

Partner

如何設定 Windows IIS log

V019

2023/11/17



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.....	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
□ 記錄所有資訊設定檔.....	7
□ 不紀錄 Cookie 資訊設定檔.....	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 2000	15
3. Windows 2003	20
4. Windows 2008	27
4. Windows 2012	42
5. Windows 2016	49
6. Windows 2019	57
7. Windows 2022	65
8. N-Reporter	72

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 IIS(Internet Information Server) 記錄。

NXLog 工具將 Windows IIS 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 Windows Server 2000 / 2003 / 2008 / 2012 / 2016 / 2019 / 2022 的版本。

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

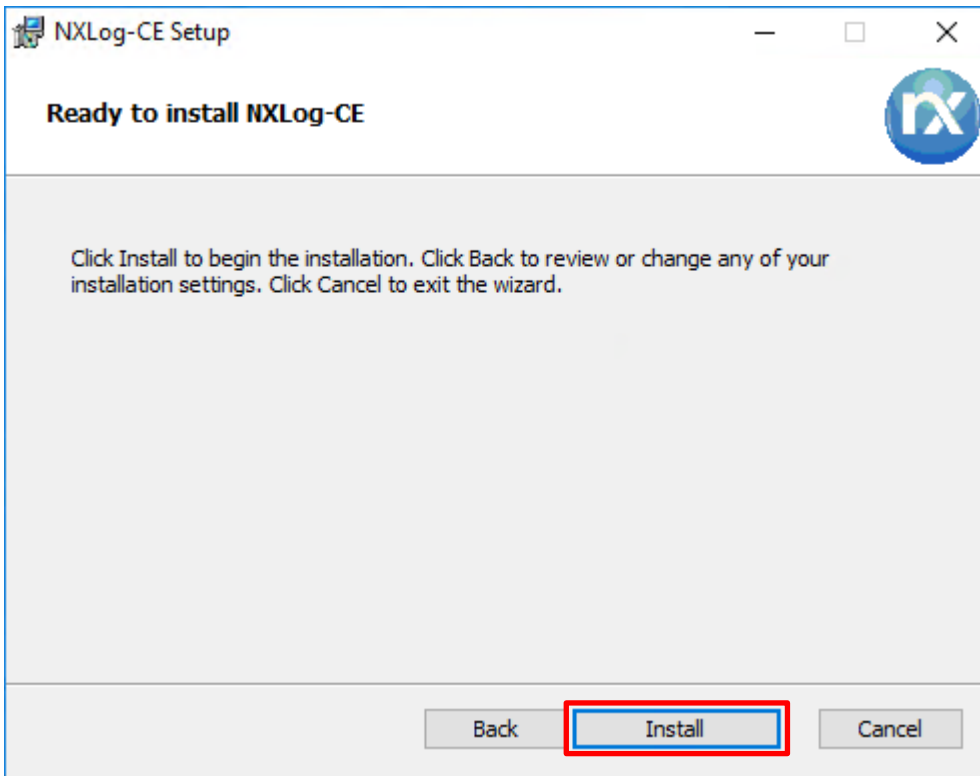
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```

```
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

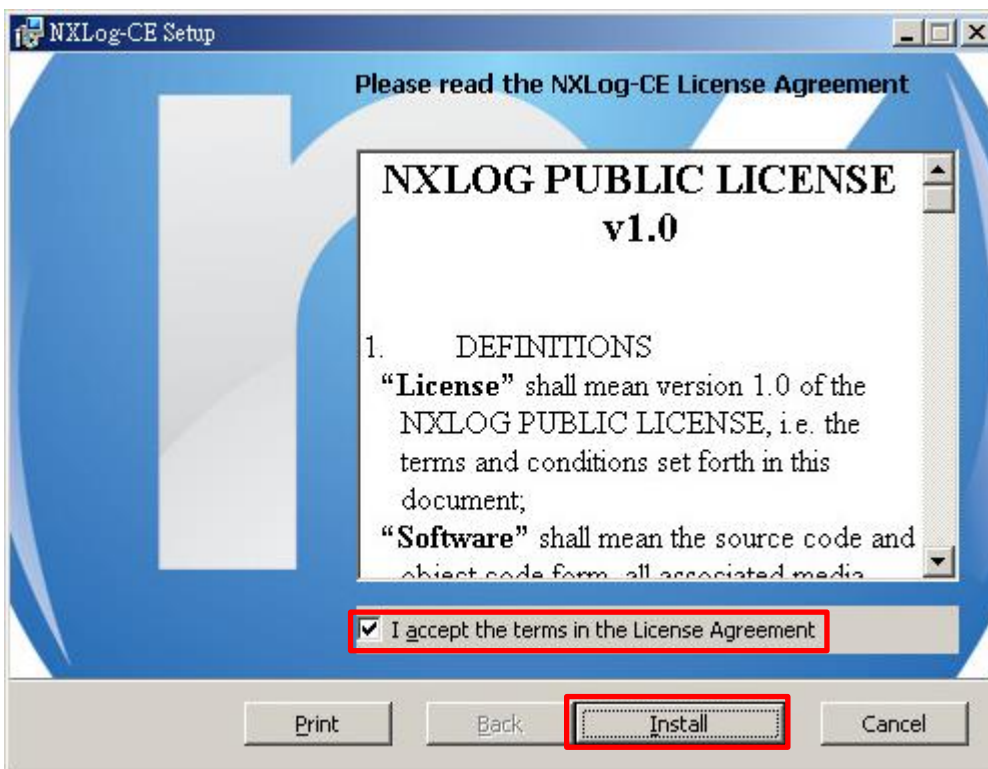
<2.2> Windows 2003

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



<2.3> Windows 2000

點擊 [nxlog-ce-2.9.1716.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) 依據需求選擇下載 NXLog Windows IIS 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔。

1. 記錄所有資訊設定檔:

下載連結：http://www.npartner.com/download/tech/nxlog_WinIIS.conf

2. 不紀錄 Cookie 資訊設定檔:

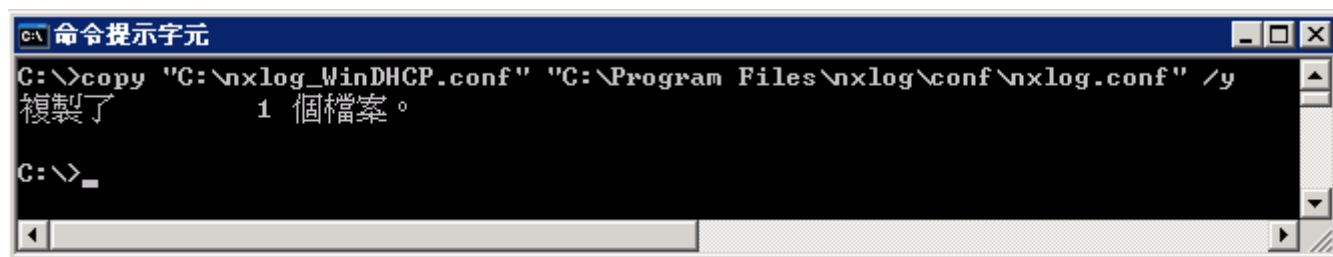
下載連結：http://www.npartner.com/download/tech/nxlog_WinIIS_no_cookie.conf

記錄所有資訊設定檔複製指令:

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

不紀錄 Cookie 資訊設定檔複製指令:

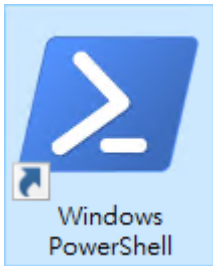
```
C:\> copy "C:\nxlog_WinIIS_no_cookie.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



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) 依據需求選擇下載 NXLog Windows IIS 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔。

1. 記錄所有資訊設定檔:

下載連結：http://www.npartner.com/download/tech/nxlog_WinIIS.conf

2. 不紀錄 Cookie 資訊設定檔:

下載連結：http://www.npartner.com/download/tech/nxlog_WinIIS_no_cookie.conf

記錄所有資訊設定檔命令下載方式:

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



不紀錄 Cookie 資訊設定檔命令下載方式:

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_WinIIS_no_cookie.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

■ 記錄所有資訊設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud    192.168.8.4
define IISpath  C:\inetpub\logs\LogFiles
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 Microsoft IIS(Internet Information Server) log file use the following:
<Input in_iislog>
  Module im_file
  File '%IISpath%\u_ex*.log'
  SavePos TRUE
  ReadFromLast TRUE
  Recursive TRUE
</Input>

<Output out_iislog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 22;
  Exec $raw_event = "IIS [info]: " + $raw_event ;
  Exec to_syslog_bsd();
</Output>

<Route iislog>
  Path in_iislog => out_iislog
</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
```

藍色文字部位請輸入 IIS 路徑

```
define IISpath  C:\inetpub\logs\LogFiles
```

■ 不紀錄 Cookie 資訊設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define IISpath C:\inetpub\logs\LogFiles
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 Microsoft IIS(Internet Information Server) log file use the following:
<Input in_iislog>
  Module im_file
  File '%IISpath%\u_ex*.log'
  SavePos TRUE
  ReadFromLast TRUE
  Recursive TRUE
</Input>

<Output out_iislog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 22;
  Exec $raw_event = "IIS [no_cookie]: " + $raw_event ;
  Exec to_syslog_bsd();
</Output>

<Route iislog>
  Path in_iislog => out_iislog
</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
```

藍色文字部位請輸入 IIS 路徑

```
define IISpath C:\inetpub\logs\LogFiles
```

1.4 NXLog 啟動服務

1.4.1 Windows 2003 或之前版本作業系統

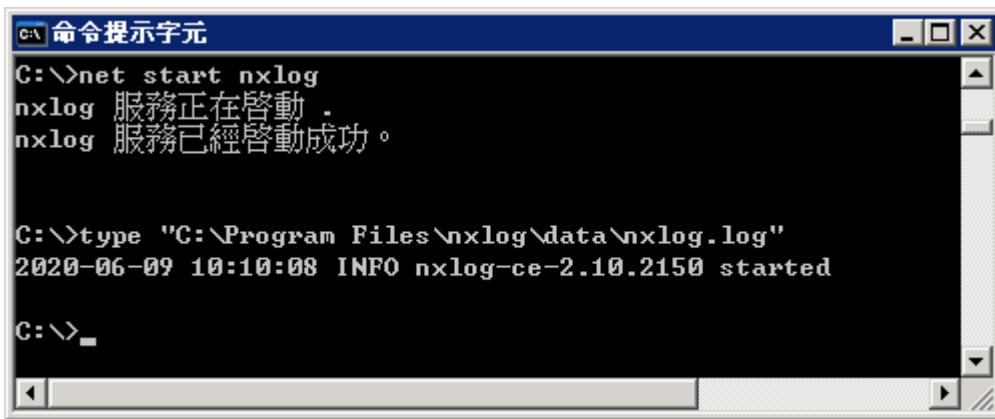
(1) 開啟 [命令提示字元]



(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"
```



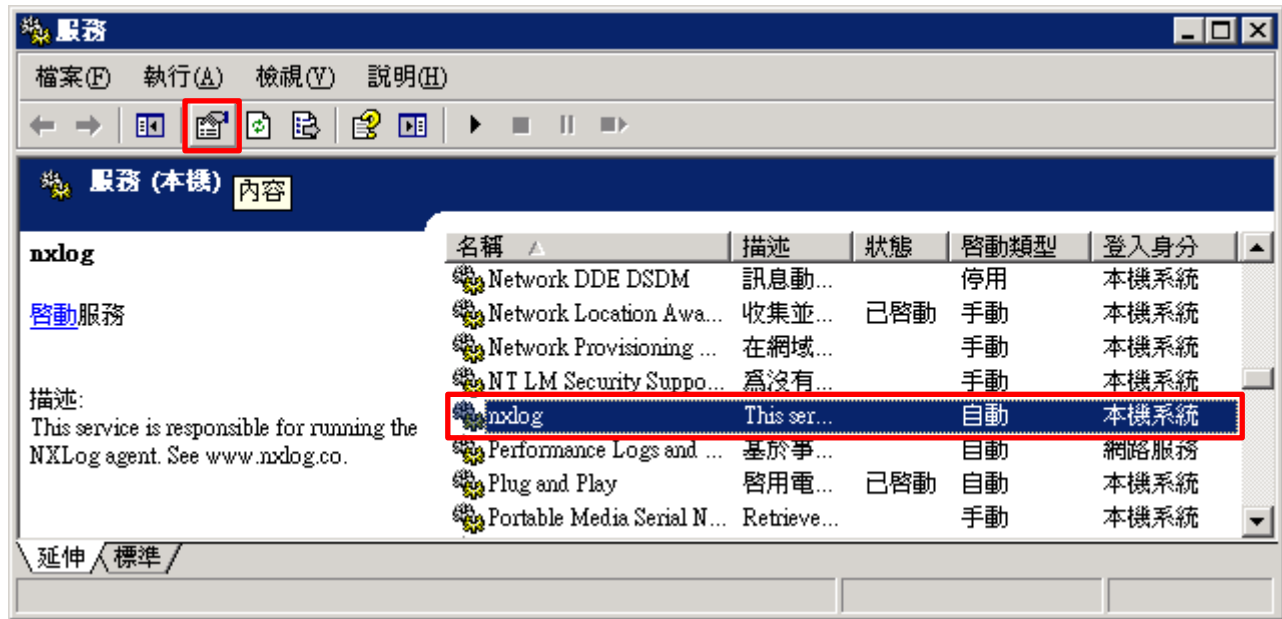
(3) 開啟 [服務] 功能

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

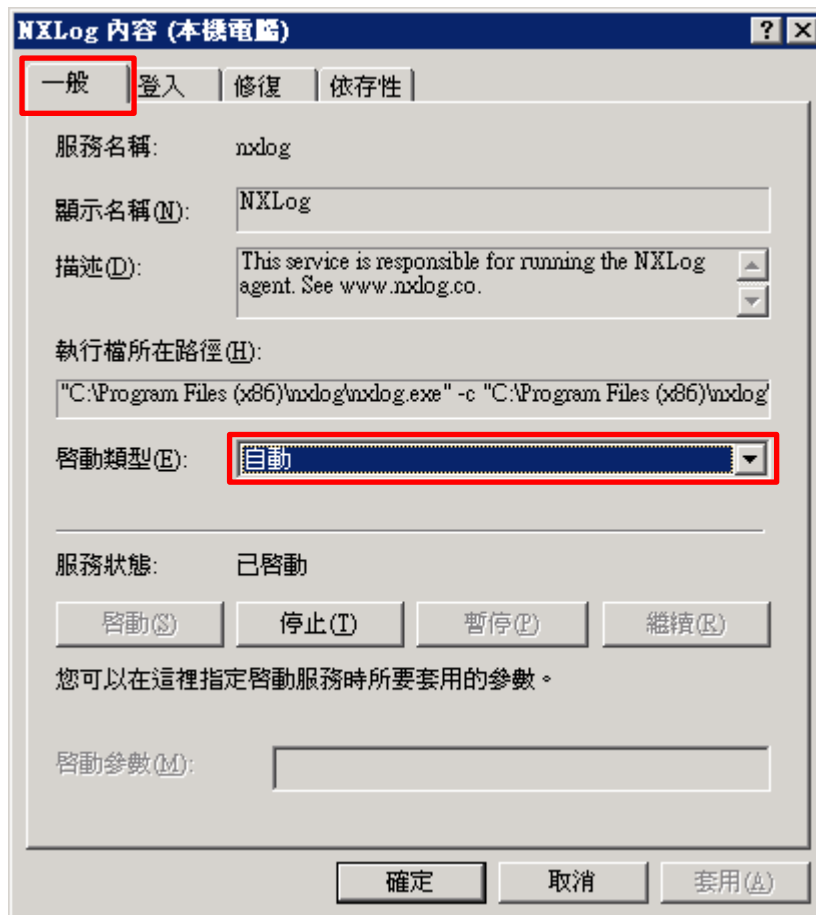


(4) 開啟 NXLog 服務內容

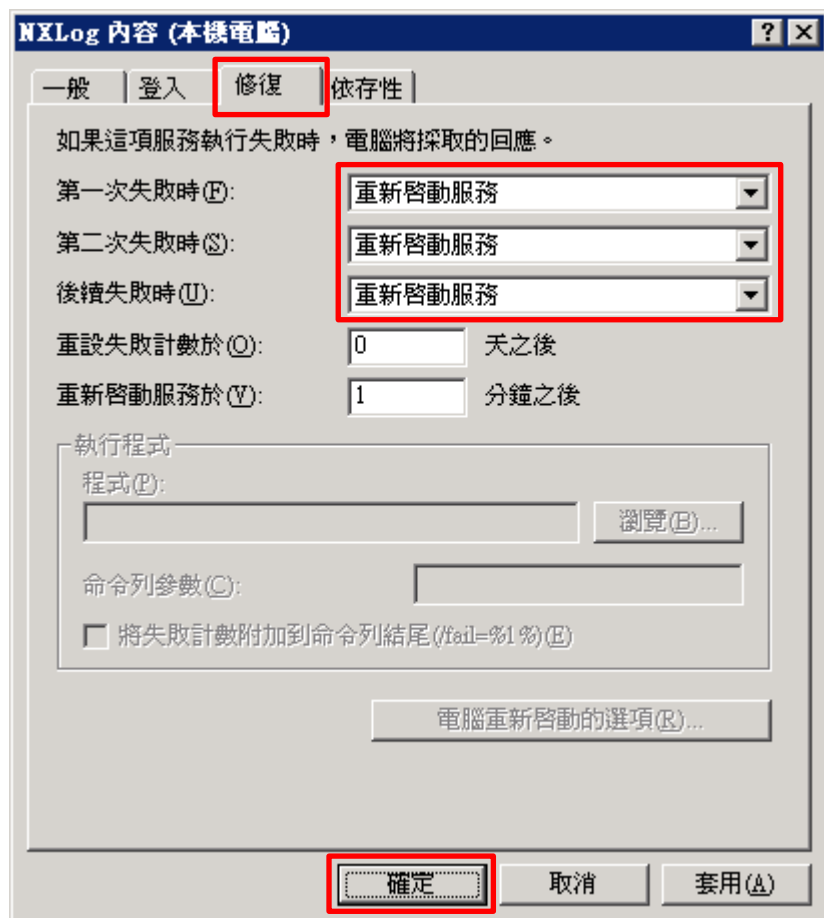
選擇 [nxlog] -> 點選  [內容]



(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]



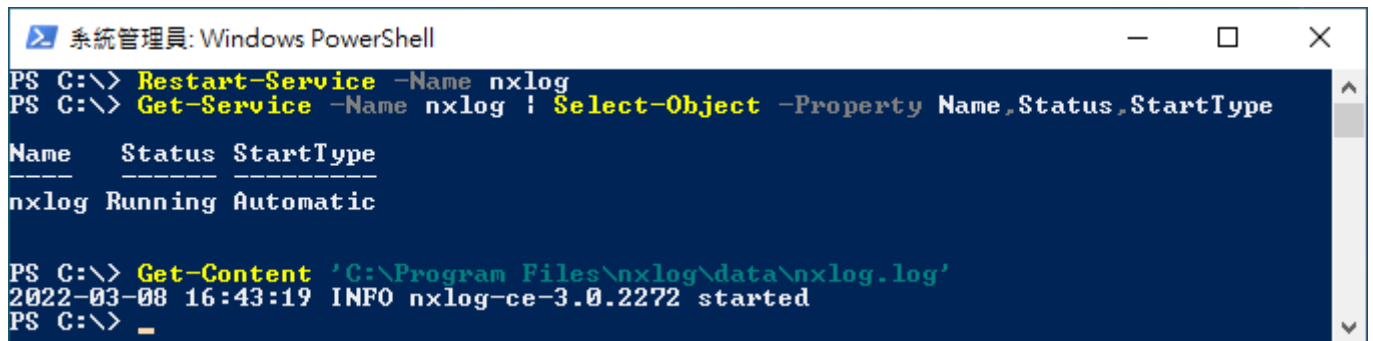
1.4.2 Windows 2008 或之後版本作業系統

(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'
```

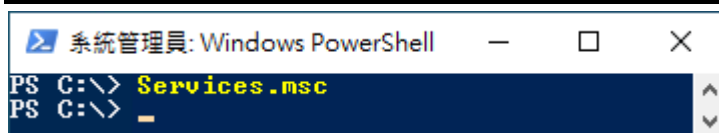
A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has standard Windows window controls (minimize, maximize, close). The command prompt shows the following commands and output:

```
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

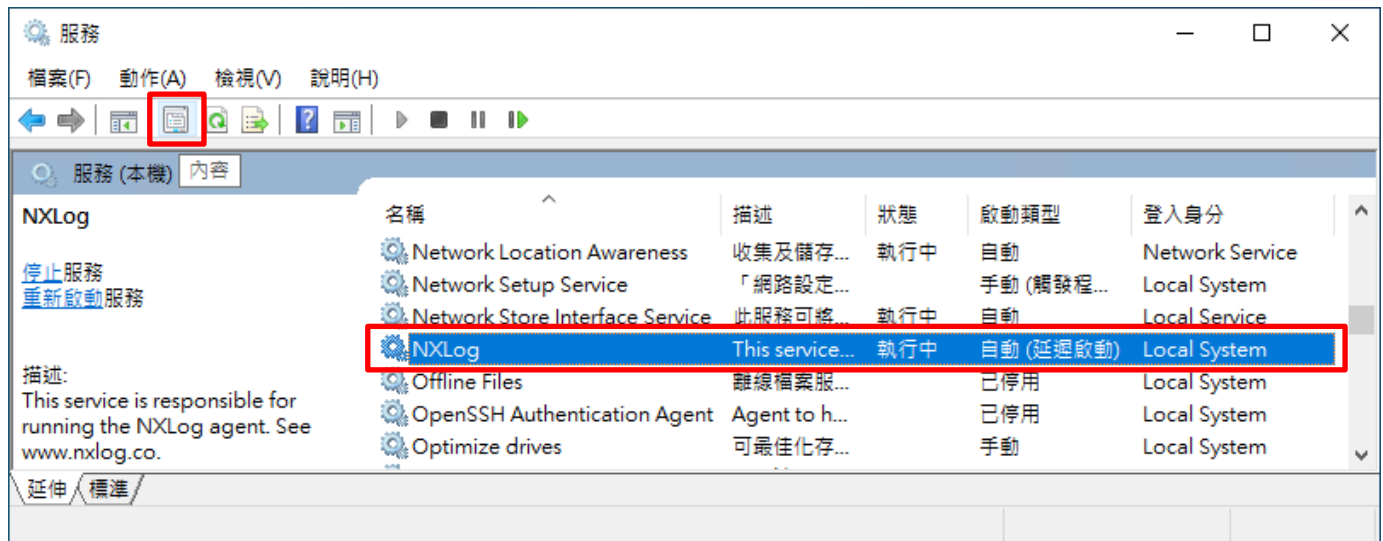
```
PS C:\> Services.msc
```

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

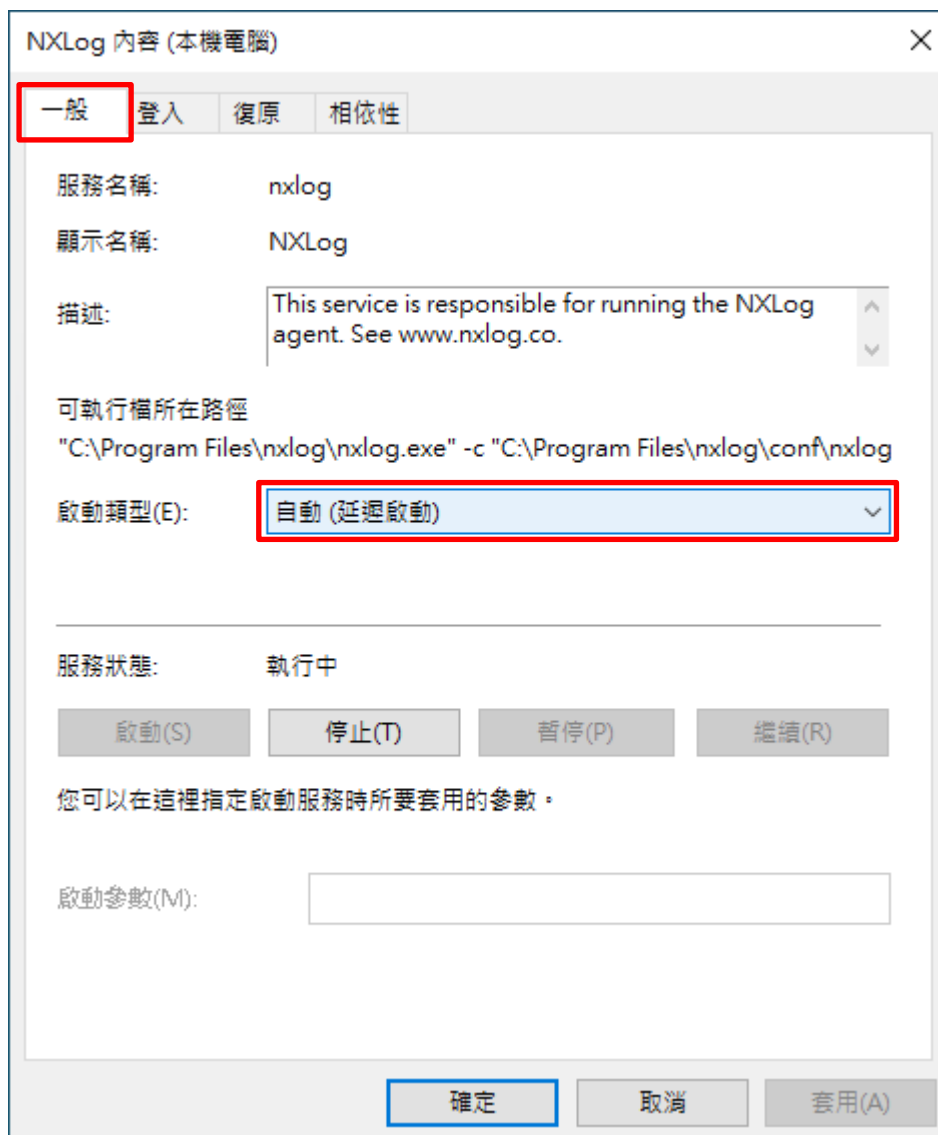
```
PS C:\> Services.msc
PS C:\> _
```

(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):

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 2000

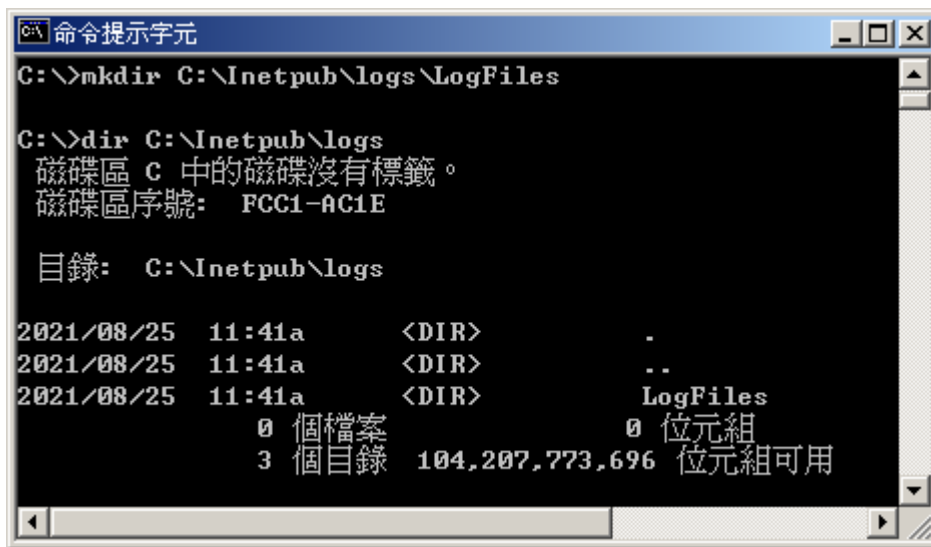
(1) 開啟 [命令提示字元]



(2) 新增 IIS LogFiles 資料夾和確認 IIS LogFiles 資料夾

