



如何設定 Windows DHCP log

V012



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	1
1 NXLog	2
1.1 NXLog 安裝	2
1.2 NXLog 設定檔下載	6
1.2.1 Windows 2003 或之前版本作業系統	6
1.2.2 Windows 2008 或之後版本作業系統	7
1.3 NXLog 設定檔	8
1.4 NXLog 啟動服務	9
1.4.1 Windows 2003 或之前版本作業系統	9
1.4.2 Windows 2008 或之後版本作業系統	12
2 Windows 2003	15
3 Windows 2008	18
3.1 DHCP IPv4	18
3.2 DHCP IPv6	21
4 Windows 2012	23
4.1 DHCP IPv4	23
4.2 DHCP IPv6	26
5 Windows 2016	28
5.1 DHCP IPv4	28
5.2 DHCP IPv6	31
6 Windows 2019	33
6.1 DHCP IPv4	33
6.2 DHCP IPv6	36
7 Windows 2022	38
7.1 DHCP IPv4	38
7.2 DHCP IPv6	41
8 N-Reporter	43
8.1 Windows 2003 或之前版本作業系統	45
8.2 Windows 2008 或之後版本作業系統	48
9 問題排除	51
9.1 調整 DHCP 記錄檔案大小	51

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

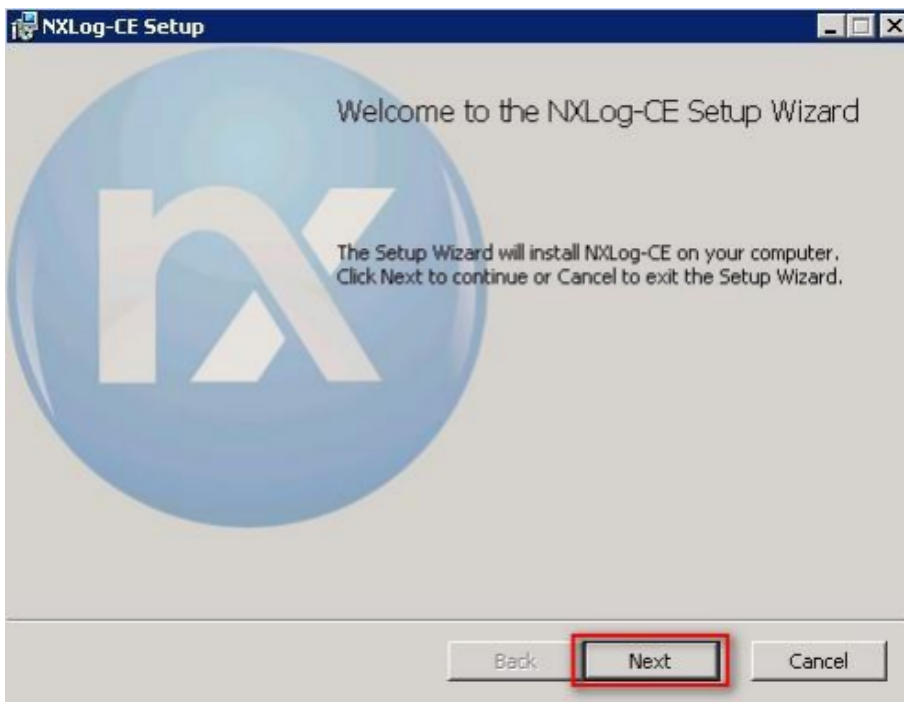


註：若需要下載 NXLog 32bit 版本，請與我們連繫。

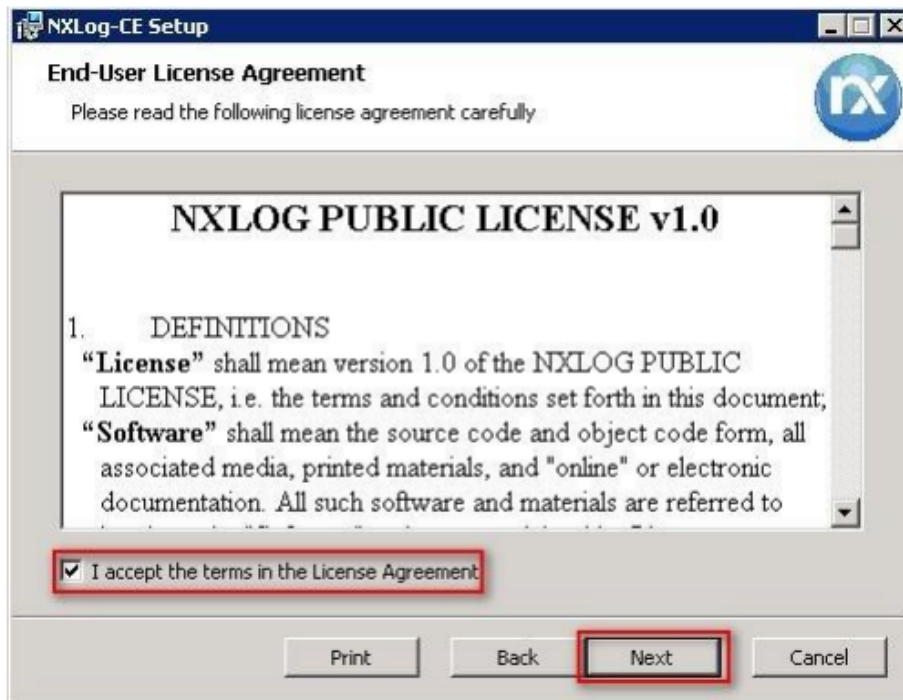
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

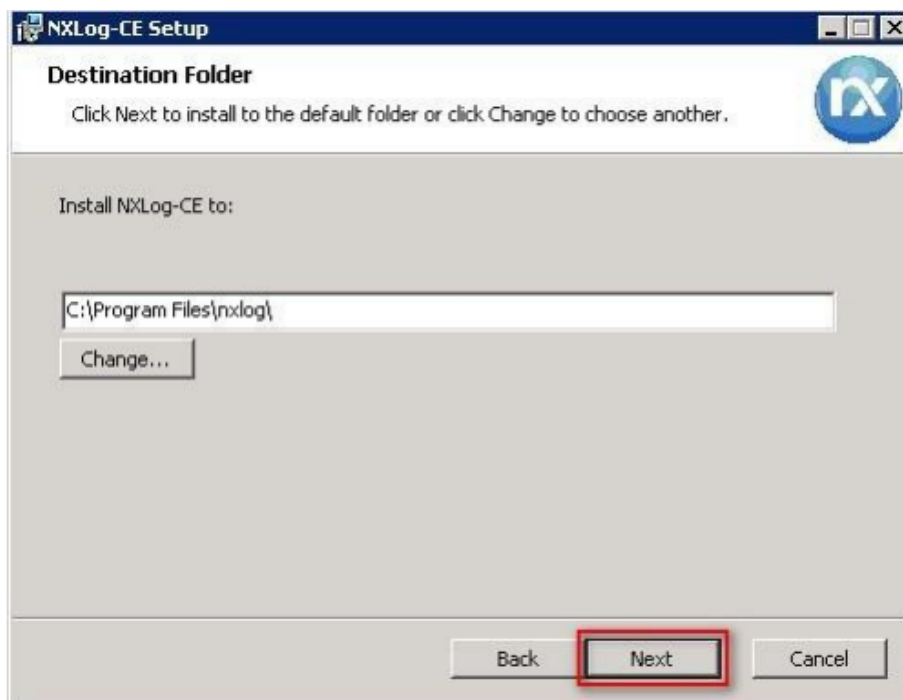
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



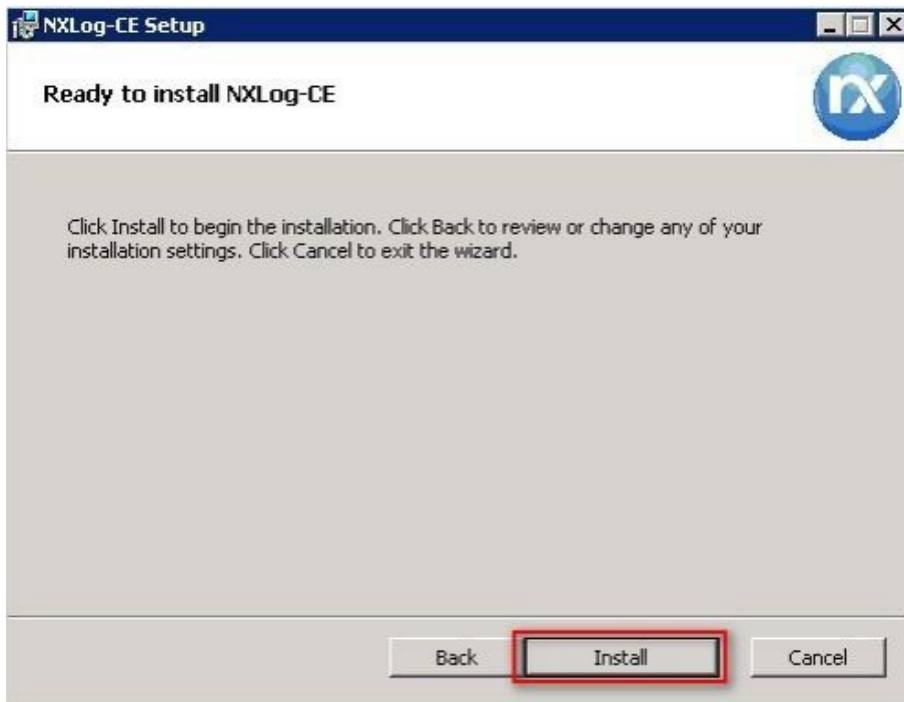
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



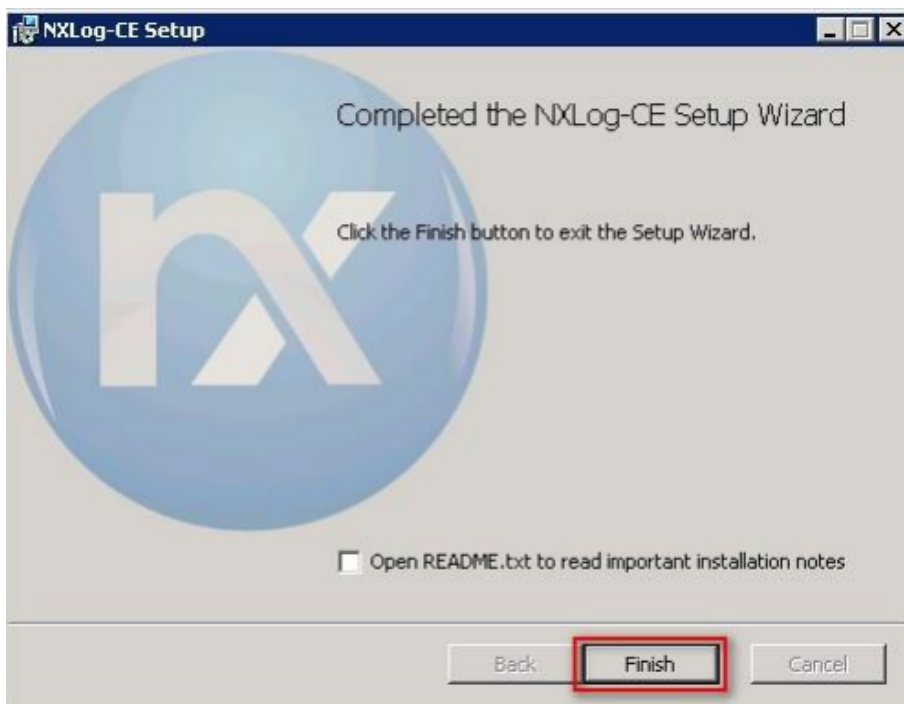
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].

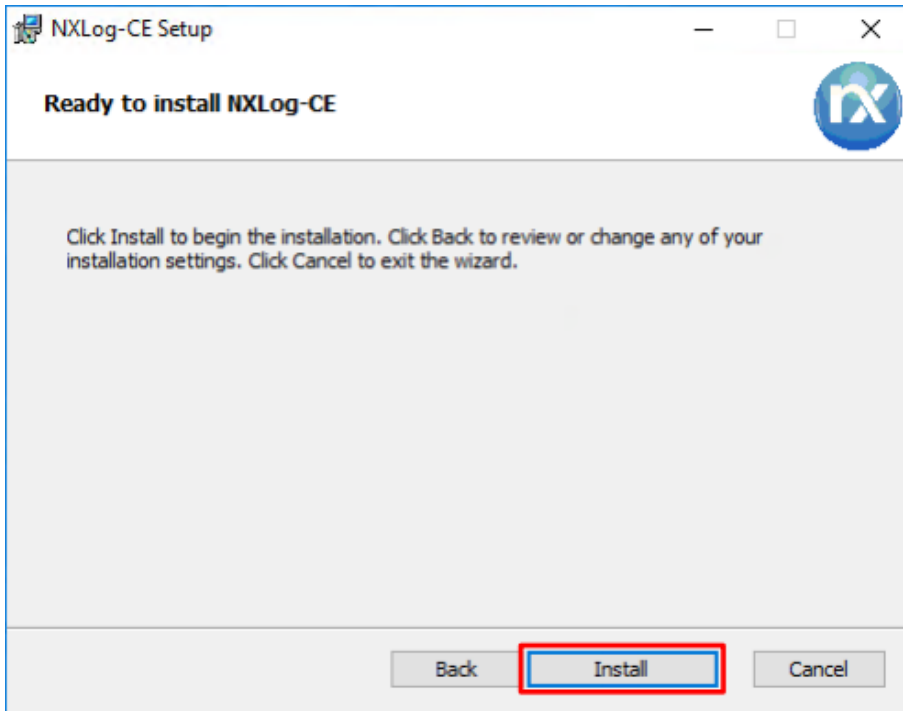


-> 按 [Finish].



