N-Partner

N-REPORTER

如何管理 IIS 稽核

V 011 (繁體)

2017/9/18

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。

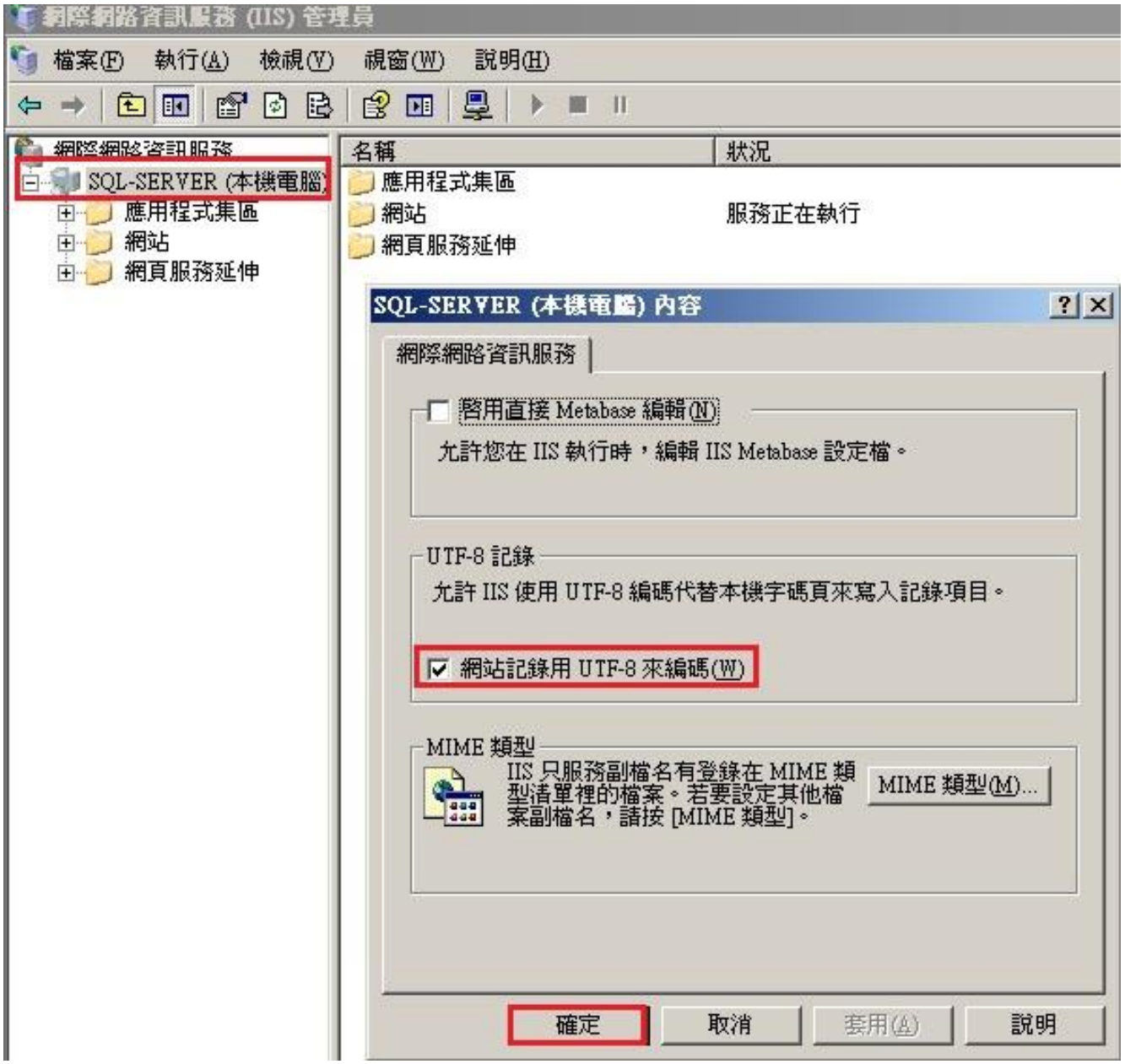
文件章節如下：

1 Windows 2003 安裝 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]。

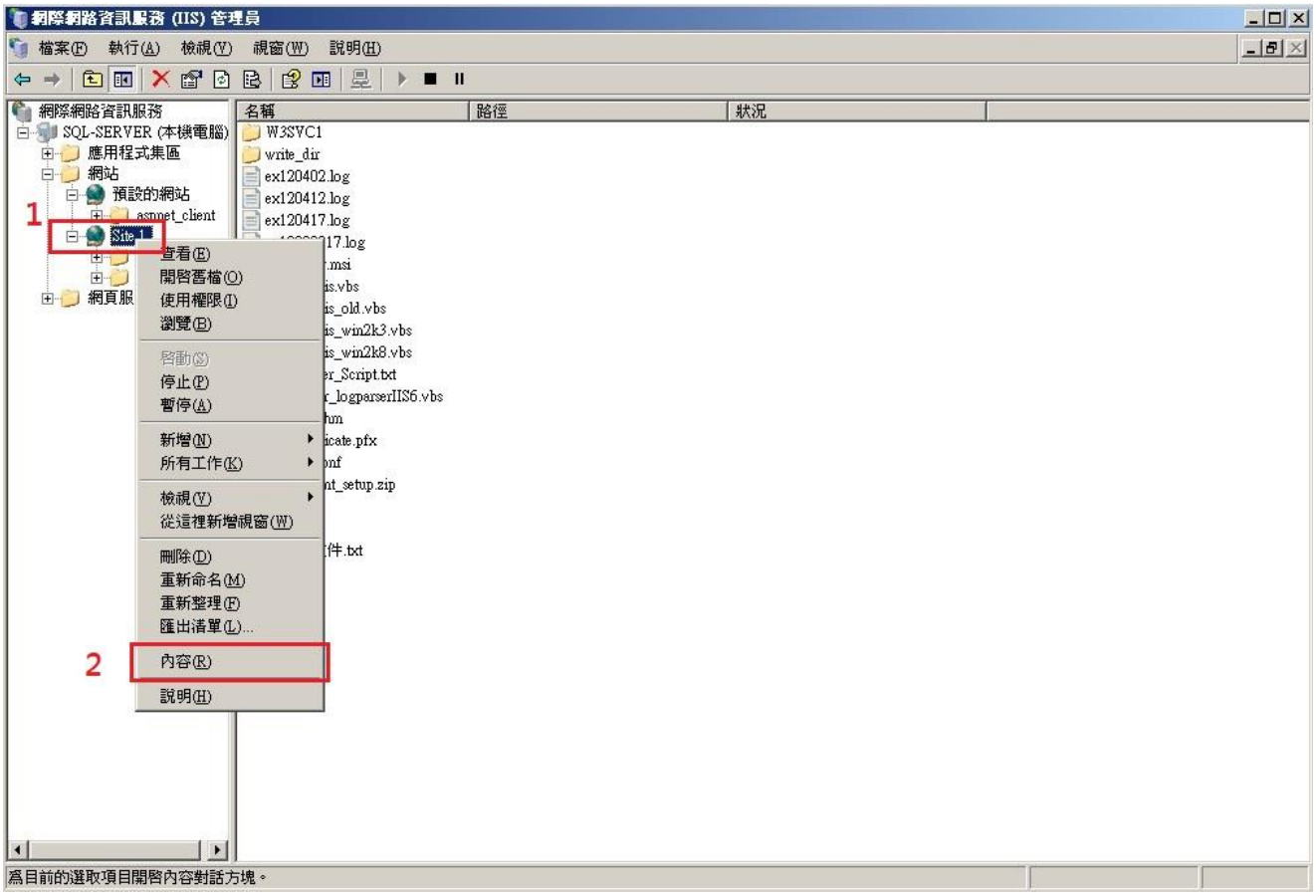
2. 滑鼠右點[本機電腦]，左點[內容]。勾選[網站記錄用 UTF-8 來編碼]，左點[確定]。



