

Partner

如何設定

MS Exchange 郵件追蹤記錄

V018

2024/04/16



版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言	2	6.3.1 組織單位.....	116
1. NXLog	3	6.3.2 群組原則.....	120
1.1 NXLog 安裝.....	3	7. N-Reporter	127
1.2 NXLog 設定檔下載.....	5	7.1 Exchange Message Tracking Log.....	128
1.3 NXLog 設定檔.....	6	7.1.1 Exchange 2007	128
1.4 NXLog 啟動服務.....	8	7.1.2 Exchange 2010	129
2. Exchange 2007	11	7.1.3 Exchange 2013 或之後版本	130
2.1 Exchange MessageTracking Log.....	11	7.2 IIS Log.....	131
2.1.1 Exchange 管理主控台	11	7.3 Event Log.....	132
2.1.2 Exchange 管理命令介面.....	13	8. 問題排除.....	133
2.2 IIS Log.....	14	8.1 Invoke-GPUUpdate 錯誤.....	133
2.3 Event Log.....	20		
2.3.1 組織單位.....	20		
2.3.2 群組原則.....	24		
3. Exchange 2010	32		
3.1 Exchange Message Tracking Log.....	32		
3.1.1 Exchange Management Console	32		
3.1.2 Exchange Management Shell	34		
3.2 IIS Log.....	35		
3.3 Event Log.....	51		
3.3.1 組織單位.....	51		
3.3.2 群組原則.....	54		
4. Exchange 2013	61		
4.1 Exchange Message Tracking Log.....	61		
4.1.1 Exchange Administrative Center.....	61		
4.1.2 Exchange Management Shell	64		
4.2 IIS Log.....	65		
4.3 Event Log.....	72		
4.3.1 組織單位.....	72		
4.3.2 群組原則.....	76		
5. Exchange 2016	83		
5.1 Exchange Message Tracking Log.....	83		
5.1.1 Exchange Administrative Center.....	83		
5.1.2 Exchange Management Shell	86		
5.2 IIS Log.....	87		
5.3 Event Log.....	94		
5.3.1 組織單位.....	94		
5.3.2 群組原則.....	98		
6. Exchange 2019	105		
6.1 Exchange Message Tracking Log.....	105		
6.1.1 Exchange Administrative Center.....	105		
6.1.2 Exchange Management Shell	108		
6.2 IIS Log.....	109		
6.3 Event Log.....	116		

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

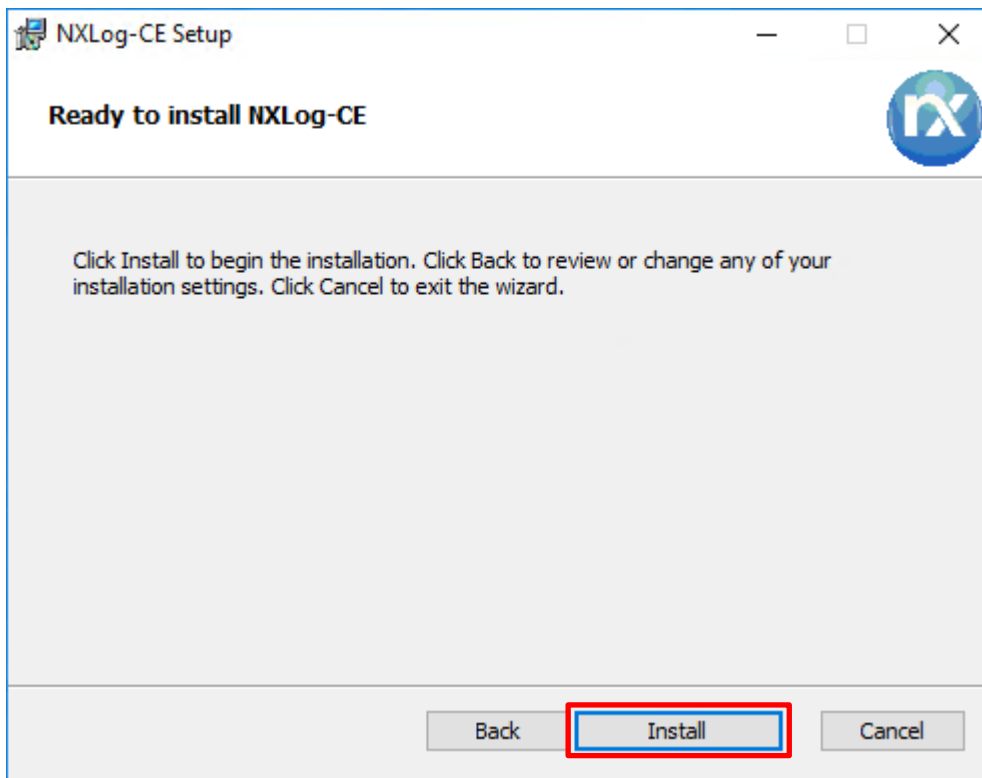
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```

```
系統管理員: Windows PowerShell
PS C:\> Install-Package .\nxlog-ce-3.0.2272.msi -Force
Name                Version            Source              Summary
-----                -
NXLog-CE            3.0.2272          C:\nxlog-ce-3...
PS C:\> _
```

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
```

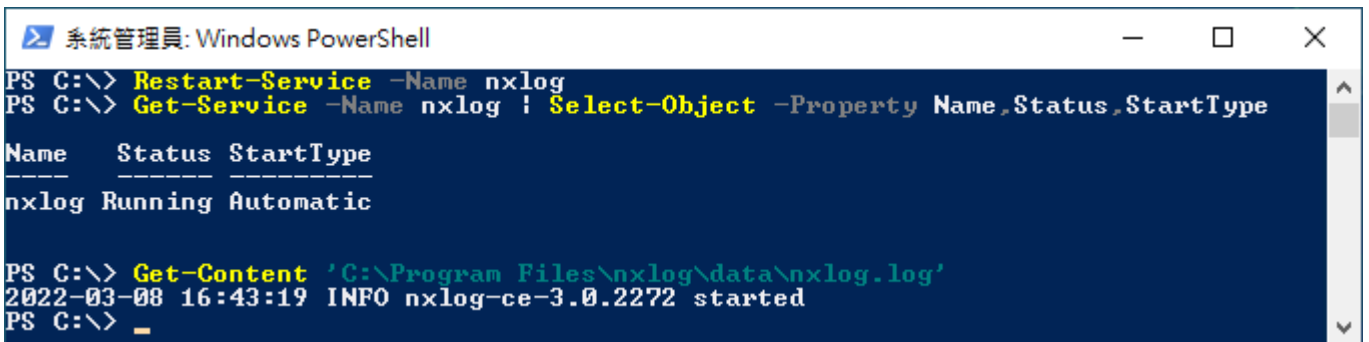
1.4 NXLog 啟動服務

(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'
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the following commands and output:

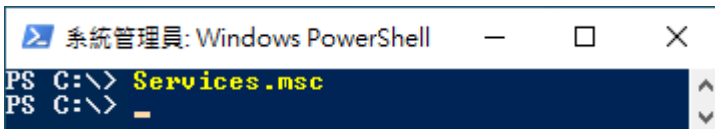
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name      Status StartType
-----
nxlog     Running Automatic

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2022-03-08 16:43:19 INFO nxlog-ce-3.0.2272 started
PS C:\> _
```

(3) 開啟 [服務] 功能

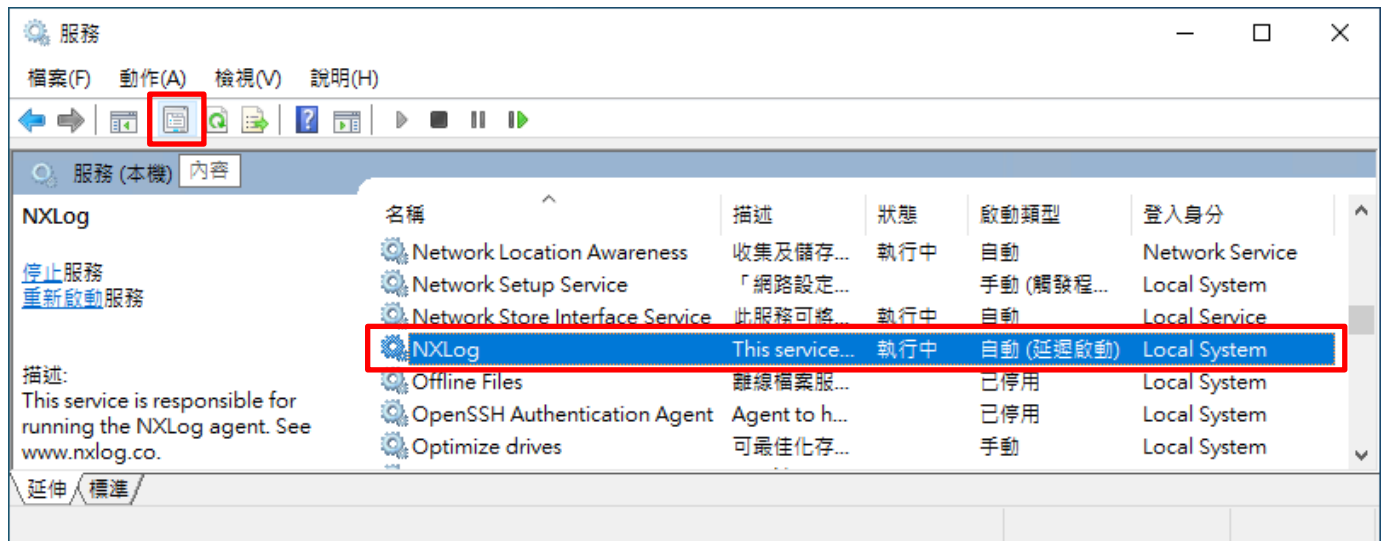
```
PS C:\> Services.msc
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the following commands and output:

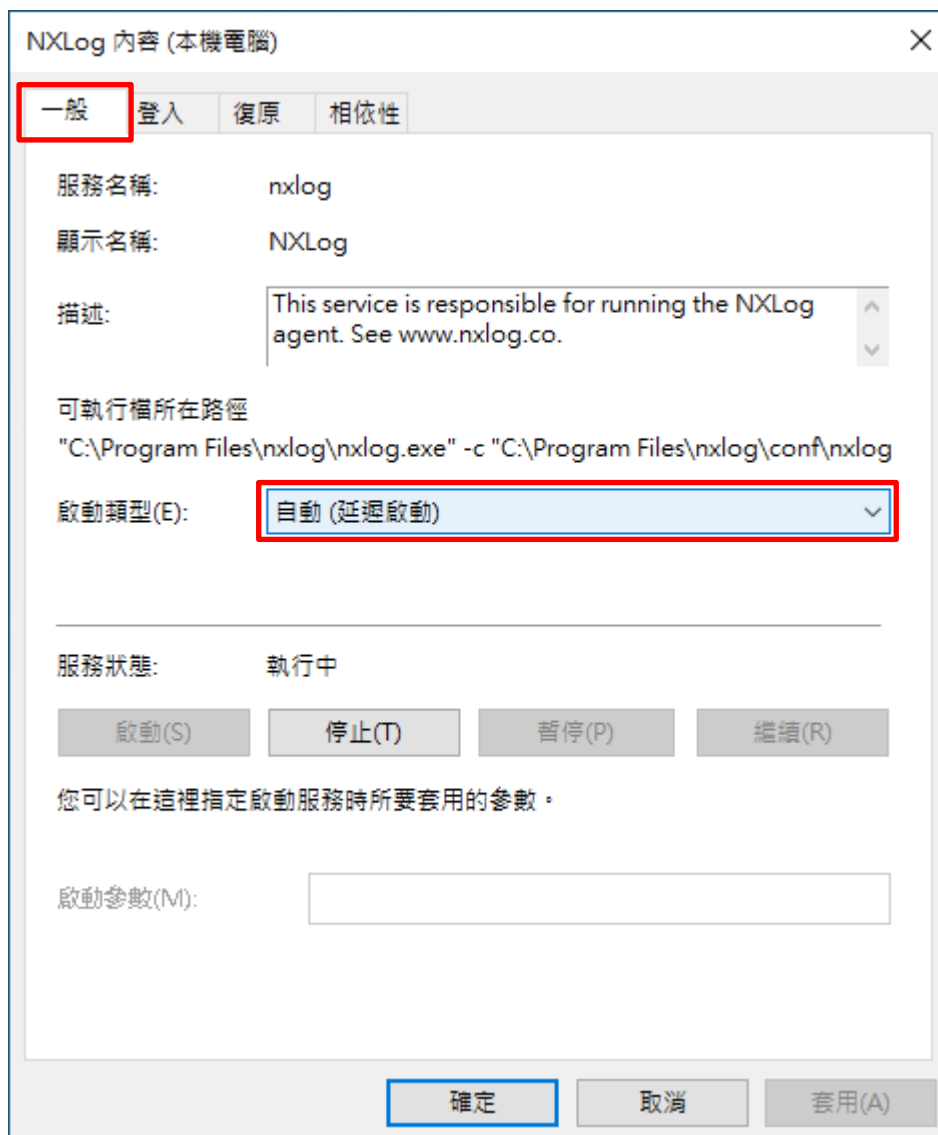
```
PS C:\> Services.msc
PS C:\> _
```

(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]

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P): 瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%)(E)

確定 取消 套用(A)

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

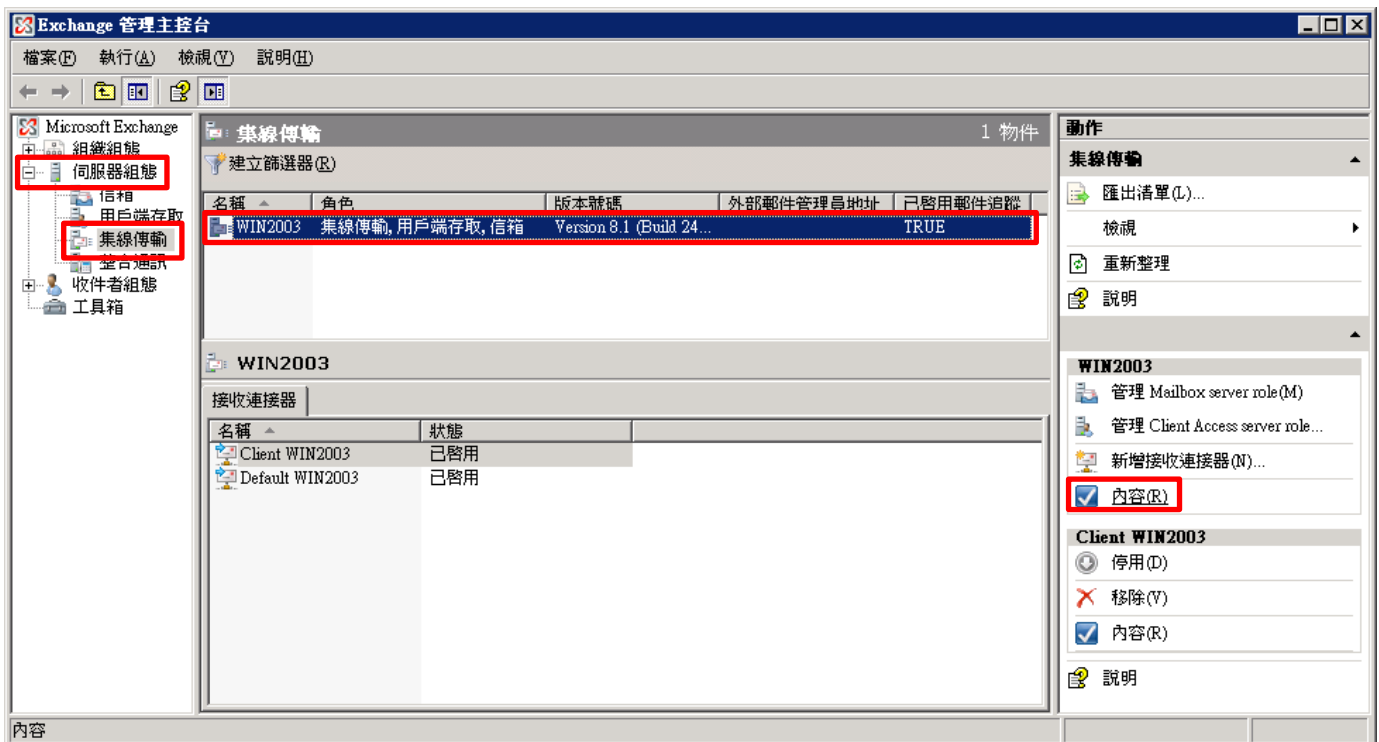
```
define MailLog C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
```

2.1.1 Exchange 管理主控台

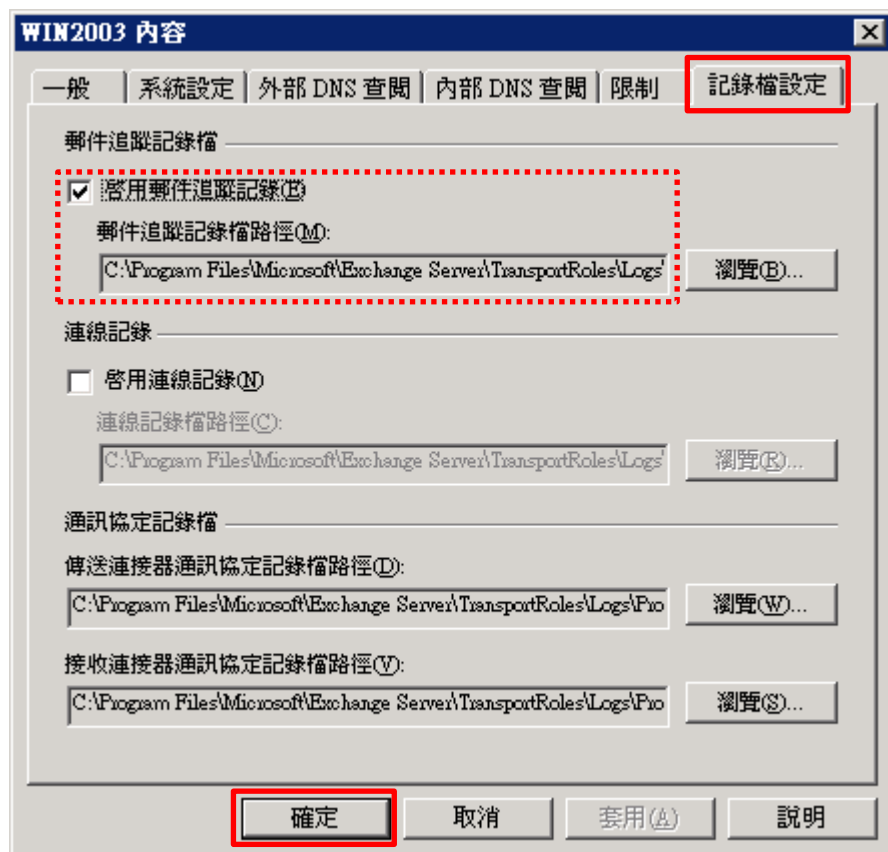
(1) 開啟 [Exchange 管理主控台]



(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]



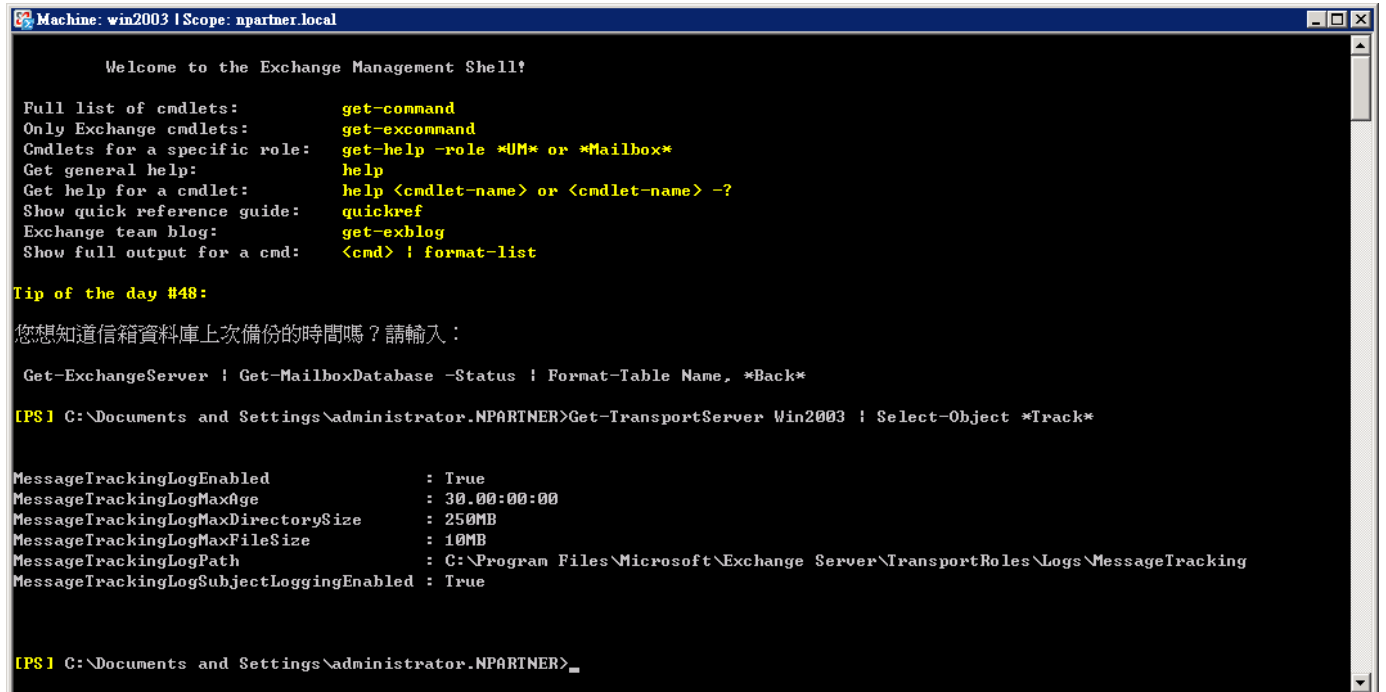
2.1.2 Exchange 管理命令介面

(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*
```

A screenshot of the Exchange Management Shell (EMS) window. The title bar reads "Machine: win2003 | Scope: npartner.local". The main content area shows the following text:

```
Welcome to the Exchange Management Shell!

Full list of cmdlets:           get-command
Only Exchange cmdlets:        get-excommand
Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
Get general help:              help
Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
Show quick reference guide:    quickref
Exchange team blog:           get-exblog
Show full output for a cmd:    <cmd> ! format-list

Tip of the day #48:
您想知道信箱資料庫上次備份的時間嗎？請輸入：

Get-ExchangeServer | Get-MailboxDatabase -Status | Format-Table Name, *Back*
```

```
[PS] C:\Documents and Settings\administrator.NPARTNER>Get-TransportServer Win2003 | Select-Object *Track*
```

```
MessageTrackingLogEnabled      : True
MessageTrackingLogMaxAge       : 30.00:00:00
MessageTrackingLogMaxDirectorySize : 250MB
MessageTrackingLogMaxFileSize  : 10MB
MessageTrackingLogPath         : C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True
```

```
[PS] C:\Documents and Settings\administrator.NPARTNER>_
```

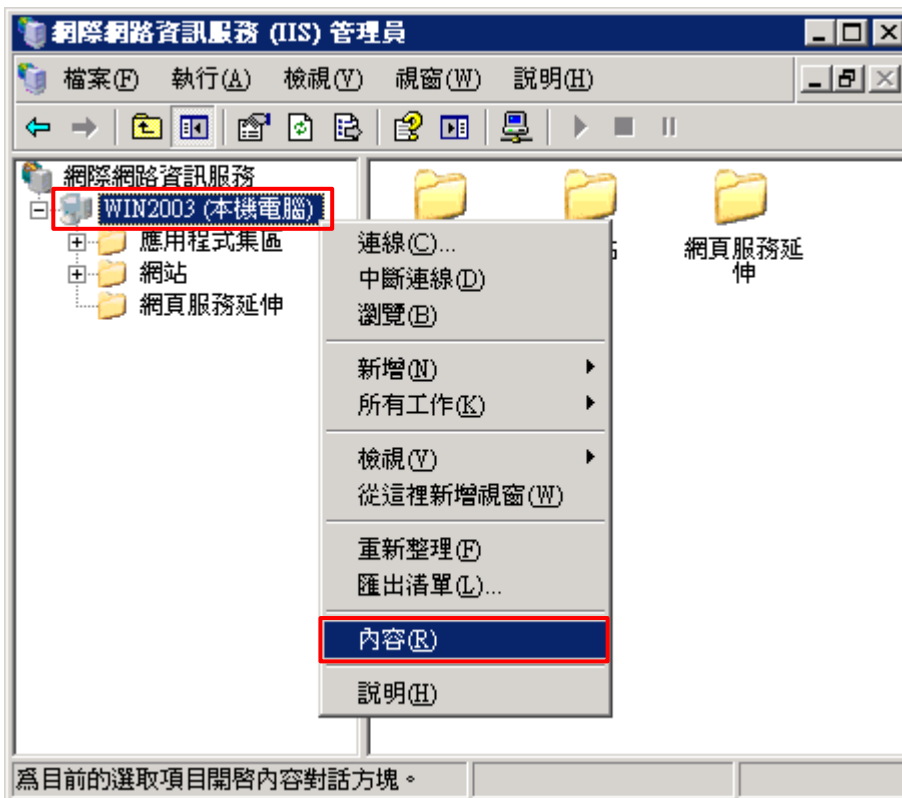
紅色文字部位請輸入 Exchange 伺服器名稱

2.2 IIS Log

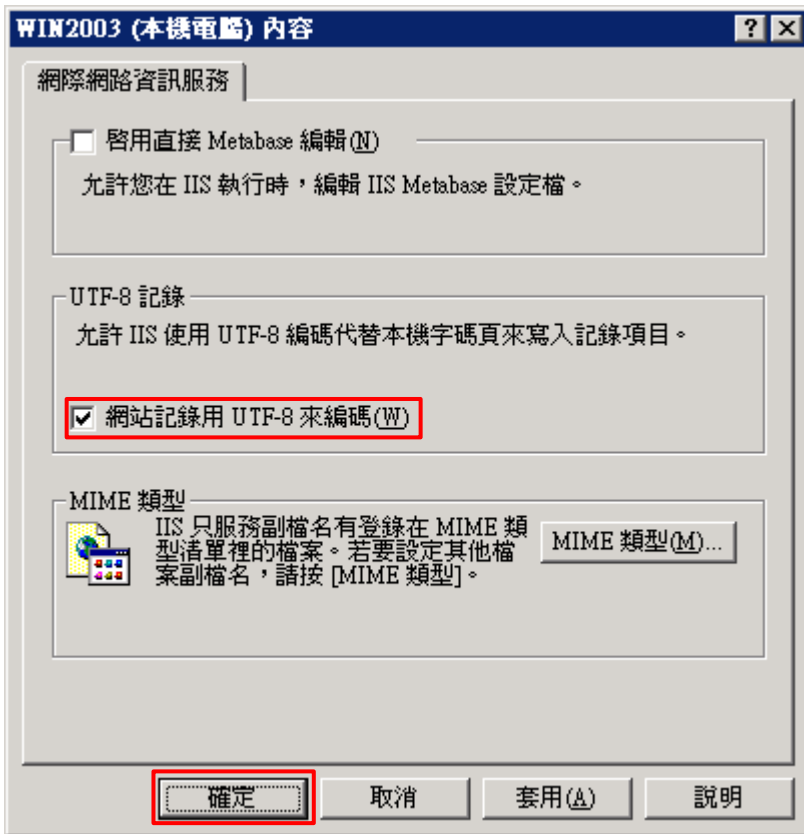
(1) 開啟 [網際網路資訊服務 (IIS) 管理員]



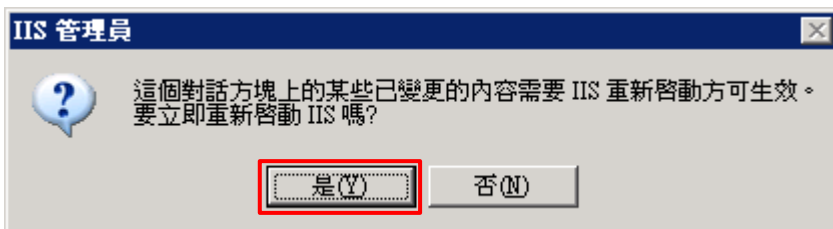
(2) 在 [IIS 伺服器] 按滑鼠右鍵 -> 選擇 [內容]



(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

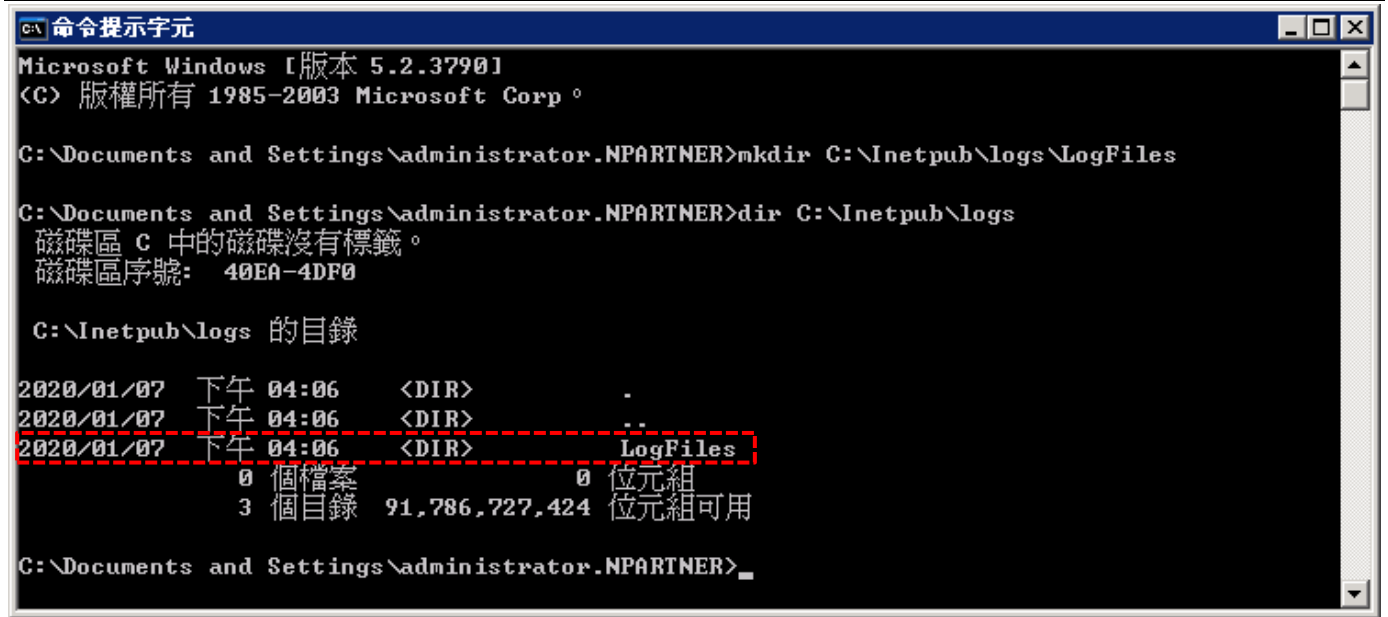


(5) 開啟 [命令提示字元]

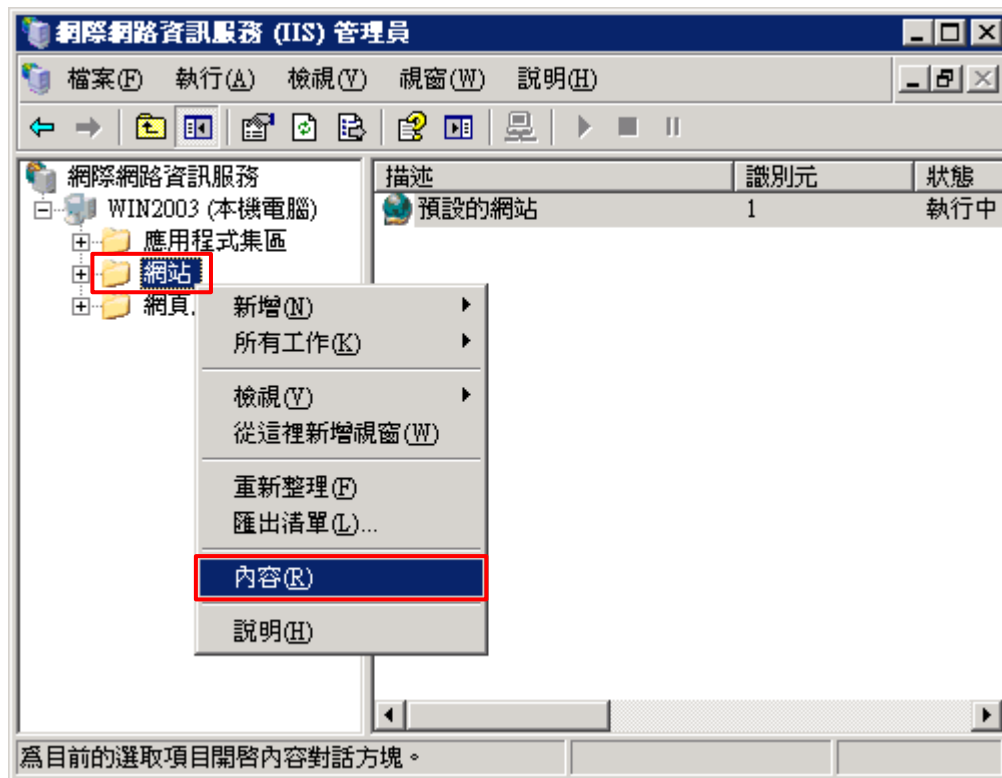


(6) 新增 IIS LogFiles 資料夾和確認 IIS LogFiles 資料夾

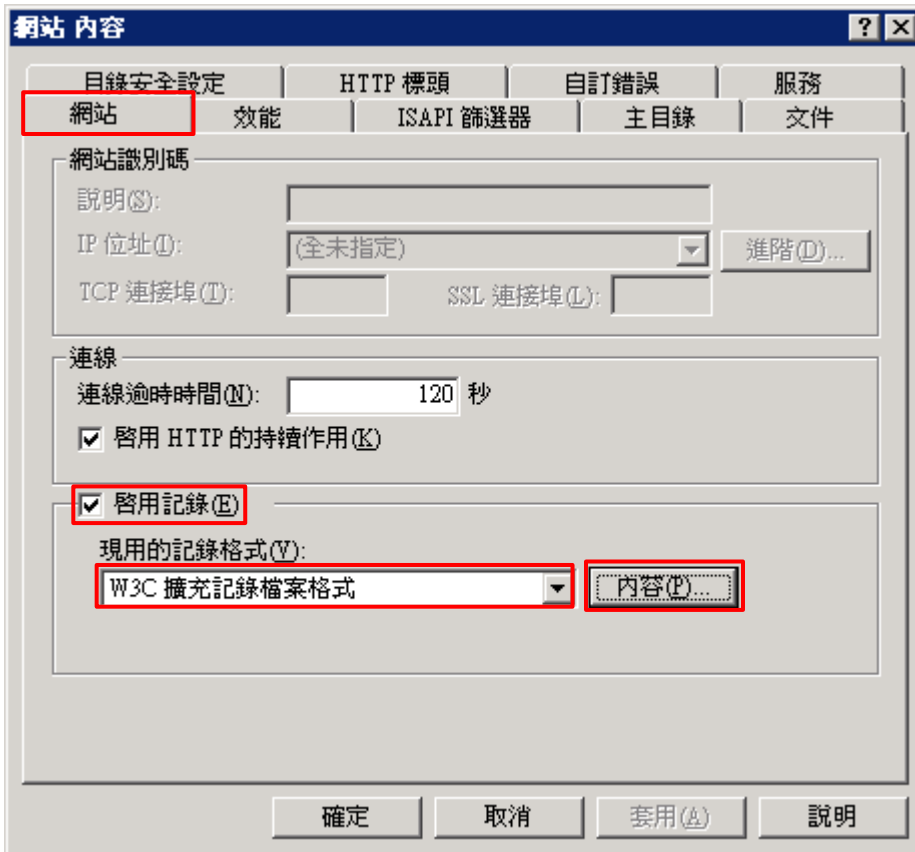
```
C:\> mkdir C:\inetpub\logs\LogFiles  
C:\> dir C:\inetpub\logs
```



(7) 在 [網站] 按滑鼠右鍵 -> 選擇 [內容]

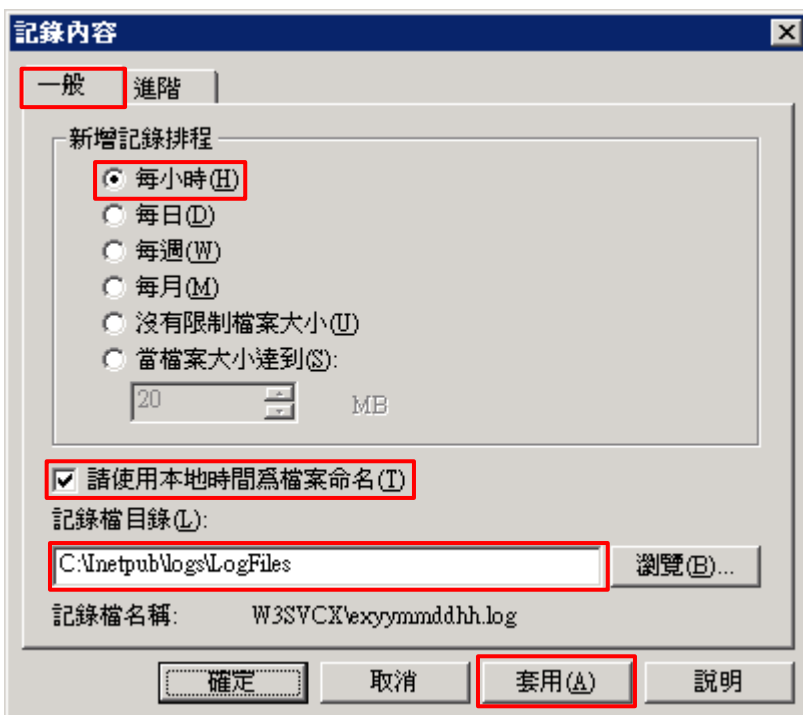


(8) [網站] 頁面: 勾選 [啟用記錄] -> 現用的記錄格式選擇 [W3C 擴充記錄檔案格式] -> 按 [內容]

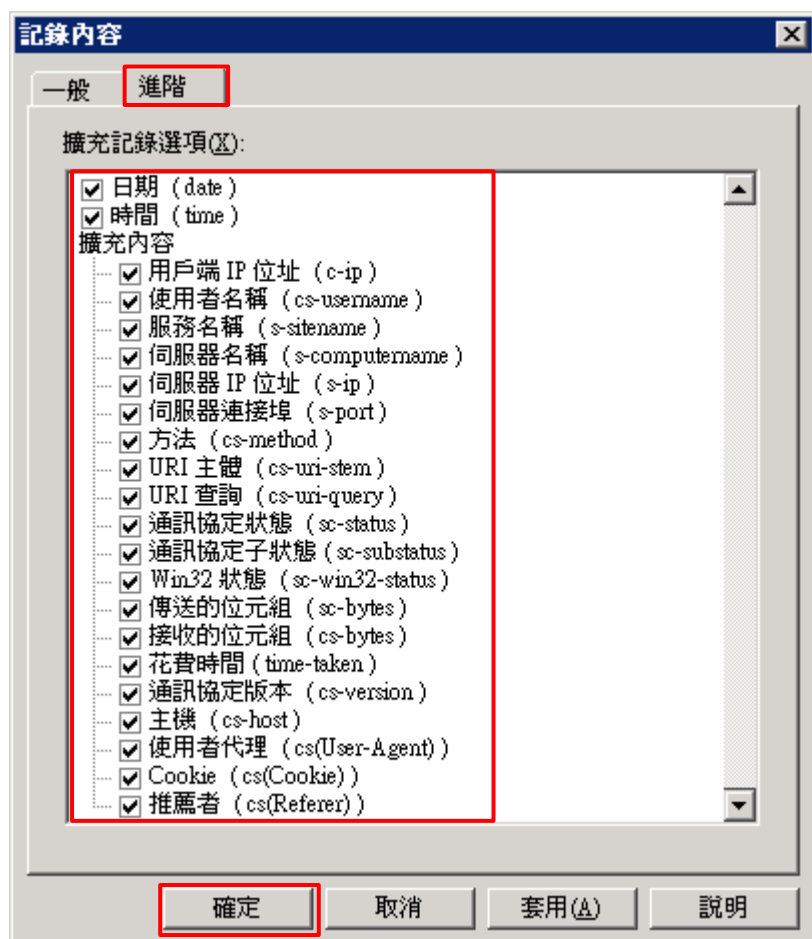


(9) [一般] 頁面: 新增記錄排程點選 [每小時] -> 勾選 [請使用本地時間為檔案命名] -> 記錄檔目錄輸入

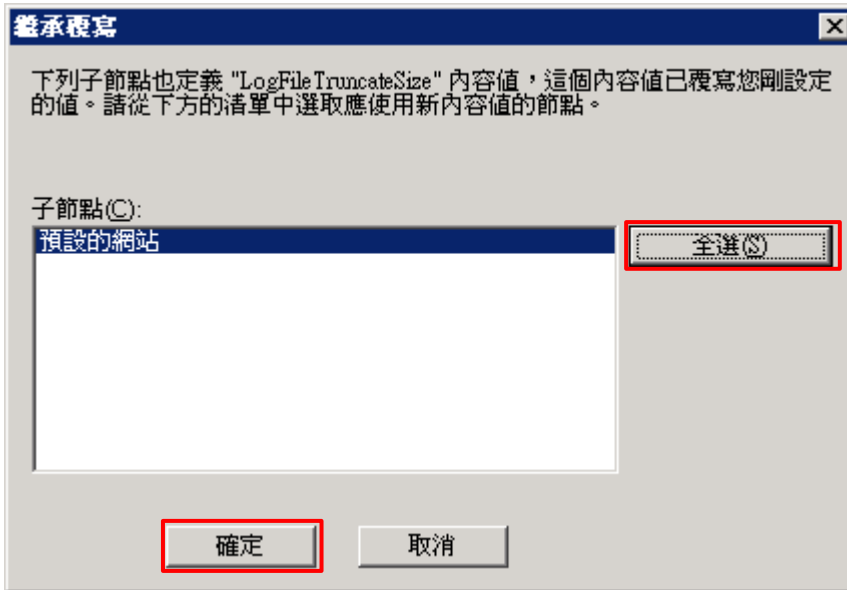
C:\inetpub\logs\LogFiles -> 按 [套用]



