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

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]

i NXLog-CE Setup	_		×
Ready to install NXLog-CE			N
Click Install to begin the installation. Click Back to review or change a installation settings. Click Cancel to exit the wizard.	ny of you	r	
Back Install		Cano	cel

(3) 下載並覆蓋 NXLog 設定檔

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

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

2	Administrator: Windows PowerShell	_		×	
PS PS	C:\Users\Administrator\Downloads> Copy-Item nxlog_WinIIS.conf 'C:\Program Files (x86)\nxlog\conf\n> C:\Users\Administrator\Downloads> _	log.	conf'		Ŷ
۲				>	





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=""></extension>
Module xm_syslog
For Microsoft IIS(Internet Information Server) log file use the following:
<input in_iislog=""/>

Module	im_file
File	'%BASEDIR%\u_ex*.log'
SavePos	TRUE
ReadFromLa	ast TRUE

Recursive TRUE

</Input>

<Output out_iislog>

Module	om_udp
Host	%NCloud%
Port	514
Exec	\$SyslogFacilityValue = 22;
Exec	<pre>\$raw_event = "IIS [info]: " + \$raw_event</pre>



Exec	to_syslog_bsd();
<route iislog=""></route>	
Path	in_iislog => out_iislog

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

🚬 Adm	inistrator: Windows Pow	erShell			_		Х	
Windows Copyrigh	PowerShell t (C) 2016 Microsof	ft Corporation.	All rights reserved.					^
PS C:\Us PS C:\Us	ers\Administrator> ers\Administrator>	Start-Service Get-Service nx	nxlog log					
Status	Name	DisplayName						
Running	nxlog	nxlog						
PS C:\Us 2019-03- PS C:\Us	ers\Administrator> 25 16:08:01 INFO n ers\Administrator>	Get-Content (log-ce-2.10.21	:\Program Files (x86) 50 started	\nxlog\d	lata\nx	log.log)'	*
<							>	:



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]

WIN2003 (本機電腦) 內容	? ×
網際網路資訊服務	
「 啓用直接 Metabase 編輯 M) 允許您在 IIS 執行時,編輯 IIS Metabase 設定檔。	
└UTF-8 記錄 九許 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(W)	
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,諸按 [MIME 類型]。	

(4) 按下 [確定]







C:\> mkdir C:\Inetpub\logs\LogFiles

C:\> dir C:\Inetpub\logs

Ŭ

📾 命令提示字元	_ 🗆 🗡
Microsoft Windows [版本 5.2.3790] <c> 版權所有 1985-2003 Microsoft Corp。</c>	
C:\Documents and Settings\Administrator>mkdir C:\inetpub\logs\LogFiles	
C:\Documents and Settings\Administrator>dir C:\inetpub\logs 磁碟區 C 中的磁碟沒有標籤。 磁碟區序號: D8B8-879B	
C:\inetpub\logs 的目錄	
2019/03/27 下午 02:12 〈DIR〉 .	
2019/03/27 卞午 02:12 〈DIR〉	
2019/03/27 下午 02:12 〈DIR〉 LogFiles	
0 個檔案 0 位元組 3 個目錄 81,343,418,368 位元組可用	
C:\Documents and Settings\Administrator>_	

(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]

目線安全設 網站	定	HTTP 樗	展現 ADI 25:35-92	自訂錯	誤	服務
- 393-1194-115年。	义肥	15.	AFI師进菇		土日嫁	214
- 新可平古最大可以も 説明(S):	Г					
IP 位址①:	G	È未指定)			-	進階(D)
TCP 連接埠	(D): [SSL 連接	埠(正): [
座線迴時時 ▼ 啓用 HT	間(N): TP的持續作	₣用(ᡌ)	120 秒			
· 建称型时时 ▼ 啓用 HT - ▼ 啓用記録 - 日 田的記録	間(M): TP的持續作 象医) 等核式(M):	₱用(<u>K</u>)	120 秒			
 ▲線週時時 ▼ 啓用 HT ▼ 啓用記録 現用的記録 ₩3C 擴考 	間(M): TP 的持續(⁴ 象(E) 錄格式(V): 光記錄檔案(F用(<u>K</u>) 容式	120 秒	T	<u>]容(P)</u>	
座線過時時 ▼ 啓用 HT ▼ 啓用記録 現用的記 ₩3C 擴列	間(L): TP 的持續([/] 泉(E)	F用(K) 格式	120 秒]容(Ľ)	
座線過時時 ▼ 啓用 HT ▼ 啓用記録 現用的記 ₩3C 擴き	間(N): TP 的持續([/] 象(E) 錄格式(V): 記錄檔案(F用(K) 各式	120 秒]容(<u>P</u>)	
座線過時時 ▼ 啓用 HT ▼ 啓用記録 現用的記 ₩3C 擴き	間(N): TP 的持續([/] 承巴 錄格式(V): ^依 記錄檔案(F用(<u>K</u>) 各式	120 秒		<u>1780)</u>	Trut
座線過時時 ▼ 啓用 HT - ▼ 啓用記録 現用的記 W3C 擴き	間(IL): TP 的持續([/] 承(E)	F用(<u>K</u>) 啓式	120 秒		9容(P)	

