



N-Partner



如何設定 Microsoft IIS log

V014

2019/08/09



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 架構	3
1.2 NXLog 安裝	4
1.3 NXLog 設定檔	5
1.4 NXLog 啟動服務	7
2. Windows 2003.....	8
3. Windows 2008.....	14
4. Windows 2012.....	29
5. Windows 2016.....	36
6. Windows 2019.....	43
7. N-Reporter	50



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 Microsoft IIS(Internet Information Server) 記錄。

NXLog 工具將 Microsoft IIS 記錄轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。

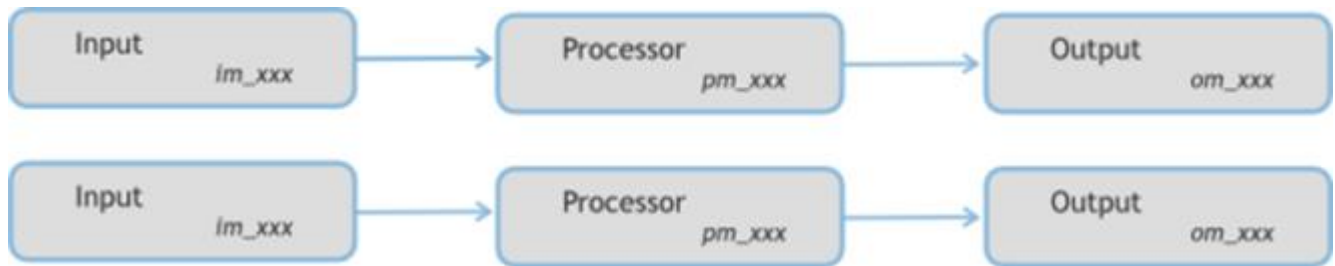
此文件適用於 Windows Server 2003 / 2008 / 2012 / 2016 / 2019 作業系統的版本。

1. NXLog

1.1 NXLog 架構

NXLog 的 plugin 架構允許任何類型的輸入讀取資料，解析和轉換訊息的格式，然後將其發送到任何類型的輸出。可以同時使用不同的輸入，處理和輸出模組來滿足事件記錄。

<https://nxlog.co/documentation/nxlog-user-guide#modules-im>



1.2 NXLog 安裝

(1) 下載 NXLog

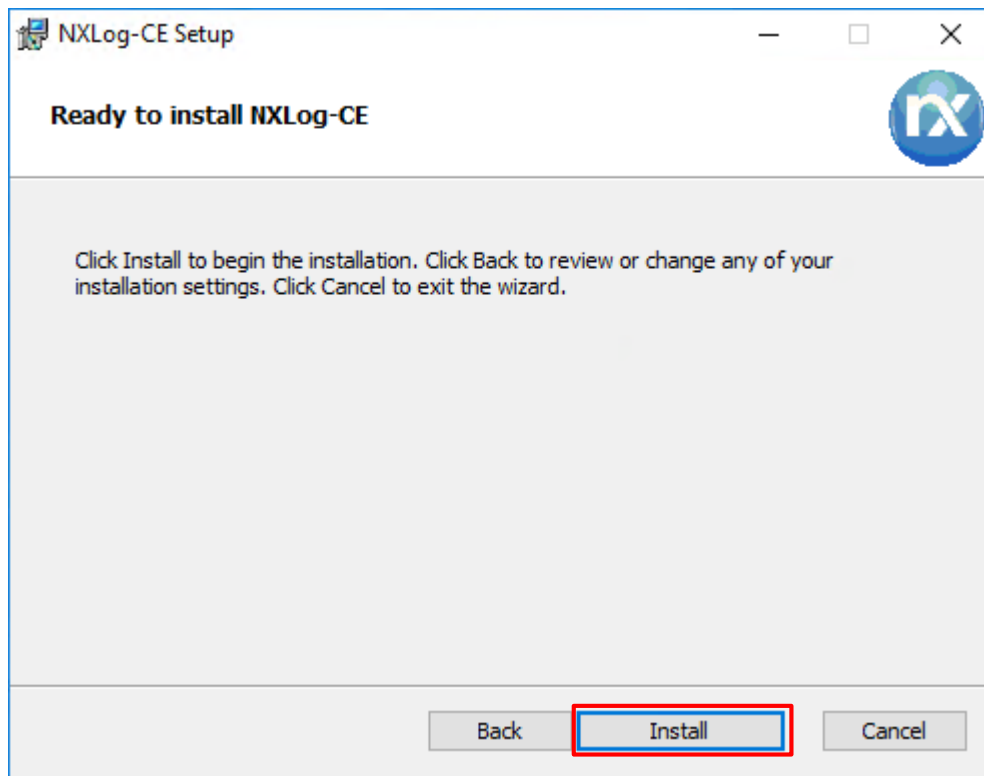
前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 nxlog-ce-x.x.xxxx.msi · 範例: nxlog-ce-2.10.2150.msi



(2) 安裝 NXLog

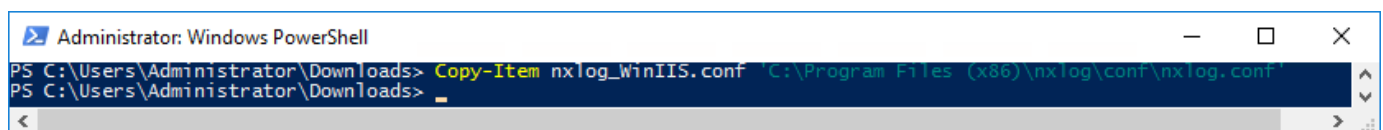
點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish]



(3) 下載並覆蓋 NXLog 設定檔

下載連結: https://www.npartnertech.com/download/tech/nxlog_WinIIS.conf ->

覆蓋 NXLog 設定檔 `Copy-Item nxlog_WinIIS.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'`



1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud    192.168.3.51
define BASEDIR   C:\inetpub\logs\LogFiles
define ROOT      C:\Program Files (x86)\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       '%BASEDIR%\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>
```

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\nxlog
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud    192.168.3.51
```

藍色文字部位請輸入 Microsoft IIS 記錄檔資料夾路徑

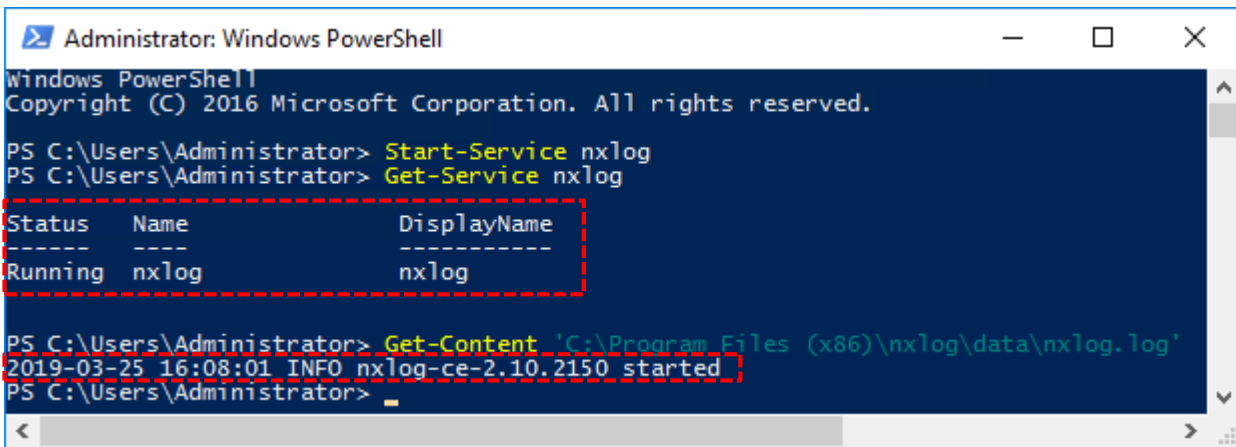
```
define BASEDIR   C:\inetpub\logs\LogFiles
```

藍色文字部位請輸入 IIS 記錄檔名稱

```
File            '%BASEDIR%\u_ex*.log'
```


1.4 NXLog 啟動服務

開啟 [Windows PowerShell] -> 輸入 `Start-Service nxlog` 啟動 nxlog 服務和 `Get-Service nxlog` 查看 nxlog 服務狀態 -> `Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息



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

PS C:\Users\Administrator> Start-Service nxlog
PS C:\Users\Administrator> Get-Service nxlog