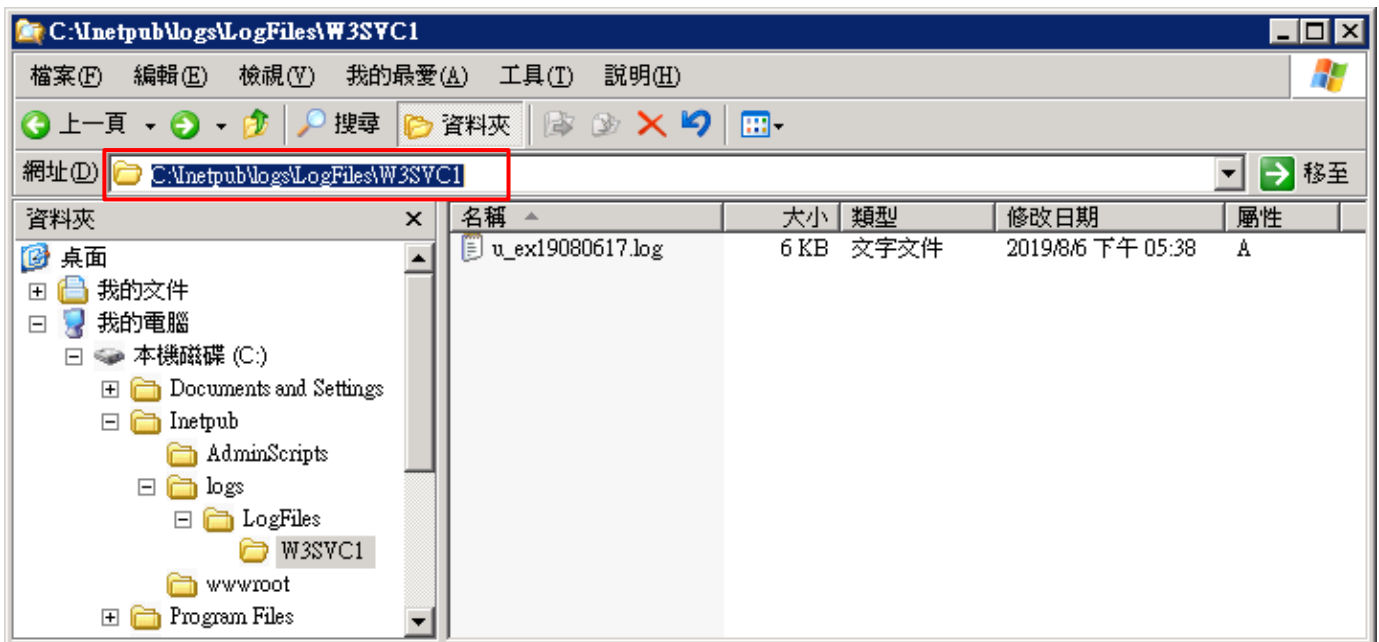
(10) [進階] 頁面：擴充記錄選項勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、[伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(cs-uri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(sc-win32-status)]、[傳送位元組(sc-bytes)]、[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

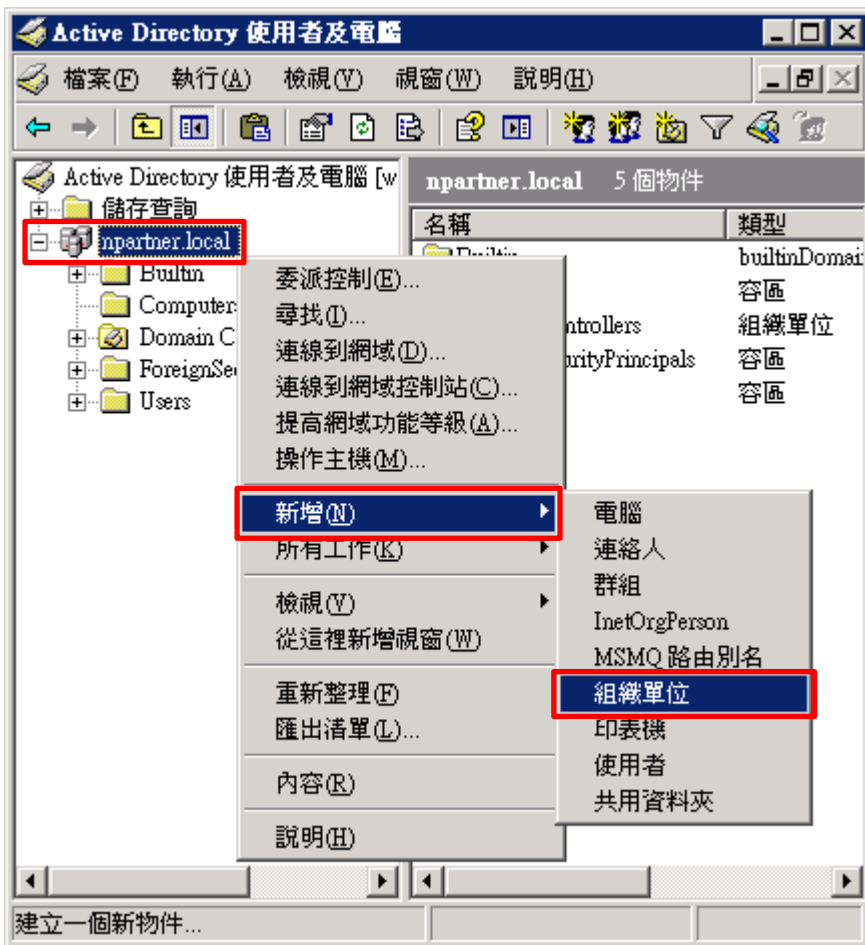
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



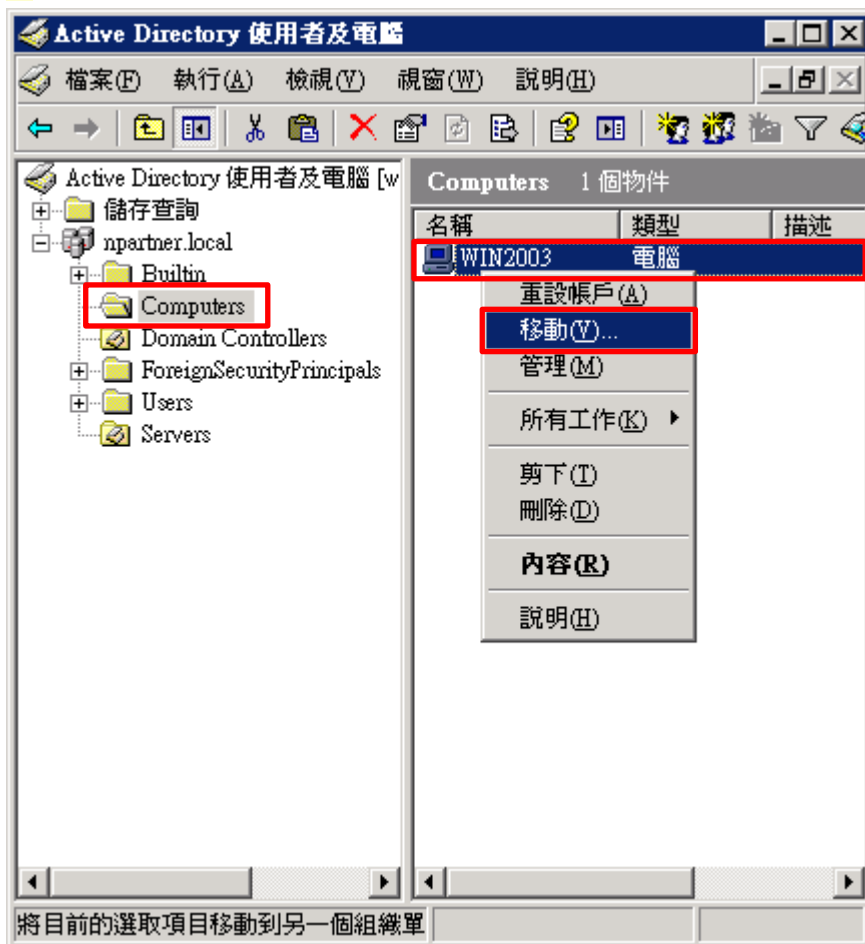
(2) 新增組織單位

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



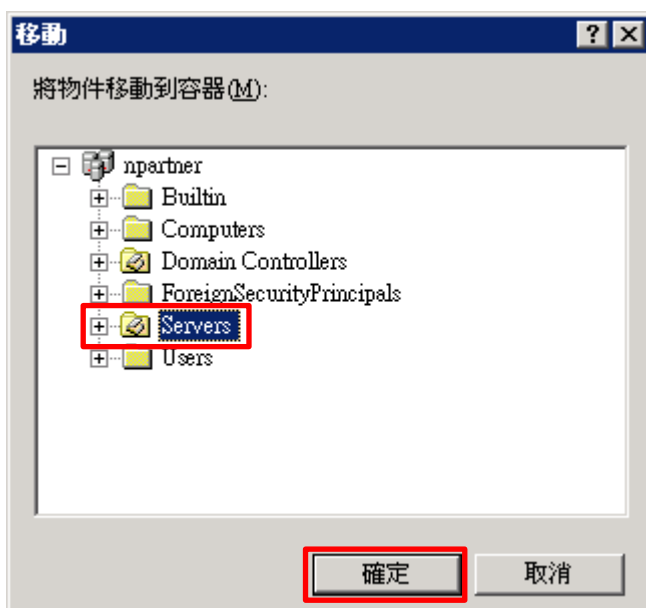
(4) 移動 Exchange 伺服器至新的組織單位

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]



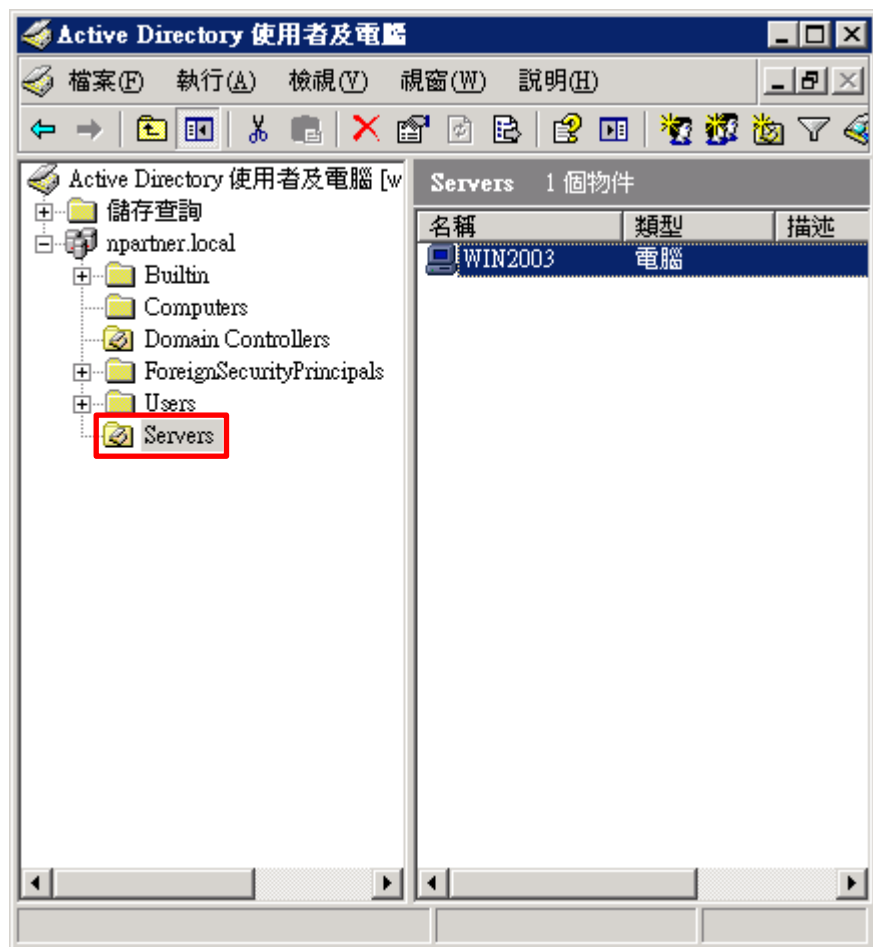
(5) 選擇組織單位

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

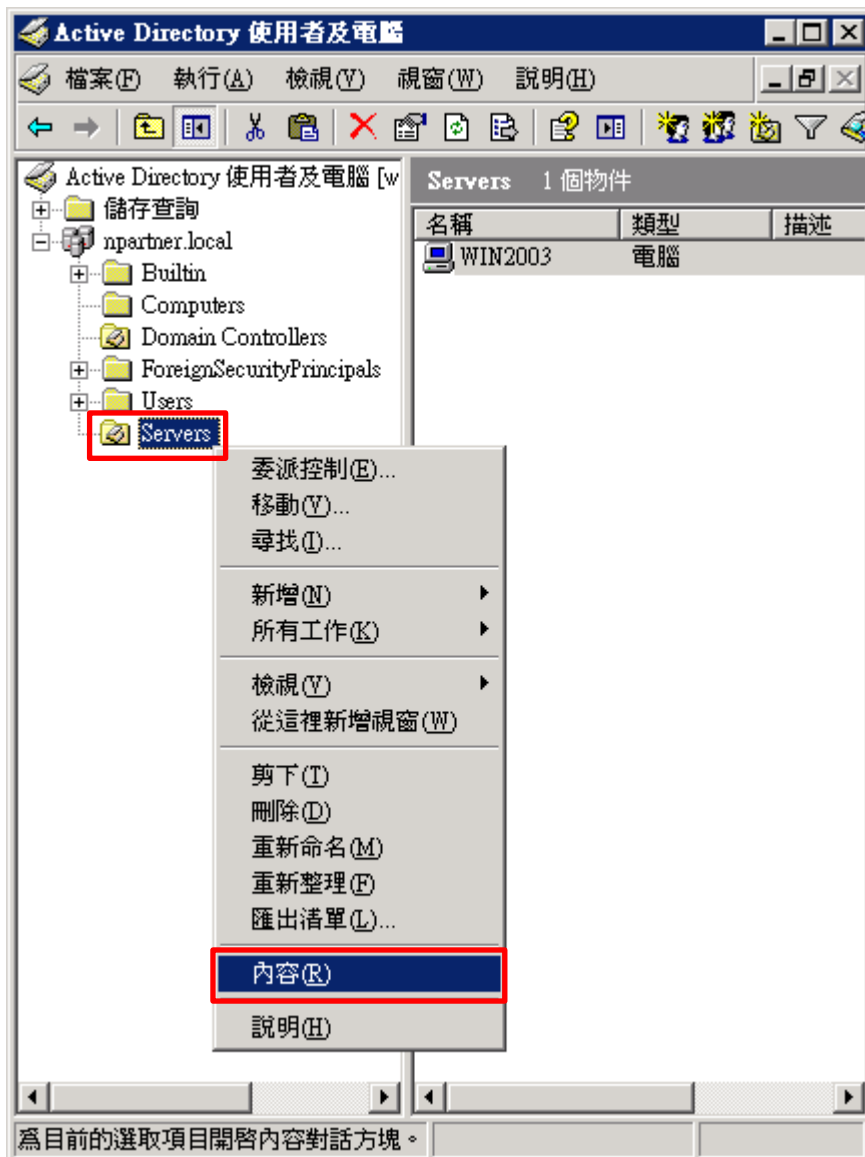
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



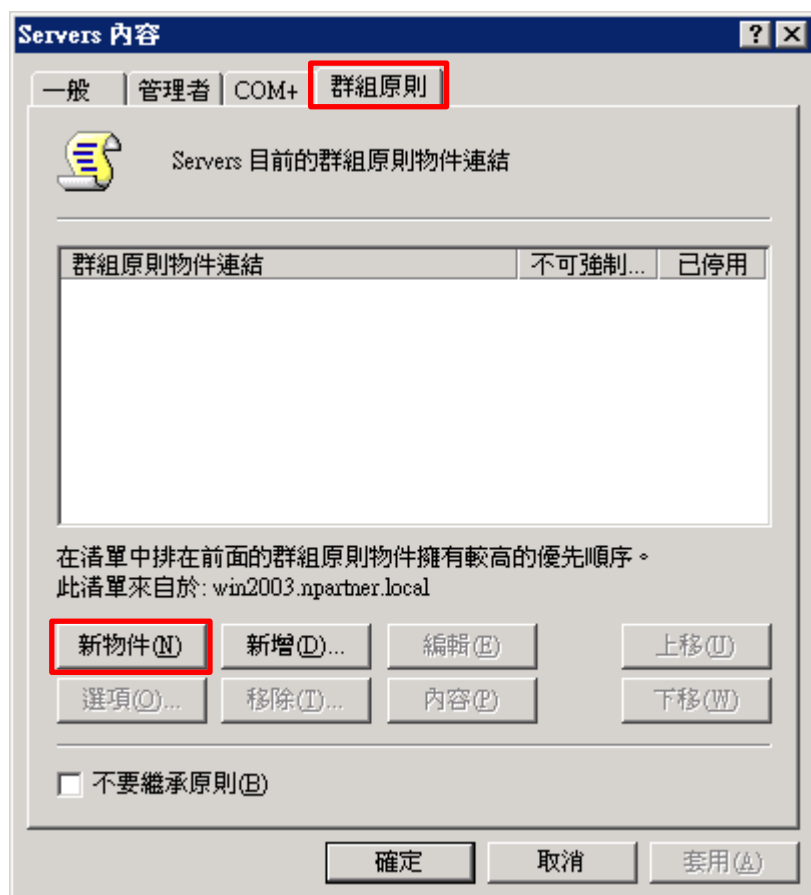
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



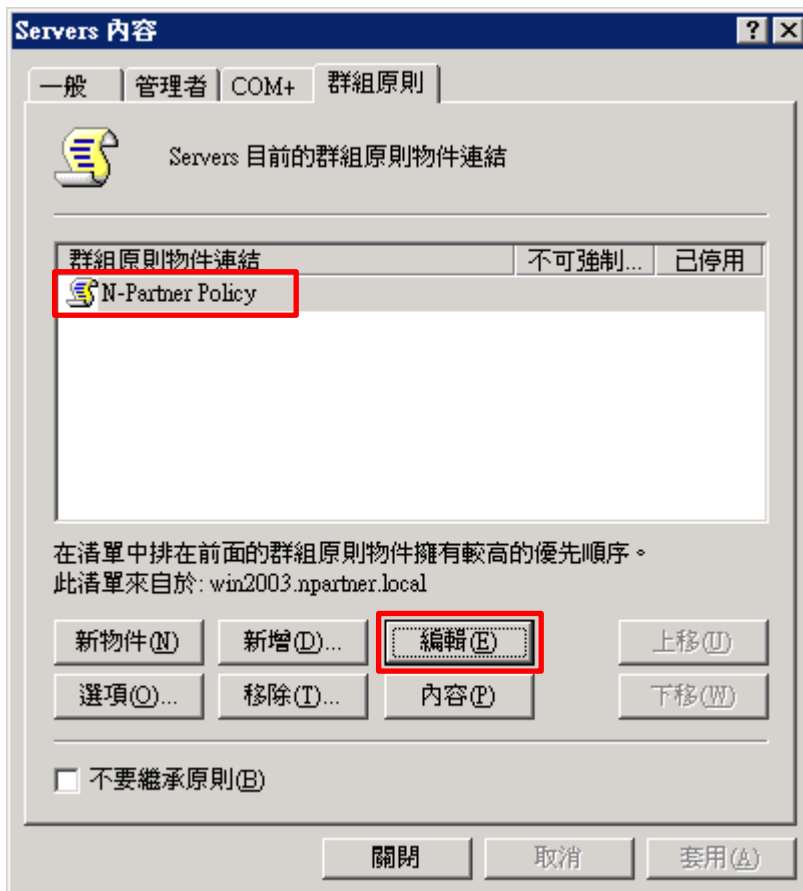
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



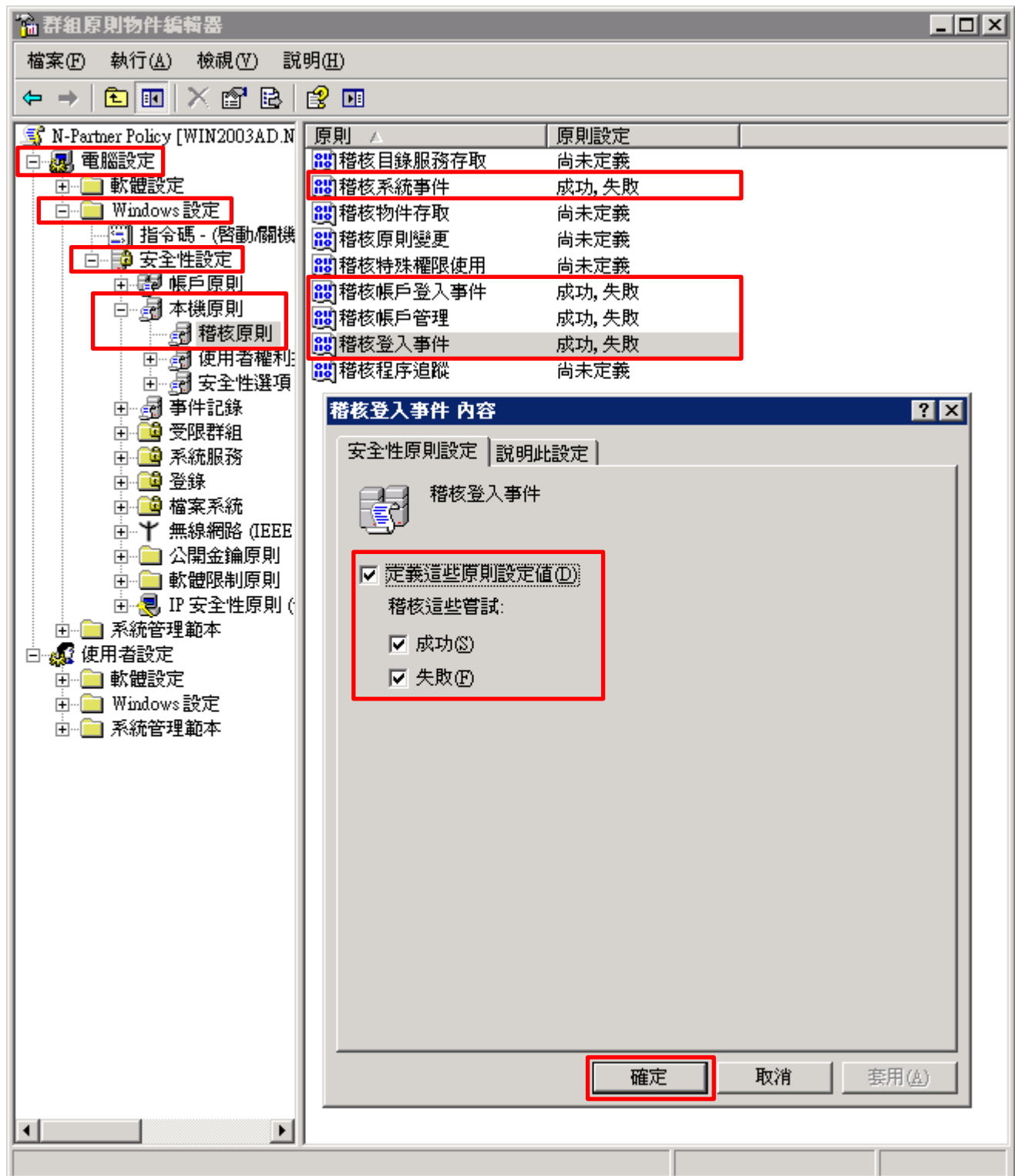
(4) 編輯群組原則物件

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]



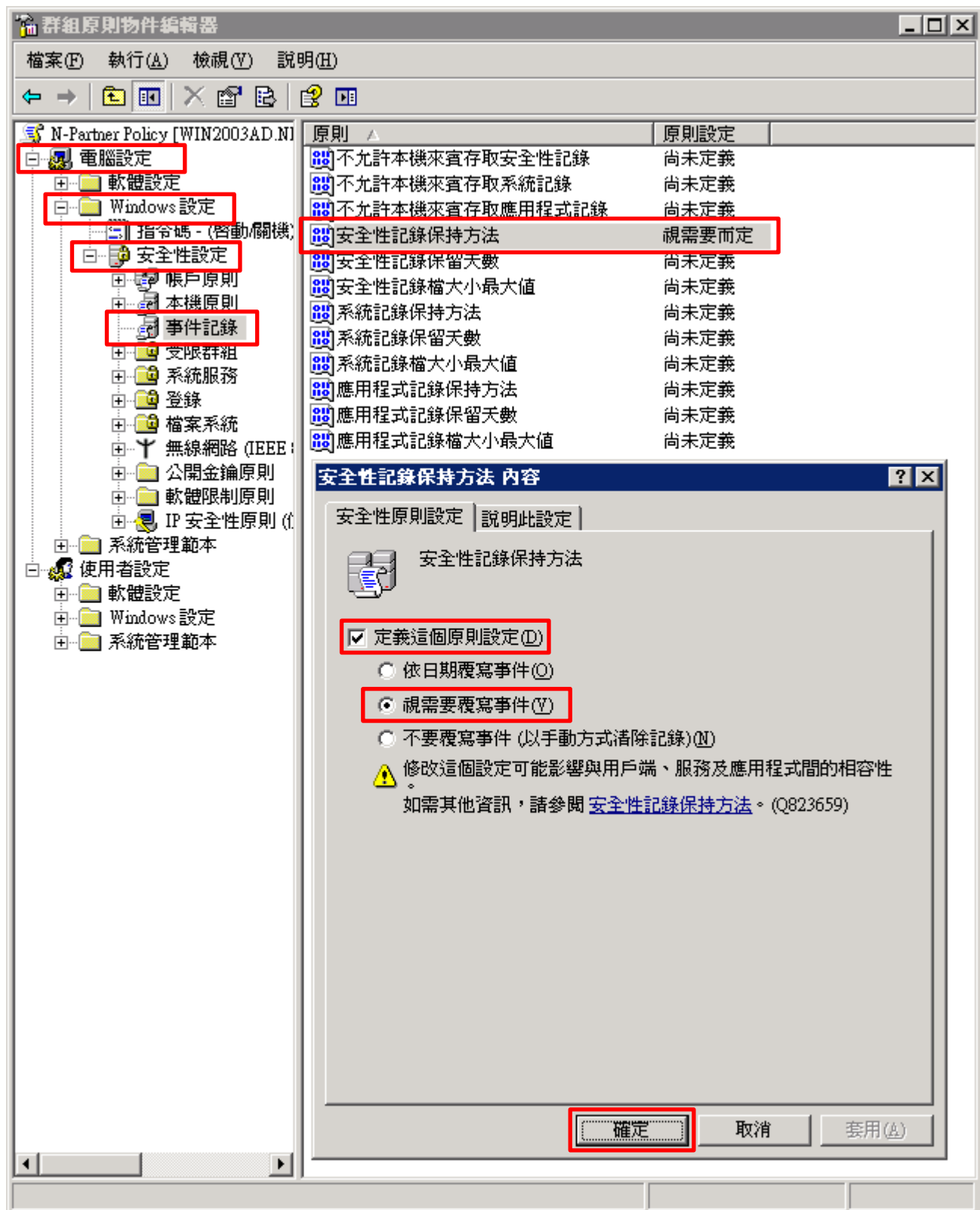
(5) 本機原則：稽核原則

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]



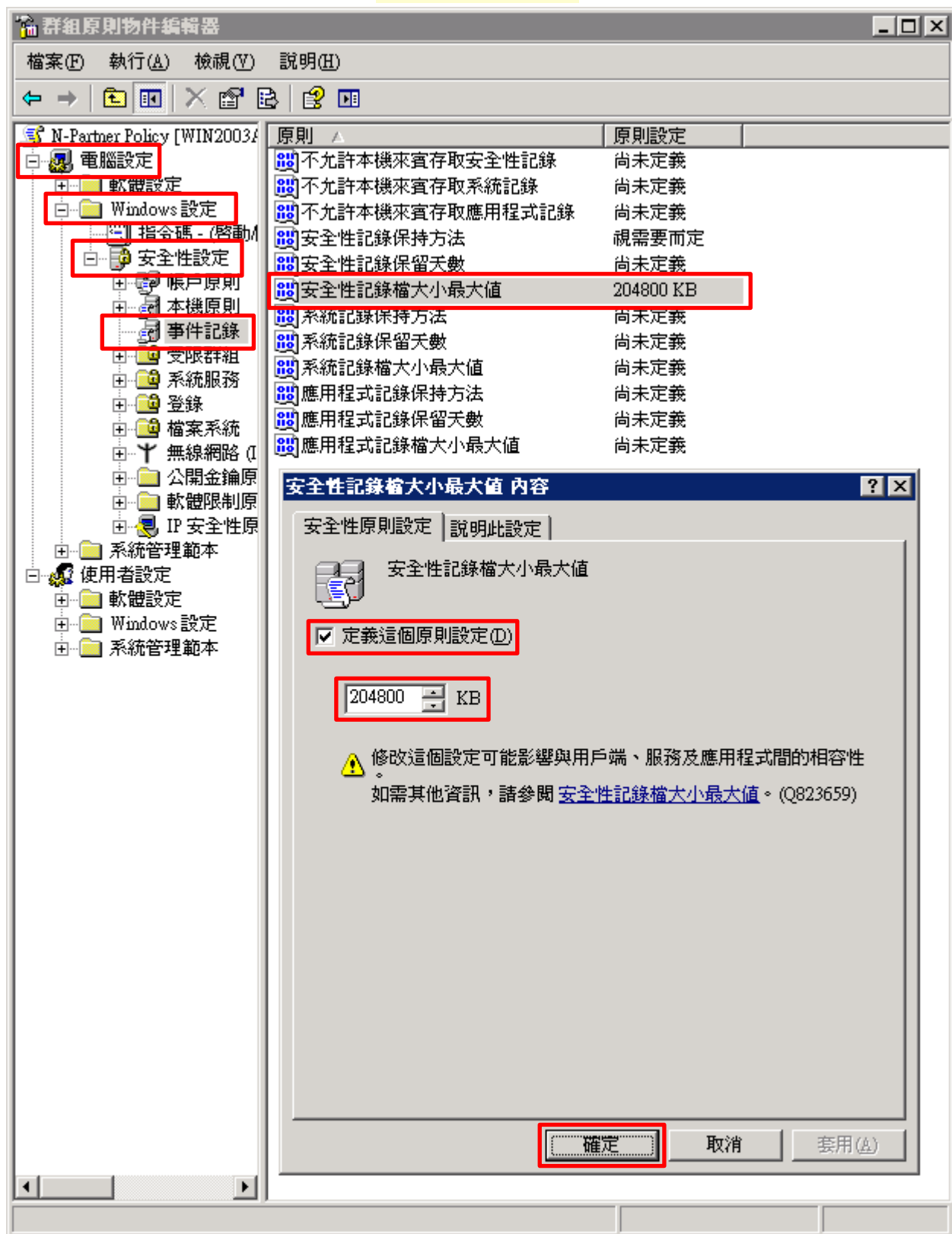
(6) 事件記錄：安全性記錄保持方法

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]



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

命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\administrator.NPARTNER>gpresult /v

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

建立於 2020/1/7 下午 04:59:31

NPARTNER\administrator 的 RSOP 資料在 WIN2003: 記錄模式
-----

OS 類型: Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition
OS 設定: 成員伺服器
OS 版本: 5.2.3790
終端機伺服器模式: 遠端系統管理
站台名稱: Default-First-Site-Name
漫遊設定檔:
本機設定檔: C:\Documents and Settings\administrator.NPARTNER
用低速連結來連線?: 否

電腦設定
-----
CN=WIN2003,OU=Servers,DC=npartner,DC=local
上次套用的群組原則: 2020/1/7 於 下午 04:58:30
套用的群組原則來自: ad.npartner.local
群組原則低速連結閾值: 500 kbps
網域名稱: npartner
網域類型: Windows 2000

已套用的群組原則物件
-----
N-Partner Policy
Default Domain Policy
```

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

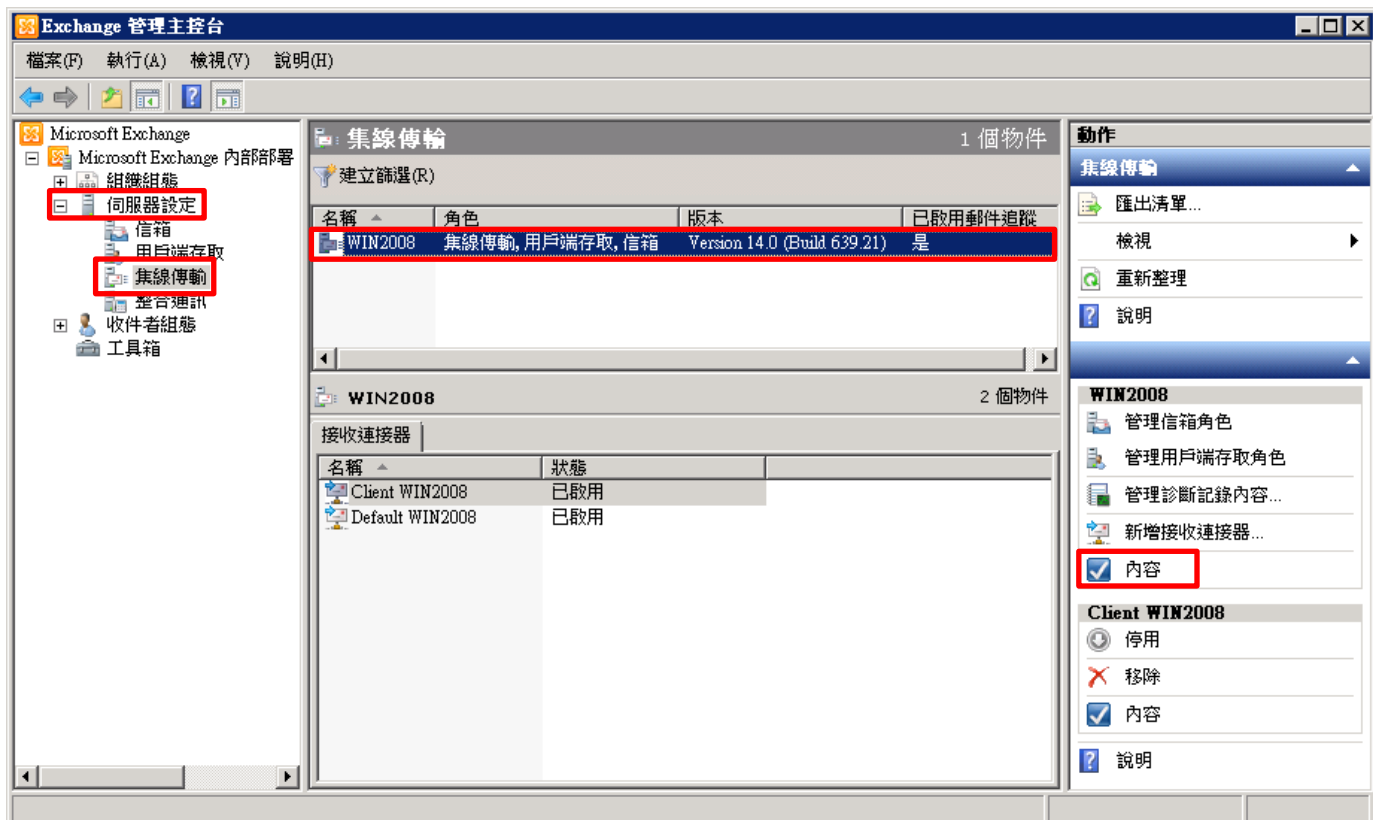
```
define MailLog C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking
```

3.1.1 Exchange Management Console

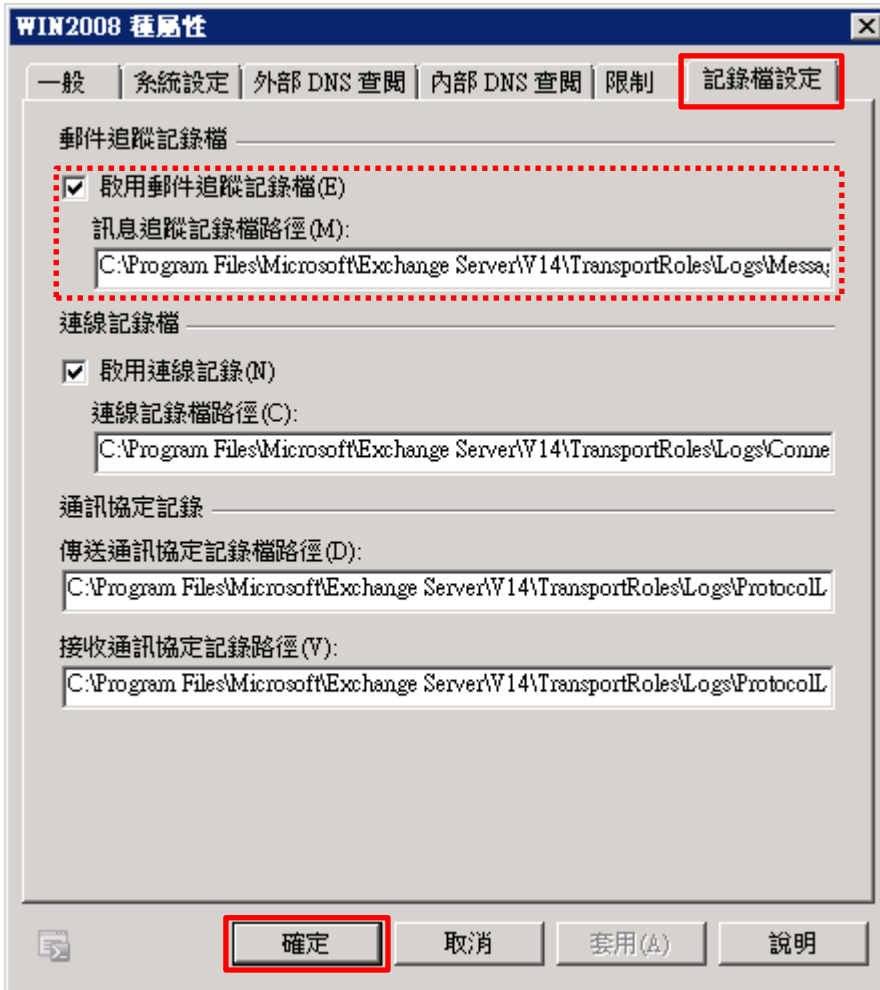
(1) 開啟 [Exchange Management Console]



(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\14\TransportRoles\Logs\MessageTracking]

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

A screenshot of a Windows command prompt window titled "Machine: Win2008.npartner.local". The terminal displays the following text:

```
Welcome to the Exchange Management Shell!

