解析 NetBIOS 名稱

A

NetBIOS 名稱是傳統的老舊名稱，早就應該被 DNS 名稱取代，可是有些傳統應用程式或服務還在使用 NetBIOS 名稱，因此除非可以完全確認不再使用 NetBIOS 名稱，例如完全採用 IPv6（NetBIOS 不支援 IPv6），否則還是需要瞭解 NetBIOS。

附註

常常有人在問 NetBIOS 與 WINS 伺服器是否還有必要存在，此問題或許可以參考**職念文**先生所寫的文章「**探討 Disable NetBIOS over TCP/IP 可行性**」，請自行上網搜尋此文章，但建議您看完第 3 與 4 章後，再來閱讀此文章。

A-1　利用 NetBIOS 名稱來與其他電腦溝通

電腦與電腦之間，需相互知道對方的 IP 位址後，雙方才可以相互溝通，可是對使用電腦的人來說，IP 位址是數字的組合，不容易看出是哪一台電腦、也不容易記憶，相反的，NetBIOS 電腦名稱不但容易從字面知道是哪一台電腦，且容易記憶。

因此使用者利用 NetBIOS 名稱會比較方便，然而當使用者利用對方的 NetBIOS 電腦名稱來與此電腦溝通時，使用者的電腦需找到此 NetBIOS 電腦名稱的 IP 位址，這個動作被稱為 **NetBIOS 名稱解析**（NetBIOS name resolution）。

何謂 NetBIOS 名稱

NetBIOS 名稱是一個佔用 16 個字元的字串，在 Microsoft 網路內會用到 NetBIOS 名稱的有電腦名稱、網域名稱、工作群組名稱等，例如 Server1、Domain1、Workgroup1。圖 A-1-1 中的電腦名稱 **Server1** 與工作群組名稱 **WORKGROUP** 都是 NetBIOS 名稱。

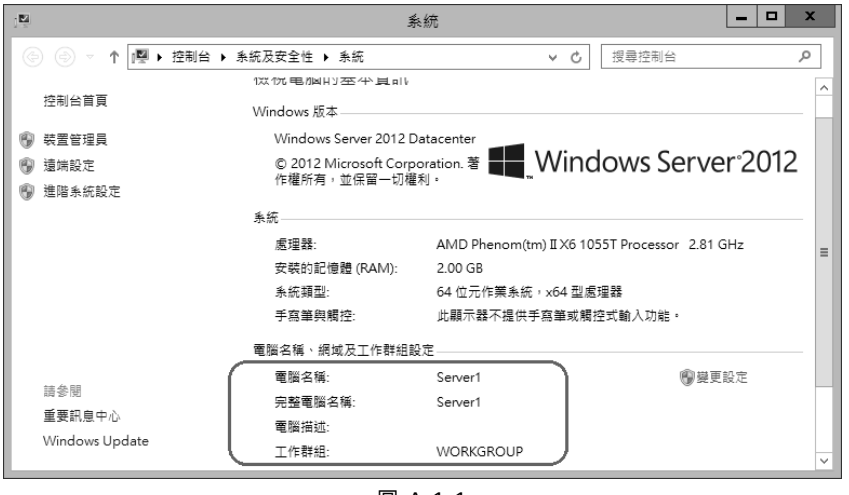

圖 A-1-1

網路中的電腦會宣告（登記）其所擁有的 NetBIOS 電腦名稱與 IP 位址，而且一個 NetBIOS 名稱在網路上只能夠被使用一次，例如若您的 NetBIOS 電腦名稱為 Server1，當此電腦啟動時，它會檢查此名稱是否已經被網路上其他電腦登記，若被登記了，您的電腦就無法使用此電腦名稱。反過來說，若您的電腦先啟動，之

後另外一台電腦名稱也是 Server1 的電腦在啟動時也會做相同的檢查動作，但是因為此電腦名稱已經被您的電腦登記了，因此另外一台電腦就無法使用此電腦名稱。

附註

若將此電腦加入網域的話，則其電腦名稱會有尾碼（也可手動設定其尾碼），例如假設尾碼為 sayms.local，則圖 A-1-1 中的**完整電腦名稱**會是 server1.sayms.local，此名稱又被稱為 **DNS 名稱**或**完整網域名稱**（Fully Qualified Domain Name，FQDN），DNS 名稱（FQDN）的解析方法與 NetBIOS 名稱的解析方法並不相同，DNS 名稱解析方法請參考第 3 章。

您可以如圖 A-1-2 所示利用 **nbtstat -n** 指令來查看此電腦目前所登記的 NetBIOS 名稱（假設其 IP 位址為 192.168.8.20。NetBIOS 名稱不分大小寫），圖中電腦名稱為 SERVER1，而 WORKGROUP 為其工作群組名稱。

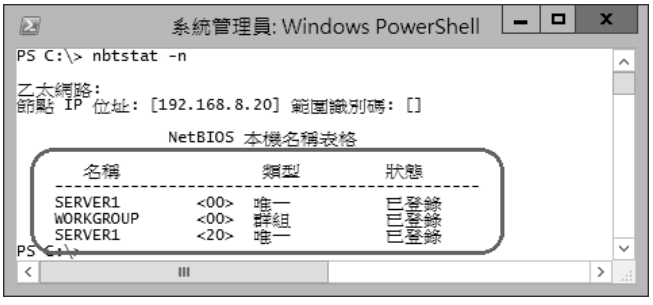

圖 A-1-2

圖中為何有兩個名稱為 SERVER1 的 NetBIOS 電腦名稱呢？因為此電腦不但會登記電腦名稱與 IP 位址，也會將它所提供的部份服務登記到網路上，因此會有多個 SERVER1 的電腦名稱。在這些名稱之後有一個特殊數值，例如第 1 個 SERVER1 後面的<20>就是用來表示此電腦所提供的服務種類。NetBIOS 電腦名稱最多 15 個字元加上 1 個有特殊用途的第 16 個字元，這個第 16 個字元就是用來代表此電腦所提供的服務種類，例如：

- **00**：代表**工作站服務**，若此服務啟動的話（這是預設值），便可以透過網路來與其他電腦溝通。
- **20**：代表**伺服器服務**，若此服務啟動的話（這是預設值），便可以讓其他電腦來與這台電腦溝通。

圖 A-1-2 中兩個 SERVER1 開頭的 NetBIOS 名稱是唯一的，也就是網路上只能夠有一台電腦來登記這個名稱。另外還有群組名稱，它可以讓多台電腦登記到同一個群組名稱之下，例如圖 A-1-2 中的“WORKGROUP　<00>”，它表示 IP 位址為 192.168.8.20 的電腦是被登記到此名稱之下，也就是說此電腦是隸屬於工作群組 WORKGROUP。此“WORKGROUP　<00>”的 NetBIOS 名稱可讓隸屬於 WORKGROUP 群組的所有電腦來登記。

電腦啟動時預設就會啟動上述的**工作站服務**（Workstation Service）與**伺服器服務**（Server Service），而您可以透過【開啟**系統管理工具➲**服務】的途徑來查看與管理這兩個服務，如圖 A-1-3 所示為**伺服器服務**（Server Service），請不要隨意變更或停止這兩個服務，否則會影響到此電腦與其他電腦之間的溝通。

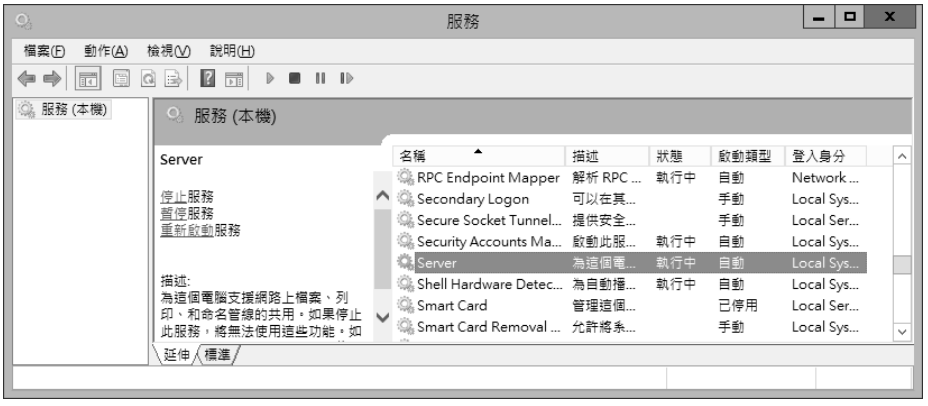

圖 A-1-3

透過 NetBIOS 名稱來解析 IP 位址

當您的電腦想要透過網路來與其他電腦溝通時，它是如何依據對方的電腦名稱來得知（解析）其 IP 位址呢？名稱解析的方法有以下幾種：

- **檢查 NetBIOS 名稱快取區**：若您的電腦之前曾經與對方電腦溝通過，則對方的電腦名稱與 IP 位址就會被儲存到您的電腦的 NetBIOS 名稱快取區。透過快取區能夠讓您的電腦快速找到對方的 IP 位址。快取區內的每一筆資料都有一定的有效期限（預設是 10 分鐘），期限到時，該筆資料就會從快取區清除。您可以利用 **nbtstat –c**（小寫 **c**）指令來查看 NetBIOS 快取區的資料，例如

圖 A-1-4 中快取區包含著電腦名稱為 DC 的 IP 位址與相關資料，此筆資料的有效期限還剩下 593 秒。

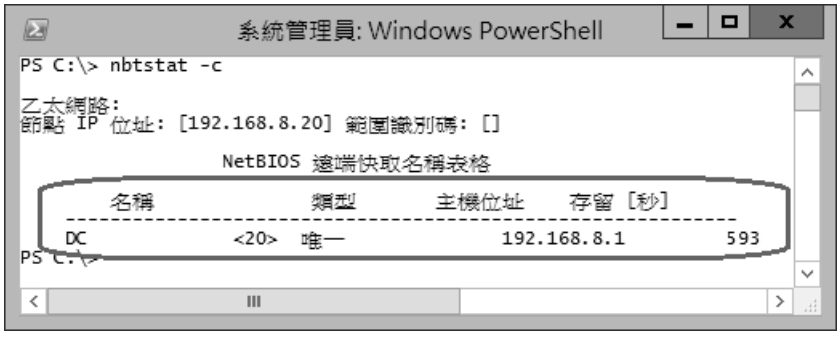

圖 A-1-4

- **廣播**：您的電腦利用送出廣播訊息的方式來找尋對方的 IP 位址，擁有此電腦名稱的電腦收到廣播訊息後，就會將它的 IP 位址告訴您的電腦。

> **注意**
>
> 應該儘量避免使用廣播方式，因為廣播封包會增加網路的負擔。

- **直接向 WINS 伺服器查詢**：由於 WINS 用戶端會將其電腦名稱與 IP 位址等資料登記到 WINS 伺服器，因此 WINS 用戶端可以透過 WINS 伺服器來得知其他 WINS 用戶端電腦的 IP 位址。

NetBIOS 節點類型

網路上的電腦會採用哪一種名稱解析方法來找尋其他電腦的 IP 位址呢？這要看該電腦所採用的 NetBIOS 節點類型（node-type）而定：

- **B 節點（B-node）**：它利用廣播方式來找尋 IP 位址。例如當電腦 PC1 欲與 PC2 溝通時，它會將“找尋 PC2 的 IP 位址”的訊息廣播出去，當 PC2 收到訊息後，就會將其 IP 位址傳送給 PC1，因此 PC1 便可以與 PC2 溝通。

  廣播訊息會增加網路負擔，且若 PC2 是位於另外一個網路的話，則廣播方式會失敗，因為路由器不會將此廣播訊息傳遞到另一個網路。

- **P 節點（P-node）**：它利用點對點的方式（peer-to-peer，對等式）直接向 WINS 伺服器詢問。例如當電腦 PC1 欲與電腦 PC2 溝通時，它會直接向 WINS 伺服器詢問 PC2 的 IP 位址。
- **M 節點（M-node）**：這是 B 節點與 P 節點的混合方式（mixed，混合式），它會先利用廣播方式，若失敗，再改向 WINS 伺服器查詢。例如當電腦 PC1 欲與 PC2 溝通時，PC1 會先利用廣播方式來找尋 PC2 的 IP 位址，若 PC2 沒有回應（例如它是位於另外一個網路內），則改向 WINS 伺服器詢問。
- **H 節點（H-node）**：這也是 P 節點與 B 節點的交互方式（hybrid，交互式），不過它是先向 WINS 伺服器查詢，若失敗，再改用廣播方式。

Windows 系統的 B 節點類型具備額外擴充能力：當廣播方式失敗時，它還會嘗試檢查 LMHOSTS 檔內是否有對方電腦的 IP 位址。由於 LMHOSTS 檔可記載其他網路內的電腦的 IP 位址，因此可解決廣播無法跨越路由器的問題。

Windows Server 2012、Windows Server 2008（R2）、Windows 8、Windows 7、Windows Vista 等預設是採用 H 節點（交互式），您可以利用 **ipconfig /all** 來查看，如圖 A-1-5 所示的節點類型為 H 節點（交互式），此畫面為在一台 Windows Server 2008 上執行的結果（Windows Server 2012、Windows Server 2008 R2、Windows 8 與 Windows 7 都誤將其翻譯成**混合式**，也就是 hybrid 與 mixed 都翻譯成**混合式**）。Windows Server 2003、Windows XP 等預設是採用 B 節點（廣播式），但若它們是 WINS 用戶端的話，則自動改為採用 H 節點。

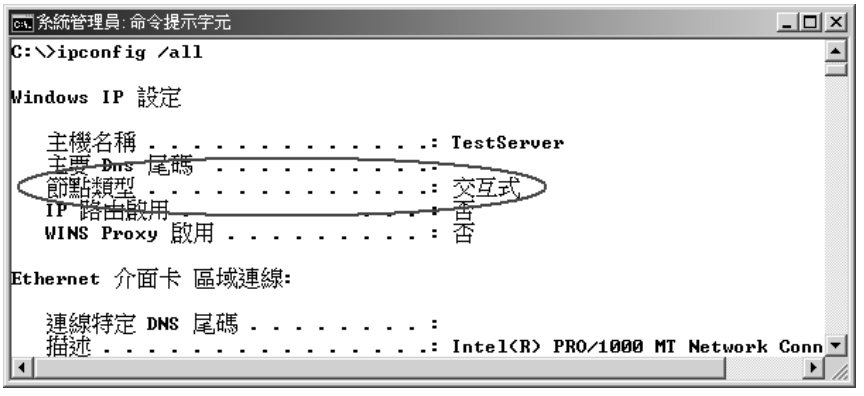

圖 A-1-5

附註

WINS 用戶端可以透過修改 NodeType 登錄值來變更節點類型，NodeType 位於以下登錄路徑：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

NodeType 值為 1 表示 B 節點，2 表示 P 節點，4 表示 M 節點，8 表示 H 節點。若沒有此數值名稱的話，請自行新增之，其資料型態為 DWORD。

採用 H 節點類型的 WINS 用戶端，其 NetBIOS 名稱解析的完整順序為：

1. 檢查所欲查詢的電腦名稱是否就是自己的電腦名稱
2. 檢查 NetBIOS 名稱快取區
3. 向 WINS 伺服器查詢
4. 送出廣播訊息
5. 檢查 LMHOSTS 檔
6. 檢查 HOSTS 檔或向 DNS 伺服器查詢

其中最後一種方法是 DNS 主機名稱解析的方法，相關說明請見第 3 章。若欲解析的名稱字元數目多於 15 個字，或名稱之中有句點（“.”）存在的話，它會自動改用 DNS 主機名稱的解析方法。

A-2 使用 LMHOSTS 檔案

若電腦是位於其他網路的話，則利用廣播方式來找尋該電腦的 IP 位址時會失敗，因為路由器不會將此廣播訊息傳遞到另一個網路，不過 Windows 系統在廣播失敗後，會直接檢查本機的 LMHOSTS 檔案內是否有對方電腦的 IP 位址。

LMHOSTS 檔的內容

您必須自行編輯 LMHOSTS 檔來將位於其他網路的電腦名稱與 IP 位址手動輸入到此檔案內。您可以用**記事本**（notepad）來建立此檔案，注意**記事本**會自動附加副

檔名.TXT，因此存檔時請在檔名前後利用 “” 括起來，也就是將檔名設定為 “LMHOSTS”，**記事本**就會以括號內的名稱來存檔，不會自動加上附檔名.TXT。請將此檔案儲存到 %*Systemroot*%\system32\drivers\etc 資料夾內，此資料夾內已經有一個名稱為 LMHOSTS.SAM 的範例檔（注意其附檔名預設被隱藏），您也可以直接修改這個檔案，不過在使用前需將檔名改為 LMHOSTS，我們利用圖 A-2-1 的範例來說明如何建立 LMHOSTS 檔。

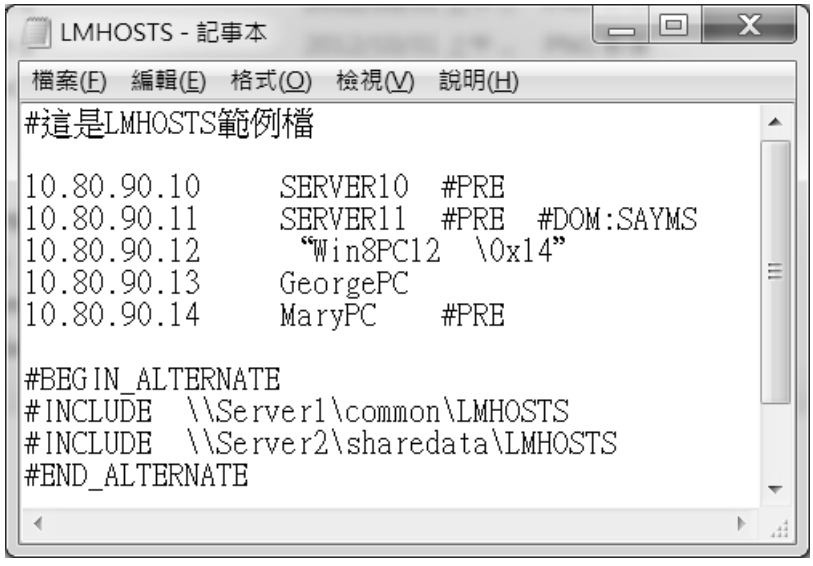

圖 A-2-1

- 每一筆資料都必須放在獨立的一行。
- IP 位址必須放在一行的第一欄（column），其後跟著相對應的電腦名稱。
- IP 位址與電腦名稱之間必須至少間隔一個空白或一個 TAB。
- 電腦名稱最多 15 個字元。
- 電腦名稱內若包含空白字元或特殊字元的話，必須用 “” 符號將整個電腦名稱括起來，例如 “Win8PC12 \0x14”，其中既有空白、又有特殊字元\0x14。
- # 符號以後的文字代表註解說明，但若 # 符號之後是跟著如表 A-2-1 所示關鍵字的話，則有特殊意義。注意這些關鍵字必須大寫，否則會被當作是註解文字。

表 A-2-1

關鍵字	說明
#PRE	此關鍵字是附加在一筆資料的後面，系統啓動時會將有#PRE 的資料預先載入（preload）到 NetBIOS 名稱快取區
#DOM:*網域名稱*	表示它是*網域名稱*所指網域的域控制站。此筆資料需要加#PRE
#INCLUDE:*檔案名稱*	將*檔案名稱*所指的另外一個 LMHOSTS 檔加入到此檔內
#BEGIN_ALTERNATE 與 #END_ALTERNATE	這兩個關鍵字之間可以有多個#INLCUDE，系統會讀取第 1 個 LMHOSTS 檔，若因故無法讀取時，它會讀取第 2 個 LMHOSTS 檔，依此類推，因此可說它具備容錯功能
\0xnn	電腦名稱內可以包含無法顯示（non-printable）的特殊字元，但是必須以 “” 符號將電腦名稱括起來
#MH	若一台電腦內有多片網路卡的話，則可以爲每一片網路卡建立一筆資料，其電腦名稱都相同，但 IP 位址爲各網路卡的 IP 位址，且請在每一筆資料最後加上#MH。MH 就是 Multihomed

- 系統透過 LMHOSTS 檔執行名稱解析動作時，是從檔案最前面開始檢查，包含註解行，故應儘量減少註解，同時將常用資料放到檔案前端，以提高查詢效率。
- 系統啟動時會將有#PRE 的資料預先載入到 NetBIOS 名稱快取區，且會一直存在快取區，除非#PRE 關鍵字被移除，且快取區被清除與重新執行預載動作。
- 由於系統啟動完成後，LMHOSTS 檔案內有#PRE 的資料不會再被存取，因此請儘量將有#PRE 的資料放到檔案最後，以提高查詢效率。
- 系統是廣播失敗後，才會使用 LMHOSTS 檔，而同一個網路區段內的電腦利用廣播即可得知其 IP 位址，不需要利用 LMHOSTS 檔，因此 LMHOSTS 檔案內應該只輸入其他網路內的電腦名稱與 IP 位址。注意您的電腦需指定預設閘道，否則這些有#PRE 的資料不會被預載到 NetBIOS 名稱快取區。

了解 LMHOSTS 的運作

LMHOSTS 檔最適合網路上沒有 WINS 伺服器的環境，因為此時只好使用廣播方式，但廣播方式無法與其他網路內的主機溝通，此時就可以利用 LMHOSTS 檔來

解決此問題。以下說明 LMHOSTS 檔如何與廣播方式相互運作（假設網路上沒有 WINS 伺服器）：

- 若 LMHOSTS 檔內有筆資料被設定為#PRE，則電腦啟動時，此筆資料就會預先被載入（preload）到 NetBIOS 名稱快取區。
- 當電腦要查詢其他電腦的 IP 位址時，它會先檢查 NetBIOS 名稱快取區內是否已存在此電腦的 IP 位址。
- 若 NetBIOS 名稱快取區內找不到對方 IP 位址的話，它將改用廣播方式。
- 若廣播方式也失敗的話，則改檢查 LMHOSTS 檔。
- 若 LMHOSTS 檔內仍然找不到對方 IP 位址的話，它會顯示警告訊息。
- 若在 LMHOSTS 檔找到對方 IP 位址的話，則此資料會被儲存到 NetBIOS 名稱快取區一段時間，以供下次使用。

您可以利用 **nbtstat -R** 指令將 NetBIOS 名稱快取區內的資料清除，它同時會重新載入 LMHOSTS 檔內的**#PRE** 記錄（您的電腦需指定預設閘道，否則不會載入），例如圖 A-2-2 中執行 **nbtstat –R** 指令後，可再透過 **nbtstat –c** 指令來查看 NetBIOS 快取區內的資料，圖中的資料都是 LMHOSTS 檔案內#PRE 的資料，其存留期為-1，表示永久有效。

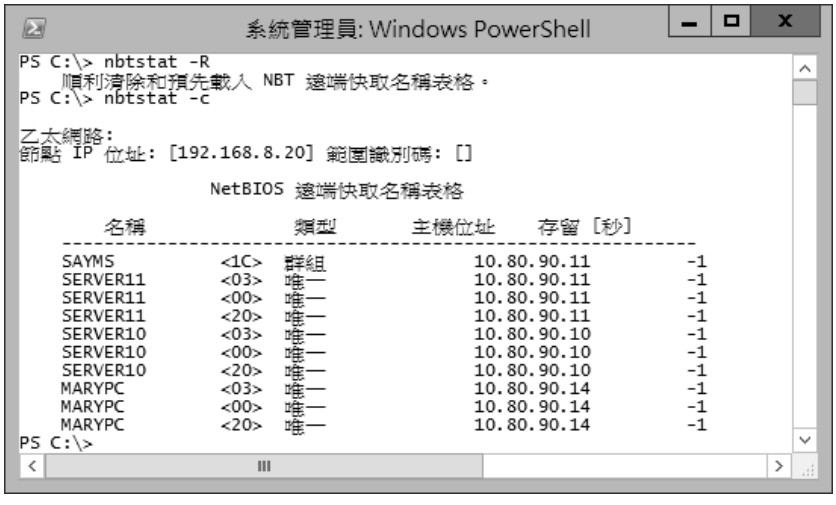

圖 A-2-2

集中管理 LMHOSTS 檔

利用 LMHOSTS 檔來解析名稱有一個缺點，哪就是每一台電腦都必須維護自己的 LMHOSTS 檔。當網路上的電腦資料有所變更時，每台電腦的 LMHOSTS 檔也都必須更改，才能確保對照表資料的一致性。

為了減少維護 LMHOSTS 檔的負擔，您可以選擇在一台電腦內建立一個共用的 LMHOSTS 檔，然後讓其他電腦利用#INCLUDE 指令來參照使用這個共用檔，如此就可以避免花費太多的時間去維護每一個 LMHOSTS 檔。例如共用的 LMHOSTS 檔是在電腦名稱為 SERVER1 的電腦內，同時假設此檔所在的資料夾被設為共用資料夾，其共用名稱為 common，則其他參照電腦的 LMHOSTS 檔內可使用以下指令來參照此共用 LMHOSTS 檔：

#INCLUDE \\SERVER1\common\LMHOSTS

注意若參照電腦無法利用廣播方式得知 SERVER1 的 IP 位址的話（若參照電腦與 SERVER1 分別位於不同網路），則需在參照電腦的 LMHOSTS 檔內設定 SERVER1 的 IP 位址與電腦名稱對照資料，且需附加＃PRE 關鍵字。例如 SERVER1 的 IP 位址為 10.80.90.1，則其他參照電腦的 LMHOSTS 檔內應該包含以下指令：

10.80.90.1 SERVER1 #PRE
#INCLUDE \\SERVER1\common\LMHOSTS

該行 IP 位址與電腦名稱的對照資料，必須在#INCLUDE 之前，否則#INCLUDE 指令無法找到 SERVER1 的 IP 位址。

附註

#INCLUDE 檔案內的每一筆資料必須加#PRE 關鍵字，以便將其預載到 NetBIOS 名稱快取區，否則該筆資料會被忽略。

啟用 LMHOSTS 檔

Windows 用戶端預設自動會透過 LMHOSTS 檔案來執行名稱解析工作。若要變更設定的話，以 Windows Server 2012 來說，可選用【按⊞鍵切換到**開始**選單➲控制台➲網路和網際網路➲網路和共用中心➲點擊**乙太網路**➲點擊內容鈕➲點擊**網際網**

路通訊協定第 4 版（TCP/IPv4）➲內容鈕**➲**進階鈕**➲WINS** 標籤**➲**如圖 A-2-3 中的**啟用 LMHOSTS 搜尋】**。

圖 A-2-3

也可以將內含 IP 位址與電腦名稱對照資料的純文字檔案（text file），透過圖 A-2-3 中的匯入 LMHOSTS（M）...鈕來將其拷貝到 %*Systemroot%*\system32\drivers\etc\LMHOSTS 檔，若此資料夾內已經有 LMHOSTS 檔存在的話，則這個現有的 LMHOSTS 檔會被改名為 LMHOSTS.BAK。

A-3 WINS 的運作原理

若要利用 WINS 來解析 NetBIOS 名稱的話，首先需要架設一台或多台 WINS 伺服器，並在用戶端指定使用 WINS 伺服器。WINS 用戶端與 WINS 伺服器之間的溝通分為以下四個動作：名稱登記（name registration）、更新登記的名稱（name renewal）、名稱查詢（name query）與名稱釋放（name release）。

Windows 用戶端最多可以指定 12 台 WINS 伺服器，其中第 1 台被稱為**主要 WINS 伺服器**（primary WINS server），其餘的被稱為**次要 WINS 伺服器**（secondary WINS server）。

WINS 用戶端會與**主要 WINS 伺服器**溝通，以便要求進行名稱登記、更新、查詢、釋放等與 NetBIOS 名稱服務有關的動作，只有在**主要 WINS 伺服器**沒有回應的情

況下（例如已經關機），才會將要求傳送給**次要 WINS 伺服器**。WINS 用戶端會依序嘗試將要求傳送給每一台**次要 WINS 伺服器**，一直到其中有一台**次要 WINS 伺服器**回應或所有的**次要 WINS 伺服器**都沒有回應為止。

