



前言

這份文件主要描述如何使用 N-Reporter 管理 IIS 稽核。第一跟第二章節分為 Windows 2003 安裝 IIS 6 環境與 Windows 2008 安裝 IIS 7 環境兩個部份分別說明如何設定 IIS。第三章節為配置 NXLOG· 將 IIS 稽核 log 轉成 syslog 發送到 N-Reporter 接收。

文件章節如下:

1	Windows 20	03 安裝 IIS 6 環境	2
	1.1	設定 IIS 6 Server	2
2	Windows 20	08 安裝 IIS 7 環境	8
	2.1	設定 IIS 7 Server	8
3	配置 NXLOG	· · · · · · · · · · · · · · · · · · ·	.15
4	將設備加入	系統及 Syslog 資料格式及 Facility 的設定	.18
遉	認給資訊		.19

1 Windows 2003 安装 IIS 6 環境

1.1 設定 IIS 6 Server

1. 以系統管理員登入 IIS Server。滑鼠左點[開始]→[系統管理工具]→[網際網路資訊服務(IIS)管理員]。



2. 滑鼠右點[本機電腦],左點[內容]。勾選[網站記錄用 UTF-8 來編碼],左點[確定]。

(115)管理	段		
續檔案正 執行(A) 檢視(V)	視窗(₩) 説明(H)		
	😫 🛄 🖳 🕨 🔳	Ш	
▲ 網際網路咨訊服務	名稱	秋況	
 □	應用程式集區 網站 網頁服務延伸	服務正在執行	
	SQL-SERVER (本機可	[篇) 內容	? ×
	網際網路資訊服務		
	┌── 啓用直接 Metal	base 編輯 (N)	
	允許您在 IIS 執行 └UTF-8 記錄	テ時・編輯 IIS Metabase 設定檔。	
	た許 IIS 使用 UTF	7-8 編碼代替本機字碼頁來寫入記錄項目 [F-8 來編碼(₩)	•
	MIME 類型 IIS 只服務 型清單裡的 案副檔名	副檔名有登錄在 MIME 類 的檔案。若要設定其他檔 ,諸按 [MIME 類型]。	<u>M</u>)
	 確定	取消	說明

註:N-Reporter 新版(Version 3.1.35 之後版本)支援 BIG5、GB2312 編碼。此設定假如沒勾選[網站記錄 用 UTF-8 來編碼]也可以,此時 IIS Server 預設以 BIG5 編碼存儲網站記錄,送出的 syslog 的 message 也是 BIG5 編碼,所以在 N-Reporter 系統新增 IIS 設備時請選擇 BIG5 編碼即可正確設定。 3. 滑鼠左點[本機電腦]右邊的"+",展開[本機電腦]。左點[網站]右邊"+",展開[網站]。

滑鼠右點[預設的網站]或欲稽核的網站,本例右點 " Site 1 " 。再左點[內容]。

🐚 洞際網路資訊服	務 (IIS) 管理員				
🌀 檔案(E) 執行(A) 檢視(V) 視窗(W)	說明(出)			_B×
⇔ ⇒ 🔁 💽	🗡 🗗 🗗 🗟 🖻	■ _ ₽ ▶ ■ ■			
← → 上 III 新際網路資訊服 → SQL-SERVEI → 網站 中→ 網站 中→ 網站 中→ 網訪 中→ 網頭服	(二) (三) (三) </th <th>Log Log Log Log 17. Log mai is.vbs is_old.vbs is_win2k3.vbs is_win2k3.vbs is_win2k8.vbs r_Script.tot </th> <th><u>, 1</u></th> <th><u> </u>大況</th> <th></th>	Log Log Log Log 17. Log mai is.vbs is_old.vbs is_win2k3.vbs is_win2k3.vbs is_win2k8.vbs r_Script.tot 	<u>, 1</u>	<u> </u> 大況	
2 <u> <u> </u> </u>	刪除①) 重新命名(M) 重新整理(P) 匯出清單① 內容(R) 說明(I) 除內容針話士捷。	#-txt			
局日期的进取項日開	有内谷到敌力呢。				

