# 『推動 IPv4/IPv6 雙軌普行方案』

# 附錄九
# 『ICP IPv4/IPv6 平台架構雙協定升級輔導手冊』

# ICP IPv4/IPv6 平台架構雙協定
# 升級輔導手冊

# 目　錄

# 圖 次

# 表 次

# 第一章 前言

IPv4/IPv6 雙軌運作又稱為 Dual Stack 或者雙協定化，可以達到相關設備及軟體具備 IPv4 和 IPv6 同時運作的能力。

讓 IPv4 跟 IPv6 同時並存的好處是可以同時服務兩種不同的 IP 位址用戶，同時也是一種從 IPv4 過渡到 IPv6 的可行方式。需要雙軌並存的原因在於同時服務 IPv4 跟 IPv6 的客戶，也可以視為未來完全支援 IPv6 的前置準備。當網站同時支援 IPv4/IPv6 時，可以服務最多的使用者，另外銜接未來的 5G 應用、物聯網等各種應用，會為網站帶來更多商機。對網站業者是言，建置 IPv4/IPv6 雙軌服務，也等於提前準備未來趨勢的變化。

網站提供 IPv4/IPv6 雙軌運作有助於：

1.涵蓋到最大範圍的使用者

2.提前準備以因應物聯網、5G 應用的合作商機

# 第二章 輔導流程

## 第一節 本篇概述

一個 IPv6 的網站導入流程可分成三個階段，在規劃導入階段，任務小組需要先針對網站現況進行評估才規劃導入方案，考慮範圍，依據網站實際現況進行評估，並協同廠商共同完成。任務小組可以參考 RFC 6883 [17]的建議來規劃導入 IPv6 方案。


圖 1 IPv6 導入工作流程

對於要支援 IPv4/IPv6 的 ICP 業者而言，我們的目標是讓 IPv6 早期用戶提早使用 IPv6 服務，同時這些 IPv6 用戶經驗可以用來改善 IPv6 導入計畫。以這種方式導入 IPv6，對於某些後台完全不接觸到訪客的主機，是可以只用 IPv4 而不用 IPv6 也不會影響整個網站對外運作的。

網站導入流程工作項目可以參考下表輔導流程工作項目清單範例，ICP 網站使用時，可依照自行需求調整，各工作項目的細節會在後面詳細說明。

表 1 輔導流程工作項目清單範例

| 編號 | 工作項目 | 完成進度 | 備註 |
|---|---|---|---|
| 1-1 | 建立負責單位，確認參與人員 | | |
| 1-2 | 進行人員訓練，建立 IPv6 種子團隊 | | |
| 2-1 | 網路架構圖、軟硬體設備盤點 | | |
| 2-2 | 網站系統盤點 | | |
| 2-3 | 支援 IPv6 所需的工作項目 | | |

| | | | |
|---|---|---|---|
| 3-1 | IPv6 導入計畫書 | | |
| 4-1 | 建立測試環境，分階段導入 | | |
| 5-1 | 進行軟硬體採購升級 | | |
| 5-2 | IPv6 之升級設定工作 | | |
| 5-3 | 進行功能測試 | | |
| 6-1 | 記錄升級過程含問題排除等資料 | | |

第二節 規劃 IPv6 導入方案

一、人員準備

（一）建立負責單位，確認參與人員（編號 1-1）

表 2 IPv6 參與人員表範例

| 負責類別 | 姓名 | 所屬機關及單位 | 職稱 |
|---|---|---|---|
| IPv6 網路督導主管 | | 總經理 | 總經理 |
| IPv6 網路升級業管主管 | | 資訊部 | 主任 |
| 網路負責人員 | | 資訊部 | 工程師 |

並建議輔導過程需要以下角色參與，參考下表輔導團隊的角色說明，並視情況指派所需的角色與人員並填寫至上述 IPv6 參與人員表。

表 3 輔導團隊的角色說明範例

| 編號 | 角色 | 工作內容 | 雲端 | 自有主機 |
|---|---|---|---|---|
| 1 | 機房工程師 | 設定網路設備如路由器、交換機、防火牆，須熟悉各種硬體設備的操作與設定 | 不需要 | 必要 |
| 2 | 雲端工程師 | 設定雲端服務，須熟悉雲端服務的設定與操作 | 必要 | 不需要 |
| 3 | 系統工程師 | 設定作業系統、網頁伺服器 | 必要 | 必要 |
| 4 | 資料庫工程師 | 設定資料庫欄位 | 必要 | 必要 |
| 5 | 前端工程師 | 處理前端頁面技術 | 必要 | 必要 |
| 6 | 後端工程師 | 處理後端程式碼，包括商業邏輯、系統串接，需要熟悉被輔導 ICP 廠商的程式語言 | 必要 | 必要 |
| 7 | 品質測試工 | 負責網站整體測試 | 必要 | 必要 |

| | | | | |
|---|---|---|---|---|
| | 程師 | | | |
| 8 | 安全工程師 | 負責檢測網路安全 | 必要 | 必要 |
| 9 | 專案經理 | 負責控管專案進度、時程與人力 | 必要 | 必要 |
| 10 | 技術經理 | 負責技術團隊的進度掌控 | 必要 | 必要 |

（二）進行人員訓練，建立 IPv6 種子團隊（編號 1-2）

IPv4/IPv6 課程可以分為四大項，包括 Pv4/IPv6 網路規劃、IPv4/IPv6 網路管理、IPv4/IPv6 伺服器管理、IPv4/IPv6 程式開發。導入團隊需要了解 IPv4/IPv6 觀念， IPv6 位址的組成結構、IPv6 位址設定及管理方法等。

二、網路環境及網站相關系統的清查

（一）網路架構圖、軟硬體設備盤點 （編號 2-1）

1.清查目前 IPv4 網路架構圖（*由 ICP 業者自行提供或協助）

2.清查目前網路相關軟硬體設備

表 4 軟硬體設備盤點表範例

| 序號 | 軟硬體資產編號 | 軟硬體類別 | 硬體廠牌型號或軟體供應商 | 作業系統/軟體版本 | 距離報廢年限 | 是否已經具備 IPv6 功能 | 是否已經啟動 IPv6 功能 | 硬體升級方式 | 軟體升級方式 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | 路由器 | | | | | | | |
| 2 | | 防火牆 | | | | | | | |
| 3 | | 負載平衡器 | | | | | | | |
| 4 | | Web 伺服器主機 | | | | | | | |
| 5 | | Web 伺 | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 服器軟體 | | | | | | | |
| 6 | | DNS 伺服器主機 | | | | | | | |
| 7 | | DNS 伺服器軟體 | | | | | | | |
| 8 | | Mail Server | | | | | | | |

（二）網站系統盤點（區分自行開發、委外設計、購買的商業軟體、開源的軟體）（編號 2-2）

表 5 網站系統盤點表範例

| | 服務系統名稱 | 服務內容說明 | 主機放置位置 | 主機數量 | 系統類型 | 主/次要服務 |
|---|---|---|---|---|---|---|
| 1 | 前端操作介面 | | | | | |
| 2 | 金流系統 | | | | | |
| 3 | 物流系統 | | | | | |
| 4 | 會員系統 | | | | | |
| 5 | 搜尋系統 | | | | | |
| 6 | 後台管理系統 | | | | | |

（三）支援 IPv6 所需的工作項目（採購設備/升級設備/請求雲端主機商支援/購買新軟體）（編號 2-3）

將各類設備依升級方式進行統計，並計入於下表之各類設備數量表。

表 6 各類設備數量表範例

| | | | 硬體升級統計 | | | | | | 軟體升級統計 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 編號 | 軟硬體設備類型 | 預計升級階段 | 軟硬體設備數量 | 整台更換 | 部分組件更換 | 不再使用此設備 | 使用Proxy方案 | 其他技術 | 軟體升級 | 更換軟體 | 改寫軟體/網頁 | 軟體升級/改寫網頁 | 使用Proxy方案 | 其他技術 |
| 1 | 路由器 | | | | | | | | | | | | | |
| 2 | 防火牆 | | | | | | | | | | | | | |
| 3 | 負載平衡器 | | | | | | | | | | | | | |
| 4 | 網頁伺服器 | | | | | | | | | | | | | |
| 5 | 網域名稱伺服器 | | | | | | | | | | | | | |
| 6 | 電 | | | | | | | | | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 子郵件伺服器 | | | | | | | | | | | | |

三、IPv6 導入計畫書範例

（一）包括網路架構、時程規劃、人力配置、經費配置、軟硬體採購列表、IPv6 位置分配表、評估服務中斷風險、異常撤退方案。（編號 3-1）

建立於 IPv6 下預計的網路架構圖，可參考下圖常見的基本網站架構圖。

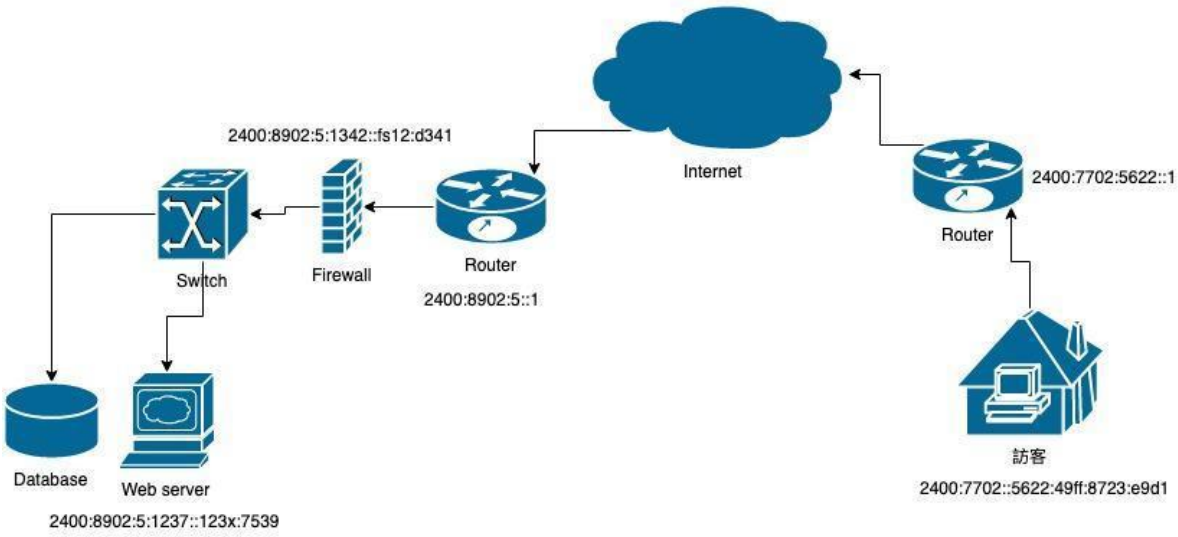



圖 2 IPv6 網站架構圖

表 7 時程規劃表

| xxxx 年 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 | 月份 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPv6 網路升級<br>清查 | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IPv6 網路技術教育訓練 | | | | | | | | | | | | |
| 升級作業規劃 | | | | | | | | | | | | |
| IPv6 網路升級試驗 | | | | | | | | | | | | |
| 主要網站服務升級 | | | | | | | | | | | | |

依時程計畫表進行人員與資源的配置，並預估作業時間，接著再分配工作給執行人員。

表 8 人員任務分配表範例

| 編號 | 交付項目 | 負責人員 | 起始日期 | 結束日期 |
|---|---|---|---|---|
| 1 | 網路設備設定支援 IPv4/IPv6 | | | |
| 2 | 網頁伺服器設定支援 IPv4/IPv6 | | | |
| 3 | DNS 設定支援 IPv4/IPv6 | | | |
| 4 | Mail Server 設定支援 IPv4/IPv6 | | | |

升級過程所需角色以及各任務內容，請參考下面表格說明，並視情況填寫至上述人員任務分配表。

表 9 輔導程序、任務與角色範例

| 編號 | 項目 | 主要內容 | 參與角色 |
|---|---|---|---|
| 1 | 溝通目標 | 溝通本次導入 IPv6 之後，雙方的目標及效益 | 專案經理 |
| 2 | 人力資源 | 確定本次輔導雙方分別需要派出具備哪些能力的人員參與本次輔導過程 | 專案經理<br>技術經理 |
| 3 | 時程 | 預估專案時程 | 專案經理 |

| | | | |
|---|---|---|---|
| | | | 技術經理 |
| 4 | 網路架構 | 請被輔導的 ICP 提供使用的網路設備及服務 | 專案經理<br>技術經理 |
| 5 | 現況盤點 | 被輔導 ICP 列出網站相關主機、程式碼、資料庫、合作廠商、服務 | 專案經理<br>技術經理 |
| 6 | DNS | 設定 DNS | 系統工程師 |
| 7 | Mail Server | 設定 Mail Server | 系統工程師 |
| 8 | 網路設備 | 設定 Firewall、Router 及 Load Balance | 網路工程師 |
| 9 | 雲端服務 | 設定雲端系統 | 雲端工程師 |
| 10 | 作業系統 | 設定作業系統 | 系統工程師 |
| 11 | 網頁伺服器 | 設定網頁伺服器 | 系統工程師 |
| 12 | 資料庫 | 檢查資料庫及程式碼是否有需要調整 | 資料庫工程師 |
| 13 | 程式碼 | 檢查程式碼是否需要調整 | 前端工程師<br>後端工程師 |
| 14 | 網路安全 | 測試網站安全項目 | 安全工程師 |
| 15 | 網站整體測試 | 測試網站所有功能，看是否可以正常運作 | 測試工程師 |

統計 IPv4/IPv6 雙協定下所需的相關經費，例如軟硬體設備購置費用等，內容可參考下表經費配置表。

表 10 經費配置表範例

| 經費描述 | 單價 | 數量 | 合計 |
|---|---|---|---|
| 人事費用 | | | |
| 軟硬體設備 | | | |
| 總計 | | | |

接續前述統計的各類設備數量表，並將需採購的軟硬體填寫至下表軟硬體採購列表，其內容亦可以跟經費分配表內的軟硬體設備相關項目金額核對。

表 11 軟硬體採購列表範例

| 設備編號 | 品名 | 建議升級階段 | 設備採購參考規格或說明 | 經費預估 | 備註說明 |
|---|---|---|---|---|---|
| | 防火牆 | | 支援 IPv6 之防火牆 | xxxxx | |
| | 路由器 | | 支援 IPv6 之路由器 | xxxxx | |
| | 負載平衡器 | | | xxxxx | |
| | 網頁伺服器 | | | | |
| | 合計 | | | xxxxx | |

針對各服務主機其正式機及測試機分配預定的 IPv6 位址網段，參考下表為 IPv6 位址網段規劃表。

表 12 IPv6 位址網段規劃表範例

| 子網路 | IPv6 address |
|---|---|
| 測試機（Web Server） | 2001:xxxx:xxxx:xx |
| 測試機（Mail Server） | 2001:xxxx:xxxx:xx |
| 測試機（Database Server） | 2001:xxxx:xxxx:xx |
| 正式機（Web Server） | 2001:xxxx:xxxx:xx |
| 正式機（Mail Server） | 2001:xxxx:xxxx:xx |
| 正式機（Database Server） | 2001:xxxx:xxxx:xx |

針對各設備紀錄其分配預定的 IPv6 位址及目前之 IPv4 位址，參考下表 IPv6 位址分配規劃表。

表 13 IPv6 位址分配規劃表範例

| 資產編號 | 設備名稱 | IPv4 位址 | IPv6 位址 |
|---|---|---|---|
| | 路由器 | | |
| | 負載平衡器 | | |

| | | | |
|---|---|---|---|
| | 防火牆 | | |
| | 第三層交換器 | | |
| | DNS | | |
| | 網站 | | |
| | Mail Server | | |

各服務系統分別以純 IPv4 網路、純 IPv6 環境以及 IPv4/IPv6 雙協定環境進行測試，規劃其驗證測試方式及異常撤退方案，可參考下表升級測試驗證作業程序表，其測試方式與撤退方案再依實際狀況修訂。

表 14 升級測試驗證作業程序表範例

| 編號 | 服務系統名稱 | 網址 | 驗證測試方式 | 撤退方案 |
|---|---|---|---|---|
| 1 | Web Server | | 1. 網路聯通測試：以用戶端電腦 Ping 主機網址確認無誤（應先確認 Ping 封包不被網路設備阻擋）<br>2. Web 網頁功能測試：使用瀏覽器進行網頁瀏覽，網頁及各項選單、按鈕、子網頁等均可順利開啟，並且無異常破圖缺圖現象 | 1. 如 IPv4/IPv6 雙協定之測試均失敗還原回原本作業系統版本及純 IPv4 之參數設定。<br>2. 如只有 IPv6 測試失敗，則持續修正錯誤之執行步驟或設定 |

四、建立測試環境，分階段導入。（編號 4-1）

測試環境之建置可參考下圖系統環境建置示意圖。

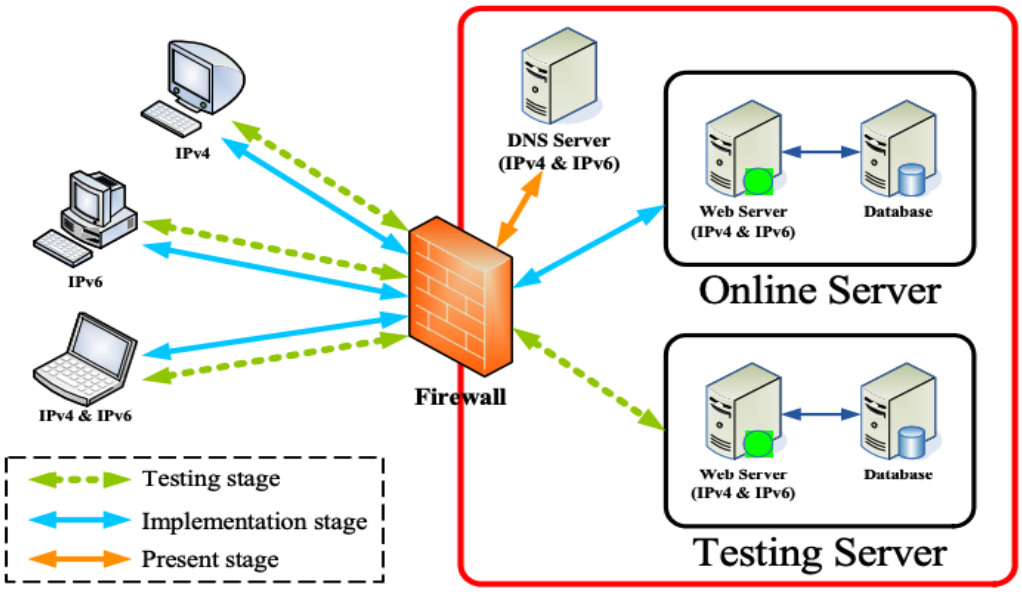



圖 3 系統環境建置示意圖

第三節 執行 IPv6 導入方案

一、進行軟硬體採購升級。（編號 5-1）

延續規劃 IPv6 導入方案內各類設備數量表，依預計升級階段排序軟硬體設備升級之動作，按進度執行其內容並標示其執行進度於下表中。

表 15 軟硬體設備升級進度表範例

| 預計升級階段 | 軟硬體設備類型 | 升級方式（更新/替換） | 是否已完成 |
|---|---|---|---|
| 第一階段 | | | |
| 第二階段 | | | |

二、IPv6 之升級設定工作（編號 5-2）

（一）對一個網站而言，升級 IPv4/IPv6 所需工作包請詳下表之 IPv6 之升級設定項目表，實際設定內容與步驟則可以比對參考章節之欄位說明，進行後續設定。

表 16 IPv6 之升級設定項目表範例

| 編號 | 分類 | 參考章節 | 說明 |
|---|---|---|---|
| 1 | 網路環境 | 第三章 | *Router 設定<br>*Firewall 設定<br>*IPv6 位址取得<br>*Load Balance 設定<br>**AWS 設定<br>**Linode 設定<br>DNS 設定 |
| 2 | 作業系統 | 第四章 | Windows Server 設定<br>CentOS Linux 設定<br>Ubuntu Linux 設定 |
| 3 | 資料庫 | 第五章 | MySQL 設定 |
| 4 | 網頁伺服器 | 第六章 | IIS 設定<br>Apache 設定<br>Nginx 設定 |

| | | | |
|---|---|---|---|
| 5 | 程式檢查 | 第七章 | PHP 設定<br>ASP.NET（C#）設定<br>Python 設定<br>Java 設定<br>Javascript 設定 |

備註：

1.上表中有打*號的對於使用 AWS、Google Cloud Platform 或者 Microsoft Azure 通常不需要設定

2.上表中有打**號的對於使用 AWS、Google Cloud Platform 或者 Microsoft Azure 等雲端服務才設定

三、進行功能測試。（編號 5-3）

（一）透過外部 IPv6 檢查網站檢驗 web server 是否可以正常運作 https://www.mythic-beasts.com/ipv6/health-check，如果設定正確，所有的檢查項目都應該要 PASS。

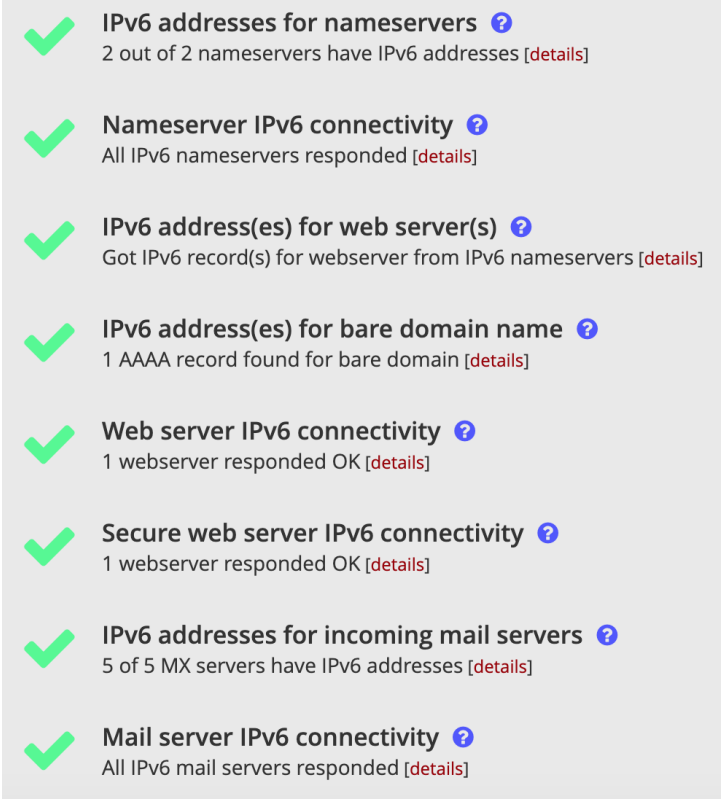



圖 4 IPv6 檢查網站檢驗通過畫面

（二）IPv6 設定檢測項目

除了上述 IPv6 檢查網站，另可參考下表所提供的測試工具，檢測 IPv6 各方面的設定。

表 17 ICP 業者的 IPv6 設定檢測表

| 編號 | 分類 | 設定測試 | 必測與否 | 通過條件 | 測試方式 | 測試工具 |
|---|---|---|---|---|---|---|
| CT-1 | 主機 | 網站的 IPv6 位址可以連上 (http 或 https) | 是 | Trying 顯示 IPv6 位址、出現 TCP_NODELAY set、Connected to Connected to 網址(IPv6 位址) port 443 、並顯示 successfully set certificate verify locations 出現 HTTP/2 200 | curl -v 網址 --head | curl |
| CT-2 | 路由器 | 沿途路由器都有 IPv6 位址 | 是 | 顯示沿途路由器 IPv6 位址 | traceroute6 根網域 | traceroute6 |
| CT-3 | DNS | 網站是否有正確設定 IPv6 位址 | 是 | 顯示 IPv6 位址 | dig aaaa 根網域 @8.8.8.8 +short | dig |
| CT-4 | DNS | 網站使用的所有 DNS Server 本身要有 IPv6 位址 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 | dig |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | +short;<br>done | |
| CT-5 | DNS | 網站使用的 DNS 的 IPv6 都可以 PING 通過 | 是 | 成功顯示 PING 到的 IPv6 位址 | ping6 根網域 | ping6 |
| CT-6 | DNS | 網站使用的 DNS 要設定網站根網域的 IPv6 位址 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short NS 根網域`;<br>do echo -n "$i => [ipv6] ";<br>dig aaaa 根網域 @$i +short;<br>done | dig |
| CT-7 | Mail Server | 網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short MX 根網域`;<br>do echo -n "$i => [ipv6] ";<br>dig aaaa $i @8.8.8.8 +short;<br>done; | dig |

第四節 記錄與後續維護

一、記錄升級過程含問題排除等資料。（編號 6-1）

於升級 IPv4/IPv6 雙協定過程中需記錄升級過程的問題內容與解決方式，以利後續移轉與維護參考，可參考下表問題記錄單。

表 18 問題記錄單範例

| 編號 | 問題內容 | 負責人 | 解決方式 | 是否完成 | 備註 |
|---|---|---|---|---|---|
| 1 | Windows XP 並未支援 IPv6 的 DNS Server（Domain Name System Server）位址的設 定 | | Windows XP 雖然不支援 IPv6 DNS，但是對 圖（三），WinXP 在 Cisco NAT-PT 之 DNS 封包截圖 - - 於 IPv4 DNS 的支援卻是無庸致疑的，因此 我們採用了給予 End Users Private IPv4 Address 的作法，但是僅提供 DNS Server 的 IPv4 Address，與 End Users 本機獨立的 Private IPv4 Address，不提供一個 IPv4 的 Gateway Address，而我們只要另外架設一 個能有 IPv6、IPv4 位址查尋的 DNS ALG Server，我們採用 Totd Version 1.5 來架設這 個 DNS ALG Server。再次強調，End Users 並無 IPv4 | 是 | |

| | | | | | |
|---|---|---|---|---|---|
| | | | 對外連線能力，僅有使用 IPv4 連線能力來查詢 IPv6 DNS Record 的能力。 | | |
| 2 | DNS 負載過重 | | 調整 DNS 伺服器的設定或是更新硬體 | 是 | |

# 第三章 網路環境升級 IPv6

## 第一節 本篇概述

IP 位址是電腦用在網際網路上用來傳遞資料與提供別人辨識主機所在位置的重要依據，就像門牌號碼一樣，只要知道目的地，就可以正確的傳送資料。IPv4 的位址為 32 位元，可以提供約 43 億個位址，但由於使用量大，目前 IPv4 位址已經分配完畢。

如何在 IPv4 位址已經分配完畢的情況下，應付未來包括物聯網、5G 服務等更多的 IP 位址需求，目前提供的解決方法為使用 IPv6。IPv6 是第六版 IP 規範（Internet Protocol version 6）的簡稱，IPv6 使用 128 位元位址空間，可以提供足夠數量的 IP 位址供未來各種服務需求。

在本章內，我們說明路由器、防火牆、分流伺服器如何支援 IPv6 的步驟。另外，針對使用雲端設備的網站業者，我們也提供了 AWS 跟 Linode 對於支援 IPv6 的說明。

表 19 自建與雲端措施差異

| 機房設備 | 建議措施 | 參考手冊 |
|---|---|---|
| 使用自有設備，包括自己採購硬體防火牆、路由器等 | 跟原廠配合，跟原廠在台灣的代理商合作，並參考下面的資料進行升級。 | 不同廠牌、不同版本的設定都會有差異，建議參考原廠的手冊進行設定。 |
| 使用 AWS 、Google Cloud Platform 跟 Microsoft Azure 雲端 | 預設都已經支援，且 ICP 業者不需要接觸硬體設備（實際上也碰不到），故不需自行設定。 | AWS 可參考 https://aws.amazon.com/tw/<br><br>Google Cloud Platform 可參考 https://cloud.google.com/docs/<br><br>Microsoft Azure 請參考 https://docs.microsoft.com/zh- |

| | | |
|---|---|---|
| | | tw/azure/ |

## 第二節 Cisco Router ASR 9000 系列路由器啟用 IPv6 的支援

依據 techspot.com 網站上的統計，市面上有在販售的路由器超過 487 台。由於設備眾多且設定都不一樣，因此我們僅能就取得的 Cisco router ASR 9000 設備提供設定資訊，其他品牌或者型號，請跟保固廠商接洽，尋求正確的設定方式。

進入 Global Configure mode

| 輸入指令 |
| --- |
| #configure terminal |

進入 Interface mode

| 輸入指令 |
| --- |
| （configure）# interface gigabitethernet 0/1/0/2 |

設定 IPv4 IP address 和 mask

| 輸入指令 |
| --- |
| （config-if）# ipv4 address 192.168.1.1 255.255.255.0 |

設定 IPv6 global IP address 和 prefix-length

| 輸入指令 |
| --- |
| （config-if）# ipv6 address 2001:a11:b22:1::1/64 |

設定 IPv6 link-local IP address

| 輸入指令 |
| --- |
| （config-if）# ipv6 address fe80::1 link-local |

啟用 IPv6 服務

| 輸入指令 |
| --- |
| （config-if）# ipv6 enable |

讓設定生效

| 輸入指令 |
| --- |
| （configure）# commit |

## 第三節 FortiGate / FortiOS 6.0.0 Firewall 防火牆啟用 IPv6

根據 Wiki 上的資料，知名的軟體防火牆至少有 34 種品牌，知名的硬體防火牆至少有 48 種品牌，合計超過 82 種品牌。每一種防火牆的軟體或者韌體版本號介於 10-100 個版本，由於版本中之間差異大，設定沒有統一的規範。因此我們僅能就取得的 FortiCate/FortiOS 6.0.0 設備提供設定步驟。如果您的防火牆設備設定方式不同，請跟保固廠商接洽，以獲得正確的設定方式。

列出已經支援 IPv6 Firewall Gateway 產品提供參考。

表 20 IPv6 Firewall Gateway 產品

| 廠商名稱 | 產品 | IPv6 支援版本 |
|---|---|---|
| Check Point | Check Point | Firewall-1 NG R55 以上 |
| Fortinet | FortiGate | FortiOS 3.0 以上 |
| Juniper | Juniper SSG<br>Juniper Netscreen | ScreenOS 5.0 以上 |
| Cisco | Cisco ASA<br>Cisco PIX | Version 7.0 以上 |

一、啟用 IPv6

路徑為： System > Config > Features

二、IPv6 policy routing

路徑為：Network > Policy Routes

Create New > IPv6 Policy Route

Adding an IPv6 Policy route

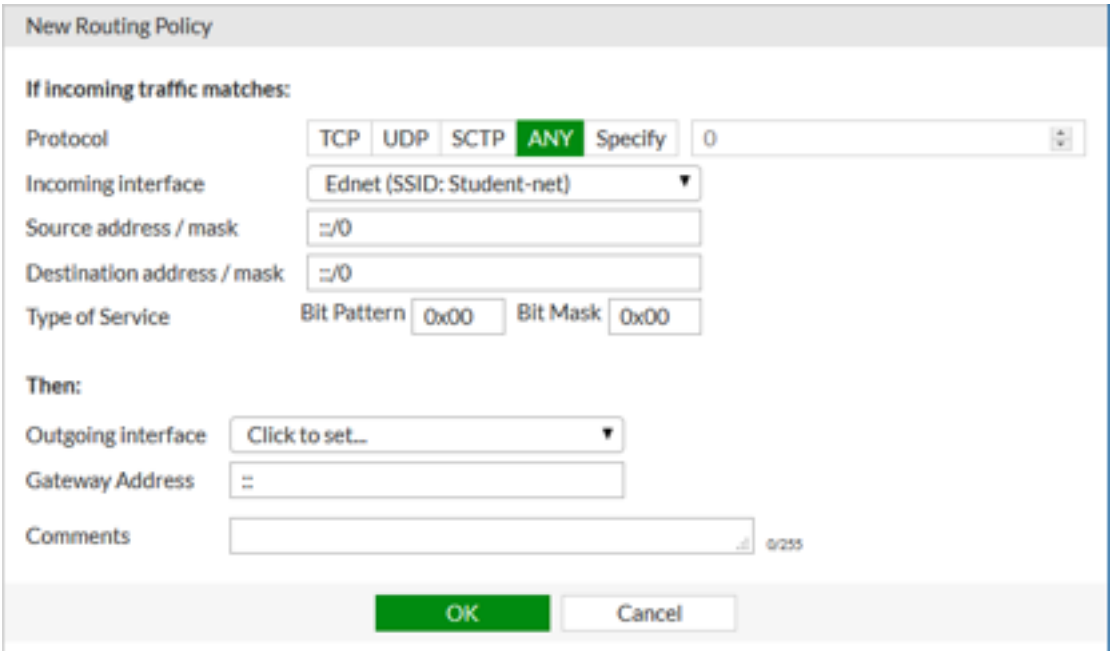



圖 5 IPv6 policy routing

三、DHCPv6-PD 設定

在 upstream 介面（port 10）啟用 Enable DHCPv6 Prefix Delegation

```
config system interface
  edit "port10"
    config ipv6
      set dhcp6-prefix-delegation enable
    end
  end
```

在 downstream 介面（port1）指定 delegated prefix

```
config system interface
  edit "port1"
    config ipv6
      set ip6-mode delegated
      set ip6-upstream-interface "port10"
      set ip6-subnet ::1:0:0:0:1/64
      set ip6-send-adv enable
      config ipv6-delegated-prefix-list
        edit 1
          set upstream-interface "port10"
          set autonomous-flag enable
          set onlink-flag enable
```

```
        set subnet 0:0:0:100::/64
      end
    end
  end
```

四、DHCPv6 server configuration

進行 delegated prefix 設定

```
config system dhcp6 server
  edit 1
    set dns-service delegated
    set interface "wan2"
    set upstream-interface "wan1"
    set ip-mode delegated
    set subnet 0:0:0:102::/64
  end
```

五、DHCPv6 relay

你可以使用以下指令來設定 FortiGate 介面來傳遞 DHCPv6 的查詢跟回覆。

```
config system interface
   edit internal
      config ipv6
         set dhcp6-relay-service enable
         set dhcp6-relay-type regular
         set dhcp6-relay-ip 2001:db8:0:2::30
      end
```

六、Obtaining IPv6 IP addresses from a DHCP server

如果透過命令列，下面指令是讓 wan2 介面取得 IPv6 位址：

```
config system interface
   edit wan2
      config ipv6
         set ip6-mode dhcp
```

```
    end
```

七、DoS 政策

如果設定 DoS（阻斷式攻擊）的政策
設定路徑：Policy & Objects > IPv6 DoS Policy

八、IPv6 forwarding

Policies, IPS, Application Control, flow-based antivirus, web filtering, and DLP

設定路徑：Policy & Objects > IPv6 Policy
Create New to add an IPv6 Security Policy

九、ICMPv6

設定路徑：Policy & Objects > Services > Create New

Enter the following CLI command:

```
config firewall service custom
    edit diagnostic-test1
        set protocol ICMP6
        set icmptype 140
        set icmpcode 0
        set visibility enable
    end
```

## 第四節 PacketX Load Balance 負載平衡伺服器啟用 IPv6

負載平衡伺服器用來分擔網路流量，將流量分散到多台設備，以提高可以服務的客戶連線數及輸出量。以下圖架構說明，我們在路由器上設定一個 mirror port，藉由這個 mirror port 將所有封包都複製一份出來，再交給兩台入侵防禦系統(IDP，Intrusion Detection and Prevention)進行資訊安全分析。

負載平衡伺服器大部分應用在主機跟路由器之間，如果路由器下有 10 台主機，透過路由器的機制，每台主機只要分擔 1/10 的客戶連線，大幅降低主機的負擔。負載平衡有支援多種分散流量的機制，包括依據忙碌狀況分攤流量、依據累積的流量數分攤流量、平均分攤流量、不同主機使用不同權重分攤流量等，例如老舊機器負責較少流量，高規格機器負擔較多流量。

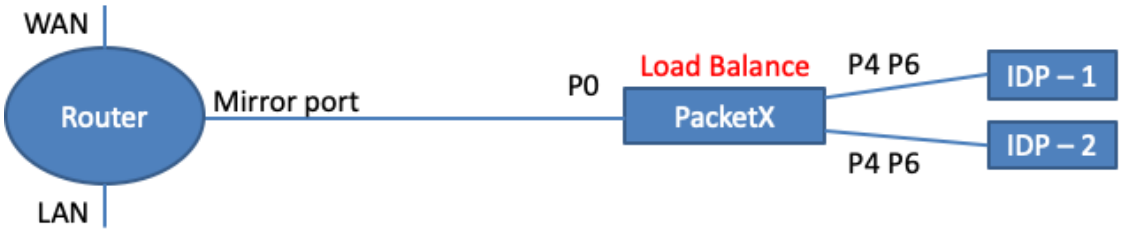



圖 6 Load Balance 設定架構圖

透過負載平衡設定，讓 PacketX 將 Router mirror 的流量（包括 IPv4/IPv6）分別導向兩台 IDP 進行資安分析。這裡用 mirror（映射）是指相同的封包複製一份到另外一個地方。

```
設定指令
<run>
  <chain id="0">
   <in>P0</in>
    <out type="loadBalance">P4,P6</out>
  </chain>
</run>
```

透過負載平衡設定，讓 PacketX 將 Router mirror 的流量（包括 IPv4/IPv6）分別導向兩台 IDP。

```
設定指令
<run>
```

```
   <filter id="100" sessionBase="no">
      <or>
         <find name="ipv6" relation="==" content="" />
      </or>
   </filter>
   <chain id="5">
      <in>V0</in>
      <fid>F100</fid>
      <out>V6</out>
      <next type="notmatch">
         <out>V4</out>
      </next>
   </chain>
</run>
```

## 第五節 Amazon AWS 網路環境啟用 IPv6

Amazon AWS 預設有支援 IPv6，但防火牆預設是禁止連入 IPv6 封包進入。以下步驟讓 IPv6 的封包可以進入網段內。

1.建立 IPv6 CIDR block（VPC 虛擬私人網路跟子網路）
2.更新路由表
3.將 IPv6 指派給實例(instance，一個 instance 可以代表一台線上虛擬主機)
4.更新安全防護規則(設定要開啟的 port、可允許連線的外部 IP、可允許連線的協定 TCP 或 UDP)

備註：由於 AWS 的硬體資源都是共用的，由一個網頁介面去管理，而在 AWS 上，每建立一台新的 Web Server 都稱為一個 instance（實例）

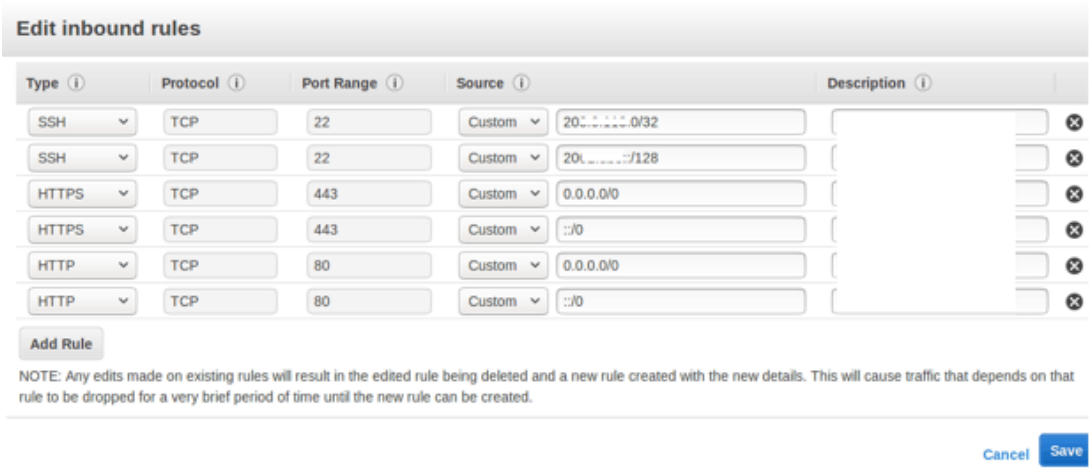



圖 7 Amazon AWS 上的設定 IPv4 跟 IPv6 都在同一個介面

第六節 Linode 的網路環境啟用 IPv6

Linode 預設有啟用 IPv6，故每一個 Linode instance 都會自動配置一個 IPv4 跟一個 IPv6 位址，不需要額外購買或者設定，只要主機啟動之後，就會自動取得。

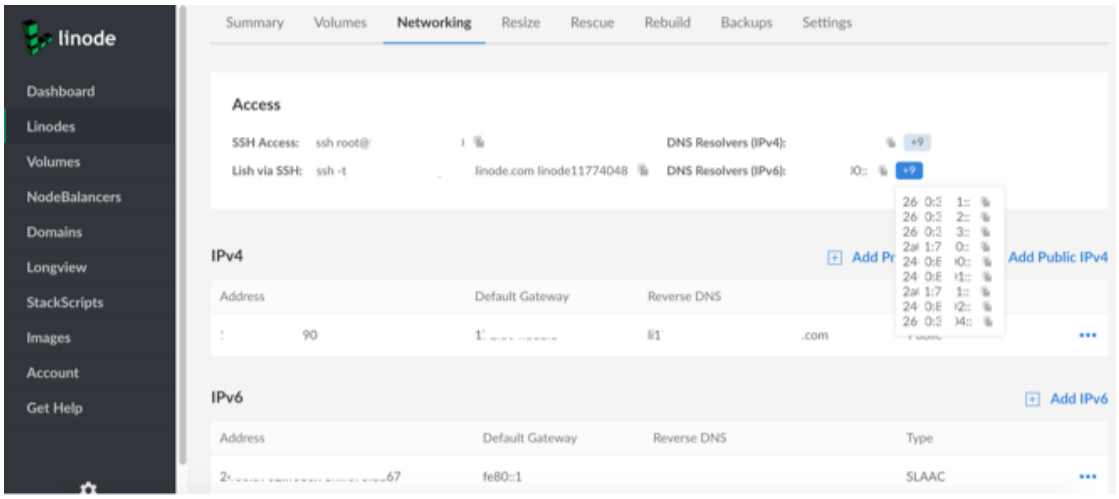



圖 8 Linode 的 ACL 設定畫面

## 第七節 DNS 連線啟用 IPv6

大部分網站業者使用在購買網域時，都會使用網域銷售平台的管理工具，用來管理網站的網址設定。目前全球最大的網域銷售網站為 GoDaddy.com，下面以 GoDaddy.com 的管理介面為範例，說明如何新增一筆 IPv6 的設定。於類型部分選擇 AAAA，並輸入要指向的 IPv6 位址。

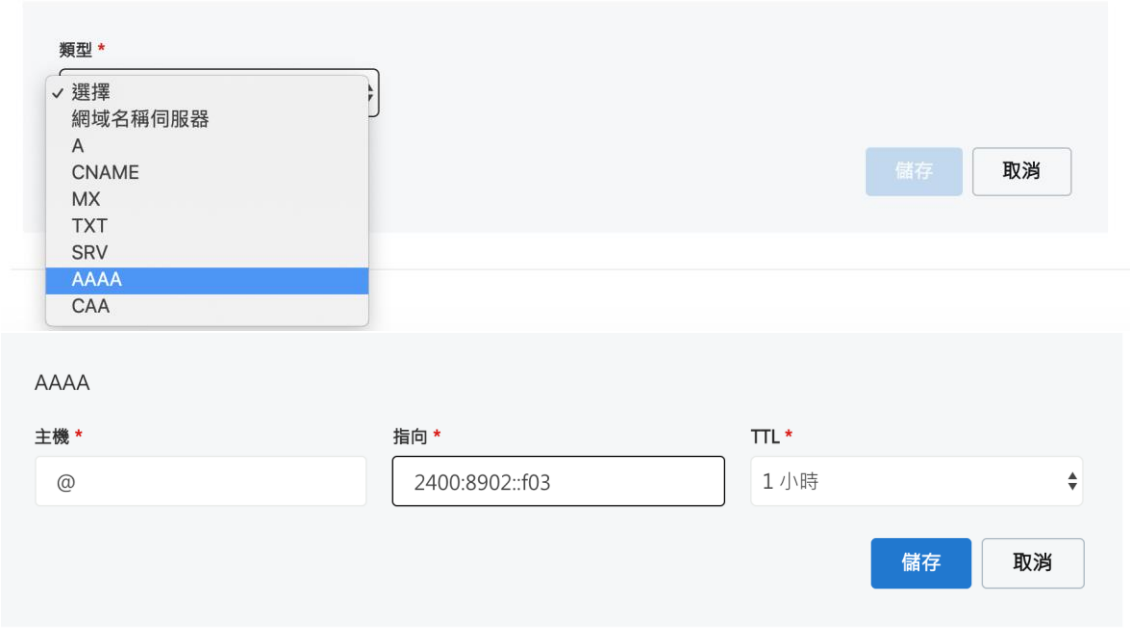



圖 9 GoDaddy.com 設定管理介面

# 第四章 Centos7/Ubuntu18/Windows 2016/Windows 2019 作業系統啟用 IPv6

## 第一節 本篇概述

IPv6 在現存的大多數作業系統都已經啟用，參考下圖可以知道在 2003 年 12 月 17 日發布 Linux 內核（Kernel）2.6.0 之後就已經完整具備 IPv6 功能。在更早之前，Linux Kernel 在 2.1.8 就加入了 IPv6 的部分功能。只是有些作業系統預設是開啟（例如 Linux），有的預設是關閉。

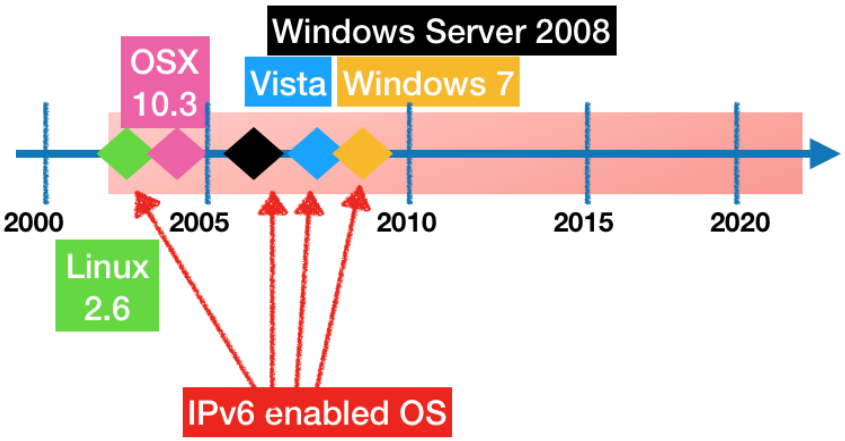



圖 10 支援 IPv6 的作業系統

由於作業系統對 IPv6 的支援牽涉到 Kernel 核心的支援狀況，如果作業系統太老舊不支援 IPv6，建議升級作業系統，這樣做的好處有：

1. 作業系統都有所謂的維護生命週期，只有在維護週期內的版本才可以獲得官方的支援。
2. 舊版的作業系統如果有新的安全漏洞，很難修復。
3. 公司招募的技術人員通常都是熟悉新的作業系統，對於舊的作業系統通常不熟。

第二節 Centos7 啟用 IPv6

一、在測試 IPv6 之前，請先確定 DNS 已經有設定 IPv6。

作法是在 DNS 加上一筆 AAAA record 指向到主機的 IPv6 位址，設定完成之後再以 dig 指令進行驗證。以下是以 Godaddy 的操作畫面為範例。Godaddy 是全球最知名的 DNS 銷售及管理廠商。

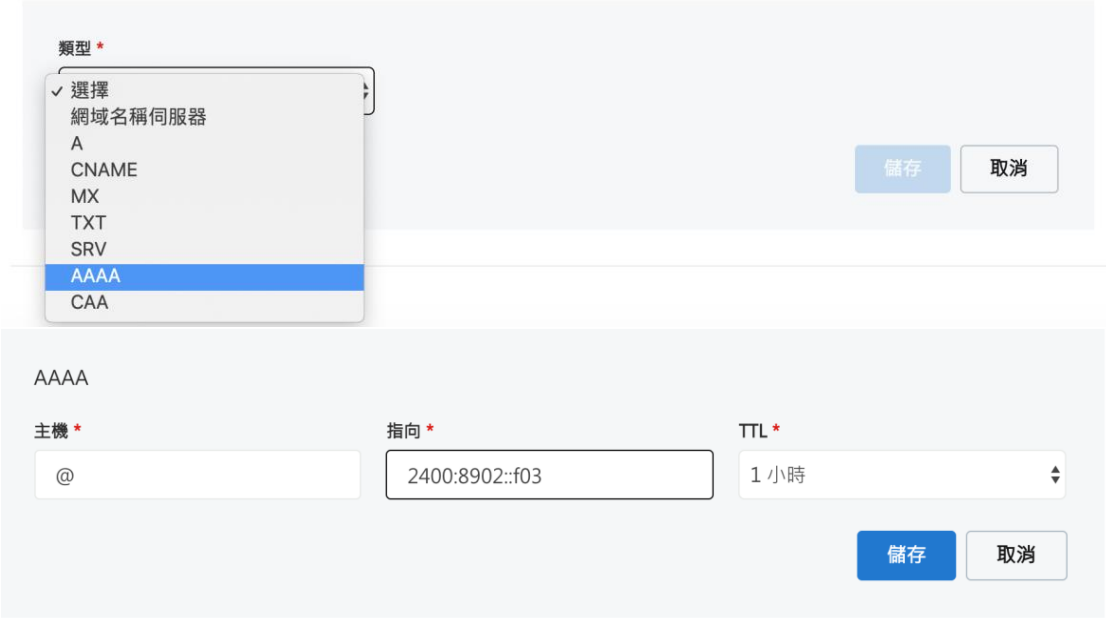



圖 11 在 Godaddy 上新增一筆 AAAA record

二、驗證 DNS 查詢是否有 IPv6

輸入指令

```
dig   hostname   AAAA
```

輸出結果

```
; <<>> DiG 9.10.6 <<>> hostname AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
```

```
; hostname.                IN      AAAA

;; ANSWER SECTION:
hostname.          3599    IN      AAAA    2400:x::x:x:x:x

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53（8.8.8.8）
;; WHEN: Fri May 17 14:54:28 CST 2019
;; MSG SIZE  rcvd: 67
```

三、修改 /etc/sysctl.conf 檔案，將 ipv6 打開

```
修改 /etc/sysctl.conf
net.ipv6.conf.all.disable_ipv6 = 0# 1 表示關閉，0 表示開啟
net.ipv6.conf.default.disable_ipv6 = 0
```

四、重新載入設定

```
輸入指令
sysctl -p

輸出結果
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
```

五、重啟網路，讓網卡取得 IPv6 位址

```
輸入指令
systemctl restart network
```

六、檢查是否取得 IPv6 位址

```
驗證方法輸入指令
ifconfig -a | grep inet6

輸出結果（x 代表配置的 IPv6 位置）
inet6 fe80::x:x:x:x  prefixlen 64  scopeid 0x20<link>
inet6 2400:x::x:x:x:x  prefixlen 64  scopeid 0x0<global>
inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

七、測試是否可以連到外部 IPv6

```
輸入指令
ping6 google.com

輸出結果
```

```
PING google.com（nrxx.xx.net （2404:x:x:x::x）） 56 data bytes
64 bytes from nrxx.xx.net （2404:x:x:x::x）: icmp_seq=1 ttl=58
time=0.803 ms
64 bytes from nrxx.xx.net （2404:x:x:x::x）: icmp_seq=2 ttl=58
time=0.707 ms
```

八、修改 web server 設定檔（這裡以 nginx 為範例）

```
listen 80 default_server; # 如果只有 listen IPv4，寫法為 listen 80
listen [::]:80; # 要支援 IPv6，則是加上 [::]:
listen 443 ssl http2;
 listen [::]:443 ssl http2;
```

如果要綁固定的 IPv6 IP，可以使用以下方法

```
listen      [2400:6180:0:d0::1f33:d001]:80 default_server;
```

如果是 Apache ，其設定可以參考下面

```
Listen 80
Listen 443
Listen [::]:80
Listen [::]:443

<VirtualHost *:80 [::]:80>
...
</VirtualHost>
```

九、重啟 web server （以 nginx 為例）

```
輸入指令
service nginx restart
```

十、檢查 web server 是否有 listen IPv6

```
輸入指令檢查
netstat -natp | grep nginx

輸出結果
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      10996/nginx:
master
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      10996/nginx:
master
tcp6       0      0 :::80                   :::*                    LISTEN      10996/nginx:
master
tcp6       0      0 :::443                  :::*                    LISTEN      10996/nginx:
```

master

十一、透過外部 IPv6 檢查網站檢驗 web server 是否可以正常運作

https://www.mythic-beasts.com/ipv6/health-check
如果設定正確，所有的檢查項目都應該要通過，下圖是一個檢查通過的範例。

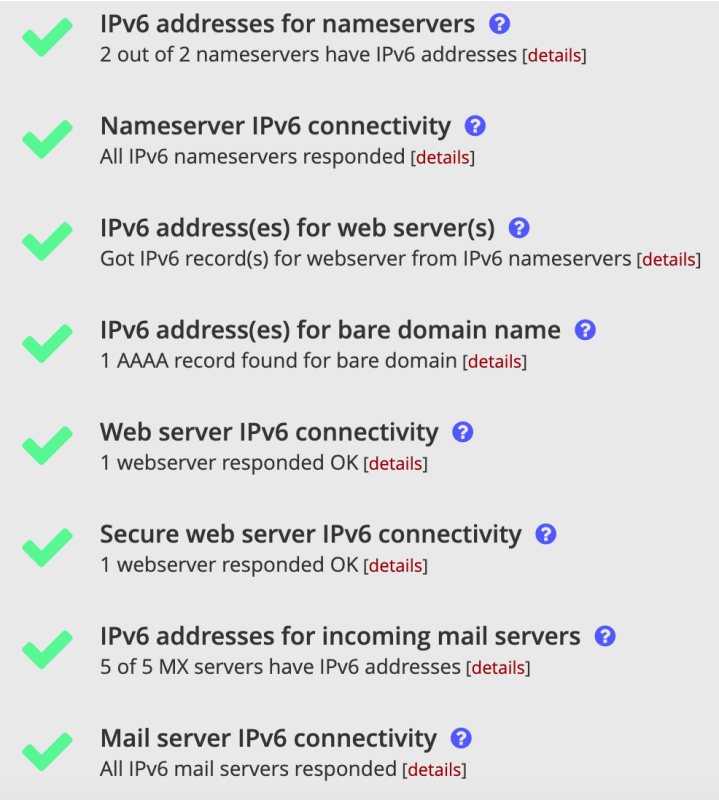



圖 12 IPv6 網站檢驗成功示意圖

第三節 Ubuntu 18 啟用 IPv6

一、設定 /etc/network/interfaces 檔案

新增以下資訊

