1-1 Active Directory 網域服務概觀

何謂 **directory** 呢？日常生活中的電話簿內記錄著親朋好友的姓名與電話等資料，這是 **telephone directory**（電話目錄）；電腦中的檔案系統（file system）內記錄著檔案的檔名、大小與日期等資料，這是 **file directory**（檔案目錄）。

這些 directory 內的資料若能夠有系統加以整理的話，使用者就能夠很容易與迅速的尋找到所需資料，而 directory service（目錄服務）所提供的服務，就是要讓使用者很容易與迅速的在 directory 內尋找所需資料。

Active Directory 網域內的 directory database（目錄資料庫）被用來儲存使用者帳戶、電腦帳戶、印表機與共用資料夾等物件，而提供目錄服務的元件就是 **Active Directory 網域服務**（Active Directory Domain Services，AD DS），它負責目錄資料庫的儲存、新增、刪除、修改與查詢等工作。

Active Directory 網域服務的適用範圍（Scope）

AD DS 的適用範圍非常廣泛，它可以用在一台電腦、一個小型區域網路（LAN）或數個廣域網路（WAN）的結合。它包含此範圍中的所有物件，例如檔案、印表機、應用程式、伺服器、網域控制站與使用者帳戶等。

名稱空間（Namespace）

名稱空間是一塊界定好的區域（bounded area），在此區域內，我們可以利用某個名稱來找到與此名稱有關的資訊。例如一本電話簿就是一個**名稱空間**，在這本電話簿內（界定好的區域內），我們可以利用姓名來找到此人的電話、地址與生日等資料。又例如 Windows 作業系統的 NTFS 檔案系統也是一個**名稱空間**，在此檔案系統內，我們可以利用檔案名稱來找到此檔案的大小、修改日期與檔案內容等資料。

Active Directory 網域服務（AD DS）也是一個**名稱空間**。利用 AD DS，我們可以透過物件名稱來找到與此物件有關的所有資訊。

在 TCP/IP 網路環境內利用 Domain Name System（DNS）來解析主機名稱與 IP 位址的對應關係，例如透過 DNS 來得知主機的 IP 位址。AD DS 也是與 DNS 緊密的

整合在一起，它的網域**名稱空間**也是採用 DNS 架構，因此網域名稱是採用 DNS 格式來命名，例如可以將 AD DS 的網域名稱命名為 sayms.local。

物件（Object）與屬性（Attribute）

AD DS 內的資源是以物件的形式存在，例如使用者、電腦等都是物件，而物件是透過**屬性**來描述其特徵，也就是說物件本身是一些**屬性**的集合。例如若要為使用者**王喬治**建立帳戶，則需新增一個物件類型（object class）為**使用者**的物件（也就是使用者帳戶），然後在此物件內輸入**王喬治**的姓、名、登入帳戶與地址等資料，其中的使用者帳戶就是物件，而姓、名與登入帳戶等就是該物件的屬性（見表 1-1-1）。另外圖 1-1-1 中的**王喬治**就是物件類型為**使用者**（user）的物件。

