N-Partner

N-REPORTER

如何管理 IIS 审核

V 1.1.10 (简体)

(01-01-02-003) 2017/4/17

前言

这份文件主要描述如何使用 N-Reporter 管理 IIS 审核。

第一步分为 Windows 2003 安装 IIS 6 环境与 Windows 2008 安装 IIS 7 环境两个部份分别说明如何设定 IIS。

第二步为配置 NXLOG，将 IIS 稽核 log 转成 syslog 发送到 N-Reporter 接收。

本文件章节

连络信息

N-Partner 公司连络方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有关技术问题请洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有关业务相关问题请洽：

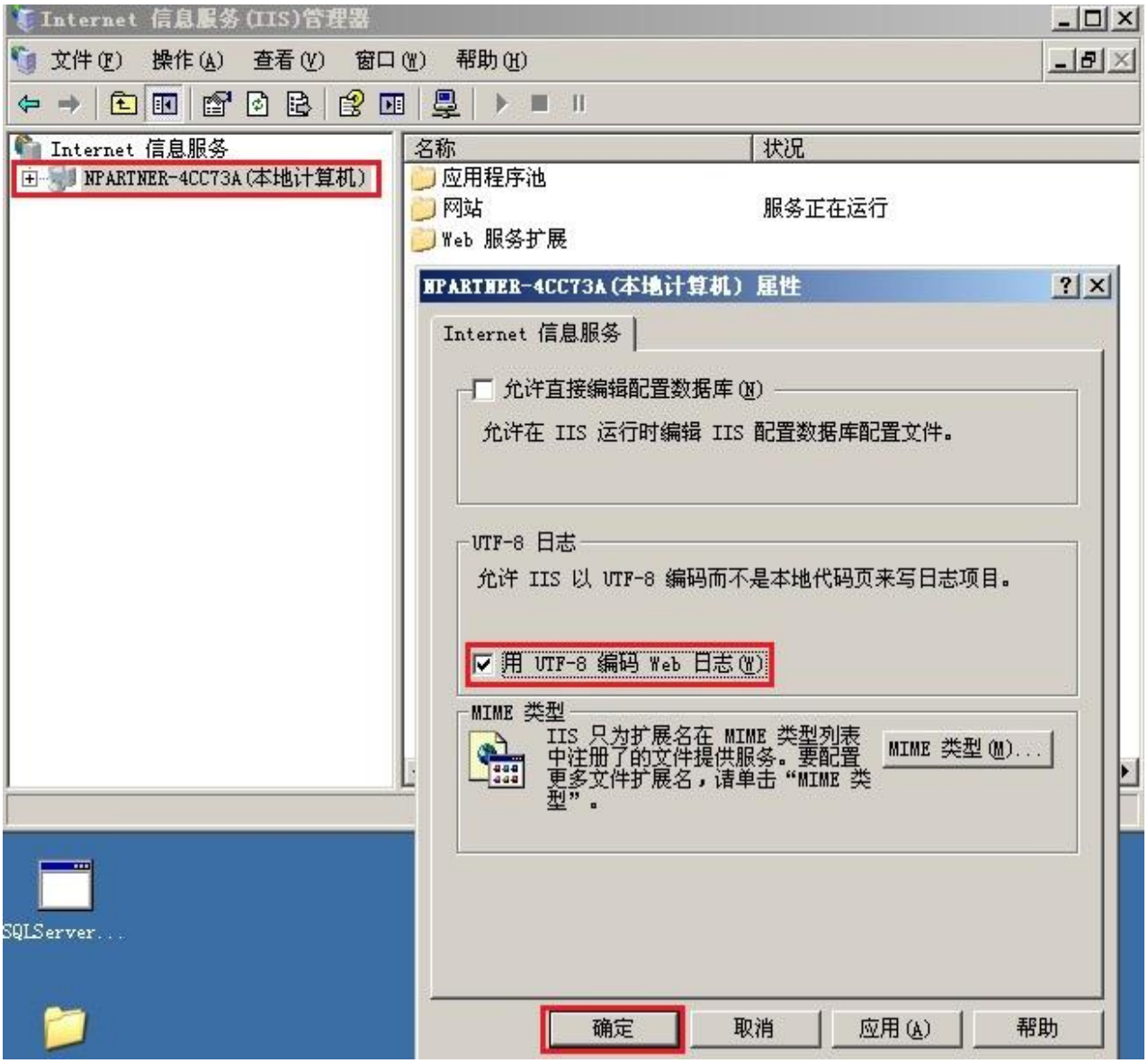
Email: sales@npartnertech.com

1 Windows 2003 安装 IIS 6 环境

1.1 设定 IIS 6 Server

