



N-Partner

N-REPORTER

使用者如何管理 Exchange Server
郵件追蹤記錄稽核

V 005 (繁體)

前言

本文件描述 N-Reporter 使用者如何管理 Exchange Server 郵件追蹤(Message Tracking)記錄稽核。第一步先配置 Exchange 的郵件追蹤記錄。第二步利用 Open Source 工具 NXLOG Community Edition(簡稱 NXLOG)將郵件追蹤記錄轉成 Syslog，發送至 N-Reporter 接收。因 Windows 與 Exchange 版本差異，使用[Exchange 管理主控台]配置可能會有差異，本文件配置的環境為 Windows 2003 64 位元作業系統安裝 Exchange 2007、Windows 2008 R 2 作業系統安裝 Exchange 2010 與 Windows 2012 作業系統安裝 Exchange 2013。

郵件追蹤記錄是與執行 Exchange Server 且已安裝集線傳輸伺服器角色(Hub Transport server role)、信箱伺服器角色(Mailbox server role)或邊際傳輸伺服器角色(Edge Transport server role)的電腦往返傳送郵件之所有郵件活動的詳細記錄。已安裝用戶端存取伺服器角色或整合通訊伺服器角色的 Exchange Server 不會有郵件追蹤記錄。本配置文件適用安裝集線傳輸伺服器角色或邊際傳輸伺服器角色的 Exchange Server。

註：Exchange Server 預設啟用郵件追蹤。

文件章節如下：

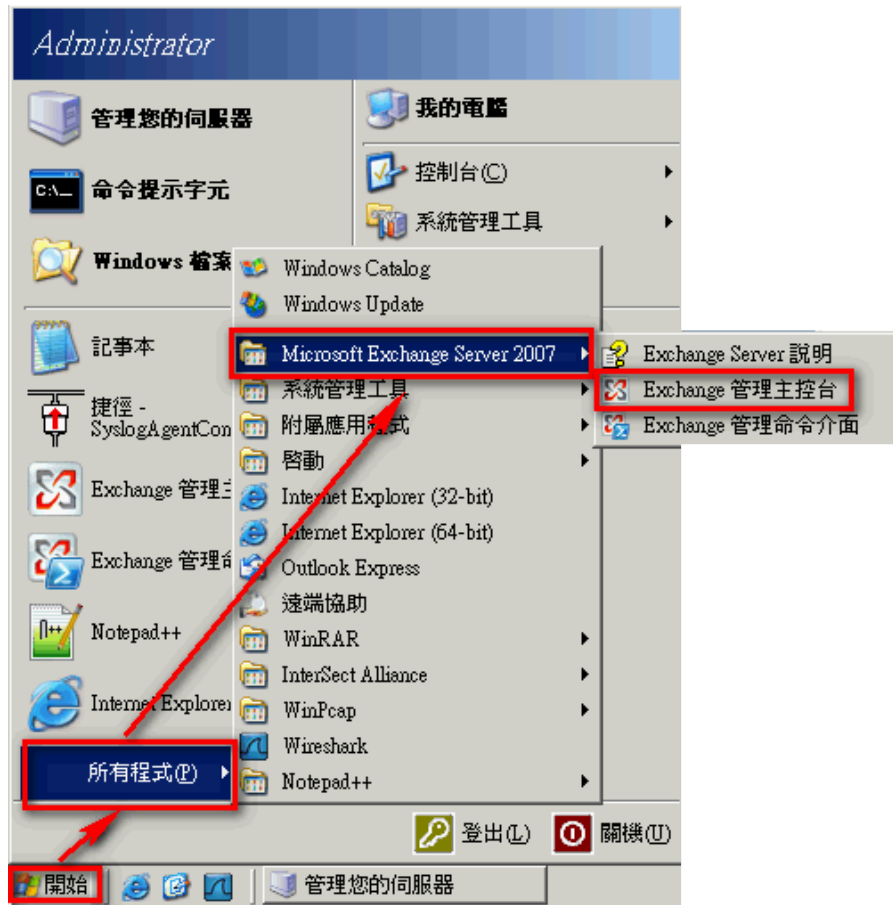
1 配置 Exchange Server 2007 郵件追蹤記錄	2
2 配置 Exchange Server 2010 郵件追蹤記錄	6
3 配置 Exchange Server 2013 郵件追蹤記錄	9
4 配置 NXLOG	12
5 將設備加入系統及 Syslog 資料格式及 Facility 的設定.....	15
連絡資訊	16