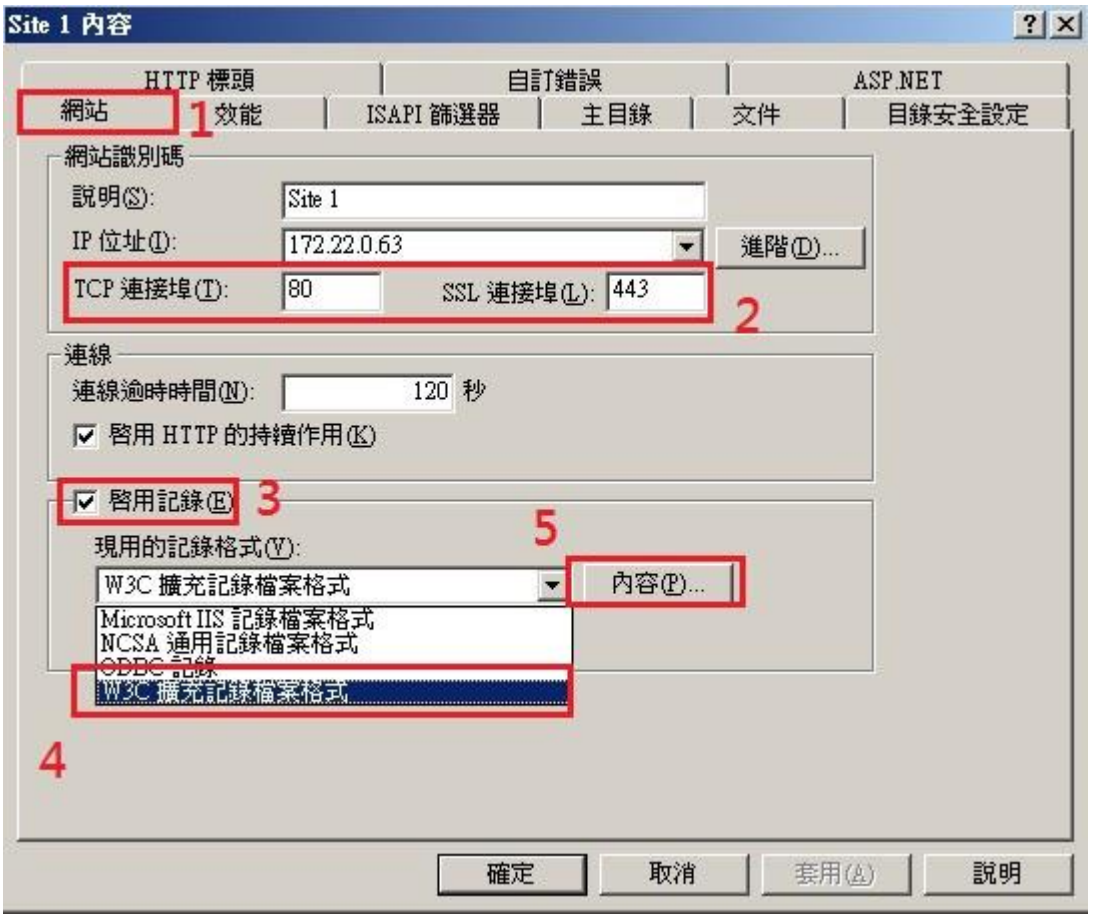
註:N-Reporter 新版(Version 3.1.35 之後版本)支援 BIG5、GB2312 編碼。此設定假如沒勾選[網站記錄用 UTF-8 來編碼]也可以，此時 IIS Server 預設以 BIG5 編碼存儲網站記錄，送出的 syslog 的 message 也是 BIG5 編碼，所以在 N-Reporter 系統新增 IIS 設備時請選擇 BIG5 編碼即可正確設定。

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]。

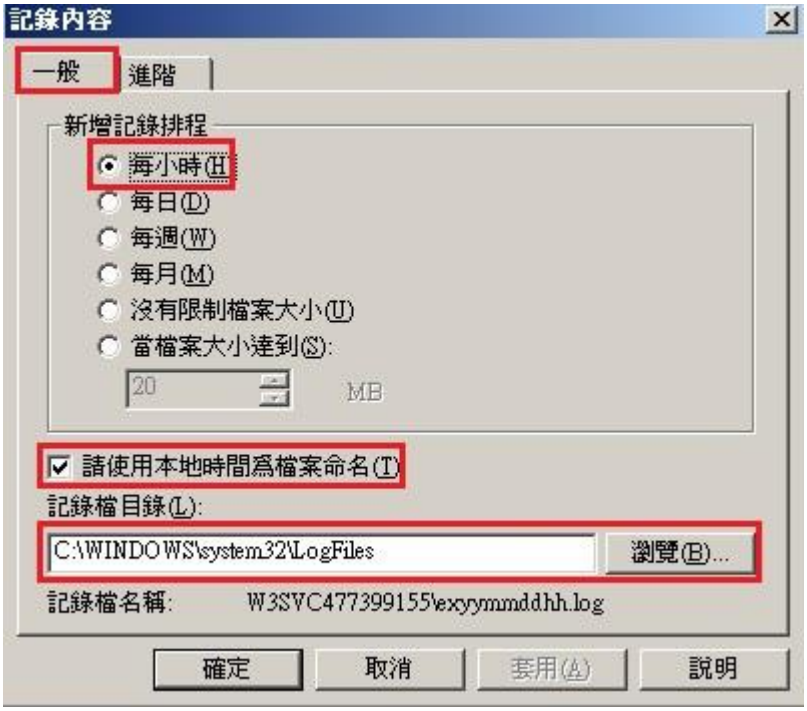
   滑鼠右點[預設的網站]或欲稽核的網站，本例右點 " Site 1 " 。再左點[內容]。