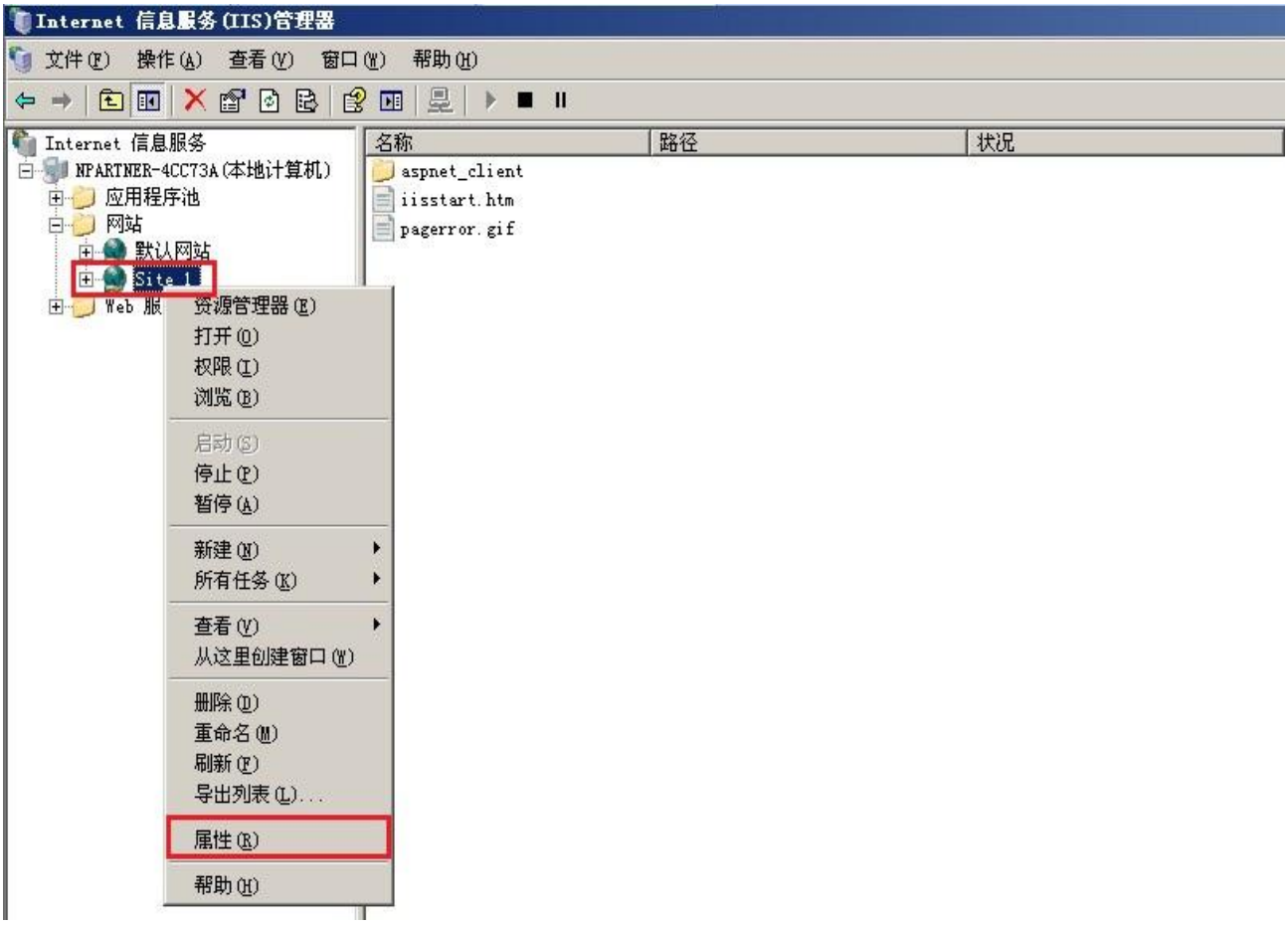
1. [开始]→[管理工具]→[Internet 信息服务(IIS)管理器]。

2. 鼠标右点[本地计算机]，左点[属性]。勾选[用 UTF-8 编码 Web 日志(W)]，左点[确定]。

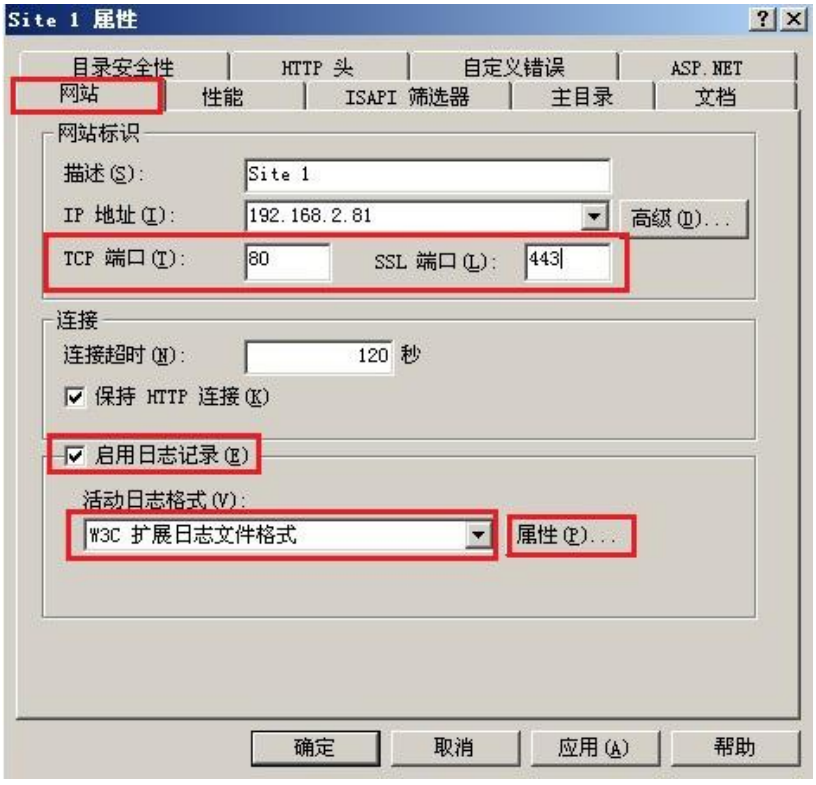


注:N-Reporter 新版(Version 3.1.35 之后版本)支持 BIG5、GB2312 编码。此设定假如没勾选[用 UTF-8 编码 Web 日志(W)] 也可以，此时 IIS Server 默认以 GB2312 编码存储 Web 日志，送出的 syslog 的 message 也是 GB2312 编码，所以在 N-Reporter 系统新增 IIS 设备时请选择 BIG5 编码即可正确配置。

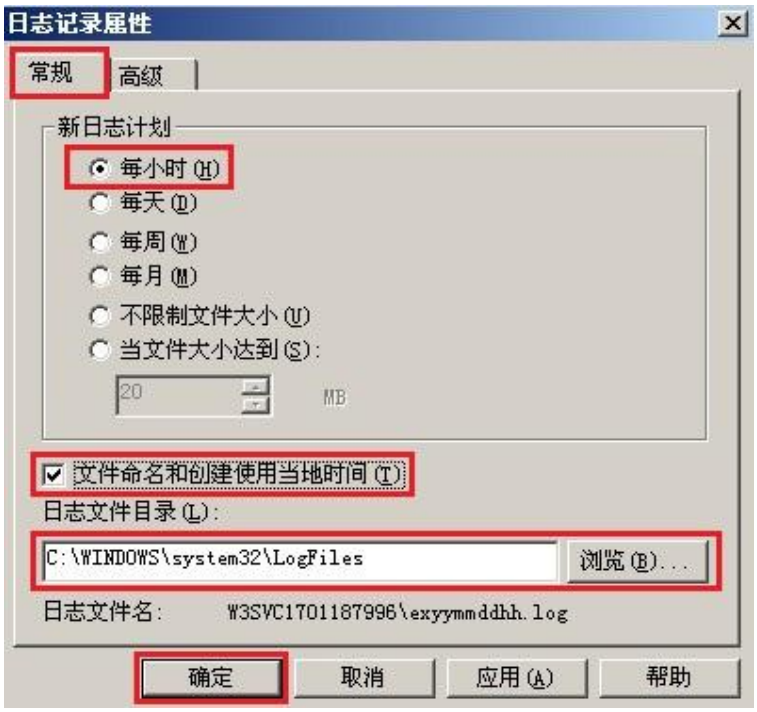
3. 鼠标左点[本地计算机]右边的"+"，展开[本地计算机]。左点[网站]右边"+"，展开[网站]。鼠标右点[默认的网站]或欲审核的网站，本例右点 " Site 1 " 。再左点[属性]。



