



N-Partner

N-REPORTER

如何管理 SQL Server 登入审核

V 1.1.5 (简体)

前言

此文件主要描述如何使用 N-Reporter 接收 SQL Server 的 log。首先必须开启 SQL Server 的 C2 audit mode 功能，透过 C2 audit mode，系统将 SQL Server 的 log 送至 Windows 的 eventlog。接着利用 NXLOG 将 eventlog 转成 syslog，再发送至 N-Reporter。

N-Reporter 支持 SQL 2005/2008/2012 Server，本例为 Windows 2003 环境安装 SQL 2005 版本的实际范例。

文件章节如下：

联络信息	1
1 如何开启 SQL Server 的 C2 audit mode	2
2 如何设定 NXLOG	8
2.1 配置 Windows Server 2003	8
2.2 配置 Windows Server 2008	12
2.3 配置 Windows Server 2012	16

联络信息

N-Partner 公司联络方式：

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 如何开启 SQL Server 的 C2 audit mode

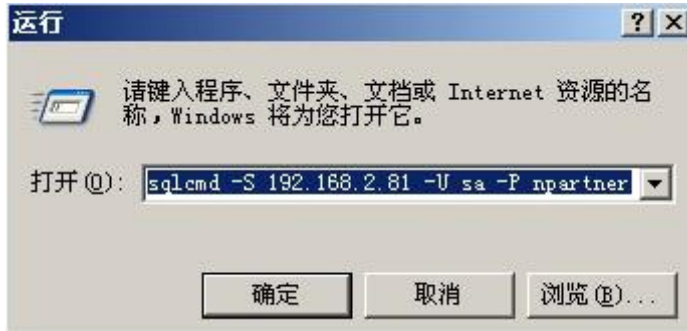
启动 C2 audit mode 提供两个方法，设定的步骤如下：

注：第一个方法必须先要在[组策略编辑器]中启动[Windows 防火墙：允许远程管理例外]，设定也较为繁杂。如果环境有安装 SQL Server Management Studio 工具，建议以第二个方法设定。

1 以 transact-sql 登入 Server，开启 C2 audit mode：

(1) 在『命令提示字符』输入 sqlcmd -S 192.168.2.81 -U sa -P npartner，其中-S 为 SQL Server 的 IP，-U 为 user，-P 为 password。请使用数据库的管理者登入。

本例管理者为 sa，密码为 npartner，IP 为 192.168.2.81。



(2) 切换 master 数据库。

输入 use master，按 enter。输入 go，按 enter 执行 sql 命令。

```
1> use master
2> go
已將資料庫內容變更為 'master'。
```

(3) 显示进阶组态选项。预设 show advanced option 为 0，将其改为 1。

a. 输入 Exec sp_configure 'show advanced option','1'，按 enter。

b. 输入 go，按 enter。

c. 输入 reconfigure，按 enter。

```
1> Exec sp_configure 'show advanced option','1'
2> go
組態選項 'show advanced options' 從 0 變更為 1。請執行 RECONFIGURE 陳述式來安裝。
1> Reconfigure
```

