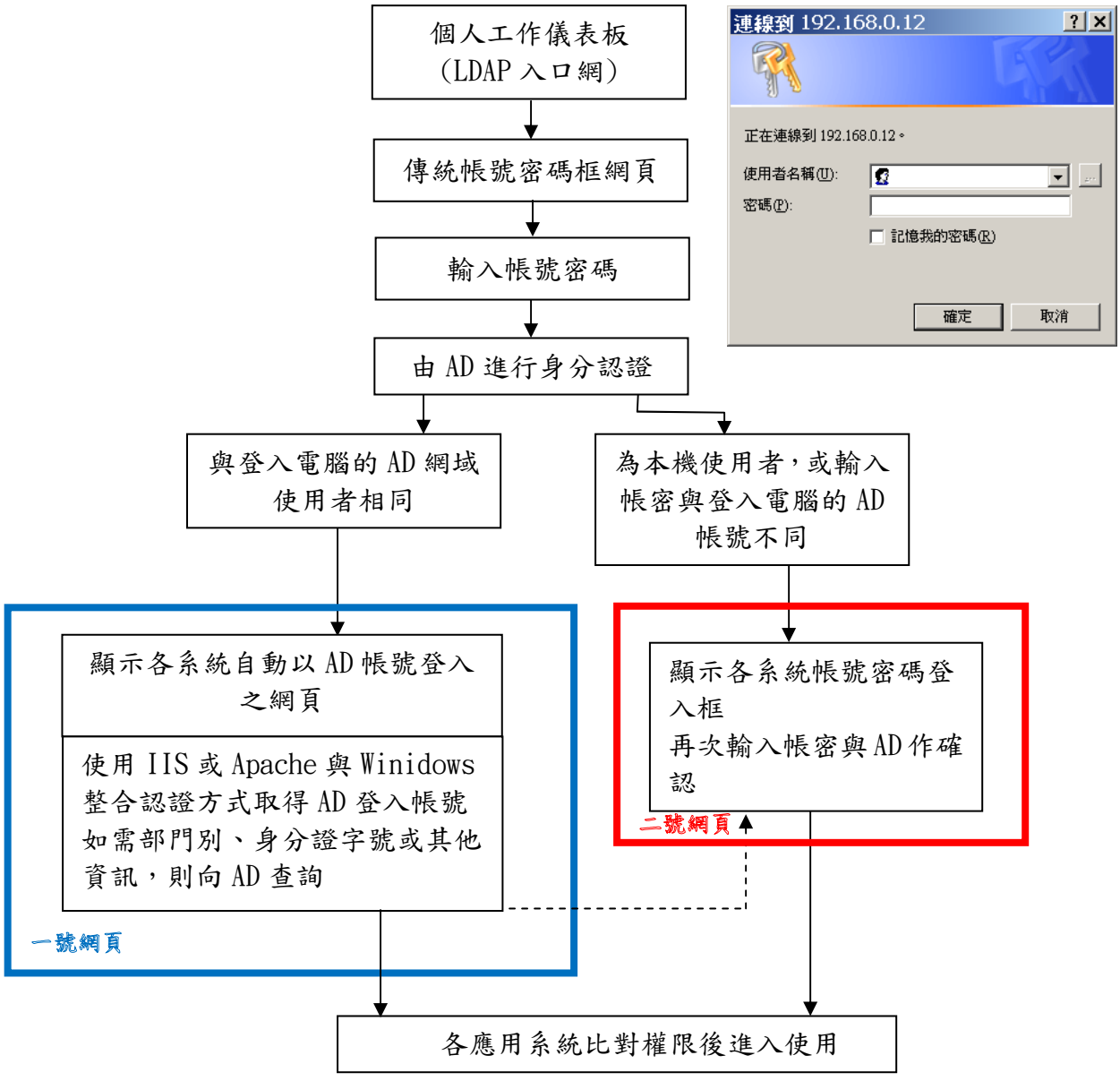


圖 3、LDAP 入口網認證流程

本中心網路由多主機工作群組走向網域集中管理，系統架構由單一帳號密碼走向 LDAP 單一簽入，再合併為單一目錄樹。以下簡述 LDAP 和 AD 網域，並分析為何採用 Active Directory 作為 LDAP 解決方案。

第二節、LDAP 概述

LDAP 衍生自 DAP 的輕型通訊協定，是一種在網際網路採用存取與整合目錄的工業協定，其特色如下：(黃添修,2004)

1、用 LDAP 很容易描述整個資料庫。

2、LDAP 的階層式樹狀架構，每一物件都具其唯一路徑。

3、LDAP 提供的查詢機制讓你可以得到所要的資訊。

4、LDAP 具有驗證的協定，也就是被驗證過的使用者才可以存取的 LDAP 資料。

LDAP 的原始精神與 DNS 的觀念相符，如：http://www.nlsc.gov.tw 是一個站台，而 ldap://o=TV site,c=tw,cn=吳宗憲 是一個人；換言之，以 LDAP 來作目錄服務、帳號管理是相當合適的，如 Outlook 等郵件軟體都支援以 LDAP 作名錄(通訊錄)來進行人員資訊的查詢。

採用真實帳號(Physical User)的優點在於存取系統服務比較直接、設定時相對簡單；缺點是無法讓其他主機在沒有建立該使用者帳號的狀態下使用任何服務；在管理方面，各系統必須自行維護使用者帳號密碼外，也沒辦法靈活的運用系統其他資源來做整合。採用 LDAP 的優點即在於不論甚麼平台，只要有一台主要的 LDAP 伺服器，其他伺服器只要設定正確能夠接收 LDAP 廣播，就能夠立刻上線服務與使用。LDAP 單一簽入架構下只需在 LDAP 伺服器端維護一份使用者資訊，其餘系統皆以虛擬使用者(Virtual User)方式於使用者存取系統資源時在 LDAP 伺服器端完成認證後取得 Sign On Key，各系統不須使用 By Real Account 方式建立帳號。除了讓帳號管理更具彈性，另一個好處是可以使用共通的 LDAP API 開發應用程式，使應用程式與

使用者高度結合。由於資料欄位可以自由擴充，機關可以依自己的需要開發出人事管理系統，而該人事資料又自動成為機關內各種應用系統的成員帳號。並且由於 LDAP API 的標準是公開的，因此不管由哪家廠商來開發都可以彼此相容。

單就使用者便利的觀點簡單切入，單一帳號密碼便已滿足簡單方便的需求；當考量系統管理的觀點，LDAP 可將使用者資訊集中管理，只需維護一份名錄。無論單位內有多少應用系統，皆存取維護同一份使用者(共通)資訊。在使用者資訊具備共通欄位的前提下，發展建置各應用系統時只需自行維護基於應用功能必須另行新增的資料欄位，具有內容一致不矛盾、一處維護多方使用、不重複建置儲存等優點；使用者資訊集中管理的另一個好處是單一的帳號密碼認證過程，各應用系統可以在開發時採取一致的作法，避免各立山頭；同時較容易檢討系統安全性及修改架構，減少系統建置和後續維護的成本。由此可見，建置 LDAP 是一項值得進行的長期投資。

第三節、Active Directory 網域概述

Windows 網路中的「網域」，是指一群電腦透過一台或多台伺服器進行帳號整合和權限控制的集中管理。採用分散式架構儲存使用者帳戶、群組、電腦、印表機…等物件，而 Active Directory 正是 Windows 網域內負責提供目錄服務的元件，負責管理與驗證存取動作、資料儲存、安全模式及信任資訊。採用 AD 來進行網域管理的工作，最大的效益在於帳號管理和電腦管理的機制。

1、帳號管理

使用者帳號（User Account）的種類可分做 2 類，第 1 類為本機使用者帳戶(Local User Account)：只能在單機使用的帳號，這個帳號無法用來登入其他電腦，除非是網域中有一帳號和密碼和本機使用者相同。第 2 類為網域使用者帳戶(Domain User Account)：為建立在網域控制器伺服器 (DC)的帳號，可以用來登入網域中的可信任電腦，並可存取網域中的資源（共享檔案、印表機…等）。目前 AD 網域的帳號管理是將 SAM 資料庫當後端，以 LDAP 通訊協定當前端提供帳號認證功能，當使用者登入網域時，就使用 Kerberos 通訊協定來傳遞密碼，密碼則使用安全性較高的 MD5 演算法來加密，其結構如下圖：

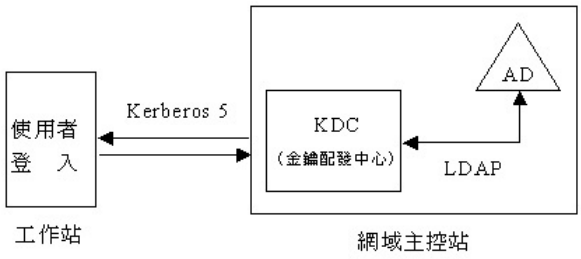


圖 4、Kerberos 通訊協定

2、電腦管理

電腦管理的問題可以分成兩方面來探討，一是電腦名稱辨識的問題，一是網域成員認證的問題。

在 AD 網域內的所有成員電腦，其名稱一律沿襲 DNS 命名法，當

某台工作站要求加入到網域內作為成員時，會透過 DNS 伺服器中的 SRV 紀錄找到網域主控站，網域主控站會為這台工作站建立一個電腦帳號(在 AD 網域中帳號區分為使用者帳號、電腦帳號和服務帳號三種)並產生 SID，然後由金鑰配發中心(KDC)配發憑證(金鑰)，SID 及憑證會儲存於網域成員電腦的系統登錄裡面，像這樣經過網域主控站認證的電腦，我們可以將它稱為「可信任電腦」。

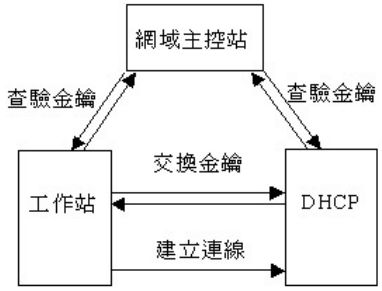


圖 5、Kerberos 雙向認證

在網域成員認證上，Windows 採用 Kerberos 5 來進行雙向認證，在使用者登入前，伺服器與工作站先交換金鑰，並向 KDC 查驗是否正確，網域主控站可藉此來決定該使用者是否有權登入該主機，如果發現該使用者有登入權限，接著再以 LDAP 向 AD 查驗帳號密碼。並且由於 Kerberos 和 LDAP 是 TCP/IP 上的標準，其他平台如 Solaris、Linux、FreeBSD…等都可透過 AD 網域帳號來進行登入。(李忠憲,2005)

第四節、為何選用 Active Directory 網域作為 LDAP？

使用者單一簽入的最完美境界堪稱是自使用者登入後，除非其登出，否則存取其他資源時，系統將自動認證，不再要求驗證帳號密碼，唯單一簽入的實施有程度上的不同。真正高度整合的單一簽入應整合所有應用系統，當然也包含人事單位的人事系統與人事資料庫(即 LDAP 目錄樹可以反映組織結構及人事資料)。當新進人員完成報到手續，由人事單位登載該員資料於人事系統的同時，該員亦新增至 LDAP 目錄樹，於是自動完成初始化動作並於各應用系統設定其相應的權限，如此新進人員可立即使用辦公所需的應用系統。同理可得，當離職人員辦理離職，該員會被停止應用系統的使用，直到完成離職手續後由人事單位確認，再自 LDAP 目錄樹刪除。過去新進人員報到的到職單裡多少有資訊單位應用系統管理人的會章，需由各應用系統負責人進行帳號開通和初始密碼設定，再由新進人員登入系統自行變更密碼，由此例可見系統高度整合單一簽入後帶來簡化報到程序的便利。

使用 AD 網域作為 LDAP 的解決方案具有從電腦開機就單一簽入的優勢，因為 AD 網域不單可以進行使用者帳號管理更結合電腦管理功能，何人可登入電腦、存取資料夾或遠端連線都可由 AD 網域進行限制，許多商業套裝軟體亦支援針對 AD 網域作細部權限設定及帳號密碼驗證。當機關導入 ISMS(Information Security Management System，資訊安全管理系統)時，可利用 WSUS(Windows Server Update Service)對網域內主機派送系統修正檔，亦可於 AD 網域直接佈署安全性原則以控管密碼的有效日期、長度、複雜度、容錯次數等條件以符合 ISMS 政策目標，對系統管理者而言，AD 網域較容易達到中央控管--將人和機器一併管理的目標，再進一步與其他行政系統高度整合，則全機關只具有單一目錄樹。AD 網域能發揮以上特點，主要原因是作業系統容易整合，而 Windows 作業系統擁有的高度市占率使多數商業套裝軟體主動支援其架構，並非微軟技術較為先進，這只算是

採用微軟自家技術帶來的某種便利。

除了 Microsoft Active Dictionary 和 Sun One Directory Server，目前較具規模的單一簽入解決方案計有 OpenLDAP、NIS、Novell eDirectory、IBM Tivoli Directory Server 等，但 NIS 只適用於 Unix 系統不符合單位需求。一般的 LDAP 解決方案多專注於組織及人員目錄樹管理並供其他系統介接，目錄服務無法直接納入電腦主機控管或必須與其他套裝軟體配合，以電腦開機登入時進行單一簽入為例，其他 LDAP 系統必須在各部電腦主機上安裝登入驗證軟體於開機時執行，有更多單位的單一簽入作法是建置一入口網頁，由使用者登入 LDAP 入口網連結出去的應用系統才進行單一簽入。過去本中心亦採用上述作法，LDAP 入口網及其他行政系統使用某一目錄服務，電腦主機、防毒等套裝軟體則結合 AD 網域管理(也不見得能交由其他 LDAP 管理)，於是存在 2 個各自獨立的目錄樹，當人員在部門或駐外單位調動，AD 網域和另一結合人事系統的 LDAP 目錄樹便出現不一致，造成人員權限控管或應用系統使用上的異常。

分析至此，並非對 Windows 存在任何偏好，只是當機關內的電腦主機在作業系統上存在如此懸殊的差距時，採用微軟的 AD 網域技術來進行 LDAP 單一簽入能夠在系統整合上較為緊密，減少一些額外工作。

第三章、異質平台導入 LDAP 可能問題及解決方案

第一節、異質平台導入 LDAP 可能問題

轉換由 AD 網域認證對機關的影響：以郵件服務為例

以本中心為例，自 98 年度「綜合行政管理資訊系統增修功能暨維護案」執行完畢後改採 AD 網域伺服器進行 LDAP 認證，各行政系統迄今亦盡數完成與 AD 網域介接工作，達成組織單一目錄樹的目標。儘管轉換過程尚屬順利，但受影響的是不屬於客製化應用系統及商業套裝軟體的郵件服務。

本中心原來的郵件伺服器運作方式為：在主機內以員工編號作為帳號編定依據以建立個別本機使用者，此型態之使用者屬於實體本機使用者，於伺服器內儲存個別帳號密碼，故使用者於收發郵件時必須在郵件伺服器端進行帳號密碼認證，使用 WebMail 的人員則由委外開發的網路郵局對伺服器進行郵件存取。此架構存在郵件伺服器端密碼與內部入口網密碼不同步問題。過去的內部入口網由廠商另行開發程式修改郵件伺服器端密碼(/etc/passwd)達到單一帳號密碼，此模式必須在郵件伺服器端建立排程定時執行批次更新，當密碼修改時，必須等待至排程執行完畢新密碼才會作用。更麻煩的問題是辦理新進人員，雖然在 LDAP 目錄樹完成新增人員，由於郵件服務未連結 LDAP 目錄，必須由機房駐點人員手動於郵件伺服器端建立新進人員收發郵件之帳號及密碼，無法完成無縫作業。

在轉換使用 AD 網域認證後，當使用者於內部入口網或個人電腦端變更密碼，原來內部入口網更改郵件伺服端密碼的功能失效，無法同步更新至郵件伺服器端之密碼，造成同仁無論使用 Outlook 等郵件軟體或使用網路郵局皆無法收發郵件問題，必須由機房人員進行終端機登入，以人工作業方式為同仁設定密碼或由委由廠商再次開發程式

進行帳號密碼同步。雖然大部分同仁的習慣是在 Outlook 等郵件軟體內設定一次密碼就不再更動，因此使用上衝擊不大，但鑑於本中心 ISMS 政策必須定期更換密碼的規定，使用電子郵件的人數眾多，但密碼原則與政策規定脫勾，實可列為不符合事項；另外網路郵局無法正常運行，未配有個人電腦的同仁無法正常收發郵件甚感不便。

大多數機關選擇運用 Linux 作業系統低成本高穩定性的優點，將其佈署於伺服器端，尤其是作為郵件伺服器的解決方案，這是目前少數 Linux 平台佔有率高於 Windows 的項目。雖然大部分使用者位於 Windows 作業平台，但是收發電子郵件卻是日常工作，當使用者身分驗證統一改由 AD 網域伺服器執行，於 Linux 作業平台辨識 AD 網域的使用者並進行帳號密碼驗證的問題便無可迴避。本中心的作業環境無異於國內一般辦公機構的資訊配置狀況，具有一定的代表性。故異質平台間進行單一簽入不是個案，而是多數機關會面臨的問題。

第二節、解決方案及分析

在尋找解決上述異質平台整合單一簽入問題可能解決方案的過程中，軟體銷售人員會建議符合需求的產品、系統開發廠商會建議開發程式，唯國內提供自由軟體或開放原始碼解決方案的服務業並不發達，以致選擇上不夠多樣化。本中心過去亦慣於委外或自行開發程式解決相關資訊問題，優點是客製化程度高、容易滿足使用者需求。但本次問題核心為單一簽入之帳號密碼認證，並非機關內部資訊系統有任何需要高度客製化之特殊需求。單一簽入在 IT 界早已存在許多成熟的解決方案，實不宜另行藉程式設計另闢途徑強達目的。應分析現況以採用普及性高且符合業界標準的單一簽入系統架構，方可避免日後需求改變或系統架構面臨調整時，緊接而來的自行開發或委外的程式設計工作。