Full list of cmdlets:           get-command
Only Exchange cmdlets:        get-excommand
Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
Get general help:              help
Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
Show quick reference guide:    quickref
Exchange team blog:           get-exblog
Show full output for a cmd:    <cmd> ! format-list

Tip of the day #1:
是否厭倦每次在執行什麼動作時都要輸入冗長的命令？設定別名！類型：

Set-Alias GetMre Get-ManagementRoleEntry

如需目前所有的別名，請輸入：

Get-Alias

VERBOSE: Connecting to Win2008.npartner.local
VERBOSE: Connected to Win2008.npartner.local.
[PS] C:\Windows\system32>Get-TransportServer Win2008 ! 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\14\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True

[PS] C:\Windows\system32>
```

紅色文字部位請輸入 Exchange 伺服器名稱

3.2 IIS Log

修改 nxlog.conf

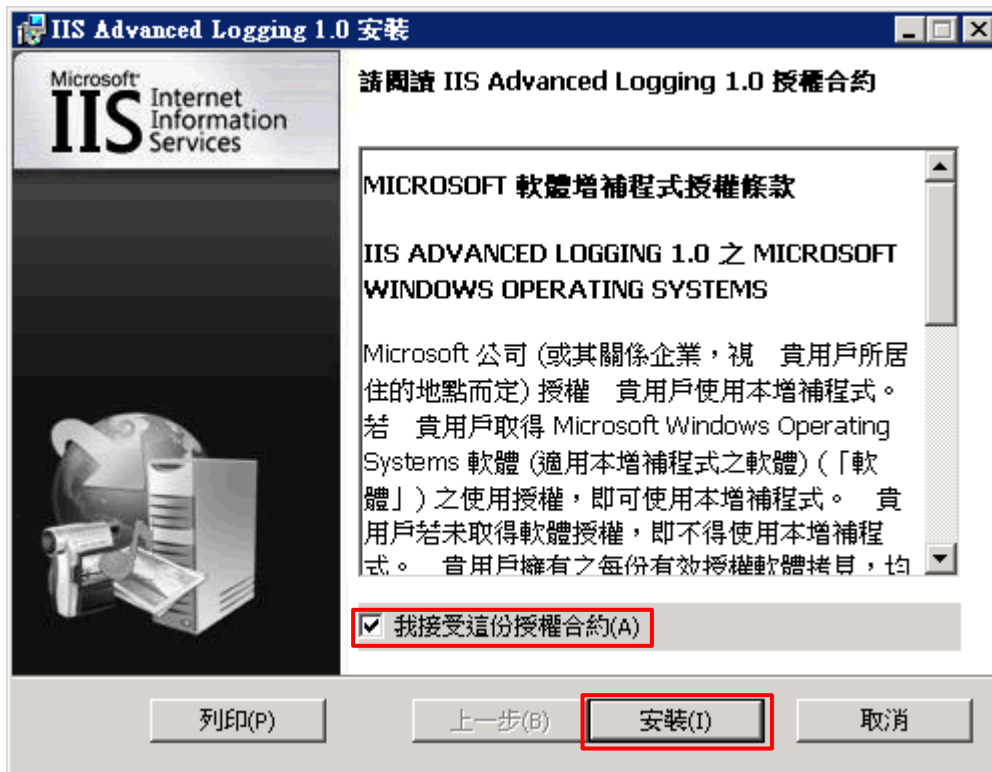
註: 參考 1.3 NXLog 設定檔

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 ·

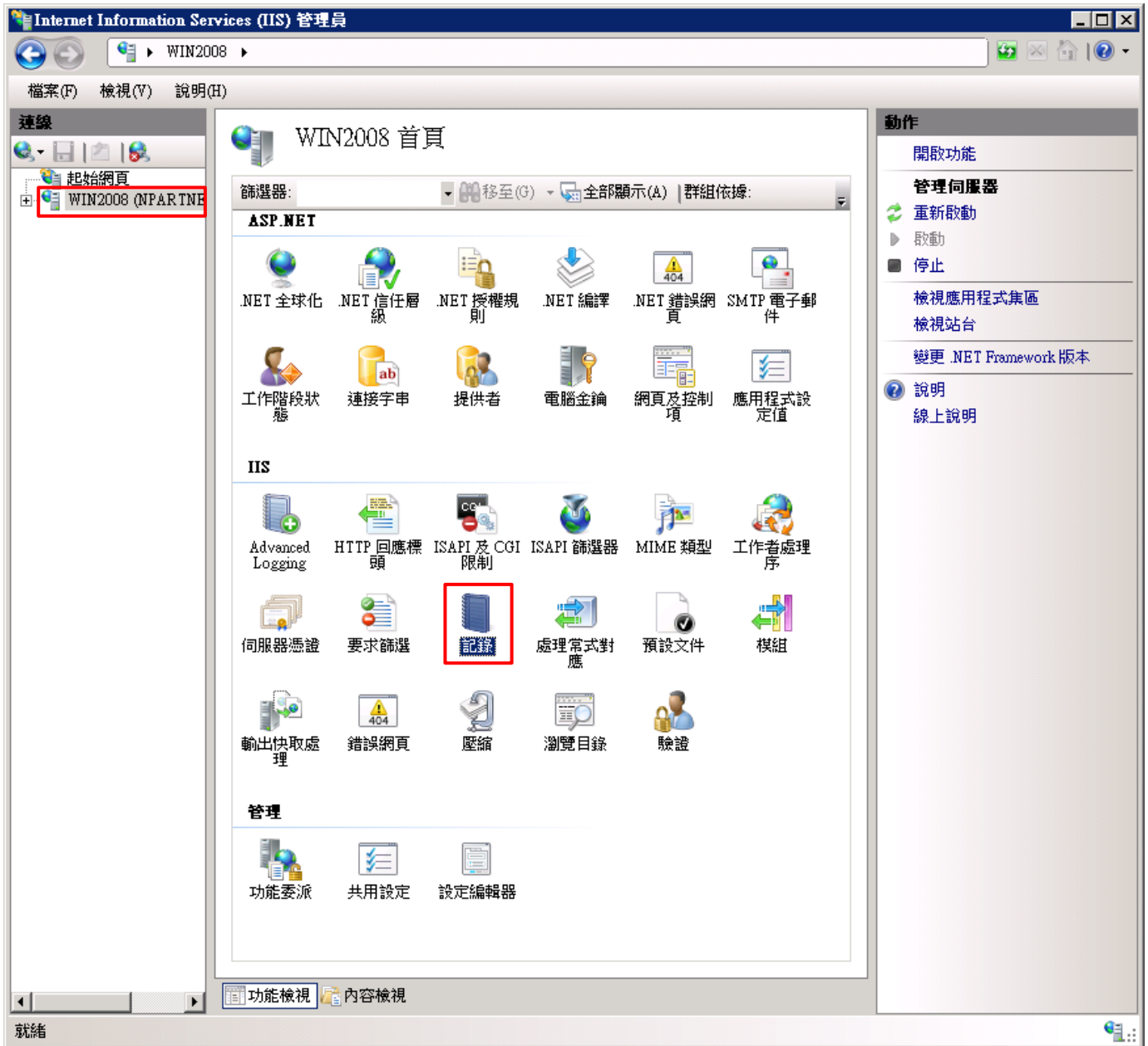
點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]



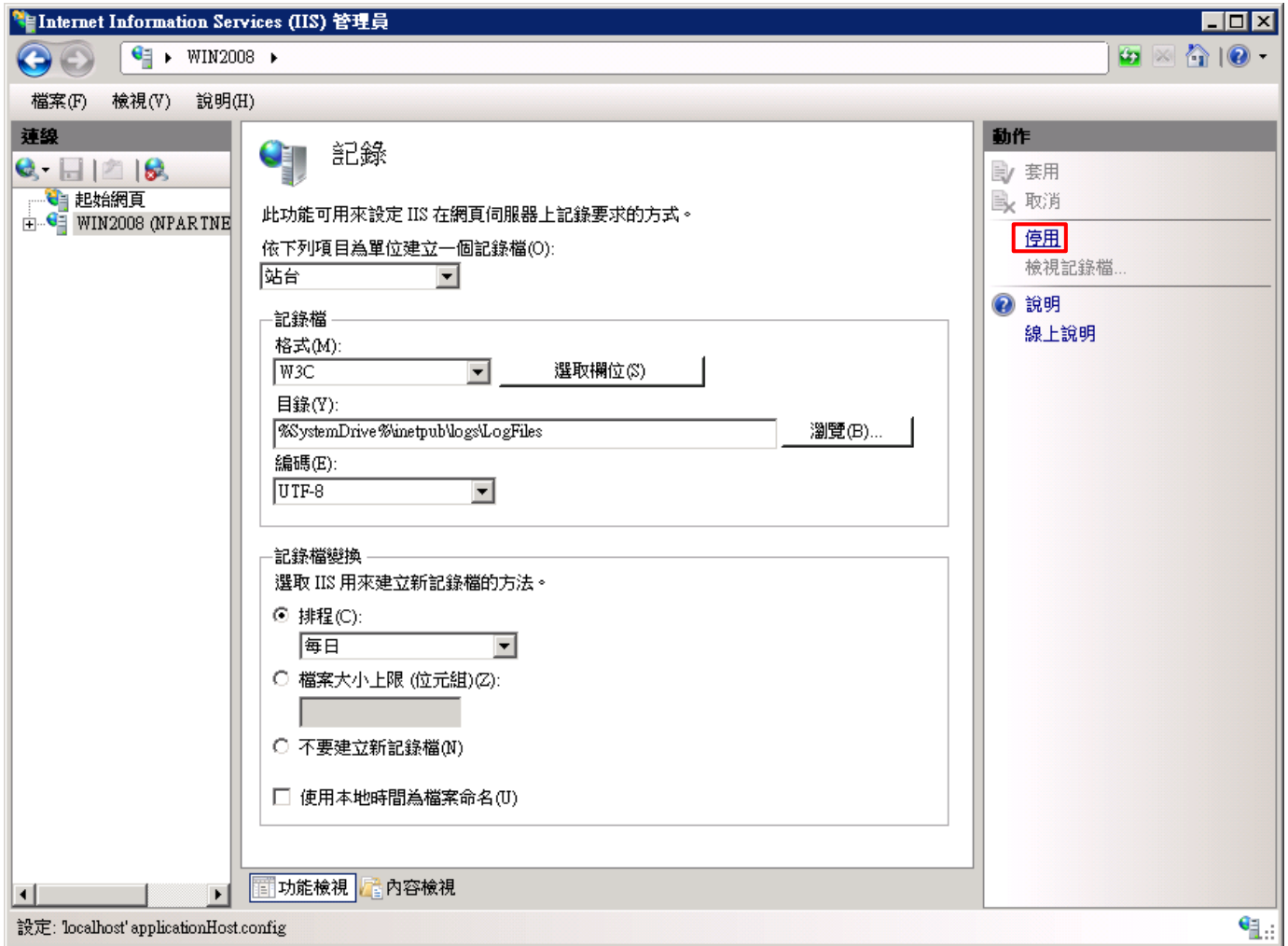
(2) 開啟 [Internet Information Services (IIS) 管理員]



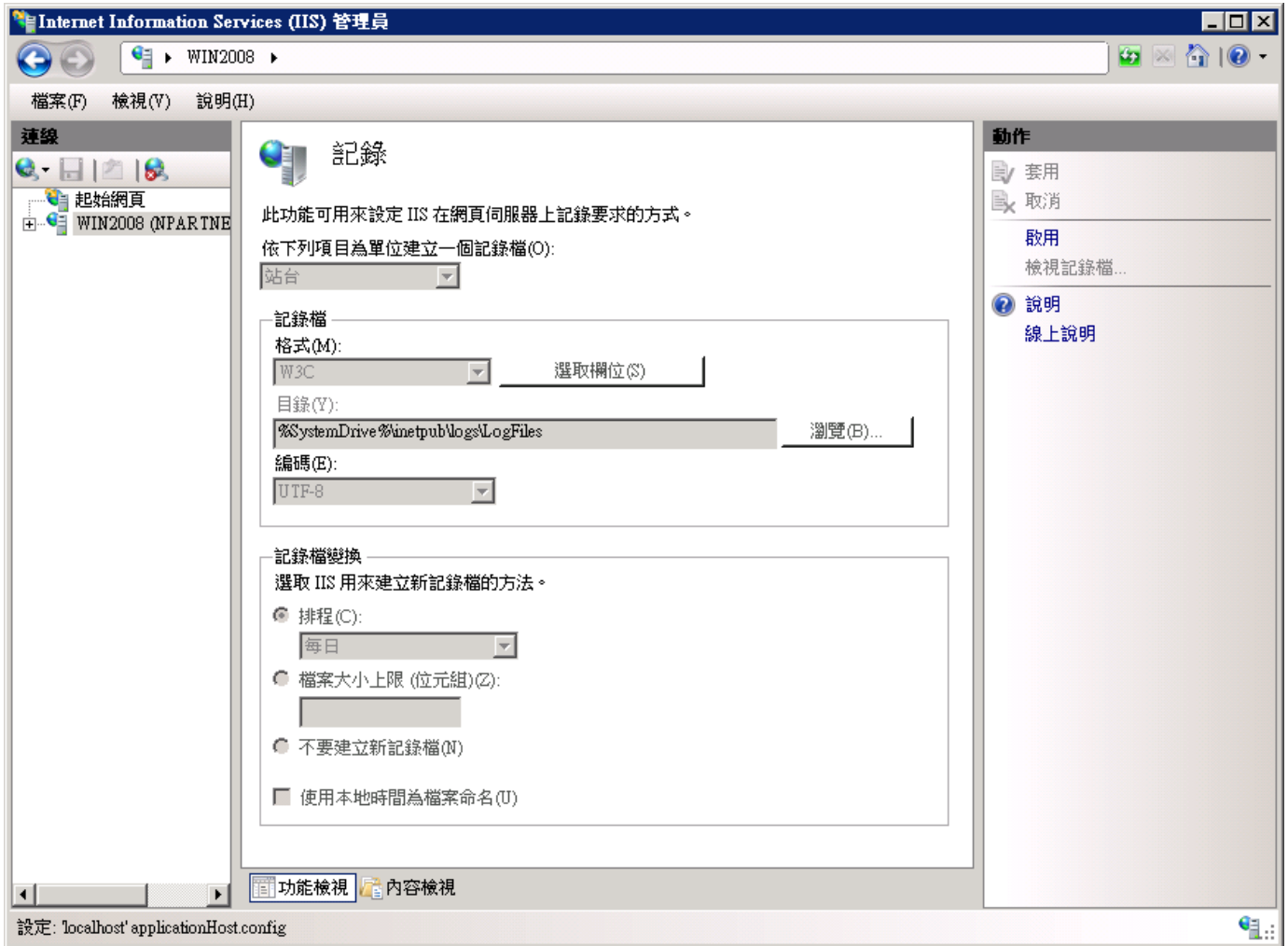
(3) 點選 [IIS 伺服器] -> [記錄]



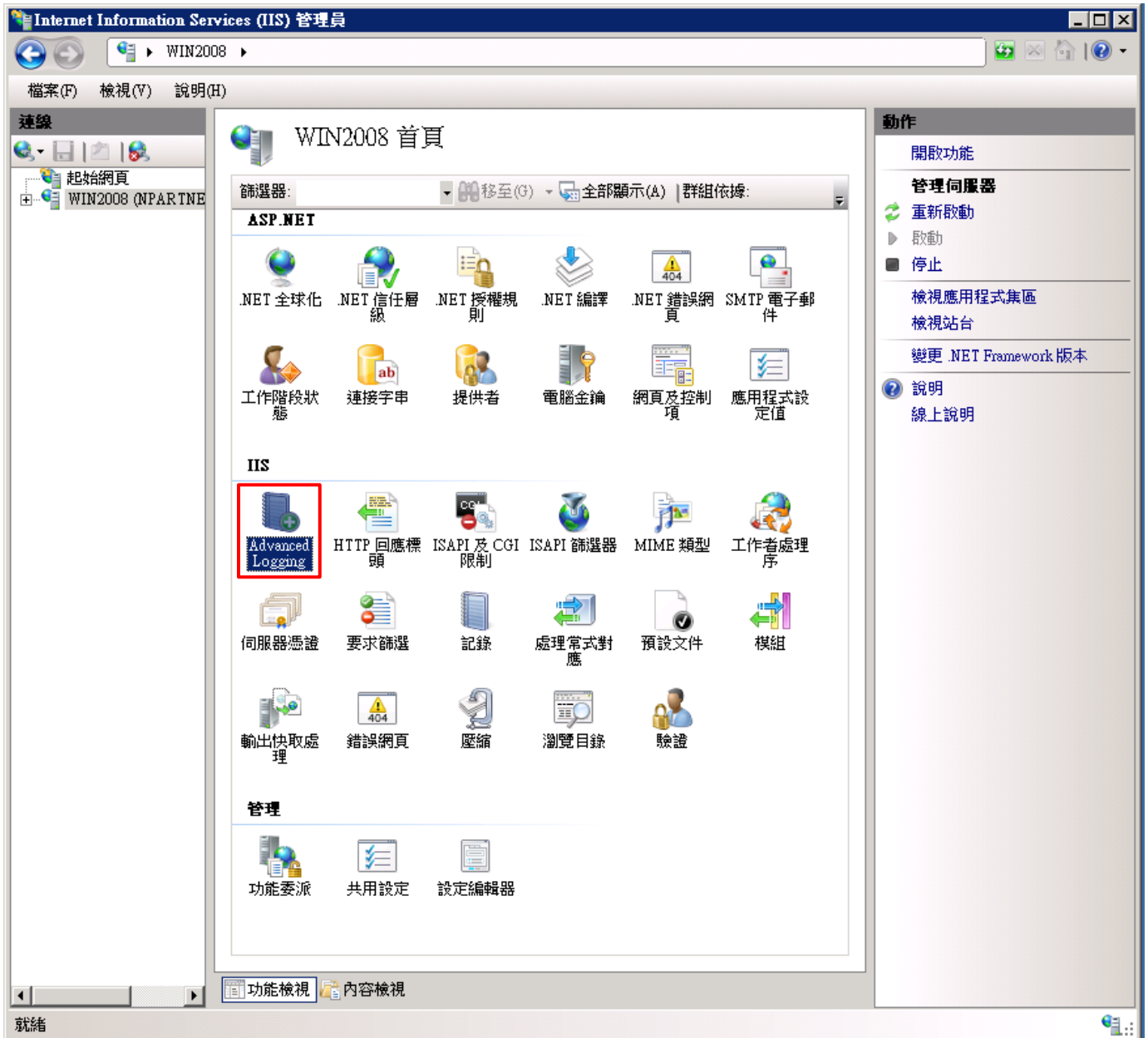
(4) 點選 [停用]



(5) 確認記錄已停用



(6) 點選 [Advanced Logging]



(7) 按 [編輯記錄欄位]

The screenshot shows the IIS Manager console for 'WIN2008'. The main pane displays the 'Advanced Logging' configuration page. The left-hand pane shows the 'Connections' tree with 'WIN2008 (NPARTNER)' selected. The right-hand pane contains a 'Alerts' section with a message 'Advanced Logging 功能已停用' and an 'Actions' section with several options. The 'Edit Log Fields...' option is highlighted with a red box.

Internet Information Services (IIS) 管理員

WIN2008

檔案(F) 檢視(V) 說明(H)

連線

起始網頁

WIN2008 (NPARTNER)

Advanced Logging

使用這個功能可以建立並管理記錄定義 (用以指定要記錄哪些伺服器端和用戶端記錄欄位)，以及設定其他記錄設定。

群組依據: 沒有分組

名稱	已啟用
%COMPUTERNAME%-Server	已啟用

功能檢視 內容檢視

設定: localhost applicationHost.config

Alerts: Advanced Logging 功能已停用

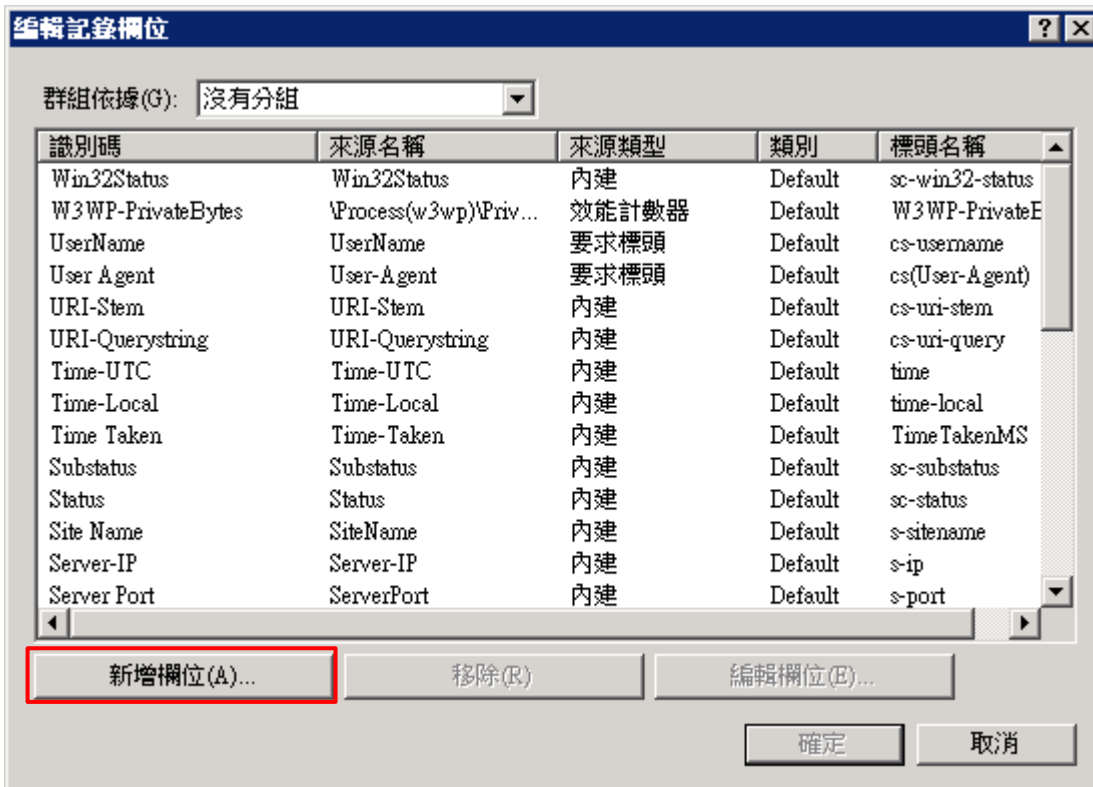
Actions:

- 新增記錄定義...
- 啟用 Advanced Logging
- 啟用用戶端記錄
- 編輯記錄欄位...**
- 編輯記錄目錄...
- 檢視記錄檔...

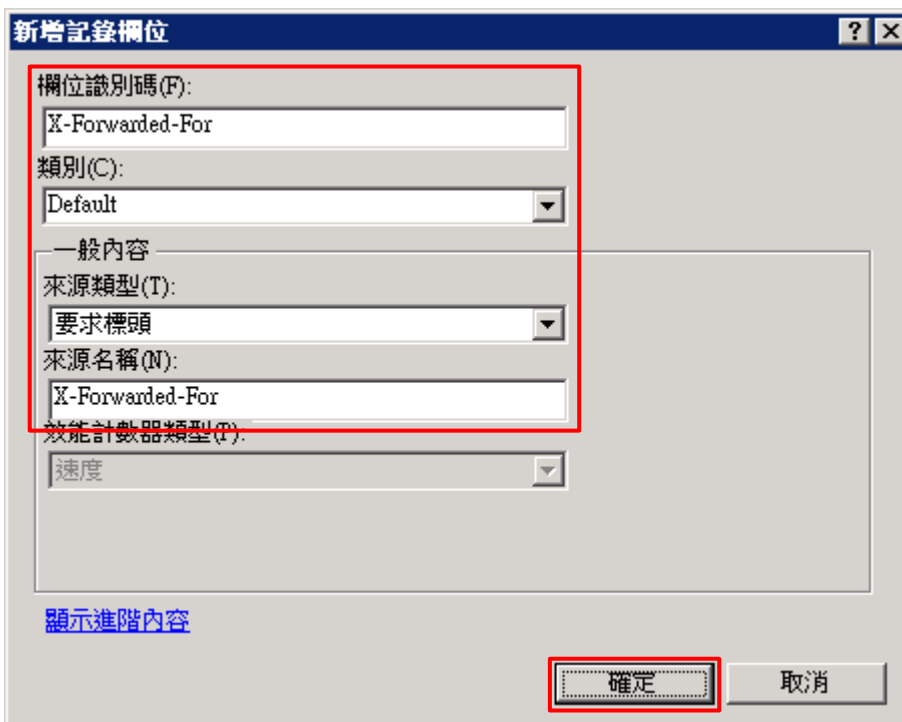
說明

- 線上說明

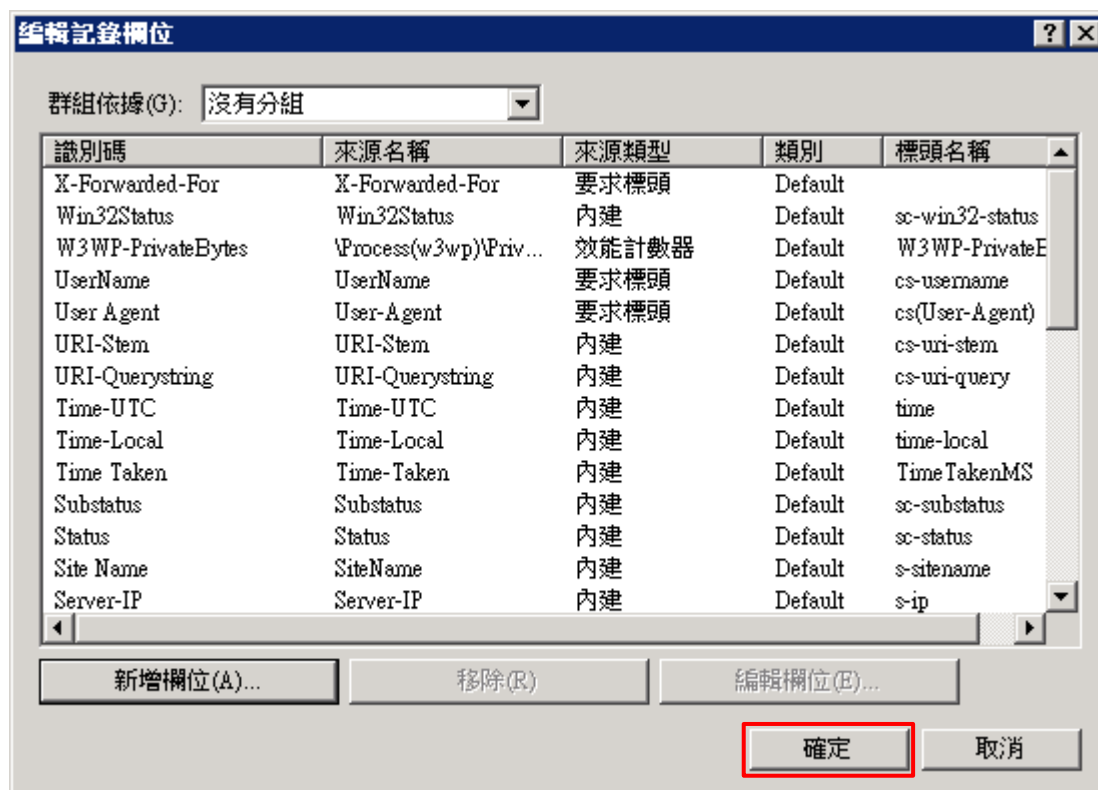
(8) 按 [新增欄位]



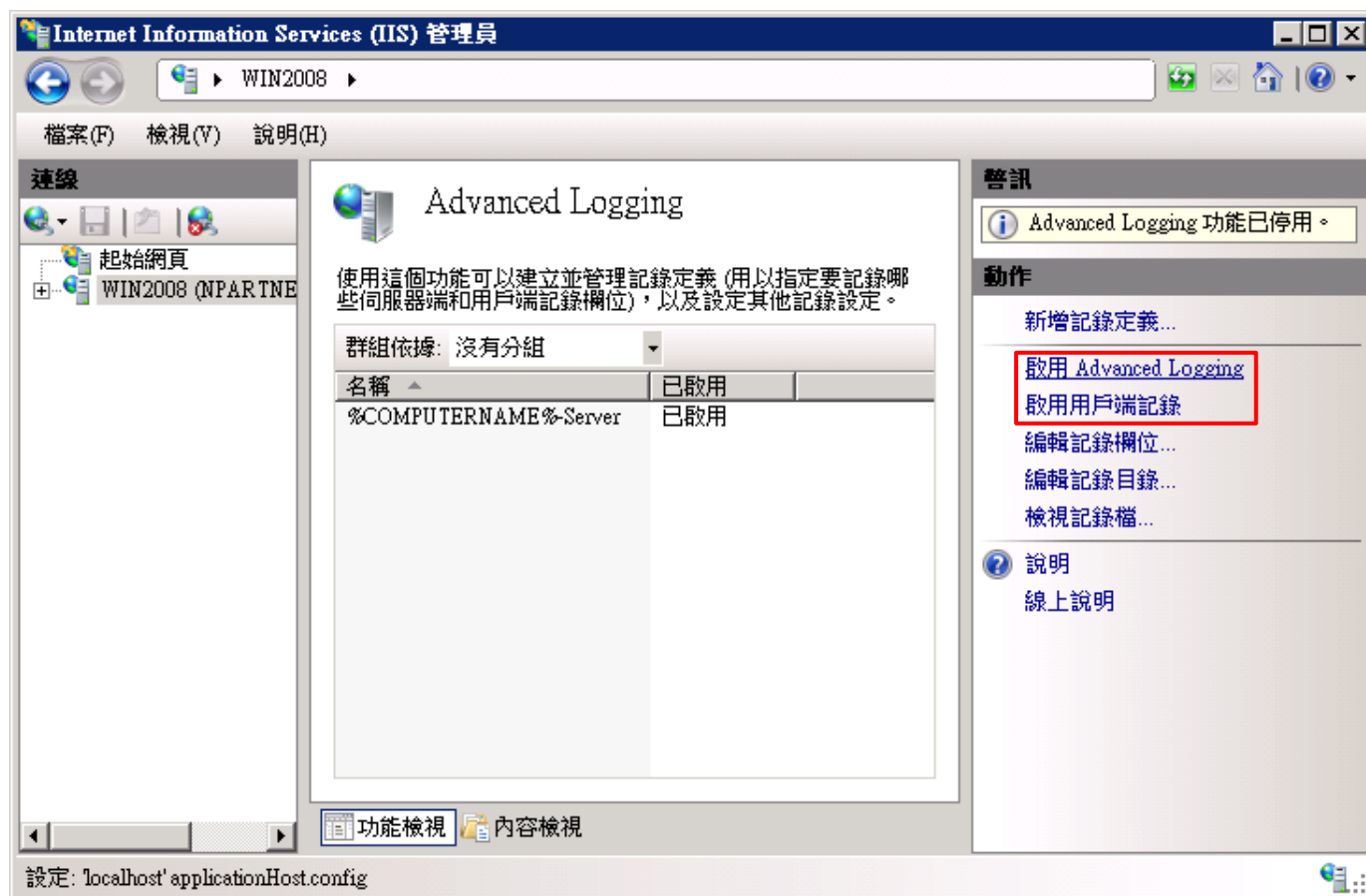
(9) 輸入欄位識別碼: **X-Forwarded-For** -> 選擇類別: [Default] -> 來源類型: [要求標頭] -> 輸入來源名稱: **X-Forwarded-For** -> 按 [確定]



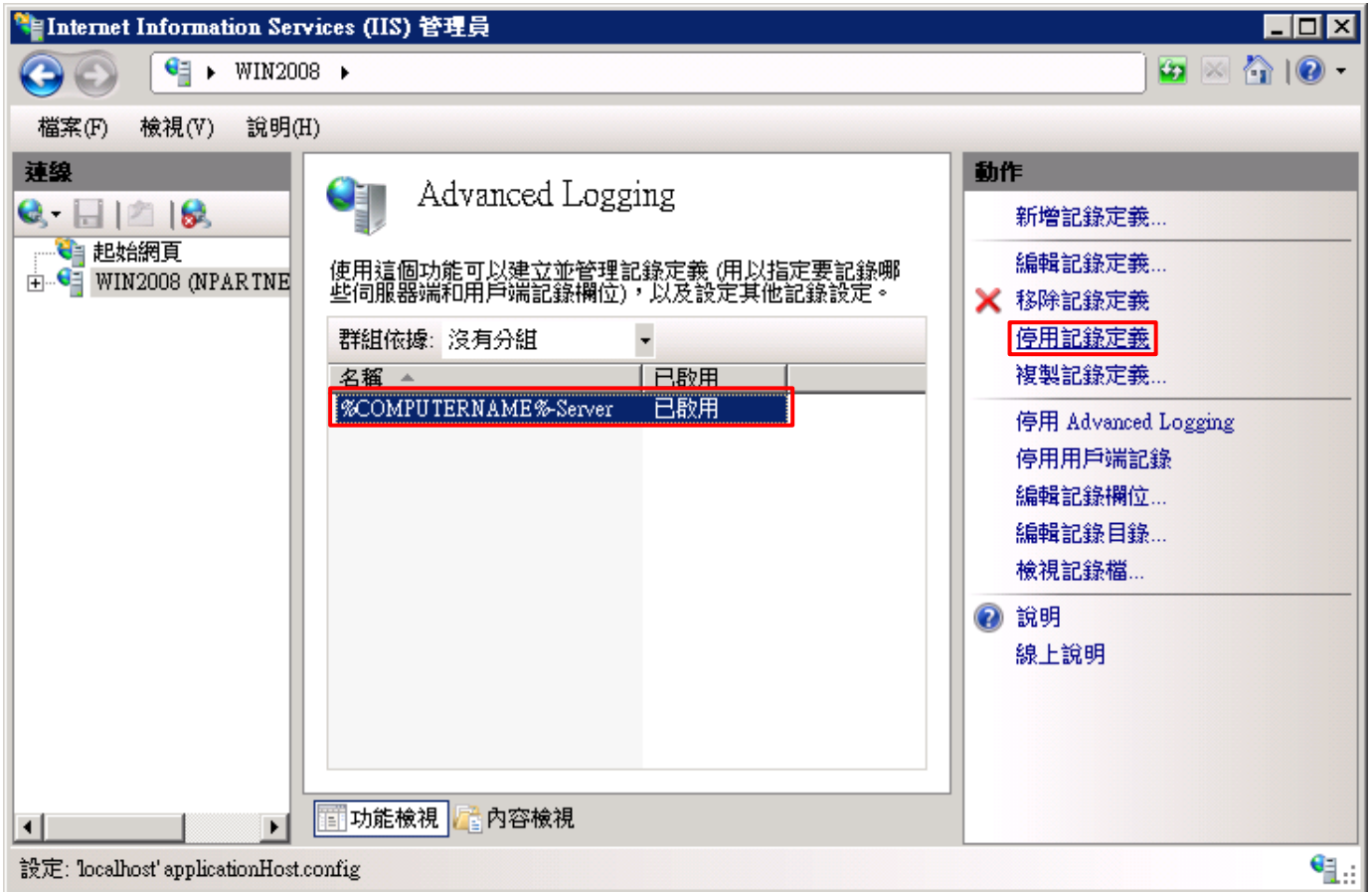
(10) 按 [確定]



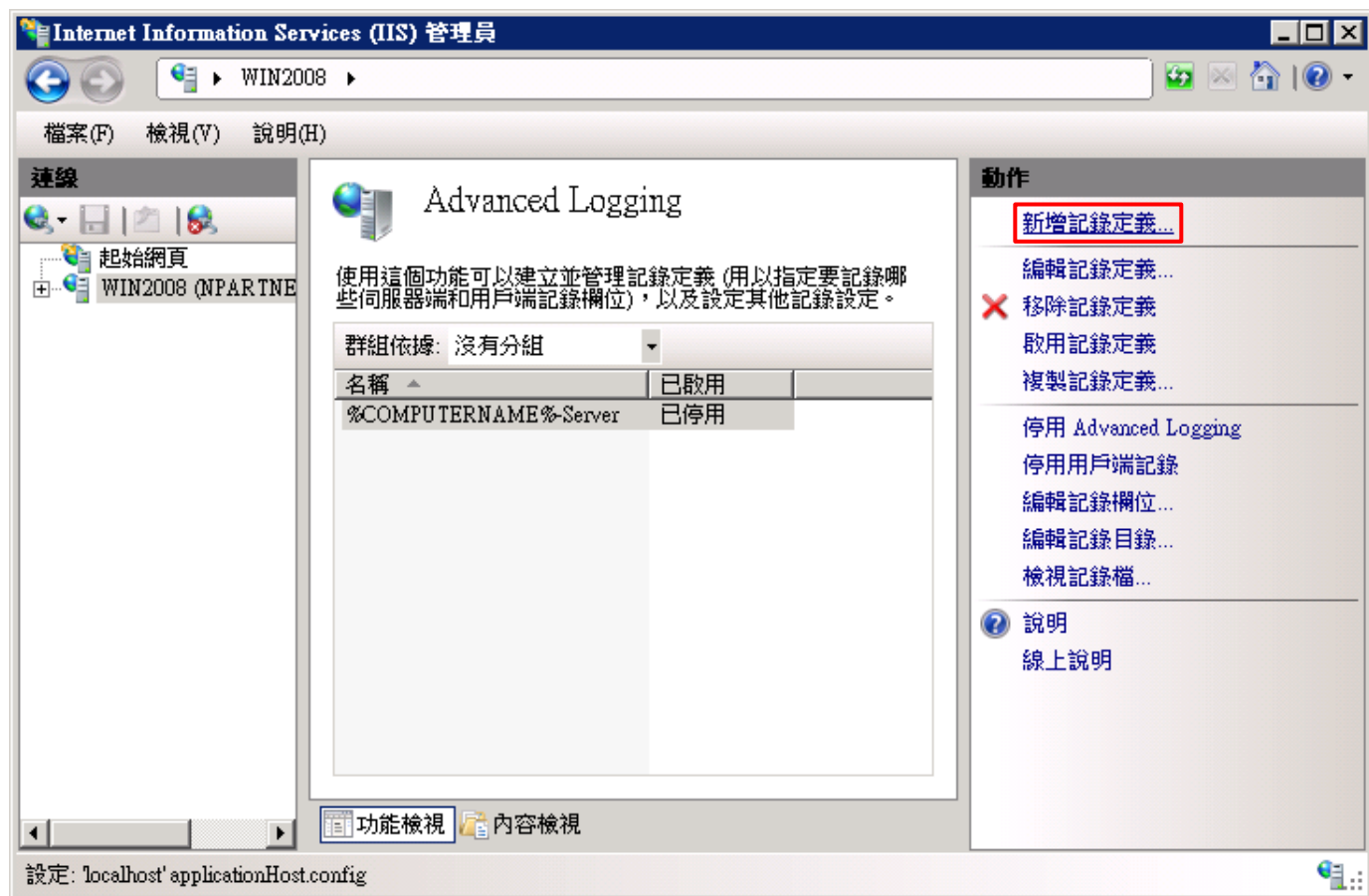
(11) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]



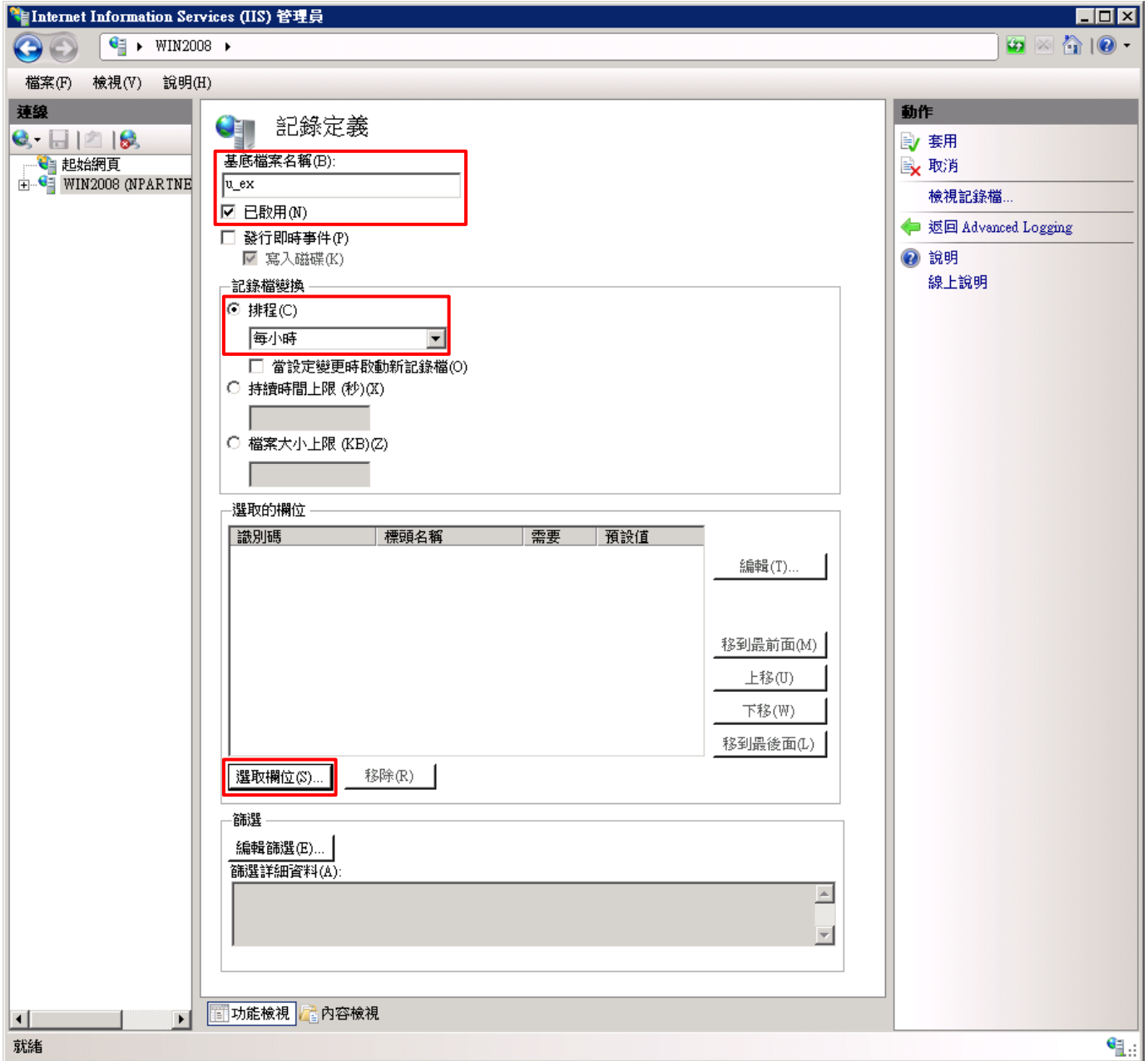
(12) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]



(13) 點選 [新增記錄定義]



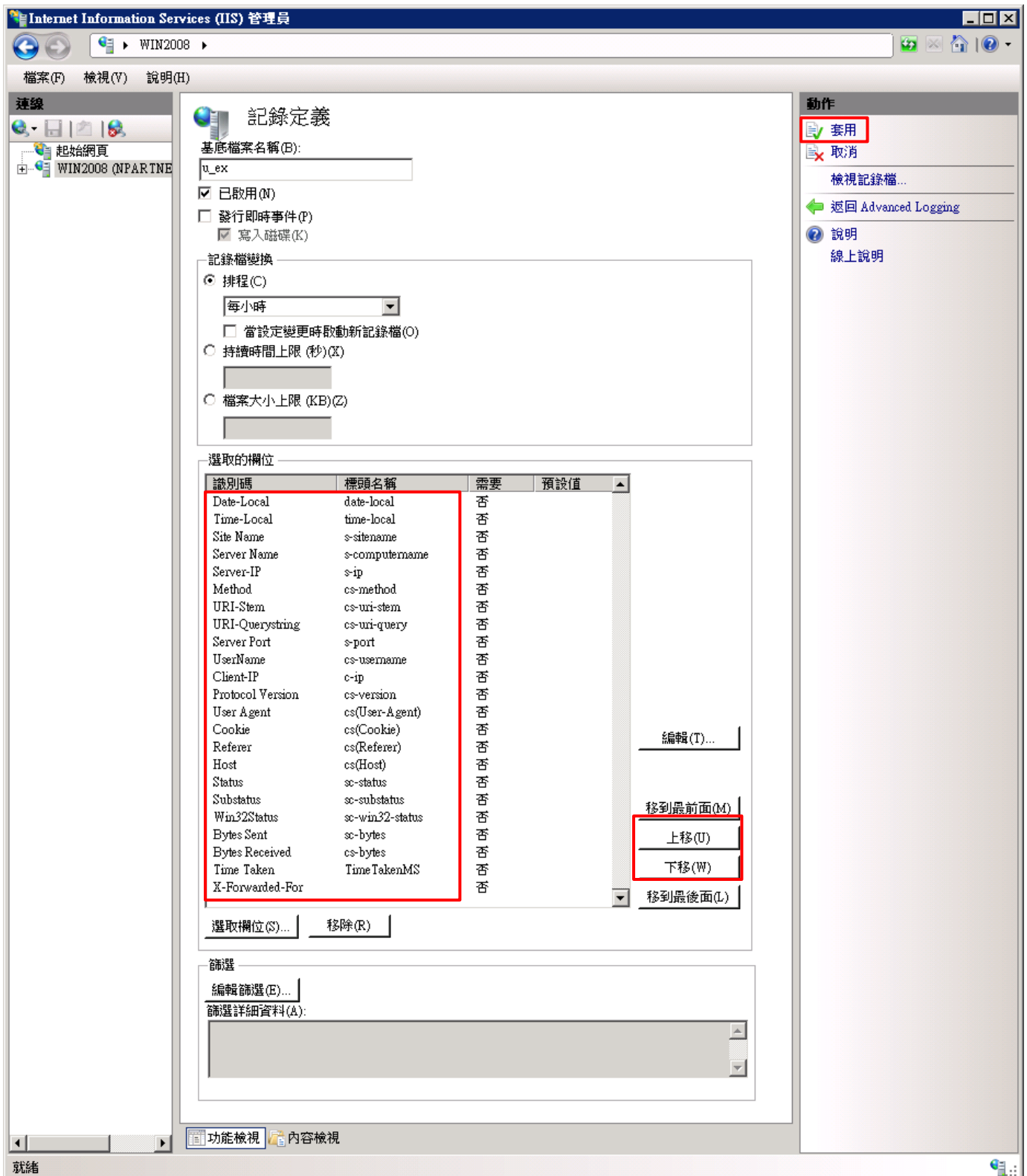
(14) 輸入基底檔案名稱: u_ex -> 勾選 [已啟用] -> 選擇排程: [每小時] -> 按 [選取欄位]