表 1-1-1

物件（object）	屬性（attributes）
使用者（user）	姓 名 登入帳戶 地址 …

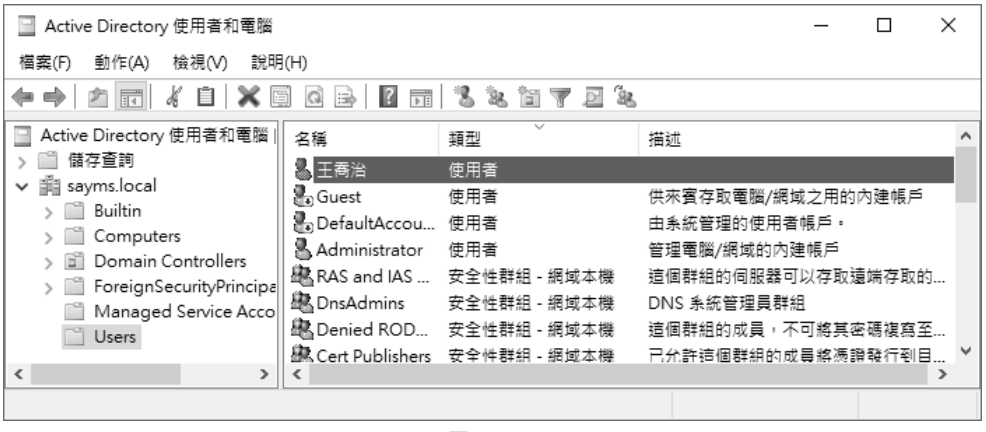

圖 1-1-1

容區（Container）與組織單位（Organization Units，OU）

容區與物件相似，它也有自己的名稱，也是一些屬性的集合，不過容區內可以包含其他物件（例如**使用者**、**電腦**等物件），也可以包含其他容區。而組織單位是一個比較特殊的容區，其內除了可以包含其他物件與組織單位之外，還有**群組原則**（group policy）的功能。

如圖 1-1-2 所示就是一個名稱為**業務部**的組織單位，其內包含著數個物件，其中兩個為**電腦**物件、兩個為**使用者**物件與兩個本身也是組織單位的物件。AD DS 是以階層式的架構（hierarchical）將物件、容區與組織單位等組合在一起，並將其儲存到 AD DS 資料庫內。

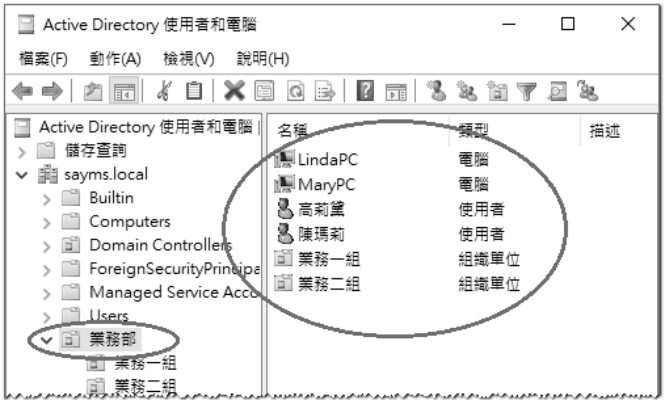

圖 1-1-2

網域樹狀目錄（Domain Tree）

您可以架設內含數個網域的網路，而且是以網域樹狀目錄（domain tree）的形式存在，例如圖 1-1-3 就是一個網域樹狀目錄，其中最上層的網域名稱為 sayms.local，它是此網域樹狀目錄的根網域（root domain）；根網域之下還有 2 個子網域（sales.sayms.local 與 mkt.sayms.local），之下總共還有 3 個子網域。

圖中網域樹狀目錄有符合 DNS 網域名稱空間的命名原則，而且是有連續性的，也就是子網域的網域名稱中包含其父網域的網域名稱，例如網域 sales.sayms.local 的尾碼中包含其前一層（父網域）的網域名稱 sayms.local；而 nor.sales.sayms.local 的尾碼中包含其前一層的網域名稱 sales.sayms.local。

