



N-Partner

如何設定 MS Exchange Server 郵件追蹤記錄

V014

2019/11/11



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	6.1.2 Exchange Management Shell	85
1. NXLog	3	6.2 IIS log	86
1.1 NXLog 架構	3	6.3 Event log	93
1.2 NXLog 安裝	4	6.3.1 組織單位(Organizational Unit)	93
1.3 NXLog 設定檔	5	6.3.2 群組原則(Group Policy Management)	96
1.4 NXLog 啟動服務	8	7. N-Reporter	103
2. Exchange 2007	9	7.1 Exchange Message Tracking log	103
2.1 使用 [Exchange 管理主控台] 設定	9	7.2 Exchange Event log	105
2.2 使用 [Exchange 管理命令介面] 設定	11	7.3 Exchange IIS log	107
3. Exchange 2010	13	連 絡 資 訊	108
3.1 Exchange Message Tracking Log	13		
3.1.1 Exchange Management Console	13		
3.1.2 Exchange Management Shell	16		
3.2 IIS log	18		
3.3 Event log	33		
3.3.1 組織單位(Organizational Unit)	33		
3.3.2 群組原則(Group Policy Management)	36		
4. Exchange 2013	41		
4.1 Exchange Message Tracking Log	41		
4.1.1 Exchange 系統管理中心 (EAC)	41		
4.1.2 Exchange Management Shell	44		
4.2 IIS log	45		
4.3 Event log	52		
4.3.1 組織單位(Organizational Unit)	52		
4.3.2 群組原則(Group Policy Management)	55		
5. Exchange 2016	62		
5.1 Exchange Message Tracking Log	62		
5.1.1 Exchange 系統管理中心 (EAC)	62		
5.1.2 Exchange Management Shell	65		
5.2 IIS log	66		
5.3 Event log	72		
5.3.1 組織單位(Organizational Unit)	72		
5.3.2 群組原則(Group Policy Management)	75		
6. Exchange 2019	82		
6.1 Exchange Message Tracking Log	82		
6.1.1 Exchange 系統管理中心 (EAC)	82		



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 Server 郵件追蹤記錄。NXLog 工具將 MS Exchange Server 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。

註: Microsoft Exchange Server 預設啟用郵件追蹤。

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

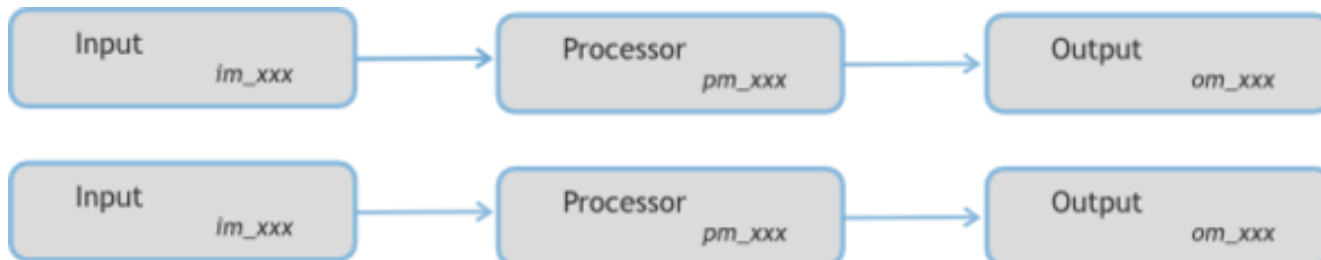
<https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

1. NXLog

1.1 NXLog 架構

NXLog 的 plugin 架構允許任何類型的輸入讀取資料、解析和轉換訊息的格式，然後將其發送到任何類型的輸出。可以同時使用不同的輸入、處理和輸出模組來滿足事件記錄。

<https://nxlog.co/documentation/nxlog-user-guide#modules-im>



1.2 NXLog 安裝

(1) 下載 NXLog

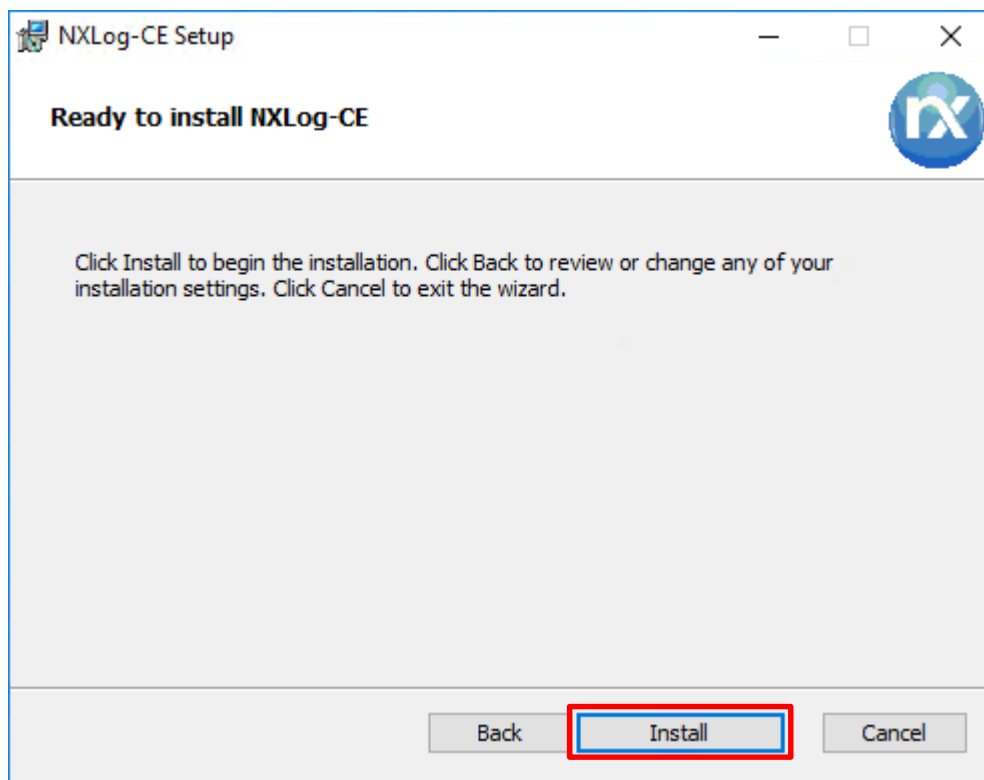
前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 nxlog-ce-x.x.xxxx.msi · 範例: nxlog-ce-2.10.2150.msi ◦



(2) 安裝 NXLog

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



(3) 下載並覆蓋 NXLog 設定檔

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

覆蓋 NXLog 設定檔 `Copy-Item nxlog_Exchange.conf '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 ROOT      C:\Program Files (x86)\nxlog
define NCloud    192.168.3.51
define MailLog   C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
define IISLog    C:\inetpub\logs\LogFiles
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_mail>
  Module im_file
  File '%MailLog%\MSGTRK*.LOG'
  ReadFromLast TRUE
  SavePos TRUE
</Input>

<Output out_mail>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 2;
```



```
Exec      $SourceName = 'Exchange';
Exec      to_syslog_bsd();
</Output>

<Route mail>
  Path     in_mail => out_mail
</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=4648)]]</Select> \
                    <Select Path="Security">*[System[(EventID=4634 or EventID=4647)]]</Select> \
                </Query> \
</QueryList>
</Input>

<Output out_eventlog>
  Module om_udp
  Host     %NCloud%
  Port     514
  Exec     $SyslogFacilityValue = 20;
  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_iis>
  Module      im_file
  File        '%IISLog%\u_ex*.log'
  ReadFromLast TRUE
  Recursive   TRUE
  SavePos     TRUE
</Input>

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

<Route iis>
  Path    in_iis => out_iis
</Route>

```

藍色文字部位請輸入 N-Reporter 系統 IP address :

```
define NCloud 192.168.3.51
```

藍色文字部位請輸入郵件追蹤記錄資料夾

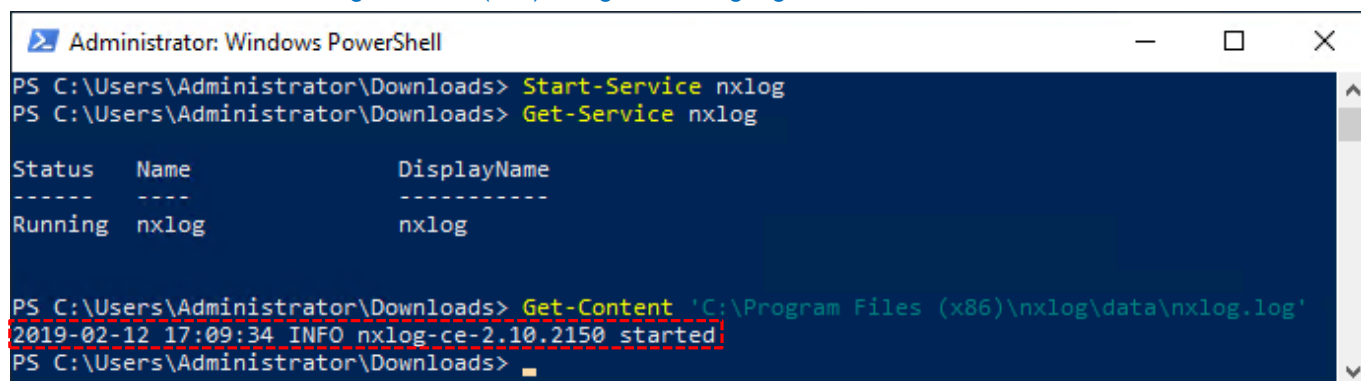
```
define Mail_Log C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

藍色文字部位請輸入 IIS log 資料夾

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

1.4 NXLog 啟動服務

開啟 [Windows PowerShell] -> 輸入 `Start-Service nxlog` 啟動 nxlog 服務和 `Get-Service nxlog` 查看 nxlog 服務狀態 -> `Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息。



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads> Start-Service nxlog
PS C:\Users\Administrator\Downloads> Get-Service nxlog

Status  Name          DisplayName
-----  -
Running nxlog         nxlog

PS C:\Users\Administrator\Downloads> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2019-02-12 17:09:34 INFO nxlog-ce-2.10.2150 started
PS C:\Users\Administrator\Downloads>
```

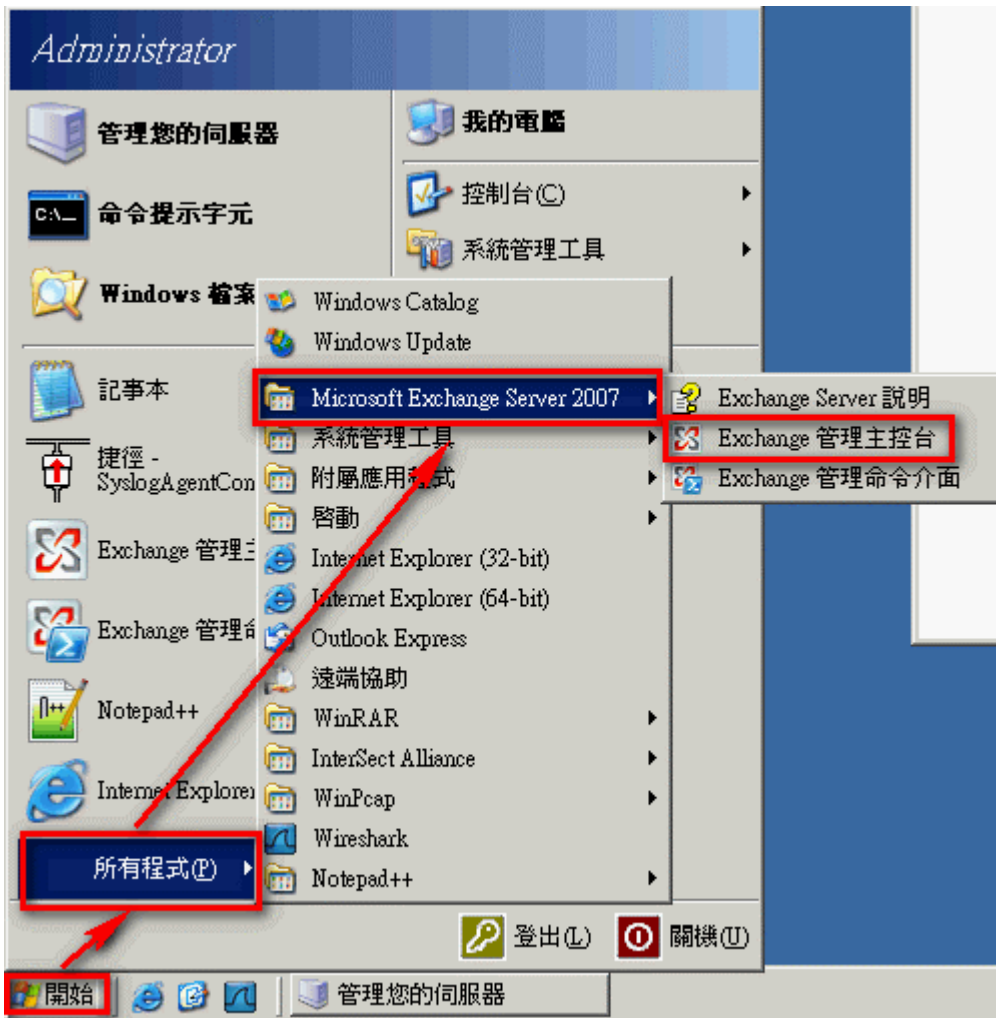
2. Exchange 2007

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。

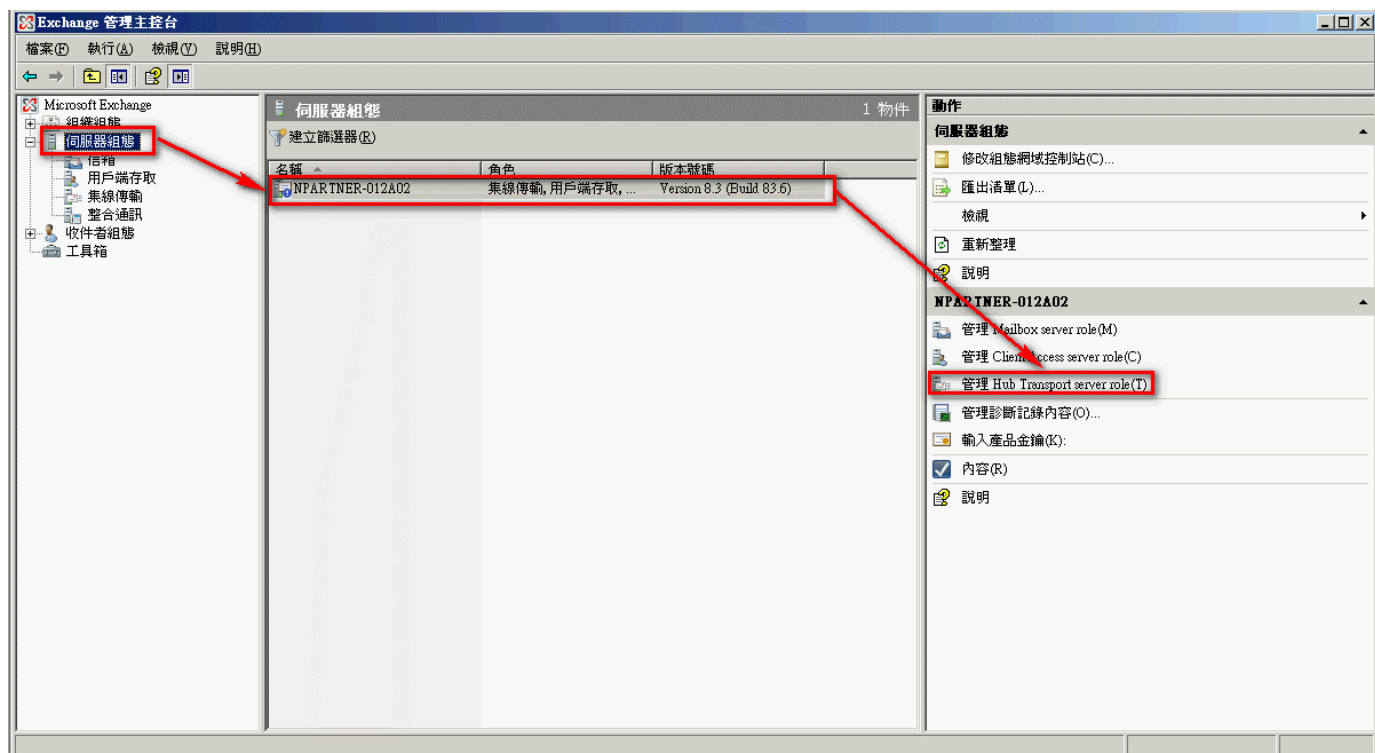
2.1 使用 [Exchange 管理主控台] 設定

(1) 以系統管理者 Administrator 登入 Exchange Server

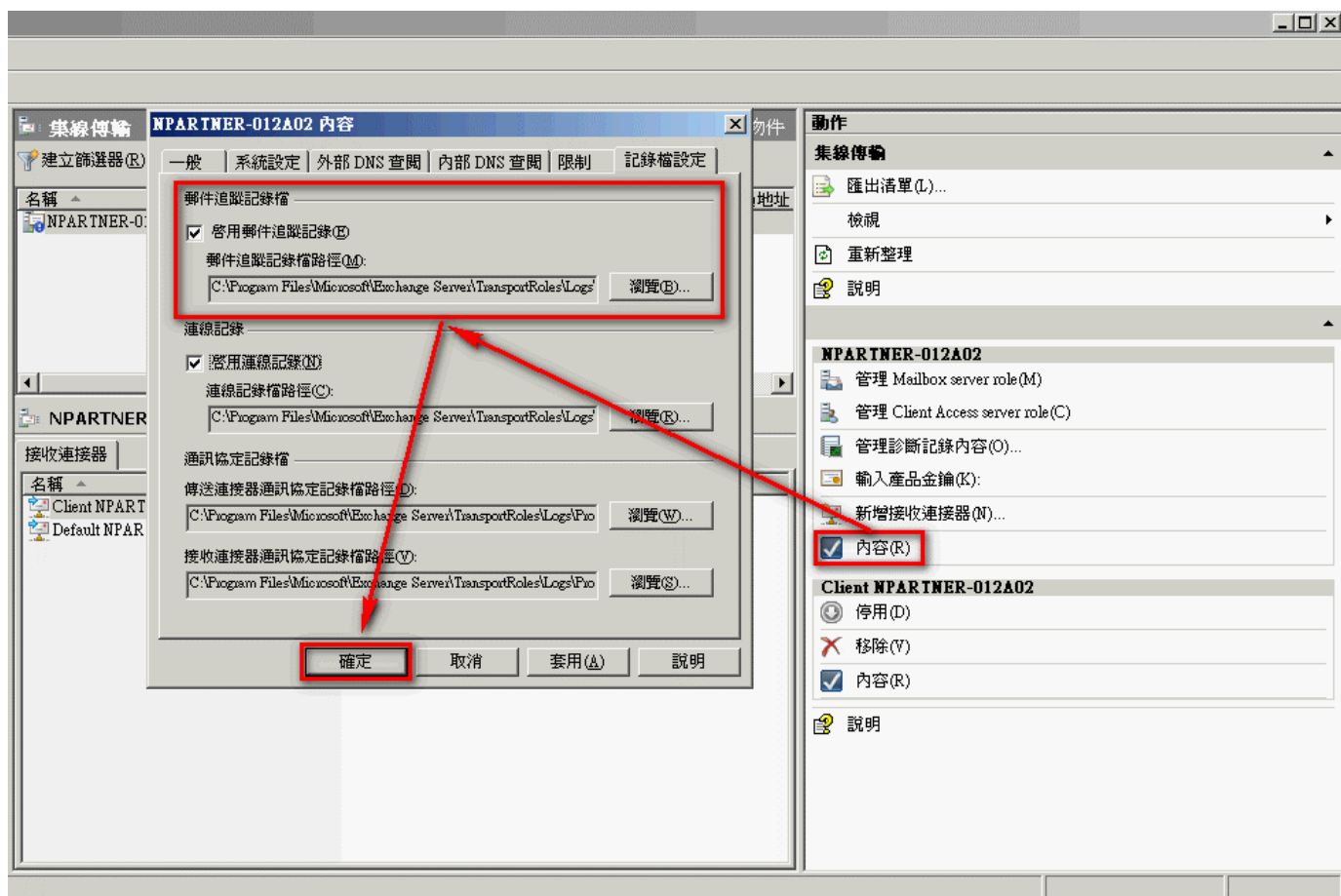
(2) 滑鼠左點[開始] -> [所有程式] -> [Microsoft Exchange Server 2007] -> [Exchange 管理主控台]



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

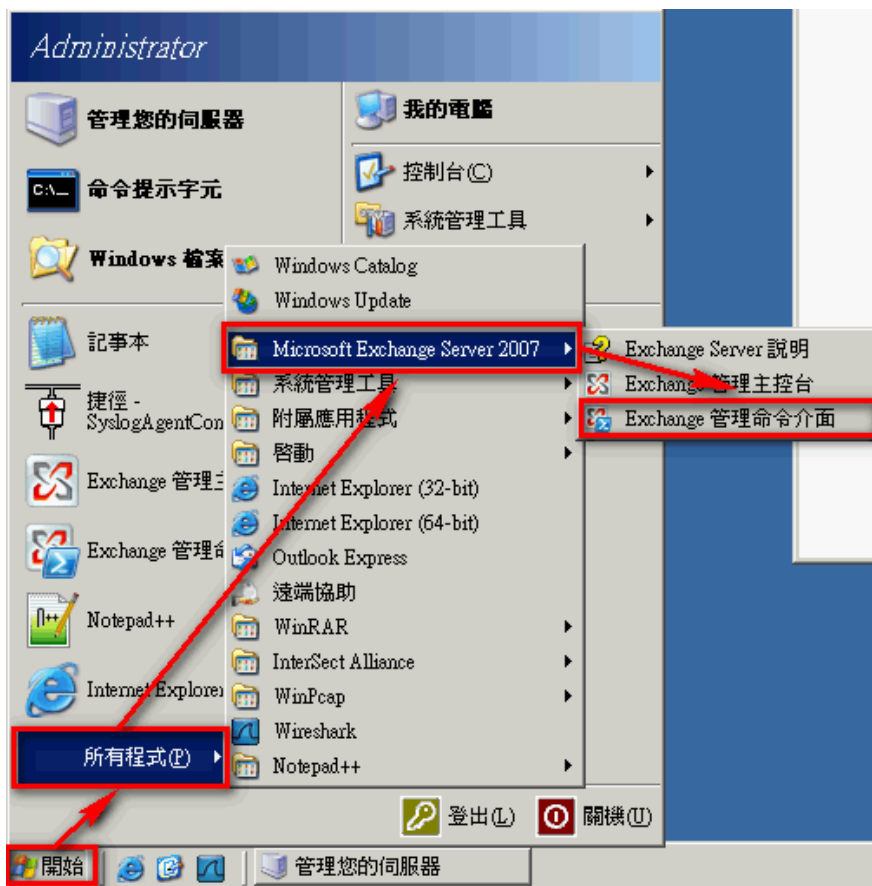


(4) 滑鼠左點 [內容]。勾選 [啟用郵件追蹤記錄]，左點 [瀏覽]，設定郵件追蹤記錄檔路徑，預設 C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking。左點 [確定]，完成配置。



2.2 使用 [Exchange 管理命令介面] 設定

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



(3) 啟用郵件追蹤。命令列輸入：

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

或

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

<ServerIdentity> 為 Exchange Server 的電腦名稱，<LocalFilePath> 為郵件追蹤記錄的路徑，預設為

C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking

本例輸入：

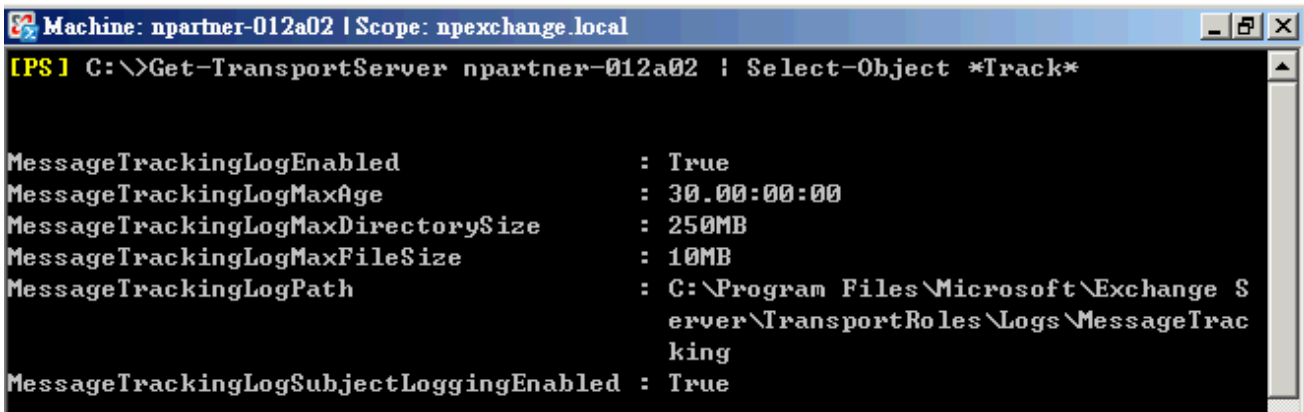
```
Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled $True -MessageTrackingLogPath  
"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"
```



```
Machine: npartner-012a02 | Scope: npexchange.local  
[PS] C:\>Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled $True -M  
essageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\TransportRoles  
\Logs\MessageTracking"  
[PS] C:\>
```

(4) 檢查郵件追蹤記錄配置。命令列輸入：

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



```
Machine: npartner-012a02 | Scope: npexchange.local  
[PS] C:\>Get-TransportServer npartner-012a02 | Select-Object *Track*  
  