(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]

Internet Information Services (IIS) 管理員

WIN2008

檔案(F) 檢視(V) 說明(H)

記錄定義

基礎檔案名稱(B):
u_ex

已啟用(M)
 發行即時事件(P)
 寫入磁碟(K)

記錄檔變換

排程(C)
 每小時

當設定變更時啟動新記錄檔(O)
 持續時間上限 (秒)(X)
 檔案大小上限 (KB)(Z)

選取的欄位

識別碼	標頭名稱	需要	預設值
Date-Local	date-local	否	
Time-Local	time-local	否	
Site Name	s-sitename	否	
Server Name	s-computename	否	
Server-IP	s-ip	否	
Method	cs-method	否	
URI-Stem	cs-uri-stem	否	
URI-QueryString	cs-uri-query	否	
Server Port	s-port	否	
UserName	cs-username	否	
Client-IP	c-ip	否	
Protocol Version	cs-version	否	
User Agent	cs(User-Agent)	否	
Cookie	cs(Cookie)	否	
Referer	cs(Referer)	否	
Host	cs(Host)	否	
Status	sc-status	否	
Substatus	sc-substatus	否	
Win32Status	sc-win32-status	否	
Bytes Sent	sc-bytes	否	
Bytes Received	cs-bytes	否	
Time Taken	Time TakenMS	否	
X-Forwarded-For		否	

編輯(T)...
 移到最前面(M)
 上移(U)
 下移(W)
 移到最後面(L)

選取欄位(S)... 移除(R)

篩選
 編輯篩選(E)...
 篩選詳細資料(A):

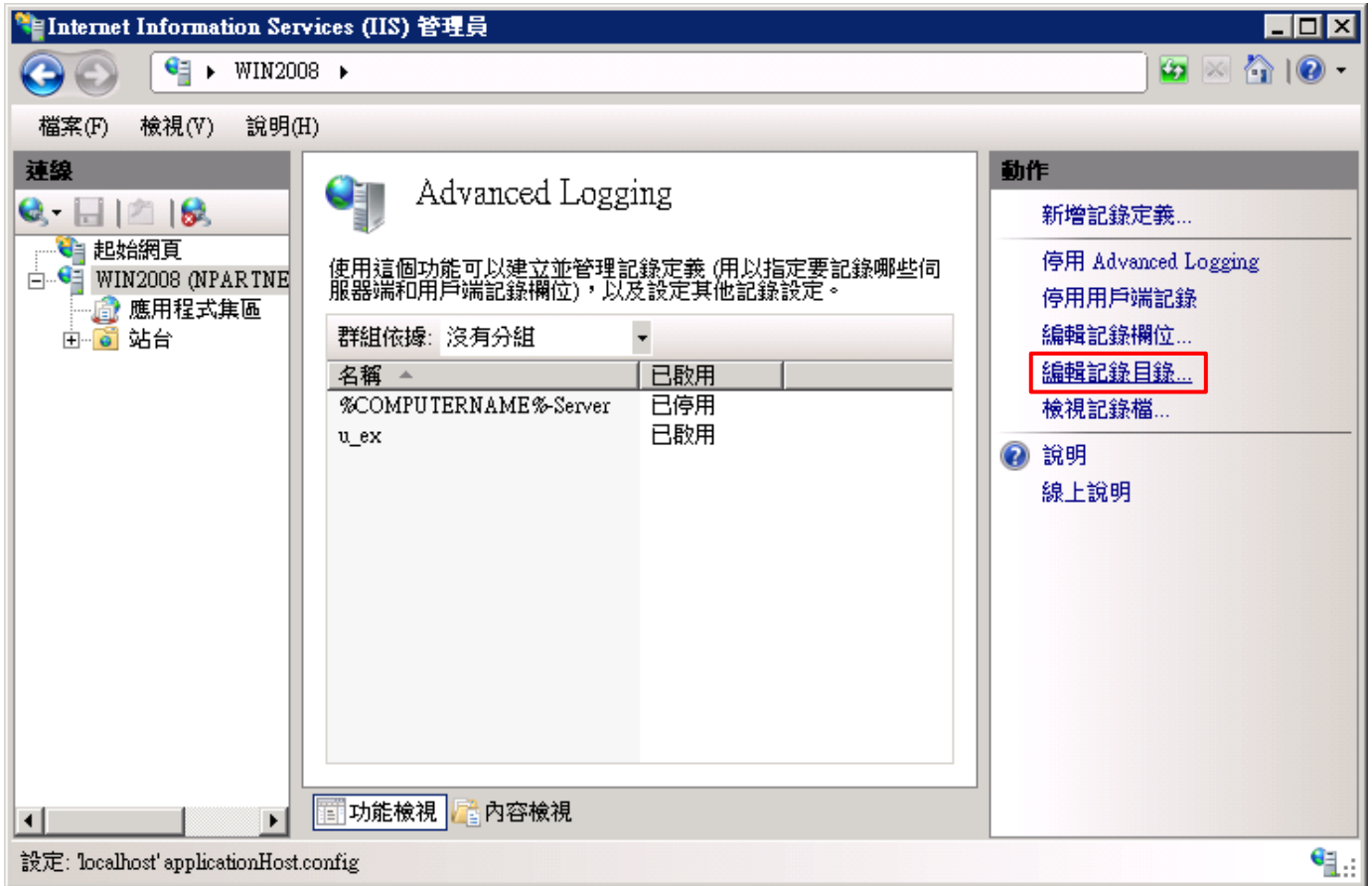
功能檢視 內容檢視

就緒

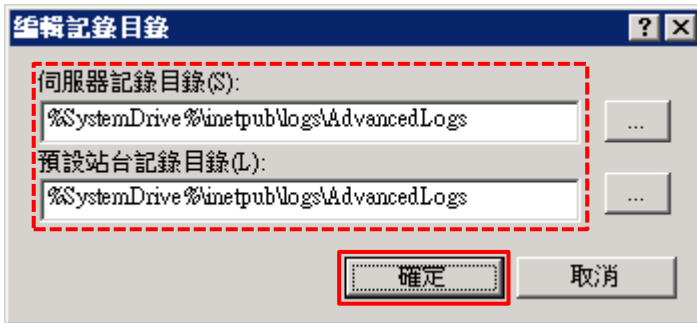
警訊
 變更已順利儲存。

動作
 套用
 取消
 檢視記錄檔...
返回 Advanced Logging
 說明
 線上說明

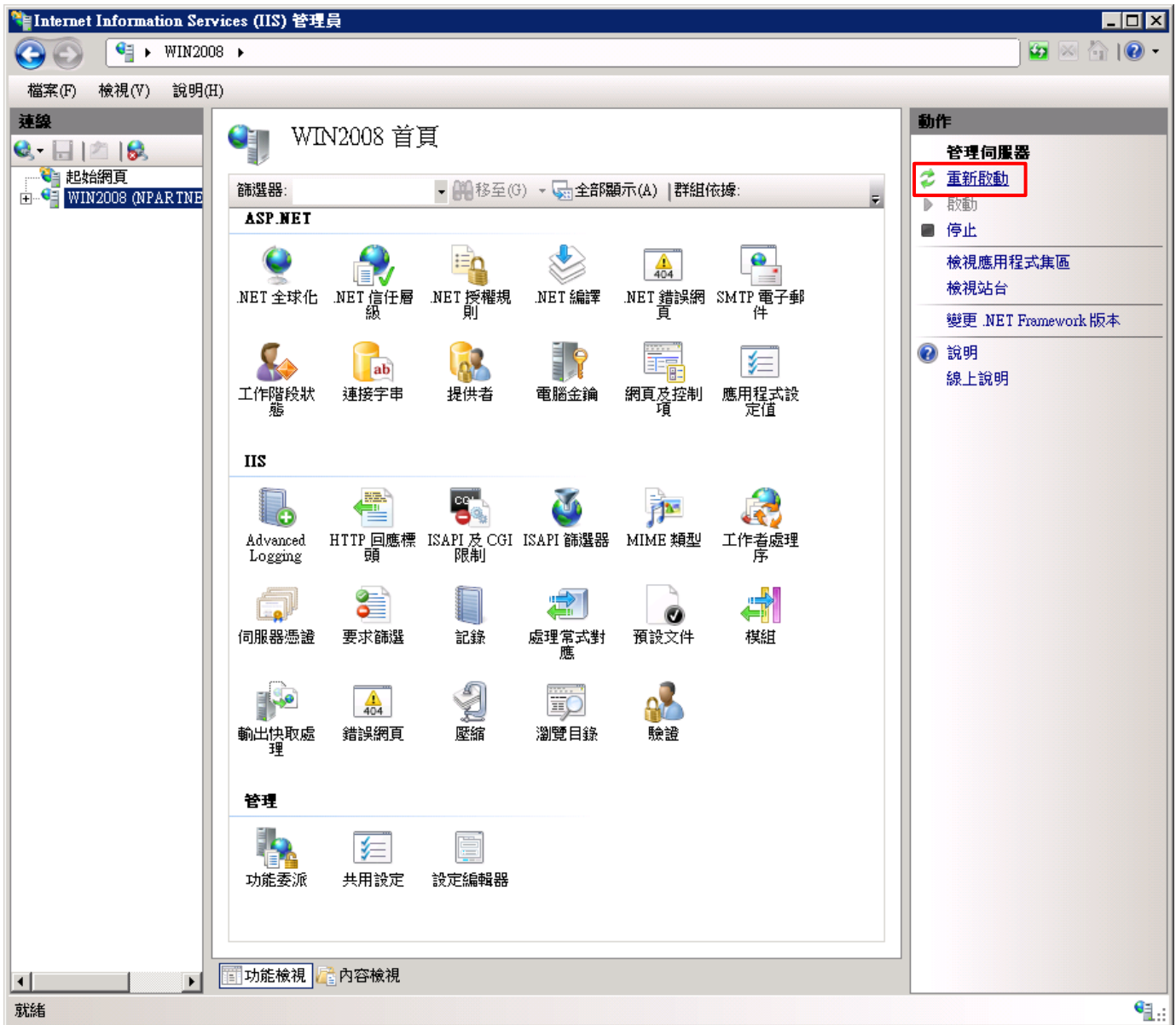
(18) 點選 [編輯記錄目錄]



(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

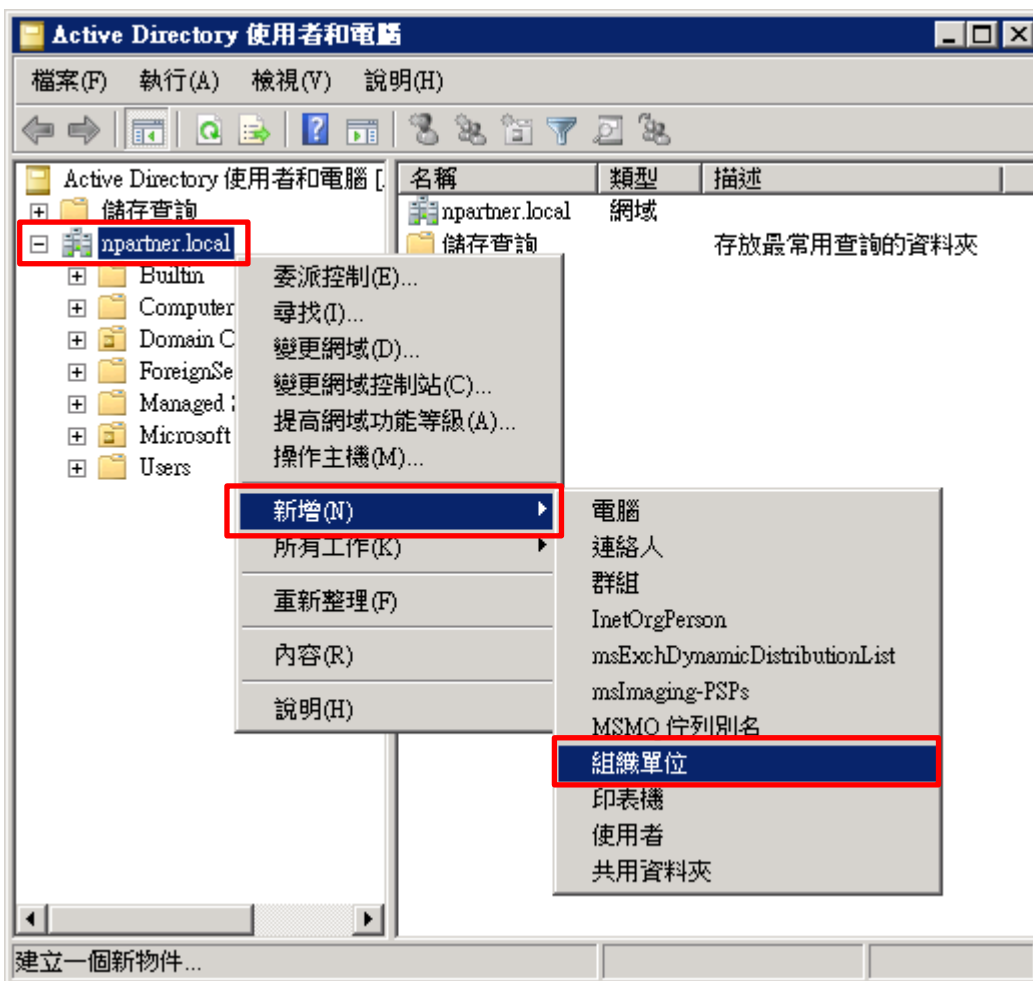
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



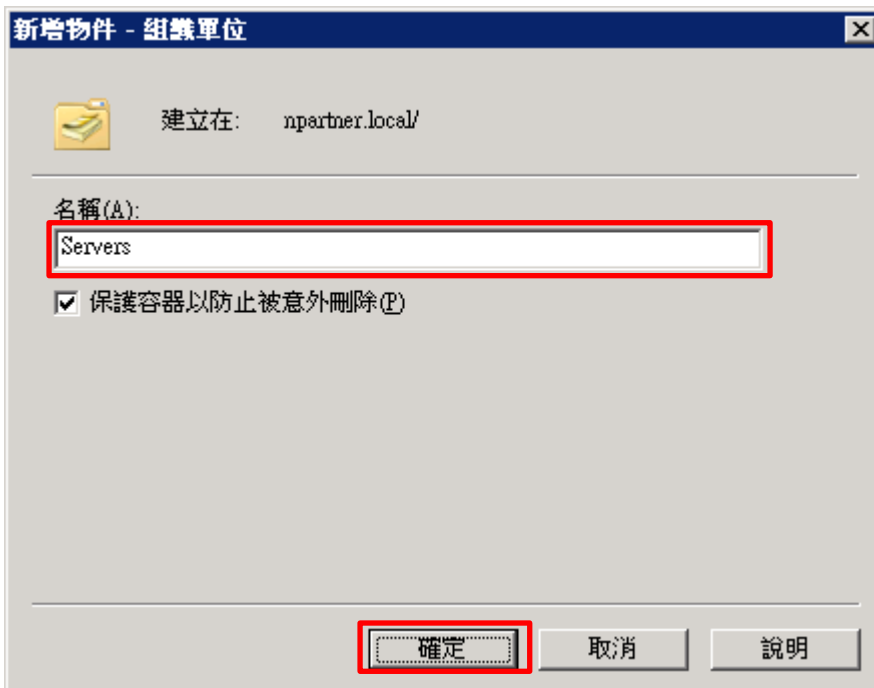
(2) 新增組織單位

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



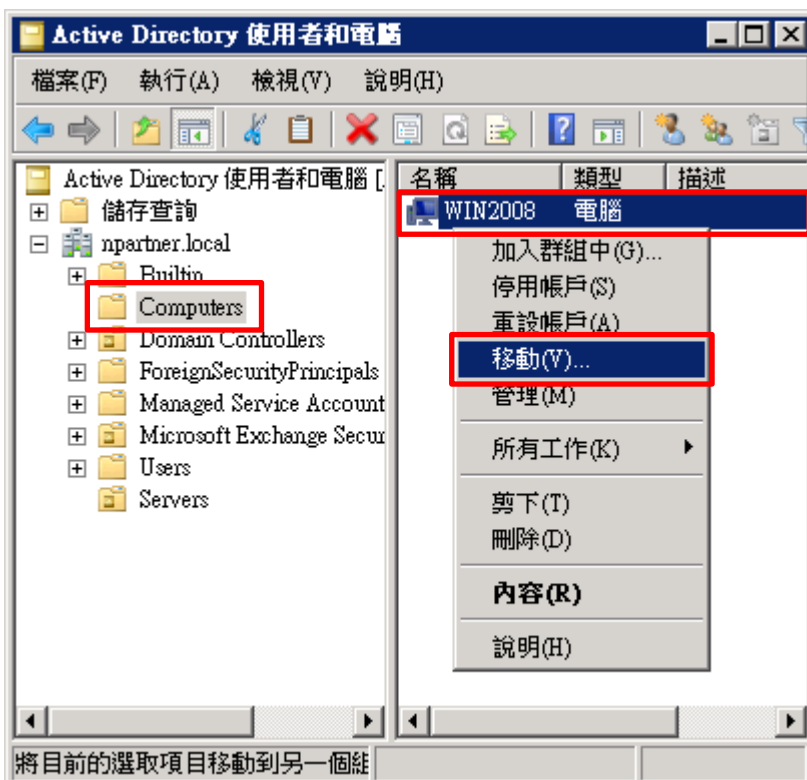
(3) 輸入組織單位名稱

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]



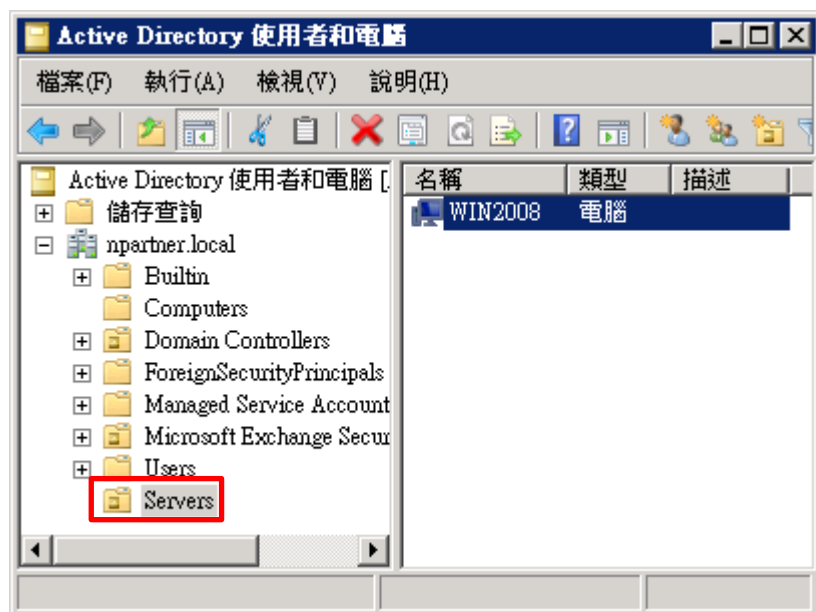
(5) 選擇組織單位

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

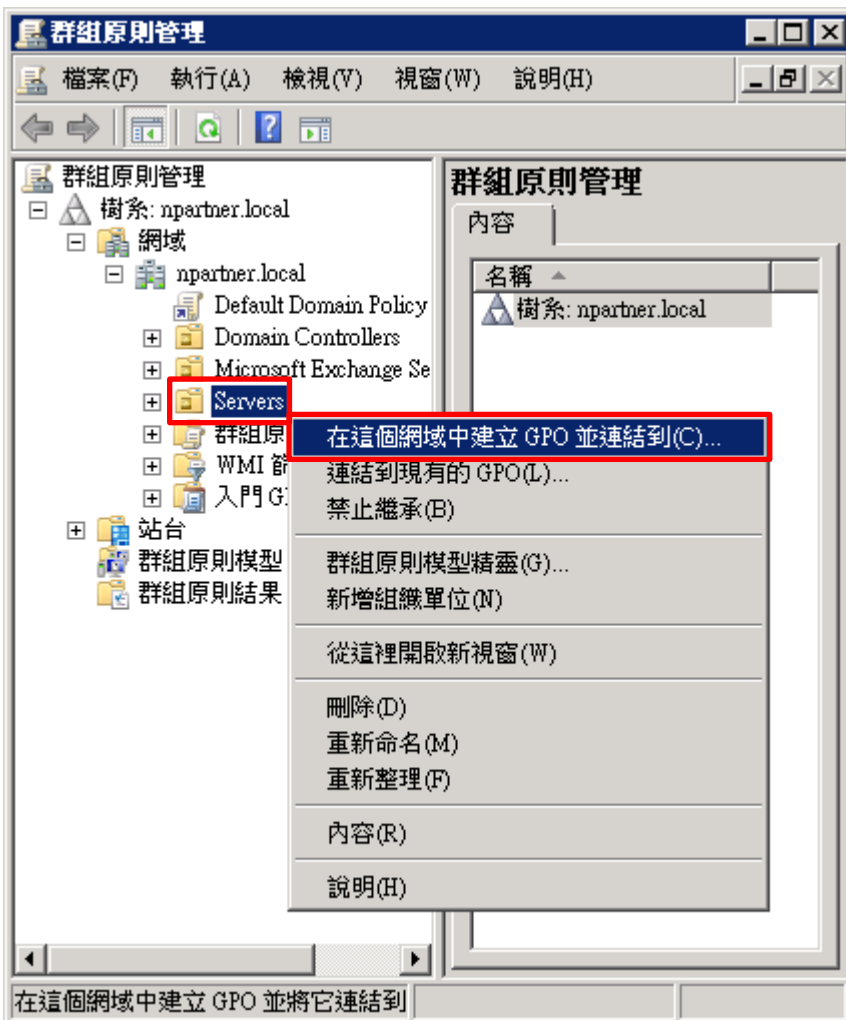
(1) 開啟群組原則管理

開啟 [群組原則管理]



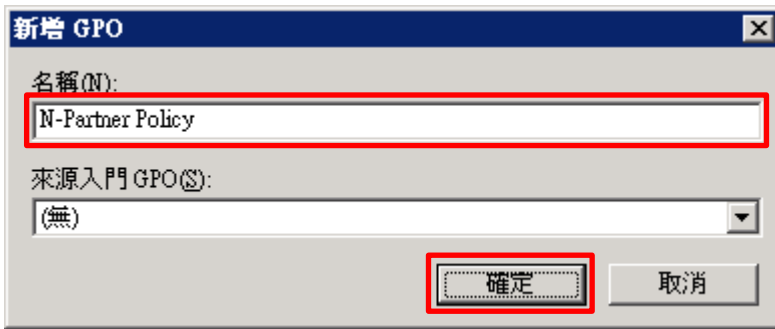
(2) 在 Servers 組織單位，新增群組原則物件

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...]



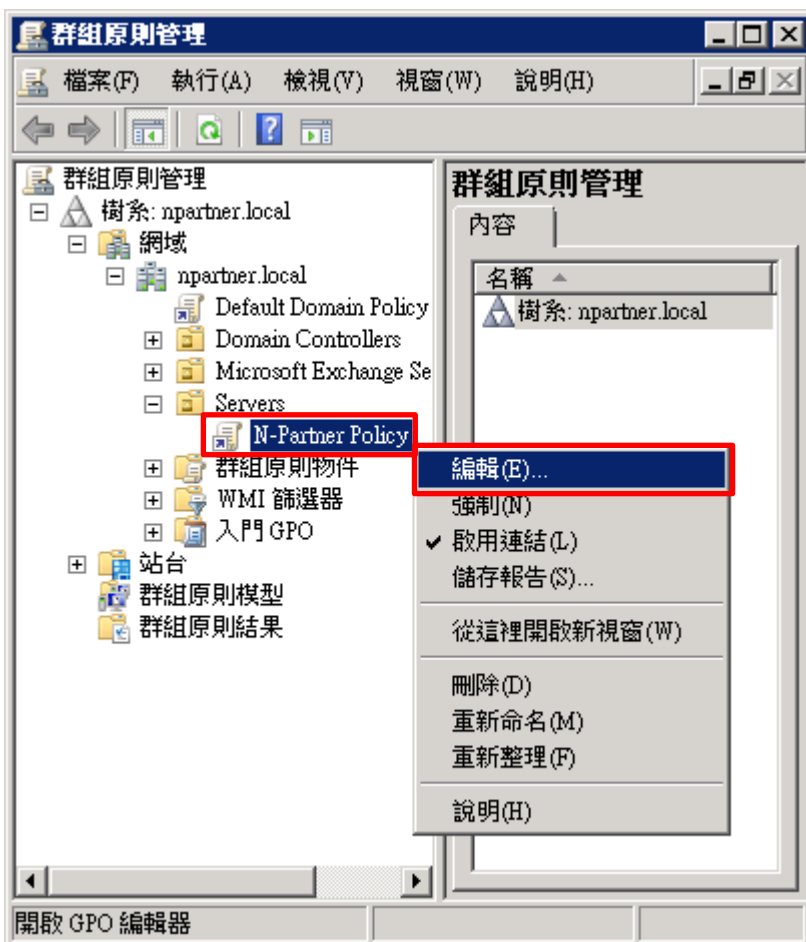
(3) 輸入群組原則物件名稱

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]



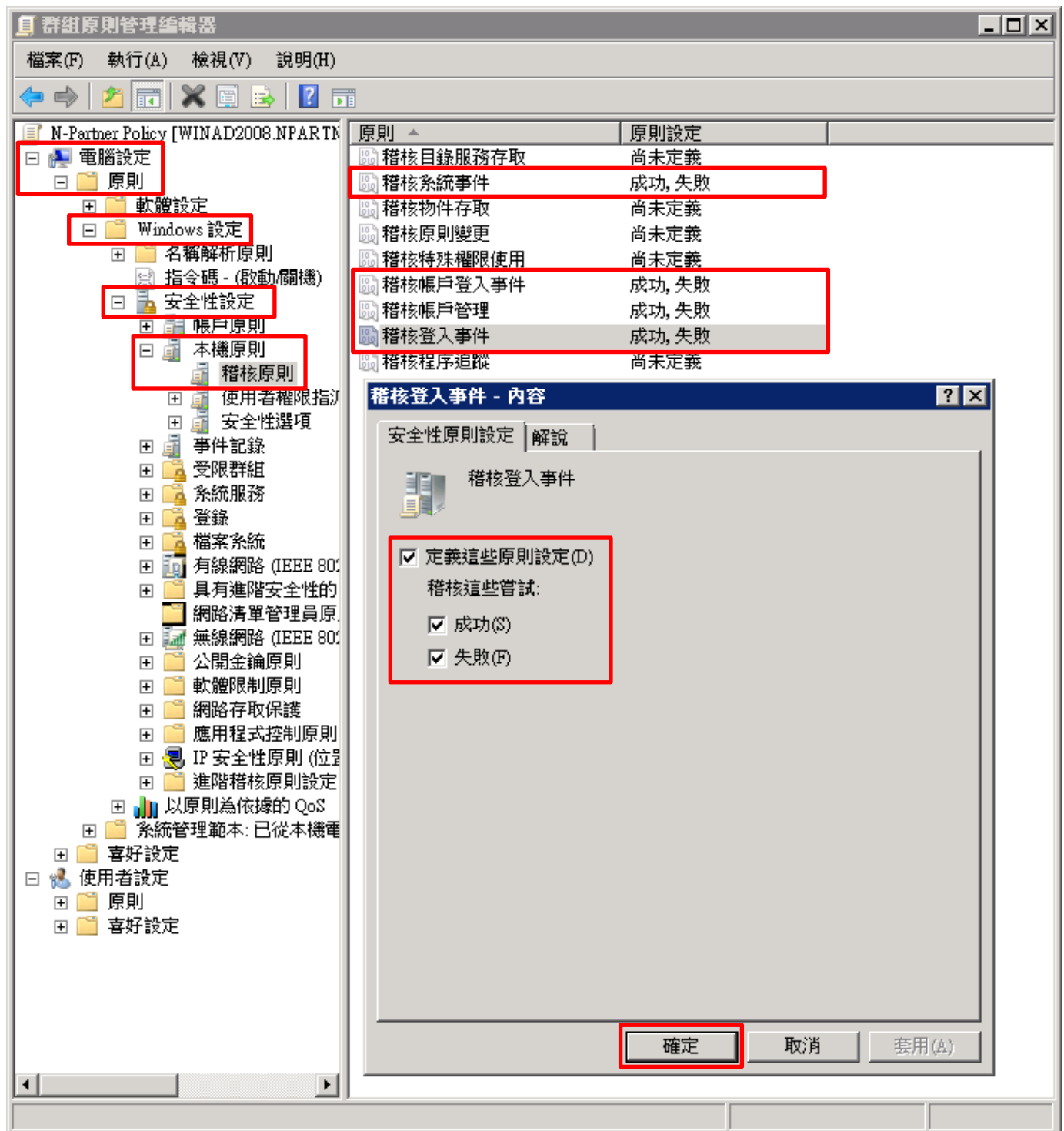
(4) 編輯群組原則物件

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



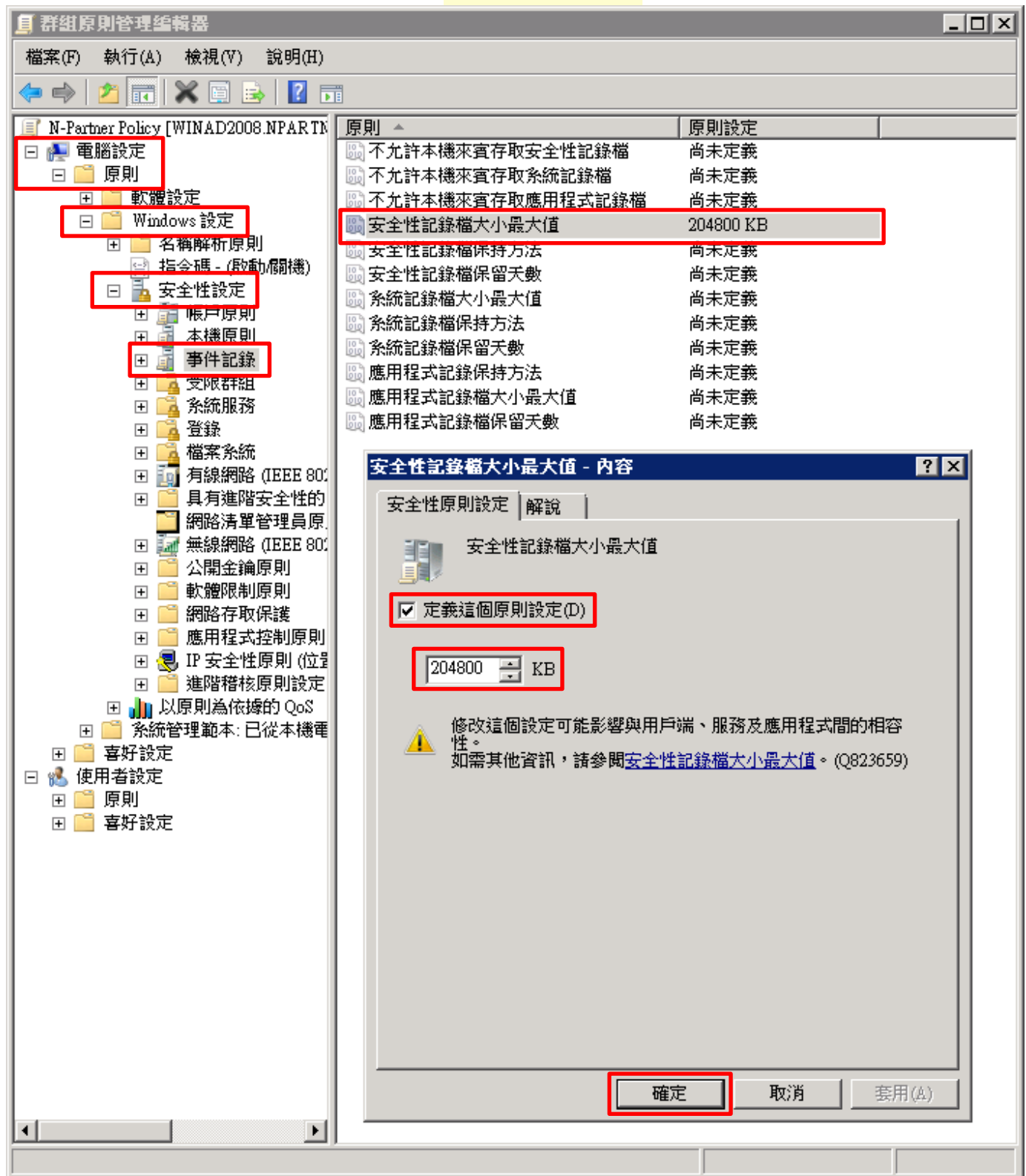
(5) 本機原則：稽核原則

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]



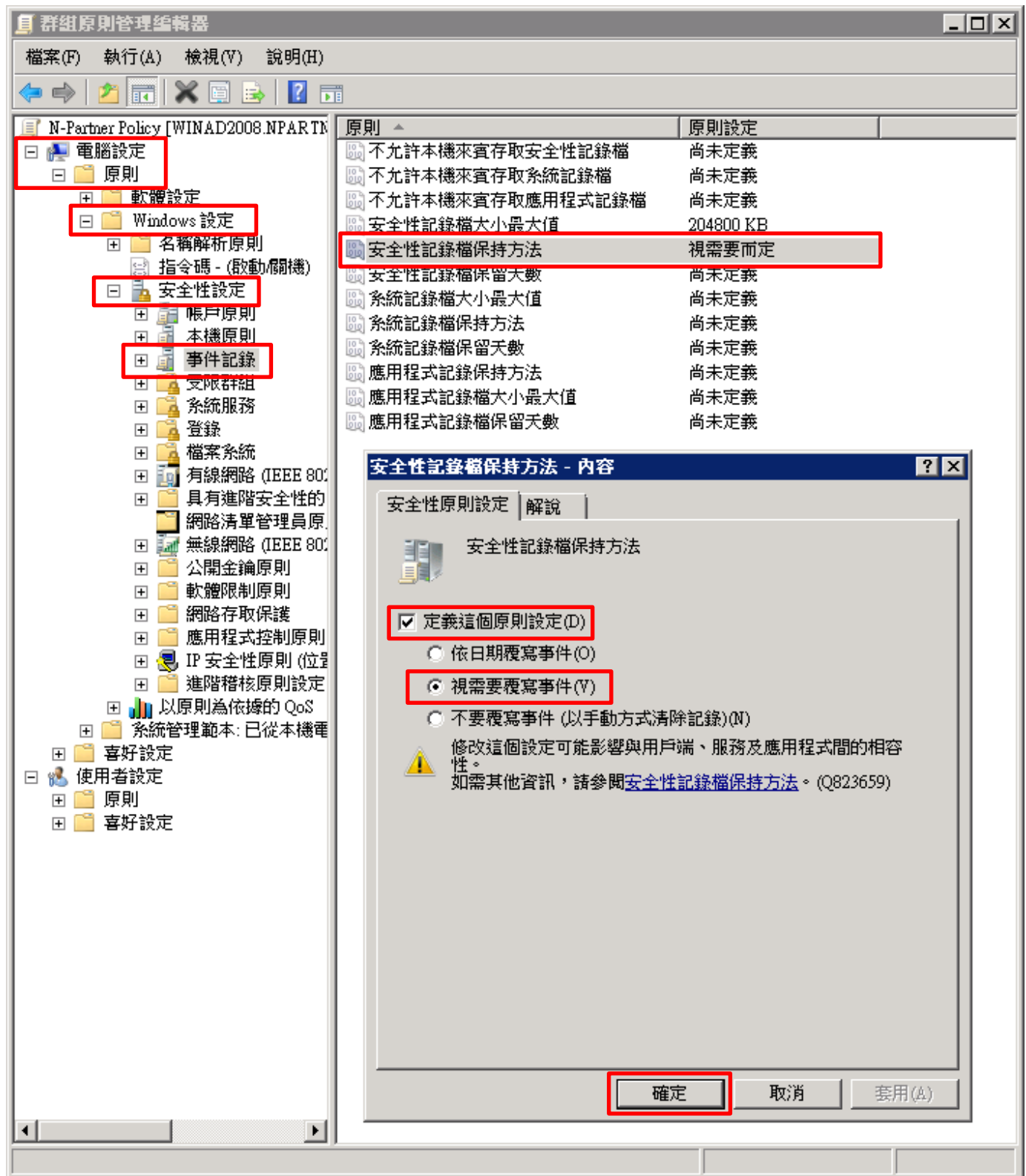
(6) 事件記錄：安全性記錄檔大小最大值

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

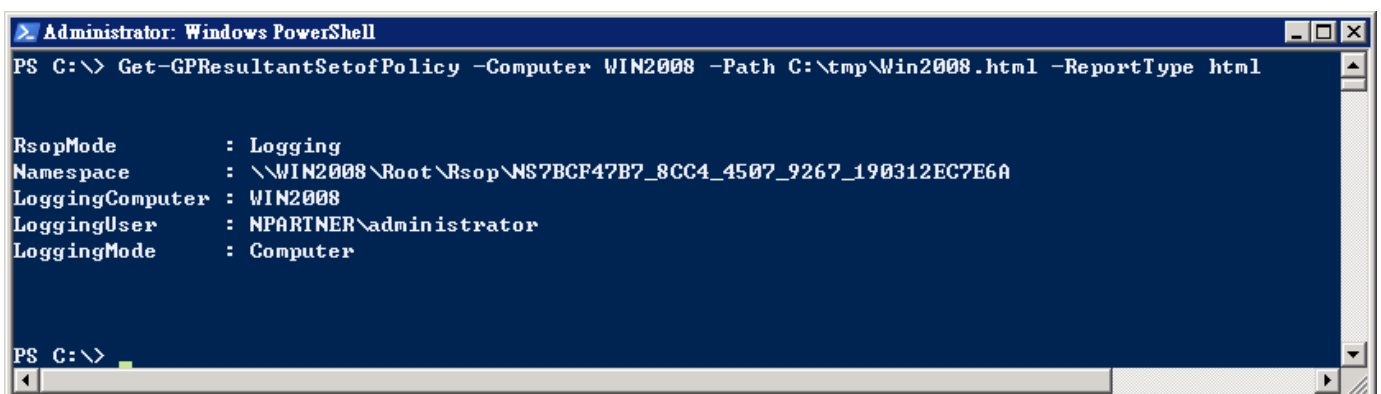


(10) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(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

NPARTNER\WIN2008 - Windows Internet Explorer

C:\tmp\Win2008.html

我的最愛 NPARTNER\WIN2008

群組原則結果

NPARTNER\WIN2008
資料收集: 2021/11/17 下午 02:14:22 顯示全部

摘要 顯示

電腦設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

公開金鑰原則/被信任的根憑證授權單位 顯示

使用者設定 顯示

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

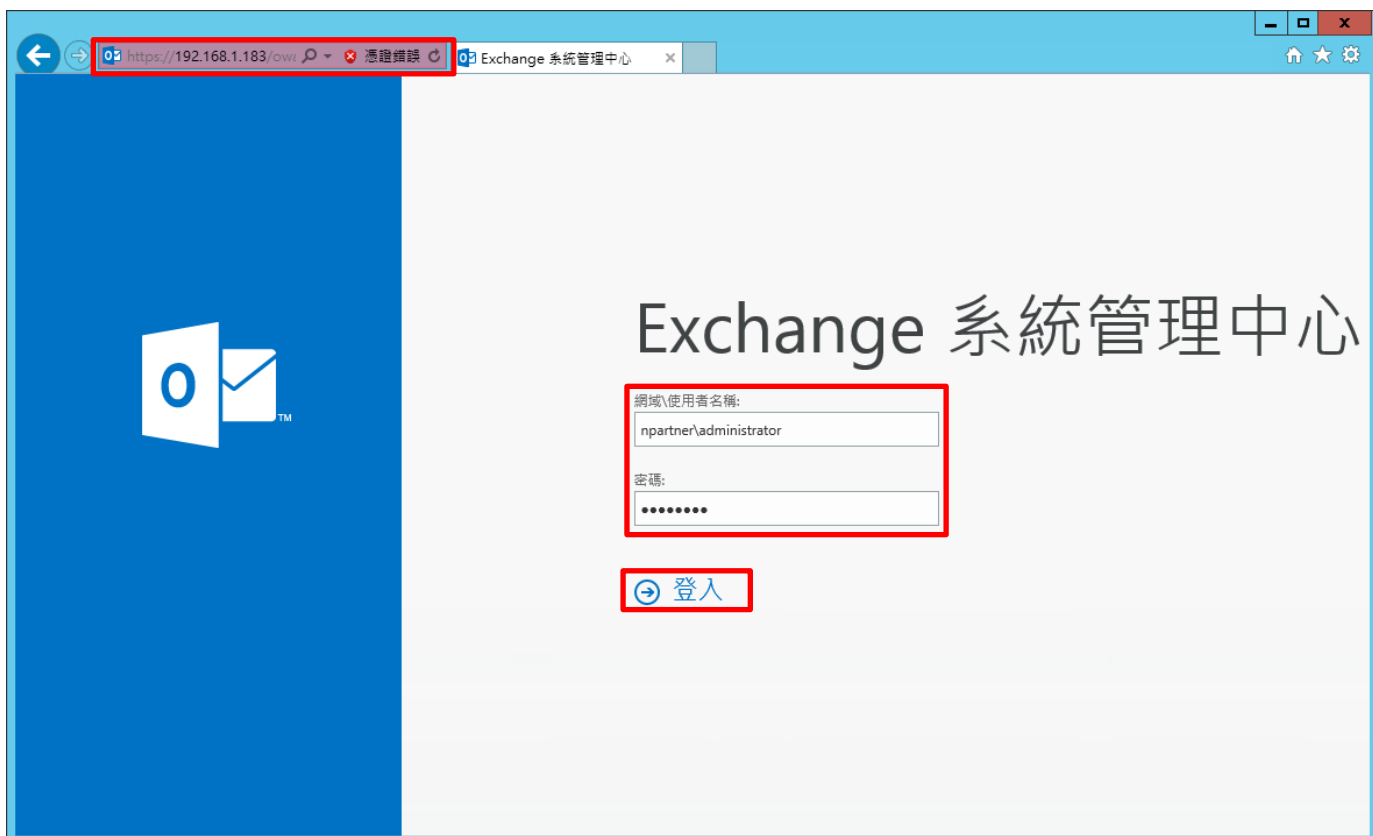
```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```


