

# 如何設定 Windows IIS log

V022





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。





前	言.		•••••••••••••••••••••••••••••••••••••••	1
1	NXL	og		2
	1.1	NXLog 3	安裝	2
	1.2	NXLog	没定檔下載	6
		1.2.1 V	Vindows 2003 或之前版本作業系統 . (	6
		1.2.2 V	Vindows 2008 或之後版本作業系統 .	7
	1.3	NXLog 言	没定檔	8
		1.3.1 言	己錄所有資訊設定檔	8
		1.3.2 7	下紀錄 Cookie 資訊設定檔	9
	1.4	NXLog	啟動服務 10	0
		1.4.1 V	Vindows 2003 或之前版本作業系統 . 10	0
		1.4.2 V	Vindows 2008 或之後版本作業系統 . 13	3
2	Win	dows 200	0	6
3	Win	dows 200	3	0
4	Win	dows 200	8	7
5	Win	dows 201	2	8
6	Win	dows 201	6	3
7	Win	dows 201	9	8
8	Win	dows 202	2	3
9	N-R	eporter .		8





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的 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



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

點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next ].

🙀 NXLog-CE Setup	
	Welcome to the NXLog-CE Setup Wizard
	The Setup Wizard will install NXLog-CE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel



-> 勾選 [I accept the terms in the License Agreement], 按 [Next].

	NXLOG PUBLIC LICENSE v1.0	
1.	DEFINITIONS	
"Li L	icense" shall mean version 1.0 of the NXLOG PUBLIC ICENSE, i.e. the terms and conditions set forth in this document	
"Se	oftware" shall mean the source code and object code form, all	
as	ssociated media, printed materials, and "online" or electronic	

-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)

NXLog-CE Setup	_ 🗆 🗙
Destination Folder Click Next to install to the default folder or click Change to choose another.	
Install NXLog-CE to:	
C:\Program Files\nxlog\	
Change	
Back Next	Cancel



#### -> 按 [Install].



-> 按 [Finish].





#### <2.2> Windows 2003

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

伊 NXLog-CE Setup	-		×
Ready to install NXLog-CE			X
Click Install to begin the installation. Click Back to review or change ar installation settings. Click Cancel to exit the wizard.	ny of you	r	
Back Install		Cano	el

#### <2.3> Windows 2000

前往 NXLog CE 舊版網址 https://sourceforge.net/projects/nxlog-ce/, 左點 [See All Activity], 下載 NXLOG CE

支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.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 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

#### <2.1> 記錄所有資訊設定檔:

下載連結:http://www.npartner.com/download/tech/nxlog\_WinIIS.conf

#### <2.2> 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:

PS 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:

PS C: <> copy "C: \nxlog\_WinIIS\_no\_cookie.conf" "C: \ Program Files \ \nxlog \conf \nxlog.conf" /y

◎ 命令提示字元	
C:\>copy "C:\nxlog_WinDHCP.conf" "C:\Program Files\nxlog\conf\nxlog.con 複製了     1 個檔案。	nf"∕y ▲
c: \>_	<b>_</b>
	► //.

本文件範例是 64 位元作業系統,若作業系統是 32 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 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

#### <2.1> 記錄所有資訊設定檔:

下載連結:http://www.npartner.com/download/tech/nxlog\_WinIIS.conf

#### <2.2> 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:

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

不紀錄 Cookie 資訊設定檔複製指令:

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

➢ 系統管理員: Windows PowerShell - □ × PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog\_WinDHCP.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf' PS C:\> \_

本文件範例是 64 位元作業系統,若作業系統是 32 位元,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

#### 1.3.1 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_iilog>
     Module
               im_file
              '%IISPath%\u_ex*.log'
     File
     SavePos
                TRUE
     ReadFromLast
                      TRUE
     Recursive
                   TRUE
 </Input>
 <Output out_iislog>
             om_udp
%NCloud%
     Module
     Host
     Port
             514
             $SyslogFacilityValue = 22;
$raw_event = "IIS [Info]: " + $raw_event ;
     Exec
     Exec
             to_syslog_bsd();
     Exec
 </Output>
 <Route dnslog>
     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

藍色文字部分請輸入 IIS 路徑

define IISpath C:\inetpub\logs\LogFiles

修改設定檔內容後需"另存新檔"覆蓋原本檔案 · 1. 存檔類型請選擇"所有檔案 (\*.\*)" · 2. 編碼請選擇"UTF-8"以免編碼錯 誤造成服務無法正常開啟。

檔案名稱(N): nxlog.conf					$\sim$
存榴類型(T): 所有檔案 (*.*) 1	所有檔案 (*.*) 1				
	編碼(E):	ANSI ~	存檔(S)	取消	]
		Unicode <u>Unicode</u> big endian UTF-8 2			



#### 1.3.2 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_iilog>
     Module
               im_file
              '%IISPath%\u_ex*.log'
     File
     SavePos
               TRUE
     ReadFromLast TRUE
                   TRUE
     Recursive
 </Input>
 <Output out_iislog>
     Module
              om udp
             %NCloud%
     Host
             514
     Port
             $SyslogFacilityValue = 22;
     Exec
             $raw_event = "IIS [no_cookie]: " + $raw_event ;
     Exec
             to_syslog_bsd();
     Exec
 </Output>
 <Route dnslog>
     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

藍色文字部分請輸入 IIS 路徑

define IISpath C:\inetpub\logs\LogFiles

修改設定檔內容後需"另存新檔"覆蓋原本檔案·1.存檔類型請選擇"所有檔案 (\*.\*)"·2. 編碼請選擇"UTF-8"以免編碼錯 誤造成服務無法正常開啟。

檔案名稱(N):	nxlog.conf		~
存檔類型(T):	所有檔案 (*.*) 1		~
藏資料夾		編碼(E): ANSI ~ 存植(S) 取 ANSI	消
		Unicode <u>Unicode</u> big endian UTF-8 2	



## 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





(3) 開啟 [服務] 功能





### (4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 🗳 點選 [內容]

<sup>‰</sup> 最務					_ [	X
檔案(E) 執行(A) 檢視(V) 說明(B)	D					
← → 🗷 🚰 🖻 🗟 😫 🖬						
<sup>%</sup> 。 <u>服務</u> (本機) 内容						
nxlog	名稱 △	描述	狀態	啓動類型	登入身分	
	🎨 Network DDE DSDM	訊息動		停用	本機系統	
<u>客動</u> 服務	🏶 Network Location Awa	收集並…	已啓動	手動	本機系統	
	🏶 Network Provisioning	在網域…		手動	本機系統	
+#**	NT LM Security Suppo	爲沒有		手動	本機系統	
/ 抽池: This service is responsible for running the	anxlog 😪	This ser		自動	本機系統	
NXLog agent. See www.nxlog.co.	🏶 Performance Logs and	基於爭…		目動	網路服務	-
	🏶 Plug and Play	啓用電	已啓動	自動	本機系統	
	🍓 Portable Media Serial N	Retrieve		手動	本機系統	-
↓延伸 / 標準 /						