1 配置 Exchange Server 2007 郵件追蹤記錄

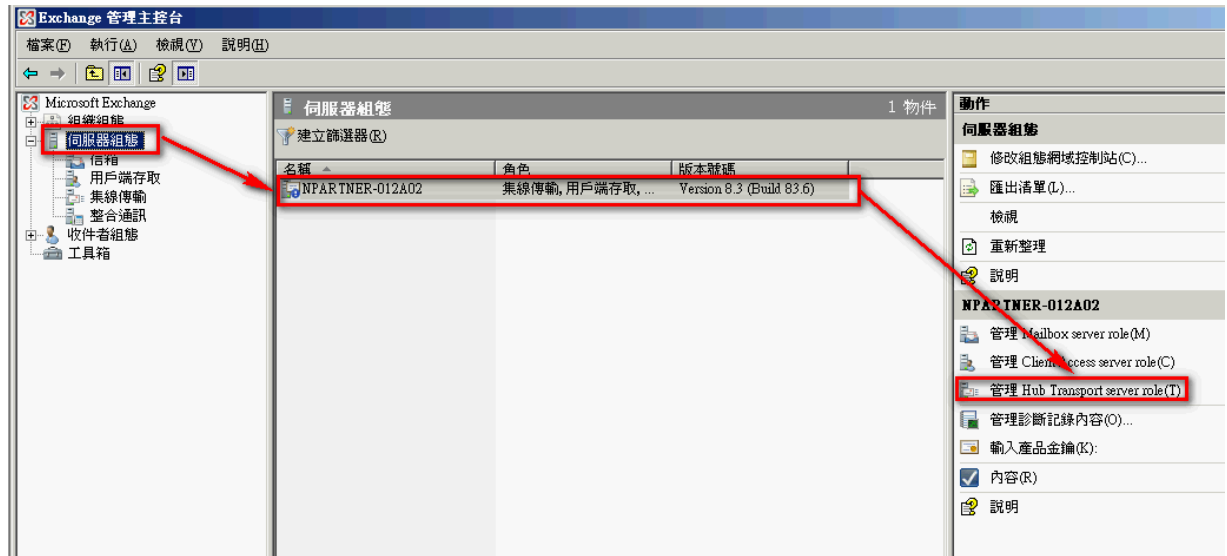
可選擇[Exchange 管理主控台]或[Exchange 管理命令介面]配置郵件追蹤記錄。

一、使用[Exchange 管理主控台] 配置：

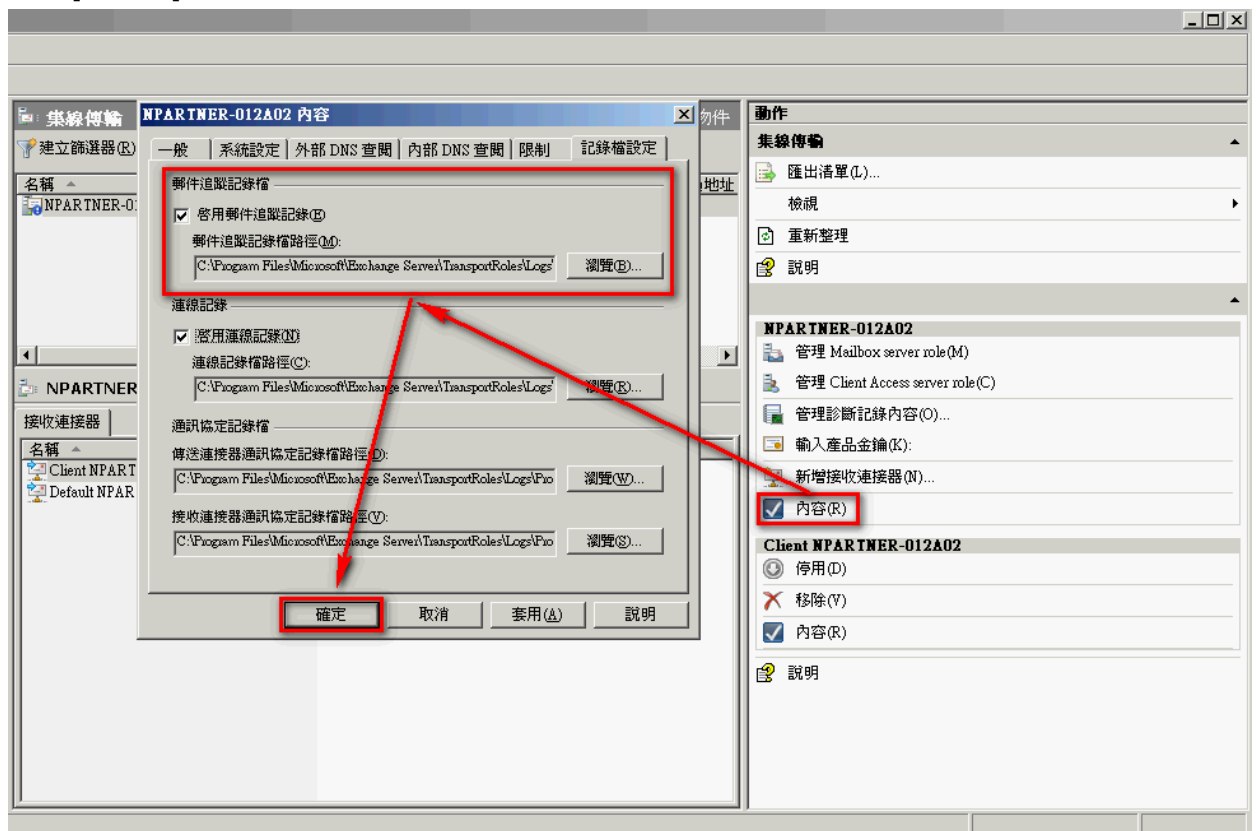
- (1) 以系統管理者 Administrator 登入 Exchange Server。
- (2) 滑鼠左點[開始] → [所有程式] → [Microsoft Exchange Server 2007]
→ [Exchange 管理主控台]。



- (3) 滑鼠左點[伺服器組態]，左點 Exchange Server，本例為"NPARTNER-012A02"，左點 [管理 Hub Transport server role]。