(4) 设定 C2 Audit。

a. 输入 Exec sp_configure 'c2 audit mode','1'，按 enter。

b. 输入 Go，按 enter。

c. 输入 Reconfigure，按 enter。

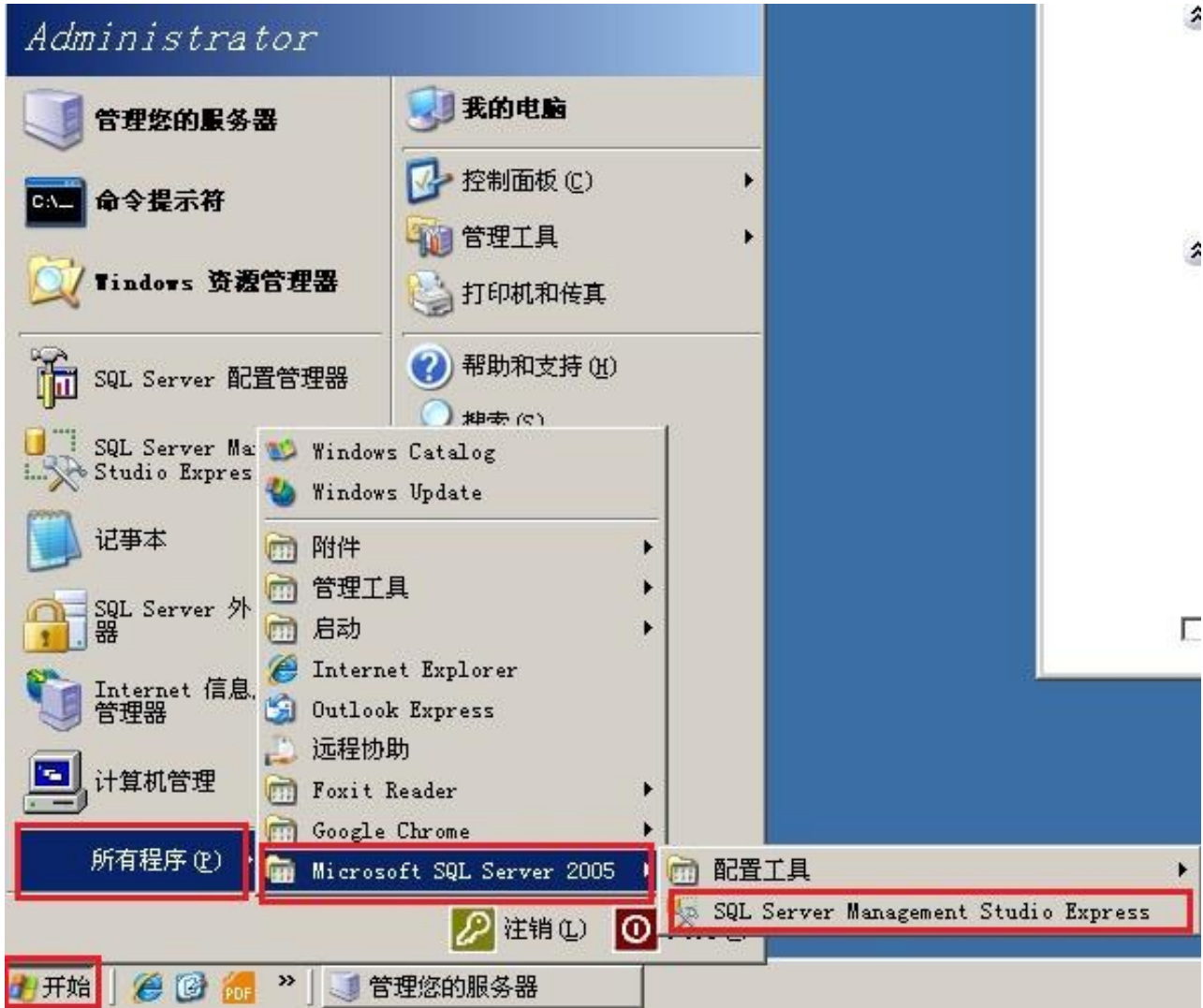
```
1> Exec sp_configure 'c2 audit mode','1'
2> go
組態選項 'c2 audit mode' 從 0 變更為 1。請執行 RECONFIGURE 陳述式來安裝。
1> Reconfigure
```

(5) 注销

输入 exit，按 enter。

2 使用 SQL Server Management Studio 登入 SQL Server , 开启 C2 audit mode :

