*i*STAR™ UUSwitch（/UUExchange）

使用手冊

Release 2.5

UUDynamics, Inc.

2005 年 1 月

目 錄

第 1 章 概述 1
1.1 *i*STAR™產品功能特性 1
1.2 *i*STAR™產品系統架構 2
第 2 章 系統安裝 5
2.1 安裝硬體 5
2.2 安裝軟體 6
第 3 章 UUSwitch(/UUExchange)部署 12
第 4 章 系統維護 13
4.1 熟悉介面操作 13
4.1.1 進入設定介面 13
4.1.2 介面間的跳轉 14
4.1.3 退出設定介面 15
4.1.4 使設定生效 15
4.2 用戶管理 16
4.2.1 添加認證伺服器和使用者 19
4.2.2 添加證書 22
4.2.3 添加角色 22
4.2.4 檢查用戶端的運行環境 23
4.2.5 添加安全域 24
4.2.6 設定本地（/遠端）管理員 29
4.2.7 不同用戶存取 UUSwitch（/UUExchange）的方法 34
4.3 日常維護 38
4.3.1 匯入（/匯出）系統的設定資訊 38
4.3.2 顯示狀態 39
4.3.3 查看系統性能 40
4.3.4 查看日誌 40
4.3.5 故障檢修 42
4.3.6 系統時間設定 42
4.3.7 系統 LOGO 設定 42
4.4 非常規任務 44
4.4.1 管理許可證 44
4.4.2 升版系統 45
4.4.3 設定日誌和報警等級 46

4.4.4 設定加密演算法 46
4.4.5 更新數位憑證 47
4.4.6 改變模式 48
4.4.7 設定叢集分攤負載 48
4.4.8 SNMP 設定 50
4.4.9 連接埠轉遞 51
4.5 UUID 管理 52
第 5 章 系統復原 58
5.1 何時需要系統復原 58
5.2 系統復原方法 58
第 6 章 故障檢測和排除 60
第 7 章 附錄 62
7.1 UUSwitch(/UUExchange)的帶寬計算 62
7.1.1 子模式 UUSwitch(/UUExchange)的帶寬預算 62
7.1.2 預算溢出的警告 63
7.1.3 “私有”從 UUSwitch(/UUExchange) 63
7.1.4 不需要從 UUSwitch(/UUExchange)（直接連接） 63
術語表 64

第1章 概述

感謝您使用 UUDynamics 公司 ***i*STAR™**系列產品。***i*STAR™** UUSwitch(/UUExchange)是 UUDynamics 公司的企業型交換單元。

本使用手冊將對 ***i*STAR™** 產品的功能特性及系統架構進行簡要描述，并詳細介紹 UUSwitch(/UUExchange)的安裝、設定與操作步驟。

1.1 *i*STAR™產品功能特性

***i*STAR™**（**I**nstant **S**ecure **T**unnel **Ar**chitecture）是 UUDynamics 公司首創的新一代安全 Instant Extranet 技術。

i*STAR™**用於構建由“發佈單元(Publisher)”向“使用者單元(Subscriber)”發佈應用程式的 Extranet，這種方式能快速且安全地解決特定應用程式跨越企業網路和組織邊界的問題。i*STAR™**技術提供了基於“使用者單元（Subscriber）”、“發佈單元（Publisher）”和“交換單元(UUSwitch/UUExchange)”的安全資訊網路模型，爲現代企業使用者和應用服務提供商（ASP）提供了應用程式或文件存取的發布、控制和管理平臺。同時，它涵蓋了傳統 VPN 的所有功能，爲現代企業網的 Intranet、Extranet、Remote Access、Application Export 等提供了安全、高效的整體解決方案；***i*STAR™** 還能快速實現企業與其分支機搆和商業夥伴之間的 B2B、供應鏈、分散式 OA 等電子業務的需求。

與其他 VPN 產品相比，***i*STAR™**具有更強大的功能和更具優勢的性價比：

1. 安全性高：

   ***i*STAR™**採用了 SSL(Secure Socket Layer)協定，從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

   - 採用了 SSL(Secure Socket Layer)協定。從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，實現應用層使用者存取管理。徹底執行基於使用者的安全政策
   - 對應用程式透明。能夠保護企業網路免於遭受來自外部以及內部的威脅
   - 可以選擇對應用程式進行加密（Encryption & Hash）
   - 支援 Radius、Windows Domain 伺服器等使用者認證方式

2. 接入方式靈活：

   - 支援有公共靜態 IP 位址和沒有公共靜態 IP 位址的使用者
   - 能爲企業夥伴提供安全的，彈性的外聯網(Extranet) 接入方式
   - 在任何時間，地點都能提供出外人員或遠端使用者即時，安全的接入

- ***i*STAR™獨特的對應用程式透明(Application Transparent)的特性，無論是 Web、client/server 應用程式，或是 file sharing，***i*STAR™能夠完全支援，不需要加裝軟體或對應用軟體作修改。支援 Web 、C/S 應用及 File Sharing
- 支援 LAN To LAN 功能（僅 UU200 支援）

3. 提供路由功能：

UU200 和 UUSwitch(/UUExchange)支援路由功能。

- 交換單元網路可以提供最適化路由的選擇
- 具備爲遠端使用者提供最適化路由的選擇

4. 經濟：

***i*STAR™的另一項獨特設計就是能夠適應有 Public IP，及/或僅具備 Private IP 的使用環境，解決了部分企業因爲 Public IP 資源不足，或是擔心伴隨著使用 Public IP 而帶來的安全性問題。

由於可以使用 Private IP，因此企業的應用軟體伺服器能夠被放置在內部網路的任何位置，而保護這些伺服器的也不需要做任何改變，真正的作到了不需要改變既有的網路與防火墻配置，適應不同網路架構的需求。

- 可以共用數位電子憑證

  ***i*STAR™還能夠將一張 SSL 數位電子憑證共用給多個使用 Private IP 的 Site 使用，節省了企業重複申請 SSL 數位電子憑證的費用。

- 充分利用網際網路以降低龐大的通訊成本

  採用了 SSL(Secure Socket Layer)協定，從應用層面建立安全機制，是 Application Sharing 的概念。通訊雙方在應用層建立通訊，除了能確保雙方的安全之外，也大幅降低規劃 IP 網路的複雜工程。

- 控制網路建設、擴充、管理、使用及維護的整體成本（TCO: Total Cost of Ownership）

5. 便於使用和管理：

- UU200 和 UUSwitch/UUExchange 支援 SNMP MIB2 等業界通用的網路標準，便於網路管理員進行管理。
- 使用者介面友好。使用 IE 瀏覽器操作，各種應用都以圖示表示。

1.2 *i*STAR™產品系統架構

***i*STAR™的系統結構如下圖所示：

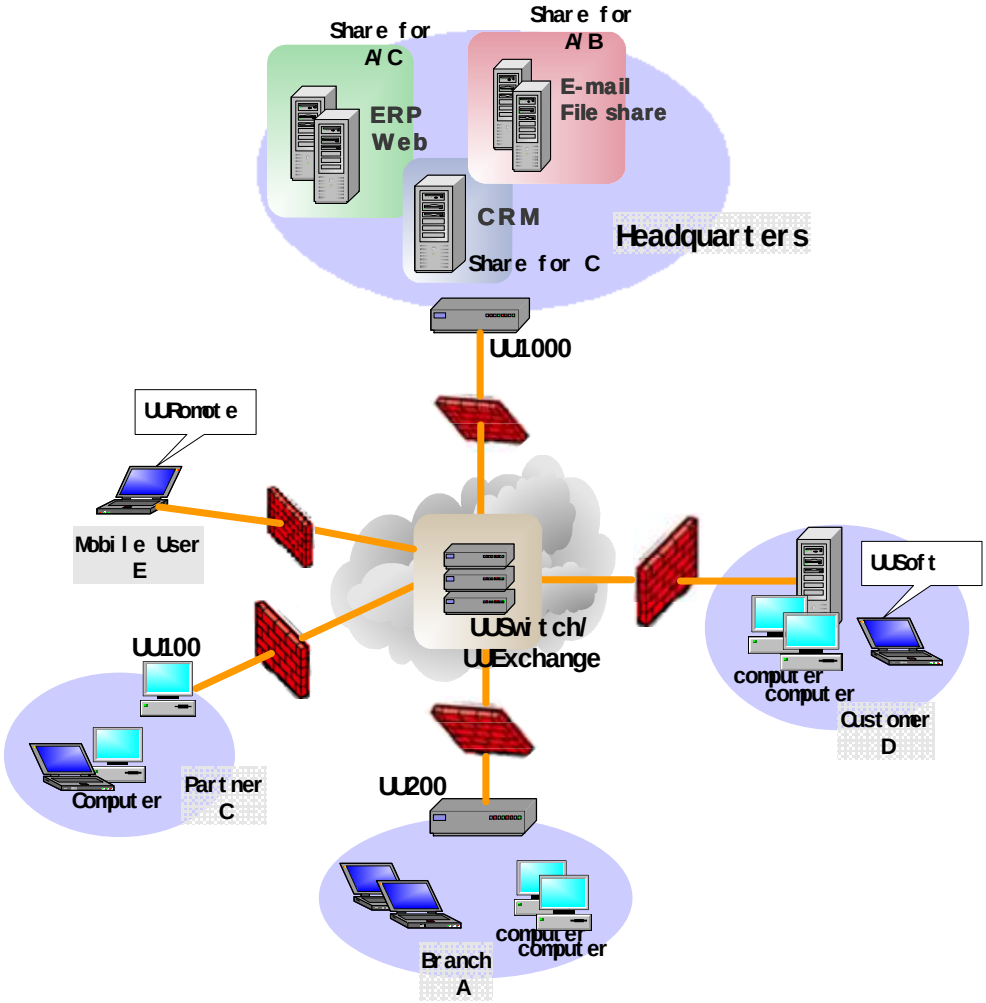


圖 1

如上圖所示，公司總部（headquarter）、合作夥伴(Partner)、分支機構(Branch)和移動使用者(Customer)間建立 ***i*STAR™**系統結構，分別以 UU200、UU100、UU1000 和中間的 UUSwitch(/UUExchange)連接建立安全隧道；公司總部發布共用的應用給特定使用者，合作夥伴、分支機構等使用該些應用，從而實現了 Instant Extranet。UU1000/UU200/UU100 均具備發布單元的功能；個人使用者單元通過 IE/HTTPS 與伺服器相連接。***i*STAR™**技術中主要構成元件簡要介紹如下。

交換單元(UUSwitch/UUExchange)

UUSwitch(/UUExchange) 是 ***i*STAR™**系統結構的中心，它類似於電話系統中的交換中心，是高效的、均衡負載的伺服器群集或群集組，它負責維護著合法使用者資料庫，具有 Public Static IP 地址，在兩方進行應用資料交換之前提供“信令交換”的功能；UUSwitch(/UUExchange)能物理上分佈在多個地點上，透明地轉發應用資料。

發佈單元（Publisher）

發佈單元（Publisher）UU100/UU200/UU1000 位於 ***i*STAR™**中發布應用的伺服器端，它可以將伺服器提供的服務安全的發布。

使用者單元（Subscriber）

即使用者端。個人使用者單元通過 IE/HTTPS 與伺服器相連接。

Registration (Logical naming)

每個發佈單元 Publisher 都必須配置成能夠到達 UUSwitch（/UUExchange），並且都有一個唯一的邏輯名字 UUID，在啓動時就用這個邏輯名字註冊到 UUSwitch(/UUExchange),從而成爲整個 ***i*STAR™**的一部分。所以發佈單元本身不一定需要 Public Static IP 位元元元址。

End to End Security Connectivity

資訊安全的含義主要包含以下幾個方面：使用者端和伺服器端的認證、資訊的私密性、資訊的完整性和授權。***i*STAR™**結構中的發佈單元和使用者單元之間的隧道是基於 SSL 的安全連接，同時滿足以上幾個方面，實現端到端的安全。

第2章 系統安裝

2.1 安裝硬體

1. 設備外觀

UUSwitch（/UUExchange）產品包含硬體、軟體兩部分。它們的硬體在外觀和安裝步驟上基本一樣。您可以依照以下步驟進行安裝：

設備的外觀如下圖 2 所示：

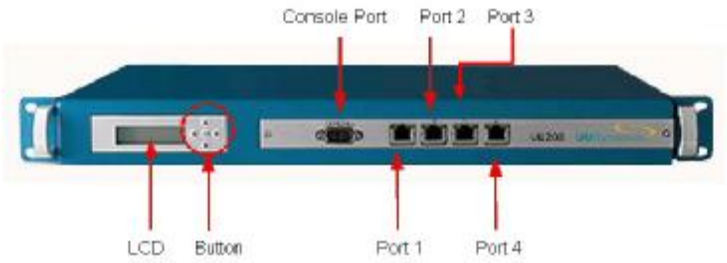


圖 2

正面從左到右爲：

Ÿ LCD 顯示螢幕：分兩行顯示 *i*STAR 底層重要的資訊。例如連接狀態、CPU 狀態、告警等。

顯示位置	回顯內容	說明
Line1	CPU 及 Memory 使用情況。	總是顯示。
Line2	正常情況下顯示連接狀態。異常情況下顯示告警資訊。 告警資訊包括： MemoryShortage CPUOverload InvalidLicense WrongSoftware IPConllision	**MemoryShortage**：當記憶體極值（threshold）達到 98%時顯示。 **CPUOverload**：當 CPU 極值（threshold）達到 80%時顯示。 **InvalidLicense**：當 license 不夠、不一致或過期時。 **WrongSoftware**：當安裝了錯誤的軟體（例如 UUSwitch 軟體）時顯示。 **IPConllision**：IP 位址和內網位址或外網位址發生衝突時顯示。

Ÿ **按鈕：**共五個。（目前暫不使用）

Ÿ **Console 埠**：在初始化時使用。 通過 NULL Modem 線與配置電腦相連接 (串列傳輸速率：38400，校驗：N，資料位置：8，停止位置：1，資料流程控制：N)

Ÿ 乙太埠：共 4 個。

埠 “1” ：爲預設的本地配置埠，首次安裝或恢復原廠設置時，應使用交叉綫連接該埠。

進行配置。

埠“2”：可在配置介面中啓用，用於進行本地配置（使用交叉綫連接）。一旦啓用該埠，埠“1”的本地配置功能即失效。

埠“3”： 可在配置介面中啓用，用於連接叢集（Cluster）中的各台 UUSwitch（/UUExchange）。一旦啓用該埠，則埠“4”的這一功能失效。

埠“4”： 可用於連接叢集（Cluster）中的各台 UUSwitch（/UUExchange）。或可連入網路。

背面爲：

- 電源線接頭
- 電源開關

2. 設備附件

- 電源線、NULL Modem 線、RJ-45 交叉線、CAT-5 UTP 網路線
- 用來配置 UUSwitch（/UUExchange）用的電腦一台（以下簡稱配置電腦）
  i. 具備 10M/100M 乙太網卡
  ii. 具備 Microsoft Internet Explorer 瀏覽器 5.0 版或以上
  iii. 建議使用解析度爲 1024x768 的監視器

3. 硬體安裝。

UUSwitch（/UUExchange）的硬體在外觀和安裝步驟上基本一樣。您可以依照以下步驟進行安裝：

① 連接 *i*STAR 硬體產品的電源線，（可以使用 110V/220V 電源）；

② 用 RJ-45 交叉線將配置電腦的乙太網路埠，連接到 *i*STAR 標示“1”的乙太網路埠；

③ 啓動 *i*STAR 電源；

& 說明：

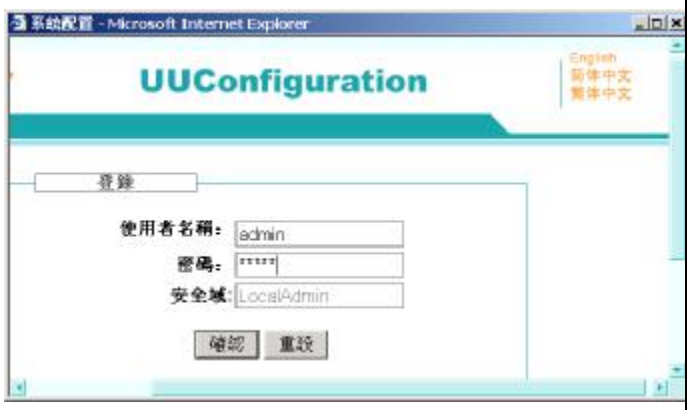
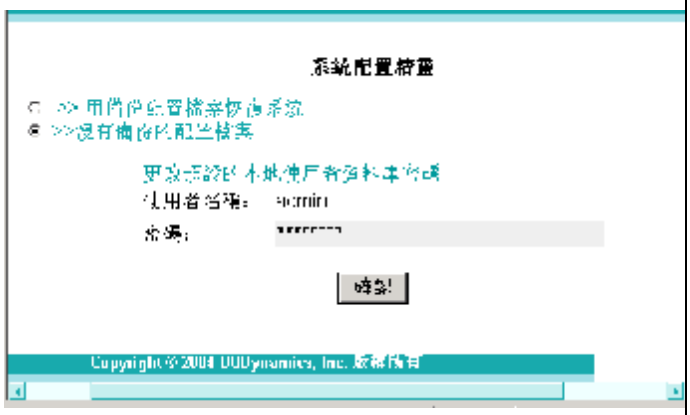
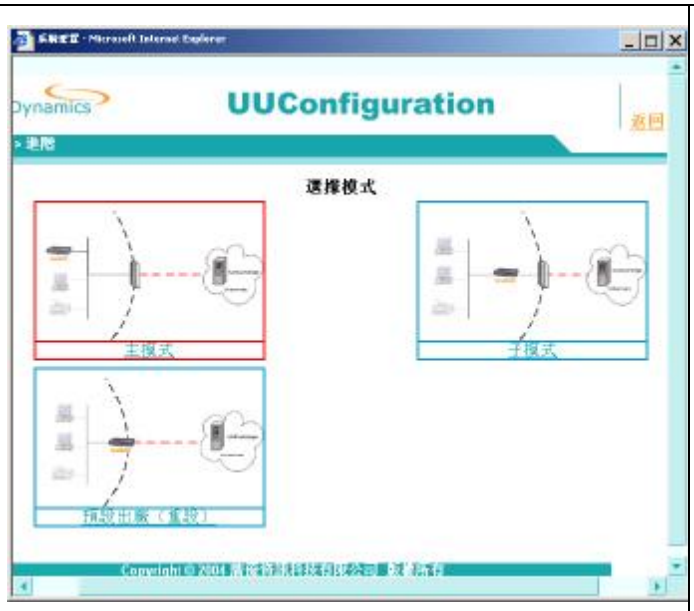
*i*STAR 的出廠預設 IP 位址是“1.1.1.1”，子網路遮罩是 255.255.255.0。

