N-Partner

如何配置
Windows IIS log

V011

2024/09/27

版权声明

商标

目錄

前言

本文描述了 N-Reporter 用户如何使用开源工具 NXLog 配置 Windows IIS（Internet 信息服务）日志。NXLog 工具会将 Windows IIS 日志转换为 syslog 格式，并转发到 N-Reporter 进行规范化、审计和分析。本文适用于 Windows Server 2000 / 2003 / 2008 / 2012 / 2016 / 2019 / 2022 版本的操作系统。

注：本文件仅作为日志输出设置的参考，建议您仍应联系设备或软件厂商寻求日志输出方式的支持。

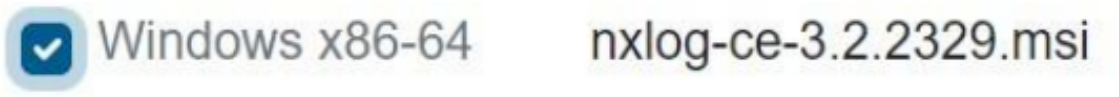
1 NXLog

1.1 NXLog 安装

(1) 下载 NXLog CE(社区版)

前往下载链接 https://nxlog.co/products/nxlog-community-edition/download

下载最新版本的 nxlog-ce-x.x.xxxx.msi，例如：nxlog-ce-3.0.2272.msi

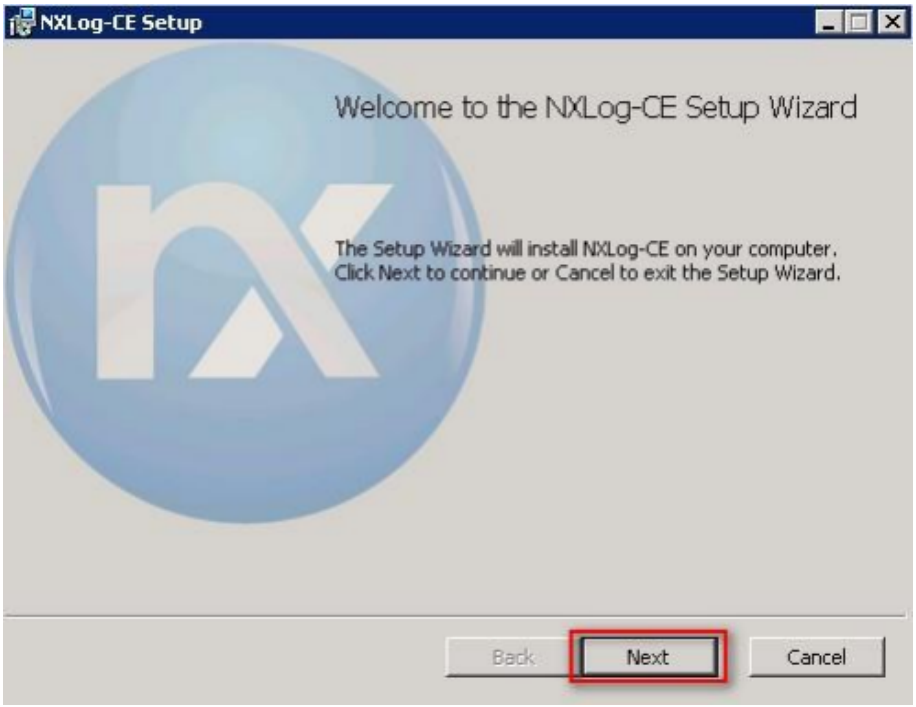


注：如果需要下载 NXLog 32 位版本，请联系相关人员。

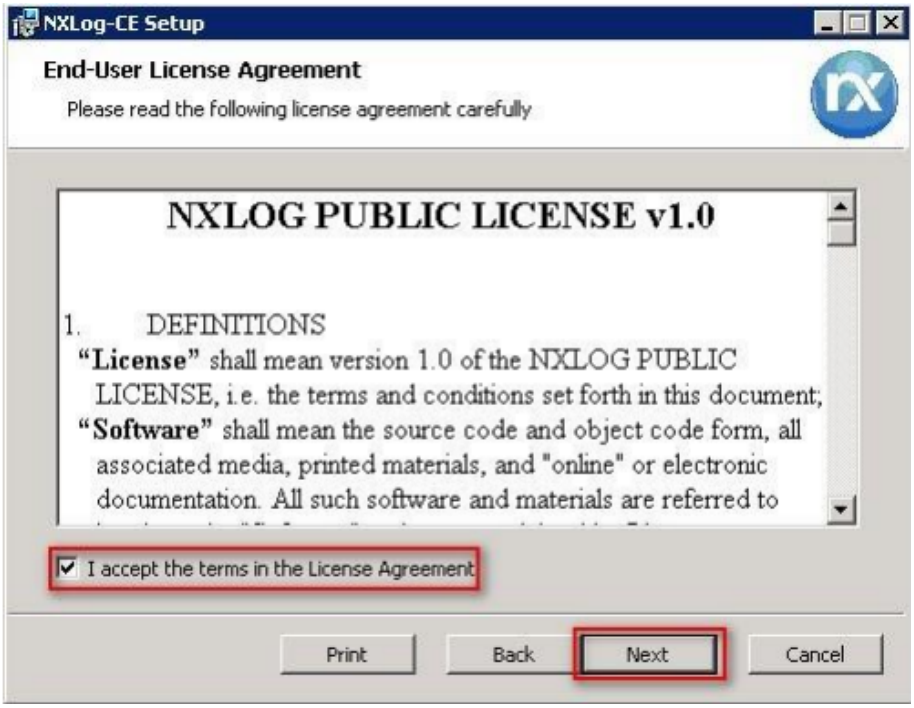
(2) 安装 NXLog

<2.1> 适用于 Windows 2008 或更高版本操作系统

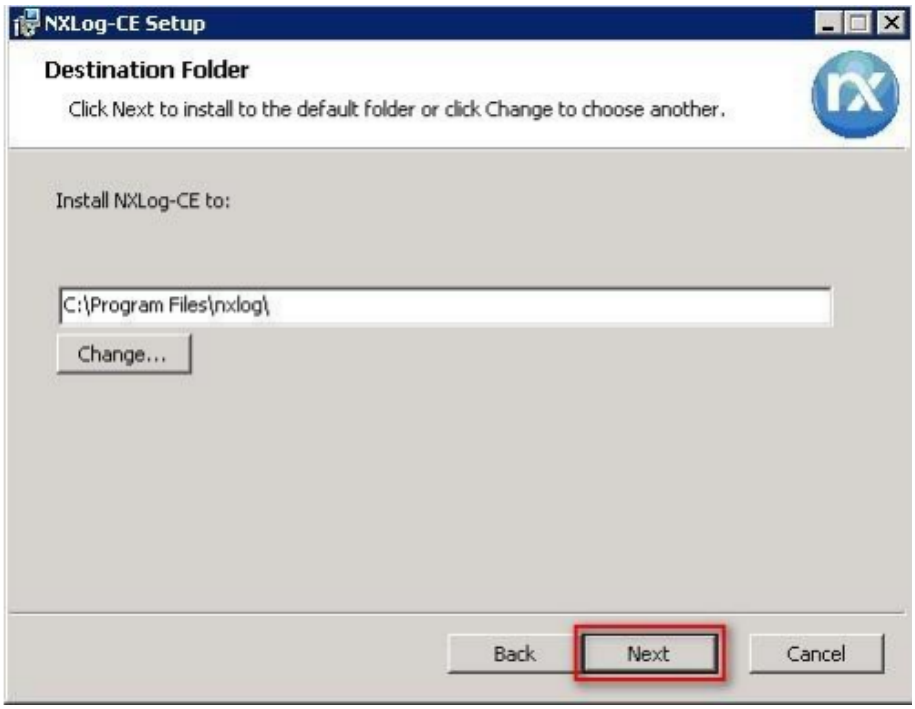
点击 [nxlog-ce-3.2.2329.msi] -> 点击 [Next].



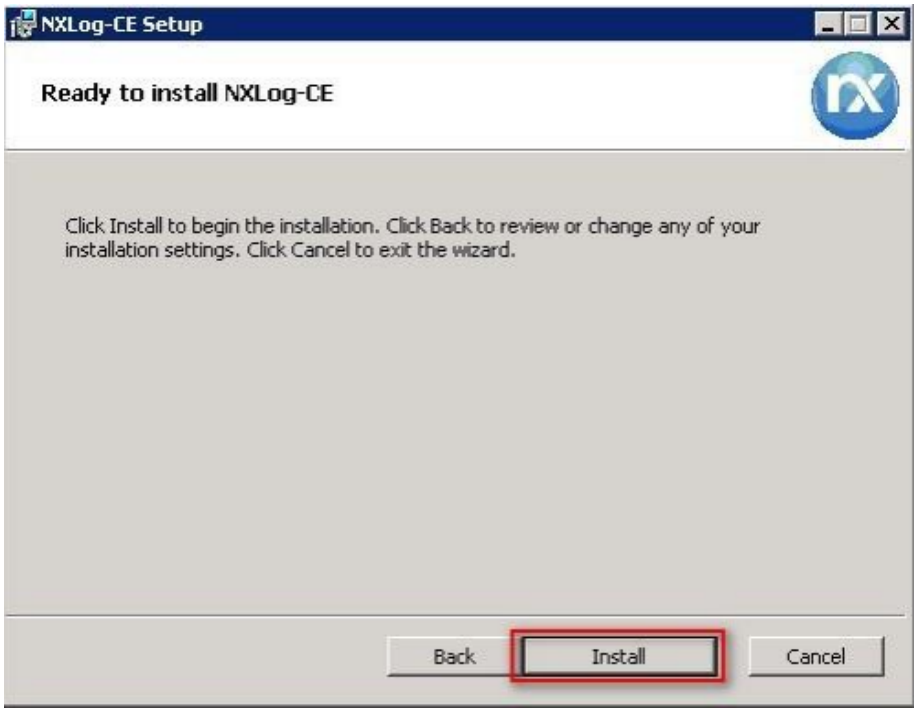
-> 勾选 [I accept the terms in the License Agreement]，然后点击 [Next] .



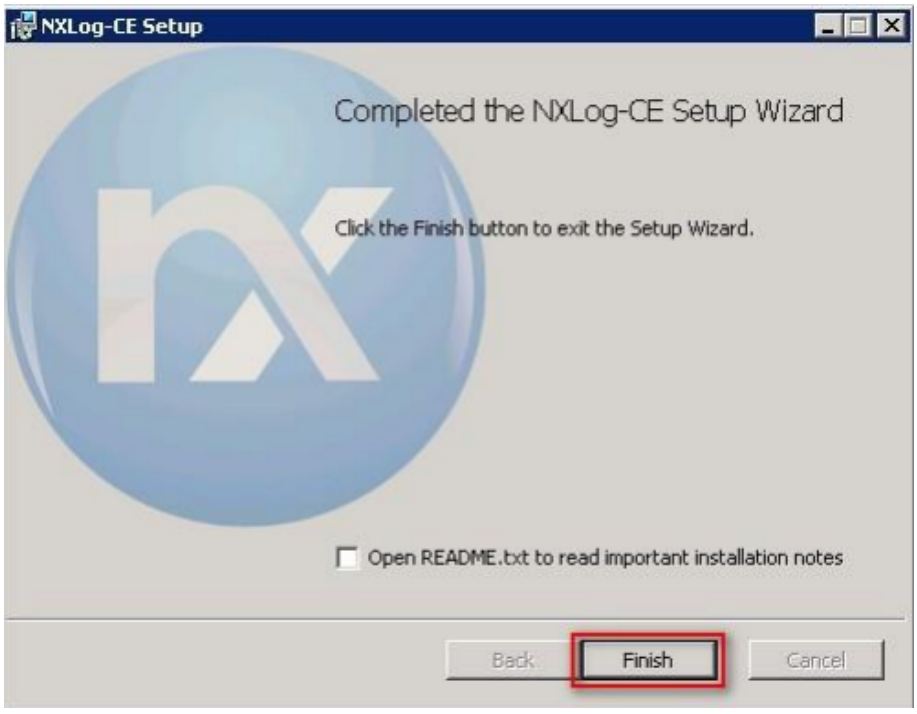
-> 点击 [Next]. (默认安装路径 C:\Program Files\nxlog\)



-> 点击 [Install].

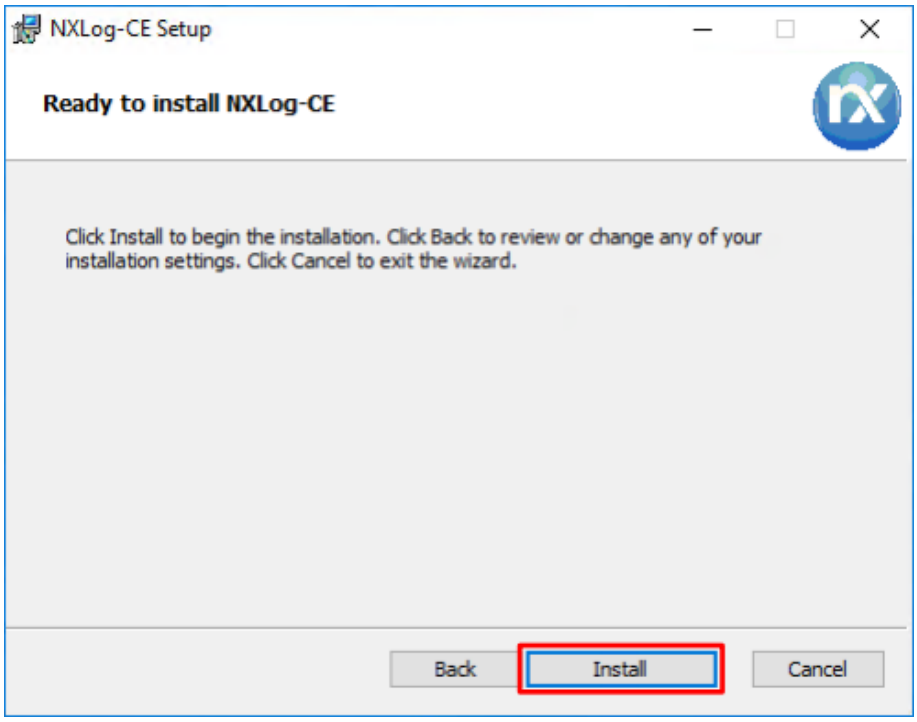


-> 点击 [Finish].



<2.2> Windows 2003

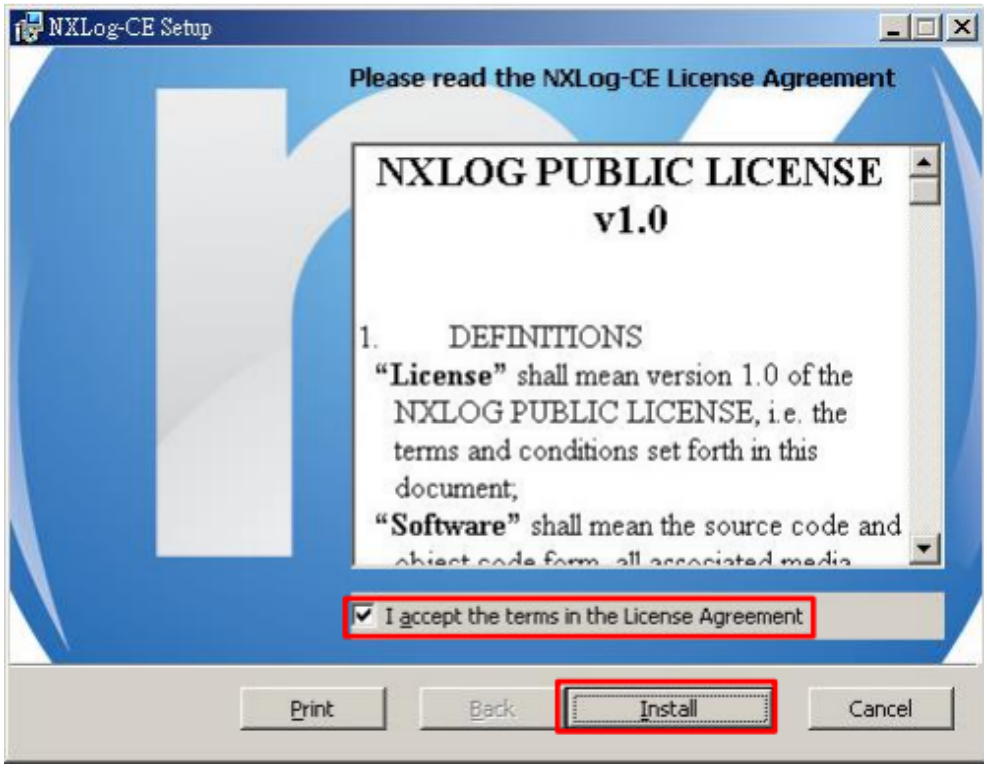
点击 [nxlog-ce-3.2.2329.msi] -> 点击 [Install] 到 [Finish].



<2.3> Windows 2000

前往 NXLog CE 旧版下载页面 https://sourceforge.net/projects/nxlog-ce/ , 点击 [See All Activity] , 下载适用于 Windows 2000 版本的 nxlog-ce-2.8.1248.msi.

点击 [nxlog-ce-2.8.1248.msi] -> 勾选 [I accept the terms in the License Agreement] -> 点击 [Install] 到 [Finish].



1.2 NXLog 配置文件下载

1.2.1 适用于 Windows 2003 或更早版本操作系统

(1) 打开 [命令提示符]

(2) 根据需求选择下载适用于 Windows IIS 的 NXLog 配置文件，并覆盖现有的 Windows 系统 NXLog 配置文件。

<2.1> 记录所有信息的配置文件:

下载链接：http://www.npartnertech.com/download/tech/nxlog_WinIIS.conf

<2.2> 不记录 Cookie 信息的配置文件:

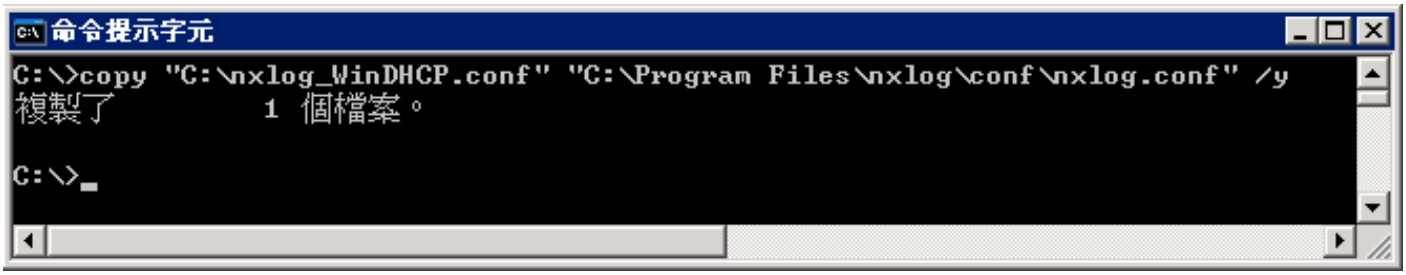
下载链接：http://www.npartnertech.com/download/tech/nxlog_WinIIS_no_cookie.conf

记录所有信息的配置文件复制指令:

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

不记录 Cookie 信息的配置文件复制指令:

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



本文件示例适用于 64 位操作系统，如果操作系统为 32 位，请按照以下红色文字部分进行更改 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

1.2.2 适用于 Windows 2008 或更高版本操作系统

(1) 打开 [Windows PowerShell]

(2) 根据需求选择下载适用于 Windows IIS 的 NXLog 配置文件，并覆盖现有的 Windows 系统 NXLog 配置文件。

<2.1> 记录所有信息的配置文件:

下载链接：http://www.npartnertech.com/download/tech/nxlog_WinIIS.conf

<2.2> 不记录 Cookie 信息的配置文件:

下载链接：http://www.npartnertech.com/download/tech/nxlog_WinIIS_no_cookie.conf

记录所有信息的配置文件复制指令:

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

不记录 Cookie 信息的配置文件复制指令:

```
PS C:\> Invoke-WebRequest -Uri`http://www.npartnertech.com/download/tech/nxlog_WinDNS_no_cookie.co
nf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf
```

本文件示例适用于 64 位操作系统，如果操作系统为 32 位，请按照以下红色文字部分进行更改 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

1.3 NXLog 配置文件

1.3.1 记录所有信息的配置文件

```
## 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_iilog>
    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 dnslog>
    Path    in_iislog => out_iislog
</Route>
```

蓝色文字部分请输入 N-Reporter 系统的 IP 地址

```
define NCloud  192.168.8.4
```

本文件示例环境为 64 位操作系统，若操作系统环境为 32 位，请按以下设置进行更改

```
define ROOT  C:\Program Files (x86)\nxlog
```

蓝色文字部分请输入 IIS 的路径

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

修改配置文件内容后需“另存为”覆盖原文件，1. 保存类型请选择“所有文件 (.)”，2. 编码请选择“UTF-8”，以免因编码错误导致服务无法正常启动。

1.3.2 不记录 Cookie 信息的配置文件

```
## 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_iilog>
    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 dnslog>
    Path    in_iislog => out_iislog
</Route>
```

蓝色文字部分请输入 N-Reporter 系统的 IP 地址

```
define NCloud  192.168.8.4
```

本文件示例环境为 64 位操作系统，若操作系统环境为 32 位，请按以下设置进行更改

```
define ROOT  C:\Program Files (x86)\nxlog
```

蓝色文字部分请输入 IIS 的路径

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

修改配置文件内容后需“另存为”覆盖原文件，1. 保存类型请选择“所有文件 (.)”，2. 编码请选择“UTF-8”，以免因编码错误导致服务无法正常启动。

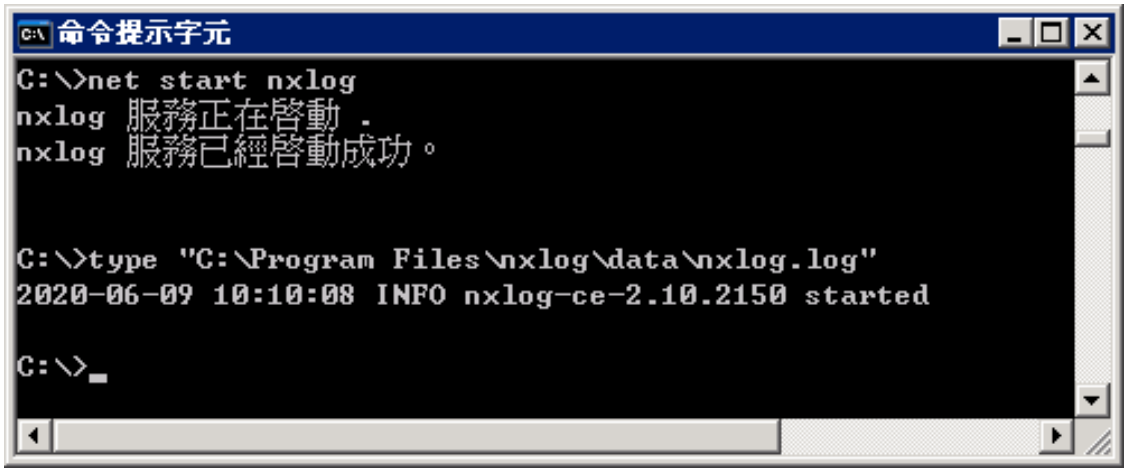
1.4 NXLog 启动服务

1.4.1 Windows 2003 或更早版本操作系统

(1) 打开 [命令提示符]