名稱登記

WINS 用戶端在啟動時，會主動將它的 NetBIOS 電腦名稱、IP 位址等資料登記到 WINS 伺服器的資料庫內，以後 WINS 用戶端的 IP 位址有異動時，它也會主動將更新資料傳給 WINS 伺服器。當 WINS 伺服器收到登記要求後，它會檢查此名稱是否已經被登記了，並據以判斷是否接受 WINS 用戶端的登記要求。WINS 用戶端在送出登記要求後，它可能收到的回應有：

- **沒有回應（no response）**：在經過 3 次登記嘗試之後，若沒有收到**主要 WINS 伺服器**的回應，則 WINS 用戶端會向**次要 WINS 伺服器**們依序提出登記要求，一直到登記成功或所有 WINS 伺服器都已嘗試過為止。

  若**主要 WINS 伺服器**與**次要 WINS 伺服器**都沒有回應的話，WINS 用戶端將改用廣播方式來找尋 WINS 伺服器。

- **接受（positive）**：若此電腦名稱還沒有被登記，則 WINS 伺服器會接受 WINS 用戶端的登記要求，並回給用戶端 positive 的訊息。此回應訊息內包含著用戶端可擁有此名稱的期限（Time-to-Live，TTL），用戶端需在期限到前，更新（renew）所登記的名稱，才能夠繼續在 WINS 伺服器資料庫內保有此名稱。

- **不接受（negative）**：若此名稱已被其他 WINS 用戶端登記，則 WINS 伺服器會先與登記此名稱的用戶端電腦溝通，若 WINS 伺服器收到它的回應，則 WINS 伺服器就不接受新用戶端的登記要求，並送給新用戶端一個 negative 的訊息。若 WINS 伺服器沒有收到原登記者的回應，它就會接受新用戶端的登記。

更新登記的名稱

登記在 WINS 伺服器的每一筆電腦名稱與 IP 位址資料，都有一定的有效期限（TTL），在期限到達之前，擁有此名稱的 WINS 用戶端必須向 WINS 伺服器更新，否則期限到達時，此名稱就會被加上**刪除標記**，而且 WINS 伺服器也不會提供查詢此名稱的服務，一段時間後此名稱就會被刪除。

用戶端預設是在有效期限過一半時，會自動向 WINS 伺服器更新，只要更新成功，此名稱的有效期限就會延長。

名稱查詢

當 WINS 用戶端要與其他電腦溝通時，例如 Windows 8 用戶端利用【按⊞+ R 鍵➲\\Server1\Tools】來存取伺服器 Server1 的共用資料夾 Tools 時，它是如何解析電腦名稱 Server1 呢？也就是如何找到 Server1 的 IP 位址呢？這要視用戶端的**節點類型**（node-type）而定（見第 3-5 頁 **NetBIOS 節點類型**）。若此用戶端的節點類型為 **H 節點**（H-node，交互式），則其 NetBIOS 名稱解析的完整過程如下：

1. 檢查電腦名稱 Server1 是否就是自己的電腦名稱
2. 檢查 NetBIOS 名稱快取區
3. 依序向主要 WINS 伺服器、次要 WINS 伺服器查詢
4. 送出廣播訊息
5. 檢查 LMHOSTS 檔
6. 檢查 HOSTS 檔或向 DNS 伺服器查詢

名稱釋放

WINS 用戶端關機時會通知 WINS 伺服器釋放它所登記的所有名稱；若用戶端將特定服務停止時（例如工作站服務），它也會通知 WINS 伺服器釋放該服務所登記的名稱。一個已經被釋放的名稱會被加上**已釋放**的標記。

當一台用戶端在登記名稱時，雖然該名稱已經被另外一台電腦登記（電腦名稱相同，IP 位址不同），不過卻有**已釋放**標記的話，則 WINS 伺服器會允許此用戶端登記。舉例來說，DHCP 用戶端在關機時會釋放所有登記的名稱，在下一次開機時，即使它所租用到的 IP 位址與之前的不相同，它還是可以正常登記，因為之前所登記的電腦名稱（不同的 IP 位址）已經被釋放了。

一個**已釋放**的名稱，經過一段時間後若沒有再被登記的話，它就會被從 WINS 伺服器的資料庫中刪除。

A-4 WINS 的設定與測試

在 Windows Server 2012 電腦上安裝 WINS 伺服器時，建議此電腦的 IP 位址最好是靜態的，也就是自行手動輸入 IP 位址，不要透過 DHCP 租用動態 IP 位址，因為每一次向 DHCP 伺服器租到的 IP 位址可能會不相同，這將造成 WINS 用戶端在指定 WINS 伺服器 IP 位址上的困擾。我們將透過圖 A-4-1 來說明如何設定 WINS 伺服器與 WINS 用戶端。

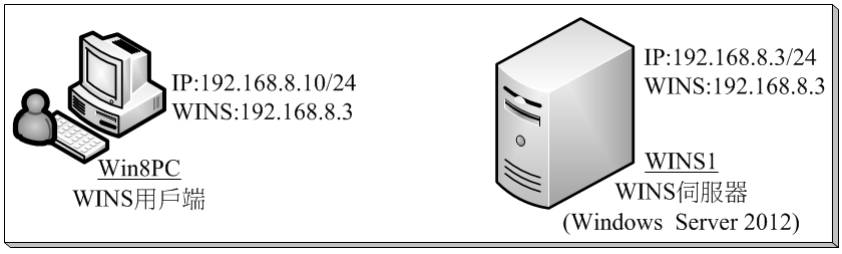

圖 A-4-1

注意

WINS 與 NetBIOS 皆不支援 Internet Protocol Version 6（IPv6）。

WINS 伺服器的安裝

將 **WINS 伺服器**安裝到 Windows Server 2012 電腦的途徑：【開啟**伺服器管理員**➲點擊**儀表版**處的**新增角色及功能**➲一直按下一步鈕到出現如圖 A-4-2 的**選取功能**畫面時勾選 **WINS 伺服器**➲…】。

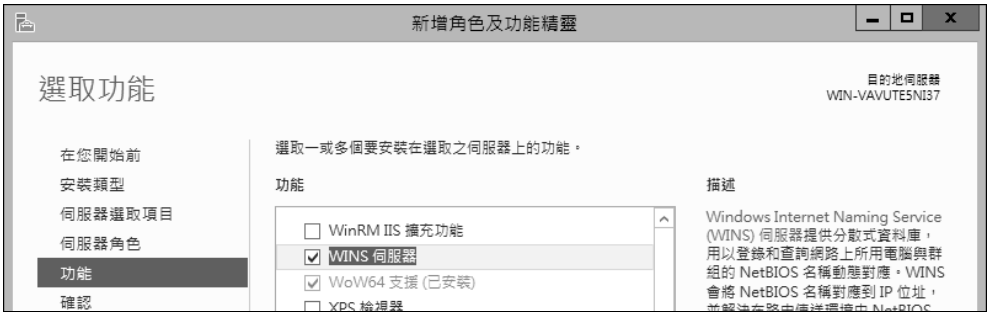

圖 A-4-2

注意

在 Windows Server 2012 內透過**伺服器管理員**安裝的角色或功能，系統都會自動在 **Windows 防火牆**例外開放與該角色或功能有關的連接埠，故安裝 WINS 伺服器時，它會自動開放所需的連接埠。

完成安裝後，可以透過【在**伺服器管理員**中點擊右上方的**工具**➲WINS】或【按 Windows 鍵⊞切換到**開始**選單➲點擊 **WINS**】的途徑來開啟 WINS 主控台、管理 WINS 伺服器；可以【在 WINS 主控台中對著 **WINS** 按右鍵➲新增伺服器】來管理其他 WINS 伺服器；可以【在 WINS 主控台中對著 WINS 伺服器按右鍵➲所有工作】來執行啟動、停止、暫停與繼續 WINS 伺服器等工作。

WINS 用戶端的設定

以 Windows 8 用戶端電腦來說：【按⊞鍵切換到**開始**選單➲控制台➲網路和網際網路➲網路和共用中心➲點擊**乙太網路**➲內容鈕➲點擊**網際網路通訊協定第 4 版（TCP/IPv4）**➲內容鈕➲進階鈕➲點擊圖 A-4-3 中 **WINS** 標籤之下的新增鈕➲輸入 WINS 伺服器的 IP 位址 192.168.8.3➲按新增鈕】，最多可指定 12 台 WINS 伺服器。WINS 伺服器本身的 TCP/IP 處也應該指定其 WINS 伺服器（自己的 IP 位址 192.168.8.3），因此請到 WINS 伺服器電腦上做相同的設定。

圖 A-4-3

DHCP 用戶端的 WINS 設定

您可以透過DHCP伺服器的選項設定，來讓DHCP伺服器在將IP位址出租給DHCP用戶端時，順便將 WINS 伺服器的 IP 位址與節點類型指派給用戶端，如圖 A-4-4 所示（DHCP 選項設定請參閱章節 2-6）。

圖 A-4-4

檢視 WINS 伺服器資料庫

WINS資料庫內包含著WINS用戶端所登記的電腦名稱、IP位址等，而要檢視WINS資料庫的話：【按 Windows 鍵⊞切換到**開始**選單➲WINS➲如圖 A-4-5 所示對著**使用中的登錄**按右鍵➲顯示記錄➲按立即尋找鈕】，之後便會如圖 A-4-6 所示顯示所有記錄。

您也可以在圖 A-4-5 中篩選欲顯示的記錄，例如透過 NetBIOS 名稱來篩選、透過 IP 位址來篩選、透過子網路來篩選。如果是透過 NetBIOS 名稱來篩選的話，可以只輸入前幾個字元即可，例如若輸入 SER，則它會顯示 NetBIOS 名稱前 3 個字是 SER 的所有記錄。

圖 A-4-5

圖 A-4-6

若 WINS 用戶端因故沒有登記成功，以致於在圖 A-4-6 中看不到該用戶端記錄的話：到該用戶端電腦上利用 **nbtstat –RR** 指令來手動重新登記（需以系統管理員身分來執行此程式；或將網路卡停用、再重新啟用）、然後【在圖 A-4-6 中對著**使用中的登錄**按右鍵➲重新整理】。

圖 A-4-6 中**類型**欄位處的數字代表服務，例如[00]代表工作站服務，[20]代表伺服器服務（也就是**檔案伺服器**服務），由此可以驗證用戶端不是只單純的登記電腦名稱與 IP 位址而已，還登記了部份其所支援的服務。

在圖 A-4-5 中還可以透過以下兩個標籤來篩選欲顯示的記錄：

- **記錄擁有者**：根據記錄的擁有者來顯示記錄。何謂擁有者？WINS 用戶端直接向 WINS 伺服器登記的記錄，其擁有者就是這台 WINS 伺服器。在 WINS 伺服器資料庫內有些記錄是從其他 WINS 伺服器複寫過來的，這些記錄的擁有者是別台 WINS 伺服器。
- **記錄類型**：例如您可以選擇只顯示代表工作站服務的記錄。

當一台 WINS 用戶端電腦啟動時，它會將所擁有的名稱登記到 WINS 伺服器內，這些名稱在 WINS 伺服器中的狀態就是**使用中**（active），而當此用戶端的服務（例如工作站服務）被停止時，與其相關的名稱就會被釋放掉，也就是這些名稱的狀態會變為**已釋放**（released，參考圖 A-4-7 中的**狀態**欄位）。

圖 A-4-7

刪除 WINS 伺服器內的記錄

有時候您可能需要手動將 WINS 資料庫內的某筆記錄刪除，例如某台用戶端電腦故障了，但其所登記的記錄仍然留在 WINS 資料庫內，而您想要立刻將該筆記錄刪除：【對著該筆記錄按右鍵➲刪除】，之後將出現圖 A-4-8 的畫面。

- **只刪除這台伺服器上的記錄**：這筆記錄之前可能已經被複寫到其他 WINS 伺服器（複寫協力電腦，後述），但選擇此選項只會將本台 WINS 伺服器內的記錄刪除，在其他 WINS 伺服器內的相同記錄並不會被刪除。

  若您發現這筆記錄只有在這台 WINS 伺服器內有問題，在其他 WINS 伺服器內都正常的話，就可以選擇此選項。

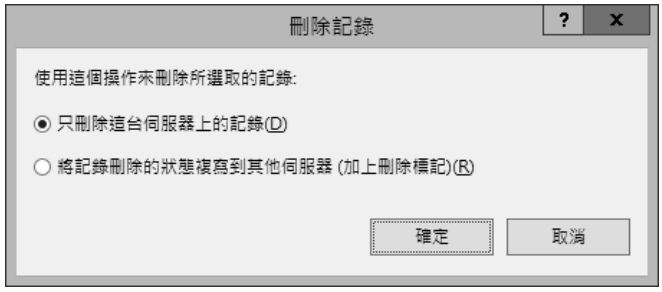

圖 A-4-8

- **將記錄刪除的狀態複寫到其他伺服器（加上刪除標記）**：被加上**刪除標記**（tombstoned）後，這筆資料還是會被留在資料庫內，並不會立刻被刪除，此刪除標記會被複寫到其他 WINS 伺服器（複寫協力電腦），如圖 A-4-9 所示為一筆被加上刪除標記的記錄。經過一段時間後，WINS 伺服器內被加上刪除標記的記錄就會被刪除（後述）。

圖 A-4-9

DNS 伺服器與 WINS 伺服器的整合

雖然 DNS 用戶端也可以啟用 NetBIOS，然後透過 WINS 伺服器來解析 NetBIOS 名稱，進而與 WINS 用戶端溝通，然而透過 DNS 與 WINS 的整合，可以讓 DNS 用戶端只需要利用 DNS 名稱解析單一方式，就可以解析到其他電腦的 IP 位址，不論其他電腦是 DNS 或 WINS 用戶端。

DNS 與 WINS 整合後，DNS 用戶端透過 DNS 伺服器來查詢 IP 位址的運作流程如下（以圖 A-4-10 為例）：

1. DNS 用戶端向 DNS 伺服器 DNS1 查詢 win8pc30.sayms.local 的 IP 位址。

2. 管轄 sayms.local 區域的 DNS1 內並沒有 win8pc30.sayms.local 的 IP 位址，因此它會向與其整合的 WINS 伺服器來查詢，不過它只擷取 win8pc30.sayms.local 字串中的 win8pc30，然後向 WINS 伺服器查詢 NetBIOS 電腦名稱為 WIN8PC30 的 IP 位址。
3. WINS 伺服器將 WIN8PC30 的 IP 位址傳給 DNS 伺服器。
4. DNS 伺服器將此 IP 位址傳給 DNS 用戶端。

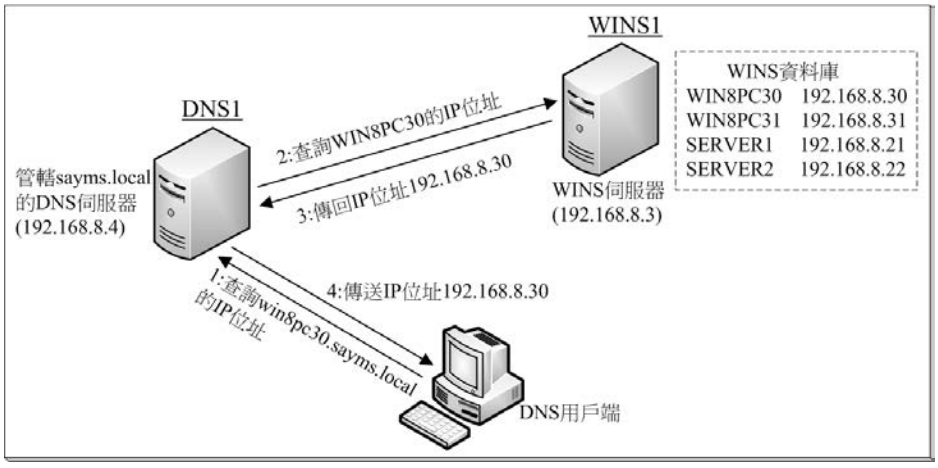

圖 A-4-10

將 DNS 區域與 WINS 伺服器整合的方法為：【對著 DNS 區域（假設是 sayms.local）按右鍵➲點擊圖 A-4-11 中的 **WINS** 標籤➲勾選**使用 WINS 正向對應**➲輸入 WINS 伺服器的 IP 位址➲按新增鈕】。圖中是將 DNS 區域 sayms.local 與 WINS 伺服器 192.168.8.3 整合。

圖 A-4-11

整合完成後，在 DNS 區域內會新增一筆類型為 **WINS 對應**的記錄，如圖 A-4-12 所示（若是反向對應區域的話，其記錄為 **WIN-R 對應**）。如果此區域的次要伺服器是其他廠牌 DNS 伺服器的話，由於它們並不支援 **WINS 對應**資源記錄，因此不可以將此記錄透過區域轉送傳送給這些次要伺服器，此時您需要透過勾選前面圖 A-4-11 中的**不要複寫這筆記錄**來達到這個目的。

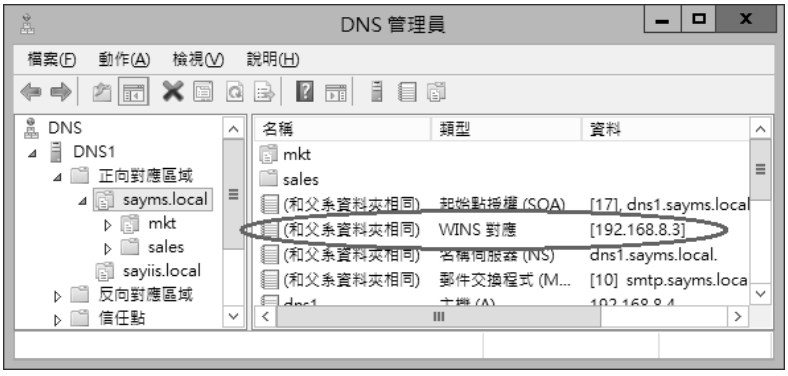

圖 A-4-12

A-5 對「非 WINS 用戶端」的支援

WINS 用戶端會向 WINS 伺服器登記，因此 WINS 用戶端之間可以透過 WINS 伺服器來得知對方的 IP 位址，進而互相的溝通。但若網路上有未啟用 WINS 功能的用戶端的話，它們並不會與 WINS 伺服器溝通，也就是既不會將其電腦名稱與 IP 位址登記到 WINS 資料庫內，也不會向 WINS 伺服器查詢其他電腦的 IP 位址，此時要如何讓 WINS 用戶端與這些「**非 WINS 用戶端**」溝通呢？

若「**非 WINS 用戶端**」與 WINS 用戶端是在同一個網路內的話，則它們可以利用廣播方式來找尋對方的 IP 位址，進而相互溝通。但若它們是分別位於不同網路的話，則廣播方式就無法發揮作用了，因為路由器不會將廣播訊息傳送到另一個網路。此時您可以利用以下兩種方法來解決這個問題：

- **利用靜態對應**：可以讓 WINS 用戶端得知「**非 WINS 用戶端**」的 IP 位址。
- **利用 WINS Proxy**：可以讓「**非 WINS 用戶端**」得知 WINS 用戶端的 IP 位址。

附註

也可以利用 LMHOSTS 檔案來解決這個問題。

靜態對應

您可以將「**非 WINS 用戶端**」的電腦名稱與 IP 位址手動輸入到 WINS 資料庫內，這就是**靜態對應**記錄，它可供 WINS 用戶端來查詢。建立靜態對應記錄的步驟為：【如圖 A-5-1 所示對著**使用中的登錄**按右鍵➲新增靜態對應➲輸入「**非 WINS 用戶端**」的電腦名稱、在**類型**處選擇**唯一**、輸入其 IP 位址➲按確定鈕】。

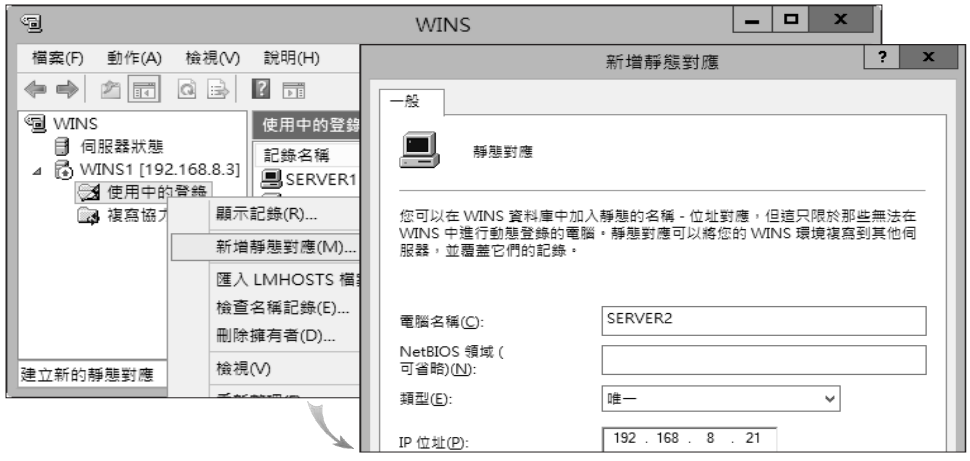

圖 A-5-1

附註

NetBIOS 領域保留空白即可。若「**非 WINS 用戶端**」有多片網路卡的話，可在**類型**處選擇**多重主目錄**（multihomed）、在 **IP 位址**處輸入每一片網路卡的 IP 位址。

它會建立 3 筆靜態記錄，如圖 A-5-2 中**靜態**欄位有 **x** 符號的 3 筆記錄，它們分別隸屬於**工作站**、**信差**與**檔案伺服器**服務，這些記錄的有效期限為**無限**。

圖 A-5-2

附註

從 Windows Vista 開始的 Windows 系統已經不支援**信差服務**（Messenger service）；**檔案伺服器**服務就是**伺服器**服務。

WINS Proxy 的設定

在 Windows 系統中只有 **WINS 用戶端**可以直接與 WINS 伺服器溝通、透過 WINS 伺服器來解析電腦名稱的 IP 位址。**「非 WINS 用戶端」**雖然可透過廣播方式取得其他用戶端的 IP 位址，但是廣播訊息無法被傳遞到其他網路，因此**「非 WINS 用戶端」**就可能無法與其他網路內的 **WINS 用戶端**溝通，此時 **WINS Proxy**（WINS 代理站）就派上用場了，如圖 A-5-3 所示。

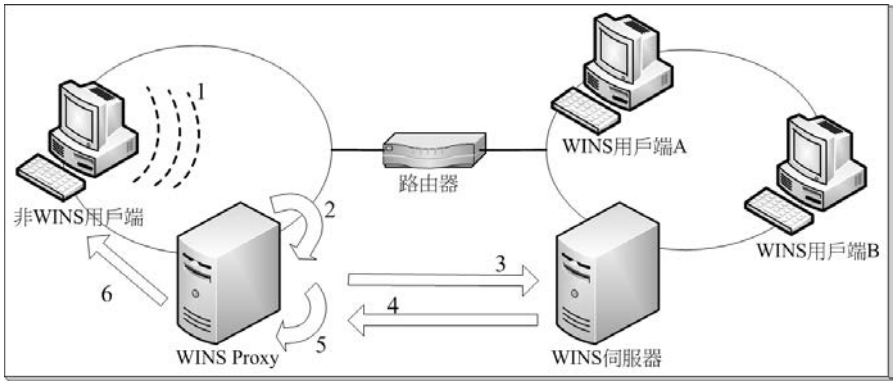

圖 A-5-3

圖左邊的**「非 WINS 用戶端」**利用廣播方式來查詢右邊 WINS 用戶端 A 的 IP 位址的流程如下所示（參照圖中的數字）：

1.「**非 WINS 用戶端**」送出查詢的廣播訊息。
2. WINS Proxy 收到此廣播訊息後，它會先檢查其快取區（cache）是否有 WINS 用戶端 A 的 IP 位址。
3. 若快取區沒有 WINS 用戶端 A 的 IP 位址的話，它會直接向圖右邊的 WINS 伺服器詢問。
4. WINS 伺服器將 WINS 用戶端 A 的 IP 位址傳送給 WINS Proxy。
5. WIN Proxy 將 WINS 用戶端 A 的電腦名稱與 IP 位址儲存到其快取區。

   當下一次有「**非 WINS 用戶端**」來向 WINS Proxy 詢問 WINS 用戶端 A 的 IP 位址時，它就會直接讀取快取區的資料，以提高查詢的速度。這份在快取區的資料，預設會被保留 10 分鐘。
6. WIN Proxy 將此 IP 位址傳送給「**非 WINS 用戶端**」。

WINS Proxy 類似於第 2 章所介紹的 **DHCP 轉送代理**，它們都是在負責解決廣播訊息無法跨越路由器的問題。WINS Proxy 本身必須是 WINS 用戶端，而將其設定為 WINS Proxy 的方法為：到該 WINS 用戶端上執行 **regedit.exe**、將位於以下路徑的數值 **EnableProxy** 設定為 1、然後重新啟動該電腦。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

若上述路徑內看不到 **EnableProxy** 數值名稱的話，請自行新增之，其資料型態為 DWORD。您可以在 WINS Proxy 電腦上透過 **ipconfig /all** 指令來查看是否已經啟用了 WINS Proxy 功能，如圖 A-5-4 所示。

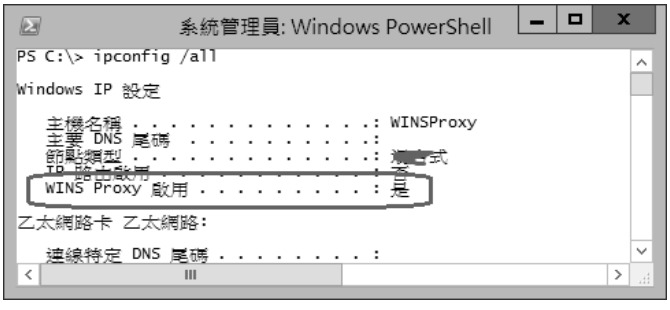

圖 A-5-4

注意

若扮演 WINS proxy 角色的電腦是 Windows Server 2012、Windows Server 2008（R2）、Windows 8、Windows 7 或 Windows Vista 的話，則您必須自行將其 **Windows 防火牆**關閉或例外開放 UDP 連接埠編號 137。

A-6 WINS 資料庫的複寫

圖 A-6-1 中有兩個網路，甲網路內所有 WINS 用戶端的 NetBIOS 名稱都是登記到 WINS 伺服器 WINS1 內，它們相互之間可以透過 WINS1 來得到對方的 IP 位址。乙網路內所有 WINS 用戶端的 NetBIOS 名稱都是登記到 WINS 伺服器 WINS2 內，它們相互之間可以透過 WINS2 來得到對方的 IP 位址。

但是甲網路內的 WINS 用戶端 Win8PC1 要如何透過 WINS1 來找到乙網路內的 WINS 用戶端 Win8PC2 的 IP 位址呢？WINS1 的資料庫內並沒有 Win8PC2 的電腦名稱與 IP 位址資料！

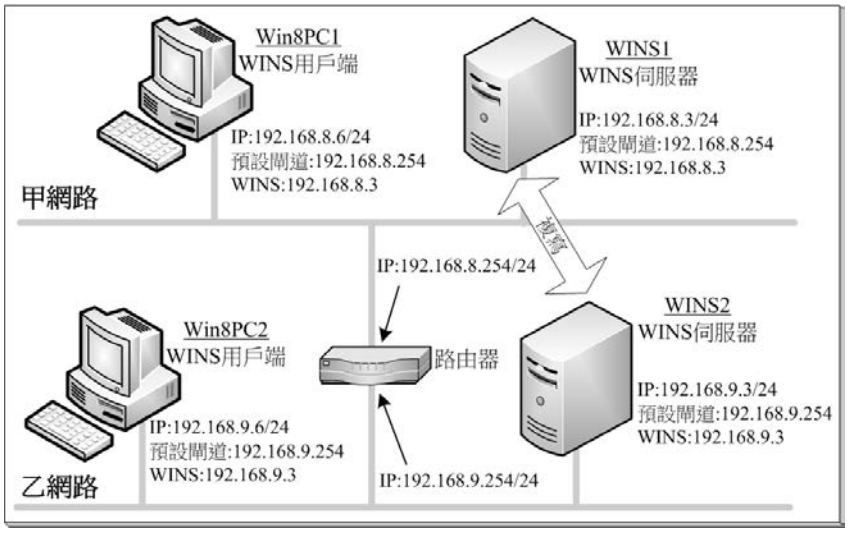

圖 A-6-1

為了解決此問題，您可以讓 WINS1 與 WINS2 之間互相複寫（複製）資料庫，如此甲網路內的 WINS 用戶端就可以透過 WINS1 來得知乙網路內的 WINS 用戶端的 IP 位址，反之亦然。