(1) [开始] → [所有程序] → [Microsoft SQL Server] → [SQL Server Management Studio]。



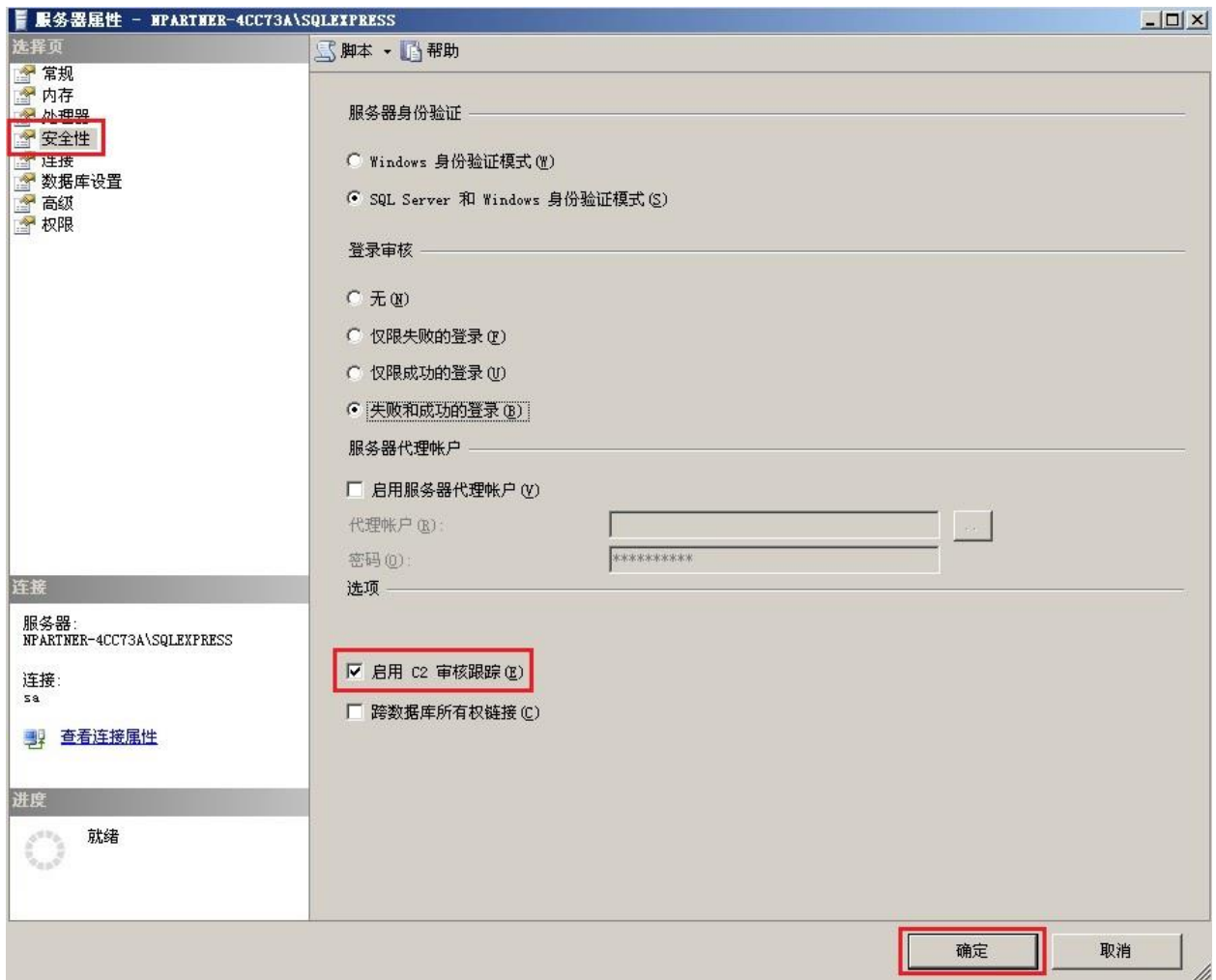
- (2) 本例服务器类型下拉[数据库引擎]，输入服务器名称，验证下拉[SQL Server 身份验证]，下拉默认用户 sa，输入密码"npartner"，鼠标左点[连接]，登入 SQL Server。



