第九屆測量學術論文研討會論文集
中華民國100年2月26日中國測量工程學會

異質平台整合進行單一簽入之研究：以郵件服務為例
The Research of Single Sign-On between Different Platforms in Mail Service

傅俊淇[1] 胡征懷[2] 李旭志[3] 蘇惠璋[4] 林燕山[5]
Chun-Chi Fu Cheng-Huai Hu Hsu-Chih Lee Huei-Jhang Su Yan-Shan Lin

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。內政部國土測繪中心(以下簡稱本中心)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LDAP目錄服務單一化，使用者資訊驗證端全數交由AD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。結果顯示整合多項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；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。

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. NLSC's mail server 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 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

[1] 內政部國土測繪中心 技士
[2] 內政部國土測繪中心 技正
[3] 內政部國土測繪中心 課長
[4] 內政部國土測繪中心 副主任
[5] 內政部國土測繪中心 主任

sign-on between different platforms, which proves that ensure institutions not only having multiple choices when developing systems but also saving cost.

關鍵詞：單一簽入(Single Sign On, SSO)、Active Directory(AD)、Samba

一、前言

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,2004)

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。

真正高度整合的單一簽入應納入所有應用系統，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。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。

但上述目標實際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 LDAP 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，通常不會直接進行帳號整合，而是建立系統各自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。

二、本中心之單一簽入系統架構

一般的 LDAP 解決方案多專注於組織及人員目錄樹管理以供其他系統介接，目錄服務無法直接將電腦主機納入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，多數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入口網所連結的應用系統才能單一簽入。過去本中心亦採用上述作法(如圖1-1)，LDAP入口網及其他行政系統使用一目錄服務，電腦主機、防毒等套裝軟體則結合AD網域管理，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。

使用AD網域作為LDAP的統一解決方案具有從電腦開機就單一簽入的優勢(如圖1-2)，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(資訊安全管理系統)時，可利用WSUS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，並非微軟技術較為先進，主要原因是作業系統容易整合，Windows作業系統擁有的高市占率使多數商業套裝軟體主動支援其架構，這只是採用微軟自家技術帶來的某種便利。

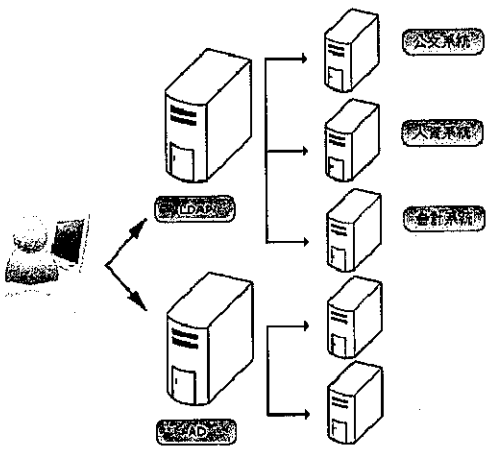

圖1-1、LDAP未統一

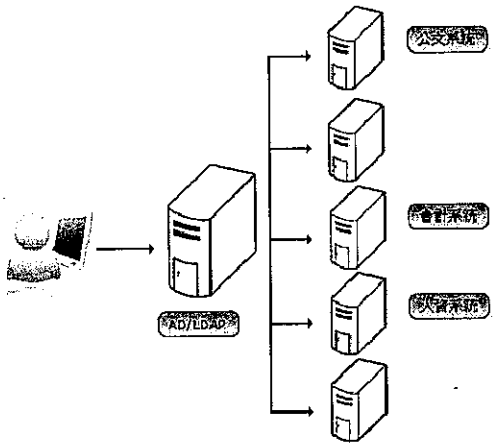

圖1-2、單一LDAP

為改善單一簽入系統架構，本中心於98年度將LDAP目錄服務更換為AD伺服器，朝目錄服務單一化發展。由於各線上系統要透過 AD 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LDAP入口網亦能自行連結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，行政系統已全數開發完成。