```
C:\> mkdir C:\inetpub\logs\LogFiles
```

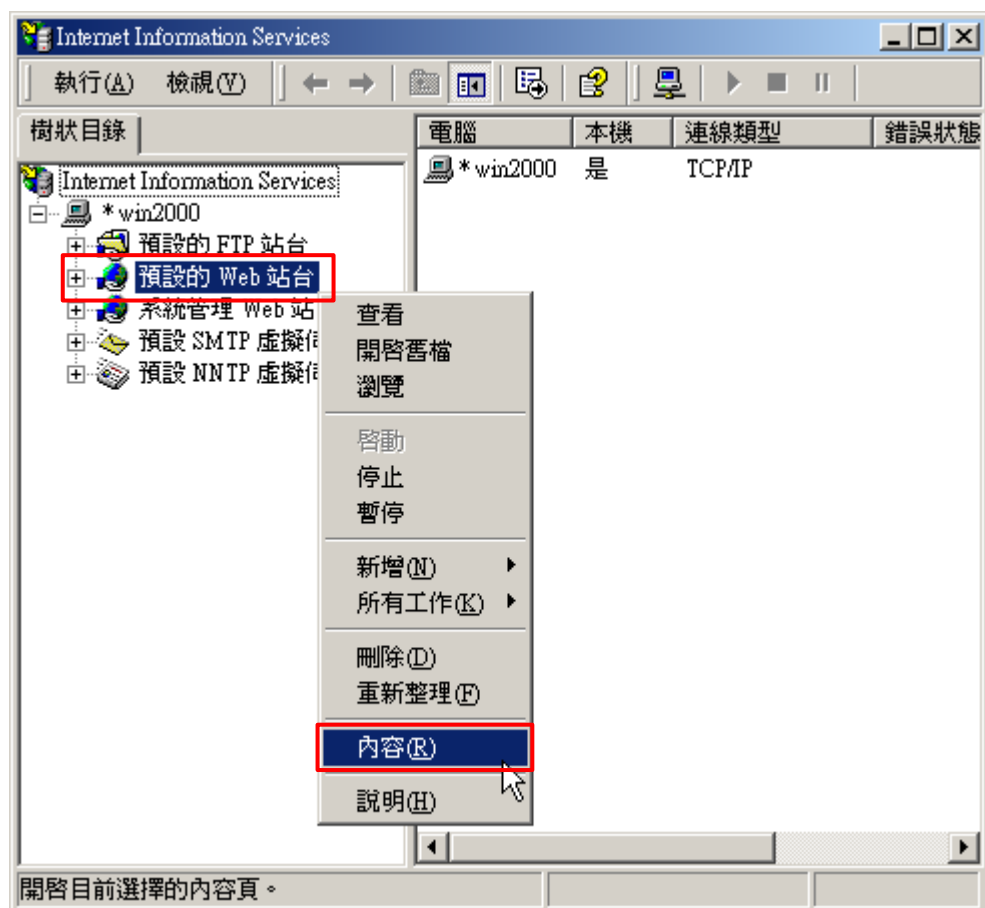
```
C:\> dir C:\inetpub\logs
```



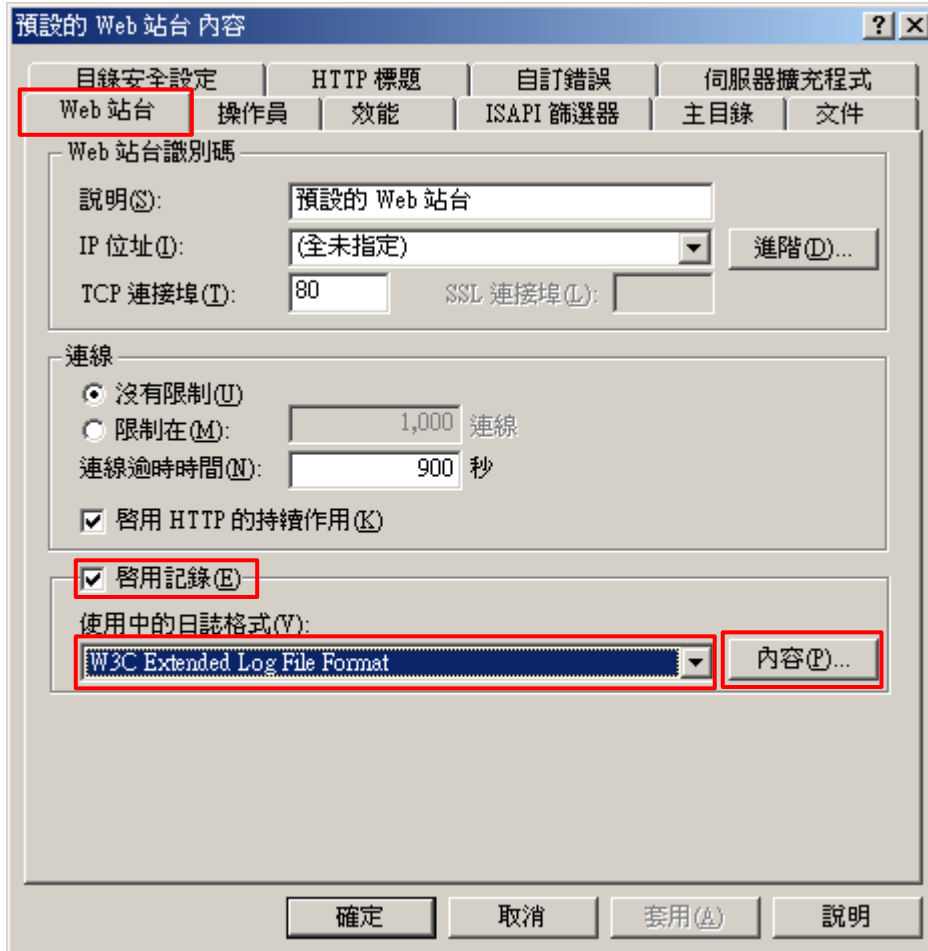
(3) 開啟 [Internet 服務管理員]



(4) 在 [Web 站台] 上按滑鼠右鍵 -> 選擇 [內容]

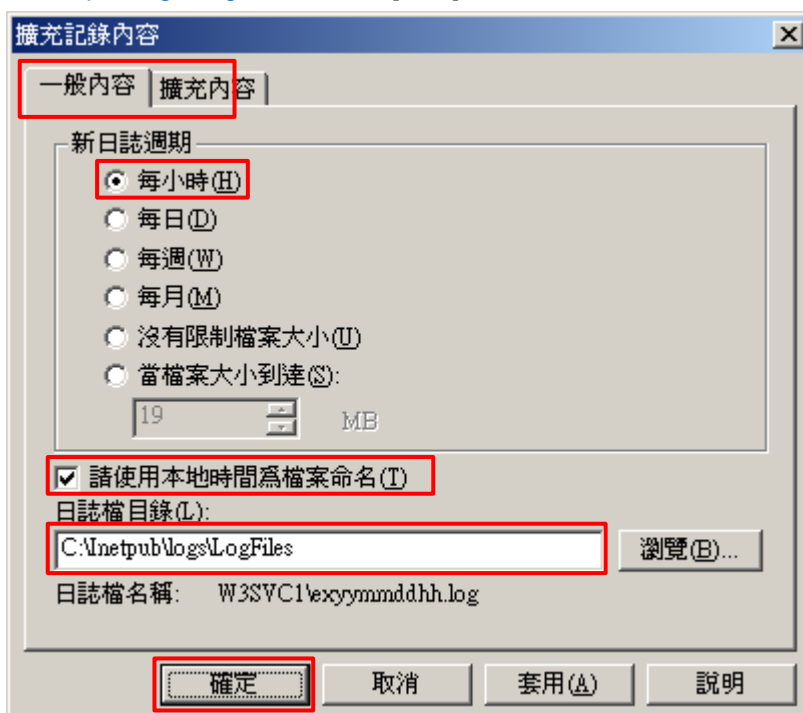


(5) [網站] 頁面: 勾選 [啟用記錄] -> 使用中的日誌格式選擇 [W3C Extended Log File Format] -> 按 [內容]



(6) [一般內容] 頁面: 新日誌週期點選 [每小時] -> 勾選 [請使用本地時間為檔案命名] -> 日誌檔目錄輸入

C:\inetpub\logs\LogFiles -> 按 [確定]

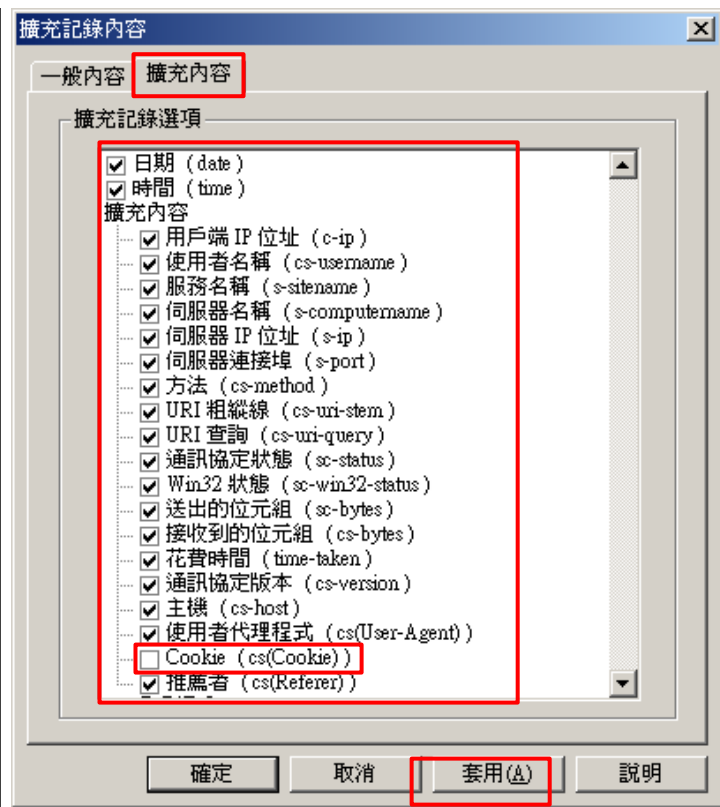
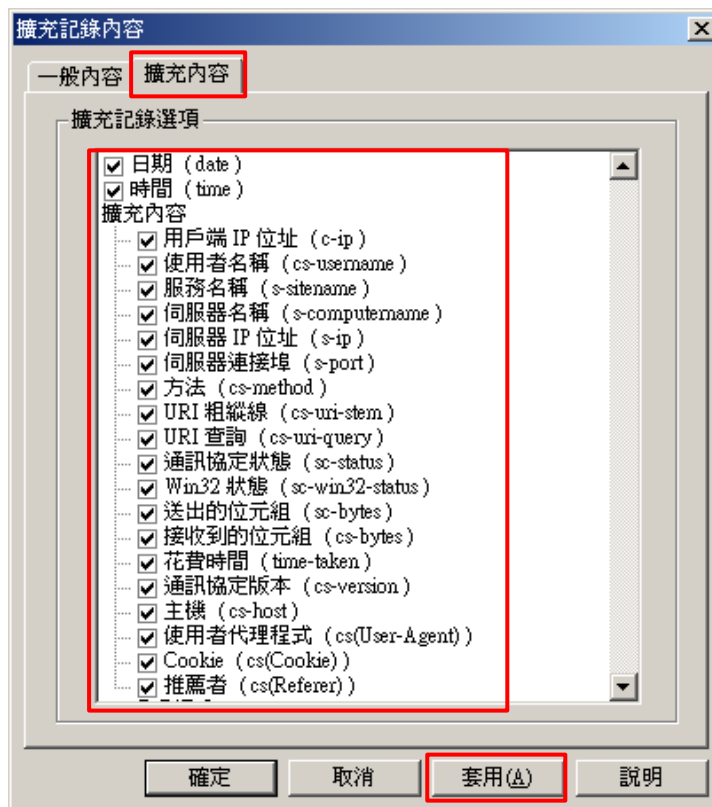


(7) [擴充內容] 頁面：擴充記錄選項勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按 [套用]

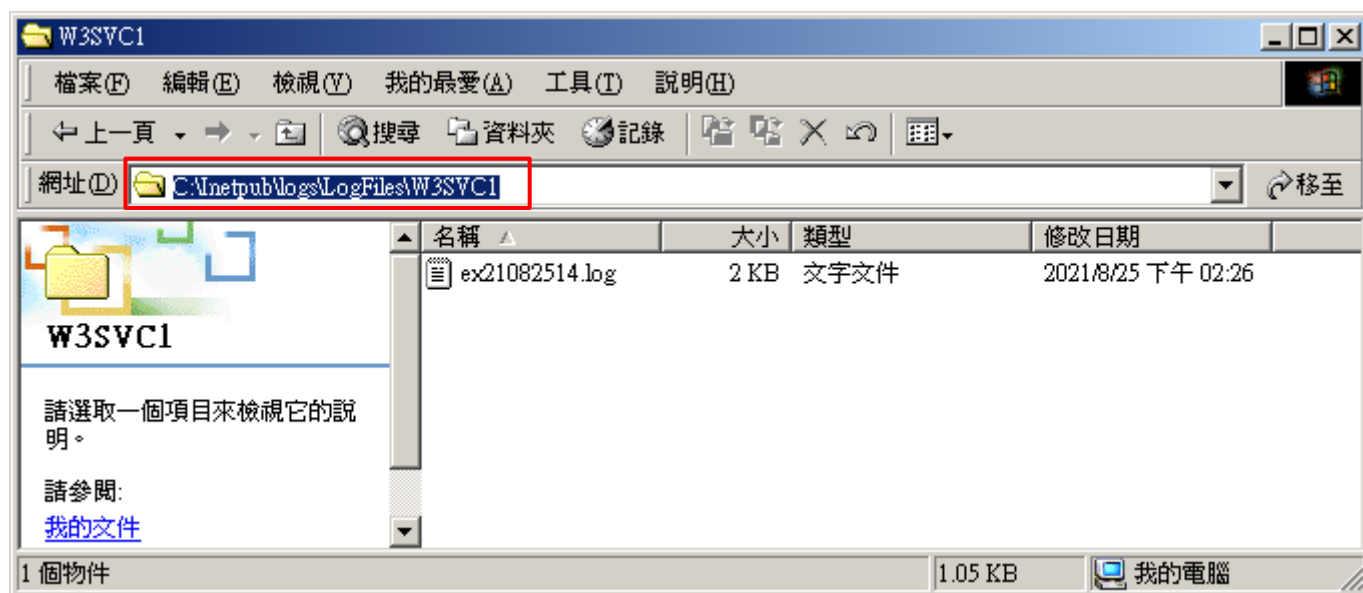
※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.1.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

記錄所有資訊:

不記錄 Cookie 資訊:



(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: ex*.log



3. Windows 2003

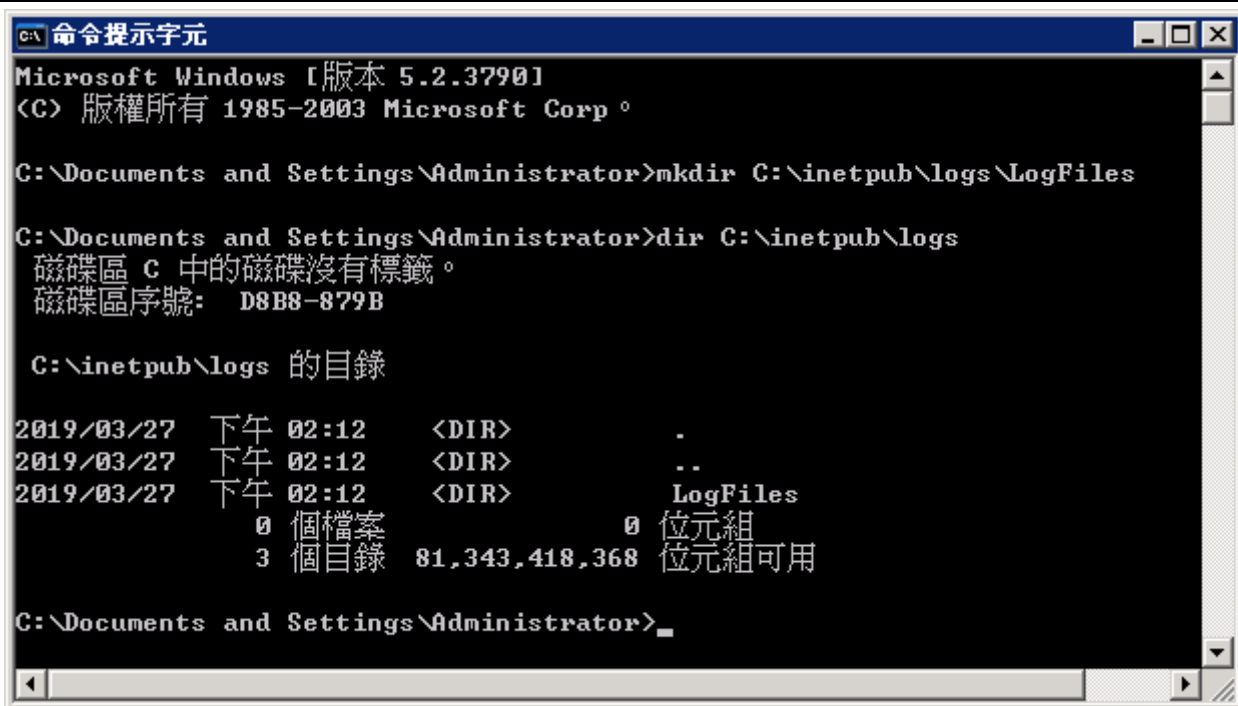
(1) 開啟 [命令提示字元]



(2) 新增 IIS LogFiles 資料夾和確認 IIS LogFiles 資料夾

