

# Partner

如何設定

Windows DHCP log

V011

2024/04/16



## 版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

## 商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

# 目錄

前言 .....	2
<b>1. NXLog .....</b>	<b>3</b>
1.1 NXLog 安裝 .....	3
1.2 NXLog 設定檔下載 .....	5
1.2.1 Windows 2003 或之前版本作業系統.....	5
1.2.2 Windows 2008 或之後版本作業系統.....	6
1.3 NXLog 設定檔 .....	7
1.4 NXLog 啟動服務 .....	8
1.4.1 Windows 2003 或之前版本作業系統.....	8
1.4.2 Windows 2008 或之後版本作業系統.....	11
<b>2. Windows 2003 .....</b>	<b>14</b>
<b>3. Windows 2008 .....</b>	<b>17</b>
3.1 DHCP IPv4.....	17
3.2 DHCP IPv6.....	20
<b>4 Windows 2012 .....</b>	<b>22</b>
4.1 DHCP IPv4.....	22
4.2 DHCP IPv6.....	25
<b>5. Windows 2016 .....</b>	<b>28</b>
5.1 DHCP IPv4.....	28
5.2 DHCP IPv6.....	31
<b>6. Windows 2019 .....</b>	<b>34</b>
6.1 DHCP IPv4.....	34
6.2 DHCP IPv6.....	37
<b>7. Windows 2022 .....</b>	<b>40</b>
7.1 DHCP IPv4.....	40
7.2 DHCP IPv6.....	43
<b>8. N-Reporter .....</b>	<b>46</b>
<b>9. 問題排除.....</b>	<b>48</b>
9.1 調整 DHCP 記錄檔案大小.....	48

## 前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 Windows DHCP 記錄。  
NXLog 工具將 Windows DHCP 記錄轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。  
此文件適用於作業系統的 Windows Server 2003 / 2008 / 2012 / 2016 / 2019 / 2022 版本。

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

# 1. NXLog

## 1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition)

前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 nxlog-ce-x.x.xxxx.msi · 範例: nxlog-ce-3.0.2272.msi



Windows

nxlog-ce-3.0.2272.msi

註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

<2.1.1> 開啟 [Windows PowerShell]



<2.1.2> 安裝 NXLog 軟體

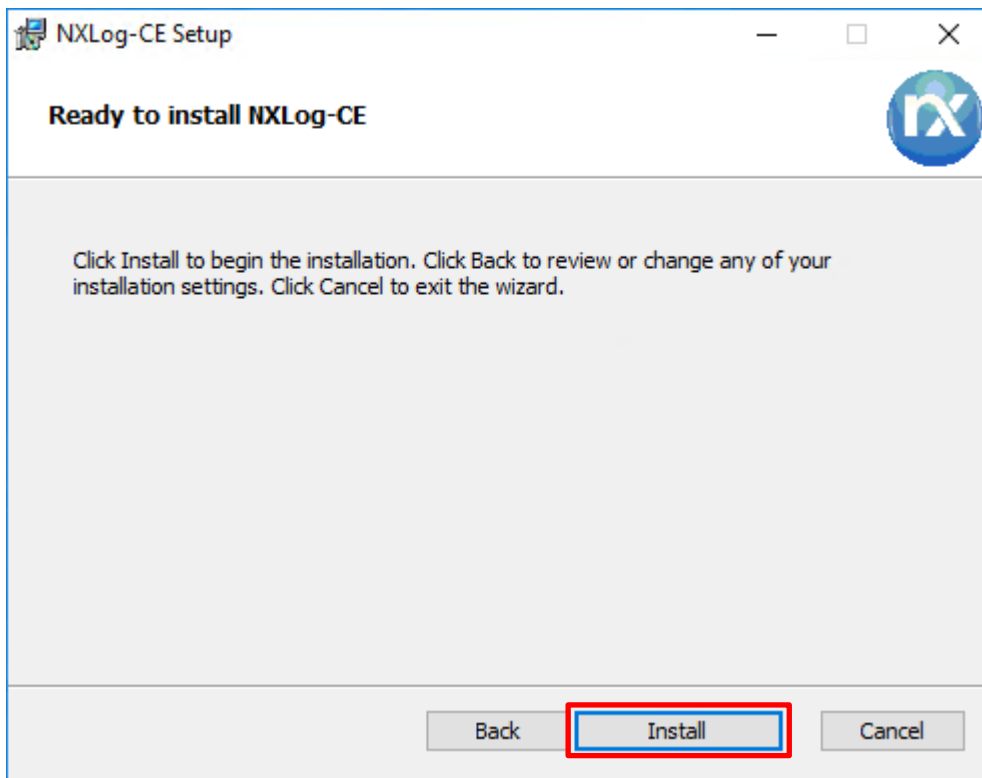
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```

```
系統管理員: Windows PowerShell
PS C:\> Install-Package .\nxlog-ce-3.0.2272.msi -Force
Name                           Version      Source      Summary
----                           -
NXLog-CE                        3.0.2272    C:\nxlog-ce-3...
PS C:\> _
```

紅色文字部位請輸入 NXLog 軟體路徑和檔案

<2.2> Windows 2003

點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish]



## 1.2 NXLog 設定檔下載

### 1.2.1 Windows 2003 或之前版本作業系統

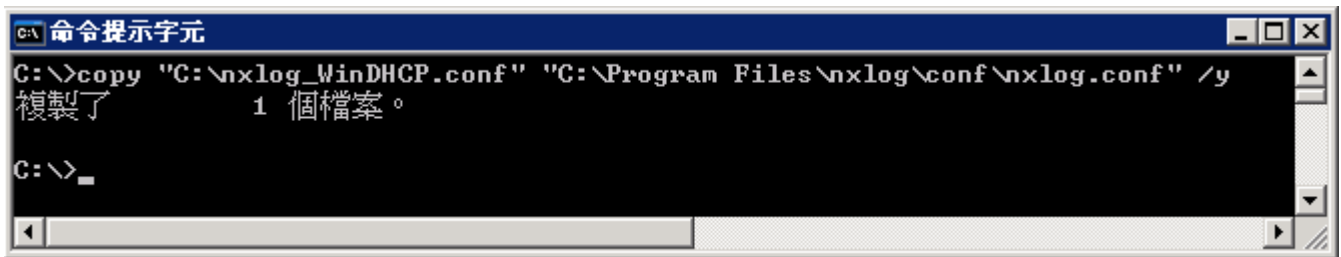
(1) 開啟 [命令提示字元]



(2) 下載 NXLog Windows 2003 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_WinDHCP.conf](http://www.npartnertech.com/download/tech/nxlog_WinDHCP.conf)

```
C:\> copy "C:\nxlog_WinDHCP.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



本文件範例是 32 位元作業系統，若作業系統是 64 位元，紅色文字部位請改以下設定 "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

## 1.2.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



(2) 下載 NXLog DHCP 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_WinDHCP.conf](http://www.npartnertech.com/download/tech/nxlog_WinDHCP.conf)

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_WinDHCP.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```



本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'



## 1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define DhcpPath C:\Windows\System32\LogFiles\DHCP
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid

## Load the modules needed by the outputs
<Extension syslog>
  Module xm_syslog
</Extension>

## For DHCP log file use the following:
<Input in_dhcplog>
  Module im_file
  File '%DhcpPath%\Dhcp*.log'
  SavePos TRUE
  ReadFromLast TRUE
</Input>

<Output out_dhcplog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 20;
  Exec to_syslog_bsd();
</Output>

<Route dhcplog>
  Path in_dhcplog => out_dhcplog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud 192.168.8.4
```

本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

```
define ROOT C:\Program Files (x86)\nxlog
```

若 NXLog 無法讀取 System32 資料夾路徑時，請輸入 Sysnative，Sysnative 是重定向資料夾

```
define ROOT C:\Windows\Sysnative\LogFiles\DHCP
```

藍色文字部位請輸入 DHCP 檔名

```
File '%DhcpPath%\Dhcp*.log'
```

## 1.4 NXLog 啟動服務

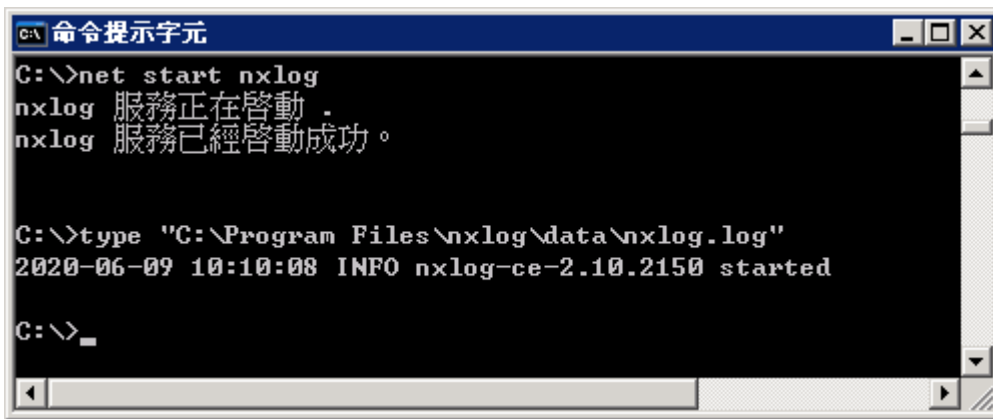
### 1.4.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]



(2) 啟動 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
C:\> net start nxlog  
C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```



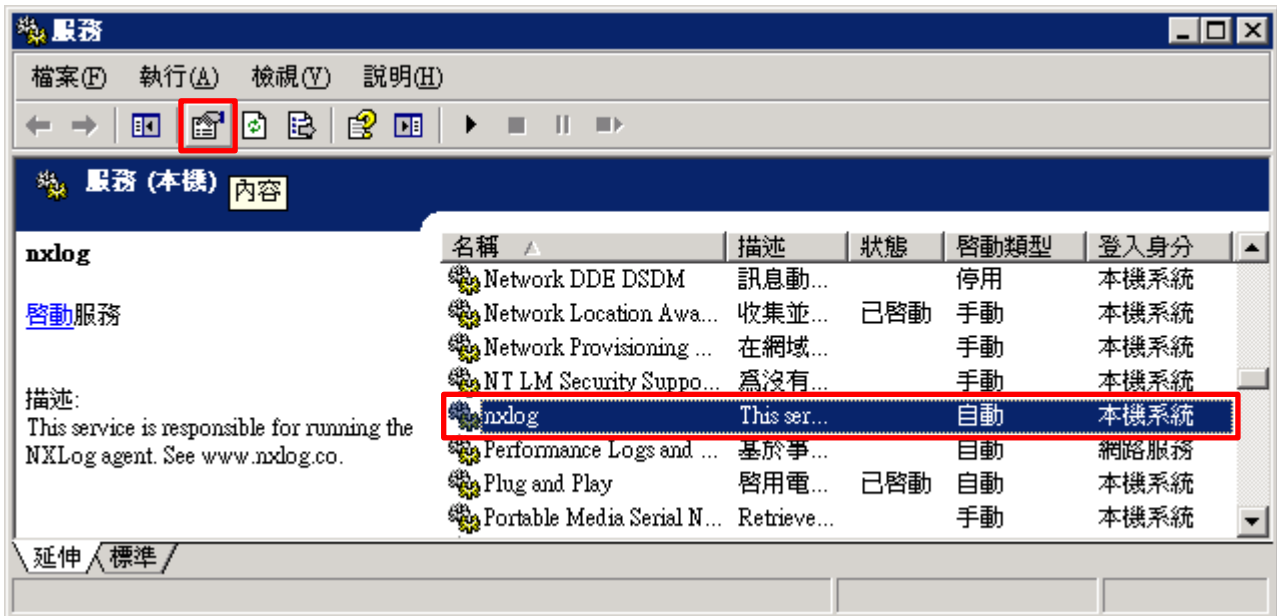
(3) 開啟 [服務] 功能

```
C:\> Services.msc
```

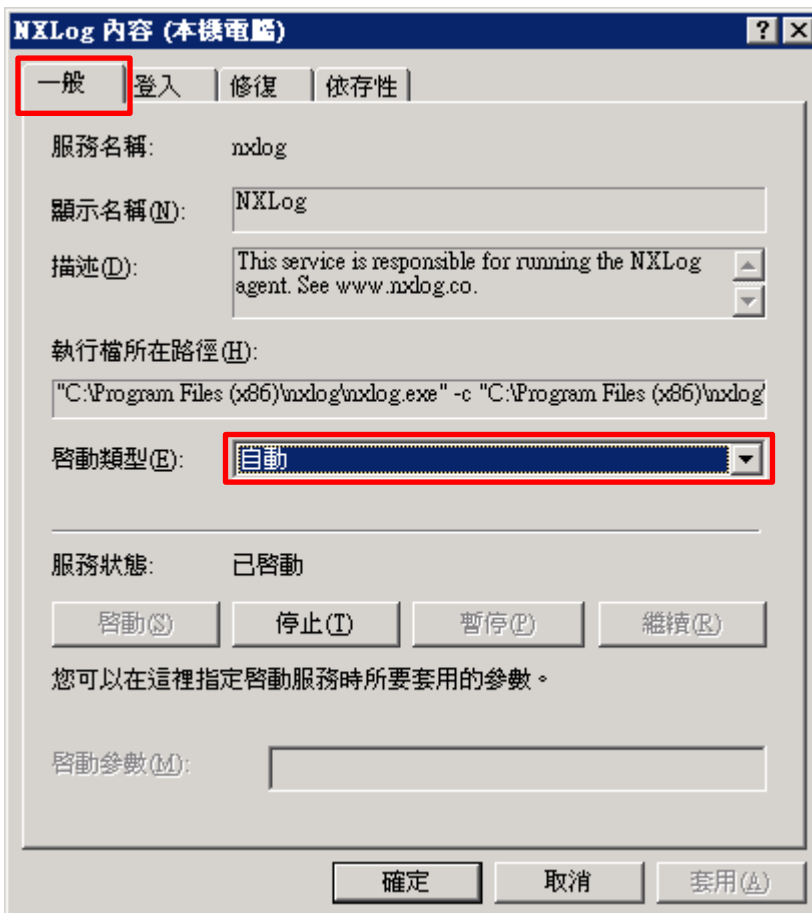


(4) 開啟 NXLog 服務內容

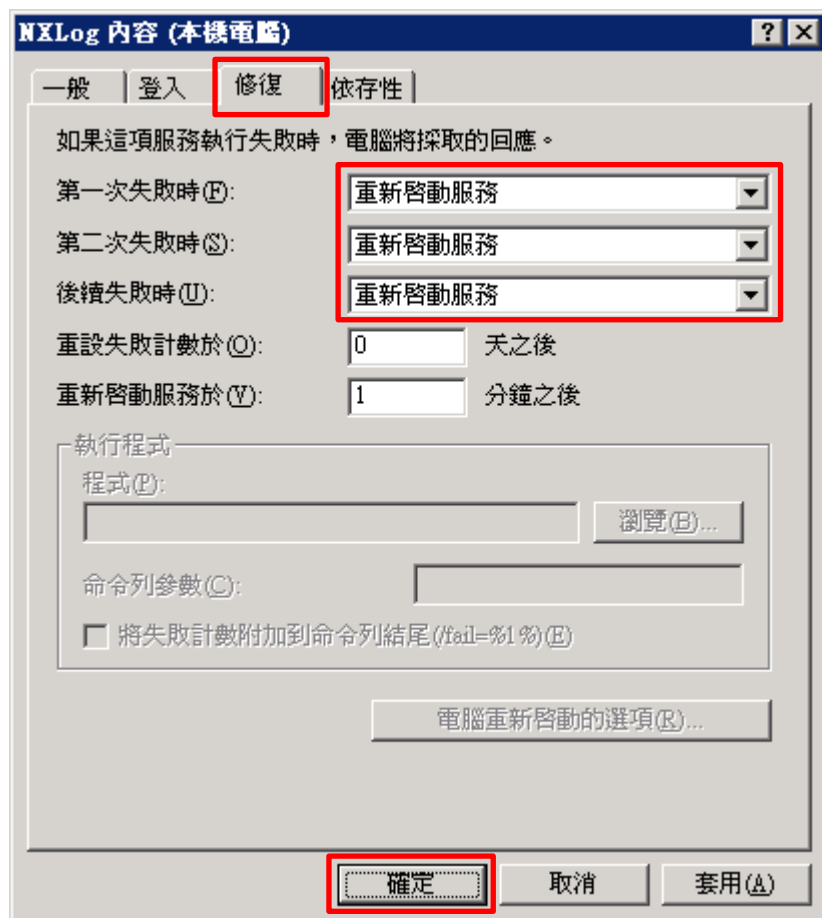
選擇 [nxlog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認 ; 啟動類型: [自動]