複寫協力電腦

我們需先設定 WINS 伺服器之間的關係，它們之間才可以相互複寫資料庫，也就是設定 WINS 伺服器的**複寫協力電腦**（replication partner），它分為以下兩種：

- **推入協力電腦（push partner）**：若 WINS1 是 WINS2 的**推入協力電腦**，則 WINS1 會將其資料庫複寫給 WINS2。**推入協力電腦**在以下幾種情況下，會主動將資料庫複寫給其**提取協力電腦**：
  - WINS 伺服器啟動時
  - 資料異動筆數已經達到指定數量時
  - WINS 伺服器資料庫內有一或多筆資料中的 IP 位址有異動時
  - 系統管理員以手動方式執行立即複寫的動作
- **提取協力電腦（pull partner）**：若 WINS2 是 WINS1 的**提取協力電腦**，則 WINS2 會接收由 WINS1 傳送過來的資料。**提取協力電腦**在以下的幾種情況下，會主動向其**推入協力電腦**索取資料：
  - WINS 伺服器啟動時
  - 指定的間隔時間到達時
  - 系統管理員以手動方式執行立即複寫的動作

當您將 WINS1 設定為 WINS2 的**推入協力電腦**時，必須也將 WINS2 設定為 WINS1 的**提取協力電腦**，否則 WINS2 會拒絕接收由 WINS1 傳送來的資料。同理當您將 WINS1 設定為 WINS2 的**提取協力電腦**時，必須也將 WINS2 設定為 WINS1 的**推入協力電腦**，否則 WINS2 會拒絕 WINS1 索取資料的要求。

故若要讓 WINS1 與 WINS2 之間能夠相互複寫資料的話，需將 WINS1 設定為 WINS2 的**推入協力電腦**與**提取協力電腦**，同時也需將 WINS2 設定為 WINS1 的**提取協力電腦**與**推入協力電腦**。

設定「複寫協力電腦」

以下步驟假設要將前面圖 A-6-1 中 WINS2 設定為 WINS1 的**複寫協力電腦**：請到伺服器 WINS1 上：【如圖 A-6-2 所示對著**複寫協力電腦**按右鍵➲新增複寫協力電腦➲輸入 WINS2 的 IP 位址➲按確定鈕】。

注意

由於 WINS2 是位於另一個網路區段內，因此 WINS1 目前無法解析 WINS2 電腦名稱的 IP 位址，故此時暫時只能夠輸入 WINS2 的 IP 位址，不過如果您在 WINS1 的 LMHOSTS 檔案內建立 WINS2 的電腦名稱與 IP 位址對照記錄的話，此處就可以輸入 WINS2 的電腦名稱。

圖 A-6-2

圖 A-6-3 為完成後的畫面。由圖中**類型**欄位可看出系統預設會將 WINS2 這台**複寫協力電腦**同時設定為**推入協力電腦**與**提取協力電腦**。

圖 A-6-3

相對的，請重複以上步驟將 WINS1 設定為 WINS2 的**複寫協力電腦**：您可以到 WINS2 電腦上來執行這些步驟，或直接在 WINS1 上【對著 WINS 按右鍵➲新增伺

服器➲輸入 WINS2 的 IP 位址】的途徑，來將 WINS2 新增到 WINS 主控台後直接執行以上步驟。

自動複寫的設定

若欲設定讓 WINS1 在指定時間到達時自動將資料複寫給 WINS2，或自動向 WINS2 索取資料的話：【點選圖 A-6-4 中 WINS1 下方**複寫協力電腦**➲點擊右方 WINS2➲點擊上方**內容**圖示➲**進階**標籤】：

圖 A-6-4

- **複寫協力電腦類型**：建議使用預設值，也就是同時設定為**推入/提取協力電腦**。若將其變更為**推入**的話，表示 WINS1 是 WINS2 的推入協力電腦；若將其變更為**提取**的話，表示 WINS1 是 WINS2 的提取協力電腦。
- **提取複寫**
  - **使用固定連線進行複寫**：兩台 WINS 伺服器建立連線、開始複寫完成後，將此連線保留不要中斷，以供下一次複寫時能夠利用此連線立即執行複寫動作，它可以節省重新建立連線的時間。
  - **開始時間**：每天開始進行複寫的起始時間。
  - **複寫間隔**：每隔多少時間複寫一次。

- **推入複寫**
  - **使用固定連線進行複寫**：說明同上
  - **在進行複寫之前版本識別碼的變更次數**：WINS 伺服器內每一筆資料都有一個版本識別碼，只要此資料有異動，其識別碼就會跟著增加。此處的意思為：WINS 伺服器內的資料變更多少筆後，才開始進行複寫動作。

附註

上述設定是針對 WINS1 的複寫協力電腦 WINS2 來設定，您也可以設定 WINS1 的複寫預設值，之後所有新增的複寫協力電腦的複寫設定會採用此預設值。WINS1 預設值的設定：【選取 WINS1➲對著**複寫協力電腦**按右鍵➲內容➲選取**推入複寫**或**提取複寫**標籤】。

手動立刻複寫

您也可以手動要求 WINS1 立刻將資料複寫給其複寫協力電腦 WINS2、或是向 WINS2 索取資料：【如圖 A-6-5 所示對著複寫協力電腦 WINS2 按右鍵➲**開始推入複寫**或**開始提取複寫**】。

圖 A-6-5

您也可以如圖 A-6-6 所示選用【對著**複寫協力電腦**按右鍵➲立即複寫】來讓 WINS1 與所有協力電腦（包含推入協力電腦與提取協力電腦）進行複寫。

圖 A-6-6

圖 A-6-7 為 WINS1（IP 位址為 192.168.8.3）與 WINS2（IP 位址為 192.168.9.3）相互複寫後，在 WINS1 資料庫內的資料，圖中**擁有者**欄位為 192.168.9.3 的資料是從 WINS2 複寫過來的。

圖 A-6-7

A-7 變更 WINS 伺服器的設定

您可以透過【對著 WINS 伺服器按右鍵➲內容】的途徑，來變更 WINS 伺服器的設定，如圖 A-7-1 所示。

圖 A-7-1

一般設定

圖 A-7-1 中的**一般**標籤內提供了以下的設定：

- **自動更新統計資料，每隔**：它會根據此處的設定來每隔一段時間自動重新統計 WINS 伺服器運作的資訊，而您可以利用【對著 WINS 伺服器按右鍵➲顯示伺服器統計資料】的途徑來檢視統計資料。
- **預設備份路徑**：設定用來備份 WINS 資料庫的資料夾。假設所設定的資料夾為 C:\WINSBackup（請事先自行建立此資料夾），則系統會每隔 24 小時自動將資料庫備份到 C:\WINSBackup\wins_bak\New 子資料夾內。
- **在伺服器關機時備份資料庫**：選擇在 WINS 服務停止時（例如電腦關機、或是【對著 WINS 伺服器按右鍵➲所有工作➲停止】），是否要自動將資料庫備份到預設備份路徑。

間隔時間設定

您可以在圖 A-7-2 的**間隔**標籤畫面中來設定以下的間隔時間：

圖 A-7-2

- **更新間隔**：WINS 用戶端必須在此間隔時間到達前，向 WINS 伺服器更新其所登記的名稱。用戶端會在此段時間過一半時自動向 WINS 伺服器更新。**更新間隔**時間太短的話，會增加 WINS 伺服器與網路的負荷。

  若用戶端在間隔時間到達時未向 WINS 伺服器更新，則此名稱會被設定為**已釋放**（released）。還有只要用戶端以正常方式關機的話，它也會自動通知 WINS 伺服器將其所登記的名稱設定為**已釋放**。若用戶端電腦不正常關機的話（例如電源中斷），此時雖然不會自動通知 WINS 伺服器，但 WINS 伺服器仍然會在**更新間隔**時間過後，自動將用戶端所登記的名稱設定為**已釋放**。

- **廢止間隔**：一個被設定為**已釋放**的名稱，在經過此**廢止間隔**時間後，會被加上**刪除標記**（tombstoned）（或稱為**已廢止**（Extinct））。

- **廢止逾時**：一個被加上**刪除標記**的名稱，在經過這段**廢止逾時**時間後，將被從 WINS 資料庫中清除（scavenge）。這段**廢止逾時**時間是為了確保這個**刪除標記**的狀態，能夠在這段時間內被複寫到其他**複寫協力電腦**。

- **確認間隔**：經過此間隔時間後，WINS 伺服器會驗證那些由其他 WINS 伺服器複寫過來的記錄是否仍然處於**使用中**（active）的狀態。

檢查資料庫

在圖 A-7-3 中的**資料庫檢查**標籤內提供了以下的設定：

- **檢查資料庫一致性，每隔...小時**：檢查 WINS 資料庫內的記錄是否與其他 WINS 伺服器的資料庫一致。它是用來檢查那些由其他 WINS 伺服器複寫過來的記錄。若本機伺服器內的記錄比較舊，就將最新記錄從其他伺服器複寫過來。由於此檢查動作會影響伺服器的運作效率，因此預設是不檢查。
- **開始檢查時間**：用來設定檢查一致性的起始時間。
- **每個間隔中所檢查的記錄最大數目**：每次檢查時，最多檢查幾筆記錄。
- **檢查對象**：
  - **擁有者伺服器**：直接透過記錄的擁有者（WINS 伺服器）來檢查。
  - **隨機選擇協力電腦**：隨機選擇協力電腦（WINS 伺服器），並透過此協力電腦來檢查。

圖 A-7-3

進階設定

在圖 A-7-4 中的**進階**標籤內提供了以下的設定：

- **將事件詳細資料記錄到 Windows 事件記錄檔中**：用來設定是否要將 WINS 資料庫的詳細異動情形記錄到**系統記錄檔**，而您可以利用**事件檢視器**來查看這些資料。若非必要，請不要啟用此功能，因為會影響到系統的運作效率。

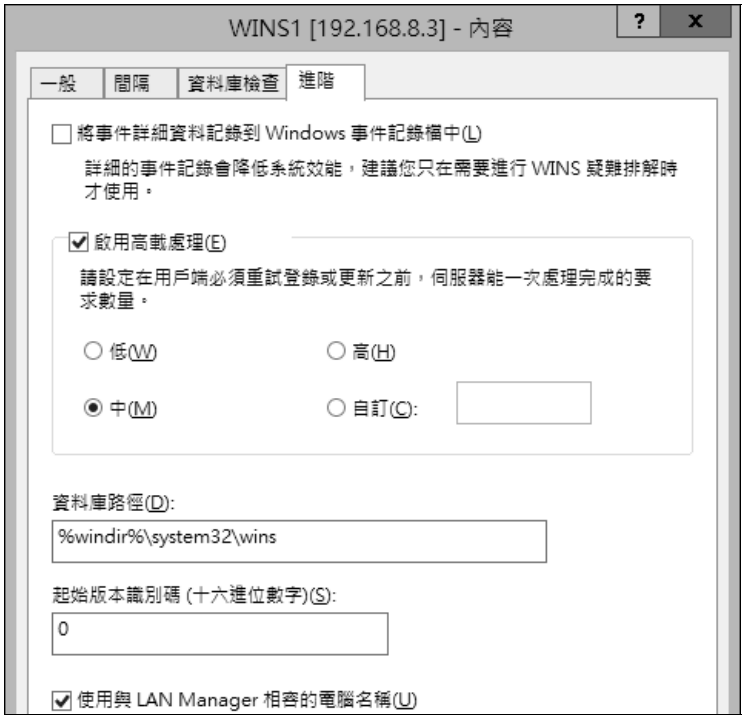

圖 A-7-4

- **啟用高載處理**：用來設定 WINS 伺服器以標準方式來處理用戶端的要求時，最多可以處理多少個用戶端要求。舉例來說，若公司突然停電，則在電恢復時，假設所有 WINS 用戶端電腦都同時啟動、同時向 WINS 伺服器登記，則可能會讓 WINS 伺服器的負擔大量增加，用戶端也可能會等很久，此時**高載處理**的功能就派用上場了。

  假設啟用了**高載處理**，也設定了最多處理 500 個用戶端要求，則 WINS 伺服器只會處理前面 500 個用戶端的登記要求，至於第 500 個以後的用戶端，WINS 伺服器僅是送一個已經登記成功的回應給它們（實際上並沒有登記成功），讓這些用戶端不需要再等待下去了，不過它們的更新間隔時間比較短、而且時間不定。第 500 個以後的用戶端收到此回應後，由於更新間隔時間較

短（以每 100 個使用者為單位：第 501-600 個用戶端為 5 分鐘，第 601-700 個用戶端為 10 分鐘，依此類推，一直到 50 分鐘為止，然後再從間隔 5 分鐘開始），因此短時間內它們就需要再來更新，此時 WINS 伺服器可能已經沒有這麼忙綠，有空來處理這些 WINS 用戶端的要求。圖中的**低**表示一次只處理前 300 個用戶端的要求、**中**表示 500 個、**高**表示 1000 個。

- **資料庫路徑**：設定 WINS 伺服器資料庫的儲存地點，預設為%*windir*%\system32\wins 資料夾，一般是 C:\Windows\system32\wins 資料夾。
- **起始版本識別碼**：資料庫內每一筆資料都有一個版本識別碼（見圖 A-7-5 的**版本**欄位）。設定**起始版本識別碼**後，之後所新增的第 1 筆資料的識別碼將依據此數值開始增加。版本識別碼是兩台 WINS 伺服器之間在複寫資料庫時，用來判別 WINS 伺服器是否擁有最新版記錄，以便做為是否需要複寫的依據。

圖 A-7-5

- **使用與 LAN Manager 相容的電腦名稱**：由於 Windows 系統是採用與 LAN Manager（MS-DOS 內提供網路功能的軟體）相同的電腦名稱命名方式，所以此處建議您不要修改。

A-8 WINS 伺服器的資料庫維護

WINS 資料庫檔案預設是儲存在 %*windir*%\System32\wins 資料夾內，如圖 A-8-1 所示。其中最主要的是資料庫檔案 wins.mdb，其他為輔助性檔案，請勿隨意變動或刪除這些檔案。

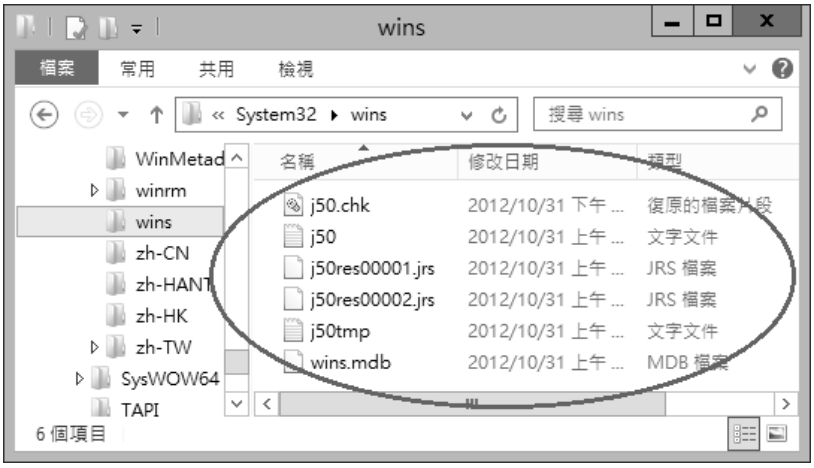

圖 A-8-1

清除資料庫

清除（scavenge）資料庫可以將已經廢棄的記錄由資料庫中刪除，或是清除由其他 WINS 伺服器複寫過來的廢棄記錄。系統會定期執行清除資料庫動作，但您也可以透過【對著 WINS 伺服器按右鍵➲清除資料庫】的途徑來手動清除，表 A-8-1 列出清除前後的結果。

表 A-8-1

清除前	清除後
此伺服器所擁有且仍使用中（active）的名稱，但是**更新間隔**的時間已過	被設定爲**已釋放**（released）
此伺服器所擁有且**已釋放**的名稱，但是**廢止間隔**的時間已過	被加上**刪除標記**（tombstoned）
此伺服器所擁有且已加上**刪除標記**的名稱，但是**廢止逾時**的時間已過	被從資料庫中刪除
由其他伺服器複寫而來，且已加上**刪除標記**的名稱，但是**廢止逾時**的時間已過	被從資料庫中刪除
由其他伺服器複寫而來，且仍然使用中的名稱，但是**確認間隔**的時間已過	被重新生效（revalidated）
由其他伺服器複寫過來的，且已加上**刪除標記**或已被刪除的名稱	被從資料庫中刪除

檢查資料庫的一致性與版本的一致性

除了在第 3-34 頁 **檢查資料庫** 內所介紹的自動檢查資料庫的一致性之外，您還可以利用【對著 WINS 伺服器按右鍵➲檢查資料庫一致性】來手動檢查。

您也可以【對著 WINS 伺服器按右鍵➲檢查版本號碼的一致性】來檢查版本號碼一致性。WINS 資料庫內的記錄會被複寫到其複寫協力電腦內，但是正常的狀況下，最新的記錄（版本號碼最高）應該是在擁有者的那一台 WINS 伺服器內。檢查版本號碼的一致性，可以用來確認在擁有者的那一台 WINS 伺服器內是否擁有最高版本號碼的記錄。

備份與還原 WINS 資料庫

當您在前面圖 A-7-1 中的**預設備份路徑**處指定了備份的資料夾後，WINS 伺服器會每隔 24 小時自動將資料庫備份到此資料夾內，而且您也可以透過勾選**在伺服器關機時備份資料庫**，讓 WINS 服務停止時自動備份資料庫。另外您還可以透過【對著 WINS 伺服器按右鍵➲備份資料庫】的途徑來手動備份。

當發現 WINS 伺服器資料庫有問題時，可以利用已備份的資料庫來將 WINS 資料庫還原。還原資料庫的步驟如下所示：

STEP 1 停止 WINS 服務：【在 WINS 主控台中對著該伺服器按右鍵➲所有工作➲停止】或執行 **net stop wins** 指令來將該服務停止。

STEP 2 將 WINS 資料庫所在的資料夾內的所有檔案都刪除（此資料夾是設定在圖 A-7-4 的**資料庫路徑**處，一般是%*windir*%\system32\wins）。

STEP 3 利用【對著該伺服器按右鍵➲還原資料庫】來將資料庫還原，還原時請提供備份資料庫的儲存地點。

STEP 4 重新啟動 WINS 服務：【在 WINS 主控台中對著該伺服器按右鍵➲所有工作➲啟動】或執行 **net start wins** 指令來啟動該服務。

B

Web Farm 與網路負載平衡

透過將多台 IIS 網頁伺服器組成 Web Farm 的方式，可以提供一個具備容錯與負載平衡的高可用性網站。本章將詳細分析 Web Farm 與 Windows 網路負載平衡（Windows Network Load Balancing，簡稱 Windows NLB 或 WNLB）。

B-1 Web Farm 與網路負載平衡概觀

將企業內部多台 IIS 網頁伺服器組成 Web Farm 後，這些伺服器將同時對使用者來提供一個不中斷的、可靠的網站服務。當 Web Farm 接收到不同使用者的連接網站要求時，這些要求會被分散的送給 Web Farm 中不同網頁伺服器來處理，因此可以提高網頁存取效率。若 Web Farm 之中有網頁伺服器因故無法對使用者提供服務的話，此時會由其他仍然正常運作的伺服器來繼續對使用者提供服務，因此 Web Farm 具備容錯功能。

Web Farm 的架構

圖 B-1-1 為一般 Web Farm 架構的範例，圖中為了避免單一點故障而影響到 Web Farm 的正常運作，因此每一個關卡，例如防火牆、負載平衡器、IIS 網頁伺服器與資料庫伺服器等都不只一台，以便提供容錯、負載平衡功能：

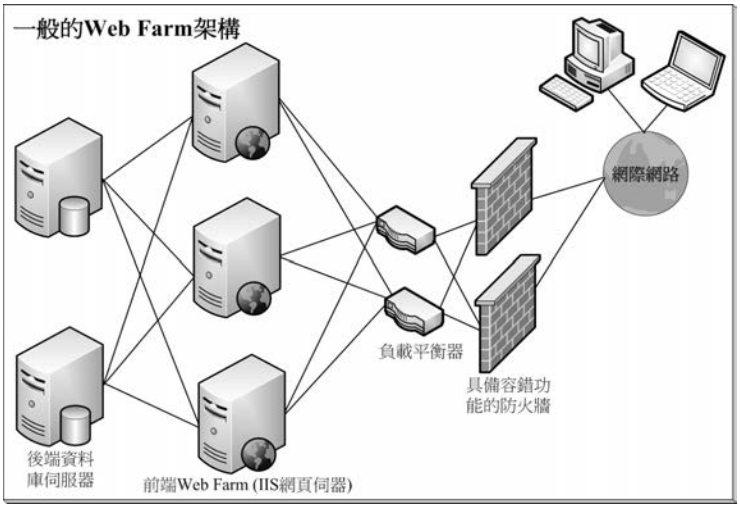

圖 B-1-1

- **防火牆**：可確保內部電腦與伺服器的安全。
- **負載平衡器**：可將連接網站的要求分散到 Web Farm 中不同的網頁伺服器。
- **前端 Web Farm（IIS 網頁伺服器）**：將多台 IIS 網頁伺服器組成 Web Farm 來對使用者提供網頁存取服務。
- **後端資料庫伺服器**：用來儲存網站的設定、網頁或其他資料。

Windows Server 2012 已經內含網路負載平衡功能（Windows NLB），因此您可以如圖 B-1-2 所示取消負載平衡器，改在前端 Web Farm 啟用 Windows NLB，並利用它來提供負載平衡與容錯功能。

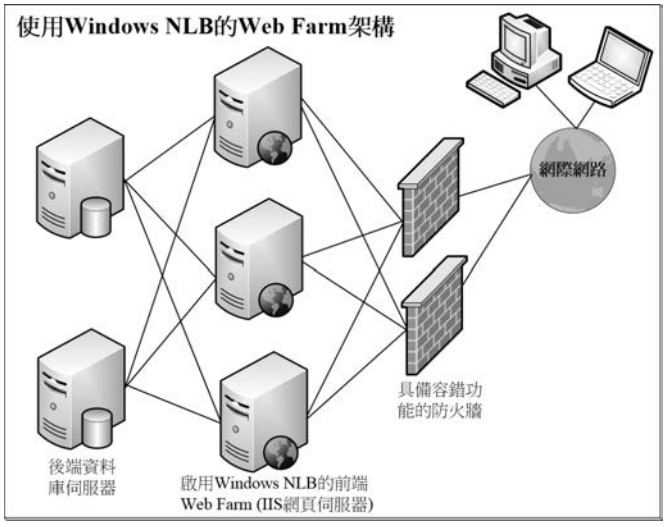

圖 B-1-2

還有因為 Microsoft Forefront Threat Management Gateway (TMG) 或 Microsoft ISA Server 等防火牆可以透過發行規則來支援 Web Farm，因此可以如圖 B-1-3 所示來建置 Web Farm 環境。

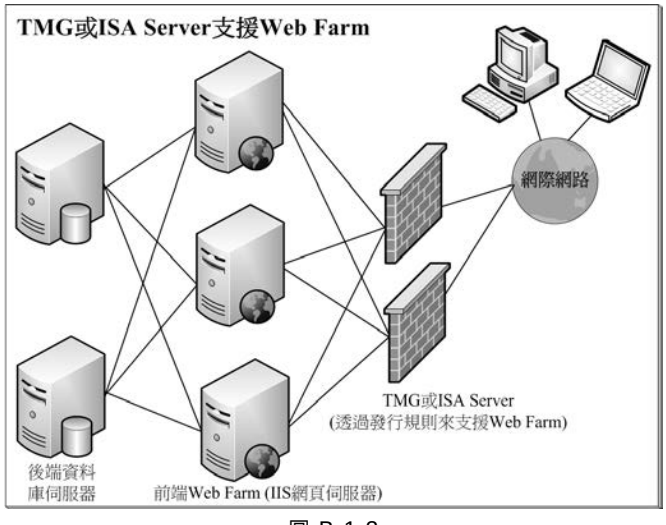

圖 B-1-3

圖中 TMG 或 ISA Server 接收到外部連接內部網站要求時，它會根據發行規則的設定，來將此要求轉交給 Web Farm 中的一台網頁伺服器處理。TMG 或 ISA Server 也具備自動偵測網頁伺服器是否停止服務的功能，因此它只會將要求轉給仍然正常運作的網頁伺服器。

網頁內容的儲存地點

您可以如圖 B-1-4 所示將網頁儲存在每一台網頁伺服器的本機磁碟內（圖中將防火牆與負載平衡器各簡化為一台），您必須讓每一台網頁伺服器內所儲存的網頁內容都相同，雖然可以利用手動複製的方式來將網頁檔案複製到每一台網頁伺服器，不過建議採用 DFS（分散式檔案系統）來自動複製，此時只要更新其中一台網頁伺服器的網頁檔案，它們就會透過 **DFS 複寫**功能自動複製到其他網頁伺服器。

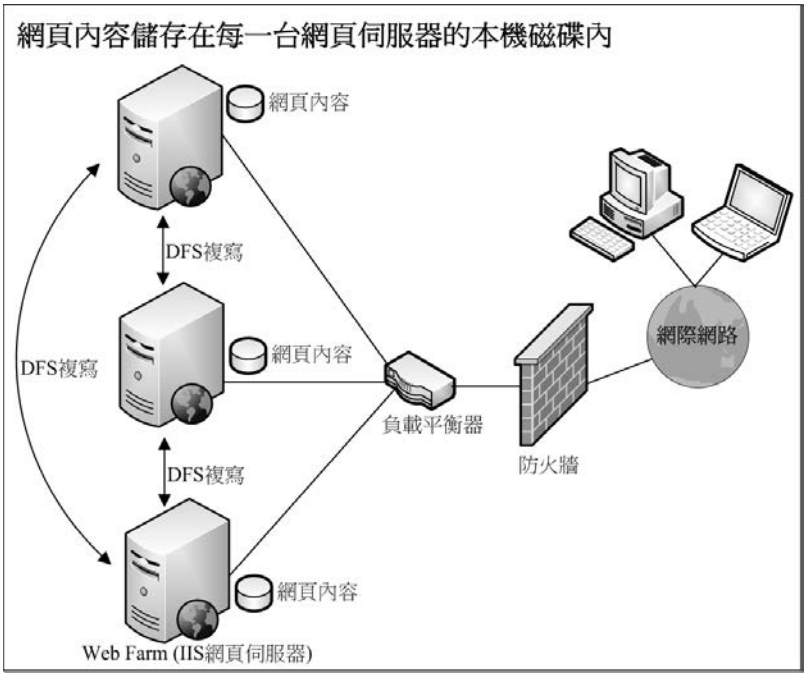

圖 B-1-4

也可以如圖 B-1-5 所示將網頁儲存到 SAN(Storage Area Network)或 NAS (Network Attached Storage)等儲存裝置內，並利用它們來提供網頁內容的容錯功能。

