

Partner

如何設定

Windows DNS log

V008

2024/04/15



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
1. NXLog.....	3
1.1 NXLog 安裝.....	3
1.2 NXLog 設定檔下載.....	4
1.3 NXLog 設定檔.....	5
1.4 NXLog 啟動服務.....	6
2. Windows 2008.....	9
3. Windows 2012.....	13
4. Windows 2016.....	17
5. Windows 2019.....	21
6. Windows 2022.....	25
7. N-Reporter.....	29

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

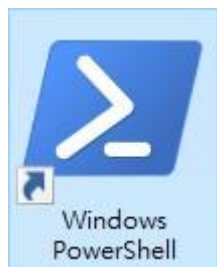


註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog

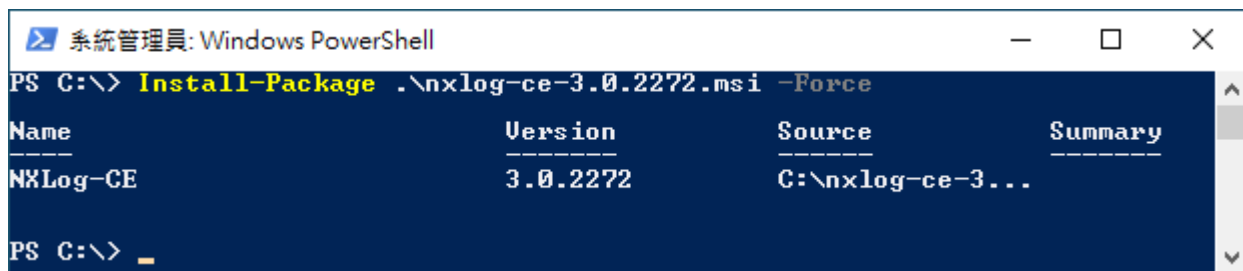
<2.1> Windows 2008 或之後版本作業系統

<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

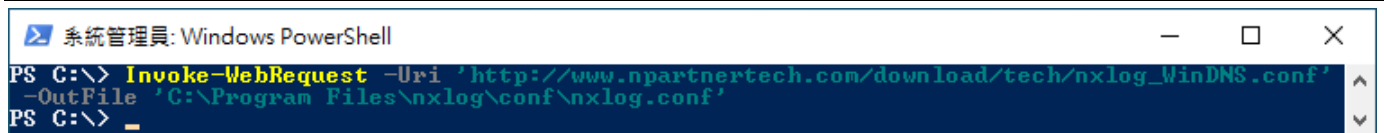
(1) 開啟 [Windows PowerShell]



(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
```

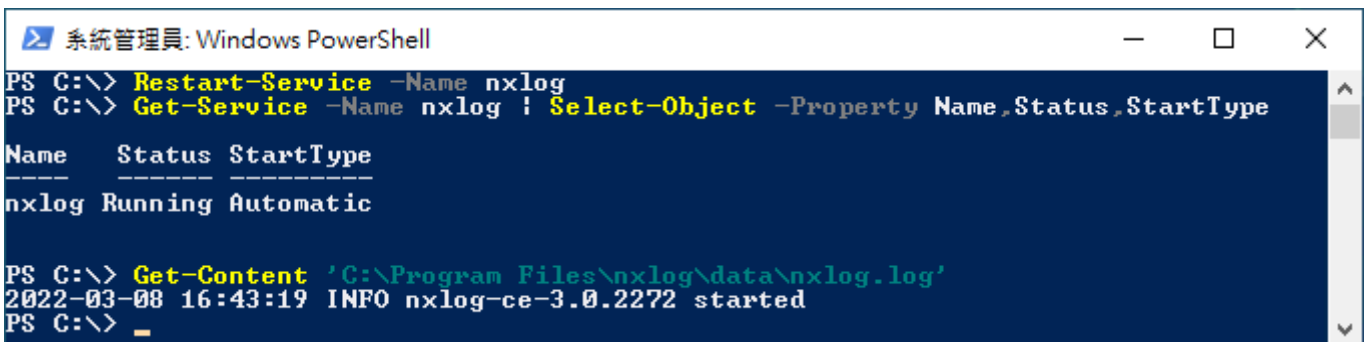
1.4 NXLog 啟動服務

(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'
```

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

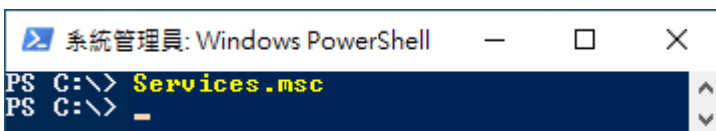
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
Name      Status StartType
-----
nxlog     Running Automatic

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.log](#)'


