N-Partner

N-REPORTER

# 用户如何管理 Exchange Server 邮件追踪记录审核

**V 1.1.4 (简体)**

(01-01-02-013) 2015/02/09

# 前言

本文件描述 N-Reporter 使用者如何管理 Exchange Server 邮件追踪(Message Tracking)记录审核。第一步先配置 Exchange 的邮件追踪记录。第二步利用 Open Source 工具 NXLOG Community Edition(简称 NXLOG)将邮件追踪记录转成 Syslog，发送至 N-Reporter 接收。因 Windows 与 Exchange 版本差异，使用[ Exchange 管理命令接口 ]配置可能会有差异，本文件配置的环境为 Windows 2003 64 位操作系统安装 Exchange 2007、Windows 2008 R 2 操作系统安装 Exchange 2010 与 Windows 2012 操作系统安装 Exchange 2013。

邮件追踪记录是与执行 Exchange Server 且已安装集线传输服务器角色(Hub Transport server role)、信箱服务器角色(Mailbox server role)或边际传输服务器角色(Edge Transport server role)的计算机往返传送邮件之所有邮件活动的详细记录。已安装客户端存取服务器角色或整合通讯服务器角色的 Exchange Server 不会有邮件追踪记录。本配置文件适用安装集线传输服务器角色或边际传输服务器角色的 Exchange Server。

