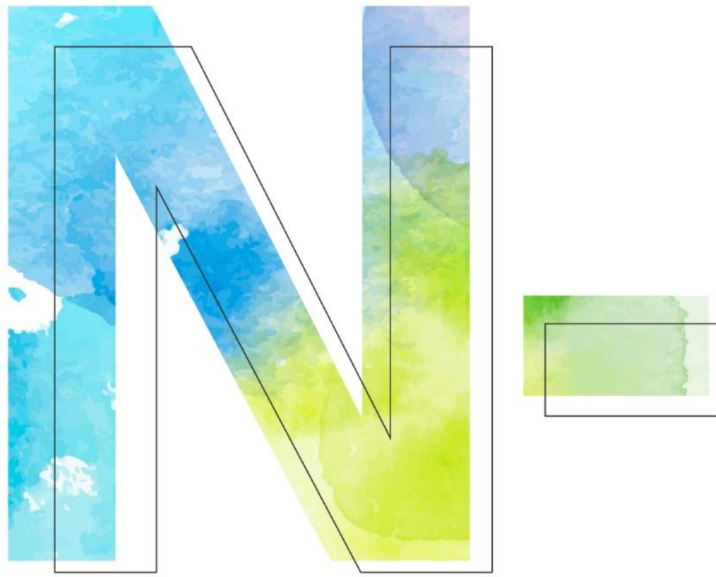




Partner

如何設定 Windows DNS log

V009

2024/07/11



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
1.3 NXLog 設定檔	7
1.4 NXLog 啟動服務	8
2 Windows 2008	11
3 Windows 2012	15
4 Windows 2016	19
5 Windows 2019	23
6 Windows 2022	27
7 N-Reporter	31

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 DNS 記錄。

NXLog 工具將 Windows DNS 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 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

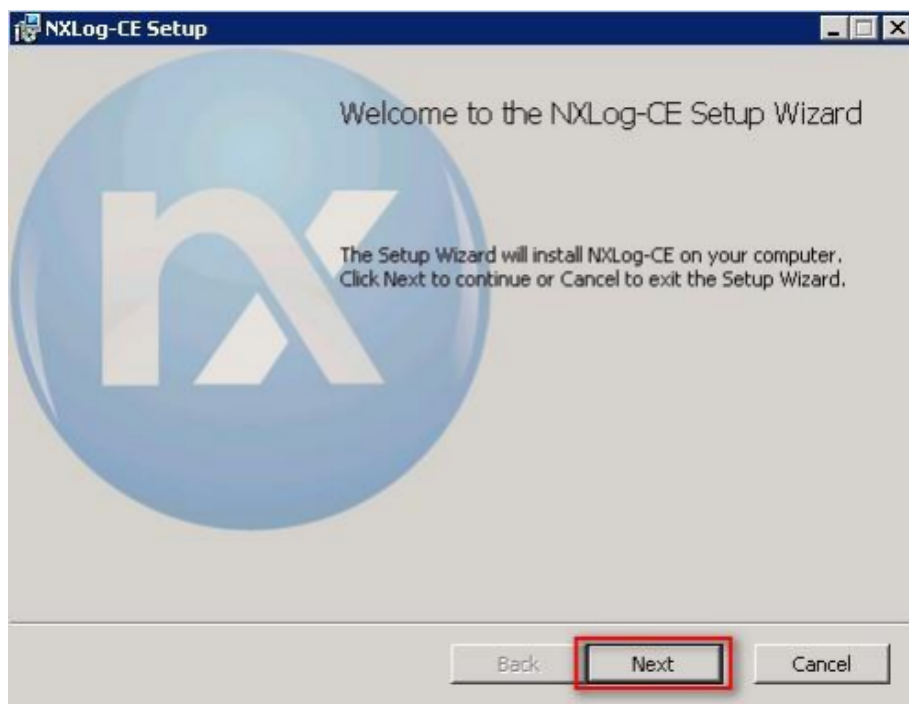


註：若需要下載 NXLog 32bit 版本，請與我們連繫。

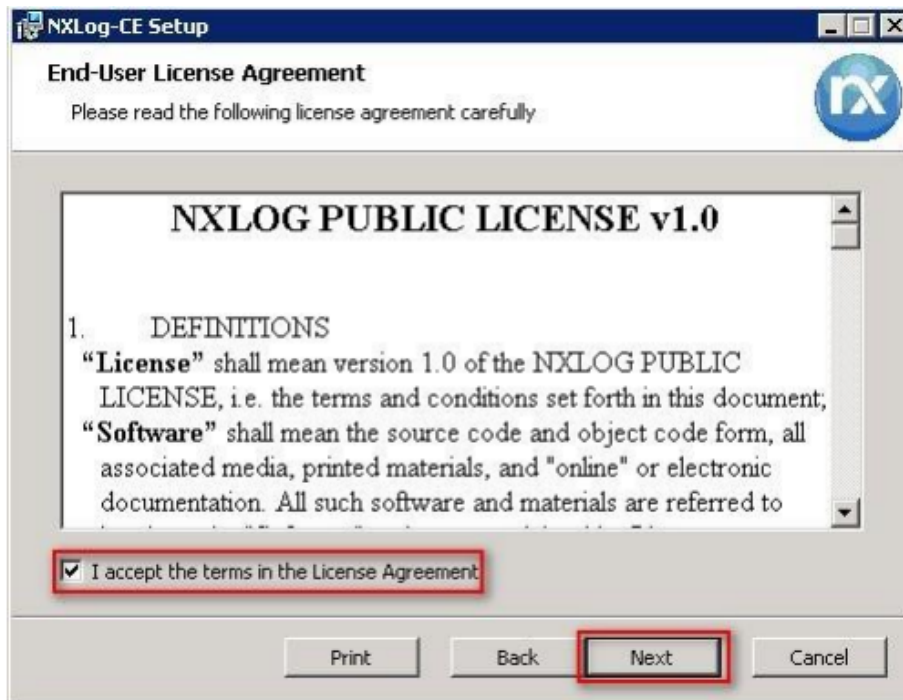
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

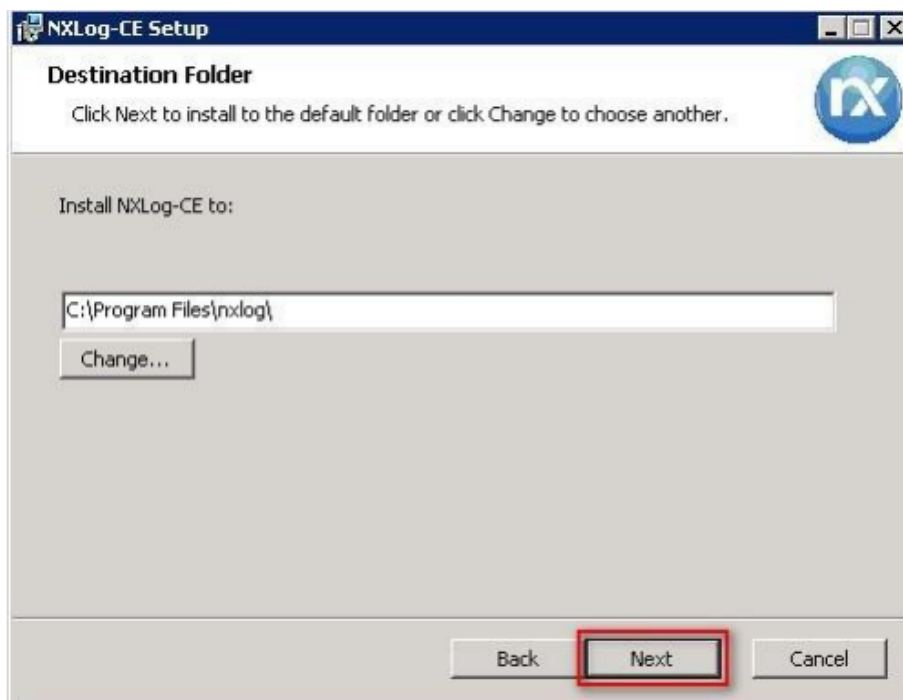
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next] .



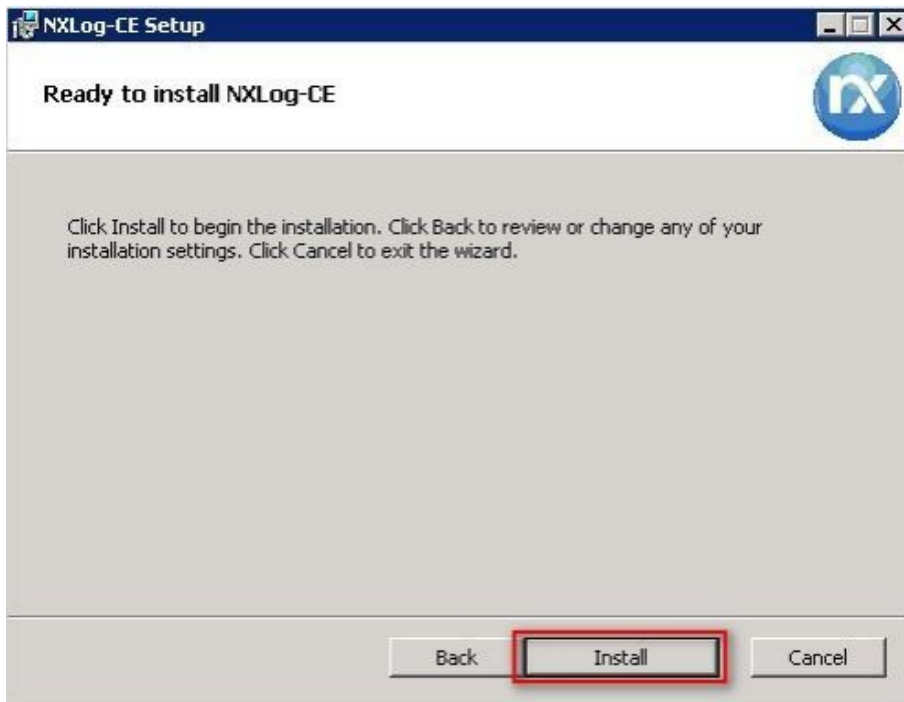
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