MessageTrackingLogEnabled           : True  
MessageTrackingLogMaxAge             : 30.00:00:00  
MessageTrackingLogMaxDirectorySize  : 250MB  
MessageTrackingLogMaxFileSize       : 10MB  
MessageTrackingLogPath               : C:\Program Files\Microsoft\Exchange S  
erver\TransportRoles\Logs\MessageTrac  
king  
MessageTrackingLogSubjectLoggingEnabled : True
```

3. Exchange 2010

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

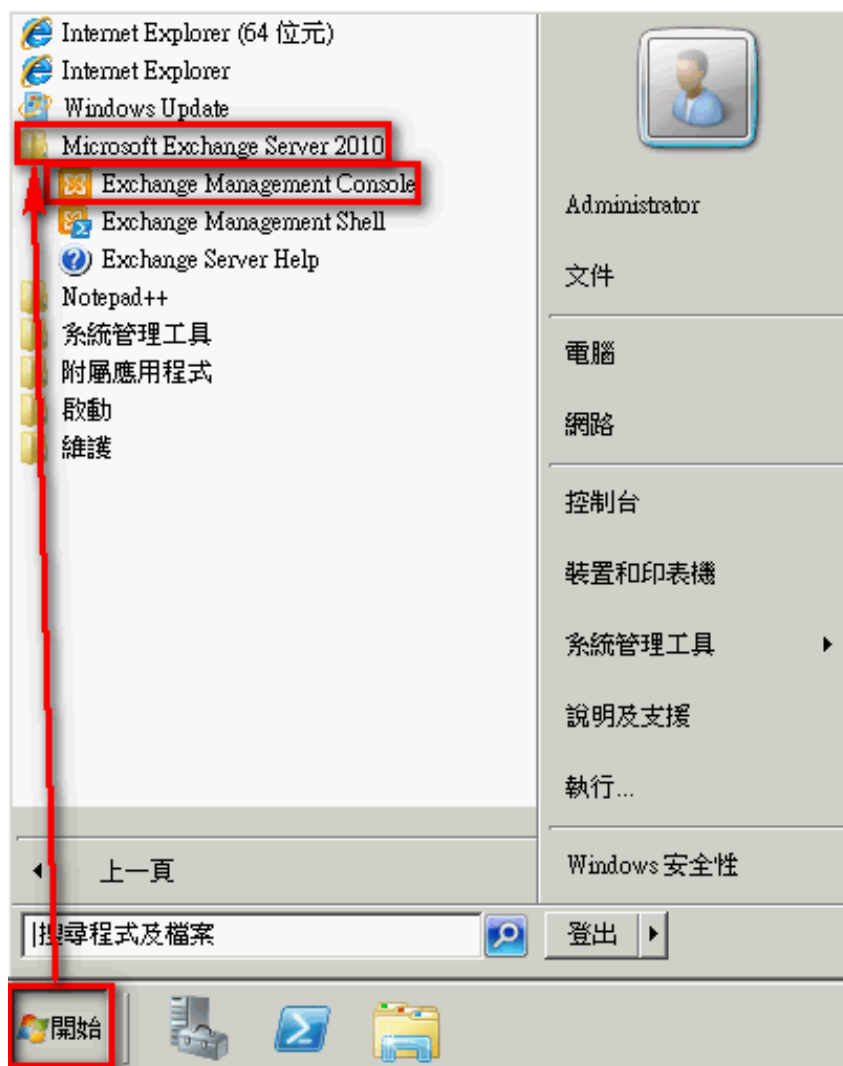
註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入郵件追蹤記錄資料夾

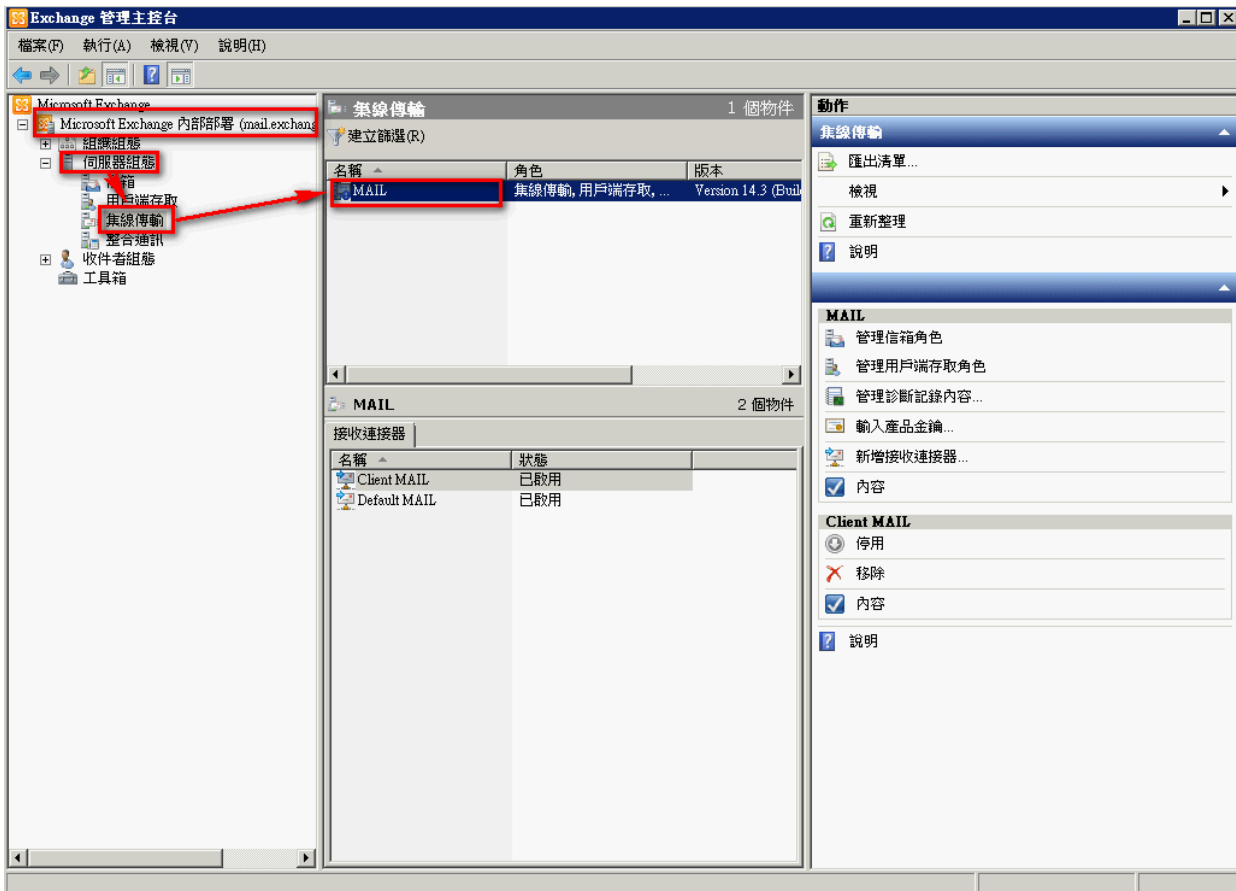
```
define Mail_Log C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking
```

3.1.1 Exchange Management Console

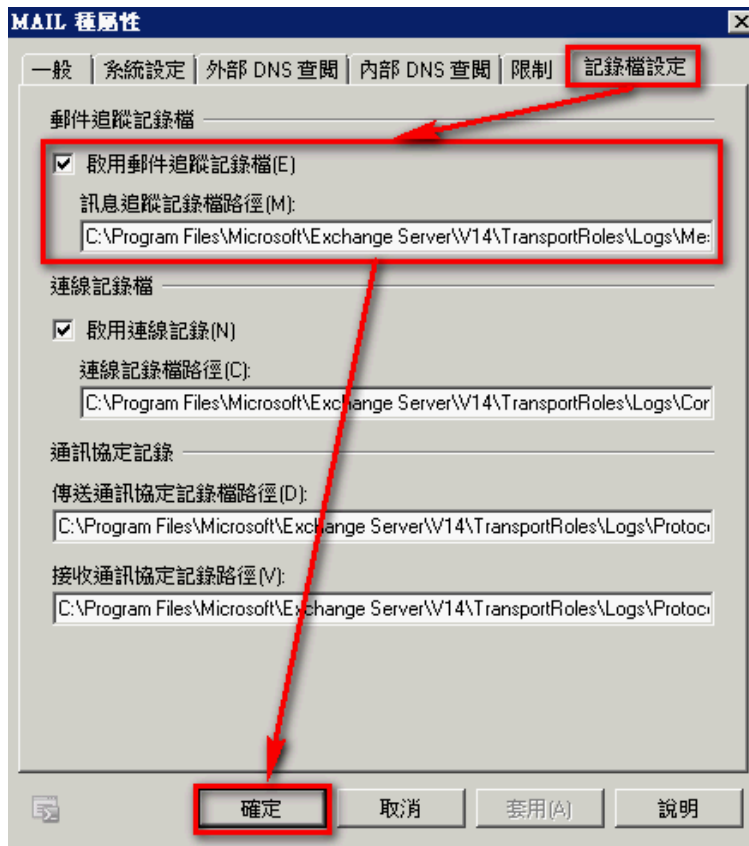
- (1) 以系統管理者 Administrator 登入 Exchange Server
- (2) 滑鼠左點 [開始] -> [所有程式] -> [Microsoft Exchange Server 2010] -> [Exchange Management Console]



(3) 滑鼠左點 [Microsoft Exchange 內部部署] -> [伺服器組態] -> [集線傳輸] 滑鼠右點 Exchange Server · 本例為 MAIL · 左點 [內容]。

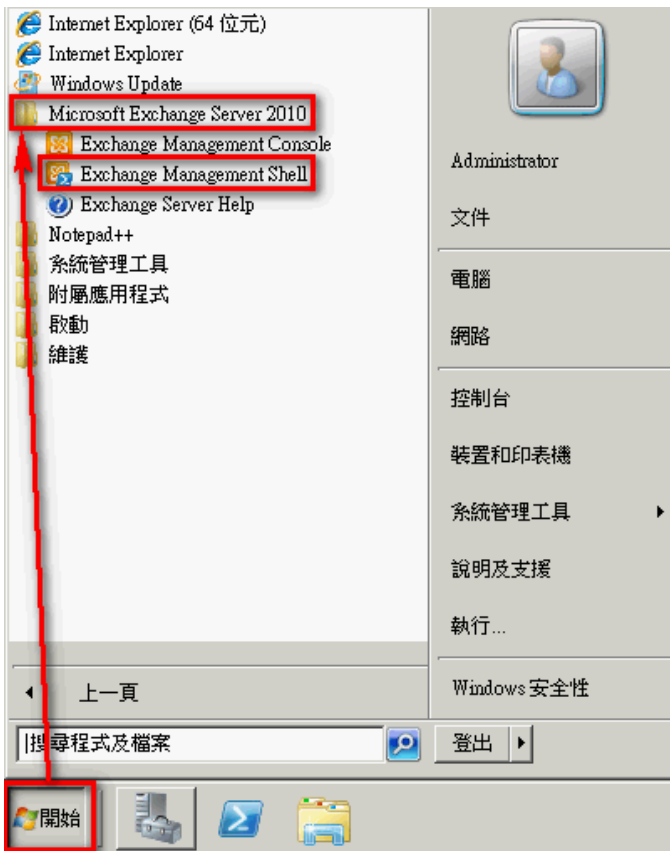


(4) 滑鼠左點 [記錄檔設定]。勾選 [啟用郵件追蹤記錄檔]，輸入 [訊息追蹤記錄檔路徑]，預設為 C:\Program Files\Microsoft\Exchange Server\14\TransportRoles\Logs\MessageTracking。左點 [確定]，完成配置。



3.1.2 Exchange Management Shell

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



- (3) 啟用郵件追蹤。命令列輸入：

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

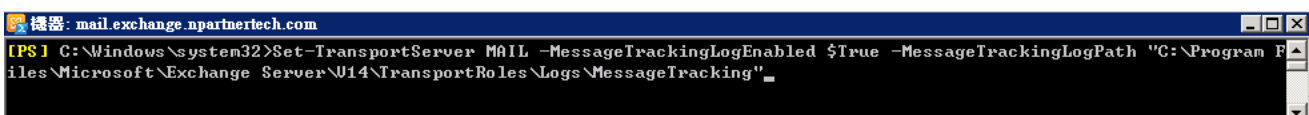
或

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

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

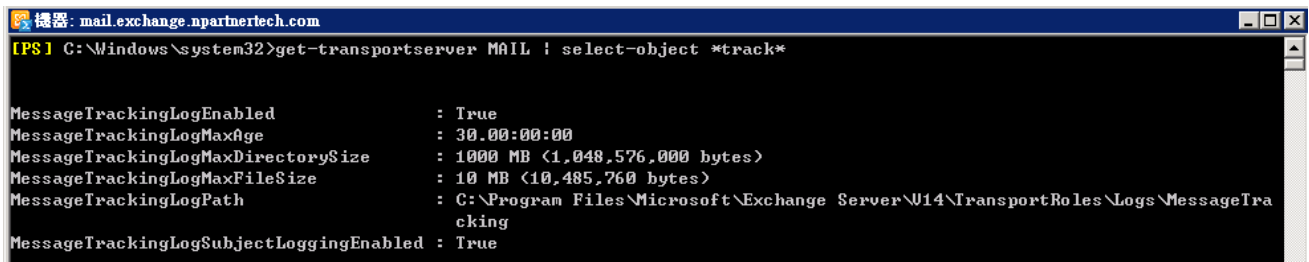
本例輸入：

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



(4) 檢查郵件追蹤記錄配置。命令列輸入：

Get-TransportServer MAIL | Select-Object *Track*



