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（參見表 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 …

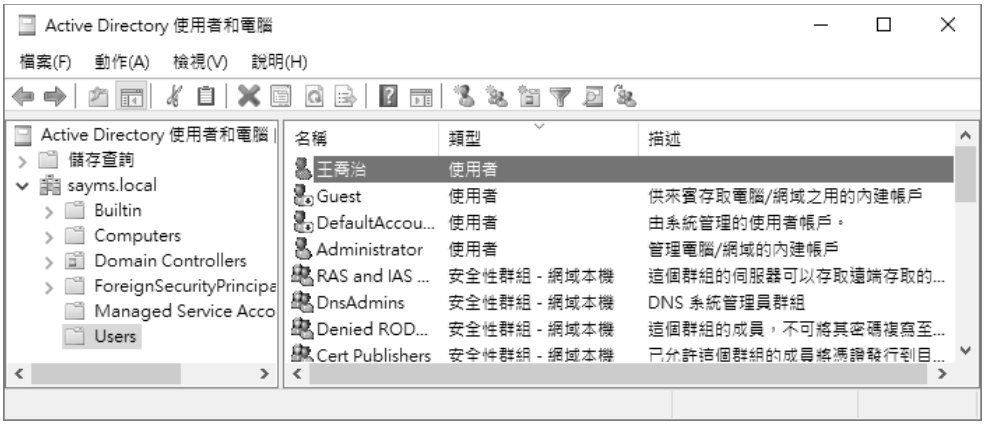

圖 1-1-1

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 會自動信任網域 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 會自動信任網域 A。結果是網域 A 和網域 C 之間也就自動地建立起雙向的信任關係。

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。

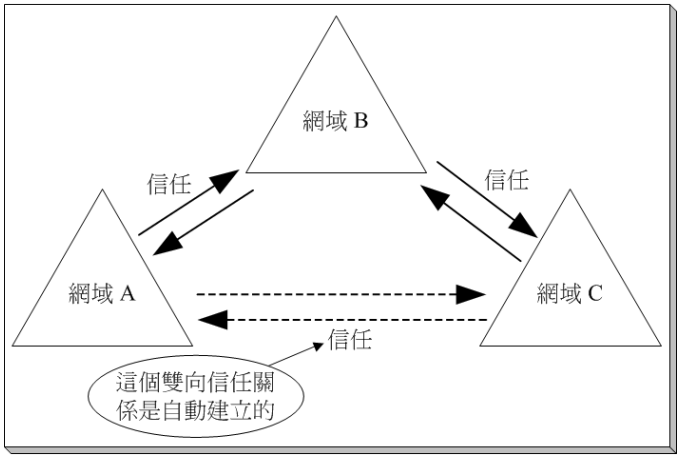

圖 1-1-4

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，

被複寫（replicate）到其他網域控制站的 AD DS 資料庫（如圖 1-1-6），以便讓所有網域控制站內的 AD DS 資料庫都能夠同步（synchronize）。

當使用者在某台網域成員電腦登入時，會由其中一台網域控制站根據其 AD DS 資料庫內的帳戶資料，來審核使用者所輸入的帳戶與密碼是否正確。若是正確的，使用者就可以登入成功；反之，會被拒絕登入。