```
iface eth0 inet6 static
pre-up modprobe ipv6
address  2404:0:x:0:x:x:x:x
netmask 64
```

重新啟動網路

輸入指令

```
/etc/init.d/networking restart
```

二、檢測

用 ifconfig 或 ip addr show 測試 IPv6 位址是否有設定正確

輸入指令

```
ifconfig
```

輸出結果

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu
1500
       inet 139.162.111.100  netmask 255.255.255.0  broadcast
139.162.111.255
       inet6 2404::x:x:x:x  prefixlen 64  scopeid 0x0<global>
      inet6 fe80::x:x:x:x  prefixlen 64  scopeid 0x20<link>
       ether f2:3c:91:4a:32:87  txqueuelen 1000  （Ethernet）
       RX packets 11778775  bytes 1641085278 （1.6 GB）
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 250621723  bytes 40629618009 （40.6 GB）
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

輸入指令

```
ip addr show
```

輸出結果

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc fq_codel state UP group default qlen 1000
   link/ether f2:3c:91:4a:32:87 brd ff:ff:ff:ff:ff:ff
   inet 139.162.111.100/24 brd 139.162.111.255 scope global eth0
      valid_lft forever preferred_lft forever
   inet6 2404:0:x:0:x:x:x:x scope global dynamic mngtmpaddr
```

```
noprefixroute
       valid_lft 2591999sec preferred_lft 604799sec
    inet6 fe80::x:x:x:x scope link
       valid_lft forever preferred_lft forever
```

## 第四節 Windows 2016 啟用 IPv6

先開啟網卡設定，開啟位置可以透過「控制台」，也可以以滑鼠點選右下角的網路卡圖示，並依據跳出的浮出選單，選擇網路控制中心，進入網卡設定。

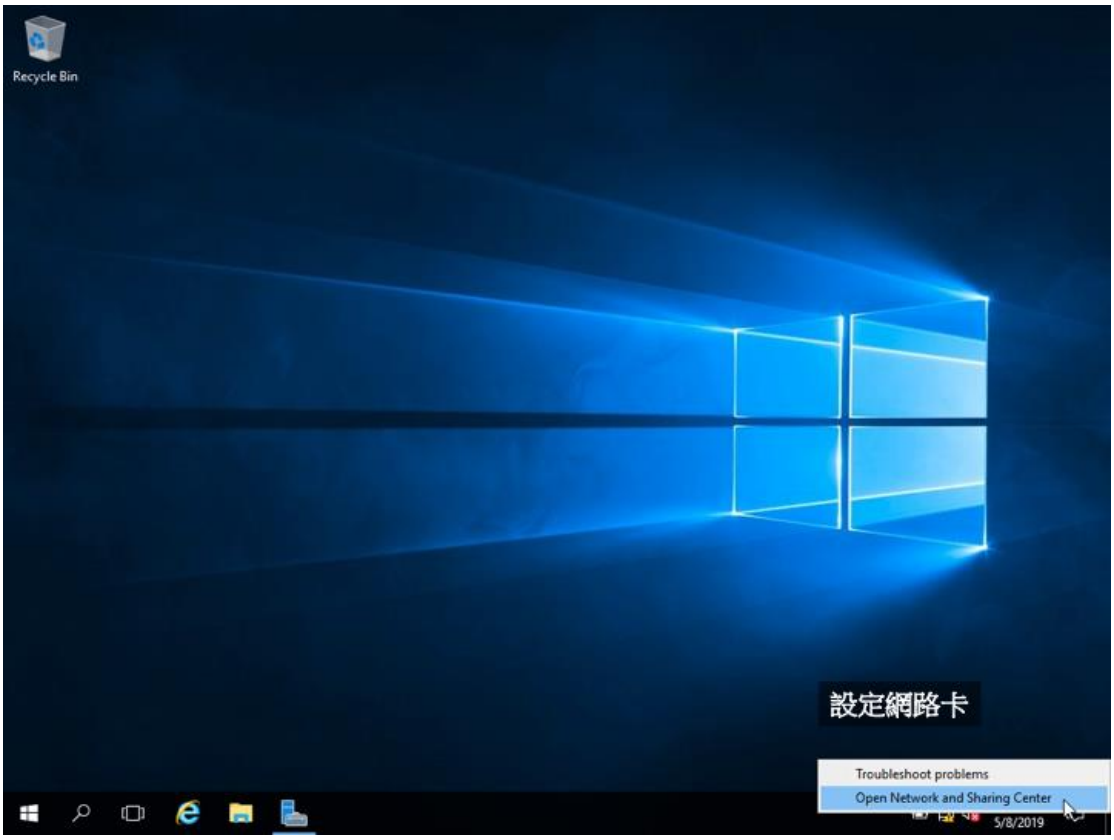



圖 13 Windows 2016 設定網卡

進入網路設定中心並選擇連上網的網卡之後，可以進行網路設定，記得選擇 TCP/IP，並依據配置的 IP 進行設定，需要設定的項目會包括 IP 位址及閘道器等，必要的話，也需要設定 DNS 負責網址跟 IP 之間的轉換。

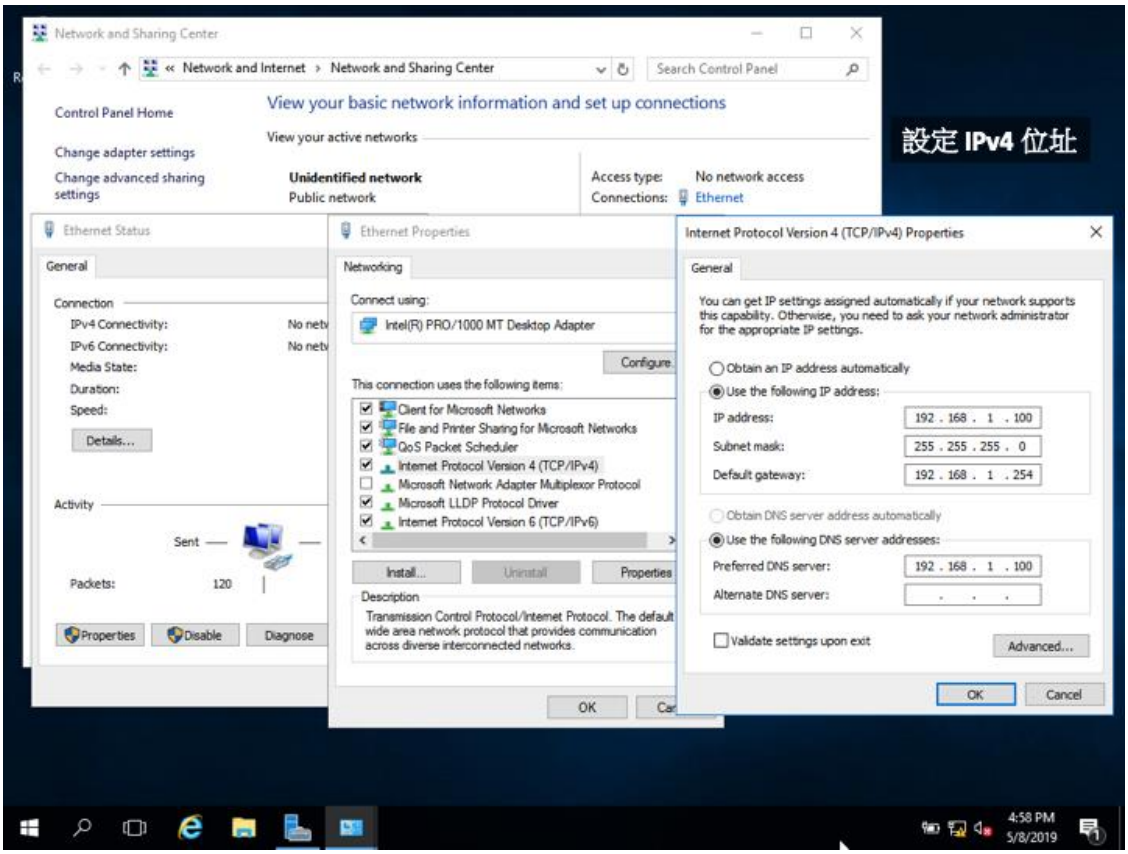



圖 14 Windows 2016 開啟網路介面

依據從 ISP 所取得的 IPv6 位址，填入到下圖的表單內。需要輸入包括 IPv6 位址、IPv6 的 prefix、網路出去的 gateway，還有 DNS server 的 IPv6 位址。

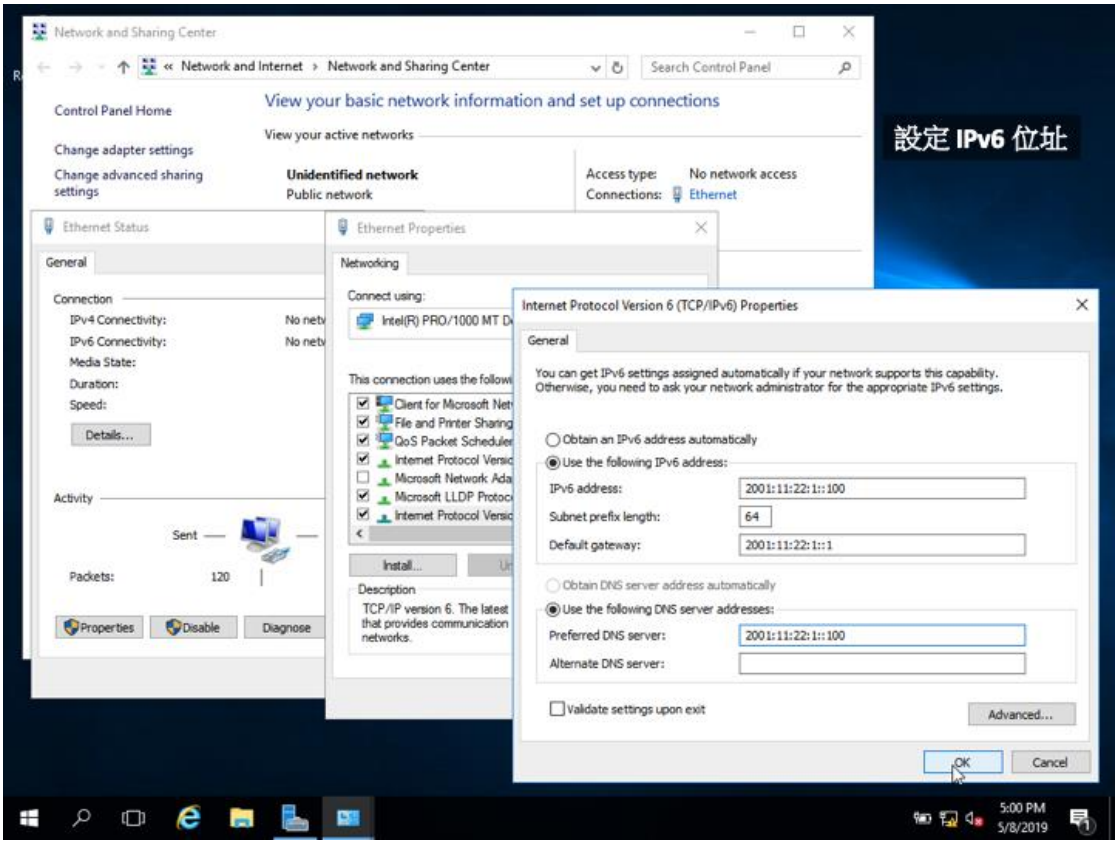



圖 15 Windows 2016 輸入 IPv6 位址

接著設定主機的 hostname，此 hostname 只是用於辨識跟顯示這台機器的顯示名稱。

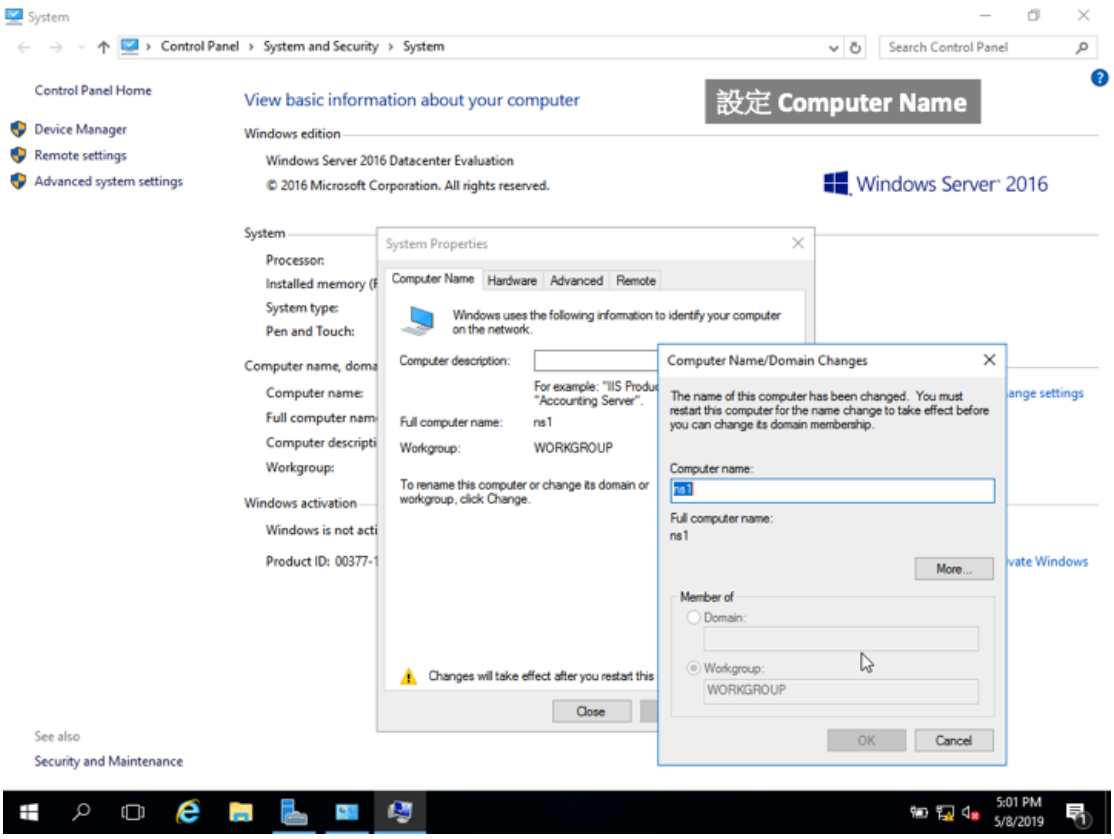



圖 16 Windows 2016 設定 hostname

在以上畫面設定完畢之後，因為已經更改了網路介面卡設定，系統會要求要重開機以啟用新的設定。此時請按下確認立即重啟，讓系統自動重新啟動。

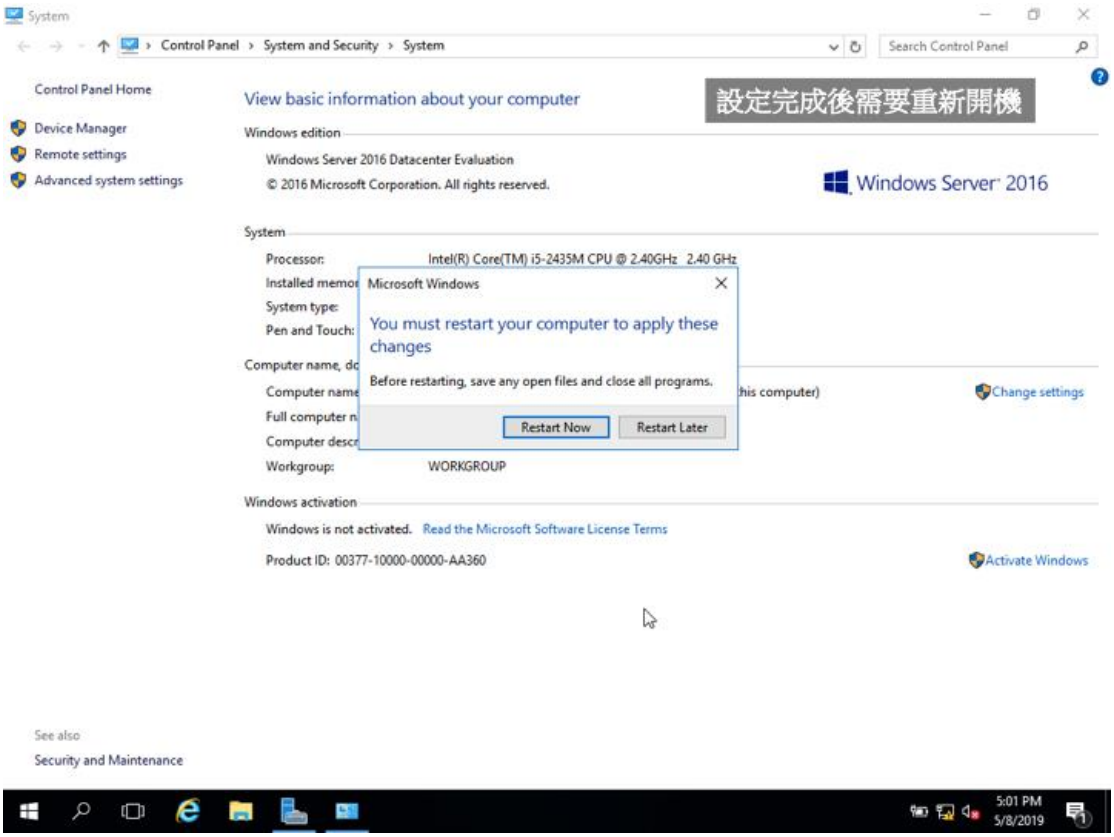



圖 17 Windows 2016 設定完成被要求重開機

重新開機進入系統之後，網卡部分已經設定完成，接著我們要設定本台主機的角色跟規則。

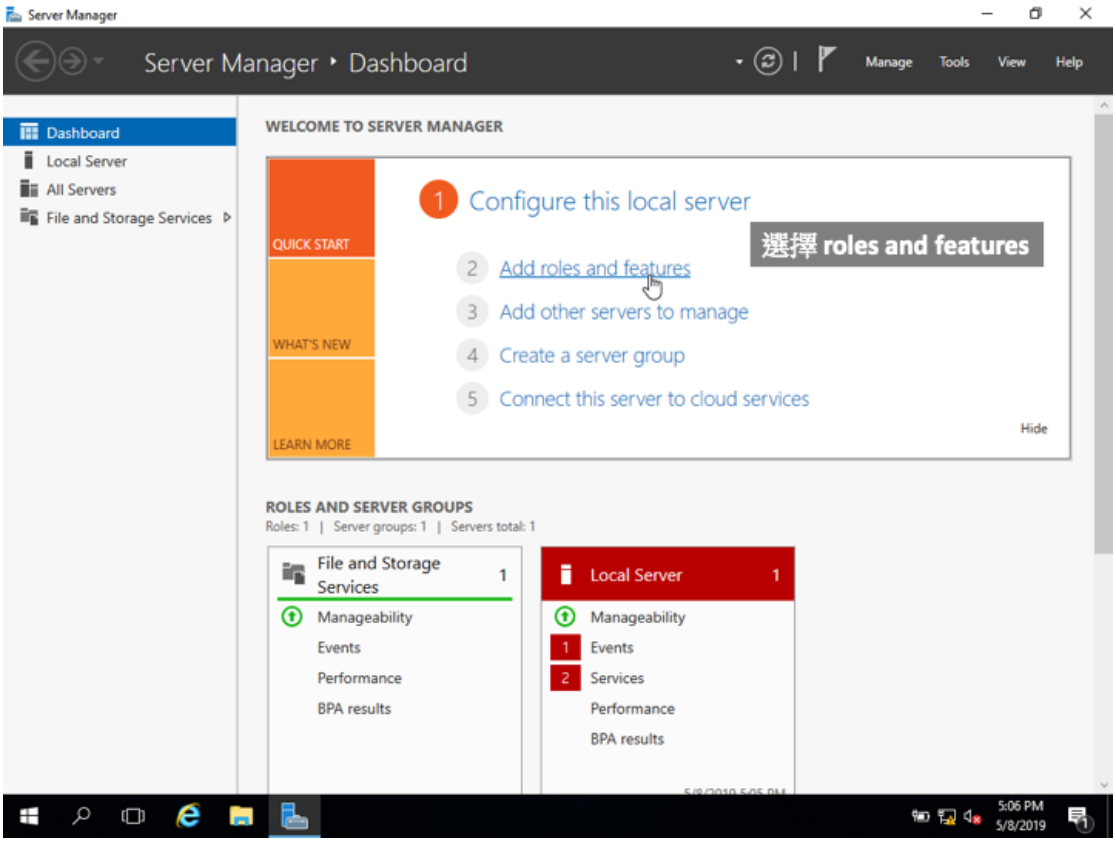



圖 18 Windows 2016 選擇 roles and features

接下來請依照設定導引精靈，按下一步按鈕，進行設定。

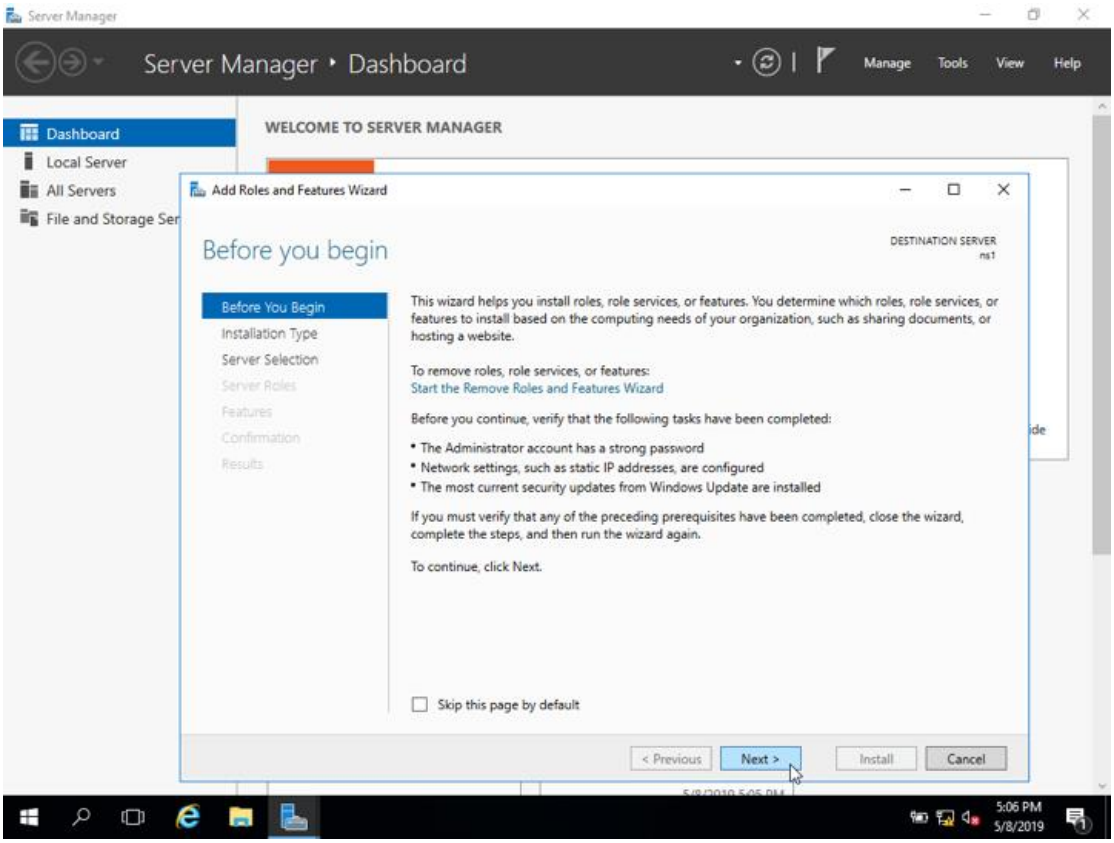



圖 19 Windows 2016 警示頁面

在這個畫面，請選擇第一個項目（第二個項目是給 VM 虛擬機使用）。

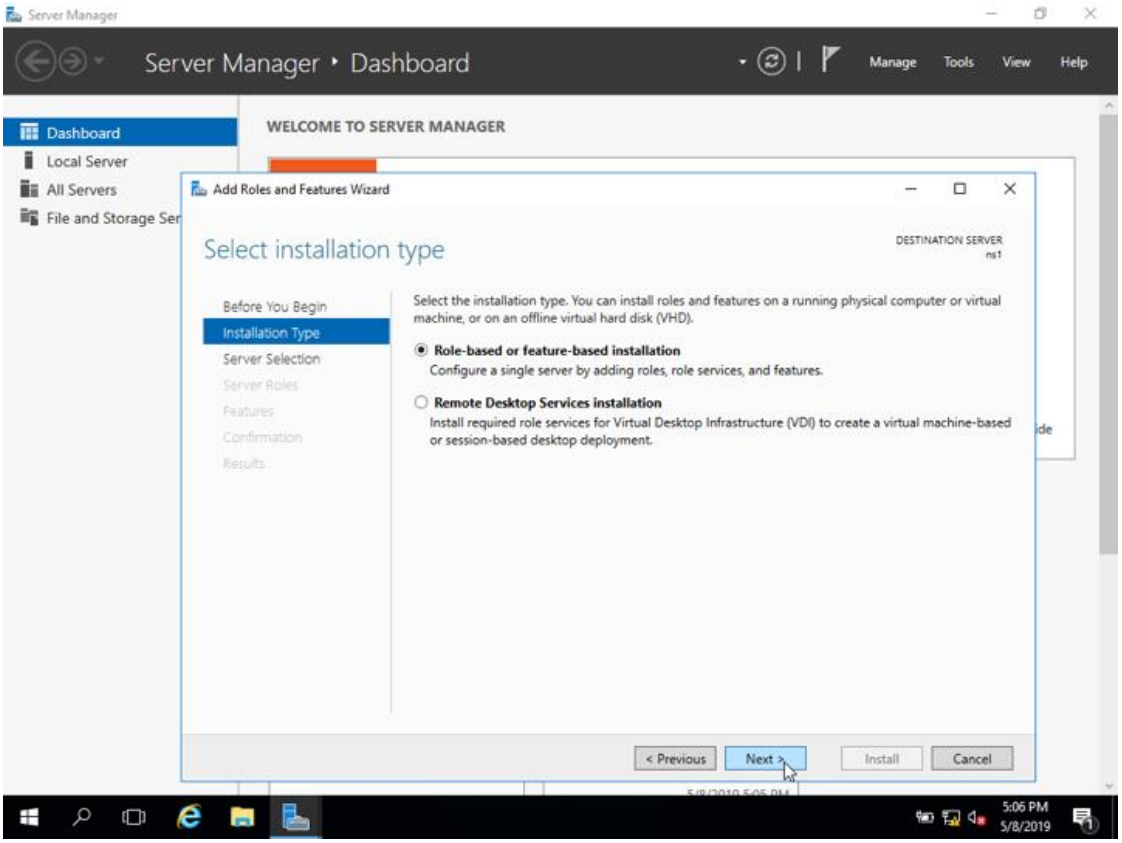



圖 20 Windows 2016 選擇安裝方式

選擇已經建立好的主機，由於此時只有一台，故直接選擇該台主機即可。

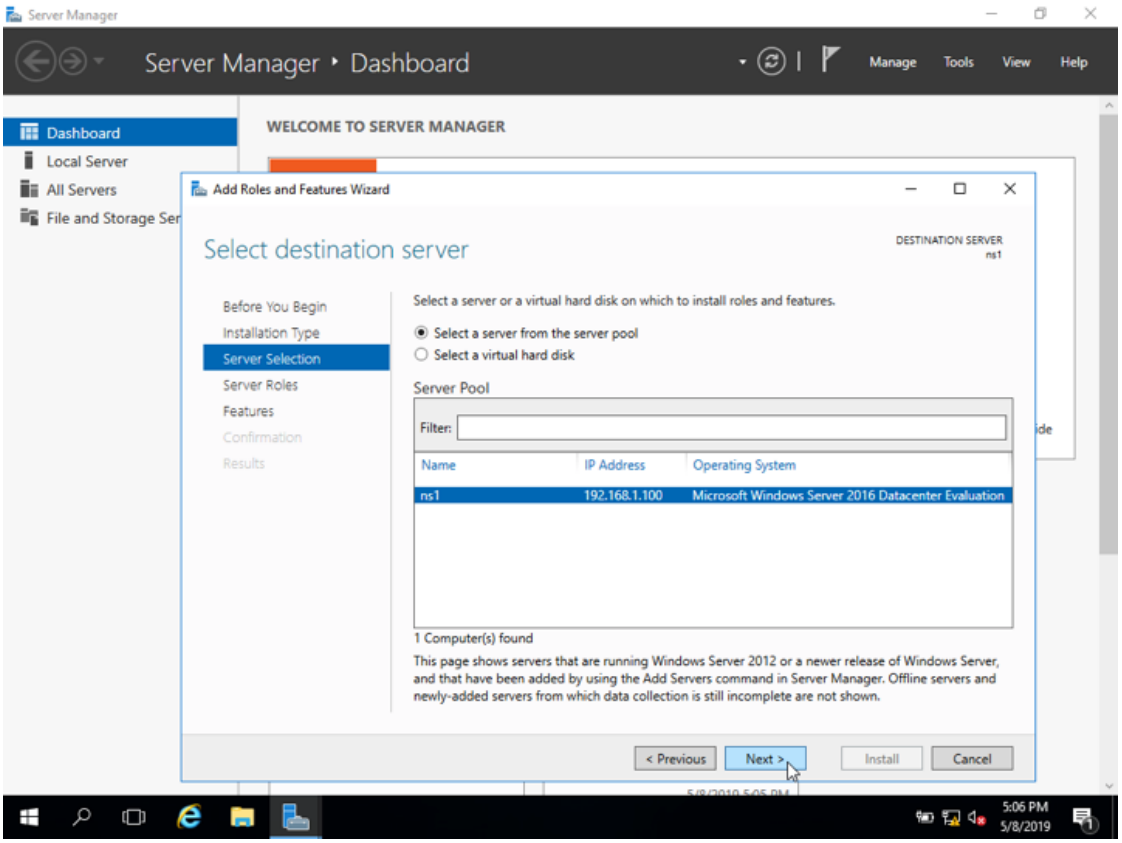



圖 21 Windows 2016 選擇目的主機

接著，依據視窗指示，選擇要將此主機設定為哪些角色。可以選擇的項目包括 DHCP Server（負責動態 IP 的配置）、DNS Server（負責網域的解析）、Web Server（負責提供網頁服務）。

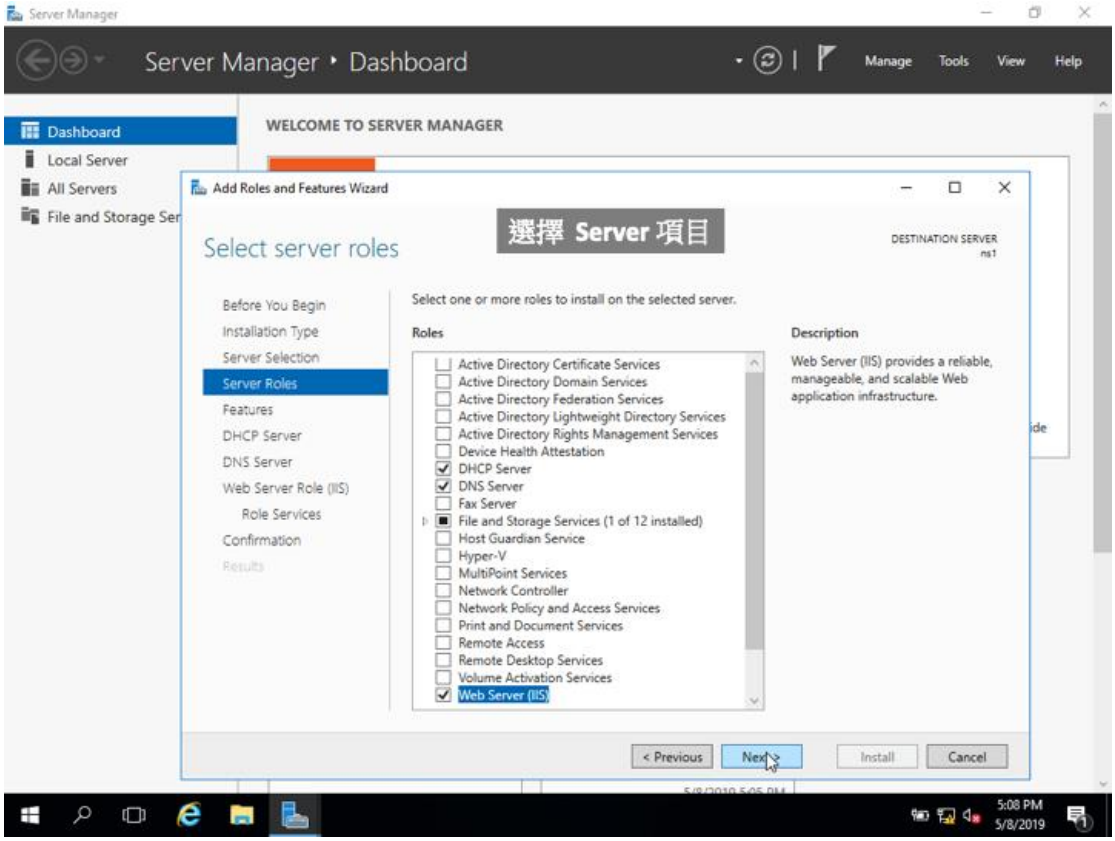



圖 22 Windows 2016 選擇 Server 項目

請選擇 DNS Server，讓此主機具備 DNS 解析功能。

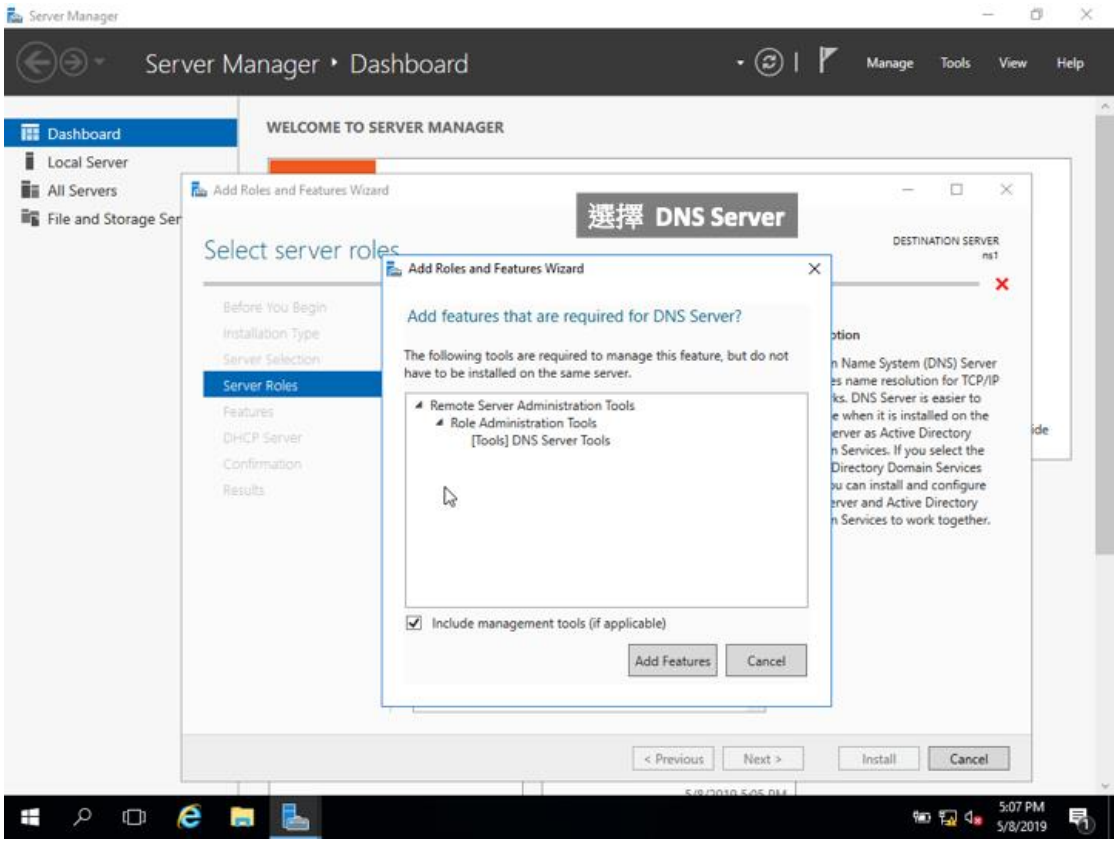



圖 23 Windows 2016 選擇 DNS Server

選擇 DHCP，讓此主機具備配置 IP 的功能。

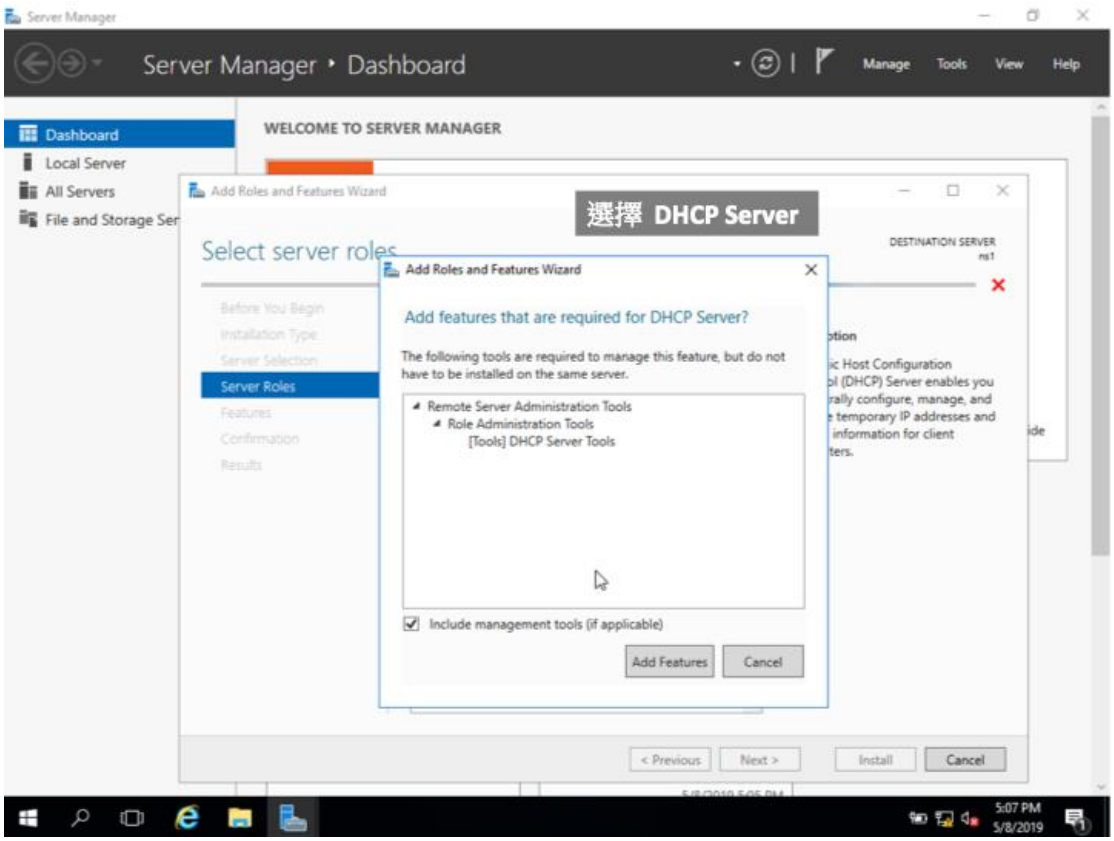



圖 24 Windows 2016 選擇 DHCP Server

選擇 IIS，讓主機具備提供網頁服務的功能。IIS 是 Microsoft 自行研發的 Web Server，功能跟 Apache 或 Nginx 類似。

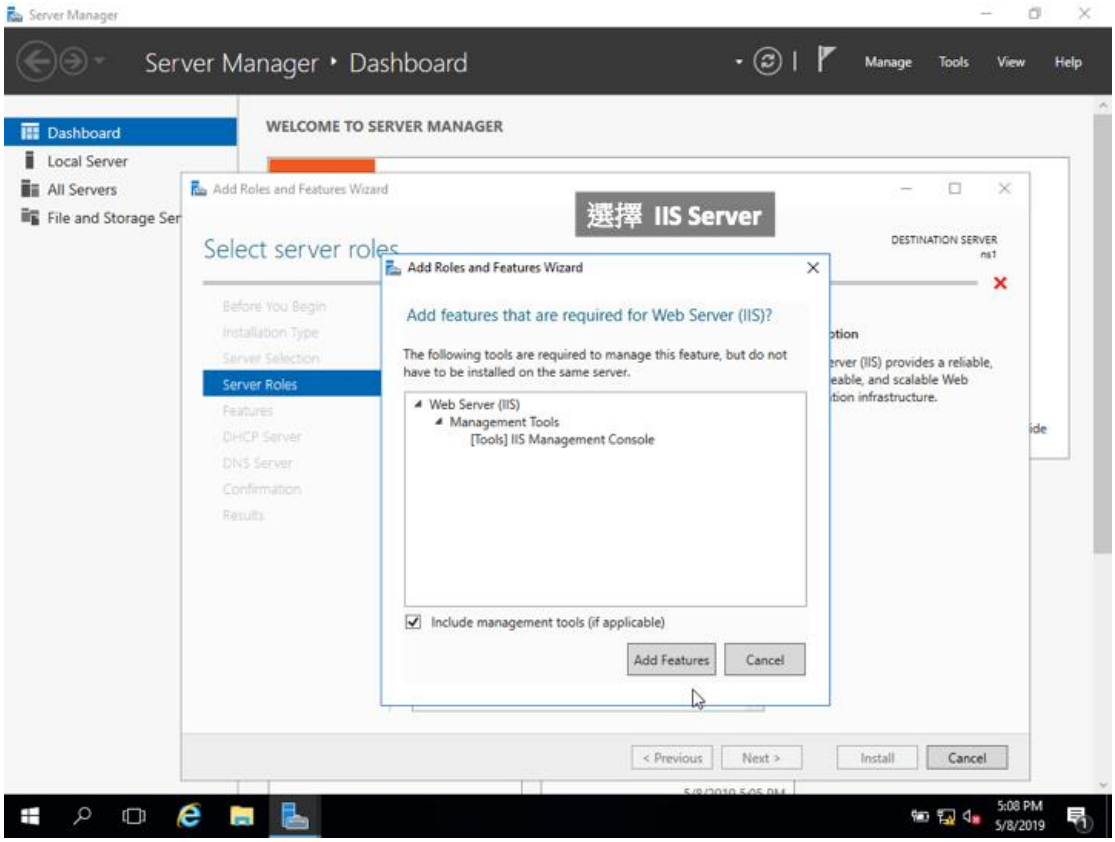



圖 25 Windows 2016 選擇 IIS Server

導引視窗告知請確認所有設定都正確，請按下確認按鈕。

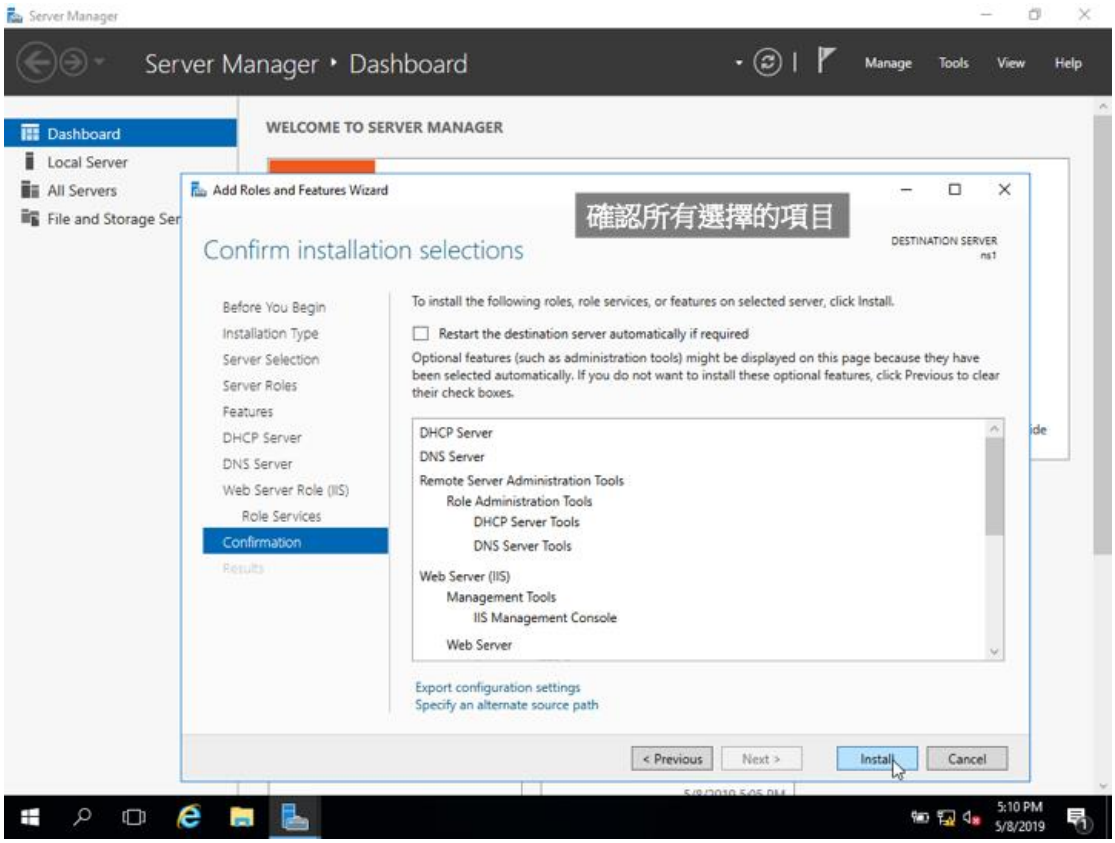



圖 26 Windows 2016 確認所有選擇的項目

系統將必要元件複製到系統上，並先初始化。

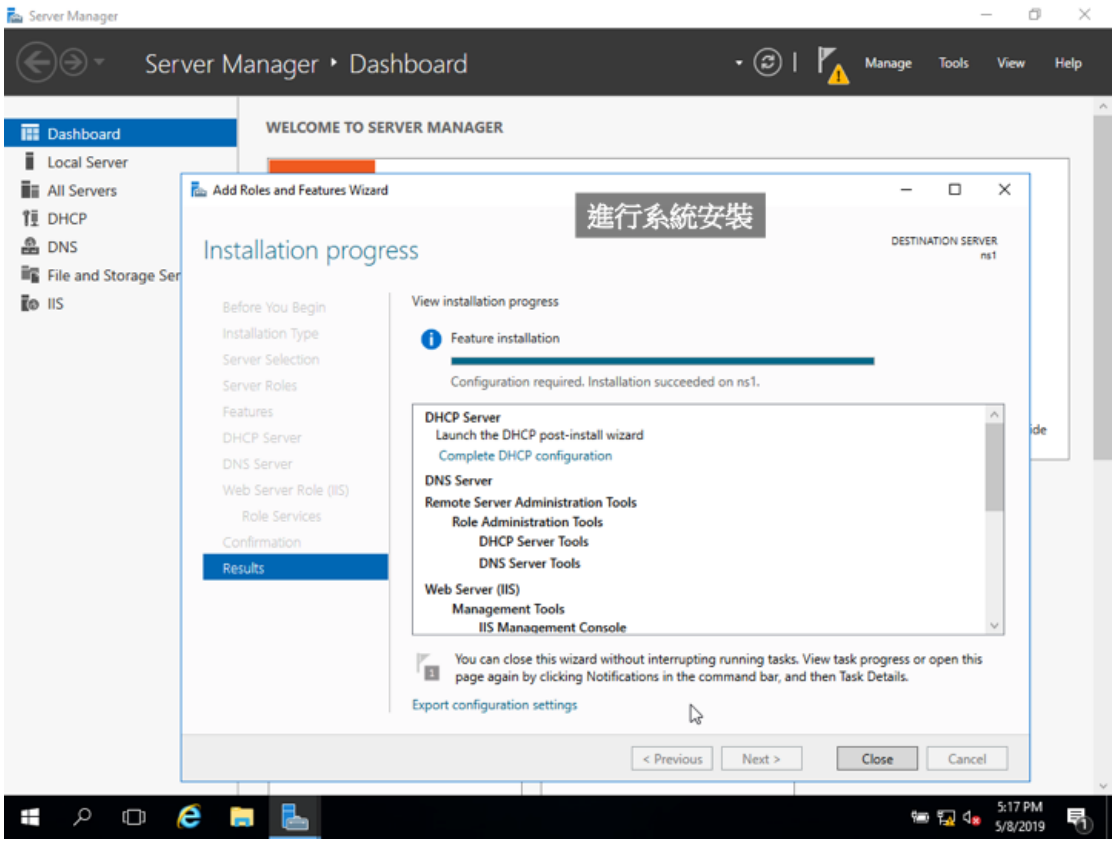



圖 27 Windows 2016 進行安裝

在上述步驟選擇好 DHCP、DNS、IIS 之後，接著要針對這些功能進行細部設定，首先我們選擇設定 DHCP Server。

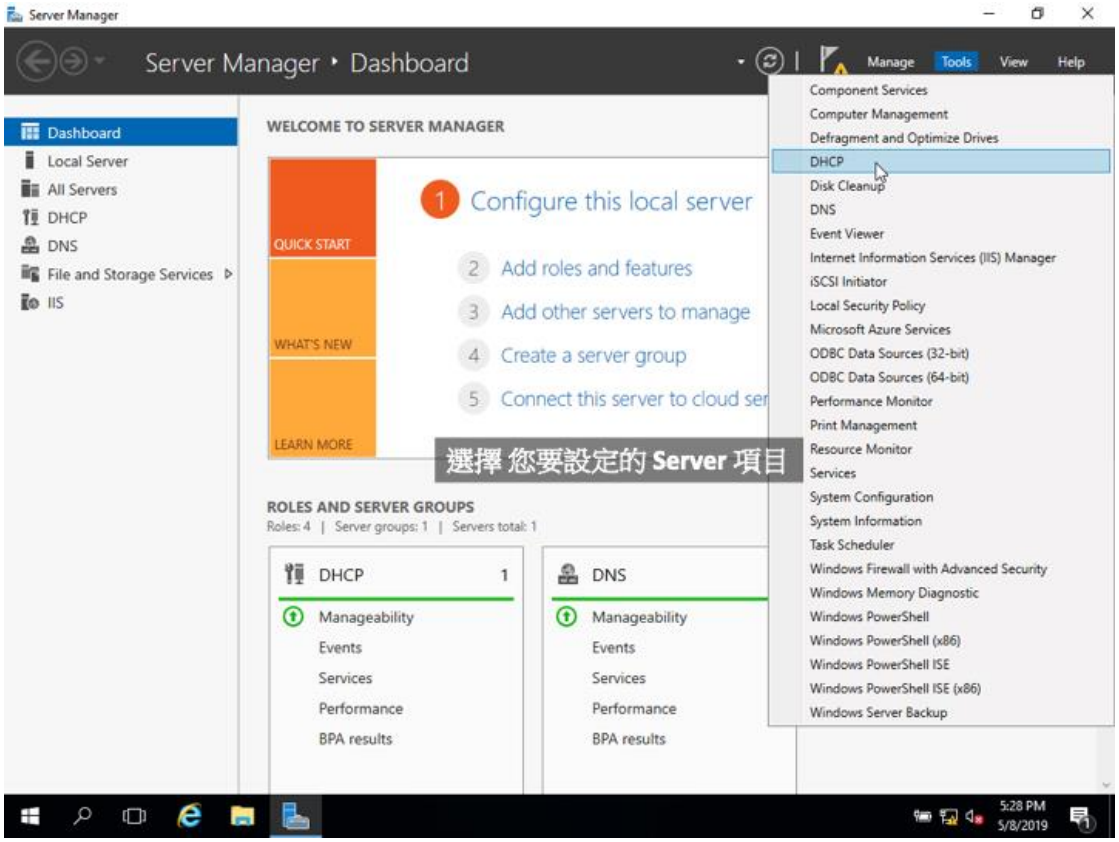



圖 28 Windows 2016 選擇設定項目

進入 DNS 設定選單之後，進行 DNS Zone 的設定。DNS 除了提供查詢網路上「主機名稱」所對應的 IP Address 正解（Forward Lookup）的功能外，也具備將 IP Address 反推「主機名稱」的反解服務（Reverse Lookup）。這裡先設定正解的部分。