```
C:\> mkdir C:\inetpub\logs\LogFiles
```

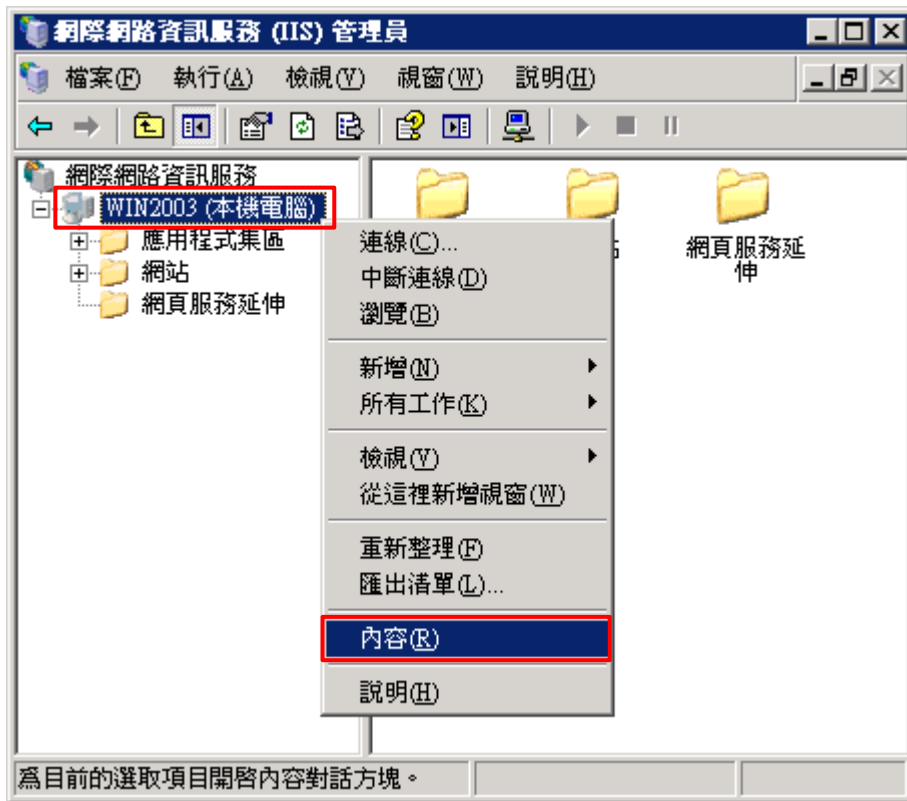
```
C:\> dir C:\inetpub\logs
```



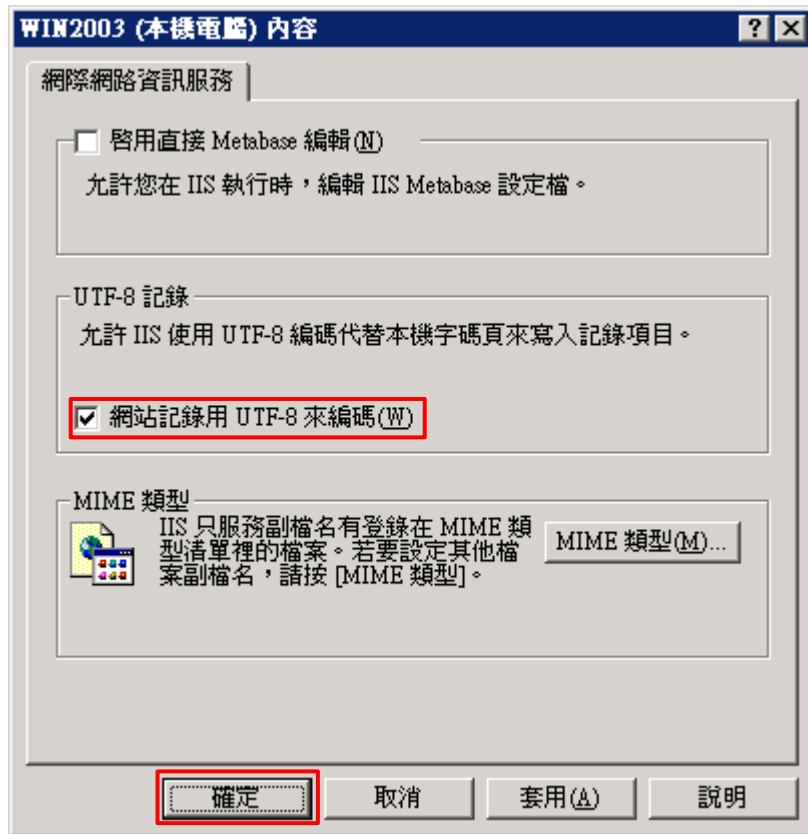
(3) 開啟 [網際網路資訊服務 (IIS) 管理員]



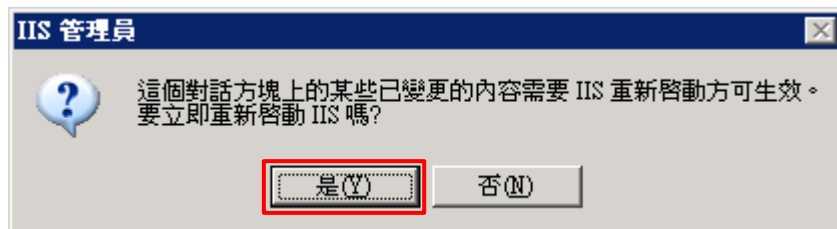
(4) 在 [IIS Server] 上按滑鼠右鍵 -> 選擇 [內容]



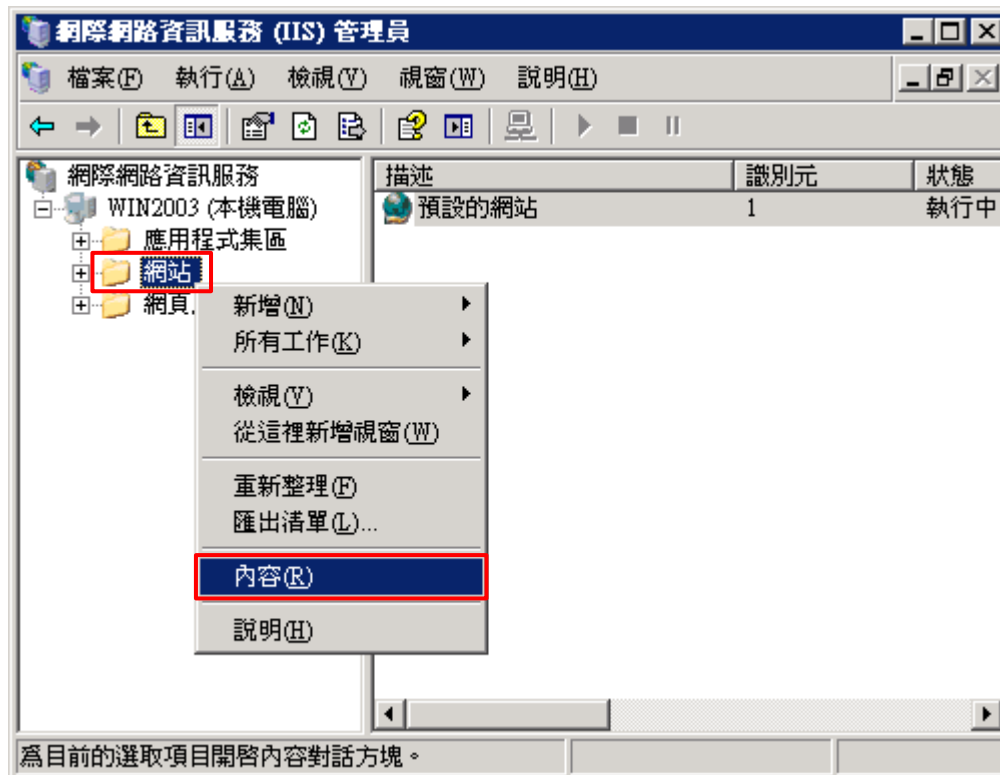
(5) 勾選 [網站記錄用 UTF-8 來編碼] -> 按下 [確定]



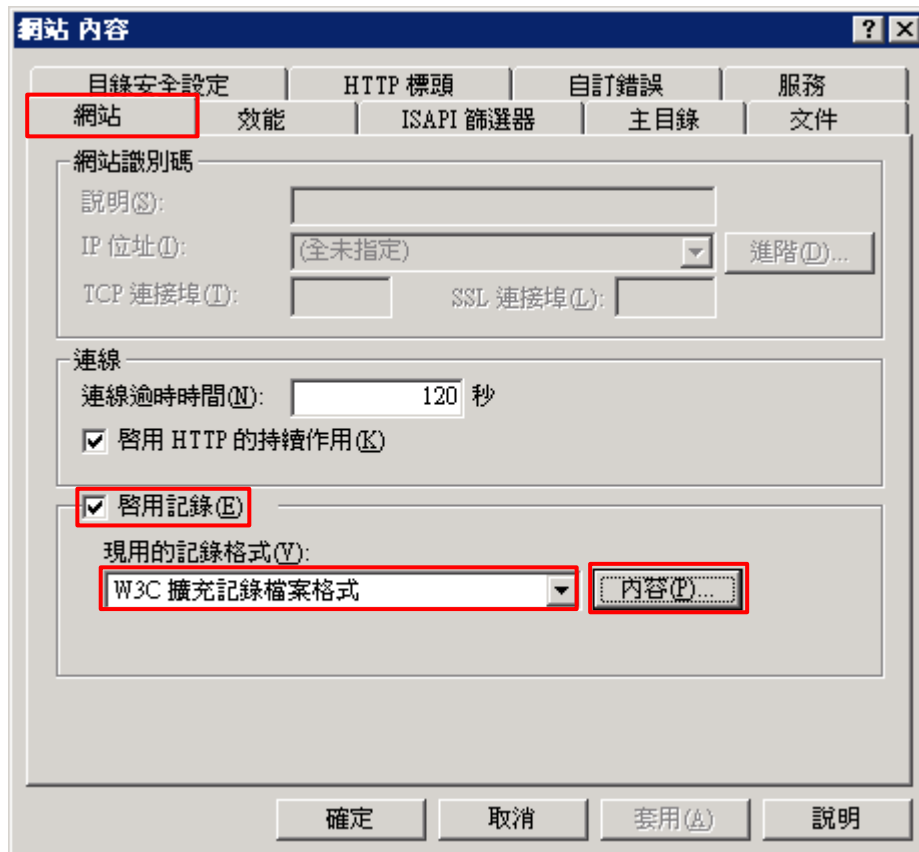
(6) 按下 [確定]



(7) 在 [網站] 上按滑鼠右鍵 -> 選擇 [內容]

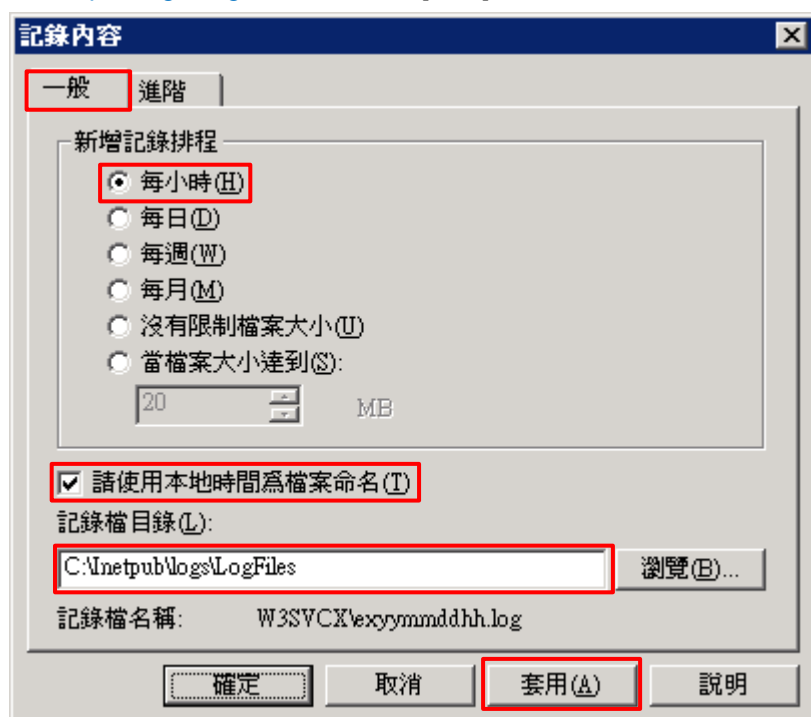


(8) [網站] 頁面: 勾選 [啟用記錄] -> 現用的記錄格式選擇 [W3C 擴充記錄檔案格式] -> 按下 [內容]



(9) [一般] 頁面: 新增記錄排程點選 [每小時] -> 勾選 [請使用本地時間為檔案命名] -> 記錄檔目錄輸入

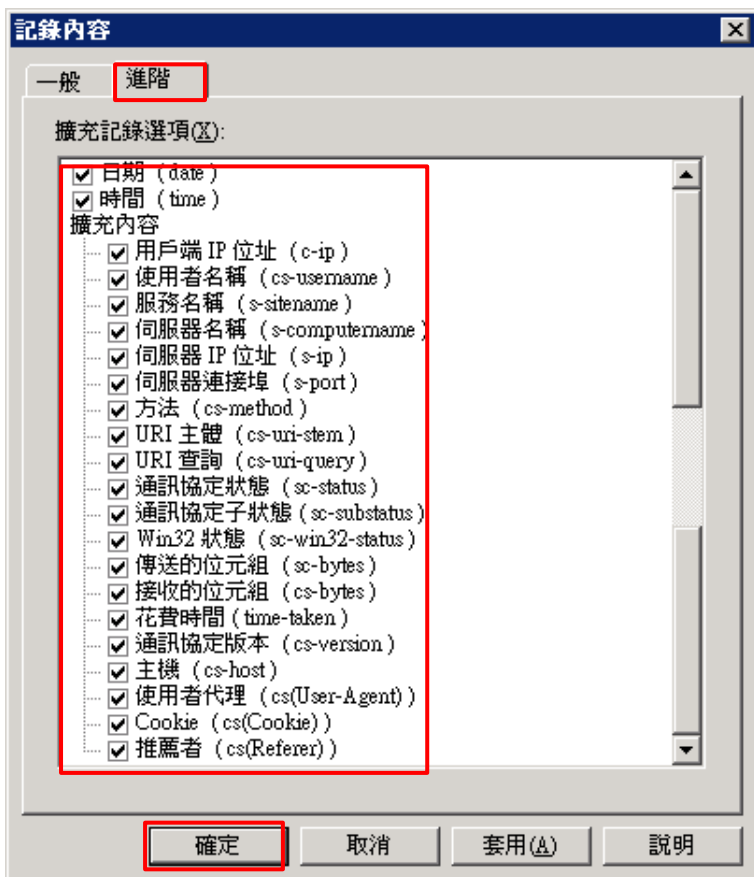
C:\inetpub\logs\LogFiles -> 按下 [套用]



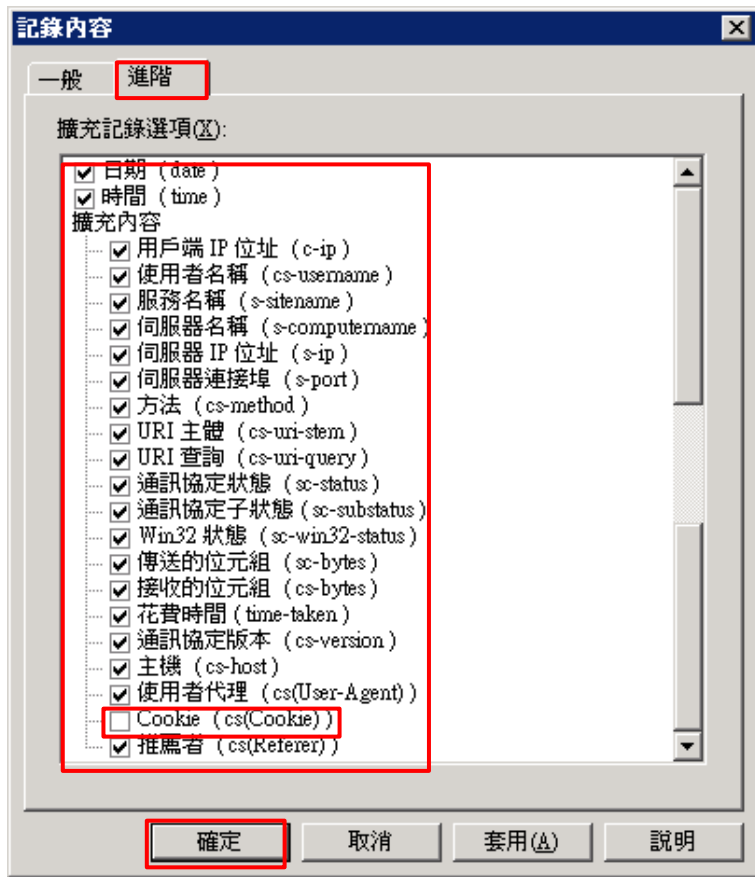
(10) [進階] 頁面：擴充記錄選項勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [確定]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.1.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

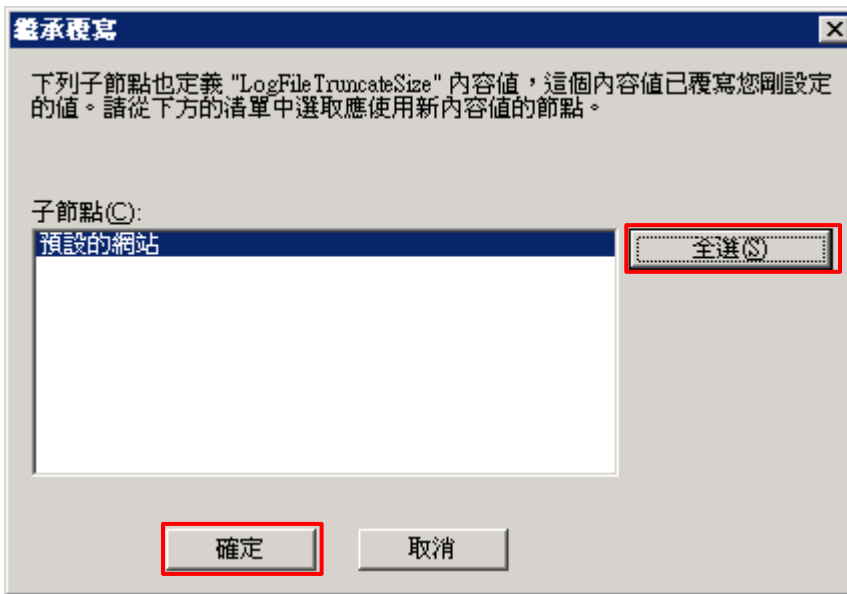
記錄所有資訊:



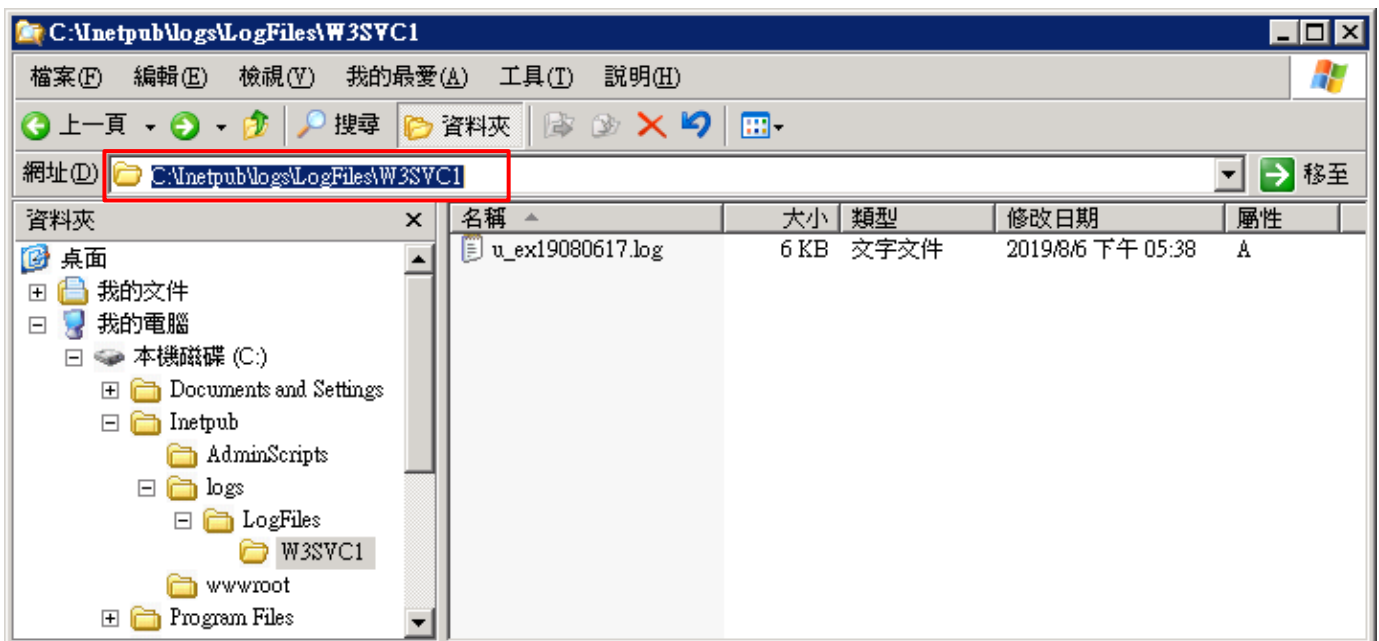
不記錄 Cookie 資訊:



(11) 按下 [全選] 和 [確定]



(12) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

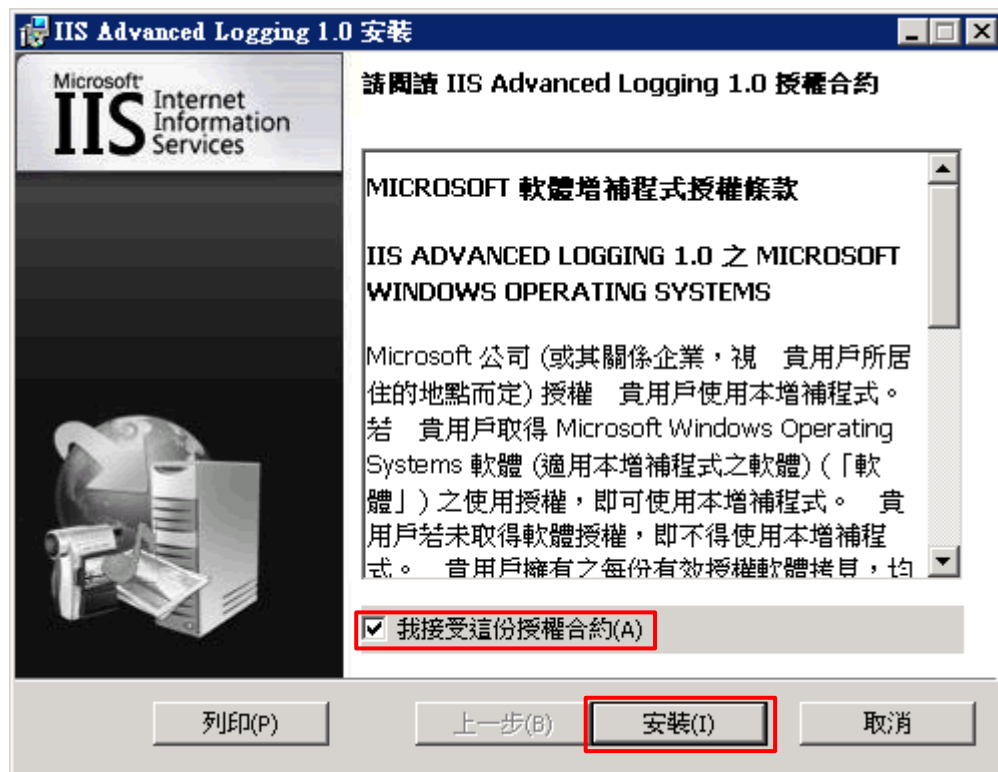


4. Windows 2008

(1) 安裝 [IIS Advanced Logging]

註：若需要下載 IIS Advanced Logging 軟體，請與我們連繫。

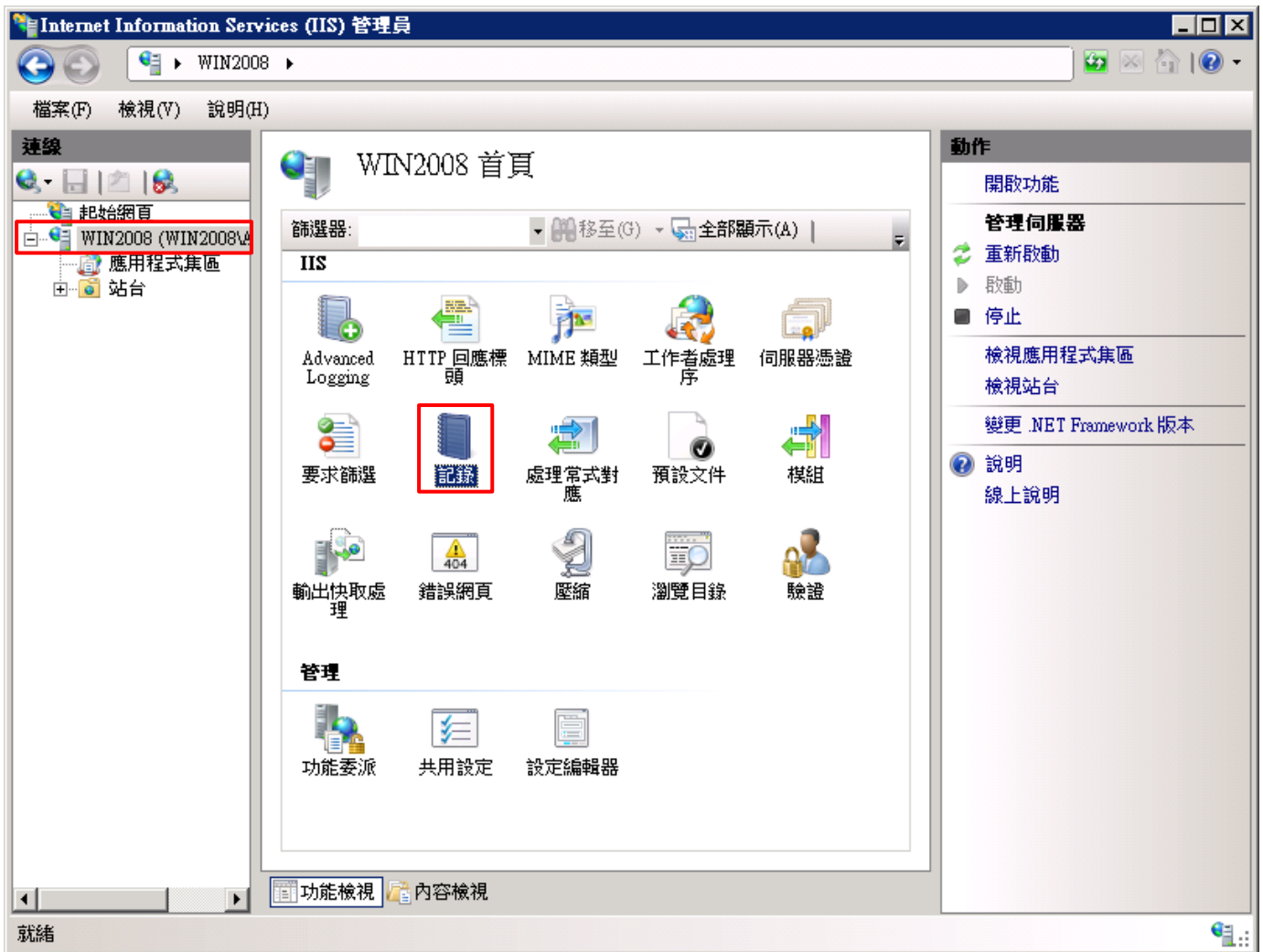