Status      Name      DisplayName
-----
Running     nxlog     nxlog

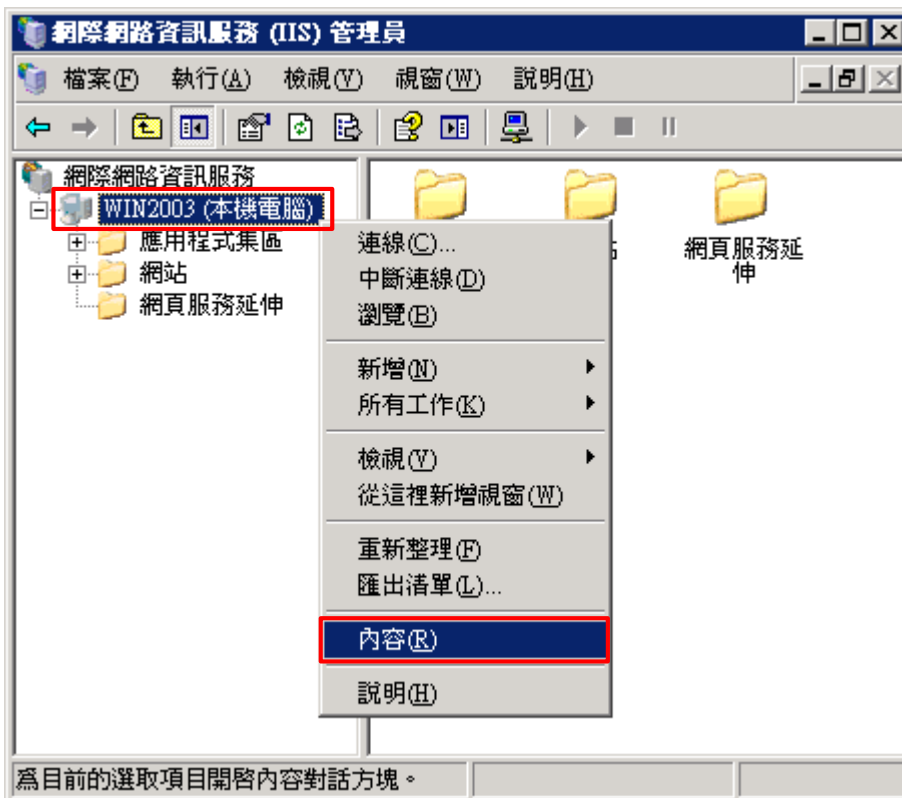
PS C:\Users\Administrator> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2019-03-25 16:08:01 INFO nxlog-ce-2.10.2150 started
PS C:\Users\Administrator>
```

2. Windows 2003

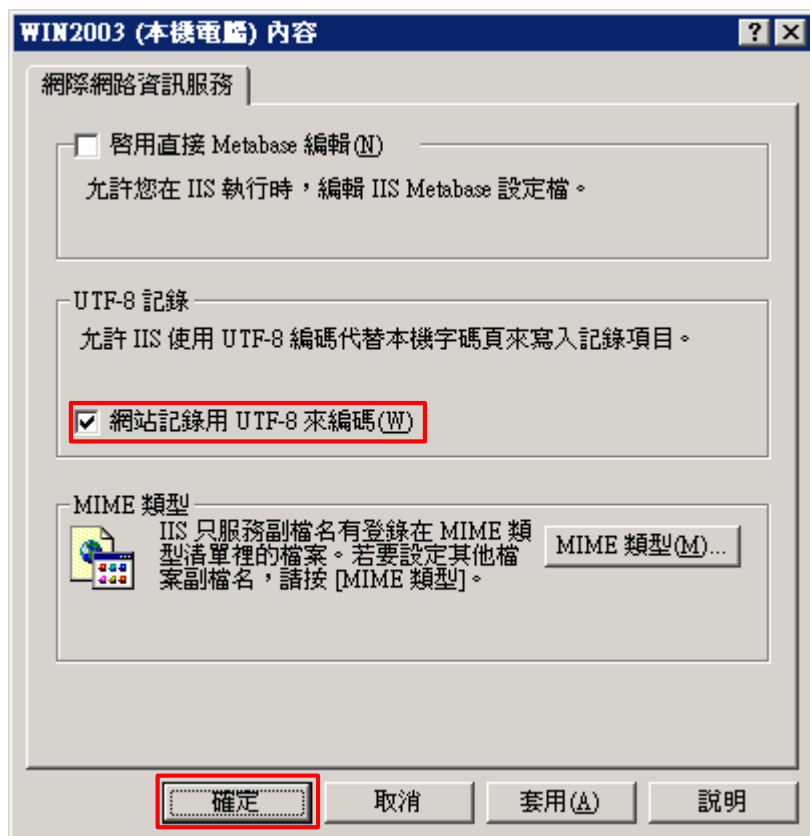
(1) 開啟 [網際網路資訊服務 (IIS) 管理員]



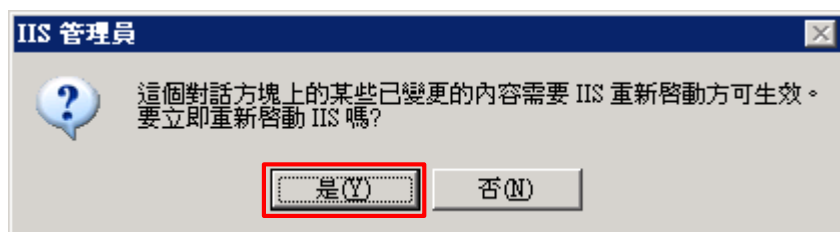
(2) 在 [IIS Server(WIN2003)] 上按滑鼠右鍵 -> 選擇 [內容]



(3) 勾選 [網站記錄用 UTF-8 來編碼]-> 按下 [確定]



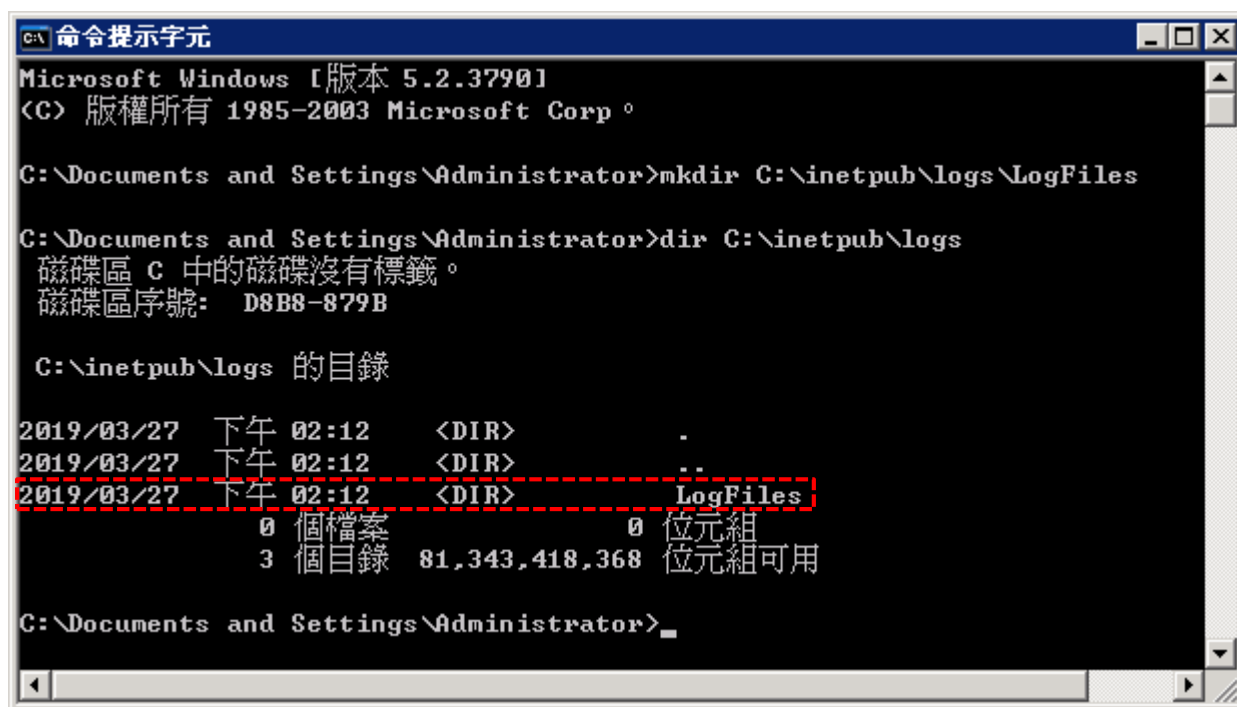
(4) 按下 [確定]



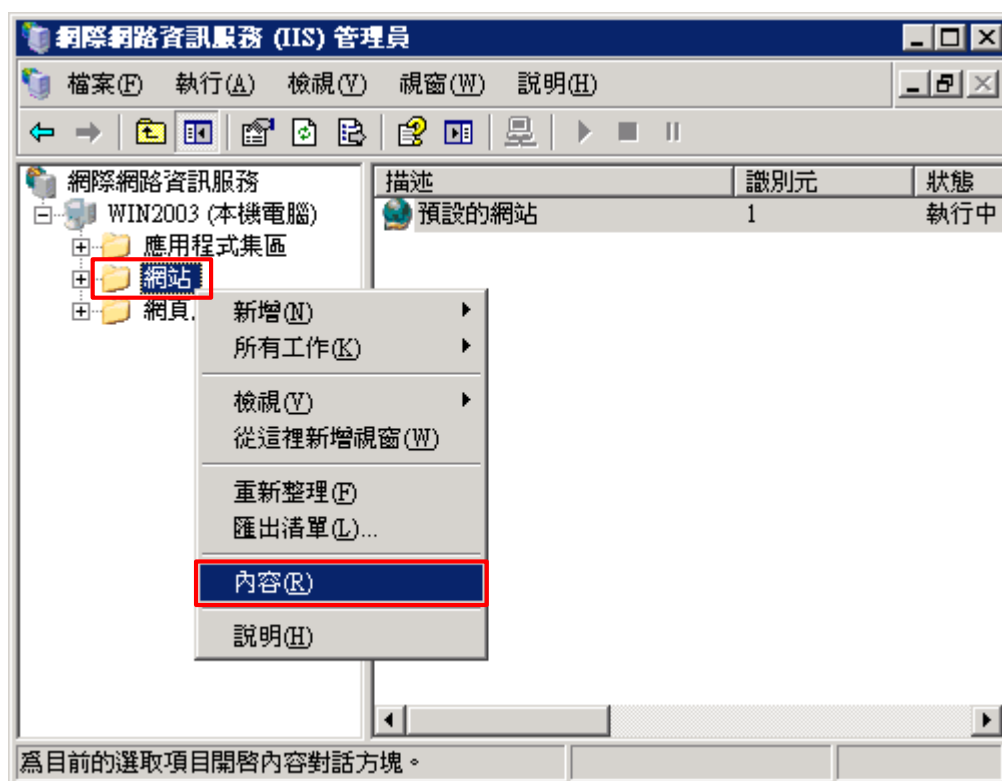
(5) 新增 IIS LogFiles 資料夾和確認 IIS LogFiles 資料夾

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

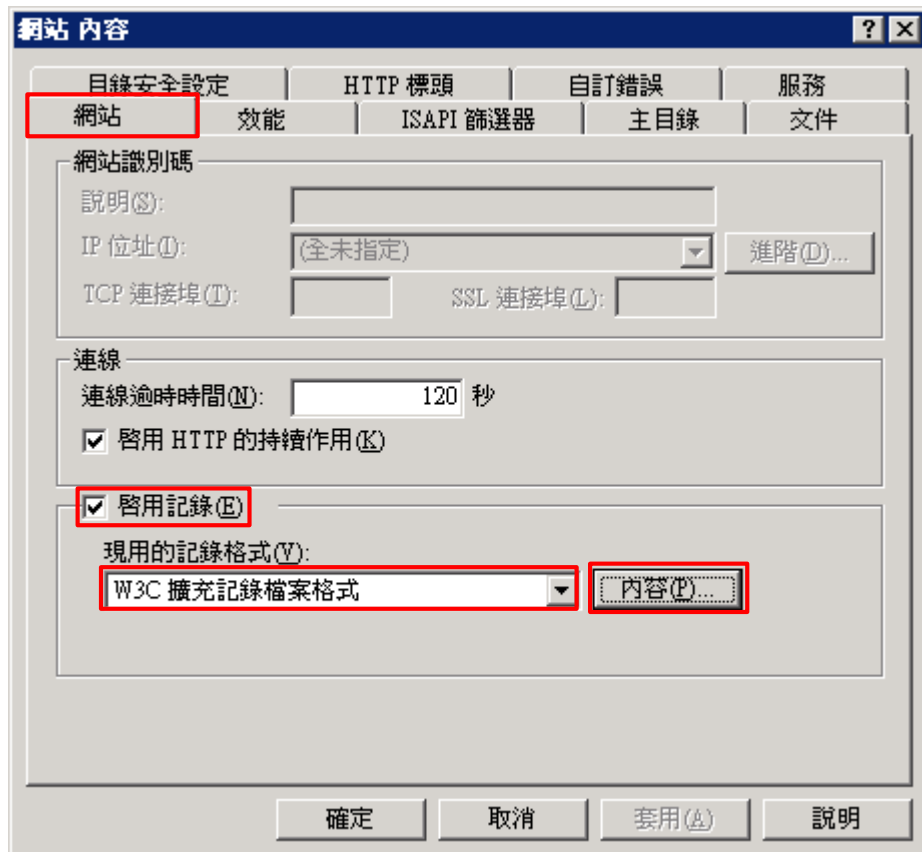
```
C:\> dir C:\inetpub\logs
```



(6) 在 [網站] 上按滑鼠右鍵 -> 選擇 [內容]

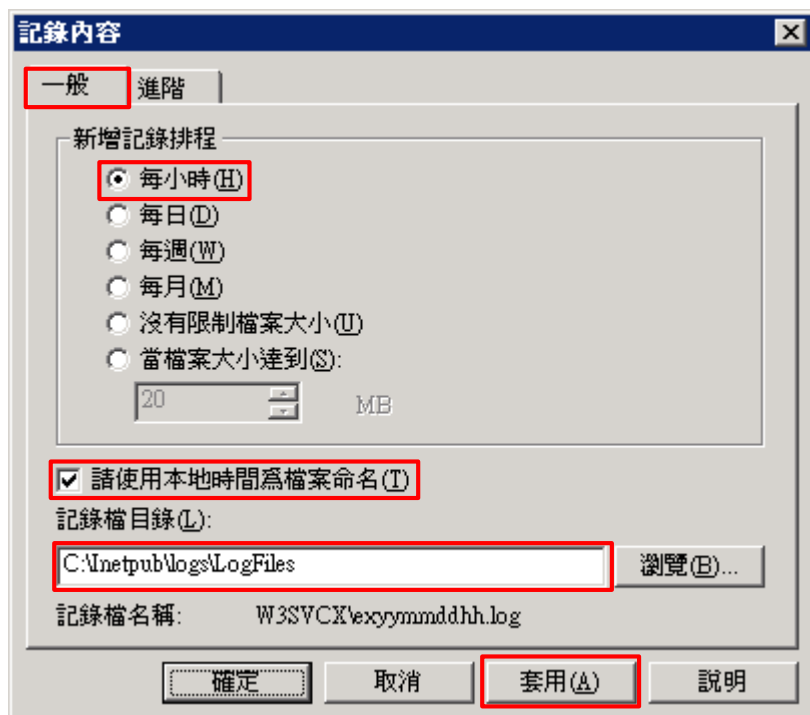


(7) [網站] 頁面: 勾選 [啟用記錄] -> 現用的記錄格式選擇 [W3C 擴充記錄檔案格式] -> 按下 [內容]

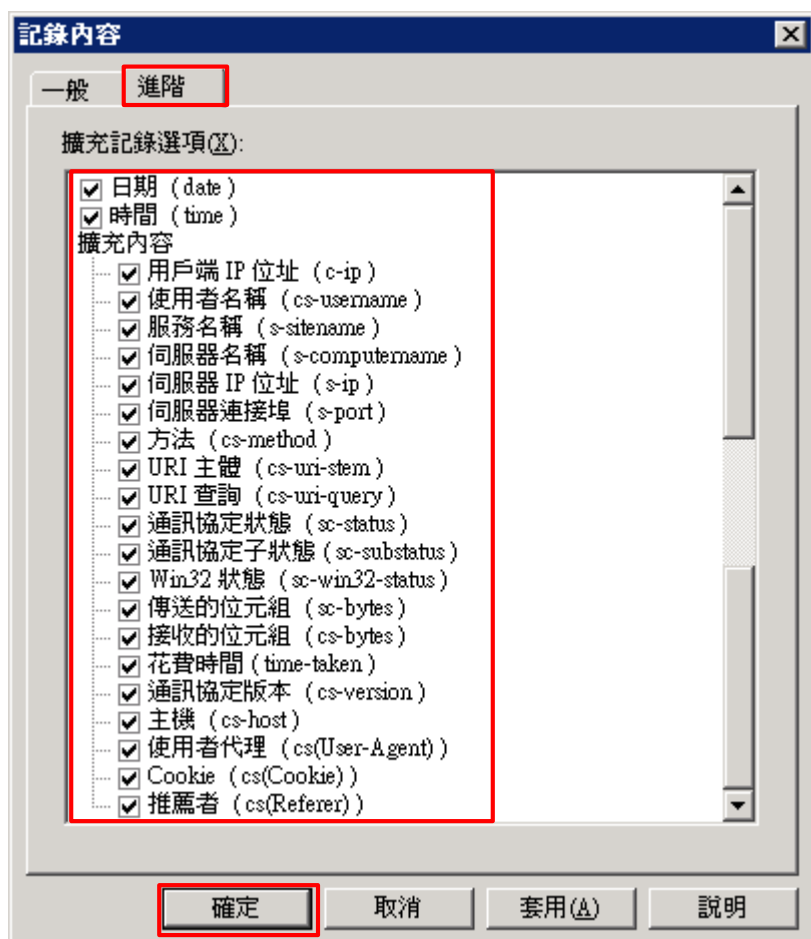


(8) [一般] 頁面: 新增記錄排程點選 [每小時] -> 勾選 [請使用本地時間為檔案命名] -> 記錄檔目錄輸入

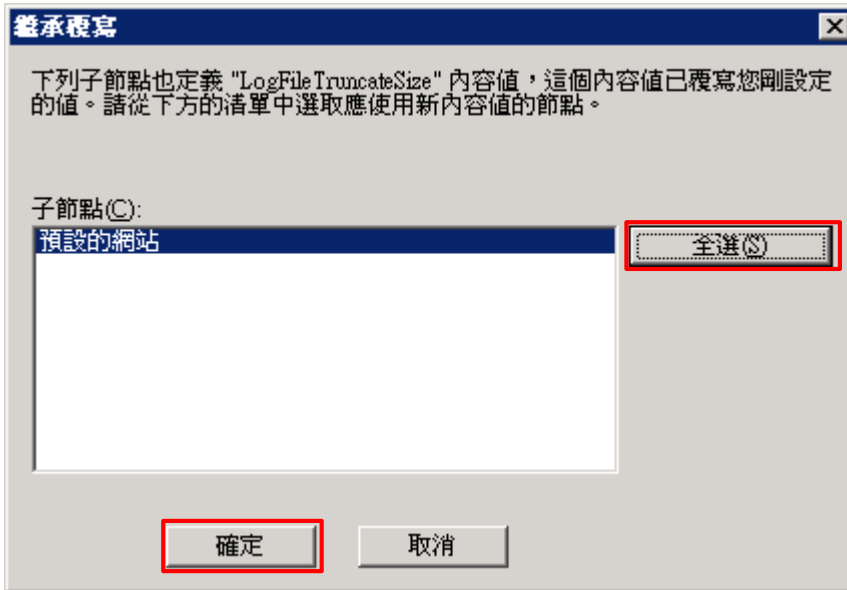
C:\inetpub\logs\LogFiles -> 按下 [套用]



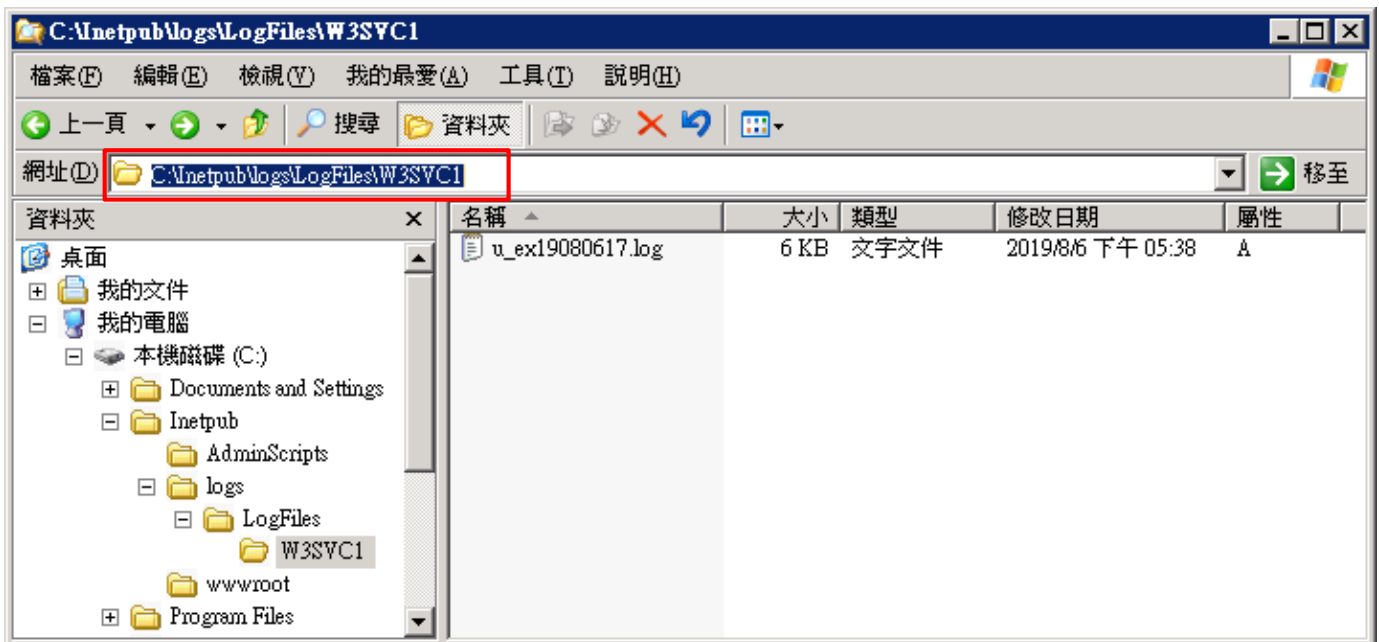
(9) [進階] 頁面：擴充記錄選項勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[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]