(3) 開啟 [服務] 功能

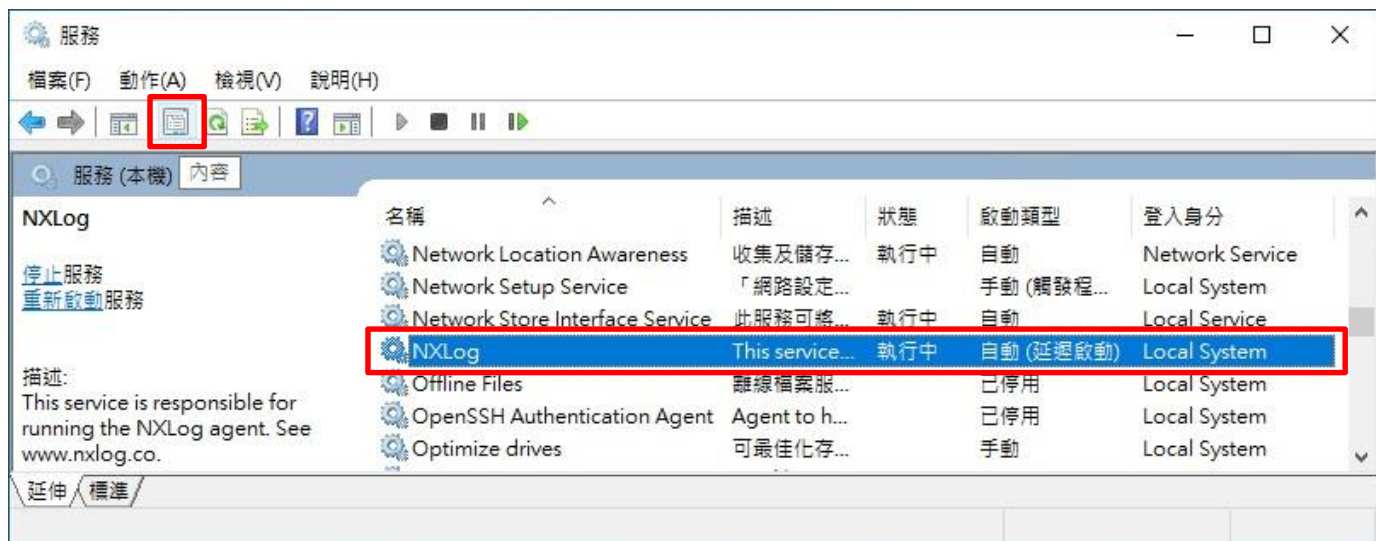
```
PS C:\> Services.msc
```

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

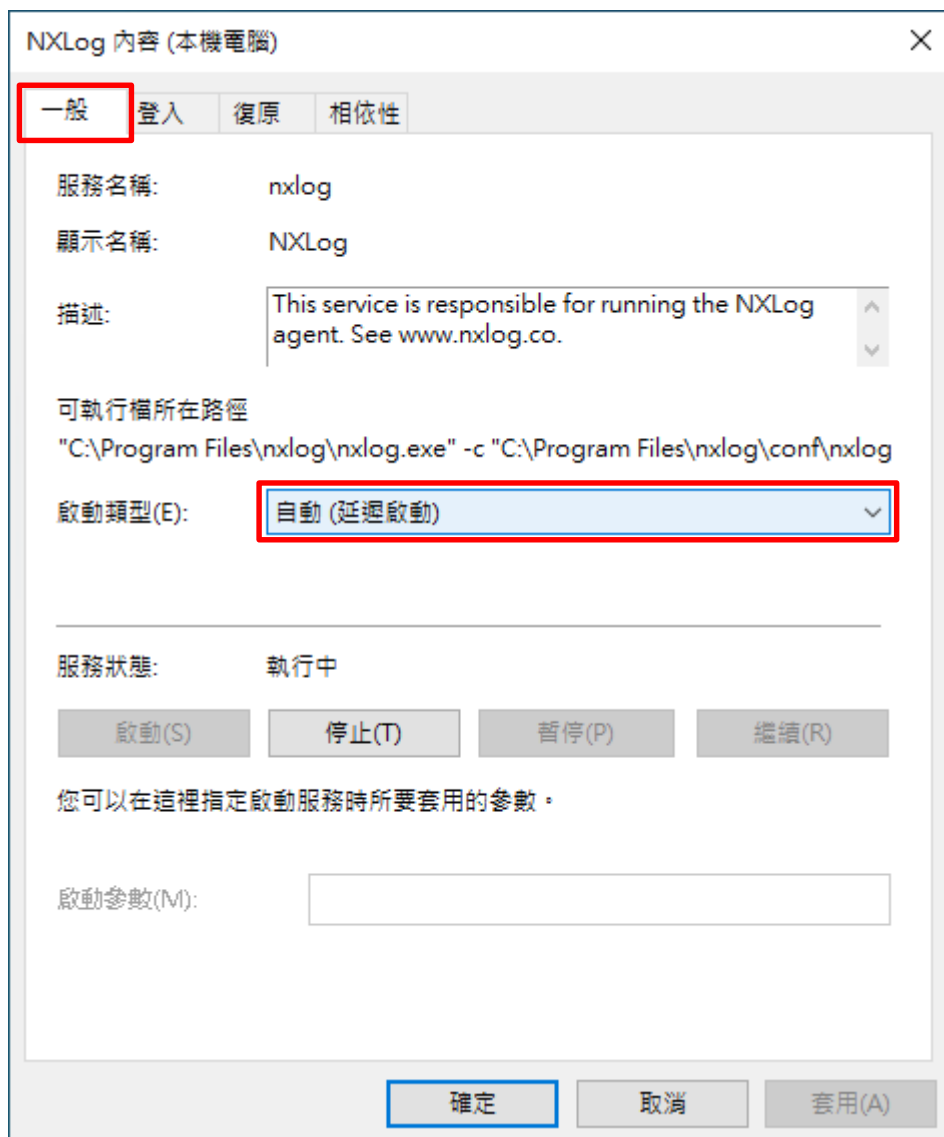
```
PS C:\> Services.msc
PS C:\> _
```


(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 2008

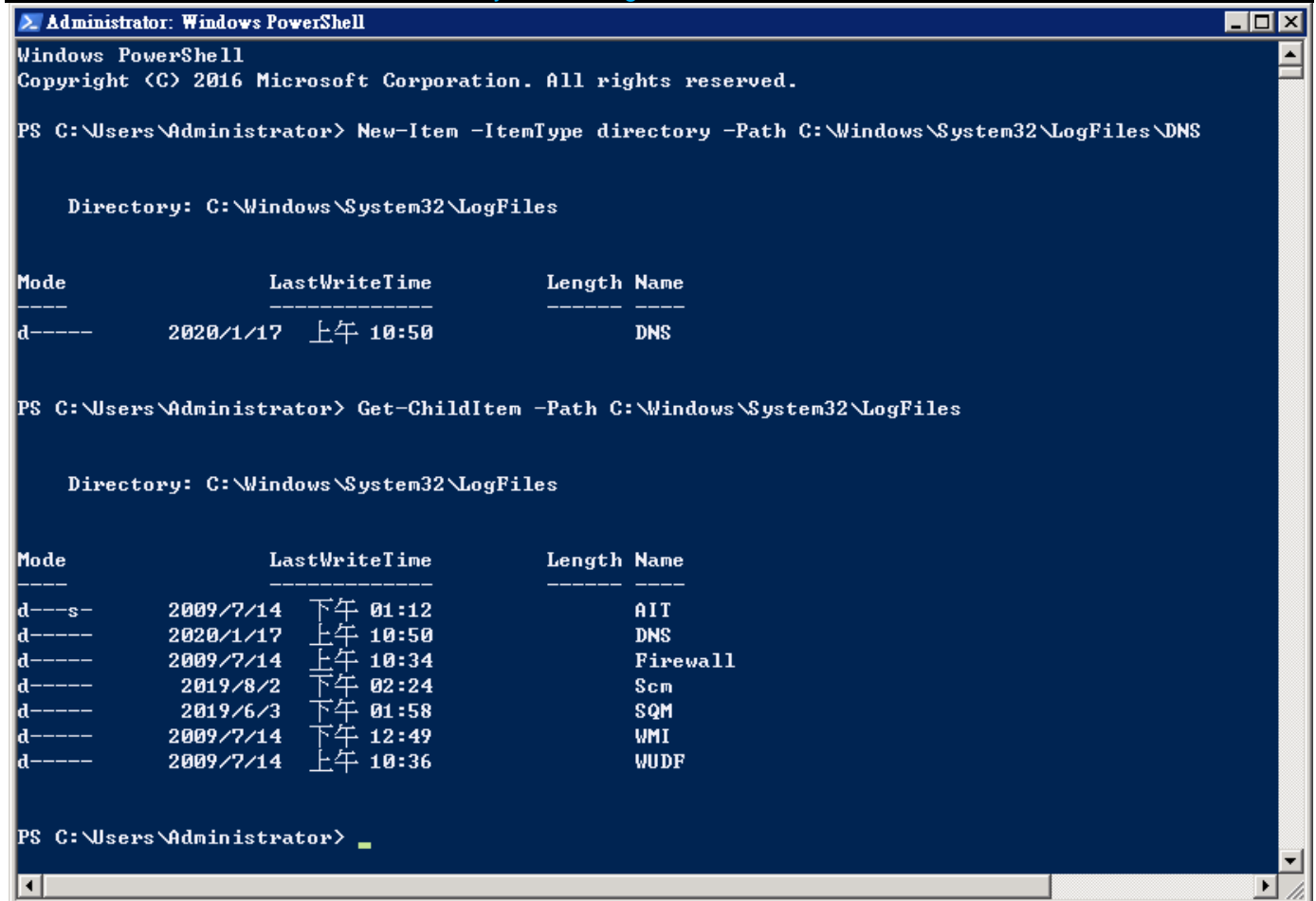
(1) 開啟 [Windows PowerShell]



(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 directory named "DNS" in the specified path. The second command, "Get-ChildItem -Path C:\Windows\System32\LogFiles", lists the contents of the "LogFiles" directory, showing a table of files and folders with their modes, last write times, lengths, and names.

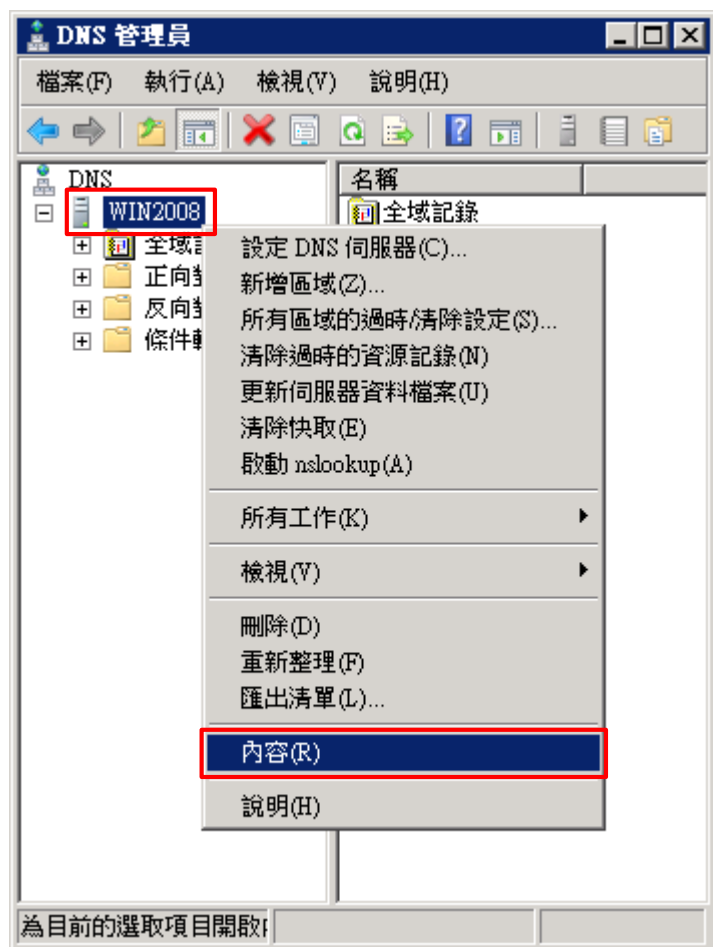
Mode	LastWriteTime	Length	Name
d-----	2020/1/17 上午 10:50		DNS