點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]



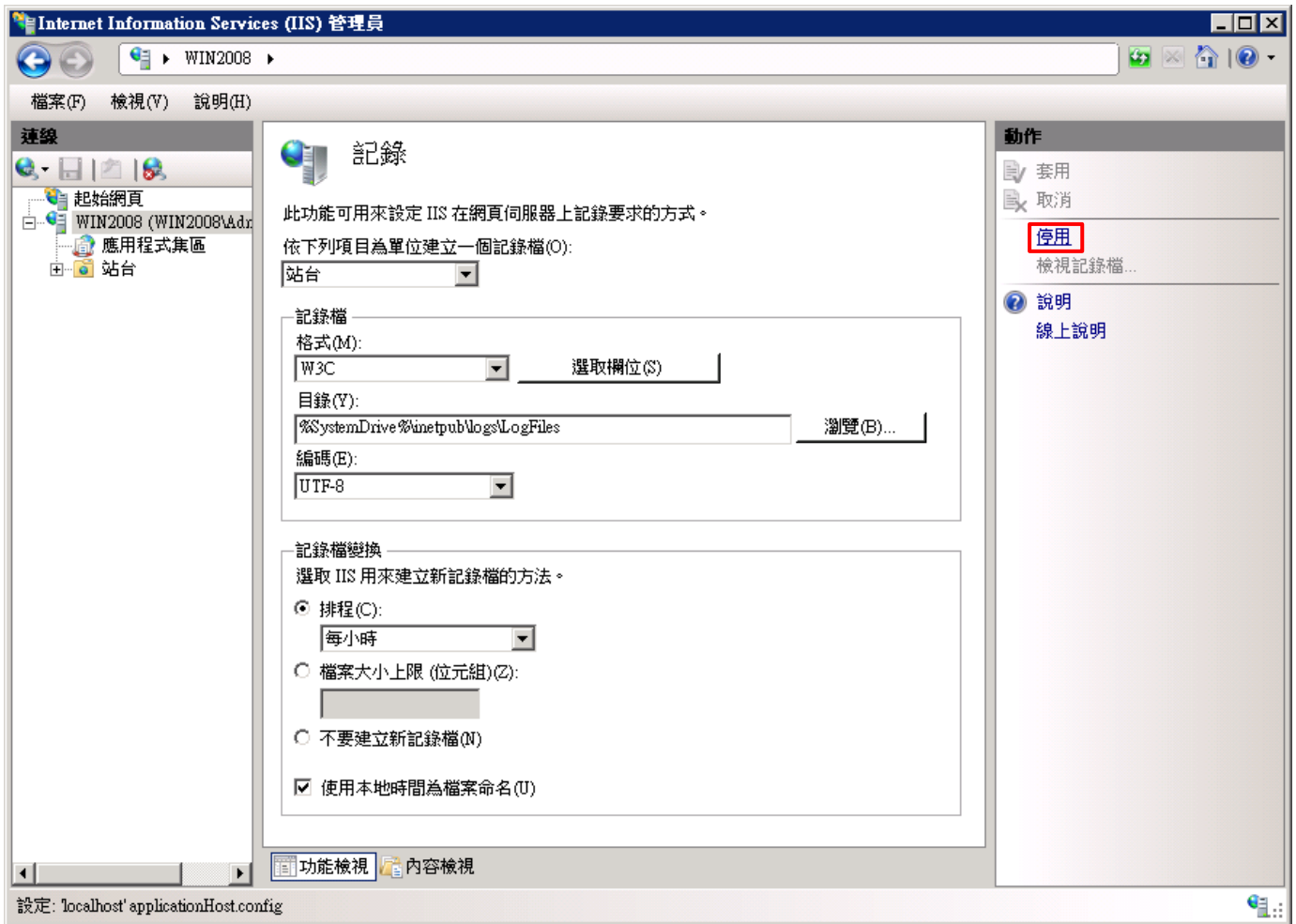
(2) 開啟 [Internet Information Services (IIS) 管理員]



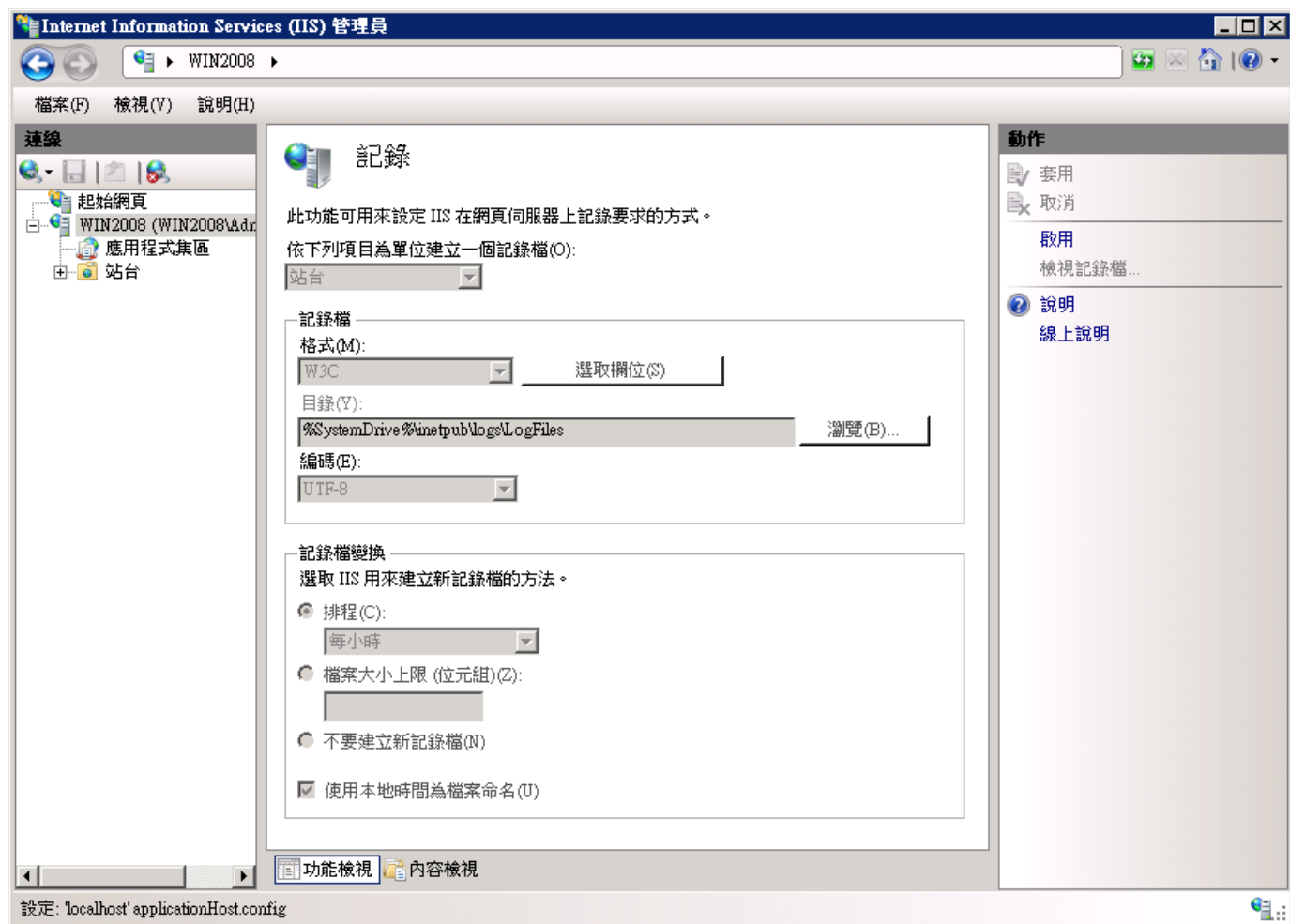
(3) 選擇 [IIS Server] -> 點選 [記錄]



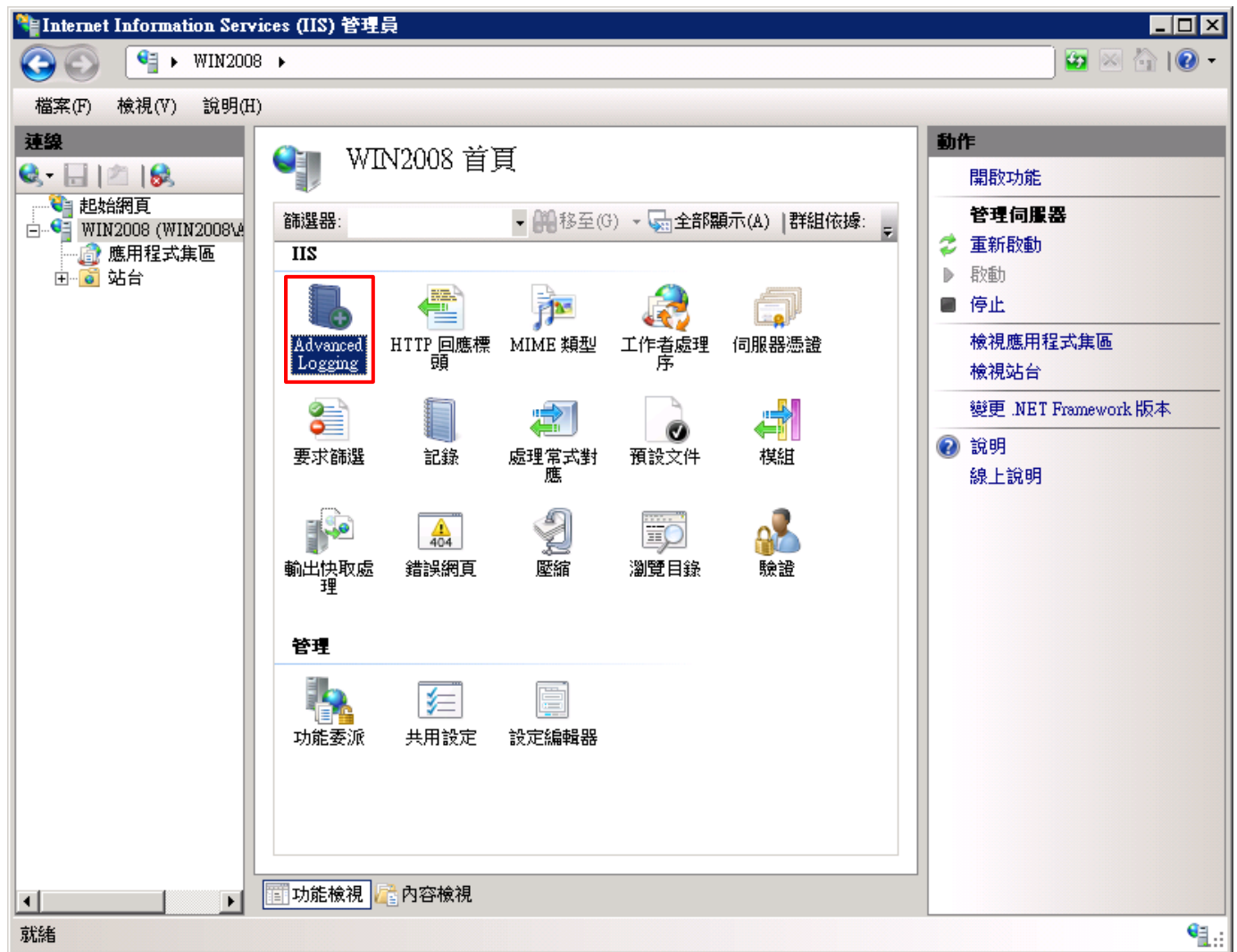
(4) 點選 [停用]



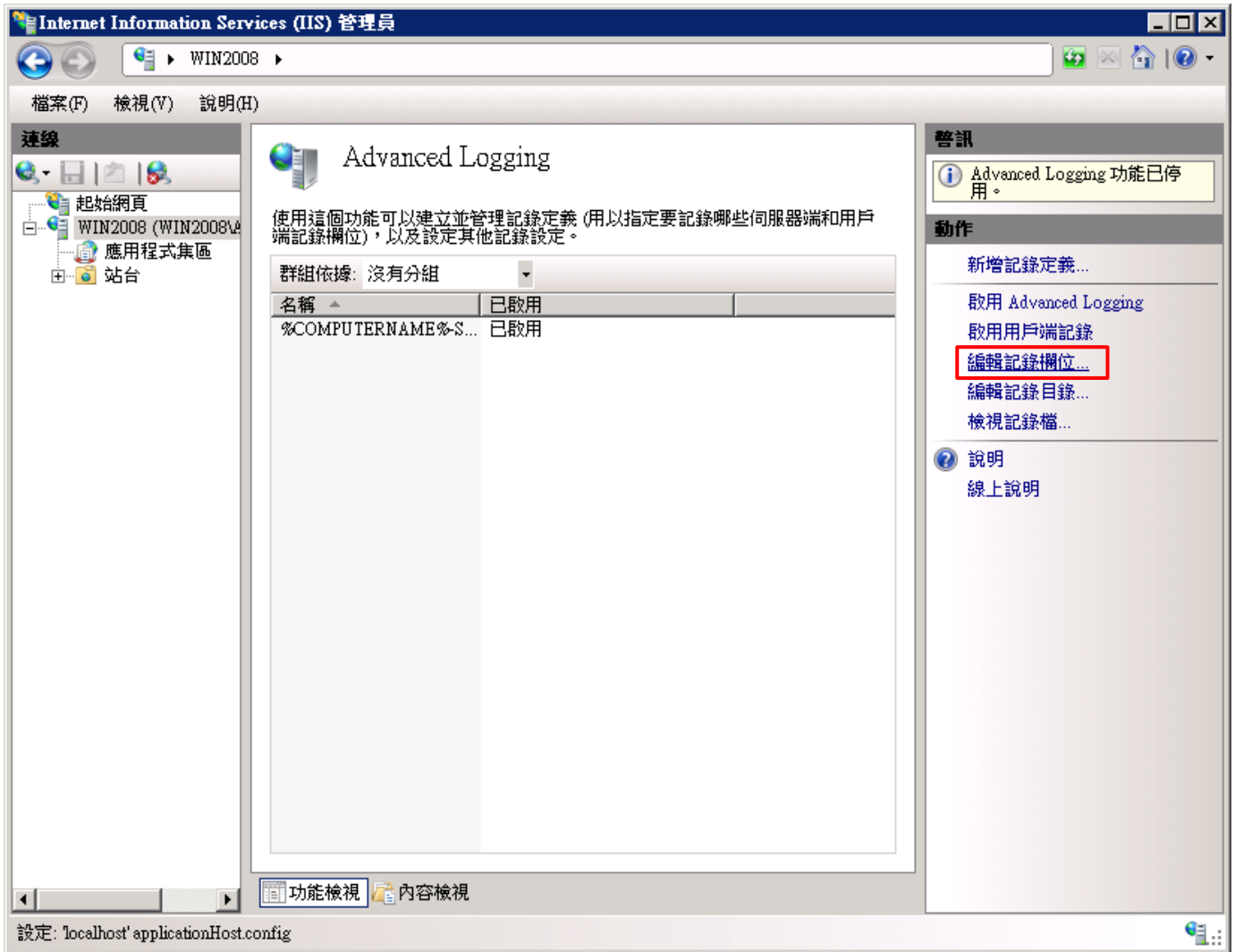
(5) 確認記錄已停用



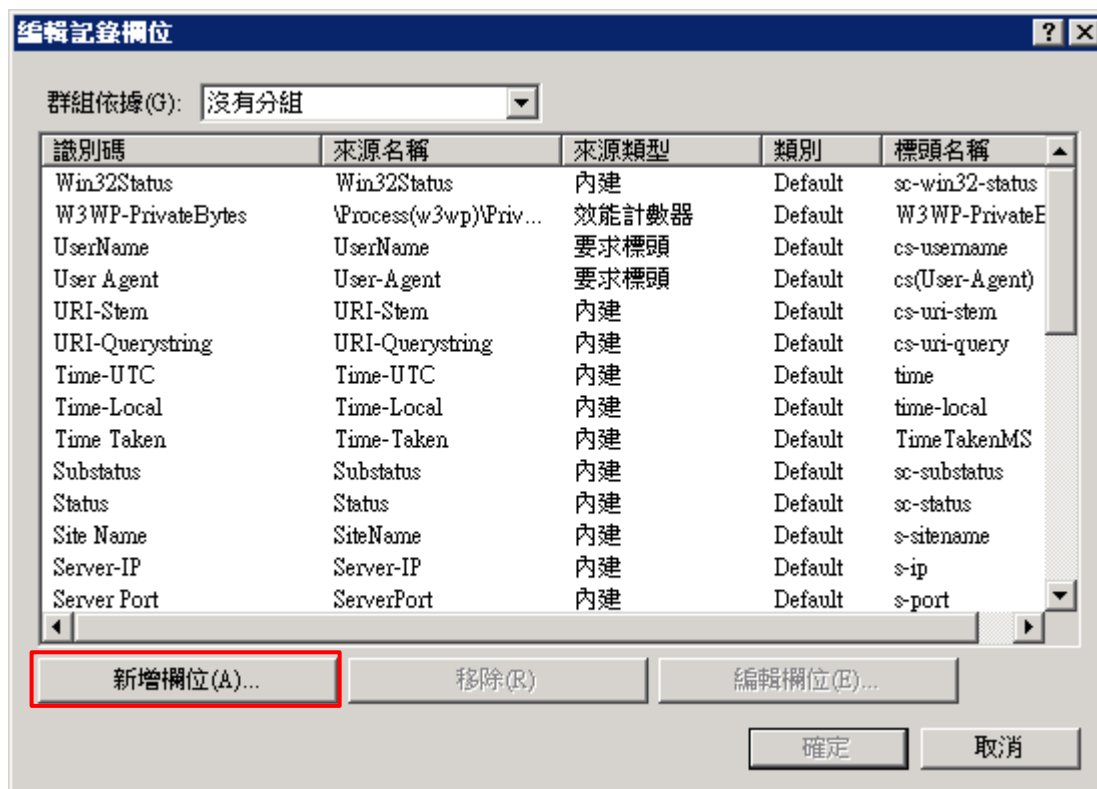
(6) 點選 [Advanced Logging]



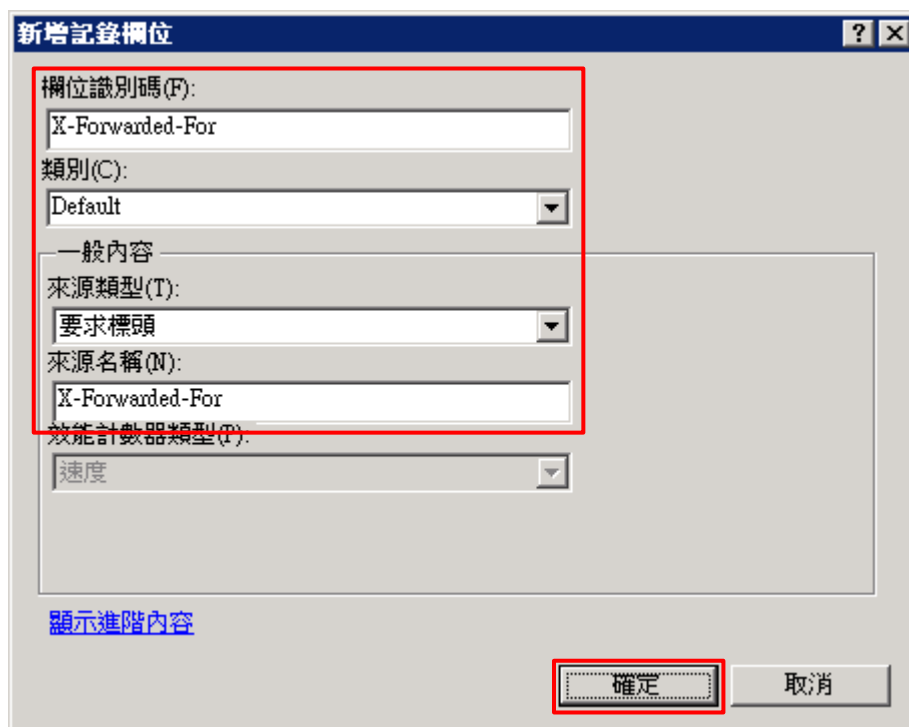
(7) 按下 [編輯記錄欄位]



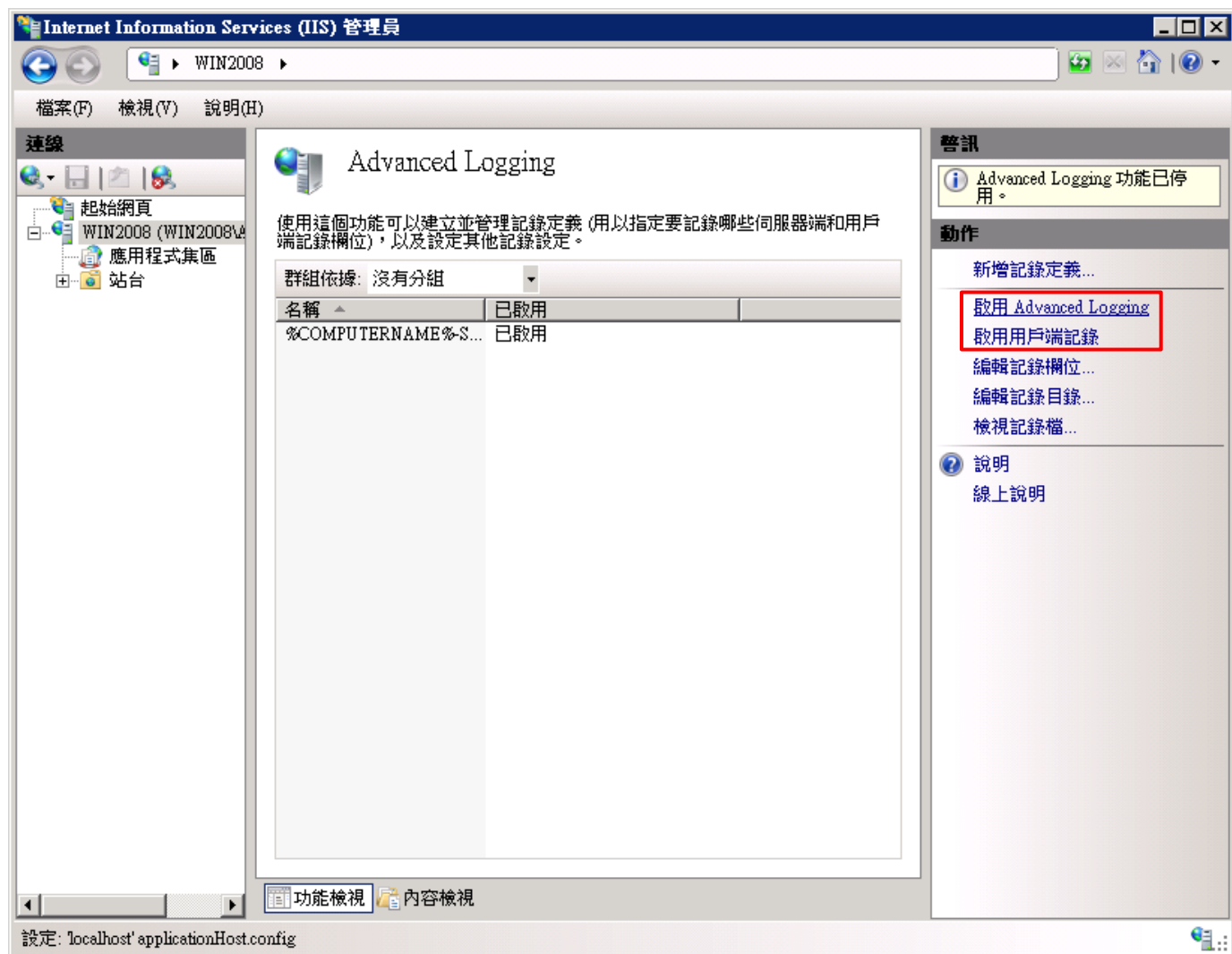
(8) 按下 [新增欄位]



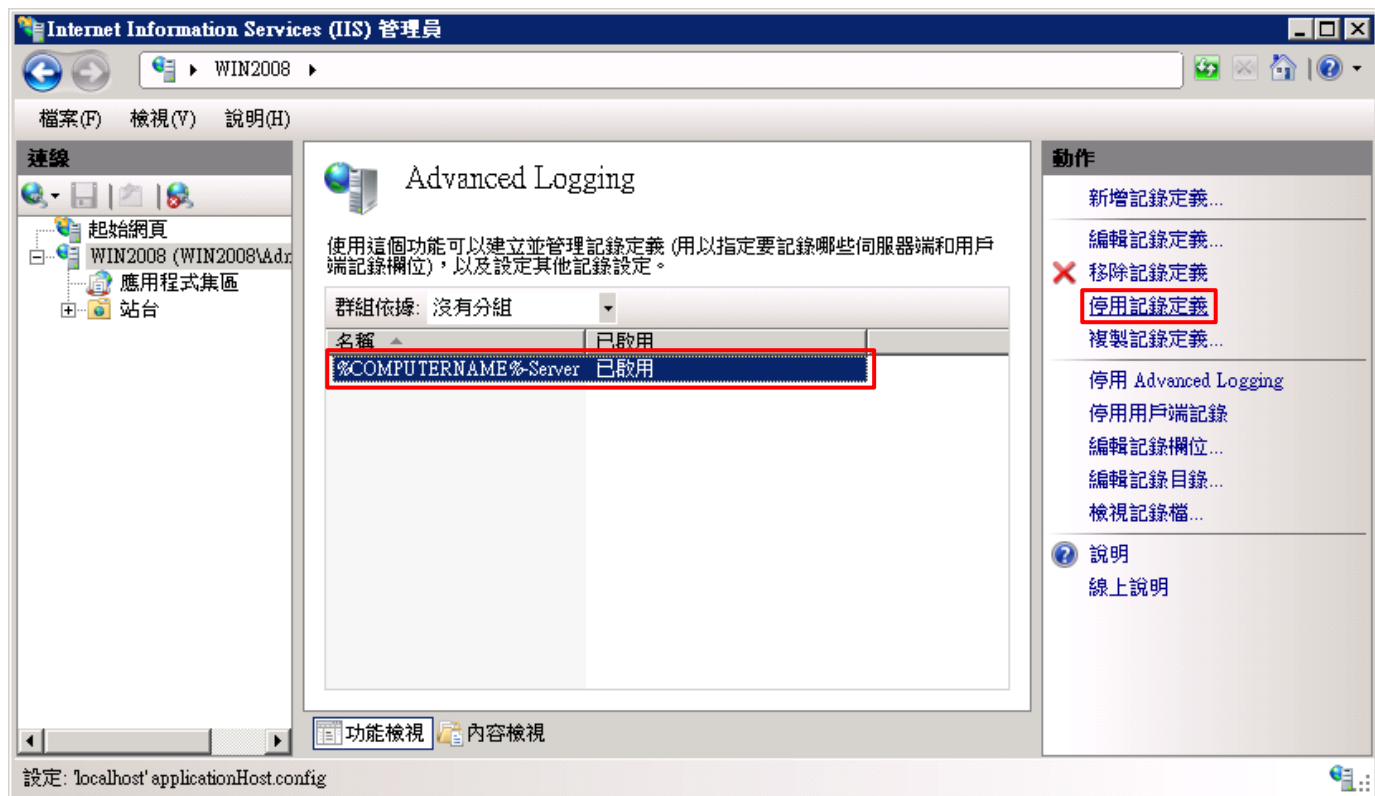
(9) 輸入欄位識別碼: **X-Forwarded-For** -> 選擇類別: [Default] -> 來源類型: [Request Header(要求標頭)] -> 輸入來源名稱: **X-Forwarded-For** -> 按下 [確定]



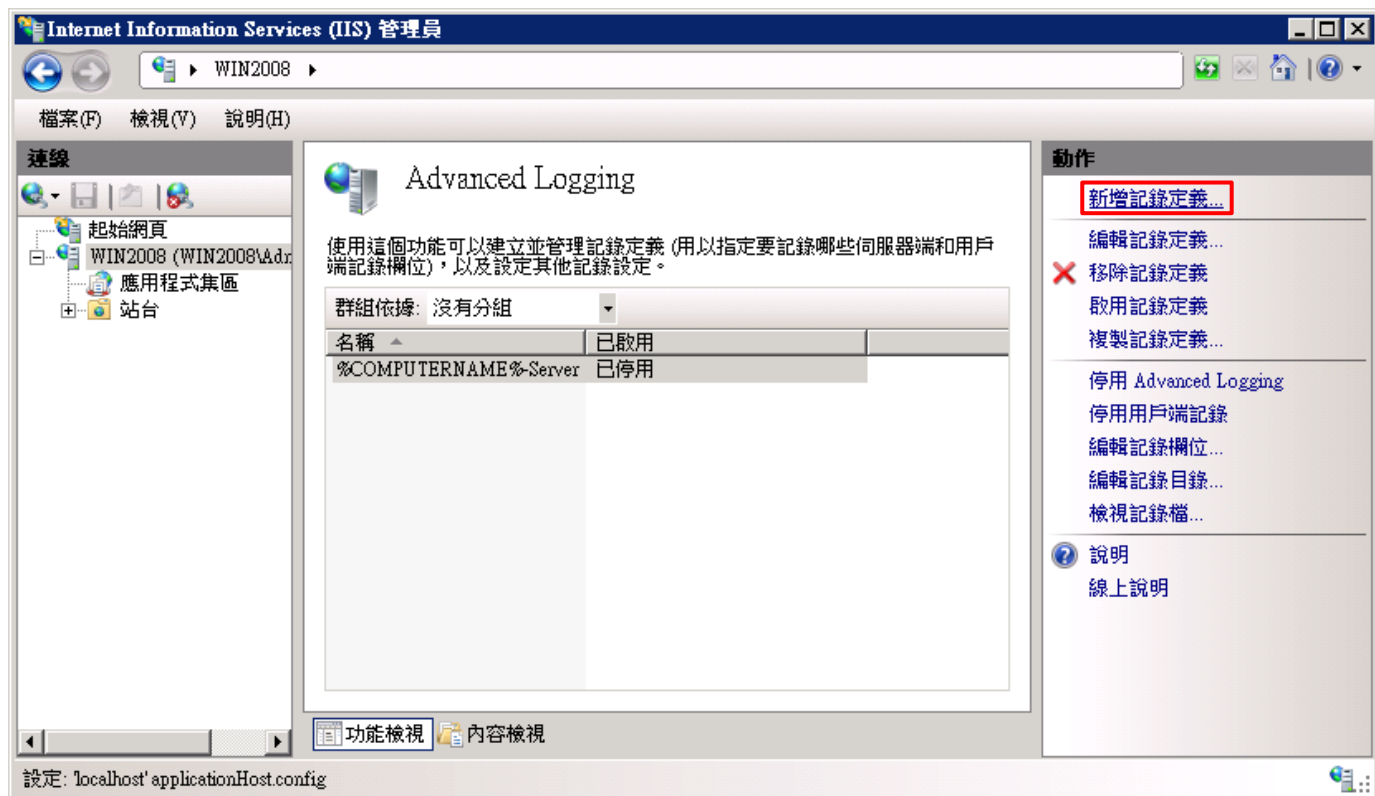
(10) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]



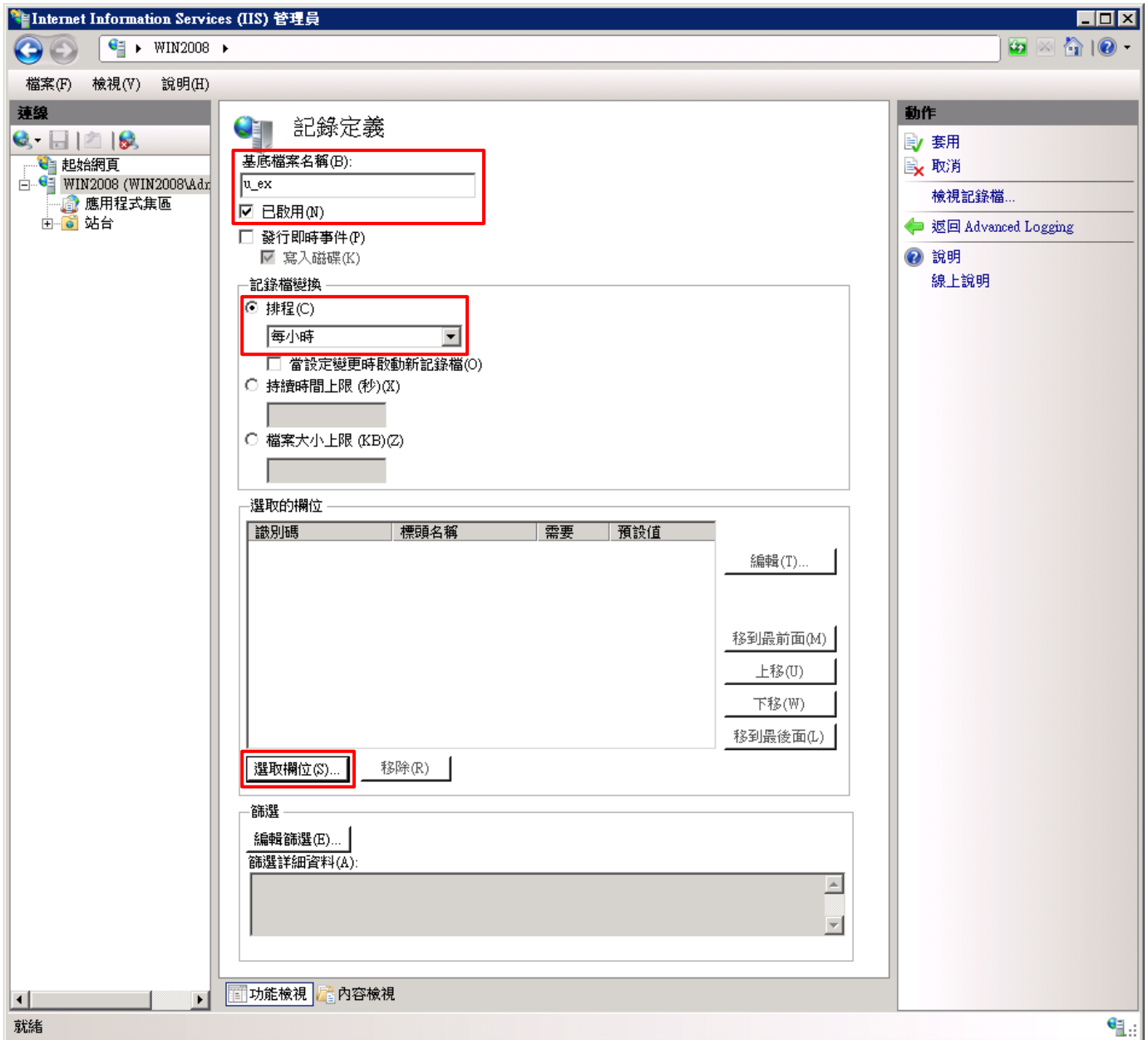
(11) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]



(12) 點選 [新增記錄定義]

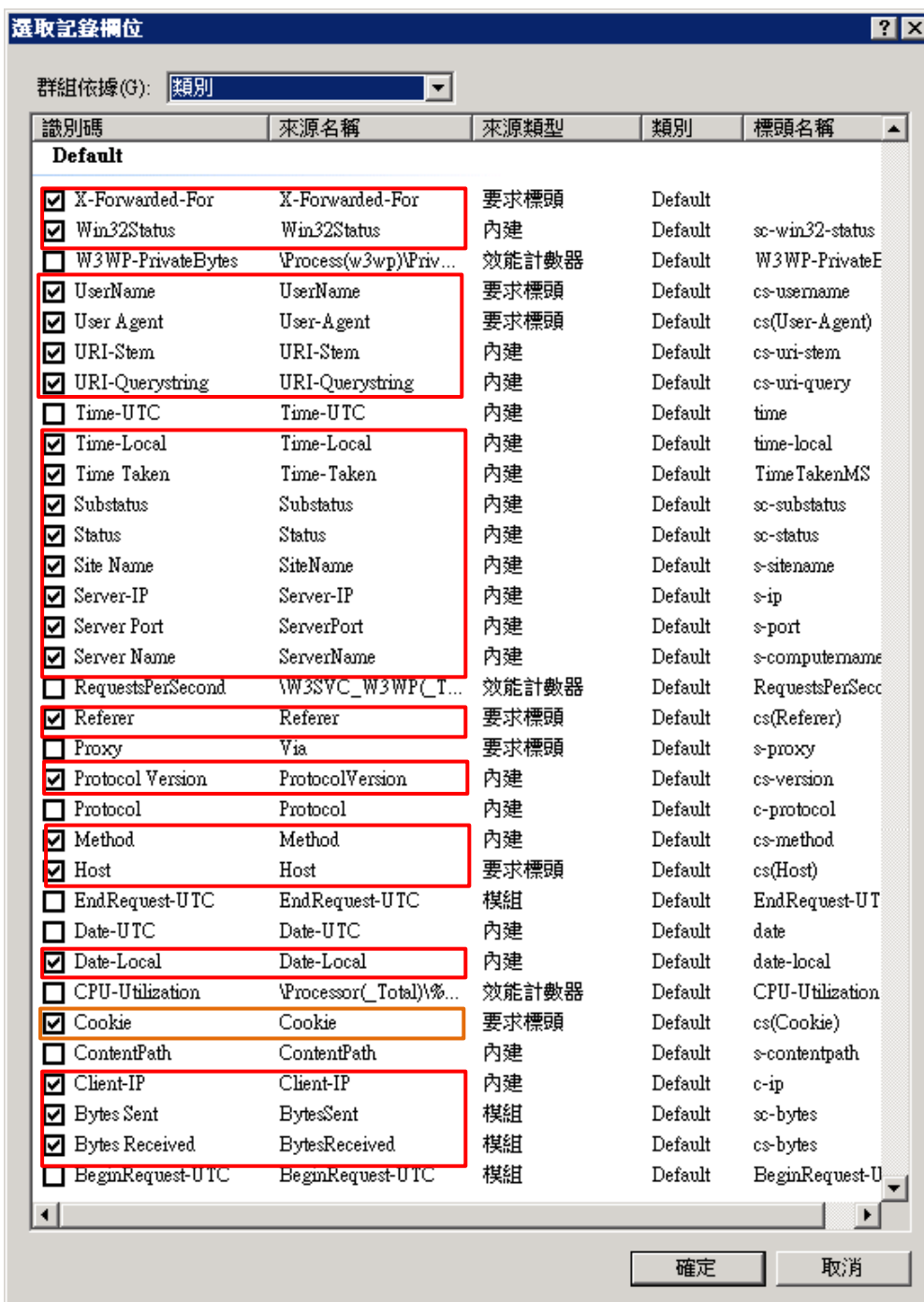


(13) 輸入基底檔案名稱: u_ex -> 勾選 [已啟用] -> 選擇排程 [每小時] -> 按下 [選取欄位]



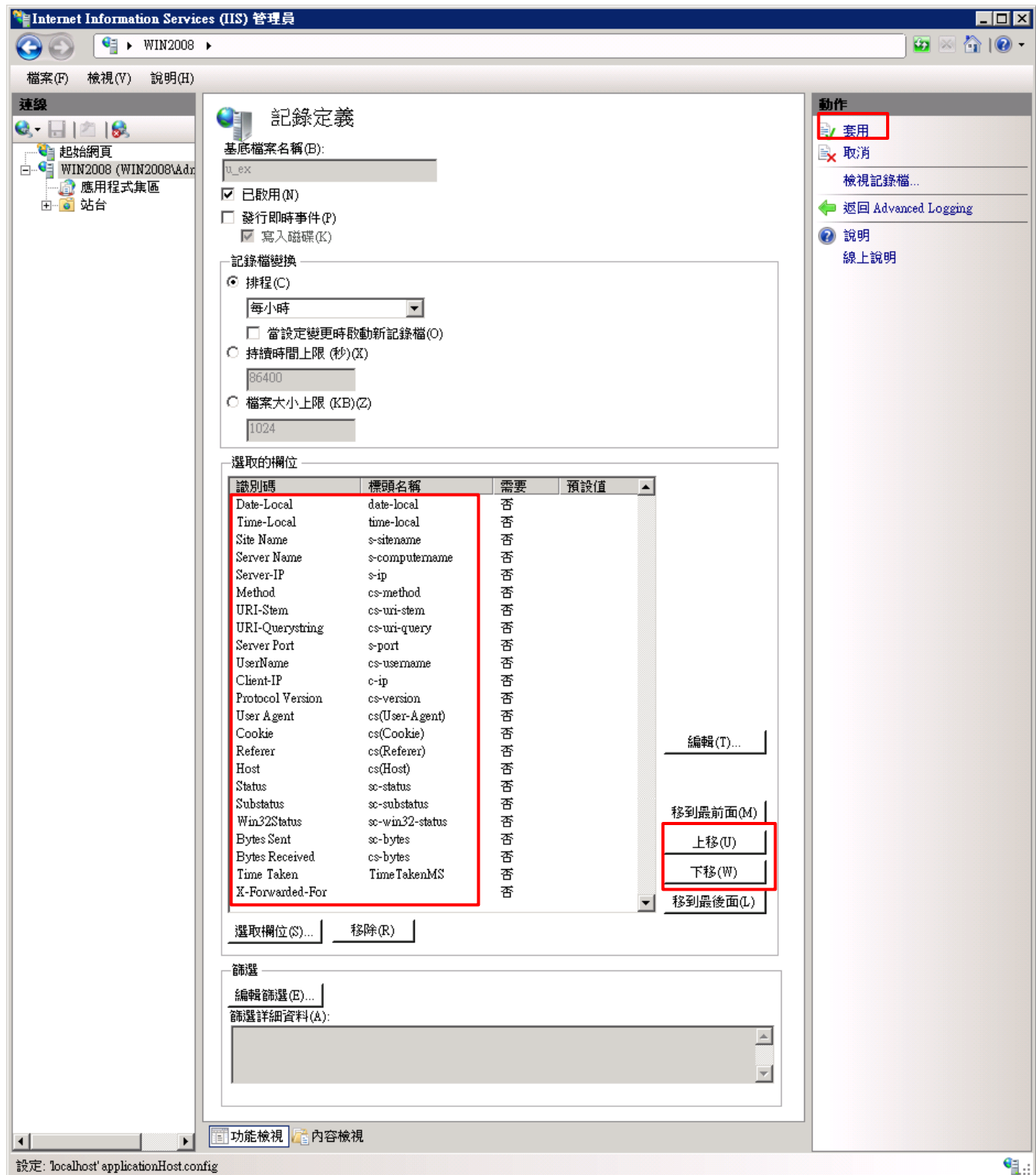
(14) 勾選 [X-Forwarded-For]、[Win32Status(sc-win32-status)]、[UserName(cs-username)]、[User Agent(cs(User-Agent))]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Time-Local(time-local)]、[Time Taken(TimeTakenMS)]、[Substatus(sc-substatus)]、[Status(sc-status)]、[Site