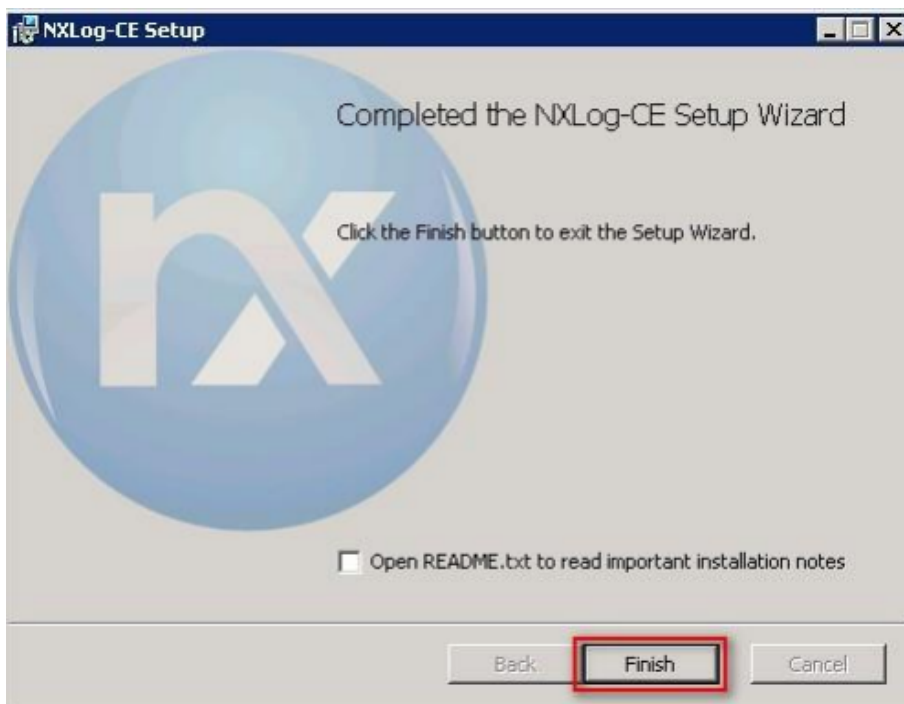
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].

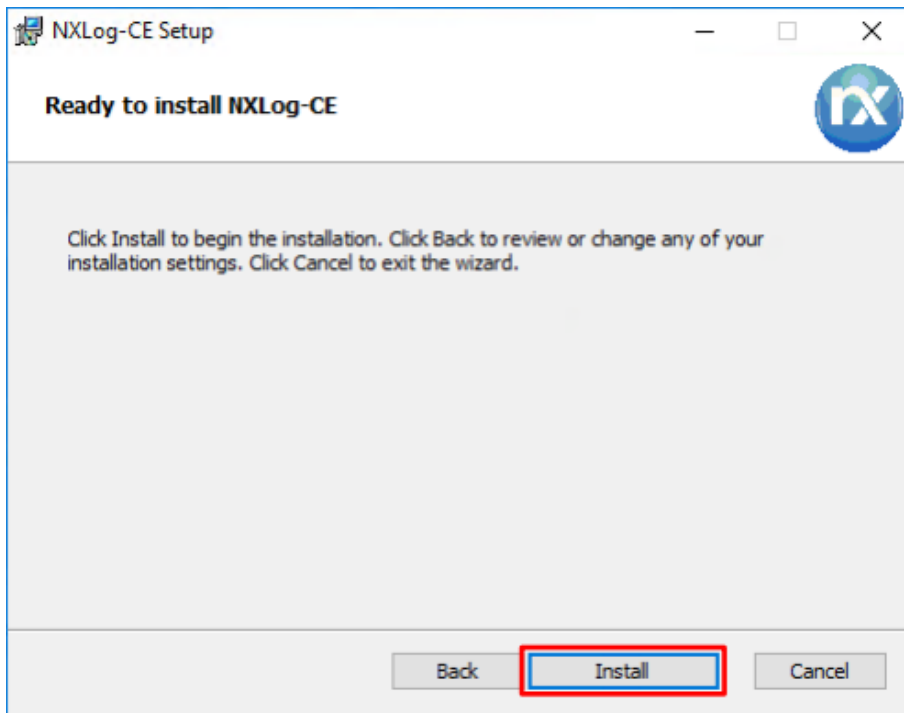


-> 按 [Finish].



<2.2> Windows 2003

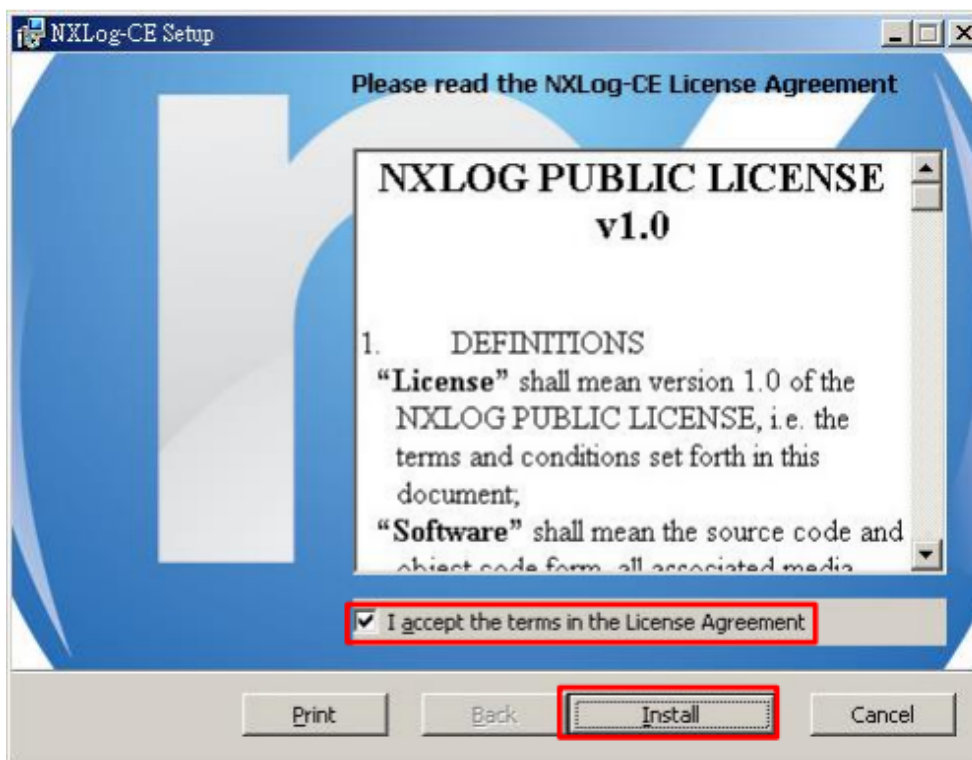
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].



<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) 開啟 [Windows PowerShell]



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

下載連結：http://www.npartnertech.com/download/tech/nxlog_WinDNS.conf

```
PS C:\> Invoke-WebRequest -Uri`http://www.npartnertech.com/download/tech/nxlog_WinDNS.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 DnsPath C:\Windows\System32\LogFiles\DNS
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 DNS log file use the following:
<Input in_dnslog>
    Module im_file
    File '%DnsPath%\dns.log'
    SavePos TRUE
    ReadFromLast TRUE
</Input>

<Output out_dnslog>
    Module om_udp
    Host %NCloud%
    Port 514
    Exec $SyslogFacilityValue = 19;
    Exec if $raw_event =~ /\d+\d+\d+\s(上午\s)(\d+:\d+:\d+\s)(.+)/ $raw_event = $1 + ' ' + $3 + 'AM ' + $4;
    Exec if $raw_event =~ /\d+\d+\d+\s(下午\s)(\d+:\d+:\d+\s)(.+)/ $raw_event = $1 + ' ' + $3 + 'PM ' + $4;
    Exec $raw_event = "WinDNS [Info]: " + $raw_event ;
    Exec to_syslog_bsd();
</Output>

<Route dnslog>
    Path in_dnslog => out_dnslog
</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 DnsPath C:\Windows\Sysnative\LogFiles\DNS
```

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。



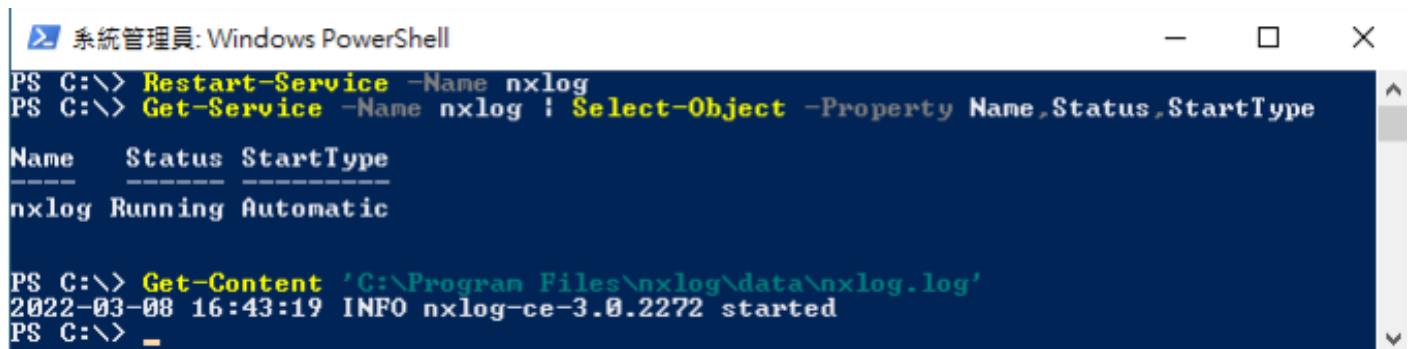
1.4 NXLog 啟動服務

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

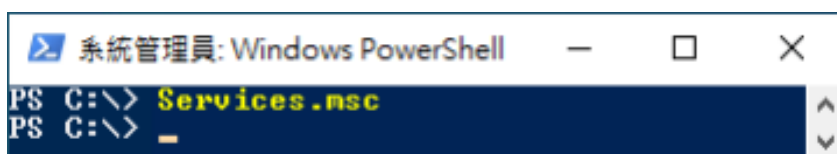
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
Name      Status StartType
-----
nxlog     Running Automatic