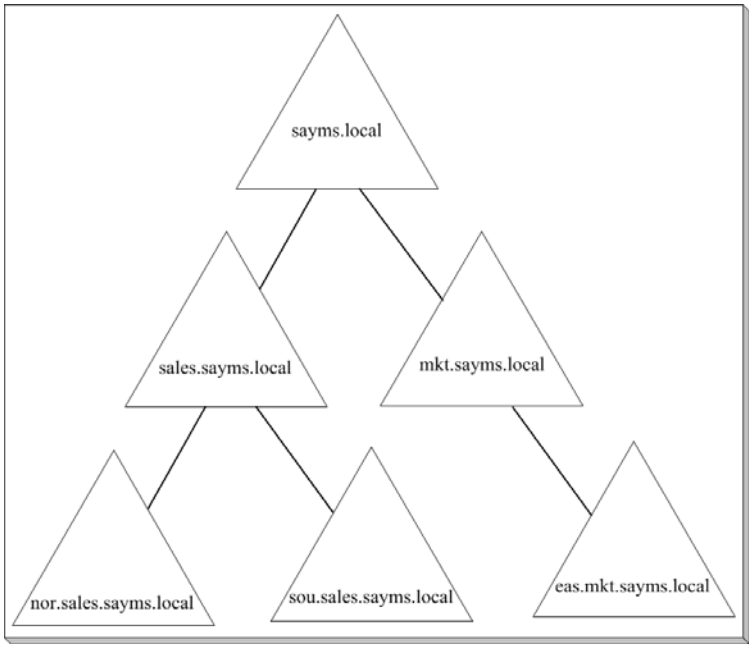

圖 1-1-3

在網域樹狀目錄內的所有網域共用一個 AD DS，也就是在此網域樹狀目錄之下只有一個 AD DS，不過其內的資料是分散儲存在各網域內，每一個網域內只儲存隸屬於該網域的資料，例如該網域內的使用者帳戶（儲存在網域控制站內）。

信任（Trust）

兩個網域之間必須擁有信任關係（trust relationship），才可以存取對方網域內的資源。而任何一個新的 AD DS 網域被加入到網域樹狀目錄後，這個網域便會自動信任其上一層的父網域，同時父網域也會自動信任此新的子網域，而且這些信任關係具備雙向轉移性（two-way transitive）。由於此信任工作是透過 Kerberos security protocol 來完成，因此也被稱為 Kerberos trust。

Q **網域 A 的使用者登入到其所隸屬的網域後，這個使用者可否存取網域 B 內的資源呢？**

A 只要網域 B 有信任網域 A 就沒有問題。

我們以圖 1-1-4 來解釋雙向轉移性，圖中網域 A 信任網域 B（箭頭由 A 指向 B）、網域 B 又信任網域 C，因此網域 A 自動信任網域 C；另外網域 C 信任網域 B（箭頭由 C 指向 B）、網域 B 又信任網域 A，因此網域 C 自動信任網域 A。結果是網域 A 和網域 C 之間自動有著雙向的信任關係。

所以當任何一個新網域加入到網域樹狀目錄後，它會自動雙向信任這個網域樹狀目錄內所有的網域，因此只要擁有適當權限，這個新網域內的使用者便可以存取其他網域內的資源，同理其他網域內的使用者也可以存取這個新網域內的資源。

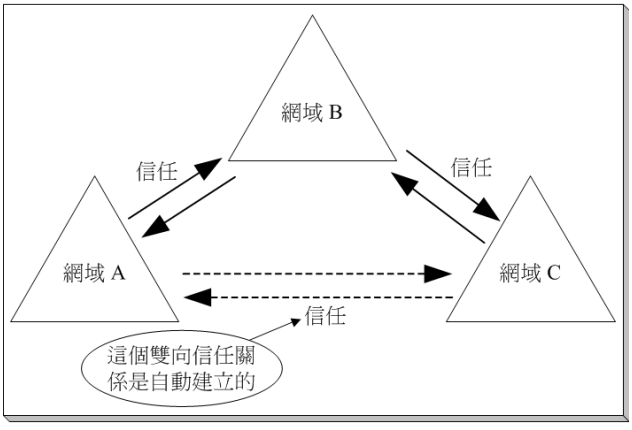

圖 1-1-4

樹系（Forest）

樹系是由一或數個網域樹狀目錄所組成，每一個網域樹狀目錄都有自己唯一的名稱空間，如圖 1-1-5 所示，例如其中一個網域樹狀目錄內的每一個網域名稱都是以 sayms.local 結尾，而另一個則都是以 say365.local 結尾。