<2.2> Windows 2003

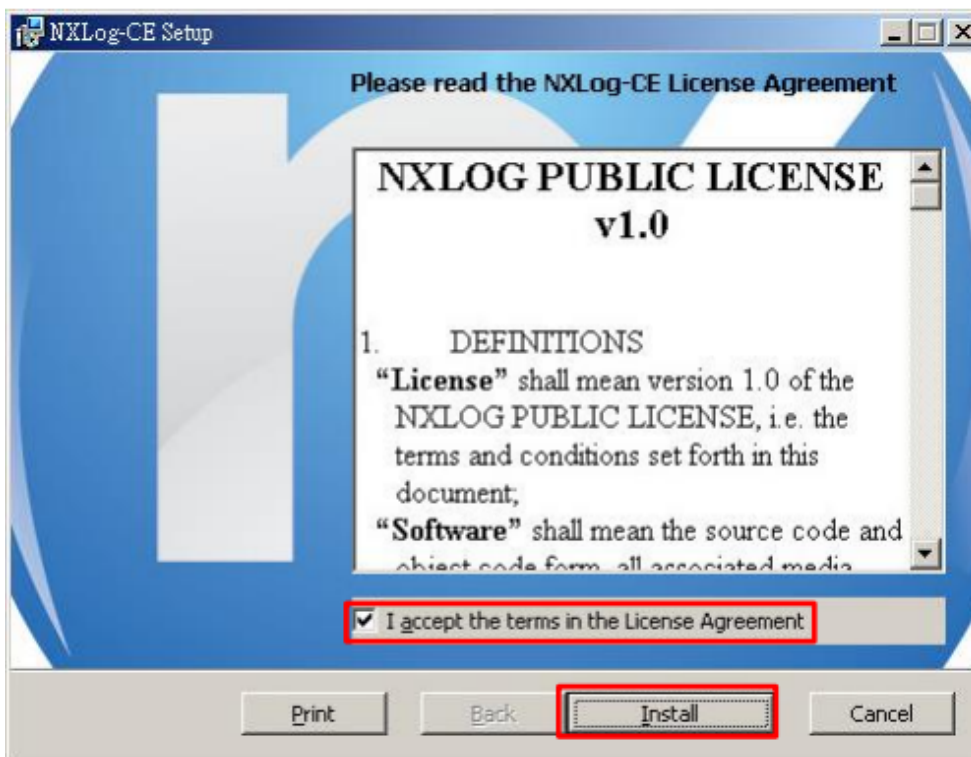
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].



<2.3> Windows 2000

前往 NXLog CE 舊版網址 <https://sourceforge.net/projects/nxlog-ce/> , 左點 [See All Activity] , 下載 NXLOG CE 支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.msi] -> 勾選 [I accept the terms in the License Agreement] -> 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

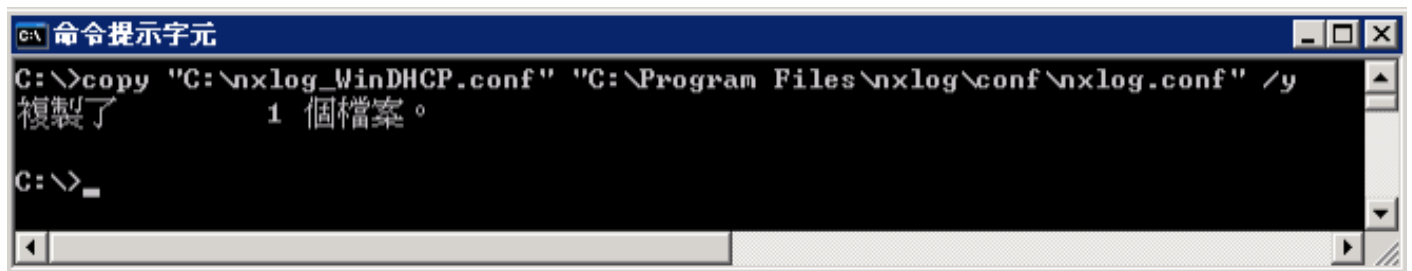
(1) 開啟 [命令提示字元]



(2) 下載 NXLog 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

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



本文件範例是 64 位元作業系統，若作業系統是 32 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

```
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 64 位元作業系統，若作業系統是 32 位元，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 192.168.3.88
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 192.168.3.88
```

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
```

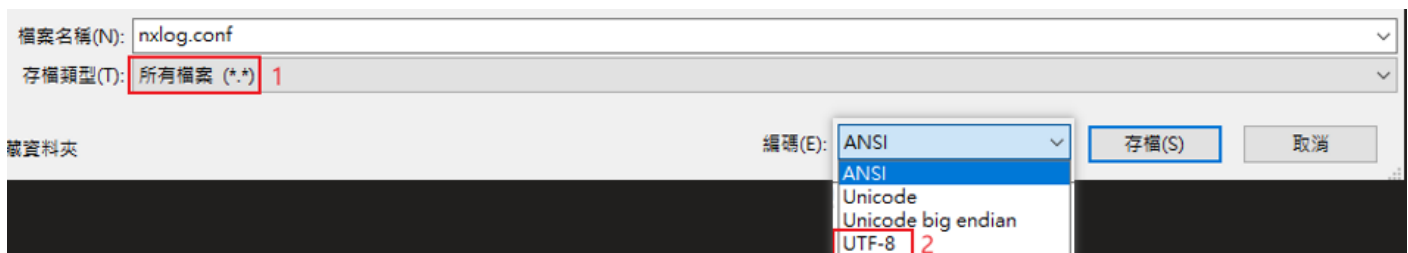
若 NXLog 無法讀取 System32 資料夾路徑時，請輸入 Sysnative，Sysnative 是重定向資料夾

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

藍色文字部位請輸入 DHCP 檔名

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

修改設定檔內容後需“另存新檔”覆蓋原本檔案，1. 存檔類型請選擇“所有檔案 (*.*)”，2. 編碼請選擇“UTF-8”以免編碼錯誤造成服務無法正常開啟。



1.4 NXLog 啟動服務

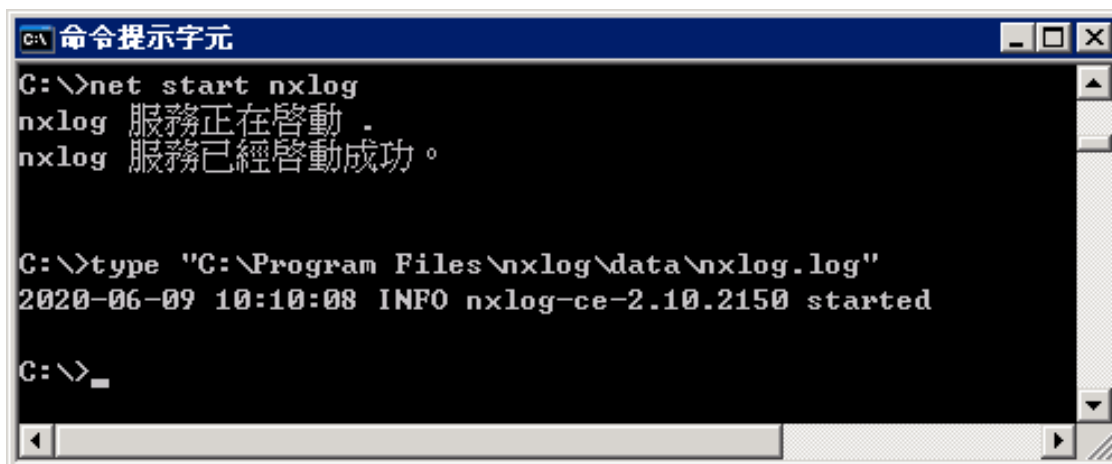
1.4.1 Windows 2003 或之前版本作業系統

(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

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



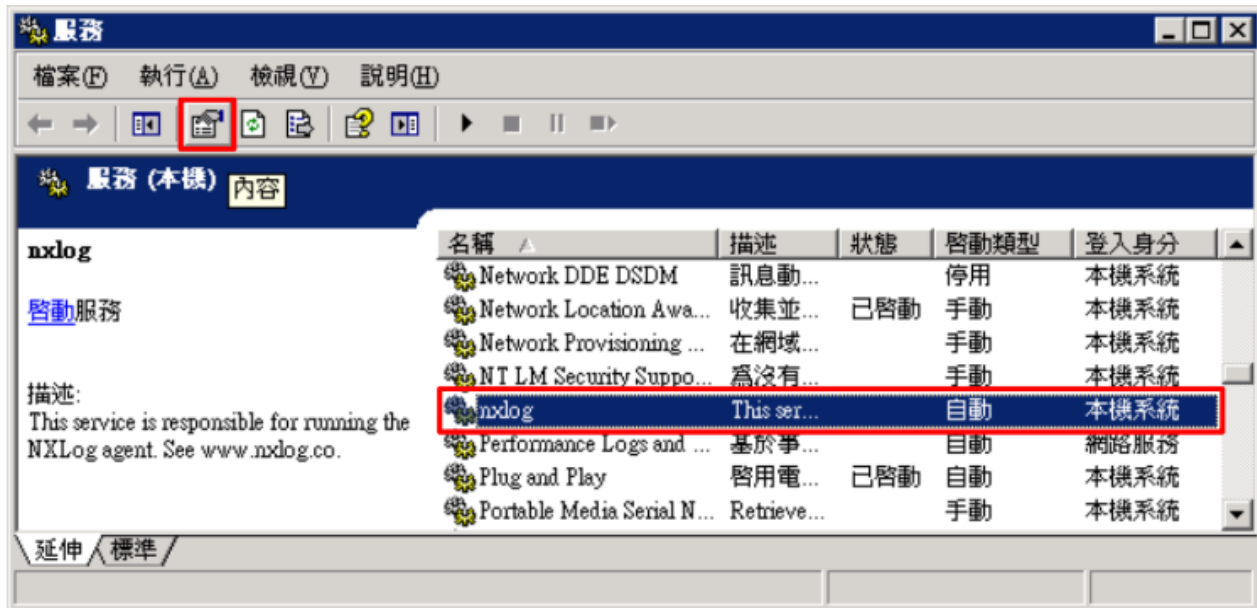
(3) 開啟 [服務] 功能

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

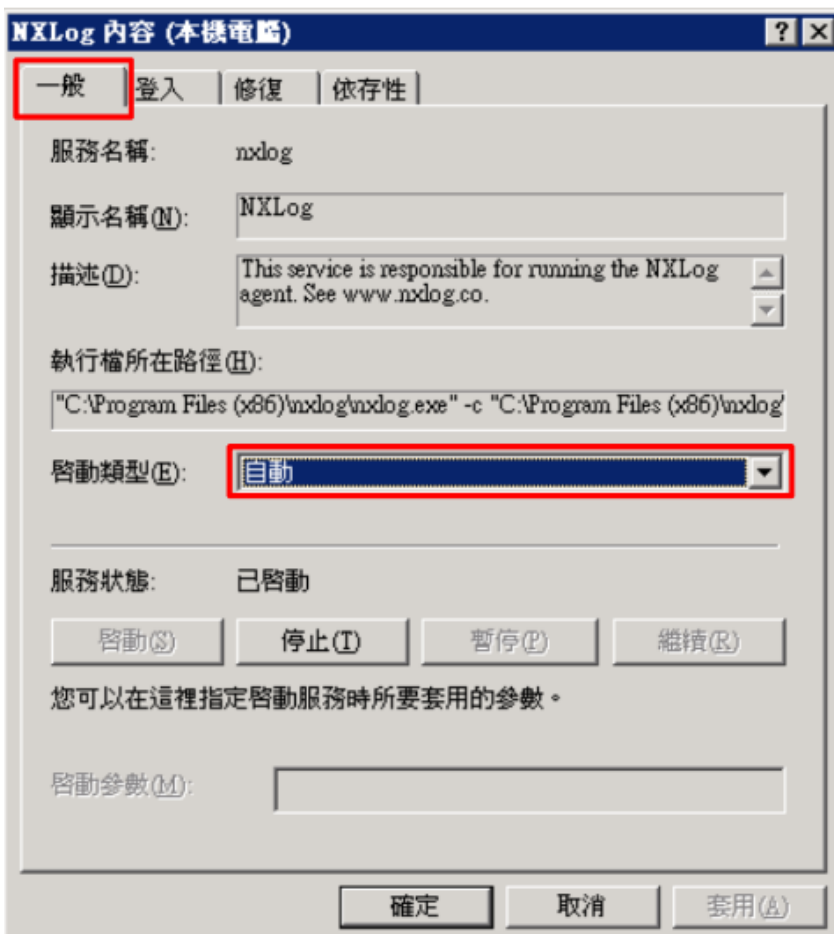


(4) 開啟 NXLog 服務內容

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]

NXLog 內容 (本機電腦)

一般 | 登入 | **修復** | 依存性

如果這項服務執行失敗時，電腦將採取的回應。

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

重設失敗計數於(O): 0 天之後

重新啟動服務於(Y): 1 分鐘之後

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)

電腦重新啟動的選項(R)...

確定 取消 套用(A)

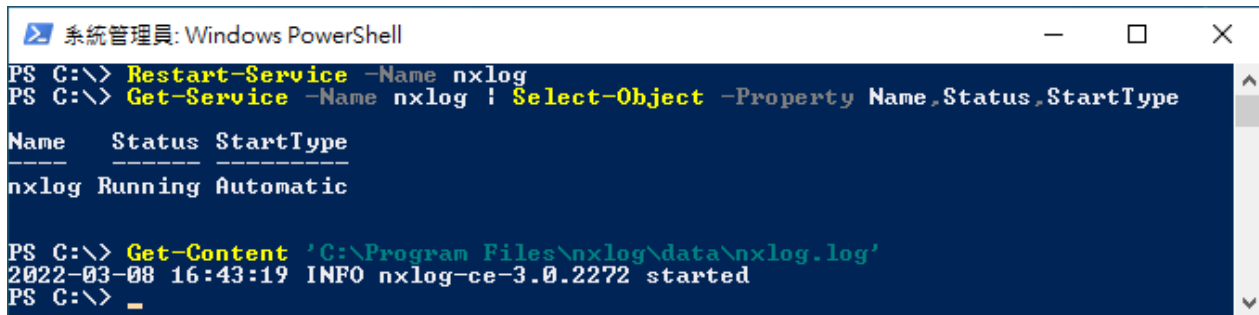
1.4.2 Windows 2008 或之後版本作業系統

(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 window titled "系統管理員: Windows PowerShell". The window shows the following commands and output:

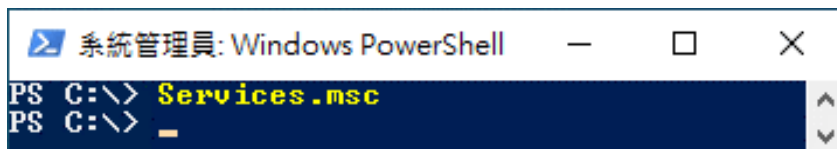
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
Name      Status StartType
-----
nxlog     Running Automatic

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:\> _
```