(10) 按下 [全選] 和 [確定]



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



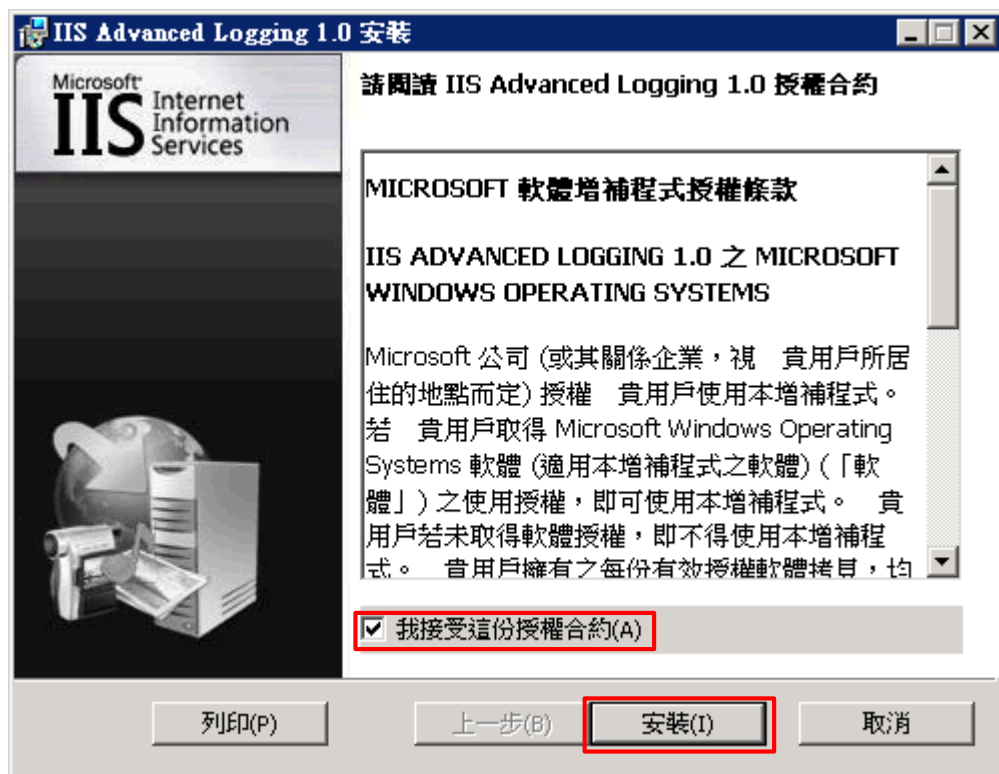
3. Windows 2008

(1) 安裝 IIS Advanced Logging

IIS Advanced Logging 提供豐富、彈性的資料集合和即時的記錄功能。記錄任何 HTTP 要求/回應標頭、IIS 伺服器變數和用戶端欄位，以追蹤使用者參與的情況。

<https://www.microsoft.com/zh-tw/download/details.aspx?id=7211>

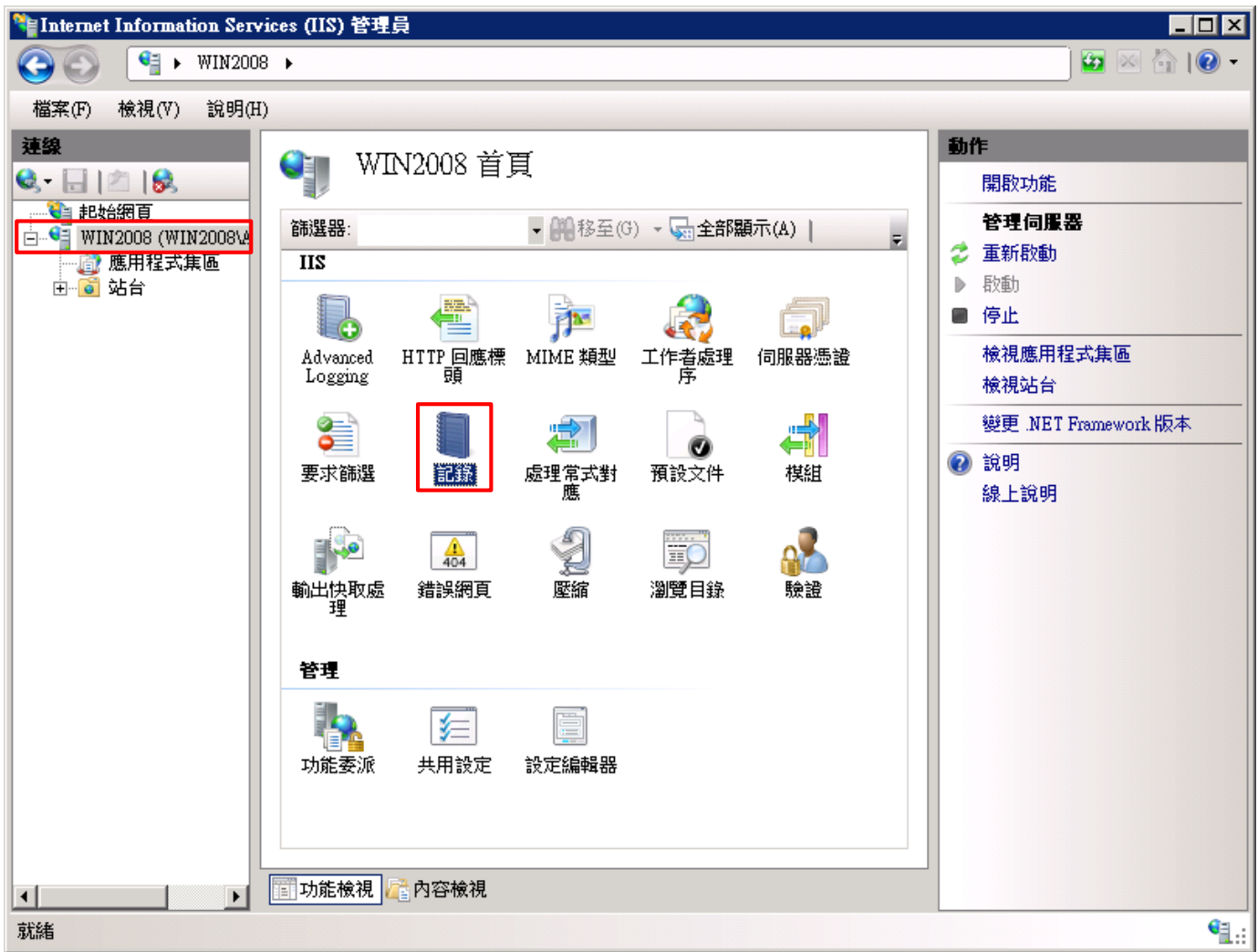
點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]



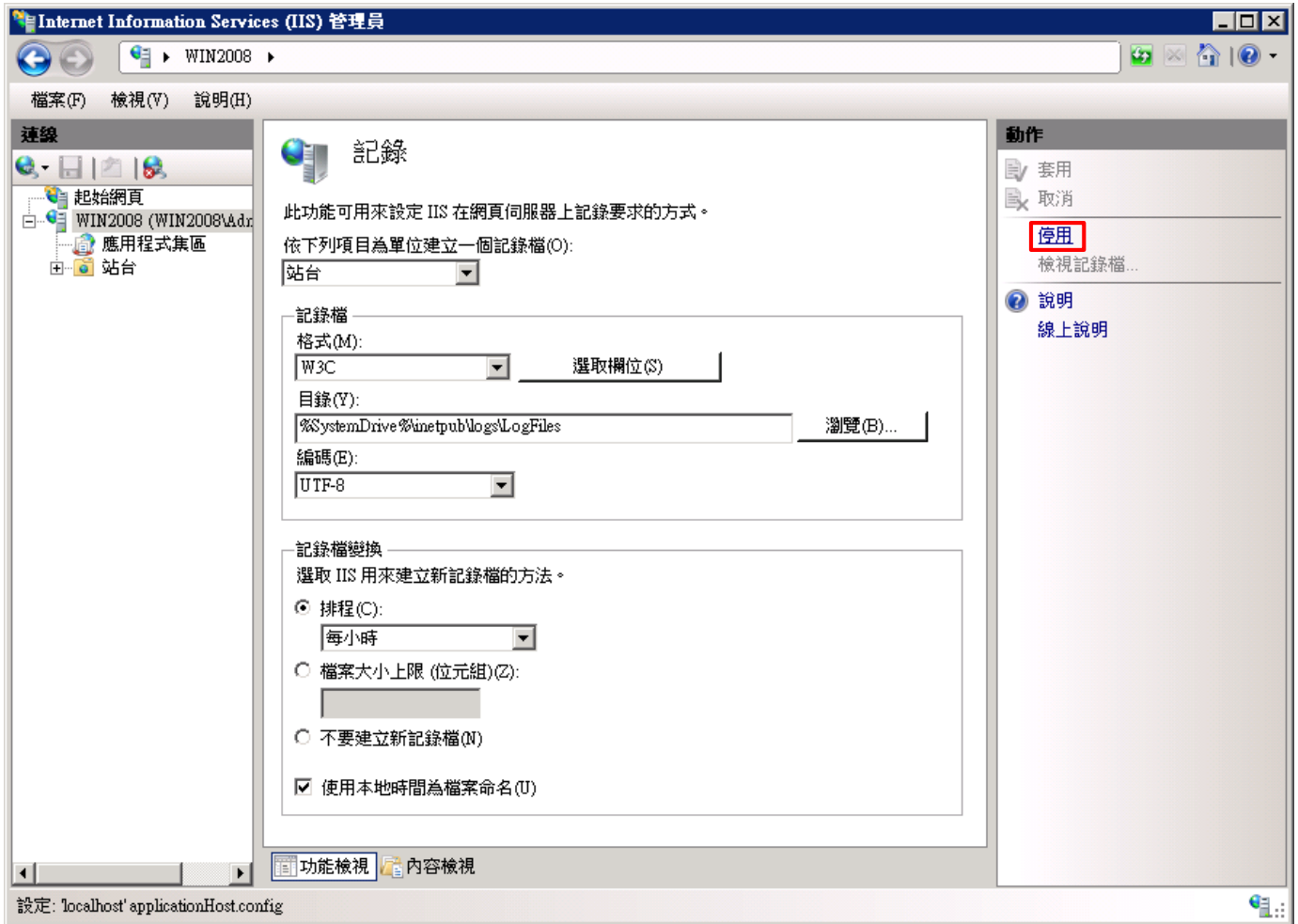
(2) 開啟 [Internet Information Services (IIS) 管理員]



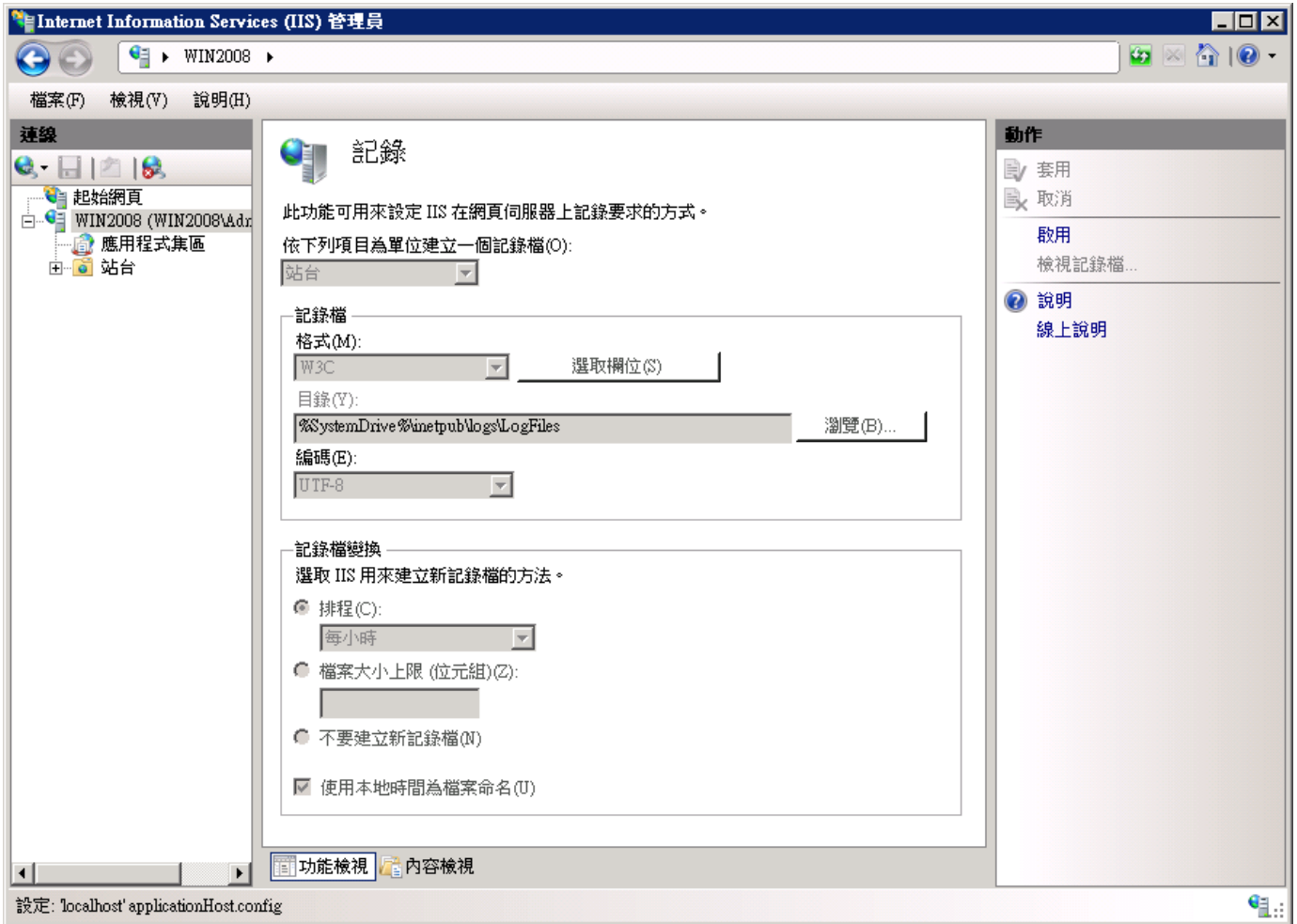
(3) 選擇 [IIS Server] -> 點選 [Logging(記錄)]



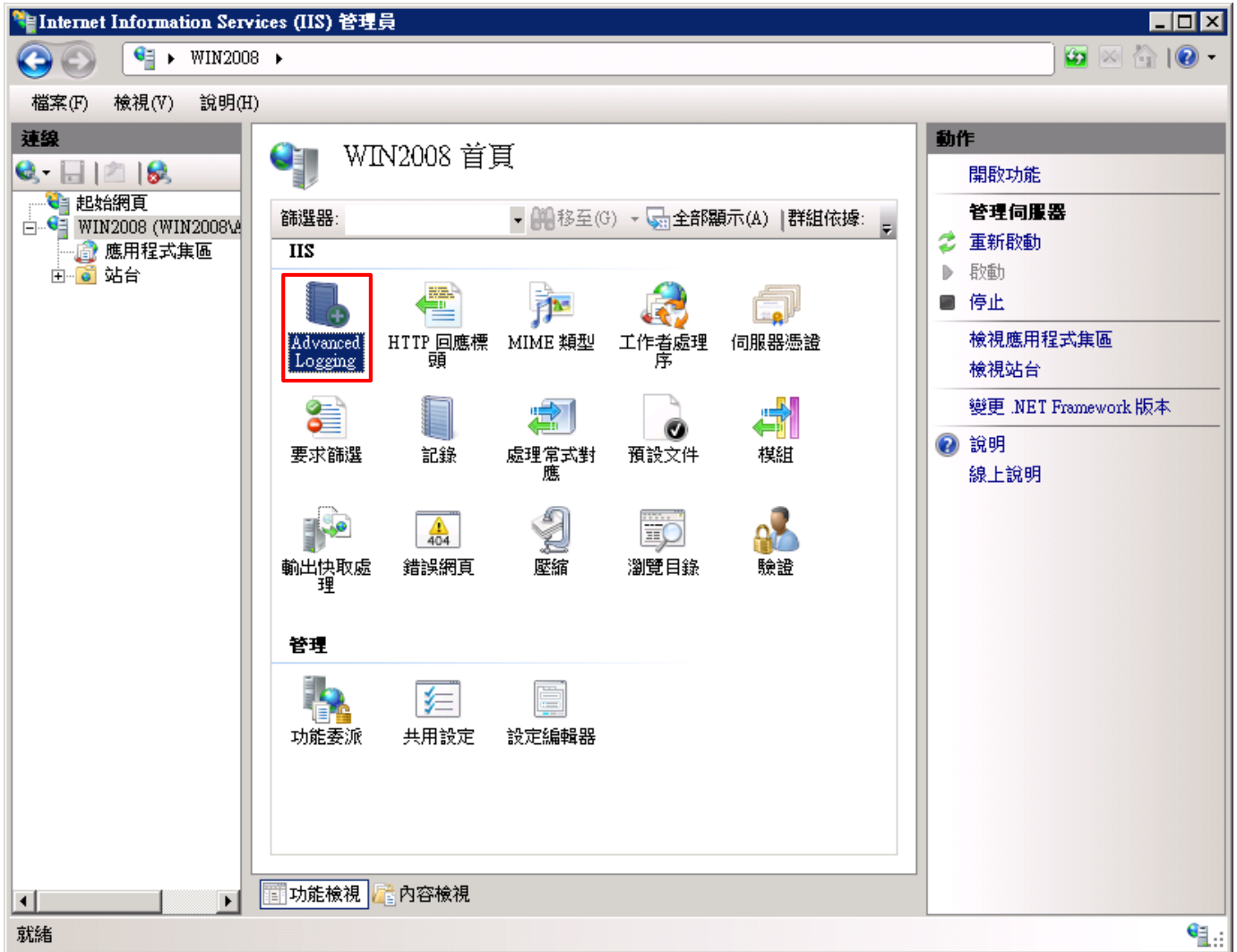
(4) 點選 [停用]



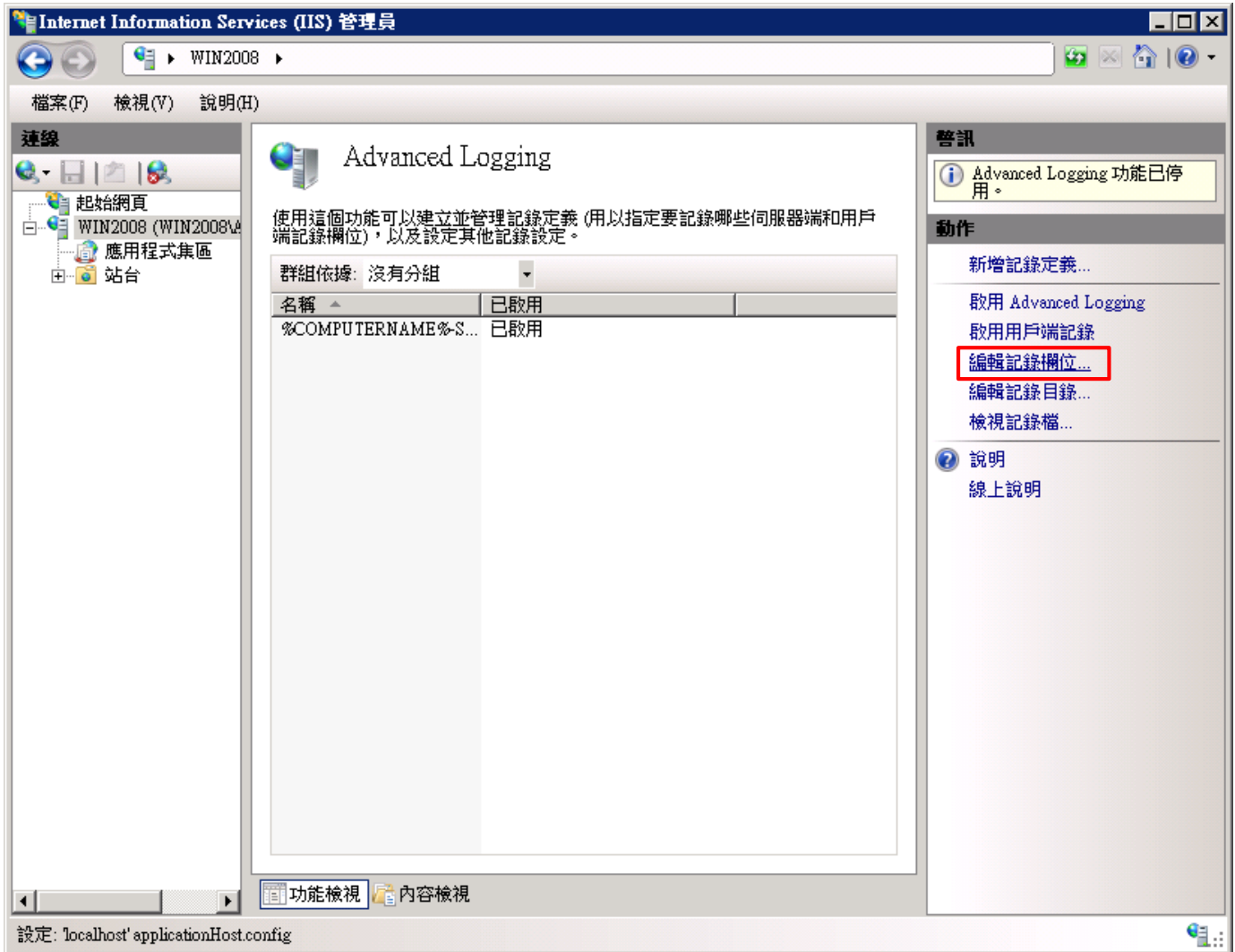
(5) 確認記錄已停用



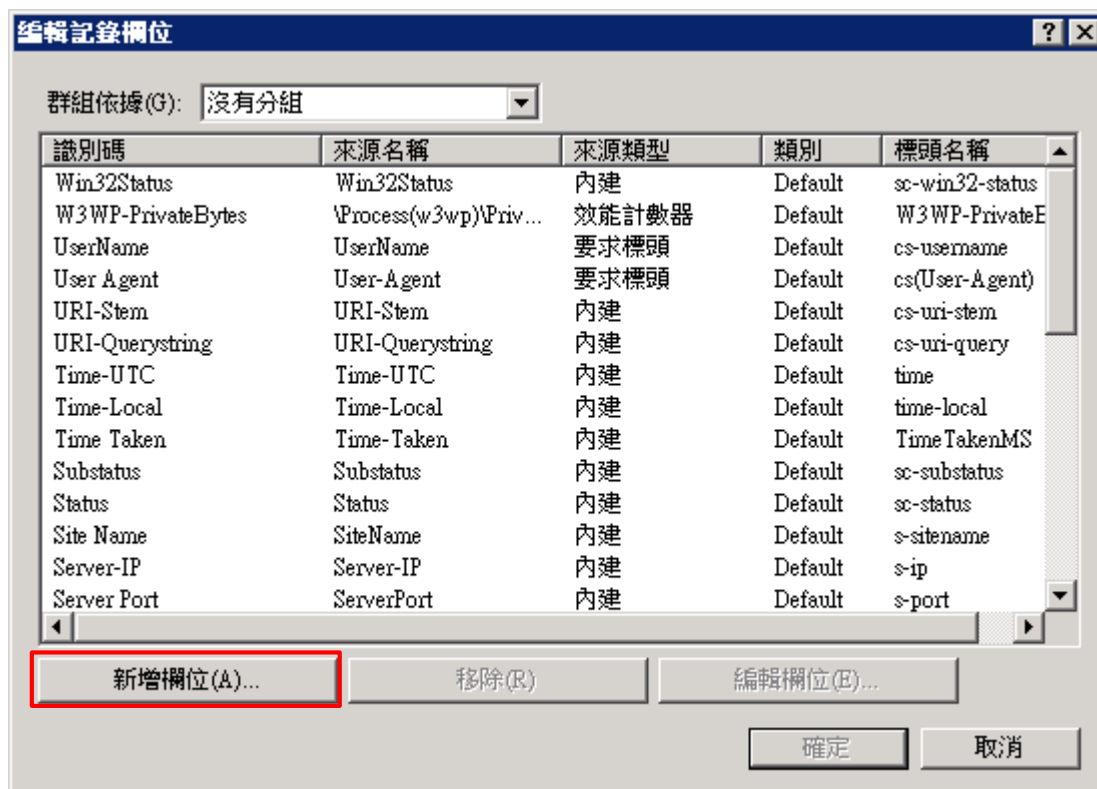
(6) 點選 [Advanced Logging]



(7) 按下 [編輯記錄欄位]



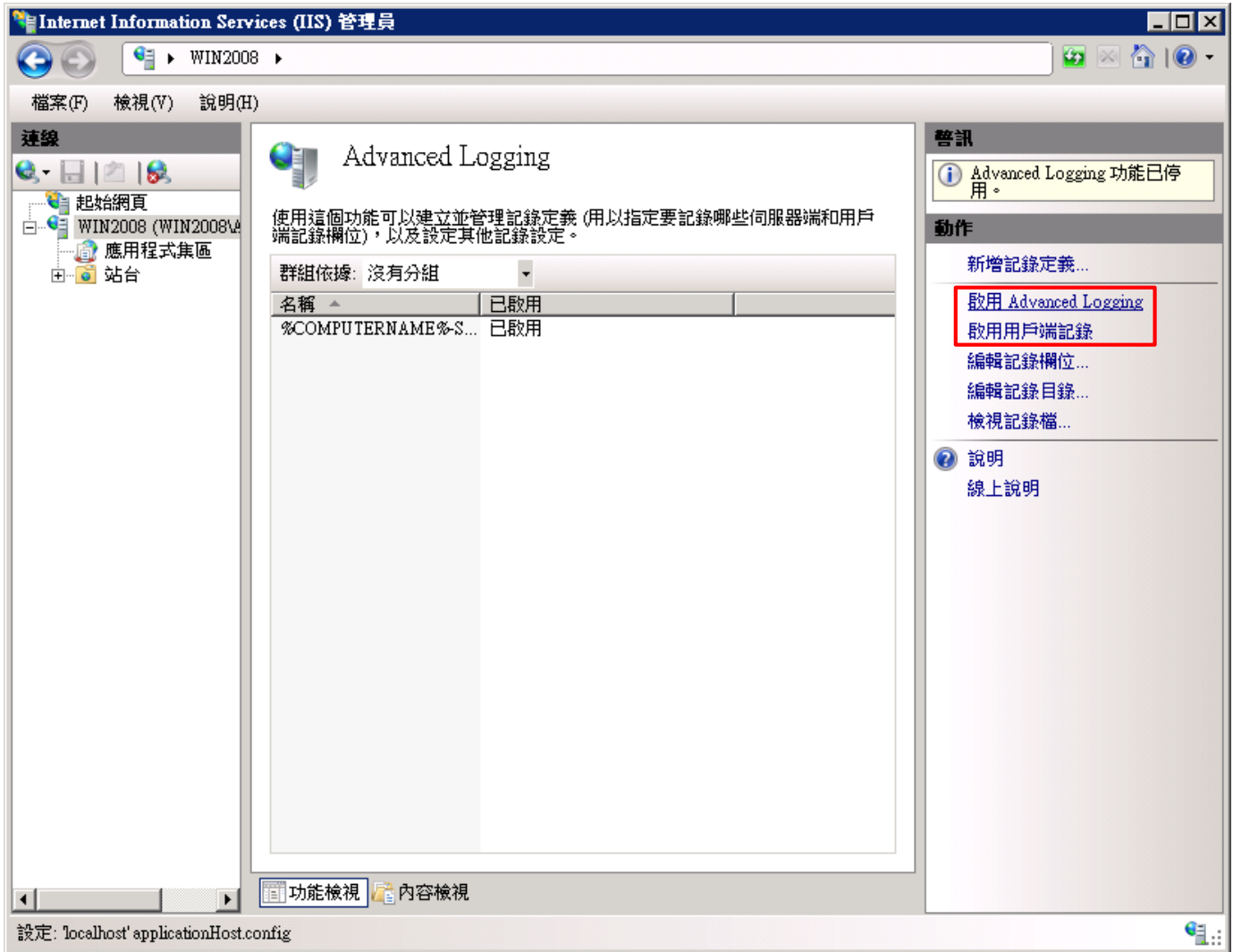
(8) 按下 [新增欄位]



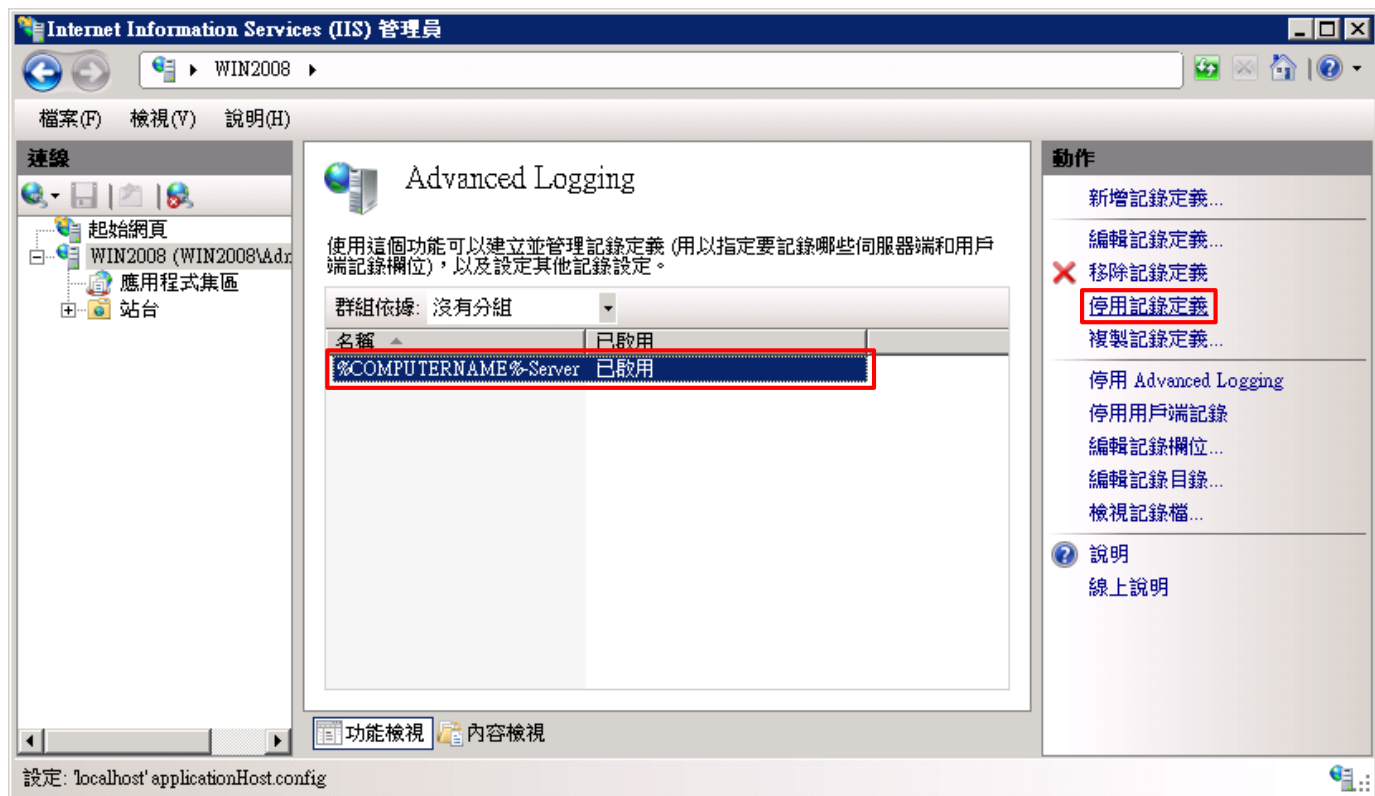
(9) 輸入欄位識別碼: **X-Forwarded-For** -> 選擇類別: [Default] -> 來源類型: [Request Header(要求標頭)] -> 輸入來源名稱: **X-Forwarded-For** -> 按下 [確定]



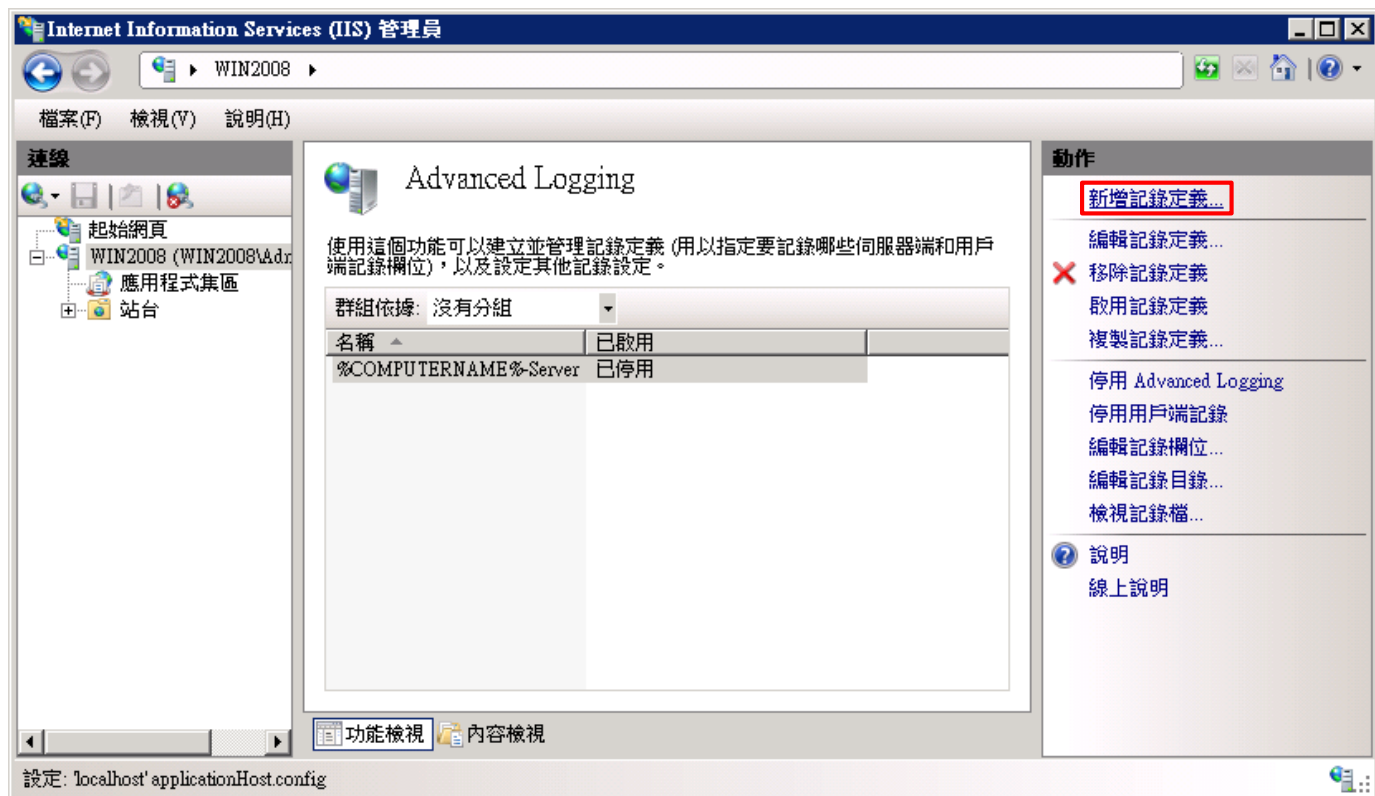
(10) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]