4.1.1 Exchange Administrative Center

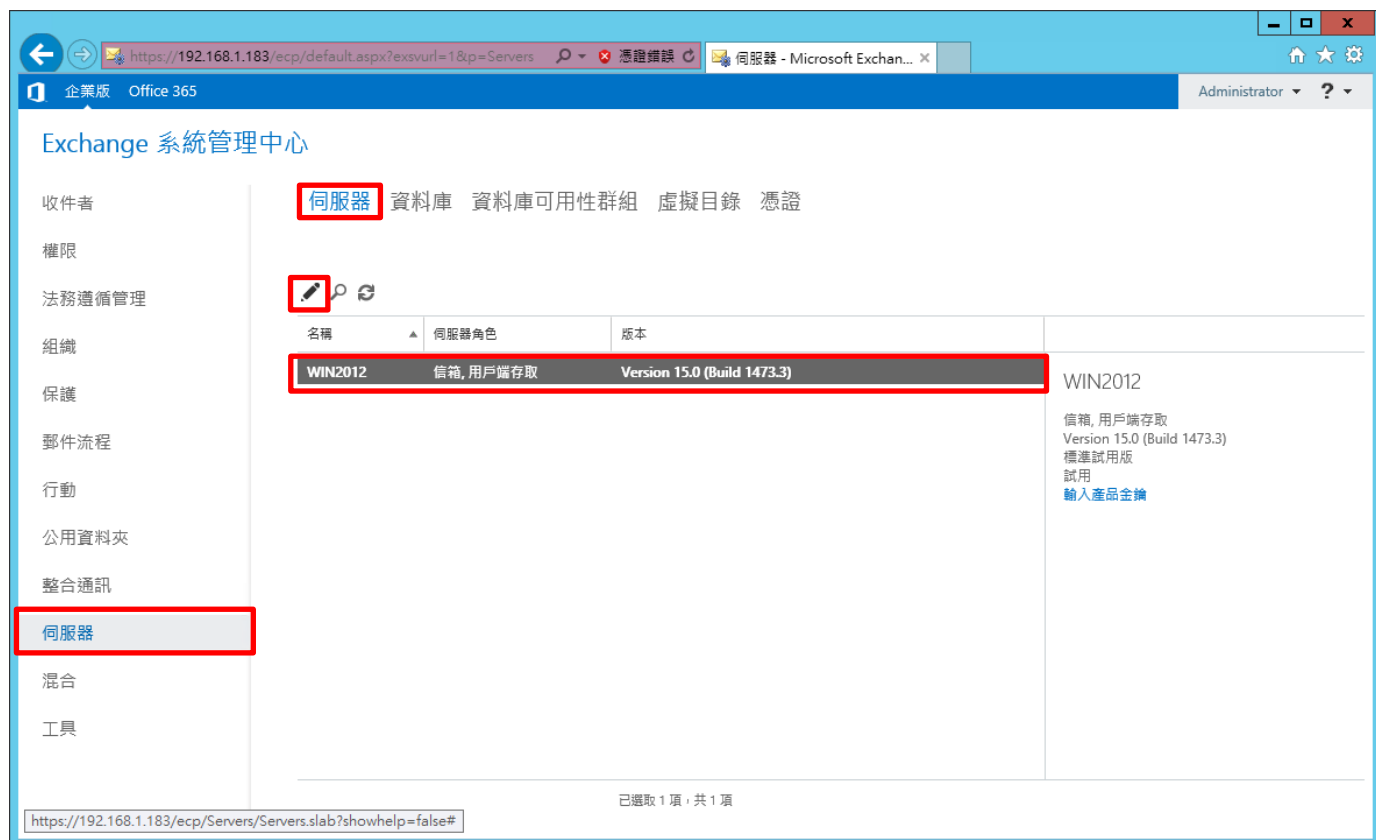
(1) 開啟 [瀏覽器]



(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)



The screenshot shows the Exchange System Management Center (EMC) interface. The left sidebar contains navigation options: 收件者, 權限, 法務遵循管理, 組織, 保護, 郵件流程, 行動, 公用資料夾, 整合通訊, 伺服器 (highlighted), 混合, and 工具. The main content area is titled "Exchange 系統管理中心" and shows a list of servers. The "伺服器" link in the top navigation bar is highlighted. Below it, there are icons for edit, search, and refresh. A table lists the server details:

名稱	伺服器角色	版本
WIN2012	信箱, 用戶端存取	Version 15.0 (Build 1473.3)

The "WIN2012" row is highlighted. To the right of the table, the server name "WIN2012" is displayed, along with its role "信箱, 用戶端存取", version "Version 15.0 (Build 1473.3)", and status "標準試用版 試用". A link "輸入產品全鍵" is also visible. At the bottom of the page, it says "已選取 1 項, 共 1 項".

(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]

Exchange 伺服器 - Internet Explorer

https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=454958ba-d6f1-431a-l 憑證錯誤

WIN2012 說明

一般
資料庫和資料庫可用性
群組
POP3
IMAP4
整合通訊
DNS 查閱
傳輸限制
▶ 傳輸記錄檔
Outlook Anywhere

郵件追蹤記錄檔
 啟用郵件追蹤記錄檔
郵件追蹤記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\Transportf

連線記錄檔
 啟用連線記錄檔
連線記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\Transportf

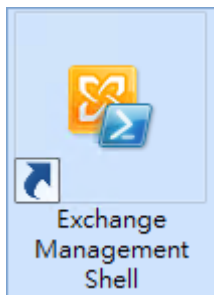
通訊協定記錄檔
傳送通訊協定記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRole
接收通訊協定記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRole

儲存 取消

https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=454958ba-d6f1-431a-l 100%

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*

機器: Win2012.npartner.local

歡迎使用 Exchange 管理命令介面!

完整的 Cmdlet 清單: Get-Command
只有 Exchange Cmdlet: Get-ExCommand
符合特定字串的 Cmdlet: 說明 *<string>*
取得一般說明: 說明
取得 Cmdlet 的說明: Help <cmdlet name> 或 <cmdlet name> -?
Exchange 團隊部落格: Get-ExBlog
顯示命令的完整輸出: <command> ! Format-List

顯示快速參考指南: QuickRef
每日提示 #16:

若要取得 Exchange 2013 伺服器上屬於已啟用整合通訊的所有使用者之清單, 請輸入:

$Mailboxes = Get-Mailbox
$Mailboxes = !ForEach < If<$_.UnEnabled -Eq $True><$_.Name>>

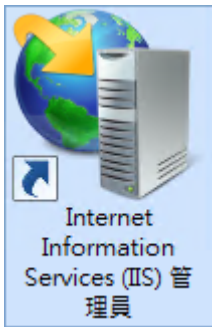
詳細資訊: 連線至 Win2012.npartner.local °
詳細資訊: 已連線至 Win2012.npartner.local °
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2013>Get-TransportService win2012 | Select-Object *Track*
MessageTrackingLogEnabled           : True
MessageTrackingLogMaxAge            : 30.00:00:00
MessageTrackingLogMaxDirectorySize  : 1000 MB (1,048,576,000 bytes)
MessageTrackingLogMaxFileSize       : 10 MB (10,485,760 bytes)
MessageTrackingLogPath              : C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True

[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2013>
```

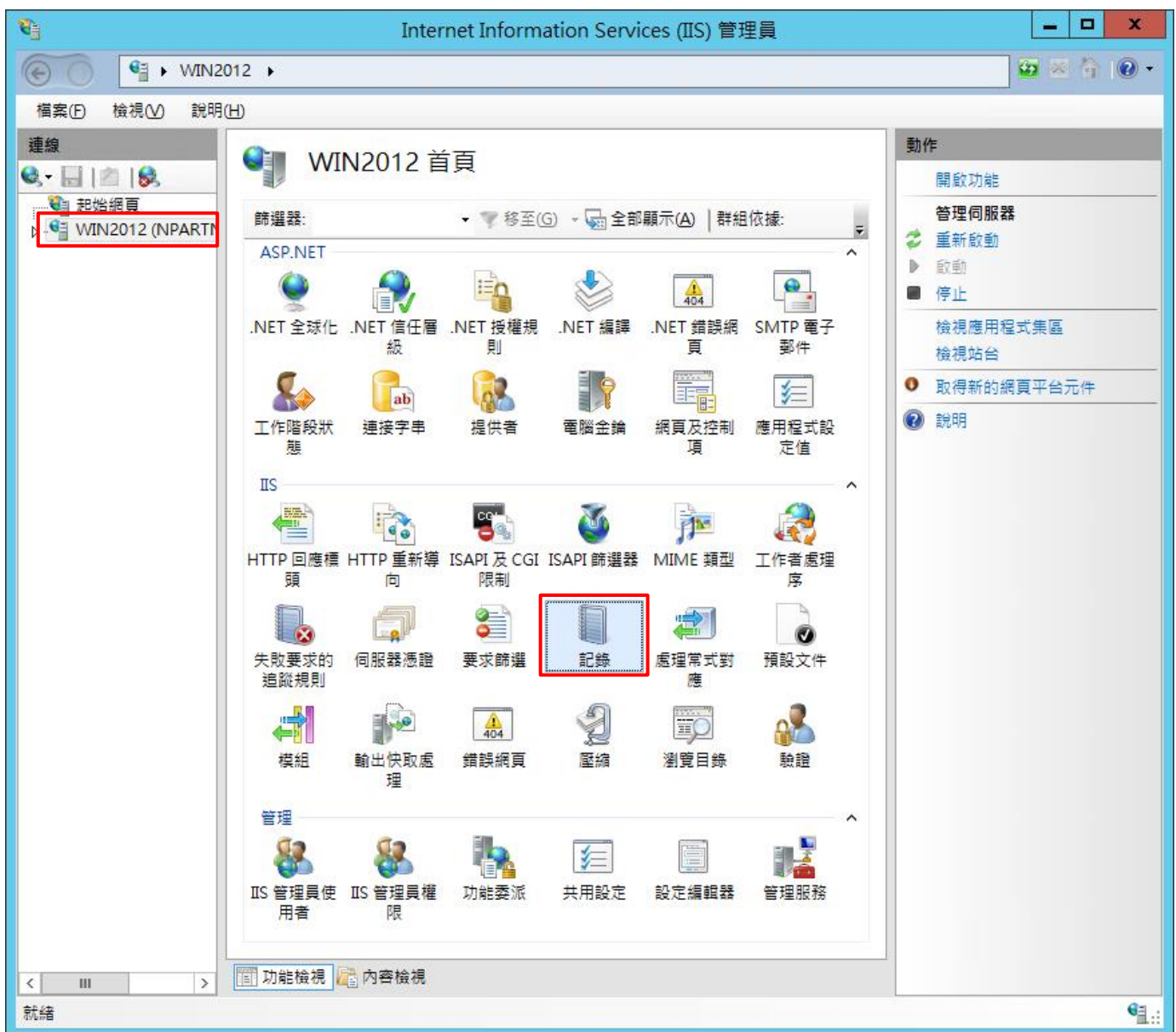
紅色文字部位請輸入 Exchange 伺服器名稱

4.2 IIS Log

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

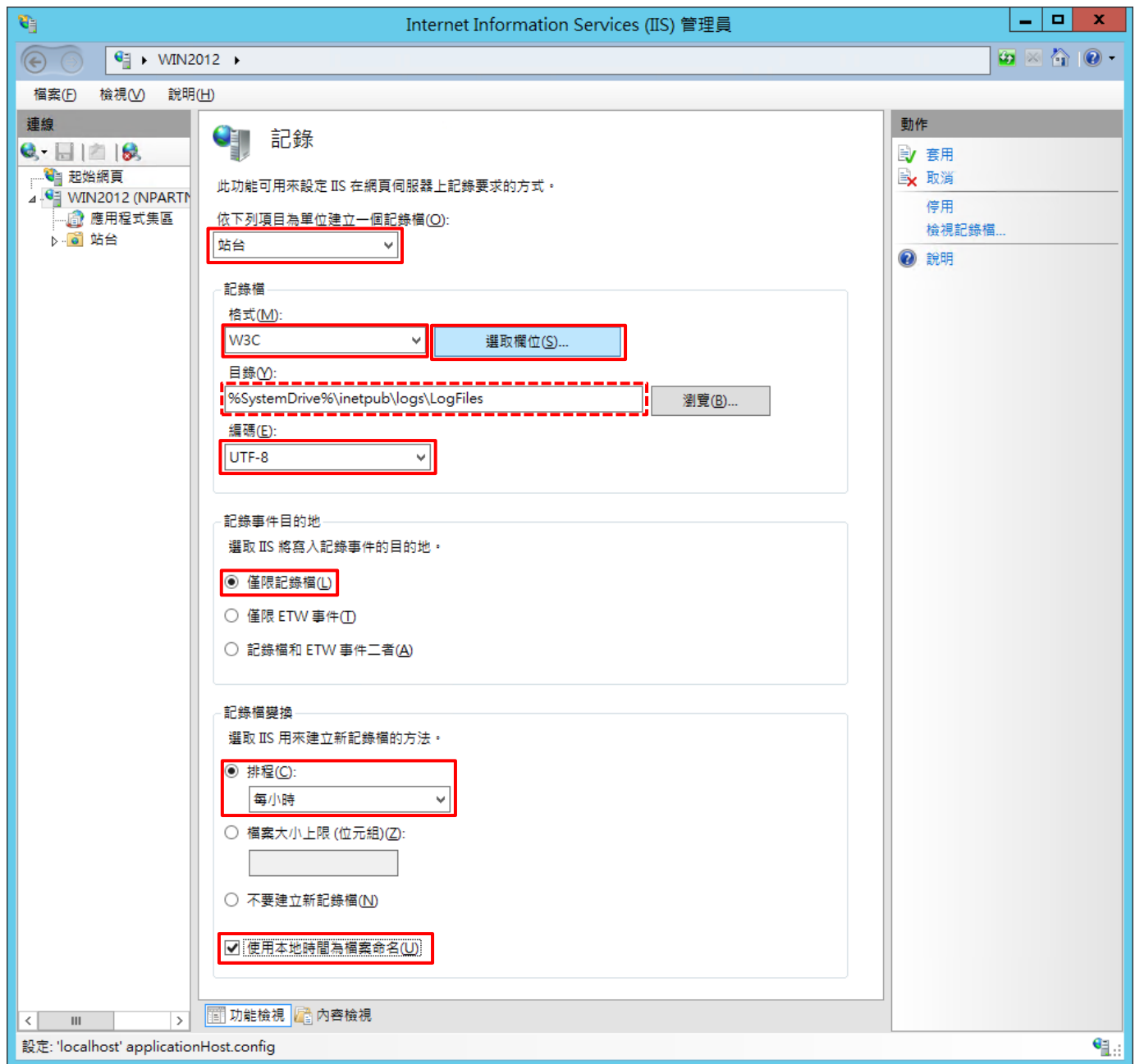


(2) 選擇 [IIS 伺服器] -> 點選 [記錄]

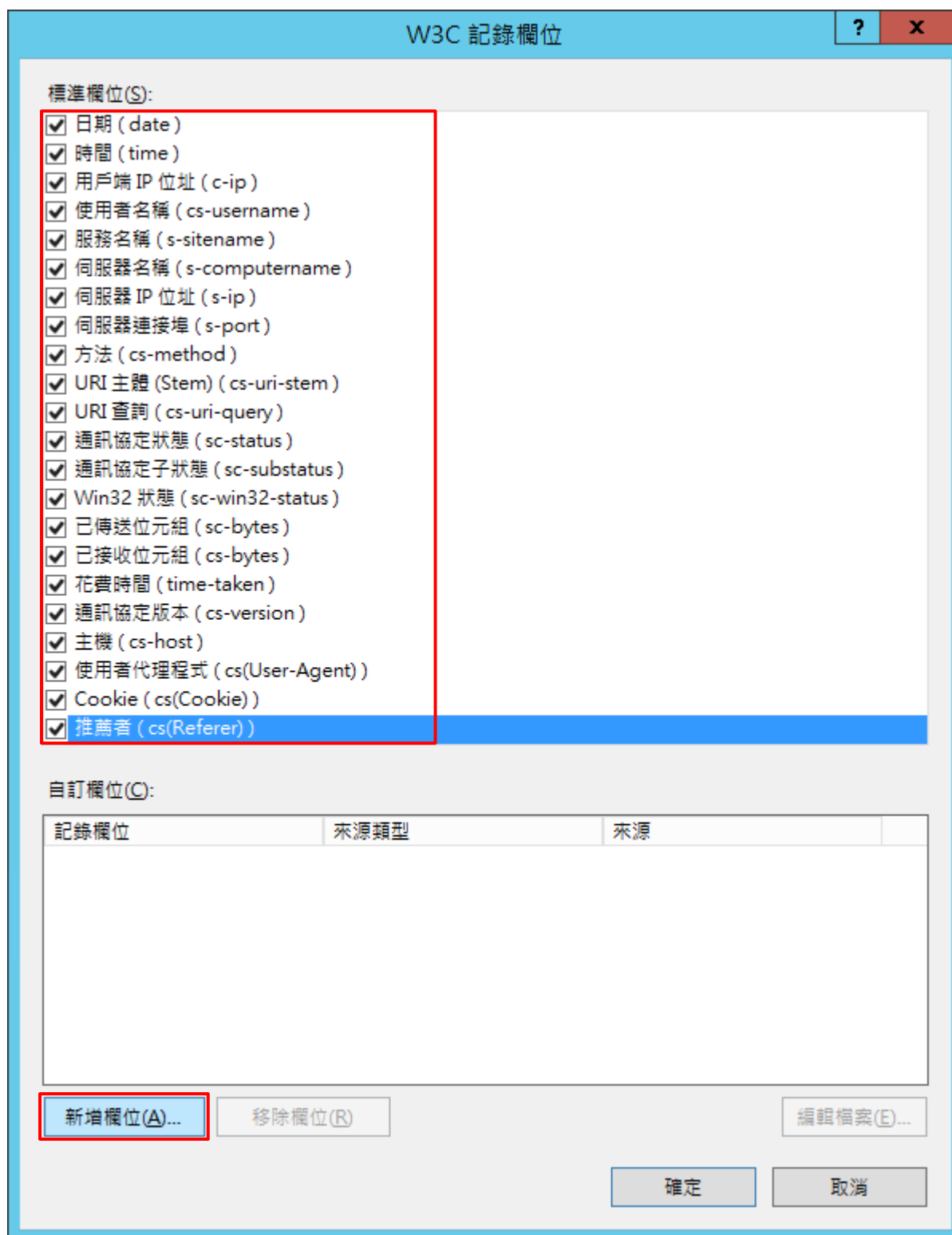


(3) 選擇依下列項目為單位建立一個記錄檔: [站台] -> 記錄檔格式: [W3C] -> 目錄:

[%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]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按 [確定]

W3C 記錄欄位

標準欄位(S):

- 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 (Stem) (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)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

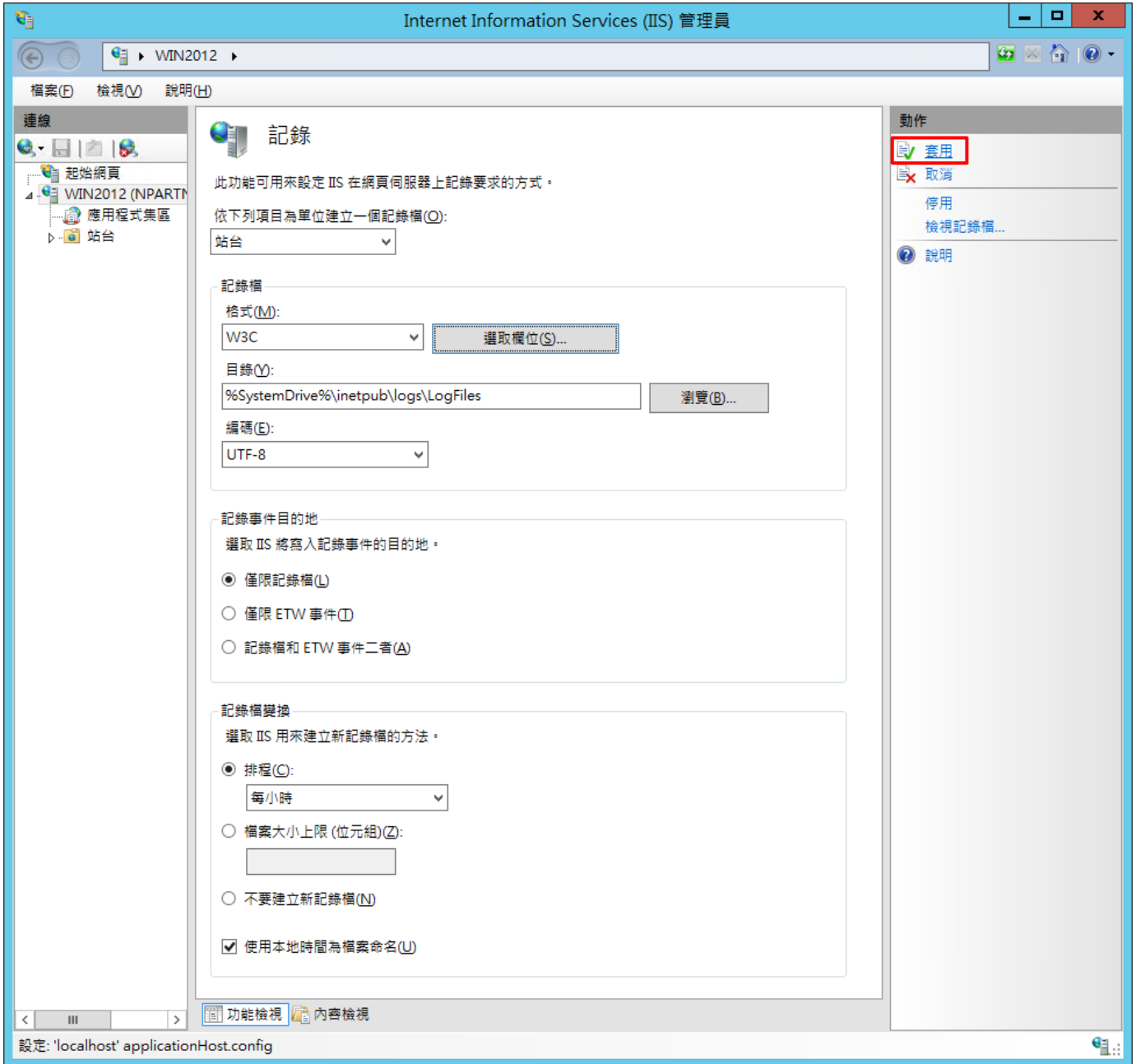
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

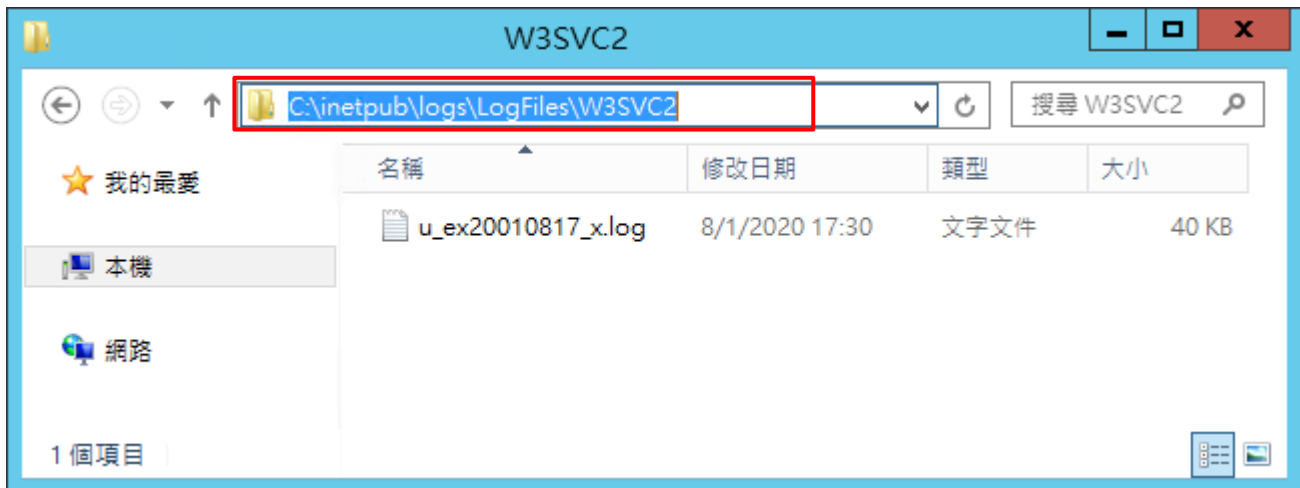
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按 [套用]



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

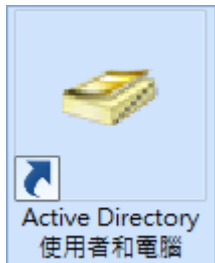


4.3 Event Log

4.3.1 組織單位

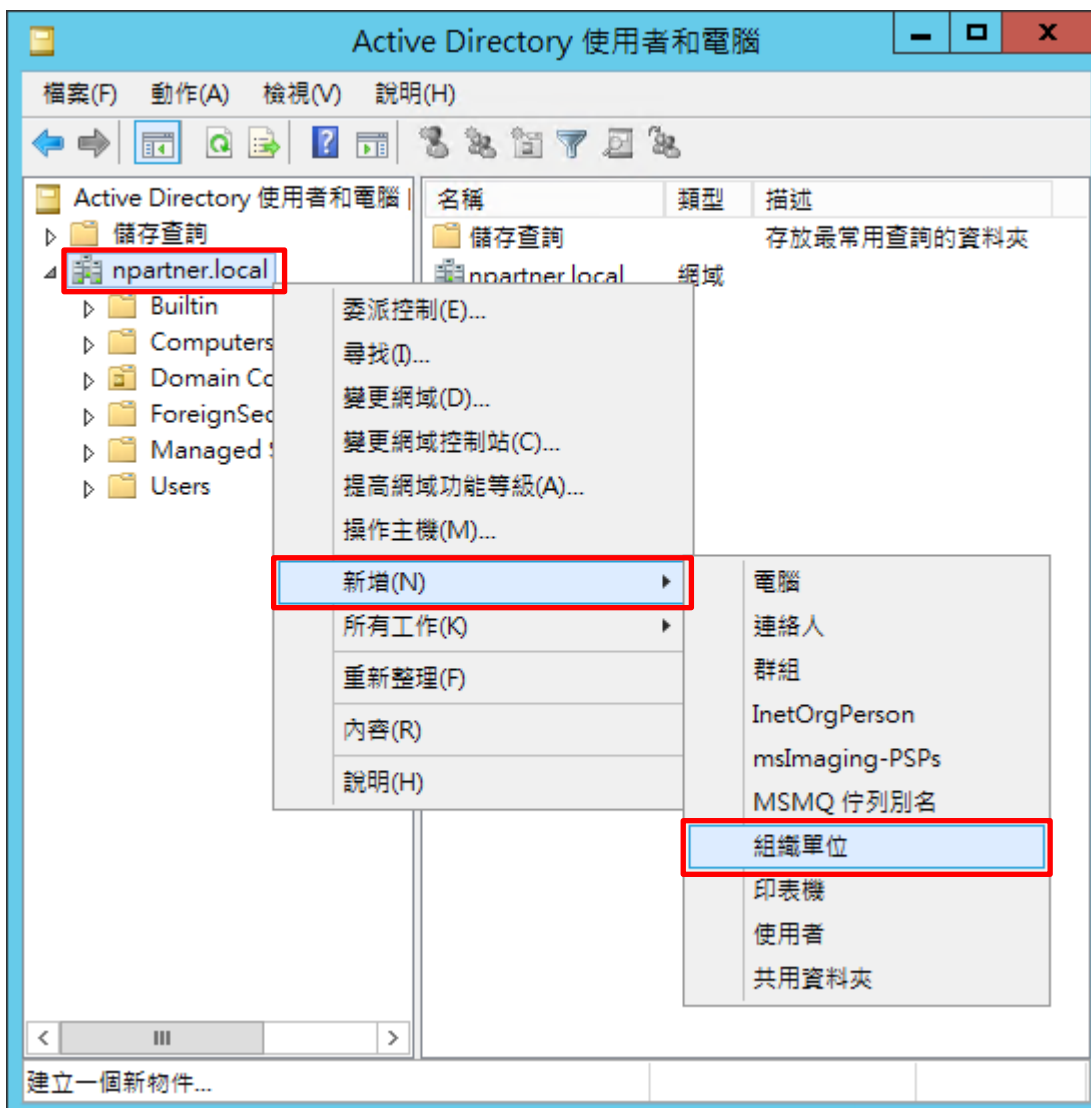
(1) 開啟 AD 使用者和電腦

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]

新增物件 - 組織單位

建立在: npartner.local/

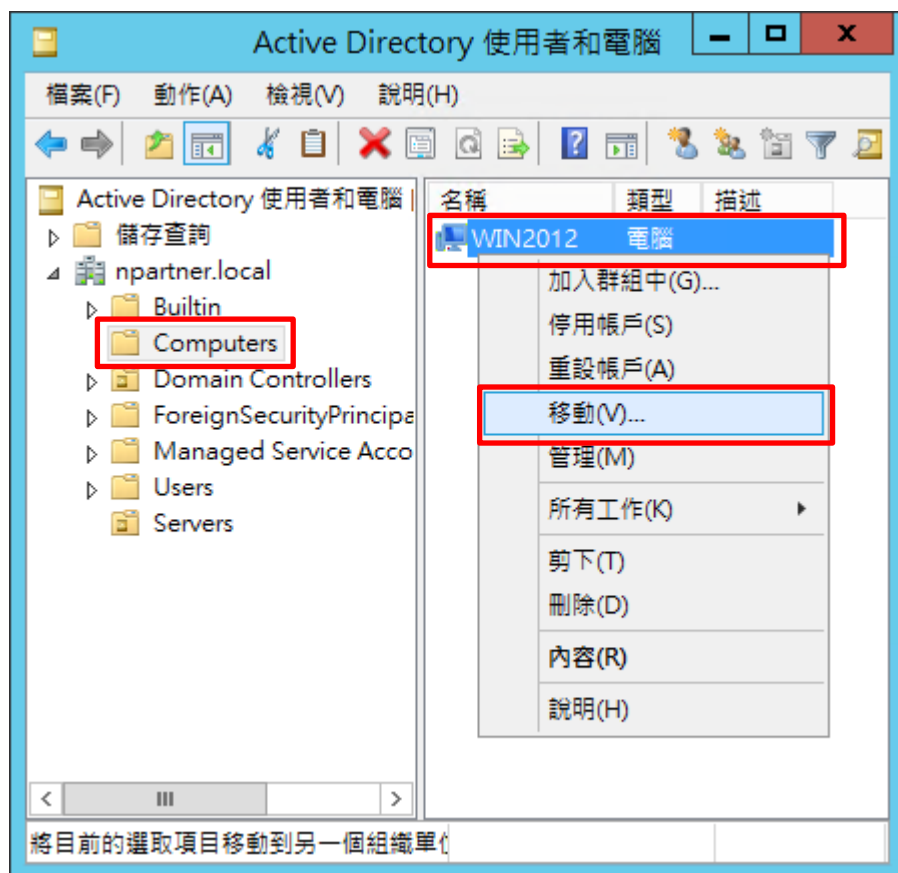
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

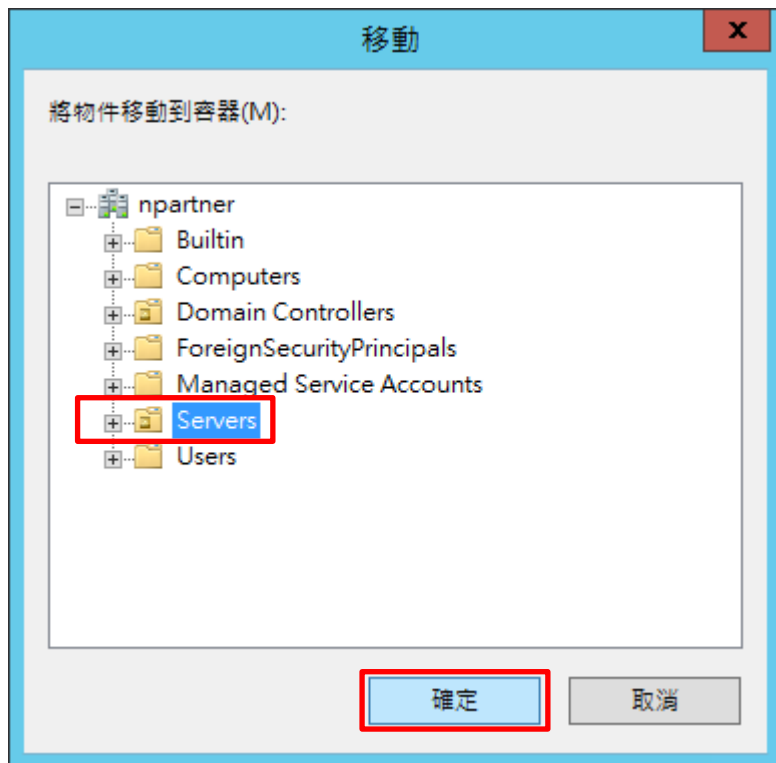
(4) 移動 Exchange 伺服器至新的組織單位

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]



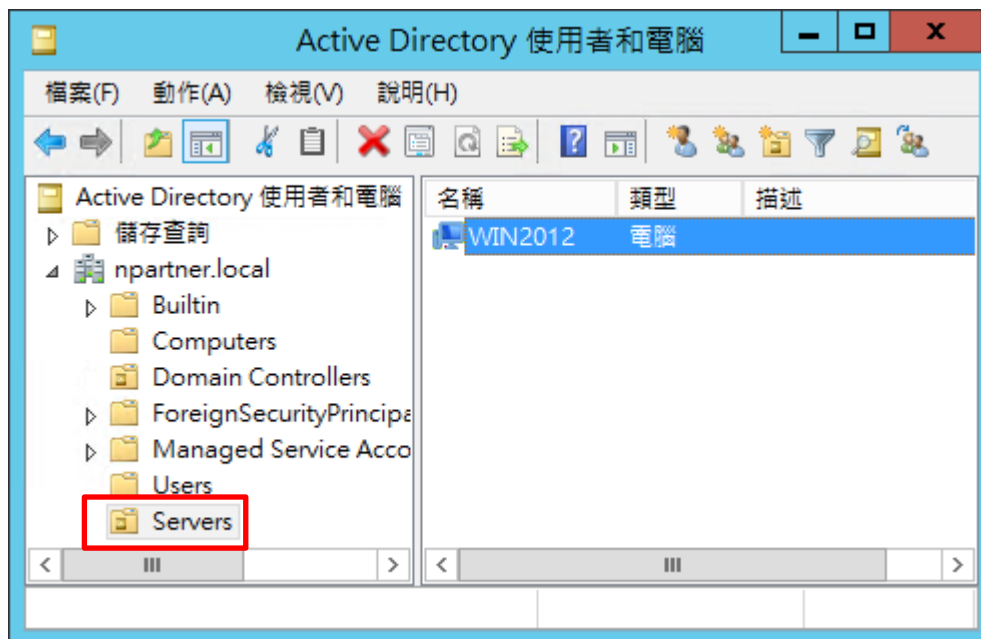
(5) 選擇組織單位

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

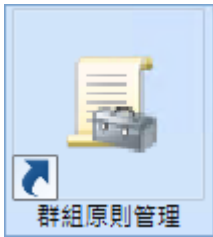
點選 [Servers] 組織單位，確認 Win2012 伺服器已移動。



4.3.2 群組原則

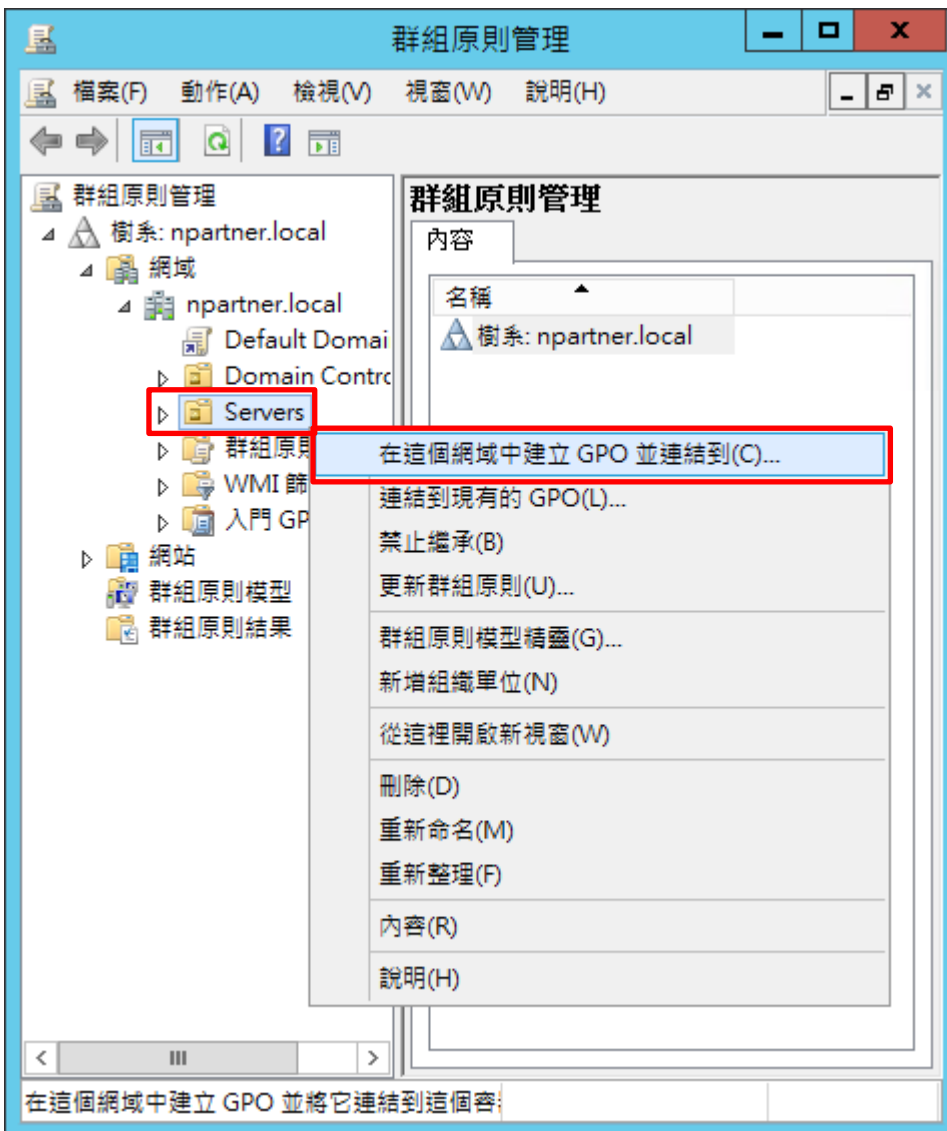
(1) 開啟群組原則管理

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...]



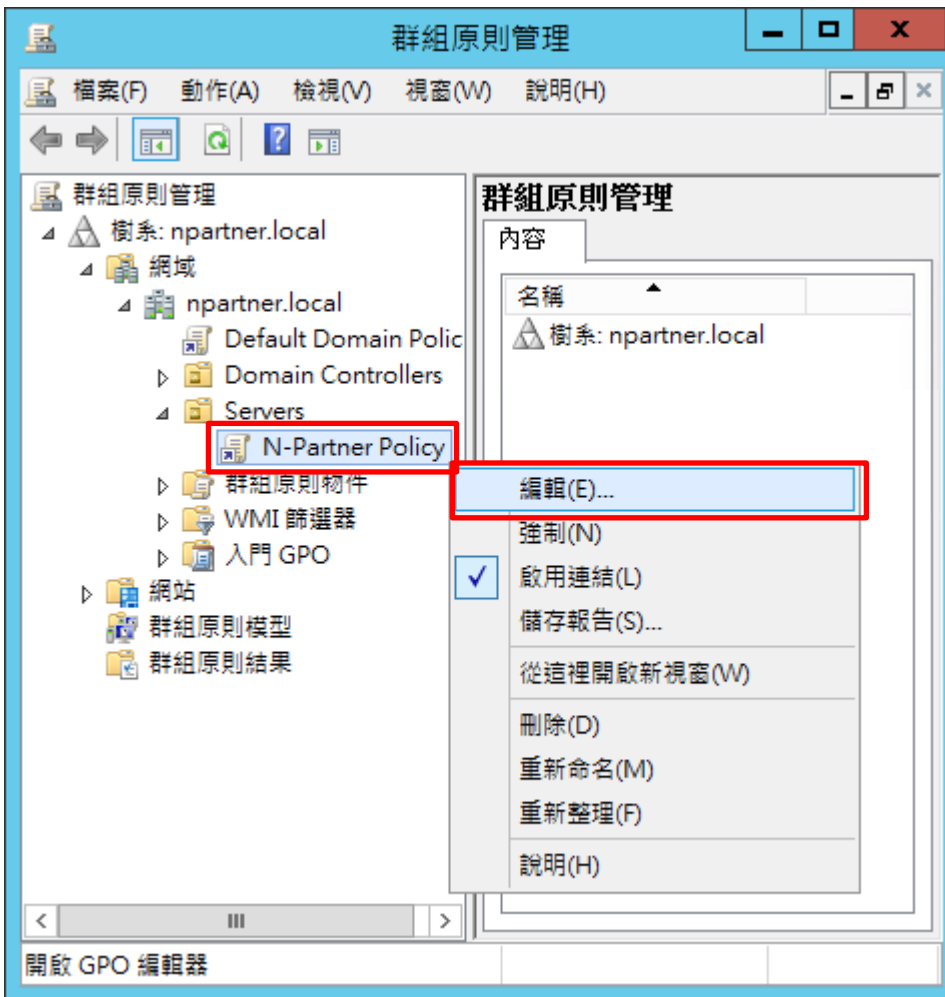
(3) 輸入群組原則物件名稱

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]



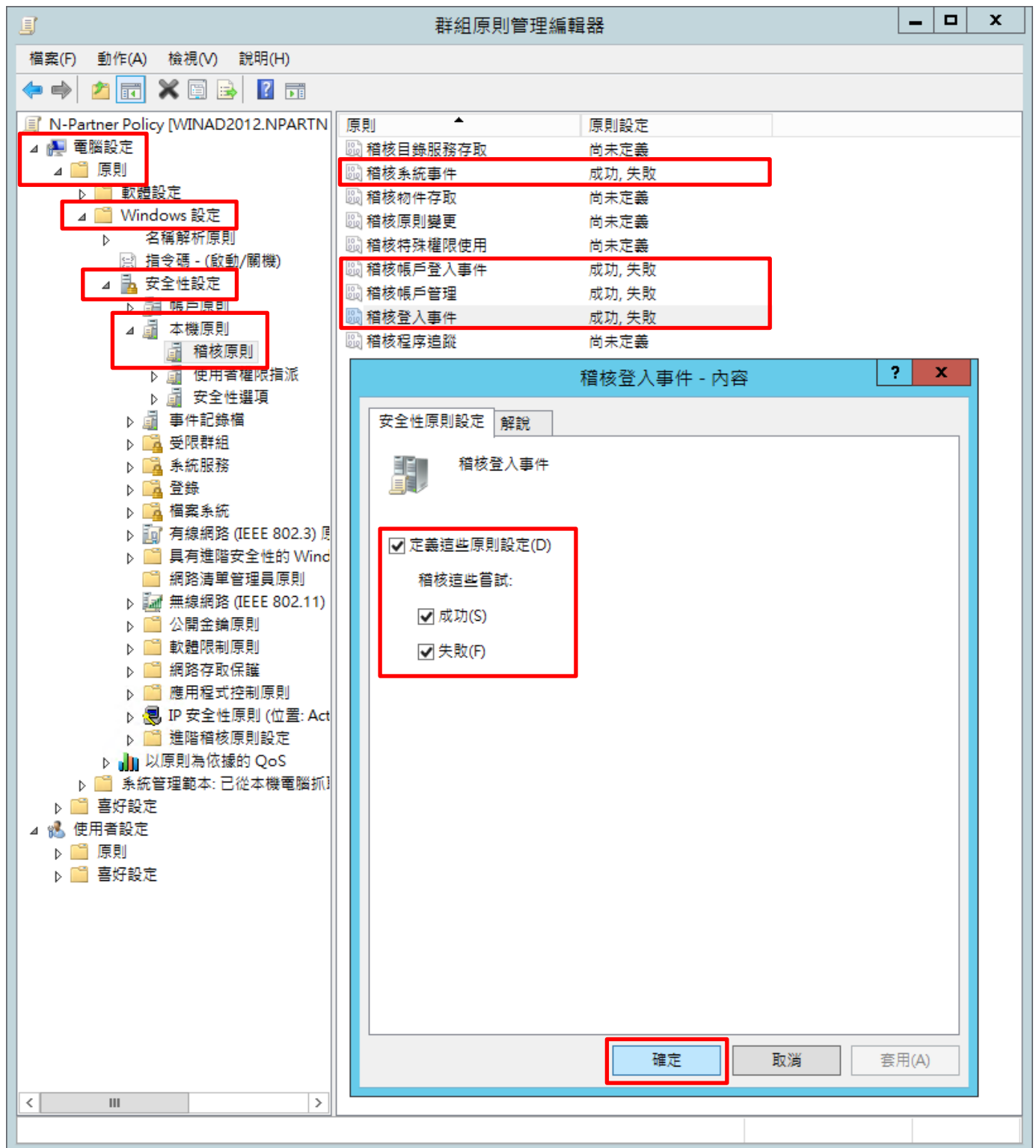
(4) 編輯群組原則物件

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

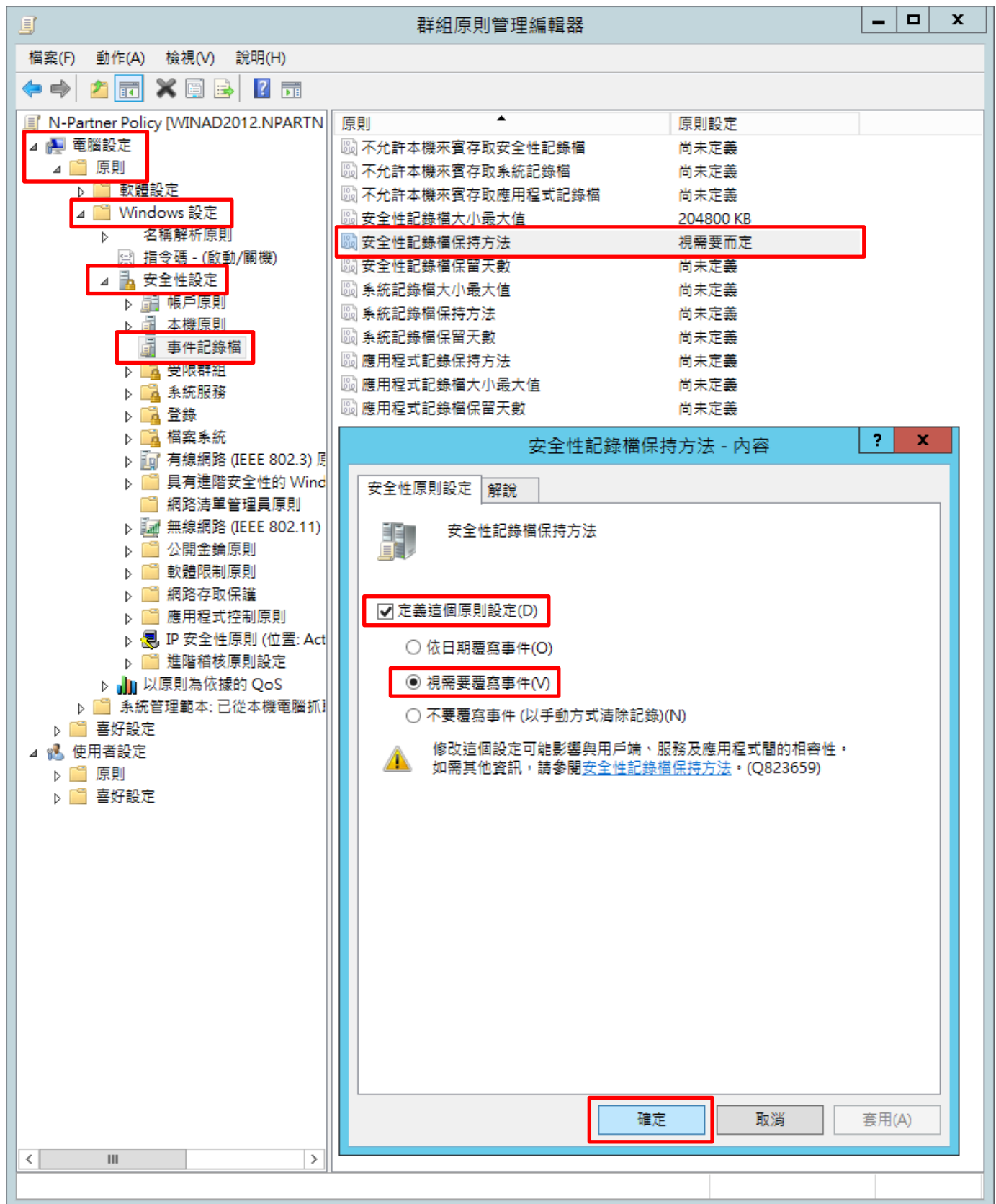
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the 'Group Policy Editor' (群組原則管理編輯器) for 'N-Partner Policy [WINAD2012.NPARTN]'. The left-hand navigation pane is expanded to show the path: 電腦設定 (Computer Configuration) > 原則 (Policy) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies, with '安全性記錄檔大小最大值' (Maximum size of security log) selected and highlighted in red. The value for this policy is set to '204800 KB'. Below the main window, a smaller dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum size of security log - Content) is open. In this dialog, the '定義這個原則設定(D)' (Define this policy setting) checkbox is checked and highlighted in red. The value '204800 KB' is entered in the text box and also highlighted in red. A warning icon and text are visible below the text box, and the '確定' (OK) button is highlighted in red at the bottom right of the dialog.

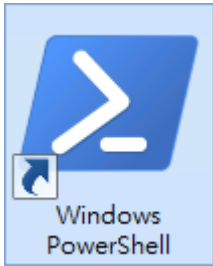
原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(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]

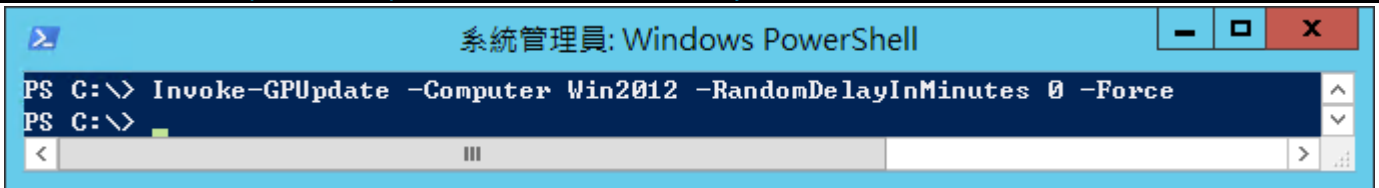


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Exchange 伺服器群組原則

