N-Partner

如何設定

Windows DNS log

V008

2024/04/15

版權聲明

商標

目錄

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

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。

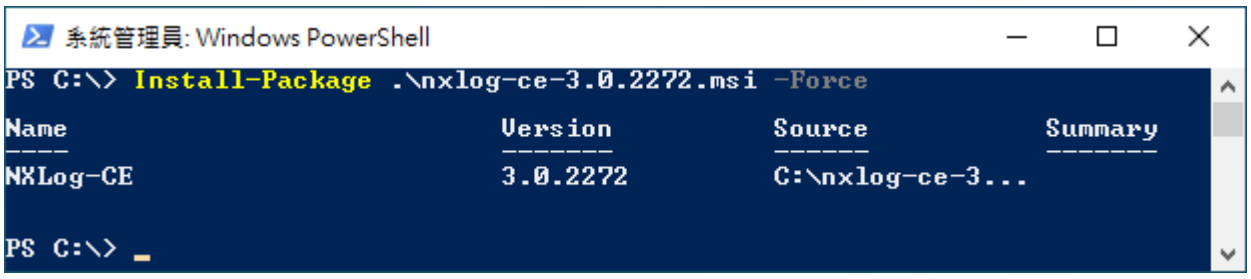
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

<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
```



紅色文字部位請輸入 NXLog 軟體路徑和檔案

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

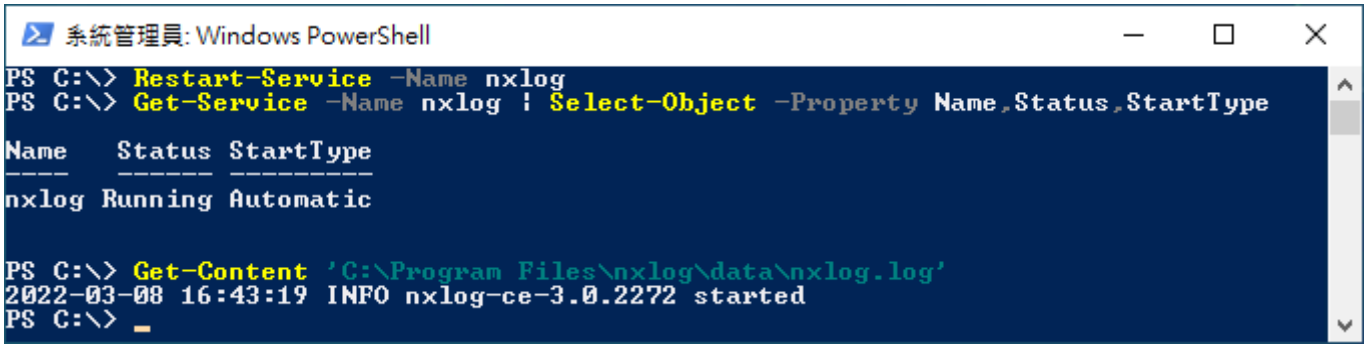
```
define DnsPath C:\Windows\Sysnative\LogFiles\DNS
```

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'
```



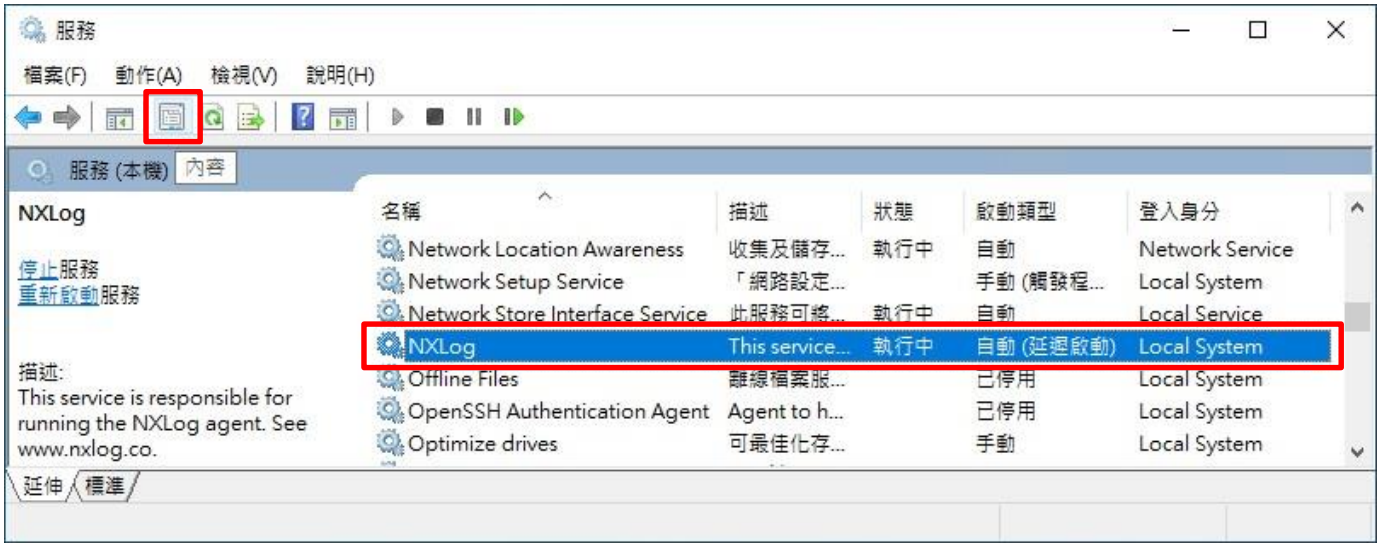
本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.log'

(3) 開啟 [服務] 功能

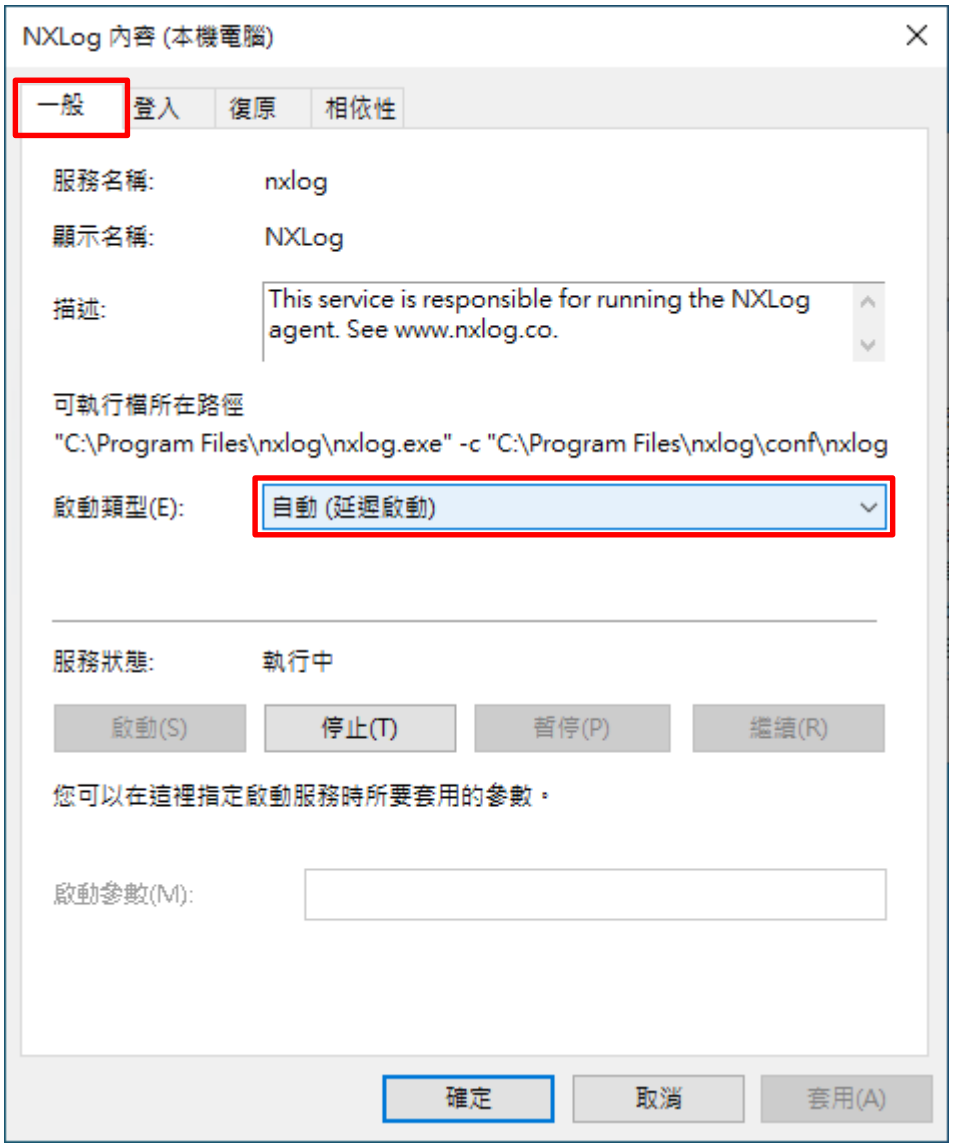
```
PS C:\> Services.msc
```

(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 (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]