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

(3) 開啟 [DNS]

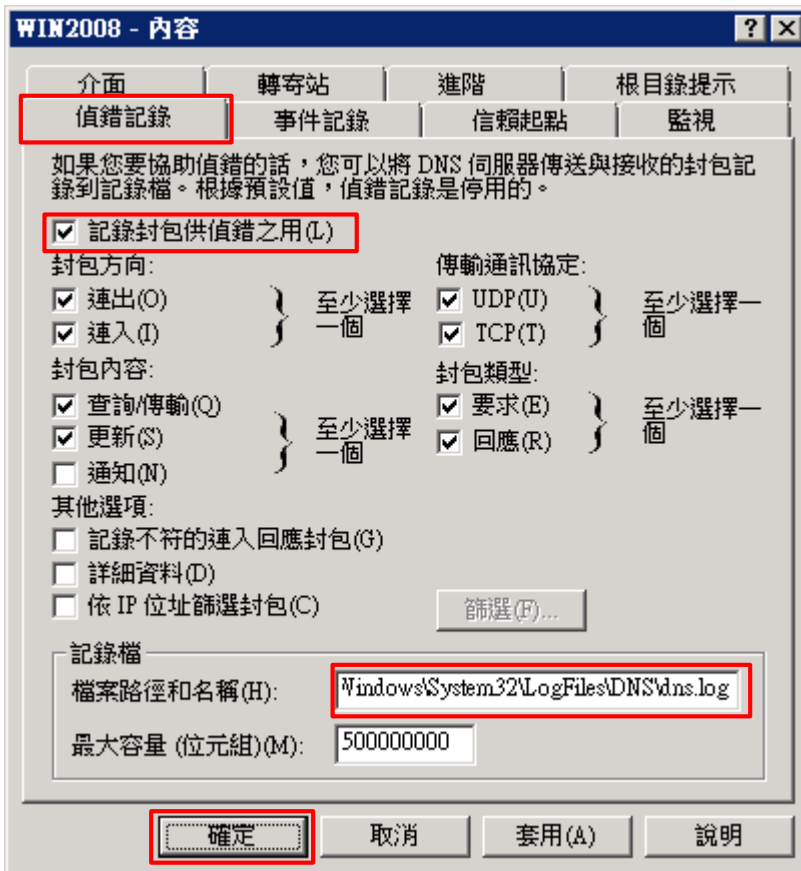


(4) 在 DNS 伺服器 [Win2008] 按滑鼠右鍵 -> 點選 [內容]



(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]

