

# 如何配置 Windows IIS log

V011



## 版权声明

N-Partner Technologies Co. 版权所有。未经 N-Partner Technologies Co. 书面许可,不得以任何形式仿制、拷贝、 誊抄或翻译本手册的任何内容。由于产品不断更新中,N-Partner Technologies Co. 保留不通知变更的权利。

## 商标

本手册内提到的任何公司产品、名称及注册商标,均属其合法注册公司所有。





前	言.				-			•		•		•		•	•	 1
1	NXL	.og														 2
	1.1	NXLog	安	虔.												 2
	1.2	NXLog	配	置文	件	下载	鈛.									 6
		1.2.1	适用	目于	W	ind	ow	s 2	200	)3	或勇	更早	2版	ō7	Σ搷	
			作	系统												 6
		1.2.2	适用	用于	W	ind	ow	s 2	200	8	或勇	更高	高版	ō7	S損	
			作	系统												 7
	1.3	NXLog	配	置文	件											 8
		1.3.1	记录	录所	有	信息	息的	配	置	文1	件					 8
		1.3.2	不ì	己录	Co	ook	ie 1	言	急的	勺酉	2置	文	件			 9
	1.4	NXLog	「启え	动服	务											 10
		1.4.1	Wir	ndo	ws	20	03	或	更	₹₿	反本	禄	作	系	统	10
		1.4.2	Wir	ndo	ws	20	80	或	更ī	高片	反本	禄	作	系	统	13
2	Wine	dows 20	000													 16
3	Wind	dows 20	003													 20
4	Wind	dows 20	800													 27
5	Wind	dows 20	)12													 38
6	Wind	dows 20	)16													 43
7	Wind	dows 20	)19													 48
8	Wind	dows 20	)22					_		_						 53
9	N-R	eporter														 58
		•														





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].

RXLog-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



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

						-
	NXLO	G PUBI	LIC LIC	CENSE	v1.0	1
1. <b>"Lic</b> "LiC "Sof	DEFINITIO ense" shall n ENSE, i.e. t tware" shall ociated media	DNS hean version he terms and mean the so a, printed ma	1.0 of the d condition urce code aterials, an	NXLOG I s set forth i and object d "online" o	PUBLIC n this docum code form, r electronic	ient; all
doc	umentation.	All such soft	ware and 1	naterials ar	e referred to	<u>•</u>

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

NXLog-CE Setup				
Destination Folder Click Next to install to the o	lefault folder or cli	ick Change to	choose another.	
Install NXLog-CE to:				
C:\Program Files\nxlog\				
Change				
	1	Back	Next	Cancel



#### -> 点击 [Install].



-> 点击 [Finish].





#### <2.2> Windows 2003

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

NXLog-CE Setup	-		×
Ready to install NXLog-CE			
Click Install to begin the installation. Click Back to review or change any installation settings. Click Cancel to exit the wizard.	of your		
Back Install		Cance	el

#### <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

■ 命令提示字元	
C:\>copy "C:\nxlog_WinDHCP.conf" "C:\Program Files\nxlog\conf\n 複製了     1 個檔案。	ixlog.conf"∕y ▲
C: \>_	•

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

条統管理員: Windows PowerShell ー PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog\_WinDH -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf' PS C:\> \_

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
              '%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>
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。

檔案名稱(N):	nxlog.conf								$\sim$
存檔類型(T):	所有檔案 (*.*)	1							$\sim$
截資料夾				編碼(E):	ANSI ANSI	· · · · · · · · · · · · · · · · · · ·	存檔(S)	取消	
					Unicode Unicode UTF-8	e big endian 2			



#### 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
              '%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>
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。

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		~	存檔(S)	取消	
					Unicode Unicode UTF-8	e big endian 2				



## 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





#### (3) 打开 [服务] 功能





## (4) 打开 NXLog 服务设置

选择 [NXLog] -> 🖆点击 [属性]

微显器					_ [	X			
檔案(E) 執行(A) 檢視(V) 說明(E)	D								
🍇 服務 (本機) <mark>內容</mark>									
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				
/用2世: 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	<b>-</b>			
	🍓 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) 在 [常规] 页面 -> 确认启动类型为 [自动]

NXLog 內容 (本街	唐重醫) <b>?</b> ×
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	Ē(H):
"C:\Program File	s (x86)\inxlog\nxlog.exe" -c "C:\Program Files (x86)\inxlog
啓動類型(正):	自動
服務狀態:	已啓動
啓動(3)	<b>停止(I)</b> 暫停(I) 繼續(B)
您可以在這裡推	定啓動服務時所要套用的參數。
啓動參數( <u>M</u> ):	
	確定 取消 套用(丛)