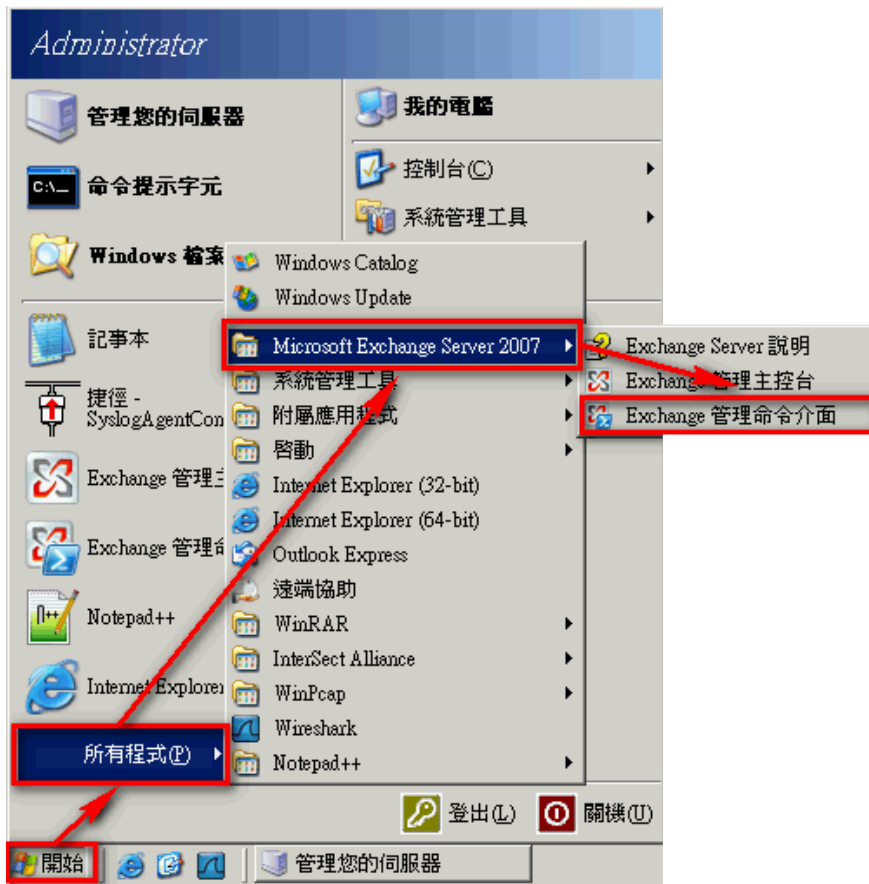


- (4) 滑鼠左點[內容]。勾選[啟用郵件追蹤記錄]，左點[瀏覽]，設定郵件追蹤記錄檔路徑，預設"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"。左點[確定]，完成配置。



二、使用[Exchange 管理命令介面] 配置：

- (1) 以系統管理者 Administrator 登入 Exchange Server。
- (2) 滑鼠左點[開始] → [所有程式] → [Microsoft Exchange Server 2007] → [Exchange 管理命令介面]。



- (3) 啟用郵件追蹤。命令列輸入：

```
Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath
<LocalFilePath>
```

或

```
Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath
<LocalFilePath>
```

<ServerIdentity>為 Exchange Server 的電腦名稱，<LocalFilePath>為郵件追蹤記錄的路徑，預設為"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"。

本例輸入：

```
Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program
Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"
```

(4) 檢查郵件追蹤記錄配置。命令列輸入：

```
Get-TransportServer npartner-012a02 | Select-Object *Track*
```

Machine: npartner-012a02 | Scope: npexchange.local

```
[PS] C:\>Get-TransportServer npartner-012a02 | Select-Object *Track*
```

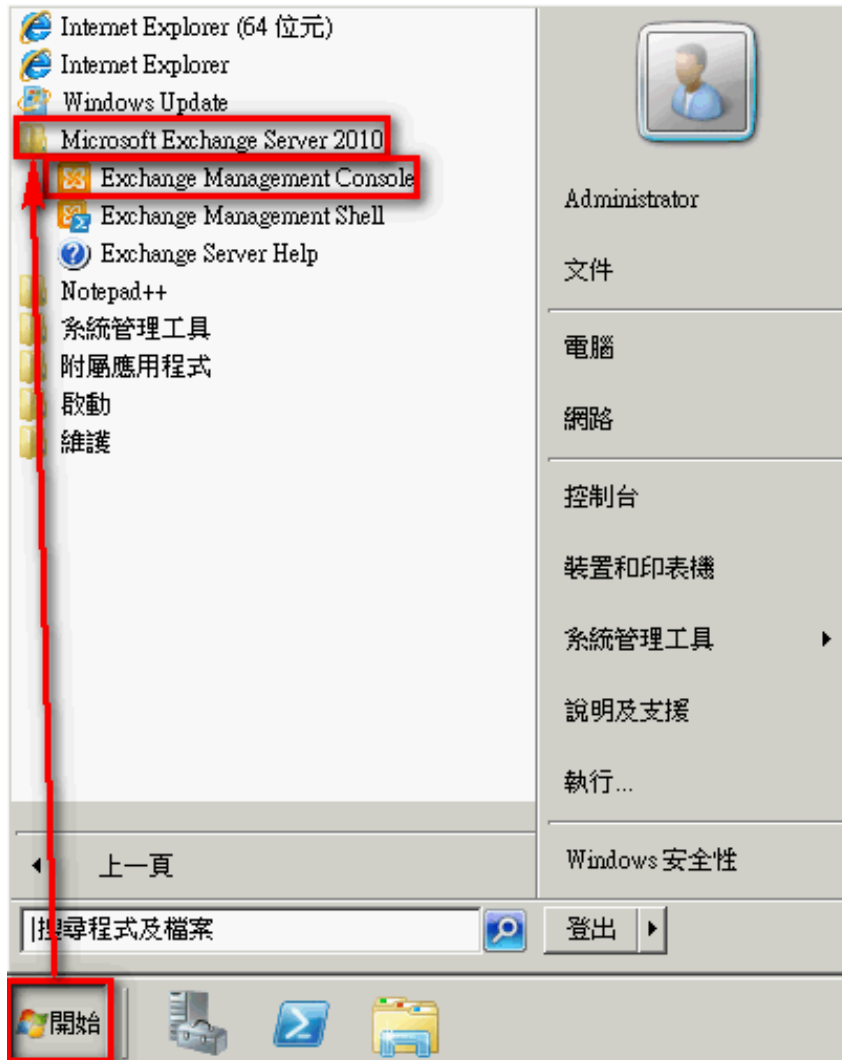
```
MessageTrackingLogEnabled           : True
MessageTrackingLogMaxAge             : 30.00:00:00
MessageTrackingLogMaxDirectorySize  : 250MB
MessageTrackingLogMaxFileSize       : 10MB
MessageTrackingLogPath               : C:\Program Files\Microsoft\Exchange S
                                     erver\TransportRoles\Logs\MessageTrac
                                     king
MessageTrackingLogSubjectLoggingEnabled : True
```

