N-Partner

N-REPORTER

How to Manage IIS Audit Log

V 1.1.10 (English)

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

Preface

This document describes how to manage the IIS Audit Log by N-Reporter. The first part introduces how to install IIS 6 in Wondows 2003 and IIS 7 in Windows 2008. The second part introduces the configuration of NXLOG and send the syslog to the N-Reporter.

Contents：

Contact

N-Partner ：

TEL: +886-4-23752865

FAX: +886-4-23757458

TAC Support：

Email: support@npartnertech.com

Skype：support@npartnertech.com

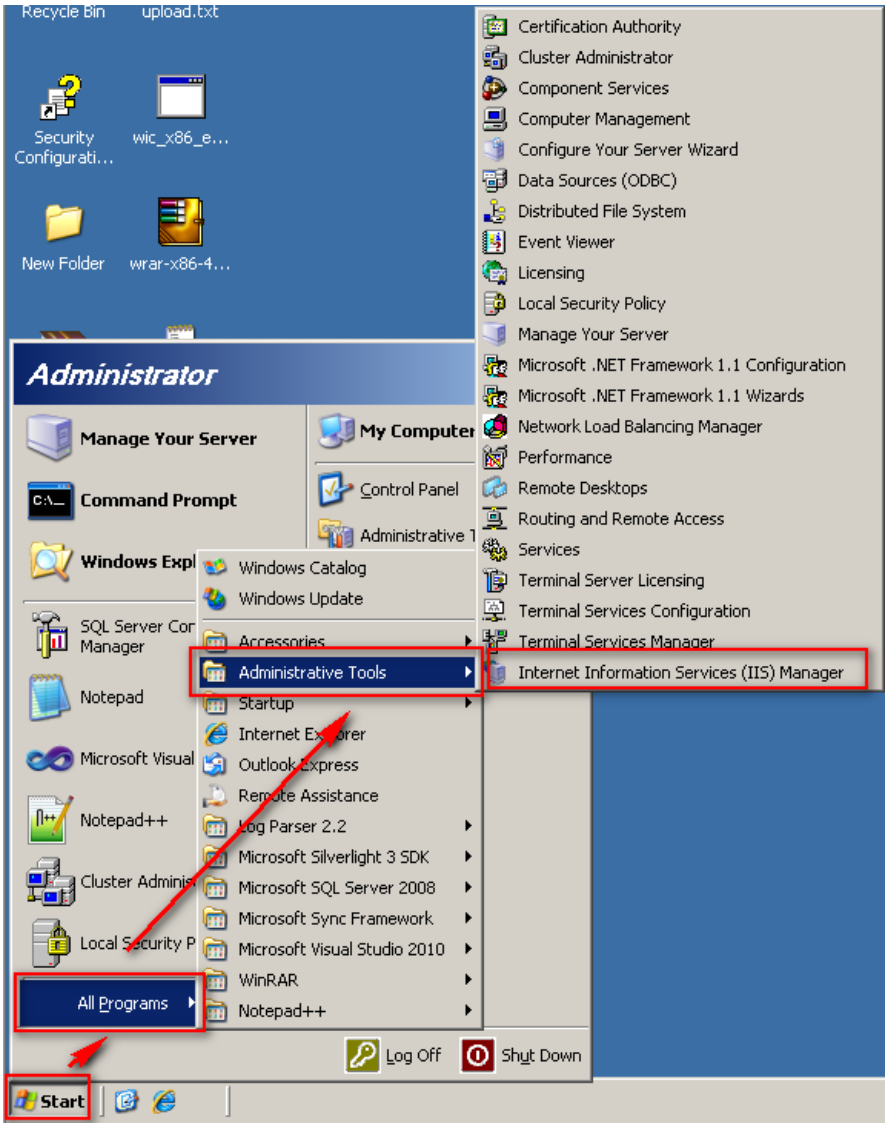
Sales Support：

Email: sales@npartnertech.com

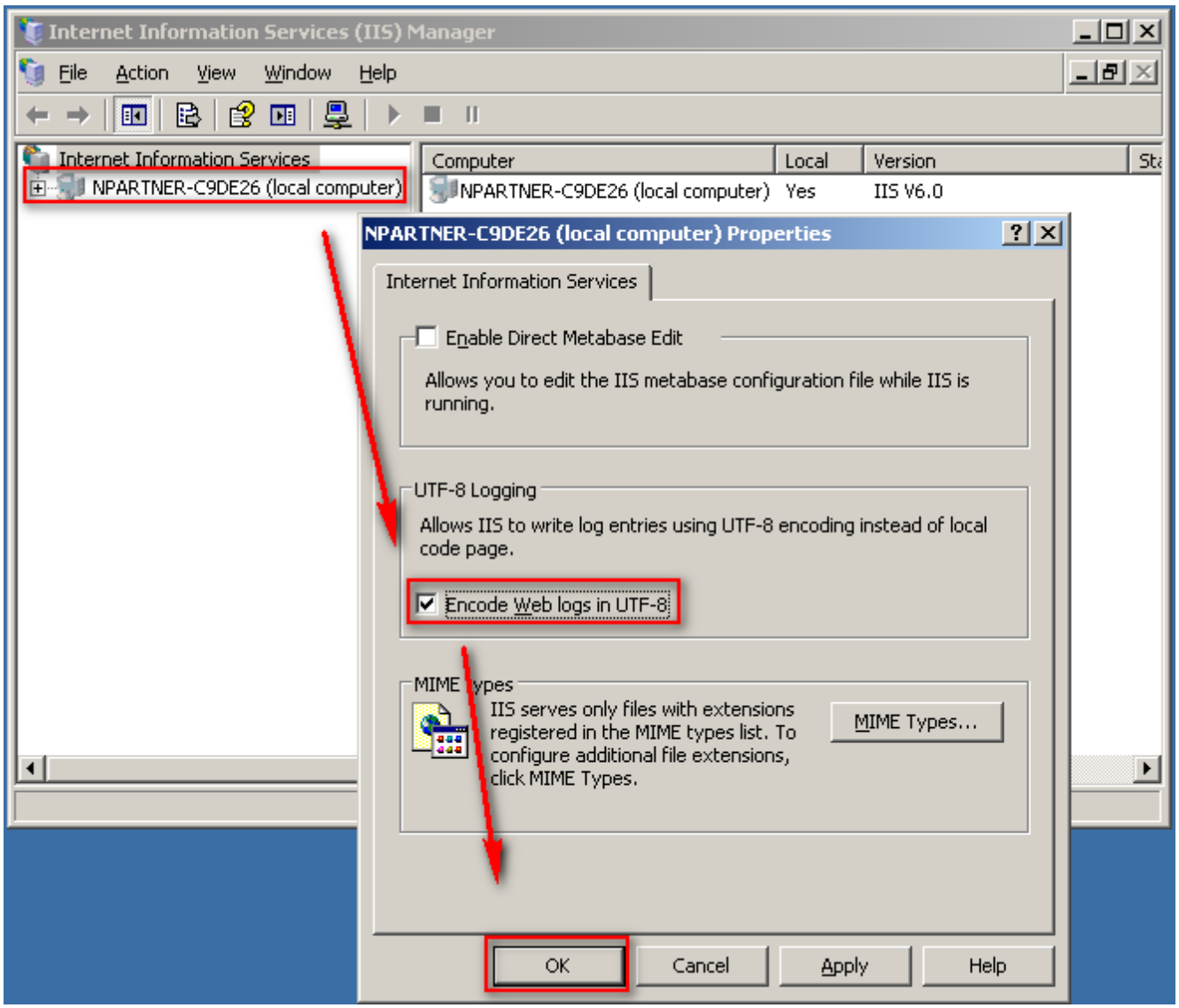
1. Set up IIS 6 on Windows 2003

1.1 Set up IIS 6 Server

1. Logon the IIS Server by administrator. Click [Start / All Programs / Administrative Tools / Internet Information Services (IIS) Manager].