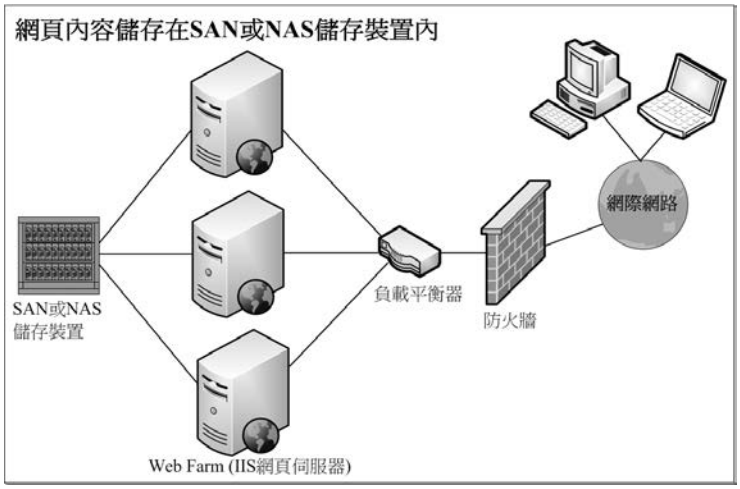

圖 B-1-5

您也可以如圖 B-1-6 所示將網頁儲存到檔案伺服器內，而為了提供容錯功能，因此應該架設多台檔案伺服器，同時還必須確保所有伺服器內的網頁內容都相同，您可以利用 **DFS 複寫**功能來自動讓每一台檔案伺服器內所儲存的網頁內容都相同。

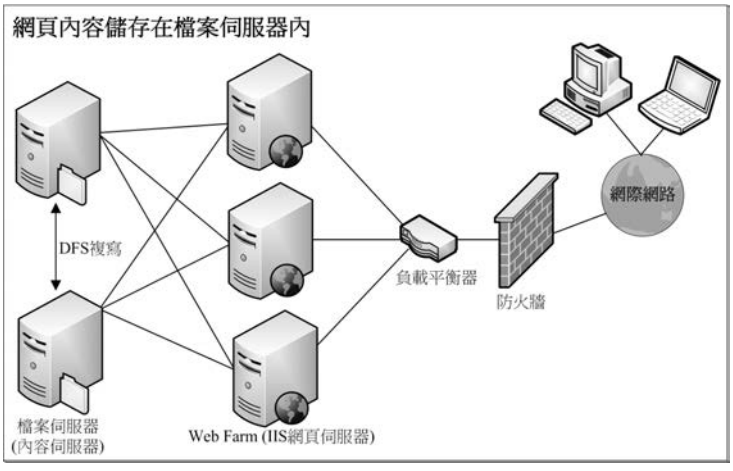

圖 B-1-6

B-2 Windows 系統的網路負載平衡概觀

由於 Windows Server 2012 系統已經內含網路負載平衡功能（Windows NLB），因此我們可以直接採用 Windows NLB 來建置 Web Farm 環境。例如圖 B-2-1 中

Web Farm 內每一台網頁伺服器的網路卡各有一個**固定 IP 位址**，這些伺服器對外的流量是透過固定 IP 位址送出。而在您建立了 NLB 叢集（NLB cluster）、啟用網路卡的 Windows NLB、將網頁伺服器加入 NLB 叢集後，它們還會共用一個相同的**叢集 IP 位址**（又稱為**虛擬 IP 位址**），並透過此叢集 IP 位址來接收外部來的上網要求，NLB 叢集接收到這些要求後，會將它們分散的交給叢集中的網頁伺服器來處理，因此可以達到負載平衡的目的，提高運作效率。

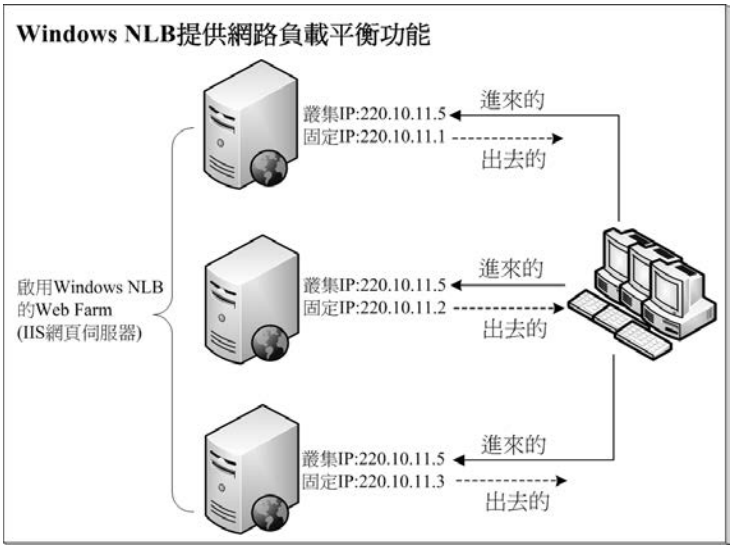

圖 B-2-1

Windows NLB 的容錯功能

若 Windows NLB 叢集內的伺服器成員有異動的話，例如伺服器故障、伺服器脫離叢集或增加新伺服器，此時 NLB 會啟動一個稱為**交集**（convergence）的程序，以便讓 NLB 叢集內的所有伺服器擁有一致的狀態與重新分配工作負擔。

舉例來說，NLB 叢集中的伺服器會隨時監聽其他伺服器的「**心跳**（heartbeat）」狀況，以便偵測是否有其他伺服器故障，若有的話，偵測到此狀況的伺服器便會啟動**交集**程序。在**交集**程序執行當中，現有正常的伺服器仍然會繼續服務，同時正在處理中的要求也不會受到影響，當完成**交集**程序後，所有連接 Web Farm 網站的要求，會重新分配給剩下仍正常的網頁伺服器來負責。例如圖 B-2-2 中最上方的

伺服器故障後，接下來所有由外部來的連接 Web Farm 網站的要求，會重新分配給其他兩台仍然正常運作的網頁伺服器來負責。

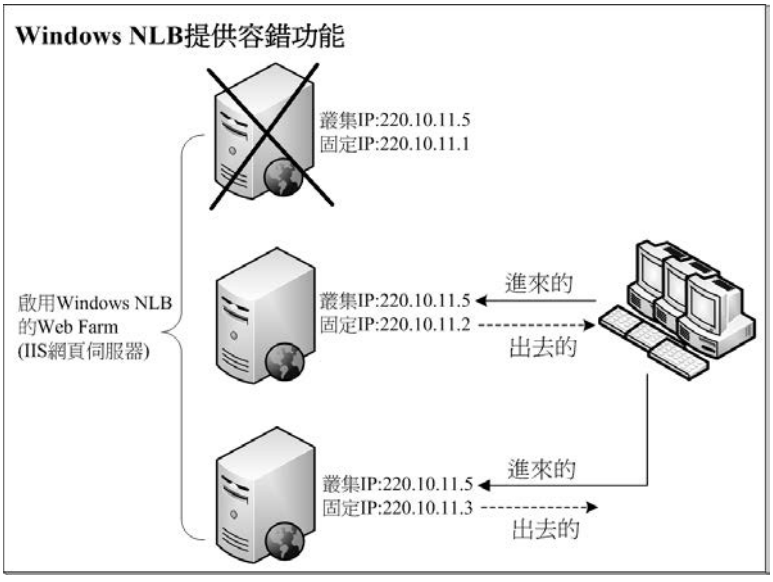

圖 B-2-2

Windows NLB 的親和性

親和性（affinity）用來定義來源主機與 NLB 叢集成員之間的關係。舉例來說，如果叢集中有 3 台網頁伺服器，當外部主機（來源主機）要連接 Web Farm 時，此要求是由 Web Farm 中的哪一台伺服器來負責處理呢？它是根據 Windows NLB 所提供的以下 3 種親和性來決定的：

- **無（None）**：此時 NLB 是根據來源主機的「IP 位址與連接埠」，來將要求指派給其中一台伺服器處理。叢集中每一台伺服器都有一個**主機識別元**（host ID），而 NLB 根據來源主機的 IP 位址與連接埠所算出來的雜湊值（hash）會與**主機識別元**有著關連性，因此 NLB 叢集會根據雜湊值，來將此要求轉交給擁有相對**主機識別元**的伺服器來負責。

  因為是同時參照來源主機的 IP 位址與連接埠，因此同一台外部主機所提出的多個連接 Web Farm 要求（來源主機的 IP 位址相同、TCP 連接埠不同），可能會分別由不同的網頁伺服器來負責。

- **單一（Single）**：此時 NLB 僅根據來源主機的 IP 位址，來將要求指派給其中一台網頁伺服器處理，因此同一台外部主機所提出的所有連接 Web Farm 要求，都會由同一台伺服器來負責。
- **網路（Network）**：根據來源主機的 Class C 網路位址，來將要求指派給其中一台網頁伺服器處理。也就是 IP 位址中最高 3 個位元組相同的所有外部主機，其所提出的連接 Web Farm 要求，都會由同一台網頁伺服器負責，例如 IP 位址為 201.11.22.1 到 201.11.22.254（它們的最高 3 個位元組都是 201.11.22）的外部主機的要求，都會由同一台網頁伺服器來負責。

雖然 Windows NLB 預設是透過親和性來將用戶端的要求指派給其中一台伺服器來負責，但我們可以另外透過**連接埠規則**（port rule）來改變親和性，例如可以在連接埠規則內將特定流量指定由優先順序較高的單一台伺服器來負責處理（此時該流量將不再具備負載平衡功能）。系統預設的連接埠規則是包含所有流量（所有連接埠），且會依照所設定的親和性來將用戶端的要求指派給某台伺服器來負責，也就是預設所有流量都具備著網路負載平衡與容錯功能。

Windows NLB 的操作模式

Windows NLB 的操作模式分為**單點傳播模式**、**多點傳送模式**、**IGMP 多點傳送模式**與 3 種：

- **單點傳播模式**：NLB 叢集內每一台網頁伺服器的網路卡的 MAC 位址（實體位址）都會被替換成一個相同的**叢集 MAC 位址**，它們透過此叢集 MAC 位址來接收外部來的連接 Web Farm 要求。不過因為 MAC 位址相同，因此叢集內的伺服器之間無法相互溝通，解決此問題的方法為：每一台伺服器內各另外安裝一片網路卡，此片網路卡不要啟用 Windows NLB，因此可以保有這片網路卡的原來 MAC 位址，伺服器之間可以透過這片網路卡來相互溝通。
- **多點傳送模式**： NLB 叢集內所有伺服器的網路卡除了擁有一個共同的**多點傳送 MAC 位址**之外，它們仍然會保留自己原來的唯一 MAC 位址，因此叢集成員之間可以正常溝通。

- **IGMP 多點傳送模式**：若叢集內的伺服器與其他非叢集成員的電腦，連接在同一個交換器的話，此模式讓傳送給叢集伺服器的流量，不會被送到非叢集成員的電腦，但上述交換器需支援 **IGMP snooping**（Internet Group membership protocol 窺探）功能。

IIS 的共用設定

Web Farm 內所有網頁伺服器的設定應該要同步，而在 Windows Server 2012 的 IIS 內透過**共用設定**功能，來讓您將網頁伺服器的設定檔儲存到遠端電腦的共用資料夾內，然後讓所有網頁伺服器都來使用相同的設定檔，這些設定檔包含：

- **ApplicationHost.config**：IIS 的主要設定檔，它儲存著 IIS 伺服器內所有站台、應用程式、虛擬目錄、應用程式集區等設定與伺服器的通用預設值。
- **Administration.config**：儲存著委派管理的設定。IIS 採用模組化設計，Administration.config 內也儲存著這些模組的相關資料。
- **ConfigEncKey.key**：在 IIS 內建置 ASP.NET 環境時，有些資料會被 ASP.NET 加密，例如 ViewState、Form Authentication Tickets（表單型驗證票）等，此時需要讓 Web Farm 內每一台伺服器來使用相同的電腦金鑰（machine key），否則當其中一台伺服器利用專有金鑰將資料加密後，其他使用不同金鑰的伺服器就無法將其解密。這些共用金鑰是被儲存在 ConfigEncKey.key 檔內。

B-3 IIS 網頁伺服器的 Web Farm 實例演練

我們將利用圖 B-3-1 來說明如何建立一個由 IIS 網頁伺服器所組成的 Web Farm，假設其網址為 www.sayms.local。我們將直接在圖中兩台 IIS 網頁伺服器上啟用 Windows NLB，而 NLB 操作模式採用多點傳送模式。

注意

某些虛擬化軟體的虛擬機器內若選用單點傳播模式的話，則 NLB 可能無法正常運作，此時請選擇多點傳送模式或使用微軟的 Hyper-V。

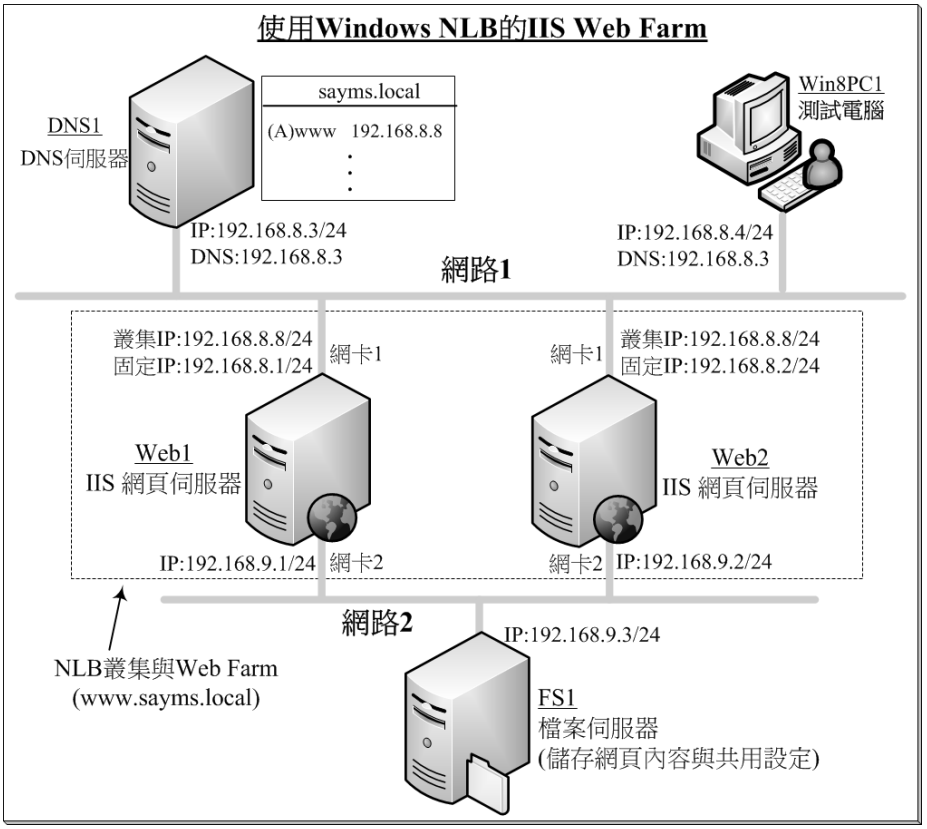

圖 B-3-1

Web Farm 的軟硬體需求

要建立圖 B-3-1 中 Web Farm 的話，其軟硬體配備需符合以下所敘述的要求（建議利用 Hyper-V 的虛擬環境來練習，可參考 **Windows Server 2012 系統建置實務**）：

- **IIS 網頁伺服器 Web1 與 Web2**：這兩台組成 Web Farm 的伺服器都是 Windows Server 2012 Enterprise，且將安裝**網頁伺服器（IIS）**角色，同時我們要建立一個 Windows NLB 叢集，並將這兩台伺服器加入到此叢集。這兩台伺服器各有兩片網路卡，一片連接**網路 1**、一片連接**網路 2**，其中只有**網卡 1** 啟用 Windows NLB，因此**網卡 1** 除了原有的固定 IP 位址（192.168.8.1、192.168.8.2）之外，

它們還有一個共同的叢集 IP 位址（192.168.8.8），並透過這個叢集 IP 位址來接收由測試電腦 Win8PC1 送來的上網要求（http://www.sayms.local/）。

- **檔案伺服器 FS1**：這台 Windows Server 2012 伺服器用來儲存網頁伺服器的網頁內容，也就是兩台網頁伺服器的主目錄都是在這台檔案伺服器的相同資料夾。兩台網頁伺服器也應該要使用相同的設定，而這些共用設定也是被儲存在這台檔案伺服器內。

附註

由於我們的重點在 Web Farm 的設定，因此將測試環境簡化為僅架設一台檔案伺服器，故網頁內容與共用設定並沒有容錯功能，您可以自行架設多台檔案伺服器，然後利用 **DFS 複寫**來同步網頁內容與共用設定，以便提供容錯功能，您也可以利用 SAN（FC SAN 或 iSCSI SAN）儲存裝置來儲存網頁內容與共用設定。關於 DFS、iSCSI SAN 的說明可請參閱 **Windows Server 2012 系統建置實務**這本書。

- **DNS 伺服器 DNS1**：我們利用這台 Windows Server 2012 伺服器來解析 Web Farm 網址 www.sayms.local 的 IP 位址。
- **測試電腦 Win8PC1**：我們將在這台 Windows 8 電腦上利用網址 http://www.sayms.local/來測試是否可以正常連接 Web Farm 網站。若要簡化測試環境的話，可以省略此電腦，直接改在 DNS1 上來測試也可以。

準備網路環境與電腦

我們將按部就班來說明如何建置圖 B-3-1 中的 Web Farm 環境，請確實遵照以下步驟來練習，以減少出錯的機率。

- 將 DNS1 與 Win8PC1 的網路卡連接到網路 1，Web1 與 Web2 的網卡 1 連接到網路 1、網卡 2 連接到網路 2，FS1 的網路卡連接到網路 2。若使用 Windows Server 2012 的 Hyper-V 虛擬環境的話，請自行建立兩個虛擬交換器（虛擬網路）來代表網路 1 與網路 2。

- 在圖中 5 台電腦上安裝作業系統：除了電腦 Win8PC1 安裝 Windows 8 之外，其他電腦都安裝 Windows Server 2012 Enterprise，並將它們的電腦名稱分別改為 DNS1、Win8PC1、Web1、Web2 與 FS1。

  若是使用虛擬機器，而且圖中 4 台伺服器是從現有虛擬機器複製的話，請在這 4 台伺服器上執行 Sysprep.exe 程式來變更其 SID（記得要勾選**一般化**）。

- 建議變更兩台網頁伺服器的 2 片網路卡名稱，以利於辨識，例如圖 B-3-2 表示它們分別是連接到網路 1 與網路 2 的網路卡：【按⊞+ X 鍵➲檔案總管➲對著**網路**按右鍵➲內容➲點擊**變更介面卡設定**➲分別對著 2 個網路連線按右鍵➲重新命名】。

圖 B-3-2

- 依照實例演練圖（圖 B-3-1）來設定 5 台電腦的網路卡 IP 位址、子網路遮罩、慣用 DNS 伺服器（暫時不要設定叢集 IP 位址，等建立 NLB 叢集時再設定，否則 IP 位址會相衝）：【開啟**控制台**➲網路和網際網路➲網路和共用中心➲點擊**乙太網路**（或**網路 1**、**網路 2**）➲點擊內容鈕➲網際網路通訊協定第 4 版（TCP/IPv4）】，本範例採用 IPv4。

- 暫時關閉這 5 台電腦的 **Windows 防火牆**（否則下一個測試步驟會被阻擋）：【開啟**控制台**➲系統及安全性➲Windows 防火牆➲檢視此電腦已連線的網路位置➲點擊**開啟或關閉 Windows 防火牆**➲將電腦所在網路位置的 **Windows 防火牆**關閉】。

- 強烈建議您執行以下步驟來測試同一個子網路內的電腦之間是否可以正常溝通，以減少後面除錯的困難度：

  - 到 DNS1 上分別利用 ping 192.168.8.1、ping 192.168.8.2 與 ping 192.168.8.4 來測試是否可以跟 Web1、Web2 與 Win8PC1 溝通。

- 到 Win8PC1 上分別利用 ping 192.168.8.1、ping 192.168.8.2 與 ping 192.168.8.3 來測試是否可以跟 Web1、Web2 與 DNS1 溝通。
- 到 Web1 上分別利用 ping 192.168.8.2（與 ping 192.168.9.2）、ping 192.168.8.3、ping 192.168.8.4 與 192.168.9.3 來測試是否可以跟 Web2、DNS1、Win8PC1 與 FS1 溝通。
- 到 Web2 上分別利用 ping 192.168.8.1（與 ping 192.168.9.1）、ping 192.168.8.3、ping 192.168.8.4 與 192.168.9.3 來測試是否可以跟 Web1、DNS1、Win8PC1 與 FS1 溝通。
- 到 FS1 上分別利用 ping 192.168.9.1 與 ping 192.168.9.2 來測試是否可以跟 Web1 與 Web2 溝通。

↘ 可重新開啟這 5 台電腦的 **Windows 防火牆**。

DNS 伺服器的設定

DNS 伺服器 DNS1 是用來解析 Web Farm 網址 www.sayms.local 的 IP 位址。請在這台電腦上透過【開啟**伺服器管理員**➲點擊**儀表板**處的**新增角色及功能**】的途徑來安裝 DNS 伺服器。

安裝完成後：【按⊞鍵切換到**開始**選單➲DNS➲對著**正向對應區域**按右鍵➲新增區域】來新增一個名稱為 sayms.local 的主要區域，並在這個區域內新增一筆 Web Farm 網址的主機記錄，如圖 B-3-3 所示，圖中假設網址為 www.sayms.local，注意其 IP 位址是叢集 IP 位址 192.168.8.8。

圖 B-3-3

然後到測試電腦 Win8PC1 上來測試是否可以解析到 www.sayms.local 的 IP 位址，例如圖 B-3-4 為成功解析到叢集 IP 位址 192.168.8.8 的畫面。

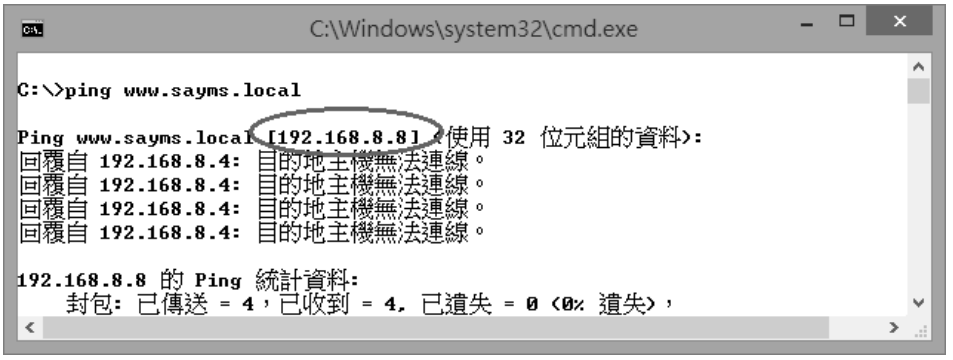

圖 B-3-4

附註

雖然成功解析到 Web Farm 網站的叢集 IP 位址，但是我們還沒有建立叢集，也還沒有設定叢集 IP 位址，故會出現類似圖中無法連線的訊息。即使叢集與叢集 IP 位址都建立好了，也可能還是會出現類似無法連線的訊息，因為 Windows Server 2012 電腦預設已經啟用 **Windows 防火牆**，它會阻擋 ping 指令的封包。

檔案伺服器的設定

這台 Windows Server 2012 檔案伺服器是用來儲存網頁伺服器的共用設定與共用網頁內容。請先在這台伺服器的本機安全性資料庫建立一個使用者帳戶，以便於兩台網頁伺服器可以利用這個帳戶來連接檔案伺服器：【按⊞鍵切換到**開始**選單➲系統管理工具➲電腦管理➲展開**本機使用者和群組**➲對著**使用者**按右鍵➲新使用者➲如圖 B-3-5 所示輸入使用者名稱（假設是 WebUser）、密碼等資料、取消勾選**使用者必須在下次登入時變更密碼**、改勾選**密碼永久有效**➲按建立鈕】。

附註

若此檔案伺服器有加入 Active Directory 網域的話，則也可利用網域使用者帳戶。

圖 B-3-5

請在此台檔案伺服器內建立用來儲存網頁伺服器共用設定與共用網頁的資料夾，假設為 C:\WebFiles，並將其設定為共用資料夾，假設共用名稱為 WebFiles，然後開放**讀取/寫入**（修改）權限給之前建立的使用者 WebUser，如圖 B-3-6 所示（若出現**網路探索及檔案共用視窗**的話，請點擊**是，開啟所有公用網路的網路探索與檔案共用**）。

圖 B-3-6

接著在此資料夾內建立兩個子資料夾，一個用來儲存共用設定、一個用來儲存共用網頁（網站的主目錄），假設資料夾名稱分別是 Configurations 與 Contents，圖 B-3-7 為完成後的畫面。

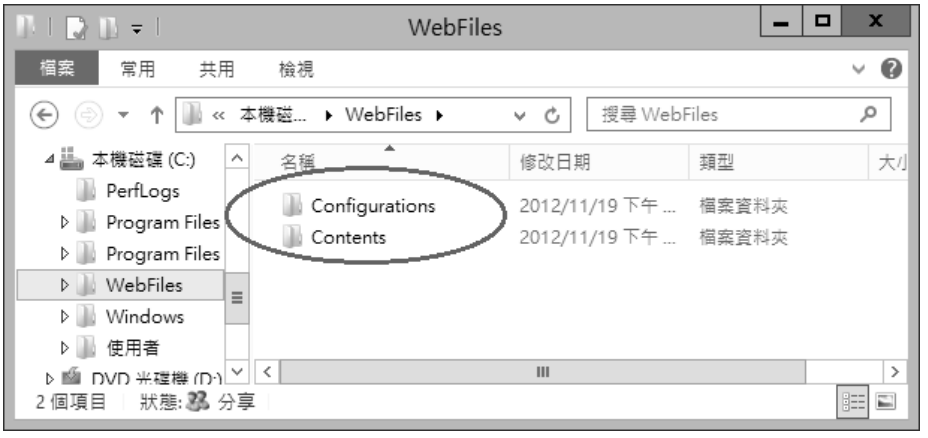

圖 B-3-7

網頁伺服器 Web1 的設定

我們將在 Web1 上安裝**網頁伺服器（IIS）**角色，同時假設網頁為針對 ASP.NET 所撰寫的程式，因此還需要安裝 **ASP.NET** 角色服務(假設是選擇 **ASP.NET 4.5**)：【開啟**伺服器管理員**➲點擊**儀表版**處的**新增角色及功能**➲持續按 下一步 鈕一直到出現**選取伺服器角色**畫面時勾選**網頁伺服器(IIS)**➲按 新增功能 鈕➲持續按 下一步 鈕一直到出現圖 B-3-8 **選取角色服務**畫面時展開**應用程式開發**➲勾選 **ASP.NET 4.5**➲…】。完成安裝後，我們使用內建的 Default Web Site 來做為本演練環境的網站。

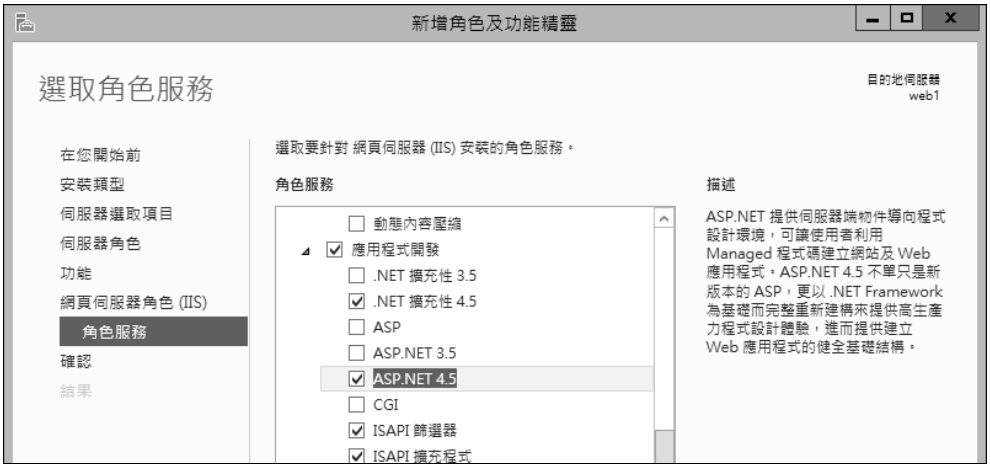

圖 B-3-8

接下來建立一個用來測試用的首頁，假設其檔名為 default.aspx，且內容為如圖 B-3-9 所示，並先將此檔案放到網站預設的主目錄 %*SystemDrive*%\inetpub\wwwroot 之下，其中的 %*SystemDrive*%一般是 C:。