另考量本中心多數主機為 Windows 作業系統、AD 網域已於早年建置完畢且多數使用者皆習以網域帳號密碼登入個人電腦的前提下，選擇採用微軟 AD 網域管理伺服器進行單一簽入，不去改變多數使用者目前的電腦使用方式應是成本最低的作法，故在此資訊配置環境的前提下，暫不考量其他的 LDAP 方案。

一、建置微軟 Exchange 伺服器：

Exchange 伺服器是微軟公司的郵件伺服器解決方案，不需安裝其他軟體即可納入 AD 網域管理並使用 AD 網域管理認證機制，具強大企業級商務通訊功能並易於管理及備援、支援叢集(Cluster)和高可用性(High Availabilty)架構、且專業管理人才較多、亦不乏微軟 Exchange 管理維護訓練課程；但授權金額高昂不易負擔。以下為建置 Exchange 伺服器所需費用試算，產品金額依據 98 年台灣銀行共同供應契約契約價(含稅)並設定以購足本中心員工數(約 650 人)所需授權計算。

Windows 2008 Server 64bits + Exchange 標準版 + 標準版用戶端存取授權

19187+19524+1879×650(人)=1260,061 元

Windows 2008 Server 64bits + Exchange 企業版 + 企業版用戶端存取授權(需先擁有標準版用戶端存取授權)

19187+106346+(1879+961)×650(人)=1971,533 元

二、進行Linux、Windows異質平台整合

本中心現行郵件伺服器為 Linux 系統，使用開放原始碼軟體Postfix、Dovecot提供郵件收發之SMTP、POP3服務，採用開放原始碼的解決方案的優點是軟體費用低廉(免費)，缺點是缺乏專業人才、進階應用之參考文件，將本案需求洽詢軟體開發、主機維護等廠商後，皆表示僅使用Linux郵件伺服器作一般電子郵件收發，未涵蓋異質平台(Windows、Linux)整合單一簽入部分。雖然目前國內使用狀況尚未普及，但由自行蒐集之部分文件顯示此方式確實可行。另外由於本中心同仁並未每人都配有個人電腦，所以部分同仁無法且不適合在特定電腦上以 Outlook Express 等 POP3 郵件軟體收發信件，Linux系統的郵件伺服器不似微軟 Exchange 伺服器已內建功能完整的WebMail，必須另行建置一支援單一簽入功能之 WebMail，若能克服以上問題，則吾人仍可使用免費穩定的開放原始碼解決方案。

一般而言，開放原始碼陣營及微軟等商業軟體公司在為使用者進行成本分析時，多使用整體擁有成本(Total Cost of Ownership,TCO)(註)為指標分析並強調該方解決方案確實具有優勢。撇除雙方各自撰述的報告論點，以下試採用整體擁有成本的觀念，以資訊系統規劃者的角度來分析以上解決方案的特點：由於微軟

Windows 作業系統在一般使用者的桌面環境擁有極高的佔有率，且微軟為 Windows 作業系統提供 AD 網域技術進行集中化管理及單一簽入，當一個單位要集中管理轄下眾多的 Windows 個人電腦時，建立 Windows 的 AD 網域是很自然而然的選擇。更因為微軟官方文件充足、相關教育訓練課程多、Windows 伺服器之管理及設定較為方便簡單，在作業系統漏洞修補上，搭配 WSUS 或 Windows Update 都較容易處理，加上大量第三方廠商在客製應用系統開發及套裝軟體的支援(如：本中心使用的防毒軟體就支援網域派送更新病毒碼，虛擬化管理軟體及安全防護工具亦支援 AD 認證，方便系統管理)，無論將來系統由委外駐點廠商或內部資訊人員來管理，在後續功能擴充及管理維護上，採用微軟解決方案能得到較可預期的後果(無論金錢上或其他因素)，這也是一般人在採用微軟產品時的考量。Linux 或開放原始碼的支持陣營在計算成本時常使用一個極具宣傳效果的字眼「免費」來概括，軟體零成本不代表使用零成本，零成本的前提是使用者能自力解決所有問題。可見在選擇方案的時候，所需金額或第一時間的建置成本並不是唯一的考量，後續的管理維護和功能擴充需一併探討。所以採用開放原始碼的成本優勢不宜過度誇大，而評估其他商業產品也不宜完全著重在金額，這個問題永遠沒有標準答案，甚至因人而異，是以資訊人員在規劃系統架構時宜多方蒐集資料並深入思考。

客觀而言，以微軟 Exchange Server 作為郵件伺服器與現行 AD 網域認證架構最具完整性，功能強大又內建 WebMail 功能，但考量本中心對於 Exchange 伺服器的諸多延伸商務功能目前尚無迫切需求且未編列大筆預算以供支用並亟於解決問題，故決計採方案二以自行研究方式利用現有硬體設備完成郵件系統移轉。

三、異質平台整合進行單一簽入的實現

異質平台整合進行單一簽入--建立一可加入微軟 Active Directory 網域之全新 Linux 伺服器提供電子郵件服務，伺服器內除

了系統管理用途所需之必要帳號(如：root)為實體使用者外，其他之一般使用者全數為虛擬使用者，並統一交由 AD 網域管理伺服器管理帳號密碼。在使用者進行 POP3 收信登入、SMTP 寄信以及使用 WebMail 時統一由 AD 網域管理伺服器進行認證，打造出全辦公環境內之資訊系統自使用者電腦開機登入開始即為單一帳號密碼、電腦主機及人員單一目錄樹、目錄服務伺服器端真正只維護一份使用者資訊之高度整合的單一簽入。

註、整體擁有成本(Total Cost of Ownership,TCO)：使用某一 IT 產品的成本，其成本計算包含所使用的軟硬體、維護/升級、內部員工訓練、以及提供技術支援的顧問等。主要是提供消費者或企業經理人在作採購時，評估某項 IT 產品的效益，以及直接、間接成本。最後所呈現的數據可反應加入各種因素後的實際採購成本。
(from CNET 字彙寶典
http://taiwan.cnet.com/enterprise/glossary/term/0,2000062921,2000055216,00.htm)

第四章、Linux、Windows 異質平台整合

將 Linux 伺服器整合到 NT/AD 網域，使 Linux 伺服器能識別 NT/AD 網域使用者，並交由 AD 網域管理伺服器進行帳號密碼認證。由於微軟 Windows 作業系統屬於封閉式作業系統，不易由外部修改系統功能，所以比較務實的作法是由開放原始碼的 Linux 系統著手，讓原先由 Linux 主機本地端控制的帳號認證機制，轉向 NT/AD 網域尋求認證，所需使用的技術如下：

一、Samba Winbind 整合： Samba 是一個符合 SMB/CIFS 協定以提供檔案及列印共享服務的開放原始碼解決方案，Winbind 則是 Samba 中用以解決的統一登入問題的元件。藉由於 Unix Like 系統端自行實作微軟 RPC 呼叫技術的方式，結合 PAM 及 NSS 模組使 Windows NT/AD 網域使用者得以如 Linux 系統本機使用者般地存取、操作 Linux 伺服器上的服務。Winbind 並具有一 winbind_idmap.tdb 資料庫，維護非 UNIX Like 系統本地端使用者的 UID、GID 與 NT SID 的對映關係。

二、PAM (Pluggable Authentication Module)：Linux 作業系統上具有一可抽換認證模組。這是個單一窗口的認證機制，所有程式只需要依循相關的規格，撰寫與 PAM 溝通的機制，其他後端的細部工作則全部由 PAM 負責。以下為 PAM 機制的示意圖(引用自「Linux 與 Windows 異質平台整合方案」，13-5)：

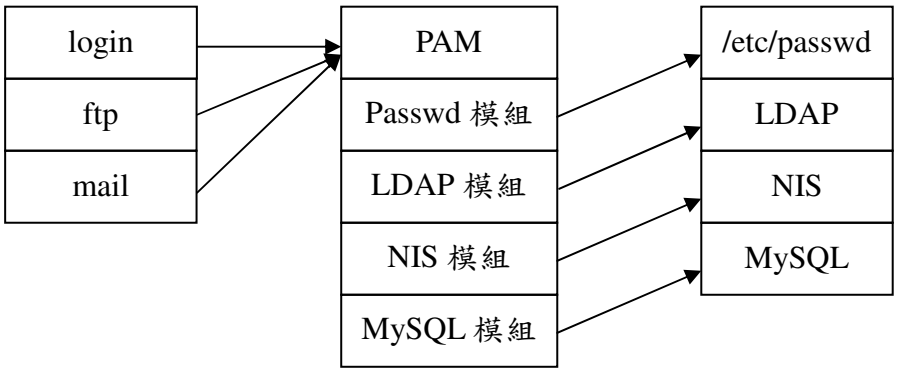


圖 6、PAM 機制示意圖

由上圖可以瞭解，當系統使用 PAM 時，只要新增一個 PAM 模組，便可以讓相容 PAM 的程式改用不同的認證機制。所以我們也可經由一個能與 NT/AD 網域溝通的 PAM 模組，達成使用 NT/AD 網域帳號的目的。

三、NSS(Name Service Switch)：NSS 被大量使用於 Unix 系統中，用於使系統解析出自不同來源的主機名稱(hostname)、郵件別名(mail alias)、使用者。當設定完成 NSS LDAP-based 功能，雖然 PAM 函式庫尚未安裝，只要完成 Winbind 服務，並且讓系統的 NSS 使用 Winbind 的 NSS 函式庫，就可以使系統辨識 AD 網域的帳號。

四、Kerberos：Kerberos 是一個網路驗證協定，使用秘密金鑰的加密技術(secret-key)，為用戶端-伺服器的應用程式提供安全驗證的服務，用戶端和伺服器使用 Kerberos 證明身分之後，可以對所有通訊進行加密，以保證資料的隱私性和完整性。由於 Windows Server 2003 的 AD 採用 Kerberos 認證機制，因此必須安裝設定 Kerberos 以便和 AD 溝通。

圖 7 表示 LDAP、Linux Posix 帳號、Samba 帳號間的關係(引用自「Samba-3 by example:pratical exercise to successful deployment」，5-11)。此處的 LDAP 系統雖為 Linux 端的 OpenLDAP，但仍可幫助我們理解在不同帳號系統間建立映像資訊的觀念。圖中表示對 Unix 系統帳號和 Samba 來說，LDAP 是身分識別管理目錄伺服器；從 LDAP 的觀點來說，Unix 系統帳號是以 POSIX 擴充綱要儲存的。Samba 在儲存帳號的時候具有自己的 schema。Samba-3 可以用 LDAP 的後端來儲存：Windows 網路使用者帳號、Windows NT 群組帳號、Unix 群組和 Windows NT 群組之間的映像資訊、從 SID 到 UID 的 ID 映像資訊。

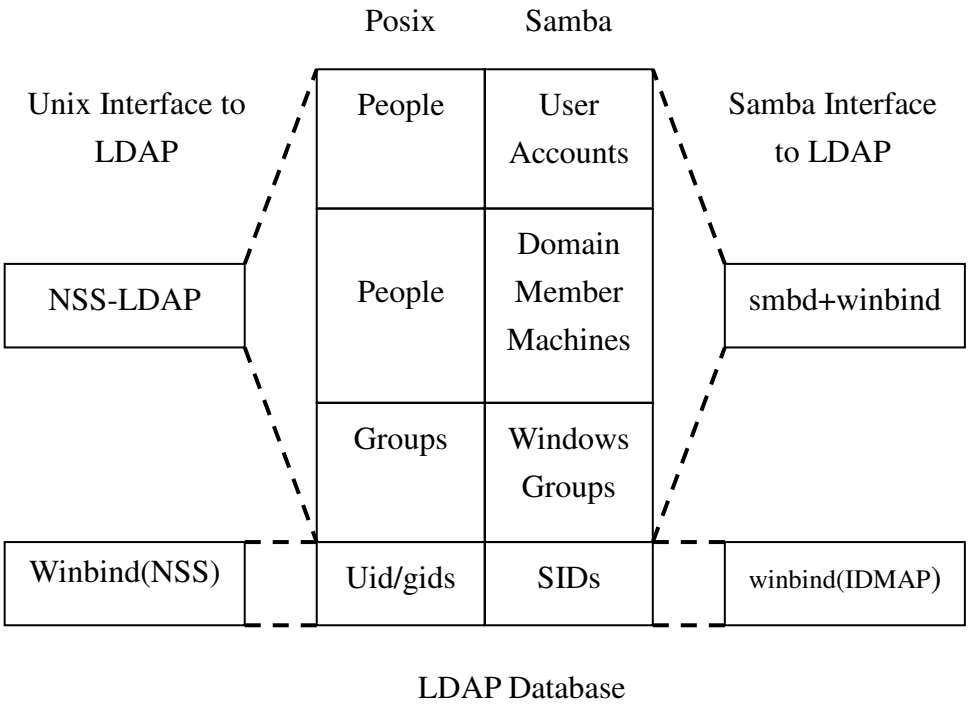


圖 7：LDAP、Linux Posix 帳號、Samba 帳號間的關係

圖 8 為 Samba 驗證後端搜尋路徑(引用自「Samba-3 by example:pratical exercise to successful deployment」，6-10)，該圖說明了 Samba-3 能夠使用多種密碼(身分識別和身分解析)後端。圖中表示 Samba 如何使用 Winbind、LDAP、NIS 或傳統的系統密碼資料庫。此處的 LDAP 系統為 Linux 端的 OpenLDAP，本中心所使用的 AD 網域表示於圖右上角之 NT 4 Domain。這張關係圖顯示了身分識別和身分解析的機制(獲取 Unix 的 UID/GID)。

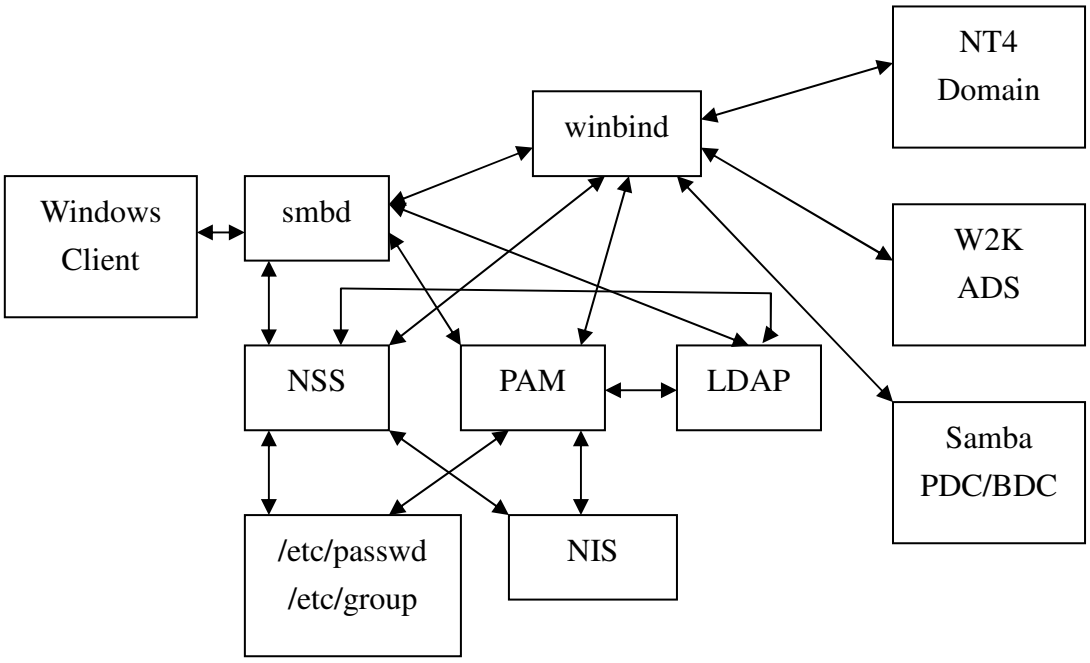


圖 8：Samba 驗證後端搜尋

圖 9 為 Winbind 運作示意圖(引用自「Linux 與 Windows 異質平台整合方案」，14-2)，圖中顯示 Winbind 運作需要 3 個元件：NSS 函式庫、PAM 函式庫、Winbind 服務程序。當在 NSS 設定檔中設定使用 Winbind 時，系統便會尋找這個函式庫，要求處理帳號的收集。PAM 函式庫讓 Linux 系統在傳統的/etc/passwd 認證機制外，也可以向 NT/AD 網域要求帳號與密碼的認證，達成使用 NT/AD 網域帳號的目的。Winbind 服務程序則是負責接收 NSS 與 PAM 函式庫的需求，使用微軟遠端程序呼叫(RPC)與 NT 網域溝通，自版本 3.0 之後也能使用 LDAP 與 AD 溝通，解決不同系統間的溝通問題。此外 Winbindd 服務程序也有一個自己的資料庫，儲存 NT/AD 網域與 Linux 系統帳號間的對應(即圖 4 所示的映像資訊)，以解決帳號資料庫格式不一致的問題。