(2) 启动 NXLog 服务并确认 NXLog 无错误信息

```
PS C:\> net start nxlog
PS C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```

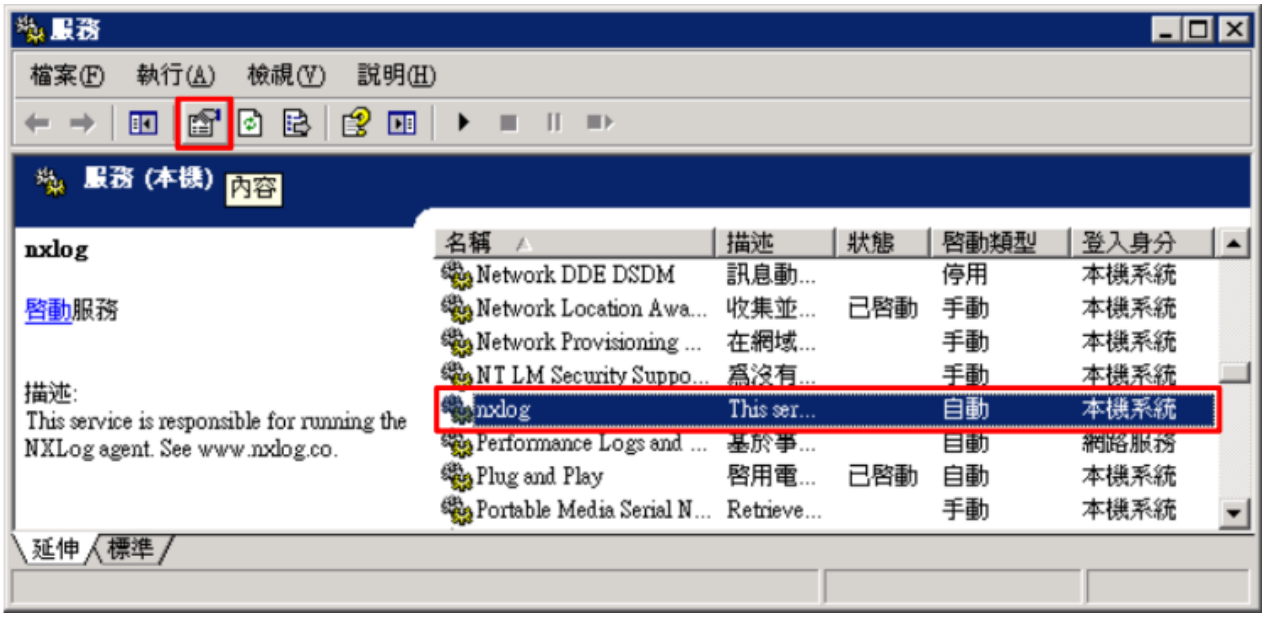


(3) 打开 [服务] 功能

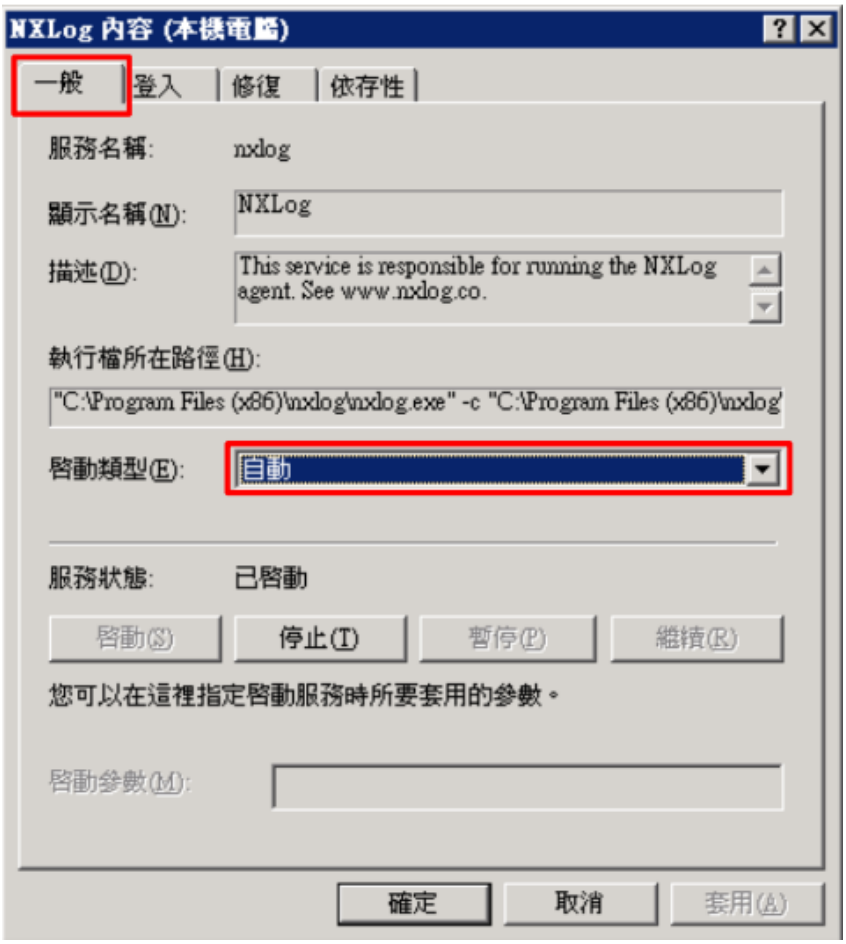
```
PS C:\>  Services.msc
```

(4) 打开 NXLog 服务设置

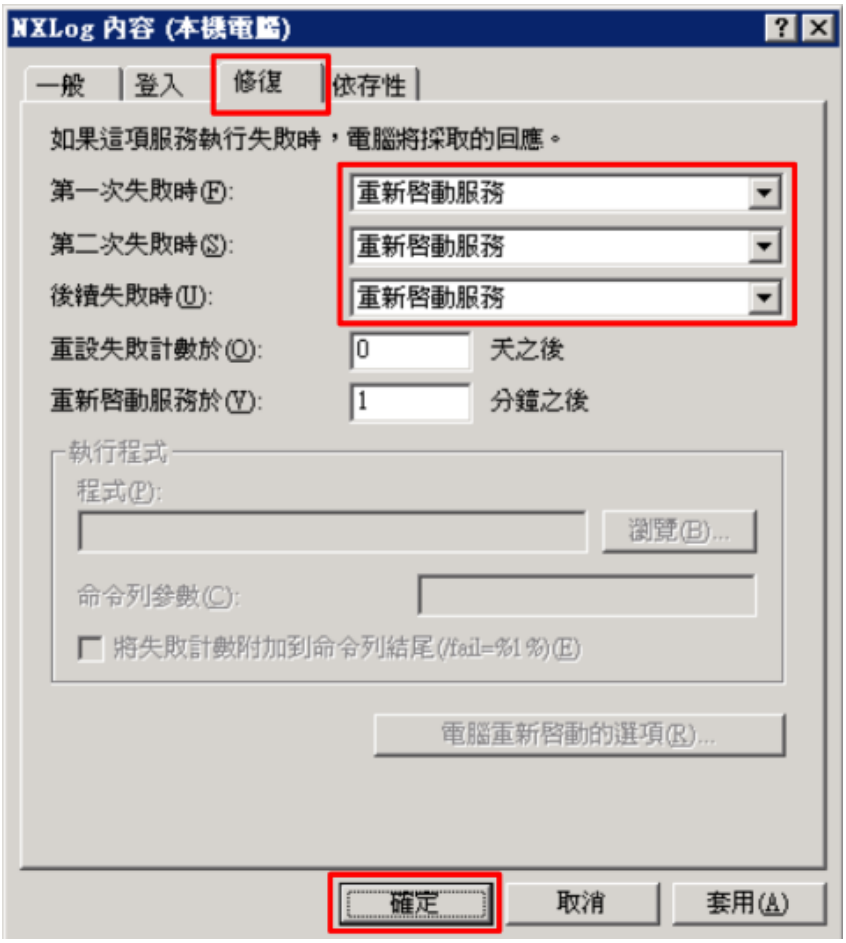
选择 [NXLog] -> 点击 [属性]



(5) 在 [常规] 页面 -> 确认启动类型为 [自动]



(6) 在 **[恢复]** 页面 **->** 确认第一次失败、第二次失败、后续失败的操作均为 **[重新启动服务] ->** 点击 **[确定]**

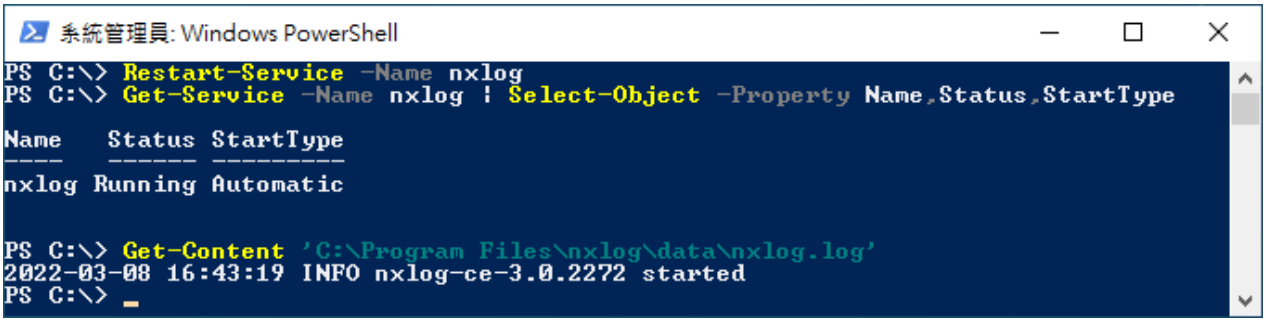


1.4.2 Windows 2008 或更高版本操作系统

(1) 打开 [Windows PowerShell]

(2) 重启 NXLog 服务，检查并确认 NXLog 无错误信息

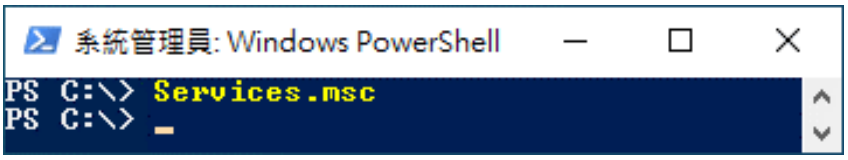
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```



本文件示例为 NXLog 64 位版本，若使用 32 位版本，请将红色文字部分按以下设置进行修改 `C:\Program Files (x86)\nxlog\conf\nxlog.conf'

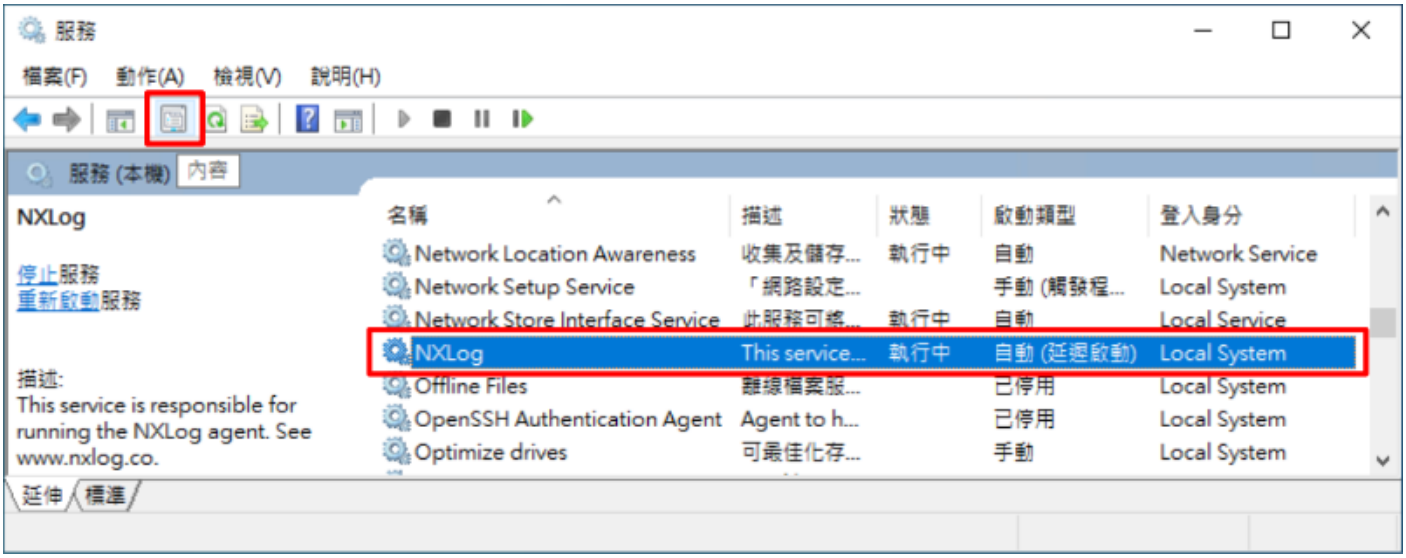
(3) 打开 [服务] 功能

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

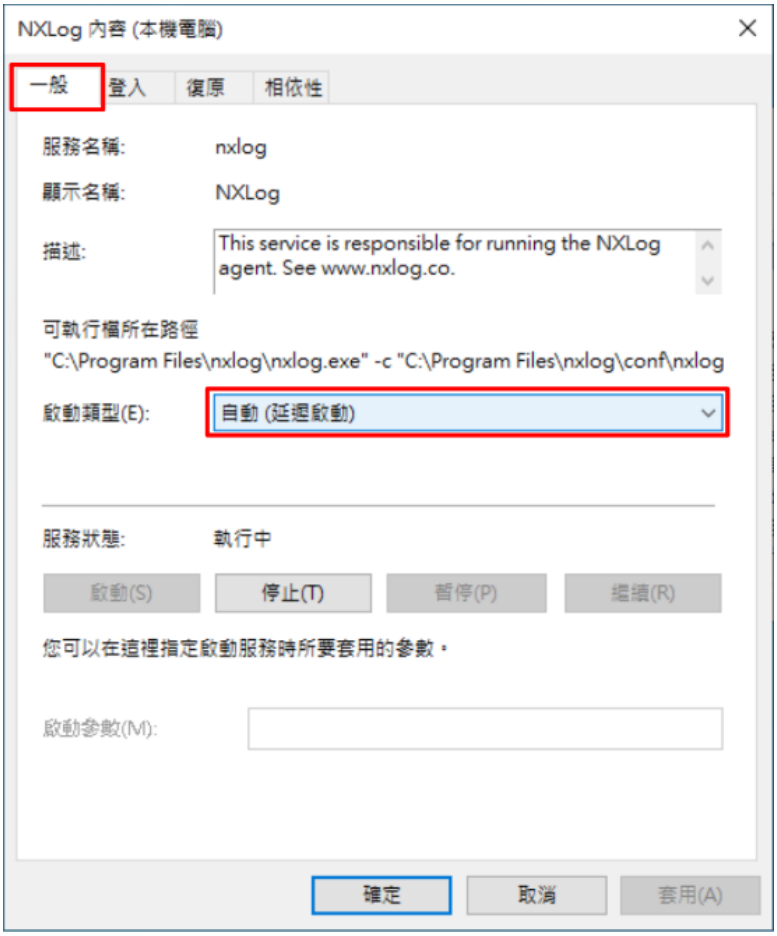


(4) 打开 NXLog 服务设置

选择 [NXLog] -> 点击 [属性]



(5) 在 [常规] 页面 -> 确认启动类型为 [自动 (延迟启动)]



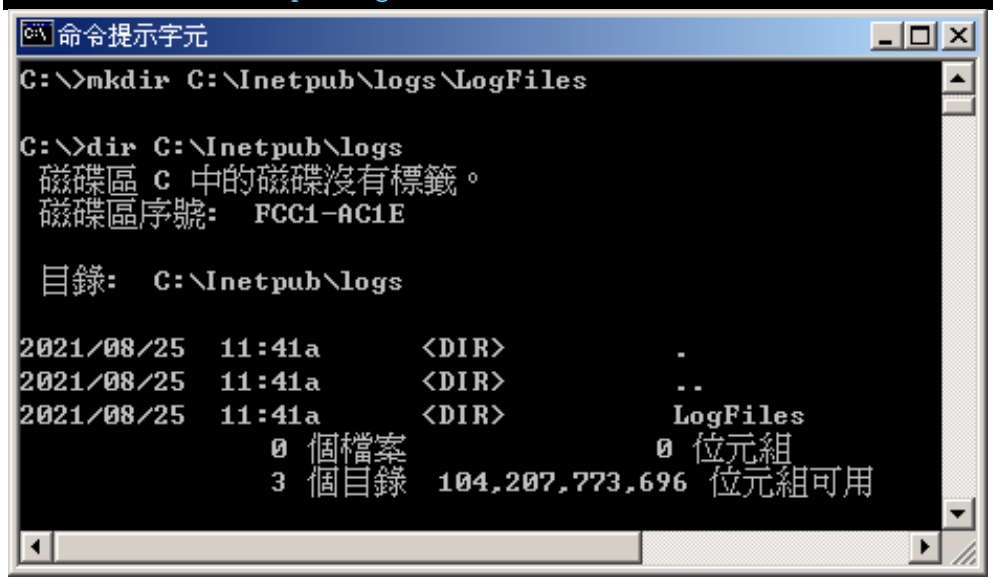
(6)　在 [恢复] 页面 -> 确认第一次失败、第二次失败、后续失败的操作均为 [重新启动服务] -> 点击 [确定]

2 Windows 2000

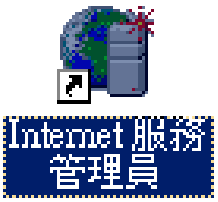
(1) 打开 [命令提示符]

(2) 新建 IIS LogFiles 文件夹并确认该文件夹的存在

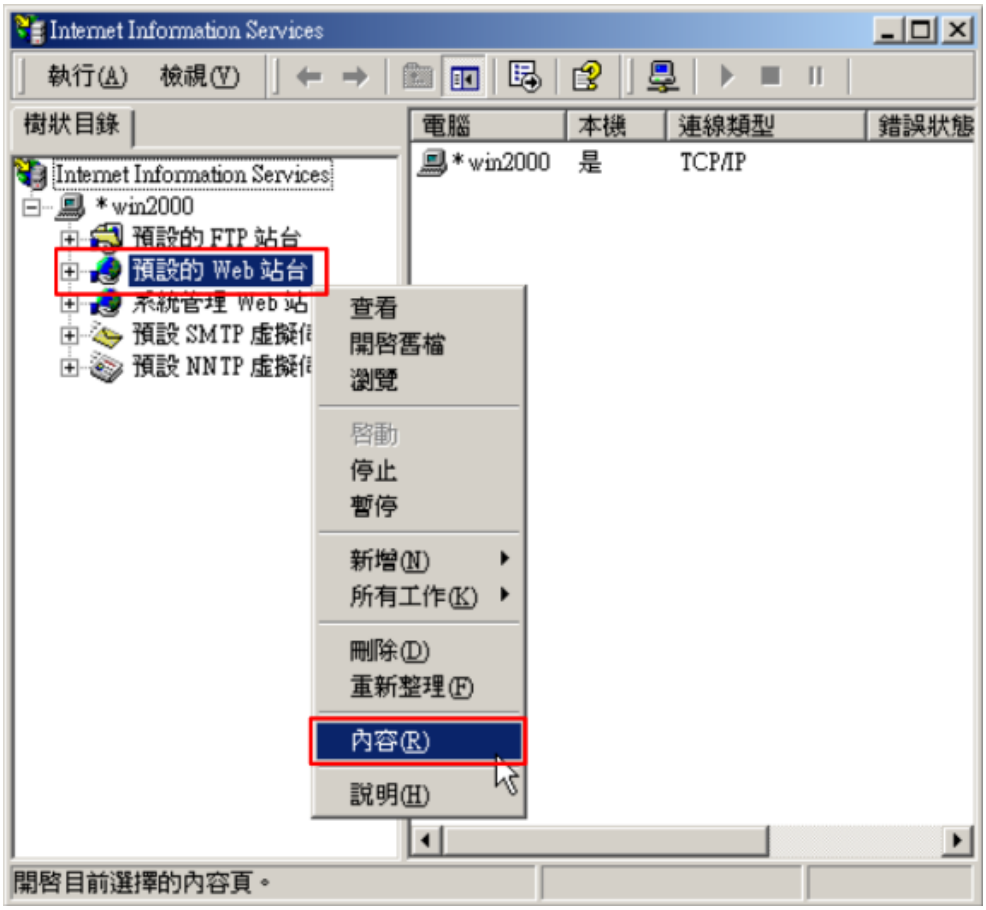
```
PS C:\> mkdir C:\Inetpub\logs\LogFiles
PS C:\> dir C:\Inetpub\logs
```



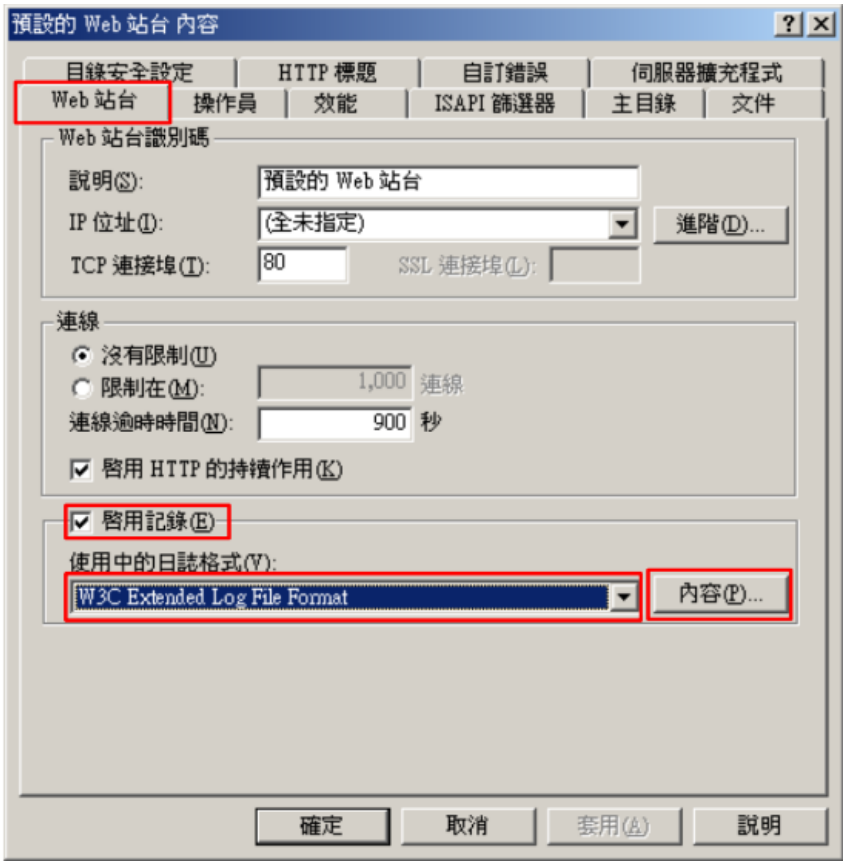
(3) 打开 [Internet 信息服务管理器]



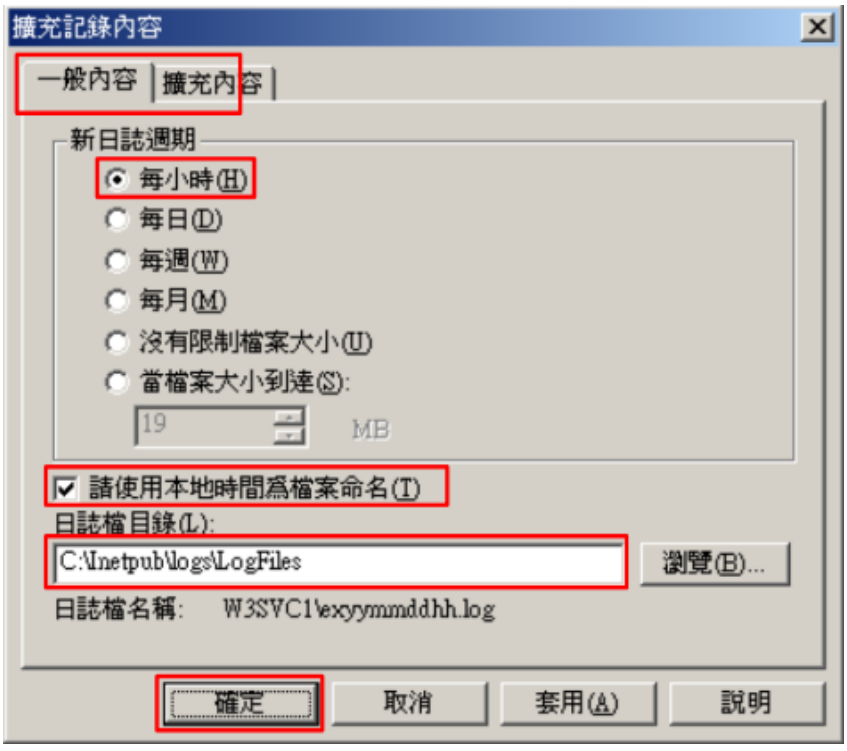
(4)　右键点击 [网站]，选择 [属性]



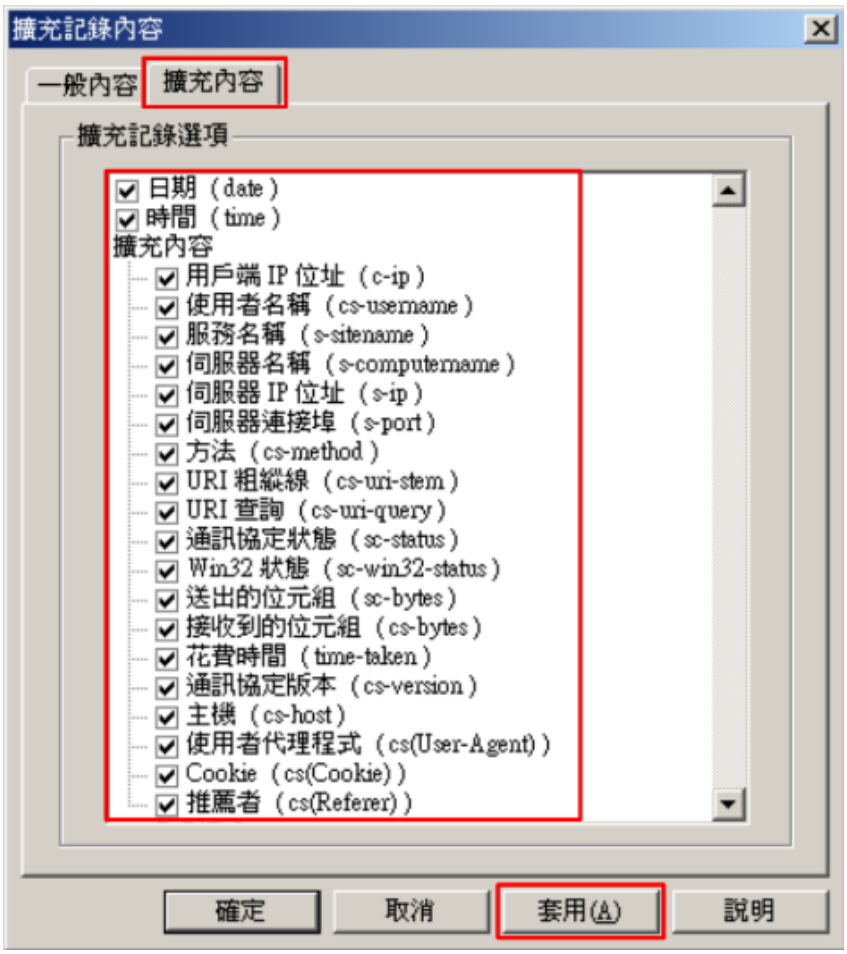
(5)　在 [网站] 页签：勾选 [启用日志] -> 当前日志格式选择 [W3C 扩展日志文件格式] -> 点击 [属性]



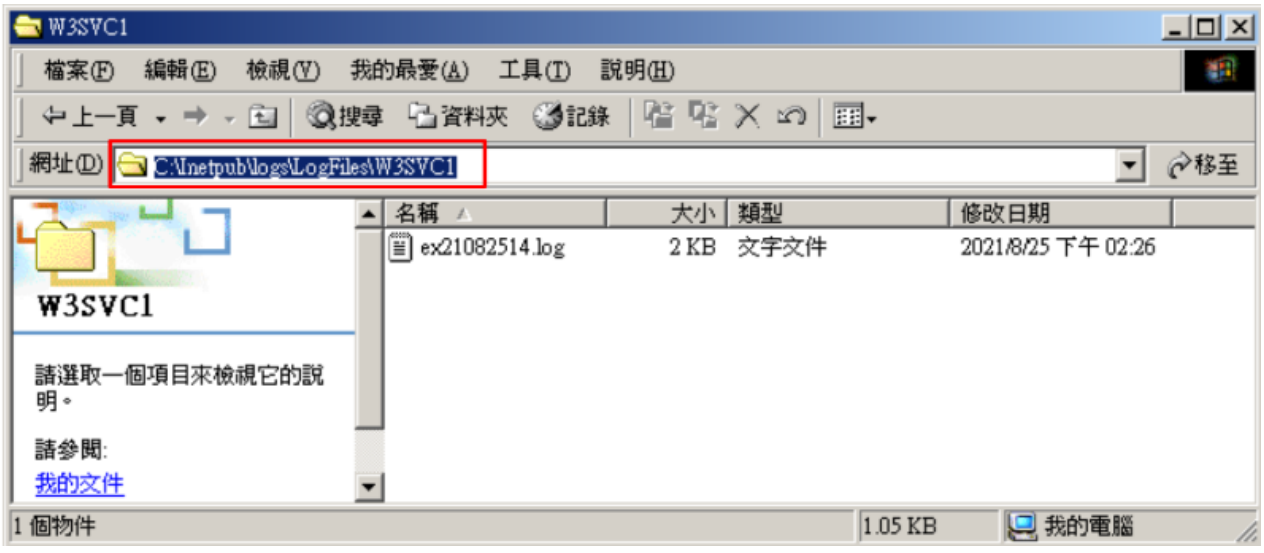
(6)　在 [常规属性] 页签：新日志周期选择 [每小时] -> 勾选 [使用本地时间为文件命名] -> 日志文件目录输入 `C:\Inetpub\logs\LogFiles` -> 点击 [确定]