3. 滑鼠左點[網站]。TCP 連接埠輸入 80。如果此站設定 HTTPS 憑證·SSL 連接埠請輸入 443。
 勾選[啟用記錄]。滑鼠左點▼,下拉選[W3C 擴充記錄檔案格式],左點[內容]。

網站識別碼 説明(2): IP 位址(1):	Site 1	3		進階の	
TCP 連接埠(T):	80	- SSL 連接均	월(L): 4 43	2	
✓ 啓用 HTTP 的引 ✓ 啓用記錄(E) 現田的記錄終づ	₩1777年177月(<u>K</u>) 3 .(V)·	5	5		
W3C 擴充記錄 Microsoft IIS 記 NCSA 通用記錄	山 檔案格式 像檔案格式 檔案格式		▼ 内容化		
W3C 擴充記錄	當案格式				

 · 为锟左點[一般],勾選[每小時],勾選[請使用本地時間為檔案命名],左點[瀏覽],選擇記錄檔目
 錄,Windows 2003 預設為" C:\WINDOWS\system32\LogFiles"。網站"
 Site 1 " 選擇 [W3C 擴充記錄檔案格式],產生的 log 放在 W3SVC\$var 資料夾下,檔案格式為
 exyymmddhh.log, \$var 為變數,會因不同網站而改變,本例記錄檔名稱為 W3SVC477399155。
 設定 SyslogAgent 時,請確認 log 路徑為 C:\WINDOWS\system32\LogFiles\W3SVC477399155。

朱內容	
-般 進階	
新增記錄排程 毎小時(田) 毎日(D) 毎周(W) 毎月(M) 沒有限制檔案大小(U) 當檔案大小達到(S): 	
✓ 請使用本地時間爲檔案命名(I)	
記錄檔目錄(上):	
C:\WINDOWS\system32\LogFiles	瀏覽(B)
記錄檔名稱: W3SVC477399155/exyymmddhd	r.log

註:如果 IIS Server 安裝多個網站(Web Sites),欲稽核的網站階請重複設定第 3~5 步驟,並將 log 記錄在多個記錄檔,其名稱為 W3SVC\$var。

☑日期 (da	te)		
☑時間(逝	ne)		
購充内容 □ 田 ⊑ □	業TP 合地 /~	-in)	
● 一戸。	商品证证(C 者名稱(cs-us	emame)	
	名稱 (s-sitena	me)	
- 🖌 伺服器	器名稱 (s-co)	nputername)	
- ▼ 伺服装	器IP 位址(S B海接埠(S	-ip)	
● 回版社	話連接埠(♡) (c∞-method)	port)	
URI 3	、co-uni-s 主體(cs-uni-s	tem)	
URI 1	誓詞 (cs-uri-q	uery)	
- ☑ 通訊	劦定狀態(sc カウス曲線(-status)	
	筋圧士状態()	sc-substatus)	