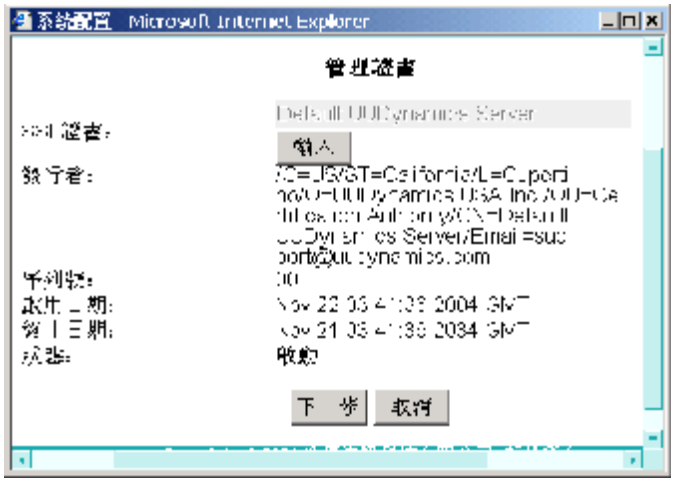
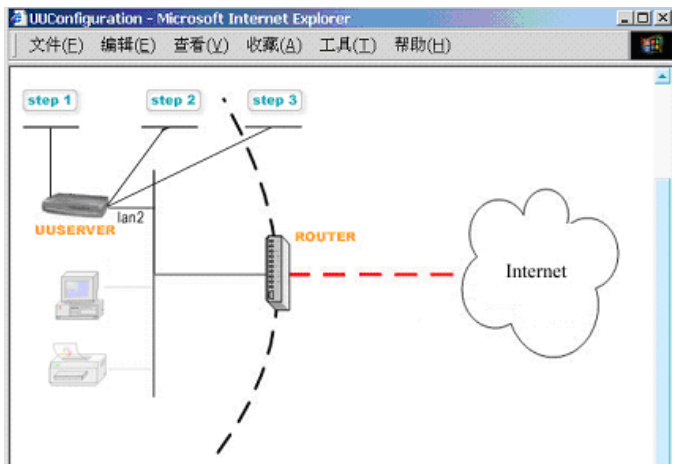
④ 啓動您設定電腦上的 Command Prompt，輸入“*ipconfig /renew*”，待獲得了 1.1.1.2 的位址之後，便可以繼續下面的步驟

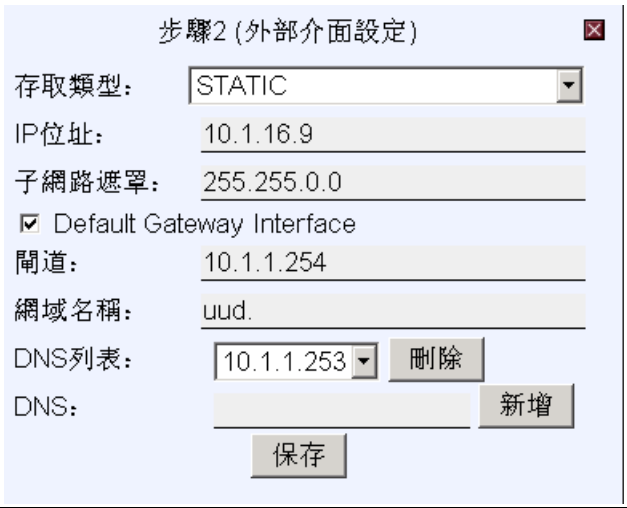
⑤ 啓動配置電腦的 IE 瀏覽器，開始安裝軟體。

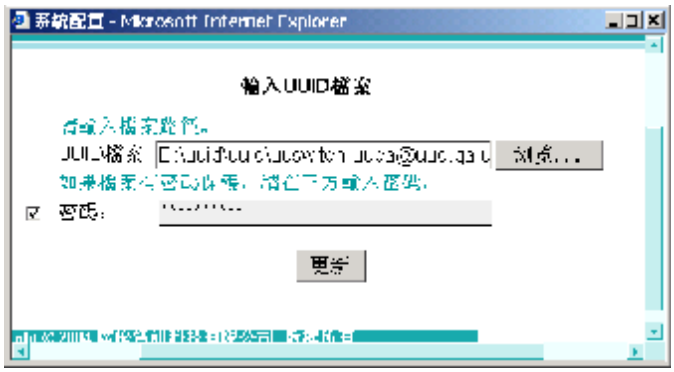
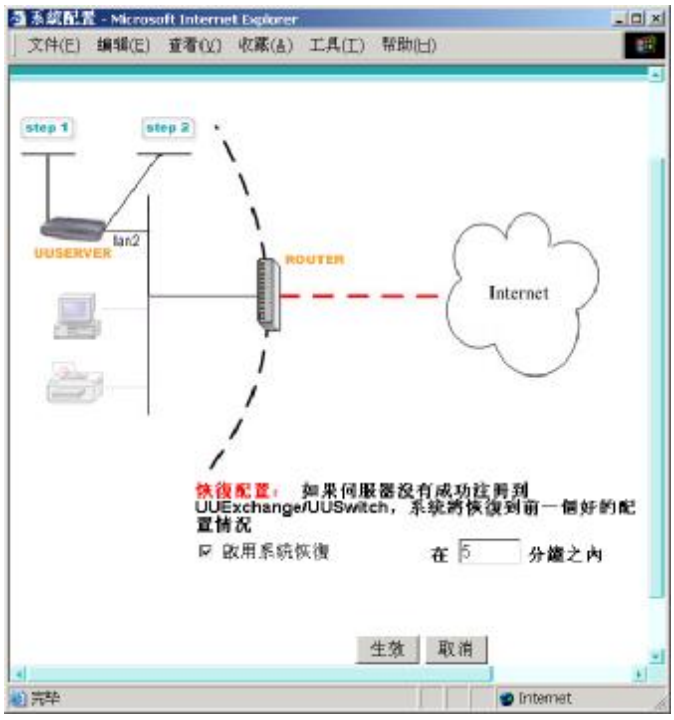
2.2 安裝軟體

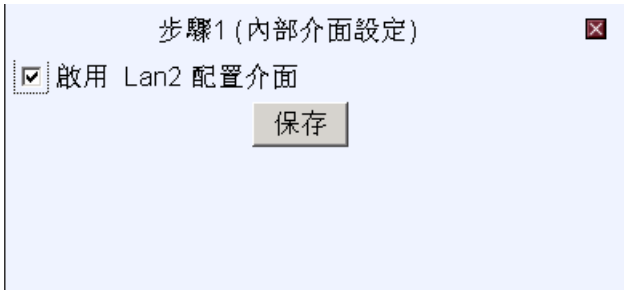
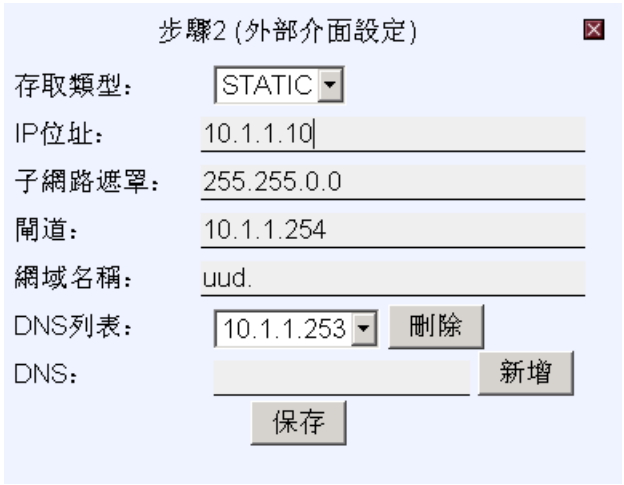
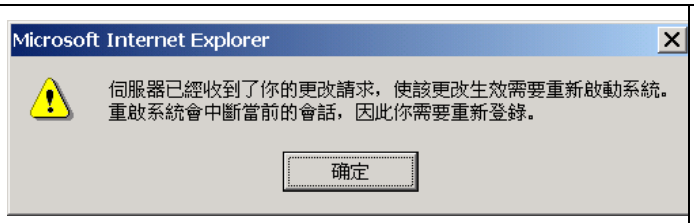
步驟序號	介面	步驟描述
A 軟體安裝		

A-1		請在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”，在彈出的視窗介面中輸入使用者名稱和密碼（兩者都是“admin”），按鍵盤上的 **Enter** 鍵或點選介面中的<確認>按鈕，進入系統配置導引精靈。
A-2		選擇是否重載以前的配置檔案。 Ÿ 如果是初次安裝或者沒有 UUSwitch（/UUExchange）的配置備份檔案，請選擇“沒有備份的配置檔案”選項； Ÿ 如果您要恢復以前備份的 UUSwitch（/UUExchange）的配置，請選擇“用備份配置文件恢復系統”； 爲保護系統安全，請立即修改預設的管理員密碼。 點選下一步進入連接方式的配置。
B 選擇 UUSwitch（/UUExchange）在網路中的放置地址		
B-1		根據您在安裝準備階段預先確定的工作模式，在“主模式”和“子模式”兩種模式中選擇，配置精靈會自動跳轉到該模式下的網路設定介面，進行網路各種參數的設定。如： **B-2：主模式下的網路參數設定** **B-6：子模式下的網路設定** 點選預設出廠（重設）可以恢復至出廠時的預設模式，重新設定各種參數。 **說明：** 兩種模式詳細說明請參見“術語表”。

B-2		**主模式下的網路參數設定** Ÿ 如果您需要匯入準備好的第三方的電子憑證。請點擊<輸入>鍵，在下一個介面中輸入另購的第三方電子數位憑證。 Ÿ 如果使用UUDynamics公司提供的預設的電子憑證，則請點擊<生效>繼續其他配置。
B-3		輸入該證書對應的 Key 檔案，證書檔案和 CA 的證書檔案，所有檔案要求是 Base64 編碼方式。 點擊<更新>，返回上層頁面。 **說明**： 第三方電子憑證的更多資訊請參見“術語表”。
B-4		**說明：** 在網路基礎設定已完成并生效後，當系統管理員重新進入此設定步驟，選上“啓用系統恢復”并在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。

B-4-a		點選“步驟 2”。 1. 配置本台 UUSwitch（/UUExchange）的配置埠。 2. 設定是否以該配置埠的 IP 作爲預設的閘道地址。 **說明：** Ÿ 埠“1”和“2”，均可作爲配置埠，但不能同時啓用。 Ÿ 配置埠（埠“1”或“2”）和埠“4”，只能有一個被用作預設的閘道。
B-4-b		點選“步驟 2”， 配置本台 UUSwitch（/UUExchange）的訪問類型。 “訪問類型”表示 UUSwitch（/UUExchange）的 IP 位址類型。 訪問類型爲“STATIC”,開啓左圖所示介面。 輸入本台 UUSwitch(/UUExchange)的公共靜態 IP 位址。對應的子網路遮罩、閘道及 DNS 等參數會自動從系統讀取。按<保存>儲存。
B-5		在 **B-4** 所示介面上，點選“步驟 3”進行叢集的設定。叢集常用於均衡負載。 **n** 勾選“啓用叢集”可以啓用叢集； 1. 輸入叢集 IP、及對應的叢集子網掩碼；每一台被叢集的 UUSwitch（/UUExchange）需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲 Private IP。 系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UUSwitch（/UUExchange）必須位於同一個子網路。 2. 輸入叢集 IP（開始）、叢集 IP （結束）資訊；以確定同一個叢集的 IP

		位址範圍。 3. 輸入完畢後按<保存>進行儲存 **n** 勾選“啓用 Lan3 叢集介面”表示啓用標示爲“3”的埠作爲叢集的埠； **說明：** 詳細的叢集的說明請參考“術語表”。
B-6		**子模式下的網路設定：** 按<輸入>鍵，在“UUID 檔案名稱：”欄中輸入 uuid 檔案（見 **B-6-a**），並在“UUSwitch（/UUExchange）伺服器”欄中輸入該子模式 UUSwitch(/UUExchange)所從屬的主模式 UUSwitch(/UUExchange)的 IP 位址或 DNS 稱，然後按<下一步>繼續，
B-6-a		點擊<瀏覽>，選擇 UUID 檔案。如果該檔案有密碼保護，請輸入正確的密碼。
B-7		**說明：** 在網路基礎設定已完成并生效後，當系統管理員重新進入此設定步驟，選上“啓用系統恢復”并在“在 □ 分鐘之內”設定相應的時間（如 5 分鐘），表示如果在 5 分鐘內，無法連接到 UUSwitch/UUExchange，網路設定將自動恢復爲原來（改變前）的網路設定。

B-7-a		點選“步驟 1”。設定是否啓用 UUSwitch(/UUExchange)上標示爲“2”的埠作爲配置埠。 如果不啓用，則仍使用預設的埠“1”作爲配置埠。
B-8		訪問類型設定爲“STATIC”時: 輸入本台 UUSwitch(/UUExchange)的公共靜態 IP 位址、及對應的子網掩碼、閘道、DNS 等參數。
C 完成		
C-1		在 **B-4** 介面上，點擊<生效>,使網路設定生效。點擊<確定>結束配置步驟。
C-2		在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”，輸入使用者名稱和密碼（兩者都是“admin”），重新登入，即可開啓左圖所示介面，進行修改設定、發佈應用、管理系統等操作。

第3章 UUSwitch(/UUExchange)部署

初始配置完成的 UUSwitch(/UUExchange)必須要部署 Internet 中（連接方法是將 UUSwitch(/UUExchange)設備的第 **2** 網口與 Internet 通過 **RJ-45 網路線**連接），您可以將 UUSwitch(/UUExchange)託管到 ISP 處或放在自己公司。爲了確保 UUSwitch(/UUExchange)的安全，UUSwitch(/UUExchange)只需要使用埠 443，所以，通常要在 UUSwitch(/UUExchange)的外面安置一個防火墻，只開放埠 443。

第4章 系統維護

完成上述 UUSwitch(/UUExchange)的系統安裝和初次配置之後，您可以隨時進行UUSwitch(/UUExchange)的系統設定。

4.1 熟悉介面操作

4.1.1 進入設定介面

圖 3

配置介面採用 WEB 方式（見圖 3），進入配置介面前需要登錄（從 remote manager 進入時不需要），某些配置後或長時間不操作後也需要登錄。

內部網使用者(通過交叉線與 UUSwitch(/UUExchange)連接)：

在 IE 瀏覽器位址欄輸入“http://1.1.1.1/admin”。

外部網（遠端）使用者：

遠端使用者可以在任何一台聯機到網際網路的電腦上通過 rm 方式開啓遠端使用者應用列表介面，即：在瀏覽器地址欄輸入“https://[*UUSwitch(/UUExchange)的 DNS 名稱/IP 地址*]/rm”。

輸入正確的使用者名和密碼(admin/admin)後，將會出現如圖 3 所示的系統主介面。原因是系統處于安全考慮，設定了“Session Timeout”（會話超時）。Timeout 的時間爲 10 分鐘。

& 說明：

如果使用者超過 10 分鐘後需要對系統繼續進行操作，系統會彈出圖 4 提示資訊，要求使用者重新登錄。

圖 4

重要：

爲了保障系統及內部資料安全，首次進入設定介面後，請務必修改 Admin 的密碼。

- 在系統主介面中，點選“安全管理”下的認證控制。選中某一使用者，點擊<編輯>，即可在開啓的介面中修改該使用者的密碼。
- 通過 IE 瀏覽器，遠端使用者可以在任何一台聯機到網際網路的電腦上通過 rm 方式開啓遠端使用者應用列表介面，在開啓的介面中雙擊“更改密碼”圖示，即可在開啓的介面中修改該使用者的密碼。

介面中各配置項功能簡要介紹如下。

【安全管理】

認證控制： 設定系統的認證類型，進行相關設定。
加密管理：可以用於選擇資料安全傳輸的加密演算法和 Hash 演算法。
本地管理：對本地管理進行授權，授權使用者可以對系統進行本地管理。
遠端管理：對遠端管理進行授權，授權使用者可以對系統進行遠端管理。
管理 UUID：UUID 管理，用於 UUID 和 Domain 的增加、移除、啓動等操作。

【Advanced】

選擇模式：模式選擇。UUSwitch(/UUExchange)有兩種選擇模式，即主模式和子模式（兩種模式的說明請參見“術語表”）；另一種模式是出廠的設定，點選該模式，即清除之前的所有設定資訊，返回出廠時的最始設定。

【網路設置】

網路設置：設定 UUSwitch(/UUExchange)的相關資訊（包括公共靜態 IP 位址、子網掩碼、閘道、DNS 等），以及主模式 UUSwitch(/UUExchange)的叢集設定。

【系統管理】

輸入配置：將原來保存好的設定檔案輸入到系統中。
輸出配置：將系統中已配置的設定檔案輸出到指定的檔案夾保存。
更新系統：輸入升級檔案，升級當前的版本。
故障檢修：選擇 Ping、TraceRoute、Netstat 命令檢測系統的網路運行狀況。
查看狀態：查看系統的狀況，包括 UUServer 的 UUID 類型、系統的模式、系統的當前運行狀態等。
查看系統性能：查看系統的各種的統計資訊。
查看日誌：查看日誌。包括查看系統每天指定時間段中，由重點到詳細的日誌情況，并可隨時保存日誌，以便隨時審閱。
日誌控制：系統日誌的設定。
警告通知設定:系統報警級別的設定。
系統設置：系統伺服器的時間設定

4.1.2 介面間的跳轉

IE 瀏覽器上自帶的“Forward（前進）”、“Back(後退)”等按鈕及“文件”、“編輯”等功能表均不再出現在介面上。

- 返回上一級介面，請點擊<返回>或<取消>。
- 保存配置的修改，請點擊<確認>或<保存>鍵。

4.1.3 退出設定介面

退出設定介面前，請退回到圖 3 所示設定介面，點選 登出 退出。否則，再次（或用同樣的使用者名稱從其他機器）登錄時，系統將提示以下資訊 ：
“使用者 [*username*] 目前已登錄到本系統”

此時，如果使用者或者管理權限更高的使用者了勾選 “停止使用者[*username*]”重新登錄系統，則將強行中斷之前以該使用者名稱登入的其他會話。
例如：使用者在上一次非正常退出後，可以勾選該選項，強制停止自己的帳號，重新登錄系統。或者，管理員可以停止其他只有“唯讀”許可權的使用者帳號，但不能停止其他管理員帳號（詳細內容請參考“設定本地/遠端管理員”章節）。