(5) [一般] 頁面 -> 確認; 啟動類型: [自動]

NXLog 內容 (本樹	電路) ? 🗙
一般 登入	修復   依存性
服務名稱:	nxlog
顯示名稱(N):	NXLog
描述( <u>D</u> ):	This service is responsible for running the NXLog agent. See www.nxlog.co.
執行檔所在路徑	( <u>H</u> ):
"C:\Program File	s (x86)\nxlog\nxlog.exe" -c "C:\Program Files (x86)\nxlog
啓動類型(E):	
服務狀態:	己啓動
啓動③	<b>停止(I)</b> 暫停(P) 繼續(R)
您可以在這裡指	定啓動服務時所要套用的參數。
啓動參數( <u>M</u> ):	
	確定 取消 雲用(鱼)



(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]

NXLog 內容 (本機電腦)	? ×
一般 登入 修復 6	· · · · · · · · · · · · · · · · · · ·
如果這項服務執行失敗時,	電腦將採取的回應。
第一次失敗時(上):	重新啓動服務
第二次失敗時(2):	重新啓動服務
後續失敗時(U):	重新啓動服務
重設失敗計數於(0):	0 天之後
重新啓動服務於(型):	1 分鐘之後
-執行程式	
	瀏覽(B)
命令列參數( <u>C</u> ):	
▶ 將失敗計數附加到命	令列結尾(/fail=%1%)(E)
	電腦重新啓動的選項(B)
	( 確定 取消 套用(▲)



#### 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



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'

(3) 開啟 [服務] 功能





### (4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 🗐 點選 [內容]

🤹 服務					_		×	
檔案(F) 動作(A) 檢視(V) 說明(H	ł)							
🗢 🌩 🖃 🖬 🖬 🖬 🖬	▶ <b>■</b> H <b>Ⅰ</b>							
Q 服務 (本機) 内容								
NXLog	名稱 ^	描述	狀態	啟動類型	登入身分		^	
信止服務	Network Location Awareness	收集及儲存	執行中	自動	Network S	Service		
重新啟動服務	Network Setup Service	「網路設定		手動 (觸發程	Local Syst	tem		
	Network Store Interface Service	此服務可將	執行中	自動	Local Sen	vice	_	
	🙀 NXLog	This service	執行中	自動 (延遲啟動)	Local Syst	tem		
	😪 Offline Files	離線檔案服		已停用	Local Syst	tem	_	
This service is responsible for	🥋 OpenSSH Authentication Agent	Agent to h		已停用	Local Syst	System		
www.nxlog.co.	Optimize drives	可最佳化存		手動	Local Syst	tem	~	,
延伸 (標準/								

(5) [一般] 頁面 -> 確認 ; 啟動類型: [自動 (延遲啟動)]

NXLog 内	] 窖 (本機	電腦)		×
一般	登入	復原	相依性	
服務名	稱:	nxlo	9	
顯示名	稱:	NXL	g	
描述:		This age	service is responsible for running th nt. See www.nxlog.co.	e NXLog 🕎
可執行 "C:\Pro	檔所在路 ogram Fi	徑 iles\nxlo	\nxlog.exe" -c "C:\Program Files\nx	klog\conf\nxlog
啟動類	型(E):	自重	(延遲啟動)	~
服務狀	態:	執行	Þ	
10 m	如(S)		停止(T) 暫停(P)	繼續(R)
您可以	在這裡指	定啟動服	務時所要套用的參數。	
啟動參	數(M):	[		
			確定取消	套用(A)



(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	ŧ	
	協助我設定復原動作。	
第二方生即味(口)。	香花动动印改	
第一大大政时(F).	里利取到版務	×
第二次失敗時(S):	重新啟動服務	~
後續失敗時(U):	重新愈動服務	~
經過下列天數後重設失敗計數(0	)): 1	<del>Σ</del>
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 □ 動行程式	り動作・電腦重	「新啟動的選項(R)
程式(P):		
		瀏覽(B)
命令列參數(C):		
□ 將失敗計數附加到命令列	信尾 (/fail=%1%)(E)	
	確定取》	<b>資</b>



# 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



(3) 開啟 [Internet 服務管理員





### (4) 在 [Web 站台] 上按滑鼠右鍵 -> 選擇 [內容]

Service Information Service	
」執行(Δ) 檢視(型) ↓ ←	• →   🛍 🖬   🖶   😫   💂   ▶ =
樹狀目錄	電腦 本機 連線類型 錯誤狀態
Internet Information Service ■ ● * win2000 ■ ● ● 預設的 FTP 站台 ■ ● ● 預設的 Web 站台 ■ ● ● 預設 SMTP 虛擬信 ■ ● ● 預設 SMTP 虛擬信 ■ ● ● 預設 NNTP 虛擬信	■*win2000 是 TCP/IP 查看 開啓舊檔 測野
	停止
	暫停
	新增(11) ▶
	所有工TF(L) 「
[	内容图
	說明( <u>H</u> ) <sup>以</sup>
開啓目前選擇的內容頁。	



(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]

預設的 Web 站台 內容	<u>?</u> ×
目錄安全設定 Web 站台 操作員	HTTP 標題   自訂錯誤   伺服器擴充程式     效能   ISAPI 篩選器   主目錄   文件
Web站台識別碼——	
說明( <u>S</u> ):	預設的 Web 站台
IP 位址(I):	(全未指定) 進階(D)
TCP 連接埠( <u>T</u> ):	80 SSL 連接埠①:
連線	
<ul> <li>○ 沒有限制(U)</li> <li>○ 限制左(A0)</li> </ul>	1.000 症線
連線逾時時間(N):	900 秒
▼ 啓用 HTTP 的持續	查作用( <u>K</u> )
▼ 啓用記錄(匹)	
使用中的日誌格式(	V):
W3C Extended Log	File Format
	確定 取消 套用(点) 説明

- (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]

擴充記錄內容	x
一般內容 擴充內容	
新日誌週期	
○ 毎日①	
○ 毎週(翌)	
○ 毎月(M)	
○ 沒有限制檔案大小(世)	
○ 當檔案大小到達(2):	
19 <u>*</u> MB	
☑ 請使用本地時間爲檔案命名(I)	
日誌檔目錄(L):	
C:\Inetpub\logs\LogFiles 瀏覽(B)	
日誌檔名稱: W3SVC1\exyymmddhh.log	
確定 取消 套用(A) 説明	