(7) 在 [扩展属性] 页签：扩展日志选项勾选 [日期 (date)]、[时间 (time)]、[客户端 IP 地址 (c-ip)]、[用户名 (cs-username)]、[服务名称 (s-sitename)]、[服务器名称 (s-computername)]、[服务器 IP 地址 (s-ip)]、[服务器端口 (s-port)]、[方法 (cs-method)]、[URI 主体 (cs-uri-stem)]、[URI 查询 (cs-uri-query)]、[协议状态 (sc-status)]、[协议子状态 (sc-substatus)]、[Win32 状态 (sc-win32-status)]、[发送字节数 (sc-bytes)]、[接收字节数 (cs-bytes)]、[耗时 (time-taken)]、[协议版本 (cs-version)]、[主机 (cs-host)]、[用户代理 (cs(User-Agent))]、[Cookie(cs(Cookie))]、[引用 (cs(Referer))] -> 点击 [应用]



(8) 确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹内是否存在 IIS 日志文件: ex*.log

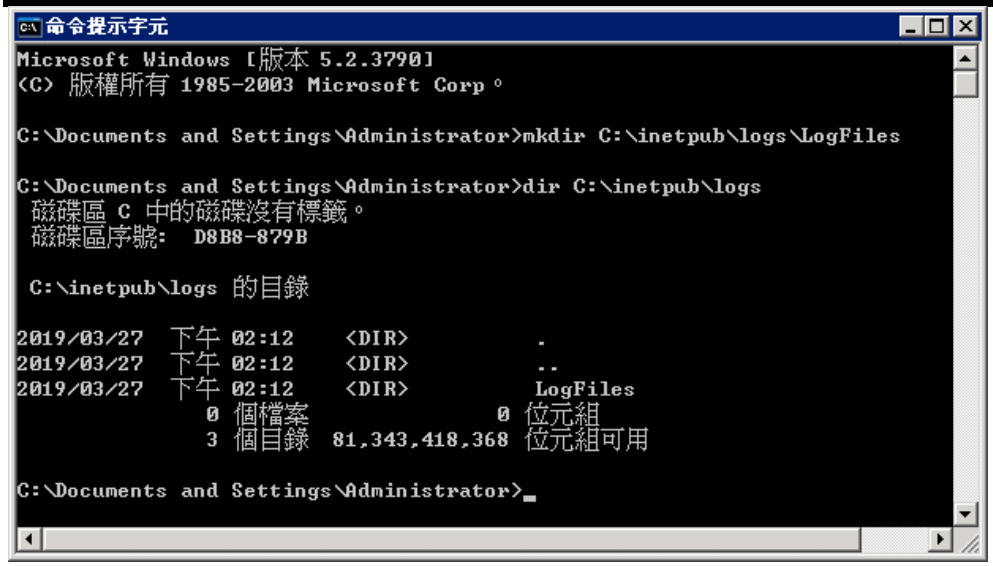


3 Windows 2003

(1) 打开 [命令提示符]

(2) 新建 IIS LogFiles 文件夹并确认该文件夹的存在

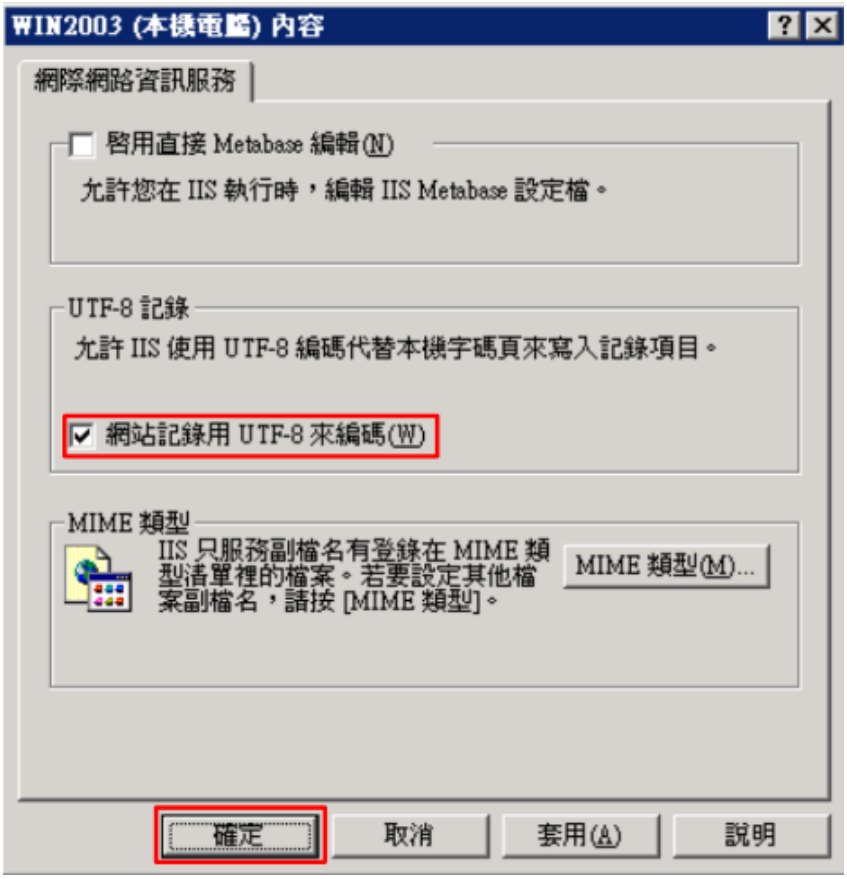
```
PS C:\> mkdir C:\Inetpub\logs\LogFiles
PS C:\> dir C:\Inetpub\logs
```



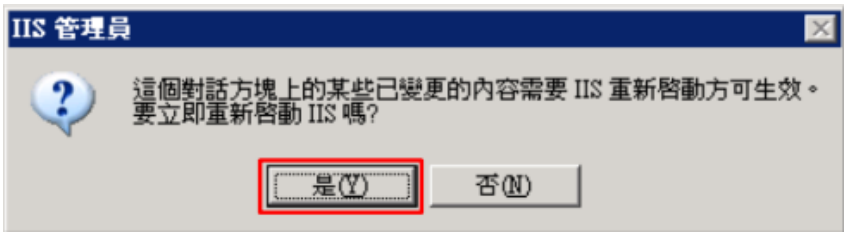
(3) 打开 [互联网信息服务 (IIS) 管理器]

(4)　在 [IIS 服务器] 上右键点击 -> 选择 [属性]

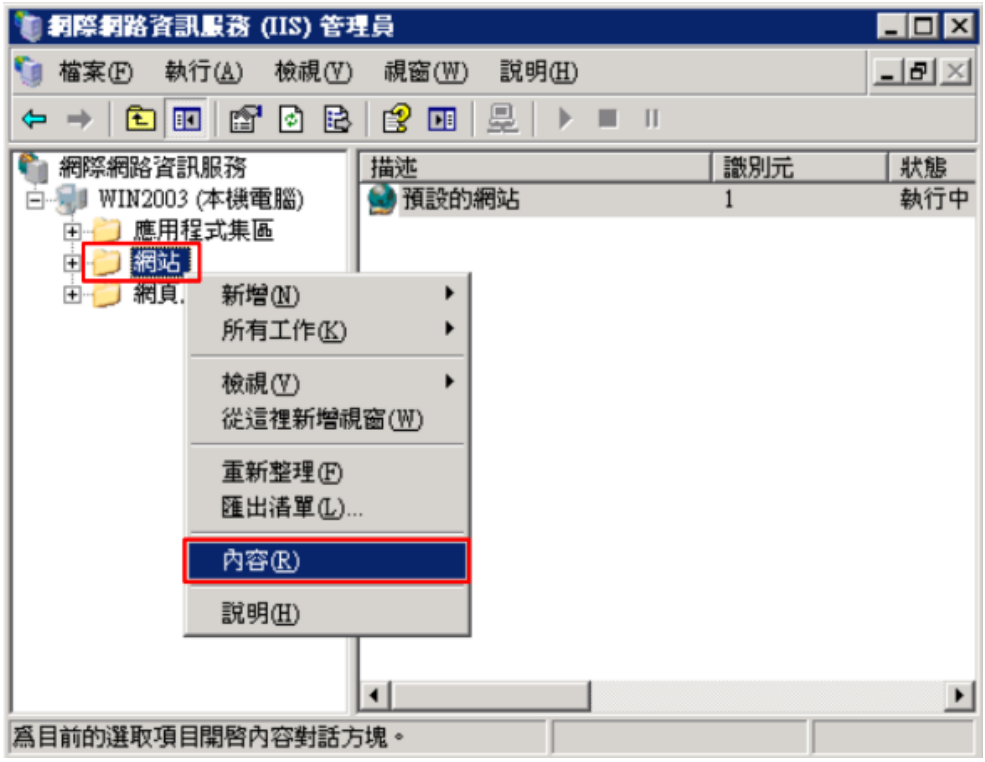
(5) 勾选 **[网站记录用 UTF-8 来编码] -> 点击 [确定]**



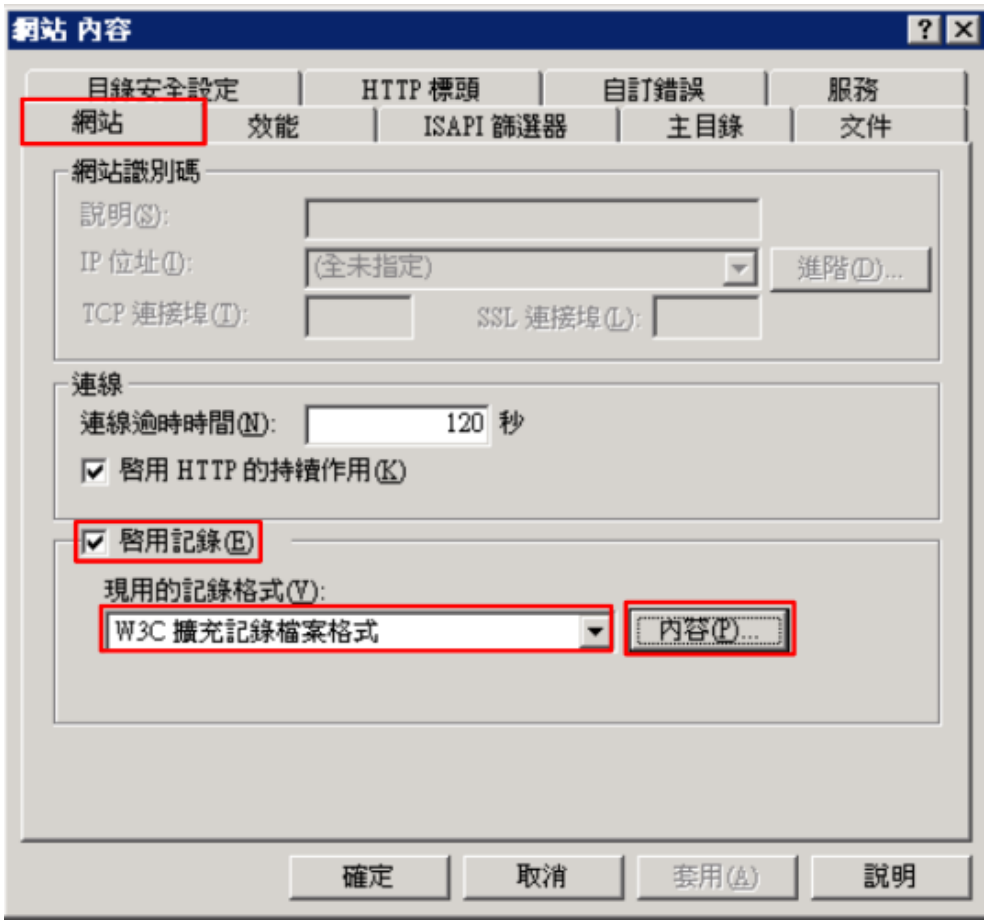
(6) 再次点击 **[确定]**



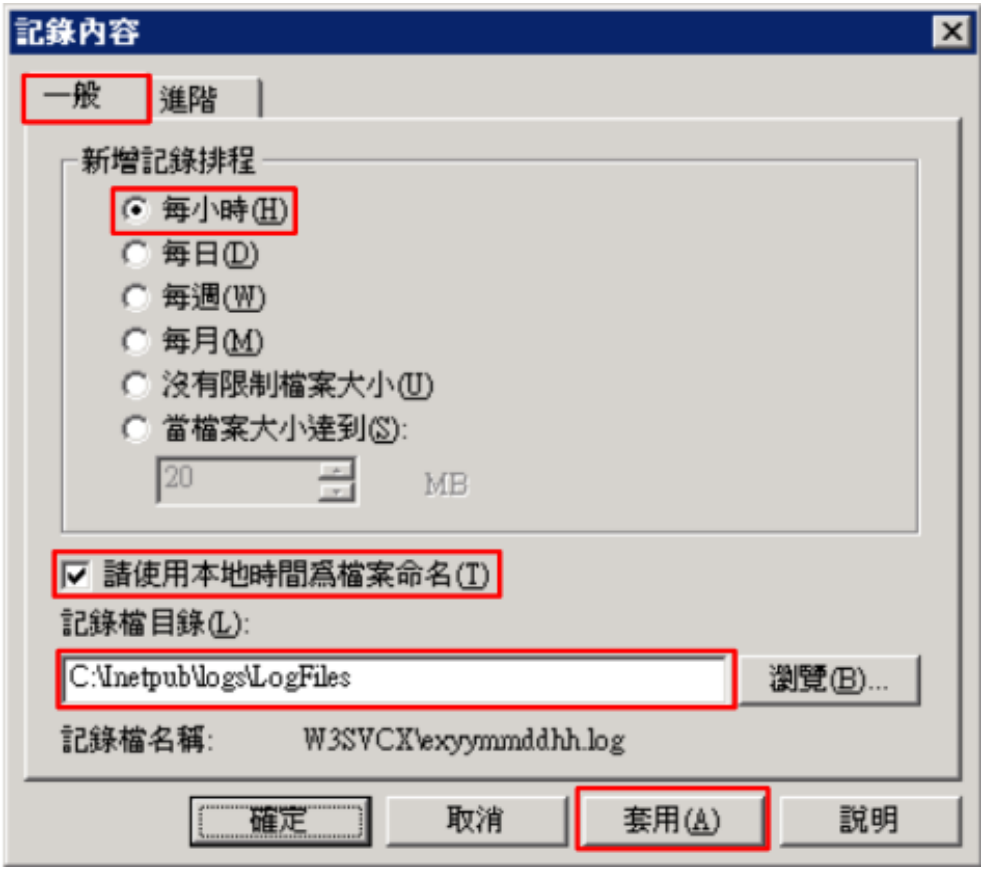
(7)　在 [网站] 上右键点击 -> 选择 [属性]



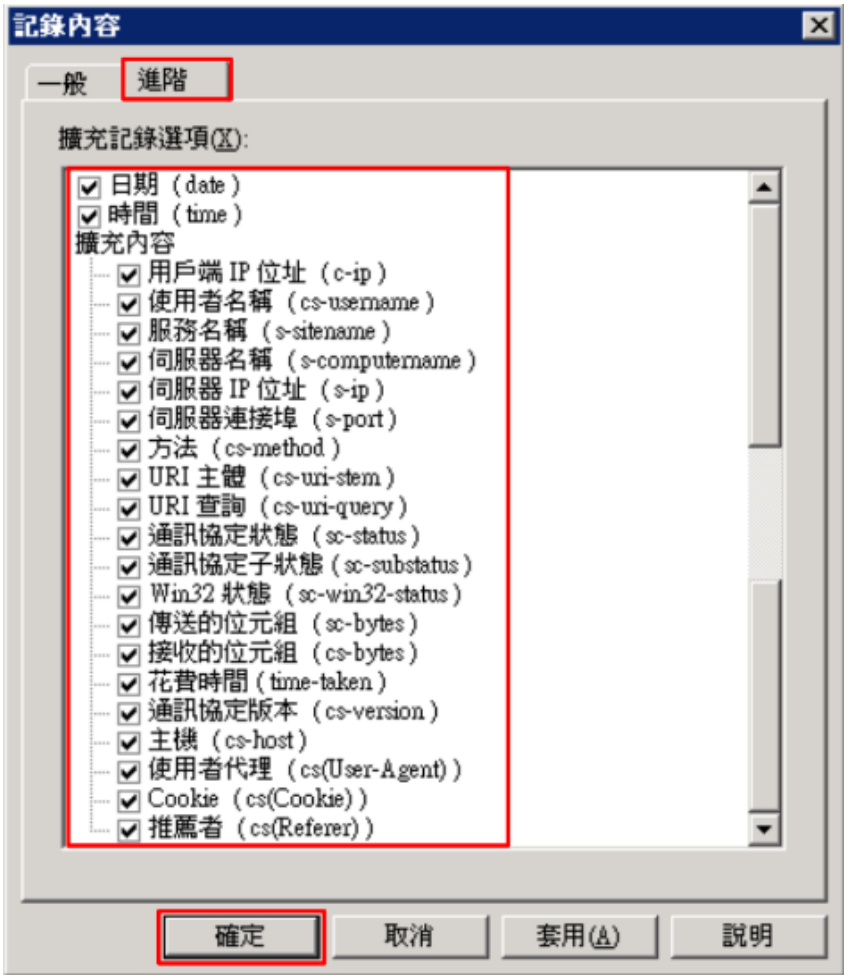
(8)　在 [网站] 页签：勾选 [启用日志] -> 当前日志格式选择 [W3C 扩展日志文件格式] -> 点击 [属性]



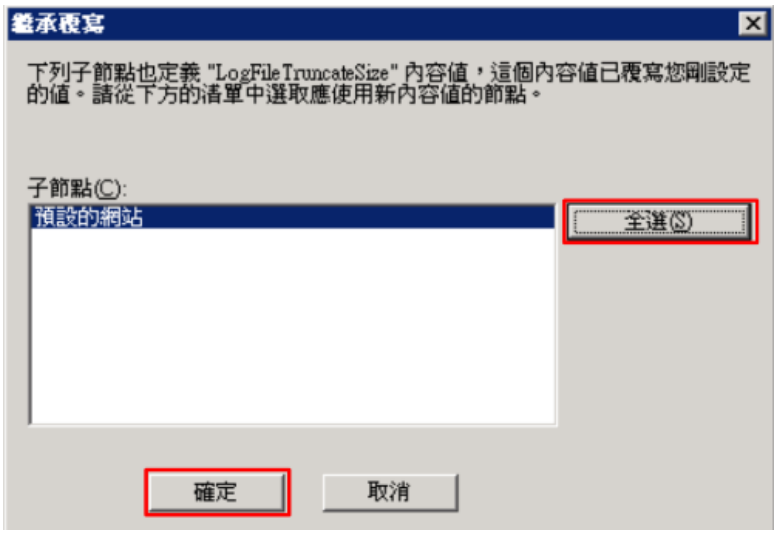
(9)　在 [常规] 页签：新增日志周期选择 [每小时] -> 勾选 [使用本地时间为文件命名] -> 日志文件目录输入 C:\Inetpub\logs\LogFiles -> 点击 [应用]



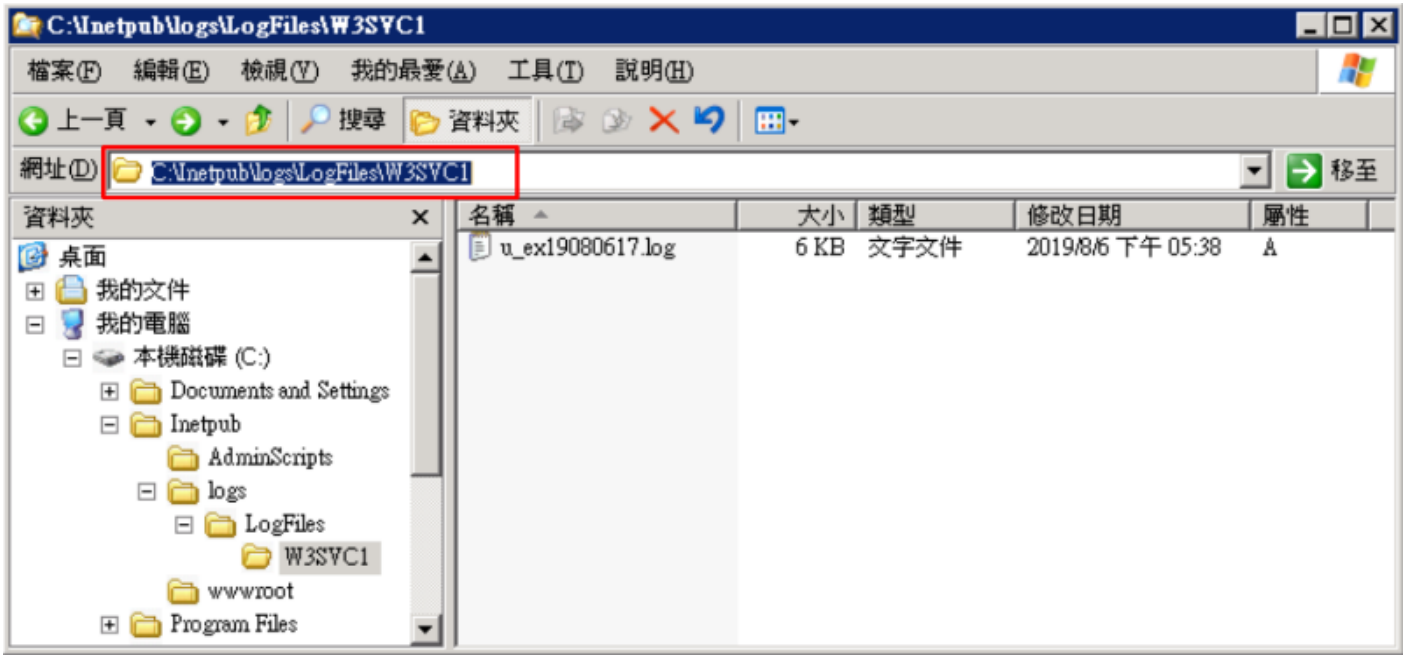
(10) 在 **[高级]** 页签：扩展日志选项勾选 **[日期 (date)]**、**[时间 (time)]**、**[客户端 IP 地址 (c-ip)]**、**[用户名 (cs-username)]**、**[服务名称 (s-sitename)]**、**[服务器名称 (s-computername)]**、**[服务器 IP 地址 (s-ip)]**、**[服务器端口 (s-port)]**、**[方法 (cs-method)]**、**[URI 主体 (cs-uri-stem)]**、**[URI 查询 (cs-uri-query)]**、**[协议状态 (sc-status)]**、**[协议子状态 (sc-substatus)]**、**[Win32 状态 (sc-win32-status)]**、**[发送字节数 (sc-bytes)]**、**[接收字节数 (cs-bytes)]**、**[耗时 (time-taken)]**、**[协议版本 (cs-version)]**、**[主机 (cs-host)]**、**[用户代理 (cs(User-Agent))]**、**[Cookie(cs(Cookie))]**、**[引荐者 (cs(Referer))]** -> 点击 **[确定]**



(11) 点击 **[全选]** 和 **[确定]**



(12)　确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹内是否存在 IIS 日志文件: ex*.log

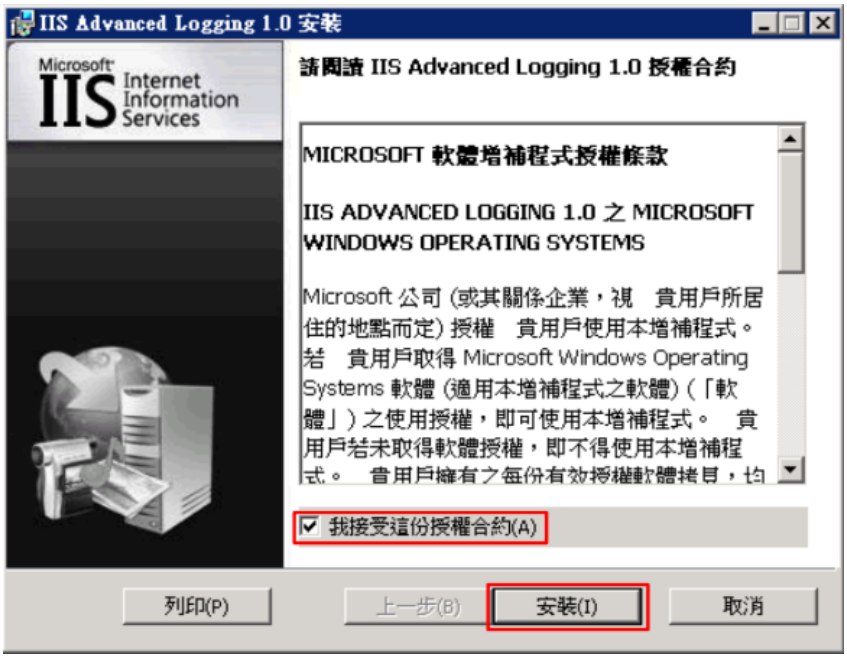


4 Windows 2008

(1) 安装 [IIS Advanced Logging]

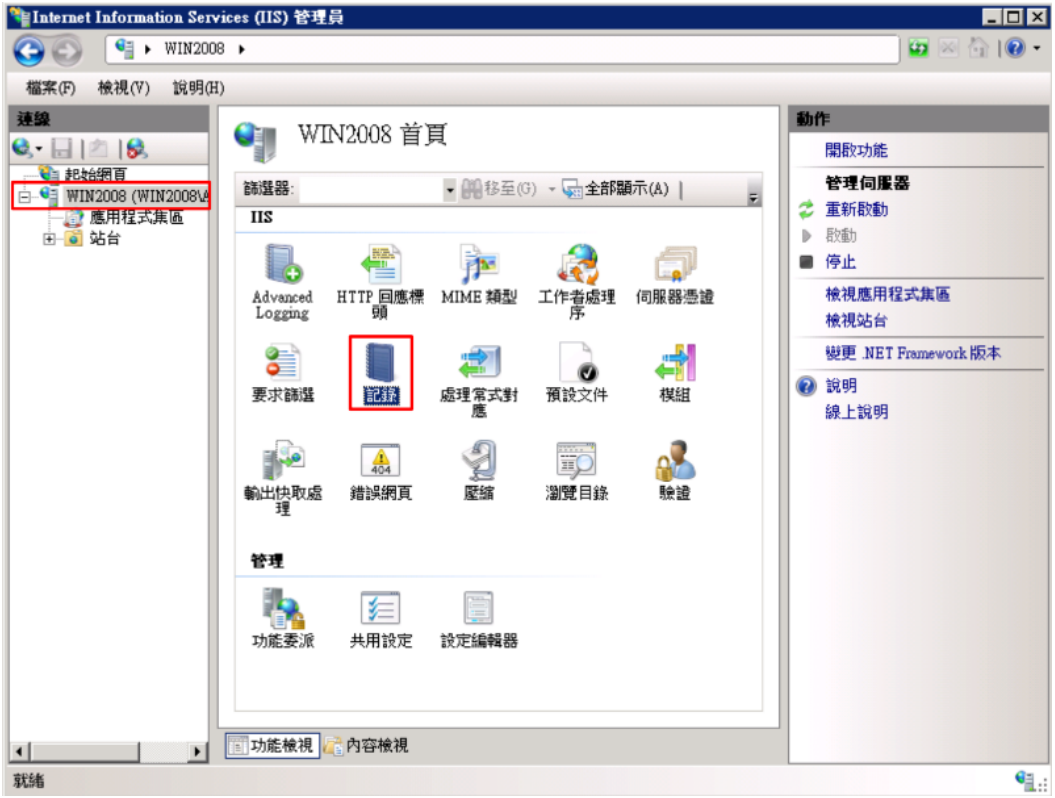
注：如需下载 IIS Advanced Logging 软件，请与我们联系。

点击 [AdvancedLogging_amd64_zh-TW.msi] -> 勾选 [我接受这份授权协议]-> 点击 [安装] 直至 [完成]

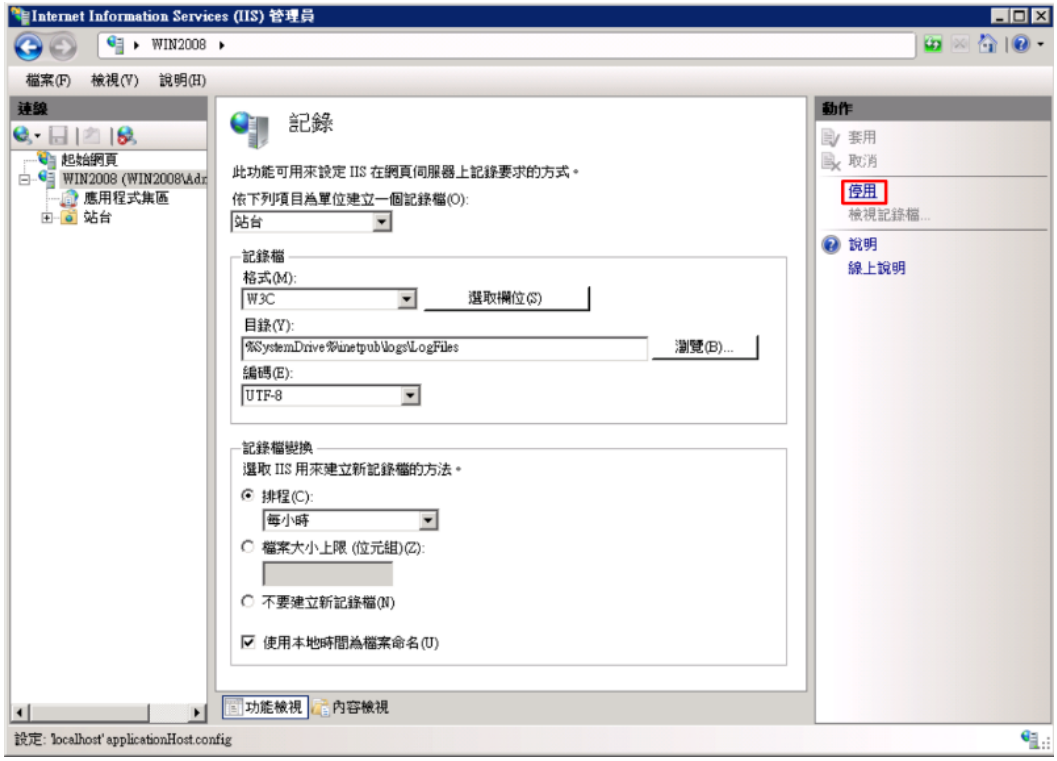


(2) 打开 [互联网信息服务 (IIS) 管理器]

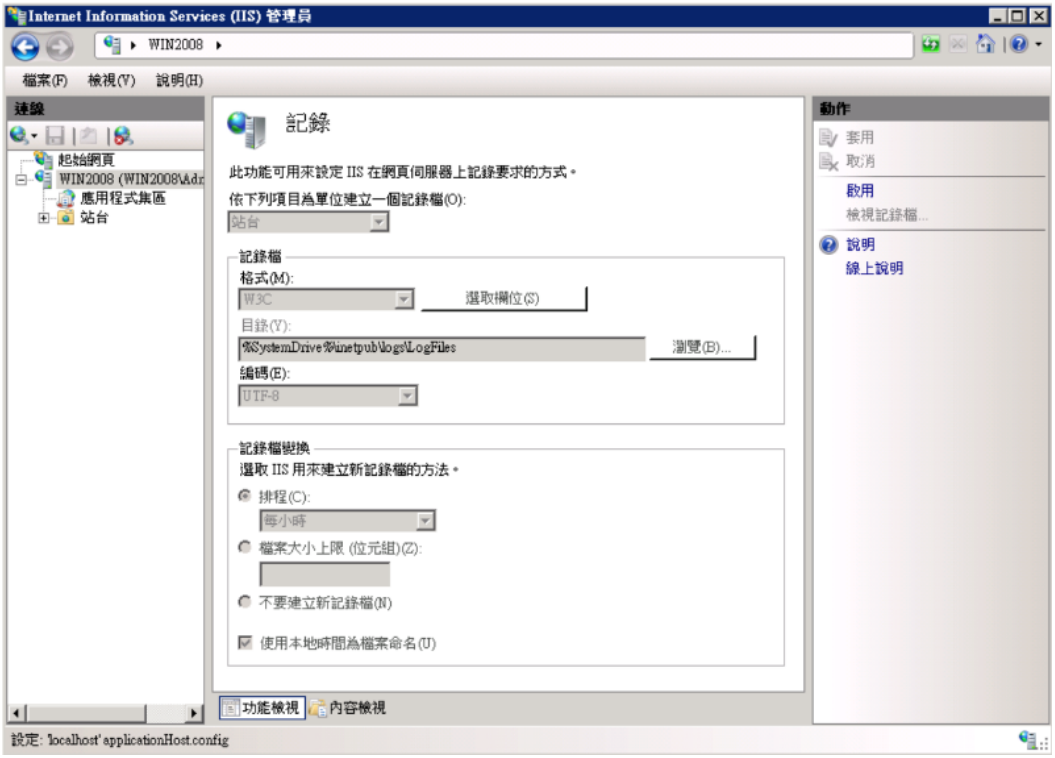
(3) 选择 [IIS 服务器] -> 点击 [日志]



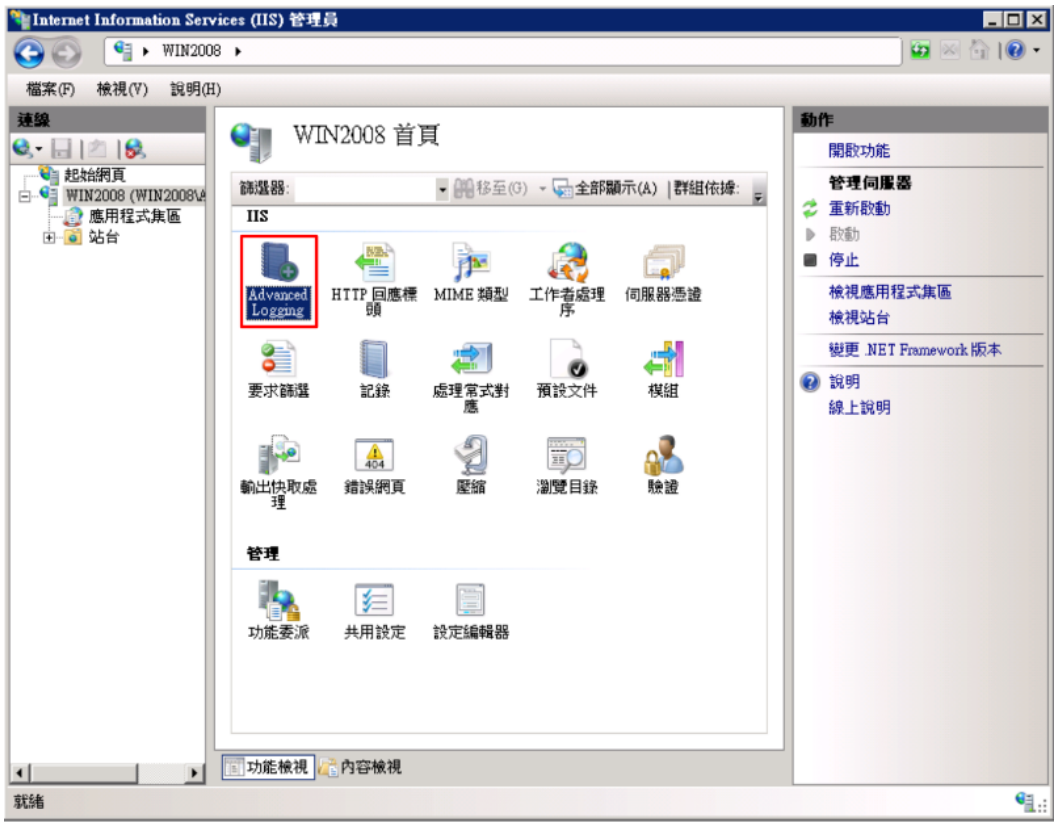
(4) 点击 [停用]



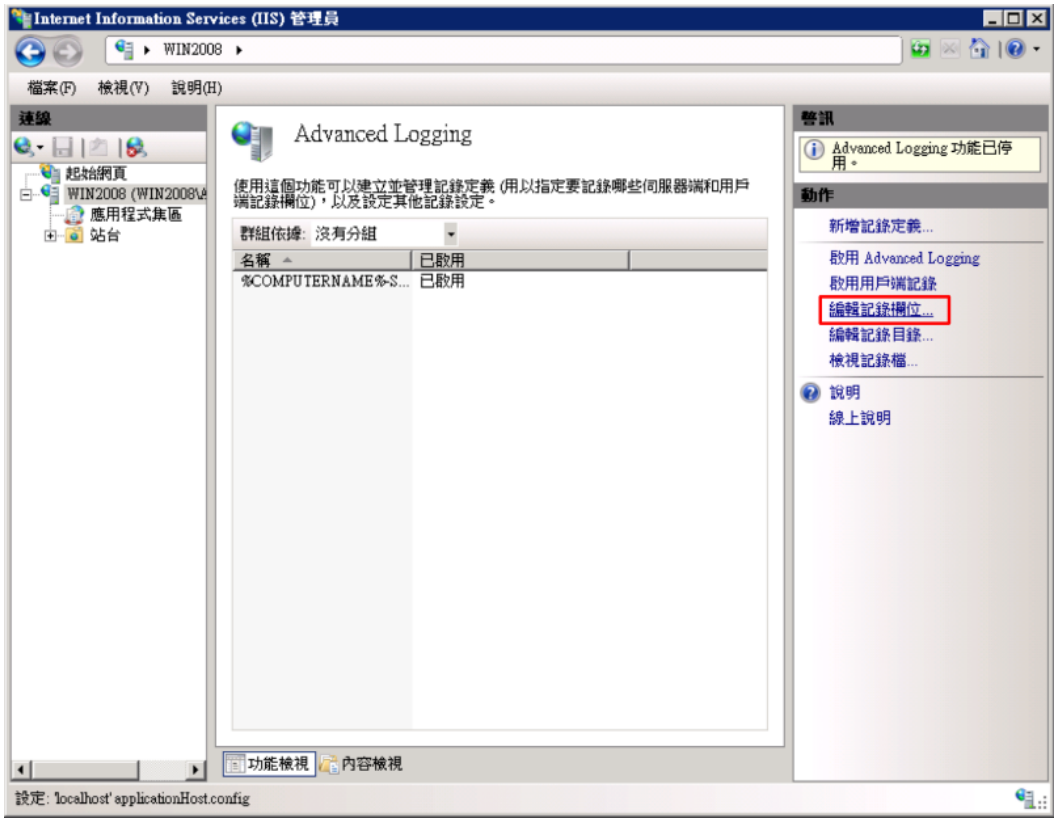
(5)　确认日志已停用



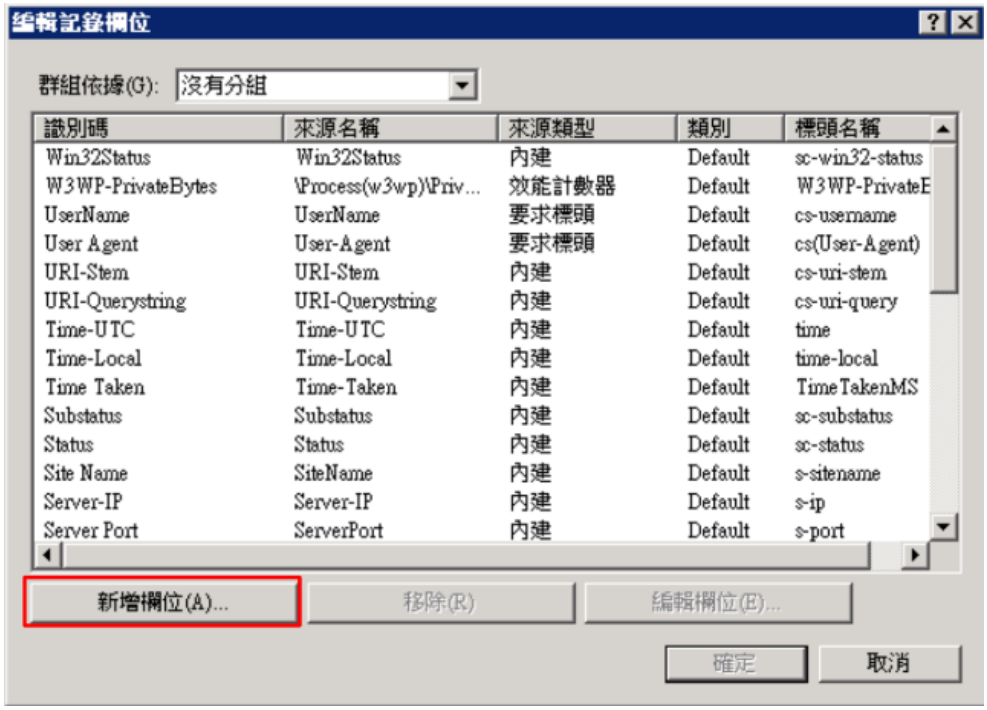
(6)　点击 [高级日志记录]



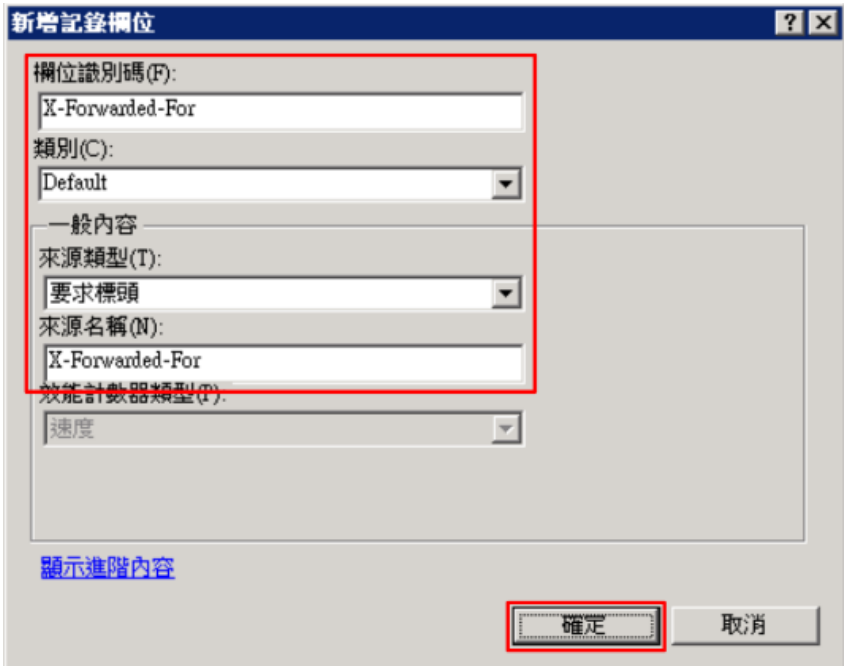
(7)　点击 [编辑日志字段]



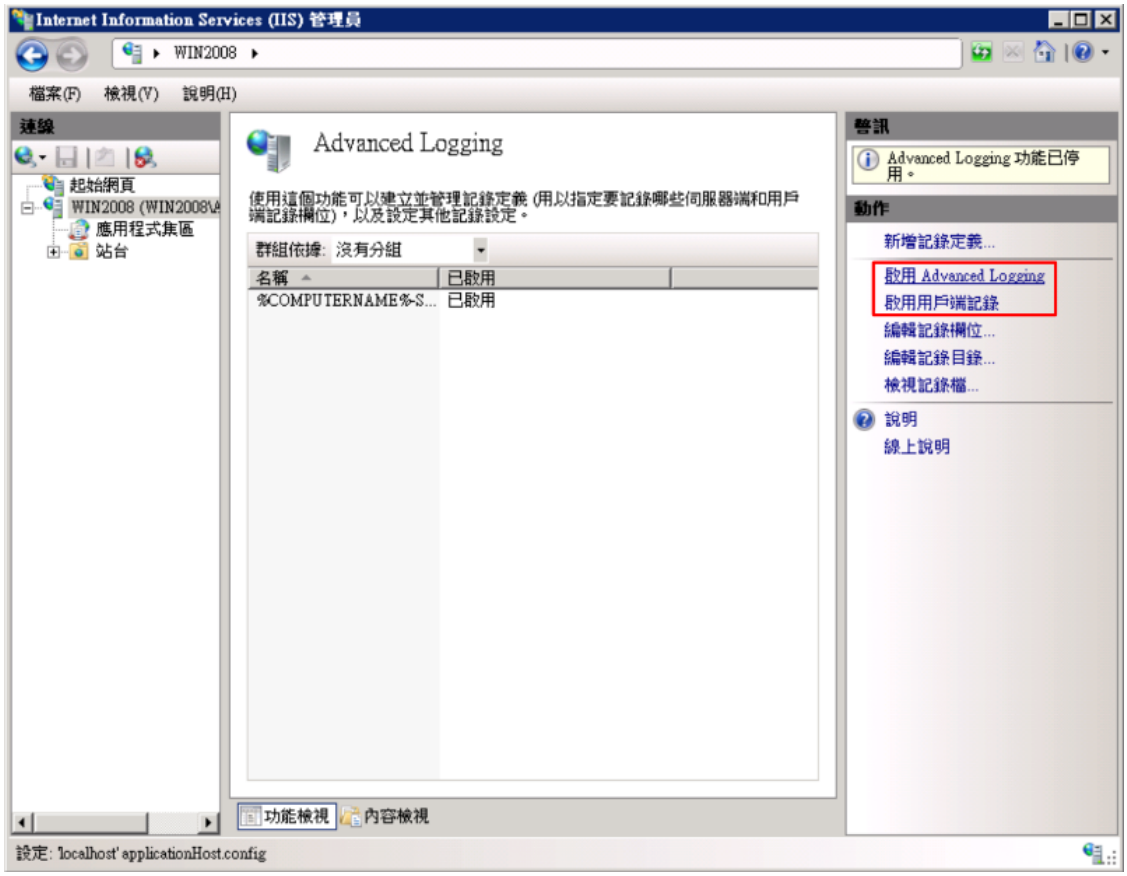
(8)　点击 [新增字段]



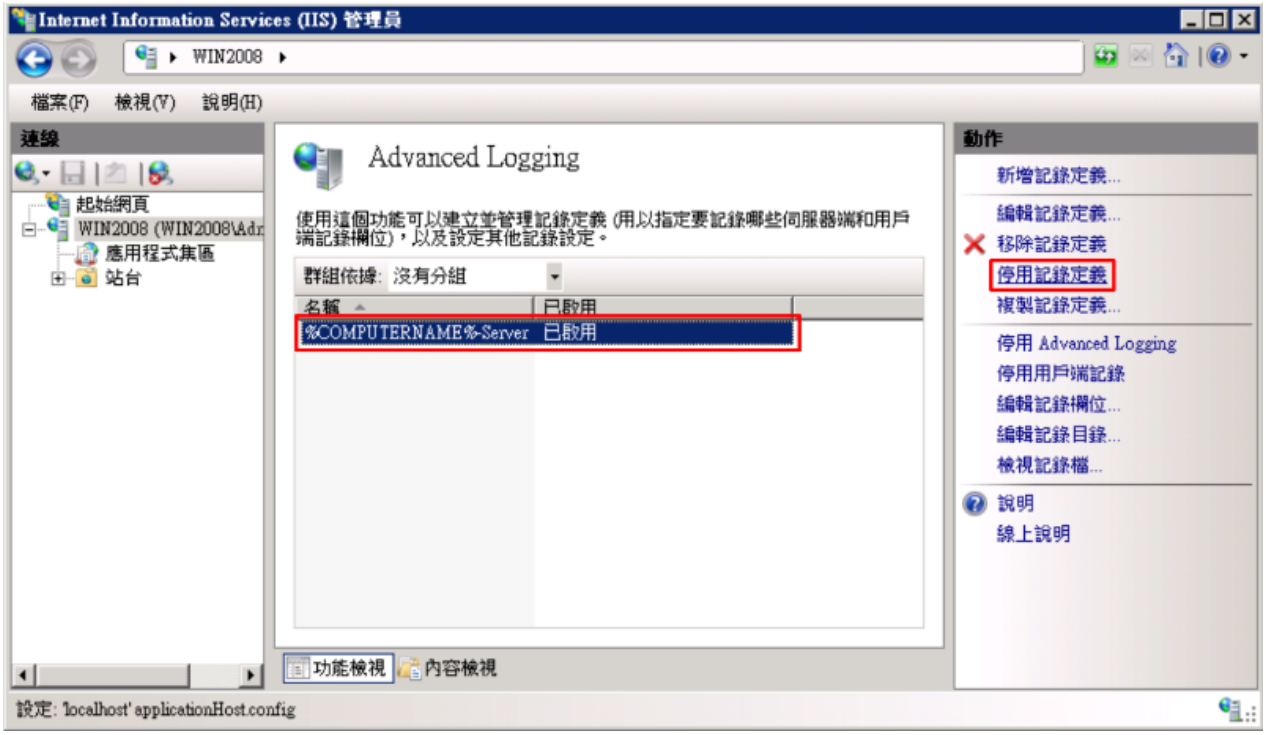
(9) 输入字段标识符: X-Forwarded-For-> 选择类别: [Default] -> 来源类型: [Request Header(请求头)] -> 输入来源名称: X-Forwarded-For-> 点击 [确定]



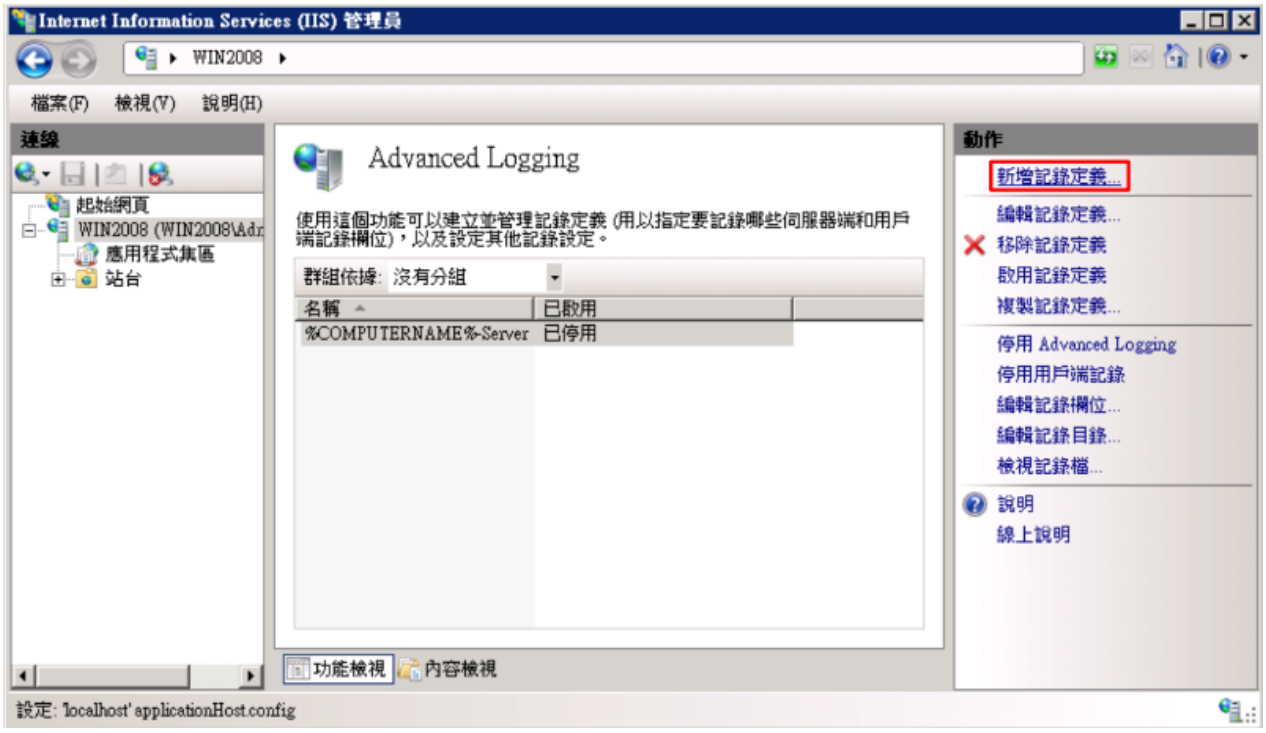
(10) 点击 [启用高级日志] 和 [启用客户端日志]



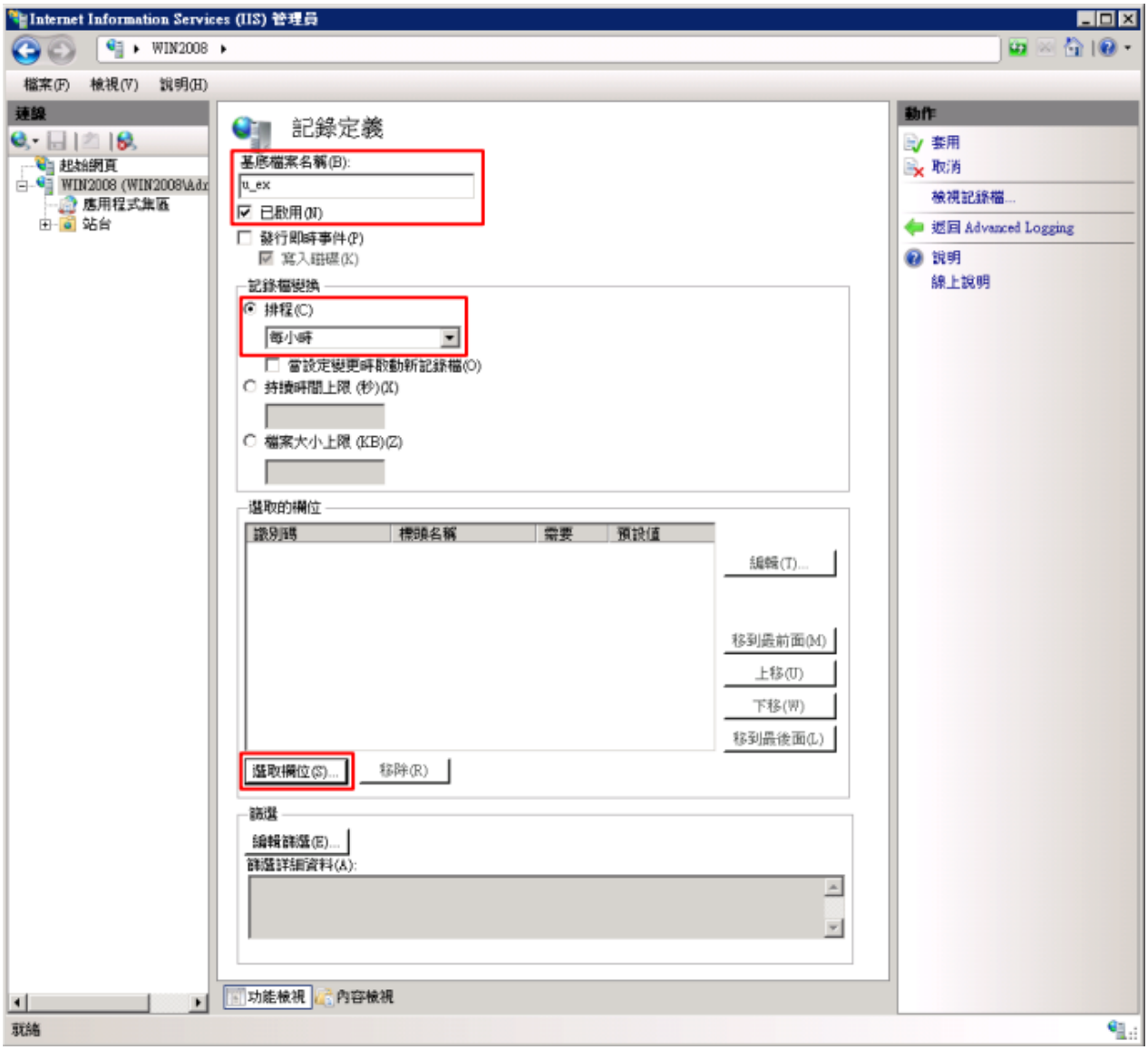
(11) 选择 **[%COMPUTERNAME%-Server] -> 点击 [停用日志定义]**



(12) 点击 **[新增日志定义]**

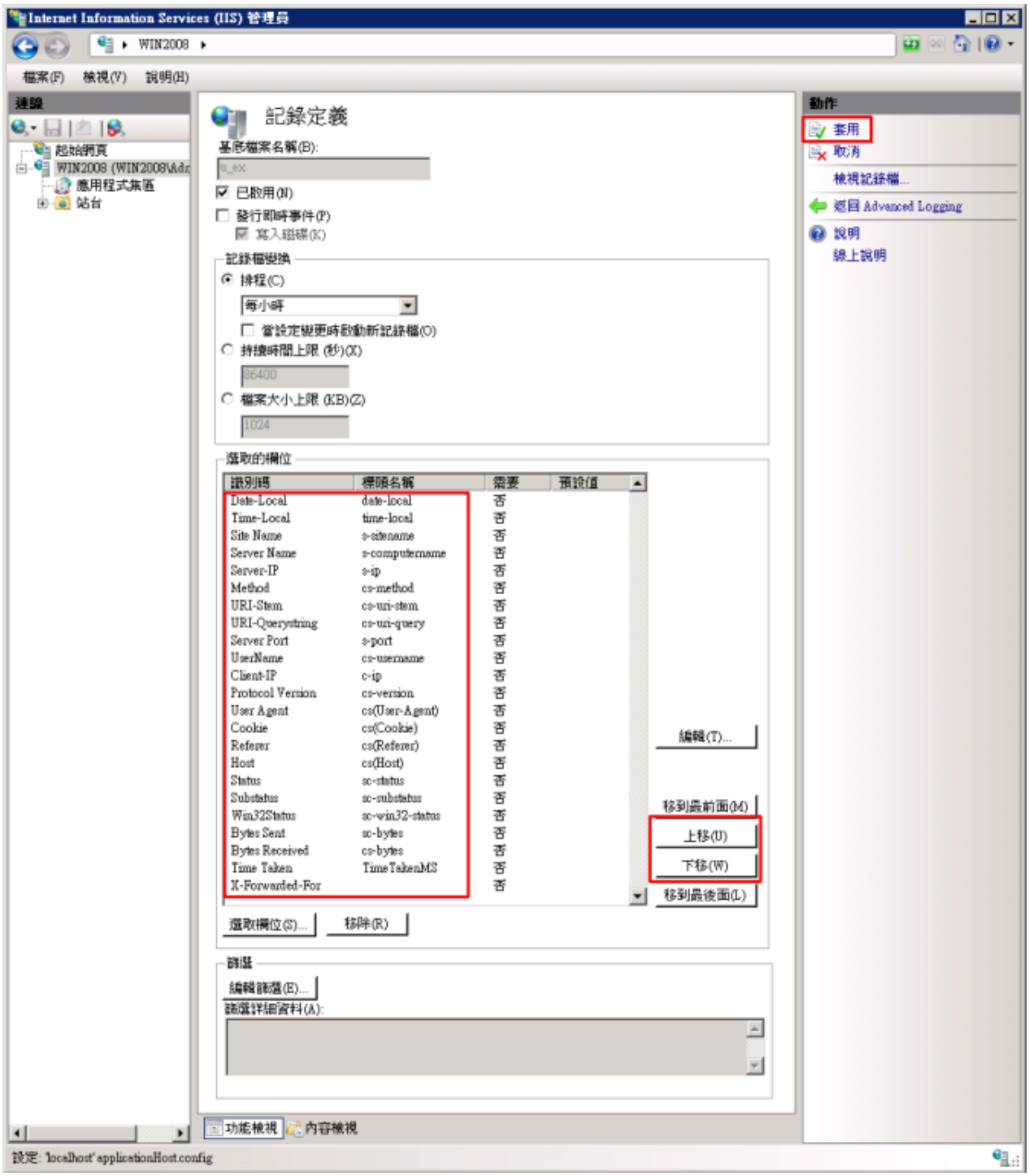


(13)　输入基础文件名称: u_ex -> 勾选 [已启用] -> 选择排程 [每小时] -> 点击 [选择字段]

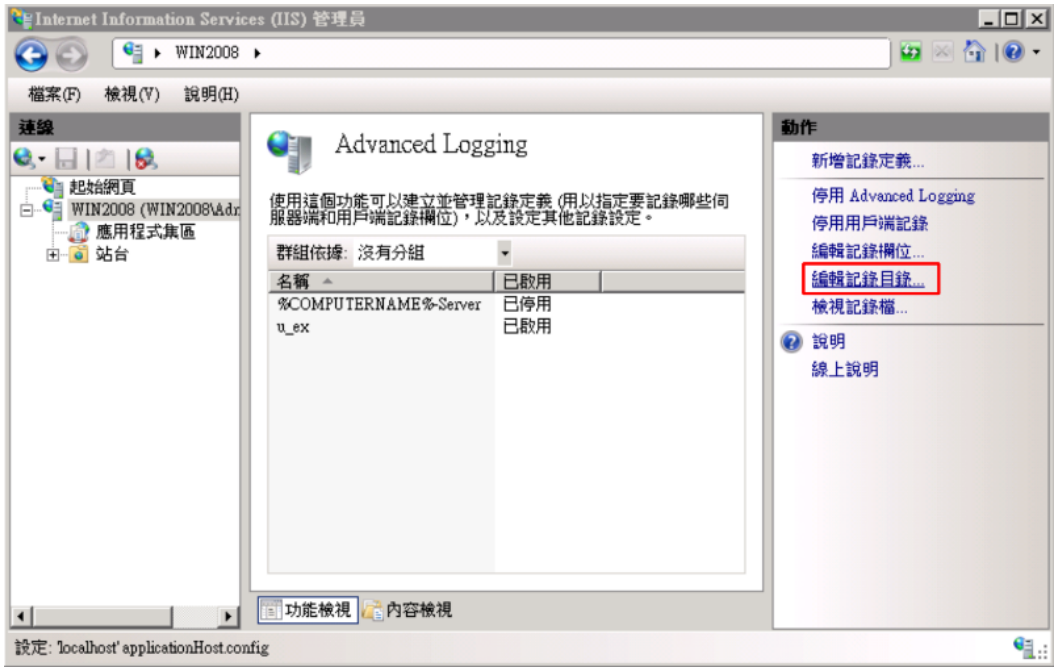


