N-Partner

如何設定
MS Exchange 郵件追蹤記錄 V018

2024/04/16

版權聲明

商標

目錄

前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 MS Exchange 郵件追蹤記錄。

NXLog 工具將 MS Exchange 郵件追蹤記錄轉成 Syslog，再轉發到 N-Reporter 做正規化、稽核與分析。

此文件適用於 MS Exchange Server 2007 / 2010 / 2013 / 2016 / 2019 版本。

郵件追蹤記錄: https://docs.microsoft.com/zh-tw/exchange/mail-flow/transport-logs/message-tracking?view=exchserver-2019

信箱審核記錄: https://docs.microsoft.com/zh-tw/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019

稽核原則建議: https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

IIS(W3C) 記錄: https://docs.microsoft.com/zh-tw/windows/win32/http/w3c-logging

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

1. NXLog

1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition)

前往網址 https://nxlog.co/products/nxlog-community-edition/download

下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.0.2272.msi

Windows nxlog-ce-3.0.2272.msi

註：若需要下載 NXLog 32bit 版本，請與我們連繫。

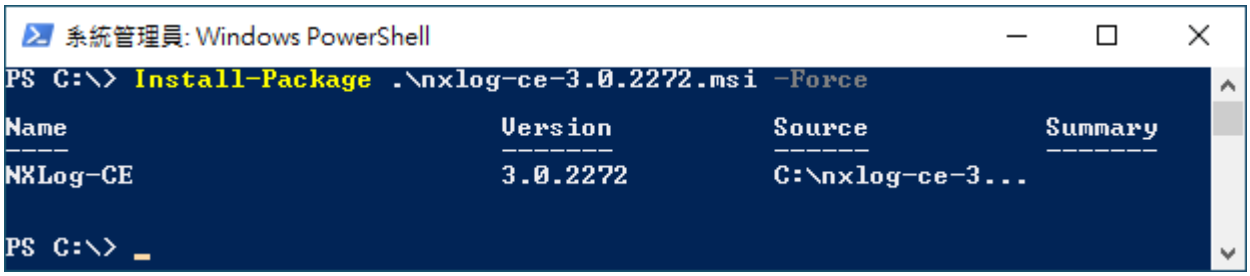
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

<2.1.1> 開啟 [Windows PowerShell]

<2.1.2> 安裝 NXLog 軟體

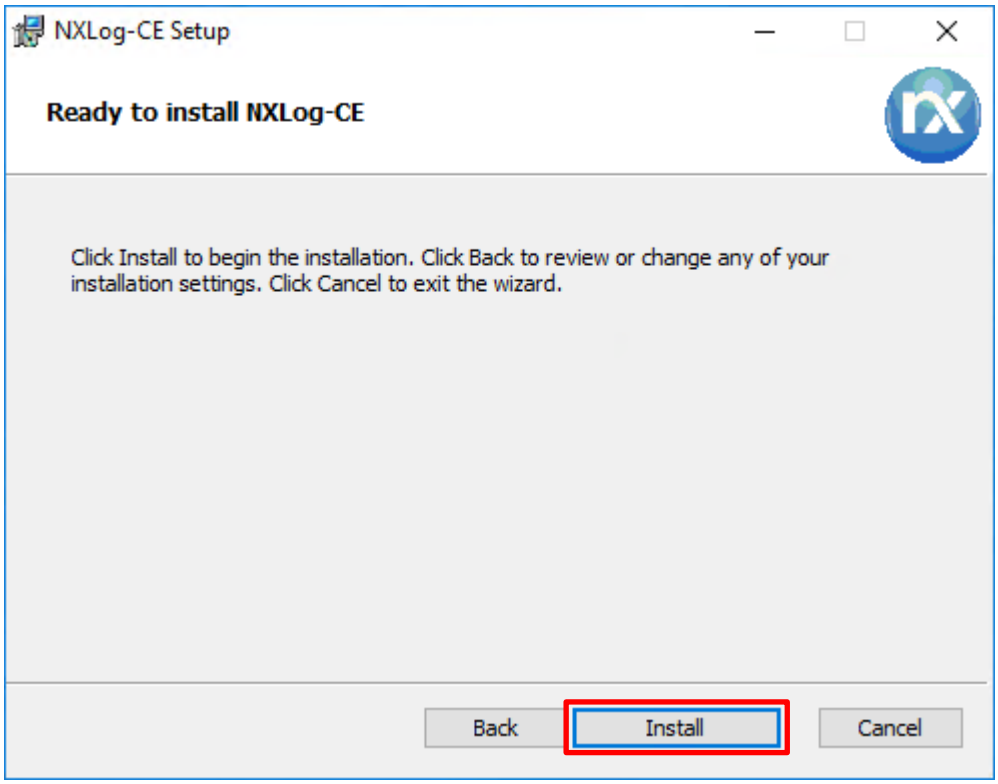
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```



紅色文字部位請輸入 NXLog 軟體路徑和檔案

<2.2> Windows 2003

點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish]



1.2 NXLog 設定檔下載

(1) 開啟 [Windows PowerShell]

(2) 下載 NXLog MS Exchange 範本設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：https://www.npartnertech.com/download/tech/nxlog_Exchange.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Exchange.conf' -OutFile
'C:\Program Files\nxlog\conf\nxlog.conf'
```

本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud    192.168.8.4
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
define IISLog    C:\inetpub\logs\LogFiles
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR    %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile    %LOGFILE%

Moduledir %ROOT%\modules
CacheDir    %ROOT%\data
Pidfile      %ROOT%\data\nxlog.pid
SpoolDir    %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
   Module xm_syslog
</Extension>

## For Exchange Message Tracking log file use the following:
<Input in_maillog>
   Module im_file
   File '%MailLog%\MSGTRK*.LOG'
   ReadFromLast TRUE
   SavePos TRUE
</Input>

<Output out_maillog>
   Module om_udp
   Host %NCloud%
   Port 514
   Exec $SyslogFacilityValue = 2;
   Exec $SourceName = 'Exchange';
   Exec to_syslog_bsd();
</Output>

<Route maillog>
   Path in_maillog => out_maillog
</Route>

## For Windows Event log use the following:
<Input in_eventlog>
   Module im_msvistalog
   ReadFromLast TRUE
   SavePos TRUE
   Query    <QueryList> \
                  <Query Id="0"> \
                        <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626 or
EventID=4627 or EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or
EventID=4672 or EventID=4675)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800 or
EventID=4801 or EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or EventID=5378 or
EventID=5632 or EventID=5633)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4768 or EventID=4769 or EventID=4770 or
EventID=4771 or EventID=4772 or EventID=4773 or EventID=4774 or EventID=4775 or EventID=4776 or
EventID=4777 or EventID=4820)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4720 or EventID=4722 or EventID=4723 or
EventID=4724 or EventID=4725 or EventID=4726 or EventID=4727 or EventID=4731 or EventID=4732 or
EventID=4733 or EventID=4734)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4735 or EventID=4738 or EventID=4739 or
EventID=4740 or EventID=4749 or EventID=4750 or EventID=4751 or EventID=4752 or EventID=4753 or
EventID=4764 or EventID=4765)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4766 or EventID=4767 or EventID=4780 or
EventID=4781 or EventID=4782 or EventID=4793 or EventID=4794 or EventID=4797 or EventID=4798 or
```

```
EventID=4799 or EventID=5376 or EventID=5377)]]</Select> \
                        <Select Path="Security">*[System[(EventID=4608 or EventID=4610 or EventID=4611 or
EventID=4612 or EventID=4614 or EventID=4615 or EventID=4616 or EventID=4618 or EventID=4621 or
EventID=4622 or EventID=4697)]]</Select> \
                        <Select Path="Security">*[System[(EventID=5024 or EventID=5025 or EventID=5027 or
EventID=5028 or EventID=5029 or EventID=5030 or EventID=5032 or EventID=5033 or EventID=5034 or
EventID=5035 or EventID=5037)]]</Select> \
                        <Select Path="Security">*[System[(EventID=5038 or EventID=5056 or EventID=5058 or
EventID=5059 or EventID=5061 or EventID=5890 or EventID=6281 or EventID=6400 or EventID=6401 or
EventID=6402 or EventID=6403)]]</Select> \
                        <Select Path="Security">*[System[(EventID=6404 or EventID=6405 or EventID=6406 or
EventID=6407 or EventID=6408 or EventID=6409 or EventID=6410)]]</Select> \
                    </Query> \
                </QueryList>
</Input>

<Output out_eventlog>
   Module om_udp
   Host %NCloud%
   Port 514
   Exec $SyslogFacilityValue = 17;
   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>

## For Microsoft IIS(Internet Information Server) log file use the following:
<Input in_iislog>
   Module im_file
   File '%IISLog%\u_ex*.log'
   ReadFromLast TRUE
   Recursive TRUE
   SavePos TRUE
</Input>

<Output out_iislog>
   Module om_udp
   Host %NCloud%
   Port 514
   Exec $SyslogFacilityValue = 22;
   Exec $raw_event = "IIS [info]: " + $raw_event ;
   Exec to_syslog_bsd();
</Output>

<Route iislog>
   Path in_iislog => out_iislog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud      192.168.8.4
```

本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本請改為以下設定

```
define ROOT        C:\Program Files (x86)\nxlog
```

藍色文字部位請輸入 Exchange log 路徑

```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

藍色文字部位請輸入 IIS log 路徑

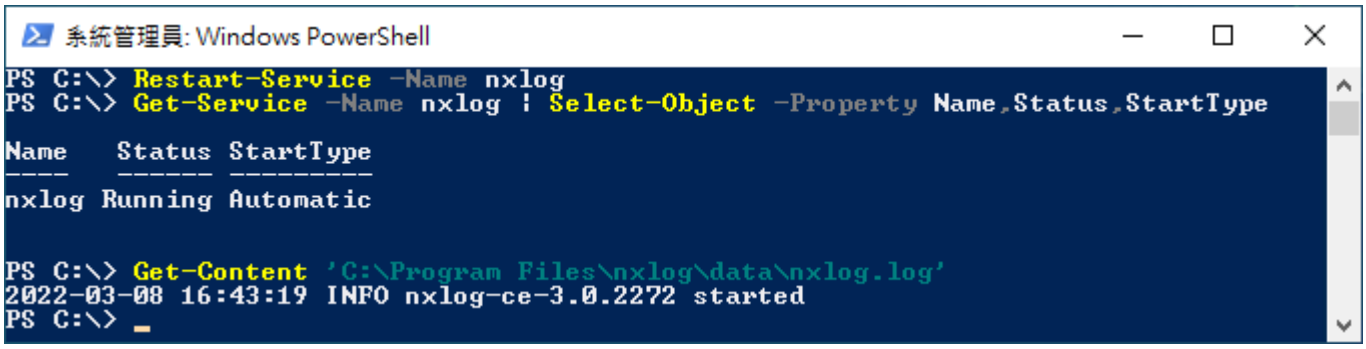
```
define IISLog    C:\inetpub\logs\LogFiles
```

1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]

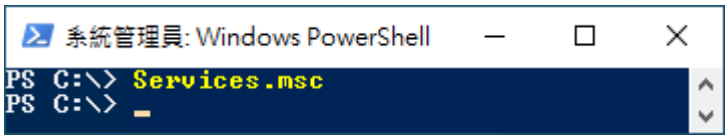
(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```



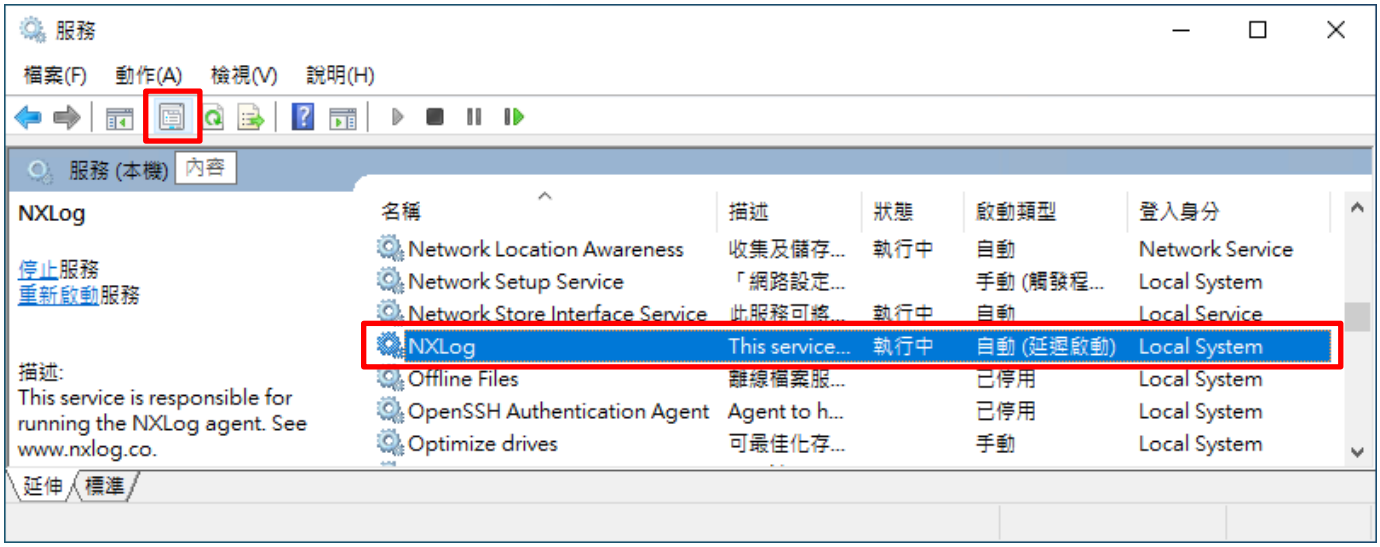
(3) 開啟 [服務] 功能

```
PS C:\> Services.msc
```

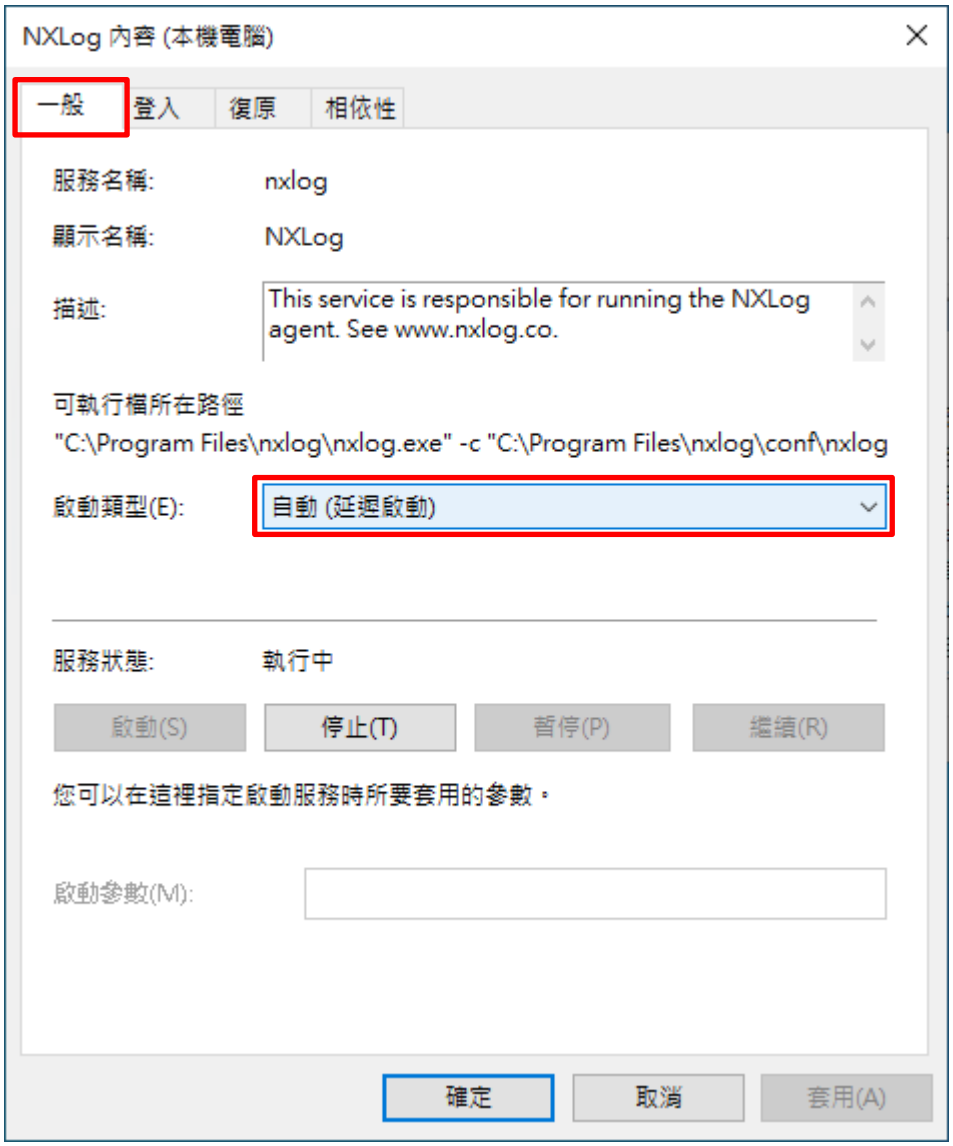


(4) 開啟 NXLog 服務內容

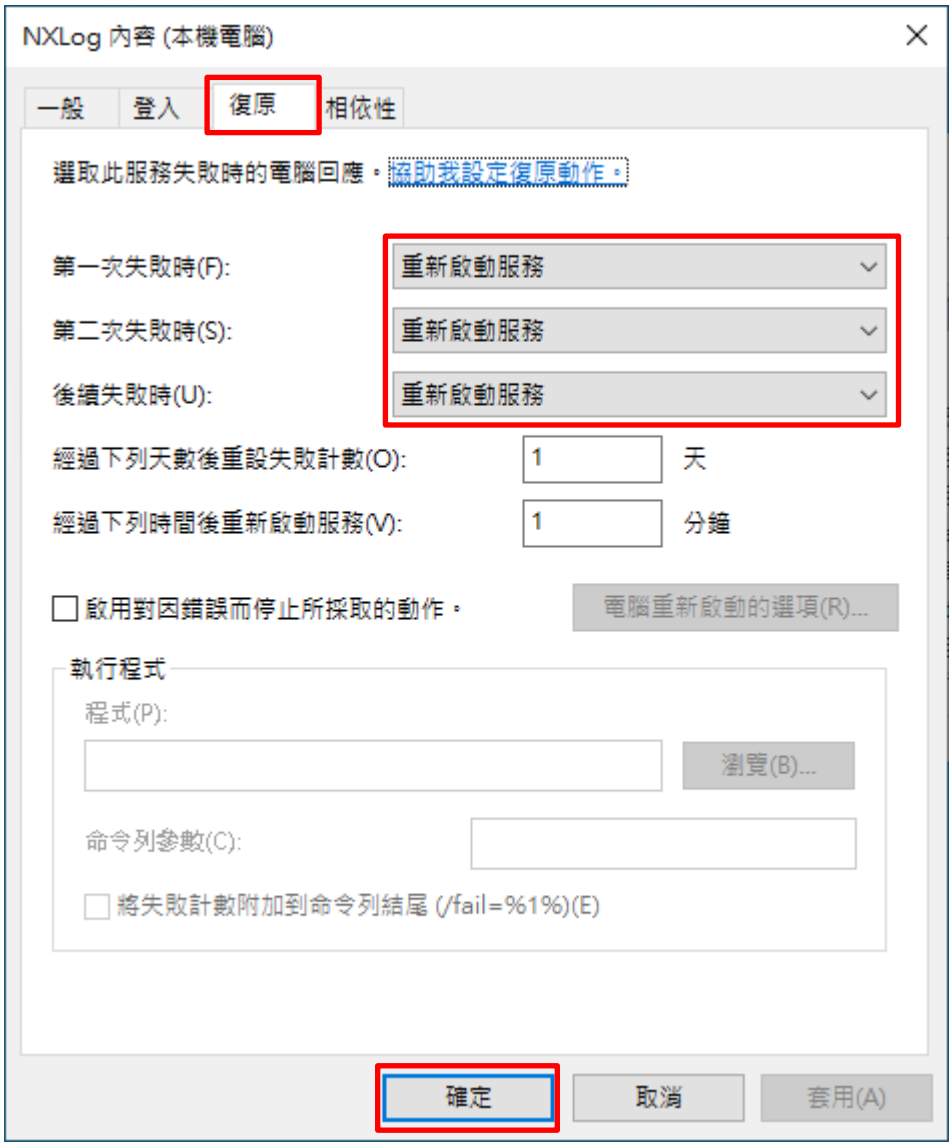
選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (延遲啟動)]



(6) [復原] 頁面 -> 確認；第一次失敗時: 和 第二次失敗時: 和 後續失敗時: [重新啟動服務] -> 按 [確定]



2. Exchange 2007

範例：Exchange 2007 安裝在 Windows 2003 伺服器。

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

2.1 Exchange MessageTracking Log

修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

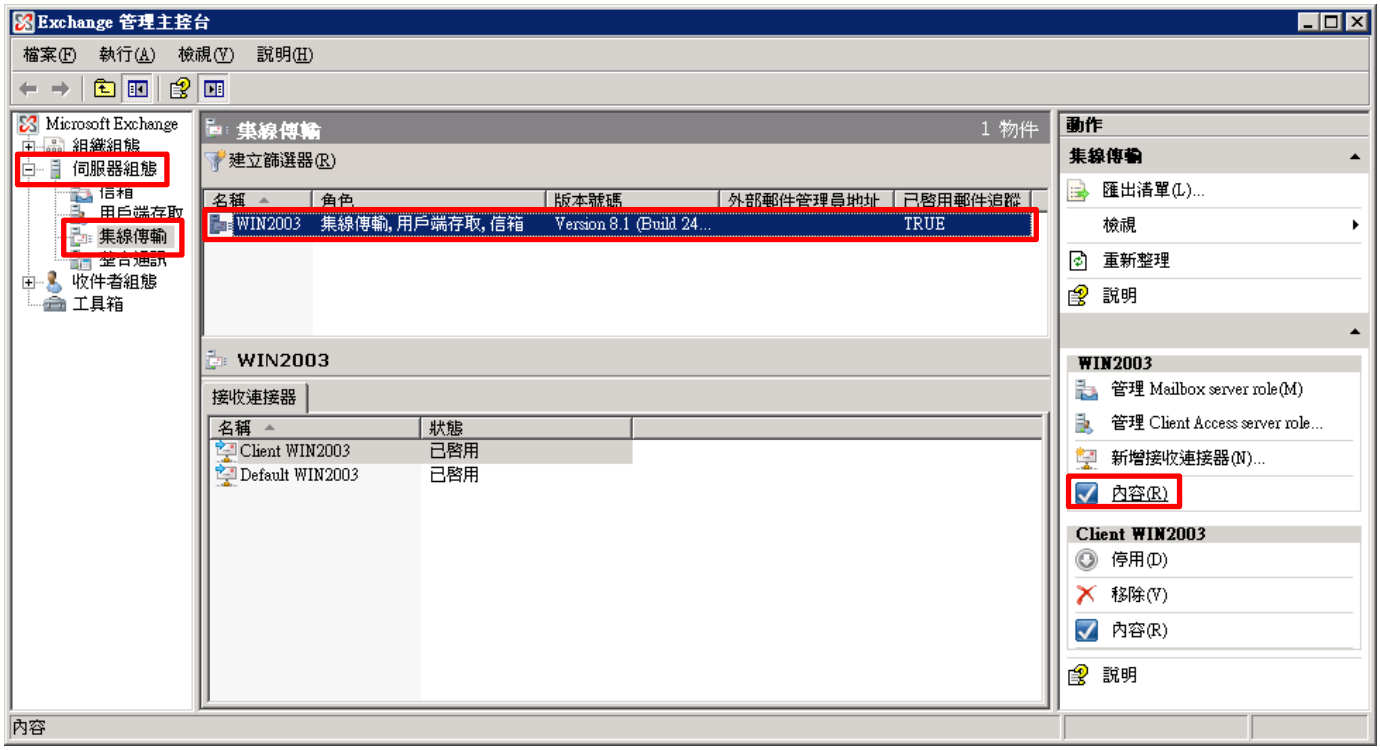
藍色文字部位請修改郵件追蹤記錄資料夾