注：Exchange Server 预设启用邮件追踪。

# 文件章节如下:



**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

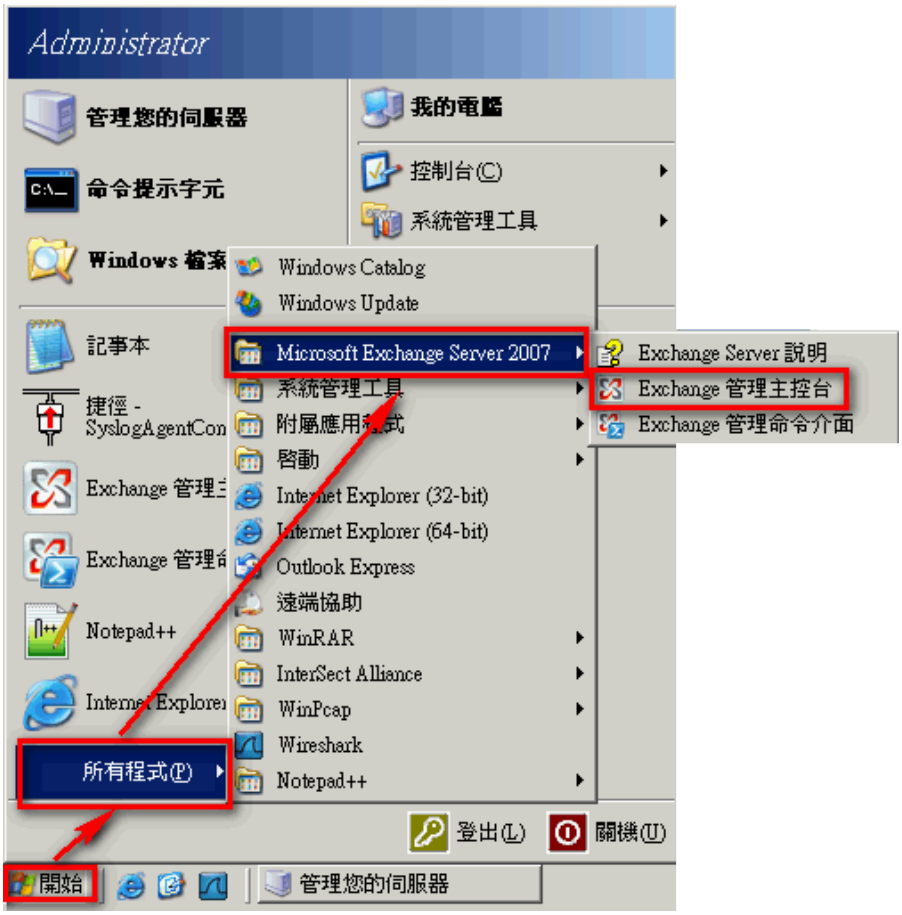
# 1 配置 Exchange Server 2007 邮件追踪记录

可选择[ Exchange 管理命令接口 ]或[ Exchange 管理命令接口 ]配置邮件追踪记录。

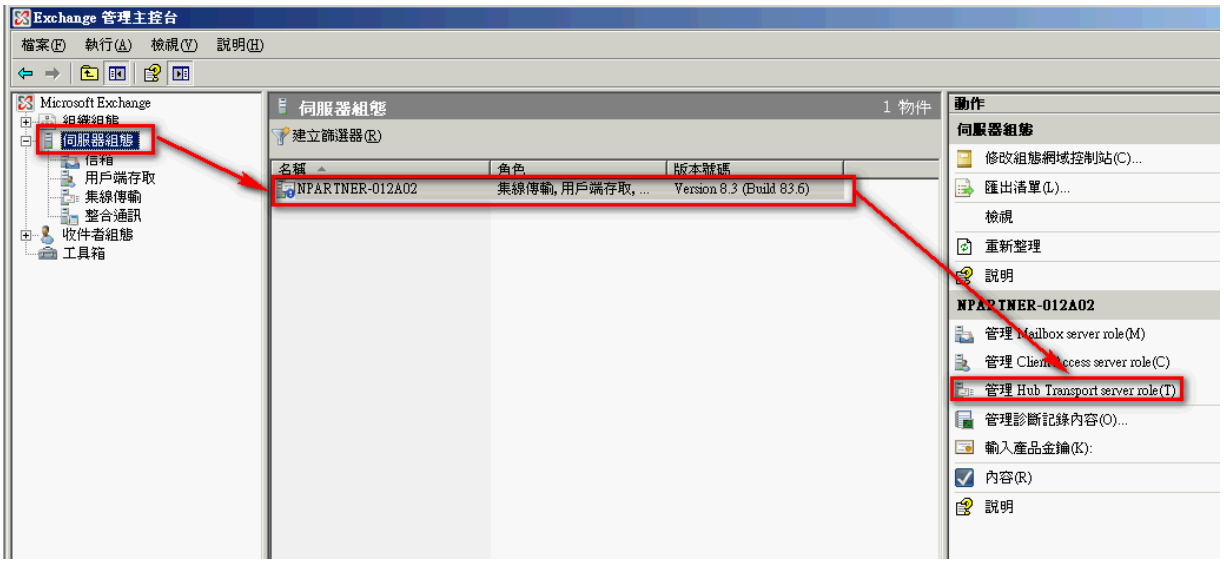
## 一、使用[ Exchange 管理命令接口 ] 配置：

(1) 以系统管理者 Administrator 登入 Exchange Server。

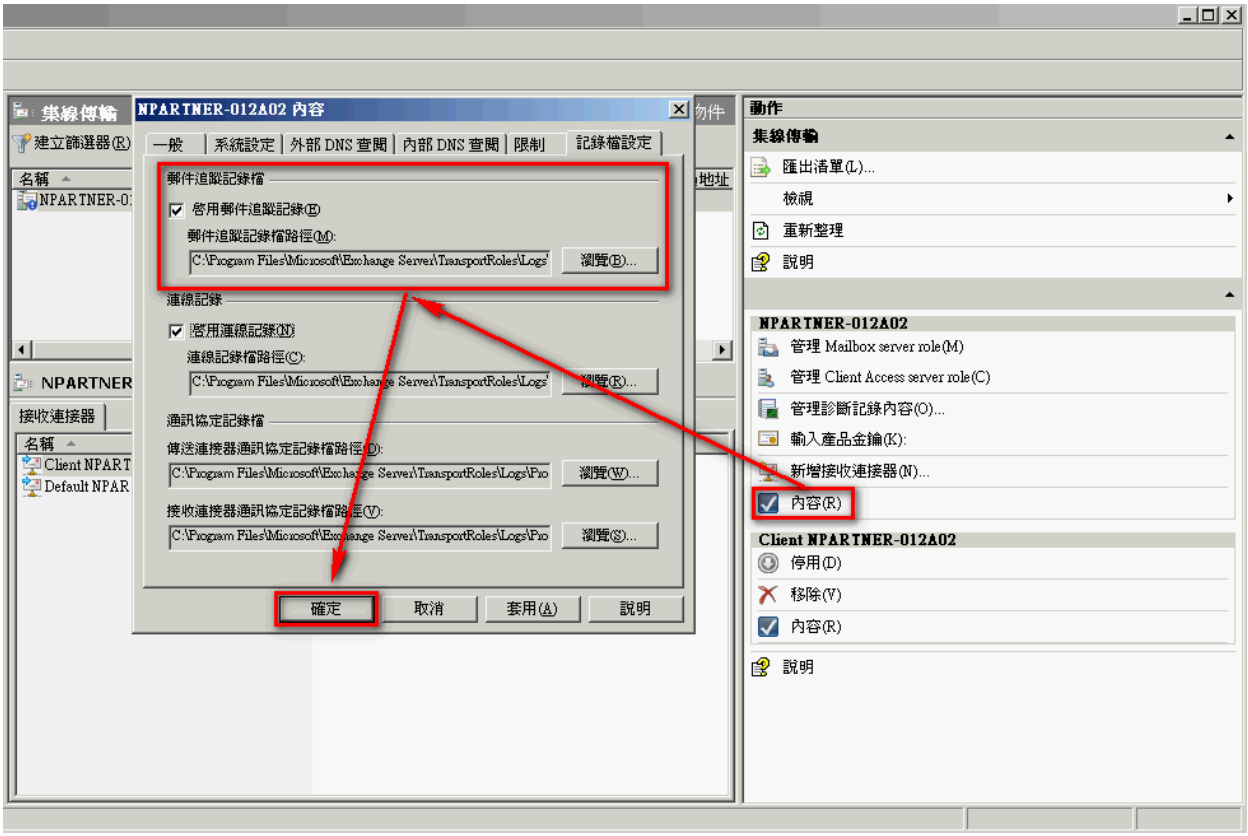
(2) 鼠标左点[ 开始 ] ➔ [ 所有程序 ] ➔ [ Microsoft Exchange Server 2007 ] ➔ [ Exchange 管理命令接口]。



(3) 鼠标左点[ 服务器组态 ] ，左点 Exchange Server，本例为"NPARTNER-012A02"，左点 [ 管理 Hub Transport server role ]。