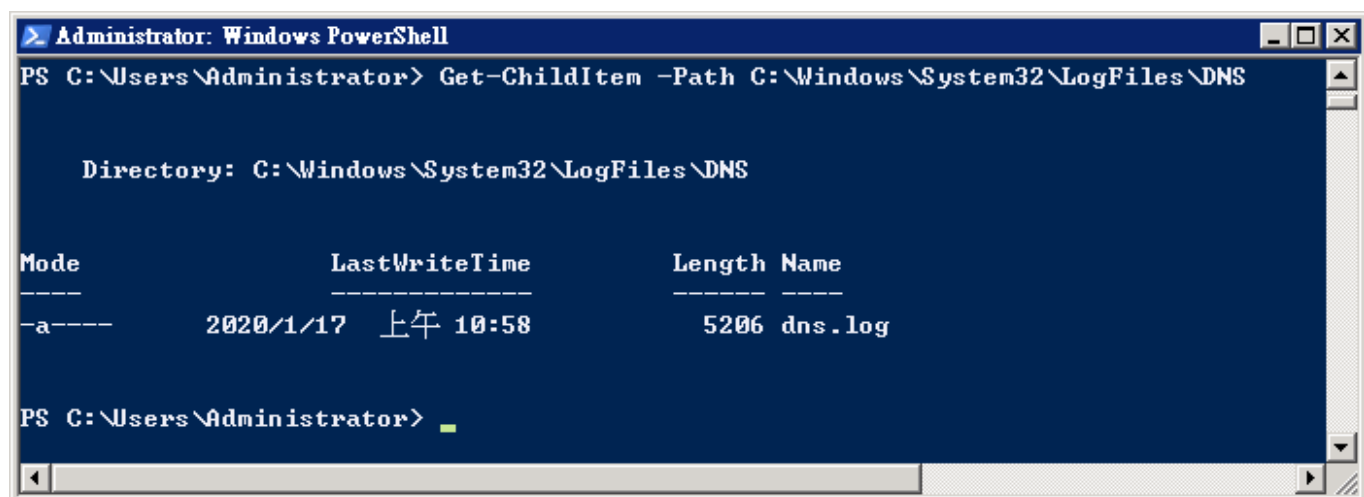


(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

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



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

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

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

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

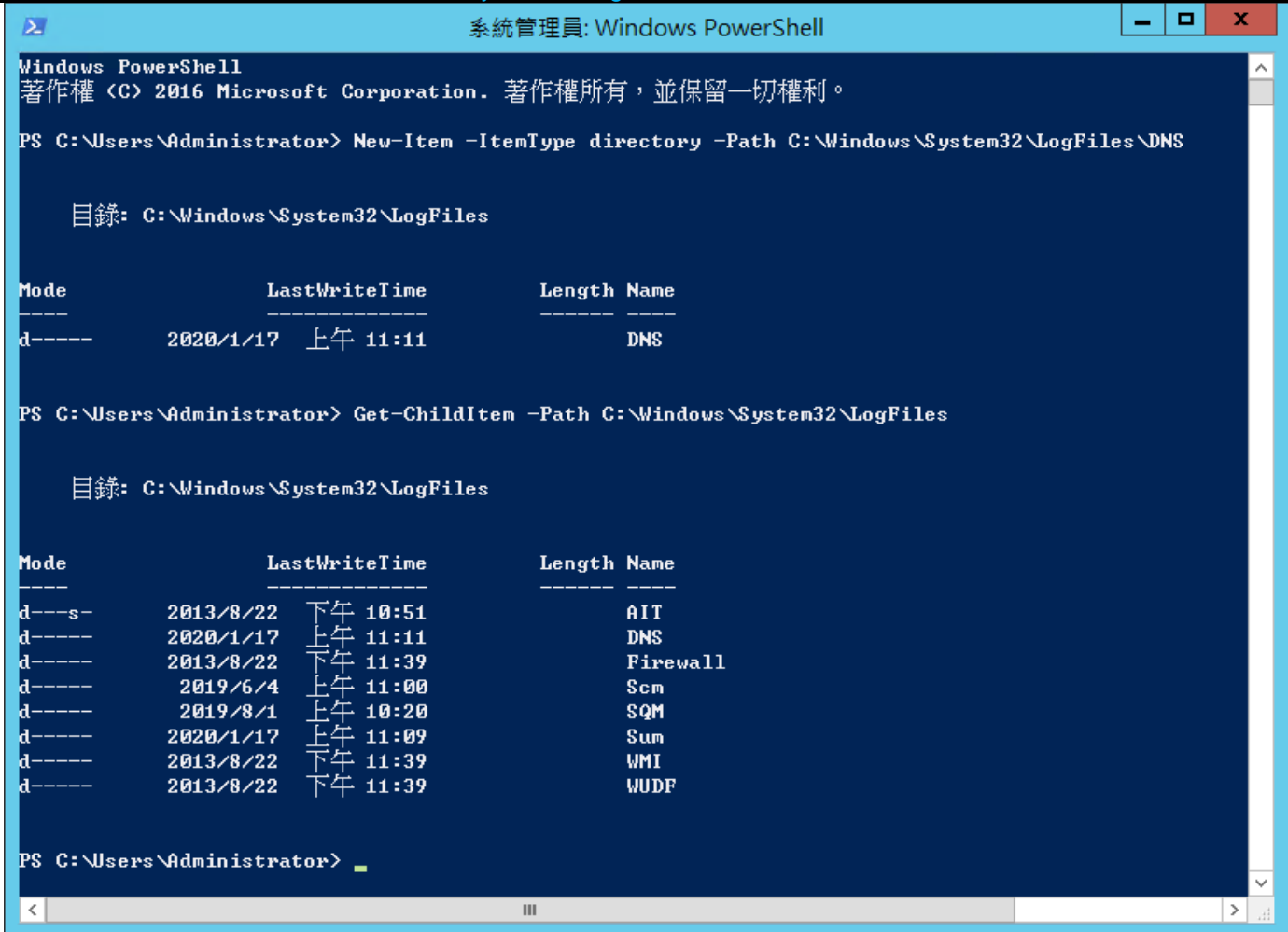
3. Windows 2012

(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
```

The screenshot shows a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window content is as follows:

Windows PowerShell
著作權 (C) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。

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

目錄: C:\Windows\System32\LogFiles

Mode	LastWriteTime	Length	Name
d----	2020/1/17 上午 11:11		DNS

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

目錄: C:\Windows\System32\LogFiles

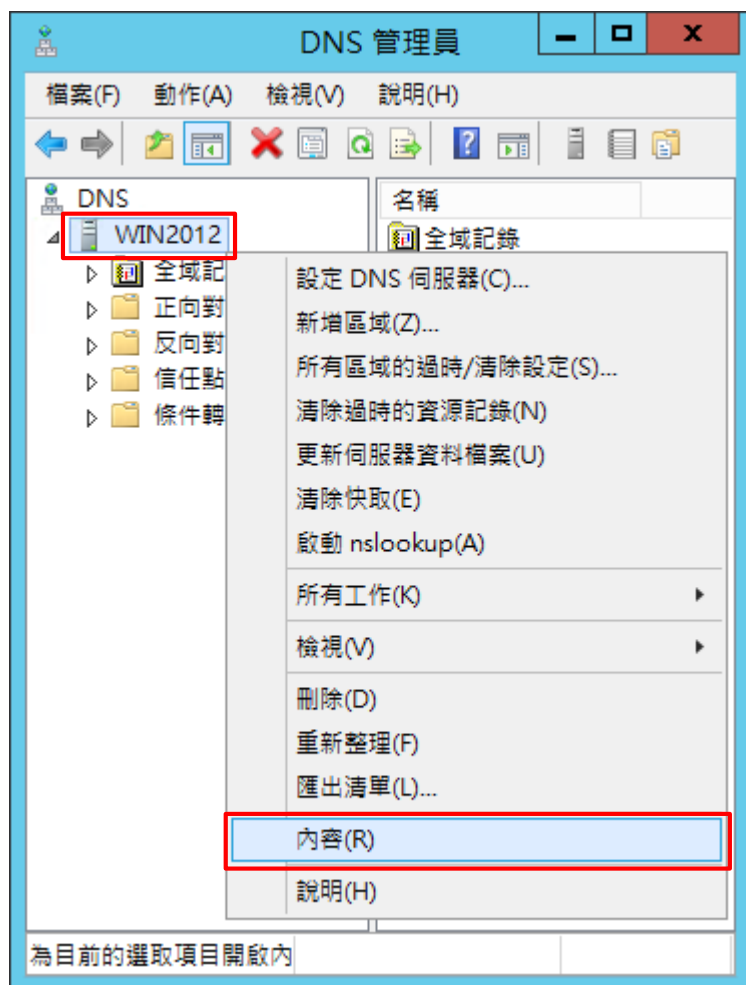
Mode	LastWriteTime	Length	Name
d---s-	2013/8/22 下午 10:51		AIT
d----	2020/1/17 上午 11:11		DNS
d-----	2013/8/22 下午 11:39		Firewall
d-----	2019/6/4 上午 11:00		Scm
d-----	2019/8/1 上午 10:20		SQM