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'`

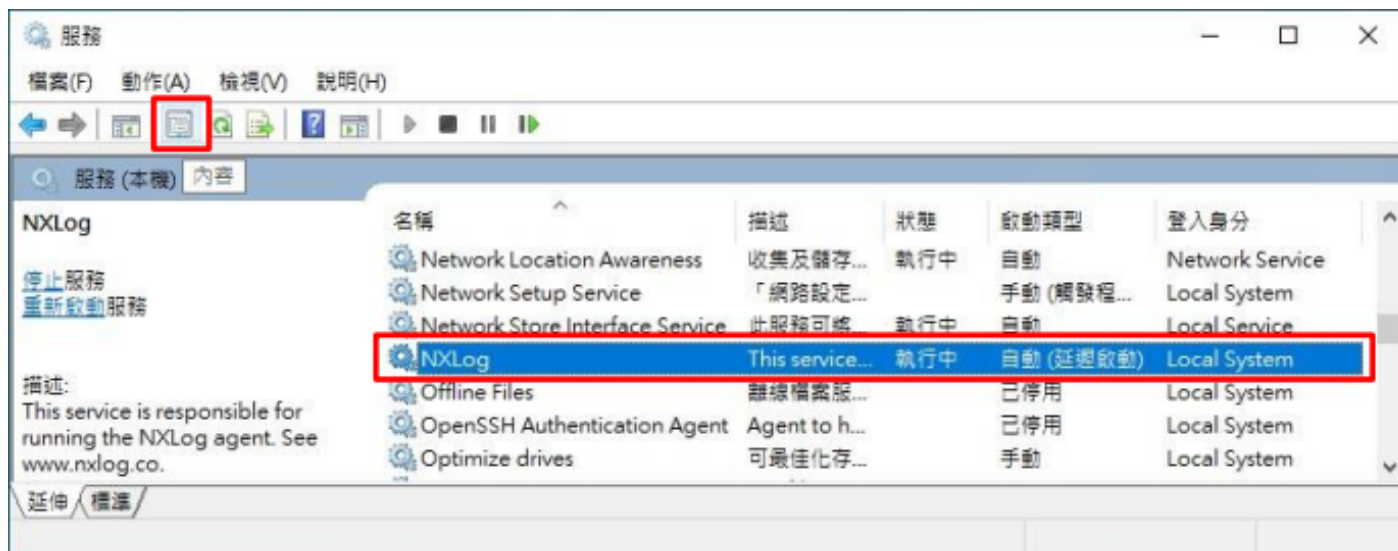
(3) 開啟 [服務] 功能

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

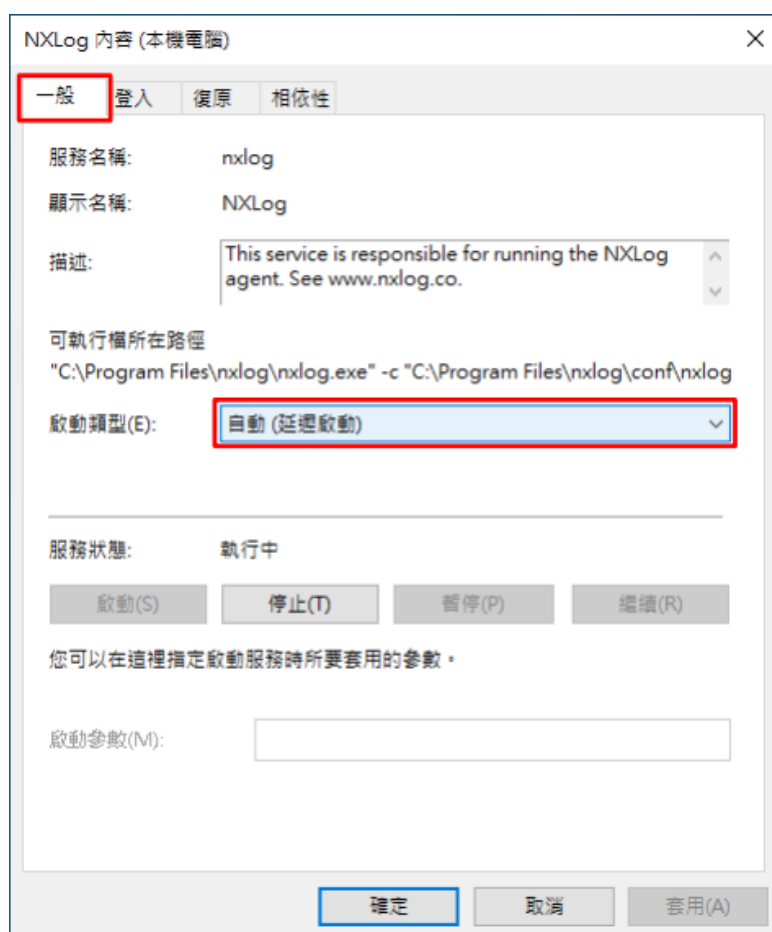


(4) 開啟 NXLog 服務內容

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

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)

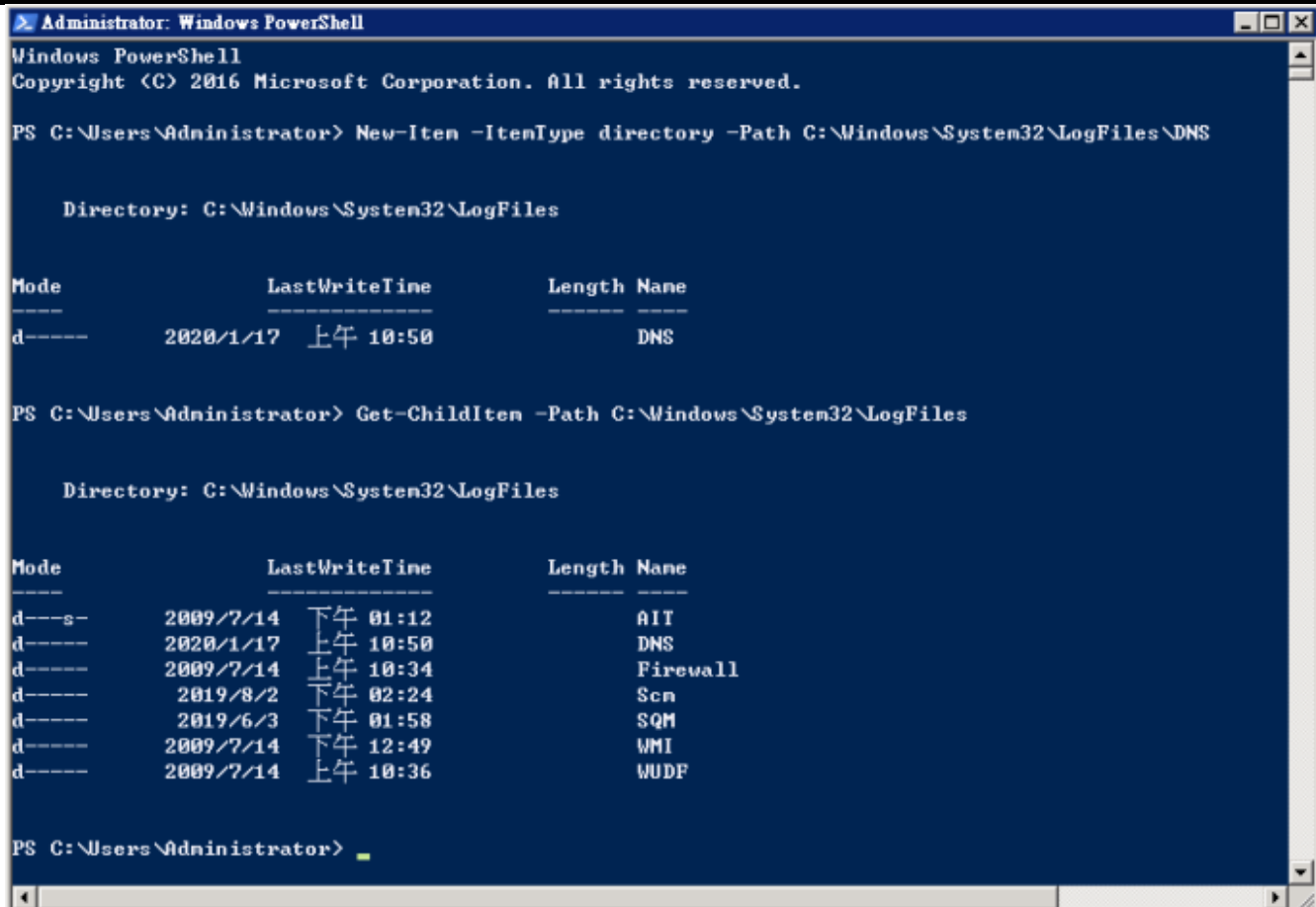
2 Windows 2008

(1) 開啟 [Windows PowerShell]



(2) 新增 DNS log 資料夾

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell". The window shows the execution of two commands. The first command, "New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS", successfully creates a new directory named "DNS". The second command, "Get-ChildItem -Path C:\Windows\System32\LogFiles", lists the contents of the "LogFiles" directory, showing a table of files and directories including "AIT", "DNS", "Firewall", "Scn", "SQM", "WMI", and "WUDF".

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----         2020/1/17 上午 10:50             DNS

PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

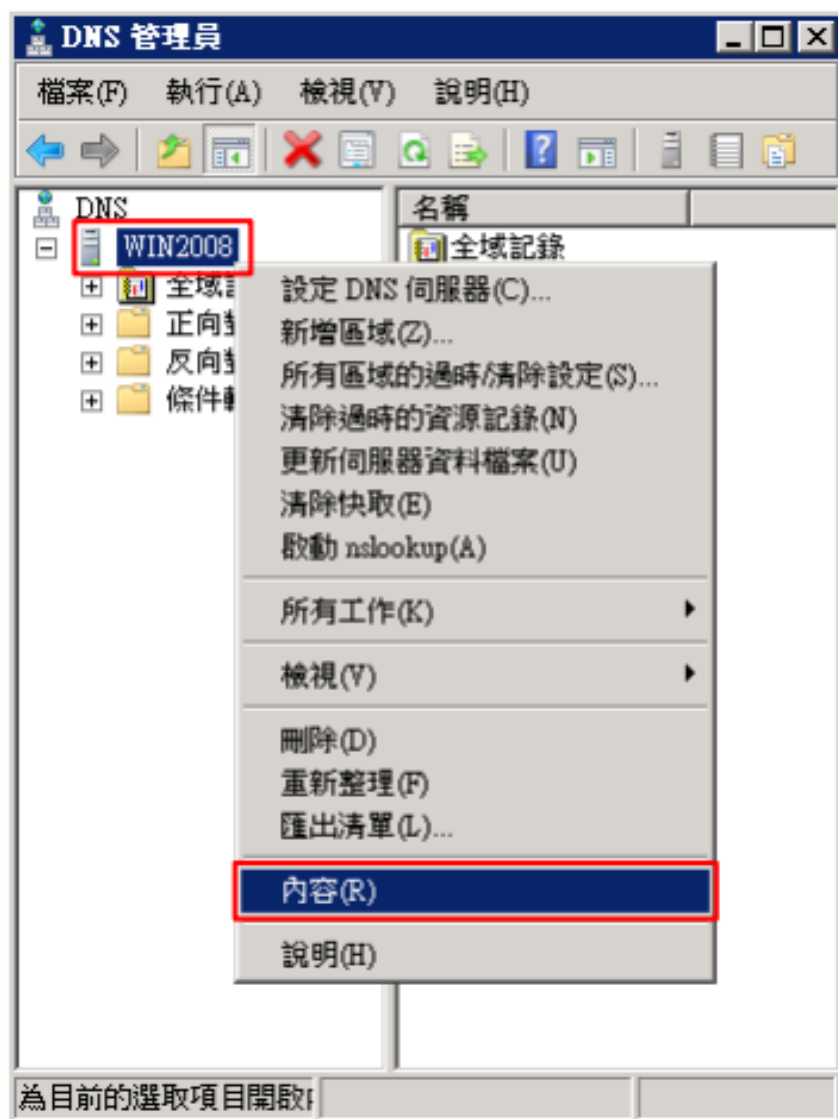
Mode                LastWriteTime         Length Name
----                -
d---s-         2009/7/14 下午 01:12             AIT
d-----         2020/1/17 上午 10:50             DNS
d-----         2009/7/14 上午 10:34          Firewall
d-----         2019/8/2 下午 02:24              Scn
d-----         2019/6/3 下午 01:58              SQM
d-----         2009/7/14 下午 12:49              WMI
d-----         2009/7/14 上午 10:36             WUDF