(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]

NXLog 內容 (本標電醫)	? ×
一般量入修復	夜存性
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(王):	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 程式(P):	
	瀏覽(B)
命令列參數(C):	
▶ 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(E)



#### 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



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





## (4) 打开 NXLog 服务设置

选择 [NXLog] -> 回 点击 [属性]

🔍 服務					_		×
檔案(F) 動作(A) 檢視(V) 說明(⊦	Ð						
🗢 🔿 🖬 🖬 🖬 🖬 🖬	▶ ■ H IÞ						
服務 (本機) 内容							
NXLog	名稱 ^	描述	狀態	啟動類型	登入身分		^
107 - L 273 304	🆏 Network Location Awareness		執行中	自動	Network S	Service	
<u>行止</u> 服務 重新動動服務	🏟 Network Setup Service	「網路設定		手動 (觸發程	Local System		
<ul> <li>檔案(F) 動作(A) 檢視(V) 說明(</li> <li>➡ ➡ 〒 □ □ □ □ □ □ □ □</li> <li>■ ■ ■ □ □ □ □</li> <li>■ ■ ■ □ □ □ □</li> <li>■ ■ ■ ■ ■ ■ ■ ■</li> <li>■ ■ ■ ■ ■</li> <li>■ ■ ■ ■</li> <li>■ ■ ■ ■</li> <li>■ ■ ■</li> <li>■ ■ ■</li> <li>■ ■<td>Ketwork Store Interface Service</td><td>此服務可將</td><td>執行中</td><td>自動</td><td>Local Serv</td><td>/ice</td><td>_</td></li></ul>	Ketwork Store Interface Service	此服務可將	執行中	自動	Local Serv	/ice	_
	🖏 NXLog	This service 執行中		自動 (延遲啟動)	Local System		
描述:	Straine Files	離線檔案服		已停用	Local System		_
running the NXL og agent. See	OpenSSH Authentication Agent	Agent to h		已停用	Local Syst	em	
www.nxlog.co.	Optimize drives	可最佳化存		手動	Local System		~
延伸 (標準/							

## (5) 在 [常规] 页面 -> 确认启动类型为 [自动 (延迟启动)]

NXLog 内	] 容 (本機	電腦)						×
一般	登入	復原	相依性					
服務名	稱:	nxlo	9					
顯示名稱:		NXL	NXLog					
描述:	描述:		service is nt. See ww	responsible w.nxlog.co	for running	the NXI	.og ^ v	
可執行 "C:\Pro	檔所在路 ogram Fi	徑 iles\nxlo	g\nxlog.ex	e" -c "C:\Pr	ogram Files\	nxlog\c	:onf\nxlog	
啟動類	型(E):	自重	的(延遲啟動	)			~	
服務狀	態:	執行	¢					
10	达動(S)		停止(T)	善	ř停(P)	纑	績(R)	
您可以	在這裡指	定啟動服	務時所要到	気用的參數。				
啟動参!	數(M):	[						
				確定	取消		套用(A)	



(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]

NXLog 內容 (本機電腦)	2	×				
一般 登入 復原 相依性	性					
	• 協助我設定復原動作。					
第一次失敗時(F):	重新啟動服務 ~					
第二次失敗時(S):	重新啟動服務 ~					
後續失敗時(U):	重新啟動服務 ~					
經過下列天數後重設失敗計數(C	0): 1 天					
經過下列時間後重新啟動服務(V	V): 1 分鐘					
□ 啟用對因錯誤而停止所採取的 動行程式	的動作。 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結尾 (/fail=%1%)(E)						
	確定 取消 套用(A)					



## 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



(3) 打开 [Internet 信息服务管理器]





### (4) 右键点击 [网站]<sup>,</sup>选择 [属性]

Service:	s X
」執行(Δ) 檢視(型) ↓ ←	• →   📾 💽   🖧   😫   ▶ = = =
樹狀目錄	電腦 本機 連線類型 錯誤狀態
<ul> <li>Internet Information Service</li> <li>■ * win2000</li> <li>● ● 預設的 FTP 站台</li> <li>● ● 預設的 Web 站台</li> <li>● ● 系統管理 Web 站台</li> </ul>	≝ *win2000 是 TCP/IP 查看
田一谷 預設 SM IP 虚擬症 豆一诊 預設 NN TP 虛擬症	開啓舊檔 瀏覽
	容動 <b>停止</b> 暫停
	新增 <u>N</u> ▶ 所有工作( <u>K</u> ) ▶
	刪除① 重新整理①
	内容( <u>R</u> )
	説明田 15
開啓目前選擇的內容頁。	