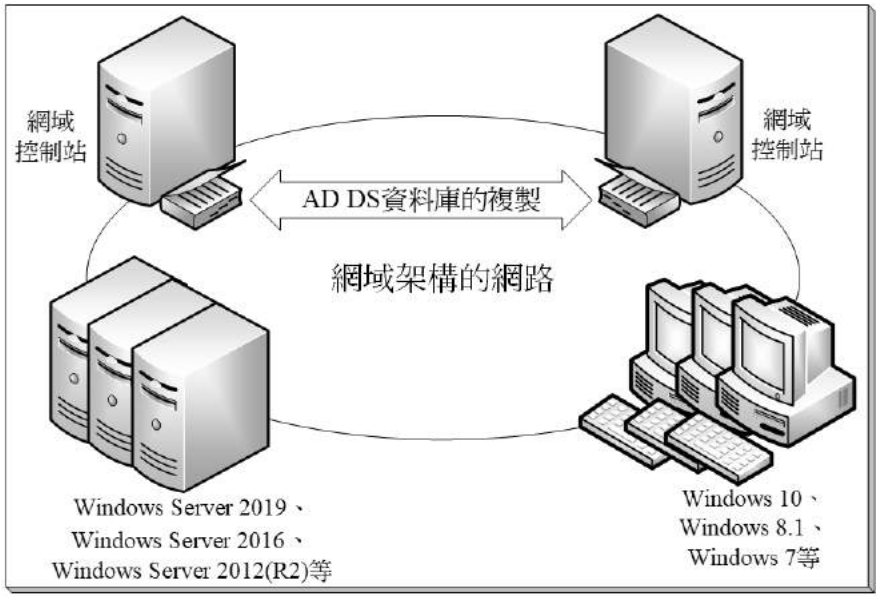

圖 1-1-6

多台網域控制站還可以提供容錯功能，例如雖然其中一台網域控制站故障了，但是其他網域控制站仍然能夠繼續提供服務。另外它也可以改善使用者的登入效率，因為多台網域控制站可以分擔審核使用者登入身分（帳戶名稱與密碼）的負擔。

網域控制站是由伺服器等級的電腦來扮演的，例如 Windows Server 2019、Windows Server 2016、Windows Server 2012（R2）等。

唯讀網域控制站（RODC）

唯讀網域控制站（Read-Only Domain Controller，RODC）的 AD DS 資料庫只可以被讀取、不可以被修改，也就是說使用者或應用程式無法直接修改 RODC 的 AD DS 資料庫。RODC 的 AD DS 資料庫內容只能夠從其他**可寫式網域控制站**複寫過

2-1 建立 AD DS 網域前的準備工作

建立 AD DS 網域的方法，可以先安裝一台伺服器，然後再將其升級（promote）為網域控制站。在建立 AD DS 網域前，請先確認以下的準備動作是否已經完成：

- 選擇適當的 DNS 網域名稱
- 準備好一台用來支援 AD DS 的 DNS 伺服器
- 選擇 AD DS 資料庫的儲存地點

選擇適當的 DNS 網域名稱

AD DS 網域名稱是採用 DNS 的架構與命名方式，因此請先為 AD DS 網域取一個符合 DNS 格式的網域名稱，例如 sayms.local（以下皆以虛擬的**最高層網域**名稱.local 為例來說明）。

準備好一台支援 AD DS 的 DNS 伺服器

在 AD DS 網域中，網域控制站會將自己所扮演的角色登記到 DNS 伺服器內，以便讓其他電腦透過 DNS 伺服器來找到這台網域控制站，因此需要一台 DNS 伺服器，且它需支援 SRV 記錄，同時最好支援**動態更新**、Incremental Zone Transfer 與 Fast Zone Transfer 等功能：

- **Service Location Resource Record（SRV RR）**：網域控制站需將其所扮演的角色登記到 DNS 伺服器的 SRV 記錄內，因此 DNS 伺服器需支援此類型的記錄。Windows Server 的 DNS 伺服器與 BIND DNS 伺服器都支援此功能。
- **動態更新**：若未支援動態更新功能的話，則網域控制站將無法自動將自己登記到 DNS 伺服器的 SRV 記錄內，此時便需由系統管理員手動將資料輸入到 DNS 伺服器，如此勢必增加管理負擔。Windows Server 與 BIND 的 DNS 伺服器都支援此功能。
- **Incremental Zone Transfer（IXFR）**：它讓此 DNS 伺服器與其他 DNS 伺服器之間在執行**區域轉送**（zone transfer）時，只會複寫最新異動記錄，而不是複

寫區域內的所有記錄。它可提高複寫效率、減少網路負擔。Windows Server 與 BIND 的 DNS 伺服器都支援此功能。

- **Fast Zone Transfer**：它讓 DNS 伺服器可以利用**快速傳送格式**將區域內的記錄複寫給其他 DNS 伺服器。**快速傳送格式**可將資料壓縮、每一筆傳送訊息內可包含多筆記錄。Windows Server 與 BIND 的 DNS 伺服器都支援此功能。