圖 B-3-9

建議變更網站讀取預設文件的優先順序，以便讓網站優先讀取 default.aspx，其設定途徑為：【如圖 B-3-10 所示點擊 Default Web Site➲點擊中間的**預設文件**➲點選 Default.aspx➲透過點擊右邊**動作**窗格的**上移**，來將 default.aspx 調整到清單的最上方】，它可以提高首頁存取效率，避免網站浪費時間去嘗試讀取其他檔案。

圖 B-3-10

接著請到測試電腦 Win8PC1 上利用瀏覽器來測試是否可以正常連接網站與看到預設的網頁，如圖 B-3-11 所示為連接成功的畫面，圖中我們直接利用 Web1 的固定 IP 位址 192.168.8.1 來連接 Web1，因為我們還沒有啟用 Windows NLB，故還無法使用叢集 IP 位址來連接網站。

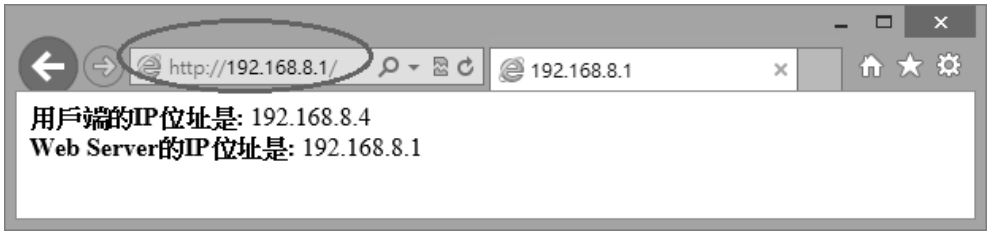

圖 B-3-11

網頁伺服器 Web2 的設定

Web2 的設定步驟大致上與 Web1 的設定相同，以下僅列出摘要：

- 在 Web2 上安裝**網頁伺服器（IIS）**角色與 ASP.NET 4.5 角色服務。
- “**不需要**”建立 default.aspx、也“**不需要**”將 default.aspx 複製到主目錄
- 直接到測試電腦 Win8PC1 上利用 http://192.168.8.2/來測試 Web2 網站是否正常運作，由於 Web2 並沒有另外建立 Default.aspx 首頁，故在 Win8PC1 上測試時，所看到的是如圖 B-3-12 所示的預設首頁。

圖 B-3-12

附註

若所架設的 Web Farm 是 SSL 網站的話，則請在 Web1 完成 SSL 憑證申請與安裝步驟、將 SSL 憑證匯出存檔、到 Web2 上透過 **Internet Information Services（IIS）管理員**來將此憑證匯入到 Web2 的網站。

共用網頁與共用設定

接下來我們要讓兩個網站來使用儲存在檔案伺服器 FS1 內的共用網頁與共用設定。

Web1 共用網頁的設定

我們將以 Web1 的網頁來當作兩個網站的共用網頁，因此請先將 Web1 主目錄 C:\inetpub\wwroot 內的測試首頁 default.aspx，透過網路複製到檔案伺服器 FS1 的

共用資料夾\\FS1\WebFiles\Contents 內：[按 ⊞+ R 鍵 ➲ 輸入\\FS1\WebFiles\Contents 後按確定鈕➲如圖 B-3-13 所示將 Default.aspx 複製到此共用資料夾內】。

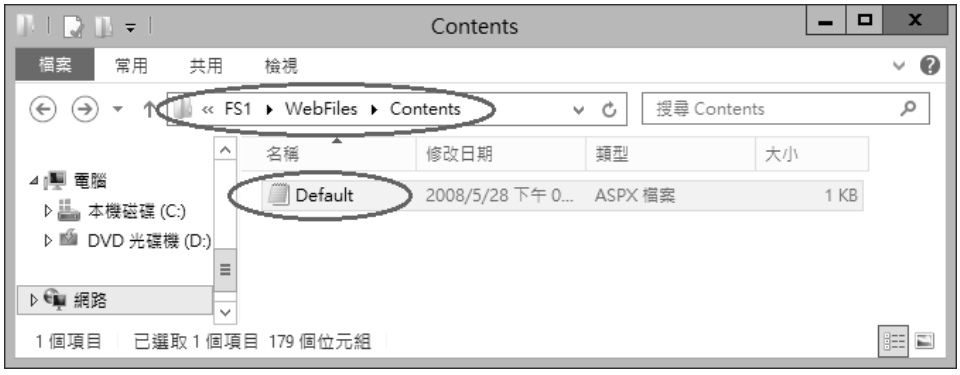

圖 B-3-13

接下來要將 Web1 的主目錄指定到\\FS1\WebFiles\Contents 共用資料夾，並且利用建立在檔案伺服器 FS1 內的本機使用者帳戶 WebUser 來連接此共用資料夾，不過在 Web1 上也必須建立一個相同名稱與密碼的使用者帳戶(請取消勾選**使用者必須在下次登入時變更密碼**、改勾選**密碼永久有效**），且必須將其加入到 **IIS_IUSRS** 群組內，如圖 B-3-14 所示。

圖 B-3-14

將 Web1 主目錄指定到\\FS1\WebFiles\Contents 共用資料夾的步驟為：

STEP 1 如圖 B-3-15 所示點擊 Default Web Site 右邊的**基本設定...**。

圖 B-3-15

STEP 2 如圖 B-3-16 所示在**實體路徑**處輸入\\FS1\WebFiles\Contents、點擊連線身分鈕。

圖 B-3-16

STEP 3 如圖 B-3-17 所示設定用來連接共用資料夾的帳戶 WebUser 後按確定鈕（請透過按設定鈕來輸入使用者名稱 WebUser 與密碼）。

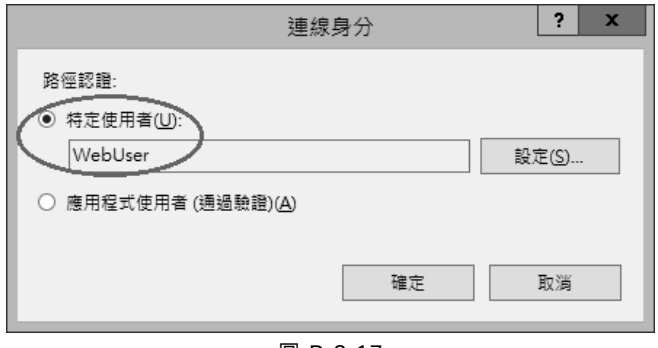

圖 B-3-17

STEP 4 點擊圖 B-3-18 中的測試設定鈕，以便測試是否可以正常連接上述共用資料夾，如前景圖所示為正常連接的畫面。按確定鈕。

圖 B-3-18

完成後，請到測試電腦 Win8PC1 上利用 http://192.168.8.1/來測試（建議先將瀏覽器的暫存檔清除），此時應該還是可以正常看到 default.aspx 的網頁。

附註

若網站因故不正常運作或安全性設定有異動的話，則您可能需要針對網站所在的應用程式集區來執行**回收**（recycle）動作，以便讓網站恢復正常或取得最新的安全設定值。舉例來說，Default Web Site 的應用程式集區為 **DefaultAppPool**，若要針對此集區來執行**回收**動作的話，請如圖 B-3-19 所示點擊 **DefaultAppPool** 右邊的**回收...**。

圖 B-3-19

Web1 的共用設定

我們將以 Web1 的設定來當作兩個網頁伺服器的共用設定，因此請先將 Web1 的設定與金鑰匯出到\\FS1\WebFiles\Configurations，然後再指定 Web1 來使用這份位於\\FS1\WebFiles\Configurations 的設定。

STEP 1 將 Web1 的設定匯出、儲存到\\FS1\WebFiles\Configurations 內。請雙擊圖 B-3-20 伺服器 WEB1 畫面中的**共用設定**。

圖 B-3-20

STEP 2 點擊圖 B-3-21 中右邊的**匯出設定...**。

圖 B-3-21

STEP 3 在圖 B-3-22 背景圖的**實體路徑**中輸入用來儲存共用設定的共用資料夾 **\\FS1\WebFiles\Configurations**➲點擊**連線身分**➲輸入有權利連接此共用資料夾的使用者名稱（WebUser）與密碼➲按確定鈕。

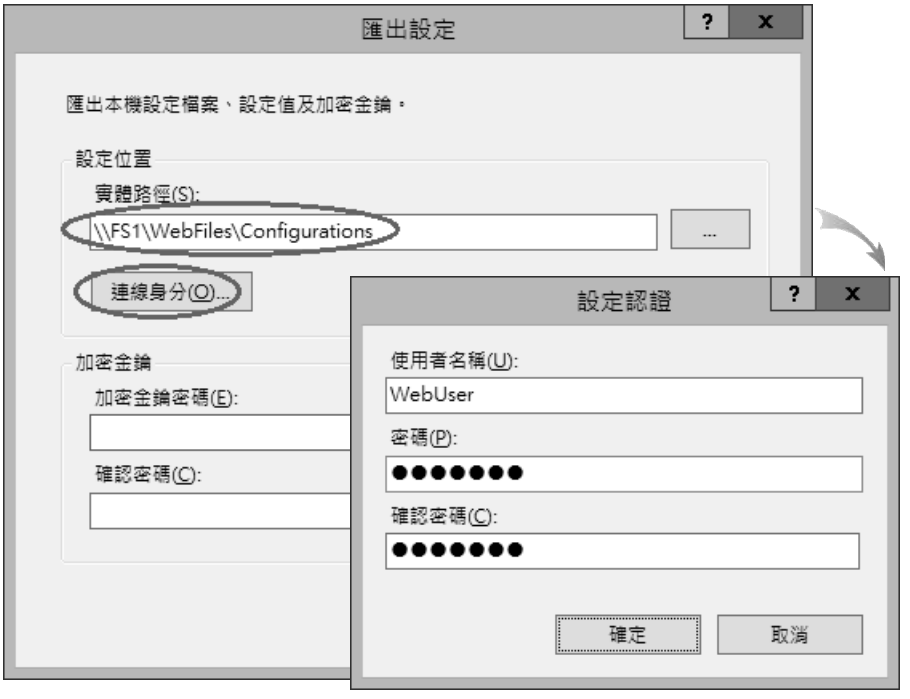

圖 B-3-22

STEP 4 在圖 B-3-23 中設定用來保護加密金鑰的密碼➲按確定鈕➲再按確定鈕。密碼必須至少 8 個字元，且需包含數字、特殊符號、英文大小寫字母。

圖 B-3-23

STEP 5 啟用 Web1 的共用設定功能：【在圖 B-3-24 中勾選**啟用共用設定**➲在**實體路徑**中輸入儲存共用設定的路徑**\\FS1\WebFiles\Configurations**➲輸入有權利連接此共用資料夾的使用者名稱（WebUser）與密碼➲點擊**套用**➲在前景圖中輸入保護加密金鑰的密碼➲按確定鈕】。

圖 B-3-24

STEP 6 持續按確定鈕來完成設定、重新啟動 IIS 管理員。Web1 的現有加密金鑰會被備份到本機電腦內用來儲存設定的目錄中（%*Systemroot*%\System32\inetsrv\config）。

完成後，請到測試電腦 Win8PC1 上利用 http://192.168.8.1/來測試（建議先將瀏覽器的暫存檔清除），此時應該還是可以正常看到 default.aspx 的網頁。

Web2 共用網頁的設定

我們要將 Web2 的主目錄指定到檔案伺服器 FS1 的共用資料夾 \\FS1\WebFiles\Contents，並利用建立在 FS1 內的本機使用者 WebUser 來連接此共用資料夾，不過在 Web2 上也必須建立一個相同名稱與密碼的使用者帳戶（請取消勾選**使用者必須在下次登入時變更密碼**、改勾選**密碼永久有效**），且必須將其加入到 **IIS_IUSRS** 群組內，如圖 B-3-25 所示。

圖 B-3-25

將 Web2 的主目錄指定到\\FS1\WebFiles\Contents 共用資料夾的步驟與 Web1 完全相同，此處不再重複，僅以圖 B-3-26 與圖 B-3-27 來說明。

圖 B-3-26

圖 B-3-27

完成後，請到測試電腦 Win8PC1 上利用 http://192.168.8.2/來測試（建議先將瀏覽器的暫存檔清除），此時應該還是可以正常看到 default.aspx 的網頁，如圖 B-3-28 所示。建議變更 Web2 預設文件的優先順序（將 default.aspx 移動到最上面），以便提高首頁存取效率，避免浪費時間去嘗試讀取其他檔案。

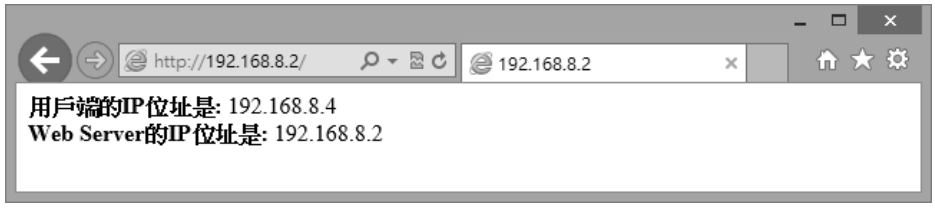

圖 B-3-28

Web2 的共用設定

我們要讓 Web2 來使用位於\\FS1\WebFiles\Configurations 內的共用設定（這些設定是之前從 Web1 匯出到此處的），其步驟如下所示。

STEP 1 請雙擊圖 B-3-29 伺服器 WEB2 畫面中的**共用設定**。

圖 B-3-29

STEP 2 在圖 B-3-30 中【勾選**啟用共用設定**➲在**實體路徑**中輸入儲存共用設定的路徑**\\FS1\WebFiles\Configurations**➲輸入有權利連接此共用資料夾的使用者名稱（WebUser）與密碼➲點擊**套用**➲在前景圖中輸入保護加密金鑰的密碼➲按確定鈕】。

圖 B-3-30

STEP 3 持續按確定鈕來完成設定、重新啟動 IIS 管理員。Web2 的現有加密金鑰會被備份到本機電腦內用來儲存設定的目錄中（%*Systemroot*%\ System32\ inetsrv\config）

完成後，請到測試電腦 Win8PC1 上利用 http://192.168.8.2/來測試（建議先將瀏覽器的暫存檔清除），此時應該還是可以正常看到 default.aspx 的網頁。

建立 Windows NLB 叢集

由於我們要在圖 B-3-31 中 Web1 與 Web2 兩台網頁伺服器上啟用 **Windows 網路負載平衡**（Windows NLB），因此需分別在這兩台伺服器上安裝**網路負載平衡**功能。

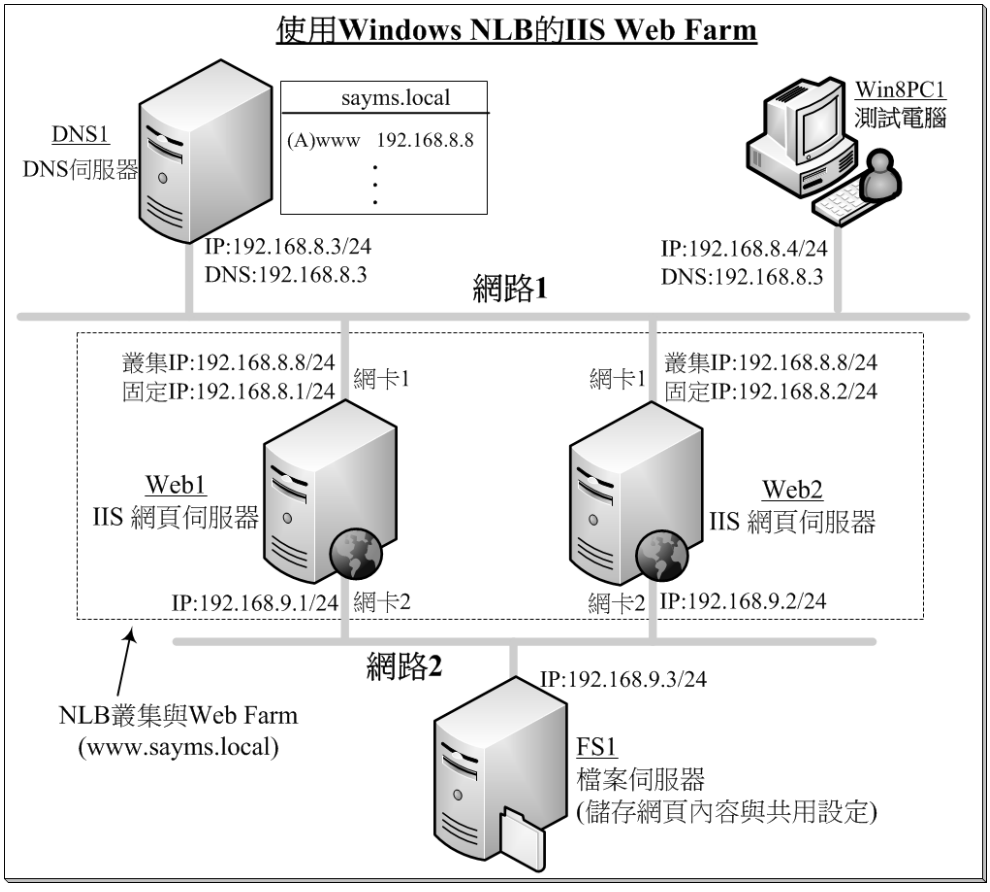

圖 B-3-31

建立 Windows NLB 叢集的步驟如下所示：

STEP 1 請分別到 Web1 與 Web2 上安裝**網路負載平衡**功能：【開啟**伺服器管理員**➲點擊**儀表版**處的**新增角色及功能**➲持續按 下一步 鈕一直到出現如圖 B-3-32 所示的**選取功能**畫面時勾選**網路負載平衡**➲…】。

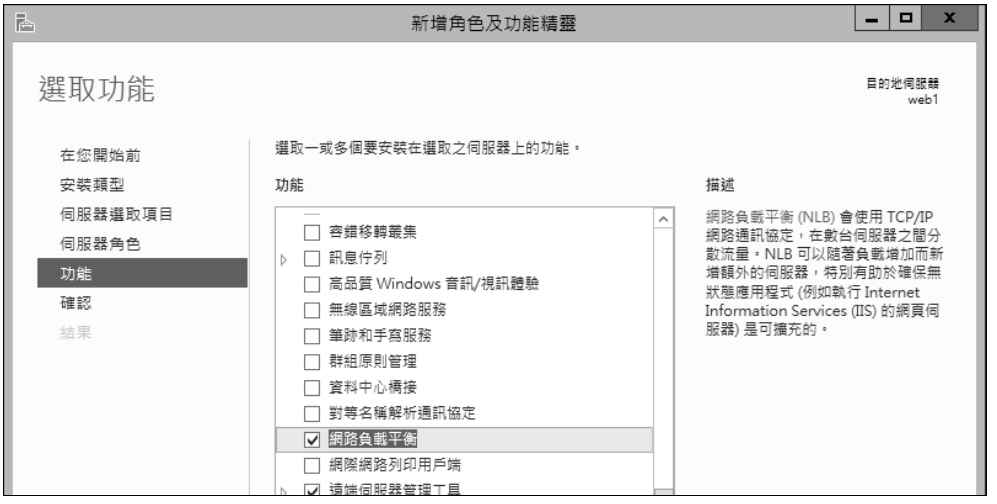

圖 B-3-32

STEP 2 到 Web1 上按⊞鍵切換到**開始**選單➲網路負載平衡管理員➲如圖 B-3-33 所示對著**網路負載平衡叢集**按右鍵➲新增叢集。

圖 B-3-33

STEP 3 在圖 B-3-34 的**主機**處輸入要加入叢集的第 1 台伺服器的電腦名稱 Web1 後按**連線**鈕，然後從畫面下方來選擇 Web1 內欲啟用 NLB 的網路卡後按**下一步**鈕。圖中我們選擇連接在網路 1 的網路卡。

圖 B-3-34

STEP 4 在圖 B-3-35 中直接按**下一步**鈕即可。圖中的**優先順序（單一主機識別元）**就是 Web1 的 host ID（每一台伺服器的 host ID 必須是唯一的），若叢集接收到的封包是未定義在**連接埠規則**內的話，它會將此封包交給優先順序較高（host ID 數字較小）的伺服器來處理。您也可以在此畫面為此網路卡新增多個固定 IP 位址。

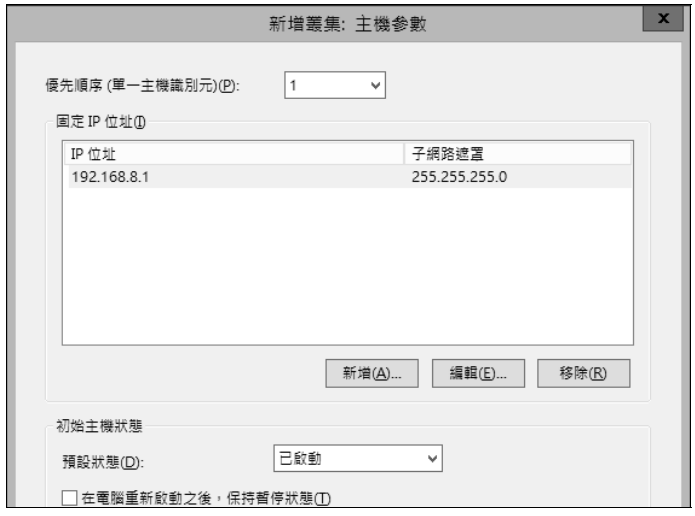

圖 B-3-35

STEP 5 在圖 B-3-36 按新增鈕、設定叢集 IP 位址（例如 192.168.8.8）與子網路遮罩（255.255.255.0）後按確定鈕。

圖 B-3-36

STEP 6 回到**新增叢集： 叢集 IP 位址**畫面時按下一步鈕（您也可以在此處新增多個叢集 IP 位址）。

STEP 7 在圖 B-3-37 的**叢集操作模式**處選擇**多點傳送**模式後按下一步鈕。

圖 B-3-37

附註

您也可以選擇**單點傳送模式**或 **IGMP 多點傳送模式**，若選擇 **IGMP 多點傳送模式**的話，叢集中的每台伺服器會定期送出 **IGMP 加入群組**的訊息，支援 **IGMP Snooping** 的交換器收到此訊息後，就可得知這些隸屬於相同多點傳送群組的叢集伺服器是連接在哪一些 port 上，如此傳送給叢集的封包只會被送到這些 port。

STEP 8 在圖 B-3-38 中直接按完成鈕來採用預設的連接埠規則。

圖 B-3-38

STEP 9 設定完成後會進入**交集**（convergence）程序，稍待一段時間後便會完成此程序，而圖 B-3-39 中**狀態**欄位也會改為圖中的**已交集**。

圖 B-3-39

STEP 10 接下來將 Web2 加入到 NLB 叢集：【如圖 B-3-40 所示對著叢集 IP 位址 192.168.8.8 按右鍵➲新增主機到叢集➲在**主機**處輸入 Web2 後按連線鈕➲從畫面下方選擇 Web2 內欲啟用 NLB 的網路卡後按下一步鈕（圖中我們選擇連接在網路 1 的網路卡）】。

附註

請先將 Web2 的 **Windows 防火牆**關閉或例外開放**檔案及印表機共用**，否則會被 **Windows 防火牆**的阻擋而無法解析到 Web2 的 IP 位址。若不想變動 **Windows 防火牆**設定的話，請直接輸入 Web2 的 IP 位址。

圖 B-3-40

STEP 11 在圖 B-3-41 中直接按下一步鈕即可，其**優先順序（單一主機識別元）**為 2，也就是 host ID 為 2。

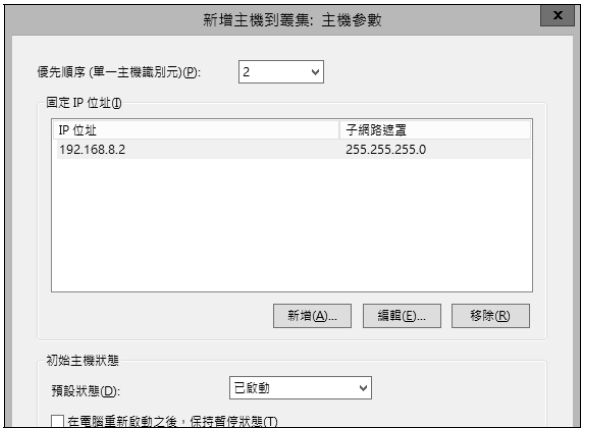

圖 B-3-41

STEP 12 在圖 B-3-42 中直接按完成鈕。

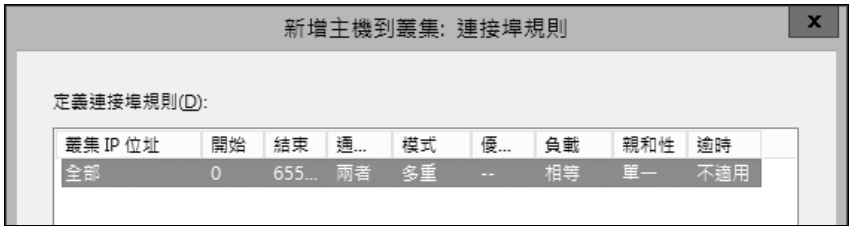

圖 B-3-42

STEP 13 設定完成後會進入**交集**（convergence）程序，稍待一段時間後便會完成此程序，而圖 B-3-43 中**狀態**欄位也會改為圖中的**已交集**。

圖 B-3-43

完成以上設定後，接下來請到測試電腦 Win8PC1 上利用瀏覽器測試是否可以連接到 Web Farm 網站，這一次我們將如圖 B-3-44 透過網址 www.sayms.local 來連接，此網址在 DNS 伺服器內所記錄的 IP 位址為叢集的 IP 位址 192.168.8,.8，故此次是透過 NLB 叢集來連接 Web Farm，圖 B-3-44 為成功連線後的畫面。

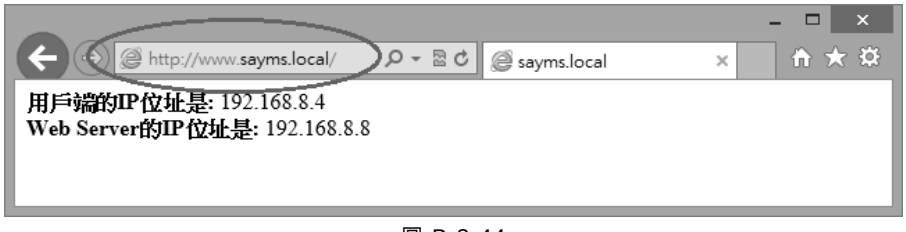

圖 B-3-44

您可以利用以下方式來進一步的測試 NLB 與 Web Farm 功能：將 Web1 關機，但保持 Web2 開機，然後再測試是否可以連接 Web Farm、看到網頁；完成後，改為將 Web2 關機，但保持 Web1 開機，然後再測試是否可以連接 Web Farm、看到網頁。為了避免 Internet Explorer 暫存檔干擾您驗證實驗結果，因此每次測試前，請先刪除暫存檔或直接按 Ctrl + F5 鍵。

B-4 Windows NLB 叢集的進階管理

如果您要變更叢集設定的話，例如新增主機到叢集、刪除叢集，請如圖 B-4-1 所示對著叢集按右鍵，然後透過圖中的選項來設定。

圖 B-4-1

您也可以針對單一伺服器來變更其設定，其設定途徑為如圖 B-4-2 所示對著伺服器按右鍵，然後透過圖中的選項來設定。圖中的**刪除主機**會將該伺服器從叢集中移除，並停用其**網路負載平衡**功能。