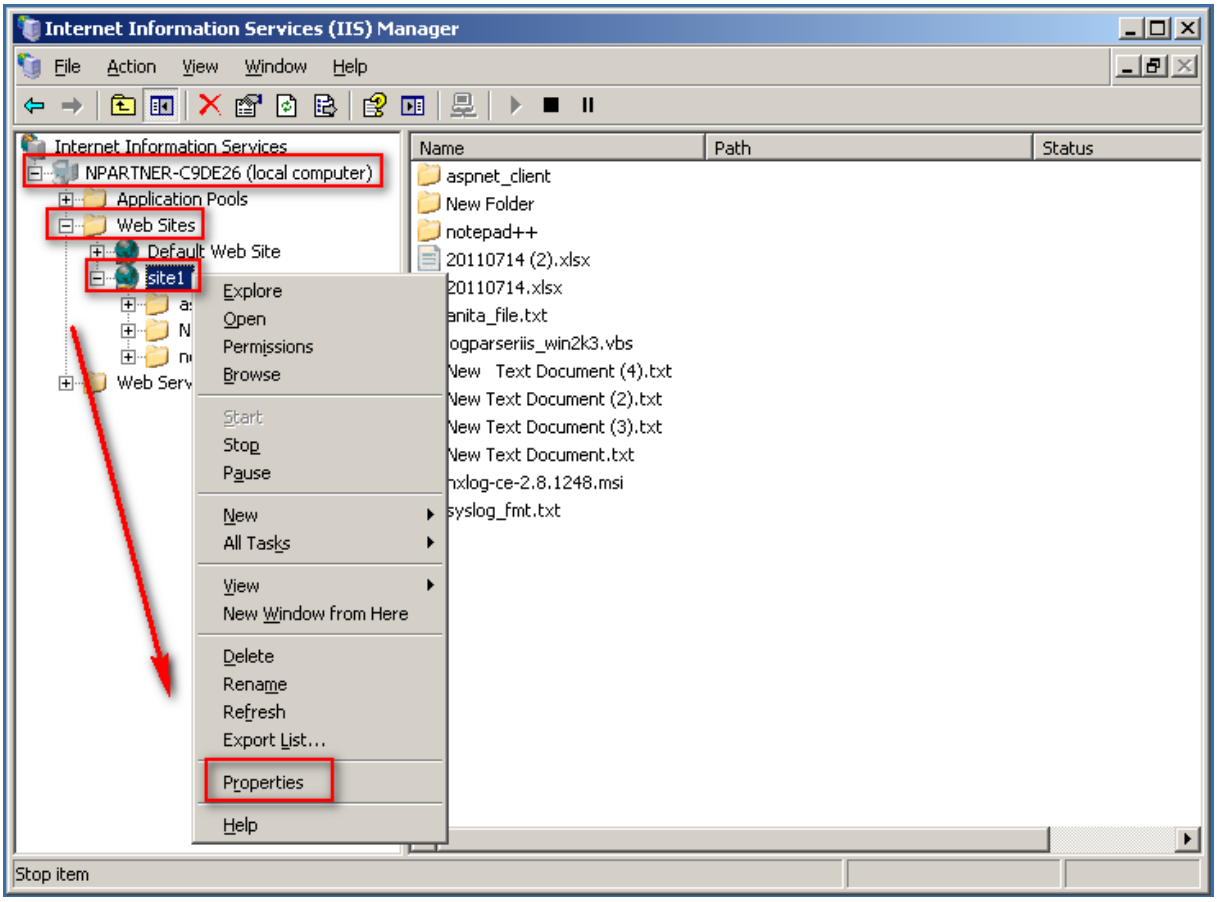


2. Right click [IIS server (local computer)]. Click [Properties] and check [Encode Web logs in UTF-8]. Click [OK].

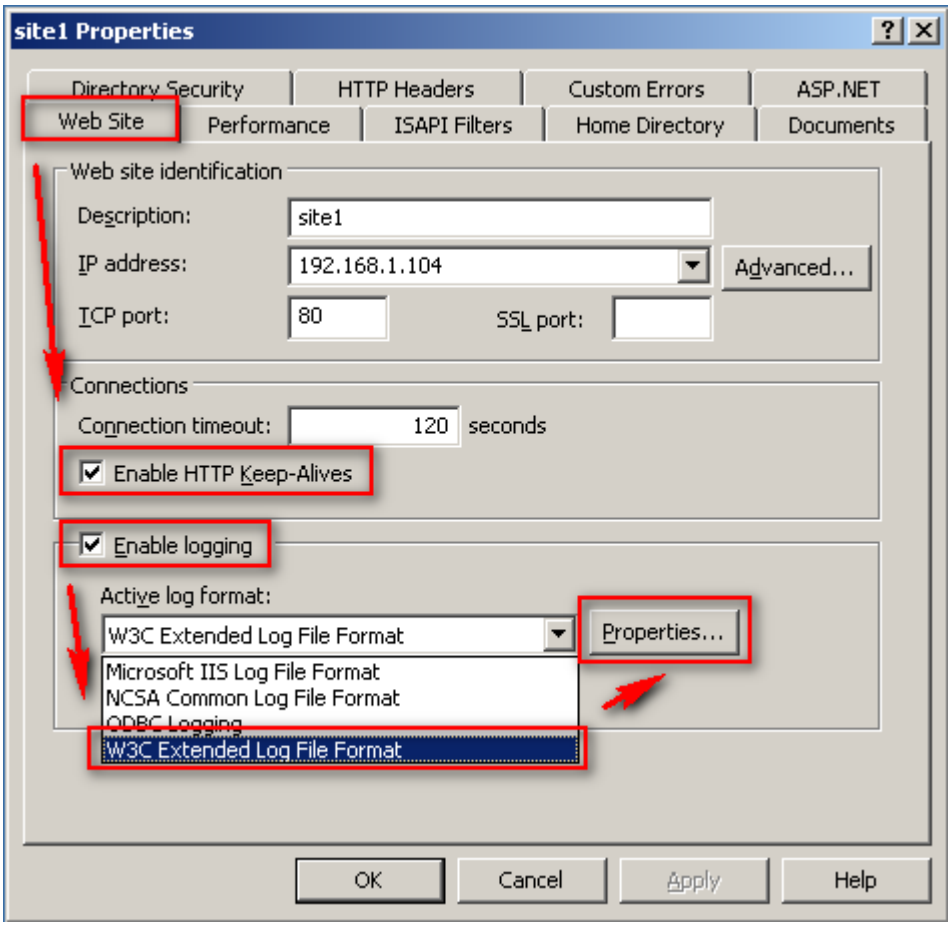


Remark: The version 3.1.35 (or later) of N-Reporter supports BIG5 and GB2312. If this setting does not checked [Encode Web logs in UTF-8], IIS Server will store web logs and send syslog message by BIG5 encode by default. So when adding devices on IIS server, please select BIG5 encode.

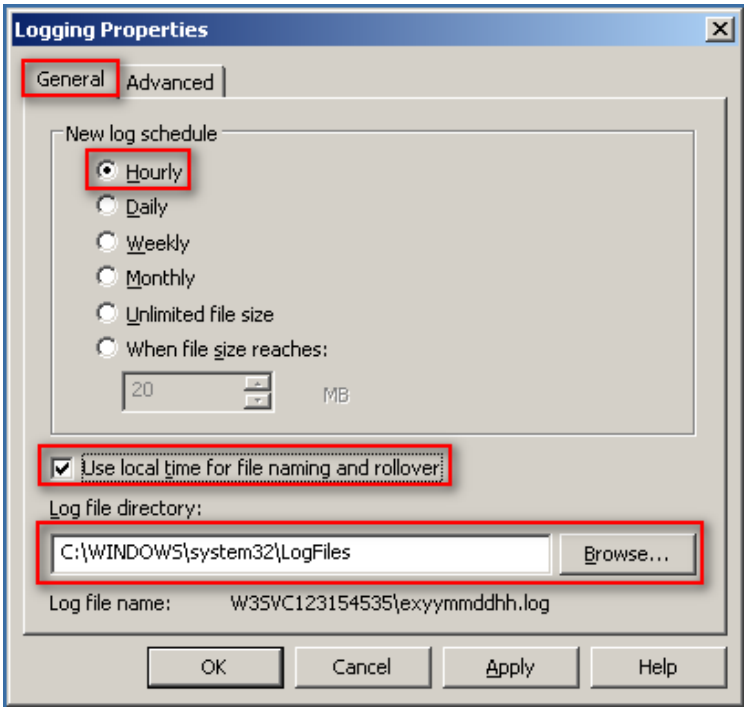
3. Click the [Local Computer / Web Sites]. Right click the web site “site1” as an example in this article for audit purpose, then click [Properties].