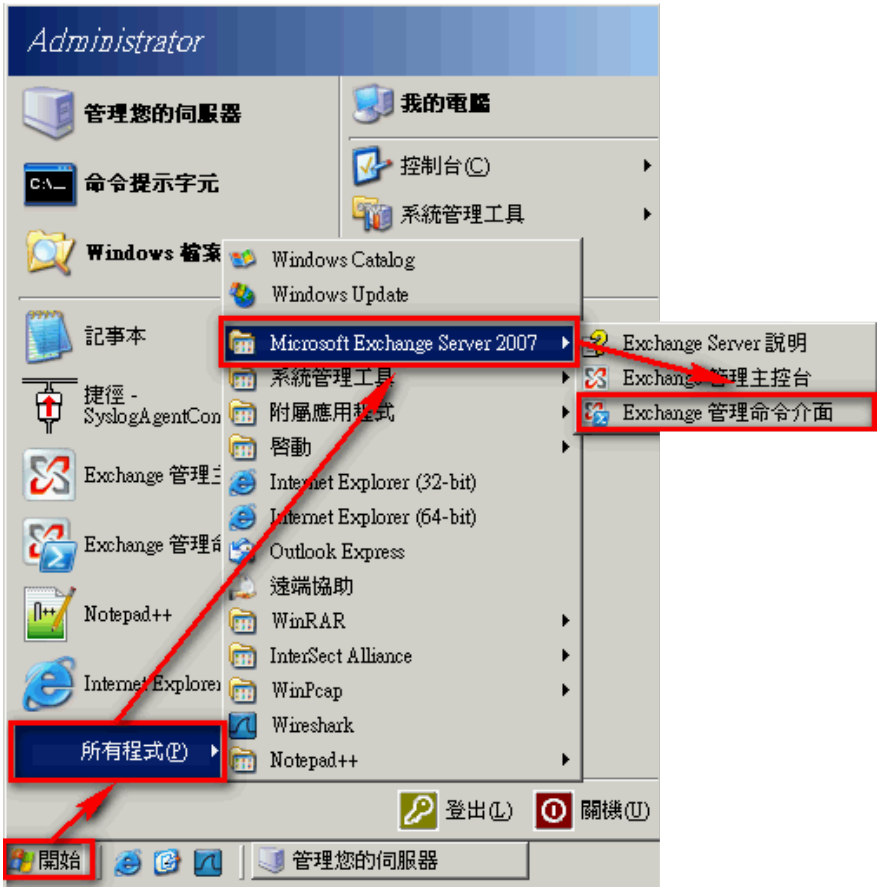

(4) 鼠標左点[ 内容 ]。勾选[ 启用邮件追踪记录 ]，左点[ 浏览 ]，设定邮件追踪记录文件路径，预设"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"。左点[ 确定 ]，完成配置。



## 二、使用[ Exchange 管理命令接口 ] 配置：

(1) 以系统管理者 Administrator 登入 Exchange Server。

(2) 鼠标左点[ 开始 ] ➔ [ 所有程序 ] ➔ [ Microsoft Exchange Server 2007 ] ➔ [ Exchange 管理命令接口 ]。




(3) 启用邮件追踪。命令行输入：

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

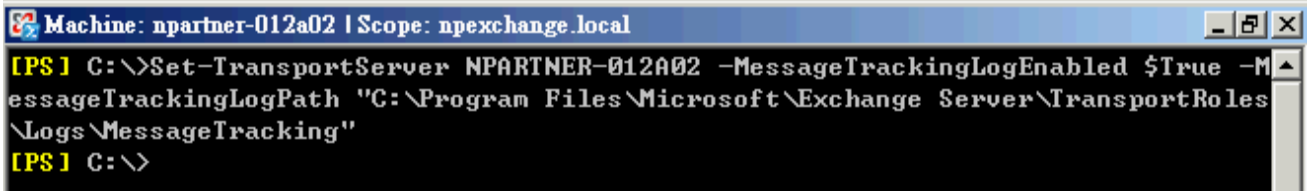
或

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

<ServerIdentity>为 Exchange Server 的计算机名称，<LocalFilePath>为邮件追踪记录的路径，预设为"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"。