2. Windows 2008

(1) 開啟 [Windows PowerShell]

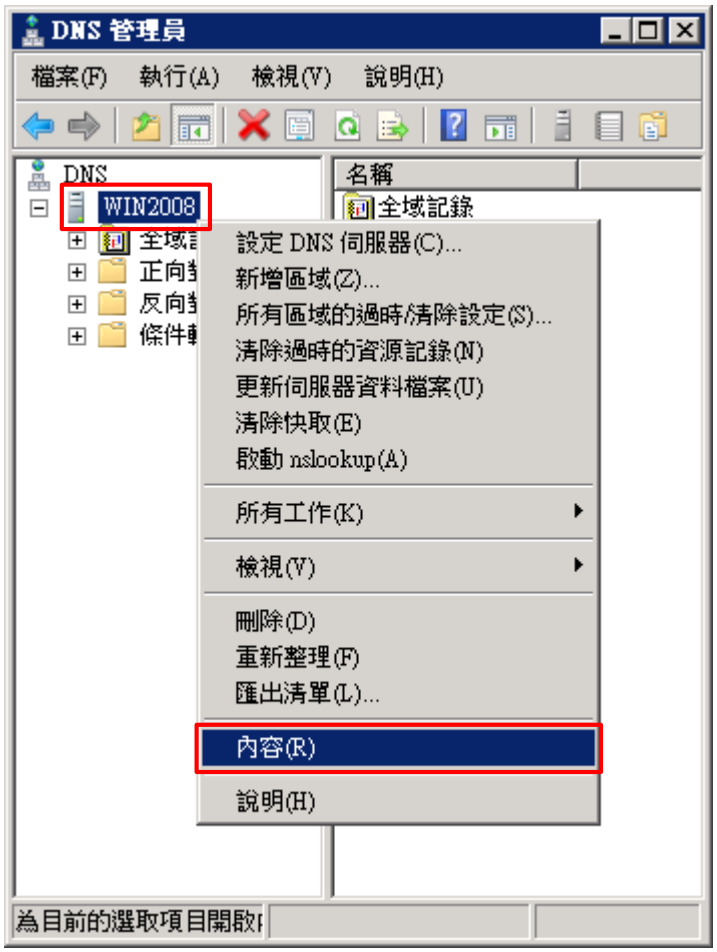
(2) 新增 DNS log 資料夾

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

```
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                Scm
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>
```

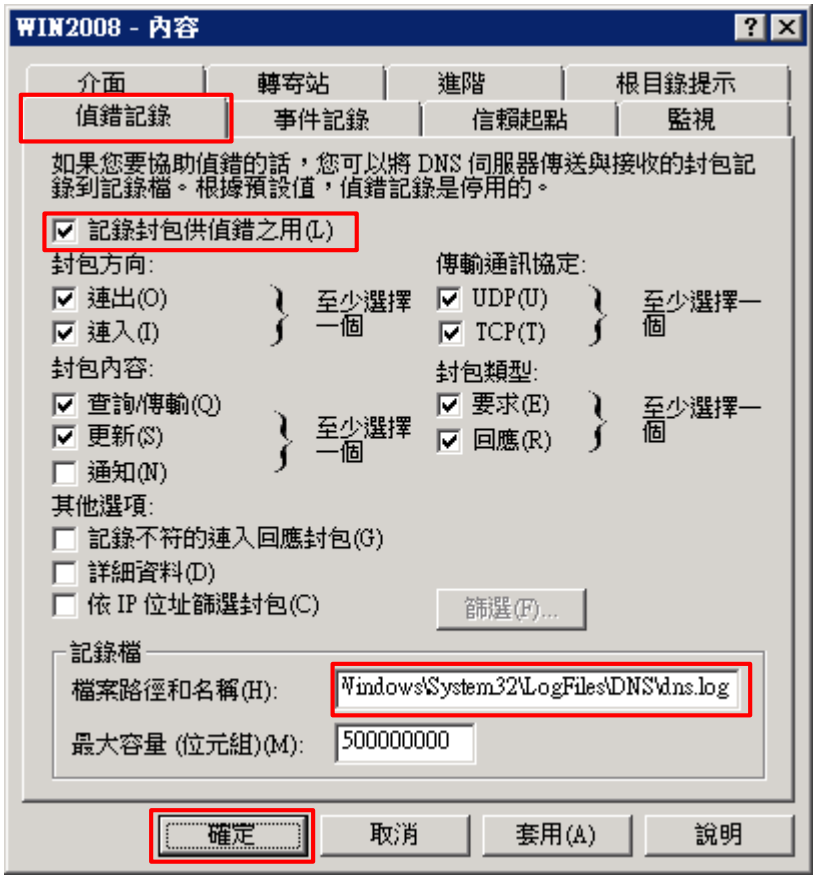
(3) 開啟 [DNS]