4. Click [Web Site] tab. Please enter “80” on TCP port and “443” on SSL port. Check [Enable HTTP Keep-Alives] and [Enable logging]. Click ▼ mark, choose [W3C Extended Log File Format] from the menu. Click [Properties].

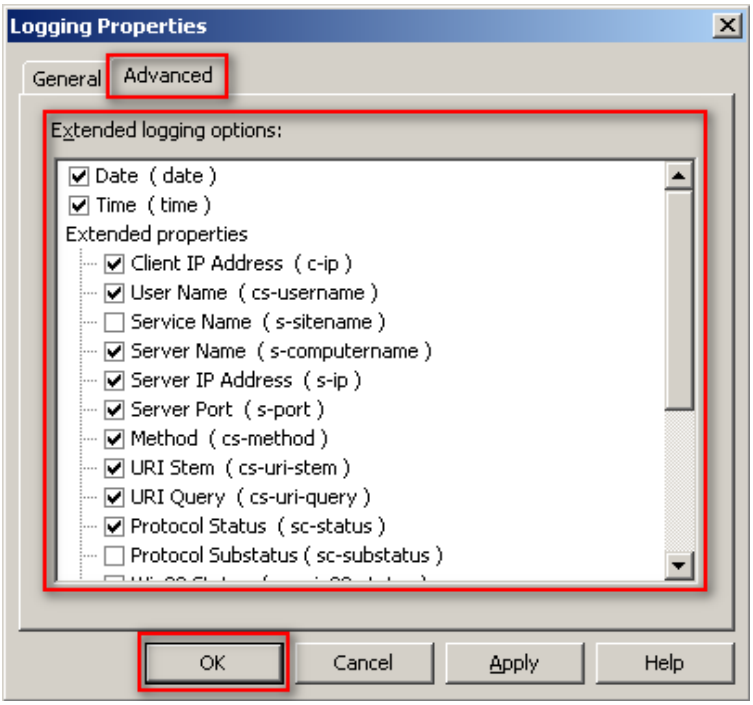


5. Click [General] tab, check [Hourly], check [User local time for file naming and rollover], click [Browse] to select the log path. The default path on Windows 2003 is C:\WINDOWS\system32\LogFiles". The log of the web site "site1" that [W3C Extended Log File Format] is saved in the folder "W3SVC$var". "$var" is a dependent variable and it will be different depend on the different web. The format of file name is exyymmddhh.log.
For example, the log file name is "W3SVC477399155". Make sure the log path is C:\WINDOWS\system32\LogFiles\W3SVC477399155 when setting up Syslogagent.

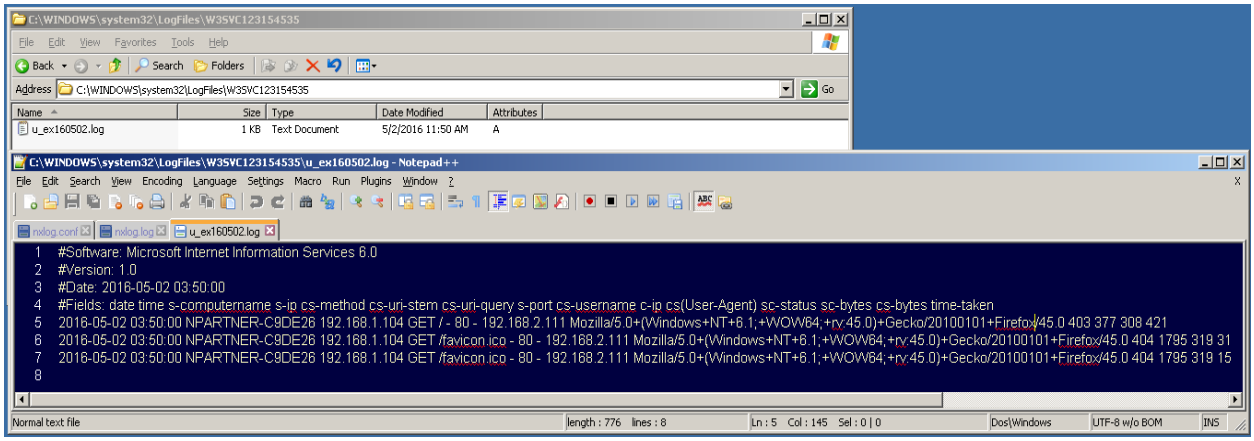


Remark：When installing more than one Web site, please repeat step 3 to step 5 and save web log for each file and name it as W3SVC$var.

6. Click [Advanced] tag. Check Data(date), Time(time), Client IP Address(c-ip), User Name(cs-username), Server Name(s-computername), Server IP Address(s-ip), Server Port(s-port), Method(cs-method), URL Stem(cs-uri-stem), URL query(cs-uri-query), Protocol Status(sc-status), Bytes Sent(sc-bytes), Bytes Received(cs-bytes), Time Taken(time-taken) and User Agent(cs(User-Agent)). Click [OK] to finish.



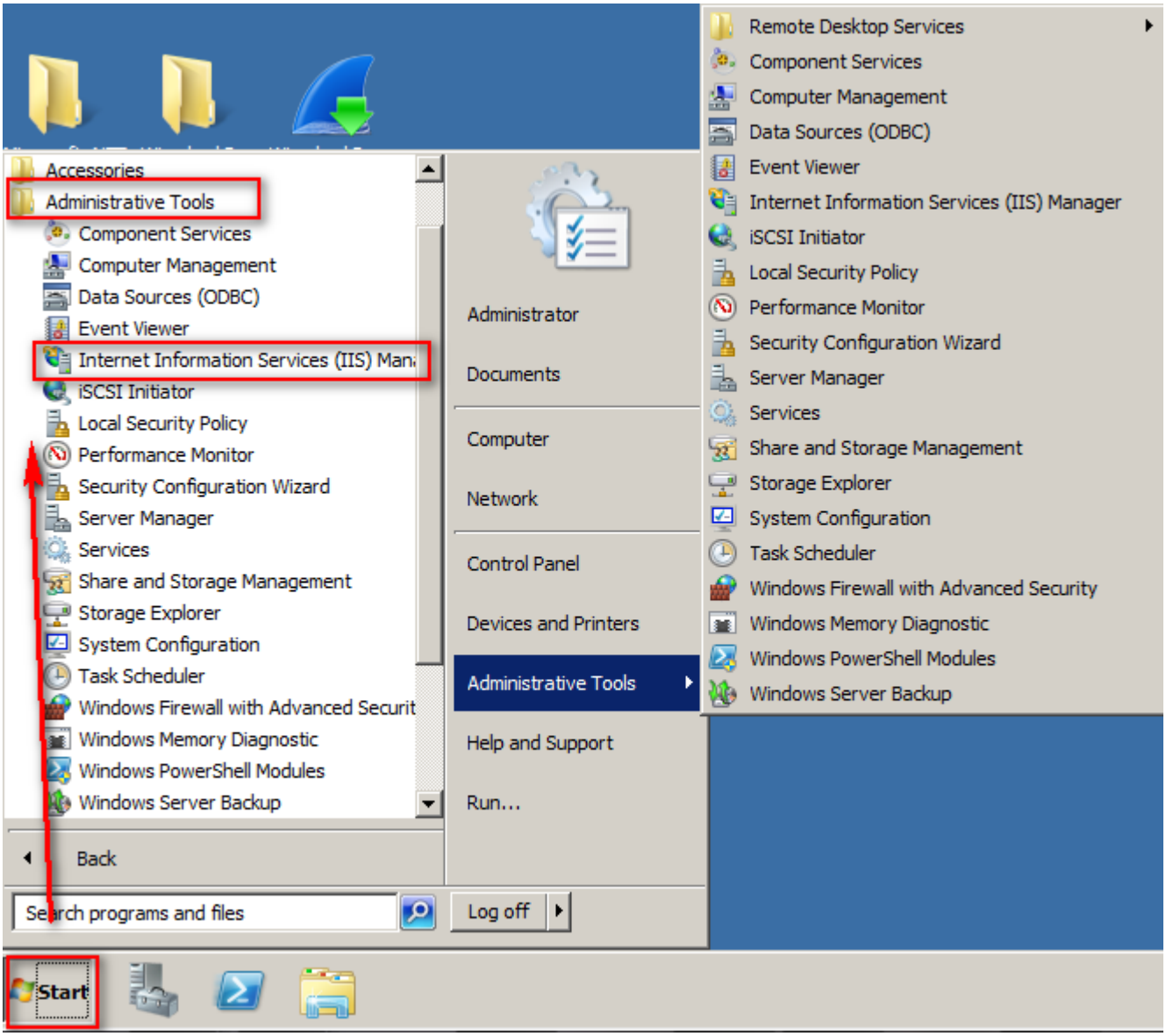
7. Check if the log was written into a file. Open browser, go to “site1” (for example here, 192.168.1.104) for few minutes, then open the log file to see if there are records here.