2 配置 Exchange Server 2010 郵件追蹤記錄

可選擇[Exchange Management Console]或[Exchange Management Shell]配置郵件追蹤記錄。

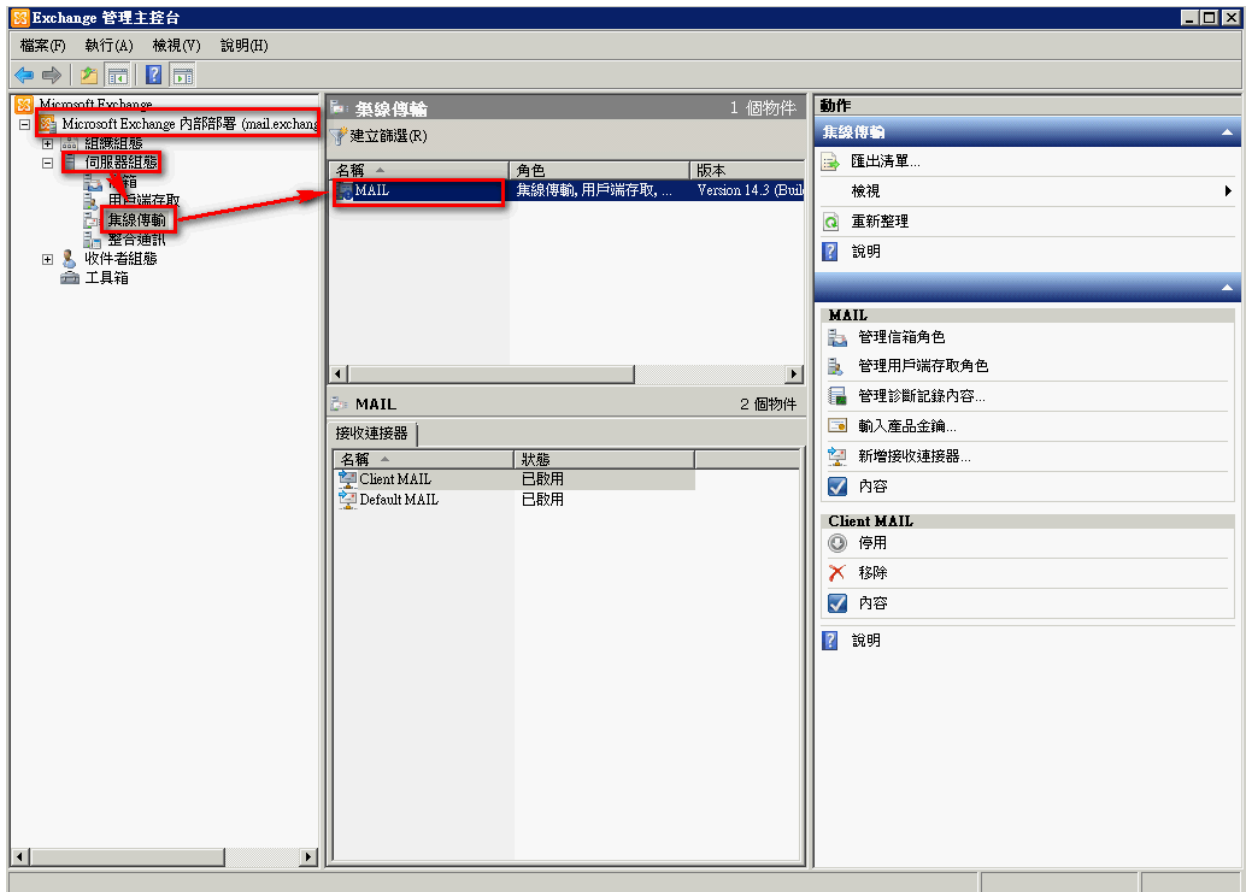
一、使用[Exchange Management Console]配置：

- (1) 以系統管理者 Administrator 登入 Exchange Server。
- (2) 滑鼠左點[開始]→ [所有程式] → [Microsoft Exchange Server 2010] → [Exchange Management Console]。