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'

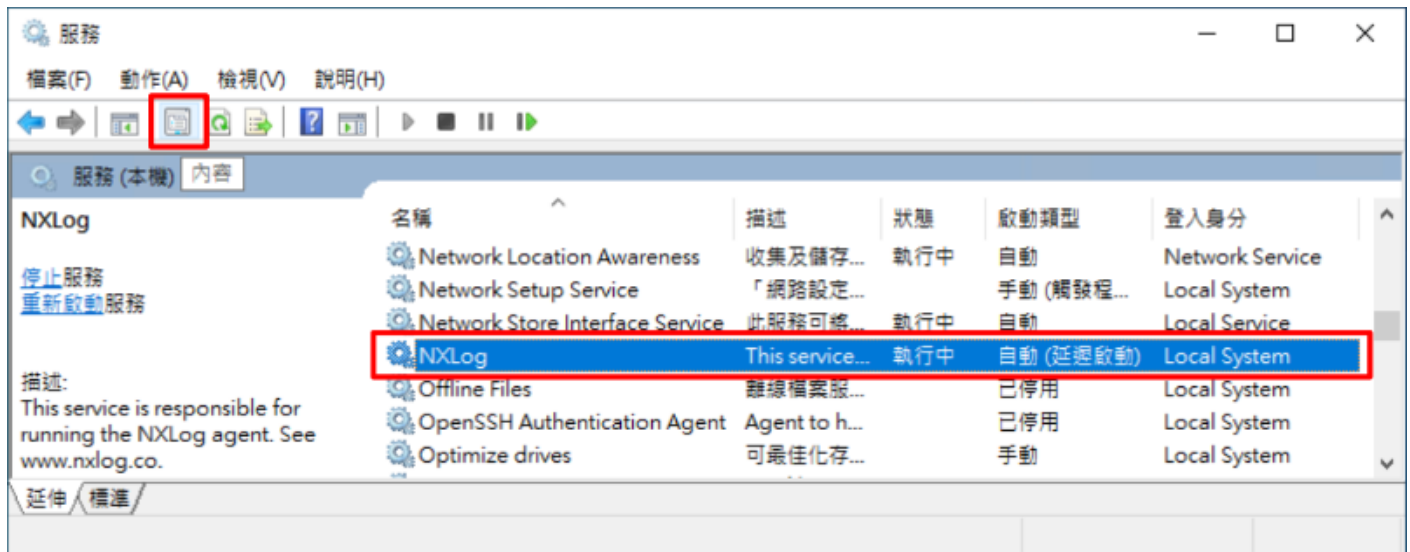
(3) 開啟 [服務] 功能

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

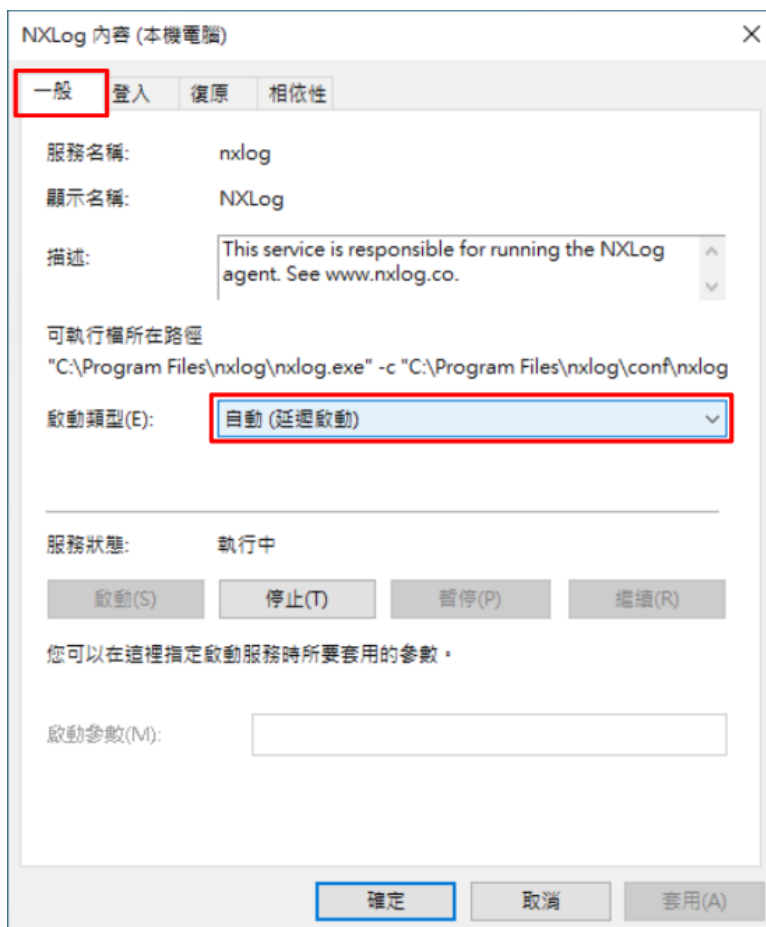


(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選 [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (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) X

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 v

第二次失敗時(S): 重新啟動服務 v

後續失敗時(U): 重新啟動服務 v

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

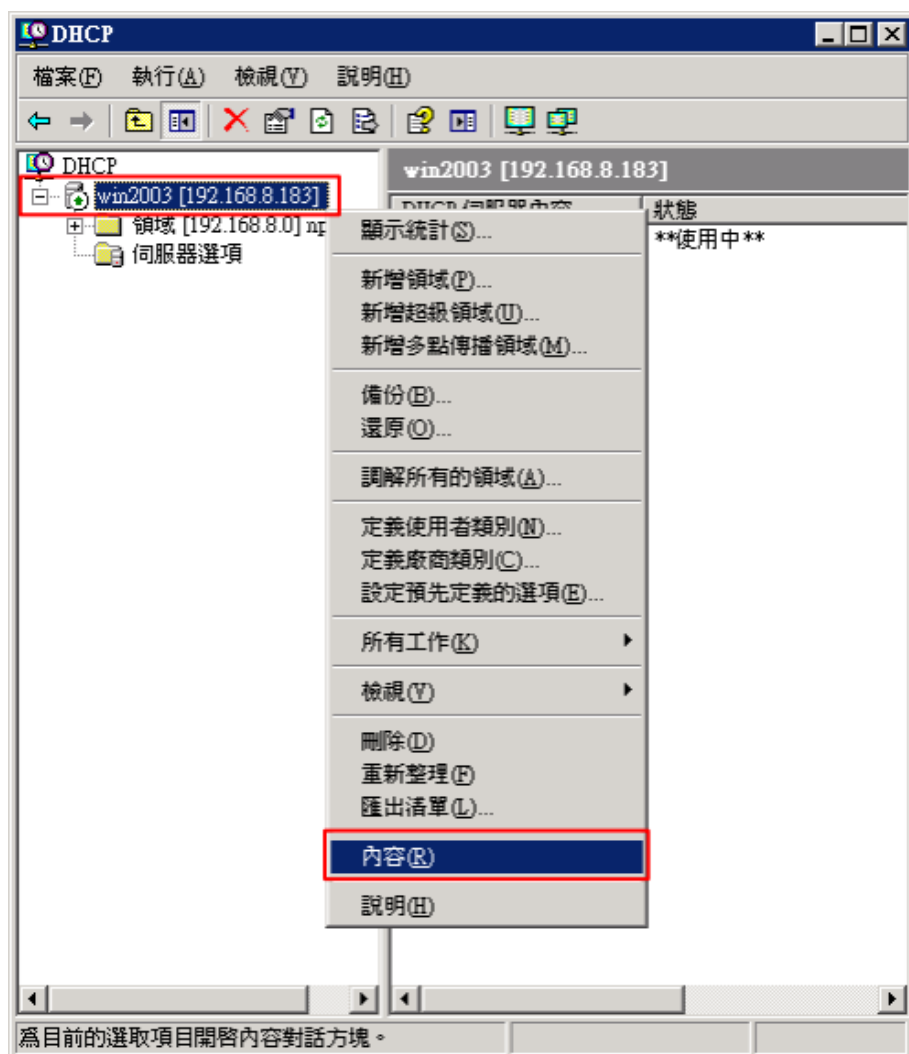
```
PS C:\> mkdir C:\Windows\System32\LogFiles\DHCP
PS C:\> dir C:\Windows\System32\LogFiles
```



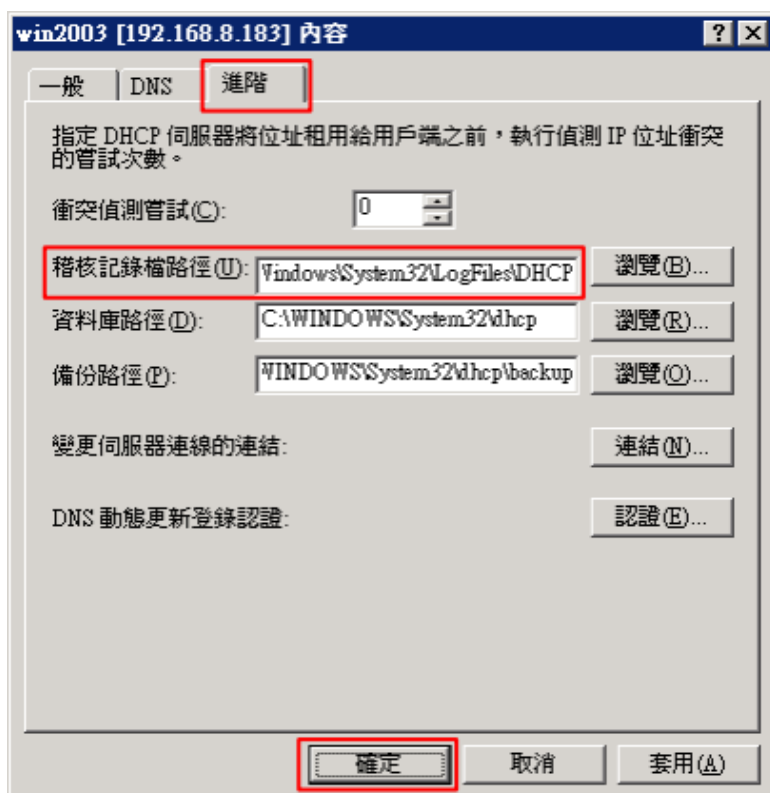
(3) 開啟 [DHCP]



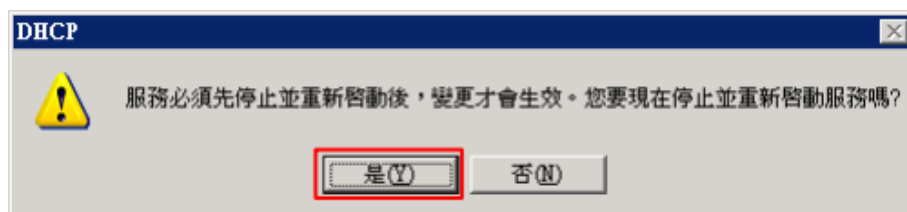
(4) 在 [DHCP 伺服器] 上按滑鼠右鍵 -> 選擇 [內容]