  Windows Server 的 DNS 伺服器預設已啟用**快速傳送**，但有些廠商的 DNS 伺服器並不支援此功能，故若要透過**區域轉送**將記錄複寫給此 DNS 伺服器的話，需停用此功能（以 Windows Server 2019 為例）：【點擊左下角**開始**圖示➲**伺服器管理員**➲點擊右上角**工具**➲DNS➲對著 DNS 伺服器按右鍵➲內容➲如圖 2-1-1 所示勾選**進階**標籤下的**啟用次要 BIND**】。

圖 2-1-1

您可以採用以下兩種方式之一來架設 DNS 伺服器：

- 在將伺服器升級為網域控制站時，順便讓系統自動在這台伺服器上安裝 DNS 伺服器，它還會自動建立一個支援 AD DS 網域的 DNS 區域，例如 AD DS 網域名稱為 sayms.local，則其所自動建立的區域名稱為 sayms.local，並自動啟用**只有安全的**動態更新。

  請先在這台即將成為網域控制站與 DNS 伺服器電腦上，清除其**慣用 DNS 伺服器**的 IP 位址或改為輸入自己的 IP 位址（如圖 2-1-2 所示），無論選擇哪一種設定方式，升級時系統都可以自動安裝 DNS 伺服器角色。

2-2 建立 AD DS 網域

以下利用圖 2-2-1 來說明如何建立第 1 個樹系中的第 1 個網域（根網域）：我們將先安裝一台 Windows Server 2019 伺服器，然後將其升級為網域控制站與建立網域。我們也將架設此網域的第 2 台網域控制站（Windows Server 2019）、第 3 台網域控制站（Windows Server 2019）、一台成員伺服器（Windows Server 2019）與一台加入 AD DS 網域的 Windows 10 電腦。

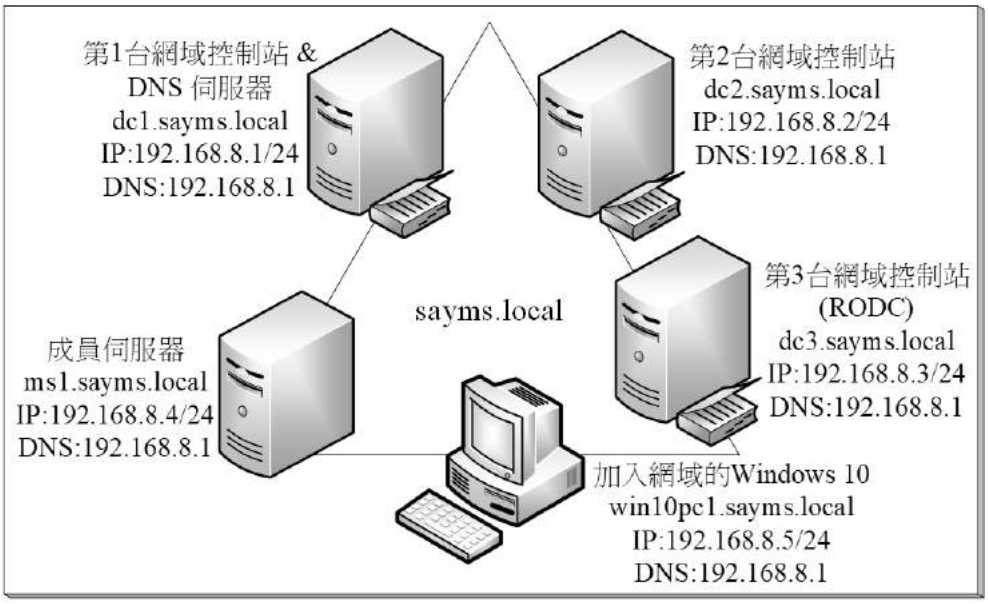

圖 2-2-1

建議利用 Windows Server 2019 Hyper-V 等提供虛擬環境的軟體來建置圖中的網路環境。若圖中的虛擬機器是從現有的虛擬機器複製來的話，記得他們需要執行 C:\windows\System32\Sysprep 內的 Sysprep.exe，並勾選**一般化**。