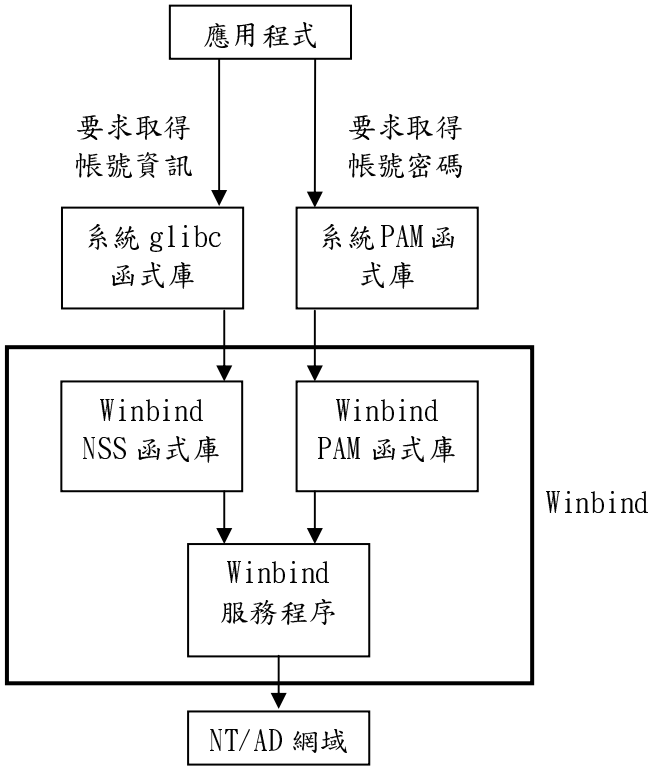


圖 9、Winbind 運作機制示意圖

本研究主題為異質平台整合單一簽入，設定以 Linux 主機加入 Windows 網域，並以郵件伺服器為實作目標；因為 Linux 平台大多作為伺服器用途，以 sendmail 或 postfix 作郵件伺服器更是最常見的應用，微軟 Windows 平台則在一般使用者的桌面環境擁有極高的比例，可見此架構合理可行。當 Linux 郵件伺服器加入 Windows AD 網域內，並可識別出 Windows AD 網域內之使用者，透過 Kerberos 加密與 AD 網域管理伺服器連線及 PAM 模組進行驗證，則使用者自然可以透過 AD 網域帳號密碼成功登入郵件伺服器內收發電子郵件，達到不被限制採用微軟特定產品或另行開發程式介接，確保機關進行系統架構規劃時可有多元的選擇，避免基於未來相容性及擴充性考量而在當下把即將採購建置的系統向特定產品傾斜。

第五章、實作方式

本研究之作業原理已由上述篇幅說明完畢，接下來是實作的部分。實際測試以現行之 AD 網域管理伺服器搭配以虛擬化技術建立的 Linux 郵件虛擬主機。虛擬化技術具有快速回復(Snapshot)、支援高可用性(High Availability)及叢集式架構(Cluster)、資源動態配置(Distributed Resource Scheduler,DRS)等特性，若日後系統負載倍增，易於調整結構。本研究 Vmware 虛擬化軟體建立 Cent OS 5.5 之虛擬 Linux 伺服器，實作步驟及環境參數如下：

實驗網域名稱	lab.gov.tw
Linux 主機名稱	Mail.lab.gov.tw
AD 網域管理伺服器 IP	10.10.10.1
AD 網域管理伺服器名稱	adserver.lab.gov.tw
AD 使用者帳號	aduser
Wins server(同 AD 主機)	10.10.10.1

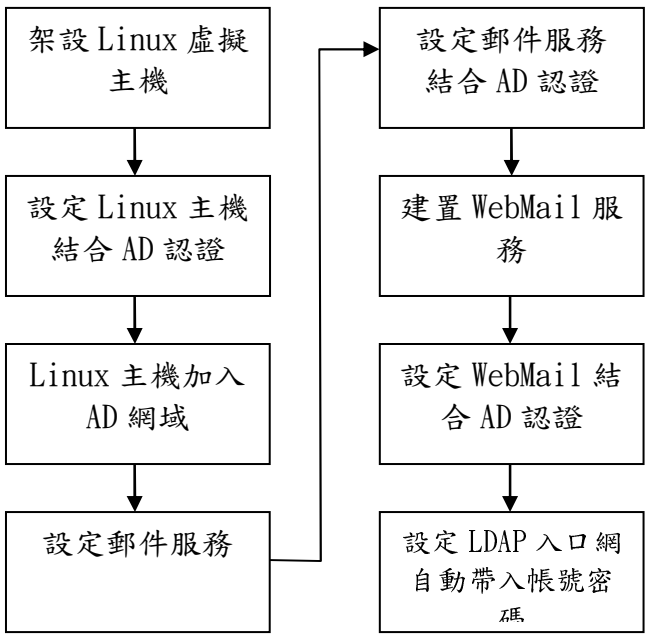


圖 10、實作流程圖

所需套件列表	
samba samba-client samba-common	httpd mod_perl postfix dovecot
nss pkinit-nss nss_ldap nss_db krb5-auth-dialog krb5-libs krb5-server krb5-workstation	pam pam_ccreds pam_krb5 pam_passwdqc pam_pkcs pam_smb passwd
perl-suidperl perl-Text-Iconv perl-Authen-Krb5 perl-Authen-Krb5-Admin perl-Authen-NTLM perl-Authen-PAM perl-Authen-Smb	選擇性安裝 perl-Compress-Zlib perl-IO-Socket-SSL perl-IO-Zlib perl-LDAP perl-libwww-perl perl-Net-SSLeay openssl

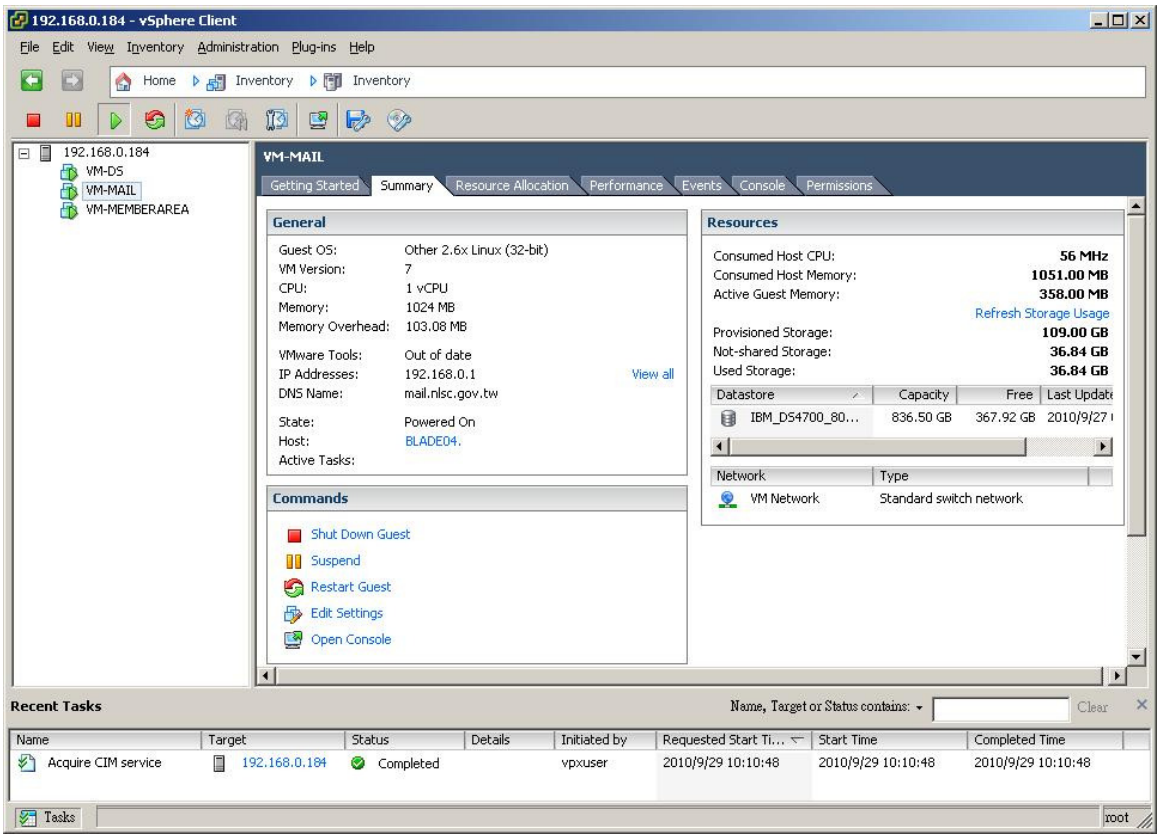


圖 11、VM-MAIL 於 vsphere Client

第一節、Samba 加入 AD 網域

為了在 Windows 主機間達到資源共享的目的，微軟發展出 SMB(Server Message Block)通訊協定，利用其網路芳鄰共享檔案系統及印表機等資源；而 Samba 在 Linux 主機上實現 SMB 通訊協定的系統，達成 Windows 與 Linux 主機的資源共享，再搭配 Winbind 模組解決 Samba 中統一登入問題。

一、Samba 3.0 伺服器設定

設定 Samba 最基礎的項目就是指定工作群組名稱(workgroup)及網域名稱，編輯 Samba 設定檔 smb.conf，以下設定都在該檔案內[global]標籤下同一段落完成。

/etc/samba/smb.conf

```
workgroup = lab
realm = LAB.GOV.TW
```

避免分享資源時出現亂碼，分別設定 Windows、Linux 的字集。

```
display charset = Big5
dos charset = CP950
```

使用 AD 網域認證必須修改 Samba 的安全層級，並指定認證主機及增加 Windows 網路相關設定。

```
security = ads
password server = adserver.nlsc.gov.tw
wins server = 10.10.10.1
encrypt passwords = yes
netbios_name = mail.lab.gov.tw
```

Linux 預設的使用者家目錄為/home/使用者名稱，針對 AD 網域使用

者必須另行設定其家目錄位置，主要參數為：%D 代表網域名稱、%U 代表使用者名稱。以下設定目的為讓網域使用者的家目錄集中在/home/網域名稱/目錄下並以使用者帳號命名，再順便讓使用者帳號自動套用網域名稱及不允許使用者離線登入。

```
template homedir = /home/%D/%U
winbind use default domain = yes
winbind offline logon = false
```

設定 AD 網域使用者帳號對應到 Linux 使用者帳號及群組的範圍。

```
idmap uid = 10000-20000
idmap gid = 10000-20000
```

預設 winbind 快取時間為 300 秒，使用指令`# getent passwd` 或`# getent group` 時，會將 NT/AD 網域的使用者與群組一併列出。當使用者、群組數量太多，winbind 會無法正常傳回資料，開啟此功能可以避免這個狀況。

```
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 300
```

若允許 AD 網域使用者以終端機方式登入系統，可指定 AD 帳號的 Shell。

```
template shell = /bin/bash
```

視需要開啟對 NT ACLs(Access Control List) 的支援。

```
nt acl support = yes
```

二、整合 Windows AD 網域帳號資訊

Samba 亦是遵循 PAM 認證模組規格的服務，故可透過編輯 PAM 認證模組的 Samba 設定，新增透過 Winbind 擷取使用者帳號、密碼認證。

/etc/pam.d/samba 加入

```
#%PAM-1.0
auth       sufficient   /lib/security/pam_winbind.so
account    sufficient   /lib/security/pam_winbind.so
```

當系統查詢使用者帳號與群組時，預設由檔案尋找(/etc/passwd、/etc/group)，為了使其搜尋不到相關資訊時，轉而使用 Winbind 向 AD 網域查詢，必須設定認證來源和順序。

/etc/nsswitch.conf

```
passwd: files winbind
shadow: files
group:  files winbind
```

設定本機 UID 與 GID 發放範圍，避免 AD 帳號與 Linux 本機帳號衝突，限制本機分配給新使用者的 uid、gid 不要超過 9999。

/etc/login.defs

```
UID_MIN 500
UID_MAX 9999
GID_MIN 500
GID_MAX 9999
CREATE_HOME yes
```

三、Linux Server 加入 AD 網域

在將主機加入網域之前，需先確認 AD 主機及 Linux 主機時間不得相差超過 5 分鐘，建議設定同一網路校時服務(Network Time

Protocol)，並設定 DNS 或 host 使 Linux 主機得知 AD 網域伺服器的 IP 位址，任修改其中一種能查詢到網域即可。

/etc/resolv.conf

```
Nameserver  10.10.10.1
```

/etc/hosts

```
10.10.10.1     adserver.lab.gov.tw
```

由於 Windows Server 2003 的 AD 是採用 Kerberos 的認證機制，因此必須設定 Kerberos 相關設定檔以便和 AD 溝通。

/etc/krb5.conf

```
[libdefaults]
default_realm = ADSERVER.LAB.GOV.TW
LAB.GOV.TW = {
  KDC = ADSERVER.NLSC.GOV.TW:88
  admin_server = ADSERVER.LAB.GOV.TW:749
  default_domain = LAB.GOV.TW
}
[domain_realm]
.LAB.GOV.TW = LAB.GOV.TW
LAB.GOV.TW = LAB.GOV.TW
```

/var/kerberos/krb5kdc/kdc.conf

```
[realms]
  LAB.GOV.TW = {
        Master_key_type = des-cdc-crc
        Supported_enctypes = des3-hmac-sha1:normal
         arcfour-hmac:normal  des-hmac-sha1:normal
         des-cbc-md5:normal  des-cbc-crc:normal
         des-cbc-crc:v4  des-cbc-crc:afs3
}
[kdcdefaults]
acl_file = /var/Kerberos/krb5kdc/kadm5.acl
dict_file = /usr/share/dict/word
admin_keytab = /var/Kerberos/krb5kdc/kadm5.keytab
v4_mode = nopreauth
```

完成以上設定後重新啟動 samba 及 winbind 並加入設開機啟動。

```
# service smb restart
# service winbind restart
# chkconfig smb on
# chkconfig winbind on
```

文字模式下指令加入 lab.gov.tw 網域，aduser 為 AD 網域之使用者，只需一般權限即可。

```
# net ads join -U aduser
aduser's password：
```

設定與 AD 伺服器溝通時的使用者。

```
# wbinfo --set-auth-user=aduser
Password:
```

一般 Windows 使用者在加入網域後存取不會有太大的問題，但 Linux Clients 使用者需要向 Kerberos 要求憑證(ticket)。可下指定測試取得 Kerberos 核發的憑證，取得後使用者不需要再輸入帳號密碼存取資源，注意網域名稱要大寫，若密碼正確會跳回命令提示字元。

```
# kinit 網域帳號@LAB.GOV.TW
```

取得 Kerberos 核發的憑證後，可以看 Kerberos 核發的 Kicket 狀態。

```
# klist
```

測試讀取 AD 帳號資訊和取得系統帳號資訊。

```
# wbinfo -u 取得網域帳號
# getent passwd
```

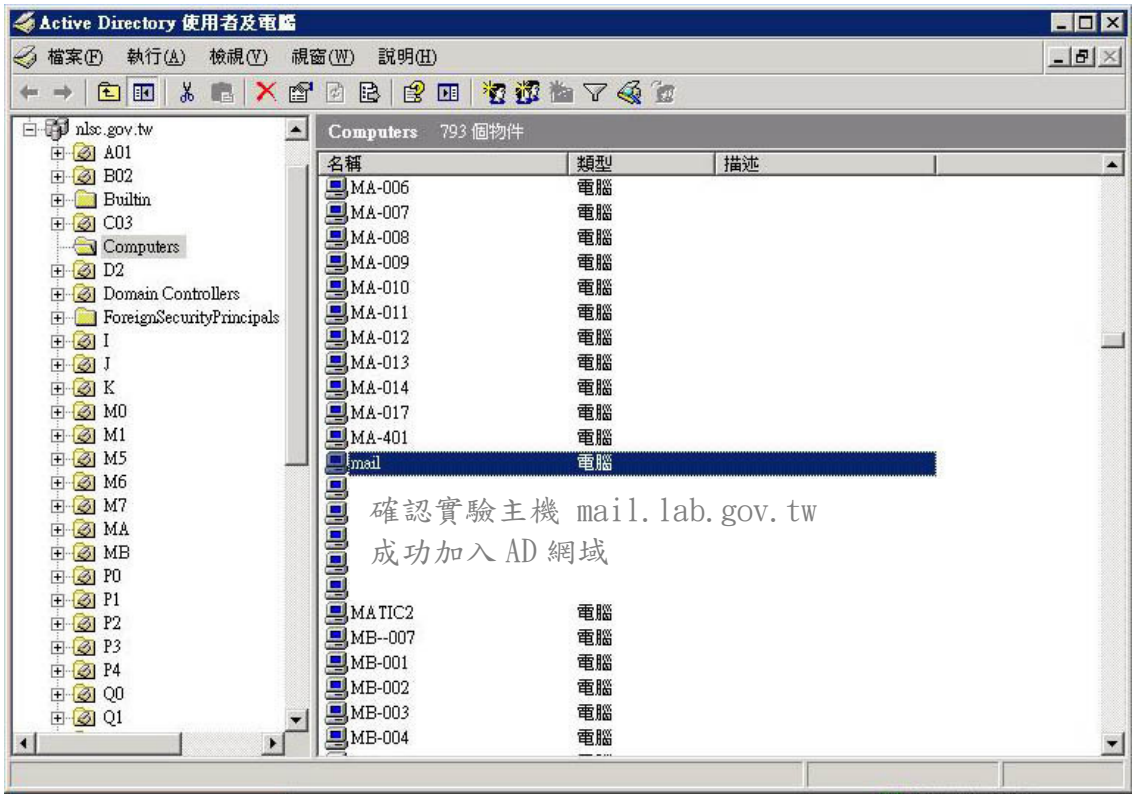


圖 12、檢視 AD 網域內之電腦

在加入網域時可能會遇到以下問題：

1、網域名稱未使用大寫，會得到下列的錯誤訊息

```
kinit(v5): Cannot find KDC for requested realm while getting initial credentials
```

2、如果輸入密碼錯誤，會得到下列的錯誤訊息

```
kinit(v5):Preauthentication failed while getting initial credentials
```

3、Administrator 密碼不能少於 6 碼，會得到下列的錯誤訊息

```
kinit(v5):KDC has no support for encryption type while getting inital credentials.
```

向 Kerberos 要求憑證時可能會遇到以下問題：

1、如果兩台機器的時間相差超過 5 分鐘，將無法獲得憑證，並得到下列的錯誤訊息

```
kinit(v5)Clock skew too great while getting initial credentials if the time difference is more than five minutes
```

2、尚未加入 Windows 網域時，就去向 Kerberos 要求憑證，會得到下列的錯誤訊息

```
kinit(v5):Cannot read password while getting initial credentials
```

大部分 Linux 主機所提供的服務會需要存取使用者家目錄，若使用者家目錄不存在，即使帳號密碼正確仍無法成功登入部份服務，所以在使用者初次成功登入時有自動產生使用者家目錄之必要。(施威銘,2002)中利用一 mknthome.awk 程式指令稿批次建立使用者家目錄