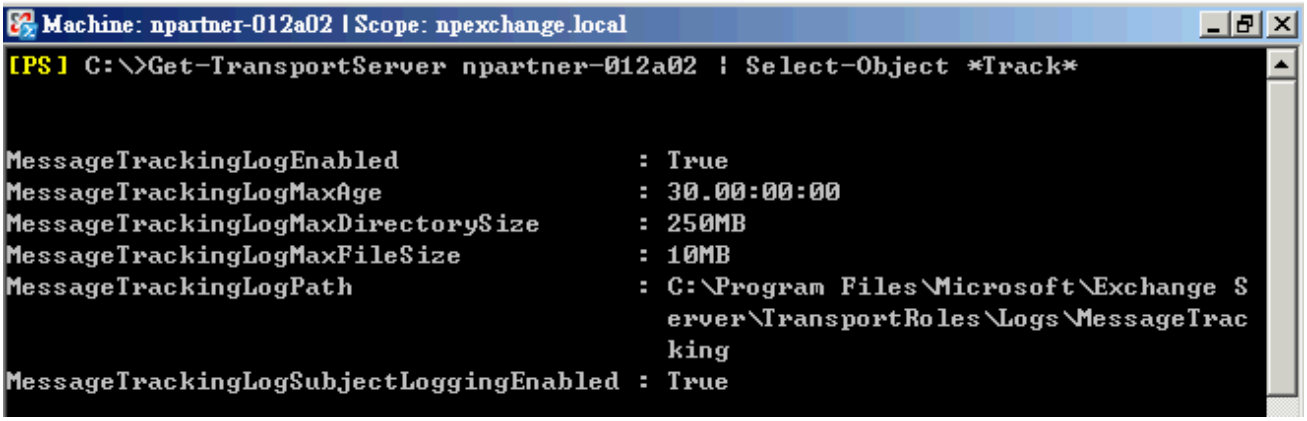
**本例输入：**

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



(4) 检查邮件追踪记录布局。命令行输入：

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



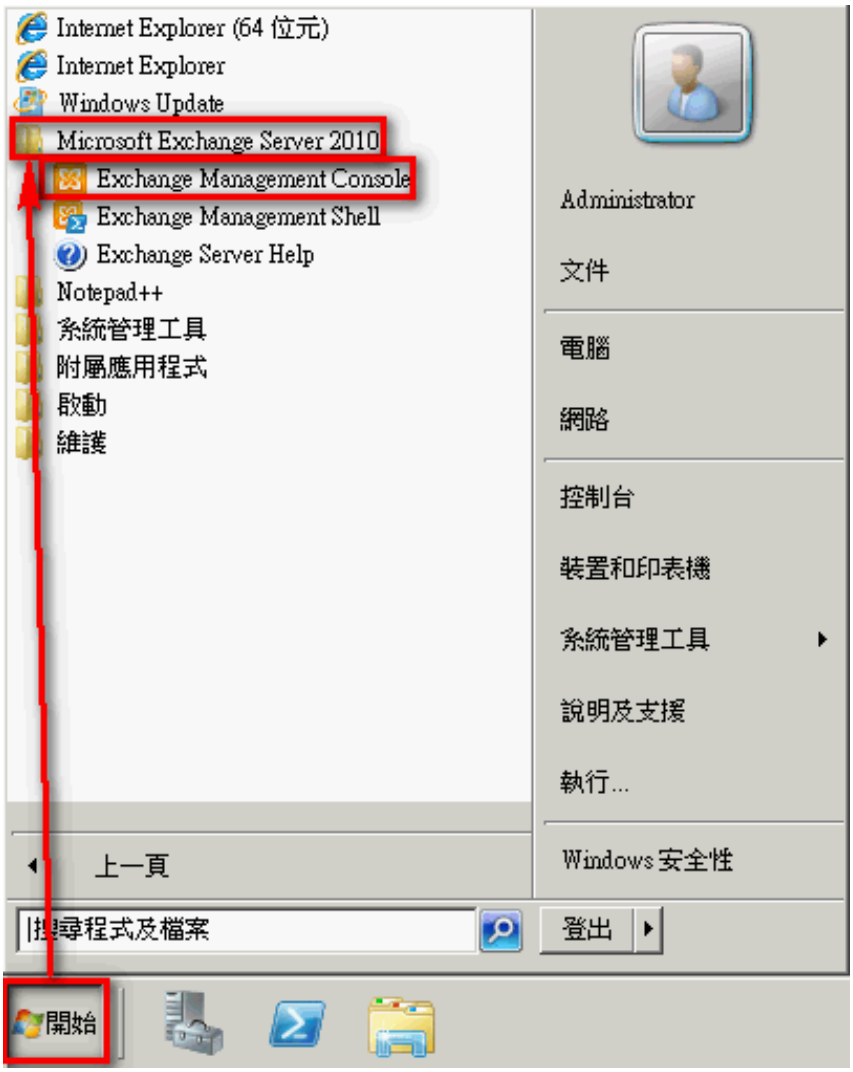
# 2 配置 Exchange Server 2010 邮件追踪记录

可选择[ Exchange Management Console ]或[Exchange Management Shell ]配置邮件追踪记录。

## 一、使用[Exchange Management Console ]配置：

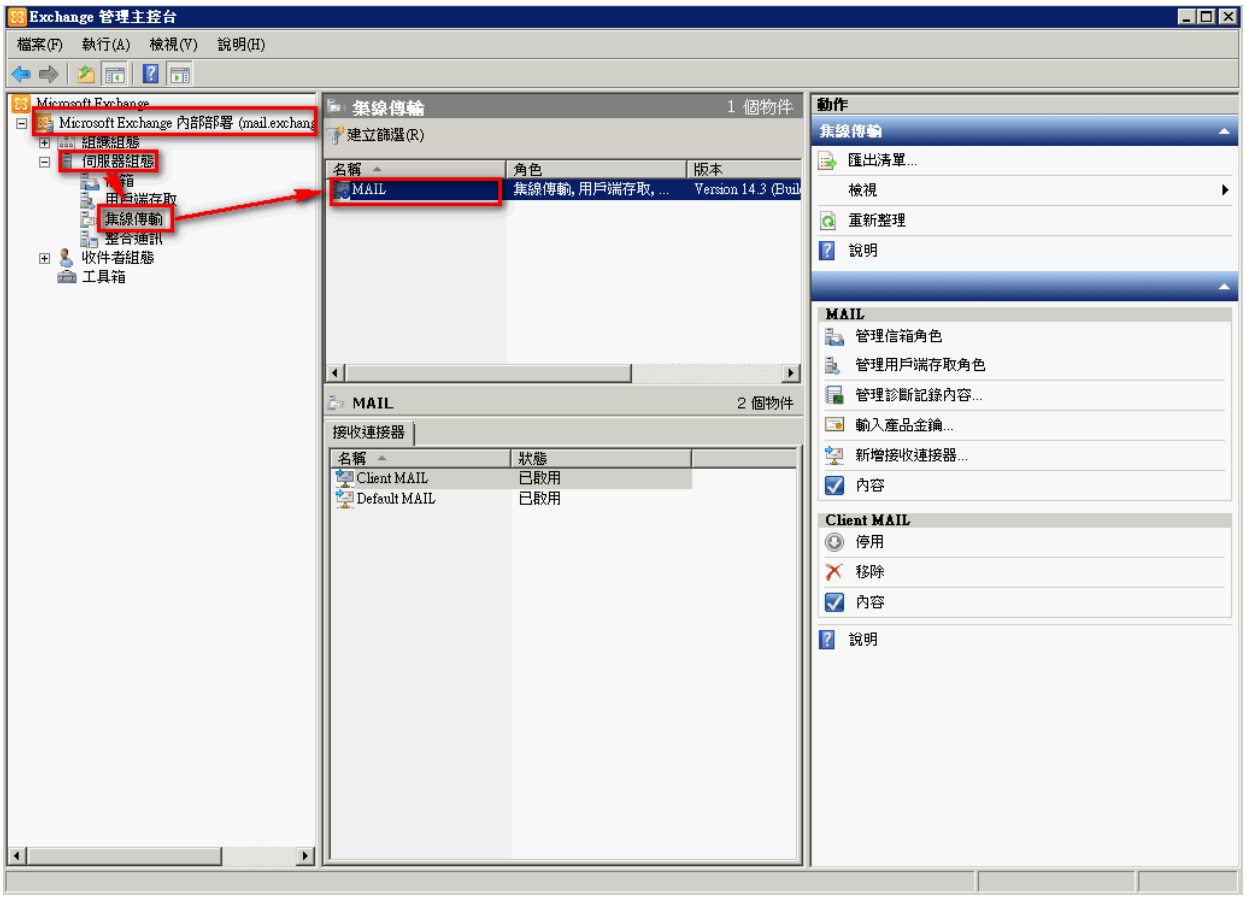
(1) 以系统管理者 Administrator 登入 Exchange Server。

(2) 鼠标左点[ 开始 ]➔ [ 所有程序 ] ➔ [ Microsoft Exchange Server 2010 ] ➔ [ Exchange Management Console]。