(3) 滑鼠左點[Microsoft Exchange 內部部署]→ [伺服器組態] → [集線傳輸]。

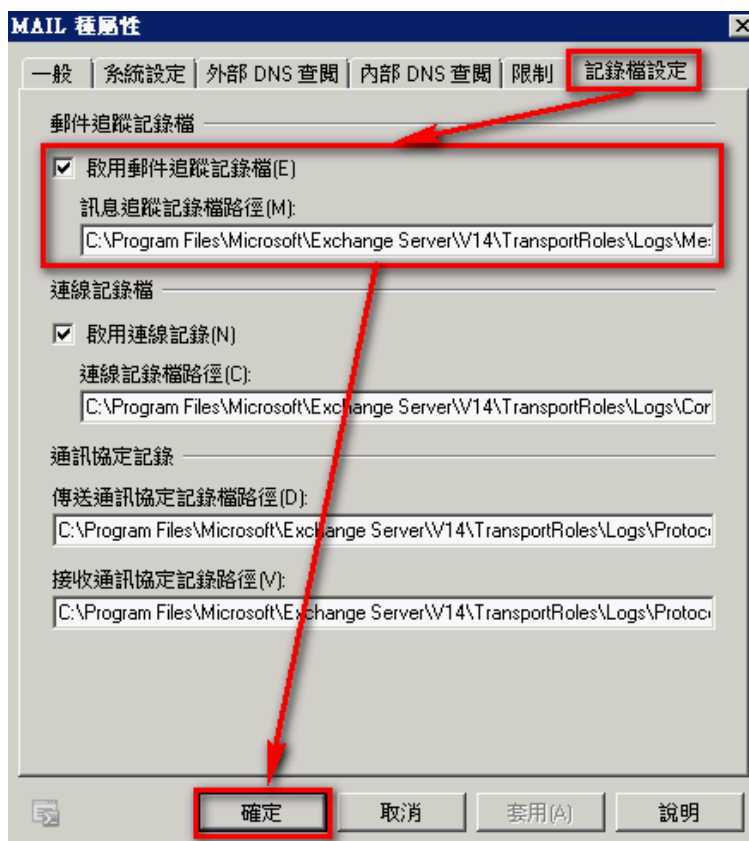
滑鼠右點 Exchange Server · 本例為"MAIL" · 左點 [內容]。



(4) 滑鼠左點[記錄檔設定]。勾選[啟用郵件追蹤記錄檔]，輸入[訊息追蹤記錄檔路徑]，

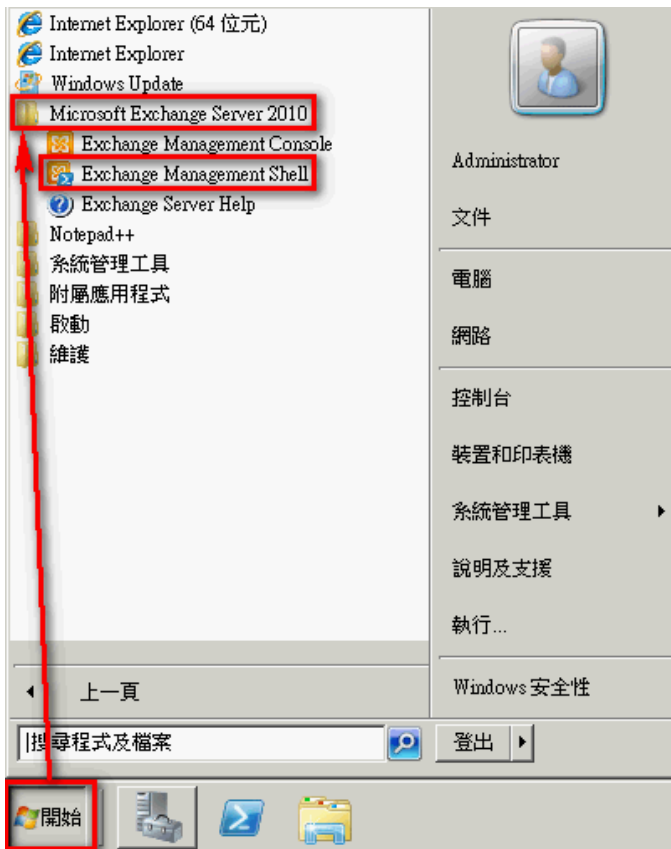
預設為"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

左點[確定]，完成配置。



二、使用[Exchange Management Shell]配置：

- (1) 以系統管理者 Administrator 登入 Exchange Server 。
- (2) 滑鼠左點[開始] → [所有程式] → [Microsoft Exchange Server 2010] → [Exchange Management Shell] 。



- (3) 啟用郵件追蹤。命令列輸入：

```
Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

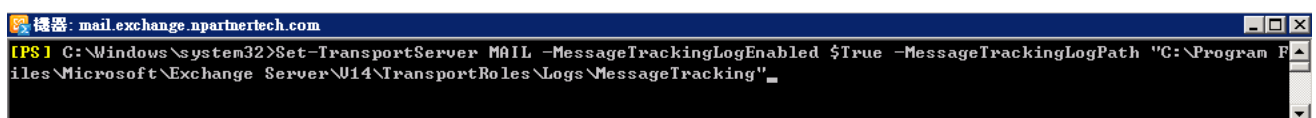
或

```
Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

<ServerIdentity>為 Exchange Server 的電腦名稱，<LocalFilePath>為郵件追蹤記錄的路徑，預設為"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

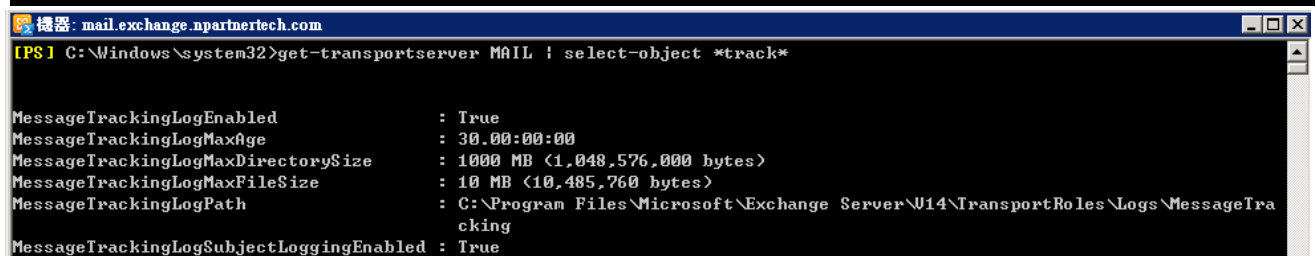
本例輸入：

```
Set-TransportServer MAIL -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"
```