並設定目錄擁有者與所屬群組，指令如下：

```
#!/bin/awk

BEGIN{
FS=":"
    uidmin=10000 ……必須與/etc/samba/smb.conf 內設定的
    uidmax=20000 ……使用者 uidmin、uidmax 一致
}
{
    if ( $3 >= uidmin && $3<= uidmax ){
    print "\nmake directory " $6 "\nchown " $3 "." $4 " " $6
    system( "mkdir -p " $6 "; chown " $3 "." $4 " " $6)
    }
}
```

mknthome.awk 指令稿內容：

```
# getent passwd|awk -f
```

以上述指令方式批次產生使用者家目錄雖然可行，然而若 AD 網域內新增使用者，必須再次下指令批次產生或人工手動建目錄，在此建議的作法是利用 PAM 模組化驗證機制，於使用者通過帳號密碼驗證成功登入後額外執行 pam_mkhomedir.so 或 pam_oddjobmkhomedir.so 模組以檢查該使用者是否已具有家目錄，若無則自動產生使用者家目錄，並以/etc/skel/目錄為範本設定目錄權限，達到完全自動化的功能。

```
session    requisite    pam_oddjob_mkhomedir.so    skel=
/etc/skel/ umask=0022
```

至此已成功將 Linux 主機加入 AD 網域，並可識別 AD 網域之使用者，再透過 AD 網域管理伺服器進行帳號密碼認證，且網域使用者可於網路芳鄰中查到 Linux 主機內具有其個人擁有之共享資料夾和終端機登入能力。

第二節、郵件帳號服務整合

電子郵件系統共使用以下 3 種通訊協定類型：

一、SMTP (Simple Mail Transfer Protocol，簡單郵件傳輸通訊協定)：取代了傳統 Remote Procedure Call(RPC)和 X.400 的傳輸機制，用於 Internet 上和不同的郵件系統進行訊息交換。屬於電子郵件「傳輸」時所使用的通訊協定，換言之，SMTP 只負責郵件的傳送，而不具備接收的能力。

二、POP (Post Office Protocol，郵局通訊協定)：負責「接收」電子郵件的通訊協定，也就是 POP 不具有傳送郵件至使用者或其他郵件主機的功能。在提供 POP 服務的主機中，當郵件寄達時會先儲存在伺服器上，然後在用戶端連接至伺服器時，POP 伺服器會先驗證使用者帳號及密碼等資訊，以決定是否將使用者信箱中的郵件下載到用戶端電腦中，並且由伺服器上刪除這些郵件。

三、IMAP(Internet Message Access Protocol，Internet 訊息存取通訊協定)：其內容包括連接方式、用戶端驗證以及 Client/Server 間的交談等，與 POP 一樣的是 IMAP 主要是用來讀取伺服器上的電子郵件，不過用戶端須先登入伺服器才可以進行電子郵件的存取。與 POP 不同的是 IMAP 支援離線模式(Offline)、線上模式(Online)、中斷連結模式(Disconnected)3 種郵件存取模式。

大部分Linux作業系統版本皆具支援以上3種通訊協定之郵件系統套件，本次採用 Postfix 套件作為 SMTP 伺服器、Dovecot 套件作為 POP/IMAP 伺服器，並另行加裝 OpenWebMail 套件，以提供使用者在使用類似 Outlook Express 之類的 POP3 Client 端軟體收發信件外，增加一藉由 Web 介面收發郵件的選擇。此外，電子郵件得以順利收發尚需要 DNS 正反解、MX 記錄、A 記錄等觀念；WebMail 架設需要 Web 伺服器相關觀念，由於以上主題與本研究較無直接關係故不予贅述。

在進行郵件帳號服務整合前，必須先決定郵件格式，mbox(MailBox)是郵件伺服器的傳統格式，其主要將使用者所有信件都放置於一個與帳號同名的信件檔內，當收到新信件時，郵件伺服器會將新信附加於該信件檔案內；而當使用者透過 POP3 或 IMAP 伺服器刪除某封信時，則會將信件檔案內該封信的段落刪除。目前大多數發行版預設都採用 mbox 格式，而對於檔案鎖定的問題都已經處理完善，不會發生郵件伺服器 POP3/IMAP 同時寫入檔案的情形(施威銘,2005)。

SMTP 郵件伺服器與 POP3/IMAP 伺服器兩者必須設定使用同一種信箱格式，否則如果 SMTP 郵件伺服器改用 mbox 格式，而 POP3/IMAP 伺服器使用 maildir 格式，便會導致使用者無法以 POP3/IMAP 收信。所以當修改 SMTP 郵件伺服器使用的格式後，也要記得修改 POP3/IMAP 伺服器的設定使用同一種格式。基於管理方便性與軟體支援度的考量下，除非有效率上的需求，否則仍建議管理者沿用傳統的 mbox 格式即可。本研究中所採用的 OpenWebMail 目前只支援 mbox 格式，故 Postfix、Dovecot 皆須強制使用 mbox 格式。

原本預設的 mbox 郵件存放位置為/var/spool/mail 目錄內，一連結/var/mail 指向/var/spool/mail 目錄，目錄內存放以使用者名稱為檔名的 mbox 檔。為了達到對使用者郵件容量(Quota)進行管制，將郵件存放位置更改為使用者家目錄以統一控管磁碟配額。網域使用者於 /home/lab/使用者名稱 目錄內存放 POP3(/IMAP)檔案，於/home/mail 目錄內存放 SMTP 檔案(先將/var/spool/mail 目錄複製到/home 內，再將/var/mail 連結指向目標改為/home/mail)；當搭配 OpenWebMail 使用時，OpenWebMail 會自動於每個使用者家目錄下產生所需的檔案及目錄，故規劃一律於/home 存放 POP3(IMAP)及 WebMail 檔案。如此進行郵件備份時，只需複製/home 目錄即可。

完成以上設定後，原本要分別讓 Postfix 及 Dovecot 2 服務結合 AD 網域認證機制；由於所有服務的認證流程皆引入 PAM 認證模組中的一般身分認證機制(Include system-auth)，故可直接將所需的共通認證部份，新增於系統的一般身分認證之中，此處設定的影響是全面性的，因為使用者有許多途徑可以修改密碼，也可以將 password 部份的內容註解起來(#)，禁止使用者於 Linux 端修改 AD 網域的密碼；對於 Dovecot、Postfix 特有的部份，再另行於 PAM 認證模組的 Dovecot、Postfix 設定中新增。

/etc/pam/system-auth 加入

```
auth        sufficient    pam_winbind.so  use_first_pass
auth        sufficient    pam_krb5.so     use_first_pass
account     sufficient    pam_winbind.so
account     sufficient    pam_krb5.so
session     sufficient    pam_winbind.so
session     optional      pam_krb5.so
password    sufficient    pam_winbind.so  useauth_ok
password    sufficient    pam_krb5.so     useauth_ok
```

/etc/pam/dovecot 加入

```
auth       sufficient   pam_krb5.so    no_user_check
validate
auth       sufficient   pam_winbind.so
account    sufficient   pam_winbind.so
account    sufficient   pam_permit.so
session    requisite    pam_oddjob_mkhomedir.so    skel=/
etc/skel/ umask=0022
```

檢查 Dovecot 組態檔，確認 Dovecot 使用 PAM 認證模組。

/etc/devecot.conf

```
passdb pam {
..............
}
```

/etc/dovecot-ldap.conf（目前備而不用）

```
hosts = 10.10.10.1
base = dc=lab,dc=gov,dc=tw
ldap_version = 3
auth_bind = yes
```

/etc/pam/smtp.postfix 加入

```
auth        sufficient    pam_winbind.so
account     sufficient    pam_winbind.so
```

完成以上設定後重新啟動 dovecot 及 postfix 服務。

```
# service dovecot restart
# service postfix restart
```

當使用者以 Outlook2003 等郵件軟體收信時，可能會出現如下的對話方塊，點選「是」繼續使用即可收信。

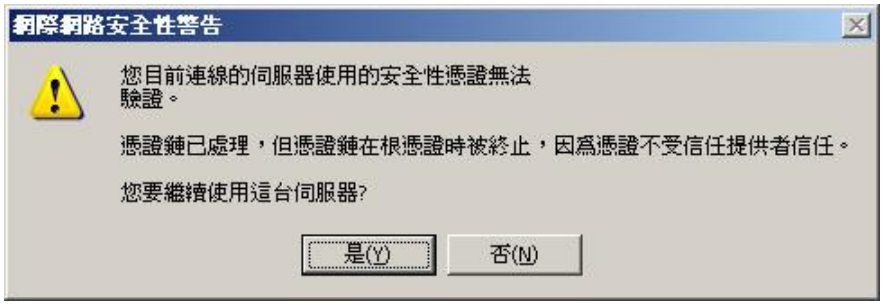


圖 13、郵件軟體對話確認框

第三節、OpenWebMail

在選擇開放原始碼 WebMail 解決方案的時候，除了注重完整的中文支援和友善的使用者介面(如：通訊錄功能、所視即所得編輯器)外，還必須確認該系統可符合本研究整合異質平台使用者的需求，由成功大學發展出的 OpenWebMail 具有支援 PAM、LDAP、多種認證模組及虛擬使用者等功能，完全合於所求。

OpenWebMail 為 Perl 所開發之直譯式程式，主機必須安裝 Perl 相關套件，特別注意需支援 suid perl，由於要透過 PAM 驗證模組透過 AD 網域管理伺服器進行使用者帳號密碼的認證，必須外掛 perl-Authen-PAM 套件，以上的套件使用 RPM 安裝。其餘大部分套件皆可由 CentOS 5.5 所提供之套件來源選取安裝，但 OpenWebMail 及 perl-Authen-PAM 套件 CentOS 5.5 預設的套件來源並無包含，必須自行下載 RPM 檔案安裝，並注意套件具有相依性，必須一次安裝 2 個 RPM。

```
安裝語法：rpm  - Uvh [套件檔名]
Rpm  - Uvh openwebmail-2.53-3.i386.rpm
           openwebmail-data-2.53-3.i386.rpm
Rpm  - Uvh perl-Authen-PAM-0.16-1.2.el5.rf.i386.rpm
```

然後執行系統第一次初始化。

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

一、OpenWebMail 進階設定

鑑於 OpenWebMail 預設設定所開啟的功能及使用者介面並不完全符合我們的需求，必須視需求調整設定；由於使用者在電腦開機登入時即可自行修改密碼或於密碼時效到期由 AD 網域管理伺服器要求

更新密碼，本中心 LDAP 入口網也提供修改密碼功能，且基於資訊安全管理系統(ISMS)所設定之安全性原則要求密碼的長度及複雜度等，故不開放供使用者於 OpenWebMail 端更改密碼，以避免密碼不符規定而發生程式例外情形。另外當使用者成功登入 OpenWebMail 後，若該使用者家目錄不存在，則無法在其下產生 OpenWebMail 運作所需檔案，當該目錄不存在，會出現以下錯誤訊息：

OpenWebMail ERROR
無法建立 /home/lab/使用者編號/mail (No such file or directory)

故需開啟自動產生家目錄功能，讓使用者在第一次成功登入後 OpenWebMail 會自動於系統家目錄 /home/lab 下自動新增以使用者名稱命名的使用者家目錄(即 家目錄/網域名稱/網域使用者名稱)，並於使用者家目錄內自動產生 mail、.openwebmail 2 個資料夾及相關檔案(mail 目錄：mail-trash、spam-mail、virus-mail，.openwebmail 目錄內所有目錄檔案)。其他基本設定詳見設定檔不再贅述。

/var/www/cgi-bin/openwebmail/openwebmail.conf

```
############################################################
# Buttons : EditFroms | EditStationary | POP3Setup |
# ChangePassword | History | Info
enable_editfrombook    yes ……[編輯通訊錄]
enable_stationery      no  ……[編輯信紙]
enable_pop3            no  ……[允許接收外部 POP3 信件]
enable_changepwd       no  ……[允許在 Openwebmail 端修
改密碼]
enable_history         no  ……[查詢歷史記錄]
enable_about           no  ……[關於對話方塊]
############################################################
# Personal Information
default_language                zh_TW.Big5 ……[語系]
default_autoreplysubject        自動回覆...[Re: $SUBJECT]
############################################################
# Display Preference
default_iconset        Cool3D.Chinese.Traditional
……[更改語系]
default_fontsize       11pt       ……[修改預設字體大小]
default_dateformat     mm/dd/yyyy ……[日期格式]
default_hourformat     24         ……[12、24 小時制]
關閉多餘功能
enable_userfolders          no  ……[使用者自訂資料夾]
enable_calendar             no  ……[行事曆]
enable_webdisk              no  ……[網路磁碟]
```

/var/www/cgi-bin/openwebmail/etc/dbm.conf

```
dbm_ext                 .db
dbmopen_ext             .db
dbmopen_haslock          no
```

設定 Apache 伺服器下 OpenWebMail 之 CGI 目錄別名，可以達到縮短網址 http://hostname/webmail 進入 OpenWebMail。

/etc/http/conf.d/openwebmail.conf

```
ScriptAlias
/openwebmail    "/var/www/cgi-bin/openwebmail/openwebmail
```

於更改設定後，套用新設定值。

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

二、加入 AD 網域帳號密碼認證機制

由於 OpenWebMail 無法識別網域使用者及交由 AD 網域管理伺服器完成驗證的工作，但其系統架構支援 PAM 認證機制，故可自行於 /etc/pam.d 下建立一 openwebmail 認證機制，帶入 AD 網域使用者資訊。

```
#%PAM-1.0
auth       sufficient   pam_winbind.so
auth       required     pam_nologin.so
account    sufficient   pam_winbind.so
session    sufficient   pam_winbind.so
session    include      system-auth
account    include      system-auth
auth       include      system-auth
```

建立完成 openwebmail 的 PAM 驗證機制後，必須自行修改程式碼將 OpenWebMail 預設的 login 機制置換成我們自行建立的驗證機制，再將 auth_unix.pl 認證模組改為使用 auth_pam.pl。

/var/www/cgi-bin/openwebmail/auth/auth_pam.pl

```
########## No configuration required from here ##############
my $servicename = $conf{'servicename'} || "openwebmail";
```

/var/www/cgi-bin/openwebmail/openwebmail.conf

```
#############################################################
auth_module     auth_pam.pl
```

於更改設定後，套用新設定值。

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

三、加入 AD 網域公用通訊錄

OpenWebMail 提供公用通訊錄的功能，可讓所有使用者查詢到同一份通訊錄，使人員或單位不必各自維護自己的通訊錄，但其作法並非直接自 LDAP 主機取得組織內的名錄，而是透過共用檔案的方式。雖然方法相對上較為落後，但還算簡單易管。OpenWebMail 公用通訊錄檔案預設為/var/www/cgi-bin/openwebmail/etc/addressbooks/global，必須指定一管理人帳號(郵件伺服器本機較容易)登入 OpenWebMail 來進行公用通訊錄管理維護，該公用通訊錄檔案的權限設定較為特殊，公用通訊錄的檔案擁有者(Owner)設為該管理人帳號有寫入的權限，Mail Users 群組(Group)有讀取權限。一般建議所有的 Mail Users 都屬於同一個群組，在新建帳戶時就全部設好群組(雖然 Linux 預設 1 個人 1 個群組)。本中心人員於郵件伺服器內皆屬於 AD 網域之 Domain User 群組，公用通訊錄管理人帳號設為 mailadmin(為編輯公用通訊錄檔案使用，故於郵件伺服器上建立本機

使用者即可)。

經測試:於 X-Window(本例使用 Gnome)中設定檔案屬性可順利存取 AD 網域中之使用者及群組設定並於清單中列出,使用 X-Window 進行設定可避免下指令繁瑣及發生系統無法辨識 AD 網域使用者、群組情形。

如下圖 、將/var/www/cgi-bin/openwebmail/etc/addressbooks/global 檔案屬性的擁有者(O)設為 mailadmin、群組(G)設為 domain users,global 這檔案就是在 OpenWebMail 通訊錄清單所看到的「公用通訊錄*」,只要名稱後面有一個 * 的就是公用的,該檔案群組下的每個使用者都可使用,建議 global 權限設為 640 不要讓其他使用者能夠修改公用通訊錄。亦可透過相應之文字指令完成。

```
# cd /var/www/cgi-bin/openwebmail/etc/addressbooks/
# chown mailadmin domain users global
# chmod 640 global
```

圖 14、global 檔案權限設定

四、從 LDAP 入口網自動登入功能

完成以上安裝設定後，於 OpenWebMail 之登入頁面輸入網域使用者帳號密碼已可交由 AD 網域伺服器端完成登入驗證。如果為了達成自中心 LDAP 入口網登入時，使用者只需登打一次帳號密碼，之後再連結其他線上系統時即可由 LDAP 入口網統一代入使用者帳號密碼交由 AD 網域伺服器認證；就必須於 LDAP 入口網新增一網頁連結以自動輸入存放於 LDAP 入口網伺服器端 sesseion 中的使用者帳號密碼給 OpenWebMail 登入頁面。

由於本中心 LDAP 入口網後端伺服器為 Apache Tomcat，故使用 JSP 及 Java Bean 技術達成，程式內容大綱如下：

1、於 LDAP 入口網新增一網頁 openwebmail_sso.jsp

2、自 LDAP 入口網伺服器端透過使用者連線 sesseion 取得使用者登入之帳號密碼。

3、再填入 OpenWebMail 登入網頁 openwebmail-main.pl 所需之表單欄位 loginname、password 即可完成自動登入。

openwebmail_sso.jsp

```
<%@page contentType="text/html"%>
<%@page pageEncoding="UTF-8"%>
<%@ page
import="tw.com.sysview.lsb.panel.PageGenerator,tw.com.sysv
iew.lsb.comm.SessionBean" %>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN"
   "http://www.w3.org/TR/html4/loose.dtd">
<%
    SessionBean bean =
    (SessionBean)session.getAttribute("sessionInfo");
    String userID="";
```

```
    String userPW="";
    if(bean == null){
         response.sendRedirect("http://LDAP 入口網主機名稱
         /openwebmail_sso_doublechk.jsp");
    }
    if(bean != null) {
        userID = bean.getAd_id();
        userPW = bean.getAd_pwd();
%>

<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;
         charset=UTF-8">
        <title>Web mail sso</title>
    </head>
    <body
         onload="document.getElementById('mform').submit()
    ;">
        <form id="mform" name="mform"
         action="http://OpenWebMail 伺服器 IP
         /openwebmail/cgi-bin/openwebmail/openwebmail-main
         .pl" method="post">
            <input type="hidden" name="loginname"
             value='<%=userID%>'>
            <input type="hidden" name="password"
             value='<%=userPW%>'>
        </form>
```

```
    </body>
</html>

<%
        }else {
            %>
                <script  language="javascript"  >
                    alert("Session 逾時，請重新登入！");
                    window.opener=null;
                    window.open("","_self");
                    window.close();
                </script>
            <%
        }
%>
```