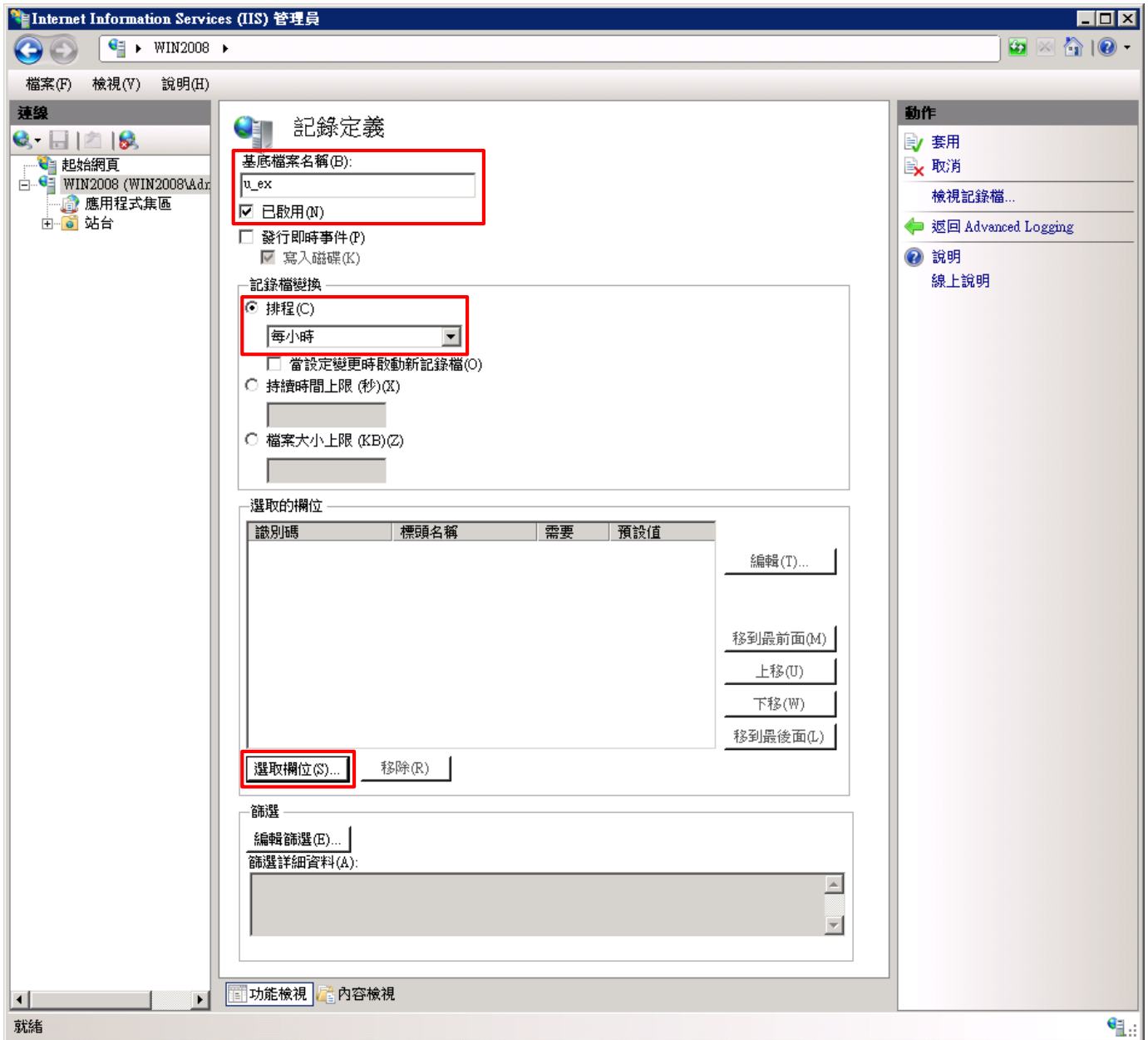
(11) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]



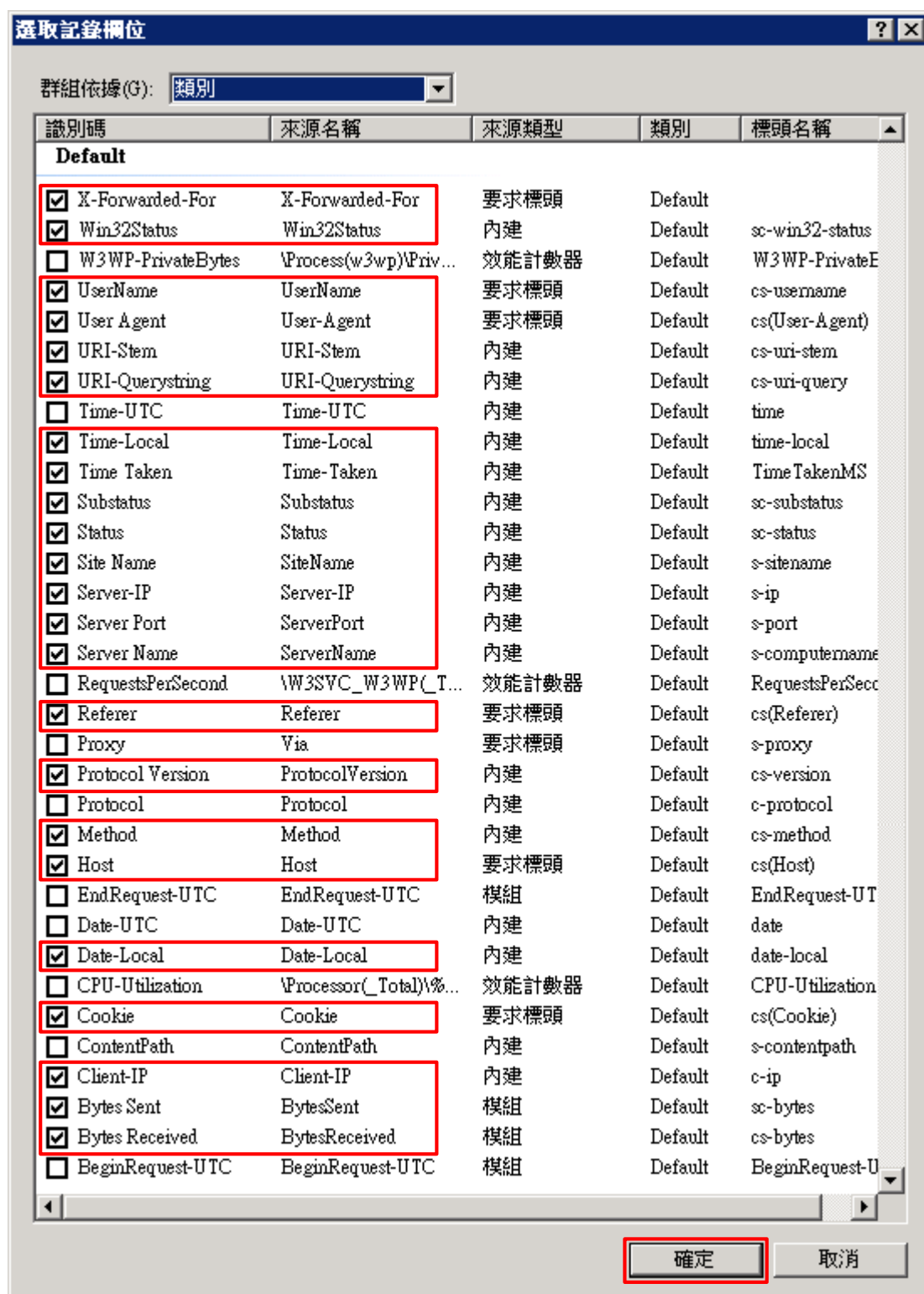
(11) 點選 [新增記錄定義]



(12) 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]



(13) 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]



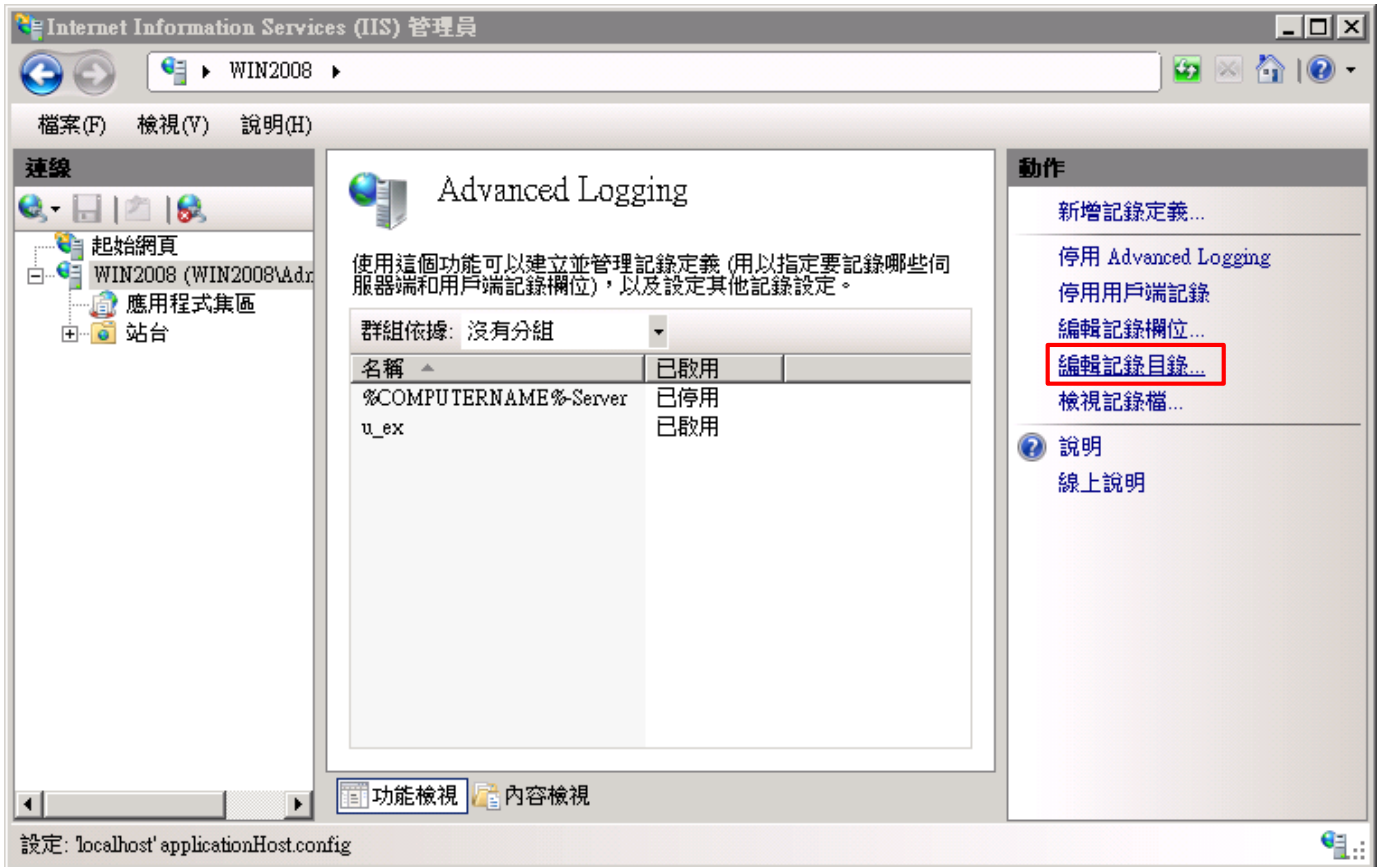
(14) 調整選取的欄位: [Data-Local(date-local)]、[Time-Local(time-local)]、[Site Name(s-sitename)]、[Server Name(s-computername)]、[Server-IP(s-ip)]、[Method(cs-method)]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Server Port(s-port)]、[UserName(cs-username)]、[Client-IP(c-ip)]、[Protocol Version(cs-version)]、[User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

The screenshot shows the 'Logging Definitions' configuration window in IIS Manager. The 'Selected Fields' table is as follows:

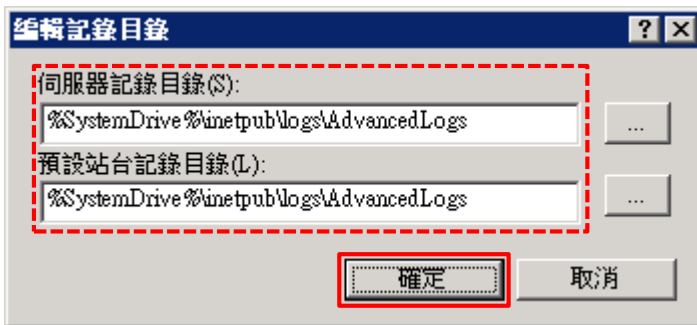
識別碼	標頭名稱	需要	預設值
Date-Local	date-local	否	
Time-Local	time-local	否	
Site Name	s-sitename	否	
Server Name	s-computername	否	
Server-IP	s-ip	否	
Method	cs-method	否	
URI-Stem	cs-uri-stem	否	
URI-Querystring	cs-uri-query	否	
Server Port	s-port	否	
UserName	cs-username	否	
Client-IP	c-ip	否	
Protocol Version	cs-version	否	
User Agent	cs(User-Agent)	否	