第 1 個網域樹狀目錄的根網域，就是整個樹系的根網域（forest root domain），同時其網域名稱就是樹系的樹系名稱。例如圖 1-1-5 中的 sayms.local 是第 1 個網域樹狀目錄的根網域，它就是整個樹系的根網域，而樹系名稱就是 sayms.local。

樹系內，每一個網域樹狀目錄的根網域與樹系根網域之間雙向的、轉移性的信任關係都會自動的被建立起來，因此每一個網域樹狀目錄中的每一個網域內的使用者，只要擁有權限，就可以存取其他任何一個網域樹狀目錄內的資源，也可以到其他任何一個網域樹狀目錄內的成員電腦登入。

「喜好設定」實例演練二

以下假設要讓組織單位**業務部**內的所有使用者，必須透過企業內部的代理伺服器（proxy server）上網。假設代理伺服器的網址為 proxy.sayms.local、連接埠號碼為 8080、用戶端的瀏覽器為 Microsoft Edge（也適用於 Chrome 等瀏覽器）。我們利用前面所建立的**測試用的 GPO** 來練習。

STEP 1 請到網域控制站 dc1 上利用網域系統管理員身分登入。

STEP 2 開啟**伺服器管理員**➲點擊右上角**工具**➲群組原則管理。

STEP 3 在圖 4-3-8 中對著組織單位**業務部**之下的**測試用的 GPO** 按右鍵➲編輯。

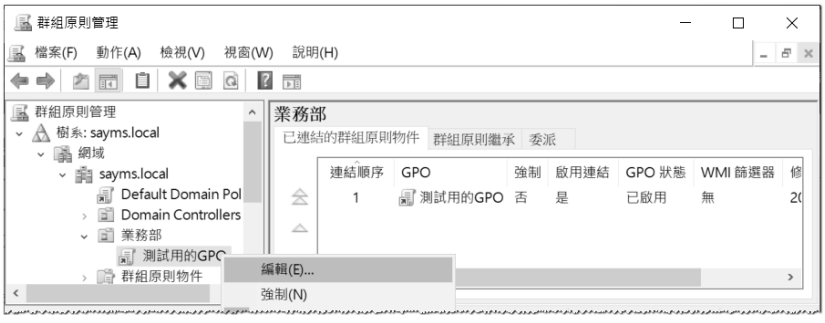

圖 4-3-8

STEP 4 如圖 4-3-9 所示展開【使用者設定➲喜好設定➲控制台設定➲】，然後【對著**網際網路設定**按右鍵➲新增➲Internet Explorer 10】（也適用於 Internet Explorer 11、Microsoft Edge 與 Chrome）。

圖 4-3-9

STEP 5 如圖 4-3-10 所示點擊**連線**標籤下的區域網路設定鈕。

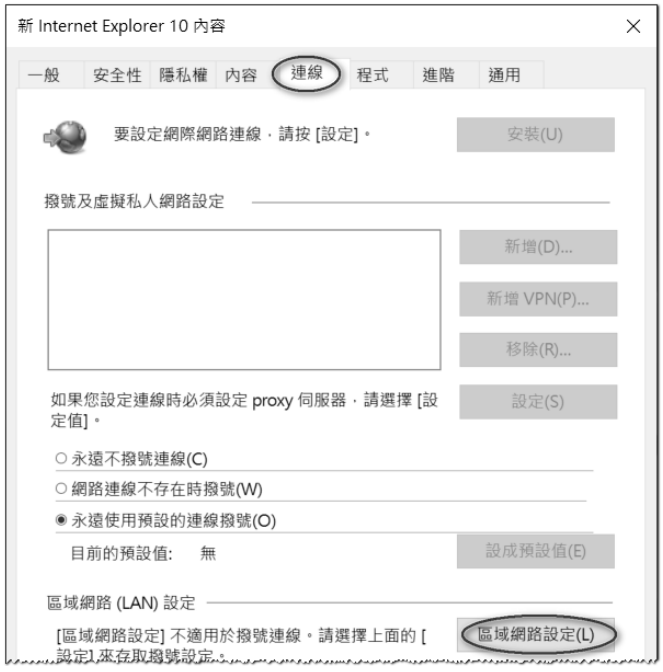

圖 4-3-10

STEP 6 如圖 4-3-11 所示來勾選後輸入代理伺服器網址與連接埠（假設分別是 proxy.sayms.local、8080）➲按 F5 鍵➲按 2 次確定鈕來結束設定】。