4. 鼠标左点[网站]。TCP 端口输入 80。如果此站设定 HTTPS 凭证，SSL 端口请输入 443。勾选[启用日志记录]。鼠标左点▼，下拉选[W3C 扩展日志记录文件格式]，左点[属性]。



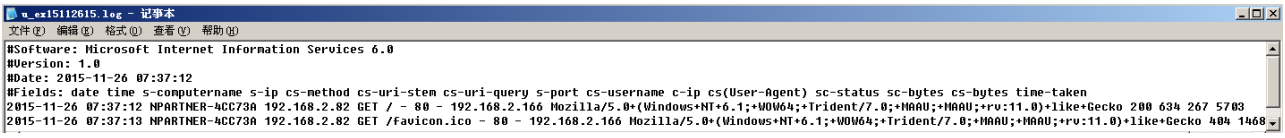
5. 鼠标左点[常规]，勾选[每小时]，勾选[文件命名和创建使用当地时间]，左点[浏览]，选择日志文件目录，Windows 2003 默认为" C:\WINDOWS\system32\LogFiles"。网站 " Site 1 " 选择[W3C 扩展日志记录文件格式]，产生的 log 放在 W3SVC$var 文件夹下，文件格式为 exyymmddhh.log ,$var 为变量 ,会因不同网站而改变 ,本例记录文件名称为 W3SVC1701187996。设定 SyslogAgent 时 ,请确认 log 路径为 C:\WINDOWS\system32\LogFiles\W3SVC1701187996。左点[确定]。



注：如果 IIS Server 安装多个网站(Web Sites)，欲审核的网站阶请重复设定第 3～5 步骤，并将 log 记录在多个记录文件，其名称为 W3SVC$var。

6. 鼠标左点[高级]。扩充记录选项勾选日期(date)、时间(time) 、客户端 IP 地址(c-ip) 、用户名(cs_username) 、服务器名 (s-computername)、服务器 IP 地址(s-ip) 、服务器端口 (s-port)、方法(cs-method)、URI 资源 (cs-uri-stem)、URI 查询(cs-uri-query) 、协议状态(sc-status)、发送的字节数(sc-bytes)、接收的字节数(cs-bytes) 、所用时间(time-taken)、用户代理(cs(User-Agent))。按[确定]。再按[确定]，完成配置。