- (3) 在[对象资源管理器]窗口中鼠标右点 SQL Server，左点[属性]。

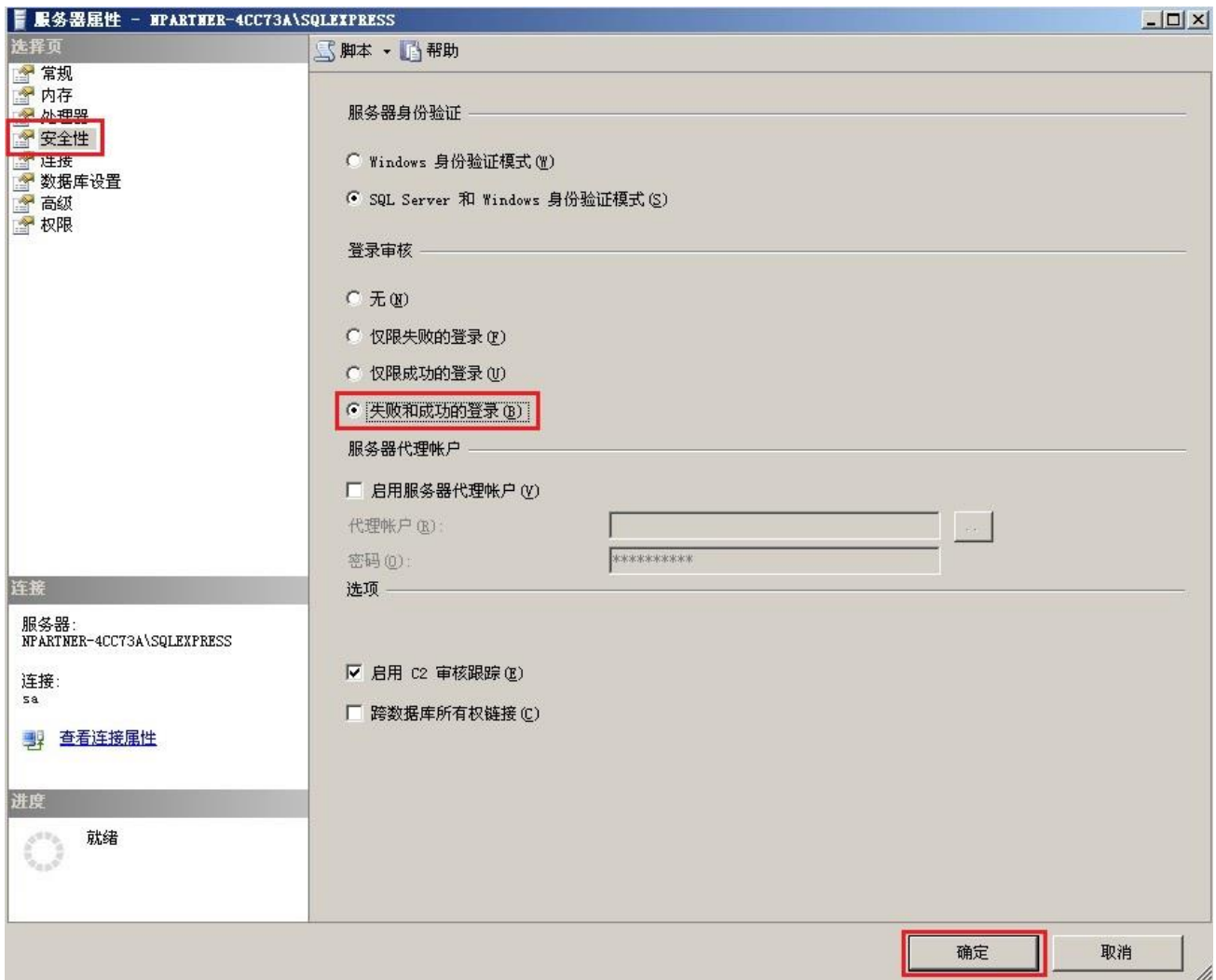


(4) 左点[安全性], 勾选[启用 C2 稽核追踪], 左点[确定], 完成开启 C2 audit mode。



3 同时审核失败和成功的登录:

- (1) 使用 SQL Server Management Studio 登入 SQL Server。
- (2) 在[对象资源管理器]窗口中鼠标右点 SQL Server，左点[属性]。
- (3) 左点[安全性]，勾选[失败和成功的登录]，左点[确定]。



4 重新启动 SQL SERVICE。有两个方法：

- (1) 『命令提示字符』输入 net stop mssqlserver 停止 SQL 服务，再输入 net start mssqlserver 开启 SQL 服务。
- (2) 使用 SQL Server Management Studio 登入后，鼠标右点 SQL Server，左点重新启动，重启 SQL 服务。如下图。



2 如何设定 NXLOG

2.1 配置 Windows Server 2003

1. 下载 NXLOG :

浏览 URL <http://sourceforge.net/projects/nxlog-ce/files/> ,
下载最新版 nxlog-ce-x.x.xxxx.msi , 本例下载 nxlog-ce-2.7.1191.msi。

2. 安装 NXLOG :