- (4) 檢查郵件追蹤記錄配置。命令列輸入：

```
Get-TransportServer MAIL | Select-Object *Track*
```



3 配置 Exchange Server 2013 郵件追蹤記錄

可選擇[Exchange 系統管理中心(Exchange Admin Center/EAC)]或[Exchange Management Shell]配置郵件追蹤記錄。

一、使用[Exchange 系統管理中心(Exchange Admin Center/EAC)]配置：

(1) 開啟瀏覽器。

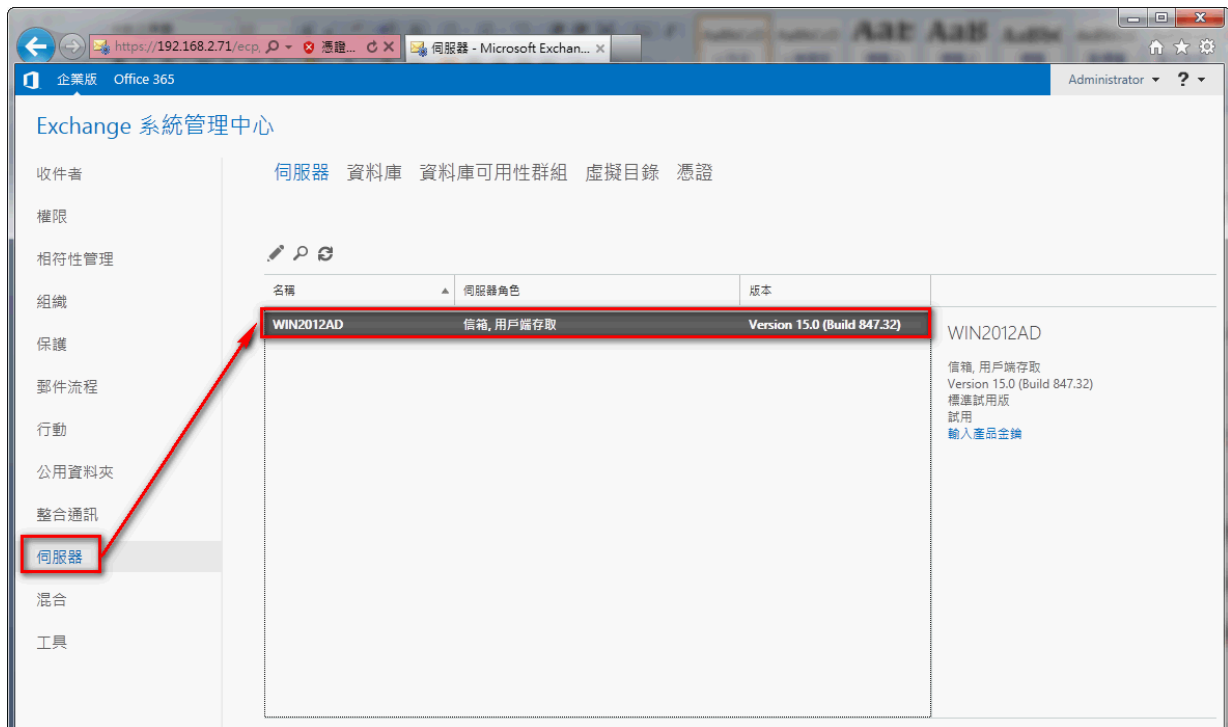
- ▶ 內部 URL：“https://<CASServerName or private IP>/ecp”，內部 URL 用來從組織防火牆內存取 EAC。
- ▶ 外部 URL：“https://<MailHostName or public IP>/ecp”，外部 URL 用來從組織防火牆外存取 EAC。