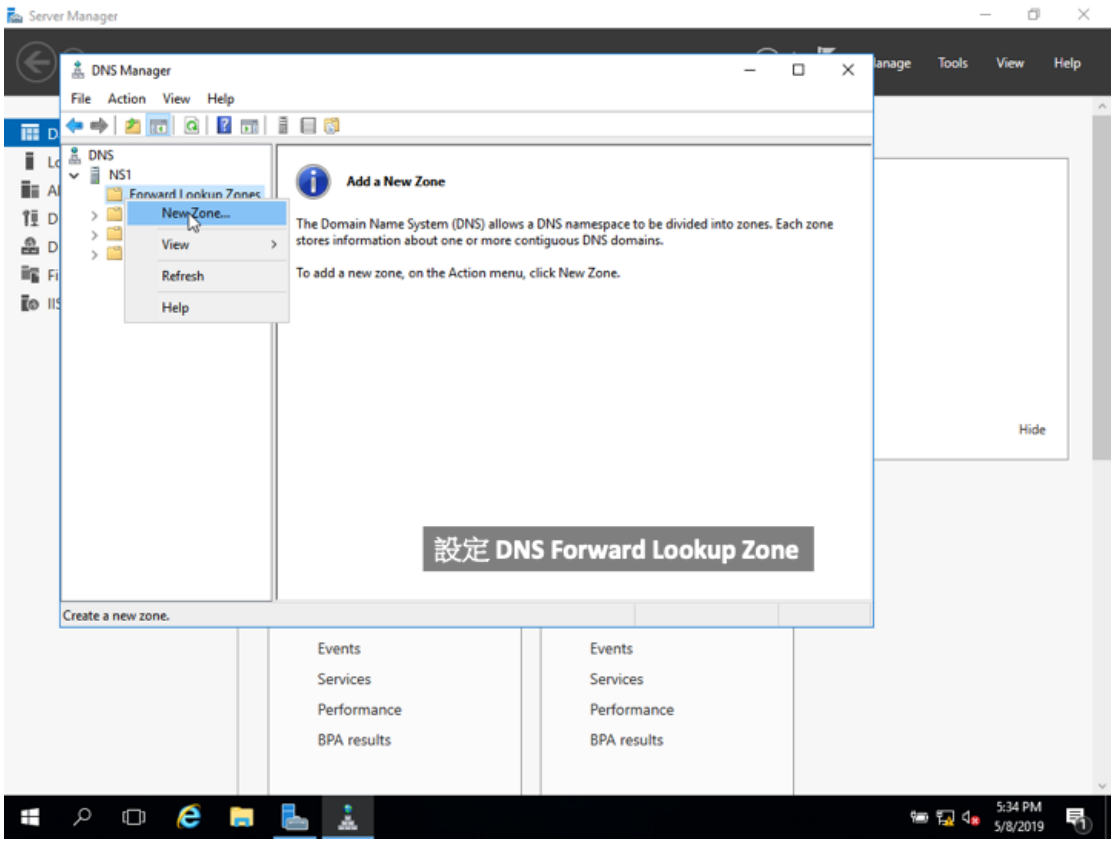



圖 29 Windows 2016 建立 DNS new zone

進入 DNS zone 的設定導引精靈，請依照設定精靈的步驟，按下一步按鈕繼續執行。

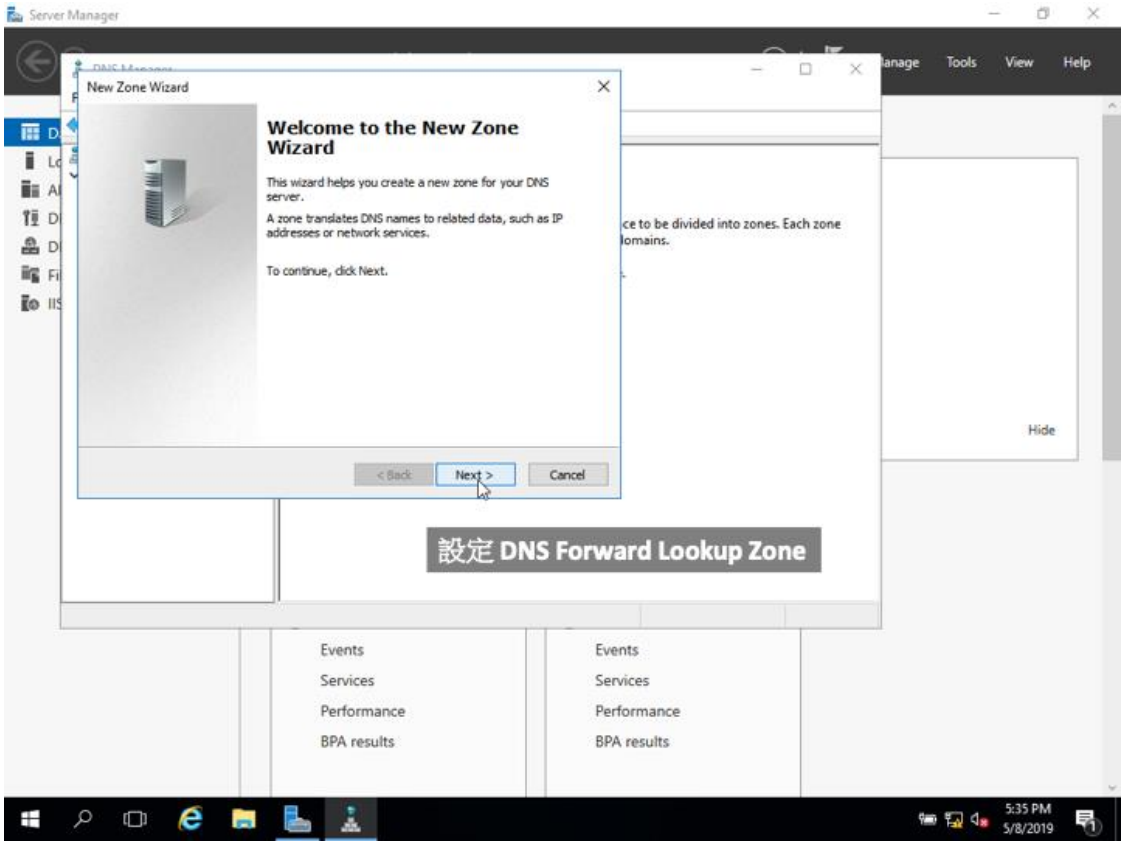



圖 30 Windows 2016 開始設定 DNS zone

我們稱一個域名為一個 Zone，這個 zone 可以是您從出售網域的網站中買到的域名，也可以是從該域名之下延伸出來的 sub-zone。由於 DNS 很重要，因為如果沒有 DNS，使用者無法連到網站，也無法連到其他服務，因為 IP 是數字，根本記不起來。既然 DNS 這麼重要，為提高其容錯能力及查詢效能，我們在架設某一單一 zone 的時侯，常以多台伺服器來負責該 zone 的服務。

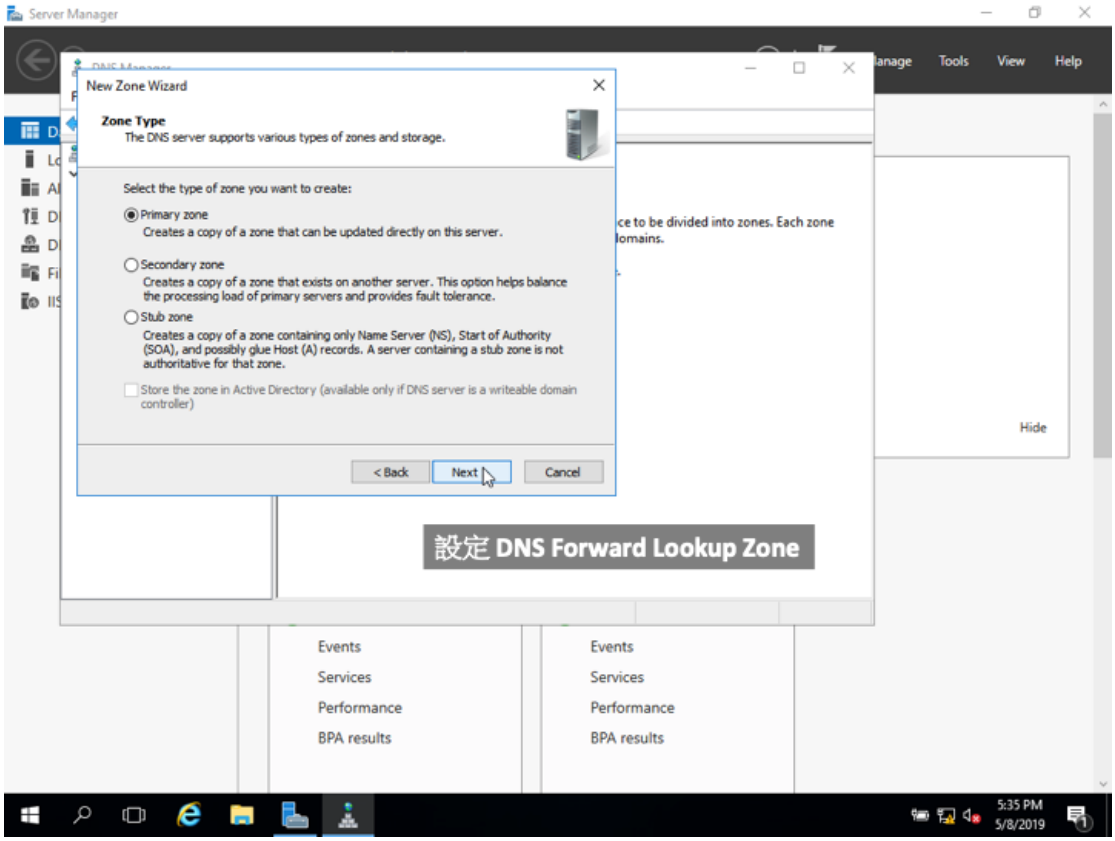



圖 31 Windows 2016 設定 zone type

在安裝精靈的導引下，接著輸入你購買的網域名稱，此時不要輸入子網域名稱，例如你購買了 server.tw 網域，這裡就是輸入 server.tw。之後如果架設一個網站，你可能會為這個網站設定為 www.server.tw，如果你架設了一個 POP3 收信主機跟 SMTP 發信主機，那你可能分別設定 pop3.server.tw 跟 smtp.server..tw。

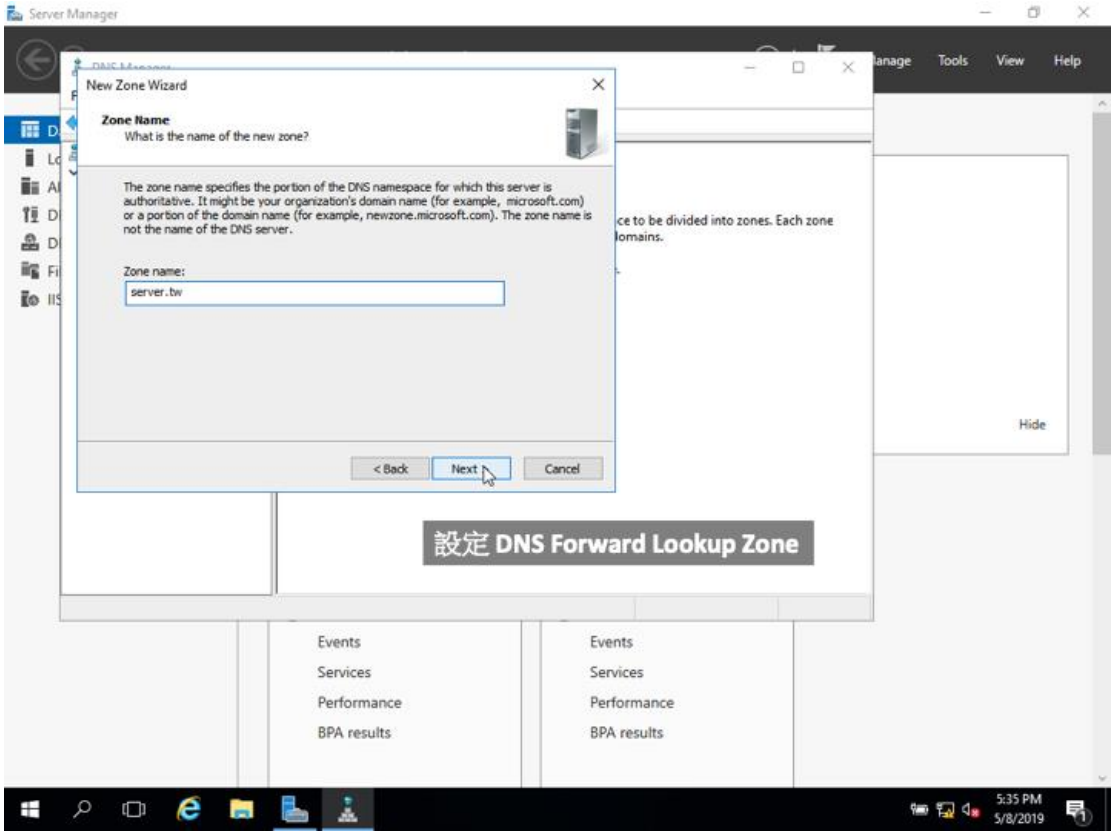



圖 32 Windows 2016 輸入 zone

DNS Server 會將所有關於網域的設定保存在 DNS zone file 內，在這個 zone file 內，記錄所有正確的 DNS 設定。依據設定精靈，請在此輸入 zone file 的名稱，我們輸入 server.tw.dns 作為 zone file 名稱。

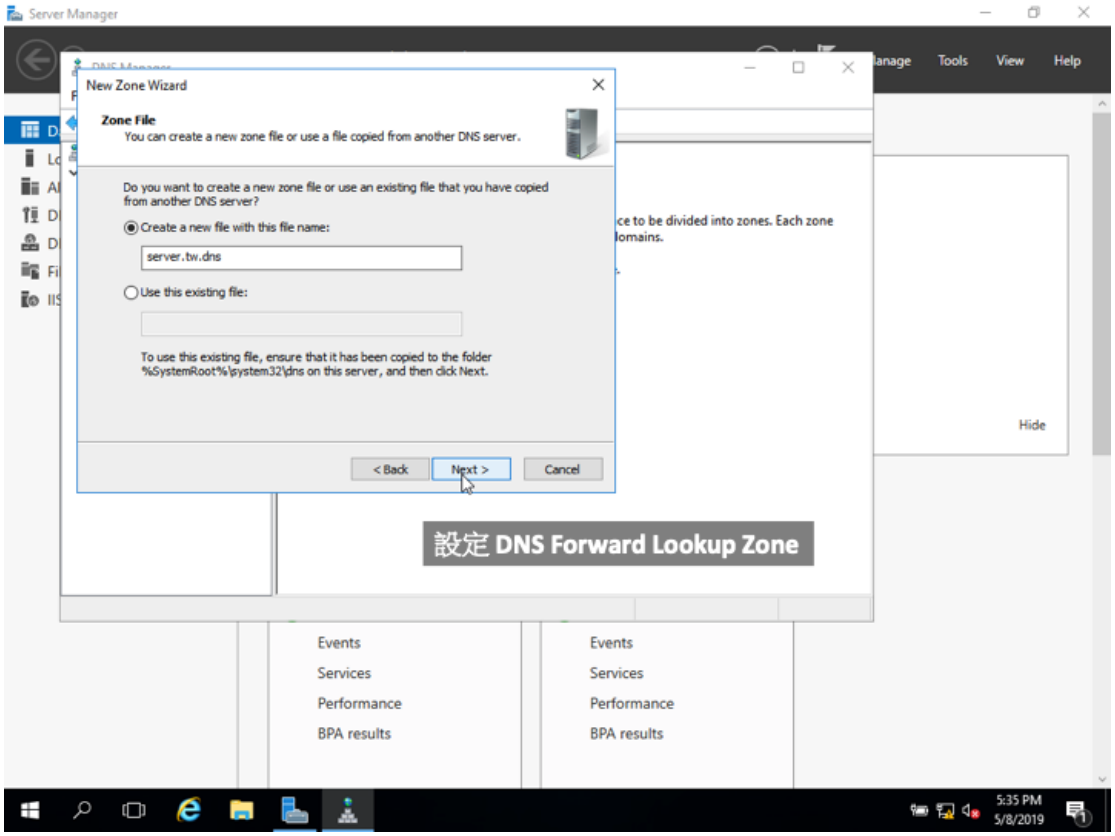



圖 33 Windows 2016 建立 zone file

由於設定為 Primary，因此請選擇不允許動態更新。所有 Primary 的 zone 都是手動更新，因為是主要來源，需要由管理人員設定跟維護，不會由其他主機提供資料進行自動更新。

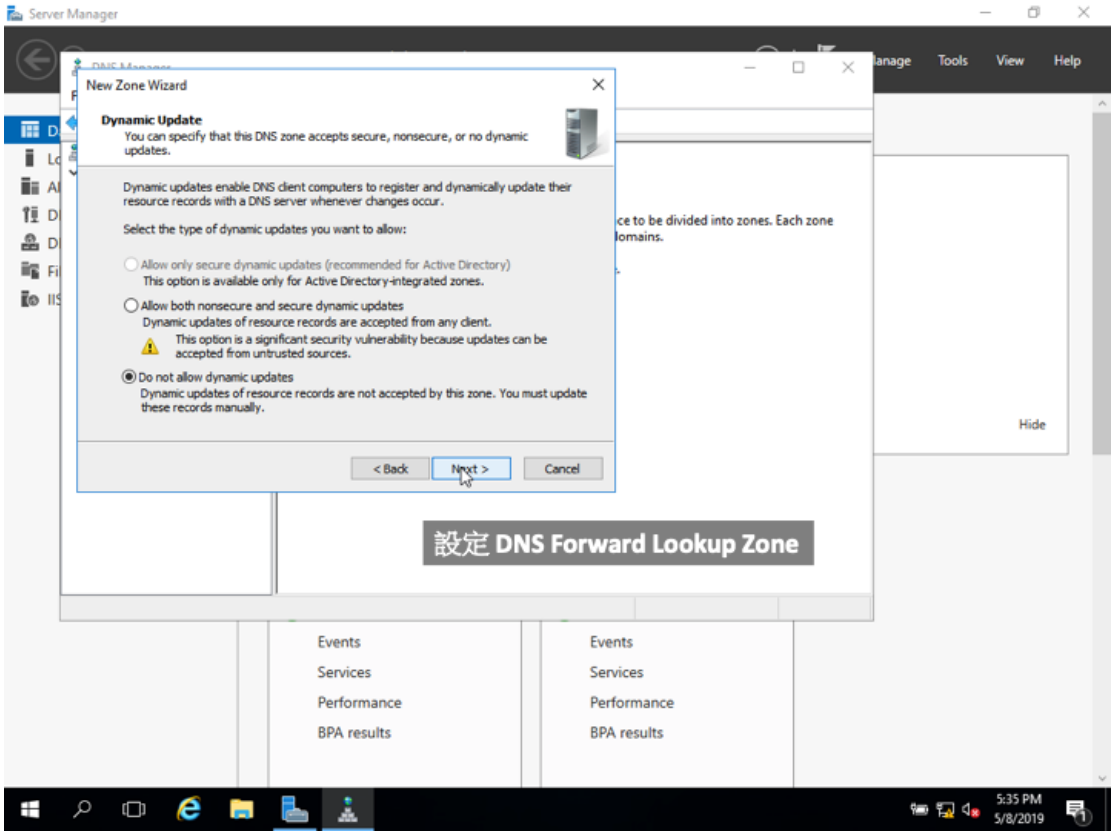



圖 34 Windows 2016 DNS 設定確認視窗

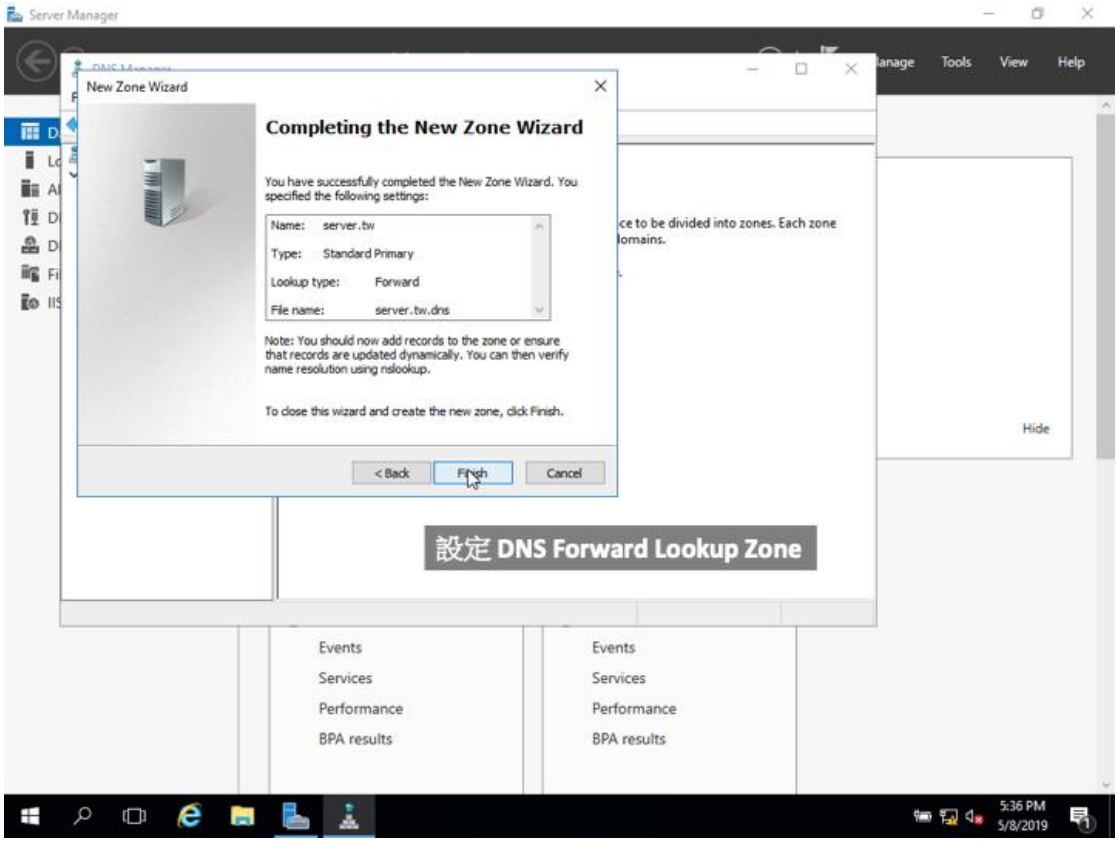



圖 35 Windows 2016 設定 DNS 完成視窗

在這裏設定要對應的主機名稱跟 IP 位址。

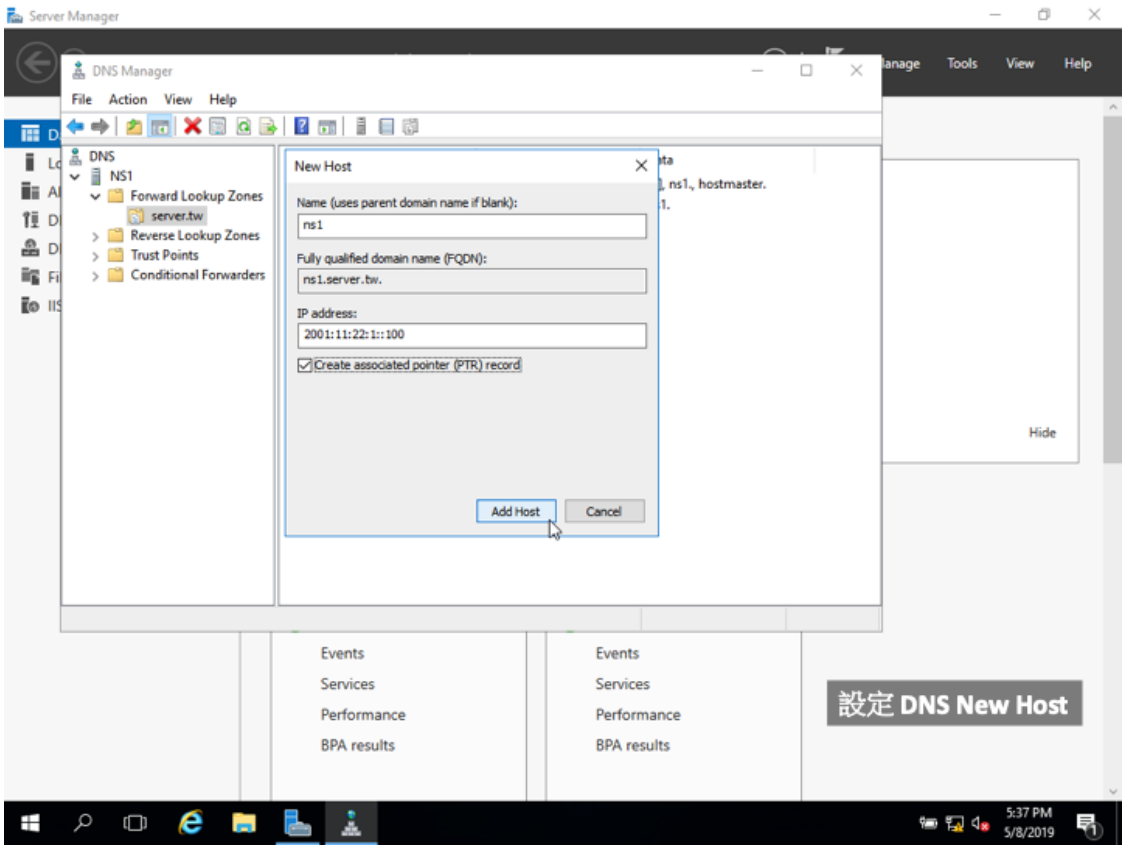



圖 36 Windows 2016 設定 DNS 新的主機

以上動作是完成一台 DNS 的 IPv4 位址設定，接下來要設定這台 DNS 主機的 IPv6 位址。請選擇建立一個新的網域，待會在下一頁則需要選擇 IPv6。

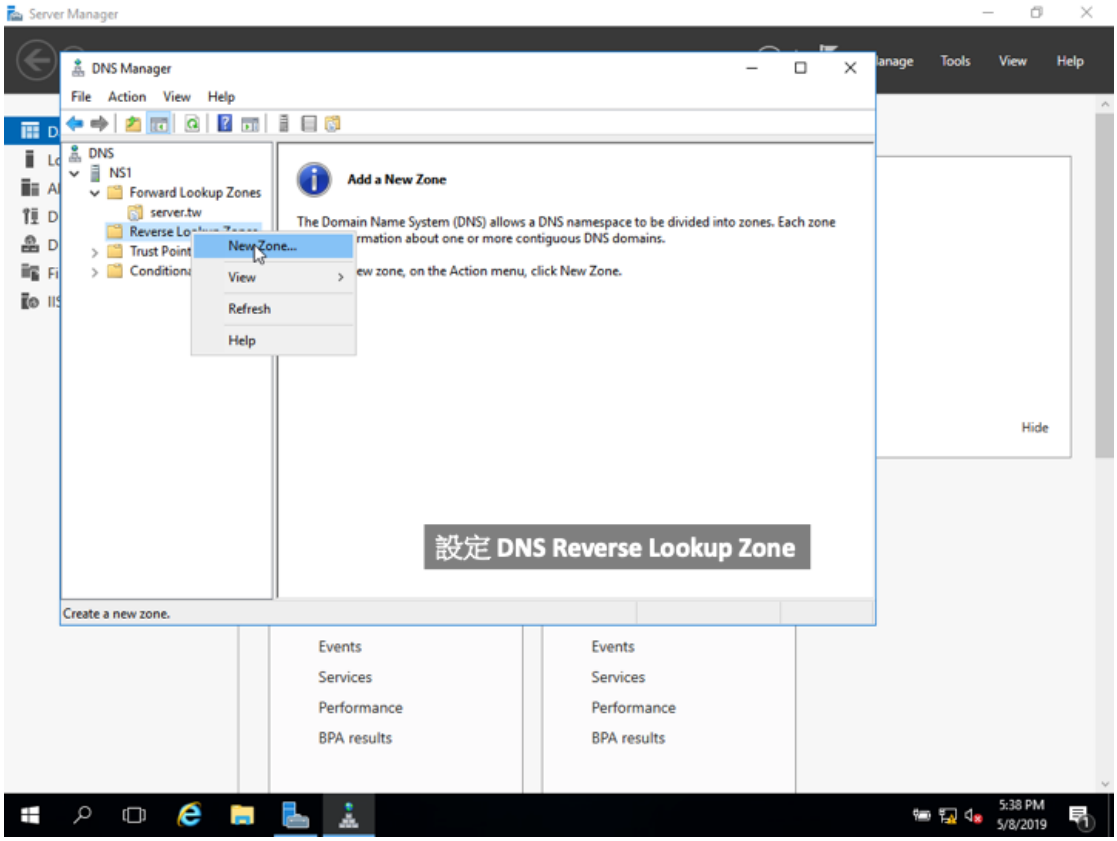



圖 37 Windows 2016 設定 DNS reverse lookup zone

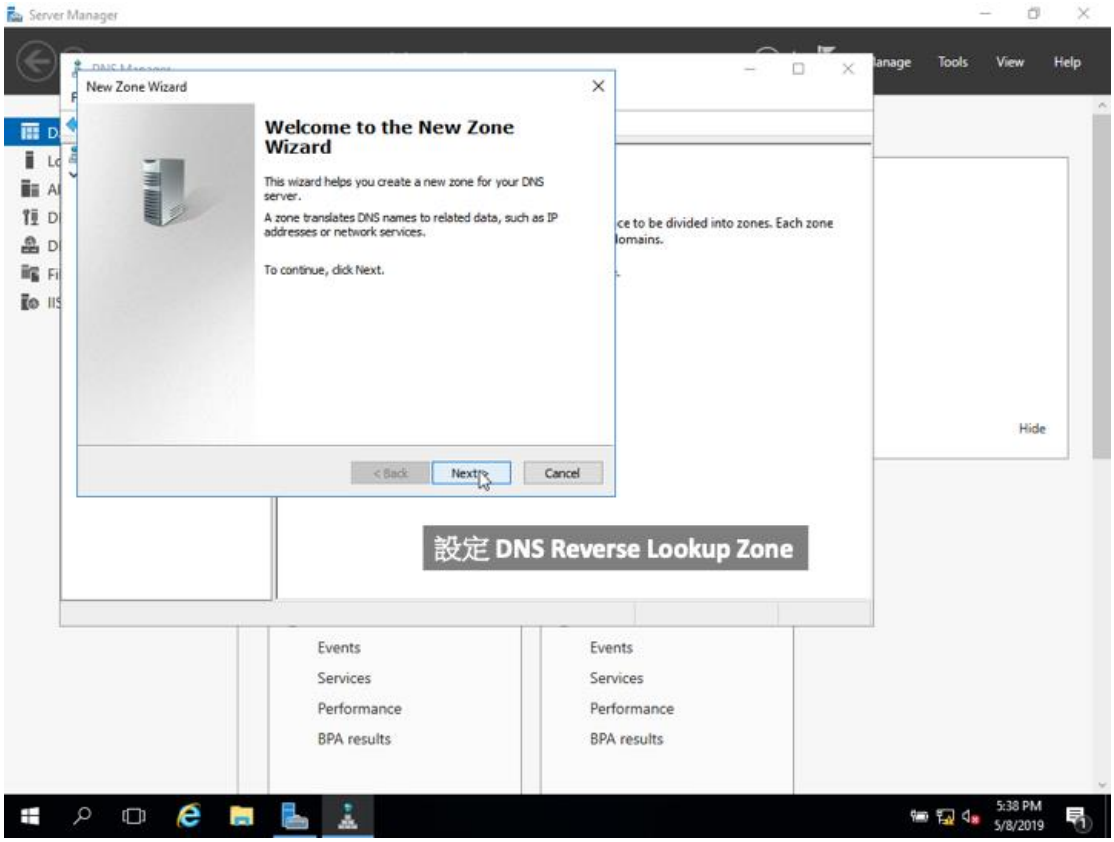



圖 38 Windows 2016 設定 DNS reverse lookup zone 歡迎畫面

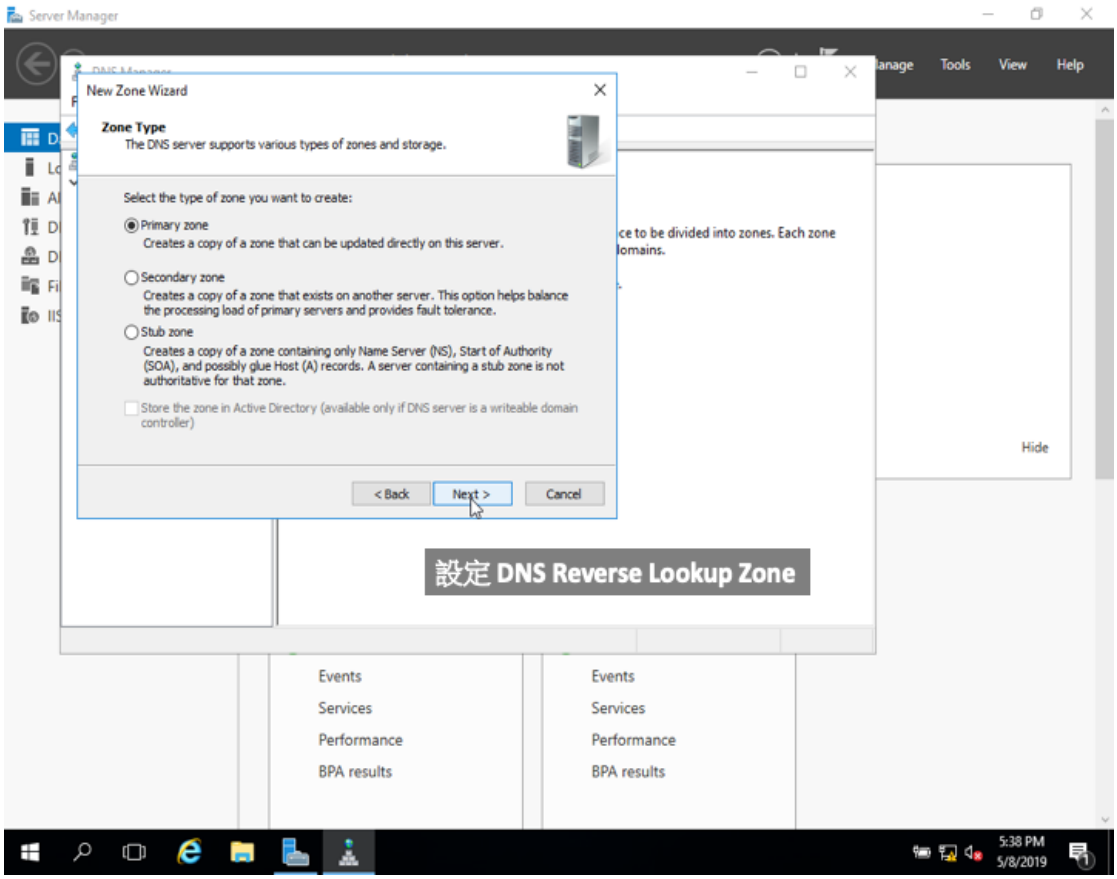



圖 39 Windows 2016 選擇 Zone 類型

這一個畫面是重點，請在這邊選擇 IPv6 選項，選擇建立 IPv6 反解的 Zone。

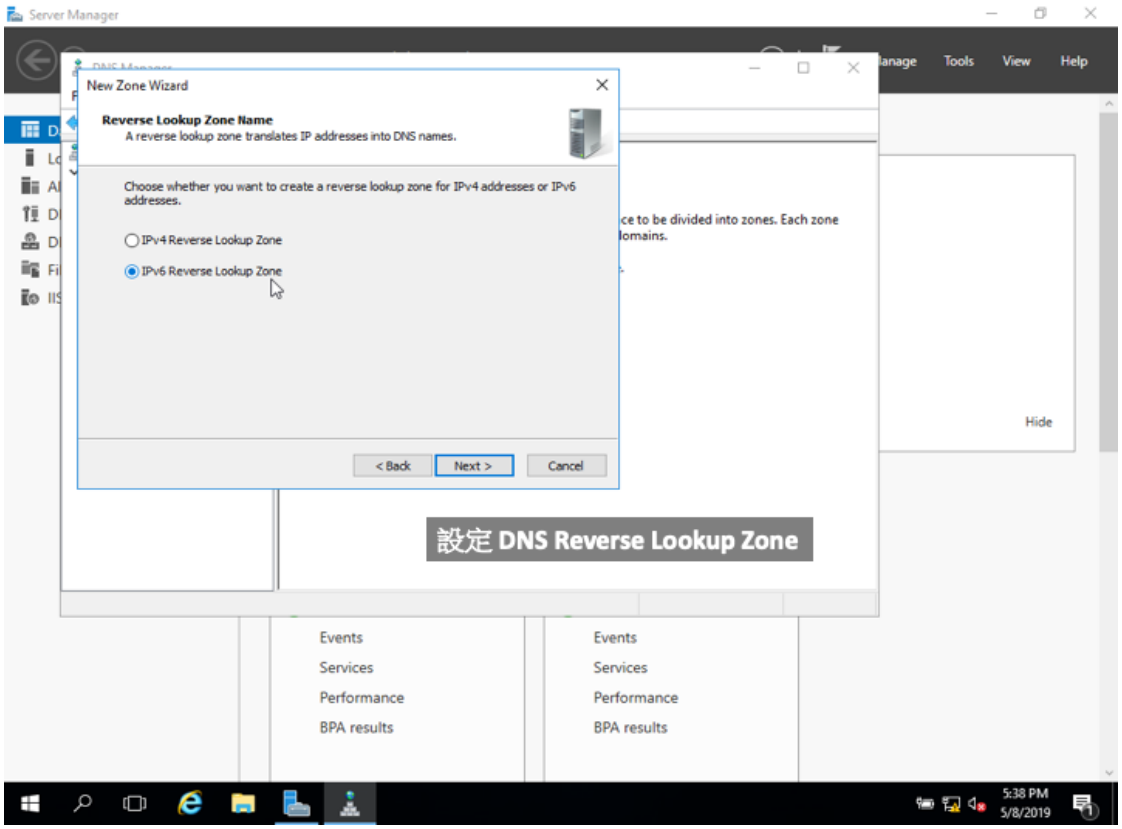



圖 40 Windows 2016 選擇 IPv6 Reverse lookup zone

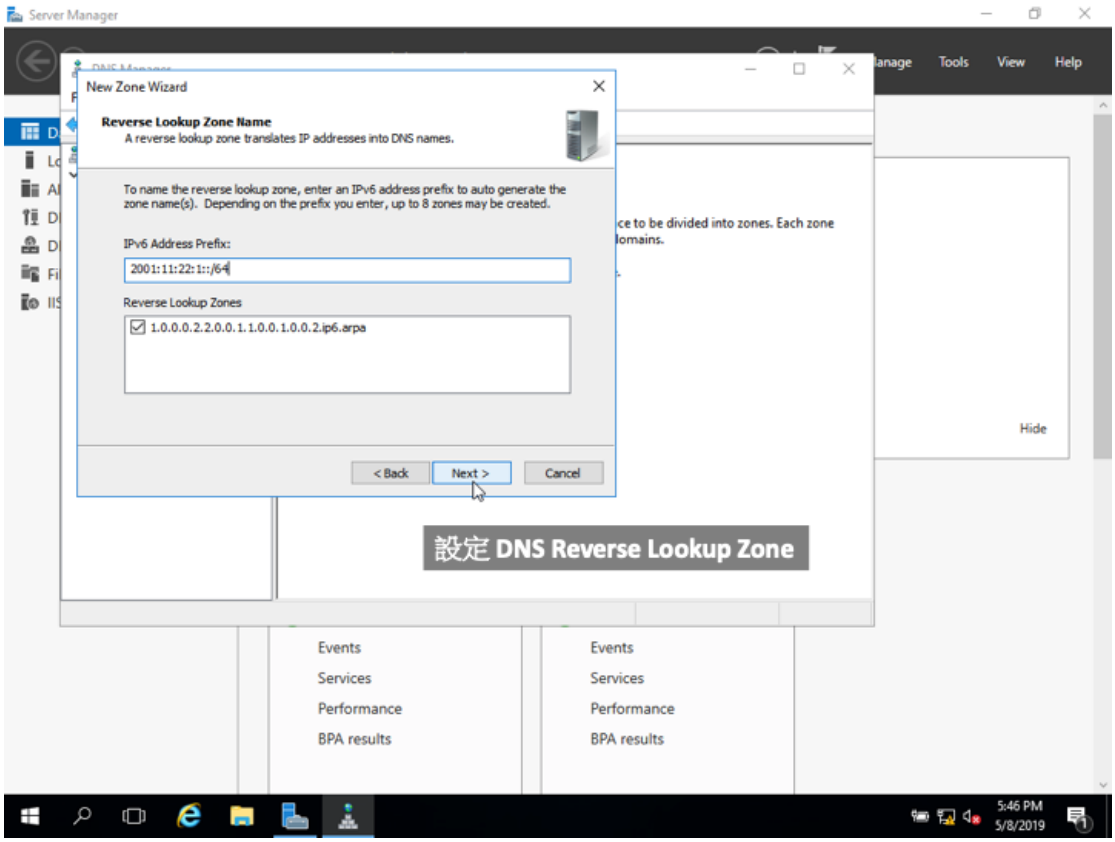


圖 41 Windows 2016 設定 DNS reverse lookup zone 輸入 IPv6 位址

在這裏一樣需要為反解建立一個檔案，用來保存反解記錄。

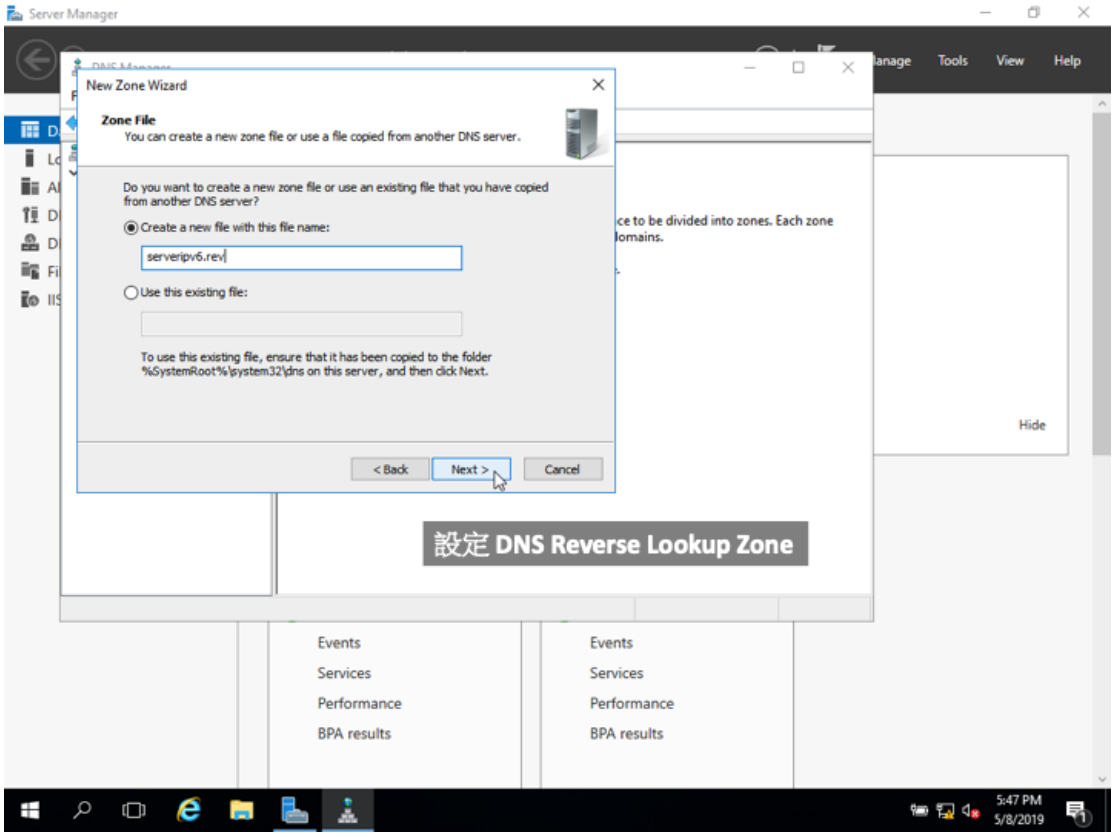



圖 42 Windows 2016 建立 DNS reverse lookup zone file

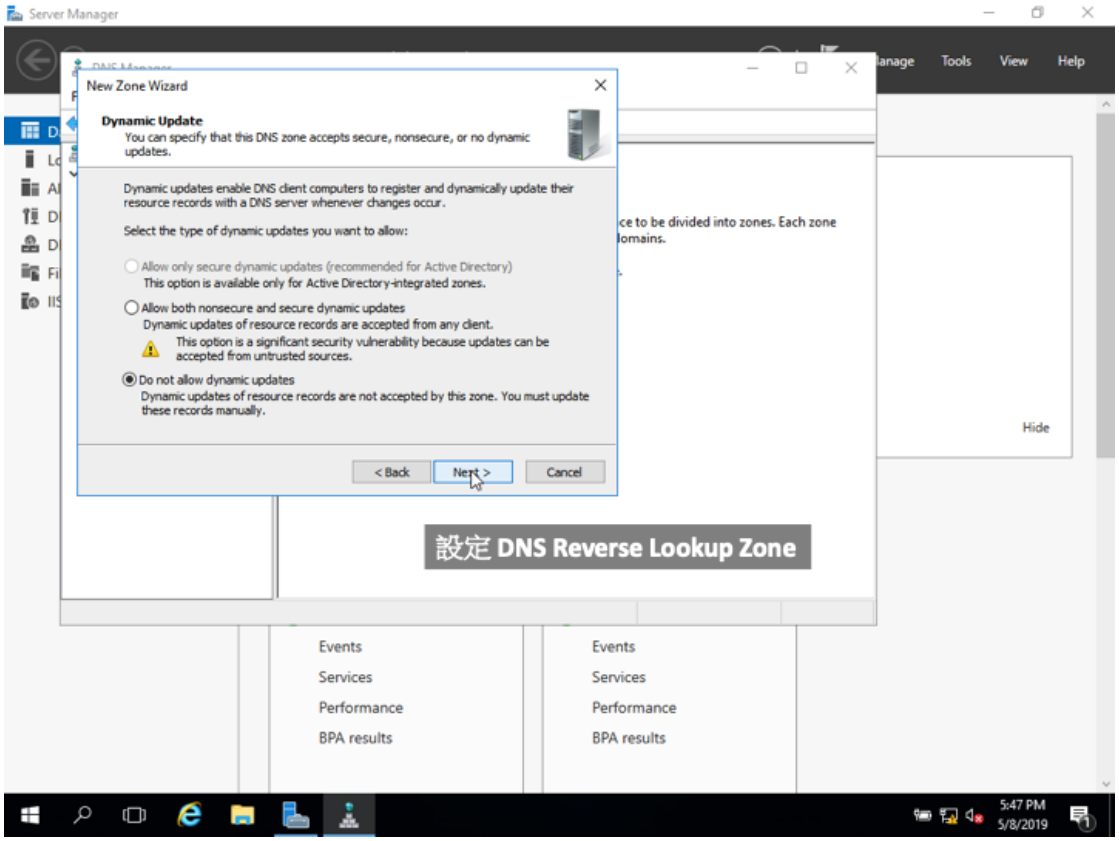



圖 43 Windows 2016 DNS reverse lookup zone 動態更新設定

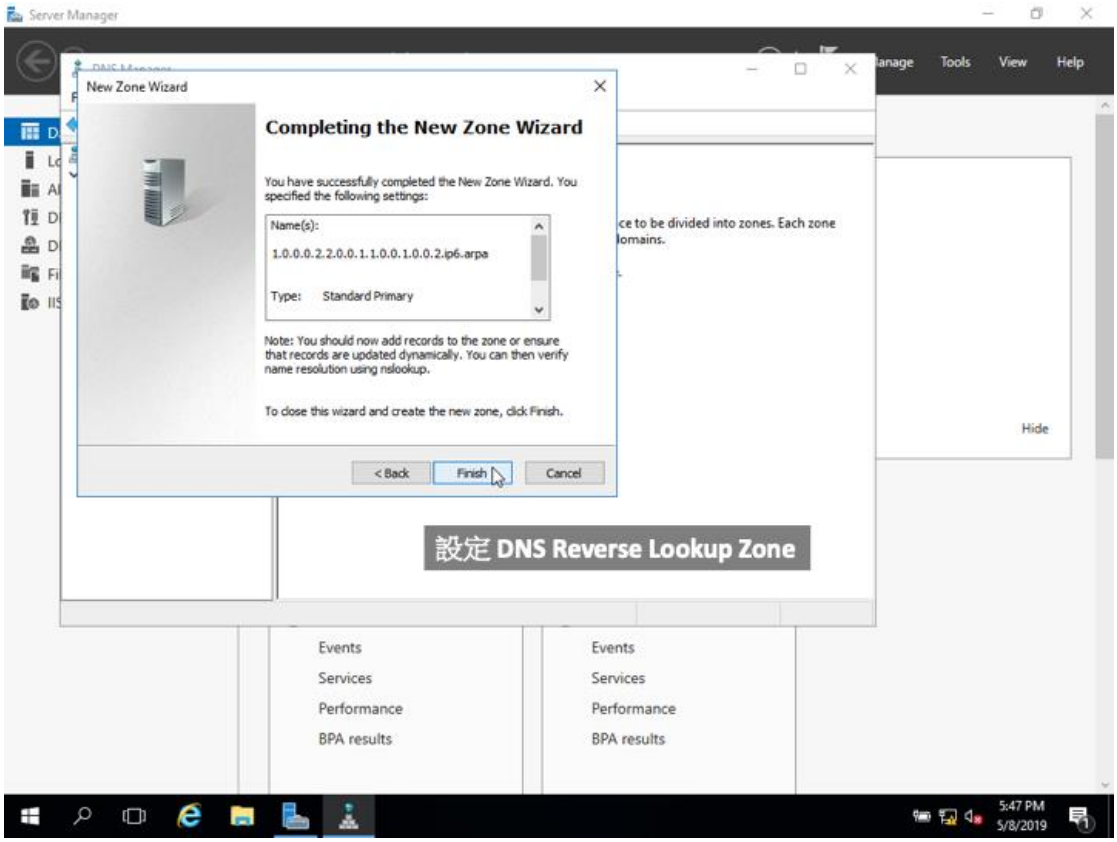



圖 44 Windows 2016 DNS reverse lookup zone 設定確認畫面

從這個視窗，可以看到目前設定成果。我們已經設定好一台 ns1 跟 www 的 IPv6 位址。之後當使用者查詢 ns1.server.tw 時，可以查詢到對應的 IPv6 位址，同樣的，當使用者要連到 www.server.tw 時，也可以查到對應的 IPv6 位址。

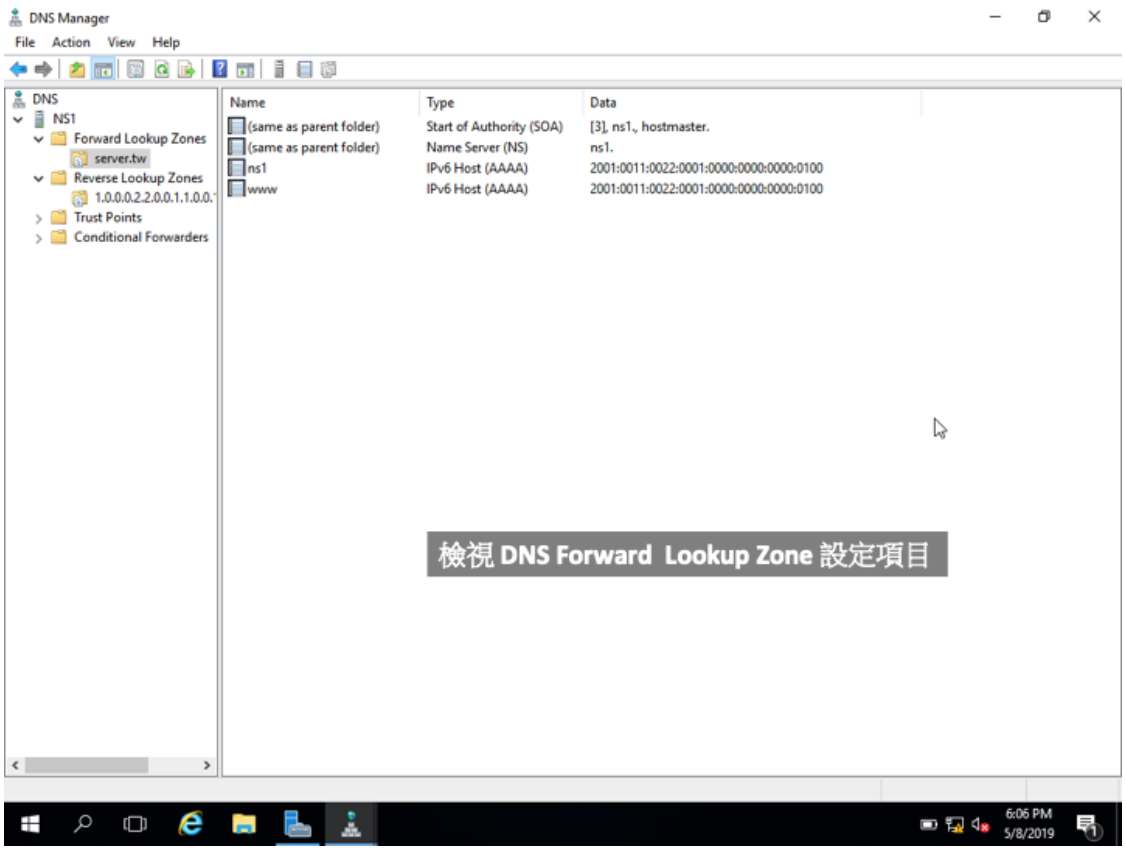



圖 45 Windows 2016 檢視 DNS forward lookup zone 設定結果

這個畫面是顯示反解的資訊，從 IP 可以反查到網域名稱。

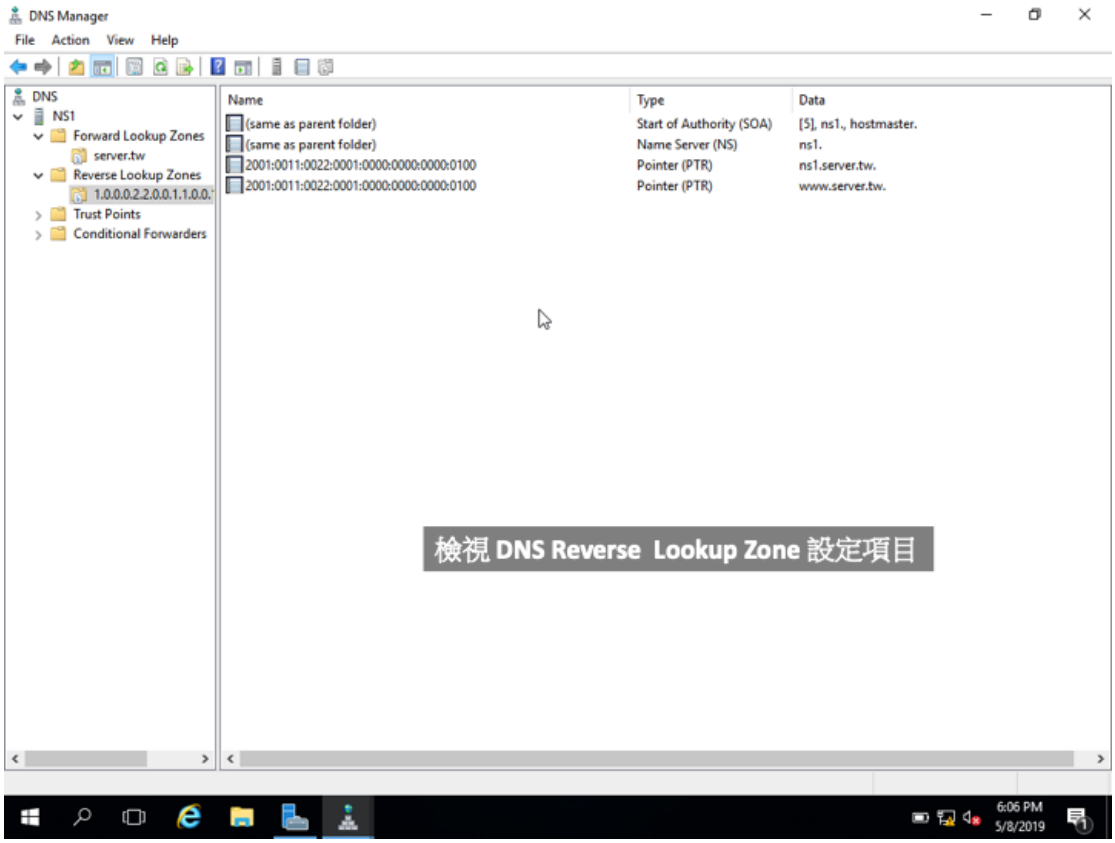



圖 46 Windows 2016 檢視 DNS reverse lookup zone 設定項目

設定完成之後，我們可以開始利用指令來驗證設定是否正確，可以使用的指令通常是 nslookup 或者 dig。dig 是比較新版的 DNS 查詢工具，可以顯示的資訊比較多，當然指令的參數也比較複雜。例如要查詢 www.server.tw 的 IP 位址時，可以用 nslookup www.server.tw。如果用 dig 指令，可以用 dig aaa www.server.tw +short。