```
機器: mail.exchange.npartnertech.com
[PS] C:\Windows\system32>get-transportserver MAIL | 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\W14\TransportRoles\Logs\MessageTra
                                     cking
MessageTrackingLogSubjectLoggingEnabled : True
```

3.2 IIS log

(1) 安裝 IIS Advanced Logging

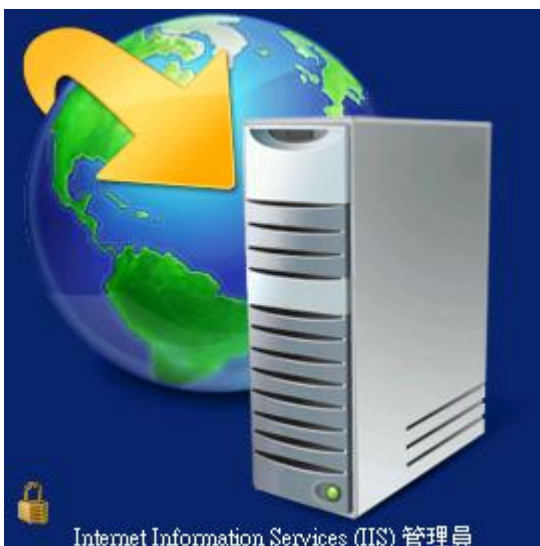
IIS Advanced Logging 提供豐富、彈性的資料集合和即時的記錄功能。記錄任何 HTTP 要求/回應標頭、IIS 伺服器變數和用戶端欄位，以追蹤使用者參與的情況。

<https://www.microsoft.com/zh-tw/download/details.aspx?id=7211>

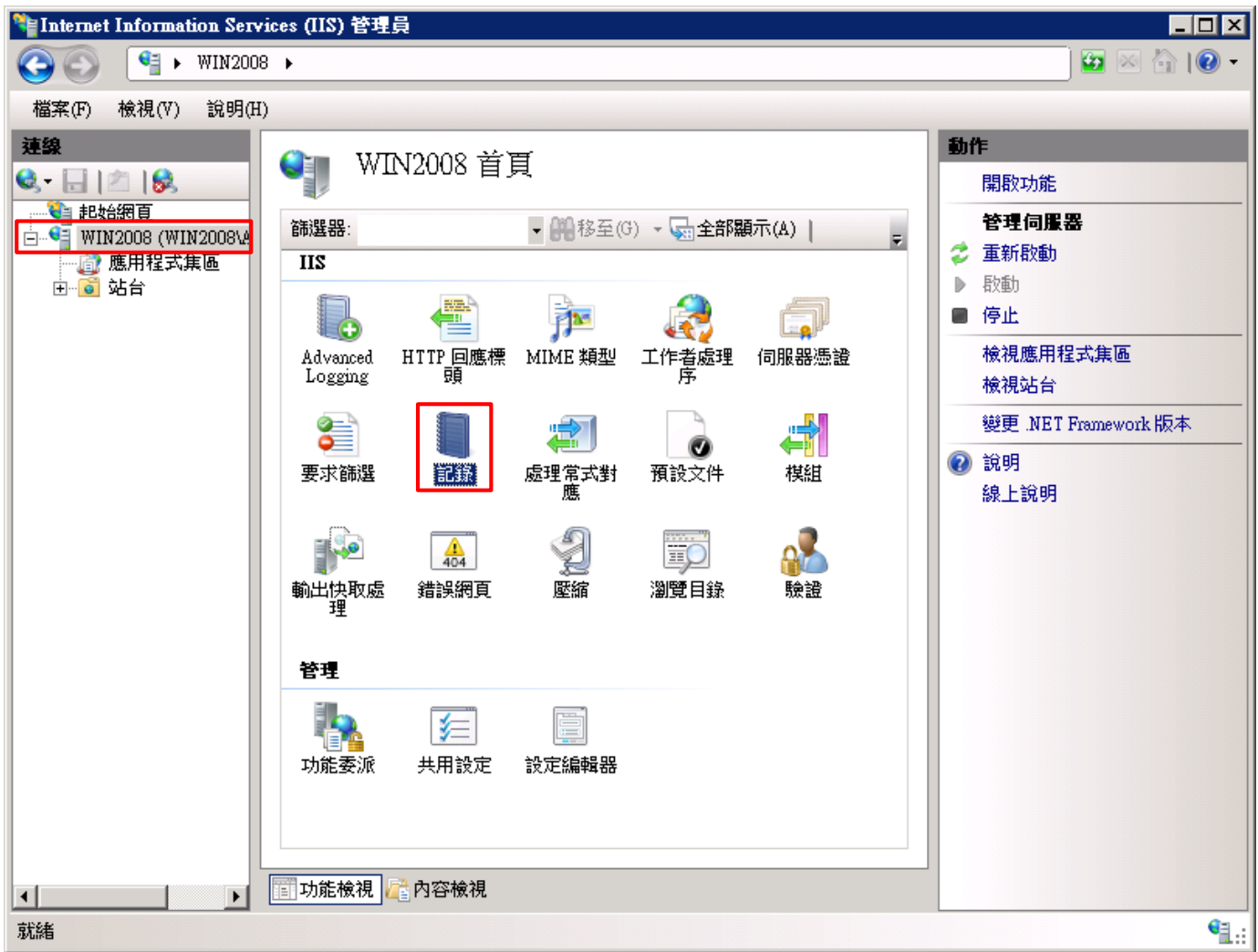
點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]



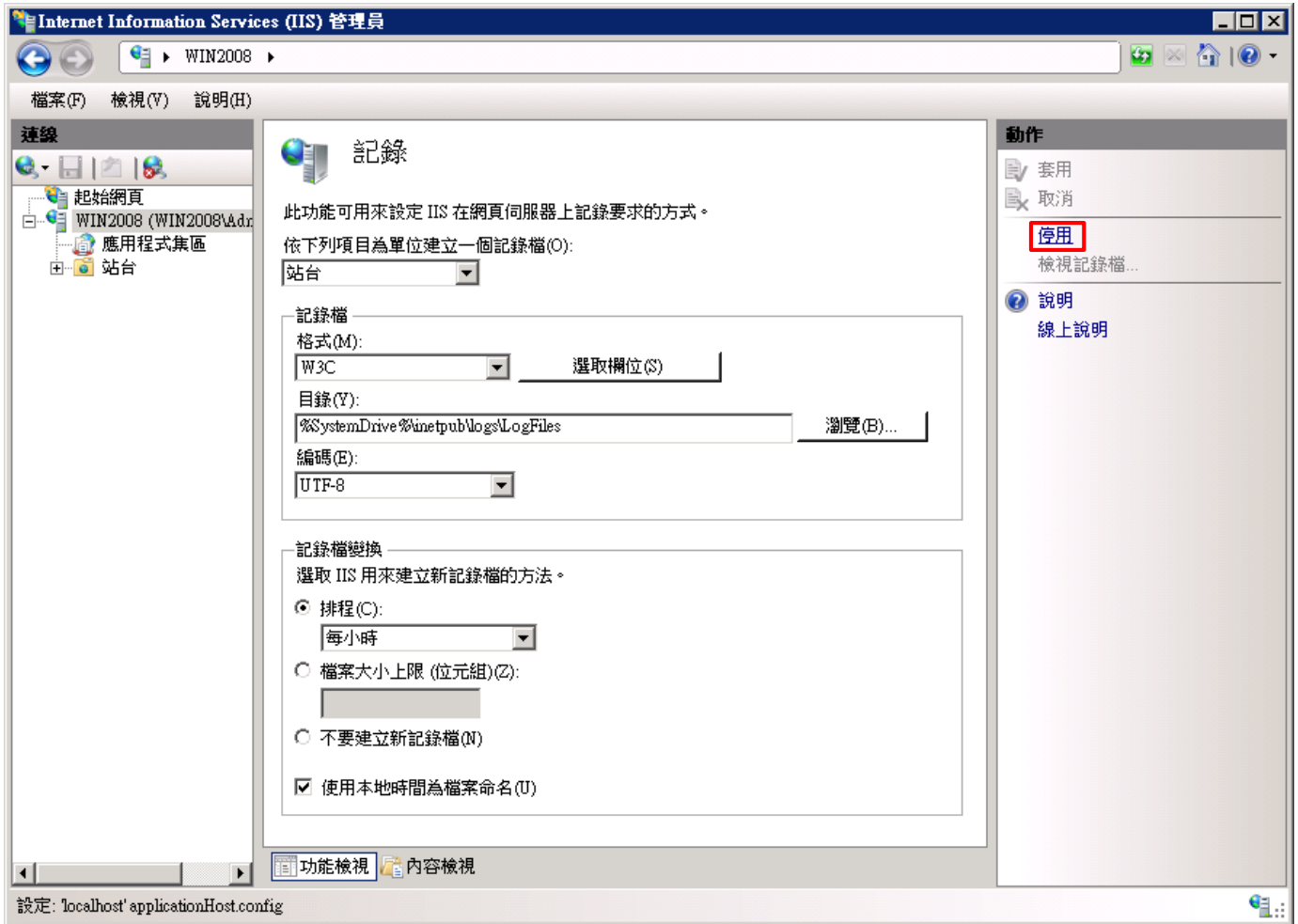
(2) 開啟 [Internet Information Services (IIS) 管理員]



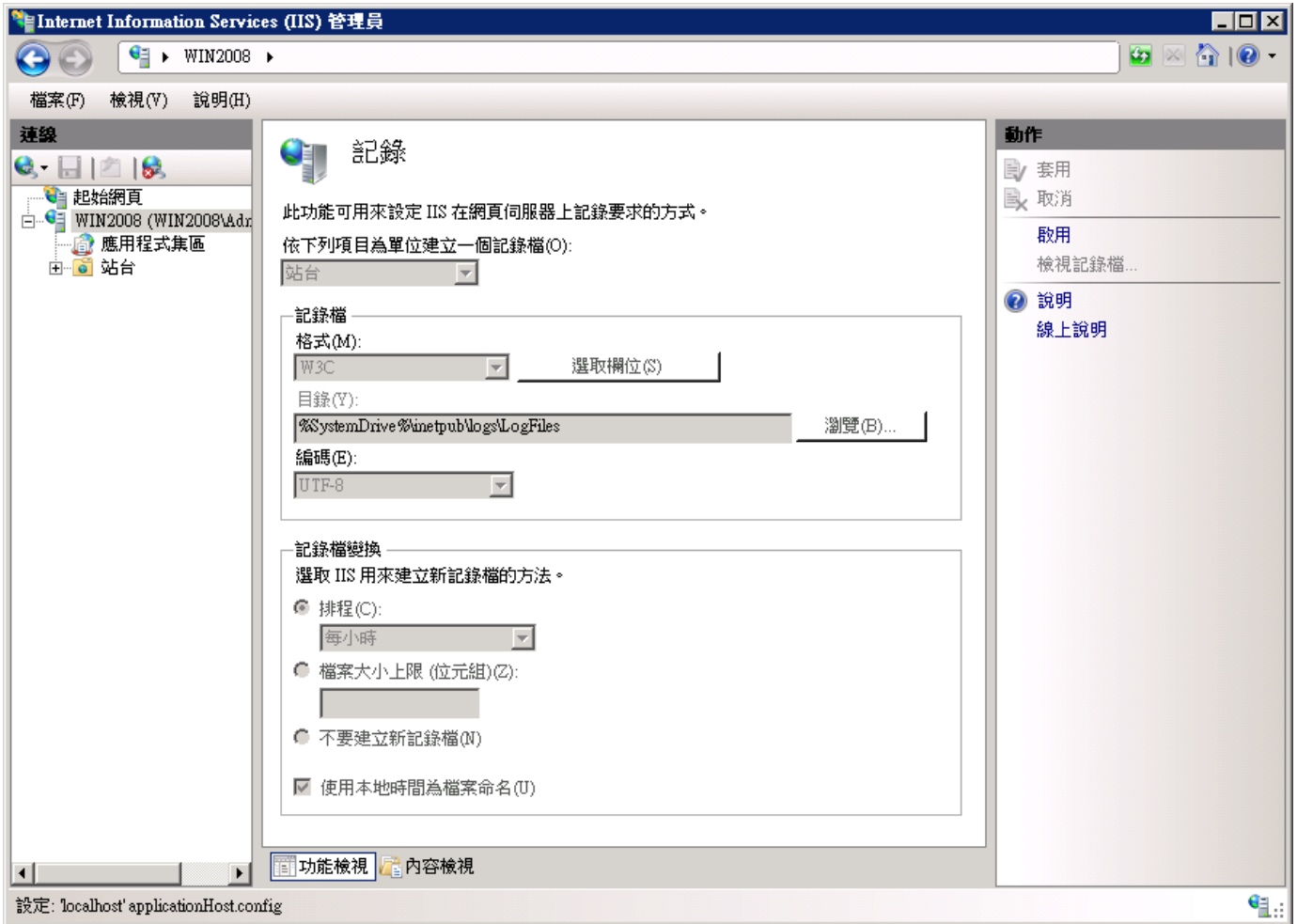
(3) 選擇 [IIS Server] -> 點選 [Logging(記錄)]



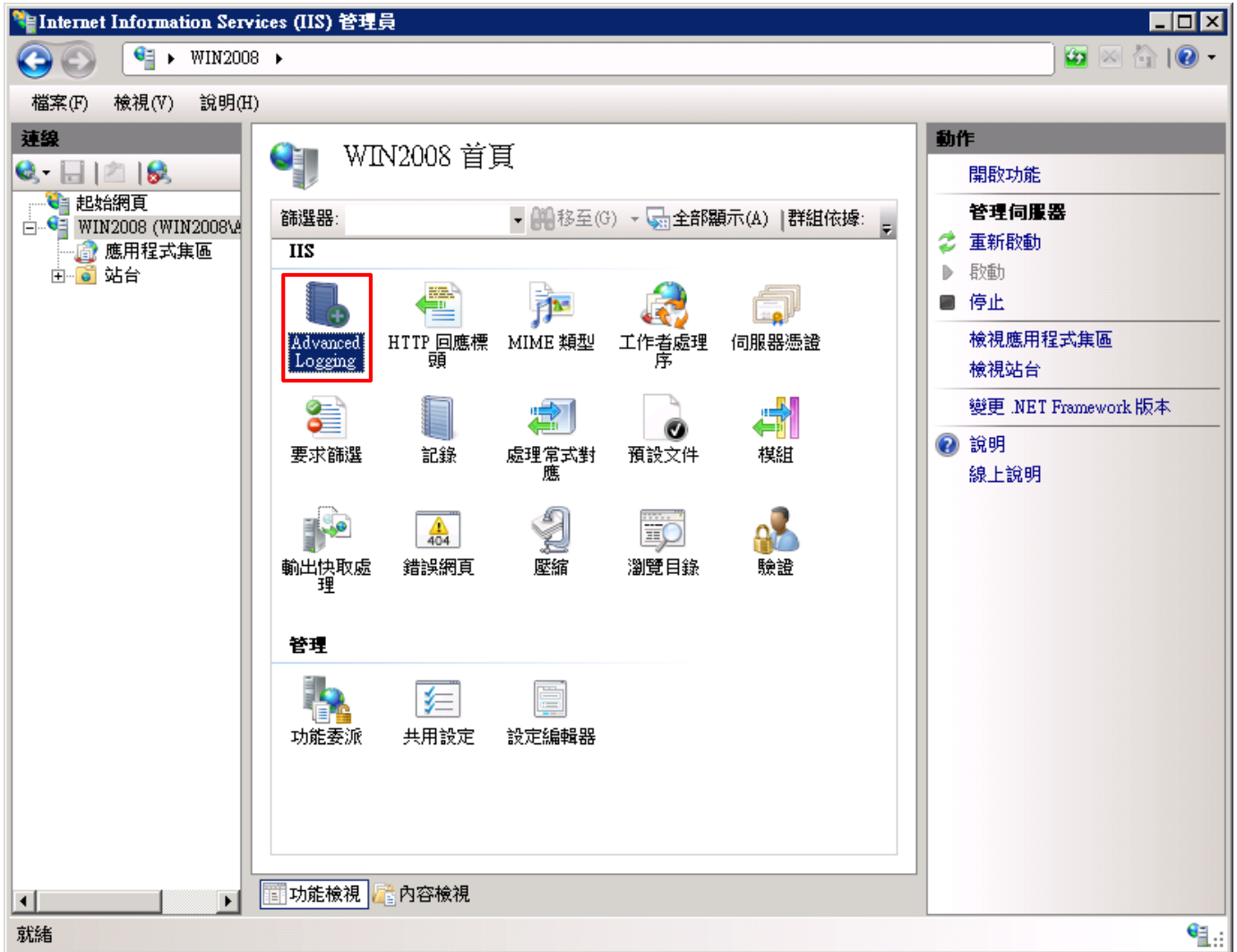
(4) 點選 [停用]



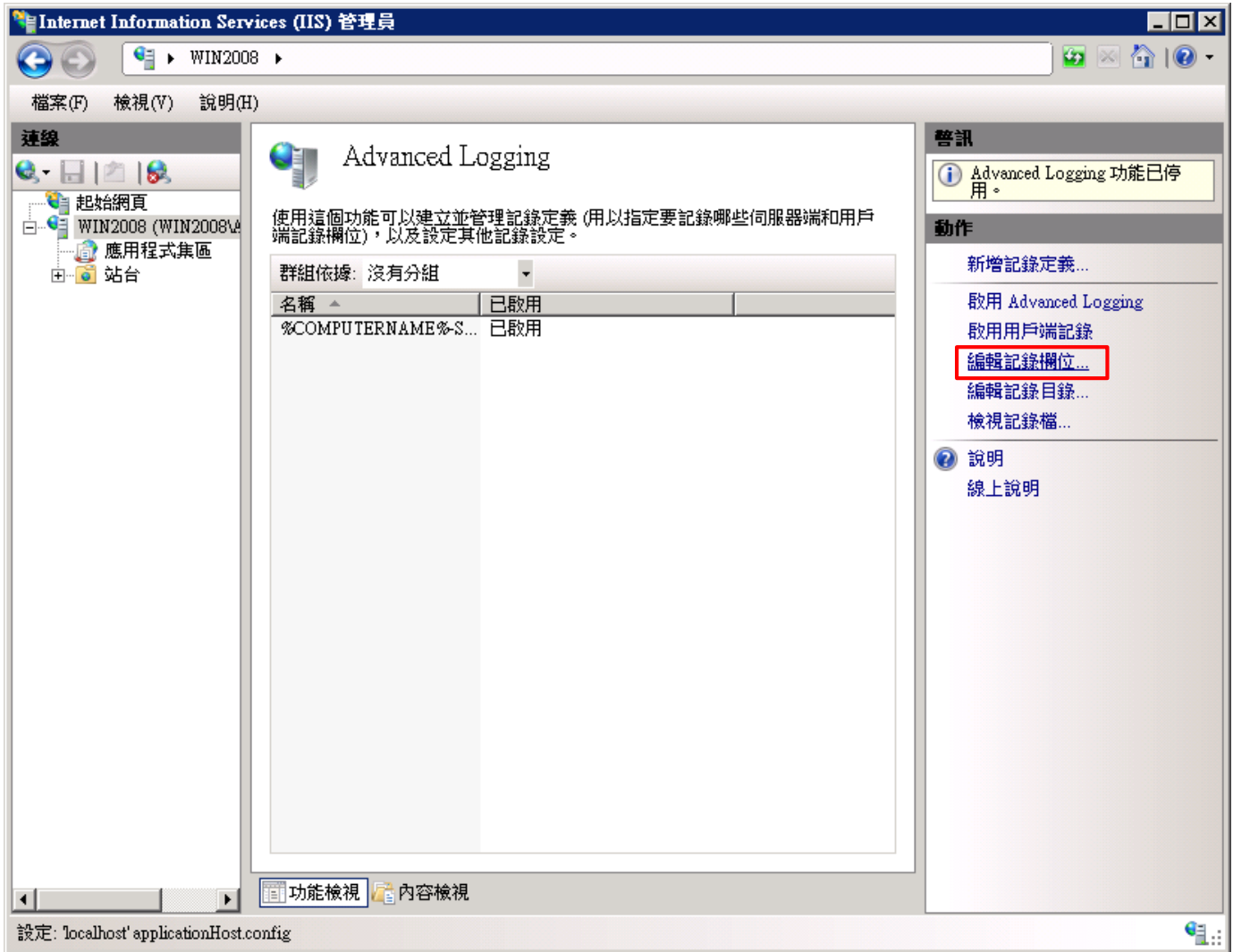
(5) 確認記錄已停用



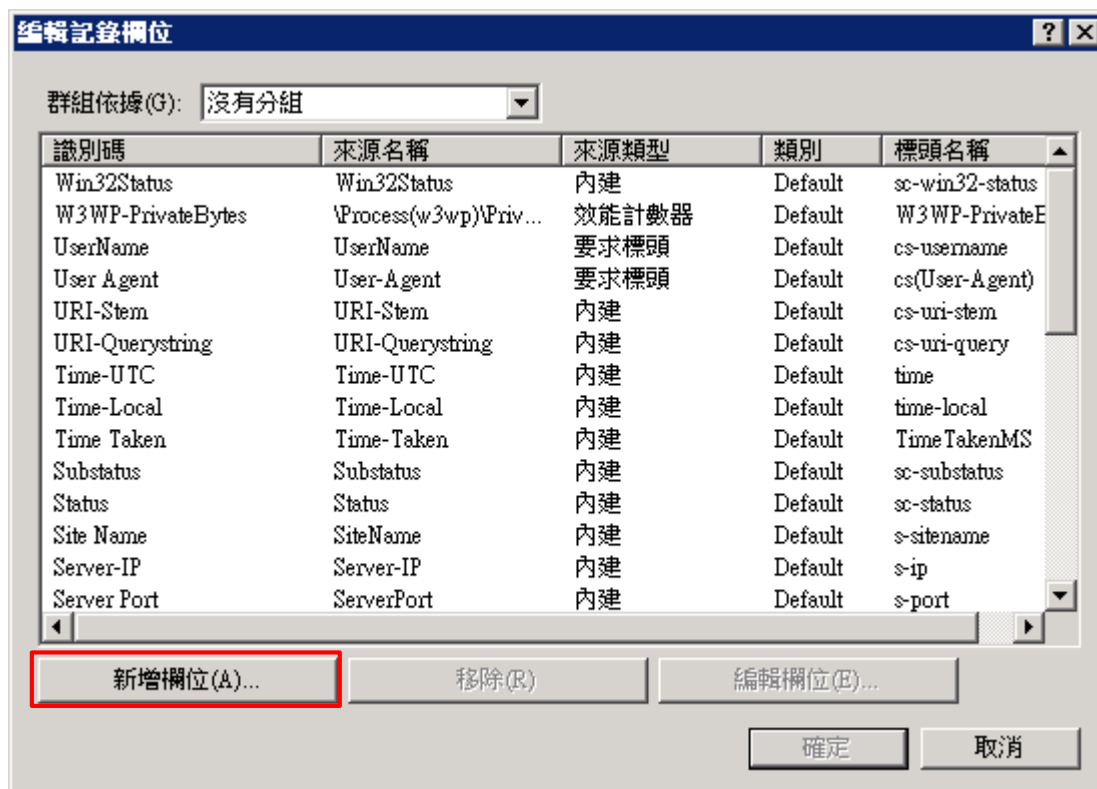
(6) 點選 [Advanced Logging]



(7) 按下 [編輯記錄欄位]



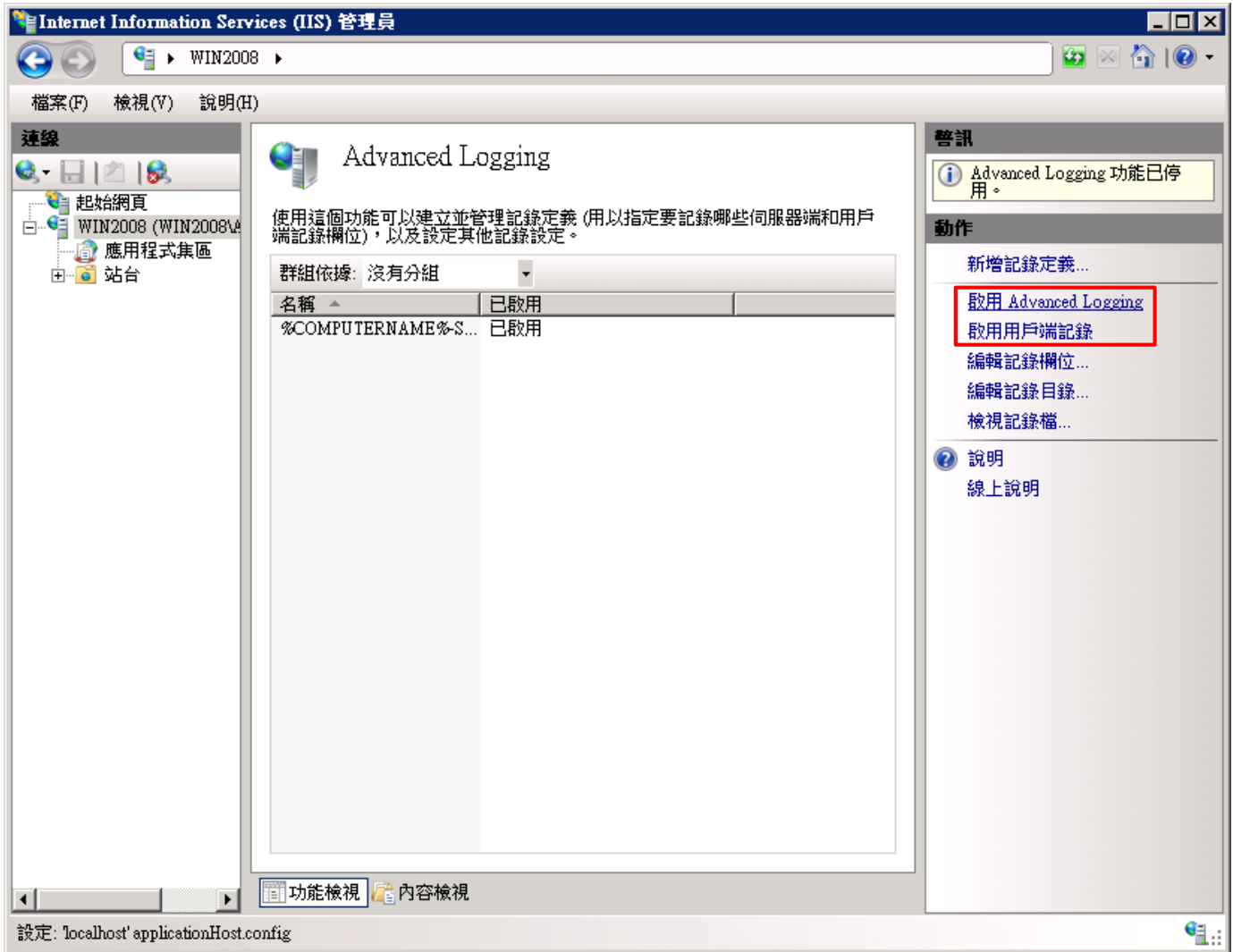
(8) 按下 [新增欄位]



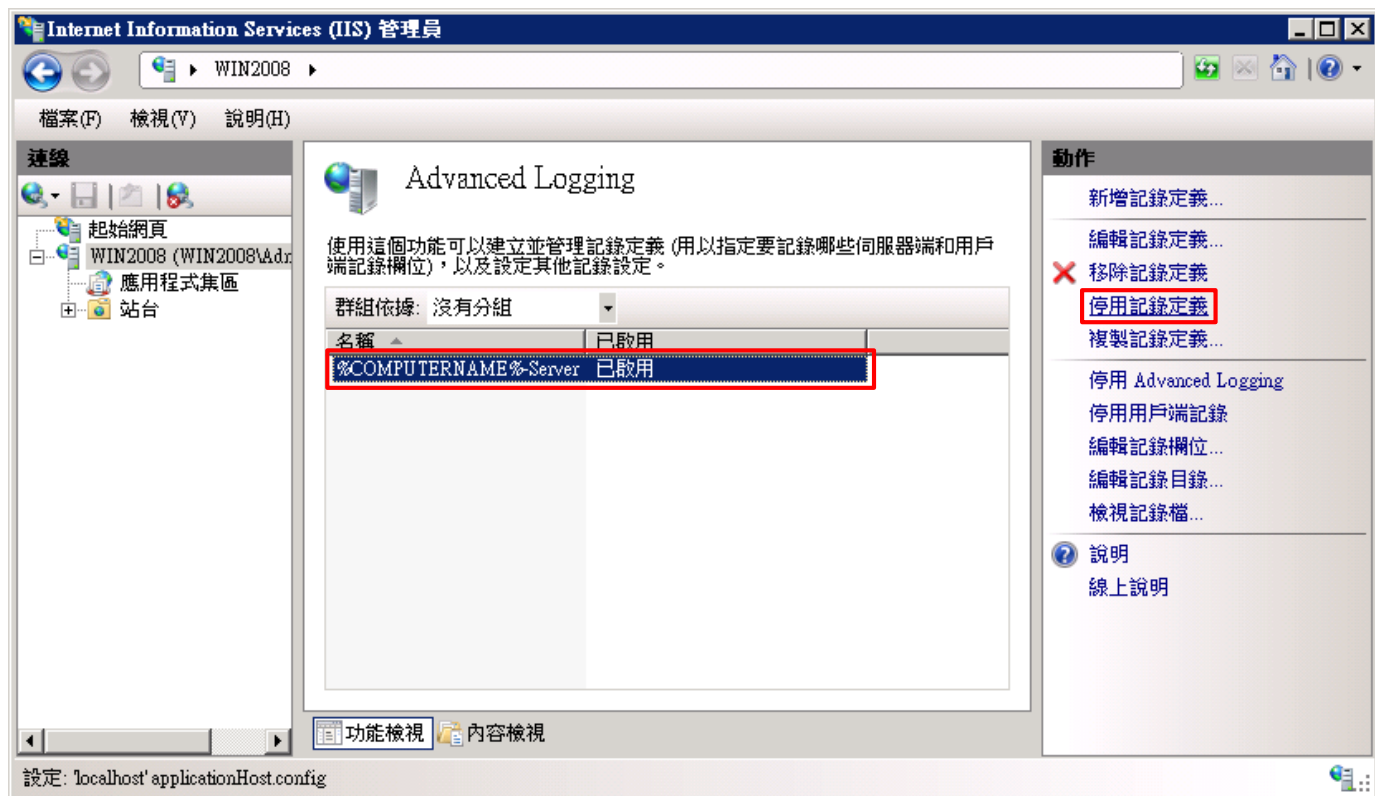
(9) 輸入欄位識別碼: X-Forwarded-For -> 選擇類別: [Default] -> 來源類型: [Request Header(要求標頭)] -> 輸入來源名稱: X-Forwarded-For -> 按下 [確定]



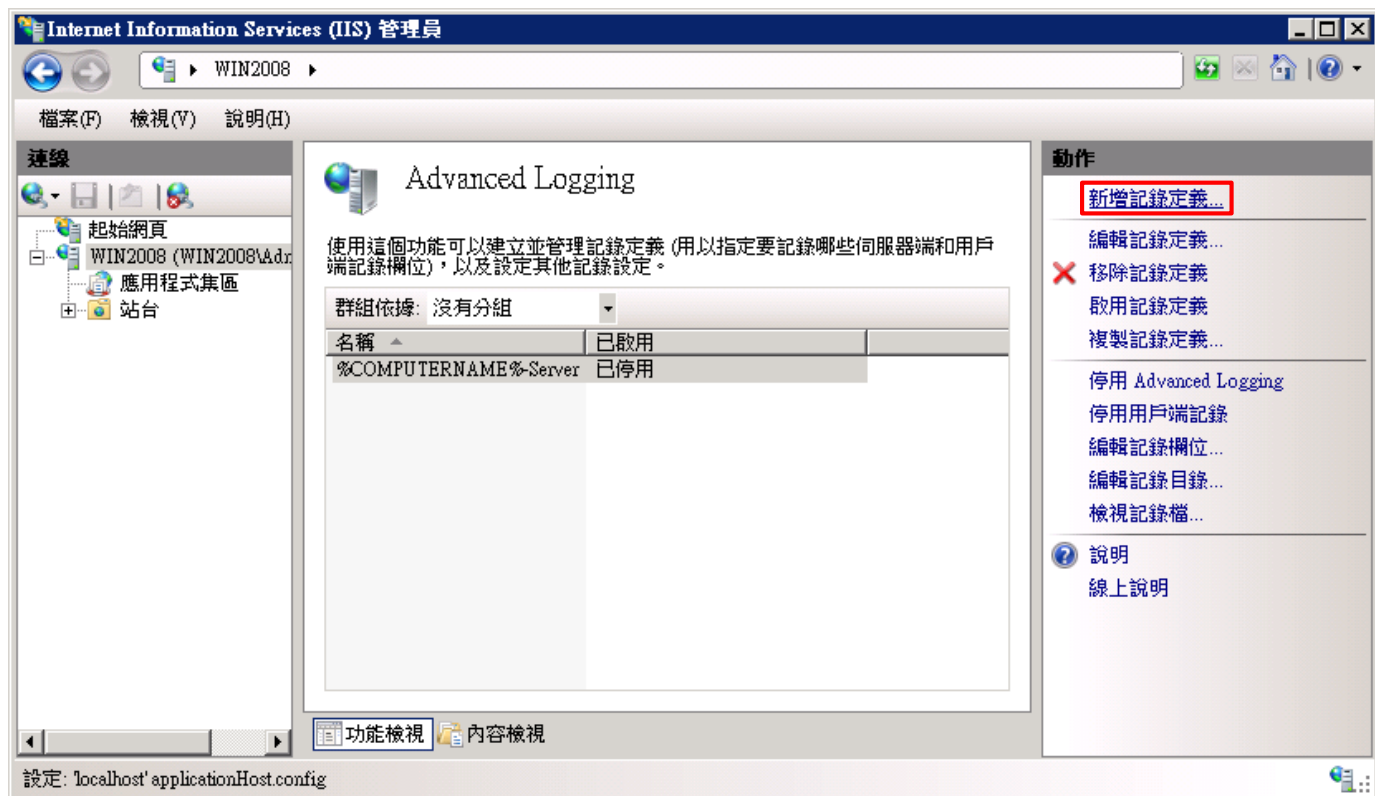
(10) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]



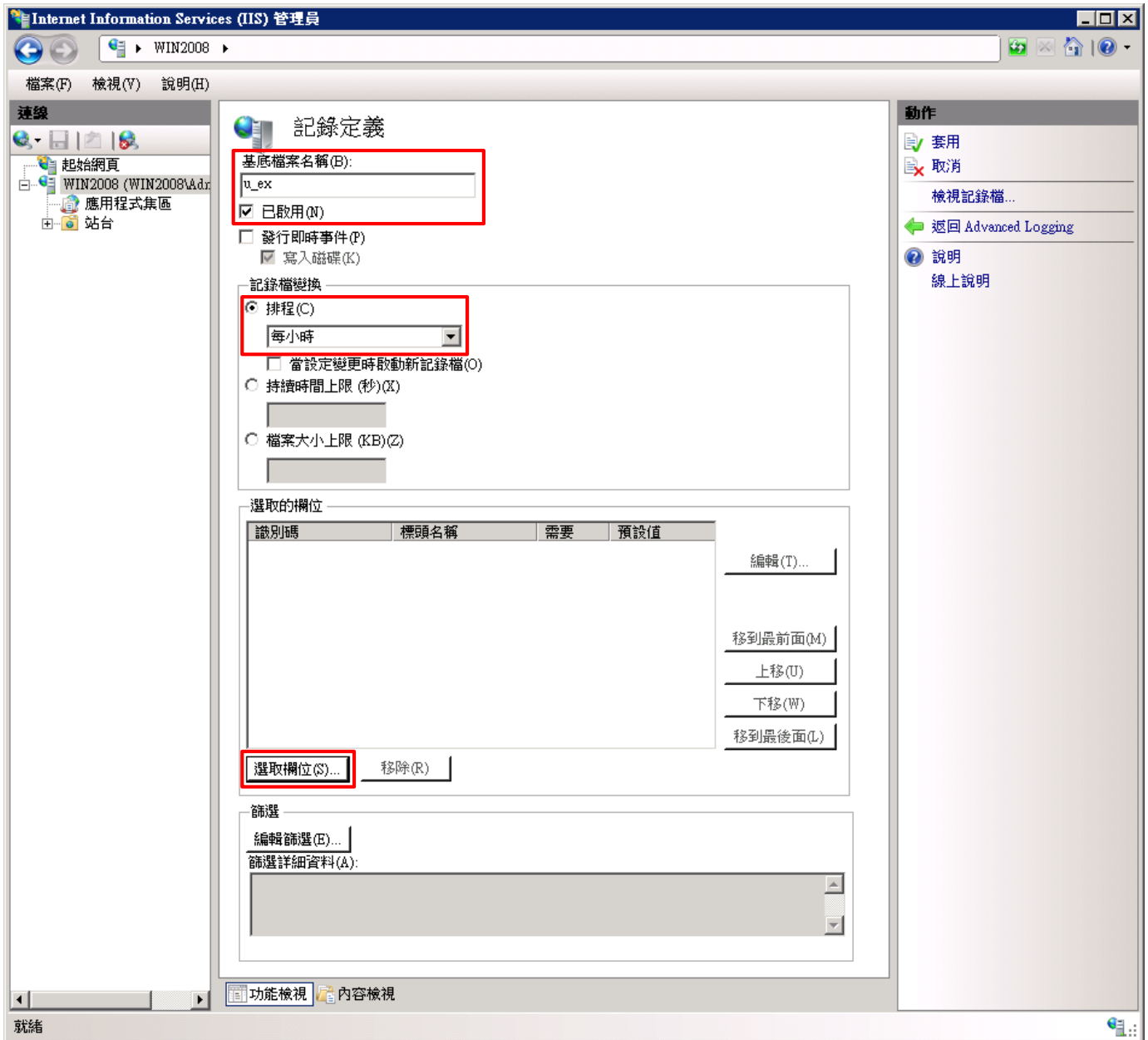
(11) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]



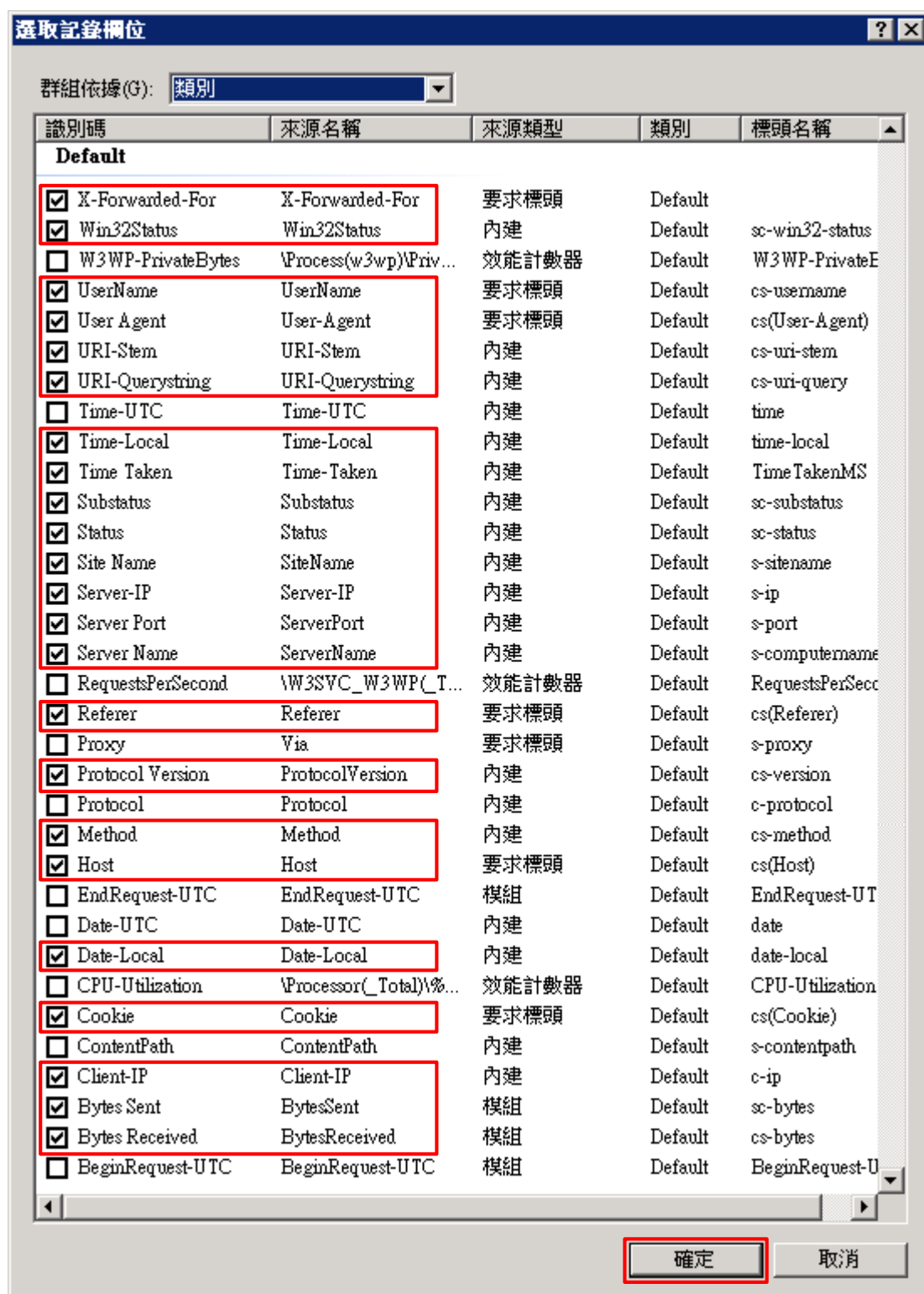
(11) 點選 [新增記錄定義]



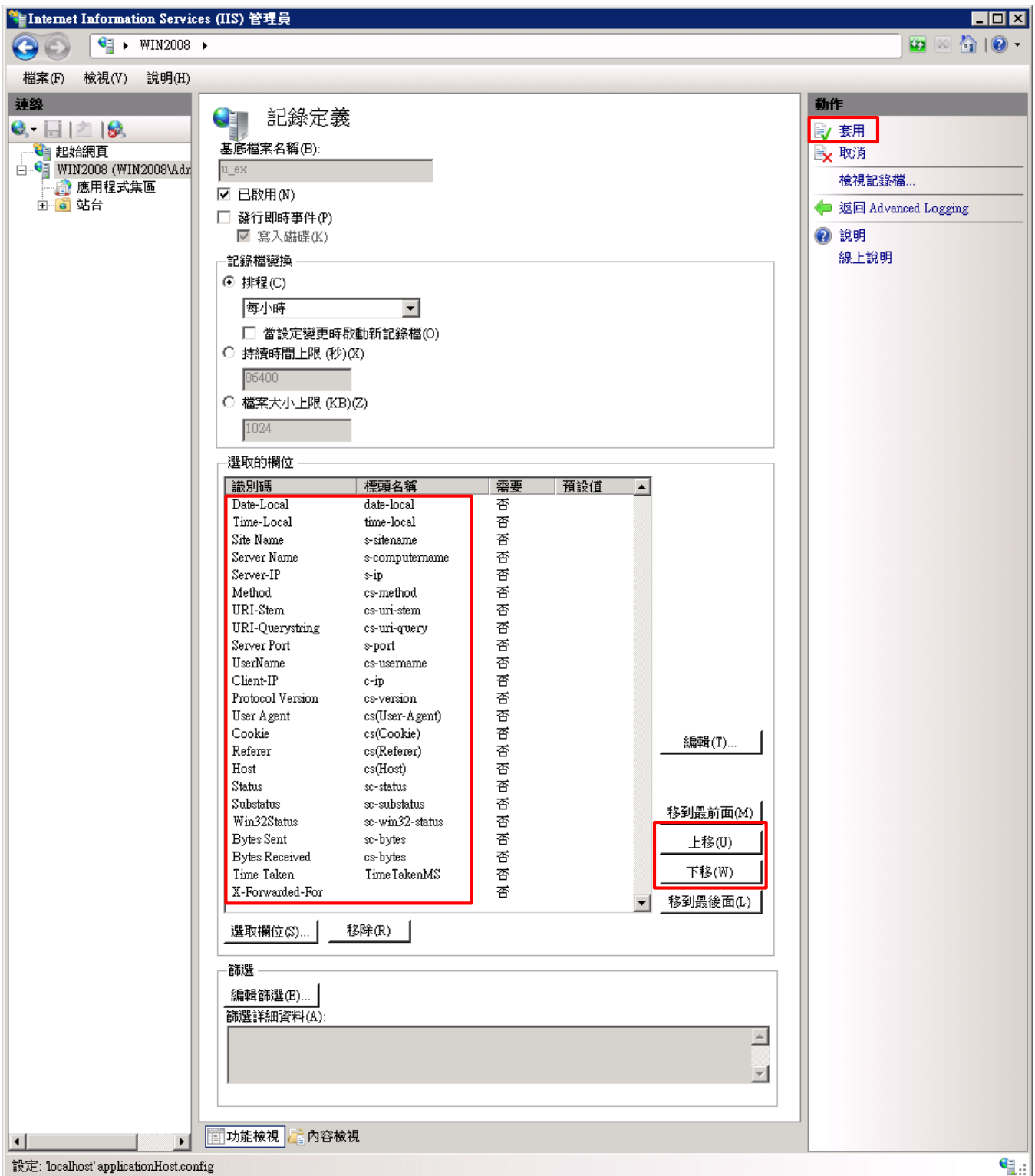
(12) 輸入基底檔案名稱: u_ex -> 勾選 [已啟用] -> 選擇排程 [每小時] -> 按下 [選取欄位]



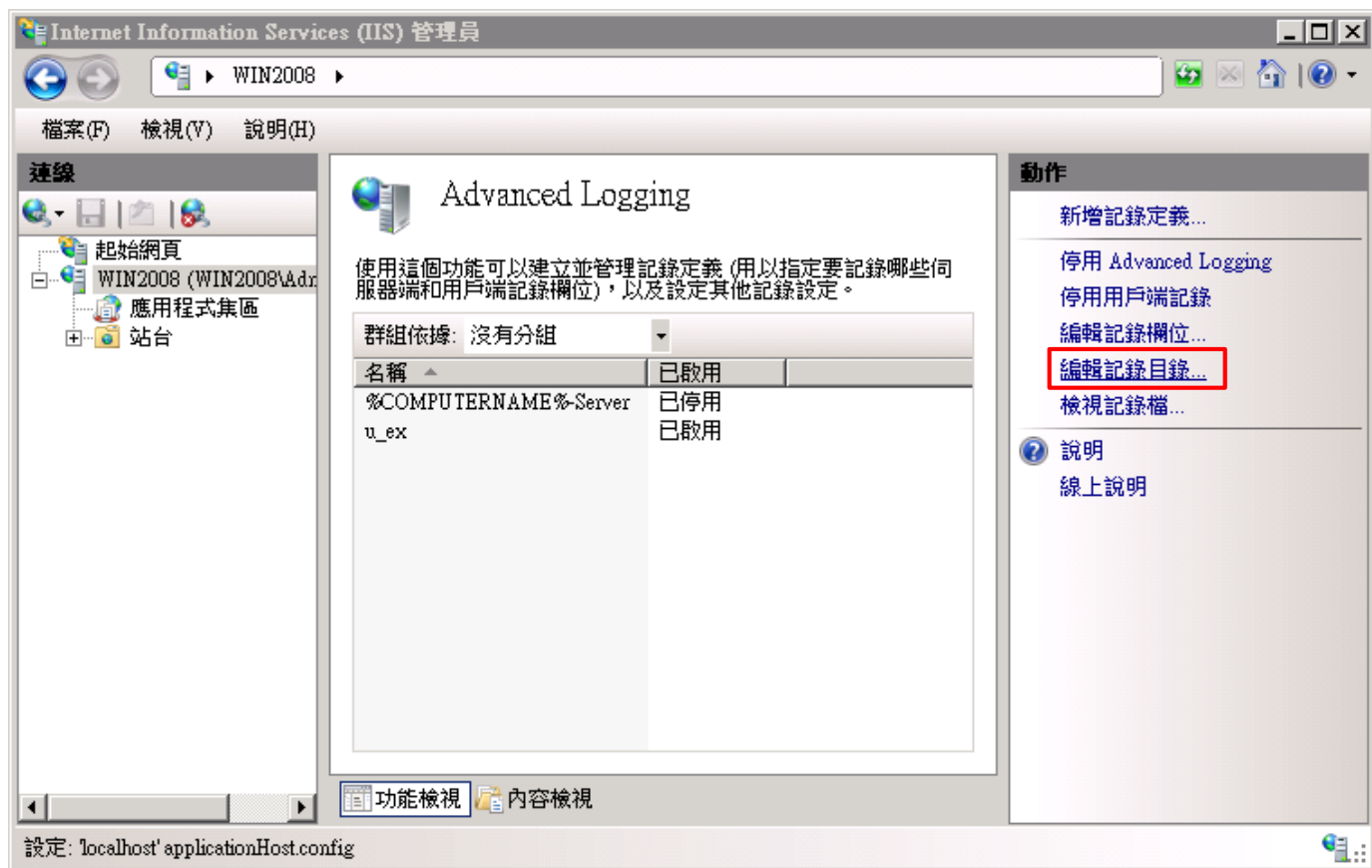
(13) 勾選 [X-Forwarded-For]、[Win32Status(sc-win32-status)]、[UserName(cs-username)]、[User Agent(cs(User-Agent))]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Time-Local(time-local)]、[Time Taken(TimeTakenMS)]、[Substatus(sc-substatus)]、[Status(sc-status)]、[Site Name(s-sitename)]、[Server-IP(s-ip)]、[Server 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)] -> 按下 [確定]



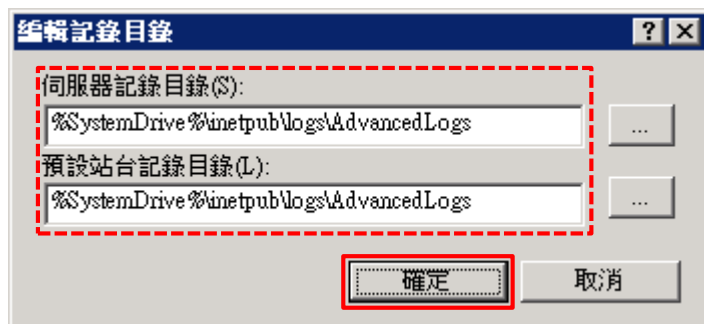
(14) 調整選取的欄位: [Data-Local(date-local)]、[Time-Local(time-local)]、[Site Name(s-sitename)]、[Server Name(s-computername)]、[Server-IP(s-ip)]、[Method(cs-method)]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Server Port(s-port)]、[UserName(cs-username)]、[Client-IP(c-ip)]、[Protocol Version(cs-version)]、[User 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] -> 按下 [套用]