在本虛擬機器正式取代現有郵件伺服器上線作業之前，為供一般使用者驗證以 AD 網域帳號密碼登入新郵件伺服器之運行情況，特使用開放原始碼內容管理系統 XOOPS(www.xoops.org)架設網站，供同仁於網路郵局進行帳號登入、收發郵件測試，並將本研究所有文件資料同步發表於該網站「網管文件」區。

圖 15、WebMail 測試網站

至此本研究之作業過程已全數說明完畢，鑑於閱讀不易且過程冗長，故另外撰寫成 3 階段簡易設定文件，訴求按部就班省卻作業原理的描述，絕大多數設定都可使用 Webmin(www.webmin.com)線上管理系統完成，供使用者快速上手或系統還原演練使用，文件完成後依其內容另行安裝一虛擬主機，確認運行無誤後同時完成以上文件有效性的驗證。

鑑於國內部份 Linux 的先進個人使用者、學者、行政院研考會、教育部或其他非官方社團推廣開放原始碼多年仍進展有限，個人觀點如下：Windows 作業系統挾其廣大的市占率、第三方應用軟體和廠商作支援，形成一個龐大的軟體服務網。許多開放原始碼的專案雖然發展卓越(如：Apache、Samba)但多屬於伺服端的運用，卻難以在桌面市場取得一定的佔有率，由此可見使用者評估 Linux 的使用成本並非「免費」。建議發展方向由主打取代 Windows 變更為和 Windows(各平台)協同作業，甚至不排斥和商業套裝軟體相互支援，並於某些應用

主題上凸顯優點以親近一般使用者(如：EPC、平板電腦)，如此方可自伺服器後端環境跨出。推廣時亦可看齊 Windows 的優點：簡單的設定環境和資訊人員進行系統管理時較低的背景知識門檻和文件。故本研究除透過上述學理方式由基礎設定達成目的，為使研究成果得以順利推廣至各機關，另行製作簡易設定文件供資訊人員參考(如：國中小資訊組老師)，讓一般或兼任的資訊人員得以擺脫技術困擾和疑慮後，在不需編列大筆預算的情況下欣然採用，達到務實推廣 Linux 的目的。

第六章、結論與建議

一、使用 Linux 郵件伺服器以 Winbind 加入 Windows AD 網域、NSS 進行帳號名稱解析、再由 Kerberos 套件進行加密後搭配 PAM 認證模組進行密碼驗證，確實符合本中心以 AD 網域管理伺服器為 Linux 郵件伺服器進行帳號密碼認證之需求，達成自行研究及系統移轉目的。

二、目前本中心所有線上系統之使用者帳號密碼認證共可透過 2 部 AD 伺服器完成，為不影響使用者登入登出速度，可設定平衡 2 部 AD 伺服器之負載。

三、為確保 AD 運作效能，應定期檢查現有帳號、群組狀態及設定。

四、目前本中心 AD 網域管理伺服器作業系統為 Windows 2003 R2 標準版、郵件伺服器採用 Samba-3 洽符合連線要求，如日後有 AD 網域管理伺服器作業系統升級包含重大結構性更新或元件升級，Linux 伺服器端可能必須配合更動認證過程，故規劃升級 Windows AD 網域伺服器時(如：Windows 2008 Server R2)，宜建立虛擬伺服器預為測試。

五、由 Samba-4 Roadmap(http://wiki.samba.org/index.php/Samba4)得知：目前開發中的 Samba-4 功能更完備，與 AD 網域管理伺服器整合性更高，屆時可視發展結果考慮升級新版本(附錄一)。

六、本研究以開放原始碼解決方案完成異質平台單一簽入的郵件伺服器。但無法完全取代 Exchange 伺服器與 AD 網域管理伺服器結合後所能提供郵件服務以外之延伸功能(如：結合行動裝置、工作行事曆、網路電話等，詳見附錄二、在 Exchange Server 2003 上執行的 Outlook 2003 與 POP/IMAP 和其他電子郵件伺服器的比較)。

七、本研究於實作時採用虛擬化技術，在成功後得到一整合上述功能之 Linux 郵件伺服器虛擬機器。虛擬化具有快速回復(Snapshot)、支援高可用性(High Availability)及叢集式架構

(Cluster)、資源動態配置(Distributed Resource Scheduler,DRS)等特性，自完成迄今具有相當之穩定性，若日後郵件流量倍增，還可擴大架構進行網路分流。若仍選擇使用實體伺服器，則此系統發展測試期間建立的虛擬機器可繼續保留作為測試機，當 Linux 系統元件發布更新時在測試機上先行修補並確認可正常作業後，再將更新檔套用至實體郵件伺服器(Production)上。

八、本研究中除 AD 網域管理伺服器外皆使用開放原始碼(Open Source)解決方案，無論在作業系統(Linux)、郵件伺服器(Postfix 架設 SMTP、Dovecot 架設 POP3、IMAP)及軟體(OpenWebMail、XOOPS)等方面確實提供完整功能，達到經濟實用的目的，並確保機關進行系統架構規劃時可有多元的選擇，避免基於未來相容性及擴充性考量而在當下把即將採購建置的系統向特定產品傾斜。

九、未來即使作業系統占有率互有消長，於使用者端出現多種平台桌面環境(Windows、Linux…)或使用終端機，在設計跨平台程式(如：JAVA 或其他 Web-based 應用系統)的使用者認證時，依然可採用本研究之異質平台整合架構。

十、採用開放原始碼解決方案之整體擁有成本(TCO)因人而異；除系統建置外，能克服系統管理、技術面等問題帶來後續使用之額外成本，方能享受其免費的特性。本研究特製作簡易設定文件分享研究成果，以期有效降低進入門檻，供一般學校資訊組老師或其他資訊預算不足的機關採用。

參考書目

SAMBA-3 實作手札 Samba-3 by example:pratical exercise to successful deployment，John H.Terpstra，上奇出版社

LDAP 系統管理 LDAP Administration,Carrier，O’ REILLY 出版社

POSTFIX 技術手札，Ralf Hildebrandt、Patrick Koetter，上奇出版社

POSTFIX 郵件伺服器白皮書，李蔚澤，金禾出版社

Linux Mail Server 技術實務，施威銘研究室，旗標出版社，2005

Linux 與 Windows 異質平台整合方案，施威銘研究室，旗標出版社，2004

Openwebmail 架設應用，林毓能，文魁出版社

Windows Server2008 Active Directory 建置實務，戴有瑋，碁峰出版社

網路資源

Samba Howto

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html#id2654004

Active Directory in Linux

http://www.linuxmail.info/active-directory-linux/

SquirrelMail Active Directory/LDAP Addressbook Howto

http://www.linuxmail.info/squirrelmail-active-directory-ldap-addressbook/

Active Directory and Fedora Directory Server Sync Howto

http://www.linuxmail.info/ad-fds-sync-howto/

Active Directory Single Sign On

http://www.linuxmail.info/active-directory-single-sign-on/

Active Directory and Dovecot PAM Authentication

http://www.linuxmail.info/active-directory-dovecot-pam-auth

entication/

Active Directory/LDAP Virtual Users for RHEL/CentOS 5

http://www.linuxmail.info/postfix-dovecot-ldap-centos-5/

Active Directory and Dovecot PAM Authentication

http://www.linuxmail.info/active-directory-dovecot-pam-authentication/

Active Directory Integration with Samba for RHEL/CentOS 5

http://www.linuxmail.info/active-directory-integration-samba-centos-5/

Troubleshooting Active Directory and Winbind

http://www.linuxmail.info/troubleshooting-active-directory-centos-5/

Auto Update SquirrelMail Personal Information

http://www.linuxmail.info/auto-update-squirrelmail-personal-information/

[整合方案]SambaPDC+LDAP

http://phorum.study-area.org/index.php/topic,36510.msg184029.html#msg184029

Postfix + Ldap + Active Directory 整合

http://phorum.study-area.org/index.php/topic,14590.0.html

LDAP + Windows AD + ad4unix

http://ssorc.tw/rewrite.php/read-197.html

A Primer to Active Directory: Microsoft's System Information Repository

http://www.enterprisenetworkingplanet.com/netsysm/article.php/2221041

Windows 網域管理，黃添修,2004

http://www.spps.tp.edu.tw/documents/memo/WINDOWS%E7%B6%B2%E5%9F%9F%E7%AE%A1%E7%90%86/WINDOWS%E7%B6%B2%E5%9F%9F%E7%AE%A

1%E7%90%86.htm

Windows 網域管理，李忠憲,2005

http://www2.meps.tp.edu.tw/documents/memo/WINDOWS%E7%B6%B2%E5%9F%9F%E7%AE%A1%E7%90%86/WINDOWS%E7%B6%B2%E5%9F%9F%E7%AE%A1%E7%90%86.htm

附錄一、Samba4 Roadmap

From SambaWiki (http://wiki.samba.org/index.php/Samba4)

What is Samba 4 meant to accomplish? In simplest terms, Samba 4 is an ambitious, yet achievable, reworking of the Samba code. Major features for Samba 4 already include:

- support of the 'Active Directory' logon and administration protocols
- new 'full coverage' testsuites
- full NTFS semantics for sharing backends
- Internal LDAP server, with AD semantics
- Internal Kerberos server, including PAC support
- fully asynchronous internals
- flexible process models
- better scalablilty from micro to very large installations
- new RPC infrastructure (PIDL)
- flexible database architecture (LDB)
- embedded scripting language (ejs)
- generic security subsystem (GENSEC)
- over 50% auto-generated code!

One of the goals of Samba4 is to implement an Active Directory compatible Domain Controller. Andrew Bartlett has written an excellent thesis on issues involved in developing an AD DC, which is also a good resource on Samba4's development in this area. The thesis was published on news.samba.org and is available here (in PDF).

Contents

Current Status

Volker Lendecke has also written an excellent Advances in Samba4 paper (in PDF), and in May 2005, Tridge gave a Samba4 Progress report and Roadmap. Since that time, we have implemented an embedded web server, a KDC and made vast improvements to the embedded LDAP server.

In short, you can join a WinNT, Win2000, WinXP or Win2003 member server to a Samba4 domain, and it will behave much as it does in AD, including Kerberos domain logins where applicable.

Samba4 development is moving very rapidly, but there is still much work to be done. A date has not been set for an official release, but the current source is available from our Git repository. To browse the source via a web browser, see Samba4's gitweb pages. For more info on obtaining the sources via a Git client, see the samba.org devel page.

Samba 4 is currently not yet in a state where it can replace existing production deployments.

Andrew Bartlett, Jelmer Vernooij and some other developers maintain a list of short-term plans and achievements.

For users

- FAQ
- HOWTO
- Fedora DS LDAP backend HOWTO
- OpenLDAP LDAP backend HOWTO
- Smart Card login (to windows clients) HOWTO
- Building Debian packages of Samba 4

For developers

- Development Resources
- Shared Library plans
- Test status
- Gtk+ frontends
- Active Directory plans
- Domain Member plans
- LDAP directory server backend plans

Previous releases

- 4.0.0-TP1
- 4.0.0-TP2
- 4.0.0-TP3
- 4.0.0-TP4
- 4.0.0-TP5
- 4.0.0alpha1
- 4.0.0alpha2

- 4.0.0alpha3
- 4.0.0alpha4
- 4.0.0alpha5
- 4.0.0alpha6
- 4.0.0alpha7
- 4.0.0alpha8

附錄二、在 Exchange Server 2003 上執行的 Outlook 2003 與 POP/IMAP 和其他電子郵件伺服器的比較

張貼日期：2004 年 8 月 13 日

訊息與協同作業解決方案的選擇，可能在今日商務環境中扮演重大關鍵的角色。瞭解 Microsoft Office Outlook 2003、POP、IMAP 與其他電子郵件伺服器部署的好壞之處，有助於讓您的整體擁有成本 (TCO) 降低，改善產能，讓辦公室之間的聯繫及與客戶的溝通更為容易。

Outlook 2003

Outlook 2003 是透過「訊息應用程式發展介面」(Messaging Application Programming Interface，MAPI) 以原生方式與 Exchange Server 2003 溝通的用戶端軟體。MAPI 提供豐富的訊息與溝通的通訊協定，包含電子郵件與內建的支援，針對排程、共用空閒(忙碌)資訊、連絡人清單、工作、目錄式通訊錄、公用資料夾等提供支援。

Outlook 支援 Exchange 信箱的最佳線上與離線存取，有了 Outlook 2003 與 Exchange 2003 的結合，Outlook 便最佳化到可以在撥接連線之類的慢速網路上展現最佳效能。Exchange 也幫助公司更輕鬆地部署、管理、支援電子郵件使用者與訊息傳送的環境，降低訊息基礎架構的整體擁有成本，同時增加可靠性、安全性與延展性。Outlook 亦提供豐富的協同作業用戶端，包含支援項目如下：

- 資訊即刻顯示
- 透過 Microsoft Office Live Communications Server 2003

與 Microsoft Office Live Meeting 使用立即訊息（Instant Messaging，IM）技術和進行會議

- 使用 Microsoft Windows SharePoint Services 與 Microsoft SharePoint Portal Server ，省去電子郵件訊息的附件，供共用工作區使用

Outlook 也能連接到 Exchange 以外的伺服器，比如它所支援的：

- 郵局通訊協定，第 3 版（Post Office Protocol 3，POP3）
- 網際網路訊息存取通訊協定，第 4 版（Internet Message Access Protocol 4，IMAP4）
- MSN Hotmail 分散式撰寫及版本處理/超文字傳輸協定（Distributed Authoring and Versioning/Hypertext Transfer Protocol，DAV/HTTP）
- 簡易郵件傳送通訊協定（Simple Mail Transfer Protocol，SMTP）

POP/IMAP

以 POP 為基礎與以 IMAP 為基礎的解決方案，最適合家用與個人使用，其資料復原能力與安全性的需求並不高。

- **POP** 的設計在於支援離線的郵件處理。有了 POP，電子郵件訊息就可以從伺服器移到本機的 POP 用戶端。這使得資料的管理與安全性的責任掌握在使用者的手中。
- **IMAP** 比較好些，提供離線與線上的雙重存取，但與 POP 相同的是，IMAP 不提供進階的協同作業功能，像是排程與群組排程、工作與連絡人管理。

Exchange 亦有內建非 Outlook 的用戶端的支援，像是網頁瀏覽器用戶端支援：

- 超文字標記語言 (Hypertext Markup Language，HTML)：Outlook Web Access
- 壓縮的 HTML (Compressed HTML，CHTML)：Outlook Mobile Access
- 無線應用程式通訊協定 (Wireless Application Protocol，WAP) 2.0：Outlook Mobile Access

Exchange 也為以 Microsoft Windows 為基礎的行動裝置提供同步處理支援，而 POP 與 IMAP 的解決方案則需要額外的伺服器應用程式以支援這些用戶端。Exchange 內含對 POP 與 IMAP 的支援，例如 Outlook Express。

基本的 POP 與 IMAP 電子郵件系統設計的目的絕非支援如此寬廣、豐富的協同作業能力，而且對於大多數的組織而言，在今日競爭的商業環境中，需要從業人員經由豐富的協同作業功能發揮更大的產能，因此只有基本的電子郵件服務是不夠的。

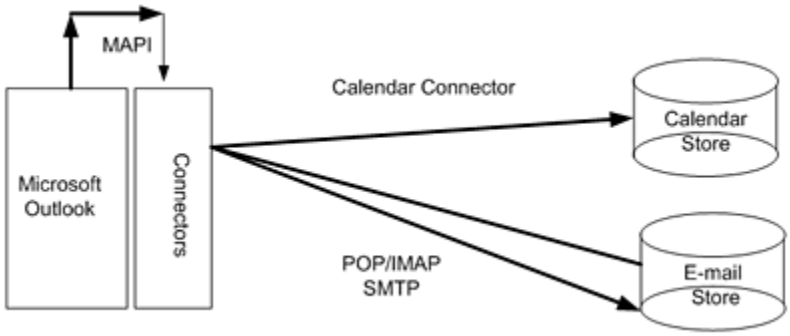
例如，如果某組織使用 Outlook 搭配電子郵件伺服器而非 Exchange，而且需要群組排程，組織會需要一個個別的排程應用程式，搭配支援 POP 或 IMAP 基礎架構的伺服器。此外，若組織想使用 Outlook 做 POP/IMAP 傳輸還有排程，那麼就需要 Outlook 連接器以與排程和 POP/IMAP 基礎架構進行溝通。

缺點是有一些，可是，當 Outlook 使用外部連接器時，包括了：

- **增加的複雜度。**由於連接器並非 Outlook 內部原生，因此安裝、支援、維護往往也較複雜。連接器通常會盡其所能模擬 Outlook 與 Exchange 一起使用的體驗，這體驗不僅只有電子郵件而已，更包含豐富的協同作業功能，搭配共用的行事曆、連絡人與工作。
- **額外的相容性測試。**由於這些連接器是新增至 Outlook

的，像是服務套件與更新檔—包含非 Microsoft 與自訂的應用程式的服務套件與更新檔新增至 Outlook，譬如 Research In Motion Limited (RIM) 桌面軟體或是客戶關係管理 (CRM) 軟體—可能會需要對連接器做額外的相容性測試。