```
define MailLog     C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
```

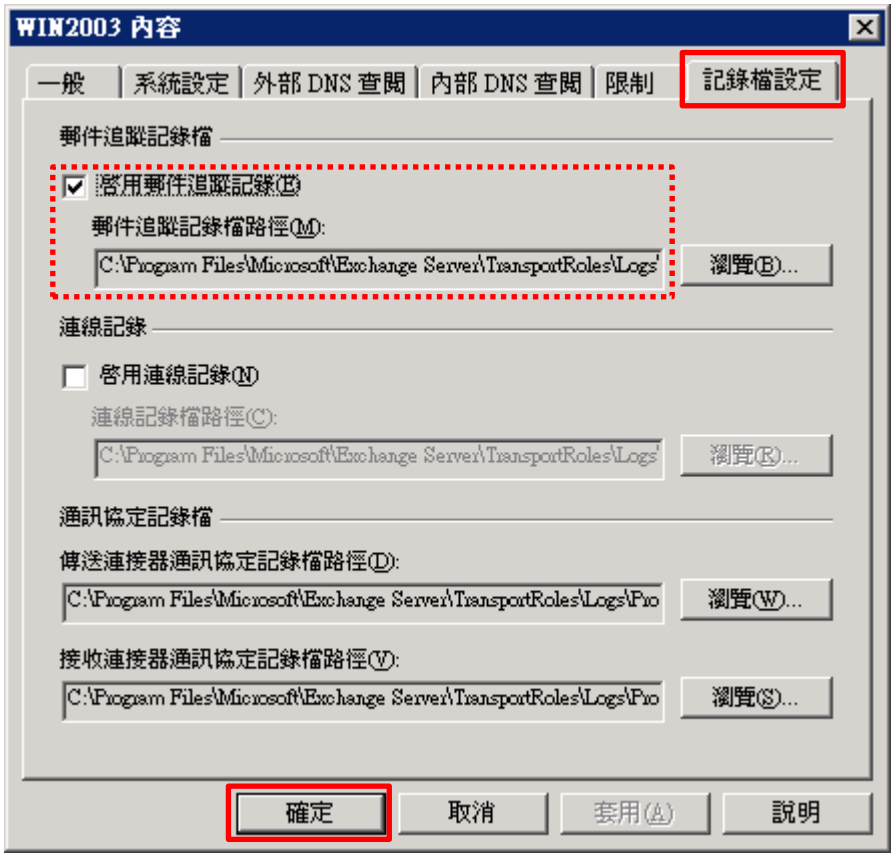
2.1.1 Exchange 管理主控台

(1) 開啟 [Exchange 管理主控台]

(2) 展開 [伺服器組態] -> 點選 [集線傳輸] -> [Exchange 伺服器(WIN2003)] -> [內容]



(3) 點選 [記錄檔設定] 頁面 -> 確認 [啟用郵件追蹤記錄] 和郵件追蹤記錄檔路徑 [C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking] -> 按 [確定]

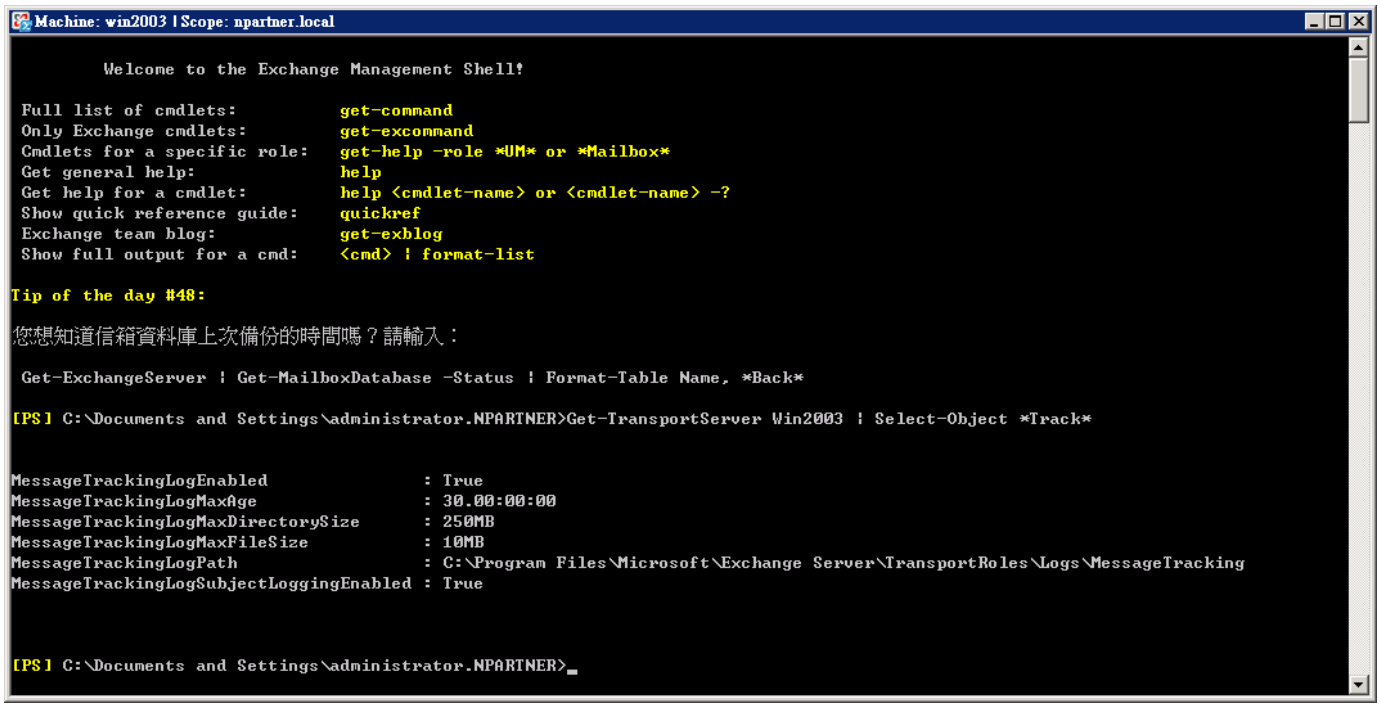


2.1.2 Exchange 管理命令介面

(1) 開啟 [Exchange 管理命令介面]

(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking]

[PS] C:\> Get-TransportServer Win2003 | Select-Object *Track*

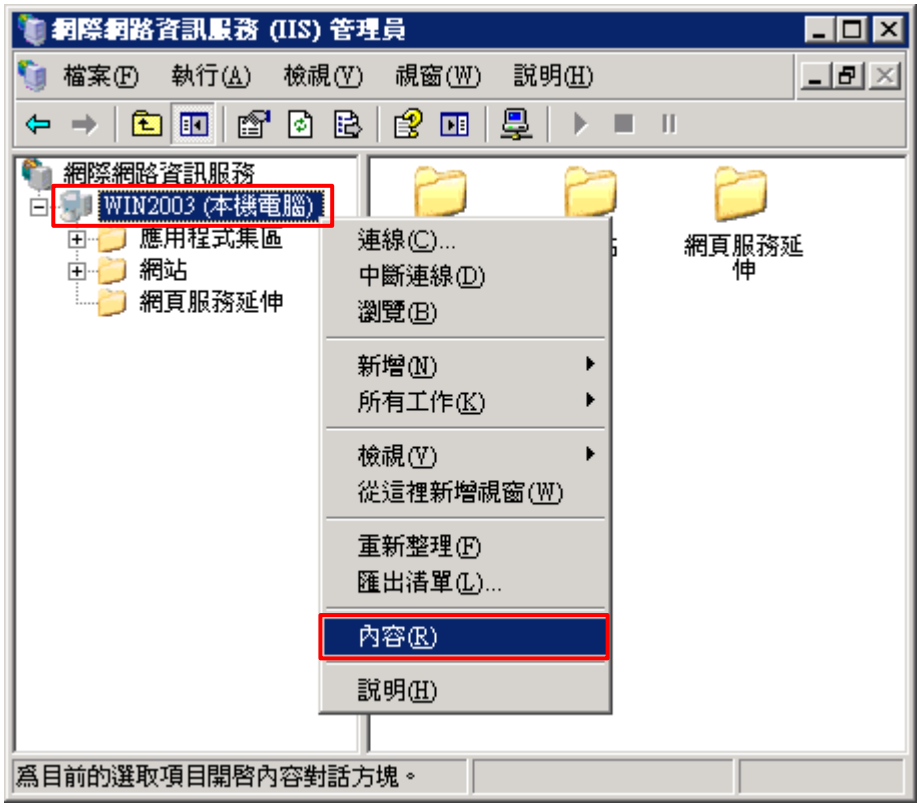


紅色文字部位請輸入 Exchange 伺服器名稱

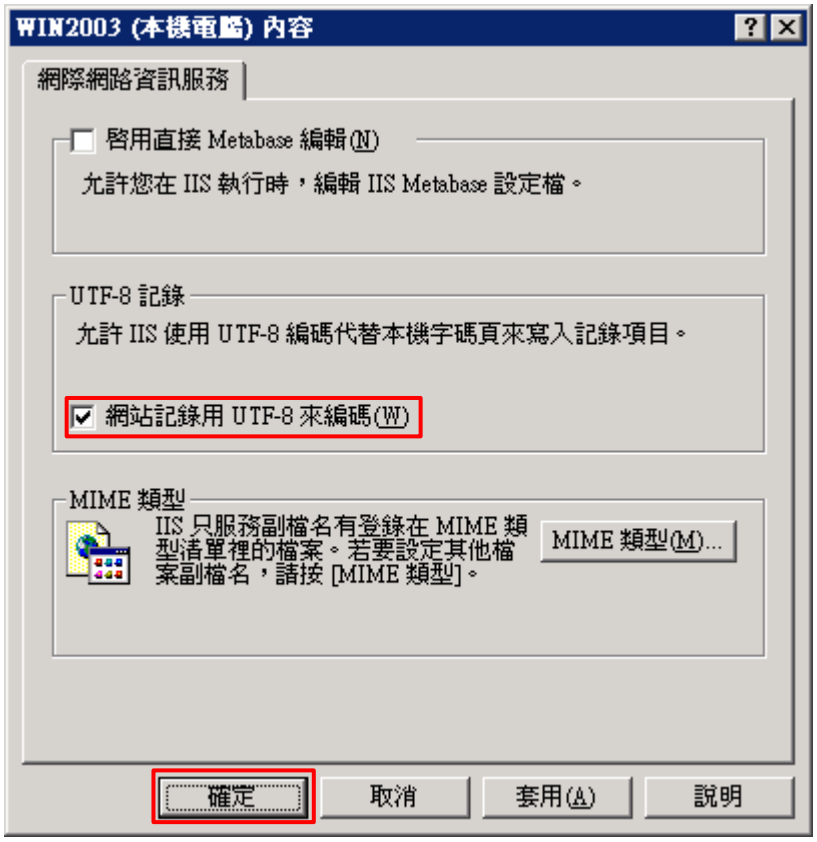
2.2 IIS Log

(1) 開啟 [網際網路資訊服務 (IIS) 管理員]

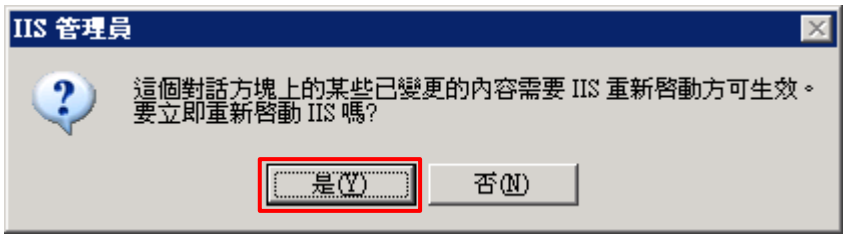
(2) 在 [IIS 伺服器] 按滑鼠右鍵 -> 選擇 [內容]



(3) 勾選 [網站記錄用 UTF-8 來編碼] -> 按 [確定]



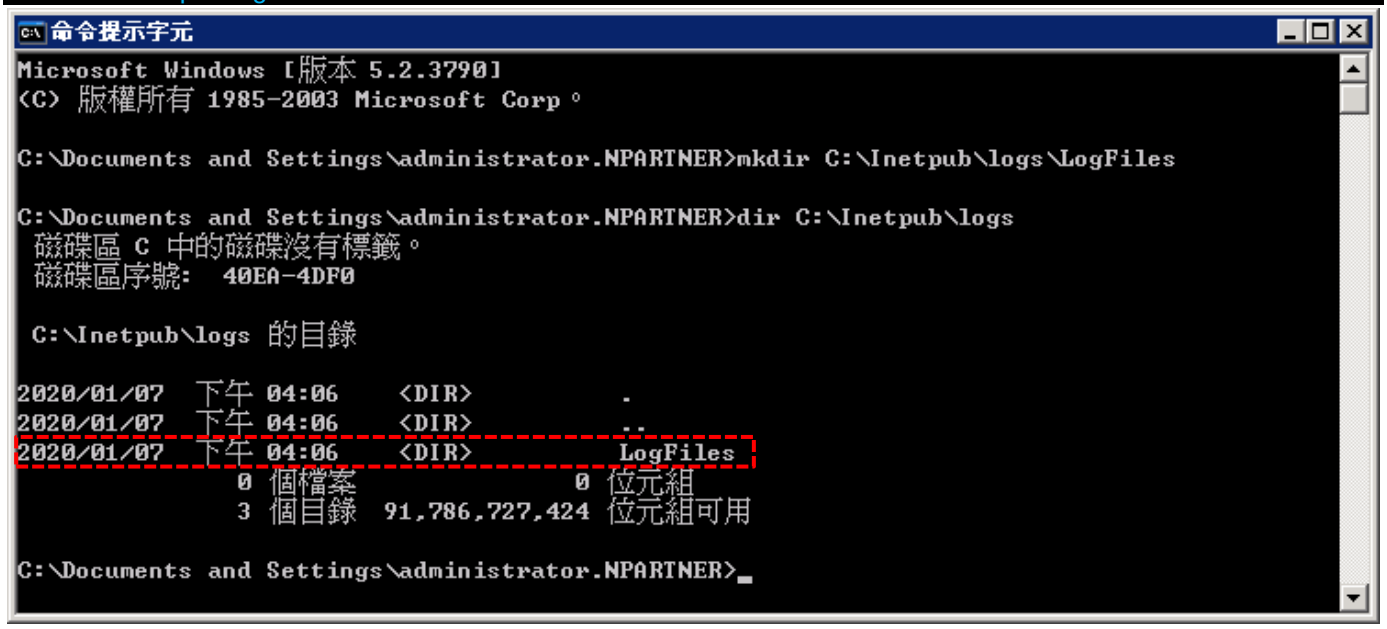
(4) 按 [確定] 重啟 IIS 服務



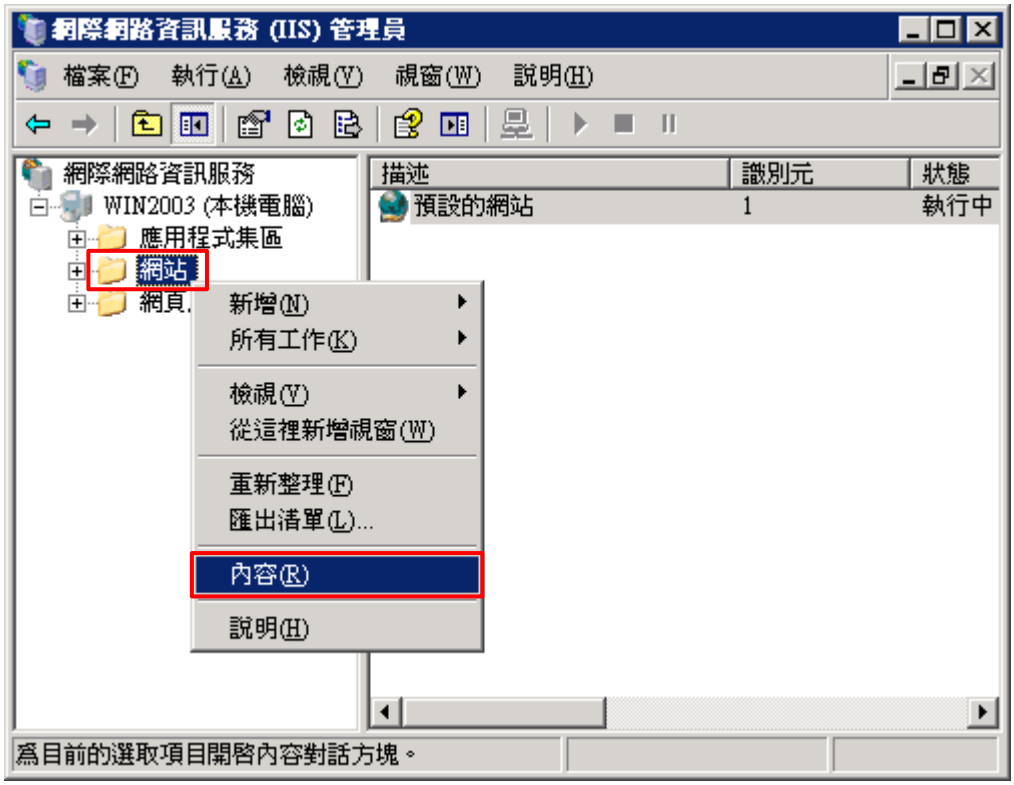
(5) 開啟 [命令提示字元]

(6) 新增 IIS LogFiles 資料夾和確認 IIS LogFiles 資料夾

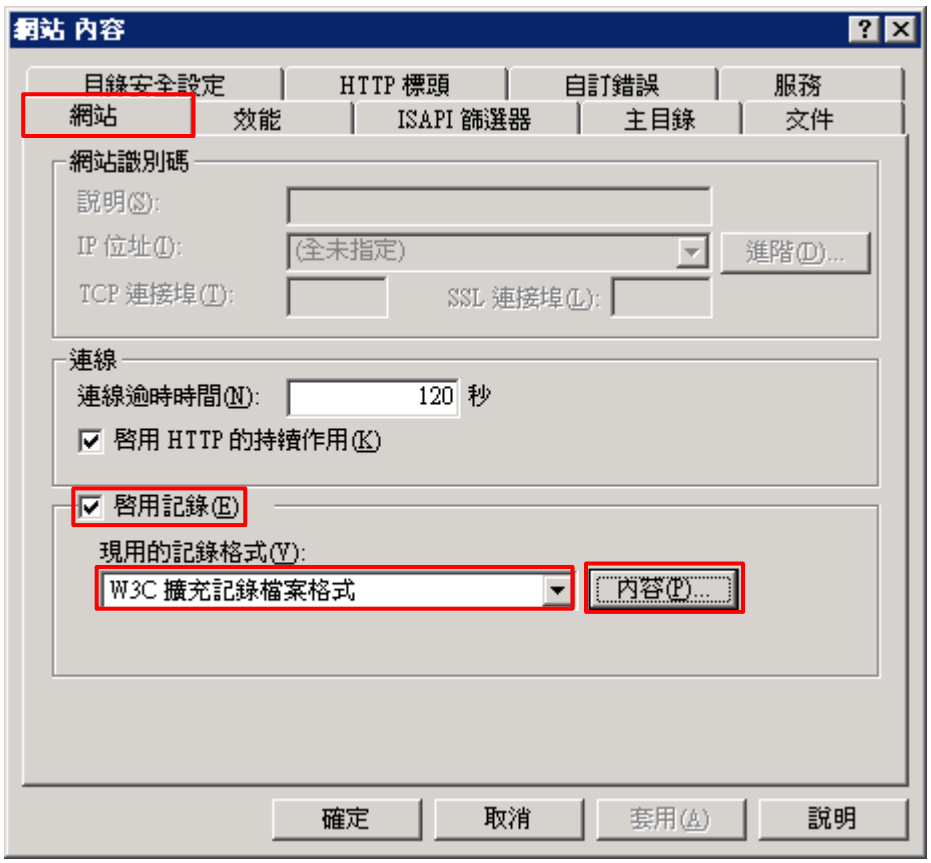
```
C:\> mkdir C:\Inetpub\logs\LogFiles
C:\> dir C:\Inetpub\logs
```



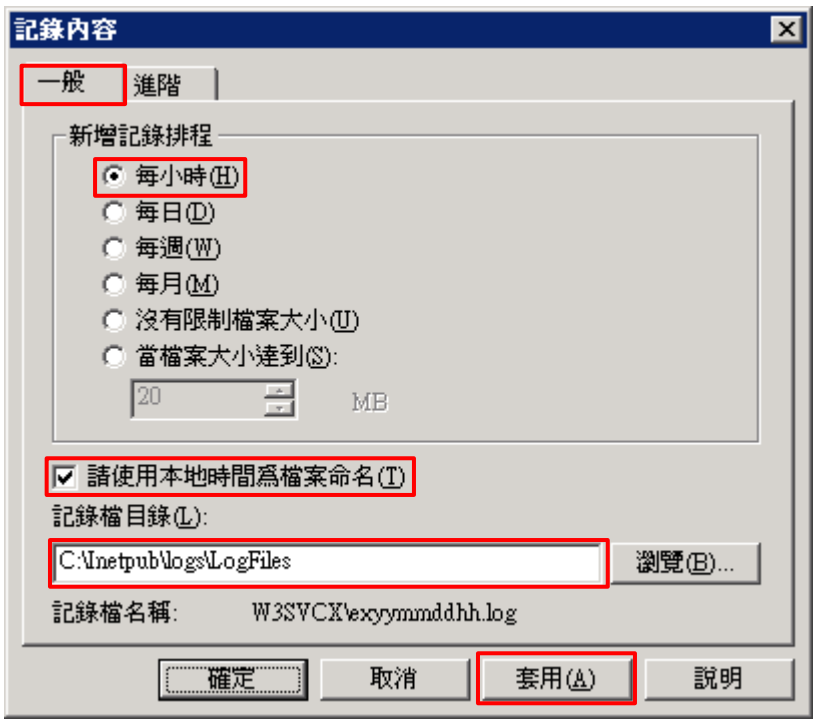
(7) 在 [網站] 按滑鼠右鍵 -> 選擇 [內容]



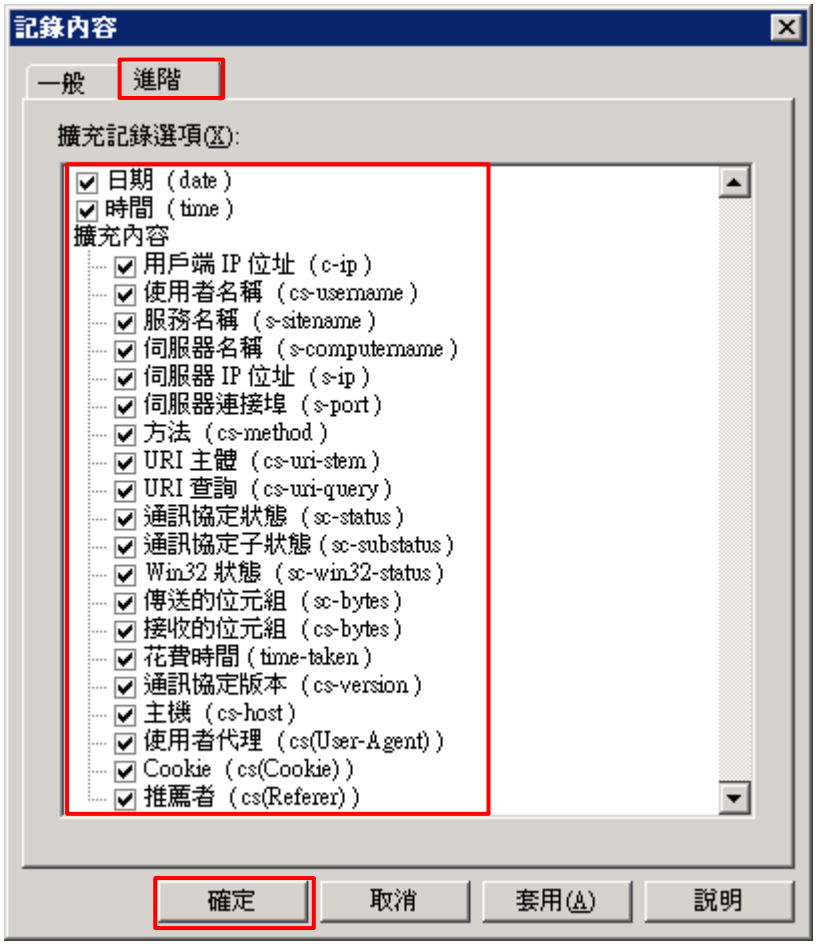
(8) [網站] 頁面: 勾選 [啟用記錄] -> 現用的記錄格式選擇 [W3C 擴充記錄檔案格式] -> 按 [內容]



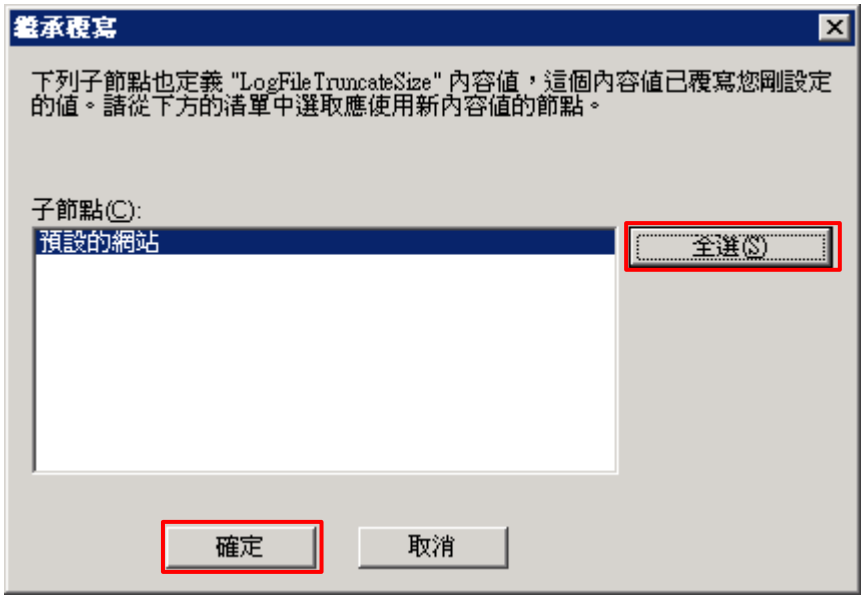
(9) [一般] 頁面: 新增記錄排程點選 [每小時] -> 勾選 [請使用本地時間為檔案命名] -> 記錄檔目錄輸入 C:\Inetpub\logs\LogFiles -> 按 [套用]



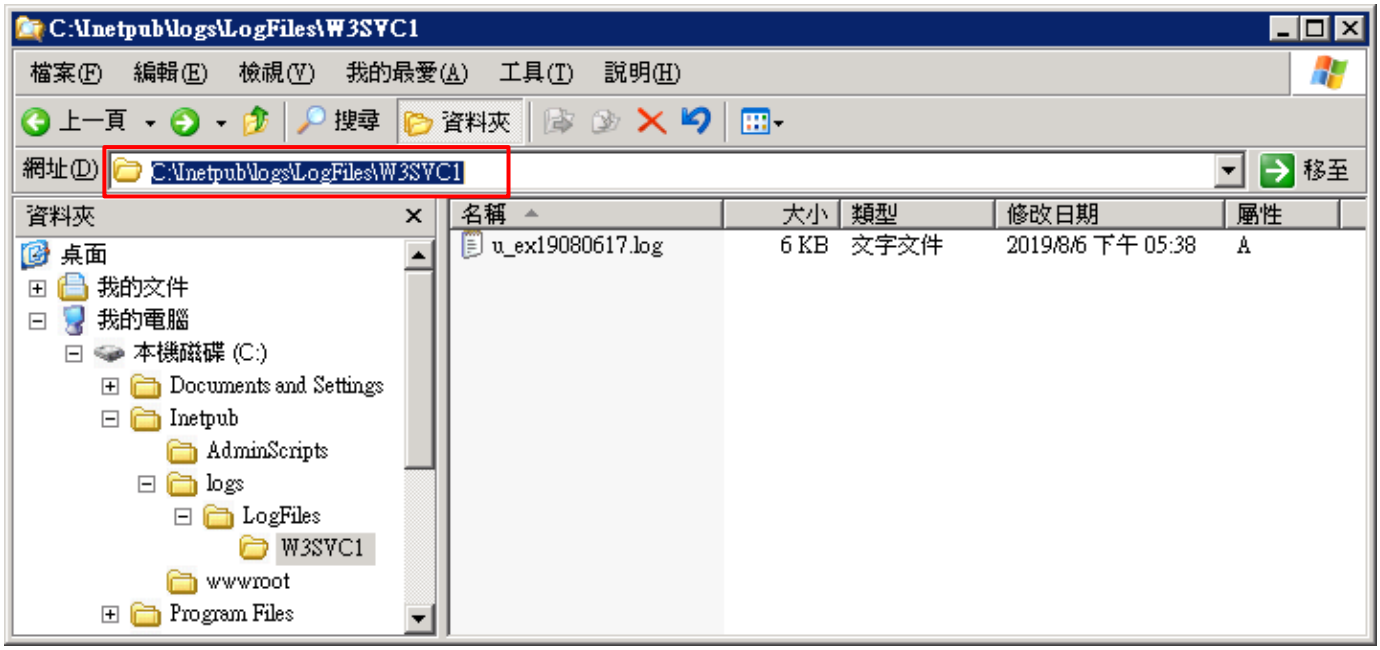
(10) [進階] 頁面：擴充記錄選項勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按 [確定]



(11) 按 [全選] 套用所有網站和 [確定]



(12) 確認 [C:\Inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



2.3 Event Log

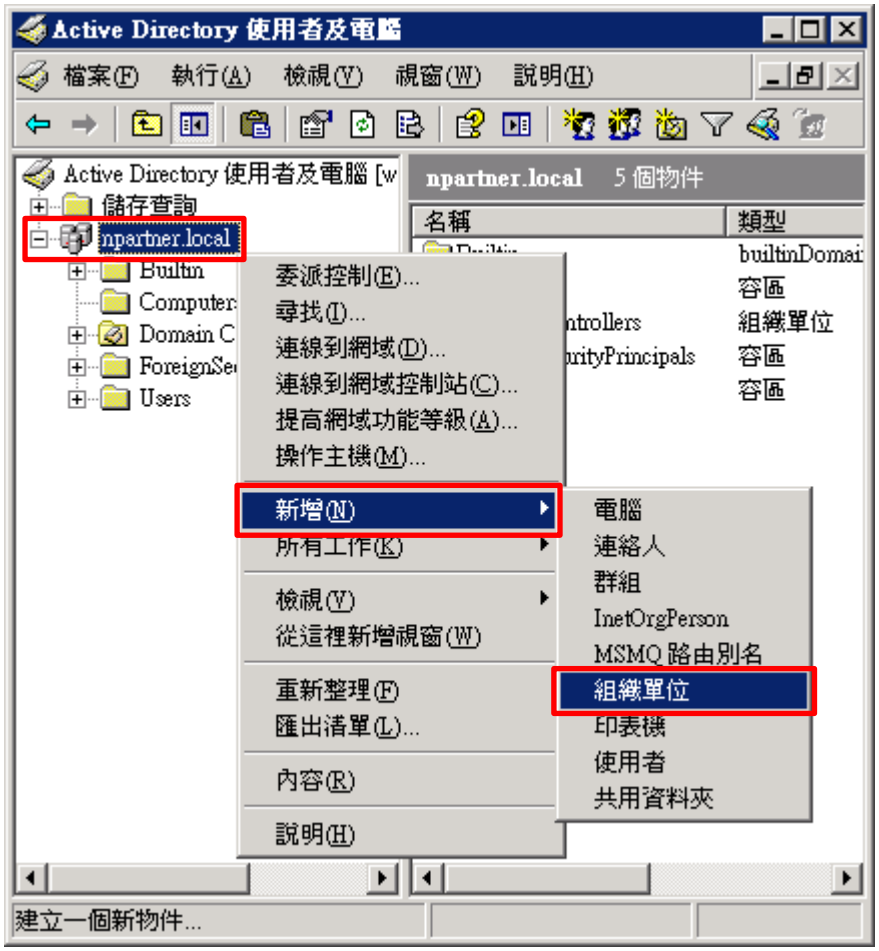
2.3.1 組織單位

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

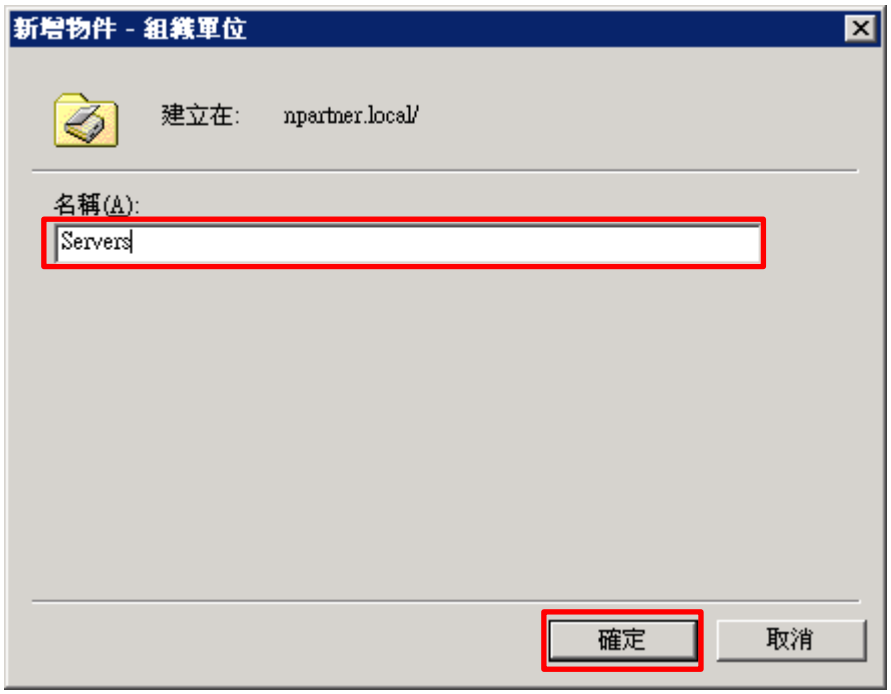
(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



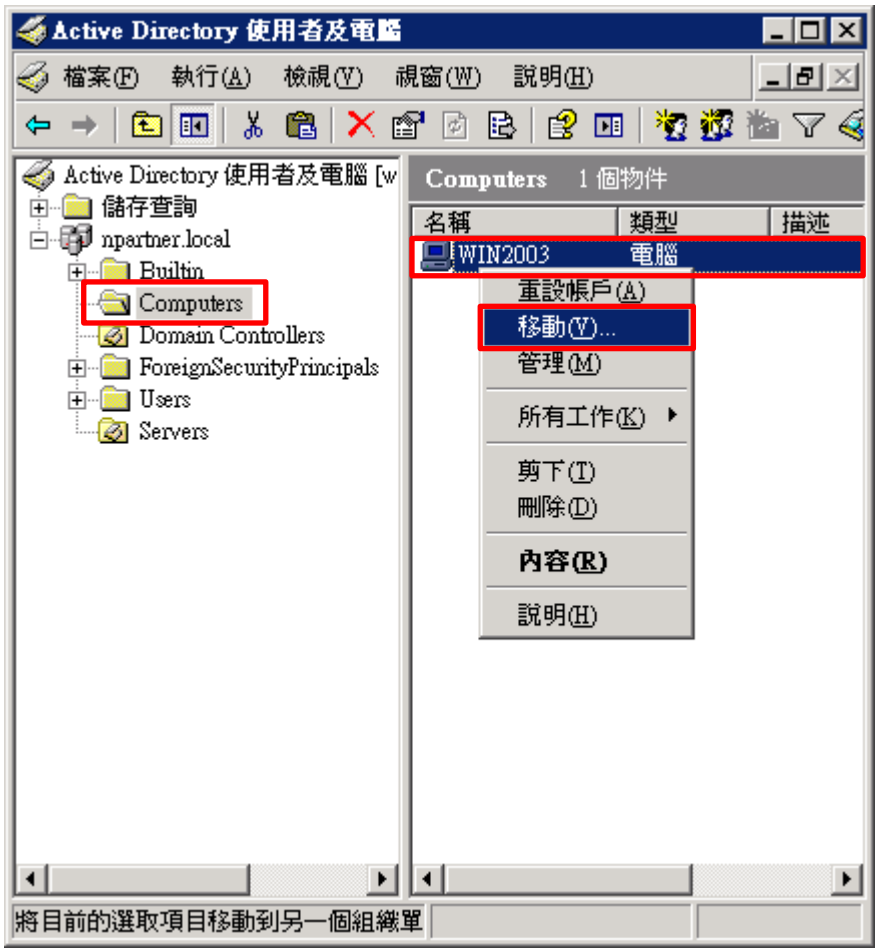
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



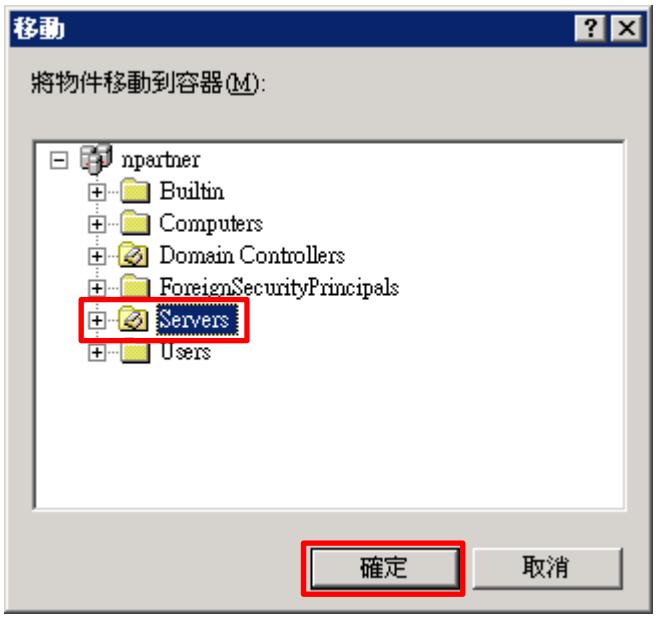
(4) 移動 Exchange 伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2003] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Exchange Server 主機 -> 點選 [移動]



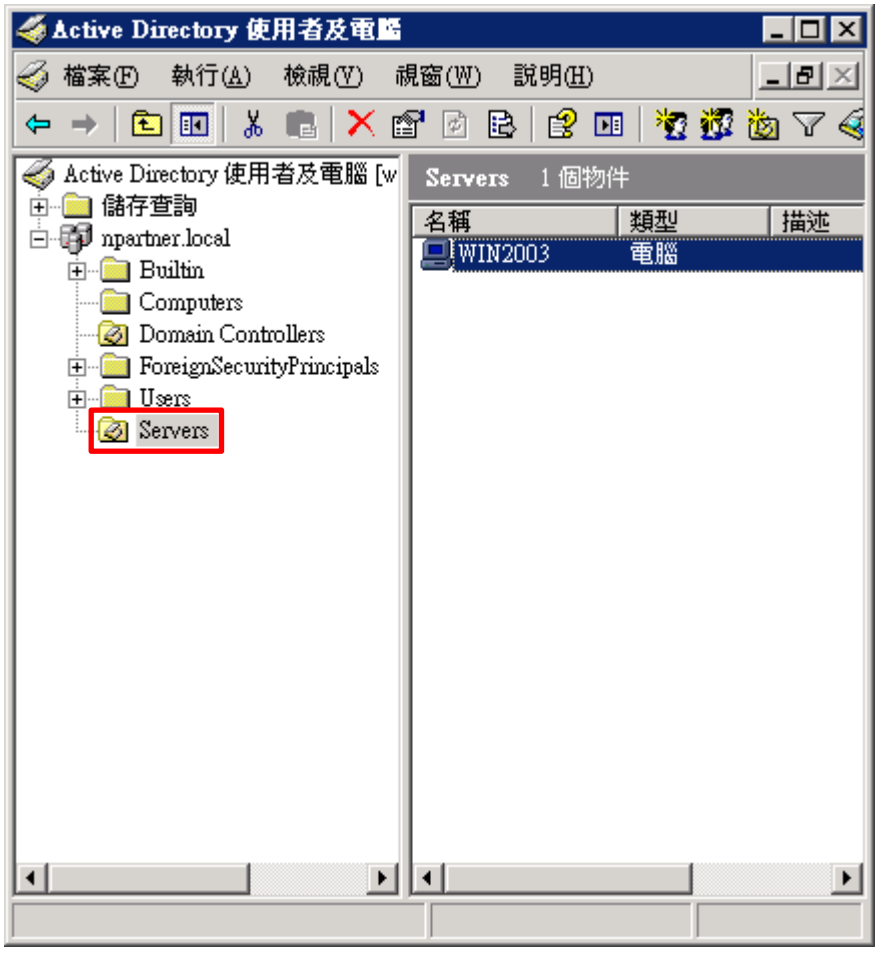
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認 Exchange 伺服器已移動至新的組織單位

點選 [Servers] 組織單位，確認 Win2003 伺服器已移動。



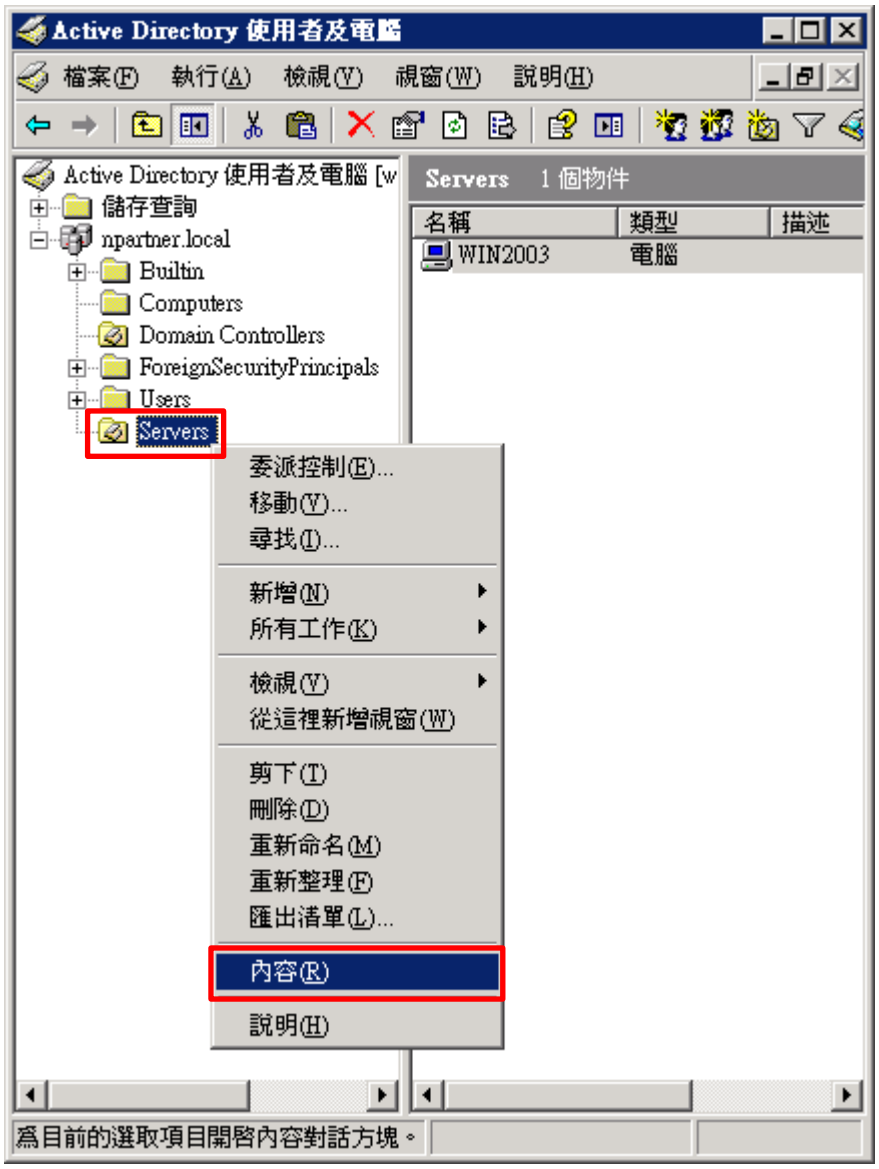
2.3.2 群組原則

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

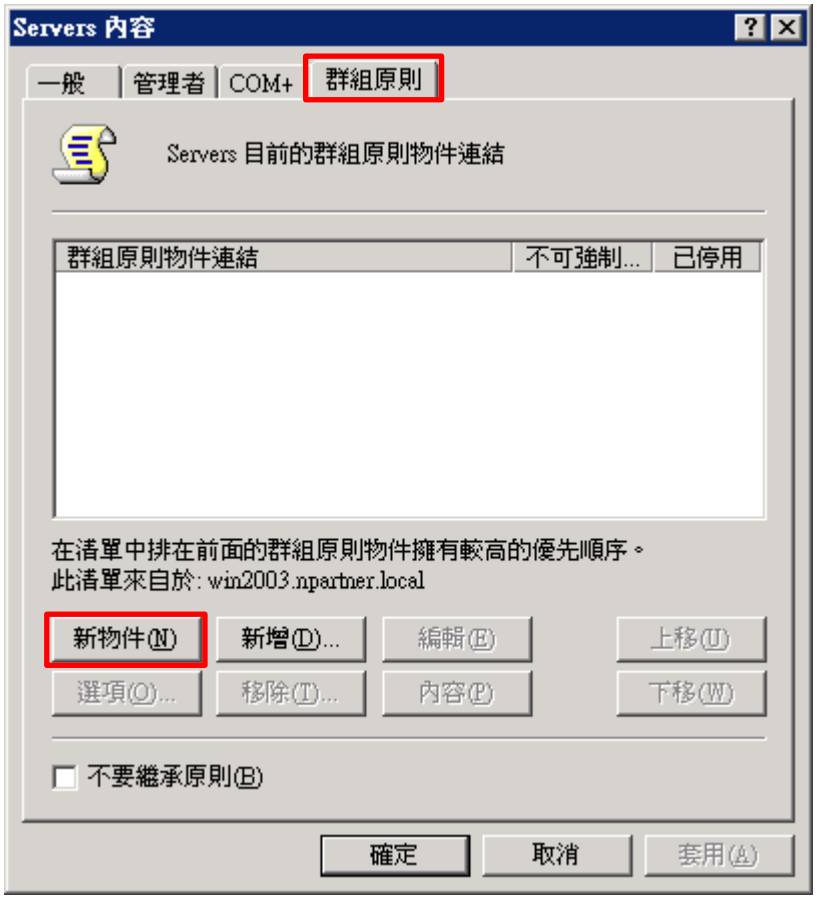
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



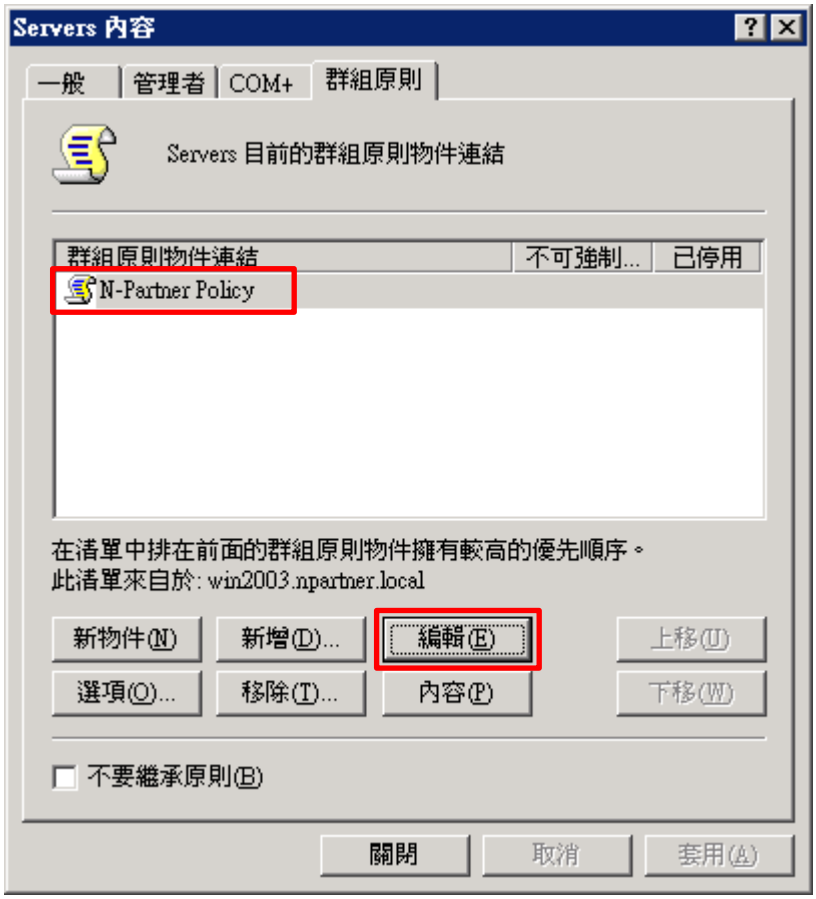
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



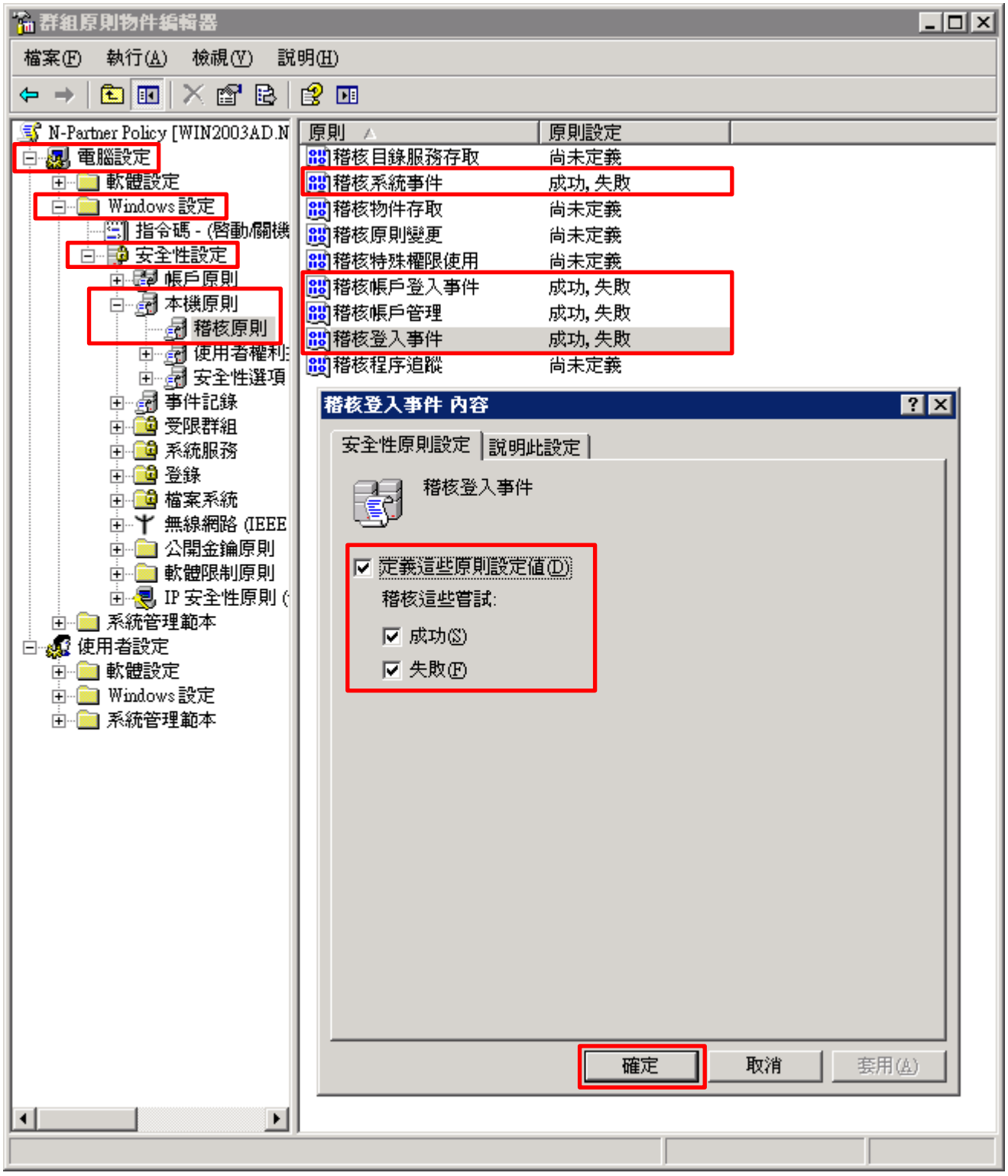
(4) 編輯群組原則物件

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [編輯]



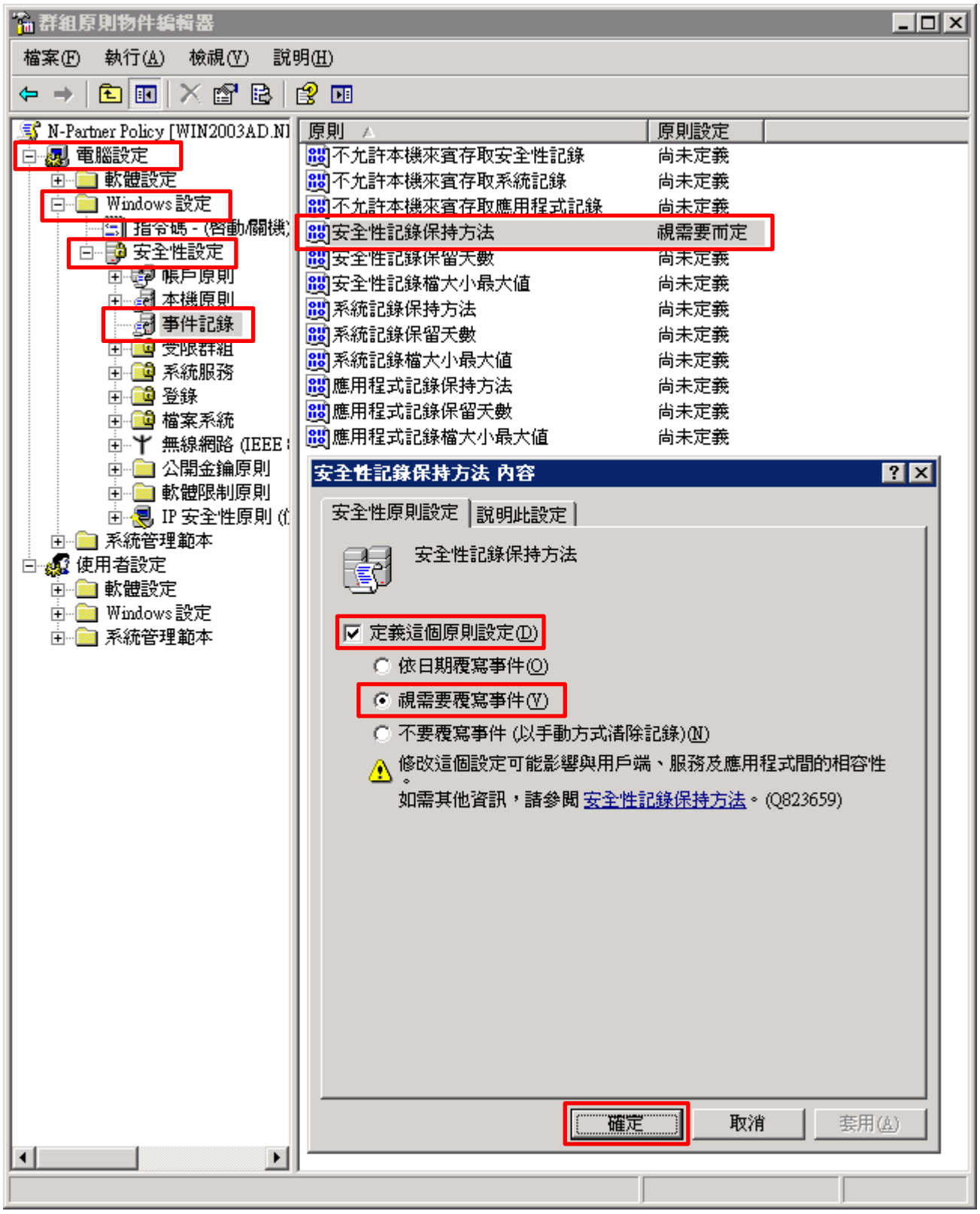
(5) 本機原則：稽核原則

選擇 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



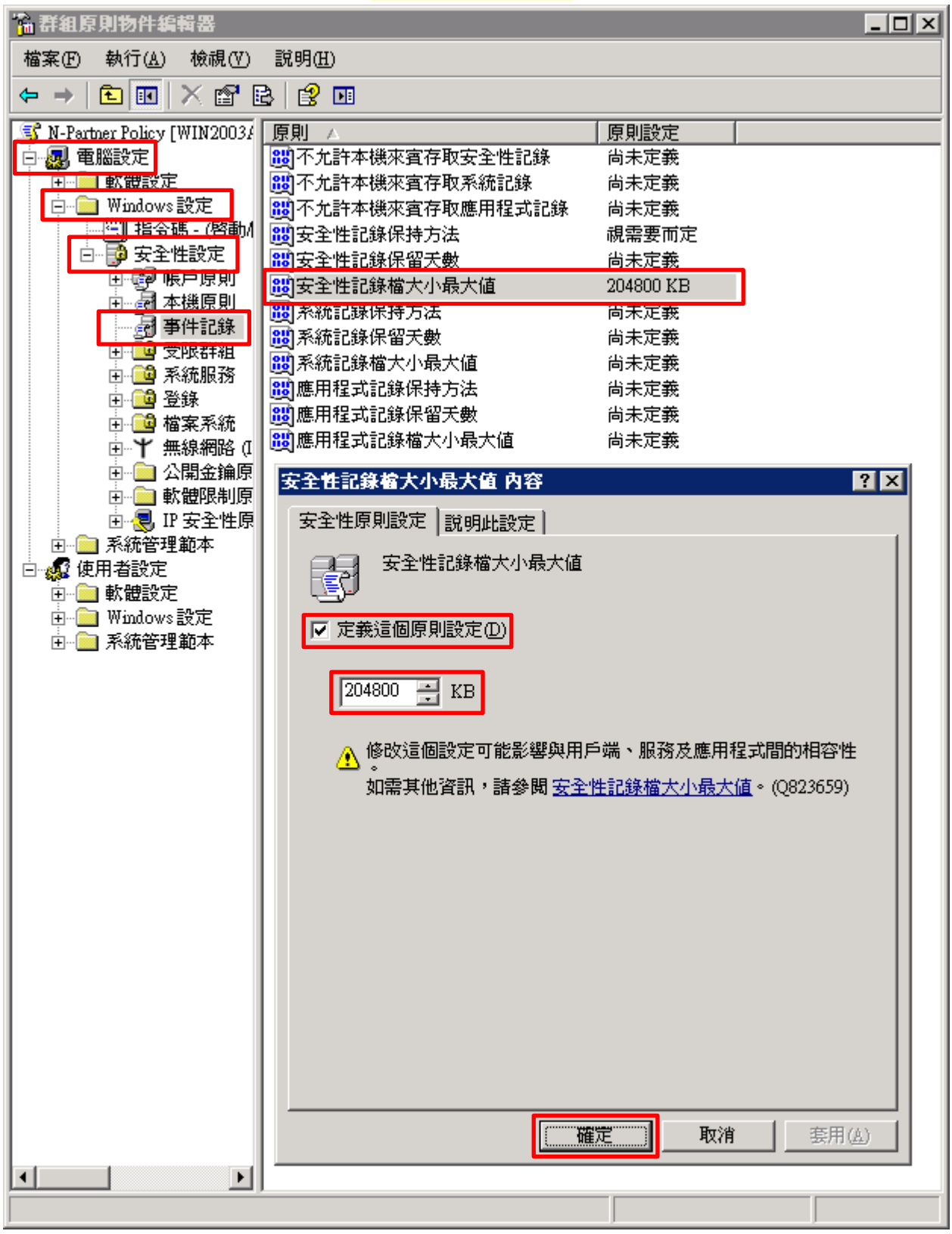
(6) 事件記錄：安全性記錄保持方法

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(7) 事件記錄：安全性記錄檔大小最大值

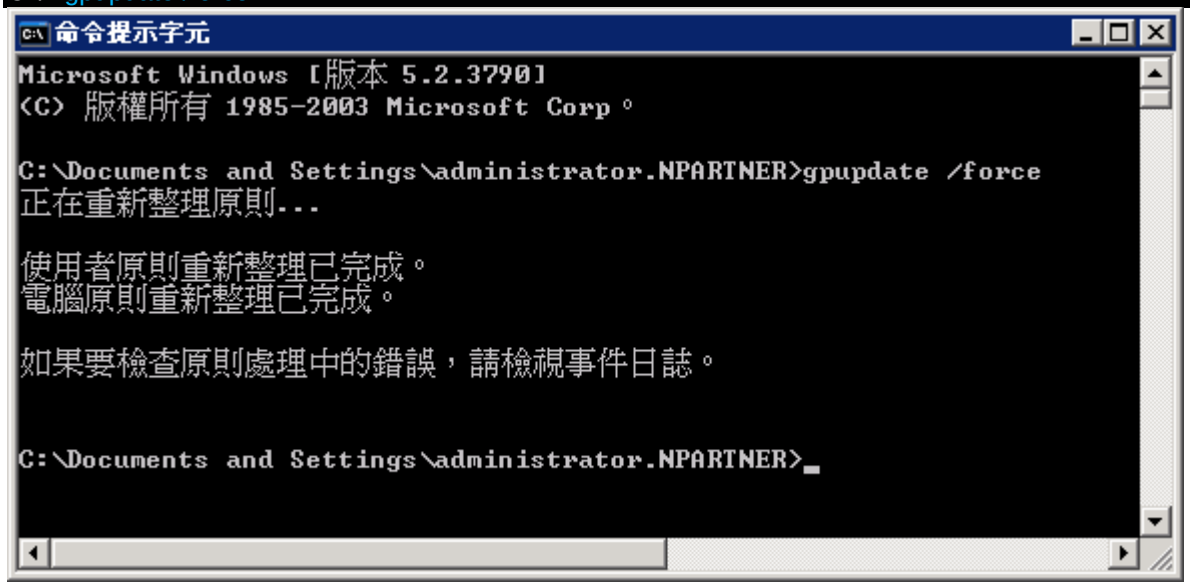
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8) 在 Exchange 伺服器 -> 開啟 [命令提示字元]

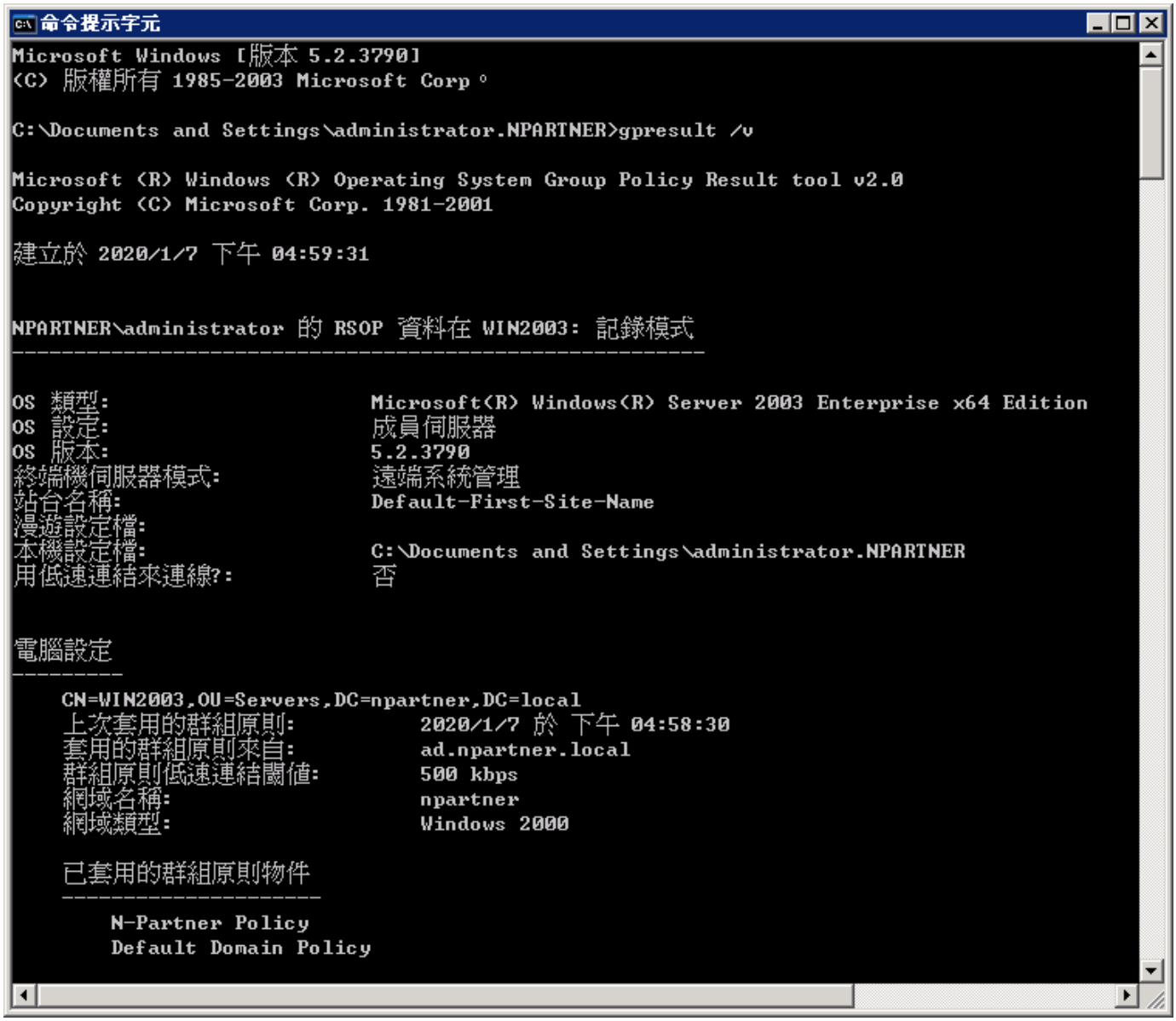
(9) 更新群組原則

```
C:\> gpupdate /force
```



(10) 查看群組原則套用情形

C:\> gpresult /v



3. Exchange 2010

範例：Exchange 2010 安裝在 Windows 2008 伺服器。

可選擇 [Exchange Management Console] 或 [Exchange Management Shell] 設定郵件追蹤記錄。

3.1 Exchange Message Tracking Log

修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

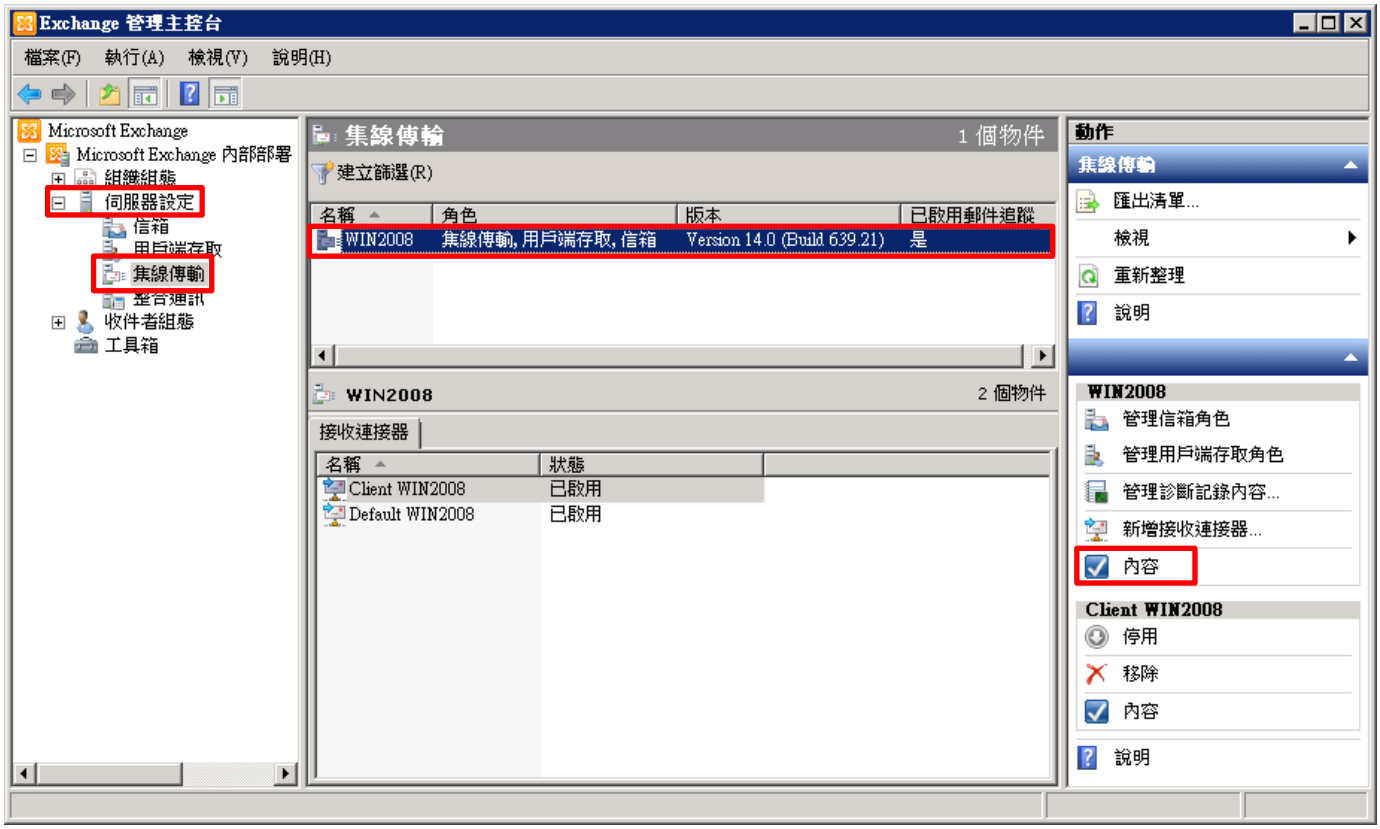
藍色文字部位請修改郵件追蹤記錄資料夾

```
define MailLog     C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking
```

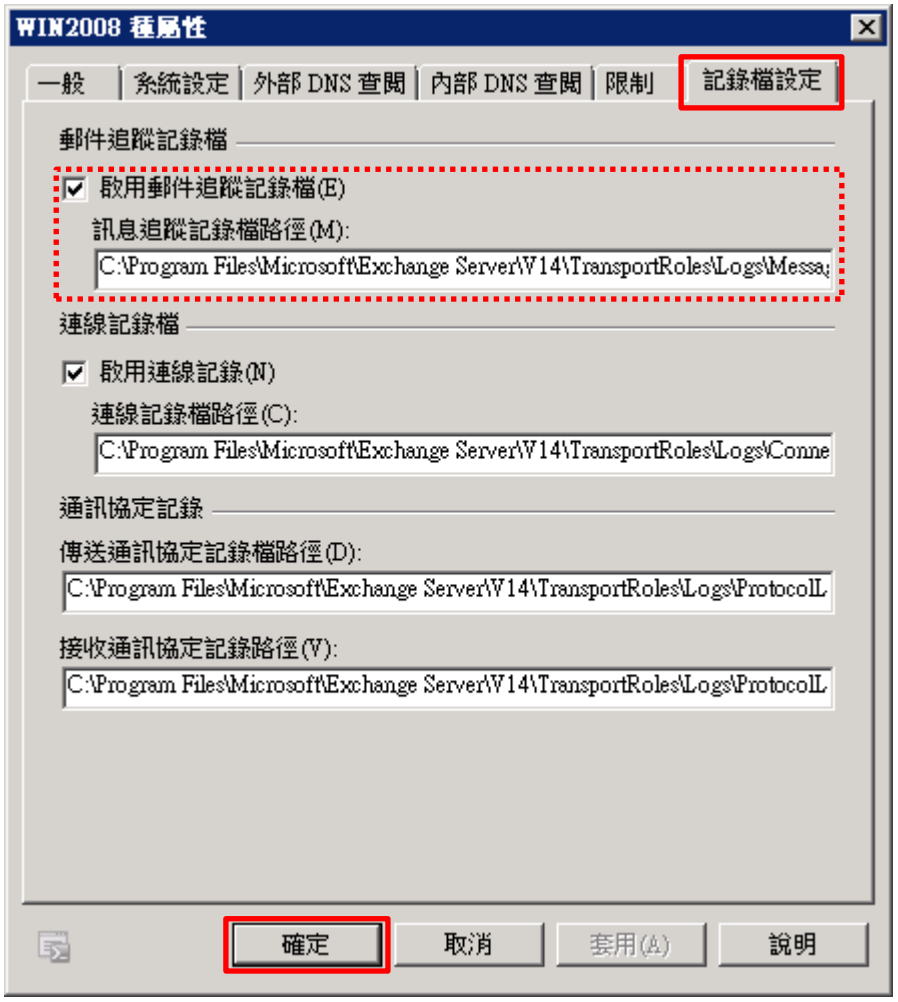
3.1.1 Exchange Management Console

(1) 開啟 [Exchange Management Console]

(2) 展開 [伺服器設定] -> 點選 [集線傳輸] -> [Exchange 伺服器(WIN2008)] -> [內容]



(3) 點選 [記錄檔設定] 頁面 -> 確認 [啟用郵件追蹤記錄] 和郵件追蹤記錄檔路徑 [C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking] -> 按 [確定]

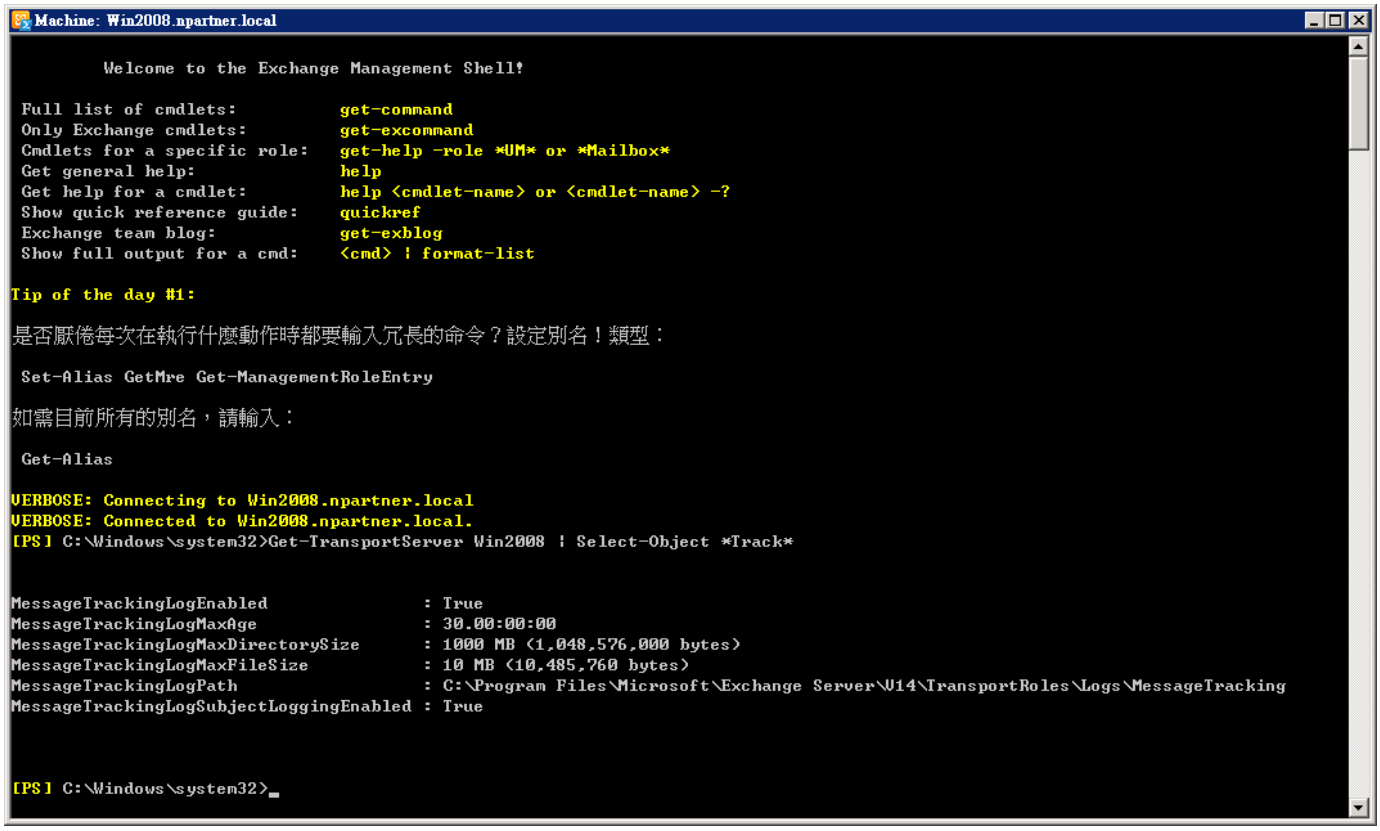


3.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]

(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking]

```
[PS] C:\> Get-TransportServer Win2008 | Select-Object *Track*
```



紅色文字部位請輸入 Exchange 伺服器名稱

3.2 IIS Log

修改 nxlog.conf

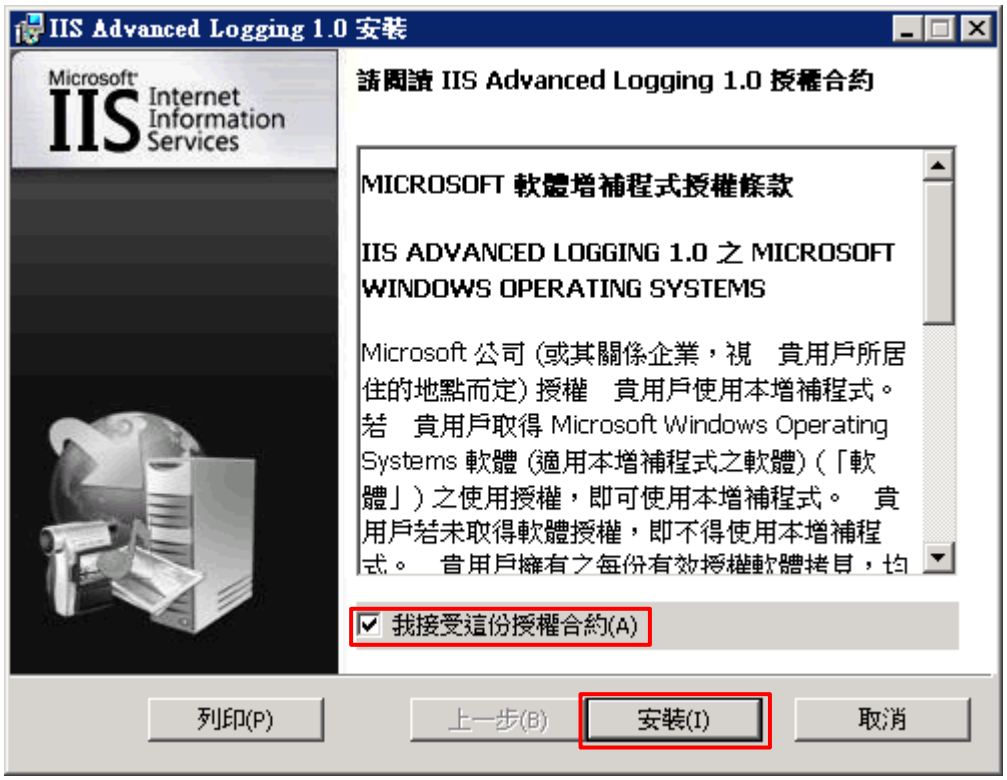
註: 參考 1.3 NXLog 設定檔

藍色文字部位請修改 IIS 記錄檔資料夾路徑