PS C:\Users\Administrator>
```

(3) 開啟 DNS

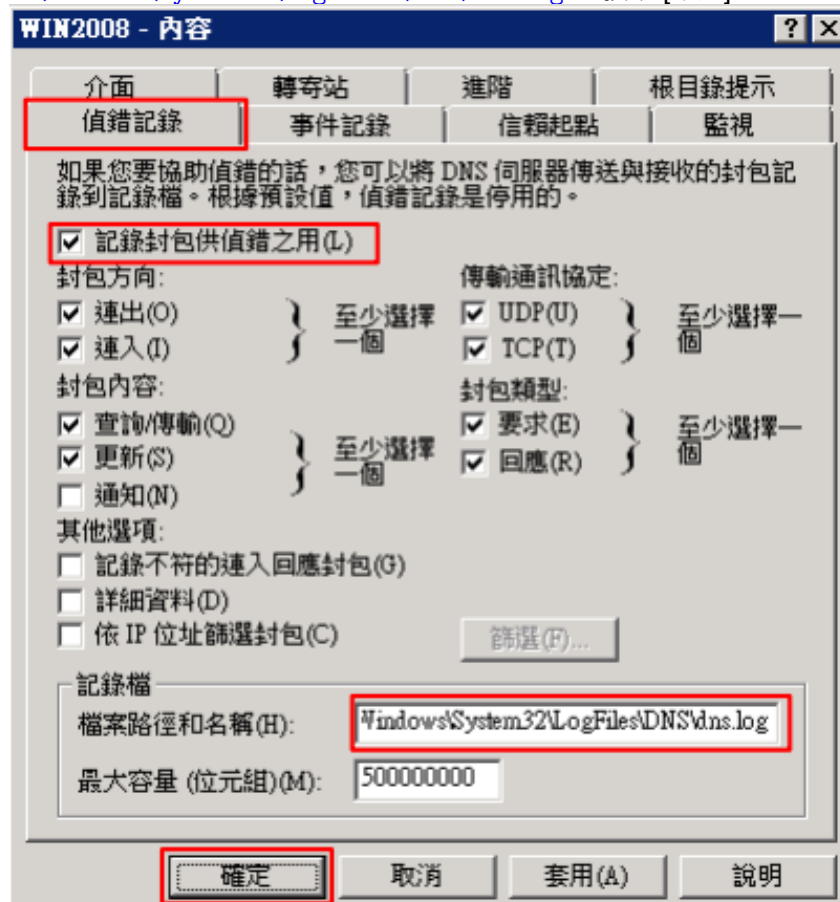


(4) 在 DNS 伺服器 [Win2008] 按滑鼠右鍵 -> 點選 [內容]



(5) [偵錯記錄] 頁面 -> 勾選 [記錄封包供偵錯之用] -> 輸入檔案路徑和名稱

C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]

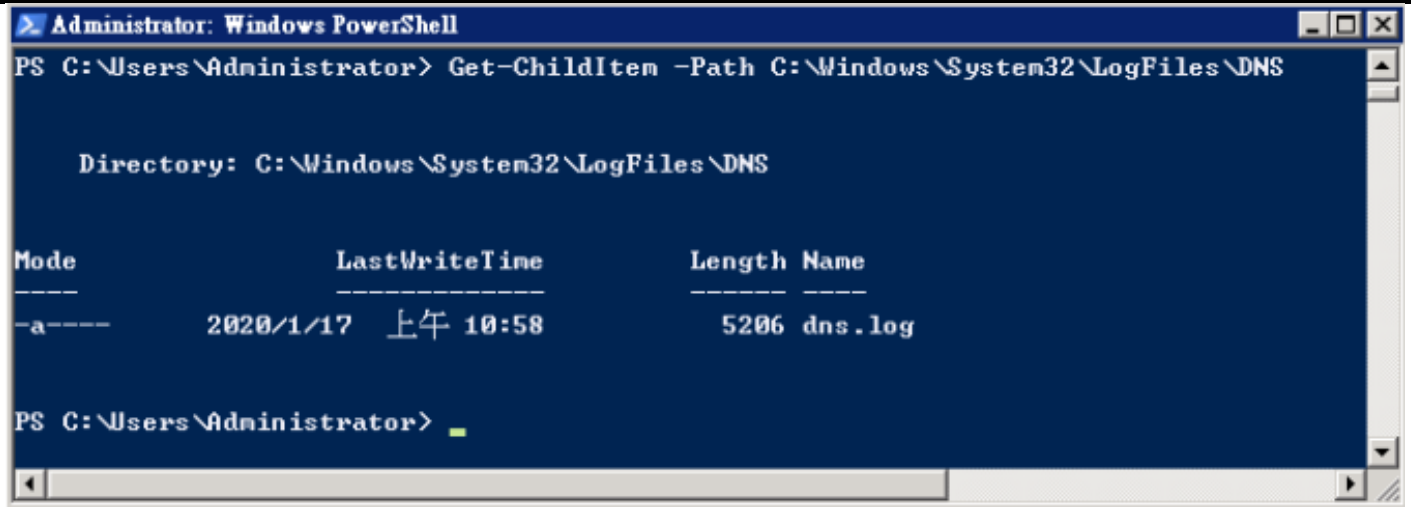


(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command executed is `Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS`. The output displays the directory path and a table of files.