若要將現有網域升級的話，則樹系中的網域控制站都必須是 Windows Server 2008（含）以上的版本，而且需先分別執行 Adprep /forestprep 與 Adprep /domainprep 指令來為樹系與網域執行準備工作，此指令檔位於 Windows Server 2019 光碟 support\adprep 資料夾。其他升級步驟與作業系統升級的步驟類似。

網域控制站之間資料的複寫

若網域內有多台網域控制站的話，則當您變更 AD DS 資料庫內的資料時，例如利用 **Active Directory 管理中心**（或 **Active Directory 使用者和電腦**）來新增、刪除、修改使用者帳戶或其他物件，則這些異動資料會先被儲存到您所連接的網域控制站，之後再自動被複寫到其他網域控制站。

您可如圖 3-1-30 所示【對著網域名稱按右鍵➲變更網域控制站➲目前的網域控制站】來得知目前所連接的網域控制站，例如圖中的 dc1.sayms.local，而此網域控制站何時會將其最新異動資料複寫給其他網域控制站呢？這分為以下兩種情況：

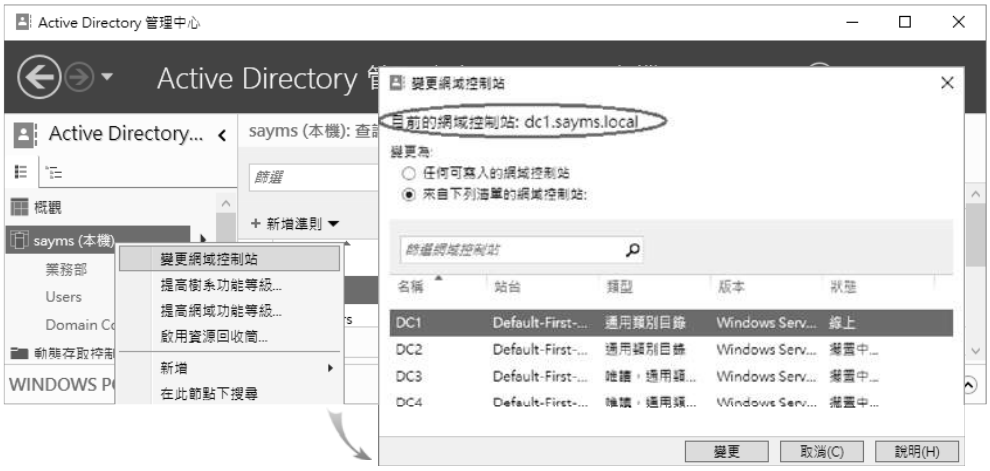

圖 3-1-30

- **自動複寫**：若是同一個站台內的網域控制站，則預設是 15 秒鐘後會自動複寫，因此其他網域控制站可能會等 15 秒或更久時間就會收到這些最新的資料；若是位於不同站台的網域控制站，則需視所排定的時程來決定（詳見第 9 章）。
- **手動複寫**：有時候可能需要手動複寫，例如網路故障造成複寫失敗，而您不希望等到下一次的自動複寫，而是希望能夠立刻複寫。以下假設要從網域控制站 DC1 複寫到 DC2。請到任一台網域控制站上【開啟**伺服器管理員**➲點擊右上角**工具**功能表➲Active Directory 站台及服務➲Sites➲Default-First-Site-Name➲Servers➲展開目的地網域控制站（DC2）➲如圖 3-1-31 所示點擊 **NTDS Settings**➲對著右邊來源網域控制站（DC1）按右鍵➲立即複寫】。

網域內的群組類型

AD DS 的網域群組分為以下兩種類型，且它們之間可以相互轉換：

- **安全性群組**（security group）：它可以被用來指定權限，例如可以指定它對檔案具備**讀取**的權限。它也可以被用在與安全無關的工作上，例如可以發送電子郵件給安全性群組。
- **發佈群組**（distribution group）：它被用在與安全（權限設定等）無關的工作上，例如您可以發送電子郵件給發佈群組，但是無法指派權限給它。