```
define IISLog       C:\inetpub\logs\AdvancedLogs
```

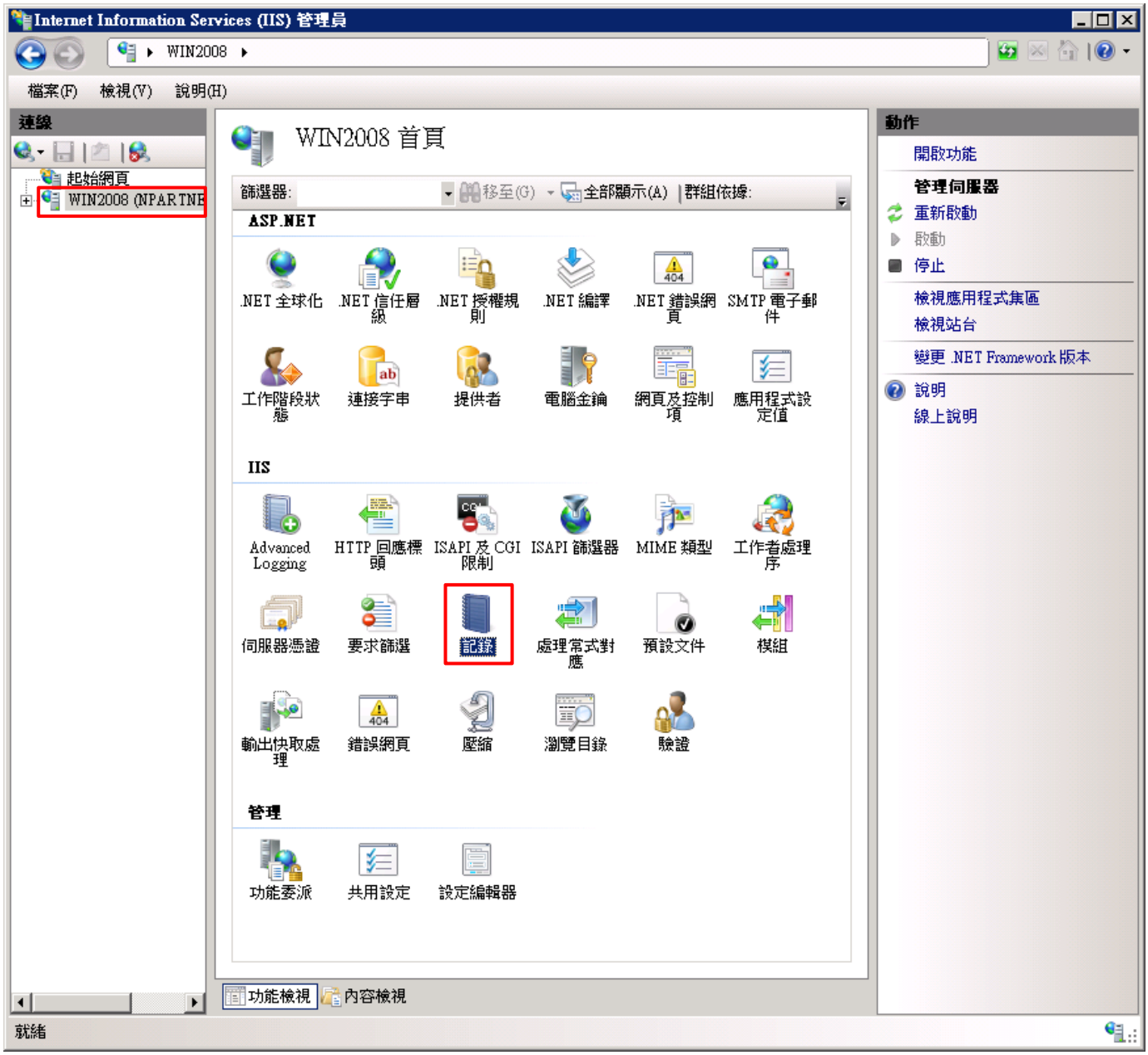
(1) 安裝 IIS Advanced Logging，適用於 Windows Server 2008。

點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]

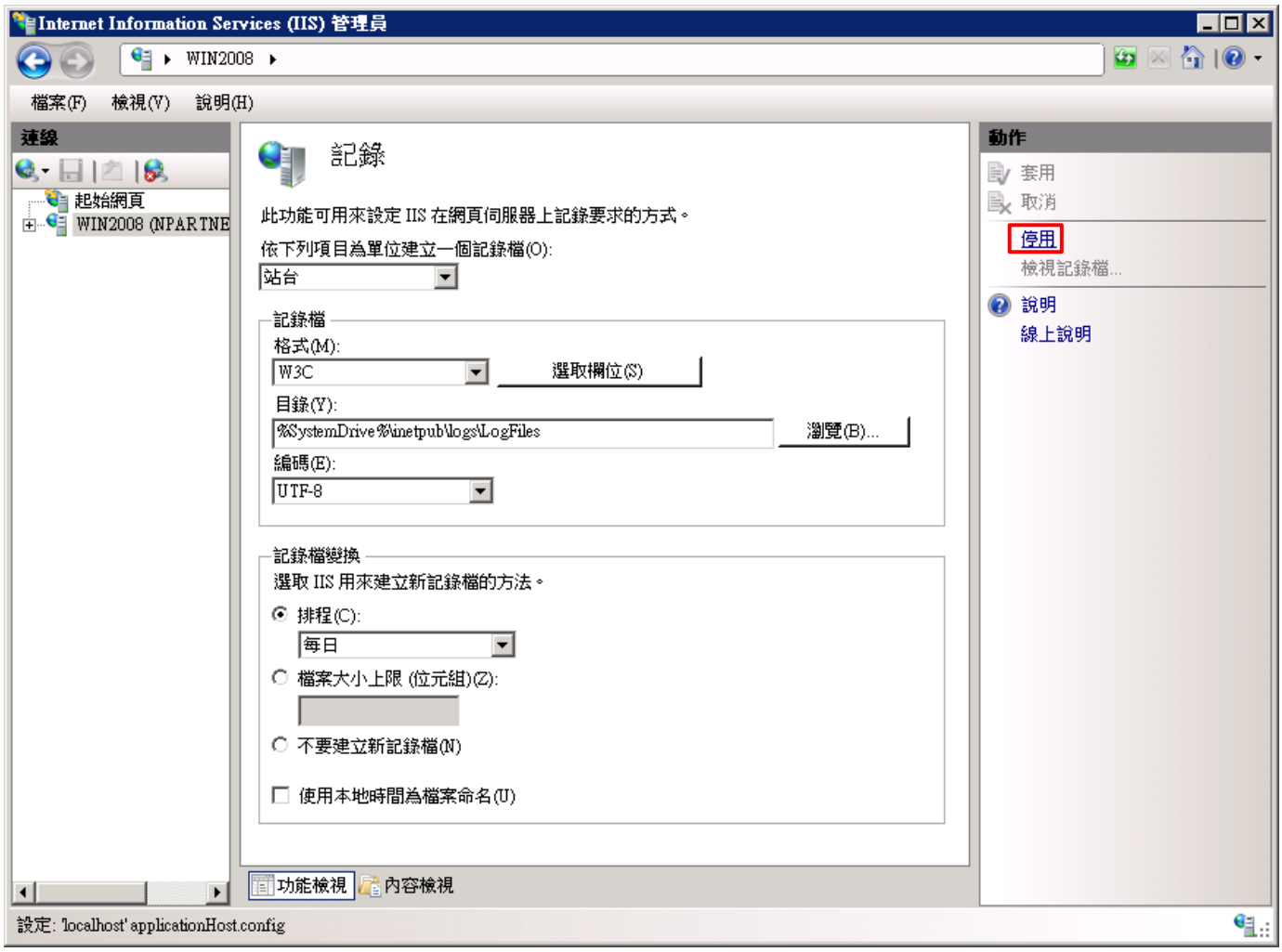


(2) 開啟 [Internet Information Services (IIS) 管理員]

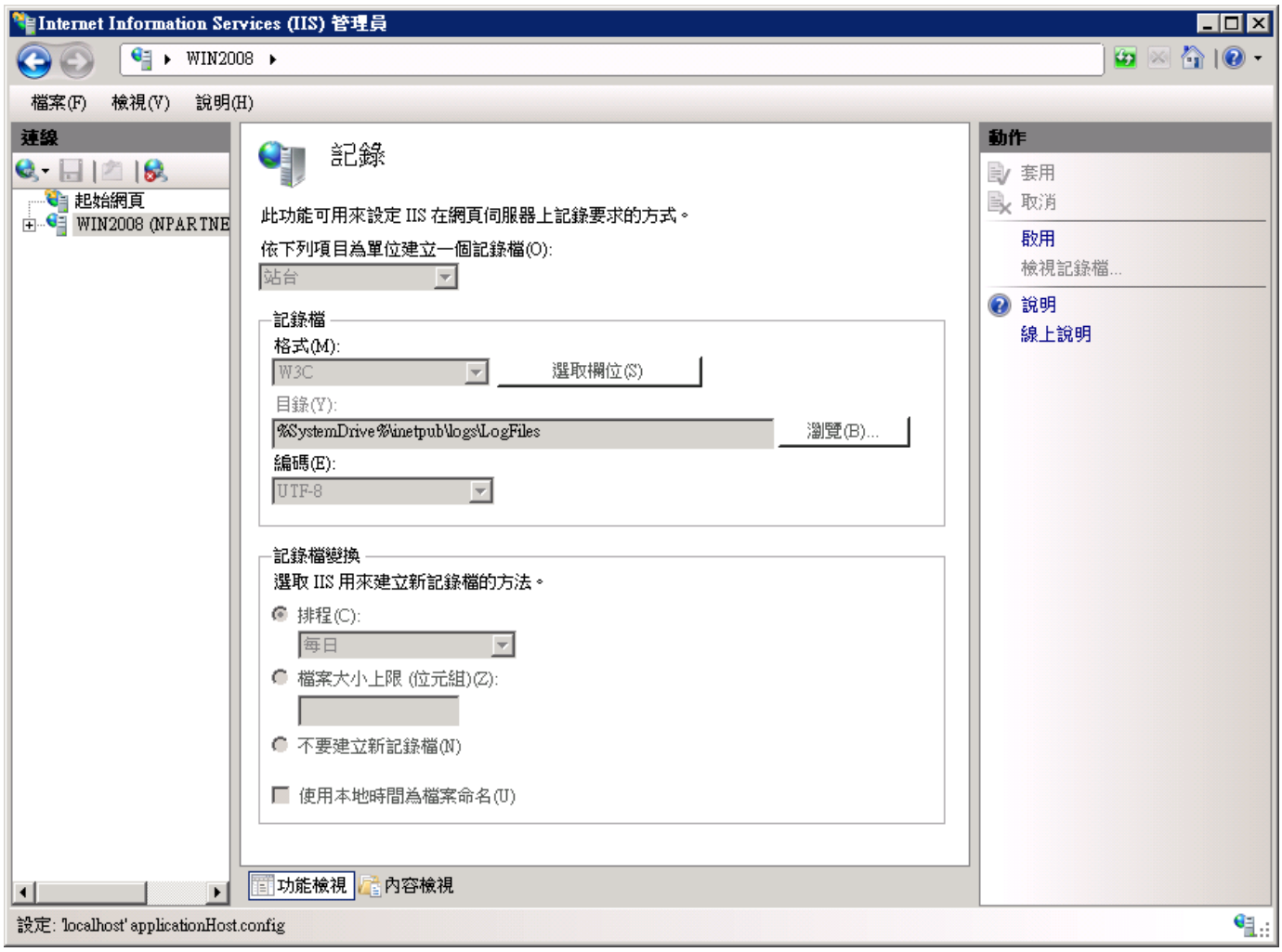
(3) 點選 [IIS 伺服器] -> [記錄]



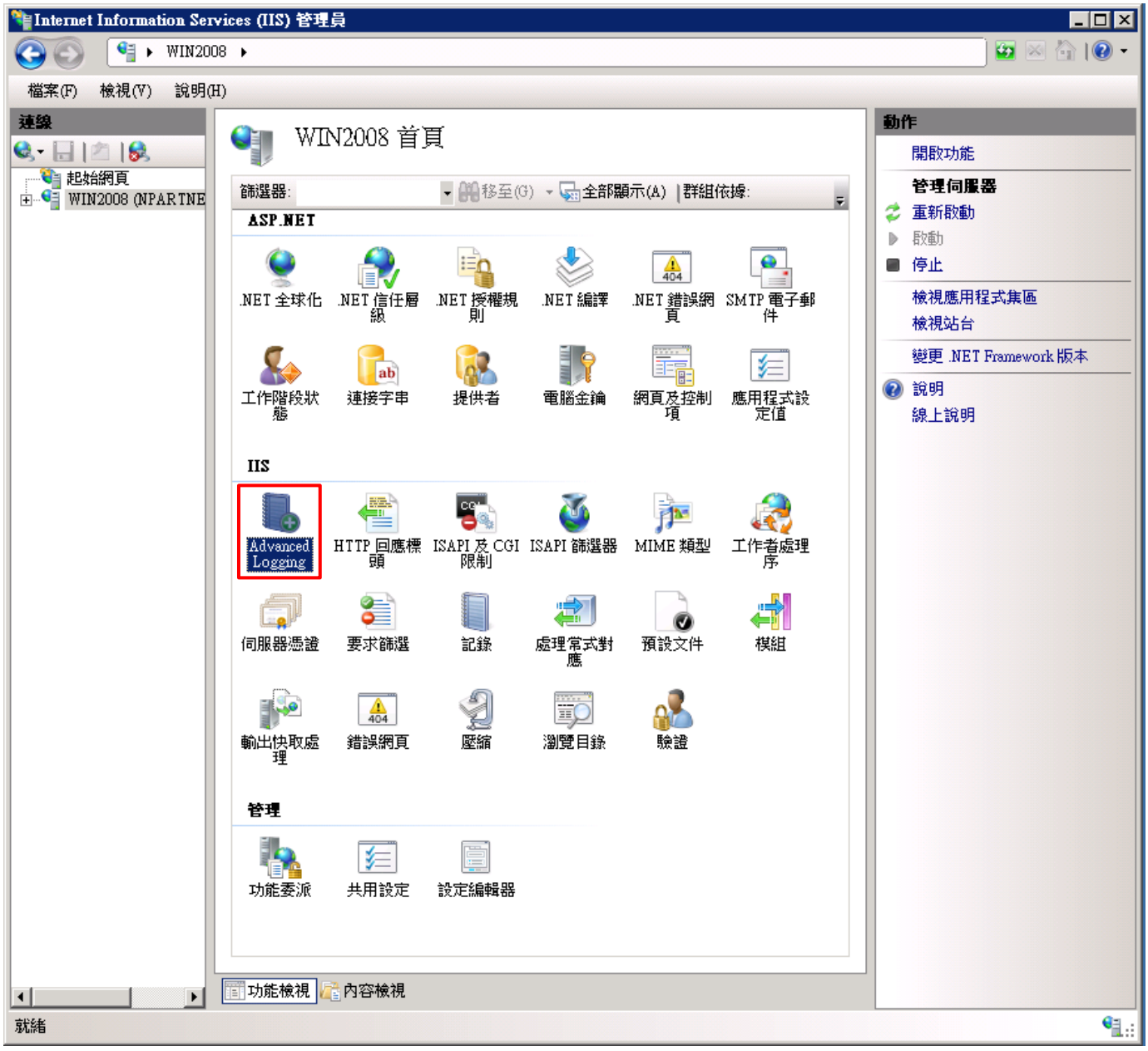
(4) 點選 [停用]



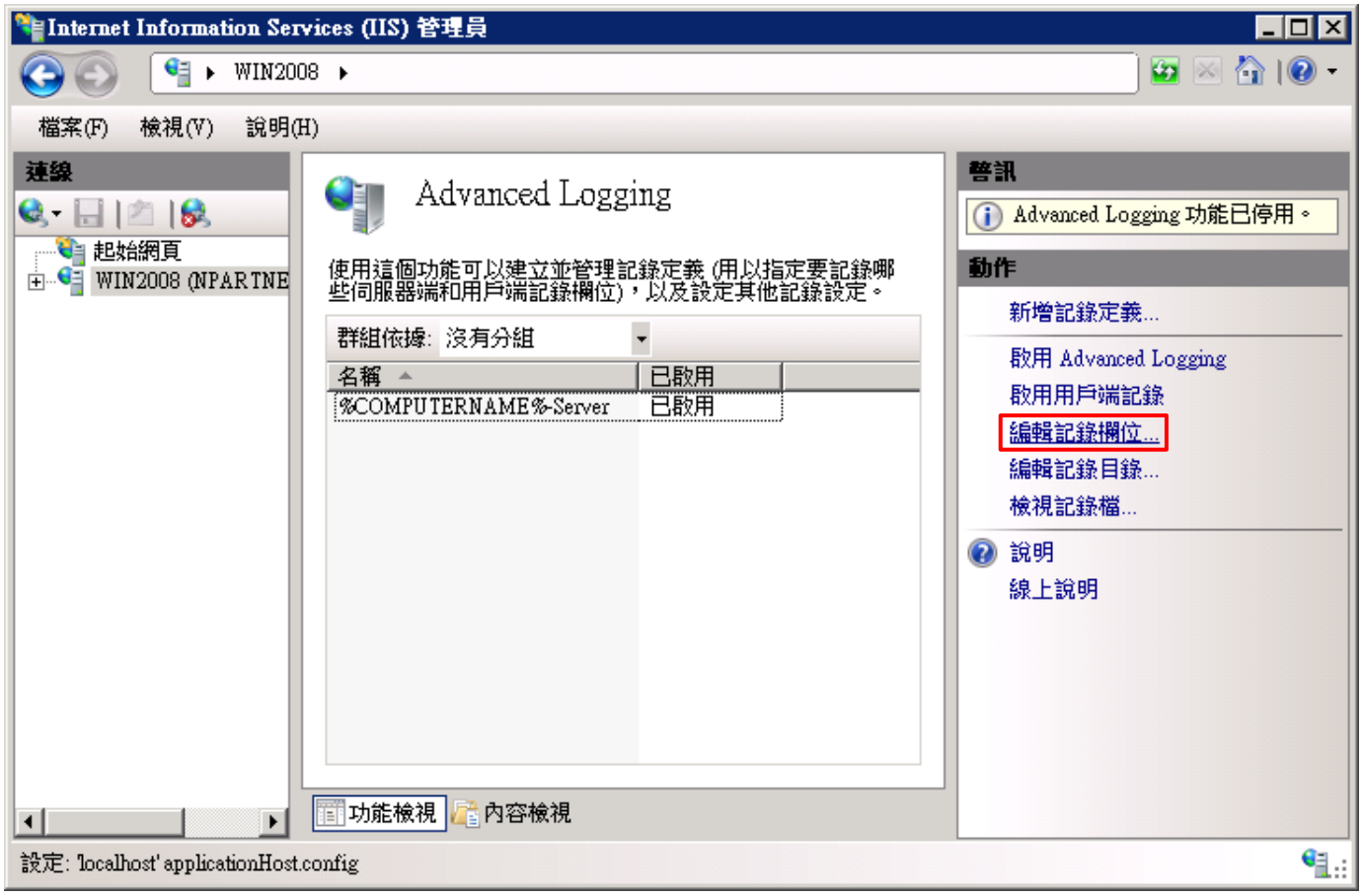
(5) 確認記錄已停用



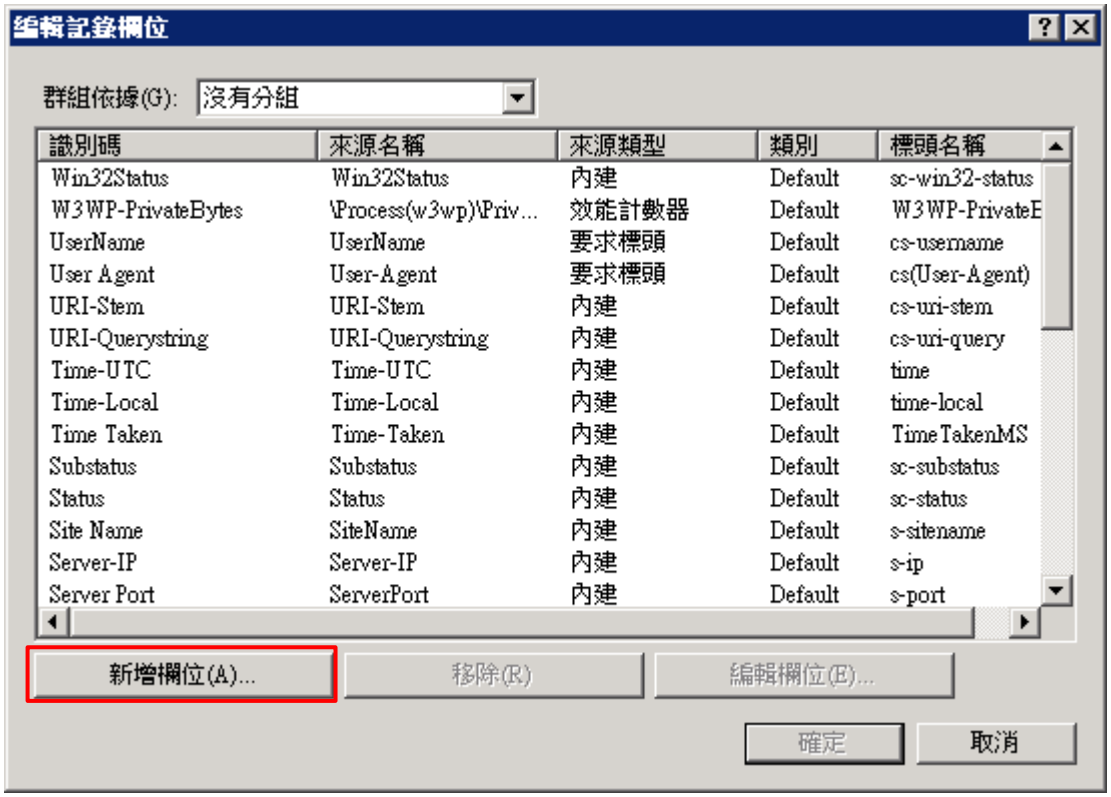
(6) 點選 [Advanced Logging]



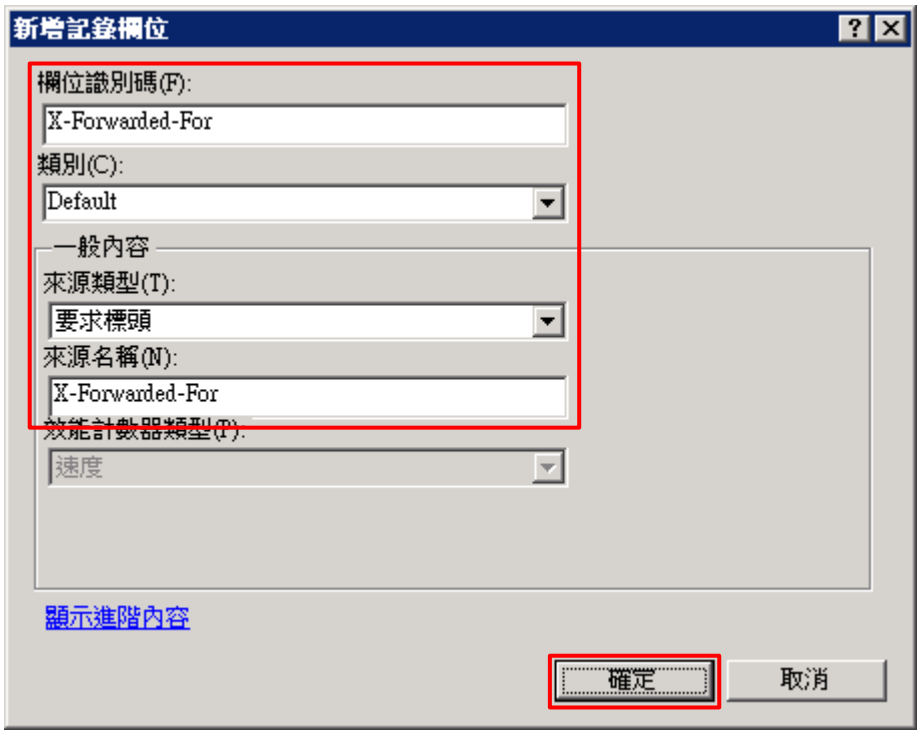
(7) 按 [編輯記錄欄位]



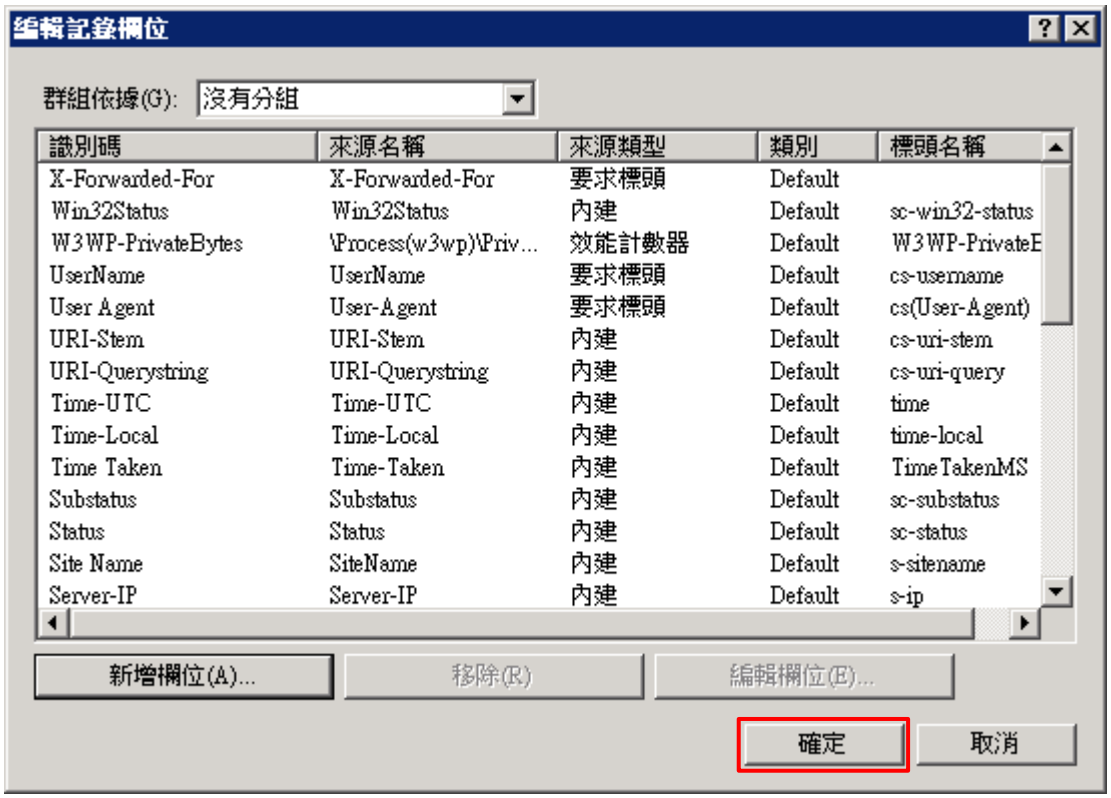
(8) 按 [新增欄位]



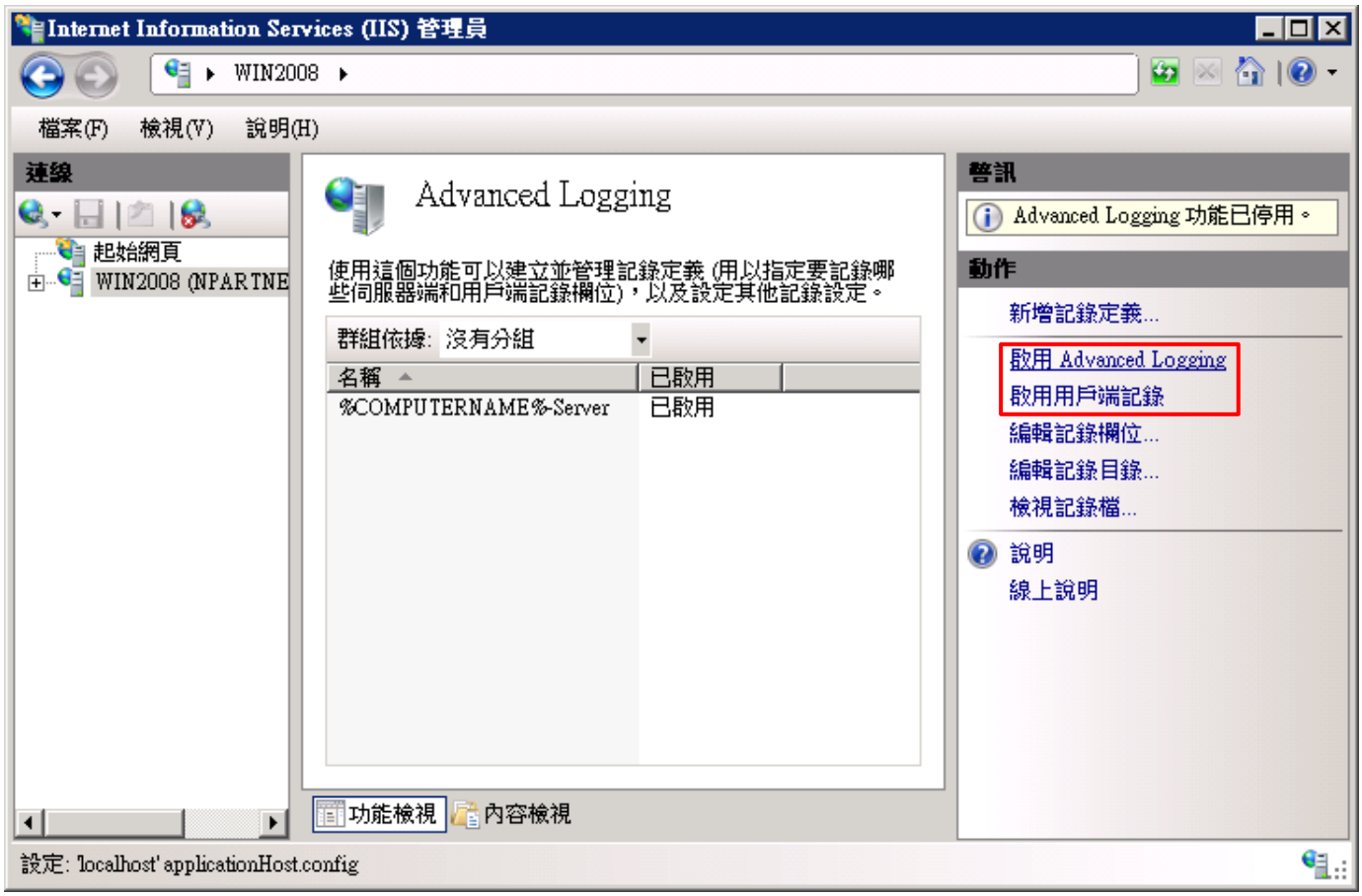
(9) 輸入欄位識別碼: X-Forwarded-For -> 選擇類別: [Default] -> 來源類型: [要求標頭] -> 輸入來源名稱: X-Forwarded-For -> 按 [確定]



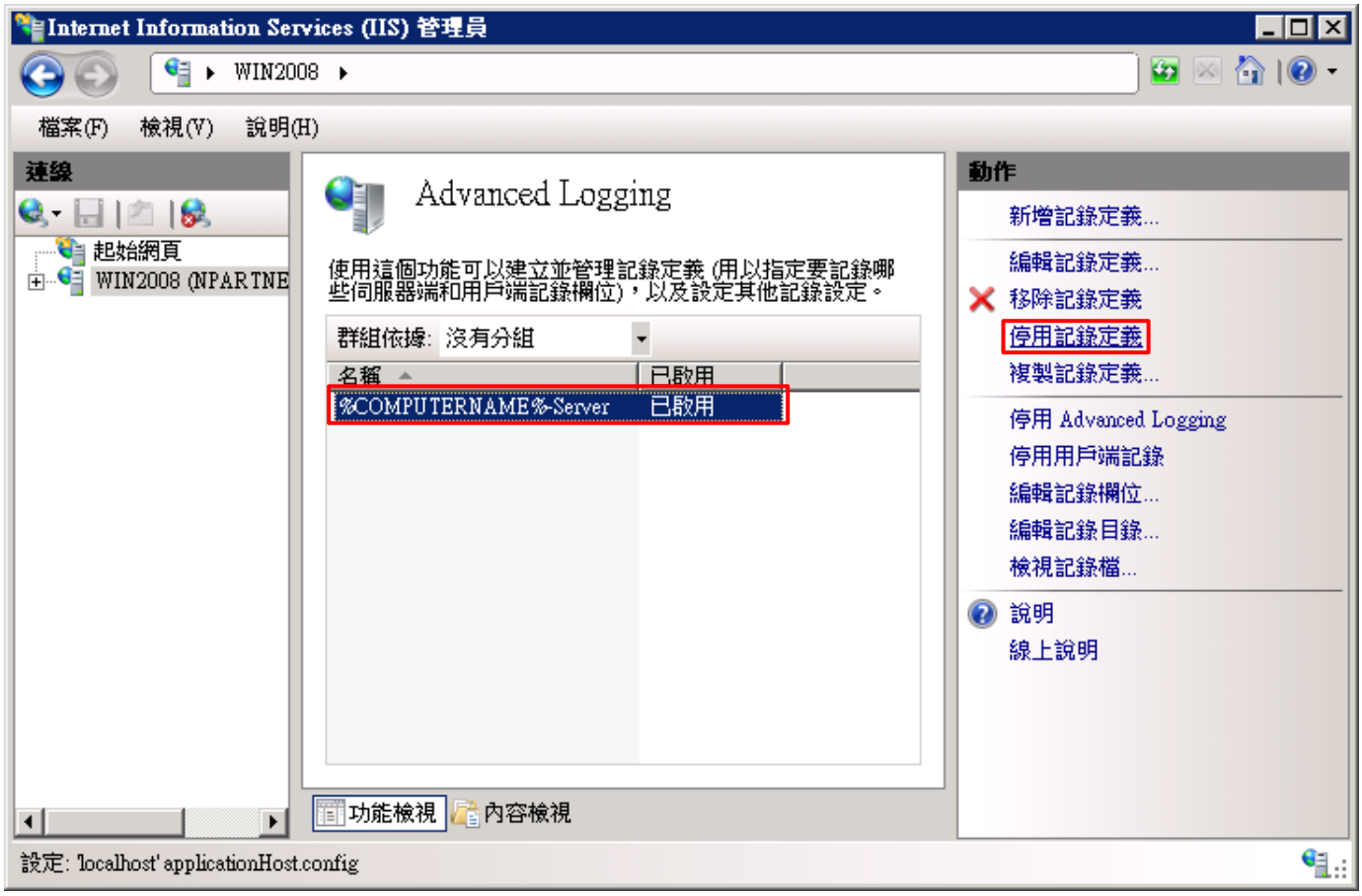
(10) 按 [確定]



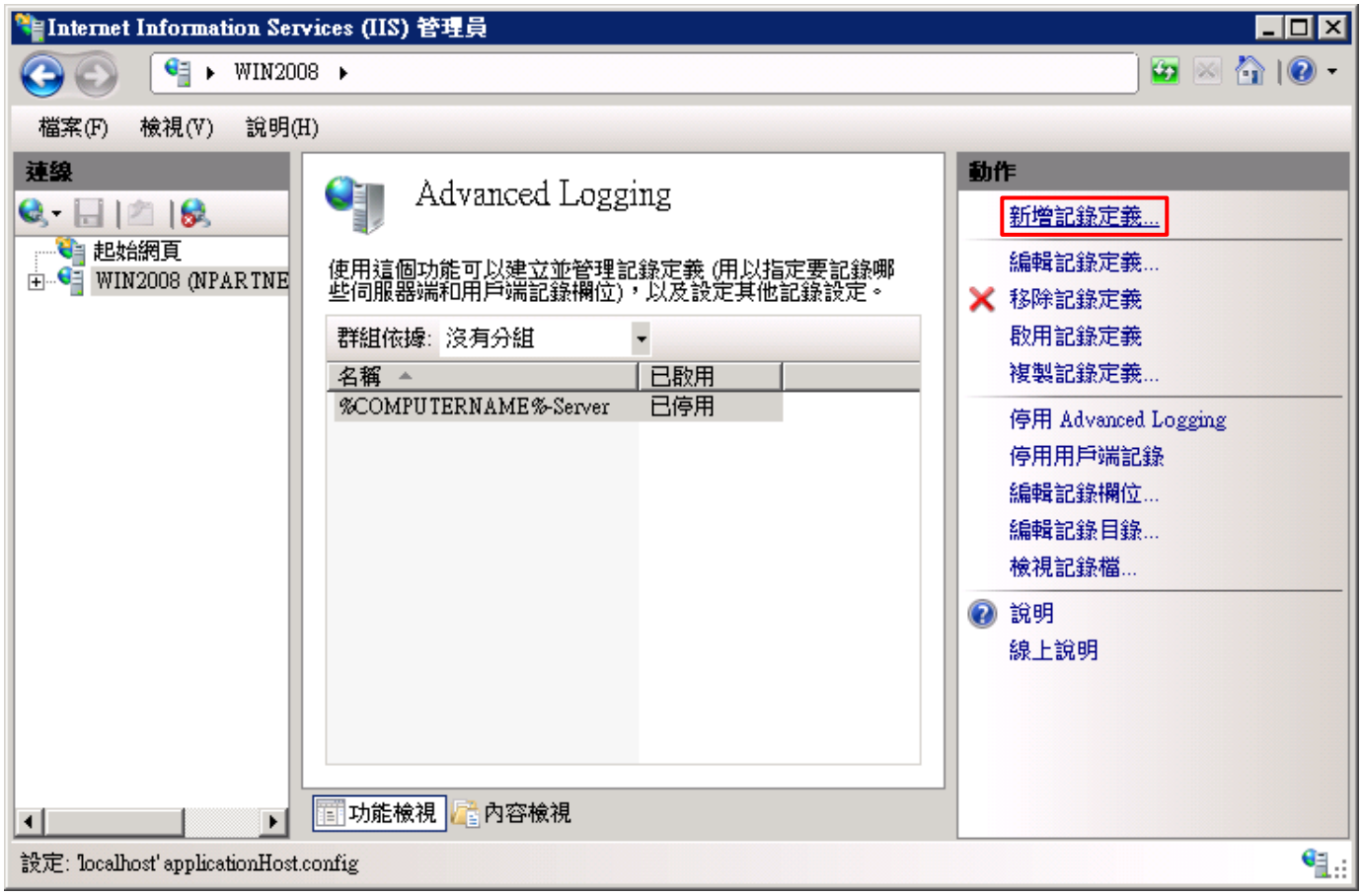
(11) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]



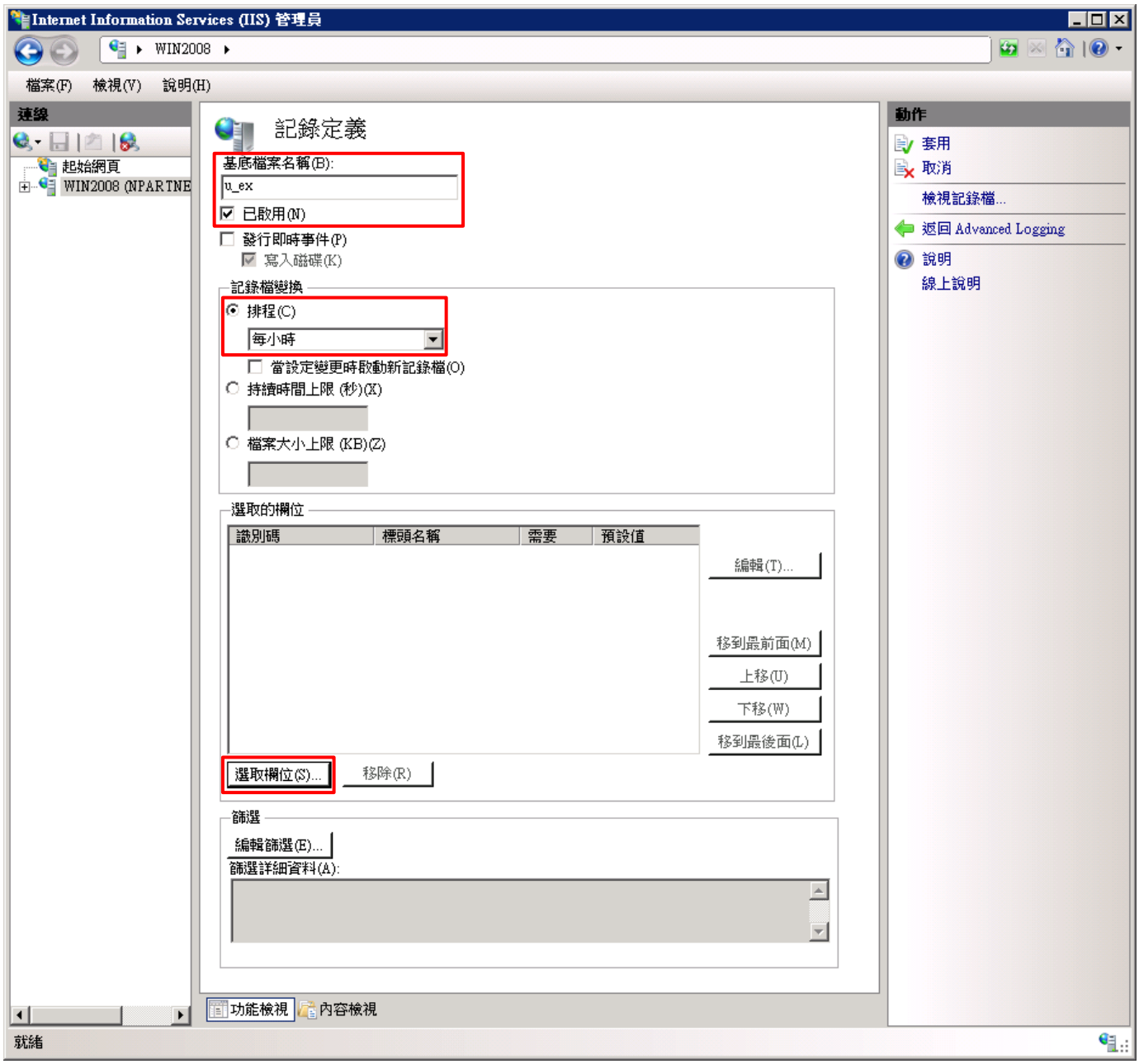
(12) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]



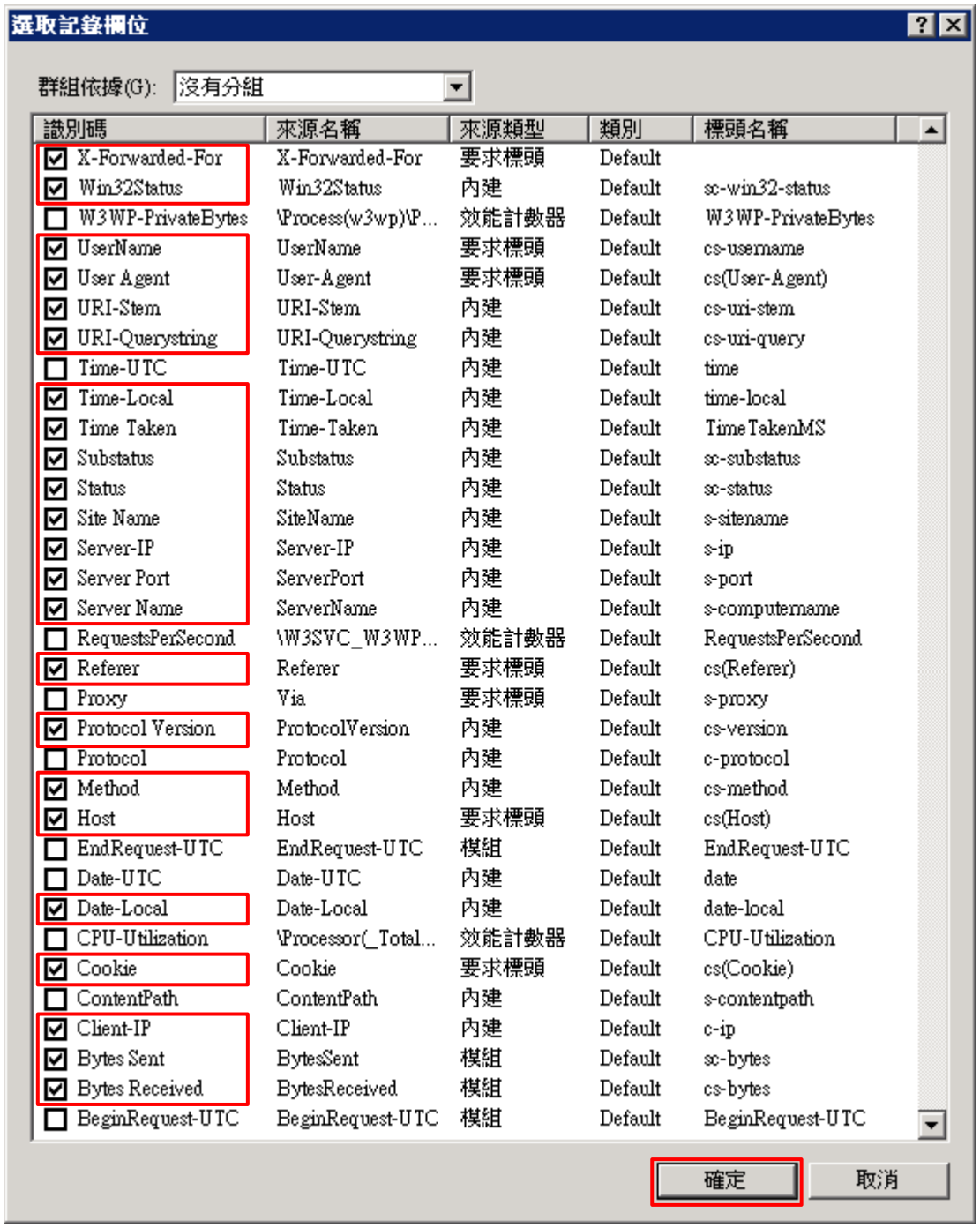
(13) 點選 [新增記錄定義]



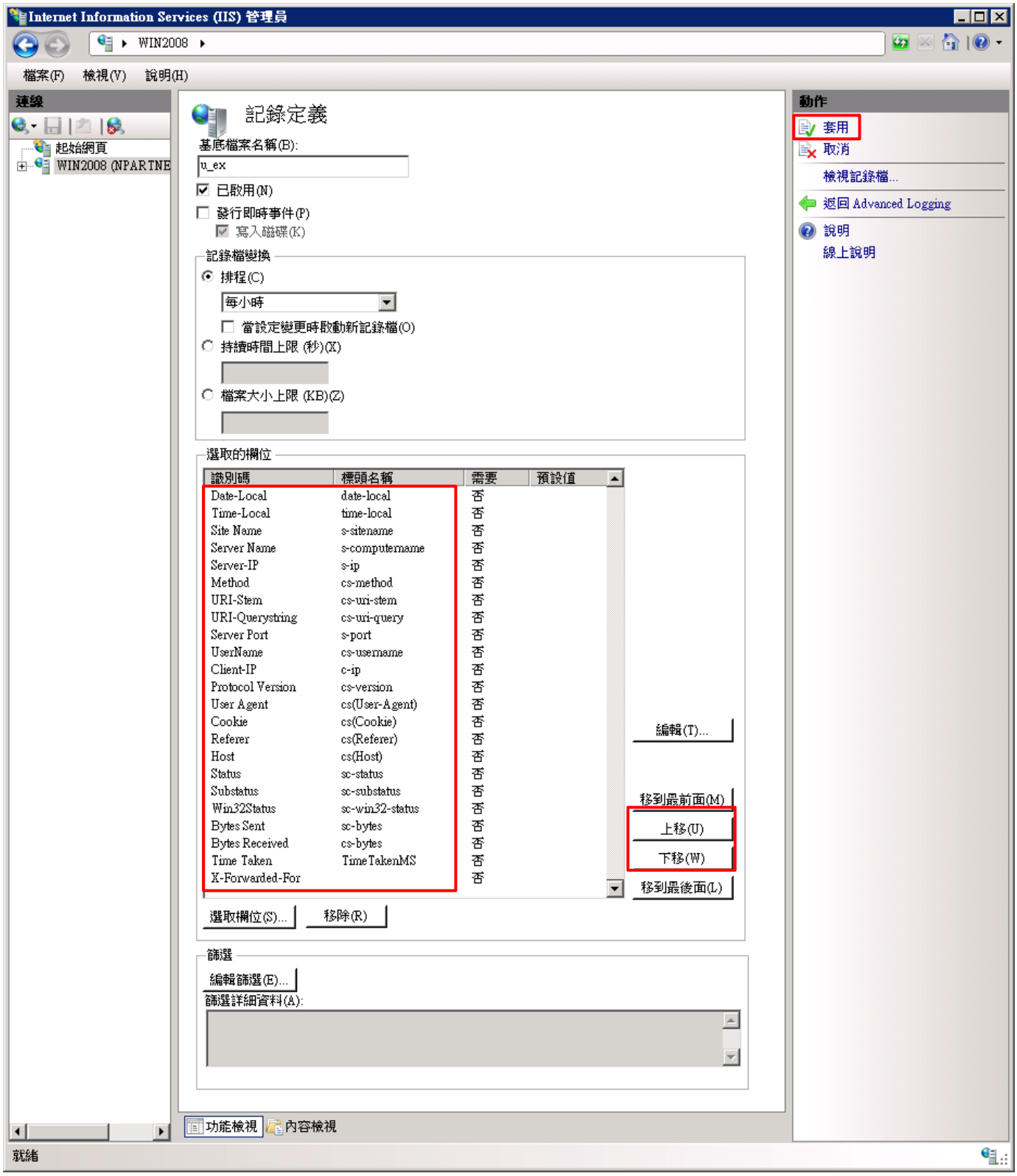
(14) 輸入基底檔案名稱: u_ex -> 勾選 [已啟用] -> 選擇排程: [每小時] -> 按 [選取欄位]



(15) 勾選 [X-Forwarded-For]、[Win32Status(sc-win32-status)]、[UserName(cs-username)]、[User Agent(cs(User-Agent))]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Time-Local(time-local)]、[Time Taken(TimeTakenMS)]、[Substatus(sc-substatus)]、[Status(sc-status)]、[Site Name(s-sitename)]、[Server-IP(s-ip)]、[Server Port(s-port)]、[Server Name(s-computername)]、[Referer(cs(Referer))]、[Protocol Version(cs-version)]、[Method(cs-method)]、[Host(cs(Host))]、[Date-Local(date-local)]、[Cookie(cs(Cookie))]、[Client-IP (c-ip)]、[Byte Sent(sc-bytes)]、[Bytes Received(cs-bytes)] -> 按 [確定]

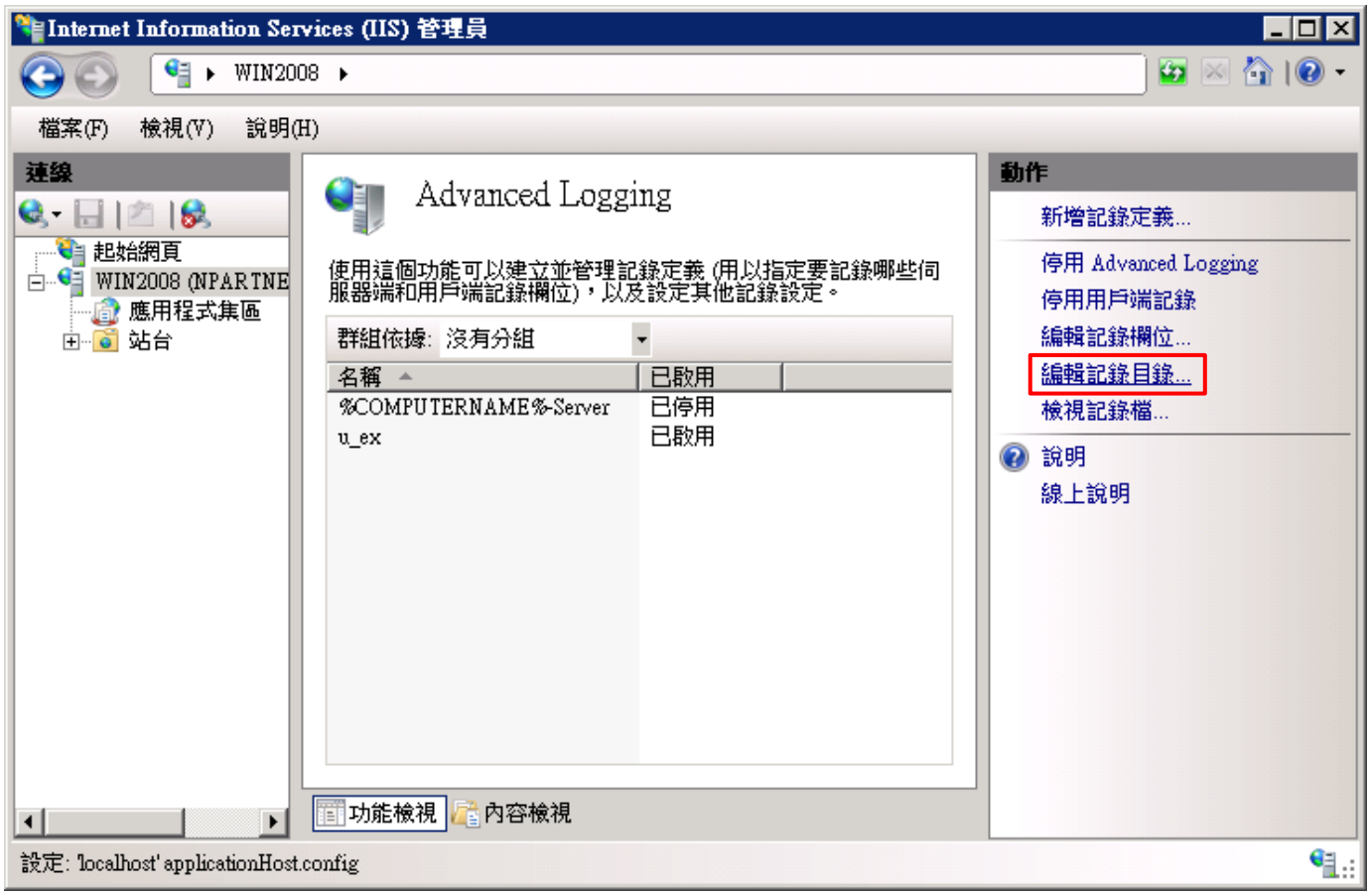