(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



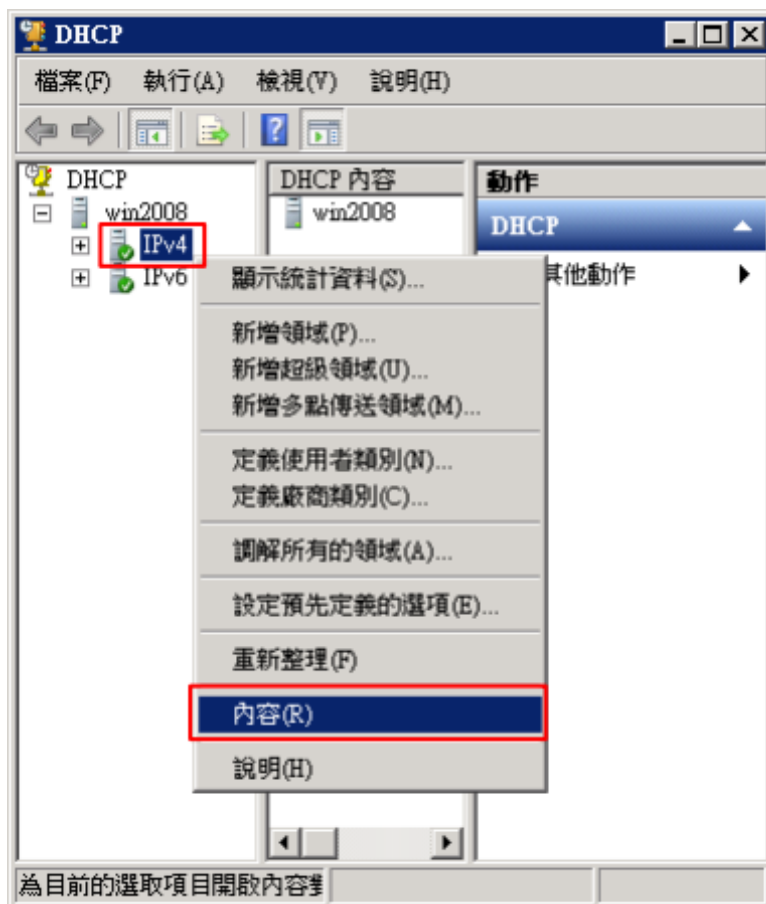
3 Windows 2008

3.1 DHCP IPv4

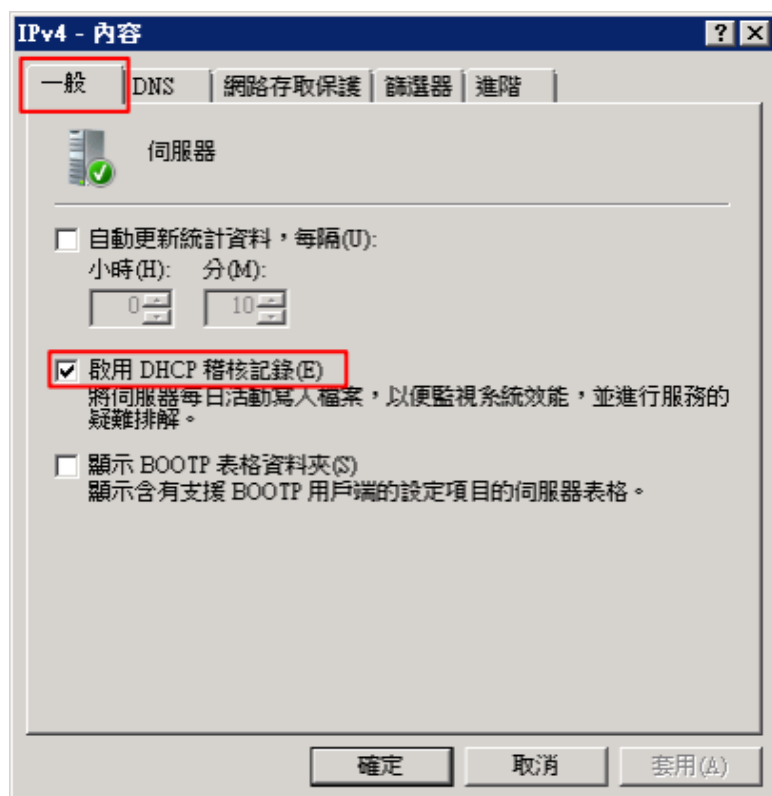
(1) 開啟 [DHCP]



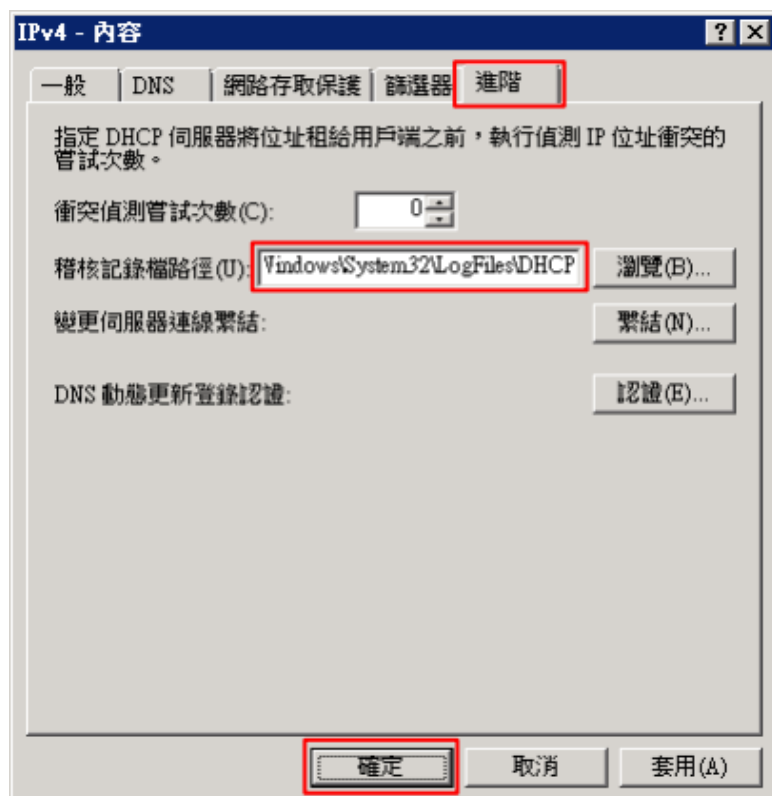
(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



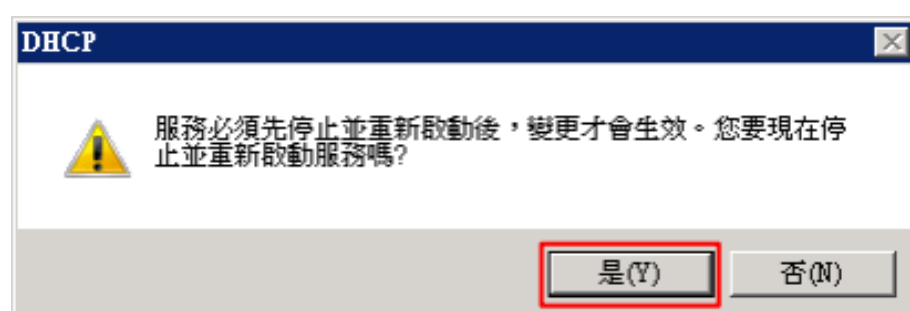
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



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

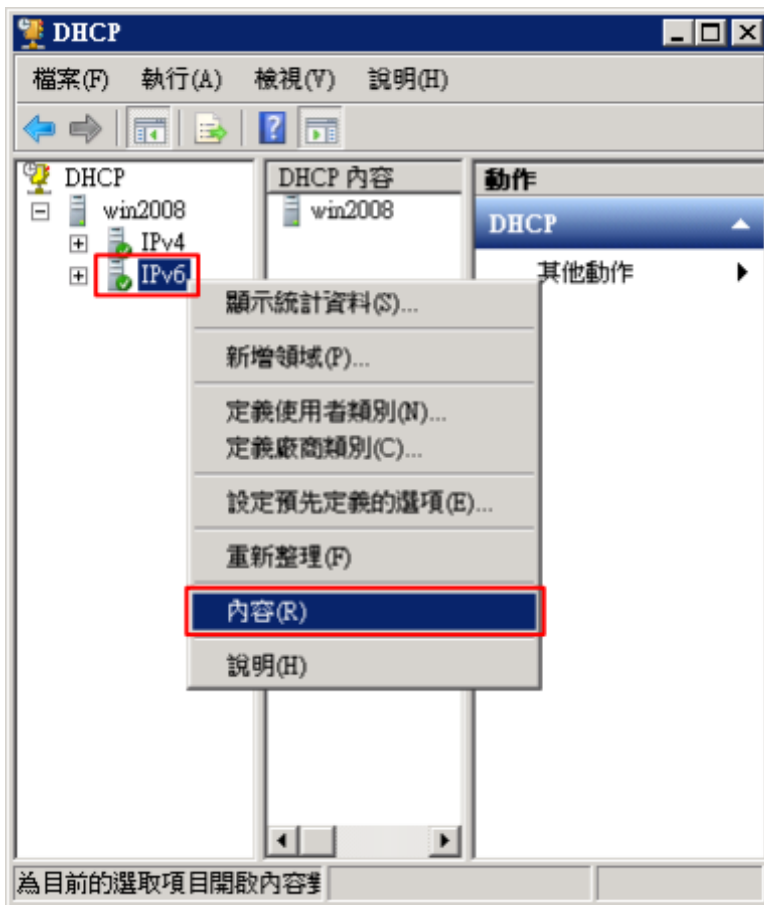


(5) 按 [是] (重啟 DHCP server 服務)

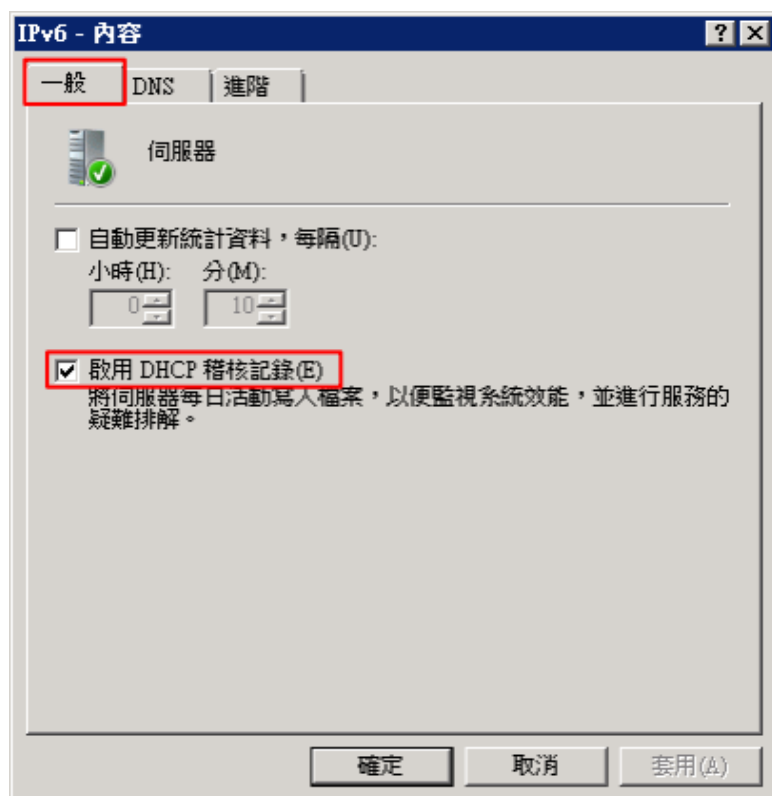


3.2 DHCP IPv6

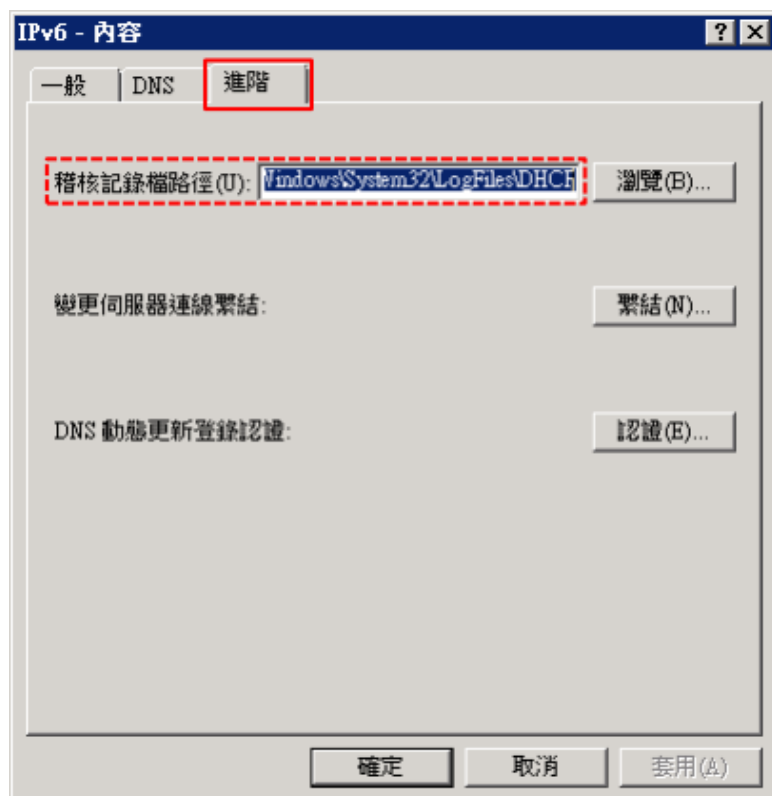
(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