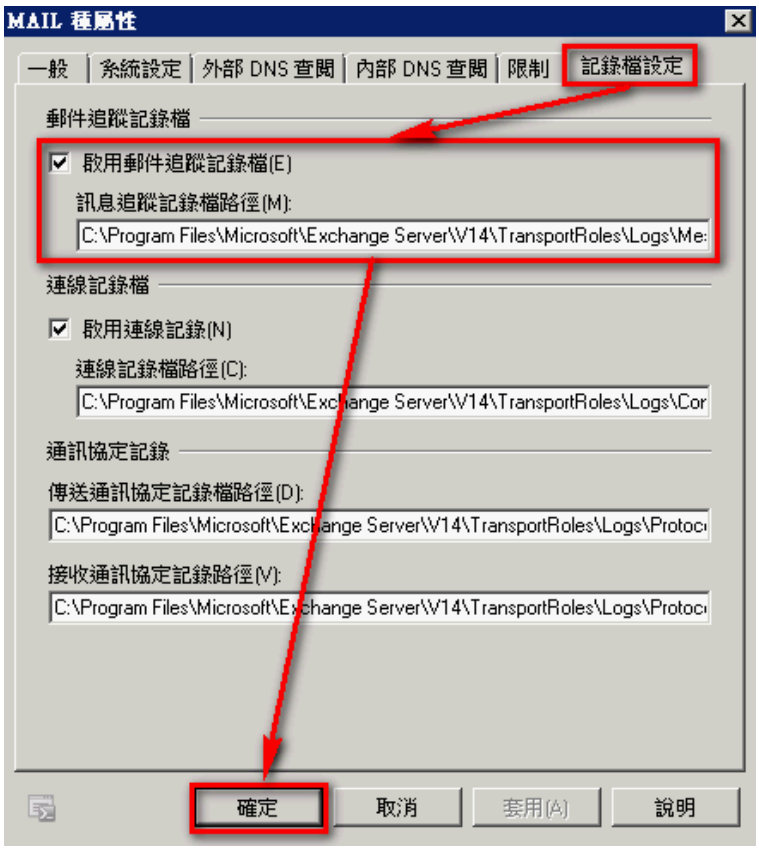
(3) 鼠标左点[ Microsoft Exchange 内部部属 ]➔ [ 服务器组态 ] ➔ [ 集线传输 ]。

鼠标右点 Exchange Server，本例为"MAIL"，左点 [ 内容 ]。




(4) 鼠标左点[ 记录文件设定 ]。勾选[ 启用邮件追踪记录文件 ]，输入[ 讯息追踪记录文件路径 ]，预设为"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

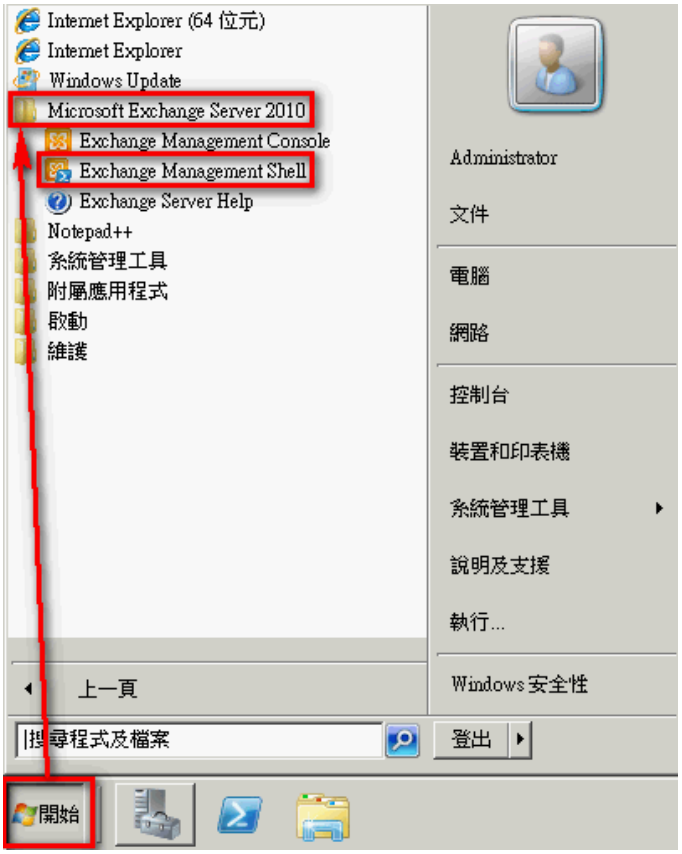
左点[ 确定 ]，完成配置。



## 二、使用[Exchange Management Shell ]配置：

(1) 以系统管理者 Administrator 登入 Exchange Server。

(2) 鼠标左点[ 开始 ] ➔ [ 所有程序 ] ➔ [ Microsoft Exchange Server 2010 ] ➔ [ Exchange Management Shell ]。




(3) 启用邮件追踪。命令行输入：

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

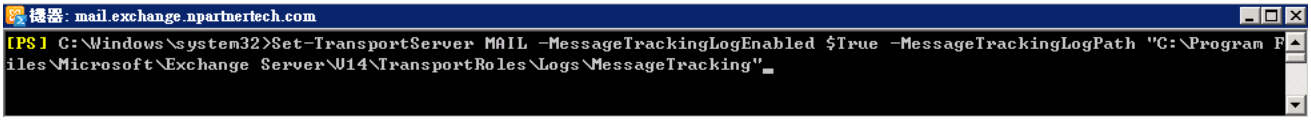
或

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

<ServerIdentity>为 Exchange Server 的计算机名称，<LocalFilePath>为邮件追踪记录的路径，默认为"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"。