(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]

頁設的 Web 站台 內容
目錄安全設定         HTTP 標題         自訂錯誤         伺服器擴充程式            Web 站台         操作員         效能         ISAPI 篩選器         主目錄         文件
Web 站台識別碼
説明(፩): 預設的 ₩eb 站台
IP 位址①: (全未指定) _ 進階 ①
TCP 連接埠(I): 80 SSL 連接埠(L);
連線
○ 沒有限制(U)
○限制在(M): 1,000 連線
連線逾時時間(11): 900 秒
▼ 啓用 HTTP 的持續作用 低)
✓ 啓用記錄(E)
使用中的日誌格式(V):
₩3C Extended Log File Format P容化
<b>確定 取消 </b>

(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

擴充記錄內容	x
一般內容 擴充內容	
新日誌週期	
○ 毎日(W) ○ 毎周(M)	
<ul> <li>○ 沒有限制檔案大小(U)</li> <li>○ 當檔案大小到達(2):</li> <li>19</li> <li>19</li> <li>MB</li> </ul>	
<ul> <li>✓ 諸使用本地時間爲檔案命名(T)</li> <li>日誌檔目錄(L):</li> </ul>	
C:\Inetpub\logs\LogFiles 瀏覽(B) 日誌檔名稱: W3SVC1\exyymmddhh.log	

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]

擴充記錄內容	×
一般內容 擴充內容	
	_ [
擴充記錄選項          ● 日期(date)       ●         ● 時間(time)          擴充內容       ●         ● 使用者名稱(cs-usemame)       ●         ● ② 個服器名稱(s-sitename)       ●         ● ② 伺服器名稱(s-computemame)       ●         ● ② 伺服器連接埠(s-port)       ●         ● ② 伺服器連接埠(s-port)       ●         ● ② URI 粗縱線(cs-uri-stem)       ●         ● ③ URI 電詢(cs-uri-query)       ●         ● ③ URI 電詢(cs-win32-status)       ●         ● ③ 送出的位元組(sc-bytes)       ●         ● ② 送出的位元組(cs-bytes)       ●         ● ② 注機(cs-host)       ●         ● ② 使用者代理程式(cs(User-Agent))       ●         ● ② Cookie (cs(Cookie))       ●	
└── ✔ 推薦者 (cs(Referer))	
確定 取消 套用(A) 説明	1

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

🔁 W3SVC1				
檔案(F) 編輯(E) 檢視(V)	我的最愛(A) 工具(I)	說明(H)		10 A
〜上─頁 → → → 🔁   Q.拍	雙尋 🔓 資料夾 🌑 記錄			
]網址(D) 🔄 C:\Inetpub\logs\LogFi	les\W3SVC1			▼ 🔗務至
	▲ 名稱 △	大小類型	修改日期	
W3SVC1	≝ ex21082514.log	2 KB 文字文件	2021/8/25 -	下午 02:26
請選取一個項目來檢視它的說   明。				
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) 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



#### (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]

WIN2003 (本機電腦) 內容	? ×
網際網路資訊服務	
□ 啓用直接 Metabase 編輯(N)	
た許您在 IIS 執行時,編輯 IIS Metabase 設定檔。	
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(₩)	
IIS 只服務副檔名有登錄在 MIME 類 刑法單裡的檔案。芜葉設定其他檔 MIME 類型(M)	
	1
	月

#### (6) 再次点击 [确定]





### (7) 在 [网站] 上右键点击 -> 选择 [属性]

(IIS) 答温馬斉紹傳劉降 🇊	王員		_ 🗆 🗡
б」檔案(E) 執行(A) 檢視(V)	視窗(₩) 説明(H)		_ ð ×
⇔ → 🗈 🖬 😭 🗟	😫 💵   💂   🕨 🔳 II		
<ul> <li>● 網際網路資訊服務</li> <li>● ● ● WIN2003 (本機電腦)</li> <li>● ● ● 應用程式集區</li> </ul>	描述	<u>識別元</u> 1	<u></u> 秋行中
由→ 一 網頁. 新增(N) 所有工作(K)	*		
檢視(型) 従這裡新增祿	• 記窗(W)		
重新整理(E) 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) 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]