鼠标双点 nxlog-ce-2.7.1191.msi , 左点[Install] , 执行安装。

3. 下载 Windows 2003 NXLOG 配置文件 nxlog_win2k3.conf :

浏览 URL : http://www.npartnertech.com/download/tech/nxlog_win2k3.conf

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

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

64 位系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2k3.conf 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>

<Input in_eventlog>
# For windows 2003 and earlier use the following:
  Module im_mseventlog
  Exec parse_syslog_bsd(); \
    if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID
== 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID
== 628 or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID
== 635 or $EventID == 636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID
== 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
    else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
    else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
  else\
  {\
    drop();\
  }
</Input>

<Output out_eventlog>
  Module om_udp
  Host 192.168.2.64
  Port 514
  Exec $Message = string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
    else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route eventlog>
  Path in_eventlog => out_eventlog
</Route>

```

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 "。

红色部位输入 N-Reporter IP，本例输入 " 192.168.2.64 "。

设定范例如下：

```

7 #define ROOT C:\Program Files\nxlog
8 define ROOT C:\Program Files (x86)\nxlog
9
10 Moduledir %ROOT%\modules
11 CacheDir %ROOT%\data
12 Pidfile %ROOT%\data\nxlog.pid
13 SpoolDir %ROOT%\data
14 LogFile %ROOT%\data\nxlog.log
15
16 <Extension syslog>
17 Module xm_syslog
18 </Extension>
19 <Input in_eventlog>
20 # For windows 2003 and earlier use the following:
21 Module im_meventlog
22 Exec parse_syslog_bsd(); \
23     if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID == 540
24         or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID == 628
25         or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635
26         or $EventID == 636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID == 646
27         or $EventID == 647) { $SyslogFacilityValue = 13; } \
28     else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
29     else if ($SourceName =~ /*MSSQL*/) { $SyslogFacilityValue = 18; } \
30     else \
31     { \
32         drop(); \
33     } \
34 </Input>
35
36 <Output out_eventlog>
37 Module cm_udp
38 Host 192.168.2.64
39 Port 514
40 Exec $Message = string($EventID) + ": " + $Message;
41 Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
42     else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
43     else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
44 Exec to_syslog_bsd();
45 </Output>
46
47 <Route eventlog>
48 Path in_eventlog => out_eventlog
49 </Route>

```

4. 启动 NXLOG：

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：

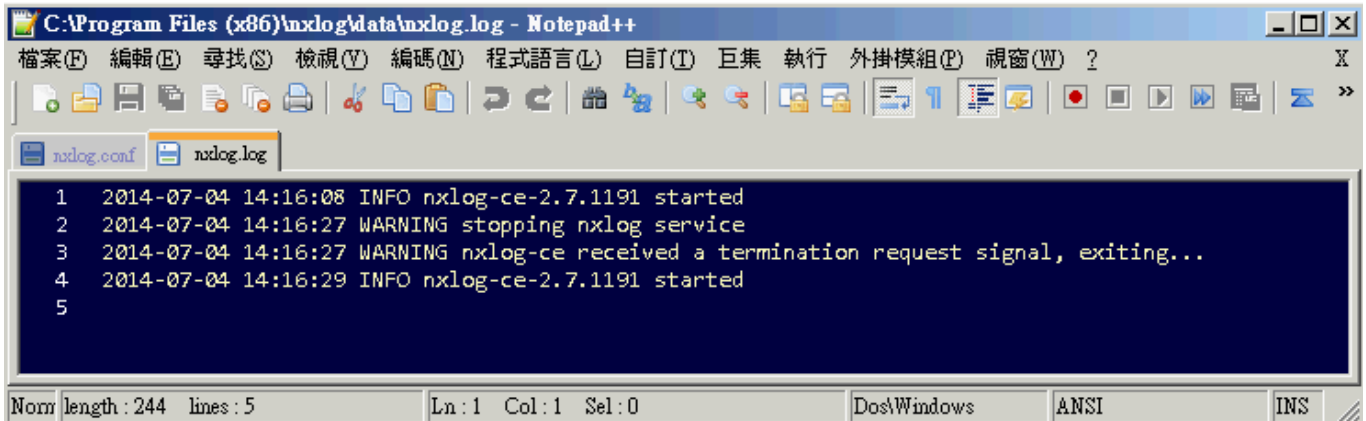
```
net stop nxlog
```