& 說明：
如果勾選“*停止使用者*[*username*]”時出錯（如圖 5），有可能是因爲您沒有許可權使該使用者失效。如果仍要登錄，請聯繫系統管理員。

圖 5

4.1.4 使設定生效

“生效”表示使你的設定生效。
修改配置後，點擊<確認>或<保存>鍵後進行保存。保存成功後，還必須點擊<生效>，設定方可生效（如圖 6）。

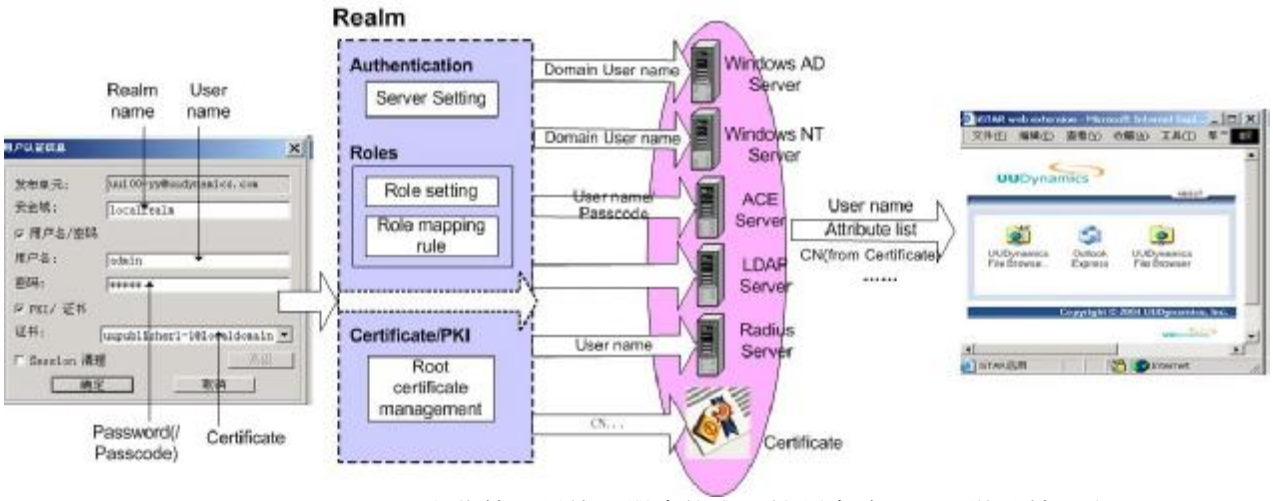
重要：
- 以下七項設定完成後，點擊<生效>會中斷 Session，同時系統會提示使用者重新 Login。因此，建議您：避免在系統繁忙時改變這幾項設定。
  網路設置；iSTAR 設置；認證控制；設定匯入
  選擇模式；管理許可證；系統升級；
- 按<生效>後有時會重新啓動系統的服務，這時介面上可能會出現“非法 IP”等資訊，這時需要稍等片刻，輸入 http://1.1.1.1/admin，重新進入設定介面。

圖 6

4.2 用戶管理

相關概念：

UUSWITCH(/UUEXCHANGE)用戶亦即 UUSWITCH(/UUEXCHANGE)管理員（或使用者）。管理者可以在本地或遠端對 UUSWITCH(/UUEXCHANGE)進行設定和維護，包括管理使用者帳號，升版系統、管理 UUID（僅限主模式）等。



UUSWITCH(/UUEXCHANGE)允許管理員使用嚴密的安全控制方式，層層驗證接入安全。包括登入身份驗證、授權和應用級驗證策略等，杜絕了各種未經認證和授權的非法連接。

爲了實現這種安全控制思想，伺服器端（UUSWITCH(/UUEXCHANGE)）需要完成相關的設定。以下對涉及到的各種概念進行說明和舉例。

- 認證：身份驗證。系統使用認證伺服器或證書驗證使用者端傳來的使用者名稱、證書中的 DN 等代表身份的資訊。身份驗證有以下幾種途徑：
  1. 使用者端輸入的使用者名稱/密碼。如果使用者名稱和密碼不符，則驗證失敗。
  2. 使用者端導入的證書的 CN 等屬性驗證。證書的可信任性由簽發的根證書負責驗證。
  3. 認證伺服器上該使用者相應的屬性。使用者屬性需要根據使用者名稱在指定的認證伺服器檢索和匹配。
  4. 一次性有效的密碼。例如 RSA 的 token code。這種一次性有效的密碼通常用於雙因數身份認證。這種方式的認證要求使用者輸入使用者名稱、passcode（PIN＋Token code）。
- 授權：應用授權。發布應用時通常將應用授權給已通過身份驗證的使用者。授權依據通常是以下一種或多種資訊：
  1. 代表使用者身份的使用者名稱
  2. 使用者隸屬的組列表
  3. 使用者對應的角色（從證書中的屬性以及使用者在認證 伺服器上對應的屬性對應而來）。

- 規定：安全管理綜合策略。管理員可以根據安全級別組合各種包括身份驗證、授權在內的所有的安全管理方法。
  例如，當安全需求極高時，可以設定一種較嚴密的規定：使用雙因數身份認證（使用者名稱 + 證書）和通過另一張證書授權，即：Client 端必須同時提供使用者名稱和證書，并通過驗證另一張證書是否給該使用者授權或授權該使用者使用何種應用。
- Certificate/PKI（根證書）：證書。由 CA 簽發，包含使用者 CN 或其他屬性等安全資訊。
  通常用於驗證使用者的身份或對通過身份驗證的使用者進行應用授權。
- 角色:角色定義。
  PKI 和 Radius 類型的伺服器中，通常將一組相同屬性定義爲一個角色。使用者屬於某一角色意味著他（/她）具有相應的所有屬性。UUSwitch（/UUExchange）在 PKI 和 Radius 兩種類型的安全域中引入了角色這一概念，目的是方便將某一應用授權給某一角色（即具有某些相同屬性的使用者）。
  角色通常在驗證 AD/Radius 伺服器上的使用者身份和應用授權時作爲主要依據。
- 安全域：每一個使用者隸屬於一個或多個安全域。安全域涵蓋了上文提及的一個或多個方面，包括認證、授權、規定、Certificate/PKI、角色。
  使用者隸屬于某個安全域，意味著該使用者將使用該域中指定的綜合安全管理策略，包括：在指定的認證伺服器或（/和）證書進行身份驗證，驗證通過後，UUSwitch(/UUExchange)將根據指定的授權策略或（/和）證書對使用者進行應用授權。安全域的使用可以參考以下例子。

& 說明：
本系統中有一個預設的安全域：LocalAdmin。LocalAdmin 中設定了一個預設的伺服器 — LocalUsers，該伺服器中有預設的 User/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。
LocalAdmin 中不允許設定 Certificate/PKI。

實例：

例一：

I 背景

某企業爲大型銀行。使用者類型包括：局域網使用者、Radius、遠端存取使用者……
其中：

User1：Local 使用者，安全需求一般。在 LocalSever 中驗證使用者名稱身份。企業的合作夥伴或代理商適合使用這種使用者身份連入企業的內部網。
User2：Local 使用者，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。
User3：Radius 使用者。安全需求高，在 Radius 伺服器上有使用者名稱/密碼，屬於某一角色。
User4：遠端使用者，安全需求極高，需要使用使用者名稱/Passcode(PIN + Token cade)，在 ACE 伺服器上驗證身份進行雙重身份認證。
Group1：成員包括 User1。

I 身份驗證設定

1. 預置以下幾個伺服器。
   RadiusUsers：類型爲 Radius；
   ACEUsers：類型爲 ACE/Server；
2. 預置以下幾個安全域。
   LocalAdmin：預設。不需增刪也不能更改。
   PKIRealm: 新增。僅需要驗證證書。

設定項	值	說明
使用以下伺服器進行認證/制定策略	None	類型：無
通過 Certificate/PKI 認證	True	選中該選項，並點擊<管理證書>選擇信任的根證書。

RadiusRealm：新增。用於驗證 Radius 域的使用者。選擇 MyRadius 作爲認證/policies 伺服器。

設定項	值	說明
使用以下伺服器進行認證/制定策略	RadiusUsers	類型：Radius
經由 Certificate/PKI 認證	False	不選中該選項。
角色		點點擊<增加/編輯映射規則…>，可以增加/修改角色 對應規則。.

ACERealm：新增。用於驗證遠端使用者。

設定項	值	說明
使用以下伺服器進行認證/制定策略	ACEUsers	類型：ACE
通過 Certificate/PKI 認證	False	不選中該選項。

3. 將 Users/Groups 按安全需求加入到相應的安全域中。
   User1/Group1：加入 LocalAdmin。使用使用者名稱/密碼在 LocalServer 上認證身份。
   User2：加入 PKIRealm，沒有使用者名稱/密碼，但持有某 CA 簽發的證書。通過證書中 DN 或其他屬性驗證使用者身份。驗證通過後，從證書中獲取該使用者的屬性，進行應用授權。
   User3：加入 RadiusRealm，在 Radius 伺服器上驗證使用者名稱/密碼，驗證通過後，從 Radius 伺服器上獲取該使用者的屬性，進行應用授權。
   User4：加入 ACERealm，使用使用者名稱/Passcode(PIN +Token code)在 ACE 伺服器上驗證身份。

例二：

- 背景

某企業爲中小型企業。使用者類型包括：局域網使用者、遠端存取使用者……
其中：
User1：遠端存取使用者，安全需求一般。在 LocalSever 中有使用者名稱/密碼。企業的合作夥伴或代理商可使用這種使用者身份連入企業的內部網。
User2：Windows NT 域使用者。安全需求較高，在 Windows NT 伺服器上有使用者名稱/密碼。需要 Windows NT 域使用者名稱進行身份認證。
Group1：成員包括 User1。群組的設定可參考使用者的設定。

- 身份驗證設定

1. 預置以下幾個伺服器。
   LocalUsers：預設。不需增刪也不能更改。類型爲 Local；
   NTUsers：類型爲 Windows NT。
2. 預置以下幾個安全域。
   LocalAdmin：預設。不需增刪也不能更改。
   NTRealm: 新增。需要驗證 NT domain 的使用者名稱/密碼。

設定項	值	說明
使用以下伺服器進行認證/制定策略	NTUsers	類型：Windows NT
經由 Certificate/PKI 認證	True	選中該選項，並點擊<管理證書>選擇信任的根證書。

3. 將 Users/Groups 按安全需求加入到相應的安全域中。
   User1/Group1：加入 LocalAdmin。使用使用者名稱/密碼在 LocalServer 上認證身份。驗證通過後，進行應用授權。

User2：加入 NTRealm，通過企業的 Windows NT 伺服器驗證使用者身份。驗證通過後，進行應用授權。

4.2.1 添加認證伺服器和使用者

添加伺服器：

1. 在系統主介面中（如圖 3）的“安全管理”下，點選 認證管理。
2. 點選圖 14 中的<增加/編輯伺服器>，進入圖 7 所示介面。

圖 7

3. 點擊<增加>，進入圖 8 所示介面。從“伺服器類型”列表中選擇類型，選擇不同的類型後，會出現不同的介面，填入相應的資料。各輸入項的填寫說明請參見下表。

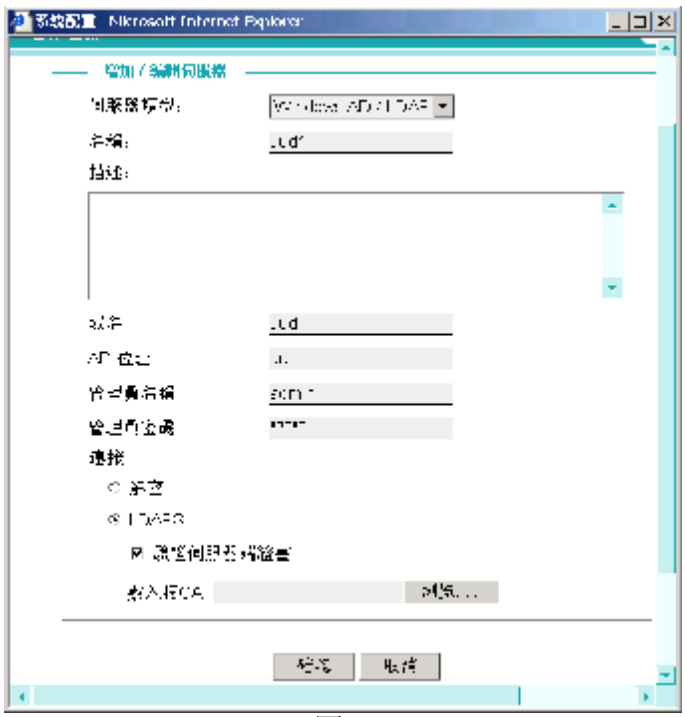


圖 8

4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。

5. 點擊<生效>，保存設定。

表：各輸入項的填寫說明

伺服器類型	輸入項		說明
Window AD/LDAP（Window AD/NTLM）	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	功能變數名稱稱		輸入對應的 DNS 名稱
	AD 位址		輸入該域服務器的 IP 位址或功能變數名稱稱（Window AD/LDAP 類型中如果下面的“連接” 選項爲 LDAPS 時，必須輸入功能變數名稱稱）
	管理員名稱/管理員密碼		輸入登錄該域的管理員使用者名稱、密碼
	連接（僅 Window AD/LDAP 類型）	解密	連接過程不加密
		LDAPS	驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書
			導入根 CA：導入簽發 Certificate 的根 CA
LocalUsers	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	使用者		在該伺服器中增加使用者
	群組		在該伺服器中增加群組
Windows NT Domain	名稱		輸入 NT 伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	網功能變數名稱稱		輸入該 NT 域的名稱
	網網網域控制器		輸入該 NT 域中的網網域控制器的 IP 位址或 DNS 名稱
	管理員名稱		輸入對 NT 伺服器管理員的登入帳號
	管理員密碼		輸入對 NT 伺服器管理員的登入密碼
LDAP(可參考表格下的實例）	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	類型		Ÿ Active Directory; Ÿ OpenLDAP; Ÿ Generic LDAP with Static Groups：除了以上兩種類型之外的其他類型
	伺服器		LDAP 伺服器的 IP 位元址或名稱
	使用預設埠		可選項。預設埠號爲： Ÿ 不加密：389 Ÿ 使用 SSL 協定加密：636 如果沒有選中該項，則需要另行設定埠號
	授權需要經過 LDAP 搜尋	Admin DN	指定在 LDAP 伺服器上搜尋管理員的目錄路徑
		密碼	輸入該管理員的密碼。
	指定如何找出使用者輸入	Base DN	指定在 LDAP 伺服器上搜尋使用者的目錄路徑
		屬性	指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲使用者名稱
		過濾器	設定過濾條件
	決定群組成員	Base DN	指定在 LDAP 伺服器上搜尋組的目錄路徑
		屬性	指定以哪個屬性類型（可以是 LDAP 伺服器管理員定制的屬性類型）作爲組名稱
		過濾器	設定過濾條件
		成員屬性	指定 LDAP 伺服器上的屬性類型(可以是 LDAP 伺服器管理員定制的屬性類型)，用於驗證靜態組的成員。
	連接	解密	連接過程不加密

		LDAPS	驗證伺服器端證書：選中該選項後，連接不但被加密，還需要驗證伺服器提供的證書 導入根 CA：導入簽發 Certificate 的根 CA
Radius	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	Radius 伺服器		輸入 Radius 伺服器的 IP 位址
	Radius 埠		輸入 Radius 伺服器的埠
	Shared Key		輸入 Shared Key
ACE/Server	名稱		輸入伺服器名稱
	描述		輸入對該伺服器的描述（可選）
	導入至		導入.REC 文件後，系統自動記錄幷回顯導入的時間
	導入新的配置檔		將相應的 .REC 文件導入。該文件由 ACE 伺服器分配。
	刪除節點 Secret		用於和 ACE/Server 端的同步。如果在某一端刪除了節點 Secret，必須在另一端也相應刪除。

舉例：LDAP 類型伺服器的目錄如下

dc= qa,dc=com
　Ou=people
　　Uid=tester1
　　Uid=tester2
　Ou=group
　　Cn=test
　　Cn=test1

說明：

管理員	DN：cn=root,dc=qa,dc=com
使用者	屬性：cn； 過濾: objectclass=person
組成員	屬性：cn； 過濾: objectclass=posixgroup, 成員屬性：MemberUid

（test、 test1 爲群組。tester1、 tester2 爲使用者，配置見圖 9）

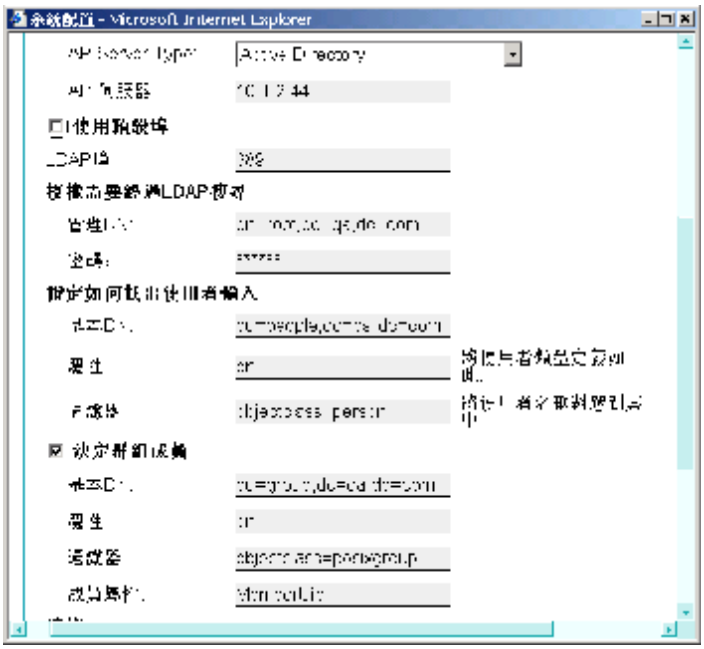


圖 9

& 說明：

Ÿ **Windows AD/LDAP** 伺服器與 **Windows AD/NTLM** 伺服器比較

前者有三條限制：

1. Windows AD/LDAP 方式下，“名稱”欄內填入的名稱必須與下一欄所指定 IP 的伺服器中存在的 AD 名稱一致。
2. Windows AD/LDAP 方式下，僅能搜索出 1000 條以下的“遠端管理員”記錄

（有關搜索遠端管理員記錄的內容請參考“**錯誤! 找不到參照來源。**設定本地（/遠端）管理員”）。

3. Windows AD/LDAP 方式下，在對應的 Windows AD 域中增加的組可能需要 20 分鐘後才能生效。增加的組包括“新增的新組”和“刪除後增加的同名稱組”。
   該組中的使用者如果無法登錄 UUSwitch(/UUExchange)，請稍候再試。

Ÿ **LocalUsers** 伺服器

LocalUsers 是預設的伺服器類型。如果選擇 LocalUsers 類型的伺服器，則表示選擇在 UUSwitch(/UUExchange)中單獨建立一個使用者認證檔案。這個檔案是經過加密保護的。換言之，使用者應使用本系統定義的帳戶和密碼連入。該伺服器中有預設的使用者/密碼：admin/admin。預設的使用者 admin、伺服器和安全域不能被刪除。這樣可以保證至少有一位具有“唯讀/更改”許可權的使用者存在。