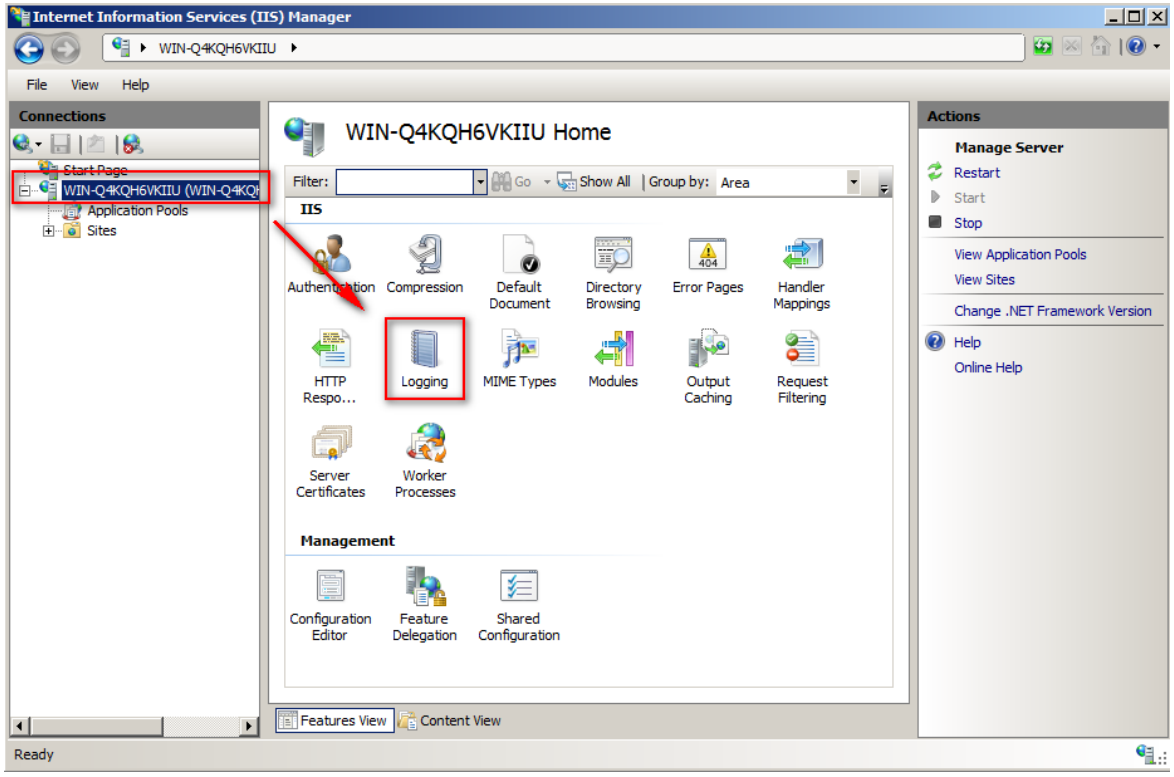
2 Set IIS7 on Windows 2008

2.1 Set IIS 7 Server

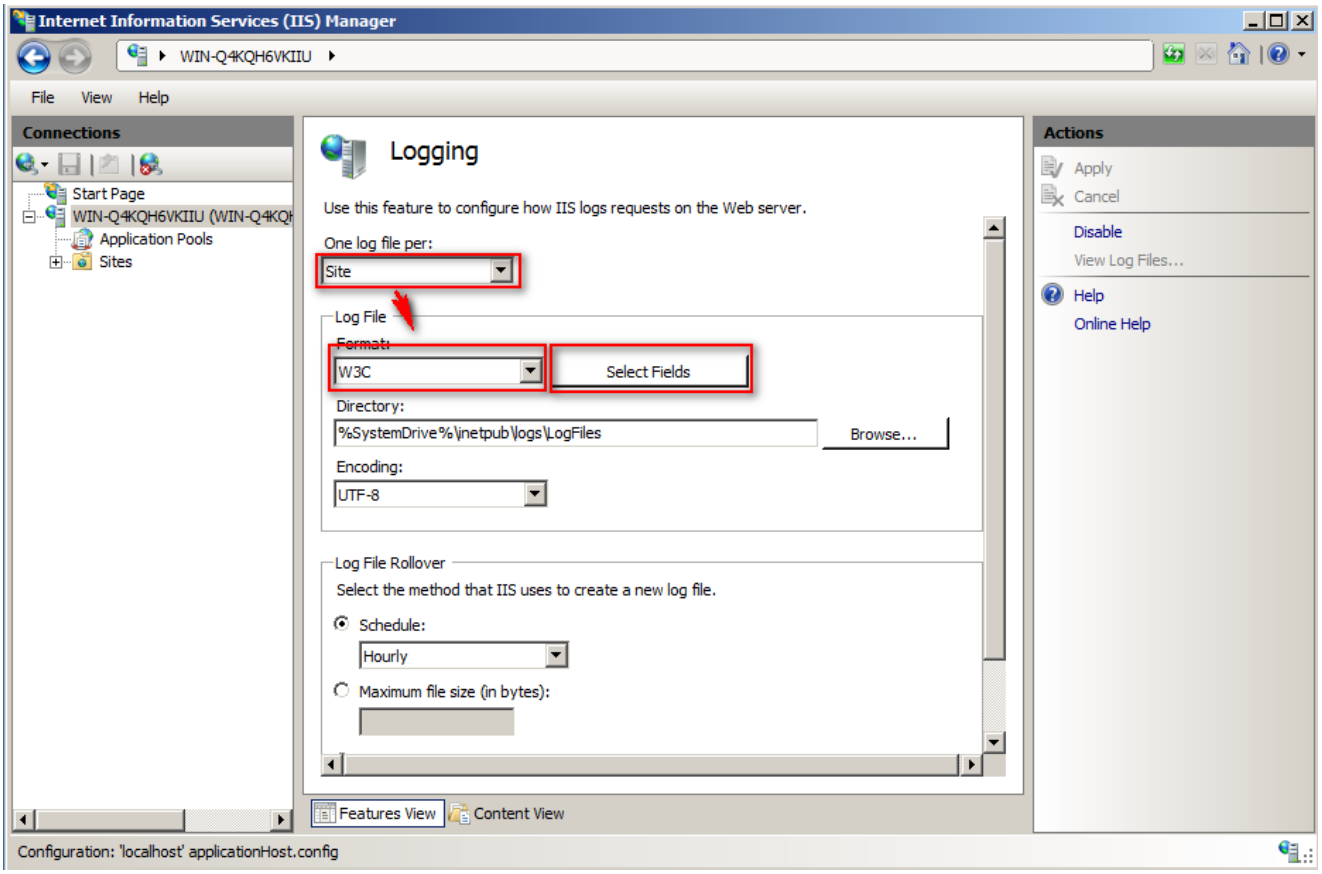
1. Logon the IIS Server by system administrator. click [Start] → [All Programs] → [Administrative] → [Internet Information Services (IIS) Manager].