(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]

擴充記錄內容	×
一般內容 擴充內容 ]	
☐ / / / / / / / / / / / / / / / / / / /	
<ul> <li>✓ 日期(date)</li> <li>✓ 時間(time)</li> <li>擴充內容</li> <li>✓ 使用者名稱(cs-usemame)</li> <li>✓ 使用者名稱(s-sitename)</li> <li>✓ 伺服器名稱(s-computemame)</li> <li>✓ 伺服器 IP 位址(s-ip)</li> <li>✓ 伺服器 IP 位址(s-ip)</li> <li>✓ 伺服器連接埠(s-port)</li> <li>✓ 方法(cs-method)</li> <li>✓ URI 粗縱線(cs-uri-stem)</li> <li>✓ URI 查詢(cs-uri-query)</li> <li>✓ 通訊協定狀態(sc-status)</li> <li>✓ Win32 狀態(sc-status)</li> <li>✓ 送出的位元組(cs-bytes)</li> <li>✓ 接收到的位元組(cs-bytes)</li> <li>✓ 花費時間(time-taken)</li> <li>✓ 連訊協定版本(cs-version)</li> <li>✓ 主機(cs-host)</li> <li>✓ 使用者代理程式(cs(User-Agent))</li> <li>✓ 推薦者(cs(Referer))</li> </ul>	
確定 取消 套用(A) 説明	

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

🔄 W3SVC1			<u>_                                    </u>
檔案(F) 編輯(E) 檢視(V)	我的最愛(A) 工具(I)	說明(出)	
」 ⇔上一頁 → ⇒ → 🔁 🛛 📿 担	雙尋 🔓 資料夾 🍏 記錄	ε <u>Έ</u> Έ Χ Ω	
」網址① 🔁 C:\Inetpub\logs\LogFi	les\W3SVC1		▼ @移至
	▲ 名稱 △	大小類型	修改日期
₩3SVC1 諸選取一個項目來檢視它的說 明。	≝ ex21082514.log	2 KB 文字文件	2021/8/25 下午 02:26
諸參閱: <u>我的文件</u>	<b>_</b>		
1 個物件		1.05	KB 📃 我的電腦 /



# 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



(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]

₩IN2003 (本機電腦) 內容	? X
網際網路資訊服務	
「 啓用直接 Metabase 編輯 (N)	_
允許您在 IIS 執行時,編輯 IIS Metabase 設定檔。	
_ UTF-8 記錄	_
允許 IIS 使用 UTF-8 編碼代替本機字碼頁來寫入記錄項目。	
✓ 網站記錄用 UTF-8 來編碼(₩)	
MIME 類型 IIS 只服務副檔名有登錄在 MIME 類 型清單裡的檔案。若要設定其他檔 案副檔名,請按 [MIME 類型]。	1

(6) 按下[確定]





(7) 在 [網站] 上按滑鼠右鍵 -> 選擇 [內容]

管 (211) 중温馬斉路降梁降 🗊	星員		
🐚 檔案(E) 執行(A) 檢視(V)	視窗(W) 説明(H)		_ ð ×
⇔ → 🗈 🖬 😭 🖻	- 😰 🖬 💂 🕨 🗉 🗉		
<ul> <li>網際網路資訊服務     <li>→→→ WIN2003 (本機電腦)     <li>●→→→ 應用程式集區     <li>●→→ 額防     </li> </li></li></li></ul>	_描述 ● 預設的網站	<u></u> 識別元 1	<u> </u> 狀態 執行中
⊕ 親貞. 新増(M) 所有工作(K)	* *		
檢視(型) 従這裡新增調	▶ 見窗( <u>W</u> )		
重新整理(F) 匯出清單(L).			
内容(R)			
說明( <u>H</u> )			
	•		Þ
爲目前的選取項目開啓內容對話力	5塊。		

(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]

					?
目錄安全設	定	HTTP 標	頭	自訂錯誤	服務
網站	效能	ISA	IPI 篩選器	主目錄	文件
網站識別碼					
説明(S):	Г				
IP 位址(I):	3	全未指定)		7	進階(D)
TCP 連接埠	co: É		SSL 連接	場(L):	
☑ 啓用 HT	TP 的持續作	乍用(匹)			
✓ 啓用 HI ✓ 啓用 記録 現用的記	TP的持續作 条(E) 錄格式(Y):	乍用(広)			
✓ 啓用 HI ✓ 啓用記録 現用的記 ₩3C 擴3	TP 的持續( 条(E) 錄格式(V): 充記錄檔案	作用 低) 格式		▼ 内容(2)	
✓ 啓用 HI ✓ 啓用記録 現用的記 ₩3C 擴3	TP 的持續作 条(E) 錄格式(V): 充記錄檔案:	格式		▼ []內容(P)	
✓ 啓用 HI ✓ 啓用記録 現用的記 ₩3C 擴き	TP 的持續( 条(E) 錄格式(V): 充記錄檔案;	格式		<ul> <li>内容の</li> </ul>	
✓ 啓用 HI ✓ 啓用記録 現用的記 ₩3C 擴き	TP 的持續( 条(E) 錄格式(V): 充記錄檔案	格式		▼ 内容(P)	
✓ 啓用 HI ● 啓用記録 現用的記 ₩3C 擴き	TP 的持續( 条(E) 錄格式(V): 充記錄檔案	格式		▼ [ 內容(P)	



(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按命名]-> 記錄檔目錄輸入

C:\Inetpub\logs\LogFiles -> 按下 [套用]

記錄內容
一般 進階
新增記錄排程
● 毎小時(出)
○ 毎日(12)
○ 毎月(M)
○ 富福菜大小達到⑥: 20 <u>_</u> MB
☑ 請使用本地時間爲檔案命名(I)
記錄檔目錄(L):
C:\Inetpub\logs\LogFiles 瀏覽(B)
記錄檔名稱: W3SVCX/exyymmddhh.log
<b>確定</b> 取消 套用(A) 説明



(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]

記錄內容	×
一般 進階	
塘安記錄)發頂(V)·	
✓ 日期 (date)	
✓ 時間 (tume) 塘井市空	
「畑田后岩田(広社) (sin)	
□ 休田老々親(	
····································	
────────────────────────────────────	
□ (司服器 IP (☆th. (~in))	
□ (回服器海塔馆 (sup)	
▼ 向版翻建按单(Sport)	
□ IIRI 主體 (co-uri-stern)	
↓ URI 查詢(cs-uri-guery)	
☑ 通訊協定狀態 (sc-status)	
✓ 通訊協定子狀態 (sc-substatus)	
₩in32 狀態 (sc-win32-status)	
■ 傳送的位元組 (sc-bytes)	
✓ 接收的位元組 (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))	•
確定 取消	を田(A)   説明
REAC AXTR	22/11(2) 2/191