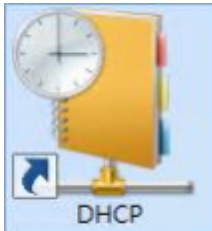
(3) [進階] 頁面 -> 輸入稽核記錄檔路徑: `C:\Windows\System32\LogFiles\DHCP` -> 按 [確定]



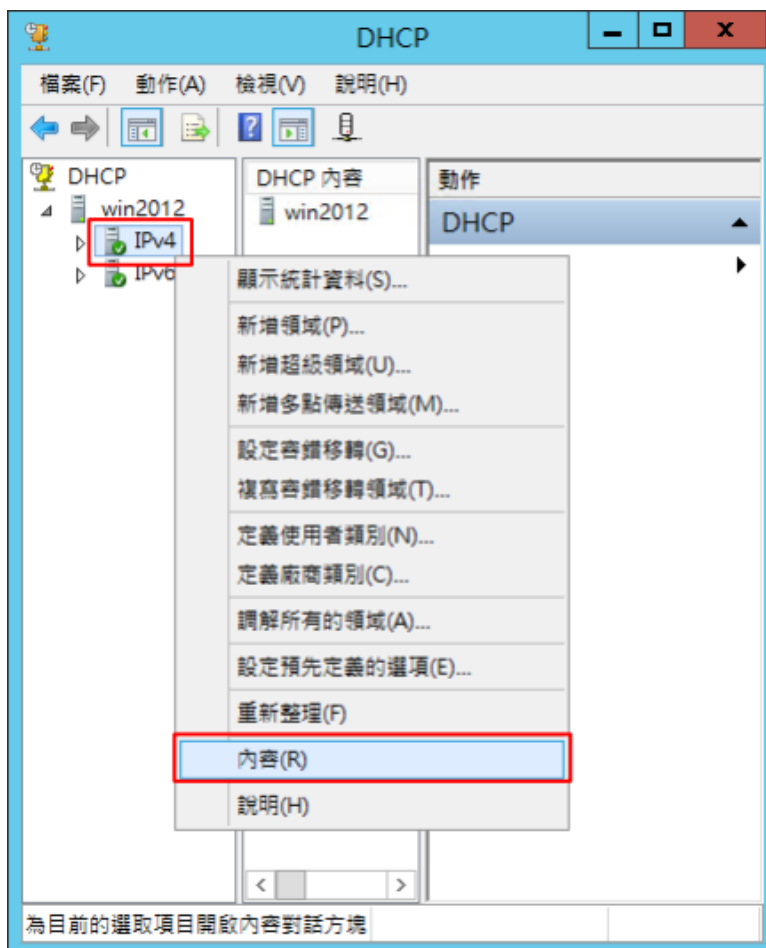
4 Windows 2012

4.1 DHCP IPv4

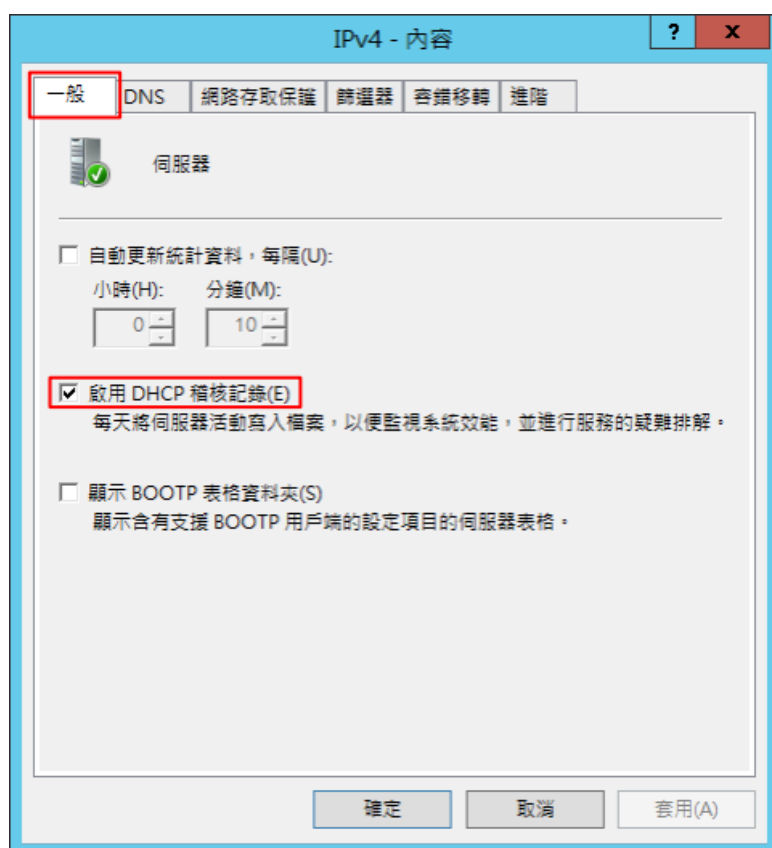
(1) 開啟 [DHCP]



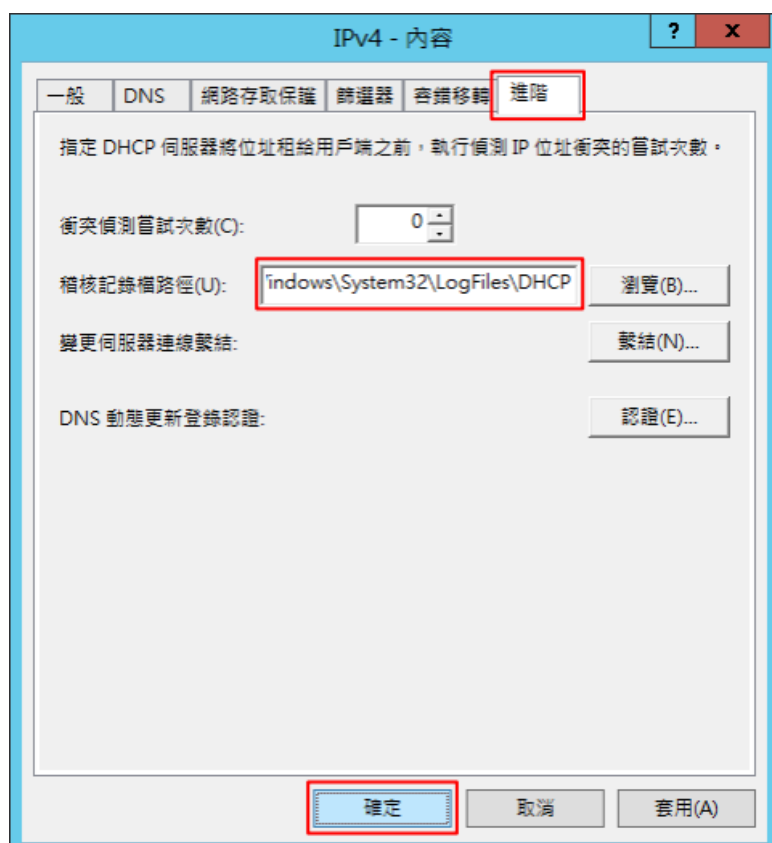
(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



(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]

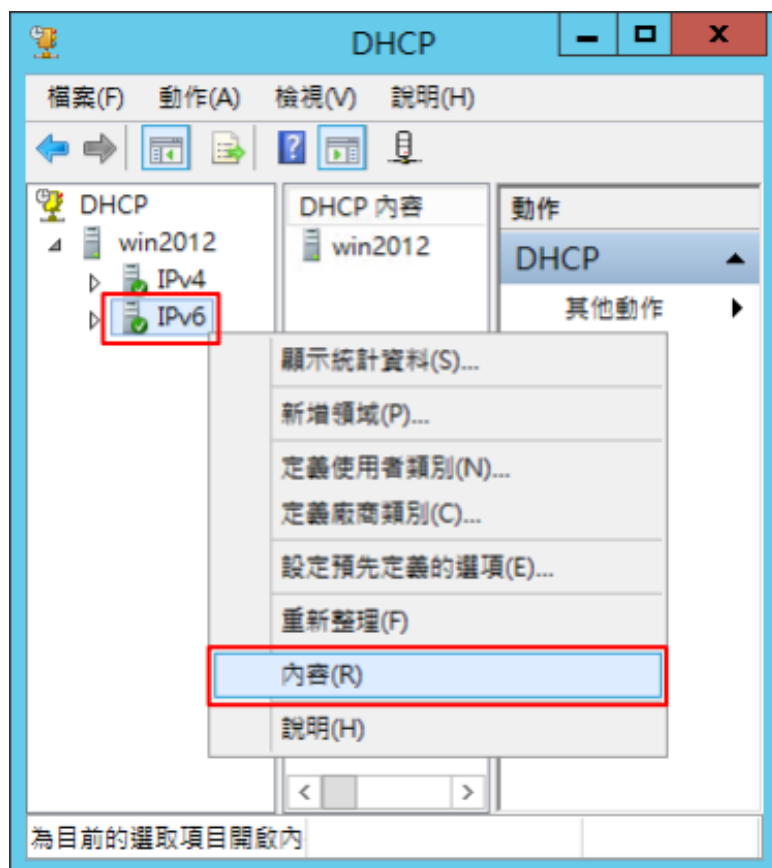


(5) 按 [是] (重啟 DHCP server 服務)

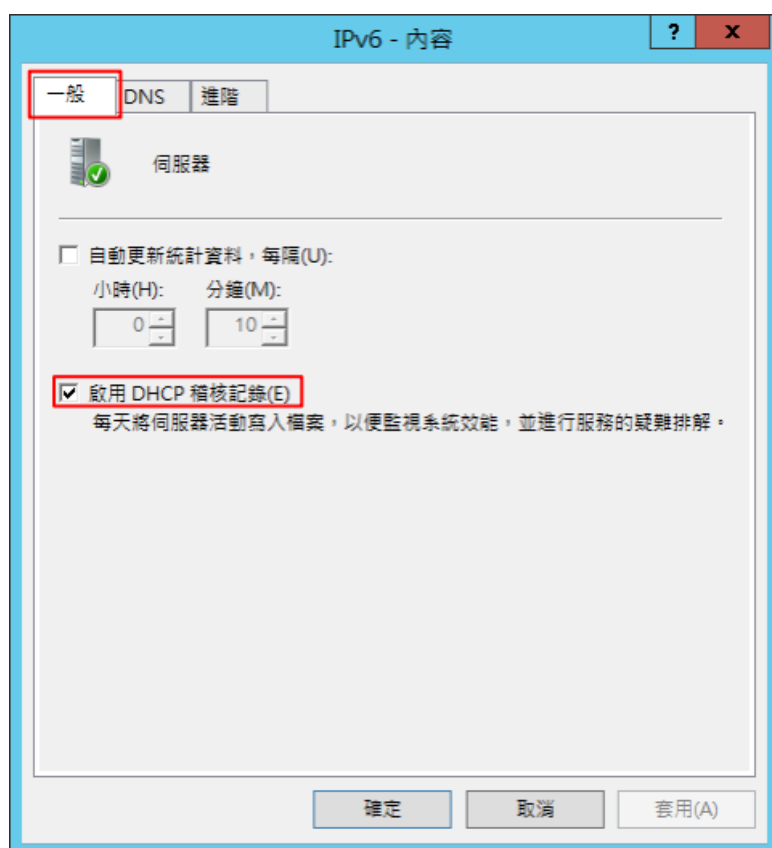


4.2 DHCP IPv6

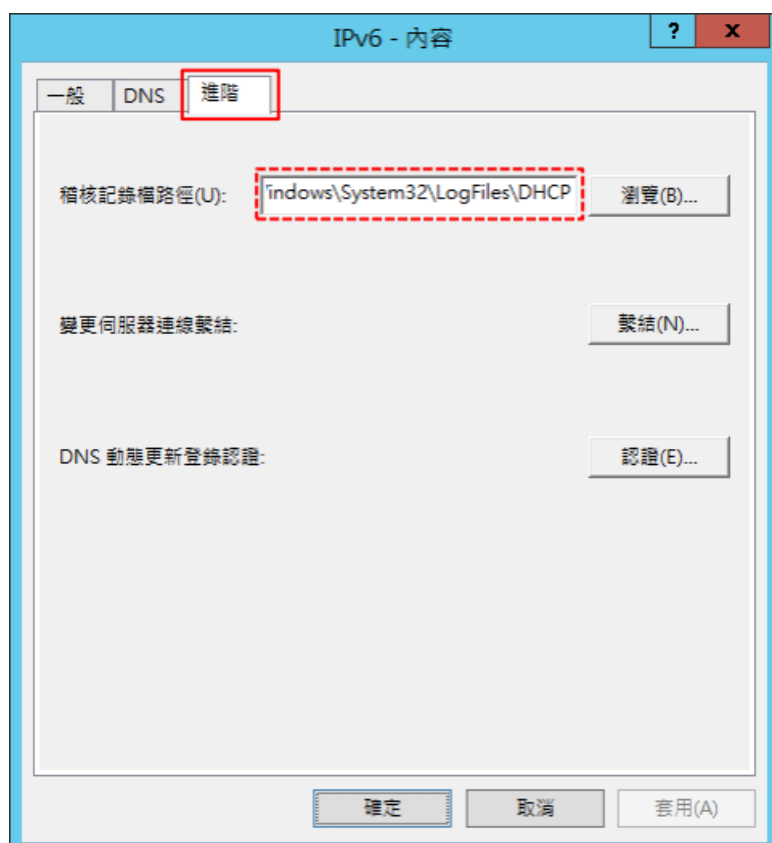
(1) 在 [IPv6] 按滑鼠右鍵 -> 選擇 [內容]