(16) 調整選取的欄位: [Date-Local(date-local)]、[Time-Local(time-local)]、[Site Name(s-sitename)]、[Server Name(s-computername)]、[Server-IP(s-ip)]、[Method(cs-method)]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Server Port(s-port)]、[UserName(cs-username)]、[Client-IP(c-ip)]、[Protocol Version(cs-version)]、[User Agent(cs(User-Agent))]、[Cookie(cs(Cookie))]、[Referer(cs(Referer))]、[Host(cs(Host))]、[Status(sc-status)]、[Substatus(sc-substatus)]、[Win32Status(sc-win32-status)]、[Bytes Send(sc-bytes)]、[Bytes Received(cs-bytes)]、[Time Taken(TimeTakenMS)]、[X-Forwarded-For] -> 按 [上移] 或 [下移] -> 按 [套用]

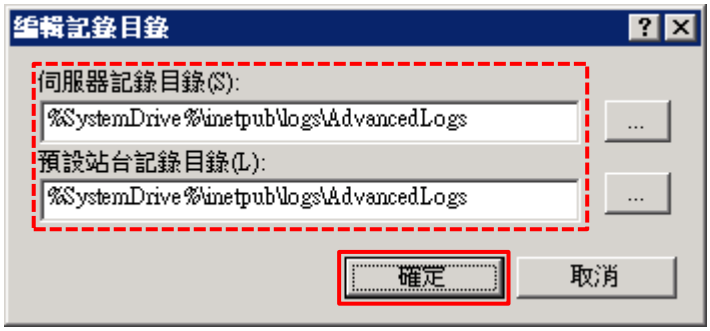


(17) 點選 [返回 Advanced Logging]

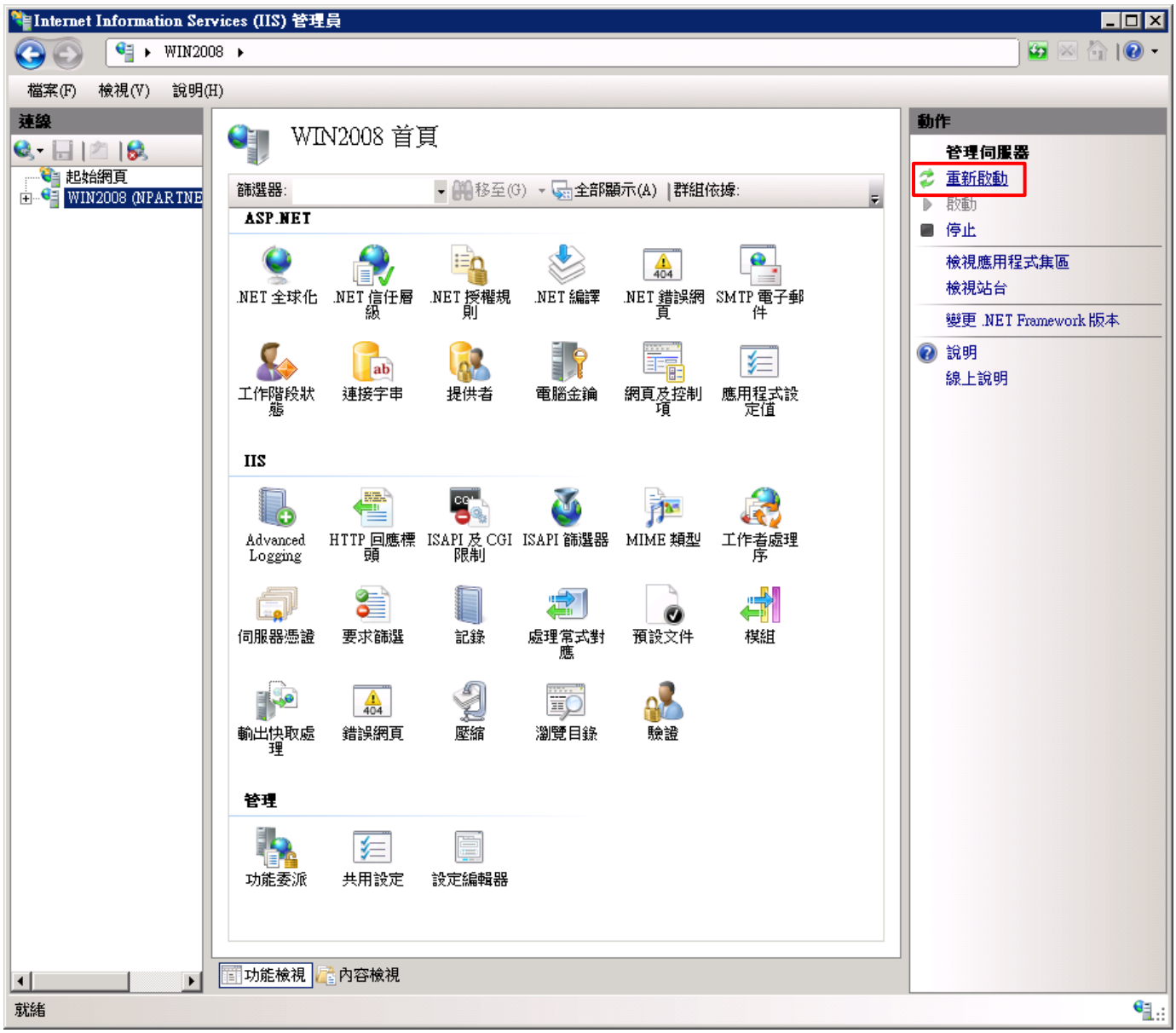
(18) 點選 [編輯記錄目錄]



(19) 確認 [伺服器記錄目錄] 和 [預設站台記錄目錄] 資料夾路徑 -> 按 [確定]



(20) 點選 [重新啟動] IIS 服務



(21) 確認 [C:\inetpub\logs\AdvancedLogs] 資料夾 IIS log 檔案: u_ex*.log

3.3 Event Log

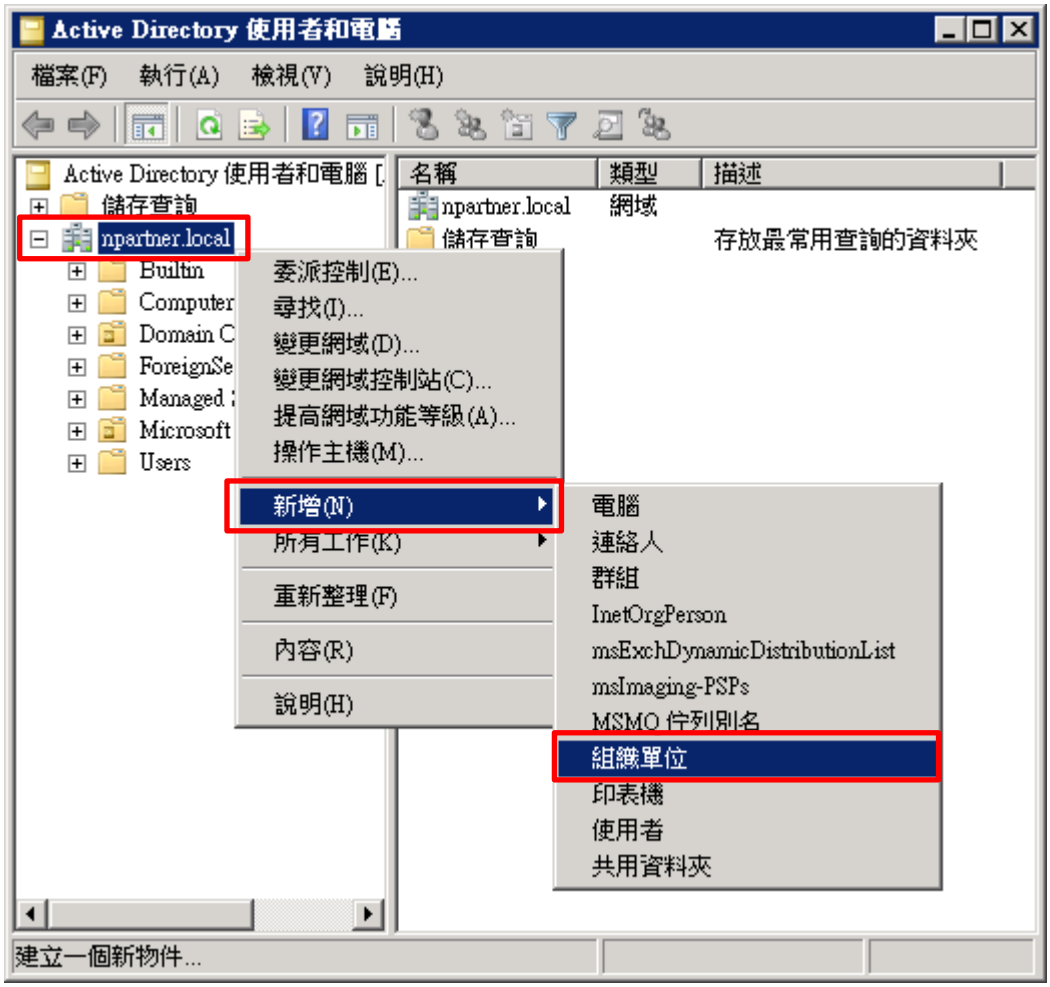
3.3.1 組織單位

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

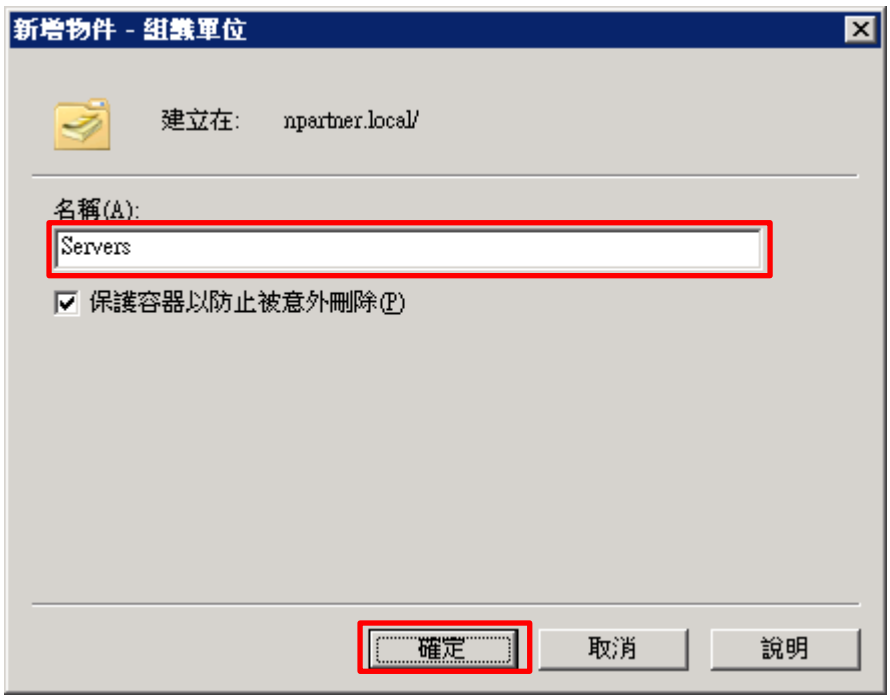
(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



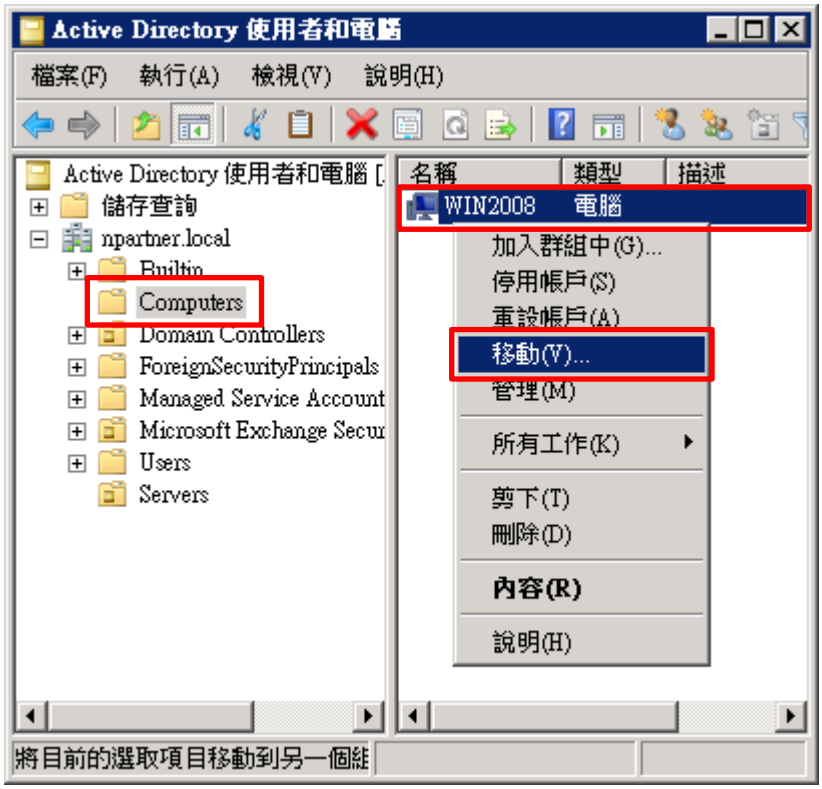
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



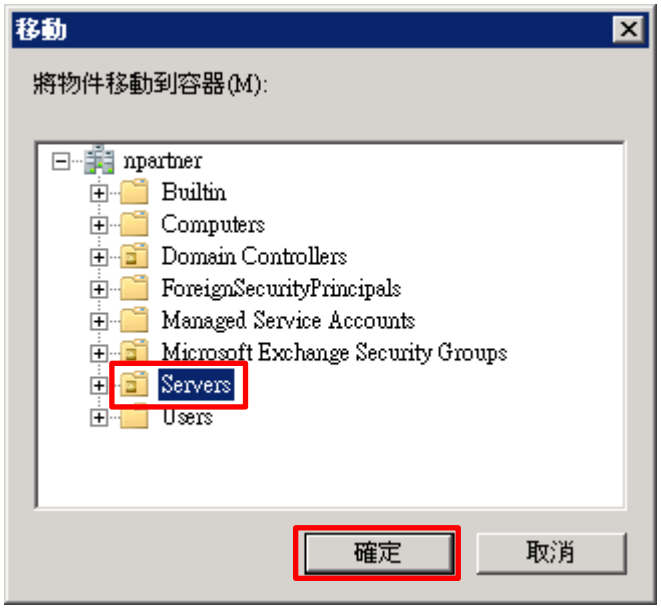
(4) 移動 Exchange 伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2008] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Exchange Server 主機 -> 點選 [移動]



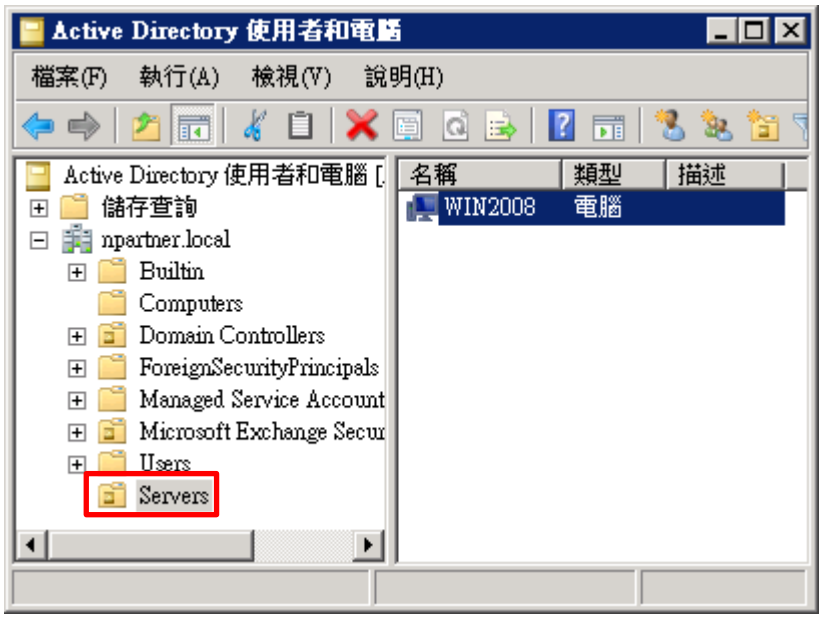
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認 Exchange 伺服器已移動至新的組織單位

點選 [Servers] 組織單位，確認 Win2008 伺服器已移動。



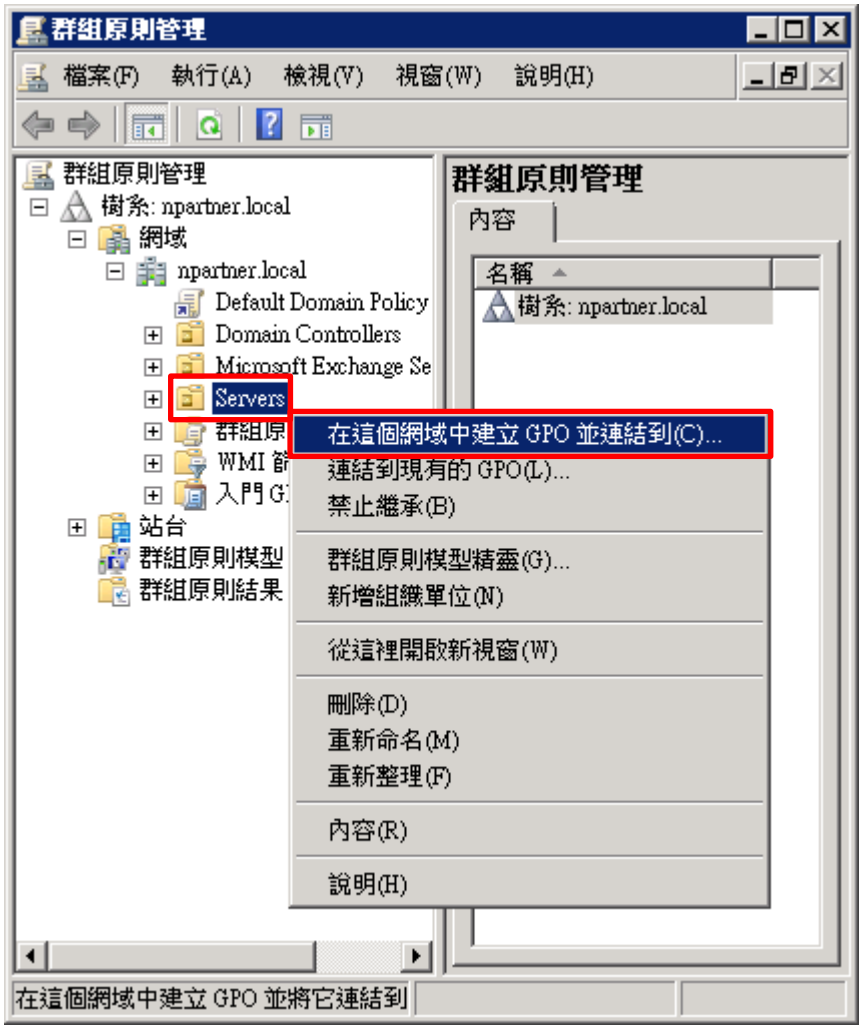
3.3.2 群組原則

(1) 開啟群組原則管理

開啟 [群組原則管理]

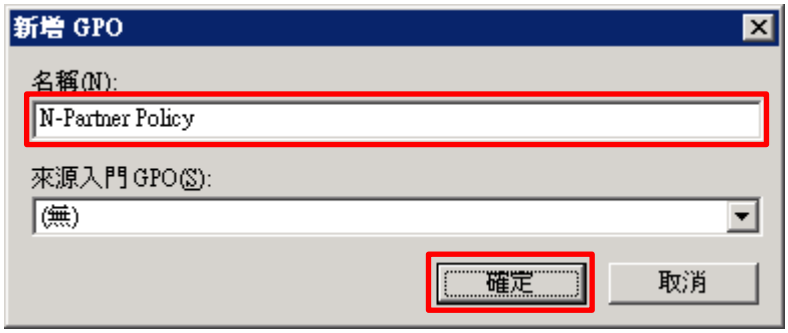
(2) 在 Servers 組織單位，新增群組原則物件

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



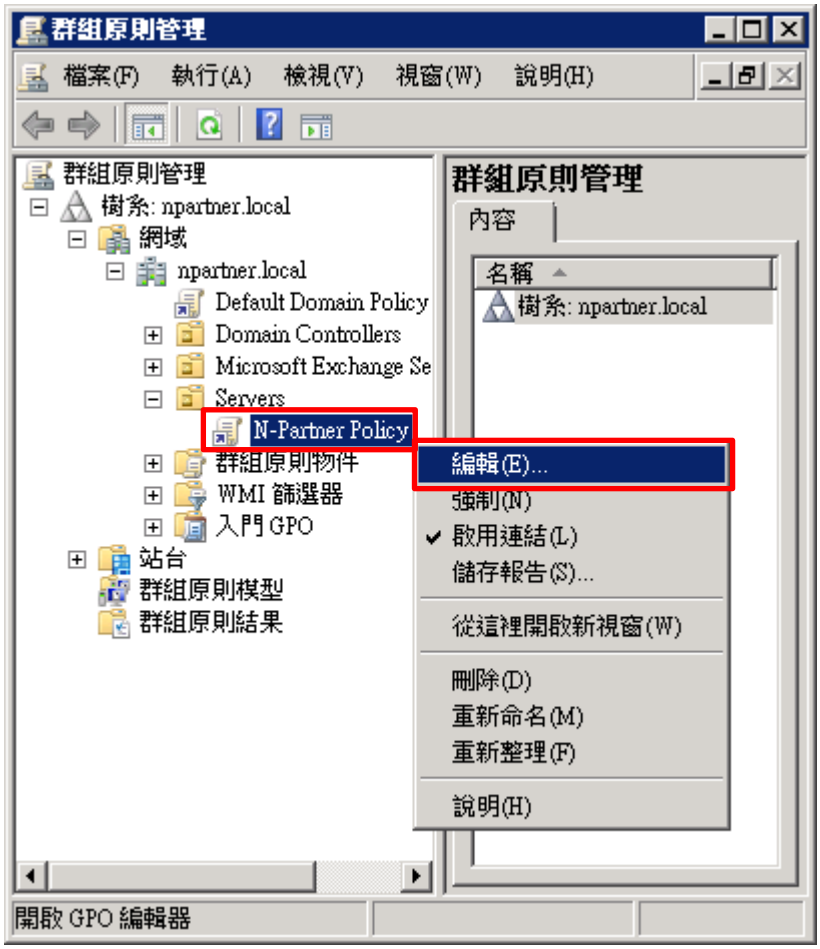
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]



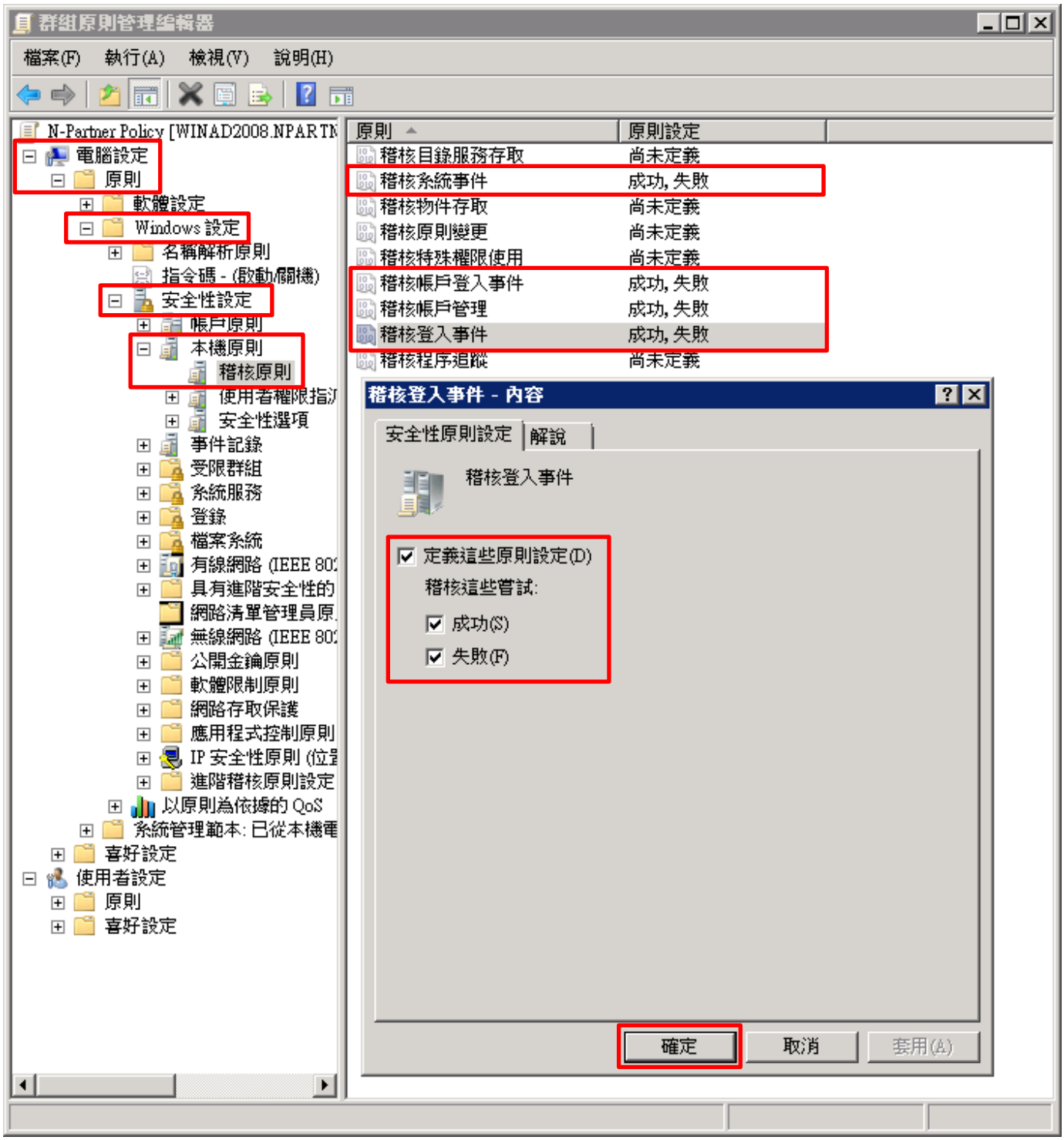
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



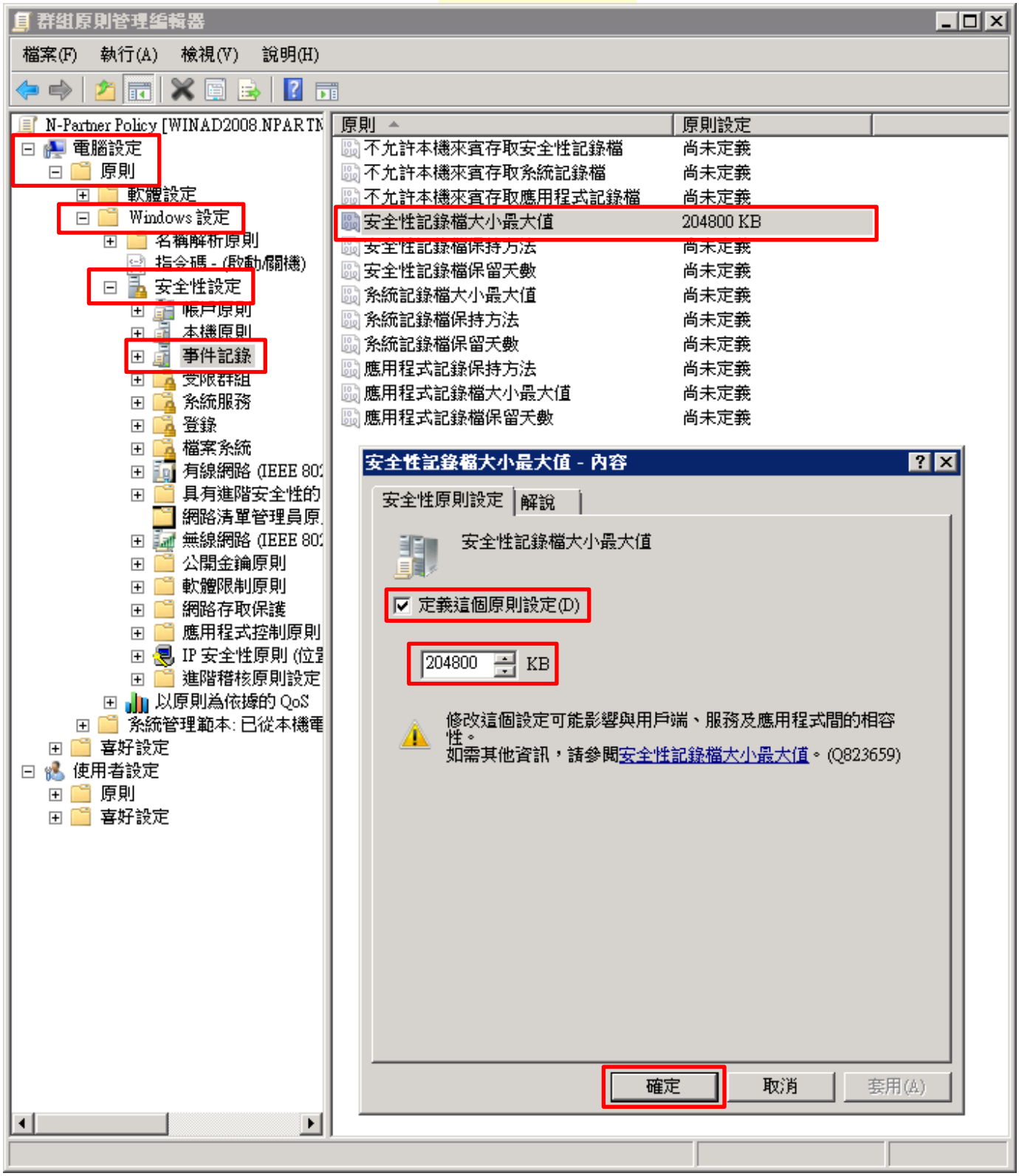
(5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



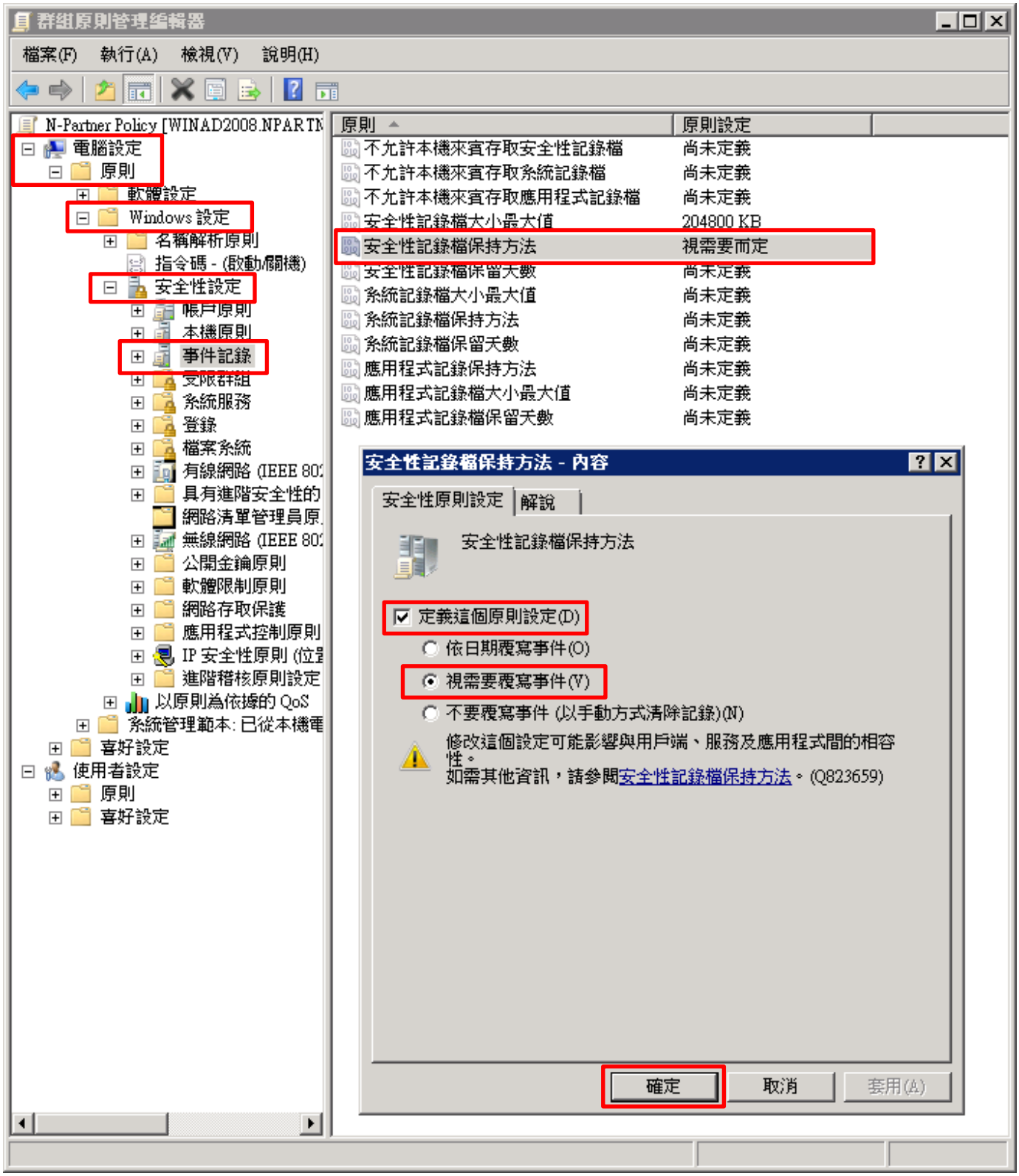
(6) 事件記錄：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(7) 事件記錄：安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 在 Exchange 伺服器 -> 開啟 [Windows PowerShell]

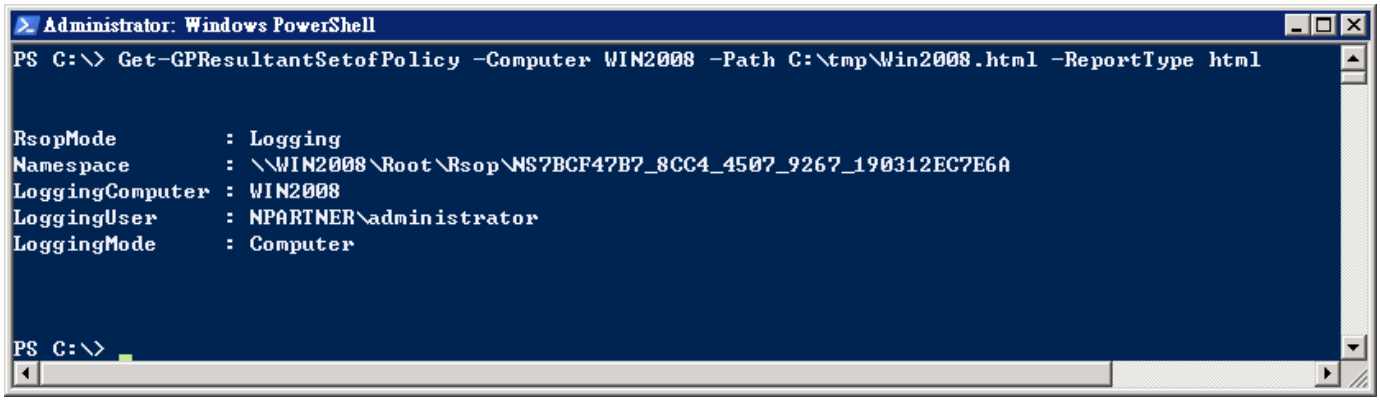
(9) 更新群組原則