群組的使用領域

以群組的使用領域來看，網域內的群組分為以下三種（見表 3-3-1）：網域本機群組（domain local group）、全域群組（global group）、萬用群組（universal group）。

表 3-3-1

特性 \ 群組	網域本機群組	全域群組	萬用群組
可包含的成員	所有網域內的使用者、全域群組、萬用群組；相同網域內的網域本機群組	相同網域內的使用者與全域群組	所有網域內的使用者、全域群組、萬用群組
可以在哪一個網域內被設定使用權限	同一個網域	所有網域	所有網域
群組轉換	可以被換成萬用群組（只要原群組內的成員不含網域本機群組即可）	可以被換成萬用群組（只要原群組不隸屬於任何一個全域群組即可）	可以被換成網域本機群組；可以被換成全域群組（只要原群組內的成員不含萬用群組即可）

網域本機群組

它主要是被用來指派其所屬網域內的權限，以便可以存取該網域內的資源。

- 其成員可以包含任何一個網域內的使用者、全域群組、萬用群組；也可以包含相同網域內的網域本機群組；但無法包含其他網域內的網域本機群組。

解決方法是強制用戶端一定要處理指定的原則，不論該原則設定值是否有異動。您可以針對不同原則來個別設定。舉例來說，假設要強制組織單位**業務部**內所有電腦必須處理（套用）**軟體安裝原則**的話：在**測試用的 GPO** 的設定中選用【電腦設定➲原則➲系統管理範本➲系統➲如圖 4-4-8 所示雙擊**群組原則**右方的**設定軟體安裝原則處理➲**點選**已啟用➲**勾選**即使群組原則物件尚未變更也進行處理➲**按確定鈕】。

原則名稱最後兩個字是**處理**（processing）的原則設定都可以做類似的變更。

若要手動讓電腦來強制處理（套用）所有的電腦原則或使用者原則設定的話，可以分別執行 **gpupdate /target:computer /force** 指令或 **gpupdate /target:user /force** 指令；而 **gpupdate /force** 指令可同時強制處理電腦與使用者設定。

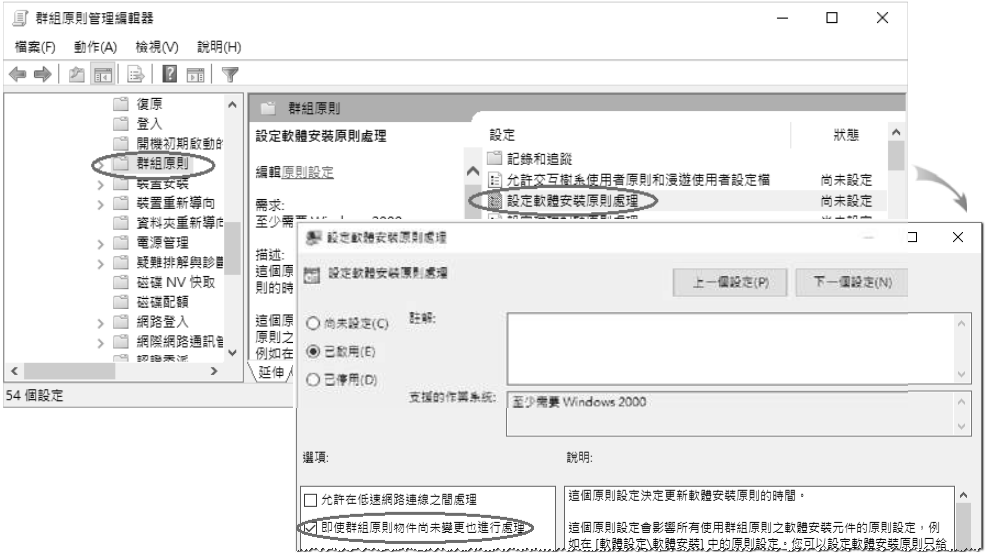

圖 4-4-8

低速連線的 GPO 處理

您可以讓網域成員電腦自動偵測其與網域控制站之間的連線速度是否太慢，若是的話，就不要套用位於網域控制站內指定的群組原則設定。除了圖 4-4-9 中**設定登錄原則處理**與**設定安全性原則處理**這兩個原則之外（無論是否低速連線都會套用），其他原則都可以設定為低速連線不套用。