(14) 勾选 **[X-Forwarded-For]**、**[Win32 状态 (sc-win32-status)]**、**[用户名 (cs-username)]**、**[用户代理 (cs(User-Agent))]**、**[URI 主体 (cs-uri-stem)]**、**[URI 查询 (cs-uri-query)]**、**[本地时间 (time-local)]**、**[耗时 (TimeTakenMS)]**、**[子状态 (sc-substatus)]**、**[状态 (sc-status)]**、**[站点名称 (s-sitename)]**、**[服务器 IP(s-ip)]**、**[服务器端口 (s-port)]**、**[服务器名称 (s-computername)]**、**[引荐者 (cs(Referer))]**、**[协议版本 (cs-version)]**、**[方法 (cs-method)]**、**[主机 (cs(Host))]**、**[本地日期 (date-local)]**、**[Cookie(cs(Cookie))]**、**[客户端 IP(c-ip)]**、**[发送字节数 (sc-bytes)]**、**[接收字节数 (cs-bytes)]** -> 点击 **[确定]**

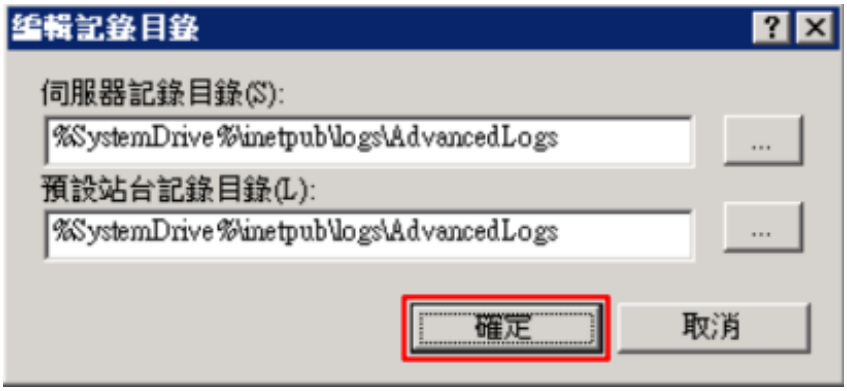
(15) 调整选择的字段: **[本地日期 (date-local)]**、**[本地时间 (time-local)]**、**[站点名称 (s-sitename)]**、**[服务器名称 (s-computername)]**、**[服务器 IP(s-ip)]**、**[方法 (cs-method)]**、**[URI 主体 (cs-uri-stem)]**、**[URI 查询 (cs-uri-query)]**、**[服务器端口 (s-port)]**、**[用户名 (cs-username)]**、**[客户端 IP(c-ip)]**、**[协议版本 (cs-version)]**、**[用户代理 (cs(User-Agent))]**、**[Cookie(cs(Cookie))]**、**[引荐者 (cs(Referer))]**、**[主机 (cs(Host))]**、**[状态 (sc-status)]**、**[子状态 (sc-substatus)]**、**[Win32 状态 (sc-win32-status)]**、**[发送字节数 (sc-bytes)]**、**[接收字节数 (cs-bytes)]**、**[耗时 (TimeTakenMS)]**、**[X-Forwarded-For]** -> 点击 **[应用]**



(16)　点击 [编辑日志目录]



(17)　确认服务器日志目录和默认站点日志目录 -> 点击 [确定]



(18)　修改 nxlog.conf

註: 参考 1.3 NXLog 配置文件

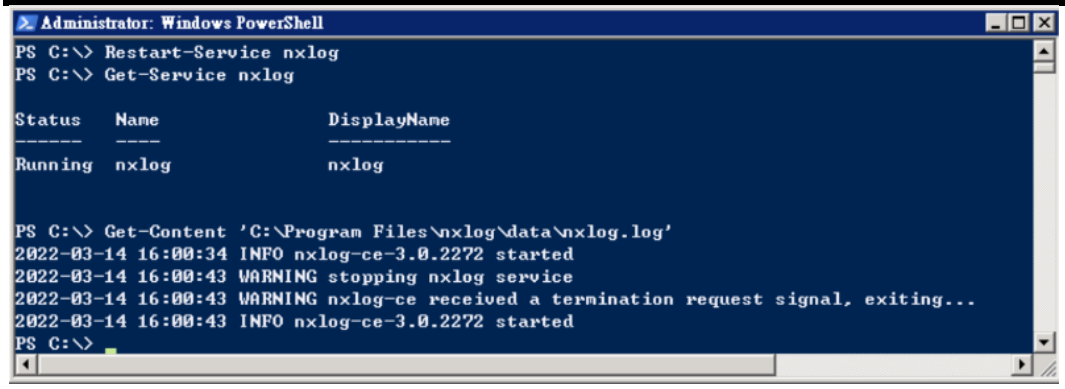
蓝色文字部分请填写 Microsoft IIS 日志文件夹路径

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

(19)　打开 [Windows PowerShell]

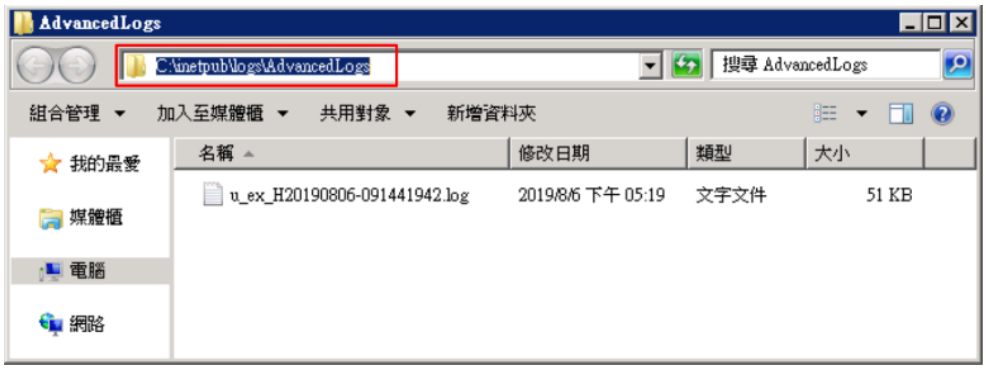
(20)　重启 nxlog 服务，检查 NXLog 服务并确认 NXLog 没有错误信息

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



(21)　点击 [重启] IIS 服务

(22)　确认 [C:\inetpub\logs\AdvancedLogs] 文件夹中是否存在 IIS 日志文件: u_ex*.log

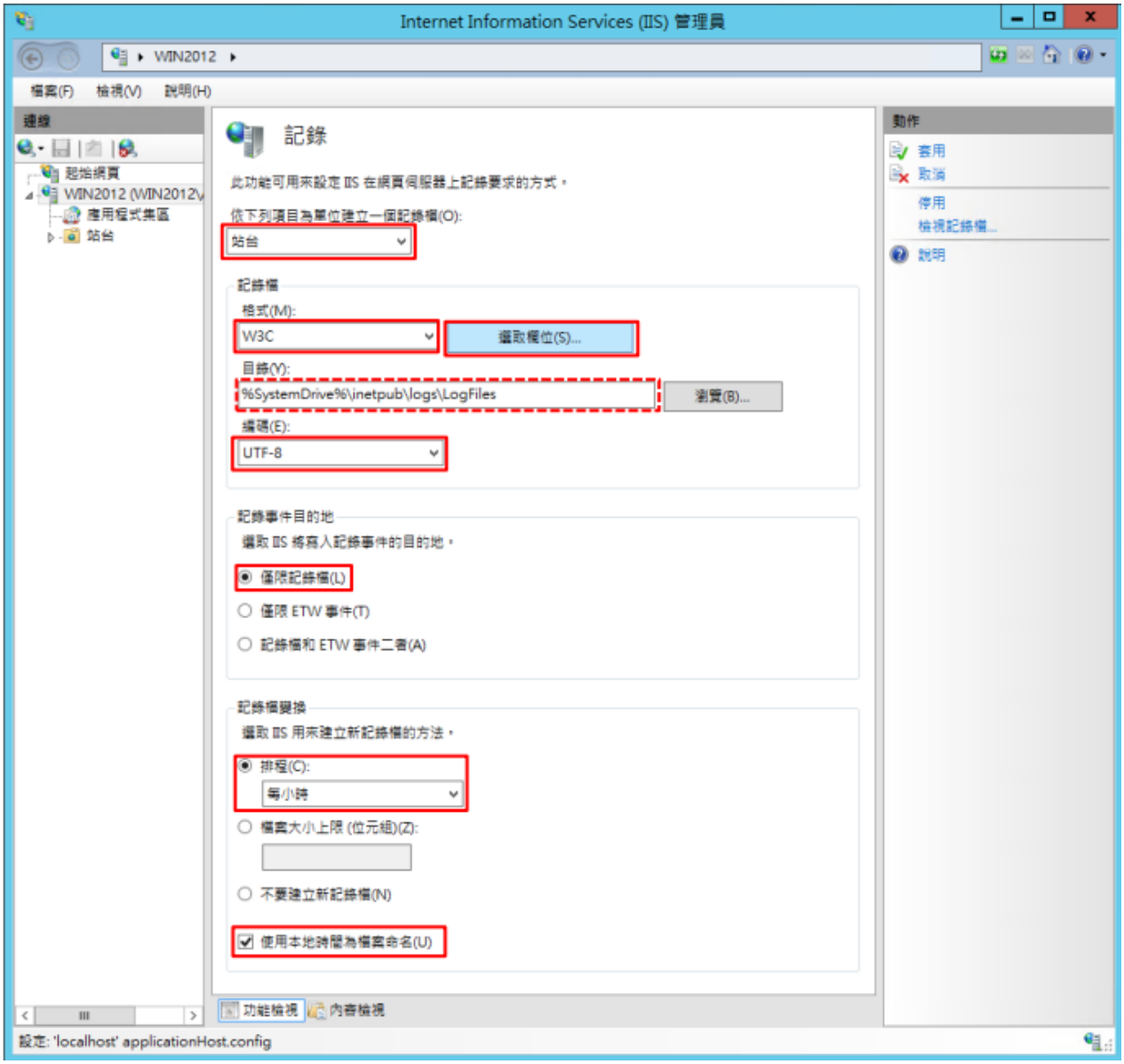


5 Windows 2012

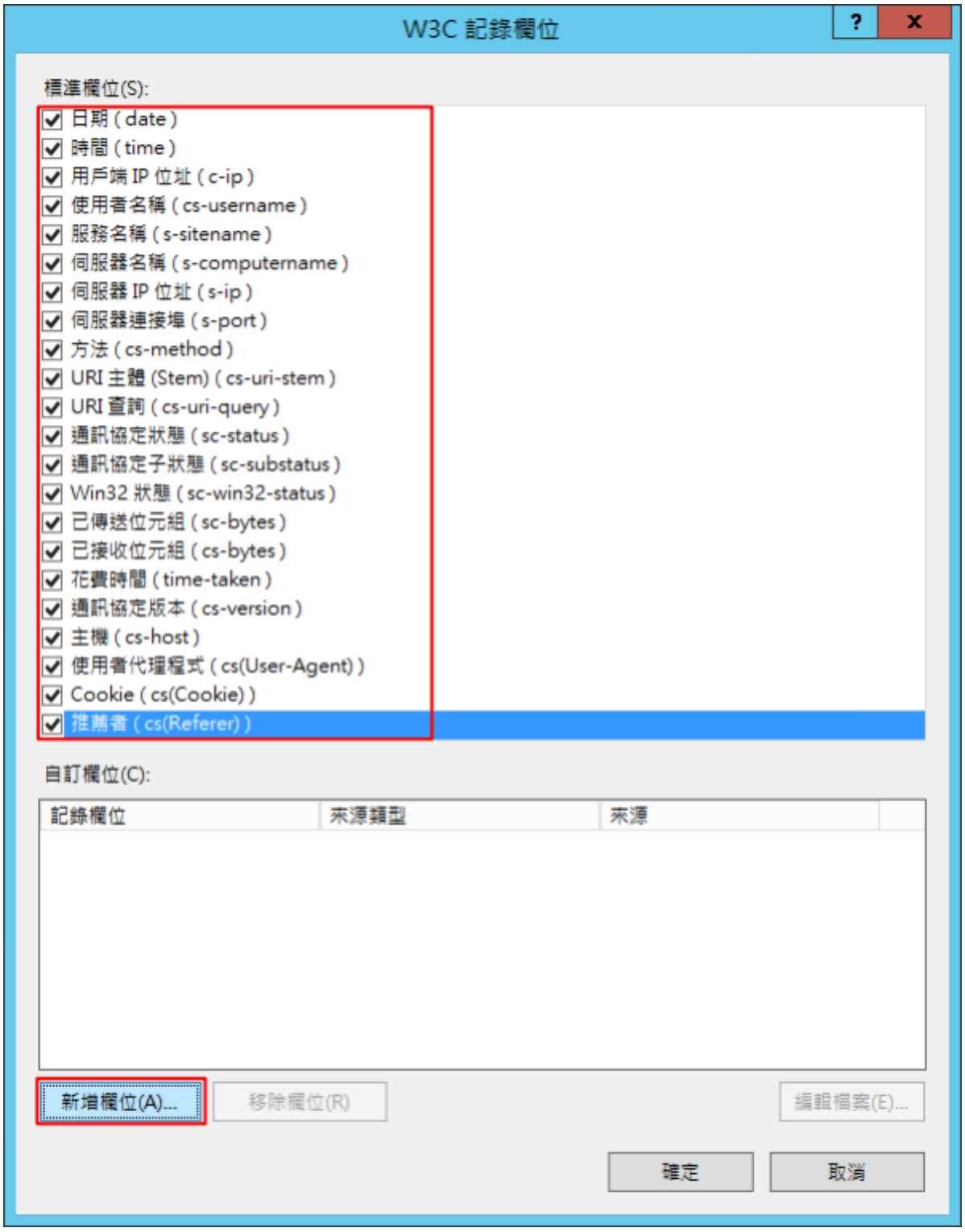
(1) 打开 [互联网信息服务 (IIS) 管理员]

(2) 选择 [IIS 服务器] -> 点击 [日志]