4. 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]。



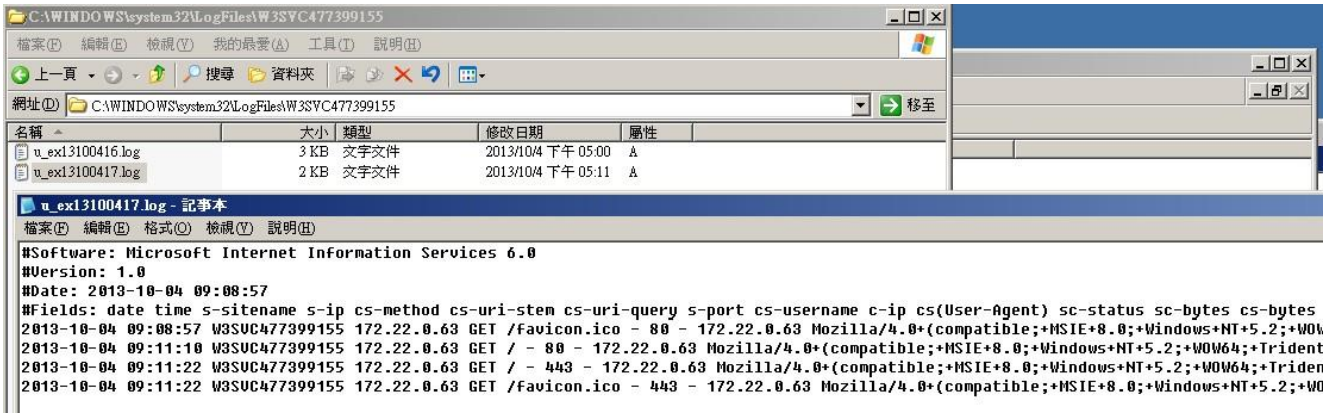
5. 滑鼠左點[一般]，勾選[每小時]，勾選[請使用本地時間為檔案命名]，左點[瀏覽]，選擇記錄檔目錄，Windows 2003 預設為"　C:\WINDOWS\system32\LogFiles"。網站 " Site 1 " 選擇 [W3C 擴充記錄檔案格式]，產生的 log 放在 W3SVC$var 資料夾下，檔案格式為 exyymmddhh.log，$var 為變數，會因不同網站而改變，本例記錄檔名稱為 W3SVC477399155。設定 SyslogAgent 時，請確認 log 路徑為 C:\WINDOWS\system32\LogFiles\W3SVC477399155。



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。

6. 滑鼠左點[進階]。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) 、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。再按確定，完成設定。

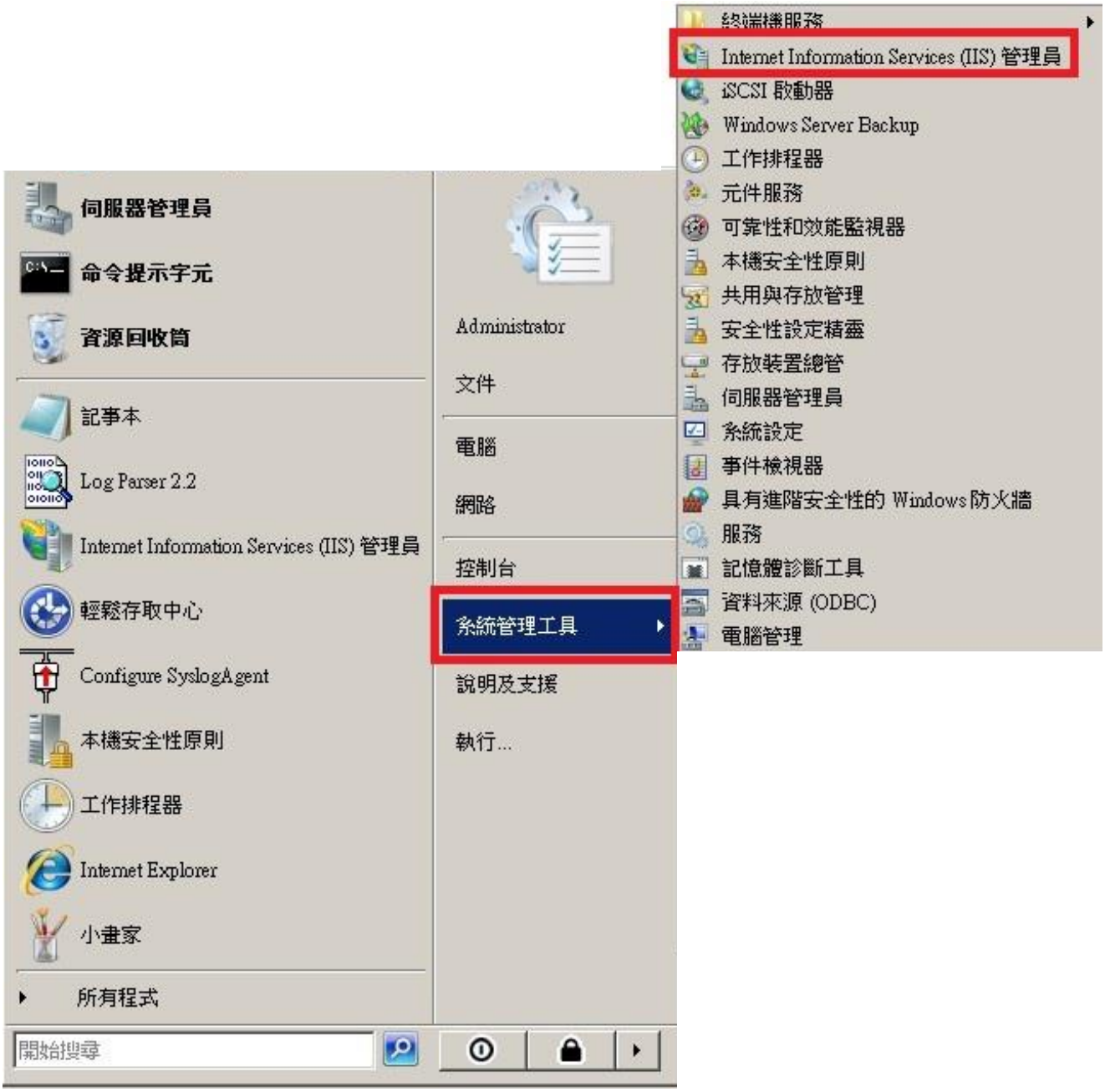
7. 檢查是否啟用記錄。瀏覽器 access 網站 " Site 1 " 後過幾分鐘，開啟記錄檔檢查 log 是否確實記錄。