Cookie	cs(Cookie)	否	
Referer	cs(Referer)	否	
Host	cs(Host)	否	
Status	sc-status	否	
Substatus	sc-substatus	否	
Win32Status	sc-win32-status	否	
Bytes Sent	sc-bytes	否	
Bytes Received	cs-bytes	否	
Time Taken	TimeTakenMS	否	
X-Forwarded-For		否	

The 'Actions' pane on the right shows the 'Apply' button highlighted with a red box. Other buttons include 'Cancel', 'View Log...', 'Return Advanced Logging', 'Help', and 'Online Help'.

(15) 點選 [編輯記錄目錄]



(16) 確認伺服器記錄目錄和預設站台記錄目錄 -> 按下 [確定]



(17) 修改 nxlog.conf

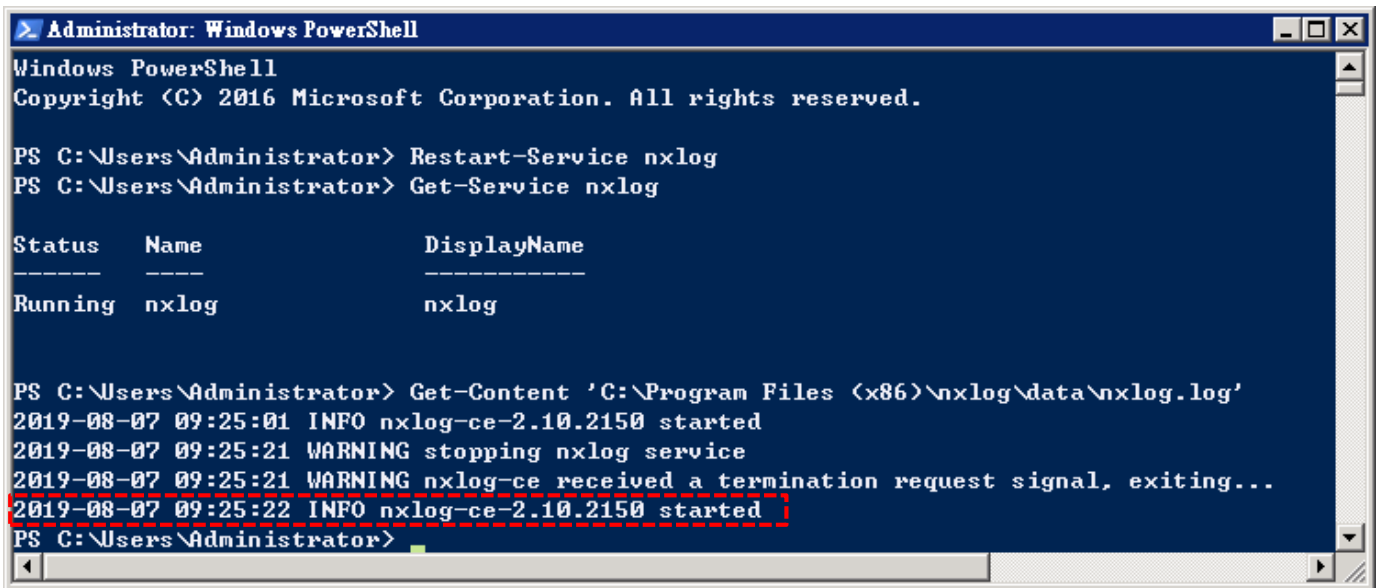
註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入 Microsoft IIS 記錄檔資料夾路徑

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

(18) 重啟 nxlog 服務

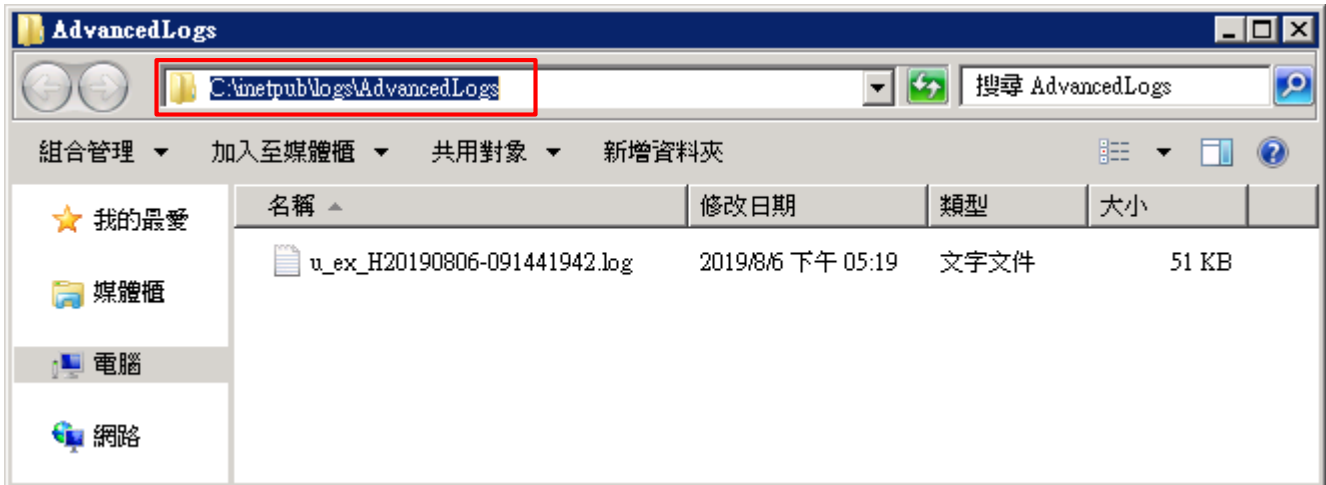
開啟 [Windows PowerShell] -> 輸入 `Restart-Service nxlog` 重新啟動 nxlog 服務和 `Get-Service nxlog` 查看 nxlog 服務狀態 -> `Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息



(19) 點選 [重新啟動] IIS 服務



(20) 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]

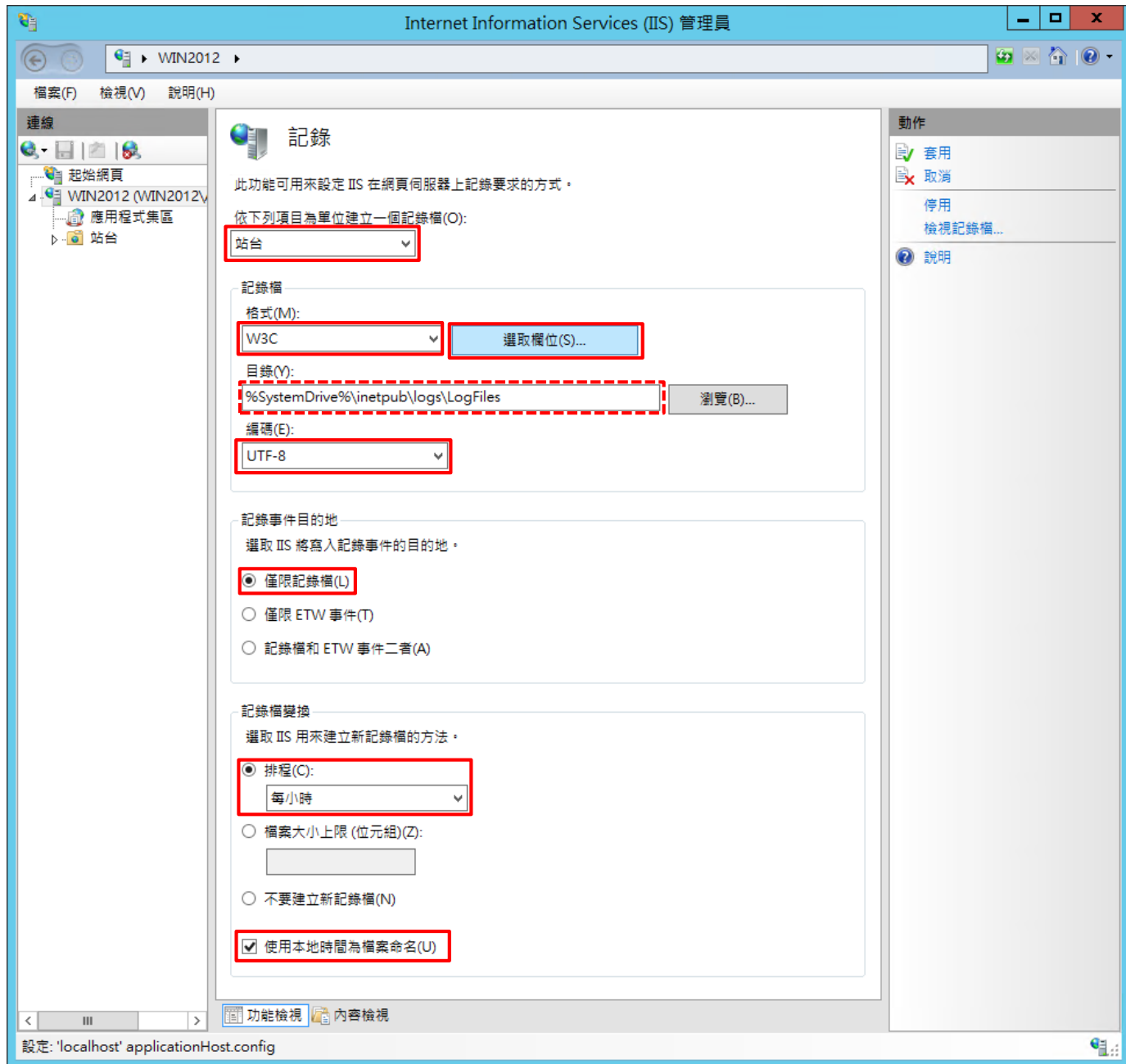


(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]

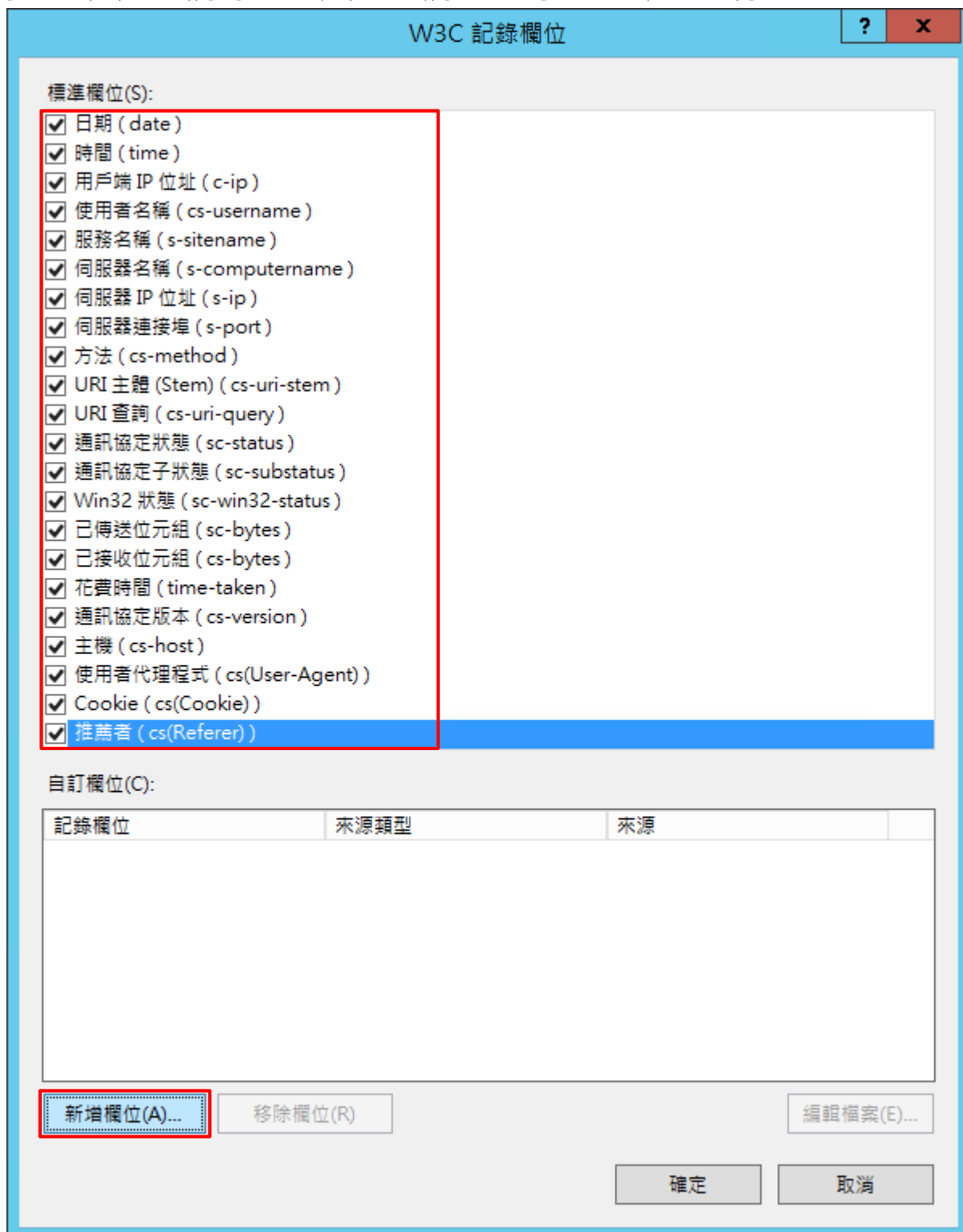


(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程:
[Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(選取檔位)]



(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)]



(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))

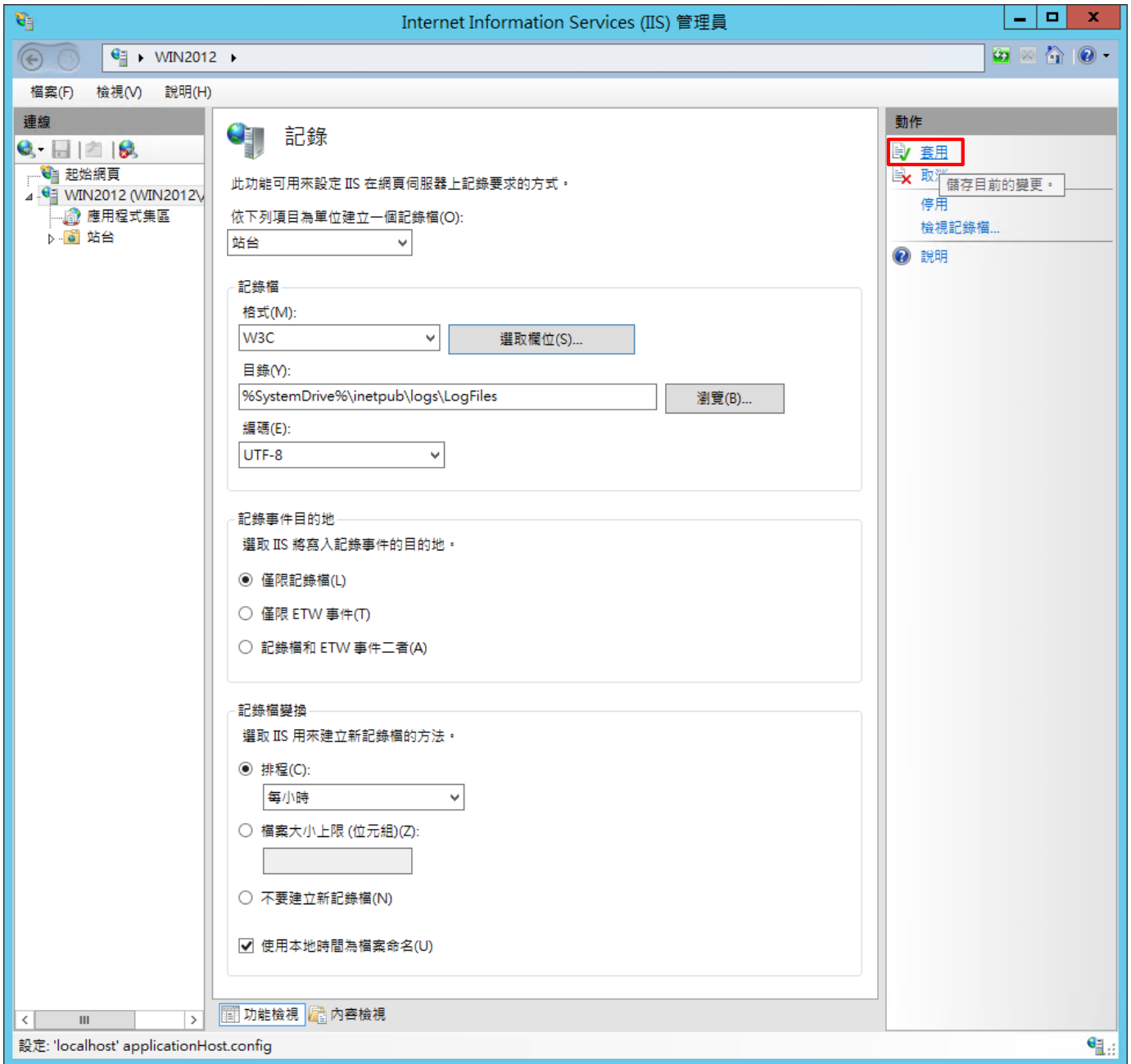
自訂欄位(C):

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

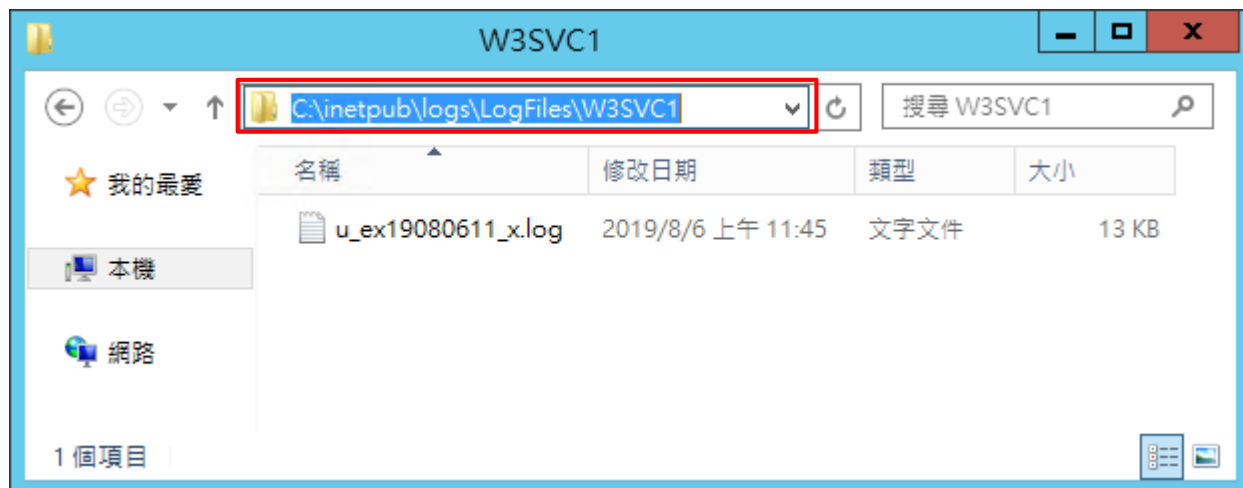
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(套用)]



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

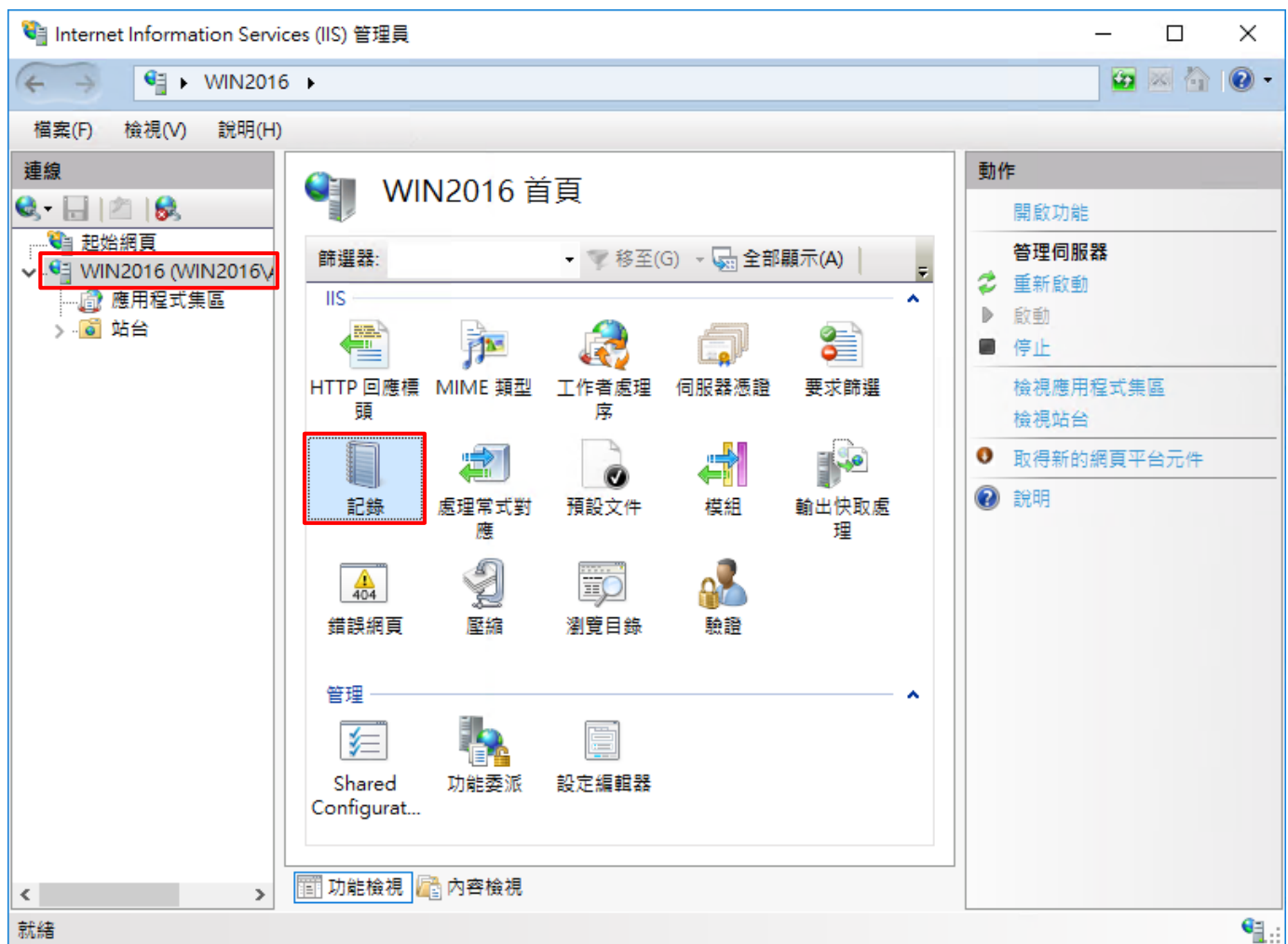


5. Windows 2016

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

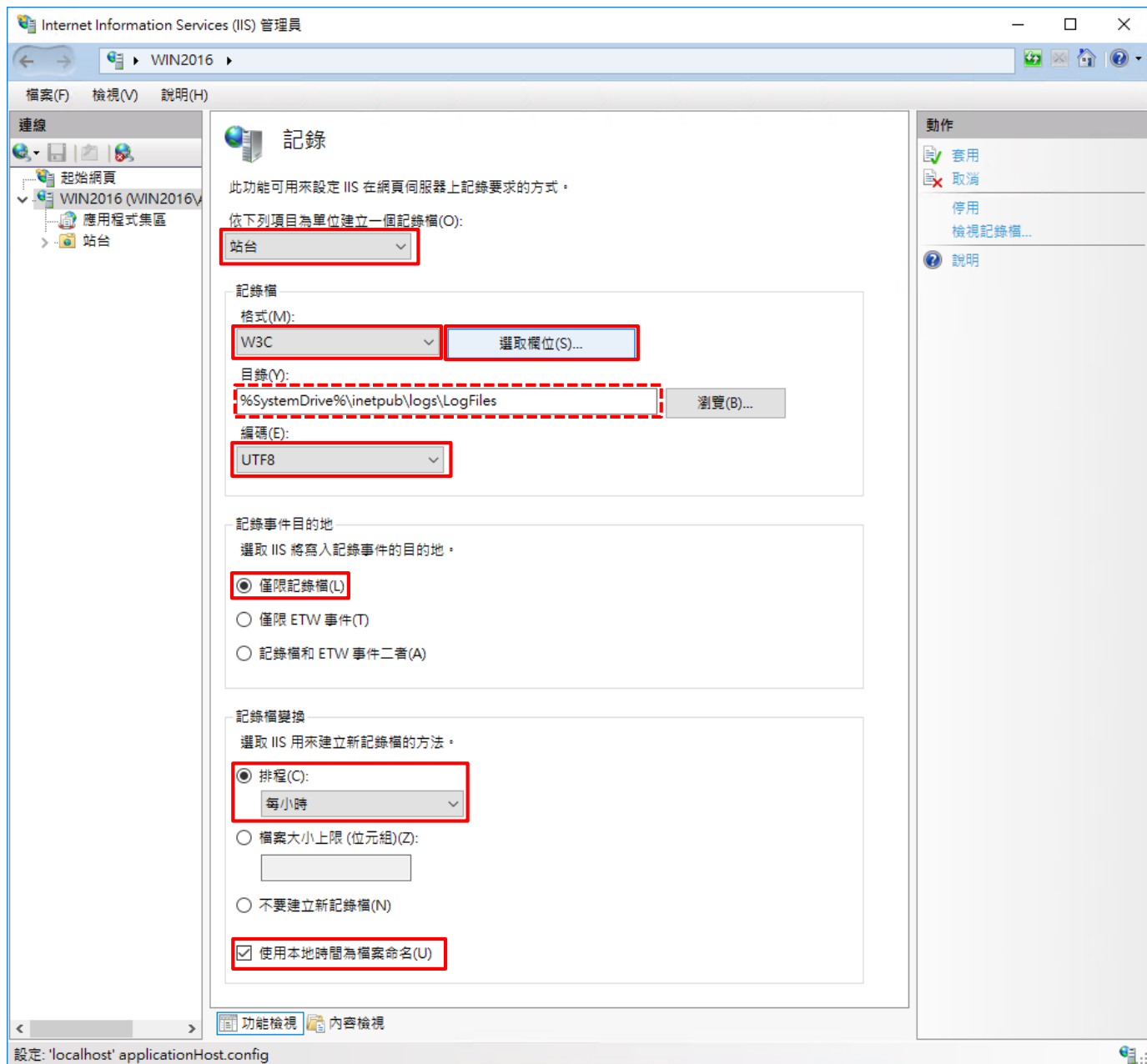


(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]

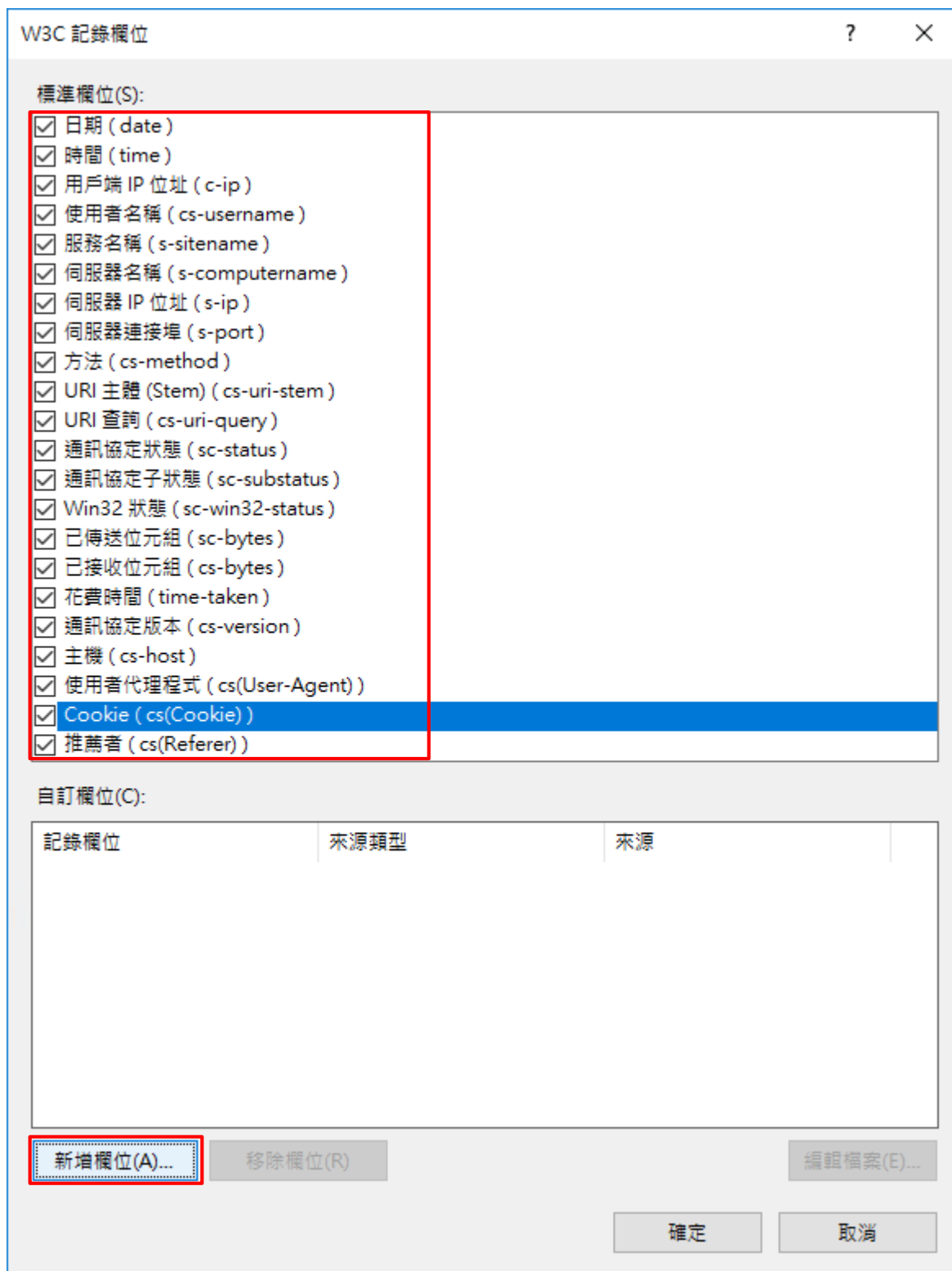


(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程: [Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(選取檔位)]



(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)]



(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))

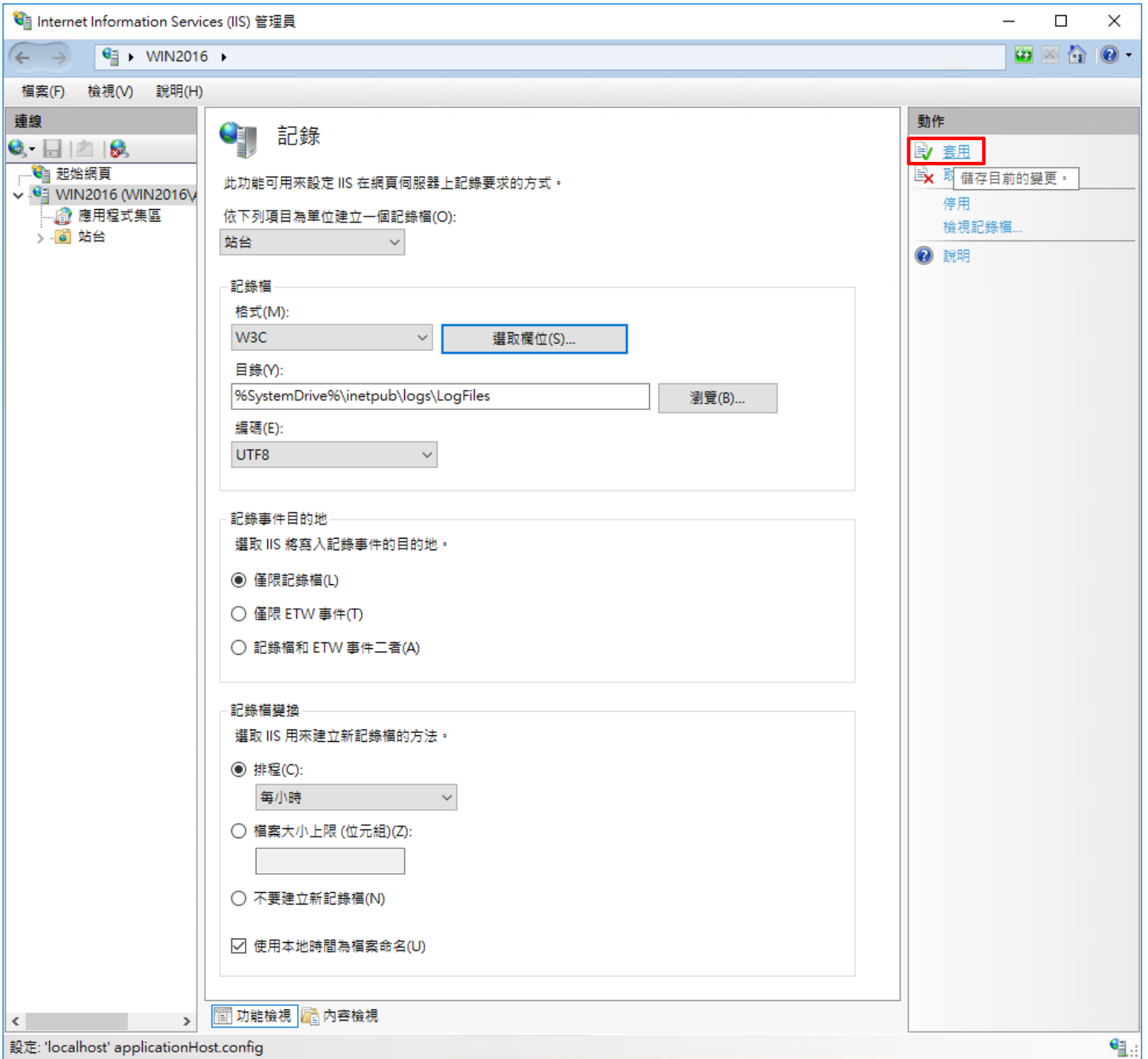
自訂欄位(C):

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

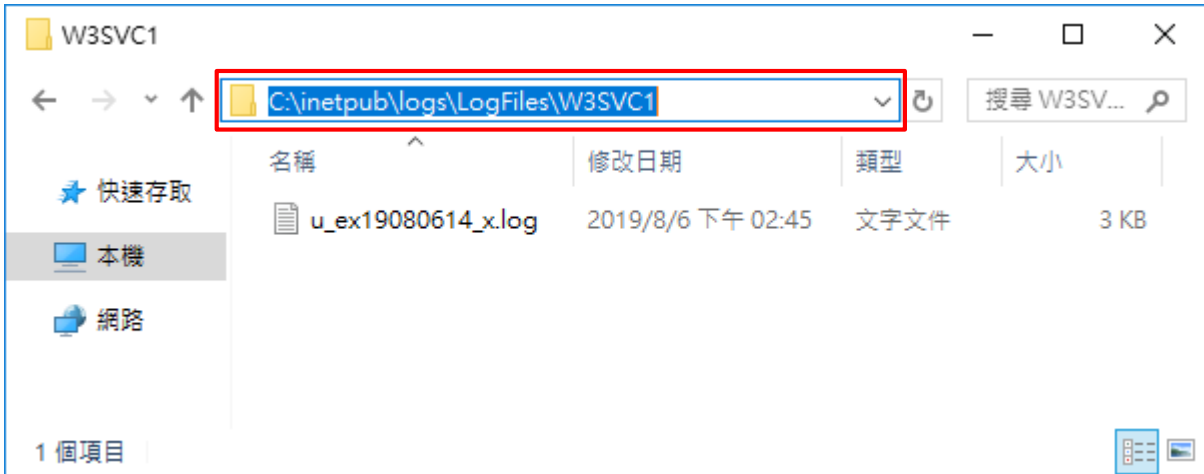
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(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]