Name(s-sitename)]、[Server-IP(s-ip)]、[Server Port(s-port)]、[Server Name(s-computername)]、[Referer(cs(Referer))]、[Protocol Version(cs-version)]、[Method(cs-method)]、[Host(cs(Host))]、[Date-Local(date-local)]、[Cookie(cs(Cookie))]、[Client-IP(c-ip)]、[Byte Sent(sc-bytes)]、[Bytes Received(cs-bytes)] -> 按下 [確定]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，下圖橘框，並依據步驟 1.2.2.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

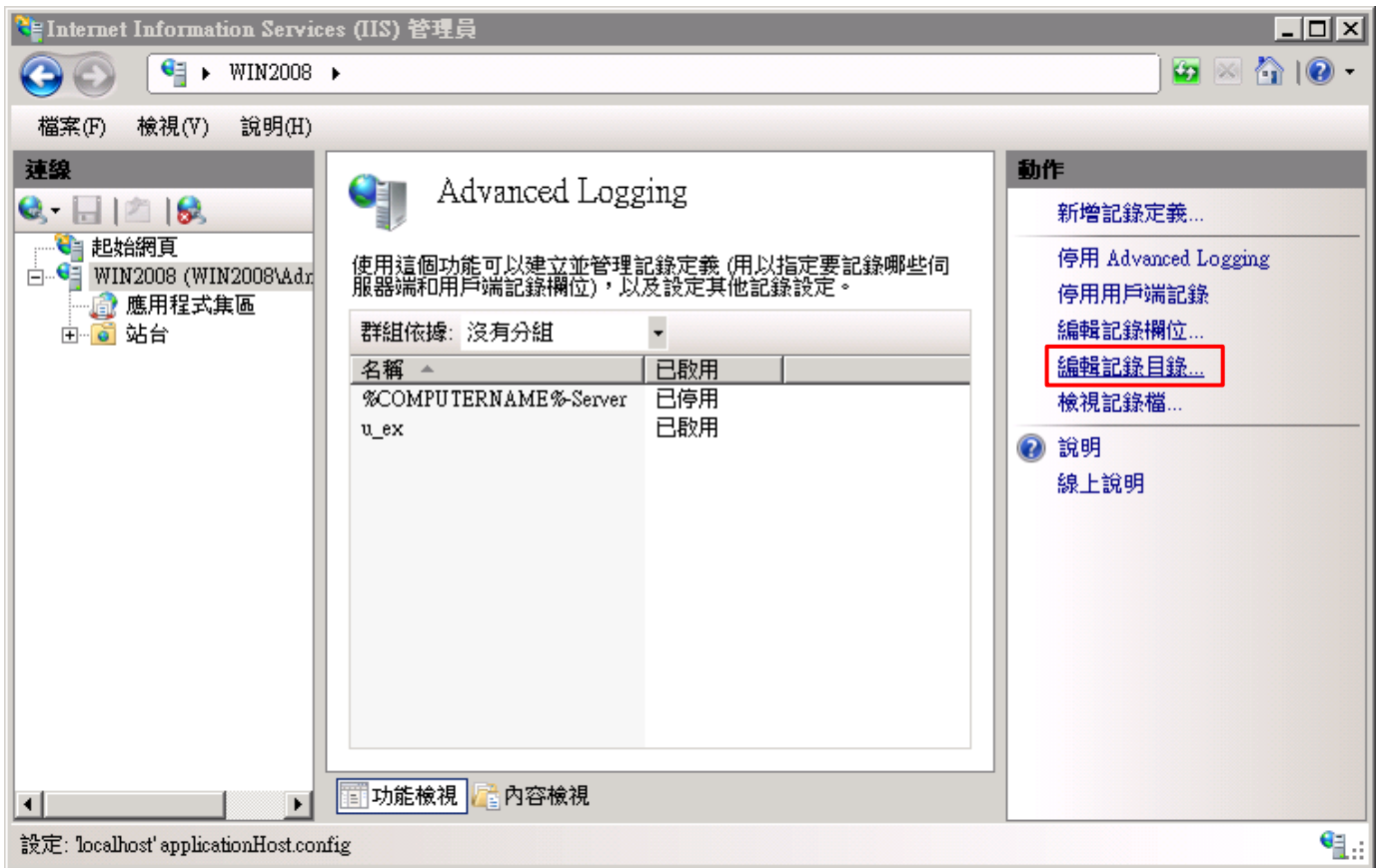


(15) 調整選取的欄位: [Data-Local(date-local)]、[Time-Local(time-local)]、[Site Name(s-sitename)]、[Server Name(s-computername)]、[Server-IP(s-ip)]、[Method(cs-method)]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Server Port(s-port)]、[UserName(cs-username)]、[Client-IP(c-ip)]、[Protocol Version(cs-version)]、[User Agent(cs(User-Agent))]、[Cookie(cs(Cookie))]、[Referer(cs(Referer))]、[Host(cs(Host))]、[Status(sc-status)]、[Substatus(sc-substatus)]、[Win32Status(sc-win32-status)]、[Bytes Send(sc-bytes)]、[Bytes Received(cs-bytes)]、[Time Taken(TimeTakenMS)]、[X-Forwarded-For] -> 按下 [套用]

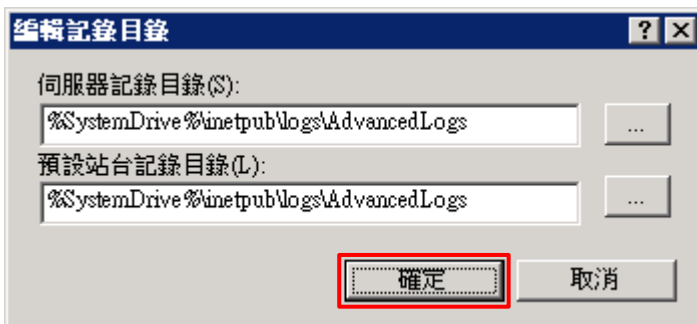
※如上一步驟未勾選 Cookie (cs(Cookie))，則此步驟不會出現 Cookie 選項。



(16) 點選 [編輯記錄目錄]



(17) 確認伺服器記錄目錄和預設站台記錄目錄 -> 按下 [確定]



(18) 修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入 Microsoft IIS 記錄檔資料夾路徑