(6) [修復] 頁面 -> 確認 ; 第一次失敗時: 和 第二次失敗時: 和 後續失敗時: [重新啟動服務] -> 按 [確定]



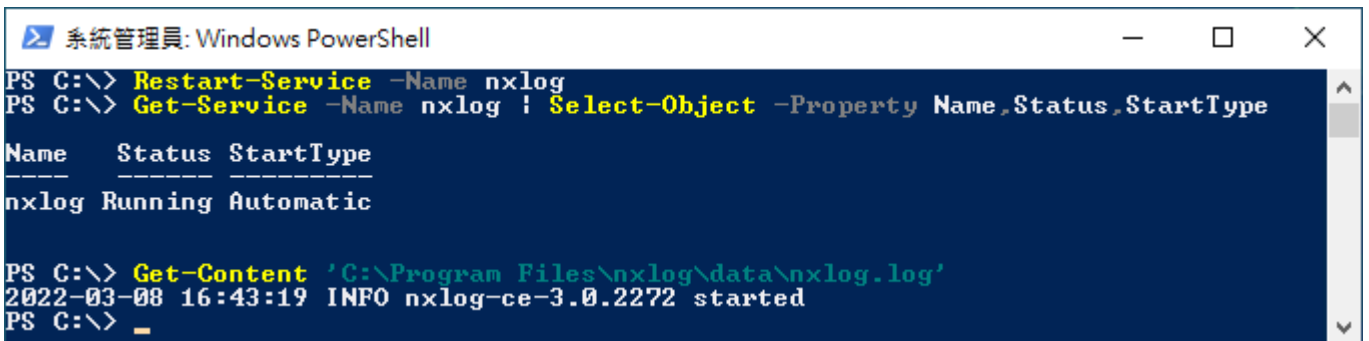
## 1.4.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```

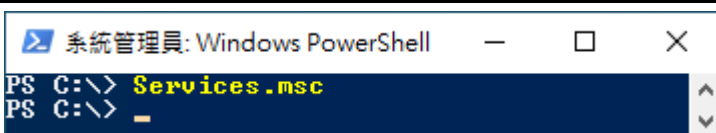
A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The console shows the following commands and output:

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
Name      Status StartType
-----
nxlog     Running Automatic

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2022-03-08 16:43:19 INFO nxlog-ce-3.0.2272 started
PS C:\> _
```


(3) 開啟 [服務] 功能

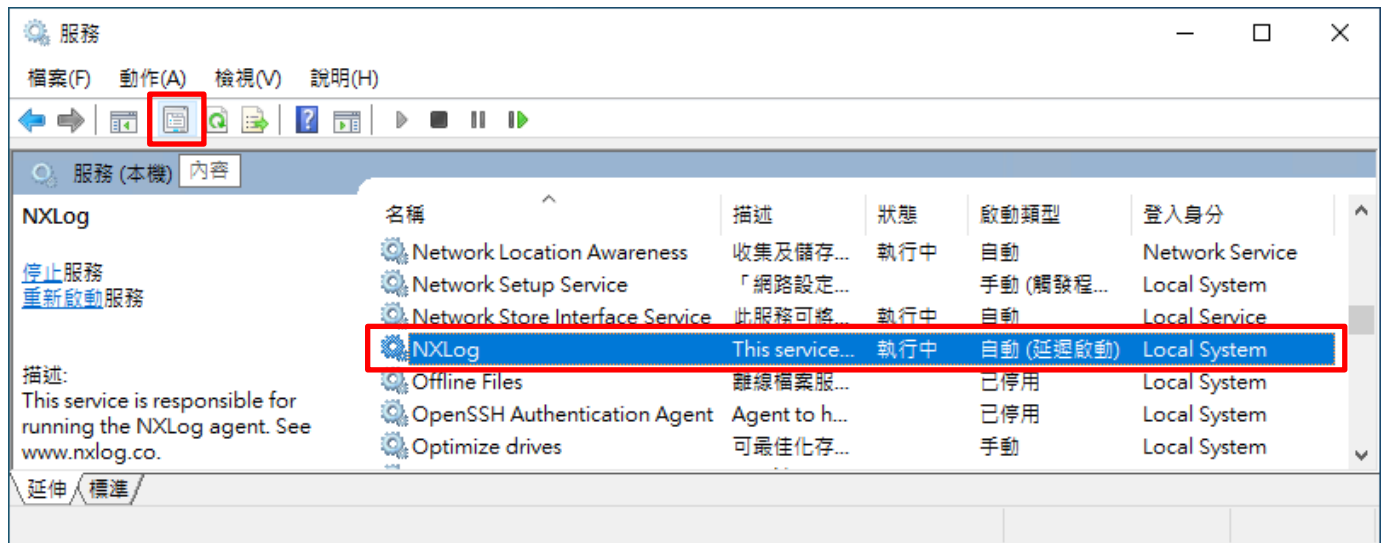
```
PS C:\> Services.msc
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The console shows the following commands and output:

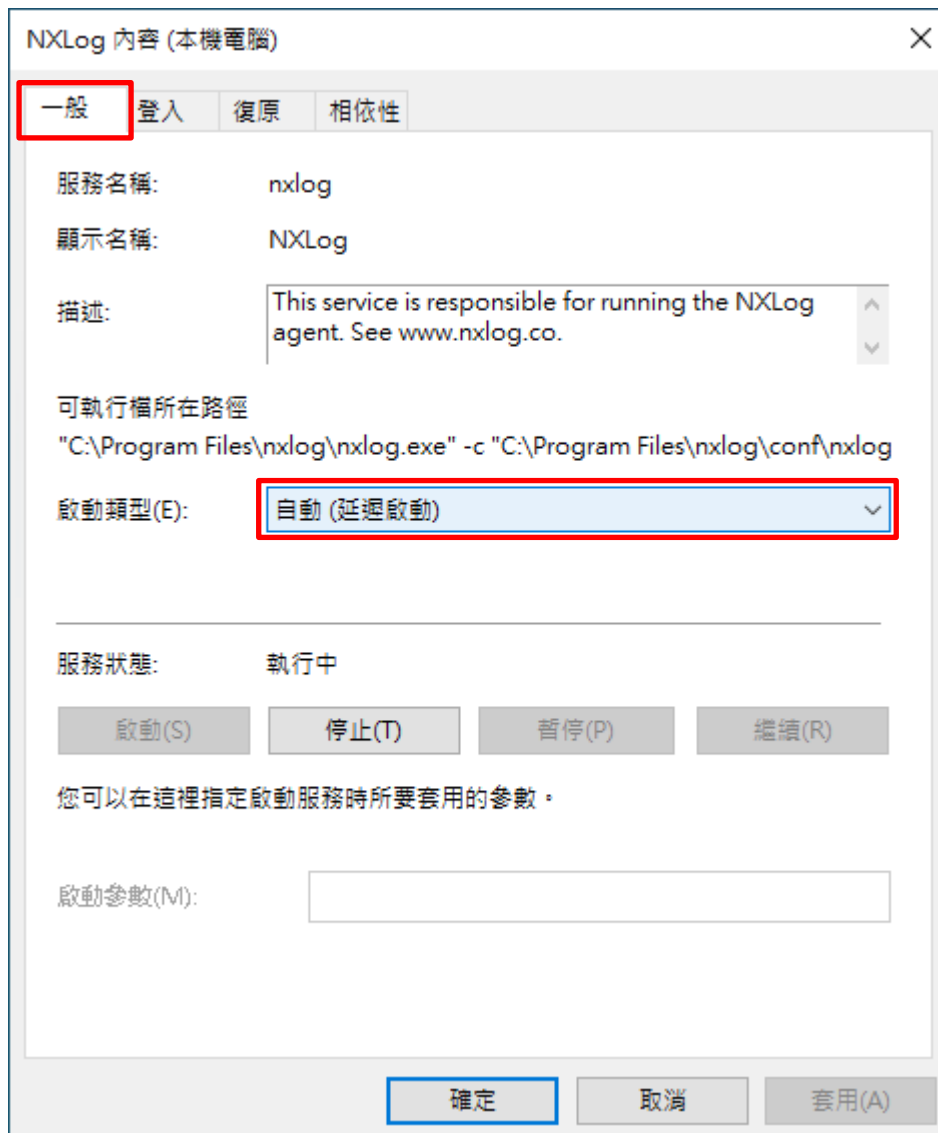
```
PS C:\> Services.msc
PS C:\> _
```

(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (延遲啟動)]



(6) [復原] 頁面 -> 確認；第一次失敗時: 和 第二次失敗時: 和 後續失敗時: [重新啟動服務] -> 按 [確定]

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P):  瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%)(E)

確定 取消 套用(A)

## 2. Windows 2003

(1) 開啟 [命令提示字元]



(2) 新增 DHCP log 資料夾

```
PS C:\> mkdir C:\Windows\System32\LogFiles\DHCP
```

```
PS C:\> dir C:\Windows\System32\LogFiles
```

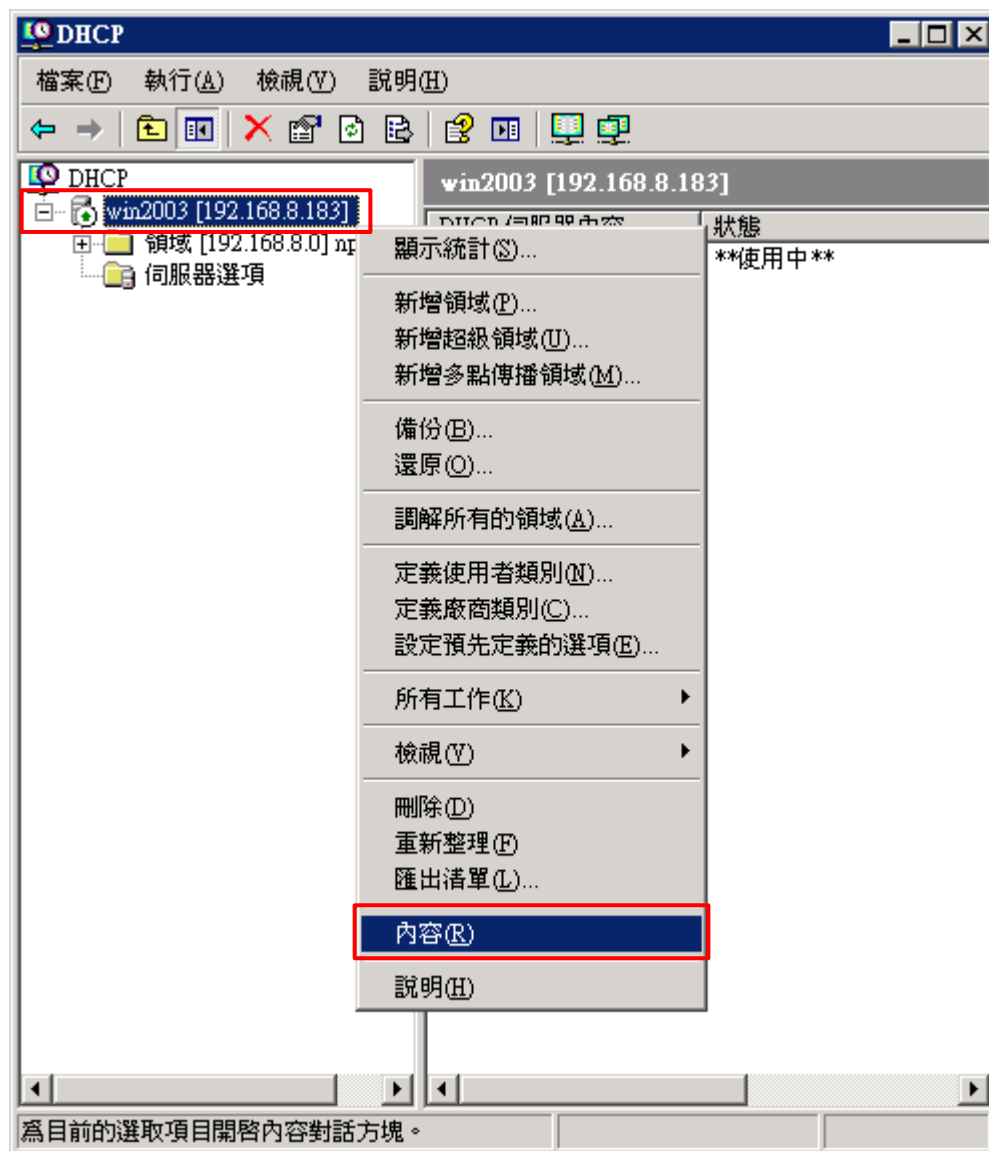


(3) 開啟 [DHCP]