圖 B-4-2

如果您在圖 B-4-1 中選擇**叢集內容**的話，就可以來變更叢集 IP 位址、叢集參數與連接埠規則，如圖 B-4-3 所示為連接埠規則的畫面。

圖 B-4-3

此處我們針對連接埠規則來做進一步的說明。請點選圖中唯一的連接埠規則後按編輯鈕，此時會出現如圖 B-4-4 所示的畫面。

圖 B-4-4

- **叢集 IP 位址**：透過此處來選擇適用此連接埠規則的叢集 IP 位址，也就是只有透過此 IP 位址來連接 NLB 叢集時，才會套用此規則。

  若此處是勾選**全部**的話，則所有叢集 IP 位址皆適用於此規則，此時這個規則被稱為**通用連接埠規則**。若您自行新增其他連接埠規則，而其設定與**通用連接埠規則**相衝突的話，則您新增的規則優先。

- **連接埠範圍**：此連接埠規則所涵蓋的連接埠範圍，預設是所有的連接埠。
- **通訊協定**：此連接埠規則所涵蓋的通訊協定，預設是同時包含 TCP 與 UDP。
- **篩選模式**
  - **多重主機**與**親和性**：叢集內所有伺服器都會處理進入叢集的網路流量，也就是共同來提供網路負載平衡與容錯功能，並依照親和性的設定來將要求交給叢集內的某台伺服器負責。親和性的原理請參閱第 7-7 頁 **Windows NLB 的親和性**。
  - **單一主機**：表示與此規則有關的流量都將交給單一伺服器來負責處理，這台伺服器是處理優先順序（handling priority）較高的伺服器，處理優先順序預設是根據 host ID 來設定（數字較小優先順序越高）。您可以變更伺服器的處理優先順序值（參考後面圖 B-4-5 中的**處理優先順序**）。
  - **停用這個連接埠範圍**：所有與此連接埠規則有關的流量都將被 NLB 叢集阻擋。

  如果圖 B-4-4 中的**篩選模式**為「**多重主機**與**親和性**」的話，則針對此規則所涵蓋的連接埠來說，叢集中每一台伺服器的負擔比率預設是相同的，若要變更單一伺服器的負擔比率的話：【對著該伺服器按右鍵➲主機內容➲**連接埠規則**標籤➲點選連接埠規則➲點擊編輯鈕➲在圖 B-4-5 中先取消勾選**相等**後、再透過**負載權數**來調整相對比率】。舉例來說，若叢集中有 3 台伺服器，且其**負載權數**值分別被設定為 50、100、150，則其負擔比率為 1：2：3。

圖 B-4-5

您可以透過【如圖 B-4-6 所示對著伺服器按右鍵➲控制主機】的途徑來啟動（開始）、停止、清空停止、暫停與繼續該台伺服器的服務。其中的**停止**會讓此伺服器停止處理所有的網路流量要求，包含正在處理中的要求；而**清空停止**（drainstop）僅會停止處理新的網路流量要求，但是目前正在處理中的要求並不會被停止。

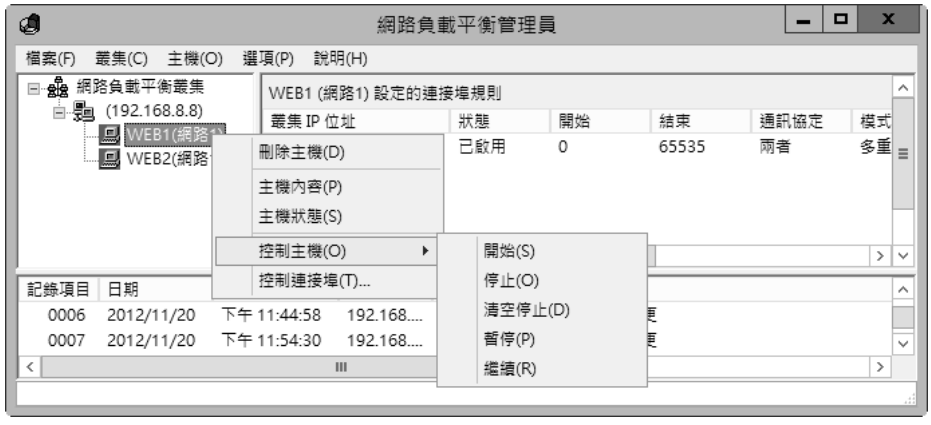

圖 B-4-6

您可以透過【如圖 B-4-7 對著伺服器按右鍵➲控制連接埠➲點選連接埠規則】的途徑來啟用、停用或清空該連接埠規則。其中的**停用**表示此伺服器不再處理與此連接埠規則有關的網路流量，包含正在處理中的要求；而**清空**（drain）僅會停止處理新的網路流量要求，但是目前正在處理中的要求並不會被停止。

圖 B-4-7

附註

您也可以利用 **NLB.EXE** 程式來執行上述的管理工作。

C

IPsec 與網路安全

我們在第 5 章介紹過利用 PKI（Public Key Infrastructure）來確保資料在網路上傳送的安全性，本章將介紹另外一種可在 IP 網路上使用的安全性通訊協定：IPsec（Internet Protocol Security）。

C-1 IPsec 概觀

C-2 獨立伺服器之間的 IPsec 設定

C-3 路由器的 IPsec 設定

C-4 透過網域群組原則來設定 IPsec

C-5 採用電腦憑證的 IPsec 設定

C-6 IPsec 跨越 NAT 的問題

C-1 IPsec 概觀

IPsec 提供以下功能來讓電腦之間能夠安全的傳送資料：

- 在開始傳送資料之前會先相互驗證對方的身分（authentication）。
- 會檢查所收到的資料是否在傳送過程中被惡意者擷取與竄改，也就是確認資料的完整性（integrity）。
- 會將傳送的資料加密（encryption），以免資料內容外洩。

兩台電腦之間在開始將資料安全的傳送出去之前，它們之間必須先協商（negotiate），以便雙方同意如何交換與保護所傳送的資料，此協商結果被稱為 SA（Security Association），它就好像是雙方所簽訂的**合約書**。SA 內包含著雙方所協商出來的安全通訊協定與 SPI（security parameter index，見附註）等資料。所採用的協商方法是標準的 IKE（Internet Key Exchange），如圖 C-1-1 所示。

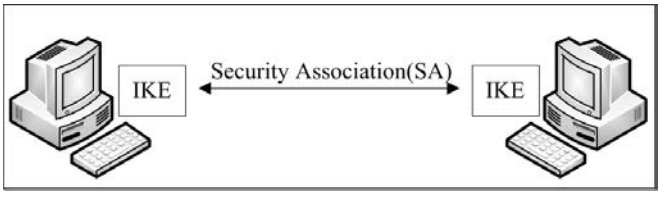

圖 C-1-1

附註

若一台電腦同時與多台電腦利用 IPsec 來溝通的話，則此電腦必然會有多個 SA，因此為了避免混淆，IPsec 利用 SA 內的 SPI 來判斷此 SA 是與哪一台電腦所協商出來的 SA。

IKE 兩階段式協商

IKE 將協商工作分為兩個階段（phase），而這兩個階段所協商出來的 SA 分別被稱為**主要模式 SA** 與**快速模式** SA。

第 1 階段：主要模式 SA（main mode SA）

此階段所建立的 SA 又稱為 **IKE SA** 或 **phase I SA**，它是為了在兩台電腦之間建立一個安全的、電腦或使用者身分（identity）經過驗證的溝通管道，之後雙方在第

2 階段中協商**快速模式 SA** 時，便能夠透過這個安全的管道來溝通。此階段會經過以下程序：

- **原則協商**：這個程序會協商出以下四個必要參數：
  - **加密方法**：例如 AES-256、AES-192、AES-128（預設）、3DES 或 DES。
  - **完整性檢查方法**：例如 SHA1（預設）或 MD5。
  - **建立金鑰的方法**：可以是 ECC P-384（Elliptic Curve Diffe-Hellman P-384）、ECC P-256、DH Group 14（Diffe-Hellman Group 14）、DH Group 2（預設）或 DH Group 1。其中 ECC P-384 與 ECC P-256 只有 Windows Vista 與 Windows Server 2008 或之後的版本才支援。
  - **驗證方法**：例如 Kerberos V5（預設）、憑證或預先共用金鑰（Preshared key）等方法，其中 Kerberos V5 只適合於網域成員電腦。
- **交換「建鑰要素」並建立主要金鑰**：為了安全性，因此金鑰並不會在網路上傳送，而是雙方各自建立金鑰，不過雙方需先交換建立金鑰所需的要素（keying material），然後再利用此**建鑰要素**來各自建立相同的**主要金鑰**（master key）。
- **驗證身分**：為了避免 man-in-the-middle 之類的攻擊行為，因此雙方身分必須經過驗證後才可以開始相互溝通，而在驗證身分時所傳送的驗證資料會透過前一個步驟所建立的**主要金鑰**來加密與解密。

第 2 階段：快速模式 SA（quick mode SA）

此階段所建立的 SA 又稱為 **IPsec SA** 或 **phase II SA**，雙方之後所傳送的資料會透過這個 SA 內的參數來確保傳送的安全性。此階段會經過以下程序：

- **原則協商**：這個程序會協商出以下幾個參數：
  - **IPsec 通訊協定**：例如 AH 或 ESP（預設）。
  - **完整性與驗證方法的雜湊演算邏輯（hash algorithm）**：例如 MD5 或 SHA1（預設）。
  - **加密方法**：例如 AES-256、AES-192、AES-128（預設）、3DES 或 DES。

- **建立「工作階段金鑰」**：第 2 階段之後雙方所傳送的資料會透過**工作階段金鑰**（session key）來加密。建立工作階段金鑰時可使用之前第 1 階段的**建鑰要素**，也可以雙方重新交換**建鑰要素**，然後利用新的**建鑰要素**來建立**工作階段金鑰**。
- **將 SA、金鑰與 SPI 傳給 IPsec 驅動程式**：雙方的 IPsec 驅動程式會根據**快速模式 SA** 內的參數與金鑰來確保資料傳送的安全性。

第 2 階段會建立兩個 SA，一個用在連入通訊，一個用在連出通訊。雖然有兩個 SA，但您利用 IPsec 監視工具查看時，畫面上只會顯示一個 SA。第 2 階段在協商安全原則與交換**建鑰要素**時，雙方所傳送資料都會受到第 1 階段的**主要金鑰**的保護。

IPsec 的運作模式

Windows 電腦的 IPsec 運作分為以下兩種模式：

- **傳輸模式（transport mode）**：表示此電腦與任何一台電腦溝通時，都需要雙方來協商使用 IPsec，例如圖 C-1-2 中左邊的 Windows 8 要與其他兩台電腦溝通時，都要求對方來協商使用 IPsec。

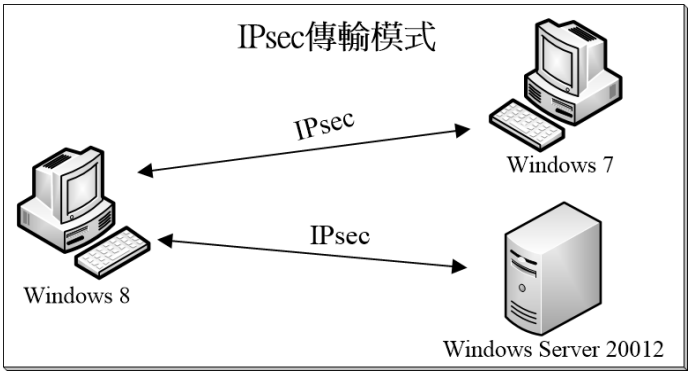

圖 C-1-2

- **通道模式（tunnel mode）**：表示此電腦只有與特定電腦溝通時才需要協商使用 IPsec，此模式適合於扮演路由器角色的電腦來使用，如圖 C-1-3 所示。圖中兩台由 Windows Server 2012 所扮演的路由器只有與對方溝通時才使用 IPsec。甲乙兩個網路內的其他電腦並不需要使用 IPsec，這兩個不同網路內的電腦要相互溝通時，會透過路由器來傳送，因而可以透過兩個路由器之間的 IPsec 通道，來確保資料在網際網路上傳送的安全性。

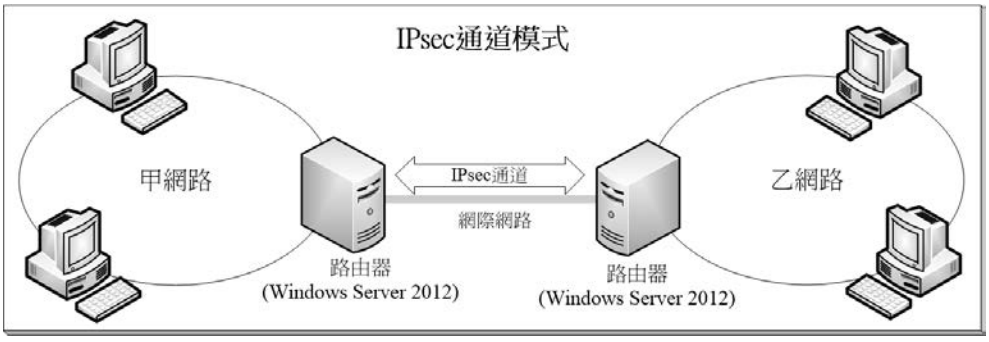

圖 C-1-3

IPsec 通訊協定

您可以透過以下兩種 IPsec 通訊協定來保護資料傳送的安全性：

- **AH（Authentication Header）**：AH 會簽署（sign）所傳送的資料，也就是它可以確認所收到的資料沒有被竄改（integrity，完整性）、可以確認資料確實是由所欲溝通的電腦傳來的（authentication）。但是 AH 不會將資料加密。圖 C-1-4 為 IP 封包經過 AH 處理前後的封包結構圖。

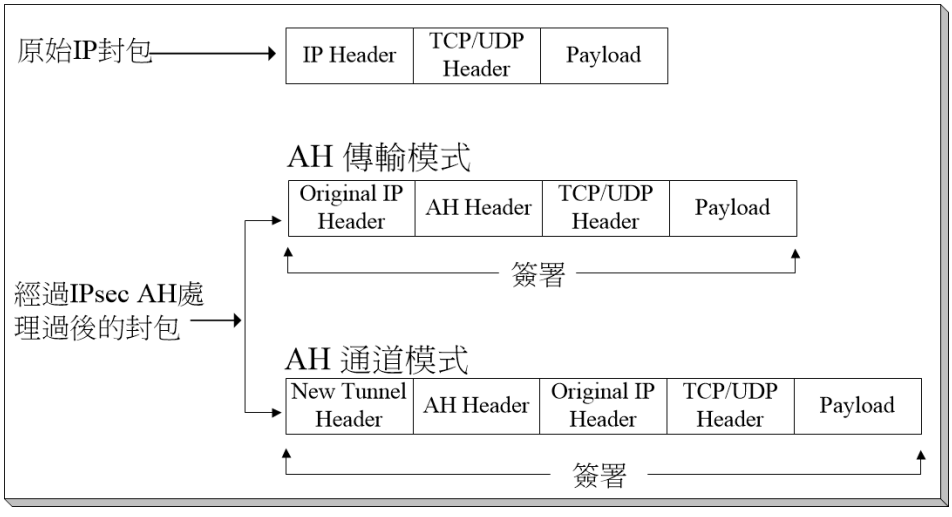

圖 C-1-4

- **ESP（Encapsulating Security Protocol）**：ESP 也會簽署所傳送的資料，也就是它可以確認所收到的資料沒有被竄改（integrity，完整性）、可以確認資料

確實是由所欲溝通的電腦傳來的（authentication），而且 ESP 會將資料加密（encryption）。圖 C-1-5 為 IP 封包經過 ESP 處理前後的封包結構圖。

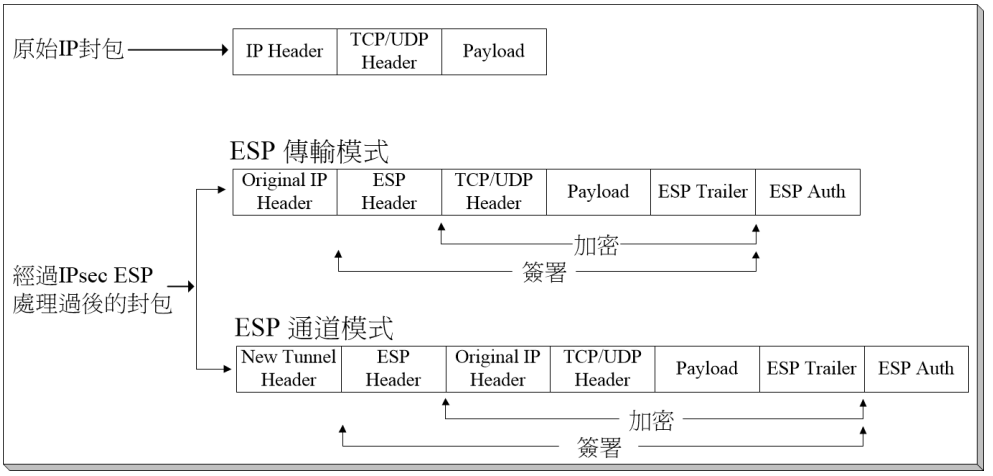

圖 C-1-5

Windows Server 2012 的 IPsec 設定

Windows Server 2012（或 Windows Server 2008(R2)、Windows 7、Windows Vista）電腦的 IPsec 可以透過建立**連線安全性規則**來啟用，而**連線安全性規則**的建立是透過**具有進階安全性的 Windows 防火牆**：

- 【開啟**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆】：它適合您來建立本機電腦的**連線安全性規則**。
- 到網域控制站上【開啟**開始**選單➲系統管理工具➲群組原則管理】：您可以透過群組原則內的**具有進階安全性的 Windows 防火牆**原則，來針對站台、網域或組織單位內的一群電腦建立**連線安全性規則**。

附註

透過**具有進階安全性的 Windows 防火牆**所建立的**連線安全性規則**，只適用於 Windows Server 2012、Windows Server 2008(R2) 、Windows 8、Windows 7 與 Windows Vista 電腦，舊版 Widows 系統的 IPsec 設定可透過自訂 **IP 安全性原則管理**主控台來完成。

C-2 獨立伺服器之間的 IPsec 設定

我們將透過圖 C-2-1 來說明如何讓圖中的兩台伺服器利用 IPsec 來安全的溝通。圖中兩台伺服器都是 Windows Server 2012 獨立伺服器，因此無法選用 Kerberos V5 驗證方法，故此處我們採用**預先共用金鑰**（Preshared key）驗證方法。請先依照圖指示設定其 IP 位址與子網路遮罩。

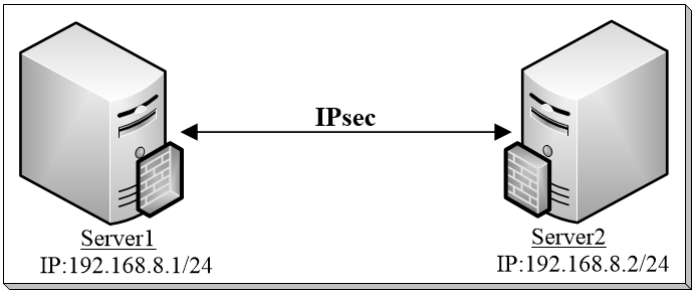

圖 C-2-1

附註

系統是以明文（clear text）的方式來傳送**預先共用金鑰**，比較不安全，因此只建議使用在測試環境。

STEP 1 我們將透過 ping 指令來確認兩台伺服器之間確實可以正常溝通，然而為了避免 ping 指令被 **Windows 防火牆**封鎖，因此請先分別在兩台伺服器上開放 ICMP 的相關流量：【按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲如圖 C-2-2 所示點擊**輸入規則**中的**檔案及印表機共用（回應要求 – ICMPv4-In）**➲點擊右邊的**啟用規則**】。

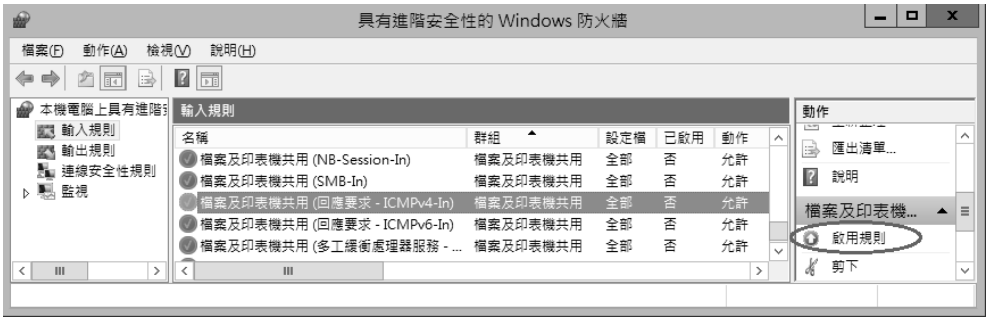

圖 C-2-2

注意

請勿將 **Windows 防火牆**關閉，否則**連線安全性規則**沒有作用。

STEP 2 請先到 Server1 上利用 ping 192.168.8.2 來測試能否與 Server2 正常溝通(如圖 C-2-3 所示為正常溝通的畫面）；然後再到 Server2 上利用 ping 192.168.8.1 來測試能否與 Server1 正常溝通。請務必執行此測試步驟，以減少之後除錯的困難度。

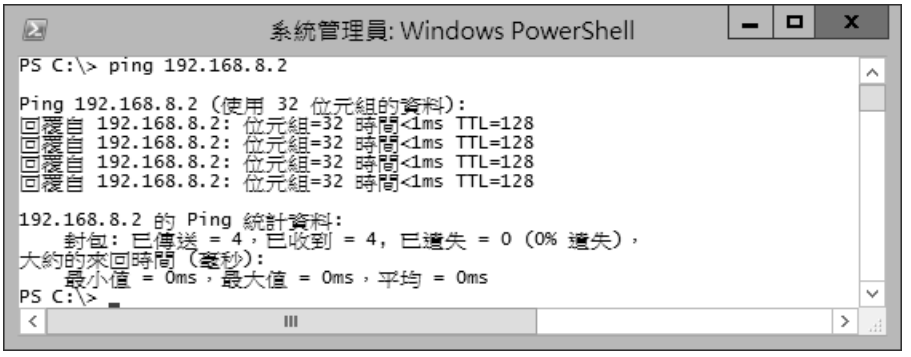

圖 C-2-3

STEP 3 請到 Server1 上開啟**具有進階安全性的 Windows 防火牆**➲如圖 C-2-4 所示點擊**連線安全性規則**右邊的**新增規則…**。

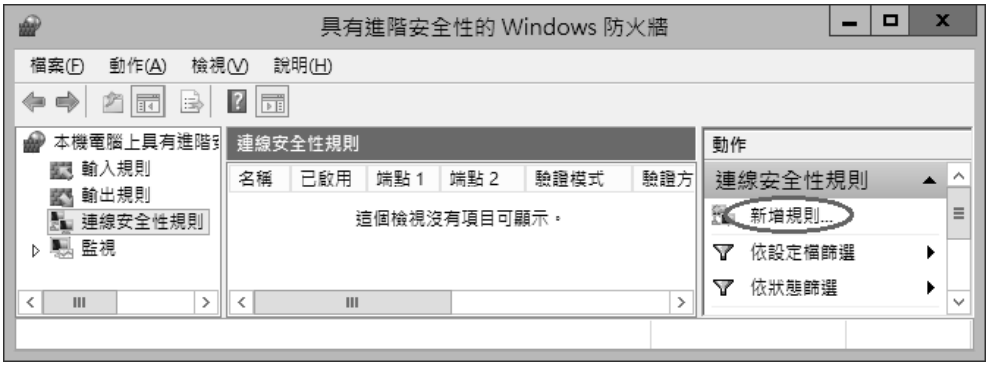

圖 C-2-4

STEP 4 在圖 C-2-5 中選擇預設的**隔離**類型後按 下一步 鈕。

圖 C-2-5

STEP 5 在圖 C-2-6 中改選第 3 個選項後按下一步鈕。圖中的三個選項：

- **要求對輸入及輸出連線執行驗證**：輸入及輸出連線都會請求對方採用 IPsec。若無法與對方協商成功的話（例如對方不具備 IPsec 功能），則採用一般連線方式亦可。
- **需要對輸入連線執行驗證並要求對輸出連線執行驗證**：輸入連線必須採用 IPsec，否則拒絕連線；輸出連線僅會請求對方採用 IPsec，若無法與對方協商成功的話，則採用一般連線方式亦可。
- **需要對輸入及輸出連線執行驗證**：無論輸入或輸出連線都必須採用 IPsec，否則拒絕連線。

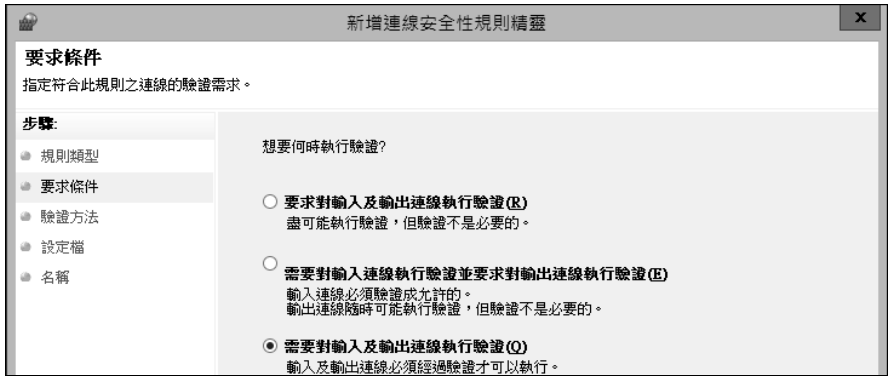

圖 C-2-6

STEP 6 在圖 C-2-7 中點選**進階**、按自訂鈕來選擇**預先共用金鑰**驗證方法。

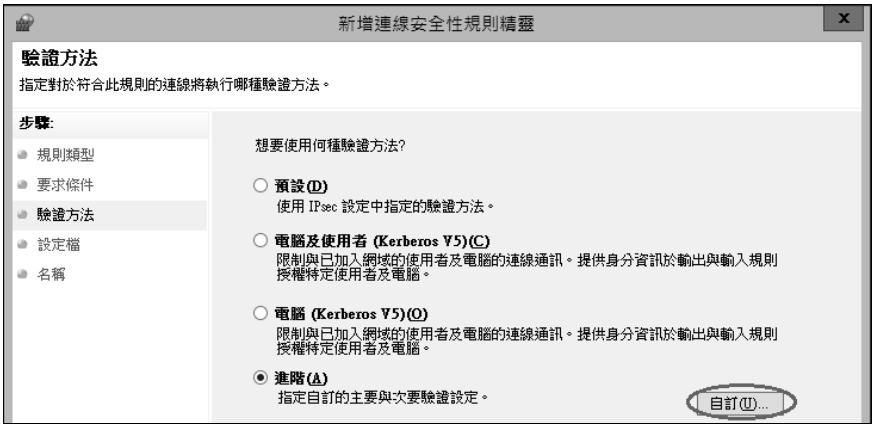

圖 C-2-7

STEP 7 在圖 C-2-8 中按新增鈕➲點選**預先共用金鑰**後輸入金鑰字串➲按確定鈕。圖中將金鑰字串設定為 1234567，對方也需設定相同的金鑰字串。

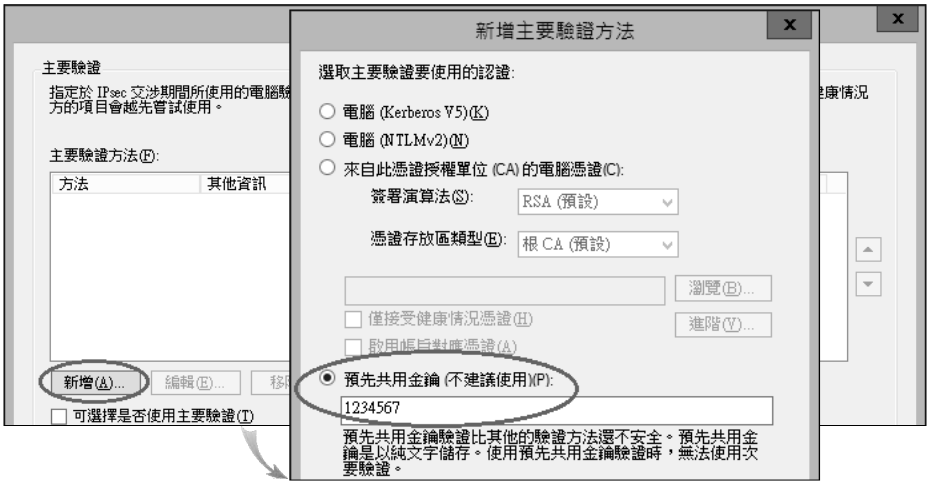

圖 C-2-8

STEP 8 繼續按確定鈕、回到**驗證方法**畫面時按下一步鈕。

STEP 9 您可以在圖 C-2-9 中選擇此電腦何時要套用此規則後按下一步鈕：

- **網域**：當此電腦連接到 Active Directory 網域時（能夠與網域控制站溝通），就套用此規則。

- **私人**：當此電腦連接到私人網路時，若無法與網域控制站溝通或該電腦非網域成員的話，就套用此規則。
- **公用**：當此電腦連接到公用網路時，就套用此規則。