2 Windows 2008 安裝 IIS 7 環境

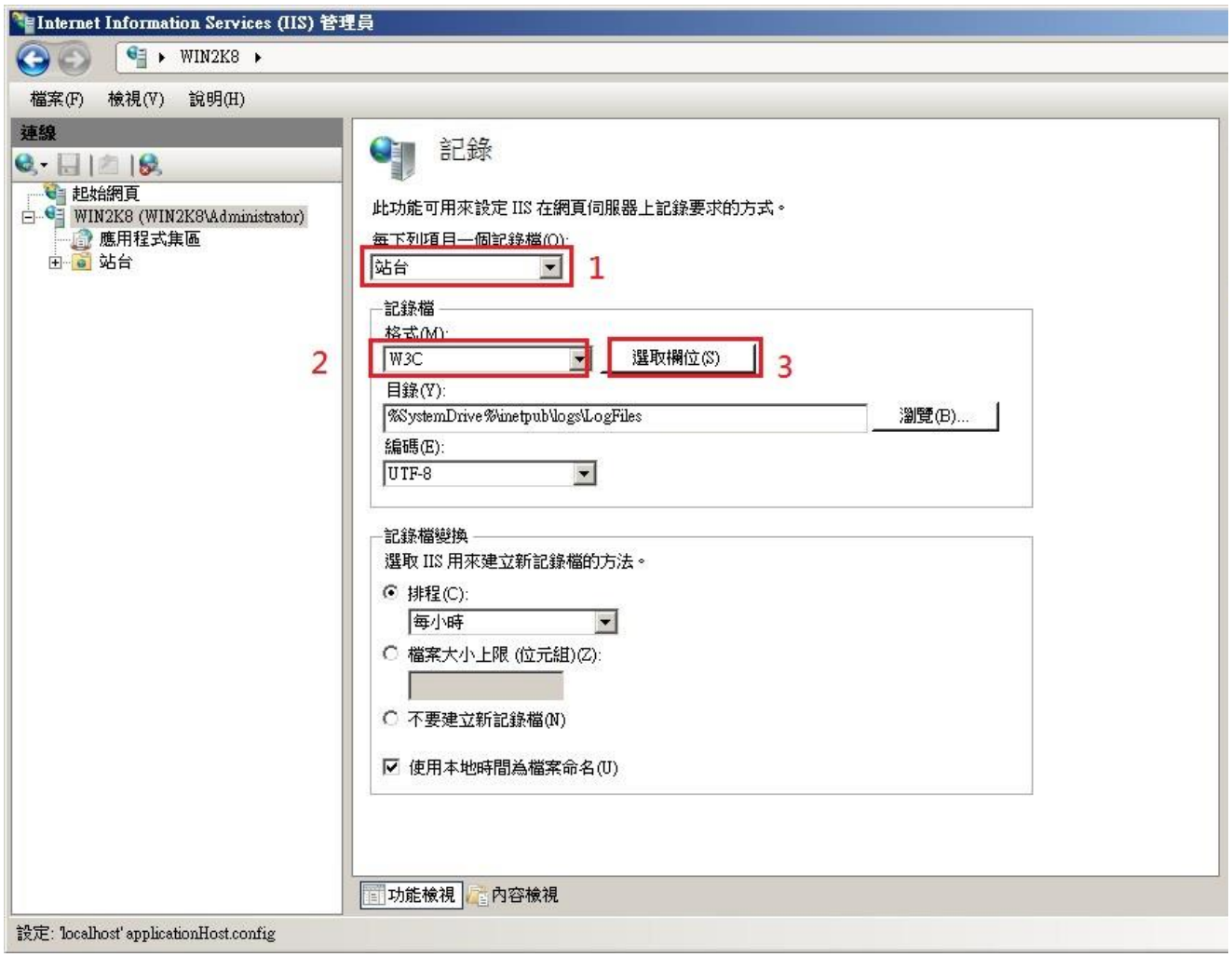
2.1 設定 IIS 7 Server

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]。

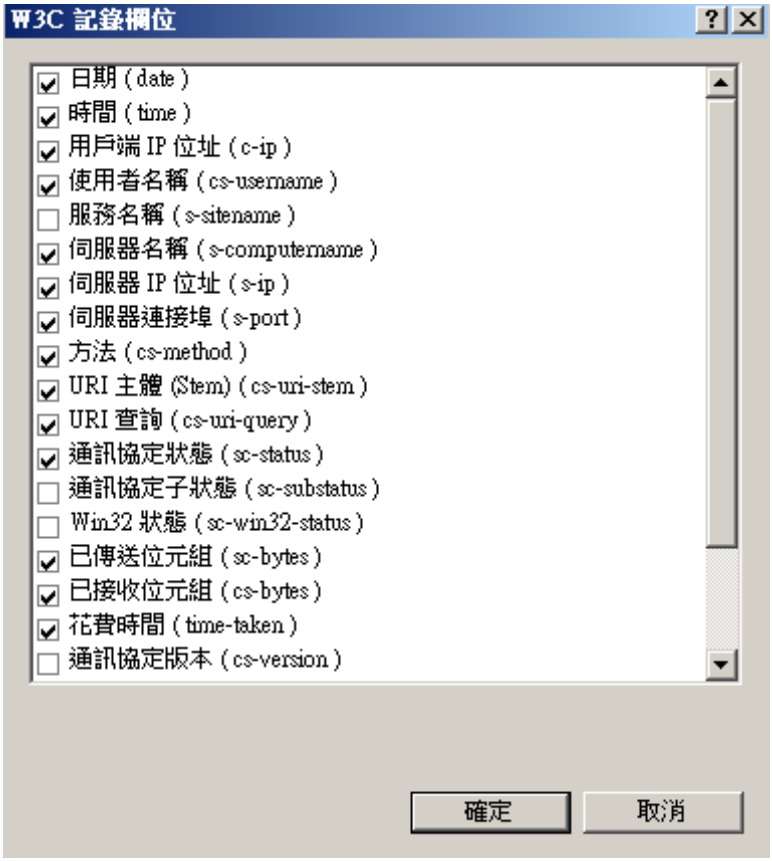


2. 設定站台層級的記錄選項。滑鼠雙點本機[WIN2K8]。滑鼠雙點[記錄]。

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]。



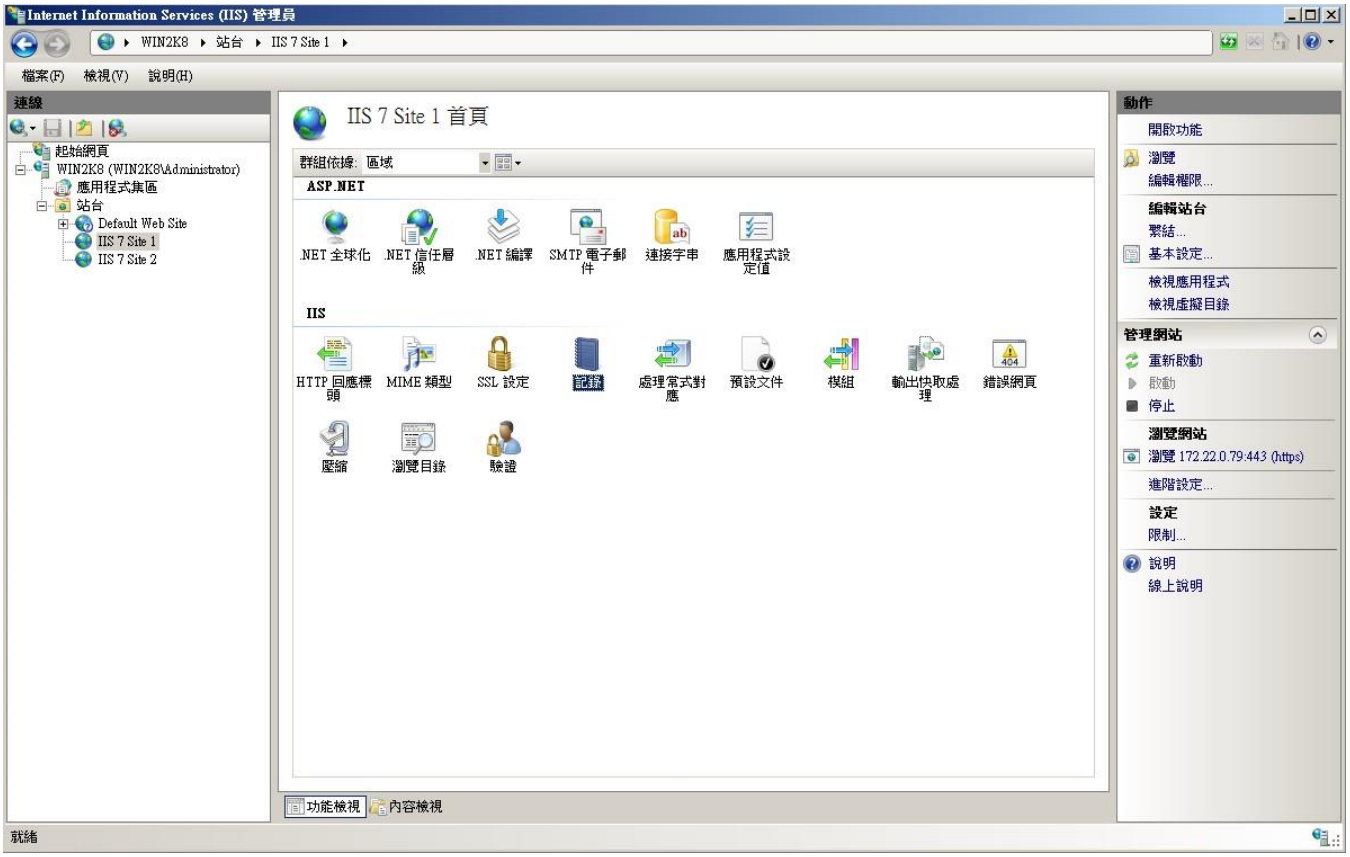
4. [W3C 記錄欄位]選項勾選日期(date)、時間(time) 、用戶端 IP 位址(c-ip) 、使用者名稱(cs_username) 