當選擇該認證類型時，每台 UUSwitch(/UUExchange)可管理 1000 個使用者帳號或組。

添加用戶：

Ÿ 僅使用證書的認證方式，不需要添加使用者。使用者存取 UUSwitch(/UUExchange)時，僅需提供證書即可。

Ÿ 在添加 LocalUsers 伺服器時，可以通過點擊<使用者>添加使用者，并設定密碼。

Ÿ 在添加其他類型伺服器時，只要按照表格中的說明填寫各輸入項，UUSwitch(/UUExchange)會自動到指定的認證伺服器獲取該伺服器中的符合條件的使用者列表。這種結合現有的認證伺服器進行用戶認證的方式，使得企業可以使用統一的安全認證策略，無需另外添加用戶。

4.2.2 添加證書

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。
2. 點選圖 14 中的<增加/編輯根證書>。在介面中點擊<增加>，在下圖所示介面中輸入相應的證書資訊。
   “證書約束條件”欄用於輸入證書的限制規則。其語法結構爲：
   [*系統變數名稱*].[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。
   舉例：
   ①Certattr.CN =’Zhang san’含義爲：證書中 CN 必須爲 Zhang san。
   ②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

   & 說明：
   ***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，
   User 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，
   User.groupname 表示該使用者名稱所屬的群組。
   Userattr 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。
   Certattr 類 包括：C,CN,L,O,OU,Email 等證書的屬性。
   操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。
3. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
4. 點擊<生效>，保存設定。

4.2.3 添加角色

如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需

要預先定義角色。以便設定規定將相應的角色與 Radius 伺服器或證書中的用戶對應起來（見圖 15）。

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。
2. 在圖 14 所示介面，點擊<增加/編輯角色>。開啓圖 10 所示介面。
3. 點擊<新建>，進入圖 11 所示介面。輸入角色名稱。

圖 10

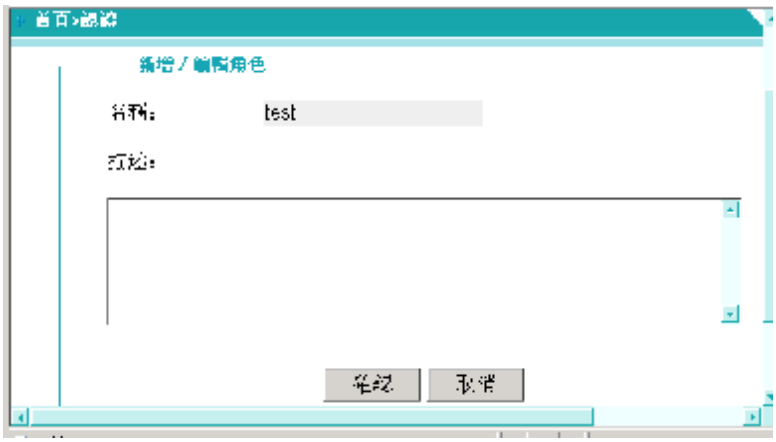


圖 11

4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
5. 點擊<生效>，保存設定。

4.2.4 檢查用戶端的運行環境

在 Server 端設定主機檢查器規則的步驟：

1. 在圖 14 所示介面，點擊<增加/編輯主機檢查器>。開啓設定介面。
2. 點擊<新增>，在開啓的頁面中輸入新規則的名稱。

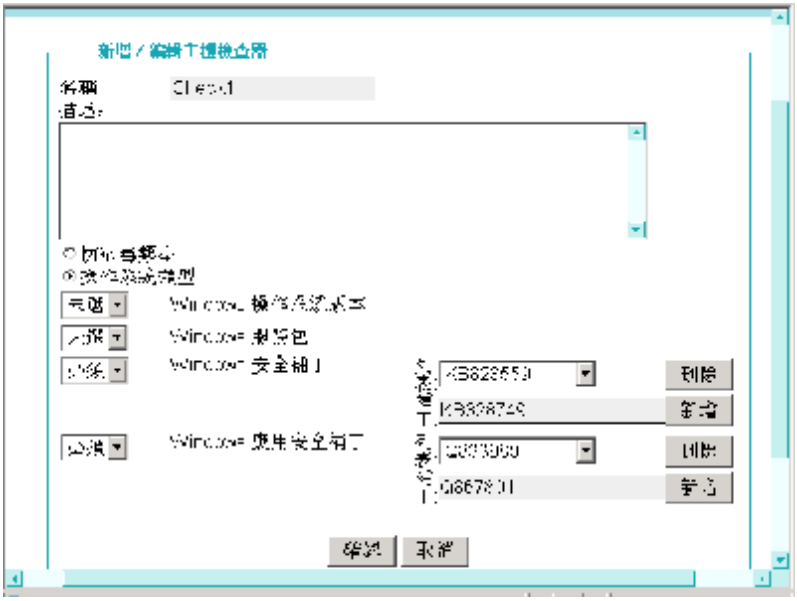


圖 12

3. 選擇對何種類型的運行環境進行檢查：
   - Ÿ 點選“防病毒類型”，可以檢測用戶端是否使用指定的防毒軟體的類型；
   - Ÿ 點選“作業系統類型”，可以檢測用戶端是否使用指定的作業系統、服務包、安全補丁以及應用安全補丁；可以將新的安全補丁和應用安全補丁 ID 加入列表，以便選擇。
     例如： KB828749（Windows 2000 補丁）、Q867801（IE 補丁）。
   - Ÿ 如果選擇了“必須”選項，則要求用戶端運行環境必須與其後的設定相吻合；
   - Ÿ 如果選擇了“拒絕”選項，則如果用戶端運行環境與其後的設定相吻合，該 UU100 將會拒絕用戶端的相應操作。
4. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
5. 點擊<生效>，保存設定。

4.2.5 添加安全域

添加安全域之前，應預先準備必須的伺服器、角色或證書等。準備的流程可參考下圖：

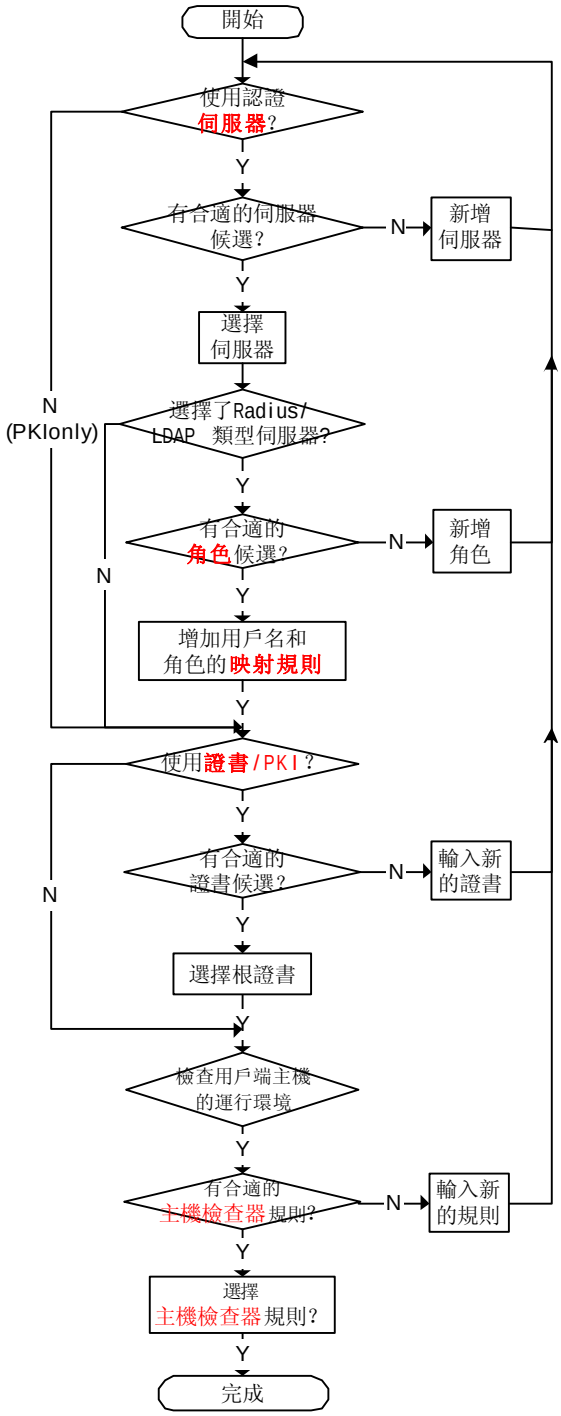


圖 13 設定流程圖

1. 在系統主介面中（如圖 3）的“安全管理” 下，點選 認證控制。

圖 14

2. 在圖 14 所示介面上點擊<增加>，可以增加新的安全域。
   選中列表中某個安全域，點擊<編輯>，可以修改該安全域的屬性。
3. 輸入或修改安全域的名稱。如果需要對該安全域進行描述，請在“描述”欄內輸入說明性文字。
   例如圖 15 中，安全功能變數名稱稱：RadiusUsers。

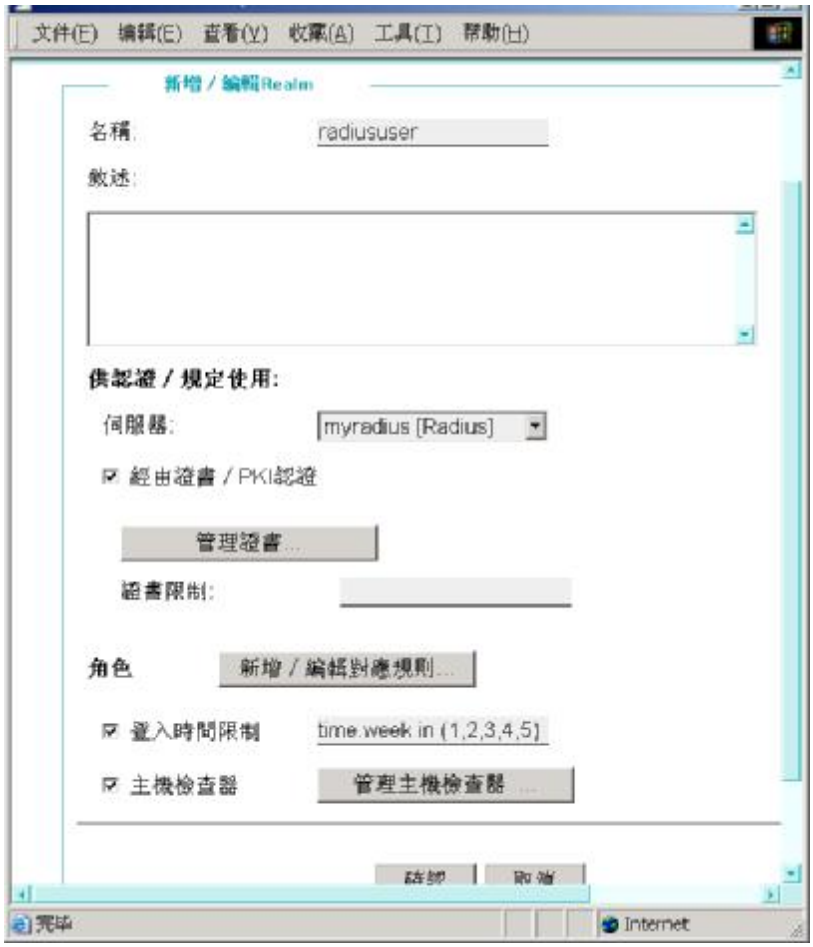


圖 15

4. 在“伺服器”欄選擇需要在哪個伺服器上進行使用者身份驗證。例如圖 15 中，選擇伺服器 MyRadius。在列表中選擇伺服器後，則直接轉至下一步繼續其他操作。但是如果列表中沒有您所需要的伺服器，請先添加伺服器。
5. 如果需要驗證 Client 端使用者提供的證書，請勾選“通過 Certificate/PKI 認證”。否則，直接跳轉至下一步（步驟 7）。

點擊<管理證書>，可以選擇已有的證書。如果沒有需要的證書，請先添加合適的證書。

6. 如果認證伺服器指定了除 “None”（僅使用 PKI）或“Radius”兩種類型之外的其他類型伺服器，跳轉至步驟 9。
   如果認證伺服器指定的是“None” （僅使用 PKI）或“Radius”類型的伺服器，則還需要爲角色設定相應的規則（見圖 15）。
7. 在圖 15 所示介面中點擊<增加/編輯映射規則…>，進入所示圖 16 介面。

圖 16

以 Radius 伺服器爲例：

點選圖 16 介面上的<增加>，進入圖 17 所示介面增加新的規則。

增加規則的內容包括：根據 Radius 伺服器中的使用者屬性，設定過濾條件，篩選出所有的符合條件的使用者，然後將這些使用者歸入某一角色中。這樣，當對某個角色進行授權或其他操作時，實際上是對所有符合規則中過濾條件的使用者同時進行操作。其語法結構爲：

[*系統變數名稱*].[*屬性名稱*]＋[*操作符*]＋[*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

舉例：

①圖 17 中的規則含義爲：Radius 伺服器中所有屬性 service-type 取值爲 framed-user 的使用者都屬於角色“admin” 。

②Certattr.CN =User.name 含義爲：證書中 CN 必須和登錄時所用的使用者名稱一致。

③當“規則”列爲空的含義爲：Radius 伺服器中所有使用者都屬於指定的角色。

& 說明：

***i*STAR™**定義了三類系統變數：User 類、Userattr 類、Certattr 類。其中，

User 類包括 name、groupname 屬性。User.name 表示登錄時所用的使用者名稱，User.groupname 表示該使用者名稱所屬的群組。

Userattr 類 包括：Service-Type、Framed-IP-Address、Framed-IP-子網掩碼等用戶屬性。

Certattr 類 包括：C,CN,L,O,OU,Email 等證書的屬性。

操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

圖 17

8. 設定完畢後，重復點擊<確認>，直到返回圖 15 所示介面。
9. 如果要限制使用者的登入時間，可以選中“登入時間限制”核取方塊，幷輸入約束條件。

   約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：time.[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

   & 說明：

   此處的 time 爲表示時間的系統變數名稱。

   屬性名稱包括 year, month, day, hour, minute, second, week。其中，

   year 表示 4 位數年份；**month** 表示月份；**day** 表示日期；

   hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；

   操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

   舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，幷在驗證成功後登入系統：

   (time.year =2005) and (time.hour between 8 and 18)
10. 設定完畢後，點擊<確認>返回圖 15 所示介面。
11. 如果要檢測用戶端的運行環境是否符合要求，請勾選“主機檢查器”選項，幷點擊<管理主機檢查器>按鈕。在開啓的視窗中選擇檢測規則。

    在”符合時便停止”列中：

    - 點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者登入。
    - 點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。如果不符合該規則，則拒絕該使用者登入。

    說明：

    - 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。
    - 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法登入該安全域。

圖 18

12. 設定完畢後，重復點擊<確認>，直到返回圖 14 所示介面。
13. 點擊<生效>，保存設定。

4.2.6 設定本地（/遠端）管理員

在系統主介面中（如圖 3）的“安全管理”之下，按下本地管理會出現如圖 19 的視窗；用以增加或移除本地系統管理員。按下 遠端管理 會出現如圖 20 的視窗；用以增加或移除遠端系統管理員。

ⅰ 注意：

1. 在本地管理 中添加的使用者爲本地管理員，能且僅能從本機登入 UUSwitch(/UUExchange)系統管理介面。
2. 在遠端管理 中添加的使用者，遠端系統管理員必須首先是本地管理員，即必須先在本地管理 中加入該使用者名稱。

Ÿ 本地管理：

1. 如圖 19，本地管理員對 UUSwitch(/UUExchange)的訪問策略爲“拒絕”，意即使用者列表中所有的使用者都不能訪問。
2. 在“使用者列表”選項組中選擇使用者類型爲“使用者”或是“群組”。在選項組下的“使用者列表”列表中勾選可以通過本地方式存取 UUSwitch(/UUExchange)的使用者(/組)，並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者（/組/角色）。
3. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：
   唯讀:表示該使用者對系統管理介面有“唯讀”許可權。
   更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
4. 以上步驟完成後，點擊<生效>保存設定結果，幷返回到圖 3 系統主介面。

Ÿ 遠端管理：

1. 如圖 20 所示，爲保證管理員遠端管理時建立的 SSL 連接的安全，您可以設定允許會話持續的最長時長和允許會話空閑的最長時長。超過設定的時長，系統會自動斷

開這次連接。

2. 如果勾選“允許同一使用者多次訪問”， 則同一管理員再次（或使用同樣的使用者名稱從其他機器）獲取管理專案列表時，不影響之前以該使用者名稱管理專案列表的其他會話。
   反之，如果不勾選該選項，則會強行中止之前的所有以該使用者名稱獲取管理專案列表的會話。
3. 選擇需要進行陽城管理的應用服務，點擊<編輯>，進入圖 21 所示介面。
4. 設定是否對該服務使用加密、哈希以及壓縮演算法。
5. 點擊<規定>設定，進入圖 22 所示的視窗。輸入您爲這個規定所取的名稱；目前UUSwitch(/UUExchange)能提供的策略包括：

   Ÿ 驗證證書：
   可以指定證書，在使用者登入、獲取應用時驗證用戶端是否提供了正確的證書。此外，還可以對該證書設定限制條件。。

   Ÿ 限制存取時間：
   如果要限制使用者的存取時間，可以選中“存取時間限制”核取方塊，幷輸入約束條件。
   約束條件所遵循的語法結構與設定 Radius 伺服器的規則類似，其語法結構爲：
   time.[*屬性名稱*] [*操作符*] [*屬性值*]（或另一 [*系統變數名稱*].[*屬性名稱*]）。

   & 說明：
   此處的 time 爲表示時間的系統變數名稱。
   屬性名稱包括 year, month, day, hour, minute, second, week。其中，
   year 表示 4 位數年份；**month** 表示 2 位數月份；**day** 表示 2 位數的日期；
   hour 表示小時（按 24 小時制）；**month** 表示分鐘；**second** 表示秒；
   操作符 是 sql 的操作符，如 =,!=,>,<,like,in 等。

   舉例：下面的約束條件限制了使用者只能在 2005 年，8:00～18:00 驗證身份，幷在驗證成功後存取應用列表：
   (time.year =2005) and (time.hour between 8 and 18)

   Ÿ 檢測用戶端運行環境：
   如果要檢測用戶端的運行環境是否符合要求，可以點擊<管理主機檢查器>。選擇在安全域設定時預先加入的檢測規則。
   在”符合時便停止”列中點選“不是”：則檢測到符合該規則後，繼續檢測下一規則；如果不符合該規則，則拒絕該使用者以遠端管理員身份登入管理介面。
   在”符合時便停止”列中點選“是”：則一旦檢測到符合該規則後，即停止繼續檢測，允許該使用者以遠端管理員身份登入管理介面。如果不符合該規則，則拒絕該使用者以遠端管理員身份登入管理介面。