```
PS C:\> Invoke-GPUUpdate -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

群組原則結果

NPARTNER\WIN2012
資料收集: 17/11/2021 16:24:11

顯示全部

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

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

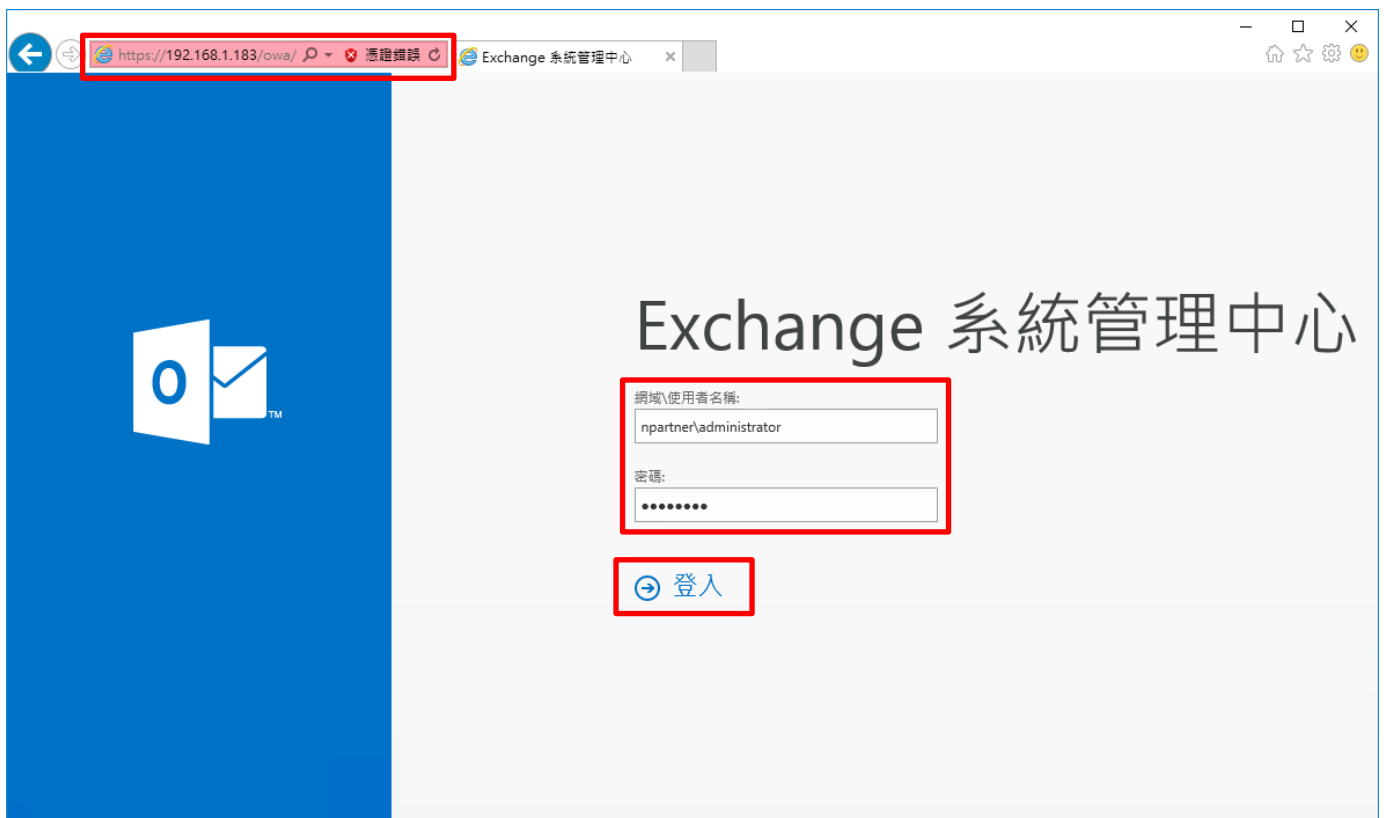
```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

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)



Exchange 系統管理中心

收件者 伺服器 資料庫 資料庫可用性群組 虛擬目錄 憑證

權限

合規性管理  

組織

保護

郵件流程

行動

公用資料夾

整合通訊

伺服器

混合

名稱	伺服器角色	版本	
WIN2016	信箱	Version 15.1 (Build ...)	WIN2016 信箱 Version 15.1 (Build 1591.10) 標準試用版 試用 輸入產品金鑰

已選取 1 個，共 1 個

<https://192.168.1.183/ecp/Servers/Servers.slabs?showhelp=false#>

(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]

Exchange 伺服器 - Internet Explorer

https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=4&ReturnObjectType=1&id=4be29b9c-8d14-4806- 憑證錯誤

WIN2016

一般
資料庫和資料庫可用性
群組
POP3
IMAP4
整合通訊
DNS 查閱
傳輸限制
▶ 傳輸記錄檔
Outlook Anywhere

郵件追蹤記錄檔
 啟用郵件追蹤記錄檔
郵件追蹤記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking

連線記錄檔
 啟用連線記錄檔
連線記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Connection

通訊協定記錄檔
傳送通訊協定記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\ProtocolLog\Send

接收通訊協定記錄檔路徑:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\ProtocolLog\Receive

儲存 取消

https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=4&ReturnObjectType=1&id=4be29b9c-8d14-4806- 100%

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*
```

The screenshot shows a terminal window titled '機器: Win2016.npartner.local'. The terminal displays the following text:

```
歡迎使用 Exchange 管理命令介面!
完整的 Cmdlet 清單: Get-Command
只有 Exchange Cmdlet: Get-ExCommand
符合特定字串的 Cmdlet: 說明 *<string>*
取得一般說明: 說明
取得 Cmdlet 的說明: Help <cmdlet name> 或 <cmdlet name> -?
Exchange 團隊部落格: Get-ExBlog
顯示命令的完整輸出: <command> | Format-List

顯示快速參考指南: QuickRef
每日提示 #4:
您知道 Identity 參數是「位置參數」嗎? 那表示您可以使用:
Get-Mailbox "user" 來代表 Get-Mailbox -Identity "user"
這是恰到好處的實用捷徑!
詳細資訊: 連線至 Win2016.npartner.local。
詳細資訊: 已連線至 Win2016.npartner.local。
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2016>Get-TransportService Win2016 | Select-Object *Track*
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\V15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True

[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2016>
```

The output of the command is highlighted with a red dashed border.

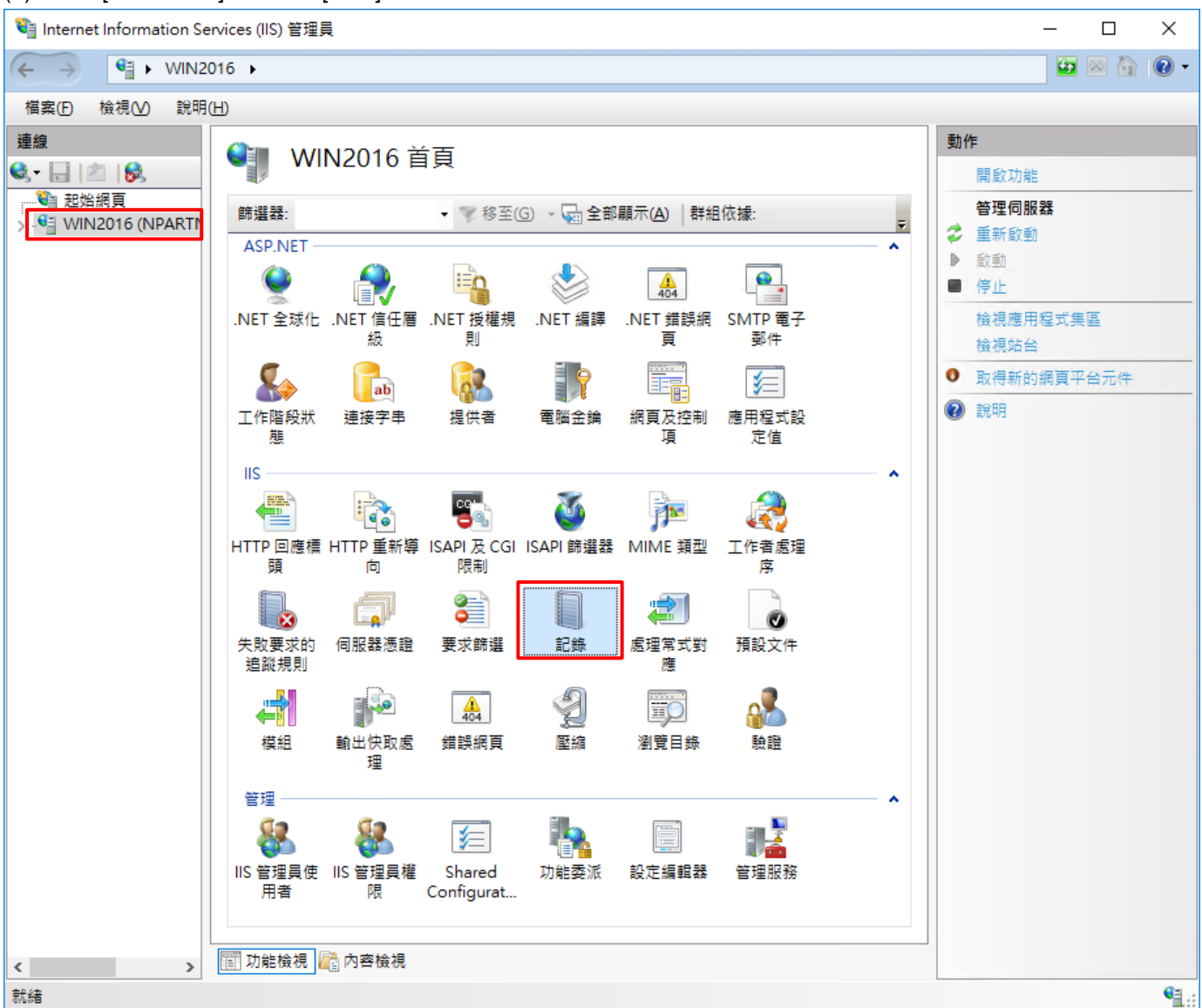
紅色文字部位請輸入 Exchange 伺服器名稱

5.2 IIS Log

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

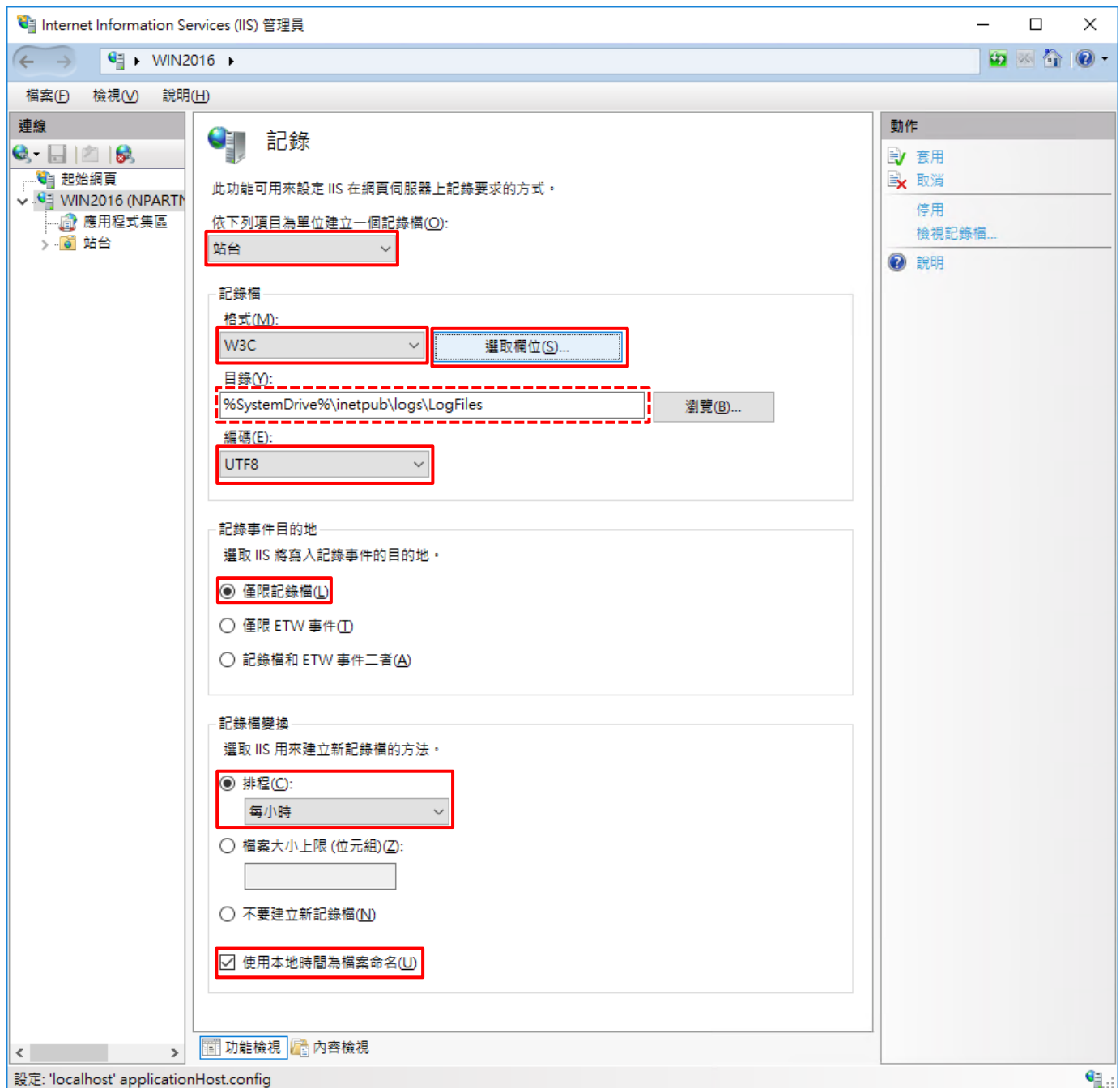


(2) 選擇 [IIS 伺服器] -> 點選 [記錄]



(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]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按下 [確定]

W3C 記錄欄位

標準欄位(S):

- 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 (Stem) (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)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

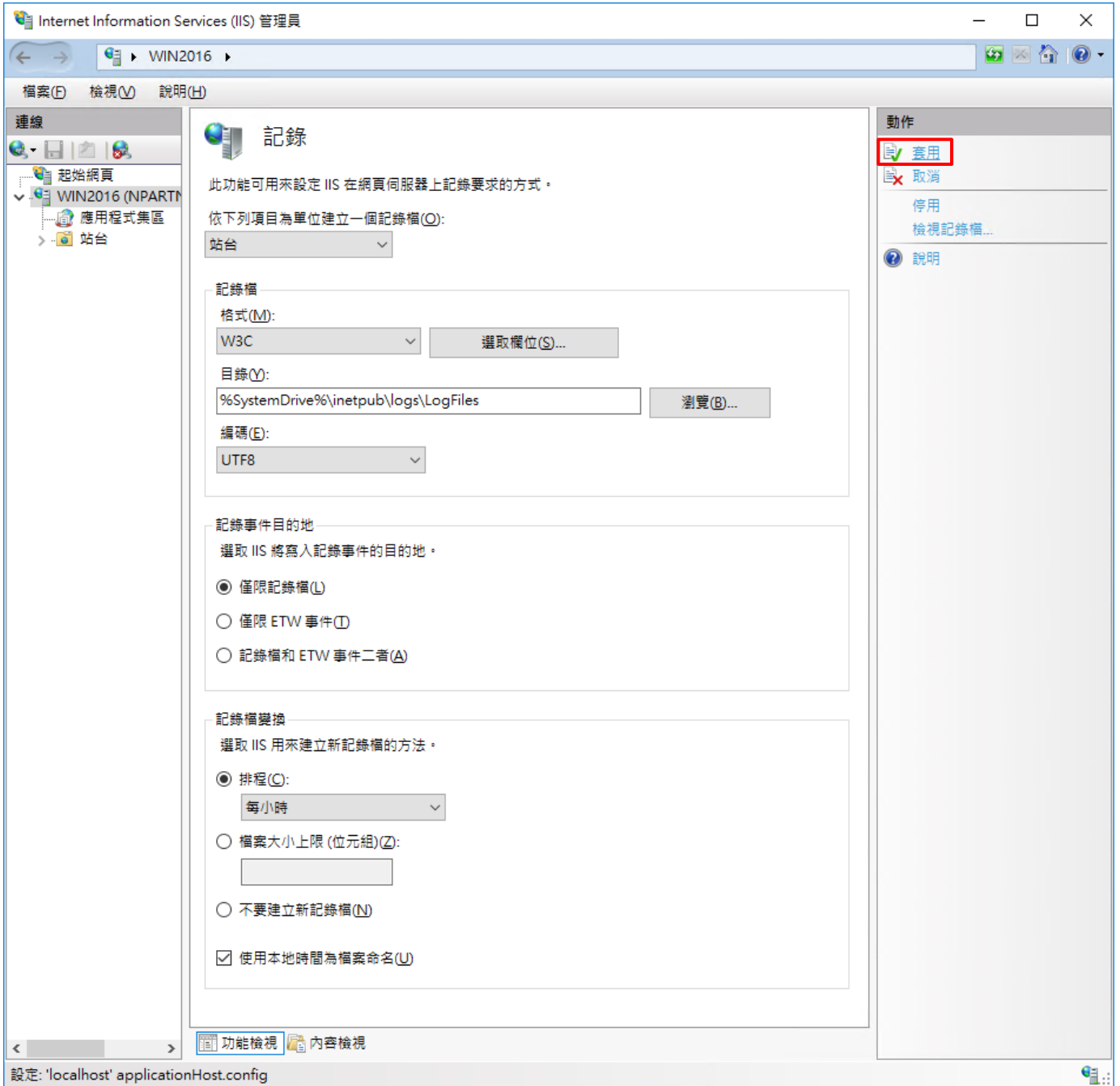
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

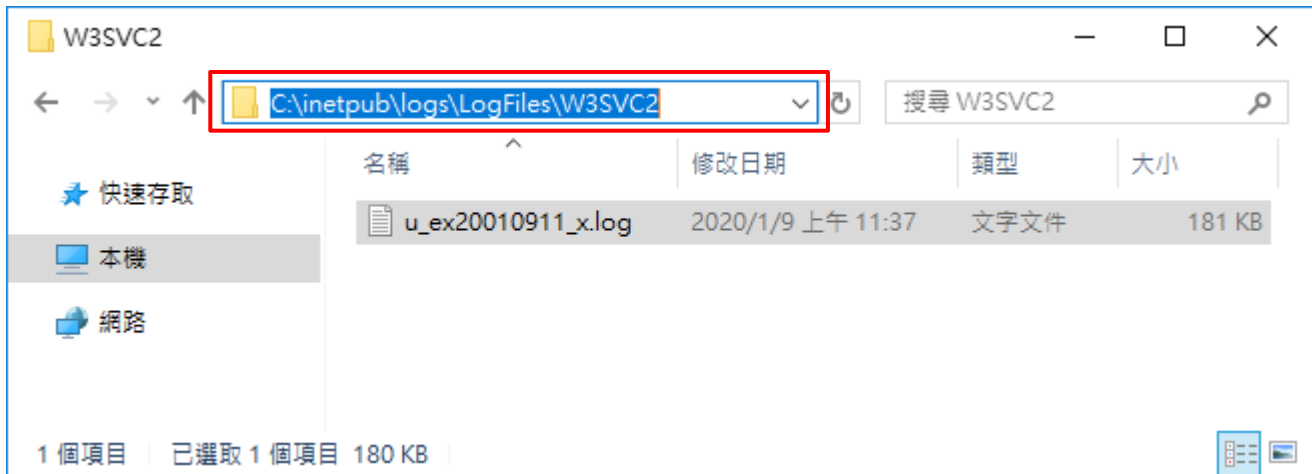
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [套用]



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

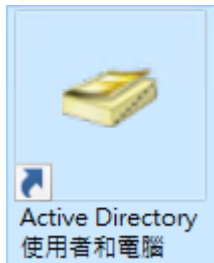


5.3 Event Log

5.3.1 組織單位

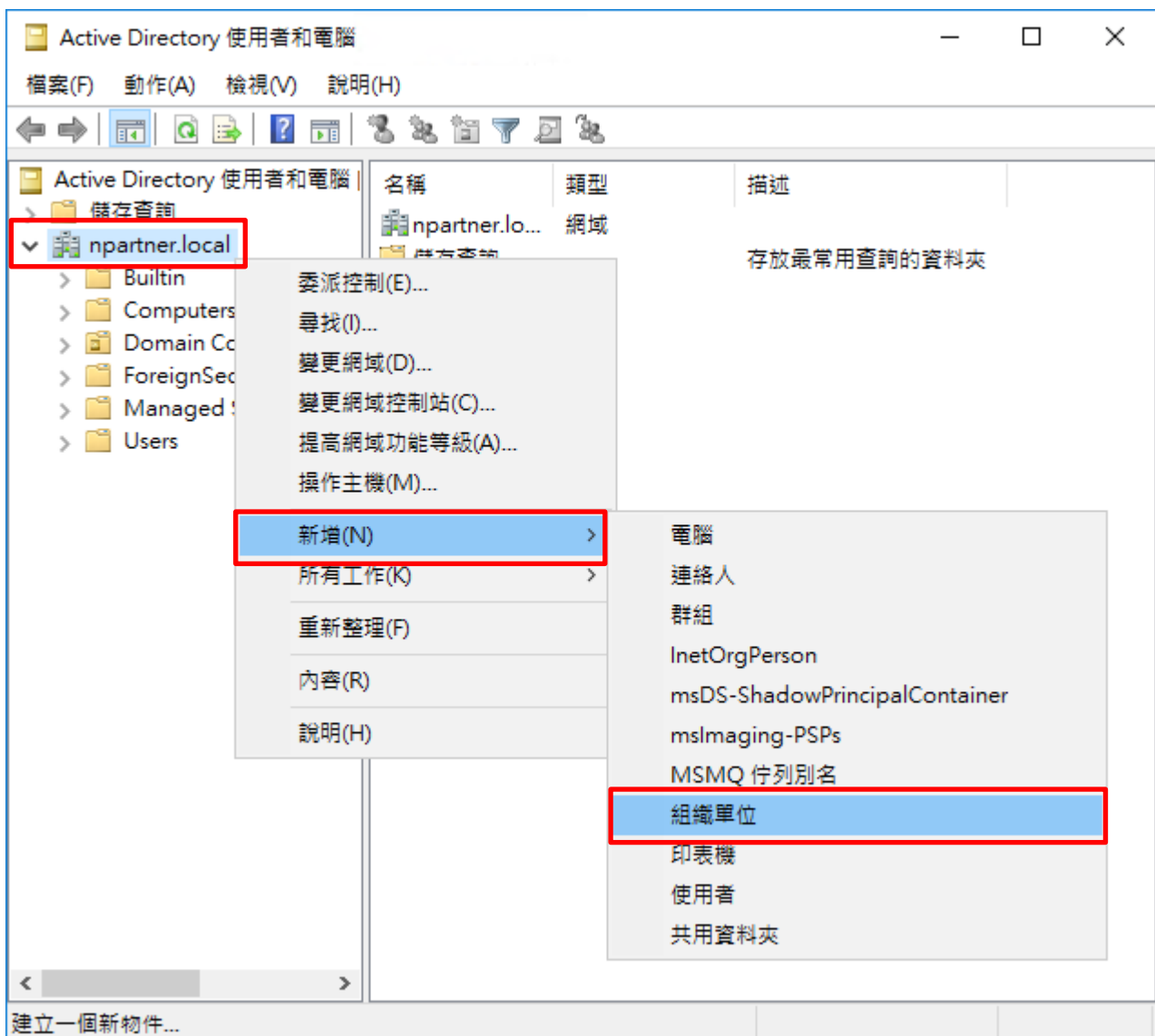
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



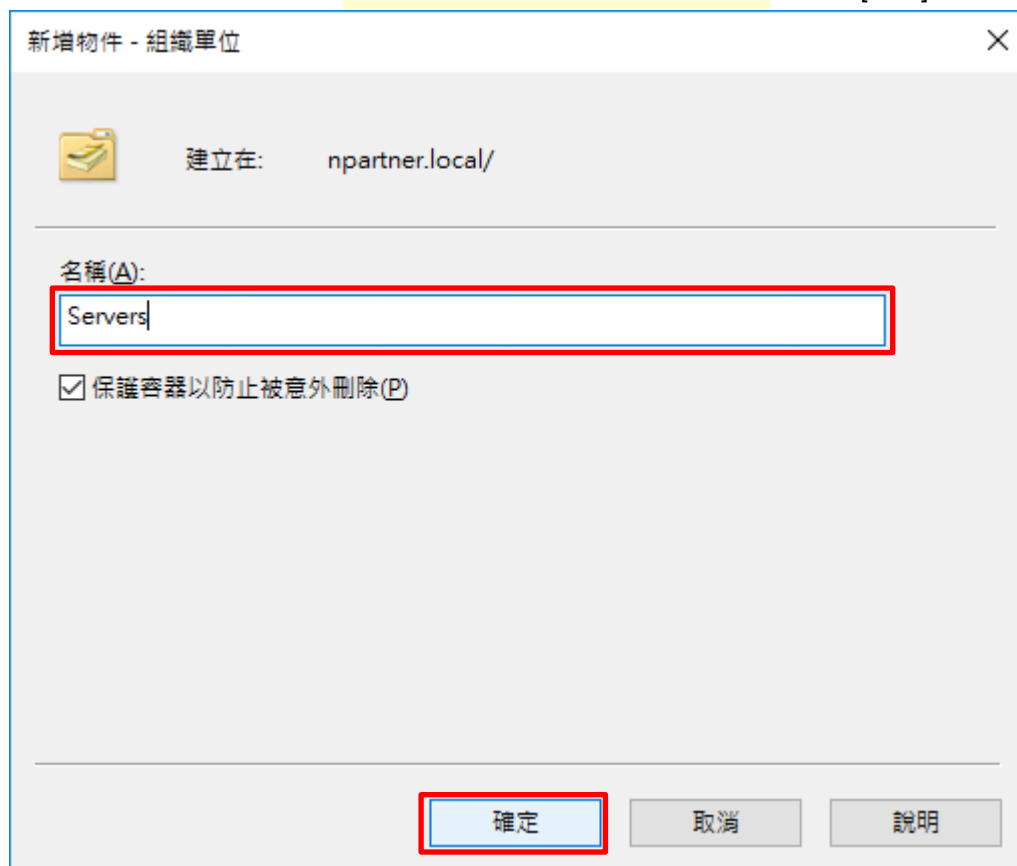
(2) 新增組織單位

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]



新增物件 - 組織單位

建立在: npartner.local/

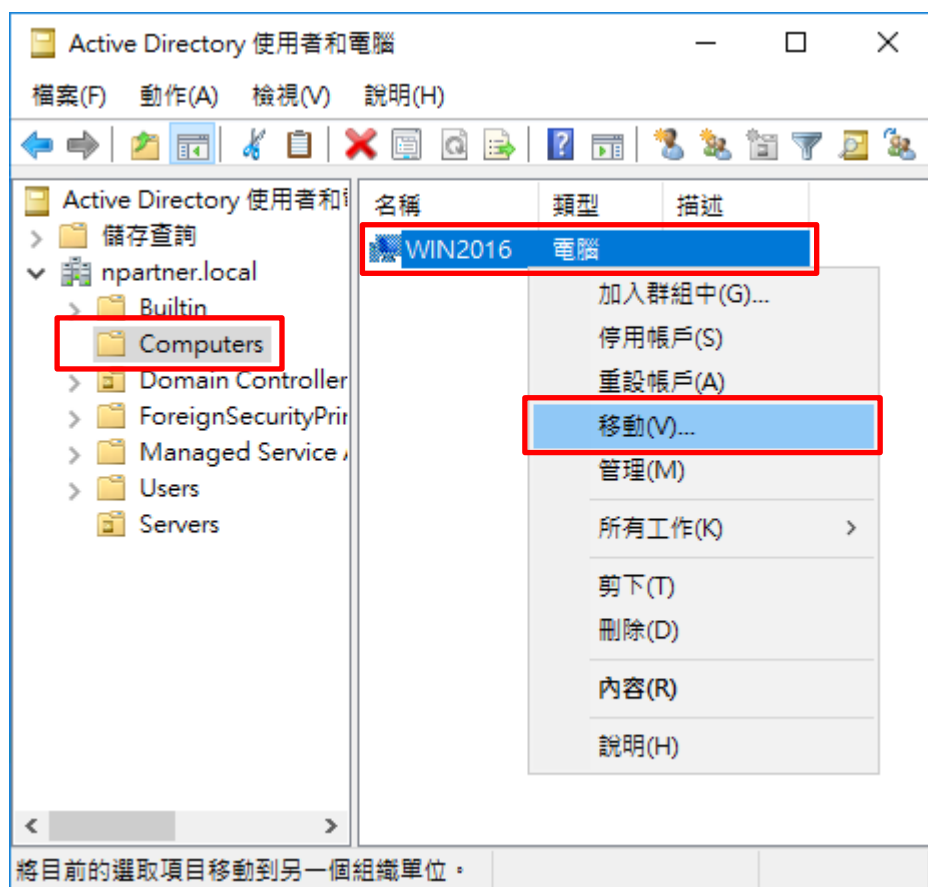
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