本例輸入 URL “https://192.168.2.71/ecp” 連上 Exchange 系統管理中心。

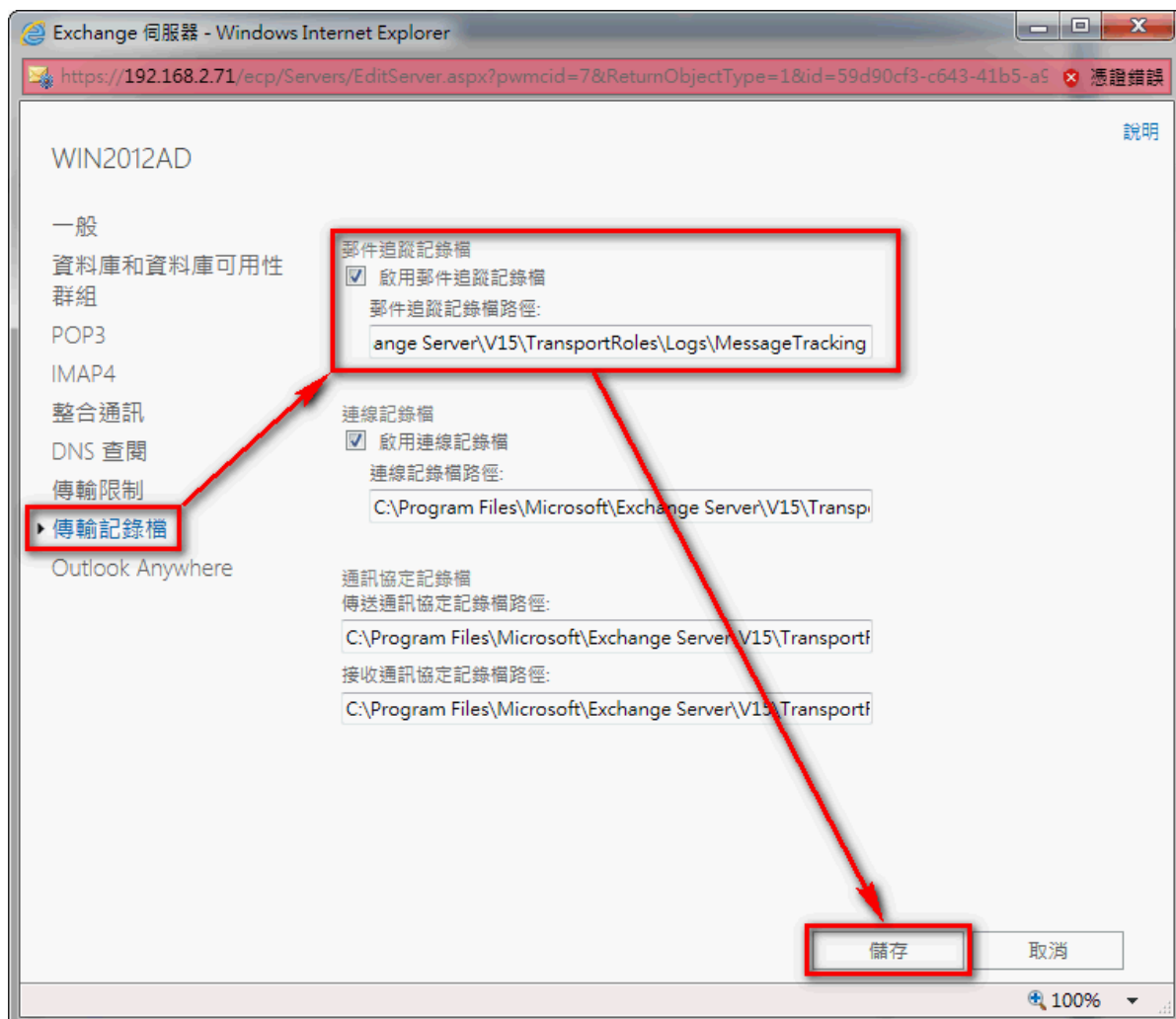
(2) Exchange 系統管理中心(Exchange Admin Center/EAC)登入頁面輸入 Exchange Server 系統管理員和密碼，登入 EAC。