d-----	2020/1/17 上午 11:09		Sum
d-----	2013/8/22 下午 11:39		WMI
d-----	2013/8/22 下午 11:39		WUDF

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

(3) 開啟 [DNS]

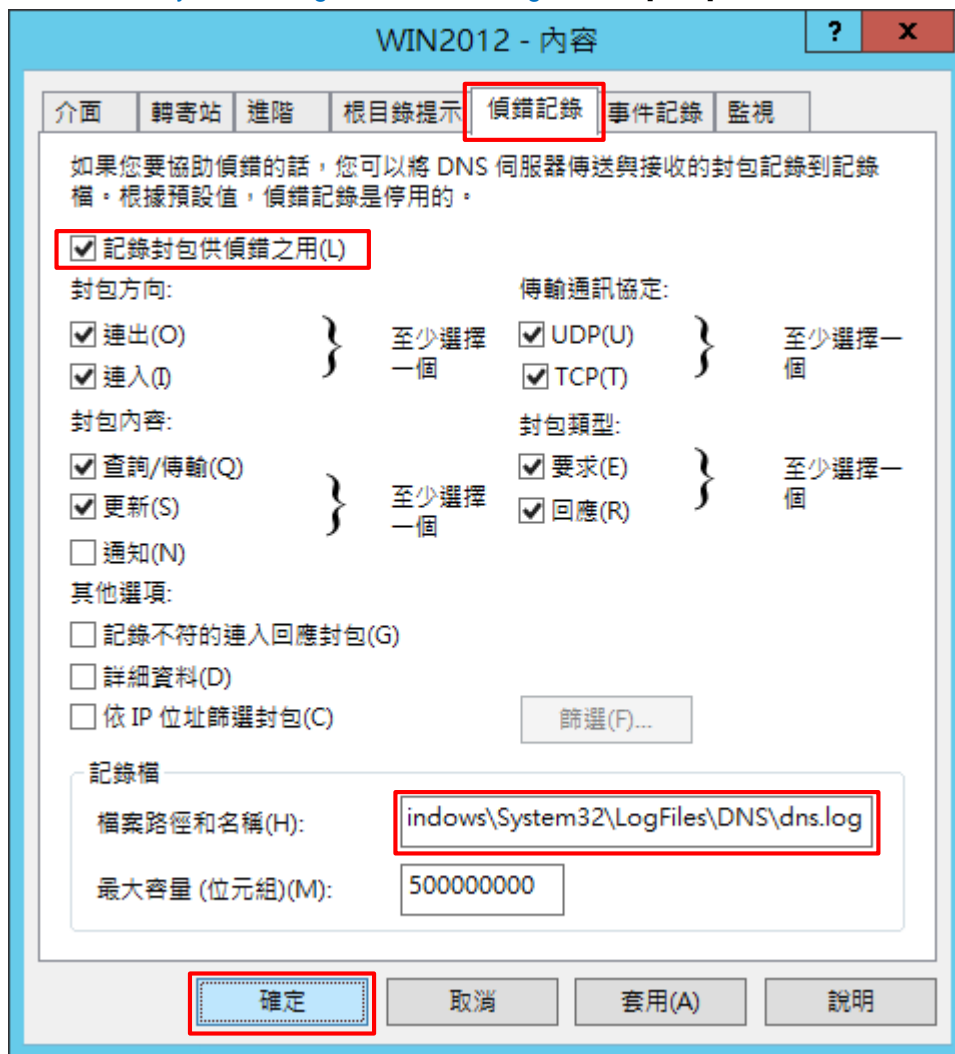


(4) 在 DNS 伺服器 [Win2012] 按滑鼠右鍵 -> 點選 [內容]



(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]

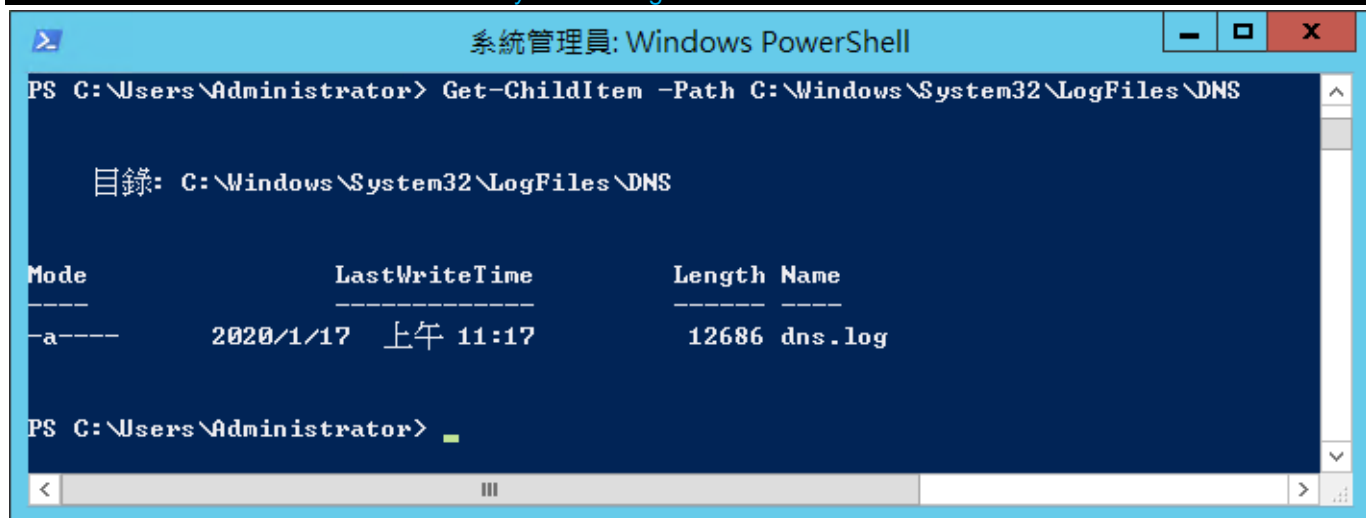


(6) 開啟 [Windows PowerShell]



(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

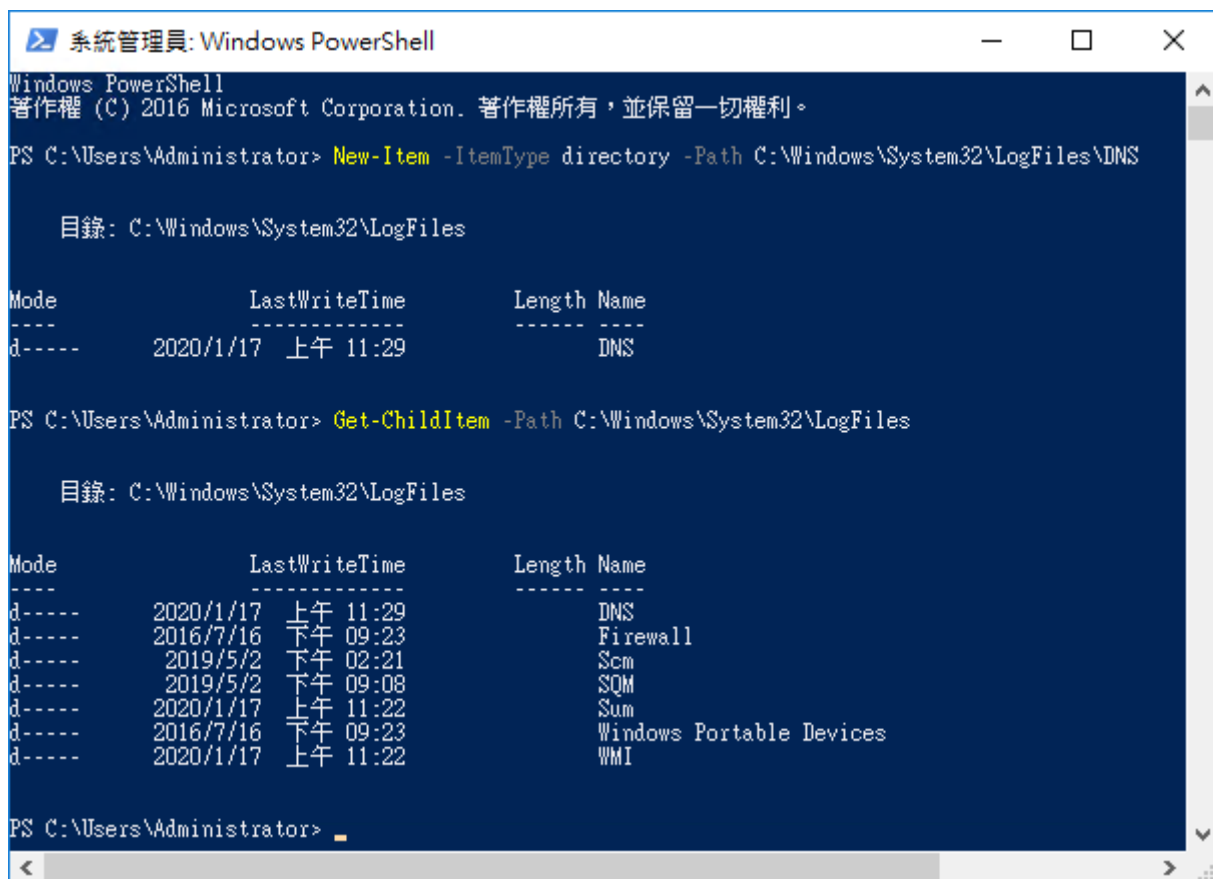
(1) 開啟 [Windows PowerShell]



(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
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The window shows the execution of two commands. The first command, `New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS`, creates a directory named "DNS" in the path `C:\Windows\System32\LogFiles`. The second command, `Get-ChildItem -Path C:\Windows\System32\LogFiles`, lists the contents of that directory. The output shows a table with columns for Mode, LastWriteTime, Length, and Name. The "DNS" directory is listed with a LastWriteTime of 2020/1/17 上午 11:29. Other directories listed include Firewall, Scm, SQM, Sum, Windows Portable Devices, and WMI.