(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

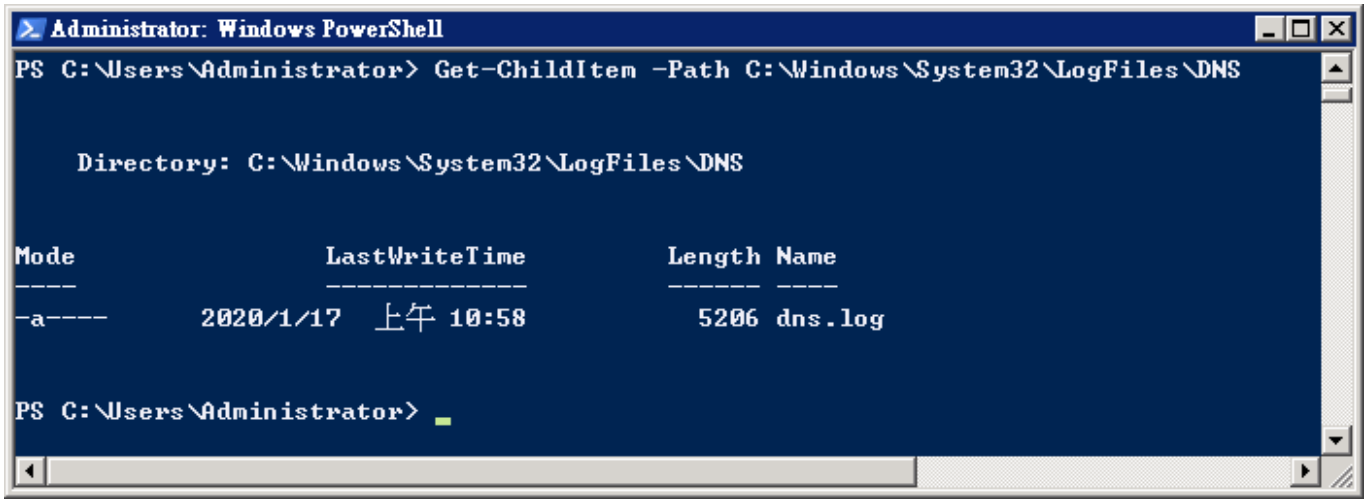
C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(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
```

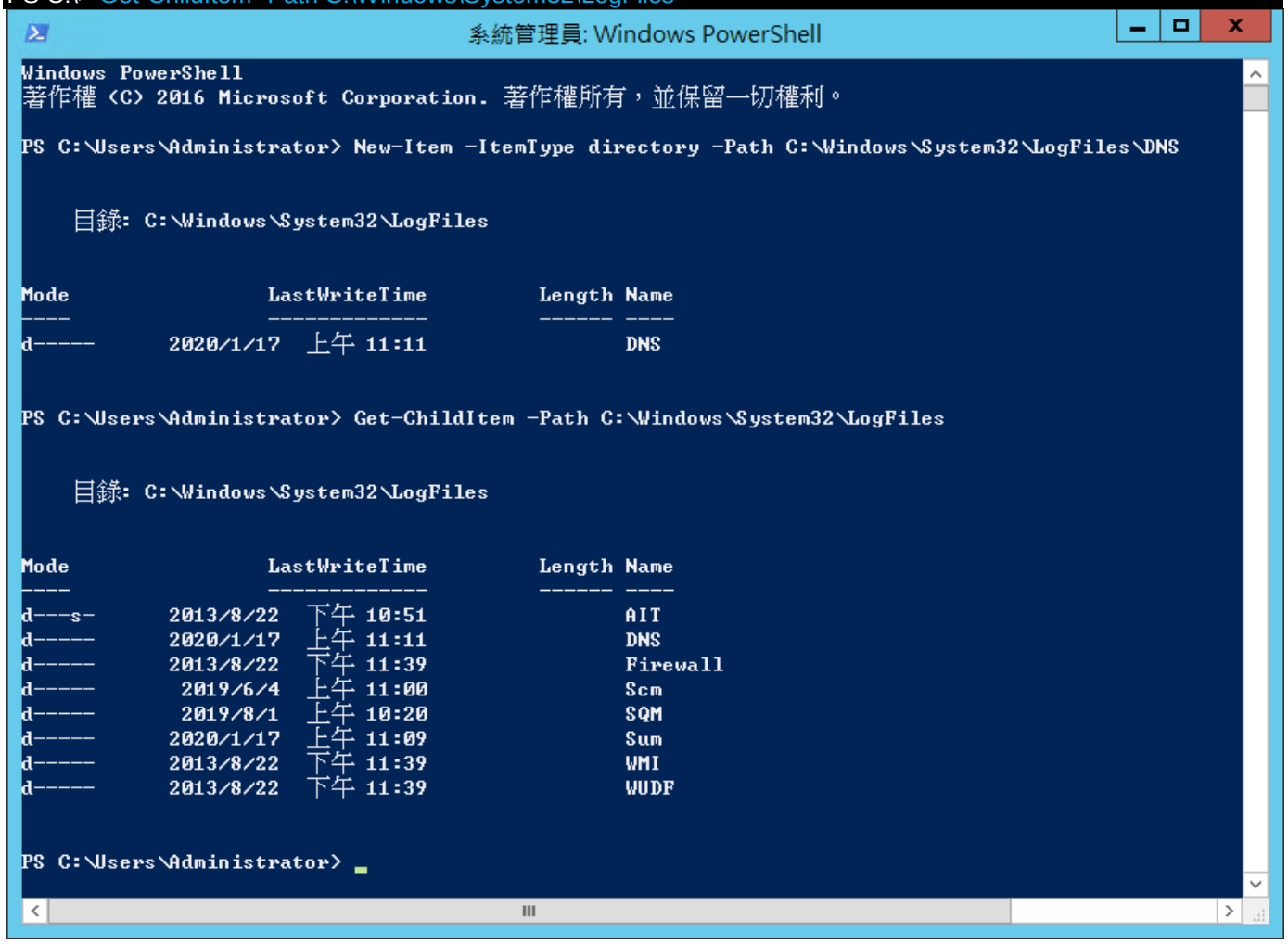


3. Windows 2012

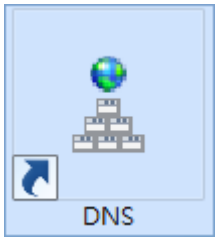
(1) 開啟 [Windows PowerShell]

(2) 新增 DNS log 資料夾

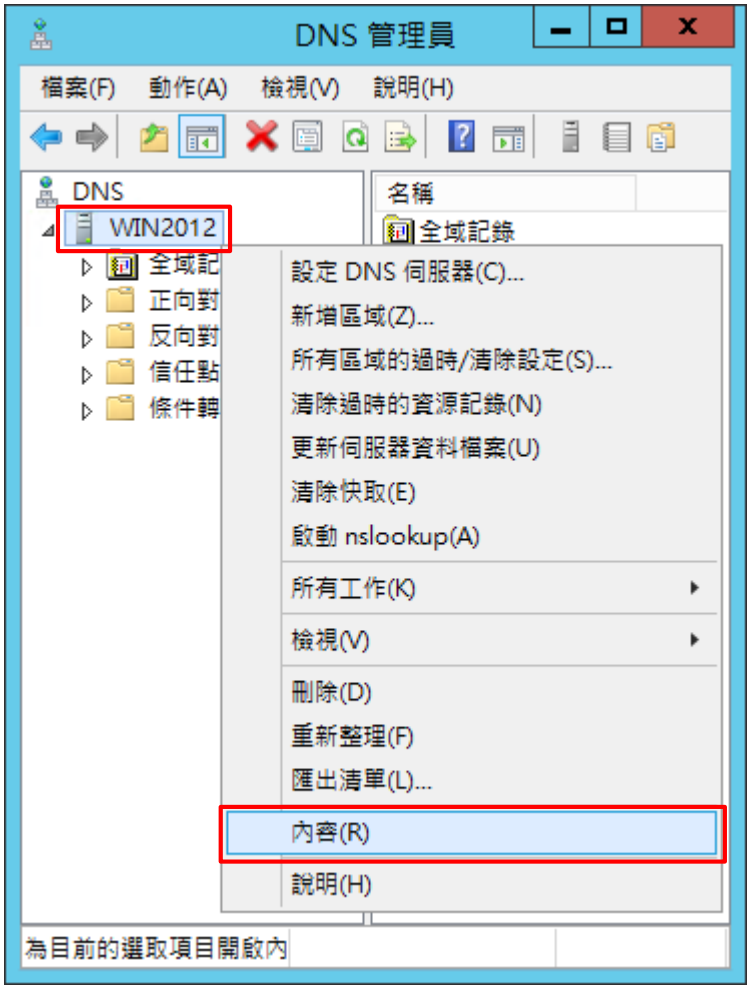
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 [DNS]

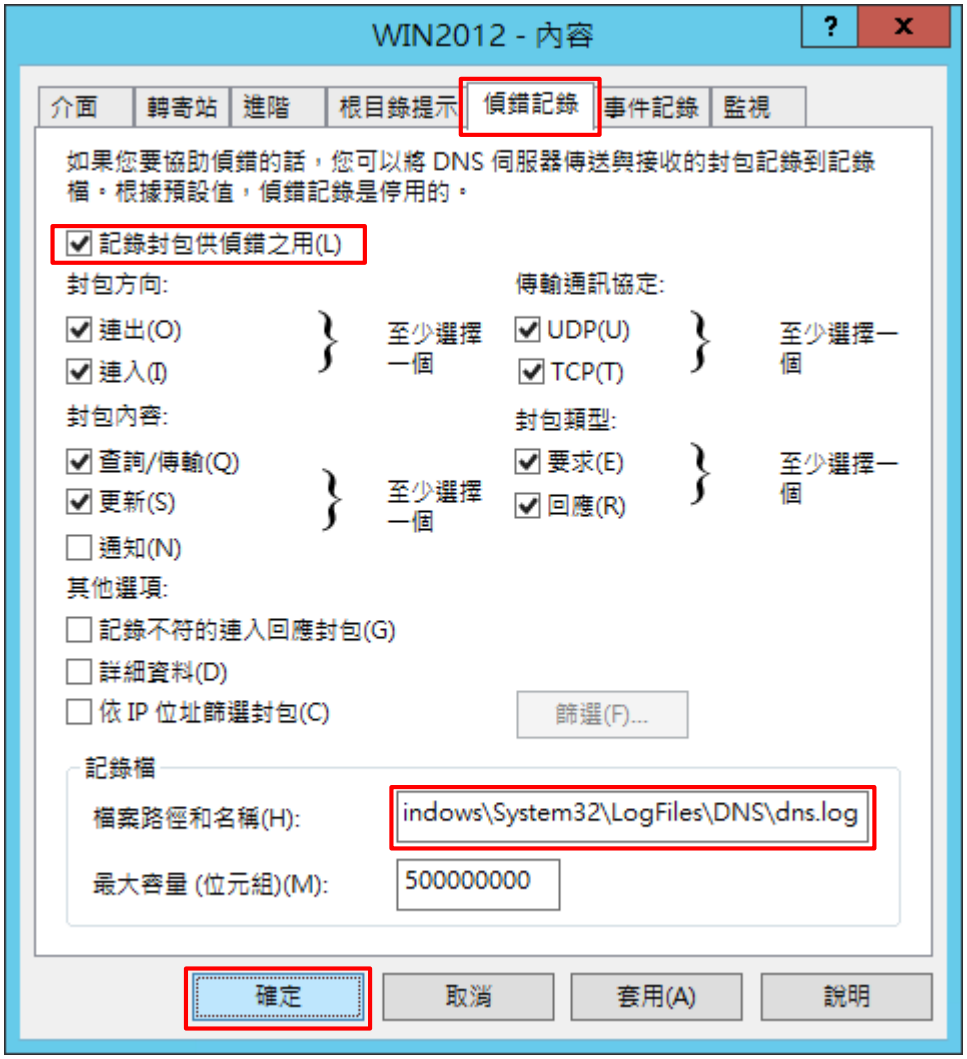


(4) 在 DNS 伺服器 [Win2012] 按滑鼠右鍵 -> 點選 [內容]



(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

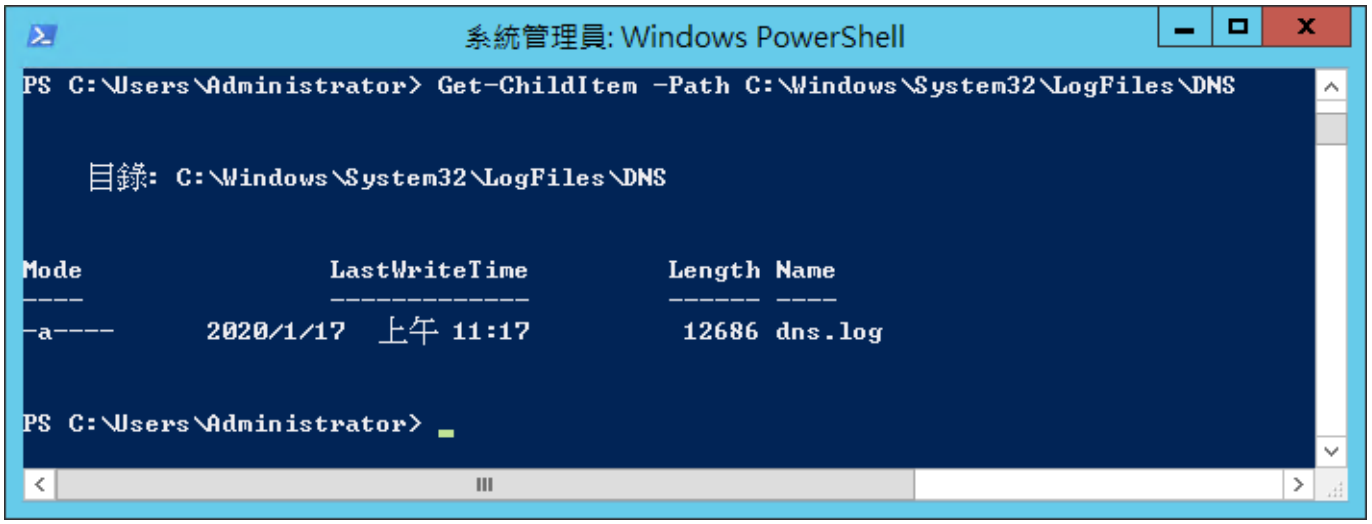
C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(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
```