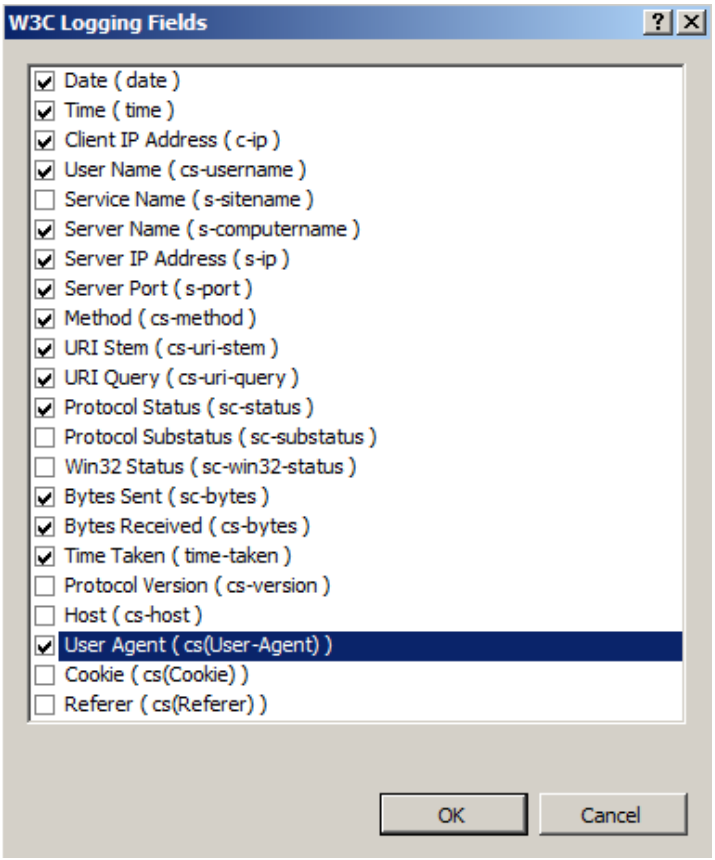
2. Set up Server Logging Options. Double click [IIS Server] to setup the Logging, for this example is WIN-Q4KQH6VKIIU. Double click on [Logging].



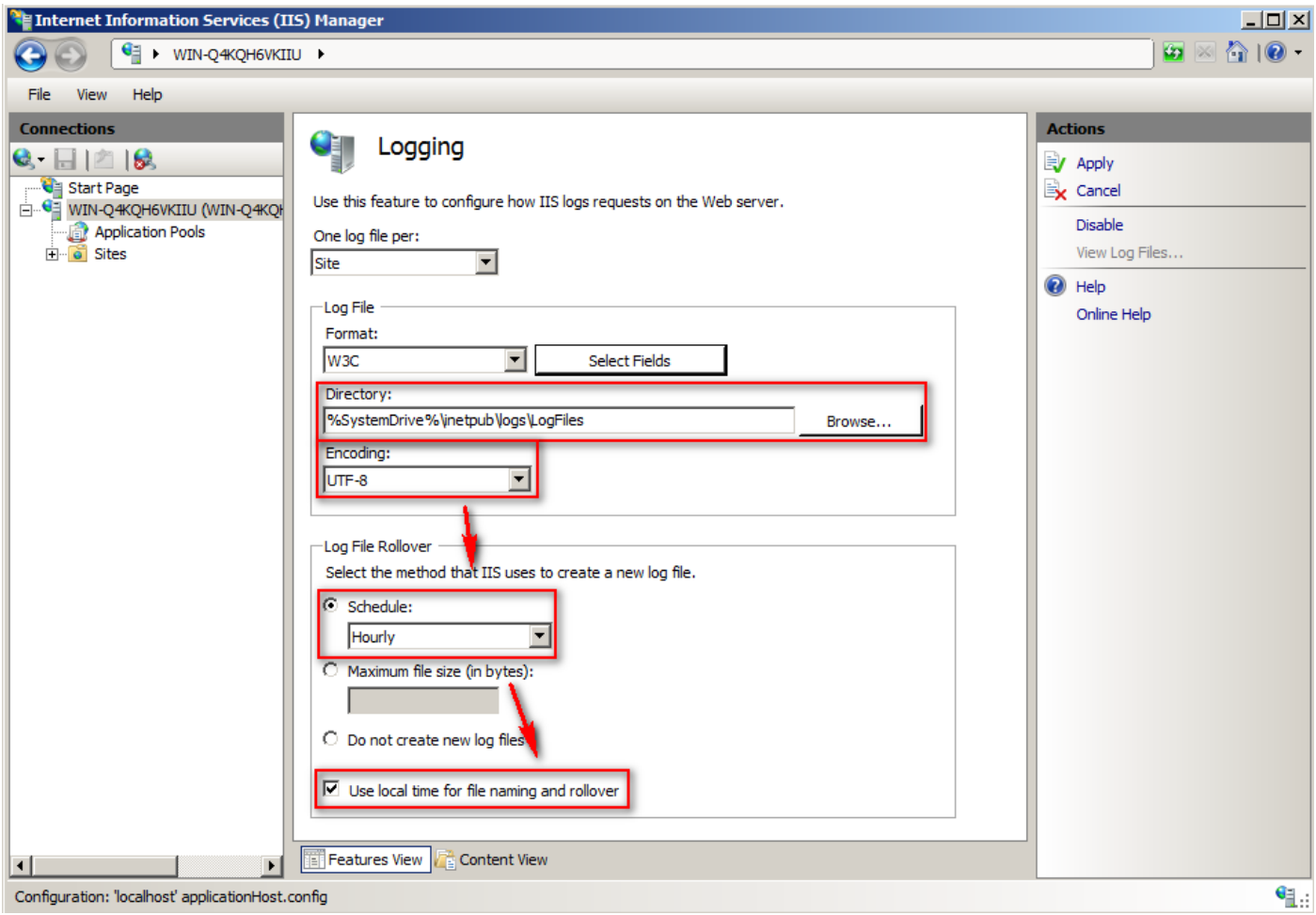
3. Select “Site” from the pull down menu of [One log file per:]. Choose [W3C]. Click [Select Fields].



4. Check Date (date)、Time (time) 、Client IP Address (c-ip) 、User name(cs_username) 、Server name (s-computername)、Server IP Address (s-ip) 、Server Port(s-port)、Method (cs-method)、URI Stem(cs-uri-stem)、URI Query (cs-uri-query) 、Protocol Status (sc-status)、Bytes Sent (sc-bytes)、Bytes Received (cs-bytes) 、Time Taken (time-taken)、User Agent (cs(User-Agent)) of [W3C Logging Fields]. Press [OK].