```
define IISpath C:\inetpub\logs\AdvancedLogs
```

(19) 開啟 [Windows PowerShell]



(20) 重啟 nxlog 服務 · 檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

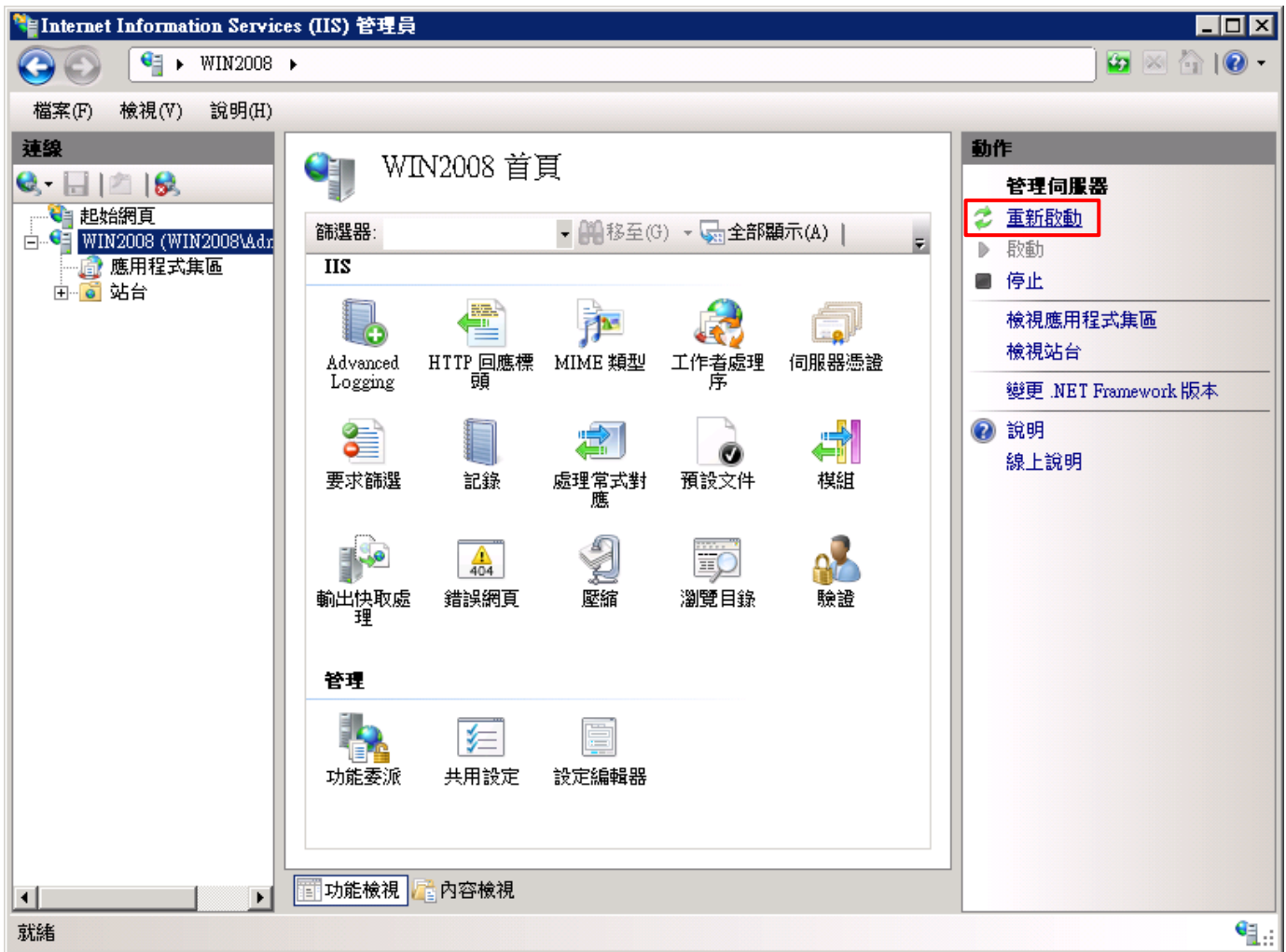
```
PS C:\> Restart-Service nxlog
PS C:\> Get-Service nxlog
PS C:\> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
```

A screenshot of a Windows PowerShell terminal window titled 'Administrator: Windows PowerShell'. The terminal shows the execution of three commands: 'Restart-Service nxlog', 'Get-Service nxlog', and 'Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log''. The output of 'Get-Service nxlog' is a table with columns 'Status', 'Name', and 'DisplayName'. The output of 'Get-Content' shows log entries for the nxlog service starting and stopping on 2022-03-14 at 16:00:34 and 16:00:43 respectively.

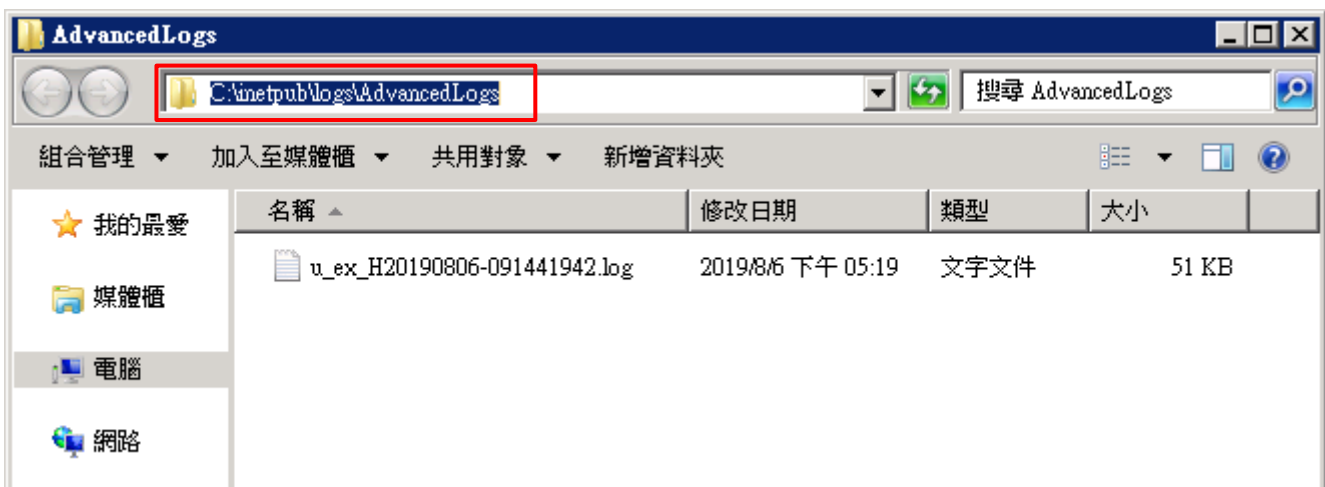
Status	Name	DisplayName
Running	nxlog	nxlog