```
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]。

5. 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。



```

1 2014-07-04 14:16:08 INFO nxlog-ce-2.7.1191 started
2 2014-07-04 14:16:27 WARNING stopping nxlog service
3 2014-07-04 14:16:27 WARNING nxlog-ce received a termination request signal, exiting...
4 2014-07-04 14:16:29 INFO nxlog-ce-2.7.1191 started
5

```

6. MS SQL 设备时语系选择：

Windows Server 2003 繁体版环境请选择[BIG5]编码。

Windows Server 2003 简体版环境请选择[GB2312]编码。

Windows Server 2003 英文版环境请选择[UTF8]编码。

注：因 NXLOG 没有 Eventlog to Syslog Utility 将事件编码转成 UTF8 编码的功能，所以新增设备时请注意语系选择，避免出现乱码。

7. 新增 MS SQL 设备时 Facility 请选择 " (18) local use 2 (local2) " 。

2.2配置 Windows Server 2008

1. 下载 NXLOG :

浏览 URL <http://sourceforge.net/projects/nxlog-ce/files/>

下载最新版 nxlog-ce-x.x.xxxx.msi , 本例下载 nxlog-ce-2.7.1191.msi。

2. 安装 NXLOG :

鼠标双点 nxlog-ce-2.7.1191.msi , 左点[Install] , 执行安装。

3. 下载 Windows 2008 NXLOG 配置文件 nxlog_win2k8.conf :

浏览 URL : http://www.npartnertech.com/download/tech/nxlog_win2k8.conf

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

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

64 位系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2k8.conf 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>

<Input in_eventlog>
# For windows 2008/vista/7/8/2012 and latter use the following:
  Module im_msvistalog
  Exec parse_syslog_bsd(); \
    if ($EventID == 4768 or $EventID == 4769 or $EventID == 4771 or $EventID == 4624 or $EventID == 4625 or $EventID == 4634 or
$EventID == 4647 or $EventID == 4648 or $EventID == 4656 or $EventID == 4719 or $EventID == 4720 or $EventID == 4722 or $EventID ==
4723 or $EventID == 4724 or $EventID == 4725 or $EventID == 4726 or $EventID == 4727 or $EventID == 4728 or $EventID == 4729 or
$EventID == 4730 or $EventID == 4731 or $EventID == 4732 or $EventID == 4733 or $EventID == 4734 or $EventID == 4735 or $EventID ==
4737 or $EventID == 4738 or $EventID == 4739 or $EventID == 4741 or $EventID == 4742 or $EventID == 4743) { $SyslogFacilityValue = 13; } \
\
    else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
    else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
  else \
  {
    drop(); \
  }
</Input>

<Output out_eventlog>
  Module om_udp
  Host 192.168.2.64
  Port 514
  Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
    else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route eventlog>
  Path in_eventlog => out_eventlog
</Route>

```

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` "。

红色部位输入 N-Reporter IP，本例输入 " `192.168.2.64` "。

设定范例如下：

```

2  ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
3
4  ## Please set the ROOT to the folder your nxlog was installed into,
5  ## otherwise it will not start.
6
7  #define ROOT C:\Program Files\nxlog
8  define ROOT C:\Program Files (x86)\nxlog
9
10 ModuleDir %ROOT%\modules
11 CacheDir %ROOT%\data
12 Pidfile %ROOT%\data\nxlog.pid
13 SpoolDir %ROOT%\data
14 LogFile %ROOT%\data\nxlog.log
15
16 <Extension syslog>
17   Module xm_syslog
18 </Extension>
19 <Input in_eventlog>
20 # For windows 2008/vista/7/8/2012 and latter use the following:
21   Module im_msvistalog
22   Exec parse_syslog_bsd(); \
23     if ($EventID == 4768 or $EventID == 4769 or $EventID == 4771 or $EventID == 4624 or $EventID == 4625 or $EventID == 4634 or $EventID == 4647
24     or $EventID == 4648 or $EventID == 4656 or $EventID == 4719 or $EventID == 4720 or $EventID == 4722 or $EventID == 4723 or $EventID == 4724
25     or $EventID == 4725 or $EventID == 4726 or $EventID == 4727 or $EventID == 4728 or $EventID == 4729 or $EventID == 4730 or $EventID == 4731
26     or $EventID == 4732 or $EventID == 4733 or $EventID == 4734 or $EventID == 4735 or $EventID == 4737 or $EventID == 4738 or $EventID == 4739
27     or $EventID == 4741 or $EventID == 4742 or $EventID == 4743) { $SyslogFacilityValue = 13; } \
28     else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
29     else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
30     else \
31     {
32       drop();\
33     }
34 </Input>
35
36 <Output out_eventlog>
37   Module om_udp
38   Host 192.168.2.64
39   Port 514
40   Exec $Message = string($SourceName) + " : " + string($EventID) + " : " + $Message;
41   Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
42   else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
43   else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
44   Exec to_syslog_bsd();
45 </Output>
46
47 <Route eventlog>
48   Path in_eventlog => out_eventlog
49 </Route>

```

4. 启动 NXLOG：

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[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]。

5. 检查 NXLOG 是否正常启动：

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