(15) 點選 [編輯記錄目錄]



(16) 確認伺服器記錄目錄和預設站台記錄目錄 -> 按下 [確定]



(17) 修改 nxlog.conf

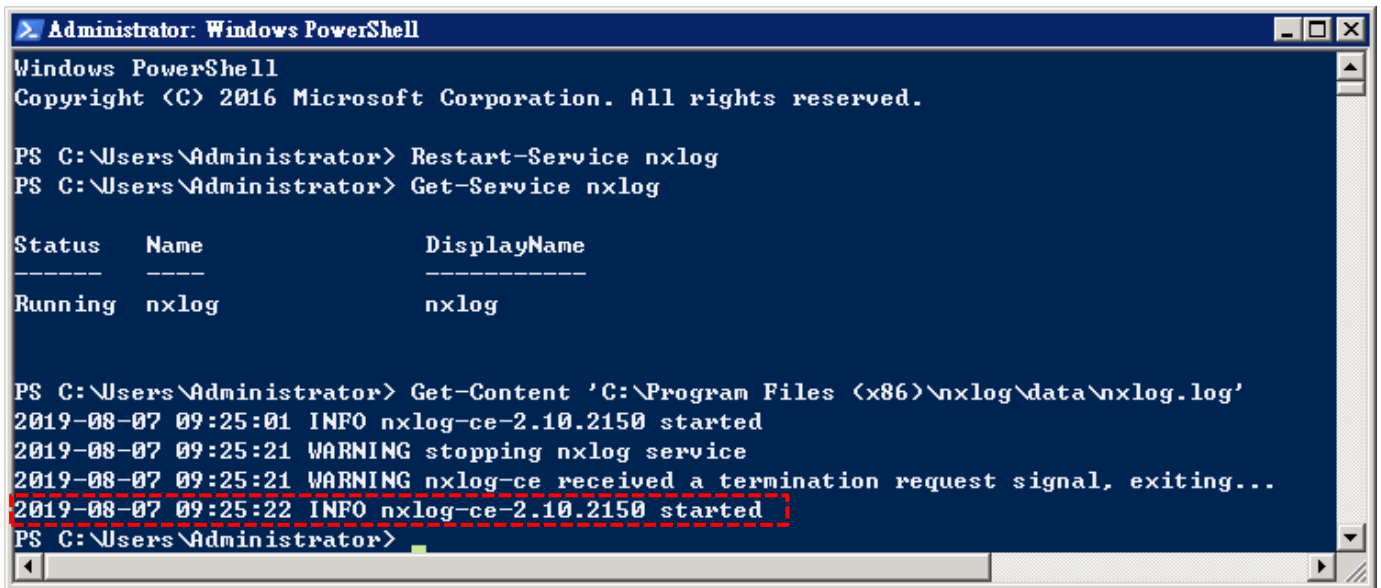
註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入 Microsoft IIS 記錄檔資料夾路徑

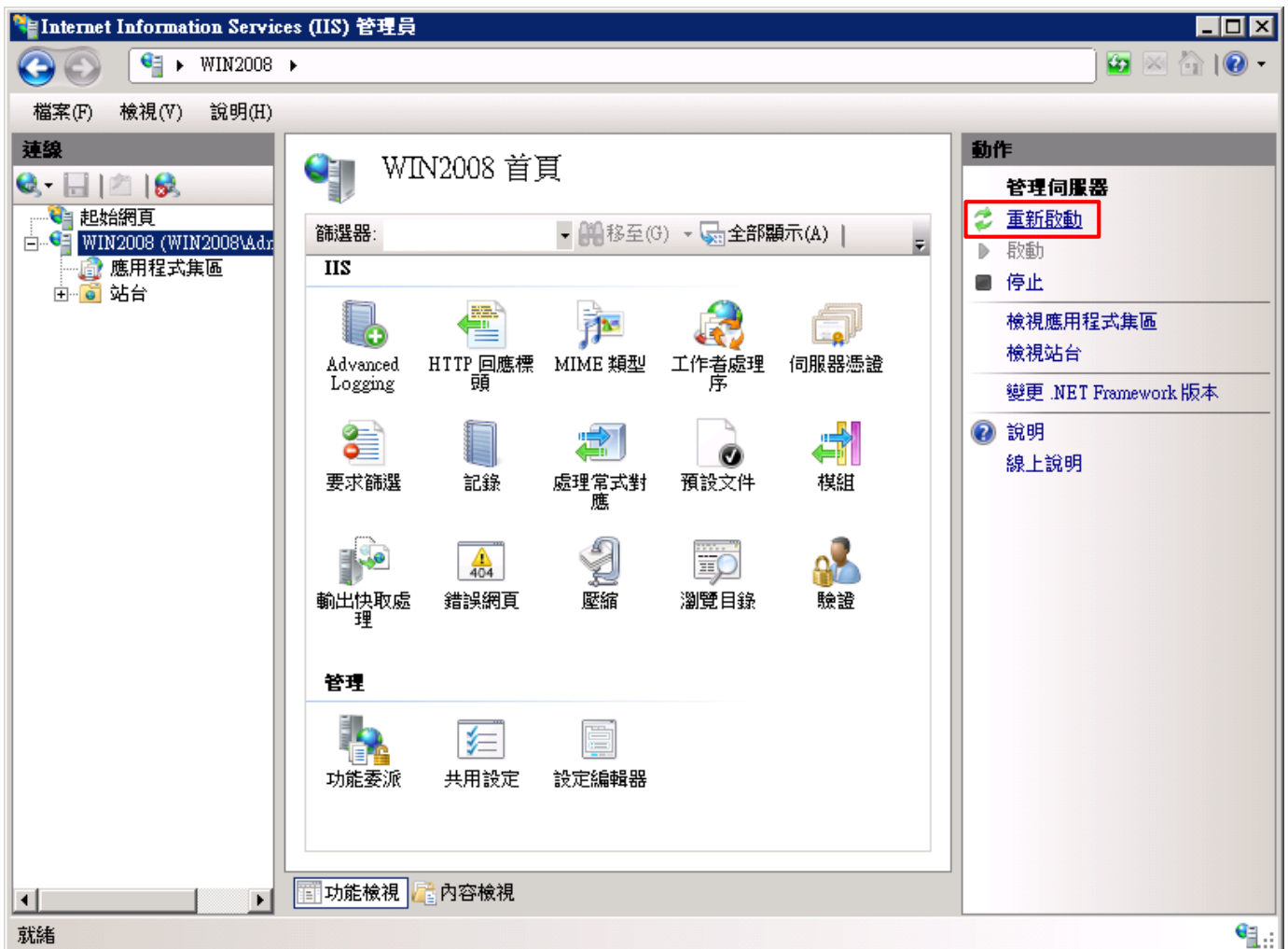
```
define BASEDIR C:\inetpub\logs\AdvancedLogs
```


(18) 重啟 nxlog 服務

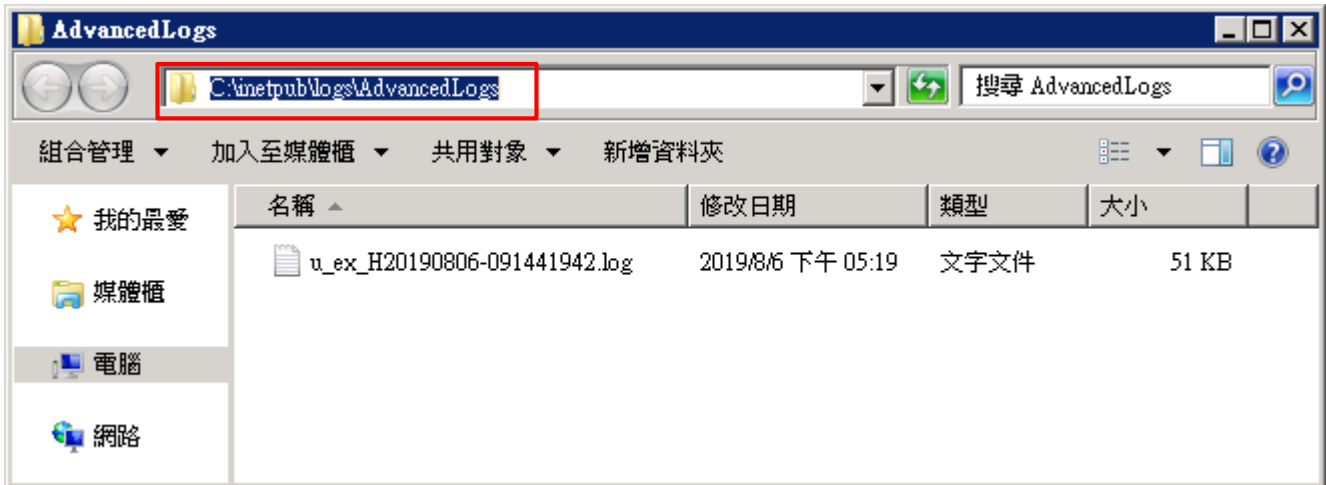
開啟 [Windows PowerShell] -> 輸入 `Restart-Service nxlog` 重新啟動 nxlog 服務和 `Get-Service nxlog` 查看 nxlog 服務狀態 -> `Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息



(19) 點選 [重新啟動] IIS 服務



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



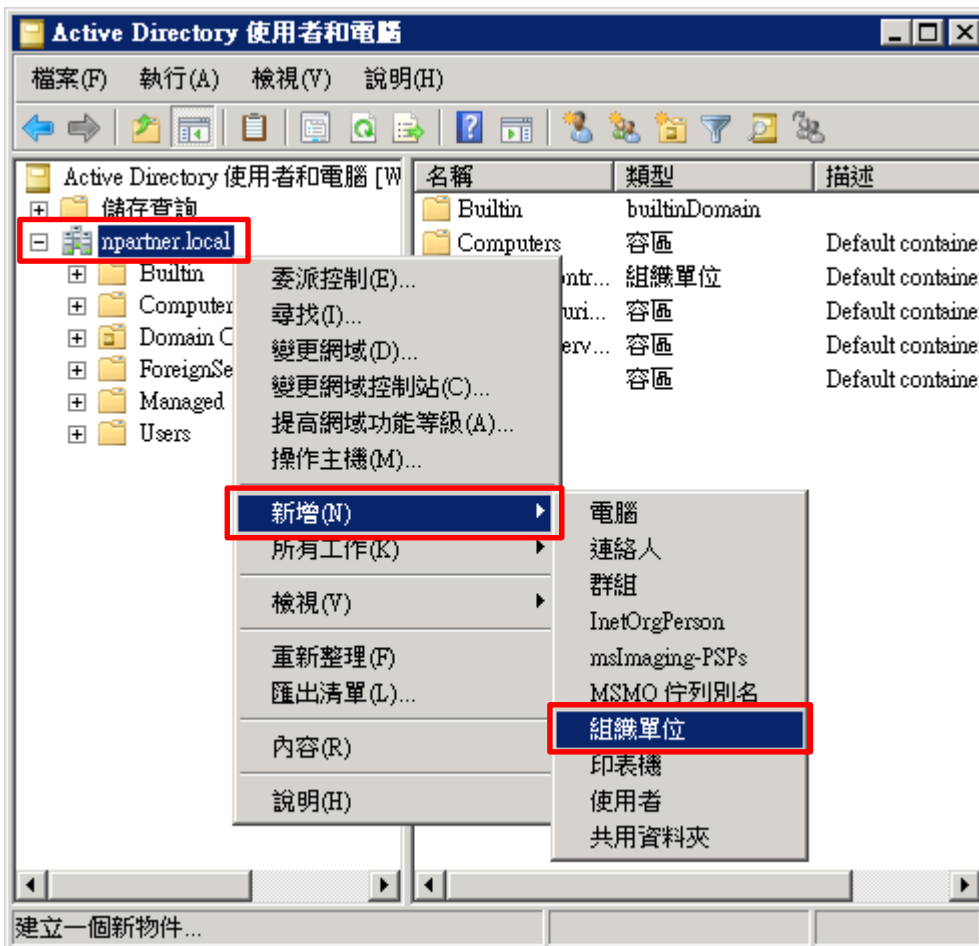
3.3 Event log

3.3.1 組織單位(Organizational Unit)

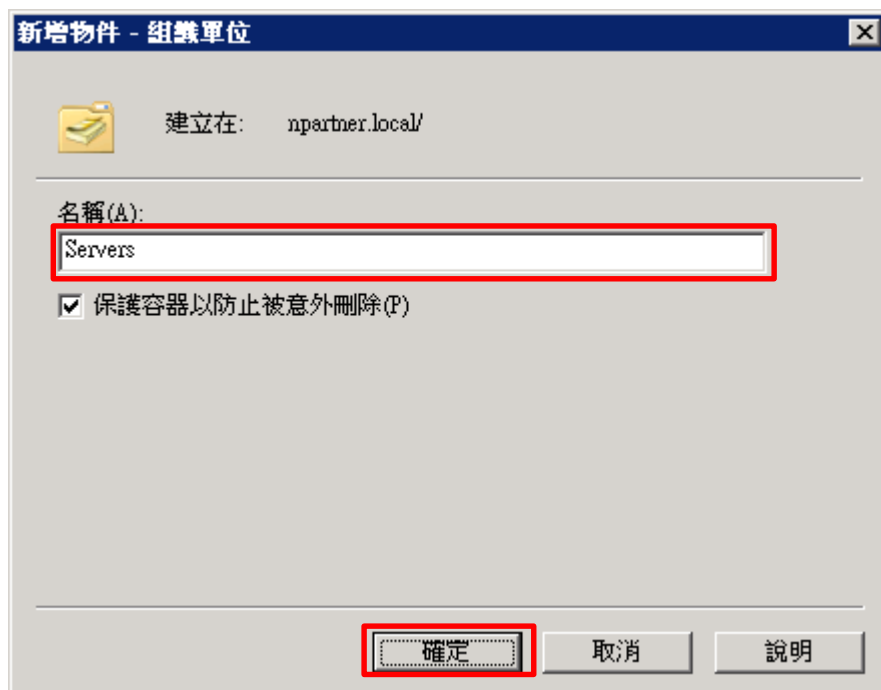
(1) 開啟 [Active Directory 使用者和電腦]



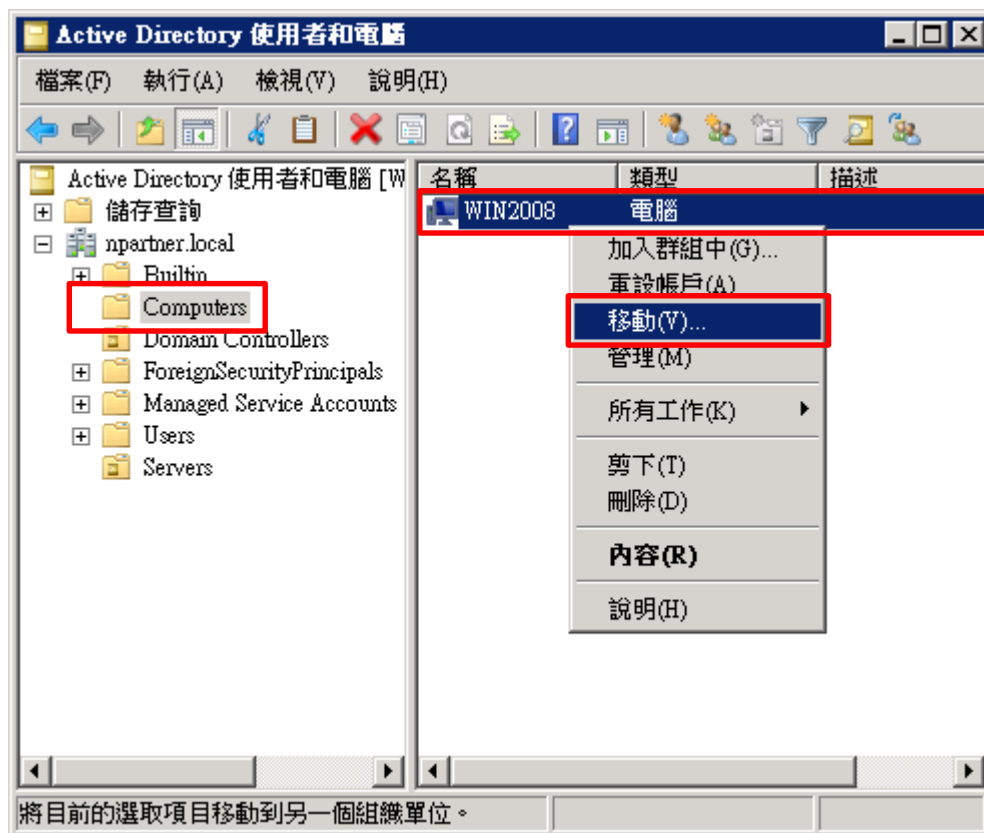
(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱: Servers -> 按下 [確定]



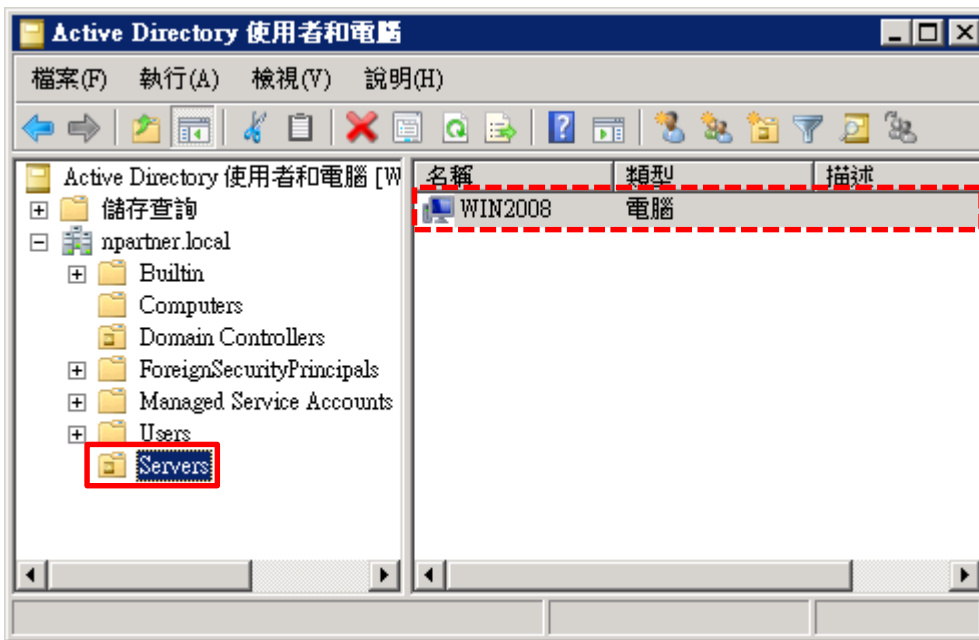
(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Win2008)] 上按滑鼠右鍵 -> 點選 [移動]



(5) 點選 [Servers] 組織單位 -> 按下 [OK]



(6) 點選 [Servers] 組織單位，確認 Exchange Server(Win2008) 伺服器已移動

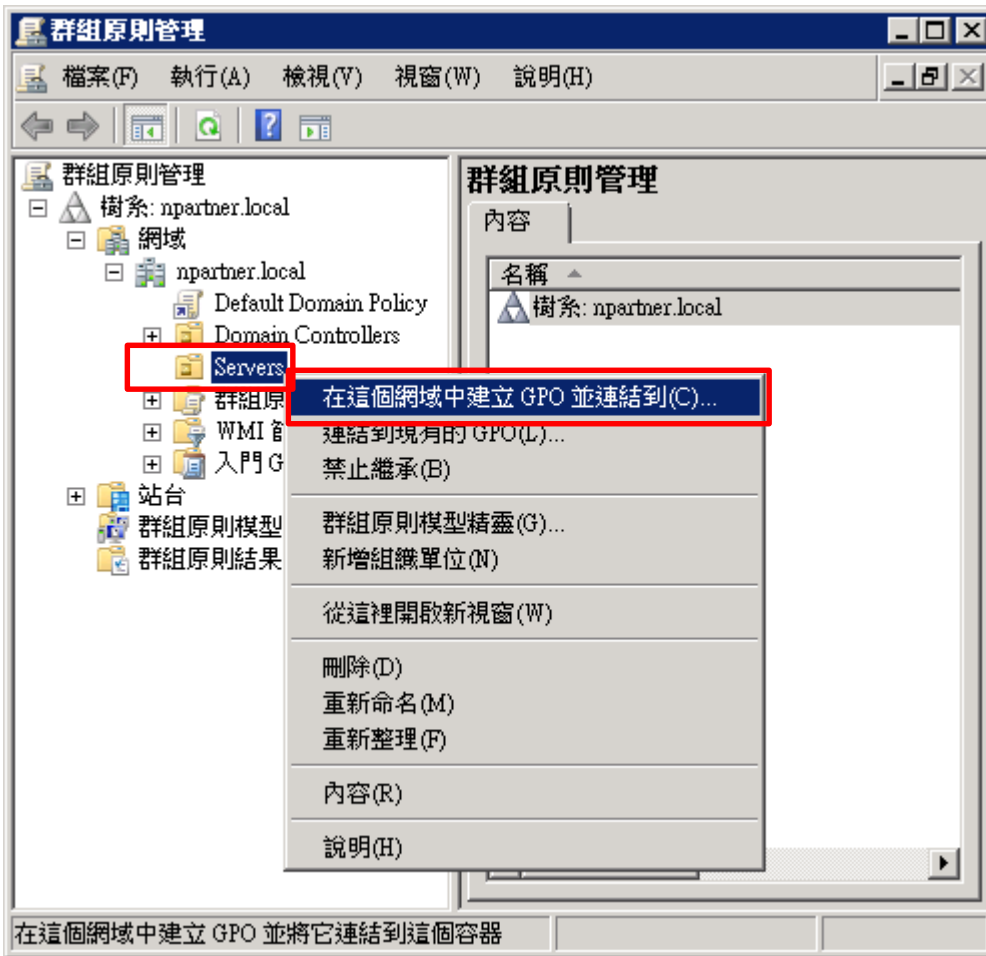


3.3.2 群組原則(Group Policy Management)

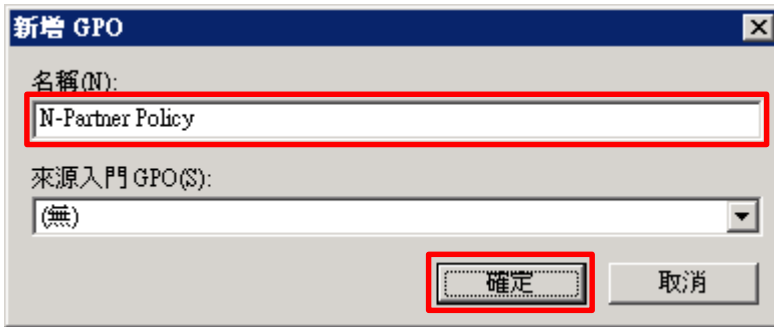
(1) 開啟 [群組原則管理]



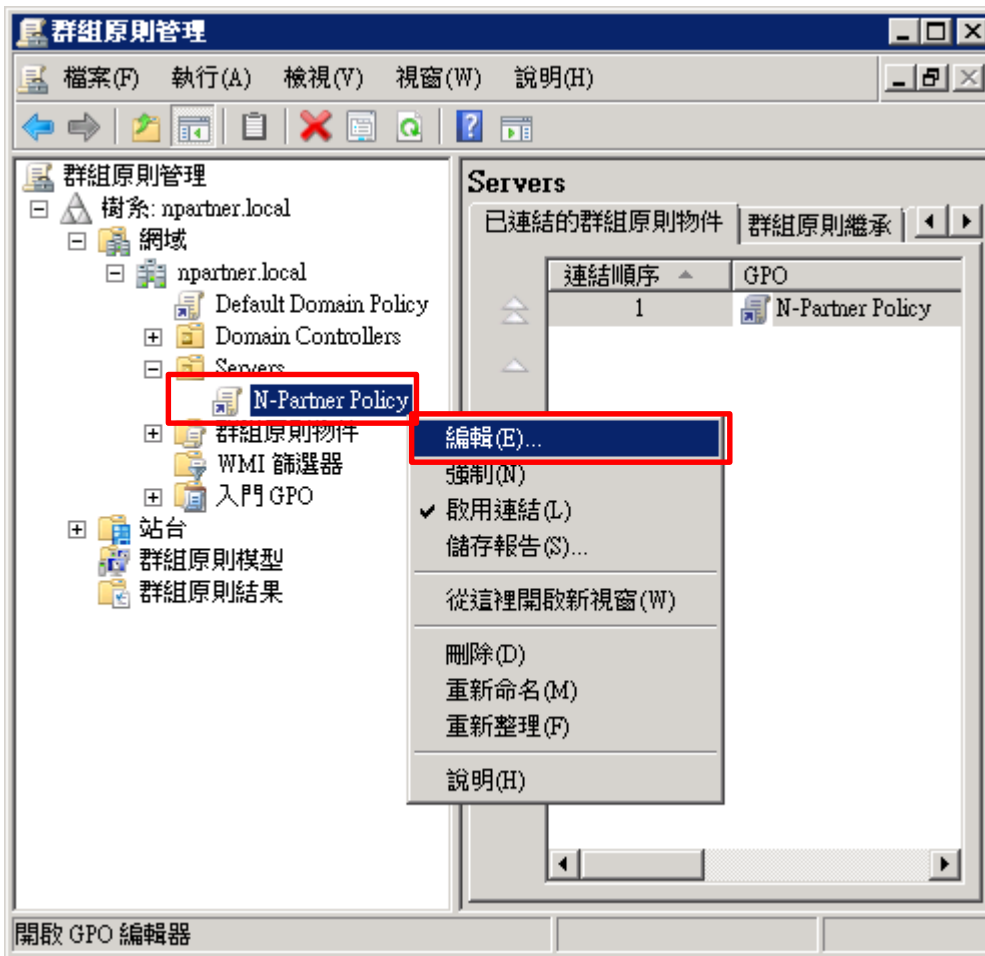
(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到]



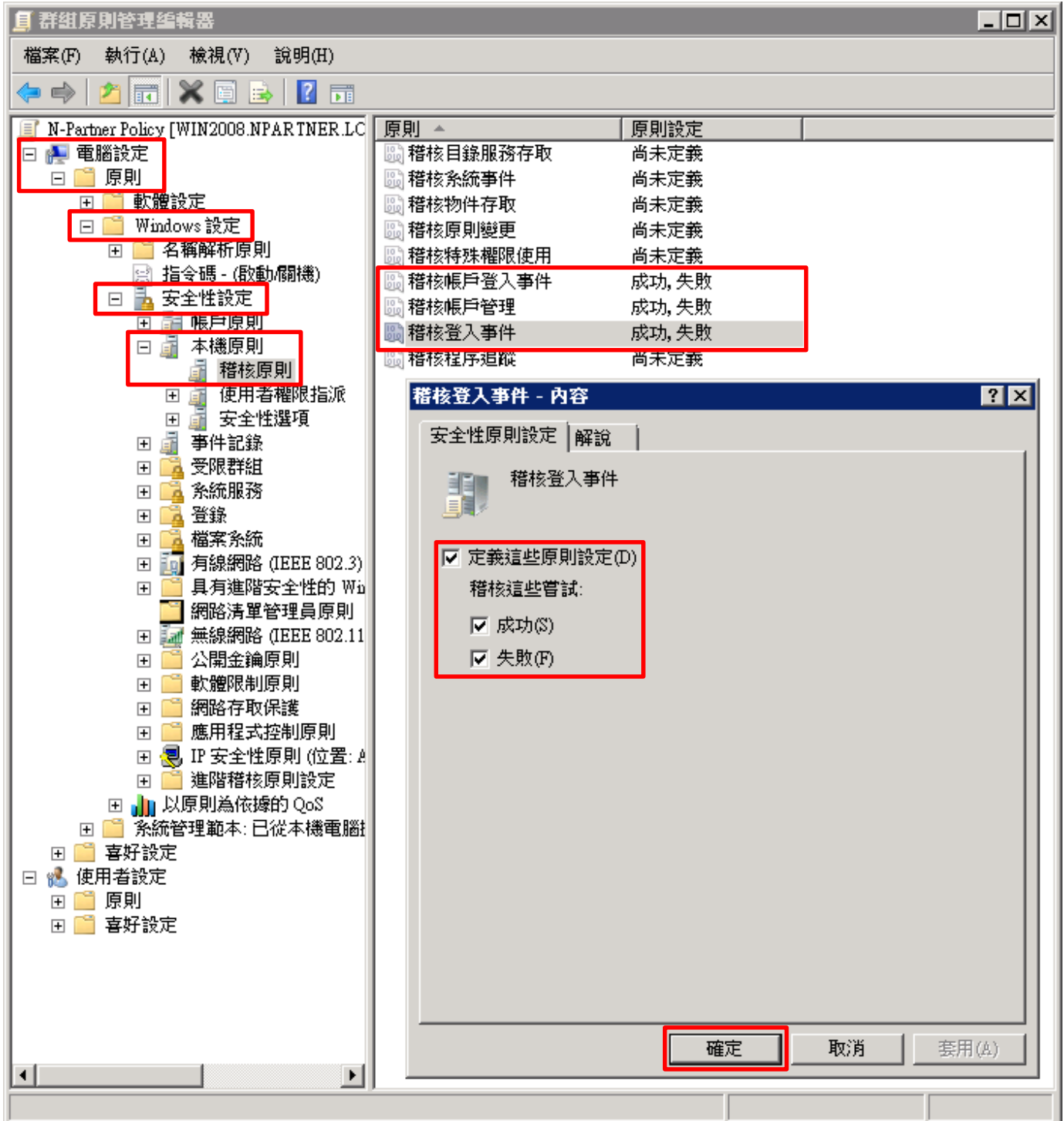
(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]



(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]



(5) 選擇 [Computer Configuration(電腦設定)] -> [Policies(原則)] -> [Windows Settings(Windows 設定)] -> [Security Settings(安全性設定)] -> [Local Policies(本機原則)] -> [Audit Policy(稽核原則)] -> 點選 [Audit account logon events(稽核帳戶登入事件)], [Audit account management(稽核帳戶管理)], [Audit logon events(稽核登入事件)] 項目 -> 勾選 [Define these policy settings(定義這些原則設定)]: & [Success(成功)] & [Failure(失敗)] -> 按下 [OK (確定)]



(6) 在 Exchange Server 伺服器更新群組原則

PS C:\> gpupdate /force



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

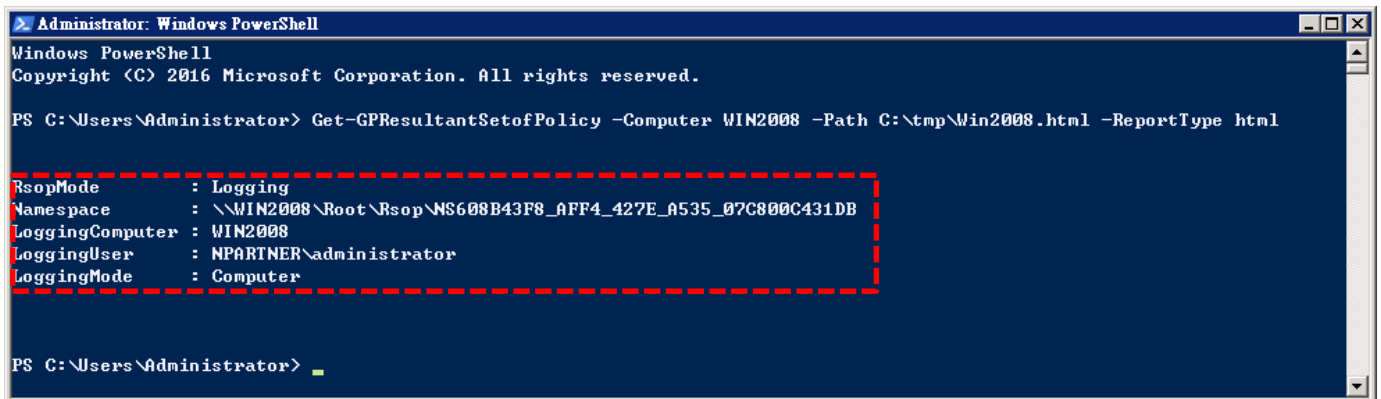
PS C:\Users\Administrator> gpupdate /force
正在更新原則...

使用者原則更新已成功完成。
電腦原則更新已成功完成。

PS C:\Users\Administrator> _
```