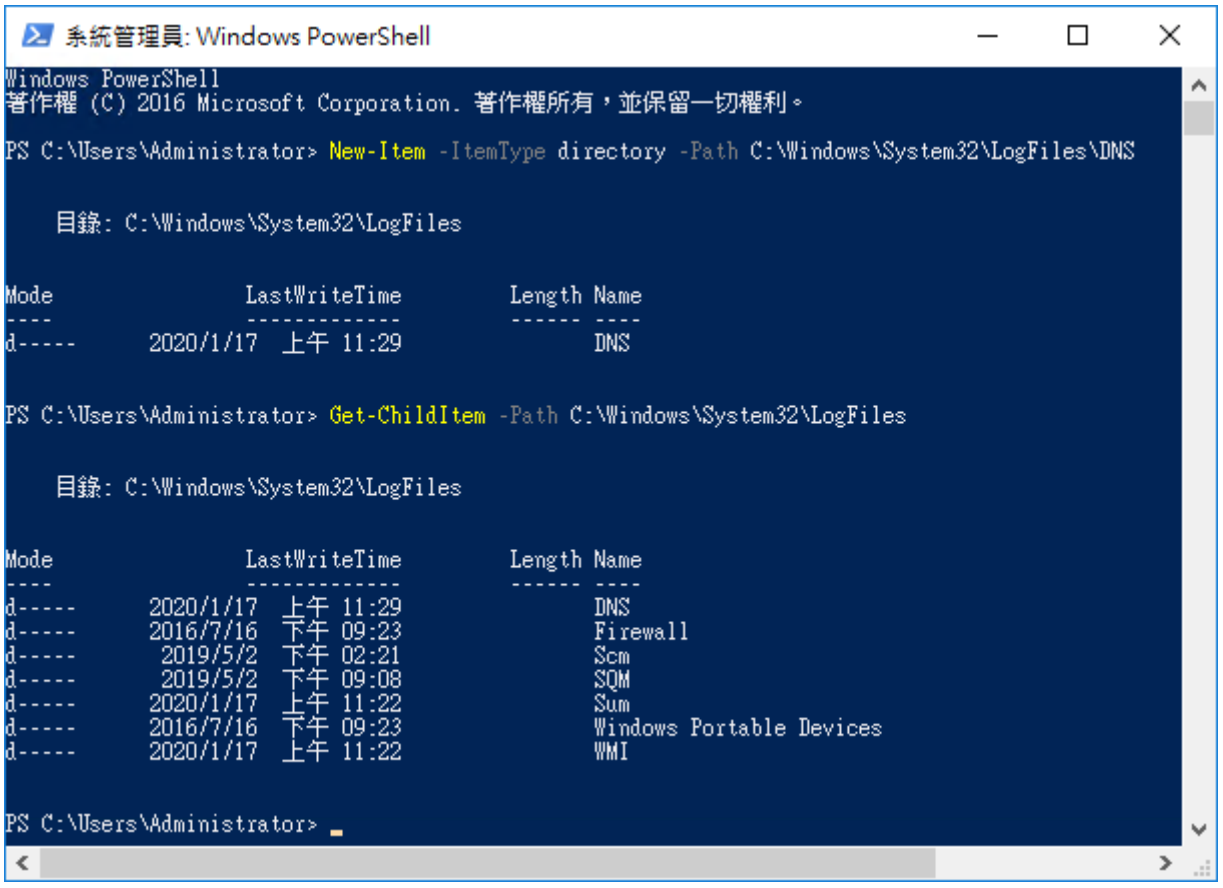


4. Windows 2016

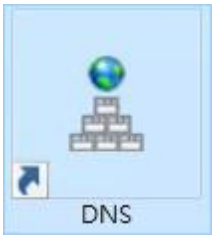
(1) 開啟 [Windows PowerShell]

(2) 新增 DNS log 資料夾

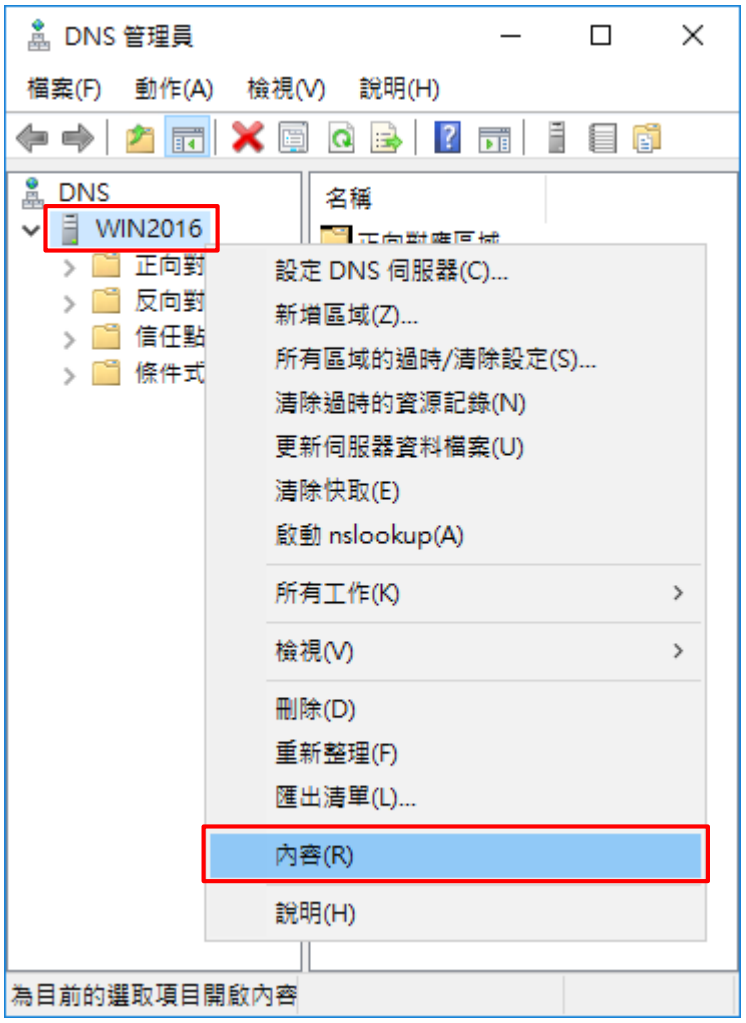
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 [DNS]