(2) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



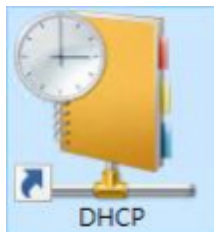
(3) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]



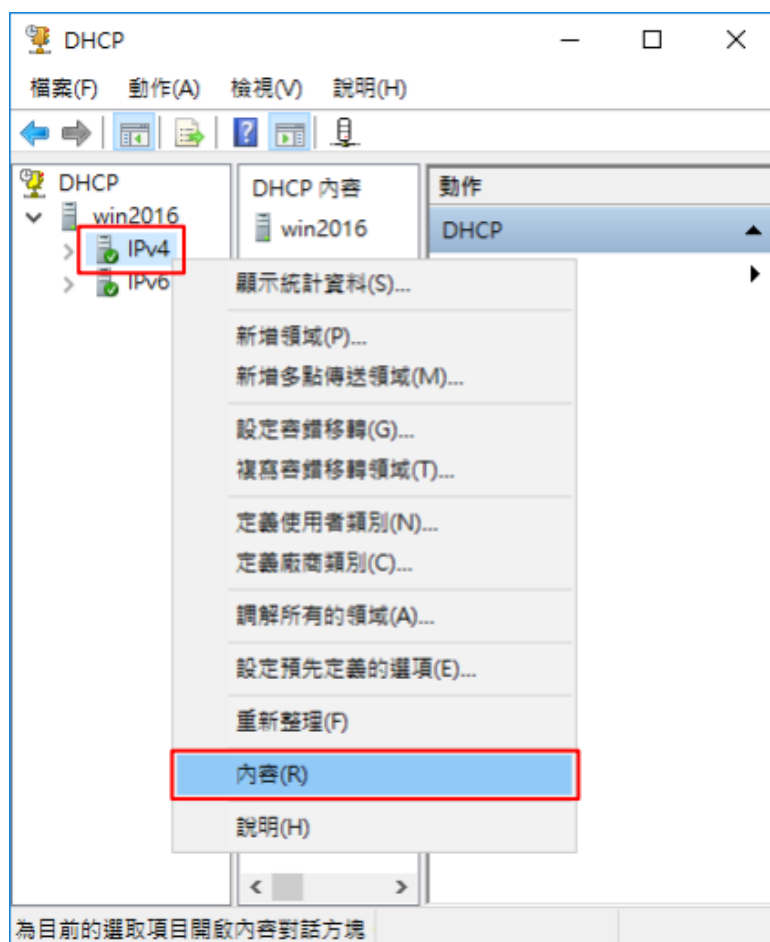
5 Windows 2016

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]

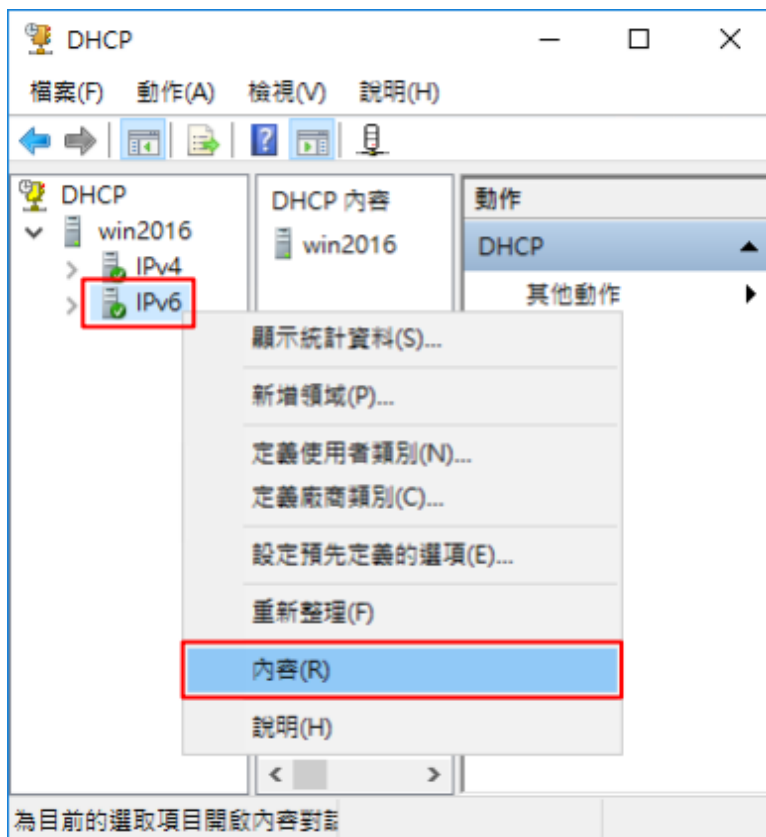


(5) 按 [是] (重啟 DHCP server 服務)

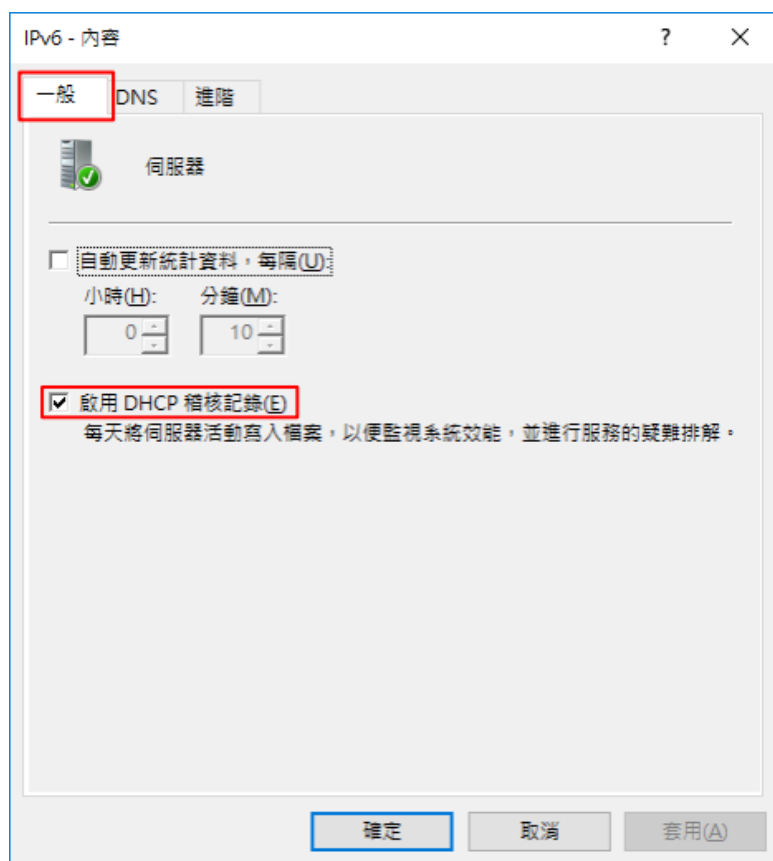


5.2 DHCP IPv6

(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]



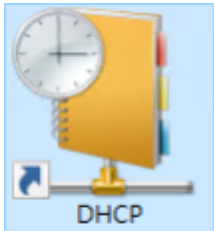
(3) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]



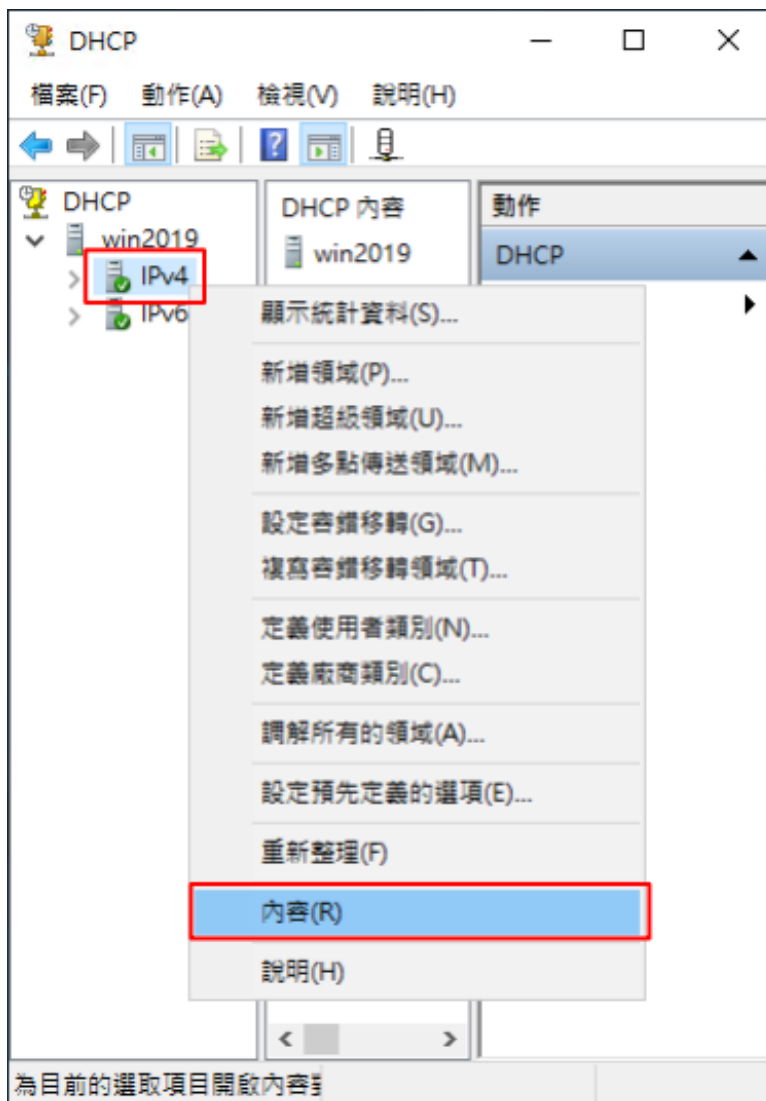
6 Windows 2019

6.1 DHCP IPv4

(1) 開啟 [DHCP]



(2) 在 [IPv4] 按滑鼠右鍵 -> 選擇 [內容]



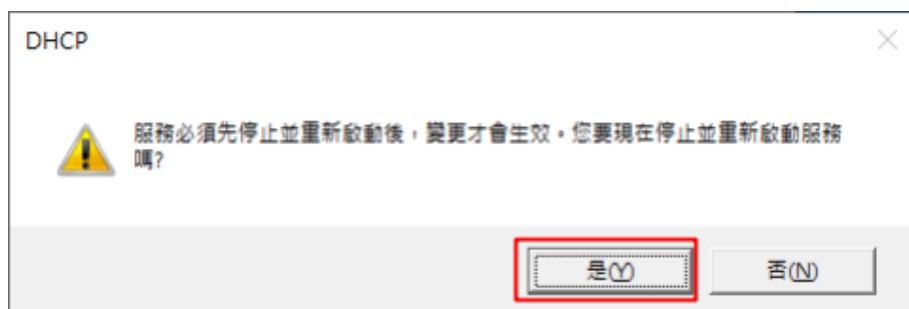
(3) [一般] 頁面 -> 確認 [啟用 DHCP 稽核記錄]



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

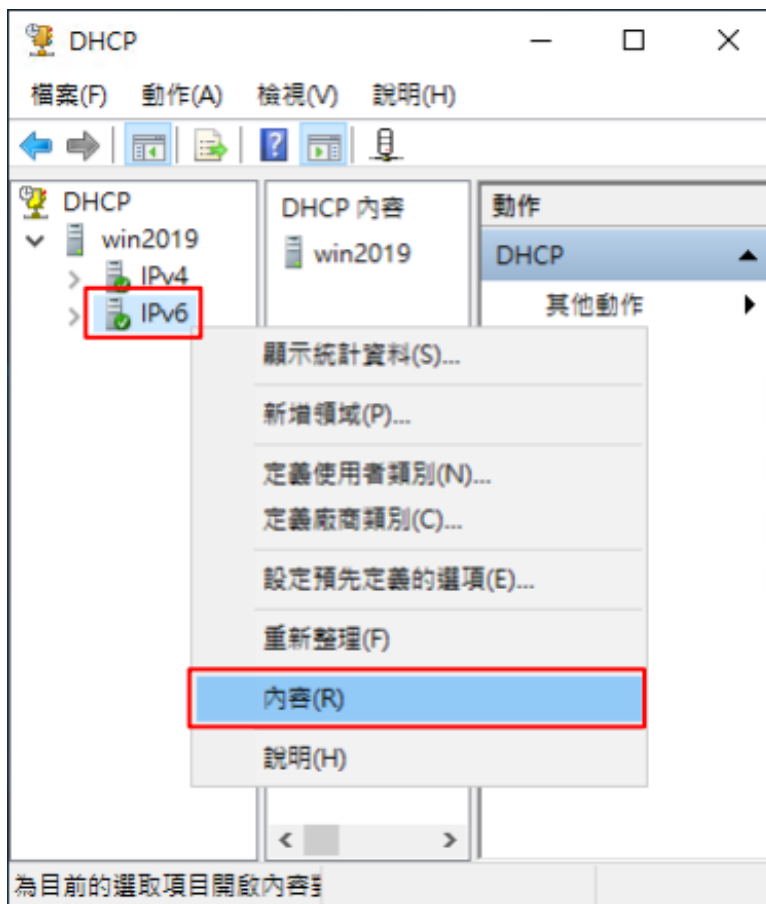


(5) 按 [是] (重啟 DHCP server 服務)