由於本中心並非所有同仁都配有個人電腦，所以具有本機登入、網域登入2種方式(如圖2)：

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。

就人事系統而言，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。

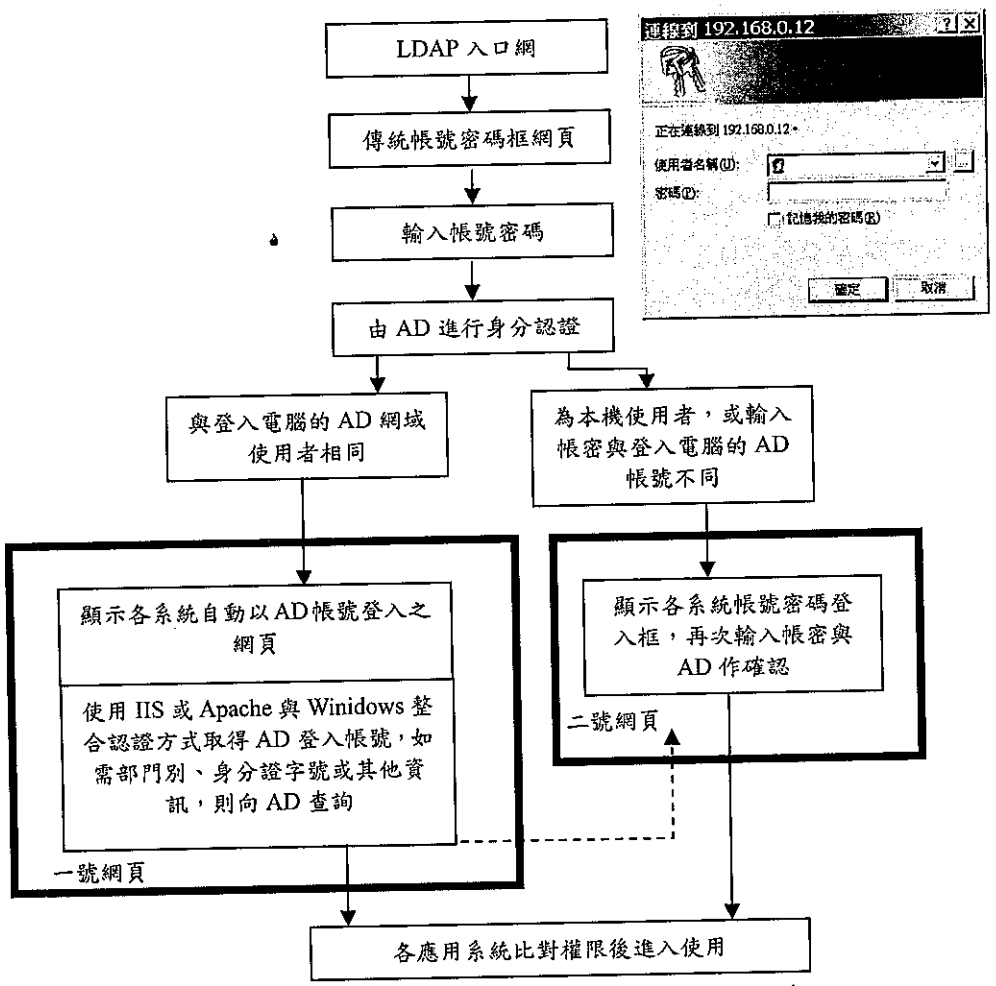

圖 2、本中心 LDAP 入口網認證流程

三、問題分析及解決方案

在調整單一簽入系統架構過程中發現：因為本中心現行郵件伺服器為 Linux 系統，無法加入 AD 網域集中管理，並完成 AD 網域使用者的帳號密碼認證。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 等單機式 POP3 郵件軟體收發信件，必須另行建置支援單一簽入功能之 WebMail。收發電子郵件以聯繫業務是日常辦公之必需，此衝擊不可謂不大。

本中心過去多委外解決相關資訊問題，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。解決方案如下：

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，主機易納入 AD 網域管理並結合 AD 網域管理認證機制，內建功能完整的 WebMail、具強大企業級商務通訊功能並易於管理及備援，但授權金額高昂。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 + 標準版用戶端授權

19187+19524+1879x650(人)=1260,061 元

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

19187+106346+(1879+961)x650(人)=1971,533 元

方案二、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，但未內建 WebMail 功能。採用開放原始碼解決方案的優點是軟體費用低廉(免費)。Linux 等開放原始碼除了應用在郵件伺服器外，更多的應用面是作為 Web 伺服器和資料庫使用。當異質平台間的主機無法彼此整合系統資源和使用者，則大大地限縮了應用的範疇；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。