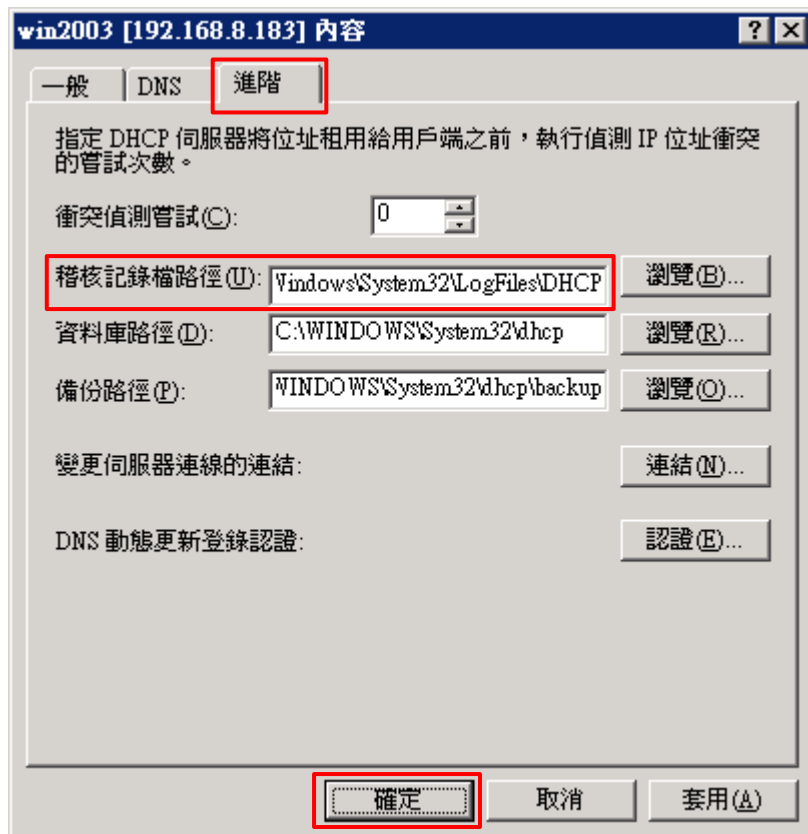




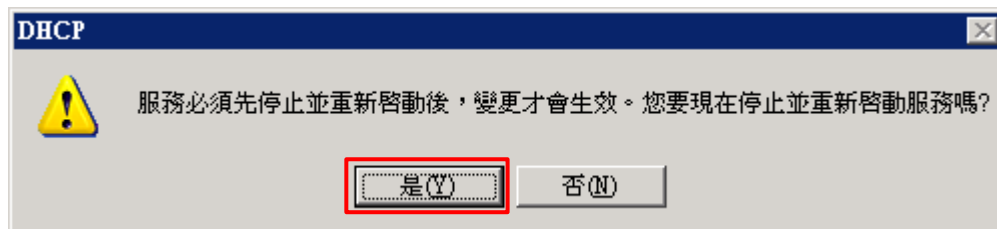
(4) 在 [DHCP 伺服器] 上按滑鼠右鍵 -> 選擇 [內容]



(5) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]



(6) 按 [是] (重啟 DHCP server 服務)



(7) 確認有產生 DHCP.log 檔案



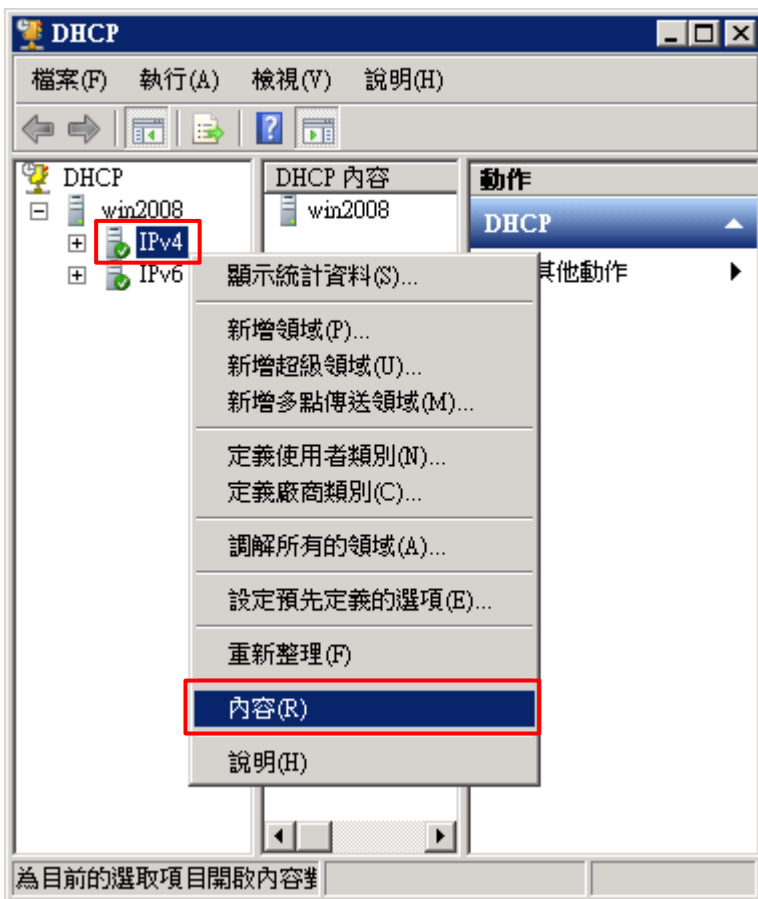
## 3. Windows 2008

### 3.1 DHCP IPv4

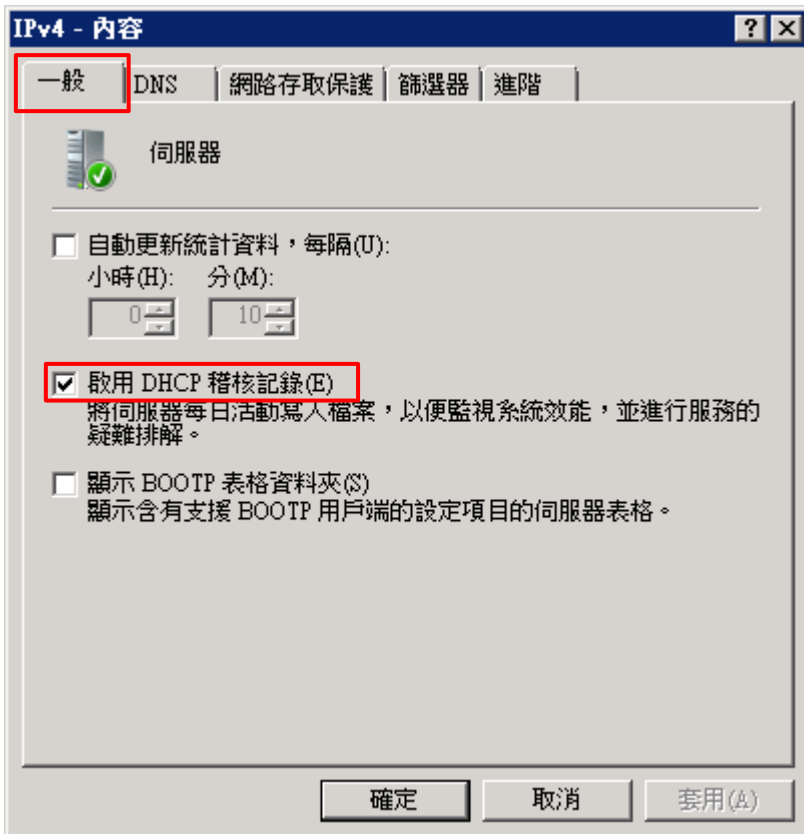
(1) 開啟 [DHCP]



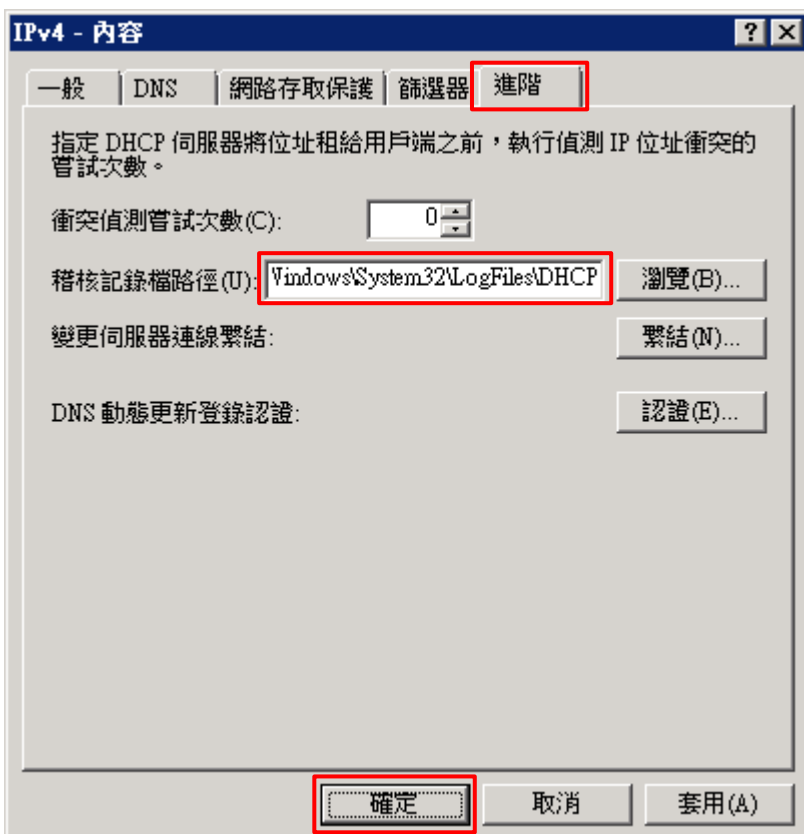
(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



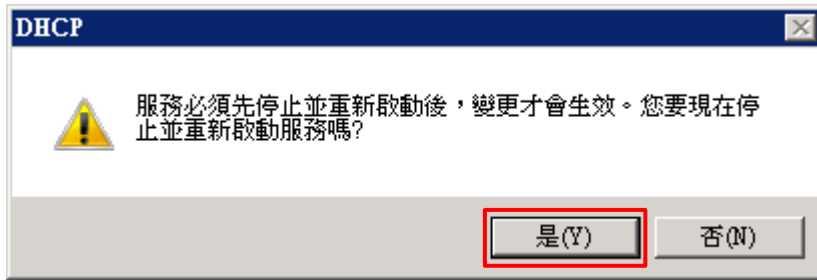
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



(4) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]

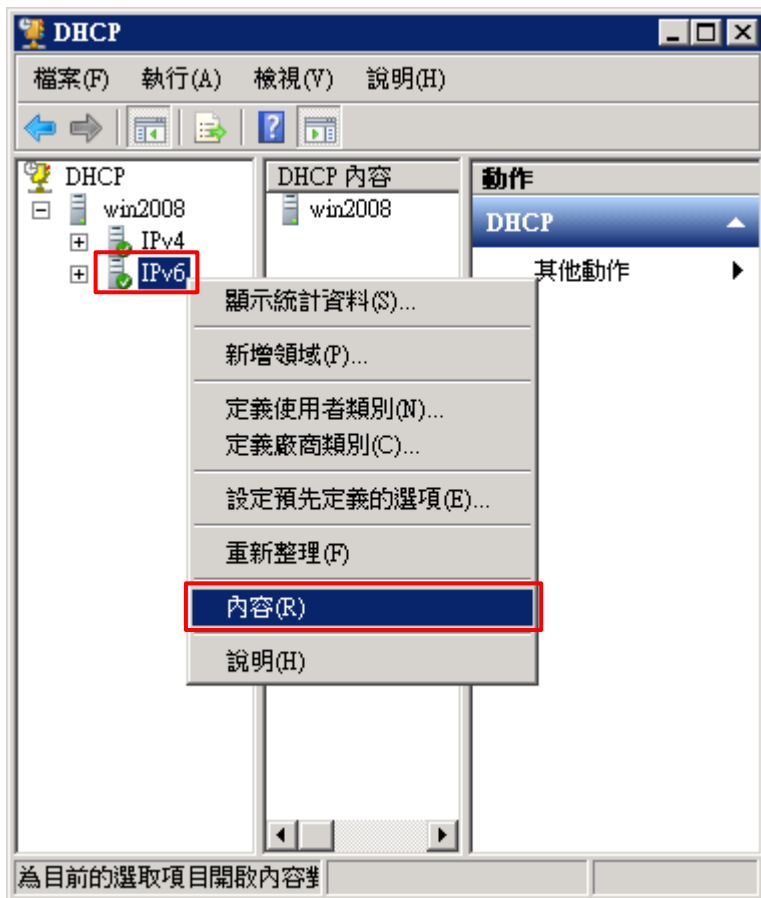


(5) 按 [是] (重啟 DHCP server 服務)