```

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(T) 巨集 執行 外掛模組(P) 視窗(W) ?
nxlog.conf nxlog.log
1 2014-07-03 17:57:22 WARNING stopping nxlog service
2 2014-07-03 17:57:22 WARNING nxlog-ce received a termination request signal, exiting...
3 2014-07-03 17:57:23 INFO nxlog-ce-2.7.1191 started
4
length:192 lines:4 Ln:1 Col:1 Sel:0 Dos\Windows ANSI INS

```

6. 新增 MS SQL 设备时 Facility 请选择 " (18) local use 2 (local2) "。

2.3配置 Windows Server 2012

1. 下载 NXLOG :

浏览 URL <http://sourceforge.net/projects/nxlog-ce/files/>

下载最新版 nxlog-ce-x.x.xxxx.msi , 本例下载 nxlog-ce-2.7.1191.msi。

2. 安装 NXLOG :

鼠标双点 nxlog-ce-2.7.1191.msi , 左点[Install] , 执行安装。

3. 下载 Windows 2012 NXLOG 配置文件 nxlog_win2012.conf :

浏览 URL : http://www.npartnertech.com/download/tech/nxlog_win2012.conf

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

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

64 位系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2012.conf 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>

<Input in_eventlog>
# For windows 2008/vista/7/8/2012 and latter use the following:
  Module im_msvistalog
  Exec parse_syslog_bsd(); \
    if ($EventID == 4768 or $EventID == 4769 or $EventID == 4771 or $EventID == 4624 or $EventID == 4625 or $EventID == 4634 or
$EventID == 4647 or $EventID == 4648 or $EventID == 4656 or $EventID == 4719 or $EventID == 4720 or $EventID == 4722 or $EventID ==
4723 or $EventID == 4724 or $EventID == 4725 or $EventID == 4726 or $EventID == 4727 or $EventID == 4728 or $EventID == 4729 or
$EventID == 4730 or $EventID == 4731 or $EventID == 4732 or $EventID == 4733 or $EventID == 4734 or $EventID == 4735 or $EventID ==
4737 or $EventID == 4738 or $EventID == 4739 or $EventID == 4741 or $EventID == 4742 or $EventID == 4743) { $SyslogFacilityValue = 13; } \
\
    else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
    else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
  else \
  {
    drop(); \
  }
</Input>

<Output out_eventlog>
  Module om_udp
  Host 192.168.2.64
  Port 514
  Exec $Message = string($SourceName) + " " + string($EventID) + " " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
    else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route eventlog>
  Path in_eventlog => out_eventlog
</Route>