   說明：
   Ÿ 在“符合時便停止”列中選擇“是”的規則應被放置在所有選擇“不是”的規則之後，否則當用戶端的運行環境符合該條設定爲“是”的規則後，將不會繼續檢測，這樣，其後的規則將不會再有機會被檢測。
   Ÿ 如果“防病毒類型”和“作業系統類型”兩種類型都有規則被選中，則要求同時檢測用戶端主機安裝的防病毒軟體和系統設定（系統設定包括：作業系統版本、系統安全補丁、應用的安全補丁等）。只要不符合這兩種類型中的任何一條規則，該用戶端都無法以遠端管理員身份登入管理介面。

   Ÿ 驗證校驗碼
   該功能用於防止非法或有潛在威脅的用戶端應用程式攻擊應用伺服器。例如被病毒或木馬篡改的應用程式的校驗碼必定與合法應用程式

的校驗碼不同，這樣，當使用者嘗試連入時，iSTAR 只要驗證用戶端運行的程式的校驗碼和伺服器端爲該程式設定的校驗碼是否一致，便可以判定用戶端的應用程式是否合法。如果合法，則該項驗證通過，否則使用者將不能啓動該應用。
校驗碼採用 SHA 1 演算法。

6. 點擊<使用者>設定該服務的遠端管理者。
7. 如圖 23 所示，將遠端管理員所屬的安全域從“可選擇”列表框中移至“已選定”列表框（設定本地管理員時，該步驟不需要）。如果選擇的是包含有角色角色資訊的 Radius 或 PKI 類型的安全域，會顯示圖 24 所示的操作介面。
8. 設定該管理員對 UUSwitch(/UUExchange)的訪問策略，系統預設的是“拒絕”，意即所有的管理員都不能訪問。
9. 在“使用者列表”中指定排除在訪問策略之外的方式。在其下的“使用者列表”列表中勾選使用者(/組/角色)方式,並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者(/組/角色)。
   通過這一步驟結合設定訪問策略步驟相結合，管理員可以靈活的設定訪問許可權，即：僅允許某一些管理員訪問，或者允許除某一些管理員外的所有管理員訪問。
   在“使用者列表”中指定排除在存取策略之外的方式。在其下的“使用者列表”列表中勾選使用者(/組/角色)方式,並按<增加>將其加入下方的“除了以下列出的”目錄中；重復在“使用者列表”中勾選，並按<增加>，可以繼續加入多個使用者(/組/角色)。
   如果安全域指定的伺服器類型爲“Windows AD/LDAP”，同時該伺服器中的“管理員名稱”中輸入的管理員屬於該域的“Domain Admins”組,則圖 23 中的“使用者列表” 列表將顯示該域中所有的使用者，否則，圖 23 中的“使用者列表” 列表只能顯示該域中的部分使用者。
10. 如果在圖 23 的視窗中的空白欄輸入要搜索的字串幷點擊<搜索/開始>，介面上將返回模糊查詢後的結果。圖中顯示了對“test”搜索的結果。(是否有搜索功能與伺服器的類型有關。)
11. 在“訪問類型”中設定該管理員的權限。各種許可權的含義分別爲：
    唯讀:表示該使用者對系統管理介面有“唯讀”許可權。
    更改:表示該使用者對系統管理介面有“唯讀”、“修改”和“使更改生效”的許可權。
12. 以上步驟完成後，保存設定結果，幷返回到圖 3 系統主介面中。

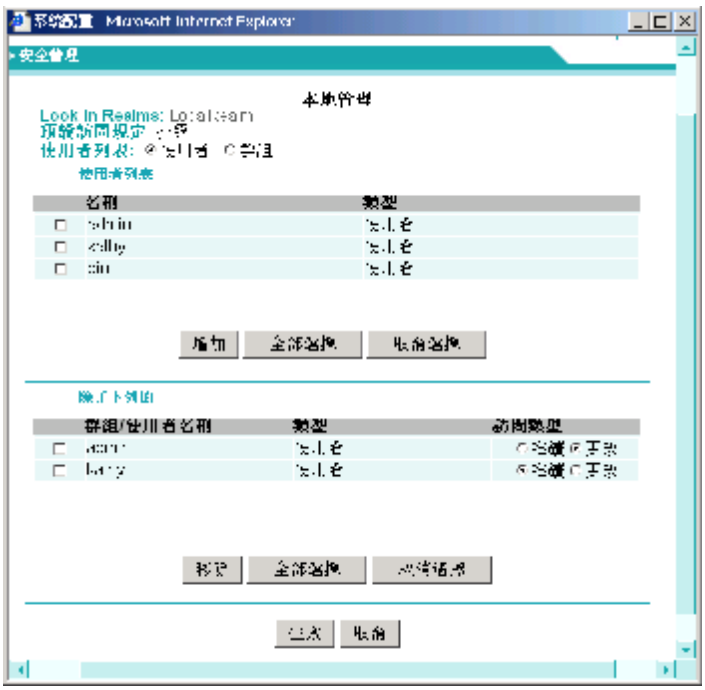


圖 19

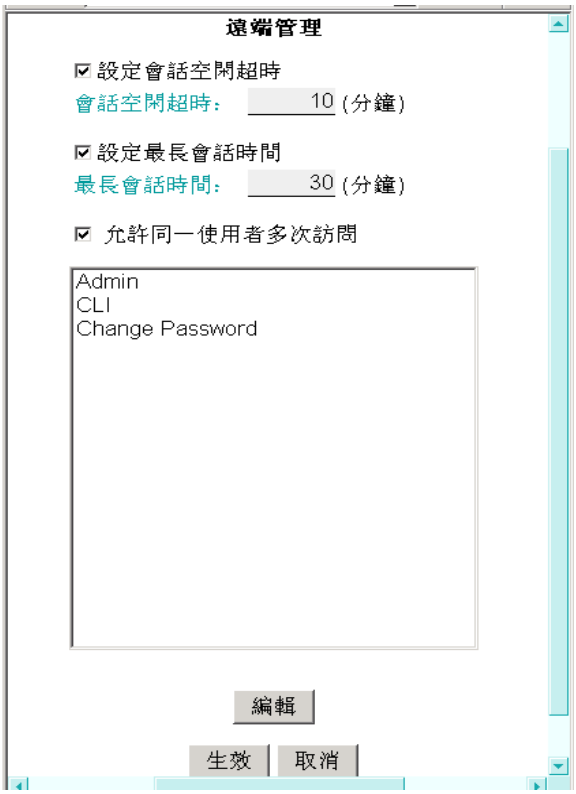


圖 20

圖 21

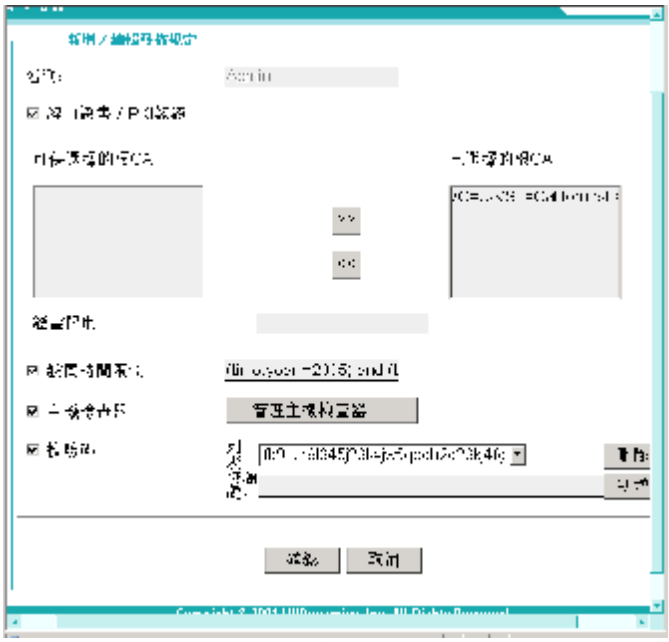


圖 22

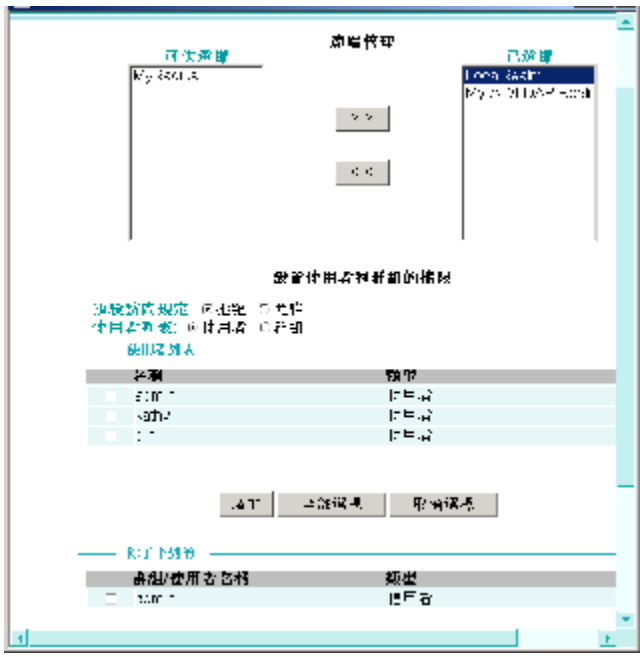


圖 23

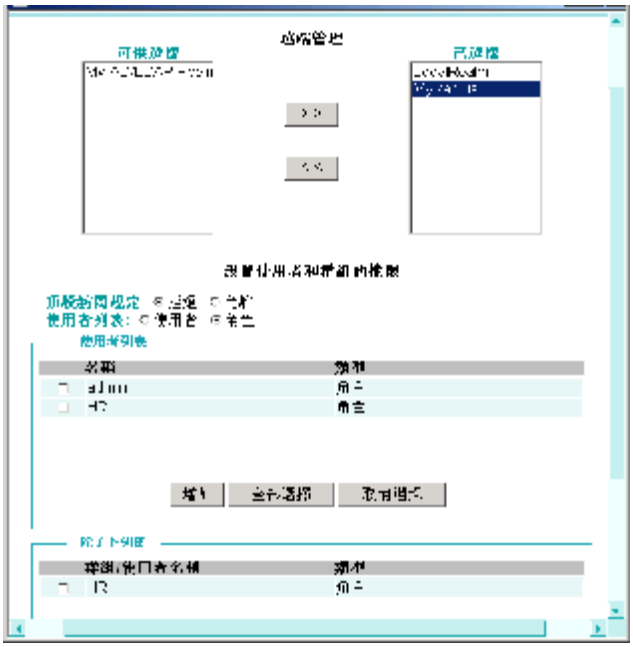


圖 24

4.2.7 不同用戶存取 UUSwitch（/UUExchange）的方法

Ÿ 本地管理員

本地管理員僅能從本機存取 UUSwitch（/UUExchange），通過身份驗證後，登入 UUSwitch（/UUExchange）進行管理。任何時候，只能有一位管理員登入。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“**錯誤! 找不到參照來源。**退出設定介面”。 但是多個不同的管理員可以同時獲取管理專案列表，前提是 遠端管理 中勾選了“允許”。

例如：

不同使用者名稱的管理員可以同時獲取管理專案列表。

不同安全域中同名的管理員可以同時獲取管理專案列表。

但是，相同安全域中同名的管理員不可以同時獲取管理專案列表。必須將原已連入的管理員停掉。這樣原已連入的會話會斷開。

獲取管理專案列表的方式：通過 IE 瀏覽器，在本機上輸入：

http://1.1.1.2/admin

顯示以下的視窗。輸入正確管理員名稱、密碼。即可登入。

圖 25

Ÿ 遠端管理員

遠端管理員僅能從遠端存取 UUSwitch（/UUExchange），通過身份驗證後，登入 UUSwitch（/UUExchange）進行管理。

獲取管理專案列表的方式：通過 IE 瀏覽器，遠端系統管理員可以在任何一台聯機到網際網路的電腦上輸入：

https://[*UUSwitch（/UUExchange）的 IP 位址*]/rm （主模式），或者，

https://[*主模式 uuswitch（/uuexchange）的 DNS 名稱或 IP 位址*]/[*子模式 UUSwitch（/UUExchange）UUID*]/rm（子模式）

顯示以下的視窗：

圖 26

在圖 26 所示介面中輸入身份認證所需要素，點擊<確定>之後，可獲取管理專案列表（如圖 27 視窗），遠端系統管理員啓動“Admin”圖示，輸入對應的管理員帳號和密碼，出現圖 39 所示介面。輸入使用者名稱和密碼，便可以對 UUSwitch（/UUExchange）進行遠端管理。如果 Admin 等服務需要證書驗證身份，則還需在圖 28 所示介面中選取正確的證書。

點選列表中的圖示，點擊滑鼠右鍵，彈出快顯功能表。

點選“配置”一項可以修改該應用程式在該用戶端存放的路徑，還可以設定相應參數；點選“啓動”一項可以啓動該應用；點選“調試選項”，可以設定調試和收集調試資訊的方

式。

調試選項說明如下：

Ÿ 追蹤應用用戶端和伺服器端的資料：

目的：記錄日誌以便跟蹤和調試。

選中該選項後，所有應用用戶端和伺服器端之間的資料都會被記錄在\windows\system32\（或者 WINNT\system32\）下的 uuspd.log 文件中。將該文件另存，便可打開進行查看。

“Custom-Network driver based C/S”、Outlook（MS exchange server 模式下）兩種應用不支援該功能。

Ÿ 切換用戶端工作方式：

目前，iSTAR 用戶端允許以兩種方式工作。當用戶端啓動應用出現問題時，可以選擇該選項，切換到另一方式工作。以便排查問題原因。

另外，選中該選項後，請檢查 iSTAR 用戶端各應用配置的參數不能爲功能變數名稱，應該設置成 IP 地址。

Ÿ 直接用戶端資料收發：

目的：測試不通過 iSTAR 的 tunnel，是否可以直接連接遠端伺服器。

iSTAR 用戶端應用列表中的某個應用不能成功啓動時，可以選擇該選項排查問題原因。如果不通過 iSTAR 的 tunnel，可以直接連接遠端伺服器，說明問題是 iSTAR 引起。如果不可達，則說明是可能存在其他因素導致連接失敗。

遠端伺服器：輸入要連接的遠端伺服器的 IP 位址。

遠端埠：輸入要啓動的應用在遠端伺服器上的埠。例如，要啓動 Web 應用，則設置遠端埠爲 80；要啓動 Telnet，則設置遠端埠爲 23。

本地埠：輸入一個本地未被使用的埠，如 1234。

另外，選中該選項後，請檢查 iSTAR 用戶端各應用配置的參數設置。

例如：

Telnet 應用：127.0.0.1 1234

Web 應用：http：//127.0.0.1：1234

任何時候，只能有一位管理員登入管理介面。如果之前未正常登出或已有其他管理員登入，需要先將原登入者停掉。詳細說明請參考“**錯誤! 找不到參照來源。**退出設定介面”。但是多個不同的使用者可以同時獲取應用列表。同一使用者也可以多次獲取應用列表，前提是 遠端管理 中勾選了“允許同一使用者多次訪問”。

例如：

- Ø 不同使用者名稱的管理員可以同時獲取管理專案列表。
- Ø 不同安全域中同名的管理員可以同時獲取管理專案列表。
- Ø 管理員在發布應用時勾選了“允許同一使用者多次訪問”，則相同安全域中同名的管理員可以同時獲取管理專案列表。
- Ø 管理員在發布應用時沒有勾選“允許同一使用者多次訪問”，則相同安全域中同名的管理員獲取應用列表時。會將原已連入的會話斷開。

& 說明：

Ÿ 如果身份認證在 LocalRealm 上進行，則僅需要輸入 LocalRealm 中的使用者名稱及密碼。

Ÿ 如果認證在 ACE 伺服器上進行，則請輸入 ACE 伺服器上的使用者名稱及密碼，並在密碼後接著輸入 Token code。（當 Token 的顯示幕顯示的六格短橫杠僅剩一格時，說明該 token code 即將失效，此時請等待 ACE 伺服器分配下一個 code，並輸入這個新的 code。

Ÿ 如果認證在其他類型的安全域中進行，則需要輸入相應認證伺服器中的使用者名稱及密碼。

Ÿ 如果在安全域進行認證需要核實 Certificate/PKI，則需要勾選“高級”，並在“證書”欄選擇證書。在安全域中使用的證書與上面提及的 Admin、CLI、Change Password 等服務中使用的證書可以不一樣。

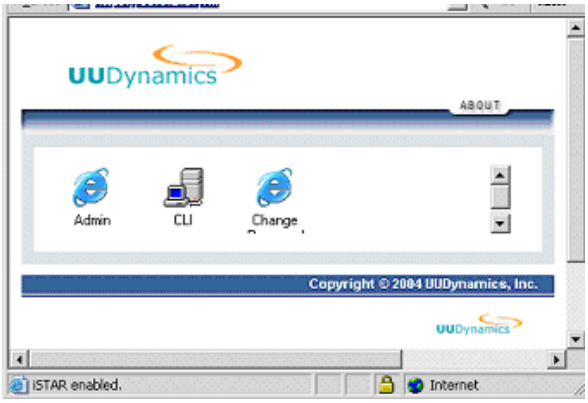


圖 27

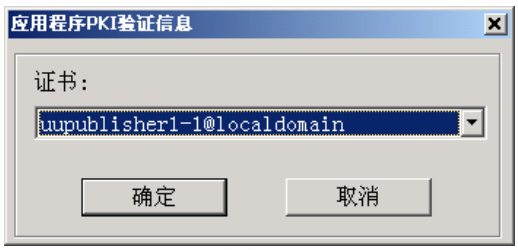


圖 28

在圖 26 所示介面中，勾選“Session 清理”。將會將電腦中的各種與該使用者相關的暫存檔案、cookies 等資訊刪除。點擊<高級>可以指定要清理的專案。系統將在 Session 結束後立即清空，並且不能撤銷，請謹慎操作。

& 說明

使用者使用共用電腦（如網吧電腦）連入 UUSwitch（/UUExchange）時，可以考慮此功能，以保護個人資訊安全。

設定項	說明	位置
Internet 瀏覽暫存	清除 Cache 中該使用者的所有臨時的 Internet 檔	[*系統盤符*]:\Documents and Settings\[*username*]\Temporary Internet Files
Internet 瀏覽歷史記錄	清除 IE 中所有的瀏覽頁面的歷史記錄	
Internet Cookies	清除 IE 中的所有 Cookies	[*系統盤符*]:\Documents and Settings\[*username*]\Cookies
鍵入的 URL	清除 IE 位址欄裏的所有的 URL 記錄	
自動填充表格	清除 IE 上所有表單中自動填充部分的內容	
自動填充密碼	清除所有自動填充的密碼	
Internet 收藏	清除該使用者在 IE 收藏夾裏的所有內容	[*系統盤符*]:\Documents and Settings\[*username*]\Favorites
暫存檔案	清除所有的暫存檔案	
Telnet 歷史記錄	清除該使用者在本機上所有的 Telnet 記錄	
垃圾箱	清空系統盤符下的垃圾箱	
運行歷史記錄	清除 Windows“開始->程式”功能表中的最近運行程式的記錄列表	[*系統盤符*]:\Documents and Settings\[*username*]\Start Menu\Programs
最近的文檔	“開始->文檔”功能表中的最近開啓文檔的記錄列表	[*系統盤符*]:\Documents and Settings\[*username*]\Recent
最後登入使用者	清除上一次登入的使用者名稱	
查找文件歷史記錄	清除上一次查找檔的搜索結果	
查找電腦歷史記錄	清除上一次查找電腦的搜索結果	