7. 检查是否启用日志记录。浏览器 access 网站 " Site 1 " 后过几分钟，开启记录文件检查 log 是否确实记录。

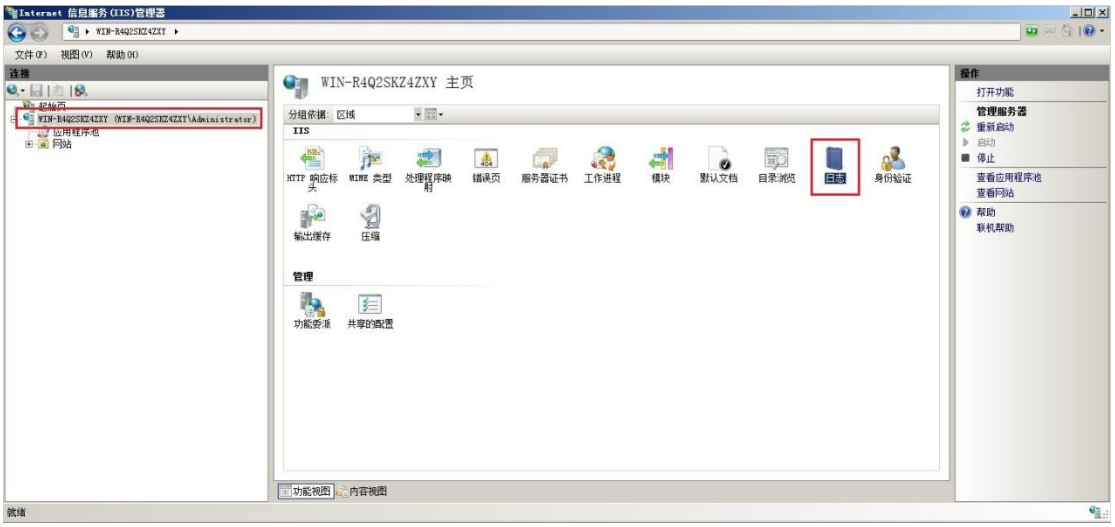


2 Windows 2008 安装 IIS 7 环境

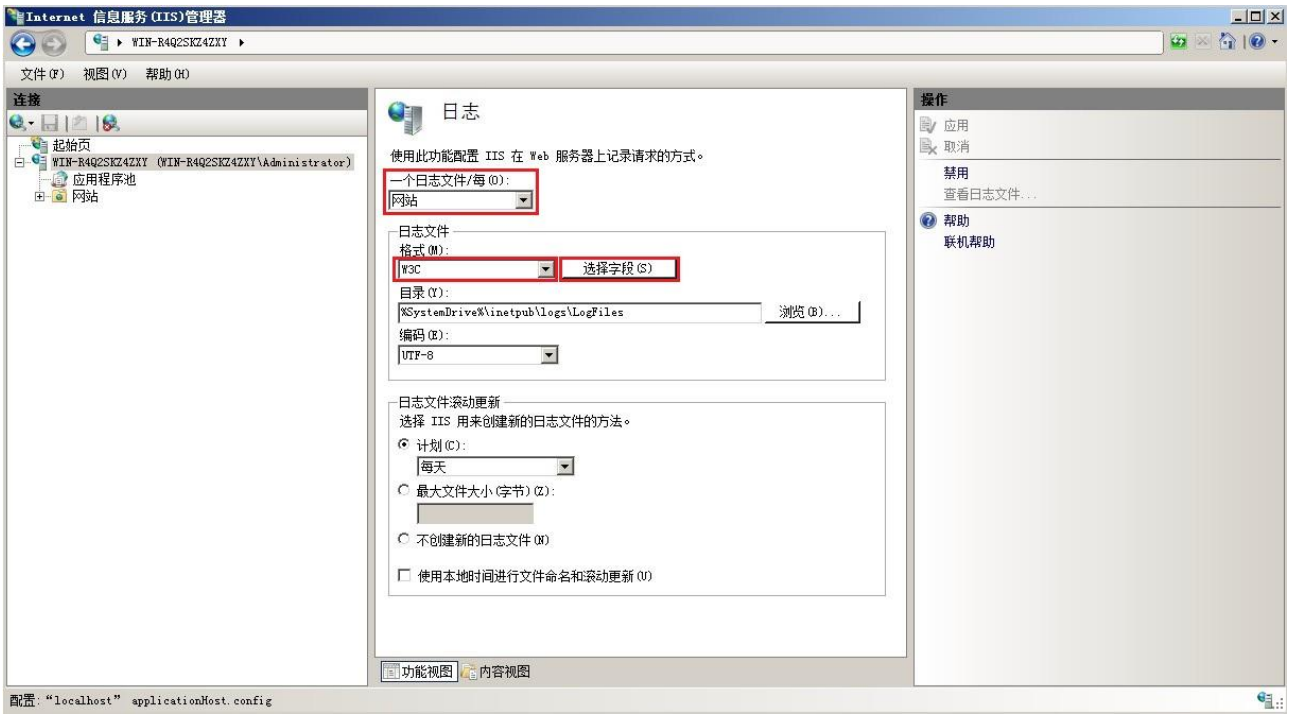
2.1 设定 IIS 7 Server

1. [开始]→[管理工具]→[Internet 信息服务(IIS)管理器]。

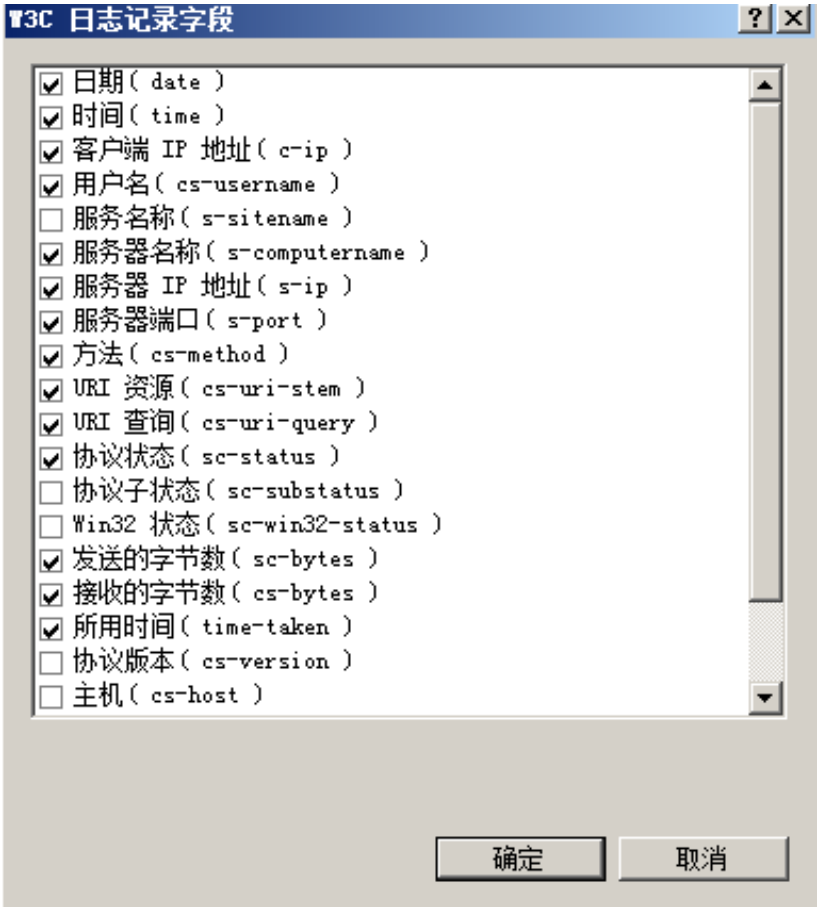
2. 设定站台层级的日志记录选项。鼠标双点本地计算机。鼠标双点[日志]。



3. 鼠标左点[一个日志文件/每]中的▼，下拉选[网站]。日志文件下拉选[W3C]，鼠标左点[选择字段]。



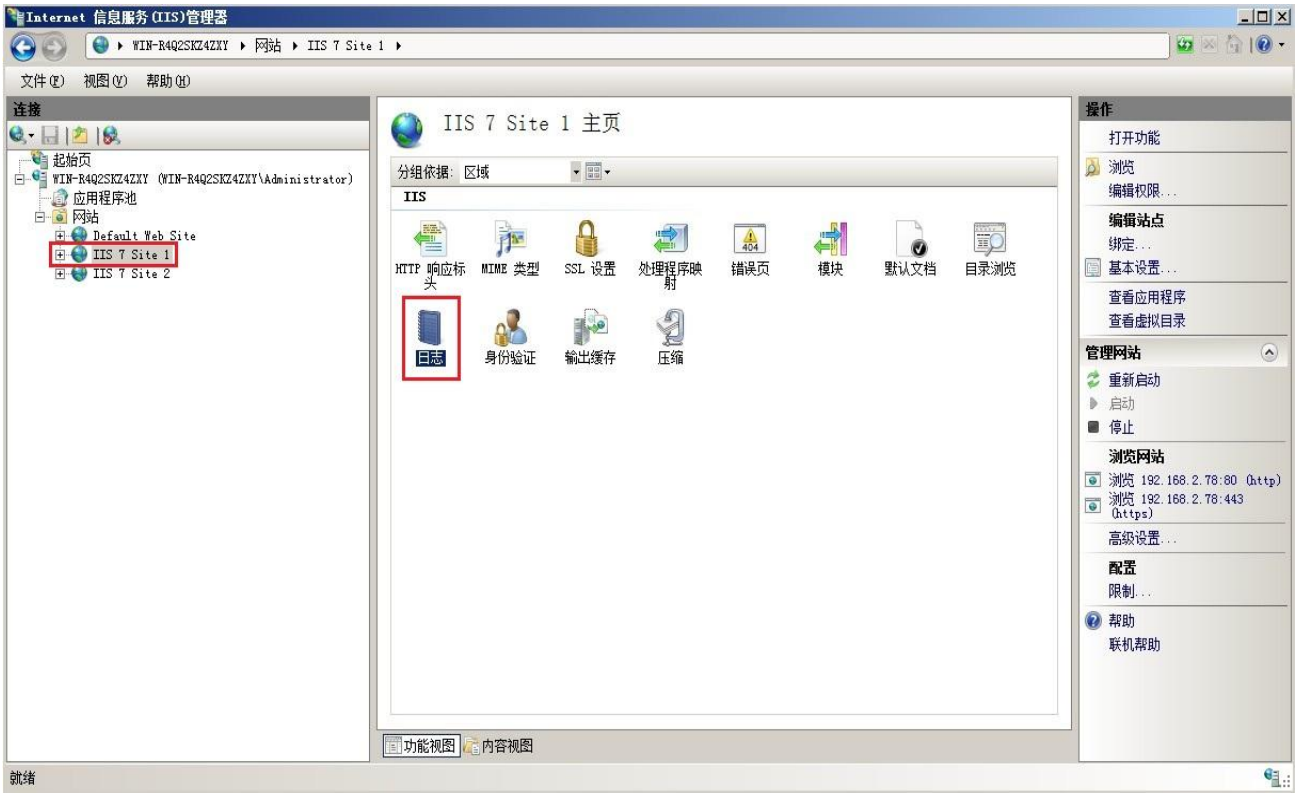
4. [W3C 选择字段]选项勾选日期(date)、时间(time) 、客户端 IP 地址(c-ip) 、用户名(cs_username) 、服务器名 (s-computername)、服务器 IP 地址(s-ip) 、服务器端口 (s-port)、方法(cs-method)、URI 资源 (cs-uri-stem)、URI 