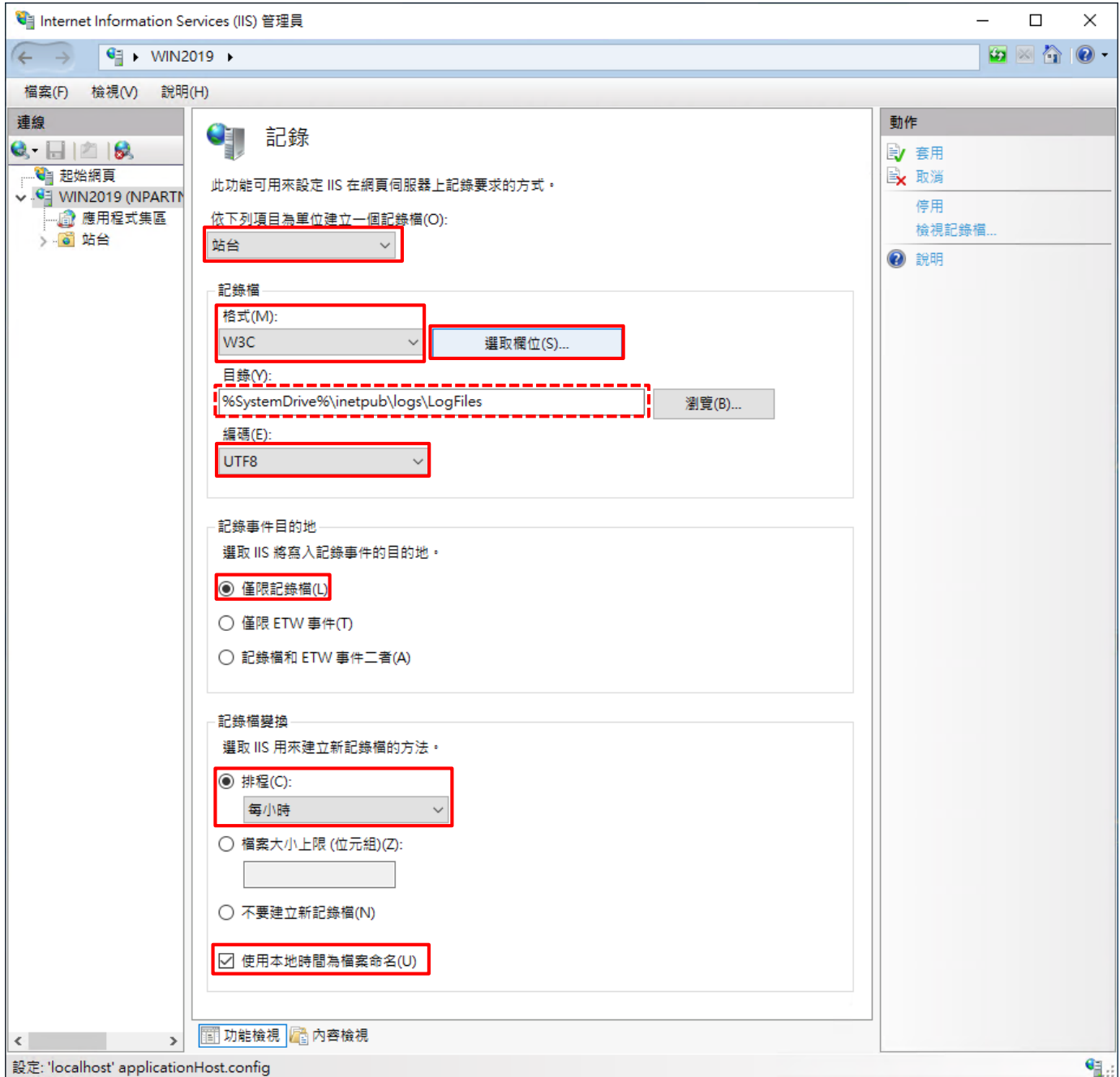


(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]



(3) 選擇依下列項目為單位建立一個記錄檔: [Site(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: [Log file only(僅限記錄檔)] -> 排程: [Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(選取檔位)]



(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)]

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))

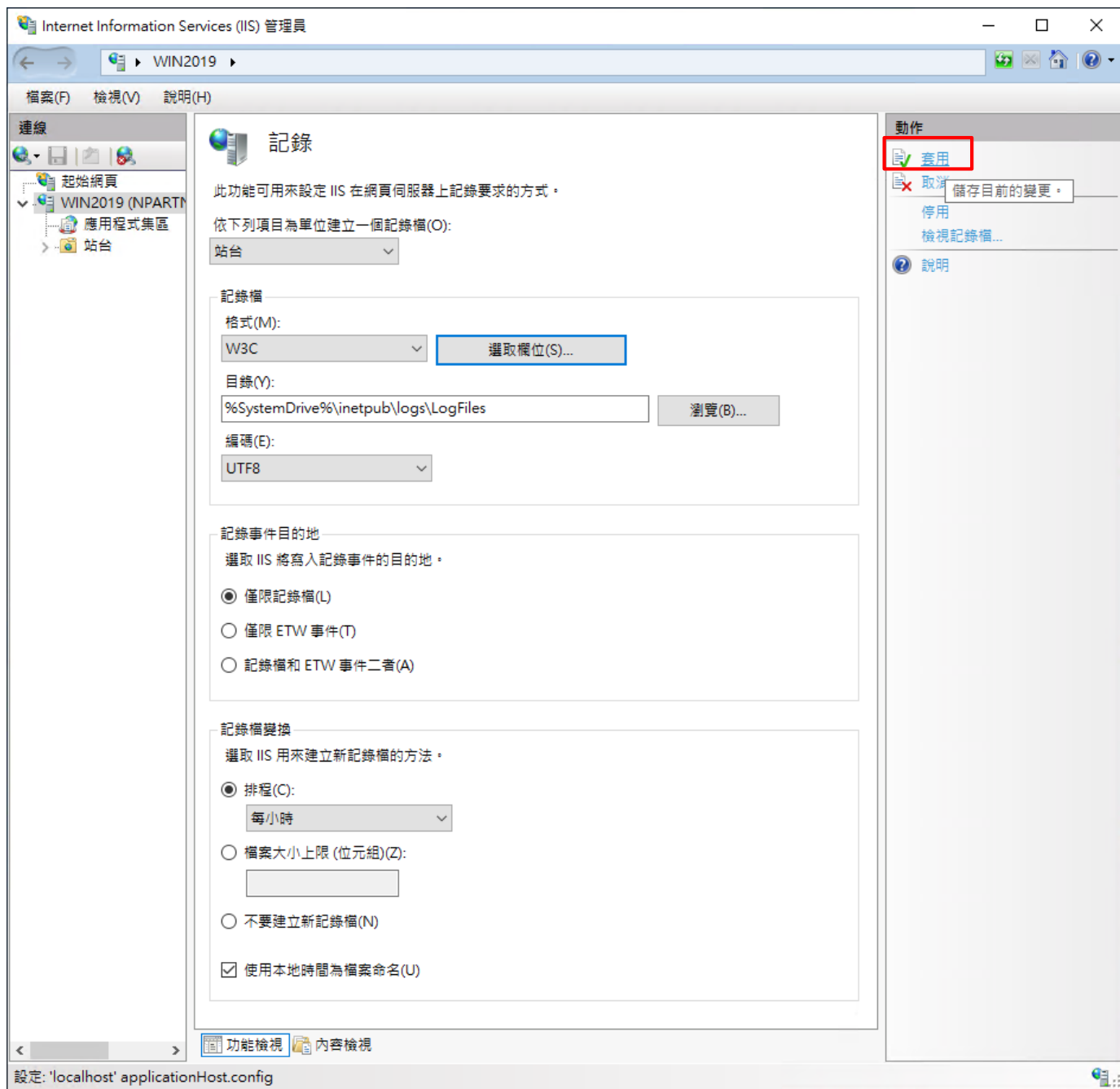
自訂欄位(C):

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

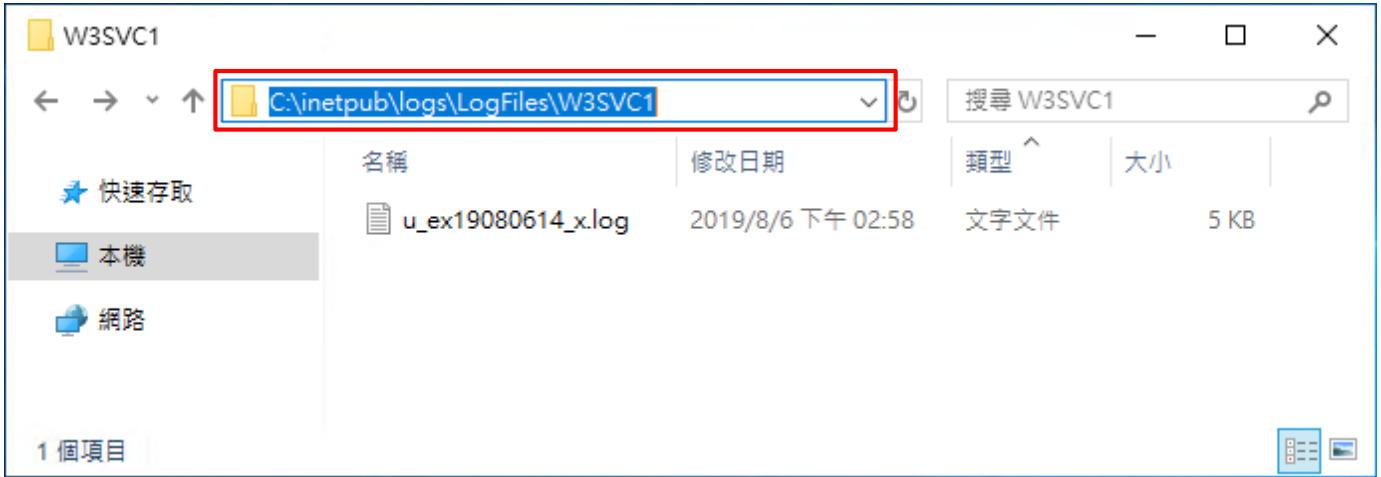
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(套用)]



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



7. 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 sidebar menu with the following items: 'Admin (Global) v', '事件' (Events), '報表' (Reports), '設備管理' (Device Management) - highlighted with a red box, '設備樹狀圖' (Device Tree View) - also highlighted with a red box, '介面列表' (Interface List), '告警樣版' (Alert Templates), '設備異常告警' (Device Abnormal Alerts), and '系統管理' (System Management). 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 a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a blue 'U' button, and a yellow speaker icon. The main content area displays a tree view for 'Global (109)' with two warning icons (red and yellow triangles) and a sub-item '未知設備 (1)' (Unknown Devices (1)).