- **額外的授權與支援成本。**連接器可能會有額外的用戶端存取授權 (CAL) 與支援成本。Outlook CAL 的權利是隨 Exchange CAL 而來，根據 Exchange 授權合約的條款，不需額外成本。
- **潛在的交互操作性問題。**有些伺服器應用程式，諸如 Oracle Collaboration Suite，需要個別的 API 模組以進行排程，增加了複雜度，也增加了訊息傳遞與其他個人資訊管理功能之間的交互操作性潛在問題。當公司使用的元件是來自有獨立電子郵件或排程伺服器的 解決方案時，可能需要針對後端伺服器所做的額外管理與系統整合。



圖一　外部連接器圖例

然而，Outlook 連接器在遷移與共存的狀況中都很好用，在這兩個狀況中，組織讓 Outlook 使用者每次都能存取一個電子郵件基礎架構以外的範圍。例如，從 IBM Lotus Notes/Domino 電子郵件系統遷移至 Exchange 的某組織，可以使用 Outlook Notes Connector for Domino Server，以協助一般使用者轉換至 Outlook 使用者介面與功能。

附錄三、簡易設定文件

Samba-3 架設應用

本段將完成

1、安裝 Samba 3.0

2、將 Samba 伺服器加入微軟 Active Dirctionary(以下簡稱 AD) 網域
示範網域：lab.gov.tw、AD 網域管理伺服器：dcserver.lab.gov.tw

3、使 Samba 伺服器可以識別微軟 AD 網域使用者，並透過 Windows AD Server 進行網域帳號密碼認證，達成單一簽入

4、網域使用者於 Samba 伺服器內具有個人之共享資料夾，存取須先完成帳號密碼認證

以上操作可使用 Webmin 完成設定

1. Samba 3.0 設定
2. 整合 Windows AD 網域帳號資訊
3. Linux Server 加入 AD 網域

4. Webmin 設定
4-1 Windows 網路選項
4-2 Winbind Options
4-3 Samba 組態檔
4-4 Kerberos5 Configuration
4-5 設定 PAM 認證

1. Samba 3.0 設定

/etc/samba/smb.conf

```
[global]
workgroup = LAB
realm = LAB.GOV.TW
netbios name = linux_Test
server string = Linux Test Samba Server
display charset = Big5
dos charset = CP950
unix charset = Big5
security = ads
password server = adserver.lab.gov.tw
encrypt passwords = yes
wins server = 10.10.10.1
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template shell = /bin/bash
winbind use default domain = yes
template homedir = /home/%D/%U
nt acl support = yes
```

2. 整合 Windows AD 網域帳號資訊

1、PAM 認證模組的 Samba 設定

/etc/pam.d/samba

```
#%PAM-1.0
auth       required     pam_nologin.so
auth       sufficient   /lib/security/pam_winbind.so
auth       required     pam_stack.so service=system-auth
account    sufficient   /lib/security/pam_winbind.so
account    required     pam_stack.so service=system-auth
session    required     pam_stack.so service=system-auth
password   required     pam_stack.so service=system-auth
```

2、編輯 NSS 設定檔

/etc/nsswitch.conf

```
passwd: files winbind
shadow: files
group: files winbind
```

3、設定本機 UID 與 GID 發放範圍，避免 AD 帳號與 Linux 本機帳號衝突

/etc/login.defs

```
UID_MIN 500
UID_MAX 9999

GID_MIN 500
GID_MAX 9999
```

3. Linux Server 加入 AD 網域

1、設定 DNS 或 hots

/etc/resolv.conf

nameserver **10.10.10.1**

或

/etc/hosts

10.10.10.1 adserver.lab.gov.tw lab.gov.tw

只要修改其中一種能查詢到 nlsc.gov.tw 網域即可。

2、修改 Kerberos

/etc/krb5.conf

```
[libdefaults]
default_realm = ADSERVER.NLSC.LAB.TW

[realms]
LAB.GOV.TW = {
  KDC = ADSERVER.NLSC.GOV.TW:88
  admin_server = ADSERVER.NLSC.GOV.TW:749
  default_domain = LAB.GOV.TW
}

[domain_realm]
.LAB.GOV.TW = LAB.GOV.TW
LAB.GOV.TW = LAB.GOV.TW
```

/var/kerberos/krb5kdc/kdc.conf

```
[realms]
LAB.GOV.TW = {
      Master_key_type = des-cdc-crc
        Supported_enctypes = des3-hmac-sha1:normal
        arcfour-hmac:normal  des-hmac-sha1:normal
        des-cbc-md5:normal   des-cbc-crc:normal
        des-cbc-crc:v4       des-cbc-crc:afs3
}
```

3、重新啟動 samba 及 winbind

```
# service smb restart
# service winbind restart
```

設定開機啟動

```
# chkconfig smb on
# chkconfig winbind on
```

4、加入 lab.gov.tw 網域

```
# net ads join -U aduser
```

← aduser 為網域帳號

```
aduser's password：
```

5、設定與 DC 溝通時的使用者

```
# wbinfo --set-auth-user=aduser
Password:
```

6、測試連線

```
# kinit 網域帳號@NLSC.GOV.TW
```

← 網域名稱要大寫

若密碼正確會跳回命令提示字元

AD 主機與 Linux 主機兩台時間不得相差超過 **5 分鐘** <- 這個部份很容易忽略，要注意。

7、測試讀取 AD 帳號資訊

```
# wbinfo -u
```

或

```
# getent passwd
```

8、自動產生使用者家目錄

mknthome.awk 程式指令稿建立使用者家目錄並設定目錄擁有者與所屬群組

（建議使用 PAM 內建模組 pam_mkhomedir.so、pam_oddjobmkhomedir.so 於使用者登入成功後自動產生家目錄）

```
# getent passwd|awk -f mknthome.awk
```

mkhomedir.awk 程式碼：

```
#!/bin/awk

BEGIN{
FS=":"

uidmin=10000
uidmax=20000
}

{
        if ( $3 >= uidmin && $3<= uidmax ){
        print "\nmake directory " $6 "\nchown " $3 "." $4 " " $6
        system( "mkdir -p " $6 "; chown " $3 "." $4 " " $6)
        }
}
```

4. Webmin 設定

1、Webmin 左側 SideBar 展開伺服器選項

伺服器

Apache 網頁伺服器
Dovecot IMAP/POP3 伺服器
MySQL 資料庫伺服器
Postfix 組態
SSH Server
Samba 視窗檔案分享

2、Webmin 右側出現 Samba 視窗檔案分享

模組組態　　Samba 分享管理　　搜尋文件

Samba 版本 3.0.33-3.28.el5

Select all. | Invert selection. | 新增檔案共用 | 新增印表機共用 | 新增複製 | 查看所有的連線

	共用名稱	路徑	安全
☐	homes	*所有使用者根目錄*	所有已知使用者可以讀/寫
☐	printers	*所有印表機*	所有已知使用者可列印到

Select all. | Invert selection. | 新增檔案共用 | 新增印表機共用 | 新增複製 | 查看所有的連線

Delete Selected Shares

全域設定


Unix 網路


Windows 網路


認證


Windows 到 Unix 列印

雜類選項

Winbind Options

檔案共用預設值

印表機共用預設值

Edit Config File

Samba 使用者

編輯 Samba 使用者和密碼

轉換 Unix 使用者到 samba 使用者

組態 Unix 和 Samba 使用者自動同步

新增和編輯 Samba 群組

組態 Unix 和 Samba 群組自動同步

Bind to Domain

重新啟動Samba伺服器

按下按鈕在系 統上重新啟動正在執行的 samba 服務。這將使當前組態立即生效。 這也會中斷所有到伺服器的連線，所以如果您不想要讓目前組態立即生效，只需要等待 1 分鐘讓 Samba 自動重新讀取組態檔案

停止Samba伺服器

按下按鈕在系 統上關閉正在執行的 samba 服務，這會強制中斷目前所有連線到伺服器的使用者。

4-1 Windows 網路選項

模組索引　　Windows 網路選項

Windows 網路選項

工作群組	○ 預設 ◉ LAB.GOV.TW		
WINS 模式	○ 作為 WINS 伺服器 ◉ 使用伺服器 10.10.10.1 ○ 沒有任何一個		
伺服器描述	○ 預 設 ○ None ◉ Samba Server Version %v		
伺服器名稱		**伺服器別名**	
預設服務		**每次都顯示服務**	global homes printers
回報磁碟空間的最大值	◉ 無限 ○ kB		
Winpopup 命令		**主瀏覽器優先順序**	20
最優先協定	預設	**主瀏覽器？**	◉ 是 ○ 否
安全	Active directory	**密碼伺服器**	10.10.10.1
遠端宣告至	◉ 沒有地方 ○ 來自清單...		

IP 地址	作為工作群組（可選）

儲存

回到 共用項目清單

4-2 Winbind Options

模組索引　　Winbind Options

Winbind Options			
Enable Winbind for local accounts?	◉ 是 ○ 否	Trust domain server users?	○ 是 ◉ 否
Disallow listing of users?	◉ 是 ○ 否	Disallow listing of groups?	◉ 是 ○ 否
Kerberos realm on domain server	LAB.GOV.TW	Seconds to cache user details for	300
Range of UIDs for Windows users	10000-20000	Range of GIDs for Windows groups	10000-20000
LDAP backend for account mapping	◉ 預設 ○		

儲存

回到 共用項目清單

4-3 Samba 組態檔

/etc/samba/smb.conf

```
#======================= Global Settings ==============================

[global]
#--authconfig--start-line--

# Generated by authconfig on 2010/05/31 09:22:36
# DO NOT EDIT THIS SECTION (delimited by --start-line--/--end-line--)
# Any modification may be deleted or altered by authconfig in future

   workgroup = LAB.GOV.TW
   password server = 10.10.10.1
   wins server = 10.10.10.1
   realm = LAB.GOV.TW
   security = ads

   display charset = Big5
   dos charset = CP950
   unix charset = Big5

   encrypt passwords = yes
   idmap uid = 10000-20000
   idmap gid = 10000-20000
   template shell = /bin/bash
   winbind use default domain = yes
   winbind offline logon = false
   winbind enum users = yes
   winbind enum groups = yes
   template homedir = /home/%D/%U
   nt acl support = yes
```

4-4 Kerberos5 Configuration

1、Webmin 左側 SideBar 展開網路選項

網路

Bandwidth Monitoring

Kerberos5

2、Webmin 右側出現 Kerberos5 Configuration

模組組態　　Kerberos5 Configuration　　搜尋文件

Log files	
Default log file	/var/log/krb5libs.log
KDC log file	/var/log/krb5kdc.log
Admin server log file	/var/log/kadmind.log
Default Configuration	
Realm	LAB.GOV.TW
Domain name	.lab.gov.tw
Default domain name	LAB.GOV.TW
Use DNS to lookup KDC	○ 是 ◉ 否
KDC	adserver.nlsc.gov.tw : 88
Admin server	adserver.nlsc.gov.tw : 749

Update Configuration

4-5 設定 PAM 認證

1、於 Webmin 左側 SideBar 展開[系統--PAM 認證]

系統
Log File Rotation
MIME Type Programs
PAM 認證
SysV 系統啟動組態

2、Webmin 右側部份[PAM 身份認證]選取設定 samba

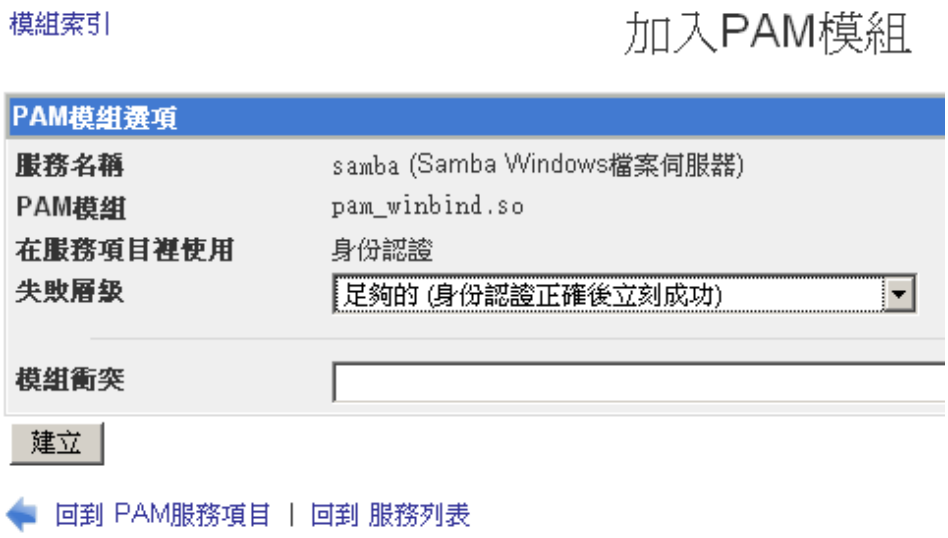
模組組態　　PAM 身份認證　　搜尋文件

新增 PAM 伺服項目

伺服器	描述
reboot	系統重新開機
remote	
run_init	
runuser	Run command as user
runuser-l	Run command as user (with login)
sabayon	
samba	Samba Windows 檔案伺服器

3、點選展開認證步驟、Account 確認步驟，並分別新增步驟給 pam_winbind.so (足

夠的(身份認證正確後立刻成功))



4、點選展開認證步驟、Account 確認步驟，並分別新增步驟給 pam_oddjobd_mkhomedir.so (必要的(在身份認證錯誤時立刻結束))，新增參數 skel=/etc/skel/ umask=0022

5、檢查全部內容

模組索引

編輯PAM服務

PAM服務項目內容

服務名稱	samba
描述	Samba Windows檔案伺服器
Configuration file	/etc/pam.d/samba

認證步驟

PAM模組	描述	失敗層級	參數	移動
pam_nologin.so	檢查/etc/nologin檔案	所要求的		↓
pam_winbind.so		足夠的		↓ ↑
Include service system-auth				↑

新增步驟給: pam_limits.so (設定資源限制) Add included service

Account確認步驟

PAM模組	描述	失敗層級	參數	移動
pam_winbind.so		足夠的		↓
Include service system-auth				↑

新增步驟給: pam_limits.so (設定資源限制) Add included service

Session設定步驟

PAM模組	描述	失敗層級	參數	移動
pam_oddjob_mkhomedir.so		必要的	skel=/etc/skel/ umask=0022	↓
pam_winbind.so		足夠的		↓ ↑
Include service system-auth				↑

新增步驟給: pam_limits.so (設定資源限制) Add included service

更改密碼步驟

PAM模組	描述	失敗層級	參數	移動
Include service system-auth				

新增步驟給: pam_limits.so (設定資源限制) Add included service

刪除PAM服務項目

回到 服務列表

Postfix、Dovecot 伺服器架設應用

進行以下步驟前應先完成 Samba-3 架設應用部份

已將 Linux 伺服器成功加入 AD 網域，並確認可由 Winbind、PAM 機制完成(網域)使用者登入服務之帳號密碼驗證登入伺服器、完成 DNS 正(反)解及 MX 記錄等設定，方可進行郵件伺服器架設

示範郵件伺服器：mail.lab.gov.tw、網域：lab.gov.tw

本段將完成

1、設定以 Postfix 提供 SMTP 服務、Dovecot 提供 POP3 服務作為郵件伺服器

2、透過 Windows AD Server 進行網域帳號密碼認證，達成單一簽入

以上操作可使用 Webmin 完成設定

1. Postfix 設定

1、Webmin 左側 SideBar 展開伺服器選項

伺服器
Apache 網頁伺服器
Dovecot IMAP/POP3 伺服器
LDAP Server
MySQL 資料庫伺服器
Postfix 組態

2、Webmin 右側出現 Postfix 郵件程式

說明... 模組組態	Postfix 郵件程式 Postfix version 2.3.3	搜尋文件


一般選項


位址重寫與偽裝


郵件別名


主要的對應表


虛擬網域


傳輸對應表


重新定位對應表


Header Checks


Body Checks


BCC Mapping


本地端遞送


一般資源控制


SMTP 伺服器選項


SMTP 客戶端選項


SMTP Authentication And Encryption


SMTP Client Restrictions


遞送速率


除錯功能


Server


Mail Queue

Processes 0 messages

Configuration Check

使用者信箱

Edit Config Files

停止 Postfix

按下這個按鈕以停止 Postfix 郵件伺服器. 這將停止其他系統寄送郵件給本地端的使用者, 並且防止客戶端以這個系統為郵件伺服器遞送郵件.

1-1 一般選項

模組索引
說明...