```
Directory: C:\Windows\System32\LogFiles\DNS
```

Mode	LastWriteTime	Length	Name
-a----	2020/1/17 上午 10:58	5206	dns.log

The command prompt shows the user is still in the `C:\Users\Administrator` directory.

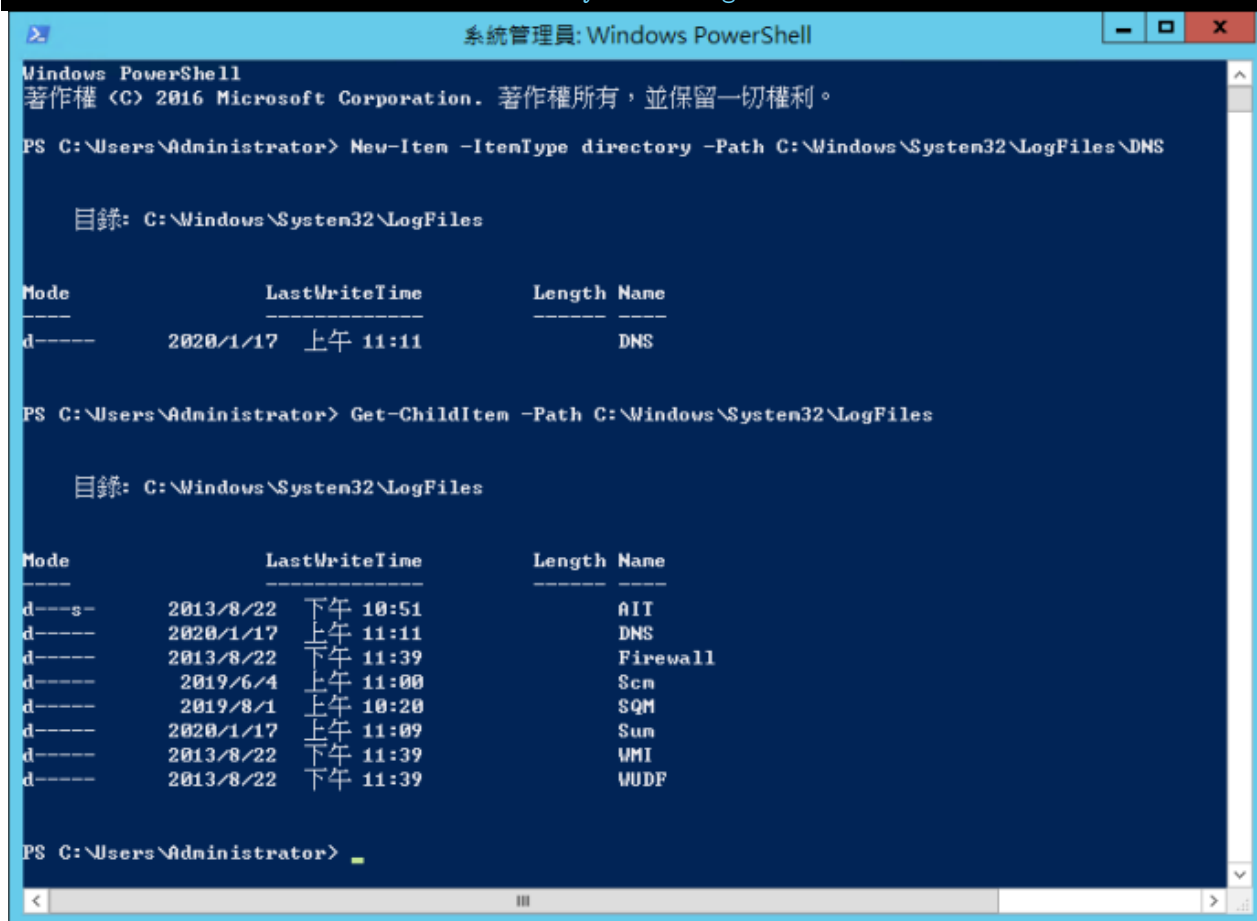
3 Windows 2012

(1) 開啟 [Windows PowerShell]



(2) 新增 DNS log 資料夾

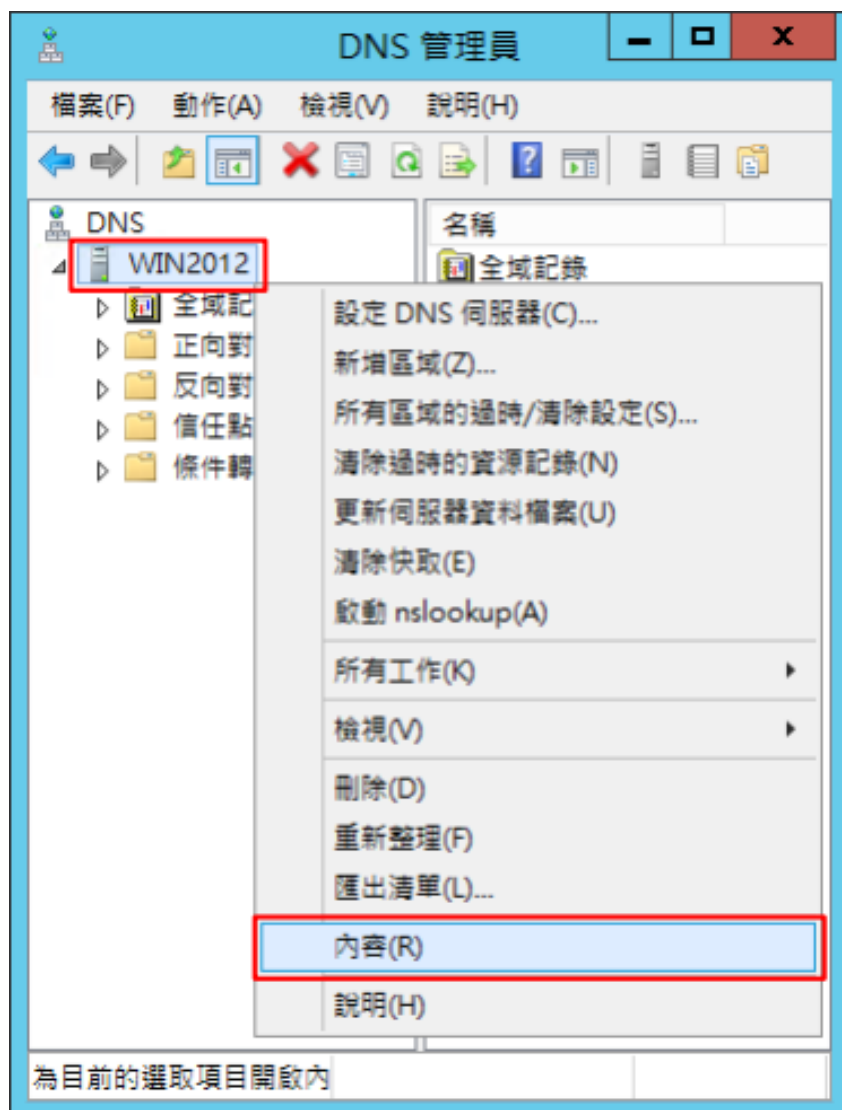
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 DNS

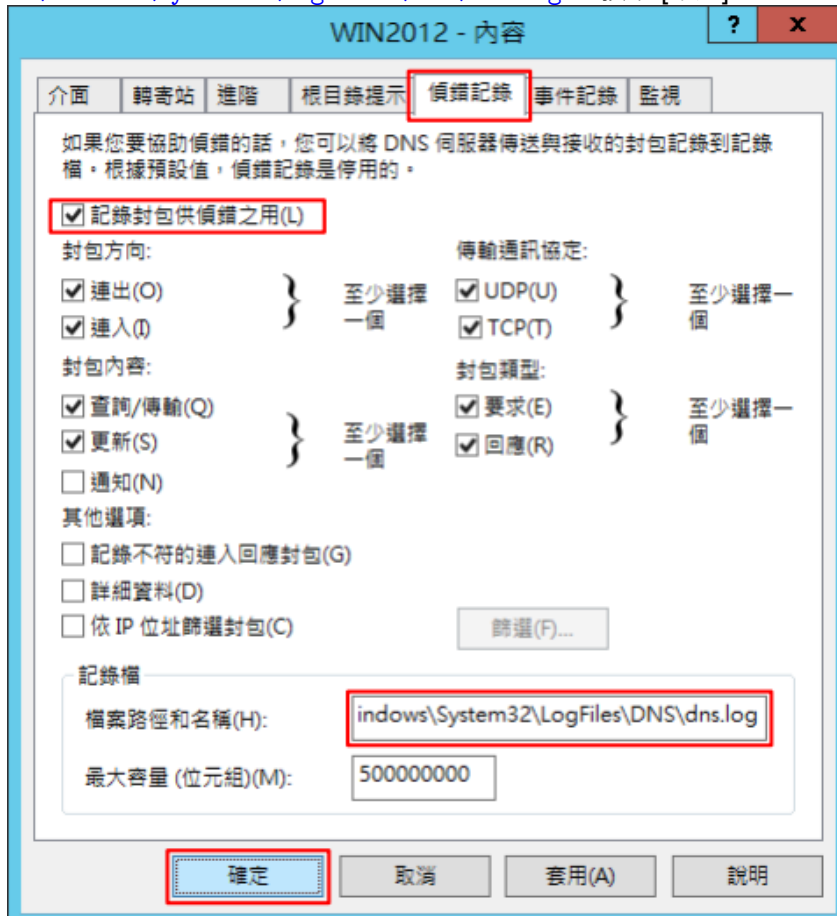


(4) 在 DNS 伺服器 [Win2012] 按滑鼠右鍵 -> 點選 [內容]



(5) [偵錯記錄] 頁面 -> 勾選 [記錄封包供偵錯之用] -> 輸入檔案路徑和名稱

C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```



系統管理員: Windows PowerShell

```
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

目錄: C:\Windows\System32\LogFiles\DNS

Mode	LastWriteTime	Length	Name
-a----	2020/1/17 上午 11:17	12686	dns.log

```
PS C:\Users\Administrator>
```

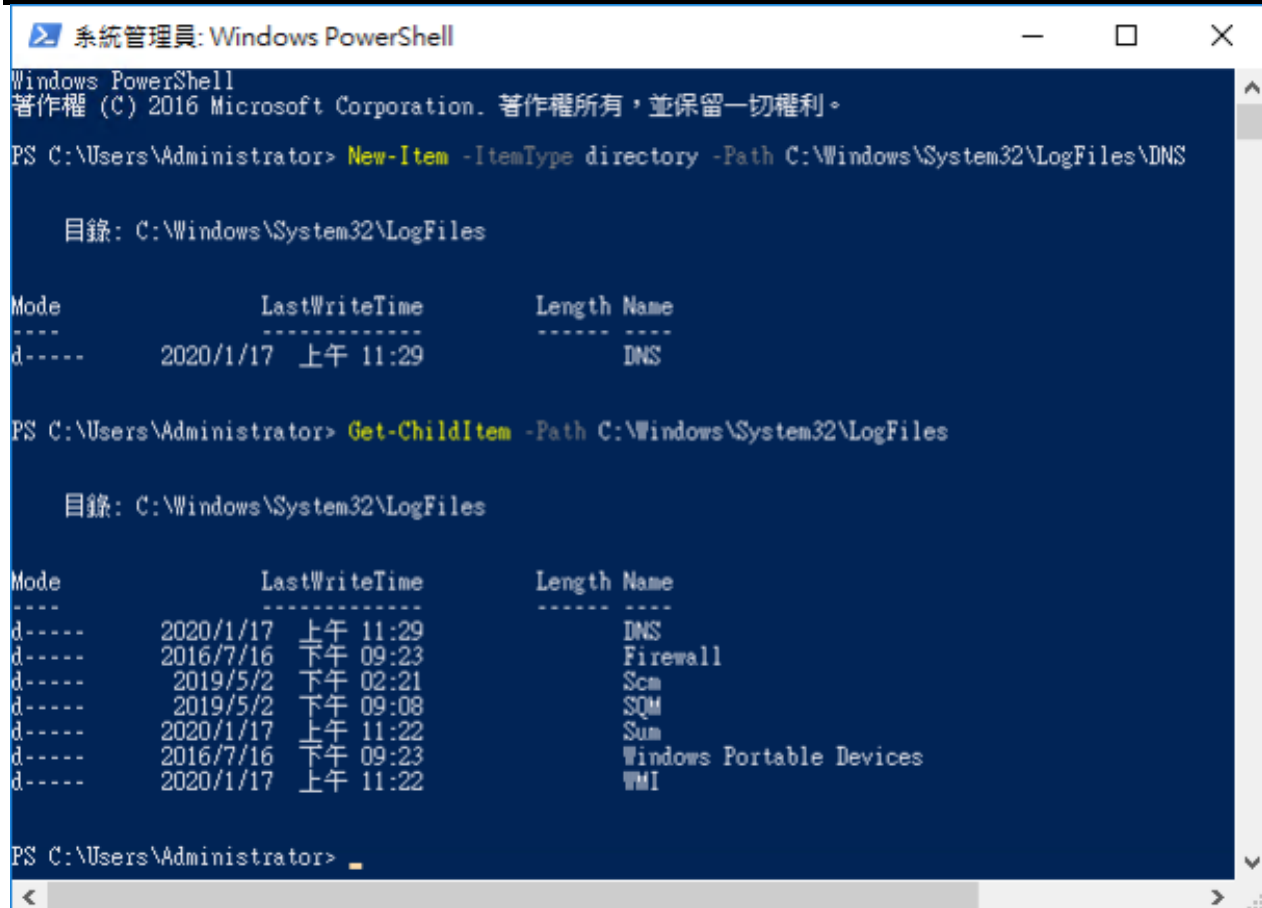
4 Windows 2016

(1) 開啟 [Windows PowerShell]