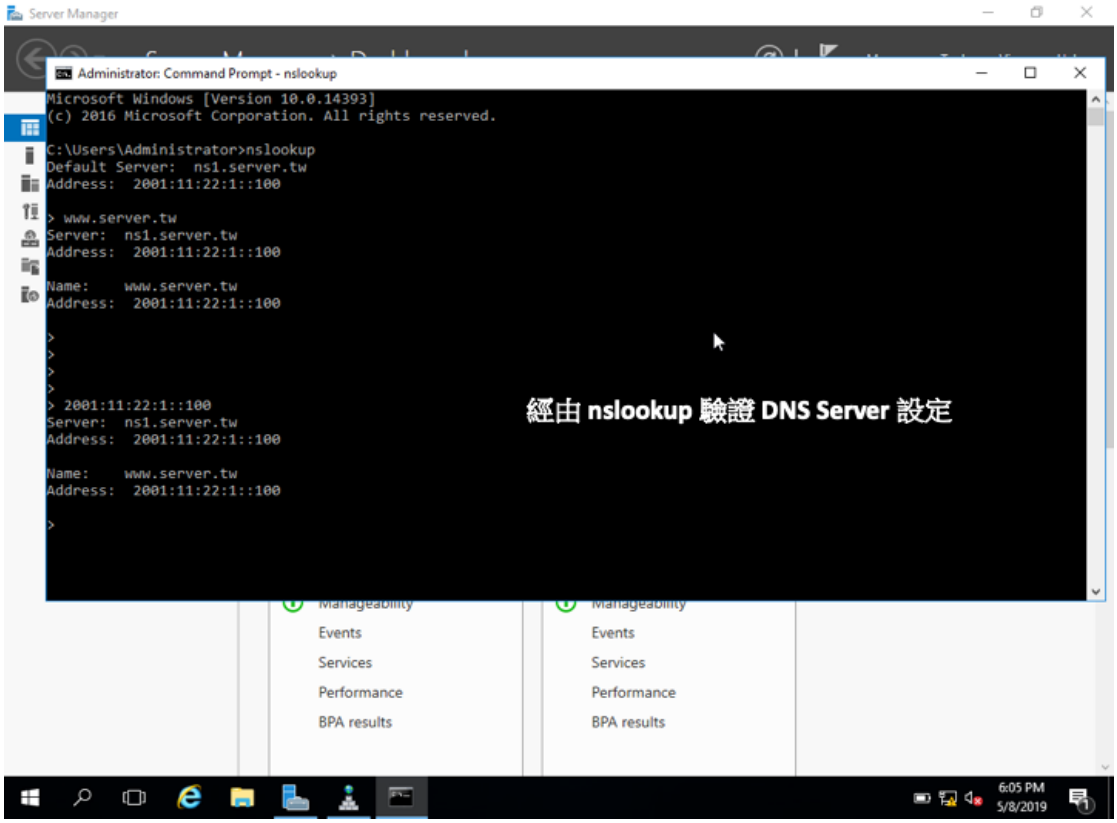


圖 47 Windows 2016 以 nslookup 指令驗證結果

接著我們進行 IIS 網頁伺服器的設定，IIS 跟 Apache 提供類似的功能，主要是用於架設網站，對外提供服務。也可以用於內部的企業系統，例如網站版本的差勤系統或者會議室登記系統等。

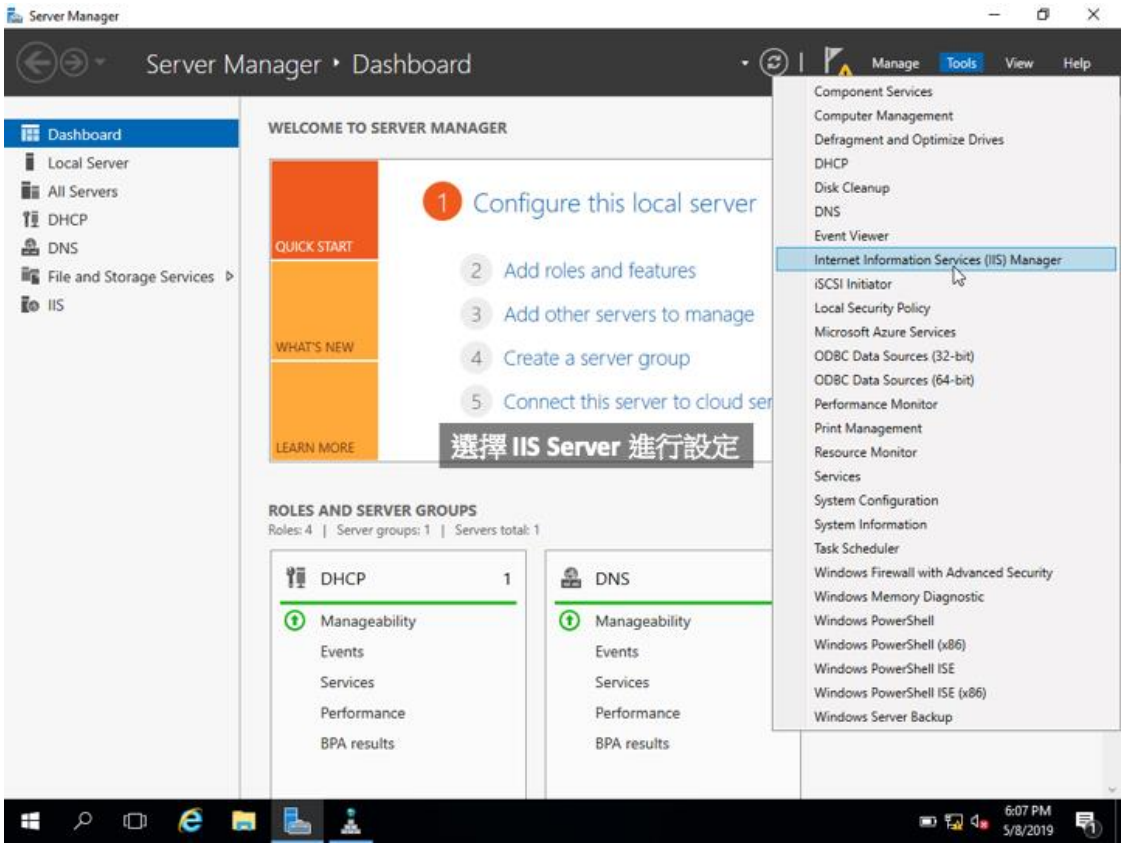


圖 48 Windows 2016 選擇 IIS server

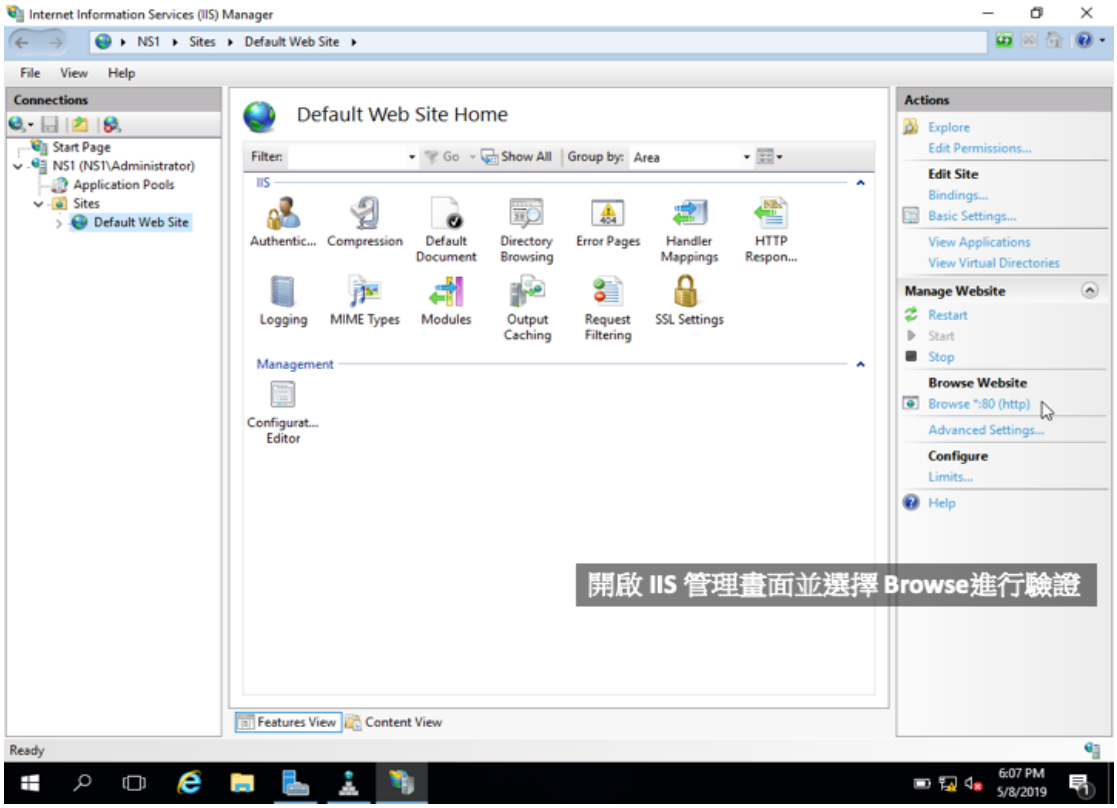



圖 49 Windows 2016 開啟 IIS 畫面

IIS 設定完成之後，也一樣使用 nslookup 或者 dig 去驗證網址對應的 IP 是否設定正確。

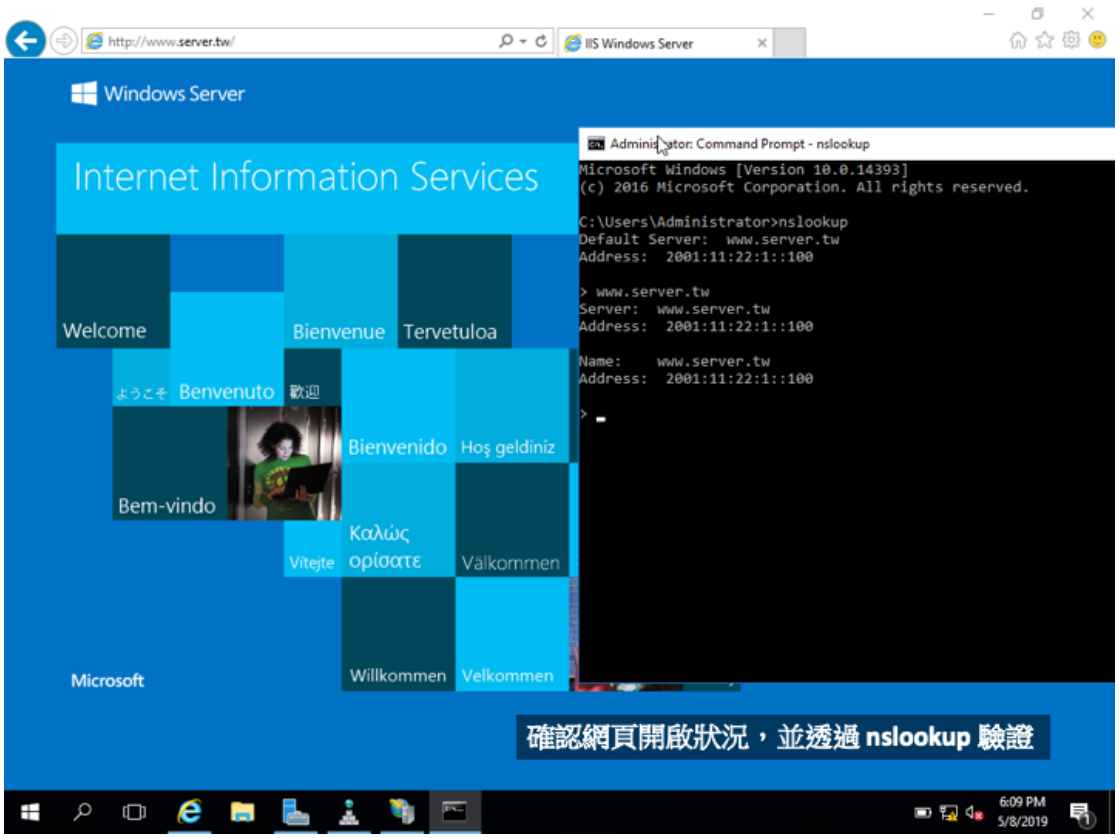



圖 50 Windows 2016 設定 IIS 並驗證網頁服務

接著我們要進行 DHCP server 的設定。DHCP server 負責動態配置 IP 給其他主機，讓其他主機可以取得 IP 之後連網。

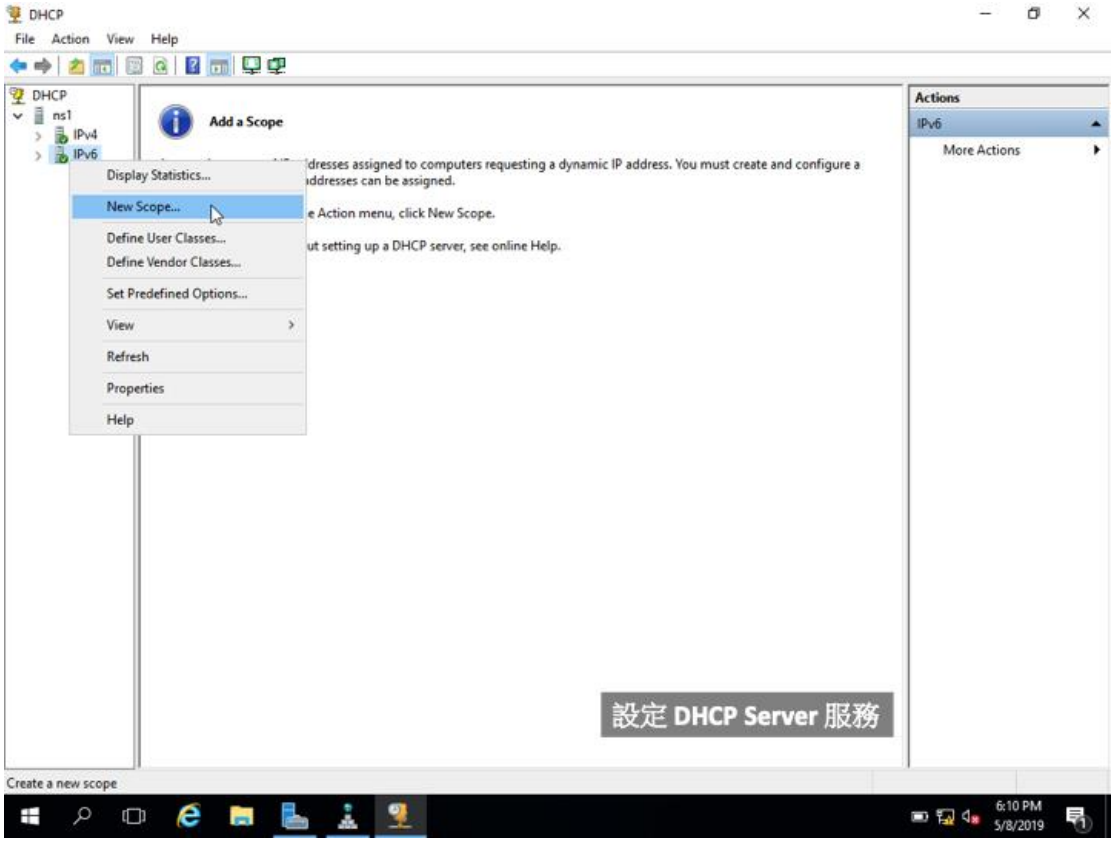



圖 51 Windows 2016 設定 DHCP 點選 new scope

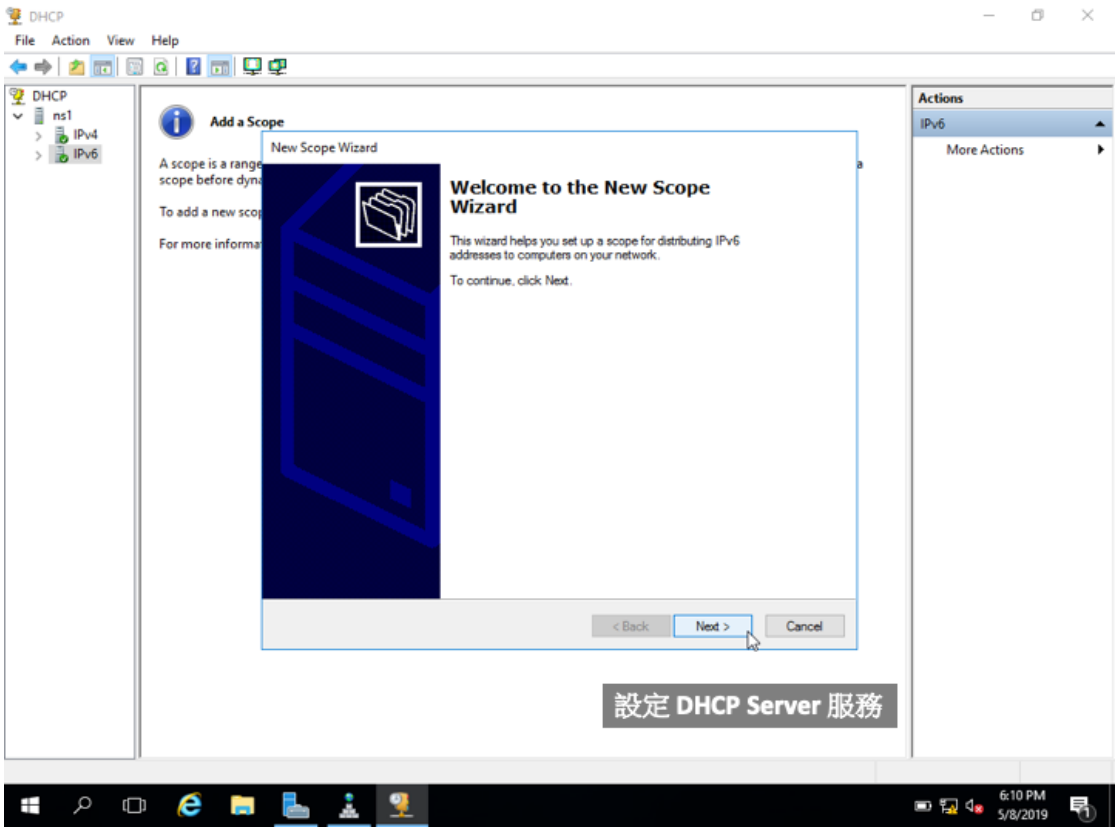



圖 52 Windows 2016 設定 DHCP 歡迎畫面

DHCP Server 因為是負責動態配置 IP，所以要指定可以分配出去的 IP 範圍，此時可以注意到，視窗內會將 IP 位址的前半段變成固定不可更動，但後面才是要可以分配給 DHCP client 的 IP 範圍。任何 DHCP client 透過跟 DHCP server 索取 IP 一定是落在你設定的這個範圍區間。

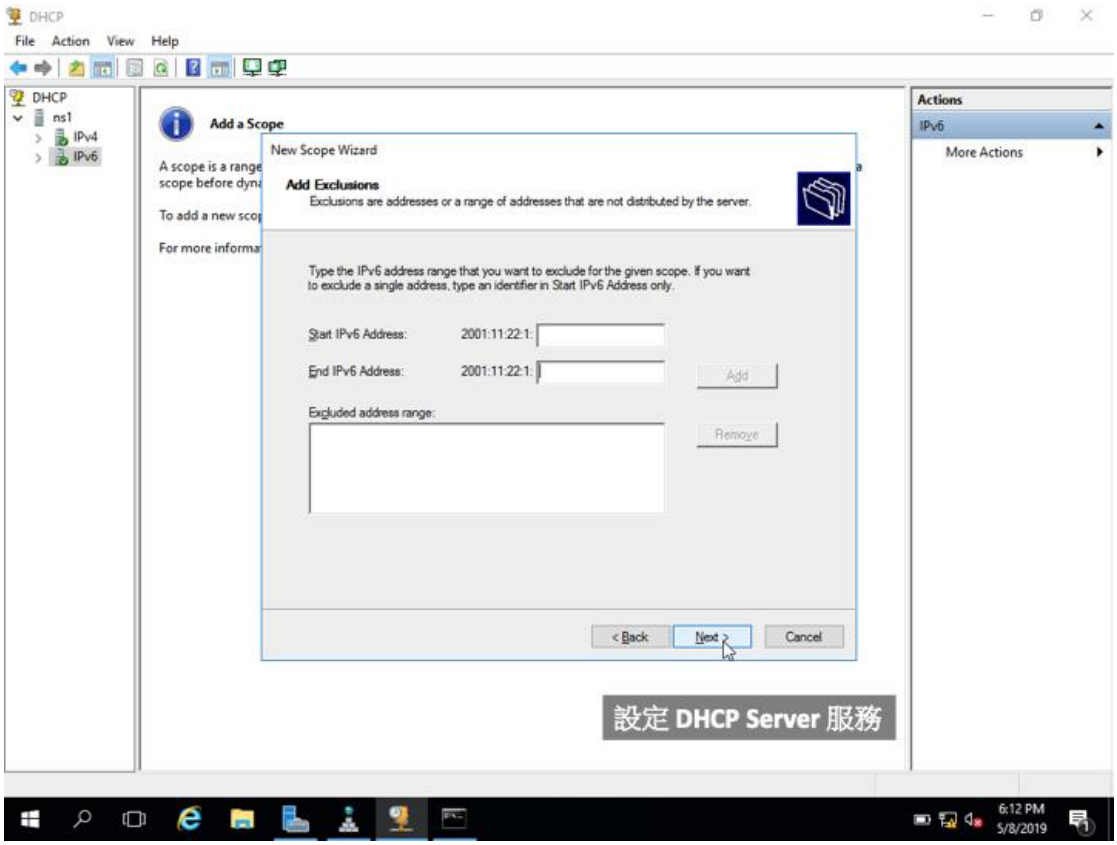



圖 53 Windows 2016 輸入 DHCP server

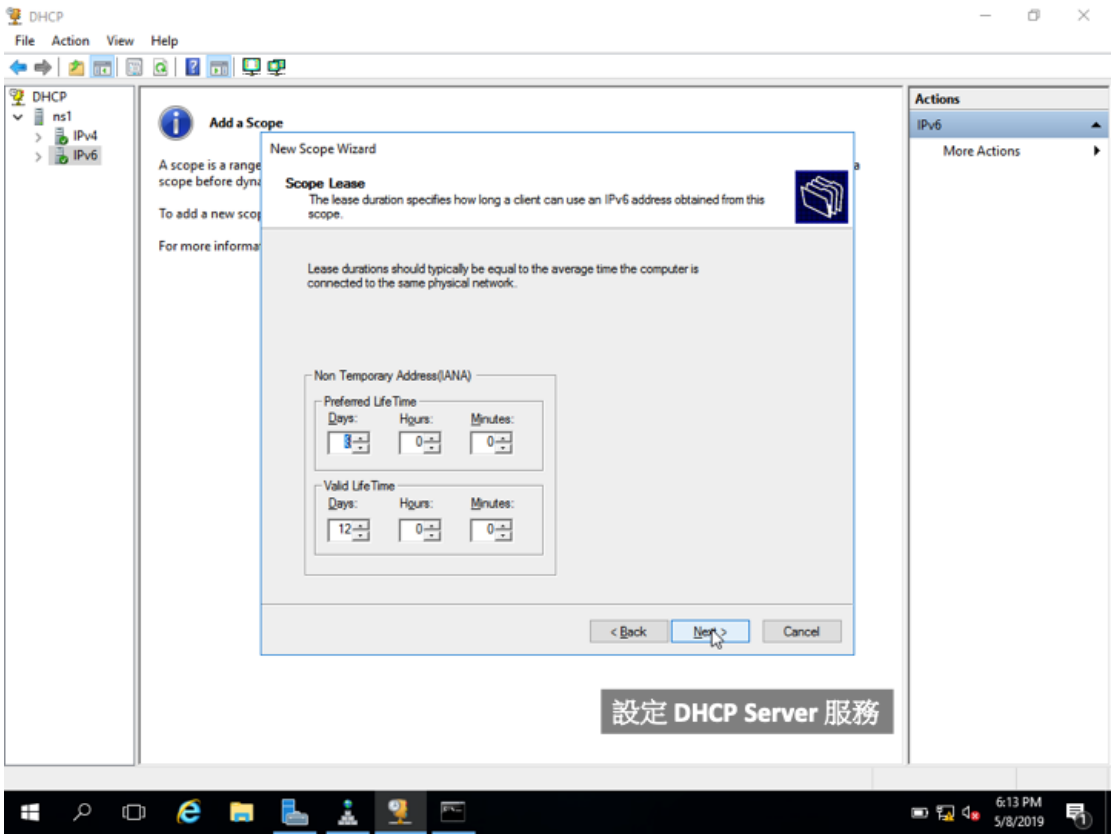



圖 54 Windows 2016 設定 scope lease

至於如何驗證 DHCP server 是否有正常運作呢? 只要使用另外一台電腦，並讓該電腦的 IP 取得方式不是手動輸入，而是自動取得。此時就是使用 DHCP 的方式跟 DHCP server 拿到 IP 位址，只要可以拿得到 IP 位址，且 gateway 及 DNS 都正常，再來就是測試連到網路是否通過，就表示 DHCP server 配置成功。

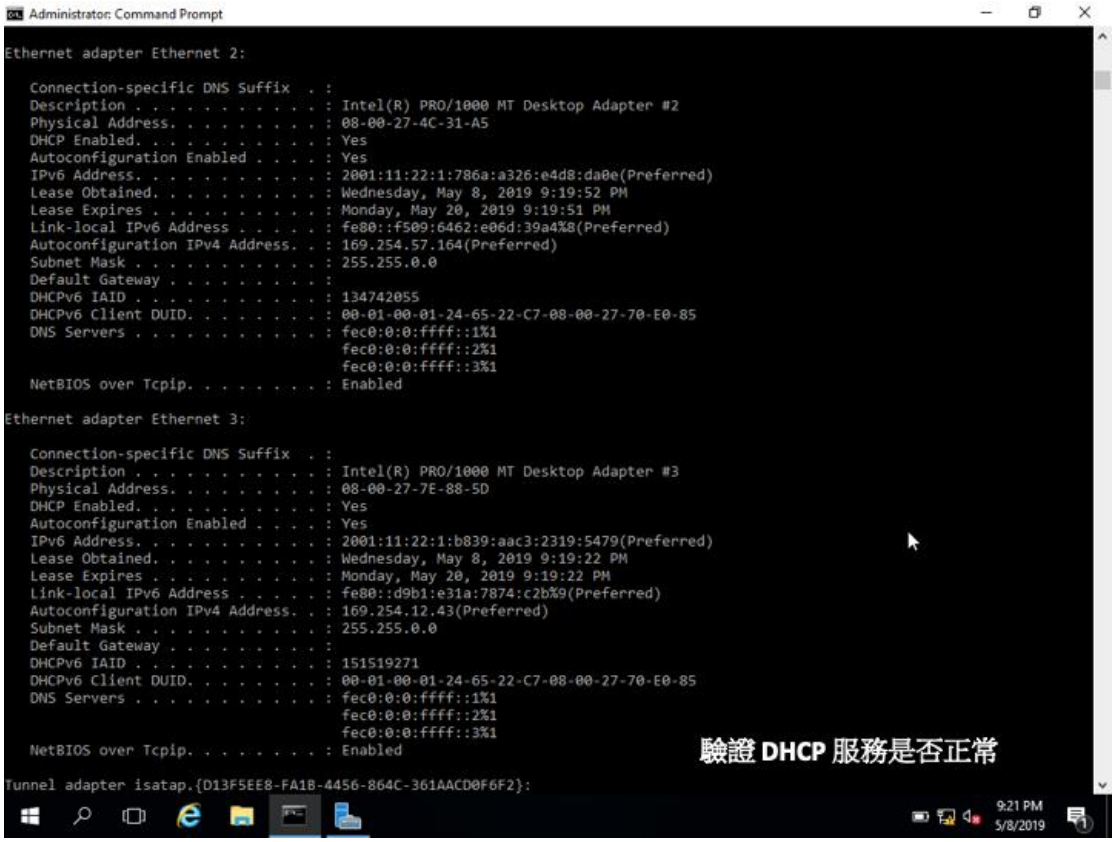


圖 55 Windows 2016 驗證 DHCP Server 服務是否正常

## 第五節 Windows 2019 啟用 IPv6

先開啟網卡設定，開啟位置可以透過「控制台」，也可以以滑鼠點選右下角的網路卡圖示，並依據跳出的浮出選單，選擇網路控制中心，進入網卡設定。

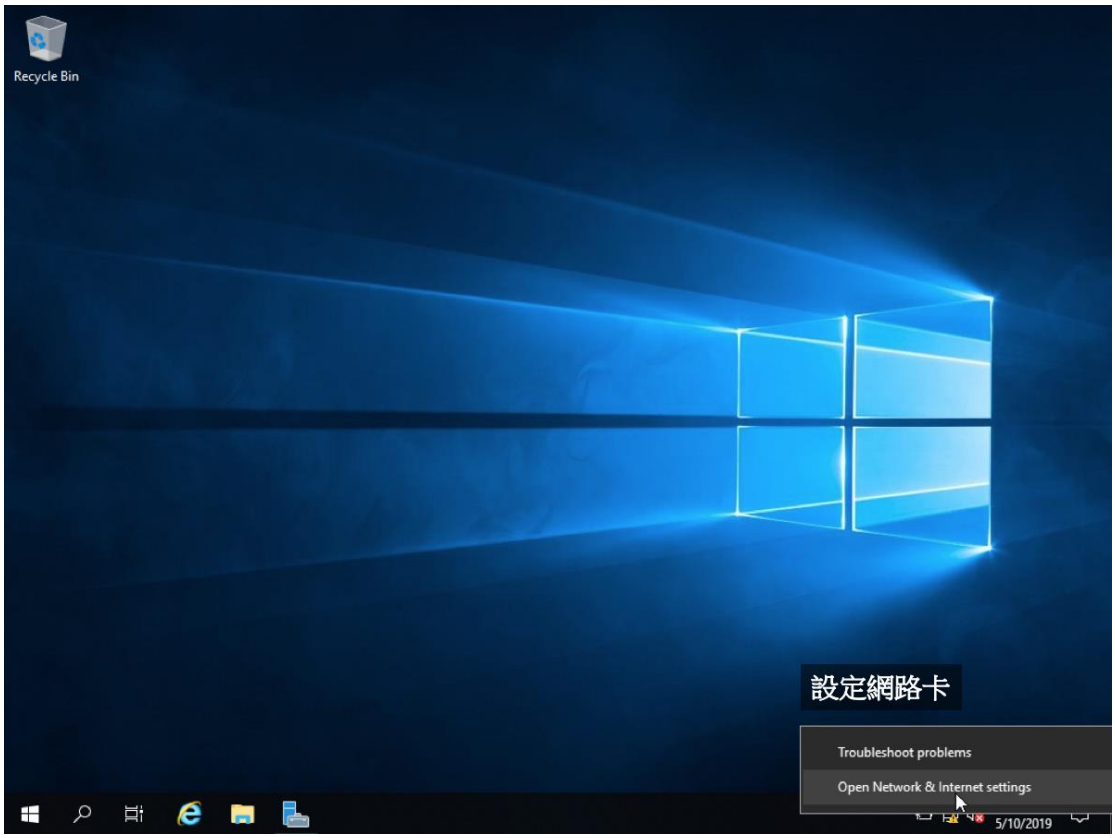



圖 56 Windows 2019 設定網卡

進入網路設定中心並選擇連上網的網卡之後，可以進行網路設定，記得選擇 TCP/IP，並依據配置的 IP 進行設定，需要設定的項目會包括 IP 位址及閘道器等，必要的話，也需要設定 DNS 負責網址跟 IP 之間的轉換。

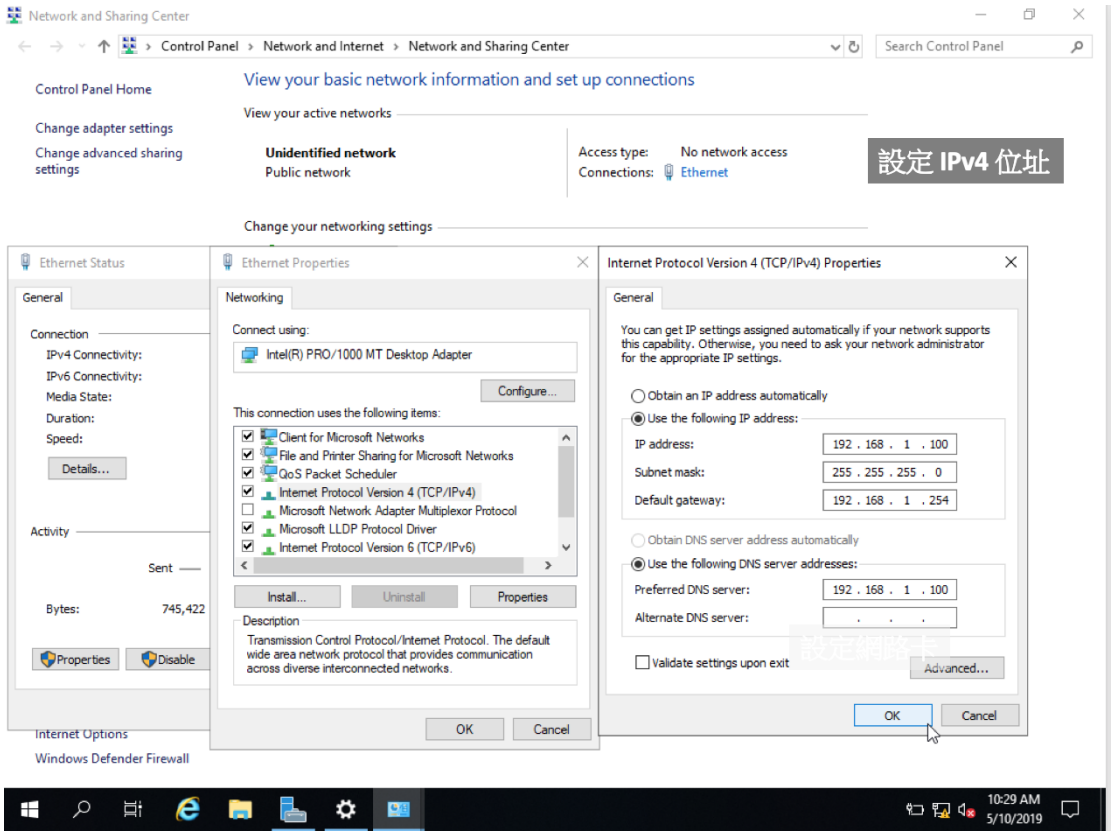



圖 57 Windows 2019 輸入 IPv4 位址

依據從 ISP 所取得的 IPv6 位址，填入到下圖的表單內。需要輸入包括 IPv6 位址、IPv6 的 prefix、網路出去的 gateway，還有 DNS server 的 IPv6 位址。

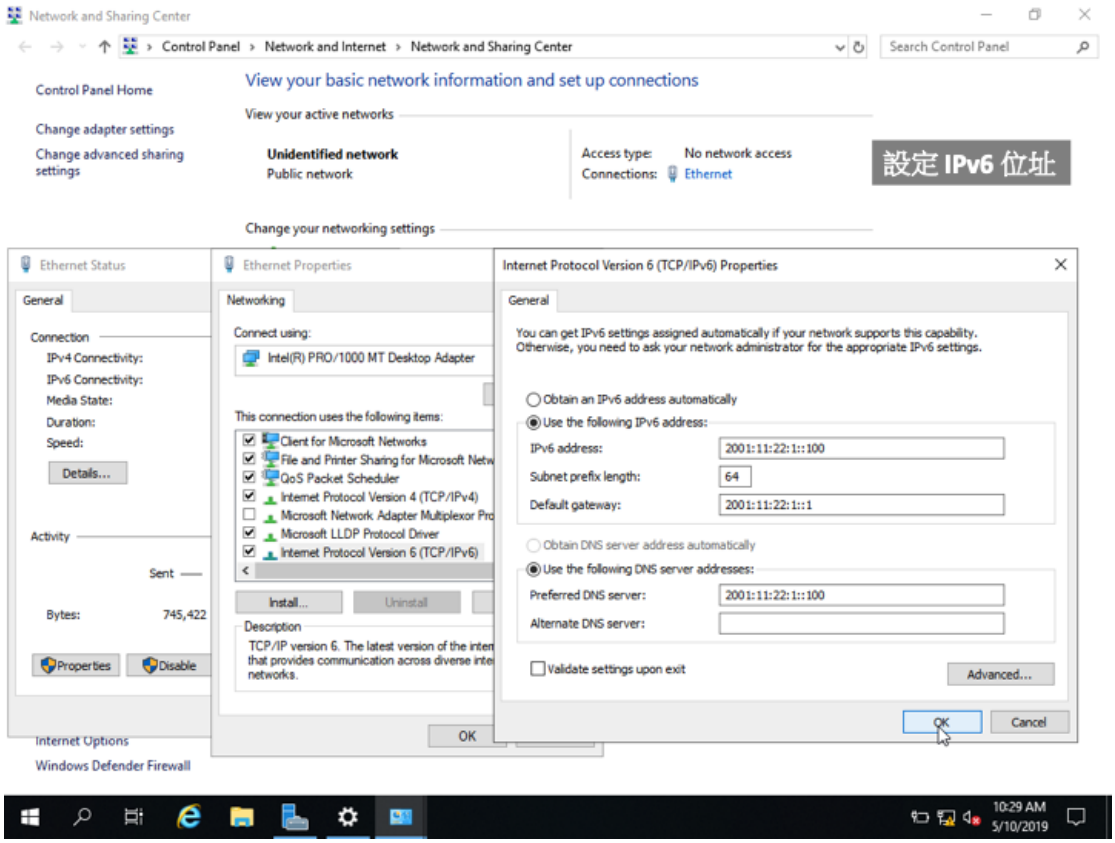



圖 58 Windows 2019 輸入 IPv6 位址

接著設定主機的 hostname，此 hostname 只是用於辨識跟顯示這台機器的顯示名稱。在設定完畢之後，因為已經更改了網路介面卡設定，系統會要求要重開機以啟用新的設定。此時請按下確認立即重啟，讓系統自動重新啟動。