- 1－24：表示要保存密碼歷史記錄。例如若設定為 5，則使用者的新密碼不可與前 5 次所使用過的舊密碼相同。
- 0：表示不保存密碼歷史記錄，因此密碼可以重複使用，也就是使用者更改密碼時，可以將其設定為以前曾經使用過的任何一個舊密碼。

AD DS 網域的預設值為 24，獨立伺服器的預設值為 0。

- **最小密碼長度**：用來設定使用者帳戶的密碼最少需幾個字元。此處可為 0－14，若為 0，表示使用者帳戶可以沒有密碼。AD DS 網域的預設值為 7，獨立伺服器的預設值為 0。

帳戶鎖定原則（account lockout policy）

您可以透過圖 4-5-6 中的**帳戶鎖定原則**來設定鎖定使用者帳戶的方式。

圖 4-5-6

- **帳戶鎖定閾值**：我們可以讓使用者登入多次失敗後（密碼錯誤），就將該使用者帳戶鎖定，在未被解除鎖定之前，使用者無法再利用此帳戶來登入。此處用來設定登入失敗次數，其值可為 0－999。預設為 0，表示帳戶永遠不會被鎖定。
- **帳戶鎖定時間**：用來設定鎖定帳戶的期限，期限過後會自動解除鎖定。此處可為 0－ 99999 分鐘，若為 0 分鐘表示永久鎖定，不會自動被解除鎖定，此時需由系統管理員手動來解除鎖定，也就是如圖 4-5-7 所示點擊使用者帳戶內容的**帳戶**區段處的**解除鎖定帳戶**（帳戶被鎖定後才會有此選項）。

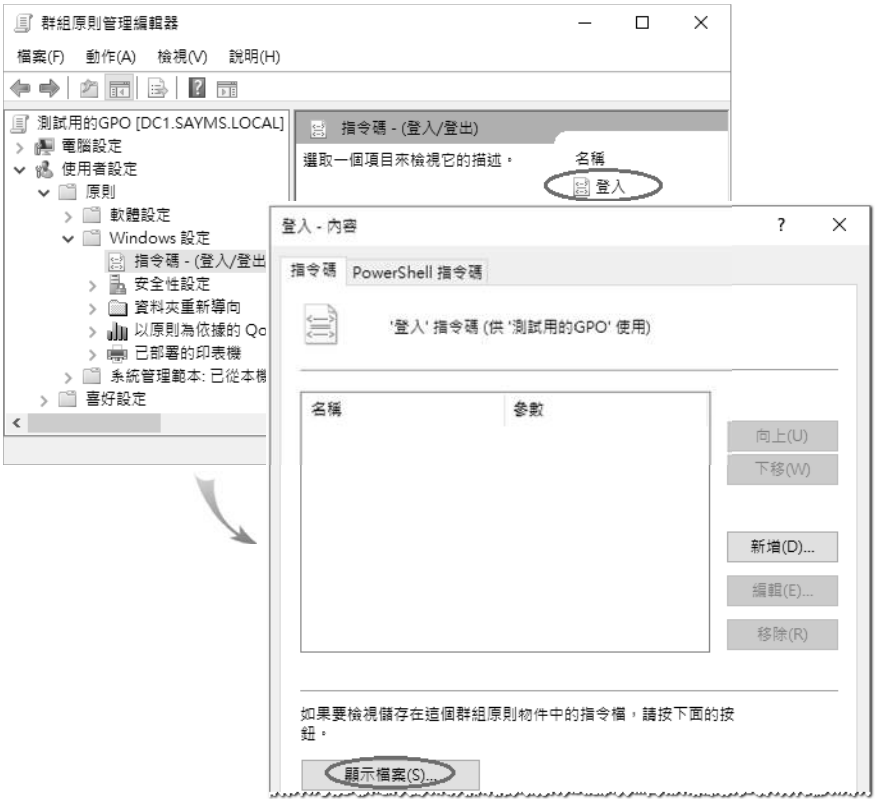

圖 4-5-10

STEP 3 出現圖 4-5-11 的畫面時，請將登入指令碼檔 logon.bat 貼到畫面中的資料夾內，此資料夾是位於網域控制站的 SYSVOL 資料夾內，其完整路徑為（其中的 *GUID* 是**測試用的 GPO** 的 GUID）：