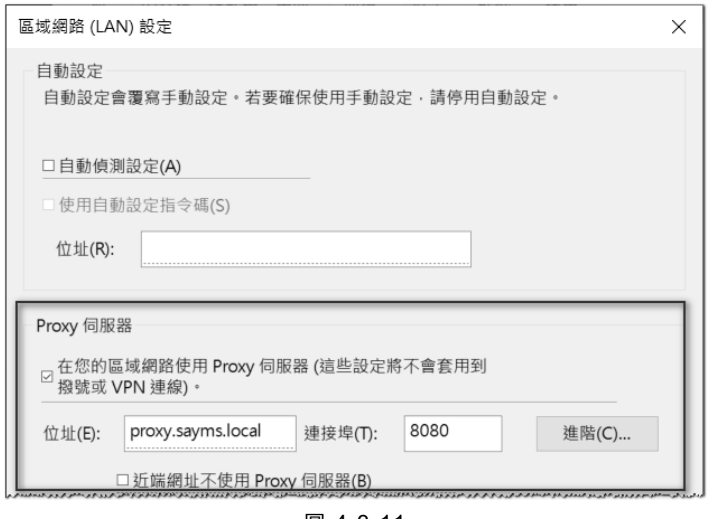

圖 4-3-11

需按 F5 鍵來啟用此標籤下的所有設定（設定項目下代表停用的紅色底線會轉變成綠色）；按 F8 鍵可停用此標籤下的所有設定；若要啟用目前所在的項目的話，請按 F6 鍵、停用請按 F7 鍵。

STEP 7 請利用**業務部**內任何一位使用者帳戶到任何一台網域成員電腦登入。

STEP 8 Windows 11 系統可以透過【點擊下方**開始**圖示➲點擊**設定**圖示➲網路和網際網路（可能需先點擊左上方三條線圖示）➲點擊右方的 **Proxy**➲點擊**手動設定 Proxy** 處的設定鈕】，如圖 4-3-12 所示來查看（而且無法變更這些設定，這是之前練習的原則設定的結果）。

也可以透過【點擊下方**檔案總管**圖示➲對著左下方的**網路**按右鍵➲內容➲點擊左下角**網際網路選項**➲點擊**連線**標籤下的 LAN 設定鈕來插看。

圖 4-3-12

4-4 群組原則的處理規則

網域成員電腦在處理（套用）群組原則時有一定的程序與規則，系統管理員必須了解它們，才能夠透過群組原則來充分的掌控使用者與電腦的環境。

一般的繼承與處理規則

群組原則設定是有繼承性的，也有一定的處理規則：

5-1 軟體部署概觀

您可以透過群組原則來將軟體部署給網域使用者與電腦，也就是網域使用者登入或成員電腦啟動時會自動安裝或很容易安裝被部署的軟體，而軟體部署分為**指派**（assign）與**發佈**（publish）兩種。一般來說，這些軟體需為 Windows Installer Package（也稱為 **MSI 應用程式**），其內包含著副檔名為.msi 的安裝檔案。

> 您也可以部署副檔名為.zap（因限制很多且不實用，故不在本書的討論範圍）或.msp 的軟體，或是將安裝檔附檔名為.exe 的軟體重新包裝成為附檔名是.msi 的 Windows Installer Package（可使用 EMCO MSI Package Builder 等軟體）。