、伺服器名稱(s-computername)、伺服器 IP(s-ip) 、伺服器連接 Port(s-port)、方法(cs-method)、URI 主體(cs-uri-stem)、URI 查詢(cs-uri-query) 、通訊協定狀態(sc-status)、已傳送位元組(sc-bytes)、已接收位元組(cs-bytes) 、花費時間(time-taken)、使用者代理(cs(User-Agent))。按[確定]。



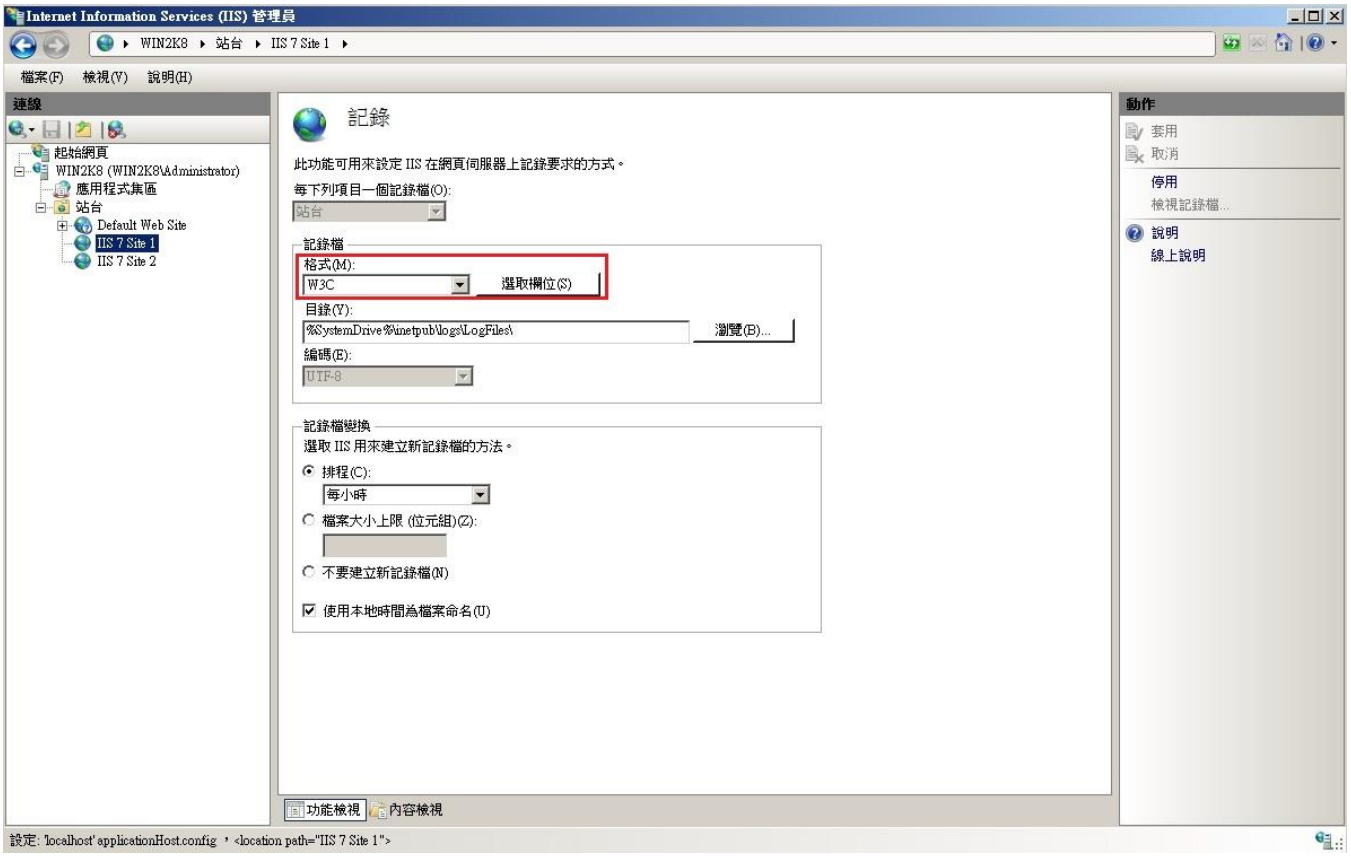
5. 按[瀏覽]，選擇記錄檔目錄，Windows 2008 預設為" %SystemDrive%\inetpub\logs\LogFiles "。
編碼選擇[UTF-8]。勾選[排程]，下拉選[每小時]。
勾選[使用本地時間為檔案命名]。**按[套用]完成站台層級的設定。**