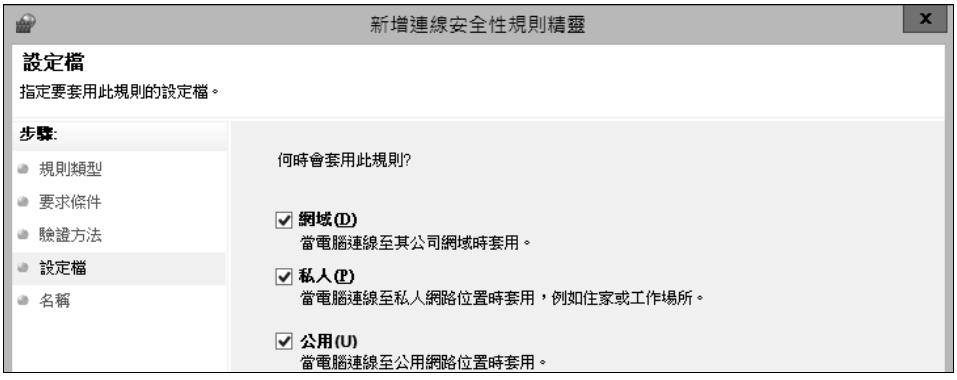

圖 C-2-9

STEP 10 在圖 C-2-10 中為此規則命名後按完成鈕。

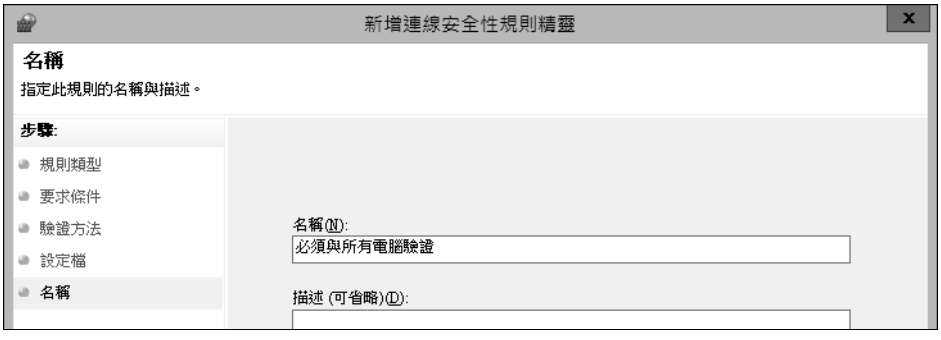

圖 C-2-10

STEP 11 圖 C-2-11 為完成後的畫面。您可以雙擊此規則來變更規則其設定，也可以【對著此規則按右鍵➲停用規則】來停用此規則。

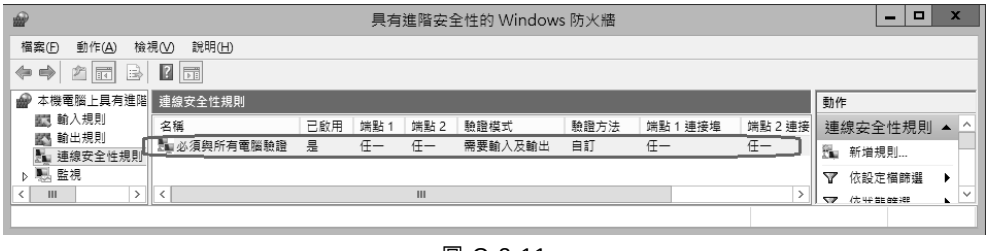

圖 C-2-11

STEP 12 由於我們所建立的規則要求無論輸入或輸出連線都必須採用 IPsec，然而目前 Server2 尚未建立**連線安全性規則**，也就是尚未啟用 IPsec，故此時若在 Server1 上利用 ping 指令來與 Server2 溝通的話，會被 Server1 拒絕，且會顯示如圖 C-2-12 **要求等候逾時**的訊息。

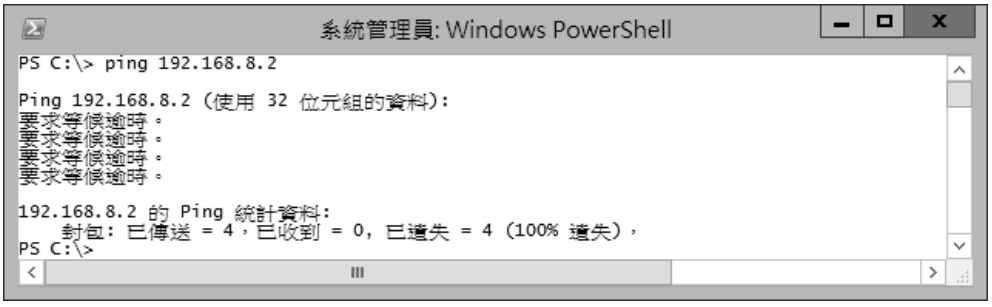

圖 C-2-12

STEP 13 換到 Server2 上來建立相同設定的**連線安全性規則**：按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲點擊**連線安全性規則**右邊的**新增規則…**➲重複 STEP 4 到 STEP 10 的步驟。

STEP 14 完成後，兩台伺服器之間利用 ping 指令應該就可以溝通，如圖 C-2-13 所示為在 Server1 上執行 ping 192.168.8.2 的畫面。

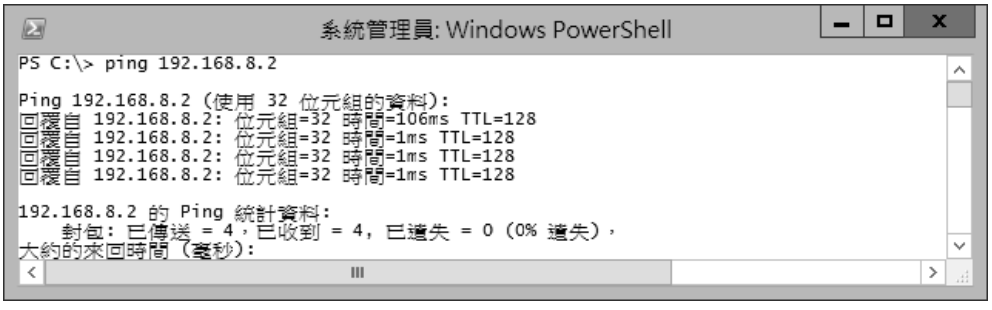

圖 C-2-13

STEP 15 如圖 C-2-14 所示可透過【點擊**監視**➲安全性關連➲**主要模式**或**快速模式**】來查看主要模式 SA 或快速模式 SA 的相關資料。

圖 C-2-14

若要變更 IPsec 預設值的話：【如圖 C-2-15 所示對著**本機電腦上具有進階安全性的 Windows 防火牆**按右鍵➲內容➲**IPsec 設定**標籤➲點擊 **IPsec 預設值**右邊的自訂鈕】，以後新建立的**連線安全性規則**就會採用此預設值。

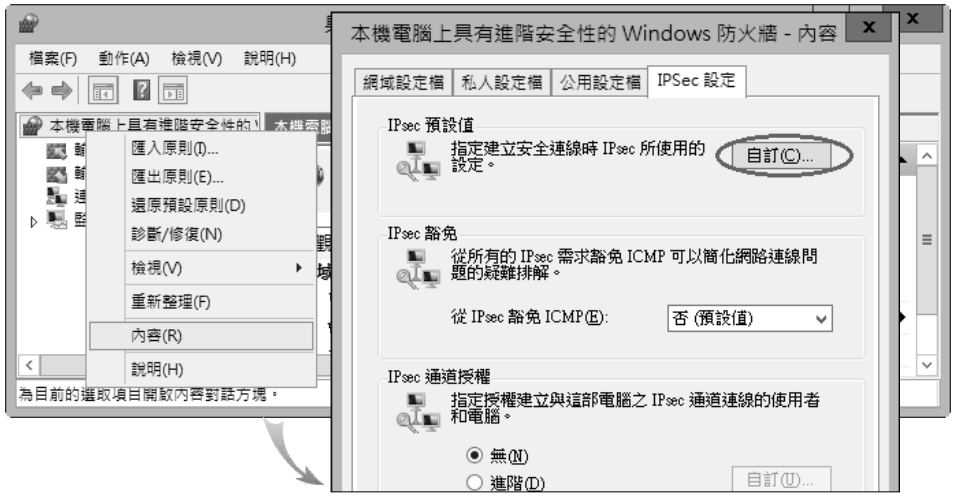

圖 C-2-15

圖中也可以透過 **IPsec 豁免**來將 ICMP 排除，也就是只要是 ICMP 流量都不需要利用 IPsec 來溝通，這個設定讓您利用 ping 指令來檢測網路電腦之間的溝通是否正常時，可以免於遭受 IPsec 的干擾。

C-3 路由器的 IPsec 設定

分別位於兩地的網路之間若要透過網際網路來安全傳送資料的話，可以在兩地的路由器之間建立 **IPsec 通道**（tunnel），如圖 C-3-1 所示，圖中只有兩台路由器之間相互溝通才需要 IPsec，例如當甲網路內的電腦要與乙網路內的電腦溝通時，它會以一般方式將資料傳給甲路由器，再由甲路由器透過 **IPsec 通道**將資料傳給乙路由器，最後再由乙路由器以一般方式將資料傳給乙網路的電腦。

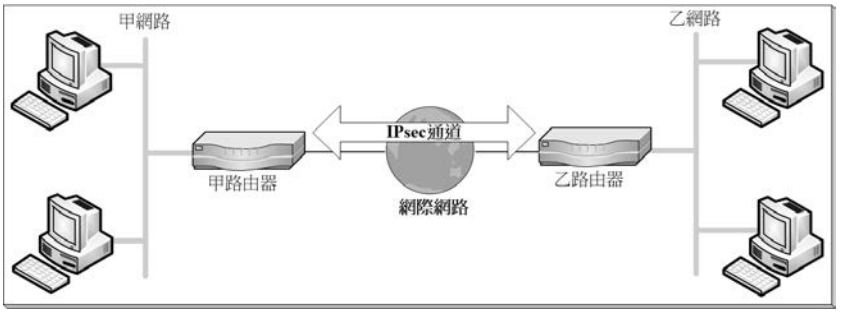

圖 C-3-1

我們透過圖 C-3-2 來說明如何在圖中兩台扮演路由器角色的 Windows Server 2012 伺服器之間建立 IPsec 通道。圖中兩台伺服器都是獨立伺服器，因此無法選用 Kerberos V5 驗證方法，故此處採用**預先共用金鑰**（Preshared key）驗證方法。請先依照圖指示設定其 IP 位址與子網路遮罩，並啟用兩台路由器的路由功能（參考章節 7-2）、然後利用 ping 指令來確認分別位於甲乙網路內的 Win8PC1 與 Win8PC2 之間可以透過路由器正常溝通 （先將兩台電腦的 **Windows 防火牆**關閉）。

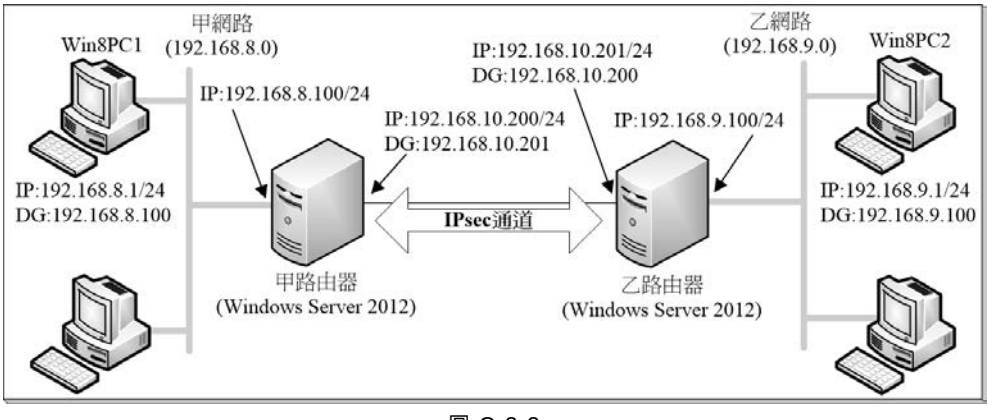

圖 C-3-2

附註

系統是以明文（clear text）的方式來傳送**預先共用金鑰**，比較不安全，因此只建議使用在測試環境。

由於建立**連線安全性規則**的方法與前一小節類似，因此本節將只說明不同之處。在兩台 Windows Server 2012 路由器透過**具有進階安全性的 Windows 防火牆**來建立**連線安全性規則**時，請如圖 C-3-3 所示選擇**通道**、**自訂設定**。

圖 C-3-3

接著在甲路由器需如圖 C-3-4 所示來設定（最後記得在**驗證方法**畫面中透過**進階**處的自訂鈕來選用**預先共用金鑰**驗證方法，假設金鑰字串為 1234567）：

圖 C-3-4

- **哪些電腦是在端點 1？**：請將本地網路（圖 C-3-2 中的甲網路）內的電腦的 IP 位址或網路識別碼輸入到此處，圖中我們輸入的網路識別碼為 192.168.8.0/24。
- **何謂本機通道端點（最靠近端點 1 中的電腦）？**：設定 **IPsec 通道**在本地網路（甲網路）這一端的端點，也就是將甲路由器的外網卡的 IP 位址 192.168.10.200 輸入到此處。
- **何謂遠端通道端點（最靠近端點 2 中的電腦）？**：設定 **IPsec 通道**在遠端網路（乙網路）那一端的端點，也就是將乙路由器的外網卡的 IP 位址 192.168.10.201 輸入到此處。
- **哪些電腦是在端點 2？**：請將遠端網路（乙網路）內的電腦的 IP 位址或網路識別碼輸入到此處，圖中我們輸入的網路識別碼為 192.168.9.0/24。

在乙路由器尚未完成 IPsec 設定之前，甲網路的 Win8PC1 無法與乙網路的 Win8PC2 溝通，您可以在 Win8PC1 利用 ping 192.168.9.1 指令來驗證之。

同理在乙路由器需如圖 C-3-5 所示來設定（最後記得在**驗證方法**畫面中透過**進階**處的自訂鈕來選用**預先共用金鑰**驗證方法，假設金鑰字串為 1234567）：

- **哪些電腦是在端點 1？**：請將本地網路（圖 C-3-2 中的乙網路）內的電腦的 IP 位址或網路識別碼輸入到此處，圖中我們輸入的網路識別碼為 192.168.9.0/24。
- **何謂本機通道端點（最靠近端點 1 中的電腦）？**：設定 **IPsec 通道**在本地網路（乙網路）這一端的端點，也就是將乙路由器的外網卡的 IP 位址 192.168.10.201 輸入到此處。

圖 C-3-5

- **何謂遠端通道端點（最靠近端點 2 中電腦）？**：設定 **IPsec 通道**在遠端網路（甲網路）那一端的端點，也就是將甲路由器的外網卡的 IP 位址 192.168.10.200 輸入到此處。
- **哪些電腦是在端點 2？**：請將遠端網路（甲網路）內的電腦的 IP 位址或網路識別碼輸入到此處，圖中我們輸入的網路識別碼為 192.168.8.0/24。

甲乙兩個路由器分別完成建立**連線安全性規則**後，甲乙兩個網路之間便可以透過 **IPsec 通道**來安全的溝通，舉例來說，當甲網路的 Win8PC1 要與乙網路的 Win8PC2 溝通時（您可以到 Win8PC1 利用 ping 192.168.9.1 指令來測試），其封包會先傳送給甲路由器，甲路由器便會自動與乙路由器建立 **IPsec 通道**，然後透過此通道將

封包傳給乙路由器，再由乙路由器將其傳給乙網路的 Win8PC2。您可以在兩台路由器上透過【開啟**具有進階安全性的 Windows 防火牆**➲展開到**監視**之下的**安全性關連**➲**主要模式**或**快速模式**（如圖 C-3-6 所示）】來查看 IPsec 通道的主要模式 SA 或快速模式 SA 的相關資料。

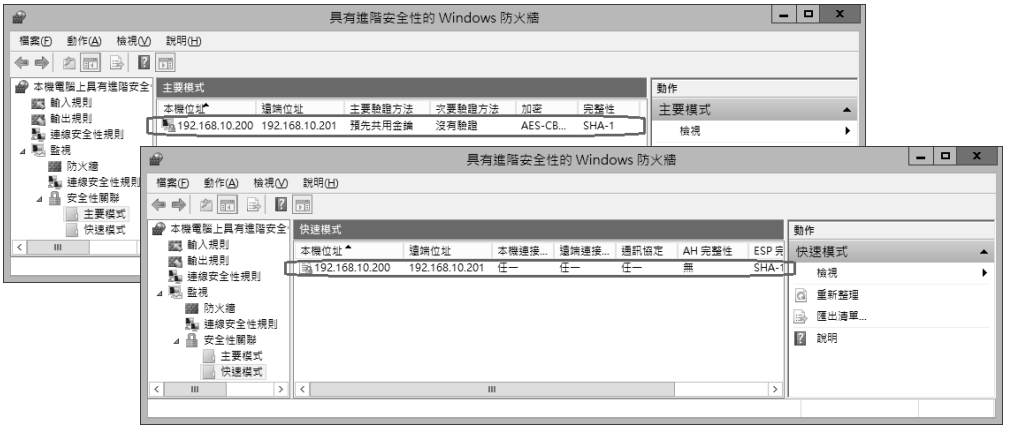

圖 C-3-6

C-4 透過網域群組原則來設定 IPsec

您可以透過 Active Directory 網域的站台、網域或組織單位的群組原則，來替網域成員電腦建立**連線安全性規則**，讓網域成員電腦之間能夠利用 IPsec 來安全的溝通。由於這些電腦都是隸屬於網域，因此可以選用 Kerberos V5 驗證方法。

我們需將 Active Directory 網域控制站排除，也就是讓網域成員與網域控制站之間的溝通不使用 IPsec，因為網域成員在利用 IPsec 驗證之前，就必須先要能夠與網域控制站正常溝通。網域控制站這類型的電腦被稱為**基礎結構電腦**，除了網域控制站之外，CA（Certificate Authority）與 DHCP 伺服器等也是隸屬於**基礎結構電腦**。若某些電腦或設備（例如路由器）不支援我們在**連線安全性規則**中所選擇的通訊協定或不支援 IPsec 的話，則也必須將它們排除在外。

我們將透過圖 C-4-1 來說明，圖中左邊甲網路的 3 台電腦都是 Windows Server 2012，其中 DC1 是網域控制站，而伺服器 Server1 與 Server2 都是網域成員伺服器。假設甲網路內的所有網域成員電腦相互之間都需要利用 IPsec 來溝通，但是將網域控制站 DC1（192.168.8.200）與路由器（192.168.8.254）排除在外。

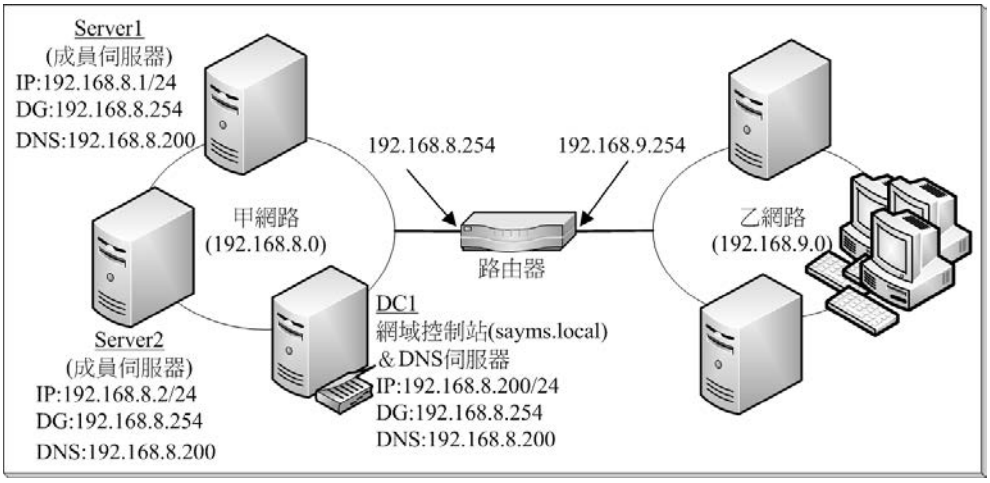

圖 C-4-1

以下將透過 Default Domain Policy 群組原則物件（ GPO）來建立**連線安全性規則**與排除規則。請先依照圖設定好左邊 3 台伺服器的 IP 位址、子網路遮罩、預設閘道、慣用 DNS 伺服器，然後建立網域與網域控制站、將 Server1 與 Server2 加入網域。可以的話，也可以安裝路由器（見第 7 章）以便做進一步的測試。

STEP 1 我們將在下一個步驟透過 ping 指令來確認圖 C-4-1 中左邊 3 台伺服器之間確實可以正常溝通，然而為了避免 ping 指令被 **Windows 防火牆**封鎖，因此請先分別在 Server1 與 Server2 上開放 ICMP 的相關流量：【按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲點擊**輸入規則**中的**檔案及印表機共用（回應要求 – ICMPv4-In）**➲點擊右邊的**啟用規則**】。網域控制站 DC1 預設已開放，不需另外再開放。

注意

請勿將 **Windows 防火牆**關閉，否則**連線安全性規則**沒有作用。

STEP 2 請分別到每一台伺服器上利用 ping 指令來測試是否可以與其他 2 台伺服器、路由器正常溝通，以便稍後來驗證我們的設定。

STEP 3 到網域控制站 DC1 上按⊞鍵切換到**開始**選單➲群組原則管理➲如圖 C-4-2 所示展開到網域 sayms.local➲對著 Default Domain Policy 按右鍵➲編輯。

圖 C-4-2

STEP 4 如圖 C-4-3 所示展開**電腦設定**➲原則➲Windows 設定➲安全性設定➲具有進階安全性的 Windows 防火牆➲具有進階安全性的 Windows 防火牆 – LDAP…➲對著**連線安全性規則**按右鍵➲新增規則。

圖 C-4-3

STEP 5 我們要先建立一個將網域控制站與預設閘道（路由器）排除的規則。請在圖 C-4-4 中選擇**豁免驗證**後按下一步鈕。

圖 C-4-4

STEP 6 如圖 C-4-5 所示按新增鈕➲輸入要被排除的網域控制站的 IP 位址 192.168.8.200➲按確定鈕。

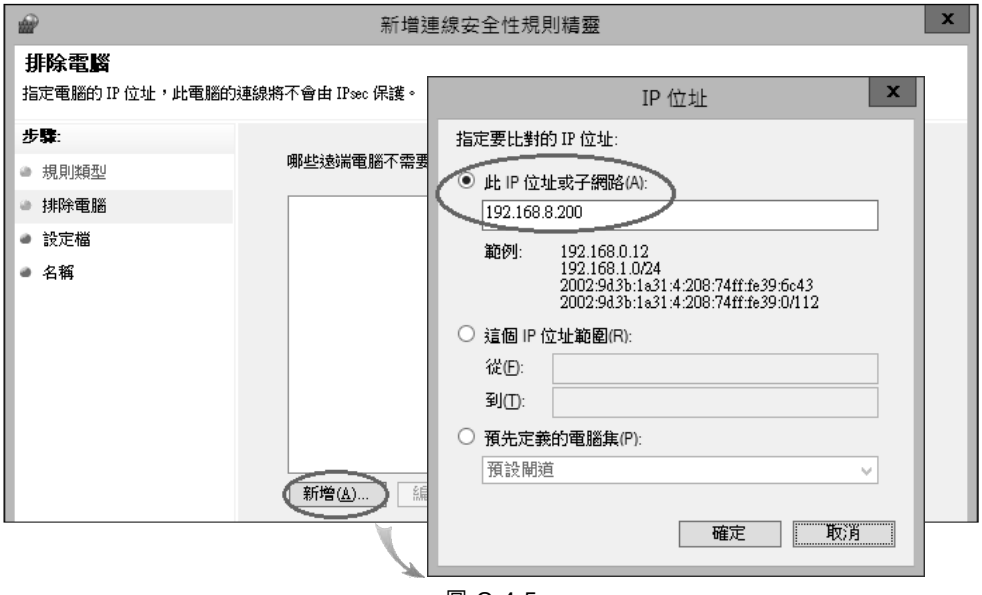

圖 C-4-5

STEP 7 如圖 C-4-6 所示繼續按新增鈕➲在**預先定義的電腦集**中選擇**預設閘道**➲按確定鈕。您也可以如前一個步驟所示自行在 **此 IP 位址或子網路**處輸入預設閘道的 IP 位址 192.168.8.254。

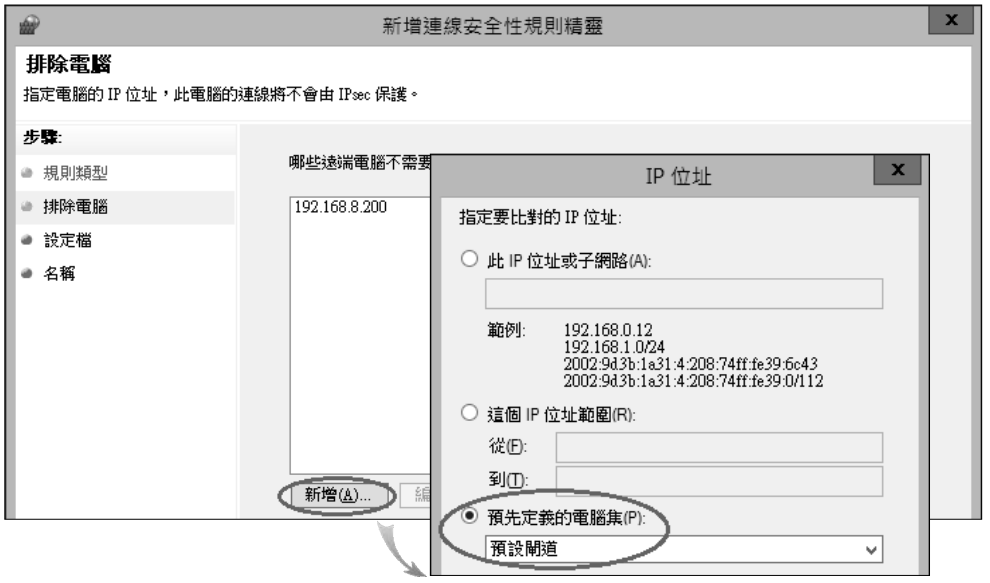

圖 C-4-6

附註

系統內建了一些**電腦集**（computer set）供您直接來選用，例如預設閘道、DHCP 伺服器、WINS 伺服器、DNS 伺服器與本機子網路等。

STEP 8 持續按下一步鈕到**名稱**畫面時為此規則設定一個好記的名稱，例如**排除網域控制站與預設閘道**。按完成鈕。

STEP 9 雙擊圖 C-4-7 中剛才所建立的排除規則。

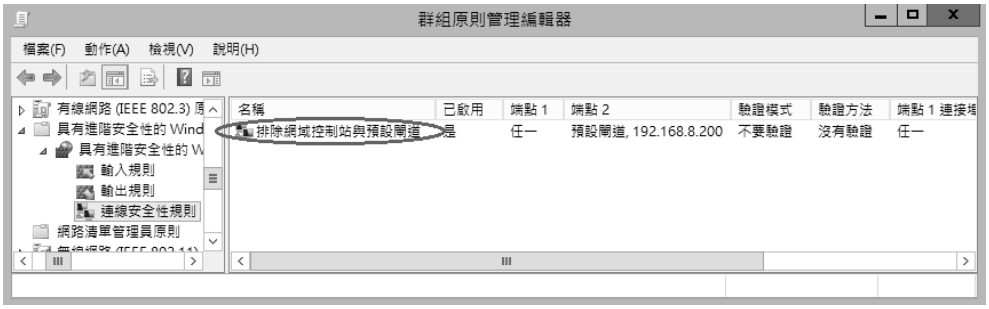

圖 C-4-7

STEP 10 在圖 C-4-8 中點擊**遠端電腦**標籤➲點選**端點 1** 處的**這些 IP 位址**➲透過按 新增 鈕來新增圖中的 IP 位址 192.168.8.0/24。此圖表示**端點 1** 處 192.168.8.0/24 子網路內的所有電腦與**端點 2** 處的預設閘道、192.168.8.200 之間相互溝通時不需要使用 IPsec。