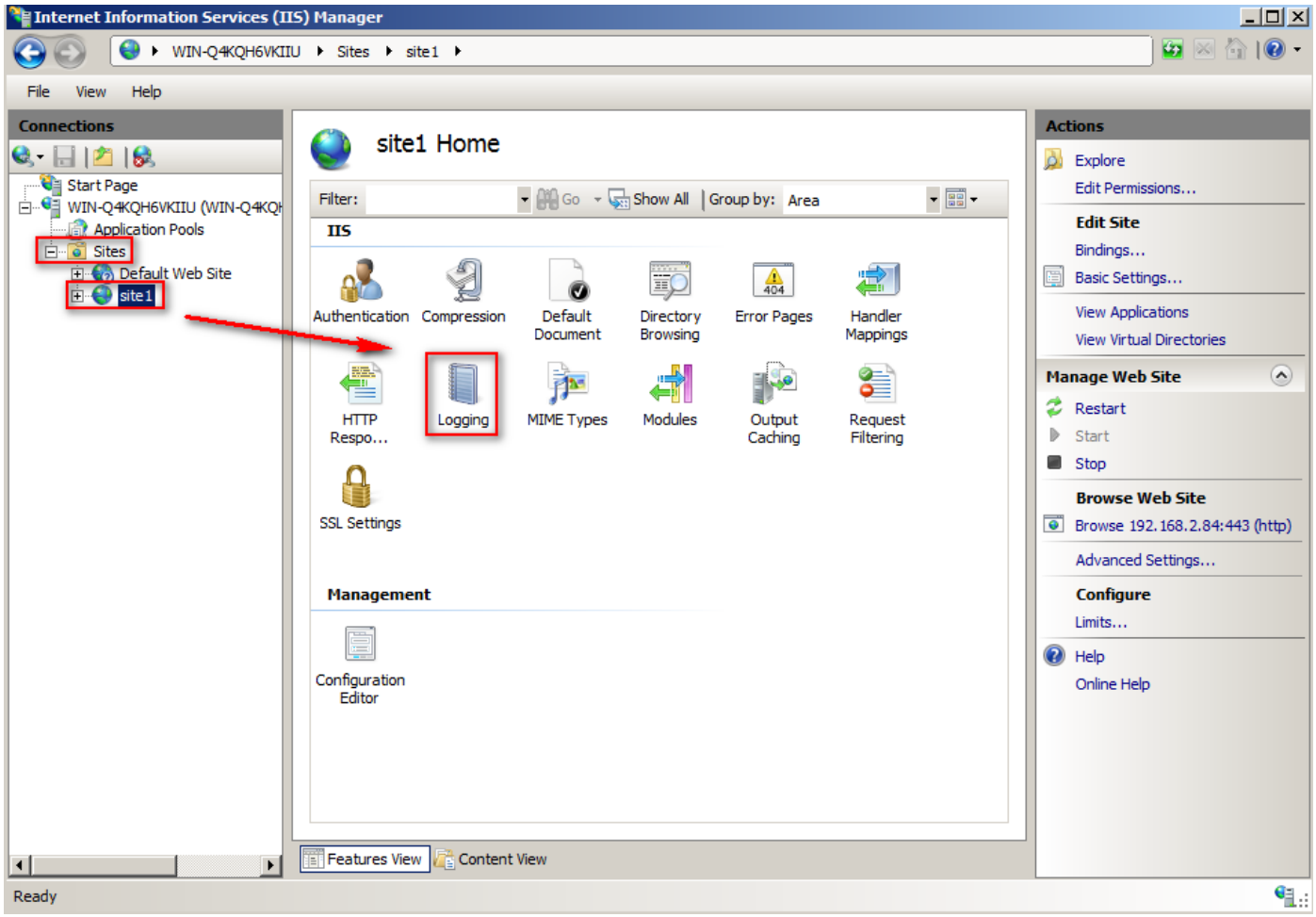


5. Choose the logging path by click on [Browse]. The default path is %SystemDrive%\inetpub\logs\LogFiles in Windows 2008. Choose language code [UTF-8], then select [Schedule] with pull down entry [Hourly]. Check [Use local time for file naming and rollover], press [Apply] to finish Server Logging Options.

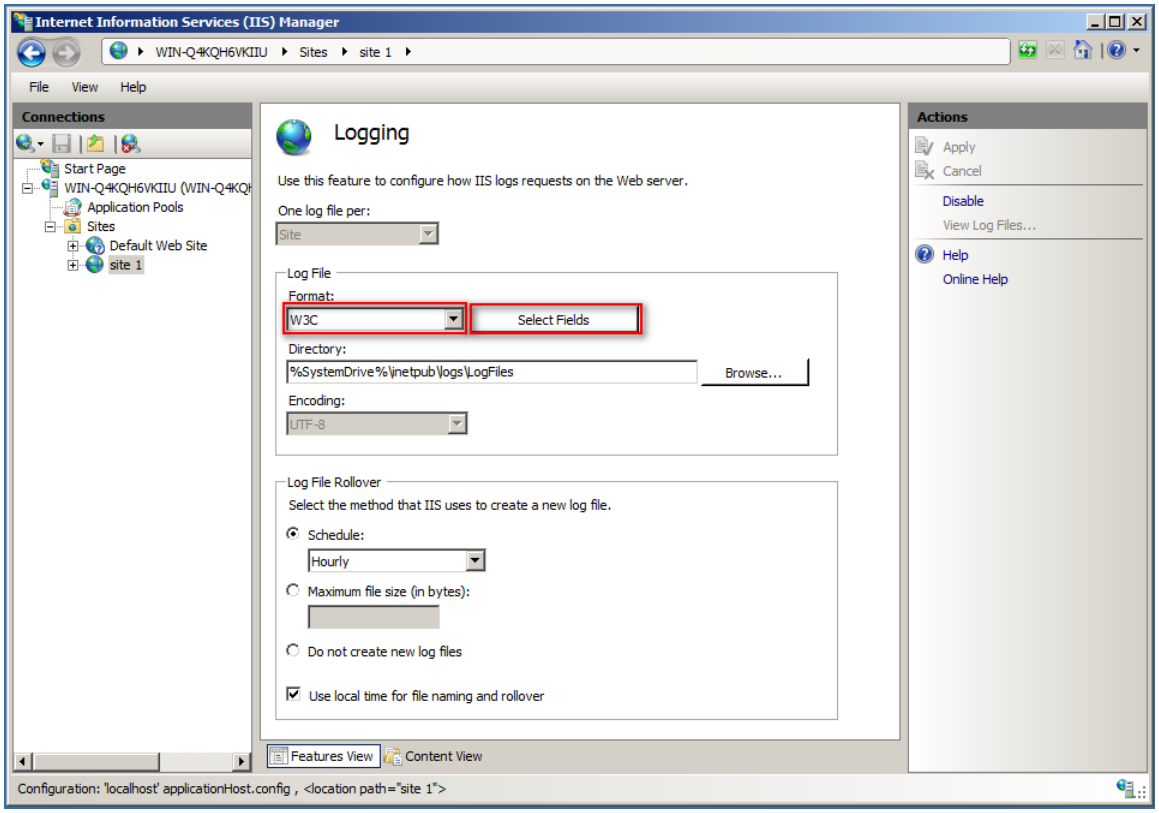


Remark: The version 3.1.35 (or later) of N-Reporter supports BIG5 and GB2312. If it is BIG5 encode in the setting, IIS Server will store web logs and send syslog message by BIG5 encode. So when adding devices on IIS server, please select BIG5 encode.

6. Set up the Logging Options for each individual site, start by double click [Sites / site1]. For example to set the logging options of "site1". Double click [Logging].