```
PS C:\> gpupdate /force
```

(10) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]，

(11) 產生 Exchange 伺服器群組原則報表。

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008 -Path C:\tmp\Win2008.html -ReportType html
```



紅色文字部位請輸入 Windows Server 伺服器名稱和資料夾路徑檔案名稱

(12) 開啟報表 -> 確認 Exchange 伺服器 -> 套用 N-Partner Policy 群組原則

4. Exchange 2013

範例：Exchange 2013 安裝在 Windows 2012 伺服器。

可選擇 [Exchange Administrative Center] 或 [Exchange Management Shell] 確認啟用郵件追蹤記錄。

4.1 Exchange Message Tracking Log

修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

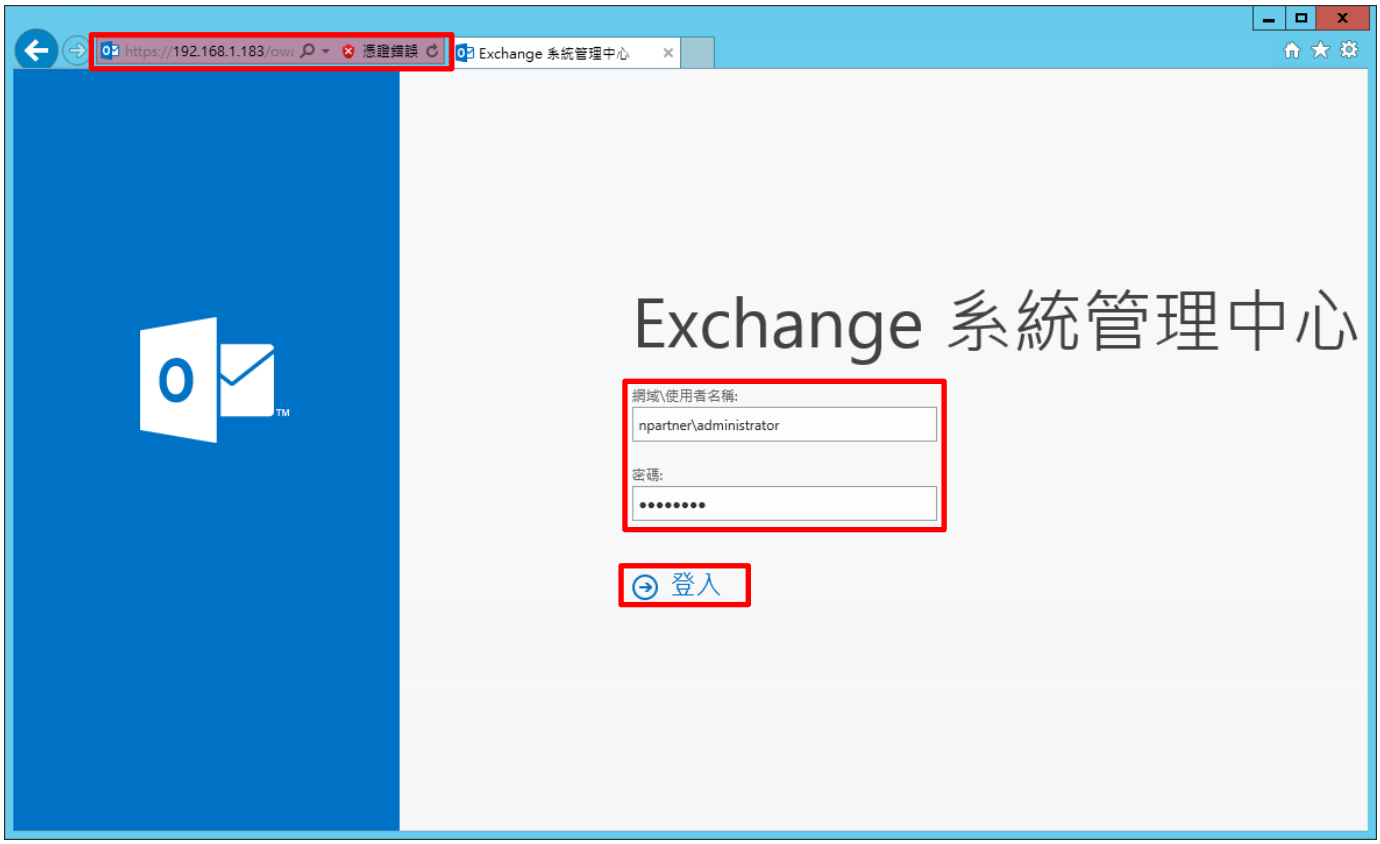
藍色文字部位請修改郵件追蹤記錄資料夾

```
define MailLog     C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

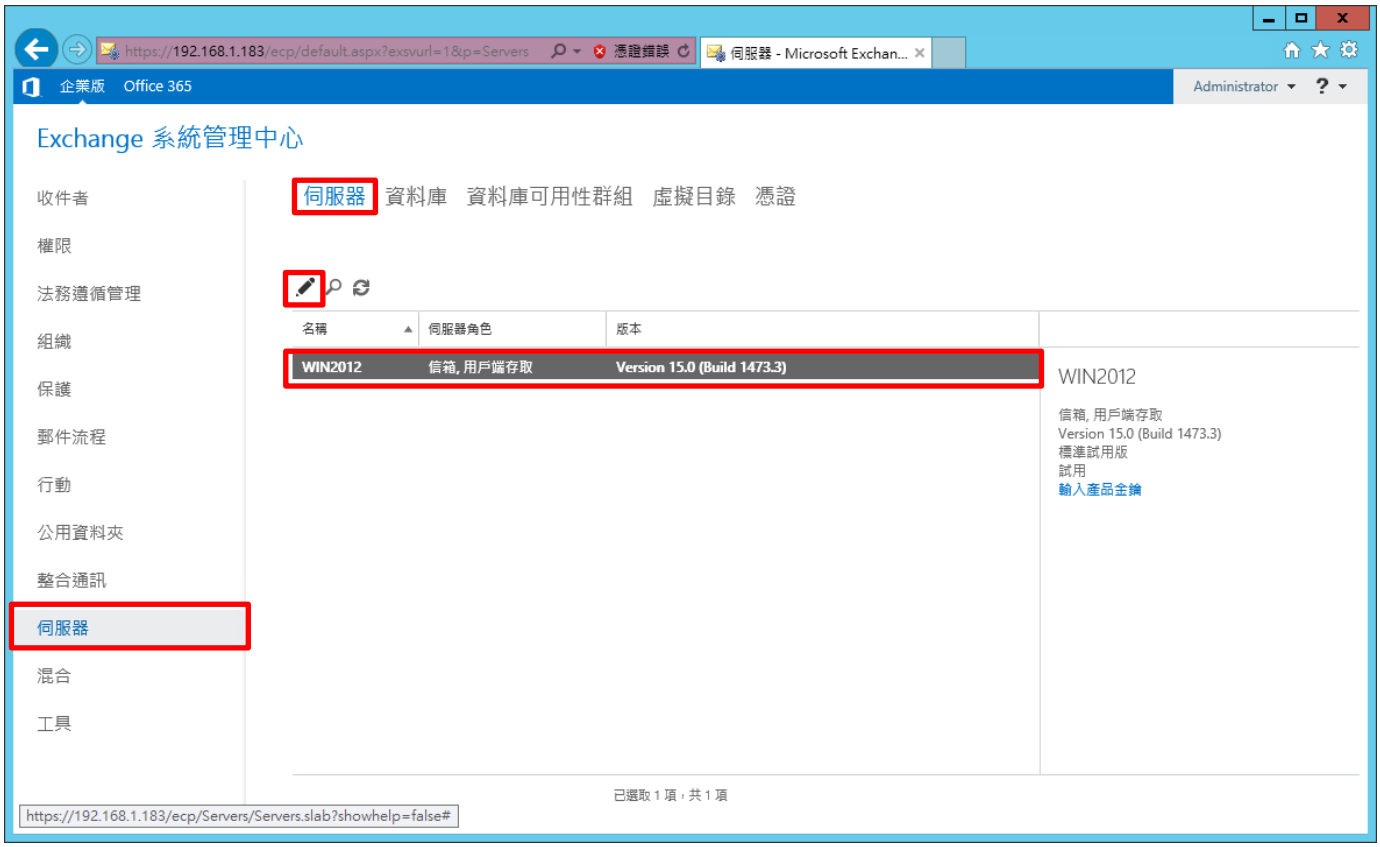
4.1.1 Exchange Administrative Center

(1) 開啟 [瀏覽器]

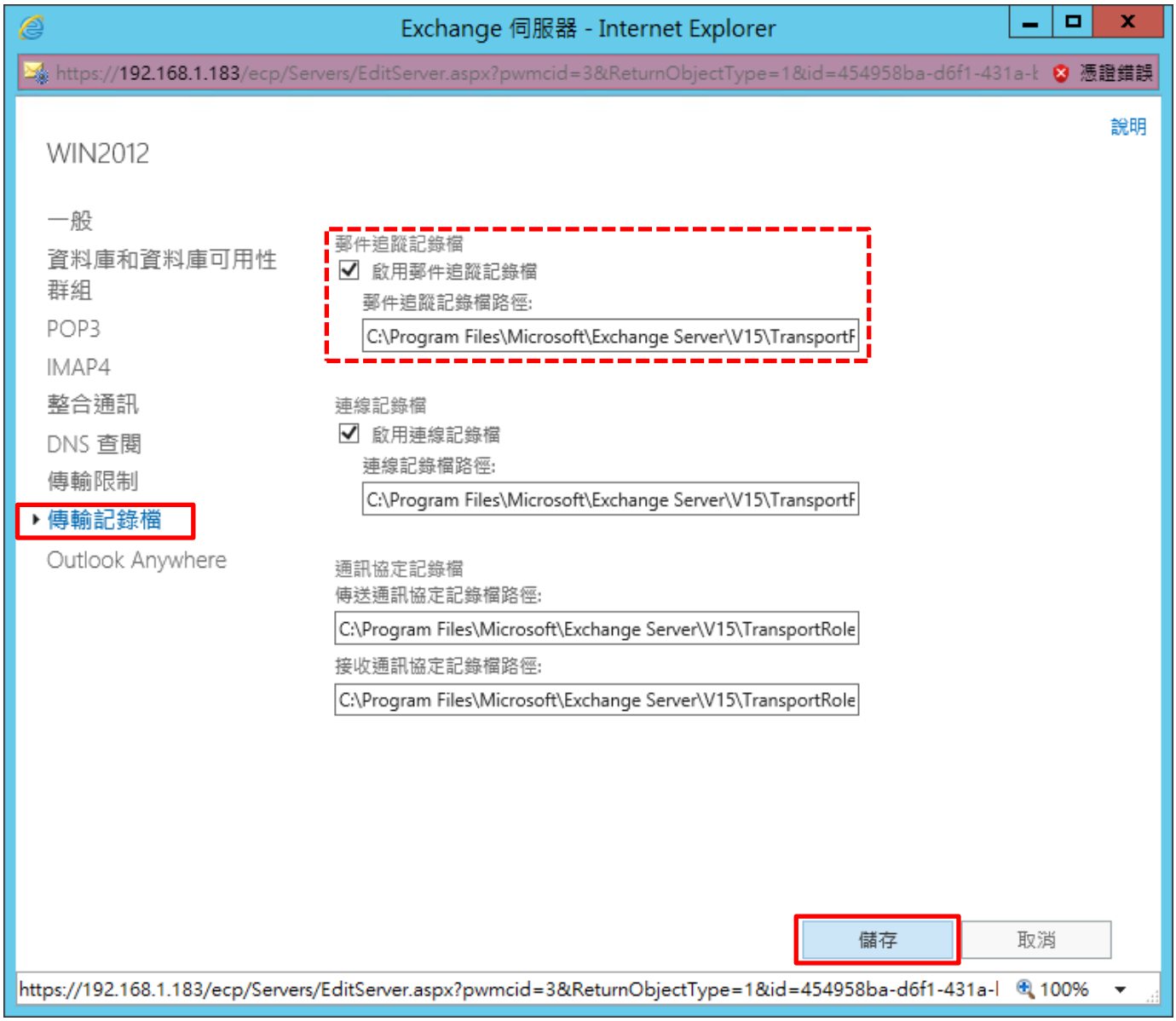
(2) URL 輸入 https://<*ExchangeIP*>/ecp ->輸入網域名稱\管理者帳號和密碼 -> 按下 [登入]



(3) 點選 [伺服器] 頁面 -> [伺服器] -> 選擇 [Mailbox 伺服器(WIN2012)] -> 點選 (編輯)



(4) 點選 [傳輸記錄檔] -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking] -> 按下 [儲存]



4.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]

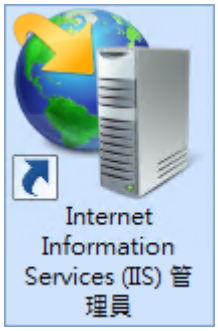
(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]

[PS] C:\> Get-TransportService win2012 | Select-Object *Track*

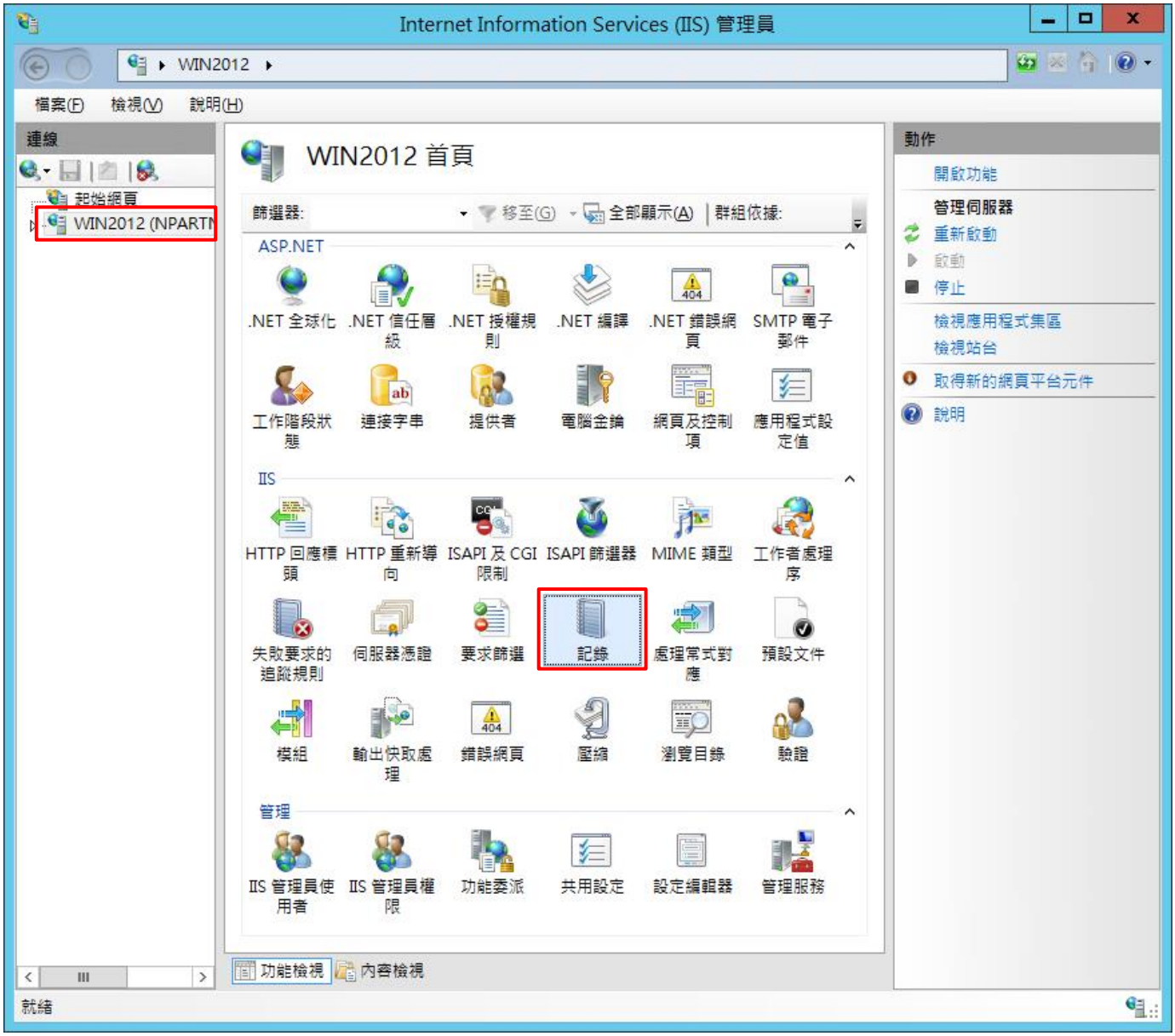
紅色文字部位請輸入 Exchange 伺服器名稱

4.2 IIS Log

(1) 開啟 [Internet Information Services (IIS) 管理員]

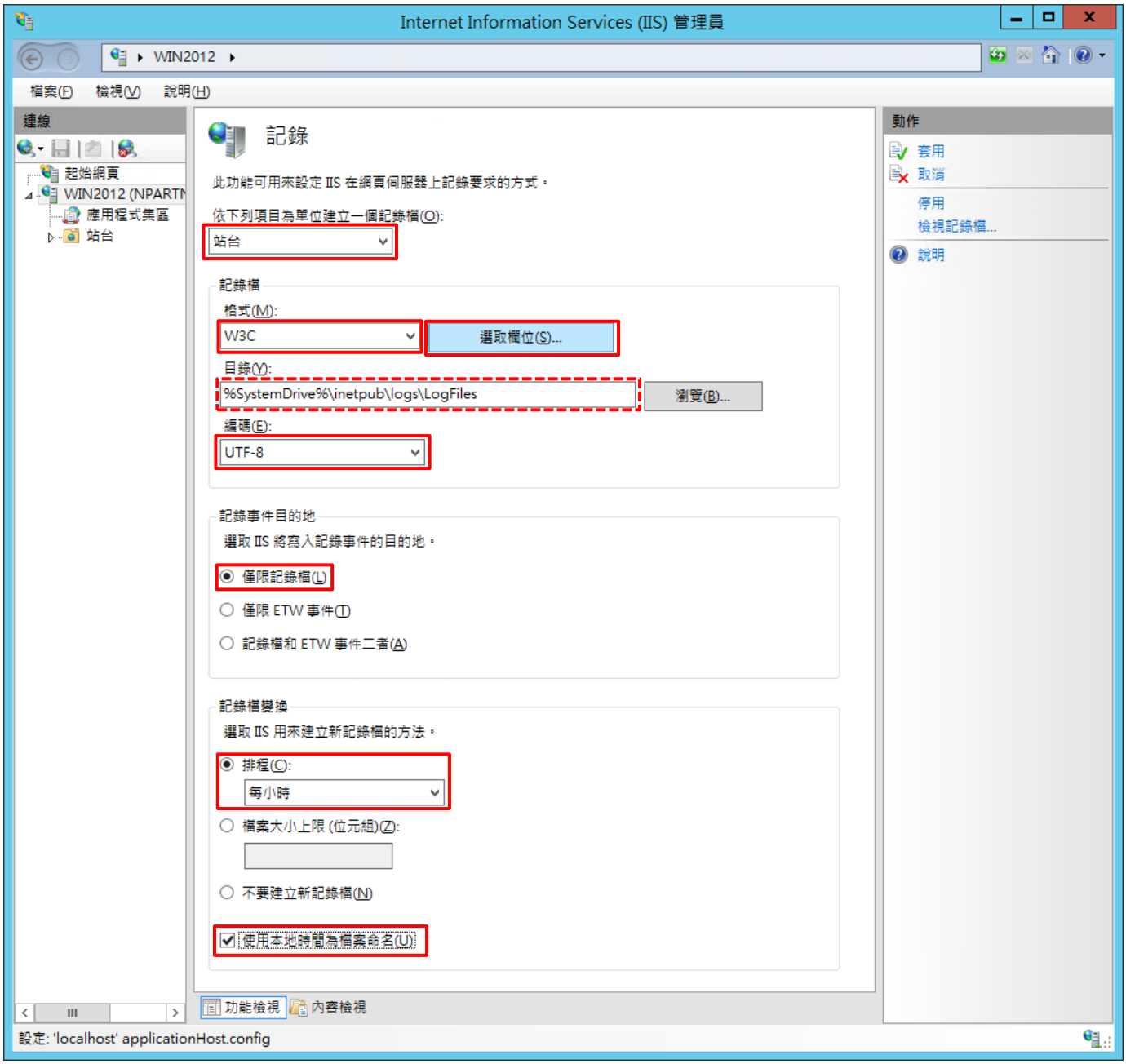


(2) 選擇 [IIS 伺服器] -> 點選 [記錄]

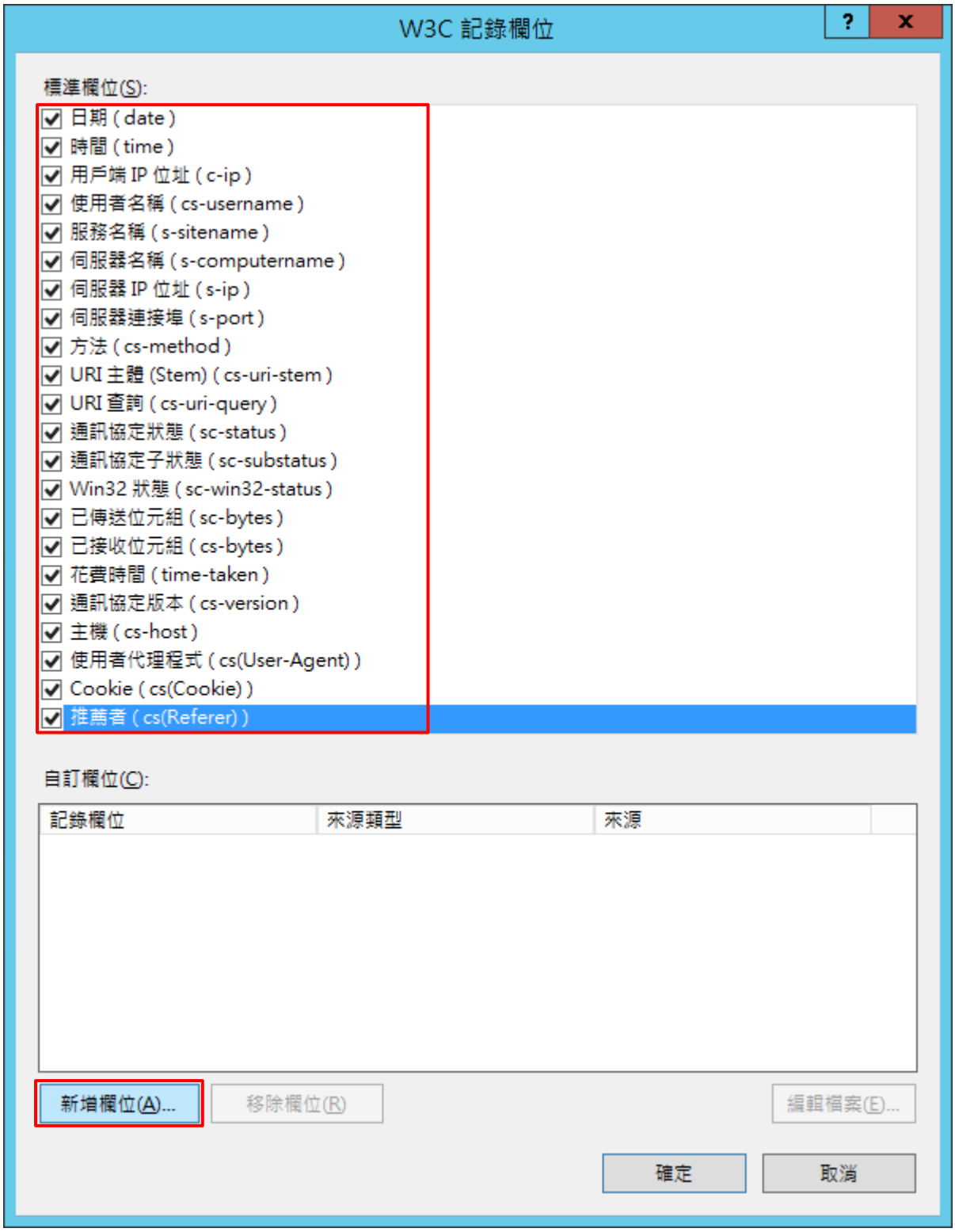


(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

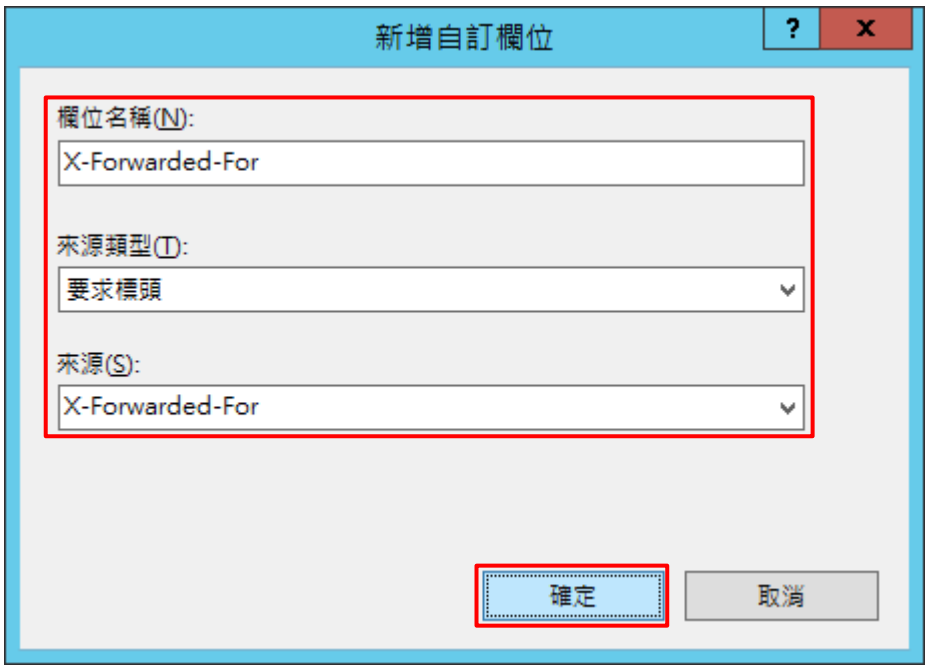
[%SystemDrive%\inetpub\logs\LogFiles] -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取檔位]



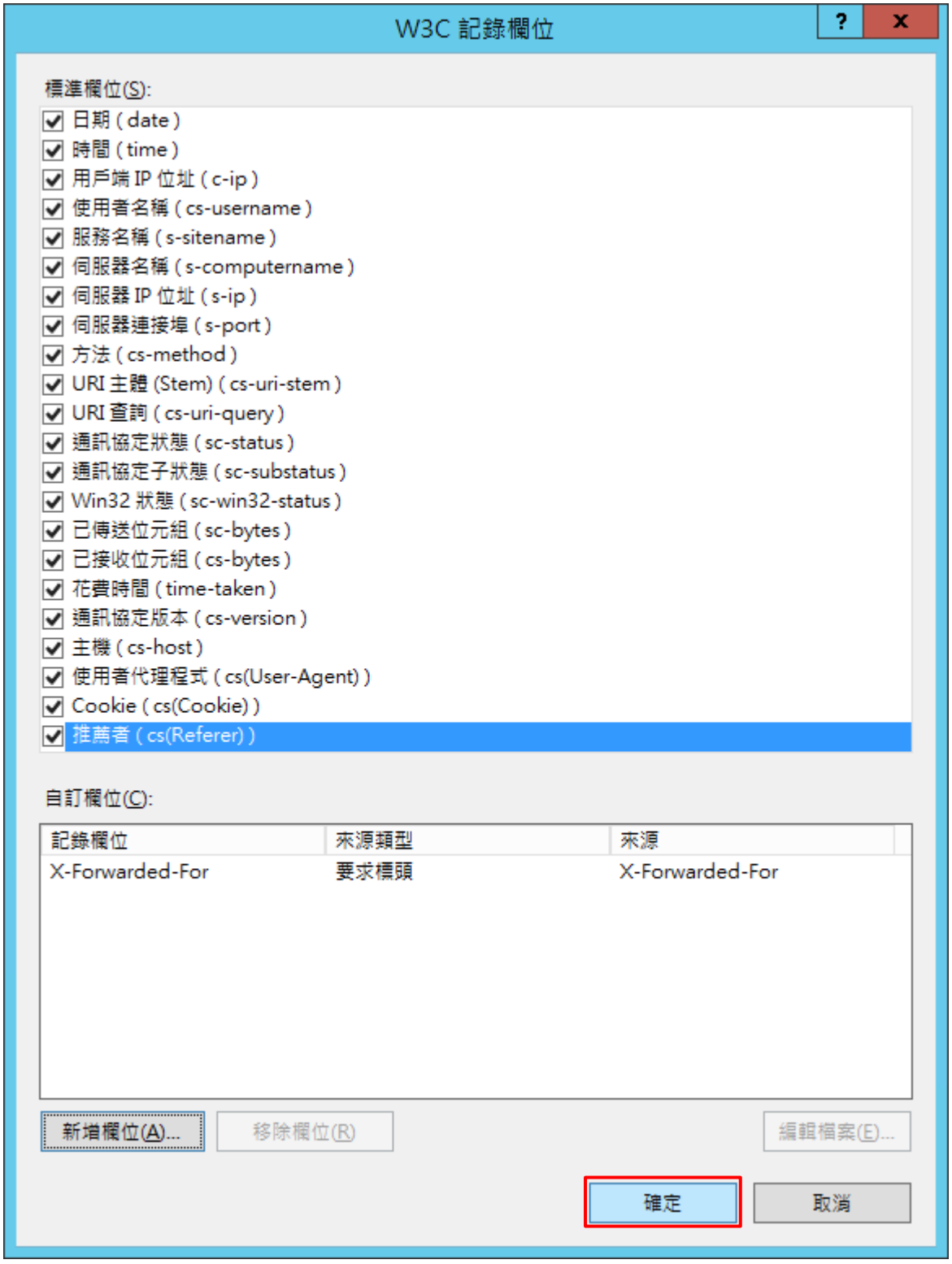
(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按 [新增欄位]



(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [要求標頭] -> 輸入來源: X-Forwarded-For -> 按 [確定]

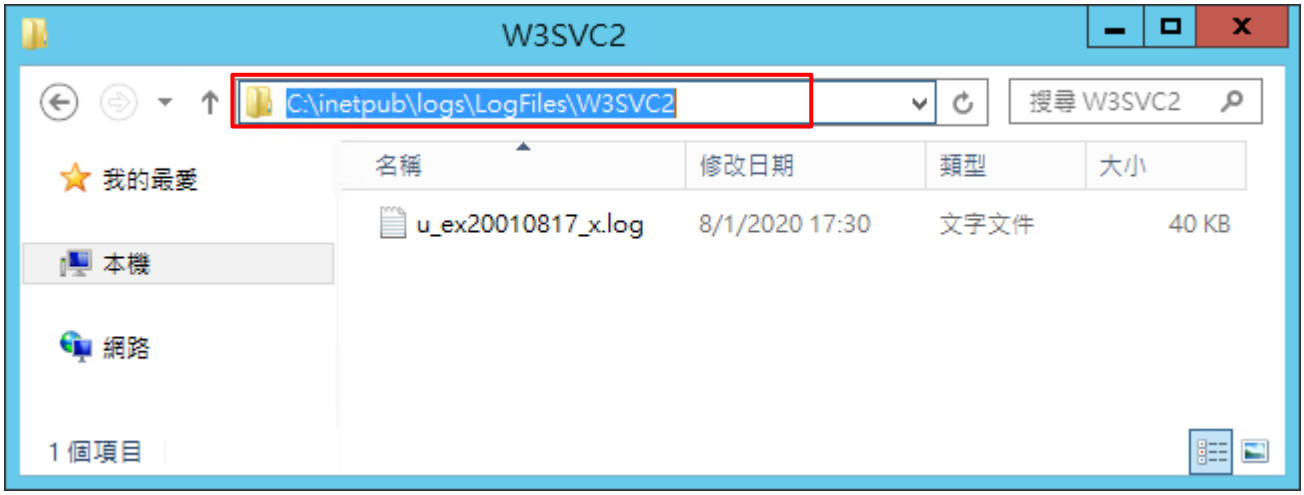


(6) 按 [確定]



(7) 按 [套用]

(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC2] 資料夾 IIS log 檔案: u_ex*.log



4.3 Event Log

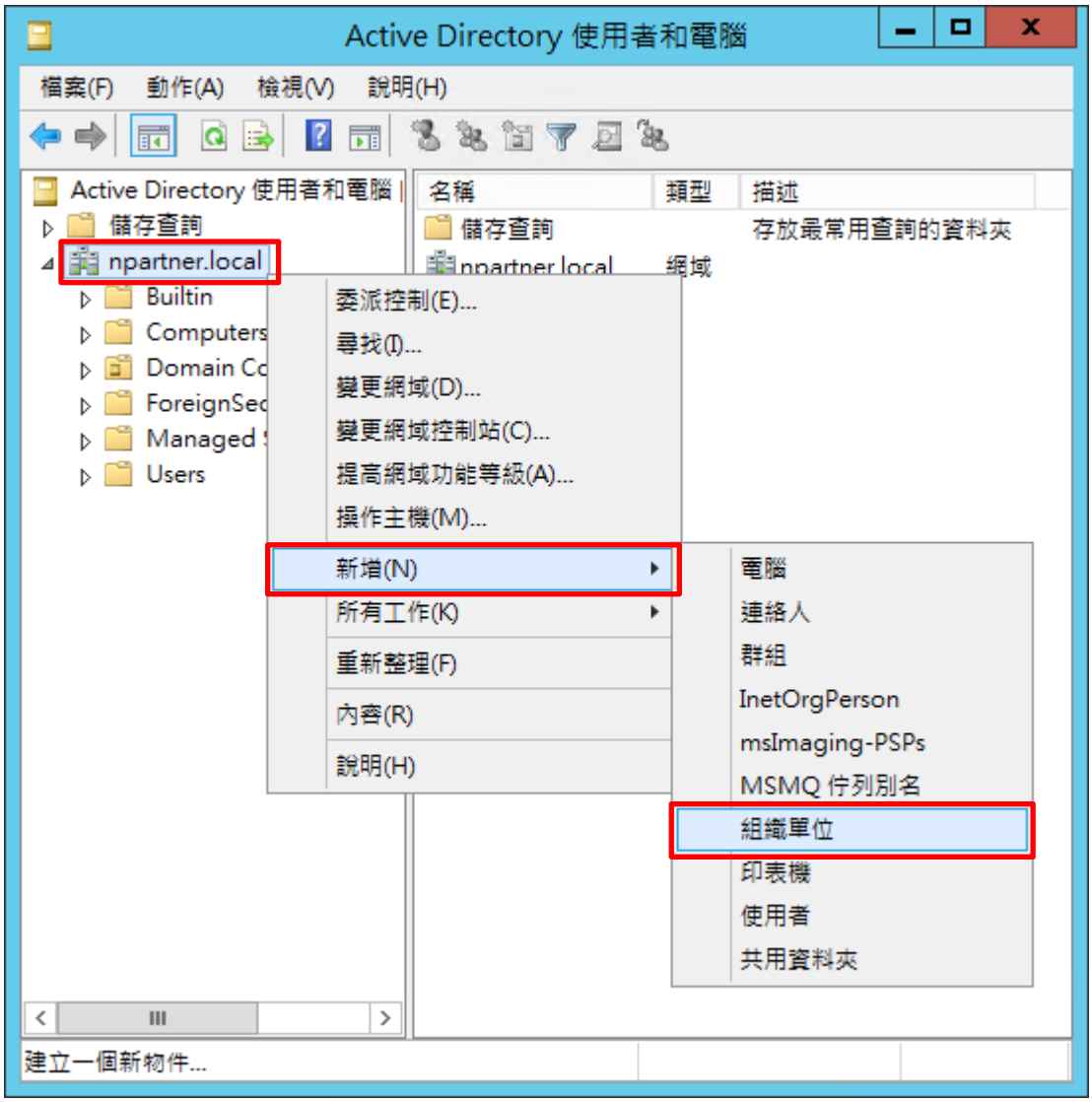
4.3.1 組織單位

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

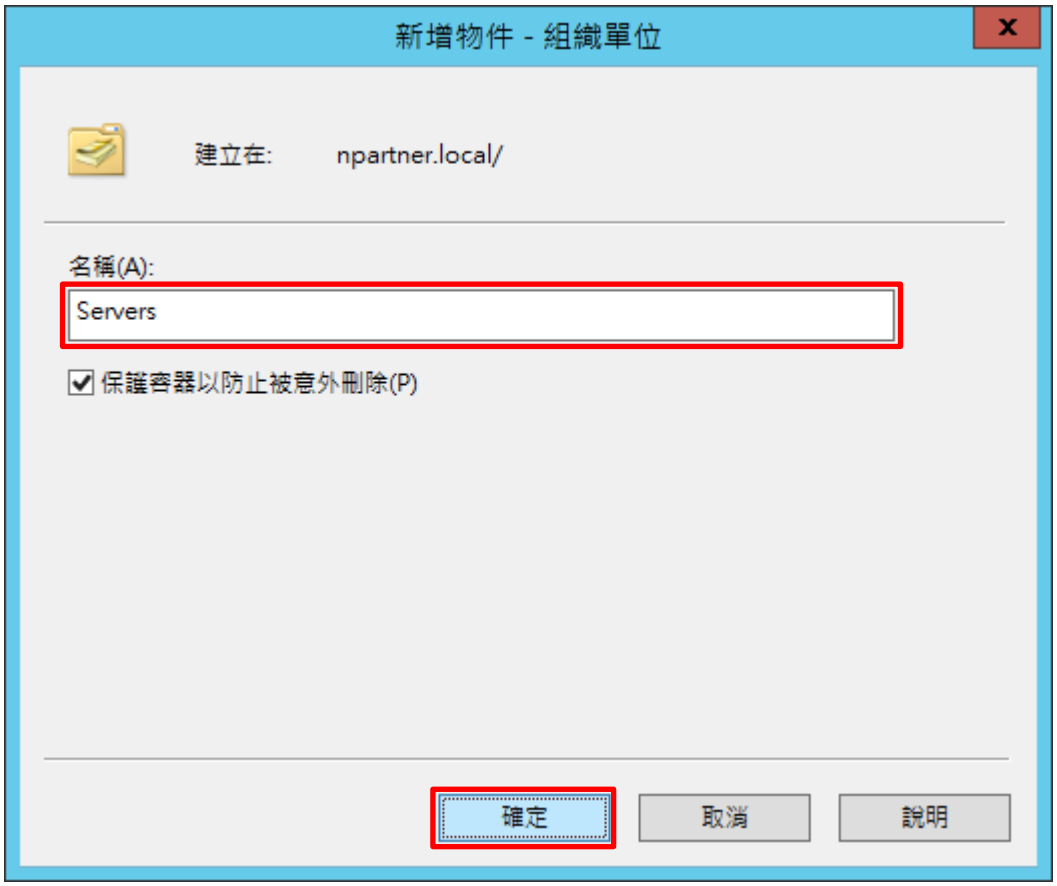
(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



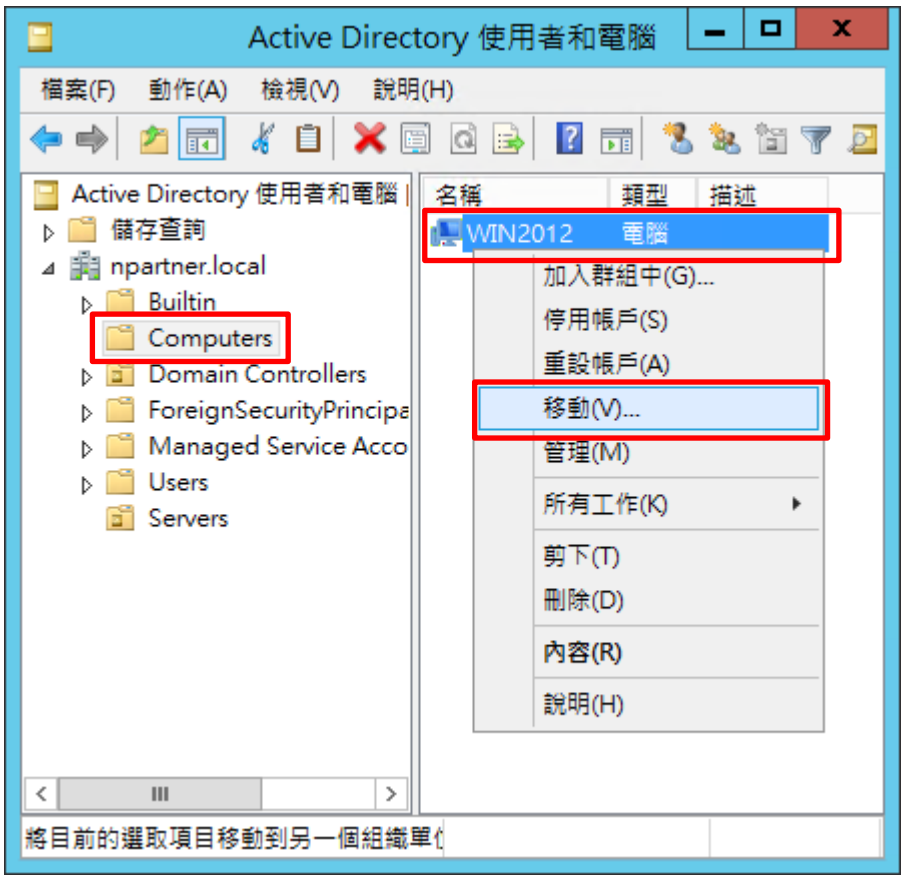
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



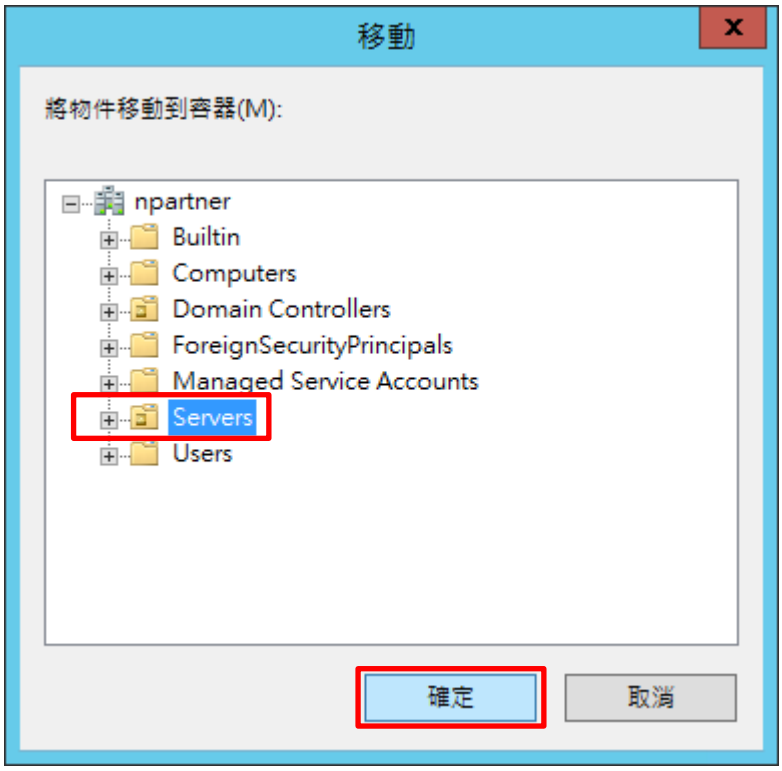
(4) 移動 Exchange 伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2012] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Exchange Server 主機 -> 點選 [移動]



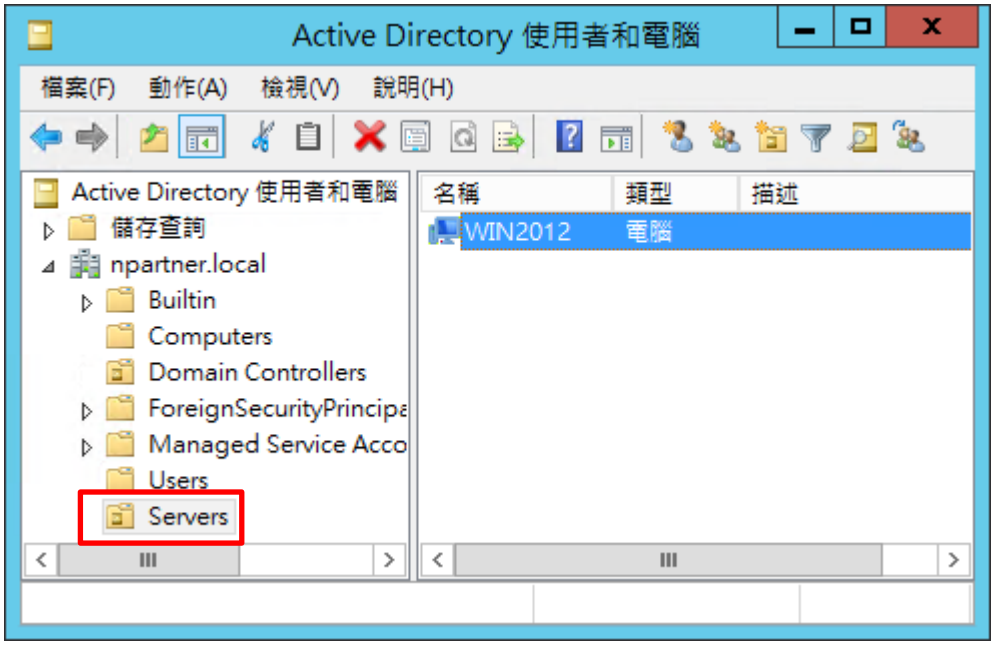
(5) 選擇組織單位

點選 [Servers] 組織單位 -> 按下 [確定]



(6) 確認 Exchange 伺服器已移動至新的組織單位

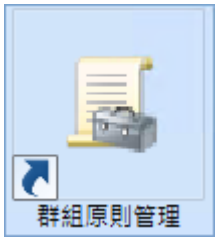
點選 [Servers] 組織單位，確認 Win2012 伺服器已移動。



4.3.2 群組原則

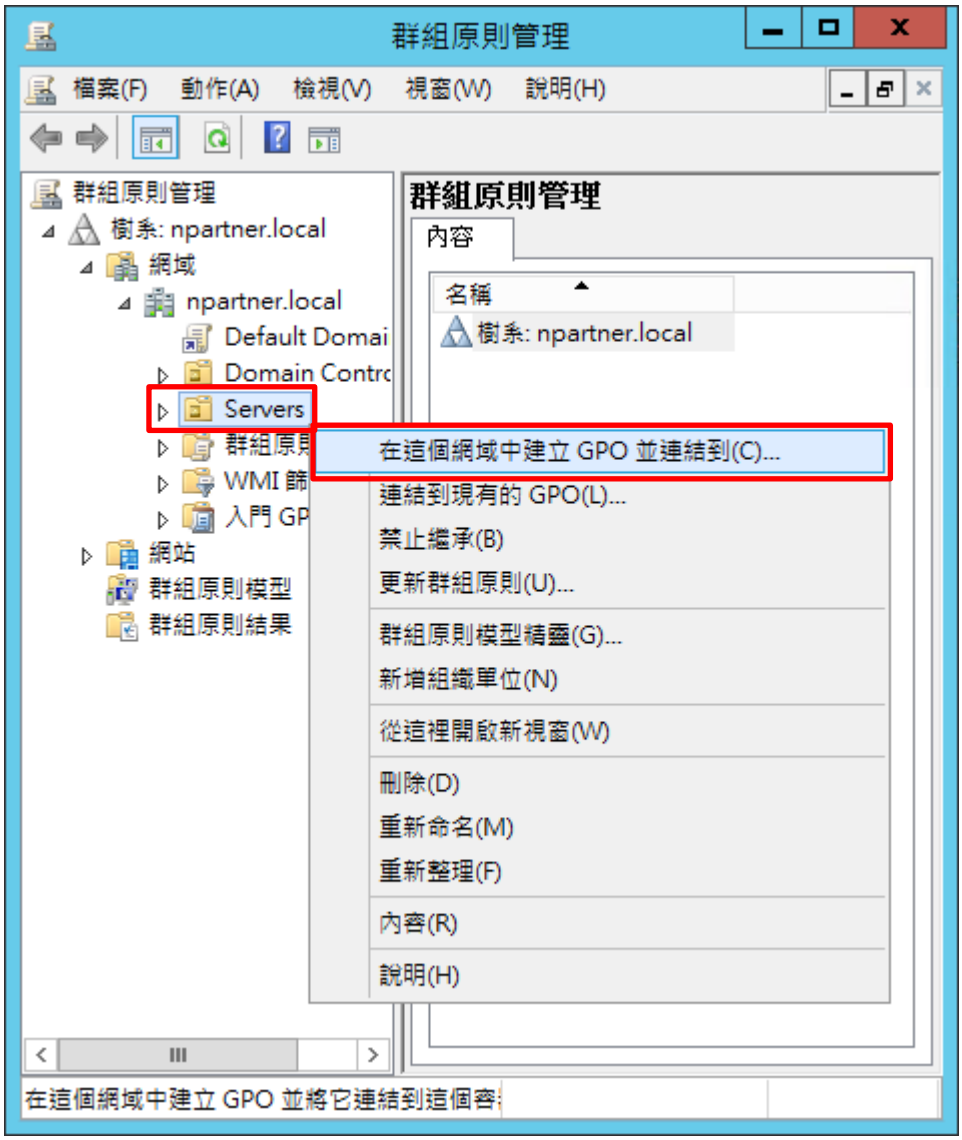
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]

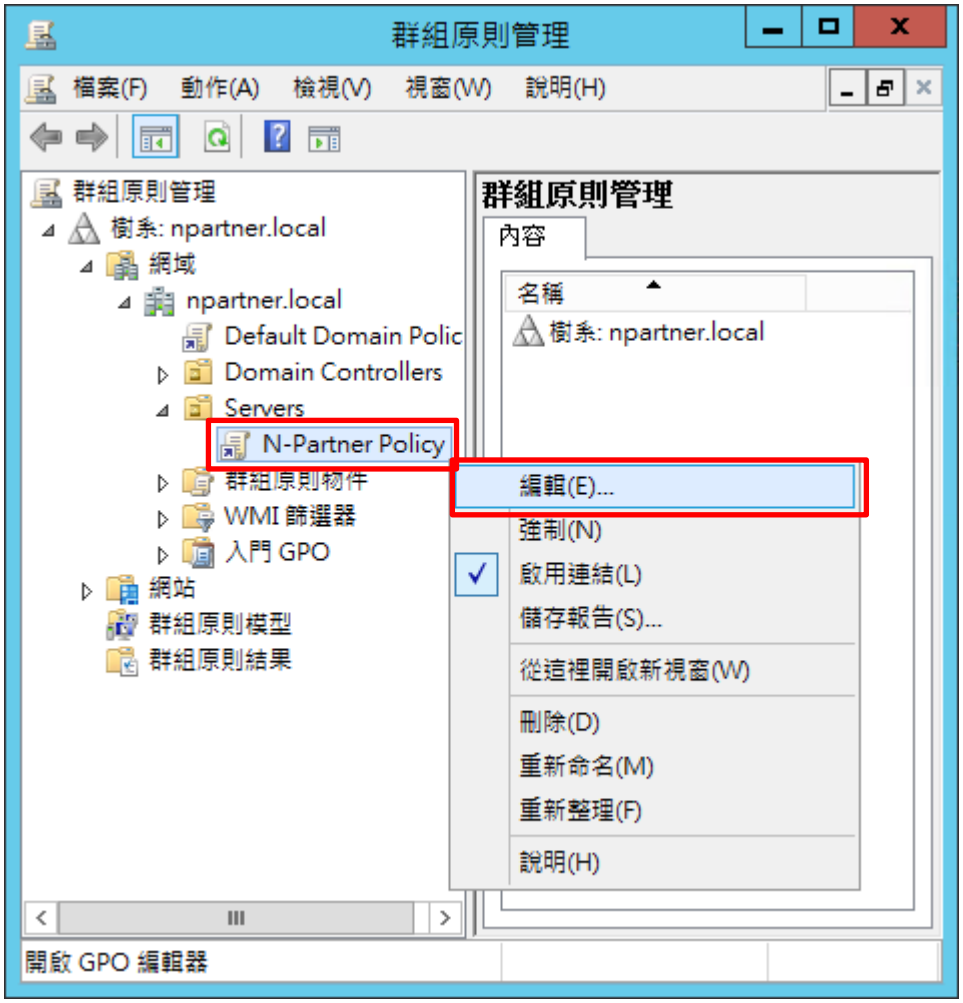


(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]

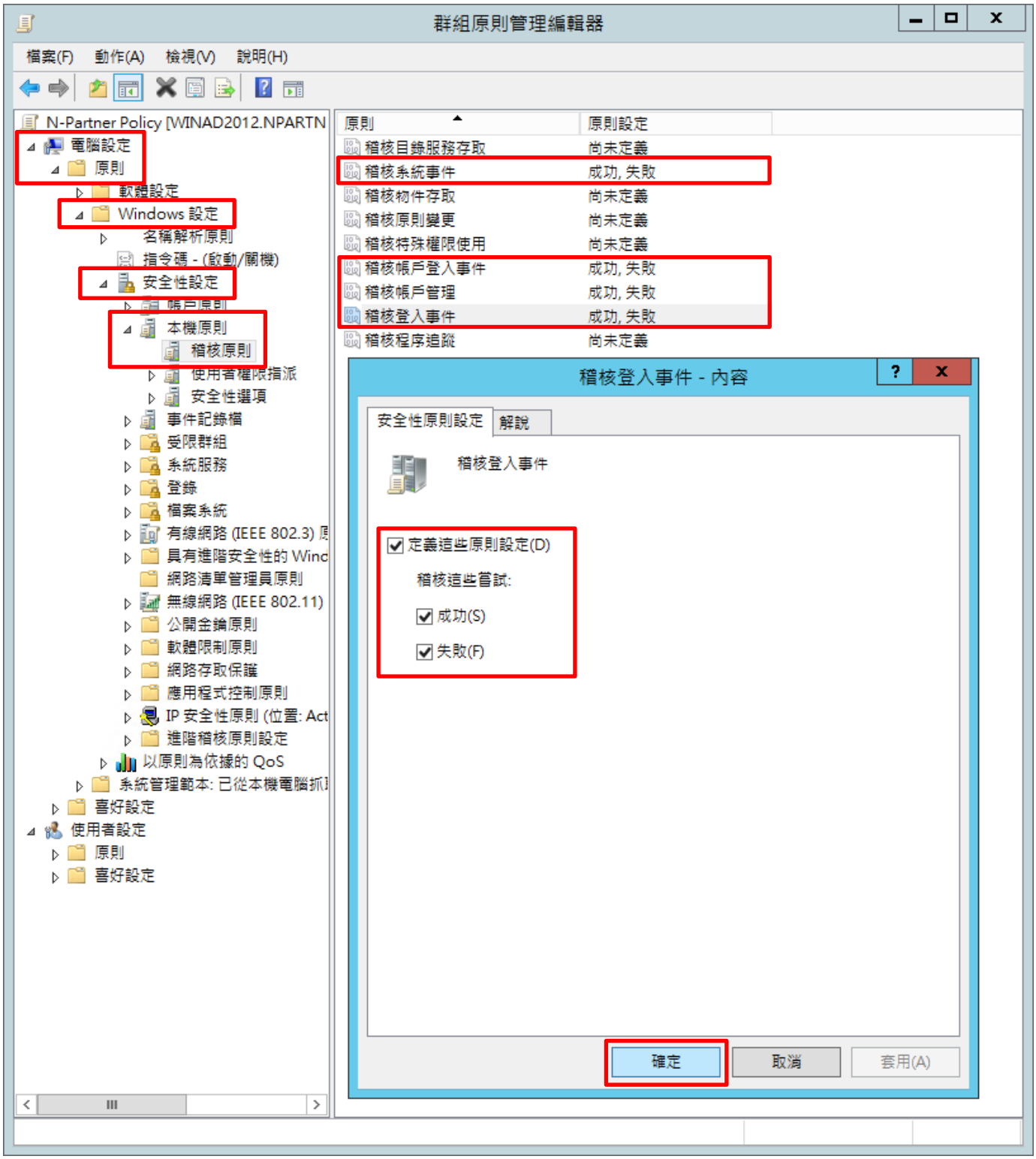
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



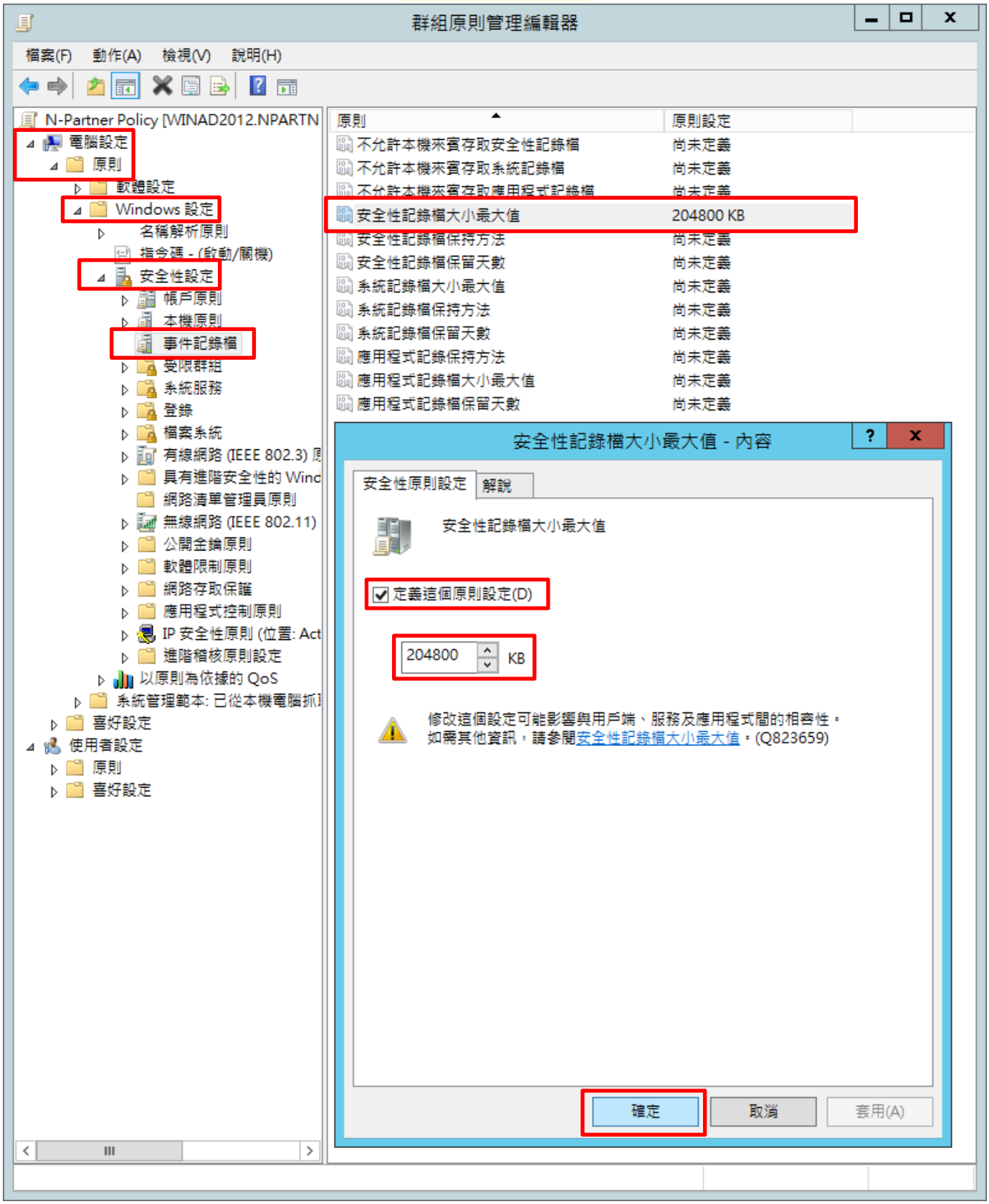
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



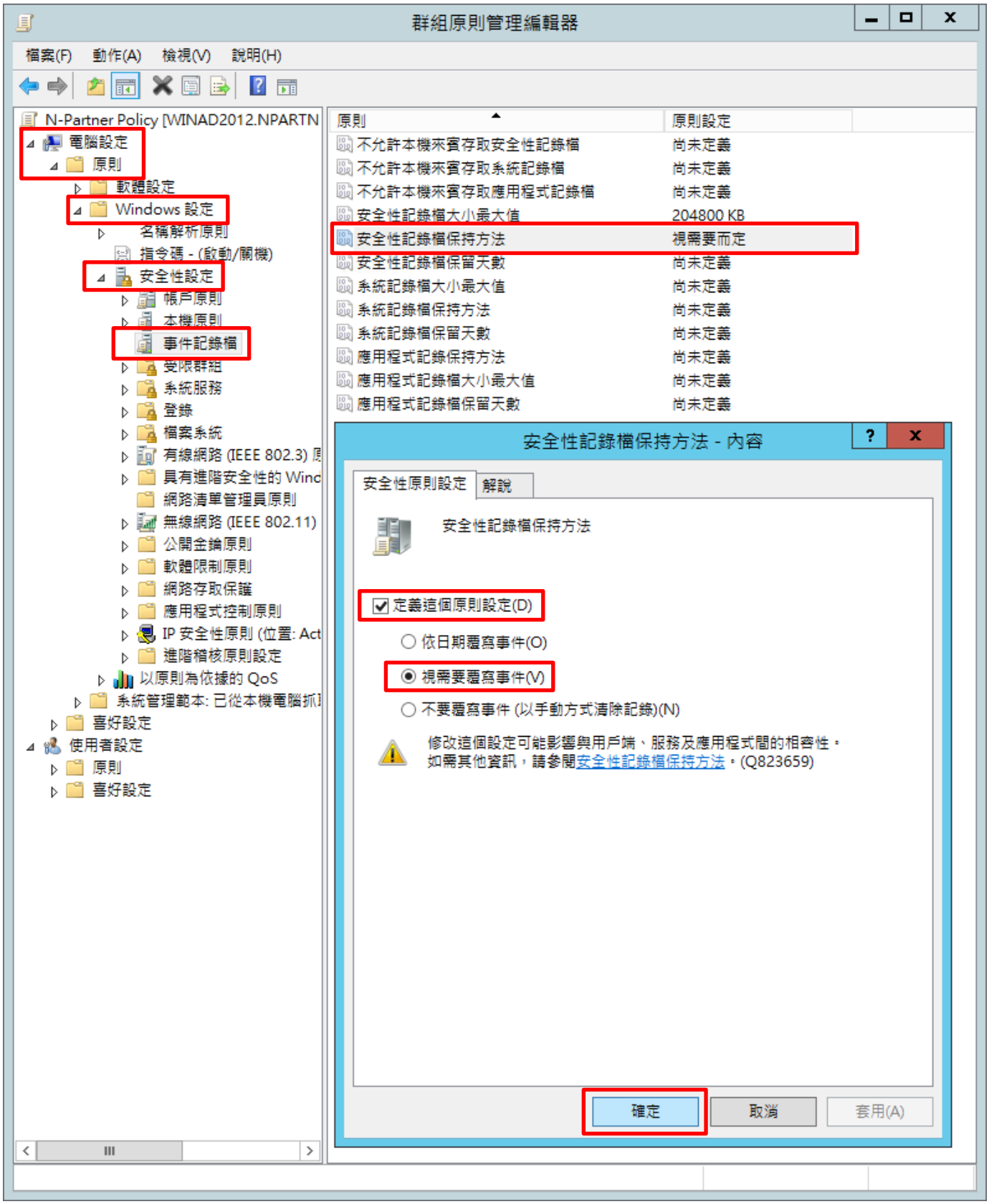
(6) 事件記錄檔：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(7) 事件記錄檔：安全性記錄檔保持方法

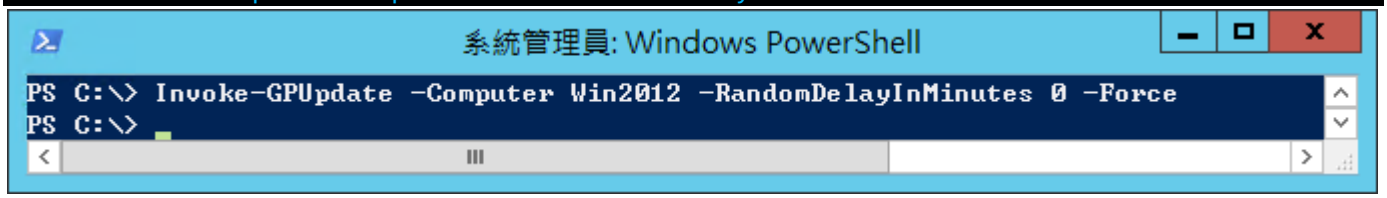
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]

(9) 更新 Exchange 伺服器群組原則

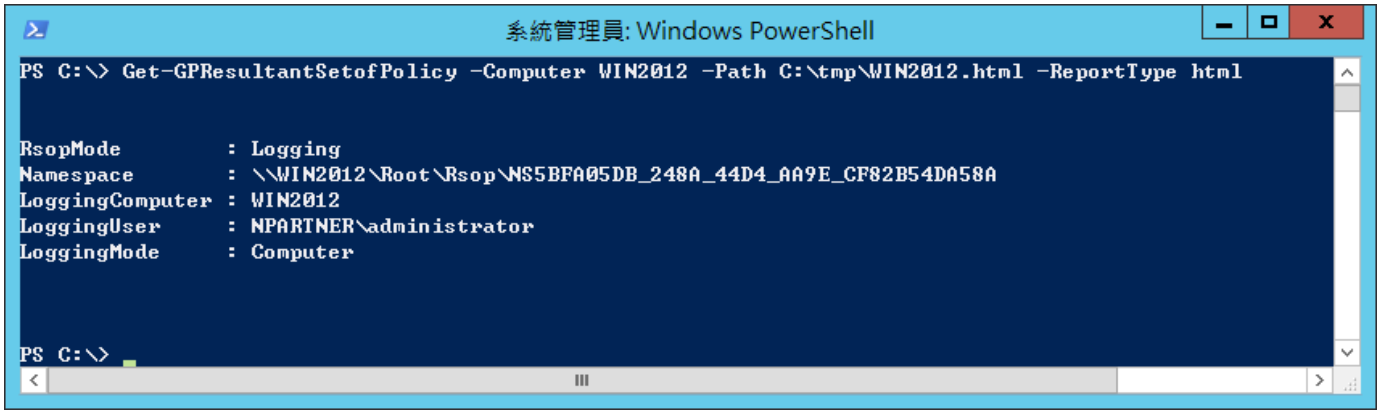
```
PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Exchange 伺服器名稱

(10) 產生 Exchange 伺服器群組原則報表。

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012 -Path C:\tmp\WIN2012.html -ReportType html
```



紅色文字部位請輸入 Exchange 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 -> 確認 Exchange Server 伺服器 -> 套用 N-Partner Policy 群組原則

5. Exchange 2016

範例：Exchange 2016 安裝在 Windows 2016 伺服器。

可選擇 [Exchange Administrative Center] 或 [Exchange Management Shell] 設定郵件追蹤記錄。

5.1 Exchange Message Tracking Log

修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

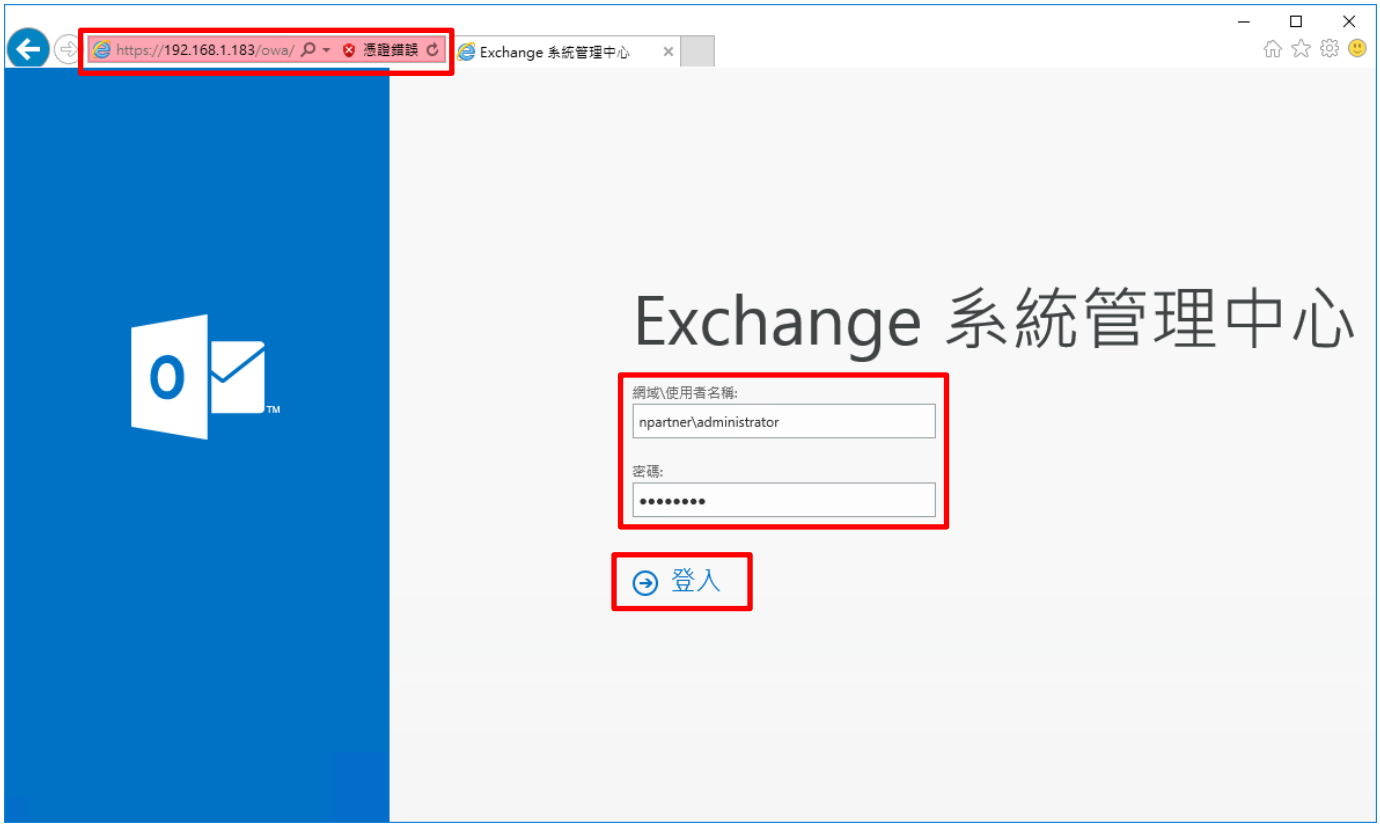
藍色文字部位請修改郵件追蹤記錄資料夾