目錄安全計	定	HTTP 標題	ē	自訂錯誤	服務
網站	效能	ISAI	智 篩選器	主目錄	文件
網站識別碼					
説明( <u>8</u> ):	Г				1
IP 位址(I):	(California)	全未指定)		Ŧ	進階(D)
TCP 連接填	(D):		SSL 連接	阜(L):	
座 啓用 H1	間(N):   TP的持續(	12 乍用 ( <u>K</u> )	20秒		
·	間(型):   TP 的持續( 線區)	12 作用( <u>K</u> ) 格式	20 秒	▼ 内容(P).	
連線迴時時 ▼ 啓用 H1 ▼ 啓用記録 現用的記 ₩3C 擴	間(11):   TP 的持續( 除(E)	12 作用 低) 格式	20 秒	▼ 内容(P).	



(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]

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) 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]

記錄內容	×
一般 進階	
擴充記錄選項(以):	
<ul> <li>✓ 日期(date)</li> <li>✓ 時間(time)</li> <li>擴充內容</li> <li>✓ 伊戶端 IP 位址(c-ip)</li> <li>✓ 使用者名稱(cs-usemame)</li> <li>✓ 很服務名稱(s-sitename)</li> <li>✓ 伺服器名稱(s-computemame)</li> <li>✓ 伺服器上接埠(s-port)</li> <li>✓ 伺服器連接埠(s-port)</li> <li>✓ 方法(cs-method)</li> <li>✓ URI 主體(cs-uri-stem)</li> <li>✓ URI 查詢(cs-uri-query)</li> <li>✓ 通訊協定状態(sc-status)</li> <li>✓ Win32 狀態(sc-substatus)</li> <li>✓ Win32 狀態(sc-substatus)</li> <li>✓ 接收的位元組(sc-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(cs(User-Agent))</li> <li>✓ 推薦者(cs(Referer))</li> </ul>	
確定 取消	套用(A)   説明

(11) 点击 [全选] 和 [确定]

繼承喪寫	×
下列子節點也定義 "LogFile TruncateSize" 內容值,這個內的值。請從下方的清單中彈動應使用新內容值的節點。	容值已覆寫您剛設定
子節點(C):	
預設的網站	全選③



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

<b>≧</b> C:\Inetpub\logs\LogFiles\₩3S¥C1			_ 🗆 🗡
檔案(F) 編輯(E) 檢視(V) 我的最愛	≹(Δ) 工具(I) 説明(H)		2
🔾 上一頁 🔹 🕤 🔹 🎓 搜尋 🌔	資料夾   🕼 🍛 🗙 🍤	<b>.</b>	
網址① 🗁 C.\Inetpub\logs\LogFiles\W3SW	7C1		💌 🌛 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>	נע_ex19080617.log	6 KB 文字文件 2019/8/6 下午 05:3	3 A



## 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]

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
				• •
<del>新</del> 体期(合(4))	\$2.0℃/₽.)	1	编辑欄位化	1



(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]

新増記錄欄位	? X
欄位識別碼(F):	
X-Forwarded-For	
類別(C):	
Default	•
——————————————————————————————————————	
來源類型(I):	
要求標頭	-
來源名稱(N):	
X-Forwarded-For	
效能計數器模型(7).	
速度	<u>~</u>
顯示進勝內容	
	10000000000000000000000000000000000000

## (10) 点击 [启用高级日志] 和 [启用客户端日志]

Nation Serv	ices (IIS) 管理員	
(3) (3) (3) (3) (3) (3) (3) (3) (3) (3)	3 •	🔛 🖂 🚹 I 😥 🕶
檔案(F) 檢視(∀) 說明(H	)	
速線         ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●         ●       ●       ●       ●	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。         難組依措:沒有分組         全編         日歇用         冬COMPUTERNAME%S         日啟用	<ul> <li>         Advanced Logging 功能已停 用。     </li> <li>         新增記錄定義         及用 Advanced Logging         政用用戶端記錄         協報記錄欄位         協職記錄相做         成現         說明         說明         說上說明         </li> </ul>
EXAE: localhost applicationHost.c	oning	1.1



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



#### (12) 点击 [新增日志定义]

Nation Service	es (21) 2:	
	<b>)</b>	🖸 🖂 🖄 I 🕲 •
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             群組依據: 沒有分組               名稿 ▲            已啟用             名稿 ▲            已啟用             %COMPUTERNAME%Server         已停用           回             ◎         功能檢視           ⋒	<ul> <li>動作</li> <li><u>新増記録定義</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>編輯記錄相錄</li> <li>檢視記錄檔</li> <li>說明</li> <li>線上說明</li> </ul>
設定: localhost'applicationHost.com	ïg	€ <u>1</u> .:



(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]

'≩Internet Information Services (IIS) 管理員	
(3) (3) № WIN2008 .	🔛 🖂 🔂 I 😥 🕶
腦菜(F) 檢視(V) 說明(H)	
第日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	<ul> <li>新作</li> <li>※ 茶用</li> <li>※ 取消</li> <li>※ 取消</li> <li>※ 取消</li> <li>※ 返回 Advanced Logging</li> <li>② 說明</li> <li>除上說明</li> </ul>
37.56	<b>1</b> .:



(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]

#### 選取記錄欄位

? ×

<b>識別碼</b>	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
<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
<ul> <li>Server Port</li> </ul>	ServerPort	內建	Default	s-port
✓ Server Name	ServerName	內建	Default	s-computernam
RequestsPerSecond	\W3SVC_W3WP(T.	效能計數器	Default	RequestsPerSec
✓ 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	d.a.te
✓ 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
Bytes Received	BytesReceived	棋組	Default	cs-bytes
BeginRequest-UTC	BeginRequest-UTC	棋組	Default	BeginRequest-U
(				•
			確定	取消



(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]

管Internet Information Services (IIS) 管理員	
😋 💬 📲 • WIN2008 •	🔛 🖂 🏠 I 😥 🕶
檔案(F) 檢視(∇) 說明(H)	
田田	<ul> <li>新作</li> <li>※ 班用</li> <li>※ 取用</li> <li>税用</li> <li>※ 返回 Advaced Logging</li> <li>※ 說明</li> <li>第上說明</li> </ul>
說定: localhost'applicationHost.config	<b>9</b> 1.:



#### (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]









#### (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

🕌 AdvancedLogs						
00 💵	\inetpub\logs\AdvancedLogs		• 🚱	搜尋 AdvancedI	ogs	2
組合管理 ▼ 加	□入至媒體櫃 ▼ 共用對象	▼ 新増資料夾		1	•	0
☆ 我的最愛	名稱 ▲	修改	日期 類	型 大/	N	
🥽 媒體櫃	📄 u_ex_H20190806-0914	41942.log 2019.	8/6 下午 05:19 文学	字文件	51 KB	
📃 電腦						
👊 網路						



## 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]

v <sub>i</sub>	Internet Information Services (IIS) 管理員	_ <b>D</b> X
€ S 112012	2 🕨	📅 🗠 🏠 🔞 •
檔案(F) 检視(V) 説明(H)		
福案(F) 检視(V) 説明(H) 建雄 ● 目   ● ● ● 認知規算 ● WIN2012 (WIN2012) ● ● 配相式集區 ● ● 站台	記録           此地球可用來設在 IS 在網頁伺服器上記錄要求的方式。           法方可見具專道健立一個記錄攝(C):           」           「公園           「記錄           「記録           「記録 <tr< td=""><td>動作         梁 奈用         梁 取消         停用         桂視記錄備         ② 說明</td></tr<>	動作         梁 奈用         梁 取消         停用         桂視記錄備         ② 說明
設定: 'localhost' applicationHo	st config	Q1 -
acc. recompart applicationing	ananing	- A.::



(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]

	W3C 記錄欄位	? X
<ul> <li>標準欄位(S):</li> <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>✓ 同服器名稱(s-sitename)</li> <li>✓ 伺服器名稱(s-computername)</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 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>✓ Win32 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>✓ 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>✓ 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) 収消



(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->

新増自訂欄位	?	x
欄位名稱(N):		
X-Forwarded-For		
來源蘋型(T):		
要求標頭	~	
來源(S):		
X-Forwarded-For	~	
確定	取消	

### (6) 点击 [确定]

	W3C į	記錄欄位	? X
<ul> <li>標準欄位(S):</li> <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>♥ 伺服器名稱(s-computernation of the second of the</li></ul>	) ame) em) itus) tus)		
記錄欄位	來源類型	來源	
X-Forwarded-For	要求種頭	X-Forward	ded-For
新増欄位(A) 移除欄	位(R)		編輯檔案(E)
		確定	取消