(7) 在 AD 網域伺服器，產生 Exchange Server 伺服器群組原則報告。參數: -Computer 為產生報告的電腦名稱，-Path 指定報告文件的路徑和檔名。

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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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

RsopMode       : Logging
Namespace      : \\WIN2008\Root\Rsop\NS608B43F8_AFF4_427E_A535_07C800C431DB
LoggingComputer : WIN2008
LoggingUser    : NPARTNER\administrator
LoggingMode    : Computer

PS C:\Users\Administrator> _
```

(8) 開啟 [C:\tmp\Win2012.html] 報表，確認套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WIN2008
資料收集: 2019/9/17 下午 01:43:42

摘要 [顯示全部](#)

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
帳戶原則/Kerberos 原則		顯示
本機原則/稽核原則		隱藏
原則	設定	優勢 GPO
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
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 [隱藏](#)

沒有可用的資料。

電腦 | 受保護模式: 關閉 | 100%

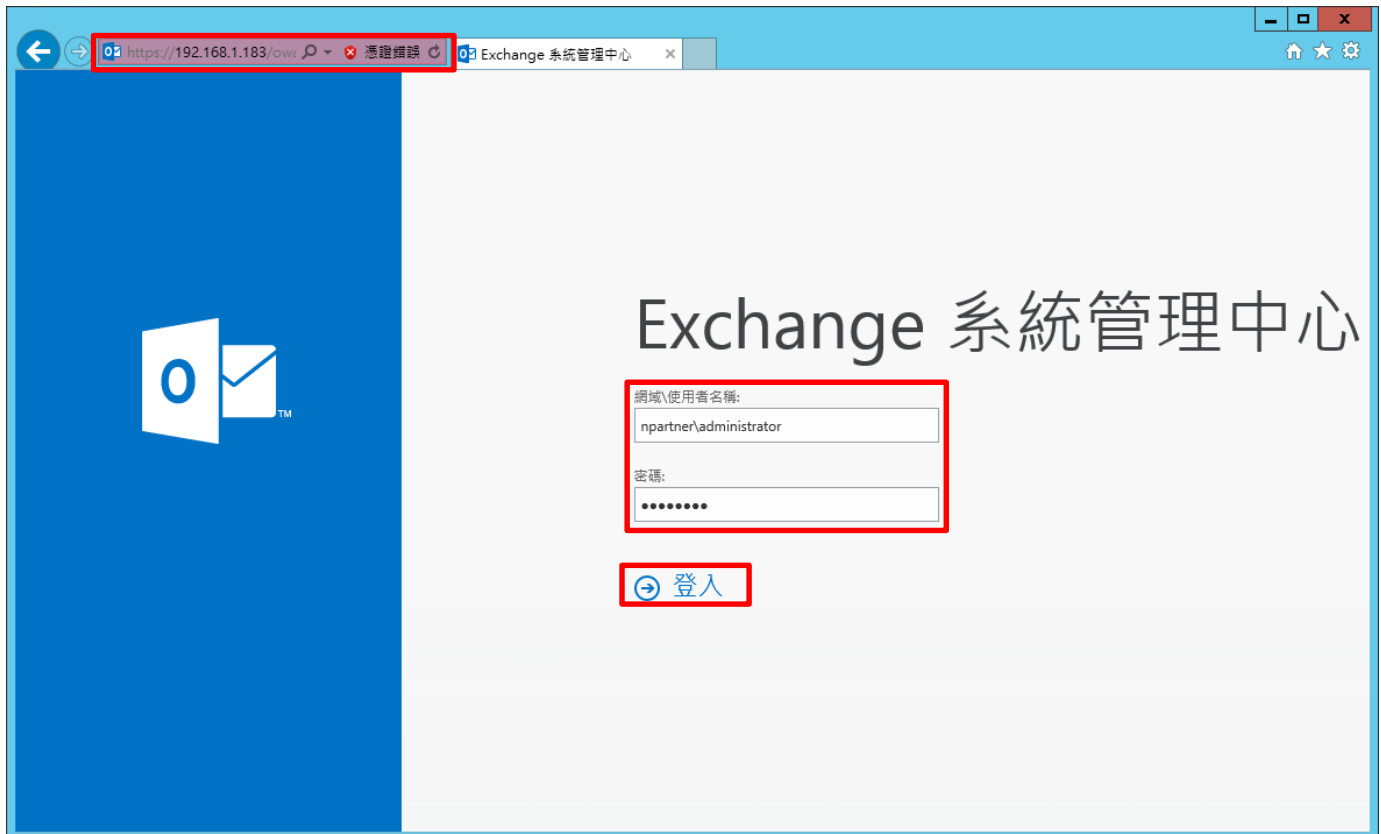
4. Exchange 2013

可選擇 [Exchange 系統管理中心] 或 [Exchange 管理命令介面] 確認啟用郵件追蹤記錄。

4.1 Exchange Message Tracking Log

4.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <https://ExchangeIP/ecp> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]



(2) 點選 [伺服器] -> [伺服器] -> 選擇 [Mailbox 伺服器] -> 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

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

混合

工具

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

WIN2012

信箱, 用戶端存取
Version 15.0 (Build 1473.3)
標準試用版
試用
[輸入產品金鑰](#)

已選取 1 項, 共 1 項

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

(3) 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\15\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 #26:
忘記內容名稱嗎? 沒問題, 因為您可以使用萬用字元來擷取符合所指定名稱之一部分的所有內容:

Get-Mailbox | Format-Table Name,*SMTP*

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\15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True

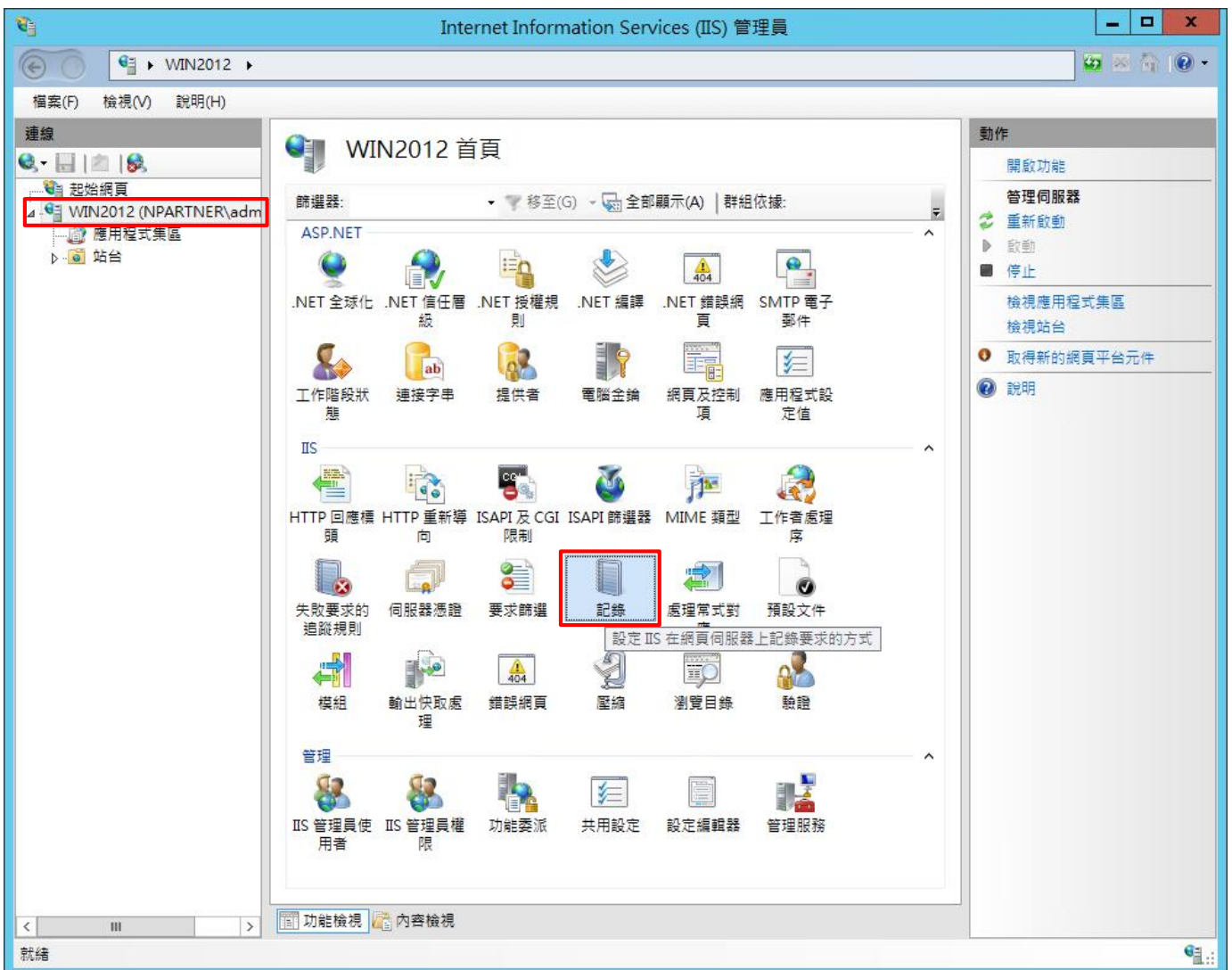
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2013>_
```

4.2 IIS log

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



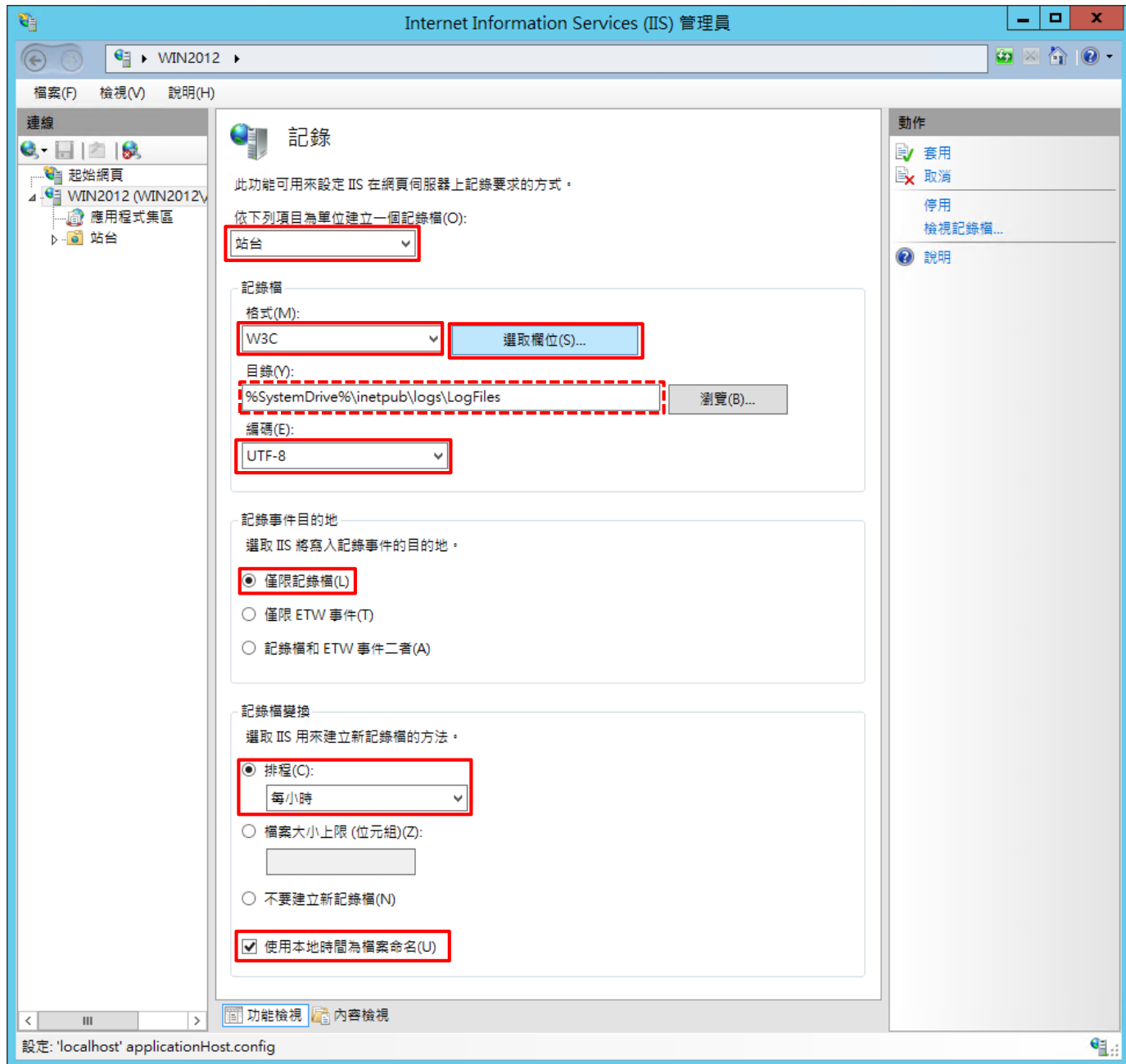
(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]



(3) 選擇依下列項目為單位建立一個記錄檔: [Site(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: [Log file only(僅限記錄檔)] -> 排程:

[Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(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 [Add Field(新增欄位)]

The screenshot shows a dialog box titled "W3C 記錄欄位" (W3C Record Fields). It has a title bar with a question mark and a close button (X). The dialog is divided into two main sections: "標準欄位(S):" (Standard Fields) and "自訂欄位(C):" (Custom Fields).

The "標準欄位(S):" section contains a list of 20 fields, each with a checked checkbox. A red rectangular box highlights the entire list of fields. The fields are:

- 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))

The "自訂欄位(C):" section contains a table with three columns: "記錄欄位" (Record Field), "來源類型" (Source Type), and "來源" (Source). The table is currently empty.

At the bottom of the dialog, there are four buttons: "新增欄位(A)..." (Add Field), "移除欄位(R)" (Remove Field), "編輯檔案(E)..." (Edit Fields), and "確定" (OK). The "新增欄位(A)..." button is highlighted with a red dashed border.

(5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(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))

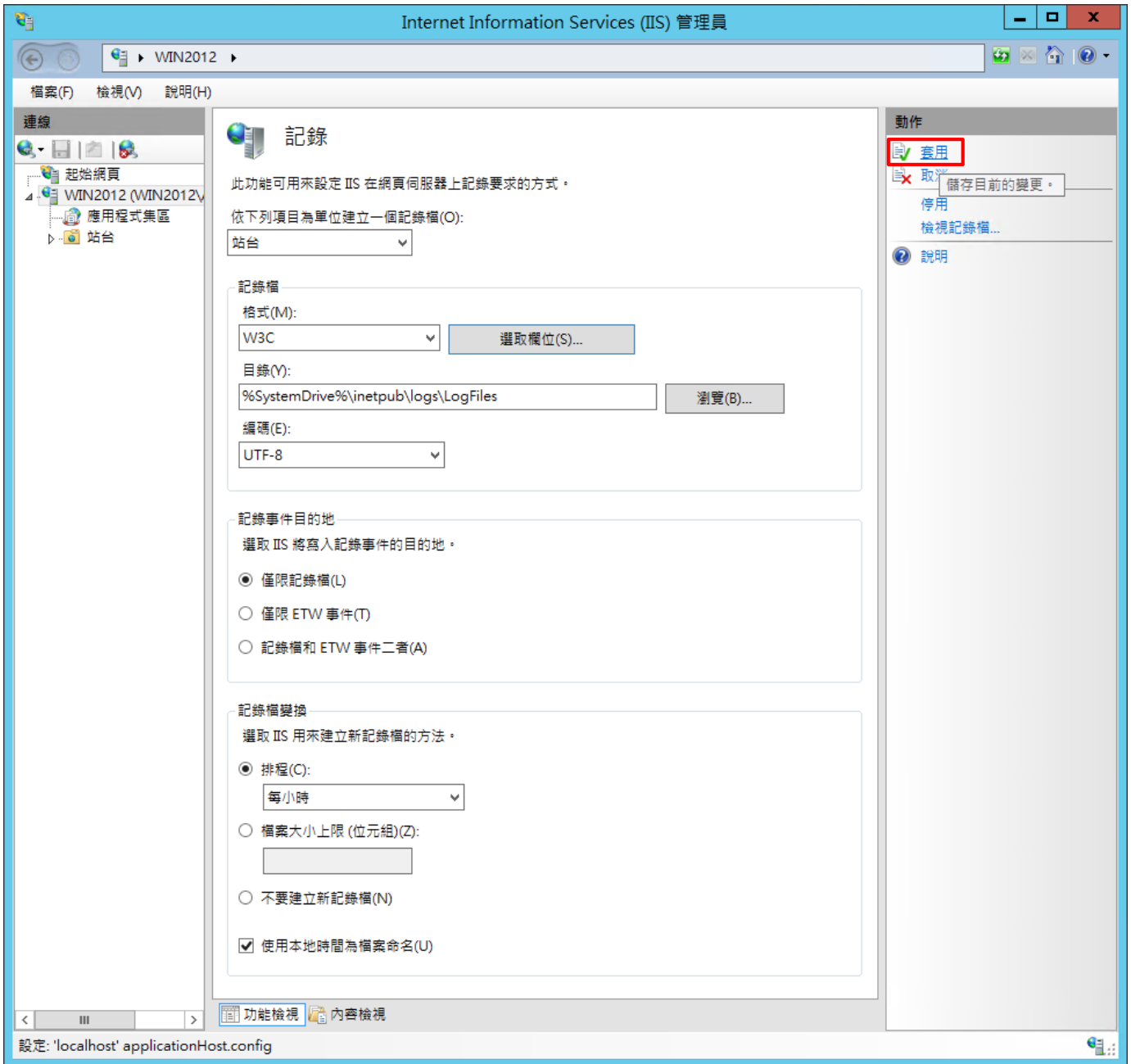
自訂欄位(C):

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

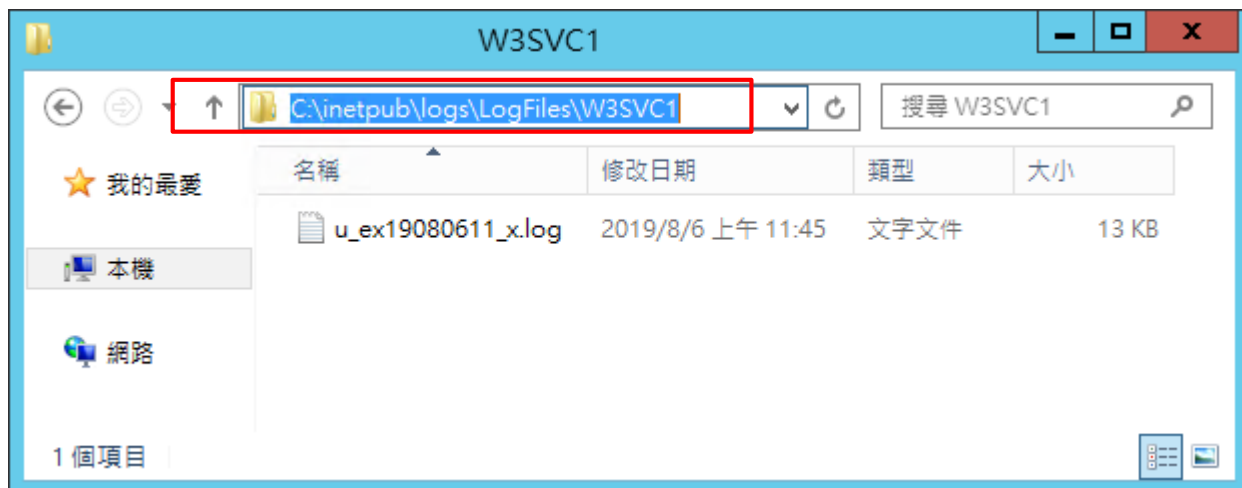
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(套用)]



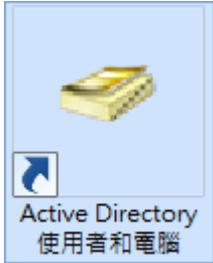
(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



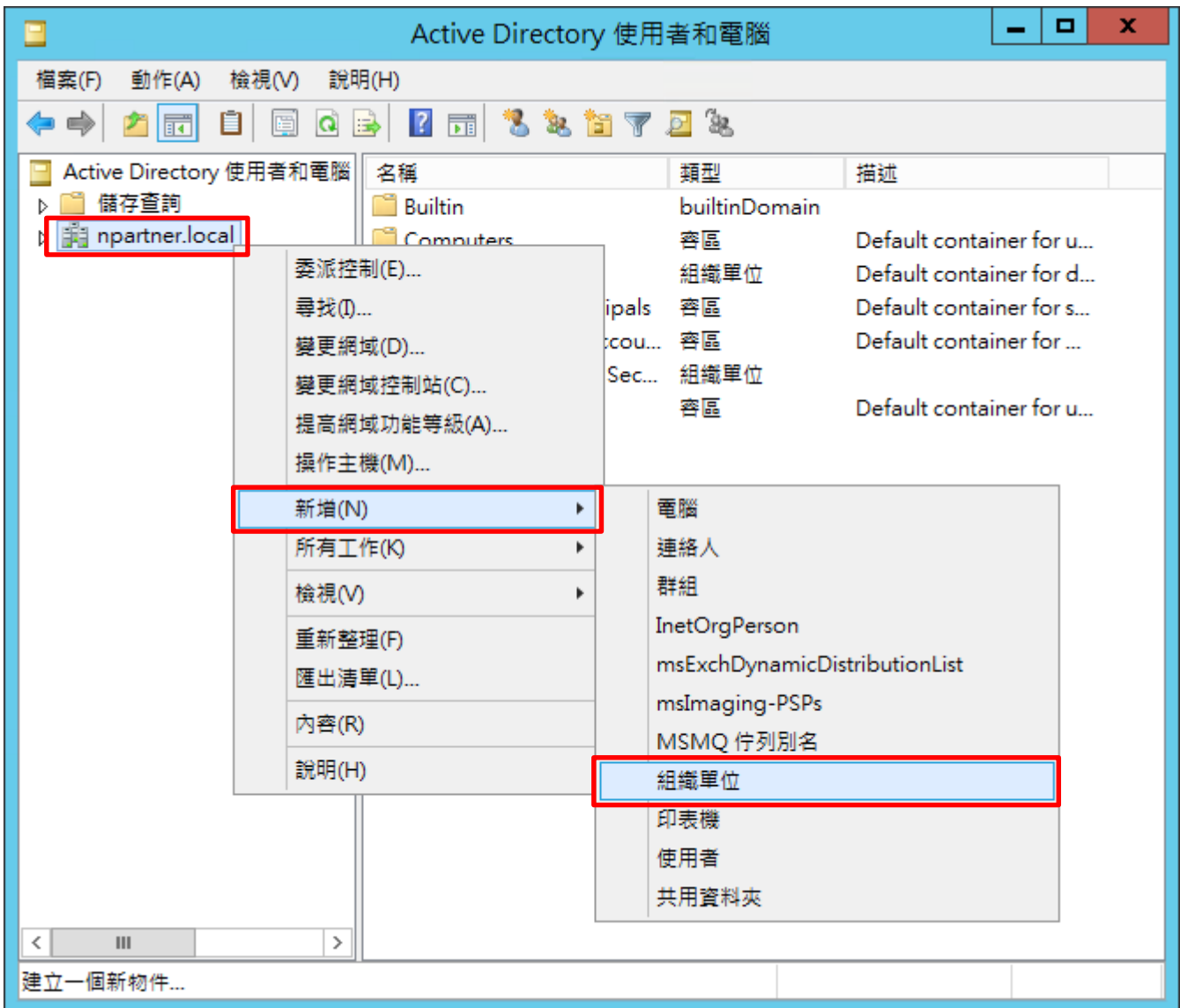
4.3 Event log

4.3.1 組織單位(Organizational Unit)

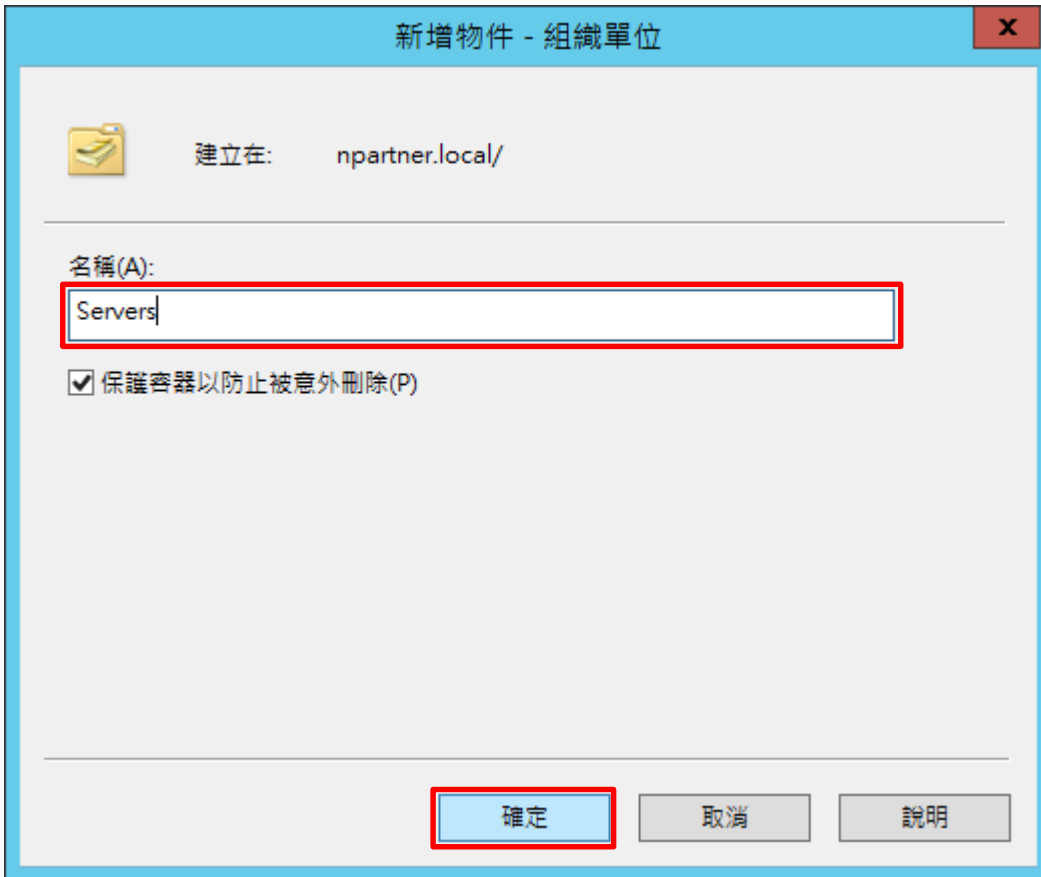
(1) 開啟 [Active Directory 使用者和電腦]



(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱: Servers -> 按下 [確定]



新增物件 - 組織單位

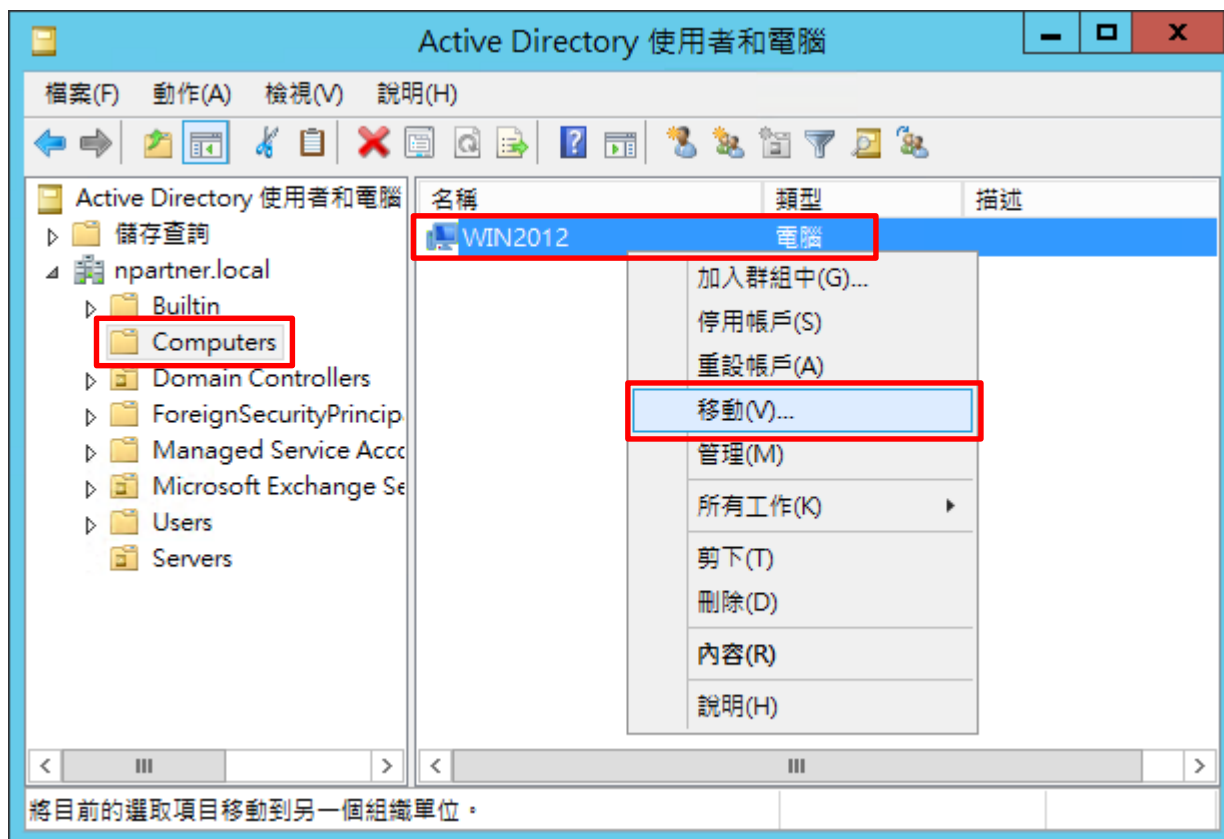
建立在: npartner.local/

名稱(A):
Servers

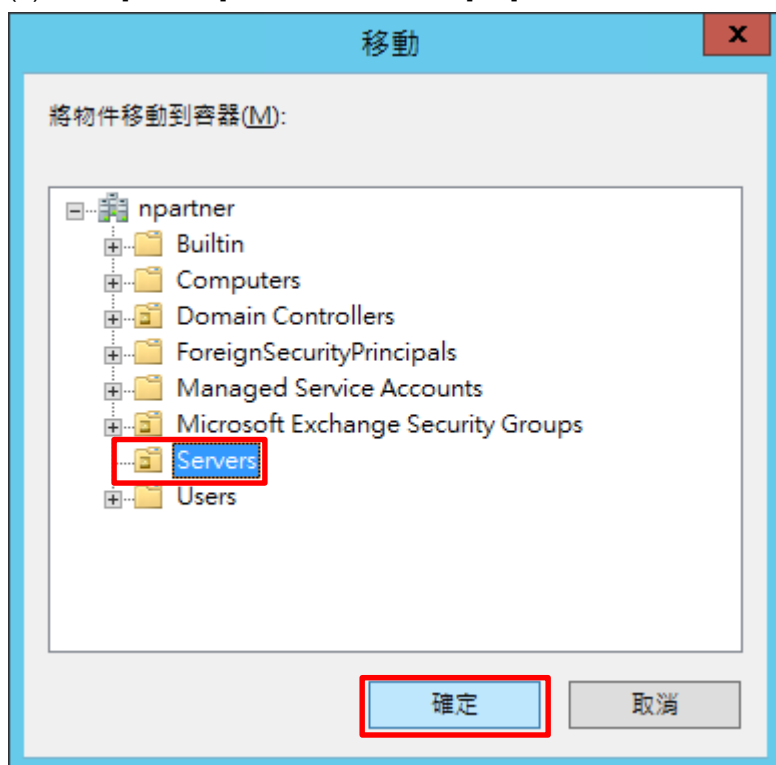
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Win2012)] 上按滑鼠右鍵 -> 點選 [移動]

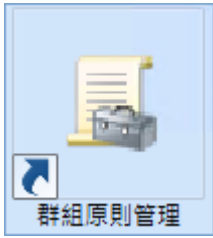


(5) 點選 [Servers] 組織單位 -> 按下 [OK]