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。

6. 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。



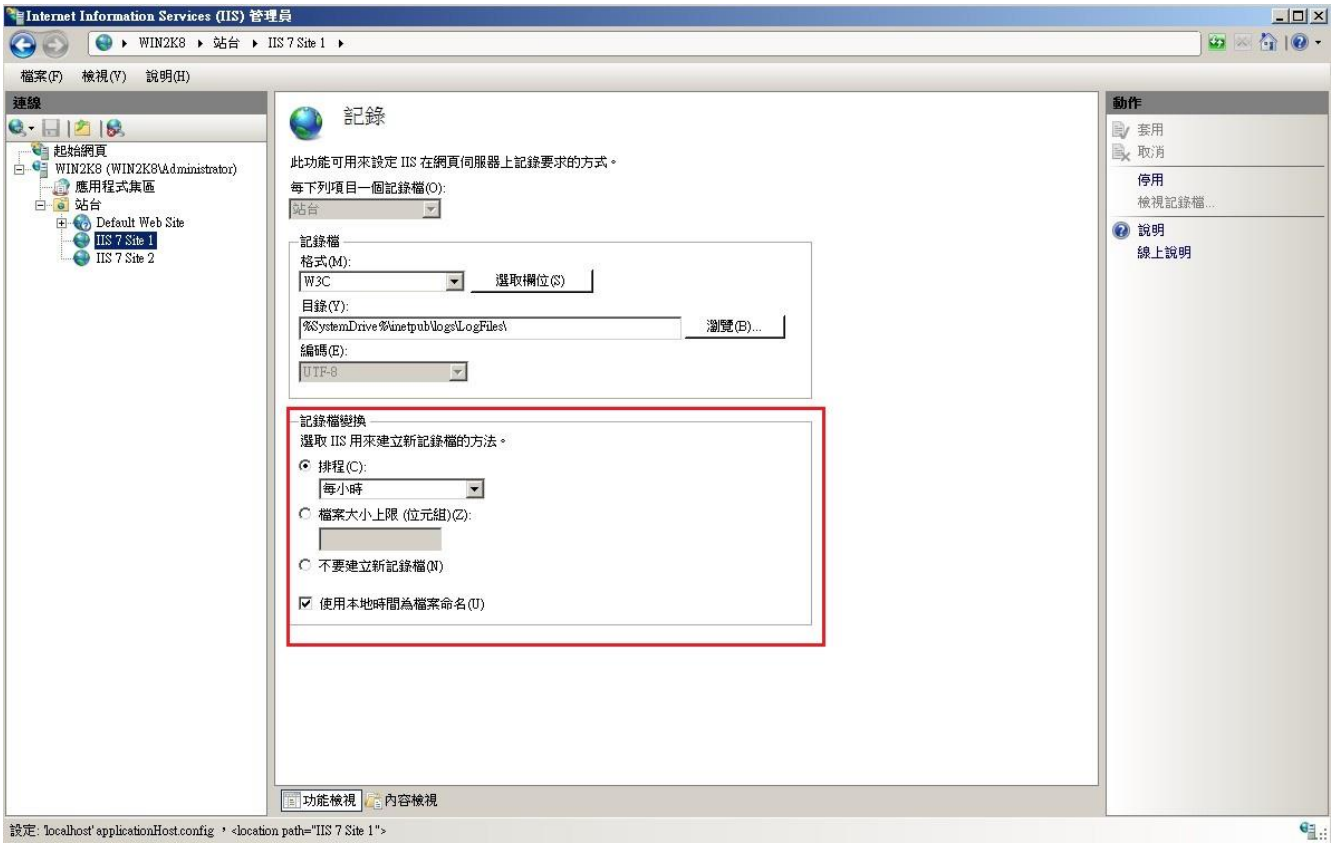
7. 記錄檔下拉選[W3C]，滑鼠左點[選取欄位]。



8. [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。**

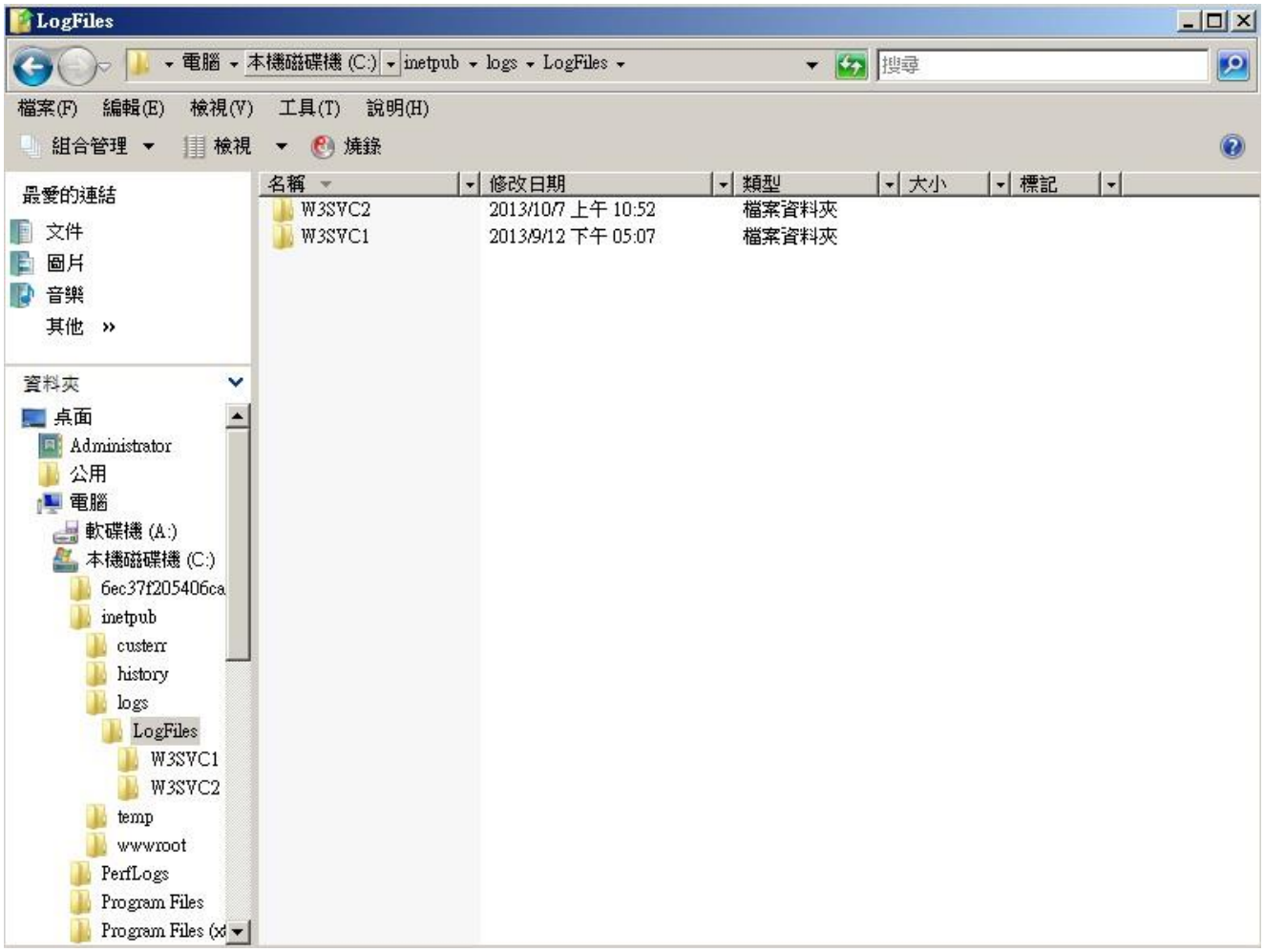


註：如果沒設定站台層級的記錄選項，編碼選擇請一定要選擇 [UTF-8]。

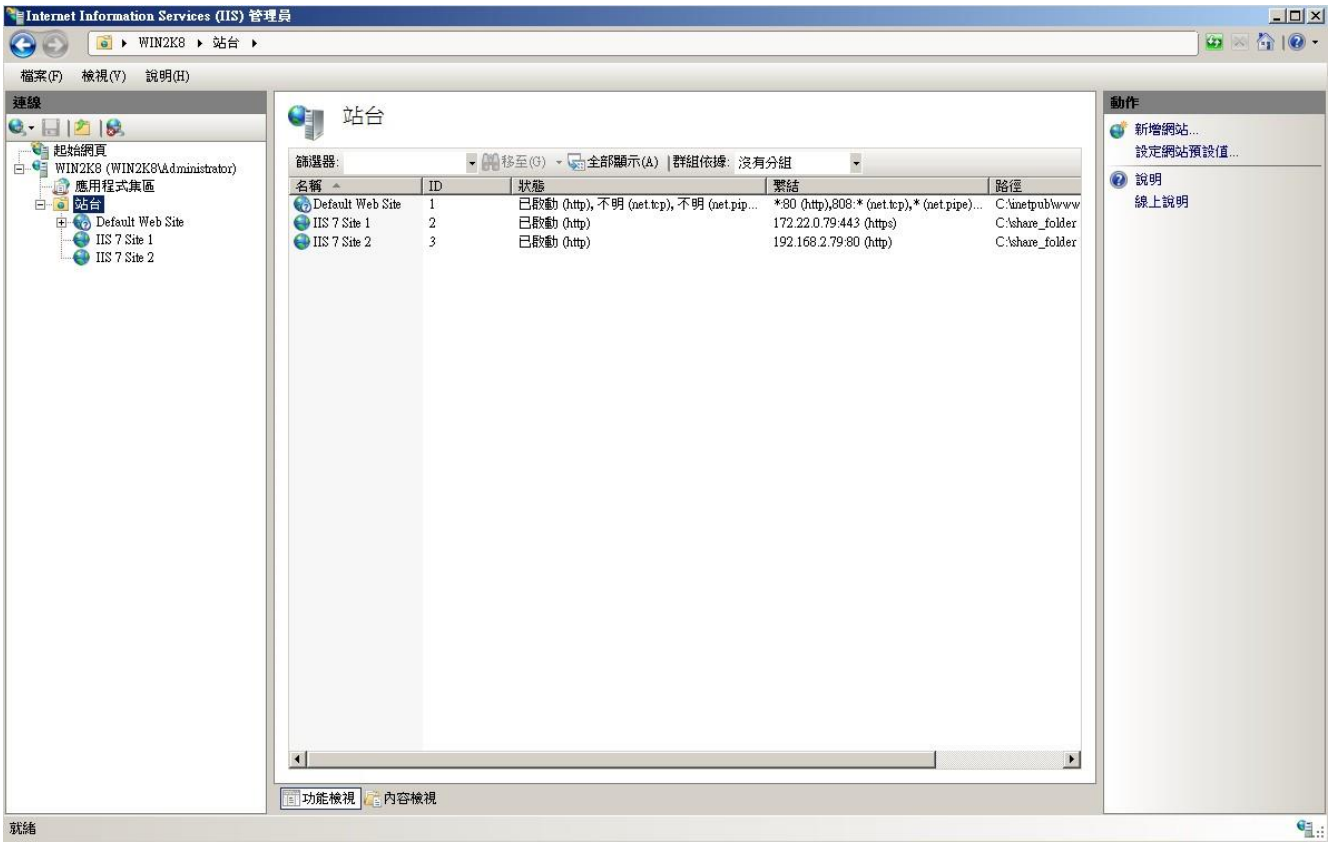
註：如果 IIS Server 有多個站台，每個站台皆需設定第 6~9 步驟。

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。

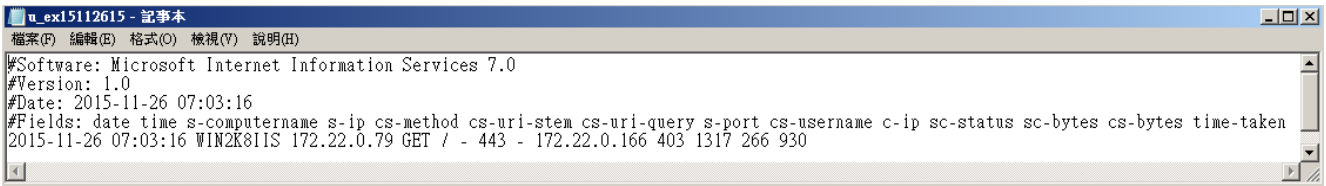


下圖知，IIS 7 Site 1 的站台 IP 為 172.22.0.79:443。



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。



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 http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.