### (7) 点击 [应用]

<b>V</b> 1	Internet Information Services (IIS) 管理員	_ <b>D</b> X
€ S ♥ WIN2012	2 >	📅 🗠 🏠 🔞 •
檔案(F) 检視(V) 説明(H)		
福葉(F) 檢視(V) 說明(H)       連結       ・       ●	記録           此功能可用未設定 IIS 在網頁伺服器上記錄要求的方式。           (次下列項目為單位建立一個記錄欄(O):           送信           「記錄           記錄           記錄           記錄           記錄           「記錄           「記錄           「記錄           「記錄           「記錄           「記錄           「「「」」           「記錄           「「」」           「「」           「「」           「「」           「「」           「「」           記錄 []           「」           記録           「」           「」           二           「」           「」           「」           「」           「」           「」           「」           「」           「」           「」           「」           「」           「           「           「           「           「           「           「           「           「           「	数作 ☆ 室田 修用 強視記録編 ② 説明
< III > > ジョン ジョン ジョン ジョン ジョン ジョン ジョン ジョン ション ジョン ション ション ション ション ション ション ション ション ション シ	ust confin	<b>6</b> 1 -
acce. localitost applicationHi	ana ang ang ang ang ang ang ang ang ang	1.:

(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]

♥a Internet Information Services (IIS) 管理員	- 🗆 X
← → ♥ WIN2016 +	🛄 🖂 🟠 🔞 •
攝案(F) 檢視(V) 說明(H)	
● このでのでしたのである。             ● ごのでのである。             ● ごのでのでのです             ● ごのでのです             ● ごのでのです             ● ごのでのです             ● ごのでのです             ●             ● ごのでのです             ●             ● ごのでのです             ●             ●	動作         副<
設定: 'localhost' applicationHost.config	Mil.:



(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]

W3C 記錄欄位		? ×
標準欄位(S): ☑ 日期 (date) ☑ 時間 (time)		
<ul> <li>☑ 用戶端 IP 位址 (c-ip)</li> <li>☑ 使用者名稱 (cs-username)</li> <li>☑ 服務名稱 (s-sitename)</li> <li>☑ 伺服器名稱 (s-computername)</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 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>☑ 已傳送位元組 (sc-bytes)</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> </ul>		
<ul> <li>✓ 主機 (cs-host)</li> <li>✓ 使用者代理程式 (cs(User-Agent))</li> <li>✓ Cookie (cs(Cookie))</li> <li>✓ 推荐者 (cs(Pofered))</li> </ul>		
e訂欄位(C):		
記錄欄位 來源類	2 來源	
新増欄位(A) 移除欄位(R)		編輯檔案(E)
	確定	取消



(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]
----	------

新増自訂欄位	?	Х
欄位名稱(N):		
X-Forwarded-For		
本语短刑(四).		
要求標頭	~	
來源(S):		
X-Forwarded-For	$\sim$	
確定	取消	

### (6) 点击 [确定]

W3C 記錄欄位				?	×
W3C 記錄欄位 標準欄位(S): ② 日期(date) ③ 時間(time) ③ 用戶端IP 位址(c-ip) ④ 使用者名稱(cs-username) ④ 個服器名稱(s-sitename) ④ 伺服器2稱(s-computernam ④ 伺服器連接埠(s-computernam ④ 伺服器連接埠(s-port) ④ 伺服器連接埠(s-port) ④ 伺服器連接埠(s-port) ④ 伺服器連接埠(s-port) ④ 伺服器連接埠(s-computernam ④ URI 查詢(cs-uri-stem ④ URI 查詢(cs-uri-stem) ④ 通訊協定式狀態(sc-status) ④ 通訊協定子狀態(sc-substatus) ④ 過訊協定式狀態(sc-vin32-status) ④ 已接收位元組(sc-bytes) ④ 已接收位元組(cs-bytes) ④ 花費時間(time-taken) ④ 通訊協定版本(cs-version) ④ 主機(cs-host) ④ 使用者代理程式(cs(User-Age	e) ) ;) )			?	×
自訂欄位(C): 記錄欄位 X-Forwarded-For	來源類型 要求種類	來源 X-Forw	arded-For		
新増欄位(A) 移除覆位	(R)		الله لك	輯檔案(E <b>取消</b>	:)



## (7) 点击 [应用]

National Internet Information Services (IIS) 管理員	– 🗆 X
← →  ♥ WIN2016 +	😐 🖂 🔂 😦 •
櫃鱉(F) 檢視(V) 說明(H)	
副         記録           ここの         定期電気振客           ここの         定期電気振客           ここの         定期電気振客           ここの         定期電気振客           ここの         定期電気振客           ここの         定期電気振客           ここの         ごの           日本型なきな一個と伴嘱(0):         送告           ごこの         運動電気に、           UFF8         ごの           ここの         ごの           ごた時電券目的地            ④ 値形に参考へ記参画中的目的地            ④ 値形に参考へ記参画中的目的地            ④ 値形に参考し記参画            ごの            ごの            ごの            ごの            ごの            ごの            ごの            ごの            ごの            「「「「」」」」」            「「」」            ごの            ごの            「「」」」            「」」」            「」」            「」」            「」」 <td>契件         ○ 室田         ○ 取用</td>	契件         ○ 室田         ○ 取用
Exc. rotanost applicationnost.comg	1.1