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，加上響應行政院研考會及教育部推廣使用開放原始碼。故以郵件服務為例，作為異質平台整合單一簽入之研究項目。除建立一可加入微軟 AD 網域之 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 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 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、組織單一目錄樹、目錄服務端真正只維護一份使用者資訊之高度整合的單一簽入。

四、作業原理

要將 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 伺服器進行帳號密碼認證。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 中用以解決統一登入問題的元件。藉由在 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。圖 3 為 PAM 機制的示意圖(施威銘,2004,13-5)：

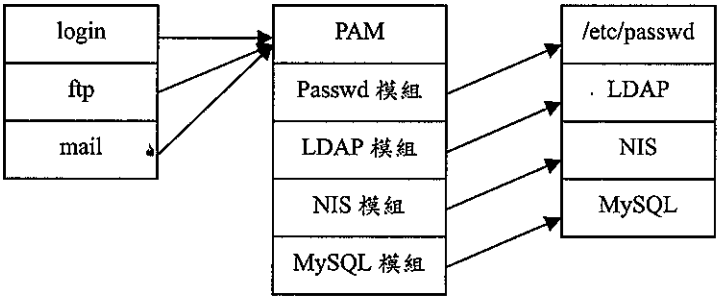

圖 3、PAM 機制示意圖

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 4 為 Samba 驗證後端搜尋路徑(John H.Terpstra,2006,6-10)，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。不過圖中的 LDAP 為 Linux 端的 OpenLDAP，作為本研究 LDAP 的 AD 伺服器位於圖中右上角之 NT 4 Domain。

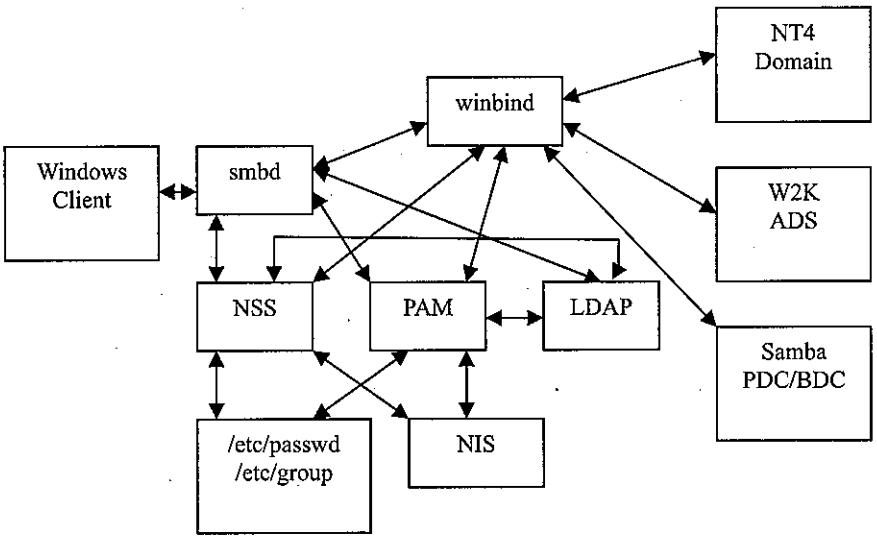

圖 4、 Samba 驗證後端搜尋

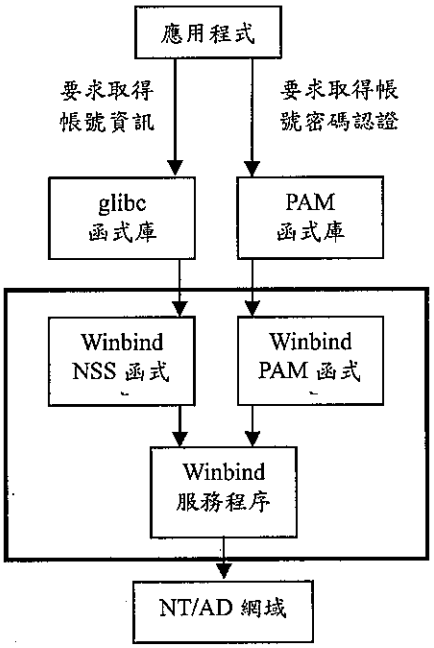

圖 5、Winbind 運作機制示意圖

圖 5 為 Winbind 運作示意圖(施威銘,2004,14-2)，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 Winbind 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，以解決帳號資料庫格式不一致的問題。