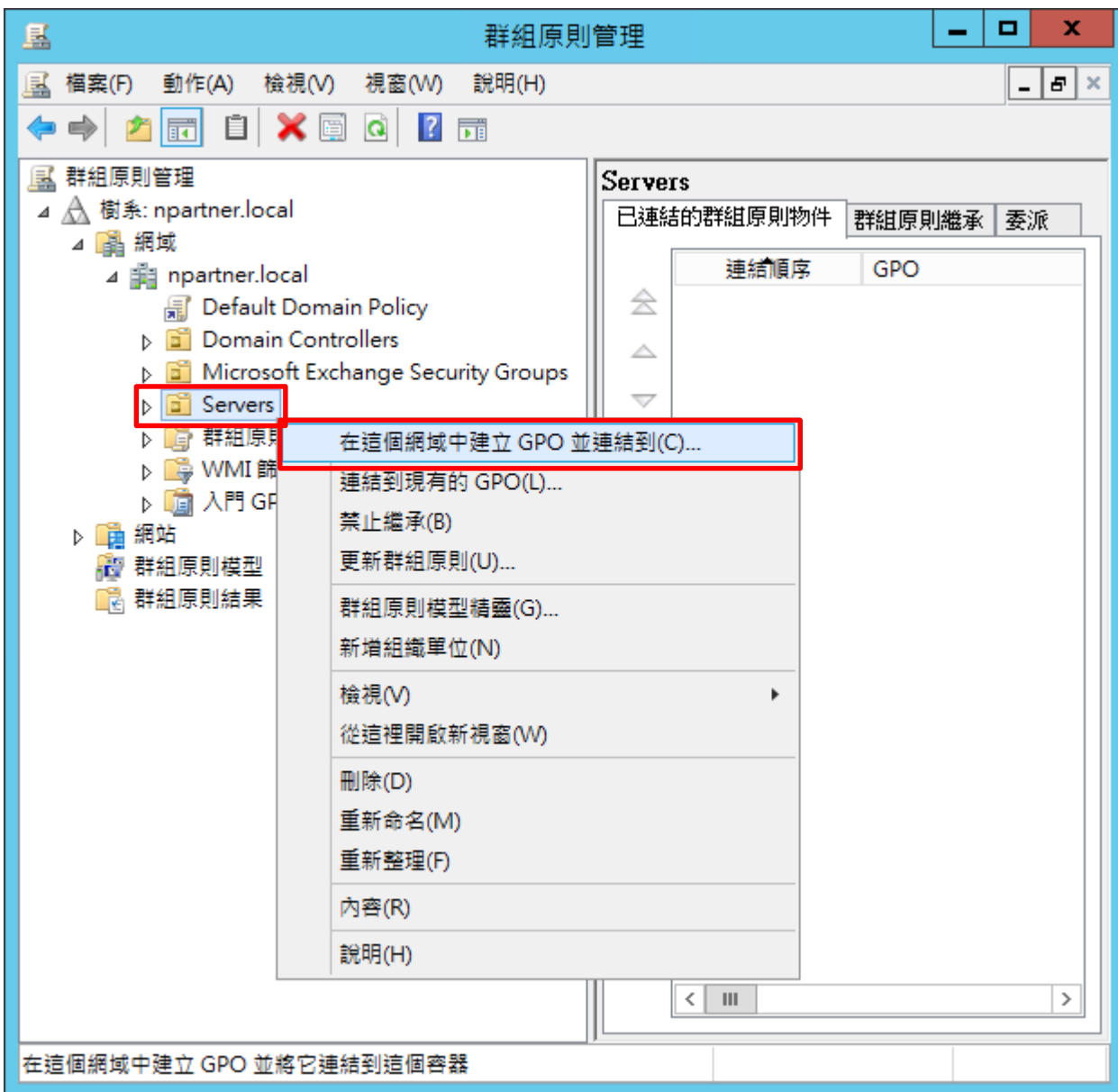


4.3.2 群組原則(Group Policy Management)

(1) 開啟 [群組原則管理]



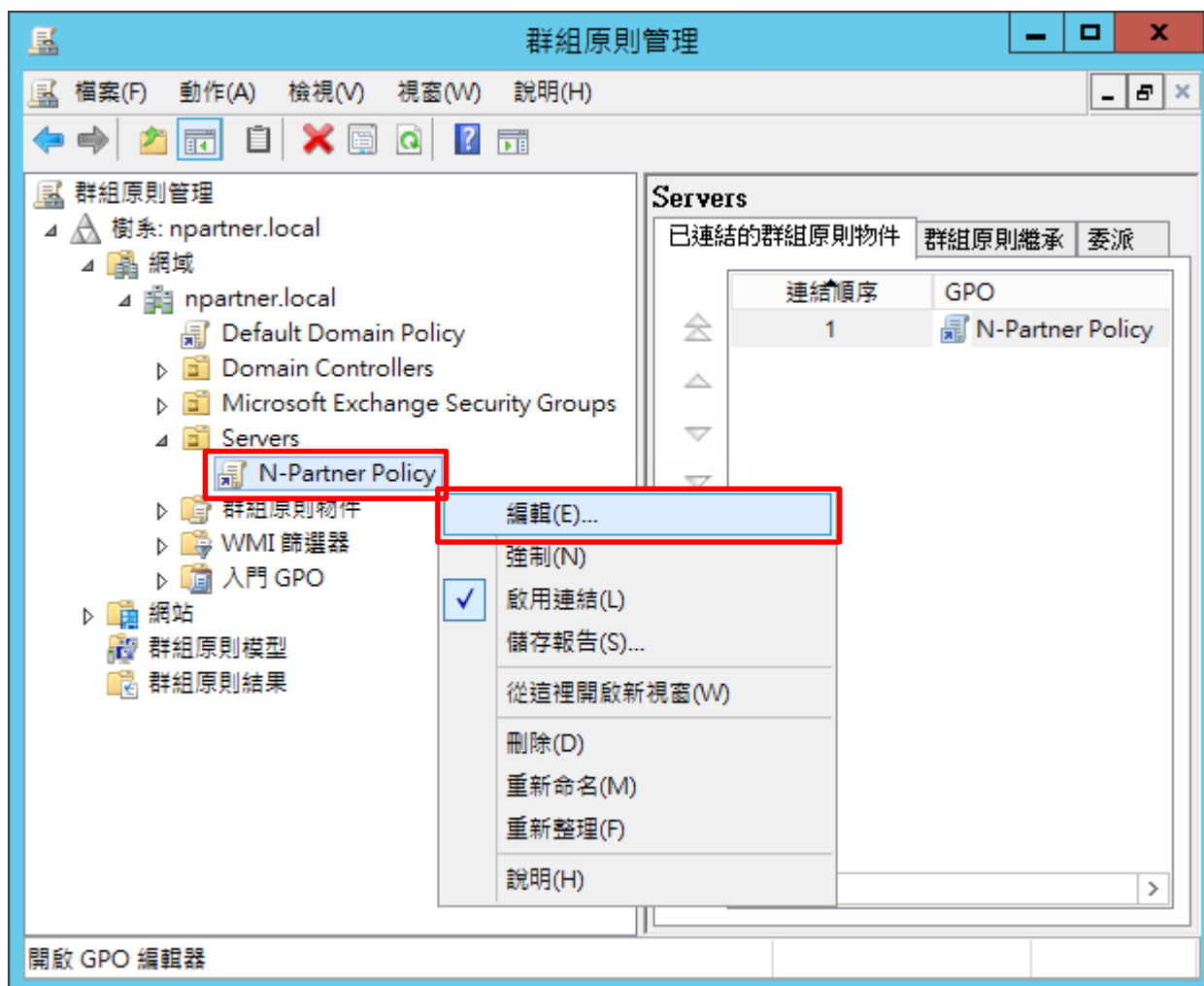
(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到]



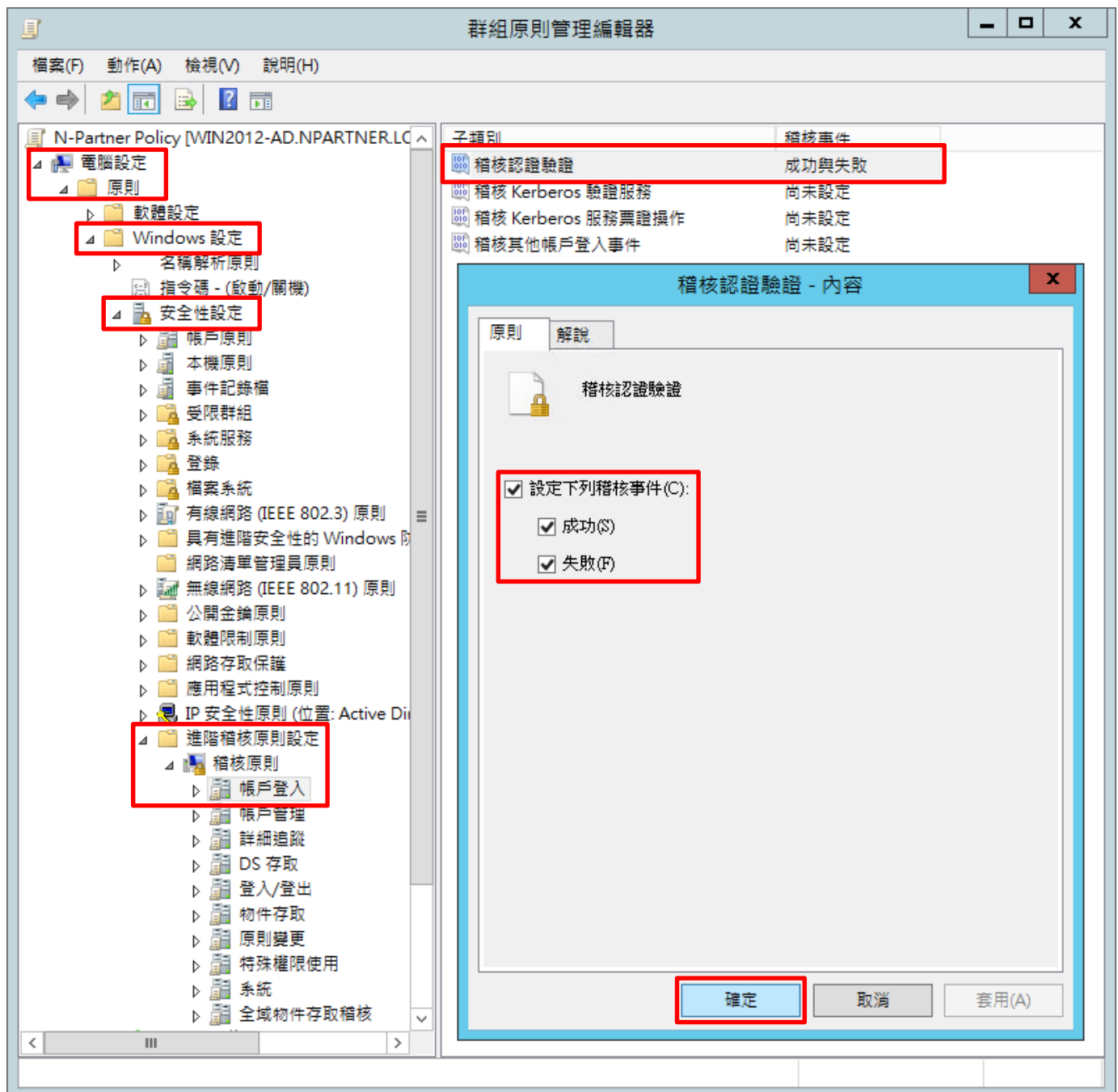
(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]



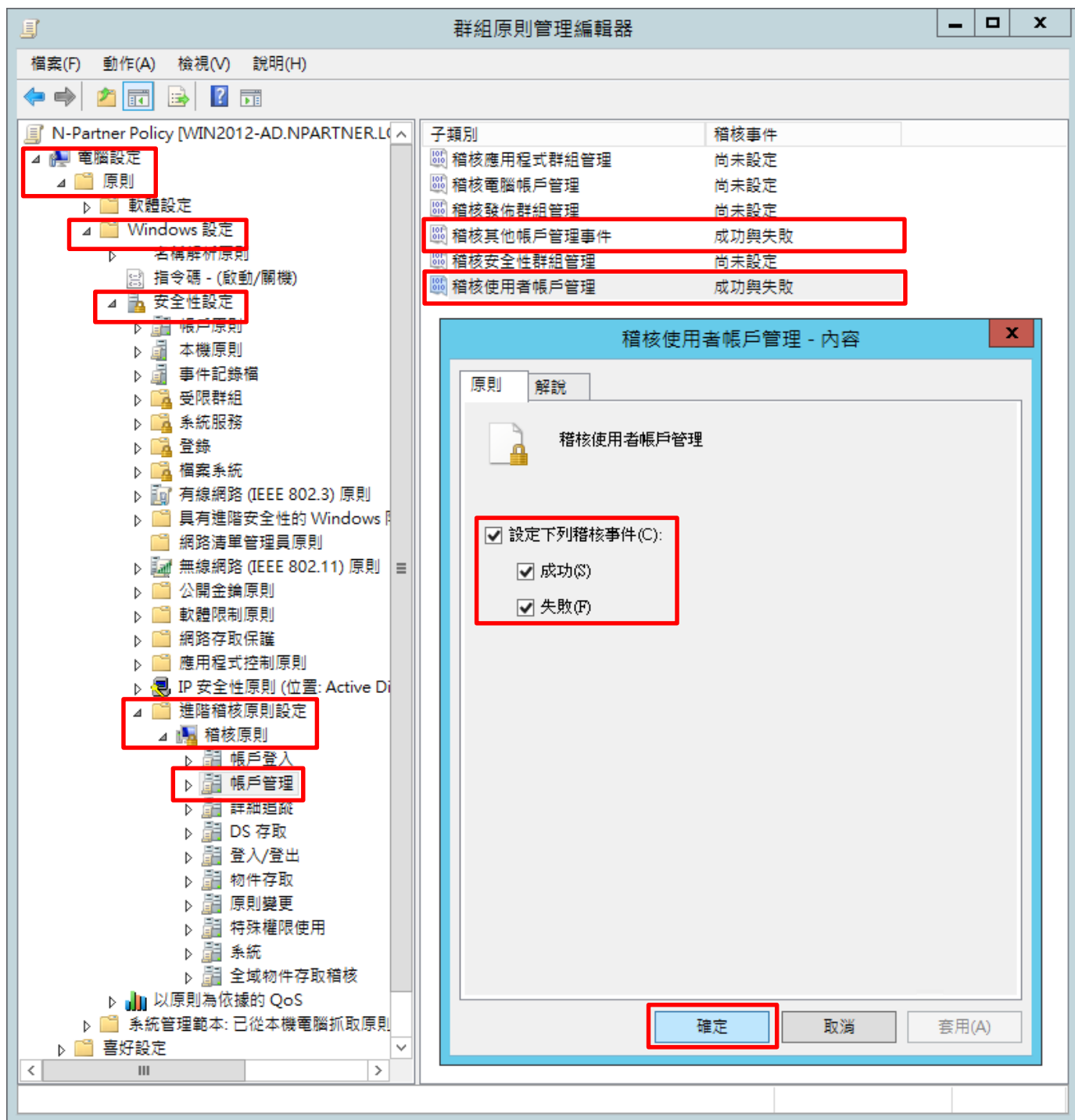
(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]



- (5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]



- (6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -> 點選 [稽核其他帳戶管理事件], [稽核使用者帳戶管理] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]



- (7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -> 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

The screenshot displays the Group Policy Management Editor interface. On the left, the navigation tree is expanded to 'Computer Settings' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Advanced Audit Policy Configuration' > 'Audit Policies' > 'Logon/Logoff'. The right pane shows a list of audit policies with the following details:

子類別	稽核事件
稽核帳戶鎖定	成功與失敗
稽核使用者/裝置宣告	尚未設定
稽核 IPsec 延伸模式	尚未設定
稽核 IPsec 主要模式	尚未設定
稽核 IPsec 快速模式	尚未設定
稽核登出	成功與失敗
稽核登入	成功與失敗
稽核網路原則伺服器	尚未設定
稽核其他登入/登出事件	尚未設定
稽核特殊登入	尚未設定

The 'Audit Logon - Content' dialog box is open, showing the 'Logon' tab. The 'Audit Logon' policy is selected, and the 'Configure Audit Events' section is checked, with 'Success (S)' and 'Failure (F)' also checked. The 'OK' button is highlighted.

(8) 在 Exchange Server 伺服器更新群組原則

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



```
Windows PowerShell
系統管理員: Windows PowerShell
Windows PowerShell
著作權 (C) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。

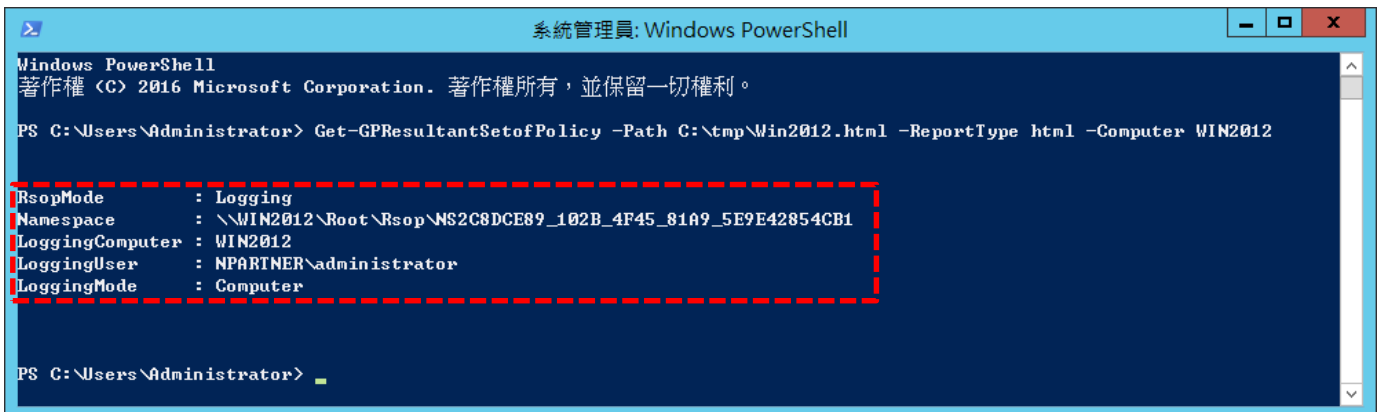
PS C:\Users\administrator.NPARTNER> gpupdate /force
正在更新原則...

電腦原則更新已成功完成。
使用者原則更新已成功完成。

PS C:\Users\administrator.NPARTNER>
```

(9) 在 AD 網域伺服器，產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱，-Path 指定報告文件的路徑和檔名。

```
PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Win2012.html -ReportType html -Computer WIN2012
```



```
Windows PowerShell
系統管理員: Windows PowerShell
Windows PowerShell
著作權 (C) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。

PS C:\Users\Administrator> Get-GPResultantSetofPolicy -Path C:\tmp\Win2012.html -ReportType html -Computer WIN2012

RsoptMode       : Logging
Namespace       : \\WIN2012\Root\Rsopt\NS2C8DCE89_102B_4F45_81A9_5E9E42854CB1
LoggingComputer : WIN2012
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer

PS C:\Users\Administrator>
```

(10) 開啟 [C:\tmp\Win2012.html] 確認啟用 [N-Partner Policy]

群組原則結果

NPARTNER\WIN2012
資料收集: 16/8/2019 10:04:28 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/安全性選項 顯示

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

進階稽核設定 隱藏

帳戶登入 隱藏

原則	設定	優勢 GPO
稽核認證驗證	成功, 失敗	N-Partner Policy

帳戶管理 隱藏

原則	設定	優勢 GPO
稽核其他帳戶管理事件	成功, 失敗	N-Partner Policy
稽核使用者帳戶管理	成功, 失敗	N-Partner Policy

登入/登出 隱藏

原則	設定	優勢 GPO
稽核帳戶鎖定	成功, 失敗	N-Partner Policy
稽核登出	成功, 失敗	N-Partner Policy
稽核登入	成功, 失敗	N-Partner Policy

群組原則物件 隱藏

已套用的 GPO 隱藏

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}] 顯示

N-Partner Policy [{C8C6D0D6-97C1-42AD-BE1E-BC6A110BF205}] 顯示

被拒絕的 GPO 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

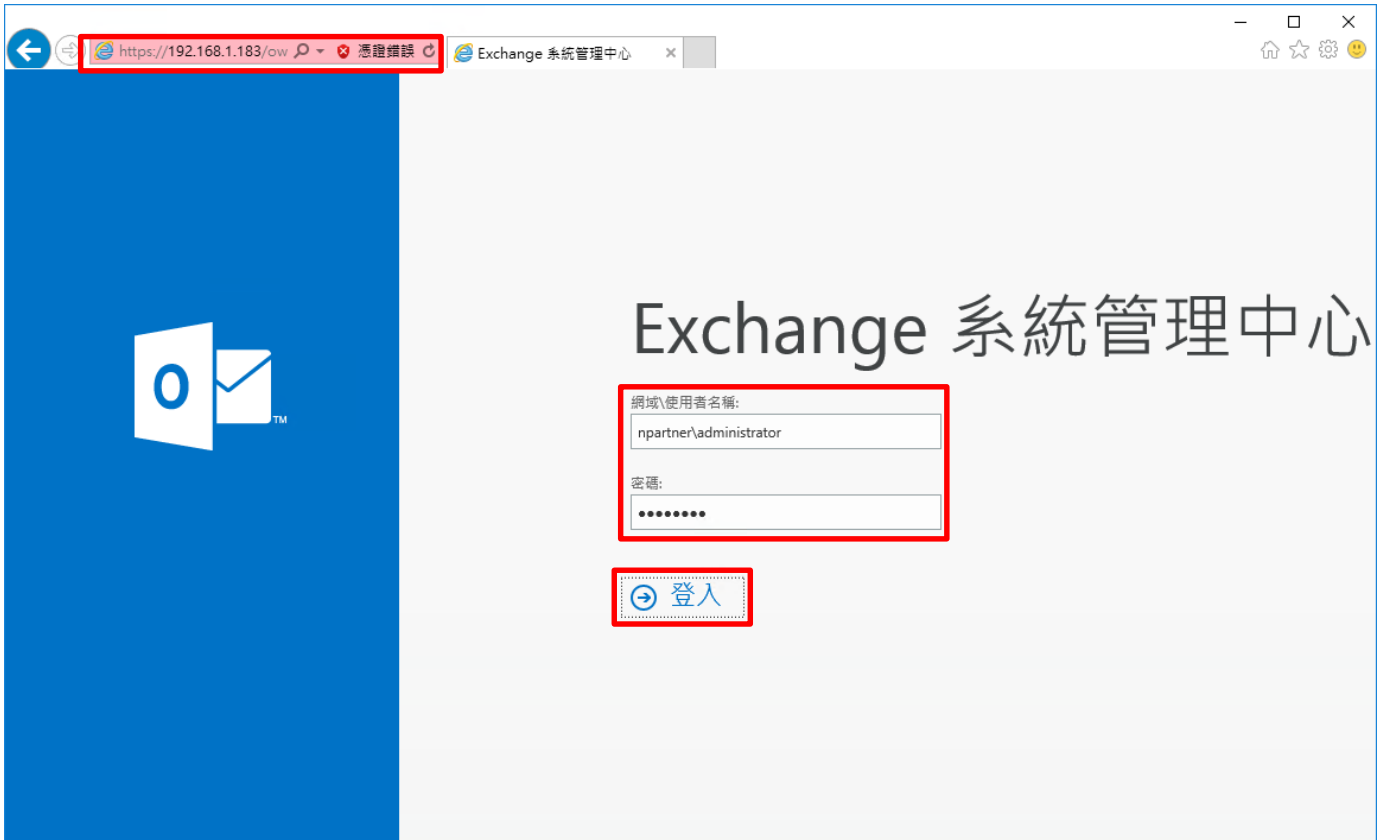
5. Exchange 2016

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。

5.1 Exchange Message Tracking Log

5.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <https://ExchangeIP/ecp> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]



(2) 點選 [伺服器] -> [伺服器] -> 選擇 [Mailbox 伺服器] -> 點選 [編輯]

Exchange 系統管理中心

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
整合通訊
伺服器
混合

伺服器 資料庫 資料庫可用性群組 虛擬目錄 憑證

編輯 搜尋 刷新

名稱	伺服器角色	版本	
EXCH2016	信箱	Version 15.1 (Build ...)	EXCH2016 信箱 Version 15.1 (Build 1713.5) 標準試用版 試用 輸入產品金鑰

已選取 1 個，共 1 個

(3) 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=2297e724-7aad-425b- 憑證錯誤

EXCH2016

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=2297e724-7aad-425b- 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 EXCH2016 | Select-Object *Track*`