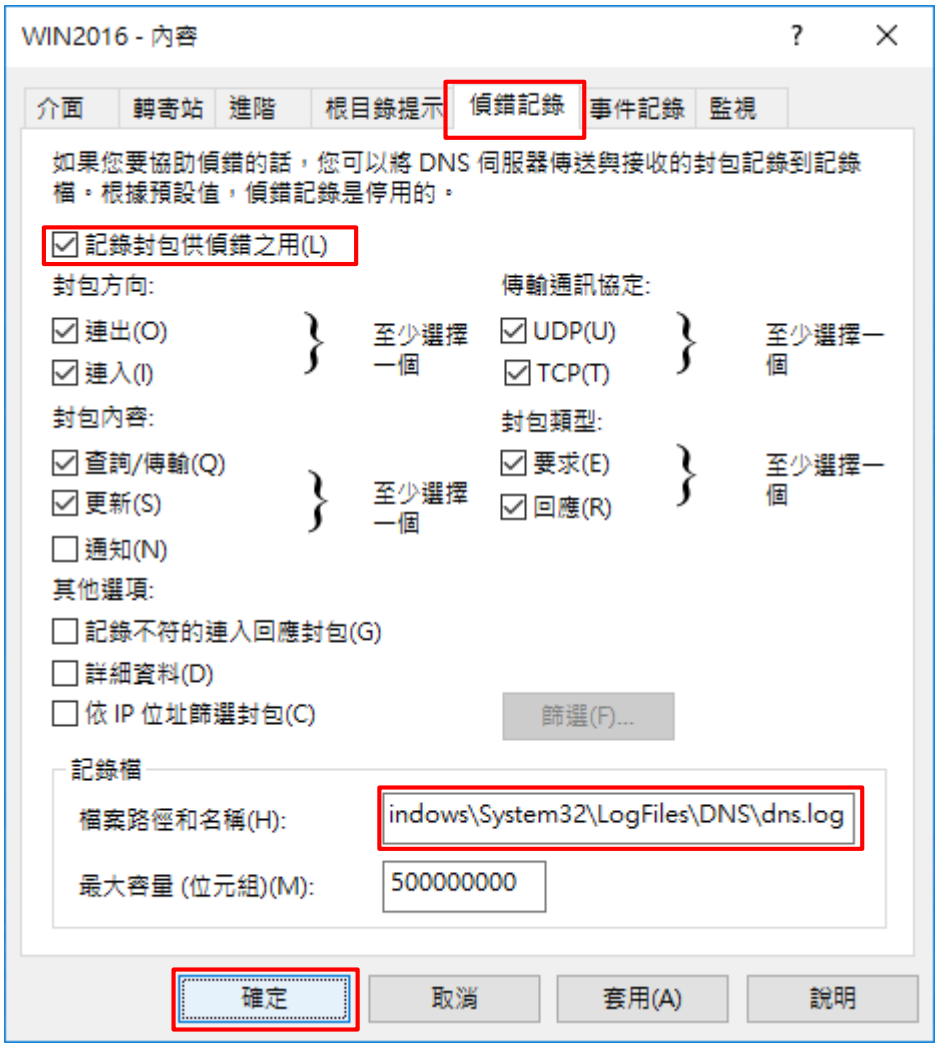


(4) 在 DNS 伺服器 [Win2016] 按滑鼠右鍵 -> 點選 [內容]