(2) 新增 DNS log 資料夾

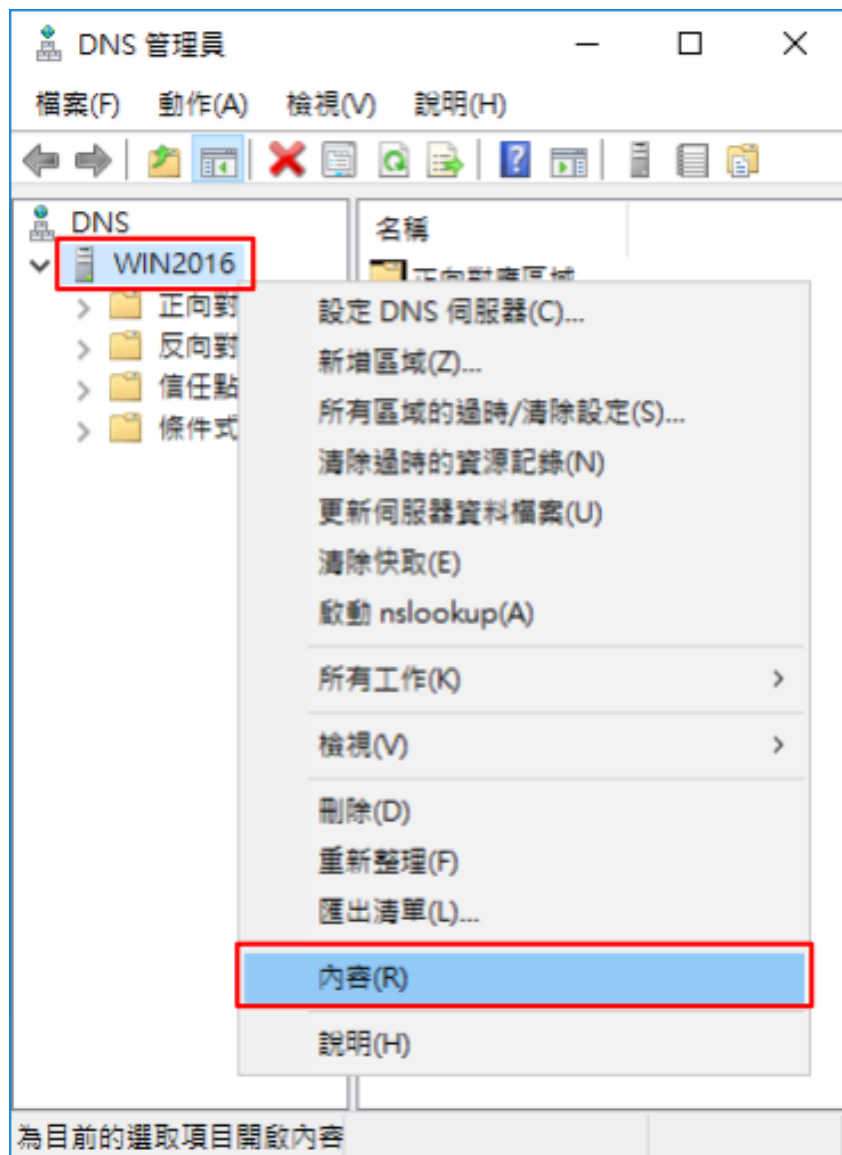
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 DNS



(4) 在 DNS 伺服器 [Win2016] 按滑鼠右鍵 -> 點選 [內容]



(5) [偵錯記錄] 頁面 -> 勾選 [記錄封包供偵錯之用] -> 輸入檔案路徑和名稱

C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]

WIN2016 - 內容

介面 轉寄站 進階 根目錄提示 偵錯記錄 事件記錄 監視

如果您要協助偵錯的話，您可以將 DNS 伺服器傳送與接收的封包記錄到記錄檔。根據預設值，偵錯記錄是停用的。

☒ 記錄封包供偵錯之用(L)

封包方向:

☒ 連出(O) } 至少選擇一個

☒ 連入(I) }

封包內容:

☒ 查詢/傳輸(Q) } 至少選擇一個

☒ 更新(S) }

☐ 通知(N)

其他選項:

☐ 記錄不符的連入回應封包(G)

☐ 詳細資料(D)

☐ 依 IP 位址篩選封包(C) 篩選(F)...

傳輸通訊協定:

☒ UDP(U) } 至少選擇一個

☒ TCP(T) }

封包類型:

☒ 要求(E) } 至少選擇一個

☒ 回應(R) }

記錄檔

檔案路徑和名稱(H): indows\System32\LogFiles\DNS\dns.log

最大容量 (位元組)(M): 500000000

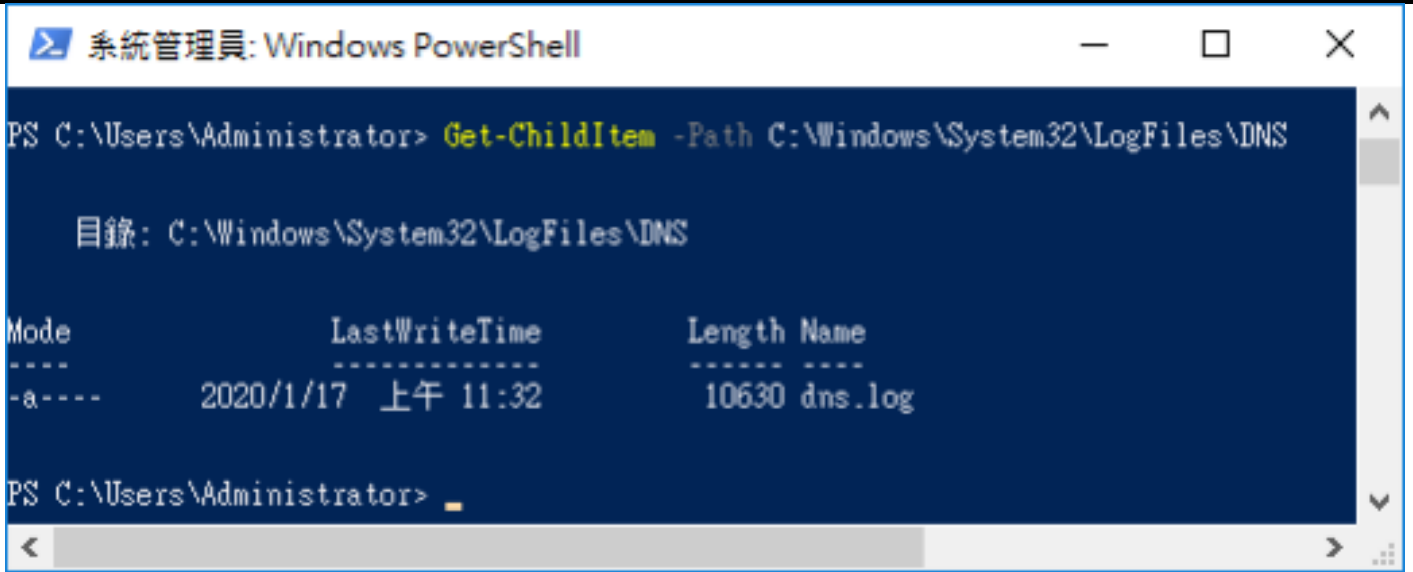
確定 取消 套用(A) 說明

(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```



系統管理員: Windows PowerShell

```
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

目錄: C:\Windows\System32\LogFiles\DNS

Mode	LastWriteTime	Length	Name
-a----	2020/1/17 上午 11:32	10630	dns.log

```
PS C:\Users\Administrator> _
```

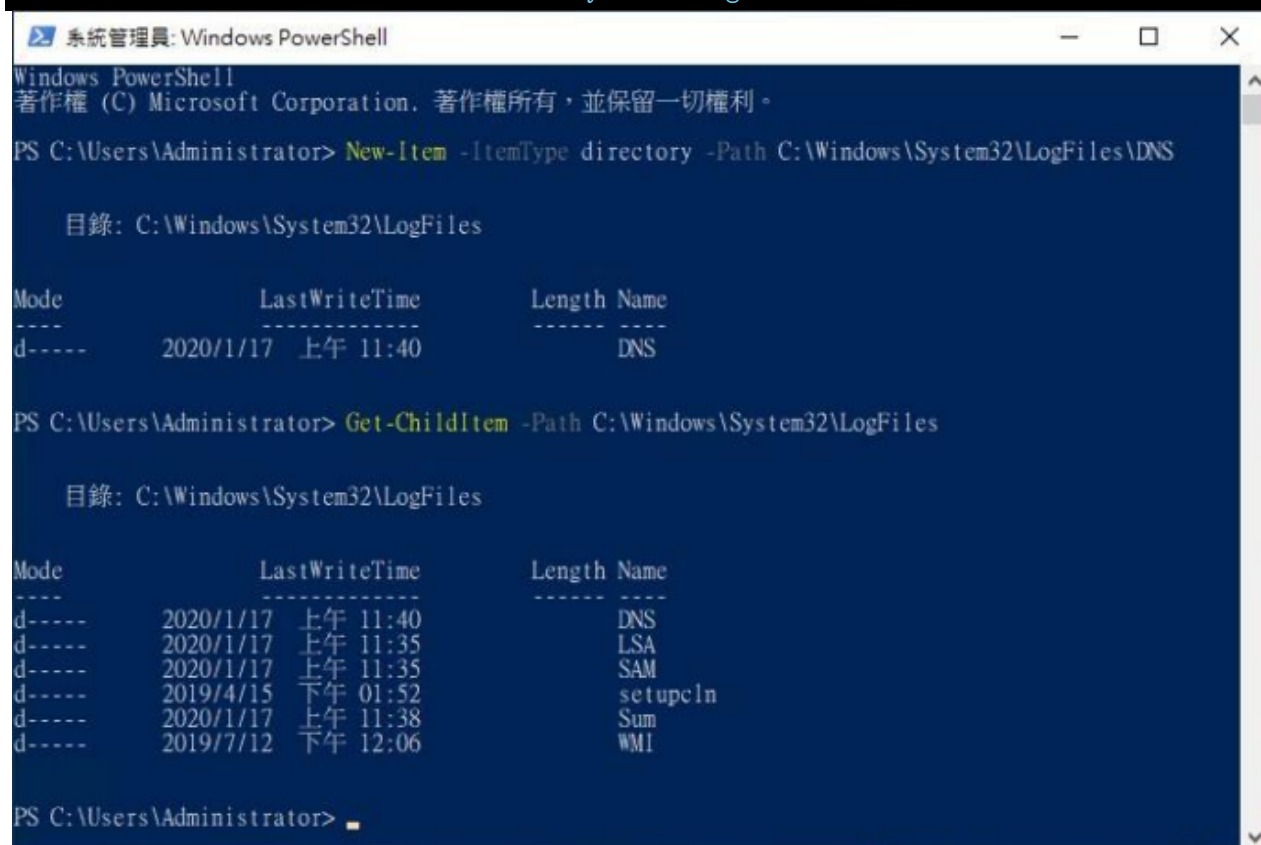
5 Windows 2019

(1) 開啟 [Windows PowerShell]



(2) 新增 DNS log 資料夾

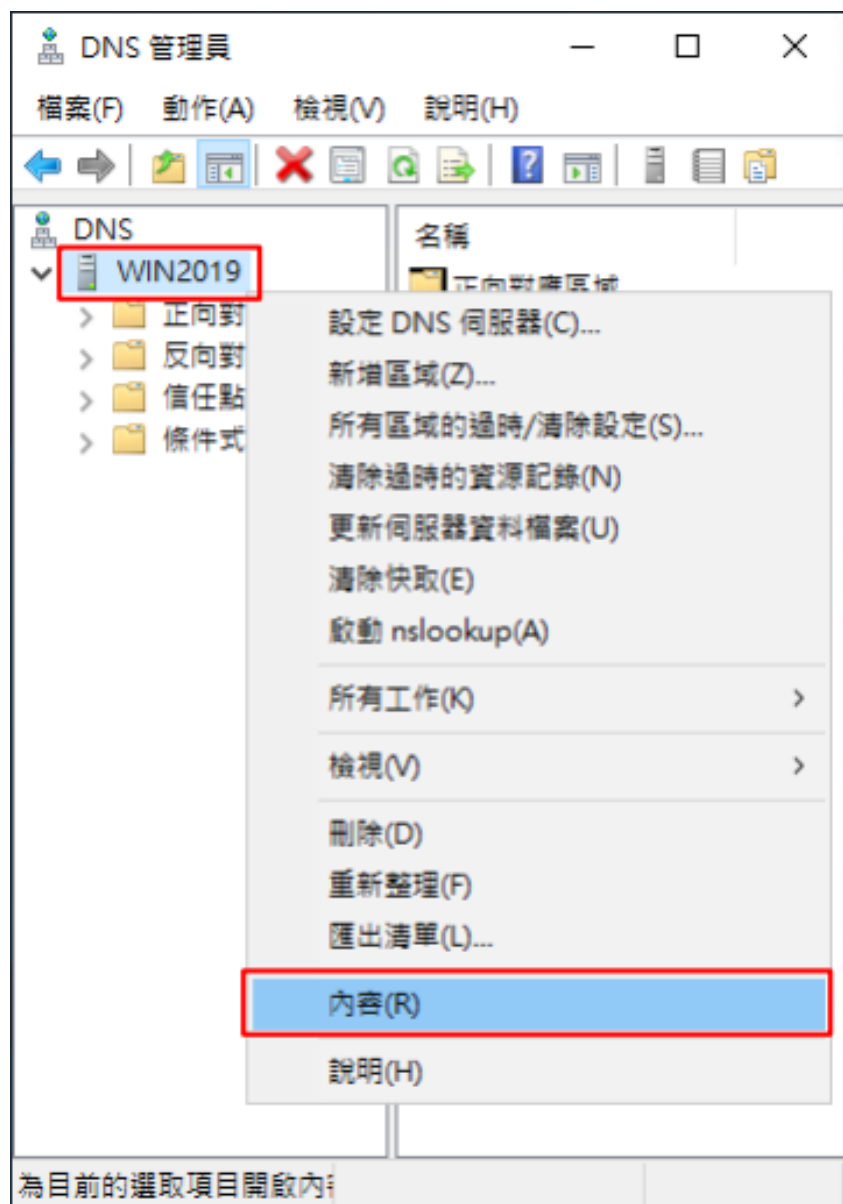
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 DNS



(4) 在 DNS 伺服器 [Win2019] 按滑鼠右鍵 -> 點選 [內容]



(5) [偵錯記錄] 頁面 -> 勾選 [記錄封包供偵錯之用] -> 輸入檔案路徑和名稱

C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]

WIN2019 - 內容

介面 轉寄站 進階 根目錄提示 偵錯記錄 事件記錄 監視

如果您要協助偵錯的話，您可以將 DNS 伺服器傳送與接收的封包記錄到記錄檔。根據預設值，偵錯記錄是停用的。

☒ 記錄封包供偵錯之用(L)

封包方向:

☒ 連出(O) } 至少選擇一個

☒ 連入(I) }

封包內容:

☒ 查詢/傳輸(Q) } 至少選擇一個

☒ 更新(S) }

☐ 通知(N)

其他選項:

☐ 記錄不符的連入回應封包(G)

☐ 詳細資料(D)

☐ 依 IP 位址篩選封包(C)

篩選(F)...

傳輸通訊協定:

☒ UDP(U) } 至少選擇一個

☒ TCP(T) }

封包類型:

☒ 要求(E) } 至少選擇一個

☒ 回應(R) }

記錄檔

檔案路徑和名稱(H): indows\System32\LogFiles\DNS\dns.log

最大容量 (位元組)(M): 500000000

確定 取消 套用(A) 說明

(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

系統管理員: Windows PowerShell