一般選項

最有用的一般選項

外送郵件所要使用的網域 ○ 使用主機名稱 ○ 使用網域名稱
○

要接收郵件的網域 ○ 本地端機器 ○ 整個網域
○ $myhostname, localhost.$mydomain, localhost

要回報個 postmaster 個錯誤 ○ 預設值 ○

其他一般選項

遞送外送郵件經由主機 ○ 直接遞送 ○

每個訊息隱藏副本的接收位址 ○ 無 ○

處理要求的逾時值 18000s

預設的資料庫類別 hash

預設的訊息遞送傳輸 smtp

退回郵件的寄件者位址 double-bounce

主列目錄下面的子目錄數目 1

佇列目錄子目錄的的分隔名稱 deferred, defer

收件人: 標頭的最大數目 50

遞送未遞送的警告前之等待時間 ○ 關閉
○

接收郵件的網路介面 ○ 全部 ○

在內部 IPC 100s

輸出入內部 3600s

客戶端中隊連結後的閒置時間		頻道的逾時值	
郵件系統時間	Postfix	郵件擁有者	postfix
官方的郵件系統版本	2.3.3		
等待下一個服務要求的等待時間	100s	在離開前處理的最大服務要求	100
這個郵件系統的網際網路主機名稱	◉ 預設值（由系統提供） ○		
本地端的網際網路網域名稱	◉ 預設值（由系統提供） ○		
本地端網路	◉ 預設值 (所有連接的網路) ○		
Automatic local networks	Same IP subnet		
送給郵件管理者通知，當退件從...	◉ 預設值 ○	送給郵件管理者通知，當 2 退件從...	◉ 預設值 ○
送給郵件管理者通知，當延遲遞送到...	◉ 預設值 ○	送給郵件管理者通知，當錯誤到...	◉ 預設值 ○
郵件佇列目錄	/var/spool/postfix		
鎖定檔案目錄，相對於佇列目錄	pid	使用者名稱/位址 的分離器	
重新定位對應查詢表	◉ 預設值（關閉） ○		

在郵件信箱上檔案關閉核心鎖定	☐ 是 ☑ 否	送出信號給守護器的最大時間	10s
Email content filter	☑ None ☐		

儲存並套用

1-2 SMTP 伺服器選項

模組索引　　SMTP 伺服器選項

SMTP 伺服器選項

SMTP 歡迎標頭	☐ 預設值 ☑ SMTP Ready		
遞送時接受的最大收件人數目	1000	關閉 SMTP VRFY 指令	☐ 是 ☑ 否
SMTP 傳送時的逾時時間	300s	在送出 4xx/5xx 錯誤回應前的逾時時間	1s
暫時忽略客戶端的錯誤計數	10	關閉連接的錯誤計數	20
HELO 是必要的	☐ 是 ☑ 否	允許不現任的路由	☐ 是 ☑ 否
限制 ETRN 指令基於...	☑ 預設值 ☐		
送出 HELO 指令的限制	☑ 預設值 ☐		
遞送者位址的限制	☑ 預設值 ☐		
收件人位址的限制	☐ 預設值 ☑ permit_mynetworks reject_unauth_destination		
郵件回應的限制	☑ 預設值 ☐		
對應侵犯	554	拒絕錯誤主機名稱的	501

的 SMTP 伺服器回應		SMTP 伺服器回應	
RBL 網域侵犯的 SMTP 伺服器回應	554	拒絕客戶端的 SMTP 伺服器回應	554
禁止中繼的 SMTP 伺服器回應	554	拒絕未知網域的 SMTP 伺服器回應	450
拒絕未知客戶端的 SMTP 伺服器回應	450	拒絕未知主機名稱的 SMTP 伺服器回應	450

儲存並套用

1-3 SMTP Authentication And Encryption

模組索引 SMTP Authentication And Encryption

SMTP Authentication And Encryption

Enable SASL SMTP authentication?	◉ 是 ○ 否	Handle non-compliant SMTP clients?	○ 是 ◉ 否
SMTP security options	☑ Reject anonymous logins		
	☐ Reject plain-text logins		
SMTP relaying restrictions	☑ Allow connections from same network		
	☐ Allow connections from this system		
	☐ Reject clients with no reverse hostname		
	☐ Allow authenticated clients		
	☑ Reject email to other domains		
	☐ Allow only relay domains		
	☐ Allow domains this system is a backup MX for		
Delay clients with failed logins?	◉ 是 ○ 否		

Enable TLS encryption?	○ 是 ◉ 否	
TLS certificate file	◉ 無	
	○	

TLS private key file

無

TLS certificate authority file

無

儲存並套用

1-4 設定 PAM 認證

1、於 Webmin 左側 SideBar 展開[系統--PAM 認證]

系統
Log File Rotation
MIME Type Programs
PAM 認證
SysV 系統啓動組態

2、Webmin 右側部份[PAM 身份認證]選取設定 smtp.postfix

模組組態　　PAM 身份認證　　搜尋文件

新增 PAM 伺服項目

伺服器	描述
reboot	系統重新開機
remote	
run_init	
runuser	Run command as user
runuser-l	Run command as user (with login)
sabayon	
samba	Samba Windows 檔案伺服器
serviceconf	
sieve	
smtp	SMTP authentication
smtp.postfix	Postfix SMTP authentication

3、點選展開認證步驟、Account 確認步驟，並分別新增步驟給 pam_winbind.so (足夠的(身份認證正確後立刻成功))


模組索引
加入PAM模組
PAM模組選項
服務名稱 smtp.postfix (Postfix SMTP authentication)
PAM模組 pam_winbind.so
在服務項目裡使用 身份認證
失敗層級 所要求的 (在身份認證錯誤後直到結束後才停止)
模組衝突
建立
回到 PAM服務項目 | 回到 服務列表

4、檢查全部內容

5、重新啟動 Dovecot

2. Devecot 設定

1、於 Webmin 左側 SideBar 展開伺服器選項

伺服器
Apache 網頁伺服器
Dovecot IMAP/POP3 伺服器
LDAP Server
MySQL 資料庫伺服器
Postfix 組態
Procmail Mail Filter
SSH Server
Samba 視窗檔案分享
SpamAssassin Mail Filter
流量監控
讀取使用者郵件

2、Webmin 右側出現 Dovecot IMAP/POP3 伺服器

模組組態　　Dovecot IMAP/POP3 伺服器　　搜尋文件

版本 1.0.7


網路及通訊協定


使用者和登入選項


Mail 檔案設定


SSL 設定


編輯設定檔

套用設定　套用目前的 Dovecot 設定去停止並且重新啟動 Dovecot 伺服器的功能.

停止 Dovecot 伺服器　關閉 Dovecot IMAP/POP3 伺服器功能，使用者將無法下載他們的電子郵件.

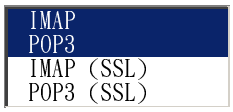
開機時啟動? ◉ 是 ○ 否　更改這個設定去開啟或者是關閉：系統開機時啟動 Dovecot 伺服器.

2-1 網路及通訊協定

模組索引　　網路及通訊協定

Dovecot 網路及 Mail 通訊協定選項

伺服器使用的 Mail 通訊協定



接受 SSL 連線? ○ 是 ○ 否 ◉ 預設 (是)

非 SSL 連線介面

◉ 預設值 ○ 全部的 IPv4 和 IPv6 ○ 全部的 IPv4

○ IP 位址

SSL 連線介面

◉ 預設值 ○ 全部的 IPv4 和 IPv6 ○ 全部的 IPv4

○ IP 位址

儲存

2-2 使用者和登入選項

模組索引　　使用者和登入選項

使用者認證和登入選項

SASL 認證範圍　○ 無 ○

預設認證範圍　○ 預設　認證方式 Anonymous / Plain-text / Digest-MD5 / Cram-MD5

○

使用者的資料來源, 主目錄和 IDs

○ 標準 Unix 使用者資料庫

○ 自訂密碼檔案

○ 總是使用 UID , GID 和主目錄

○ VPOPMail library

○ LDAP, 使用設定檔

○ PostgreSQL, 使用設定檔

○ SQL 資料庫, 使用設定檔

○ 其它 Dovecot 設定

密碼認證來源

○ Unix passwd 檔案

○ Unix shadow 檔案

○ 預設的 PAM 服務 (dovecot)

○ PAM 服務

☐ 開啟和關閉 PAM sessions

使用 cache key ◉ 無 ☐

☐ 自訂密碼檔案

☐ VPOPMail library

☐ LDAP, 使用設定檔

☐ PostgreSQL, 使用設定檔

☐ SQL 資料庫, 使用設定檔

☐ BSD 認證

使用 cache key ◉ 無 ☐

☐ 外部密碼檢查程式

☐ 其它 Dovecot 設定

UID 的最小值	☐ 預設 (500) ◉	UID 的最大值	☐ 預設 (無) ◉
群組 GID 的最小值	☐ 預設 (1) ◉	群組 GID 的最大值	☐ 預設 (無) ◉
附加第二個群組	◉ 無 ☐		
Mail 處理使用 Chroot 目錄	◉ 無 ☐		

登入處理的最大值 ◉ 預設 (128) ☐

登入處理的起始值 ◉ 預設（3） ○

儲存

2-3 Mail 檔案設定

模組索引　　Mail 檔案設定

Mail 位置和讀取選項

Mail 檔案位置	☐	自動偵測
	☐	收件匣和資料夾都在 ~/Maildir
	☐	收件匣在 /var/mail, 資料夾在 ~/mail
	☐	收件匣在 ~/Maildir, 資料夾在 ~/mail
	◉	**其它 Dovecot 位置** mbox:/%h/%d/:INBOX=/%h/%d/%u
索引檔案位置	◉	預設值（在 Maildir 資料夾）
	☐	僅在記憶體
	☐	其他資料夾
控制檔案位置	◉	預設值（在 Maildir 資料夾）
	☐	其他資料夾

郵件檢查的間隔時間	☐	不檢查 ☐ 秒 ◉ 預設
當空閒時的郵件檢查間隔時間	☐	不檢查 ☐ 秒 ◉ 預設（30）
允許存取到所有的 file system?	☐	是 ☐ 否 ◉ 預設（否）

Mail 結束的最末端儲存一個 CRLF 的控制?	○ 是 ○ 否 ◉ 預設（否）
使用其它程式處理 Mail 變更?	○ 是 ○ 否 ◉ 預設（是）
新檔案的權限設定	◉ 預設 ○
UIDL 格式	尚未設定（警告 - Dovecot 也許沒有
允許使用 POP3 的 LAST 指令?	◉ 預設（否） ○ 是 ○ 否
索引檔鎖定方式	預設（fcntl function）
Mailbox 讀取鎖定方式	◉ 預設（fcntl function） ○ 選擇如下，依照順序 ..
	<無> <無> <無> <無>
Mailbox 寫入鎖定方式	◉ 預設（fcntl function） ○ 選擇如下，依照順序 ..
	<無> <無> <無> <無>

儲存

2-4 SSL 設定

模組索引　　SSL 設定

IMAP 和 POP3 SSL 模式選項

SSL 認證檔案	◉ 預設 (/etc/pki/dovecot/certs/dovecot.pem) ○	
SSL 私鑰檔案	◉ 預設 (/etc/pki/dovecot/private/dovecot.pem) ○	
Password for key file	◉ None needed ○	
SSL CA certificate file	◉ 預設 (無) ○	
SSL 參數重新產生間隔時間	◉ 預設 (168) ○	小時
不允許使用 Plain-text 認證在非 SSL 模式?	○ 是 ○ 否 ◉ 預設 (否)	

儲存

回到 模組索引

2-5 設定 PAM 認證

1、於 Webmin 左側 SideBar 展開[系統--PAM 認證]

系統
Log File Rotation
MIME Type Programs
PAM 認證
SysV 系統啟動組態

2、Webmin 右側部份[PAM 身份認證]選取設定 dovecot

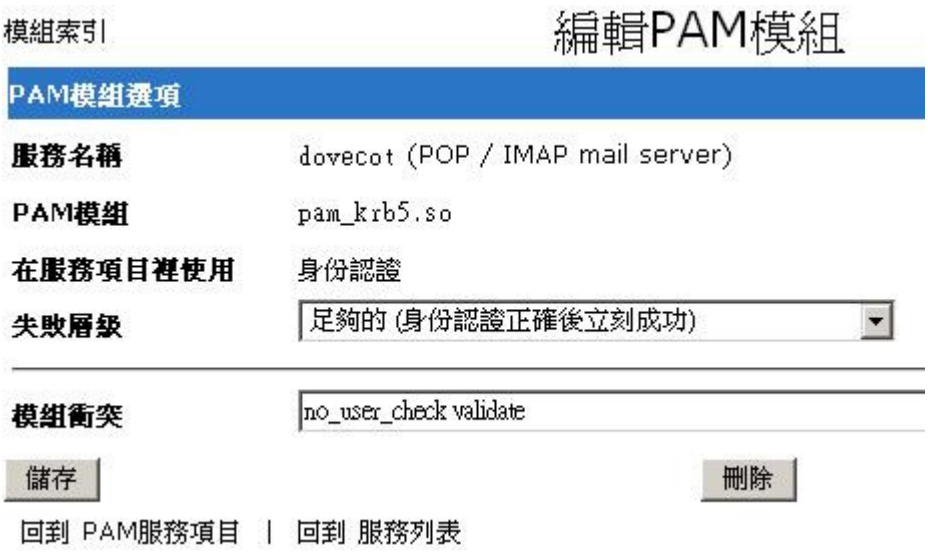
模組組態　　PAM 身份認證　　搜尋文件

新增 PAM 伺服項目

伺服器	描述
atd	Scheduled commands daemon
authconfig	
authconfig-gtk	
authconfig-tui	
chfn	更改 finger 資訊
chsh	更改 shell
config-util	Configuration utilities
cpufreq-selector	
crond	Cron daemon
cups	CUPS printing
dateconfig	
dovecot	POP / IMAP mail server

3、點選展開認證步驟、Account 確認步驟，並分別新增步驟給 pam_winbind.so (足夠的(身份認證正確後立刻成功))

4、點選展開認證步驟，並分別新增步驟給 pam_krb5.so (必要的(在身份認證錯誤時立刻結束))，新增參數 no_user_check validate



5、點選展開 Session 設定步驟，並 分別新增步驟給 pam_oddjob_mkhomedir.so (必要的(在身份認證錯誤時立刻結束))，新增參數 skel=/etc/skel/ umask=0022

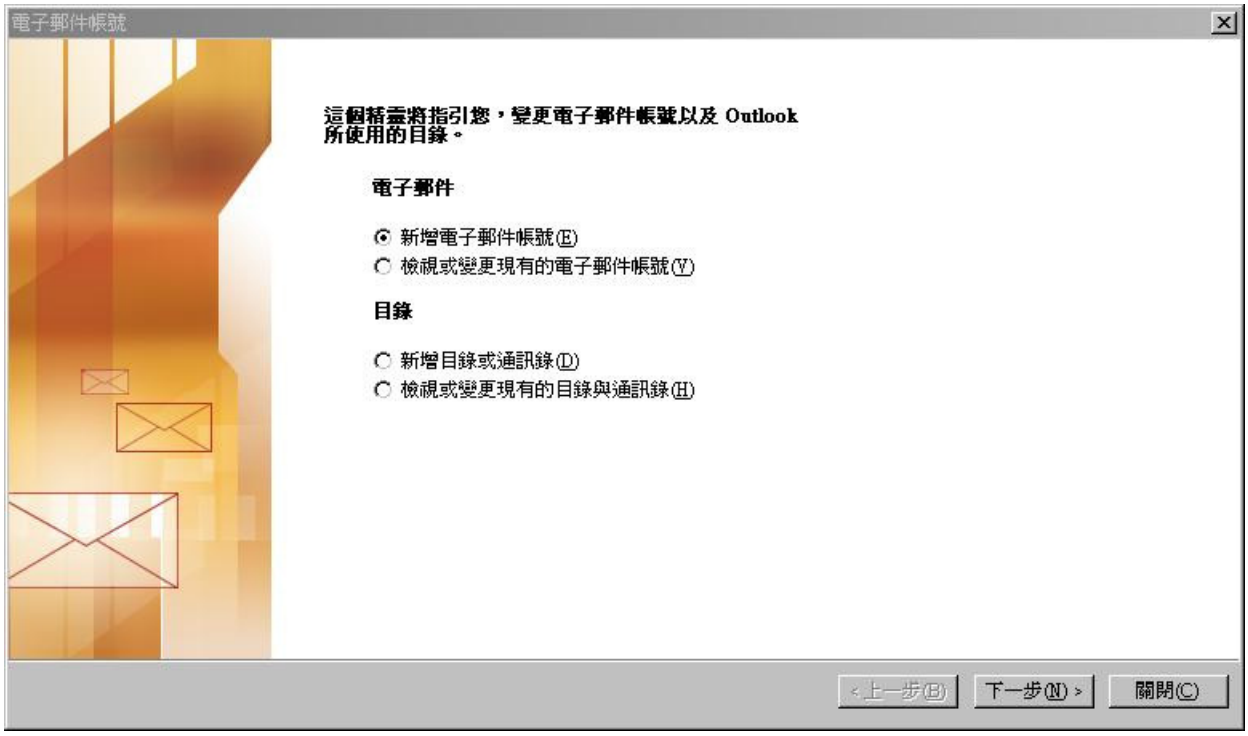

模組索引
加入PAM模組
PAM模組選項
服務名稱
dovecot (POP / IMAP mail server)
PAM模組
pam_oddjob_mkhomedir.so
在服務項目裡使用
Session設定
失敗層級
必要的 (在身份認證錯誤時立刻結束)
模組衝突
skel=/etc/skel/ umask=0022
建立
回到 PAM服務項目 | 回到 服務列表