查询(cs-uri-query) 、协议状态(sc-status)、发送的字节数(sc-bytes)、接收的字节数(cs-bytes)、所用时间(time-taken)、用户代理(cs(User-Agent))。按[确定]。



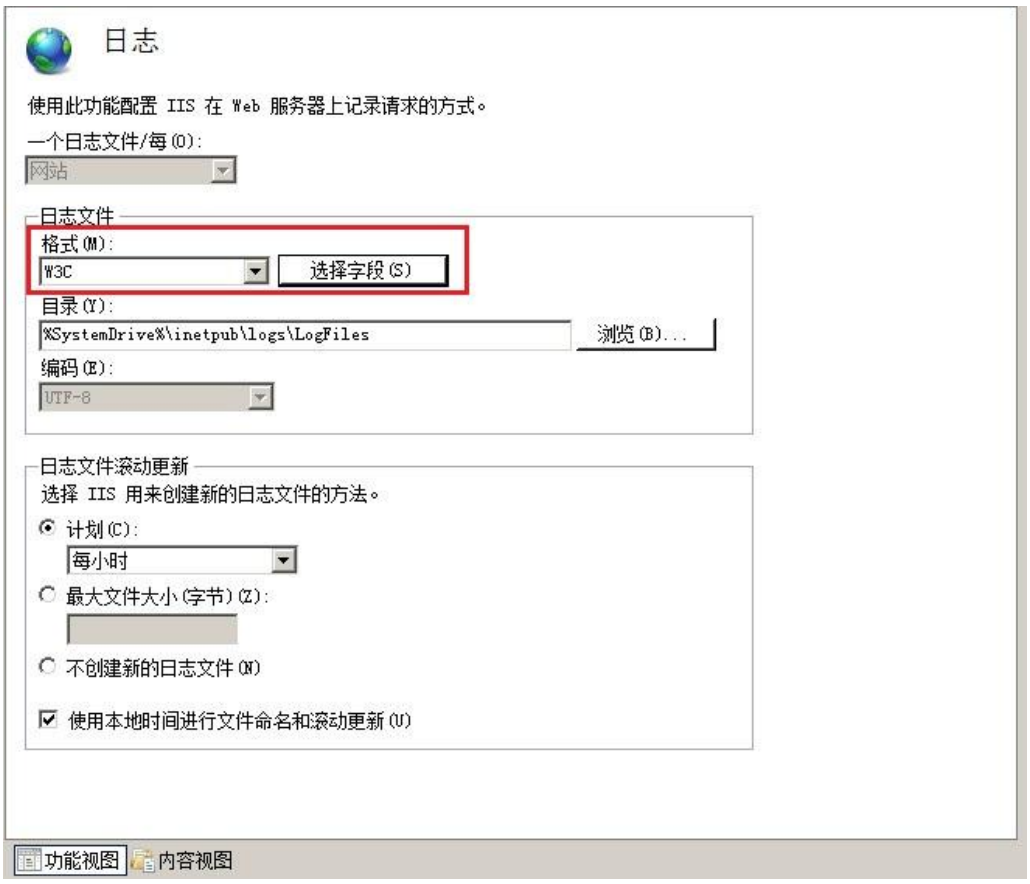
5. 按按[浏览]，选择记录文件目录，Windows 2008 默认为
" %SystemDrive%\inetpub\logs\LogFiles "。编码选择[UTF-8]。勾选[计划]，下拉选[每小时]。勾选[使用本地时间进行文件命名和滚动更新]。**按[应用]完成站台层级的配置。**

注:N-Reporter 新版(Version 3.1.35 之后版本)支持 BIG5、GB2312 编码。此设定假如选 GB2312 编码，IIS Server 将以 GB2312 编码存储网站记录，送出的 syslog 的 message 也是 GB2312 编码，所以在 N-Reporter 系统新增 IIS 设备时请选择 GB2312 编码。

6. 设定个别站台的日志记录选项。双点[网站]，展开所有 Site。
鼠标右点欲审核的网站 " IIS 7 Site 1 " ，再双点[日志]，设定此网站的日志配置。