(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

記錄內容	×
一般進階	
新增記錄排程 毎小時(出) 毎日(1) 毎周(1) 毎月(1) 沒有限制檔案大小(1) 當檔案大小達到(2): 	
▶ 請使用本地時間為備乗叩省(L) 記錄##日報点)	
C.'Inetpub/logs/LogFiles 瀏覽(B)	
記錄檔名稱: W3SVCX/exyymmddhh.log	
(確定) 取消 套用(A) 説明	

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(csusername)]、[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(scstatus)]、[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]

2巻承喪寫 ×
下列子節點也定義 "LogFileTruncateSize" 內容值,這個內容值已覆寫您剛設定 的值。請從下方的清單中選取應使用新內容值的節點。
子節點(<u>C</u>): 預設的網站
確定 取消

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

😂 C:\Inetpub\logs\LogFiles\₩3S¥C	1					!	□×
檔案(F) 編輯(E) 檢視(V) 我的最	逶(A) 工具(I) 說明(H)					R
③ 上─頁 • ③ • ▶ 搜尋	> 資	料夾 🕼 🌛 🗙 🍤					
網址D) C:\Inetpub\logs\LogFiles\W3	SVC1	I				- 🔁	移至
資料夾 2	×	名稱 ▲	大小 🎽	領型	修改日期	屬性	
 ◎ 点面	ъГ	🗐 u_ex19080617.log	6 KB 호	文字文件	2019/8/6 下午 05:38	A	
■ 🔒 我的文件							
🖂 🕎 我的電腦							
🖻 🥪 本機磁碟 (C:)							
표 🛅 Documents and Settings							
🖃 🧰 Inetpub							
🛅 AdminScripts							
🗆 🗀 logs							
🖃 🚞 LogFiles							
🗁 W3SVC1							
🛅 www.root							
🕀 🛅 Program Files	-						





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













(7) 按下[編輯記錄欄位]







(8) 按下 [新增欄位]

辑記錄欄位 群組依據(G): 沒有分組				?)
識別碼	·	 來源類型		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 💌
•				
新増欄位(A)…	移除(R)		編輯欄位(E)	,
			確定	取消

(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	
)迷度	
	確定 取消





(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]

Nation Service	es (IIS) 管理員	
G S № WIN2008	>	🖸 🖬 🖬 🖉 🕶
檔案(F) 檢視(∀) 說明(H)		
建築 ● ●	Advanced Logging 使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。 群組依據: 沒有分組 名種 日取用 ※COMPUTERNAME%-Server 日散用	 勤作 新增記錄定義 編輯記錄定義 冬除記錄定義 夜用記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 編輯記錄欄位 織戰記錄欄 說明 線上說明
設定: 'localhost' applicationHost.con	fig	4 .:

(11) 點選 [新增記錄定義]

Ne Internet Information Services (IIS) 管理員	
	🗾 🖸 🖂 🚹 I 🛛 🕶
檔案(F) 檢視(V) 說明(H)	
建築 Advanced Logging ● ●	 勤作 新增記錄定義 編輯記錄定義 移除記錄定義 啟用記錄定義 複製記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 編輯記錄欄位 續輯記錄欄 說明 線上說明
設定: localhost'applicationHost.config	Sec. 1





(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]

National Information Services (IIS) 管理員	
	🔛 🖂 🚹 I 😢 🕶
檔案(F) 檢視(V) 說明(H)	
TAKE () 1990 TAKE	 新作 東川 取消 検視記錄檔 返回 Advanced Logging 說明 線上說明
就緒	• 1 .:





(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]