A screenshot of a Windows terminal window titled '機器: Exch2016.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 #77:  
你知道從佇列匯出訊息時, 必須使用 AssembleMessage 指令碼嗎? 例如, 若您要從伺服器 Mailbox1 上的 contoso.com 佇列匯出訊息 ID 1234 的訊息, 則需執行下列命令:  
Export-Message -Identity Mailbox1\contoso.com\1234 | AssembleMessage -Path "C:\ExportedMessages\Message1234.eml"  
詳細資訊: 連線至 Exch2016.npartner.local。  
詳細資訊: 已連線至 Exch2016.npartner.local。  
[PS] C:\Windows\system32>Get-TransportService EXCH2016 | 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:\Windows\system32>
```

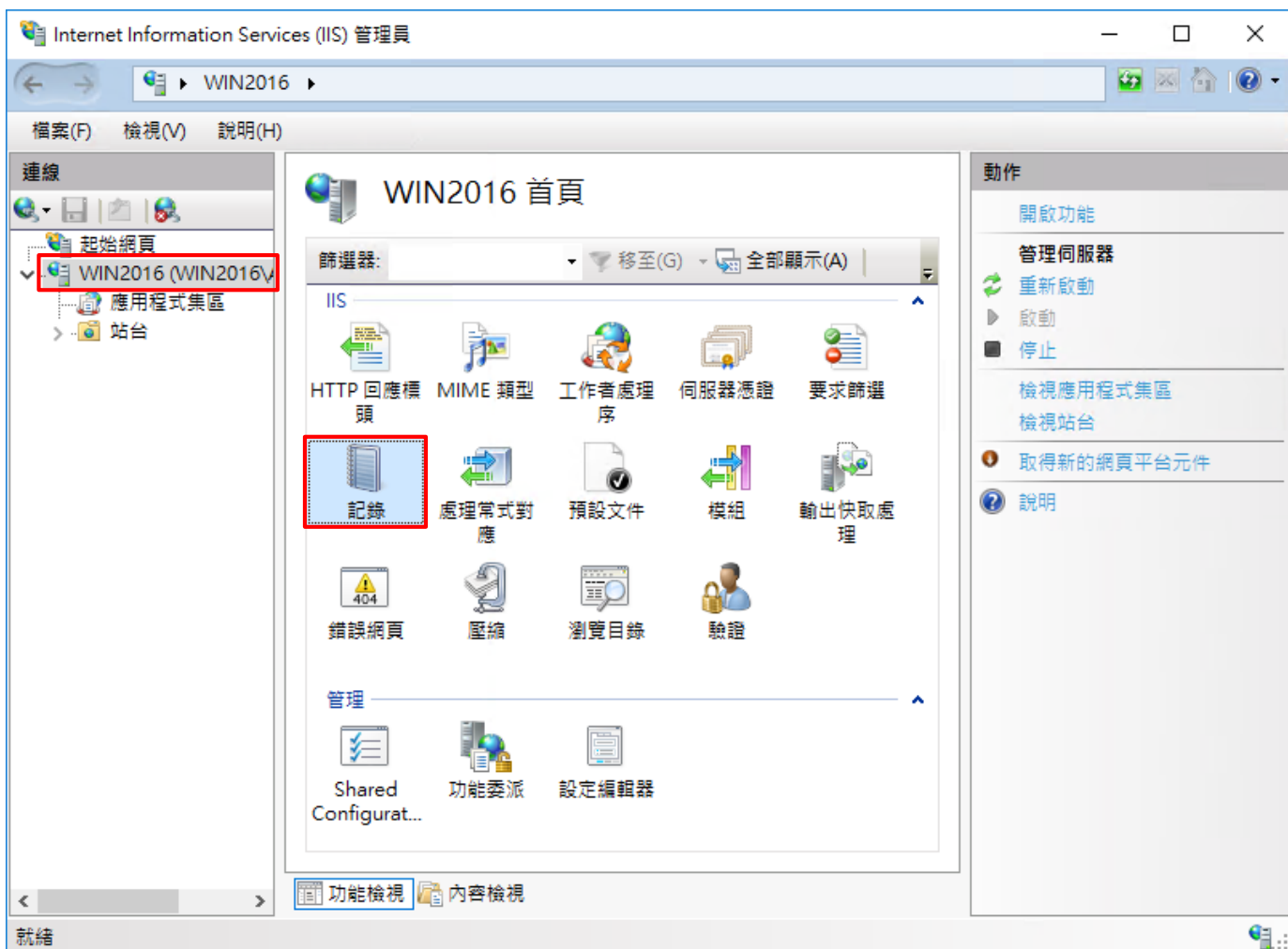
The output of the command is highlighted with a red dashed border.

5.2 IIS log

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



(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]



(3) 選擇依下列項目為單位建立一個記錄檔: [Site(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: [Log file only(僅限記錄檔)] -> 排程: [Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(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 [Add Field(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: [Request Header(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))

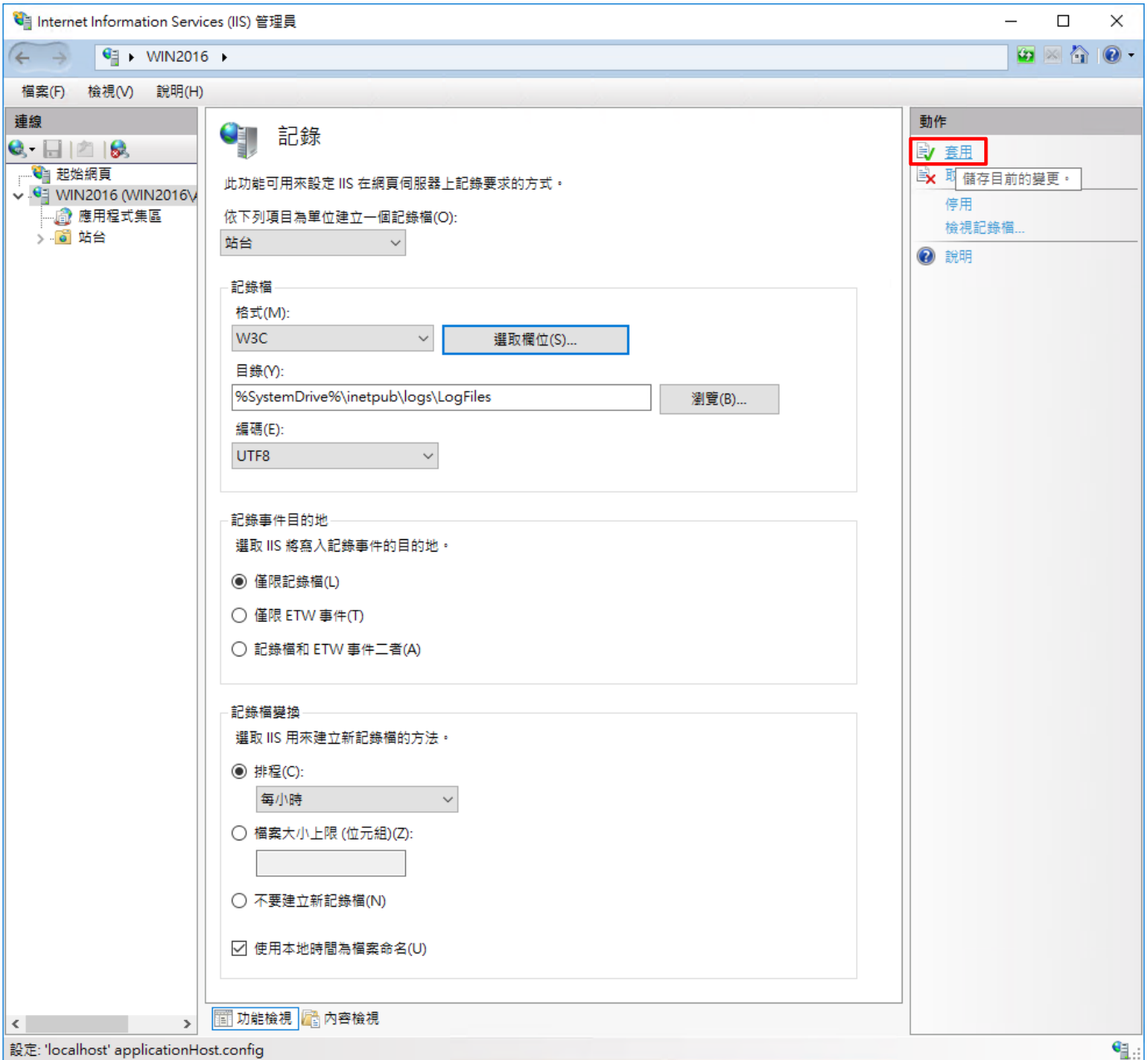
自訂欄位(C):

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

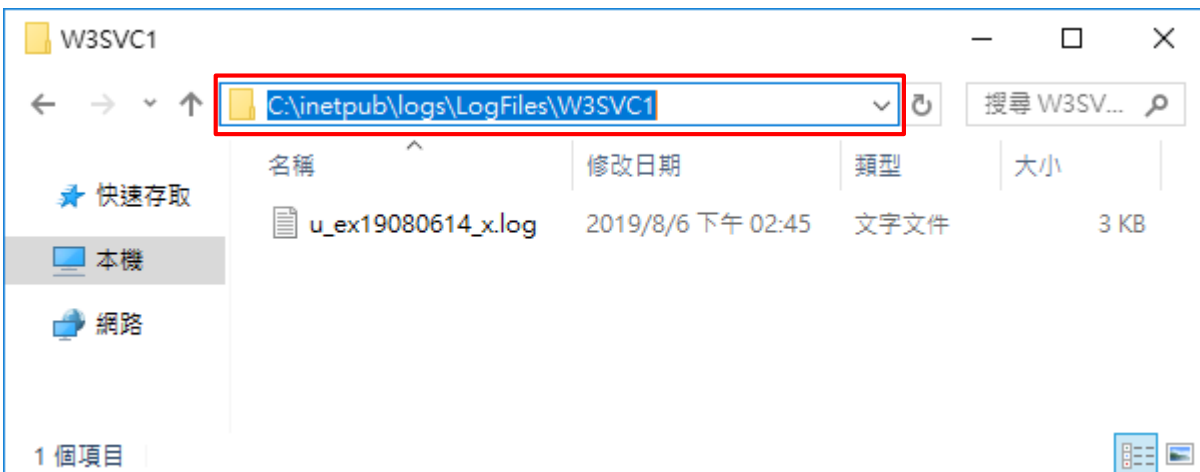
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(套用)]



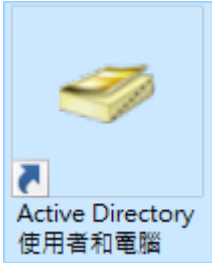
(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



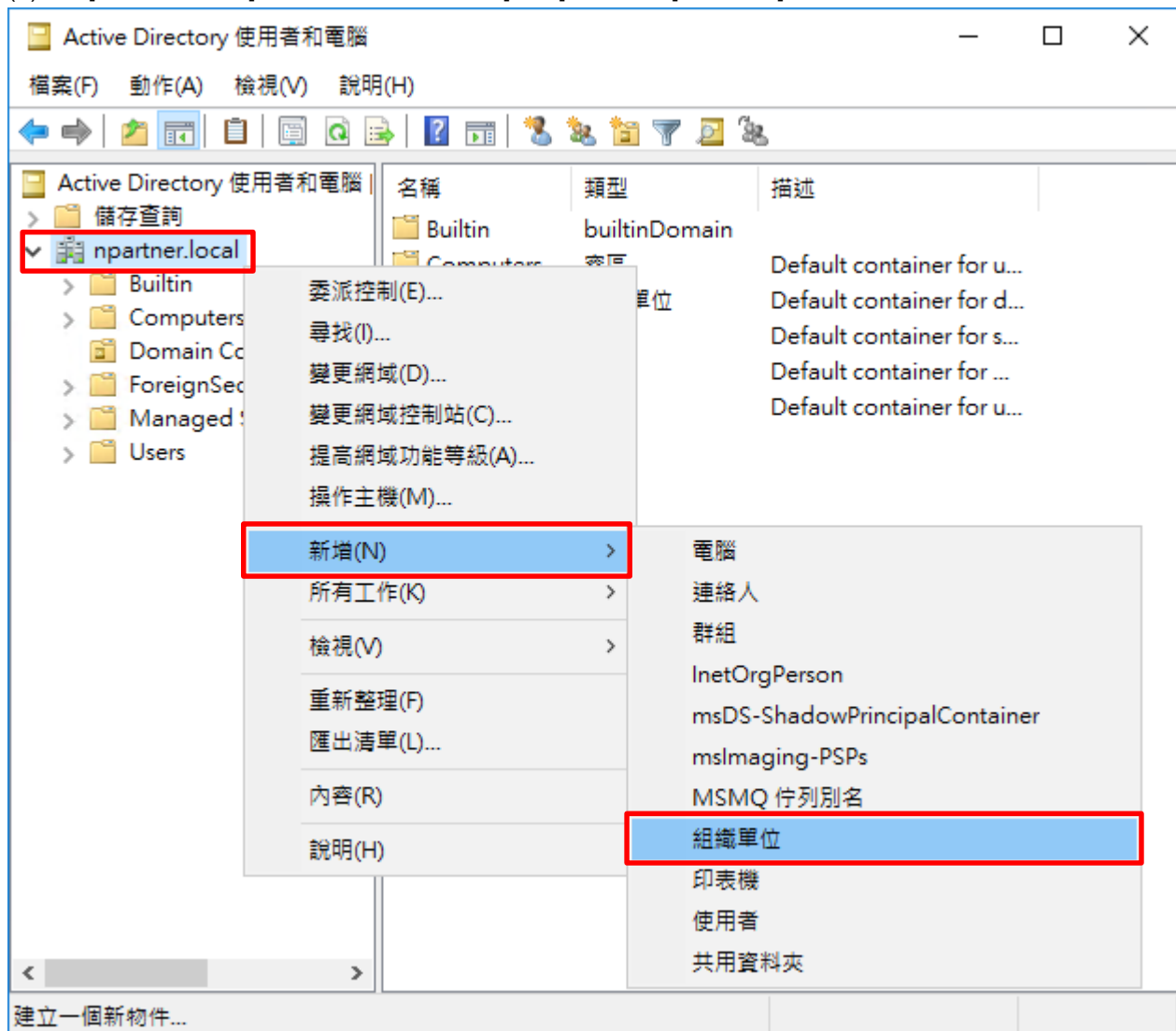
5.3 Event log

5.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



(2) 在 [Domain Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱: Servers -> 按下 [確定]

新增物件 - 組織單位

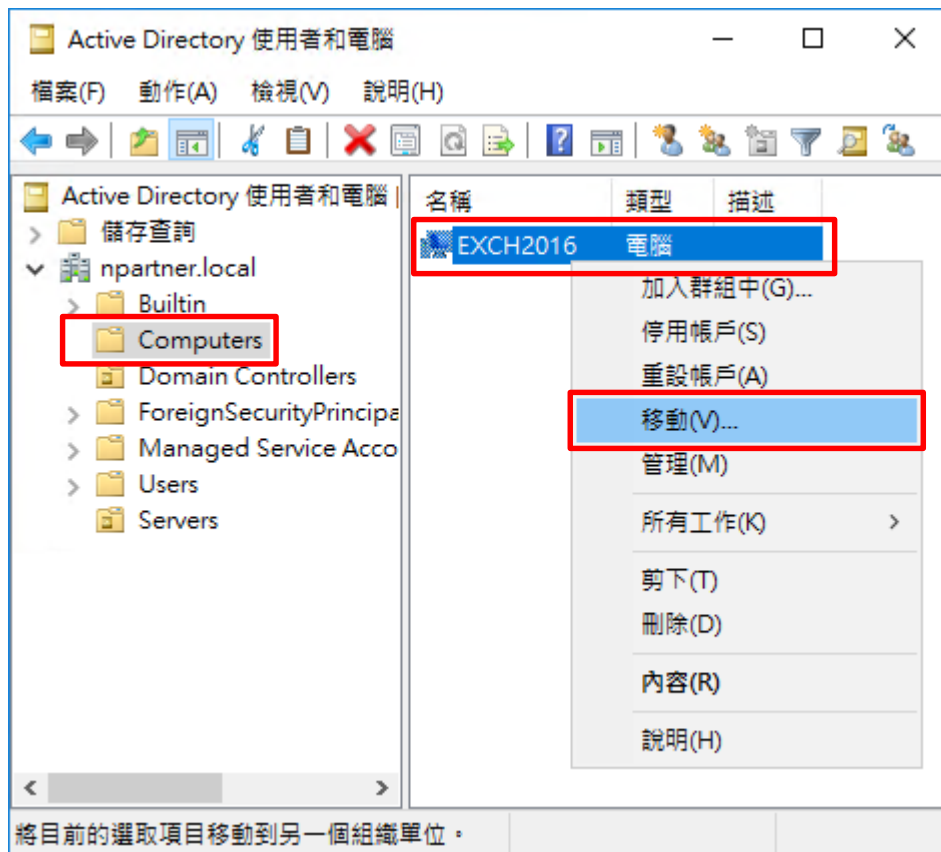
建立在: npartner.local/

名稱(A):
Servers

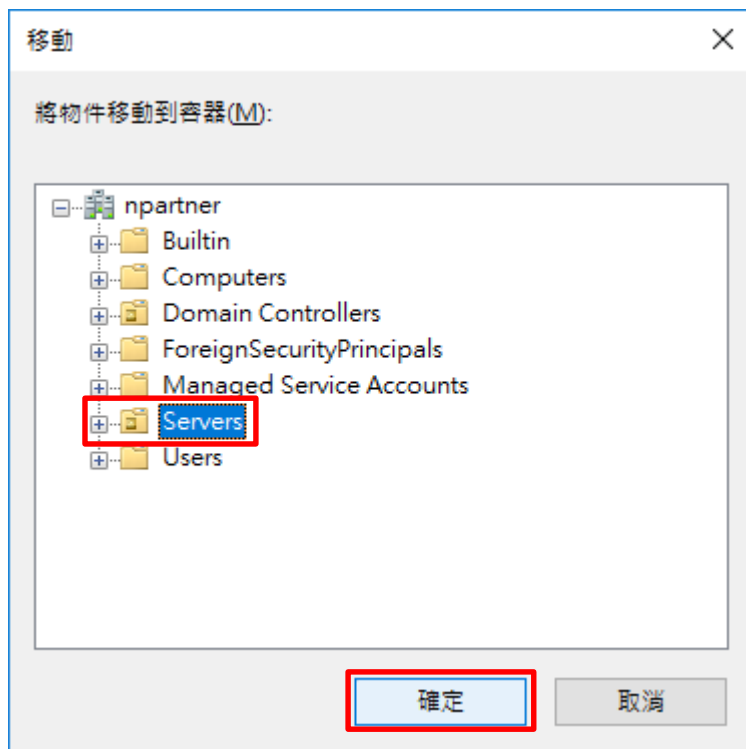
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Exch2016)] 上按滑鼠右鍵 -> 點選 [移動]

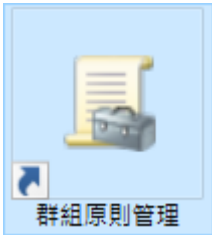


(5) 點選 [Servers] 組織單位 -> 按下 [OK]

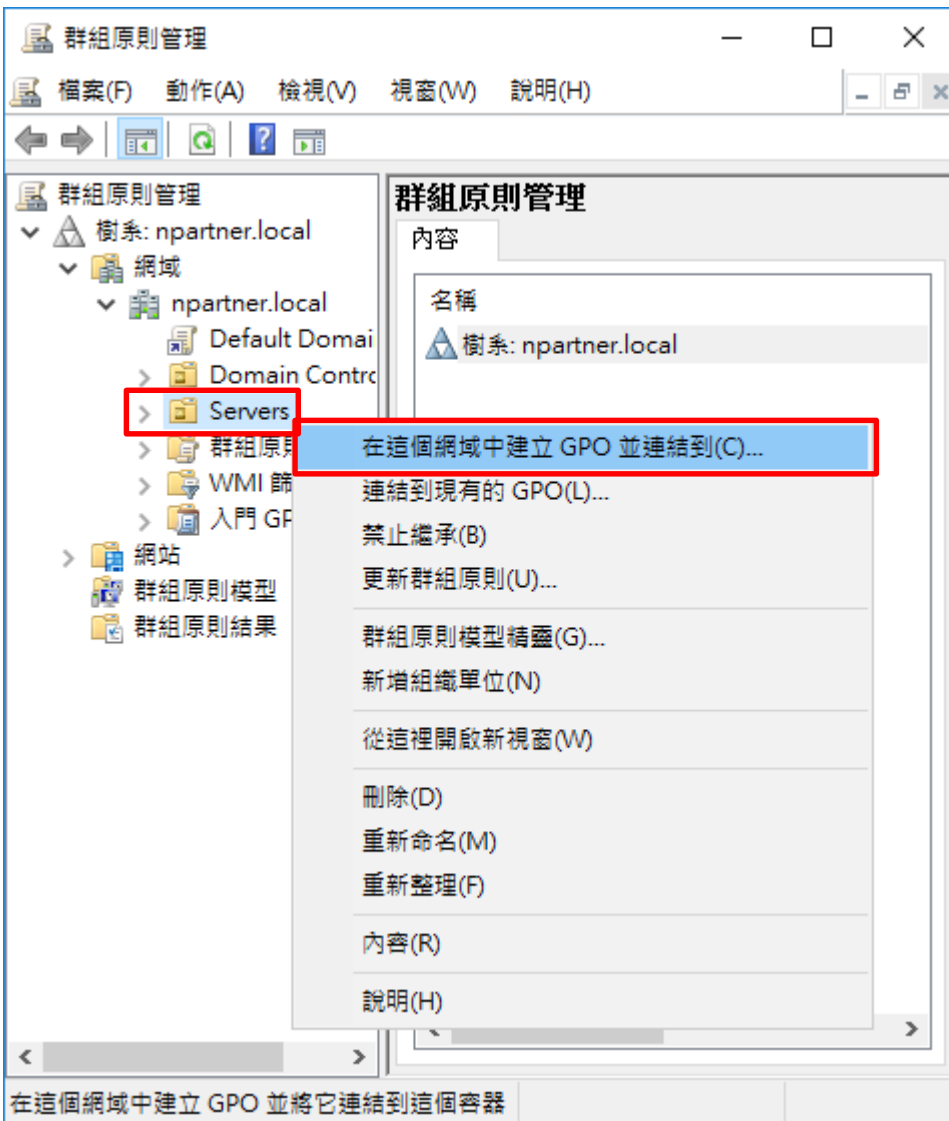


5.3.2 群組原則(Group Policy Management)

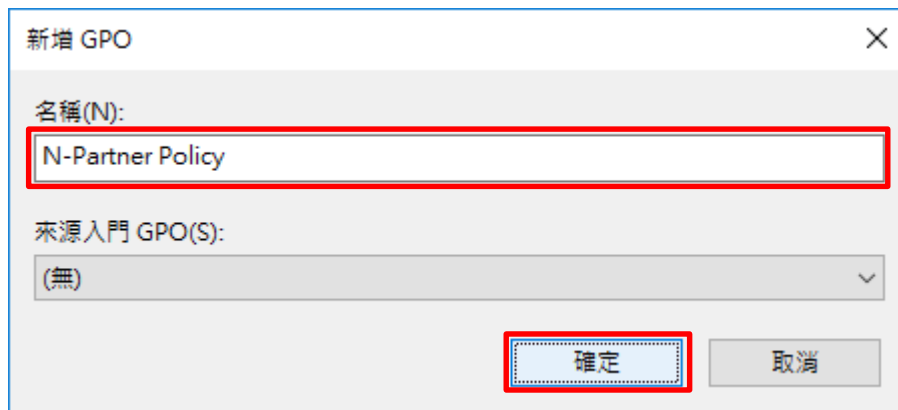
(1) 開啟 [群組原則管理]



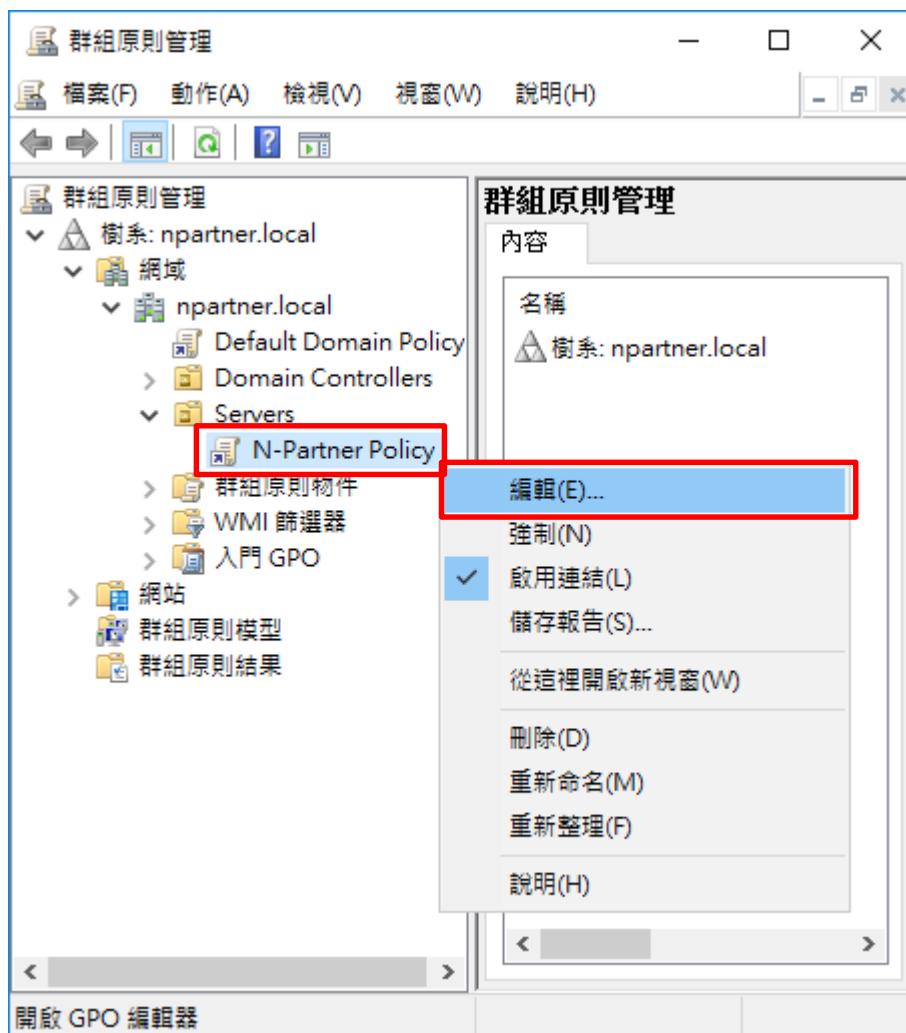
(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到這裡]



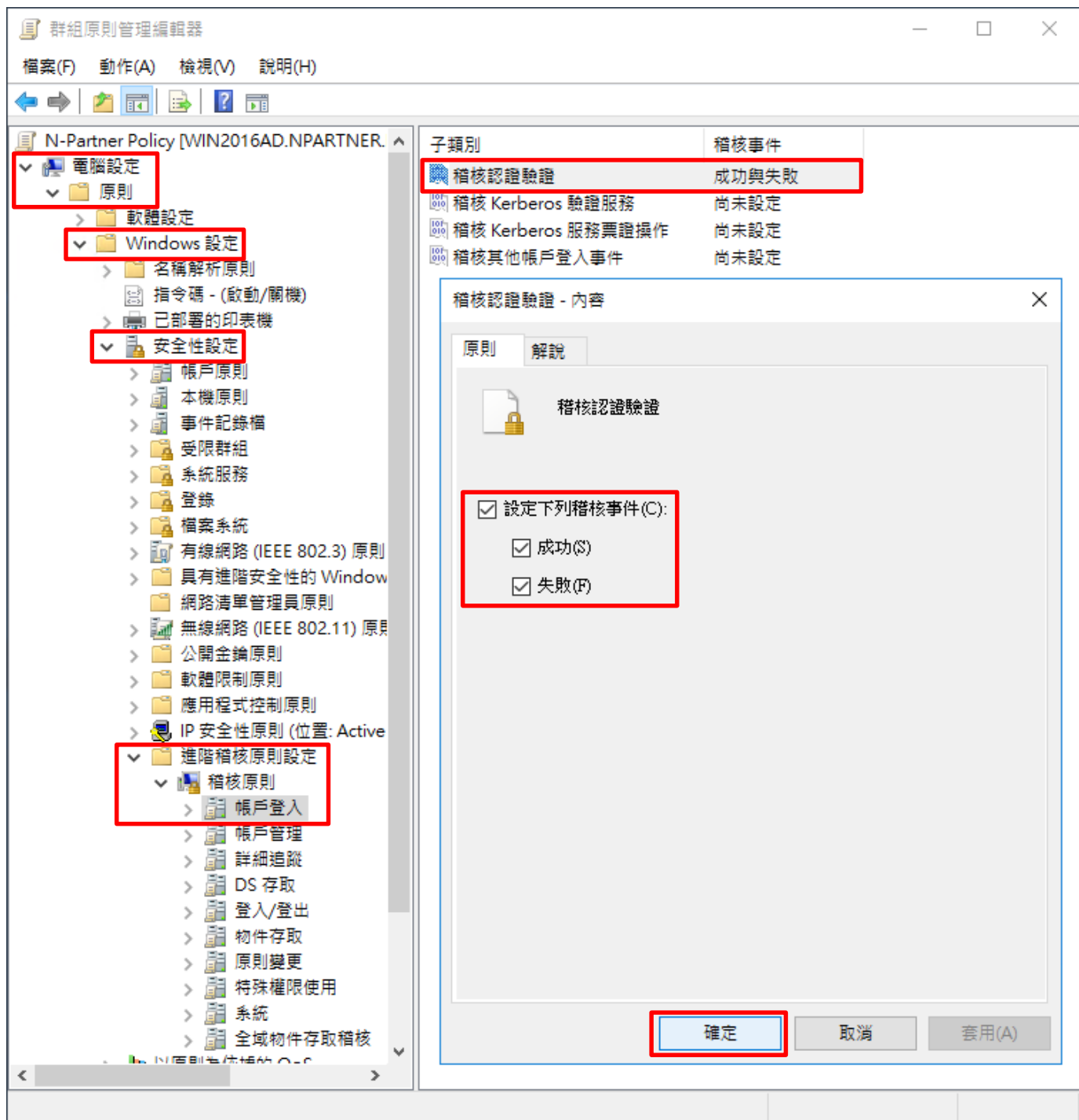
(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]



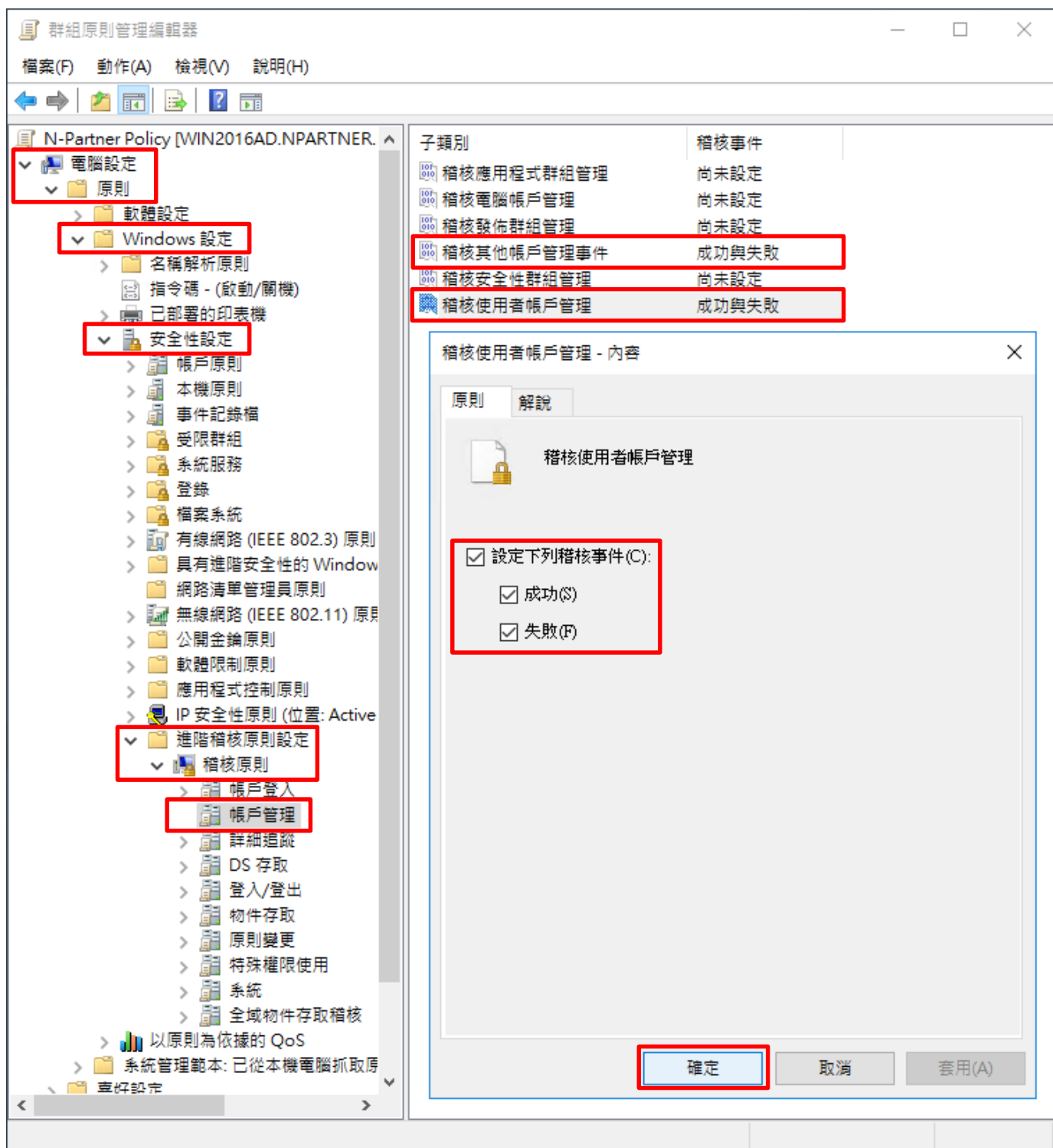
(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]



- (5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]



- (6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -> 點選 [稽核其他帳戶管理事件], [稽核使用者帳戶管理] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]



- (7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -> 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [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 [WIN2016AD.NPARTNER.LOCAL]

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) 原則

具有進階安全性的 Windows 防火牆

網路清單管理員原則

無線網路 (IEEE 802.11) 原則

公開金鑰原則

軟體限制原則

應用程式式控制原則

IP 安全性原則 (位置: Active Directory)

進階稽核原則設定

稽核原則

帳戶登入

帳戶管理

詳細追蹤

DS 存取

登入/登出

物件存取

原則變更

特殊權限使用

系統

全域物件存取稽核

以原則為依據的 QoS

系統管理範本: 已從本機電腦抓取原則

喜好設定

使用者設定

原則

喜好設定

子類別	稽核事件
稽核帳戶鎖定	成功與失敗
稽核使用者/裝置宣告	尚未設定
稽核群組成員資格	尚未設定
稽核 IPsec 延伸模式	尚未設定
稽核 IPsec 主要模式	尚未設定
稽核 IPsec 快速模式	尚未設定
稽核登出	成功與失敗
稽核登入	成功與失敗
稽核網路原則伺服器	尚未設定
稽核其他登入/登出事件	尚未設定
稽核特殊登入	尚未設定

稽核登入 - 內容

原則 解說

稽核登入

設定下列稽核事件(C):

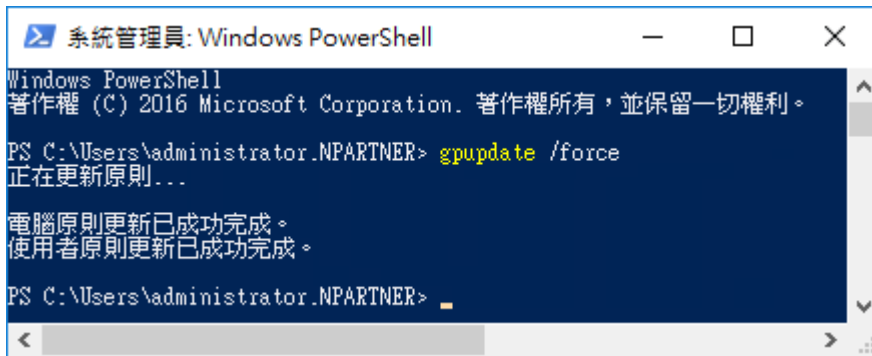
成功(S)

失敗(F)

確定 取消 套用(A)

(8) 在 Exchange Server 伺服器更新群組原則

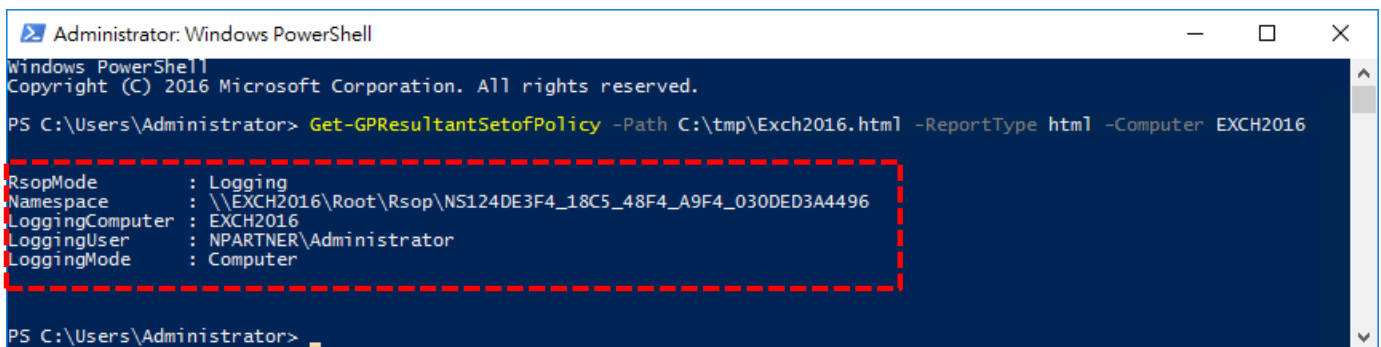
```
PS C:\> gpupdate /force
```