```
Windows PowerShell
著作權 (C) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。

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

目錄: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----          2020/1/17 上午 11:29             DNS

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

目錄: C:\Windows\System32\LogFiles

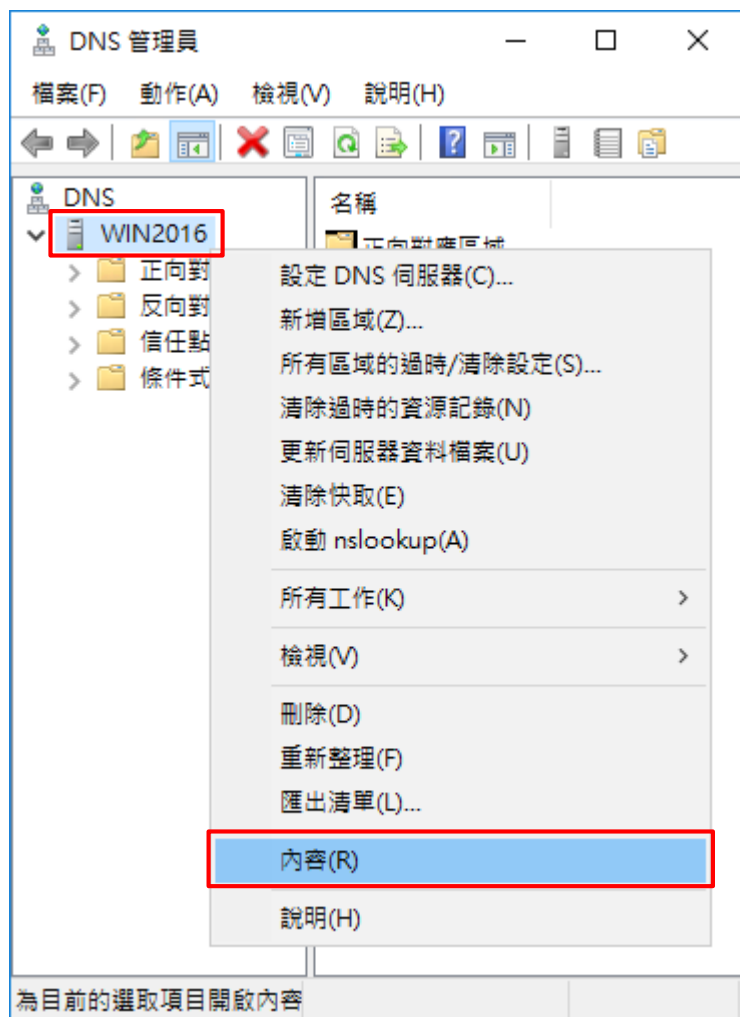
Mode                LastWriteTime         Length Name
----                -
d-----          2020/1/17 上午 11:29             DNS
d-----          2016/7/16 下午 09:23            Firewall
d-----          2019/5/2 下午 02:21             Scm
d-----          2019/5/2 下午 09:08             SQM
d-----          2020/1/17 上午 11:22             Sum
d-----          2016/7/16 下午 09:23    Windows Portable Devices
d-----          2020/1/17 上午 11:22             WMI