(3) 选择以下项目为单位建立一个日志文件: [站点] -> 日志格式: [W3C] -> 目录: %SystemDrive%\inetpub\logs\LogFiles -> 编码: [UTF-8] -> 日志事件目的地: [仅限日志文件] -> 排程: [每小时] -> 勾选 [使用本地时间为文件命名] -> 点击 [选择字段]

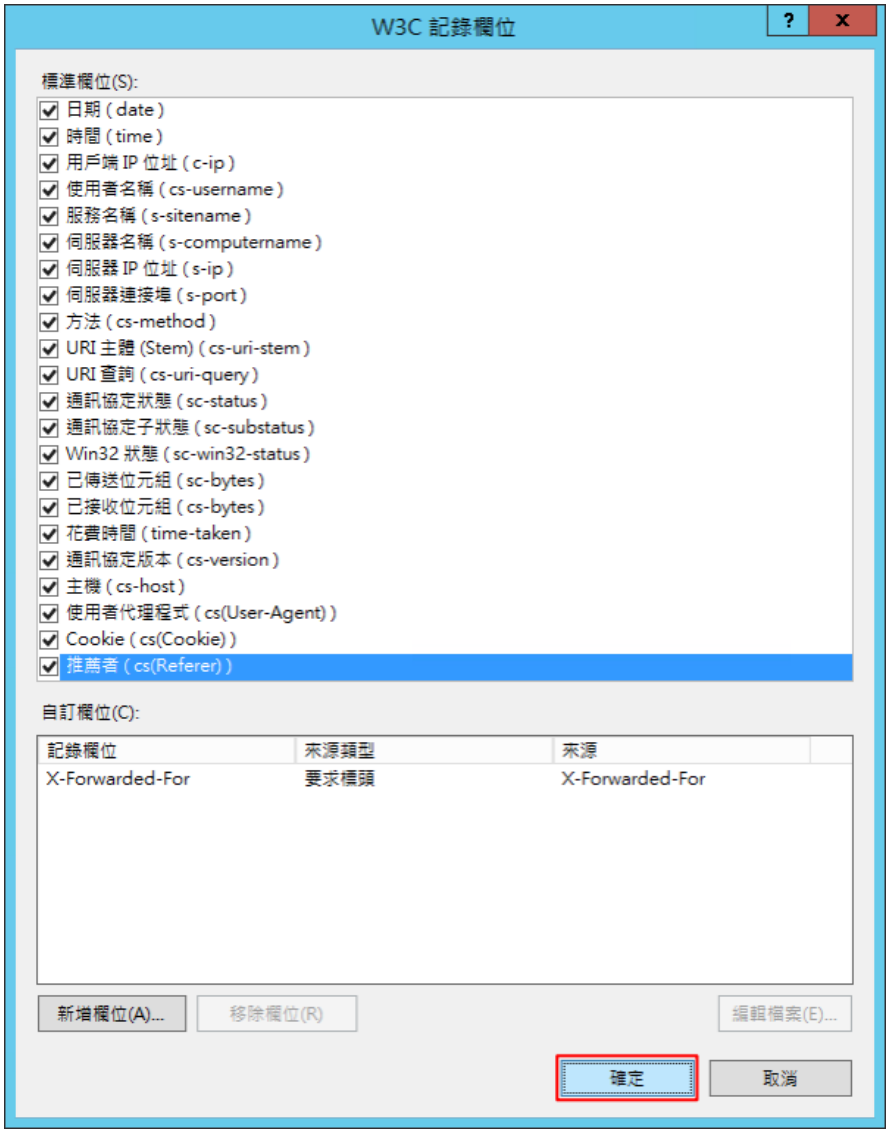


(4) 勾选 [日期 (date)]、[时间 (time)]、[客户端 IP 地址 (c-ip)]、[用户名 (cs-username)]、[服务名称 (s-sitename)]、[服务器名称 (s-computername)]、[服务器 IP 地址 (s-ip)]、[服务器端口 (s-port)]、[方法 (cs-method)]、[URI 主体 (cs-uri-stem)]、[URI 查询 (cs-uri-query)]、[协议状态 (sc-status)]、[协议子状态 (sc-substatus)]、[Win32 状态 (sc-win32-status)]、[发送字节数 (sc-bytes)]、[接收字节数 (cs-bytes)]、[耗时 (time-taken)]、[协议版本 (cs-version)]、[主机 (cs-host)]、[用户代理 (cs(User-Agent))]、[Cookie(cs(Cookie))]、[推荐者 (cs(Referer))] -> 点击 [添加字段]

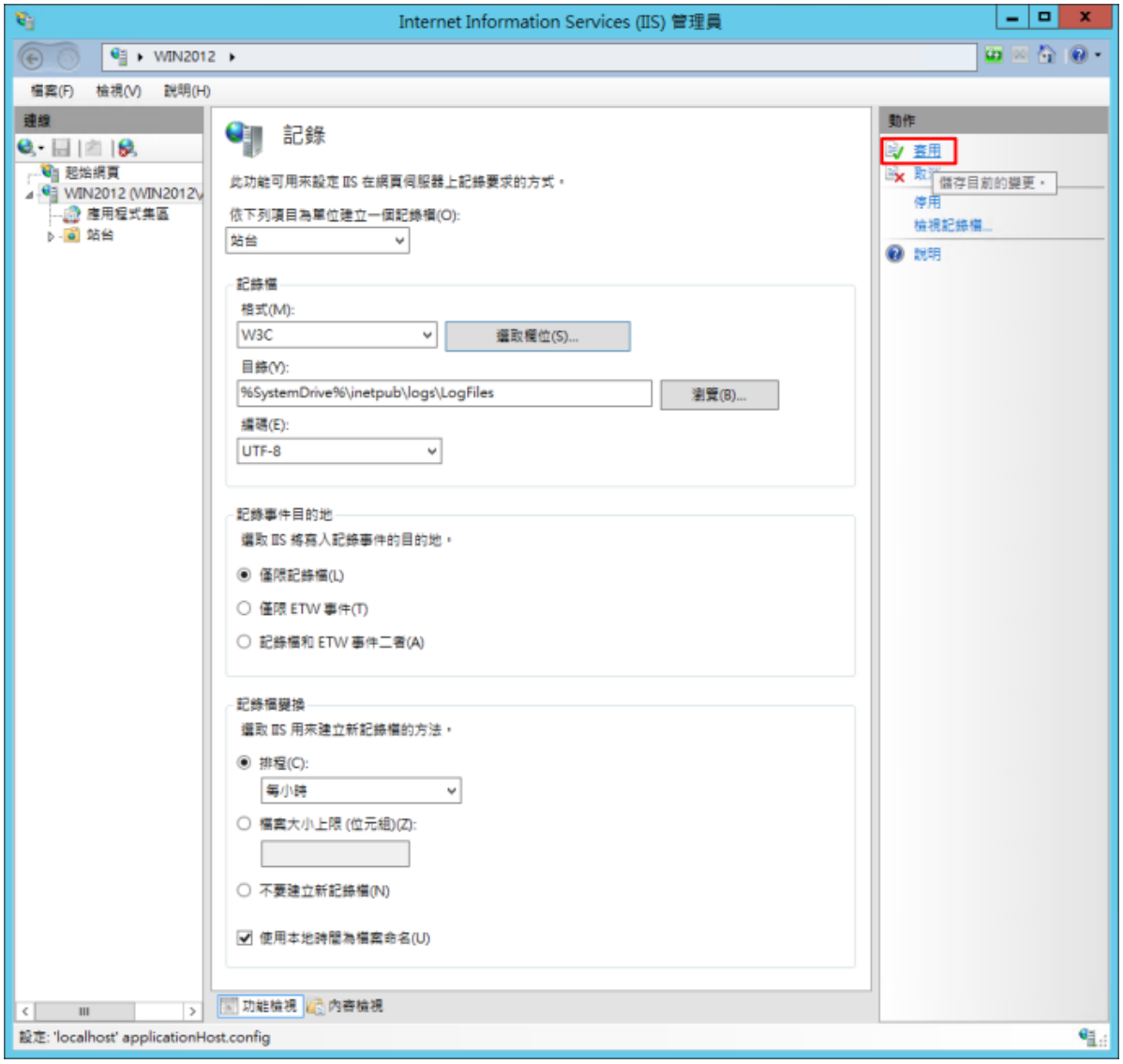


(5) 输入字段名称: X-Forwarded-For-> 选择来源类型: **[Request Header(请求头)]** -> 输入来源: X-Forwarded-For-> 点击 **[确定]**

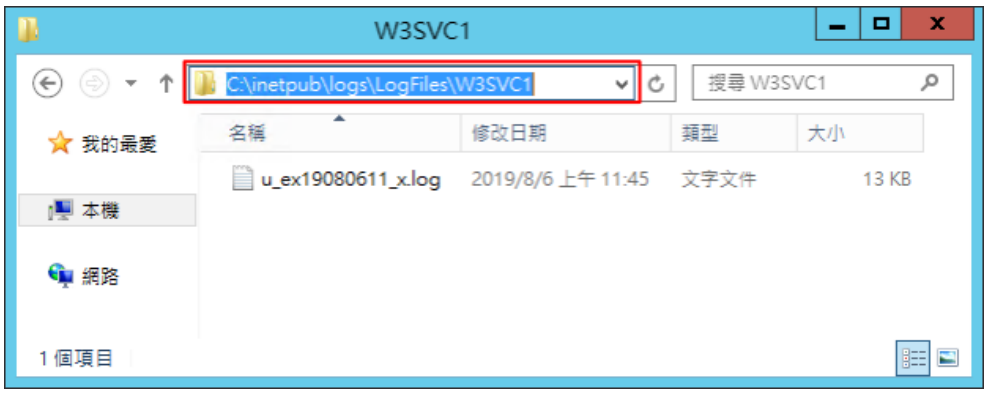
(6) 点击 **[确定]**



(7)　点击 [应用]



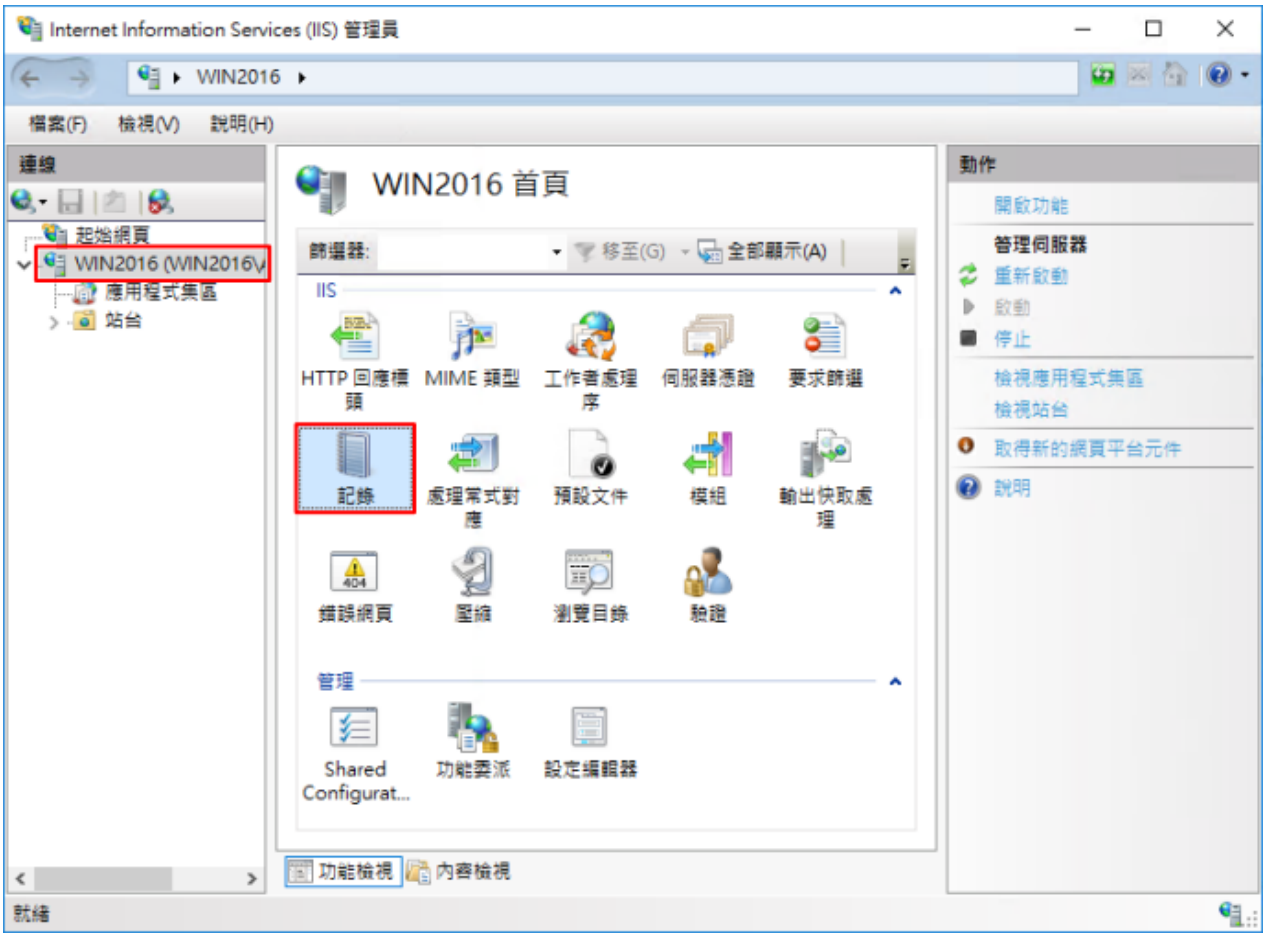
(8)　确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹中的 IIS 日志文件: ex*.log



6 Windows 2016

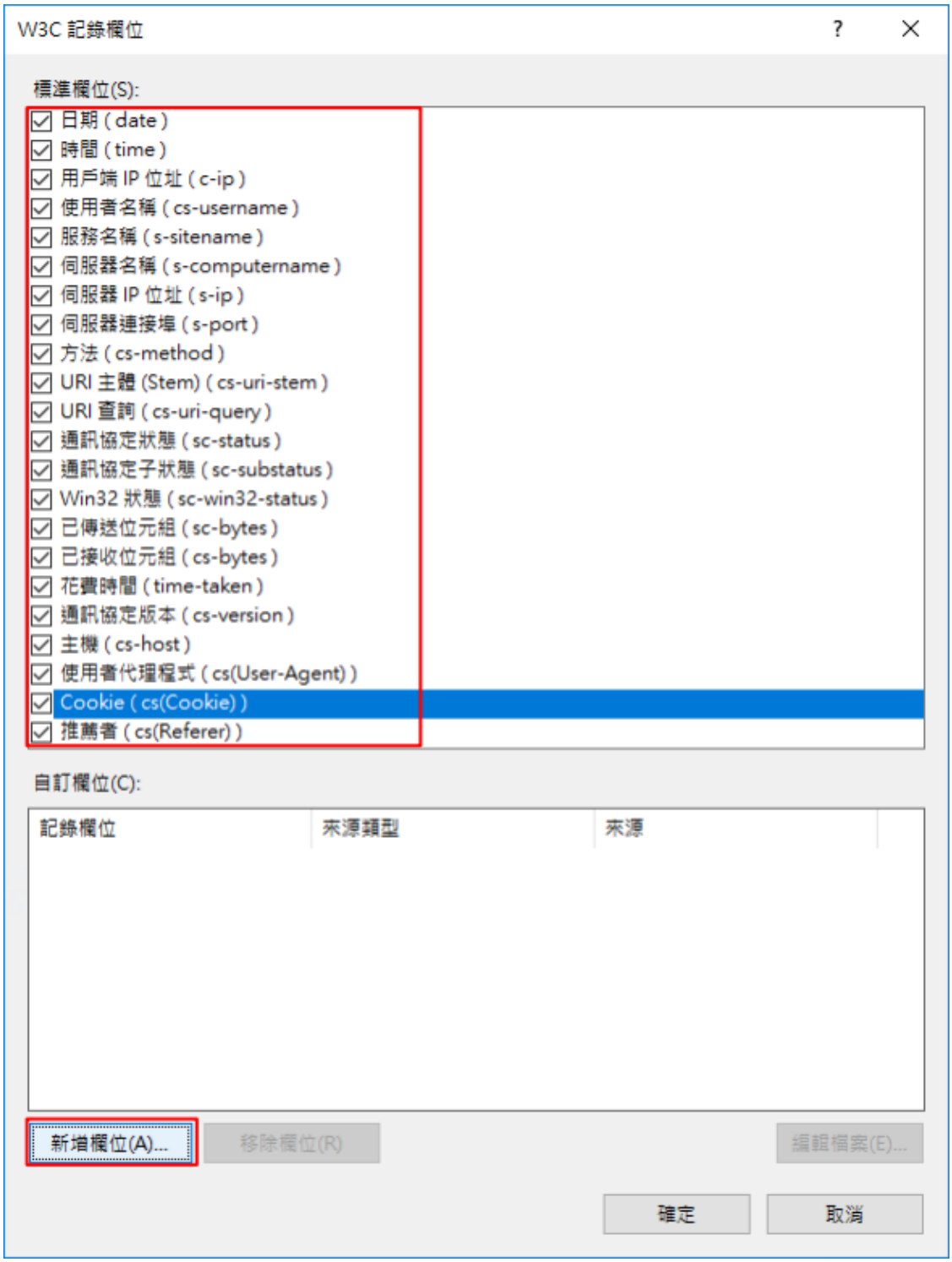
(1) 打开 [互联网信息服务 (IIS) 管理员]

(2) 选择 [IIS 服务器] -> 点击 [日志]

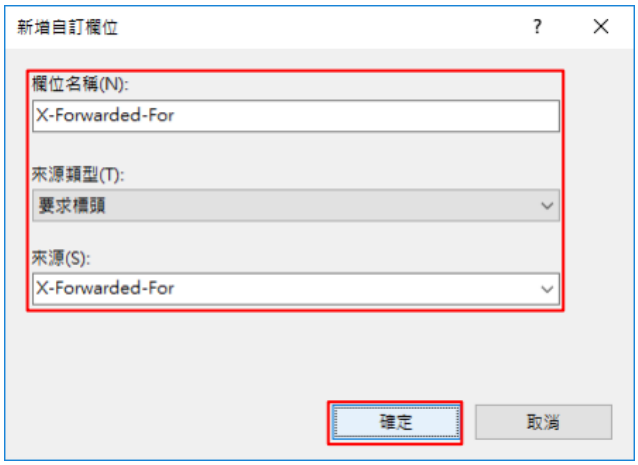


(3) 选择以下项目为单位创建一个日志文件: [站点] -> 日志格式: [W3C] -> 目录: %SystemDrive%\inetpub\logs\LogFiles -> 编码: [UTF-8] -> 日志事件目的地: [仅限日志文件] -> 排程: [每小时] -> 勾选 [使用本地时间为文件命名] -> 点击 [选择字段]

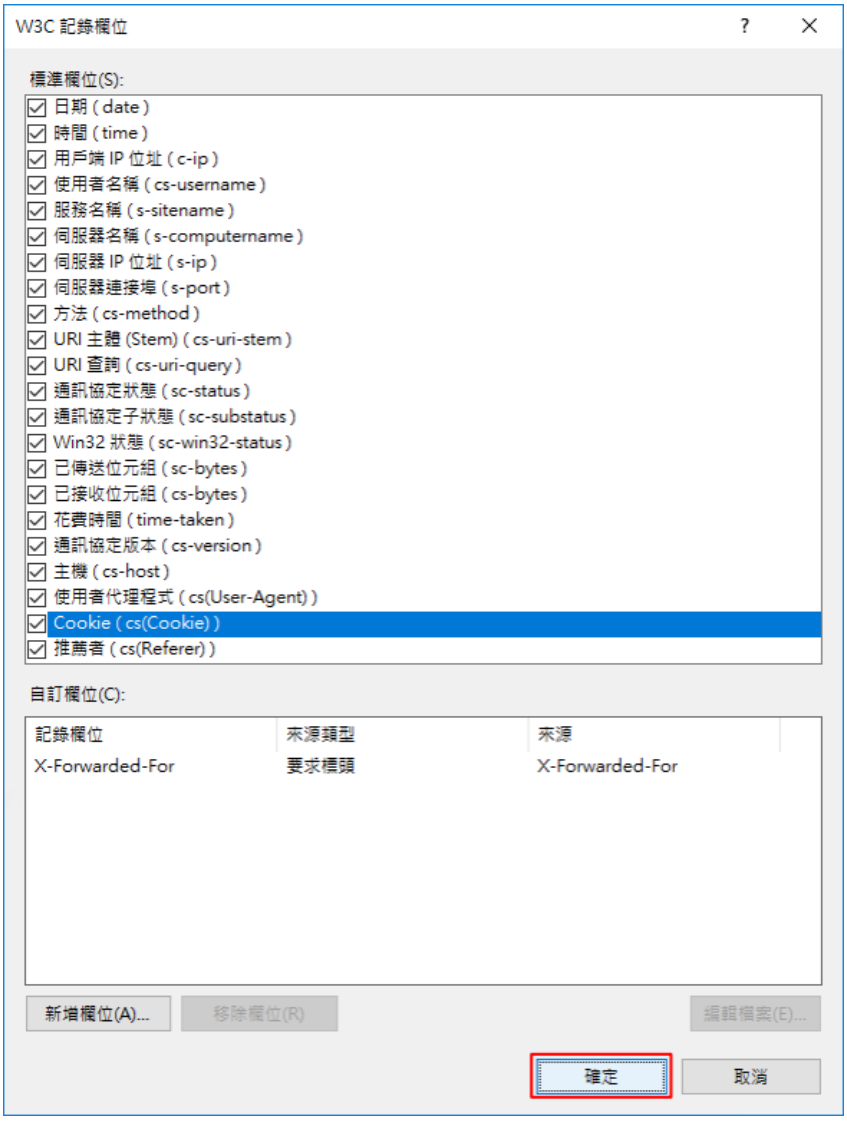
(4) 勾选 [日期 (date)]、[时间 (time)]、[客户端 IP 地址 (c-ip)]、[用户名 (cs-username)]、[服务名称 (s-sitename)]、[服务器名称 (s-computername)]、[服务器 IP 地址 (s-ip)]、[服务器端口 (s-port)]、[方法 (cs-method)]、[URI 主体 (cs-uri-stem)]、[URI 查询 (cs-uri-query)]、[协议状态 (sc-status)]、[协议子状态 (sc-substatus)]、[Win32 状态 (sc-win32-status)]、[发送字节数 (sc-bytes)]、[接收字节数 (cs-bytes)]、[耗时 (time-taken)]、[协议版本 (cs-version)]、[主机 (cs-host)]、[用户代理 (cs(User-Agent))]、[Cookie(cs(Cookie))]、[推荐者 (cs(Referer))] -> 点击 [添加字段]