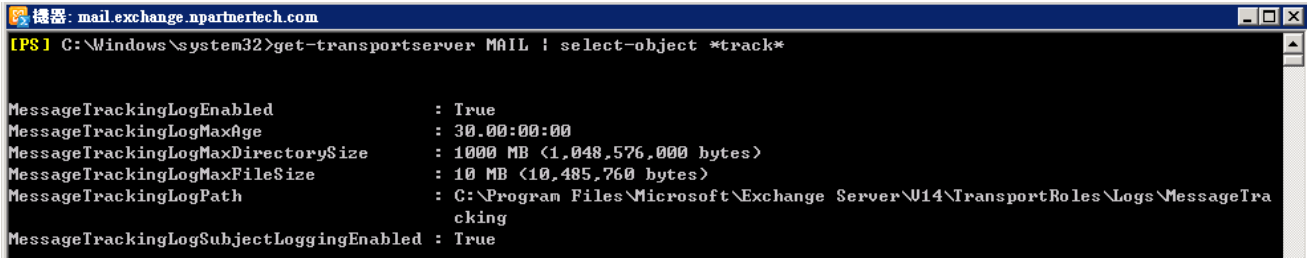
本例输入：

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




(4) 检查邮件追踪记录布局。命令行输入：

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



# 3 配置 Exchange Server 2013 邮件追踪记录

可选择[ Exchange 系统管理中心(Exchange Admin Center/EAC) ]或[ Exchange Management Shell ]配置邮件追踪记录。

**一、使用[ Exchange 系统管理中心(Exchange Admin Center/EAC) ]配置：**

(1) 开启浏览器。

► 内部 URL：”https://<CASServerName or private IP>/ecp”，内部 URL 用来从组织防火墙内存取 EAC。

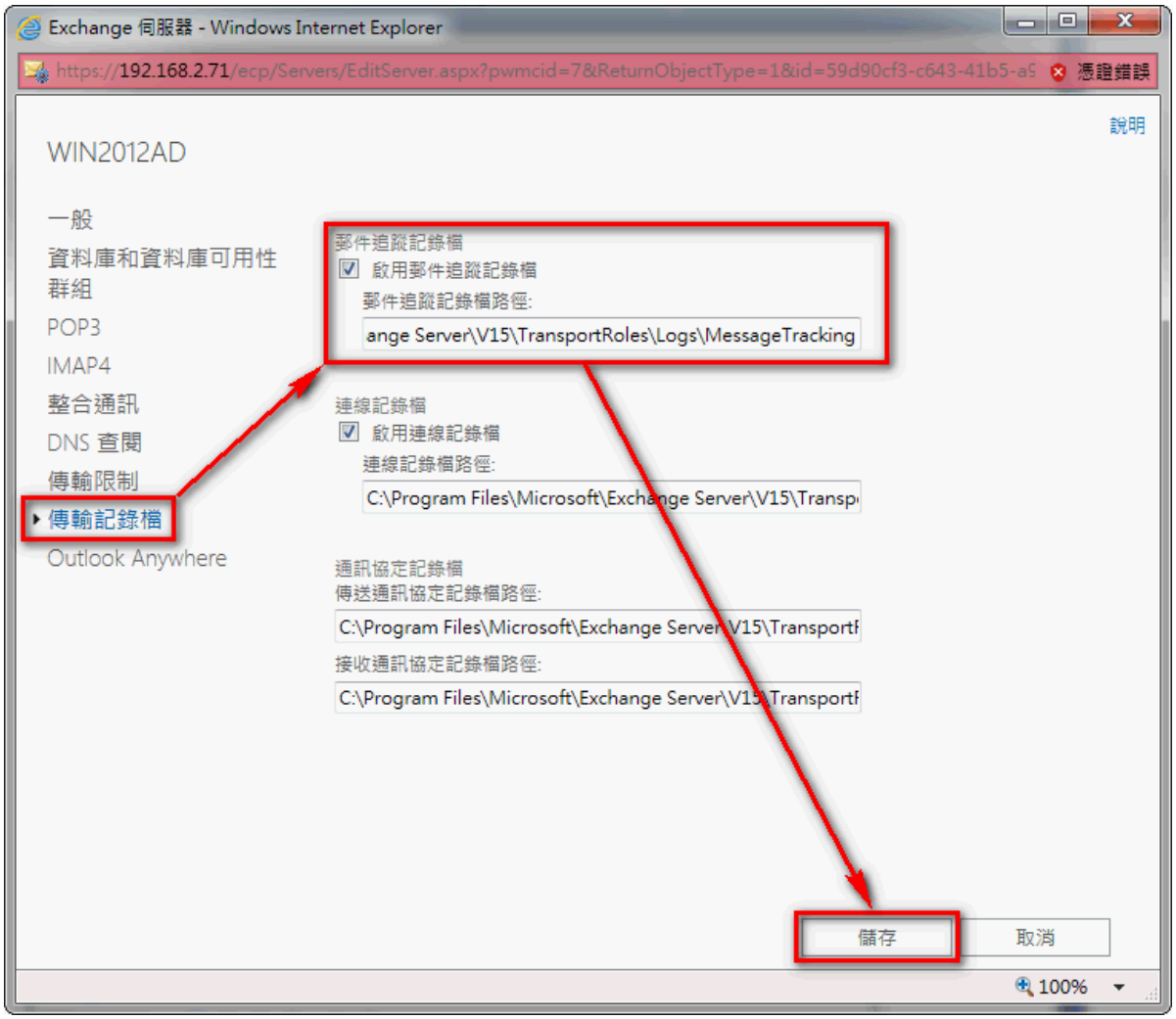
► 外部 URL：”https://<MailHostName or public IP>/ecp”，外部 URL 用来从组织防火墙外存取 EAC。

**本例输入 URL " https://192.168.2.71/ecp " 连上 Exchange 系统管理中心。**

(2) Exchange 系统管理中心(Exchange Admin Center/EAC)登入页面输入 Exchange Server 系统管理员和密码，登入 EAC。