(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

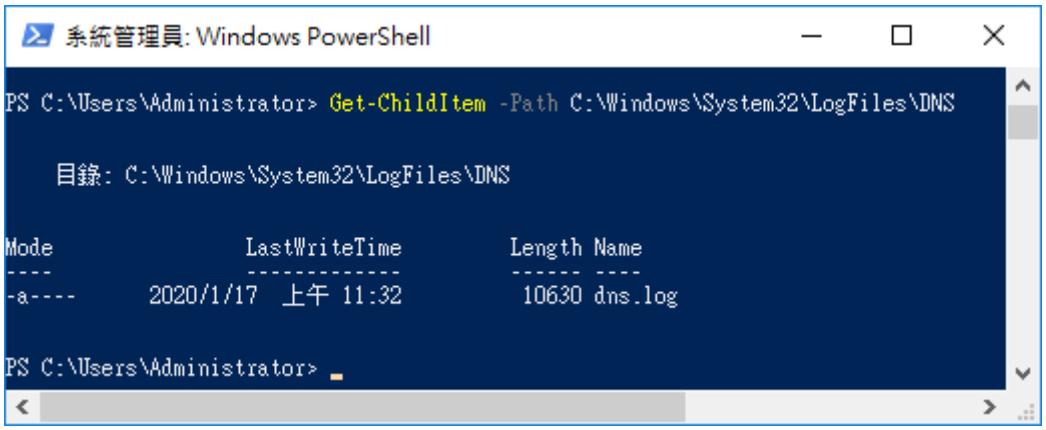
C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(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
```

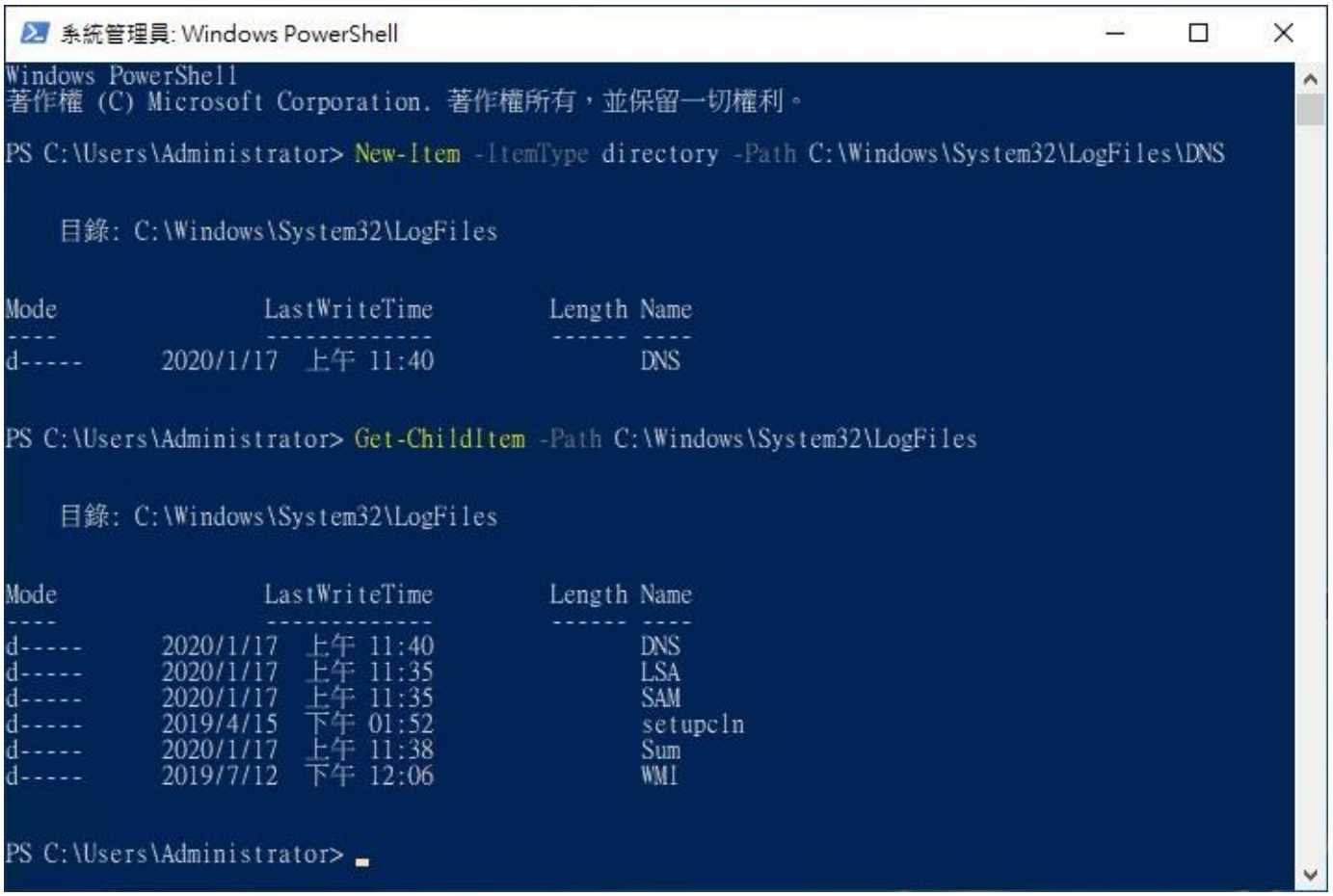


5. Windows 2019

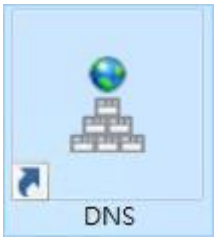
(1) 開啟 [Windows PowerShell]

(2) 新增 DNS log 資料夾

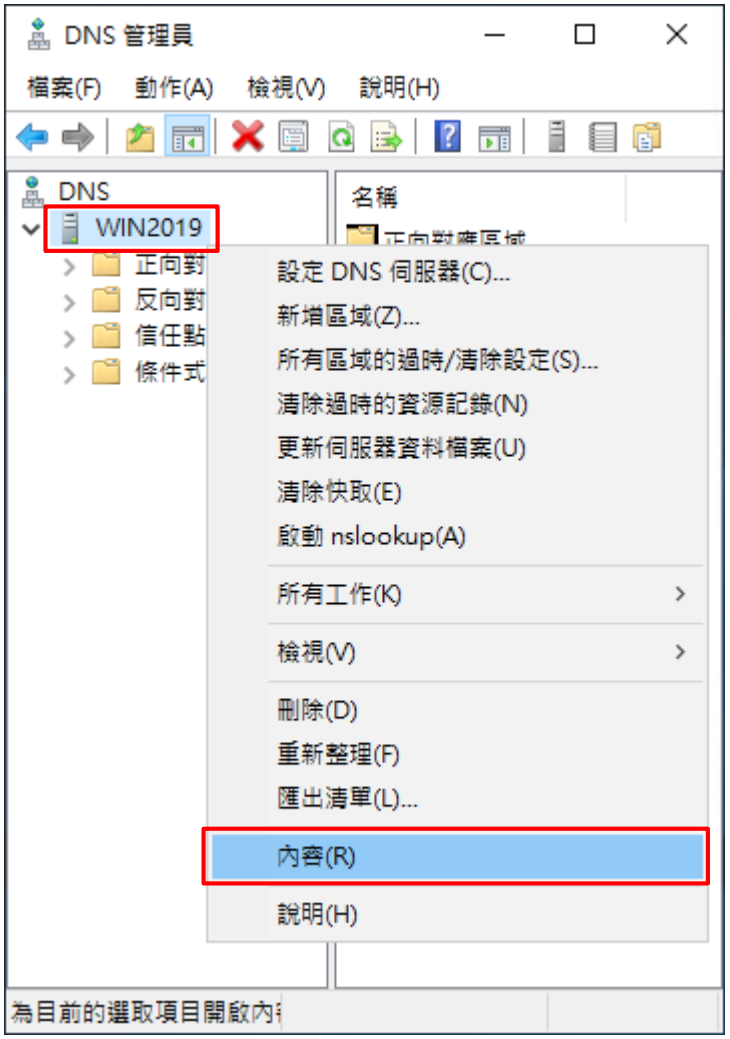
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```



(3) 開啟 [DNS]

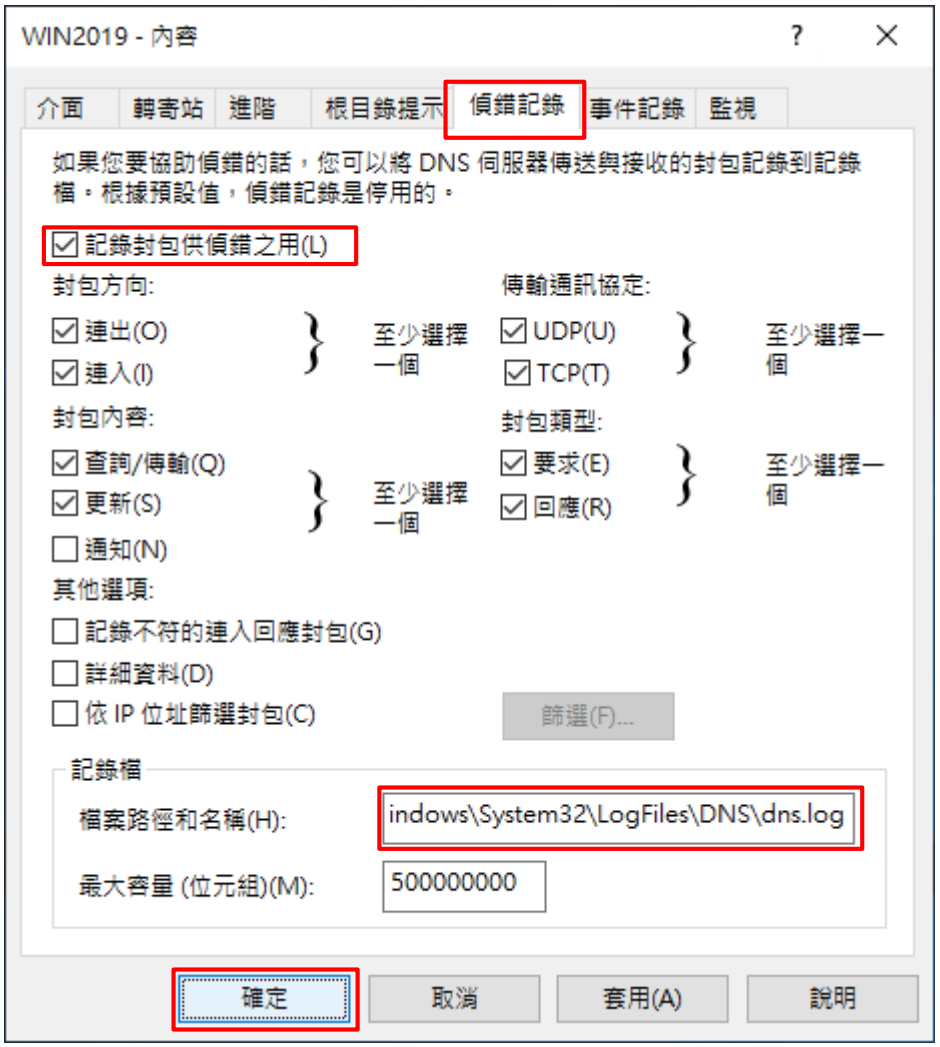


(4) 在 DNS 伺服器 [Win2019] 按滑鼠右鍵 -> 點選 [內容]



(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

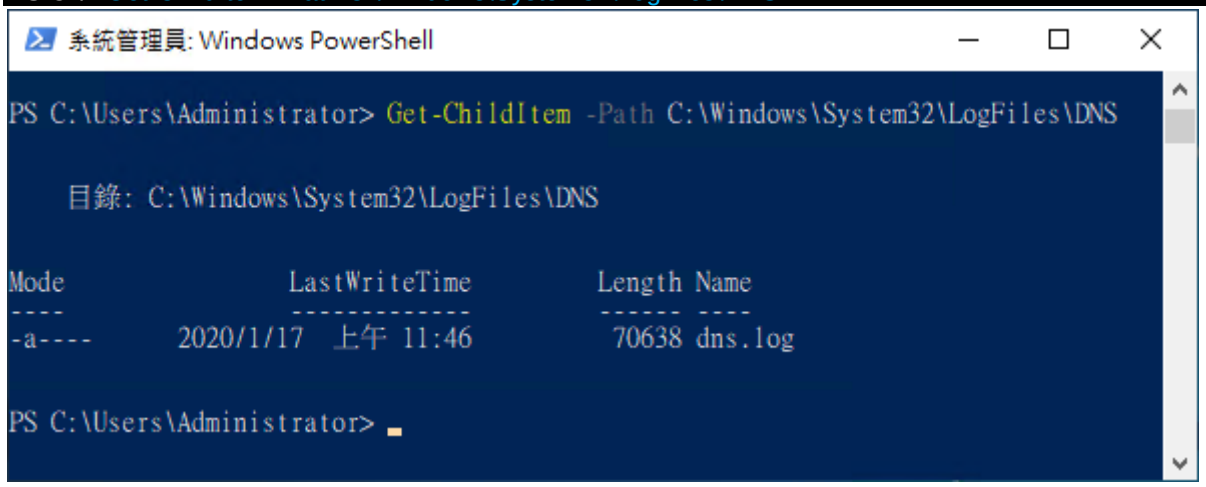
C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(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
```