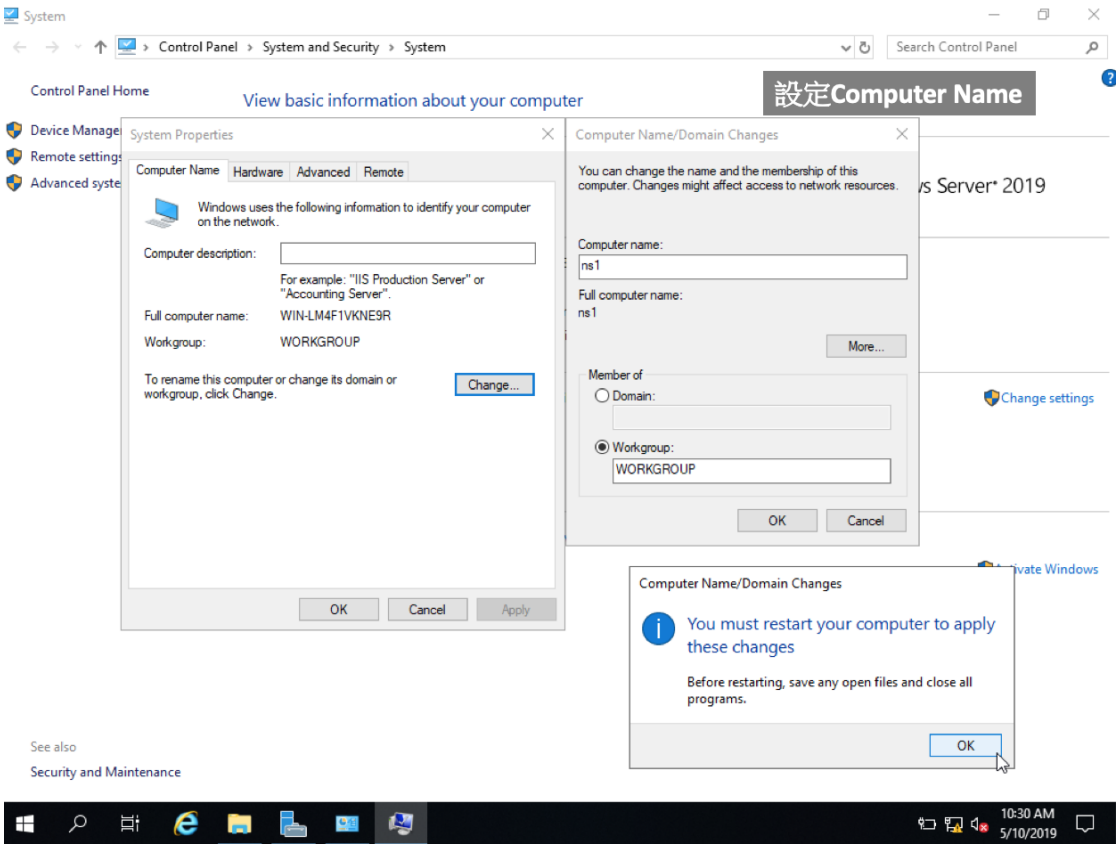



圖 59 Windows 2019 設定 hostname

重新開機進入系統之後，網卡部分已經設定完成，接著我們要設定本台主機的角色跟規則。

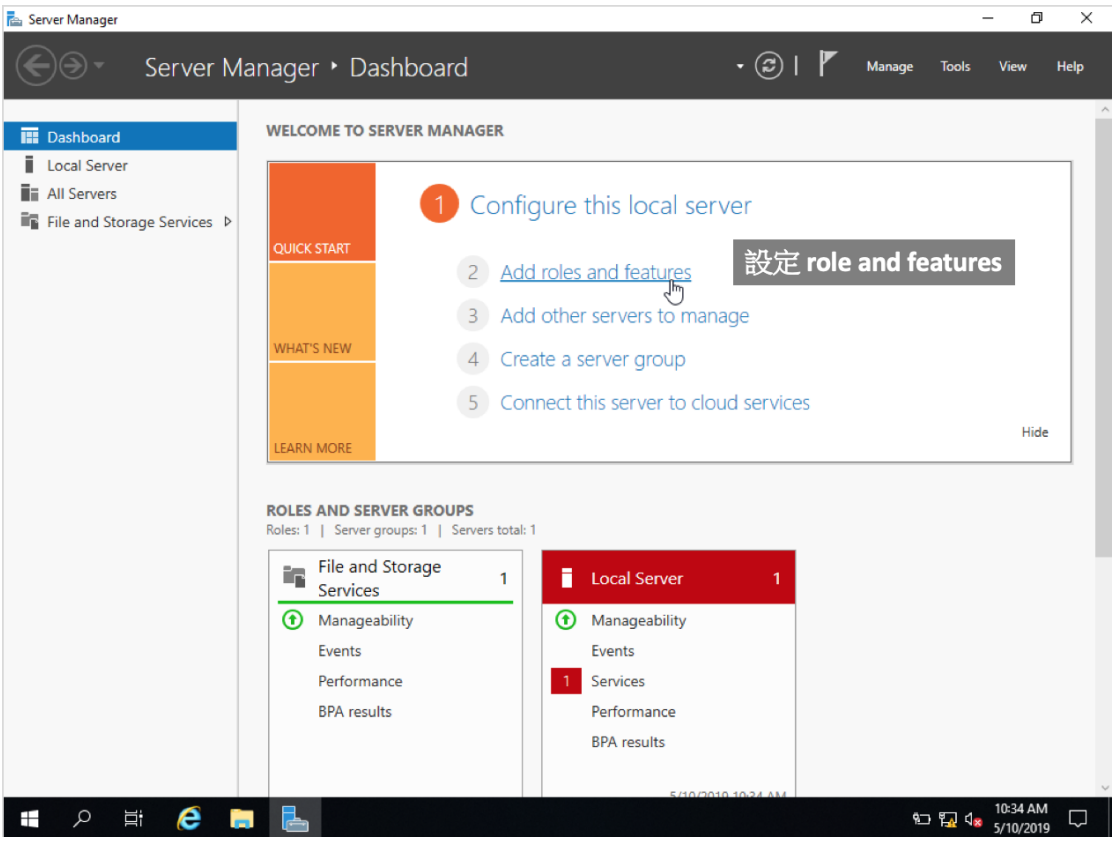



圖 60 Windows 2019 設定 roles and features

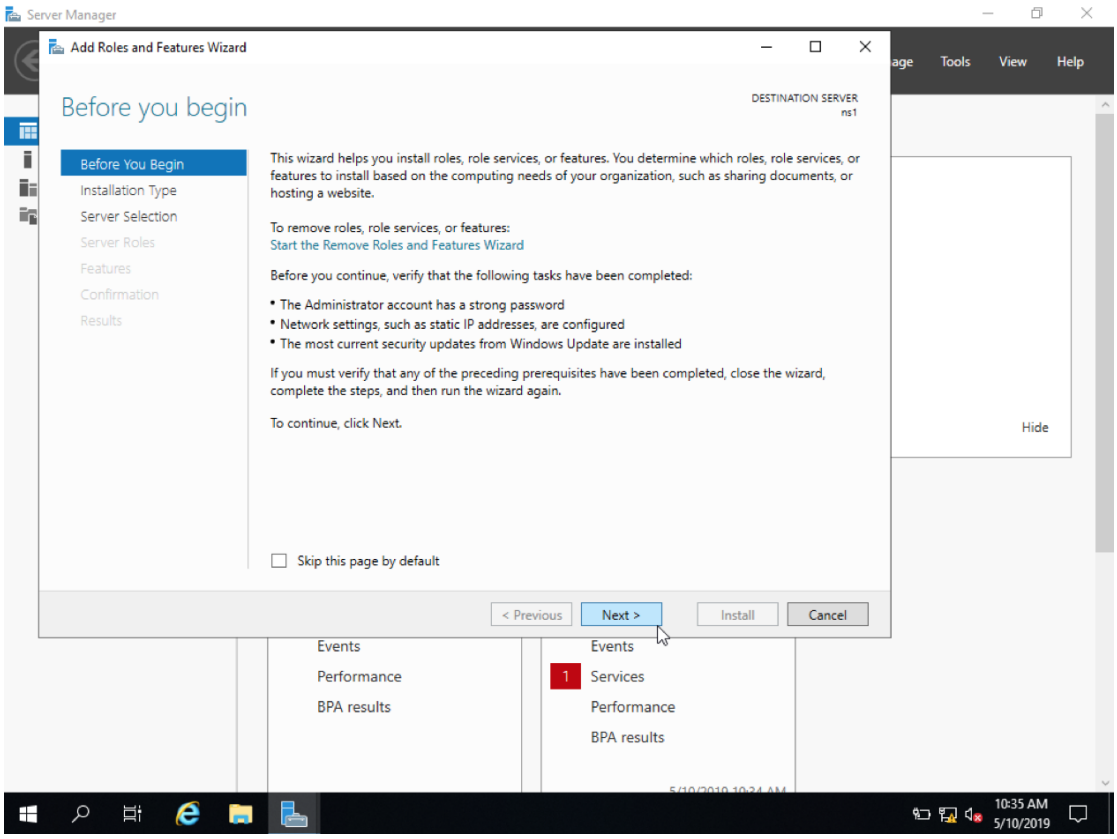



圖 61 Windows 2019 警示頁面

在這個畫面，請選擇第一個項目（第二個項目是給 VM 虛擬機使用）。

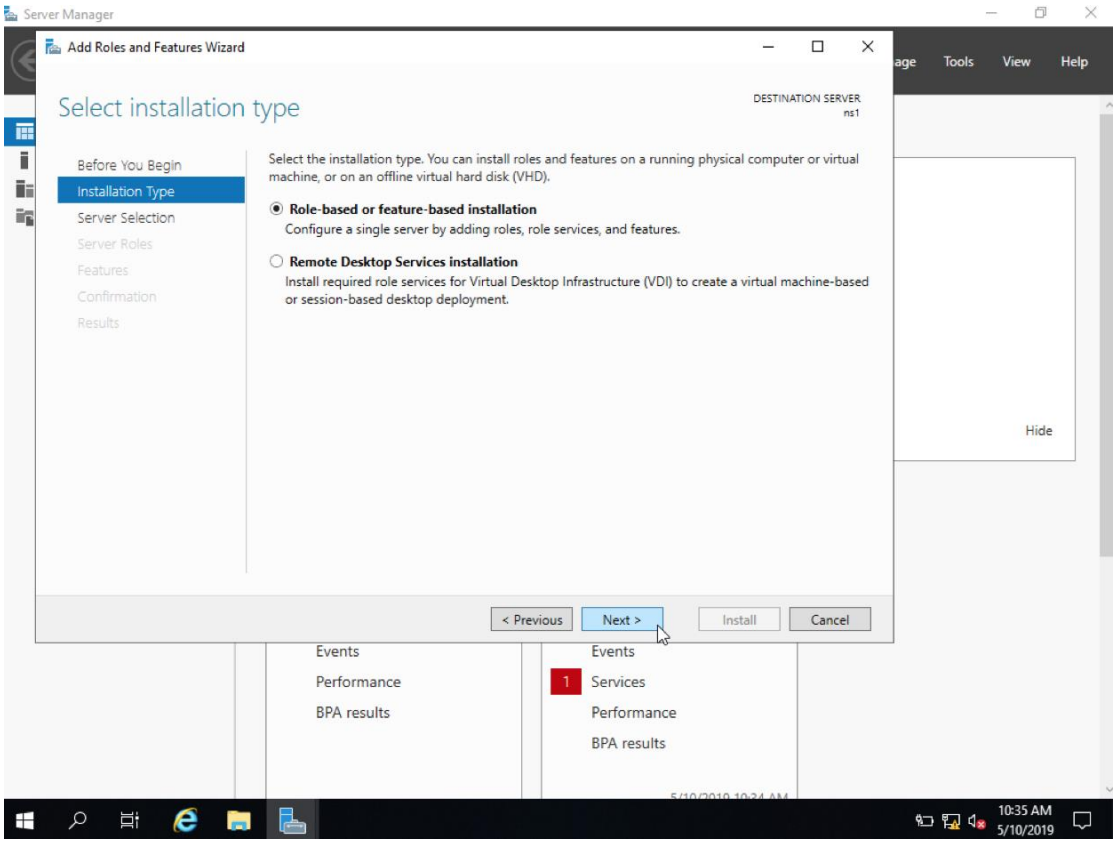



圖 62 Windows 2019 選擇安裝方式

選擇已經建立好的主機，由於此時只有一台，故直接選擇該台主機即可。

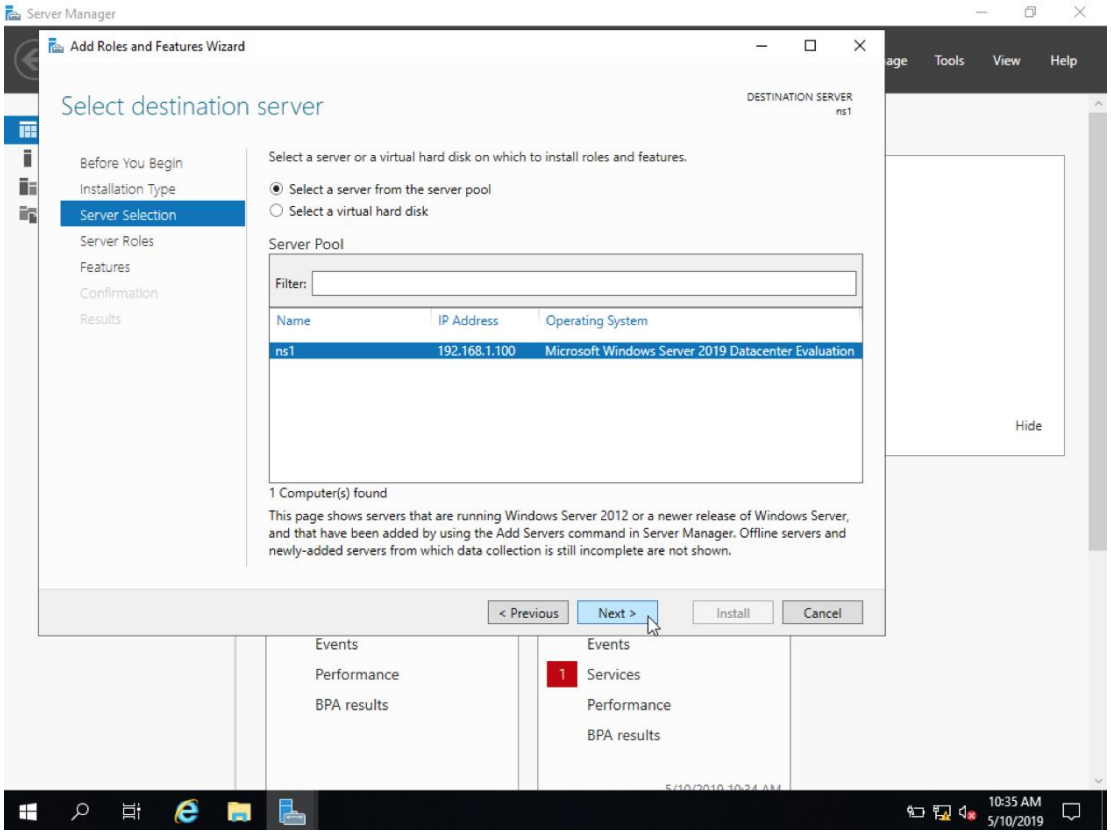



圖 63 Windows 2019 選擇目的主機

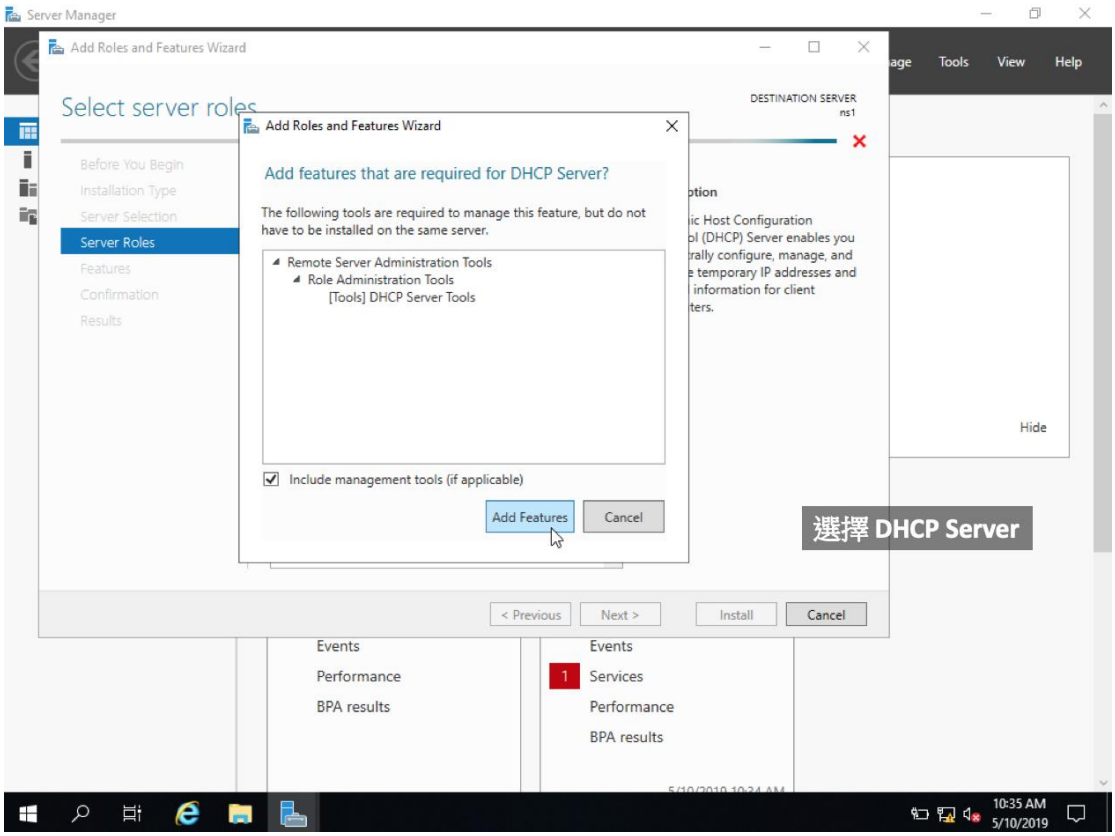



圖 64 Windows 2019 設定 DHCP Server

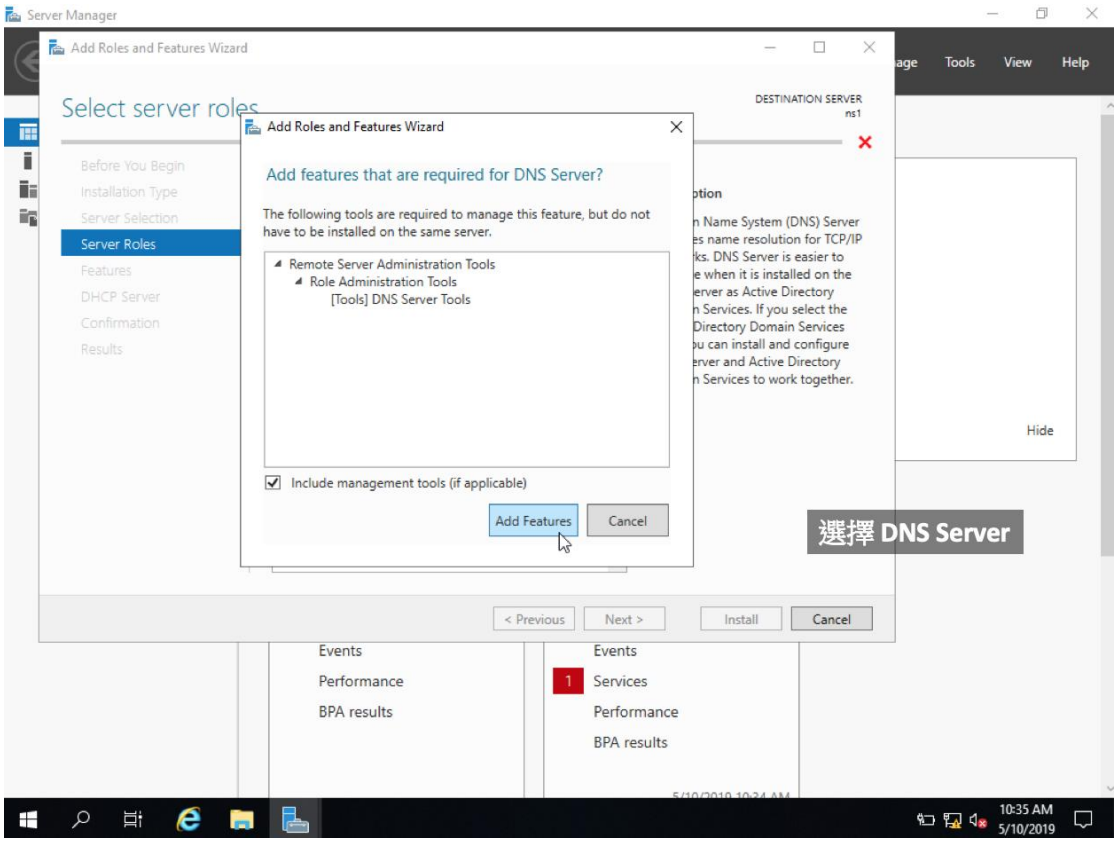



圖 65 Windows 2019 選擇 DNS Server

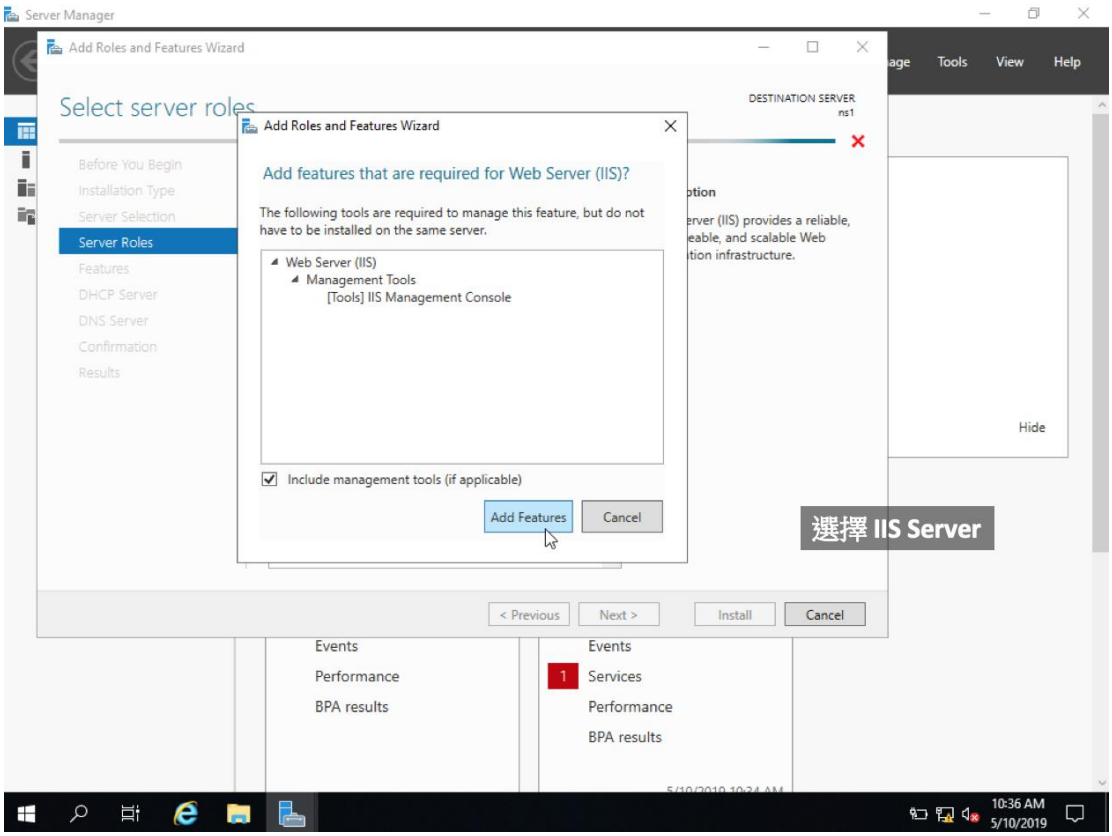



圖 66 Windows 2019 選擇 IIS Server

接著，依據視窗指示，選擇要將此主機設定為哪些角色。可以選擇的項目包括 DHCP Server（負責動態 IP 的配置）、DNS Server（負責網域的解析）、Web Server（負責提供網頁服務）。

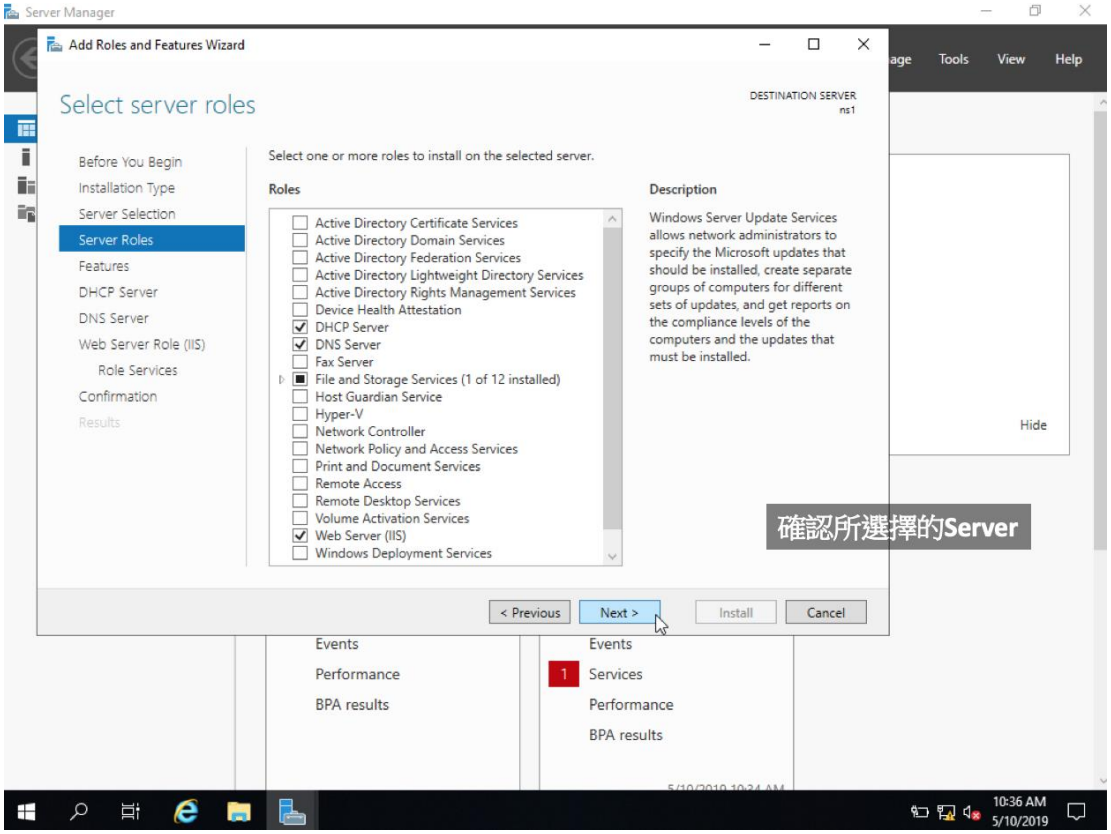



圖 67 Windows 2019 確認所有選擇的項目

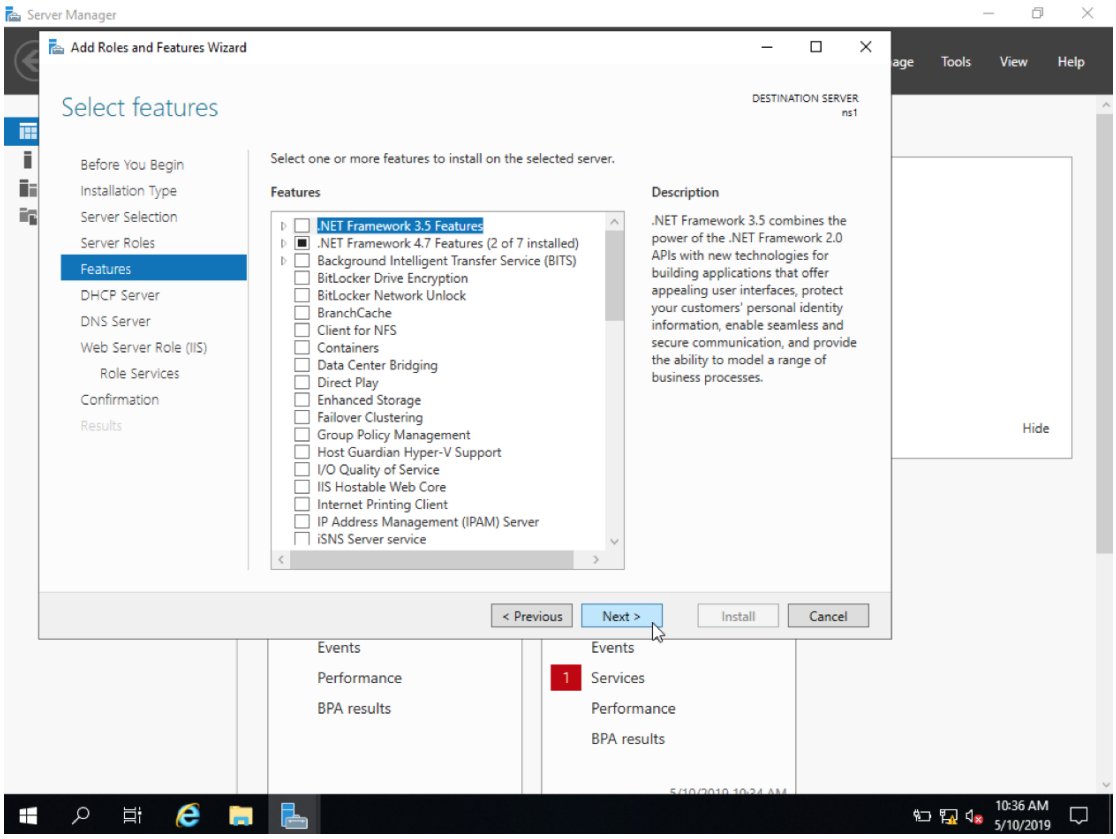



圖 68 Windows 2019 進行安裝

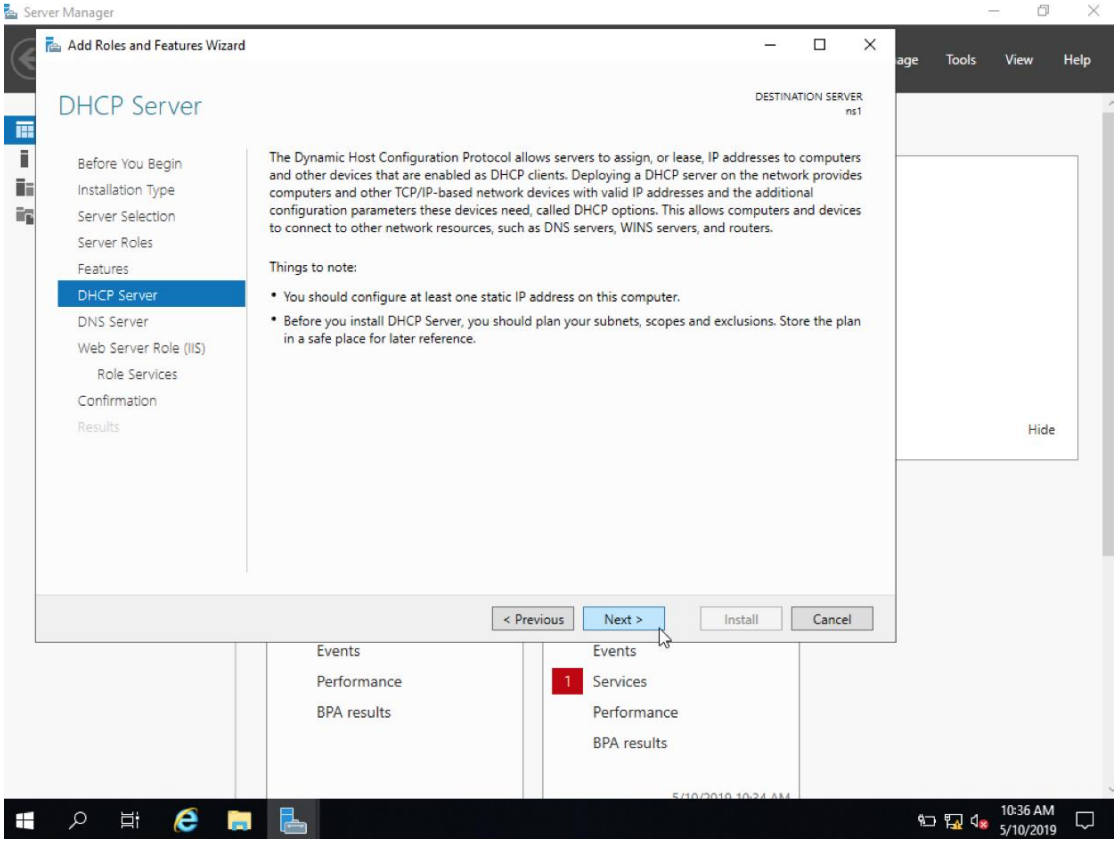



圖 69 Windows 2019 設定 DHCP Server

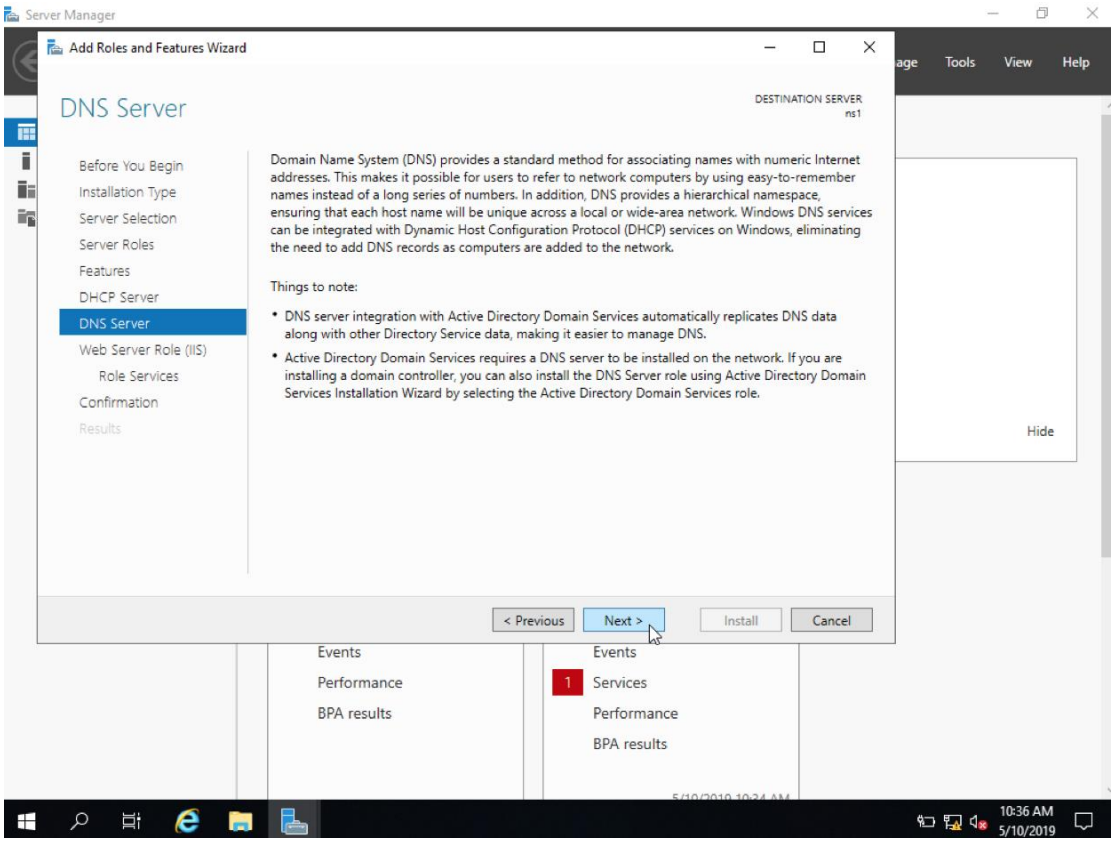



圖 70 Windows 2019 選擇設定 DNS forward

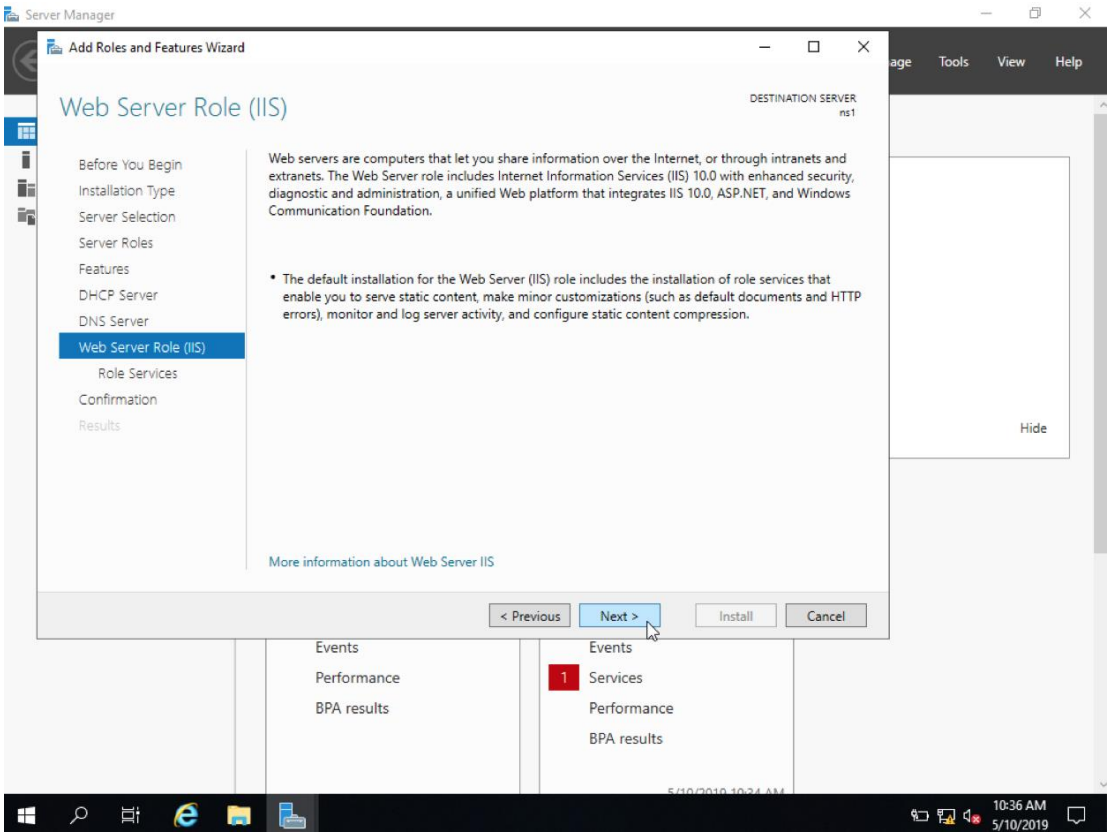



圖 71 Windows 2019 設定 IIS Server 步驟

選擇 IIS，讓主機具備提供網頁服務的功能。IIS 是 Microsoft 自行研發的 Web Server，功能跟 Apache 或 Nginx 類似。這裡可以勾選要讓 IIS 啟用的功能。

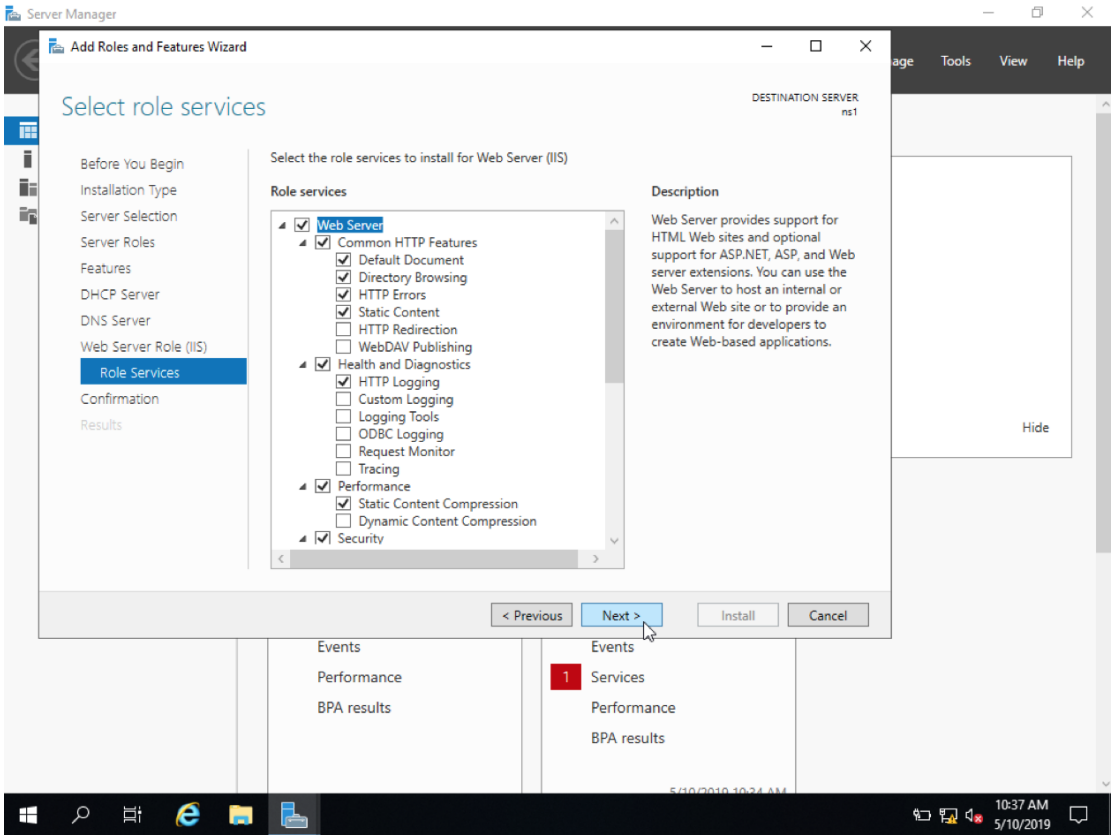



圖 72 Windows 2019 設定 Role Services

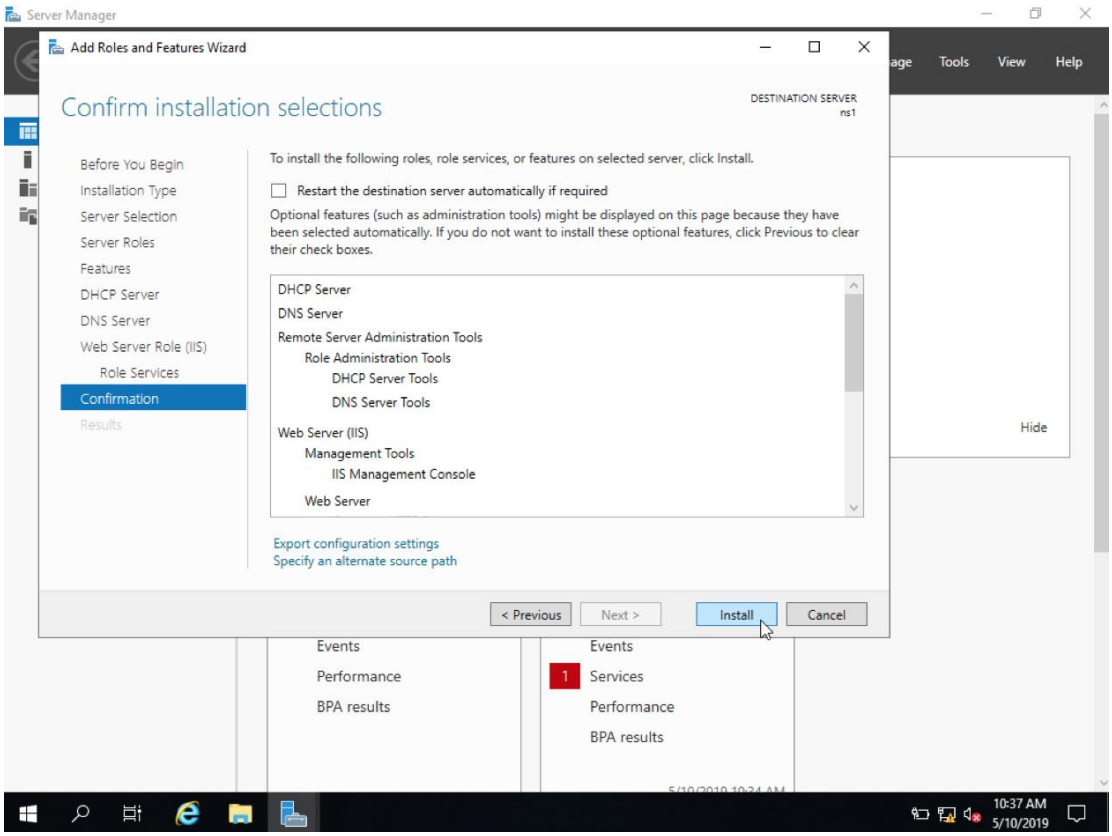



圖 73 Windows 2019 確認視窗

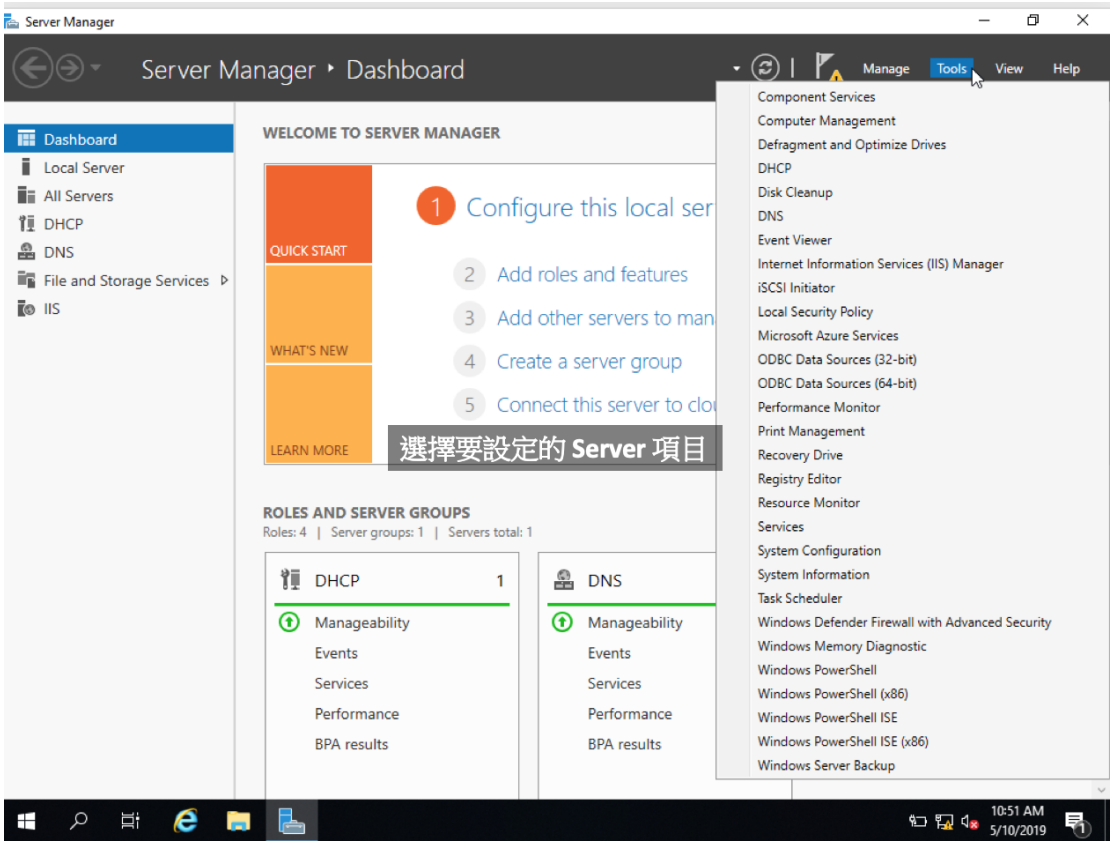



圖 74 Windows 2019 選擇要設定的 Server

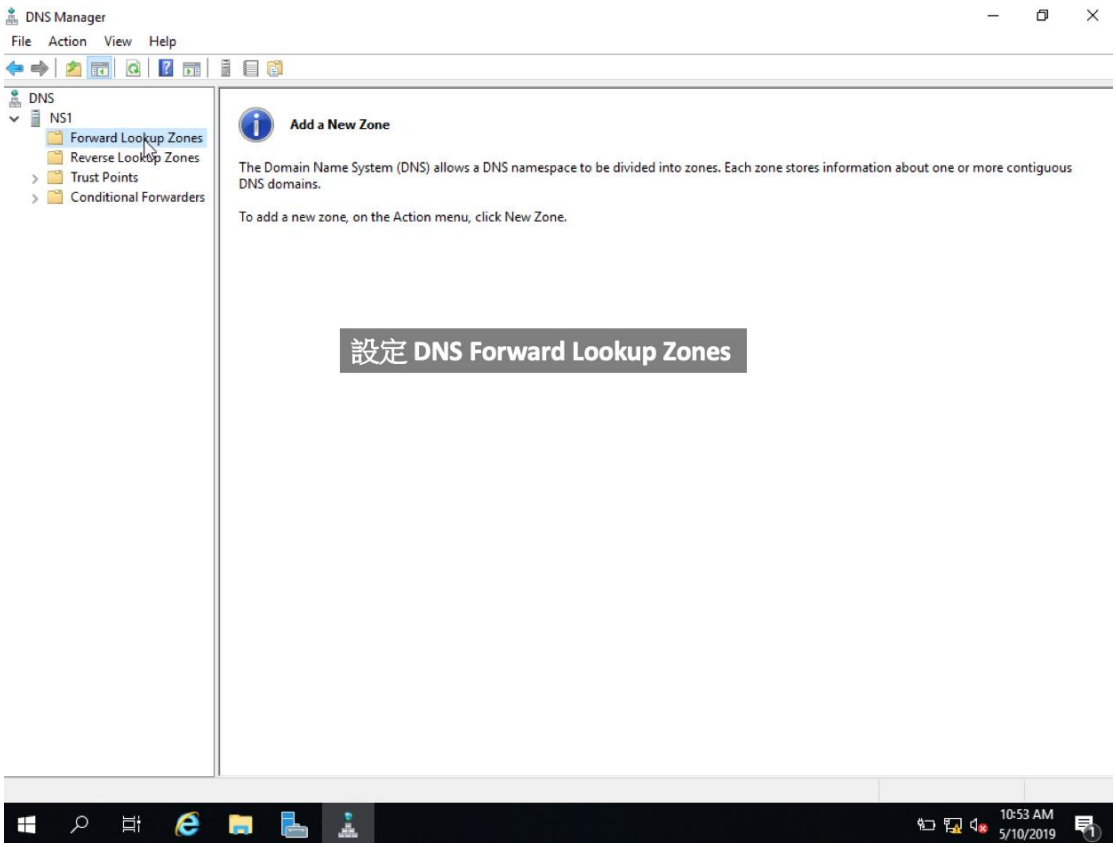



圖 75 Windows 2019 選擇設定 DNS forward lookup zone

進入 DNS 設定選單之後，進行 DNS Zone 的設定。DNS 除了提供查詢網路上「主機名稱」所對應的 IP Address 正解（Forward Lookup）的功能外，也具備將 IP Address 反推「主機名稱」的反解服務（Reverse Lookup）。這裡先設定正解的部分。

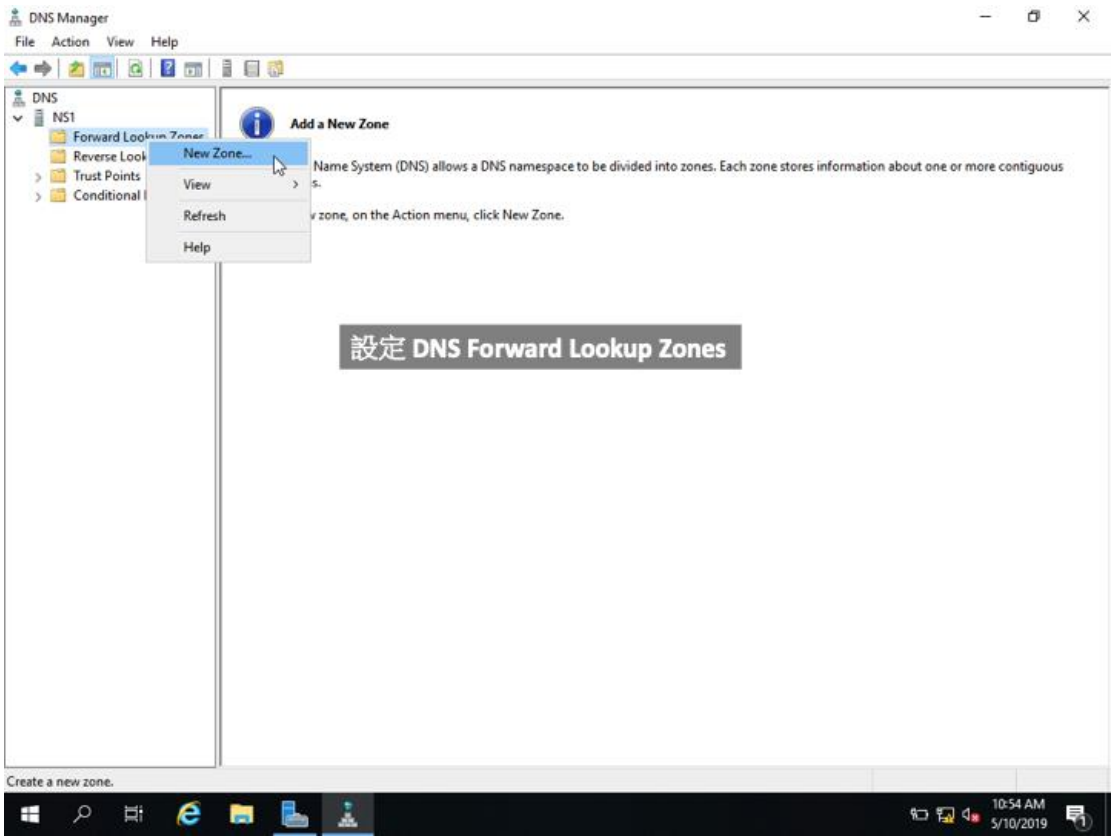



圖 76 Windows 2019 建立 DNS new zone

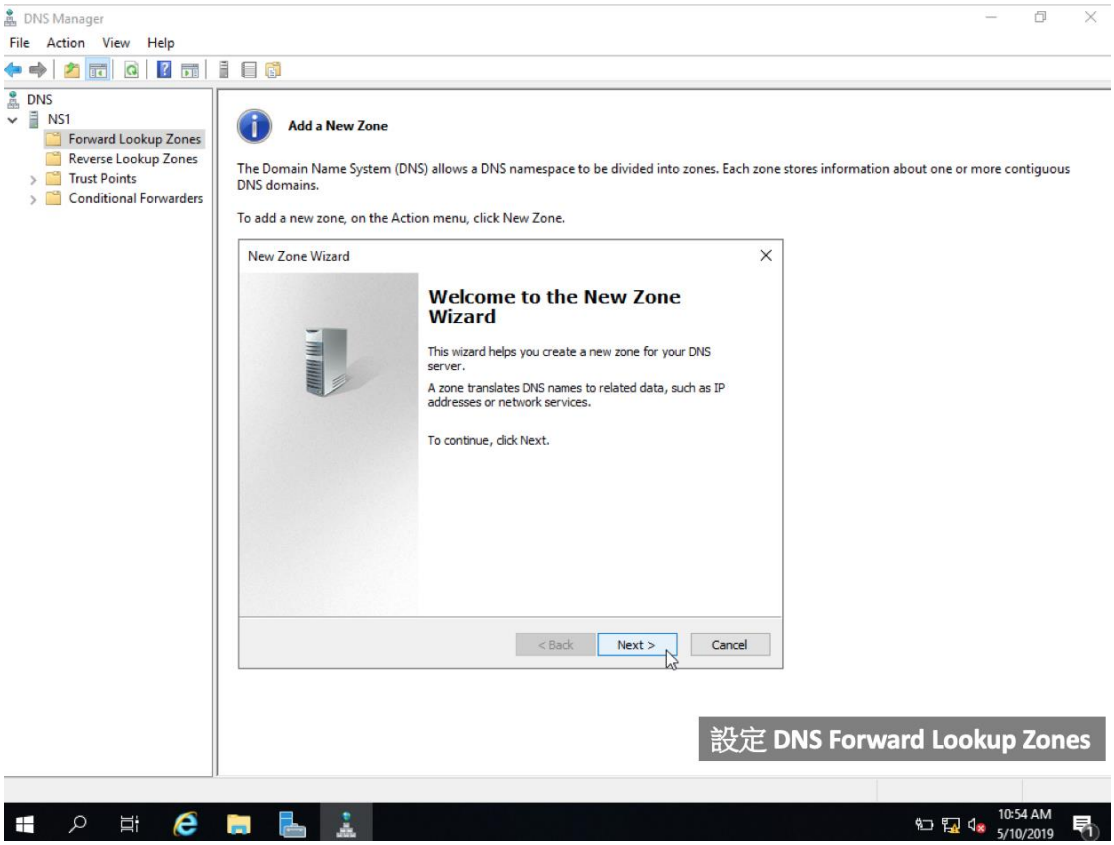



圖 77 Windows 2019 開始設定 DNS zone

我們稱一個域名為一個 Zone，這個 zone 可以是您從出售網域的網站中買到的域名，也可以是從該域名之下延伸出來的 sub-zone。由於 DNS 很重要，因為如果沒有 DNS，使用者無法連到網站，也無法連到其他服務，因為 IP 是數字，根本記不起來。既然 DNS 這麼重要，為提高其容錯能力及查詢效能，我們在架設某一單一 zone 的時侯，常以多台伺服器來負責該 zone 的服務。

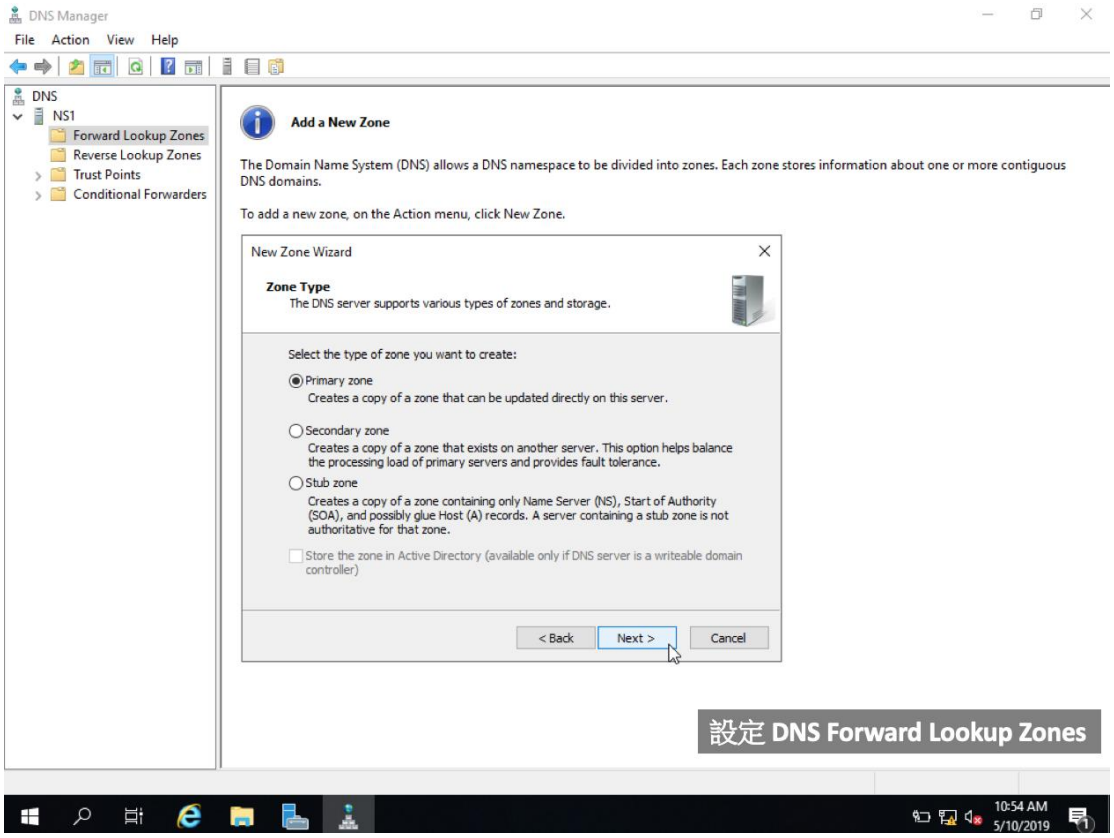



圖 78 Windows 2019 設定 zone type

在安裝精靈的導引下，接著輸入你購買的網域名稱，此時不要輸入子網域名稱，例如你購買了 server.tw 網域，這裡就是輸入 server.tw。之後如果架設一個網站，你可能會為這個網站設定為 www.server.tw，如果你架設了一個 POP3 收信主機跟 SMTP 發信主機，那你可能分別設定 pop3.server.tw 跟 smtp.server..tw。

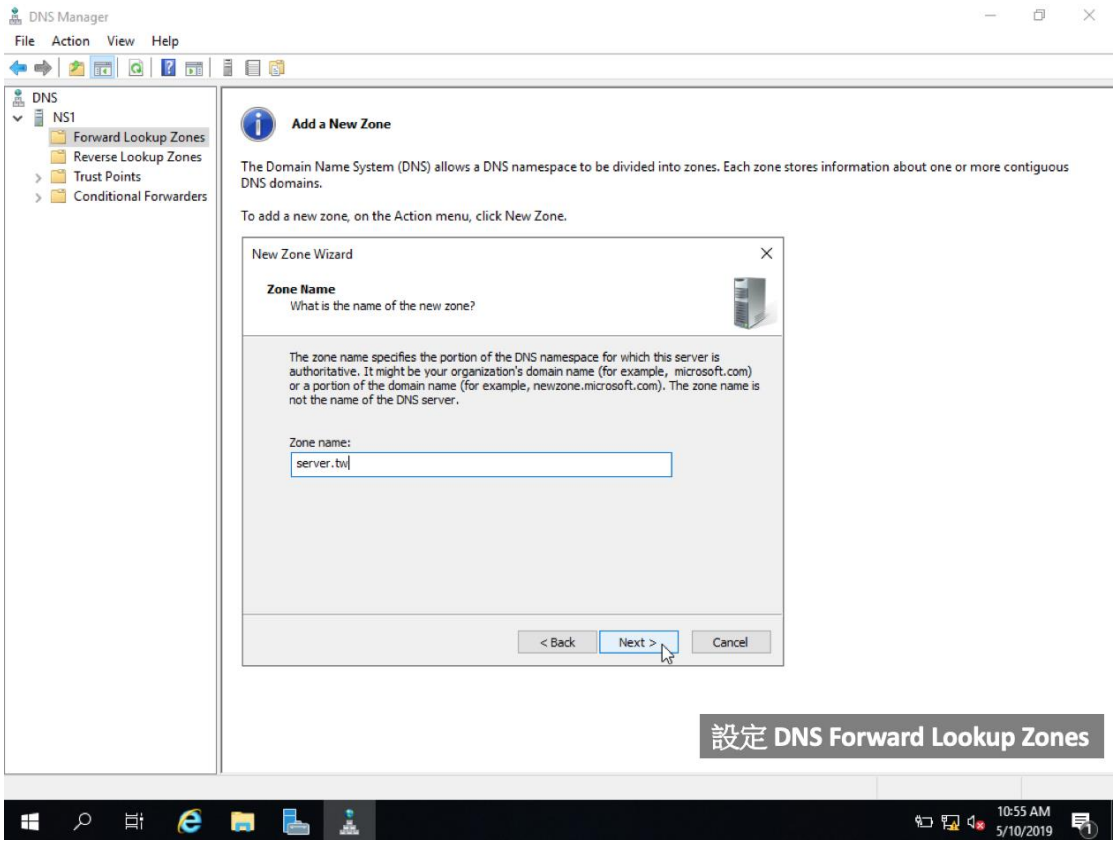



圖 79 Windows 2019 輸入 zone

DNS Server 會將所有關於網域的設定保存在 DNS zone file 內，在這個 zone file 內，記錄所有正確的 DNS 設定。依據設定精靈，請在此輸入 zone file 的名稱，我們輸入 server.tw.dns 作為 zone file 名稱。

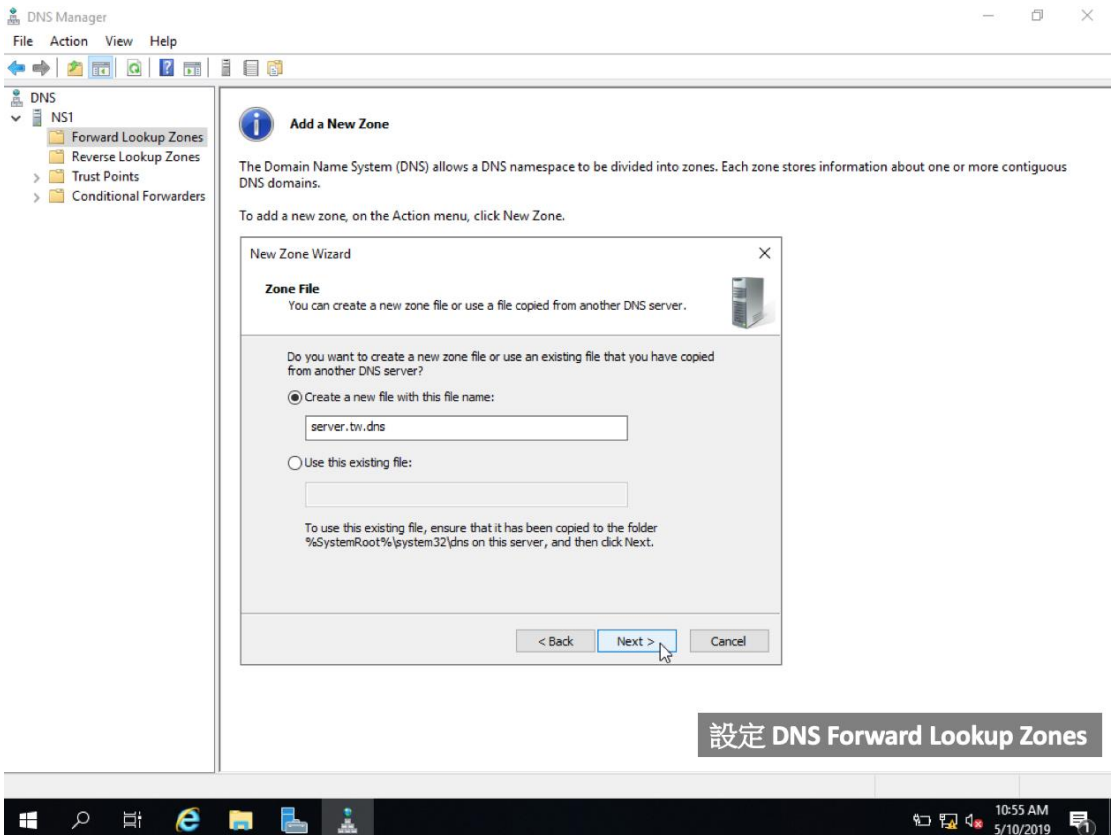



圖 80 Windows 2019 建立 zone file

由於設定為 Primary，因此請選擇不允許動態更新。所有 Primary 的 zone 都是手動更新，因為是主要來源，需要由管理人員設定跟維護，不會由其他主機提供資料進行自動更新。