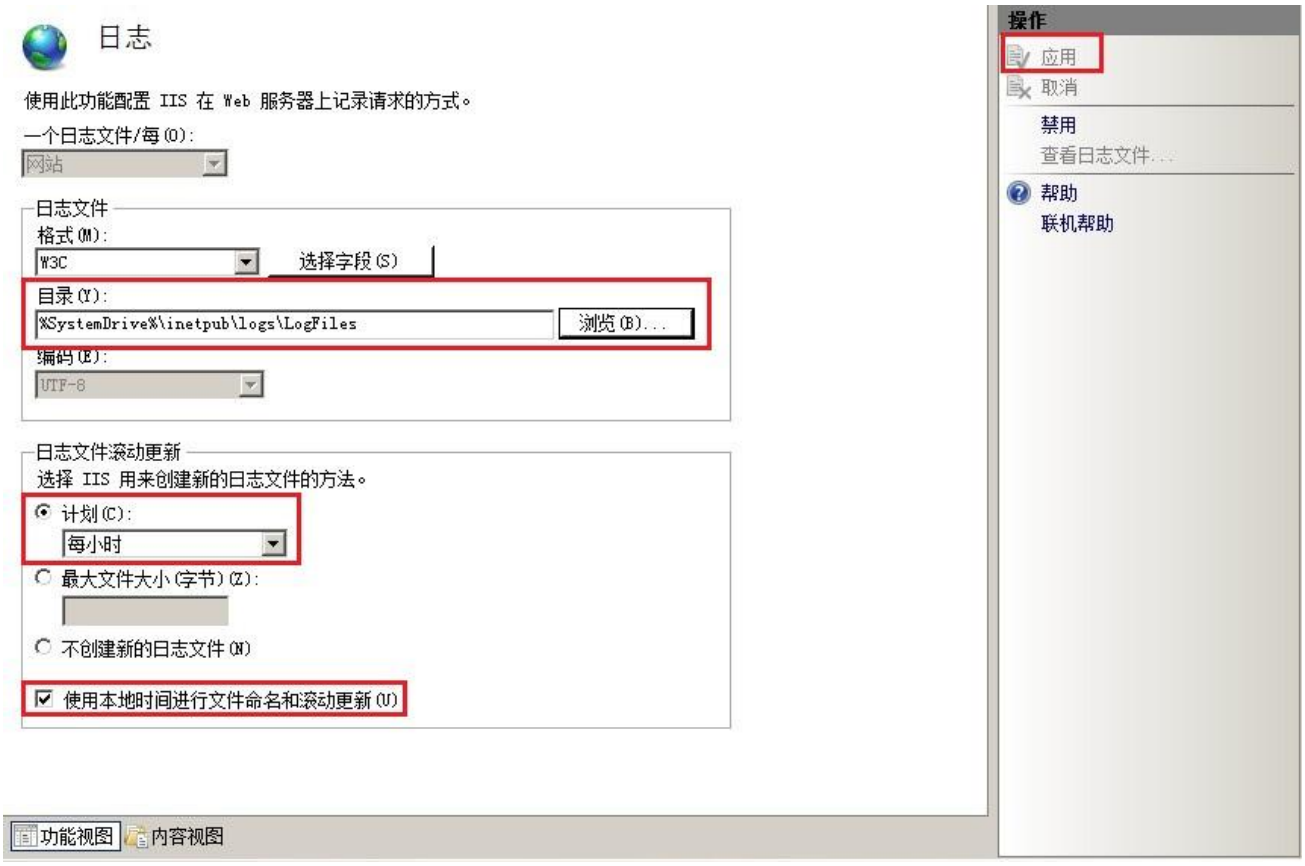
7. 日志文件下拉选[W3C]，鼠标左点[选择字段]。



8. [W3C 记录字段]选项勾选日期(date)、时间(time) 、客户端 IP 地址(c-ip) 、使用者名称(cs_username) 、服务器名称(s-computername)、服务器 IP(s-ip) 、服务器连接 Port(s-port)、方法(cs-method)、URI 主体(cs-uri-stem)、URI 查询(cs-uri-query) 、通讯协议状态(sc-status)、已传送字节(sc-bytes)、已接收字节(cs-bytes) 、所用时间(time-taken)、用户代理(cs(User-Agent))。按[确定]。

注：若已在步骤 3、4 设定记录字段，并检查一致，请左点[取消]。

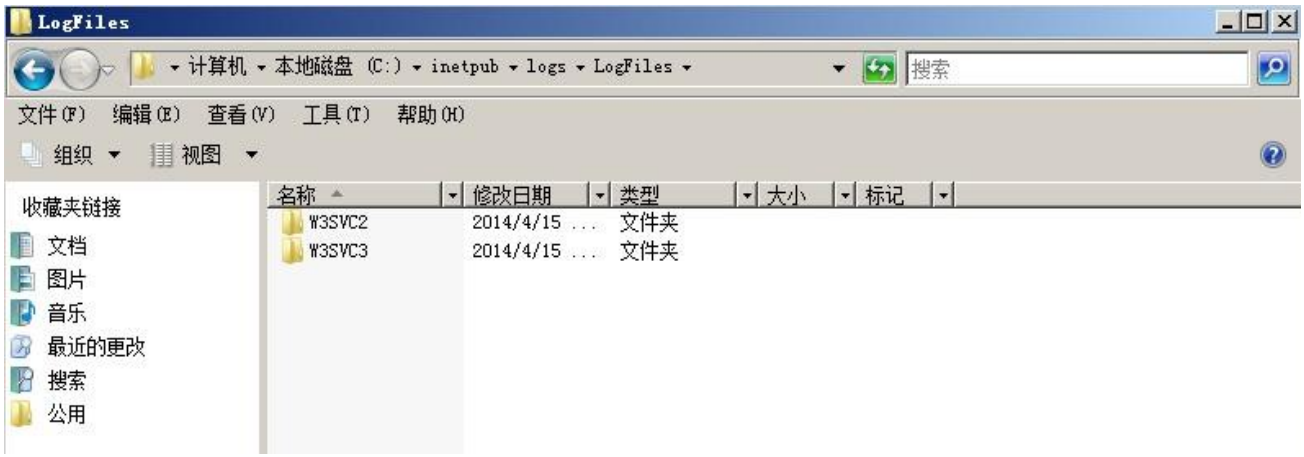
9. 按[浏览]，选择日志文件目录，Windows 2008 默认为
" %SystemDrive%\inetpub\logs\LogFiles "。勾选[计划]，下拉选[每小时]。勾选[使用本地时间进行文件命名和滚动更新]。
按[应用]完成站台 " IIS 7 Site 1 " 设定。按[套用]完成站台 " IIS 7 Site 1 " 设定。