7. 檢查是否啟用記錄。瀏覽器 access 網站 "Site 1 "後過幾分鐘,開啟記錄檔檢查 log 是否確實記錄。

C:\WINDOWS\system32\LogI	files\₩3S¥C477.	399155				×	
檔案E 編輯E) 檢視(V) 我	的最愛(A) 工具	(I) 説明(H)				/	and the second
3 上一頁 🔹 🕥 🖌 🎾 🎾 搜網	季 🜔 資料夾	\$ 2 × 17					
網址(D) 🗁 C:\WINDOWS\system3	2\LogFiles\W3SVC4	77399155			▶ 🔁 移至	i	<u>-187</u>
名稱 🔺	大小	類型	修改日期	層性			
🗐 u_ex13100416.log	3 KB	文字文件	2013/10/4 下午 05:00	A			
🗐 u_ex13100417.log	2 KB	文字文件	2013/10/4 下午 05:11	A		- 26	
] u_ex13100417.log - 記事本							
檔案(F) 編輯(E) 格式(O) 檢補	蜆(型) 説明(H)						
#Software: Microsoft	Internet Inf	ormation Se	rvices 6.0				
#Version: 1.0							
#Date: 2013-10-04 09:0	08:57						
#Fields: date time s-s	sitename s-i	p cs-method	cs-uri-stem cs-uri	-query s-por	t cs-username c-ip cs	(User-Agent) sc-s	tatus sc-bytes cs-bytes
2013-10-04 09:08:57 W	35VC47739915	5 172.22.0.	63 GET /favicon.icc) - 80 - 172.	.22.0.63 Mozilla/4.0+(compatible;+MSIE+	8.0;+Windows+NT+5.2;+WOW
2013-10-04 09:11:10 W	3SVC47739915	5 172.22.0.	63 GET / - 80 - 172	2.22.0.63 Moz	illa/4.0+(compatible;	+MSIE+8.0;+Window	/s+NT+5.2;+WOW64;+Trident
2013-10-04 09:11:22 W	3SVC47739915	5 172.22.0.	63 GET / - 443 - 17	2.22.0.63 Mc	zilla/4.0+(compatible	;+MSIE+8.0;+Windo	ws+NT+5.2;+WOW64;+Triden
2013-10-04 09:11:22 W	3SVC47739915	5 172.22.0.	63 GET /favicon.icc) - 443 - 172	2.22.0.63 Mozilla/4.0+	(compatible;+MSIE	+8.0;+Windows+NT+5.2;+W0

2 Windows 2008 安装 IIS 7 環境

2.1 設定 IIS 7 Server

以系統管理員登入 IIS Server。滑鼠左點[開始]→[系統管理工具]→[網際網路資訊服務(IIS)管理員]。 1.



2. 設定站台層級的記錄選項。滑鼠雙點本機[WIN2K8]。滑鼠雙點[記錄]。

() (1) WIN2K8 →) 🖾 🖂 🕞 I 🕢 🕶
檔案(F) 檢視(♡) 說明(H)	
建築 WIN2KS 首頁 ● 建設指紹頂 ● 應用程式集區 ● 站台 1 ● ● 站台 ● 站台 ● 站台 1 ● ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ※ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● </th <th> ▲ ● 静理伺服器 ● 重新段動 ● 段動 ● 停止 檢視遮用程式集區 檢視站台 ④ 說明 線上說明 </th>	 ▲ ● 静理伺服器 ● 重新段動 ● 段動 ● 停止 檢視遮用程式集區 檢視站台 ④ 說明 線上說明
就維	G ^a

3. 滑鼠左點[每下列項目一個記錄檔]中的▼,下拉選[站台]。記錄檔下拉選[W3C],

滑鼠左點[選取欄位]。

檔案(P) 檢視(V) 說明(E) 建線 ● <t< th=""></t<>
連線 記録 ● 認知 ● 記録 ● 認知 ● 認知 ● 認知 ● 認知 ● 認知 ● 記録 ● 認知 ● 記録 ● 認知 ● 記録 ● 記録
記錄檔塑換 選取 IIS 用來建立新記錄檔的方法。 ④ 排程(C): 每小時 ● 個案大小上限 (位元組)(Z): ● ● ● 「不要建立新記錄檔(N) ● 使用本地時間為檔案命名(U)

4. [W3C 記錄欄位]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) 、伺服器名稱(s-computername)、伺服器 IP(s-ip) 、伺服器連接 Port(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)、已傳 送位元組(sc-bytes)、已接收位元組(cs-bytes) 、花費時間(time-taken)、使用者代理(cs(User-



Agent))。按[確定]。

按[瀏覽],選擇記錄檔目錄,Windows 2008 預設為"%SystemDrive%\inetpub\logs\LogFiles "。
 編碼選擇[UTF-8]。勾選[排程],下拉選[每小時]。

勾選[使用本地時間為檔案命名]。按[套用]完成站台層級的設定。

当Internet Information Services (IIS) 管理員	
 福来(t) 被視(v) 致時(d) 正 (x) (x) (x) (x) (x) (x) (x) (x) (x) (x)	 5 新作 東方 停用 被視記錄檔 ? 說明 線上說明
設定: localhost'applicationHost.config	G1.