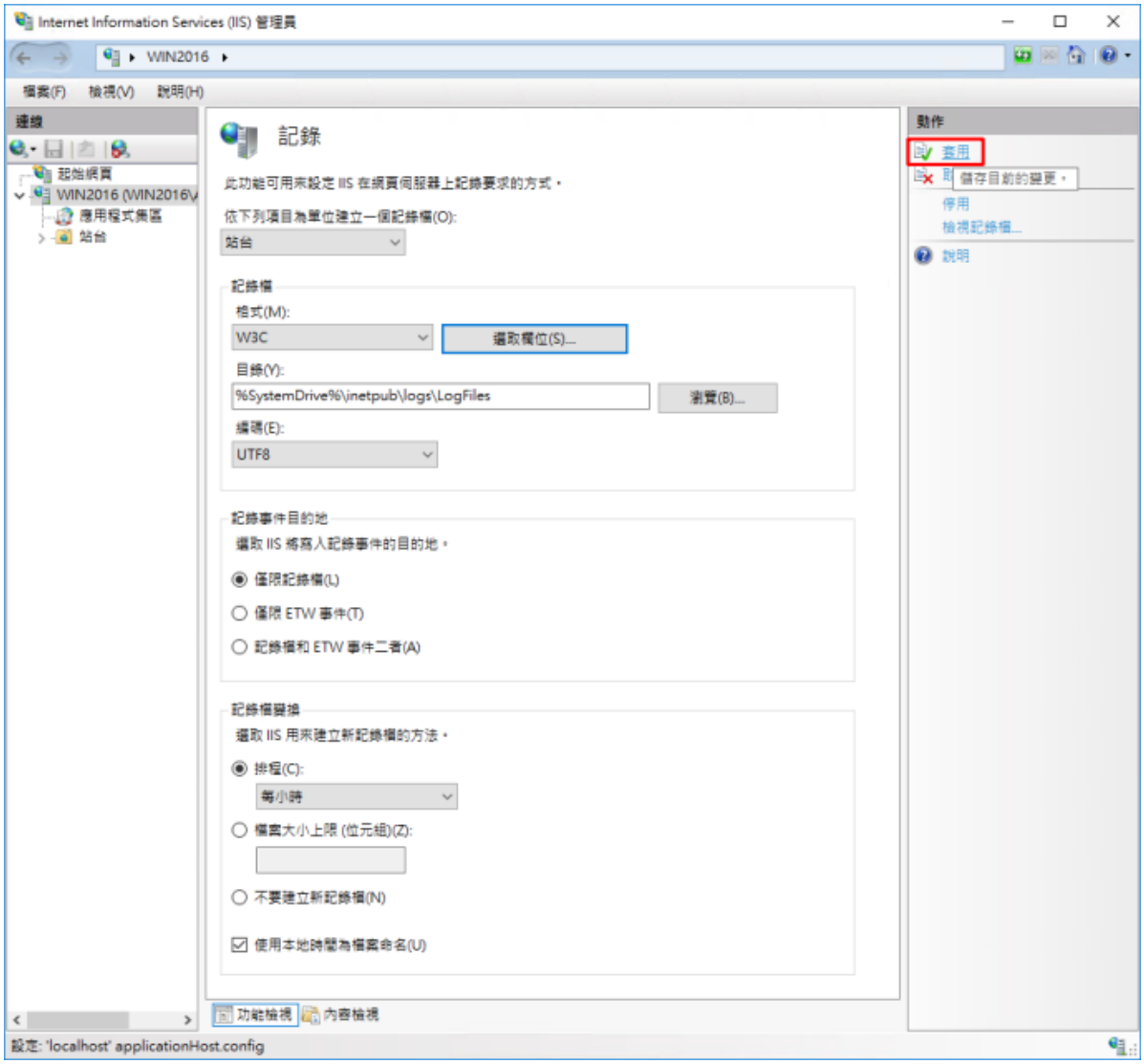
(5) 输入字段名称: `X-Forwarded-For`-> 选择来源类型: **[Request Header(请求头)]** -> 输入来源: `X-Forwarded-For`-> 点击 **[确定]**



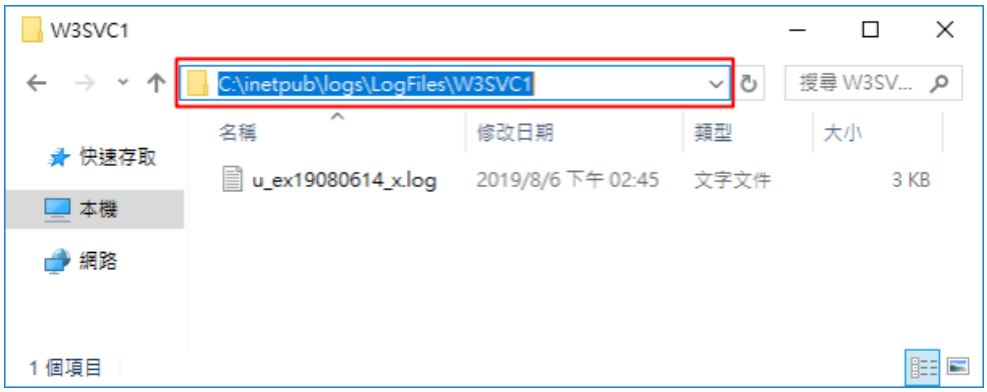
(6) 点击 **[确定]**



(7)　点击 [应用]



(8)　确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹中的 IIS 日志文件: ex*.log

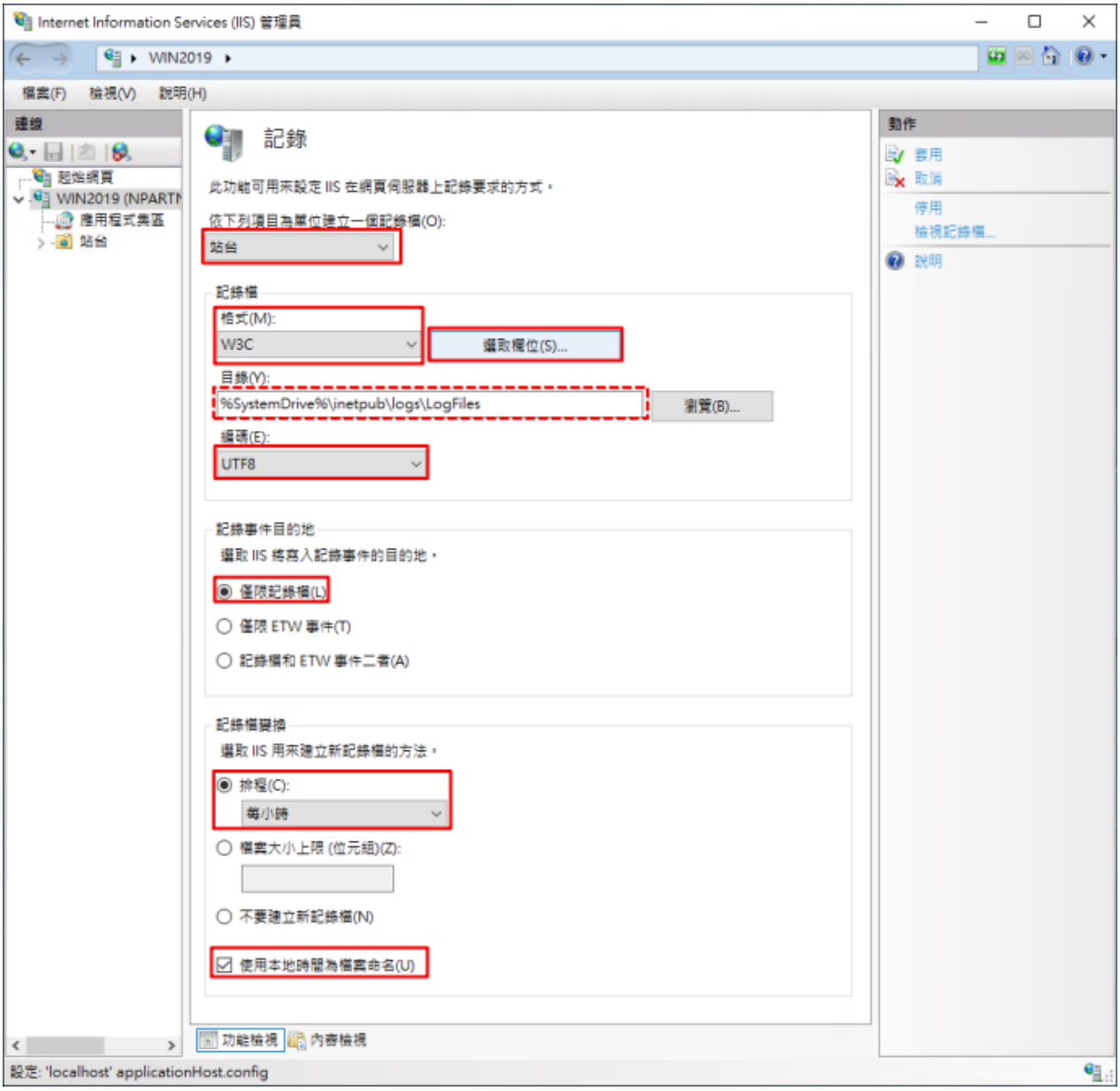


7 Windows 2019

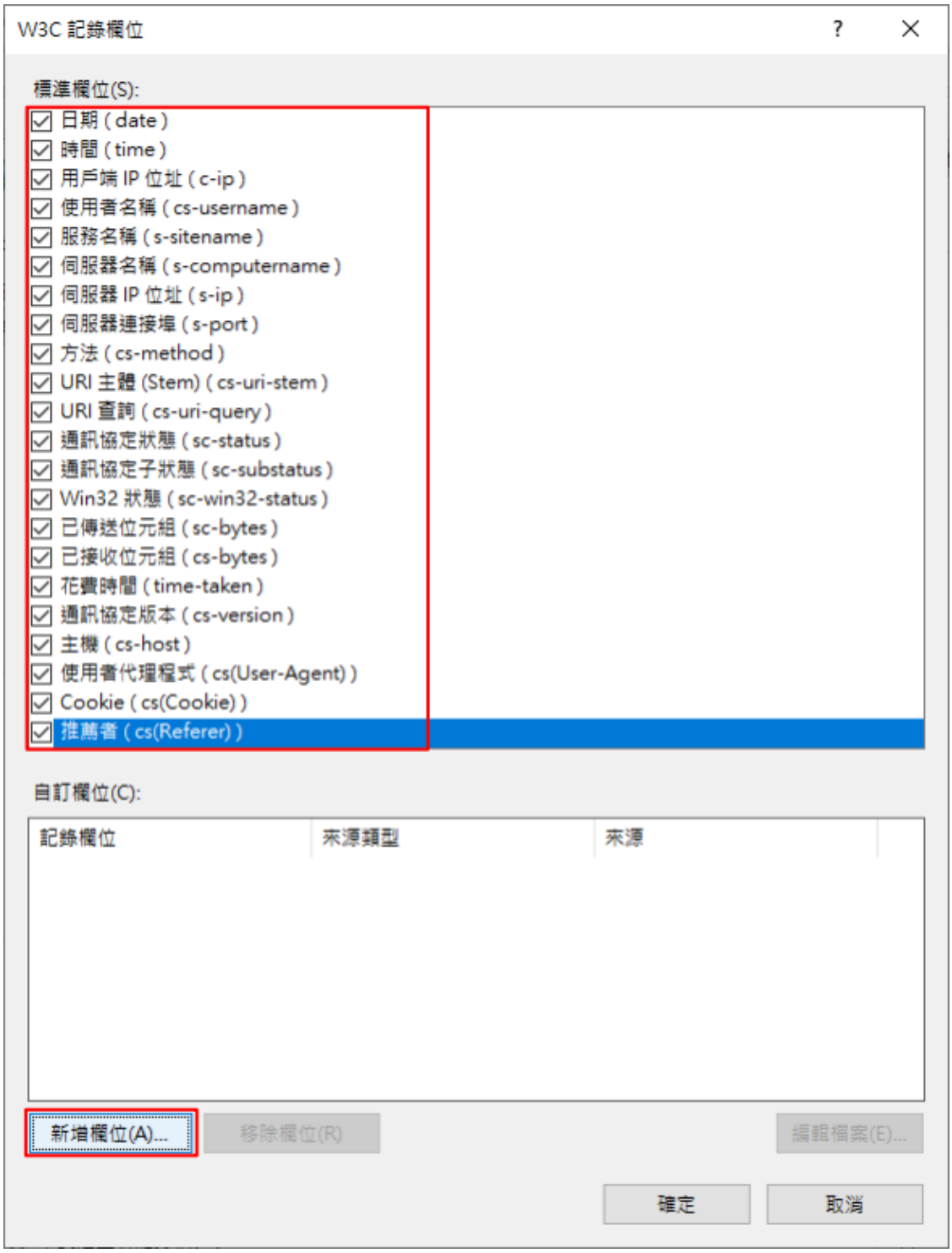
(1) 打开 [互联网信息服务 (IIS) 管理员]

(2) 选择 [IIS 服务器] -> 点击 [日志]

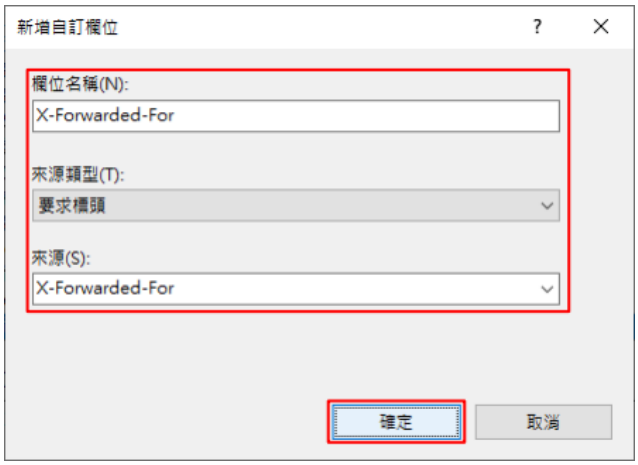
(3) 选择以下项目为单位建立一个日志文件: [站点] -> 日志格式: [W3C] -> 目录: %SystemDrive%\inetpub\logs\LogFiles -> 编码: [UTF-8] -> 日志事件目的地: [仅限日志文件] -> 排程: [每小时] -> 勾选 [使用本地时间为文件命名] -> 点击 [选择字段]



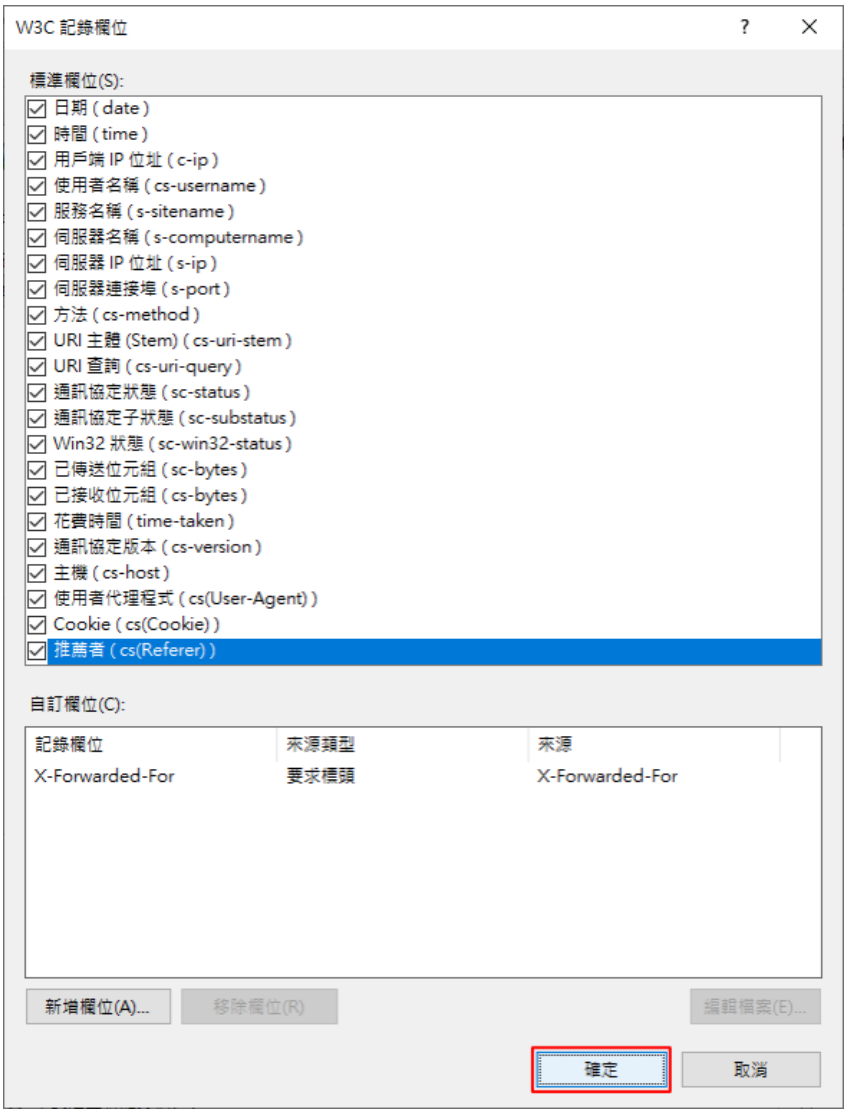
(4) 勾选 [日期 (date)]、[时间 (time)]、[客户端 IP 地址 (c-ip)]、[用户名 (cs-username)]、[服务名称 (s-sitename)]、[服务器名称 (s-computername)]、[服务器 IP 地址 (s-ip)]、[服务器端口 (s-port)]、[方法 (cs-method)]、[URI 主体 (cs-uri-stem)]、[URI 查询 (cs-uri-query)]、[协议状态 (sc-status)]、[协议子状态 (sc-substatus)]、[Win32 状态 (sc-win32-status)]、[发送字节数 (sc-bytes)]、[接收字节数 (cs-bytes)]、[耗时 (time-taken)]、[协议版本 (cs-version)]、[主机 (cs-host)]、[用户代理 (cs(User-Agent))]、[Cookie(cs(Cookie))]、[推荐者 (cs(Referer))] -> 点击 [添加字段]



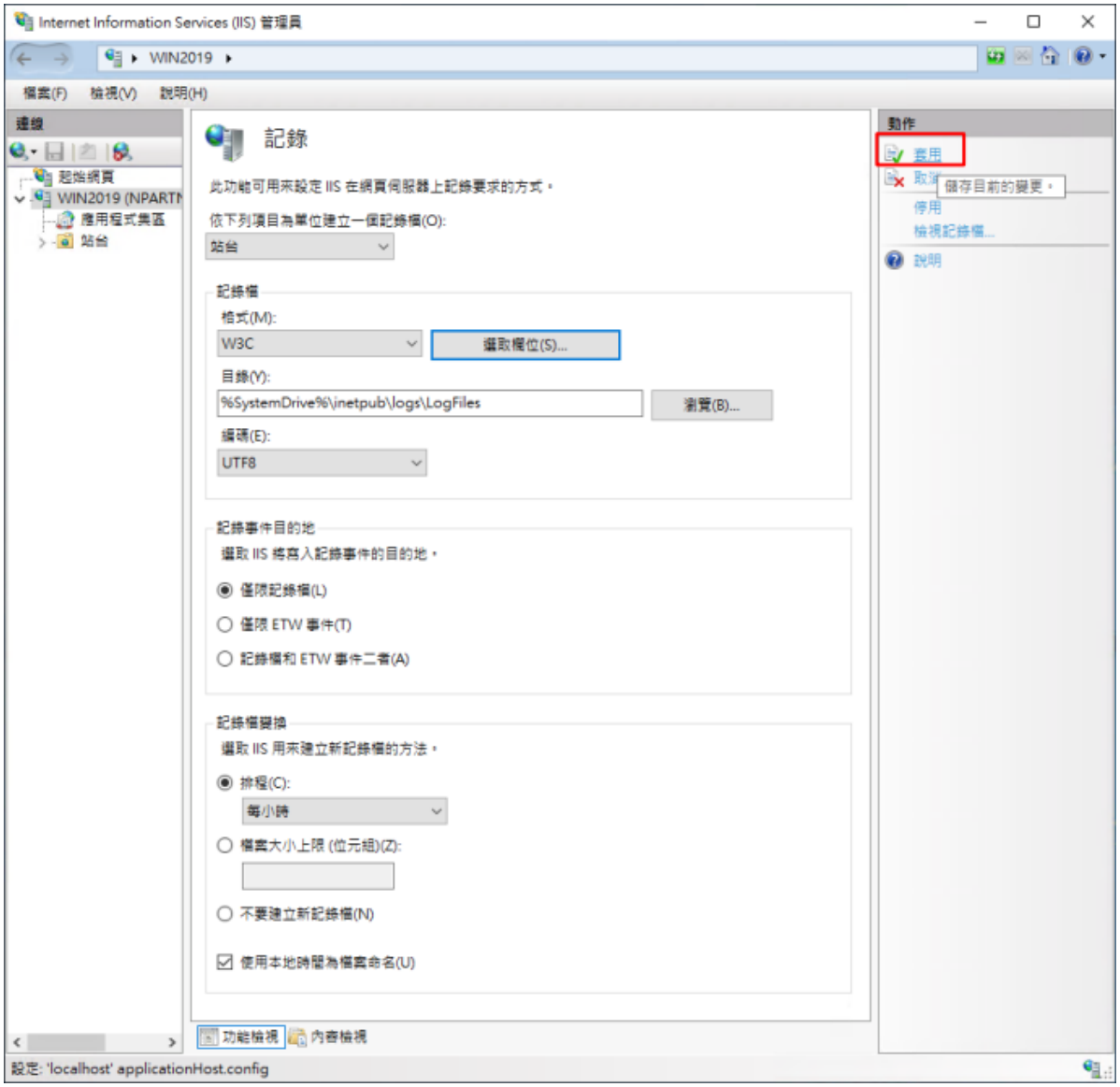
(5) 输入字段名称: `X-Forwarded-For`-> 选择来源类型: **[Request Header(请求头)]** -> 输入来源:: `X-Forwarded-For`-> 按下 **[確定]**



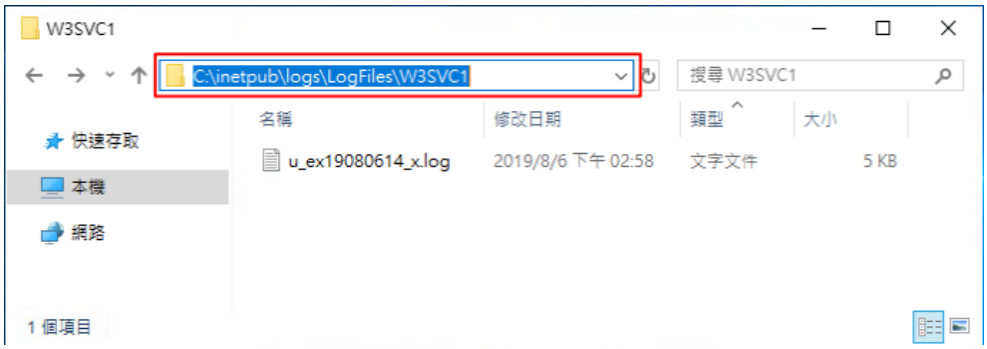
(6) 点击 **[确定]**



(7) 点击 [应用]



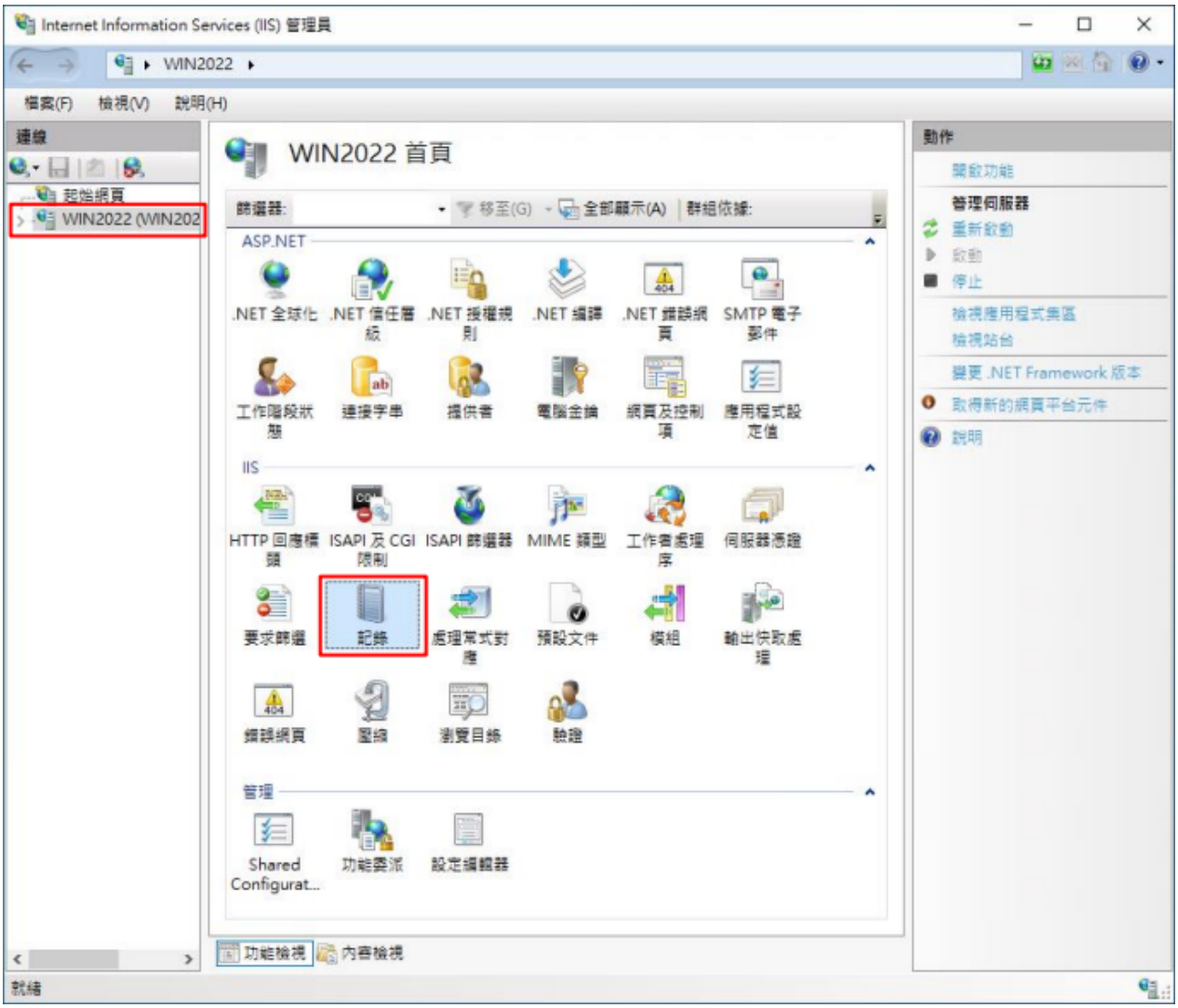
(8) 确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹中的 IIS 日志文件: ex*.log



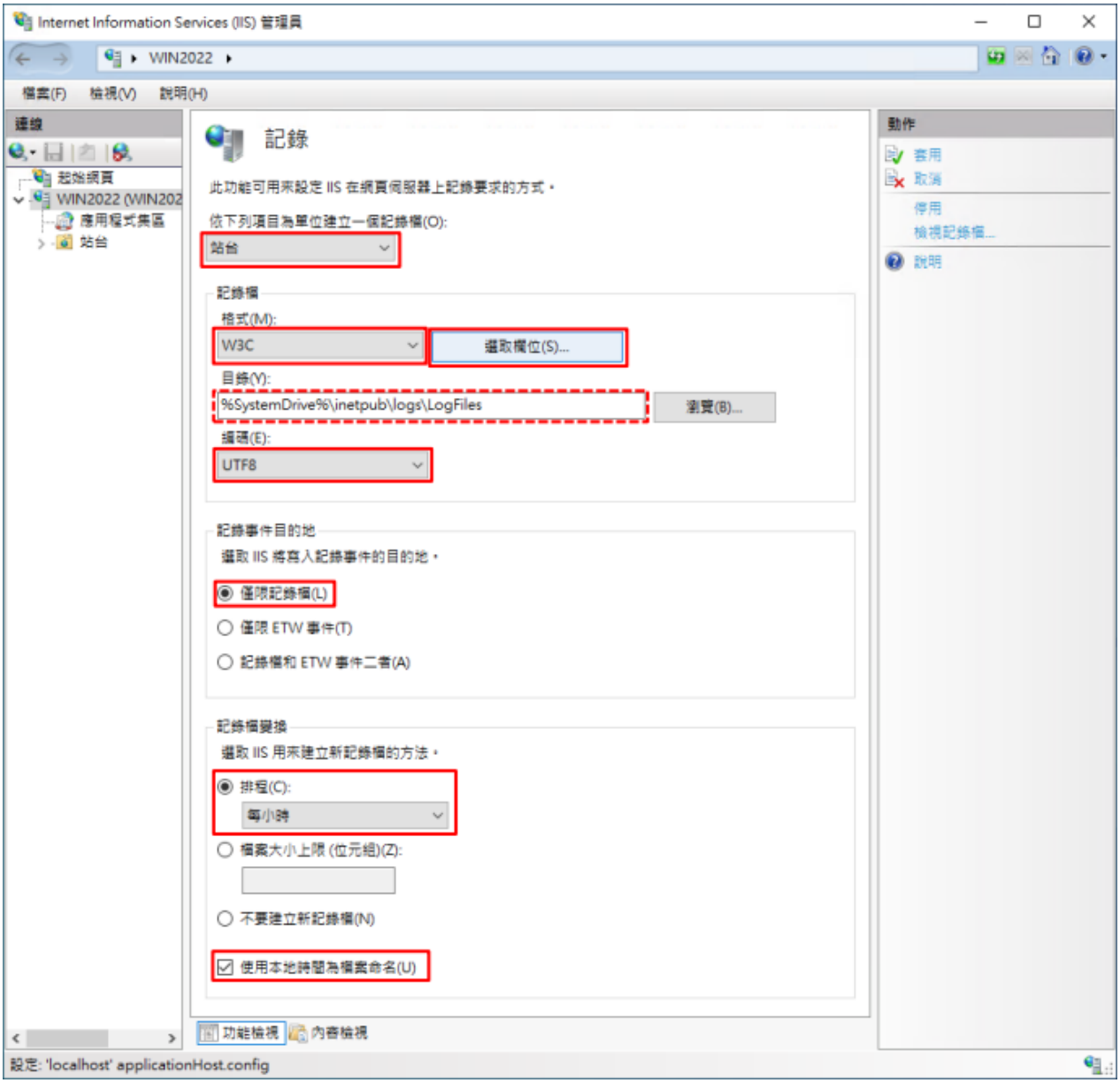
8 Windows 2022

(1) 打开 [互联网信息服务 (IIS) 管理员]

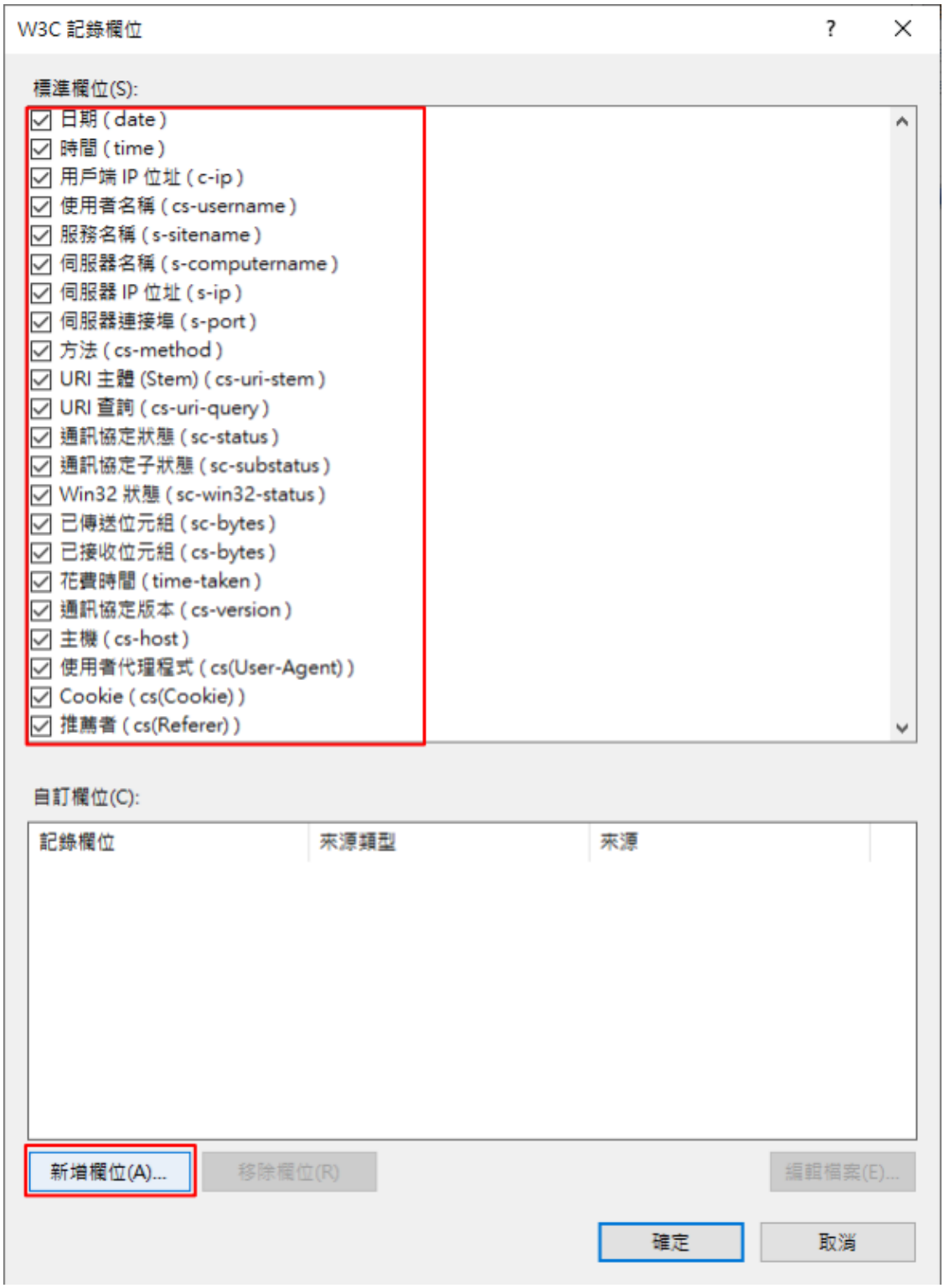