將軟體指派給使用者

當您將一個軟體透過群組原則指派給網域使用者後，使用者在任何一台網域成員電腦登入時，這個軟體會被**通告**（advertised）給該使用者，但系統尚未安裝此軟體，而是會設定與此軟體有關的部分資訊而已，例如可能會在**開始**視窗中自動建立該軟體的捷徑（需視該軟體是否支援此功能而定）。

使用者透過點擊該軟體在**開始**視窗（或**開始**功能表）中的捷徑後，就可以安裝此軟體。使用者也可以透過**控制台**來安裝此軟體，以 Windows 11 用戶端來說，其安裝途徑可為【按 Windows 鍵⊞+ R 鍵➲輸入 control 後按 Enter 鍵➲點擊**程式集**處的**取得程式**】。

將軟體指派給電腦

當您將一個軟體透過群組原則指派給網域成員電腦後，這些電腦啟動時就會自動安裝這個軟體（完整或部分安裝，視軟體而定），而且任何使用者登入都可以使用此軟體。使用者登入後，就可以透過**開始**視窗中的捷徑來使用此軟體。

將軟體發佈給使用者

當您將一個軟體透過群組原則發佈給網域使用者後，此軟體並不會自動被安裝到使用者的電腦內，不過使用者可以透過**控制台**來安裝此軟體，以 Windows 11 用戶

端來說，其安裝途徑可為【按 Windows 鍵⊞+ R 鍵➲輸入 control 後按 Enter 鍵➲點擊**程式集**處的**取得程式**】。

只可以指派軟體給電腦，無法發佈軟體給電腦。

自動修復軟體

被發佈或指派的軟體可以具備自動修復的功能（視軟體而定），也就是用戶端在安裝完成後，之後若此軟體程式內有關鍵性的檔案損毀、遺失或不小心被使用者刪除的話，則在使用者執行此軟體時，其系統會自動偵測到此不正常現象，並重新安裝這些檔案。

移除軟體

一個被發佈或指派的軟體，在用戶端將其安裝完成後，若您之後不想要再讓使用者來使用此軟體的話，可在群組原則內從已發佈或已指派的軟體清單中將此軟體移除，並設定讓用戶端下次套用此原則時（例如使用者登入或電腦啟動時），自動將這個軟體從用戶端電腦中移除。

5-2 將軟體發佈給使用者

以下沿用前幾章的組織單位**業務部**中的**測試用的 GPO**，來練習將 **MSI 應用程式**（Windows Installer Package）發佈給**業務部**內的使用者，並讓使用者透過**控制台**來安裝此軟體。若您還沒有建立組織單位**業務部**與**測試用的 GPO** 的話，請先利用 **Active Directory 管理中心**（或 **Active Directory 使用者和電腦**）與**群組原則管理**來建立，並在**業務部**內新增數個用來練習的使用者帳戶。

發佈軟體

以下步驟將先建立**軟體發佈點**（software distribution point，也就是用來儲存 **MSI 應用程式**的共用資料夾）、接著設定軟體預設的儲存地點、最後再將軟體發佈給使用者。以下將利用免費的文字編輯軟體 AkelPad 來練習，請自行上網下載。

AkelPad 原始安裝檔案是.exe 執行檔，這些檔案可到以下網址下載：
https://sourceforge.net/projects/akelpad/files/

筆者已將其重新包裝為 **MSI 應用程式**，此包裝過的檔案可到碁峰網站下載（http://books.gotop.com.tw/download/ACA027300）。

STEP 1 請在網域中的任何一台伺服器內（假設為 dc1）建立一個用來作為**軟體發佈點**的資料夾，例如 C:\Packages，它將用來儲存 **MSI 應用程式**（Windows Installer Package），例如我們要用來練習的軟體為 **AkelPad 4.4.3** 版。

STEP 2 透過【對著此資料夾按右鍵➲授與存取權給➲特定人員】的途徑，來將此資料夾設定為**共用資料夾**、賦與 Everyone **讀取**權限。

STEP 3 在此共用資料夾內建立用來存放 **AkelPad 4.4.3** 的子資料夾，然後將 **AkelPad 4.4.3** 拷貝到此資料夾內，如圖 5-2-1 所示。