```
define MailLog     C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

5.1.1 Exchange Administrative Center

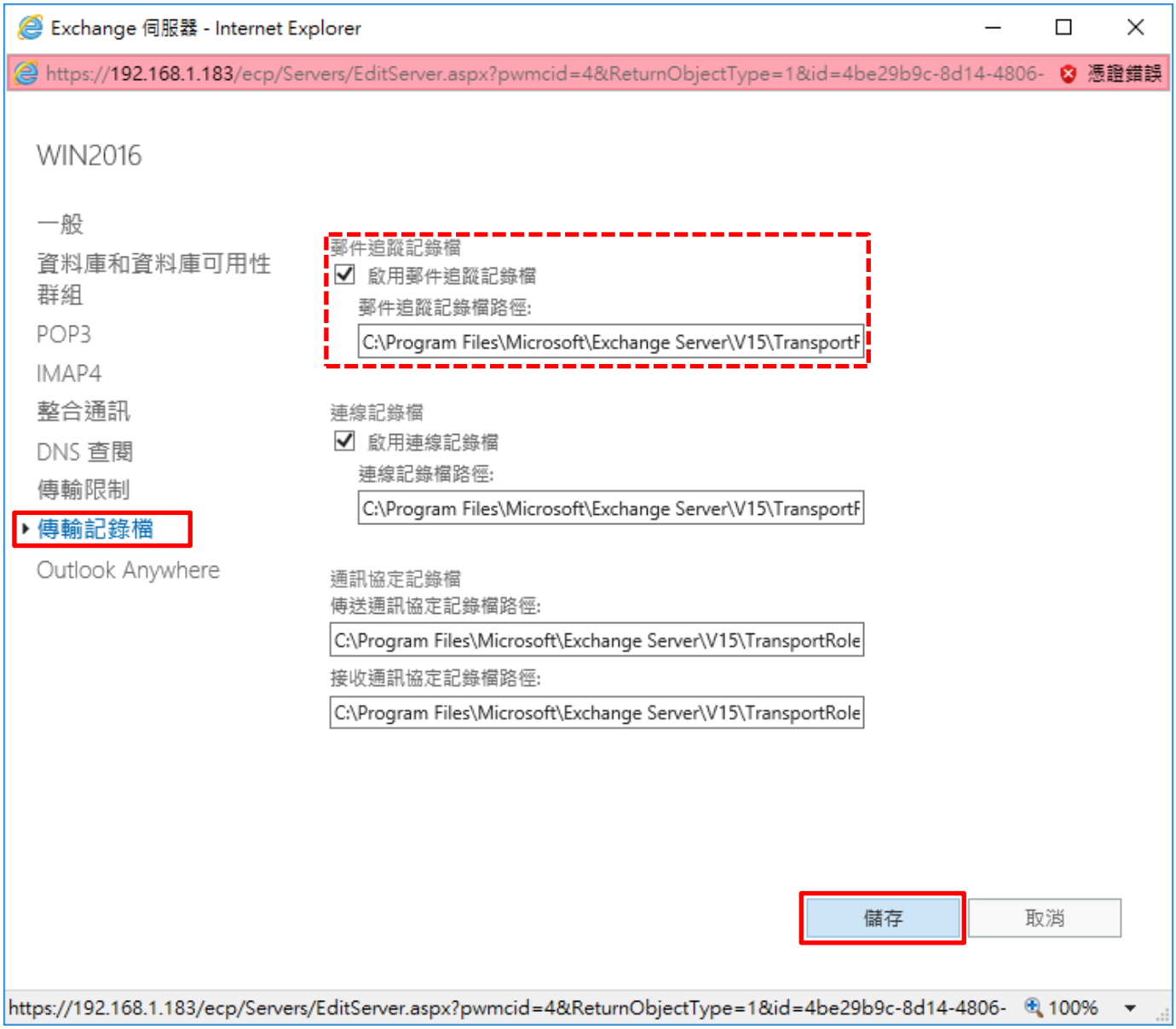
(1) 開啟 [瀏覽器]

(2) URL 輸入 https://<*ExchangeIP*>/ecp -> 輸入網域名稱\管理者帳號和密碼 -> 按 [登入]



(3) 點選 [伺服器] 頁面 -> [伺服器] -> 選擇 [Mailbox 伺服器(WIN2016)] -> 點選 (編輯)

(4) 點選 [傳輸記錄檔] 頁面 -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking] -> 按 [儲存]

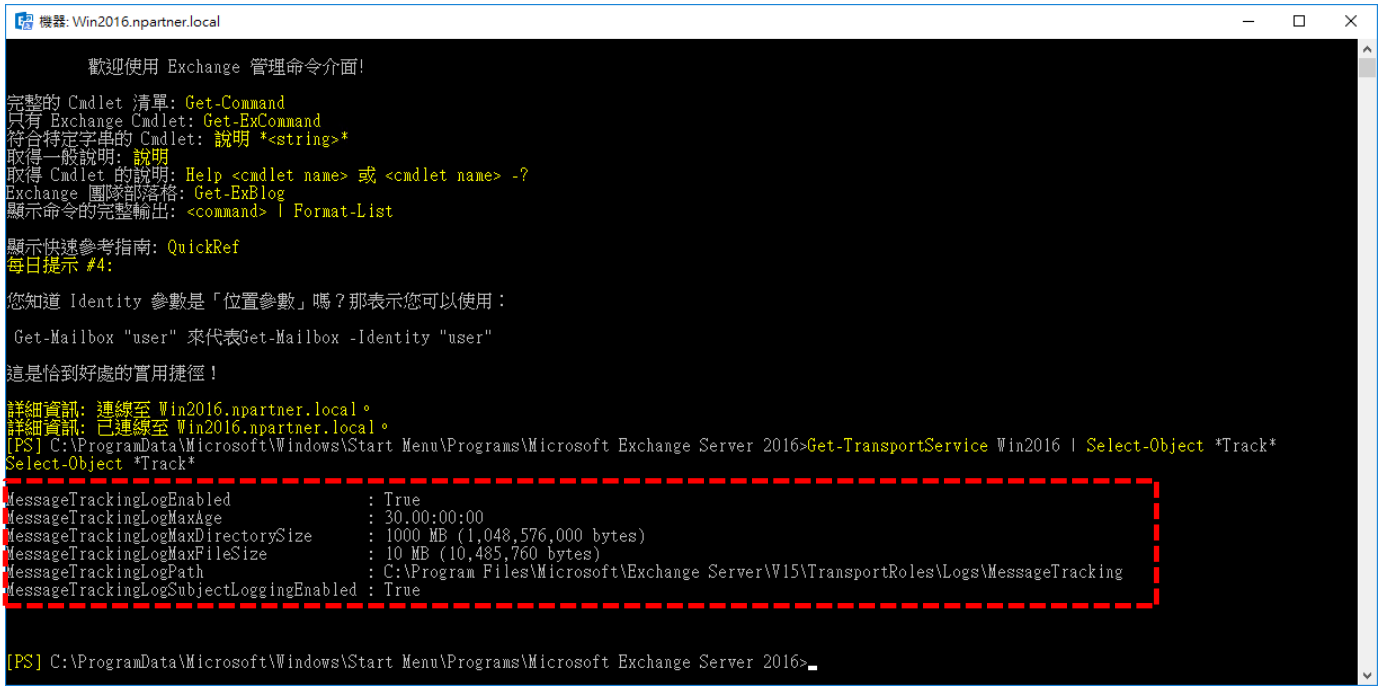


5.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]

(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]

```
[PS] C:\> Get-TransportService Win2016 | Select-Object *Track*
```

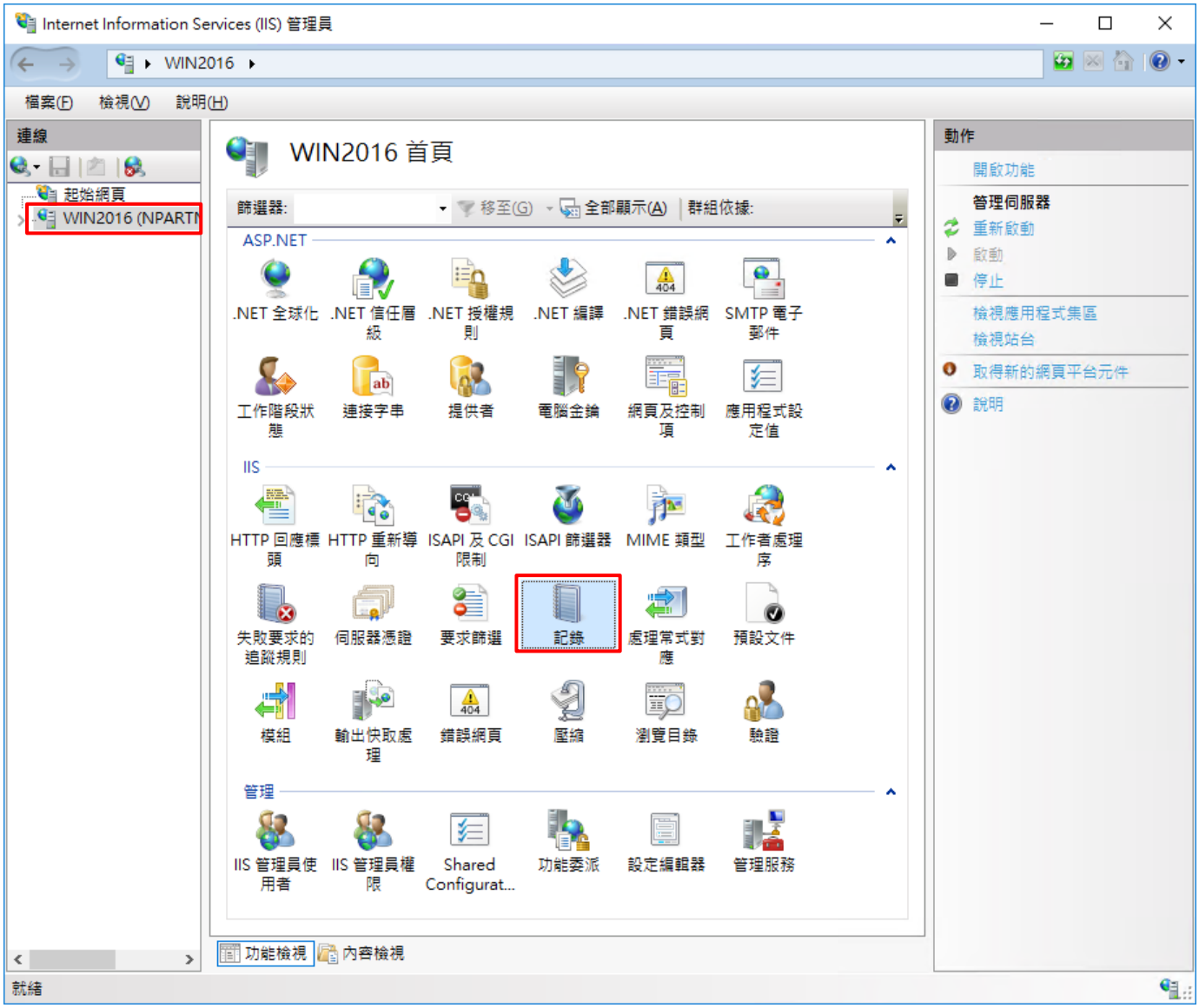


紅色文字部位請輸入 Exchange 伺服器名稱

5.2 IIS Log

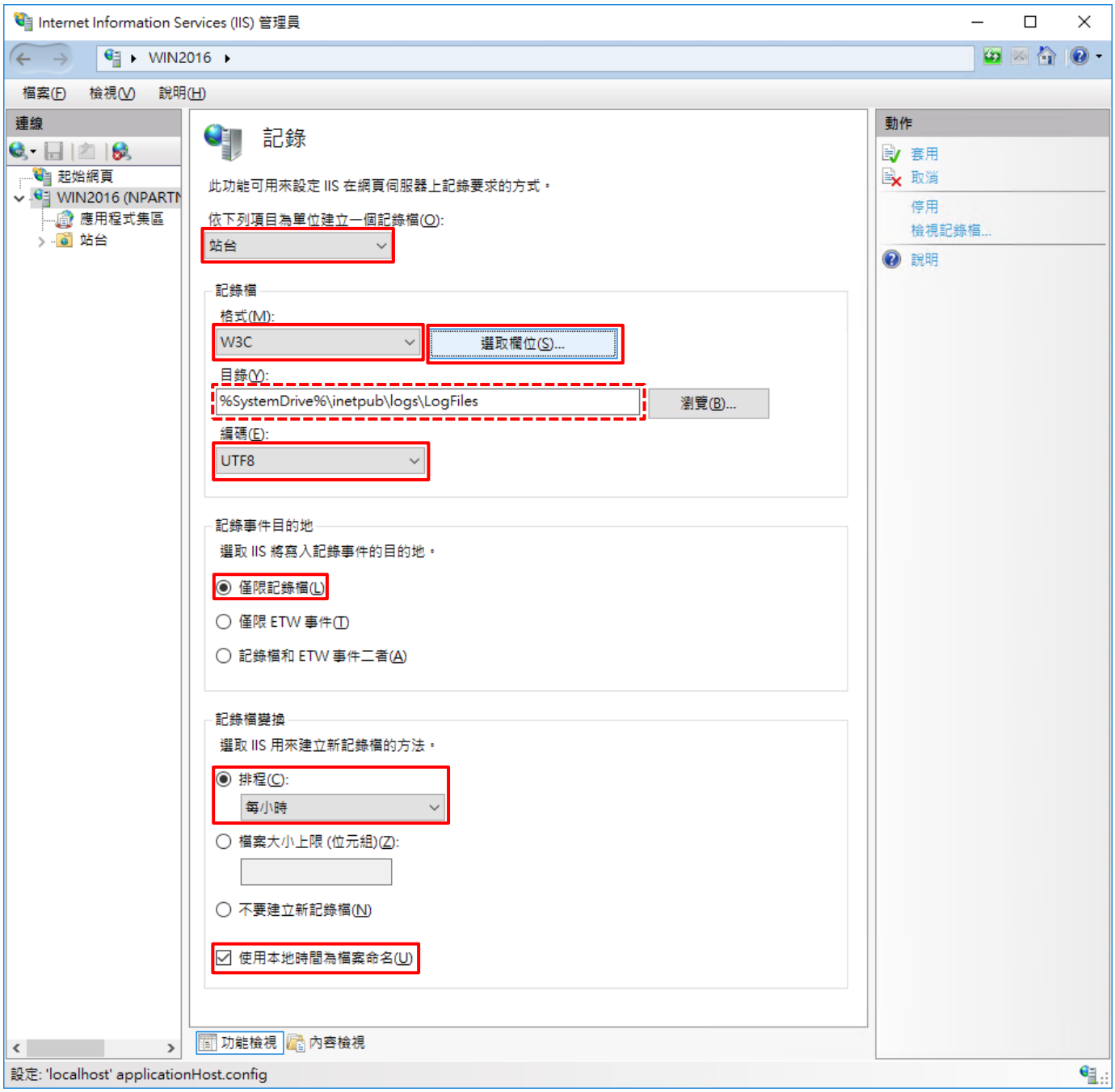
(1) 開啟 [Internet Information Services (IIS) 管理員]

(2) 選擇 [IIS 伺服器] -> 點選 [記錄]

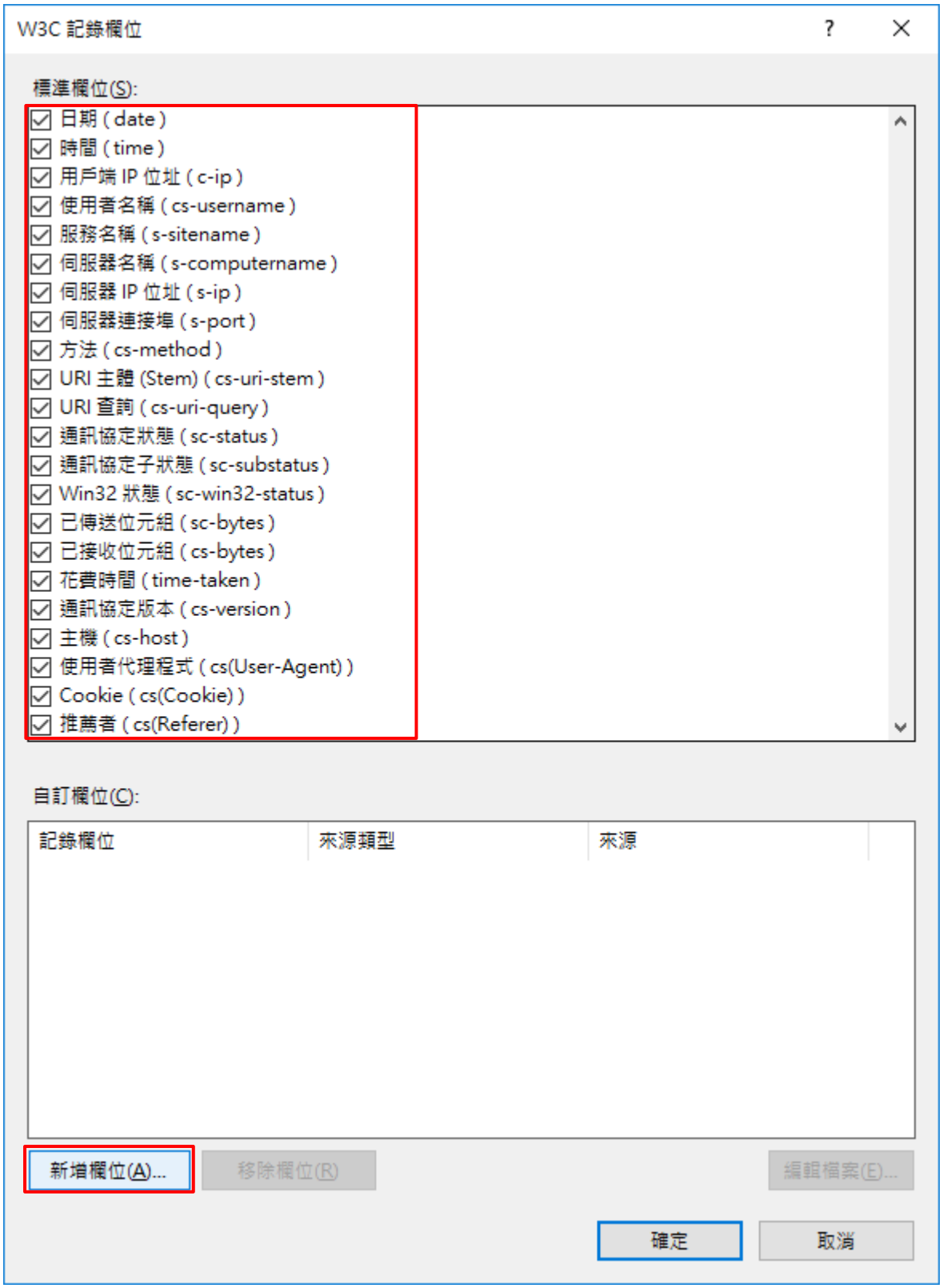


(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

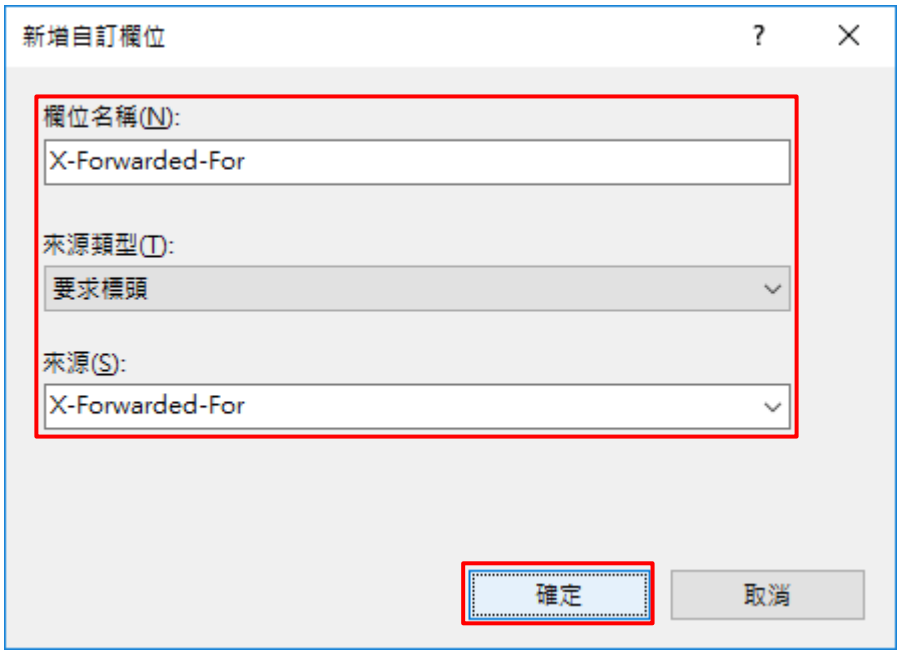
[%SystemDrive%\inetpub\logs\LogFiles] -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取檔位]



(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [新增欄位]

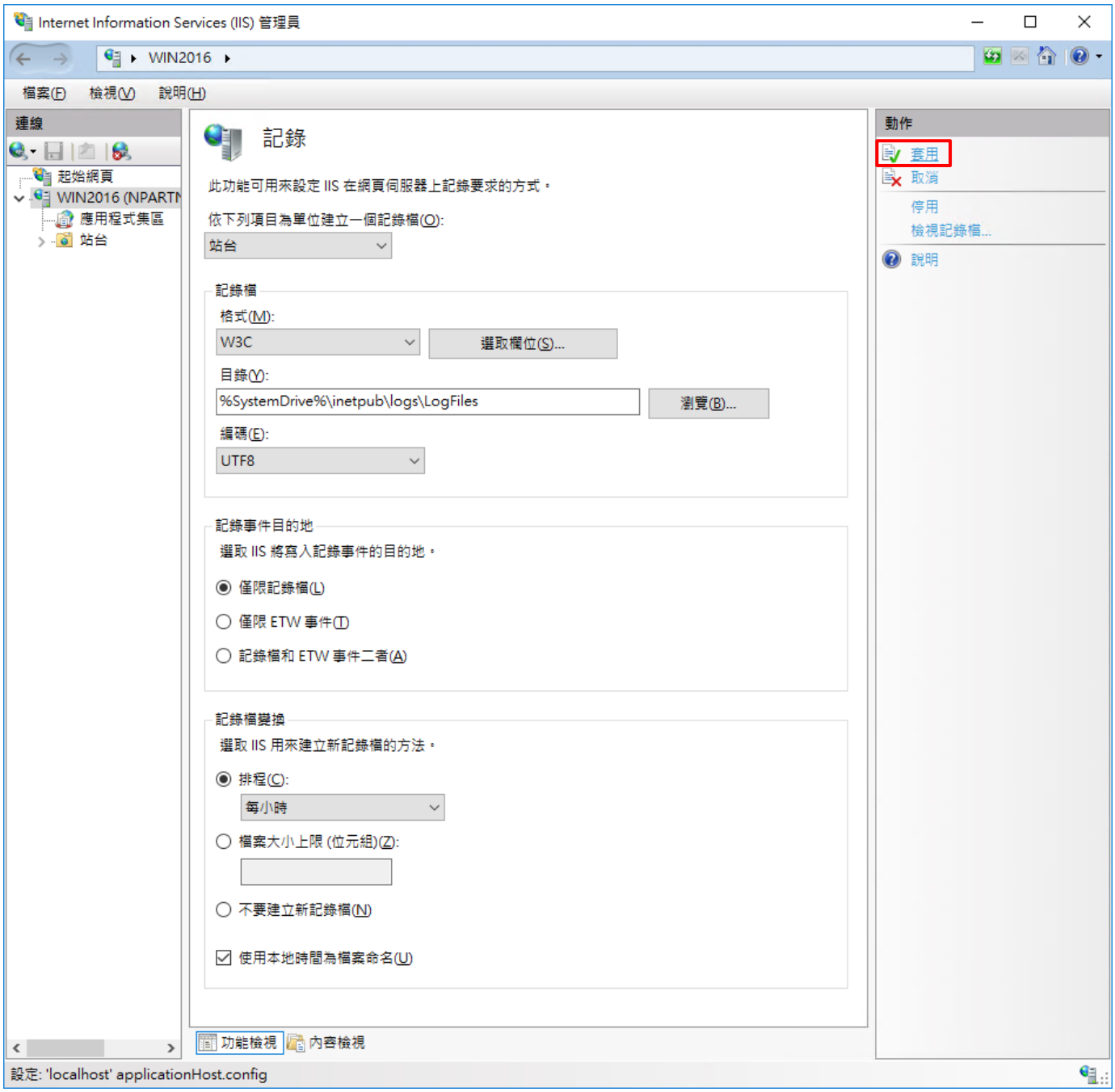


(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [要求標頭] -> 輸入來源: X-Forwarded-For -> 按下 [確定]

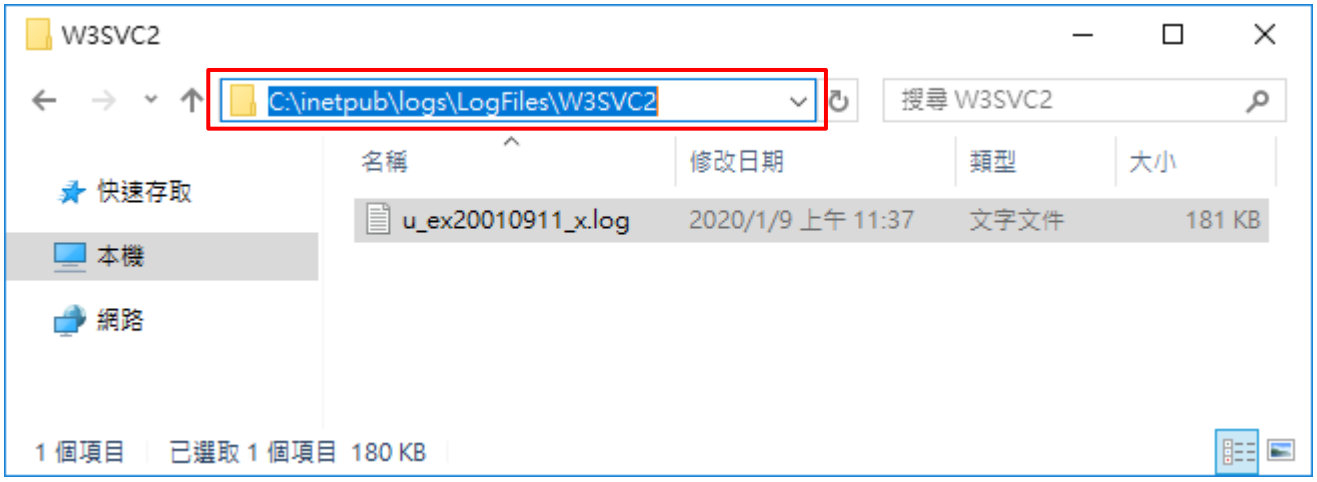


(6) 按下 [確定]

(7) 按下 [套用]



(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC2] 資料夾 IIS log 檔案: u_ex*.log

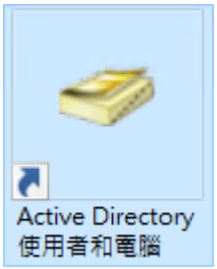


5.3 Event Log

5.3.1 組織單位

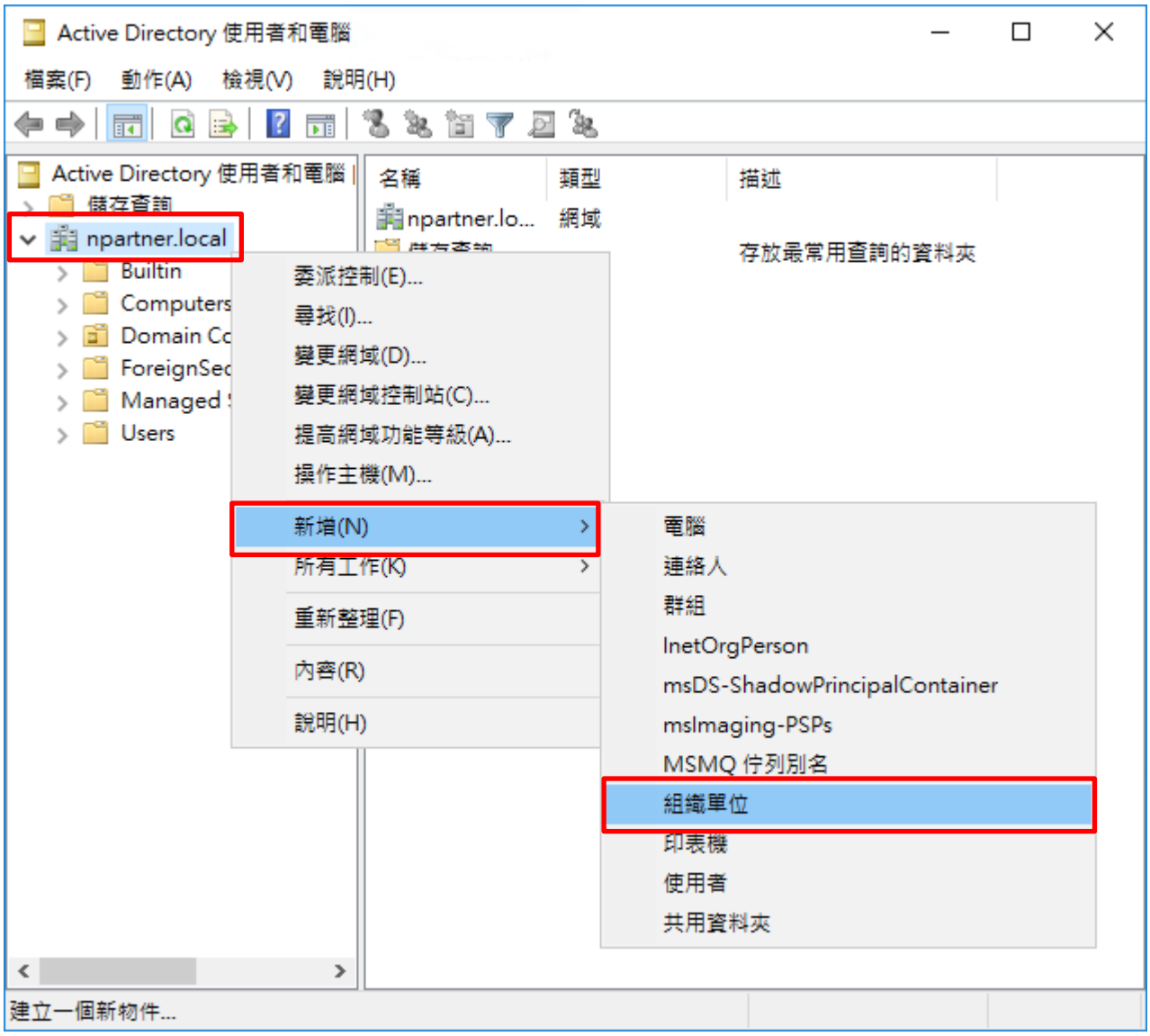
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



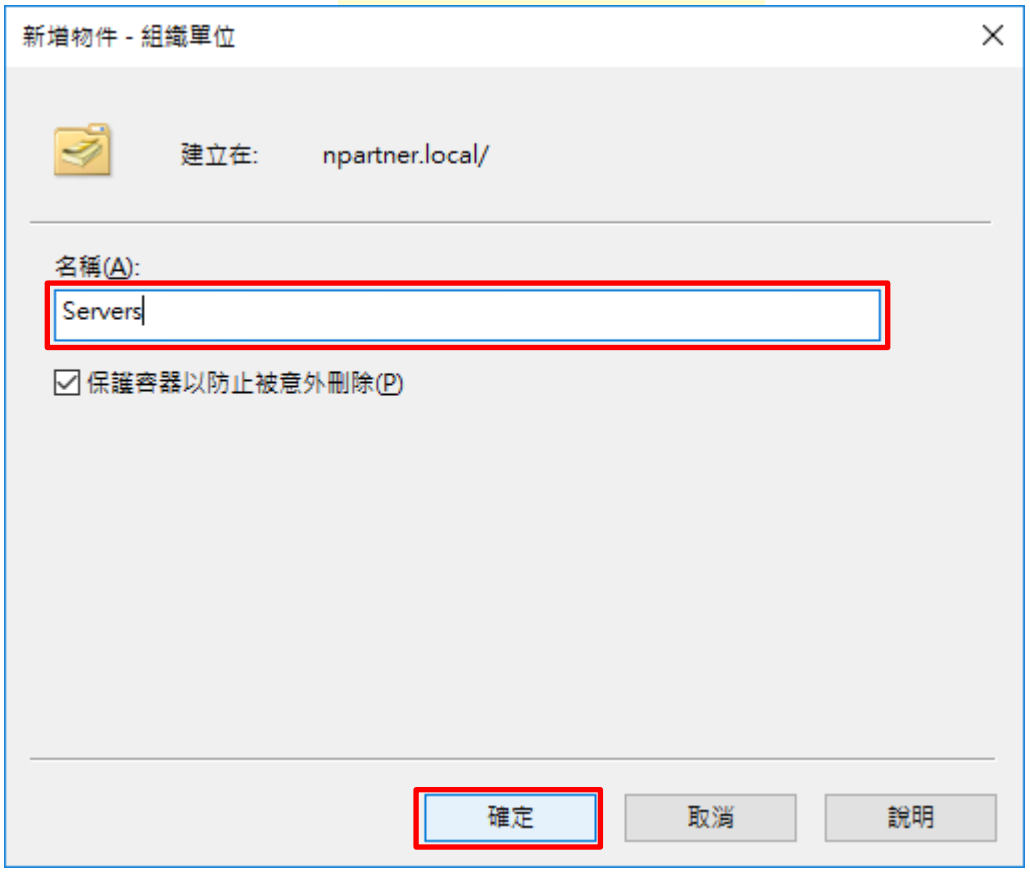
(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



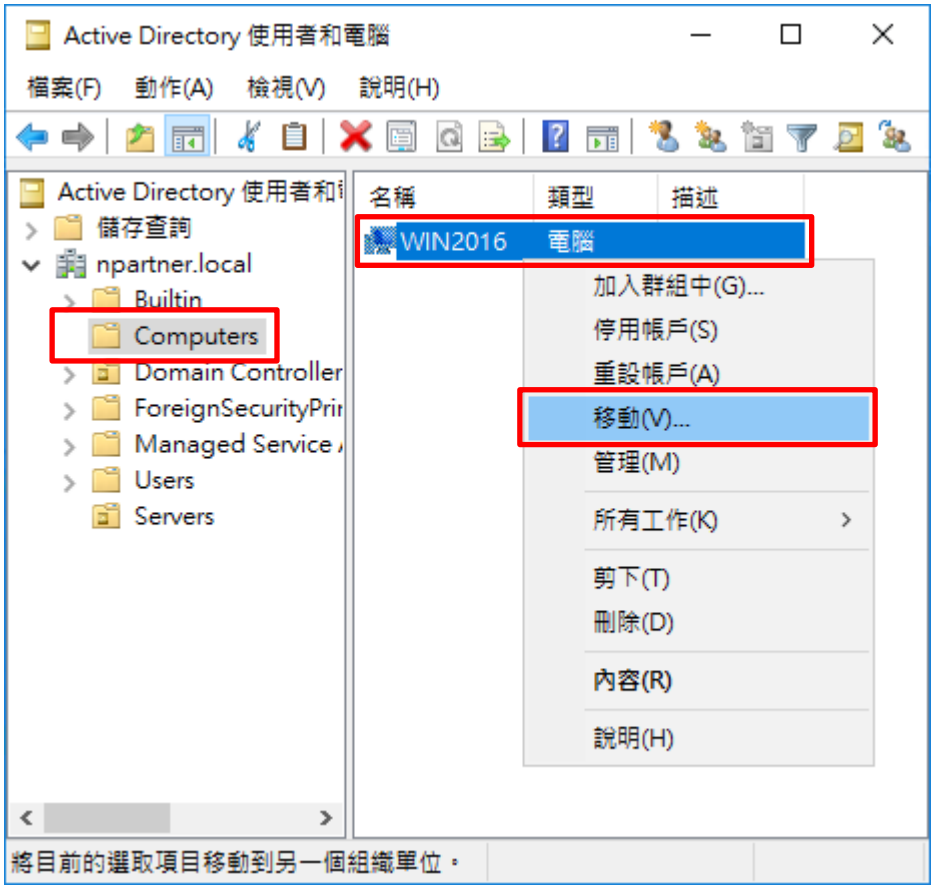
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



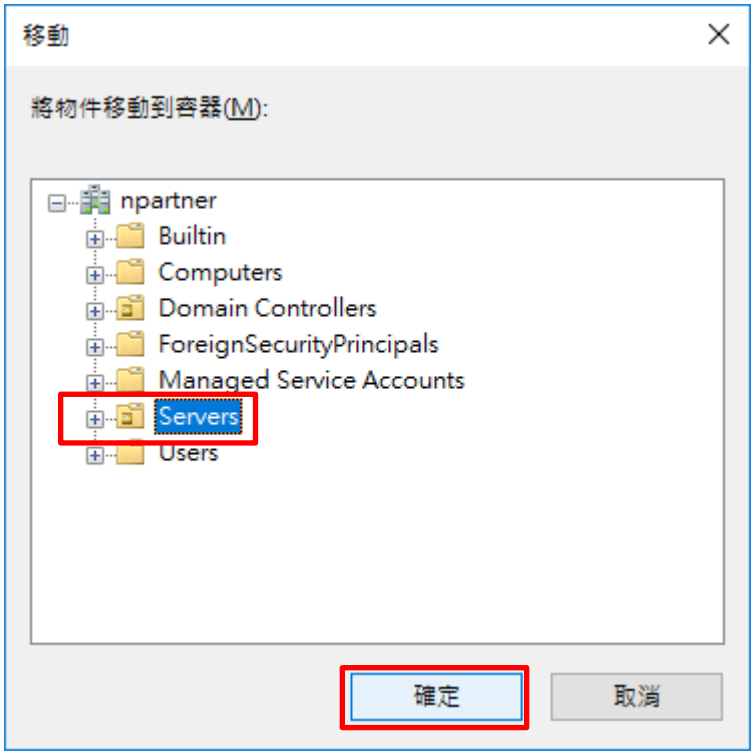
(4) 移動 Exchange 伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2016] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Exchange Server 主機 -> 點選 [移動]



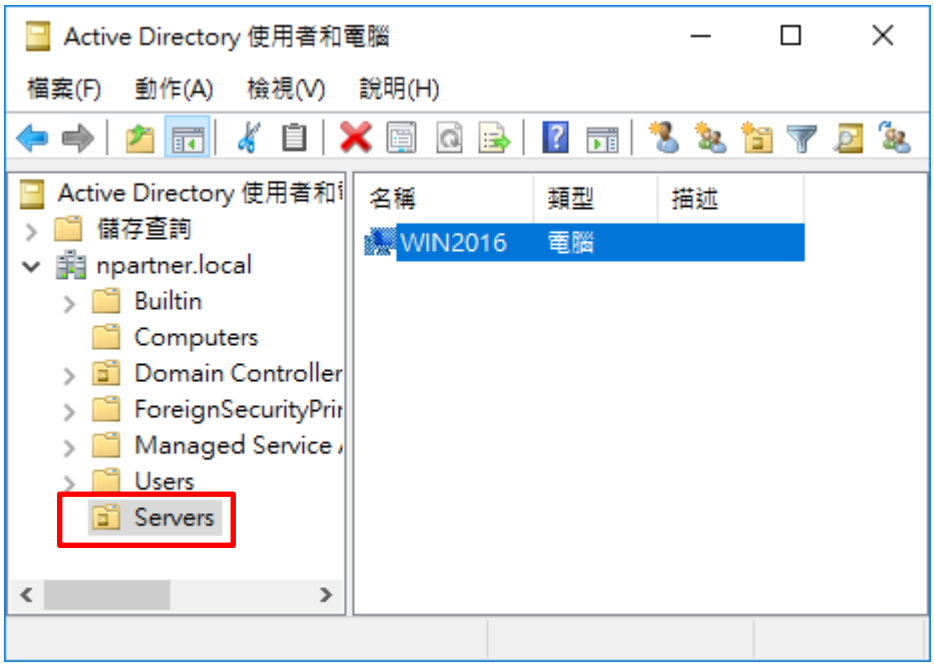
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認 Exchange 伺服器已移動至新的組織單位

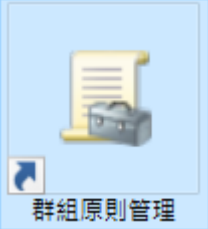
點選 [Servers] 組織單位，確認 Win2016 伺服器已移動。



5.3.2 群組原則

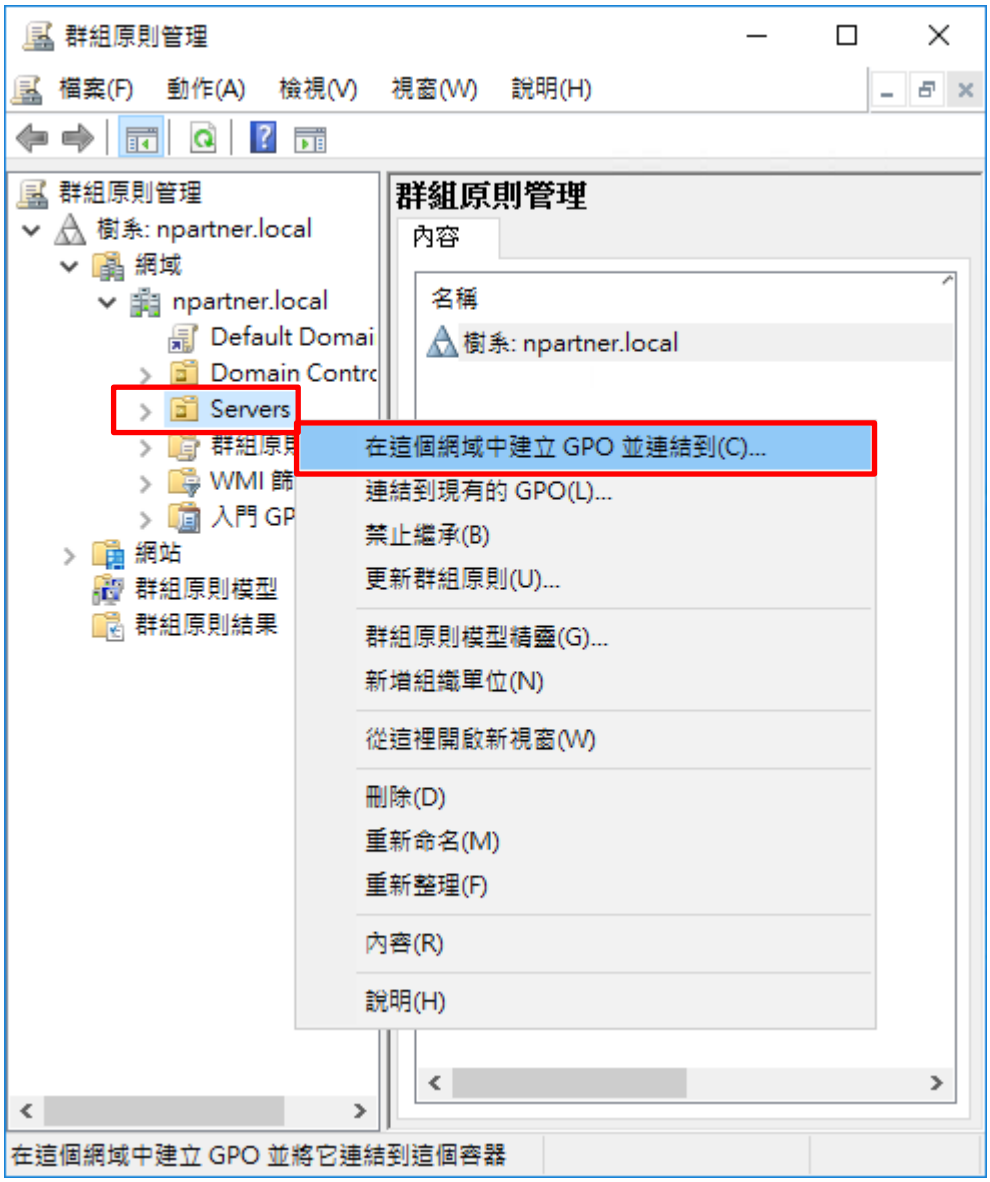
(1) 開啟群組原則管理

開啟 [群組原則管理]



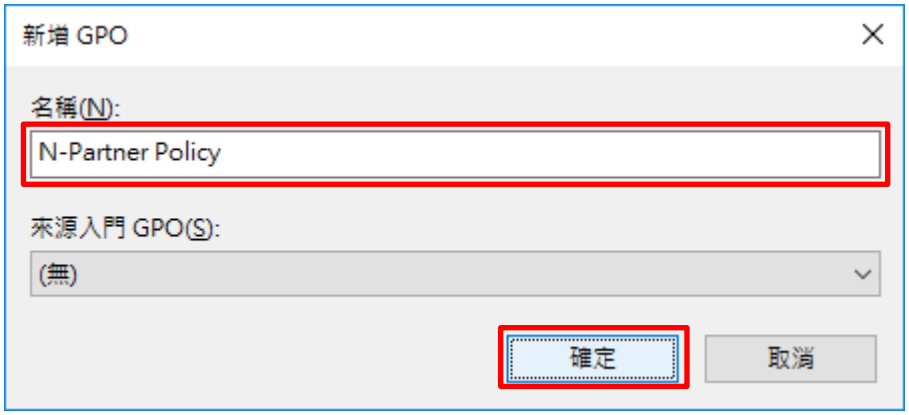
(2) 在 Servers 組織單位，新增群組原則物件

在 [Servers] 組織單位上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



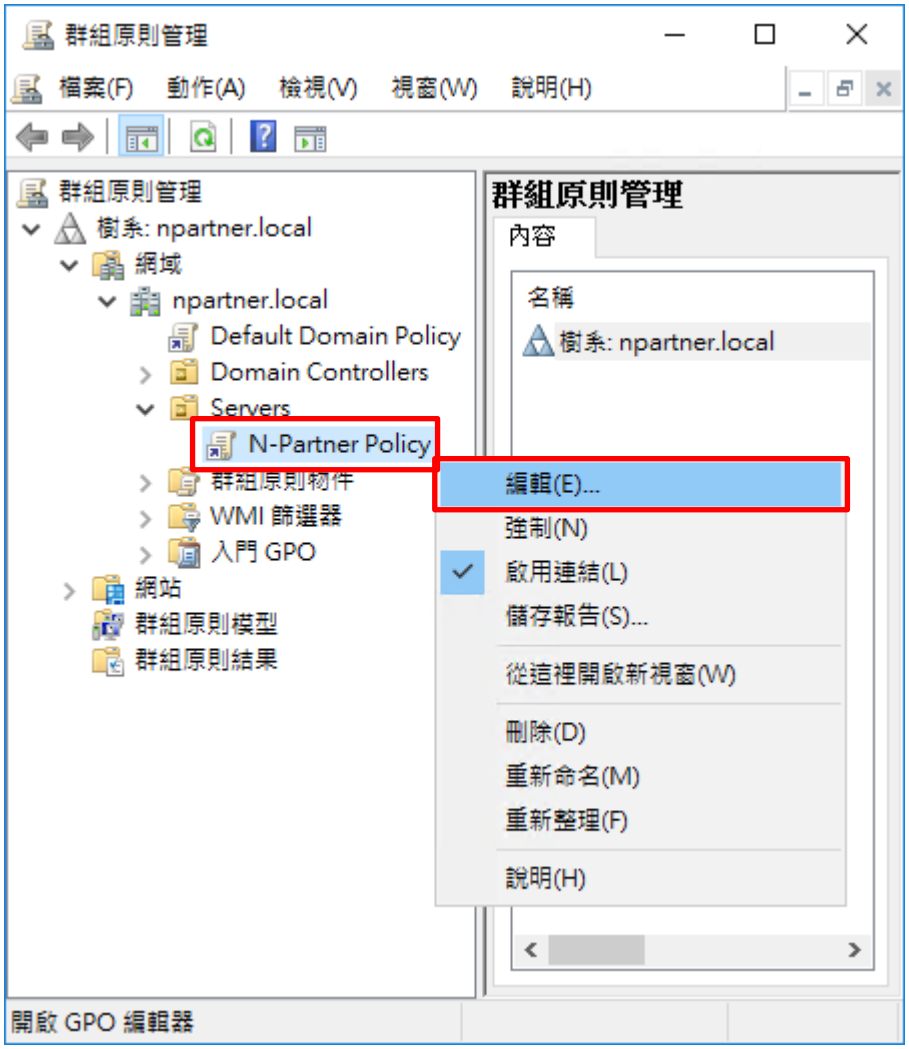
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]



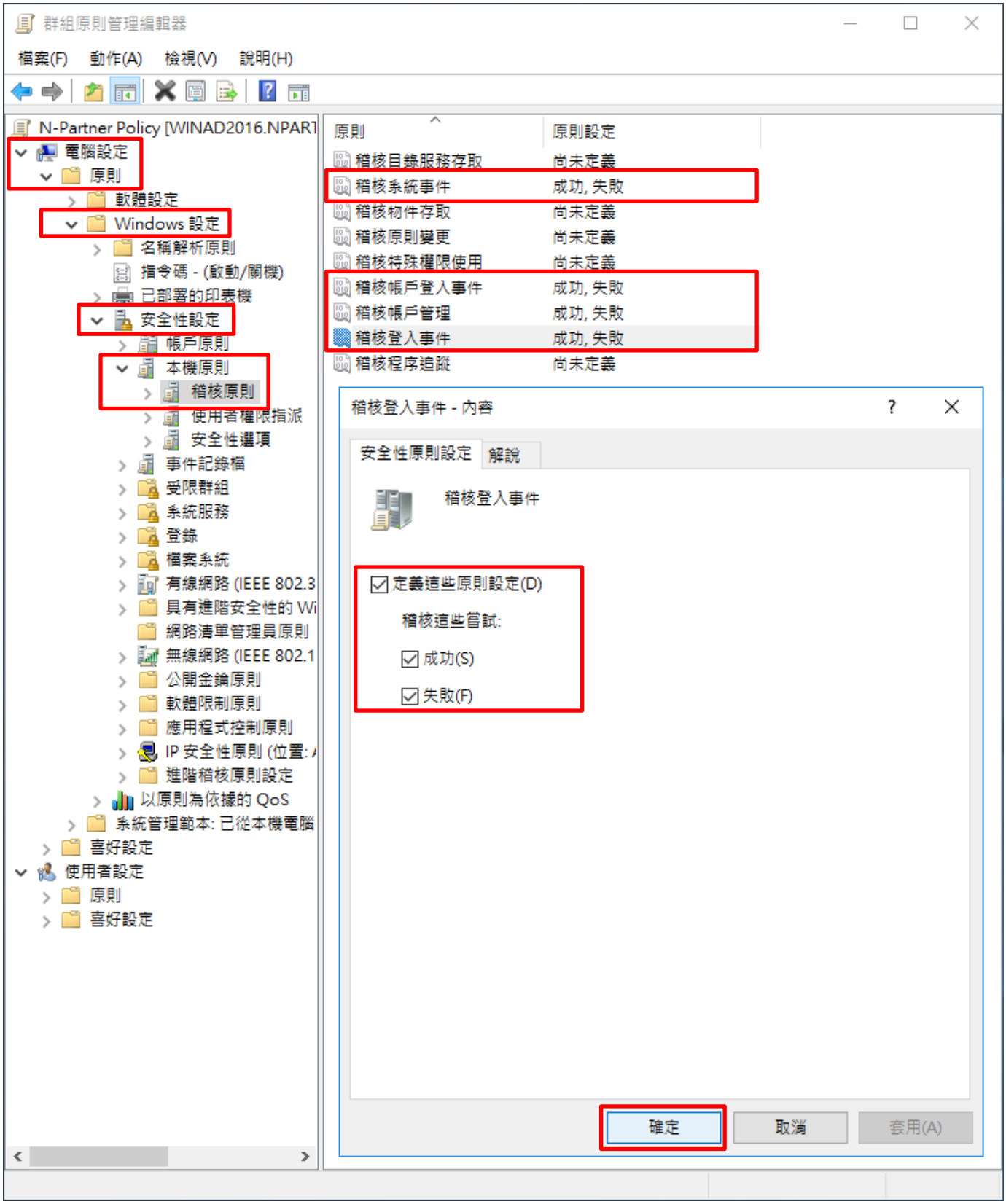
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