(2) 选择 [IIS 服务器] -> 点击 [日志]



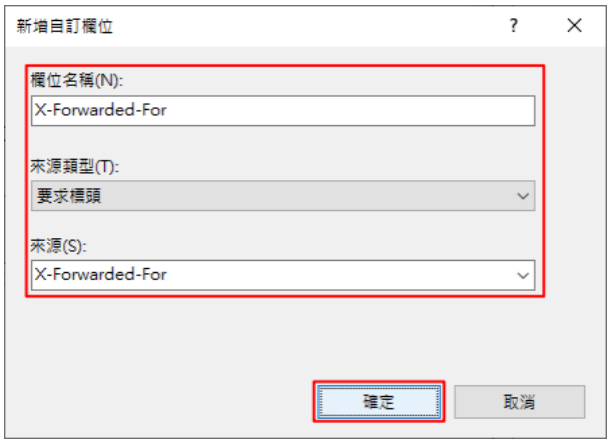
(3) 选择以下项目为单位建立一个日志文件: [站点] -> 日志格式: [W3C] -> 目录: %SystemDrive%\inetpub\logs\LogFiles -> 编码: [UTF-8] -> 日志事件目的地: [仅限日志文件] -> 排程: [每小时] -> 勾选 [使用本地时间为文件命名] -> 点击 [选择字段]



(4) 勾选 **[日期 (date)]**、**[时间 (time)]**、**[客户端 IP 地址 (c-ip)]**、**[用户名 (cs-username)]**、**[服务名称 (s-sitename)]**、**[服务器名称 (s-computername)]**、**[服务器 IP 地址 (s-ip)]**、**[服务器端口 (s-port)]**、**[方法 (cs-method)]**、**[URI 主体 (cs-uri-stem)]**、**[URI 查询 (cs-uri-query)]**、**[协议状态 (sc-status)]**、**[协议子状态 (sc-substatus)]**、**[Win32 状态 (sc-win32-status)]**、**[发送字节数 (sc-bytes)]**、**[接收字节数 (cs-bytes)]**、**[耗时 (time-taken)]**、**[协议版本 (cs-version)]**、**[主机 (cs-host)]**、**[用户代理 (cs(User-Agent))]**、**[Cookie(cs(Cookie))]**、**[推荐者 (cs(Referer))]** **->** 点击 **[添加字段]**

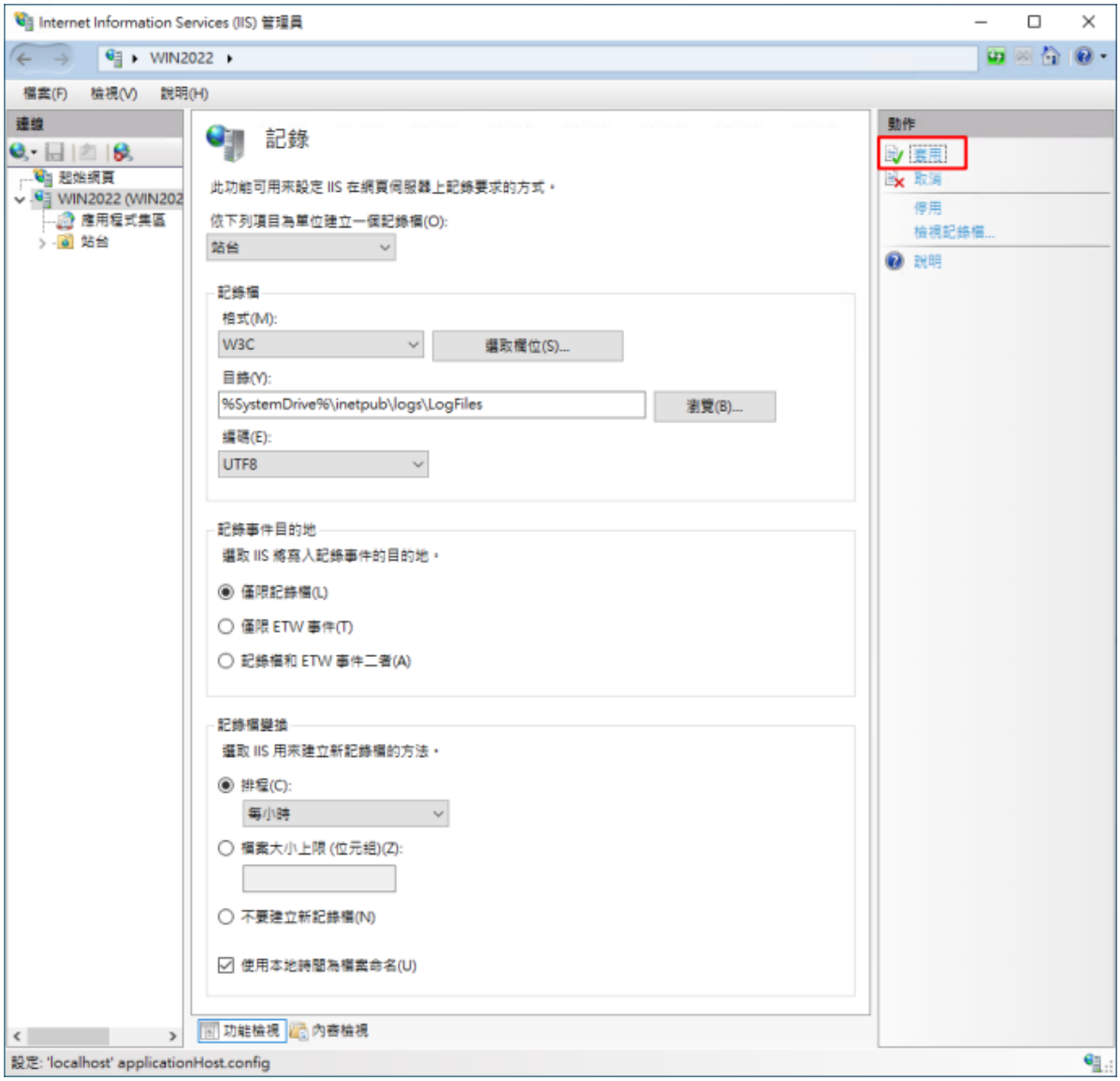


(5) 输入字段名称: `X-Forwarded-For`-> 选择来源类型: **[Request Header(请求头)]** -> 输入来源: `X-Forwarded-For`-> 点击 **[确定]**

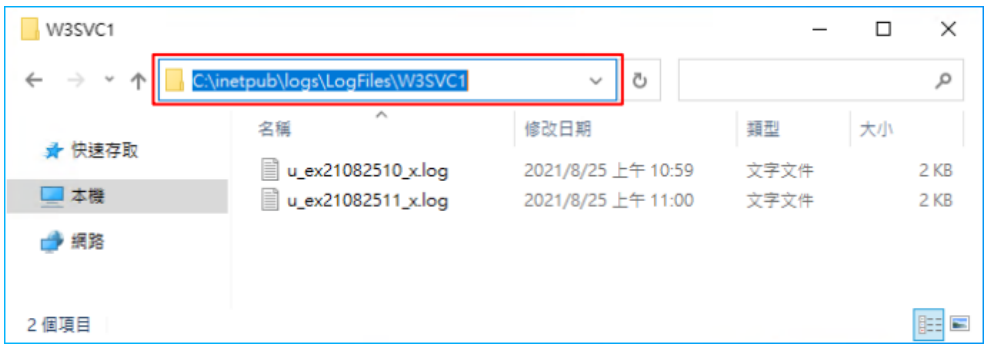


(6) 点击 **[确定]**

(7) 点击 [应用]



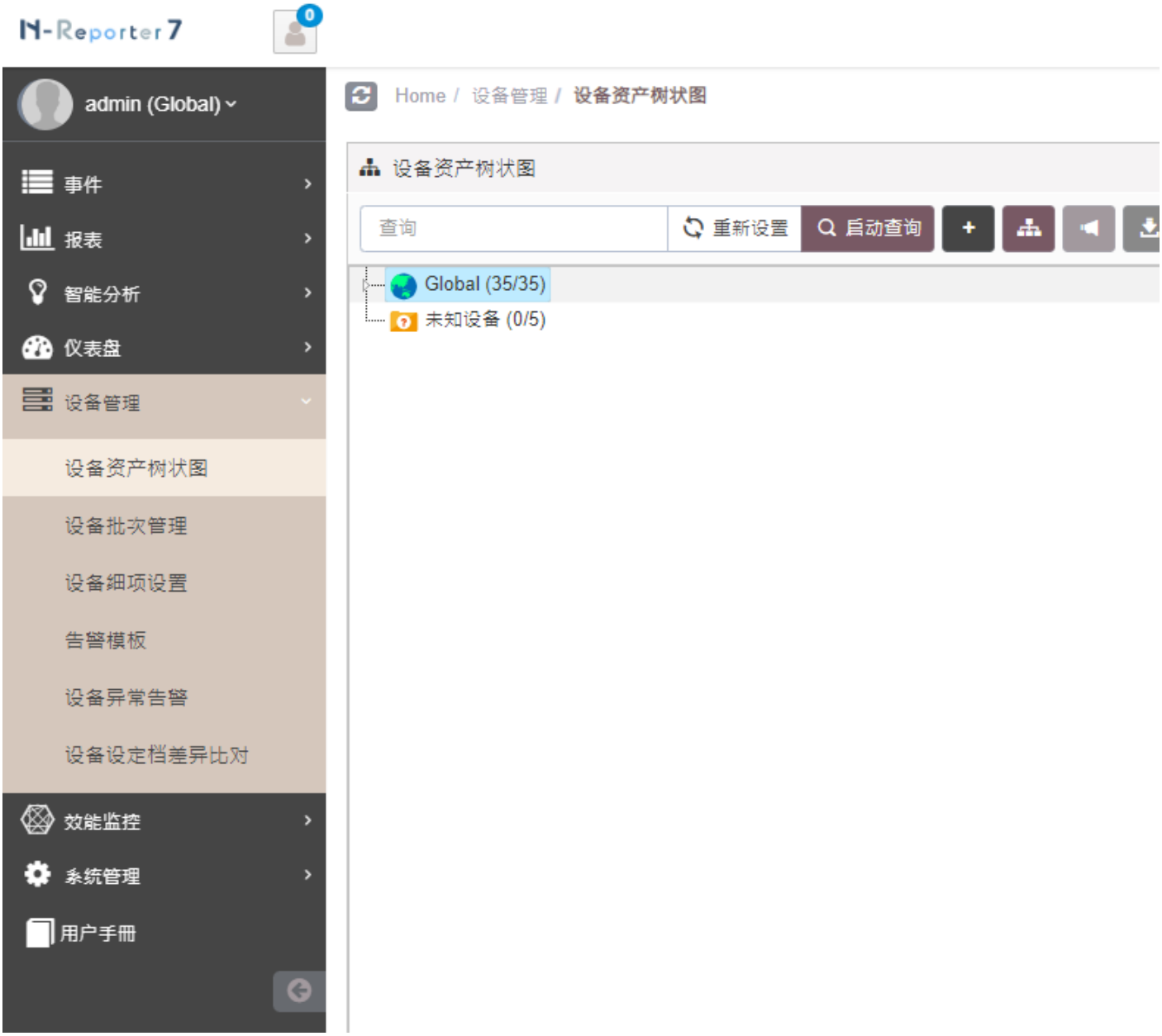
(8) 确认 [C:\Inetpub\logs\LogFiles\W3SVC1] 文件夹中的 IIS 日志文件: ex*.log



9 N-Reporter

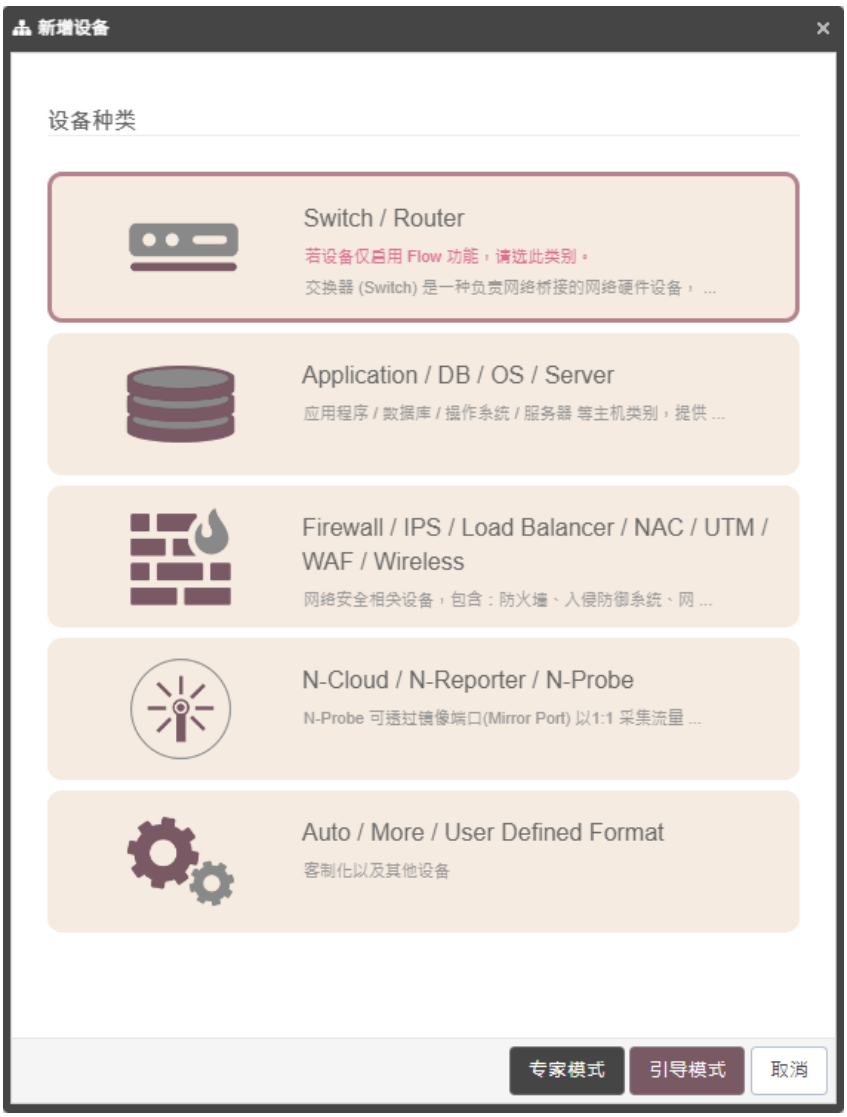
(1) 新增 IIS 设备

[设备管理] -> [设备树状图] -> 点击 [新增]



(2) 选择设备种类

选择 [Application/DB/OS/Server] -> 点击 [引导模式]



(3) 设备基本设置

输入设备名称和IP->Syslog 数据格式选择 [IIS] -> 点击 [下一步]

(4) Syslog 相关设置

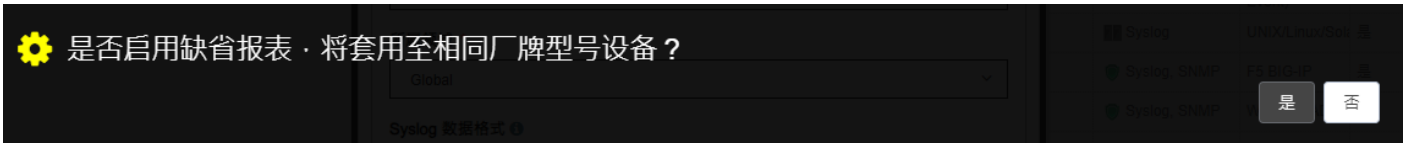
Facility 选择 [(22) local use 6 (local6)] -> 点击 [下一步]

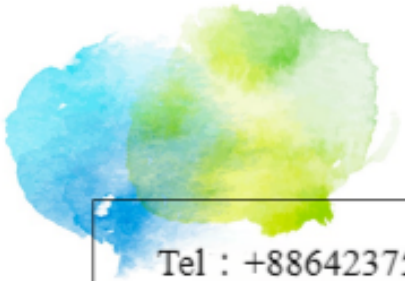
(若勾选 [Raw Data 保留]，则 [事件查询] 显示 Raw Data 信息)

(5) 其他

设备图标选择 [Host] -> 接收状态选择 [启用] -> 点击 [下一步] -> [确认]

是否启用默认报表，将应用至相同品牌型号设备 -> 点击 [否]





Tel：+886423752865　Fax：+886423757458
业务咨询：sales@npartner.com
技术咨询：support@npartner.com