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

W3SVC1				- C	) X
$\leftarrow \rightarrow \cdot \uparrow$	C:\inetpub\logs\LogFiles\W3SVC1		~ Ū	搜尋 W3	sv , <b>p</b>
3. 柿油东西	名稱 ^	修改日期	類型	大小	
★ 大述1子和	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) 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]

鞜 Internet Information Services (IIS) 管理員		_		×
← →  ♥ WIN2019 >		-	× 🟠	•
欄需(F) 檢視(V) 說明(H)				
第25000000000000000000000000000000000000	助作         ●       要用         ●       取消         (停用         检視記錄         ●       説明	g		
設定: 'localhost' applicationHost.config				1.1



(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]

W3C 記錄欄位		?	×
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>◇ 伺服器名稱(s-computername)</li> <li>◇ 伺服器名稱(s-computername)</li> <li>◇ 伺服器連接埠(s-port)</li> <li>◇ 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>◇ Win32 狀態(sc-substatus)</li> <li>◇ Win32 狀態(sc-substatus)</li> <li>◇ Win32 狀態(sc-bytes)</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		
新博士		価報福令/1	5)
		) 外表 田「 4年 勝点	-)
	確定	取消	



(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->

新増自訂欄位	?	×
欄位之稱(N)-		
X-Forwarded-For		
來源類型(T):		
要求標頭	~	
來源(S):		
X-Forwarded-For	~	
確定	取消	

### (6) 点击 [确定]

W3C 記錄欄位			?	×
语准暇(广(C)。				
標準佩12(5):				
✓ 日期 (date)				
✓ 時間(time)				
✓ 使用者名稱 (cs-username)				
✓ 服務者備 (s-sitename)	>			
☑ 伺服器 D 位批 (s-computernan)	ne)			
✓ 何服務建接焊 (s-port)				
✓ 万法 (cs-metriod)	- )			
☑ URI 查詢 (cs-uri-quequ)	1)			
☑ 通知協定計能(sc-status)				
	(F)			
✓ Win32 計能 (sc-win32-statu	5) 5)			
図 已傳送位元组(sc-bytes)	3)			
図 已接近位元组 (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	要求種頭	X-Forwarded-For		
	344 B.M	X Tornarded Tor		
★ 塔爾片(A) 約 時間	5/D)	15	5:87:22 中/1	
新増催Ⅲ(A) 修际催Ⅱ		13		L)
			T- NK	
		4年正	取消	



## (7) 点击 [应用]

National Information Services (IIS) 管理員	– 🗆 ×
← →  ♥ WIN2019 >	😐 🖂 🏠 🔞 •
櫾案(F) 檢視(∀) 說明(H)	
第2000       記録         ● 記録       小地町用床設をIIS 在頃買伺服器上記録要求的方式。         ● 水田町用床設をIIS 在頃買伺服器上記録要求的方式。       位下列項目為單位建立一個記錄層(O):         ● 酒店(I):       一日         ● 御信(I):       一日         ● 御信(I):       ●         ● 御信(I):       ●	動作         ●       部2         ●       部2         ●       設明
設定: 'localhost' applicationHost.config	<b>9</b> 1.1

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

W3SVC1				_		×
$\leftarrow \rightarrow \cdot \uparrow$	C:\inetpub\logs\LogFiles\W3SVC1	ې م	搜尋 W3SVC	1		Q
	名稱	修改日期	<u>類型</u> ^	大小		
☞ 沃速仔収	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						



## 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]

输 Internet Information Services (IIS) 管理員	– 🗆 X
← → ♥ → WIN2022 →	📅 🖂 🔂 🕡 •
檔案(F) 檢視(V) 說明(H)	
・          ・       記録         ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・          ・ <td><ul> <li>● 新用</li> </ul></td>	<ul> <li>● 新用</li> </ul>
ke.c. iocanios: applicationnos:coning	1.1



(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]