網路歷史記錄	清除“網路芳鄰”中所有的映射目錄	[*系統盤符*]:\Documents and Settings\[*username*]\NetHood

4.3 日常維護

4.3.1 匯入（/匯出）系統的設定資訊

在圖 3 所示的系統主介面中，點選“系統管理”下的設定匯入，進入如圖 29 所示的介面，將原來保存好的配置檔案匯入到系統中。

圖 29

點擊<瀏覽…>鍵，選擇您原先輸出的系統設定檔案.uud（參見本節後面的內容），然後點擊<輸入>，會顯示如圖 30 訊息方塊，如果您匯入設定包括網路設定等基本資訊，UUSwitch(/UUExchange)會重新啓動。點擊<確定>後就會匯入設定。

圖 30

在圖 3 所示的系統主介面中，點選“系統管理”下的設定匯出，進入如圖 31 所示的介面， 您可以將設定檔案匯出到一個檔案夾裏，保存起來。可以匯出 UUSwitch(/UUExchange)的基本設定（Basic Configuration）、UUSwitch(/UUExchange)的其他如叢集、UUID 等設定資訊（Server Configuration）或整個設定（Whole Configuration）。

圖 31

選擇了匯出某一種設定，在開啓的提示介面中按<保存>就可以把

UUSwitch(/UUExchange)的設定保存到指定的檔案夾裏。

圖 32

4.3.2 顯示狀態

在圖 3 所示的系統主介面中，點選“系統管理”下的查看狀態,將進入圖 33。顯示當前系統的基本資訊，包括：伺服器類型，系統模式，版本資訊，基本 OS 版本資訊，系統狀態和系統的 Interface、Routing 等資訊。

點選圖 33 中的“在綫 UUID”和“在綫 UUSwitch”可以看到當前註冊到這個 UUSwitch(/UUExchange)上的所有 UUID（包括 UU100,UU200,UUSwitch(/UUExchange)等）和所有 UUSwitch(/UUExchange)的 UUID。介面如圖 34，圖 35 所示。

圖 33

圖 34

圖 35

在配置了叢集的情況下，在查看狀態中會看到叢集的頁面。所有叢集中的 IP 會顯示出來。點選任何一個叢集 IP 的鏈結，將使 GUI 跳轉到叢集 IP 的伺服器中。

4.3.3 查看系統性能

在圖 3 的視窗中，選擇在“系統管理”之下的查看系統性能，可以選擇“Remote desktops”：查看連入 UUSwitch(/UUExchange)的連接數（Remote desktops），或者“System Utilization View”查看 UUSwitch（/UUExchange）硬體的 CPU 和 Memory 的使用情況。

如圖 36 中所示，座標圖中的橫軸爲時間點，縱軸爲數量。不同顏色曲綫代表不同的跟蹤項的數量變化軌迹。如果近期 Remote-desktops 的數量持續逼近 Licence 數值，則說明該 UUSwitch 的使用者數量已趨近最大值，此時應該考慮購買更多 Licence 以滿足日漸增長的需求。

點點擊<顯示>，靜態顯示選定時間段的統計資訊；

點點擊<當前>，動態顯示即時的統計資訊；

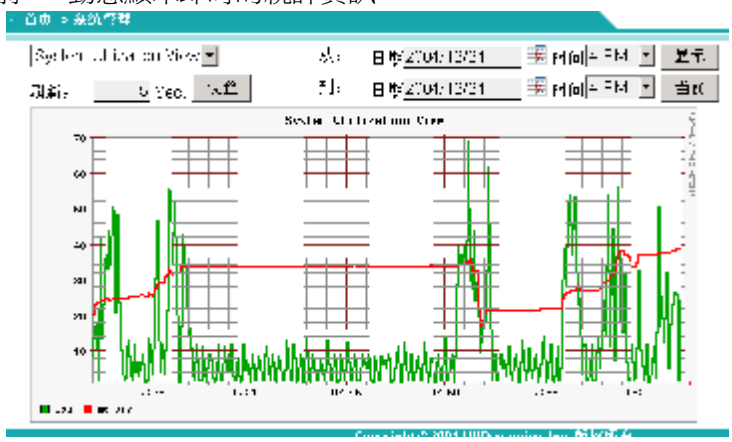


圖 36

4.3.4 查看日誌

在圖 3 所示的系統主介面中，點選“系統管理”下的查看日誌，將進入如圖 38 所示的

介面。系統管理員可以查看系統每天指定時間段中，由重點到詳細的日誌情況，并可隨時保存日誌，以便隨時審閱。

點擊<顯示>鍵可以顯示指定條件的日誌；初次進入這個介面，會彈出安裝 ActiveX 的提示介面。 您必須按<是>，才能繼續完成輸出配置檔案。 (這是一個資料下載的控制項，不會對您的系統造成影響)

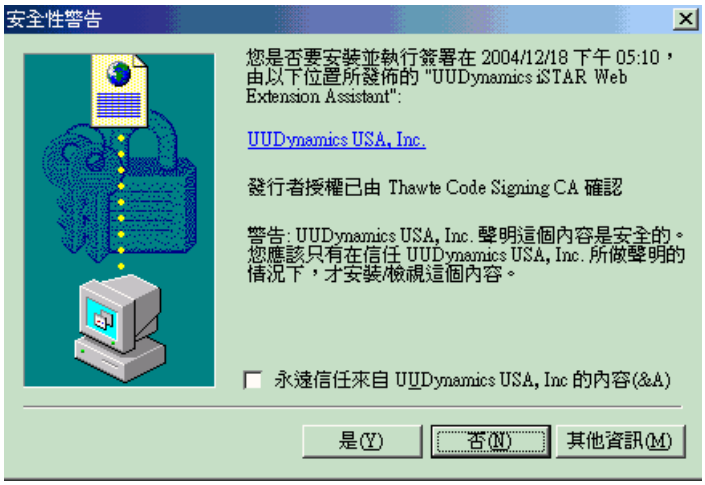


圖 37

按<保存顯示日誌>，則可以將螢幕上顯示的日誌保存到指定檔案路徑；

如果在設定日誌等級時已勾選了“收集調試資訊”核取方塊，按下<全部保存>,則保存的 Log 文件中不僅包括螢幕上顯示的日誌而且包含系統的 debug 資訊。

注意：

1. UUSwitch 日誌中所紀錄的日期及時間，是根據 UUSwitch 伺服器作業系統的設定日期及時間進行紀錄；您必需確定 Windows 伺服器的日期及時間設定正確，才能獲得正確的日誌紀錄。
2. 日誌資訊[ ]符號外部的內容，爲出錯提示，供使用者參考。[ ]內部的內容，爲系統內部資訊，供開放人員跟蹤。使用者可以不予理會，如有需要，亦可將其告知我公司技術支援人員。

圖 38

4.3.5 故障檢修

我們爲您提供了三種常用的網路檢測工具：ping（檢測遠端主機或本地主機的連通性），traceroute（檢測從本地主機到遠端主機的路由），netstat（顯示網路連接、路由表和網路介面資訊）。您可以方便得在 UUSwitch(/UUExchange)的管理介面下使用這三種標準的檢測工具，監視和分析現有網路狀態，檢測網路連接性。(圖 39)

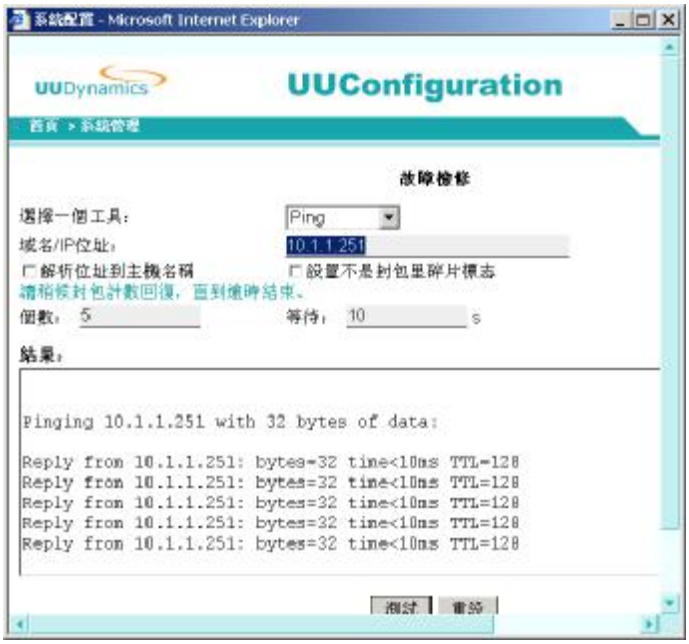


圖 39

4.3.6 系統時間設定

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定,您可以修改 UUSwitch(/UUExchange)的系統時間（圖 40）。

圖 40

4.3.7 系統 LOGO 設定

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定,您可以修改顯示在左上角的 LOGO 檔(圖 41)，您可以使用您公司的 LOGO 替換它，但必須是 gif 檔格式，Size 小於 5KB。

圖 41

4.4非常規任務

當 UUSwitch（/UUExchange）安裝成功，并正確完成了初始設定後，UUSwitch（/UUExchange） 即可正常工作。除非運行環境或使用者發生改變，否則，請不要輕易改變以下設定：網路設置；iSTAR 設置；認證控制；選擇模式；管理許可證；系統升級；匯入設定。以免系統出現非預期的故障。

ⅰ 注意：

- 更改以上這些設定後，點擊<生效>系統會自動中斷 Session，並提示使用者重新 Login 更改後的系統。因此，建議您：避免在系統繁忙時改變這幾項設定。
- 按<生效>後有時會重新啓動系統的服務，這時介面上可能會出現“非法 IP”等資訊，這時需要稍等片刻，輸入 http://1.1.1.1/admin，重新進入配置介面。

4.4.1 管理許可證

許可證用來控制可以連接到 UUSwitch(/UUExchange)的最大併發使用者數。UUSwitch(/UUExchange)出廠時預設一個允許 500 個併發使用者的許可證。

如果您已購買額外的許可證，可以通過以下步驟升級許可證：

1. 點選“系統管理”下的 管理許可證，進入下圖所示介面（圖 42）

圖 42

2. 點擊<上傳>，在圖 43 所示介面中點擊<瀏覽>，選擇要替換的證書的完整路徑和檔案名，點擊<確認>。

圖 43

3. 最後按<生效>，使設定生效。

4.4.2 升版系統

您可以在本機或者通過遠端按照以下操作步驟升級系統版本：

1. 點選“系統管理”下的系統升級，進入圖 44 所示介面。

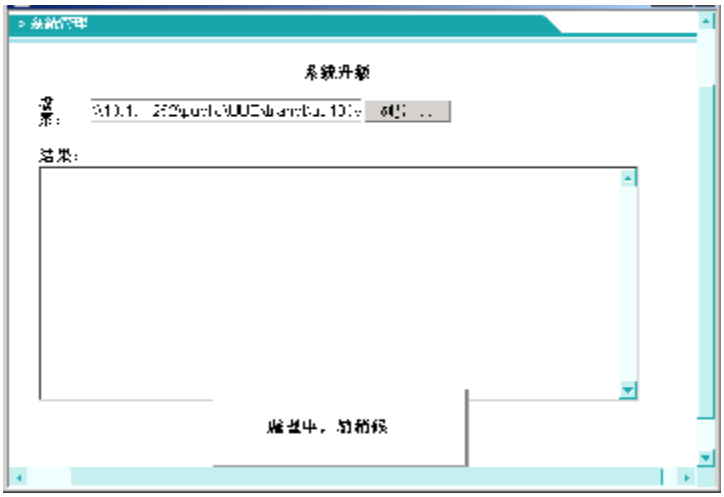


圖 44

2. 點擊<瀏覽……>，選擇新版本的安裝程式的完整路徑和檔案名，點擊<更新>，系統將自動進行版本升級，幷在升級完成後，彈出提示框見圖 45 要求使用者重新登錄。

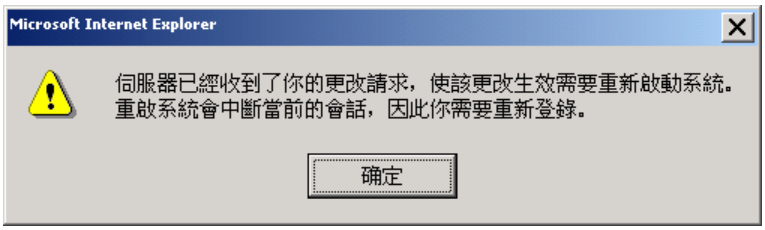


圖 45

重要：

在點擊<更新>升級系統後，而提示框未出現之前，請不要人爲中止升級過程，否則，會導致UUSwitch(/UUExchange)系統發生嚴重後果。

4.4.3 設定日誌和報警等級

在圖 3 所示的系統主介面中，分別點選“系統管理”下的日誌控制 和告警控制，將進入如圖 46 所示的介面，系統管理員可以進行系統日誌和報警的設定。

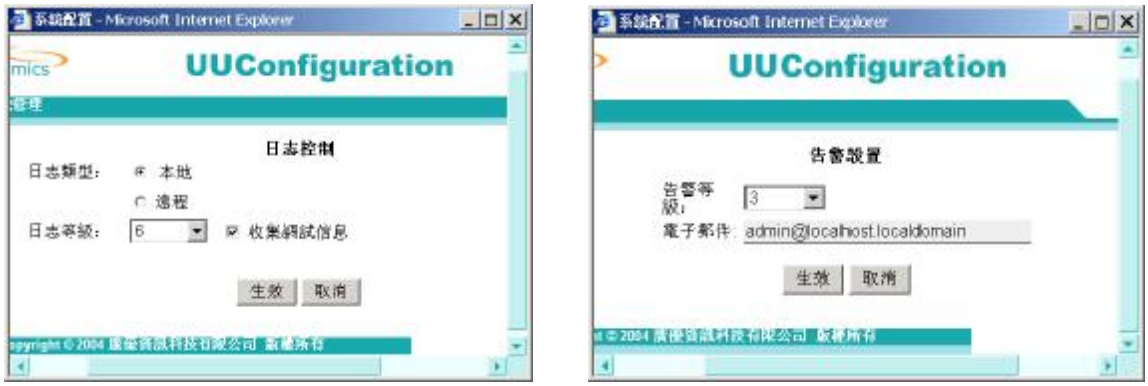


圖 46

其中，“日誌類型”是指定日誌保存的地方。有“本地”和“遠端”兩種，本地是指 UUSwitch（/UUExchange）的日誌保存在本機上，遠端是指 UUSwitch（/UUExchange）的日誌保存在遠端的 syslog 日誌伺服器上。

日誌等級是指顯示和保存的日誌詳細程度，總共有 0-6 級，級別越高，日誌越詳細，0 級表示不記日誌。系統管理員可以根據需要來設定。

勾選選中“收集調試資訊”核取方塊後，系統會將 debug 資訊寫入 Log 文件。

“告警等級”是指發出警告資訊的日誌級別，例如，設定告警等級爲 5，則表示如果有 5 級及以下的日誌產生的話，就以警告的形式通知系統管理員。

系統管理員可以設定報警等級，并發往指定的電子郵件地址。

4.4.4 設定加密演算法

在系統主介面中（如圖 3）的“安全管理”下，按下加密管理， 會出現如圖 47 的視窗； 用來選擇對資料的加密演算法和 Hash 演算法，以確保資料傳輸的安全。

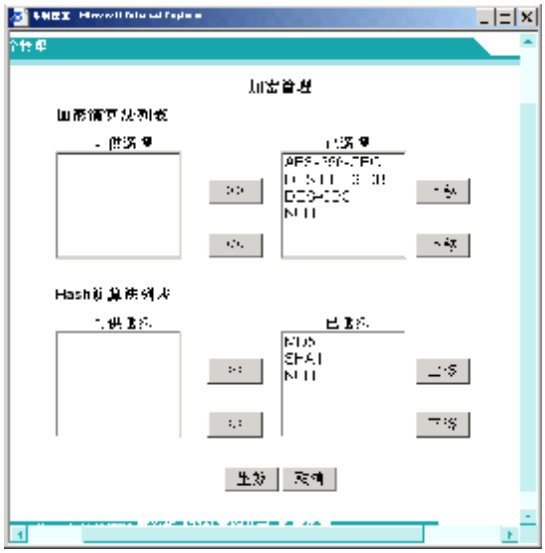


圖 47

右邊 Selected 視窗內的是當前被啓動且使用中的加密和 Hash 演算法； 如果使用者想要停止其中任何一種或多種的加密和 Hash 演算法， 可以使用 << ，將其移至左邊的 Available 視窗內； 反之可以使用 >> ，將其再加回到右邊的 Selected 視窗內。

在 Selected 視窗右側的“上移”以及“下移”，用於調整各種加密和 Hash 演算法的協商優先等級； 在上端的優先等級較高，在下端的優先等級較低，使用者可以根據實際狀況自行調整。

4.4.5 更新數位憑證

這是一個可選功能；UUSwitch(/UUExchange)系統中預設了一張數位憑證。您可以使用系統預設的數位憑證，也可以選擇將其更新爲第三方的數位憑證。如圖 49 所示，需要輸入該證書對應的 Key 文件，證書文件和 CA 的證書文件，所有文件要求是 Base64 編碼方式。

& 說明：

UUSwitch(/UUExchange)預設的數位憑證是由 UUDynamics, Inc.所簽發，其根憑證並沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中； 詳情請參照本手冊 2.1 的說明“數位憑證”。

更新數位憑證，如圖 3，點選“網路設置”下的管理證書，進入更新數位憑證介面，如圖 48：

圖 48

圖 49

4.4.6 改變模式

如圖 3，點選“進階”下的 選擇模式。根據工作模式選擇“主模式”或者“子模式”。兩種模式的區別請參見“術語表”。

模式改變後，系統會根據所選的工作模式，引導您繼續配置其他的網路參數。具體步驟請參見“**錯誤! 找不到參照來源。**安裝軟體”章節。

4.4.7 設定叢集分攤負載

1. 叢集概述

UUDynamics 在其所有的安全設備上均使用了叢集技術以保證系統的高可用性和負載分流。此項技術被應用在 UUDynamics 的所有安全設備中，包括主模式下的 UUSwitch (/UUExchange)，和 UU200 發布單元。

當網路中有多台 UUExchange(/UUSwitch)，并且負載非常不均衡，可以考慮使用叢集的方式平衡它們之間的工作量負載。叢集的最大值可達 10 台。

Ÿ 容量規劃: N+1

叢集功能使參與叢集的伺服器得到了綫性的增長。在特定的應用環境下，參與叢集的伺服器數目依賴於必須使用的伺服器數目 N（N 的值由計劃的容量計算所決定）。幷增加一台用於冗余和容錯。