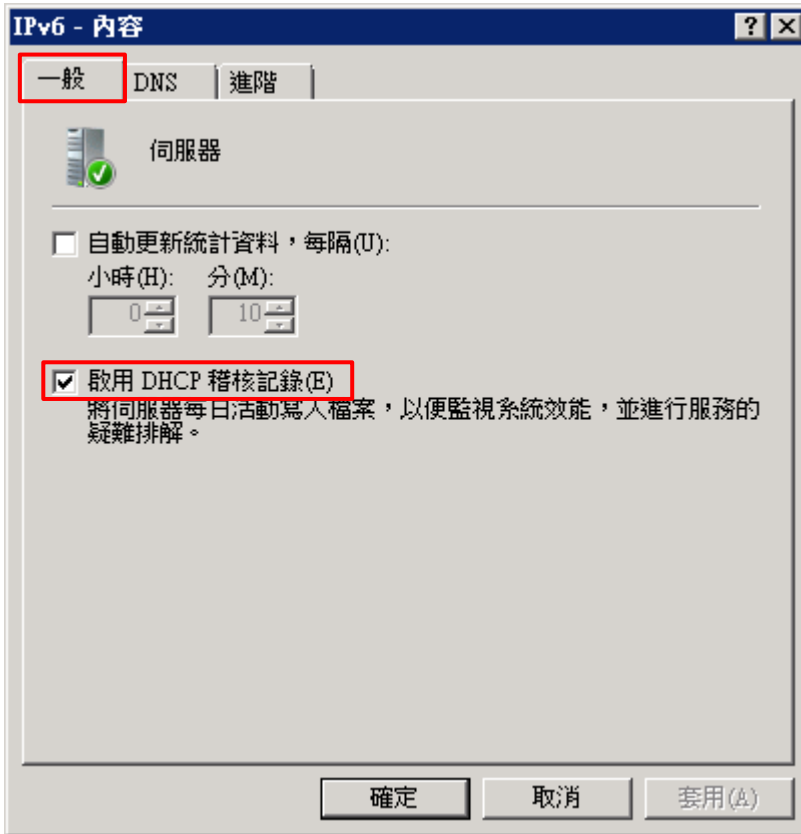


## 3.2 DHCP IPv6

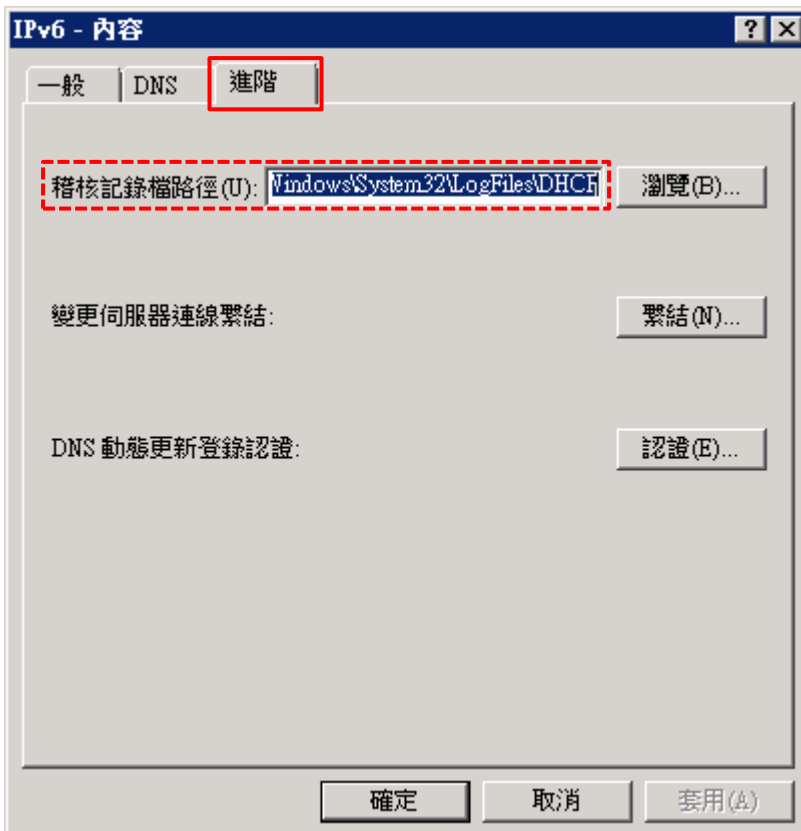
(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



(3) [進階] 頁面 -> 確認稽核記錄檔路徑: [C:\Windows\System32\LogFiles\DHCP]



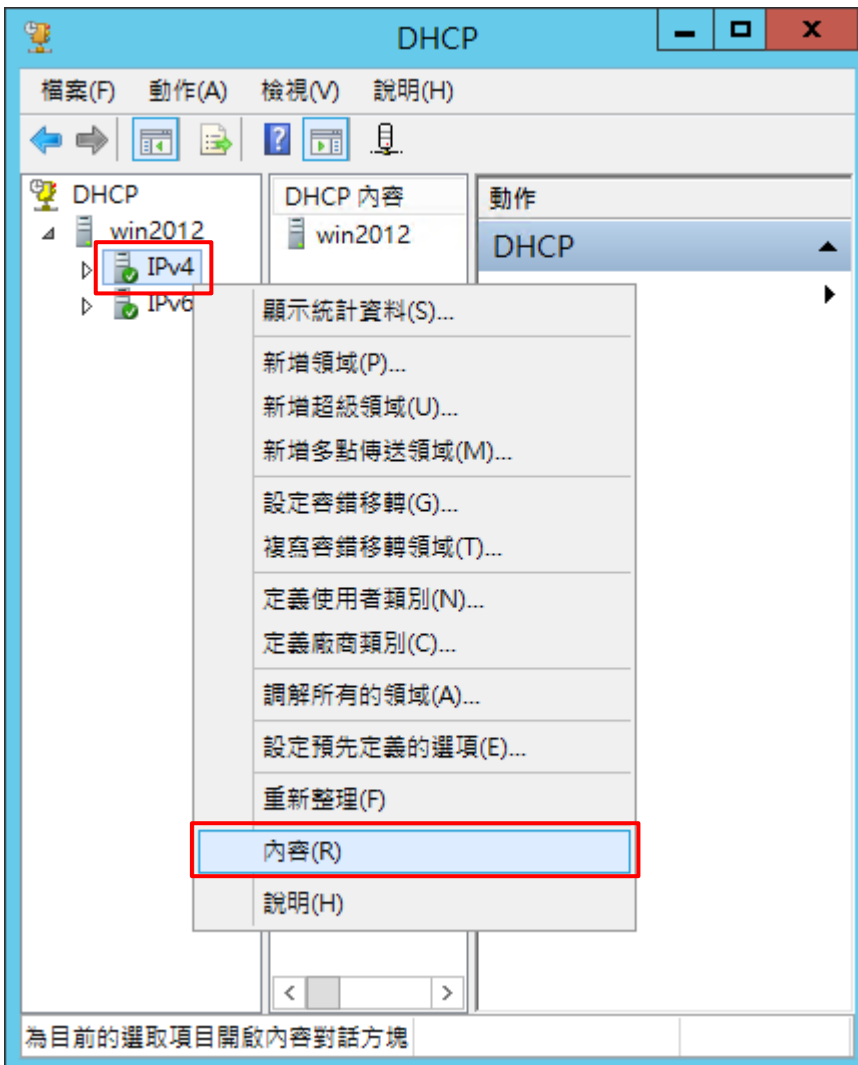
## 4 Windows 2012

### 4.1 DHCP IPv4

(1) 開啟 [DHCP]

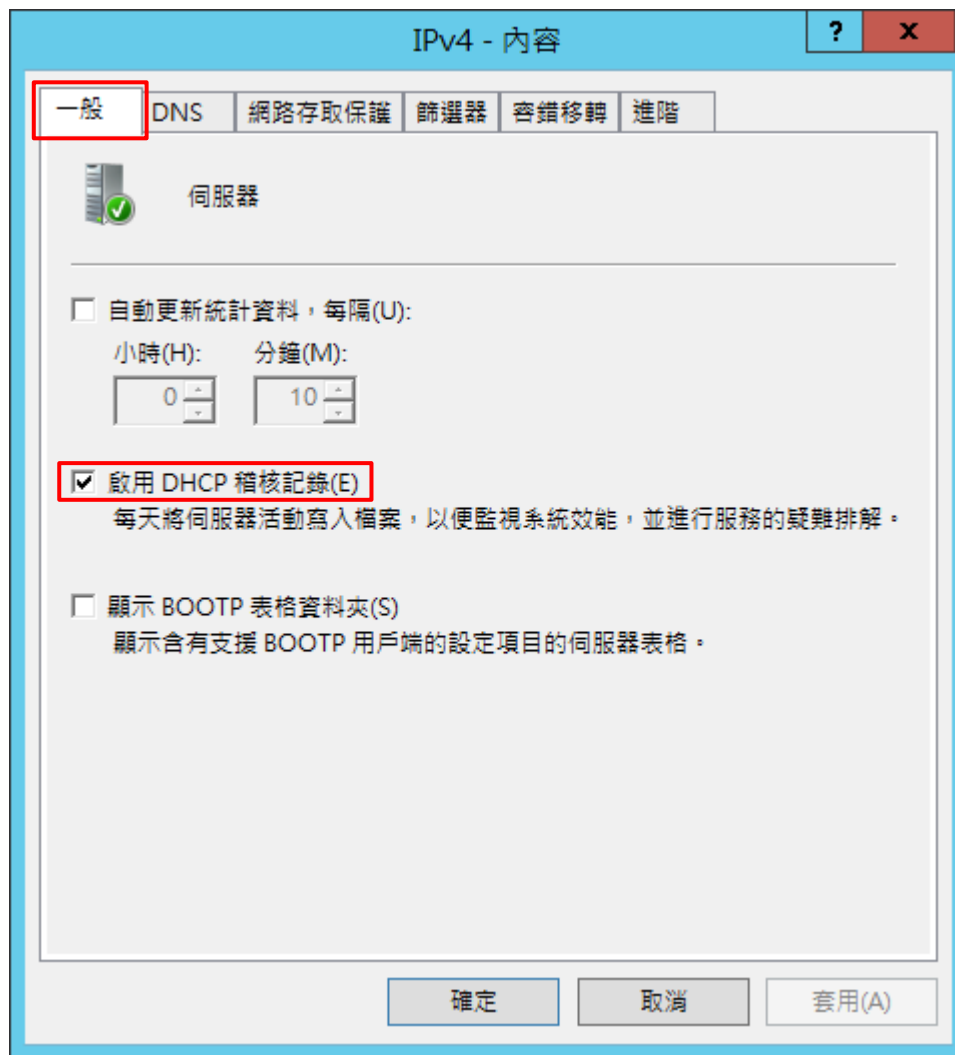


(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]

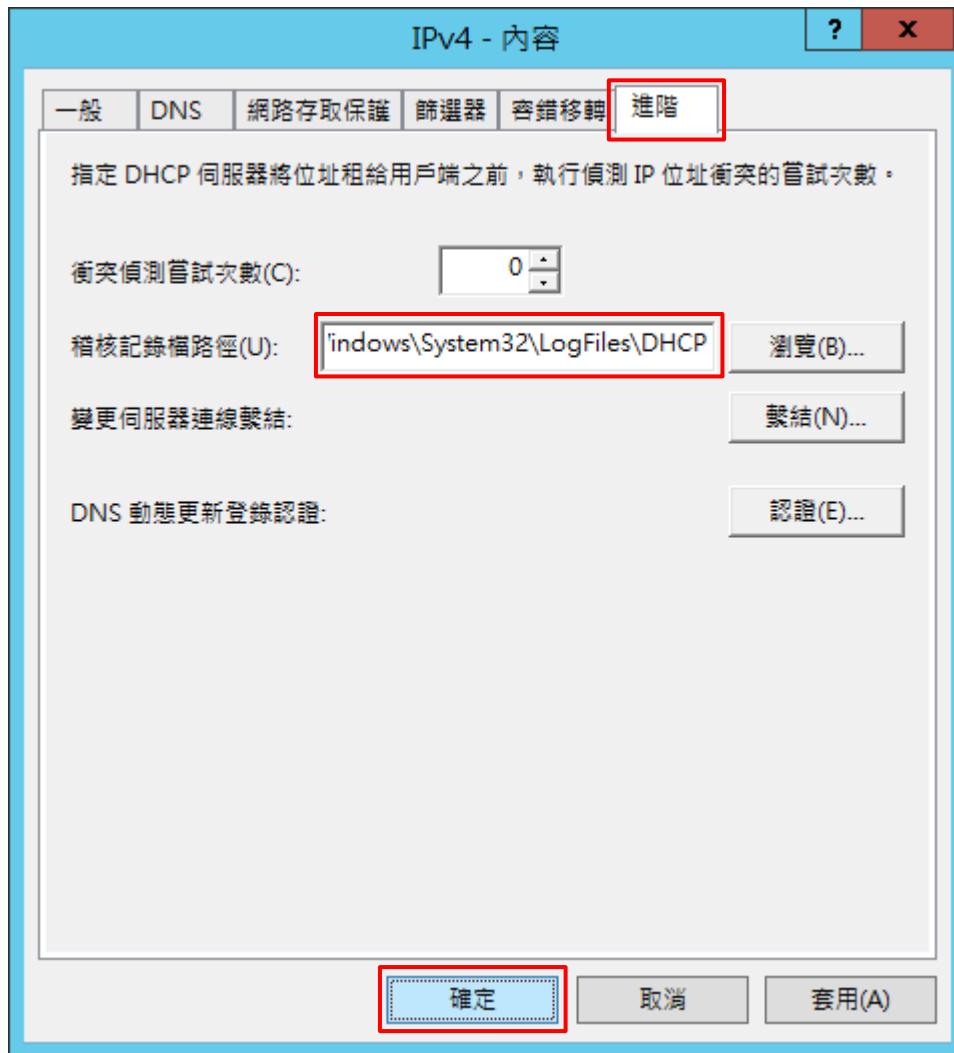




(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



(4) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]

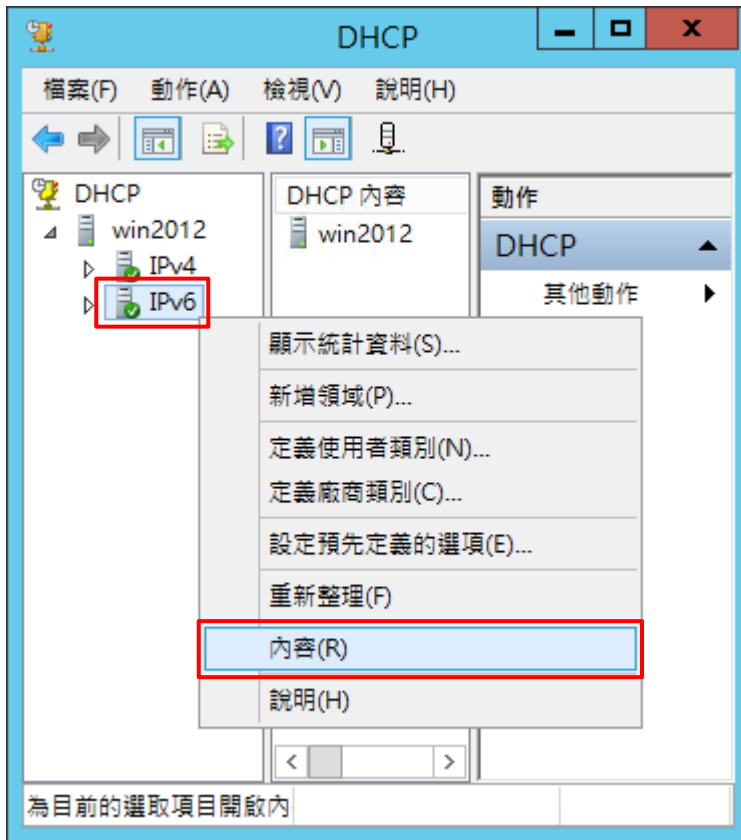


(5) 按 [是] (重啟 DHCP server 服務)