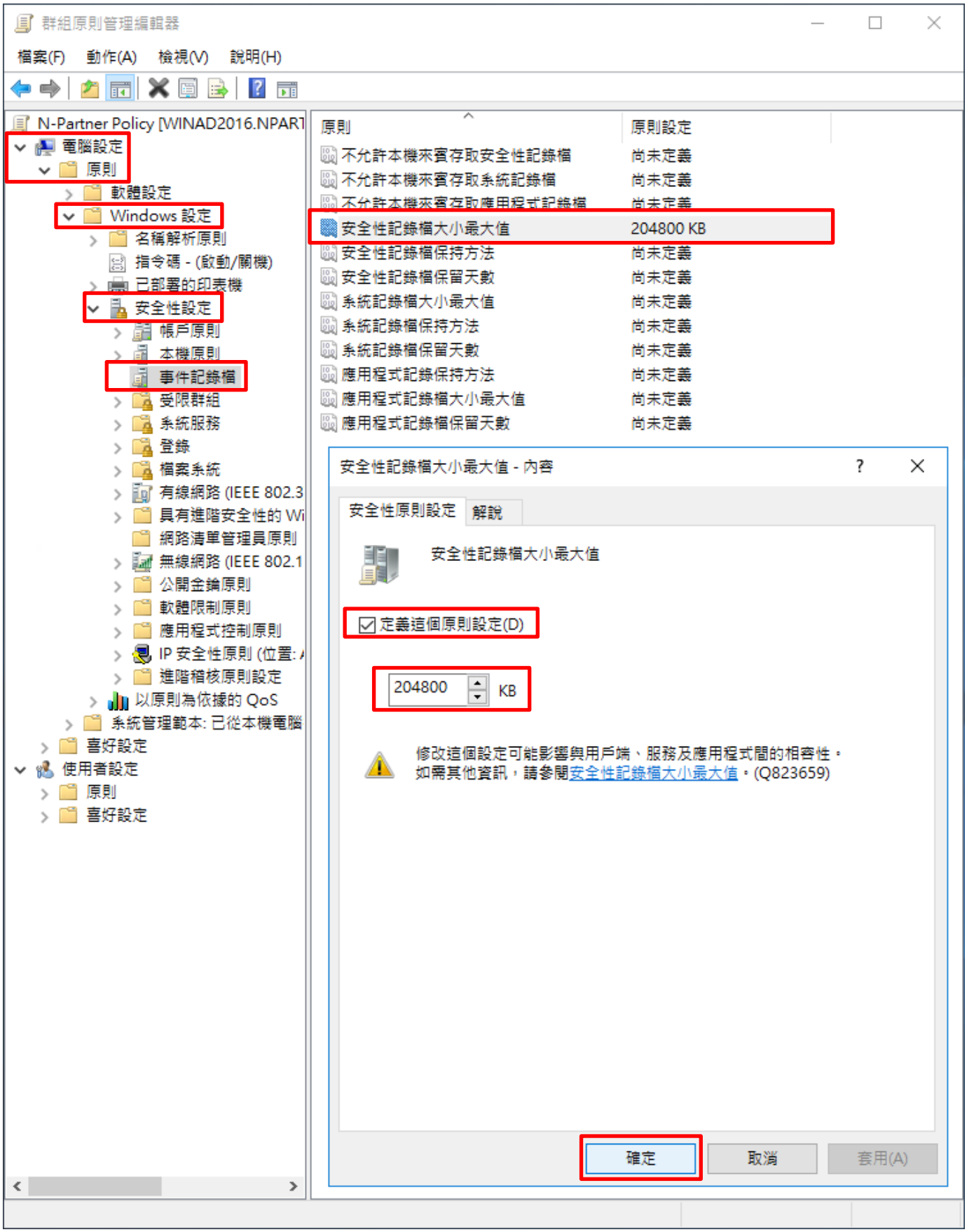
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



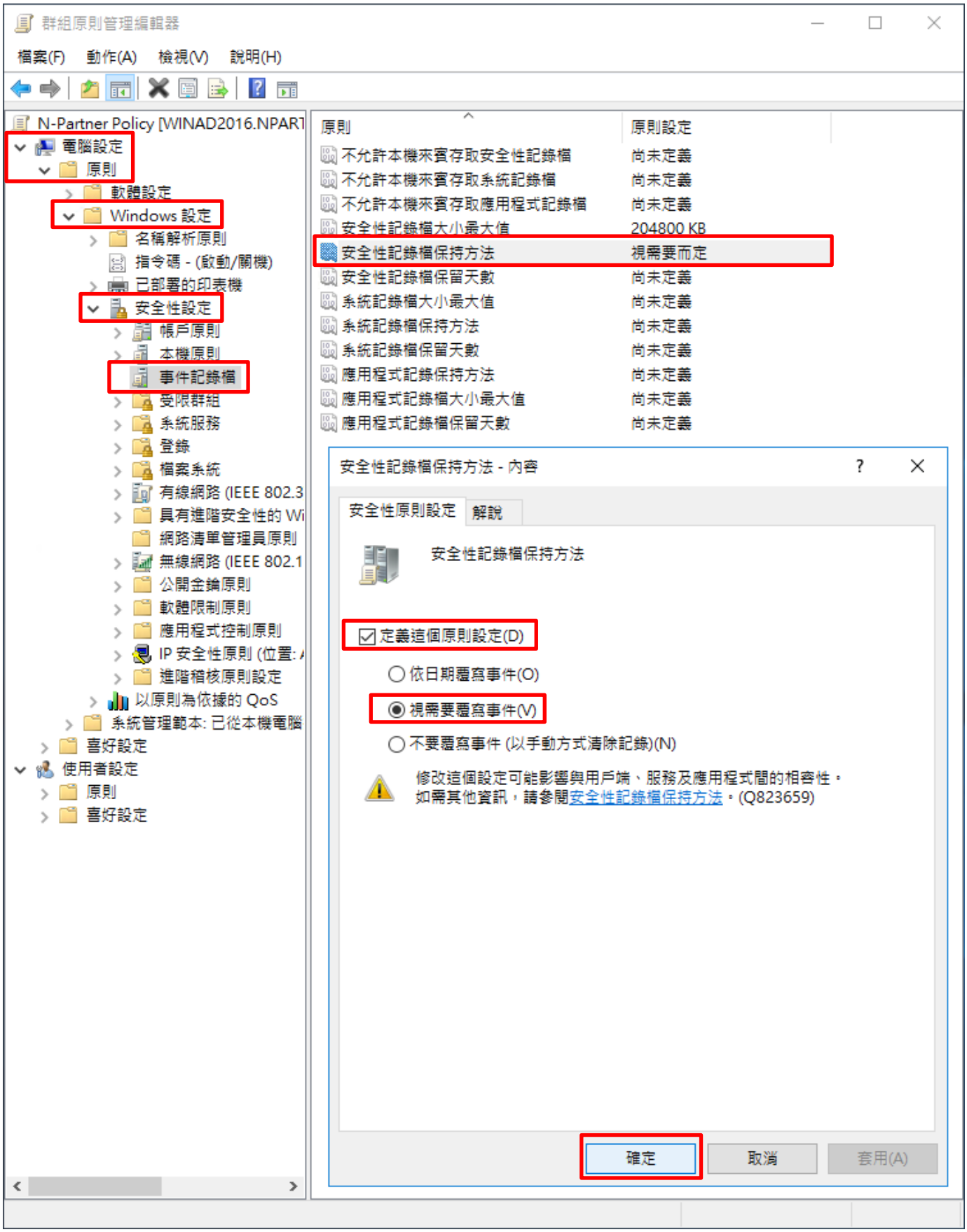
(6) 事件記錄檔：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

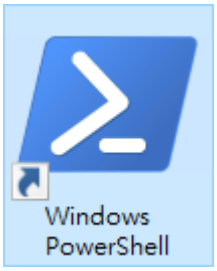


(7) 事件記錄檔：安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]

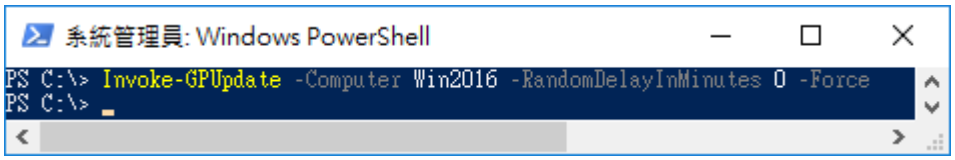


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Exchange Server 群組原則

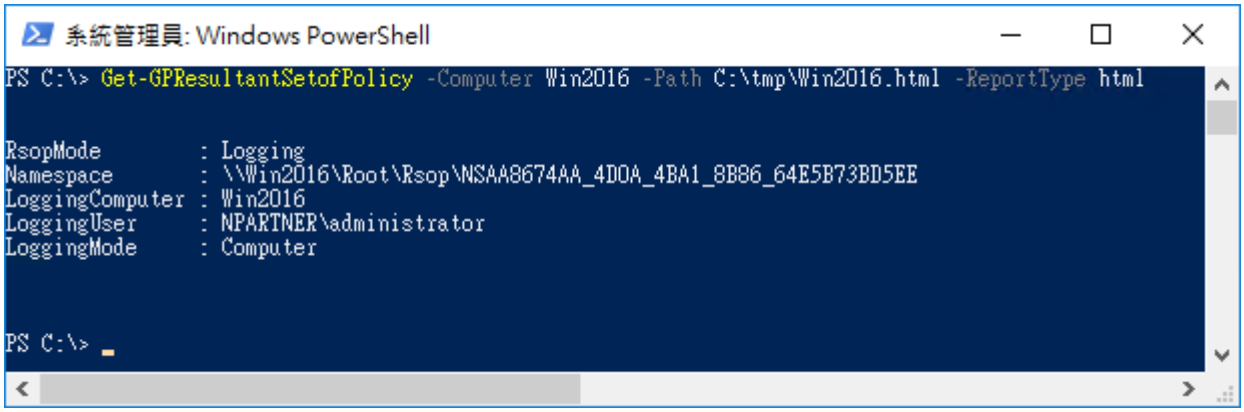
```
PS C:\> Invoke-GPUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Exchange 伺服器名稱

(10) 在 AD 網域伺服器 -> 產生 Exchange 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016 -Path C:\tmp\Win2016.html -ReportType html
```



紅色文字部位請輸入 Exchange 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 -> 確認 Exchange 伺服器 -> 套用 N-Partner Policy 群組原則

6. Exchange 2019

範例：Exchange 2019 安裝在 Windows 2019 伺服器。

可選擇 [Exchange Administrative Center] 或 [Exchange Management Shell] 確認啟用郵件追蹤記錄。

6.1 Exchange Message Tracking Log

修改 nxlog.conf

註: 參考 1.3 NXLog 設定檔

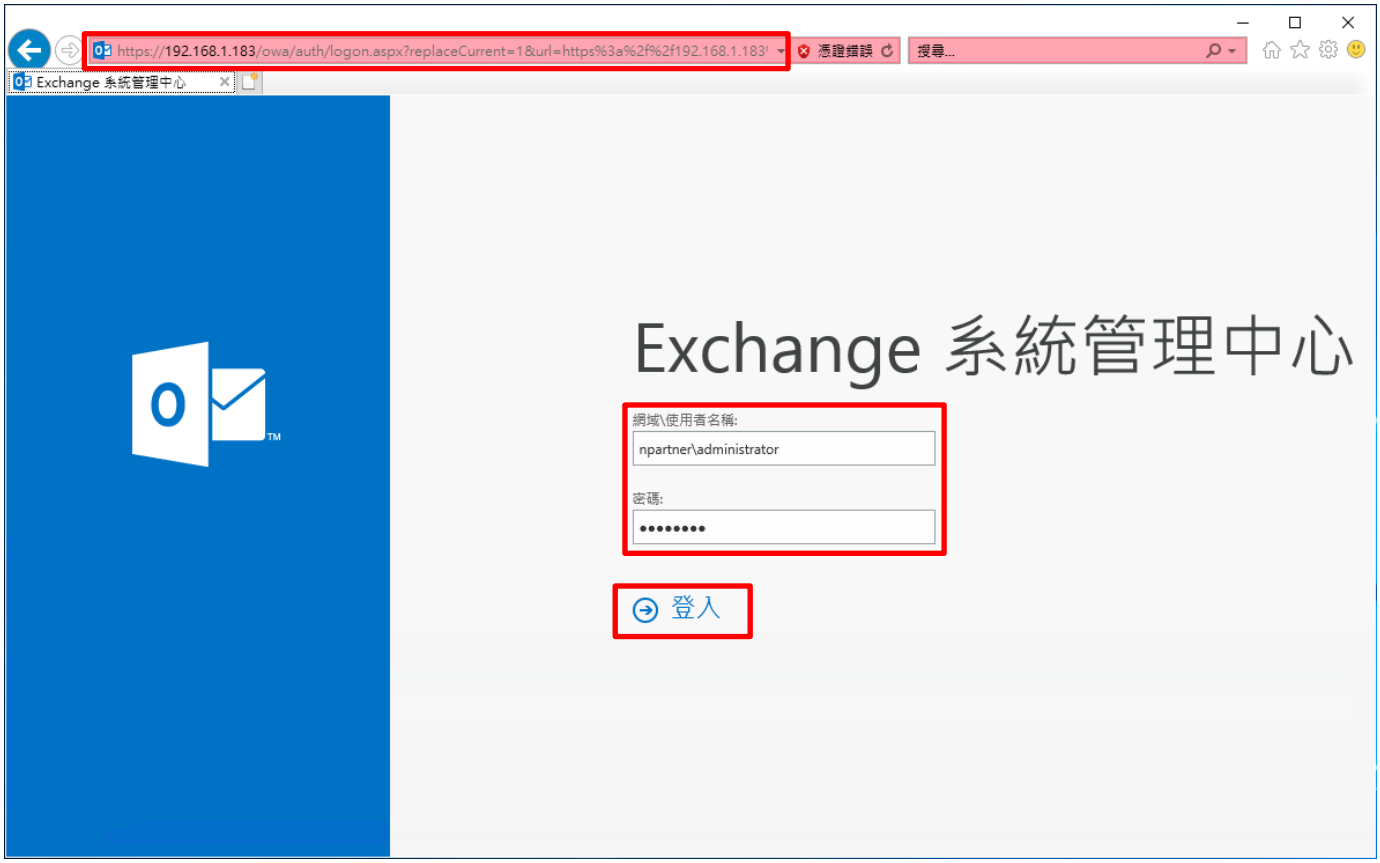
藍色文字部位請修改郵件追蹤記錄資料夾

```
define MailLog    C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

6.1.1 Exchange Administrative Center

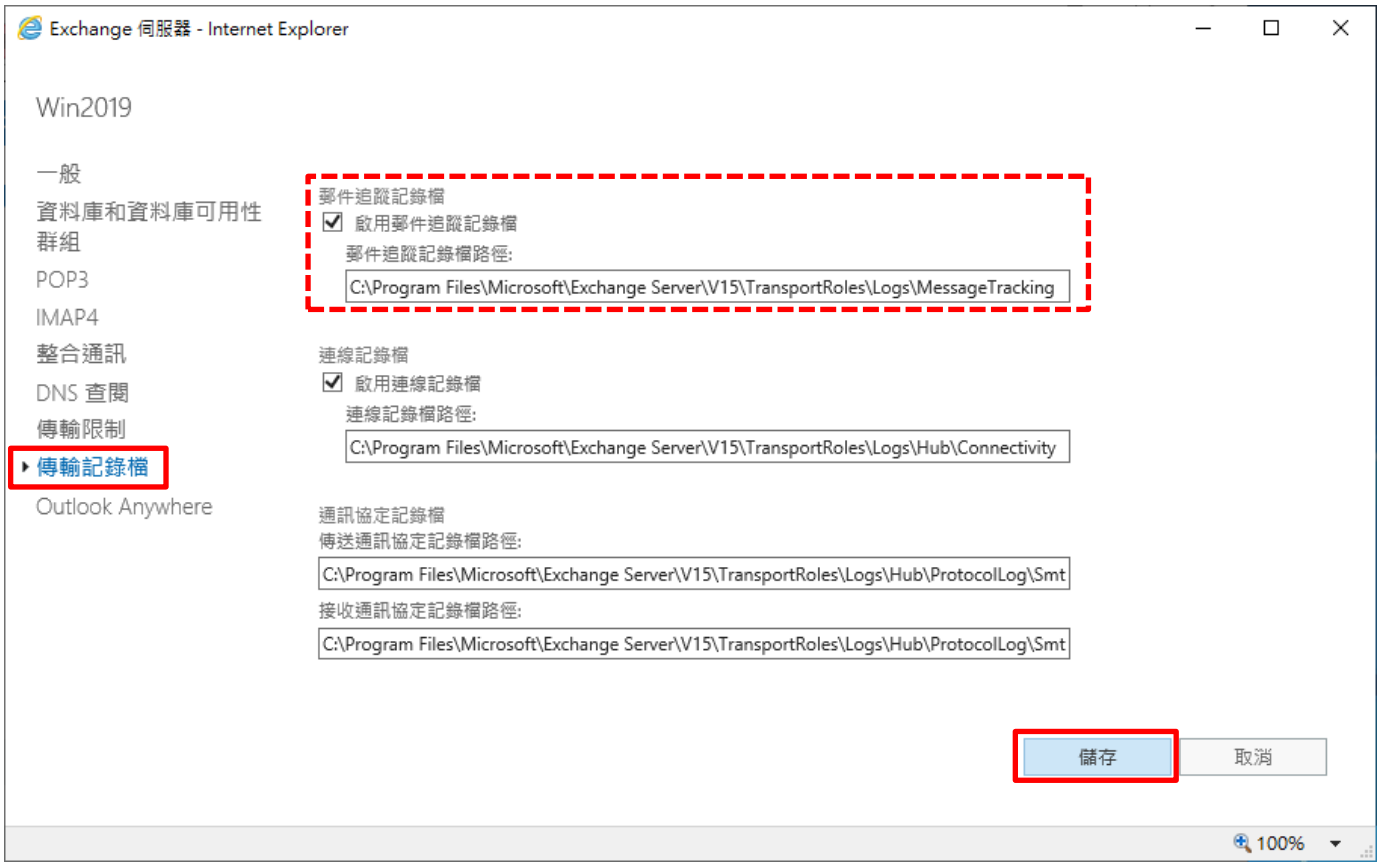
(1) 開啟 [瀏覽器]

(2) URL 輸入 https://<*ExchangeIP*>/ecp -> 輸入網域名稱\管理者帳號和密碼 -> 按下 [登入]



(3) 點選 [伺服器] 頁面 -> [伺服器] -> 選擇 [Mailbox 伺服器(Win2019)] -> 點選 (編輯)

(4) 點選 [傳輸記錄檔] -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking] -> 按下 [儲存]

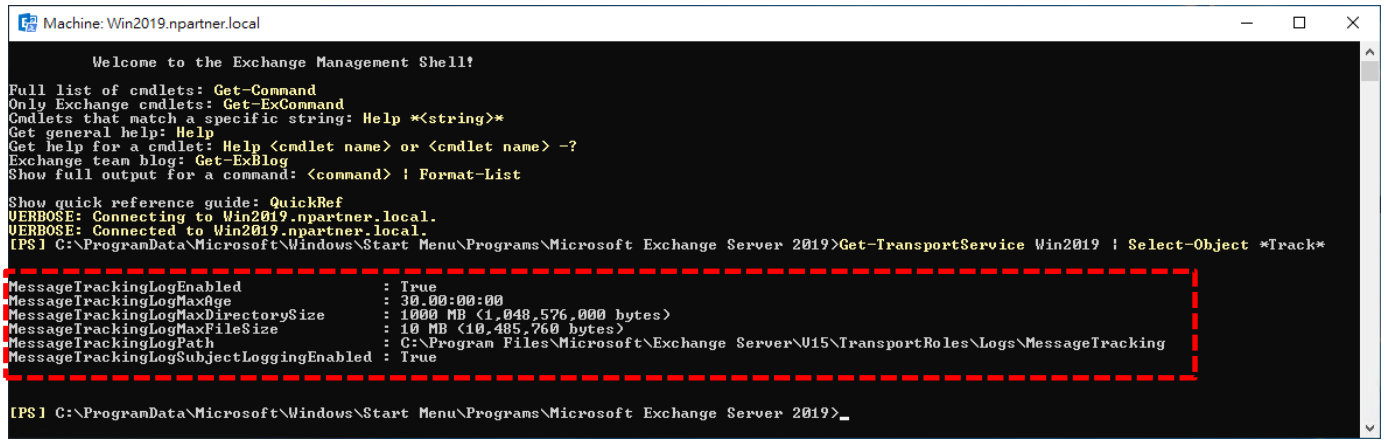


6.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]

(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]

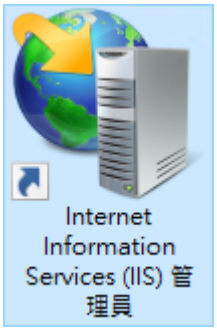
```
[PS] C:\> Get-TransportService Win2019 | Select-Object *Track*
```



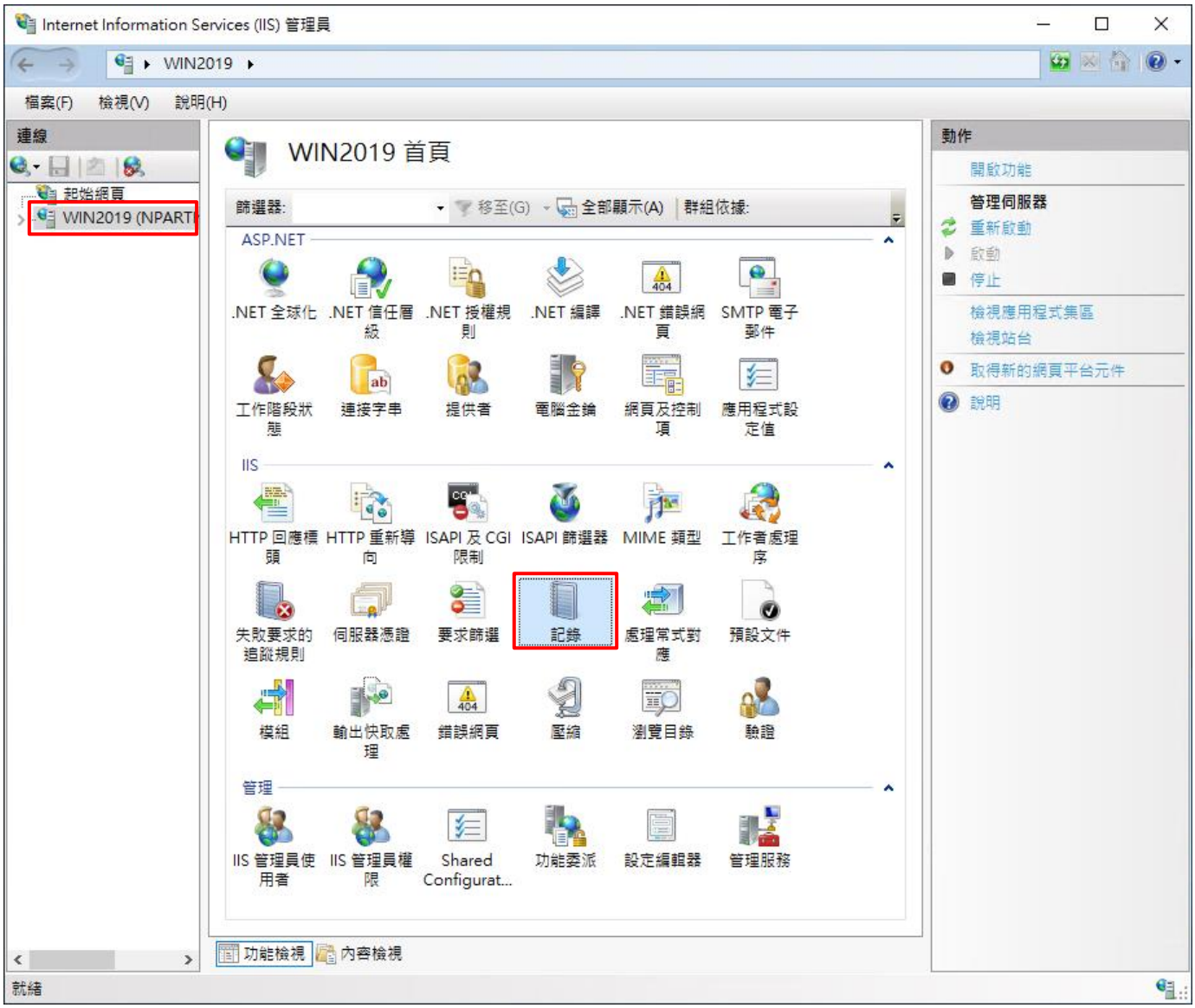
紅色文字部位請輸入 Exchange 伺服器名稱

6.2 IIS Log

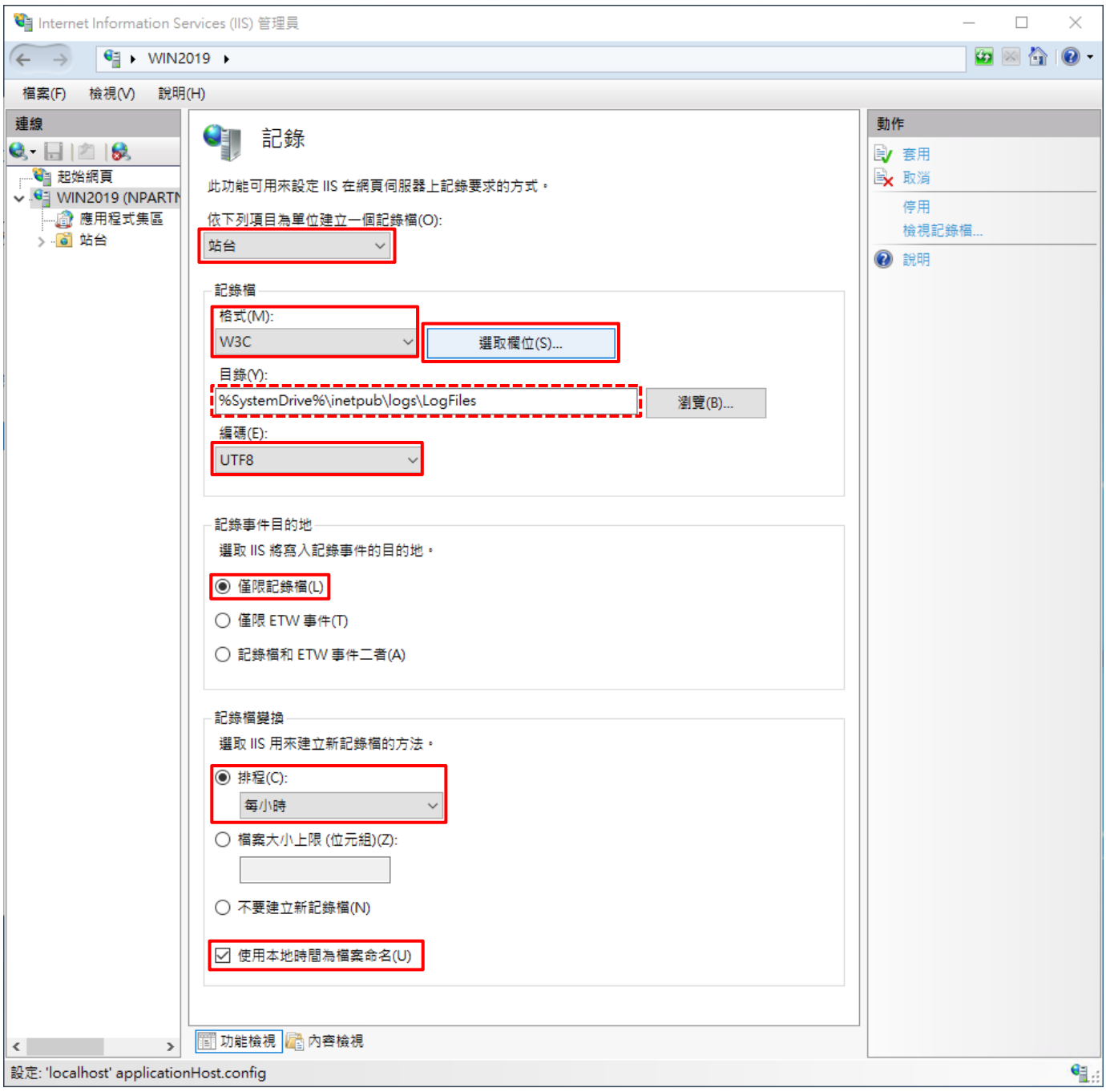
(1) 開啟 [Internet Information Services (IIS) 管理員]



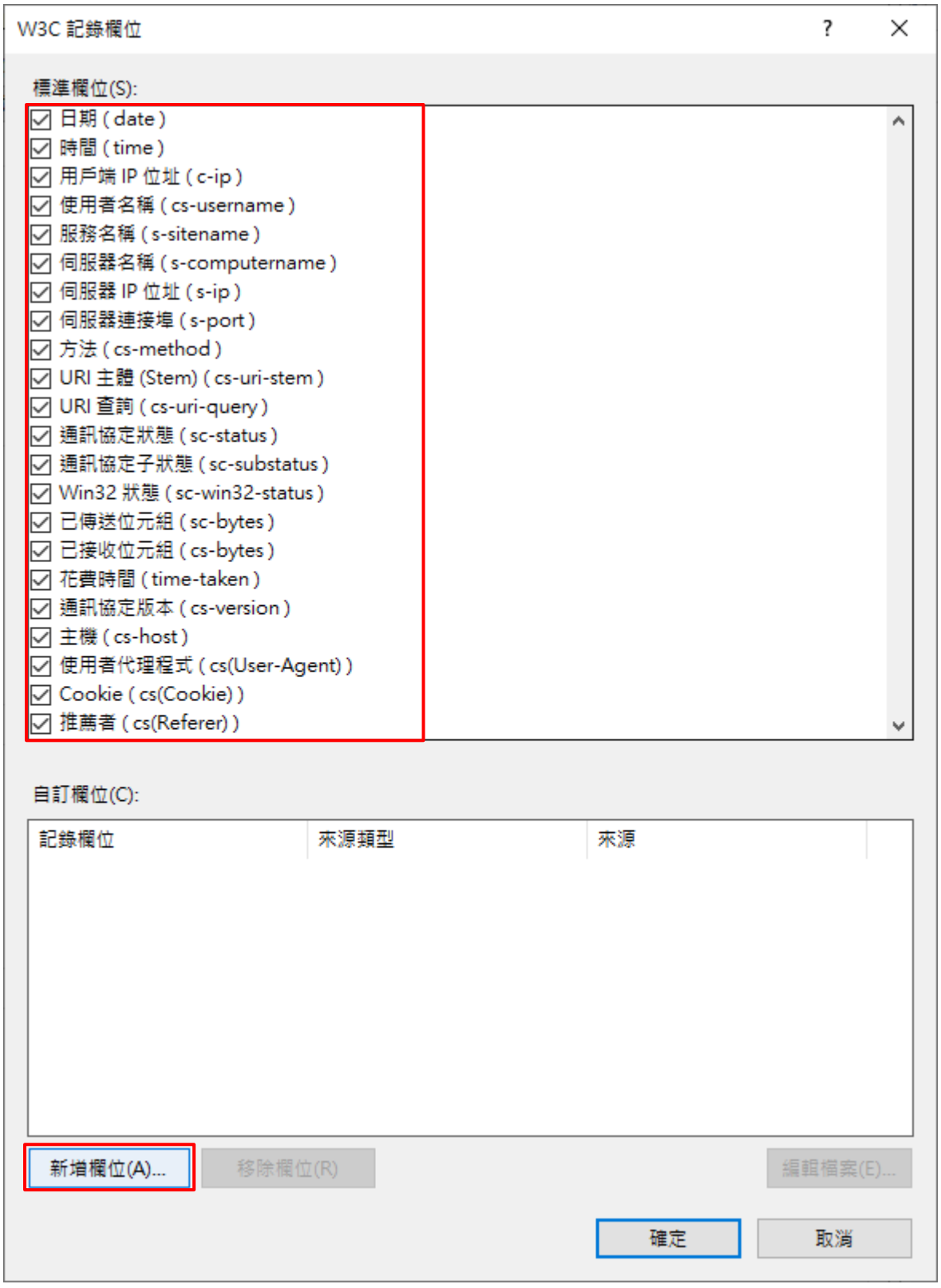
(2) 選擇 [IIS 伺服器] -> 點選 [記錄]



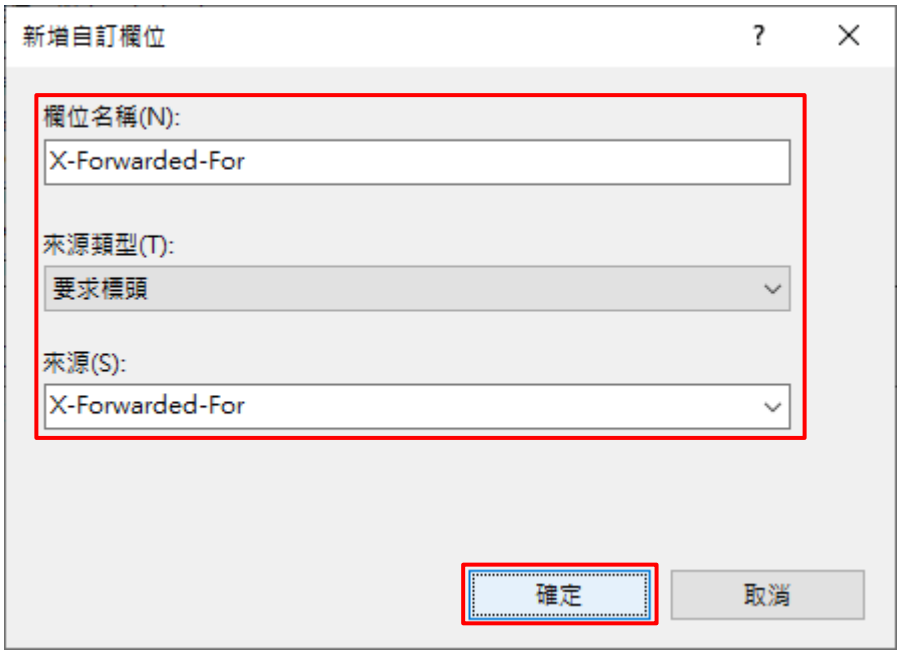
(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄: [%SystemDrive%\inetpub\logs\LogFiles] -> 編碼: [UTF-8] -> 記錄事件目的地: [僅限記錄檔] -> 排程: [每小時] -> 勾選 [使用本地時間為檔案命名] -> 按下 [選取檔位]



(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(cs-version)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [新增欄位]

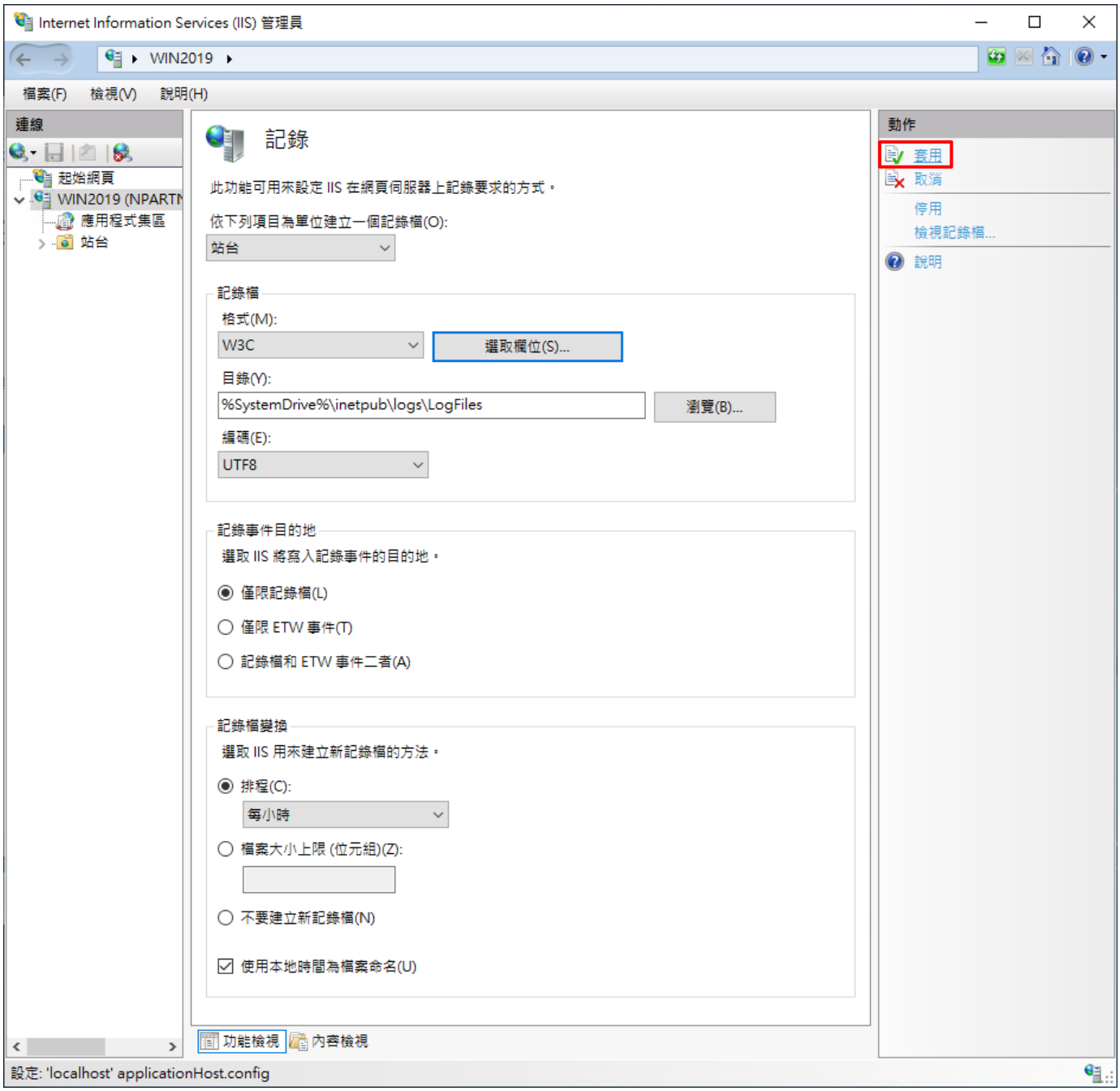


(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [要求標頭] -> 輸入來源: X-Forwarded-For -> 按下 [確定]

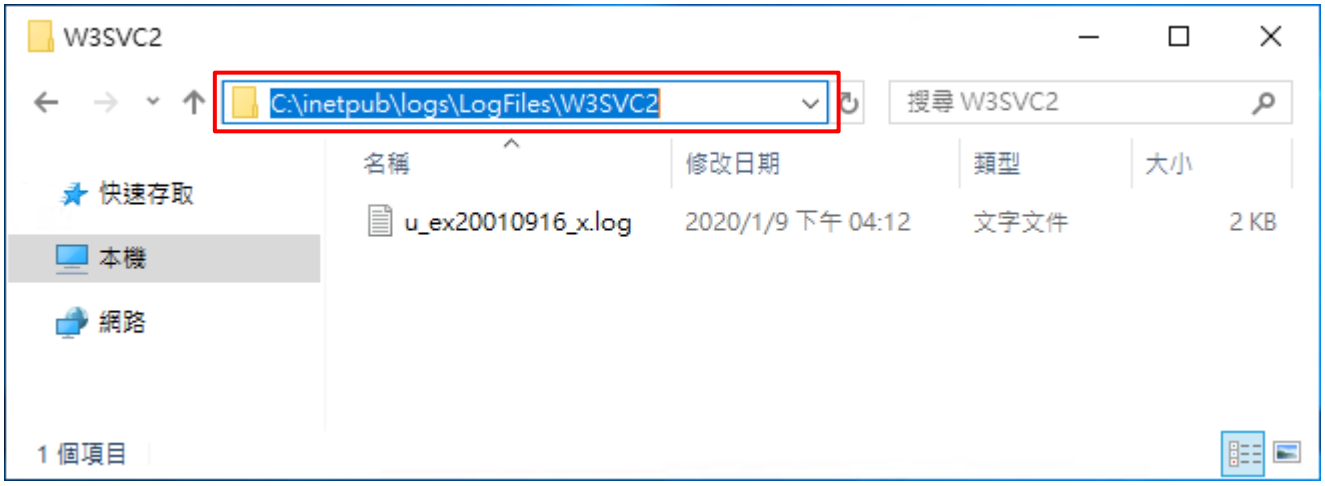


(6) 按下 [確定]

(7) 按下 [套用]



(8) 確認 [C:\ inetpub\logs\LogFiles\W3SVC2] 資料夾 IIS log 檔案: u_ex*.log

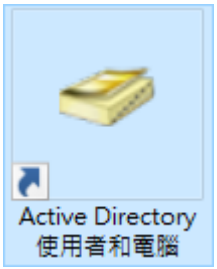


6.3 Event Log

6.3.1 組織單位

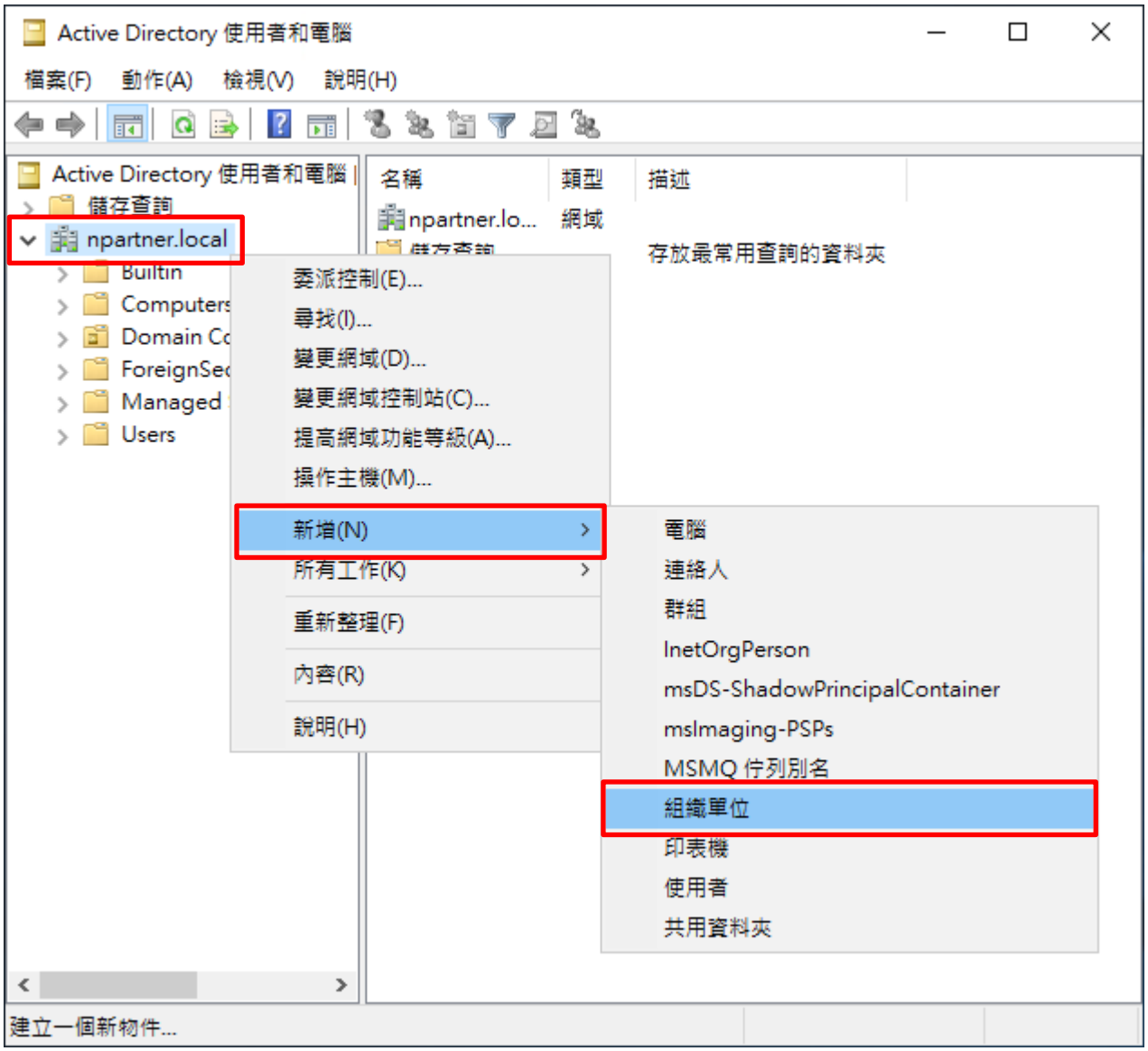
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



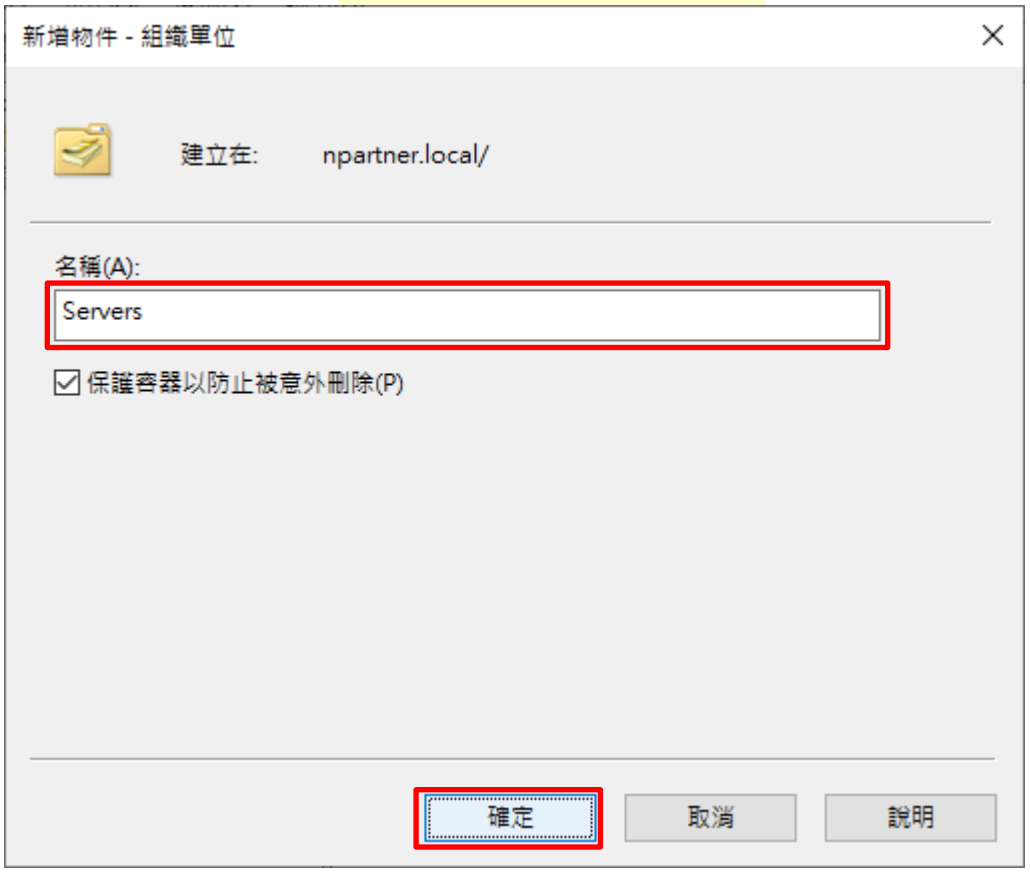
(2) 新增組織單位

在 [網域名稱] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



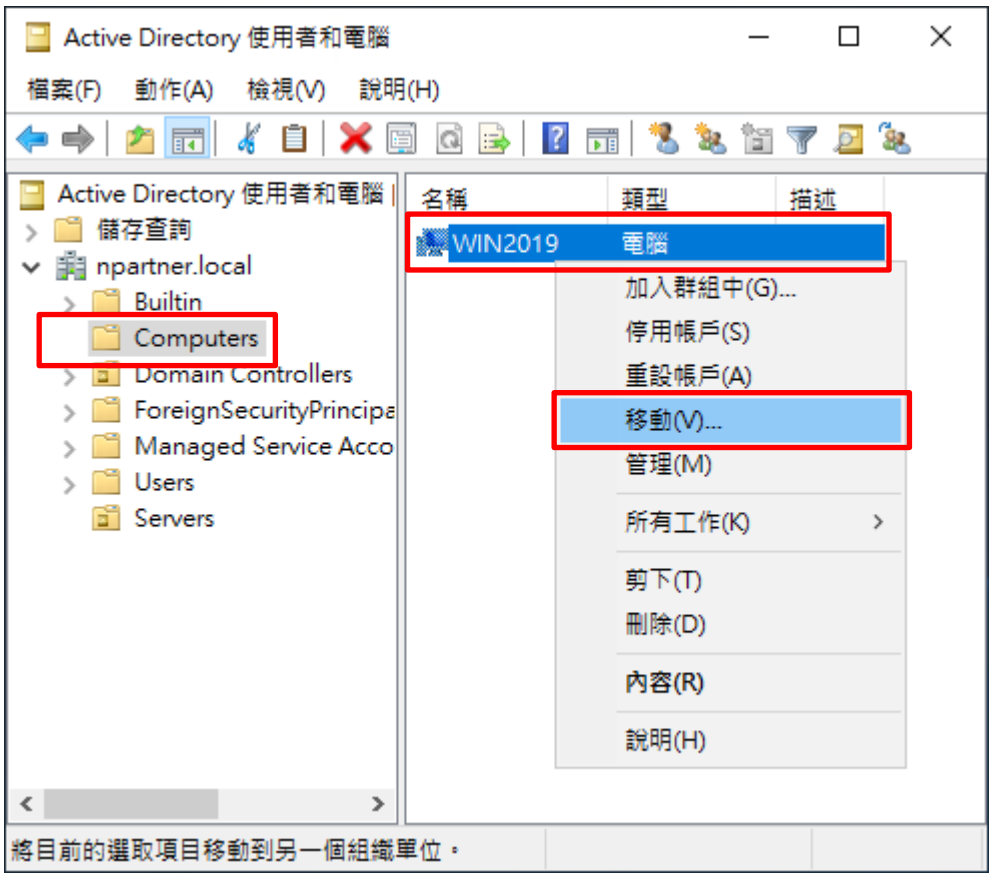
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



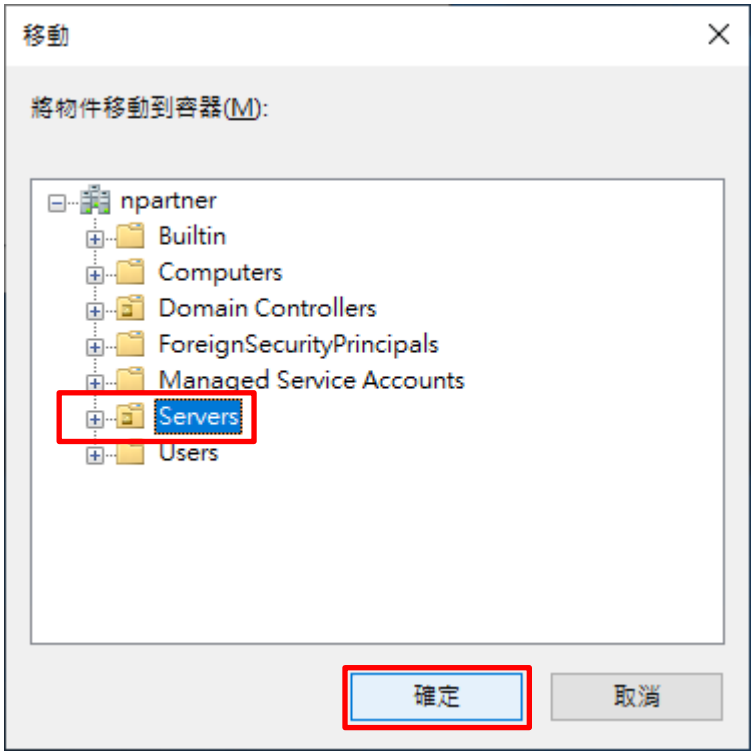
(4) 移動 Exchange 伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2019] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Exchange Server 主機 -> 點選 [移動]



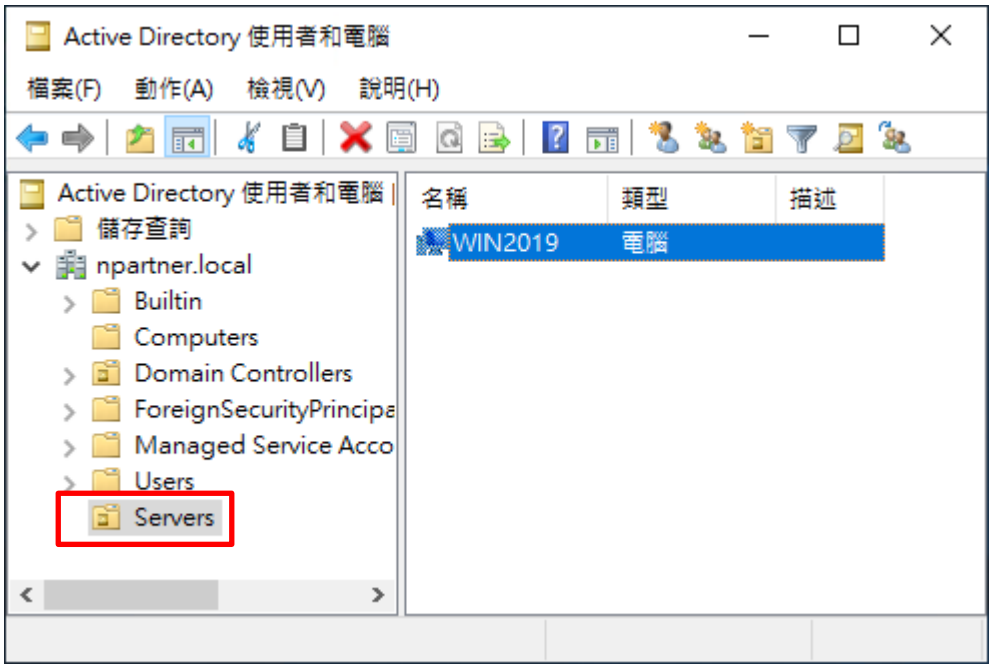
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認 Exchange 伺服器已移動至新的組織單位

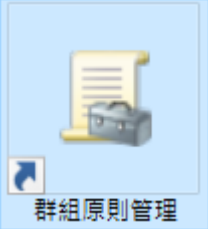
點選 [Servers] 組織單位，確認 Win2019 伺服器已移動。



6.3.2 群組原則

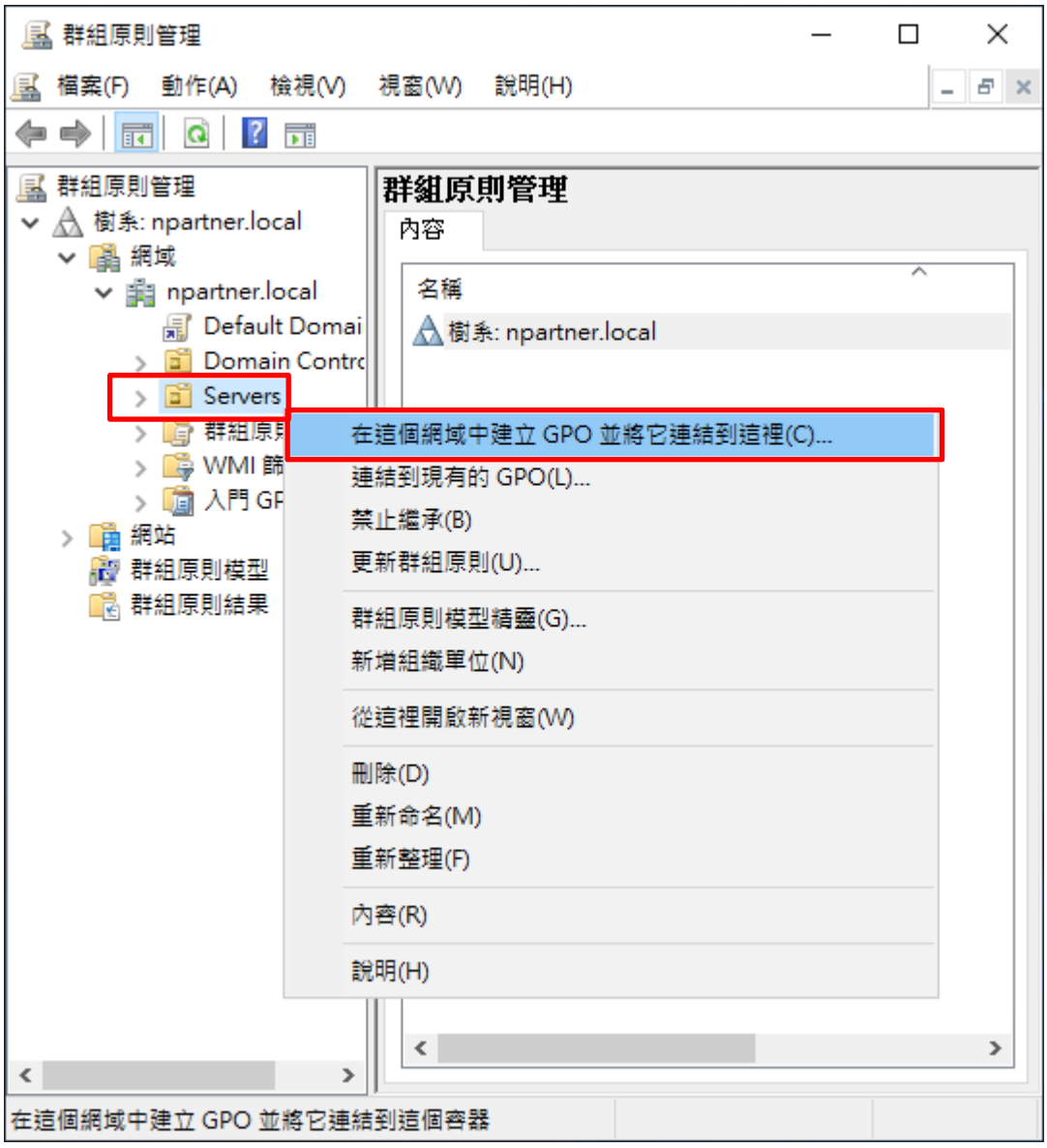
(1) 開啟群組原則管理

開啟 [群組原則管理]



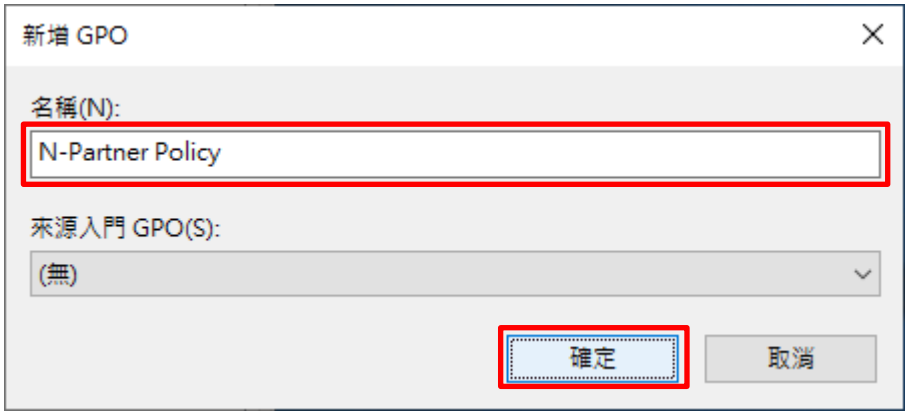
(2) 在 Servers 組織單位，新增群組原則物件

在 [Servers] 組織單位上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]



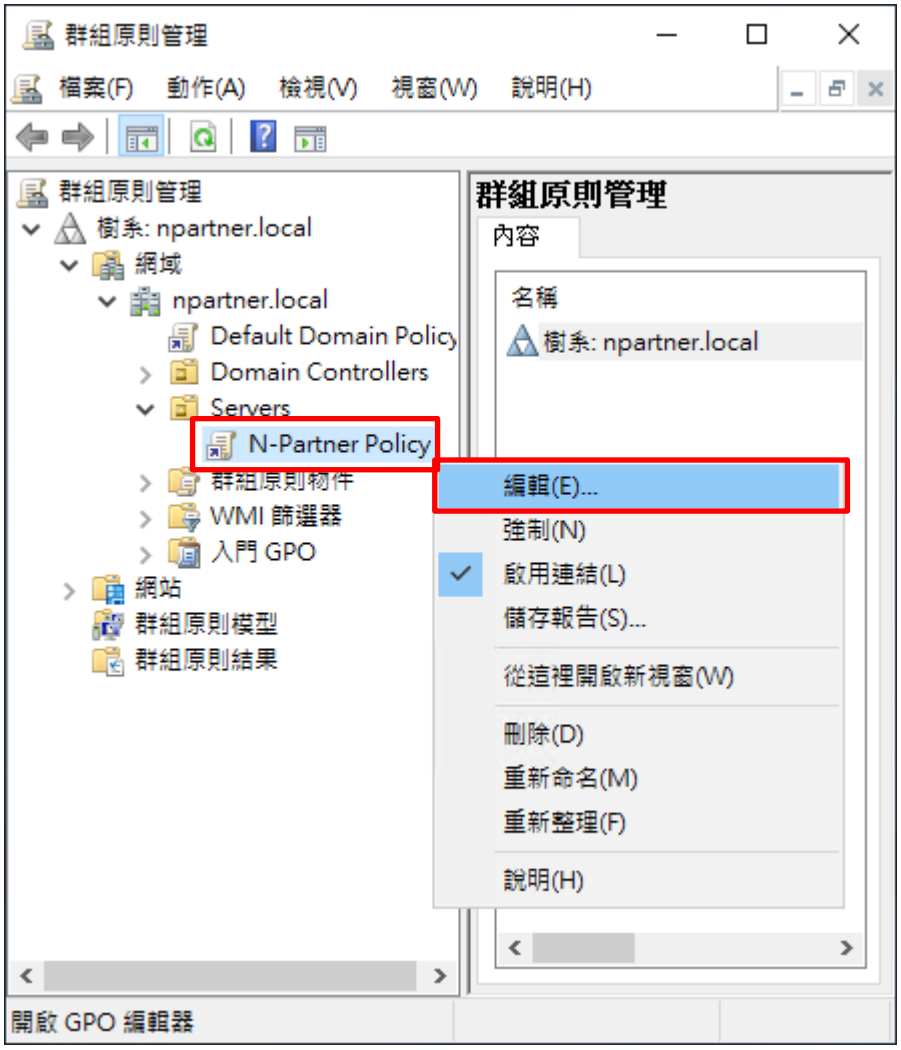
(3) 輸入群組原則物件名稱

輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]



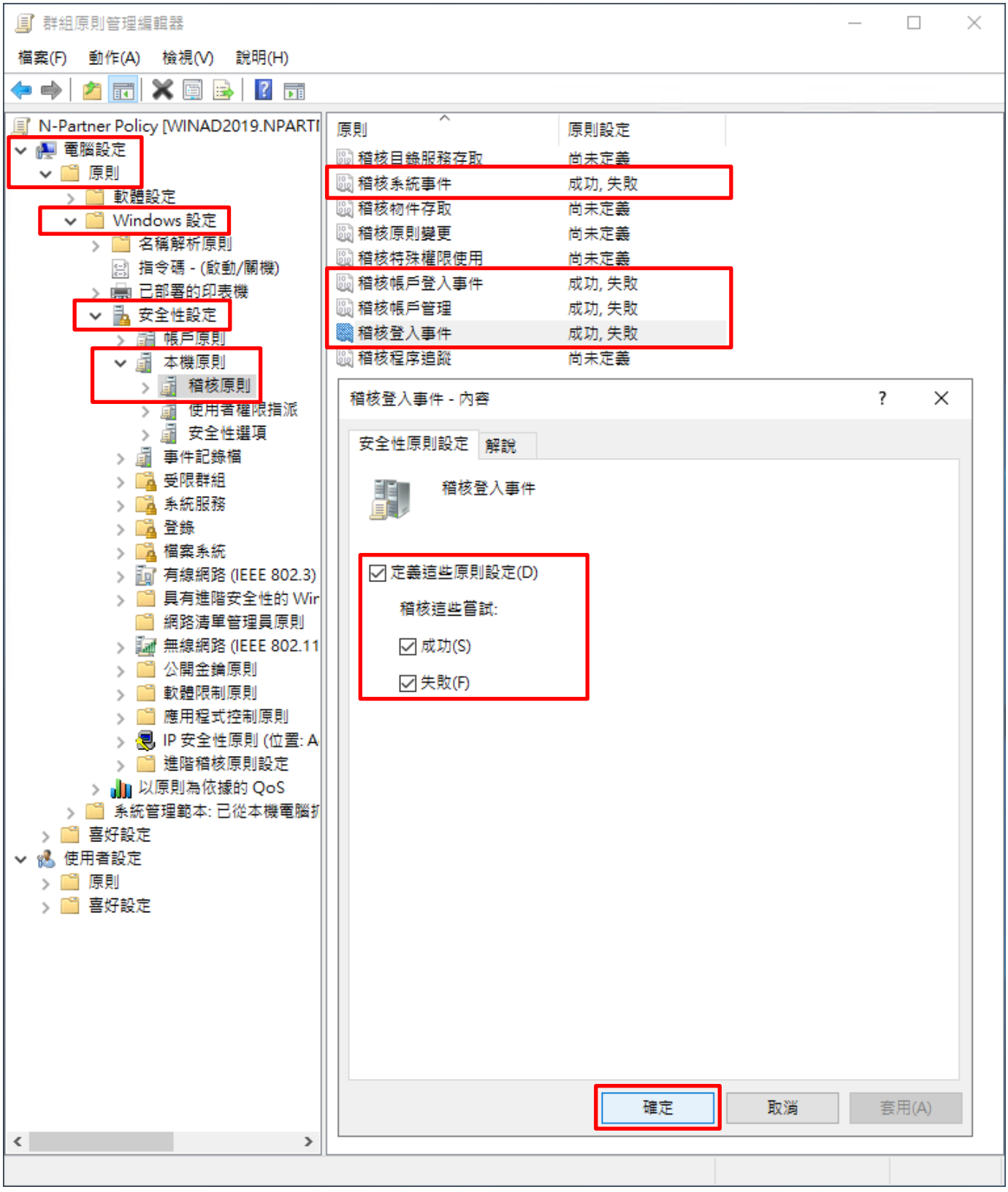
(4) 編輯群組原則物件

在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]



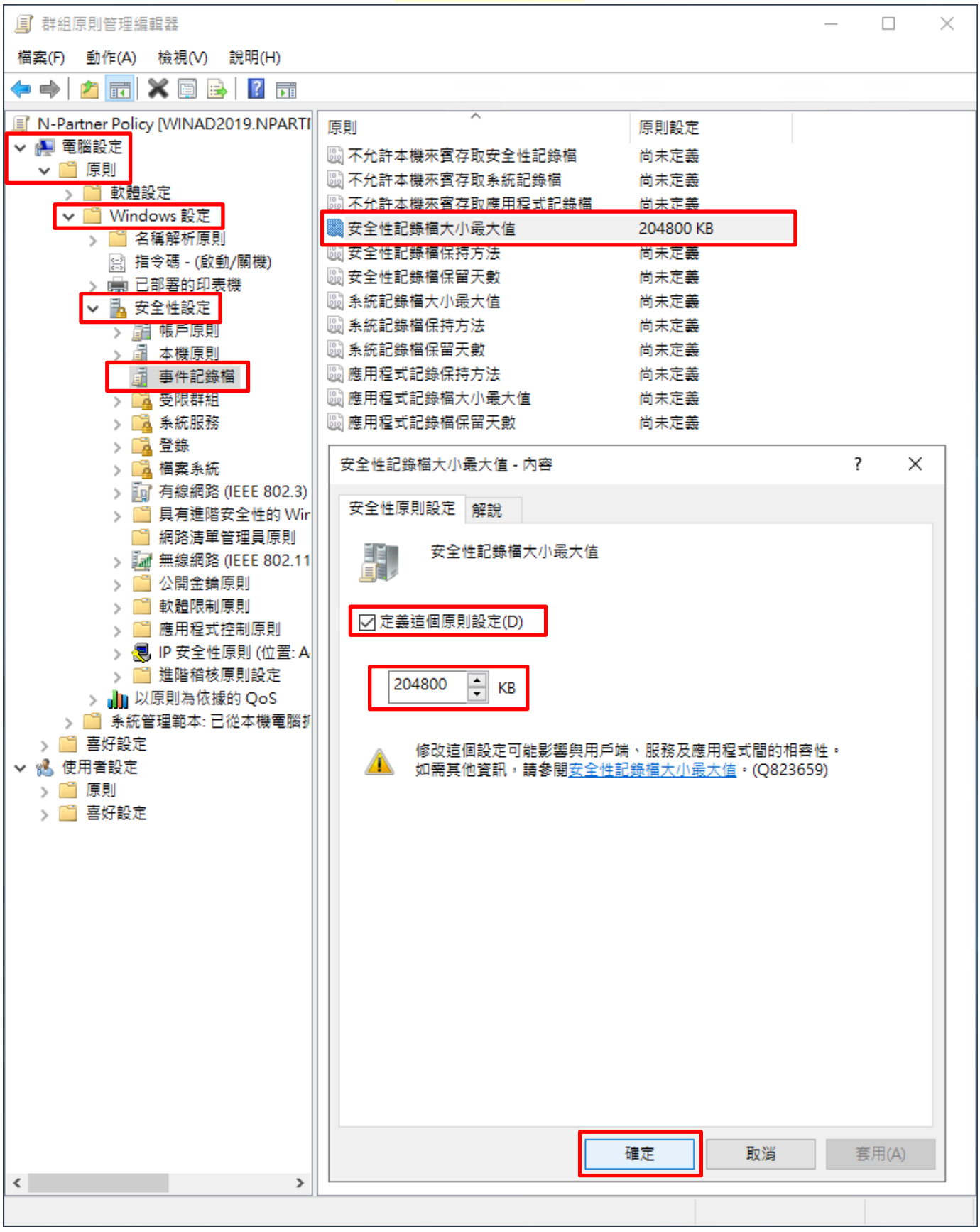
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



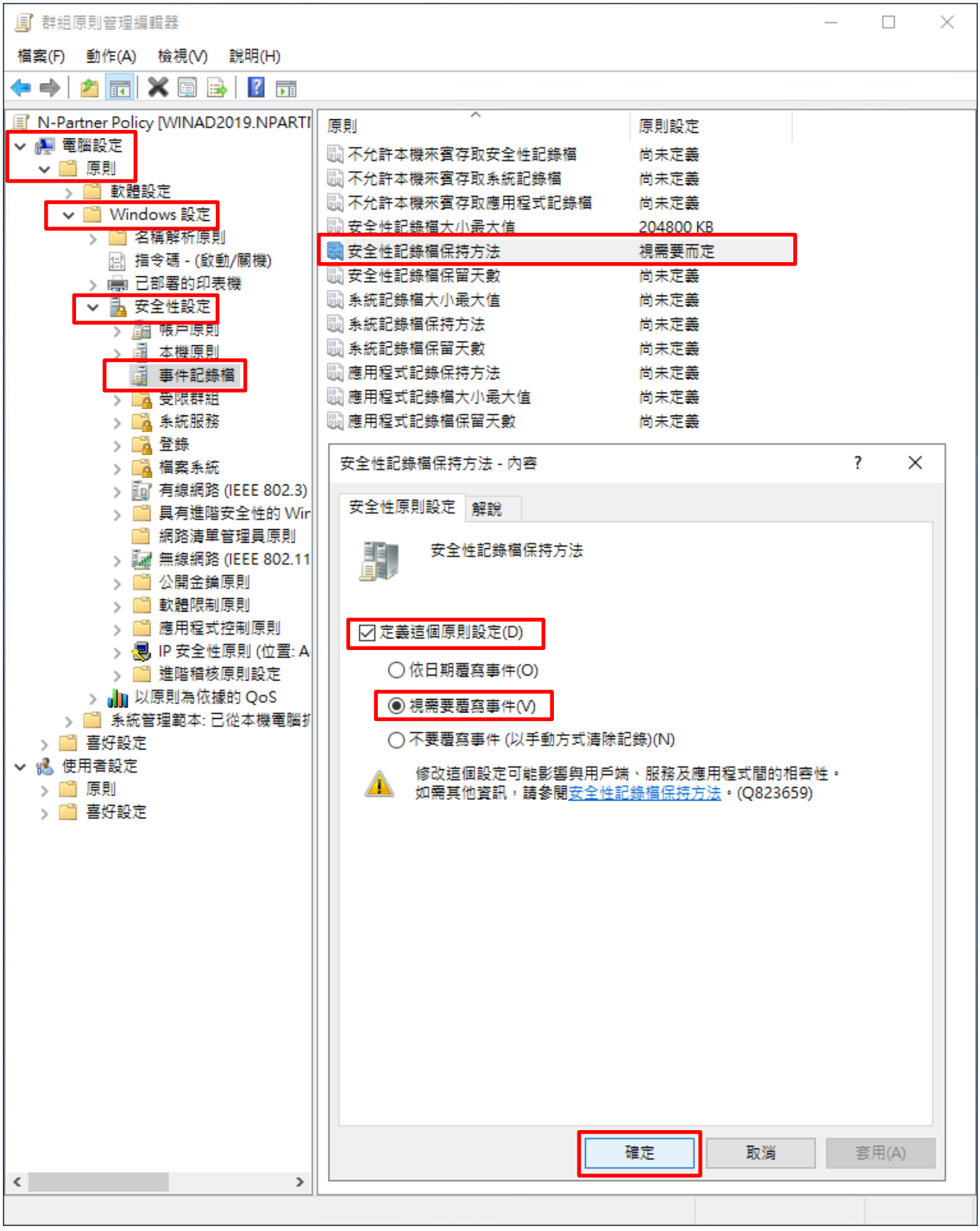
(6) 事件記錄檔：安全性記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

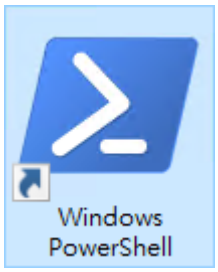


(7) 事件記錄檔：安全性記錄檔保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



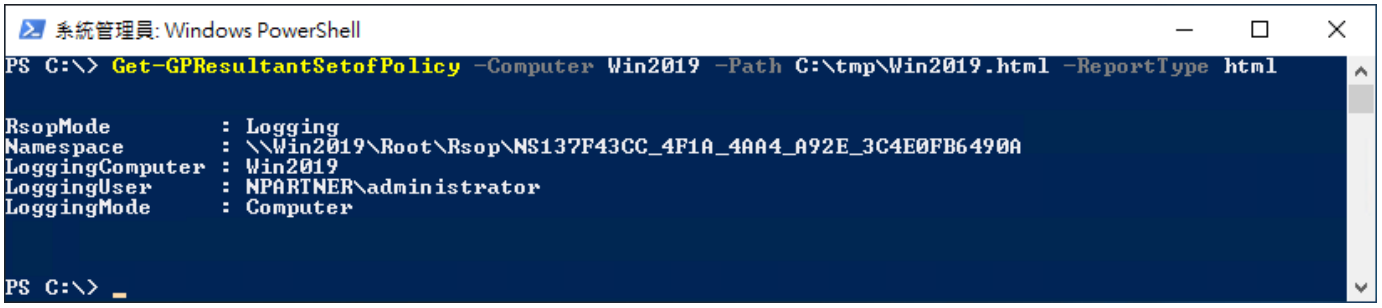
(9) 更新 Exchange Server 群組原則