```
PS C:\> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2022-03-14 16:00:34 INFO nxlog-ce-3.0.2272 started
2022-03-14 16:00:43 WARNING stopping nxlog service
2022-03-14 16:00:43 WARNING nxlog-ce received a termination request signal, exiting...
2022-03-14 16:00:43 INFO nxlog-ce-3.0.2272 started
PS C:\>
```

(21) 點選 [重新啟動] IIS 服務

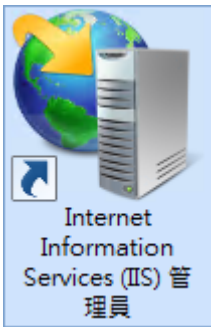


(22) 確認 [C:\inetpub\logs\AdvancedLogs] 資料夾 IIS log 檔案: u_ex*.log

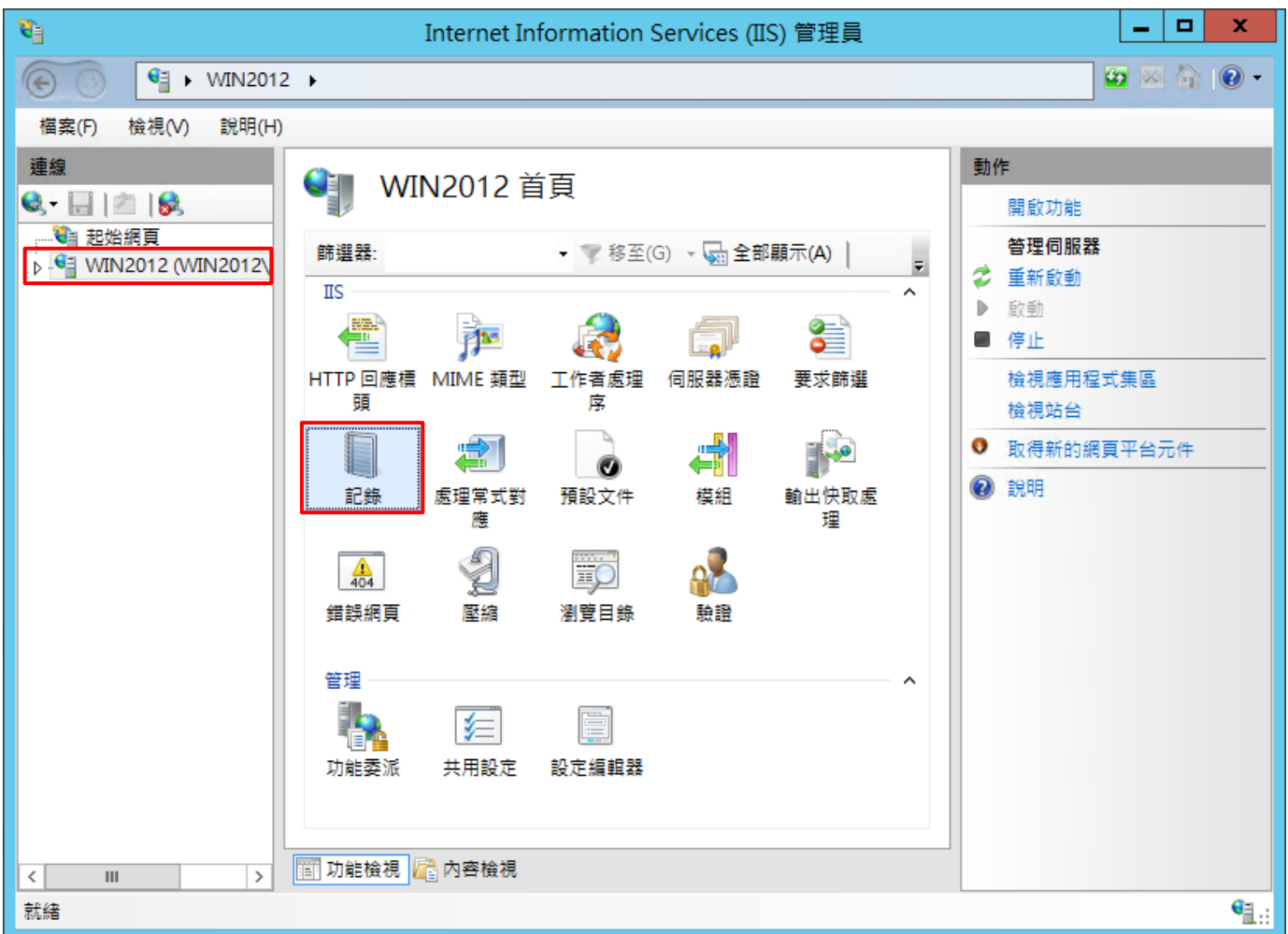


4. Windows 2012

(1) 開啟 [Internet Information Services (IIS) 管理員]

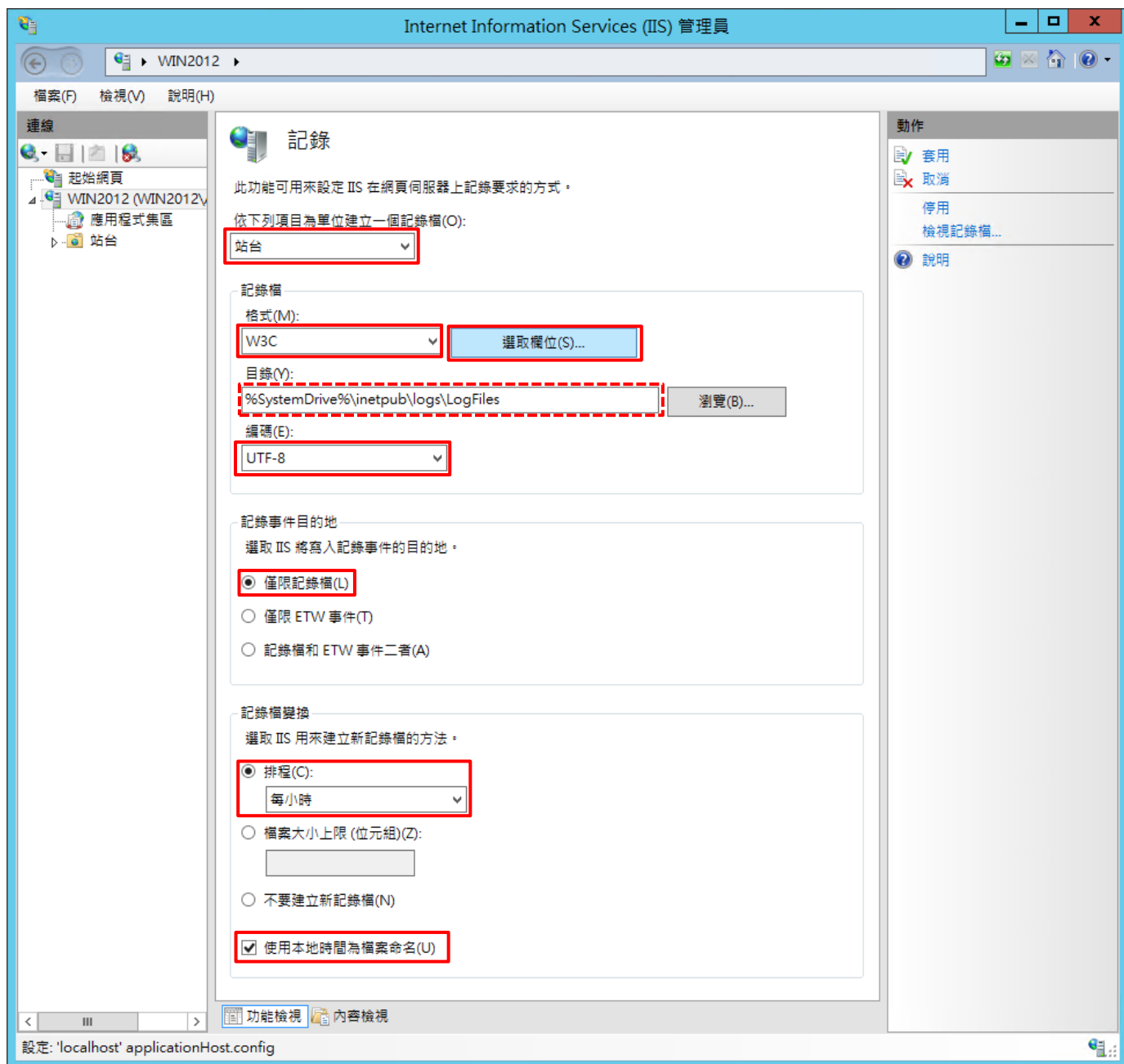


(2) 選擇 [IIS Server] -> 點選 [記錄]



(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取欄位]

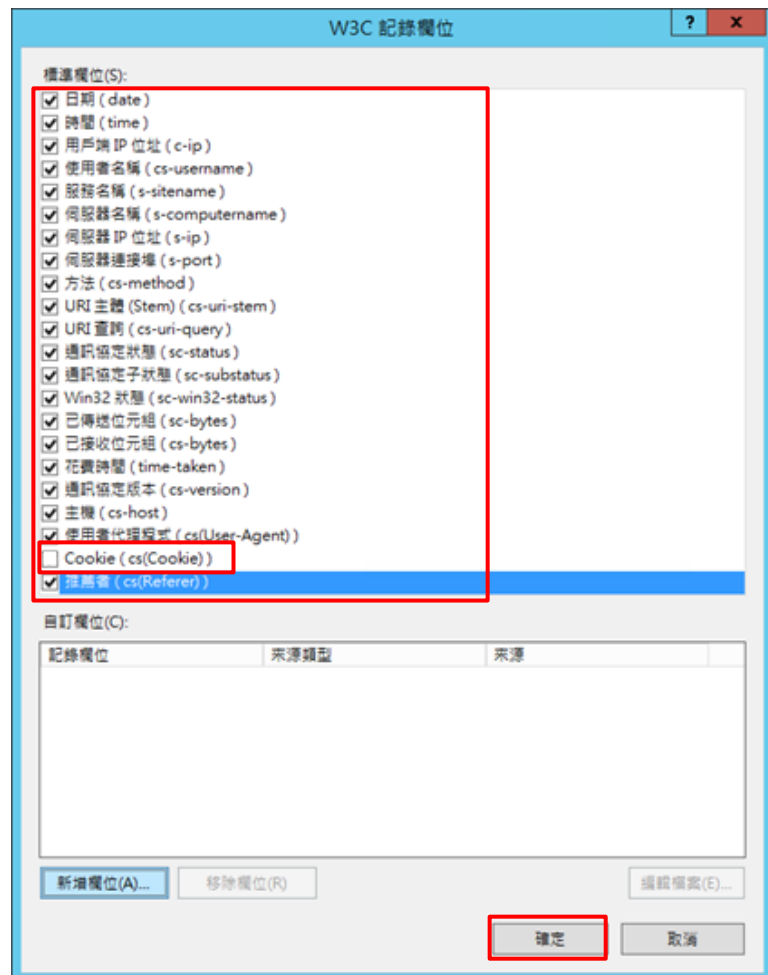
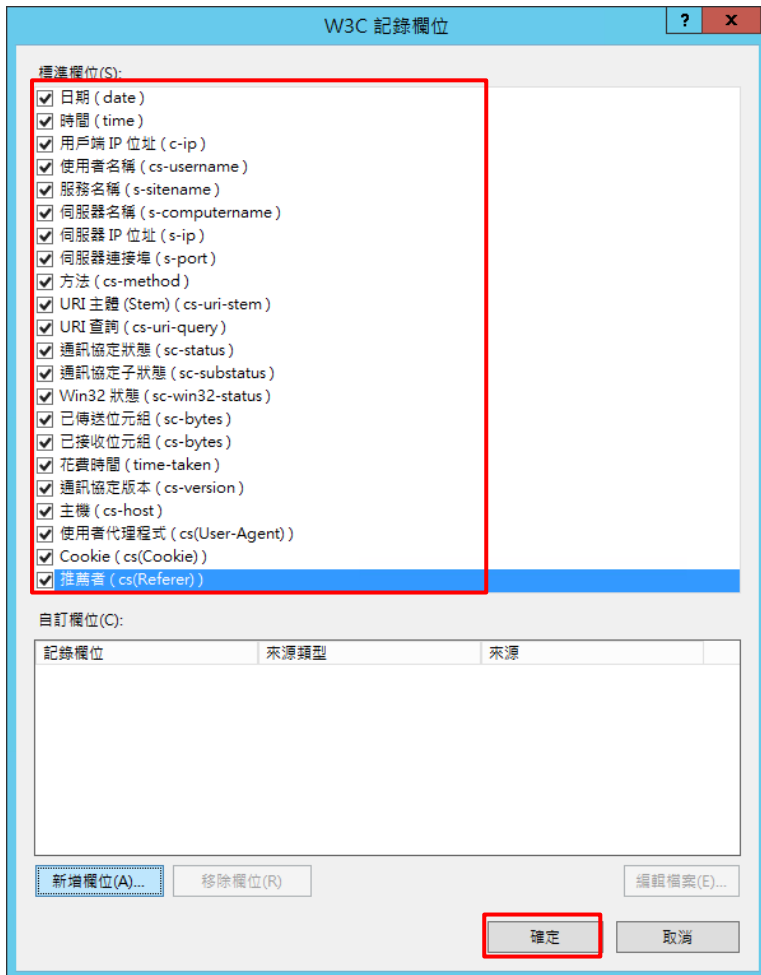


(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.2.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

記錄所有資訊:

不記錄 Cookie 資訊:



(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For
-> 按下 [確定]

新增自訂欄位

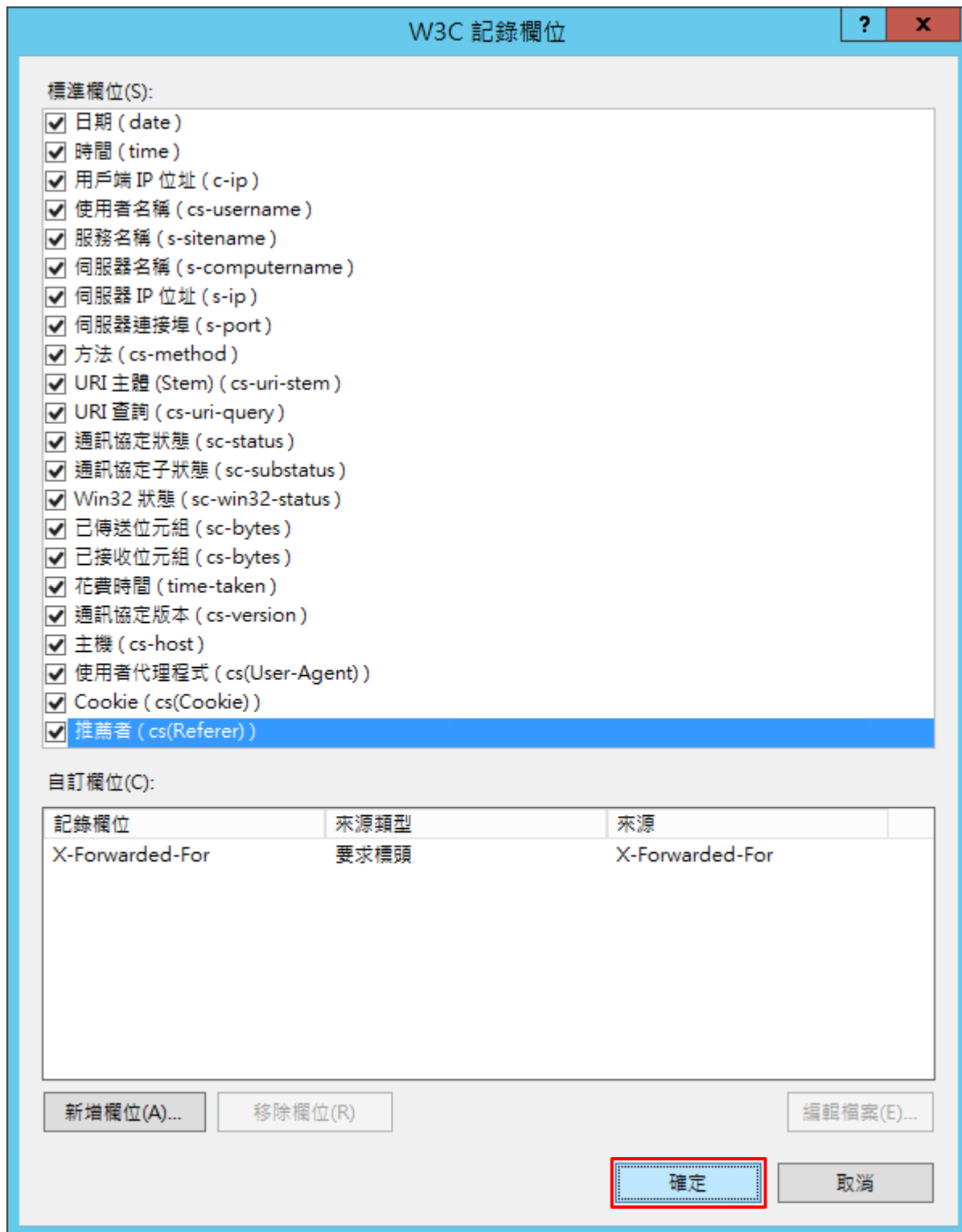
欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

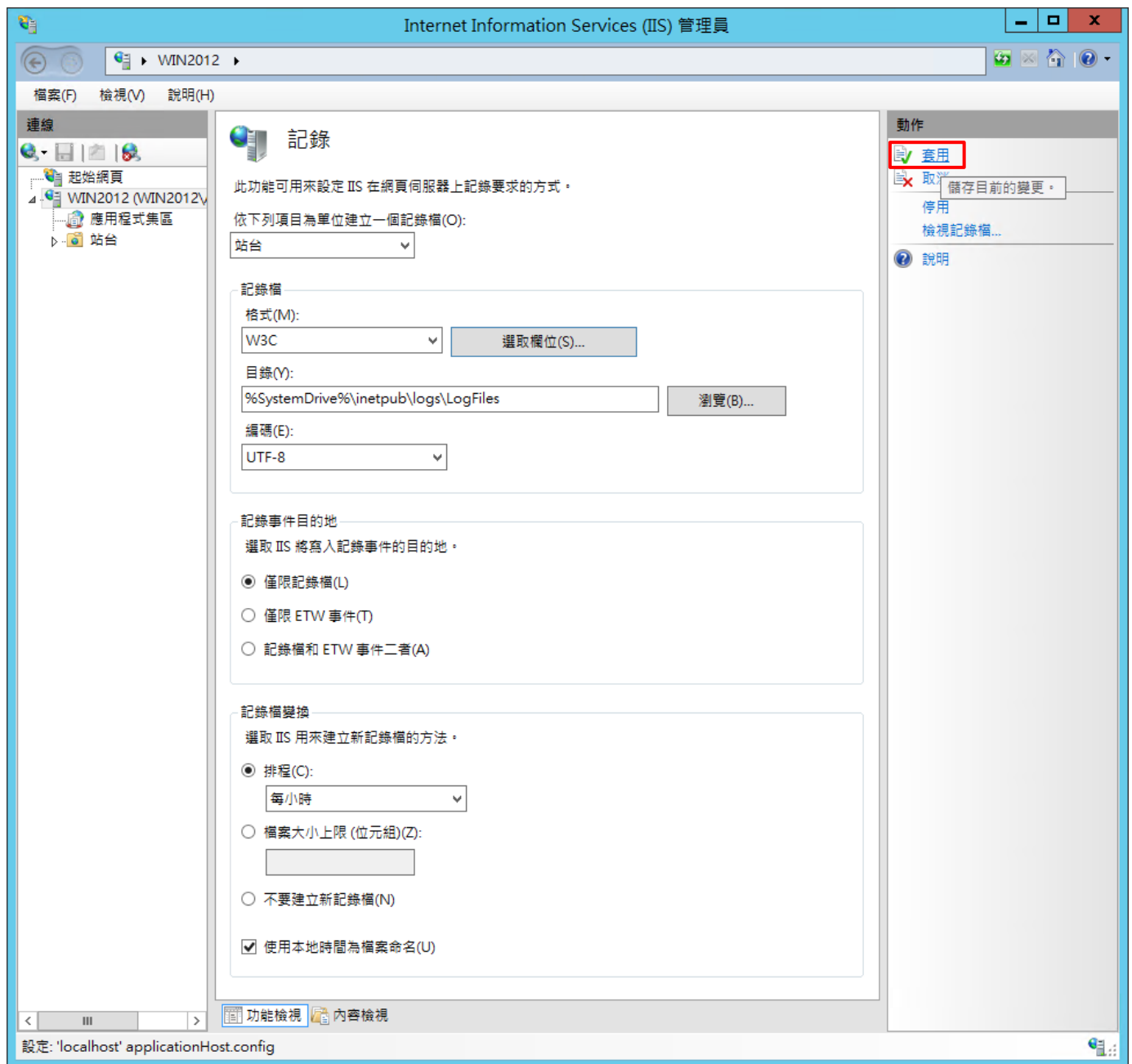
來源(S):
X-Forwarded-For

確定 取消

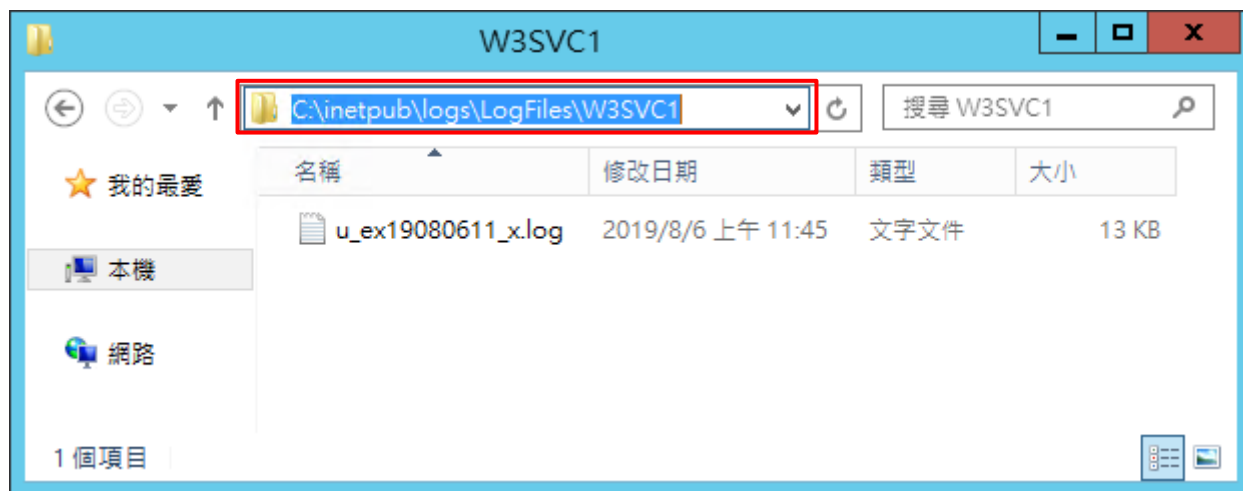
(6) 按下 [確定]



(7) 按下 [套用]

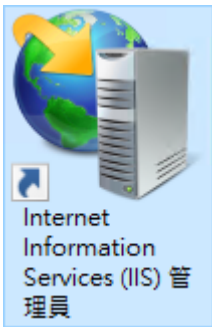


(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

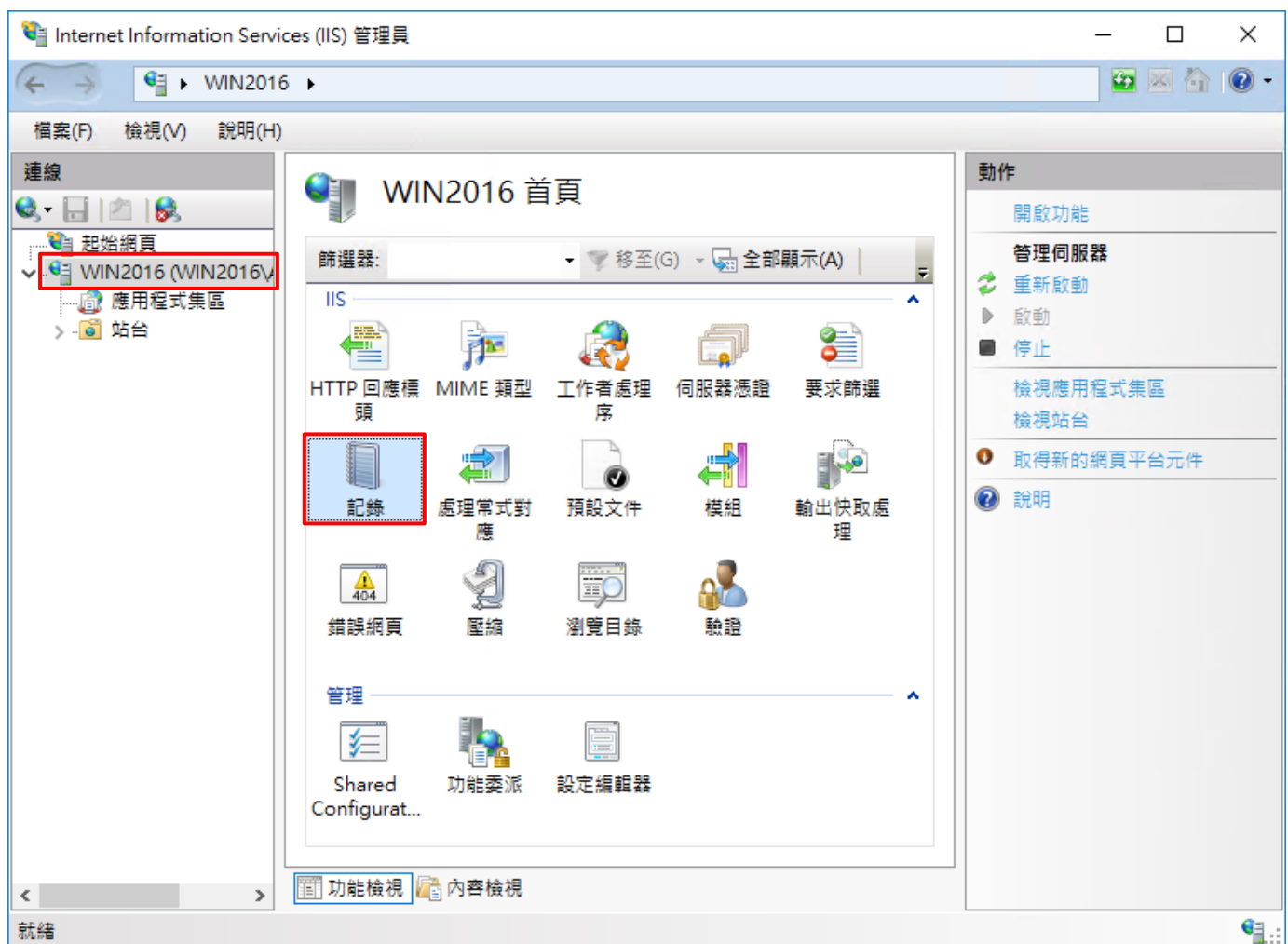


5. Windows 2016

(1) 開啟 [Internet Information Services (IIS) 管理員]

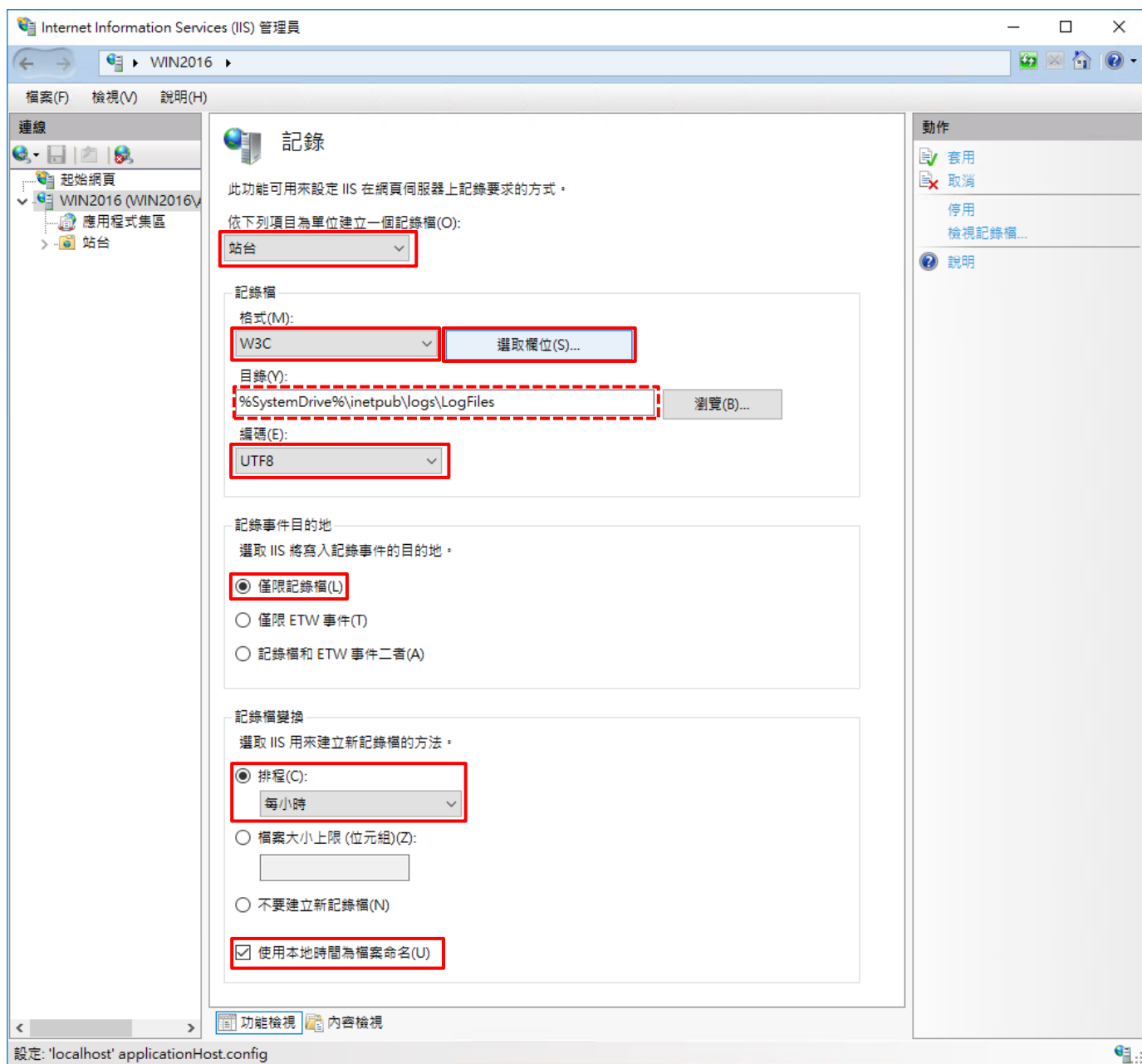


(2) 選擇 [IIS Server] -> 點選 [記錄]



(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取欄位]



(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.2.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

記錄所有資訊:

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

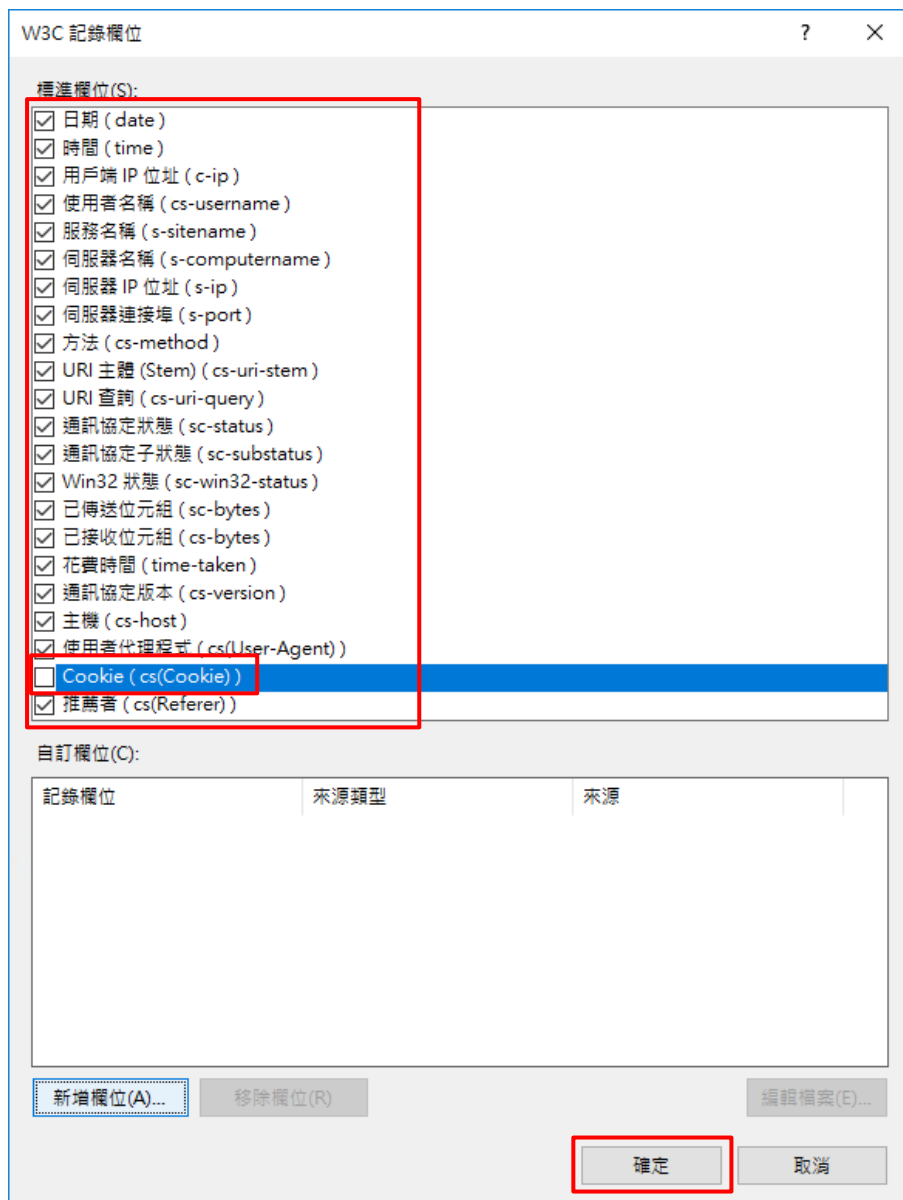
自訂欄位(C):

記錄欄位	來源類型	來源
------	------	----

新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

不紀錄 Cookie 資訊:



(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For
-> 按下 [確定]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按下 [確定]

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

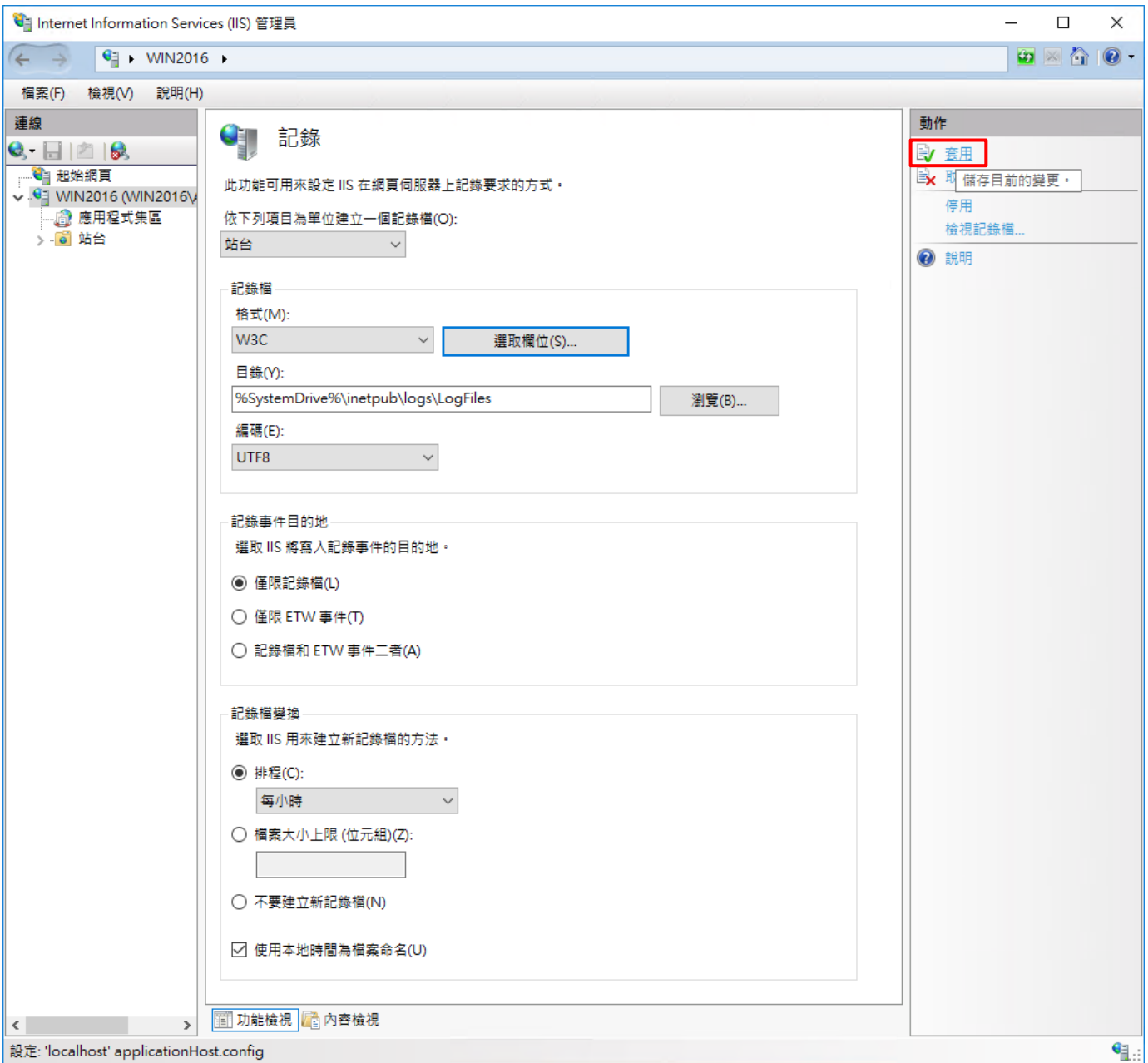
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

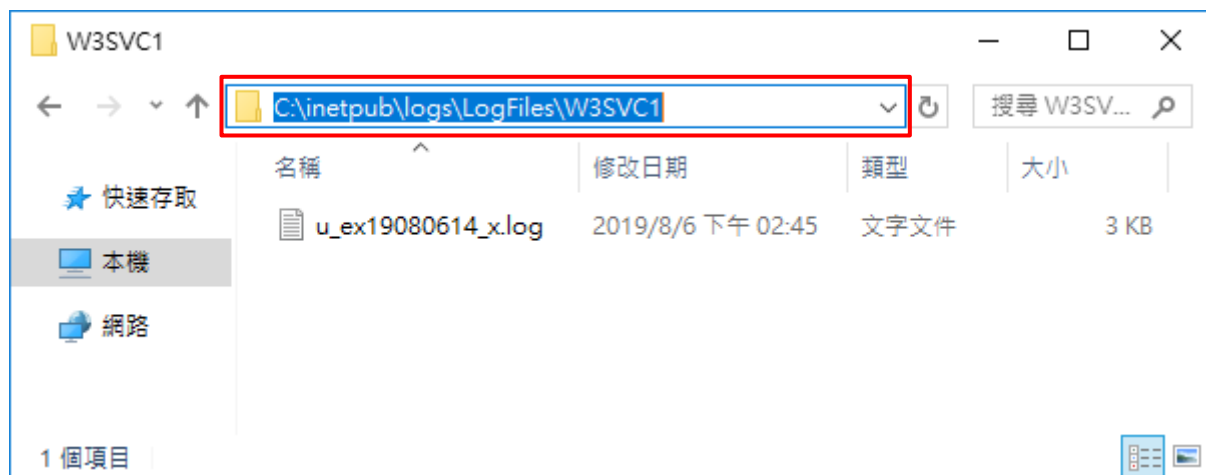
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [套用]

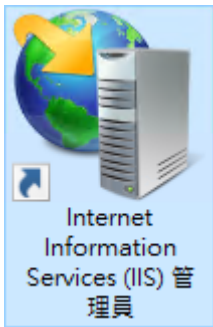


(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



6. Windows 2019

(1) 開啟 [Internet Information Services (IIS) 管理員]

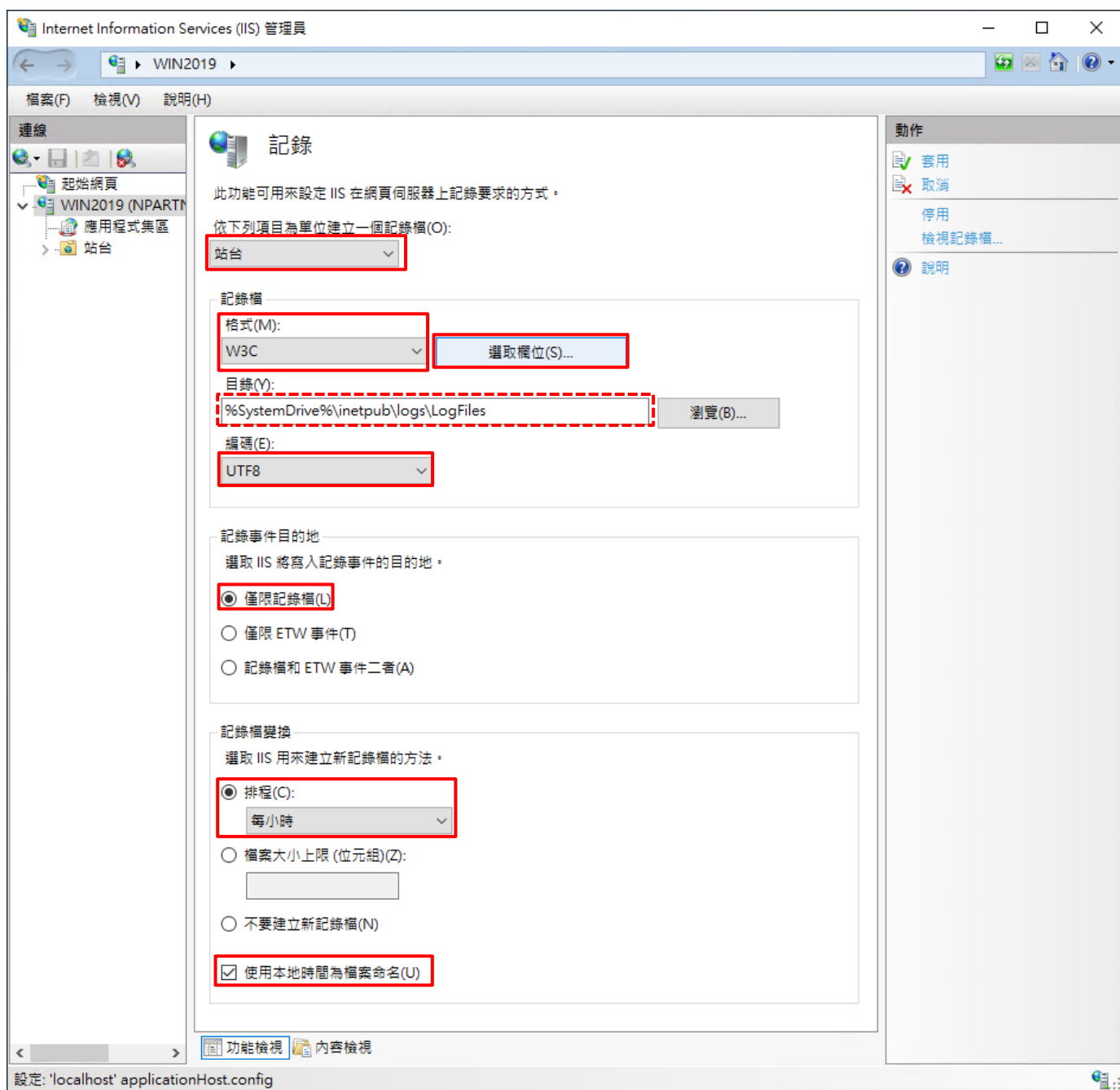


(2) 選擇 [IIS Server] -> 點選 [記錄]



(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取欄位]



(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.2.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

記錄所有資訊:

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

自訂欄位(C):

記錄欄位	來源類型	來源

新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

不記錄 Cookie 資訊:

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

自訂欄位(C):

記錄欄位	來源類型	來源