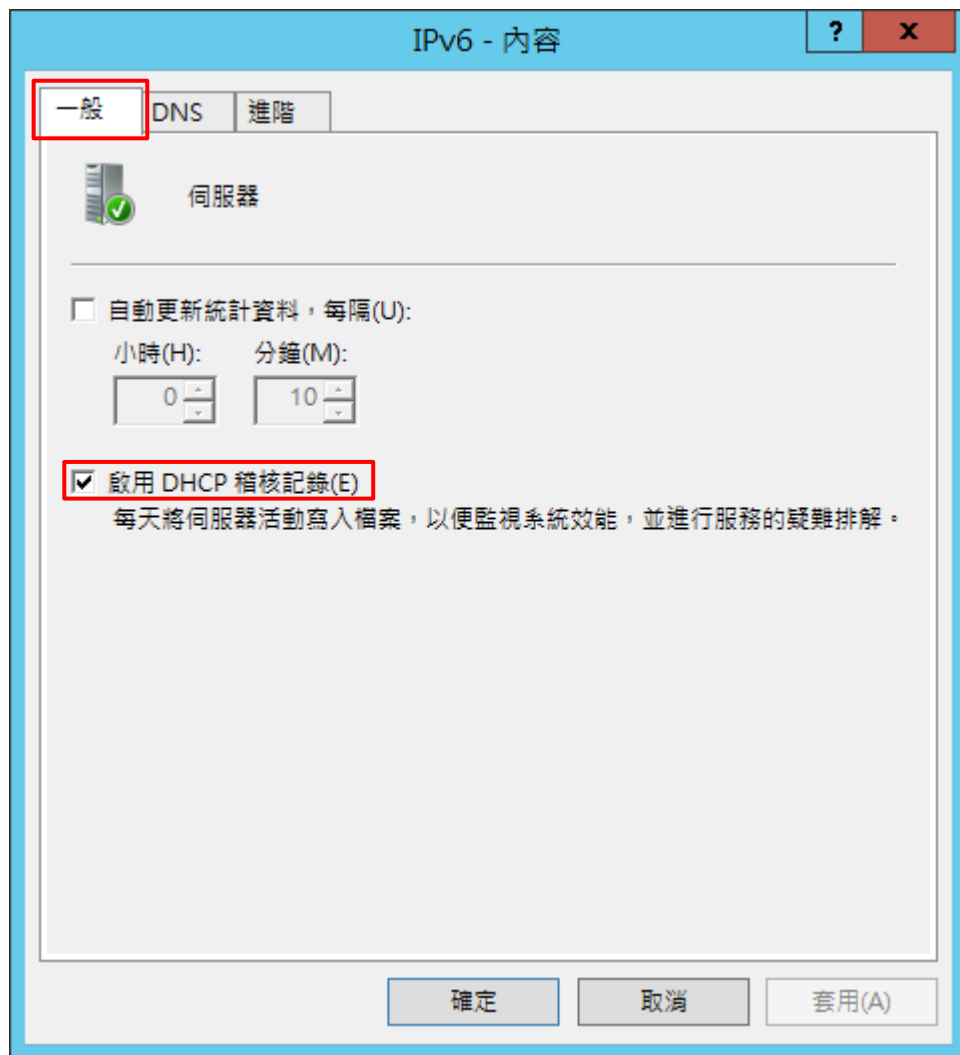


## 4.2 DHCP IPv6

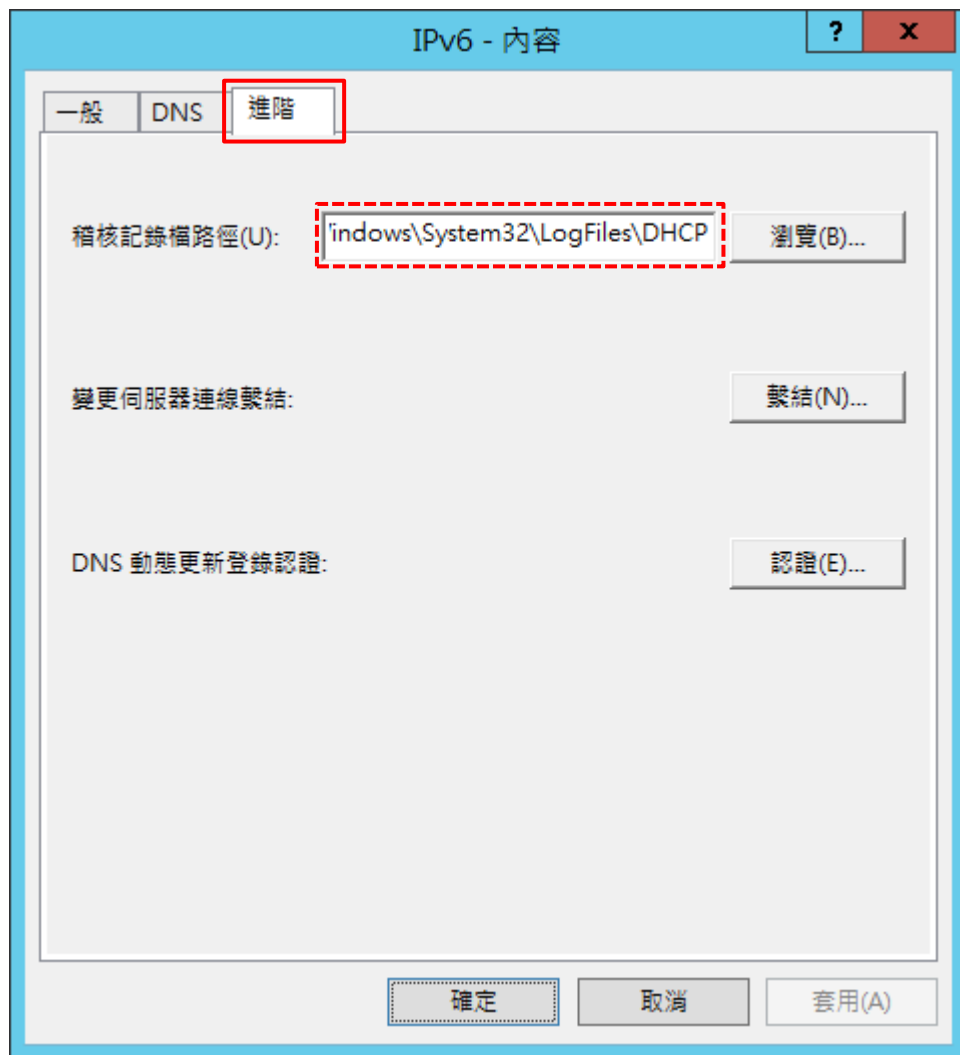
(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



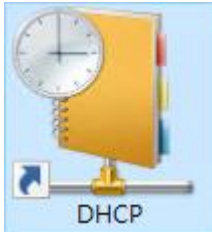
(3) [進階] 頁面 -> 確認稽核記錄檔路徑: [C:\Windows\System32\LogFiles\DHCP]



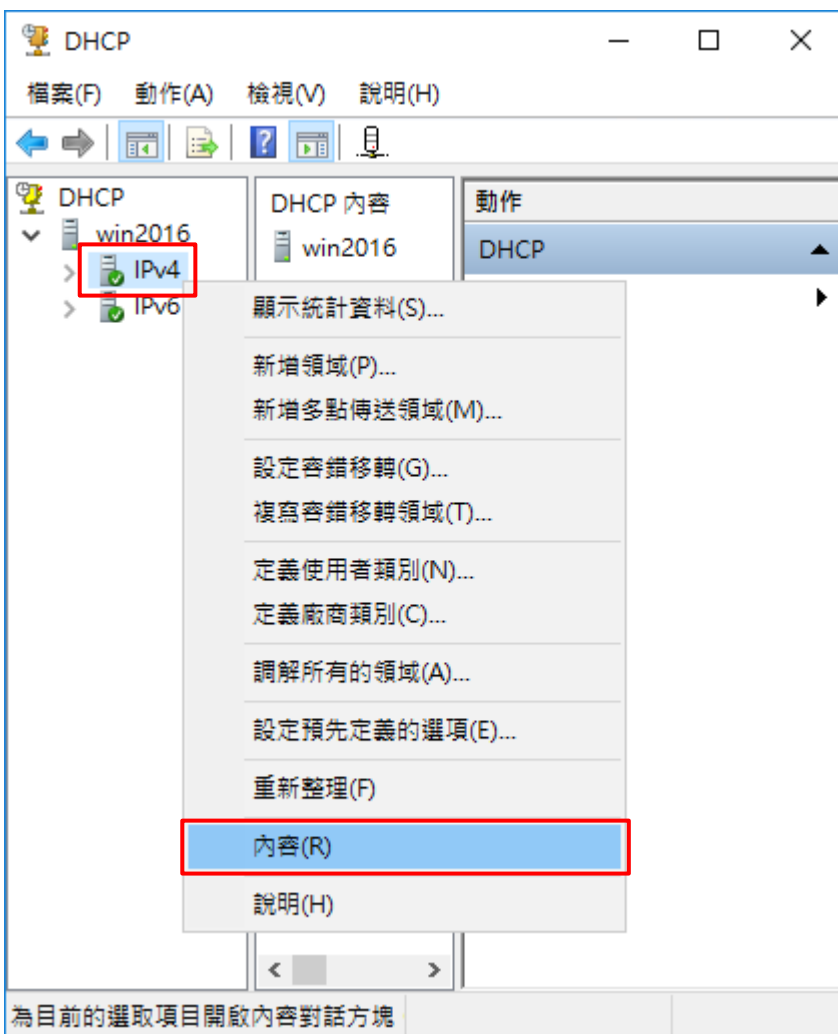
## 5. Windows 2016

### 5.1 DHCP IPv4

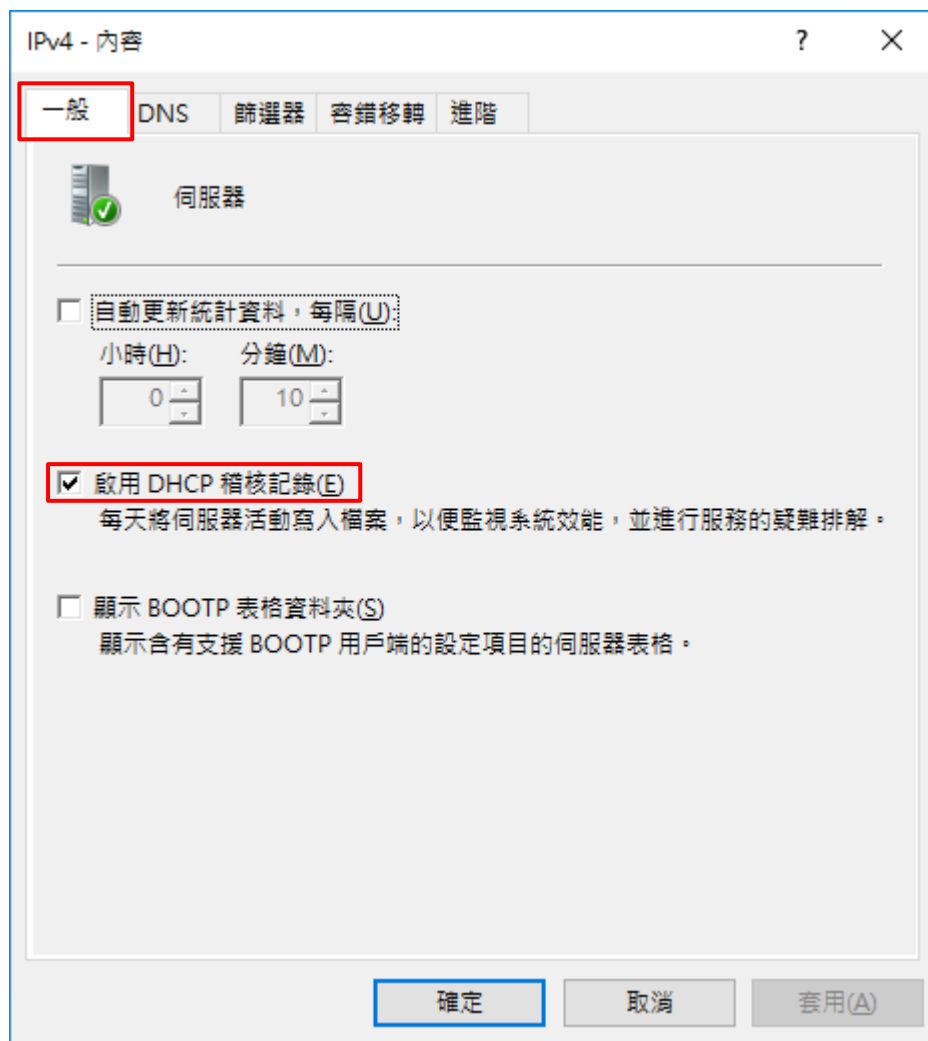
(1) 開啟 [DHCP]



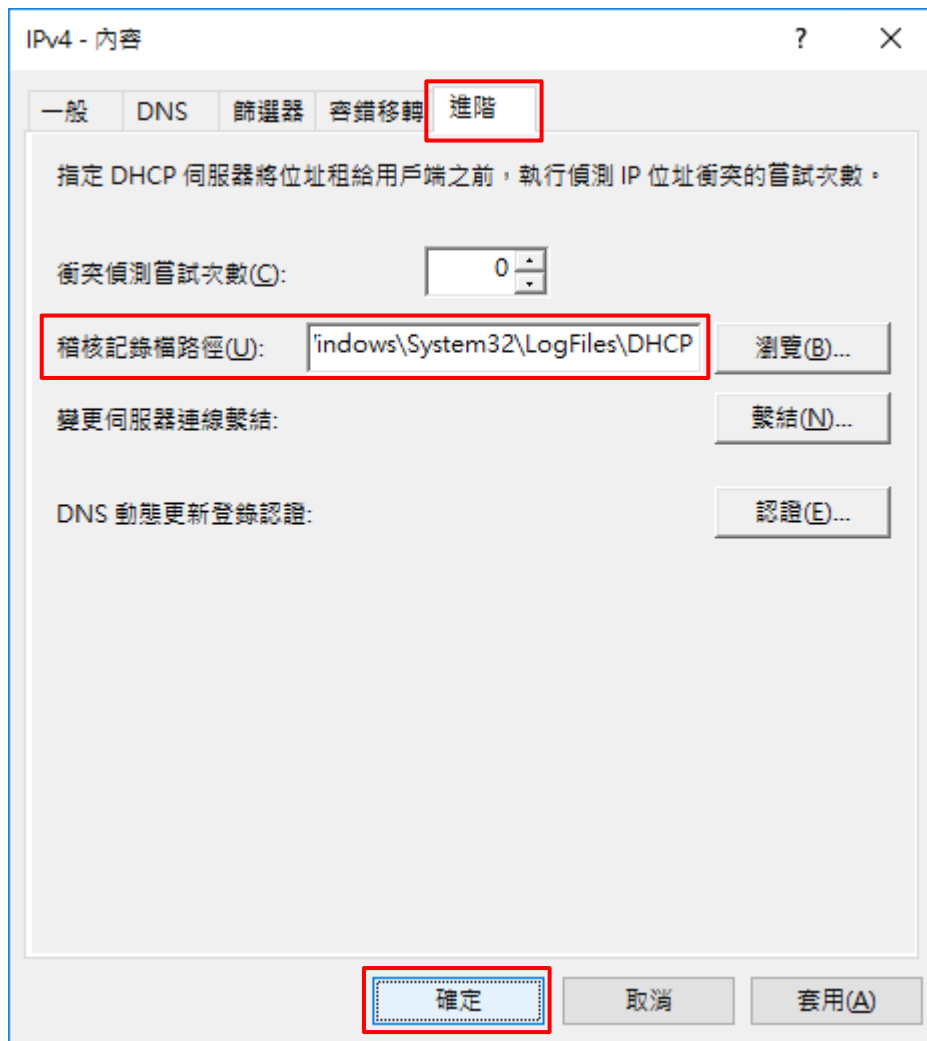
(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