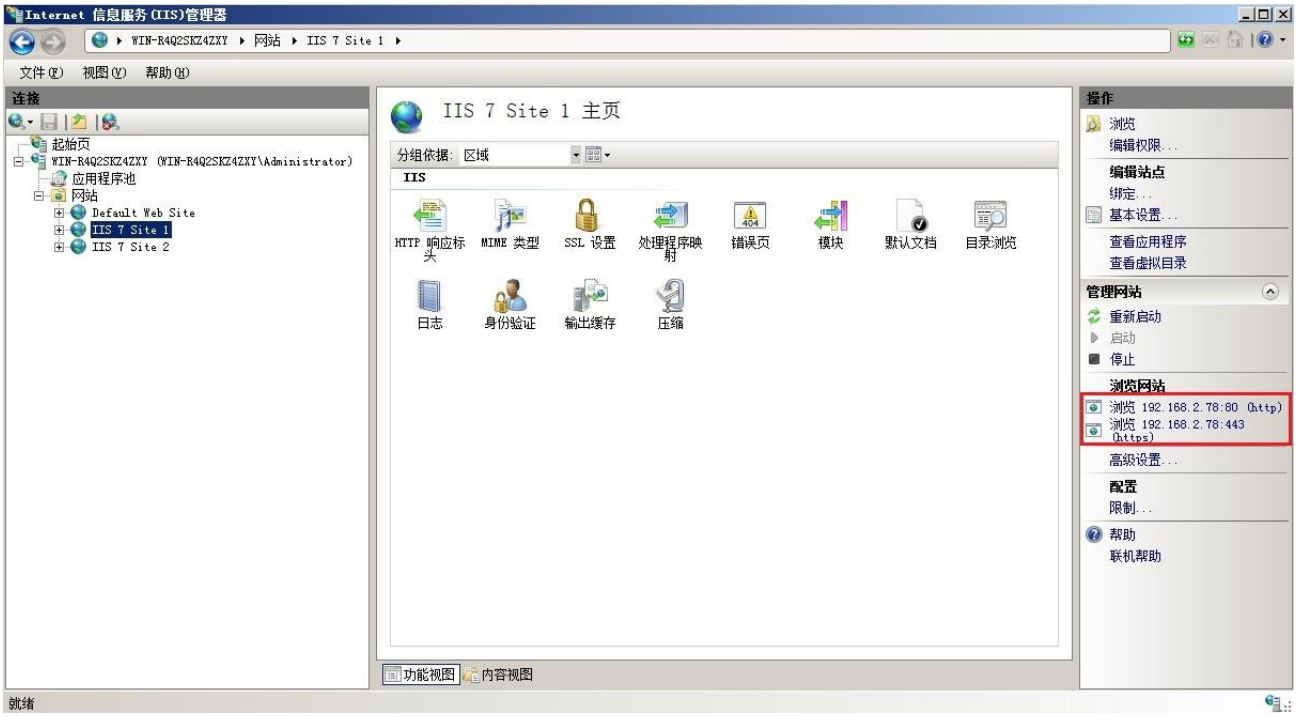
注：如果没设定站台层级的记录选项，编码选择请一定要选择 [UTF-8]。

注：如果 IIS Server 有多个站台，每个站台皆需设定第 6~9 步骤。

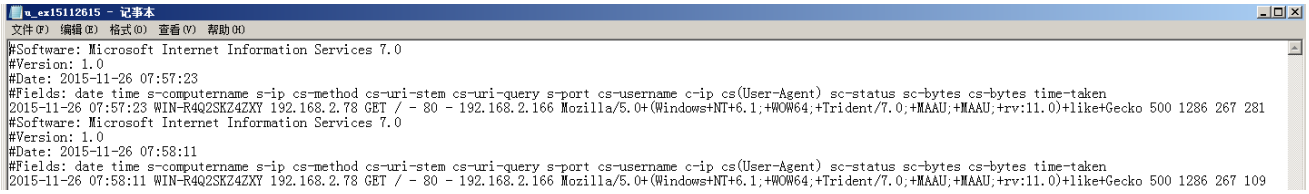
10. 若 IIS Server 有多个站台，每个 Site 的记录档案为 W3SVC$var，其中$var 为变量。请确认 IIS 7 Site 1 的记录档案正确路径。例如下图为两个站台的记录文件。



下图知，IIS 7 Site 1 的站台 IP 为 192.168.2.78。



检查 W3SVC2 和 W3SVC1 的 log，得知站台 " IIS 7 Site 1 " 的日志文件路径为 C:\inetpub\logs\LogFiles\W3SVC2。



检查是否启用日志记录。浏览器 access 网站 " IIS 7 Site 1 " 后过几分钟，开启记录文件检查 log 是否确实记录。

3 配置 NXLOG

1. 以系统管理者 Administrator 登入 IIS Server。
2. **下载 NXLOG：**http://sourceforge.net/projects/nxlog-ce/files/