(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]

The screenshot shows a web-based configuration window titled "設備資訊編輯" (Device Information Edit). The window is divided into several sections:

- 設備基本設定** (Device Basic Settings):
 - 名稱** (Name): Win_IIS-192.168.2.127
 - IP**: 192.168.2.127
- 設備種類** (Device Type):
 - Syslog
 - Flow
 - SNMP
- Syslog 相關設定** (Syslog Related Settings):
 - 資料格式** (Data Format): IIS
 - Facility**: (22) local use 6 (local6)
 - 編碼方式** (Encoding): UTF-8
- 設備進階設定** (Device Advanced Settings):
 - 設備 Icon**: icon-host
 - Login Account**: (empty text box)
 - Login Password**: (empty text box)
 - Action 設備**:
 - 是否為 Action 設備
 - 接收狀態** (Receive Status):
 - 啟用
 - 停用
 - 暫無資料告警** (No Data Alert):
 - 啟用 Syslog/Flow 暫無資料告警

At the bottom right, there are two buttons: "確定" (Confirm) and "取消" (Cancel).



連絡資訊

TEL: +886-4-23752865

FAX: +886-4-23757458

技術問題請洽：

Email: support@npartnertech.com

Skype: [support@npartnertech.com](https://www.skype.com/people/support@npartnertech.com)

業務相關請洽：

Email: sales@npartnertech.com