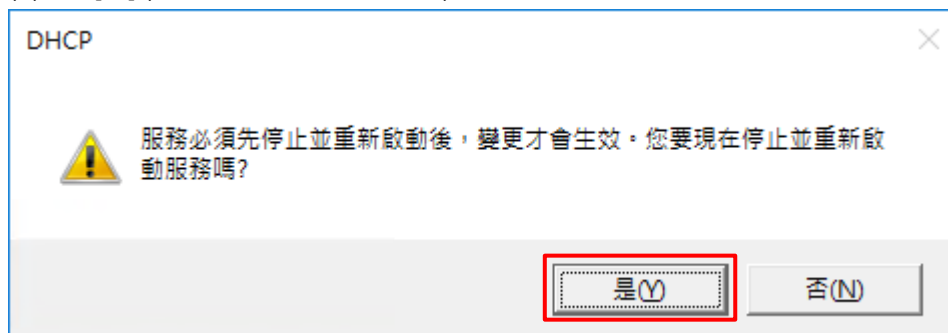
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



(4) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]



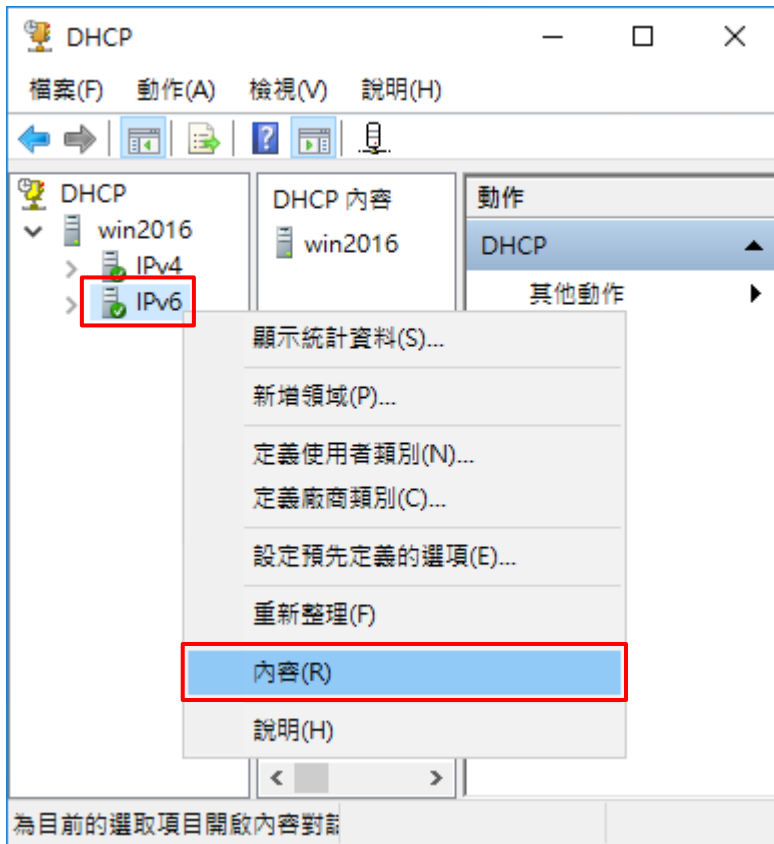
(5) 按 [是] (重啟 DHCP server 服務)



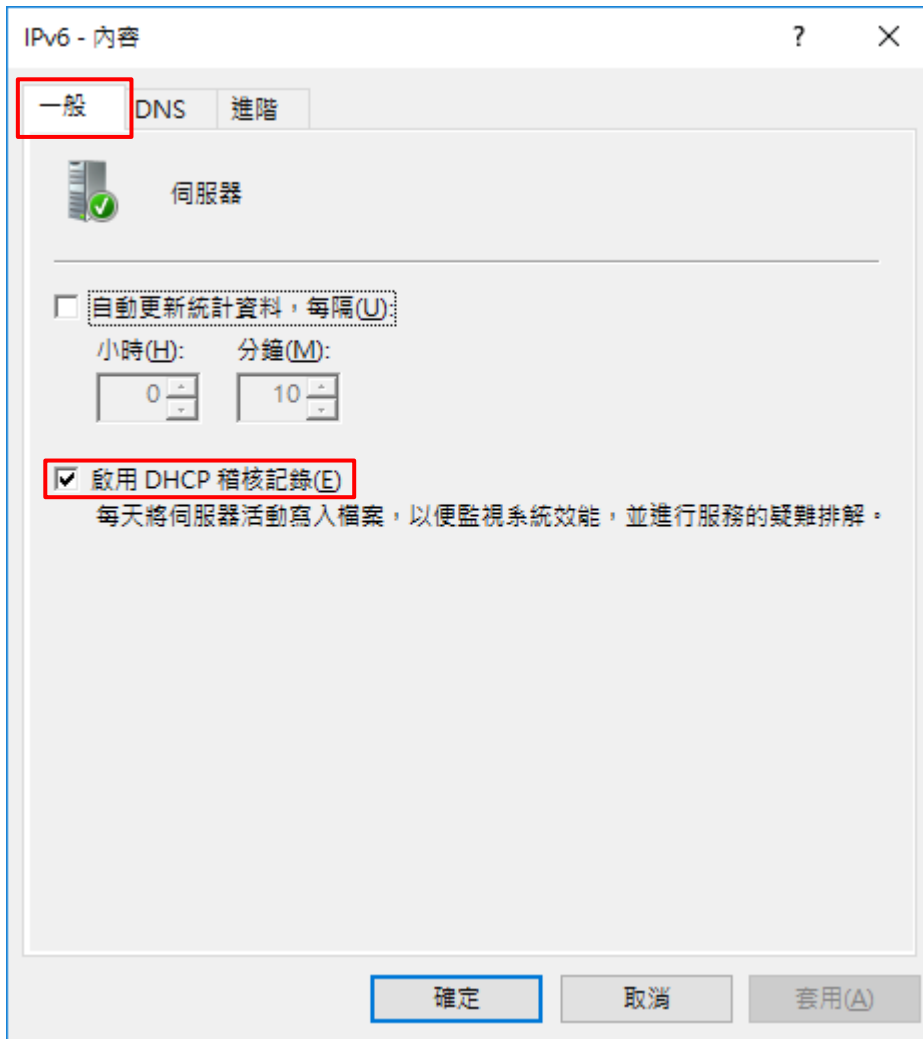


## 5.2 DHCP IPv6

(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



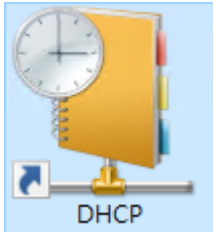
(3) [進階] 頁面 -> 確認稽核記錄檔路徑: [C:\Windows\System32\LogFiles\DHCP]



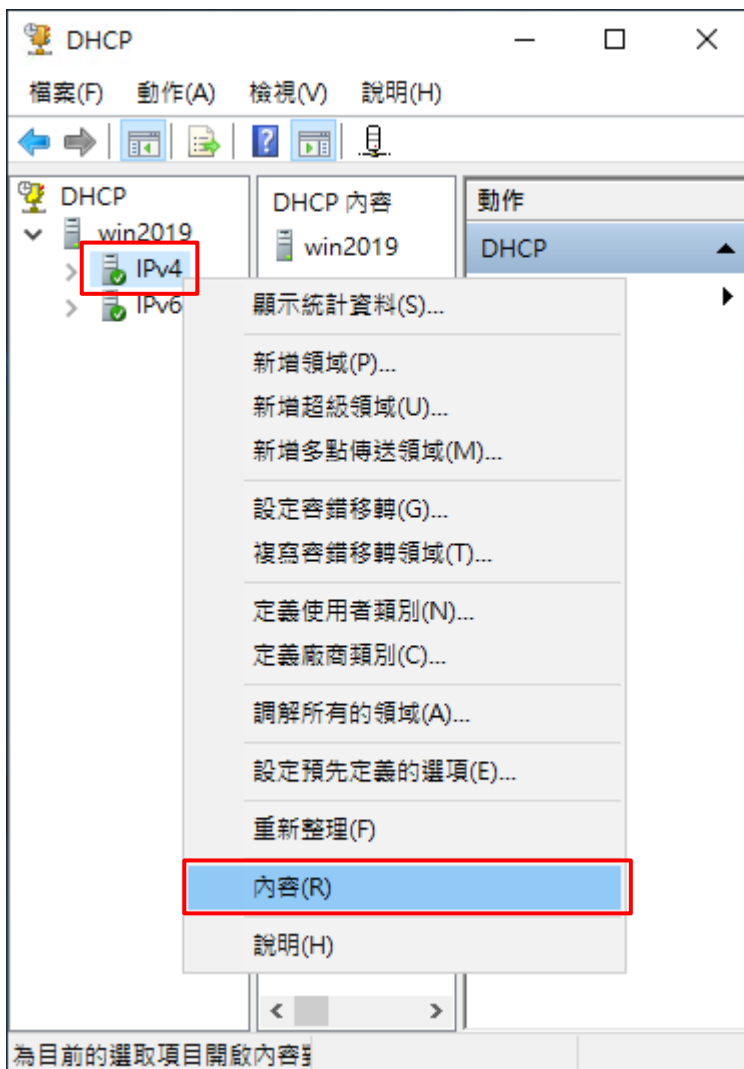
## 6. Windows 2019

### 6.1 DHCP IPv4

(1) 開啟 [DHCP]



(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



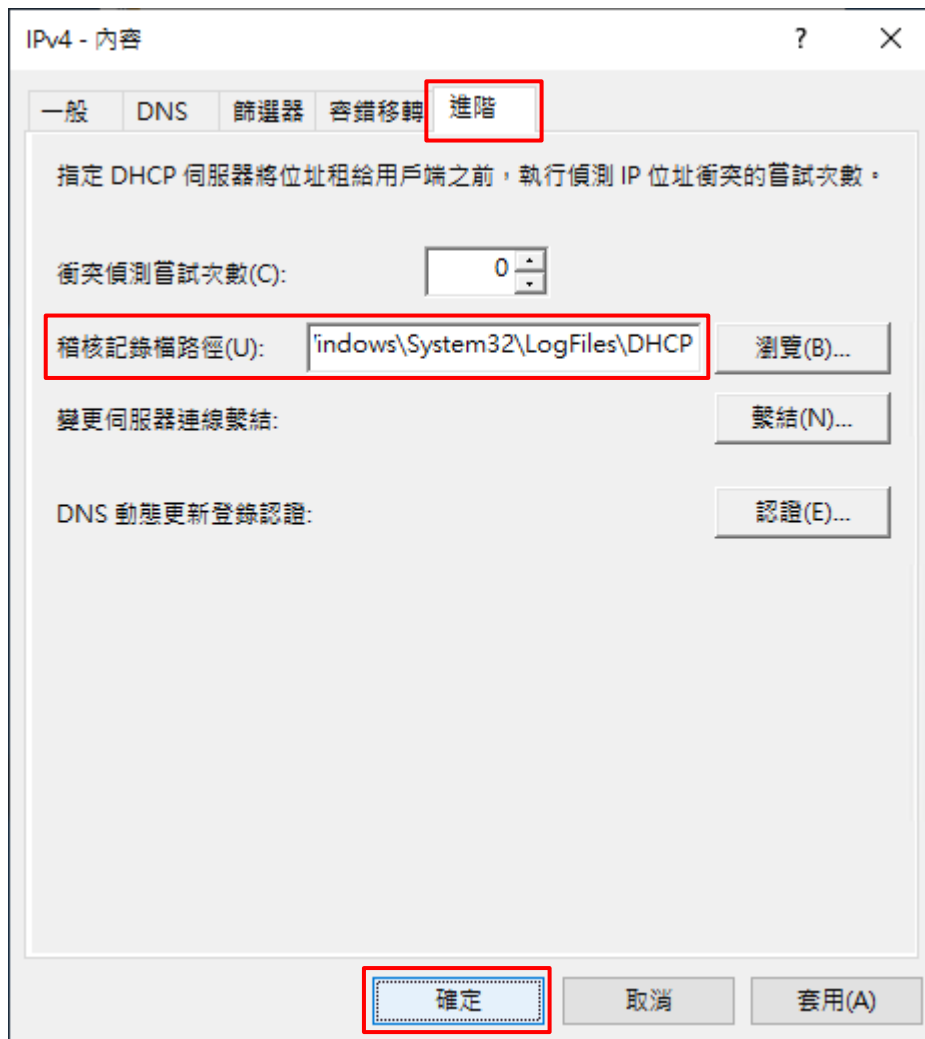
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]

The image shows a screenshot of the 'IPv4 - 內容' (IPv4 - Content) configuration window. The '一般' (General) tab is selected and highlighted with a red box. The window title bar includes a question mark and a close button. Below the tabs, there is a '伺服器' (Server) icon with a green checkmark. The main content area contains three options:

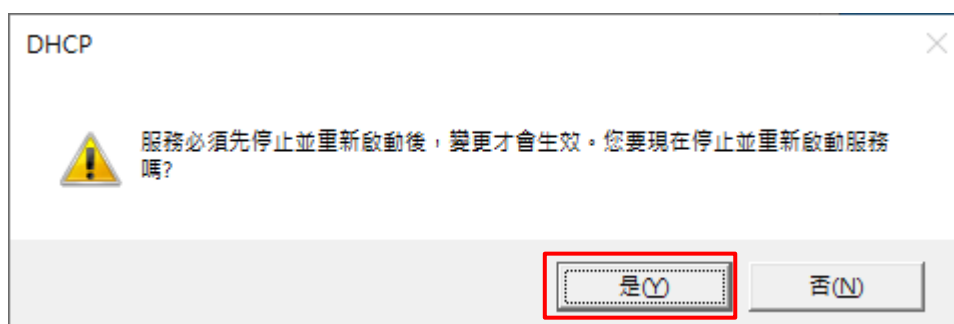
- 自動更新統計資料，每隔(U):  
小時(H): 分鐘(M):  
0 10
- 啟用 DHCP 稽核記錄(E)  
每天將伺服器活動寫入檔案，以便監視系統效能，並進行服務的疑難排解。
- 顯示 BOOTP 表格資料夾(S)  
顯示含有支援 BOOTP 用戶端的設定項目的伺服器表格。

At the bottom of the window, there are three buttons: '確定' (OK), '取消' (Cancel), and '套用(A)' (Apply).