```
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

目錄: C:\Windows\System32\LogFiles\DNS

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	2020/1/17 上午 11:46	70638	dns.log

```
PS C:\Users\Administrator> █
```

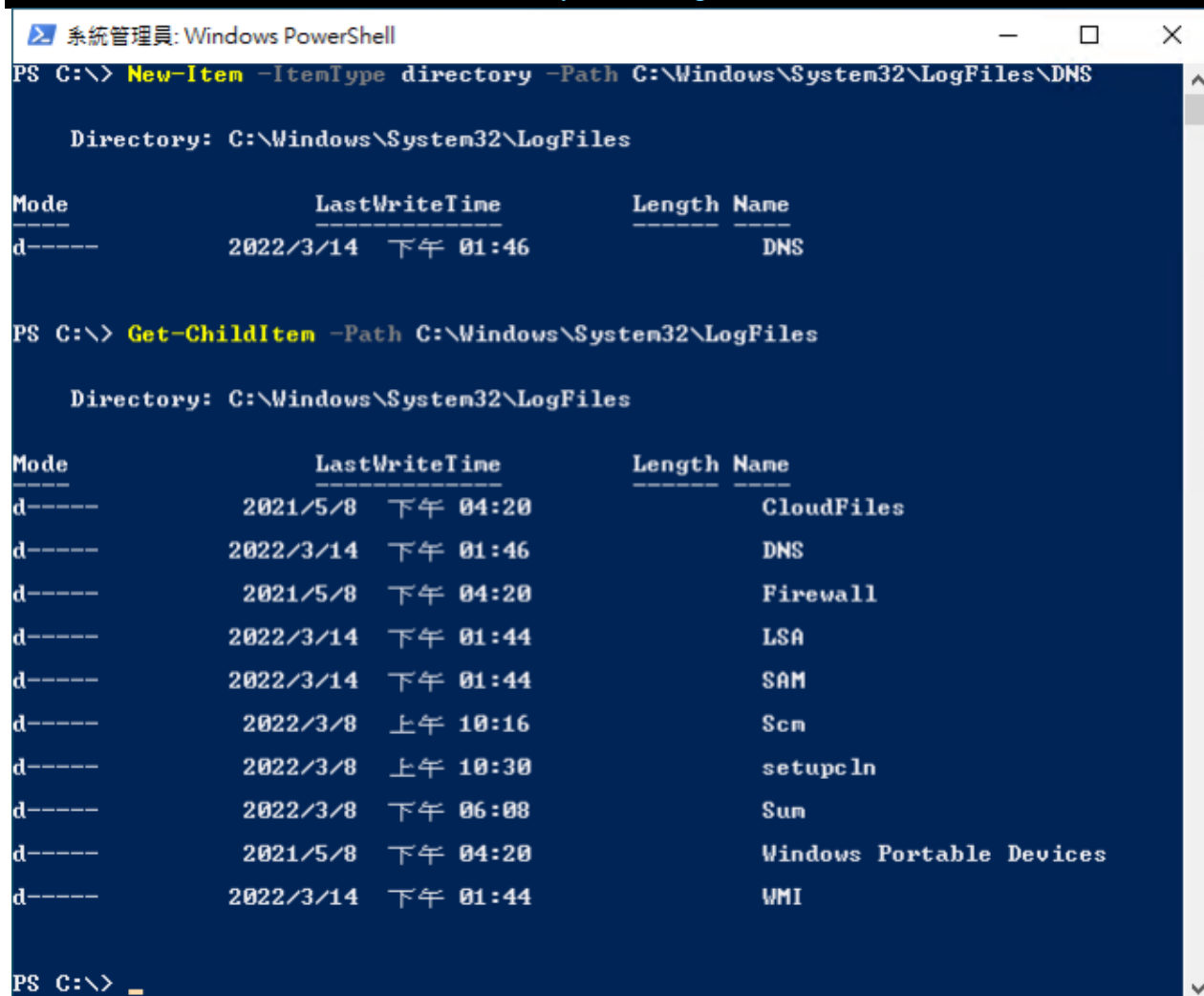
6 Windows 2022

(1) 開啟 [Windows PowerShell]



(2) 新增 DNS log 資料夾

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command prompt shows the execution of two commands. The first command, "New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS", creates a new directory named "DNS" in the "C:\Windows\System32\LogFiles" path. The second command, "Get-ChildItem -Path C:\Windows\System32\LogFiles", lists the contents of the "C:\Windows\System32\LogFiles" directory. The output shows a table of files and directories, including "CloudFiles", "DNS", "Firewall", "LSA", "SAM", "Scm", "setupcln", "Sun", "Windows Portable Devices", and "WMI".

```
系統管理員: Windows PowerShell
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----          2022/3/14 下午 01:46             DNS

PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

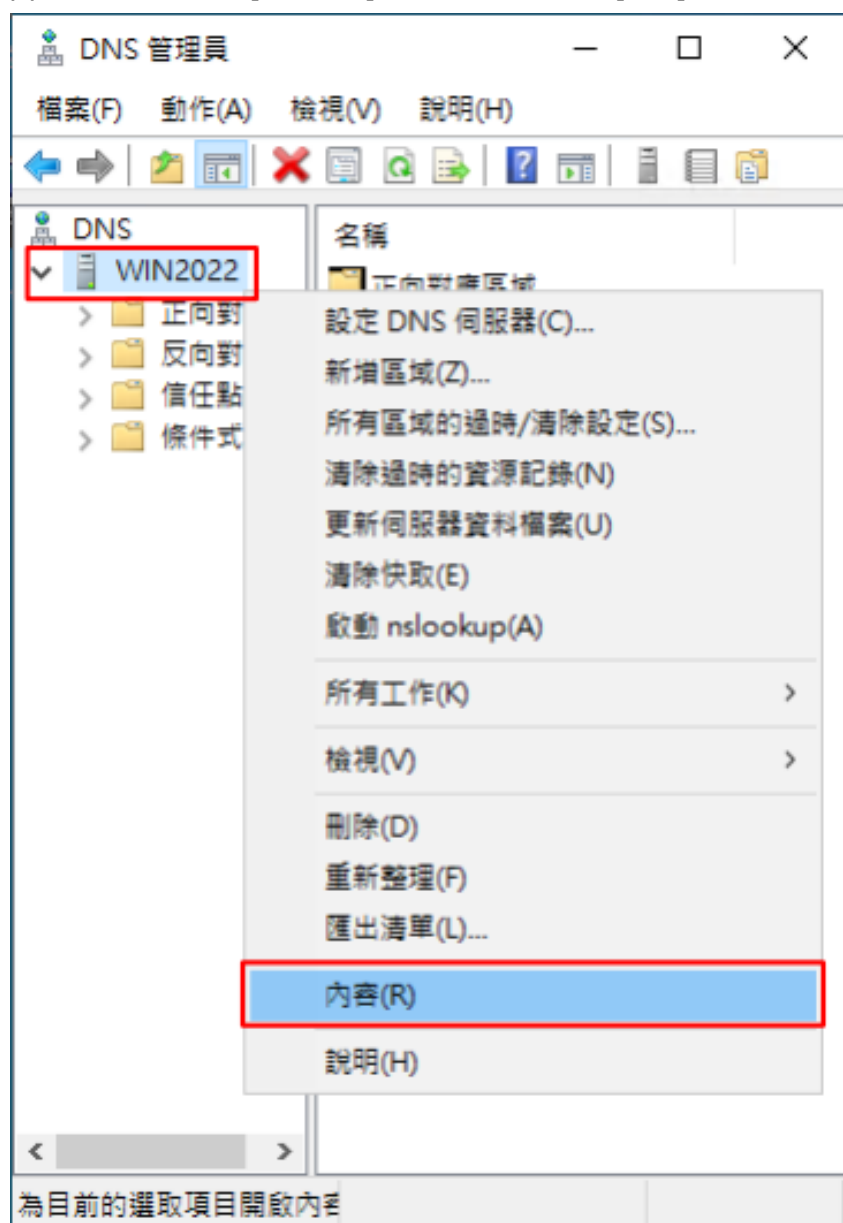
Mode                LastWriteTime         Length Name
----                -
d-----          2021/5/8 下午 04:20             CloudFiles
d-----          2022/3/14 下午 01:46             DNS
d-----          2021/5/8 下午 04:20             Firewall
d-----          2022/3/14 下午 01:44             LSA
d-----          2022/3/14 下午 01:44             SAM
d-----          2022/3/8 上午 10:16             Scm
d-----          2022/3/8 上午 10:30             setupcln
d-----          2022/3/8 下午 06:08             Sun
d-----          2021/5/8 下午 04:20             Windows Portable Devices
d-----          2022/3/14 下午 01:44             WMI

PS C:\> _
```