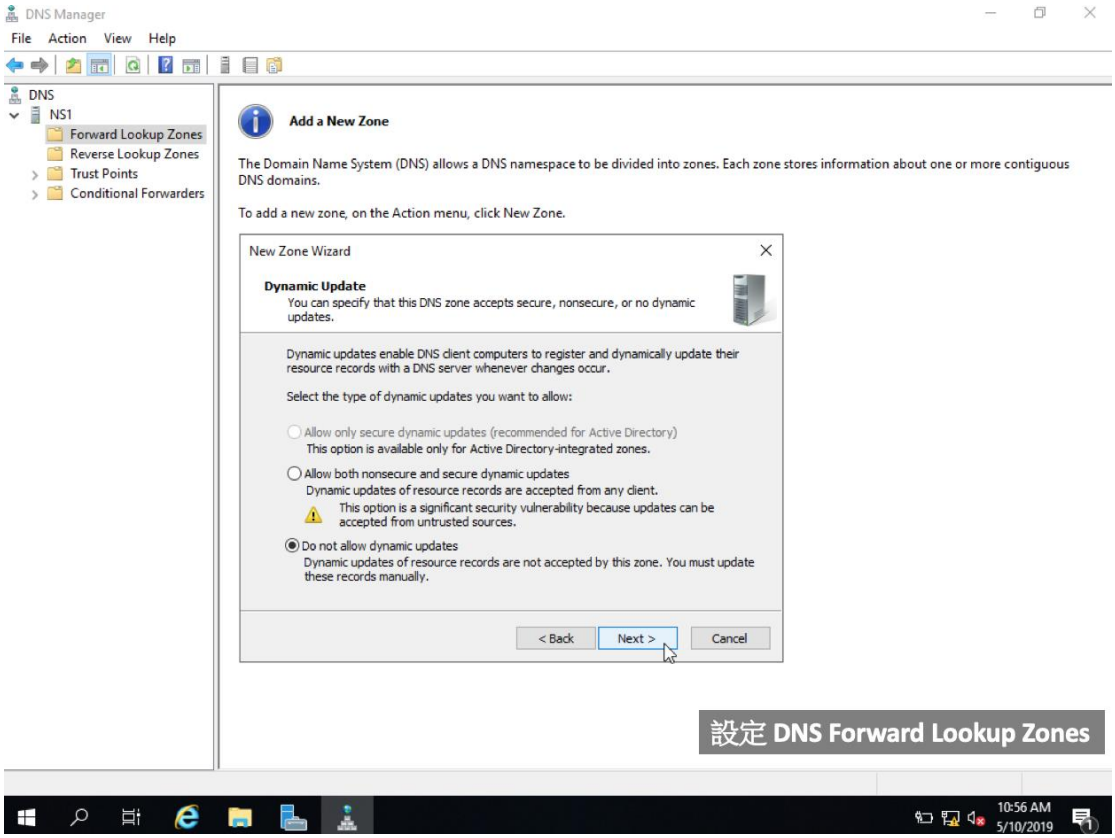



圖 81 Windows 2019 DNS 設定確認視窗

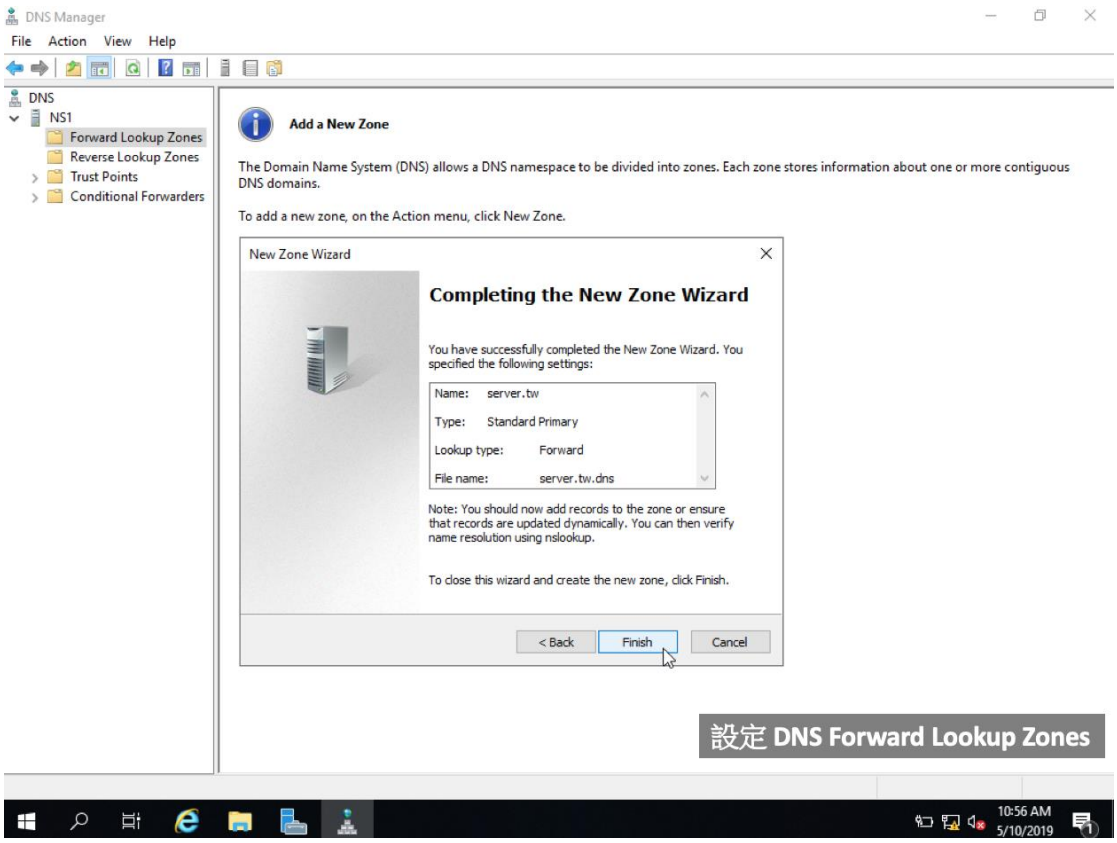



圖 82 Windows 2019 設定 DNS 完成視窗

接下來要幫主機設定 IPv6 的對應，需要在 DNS 主機內新增一筆 AAAA 記，A 是給 IPv4 使用，而 AAAA 則是給 IPv6 使用。

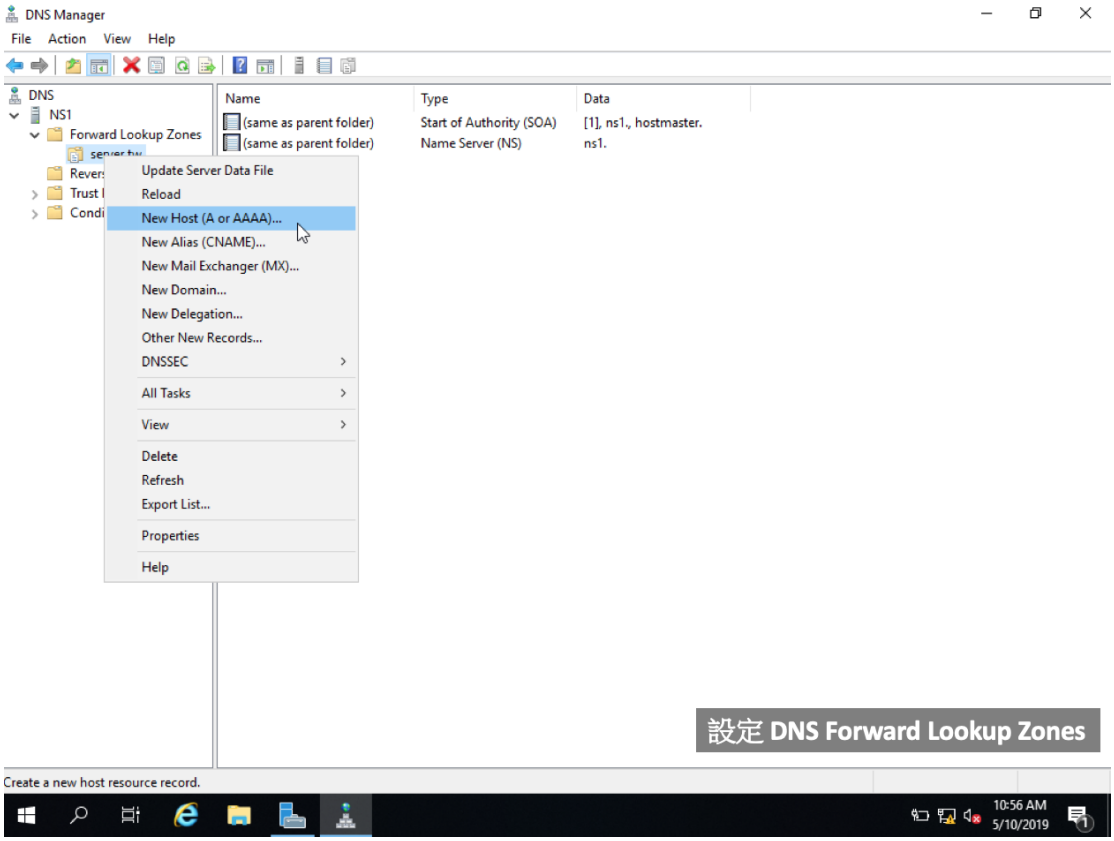



圖 83 Windows 2019 設定 DNS 新的主機

選擇 DNS 主機之後，選擇要加入主機。在這裏我們建立一個 ns1 的子網域，並將 ns1.server.tw 對應的 IPv6 位址填入。

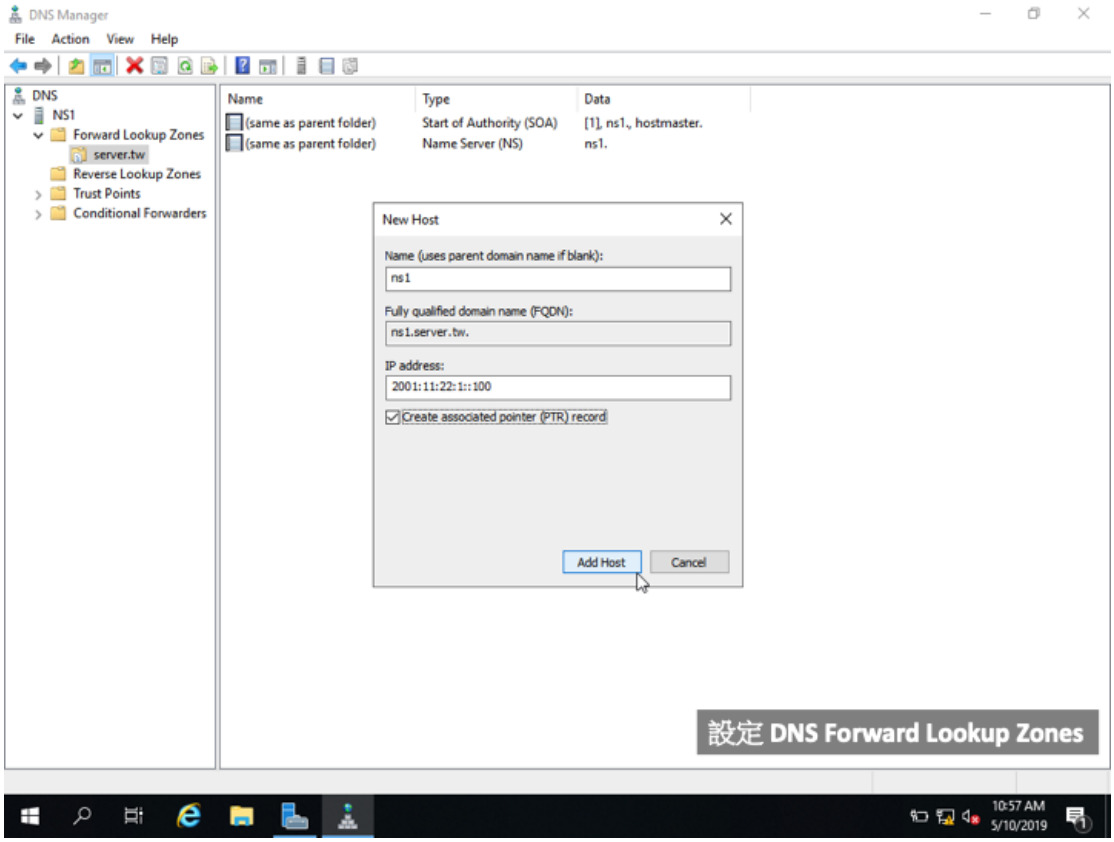



圖 84 Windows 2019 設定 DNS reverse lookup zone

在這裏我們建立一個 ns1 的子網域，並將 www.server.tw 對應的 IPv6 位址填入。

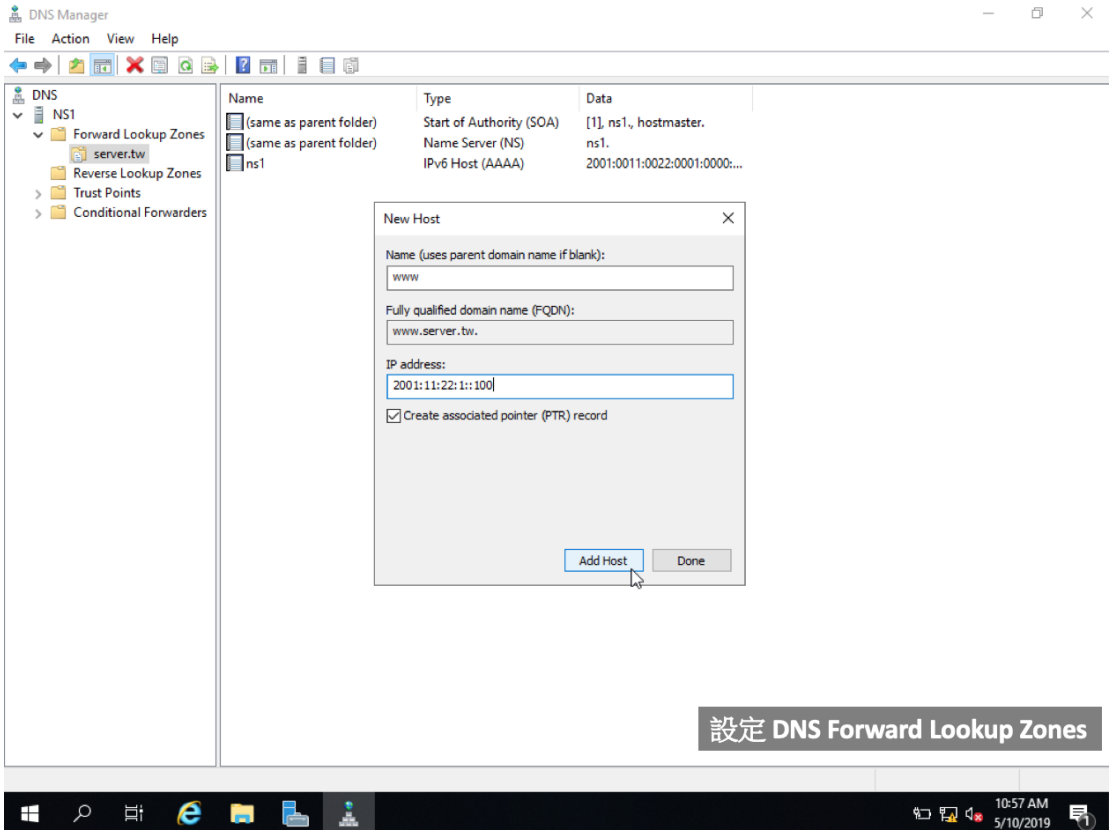



圖 85 Windows 2019 指派 IPv6 位址

從這個視窗，可以看到目前設定成果。我們已經設定好一台 ns1 跟 www 的 IPv6 位址。之後當使用者查詢 ns1.server.tw 時，可以查詢到對應的 IPv6 位址，同樣的，當使用者要連到 www.server.tw 時，也可以查到對應的 IPv6 位址。

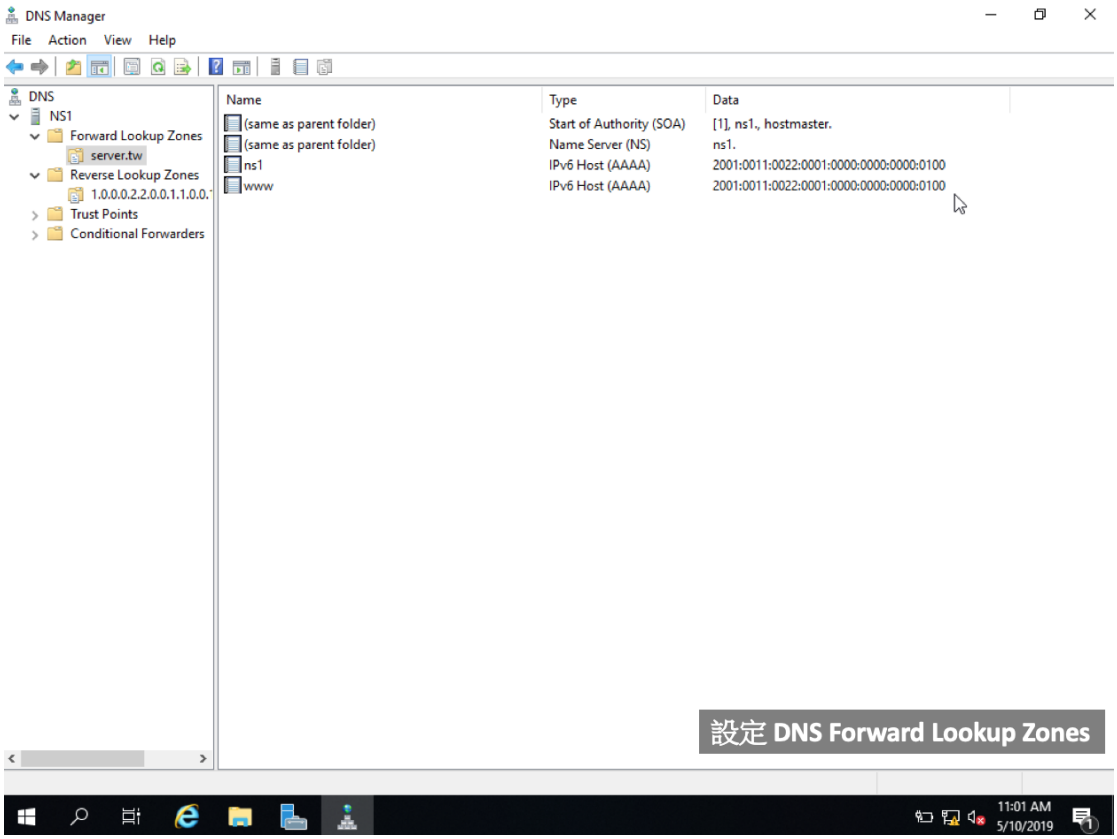



圖 86 Windows 2019 檢查 DNS 設定結果

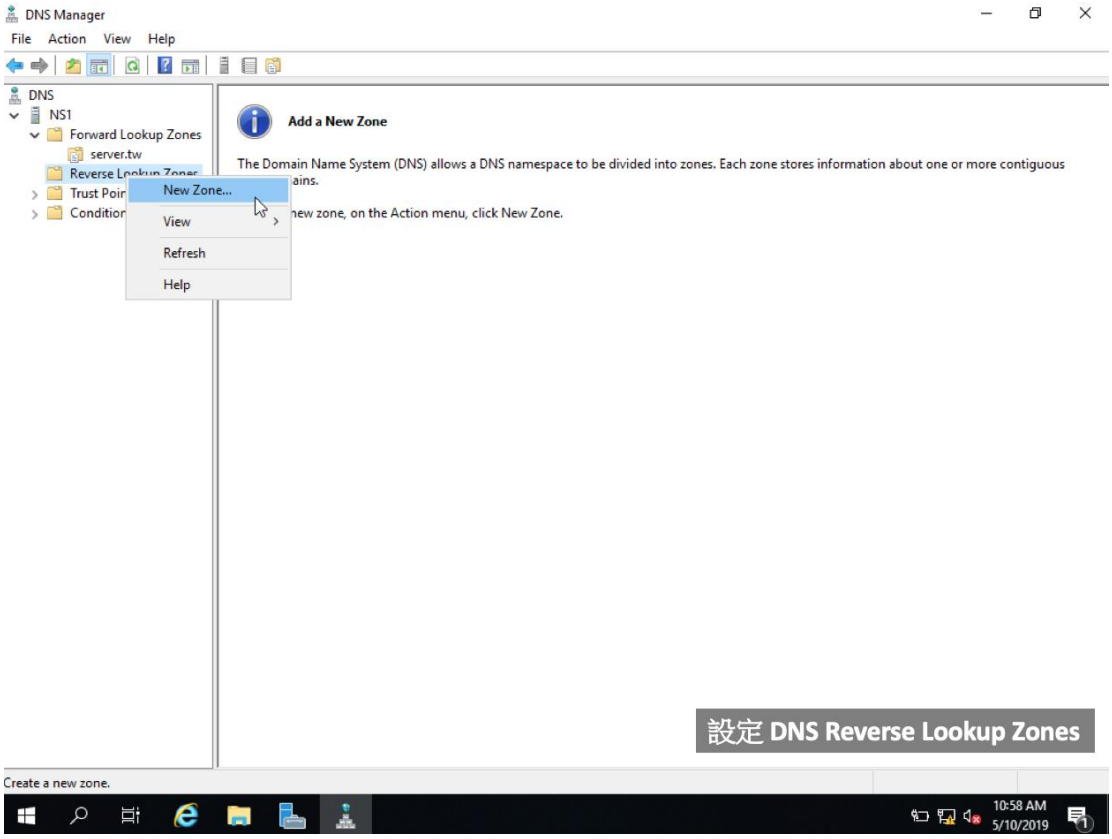



圖 87 Windows 2019 設定 DNS reverse lookup zone

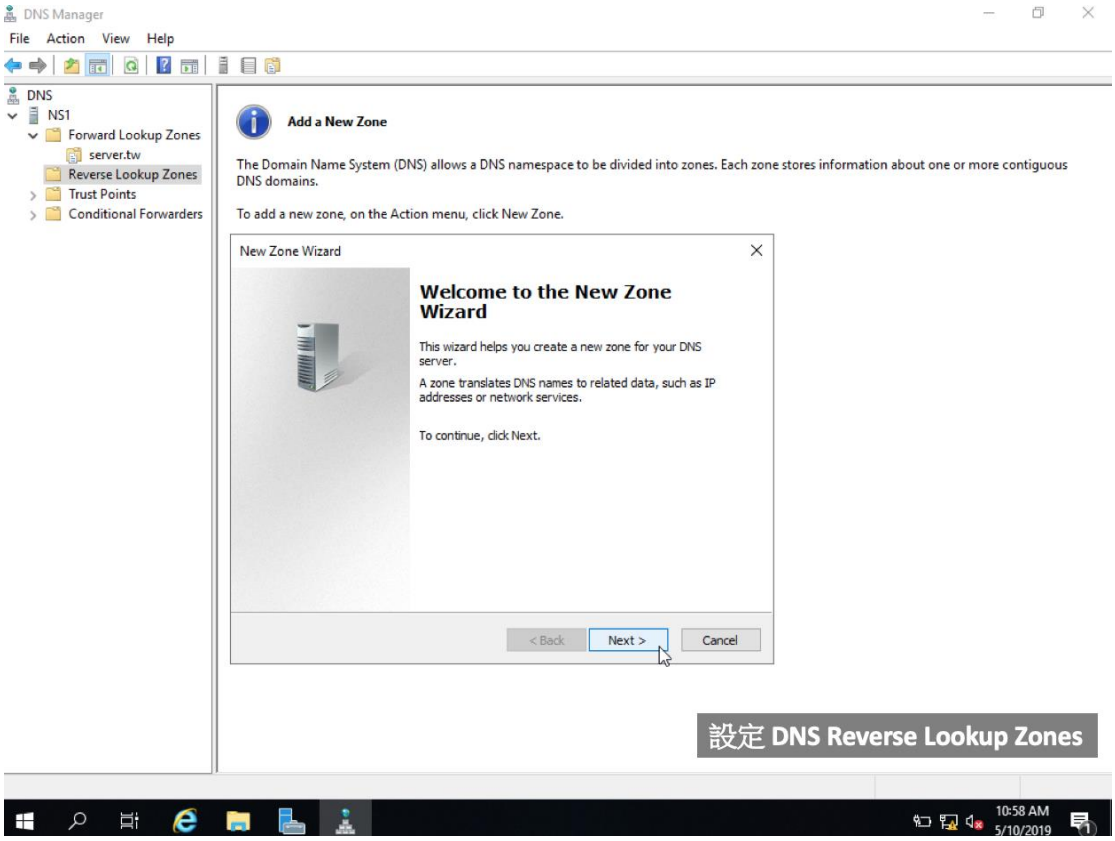



圖 88 Windows 2019 設定 DNS reverse lookup zone 歡迎畫面

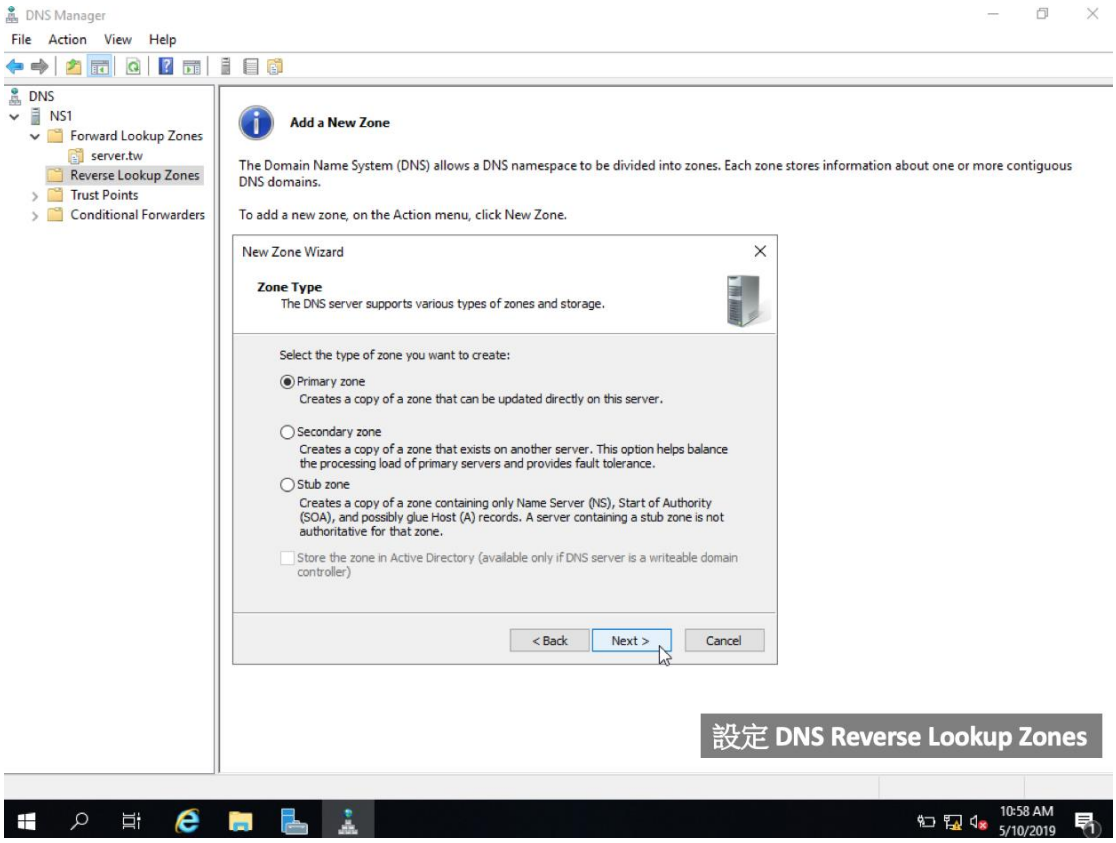



圖 89 Windows 2019 選擇 Zone 類型

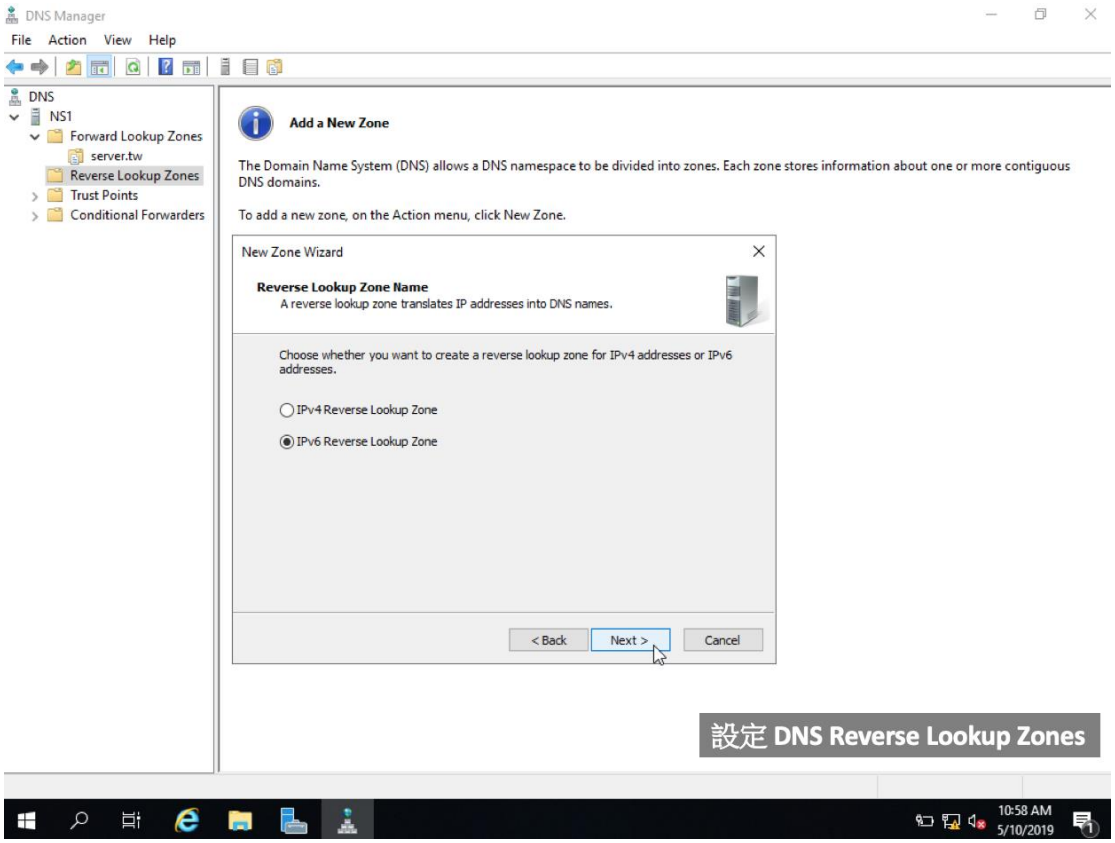



圖 90 Windows 2019 選擇 IPv6 Reverse lookup zone

接下來要設定反解，所謂的反解就是用 IP 去查出此 IP 的網域名稱。

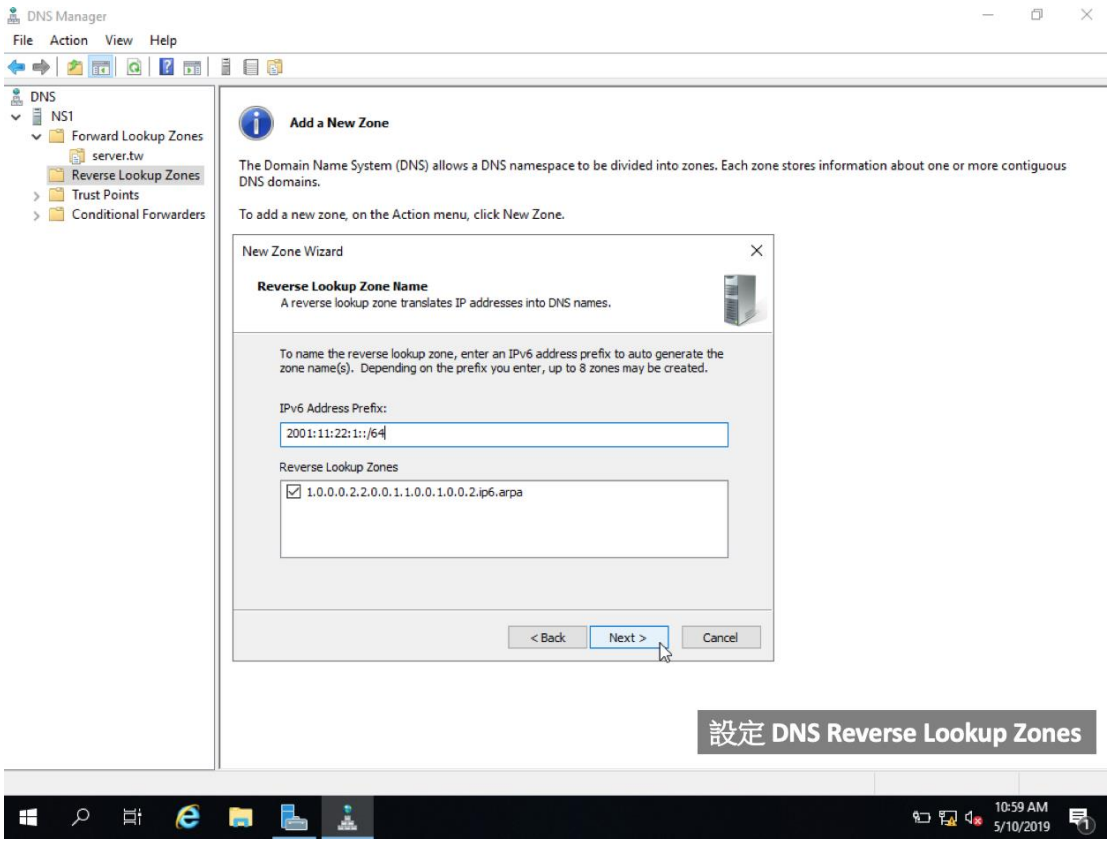



圖 91 Windows 2019 設定 DNS reverse lookup zone 輸入 IPv6 位址

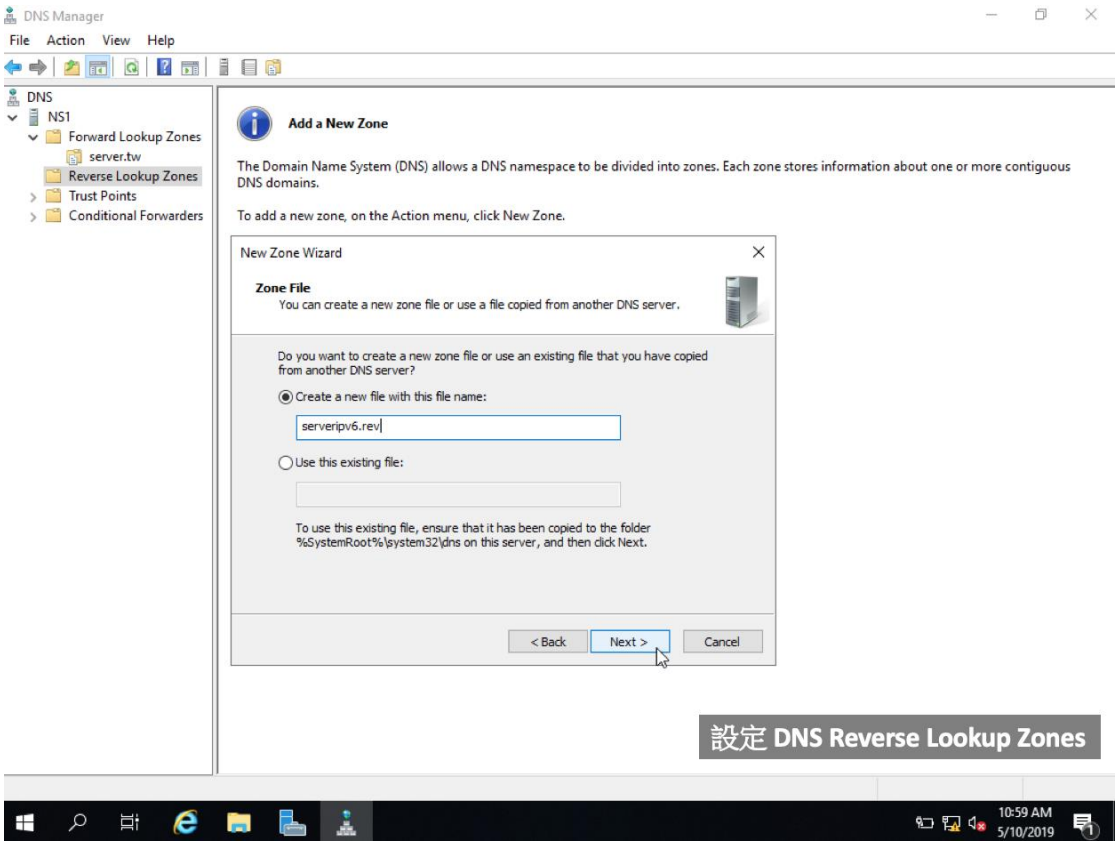


圖 92 Windows 2019 建立 DNS reverse lookup zone file

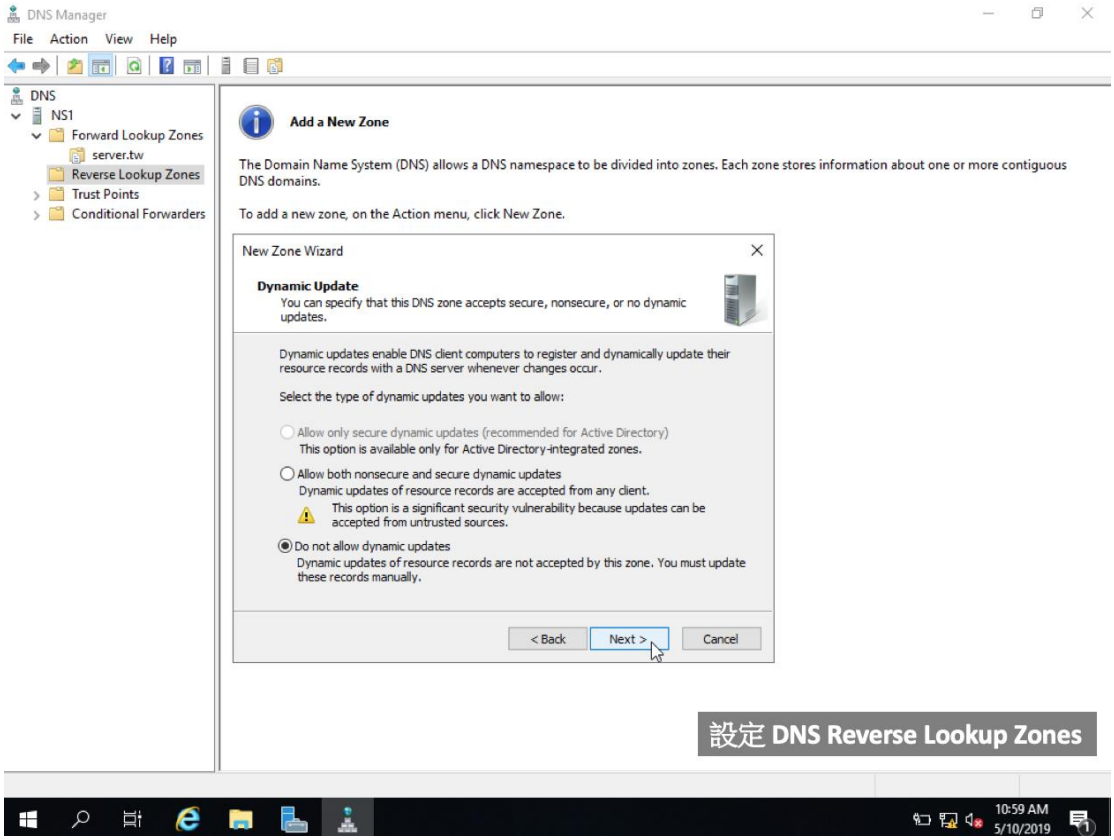



圖 93 Windows 2019 DNS reverse lookup zone 動態更新設定

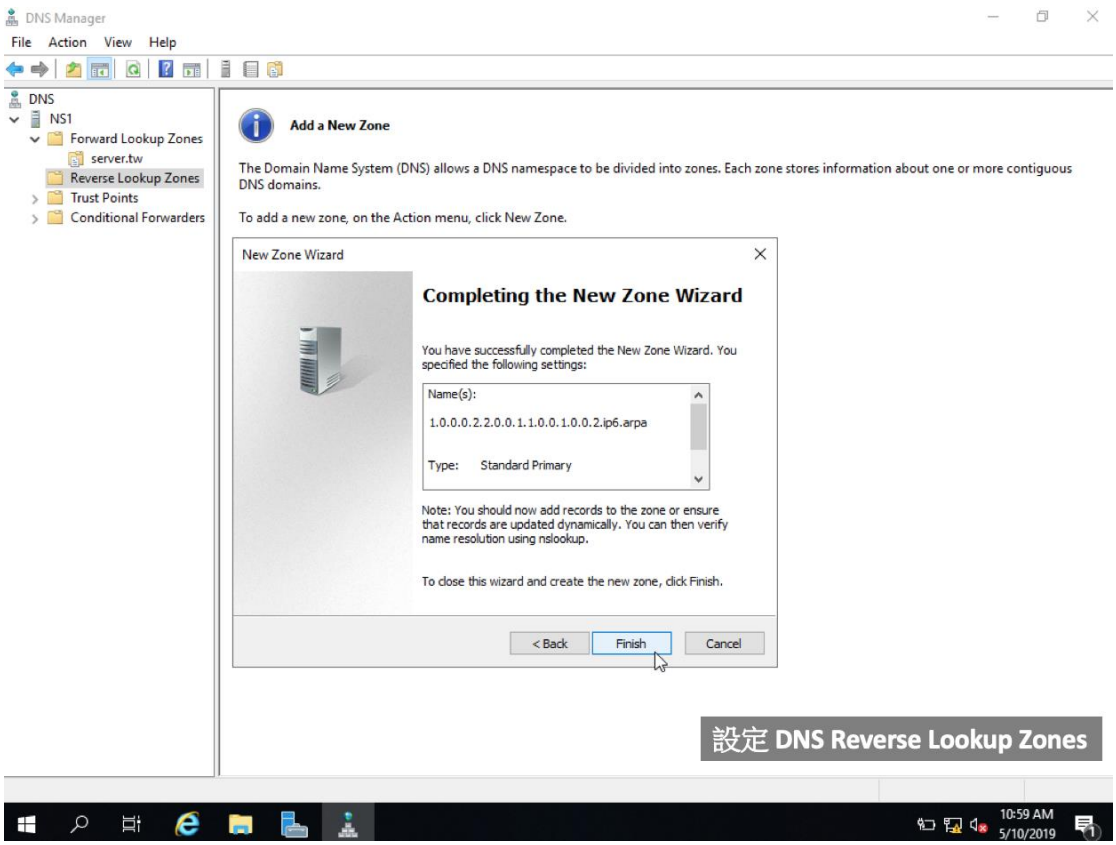



圖 94 Windows 2019 DNS reverse lookup zone 設定確認畫面

IP「反解」在 DNS 的「資源紀錄」（ Resource Record,簡稱 RR ）中屬於「PTR」類別，用來將 IP 位址對映到主機的「FQDN」（ Fully qualified domain name,也就是指 Domain Name ）。（ 相對地，所謂「正解」便是指 FQDN 對映到 IP 的關聯定義。 ）

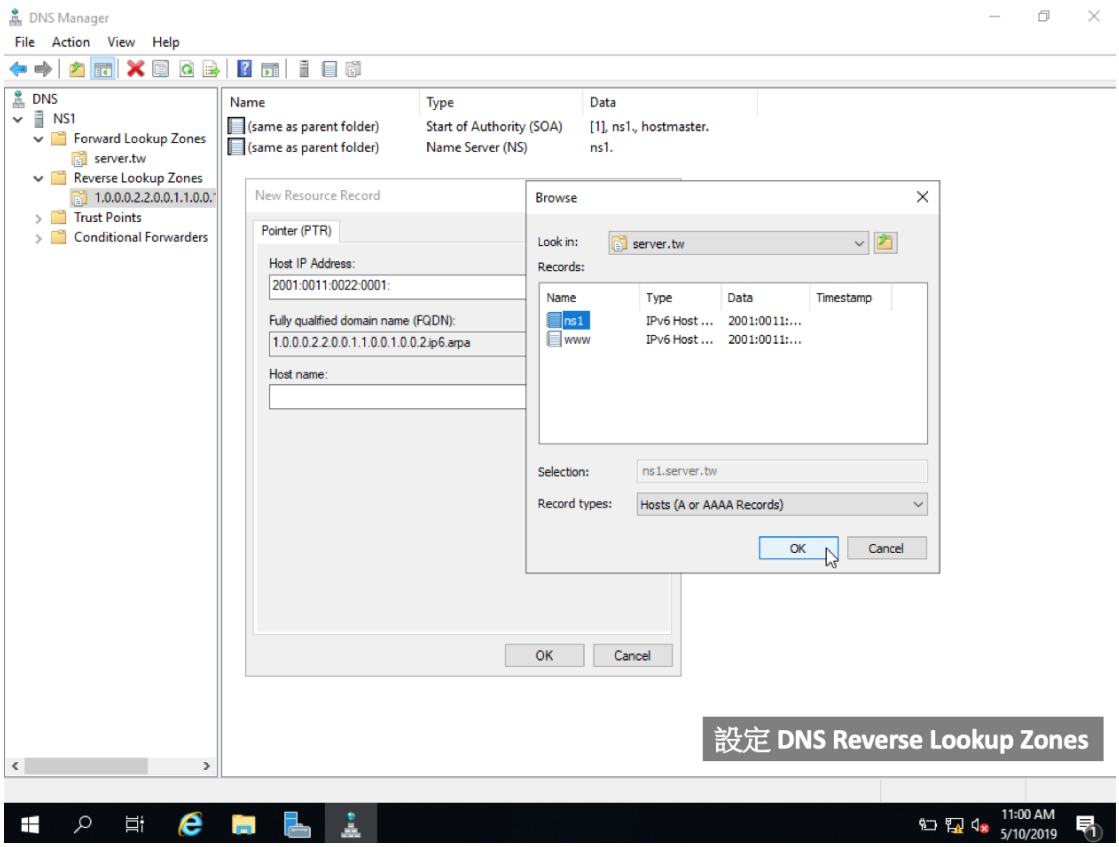



圖 95 Windows 2019 檢視 DNS reverse lookup zone 設定結果一

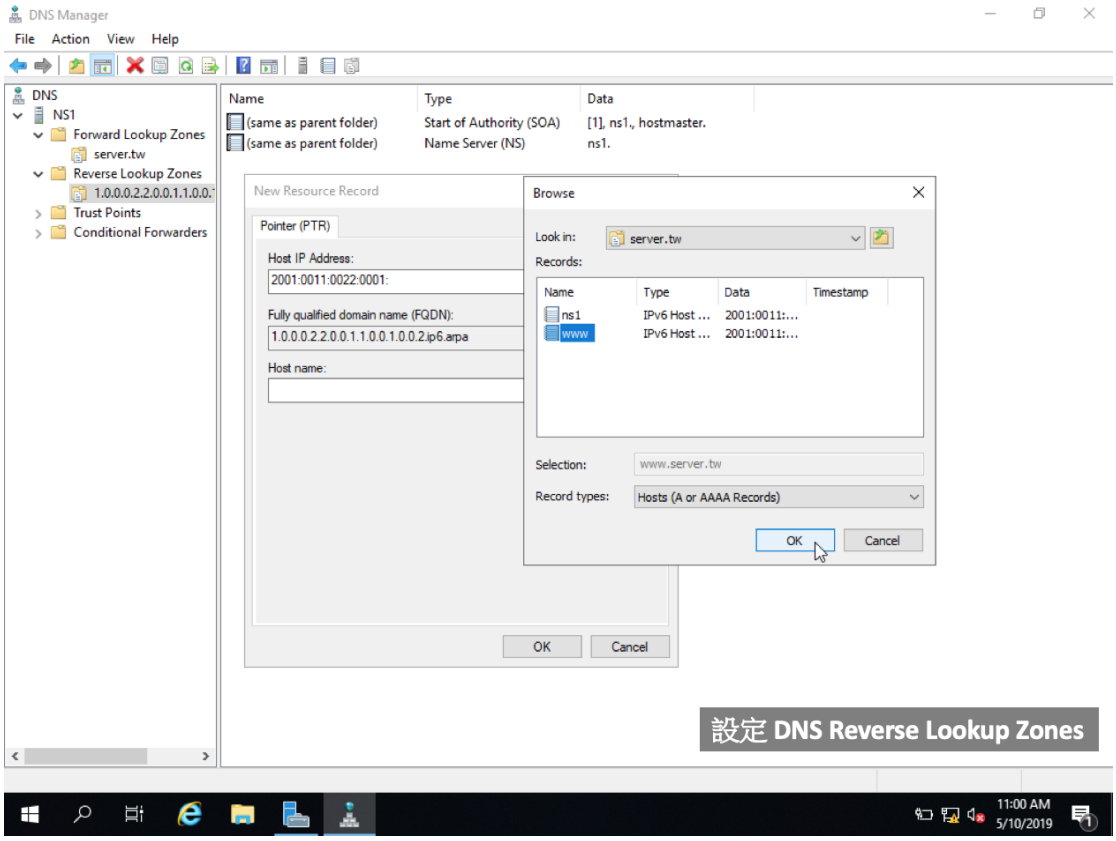



圖 96 Windows 2019 檢視 DNS reverse lookup zone 設定結果二

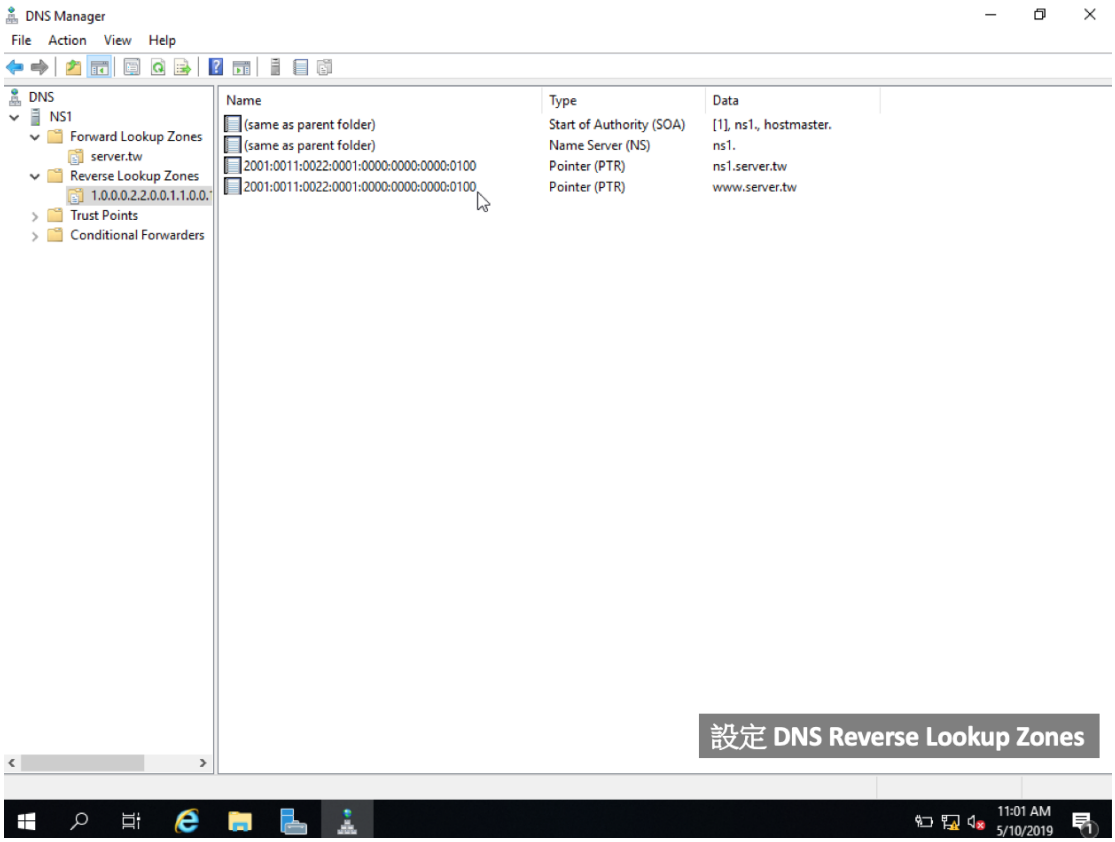



圖 97 Windows 2019 檢視 DNS reverse lookup zone 設定項目

設定完成之後，我們可以開始利用指令來驗證設定是否正確，可以使用的指令通常是 nslookup 或者 dig。dig 是比較新版的 DNS 查詢工具，可以顯示的資訊比較多，當然指令的參數也比較複雜。如要查詢 www.server.tw 的 IP 位址時，可以用 nslookup www.server.tw。如果用 dig 指令，可以用 dig aaa www.server.tw +short