(4) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]

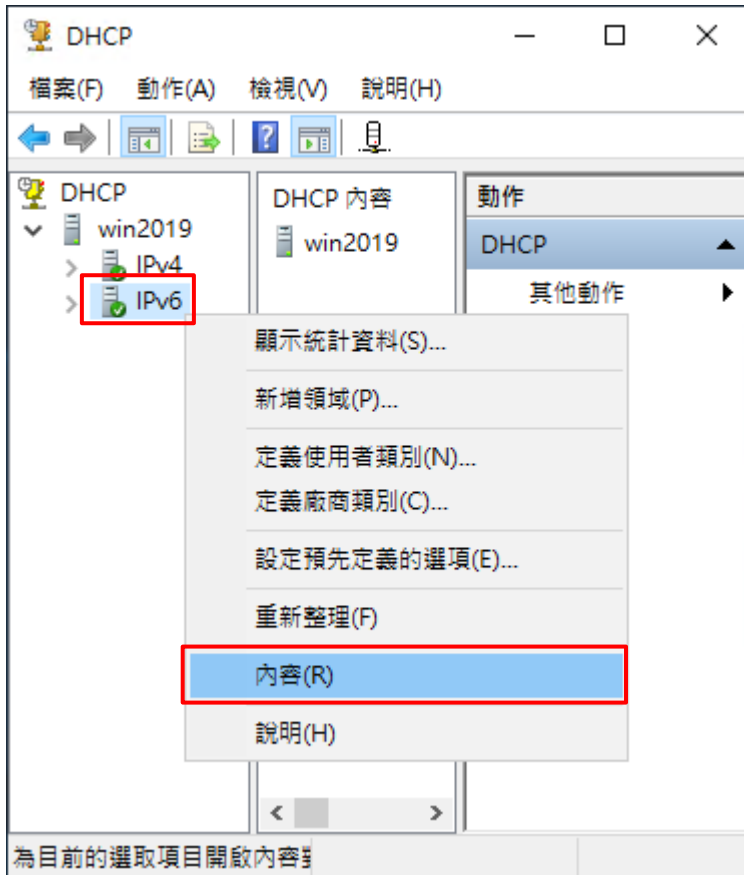


(5) 按 [是] (重啟 DHCP server 服務)



## 6.2 DHCP IPv6

(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]

The screenshot shows a window titled "IPv6 - 內容" with three tabs: "一般" (General), "DNS", and "進階" (Advanced). The "一般" tab is selected and highlighted with a red box. Below the tabs is a server icon with a green checkmark and the label "伺服器".

There are two main options in the "一般" tab:

- 自動更新統計資料，每隔(U):  
小時(H): 分鐘(M):  
0 10
- 啟用 DHCP 稽核記錄(E)  
每天將伺服器活動寫入檔案，以便監視系統效能，並進行服務的疑難排解。

At the bottom of the window are three buttons: "確定" (OK), "取消" (Cancel), and "套用(A)" (Apply).



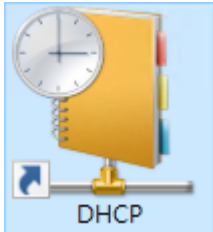
(3) [進階] 頁面 -> 確認稽核記錄檔路徑: [C:\Windows\System32\LogFiles\DHCP]



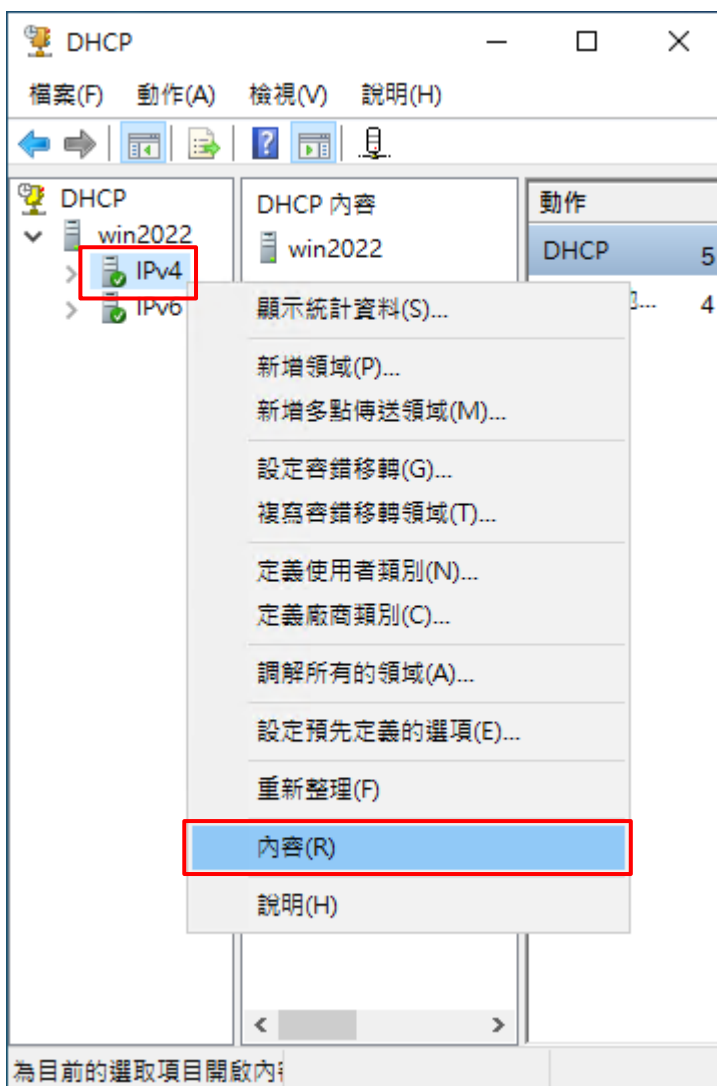
## 7. Windows 2022

### 7.1 DHCP IPv4

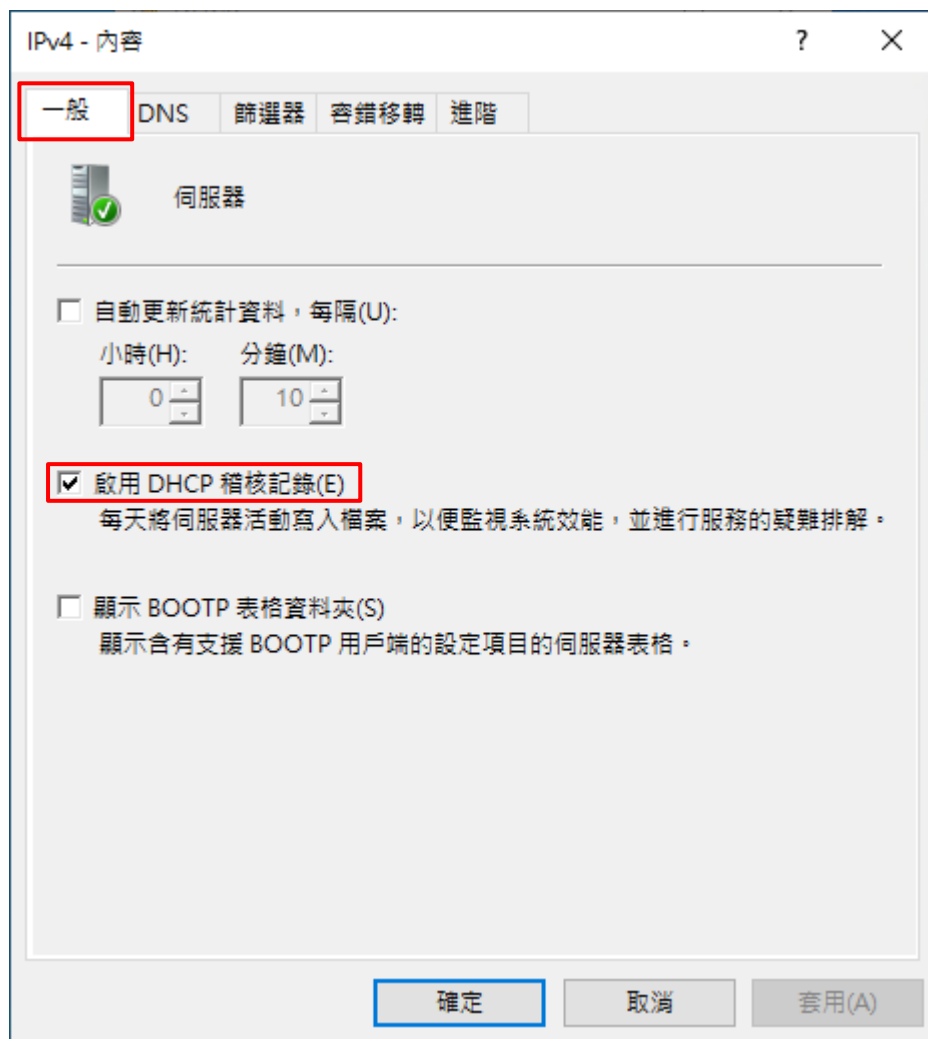
(1) 開啟 [DHCP]



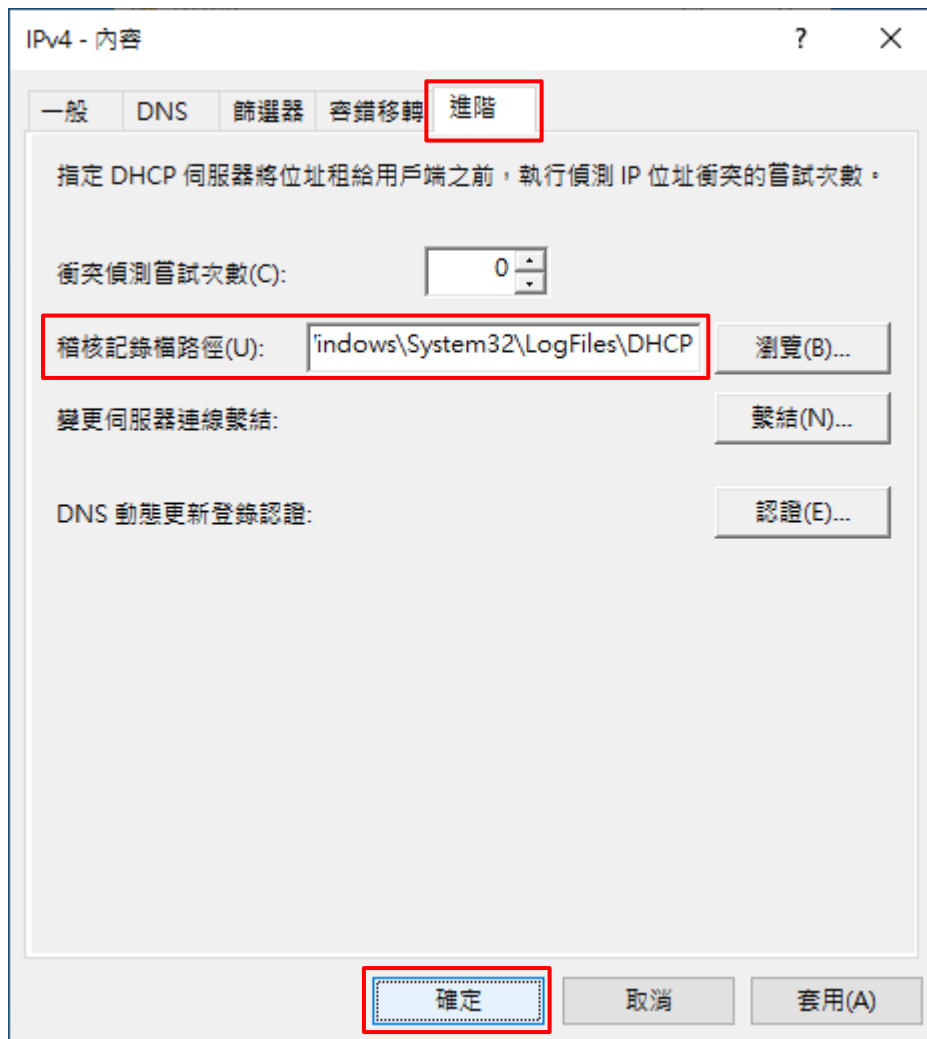
(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



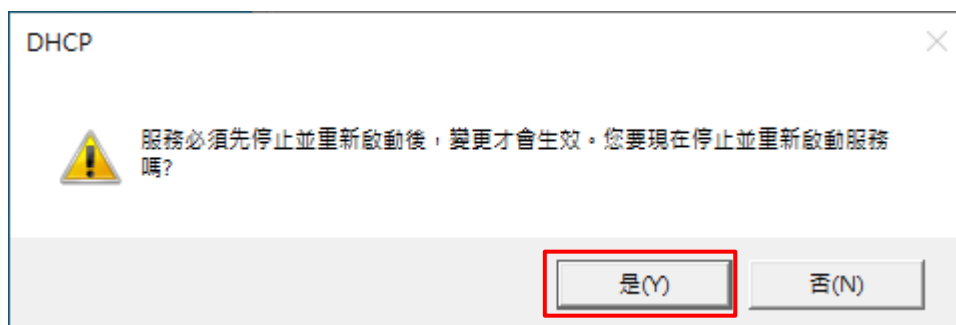
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



(4) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]

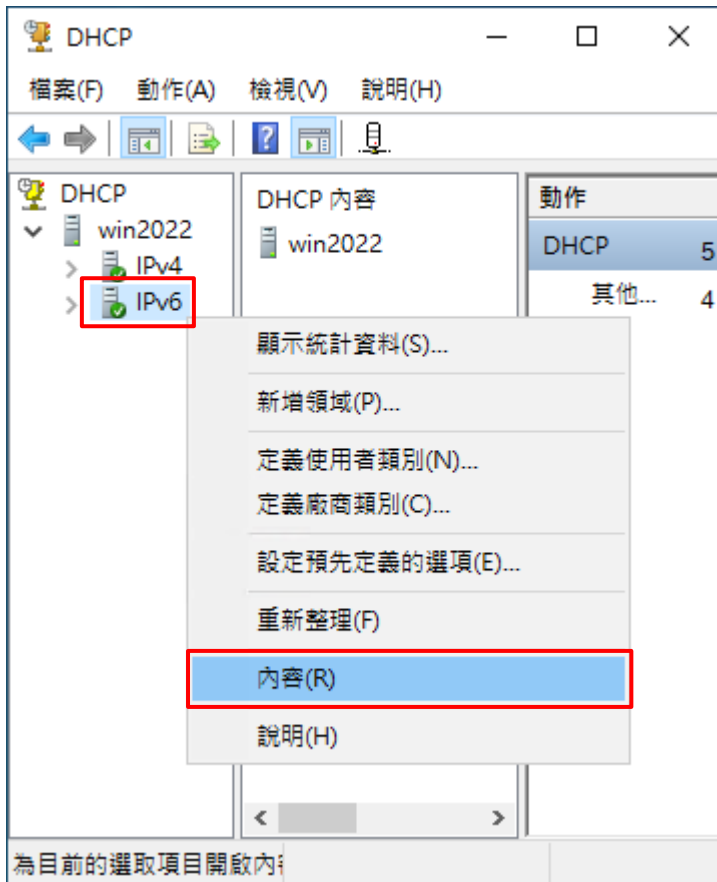


(5) 按 [是] (重啟 DHCP server 服務)



## 7.2 DHCP IPv6

(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]

The screenshot shows a window titled "IPv6 - 內容" with three tabs: "一般" (General), "DNS", and "進階" (Advanced). The "一般" tab is selected and highlighted with a red box. Below the tabs is a server icon and the label "伺服器". There are three checkboxes: "自動更新統計資料，每隔(U):" (unchecked), "啟用 DHCP 稽核記錄(E)" (checked and highlighted with a red box), and "每天將伺服器活動寫入檔案，以便監視系統效能，並進行服務的疑難排解。" (unchecked). Below the "自動更新統計資料" checkbox are two spinners for "小時(H):" (set to 0) and "分鐘(M):" (set to 10). At the bottom are three buttons: "確定" (OK), "取消" (Cancel), and "套用(A)" (Apply).