6. Windows 2022

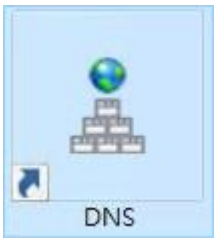
(1) 開啟 [Windows PowerShell]

(2) 新增 DNS log 資料夾

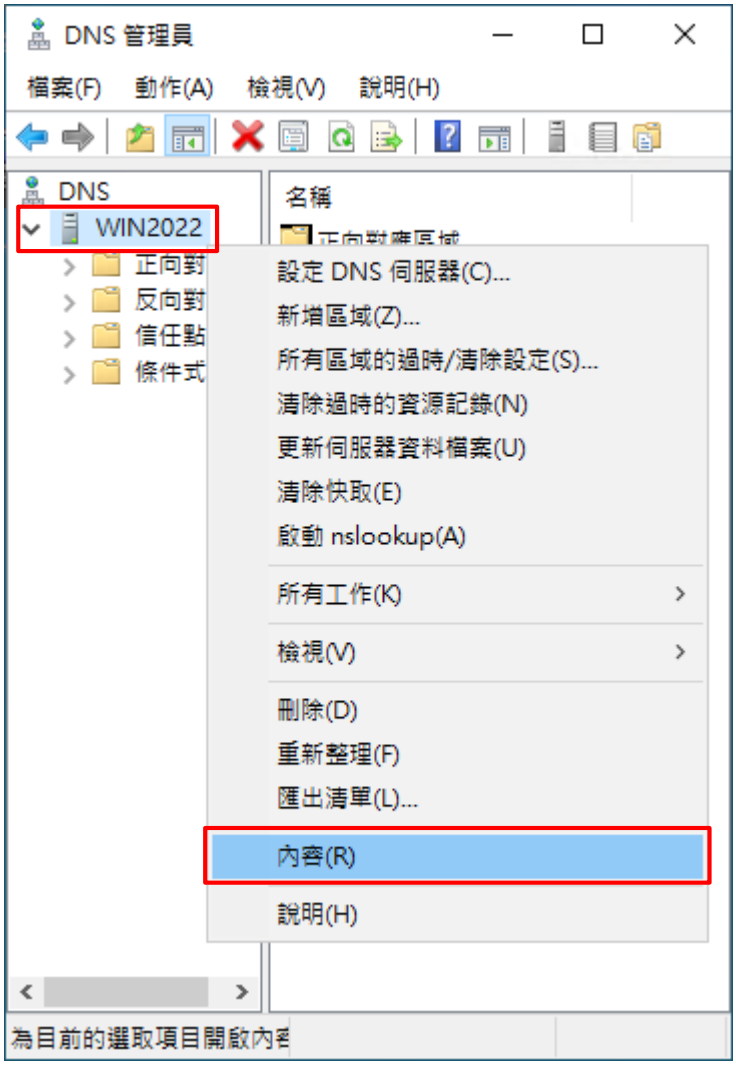
```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

```
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                Sum
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]

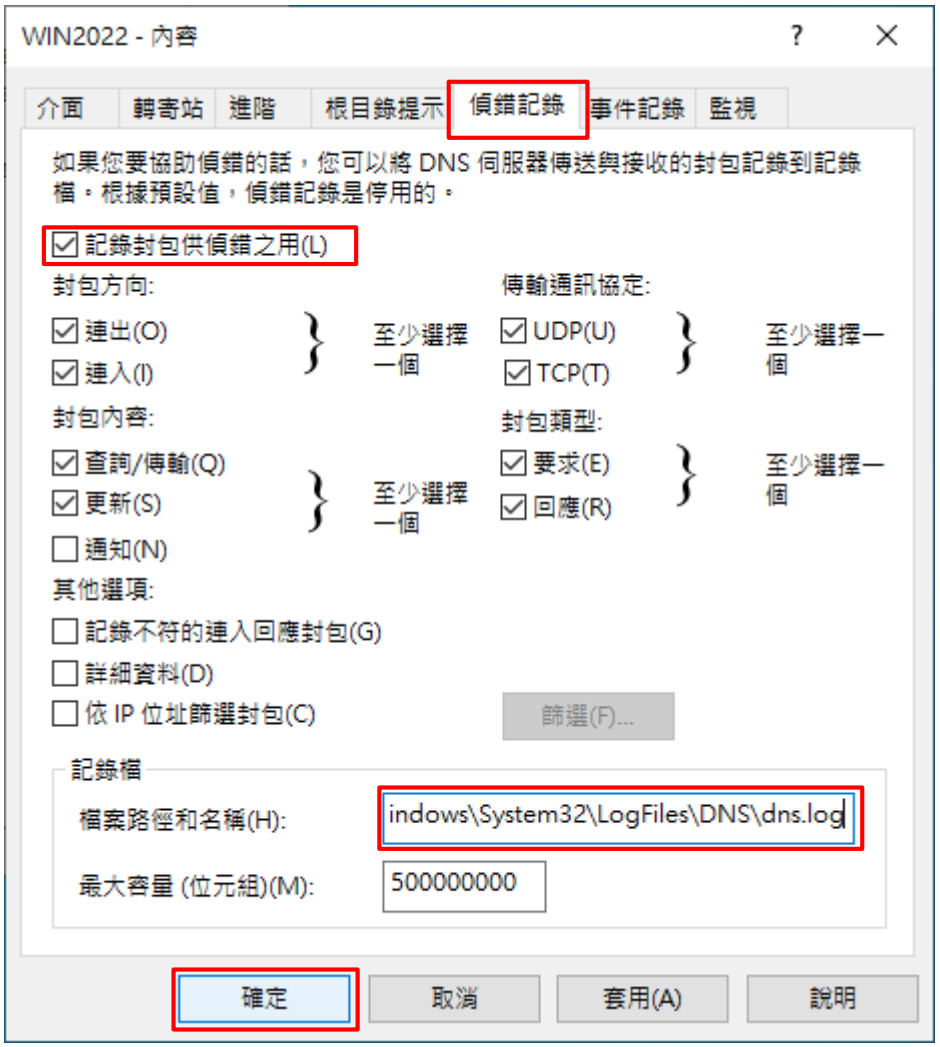


(4) 在 DNS 伺服器 [Win2022] 按滑鼠右鍵 -> 點選 [內容]



(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

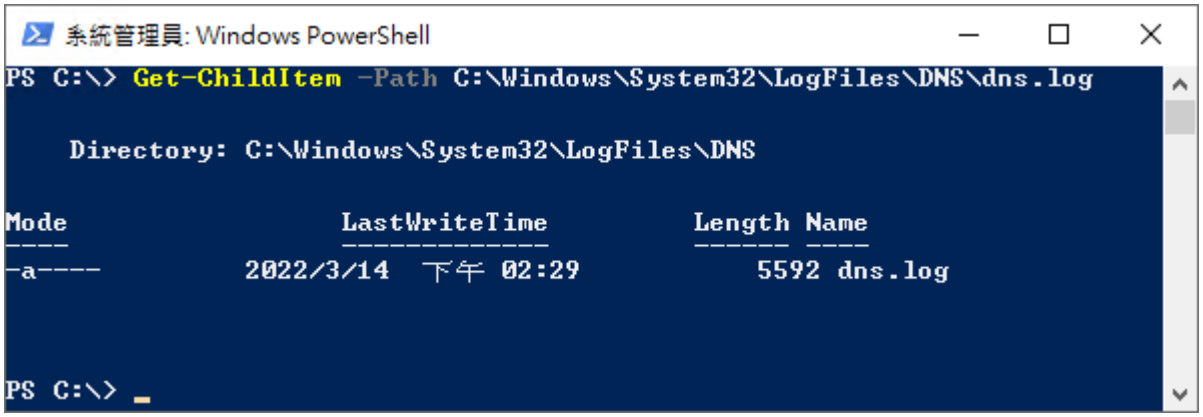
C:\Windows\System32\LogFiles\DNS\dns.log -> 按下 [確定]