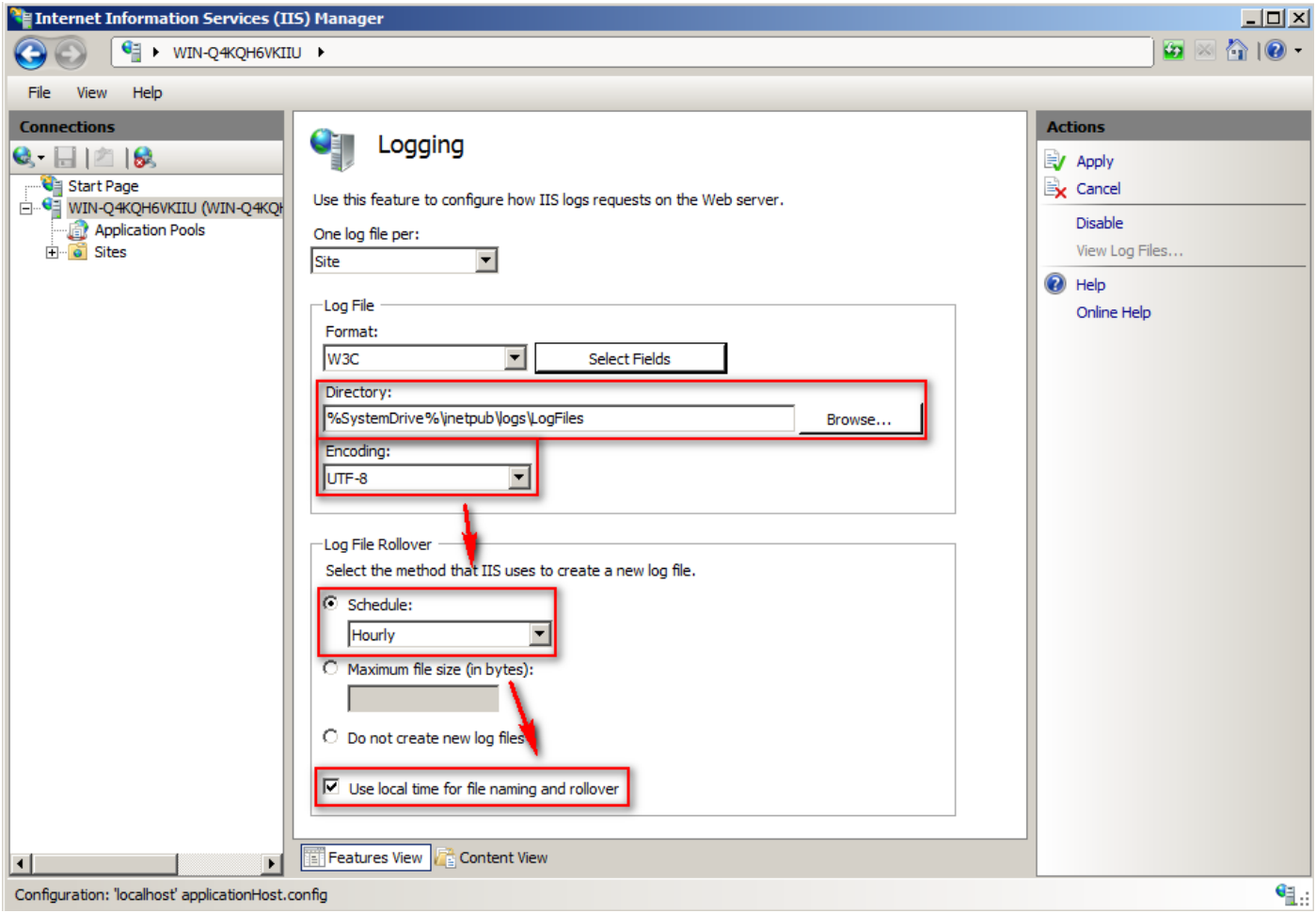


7. Choose [W3C]. Click [Select Fields].



8. Check Date (date)、Time (time) 、Client IP Address (c-ip) 、User name(cs_username) 、Server name (s-computername)、Server IP Address (s-ip) 、Server Port(s-port)、Method (cs-method)、URI Stem(cs-uri-stem)、URI Query (cs-uri-query) 、Protocol Status (sc-status)、Bytes Sent (sc-bytes)、Bytes Received (cs-bytes) 、Time Taken (time-taken)、User Agent (cs(User-Agent)) of the [W3C Logging Fields]. Press [OK] to finish Site Logging Options.

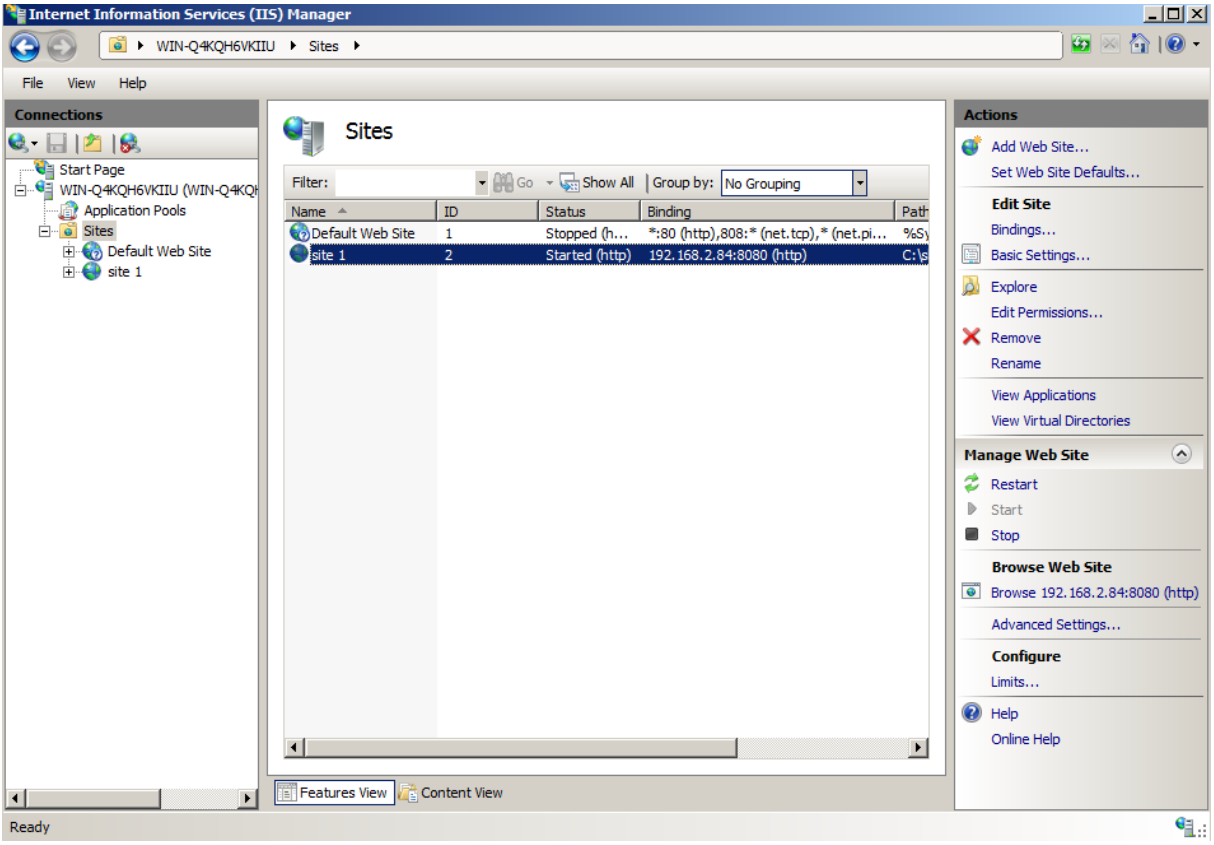
9. Choose the logging path by click on [Browse]. The default path is %SystemDrive%\inetpub\logs\LogFiles in Windows 2008. Select [Schedule] with pull down entry [Hourly].。Select [Use local time for file naming and rollover], press [Apply] to finish the setup for "site1" .



Remark：When installing more than one Web site, please repeat step 6 to step 9 for each web site.

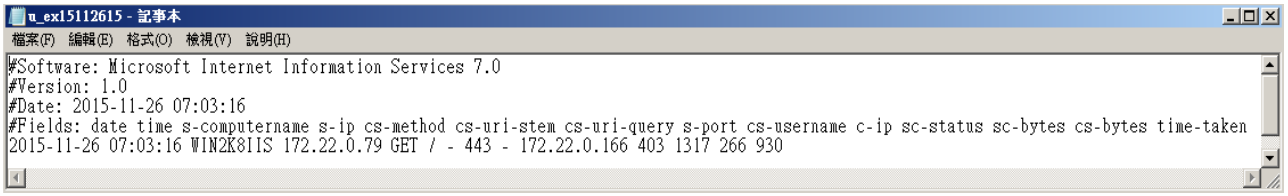
10. Site logging file directory is W3SVC$var as its format for multiple sites in IIS Server, where $var is variable. After all, please confirm the proper site logging file directory setup of site1.