五、OpenWebMail：採用國立成功大學發展出的 OpenWebMail，具有支援 PAM、LDAP、多種認證模組及虛擬使用者等功能。雖然 OpenWebMail 預設無法識別 AD 網域使用者並完成驗證的工作，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。再自行修改程式碼將 OpenWebMail 預設的 login 機制置換成自行建立的 PAM 驗證機制，並將 auth_unix.pl 認證模組改為使用 auth_pam.pl。

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，並以郵件伺服器作為實作目標；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，可見此架構能套用於多數環境。當 Linux 郵件伺服器加入 Windows AD 網域內，並可識別出 AD 網域內之使用者，透過 Kerberos 加密與 AD 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。

五、實作方式

實際測試以本中心現行之AD伺服器(Windows 2003 Server)搭配虛擬化技術建立的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(Scalable)。本研究以VMware虛擬化軟體建立Cent OS 5.5 之虛擬Linux伺服器(VM-Mail)，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伺服器IP	10.10.10.1
AD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

Linux伺服器所需套件列表 (Cent OS 5.5)	
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	選擇性安裝
perl-Text-Iconv perl-Authen-Krb5 perl-Authen-Krb5-Admin perl-Authen-NTLM perl-Authen-PAM perl-Authen-Smb	perl-Compress-Zlib perl-IO-Socket-SSL perl-IO-Zlib perl-LDAP perl-libwww-perl perl-Net-SSLeay openssl

檢視結果如圖 7，mail.lab.gov.tw 已成功加入 AD 網域，並順利提供郵件服務及 WebMail，圖 8 為虛擬化管理工具 vsphere Client 中所見之虛擬實驗主機 VM-Mail(即 mail.lab.gov.tw)之基本資料。