PS C:\Users\Administrator>
```

(3) 開啟 [DNS]

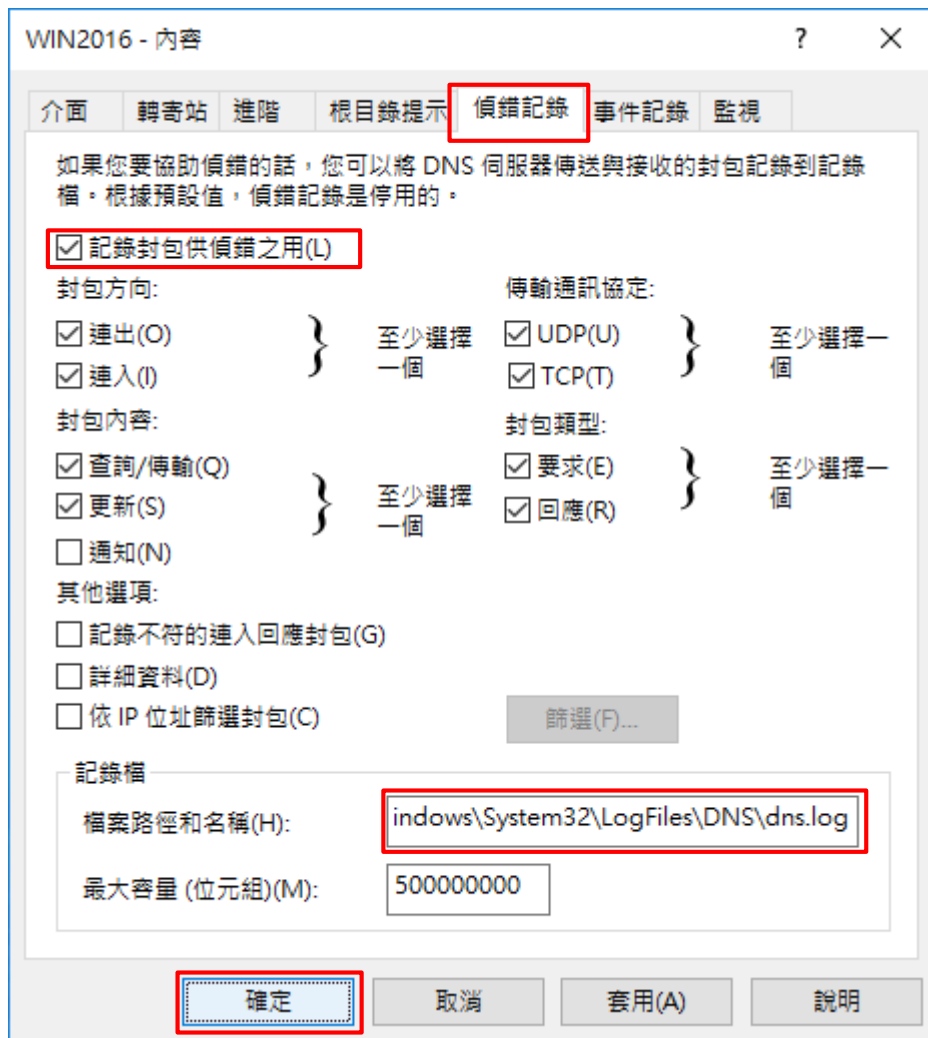


(4) 在 DNS 伺服器 [Win2016] 按滑鼠右鍵 -> 點選 [內容]



(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]

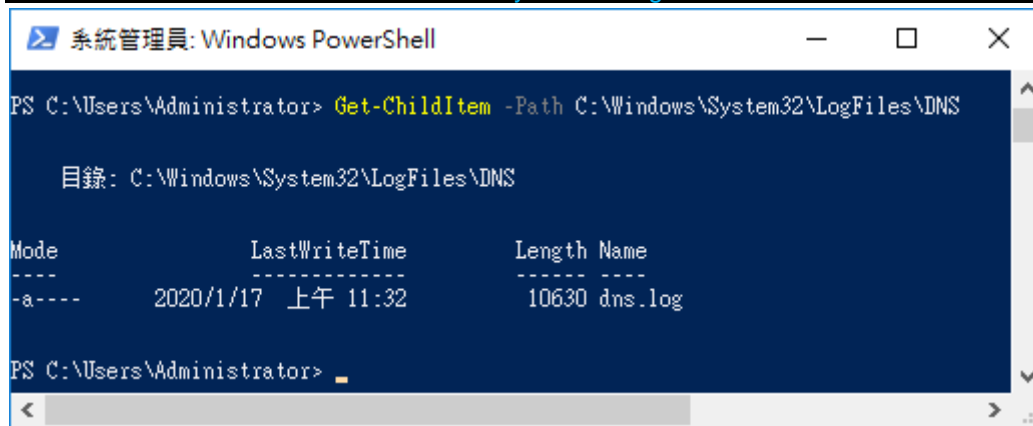


(6) 開啟 [Windows PowerShell]



(7) 確認有產生 dns.log 檔案

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



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

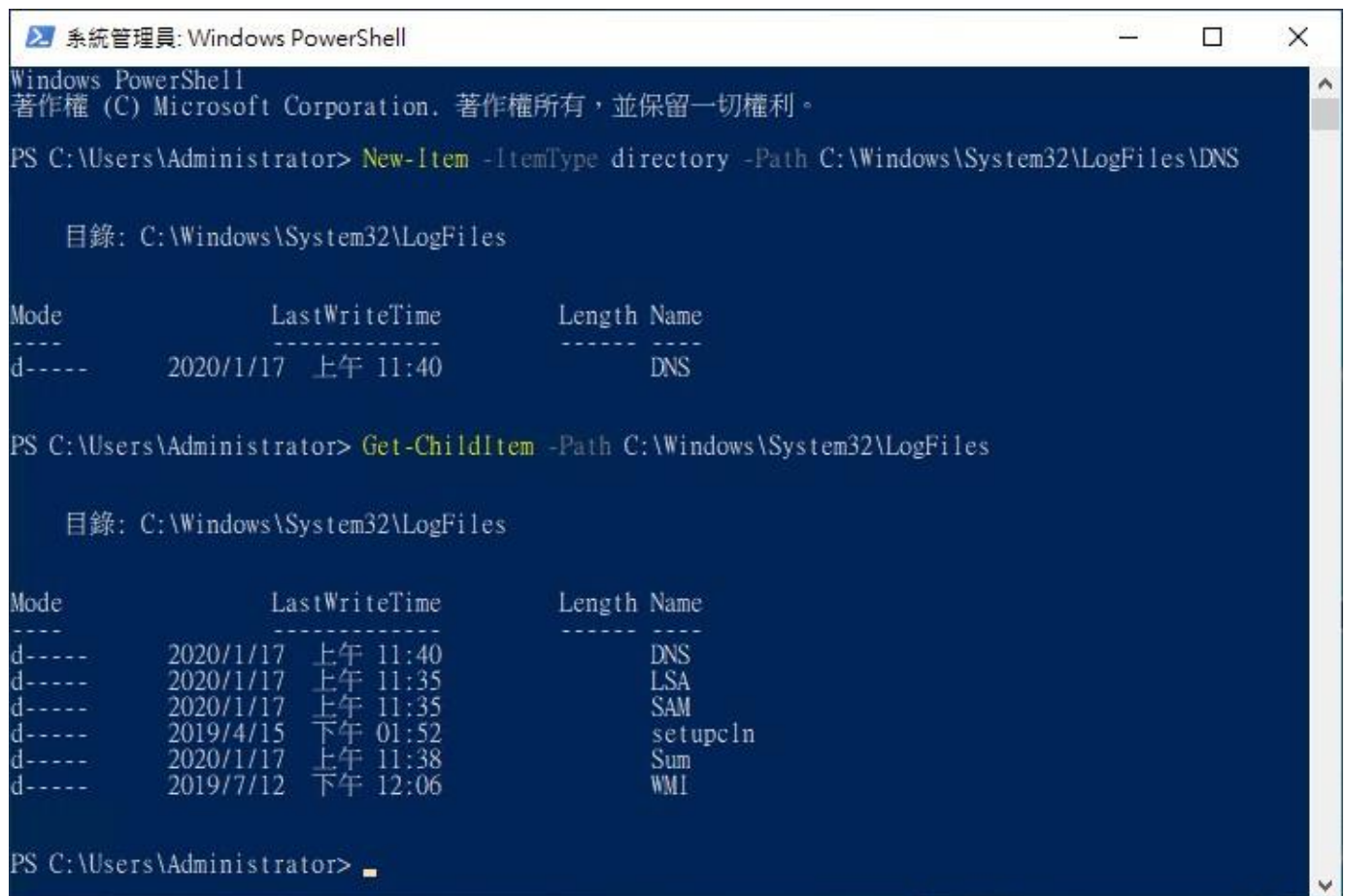
(1) 開啟 [Windows PowerShell]



(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
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window shows the execution of two commands. The first command, `New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS`, is followed by a directory listing for `C:\Windows\System32\LogFiles` showing a new directory named "DNS" created on 2020/1/17 at 11:40. The second command, `Get-ChildItem -Path C:\Windows\System32\LogFiles`, is followed by a directory listing showing several existing subdirectories: "DNS", "LSA", "SAM", "setupc\ln", "Sum", and "WMI".

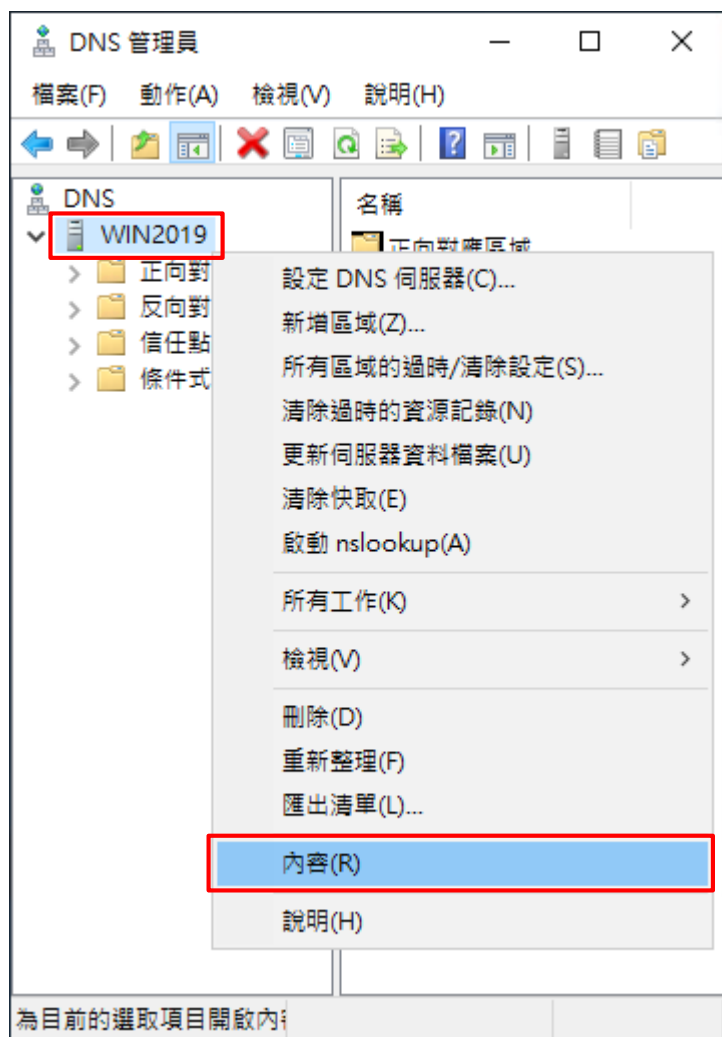
Mode	LastWriteTime	Length	Name
d-----	2020/1/17 上午 11:40		DNS

Mode	LastWriteTime	Length	Name
d-----	2020/1/17 上午 11:40		DNS
d-----	2020/1/17 上午 11:35		LSA
d-----	2020/1/17 上午 11:35		SAM
d-----	2019/4/15 下午 01:52		setupc\ln
d-----	2020/1/17 上午 11:38		Sum
d-----	2019/7/12 下午 12:06		WMI

(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)...

記錄檔

檔案路徑和名稱(H):

最大容量 (位元組)(M):

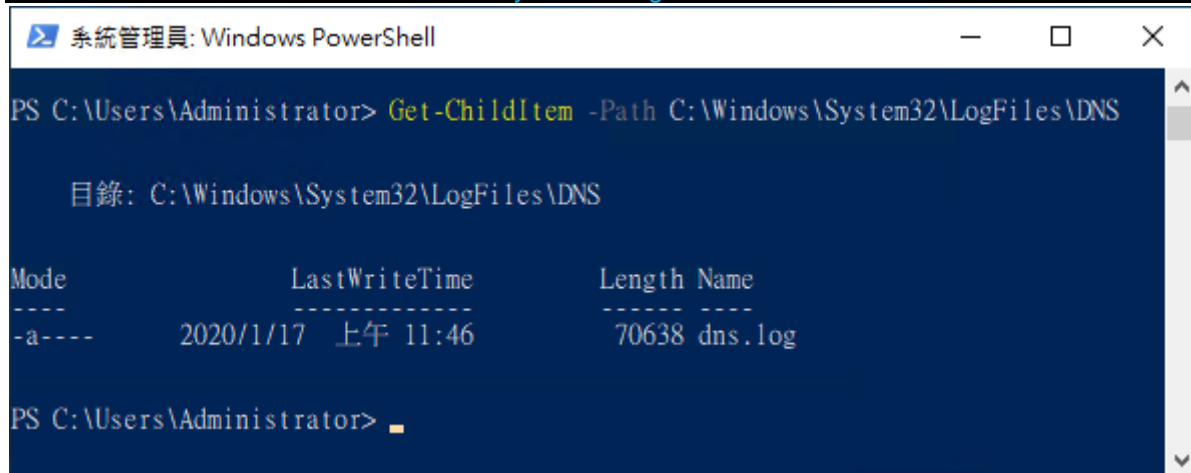
取消 套用(A) 說明

(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

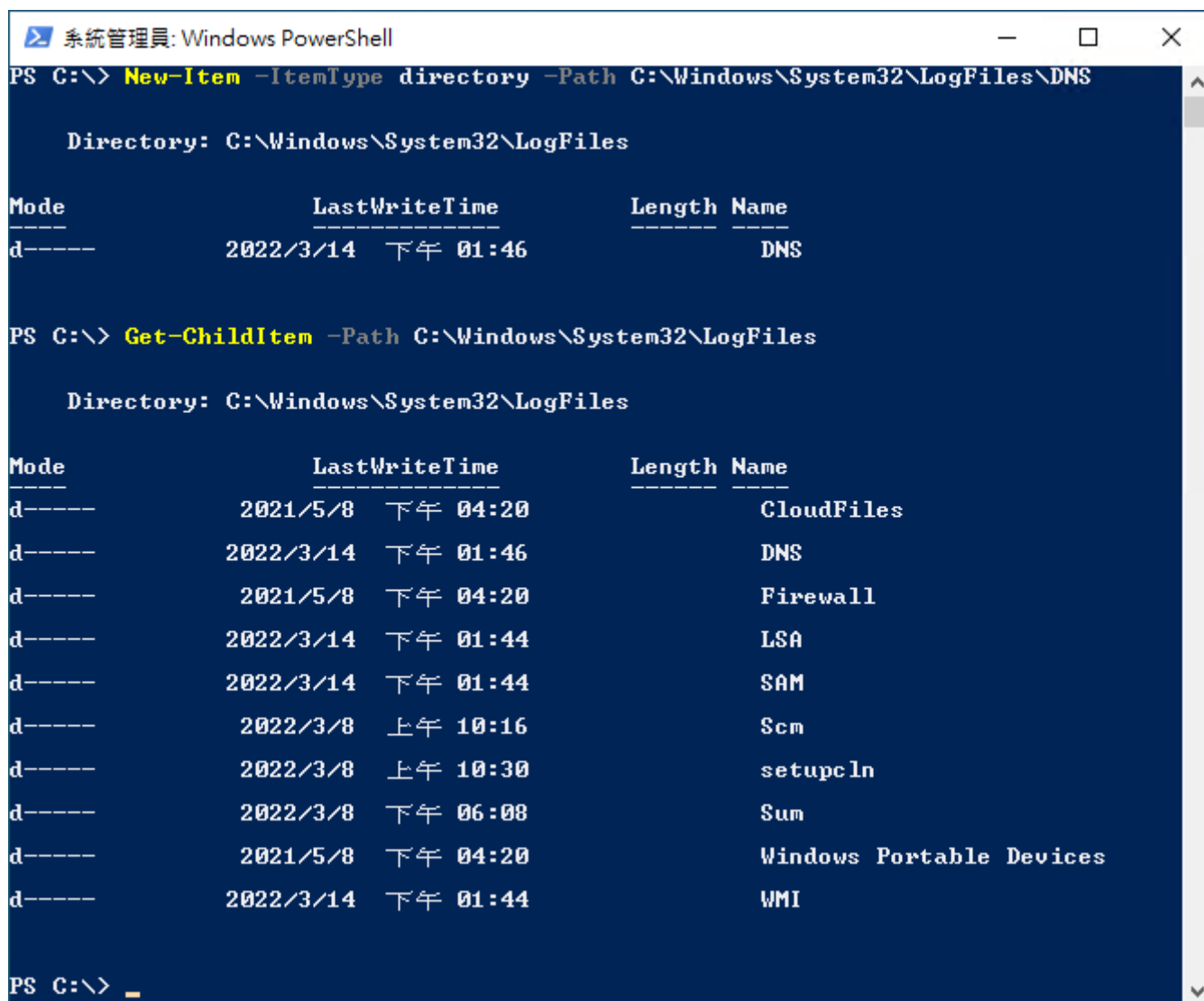
(1) 開啟 [Windows PowerShell]



(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
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window 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" under "C:\Windows\System32\LogFiles". The second command, "Get-ChildItem -Path C:\Windows\System32\LogFiles", lists the contents of that directory. The output shows a table of files and directories with columns for Mode, LastWriteTime, Length, and Name.