(6) 開啟 [Windows PowerShell]

(7) 確認有產生 dns.log 檔案

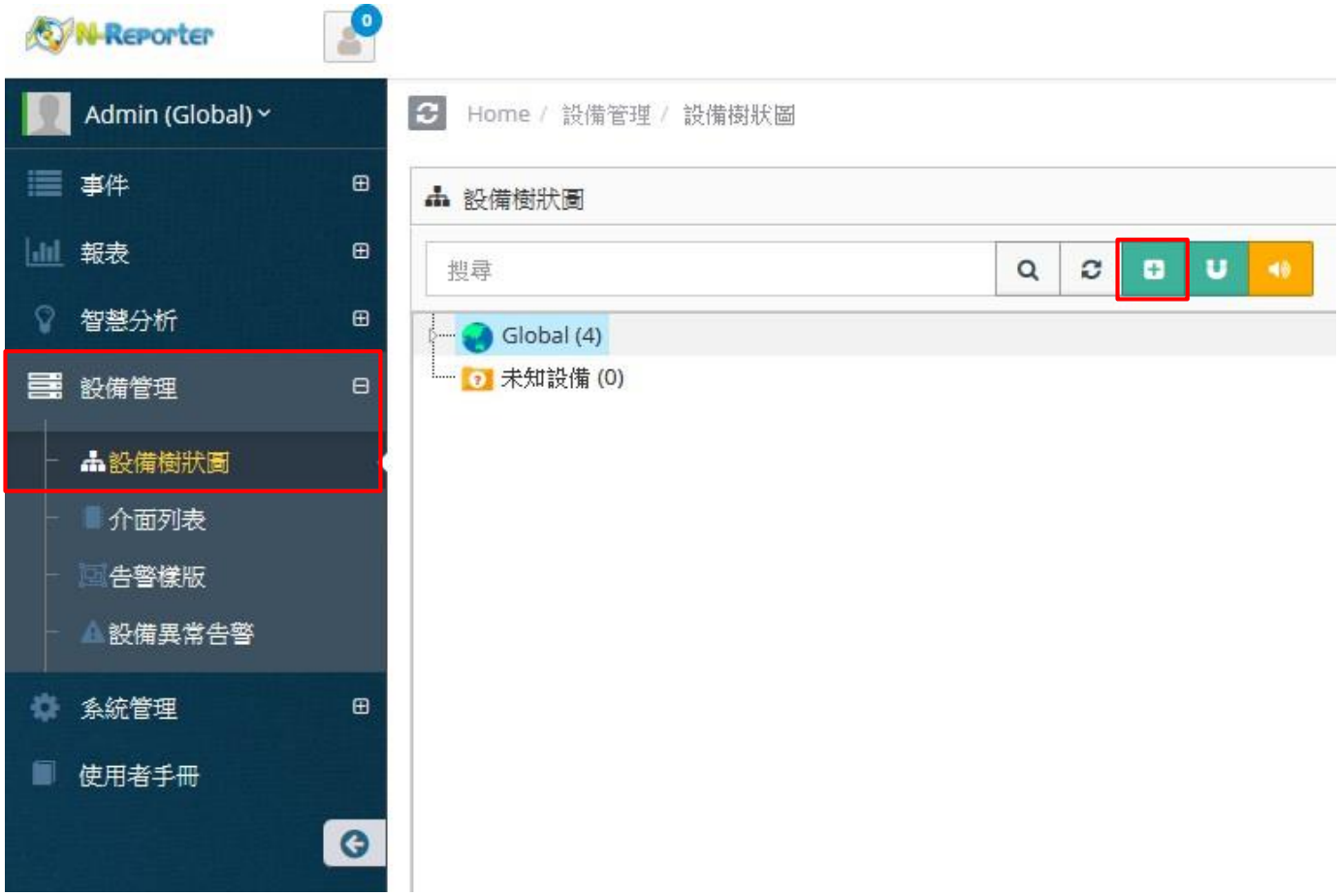
```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS\dns.log
```



7. N-Reporter

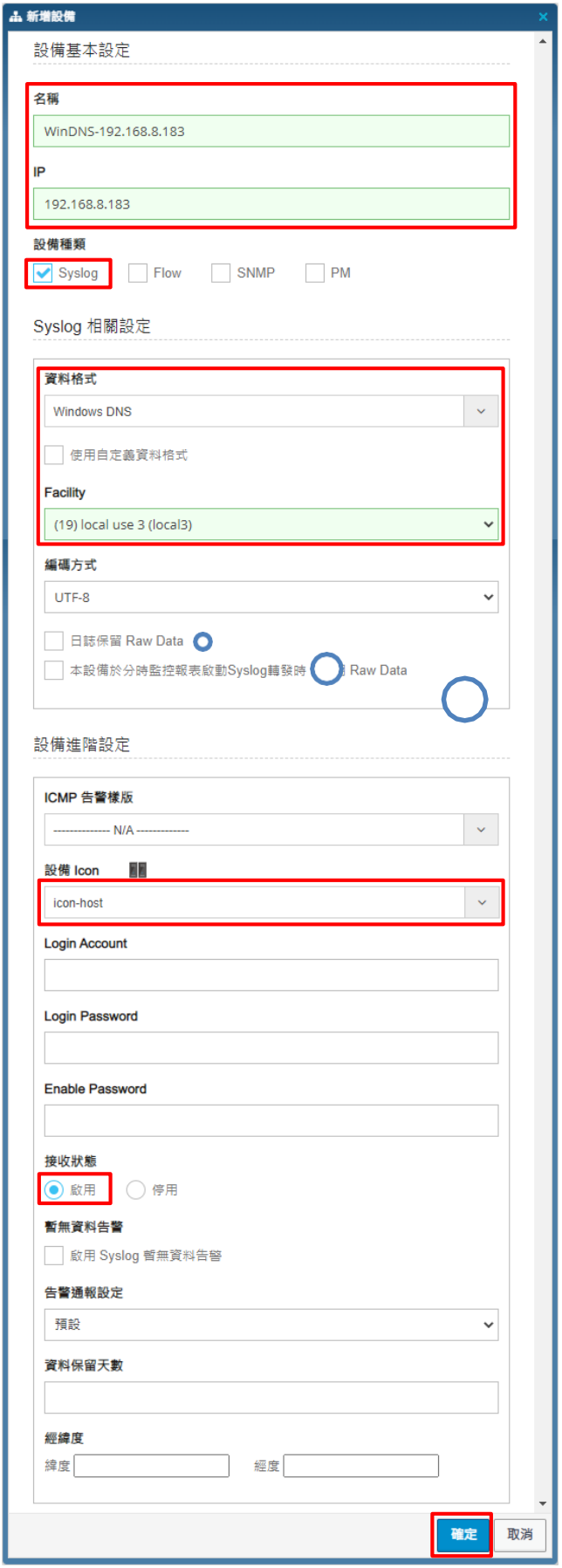
(1) 新增 Windows DNS 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



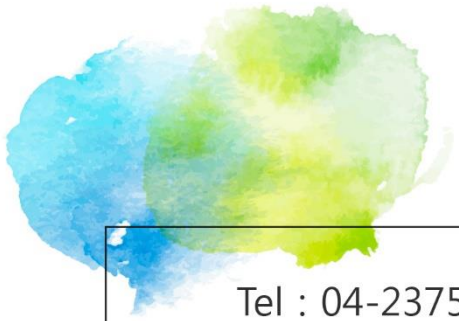
(2) 設定 Windows DNS 記錄的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows DNS] 和 Facility: [(19) local use 3 (local3)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊



Tel：04-23752865　　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com