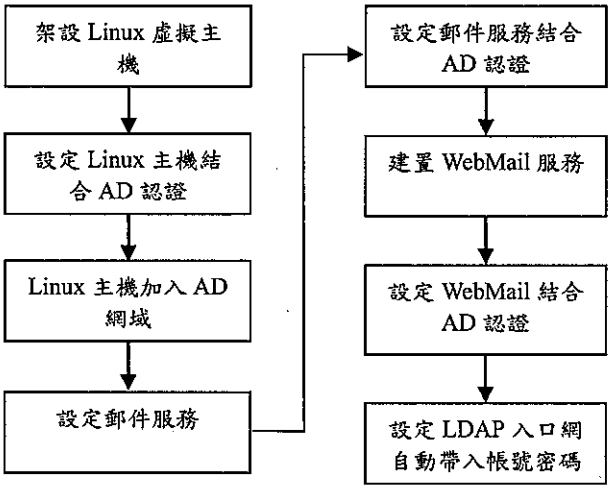

圖 6、實作流程圖

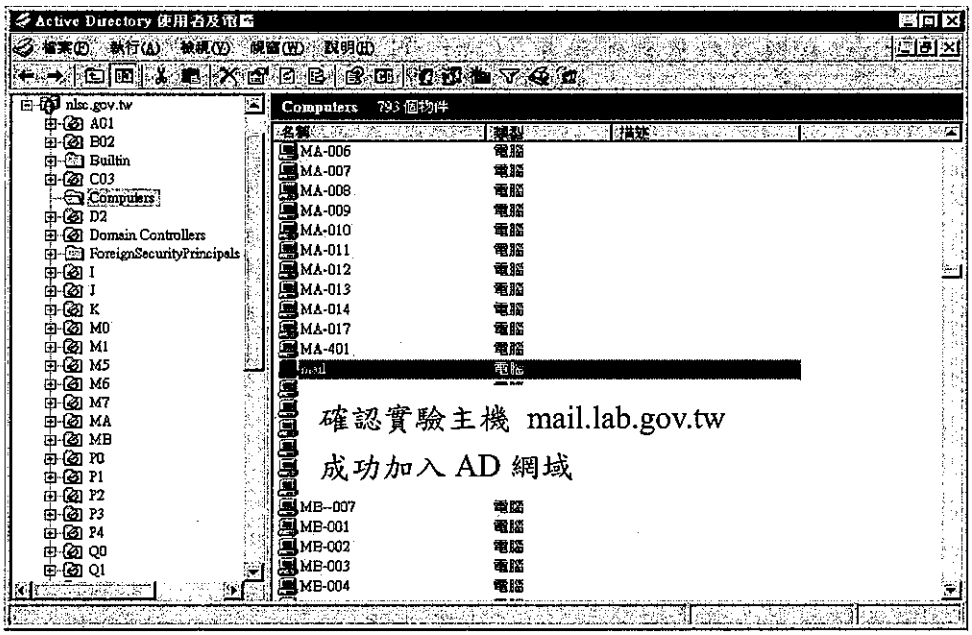

圖 7、檢視 AD 網域內之電腦

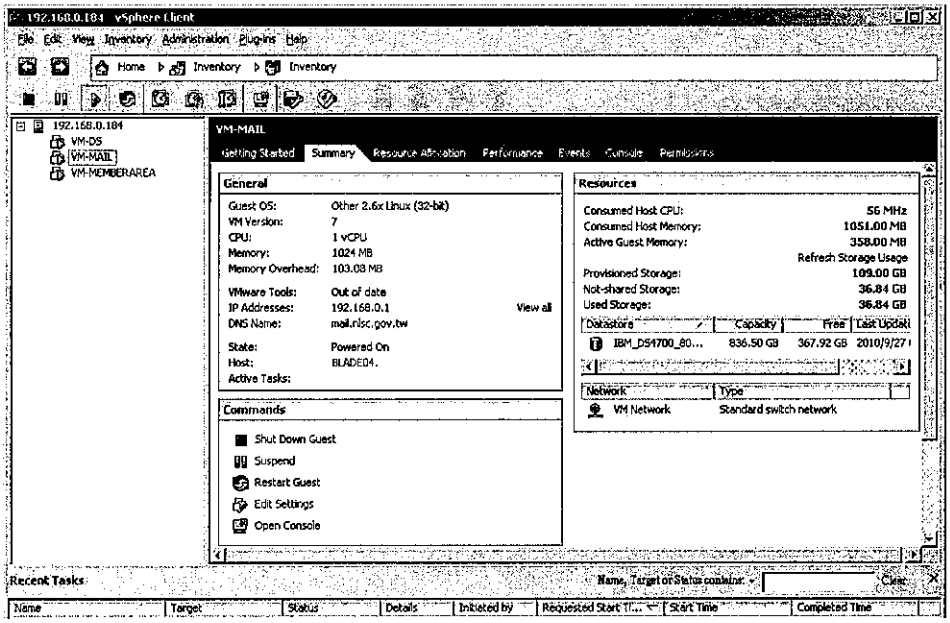

圖 8、VM-MAIL 於 vsphere Client

六、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 伺服器為 Linux 郵件伺服器進行帳號密碼認證之需求，達成自行研究及轉換系統架構的目的。

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、本研究之 AD 伺服器作業系統為 Windows 2003 R2 標準版，Linux 採用 Samba-3 進行整合，如日後規劃於任一端做重大結構性更新或元件升級，宜預為測試。

五、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。但仍無法完全取代 Exchange 伺服器所能提供郵件服務以外之延伸功能(行事曆、會議通知、結合行動裝置等)。

六、本研究於實作時採用虛擬化技術，虛擬化具有快速回復、支援高可用性及叢集式架構、資源動態配置等特性，並達到節能減碳、提高硬體資源使用率。自完成迄今具有相當之穩定性，若日後使用者及郵件流量倍增，導致系統過度負載，還可彈性擴大架構進行網路分流。

七、本研究中除 AD 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、郵件伺服器及軟體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。

八、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。期望

本研究成果可有效降低進入門檻，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

Carrier,2003。LDAP 系統管理(LDAP Administration), O'REILLY 出版社

John H.Terpstra,2006。SAMBA-3 實作手札(Samba-3 by example: practical exercise to successful deployment), 上奇出版社, 6-10

施威銘研究室,2004。Linux 與 Windows 異質平台整合方案, 旗標出版社,13-3、13-5、14-2

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/

Active Directory Single Sign On

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