- 負載分流

  在綫工作期間，負載被平均地分流到所有的 N+1 個伺服器。

- 單系統鏡像

  不論加入了多少個伺服器，一個叢集意味著單個系統，即被叢集的所有伺服器可被視爲一個整體。除了 LAN Settings，叢集中的所有伺服器的配置資料庫都可以作爲一個整體被維護。對於 LAN Settings，可以通過在叢集中選擇特定的伺服器進行在綫修改。

  要支援 UUSwitch (/UUExchange)的單系統鏡像，需要先支援 DNS 服務，以便該叢集中的伺服器可以共用同一個 DNS 功能變數名稱稱。

- 高可用性

  一旦檢測到任何錯誤，負載都將在剩餘的正常工作的伺服器上重新分配。當某台伺服器出錯時，其他 N 台伺服器將會自動接管網路中的所有工作量負載，

- 重構

  可以毫不費力地加入新的伺服器以增加網路的額外容量。此時，網路中原有的叢集僅需要重新配置一下“Lan settings”。當前正在運行的伺服器將會自動地更新現行的應用服務的相應配置。新加入的伺服器所運行的軟體版本也會和叢集中的其他伺服器保持一致。

2. 工作量均攤原理

- UUExchange/UUSwitch 的工作量均攤

  當檢測到錯誤時，工作量負載會被重新分配到其他的伺服器。重新分配的負載包括伺服器註冊的維護工作和將子模式 UUSwitch (/UUExchange)重新連接主模式 UUSwitch (/UUExchange)。在成功地重建叢集之前，受到影響的發布單元和子模式 UUSwitch (/UUExchange)會暫時無法註冊或者連接到主模式 UUSwitch (/UUExchange)。系統會自動執行後續的重新註冊和重新連接。

- 工作量負載重分配對用戶端的影響

  在負載重分配過程中，用戶端已搭建好的通道可能會面臨連接斷開的情況。但是，連接斷開卻幷不一定說明發布單元存在問題。下面列出了通道斷開的幾種可能情況：

  - 發布單元的工作量重分配，可能是由於伺服器出現問題或新加入了新的發布單元。
  - 用戶端和發布單元之間的路由器受到的網路幹擾。
  - 發布單元因爲會話超時而斷開連接。
  - 用戶端因爲會話超時而主動斷開連接。

出於安全考慮，那些爲 Remote Desktop (UUApp) 和 UURemote 而建立的通道不會自動重新連接。用戶必須手動地重新登入。而爲 UUSoft 建立的通道，則會自動重新進行連接。

3. 叢集的設定

1. 如圖 3主功能表介面，點選“網路設定”下的 網路設定，進入網路參數設定介面。點選“Step2”設定叢集。
2. 勾選“啓用叢集”表示啓用叢集；
3. 輸入叢集 IP、及對應的叢集子網掩碼；

   每一台被叢集的 UUSwitch (/UUExchange)需要一個專用的靜態 IP 位址，稱爲叢集 IP，一般爲私有 IP。

   系統管理員可以自由設定這些叢集 IP，但同一個叢集的 UUSwitch (/UUExchange)必須位於同一個子網路。同時，叢集 IP 不能與任何私有地址相同。在路由模式下，叢集 IP 不但不能與任何私有 IP 位址相同，而且不能與任何公共 IP 位址相同。否則會導致衝突。
4. 輸入叢集 IP(開始)、叢集 IP（結束）資訊；這是用於描述同一個叢集內 UUSwitch (/UUExchange)的 IP 位址範圍。

   叢集中所有的叢集 IP 位址必須在叢集 IP 位址範圍內。
5. 輸入完畢後按<保存>進行儲存幷返回網路參數設定介面。
6. 點擊<生效>，結束叢集設定。

4.4.8 SNMP 設定

UUSwitch(/UUExchange) 支援 SNMP 協定，所有 SNMP 工具或應用可以方便的對 UUSwitch(/UUExchange)硬體這個受管節點進行管理。

在圖 3 的視窗中，選擇在“系統管理”之下的 系統設定,您可以設定與 SNMP 相關的資訊，以便管理員參考（如圖 50）。

圖 50

點擊<新增>，設定哪些機器可以使用 SNMP 工具存取 UUSwitch(/UUExchange)（如圖 51）

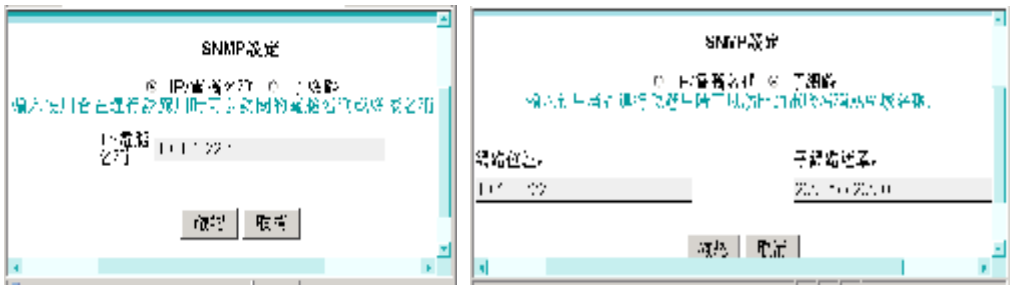


圖 51

例如：添加了一個 IP 位址爲 10.1.1.24 的機器。則在這台機器上運行某個 SNMP 工具，指定 UUSwitch(/UUExchange)的 IP 位址後，下列物件 ID（OID） 反映配置檔中的指引值：

Name/OID	Value
sysDescr.0	UUDynamics BaseOS 2.1.5, UUSwitch 2....
sysObjectID.0	.1.3.6.1.4.1.2021.250.10
sysUpTime.0	1562
sysContact.0	support@uudynamics.com
sysName.0	localhost
sysLocation.0	UUDynamics.com
sysServices.0	14
.1.3.6.1.2.1.1.8.0	0
.1.3.6.1.2.1.1.9.1.2.1	.1.3.6.1.2.1.31
.1.3.6.1.2.1.1.9.1.2.2	.1.3.6.1.6.3.1

圖 52

sysdescr：受管節點的文字說明。圖中該欄的值表示：該受管節點爲 UUDynamics 公司出品的 UUSwitch(/UUExchange)，硬體的作業系統版本號爲 2.1.5。

sysname：圖中的“localhost”表示 UUSwitch(/UUExchange)以主模式工作。如果 UUSwitch(/UUExchange)以子模式時，顯示該 UUSwitch(/UUExchange)的 UUID。

sysservices：指出這個受管節點可能提供的一組服務的值。預設爲 14

syscontact：聯絡的文字識別方式。如果未在圖 50 中設定該欄的值，則該值的字串長度爲 0。

syslocation：這個受管節點的管理指派名稱。依慣例，這是節點的完整網功能變數名稱稱。如果未在圖 50 中設定該欄的值，則該值的字串長度爲 0。

4.4.9 連接埠轉遞

在圖 3 的視窗中，選擇在“系統管理”之下的系統設定，啓用“連接埠轉遞”可以將一個或多個防火墻外部的 IP 位址對應到某個防火墻後面的內網 IP 位址上（圖 53）。

在“外部 IP 位址”輸入列填入外網 IP，點擊<新增>，可以指定新的外網 IP 位址。

選中列表中的外網 IP 位址，點擊<刪除>，可以移除該外網 IP 的對應。

說明：

當多個 UUSwitch(/UUExchange)作叢集時，指定的內網 IP 位址不能與叢集中的其他 UUSwitch(/UUExchange)的 IP 位址相同，否則會引起衝突。此處指定的內網 IP 位址爲整個叢集的代用 IP。當其他機器存取這個內網 IP 位址時，訪問的實際上是叢集中的任一台 UUSwitch(/UUExchange)。這樣，當叢集中的某一台 UUSwitch(/UUExchange)未能聯機時，負載可以無隙的轉移到叢集中的其他 UUSwitch(/UUExchange)上。

圖 53

4.5 UUID 管理

僅主模式的 UUSwitch(/UUExchange)可以對 UUID 進行管理，子模式的 UUSwitch(/UUExchange)則是不可以對 UUID 進行管理的，在 ***i*STAR™**系列產品中，所有子模式的 UUSwitch(/UUExchange)以及 Publisher（UU100/UU200 等）都必須有一個 UUID 檔案； 而主模式的 UUSwitch(/UUExchange)則是爲它們提供 UUID 檔案的來源。（注，UUID 是唯一標識 UU100,UU200,從 UUSwitch(/UUExchange)的 ID，其格式如 Email 一樣：AAA@bbb.ccc，其中 bbb.ccc 是 Domain 名）

① 管理域

對 UUID 的命名，實際上決定了獲得該 UUID 設備（UUSwitch(/UUExchange)或是 Publisher）的名稱；爲了方便日後的管理，系統管理員可以根據實際的需要對 UUID 以功能變數名稱稱的方式進行分組及管理。

- **增加域**

在圖 3 的系統主介面中，

1. 點選“安全管理”下的管理 UUID，在開啓的介面上選中“域管理”，進入增加域介面（如圖 55）；
2. 在“功能變數名稱:”右邊的欄內輸入相關的域資訊（如 abc.com，可以根據實際的需要命名），
3. 按<增加域>，在“域列表”的視窗內將會顯示所加入的域資訊。

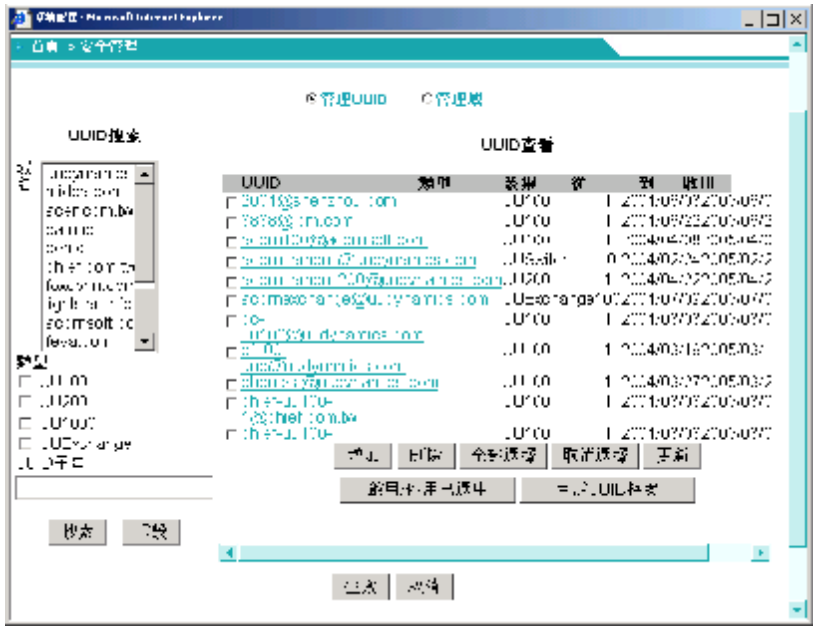


圖 54

圖 55

② 管理 UUID

在圖 3 的系統主介面中，點選“系統管理”下的管理 UUID，進入管理 UUID 介面（如圖 54）；

– **增加 UUID：**

如果增加單個 UUID：

1. 如圖 54，在管理 UUID 介面上，按<增加>鍵進入“增加 UUID”介面（如圖 56），
2. 輸入相關的 UUID 資訊後（UUID 中的英文字母是不區分大小寫的），點擊<確認>，系統將回到圖 54 所示的介面，并在“UUID 查看”下的視窗內顯示已增加的 UUID 列表。
3. 最後點擊<生效>,即增加 UUID 完成,點擊<取消>，退出此介面

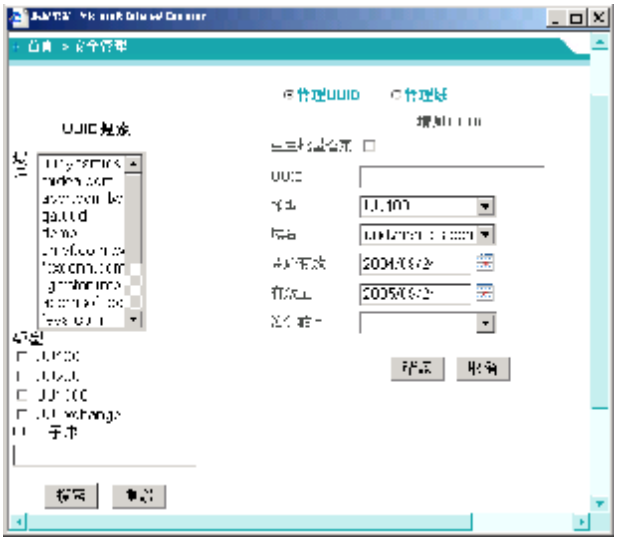


圖 56

如果增加整批的 UUID：

1. 如圖 57 勾選“產生批量檔案”，輸入相關的 UUID 資訊（UUID 中的英文字母是不區分大小寫的）；
2. 輸入指定 UUID 的字首和起始編號；
3. 點擊<確認>，系統將回到圖 54 所示的介面。並在“UUID 查看”下的視窗內顯示已增加的 UUID 列表。
4. 點擊<生效>,返回圖 3 所示的主功能表介面，即增加 UUID 完成。

所謂成批增加，是指你指定 UUID 的字首和起始編號、一次創建個數，一次可以創建如 user00、user01、user02……多個 UUID。

注意：

新增 UUID 後必須要按<生效>按鈕，才能生效。然後可以按照第 4 步的操作來生成 UUID 文件。

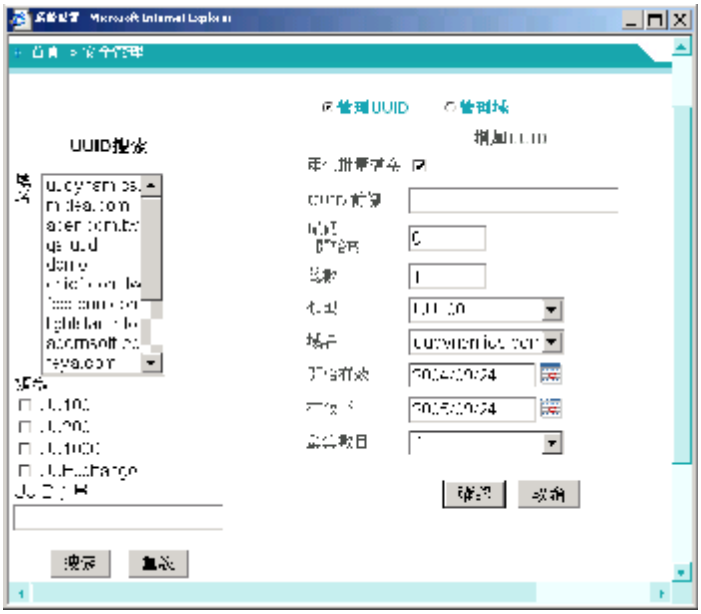


圖 57

介面上的各控制項說明請參考下表：

控制項	說明	備註
“產生批量檔案”	勾選時可以增加整批的 UUID	
“UUID 字首”	輸入欲增加的 UUID 名稱的字首以便識別	
“尾碼開始於”	表示整批 UUID 的起始編號	該控制項僅在勾選 “Batch Creation”後顯示
“總數”	表示整批 UUID 的一次創建個數	該控制項僅在勾選 “Batch Creation”後顯示
“類型”	點選右邊選項框內的倒三角形，可以選擇 UUID 的類型（即該 UUID 是屬於 UU100 或 UU200	
“開始有效”	指該 UUID 的啓始的有效時間。	
“有效至”：	指該 UUID 的無效的截止時間。	
“叢集數目” ：	表示生成的 UUID 可以同時在同一個叢集裏的不同的伺服器（如 UU100 或 UU200）上使用，倒三角型裏的下拉清單裏表示選擇伺	

	服器的個數。	

– 啓用/停用 **UUID**

新增加的 UUID 預設爲啓用。

在圖 54 所示介面，選上指定的 UUID，點選“選中啓用/停用已選中”鍵可以改變該 UUID 的狀態。

– **生成 uuid 檔案**

1. 如圖 54，在“UUID 查看”下的視窗內選上指定的 UUID；
2. 點擊<生成 UUID 檔案>，進入如圖 49 的介面。系統預設産生的 UUID 檔案沒有密碼的保護(即“不使用密碼保護 UUID 檔案。”)；

   選擇“使用密碼保護 UUID 檔案。”，則需要密碼的保護（如圖 59。在橫線上輸入保護的密碼。
3. 點擊<確認>, 彈出如圖 60，點擊<保存>，輸入 uuid 保存的的路徑，即可生成與之 UUID 相對應的 UUID 檔案。

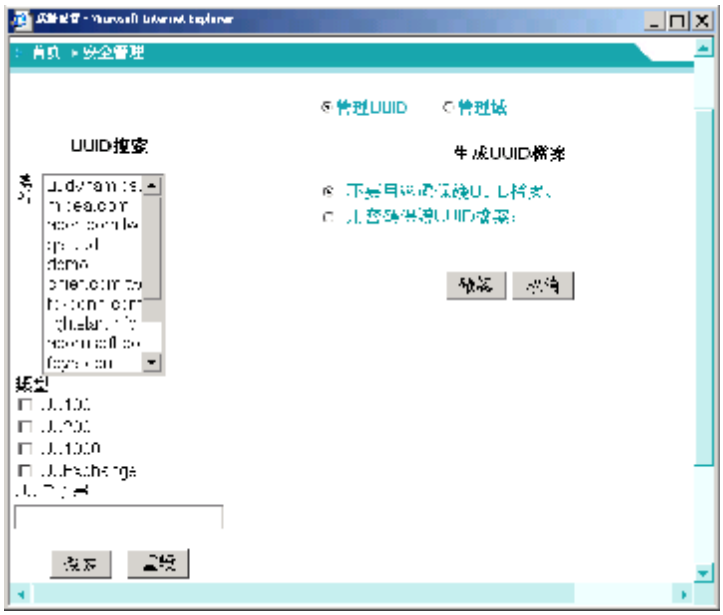


圖 58

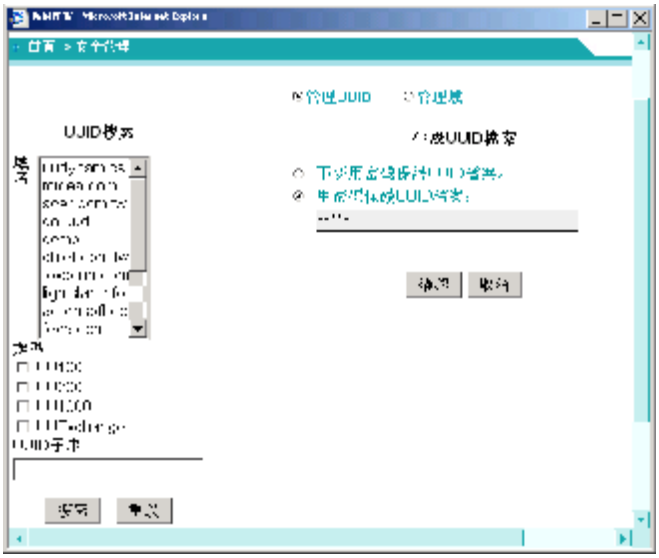


圖 59

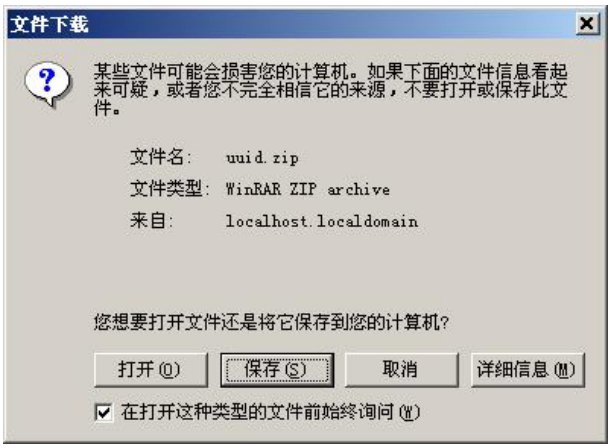


圖 60

– 更新 **UUID**

如圖 54，在選中某個或某些 UUID 後，點擊<更新>按鈕，就可以把選中的 UUID 所對應的原有的舊 UUID 文件作廢，需要重新按照上一步生成來生成新的 UUID 文件來使用。