(11) 按下 [全選] 和 [確定]

繼承喪寫	×
下列子節點也定義 "LogFileTruncateSize" 內容值,這個內 的值。請從下方的講單中選取應使用新內容值的節點。	容值已覆寫您剛設定
子節點( <u>C</u> ):	
預設的網站	全選囚
1	
確定 取消	



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

💐 C:\Inetpub\logs\LogFiles\₩3S¥C1			
檔案(F) 編輯(E) 檢視(V) 我的最愛	( <u>A</u> ) 工具( <u>T</u> ) 説明( <u>H</u> )		<b></b>
🔇 上一頁 🔹 🜍 🔹 🎓 搜尋 💫	資料夾 🕼 🍛 🗙 🍤	<b></b> -	
網址① 🗁 C.Unetpubliogs/LogFiles/W3SV	7C1		💌 🄁 移至
資料夾 ×	名稱  ▲	大小 類型 修改日期	屬性
<ul> <li> ● 桌面 ● 我的文件 ● 我的電腦 ● 本機磁碟 (C:) ● Documents and Settings ● Inetpub ● AdminScripts ● logs ● LogFiles ● W3SVC1 ● wwwroot ● Program Files </li> </ul>	⊫ u_ex19080617.log	6 KB 文字文件 2019/8/6 下午 05	5:38 A



# 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]

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	Nation Service	es (211) 32	_ <b>_</b> X
<ul> <li>御来(0) 後視(7) 説明(3)</li> <li>● 記録</li> <li>● 正書</li> <li>● 四書</li> <li>●</li></ul>	(3) (1) WIN2008	>	📴 🖂 🟠 I 🔞 🗸
建設       シー       シー <t< td=""><td>檔案(F) 檢視(∀) 說明(H)</td><td></td><td></td></t<>	檔案(F) 檢視(∀) 說明(H)		
說定: localhost applicationHost config	建築       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・       ・     ・	シレント       第二条         此功能可用來說定 IIS 在網頁(伺服器上記錄要求的方式。         (在下列以頁目為單位建立一個記錄欄(0):         (送給         記錄欄         「記錄欄         「「「「」」」」」         「記錄欄         「「「」」」」         「記錄欄         「「「」」」」         「「」」」         「「」」」         「「」「」」」         「「」」」         「「」「」」」」         「記錄欄一         「「」「」」」」」         「「」」」         「「」」」         「「」」」         「「」」」         「「」」」         「」」         「」」         「」」         「」」」         「」」」         「」」」         「」」」         「」」」         「」」」         「」」」         「」」」         「」」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」         「」」	新作         ● 取消         ● 取消         ● 取明         ● 取明 <ul> <li>● 取明</li> <li> </li></ul> ● 取明 <ul> <li>● 取明</li> <li> </li></ul>
	設定: localhost'applicationHost.com	fig	<b>1</b> .:



#### (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]

識別碼	來源名稱	來源類型	類別	標頭名稱 ▲
Win32Status	Win32Status	內建	Default	sc-win32-status
W3WP-PrivateBytes	\Process(w3wp)\Priv	效能計數器	Default	W3WP-PrivateE
UserName	UserName	要求標頭	Default	cs-username
User Agent	User-Agent	要求標頭	Default	cs(User-Agent)
URI-Stem	URI-Stem	內建	Default	cs-uri-stem
URI-Querystring	URI-Querystring	內建	Default	cs-uri-query 👘
Time-UTC	Time-UTC	內建	Default	time
Time-Local	Time-Local	內建	Default	time-local
Time Taken	Time-Taken	內建	Default	Time TakenMS
Substatus	Substatus	內建	Default	sc-substatus
Status	Status	內建	Default	sc-status
Site Name	SiteName	內建	Default	s-sitename
Server-IP	Server-IP	內建	Default	s-ip
Server Port	ServerPort	內建	Default	s-port 🚬
				•
新婚期(行位)	和除化	1	编辑欄位化	1



- (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]

新増記錄欄位	? ×
欄位識別碼(F):	
X-Forwarded-For	
類別(C):	
Default	
來源類型(T):	
要求標頭	
來源名稱(N):	
X-Forwarded-For	
双形計数器與型(I).	
」	<u> </u>
顯示進階內容	
	<b>確定</b> 取消

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

Nation Serve	ices (IIS) 管理員	
(3) (1) WIN2008	•	🖸 🖂 🟠 I 🕡 🔹
檔案(F) 檢視(V) 說明(H)		
建築         ●       記知台網頁         ●       認知台         ●       通知台         ●       通知台	Yumma Advanced Logging         (集用這個功能可以建立並管理記錄定義、(用以指定要記錄哪些伺服器端和用戶 端記錄欄位),以及設定其他記錄設定。         評組依違: 沒有分組         全種         全職         Accomputername%s         已啟用         尔COMPUTERNAME%s         日啟用         第COMPUTERNAME%s         日啟用         小         小         ●         <	<ul> <li>◆ Advanced Logging 功能已停用。</li> <li>新增記錄定義</li> <li>股用 Advanced Logging</li> <li>股用用戶端記錄</li> <li>編輯記錄目錄</li> <li>檢視記錄檔</li> <li>說明</li> <li>錄上說明</li> </ul>
設定: localhost applicationHost.co	onfig	•1.:



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



#### (12) 點選 [新增記錄定義]

Nation Service	es (11) 管理員	
(3) (1) WIN2008	>	😐 🖂 i 🛛 🕶
檔案(F) 檢視(V) 說明(H)		
建築	Advanced Logging         使用這個功能可以建立並管理記錄定錄 (用以指定要記錄哪些伺服器端和用戶端記錄欄位),以及設定其他記錄設定。         群組依據: 沒有分組         名稱        已啟用         名稱        已啟用         冬COMPUTERNAME%-Server       日停用	<ul> <li>動作</li> <li><u>新増記錄定義</u></li> <li>編輯記錄定義</li> <li>※ 移除記錄定義</li> <li>政用記錄定義</li> <li>複製記錄定義</li> <li>停用 Advanced Logging</li> <li>停用用戶端記錄</li> <li>編輯記錄欄位</li> <li>編輯記錄相算</li> <li>檢視記錄檔</li> <li>② 說明</li> <li>線上說明</li> </ul>
設定: localhost'applicationHost.com	ĩig	<b>€</b> <u>1</u> .:



(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]

警Internet Information Services (IIS) 管理員	
(3) (3) + WIN2008 +	🖸 🖂 🔂 I 🚱 🔹
槛案(F) 檢視(V) 說明(H)	
	<ul> <li>新作</li> <li>● 液消</li> <li>液消記録欄</li> <li>● 返回 Advanced Logging</li> <li>● 説明 論上說明</li> </ul>
37.56	<b>N</b> .:



(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)] \ [TimeTaken(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]

#### 遻

<b>秋記登欄位</b>				?
野绀(赤燥(雪)、   精明		ſ		
		( -+	( ##Du	1 JEEE 10 102
識別碼 D-4	米源名稱	米源類型	類別	標頭名稱   ▲
Delault				
✓ X-Forwarded-For	X-Forwarded-For	要求標頭	Default	
✓ Win32Status	Win32Status	內建	Default	sc-win32-status
W3WP-PrivateBytes	Process(w3wp)Priv	. 效能計數器	Default	W3WP-PrivateE
✓ UserName	UserName	要求標頭	Default	cs-username
🗸 User Agent	User-Agent	要求標頭	Default	cs(User-Agent)
🗸 URI-Stem	URI-Stem	內建	Default	cs-uri-stem
<ul> <li>URI-Querystring</li> </ul>	URI-Querystring	內建	Default	cs-uri-query
Time-UTC	Time-UTC	內建	Default	time
✓ Time-Local	Time-Local	內建	Default	time-local
✔ Time Taken	Time-Taken	內建	Default	Time TakenMS
🗸 Substatus	Substatus	內建	Default	sc-substatus
✓ Status	Status	內建	Default	sc-status
✔ Site Name	SiteName	內建	Default	s-sitename
Server-IP	Server-IP	內建	Default	s-ip
Server Port	ServerPort	內建	Default	s-port
Server Name	ServerName	內建	Default	s-computername
RequestsPerSecond	\W3SVC_W3WP(_T	效能計數器	Default	RequestsPerSecc
✔ Referer	Referer	要求標頭	Default	cs(Referer)
Proxy	Via	要求標頭	Default	s-proxy
Protocol Version	ProtocolVersion	內建	Default	cs-version
Protocol	Protocol	內建	Default	c-protocol
✓ Method	Method	內建	Default	cs-method
✓ Host	Host	要求標頭	Default	cs(Host)
EndRequest-UTC	EndRequest-UTC	棋組	Default	EndRequest-UT
Date-UTC	Date-UTC	內建	Default	date
🗸 Date-Local	Date-Local	內建	Default	date-local
CPU-Utilization	\Processor(_Total)\%.	效能計數器	Default	CPU-Utilization
🗸 Cookie	Cookie	要求標頭	Default	cs(Cookie)
ContentPath	ContentPath	內建	Default	s-contentpath
✓ Client-IP	Client-IP	內建	Default	c-ip
🗸 Bytes Sent	BytesSent	棋組	Default	sc-bytes
<ul> <li>Bytes Received</li> </ul>	BytesReceived	棋組	Default	cs-bytes
BeginRequest-UTC	BeginRequest-UTC	棋組	Default	BeginRequest-U
(				
			確定	取消



(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(csuri-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(scstatus)]、[Substatus(sc-substatus)]
[Win32Status(sc-win32-status)]、[Bytes Send(sc-bytes)]、[Bytes Received(csbytes)]、[Time Taken(TimeTakenMS)]、
[X-Forwarded-For] -> 按下 [套用]





#### (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



(21) 點選 [重新啟動] IIS 服務

Nation Servic	es (IIS) 管理員			
(3) (1) WIN2008	•			🖸 🖂 🔂 🖬
檔案(F) 檢視(∀) 說明(H)				
連線         ● <th>WIN2008 首引         翻選器:         IIS         Advanced Logging       HITP 回應標 明         要求範選       記錄         範出快取處       編誤網頁         管理       資金派         功能發派       其用設定</th> <th><ul> <li>● ●●移至(G) - ●●全部</li> <li>●●●を部</li> <li>●●●を部</li> <li>●●●●の</li> <li>●●●●●の</li> <li>●●●●●の</li> <li>●●●●●●の</li> <li>●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●</li></ul></th> <th>鎮示(A)  </th> <th><ul> <li>         bread (1)         bread</li></ul></th>	WIN2008 首引         翻選器:         IIS         Advanced Logging       HITP 回應標 明         要求範選       記錄         範出快取處       編誤網頁         管理       資金派         功能發派       其用設定	<ul> <li>● ●●移至(G) - ●●全部</li> <li>●●●を部</li> <li>●●●を部</li> <li>●●●●の</li> <li>●●●●●の</li> <li>●●●●●の</li> <li>●●●●●●の</li> <li>●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●●</li> <li>●●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●●●●●●●●●●●●●</li> <li>●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●</li></ul>	鎮示(A)	<ul> <li>         bread (1)         bread</li></ul>
就绪				¶ <u>1</u> .:

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

🕌 AdvancedLogs						
00 💵	\inetpub\logs\AdvancedLogs		<b>▼</b> 🐓	搜尋 Advan	cedLogs	2
組合管理 ▼ 加	□入至媒體櫃 ▼ 共用對象	▼ 新増資料夾			-	0
☆ 我的最愛	名稱 🔺	修i	改日期	類型	大小	
🥽 媒體櫃	📄 u_ex_H20190806-0914	41942.log 201	19/8/6 下午 05:19 []	文字文件	51 KB	
📕 電腦						
👊 網路						



# 5 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]

<b>v</b> 1	Internet Information Services (IIS) 管理員	_ <b>D</b> X
🕞 💽 📲 🕨 WIN2012	•	🖬 🖬 🟠 🔞 •
檔案(F) 检視(V) 説明(H)		
福寫(F) 檢視(V) 說明(H)       連總       ●・□       ● 認知得買       ● WIN2012 (WIN2012V)       ● 通知規式集區       ● 通知台	記録           此功能可用未敢在 IIS 在線貫 伺服器上記錄要求的方式。           水丁····································	動作         ●       数第         使用       後規記締編         ●       説明
設定: 'localhost' applicationHo	st.config	91.d



(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)]

	W30	C 記錄欄位		? X
標準欄位(S): ✓ 日期(date) ✓ 時間(time) ✓ 時間(time) ✓ 用戶端 IP 位址(c-ip) ✓ 使用者名稱(cs-username) ✓ 使用者名稱(s-computername) ✓ 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-steme) ✓ URI 查詢(cs-uri-query) ✓ 通訊協定狀態(sc-substatue) ✓ 通訊協定光態(sc-substatue) ✓ 通訊協定光態(sc-substatue) ✓ 三傳送位元組(sc-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-Agenetic of the statue)) ✓ 非萬者(cs(Referer)) 自訂欄位(C):	ee) )) s);) ent))		本语	
■L 30K11萬 12 新増欄位(A) 移除欄位	小标频坐 (R)		確定	編輯檔案(E) 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->