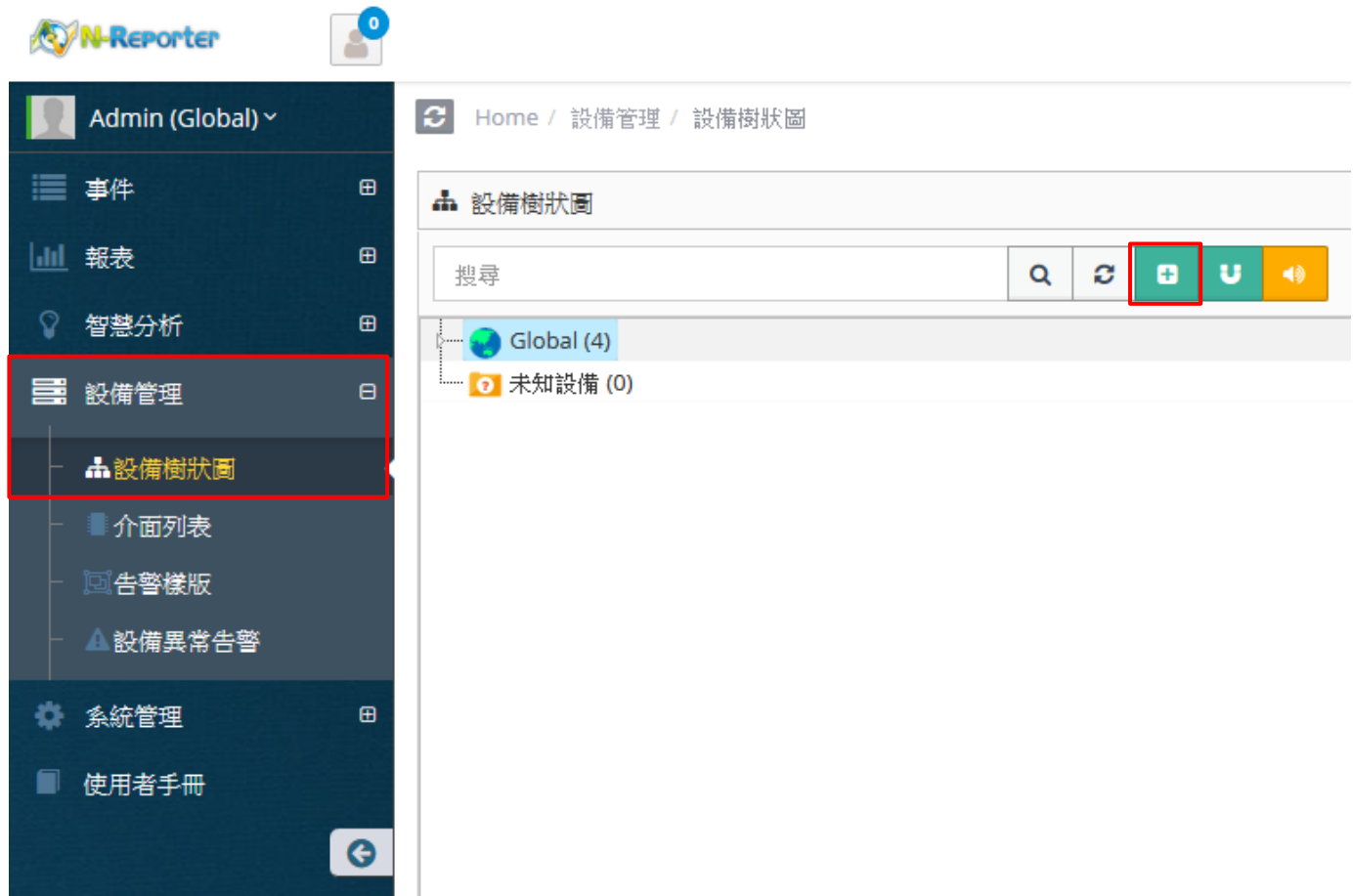
(3) [進階] 頁面 -> 確認稽核記錄檔路徑: [C:\Windows\System32\LogFiles\DHCP]



## 8. N-Reporter

(1) 新增 Windows DHCP 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



The screenshot displays the N-Reporter web application interface. On the left is a dark blue navigation sidebar with the following items: 'Admin (Global) v', '事件', '報表', '智慧分析', '設備管理' (highlighted with a red box), '設備樹狀圖' (highlighted with a red box), '介面列表', '告警樣版', '設備異常告警', '系統管理', and '使用者手冊'. The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖' and the title '設備樹狀圖'. Below the title is a search bar with a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a green 'U' button, and a yellow speaker icon. The main content area lists 'Global (4)' and '未知設備 (0)'.



(2) 設定 Windows DHCP 記錄的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows DHCP] 和 Facility: [(20) local use 4 (local4)]  
和編碼方式: [BIG5] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

設備資訊編輯

設備基本設定

名稱  
WinDHCP-192.168.8.183

IP  
192.168.8.183

設備種類  
 Syslog  Flow  SNMP  PM

Syslog 相關設定

資料格式  
Windows DHCP

使用自定義資料格式

Facility  
(20) local use 4 (local4)

編碼方式  
BIG5

日誌保留 Raw Data  Raw Data

本設備於分時監控報表啟動Syslog轉發時  Raw Data

設備進階設定

ICMP 告警樣版  
----- N/A -----

設備 Icon  
icon-host

Login Account

Login Password

Enable Password

接收狀態  
 啟用  停用

暫無資料告警  
 啟用 Syslog 暫無資料告警

告警通報設定  
預設

資料保留天數

經緯度  
緯度  經度

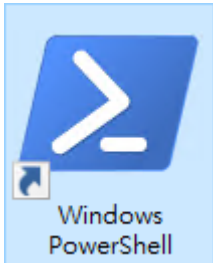
確定 取消

若勾選 [日誌保留 Raw Data] ·  
[事件查詢] 顯示 Raw Data 資訊

## 9. 問題排除

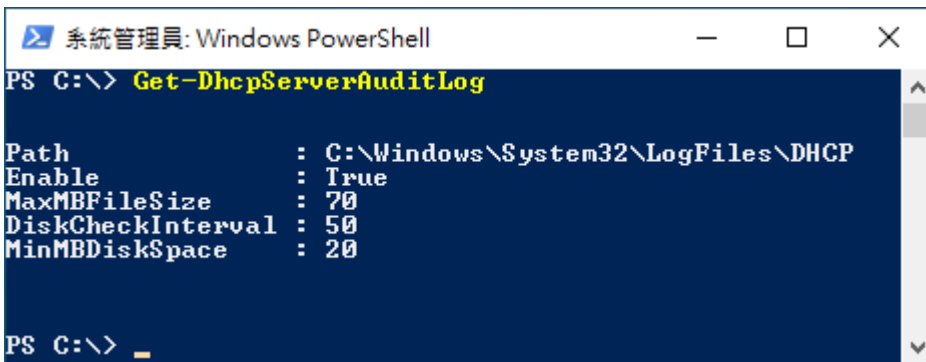
### 9.1 調整 DHCP 記錄檔案大小

(1) 開啟 [Windows PowerShell]



(2) 查看 DHCP Server 稽核 Log 設定

```
PS C:\> Get-DhcpServerAuditLog
```

A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command "Get-DhcpServerAuditLog" has been executed, and the output is displayed in a dark blue background with white text. The output shows the following settings: Path: C:\Windows\System32\LogFiles\DHCP, Enable: True, MaxMBFileSize: 70, DiskCheckInterval: 50, and MinMBDiskSpace: 20. The prompt "PS C:\> \_" is visible at the bottom.

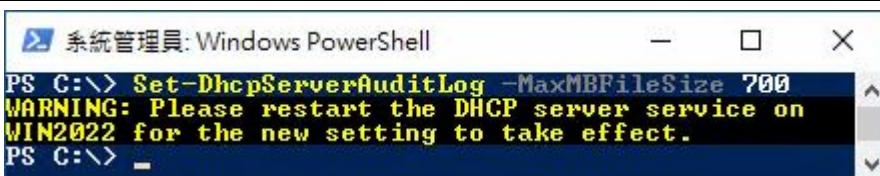
```
系統管理員: Windows PowerShell
PS C:\> Get-DhcpServerAuditLog

Path           : C:\Windows\System32\LogFiles\DHCP
Enable        : True
MaxMBFileSize  : 70
DiskCheckInterval : 50
MinMBDiskSpace : 20

PS C:\> _
```

(3) 設定 DHCP Log 檔案大小

```
PS C:\> Set-DhcpServerAuditLog -MaxMBFileSize 700
```

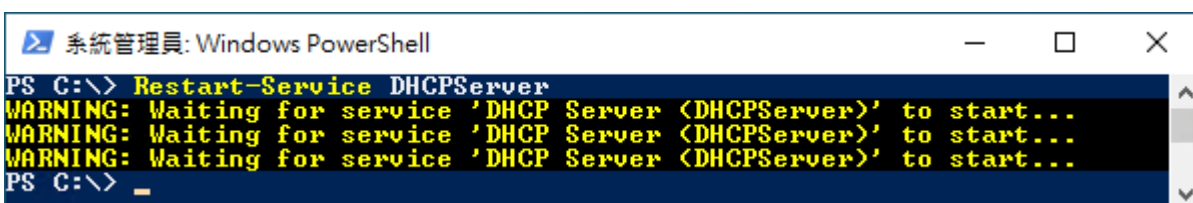
A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command "Set-DhcpServerAuditLog -MaxMBFileSize 700" has been executed. The output shows a warning message: "WARNING: Please restart the DHCP server service on WIN2022 for the new setting to take effect." followed by the prompt "PS C:\> \_".

```
系統管理員: Windows PowerShell
PS C:\> Set-DhcpServerAuditLog -MaxMBFileSize 700
WARNING: Please restart the DHCP server service on
WIN2022 for the new setting to take effect.
PS C:\> _
```

參數 -MaxMBFileSize 700 · 700MB 除以 7 天等於單檔最大 100MB

(4) 重啟 DHCP Server 服務

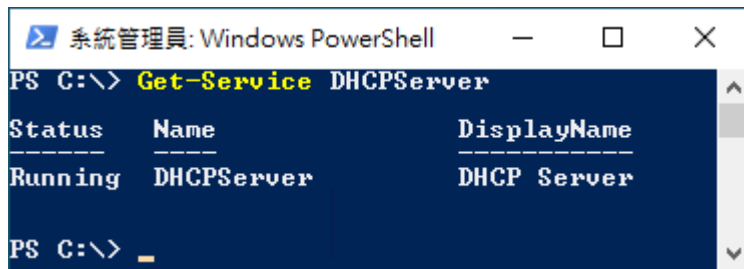
```
PS C:\> Restart-Service DHCPServer
```

A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command "Restart-Service DHCPServer" has been executed. The output shows three warning messages: "WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...", "WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...", and "WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...". The prompt "PS C:\> \_" is visible at the bottom.

```
系統管理員: Windows PowerShell
PS C:\> Restart-Service DHCPServer
WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...
WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...
WARNING: Waiting for service 'DHCP Server (DHCPService)' to start...
PS C:\> _
```

(5) 查看 DHCP Server 服務

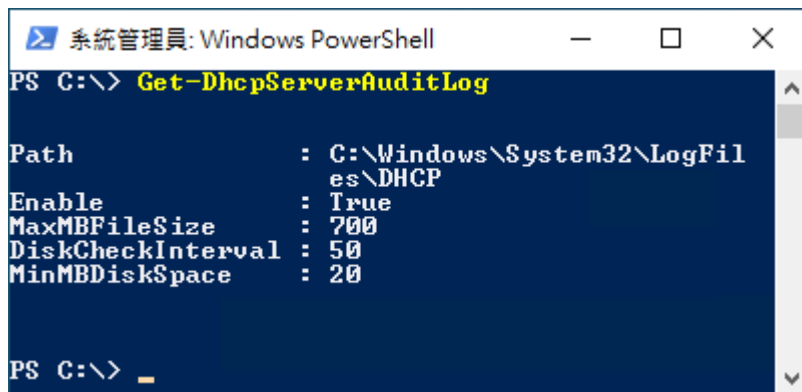
PS C:\> `Get-Service DHCPServer`



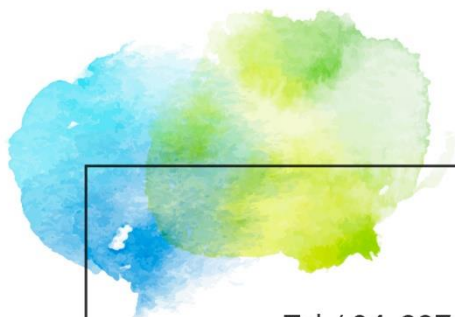
```
系統管理員: Windows PowerShell
PS C:\> Get-Service DHCPServer
-----
Status      Name          DisplayName
-----
Running     DHCPServer    DHCP Server
PS C:\> _
```

(6) 查看 DHCP Server 稽核 Log 設定

PS C:\> `Get-DhcpServerAuditLog`



```
系統管理員: Windows PowerShell
PS C:\> Get-DhcpServerAuditLog
Path           : C:\Windows\System32\LogFiles\DHCP
Enable         : True
MaxMBFileSize  : 700
DiskCheckInterval : 50
MinMBDiskSpace : 20
PS C:\> _
```



Tel / 04-23752865    Fax / 04-23757458  
業務詢問 / [sales@npartnertech.com](mailto:sales@npartnertech.com)  
技術詢問 / [support@npartnertech.com](mailto:support@npartnertech.com)