IP address of site1 is 192.168.2.84:80. Browse site1.



Check the log of W3SVC1and W3SVC2. The log path of "site1"is C:\inetpub\logs\LogFiles\W3SVC2.

To check if the log is enabled, view the log file after several minutes once access the site “site 1”.



3 Setup NXLOG

1. Logon the IIS Server by Administrator.
2. **Download NXLOG：http://sourceforge.net/projects/nxlog-ce/files/**

   Download 『nxlog-ce-x.x.x.msi』.
3. **Install NXLOG : Install the NXLOG by double click on the file 『nxlog-ce-x.x.x.msi』ro install NXLOG.**

   Remark：NXLOG install at "C:\Program Files\nxlog\conf\nxlog.conf" in 32 Bit OS.

   NXlog install at "C:\Program Files (x86)\nxlog\conf\nxlog.conf" in 64 Bit OS.
4. **NXLOG Configuration：**

   (1) Download IIS NXLOG config file: nxlog_iis.conf：

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

   Edit NXLOG configuration file "C:\Program Files (x86)\nxlog\conf\nxlog.conf". Paste nxlog_iis.conf over nxlog.conf.

```
## 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. Fill in a proper installation path of NXLOG in the **green portion.**

For example "define ROOT C:\Program Files (x86)\nxlog" for 64 Bit OS.

b. **For yellow portion** " define IIS_SITE1 $dir ". Where $dir is the log path of IIS Server.

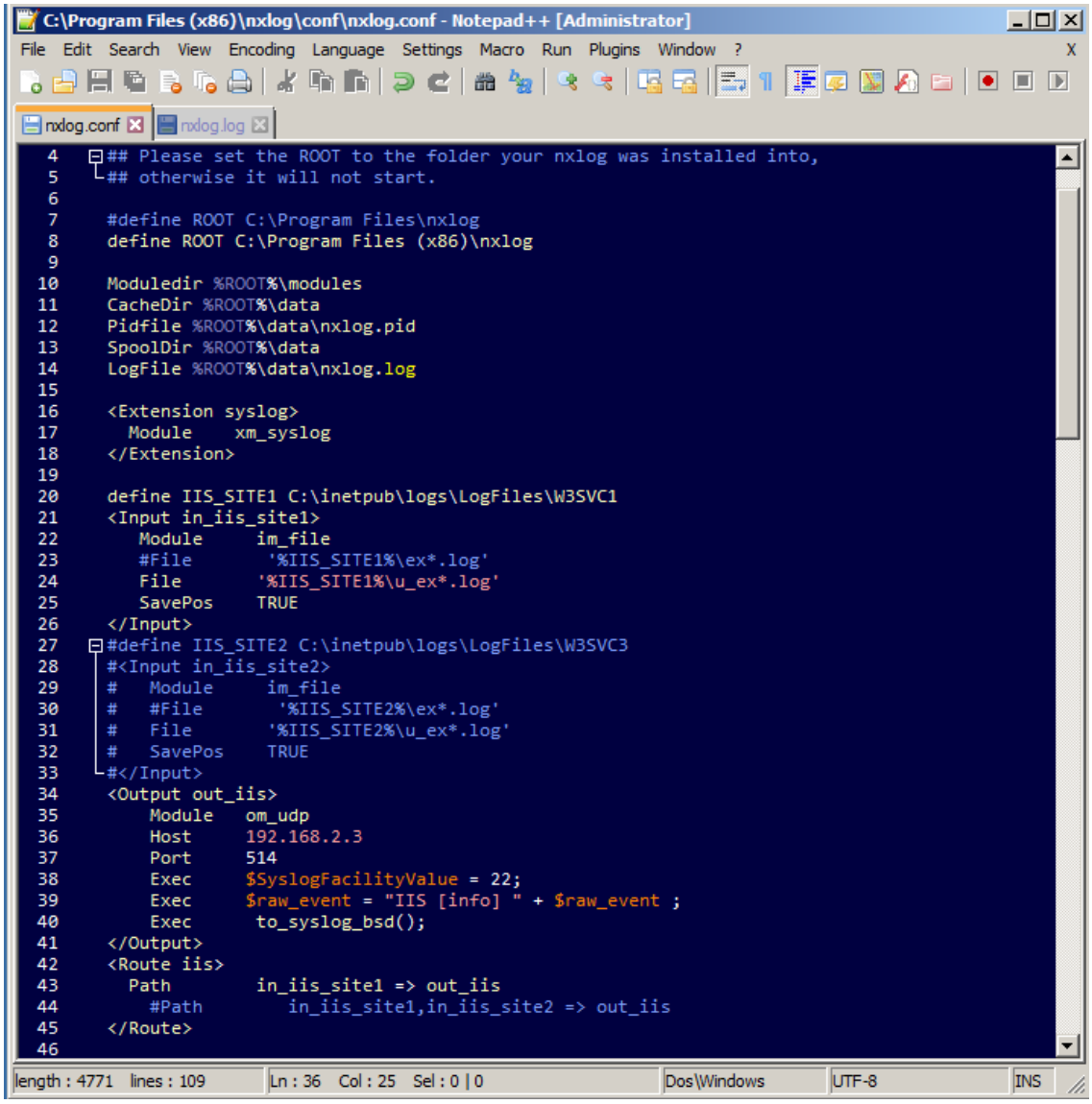
For example "C:\inetpub\logs\LogFiles\W3SVC2".

c. **For red portion** " Host $N_Reporter_IP", please fill in the IP address of the N-Reporter.

For example, 192.168.2.3.

d. In this example, the language code is UTF-8. The log file format is u_ex*.log. Therefore the path is " File '%IIS_SITE1%\u_ex*.log'". For BIG5 or GB2312 encode, the log file format is ex*.log. Therefore the path is " File '%IIS_SITE1%\ex*.log'".

For example :



e. If there are multiple sites in IIS Server, please remove the remark "#" for line 27 to 33. And remove the remark "#" for line 44 to set " Path in_iis_site1,in_iis_site2 => out_iis". Send out the log of these two site by syslog format.

(2) Enable NXLOG：

a. [Start]→[All Programs]→[Accessories]. Right click [Command Prompt], click [Run as administrator].

Command line：

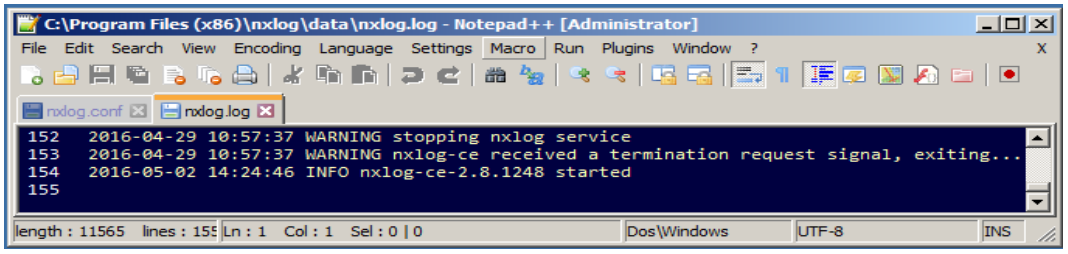
```
net stop nxlog
net start nxlog
```

b. [Start] → [All Programs]→[Administrative Tools]→[Services]. Right click [nxlog], click [Start] or [Restart].

(3) Check NXLOG function：

Check the log file of NXLOG. The path is ″ C:\Program Files (x86)\nxlog\data\nxlog.log″ .

If there is no error message here, it means NXLOG run without problem.



N-Partner

Sales Support：sales@npartnertech.com

TAC Support：support@npartnertech.com