新増自訂欄位	?	x
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]

<u> </u>	W3C 記	錄欄位	? X
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) ♥ 個服器名稱(s-computername) ♥ 伺服器名稱(s-computername) ♥ 伺服器理境(s-computername) ♥ 伺服器連境場(s-computername) ♥ 切配基題(sc-method) ♥ URI 主體(Stem)(cs-uri-steme) ♥ URI 查詢(cs-uri-query) ♥ 通訊協定狀趣(sc-status) ♥ 通訊協定狀趣(sc-status) ♥ 通訊協定狀趣(sc-substatus) ♥ 已接收位元組(cs-bytes) ♥ 已接收位元組(cs-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-Age ♥ Cookie(cs(Cookie)) ♥ 推薦者(cs(Referer)) 自訂欄位(C):	ee) ) s) ent))		
記録欄1辺 X-Forwarded-For	米源頻型 要求標頭	米源 X-Forwarded-For	
新増欄位(A) 移除欄位	(R)	種定	編輯檔案(E) 取満



(7) 按下[套用]

●         ●	<b>v</b> 1	Internet Information Services (IIS) 管理員	_ <b>D</b> X
雪菜(含) 後視(?) 登場(?)         雪菜(含) 後視(?) (MN2012)         ● ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	🕞 🕤 📲 🕨 WIN 201	2 •	📅 🖂 🔂 🕡 •
	檔案(F) 檢視(V) 說明(H	)	
< Ⅲ > Image: Section Host.config Image: Sectio	福室(F) 檢視(V) 說明(H)       遵確       ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	記録           此助範可用來設定 IIS 在網頁伺服器上記錄要求的方式。           位下列項目為單位建立一個記錄欄(O):           防衛           常年           程式(M):           V3C           2           記錄幅           程式(M):           V3C           運動價位(S)           目錄(Y):           %SsystemDrive%\inetpub\logs\LogFiles           增養(E):           UTF-8           V           超數 IIS 終高入記錄事件的目的地。           @ 儀限記錄幅(L)           @ 儀限記錄幅(L)           @ 儀限記錄幅(L)           @ 儀限記錄幅(L)           @ 猛眼 ETW 事件二看(A)           記錄幅和 ETW 事件二看(A)           記錄幅和 ETW 事件二看(A)           ①           @ 旗號 US 用來建立新記錄幅的方法。           @ 旗號 US 用來建立新記錄幅的方法。           @ 講主, 小上限 (位元祖)(2):           []           []           @ 梁建立新記錄幅(N)           []           @ 《四本並說是編	數作 ☆ 室田 保用 始視記詩編 ② 説明
設走: 'localhost' applicationHost.config	S III	🔝 功能檢視 💦 內容檢視	
	設定: 'localhost' applicationH	ost.config	<b>9</b> 1.:

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





# 6 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]

Internet Information Servi	ces (IIS) 管理員	– 🗆 X
← → ♥ WIN2010	5 <b>•</b>	📅 🔤 🏠 🔞 •
福霖(F) 檢視(V) 說明(H)		
建設 ● ● ● ② 認知保育 ● ○ ○ 認知保育 ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	記録         此功能可用未設定 IIS 在規貫伺服器上記錄要求的方式。         佐丁列項目為單位建立一個記錄幅(0):         防告         「記錄幅         培式(M):         「「「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「「」」         「」         「」         「」         「「」         「」         「」         「」         「「」         「「」         「「         「「         「         「         「         「         「         「         「         「         「         「         「         「         「         「         「         「         「         「         「	對作         ● 取消         例用         他視記錄欄         ● 說明
設定: 'localhost' applicationHo	ost.config	¶1.:



(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 (csuri-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 (scwin32-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 (csversion)]、[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		?	Х
標準欄位(S):			
<ul> <li>✓ 日期(date)</li> <li>✓ 時間(time)</li> <li>✓ 用戶端IP位址(c-ip)</li> <li>✓ 使用者名稱(cs-username)</li> <li>✓ 使用者名稱(s-computername)</li> <li>✓ 伺服器名稱(s-computername)</li> <li>✓ 伺服器連接埠(s-port)</li> <li>✓ 伺服器連接埠(s-port)</li> <li>✓ 方法(cs-method)</li> <li>✓ URI 主體(Stem)(cs-uri-stem)</li> <li>✓ URI 查詢(cs-uri-query)</li> <li>✓ 通訊協定狀態(sc-status)</li> <li>✓ 通訊協定子狀態(sc-substatus)</li> <li>✓ Win32 狀態(sc-substatus)</li> <li>✓ 已接收位元組(cs-bytes)</li> <li>✓ 花費時間(time-taken)</li> <li>✓ 通訊協定版本(cs-version)</li> <li>✓ 主機(cs-host)</li> <li>✓ 使用者代理程式(cs(User-Agent))</li> <li>✓ Cookie(cs(Cookie))</li> <li>✓ 推薦者(cs(Referer))</li> </ul>			
記錄欄位 來源類型	來源		
新増欄位(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]
```

f増自訂欄位	?	×
擱位之稱(N)-		
X-Forwarded-For		
來須類刑(口)-		
要求標頭	~	
來源(S):		
X-Forwarded-For	~	

### (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)				
✓ 何服器石碑 (s-computernam)	ne)			
✓ 何服務建接焊 (s-port)				
☑ JPL 十階 (Storm) (cc. uri storm	.)			
☑ URI 查詢 (cs-uri-queny)	1)			
☑ 通訊協定狀態(sc-status)				
☑ 通訊協定/// 2 (sc-substatu	(2)			
☑ Win32 狀態 (sc-win32-statu	s)			
☑ 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-Ag	ent))			
🗹 Cookie ( cs(Cookie) )				
✓ 推薦者 (cs(Referer))				
記錄欄位	來源類型	來源		
X-Forwarded-For	要求櫄頭	X-Forwarded-For		
新増欄位(A)	7(R)	4		F)
The second secon				
			T-NV	
		罐定	取消	



(7) 按下[套用]

🐚 Internet Information Servic	es (IIS) 管理員	– 🗆 X
← → ♥ WIN2016	•	📅 🖂 🔂 🕢 -
福興(F) 檢視(V) 說明(H)		
<ul> <li>編集(F) 被視(V) 説明(H)</li> <li>建線</li> <li>● 2 0.</li> <li>● 2006(頁)</li> <li>● 2006(월)</li> <li>● 2006(B)</li> <li>● 2006(B)</li></ul>	・          ・            ・ <td< td=""><td>動作         ● 室田         ● 田         ● 田         ● 説用</td></td<>	動作         ● 室田         ● 田         ● 田         ● 説用
	Thirtida 🕞 Azadda	
<ul> <li>設定: 'localhost' applicationHost</li> </ul>	Line where an one leads a start at the	€a.,
and the appression of the	3	1.:

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

W3SVC1				- C	ı x
$\leftarrow \rightarrow \cdot \uparrow$	C:\inetpub\logs\LogFiles\	C:\inetpub\logs\LogFiles\W3SVC1 ~		搜尋 W3	<b>م</b> رV2
J. 他进方面		修改日期	類型	大小	
× ⊡∞≊1+4X	u_ex19080614_x.log	2019/8/6 下午 02:45	文字文件		3 KB
🔤 本機					
💣 網路					
1 個項目					



# 7 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]

🍓 Internet Information Services (IIS) 管理員	– 🗆 X
← →  ♥ WIN2019 >	📅 🖂 🔂 🖌 🐻 🗸
欄業(F) 檢視(V) 說明(H)	
記録編集         記録線           ● ごおき編集         近期地可用用現金で加り一個記録東回(0):           ● 運動用空式異面         注册場           ● 注册場         「「「」」」」」           ● 注册場         「「」」」」           ● 注册場         「「」」」」           ● 空間記録場()         「」」」           ● 空間記録         「」」」           ● 空間記録場         ● 「」」           ● 空間記録場         ● 「」」           ● 空間記録場         ● 「」」           ● 空間記録場         ● 「」」           ● 理想 ITV 事件(1)         ● 記録場 電話記録 一           ● ご読録量         ● 「」」           ● 理想 ITV 事件(1)         ● 記録場           ● 記録         ● 「」           ● 理想 ITV 事件(1)         ● 記録場 報告           ● 評場(0):         ● 」           ● 評場(1):         ● 」           ● 評場(2):         ● 」           ● 評場(1):         ● 」           ● 評場(1):         ● 」           ● 評場(1):         ● 」           ● 評場 (1):         ● 」           ● 評場 (1):         ● 」           ● 理想 1:         ● 」           ● 「         ● 」           ● 「         ● 」           ● 「         ● 」           ● ご知 (1):         ● 」           ●	<ul> <li>勤作</li> <li>● 歌用</li> <li>● 取消</li> <li>使用</li> <li>检視記錄幅</li> <li>● 説明</li> </ul>
設定: 'localhost' applicationHost.config	<b>1</b> .:



(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 (csuri-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 (scwin32-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 (csversion)]、[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) ○ 月戶端IP位址(c-ip) ○ 使用者名稱(cs-username) ○ 使用者名稱(s-sitename) ○ 伺服器名稱(s-computername) ○ 伺服器2A稱(s-computername) ○ 伺服器連接埠(s-port) ○ 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) ○ Win32 狀態(sc-status) ○ 过 通訊協定所態(sc-substatus) ○ Vin32 狀態(sc-win32-status) ○ 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))			
目訂欄位(C): 記錄欄位	來源		
新増欄位(A) 移除欄位(R)	確定	編輯檔案() 取消	E)



(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]
```