1	T	2.7	22		
臸.	Ы.	Ξ.	垂	10	14
	_	_			_

? ×

畿別碼	來源名稱	來源類型	類別	標頭名稱
Default				
✓ 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
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
Z Time Taken	Time-Taken	內建	Default	Time TakenMS
🛛 Substatus	Substatus	內建	Default	sc-substatus
Z Status	Status	內建	Default	sc-status
Z 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	RequestsPerSeco
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
Z 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
Z 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
Bytes Received	BytesReceived	棋組	Default	cs-bytes
BeginRequest-UTC	BeginRequest-UTC	棋組	Default	BeginRequest-U
	- 			-
1				





(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 Send(sc-bytes)]、[Bytes Received(cs-bytes)]、[Time Taken(TimeTakenMS)]、[X-Forwarded-For]-> 按下[套]





(15) 點選 [編輯記錄目錄]

😝 Internet Information Services (IIS) 管理員	
	🖸 🖂 🏠 I 🕐 👻
檔案(F) 檢視(V) 說明(H)	
建築 ● ● ● <td< td=""><td> 勤作 新增記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 兪視記錄檔 값明 線上說明 </td></td<>	 勤作 新增記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 兪視記錄檔 값明 線上說明
設定: localhost' applicationHost.config	¶.:

(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

🕌 AdvancedLogs					_	
00 💵	\inetpub\logs\AdvancedLogs		-	▶ 搜尋 Advar	ncedLogs	2
組合管理 ▼ 加	1入至媒體櫃 🔻 共用對象	▼ 新增資料	4夾		· ·	(?)
🚖 我的最愛	名稱 ▲		修改日期	類型	大小	
;;; 媒體櫃	📋 u_ex_H20190806-09144	41942.log	2019/8/6 下午 05:19	文字文件	51 KB	
📜 電腦						
👊 網路						





4. Windows 2012

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



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



Copyright © All rights are reserved by N-Partner Technologies Co



(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)]

Internet Information Services (IIS) 管理員	_ D X
€ • WIN2012 >	😰 🛛 🏠 🔞 🗸
檔案(F) 檢視(∀) 說明(H)	
正式(*) [*]	F 客用 取消 停用 檢視記錄稿< 說明
REAL: localnost applicationHost.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(ssitename)]、[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(csmethod)]、[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		? X
種進欄位(S)∙			
 (標準備型(S): ○ 日期(date) ○ 時間(time) ○ 用戶端 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) ○ 伺服器連接埠(s-port) ○ 伺服器連接埠(s-port) ○ 有法(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-substatus) ○ Win32 狀態(sc-substatus) ○ 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) ○ 了推薦者(cs(Referer)) 			
記錄欄位來		來源	
新増欄位(A) 移除欄位(R)		羅定	軭檔案(E) 取消





-> 按下[確定]

新增自訂欄位	?	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	权 消	



(6) 按下 [確定]

	W3C 記錄	_張 欄位	? X
種進欄位(S)∙			
☑ 日期 (date)			
✔ 時間(time)			
☑ 用戶端IP 位址 (c-ip)			
↓ 使用者名稱(cs-usern)	ame)		
☑ 昵称名稱 (s-sitename))		
☑ 伺服器名稱 (s-computed)	/ tername)		
☑ 伺服器IP位址(s-in)	tername y		
✔ 伺服器連接埠 (s-port))		
☑ 方法(cs-method)	, ,		
✔ URI 主體 (Stem) (cs-u	ri-stem)		
✔ URI 査詢 (cs-uri-quen	v)		
☑ 通訊協定狀態 (sc-stat	us)		
☑ 通訊協定子狀態(sc-su	ibstatus)		
✔ Win32 狀態 (sc-win32	-status)		
☑ 已傳送位元組 (sc-byte	es)		
☑ 已接收位元組(cs-byte	es)		
☑ 花費時間(time-taken)		
☑ 通訊協定版本 (cs-vers	ion)		
✔ 主機 (cs-host)			
☑ 使用者代理程式 (cs(U))	ser-Agent))		
Cookie (cs(Cookie))	U		
✔ 推薦者(cs(Referer))			
自訂欄位(C):			
記錄欄位	來源類型	來源	
X-Forwarded-For	要求種頭	X-Forwarded-For	

記録懶12	**冰頬型	2代2県	
X-Forwarded-For	要求櫄頭	X-Forwarded-For	
新増欄位(A) 移除欄位	2(R)		編輯檔案(E)
		確定	取消