```
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

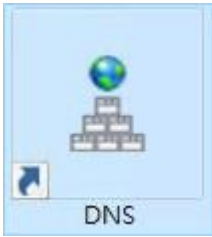
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

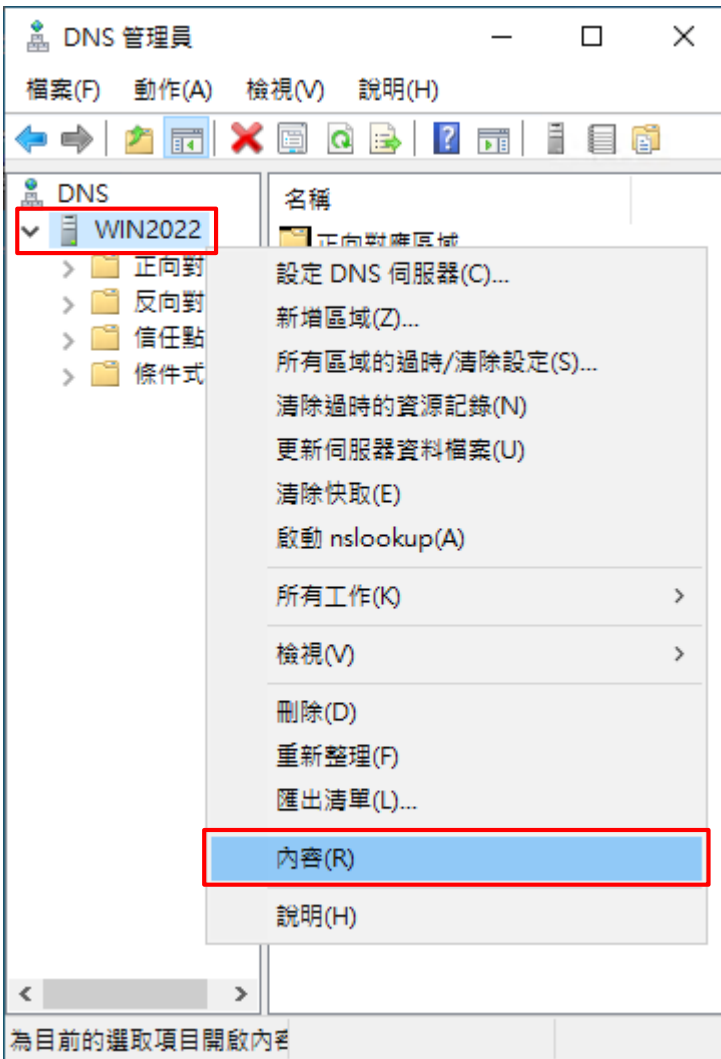
Mode                LastWriteTime         Length Name
----                -
d-----            2021/5/8 下午 04:20             CloudFiles
d-----            2022/3/14 下午 01:46             DNS
d-----            2021/5/8 下午 04:20             Firewall
d-----            2022/3/14 下午 01:44             LSA
d-----            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]

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: 傳輸通訊協定:

連出(O) } 至少選擇一個 UDP(U) } 至少選擇一個

連入(I) } TCP(T) }

封包內容: 封包類型:

查詢/傳輸(Q) } 至少選擇一個 要求(E) } 至少選擇一個

更新(S) } 回應(R) }

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):

最大容量 (位元組)(M):

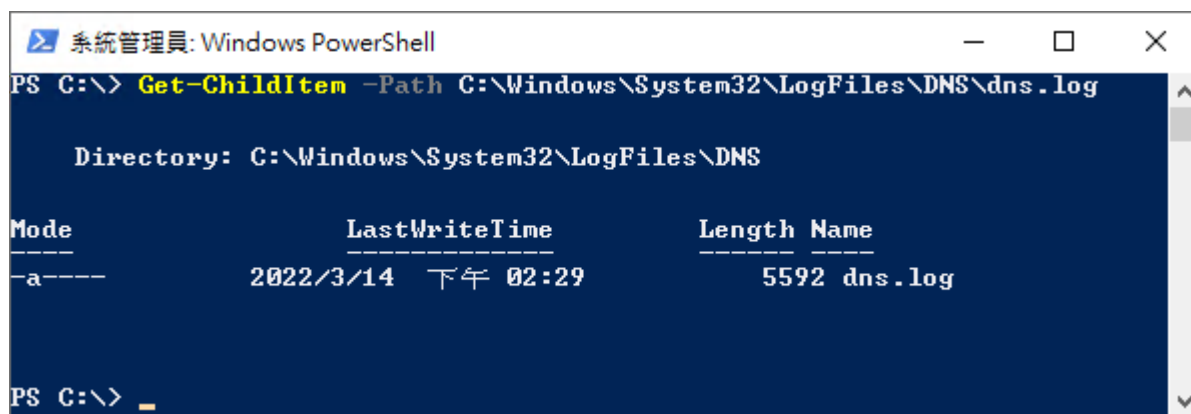
取消 套用(A) 說明

(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\dns.log
```



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command executed is `Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS\dns.log`. The output displays the directory path and a table of file details.

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

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

The prompt at the bottom is `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]

The screenshot displays the N-Reporter web application interface. On the left is a dark blue sidebar menu with the following items: 'Admin (Global)' (with a dropdown arrow), '事件' (Events), '報表' (Reports), '智慧分析' (Smart Analysis), '設備管理' (Device Management) - this item and its sub-menu are highlighted with a red box, '系統管理' (System Management), and '使用者手冊' (User Manual). The sub-menu under '設備管理' includes '設備樹狀圖' (Device Tree), '介面列表' (Interface List), '告警樣版' (Alert Template), and '設備異常告警' (Device Abnormal Alert). The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖'. Below the breadcrumb is a search bar with the text '搜尋' and buttons for search, refresh, add (highlighted with a red box), update, and back. The main content area displays a tree structure with 'Global (4)' and '未知設備 (0)' (Unknown Devices).

(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]

新增設備

設備基本設定

名稱
WinDNS-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 DNS

使用自定義資料格式

Facility
(19) local use 3 (local3)

編碼方式
UTF-8

日誌保留 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

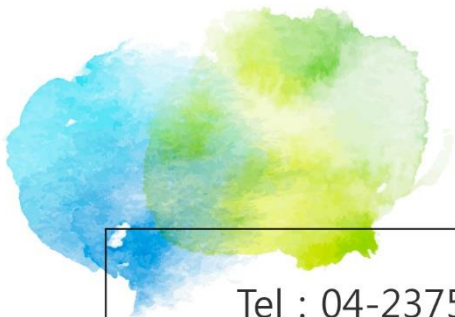
告警通報設定
預設

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



Tel : 04-23752865 Fax : 04-23757458

業務詢問 : sales@npartner.com

技術詢問 : support@npartner.com