%*systemroot*%\SYSVOL\sysvol*網域名稱*\Policies\{*GUID*}\User\Scripts\Logon

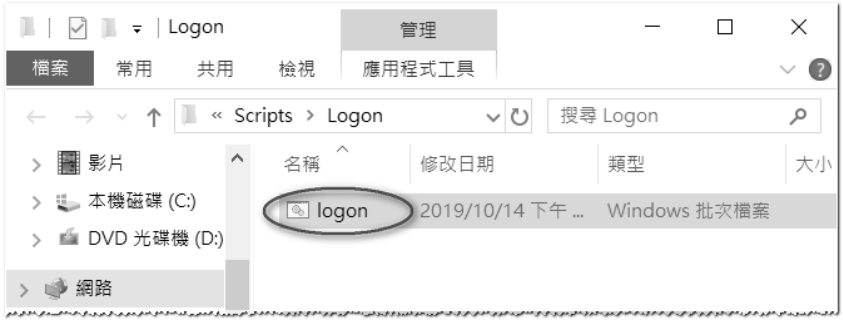

圖 4-5-11

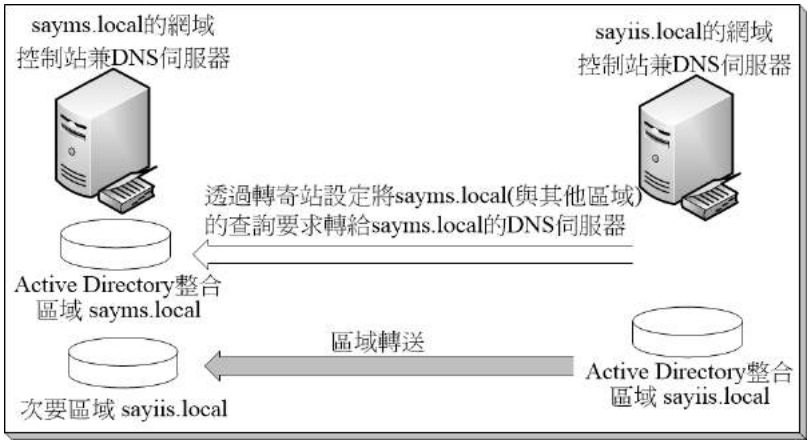

圖 7-3-3

不過您還必須在左邊的 DNS 伺服器內自行建立一個 sayiis.local 次要區域，此區域內的記錄需要透過**區域轉送**從右邊的 DNS 伺服器複寫過來，它讓網域 sayms.local 的成員電腦可以找到網域 sayiis.local 的成員電腦。

您也可以在左邊的 DNS 伺服器內，透過**條件轉寄站**只將 sayiis.local 的查詢轉給右邊的 DNS 伺服器，如此就可以不需要建立次要區域 sayiis.local，也不需區域轉送。注意由於右邊的 DNS 伺服器已經使用**轉寄站**設定將 sayiis.local 之外的所有其他區域的查詢，轉寄給左邊的 DNS 伺服器，因此左邊 DNS 伺服器請使用**條件轉寄站**，而不要使用一般的**轉寄站**，否則除了 sayms.local 與 sayiis.local 兩個區域之外，其他區域的查詢將會在這兩台 DNS 伺服器之間循環。

建立第 2 個網域樹狀目錄

以下採用圖 7-3-3 的 DNS 架構來建立樹系中第 2 個網域樹狀目錄 sayiis.local，且是透過將前面圖 7-3-1 中 dc5.sayiis.local 升級為網域控制站的方式來建立此網域樹狀目錄，這台伺服器可以是獨立伺服器或隸屬於其他網域的現有成員伺服器。