<i>8</i>]	Internet Information Services (IIS) 管理員	_ _ ×
🕞 💽 🍕 🕨 WIN 201	2 •	🖸 🛛 🟠 🔞 🗸
檔案(F) 檢視(V) 說明(H)	
連線 ● ● ● ● ● ● ● ●	記録 此功能可用來設定 IIS 在網頁伺服器上記錄要求的方式。 依下列項目為單位建立一個記錄欄(O): 座 「記錄欄 格式(M): 「以了 「「「」」」 「記錄欄 格式(M): 「「」」」 「「」 「「」 「「」 「「」 「「」」 「「」 「「」 「「」 「「」 「「」 「「」 「「」 「「」 「」 「」 「」 「」 「」 」 「「」 」 」 「」 」 「」 」 「」 」 「」 」 「」 」 「」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」	 勤作 ● 意思」 ● 停用 檢視記錄欄 ● 説明
設定: 'localhost' applicationH	ost.config	€ 1.:





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

	W3SVC	:1		_ □	x
€ ⊚ - ↑	퉬 C:\inetpub\logs\LogFiles\	<u>W3SVC1 v </u> さ	搜尋 W3S	VC1	Q.
☆ 我的最愛	名稱	修改日期	類型	大小	
	u_ex19080611_x.log	2019/8/6 上午 11:45	文字文件	13 K	В
』製 本機					
👊 網路					
1 個項目				[:==





(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)]

♥iii Internet Information Services (IIS) 管理員	- 🗆 X
(← →) ♥ > WIN2016 >	📴 🖂 🙆 🕡 -
檔案(F) 檢視(V) 說明(H)	
 審案() 独視(Y) 設想(H) 事業 (A) (A) 設想(H) (A) (A) (A) (A) (A) (A) (A) (A) (A) (A)	動作 訳 原用 後視記錄檔 ② 説明
設定: 'localhost' applicationHost.config	¶.::





(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(ssitename)]、[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(csmethod)]、[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		?	\times
標進欄位(S):			
備準欄位(S): ✓ 日期(date) ✓ 時間(time) ✓ 用戶端IP位址(c-ip) ✓ 使用者名稱(cs-username) ✓ 使用者名稱(s-sitename) ✓ 伺服器名稱(s-computername) ✓ 伺服器24種(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) ✓ 通訊協定子狀態(sc-substatus) ✓ Win32 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):			
^{■L} 郧儞业 水源頻型 新増欄位(A) 移除欄位(R)	75. <i>I</i> F	編輯檔案(1	Ε)
	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]

増自訂欄位		?	\times
欄位名稱(N):			
X-Forwarded-For			
來源類型(T):			
要求櫄頭		~	
來源(S):			
X-Forwarded-For		\sim	



(6) 按下 [確定]

W3C 記錄欄位			?	\times
W3C 記錄欄位 標準欄位(S): 「日期(date) 「日期(date) 「日期(date) 「日期(date) 「日期(date) 「日期(date) 「日期(date) 「日期(c-ip) 「日期(c-ip) 「日間者名稱(cs-username) 「日服器名稱(s-sitename) 「日服器名稱(s-computernate) 「日服器名稱(s-computernate) 「日服器注度埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-port) 「日服器連接埠(s-substate) 「通訊協定光態(sc-substate) 「日接收位元組(sc-bytes) 「花費時間(time-taken) 「連訊協定版本(cs-version) 「主機(cs-host) 「使用者代理程式(cs(User-Age) 「推薦者(cs(Referer))	me) m) us) us)		?	
自訂欄位(C): 記錄欄位 X-Forwarded-For	來源類型 要求櫄頭	來源 X-Forwarded-For		
新増欄位(A) 移除欄(立(R)	確定	輯檔案() 取消	E)





(7) 按下 [Apply(套用)]







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

A





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)]

♥iii Internet Information Services (IIS) 管理員	– 🗆 X
(← → (← → WIN2019 →	😰 🛛 🟠 🔞 -
檔案(F) 檢視(V) 說明(H)	
	動作 訳 音用 取満 停用 検視記錄欄 ② 説明
REACT rocamost applicationnost.comig	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(ssitename)]、[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(csmethod)]、[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	? ×	<
 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) 伺服器指(s-computername) 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) URI 查詢(cs-win32-status) 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-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]

欄位名稱(N):		
IN CELEMATING OF		
X-Forwarded-For		
來源蘋型(T):		
要求櫄頭	~	
來源(S):		
X-Forwarded-For	~	



(6) 按下 [確定]