```

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` "。

红色部位输入 N-Reporter IP，本例输入 " `192.168.2.64` "。

设定范例如下：

```

6
7 #define ROOT C:\Program Files\nxlog
8 define ROOT C:\Program Files (x86)\nxlog
9
10 Moduledir %ROOT%\modules
11 CacheDir %ROOT%\data
12 Pidfile %ROOT%\data\nxlog.pid
13 SpoolDir %ROOT%\data
14 LogFile %ROOT%\data\nxlog.log
15
16 <Extension syslog>
17   Module    xm_syslog
18 </Extension>
19 <Input in_eventlog>
20 # For windows 2008/vista/7/8/2012 and latter use the following:
21   Module    im_msvistalog
22   Exec      parse_syslog_bsd(); \
23     if ($EventID == 4768 or $EventID == 4769 or $EventID == 4771 or $EventID == 4624 or $EventID == 4625 or $EventID == 4634 or $EventID == 4647 or
24     $EventID == 4648 or $EventID == 4656 or $EventID == 4719 or $EventID == 4720 or $EventID == 4722 or $EventID == 4723 or $EventID == 4724 or
25     $EventID == 4725 or $EventID == 4726 or $EventID == 4727 or $EventID == 4728 or $EventID == 4729 or $EventID == 4730 or $EventID == 4731 or
26     $EventID == 4732 or $EventID == 4733 or $EventID == 4734 or $EventID == 4735 or $EventID == 4737 or $EventID == 4738 or $EventID == 4739 or
27     $EventID == 4741 or $EventID == 4742 or $EventID == 4743) { $SyslogFacilityValue = 13; } \
28     else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
29     else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
30     { \
31       drop(); \
32     }
33 </Input>
34
35 <Output out_eventlog>
36   Module    om_udp
37   Host      192.168.2.64
38   Port      514
39   Exec      $Message = string($SourceName) + " : " + string($EventID) + " : " + $Message;
40   Exec      if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
41             else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
42             else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
43   Exec      to_syslog_bsd();
44 </Output>
45
46 <Route eventlog>
47   Path      in_eventlog => out_eventlog
48 </Route>

```

3. 启动 NXLOG：

步骤 a：利用[Windows PowerShell]启动 NXLOG 或 步骤 b：[服务]启动 NXLOG。

a. 鼠标左点[开始]，鼠标右点[Windows PowerShell]，左点[以系统管理员身分执行]。

[Windows PowerShell]输入：

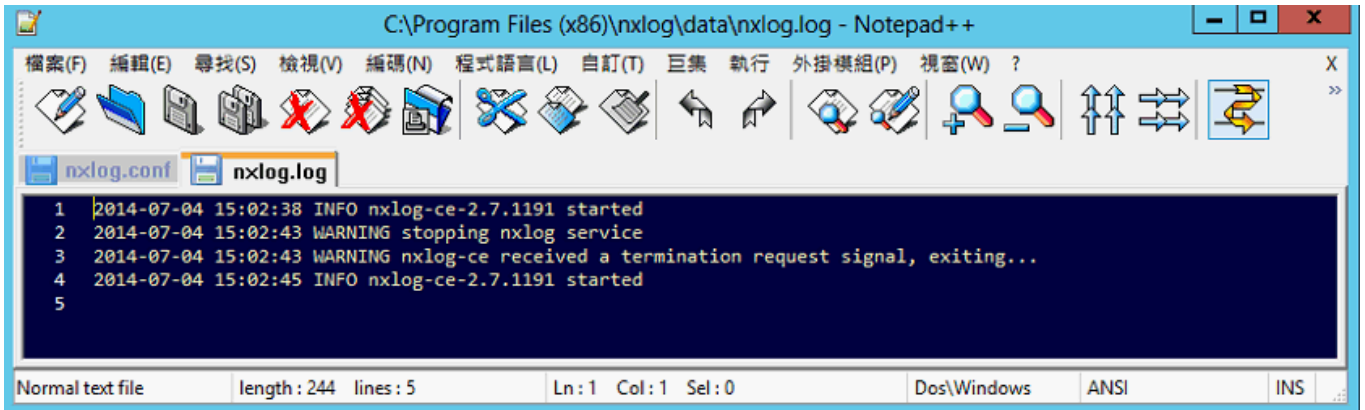
```
net stop nxlog
```

```
net start nxlog
```

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

4. 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。



```

1 2014-07-04 15:02:38 INFO nxlog-ce-2.7.1191 started
2 2014-07-04 15:02:43 WARNING stopping nxlog service
3 2014-07-04 15:02:43 WARNING nxlog-ce received a termination request signal, exiting...
4 2014-07-04 15:02:45 INFO nxlog-ce-2.7.1191 started
5

```

5. 新增 MS SQL 设备时 Facility 请选择 " (18) local use 2 (local2) " 。



采购与销售合作 : sales@npartnertech.com

技术咨询 : support@npartnertech.com