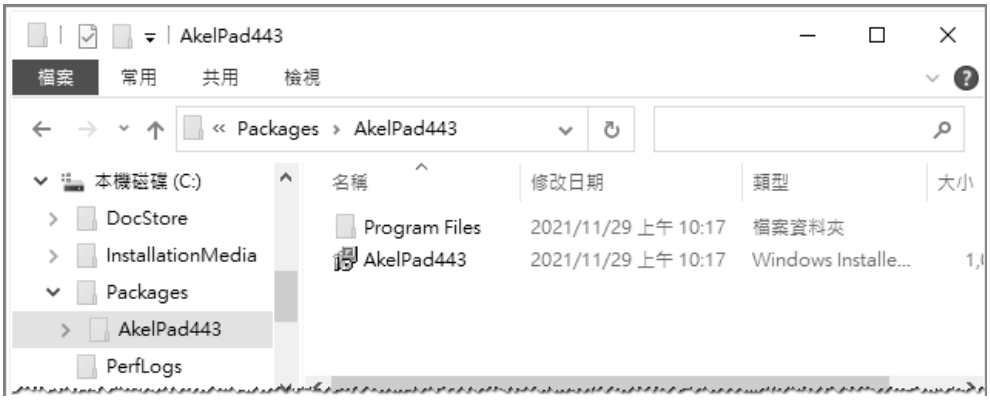

圖 5-2-1

STEP 4 接著設定軟體預設的儲存地點：在網域控制站上【開啟**伺服器管理員**➲點擊右上角**工具**➲群組原則管理➲展開到組織單位**業務部**➲對著**測試用的 GPO** 按右鍵➲編輯➲在圖 5-2-2 中展開**使用者設定**➲原則➲軟體設定➲軟體安裝➲點擊上方的**內容**圖示】。

6-1 軟體限制原則概觀

我們在章節 4-5 內介紹過如何利用檔案名稱來限制使用者可以或不可以執行指定的應用程式，然而若使用者有權變更檔案名稱的話，就可以突破此限制，此時我們仍然可以透過本章的**軟體限制原則**來控管。此原則的安全等級分為以下三種：

- **沒有限制**：也就是所有登入的使用者都可以執行指定的程式（只要使用者擁有適當的存取權限，例如 NTFS 權限）。
- **不允許**：不論使用者對程式檔案的存取權限為何，都不允許執行。
- **基本使用者**：允許以一般使用者的權限（users 群組的權限）來執行程式。

系統預設的安全等級是所有程式都**沒有限制**，也就是只要使用者對欲執行的程式檔案擁有適當存取權限的話，他就可以執行此程式。不過您可以透過**雜湊規則**、**憑證規則**、**路徑規則**與**網路區域規則**等 4 種規則來建立例外的安全等級，以便拒絕使用者執行所指定的程式。

雜湊規則

雜湊（hash）是根據程式的檔案內容所算出來的一連串位元組，不同程式有著不同的雜湊值，所以系統可用它來辨識程式。在您替某個程式建立**雜湊規則**，並利用它限制使用者不允許執行此程式時，系統就會為該程式建立雜湊值。而當使用者要執行此程式時，其 Windows 系統就會比對自行算出來的雜湊值是否與軟體限制原則中的雜湊值相同，若相同，表示它就是被限制的程式，因此會被拒絕執行。

即使此程式的檔案名稱被改變或被搬移到其他地點，也不會改變其雜湊值，因此仍然會受到雜湊規則的約束。

若使用者電腦端的程式檔案內容被變更的話（例如感染電腦病毒），此時因為使用者的電腦所算出的雜湊值，並不會與雜湊規則中的雜湊值相同，因此不會認為它是受限制的程式，故不會拒絕此程式的執行。