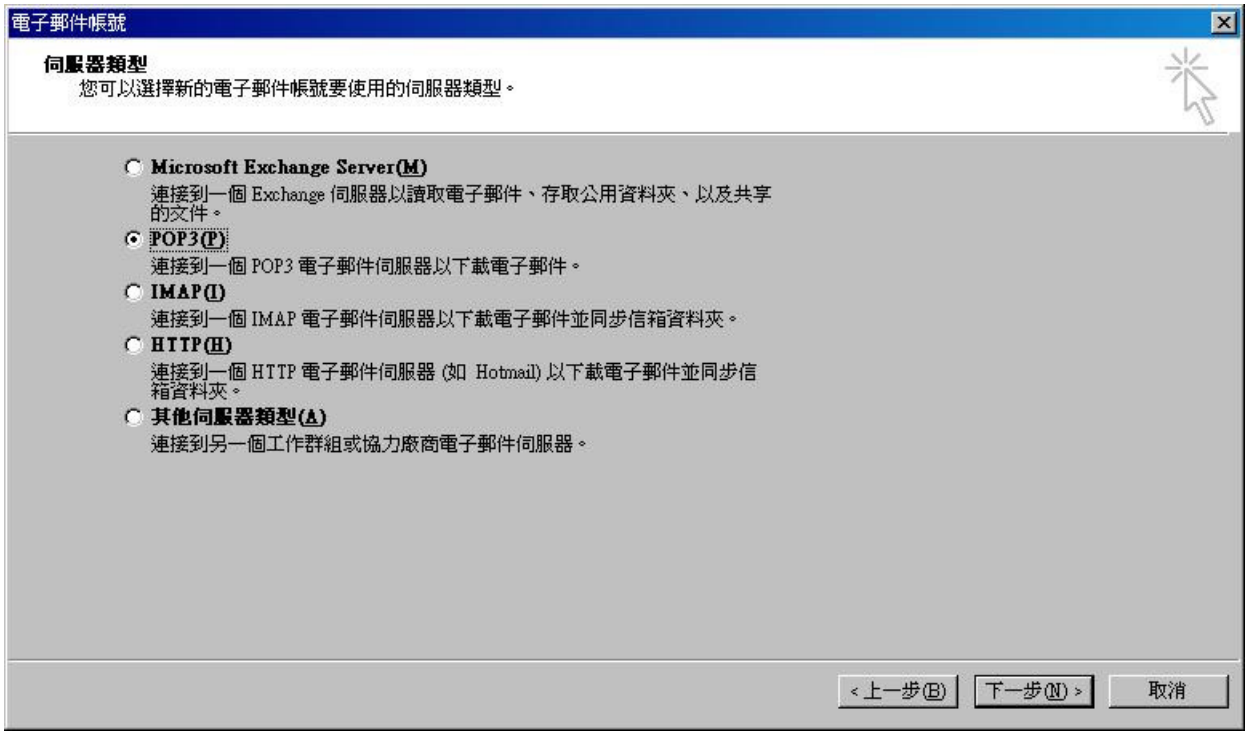
5、檢查全部內容

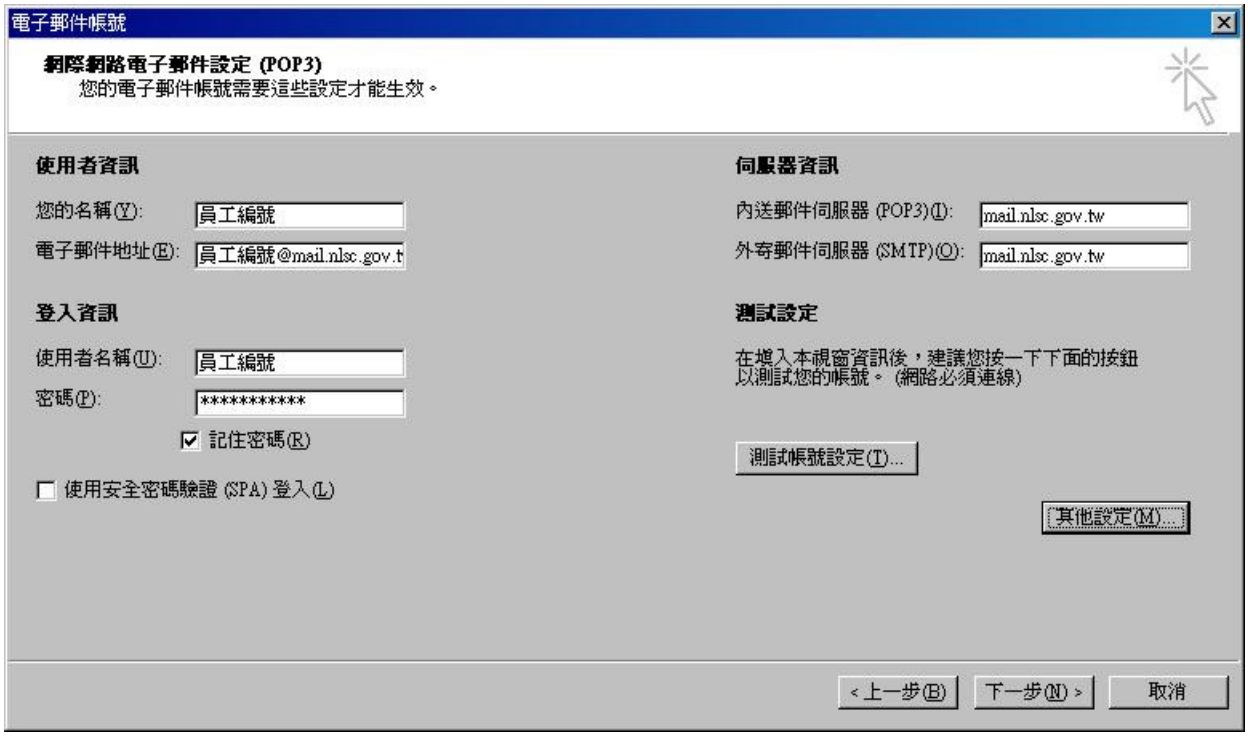
6、重新啟動 Dovecot

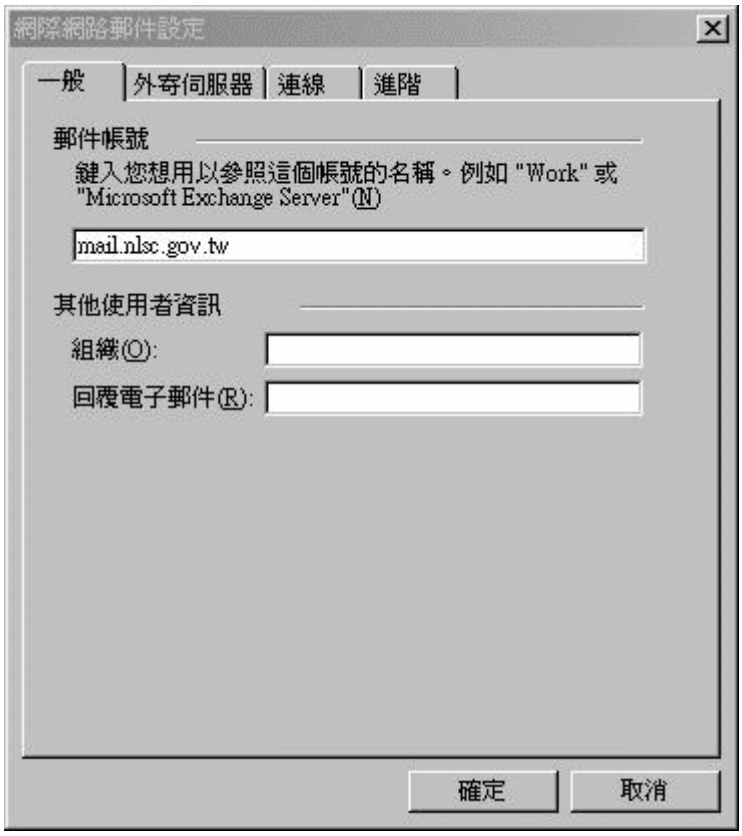
3. 收信軟體設定

以 Microsoft Outlook2003 為例：




電子郵件帳號
伺服器類型
您可以選擇新的電子郵件帳號要使用的伺服器類型。
Microsoft Exchange Server(M)
連接到一個 Exchange 伺服器以讀取電子郵件、存取公用資料夾、以及共享的文件。
POP3(P)
連接到一個 POP3 電子郵件伺服器以下載電子郵件。
IMAP(I)
連接到一個 IMAP 電子郵件伺服器以下載電子郵件並同步信箱資料夾。
HTTP(H)
連接到一個 HTTP 電子郵件伺服器 (如 Hotmail) 以下載電子郵件並同步信箱資料夾。
其他伺服器類型(A)
連接到另一個工作群組或協力廠商電子郵件伺服器。
< 上一步(B)
下一步(N) >
取消


電子郵件帳號
網際網路電子郵件設定 (POP3)
您的電子郵件帳號需要這些設定才能生效。
使用者資訊
您的名稱(Y):
員工編號
電子郵件地址(E):
員工編號@mail.nlsc.gov.t
登入資訊
使用者名稱(U):
員工編號
密碼(P):
****
記住密碼(R)
使用安全密碼驗證 (SPA) 登入(L)
伺服器資訊
內送郵件伺服器 (POP3)(I):
mail.nlsc.gov.tw
外寄郵件伺服器 (SMTP)(O):
mail.nlsc.gov.tw
測試設定
在填入本視窗資訊後，建議您按一下下面的按鈕以測試您的帳號。 (網路必須連線)
測試帳號設定(T)...
其他設定(M)...
< 上一步(B)
下一步(N) >
取消


網際網路郵件設定
一般
外寄伺服器
連線
進階
郵件帳號
鍵入您想用以參照這個帳號的名稱。例如 "Work" 或 "Microsoft Exchange Server"(N)
mail.nlsc.gov.tw
其他使用者資訊
組織(O):
回覆電子郵件(R):
確定
取消


測試帳號設定
恭喜您！已成功完成所有的測試。按一下 [關閉] 再繼續。
停止(S)
關閉(C)
工作
錯誤
工作
狀態
建立網路連線
已完成
尋找外寄郵件伺服器 (SMTP)
已完成
尋找內送郵件伺服器 (POP3)
已完成
登入到內送郵件伺服器 (POP3)
已完成

OpenWebMail 架設應用

進行以下步驟前應先完成 Samba-3 架設應用、Postfix、Dovecot 伺服器架設應用

確認郵件伺服器可由 Winbind、PAM 機制完成(網域)使用者登入服務之帳號密碼驗證並且收發信件無誤，方可進行 OpenWebMail 安裝設定

本段將完成

1、安裝 OpenWebMail

2、透過 Windows AD Server 進行網域帳號密碼認證，達成單一簽入

3、建立並維護 AD 網域使用者之公用通訊錄，供所有使用者使用

1. OpenWebMail 安裝
2. 修改 OpenWebMail 預設設定
3. 加入 AD 網域帳號密碼認證
4. 加入公用通訊錄
5. 升級 OpenWebMail 2.53 可能會遇到的問題及解決方式

1. OpenWebMail 安裝

1、OpenWebMail 安裝需求

支援 CGI 的 Web server
Perl 5.005 以上（需有 suid perl 支援）
CGI.pm-3.05（必要）
MIME-Base64-3.01（必要）
Digest-1.08（必要）
Digest-MD5-2.33（必要）
libnet-1.19（必要）
Text-Iconv-1.2（必要）
Authen-PAM-0.14（必要，外掛式認證）
Quota-1.4.10（必要，Quota control）
CGI-SpeedyCGI-2.22（可選擇，常駐執行—加快速度）
Compress-Zlib-1.33（可選擇，網頁壓縮—加快速度）
libiconv-1.9.1（可選擇，多國語言內碼轉換）
ImageMagick-5.5.3（可選擇，縮圖製作）
openssl-0.9.7d（可選擇，POP3 的 SSL 支援，若系統有 libssl 則不需要）
Net_SSLeay.pm-1.25（可選擇，POP3 的 SSL 支援）
IO-Socket-SSL-0.96（可選擇，POP3 的 SSL 支援）
以上的套件使用 RPM 安裝。

大部分可由 CentOS5［新增/移除軟體]之套件管理員選取安裝，但 Openwebmail 及 perl-Authen-PAM 必須另行下載檔案安裝。

安裝語法：rpm －Uvh［套件檔名］
Rpm －Uvh openwebmail-2.53-3.i386.rpm openwebmail-data-2.53-3.i386.rpm
Rpm －Uvh perl-Authen-PAM-0.16-1.2.el5.rf.i386.rpm
※OpenWebMail 具有套件相依性，必須一次安裝 2 個 RPM

2、執行系統第一次初始化

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

2. 修改 OpenWebMail 預設設定

1、/var/www/cgi-bin/openwebmail/openwebmail.conf　功能及使用者介面設定

```
##############################################
# Buttons : EditFroms | EditStationary | POP3Setup | ChangePassword |
# History | Info

enable_editfrombook     yes   [編輯通訊錄]
enable_stationery        no    [編輯信紙]
enable_pop3             no   [允許接收外部 POP3 信件]
enable_changepwd        no   [允許在 Openwebmail 端修改密碼]
enable_history           no   [查詢歷史記錄]
enable_about            no  [關於對話方塊]

##############################################
# Personal Information

default_language                zh_TW.Big5    [語系]
default_autoreplysubject        自動回覆...[Re: $SUBJECT]


##############################################
# Display Preference

default_iconset         Cool3D.Chinese.Traditional [更改語系]
default_fontsize        11pt [修改預設字體大小]
default_dateformat      mm/dd/yyyy [日期格式]
default_hourformat      24 [12、24 小時制]

 關閉多餘功能
enable_userfolders              no [使用者自訂資料夾]
enable_calendar                 no [行事曆]
enable_webdisk                  no [網路磁碟]
enable_autoreply                no [自動回覆]
enable_globalfilter             no [郵件規則]
enable_userfilter               no [使用者自訂郵件規則]
enable_preference               no [使用者修改偏好設定]
enable_spellcheck               no [拼字檢查]
```

```
create_syshomedir           yes  [自動建立使用者家目錄]

default_charset             big5 [配合 Active Dirctionary 之使用者名
                                  稱編碼]
default_locale              zh_TW.Big5
暫不啟用：
default_charset             auto [設定預設的編碼，若設為 auto 且使用
                                  Apache2.0 以上版本，httpd.conf 內必
                                  須將 AddDefaultcharset 設定為 off ]
default_readwithmsgcharset  yes  [以郵件編碼開啟郵件內容]
```

2、/var/www/cgi-bin/openwebmail/etc/dbm.conf

```
dbm_ext             .db
dbmopen_ext         .db
dbmopen_haslock      no
```

3、/etc/http/conf.d/openwebmail.conf

設定 Apache 伺服器下 OpenWebMail 之 CGI 目錄別名
可以達到縮短網址 http://hostname/webmail 進入 OpenWebMail

```
ScriptAlias
/openwebmail   "/var/www/cgi-bin/openwebmail/openwebmail.pl"
```

4、套用設定值

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

3. 加入 AD 網域帳號密碼認證

1、於/etc/pam.d 新增 openwebmail 認證機制

```
#%PAM-1.0
auth       sufficient   pam_winbind.so
auth       required     pam_nologin.so
account    sufficient   pam_winbind.so
session    sufficient   pam_winbind.so
session    include      system-auth
account    include      system-auth
auth       include      system-auth
```

2、\var\www\cgi-bin\openwebmail\auth\auth_pam.pl

```
########## No configuration required from here ###################
#將預設的 login 更改為 openwebmail (須於 \etc\pam.d 新增 openwebmail
#認證
my $servicename = $conf{'servicename'} || "openwebmail";
```

3、\var\www\cgi-bin\openwebmail\openwebmail.conf

```
#########################################################
#將 auth_unix.pl 認證模組改為 auth_pam.pl
auth_module     auth_pam.pl
```

4、套用設定值

```
#/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
```

4. 加入 AD 網域公用通訊錄

1、Openwebmail 公用通訊錄檔案預設為
/var/www/cgi-bin/openwebmail/etc/addressbooks/global

2、把公用通訊錄的檔案擁有者(Owner)設為該管理人帳號有寫入的權限，Mail Users 群組(Group)有讀取權限

3、一般人員於郵件伺服器內屬於 AD 網域之 Domain User 群組，公用通訊錄管理人帳號設為 mailadmin

如下圖、將/var/www/cgi-bin/openwebmail/etc/addressbooks/global 檔案屬性
擁有者(O) 設為 mailadmin
群組(G) 設為 domain users

```
# cd /var/www/cgi-bin/openwebmail/etc/addressbooks/
# chown mailadmin.domain users global
# chmod 640 global
```

global 這檔案其實就是在 OpenWebMail 通訊錄清單看到的「公用通訊錄*」
注意：global 權限一定要設 640 不要讓其他使用者修改公用通訊錄

5. 升級 OpenWebMail 2.53 可能會遇到的問題及解決方式

寫在前面：底下是站主管理的部份機器從 OpenWebMail 2.52 升級至 OpenWebMail 2.53 部份使用者遇到的情況，並非所有的使用者都會遇到，僅供有同樣情況的管理者、使用者參考 --- 其實主要的原因還是字元編碼的問題。

Q: 部份信件寄件者、標題出現亂碼：常見於對方使用 BIG-5 編碼的純文字或電子報，而 OpenWebMail 設成 UTF-8 編碼。
A: 「設定」-> 「字集」選「big5」（BIG-5 在台灣盛行畢竟有其歷史因素 ）。

參考資料：
正確設為 BIG-5 字集後， ~/.openwebmail/openwebmailrc 內的設定應為
locale=zh_TW.Big5
language=zh_TW
charset=big5
而非 UTF-8 字集的
locale=zh_TW.UTF-8
language=zh_TW
charset=utf-8

Q: 設定 big5 字集後，部份 BIG-5 信件寄件者、標題會出現 [UTF-8?] 干擾閱讀。
A: 系統管理者需修改程式，加入刪除 [UTF-8?] 程式碼。

修改三個檔案

/var/www/cgi-bin/openwebmail/openwebmail-main.pl

找到 my ($from, $to, $subject)=iconv('utf-8' , ...
加入
$from =~ s/\[UTF-8\?\]//g;
$to =~ s/\[UTF-8\?\]//g;
$subject =~ s/\[UTF-8\?\]//g;

/var/www/cgi-bin/openwebmail/openwebmail-read.pl

找到 ($body) = iconv($convfrom, $readcharset, $body) ...
加入
$from =~ s/\[UTF-8\?\]//g;
$replyto =~ s/\[UTF-8\?\]//g;
$to =~ s/\[UTF-8\?\]//g;
$cc =~ s/\[UTF-8\?\]//g;
$bcc =~ s/\[UTF-8\?\]//g;
$subject =~ s/\[UTF-8\?\]//g;

/var/www/cgi-bin/openwebmail/openwebmail-send.pl

找到 ($h)=iconv('utf-8', $composecharset, $h);
加入
$h =~ s/\[UTF-8\?\]//g;
找到($subject, $to,
$cc)=iconv('utf-8',$composecharset,$subject,$to,$cc);
加入
$to =~ s/\[UTF-8\?\]//g;
$cc =~ s/\[UTF-8\?\]//g;
$subject =~ s/\[UTF-8\?\]//g;
找到 ($h, $subject)=iconv('utf-8', $composecharset, $h, $subject);
加入
$h =~ s/\[UTF-8\?\]//g;
$subject =~ s/\[UTF-8\?\]//g;
找到 ($subject,
$replyto)=iconv('utf-8',$composecharset,$subject,$replyto);
加入
$subject =~ s/\[UTF-8\?\]//g;
$replyto =~ s/\[UTF-8\?\]//g;
找到 ($subject)=iconv('utf-8', $composecharset, $subject);
加入
$subject =~ s/\[UTF-8\?\]//g; [站內相關]