圖 C-4-8

STEP 11 等網域成員電腦自動或手動套用群組原則設定後再繼續下一個步驟。若要手動套用的話，請直接到 DC1、Server1 與 Server2 上執行 **gpupdate /force** 指令，然後分別在這 3 台伺服器上透過【按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲連線安全性規則】來查看是否已經套用成功，若成功的話，該規則就會如圖 C-4-9 所示顯示在畫面上。請務必確認這 3 台電腦都成功的套用此規則後再繼續下一個步驟。

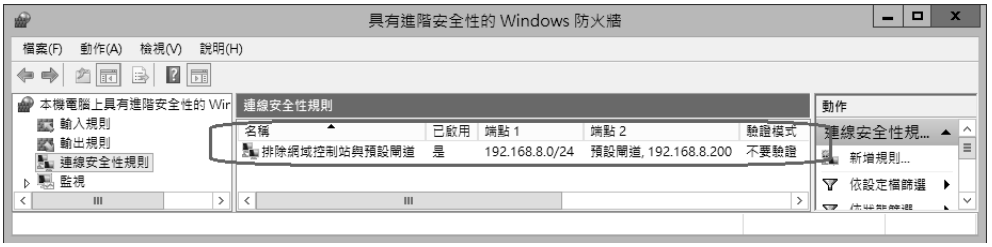

圖 C-4-9

STEP 12 接下來將建立一個要求網域成員之間需 IPsec 的規則。請繼續在 DC1 編輯群組原則：如圖 C-4-10 所示【對著**連線安全性規則**按右鍵➲新增規則】。

圖 C-4-10

STEP 13 在圖 C-4-11 中選擇**伺服器對伺服器**後按下一步鈕。

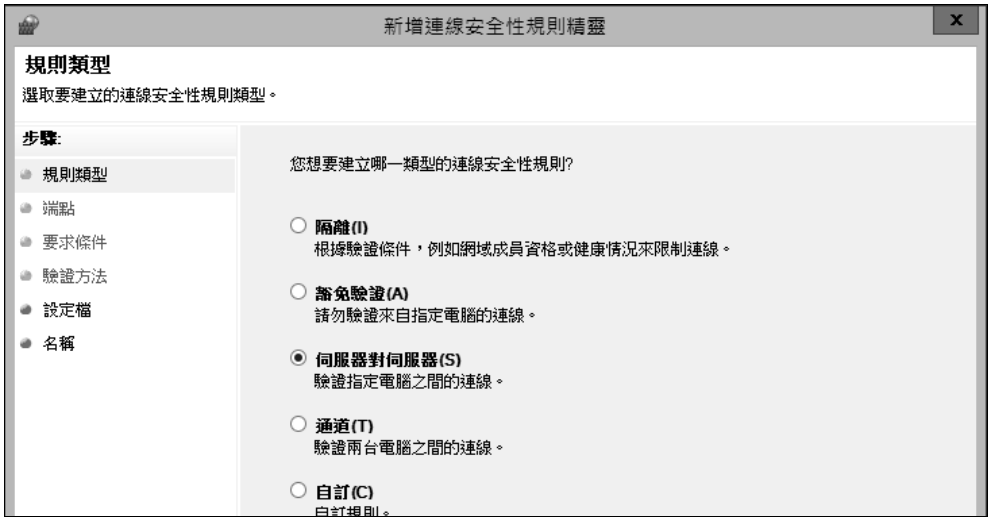

圖 C-4-11

STEP 14 在圖 C-4-12 中透過按新增鈕來設定端點 1 與端點 2 內的 IP 位址範圍，表示端點 1 與端點 2 之間的電腦相互溝通時需 IPsec。此圖為完成設定後的畫面，圖中端點 1 與端點 2 我們都將其設定為 192.168.8.0 這個子網路。

圖 C-4-12

STEP 15 在圖 C-4-13 中選擇**需要對輸入及輸出連線執行驗證**後按下一步鈕。

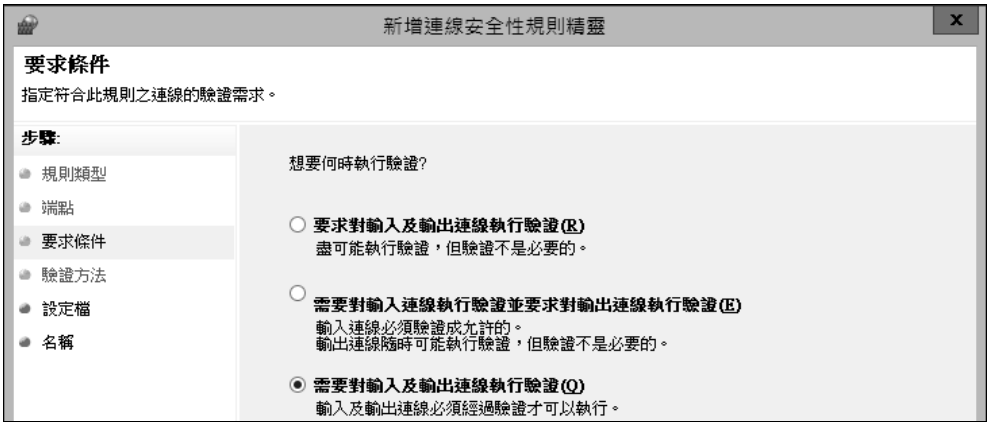

圖 C-4-13

STEP 16 透過圖 C-4-14 中**進階**處的自訂鈕來選擇 Kerberos V5 驗證。

圖 C-4-14

STEP 17 在圖 C-4-15 中按新增鈕➲點選**電腦 (Kerberos V5)**➲按確定鈕。

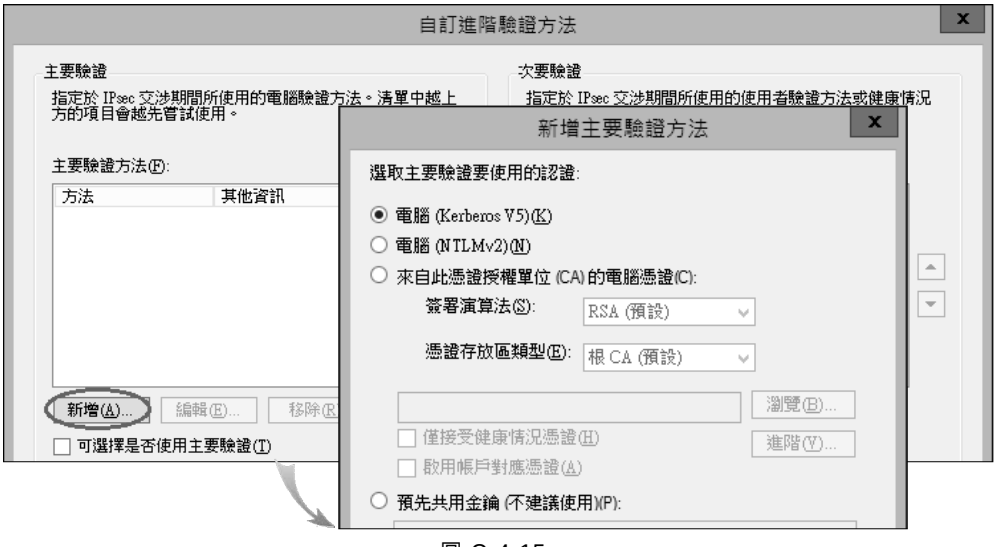

圖 C-4-15

STEP 18 回到圖 C-4-16 的畫面時按確定鈕。

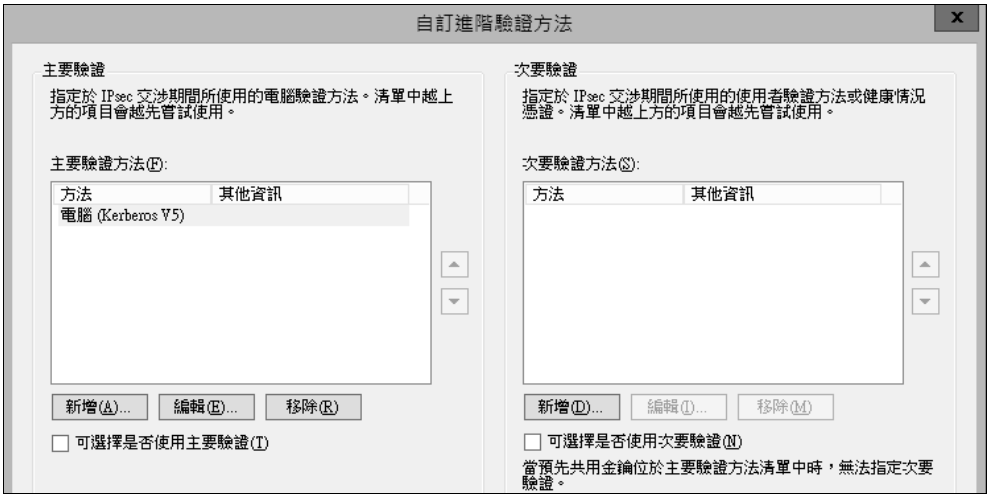

圖 C-4-16

附註

圖中只驗證電腦身分，若您也要驗證使用者身分的話，請透過畫面右方**次要驗證**的新增鈕來增加選擇**使用者（Kerberos V5）**。這樣的話，除了驗證電腦身分之外，還會驗證使用者身分，也就是連接對方時，必須利用網域使用者帳戶來連線，而系統預設會利用使用者登入的帳戶來連線。

STEP 19 持續按下一步鈕到**名稱**畫面時為此規則設定一個好記的名稱，例如**位於 192.168.8.0 的網域成員需驗證**。按完成鈕。

STEP 20 圖 C-4-17 為完成後的畫面。

圖 C-4-17

STEP 21 等網域成員電腦自動套用這個原則設定，或直接到 DC1、Server1 與 Server2 上執行 **gpupdate /force** 指令來手動套用。然後分別在這 3 台伺服器上透過【開啟**具有進階安全性的 Windows 防火牆**➲連線安全性規則】來查看是否已經套用成功（若成功的話，則此時共有 2 個規則會出現）。

注意

若您先建立圖中的**位於 192.168.8.0 的網域成員需驗證**規則，並讓 3 台伺服器套用此規則的話，則之後兩台成員伺服器將無法與網域控制站溝通，因為網域成員無法透過 IPsec 來與網域控制站等基礎結構電腦溝通，因此就算之後您建立了排除規則，Server1 與 Server2 也無法從網域控制站取得與套用這個排除規則。此時您可以先暫時將 Server1、Server2 與網域控制站的 **Windows 防火牆**關閉，以便讓**連線安全性規則**的 IPsec 設定無效，然後在網域控制站上利用 **gpupdate /force** 手動套用，完成後再分別到兩台伺服器上利用 **gpupdate /force** 來手動套用，最後再重新啟用這 3 台電腦的 **Windows 防火牆**。

完成以上所有設定後，請到 Server1（192.168.8.1）利用 ping 指令來測試，請同時開啟 3 個 **Windows PowerShell** 或**命令提示字元**視窗，然後分別執行以下 3 個指令：Ping 192.168.8.2、Ping 192.168.8.200 與 Ping 192.168.8.254。

由於我們已經開放所有伺服器的 ICMP 連入流量，因此應該 3 個連線測試都會成功收到對方的回應。接著請在 Server1 上【按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲監視➲安全性關連➲**主要模式**或**快速模式** SA】，從圖 C-4-18 可知 Server1（192.168.8.1）與 Server2（192.168.8.2）之間已經成功的建立了**主要模式 SA**，也就是透過 IPsec 在溝通。

圖 C-4-18

圖中為何沒有看到 Server1 與網域控制站、預設閘道之間的 IPsec 連線呢？因為 Server1 與網域控制站（192.168.8.200）、預設閘道（192.168.8.254）之間的溝通並不需要 IPsec（透過排除規則）。

C-5 採用電腦憑證的 IPsec 設定

我們將透過圖 C-5-1 來說明如何讓圖中兩台伺服器利用 IPsec 來安全的溝通，並且採用電腦憑證的驗證方式。圖中 3 台伺服器為 Windows Server 2012 獨立伺服器或成員伺服器皆可，其中 CA 是用來發放電腦憑證的伺服器，假設其為獨立 CA。請依照圖指示設定 3 台電腦的 IP 位址與子網路遮罩。本節將僅列出重點說明，其中與憑證申請有關的步驟，有需要的話，請參考第 5 章。

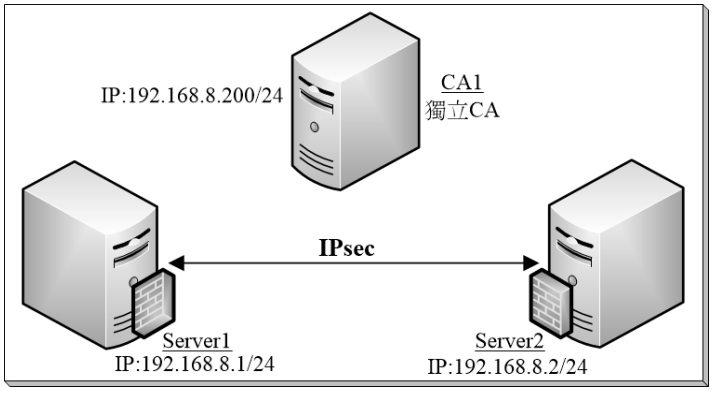

圖 C-5-1

- 請分別在 Server1 與 Server2 上開放 ICMP 的相關流量：【按⊞鍵切換到**開始**選單➲系統管理工具➲具有進階安全性的 Windows 防火牆➲點擊**輸入規則**中的**檔案及印表機共用（回應要求 – ICMPv4-In）**➲點擊右邊的**啟用規則**】。
- 到 Server1 上執行 ping 192.168.8.2、到 Server2 上執行 ping 192.168.8.1，以便測試雙方是否能夠正常溝通。
- 到 CA 電腦上安裝 **Active Directory 憑證服務**角色：【開啟**伺服器管理員**➲點擊**儀表版**處的**新增角色及功能**➲持續按 下一步 鈕一直到出現**選取伺服器角色**畫面時勾選 **Active Directory 憑證服務**➲…➲在**選取角色服務**畫面上增加勾選**憑證授權單位網頁註冊**➲…➲點擊完成安裝畫面中的**設定目的地伺服器上的 Active Directory 憑證服務**➲…】。

- 到 Server1 電腦上申請電腦憑證、安裝此憑證。

  在 Windows Server 2012 電腦上利用瀏覽器向 CA 網站申請電腦憑證時需要利用以下兩種方式之一：

  - 利用 https 方式來連接 CA 網站，但需將 CA 網站加入到**信任的網站**。
  - 利用 http 方式來連接 CA 網站，但請暫時將 Internet Explorer 的**近端內部網路**的安全性等級降為**低**等級，同時將 CA 網站加入到**近端內部網路**。

  其中第 1 種方法的 CA 網站必須申請與安裝 SSL 憑證，比較麻煩，故此處我們採用第 2 種方法來替 Sever1 申請電腦憑證。

  - 先利用 **http://192.168.8.200/certsrv/**來信任 CA（將 CA 憑證安裝到 Server1）。若是企業 CA 的話，因為網域成員會自動信任企業 CA，故網域成員可免除此步驟。信任 CA 的步驟請參考章節 5-2 的說明。
  - 將 Internet Explorer 的**近端內部網路**的安全性等級降為**低**等級，同時也將 CA 網站加入到**近端內部網路**：【開啟 Internet Explorer➲按一下 Alt 鍵➲**工具**功能表➲網際網路選項➲**安全性**標籤➲點擊**近端內部網路**➲將安全等級降為**低**➲點擊右上方網站鈕➲按進階鈕➲將 CA 網站 http://192.168.8.200/加入此區域後按關閉鈕、按 2 次確定鈕】。
  - 執行 Internet Explorer，然後利用 **http://192.168.8.200/certsrv/**來向 CA 申請憑證：【要求憑證➲進階憑證要求➲向這個 CA 建立並提交一個要求➲如圖 C-5-2 所示在**需要的憑證類型處**選擇**用戶端驗證憑證**➲勾選**將金鑰標示成可匯出**➲按提交鈕】（若是企業 CA 的話，請在**憑證範本**處選擇**系統管理員**，並可直接下載與安裝憑證檔案，因此請跳過以下兩個步驟）。

注意

我們需將所申請的憑證儲存到**本機電腦憑證存放區**，然而利用 Internet Explorer 向 Windows Server 2012 CA 申請憑證時，畫面中並沒有**將憑證存放在本機電腦憑證存放區**的選項，因此所申請的憑證會被儲存到**使用者憑證存放區**。我們將透過以下方法來解決此問題：先將此憑證從**使用者憑證存放區**匯出、再將其匯入到**本機電腦憑證存放區**。

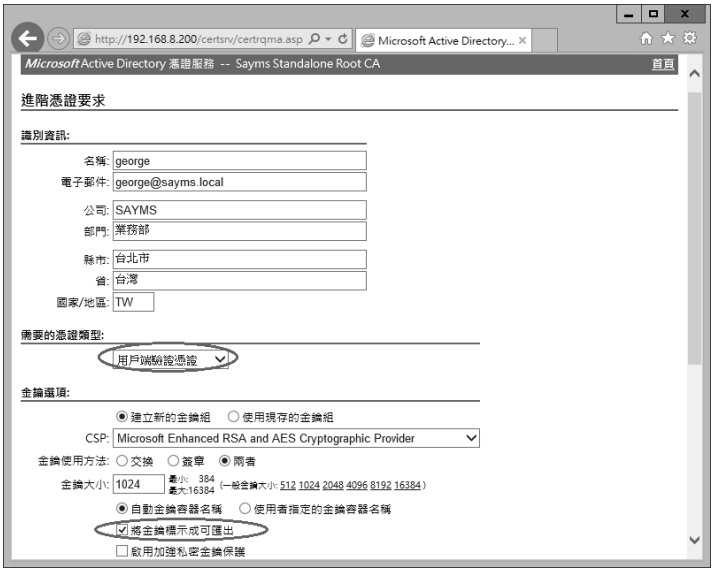

圖 C-5-2

- 到 CA 電腦上【按⊞鍵切換到**開始**選單➲系統管理工具➲憑證授權單位➲擱置要求➲對著憑證要求按右鍵➲所有工作➲發行】來發放憑證。
- 到 Server1 下載與安裝憑證：在 IE 內輸入 **http://192.168.8.200/certsrv/**➲檢視擱置的憑證要求狀態➲…➲安裝這個憑證。
- 按⊞+ R 鍵➲輸入 **MMC** 後按 Enter 鍵➲**檔案**功能表➲新增/移除嵌入式管理單元➲從**可用的嵌入式管理單元**清單中選擇**憑證**後按新增鈕➲點選**我的使用者帳戶**後按完成鈕➲重新從**可用的嵌入式管理單元**清單中選擇**憑證**後按新增鈕➲改選**電腦帳戶**後按下一步鈕、完成鈕與確定鈕。
- 透過【如圖 C-5-3 所示展開**憑證 – 目前的使用者**➲個人➲憑證➲對著之前安裝的憑證按右鍵➲所有工作➲匯出➲按下一步鈕➲點選**是，匯出私密金鑰**後按 2 次下一步鈕➲設定密碼➲…】的途徑將憑證匯出存檔。

圖 C-5-3

■ 透過如圖 C-5-4 所示【展開**憑證（本機電腦）**➲對著**個人**按右鍵➲所有工作➲匯入➲…】的途徑將之前匯出的憑證匯入。

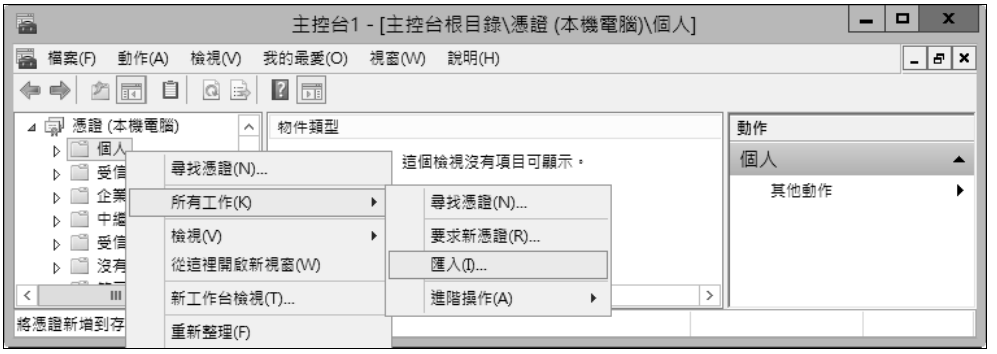

圖 C-5-4

■ 將 Internet Explorer 的**近端內部網路**的安全性等級恢復為**中低**等級。

↘ 在 Server1 上透過**具有進階安全性的 Windows 防火牆**來建立**連線安全性規則**：【在**規則類型**畫面中選擇**隔離**➲在**要求條件**畫面中選擇**需要對輸入及輸出連線執行驗證**➲在圖 C-5-5 的**驗證方法**畫面中點擊**進階**處的自訂鈕➲點擊**主要驗證方法**處的新增鈕➲在圖 C-5-6 中透過瀏覽鈕來選擇發放電腦憑證的 CA➲…】。

圖 C-5-5

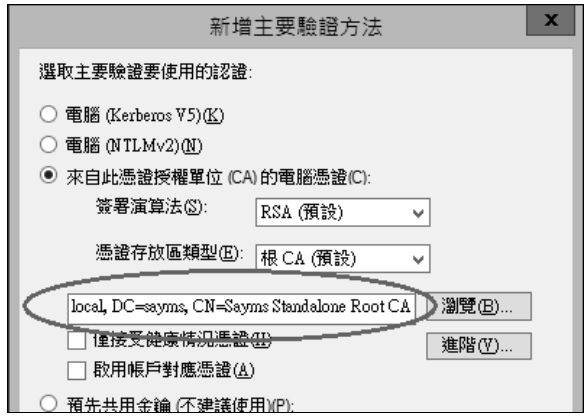

圖 C-5-6

- 由於所建立的規則要求無論輸入或輸出連線都必須採用 IPsec，然而目前 Server2 尚未建立**連線安全性規則**，也就是尚未啟用 IPsec，故此時若在 Server1 上利用 ping 指令來與 Server2 溝通的話，此連線會被 Server1 拒絕。
- 到 Server2 電腦上重複上述步驟：申請電腦憑證、安裝此憑證、透過**具有進階安全性的 Windows 防火牆**來建立**連線安全性規則**。
- 在兩台伺服器上利用 ping 指令來測試，此時雙方應該可透過 IPsec 來相互溝通。圖 C-5-7 為其所建立的**主要模式 SA**，其驗證方法為**電腦憑證**。

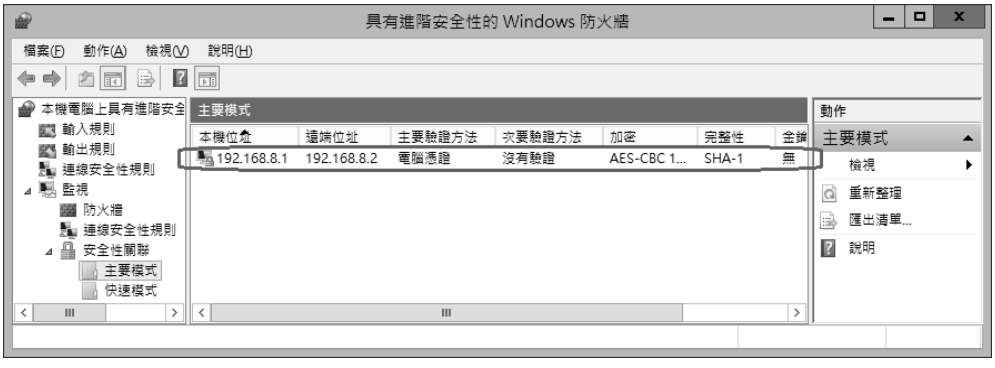

圖 C-5-7

C-6 IPsec 跨越 NAT 的問題

NAT（Network Address Translation，見第 8 章）讓位於內部網路的多台電腦只需要共用一個 public IP 位址，就可以連接網際網路、瀏覽網頁與收發電子郵件等，可是若同時採用 IPsec 來確保資料傳送安全性的話，就可能會有問題產生，因為 NAT 會改變封包的 header，然而 IPsec 卻不允許其封包內的 header 被修改：

- **AH 傳輸模式與 AH 通道模式**：無論是 AH 傳輸模式或 AH 通道模式，IPsec 都會將整個封包簽署（見前面的圖 C-1-4），也就是不允許修改封包內的任何資料，因此 NAT 變更封包內的 IP 位址或 TCP/UDP 連接埠號碼後，IPsec 會將此封包視為無效封包。

- **ESP 傳輸模式與 ESP 通道模式**：ESP 傳輸模式的 Original IP header（見前面的圖 C-1-5），或 ESP 通道模式的 New Tunnel Header 都還是保留原狀，並沒有被 IPsec 簽署或加密，但是 TCP/UDP 連接埠號碼卻被加密無法讀取，因此雖然 NAT 可以變更在傳輸模式中的用戶端 IP 位址、或是通道模式中的端點（end-point）電腦的 IP 位址，但 NAT 卻無法變更連接埠號碼，更可況連接埠號碼還被簽章，不允許變更。

NAT-T（NAT-Traversal）可以解決 IPsec 無法跨越 NAT 的問題，Windows Server 2012、Windows Server 2008（R2）、Windows 8、Windows 7、Windows Vista 與 Windows XP SP2 等系統都有支援 NAT-T。若要讓 IPsec 封包能夠跨越 NAT 的話，請採用 ESP 通訊協定，因為支援 NAT-T 的 IPsec 主機會自動偵測到 NAT 的存在，並將 IPsec ESP 封包，封裝（Encapsulate）到 UDP Header 內（UDP 連接埠為 500），如圖 C-6-1 所示（以 ESP 通道模式為例）。圖中 ESP Header 被封裝到 UDP Header 內，封包內的 Original Tunnel Header 與 UDP Header 都沒有被加密與簽署，因此 NAT 可以變更其 IP 位址與 UDP 連接埠號碼。利用 IPsec 溝通的兩端電腦都必須支援 NAT-T。

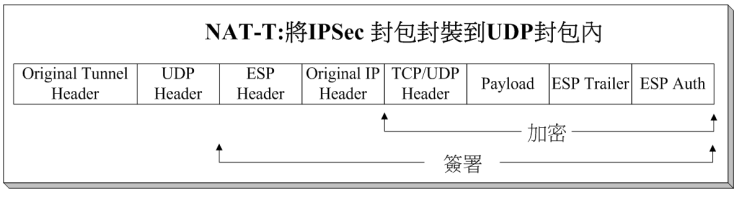

圖 C-6-1