W3C 記錄電位 ? × 福濃電位(S): (416) 9時間(time) 月戸端 IP 位址(c-ip) 9 使用者名幫(c-scomputername) 回服器名幫(s-computername) 9 伺服器生育(s-computername) 何服器生育(s-computername) 9 伺服器生育(s-computername) 何服器生育(s-computername) 9 伺服器生育(s-computername) 何服器生育(s-computername) 9 伺服器生育(s-computername) 何服器生育(s-computername) 9 伺服器生育(s-computername) 10 Rl 言葉(s-scomputername) 9 伺服器生育(s-computername) 10 Rl 言葉(scomputername) 9 伺服器生育(s-scomputername) 10 Rl 言葉(scomputername) 10 Rl 言葉(scomputername) 11 Rl fragge 10 Rl 言葉(scomputername) 11 Rl fragge 11 Rl fragge 11 Rl fragge 12 Rl fragge 11 Rl fragge 13 Rl fragge 11 Rl fragge 14 Rl fragge 11 Rl fragge 15 Rl fra					
福華電位(S): 9 日雨(date) 9 時間(time) 9 月戸端 IP 位北(c-ip) 9 使用者名稱(c-suername) 9 伺服器4 (s-computername) 9 伺服器/Egk (s-port) 7 方法(cs-method) 9 何服 建煤 (s-port) 7 方法(cs-method) 9 何服 建煤 (s-port) 7 方法(cs-method) 9 何服 建煤 (s-port) 9 月間 確定 大都恵(sc-substatus) 9 週間 協定 大雅曼(sc-substatus) 9 週間 協定 た (sc-vin32-status) 9 目標 地位元組(s-bytes) 9 日春 位 (sc-vin4) 9 日春 位 (sc-vin5) 9 日春	W3C 記錄欄位			?	\times
 ✓ 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 新埔欄位(A) 移除穩位(R) 編輯檔案(E) 確定 取消 	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) 「使用者名稱(cs-username) 「使用者名稱(s-computernam 「伺服器名稱(s-computernam 「伺服器注度埠(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-substatu 「URI 查詢(cs-uri-query) 」通訊協定狀態(sc-substatu 「URI 查詢(cs-win32-status) 「這訊協定版本(cs-version) 」主機(cs-host) 「使用者代理程式(cs(User-Ag	ne) n) is) s)		?	×
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 新増欄位(A) 移除欄位(R)	☑ Cookie (cs(Cookie)) ☑ 推薦者 (cs(Referer))				
記錄欄位 來源類型 來源 X-Forwarded-For 要求標頭 X-Forwarded-For 新増欄位(A) 移除欄位(R) 編輯檔案(E) 確定 取消					
X-Forwarded-For 要求標頭 X-Forwarded-For 新増欄位(A) 新増欄位(R) 編輯檔案(E) 確定 取消	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	X-Forwarded-For	要求櫄頭	X-Forwarded-For		
新増欄位(A) 移除欄位(R) 編輯檔案(E) 確定 取消					
確定取消	新増欄位(A) 移除欄位	2(R)		編輯檔案(E)
			確定	取消	





Name and the services (IIS) 管理員	– 🗆 X
← → ♥ WIN2019 →	😰 🛛 🟠 🔞 🗸
檔案(F) 檢視(V) 說明(H)	
建築 記録 小田市町用来設定IIS 在網頁伺服業上記録要求的方式・ 公 1900 (NART) 企 1900 (NART) 金 酒屋空菜 金 酒屋空菜 一 2 公会 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	動作 ● 査用 ● 取消 個存目前的變更。 停用 検視記録欄 ② ② 說明
設定: 'localhost' applicationHost.config	• <u> </u>





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

W3SVC1				_		×
← → · ↑ 📙 🖸	inetpub\logs\LogFiles\W3SVC1	~ Ū	搜尋 W3SVC	1		Q
	名稱	修改日期	<u>類型</u> ^	大小		
₩ 沃迷仔収	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						





7. N-Reporter

(1) 新增 IIS 設備

[設備管理]->[設備樹狀圖]-> 點選[新增]







(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]

よ 設備資訊編輯		×
設備基本設定		• • •
名稱		n II.
Win_II5-192.168.2.127		
IP		
192.168.2.127		
		-
Syslog Flow SNMP		
Syslog 相關設定		
資料格式		1
IIS	~	
Facility		
(22) local use 6 (local6)	~	
編碼方式		
UTF-8	~	
設備進階設定		
設備 Icon		
icon-host	~	
Login Account		
Login Password		
Action 設備		
是否為 Action 設備		
接收狀態		
● 啟用 ○ 停用		
暫無資料告警		
□ 政用 ɔysiog/riuw 智無其科告言		
	席守	eftr Sale
	唯足	収洞

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 業務相關請洽: Email: sales@npartnertech.com