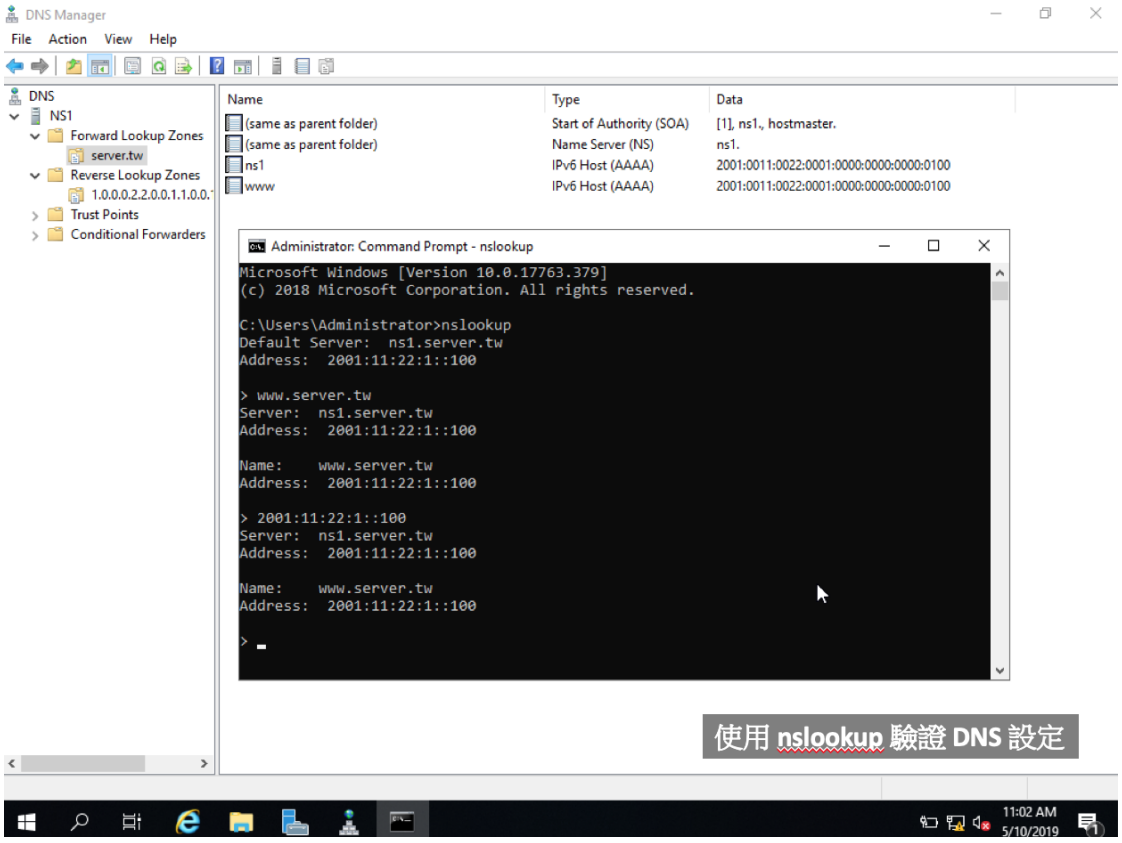



圖 98 Windows 2019 使用 nslookup 指令驗證結果

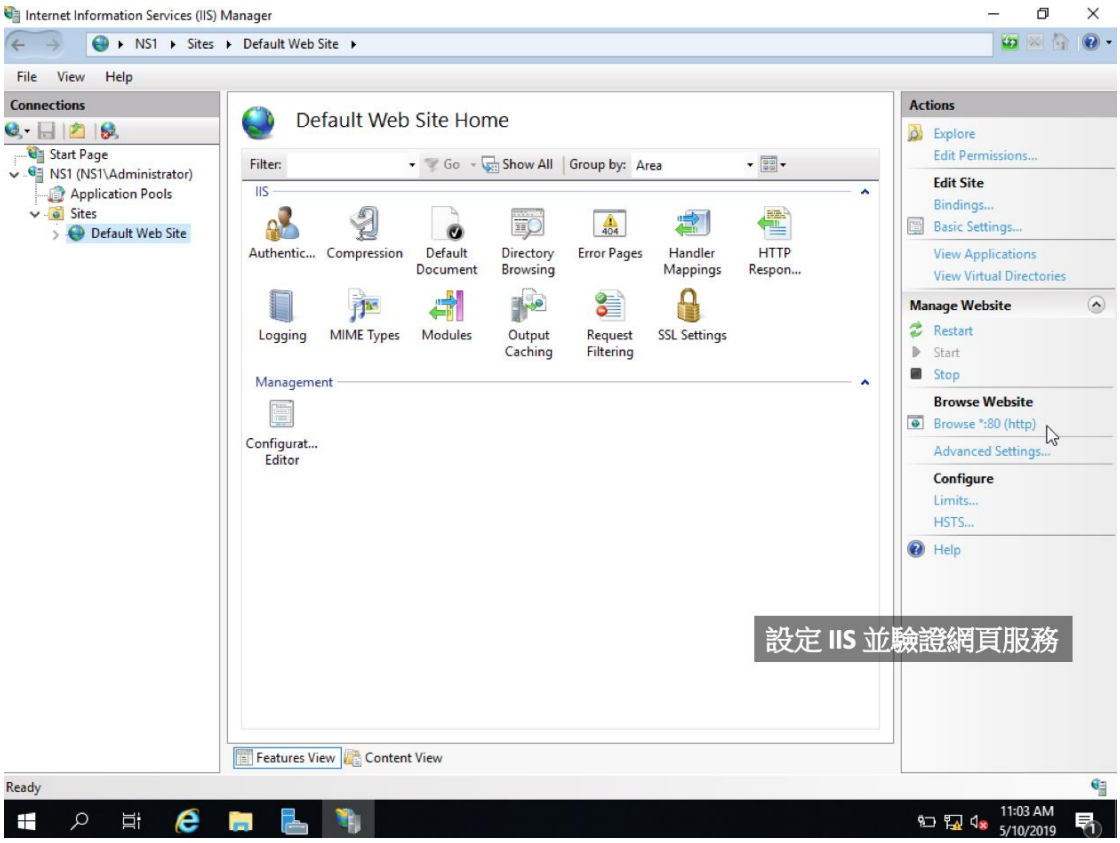



圖 99 Windows 2019 開啟 IIS 畫面

IIS 設定完成之後，也一樣使用 nslookup 或者 dig 去驗證網址對應的 IP 是否設定正確。還有透過瀏覽器去瀏覽，確定網站可以連得上。

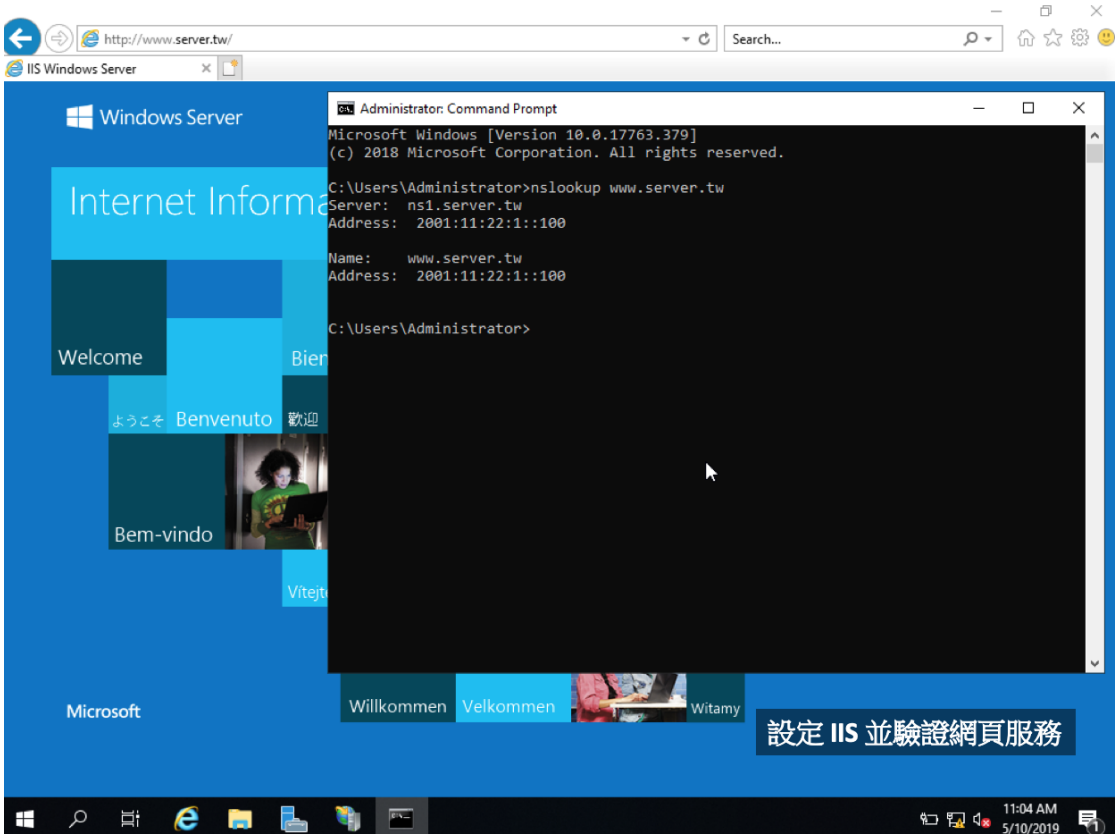



圖 100 Windows 2019 設定 IIS 並驗證網頁服務

接著我們要進行 DHCP server 的設定。DHCP server 負責動態配置 IP 給其他主機，讓其他主機可以取得 IP 之後連網。

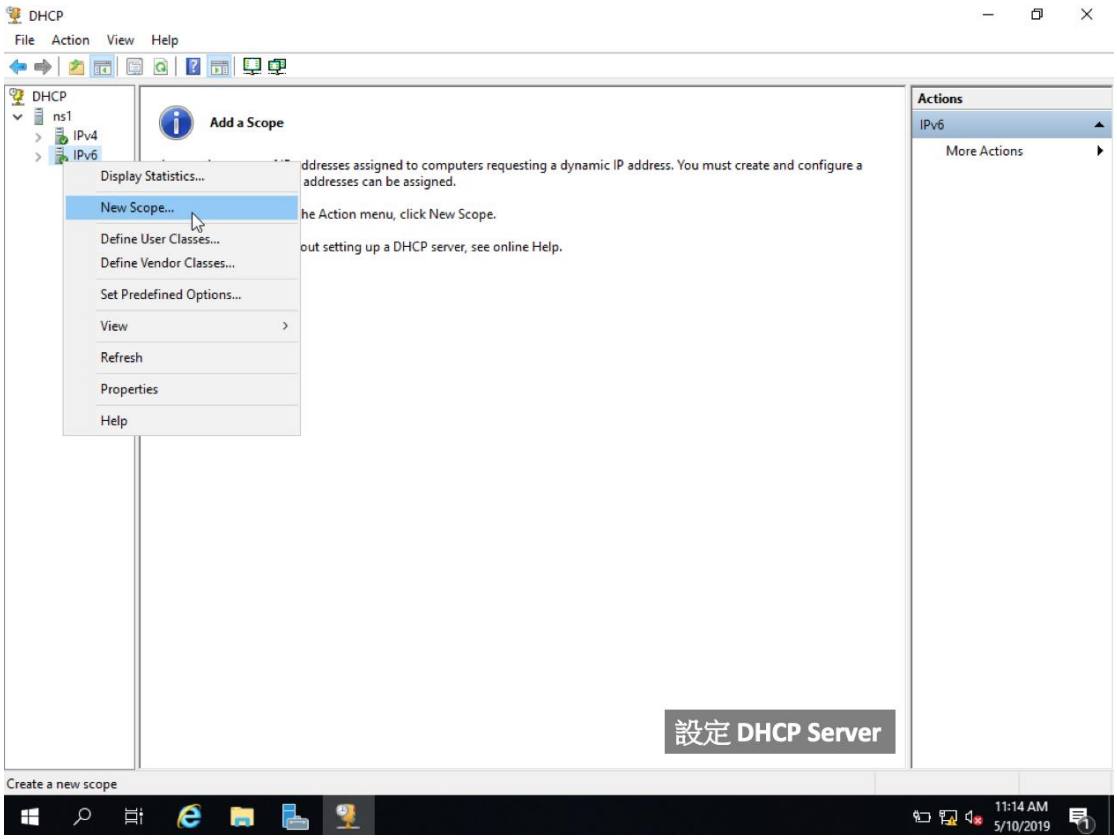



圖 101 Windows 2019 設定 DHCP 點選 new scope

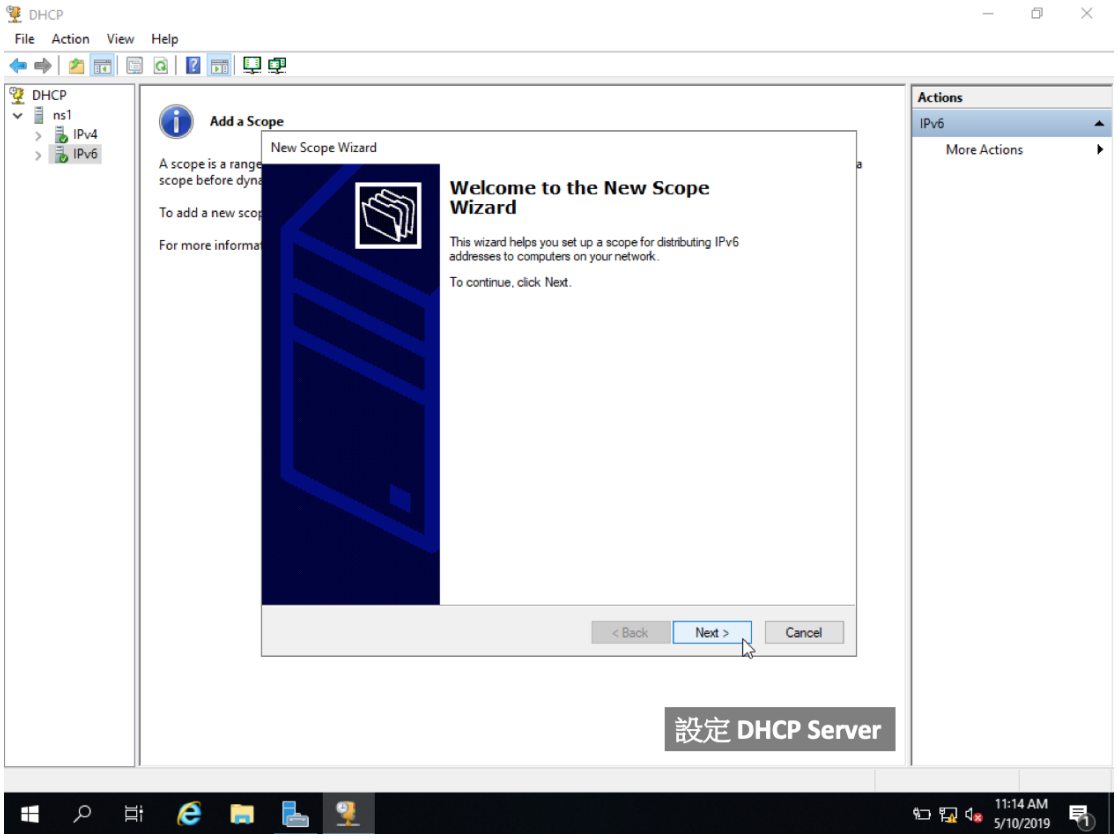



圖 102 Windows 2019 設定 DHCP 歡迎畫面

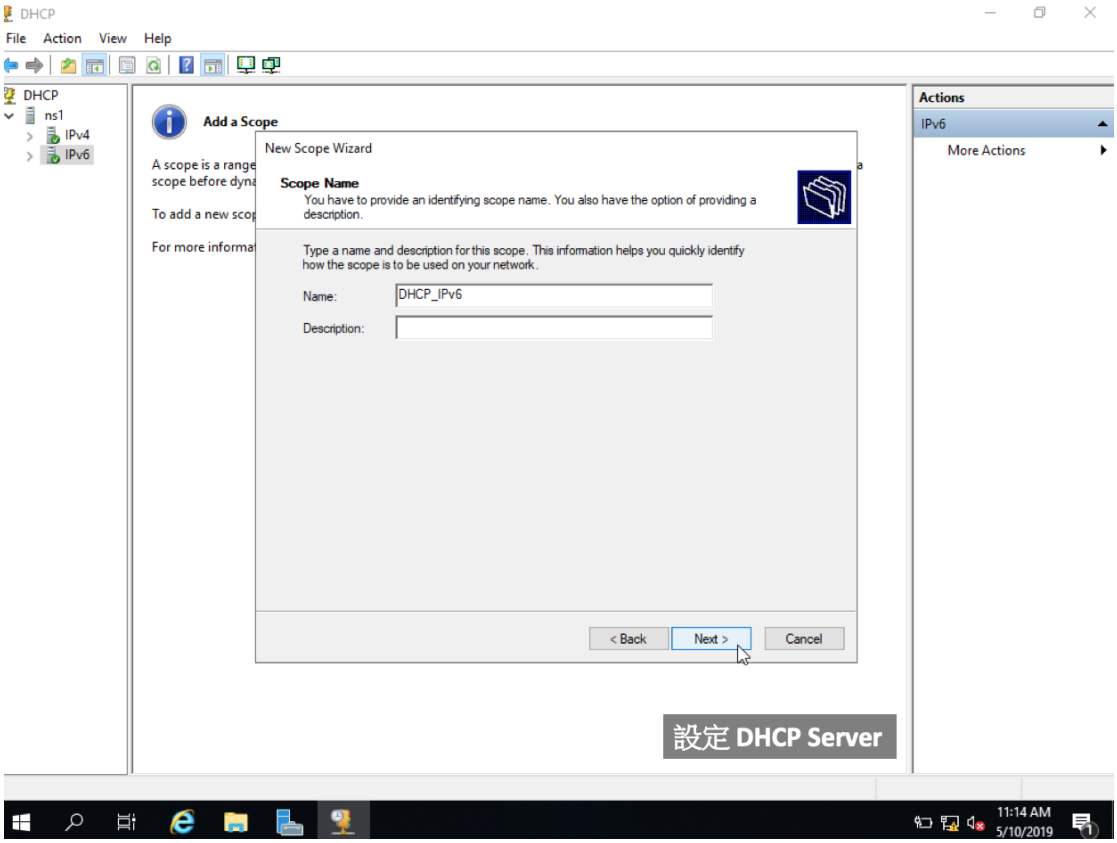



圖 103 Windows 2019 輸入 DHCP server

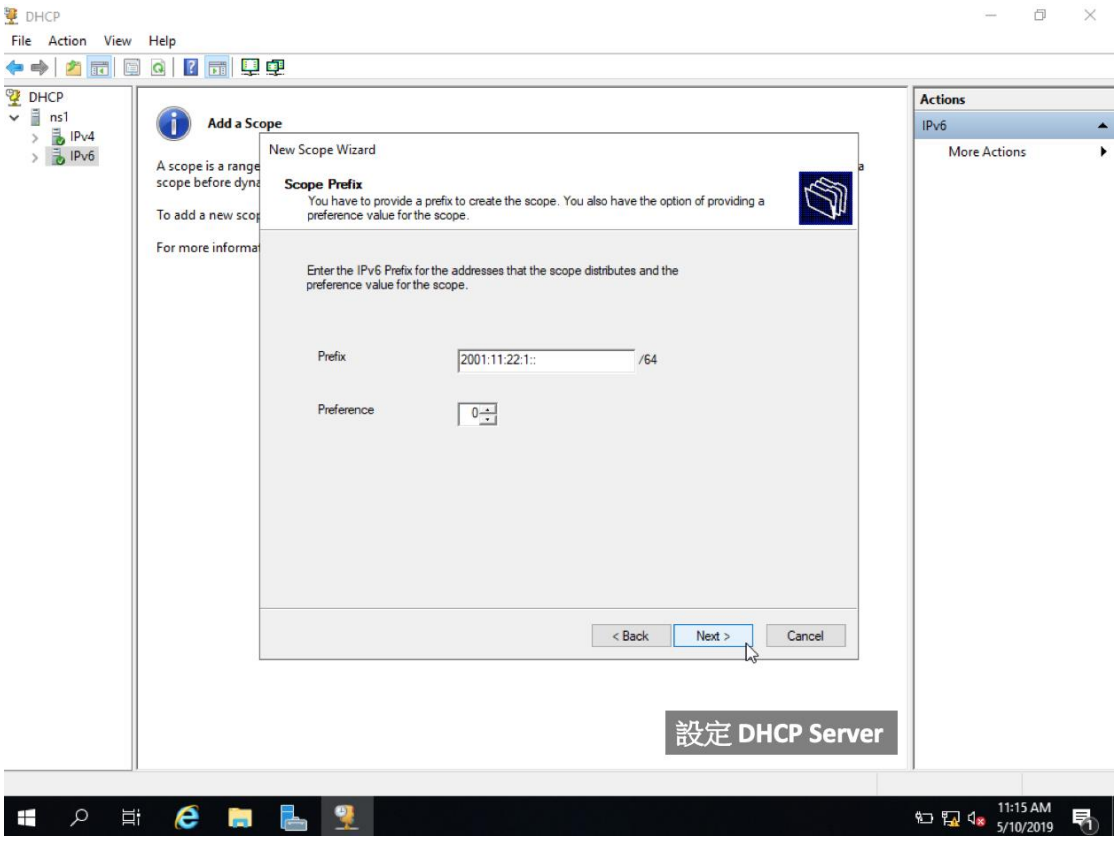



圖 104 Windows 2019 設定 scope prefix

DHCP Server 因為是負責動態配置 IP，所以要指定可以分配出去的 IP 範圍，此時可以注意到，視窗內會將 IP 位址的前半段變成固定不可更動，但後面才是要可以分配給 DHCP client 的 IP 範圍。任何 DHCP client 透過跟 DHCP server 索取 IP 一定是落在你設定的這個範圍區間。

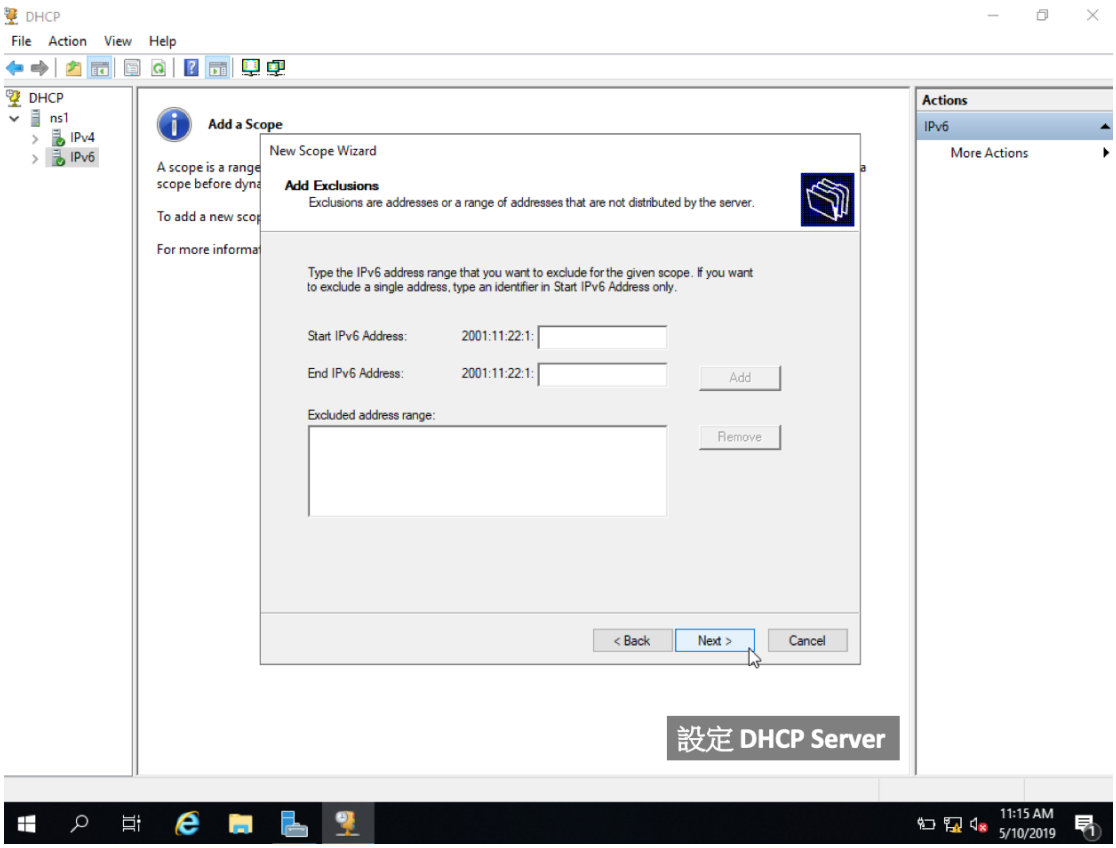



圖 105 Windows 2019 設定配置範圍

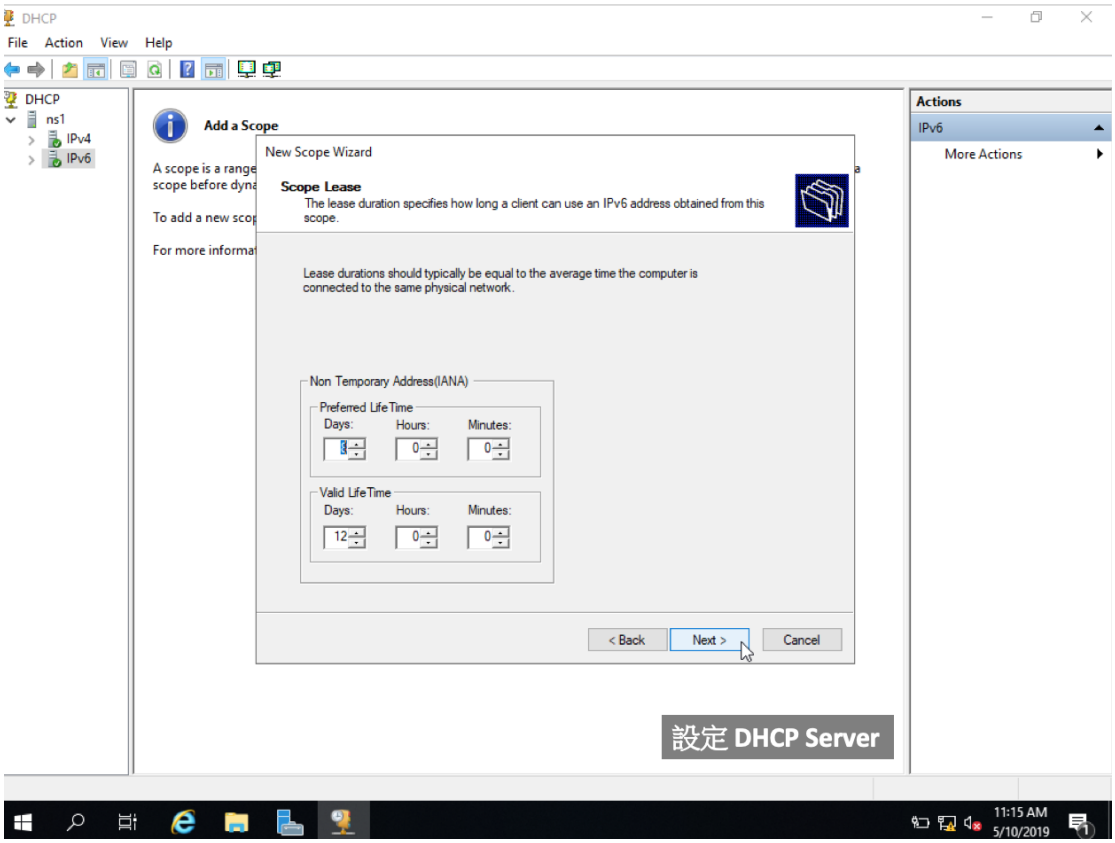



圖 106 Windows 2019 設定 scope lease

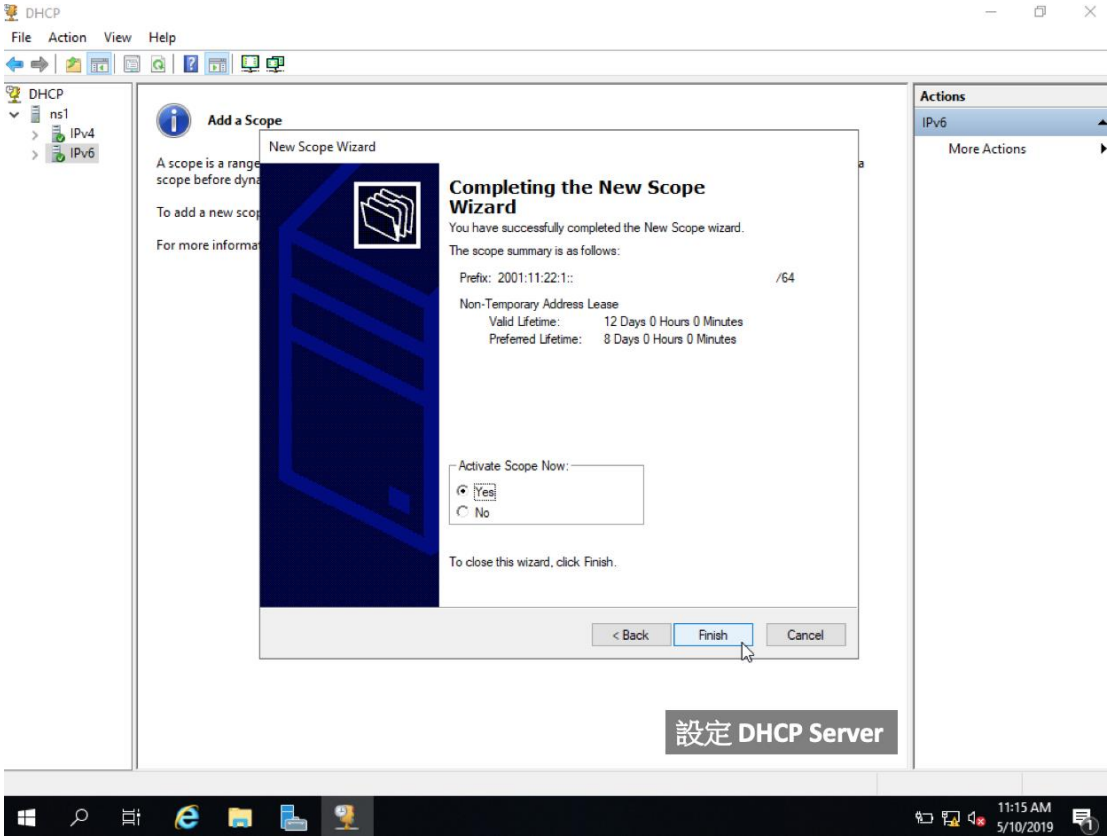



圖 107 Windows 2019 確認是否啟用

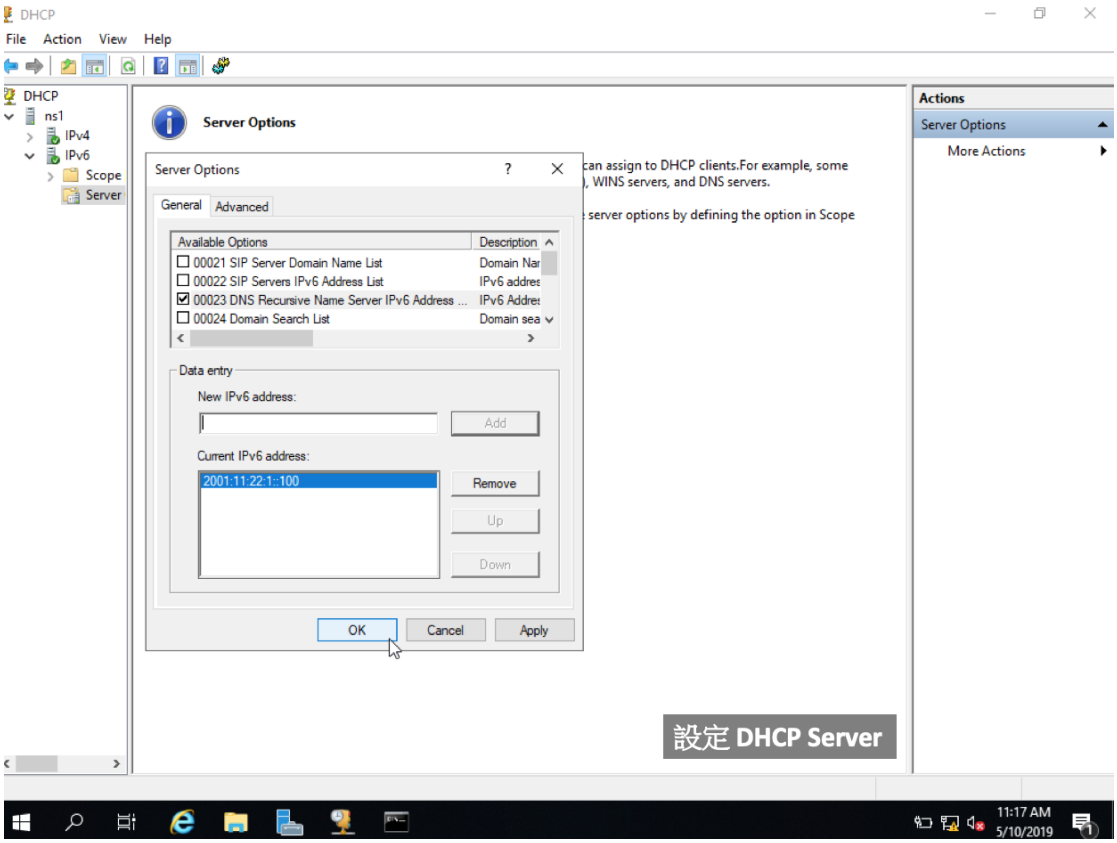



圖 108 Windows 2019 驗證 IPv6 位址

至於如何驗證 DHCP server 是否有正常運作呢? 只要使用另外一台電腦，並讓該電腦的 IP 取得方式不是手動輸入，而是自動取得。此時就是使用 DHCP 的方式跟 DHCP server 拿到 IP 位址，只要可以拿得到 IP 位址，且 gateway 及 DNS 都正常，再來就是測試連到網路是否通過，就表示 DHCP server 配置成功。

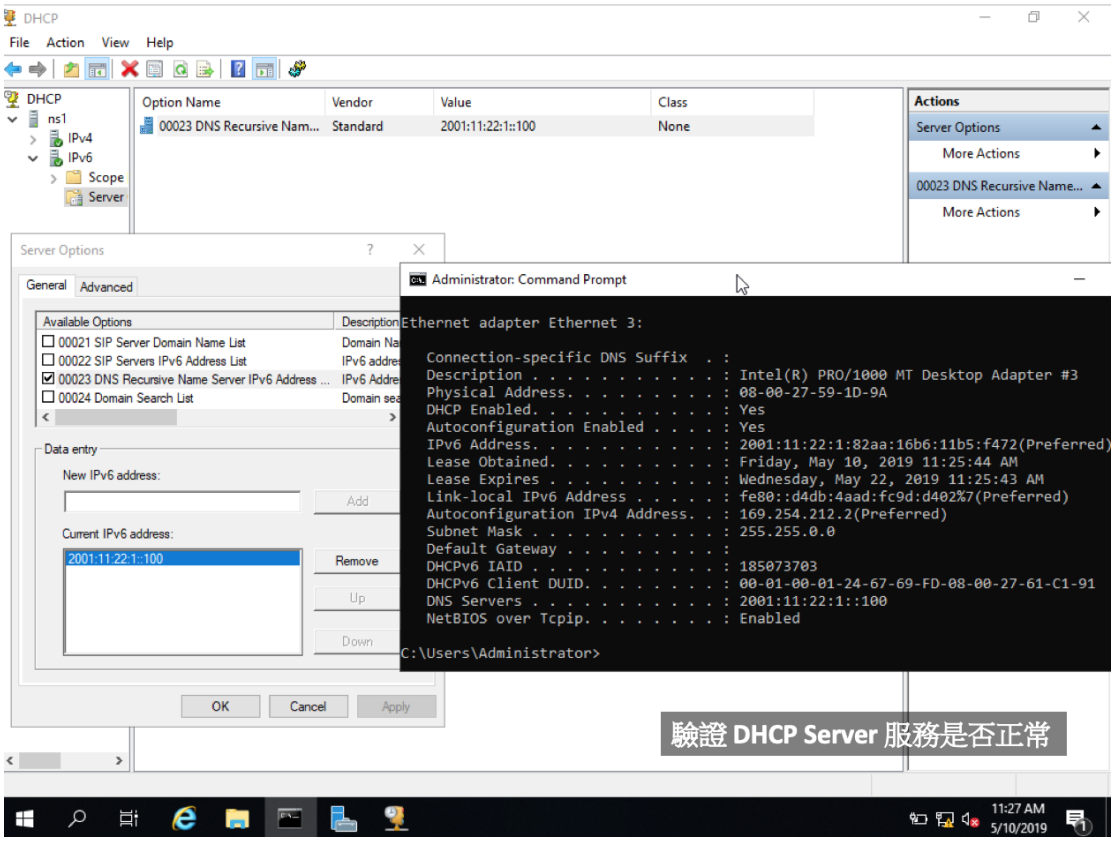


圖 109 Windows 2019 驗證 DHCP Server 服務是否正常

# 第五章 MySQL5 資料庫啟用 IPv6

## 第一節 本篇概述

資料庫主要負責儲存資料，由於不對外連線，因此對 ICP 業者而言，通常要注意的部分並非是開啟 IPv6 設定，而是注意資料庫若有儲存訪客的 IP 位址，需要保留足夠的長度，才可以儲存訪客的 IPv6 位址。由於網站大都以 MySQL 為主要資料庫，本章以 MySQL 為範例做說明，因只需要修改儲存 IPv6 位址欄位的長度設定，故不同版本下設定方法並無差異。

## 第二節 MySQL5 啟用 IPv6

儲存 IPV6 的欄位長度需要為 varchar（39） 如果是要存 varbinary 則為 varbinary（16）

如果需要指定 IPv6 address，可以在 my.cnf 內設定

```
bind_address=<ipv6 位址>
```

範例：

```
[mysqld]
bind_address= *
```

如果要限定只能用 Ipv6 連線，可以設定成 bind_address = ::1
當設定之後，從 console 連進 MySQL 時，需要先建立一個 ipv6 的帳號

```
以下指令需要進入 MySQL console 才可以執行
mysql> create user ‘ipv6user’@‘::1’ identified by ‘ipv6pass’;
mysql> create user ‘remoteipv6user’@‘2001:db8:0:f101::2’ identified by ‘remoteipv6pass’;
```

之後從 console 連進 MySQL

```
以下指令是在 bash shell 下執行
mysql -h ::1 -u ipv6user -p
mysql -h 2001:db8:0:f101::1 -u remoteipv6user -p
```

檢查連線狀態可以使用以下指令

```
以下指令需要進入到 MySQL console 才可以執行
mysql> select current_user（）, @@bind_address;
mysql> status;
```

# 第六章 Microsoft IIS/Apache2/Nginx 網頁伺服器啟用 IPv6

## 第一節 本篇概述

網頁伺服器並不是硬體，而是指可以提供網站服務的軟體，只是翻譯上大家都稱為網頁伺服器或者稱為 Web Server。在早期，以 IIS 跟 Apache 兩套為主，使用者多，且相關文件豐富。近幾年，Nginx 的高效能讓它變成許多大流量的網站的首選。跟 Apache 相比較，Nginx 優異的處理速度，讓許多技術人員放棄 Apache 改用 Nginx。

## 第二節 Microsoft IIS 啟用 IPv6

IIS 內建支援 IPv6，所以在 Windows Server 主機建立 IPv6 協定連線後，只要驗證伺服器可提供 IPv6 服務即可。

開啟 Windows Server 主機 Server Manager 的畫面後，選擇 Internet Information Services（IIS）Manager 選項進行 IIS 的設定。

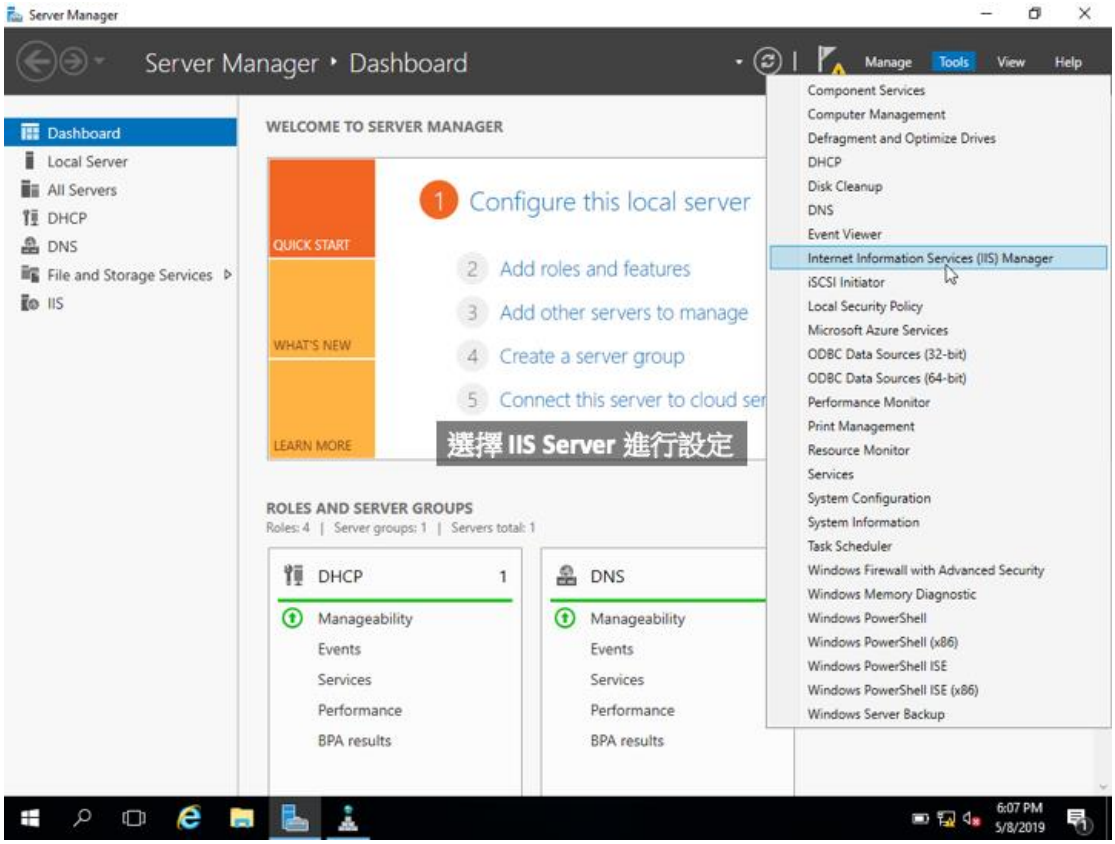
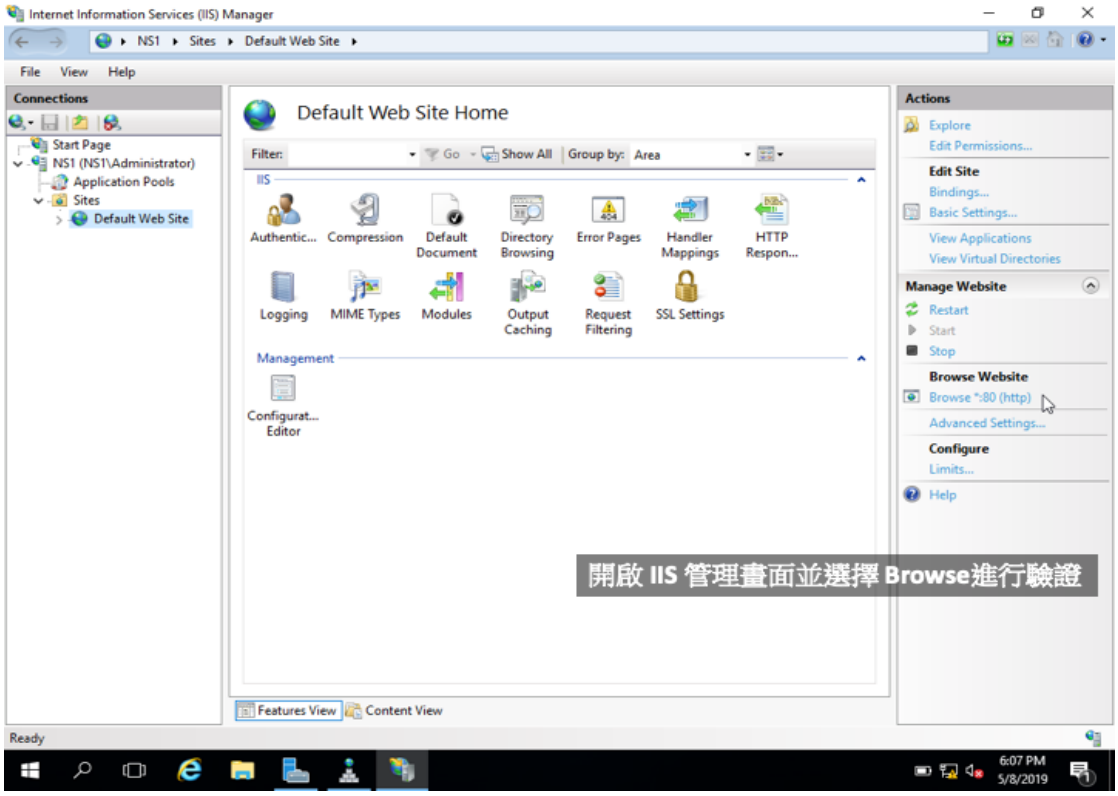



圖 110 開啟 Microsoft IIS




進入 Information Services（IIS）Manager 設定畫面後，選擇 Browse Website 選項開始準備驗證的動作。

圖 111 選擇 browse 進行驗證

於開啟瀏覽器後，於終端機中輸入指令 nslookup，如 Address 有出現 IPv6 的位址，即表示啟用 IPv6 成功，如果只有出現 IPv4 位址，即代表 IPv6 啟用失敗。如果啟用失敗，請重新執行設定步驟。如果重新執行上述步驟仍舊無法啟用 IPv6，請洽詢維護廠商。

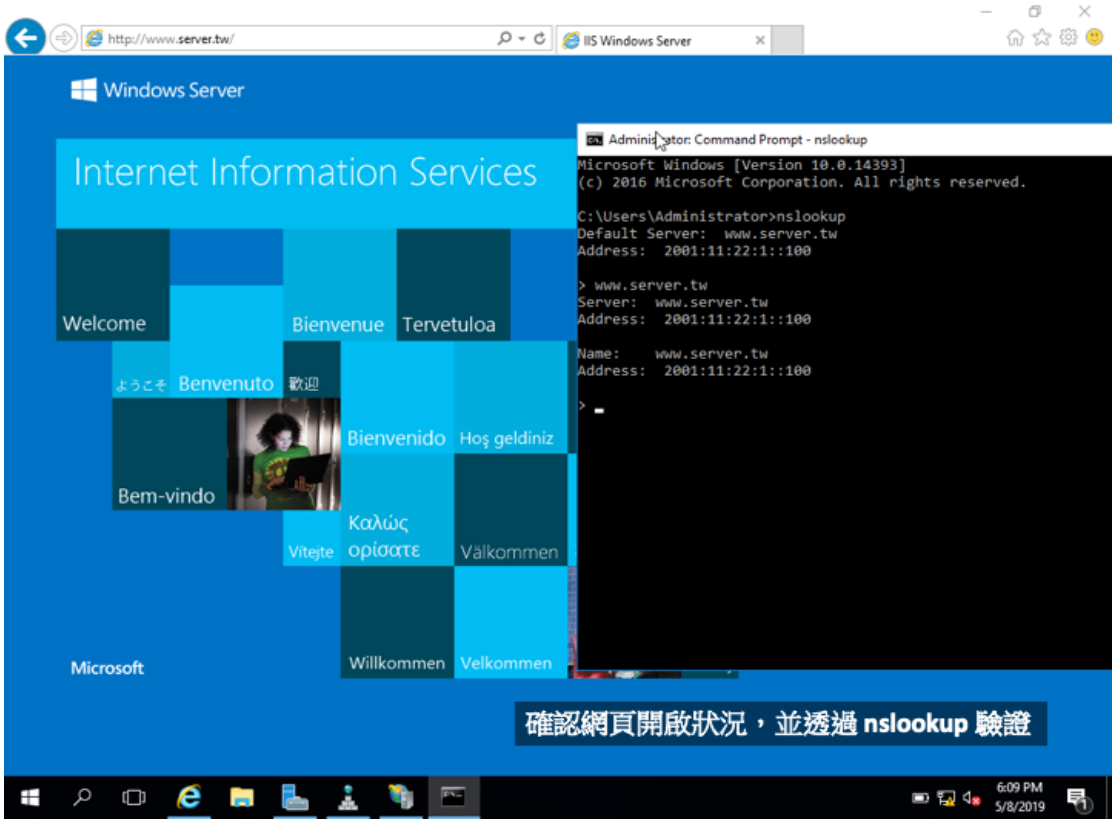



圖 112 以 nslookup 驗證

## 第三節 Apache2 支援 IPv6

Apache 是 Linux 系統上最廣泛用來架設 Web 伺服器的架站軟體，Apache 2.0 版本開始支持 IPv6，設定 Apache 時主要工作是設定一些基本 Web Server 的選項，將 Apache 服務與指令的 address 與 port 結合，即可啟用 Apache 的 IPv6 功能。

安裝完 Apache 後，預設會在所有的網路介面提供 80 port 的連線，如只需要針對特定的 IPv6 位址介面提供服務，需手動將 IPv6 位址的 TCP 80 設定給 Apache Server 使用。設定的步驟如下，先開啟設定檔 httpd.conf，並自行手動增加所需之設定，例如加入以下設定，Listen [2001::b000:xxxx:xxxx:xxxx:xxxx]:80。

```
Listen 80
Listen 443
Listen [2001::b000:xxxx:xxxx:xxxx:xxxx]:80
Listen [::]:443

# 以下設定統一加入在 httpd.conf 內。
<VirtualHost *:80 [::]:80>
...
</VirtualHost>
```

以下是 httpd virtual hosting 的設定範例

```
# 以下是設定一個 IPv4 的 VirtualHost，位址為 1.2.3.4
<VirtualHost 1.2.3.4>
...
</VirtualHost>
# 以下是設定一個 IPv6 的 VirtualHost，位置為 2607:f:1:11::4
<VirtualHost [2607:f:1:11::4]>
</VirtualHost>
# 以下是允許所有 port 80 的 IPv4 跟 IPv6 連線
<VirtualHost *:80>
</VirtualHost>
# 以下是設定 IPv6 位址 2001:288:2:2::1 上開啟 Port 80
<VirtualHost [2001:288:2:2::1]:80>
</VirtualHost>

<VirtualHost 163.1.2.3:80>
</VirtualHost>
```

```
<VirtualHost 163.1.2.3:80 [2001:1:2:2::1]:80>
</VirtualHost>
```

## 第四節 Nginx 支援 IPv6

Nginx 從 0.7.36 的版本後開始支持 IPv6，如果要驗證現行的 nginx 版本是否已經啟用 ipv6，可以執行 nginx -V 的指令，如結果有出現「--with-ipv6」即表示有支援 IPv6。

```
執行指令
nginx -V

輸出結果
nginx version: nginx/0.8.46
built by gcc 4.1.2 20080704 （Red Hat 4.1.2-48）
TLS SNI support disabled
configure arguments: --without-http_autoindex_module --without-
http_userid_module --without-http_auth_basic_module --without-
http_geo_module --without-http_fastcgi_module --without-
http_empty_gif_module --with-poll_module --with-
http_stub_status_module --with-http_ssl_module --with-ipv6
```

如沒有出現「--with-ipv6」則需要重新修改參數或是直接重新安裝 Nginx，需要修改的參數內容可以參考以下指令。

```
執行指令
./configure --user=www --group=www --prefix=/usr/local/nginx --with-
http_stub_status_module --with-http_ssl_module --with-ipv6
```

確認有支援 IPv6 後進行 Nginx Server 的配置，其設定檔為 nginx.conf ，不過如果有 include 其他的設定檔，則寫在各自的設定檔中。

如要增加 Listen 對 443 port 要啟用 IPv6 的服務，設定步驟如下，先開啟設定檔 nginx.conf 並自行手動增加所需之設定，例如加入以下設定，listen [::]: 443 ssl http2。如只需要針對特定的 IPv6 位址介面提供服務，則設定步驟如下，先開啟設定檔 nginx.conf 並自行手動增加所需之設定，例如加入以下設定，listen [2607:f0d0:xxxx:xxxx:xxxx:xxxx]:80。

```
Server {
listen 80 default_server;
   listen [2607:f0d0:xxxx:xxxx:xxxx:xxxx]:80;
   listen 443 ssl http2;
   listen [::]:443 ssl http2;
}
```

# 第七章 PHP/C#/Python/Java/Javascript 程式支援 IPv6

## 第一節 本篇概述

許多程式語言都可以用來開發網站，但目前普遍以 PHP、Python 跟 C#為主。至於網頁效果（例如滑動、電視牆、輪播、跳出視窗）則以 Javascript 為主。

程式語言可以用來處理各種需求，與 IPv4/IPv6 有關的部分則落在底層的傳輸，注意用的函式是否支援 IPv6 修改網頁程式支援 IPv6 最重要的工作是將網頁連結處以 Domain Name 取代 IP 位址以取得彈性，同時改用對於 IPv4 及 IPv6 均可以支援的程式語法，儲存 IP 位址的資料庫以及提供用戶輸入位址的操作介面也必須修改為支援 128 位元 IPv6 位址的格式，就可以避開網站在 IPv6 環境下發生問題。