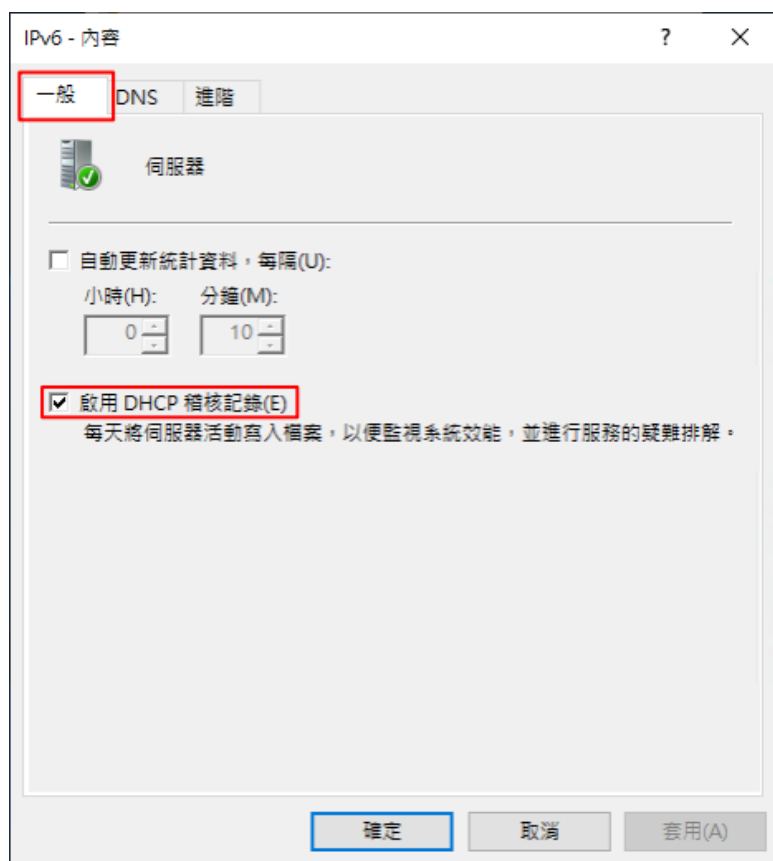


6.2 DHCP IPv6

(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]



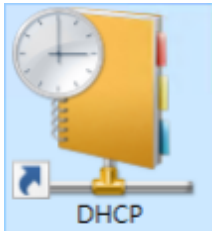
(3) [進階] 頁面 -> 輸入稽核記錄檔路徑: C:\Windows\System32\LogFiles\DHCP -> 按 [確定]



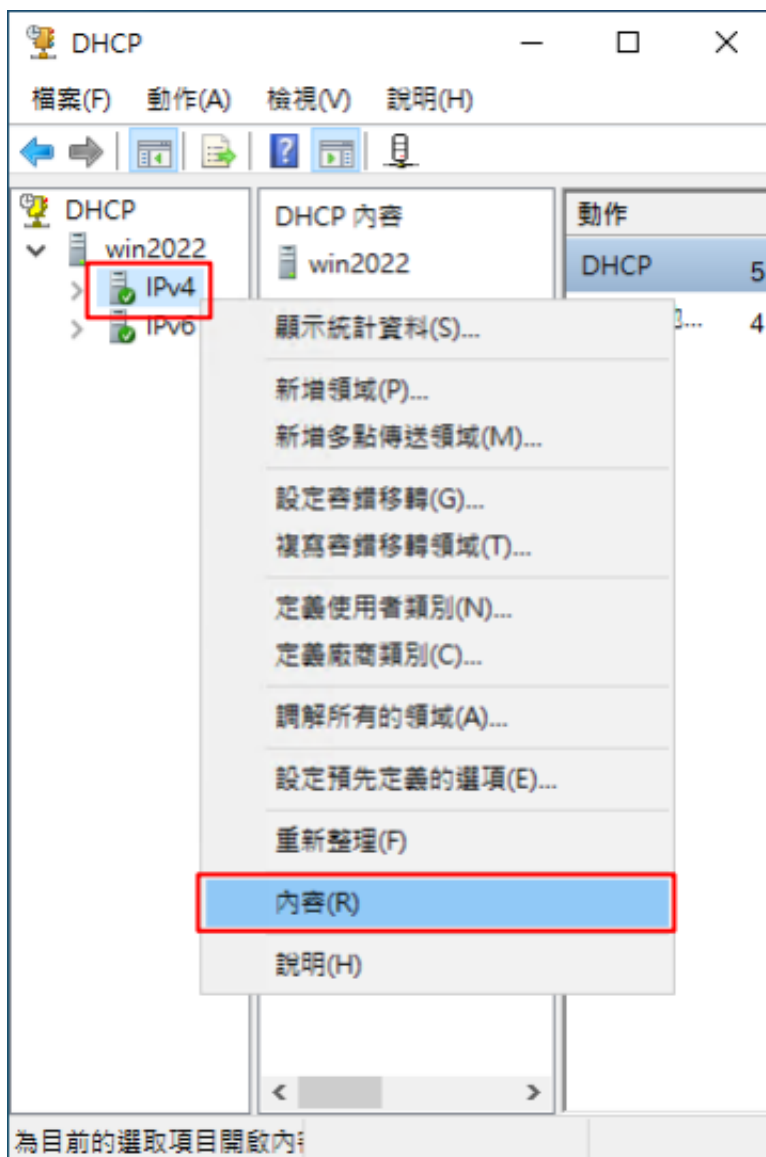
7 Windows 2022

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]

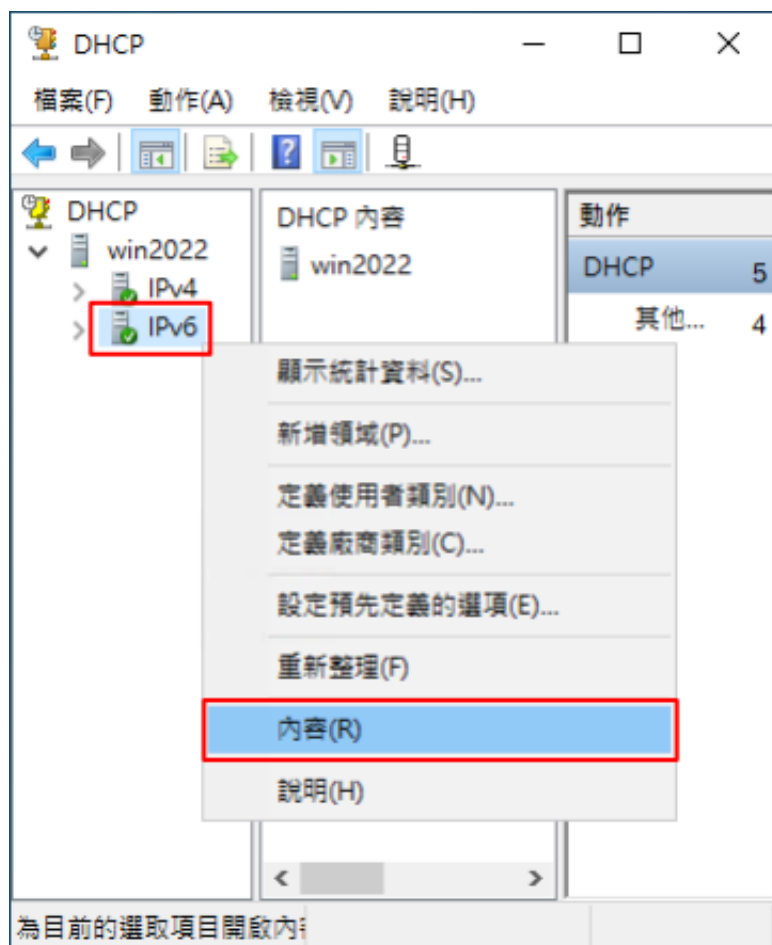


(5) 按 [是] (重啟 DHCP server 服務)

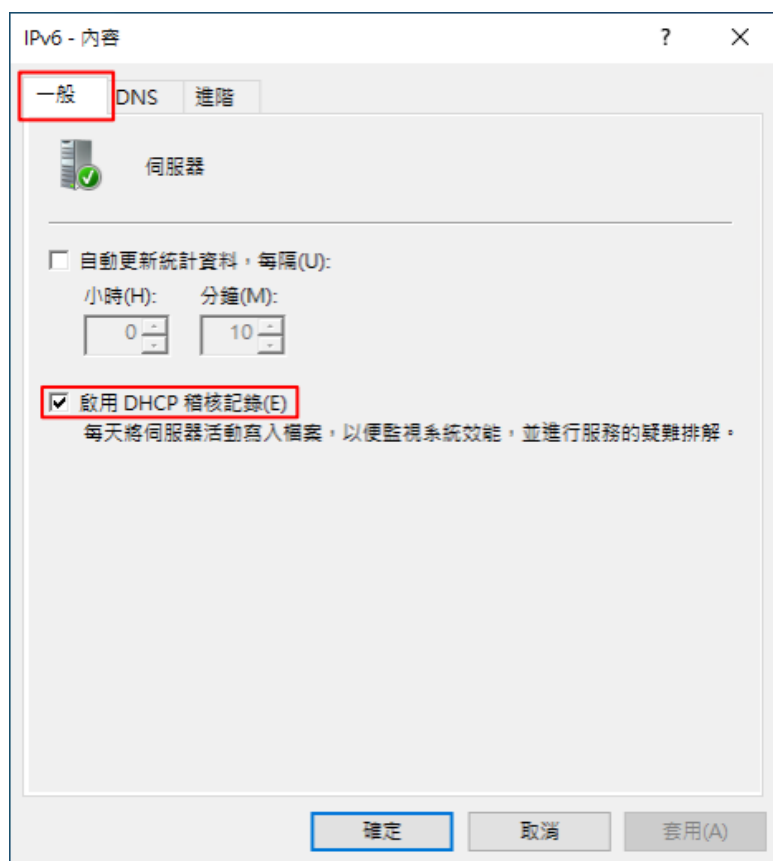


7.2 DHCP IPv6

(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]



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



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 7 web application interface. On the left is a dark sidebar menu with the following items: 'admin (Global)' (with a dropdown arrow), '事件' (Events), '報表' (Reports), '智慧分析' (Smart Analysis), 'Dashboard', '設備管理' (Device Management) - which is highlighted with a red box and has a checkmark, '設備資產樹狀圖' (Device Asset Tree) - also highlighted with a red box, '設備批次管理' (Device Batch Management), '設備細項設定' (Device Detailed Settings), '告警樣版' (Alert Template), '設備異常告警' (Device Abnormal Alert), '設備設定檔差異比對' (Device Configuration Profile Difference Comparison), '效能監控' (Performance Monitoring), '系統管理' (System Management), and '使用者手冊' (User Manual). The main content area shows the breadcrumb 'Home / 設備管理 / 設備資產樹狀圖'. Below this is a header for '設備資產樹狀圖' containing a search bar, a '重新輸入' (Re-enter) button, a '啟動查詢' (Start Query) button, and a '+' button (highlighted with a red box). The main content area shows a tree structure with 'Global (10/10)' selected and a sub-item '未知設備 (0/3)' (Unknown Device (0/3)).