------	------	----

新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For
-> 按下 [確定]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按下 [確定]

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

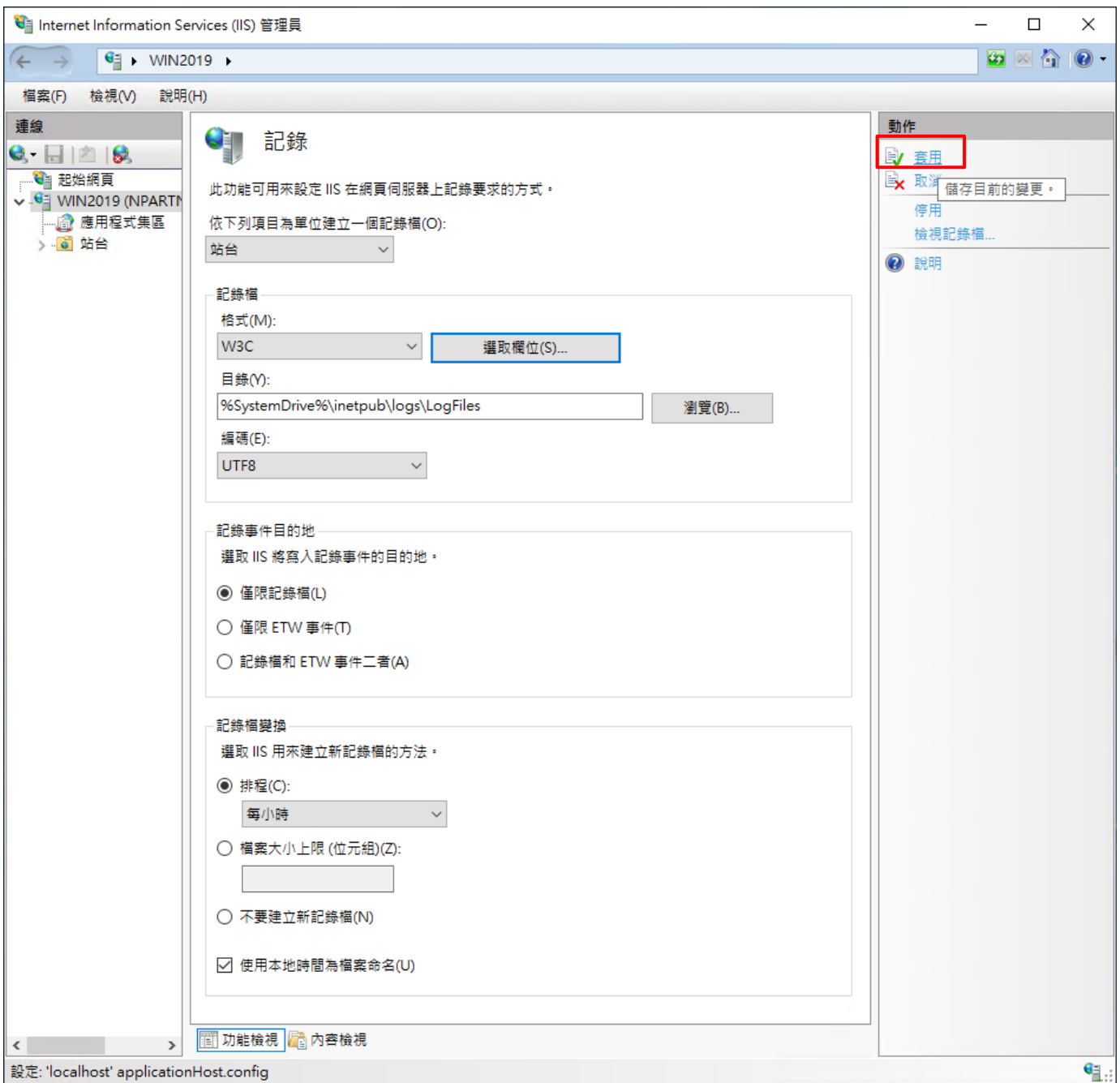
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

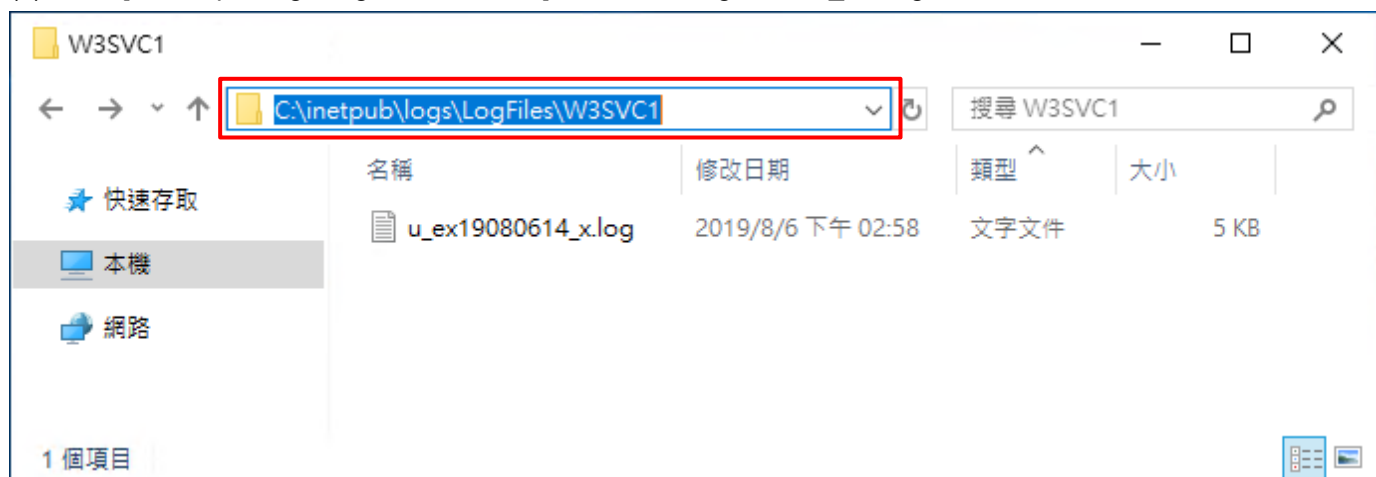
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [套用]

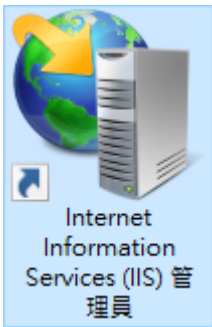


(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

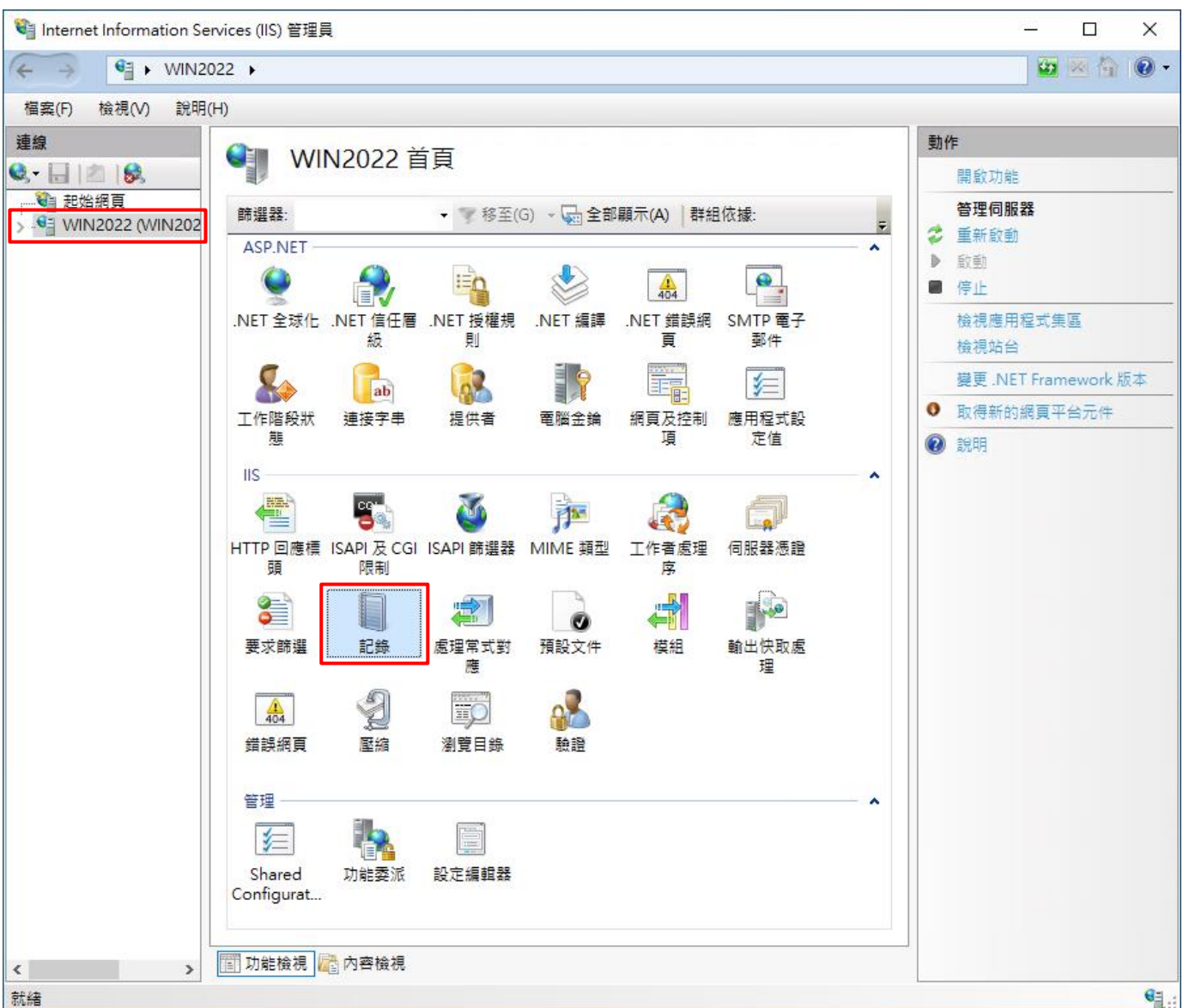


7. Windows 2022

(1) 開啟 [Internet Information Services (IIS) 管理員]

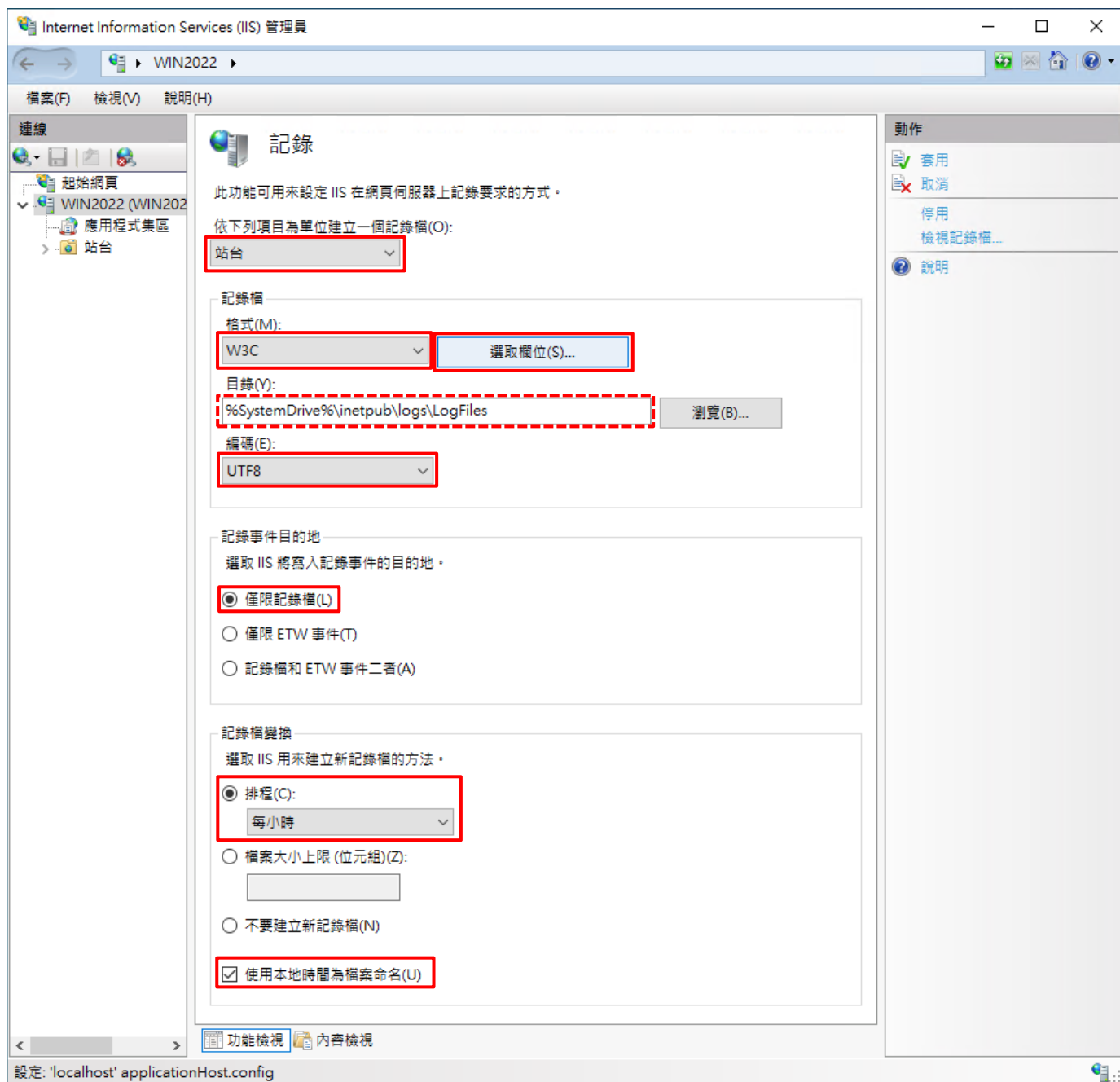


(2) 選擇 [IIS Server] -> 點選 [記錄]



(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選
[使用本地時間為檔案命名] -> 按下 [選取欄位]



(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [新增欄位]

※如不須紀錄 Cookie，可不勾選 Cookie (cs(Cookie))，並依據步驟 1.2.2.(2)下載”不紀錄 Cookie 資訊設定檔”，並套用。

記錄所有資訊：

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

自訂欄位(C):

記錄欄位	來源類型	來源
------	------	----

新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

不記錄 Cookie 資訊:

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

自訂欄位(C):

記錄欄位	來源類型	來源
------	------	----

新增欄位(A)... 移除欄位(R) 編輯欄位(E)...

確定 取消

(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [要求標頭] -> 輸入來源: X-Forwarded-For -> 按下 [確定]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按下 [確定]

W3C 記錄欄位

標準欄位(S):

- 日期 (date)
- 時間 (time)
- 用戶端 IP 位址 (c-ip)
- 使用者名稱 (cs-username)
- 服務名稱 (s-sitename)
- 伺服器名稱 (s-computername)
- 伺服器 IP 位址 (s-ip)
- 伺服器連接埠 (s-port)
- 方法 (cs-method)
- URI 主體 (Stem) (cs-uri-stem)
- URI 查詢 (cs-uri-query)
- 通訊協定狀態 (sc-status)
- 通訊協定子狀態 (sc-substatus)
- Win32 狀態 (sc-win32-status)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

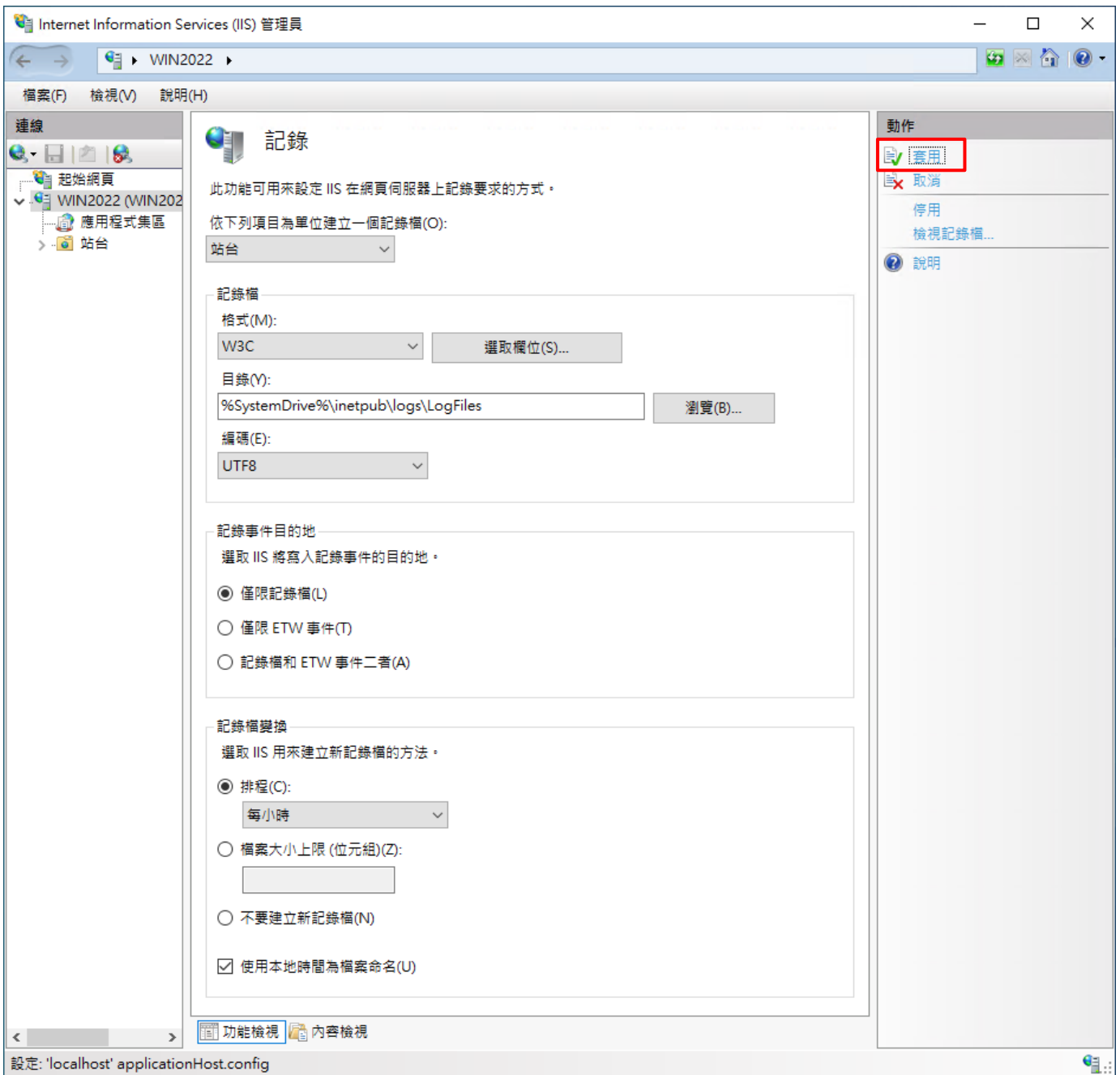
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

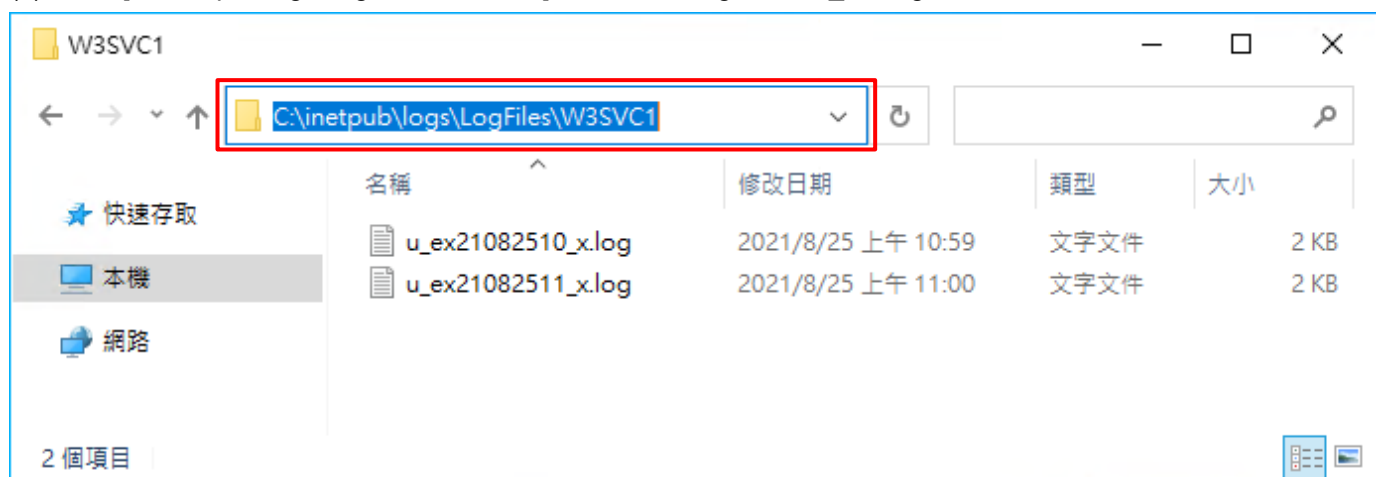
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [套用]



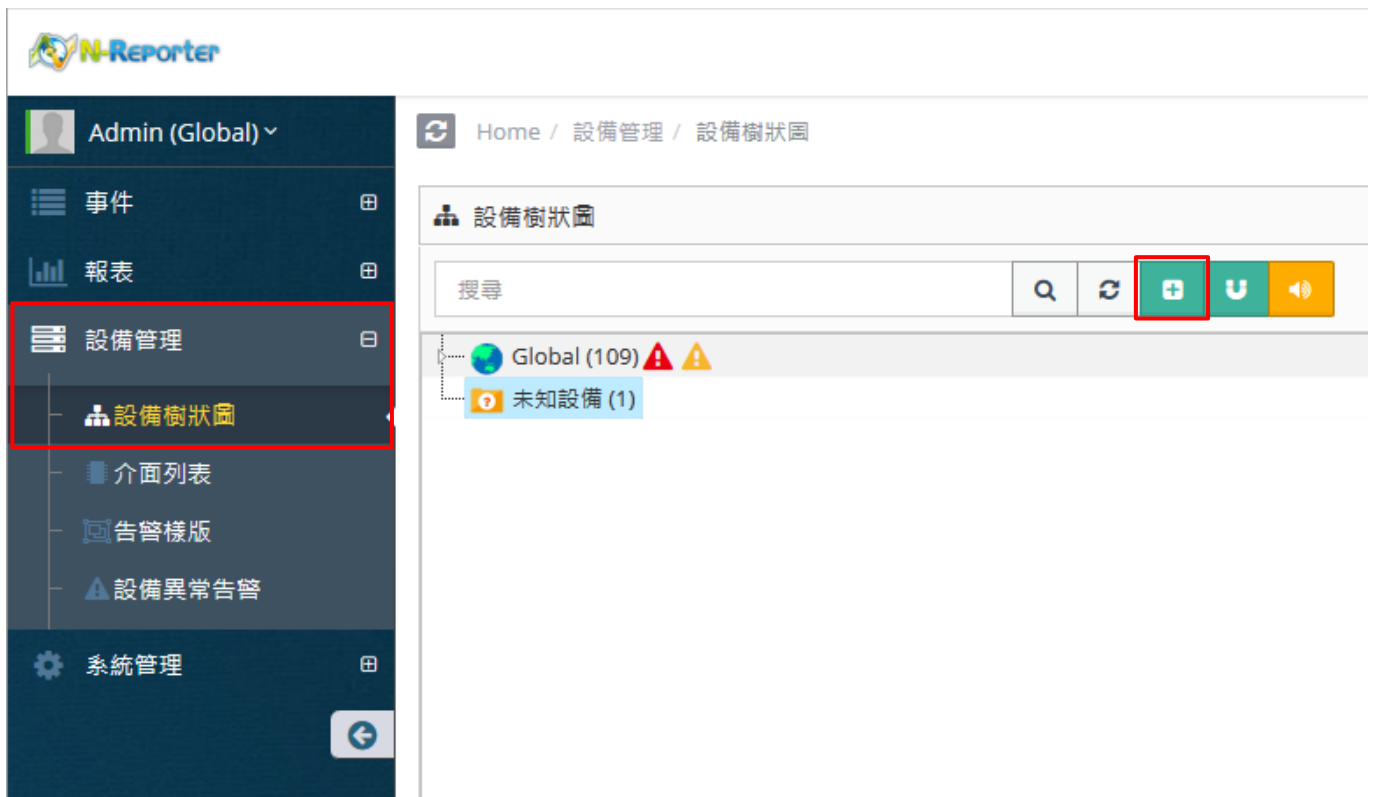
(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



8. N-Reporter

(1) 新增 IIS 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', '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', and '系統管理'. 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 '+', a blue 'U', and a yellow speaker icon. The main content area shows a tree structure with 'Global (109)' (with two warning icons) and '未知設備 (1)' (with one warning icon).

(2) 設定 IIS 設備的資料格式和 Facility

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [IIS] 和 Facility: [(22) local use 6 (local6)] -> 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
WinIIS-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
IIS

使用自定義資料格式

Facility
(22) local use 6 (local6)

編碼方式
UTF-8

日誌保留 Raw Data 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

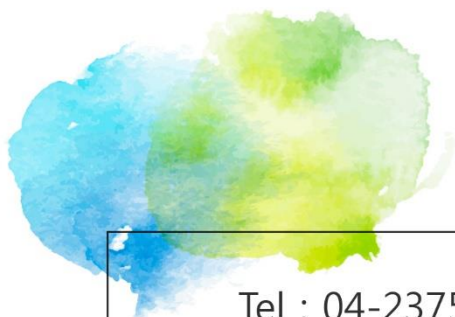
資料保留天數

經緯度
緯度 經度

確定 取消

若勾選 [日誌保留 Raw Date] ·

[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