#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
<Extension syslog>
   Module       xm_syslog
</Extension>
define IIS_SITE1 C:\inetpub\logs\LogFiles\W3SVC1
<Input in_iis_site1>
    Module        im_file
    #File          '%IIS_SITE1%\ex*.log'
    File           '%IIS_SITE1%\u_ex*.log'
    SavePos       TRUE
</Input>
#define IIS_SITE2 C:\inetpub\logs\LogFiles\W3SVC2
#<Input in_iis_site2>
#    Module        im_file
#    #File          '%IIS_SITE2%\ex*.log'
#    File           '%IIS_SITE2%\u_ex*.log'
#    SavePos       TRUE
#</Input>
<Output out_iis>
    Module     om_udp
    Host       192.168.2.3
    Port       514
    Exec       $SyslogFacilityValue = 22;
    Exec       $raw_event = "IIS [info] " + $raw_event ;
    Exec       to_syslog_bsd();
</Output>
<Route iis>
    Path           in_iis_site1 => out_iis
    #Path           in_iis_site1,in_iis_site2 => out_iis
</Route>
```

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，

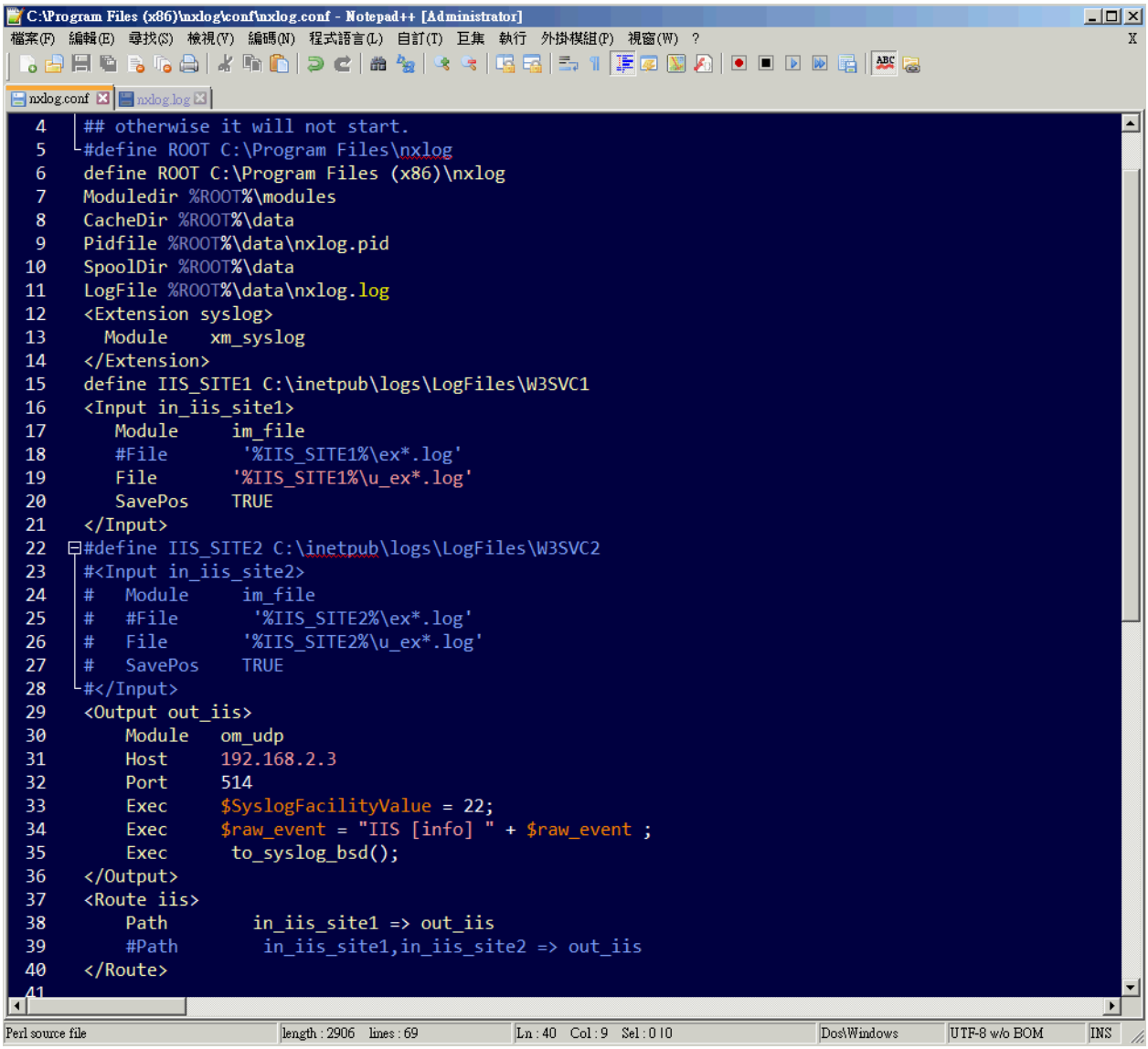
本例路徑為 " C:\inetpub\logs\LogFiles\W3SVC2 " 。

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。

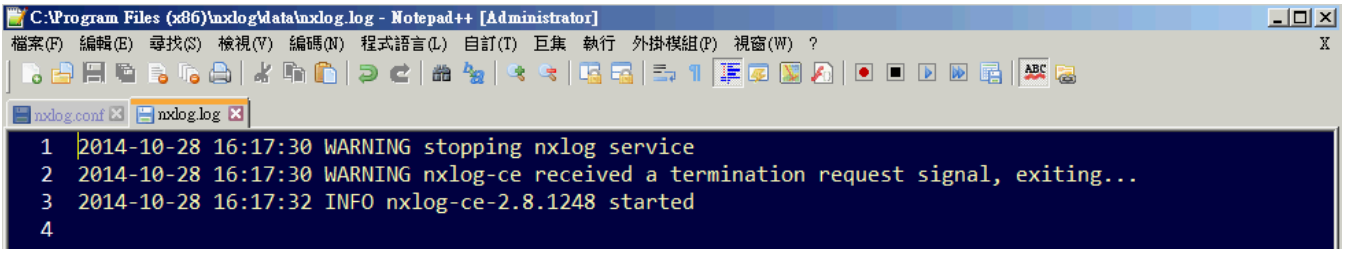
命令提示字元輸入：

```
net stop nxlog
net start nxlog
```

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

(2) 滑鼠點選[設備管理 / Syslog 設備]

(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

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

N-Partner