W3C 記錄欄位		?	×
標準欄位(S):			
(標準備Ш(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) ○ 伺服器名稱(s-computername) ○ 伺服器24年(s-computername) ○ 伺服器IP位址(s-ip) ○ 伺服器連接埠(s-port) ○ 方法(cs-method) ○ URI主體(Stem)(cs-uri-stem) ○ URI 查詢(cs-uri-query) ○ 通訊協定狀態(sc-status) ○ 通訊協定狀態(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))			
目引欄位(C):	太海		
	小体		
新増欄位(A) 移除欄位(R)		編輯檔案(	E)
	確定	取消	



(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->

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

## (6) 点击 [确定]

W3C 記錄欄位			?	×
/ 播 ) / (C)-				
1県≄1間12(3).				
✓ 山痢 (date)				
	-)			
☑ 使用有有悔 (CS-username)	-)			
☑ 個明界交通 (s-scomputer)	nama)			
✓ 伺服器 ID 位址 (s-in)	name)			
☑ 方法(cs-method)				
☑ URI 主體 (Stem) ( cs-uri-s	tem )			
☑ URI 查詢 (cs-uri-query)				
☑ 通訊協定狀態 (sc-status)				
☑ 通訊協定子狀態 (sc-subs)	tatus )			
✓ Win32 狀態 (sc-win32-st	atus)			
 ☑ 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	1)			
☑ 主機 (cs-host)				
☑ 使用者代理程式(cs(User	-Agent) )			
Cookie ( cs(Cookie) )				
☑ 推薦者 ( cs(Referer) )				$\sim$
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		
新増欄位(A) 移除	確位(R)			E)
			_	
		確定	取消	



## (7) 点击 [应用]

🞕 Internet Information Services (IIS) 管理員		- 0	×	
← →  ♥ WIN2022 +			😈 🔤 🏠 (	• •
檔案(F) 檢視(V) 說明(H)				
連線       ●       ●       記録         ● </td <th>離上記錄要求的方式。 ■(O): ■ ■ ■ ■ ■ ■ ■ ■ ■ ■</th> <td>▲ 小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田</td> <td><u></u></td> <td></td>	離上記錄要求的方式。 ■(O): ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	▲ 小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田	<u></u>	
設定: 'localhost' applicationHost.config				•

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

W3SVC1			_		×
🤟 🔶 👻 🛧 📙 C.\in	etpub\logs\LogFiles\W3SVC1	ٽ ٽ			Q
2. 柏油方面	2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	- ロ * ひ 修改日期 類型 大小 2021/8/25 上午 10:59 文字文件 2021/8/25 上午 11:00 文字文件	2 KB		
🥔 網路					
2 個項目	ー □ × netpub\logs\LogFiles\W3SVC1 v む の 名稱 修改日期 類型 大小 ■ u_ex21082510_xlog 2021/8/25 上午 10:59 文字文件 2 KB ■ u_ex21082511_xlog 2021/8/25 上午 11:00 文字文件 2 KB				



## 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]

听增设备 - 设备基本设定				
设备基本设定				^
设备名称 *				
WinIIS-192.168.8.195				
IP *				
192.168.8.195				
所属领域 *				
Global				~
Syslog 数据格式 🕕				
IIS				~
自订数据格式 🕄 🛨				
				~
SNMP Model ()				
未启用				~
Web 监控 🚯				
后用网页监控功能				
	1			
		上一步	下一步	収ル



### (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)

*	新增设备 - Syslog 相关设定	×
	Syslog 相关设定 ^	
	Facility ()	
	(22) local use 6 (local6) ~	
	编码方式	
	UTF-8 ~	
	Syslog 正规化资料保留天数上限 🚯	
	Raw Data 保留         ✓ Raw Data 保留         本设备于分时监控报表启动 Syslog 转发时,采用 Raw Data 格式         转发方式将使用来源设备的 IP	
		_
	上一步下一步取消	



#### (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]

其它       ▲         股金銀标       ●         日本       ●         「○       日日         ●       日日	新増设备 - 其	\$					>
快告報告       ()         新注       ()         小       ()         小	其它					^	
Hot       、         新注          新注          新注          小	设备图标						
	Host					~	
会注         余度         () ● 日用 ● () ● () ●	备注						
好度           皮皮状応           ● 月用 ● 伊用	备注						
结度 按收状态 ④ 百用 ● 停用	经纬度			_			
接收状态 ● 后用 ● 停用	纬度		经度				
	接收状态						
		0 ाङ्गतः					
				上一步	下一步	取消	

是否启用默认报表,将应用至相同品牌型号设备 -> 点击 [否]