註:N-Reporter 新版(Version 3.1.35 之後版本)支援 BIG5、GB2312 編碼。此設定假如選 BIG5 編碼,

IIS Server 以 BIG5 編碼存儲網站記錄,送出的 syslog 的 message 也是 BIG5 編碼,

所以在 N-Reporter 系統新增 IIS 設備時請選擇 BIG5 編碼。

 設定個別站台的記錄選項。雙點[站台],展開所有 Site。滑鼠右點欲稽核的網站 "IIS 7 Site 1 ", 再雙點[記錄],設定此網站的 log 路徑。

Timeinet intoimanon seivices (115) 日·社員	
③ ● → WIN2K8 → 站台 → IIS 7 Site 1 →	💮 I 🕜 🗸
檔案(F) 檢視(V) 說明(H)	
 ● Finance Fail + Internet + ● WIN2EB (WIN2EB Administrator) ● Bable Babl	(https)
近流 依視 近流 依視 近 () 許容依視 近 () 許容依相 近 () 許否	

7. 記錄檔下拉選[W3C]·滑鼠左點[選取欄位]。

檔案(F) 檢視(Y) 說明(H)	
課題 ● <th> 勤作 承用 予約 使用 檢視記錄檔 ② 說明 線上說明 </th>	 勤作 承用 予約 使用 檢視記錄檔 ② 說明 線上說明

 [W3C 記錄欄位]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) 、伺服器名稱(s-computername)、伺服器 IP(s-ip) 、伺服器連接 Port(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)、已傳 送位元組(sc-bytes)、已接收位元組(cs-bytes) 、花費時間(time-taken)、使用者代理(cs(User-Agent))。按[確定]。

注: 若已在步驟 3、4 設定記錄欄位, 並檢查一致, 請左點[取消]。

9. 按[瀏覽],選擇記錄檔目錄,Windows 2008 預設為"%SystemDrive%\inetpub\logs\LogFiles"。
 勾選[排程],下拉選[每小時]。勾選[使用本地時間為檔案命名]。按[套用]完成站台"IIS 7 Site 1"
 設定。

[%] Internet Information Services (IIS) 管理員	
③ ● → WIN2K8 → 站台 → HS 7 Site 1 →) 🖾 🖂 🎲 I 🙆 🗸
檔案(F) 檢視(V) 說明(H)	
Setation Constrained by the state of	 bht 家用 取済 停用 検視記録描 予 説明 線上説明
設定: localhost applicationHost.config ' <location path="IIS 7 Site 1"></location>	GI.:

註:如果沒設定站台層級的記錄選項,編碼選擇請一定要選擇 [UTF-8]。

註:如果 IIS Server 有多個站台,每個站台皆需設定第 6~9 步驟。

10. 若 IIS Server 有多個站台,每個 Site 的記錄檔案為 W3SVC\$var,其中\$var 為變數。

請確認 IIS 7 Site 1 的記錄檔案正確路徑。例如下圖為兩個站台的記錄檔。



下圖知, IIS 7 Site 1 的站台 IP 為 172.22.0.79:443。

°≇Internet Information Services (IIS) 참컉	員					<u>_ ×</u>
③ ⑥ ▶ WIN2K8 ▶ 站台 ▶						😐 🖂 🟠 I 🔞 🔹
檔案(F) 檢視(∀) 說明(H)						
連線						動作
💐 🔛 🖄 😣						
- Si 起始網頁 - Si WIN2K8 (WIN2K8)&dministrator)	篩選器:	→ ∰移至(G) → 駴	全部顯示(A) 群組依據: 沒有	分組 🔹		設定網站預設值
·····································	名稱 🔺	ID 狀態		繁結	路徑	😧 說明
Big Opfault Web Site Big Opfault Big		1 日散動 (http) 2 日歌動 (http) 3 日歌動 (http)	,不明 (nettrp), 不明 (netpip	*80 (http),808:* (net.trp),* (net.pipe) 172.22.0.79:443 (https) 192.168.2.79:80 (http)	Clinetpublwww Clishare_folder Clishare_folder	級上說明
	< 回功能檢視 一 の容	檢視			F	

檢查 W3SVC2 和 W3SVC1 的 log · 得知站台 " IIS 7 Site 1 " 的記錄檔路徑為

C:\inetpub\logs\LogFiles\W3SVC2 •

檢查是否啟用記錄。瀏覽器 access 網站 "IIS 7 Site 1 "後過幾分鐘,開啟記錄檔檢查 log 是否確 實記錄。

■ u_ex15112615 - 宝事本	_ 🗆 🗵
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)	
#Software: Microsoft Internet Information Services 7.0 #Version: 1.0	_
#Date: 2015-11-26 07:03:16	hon
2015-11-26 07:03:16 WIN2K8IIS 172.22.0.79 GET / - 443 - 172.22.0.166 403 1317 266 930	ken 🚽
I	

3 配置 NXLOG

- 1. 以系統管理者 Administrator 登入 IIS Server。
- 2. 下載 NXLOG: http://sourceforge.net/projects/nxlog-ce/files/

下載『nxlog-ce-x.x.x.msi』。

3. 安裝 NXLOG: 滑鼠左點『nxlog-ce-x.x.x.msi』, 安裝 NXLOG。

註:32 位元作業系統 NXLOG 安裝在 " C:\Program Files\nxlog\conf\nxlog.conf " 。

64 位元作業系統 NXLOG 安裝在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "。

4. 配置 NXLOG:

(1) 下載 IIS NXLOG 配置檔 nxlog_iis.conf:

瀏覽 URL: http://www.npartnertech.com/download/tech/nxlog_iis.conf

編輯 NXLOG 設定檔 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。將 IIS NXLOG 配置

檔設定貼上並覆蓋 nxlog.conf 設定。。

## This is a sample configuration file. See the nxlog reference manual about the							
## online at h	## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html						
## Please set	## Please set the ROOT to the folder your nxlog was installed into,						
## otherwise i	## otherwise it will not start.						
#define ROO	F C:∖Program Files∖nxlog						
define ROOT	C:\Program Files (x86)\nxlog						
Moduledir %R	OOT%\modules						
CacheDir %R	OOT%\data						
Pidfile %ROO	T%\data\nxlog.pid						
SpoolDir %R0	DOT%\data						
LogFile %RO	OT%\data\nxlog.log						
<extension sy<="" th=""><th>islog></th></extension>	islog>						
Module	xm_syslog						
define IIS_SIT	'E1 C:\inetpub\logs\LogFiles\W3SVC1						
<input in_iis_s<="" th=""/> <th>site1></th>	site1>						
Module	im_file						
#File	'%IIS_SITE1%\ex*.log'						
File	'%IIS_SITE1%\u_ex*.log'						
SavePos	TRUE						
#define IIS_S	TE2 C:\inetpub\logs\LogFiles\W3SVC2						
# <input in_iis<="" th=""/> <th>_site2></th>	_site2>						
# Module							
# #File	'%IIS_SITE2%\ex*.log'						
# File	'%IIS_SITE2%\u_ex*.log'						
# SavePos	TRUE						
#							
<output out_i<="" th=""><th>is></th></output>	is>						
Module	om_udp						
Host	192.168.2.3						
Port	514						
Exec	\$SyslogFacilityValue = 22;						
Exec	<pre>\$raw_event = "IIS [info] " + \$raw_event ;</pre>						
Exec	to_syslog_bsd();						
<route iis=""></route>							
Path	in_iis_site1 => out_iis						
#Path	in_iis_site1,in_iis_site2 => out_iis						