(3) 鼠标左点[ 服务器 ] ，双点 Exchange Server，本例为双点"WIN2013AD"。

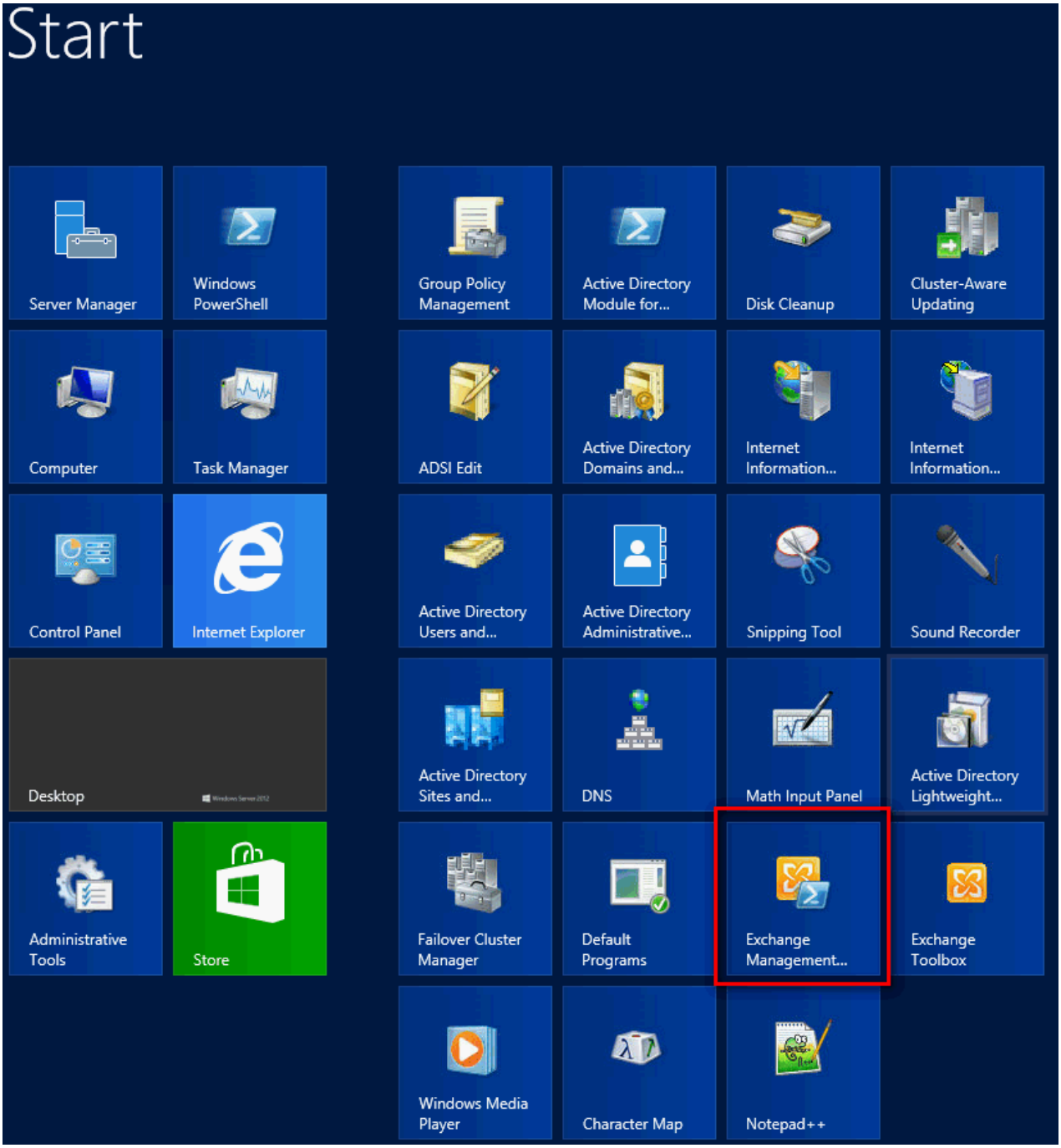

(4) 鼠標左点[ 传输记录文件 ]。勾选[ 启用邮件追踪记录文件 ]。设定邮件追踪记录文件路径，Exchange 2013 默认"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking"。左点[ 储存 ]，完成配置。



## 二、使用[ Exchange Management Shell ]配置：

(1) 以系统管理者 Administrator 登入 Exchange Server。

(2) 鼠标左点[ Start ] → [Exchange Management Shell ]。

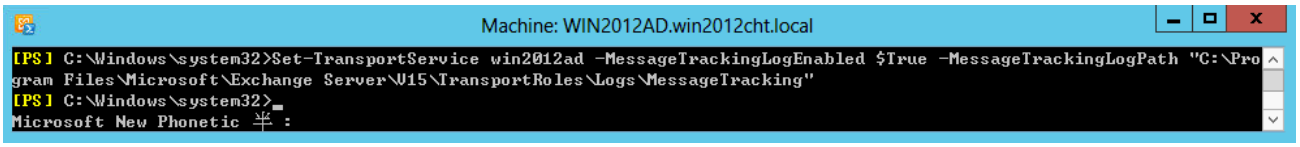



(3) 启用邮件追踪。命令行输入：

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

<ServerIdentity>为 Exchange Server 的计算机名称，<LocalFilePath>为邮件追踪记录的路径，默认为"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking"。本例输入：