```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```

紅色文字部位請輸入 Exchange 伺服器名稱

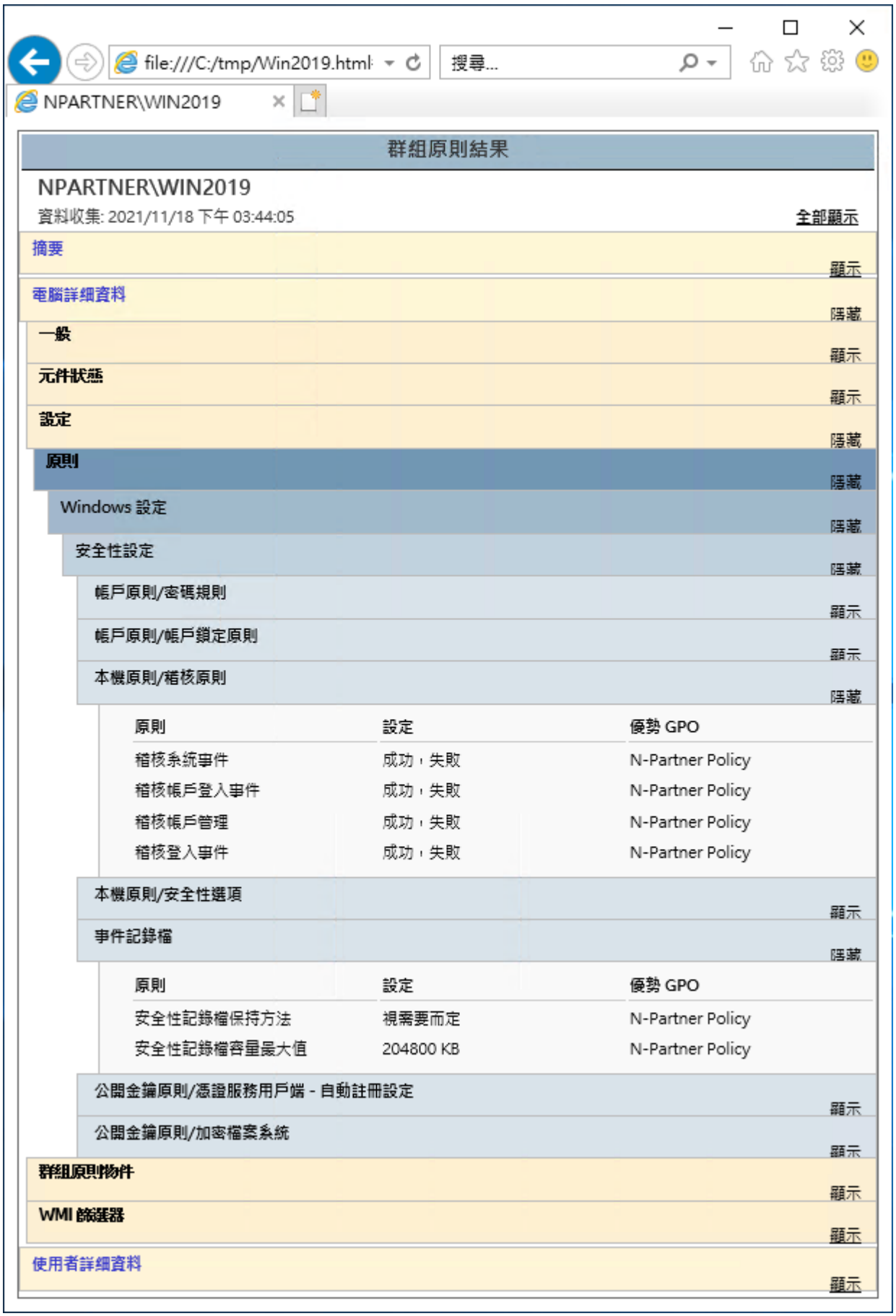
(10) 在 AD 網域伺服器 -> 產生 Exchange 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2019 -Path C:\tmp\Win2019.html -ReportType html
```



紅色文字部位請輸入 Exchange 伺服器名稱和資料夾路徑檔案名稱

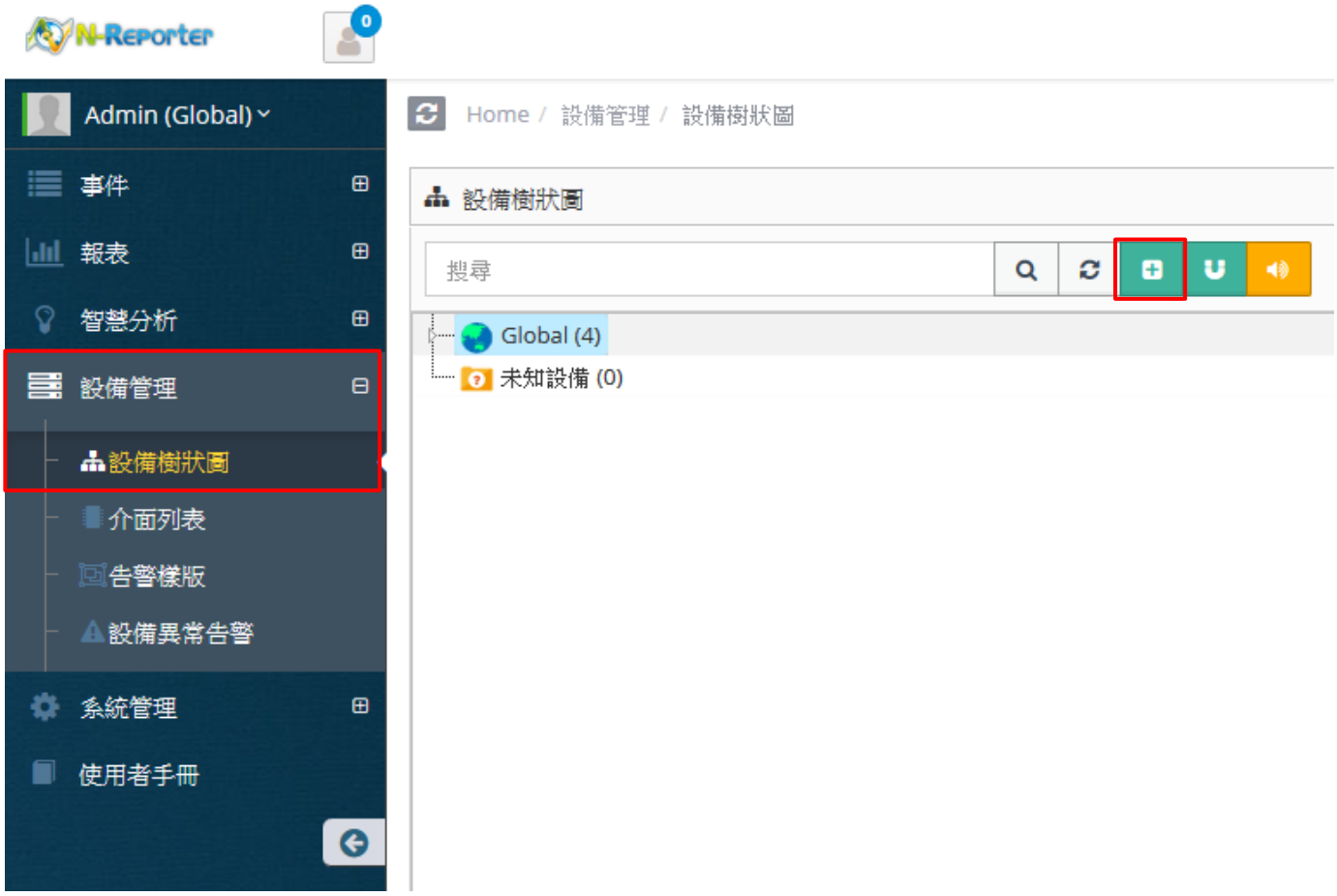
(11) 開啟報表 -> 確認 Exchange 伺服器 -> 套用 N-Partner Policy 群組原則



7. N-Reporter

(1) 新增 MS Exchange 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



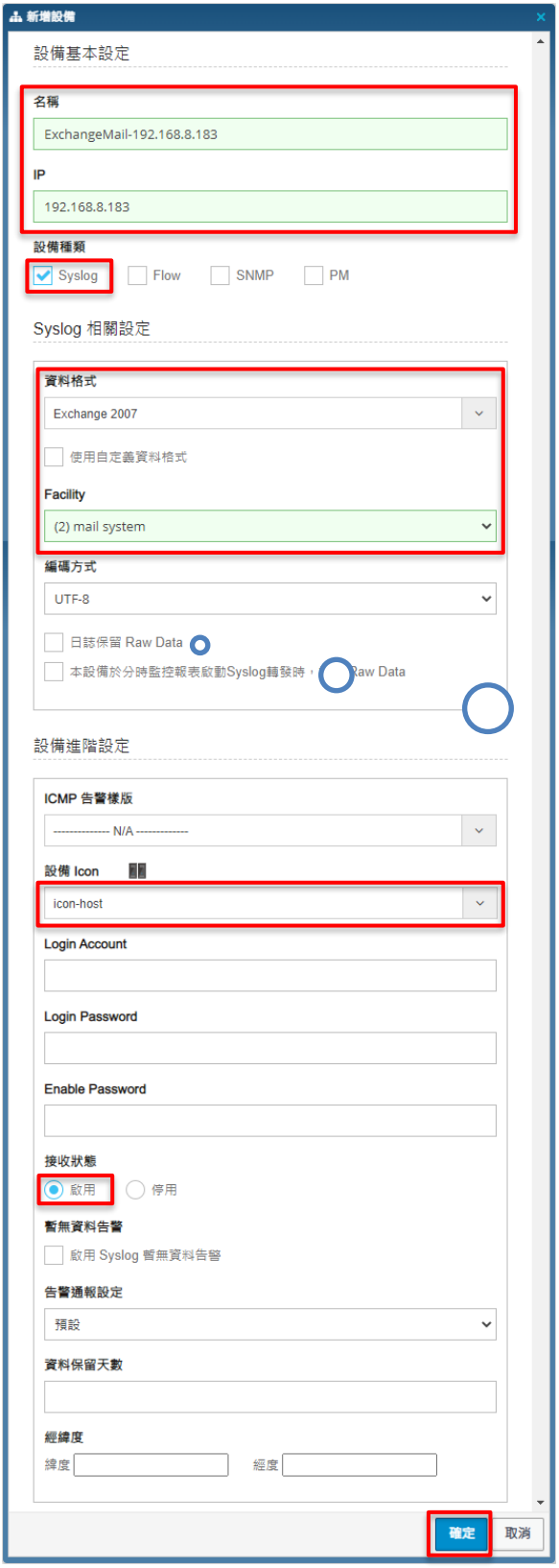
7.1 Exchange Message Trackng Log

7.1.1 Exchange 2007

(2) 設定 Exchange Message Tracking log 設備的資料格式和 Facility

輸入設備名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Exchange 2007] 和 Facility: [(2) mail system] ->

選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



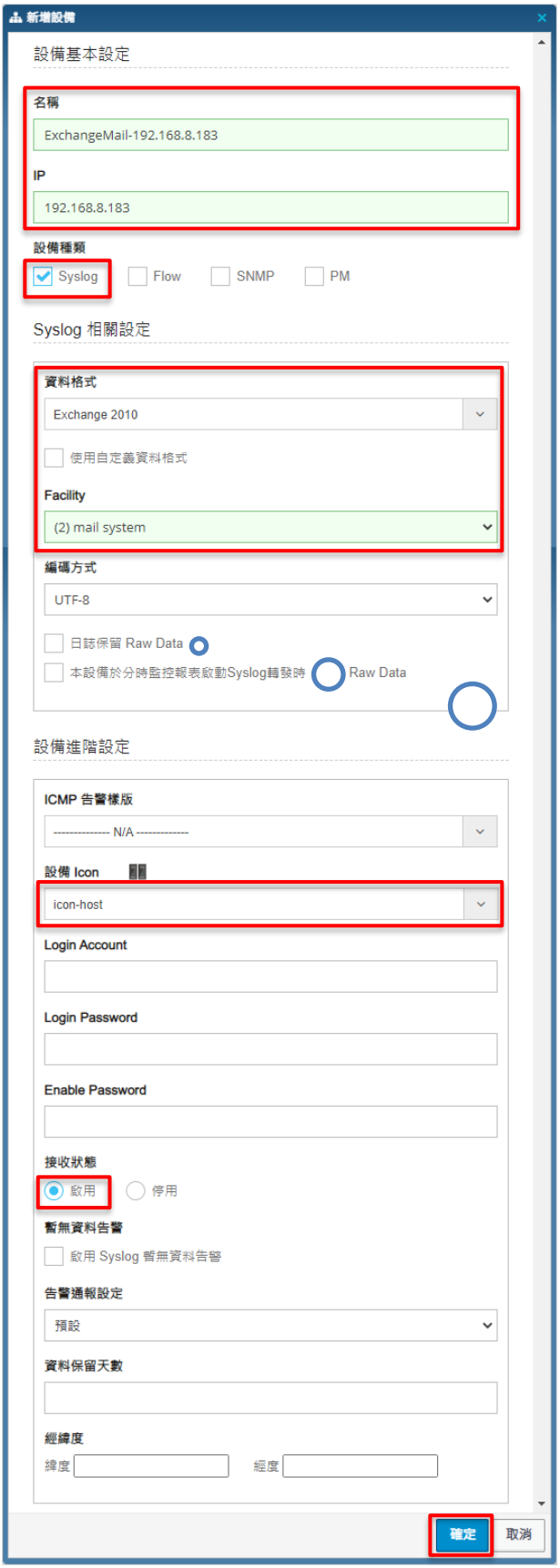
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

7.1.2 Exchange 2010

(2) 設定 Exchange Message Tracking log 設備的資料格式和 Facility

輸入設備名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Exchange 2010] 和 Facility: [(2) mail system] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



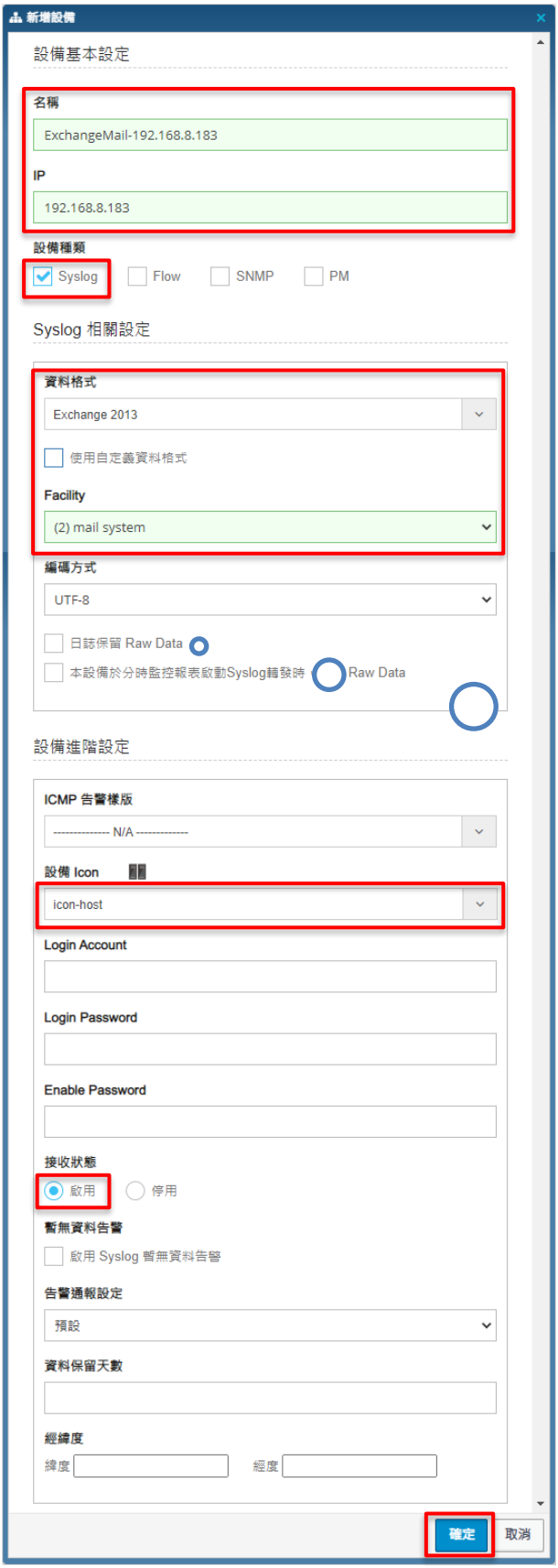
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

7.1.3 Exchange 2013 或之後版本

(2) 設定 Exchange Message Tracking log 設備的資料格式和 Facility

輸入設備名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Exchange 2013] 和 Facility: [(2) mail system] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



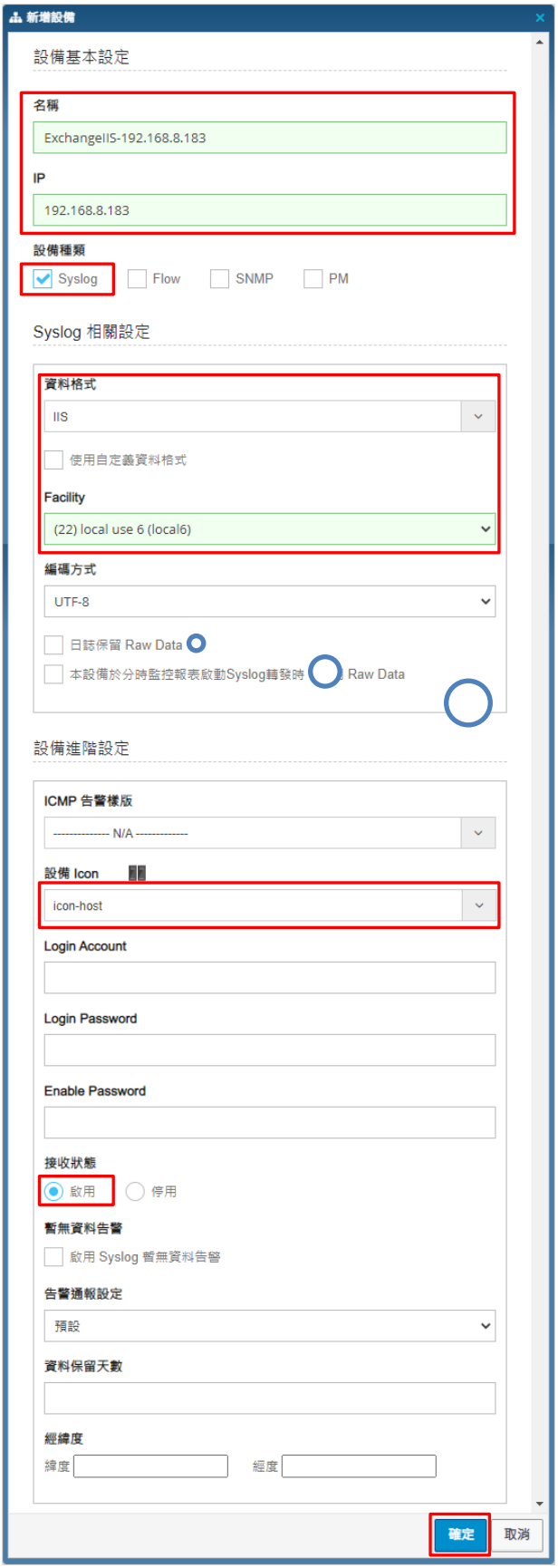
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

7.2 IIS Log

(2) 設定 Exchange IIS log 設備的資料格式和 Facility

輸入設備名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [IIS] 和 Facility: [(22) local use 6 (local6)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



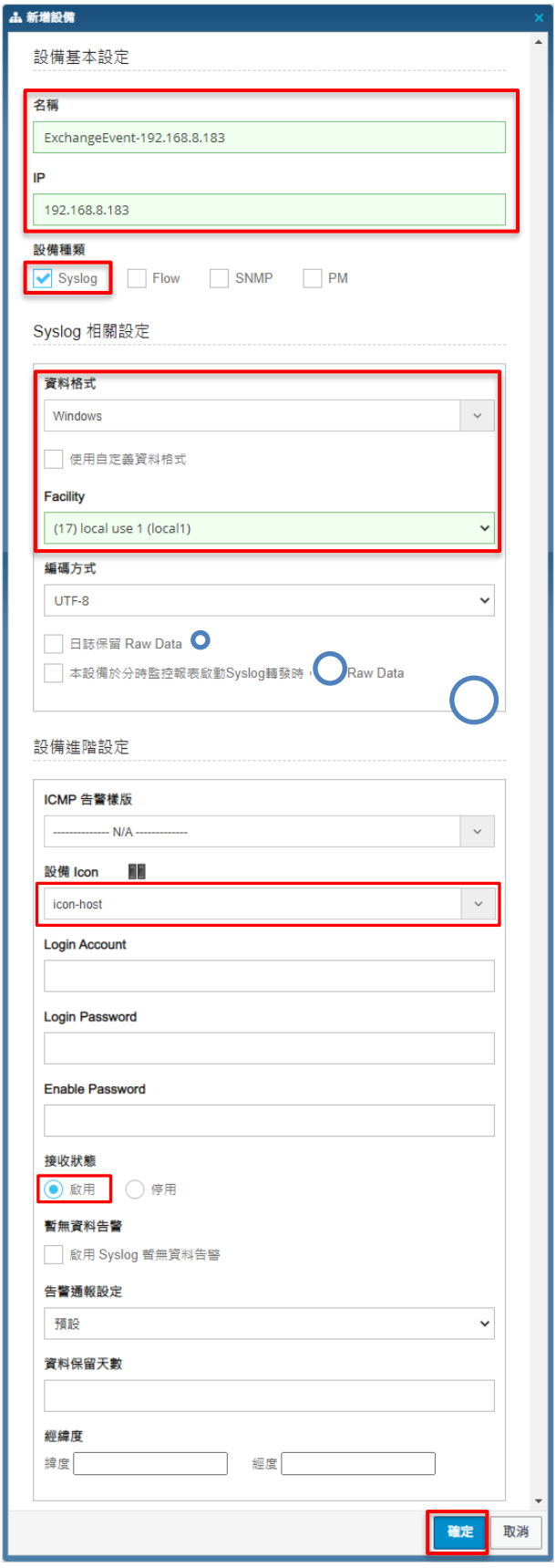
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

7.3 Event Log

(2) 設定 Exchange Event log 設備的資料格式和 Facility

輸入設備名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] 和 Facility: [(17) local use 1 (local1)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



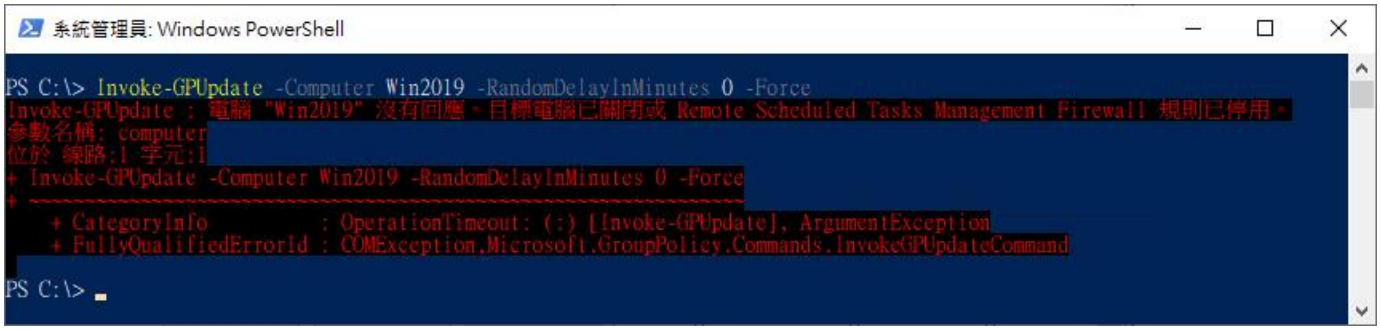
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

8. 問題排除

8.1 Invoke-GPUpdate 錯誤

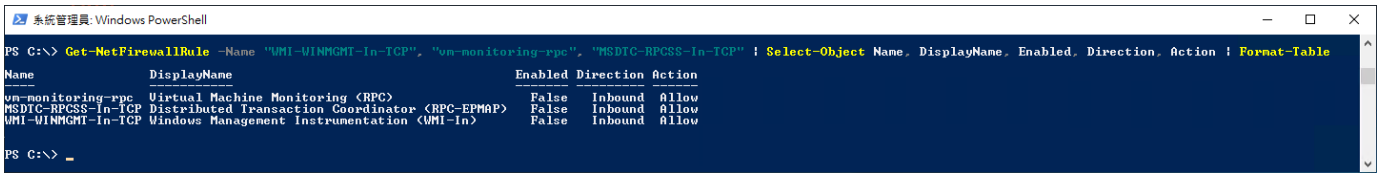
(1) 在 AD 網域伺服器 -> 執行 Invoke-GPUpdate 更新 Windows Server 群組原則出現錯誤訊息



(2) 在 Windows Server 開啟 [Windows PowerShell]

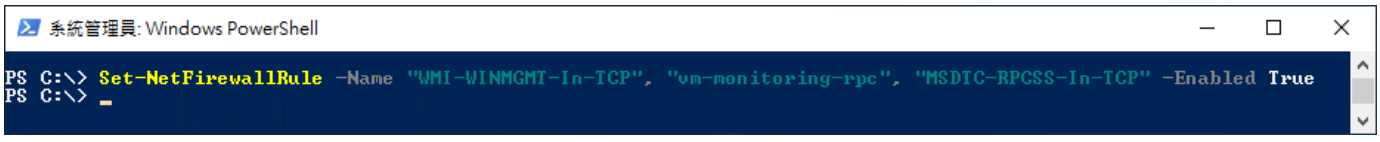
(3) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



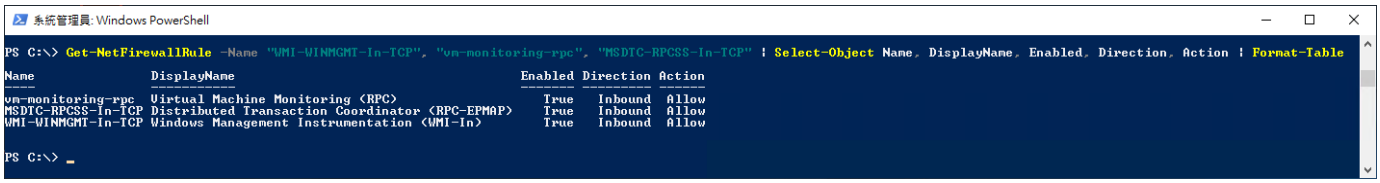
(4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
```



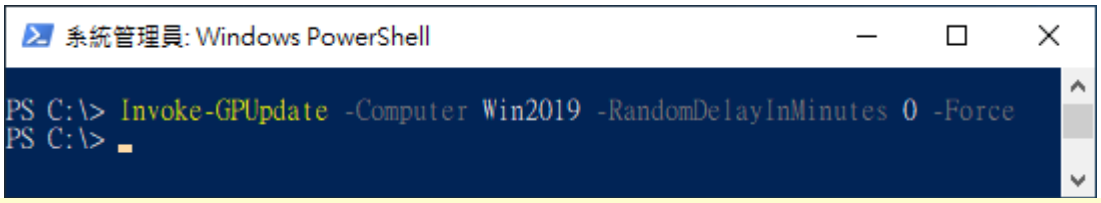
(5) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```

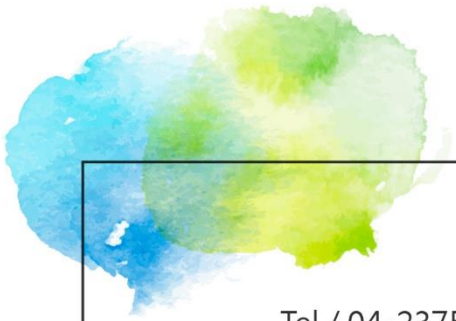


(6) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱



Tel / 04-23752865 Fax / 04-23757458
業務詢問 / sales@npartnertech.com
技術詢問 / support@npartnertech.com