- a. **綠色部位**請選擇 NXLOG 正確的安裝路徑[,] 本例環境為 64 位元系統選擇 " define ROOT C:\Program Files (x86)\nxlog " 。
- b. 黃色部分"define IIS_SITE1 \$dir "行中的\$dir 請輸入 IIS Server 站台的記錄路徑, 本例路徑為 " C:\inetpub\logs\LogFiles\W3SVC2 "。
- c. **紅色部分**"Host \$N_Reporter_IP"行中的\$N-Reporter_IP 改成 N-Reporter IP[,] 本例 IP 為 192.168.2.3[。]
- d. 本例 IIS 站台的編碼為 UTF-8,記錄檔的格式為 u_ex*.log,所以設定為

"File '%IIS_SITE1%\u_ex*.log' "。如果 IIS 站台的記錄為 BIG5 或 GB2312 編碼, 則記錄檔的格式為 ex*.log,請將設定改為 "File '%IIS_SITE1%\ex*.log' "。 本例配置範例:



e. 如果 IIS Server 為多個站台,請刪除配置範例第 22~28 行的註解符號"#",定義第二個站台的 儲存路徑 IIS_SITE2 與新增 input 的 in_iis_site2,並且選擇第 38 行設定 " Path in_iis_site1,in_iis_site2 => out_iis ",將兩個台站的 log 轉成 syslog 送出。

- (2) 啟動 NXLOG: 選擇 步驟 a 利用 [命令提示字元] 啟動 NXLOG 或 步驟 b [服務] 啟動 NXLOG。
- a. [開始]→[所有程式]→[應用附屬程式]·滑鼠右點[命令提示字元]·左點[執行身分]· 以系統管理員身分執行。

命令提示字元輸入:



- b. [開始]→[所有程式]→[系統管理工具]→[服務], 右點服務[nxlog], 左點[啟動]或
 [重新啟動]。
- (3) 檢查 NXLOG 是否正常啟動:

檢查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log " · 沒有顯示 Error 的訊

息,表示正常啟動。



- 4 將設備加入系統及 Syslog 資料格式及 Facility 的設定
- (1) 登入 N-Reporter / N-Cloud 系統



(3) 滑鼠點選 [未知設備的編輯圖示]·在 IP 欄位中應該能看見此台的設備的 IP。請輸入一個方便記 憶的設備名稱·接著在[資料格式]下拉選單中選擇{IIS}·Facility 選(22)·勾選[啟動接收]·按下

[確定],即完成 IIS 設備系統新增程序

G	設備管理 ▶ Syslog 設備 🗌 頁面自動更新 (120秒)			新增或編輯Syslog設備			×
	所屬:頁域 ▶	All Devices	 	step 1	區域: 名稱·	Root	~
0	總筆数:15				設備IP:	192.168.2.79	
2	17F	PT/> 圖·賀邓 ◆	19		設備種類:	□ Action 設備	~
	_	未知設備			資料格式:	IIS	~
	S	(Global)			Facility:	(22) local use 6 (local6)	\sim
					語系:	UTF8	\sim
	1	未知設備 (Global)	192.168.2.15	step 2	接收狀態: 所屬資料夾:	● 啟動接收 ○ 暫停接收 其他 [18]	~
	S W	Global	192.168.0.251			砳	定取消

18



連絡資訊 N-Partner 公司連絡方式: TEL: +886-4-23752865 FAX: +886-4-23757458 有關技術問題請洽: Email: support@npartnertech.com Skype : support@npartnertech.com

有關業務相關問題請洽:

Email: sales@npartnertech.com