(3) 開啟 DNS



(4) 在 DNS 伺服器 [Win2022] 按滑鼠右鍵 -> 點選 [內容]



(5) [偵錯記錄] 頁面 -> 勾選 [記錄封包供偵錯之用] -> 輸入檔案路徑和名稱

C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]

WIN2022 - 內容

介面 轉寄站 進階 根目錄提示 偵錯記錄 事件記錄 監視

如果您要協助偵錯的話，您可以將 DNS 伺服器傳送與接收的封包記錄到記錄檔。根據預設值，偵錯記錄是停用的。

☒ 記錄封包供偵錯之用(L)

封包方向:

☒ 連出(O) } 至少選擇一個

☒ 連入(I) }

封包內容:

☒ 查詢/傳輸(Q) } 至少選擇一個

☒ 更新(S) }

☐ 通知(N)

其他選項:

☐ 記錄不符的連入回應封包(G)

☐ 詳細資料(D)

☐ 依 IP 位址篩選封包(C) 篩選(F)...

記錄檔

檔案路徑和名稱(H): indows\System32\LogFiles\DNS\dns.log

最大容量 (位元組)(M): 500000000

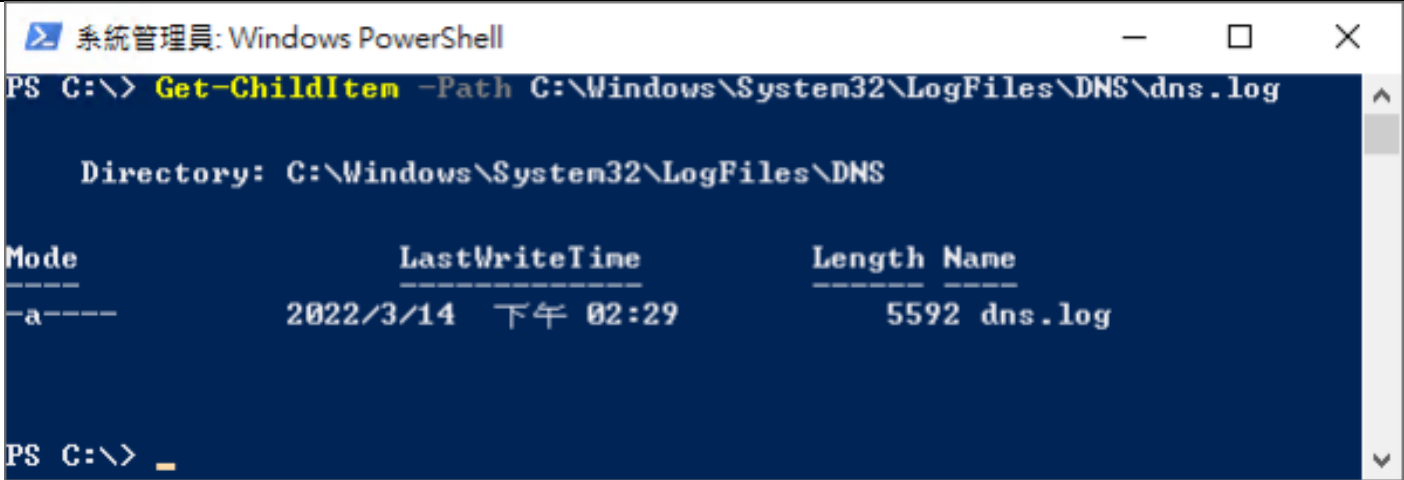
確定 取消 套用(A) 說明

(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```



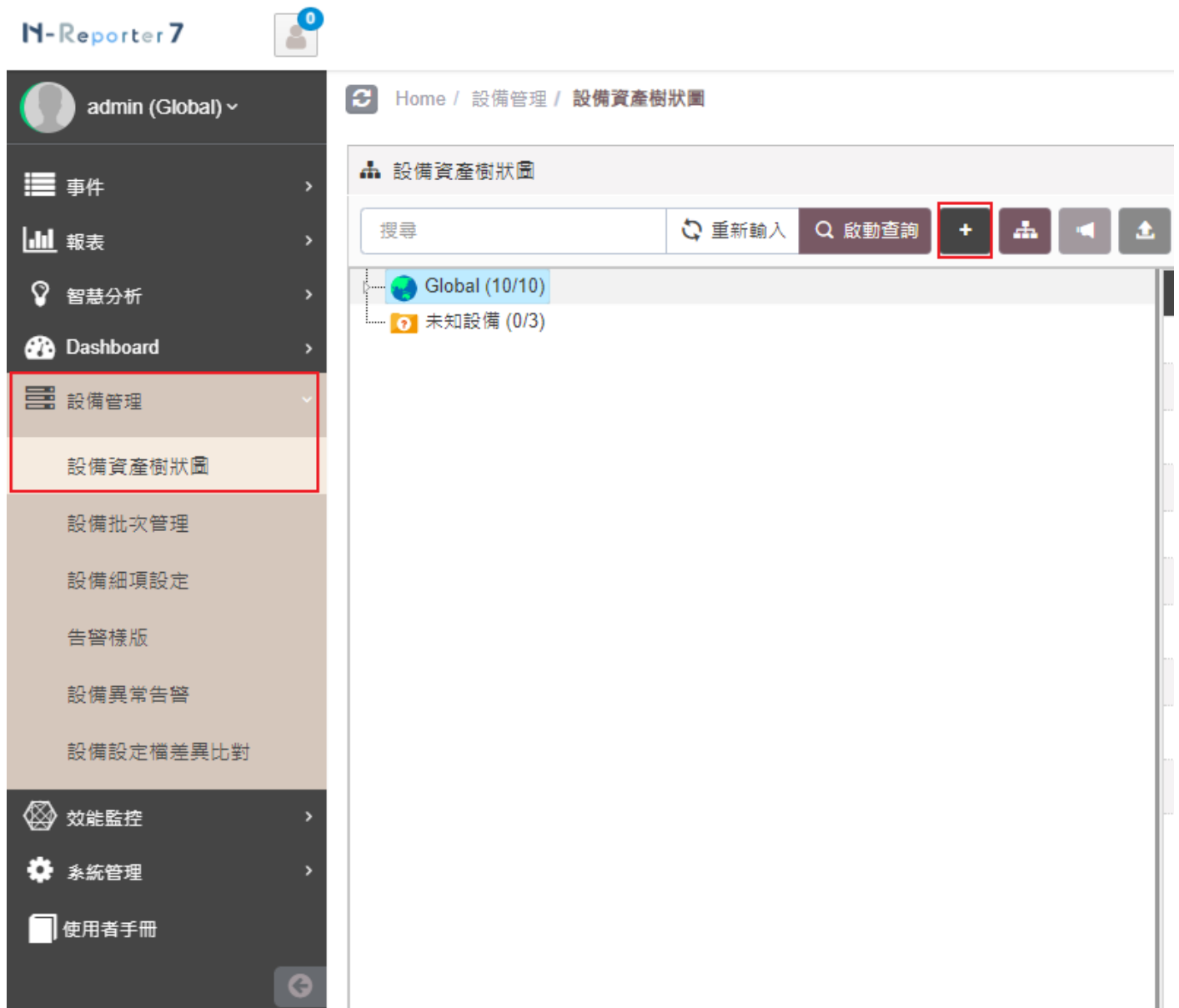
Mode	LastWriteTime	Length	Name
-a----	2022/3/14 下午 02:29	5592	dns.log

```
PS C:\> _
```

7 N-Reporter

(1) 新增 Windows DNS 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

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



(3) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows DNS]-> 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 *

WinDNS-192.168.8.195

IP *

192.168.8.195

所屬領域 *

Global

Syslog 資料格式 ⓘ

Windows DNS

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

(4) Syslog 相關設定

Facility 選擇 [(19) local use 3 (local3)]-> 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 ⓘ

(19) local use 3 (local3)

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

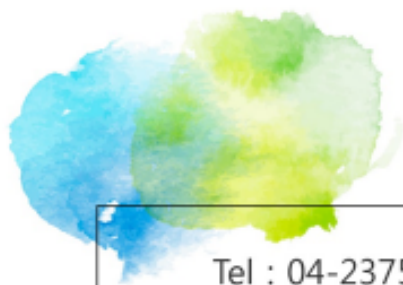
☐ 轉發方式將使用來源設備的 IP

上一步 下一步 取消

(5) 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]



Tel : 04-23752865 Fax : 04-23757458

業務詢問 : sales@npartner.com

技術詢問 : support@npartner.com