   下载『nxlog-ce-x.x.x.msi』。
3. **安装 NXLOG：**鼠标左点『nxlog-ce-x.x.x.msi』，安装 NXLOG。

   注：32 位操作系统 NXLOG 安装在 " C:\Program Files\nxlog\conf\nxlog.conf " 。

   64 位操作系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。
4. **配置 NXLOG：**

   (1) 下载 IIS NXLOG 配置文件 nxlog_iis.conf：

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

   编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。将 IIS NXLOG 配置文件设定贴上并覆盖 nxlog.conf 设定。。

```
## 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. **绿色部位**请选择 NXLOG 正确的安装路径，

本例环境为 64 位系统选择 " define ROOT C:\Program Files (x86)\nxlog " 。

b. **黄色部分**"define IIS_SITE1 $dir "行中的$dir 请输入 IIS Server 站台的记录路径，

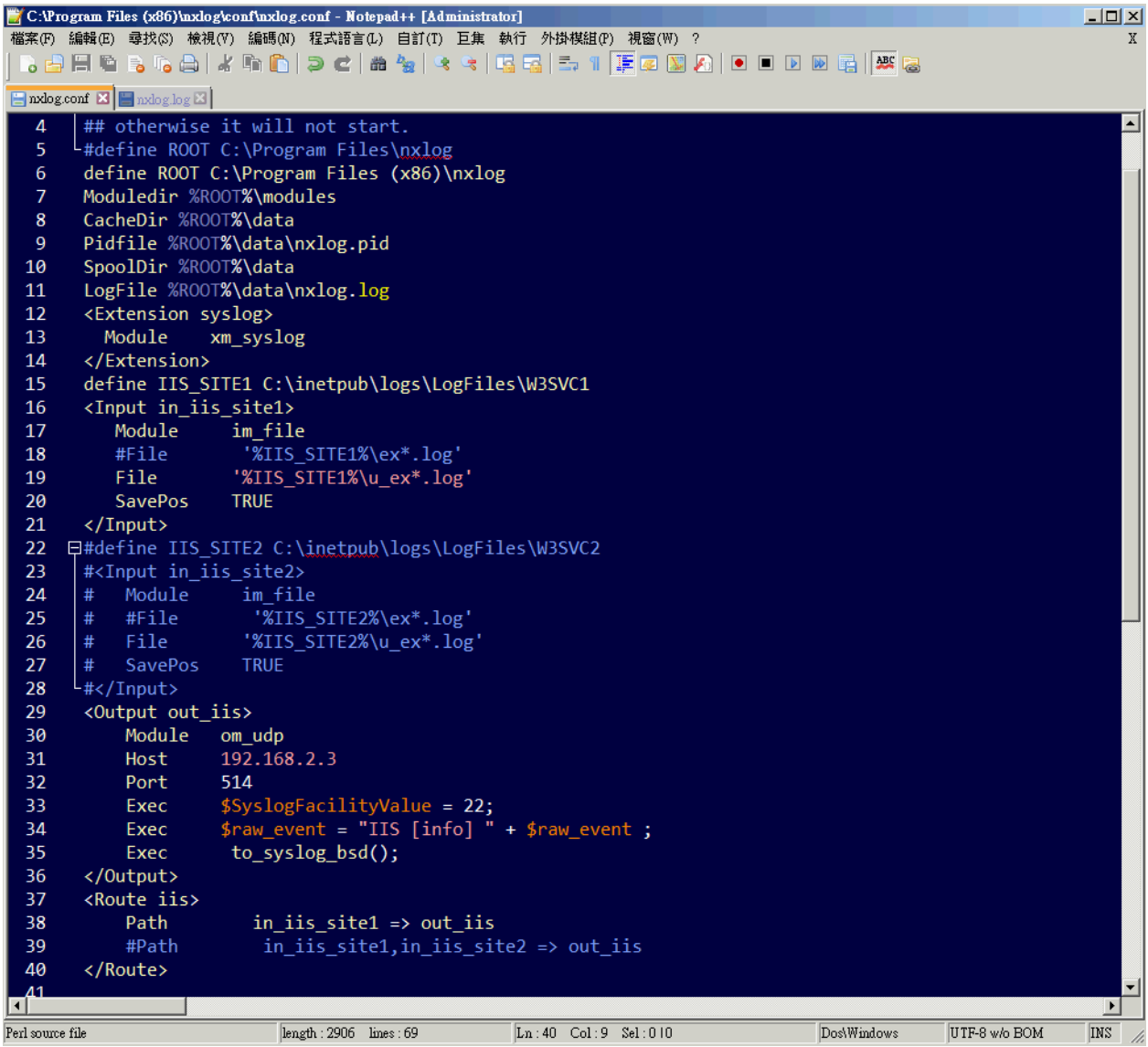
本例路径为 " C:\inetpub\logs\LogFiles\W3SVC2 " 。

c. **红色部分**"Host $N_Reporter_IP"行中的$N-Reporter_IP 改成 N-Reporter IP，

本例 IP 为 192.168.2.3。

d. 本例 IIS 站台的编码为 UTF-8，记录文件的格式为 u_ex*.log，所以设定为 " File '%IIS_SITE1%\u_ex*.log' " 。如果 IIS 站台的记录为 BIG5 或 GB2312 编码，则记录文件的格式为 ex*.log，请将设定改为 " File '%IIS_SITE1%\ex*.log' " 。

本例配置范例：



e. 如果 IIS Server 为多个站台，请删除配置范例第 22 ~ 28 行的批注符号"#"，定义第二个站台的储存路径 IIS_SITE2 与新增 input 的 in_iis_site2，并且选择第 38 行设定 " Path in_iis_site1,in_iis_site2 => out_iis " ，将两个台站的 log 转成 syslog 送出。

(2) 启动 NXLOG：选择**步骤 a** 利用[命令提示字符]启动 NXLOG 或**步骤 b**[服务]启动 NXLOG。

a. [开始]→[所有程序]→[应用附属程序] ,鼠标右点[命令提示字符] ,左点[执行身分] ,以系统管理员身分执行。

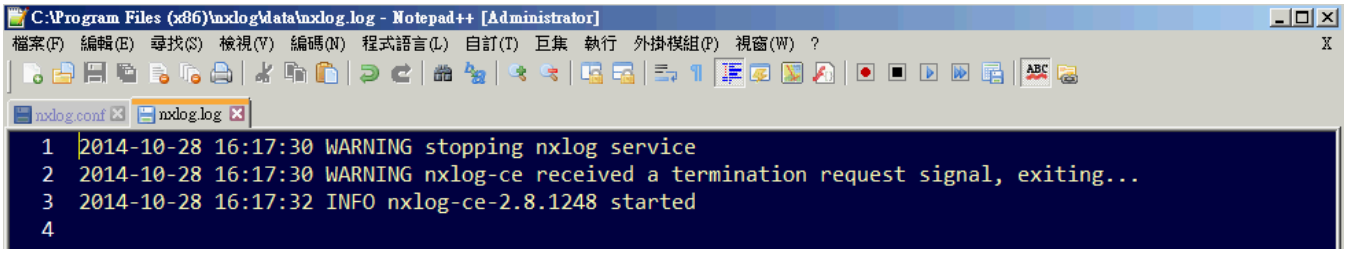
命令提示字符输入：

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

b. [开始] →[所有程序]→[系统管理工具]→[服务] , 右点服务[nxlog] , 左点[启动]或[重新启动]。

(3) 检查 NXLOG 是否正常启动：

检查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log " ,没有显示 Error 的讯息，表示正常启动。



采购与销售合作：sales@npartnertech.com
技术咨询：support@npartnertech.com