(2) 選擇設備種類

選擇 [Application/DB/OS/Server]-> 點選 [引導模式]



8.1 Windows 2003 或之前版本作業系統

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows DHCP]-> 點選 [下一步]

新增設備 - 設備基本設定

設備基本設定

設備名稱 *

WinDHCP-192.168.2.159

IP *

192.168.2.159

所屬領域 *

Global

Syslog 資料格式 ⓘ

Windows DHCP

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

未啟用

Web 監控 ⓘ

☐ 啟用網頁監控功能

上一步 下一步 取消

(2) Syslog 相關設定

Facility 選擇 [(20) local use 4 (local4)] 和編碼方式: [BIG 5] -> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ

(20) local use 4 (local4)

編碼方式

BIG5

Syslog 正規化資料保留天數上限 ⓘ

Raw Data 保留與轉發

☒ Raw Data 保留

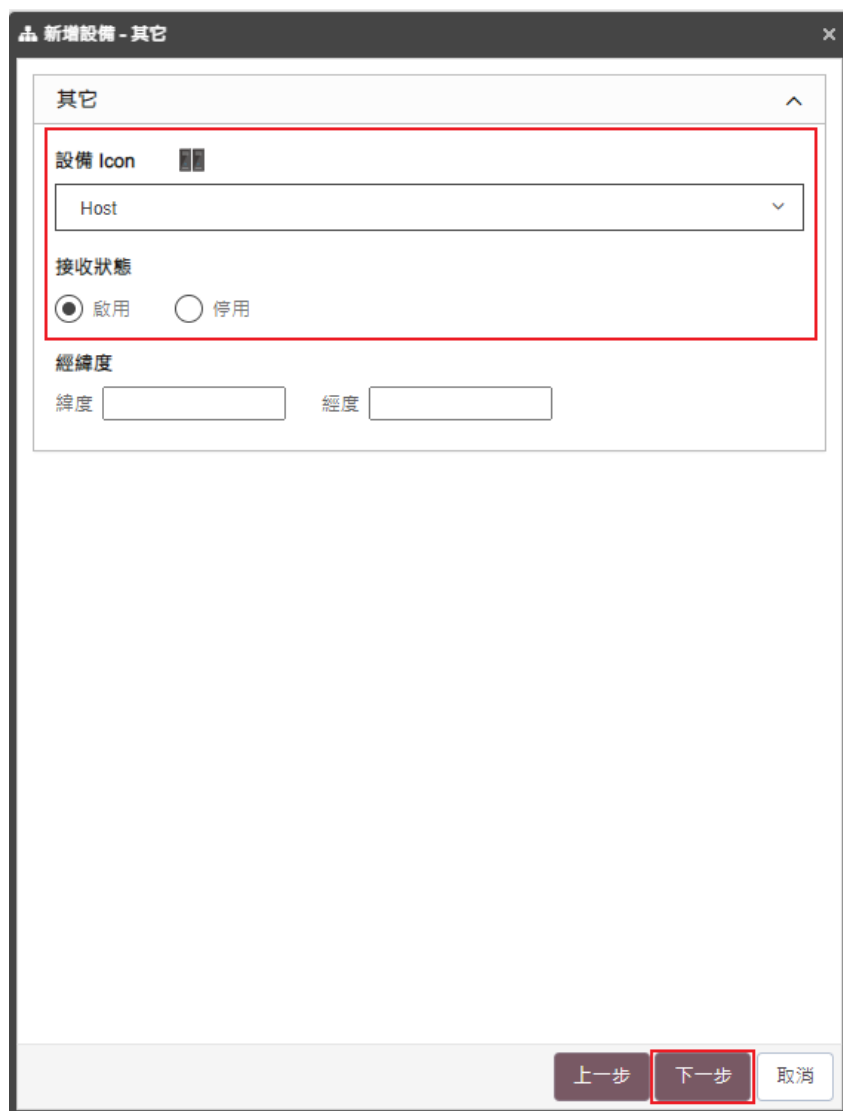
☐ 本設備於分時監控報表啟動 Syslog 轉發時，採用 Raw Data 格式

☐ 轉發方式將使用來源設備的 IP

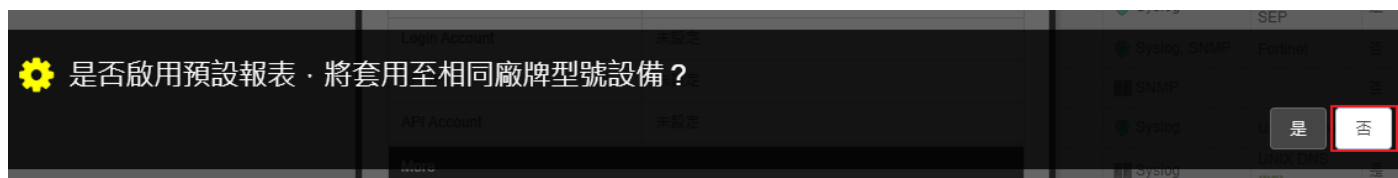
上一步 下一步 取消

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]



是否啟用預設報表，將套用至相同廠牌型號設備-> 點擊 [否]



8.2 Windows 2008 或之後版本作業系統

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows DHCP]-> 點選 [下一步]

新增設備 - 設備基本設定

設備基本設定

設備名稱 *

WinDHCP-192.168.2.159

IP *

192.168.2.159

所屬領域 *

Global

Syslog 資料格式 ⓘ

Windows DHCP

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

未啟用

Web 監控 ⓘ

☐ 啟用網頁監控功能

上一步 下一步 取消

(2) Syslog 相關設定

Facility 選擇 [(20) local use 4 (local4)] 和編碼方式: [UTF-8] -> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ

(20) local use 4 (local4)

編碼方式

UTF-8

Syslog 正規化資料保留天數上限 ⓘ

Raw Data 保留與轉發

☒ Raw Data 保留

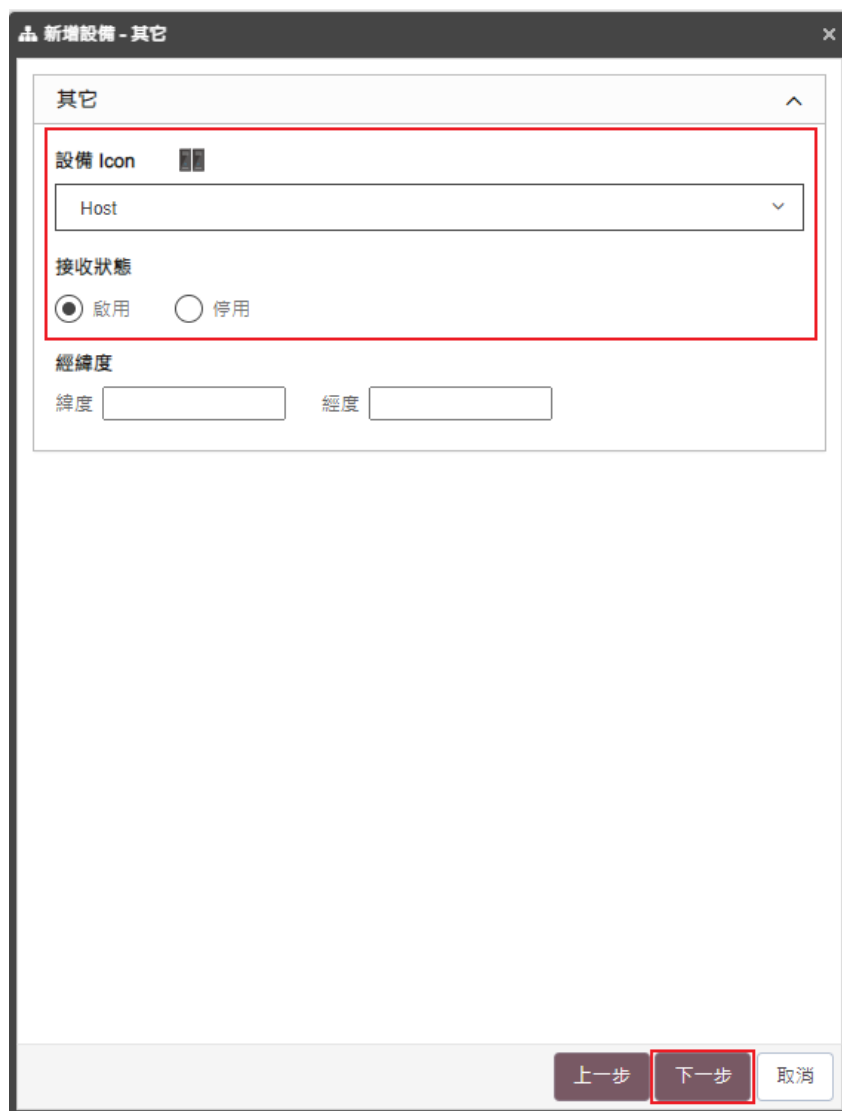
☐ 本設備於分時監控報表啟動 Syslog 轉發時，採用 Raw Data 格式

☐ 轉發方式將使用來源設備的 IP

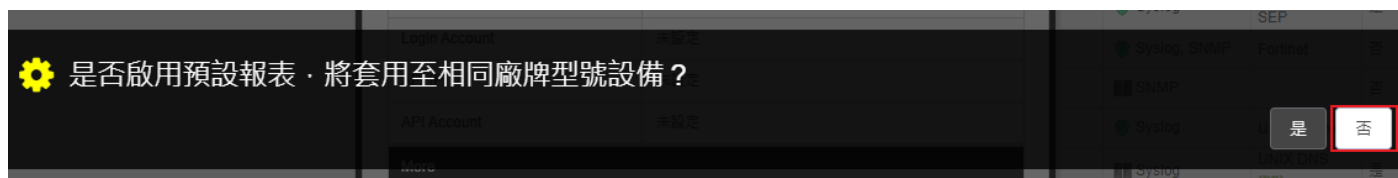
上一步 下一步 取消

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]



是否啟用預設報表，將套用至相同廠牌型號設備-> 點擊 [否]



9 問題排除

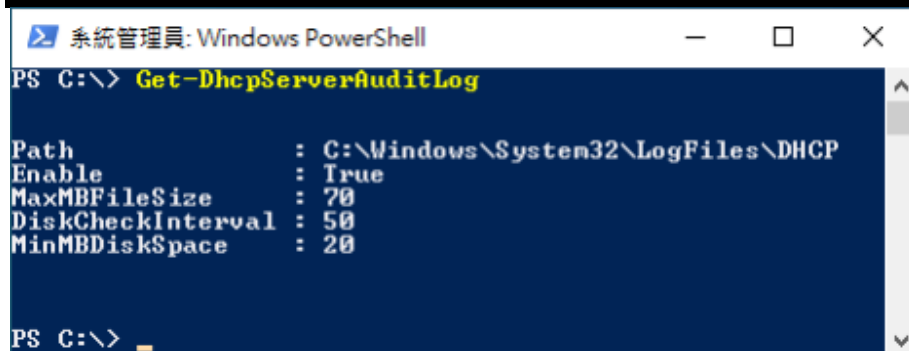
9.1 調整 DHCP 記錄檔案大小

(1) 開啟 [Windows PowerShell]



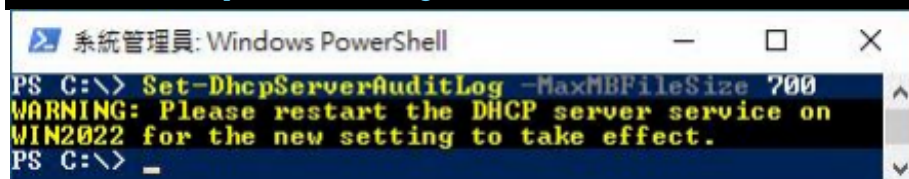
(2) 查看 DHCP Server 稽核 Log 設定

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



(3) 設定 DHCP Log 檔案大小

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



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

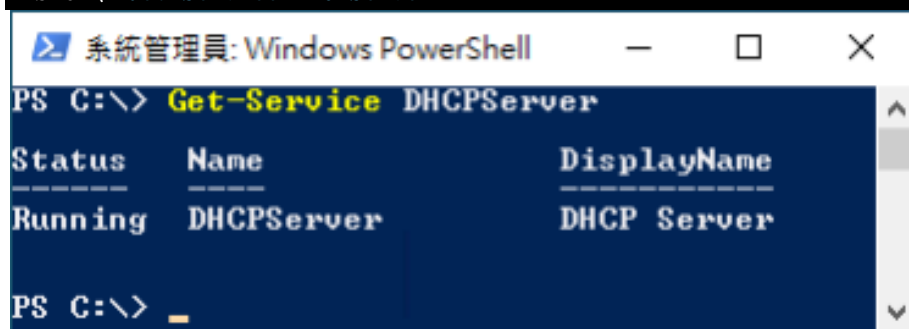
(4) 重啟 DHCP Server 服務

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



(5) 查看 DHCP Server 服務

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

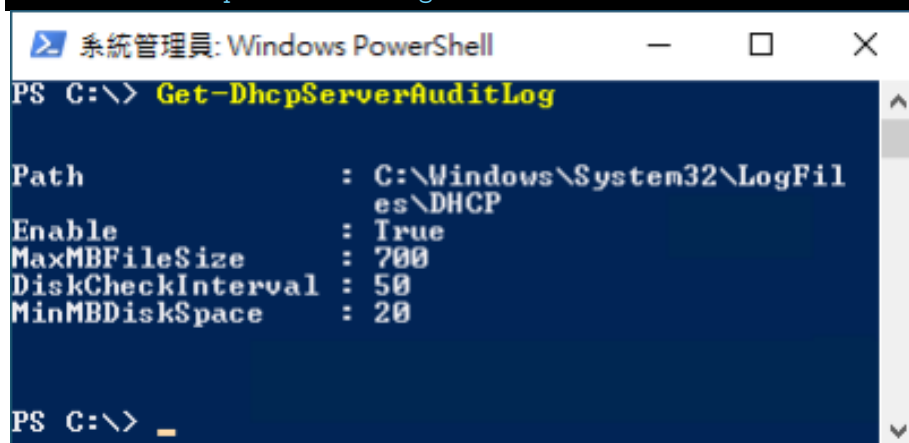


The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command `Get-Service DHCPServer` has been executed. The output is a table with three columns: Status, Name, and DisplayName. The status is "Running", the name is "DHCPServer", and the display name is "DHCP Server".

Status	Name	DisplayName
Running	DHCPServer	DHCP Server

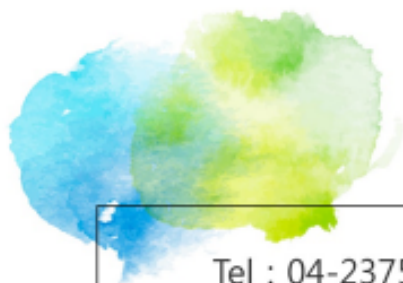
(6) 查看 DHCP Server 稽核 Log 設定

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



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command `Get-DhcpServerAuditLog` has been executed. The output shows the following settings:

- Path : C:\Windows\System32\LogFiles\DHCP
- Enable : True
- MaxMBFileSize : 700
- DiskCheckInterval : 50
- MinMBDiskSpace : 20



Tel : 04-23752865 Fax : 04-23757458

業務詢問 : sales@npartner.com

技術詢問 : support@npartner.com