- (3) 滑鼠左點[伺服器]，雙點 Exchange Server，本例為雙點"WIN2013AD"。

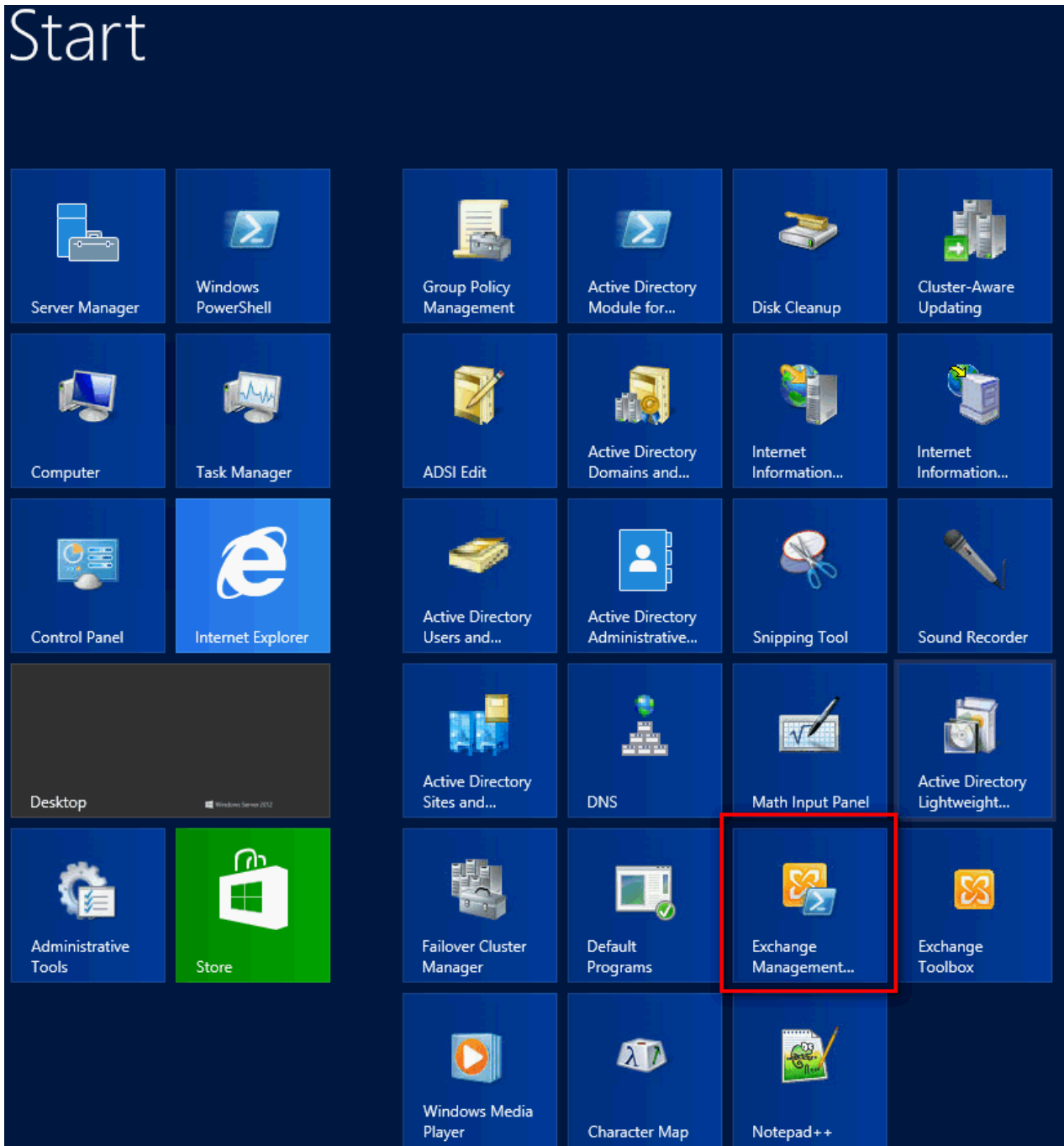


- (4) 滑鼠左點[傳輸記錄檔]。勾選[啟用郵件追蹤記錄檔]。設定郵件追蹤記錄檔路徑，Exchange 2013 預設"C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking"。左點[儲存]，完成配置。



二、使用[Exchange Management Shell]配置：

- (1) 以系統管理者 Administrator 登入 Exchange Server 。
- (2) 滑鼠左點[Start] → [Exchange Management Shell] 。



- (3) 啟用郵件追蹤。命令列輸入：

```
Set-TransportService <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

<ServerIdentity>為 Exchange Server 的電腦名稱，<LocalFilePath>為郵件追蹤記錄的路徑，預設為"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking"。本例輸入：

```
Set-TransportService win2012ad -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking"
```

```
Machine: WIN2012AD.win2012cht.local
[PS] C:\Windows\system32>Set-TransportService win2012ad -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\U15\TransportRoles\Logs\MessageTracking"
[PS] C:\Windows\system32>_
Microsoft New Phonetic 半 :
```

- (4) 檢查郵件追蹤記錄配置。

命令列輸入：

Get-TransportService win2012ad | Select-Object *Track*

```
Machine: WIN2012AD.win2012cht.local
[PS] C:\Windows\system32>Get-TransportService win2012ad | select-object *Track*

MessageTrackingLogEnabled      : True
MessageTrackingLogMaxAge       : 30.00:00:00
MessageTrackingLogMaxDirectorySize : 1000 MB (1,048,576,000 bytes)
MessageTrackingLogMaxFileSize  : 10 MB (10,485,760 bytes)
MessageTrackingLogPath         : C:\Program Files\Microsoft\Exchange Server\U15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True

[PS] C:\Windows\system32>_
Microsoft New Phonetic 半 :
```

4 配置 NXLOG

- (1) 以系統管理者 Administrator 登入 Exchange Server。
- (2) 下載 NXLOG：瀏覽 <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 位元系統 NXLOG 安裝在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

(4) 配置 NXLOG :

(1) 下載 NXLOG Exchange 配置檔範例 :

http://www.npartnertech.com/download/tech/nxlog_exchange.conf

(2) 編輯 NXLOG 設定檔 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。複製 NXLOG Exchange 配置檔範例 nxlog_exchange.conf 內容，貼上並覆蓋 nxlog.conf 。

```
#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 BASEDIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
<Input in_exchange>
    Module      im_file
    File        '%BASEDIR%\MSGTRK20?????*.LOG'
    SavePos     TRUE
</Input>
<Output out_exchange>
    Module      om_udp
    Host         192.168.2.64
    Port        514
    Exec        $SyslogFacilityValue = 2;
    Exec        $SourceName = 'Exchange';
    Exec        to_syslog_bsd();
</Output>
<Route exchange>
    Path        in_exchange => out_exchange
</Route>
```

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` " 。

紅色部分"`define BASEDIR $dir`"行中的\$dir 請輸入 Exchange Server 郵件追蹤記錄路徑。

本例使用 Exchange 2007

預設路徑 " `C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking` " 。

紅色部分"`Host $N-Reporter_IP`"行中的\$N-Reporter_IP 改成 N-Reporter IP。

本例 IP 為 192.168.2.64。

本例配置範例：

```

1  ## This is a sample configuration file. See the nxlog reference manual about the
2  ## configuration options. It should be installed locally and is also available
3  ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
4  ## Please set the ROOT to the folder your nxlog was installed into,
5  ## otherwise it will not start.
6  #define ROOT C:\Program Files\nxlog
7  define ROOT C:\Program Files (x86)\nxlog
8  Moduledir %ROOT%\modules
9  CacheDir %ROOT%\data
10 Pidfile %ROOT%\data\nxlog.pid
11 SpoolDir %ROOT%\data
12 LogFile %ROOT%\data\nxlog.log
13 <Extension syslog>
14     Module      xm_syslog
15 </Extension>
16 define BASEDIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
17 <Input in_exchange>
18     Module      im_file
19     File         '%BASEDIR%\MSGTRK20?????*.LOG'
20     SavePos      TRUE
21 </Input>
22 <Output out_exchange>
23     Module      om_udp
24     Host         192.168.2.64
25     Port         514
26     Exec         $$SyslogFacilityValue = 2;
27     Exec         $$SourceName = 'Exchange';
28     Exec         to_syslog_bsd();
29 </Output>
30 <Route exchange>
31     Path         in_exchange => out_exchange
32 </Route>
  
```

(5) 啟動 NXLOG：

a. 利用[命令提示字元]啟動 NXLOG 或 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]。

(6) 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。

5 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]下拉選單中依設備的類型選擇 Exchange 2007 或 2010 或 2013，勾選[啟動接收]，按下[確定]，即完成設備的系統新增程序



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