<sup>,</sup> 增自訂欄位	?	$\times$
塑在空锤/40.		
佩亚者佛(N): X-Eonwarded-Eor		
X-roiwaided-roi		
來源類型(T):		
要求槽頭	~	
來源(S):		
X-Forwarded-For	~	

#### (6) 按下[確定]

W3C 記錄欄位			?	×
迺准鋼(h)(C)-				
(県4年(開)业(S):				
✓ 日期 (date)				
✓ 時間(time)				
↓ 使用者名稱 (cs-username)				
✓ 服務名構 (s-sitename)				
✓ 伺服器名稱 (s-computernan)	ne)			
✓ 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-sten	n)			
☑ URI 查詢 (cs-uri-query)				
☑ 通訊協定狀態 (sc-status)				
☑ 通訊協定子狀態 (sc-substatu	us )			
☑ Win32 狀態 (sc-win32-statu	s)			
☑ 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-Ag	ent))			
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		
新瑁欄位(A) 移除欄位	2(R)	3E		)
		確定	取消	
		L		



(7) 按下[套用]

・         ・         ●	●         ●		鞜 Internet Information Services (IIS) 管理員	– 🗆 X
個性(小) 20時(小) 20時(小)   正規編   ● 20時(第)   ● 20年(1)   ● 20年(1)	(重要) 始現() 数理() (第) (NART) (第) 記録 (第) 記録 (第) 記録 (年) 記録 (日) 記録 <	第五代の 社場(小) 社場(小) 第五代の 社場(中) 第五代の 日本(小) 第二代の日本(小) 第二代の日本(小	← →  ♥ WIN2019 >	😐 🖂 🚱 •
連載       記録         ● 以後の目の「NPART」       小町可用来設定 IIS 在網頁伺服器上記錄要求的方式。         ● 小町福安式美国区       小町可用来設定 IIS 在網頁伺服器上記錄要求的方式。         ● 小町福安式 美国       小町町 中田東山田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	建理         記録:         正:         正:         : <th:< td=""><td>●       ●</td><td>欄案(F) 檢視(∀) 說明(H)</td><td></td></th:<>	●       ●	欄案(F) 檢視(∀) 說明(H)	
<ul> <li>● 排径(U):</li> <li>● 排径(U):</li> <li>● 榴繁大小上限(位元組)(Z):</li> <li>● 不要建立新記錄懂(N)</li> <li>● 不要建立新記錄懂(N)</li> <li>● 使用本地時閣為檔案命名(U)</li> </ul>			単型         記録           ● 記録:(第二 ● 取時項目 ● 注册:(第二 ● 注册:(第二 ● 注册:(第二 ● 注册:(第二 ● 注册:(第二 ● 注册:(第二))))         記録:(第二 ● 記録:(第二)))           ● 記録:(第二 ● 記録:(第二))         「記録:(第二))           ● 記録:(第二) ● 記録:(第二))         「記録:(第二))           ● 記録:(第二) ● 記録:(第二))         「記録:(第二))           ● 記録:(第二))         「記録:(第二))           ● 記録:(第二))         ● 注册:(第二))           ● 記録:(第二))         ● 記録:(第二))           ● 記録:(第二))         ● 記録:(第1))           ● 記録:(第1))         ● 記録:(第1))           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])           ● [1])         ● [1])	<ul> <li>勤作</li> <li>○ 整用</li> <li>④用</li> <li>检視記錄欄</li> <li>② 説明</li> </ul>
★ 回 功能檢視 續 內麥檢視		段定: 'localhost' applicationHost.config	設定: 'localhost' applicationHost.config	• <u>1</u> .:
		유문: 'localhost' applicationHost.config	< > /// // // // // // // // // // // //	Q2