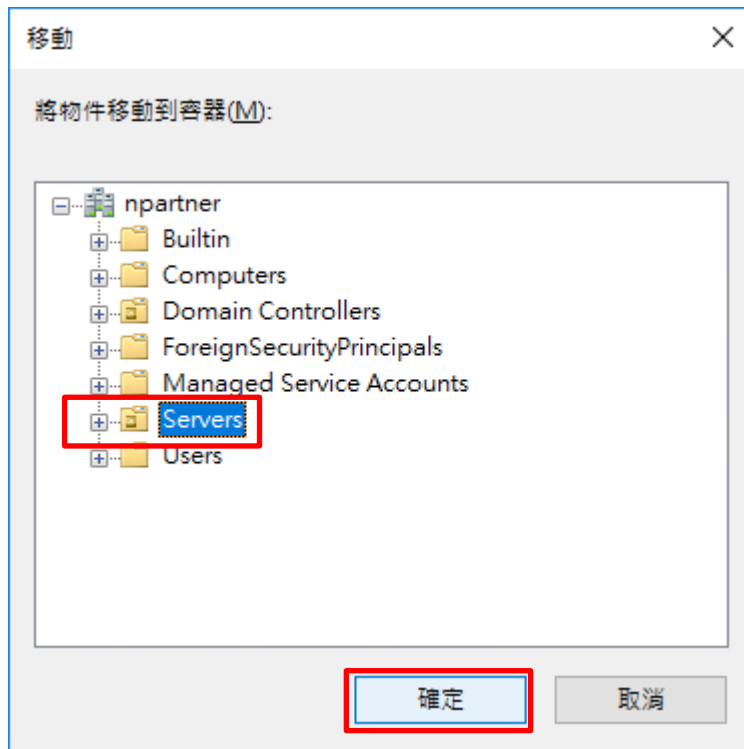
(4) 移動 Exchange 伺服器至新的組織單位

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]



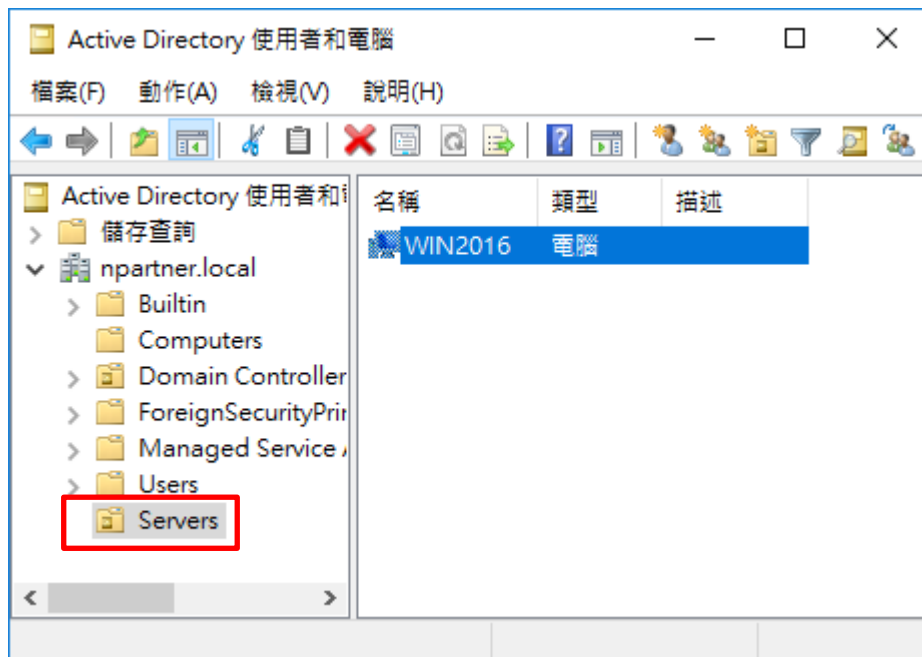
(5) 選擇組織單位

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

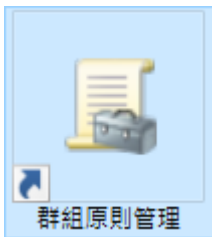
點選 [Servers] 組織單位，確認 Win2016 伺服器已移動。



5.3.2 群組原則

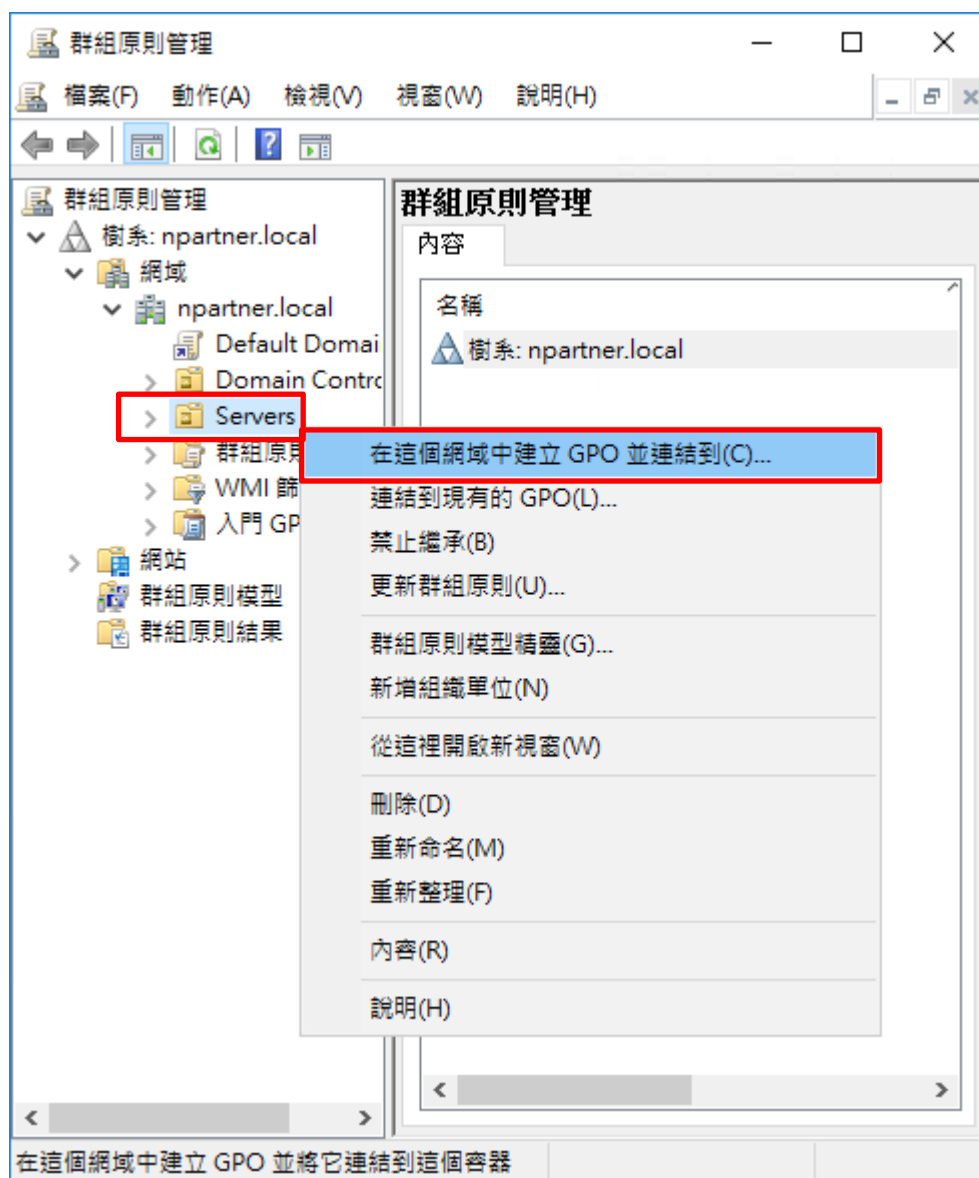
(1) 開啟群組原則管理

開啟 [群組原則管理]



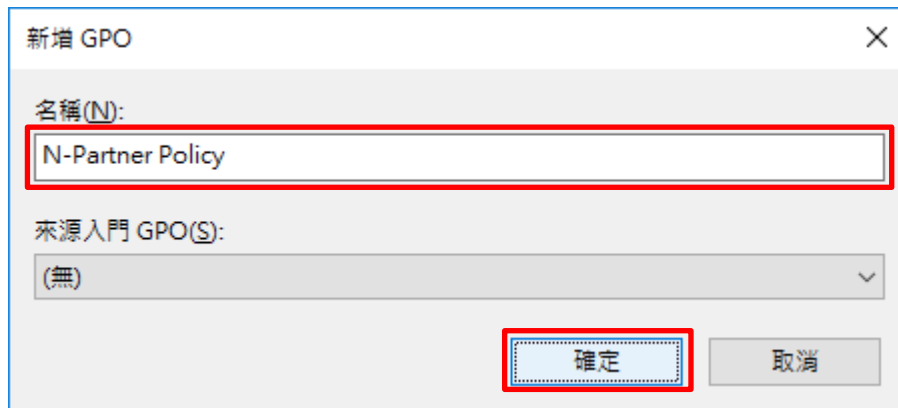
(2) 在 Servers 組織單位，新增群組原則物件

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...]



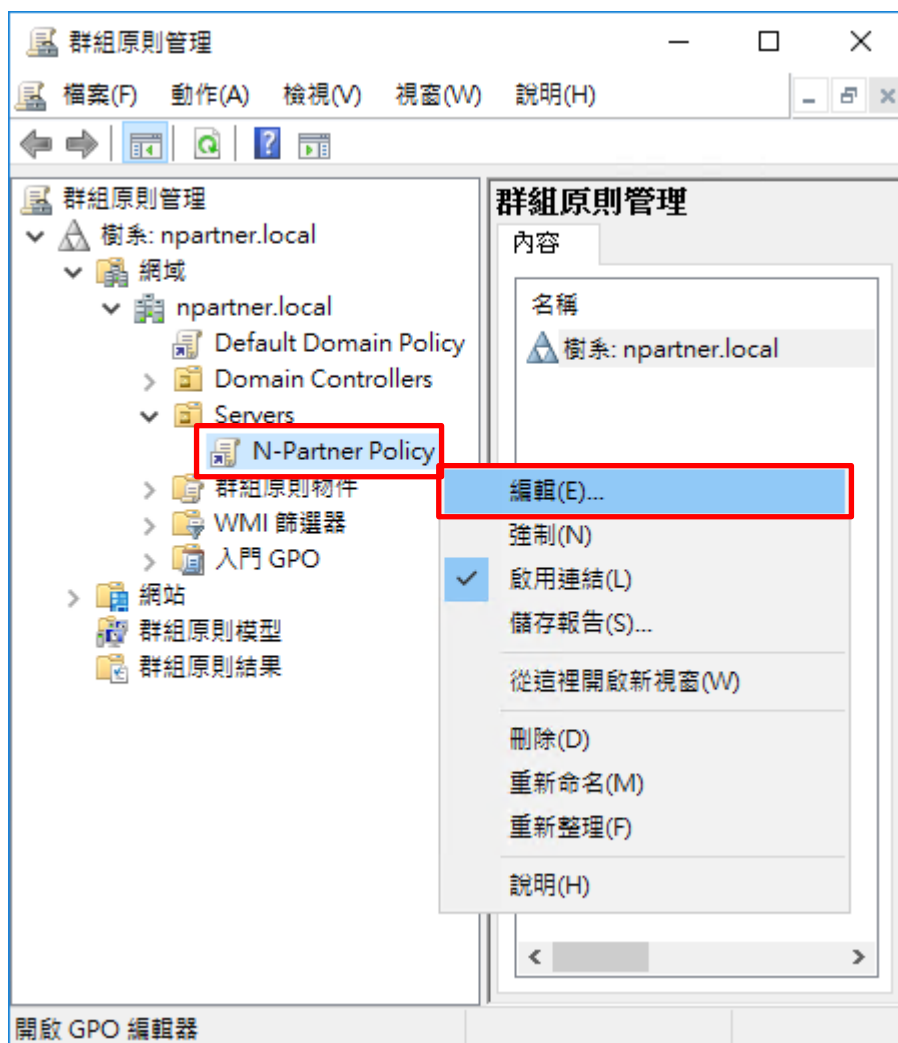
(3) 輸入群組原則物件名稱

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]



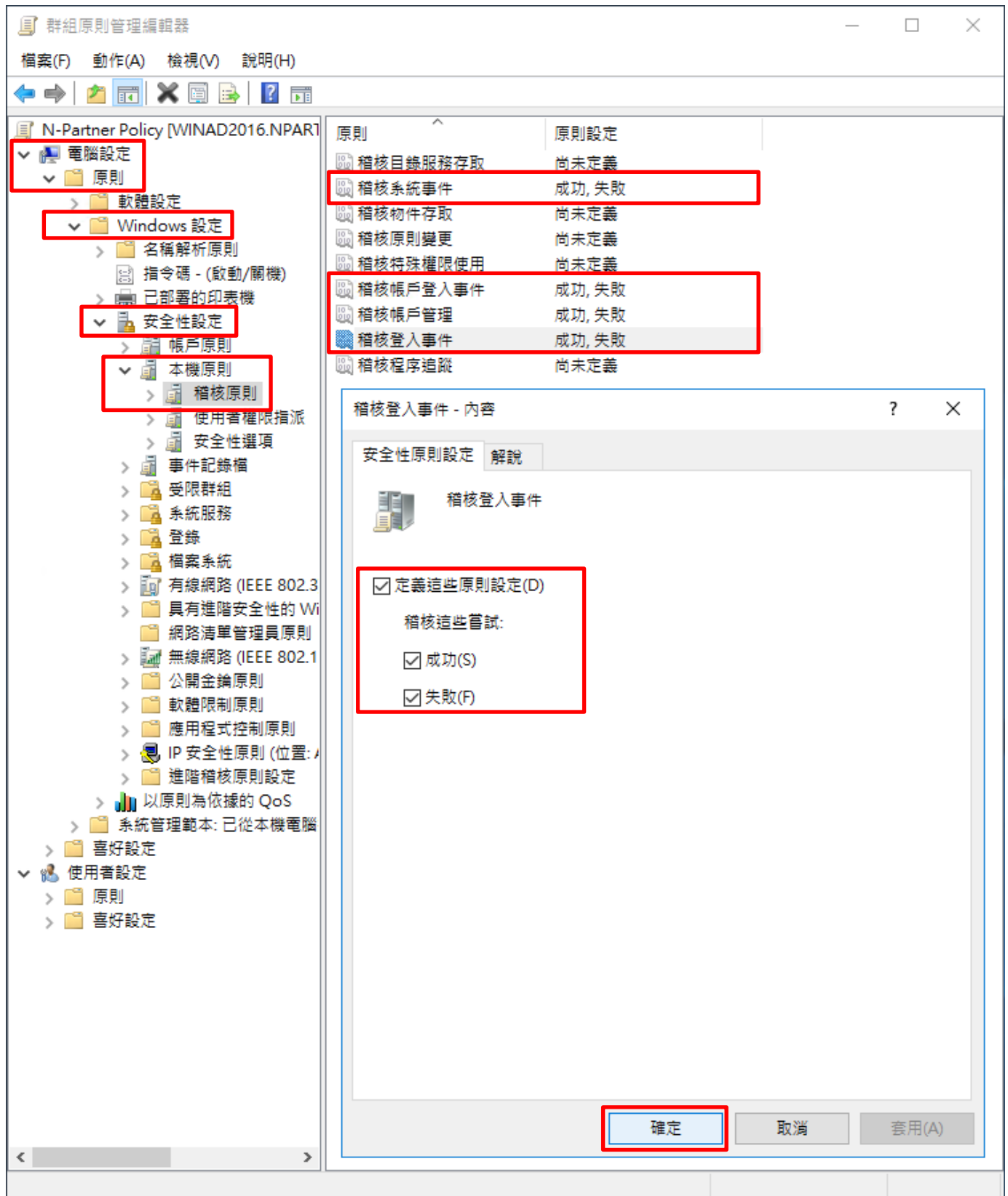
(4) 編輯群組原則物件

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]

The screenshot shows the 'N-Partner Policy Management Editor' window. The left sidebar shows a tree view with 'Computer Settings' expanded to 'Principles' > 'Windows Settings' > 'Security Settings' > 'Event Log'. The main pane shows a list of policies, with 'Security Log Size Maximum' selected and its value set to '204800 KB'. A dialog box titled 'Security Log Size Maximum - Content' is open, showing the 'Define this policy setting' checkbox checked and the value '204800 KB' entered. A warning message at the bottom of the dialog states: 'Changing this setting may affect compatibility with user applications, services, and applications. For more information, see Security Log Size Maximum (Q823659)'. The 'OK' button is highlighted.

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(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]

群組原則管理編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

N-Partner Policy [WINAD2016.NPART]

電腦設定

原則

軟體設定

Windows 設定

名稱解析原則

指令碼 - (啟動/關機)

已部署的印表機

安全性設定

帳戶原則

本機原則

事件記錄檔

受限群組

系統服務

登錄

檔案系統

有線網路 (IEEE 802.3)

具有進階安全性的 Wi

網路清單管理員原則

無線網路 (IEEE 802.1

公開金鑰原則

軟體限制原則

應用程式控制原則

IP 安全性原則 (位置: /

進階稽核原則設定

以原則為依據的 QoS

系統管理範本: 已從本機電腦

喜好設定

使用者設定

原則

喜好設定

原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	視需要而定
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄檔保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

安全性記錄檔保持方法 - 內容

安全性原則設定 解說

安全性記錄檔保持方法

定義這個原則設定(D)

依日期覆寫事件(O)

視需要覆寫事件(V)

不要覆寫事件 (以手動方式清除記錄)(N)

修改這個設定可能影響與用戶端、服務及應用程式間的相容性。
如需其他資訊，請參閱[安全性記錄檔保持方法](#)。(Q823659)

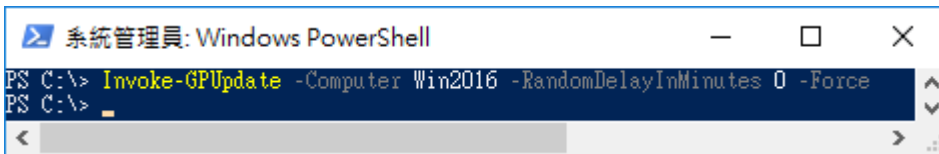
確定 取消 套用(A)

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



(9) 更新 Exchange Server 群組原則

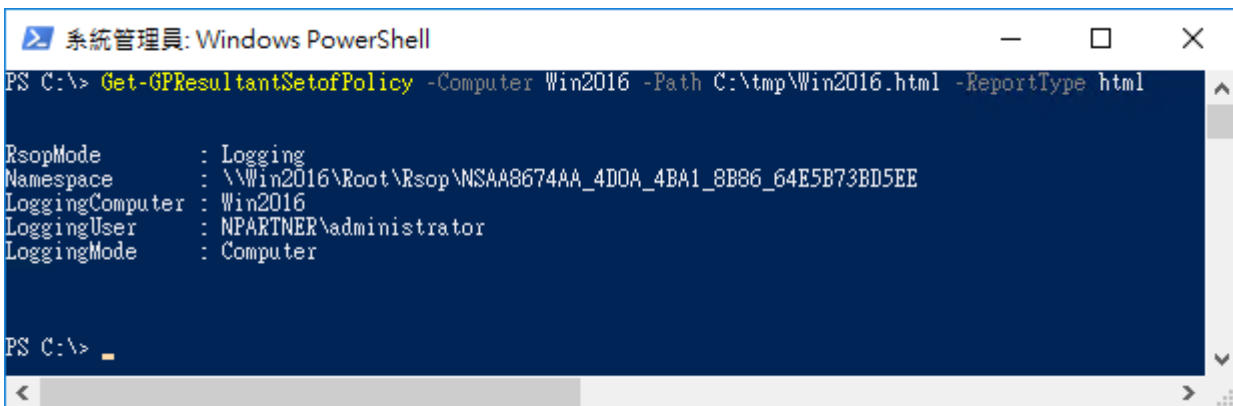
```
PS C:\> Invoke-GPUdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



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

群組原則結果

NPARTNER\WIN2016
資料收集: 2021/11/17 下午 05:50:00 全部顯示

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

系統管理範本 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

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

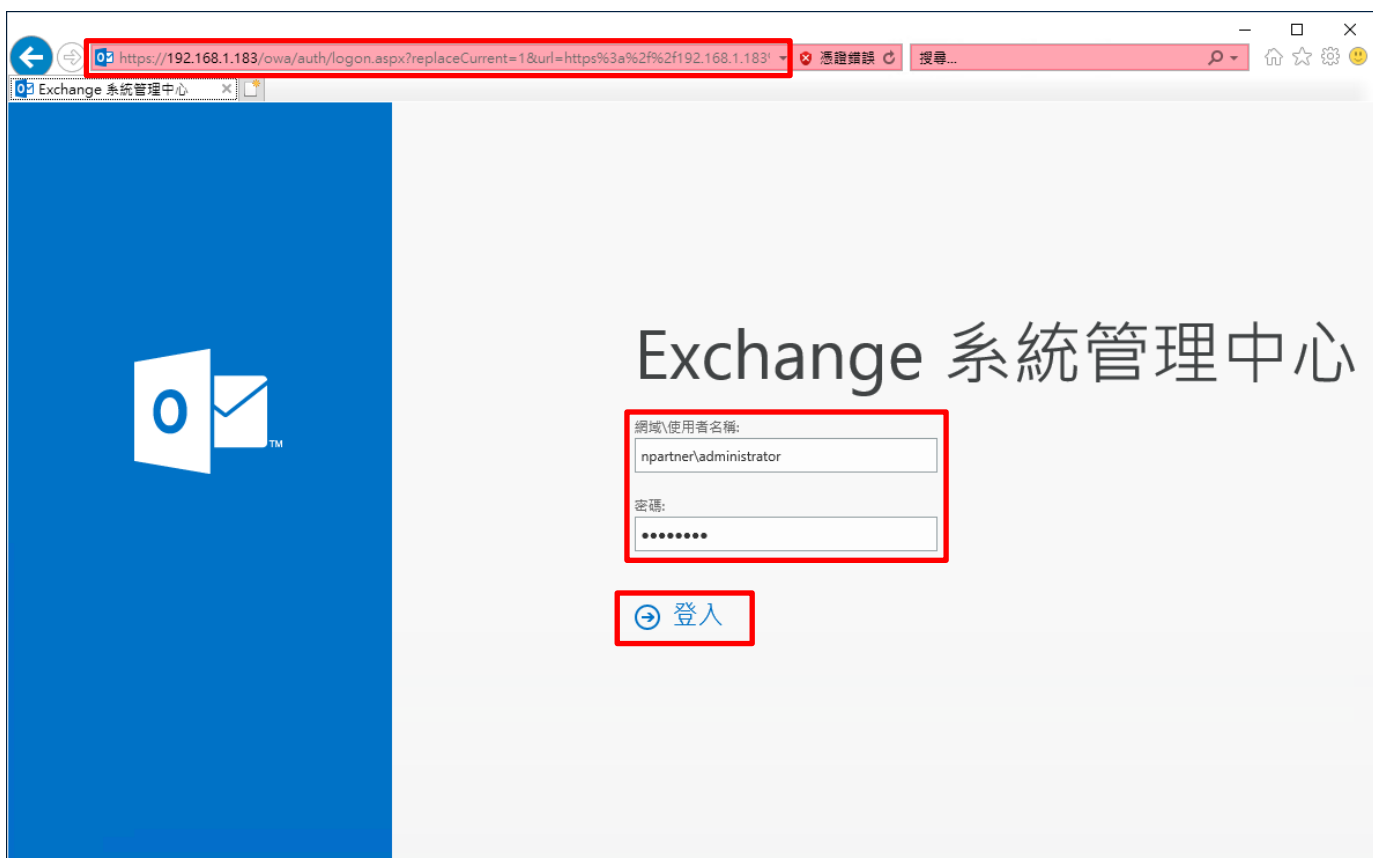
```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```


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)

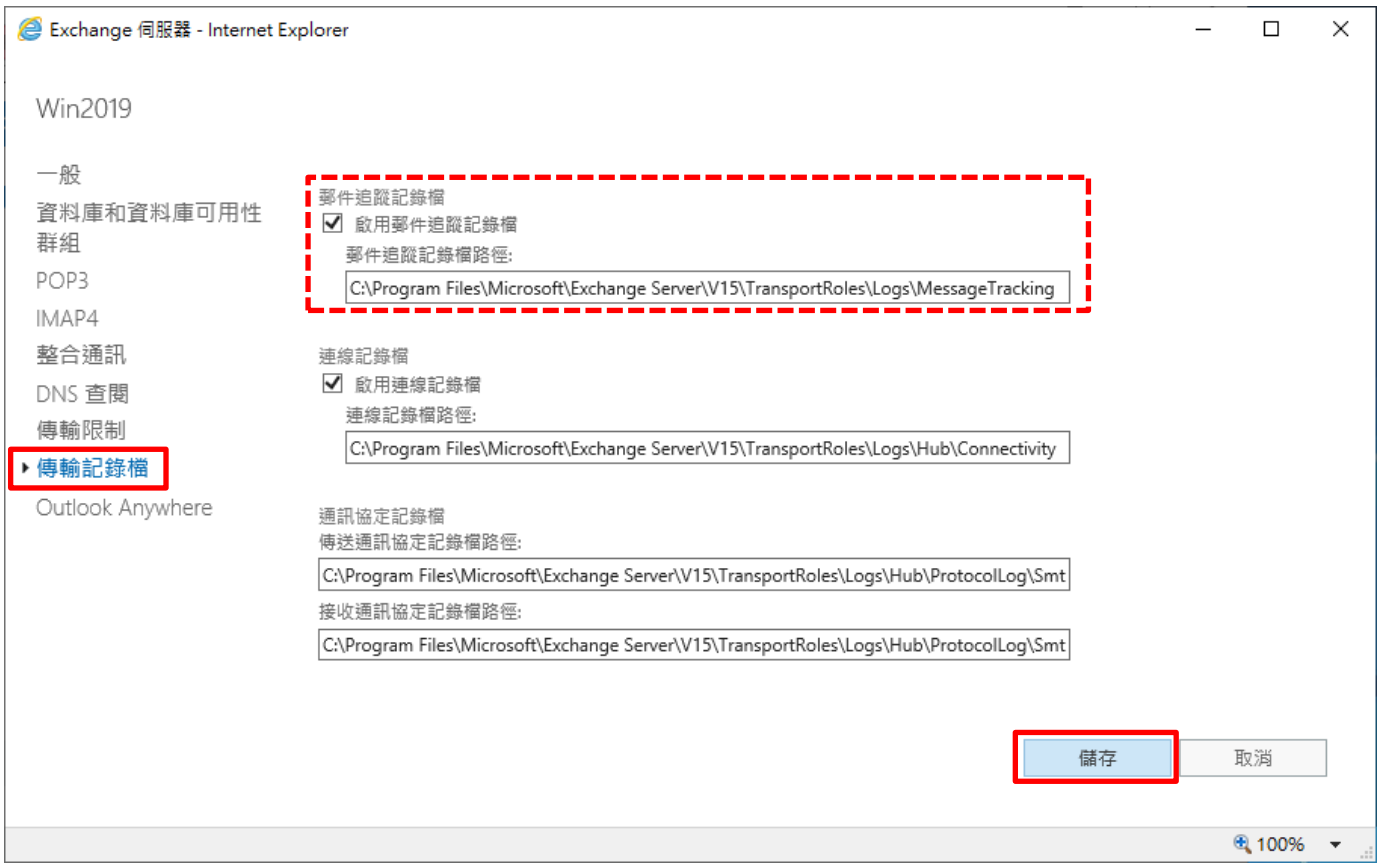


The screenshot shows the Exchange System Management Center (EMC) interface. The left sidebar contains navigation options: 收件者, 權限, 合規性管理, 組織, 保護, 郵件流程, 行動, 公用資料夾, **伺服器** (highlighted), and 混合. The main content area is titled "Exchange 系統管理中心" and includes a breadcrumb trail: **伺服器** > 資料庫 > 資料庫可用性群組 > 虛擬目錄 > 憑證. Below the breadcrumb is an edit icon. A table lists server configurations:

名稱	伺服器角色	版本	
Win2019	信箱	Version 15.2 (Build 330.5)	Win2019 信箱 Version 15.2 (Build 330.5) 標準試用版 試用 輸入產品金鑰

At the bottom of the table, it indicates "已選取 1 個, 共 1 個".

(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

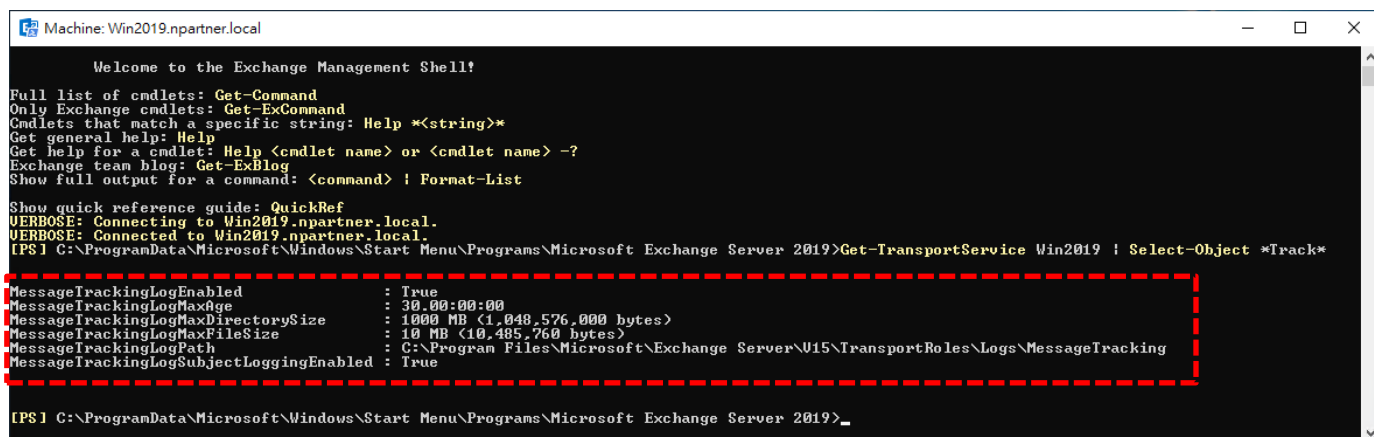
(1) 開啟 [Exchange Management Shell]



(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*
```

A screenshot of the Exchange Management Shell terminal window. The window title is 'Machine: Win2019.npartner.local'. The terminal shows the following text:

```
Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *(string)*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List
Show quick reference guide: QuickRef
VERBOSE: Connecting to Win2019.npartner.local.
VERBOSE: Connected to Win2019.npartner.local.
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2019>Get-TransportService Win2019 | 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\V15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2019>_
```

The output of the command is highlighted with a red dashed border.

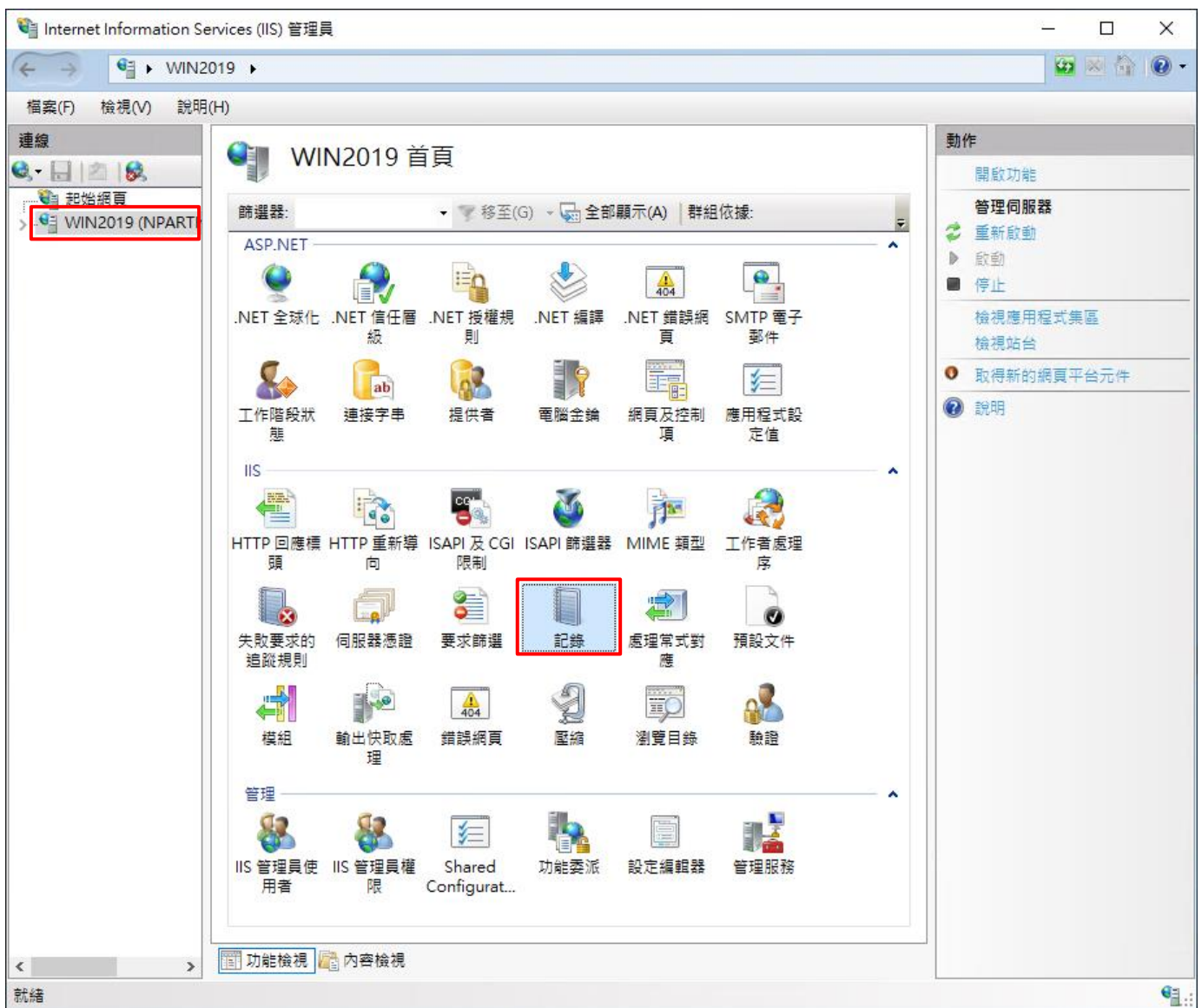
紅色文字部位請輸入 Exchange 伺服器名稱

6.2 IIS Log

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

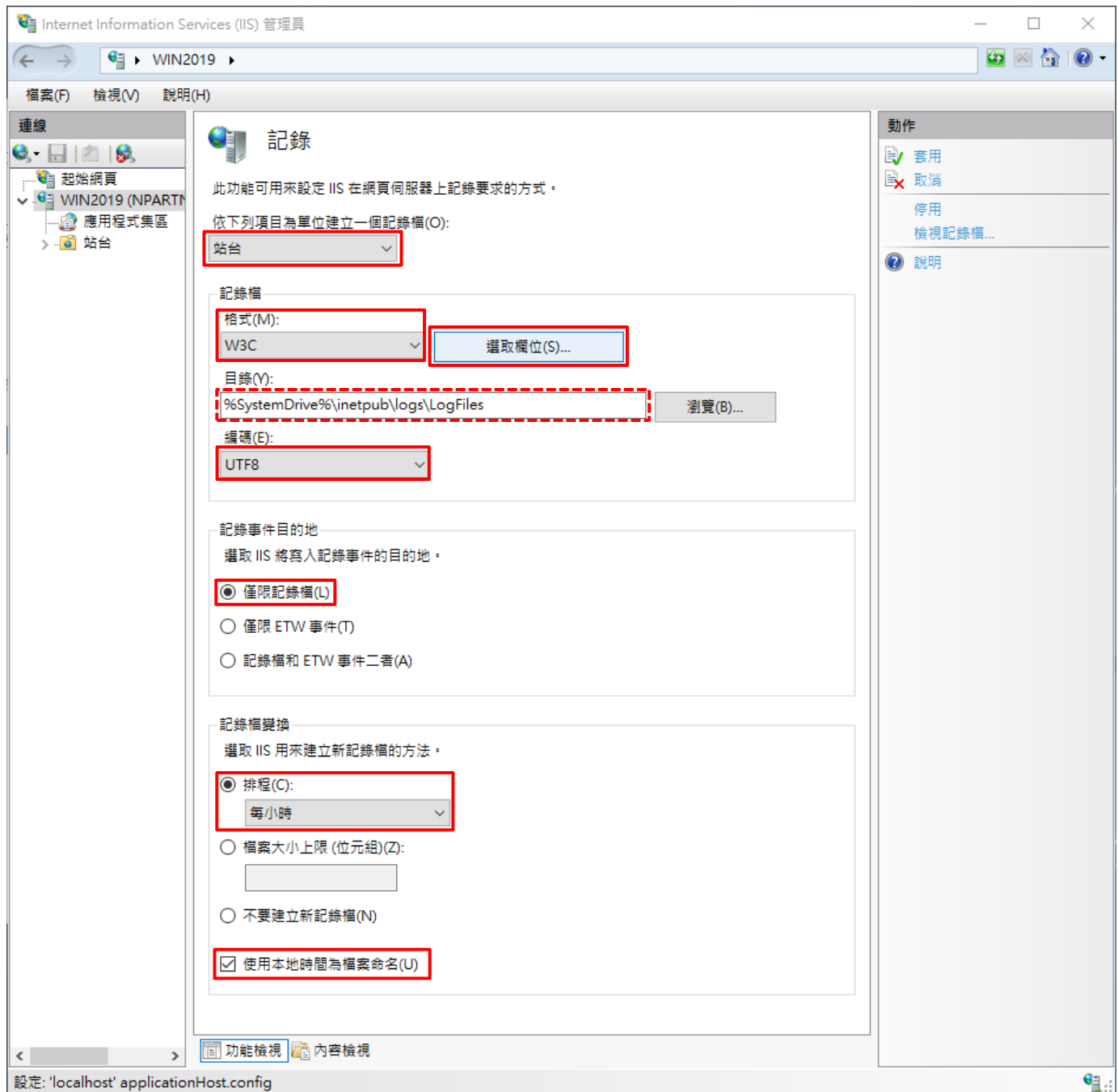


(2) 選擇 [IIS 伺服器] -> 點選 [記錄]



(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]

W3C 記錄欄位

標準欄位(S):

- 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 (Stem) (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)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

自訂欄位(C):

記錄欄位	來源類型	來源
------	------	----

新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(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]

新增自訂欄位

欄位名稱(N):
X-Forwarded-For

來源類型(T):
要求標頭

來源(S):
X-Forwarded-For

確定 取消

(6) 按下 [確定]

W3C 記錄欄位

標準欄位(S):

- 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 (Stem) (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)
- 已傳送位元組 (sc-bytes)
- 已接收位元組 (cs-bytes)
- 花費時間 (time-taken)
- 通訊協定版本 (cs-version)
- 主機 (cs-host)
- 使用者代理程式 (cs(User-Agent))
- Cookie (cs(Cookie))
- 推薦者 (cs(Referer))

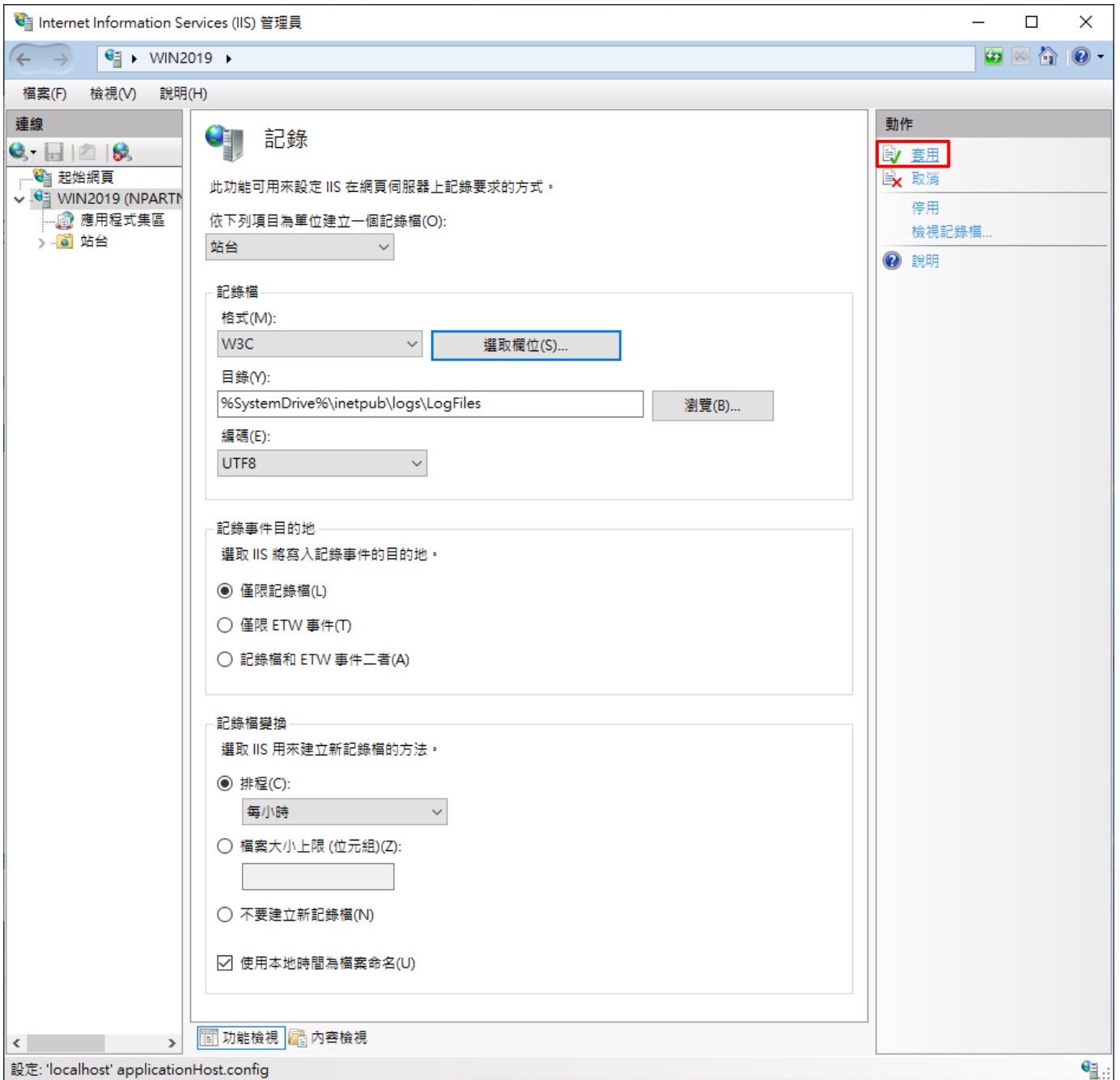
自訂欄位(C):

記錄欄位	來源類型	來源
X-Forwarded-For	要求標頭	X-Forwarded-For

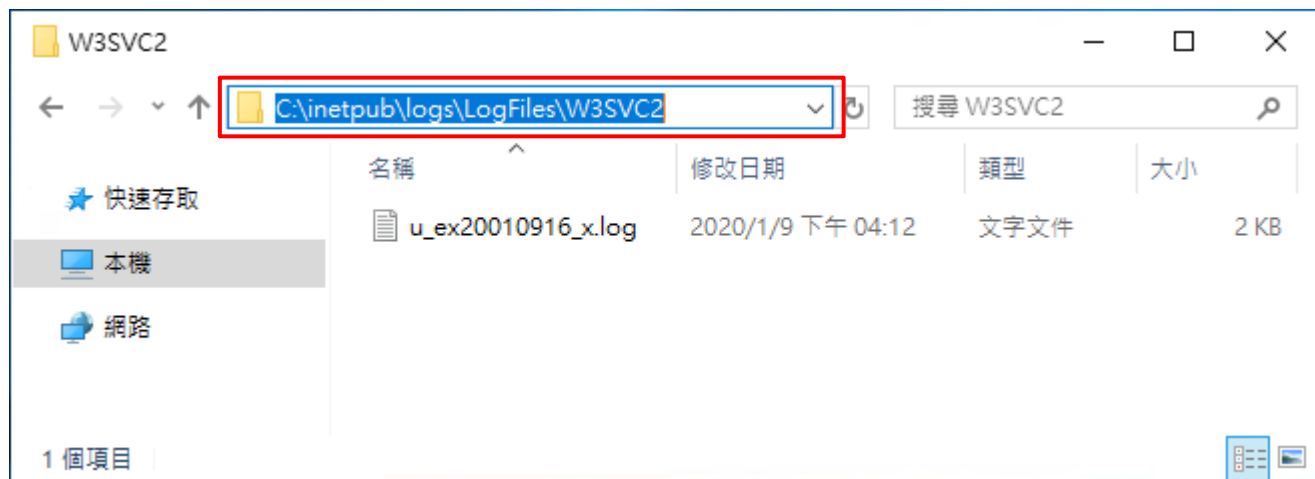
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [套用]



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

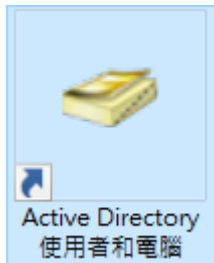


6.3 Event Log

6.3.1 組織單位

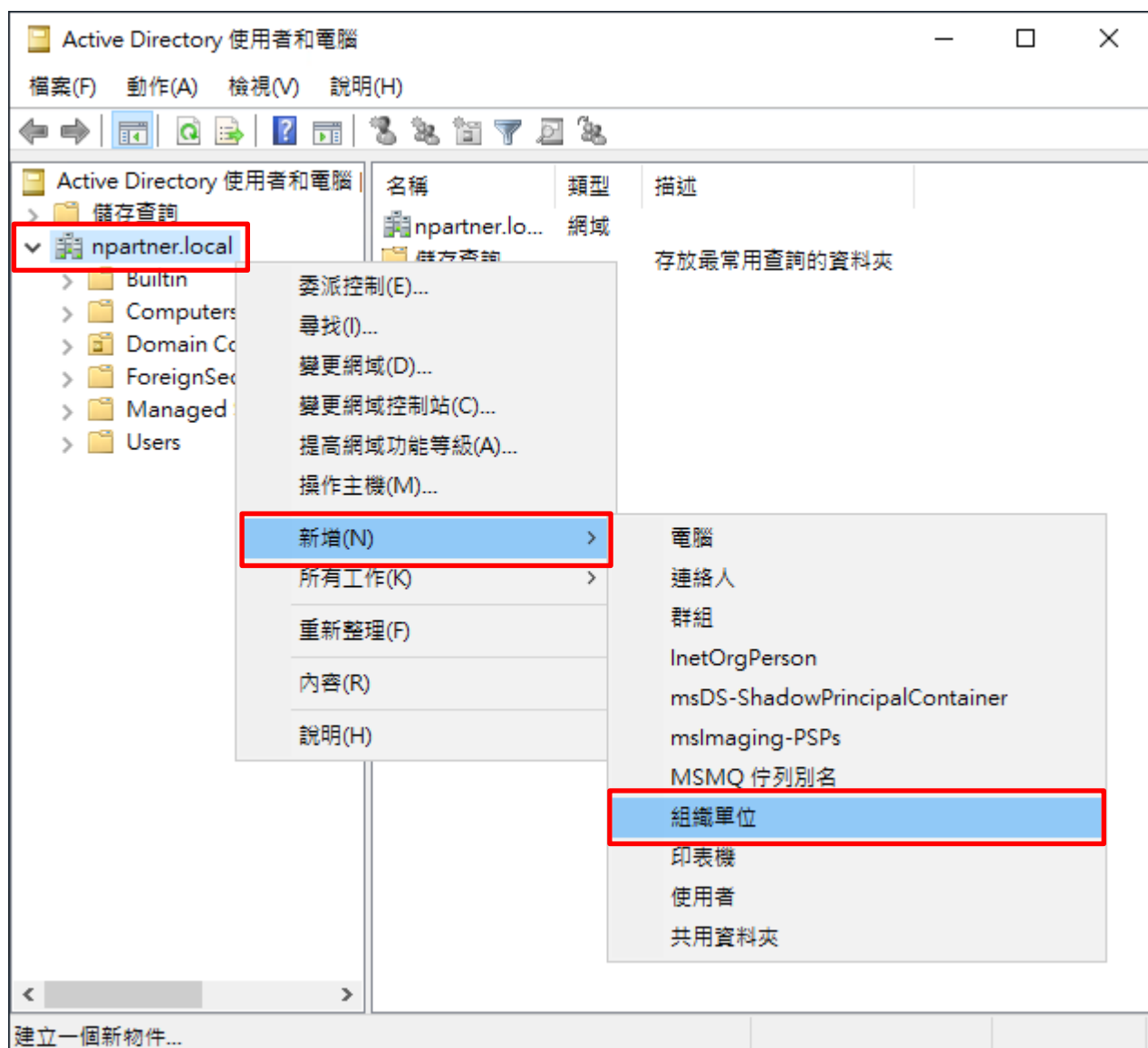
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



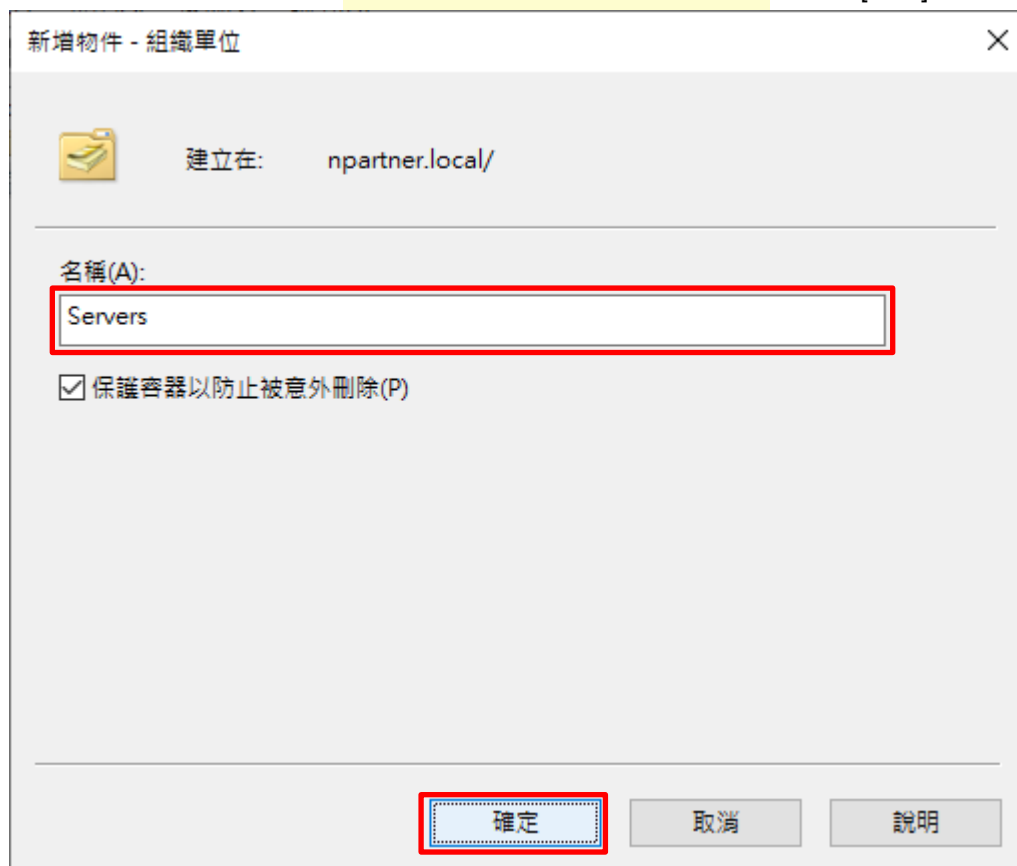
(2) 新增組織單位

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]



新增物件 - 組織單位

建立在: npartner.local/

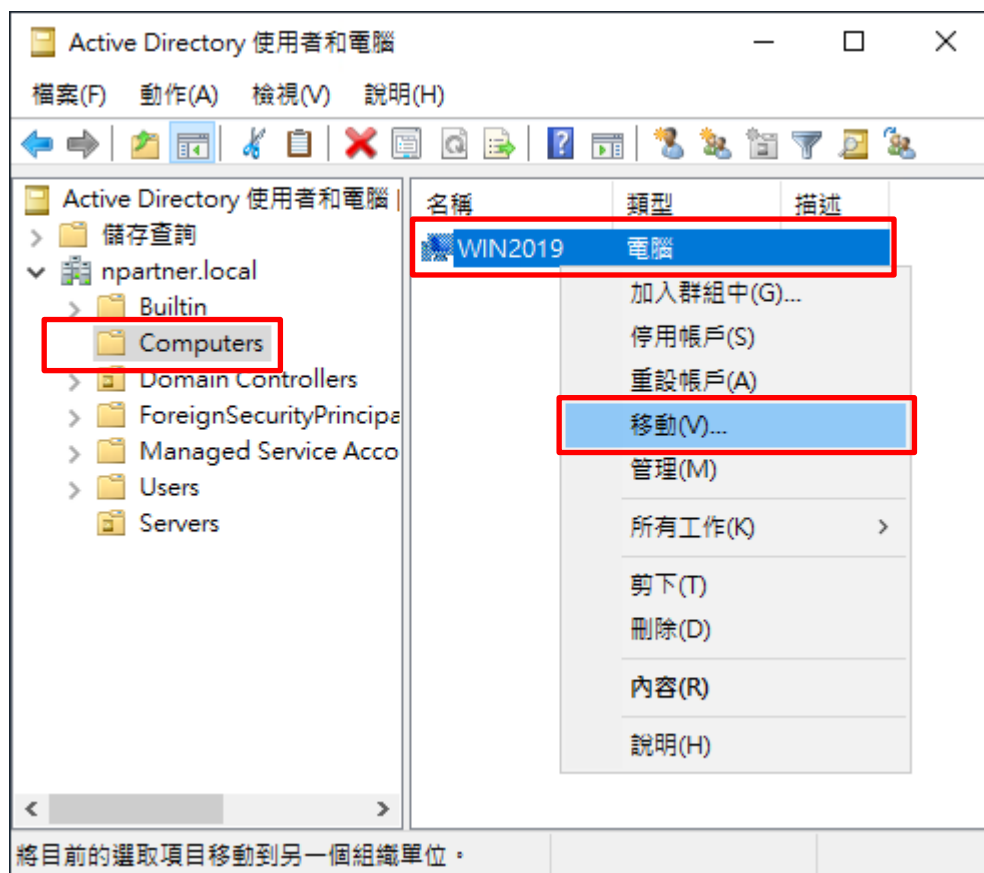
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

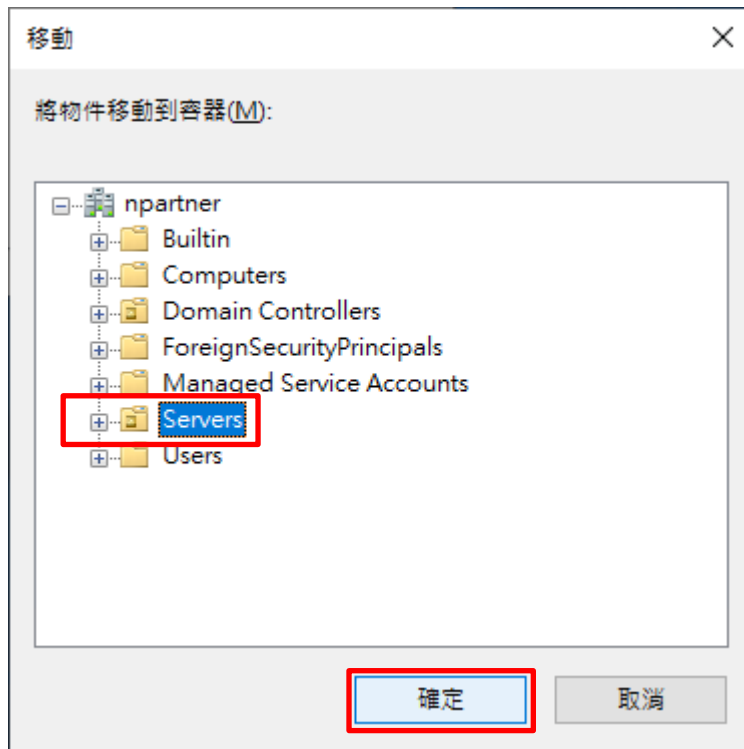
(4) 移動 Exchange 伺服器至新的組織單位

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]



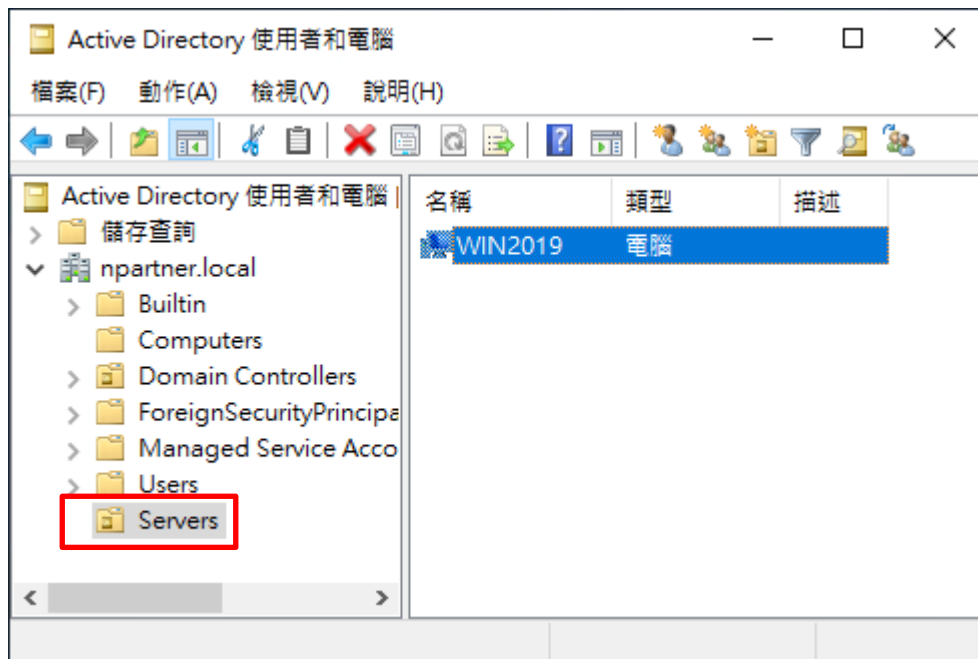
(5) 選擇組織單位

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

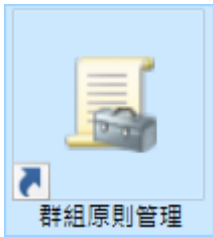
點選 [Servers] 組織單位，確認 Win2019 伺服器已移動。



6.3.2 群組原則

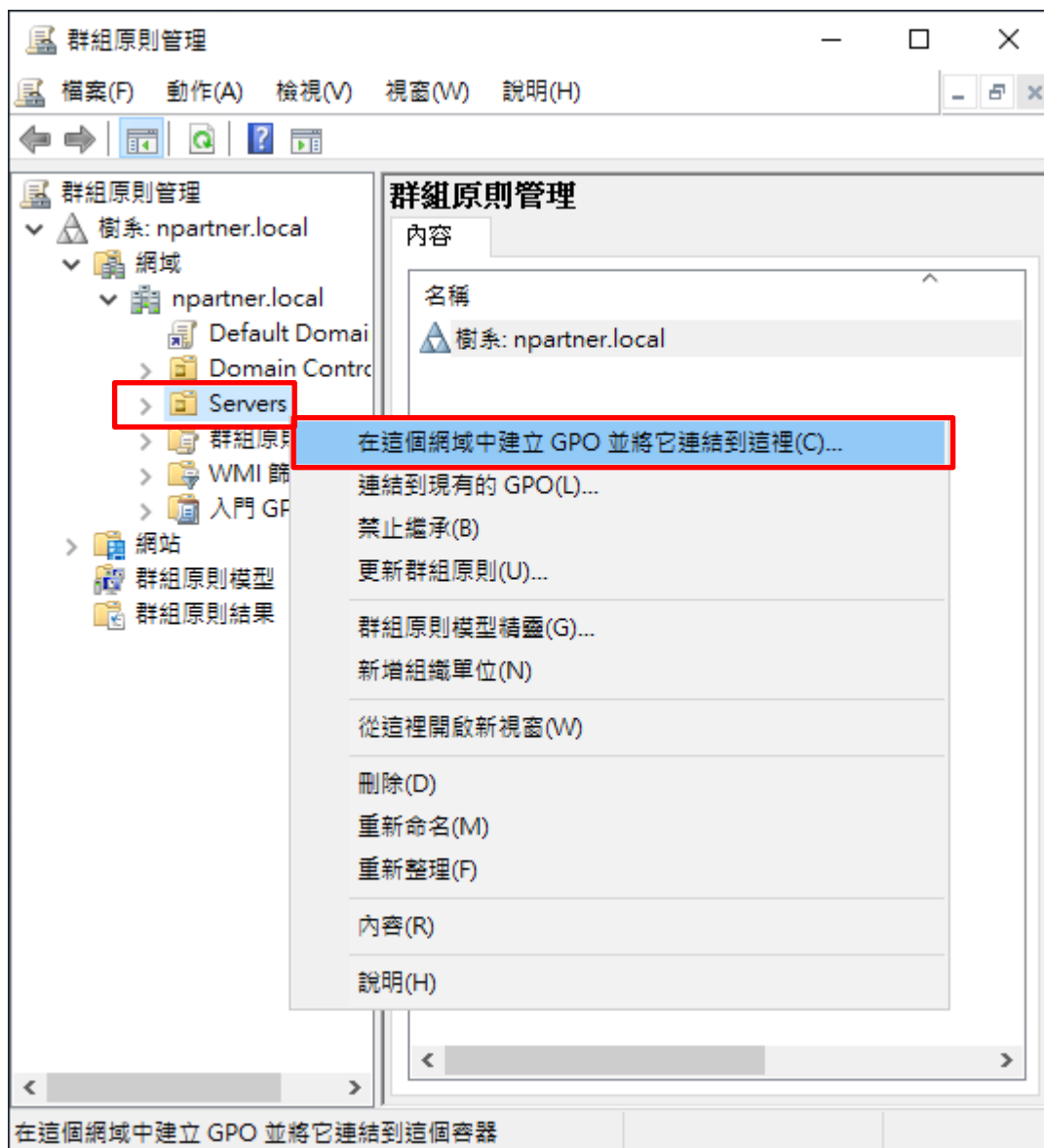
(1) 開啟群組原則管理

開啟 [群組原則管理]



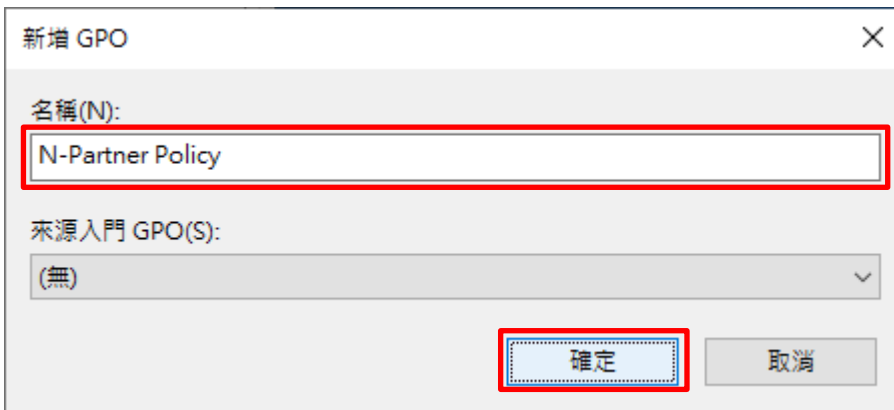
(2) 在 Servers 組織單位，新增群組原則物件

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...]



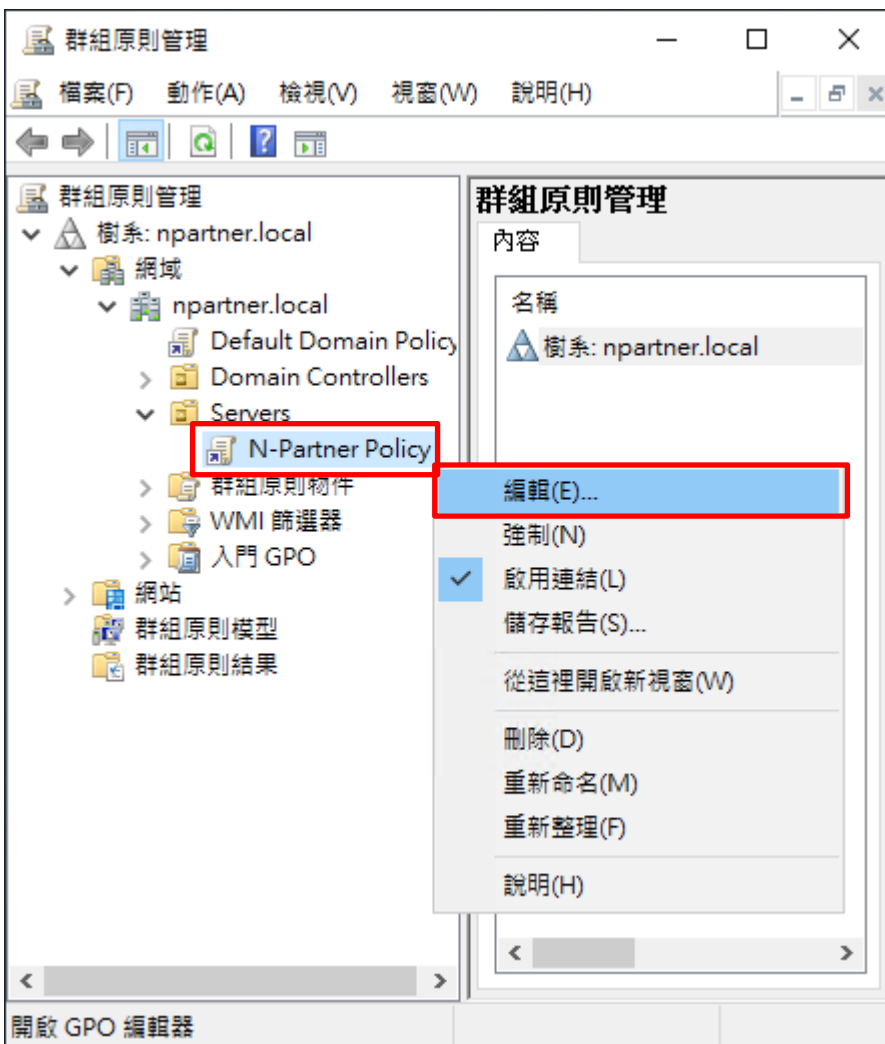
(3) 輸入群組原則物件名稱

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]



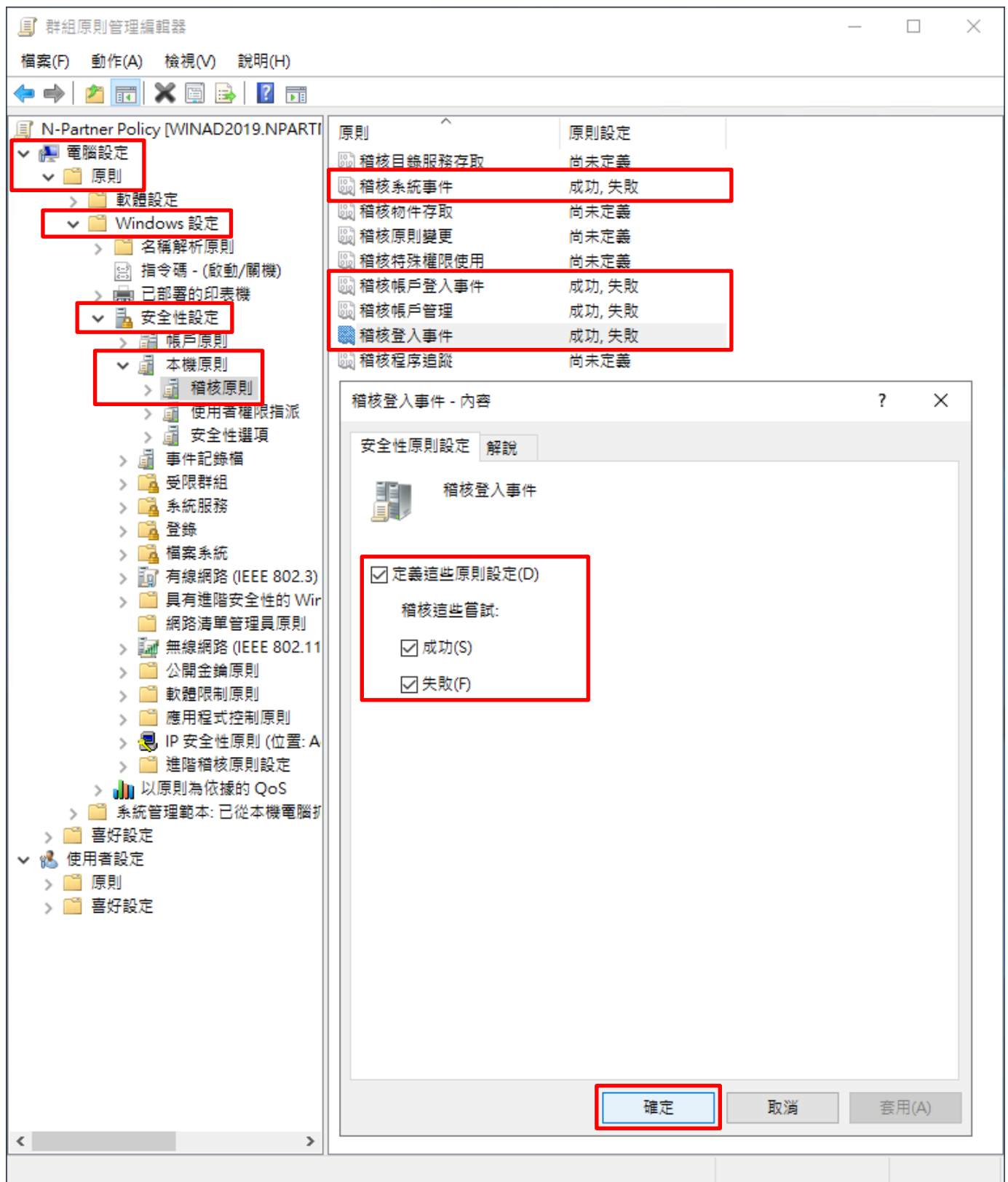
(4) 編輯群組原則物件

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

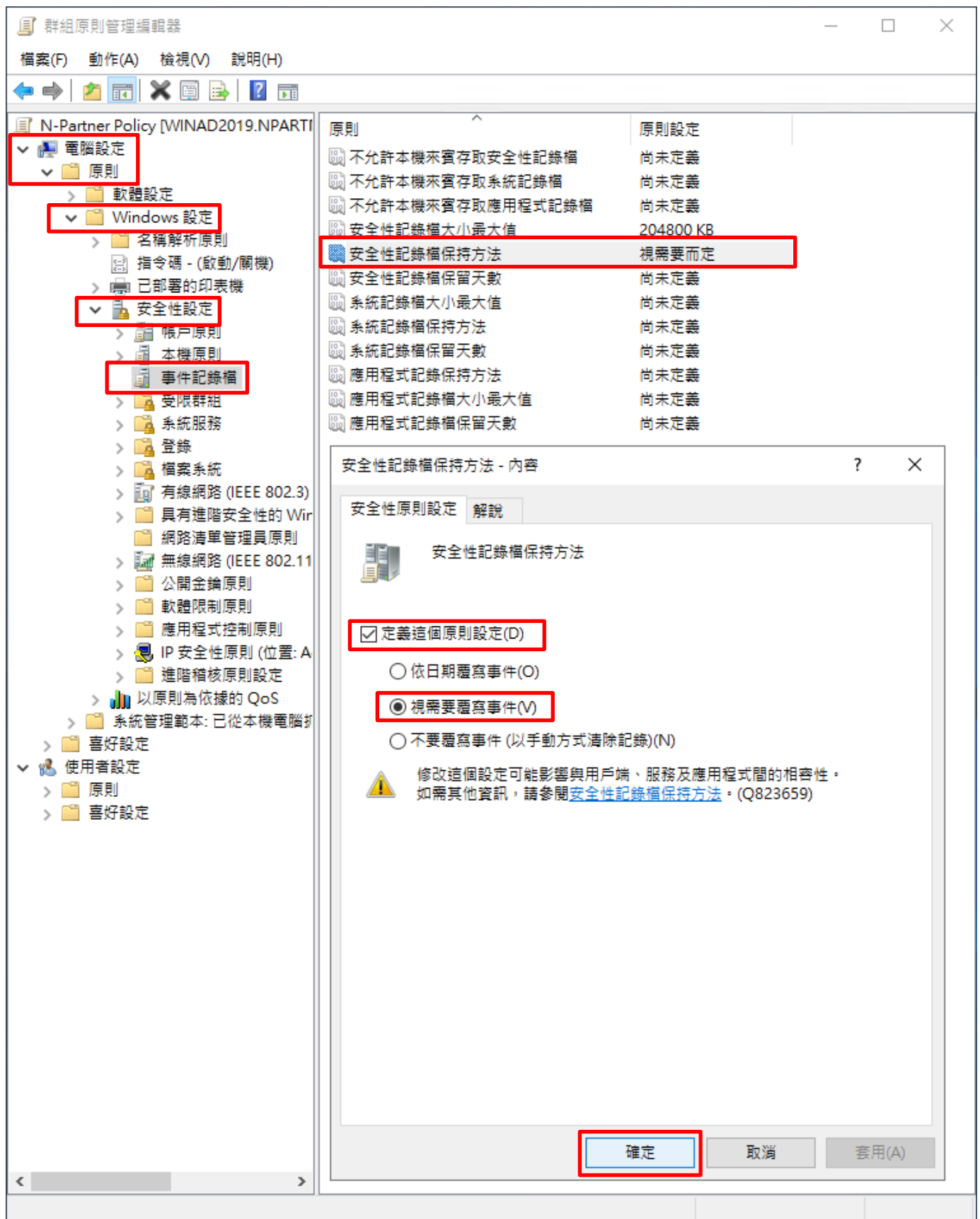
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Editor window titled "群組原則管理編輯器". The left-hand navigation pane is expanded to show the following path: 電腦設定 > 原則 > Windows 設定 > 安全性設定 > 事件記錄檔. The right-hand pane displays a list of policies. The policy "安全性記錄檔大小最大值" is selected and highlighted, showing a value of 204800 KB. Below this, a dialog box titled "安全性記錄檔大小最大值 - 內容" is open. In this dialog, the "定義這個原則設定(D)" checkbox is checked. The value "204800" is entered in the text box, followed by "KB". A warning icon and text are visible below the input field, stating: "修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)". At the bottom of the dialog, the "確定" button is highlighted with a red box.

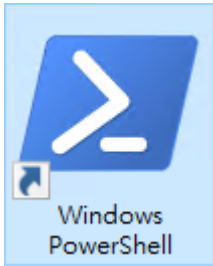
原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(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-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command `Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force` being entered. The text "Win2019" is highlighted in red in the original image. The prompt ends with a cursor.

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
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command `Get-GPResultantSetofPolicy -Computer Win2019 -Path C:\tmp\Win2019.html -ReportType html` being entered. The text "Win2019" and "C:\tmp\Win2019.html" are highlighted in red in the original image. The output of the command is displayed as follows:
RsopMode : Logging
Namespace : \\Win2019\Root\Rsop\NS137F43CC_4F1A_4AA4_A92E_3C4E0FB6490A
LoggingComputer : Win2019
LoggingUser : NPARTNER\administrator
LoggingMode : Computer
The prompt ends with a cursor.

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

群組原則結果

NPARTNER\WIN2019
資料收集: 2021/11/18 下午 03:44:05 全部顯示

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/安全性選項 顯示

事件記錄檔 隱藏

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

7. N-Reporter

(1) 新增 MS Exchange 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]

The screenshot displays the N-Reporter web application interface. On the left is a dark blue sidebar menu with the following items: 'Admin (Global) v', '事件', '報表', '智慧分析', '設備管理' (highlighted with a red box), '設備樹狀圖' (highlighted with a red box), '介面列表', '告警樣版', '設備異常告警', '系統管理', and '使用者手冊'. The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖' and the title '設備樹狀圖'. Below the title is a search bar with a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a green 'U' button, and a yellow speaker icon. The main content area lists 'Global (4)' and '未知設備 (0)'.

7.1 Exchange Message Tracking 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]

新增設備

設備基本設定

名稱
ExchangeMail-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
Exchange 2007

使用自定義資料格式

Facility
(2) mail system

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

本設備於分時監控報表啟動Syslog轉發時， Raw Data

設備進階設定

ICMP 告警樣版
----- N/A -----

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

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]

新增設備

設備基本設定

名稱
ExchangeMail-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
Exchange 2013

使用自定義資料格式

Facility
(2) mail system

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

設備進階設定

ICMP 告警樣版
N/A

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

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]

新增設備

設備基本設定

名稱
ExchangeIIS-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
IIS

使用自定義資料格式

Facility
(22) local use 6 (local6)

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

本設備於分時監控報表啟動Syslog轉發時 Raw Data

設備進階設定

ICMP 告警樣版
N/A

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

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]

新增設備

設備基本設定

名稱
ExchangeEvent-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
Windows

使用自定義資料格式

Facility
(17) local use 1 (local1)

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

設備進階設定

ICMP 告警樣版
N/A

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

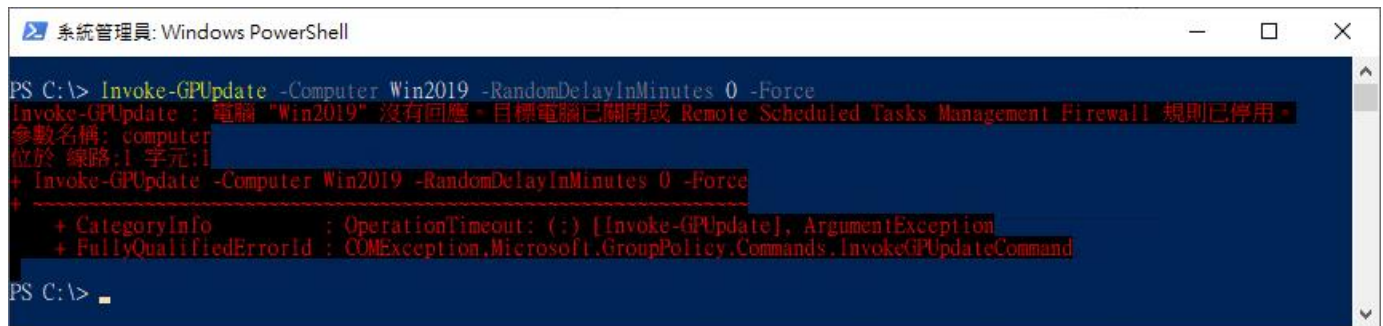
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

8. 問題排除

8.1 Invoke-GPUdate 錯誤

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



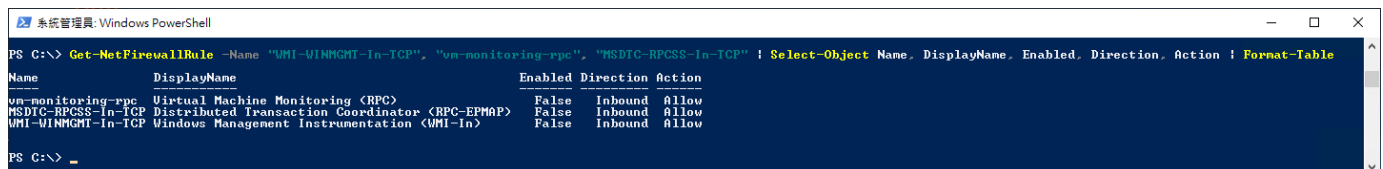
```
PS C:\> Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
Invoke-GPUdate : 電腦 "Win2019" 沒有回應。目標電腦已關閉或 Remote Scheduled Tasks Management Firewall 規則已停用。
參數名稱: computer
位於 線路:1 字元:1
+ Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
+ ~~~~~
+ CategoryInfo          : OperationTimeout: (:) [Invoke-GPUdate], ArgumentException
+ FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUdateCommand
PS C:\> _
```

(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

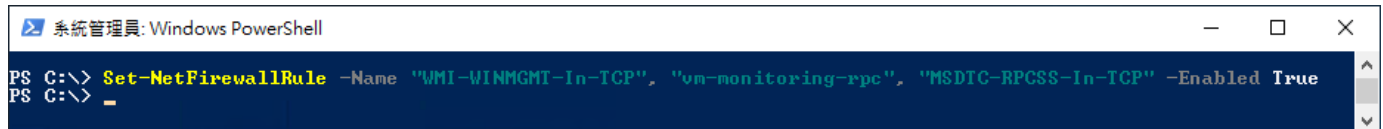
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
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
Name                DisplayName          Enabled Direction Action
-----
vm-monitoring-rpc   Virtual Machine Monitoring (RPC)      False  Inbound  Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP) False  Inbound  Allow
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In) False  Inbound  Allow
PS C:\> _
```

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

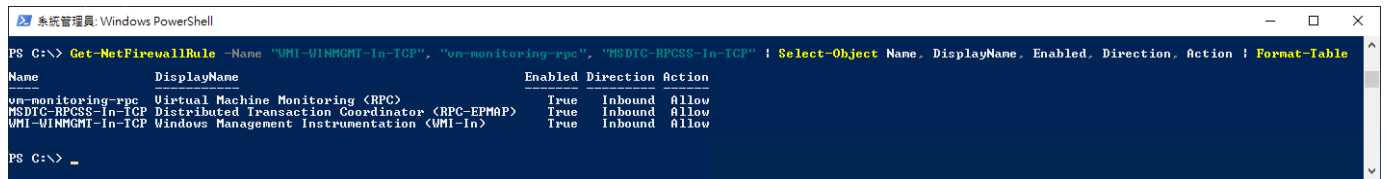
```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -
Enabled True
```



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

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

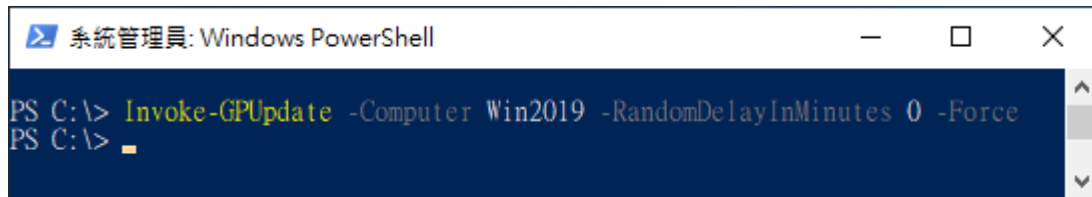
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |  
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
系統管理員: Windows PowerShell  
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  
Name                DisplayName                Enabled Direction Action  
-----  
vm-monitoring-rpc   Virtual Machine Monitoring <RPC>      True    Inbound Allow  
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator <RPC-EPMAP> True    Inbound Allow  
WMI-WINMGMT-In-TCP Windows Management Instrumentation <WMI-In> True    Inbound Allow  
PS C:\> _
```

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

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



```
系統管理員: Windows PowerShell  
PS C:\> Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force  
PS C:\> _
```

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