第二節 PHP 支援 IPv6

於 PHP 中没有直接提供函數實現 IPv6 位址的轉換，因此於 PHP 手冊中提到可以透過執行的指令進行 IPv6 位址格式與 long 的資料型態的轉換，參考連結 https://www.php.net/manual/zh/function.ip2long.php#94477，並於執行前先安裝 php-gmp 模組，安裝教學則參考 https://www.php.net/manual/en/gmp.installation.php。

```
// 將 long 資料型態轉換為 IPv6 位址
function long2ip6($ipv6long) {

  $bin = gmp_strval(gmp_init($ipv6long,10),2);
  if (strlen($bin) < 128) {
    $pad = 128 - strlen($bin);
    for ($i = 1; $i <= $pad; $i++) {
    $bin = "0".$bin;
    }
  }
  $bits = 0;
  while ($bits <= 7) {
    $bin_part = substr($bin,($bits*16),16);
    $ipv6 .= dechex(bindec($bin_part)).":";
    $bits++;
  }
  // compress

  return inet_ntop(inet_pton(substr($ipv6,0,-1)));
}

// 將 IPv6 位址轉換為 long 資料型態
function ip2long6($ipv6) {
  $ip_n = inet_pton($ipv6);
  $bits = 15; // 16 x 8 bit = 128bit
  while ($bits >= 0) {
    $bin = sprintf("%08b",(ord($ip_n[$bits])));
    $ipv6long = $bin.$ipv6long;
    $bits--;
  }
  return gmp_strval(gmp_init($ipv6long,2),10);
}
```

無類別域間路由（Classless Inter-Domain Routing、CIDR）是一個用於給用戶分配 IP 位址以及在網際網路上有效地路由 IP 封包的對 IP 位址進行歸類的方法，於 PHP 中也無提供直接處理 IPv6 CIDR 的函數，故需要透過以下函數進行轉換。filter_var 函數在驗證 IP 時，除了使用 FILTER_VALIDATE_IP 之外，也可以使用 FILTER_FLAG_IPV4 來驗證 IPv4 或用 FILTER_FLAG_IPV6 來驗證 IPv6，儲存 IPv6 的欄位長度需要為 varchar（39），如果是要存 varbinary 則為 varbinary（16）。

```
// 將 IPv6 CIDR 取出 first & end ip
function cidr_to_range6（$cidr）{
$a = explode（"/", $cidr）;
$firstaddrstr = $a[0];
if（!filter_var（$firstaddrstr, FILTER_VALIDATE_IP,
FILTER_FLAG_IPV6））{
return null;
}
$prefixlen = $a[1];
$firstaddrbin = inet_pton（$firstaddrstr）;
$firstaddrhex = reset（unpack（'H*', $firstaddrbin））;
$firstaddrstr = inet_ntop（$firstaddrbin）;
$flexbits = 128 - $prefixlen;
$lastaddrhex = $firstaddrhex;
$pos = 31;
while （$flexbits > 0）{
  $orig = substr（$lastaddrhex, $pos, 1）;
  $origval = hexdec（$orig）;
  $newval = $origval |（pow（2, min（4, $flexbits））- 1）;
  $new = dechex（$newval）;
  $lastaddrhex = substr_replace（$lastaddrhex, $new, $pos, 1）;
  $flexbits -= 4;
  $pos -= 1;
}
$lastaddrbin = pack（'H*', $lastaddrhex）;
$lastaddrstr = inet_ntop（$lastaddrbin）;
return ['startip' => $firstaddrstr, 'endip' => $lastaddrstr];
}
```

除了使用上述提供的自訂函數外，如果使用 composer 開發，可以安裝 dTR-IP 套件，來達成上述自訂函數的功能， dTR-IP 套件下載連結與設定說明請參考 http://mikemackintosh.github.io/dTR-IP/。

第三節 ASP.NET（C#）支援 IPv6

C#.NET framework v1.1 版本如果要使用 IPv6 請參考以下範例，如果用 C# 寫一個可以接收用戶端連線的伺服器，此時就會用到底層的 Socket Library，而底層 Socket Library 支援 IPv6 的用法如下：

```
if（!Socket.SupportsIPv6）{
   Console.Error.WriteLine（"Your system does not support IPv6\r\n" +
      "Check you have IPv6 enabled and have changed
machine.config"）;
   return;
}
# 重點在這一行，需要使用 AddressFamily.InterNetworkV6
Socket listener = new Socket（ AddressFamily.InterNetworkV6,
SocketType.Stream, ProtocolType.Tcp）;
listener.Bind（new IPEndPoint（ IPAddress.IPv6Any, PORT））;
listener.Listen（0）;
```

如果用 C#寫用戶端的端程式，以下是用戶端端的範例

```
IPAddress ipa = IPAddress.Parse（IPv6_ADDR）;
IPEndPoint ipeh = new IPEndPoint（ipa, PORT）;
# 重點在 AddressFamily.InterNetworkV6
Socket connection = new Socket（ AddressFamily.InterNetworkV6,
SocketType.Stream, ProtocolType.Tcp）;
```

在取得用戶端 IP address 部分，需要使用 IPv6 的 functions

1.IPAddress.Equals()
2.IPAddress.MapToIPv4() 將 IPAddress 物件對應至 IPv4 位址
3.IPAddress.MapToIPv6()將 IPAddress 物件對應至 IPv6 位址

如果是 Socket 要支援 IPv6

1.TcpListener tcpListenerV4 = new TcpListener（IPAddress.Any, port）;
2.TcpListener tcpListenerV6 = new TcpListener（IPAddress.IPv6Any, port）; # 使用 IPv6Any 欄位來表示 Socket 必須在所有網路介面上接聽 IPv6 用戶端活動

如果作業系統支援 IPv4 跟 IPv6，可以使用

```
TcpClient client = new TcpClient（AddressFamily.InterNetwork）;
```

如果作業系統僅之支援 IPv6，可以使用

```
TcpClient client = new TcpClient（AddressFamily.InterNetworkV6）;
```

在 Unity4.7.2 以及 Unity 5.3.x 版本中對 IPv6 進行了支援，於程式碼中要增加以下設定。

```
原設定
mSocket = new Socket（AddressFamily.InterNetwork,
SocketType.Stream, ProtocolType.Tcp）;

更新後設定
mSocket = new Socket（AddressFamily.InterNetworkV6,
SocketType.Stream, ProtocolType.Tcp）;
```

## 第四節 Python 支援 IPv6

Python 3.7 以後的版本都是有支援 IPv6，不需要引用額外的 Library，細節可以參考 ipaddress.py，官方說明 https://docs.python.org/3/library/ipaddress.html。

使用範例如下

```
socket.getaddrinfo（"www.python.org", 80, 0, 0, socket.SOL_TCP）
[（2, 1, 6, ", （'82.94.164.162', 80））, （10, 1, 6, ",
（'2001:888:2000:d::a2', 80, 0, 0））]
ourSocket = socket.socket（socket.AF_INET6,
socket.SOCK_STREAM, 0）
ourSocket.connect（（'2001:888:2000:d::a2', 80, 0, 0））
```

如果使用 SimpleHTTPServer 模組建立簡單的 Web 伺服器時，由於 SimpleHTTPServer 本身是不支援 IPv6 ，要讓 SimpleHTTPServer 可以支援 Ipv6 時，修改 /usr/lib/python2.7/SimpleHTTPServer.py 檔案內容，結果如下：

```
import socket
def test（HandlerClass = SimpleHTTPRequestHandler,
        ServerClass = BaseHTTPServer.HTTPServer）:
    ServerClass.address_family = socket.AF_INET6
    ServerClass（（'::',8000）,HandlerClass）.serve_forever（）
```

另 SimpleHTTPServer 模組是使用 Python2 語法，於 Python3 時合併至 http.server 中，要讓 http.server 可以支援 IPv6 時，有兩種方法進行調整。

方法一：修改 http.server 模組的內容（/usr/lib/python3.x/http/server.py），於該檔案中加入程式碼，結果如下：

```
    server_address = (bind, port)

#增加以下兩行程式碼
    if ':' in bind:
        ServerClass.address_family = socket.AF_INET6

    HandlerClass.protocol_version = protocol
```

```
    httpd = ServerClass(server_address, HandlerClass)
```

方法二：自行定義 httpserver

```
import http.server
import socketserver
import socket
class HTTPServerV6(http.server.HTTPServer):
  address_family = socket.AF_INET6

Handler = http.server.SimpleHTTPRequestHandler
server = HTTPServerV6(('::', 8000), Handler)
server.serve_forever(
```

如於 Python 2.6 中透過 urlparse 模組解析 url 中的引數，該模組無法正確解析 IPv6 網址，因此於 Python 2.7 與 Python 3 時有修正該錯誤，同時 Python 3 時將 urlparse 模組改成 urllib.parse 模組。故如要進行解析可以直接將 Python 版本升級到 2.7 以上的版本。但如果必須用 Python 2.6 時，則可以從 Python 2.7 複製 urlparse 模組並取成不一樣的模組名稱例如 urlparseipv6，接著再 import 進來即可，可參考以下指令。

```
from external import urlparseipv6 as urlparse
```

## 第五節 Java 支援 IPv6

Java 從 1.4 版開始支持 Linux 和 Solaris 平台上的 IPv6。1.5 版起又加入了 Windows 平台上的支持。Java 很好封裝了 IPv4 和 IPv6 兩種版本的不同，Java 一般不需要在程式碼額外編寫如何支援 IPv6， Java 提供了 java.net.preferIPv4Stack、java.net.preferIPv6Addresses 兩個系統屬性進行設置所使用的 IP 協議。

Java 要使用 IPv6 時，需要設定以下設定

```
System.setProperty（"java.net.preferIPv6Addresses","true"）
```

如果要在 JVM 支援 IPv6，則需要使用以下設定

```
-Djava.net.preferIPv4Stack=false
-Djava.net.preferIPv6Addresses=true
```

另外，使用 InetAddress.getLocalHost ()函數可以返回本機 IP 地址，最终返回的是 IPv4 還是 IPv6 位址，則由 java.net.preferIPv6Addresses 的值來決定，當 java.net.preferIPv6Addresses 為預設值 false 時，則優先使用 IPv4 位址，反之設為 true，則會優先使用 IPv6 地址。

## 第六節 Javascript 支援 IPv6

如果是 nodejs 內要使用 IPv6，可以使用 node-ip6addr 這個 library，資料可以從 https://github.com/joyent/node-ip6addr 網路上下載。

安裝方式

執行指令
npm install ip6addr

以下為使用範例參考

```
> var addr1 = ip6addr.parse（'fd00::0123'）
> addr1.toString（）
'fd00::123'
> var addr2 = ip6addr.parse（'1.2.3.4'）
> addr2.toString（）
'1.2.3.4'
> var addr3 = ip6addr.parse（'::ffff:127.0.0.1'）
> addr3.toString（）
'::ffff:127.0.0.1'

> var sub1 = ip6addr.createCIDR（'fe80::/10'）
> sub1.toString（）
'fe80::/10'
> var sub2 = ip6addr.createCIDR（'fc00::', 7）
> sub2.toString（）
'fc00::/7'
> var sub3 = ip6addr.createCIDR（'10.0.0.0', 8）
> sub3.toString（）
'10.0.0.0/8'
```

# 第八章 檢測項目

## 第一節 IPv6 設定檢測

針對 IPv6 之設定是否已成功完成，將其必要的統整項目整理至下表中，可透過表格中敘述的測試工具與測試方式，判斷網路設備是否已支援 IPv6。

表 21 ICP 業者的 IPv6 設定檢測表

| 編號 | 分類 | 設定測試 | 必測與否 | 通過條件 | 測試方式 | 測試工具 |
|---|---|---|---|---|---|---|
| CT-1 | 主機 | 網站的 IPv6 位址可以連上 (http 或 https) | 是 | Trying 顯示 IPv6 位址、出現 TCP_NODELAY set、Connected to Connected to 網址(IPv6 位址) port 443 、並顯示 successfully set certificate verify locations 出現 HTTP/2 200 | curl -v 網址 --head | curl |
| CT-2 | 路由器 | 沿途路由器都有 IPv6 位址 | 是 | 顯示沿途路由器 IPv6 位址 | traceroute6 根網域 | traceroute6 |
| CT-3 | DNS | 網站是否有正確設定 IPv6 位址 | 是 | 顯示 IPv6 位址 | dig aaaa 根網域 @8.8.8.8 +short | dig |
| CT-4 | DNS | 網站使用的所有 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short NS | dig |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | DNS Server 本身要有 IPv6 位址 | | | 根網域`;<br>do echo -n "$i => [ipv6] ";<br>dig aaaa $i @8.8.8.8 +short;<br>done | |
| CT-5 | DNS | 網站使用的 DNS 的 IPv6 都可以 PING 通過 | 是 | 成功顯示 PING 到的 IPv6 位址 | ping6 根網域 | ping6 |
| CT-6 | DNS | 網站使用的 DNS 要設定網站根網域的 IPv6 位址 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short NS 根網域`;<br>do echo -n "$i => [ipv6] ";<br>dig aaaa 根網域 @$i +short;<br>done | dig |
| CT-7 | Mail Server | 網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上 | 是 | 顯示 IPv6 位址 | for i in `dig @8.8.8.8 +short MX 根網域`;<br>do echo -n "$i => [ipv6] ";<br>dig aaaa $i @8.8.8.8 +short;<br>done; | dig |

以 TWNIC 財團法人台灣網路資訊中心（www.twnic.net.tw）為例，分別針對上表 ICP 業者的 IPv6 設定檢測表的測試項目進行測試。

1.網站的 IPv6 位址可以連上（http 或 https）

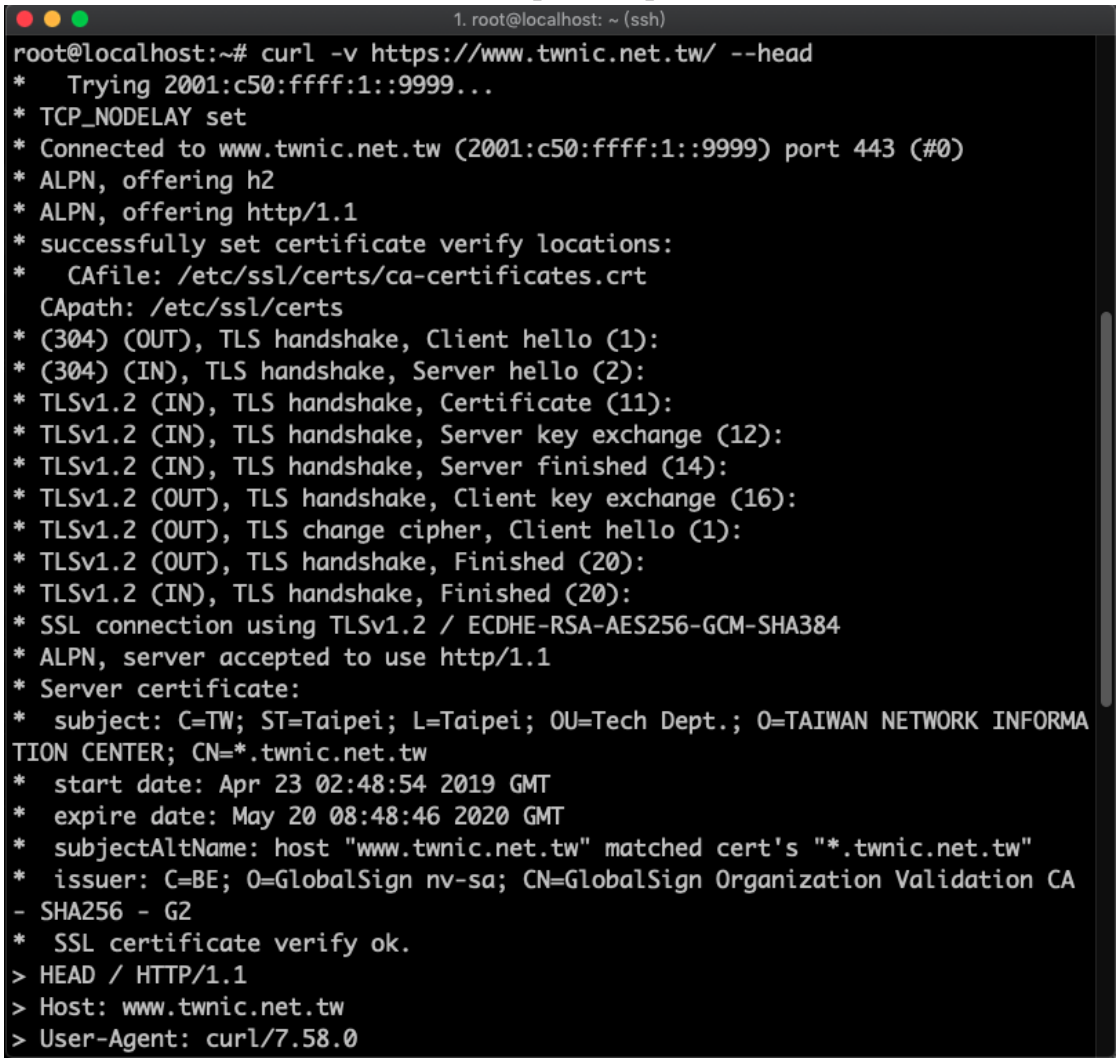



圖 113 TWNIC CT-1 測試結果畫面之一

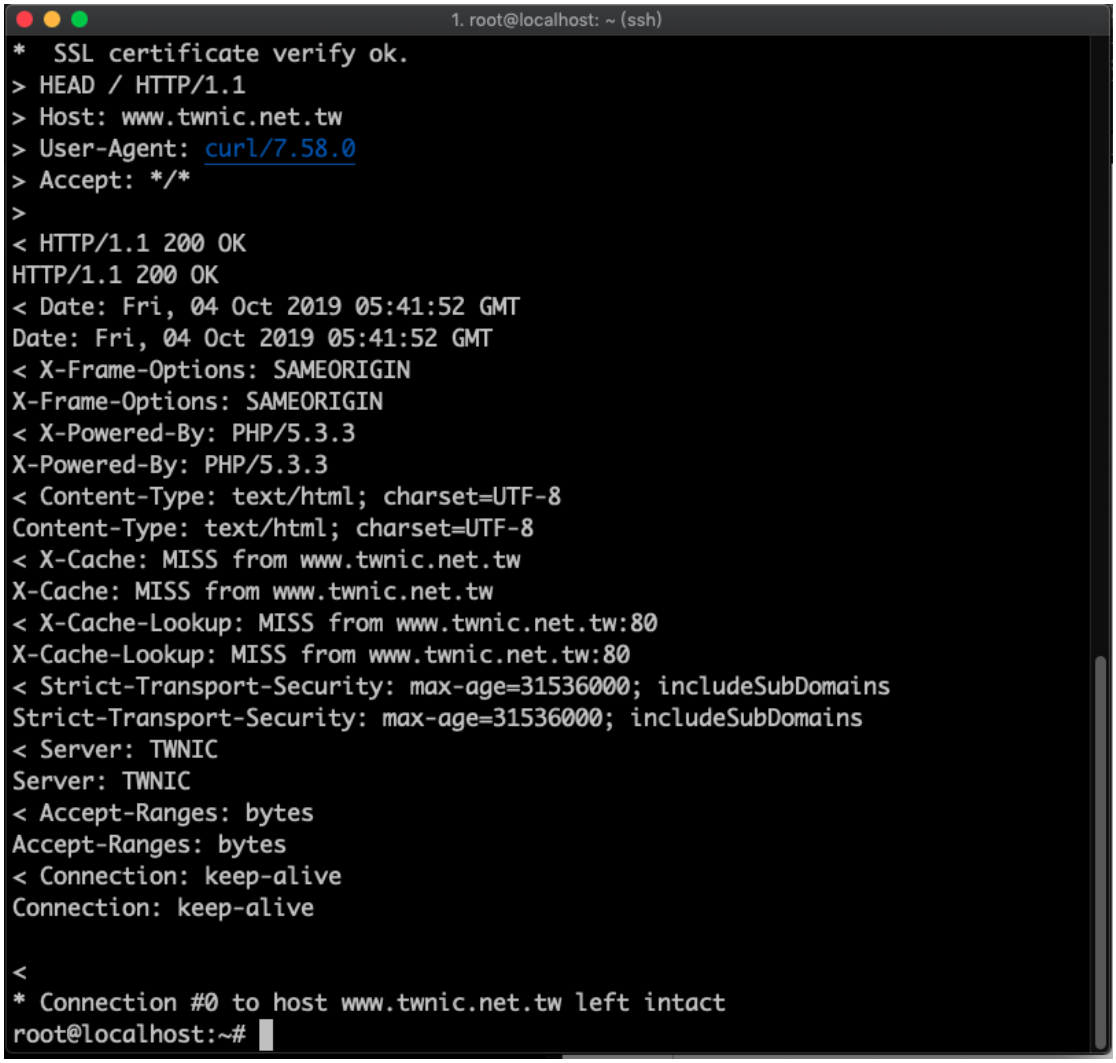



圖 114 TWNIC CT-1 測試結果畫面之二

2.沿途路由器都有 IPv6 位址

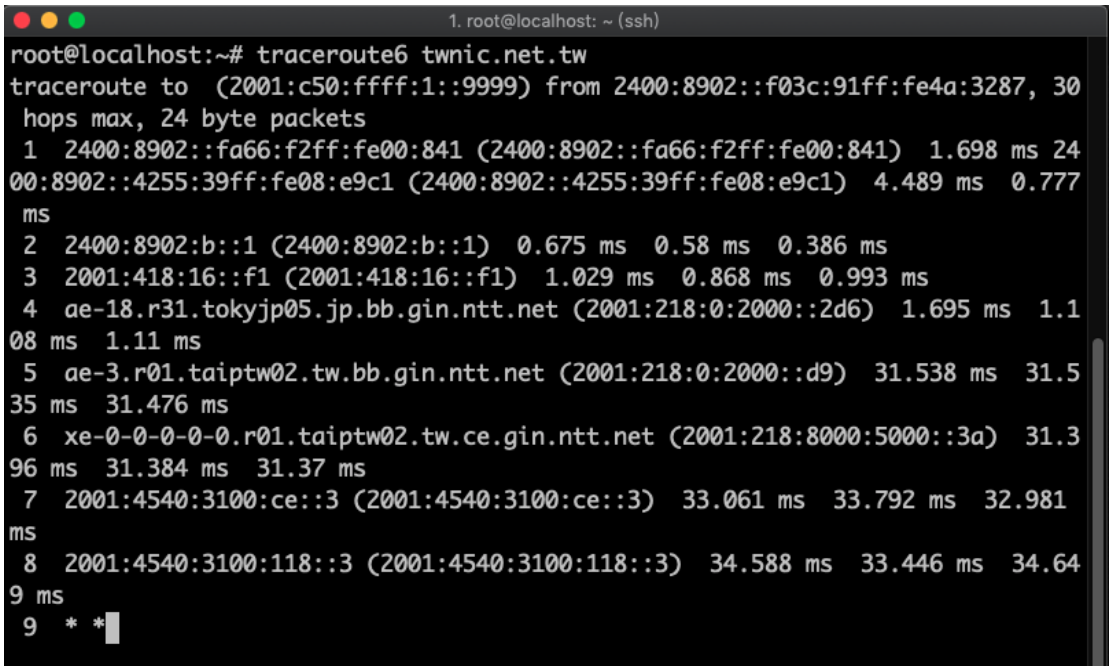


圖 115 TWNIC CT-2 測試結果畫面

3.網站是否有正確設定 IPv6 位址

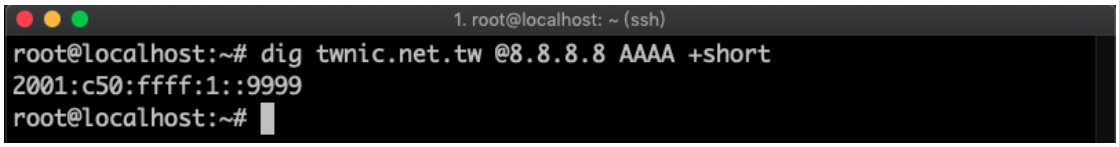



圖 116 TWNIC CT-3 測試結果畫面

4.網站使用的所有 DNS Server 本身要有 IPv6 位址

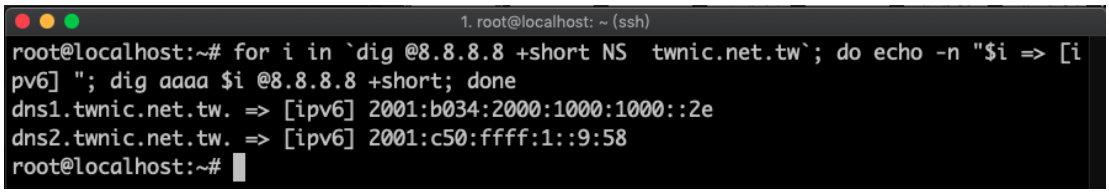



圖 117 TWNIC CT-4 測試結果畫面

5.網站使用的 DNS 的 IPv6 都可以 PING 通過

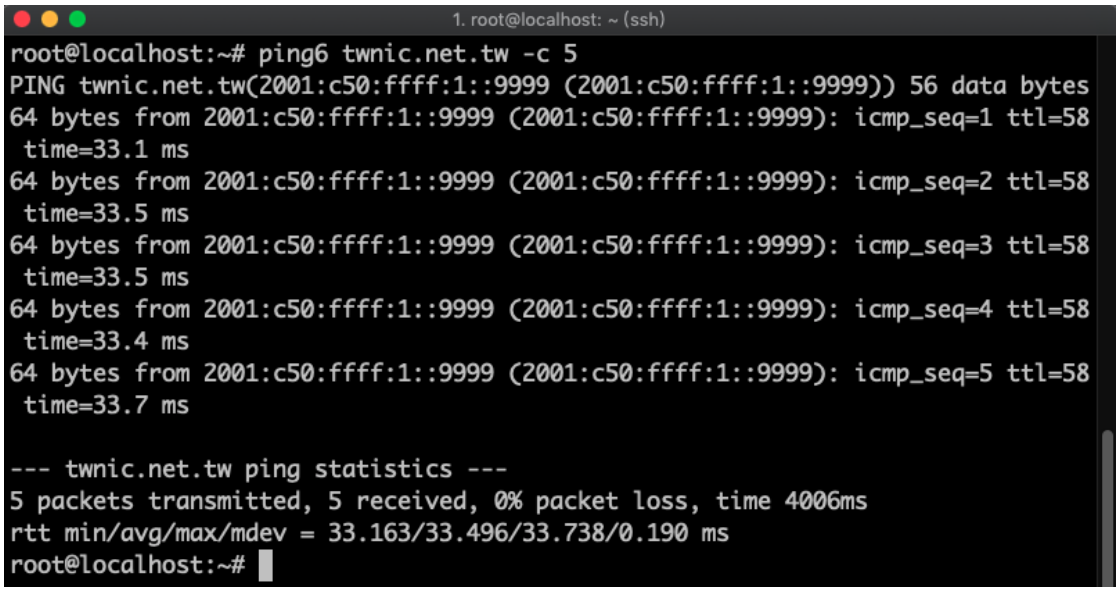



圖 118 TWNIC CT-5 測試結果畫面

6.網站使用的 DNS 要設定網站根網域的 IPv6 位址(如果沒出現，代表該主機不支援 IPv6)

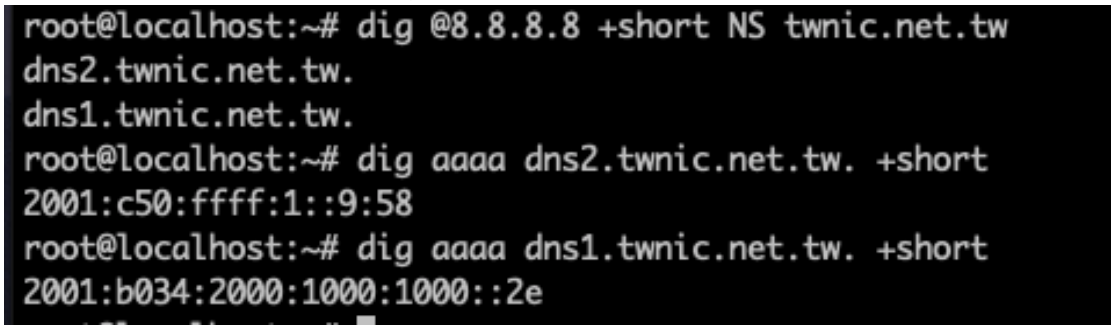


圖 119 TWNIC CT-6 測試結果畫面

7.網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上 (TWNIC 的 MX 沒有設定 IPv6）

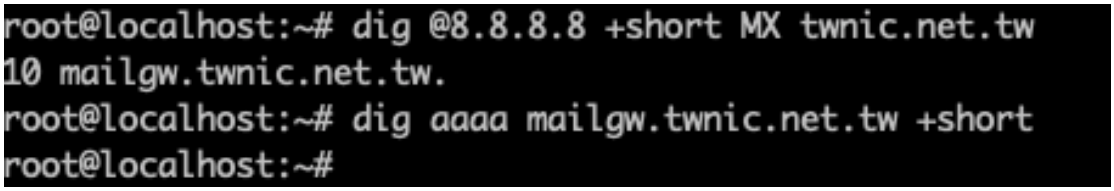



圖 120 TWNIC CT-7 測試結果畫面

## 第二節 網路安全檢查檢測

下表列出雙協定網路下可以檢測的安全項目與工具，透過測試工具可以模擬外界常見的網路攻擊，並檢視其結果是否通過，惟並非所有工具皆可已從外網進行測試，故於表格後僅提供可以從外網進行的測試結果範例，其餘工具還要自行於內網中進行測試並檢測其結果。

表 22 雙協定網路安全檢測項目

| 編號 | 分類 | 網路安全測試項目 | 必測與否 | 測試方式 | 測試工具 |
|---|---|---|---|---|---|
| 以下為 IPv6 測試使用(可於外網進行測試) | | | | | |
| ST-1 | 路由器 | 未經驗證或者偽照的裝置 | 是 | thcsyn6 [-AcDrRS] [-p port] [-s sourceip6] interface target port | thcsyn6 |
| ST-2 | 路由器 | 未經驗證或者偽照的裝置 | 是 | exploit6 interface destination [test-case-number] | exploit6 |
| ST-3 | 路由器 | DDoS 攻擊（ICMPv6） | 是 | fuzz_ip6 [-x] [-t number \| -T number] [-p number] [-IFSDHRJ] [-X\|-1\|-2\|-3\|-4\|-5\|-6\|-7\|-8\|-9\|-0 port] interface unicast-or-multicast-address [address-in-data-pkt] | fuzz_ip6 |
| ST-4 | 路由器 | Ping of Death（PoD） | 是 | frag6 -i [interface] --frag-id-policy -d [destination] | frag6 |
| ST-5 | 路由器 | 網路掃描 | 是 | flow6 -i [interface] --flow-label-policy -d [destination] -v | flow6 |

| | | | | | |
|---|---|---|---|---|---|
| ST-6 | 網站主機 | DDoS 攻擊（Smurf 攻擊） | 是 | implementation6 [-p] [-s sourceip6] interface destination [test-case-number] | implementation6 |
| ST-7 | 其他 | DDos 攻擊（Duplicate Address Detection） | 是 | flood_mld6 interface | flood_mld6 |
| ST-8 | 其他 | Upper Layer Header 的攻擊 | 是 | flood_mld26 interface | flood_mld26 |
| ST-9 | 其他 | Atomic Fragment 攻擊 | 是 | denial6 interface destination test-case-number | denial6 |
| 以下為 IPv6 測試使用(需於內網進行測試) | | | | | |
| ST-10 | 路由器 | DDoS 攻擊（Router Advertisement） | 是 | inject_alive6 [-ap] interface | alive6 |
| ST-11 | 路由器 | DDoS 攻擊（neighbor advertisements） | 是 | inject_alive6 [-ap] interface | alive6 |
| ST-12 | 路由器 | DDoS 攻擊（MLD reports） | 是 | redir6 interface victim-ip target-ip original-router new-router [new-router-mac] [hop-limit] | redir6 |

| | | | | | |
|---|---|---|---|---|---|
| ST-13 | 路由器 | DDoS 攻擊（MLDv2 reports） | 是 | dos-new-ip6 interface | dos-new-ip6 |
| ST-14 | 路由器 | 中間人攻擊 | 是 | fake_mipv6 interface home-address home-agent-address care-of-address | fake_mipv6 |
| ST-15 | 路由器 | DDoS 攻擊（unknown options） | 是 | fake_advertise6 [-DHF] [-Ors] [-n count] [-w seconds] interface ip-address-advertised [target-address [mac-address-advertised [source-ip-address]]] | fake_advertiser6 |
| ST-16 | 網站主機 | DDoS 攻擊（Smurf 攻擊） | 是 | implementation6d interface | implementation6d |
| ST-17 | DNS | 滲透測試 | 是 | flood_dhcpc6 [-n\|-N] [-1] [-d] interface [domain-name] | flood_dhcpc6 |
| ST-18 | DNS | 未經驗證或者偽照的裝置 | 是 | toobig6 [-u] interface target-ip existing-ip mtu [hop-limit] | toobig6 |
| ST-19 | DNS | 未經驗證或者偽照的裝置 | 是 | fake_dns6d interface ipv6-address [fake-ipv6-address [fake-mac]] | fake_dns6d |
| ST-20 | DNS | 未經驗證或者偽照的裝置 | 是 | fake_dnsupdate6 dns-server full-qualified-host-dns-name ipv6address | fake_dnsupdate6 |

| | | | | | |
|---|---|---|---|---|---|
| ST-21 | 作業系統 | CVE-2003-0429 Ethereal OSI 解析緩衝區溢位漏洞 | 是 | mitm6.py [-h] [-i INTERFACE] [-l LOCALDOMAIN] [-4 ADDRESS] [-6 ADDRESS] [-m ADDRESS] [-a] [-v] [--debug] [-d DOMAIN] [-b DOMAIN] [-hw DOMAIN] [-hb DOMAIN] [--ignore-nofqdn] | mitm6 |
| ST-22 | 作業系統 | CVE-2004-0257 OpenBSD ICMPv6 處理遠程 DDoS 攻擊漏洞 | 是 | fake_mld6 [-l] interface add\|delete\|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]] | fake_mld6 |
| ST-23 | 防火牆 | DDoS 攻擊（TCP-SYN） | 是 | fake_mld26 [-l] interface add\|delete\|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]] | fake_mld26 |
| ST-24 | 防火牆 | 網路掃描 | 是 | fake_mldrouter6 [-l] interface advertise\|solicitate\|terminate [own-ip [own-mac-address]] | fake_mldrouter6 |
| ST-25 | 防火牆 | 基本設定 | 是 | fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router- | fake_router6 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ip-link-local [mtu [mac-address]]]] | |
| ST-26 | 防火牆 | 基本設定 | 是 | flood_router6 [-HFD] interface | flood_router6 |
| ST-27 | 其他 | DDoS 攻擊 | 是 | flood_advertise6 [-k \| -m mac] interface [target] | flood_advertise6 |
| ST-28 | 其他 | 未經驗證或者偽照的裝置 | 是 | ndpexhaust26 [-acpPTUrR] [-s sourceip6] interface target-network | ndpexhaust26 |
| ST-29 | 其他 | 未經驗證或者偽照的裝置 | 是 | parasite6 [-lRFHD] interface [fake-mac] | parasite6 |
| ST-30 | 其他 | 安全評估工具（flow label） | 是 | smurf6 interface victim-ip [multicast-network-address] | smurf6 |
| ST-31 | 其他 | 掃描工具 | 是 | rsmurf6 interface victim-ip | rsmurf6 |
| 以下為 IPv4 測試使用 | | | | | |
| ST-32 | 路由器 | 中間人攻擊 | 是 | arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP] | Arpspoof |
| ST-33 | 防火牆 | DDoS 攻擊 | 是 | hping3 --traceroute -V -1 網站 | hping3 |
| ST-34 | 防火牆 | 中間人攻擊 | 是 | 圖形化介面操作 | ettercap |
| ST-35 | 防火牆 | DDoS 攻擊, 中間人攻擊 | 是 | 圖形化介面操作 | Evil FOCA |

1.使用 thcsyn6 測試工具

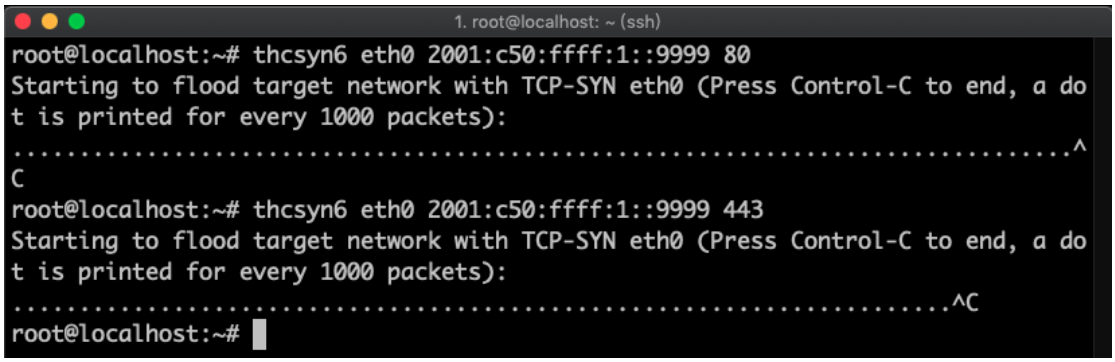



圖 121 TWNIC ST-1 測試結果畫面

2.使用 exploit6 測試工具

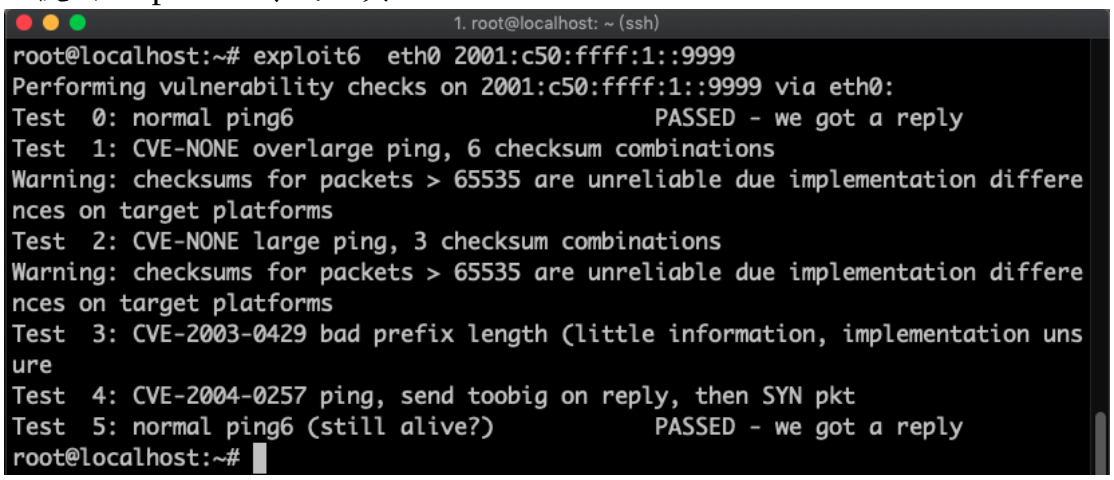



圖 122 TWNIC ST-2 測試結果畫面

3.使用 fuzz_ip6 測試工具


圖 123 TWNIC ST-3 測試結果畫面

4.使用 frag6 測試工具

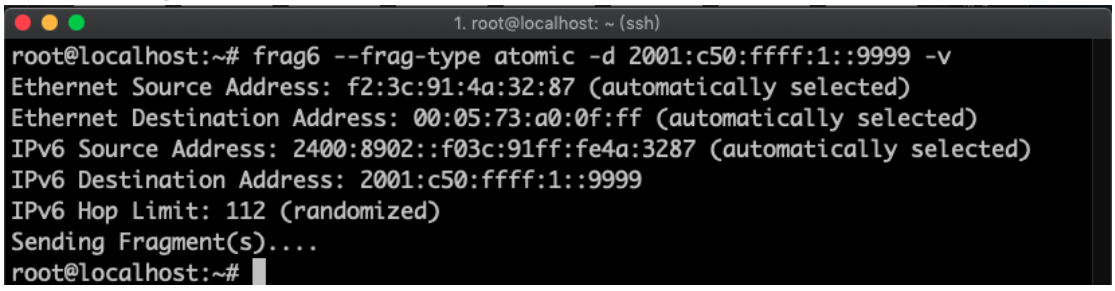



圖 124 TWNIC ST-4 測試結果畫面

5.使用 flow6 測試工具

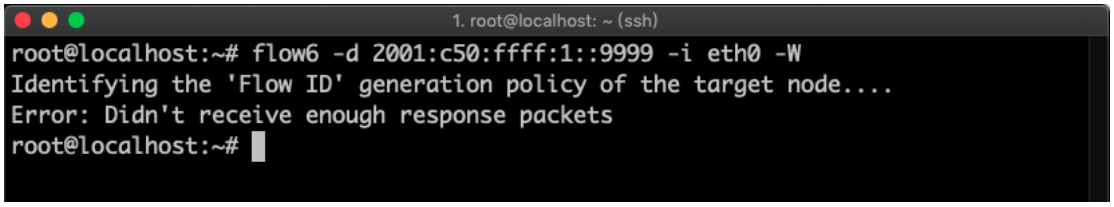



圖 125 TWNIC ST-5 測試結果畫面

6.使用 implementation6 測試工具

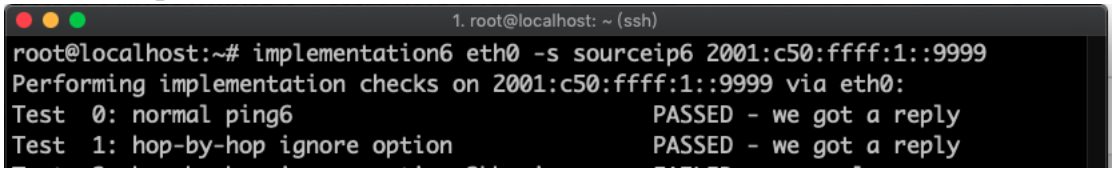



圖 126 TWNIC ST-6 測試結果畫面

7.使用 flood_mld6 測試工具


圖 127 TWNIC ST-7 測試結果畫面

8.使用 flood_mld26 測試工具


圖 128 TWNIC ST-8 測試結果畫面

9.使用 denial6 測試工具


圖 129 TWNIC ST-9 測試結果畫面

# 參考資料


[1]RFC 1576 TN3270 Current Practices
https://tools.ietf.org/html/rfc1576
[2]RFC 1883 Internet Protocol, Version 6 （IPv6） Specification
https://tools.ietf.org/html/rfc1883
[3]RFC 2401 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc2401
[4]RFC 2402 IP Authentication Header
https://tools.ietf.org/html/rfc2402
[5]RFC 2406 IP Encapsulating Security Payload （ESP）
https://tools.ietf.org/html/rfc2406
[6]RFC 2460 Internet Protocol, Version 6 （IPv6） Specification
https://tools.ietf.org/html/rfc2460
[7]RFC 2462 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc2462
[8]RFC 3852 Cryptographic Message Syntax （CMS）
https://tools.ietf.org/html/rfc3852
[9]RFC 4301 Security Architecture for the Internet Protocol
https://tools.ietf.org/html/rfc4301
[10]RFC 4862 IPv6 Stateless Address Autoconfiguration
https://tools.ietf.org/html/rfc4862
[11]RFC 4864 Local Network Protection for IPv6
https://tools.ietf.org/html/rfc4864
[12]RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
https://tools.ietf.org/html/rfc4941
[13]RFC 5902 IAB Thoughts on IPv6 Network Address Translation
https://tools.ietf.org/html/rfc5902
[14]RFC 5996 Internet Key Exchange Protocol Version 2 （IKEv2）
https://tools.ietf.org/html/rfc5996
[15]RFC 6437 IPv6 Flow Label Specification
https://tools.ietf.org/html/rfc6437
[16]RFC 6564 A Uniform Format for IPv6 Extension Headers
https://tools.ietf.org/html/rfc6564
[17]RFC 6883 IPv6 Guidance for Internet Content Providers and Application Service Providers
https://tools.ietf.org/html/rfc6883
[18]A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients
https://petsymposium.org/2015/papers/02_Perta.pdf
[19]Understanding IPv6 And DNS Leaking, by Jay H Simmons
https://www.vpncrew.com/understanding-ipv6-and-dns-leaking/

[20]IPv6 Address Representation and Address Types, by Rick Graziani., 03 Oct 2017
http://www.ciscopress.com/articles/article.asp?p=2803866&seqNum=5
[21]The Difference Between IPv6 and IPv4 IP Addresses
https://www.coursehero.com/file/15205432/The-Difference-Between-IPv6-and-IPv4-IP-Addresses/
[22]IPV6 MULTICAST - MULTICAST LISTENER DISCOVERY（MLD）, by INE
https://blog.ine.com/2009/12/26/ipv6-multicast-multicast-listener-discovery-mld
[23]Internet Protocols: Versions 4 and 6 Analysis and Comparison of IPv4 and IPv6, by Wushi09, 21 Sep 2015
https://www.cybrary.it/0p3n/internet-protocols-versions-4-and-6-analysis-and-comparison-of-ipv4-and-ipv6/
[24]為何值得為 IPv6 的建置努力的三大理由, 台網中心電子報 2019/02
https://blog.twnic.net.tw/2019/01/31/2361/
[25]What is IPv6 stateless address auto-configuration?
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiBpeiroq3kAhXMGKYKHWMhAbYQFjACegQIDBAG&url=https%3A%2F%2Fmysupport.netapp.com%2FNOW%2Fpublic%2Feseries%2Fsam%2FGUID-8538272A-B802-49D9-9EA2-96C82DAD26A2%2FGUID-06C52868-5C1F-4E76-86D5-4815C2E9EBC6.html&usg=AOvVaw2Bil-09MU4QCW5earvN8lT
[26]中華電信公司 HiNet IPv6 用戶連線參考手冊
http://adsl.hinet.net/download/HiNet-IPv6_User_Guide.pdf
[27]中華電信 HiNet IPv6 固定制服務說明
http://adsl.hinet.net/static_ipv6.html
[28]QoS － 未來行動網路的服務品質保證
https://www.ctimes.com.tw/DispArt/tw/-IPv4/IETF/-IEEE/-MOD/-VoIP/0404251100SZ.shtml
[29]IPv6 Routing for Mobility Environments
https://www.researchgate.net/publication/228395858_IPv6_Routing_for_Mobility_Environments
[30]台灣 2018 年 IPv6 成長速度創全球第一, 台網中心電子報 2019/04
https://blog.twnic.net.tw/2019/03/29/3058/
[31]IPv6/IPv4 IPv6/IPv4 轉換技術
http://www.ipv6.org.tw/docu/elearning8_2005/1009402616b-19.pdf
[32]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6

https://books.google.com.tw/books?id=FbYjJjZNA5gC&pg=PA335&lpg=PA335&dq=ipv6+0x0800+0x86DD&source=bl&ots=5mIjGIwW_E&sig=ACfU3U34zzWevIUhxbY4H7HL3ofpwDgKpg&hl=zh-TW&sa=X&ved=2ahUKEwjbxp3A167kAhXjGKYKHYrSCbIQ6AEwEnoECAcQAQ#v=onepage&q=ipv6%200x0800%200x86DD&f=false
[33]IPv6 跟現階段 IP 位址配發差異與發展技術介紹
https://www.cadch.com/modules/news/article.php?storyid=132
[34]剖析 IPv6 的安全風險問題
http://www.rl-tech.com.tw/zh-tw/article_info.php?id=13
[35]IPv6 Security
https://books.google.com.tw/books?id=kwOv0Aw2lIUC&pg=PT360&lpg=PT360&dq=ipv6+esp&source=bl&ots=Qmr93IAZ4f&sig=ACfU3U171Cq1dpyz0vyy1eSsYSmXg8hB7g&hl=zh-TW&sa=X&ved=2ahUKEwjSoJSL36_kAhUNCqYKHRuuCGM4ChDoATADegQIBhAB#v=onepage&q=ipv6%20esp&f=false
[36]Configuring IPv6 For Cisco IOS
https://books.google.com.tw/books?id=rj45JvYuOdIC&pg=PA275&lpg=PA275&dq=HMAC+ipv6&source=bl&ots=_jaIgiQBij&sig=ACfU3U1uuYAvFBGqK4JpBhDLJQBrPYiMuA&hl=zh-TW&sa=X&ved=2ahUKEwinmbC24a_kAhVHGaYKHTFbBTYQ6AEwB3oECAcQAQ#v=onepage&q=HMAC%20ipv6&f=false
[37]剖析 IPv6 的安全風險問題
http://www.rl-tech.com.tw/zh-tw/article_info.php?id=13
[38]IPv6 作業系統與應用服務建置實習（Linux）
http://www.wkb.idv.tw/moodle/pluginfile.php/15554/mod_page/content/7/IPv6%20Linux 講義.pdf
[39]中華電信 IPv6 通訊協定與特性介紹
http://163.28.82.8/data2/seminar99/ipv611.pdf
[40]IPv6 Packet Security
http://www.ipv6now.com.au/primers/IPv6PacketSecurity.php
[41]IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
https://books.google.com.tw/books?id=AMkmDwAAQBAJ&pg=PT111&lpg=PT111&dq=why+ipv6+doesn%27t+need+ihl&source=bl&ots=dpjoVgYmmv&sig=ACfU3U0XBRFNlOAC8zLPTf9zs5k1rp-rHw&hl=zh-TW&sa=X&ved=2ahUKEwj1l_7y06rkAhUiy4sBHTweC5QQ6AEwCnoECAgQAQ#v=snippet&q=security&f=false
[42]An integrated testing system for IPv6 and DNSSEC
https://jwcn-

eurasipjournals.springeropen.com/articles/10.1186/s13638-016-0675-4
[43]IPv6 Security: Attacks and Countermeasures in a Nutshell
https://www.sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pd
[44]IPv6-ready system check
http://tldp.org/HOWTO/Linux+IPv6-HOWTO/ch04s01.html
[45]ROGUE ROUTER ADVERTISEMENT ATTACK
http://6lab.cz/rogue-router-advertisement-attack/
[46]How To Detect & Prevent Rogue Devices on Your Network with UDT
https://www.youtube.com/watch?v=EZBaiEDTrfQ
[47]Attackers Can Use IPv6 to Launch Man-in-the-Middle Attacks
https://www.eweek.com/security/attackers-can-use-ipv6-to-launch-man-in-the-middle-attacks
[48]IPv6 MITM via fake router advertisements
https://isc.sans.edu/forums/diary/IPv6+MITM+via+fake+router+advertisements/10660/
[49]35 Types of DDoS Attacks Explained
https://javapipe.com/blog/ddos-types/
[50]Could IPv6 Result in More DDoS Attacks?
https://www.allot.com/blog/ipv6_ddos_attack_vulnerability/
[51]How to Prepare for IPv6 DDoS attack
https://medium.com/@CybriantMSSP/how-to-prepare-for-ipv6-ddos-attack-4620cba369fc
[52]IPv6 DDoS and Protection Measures
https://community.infoblox.com/t5/IPv6-CoE-Blog/IPv6-DDoS-and-Protection-Measures/ba-p/12830
[53]IPv6 extension headers and security: Analyzing the risk
https://searchsecurity.techtarget.com/tip/IPv6-extension-headers-and-security-Analyzing-the-risk
[54]IPv6 Extension Headers Review and Considerations
https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html
[55]Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers
https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering-04
[56]Security implication and detection of threats due to manipulating IPv6 extension headers
https://ieeexplore.ieee.org/document/6726061
[57]Security Impacts of Abusing IPv6 Extension Headers
https://media.blackhat.com/ad-12/Atlasis/bh-ad-12-security-impacts-atlasis-wp.pdf

[58]thc-ipv6 工具包
https://www.mankier.com/package/thc-ipv6
[59]Get your site ready for IPv6: a step-by-step guide
https://blog.mythic-beasts.com/2014/09/15/get-your-site-ready-for-ipv6-a-step-by-step-guide/
[60]How To Configure Tools to Use IPv6 on a Linux VPS, by Justin Ellingwood, 01 Apr 2014
https://www.digitalocean.com/community/tutorials/how-to-configure-tools-to-use-ipv6-on-a-linux-vps#checking-ipv6-dns-informatio
[61] ICANNWiki
https://icannwiki.org/IPv6
[62]IPv6 Multicast Address Space Registry
https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml
[63]IPv6 multicast addresses
https://study-ccna.com/ipv6-multicast-addresses/

# 中英專有名詞對照

A

ACL 存取控制列表（Access Control List）

ARP 位址解析協定（Address Resolution Protocol）

D

DDoS attack 阻斷服務攻擊（distributed denial-of-service attack）

DNS 網域名稱伺服器（Domain Name System）

DHCP 動態主機組態協定（Dynamic Host Configuration Protocol）

Dual Stack IPv4/ IPv6 雙協定（Dual Stack）

E

Email 電子郵件（Electronic mail）

F

Firewall 防火牆

FTP 檔案傳輸協定（File Transfer Protocol）

I

IaaS 基礎設施即服務（Infrastructure as a Service）

IAB 網際網路結構委員會（Internet Architecture Board）

ICMP 網際網路控制訊息協定（Internet Control Message Protocol）

ICMPv6 網際網路控制訊息協定 第六版（Internet Control Message Protocol Version 6）

ICP 網路內容供應商（Internet Content Provider）

IETF 網際網路工程任務小組（Internet Engineering Task Force）

IDC 資訊機房（Internet Data Center）

IPsec 網際網路安全機制（Internet Protocol Security）

IPv4 網際網路通訊協定第四版（Internet Protocol version 4）

IPv6 網際網路通訊協定第六版（Internet Protocol version 6）

IPv6 Day IPv6 日（IPv6 Day）

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章

IPv4/IPv6 Dual Stack 網際網路通訊協定第四版及第六版雙軌並行（IPv4/v6 Dual Stack）

ISP 網際網路服務提供者（Internet Service Provider）

IASP 網際網路服務提供者（Internet Access Service Provider）

IT 資訊技術（Information Technology）

L

L3 Switch 第三層交換器（Layer 3 Switch）

Load Balancers 負載平衡器

M

Mobile Internet 行動上網（Mobile Internet）

N

NAT 網路位址轉譯（Network Address Translation）

Network Layer 網路層（Network Layer）

P

Proxy 代理伺服器

Q

QoS 服務品質（Quality of Service）

R

RARP 逆位址解析協定（Reverse Address Resolution Protocol）

RFC 網際網路協定規範（Request For Comments）

Router 路由器

T

TCP 傳輸控制協定（Transmission Control Protocol）

TWNIC 財團法人台灣網路資訊中心（Taiwan Network Information Center）

W

WWW 全球資訊網（World Wide Web）

WiFi AP 無線基地台（WiFi AP）