如果不按<更新>，該 uuid 多次生成的檔案是相同的。

– **UUID** 搜索

如圖 54，選上指定條件的 UUID（包括選擇 UUID 域，選擇 UUID 的類型，UUID 子串），點擊<搜索>，在右邊 UUID 顯示的區域內將會顯示滿足條件的 UUID 的資訊。

第5章 系統復原

5.1 何時需要系統復原

系統復原是指將系統恢復到出廠狀態，復原的過程會導致：

- UUDynamics 套裝軟體丟失
- UUSwitch(/UUExchange)中的設定資訊丟失

復原後必須重新安裝 UUDynamics 套裝軟體，重新配置系統，丟失的配置資訊將永久性不可恢復。因此，我們強烈建議您經常輸出幷備份系統配置資訊，在系統無法工作，幷且按 UUDynamics 技術支援無法解決時才使用系統復原功能。

重要：
不當的系統復原會產生嚴重的後果，不到萬不得已，不要執行系統復原操作！

5.2 系統復原方法

在 UUSwitch(/UUExchange)系統在設定處理時出現停電等情況可能會導致系統備破壞，這時需要進行系統復原工作。

1. 準備工作
   （1） 準備一台配置 PC 電腦，設定成動態獲取 IP 位址；
   （2） 將備份的系統配置資訊複製到該配置電腦上；
   （3） 與 UUDynamics 技術支援聯繫，獲取 UUDynamics 套裝軟體；
2. 用 Null Modem 線與 UUSwitch(/UUExchange)的 Console 介面連接，重新開啓 UUSwitch(/UUExchange)設備的電源，系統啓動過程中在超級終端的螢幕上會看顯示提示資訊：

   UUDynamics iStar Server:
   We will pause for 5 seconds to give you a chance to execute recovery if desired.

   Press "Tab" first to enter into recovery process.
   Please enter "R" behind the "boot: " prompt for recovery, or "N" for No-recovery
   boot:

   選擇“R”即開始系統復原；
3. 選擇 UUSwitch(/UUExchange)上標“1”字樣的網口，用交叉線將配置電腦與 UUSwitch(/UUExchange)連接起來；
4. 在配置電腦上開啓瀏覽器，輸入 URL: http://1.1.1.1/admin, 得到如圖 61 所示的介面。

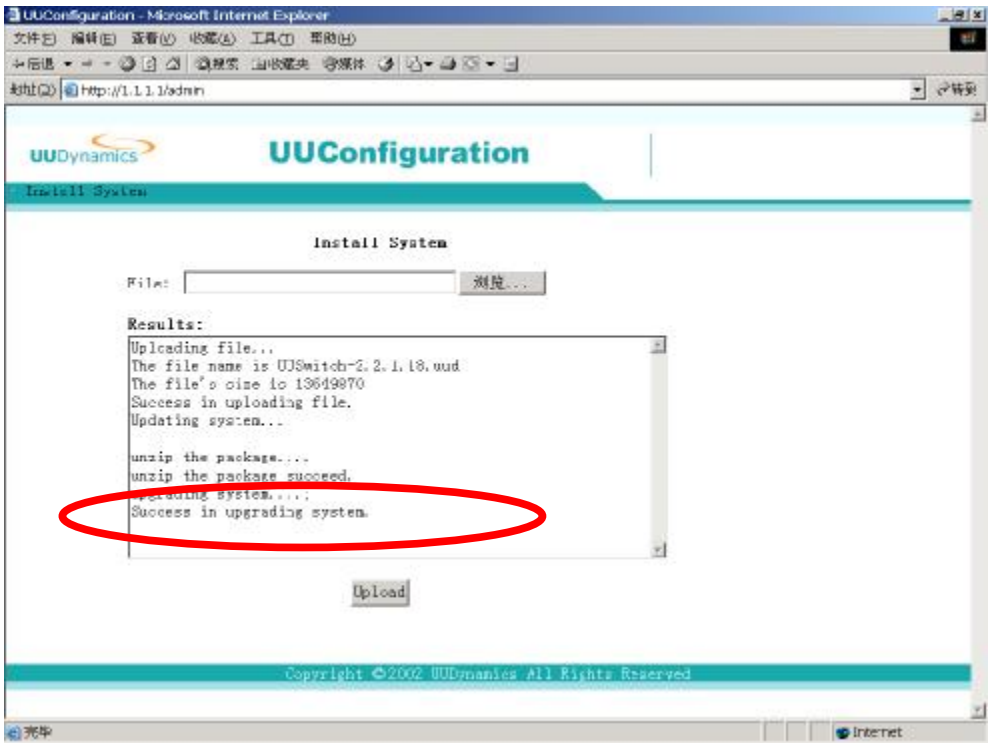


圖 61

5. 按<瀏覽……>，選擇 UUDynamics 套裝軟體，然後按<Upload>，系統會進行安裝。
6. 當“Results”框裏顯示“Success in upgrading system.”資訊，表明安裝完成，請關閉 UUSwitch(/UUExchange)電源，數秒後重新開啓。
7. 當面板上的 LCD 顯示“Unregester”後，在瀏覽器中重新輸入：http://1.1.1.1/admin。
出現使用者登入介面，接下去的操作同本手冊 “安裝 UUSwitch(/UUExchange)軟體”部分。

第6章 故障檢測和排除

（1） 啓動配置環境時，用交叉綫方式將用於配置電腦與 UUSwitch(/UUExchange)連接起來，進行相關 IP 位址的修改後，重啓 UUSwitch(/UUExchange)，但是配置電腦與 UUSwitch(/UUExchange)不能建立連接？

a) 檢查網路是否連通；

b) 檢查網線是否完好無損；

c) 檢查網口是否已插好網線；

（2） 完成基礎設定後，從 UUSwitch（/UUExchange）結果連接或註冊 UUSwitch（/UUExchange）失敗，爲什麼？

a) 網路設定不正確，請檢查路由，使用 ping 工具檢查是否能夠 ping 通 UUSwitch（/UUExchange）；

b) 如果無法 ping 通，且網路設定正確，則應檢查 UUSwitch（/UUExchange）是否啓動；

c) 如果連接成功，註冊不成功，檢查密碼是否正確；

d) 如果密碼正確，則檢查 UUSwitch（/UUExchange），是否確實有此 UUID，且 UUSwitch（/UUExchange）的服務是否已經啓動；

e) 如果 UUSwitch（/UUExchange）的服務已經啓動，則檢查是否已有相同 UUID 註冊。

（3） 配置好叢集後，在查看狀態中沒有見到所有伺服器的叢集 IP。

a) 過一會再看，因爲叢集需要一段時間，才能夠完全叢集成功。

b) 仍然沒有看到，應檢查叢集的配置。各台伺服器上的子網掩碼, 叢集 IP（開始），叢集 IP（結束）是否完全一致。叢集 IP 有沒有衝突。

c) 檢查網綫是否插好，各伺服器是否在同一個 Lan 裏面。

d) 以上一切都正確，但是叢集仍然無法成功，重啓所有的伺服器。

（4） 無法通過 IE 下載使用者端軟體，原因何在，如何解決？

當使用者無法遠端下載使用者端軟體時，請考慮以下兩種可能的原因：

a) 使用者許可權不足；

該使用者可能不具備下載或安裝 ActiveX 元件的許可權，請聯繫管理員確認。

b) 系統是否不支援 ActiveX 元件的下載；

和其他大多數 SSL VPN 產品一樣，UUSwitch(/UUExchange)使用者端機器對 IE 的安全設定有以下要求：

“ActiveX 元件和插件”設定項	設定值

對已標誌爲可安全執行腳本的 ActiveX 元件執行腳本	啓用/提示
下載已簽名的 ActiveX 元件	啓用/提示
運行 ActiveX 元件和插件	啓用/提示

c) 否則 IE 將拒絕下載 UUSwitch(/UUExchange)的使用者端軟體，使用者介面也不會顯示在螢幕上。您可以存取網頁“http://autos.msn.com/gallery/”（該網頁有一些 ActiveX 元件）。通過查看是否所有的圖片都能在該網頁正確顯示，由此可驗證是否能排除這種可能。如果這些圖片確實不能在該網頁正確顯示，請修改您機器上的安全設定。

第7章 附錄

7.1 UUSwitch(/UUExchange)的帶寬計算

在部署一個 iSTAR 時，估測中心交換單元的帶寬需求非常重要。傳統的基於“厄蘭”計算的“電信工程”方法不能真正地在這裏應用，原因是網路包交換的流量模式是不可預測的。Internet 流量的建模和度量雖然已經有很多研究但還沒有很成熟的方法。目前還沒有一種簡單的方法通過公式來計算部署所需的帶寬。基於這種狀況，我們建議一組與部署相關的指導和工具。

4. 爲了算出需要多少個子模式的 UUSwitch(/UUExchange)，我們建議如下：

1. 計算出所需要的帶寬預算，并把它轉換成需要部署在不同 IDC 內的子模式的 UUSwitch(/UUExchange)的個數。希望每個 UUSwitch(/UUExchange)分擔它的 **PAB**(預設的帶寬數量)。
2. 對於每一個子模式的 UUSwitch(/UUExchange)，其性能資料可以由 UUSwitch(/UUExchange)管理軟體來提供。當實際流量超過 PAB 時，UUSwitch(/UUExchange)會產生一個警告資訊。iSTAR 提供者應該定期檢查這個報告并做出相應調整。
3. 我們建議 iSTAR 提供者提供一個連帶式的服務。這時各個使用者就不要共用 iSTAR 社區中共用的子模式 UUSwitch(/UUExchange)，爲了對子模式 UUSwitch(/UUExchange)有更好的可管理性，應該自己租用他們自己的子模式 UUSwitch(/UUExchange)。

7.1.1 子模式 UUSwitch(/UUExchange)的帶寬預算

爲了簡化計算預算過程的複雜性，我們假設所有的 UUSwitch(/UUExchange)都 Co-Lo 在同一個 IDC。對於有不同地點的多個 IDC 的分散式配置，這個方法也要作相應的調整。

對於每一個客戶，我們需要找出兩個參數：

IBI: 客戶占 iSTAR 流量的 Internet 帶寬預算的平均百分比；

SBM: 所售的總帶寬和從上級提供商得到的總帶寬的比率。例如，如果一個服務提供商有一個 T3 連接到主幹（45M），但是，賣了 500 個 0.5M 帶寬的 DSL 連接，則 SBM 爲：(0.5 * 500)/45, 或 5.5.

對於 IDC，我們需要知道：

IBM: 所售給 Co-Lo 客戶的總帶寬和從上級提供商得到的總帶寬的比率。

假設每個從 模式 UUSwitch(/UUExchange)連接一條 100M 的乙太網介面連接到 IDC 主幹網，爲每個 UUSwitch(/UUExchange) 給定一個名義上的 iSTAR 帶寬 50M。對於每一個

UUSwitch(/UUExchange)，所支援的 0.5M DSL 客戶的數量爲：

PAB / ((0.5 * IBI) / SBM), 也就是 (100 * (SBM/IBM))/IBI

PAB 是 50/IBM

很明顯，不同的服務提供商有不同的 SBM。假設最可能的情景是，SBM 和 IBM 有相同的取值範圍，IBI 是 25%(就是說，VPN 流量占 DSL 線路的四分之一)，則每個子模式的 UUSwitch(/UUExchange)支援的客戶數爲 400。（這顯示 IBM 可以是一個比 SBM 更大的倍數）

7.1.2 預算溢出的警告

Co-Lo 的 UUSwitch(/UUExchange)的 100M 名義 iSTAR 帶寬，對於根據原有的貸款預算來監控可能的擁塞問題是令人誤解的和不可靠的。iSTAR 提供者必須收集平均的有效帶寬是多少或每個 UUSwitch(/UUExchange)的 PAB 等資訊。例如，對於一個 45M 連接到主幹的帶寬，賣給 100 個 co-lo 客戶，則最大的有效帶寬應該是 0.45M。（注意，這裏我們也假設所有的流量都要流經主幹網，如果有“內部服務提供”流量，則這 0.45M 還會上升一點）如果 iSTAR 提供者給 UUSwitch(/UUExchange)確定一個預算的帶寬後，UUSwitch(/UUExchange)要監控平均運行流量，當超過設定的預算時，要警告管理員；iSTAR 提供者由此需要考慮增加 UUSwitch(/UUExchange)集群池的數量。

7.1.3 “私有”從 UUSwitch(/UUExchange)

如果對 UUSwitch(/UUExchange)帶寬的消耗充分地超過平均，一個 iSTAR 客戶可以要求一個或多個專用的從 UUSwitch(/UUExchange)。這是一個“批發”銷售，與共用 UUSwitch(/UUExchange)相比應該有一個相對低價。對於 UUSwitch(/UUExchange)而言，是根據同一個公司的發佈單元（Publisher）的 UUID 的域副檔名來識別的。例如，“abc.com”有 5 個發佈單元，名字爲 A@abc.com, B@abc.com, C@abc.com，等等，UUSwitch(/UUExchange)架構就根據具有相同的域擴展命名（abc.com）的 UUID 來確定從 UUSwitch(/UUExchange)。

7.1.4 不需要從 UUSwitch(/UUExchange)（直接連接）

當連接的一方有一個 Public IP 且可以從 Internet 上存取到時，資料就沒有必要通過 UUSwitch(/UUExchange)交換架構來傳輸。如一個發佈單元有靜態 IP，而使用者單元用撥號，就是這種情況。但是，獲得一個“私有的”從 UUSwitch(/UUExchange)可能會比獲得一個靜態 IP 要便宜。

STUN(UDP 簡單穿越 NAT)

STUN 是一個新的通過 UDP 存取 NAT 後面的設備的協定。iSTAR 將會提供對 STUN 的支援，以此來進一步減少對 UUSwitch(/UUExchange)的依賴。

術語表

10~15 劃 …….. 64
10~15 劃 …….. 64
A~Z …….. 65

1~10 劃

主模式/子模式

UUSwitch/UUExchange 有兩種模式可供選擇：主模式和子模式。這兩種模式具有不同的功能。

- 主模式除了提供數據傳輸的功能外，還有管理 UUID 的功能。主模式 UUSwitch/UUExchange 爲其下屬的所有 UU100、UU200 和子模式 UUSwitch/UUExchange 提供 UUID 檔案。在部署的時候，必須有至少一個主模式的 UUSwitch/UUExchange。
- 子模式作爲 UUSwitch/UUExchange 的擴展，可承擔數據傳輸的功能，有效的改善網絡性能。另外，子模式 UUSwitch/UUExchange 隸屬於主模式 UUSwitch/UUExchange，不具有管理 UUID 的功能。子模式 UUSwitch/UUExchange 必須擁有一個由主模式 UUSwitch/UUExchange 頒發的 UUID 文件，并以該 UUID 註冊到主模式 UUSwitch/UUExchange 後，才能夠正常工作。

用戶可根據實際頻寬需求規劃需要使用子模式的 UUSwitch/UUExchange 個數。具體演算法可參考**錯誤! 找不到參照來源。** “UUSwitch(/UUExchange)的帶寬計算”

10~15 劃

第三方證書（數位元電子憑證）

第三方證書是用於該 UUSwitch(/UUExchange)和使用者端之間建立 https 安全連接時所需的標識該伺服器的數位證書。

從第三方發證機構處獲得數位元憑證的申請的方式及費用可以參考以下兩個網站。

http://www.hitrust.com.tw/hitrustexe/frontend/verisign_price.asp

http://www.globaltrust.com.tw/apply/index.html

某些發證機構所簽發的數位憑證，其根憑證沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，在這種情況下，除非使用者將該根憑證輸入到使用者的 IE 瀏覽器根憑證資料庫中，不然會在使用者端跳出一個警告資訊，此時使用者可以用<查看證書>功能鍵檢視數位憑證的詳細內容，待確定之後，按<是>鍵繼續進行操作。

無論第三方發證機構的根憑證有沒有被 Microsoft 公司預先包括在其 IE 的受信任根憑證資料庫之中，都不會影響 iSTAR™的功能。

以下這個網站有詳述 User 如何製作自身的 CSR 檔案，然後再至認證中心申請憑證檔。

http://www.globaltrust.com.tw/support/index.html

http://www.openssl.org/related/binaries.html

注意事項：

- 申請的憑證必須符合 Apache Server 的格式。客戶或經銷商可以利用 OpenSSL 產生 CSR 檔案。
- 由於涉及資訊安全，建議客戶自行辦理較好。

- 建議經銷商或客戶在申請電子憑證時，最好是選擇 DNS Name 而不是 IP。
- 通常辦理電子憑證需，在資料齊全的情況下，應該一個工作天可以完成。

A~Z

UUID

UUID 由主模式 UUSwitch（/UUExchange）分配。UUID 必須是唯一的。用於有效標識發布單元 Publisher（例如：UU100,UU200），以及子模式 UUSwitch(/UUExchange)。

如果 Publisher 的連接方式爲 Private Access 方式，則該 Publisher 必須擁有一個唯一的 UUID。在啓動時 Publisher 用 UUID 註冊到 UUSwitch（/UUExchange）,從而成爲整個 ***i*STAR™**的一部分。

UUID 的格式如 Email 一樣：AAA@bbb.ccc，其中 bbb.ccc 是 Domain 名，例如：aaa@uudynamics.com。

在安裝 Publisher 前，請先聯繫 UUSwitch（/UUExchange）管理員獲取壓縮的 UUID 檔案。