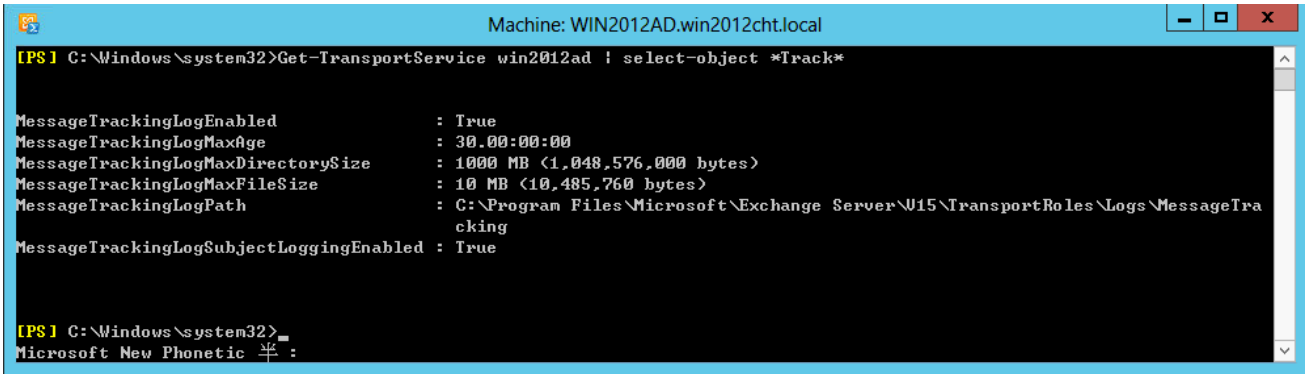
```
Set-TransportService win2012ad -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking"
```




(4) 检查邮件追踪记录布局。

命令行输入：

```
Get-TransportService win2012ad | Select-Object *Track*
```




# 4 配置 NXLOG

**(1) 以系统管理者 Administrator 登入 Exchange Server。**

**(2) 下载 NXLOG：**浏览 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 位系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "**

**(4) 配置 NXLOG：**

(1) 下载 NXLOG Exchange 配置文件范例：

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

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

复制 NXLOG Exchange 配置文件范例 nxlog_exchange.conf 内容，贴上并覆盖 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>
```

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 " 。

红色部分"define BASEDIR $dir "行中的$dir 请输入 Exchange Server 邮件追踪记录路径，

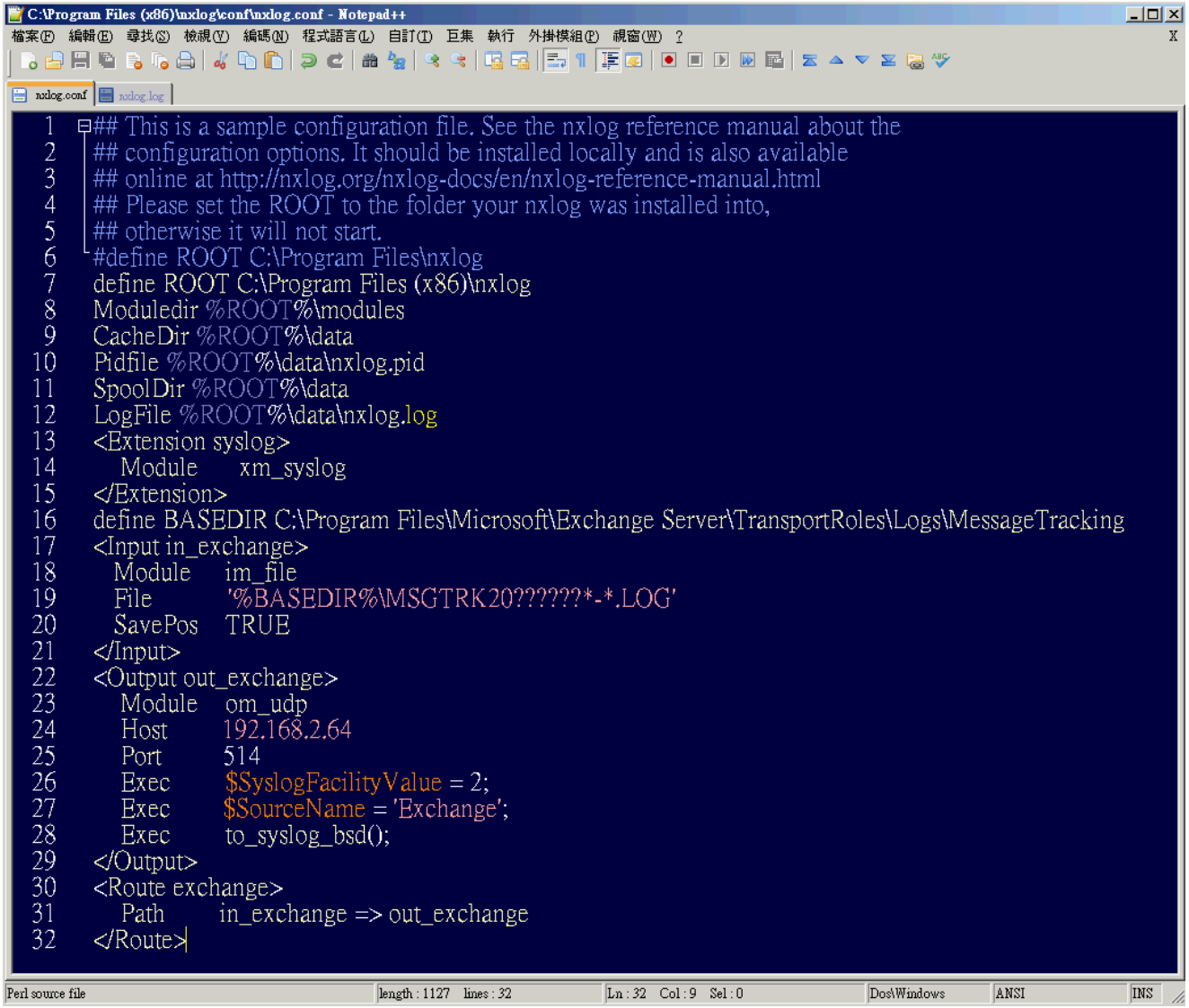
**本例使用 Exchange 2007**

默认路径 " C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking " 。

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

本例 IP 为 192.168.2.64。

本例配置范例：




**(3) 启动 NXLOG：**

a.利用[ 命令提示字符 ]启动 NXLOG 或 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 ]。

**(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。

**采购与销售合作：**sales@npartnertech.com

**技术咨询：**support@npartnertech.com