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

W3SVC1				-		х
$\leftarrow \rightarrow \cdot \uparrow$	C:\inetpub\logs\LogFiles\W3SVC1	~ ت	搜尋 W3SVC1	1		<i>م</i>
	名稱	修改日期	<u>類型</u> ^	大小		
★ 法迷仔权	u_ex19080614_x.log	2019/8/6 下午 02:58	文字文件		5 KB	
🔜 本機						
🧁 網路						
1 個項目						



# 8 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 (csuri-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 (scwin32-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 (csversion)]、[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):                 ● 時間(time)                  夕 時間(time)                 夕 用戶端IP位址(c-ip)                 使用者名稱(cs-username)                 ⑦ 一周股器名稱(s-sitename)                 ⑦ 一周股器名稱(s-computername)                 ⑦ 一周股器名稱(s-computername)                 ⑦ 一周股器連接埠(s-port)                 ⑦ 一周股器連接埠(s-port)                 ⑦ 一周股器連接埠(s-port)                 ⑦ 一周股器連接埠(s-port)                 ⑦ 一周股器連接埠(s-port)                 ⑦ 一周服器連接埠(s-port)                 ⑦ 一周服器連接埠(s-substatus)                 ⑦ URI 査詢(cs-uri-query)                 ⑦ 通訊協定状態(sc-status)                 ⑦ 通訊協定大態(sc-win32-status)                 ⑦ 一一個送位元組(sc-bytes)                 ⑦ 一一一一一一一一一一一一一一一一一一一一一一一一		~
自訂欄位(C): 記錄欄位 來源類型 來源		
新増欄位(A) 移除欄位(R) 確定	編輯檔案(E) 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]
----	------

	?	×
/////////////////////////////////////		
X-Forwarded-For		
來源類型(T)·		
要求標頭	~	
來源(S):		
X-Forwarded-For	~	

### (6) 按下[確定]

W3C 記錄欄位			?	×
/ · · · · · · · · · · · · · · · · · · ·				
信/年間1型(3).				
☑ 時間 (time)				
☑ 用戶端 IP 位址 (c-in)				
☑ 佈田者名稱 (cs-usernam	e)			
✓ 使用音音读(cs-username)				
☑ 伺服器名稱 (s-compute	mame)			
☑ 伺服器 IP 位址 (s-in)	manie )			
☑ 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	)			
	status )			
☑ Win32 狀態 (sc-win32-s	tatus )			
☑ 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-versio	n)			
☑ 主機 (cs-host)				
✓ 使用者代理程式 (cs(User)	r-Agent) )			
Cookie ( cs(Cookie) )				
✓ 推薦者 (cs(Referer))				$\checkmark$
自訂欄位(C):				
記錄欄位	來源類型	來源		
X-Forwarded-For	要求櫄頭	X-Forwarded-For		
+*112100 (L. (A)		2	=+= #= #= /	
新瑁欄位(A) 移向	(俺位(尺)	2		E)
		]ia ⇔	HT NH	
		理人上	<b>用X //用</b>	



(7) 按下[套用]

National Information Services (IIS) 管理員	– 🗆 X
← →  ♥ WIN2022	🚥 🖂 🟠 🔞 •
檔案(F) 檢視(V) 說明(H)	
連盟         記録           ● 建用程式集區         ● 世路編           ● 使用程式集區         ● 世路編           ● 使用程式集區         ● 世路編           ● 使用程式集區         ● 世路編           ● 使用電式集區         ● 世路編           ● 使用電式集區         ● 世路編           ● 使用電話錄幅(1)         ● 個限記錄圖(1)           ● 個限記錄圖(1)         ● 個限記錄圖           ● 個限記錄圖         ● 健康已報           ● 個限記錄圖         ● ● 個限記錄圖           ● 個限記錄圖         ● ● 個限記錄圖           ● 個限記錄圖         ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
R.A. Iocainost applicationPlost.config	

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

W3SVC1			_		×
· 🔶 -> -> 🕆 📙 🖾	netpub\logs\LogFiles\W3SVC1	ٽ ~			<i>م</i>
2. 仲法方际	名稱 ^	修改日期	類型	大小	
	u_ex21082510_x.log	2021/8/25 上午 10:59	文字文件		2 KB
本機	u_ex21082511_x.log	2021/8/25 上午 11:00	文字文件		2 KB
🥔 網路					
2 個項目					



# 9 N-Reporter

(1) 新增 IIS 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]





#### (2) 選擇設備種類

# 選擇 [Application/DB/OS/Server]-> 點選 [引導模式]

# \$	<b>听</b> 增設備		×
	設備種類		
		Switch / Router 若設備僅設用 Flow 功能, 請選此類別。 交換器 (Switch) 是一種負責網路構接的網路硬體設備,	
		Application / DB / OS / Server 應用程式 / 資料庫 / 作業系統 / 伺服器 等主機類別,提供	
		Firewall / IPS / Load Balancer / NAC / UTM / WAF / Wireless 網路安全相關設備,包含:防火牆、入侵防禦糸統、網	
		N-Cloud / N-Reporter / N-Probe NCloud 與 NReporter 可轉發系統所收到的 Syslog。 N	
	<b>O</b> o	Auto / More / User Defined Format 客制化以及其他設備	
		專家模式 引導模式 取消	



### (3) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [IIS]-> 點選 [下一步]

設備基本設定	
設備名稱 *	
WinIIS-192.168.8.195	
P *	
192.168.8.195	
所屬領域 *	
Global	~
Syslog 資料格式 ❶	
IIS	~
自定義資料格式 🕄 🕇 🕇	
未愈用	
SNMP Model ()	
未愈用	~
Web 監控 🕄	
愈用網頁監控功能	



(4) Syslog 相關設定

Facility 選擇 [(22) local use 6 (local6)]-> 點選 [下一步]

(若勾選 [Raw Data 保留] · 則 [事件查詢] 顯示 Raw Data 資訊)

盀 新増設備 - Sy	alog 相關設定						×
Syslog 相關	制設定					^	
Facility 6							
(22) local	use 6 (local6)					~	
編碼方式							
UTF-8						~	
Syslog 正規	化資料保留天	數上限 🚯					
Raw Data	R留與轉發						
▼ Raw Da	NTA 保留 於分時監控報表	版動 Syslog 轉發	痔,採用 Raw I	Data 格式			
轉發方:	式將使用來源設	。 備的 IP					
							ļ
			1				1
				上一步	下一步	取消	



### (5) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

新増設備 - 其	ġ						>
其它						^	
設備 Icon							
Host						~	
接收狀態							
● 啟用	◯ 停用						
經緯度		_					
緯度		經度					
				上一步	下一步	取消	

是否啟用預設報表,將套用置相同廠牌型號設備-> 點擊 [否]