```
系統管理員: Windows PowerShell
Windows PowerShell
著作權 (C) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。
PS C:\Users\administrator.NPARTNER> gpupdate /force
正在更新原則...
電腦原則更新已成功完成。
使用者原則更新已成功完成。
PS C:\Users\administrator.NPARTNER> _
```

(9) 在 AD 網域伺服器，產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱，-Path 指定報告文件的路徑和檔名。

```
PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2016.html -ReportType html -Computer EXCH2016
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2016.html -ReportType html -Computer EXCH2016
RsopMode       : Logging
Namespace      : \\EXCH2016\Root\Rsop\NS124DE3F4_18C5_48F4_A9F4_030DED3A4496
LoggingComputer : EXCH2016
LoggingUser    : NPARTNER\Administrator
LoggingMode    : Computer
PS C:\Users\Administrator> _
```

(10) 開啟 [C:\tmp\EXCH2016.html] 確認啟用 [N-Partner Policy]

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/安全性選項	顯示												
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												
進階稽核設定	隱藏												
帳戶登入	隱藏												
<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>稽核認證驗證</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	原則	設定	優勢 GPO	稽核認證驗證	成功, 失敗	N-Partner Policy							
原則	設定	優勢 GPO											
稽核認證驗證	成功, 失敗	N-Partner Policy											
帳戶管理	隱藏												
<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>稽核其他帳戶管理事件</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> <tr> <td>稽核使用者帳戶管理</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	原則	設定	優勢 GPO	稽核其他帳戶管理事件	成功, 失敗	N-Partner Policy	稽核使用者帳戶管理	成功, 失敗	N-Partner Policy				
原則	設定	優勢 GPO											
稽核其他帳戶管理事件	成功, 失敗	N-Partner Policy											
稽核使用者帳戶管理	成功, 失敗	N-Partner Policy											
登入/登出	隱藏												
<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>稽核帳戶鎖定</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> <tr> <td>稽核登出</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> <tr> <td>稽核登入</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	原則	設定	優勢 GPO	稽核帳戶鎖定	成功, 失敗	N-Partner Policy	稽核登出	成功, 失敗	N-Partner Policy	稽核登入	成功, 失敗	N-Partner Policy	
原則	設定	優勢 GPO											
稽核帳戶鎖定	成功, 失敗	N-Partner Policy											
稽核登出	成功, 失敗	N-Partner Policy											
稽核登入	成功, 失敗	N-Partner Policy											

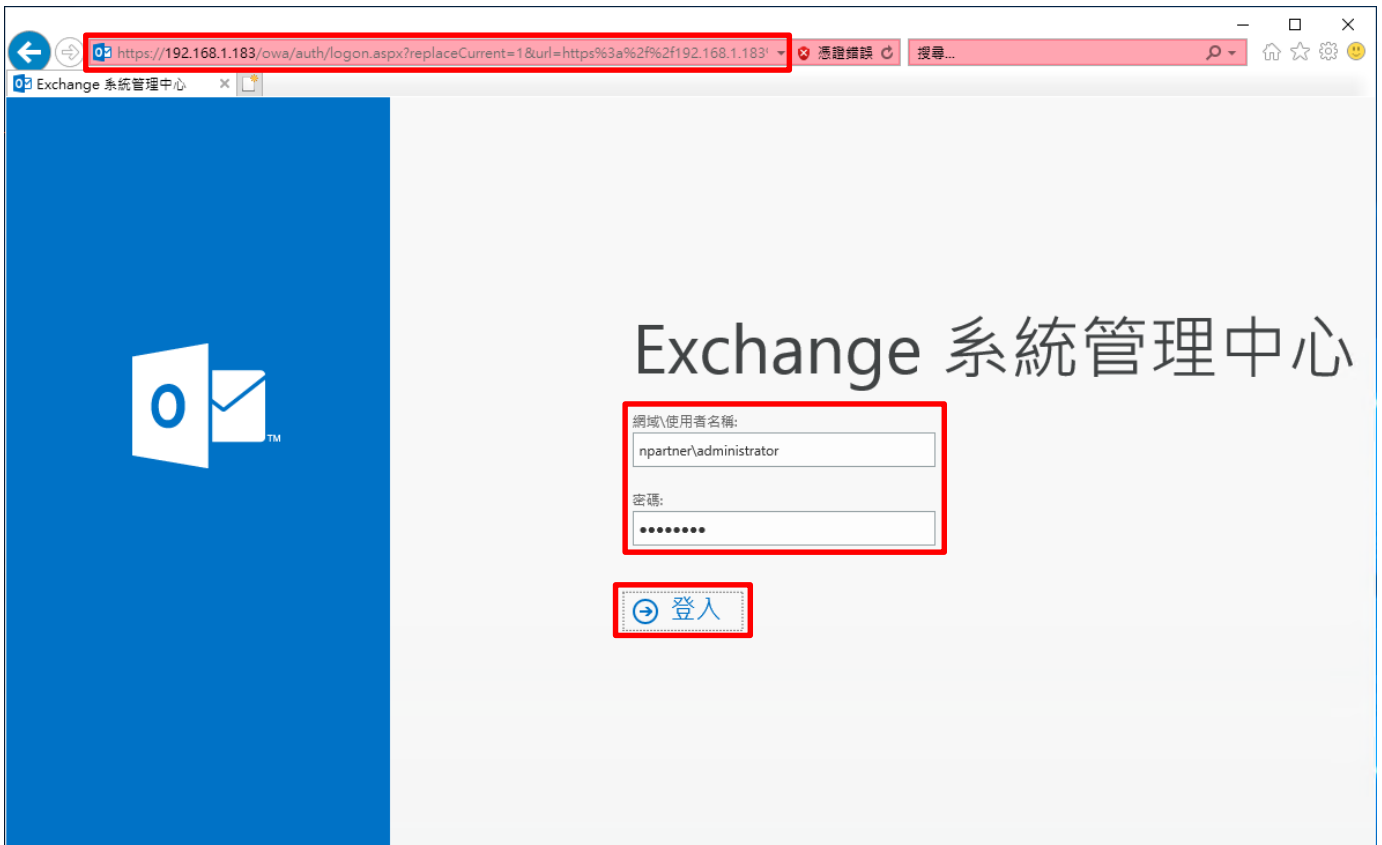
6. Exchange 2019

可選擇 [Exchange 系統管理中心] 或 [Exchange 管理命令介面] 確認啟用郵件追蹤記錄。

6.1 Exchange Message Tracking Log

6.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <https://ExchangeIP/ecp> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]



(2) 點選 [伺服器] -> [伺服器] -> 選擇 [Mailbox 伺服器] -> 點選 [編輯]

Exchange 系統管理中心

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

混合

伺服器 資料庫 資料庫可用性群組 虛擬目錄 憑證

名稱	伺服器角色	版本	
EXCH2019	信箱	Version 15.2 (Build ...)	EXCH2019 信箱 Version 15.2 (Build 330.5) 標準試用版 試用 輸入產品金鑰

已選取 1 個, 共 1 個

(3) 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=95fc12aa-c374-49ca-b 憑證錯誤

EXCH2019

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\Transport...

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\Transport...

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=95fc12aa-c374-49ca-b 100%

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 EXCH2019 | Select-Object *Track*

A screenshot of a terminal window titled '機器: Exch2019.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 #10:
Unix 使用者應該很熟悉波浪字元 (~)。 它代表根目錄的捷徑。 若要知道它預設的評估結果, 請輸入:
Dir ~
您可以將它作為有用的捷徑:
Cp SomeFile "~\My Documents"
詳細資訊: 連線至 Exch2019.npartner.local。
詳細資訊: 已連線至 Exch2019.npartner.local。
[PS] C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Exchange Server 2019>Get-TransportService EXCH2019 | 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.

6.2 IIS log

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



(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]

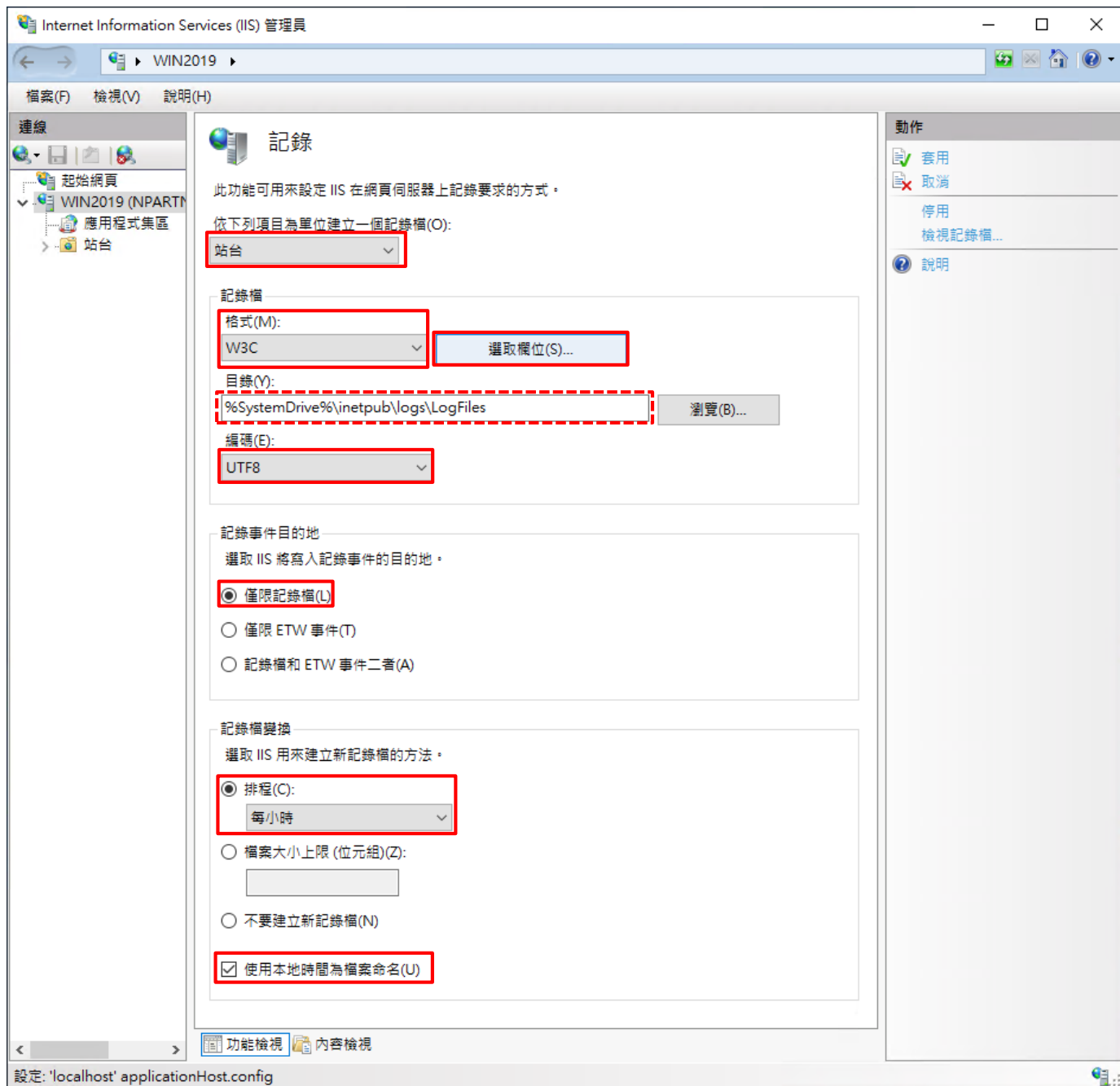


(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程:

[Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select

Fields(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 [Add Field(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) 編輯欄案(E)...

確定 取消

- (5) 輸入欄位名稱: **X-Forwarded-For** -> 選擇來源類型: [Request Header(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))

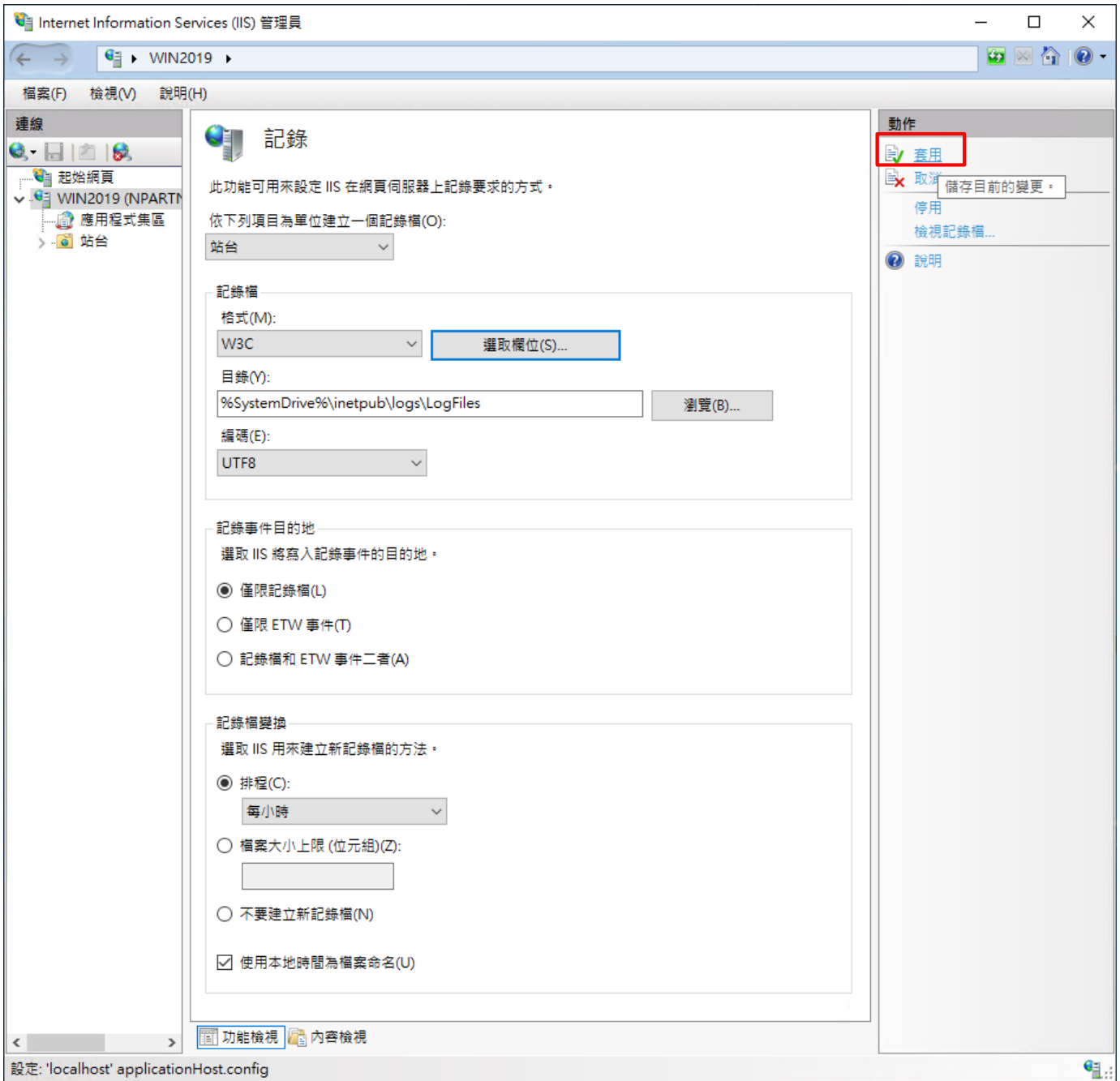
自訂欄位(C):

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

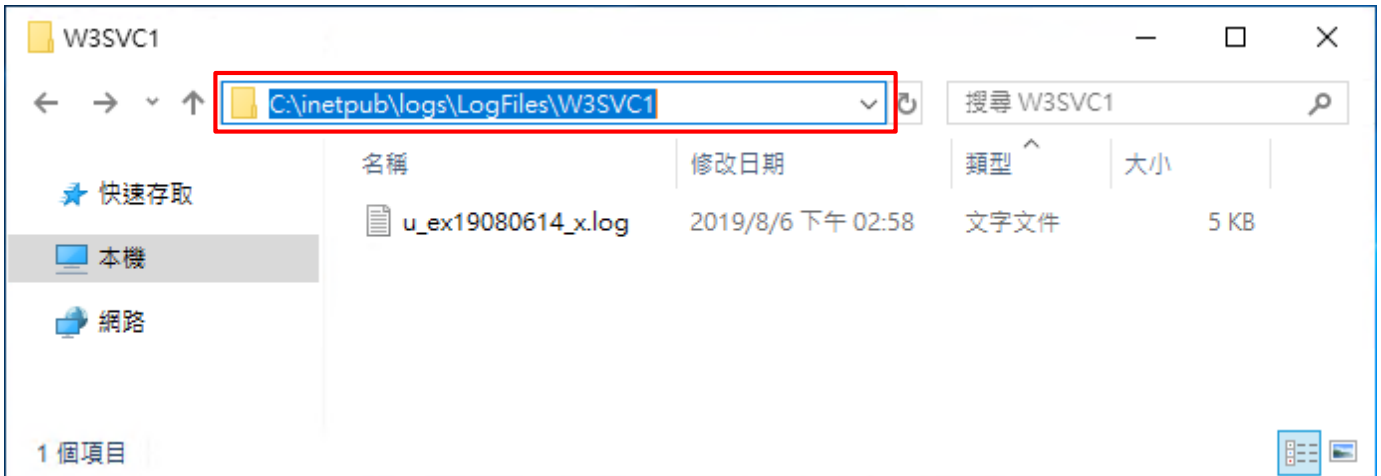
新增欄位(A)... 移除欄位(R) 編輯檔案(E)...

確定 取消

(7) 按下 [Apply(套用)]



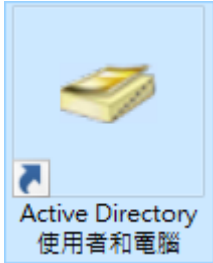
(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log



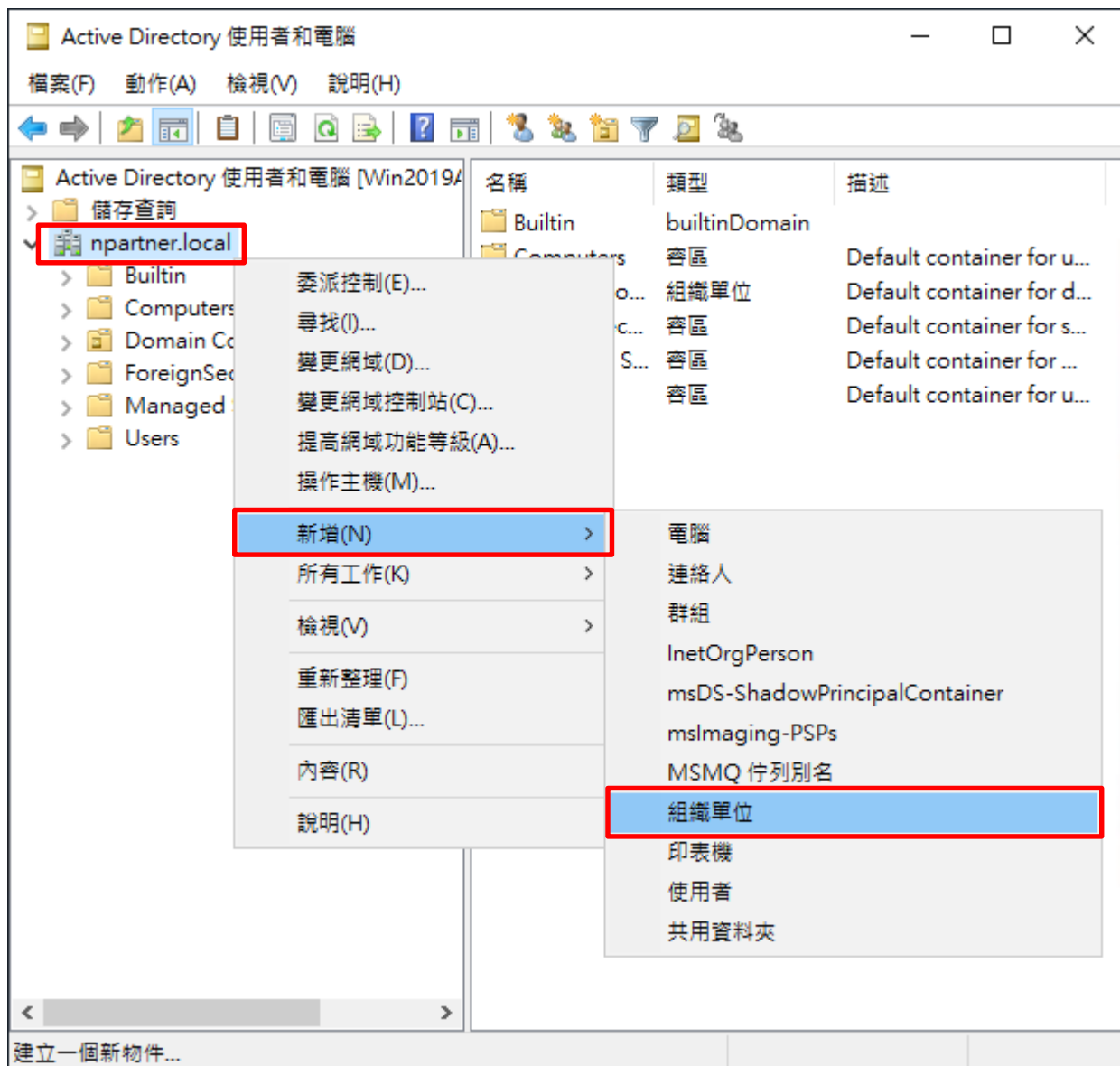
6.3 Event log

6.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱: Servers -> 按下 [確定]

新增物件 - 組織單位

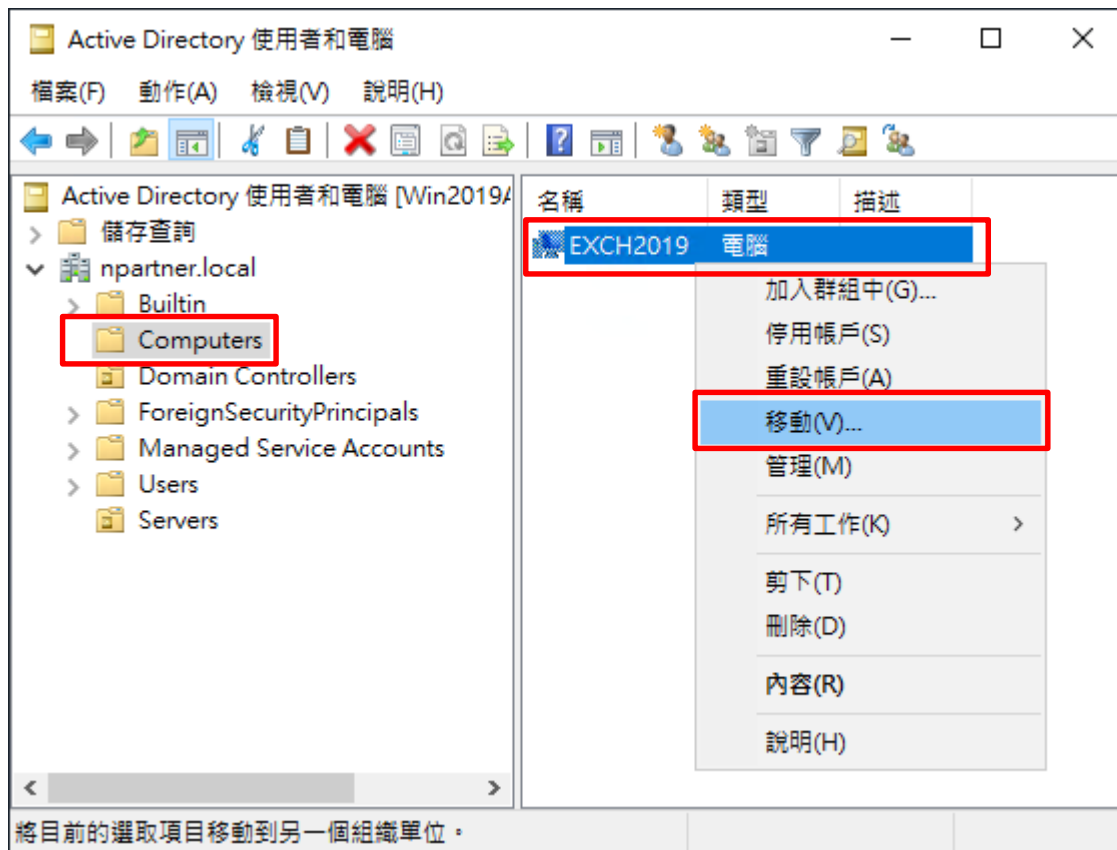
建立在: npartner.local/

名稱(A):
Servers

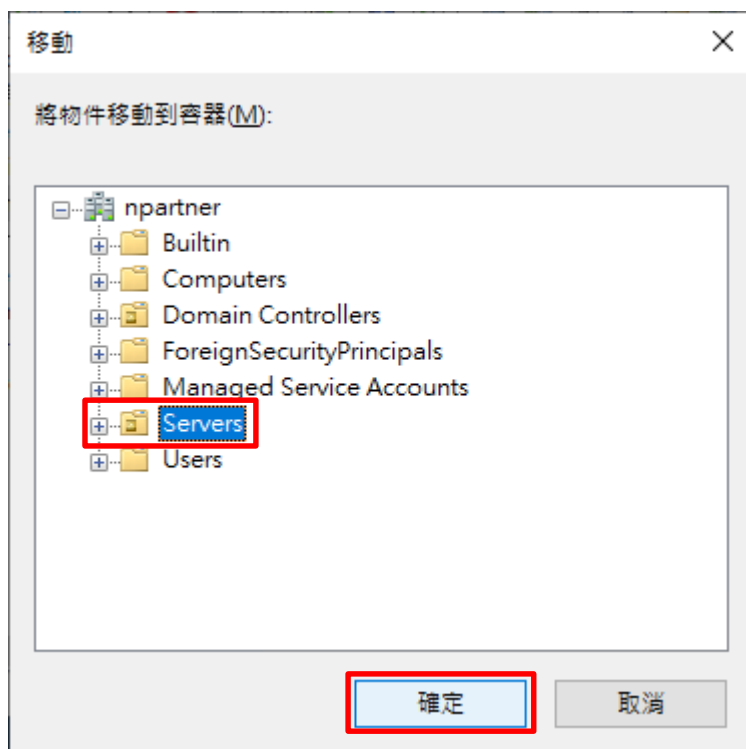
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Exch2019)] 上按滑鼠右鍵 -> 點選 [移動]

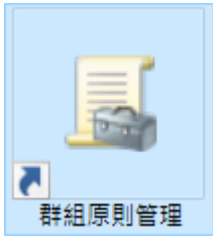


(5) 點選 [Servers] 組織單位 -> 按下 [OK]

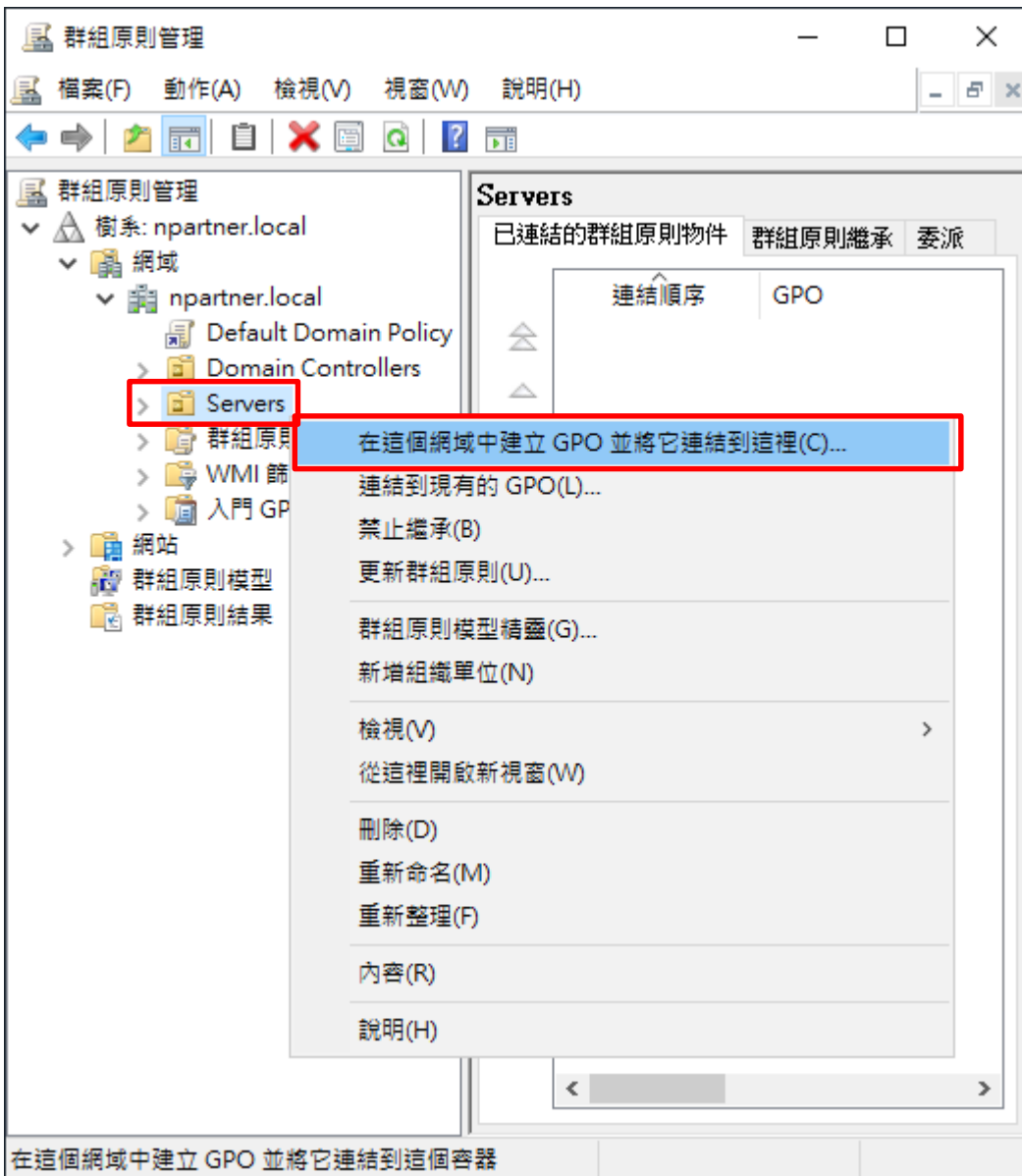


6.3.2 群組原則(Group Policy Management)

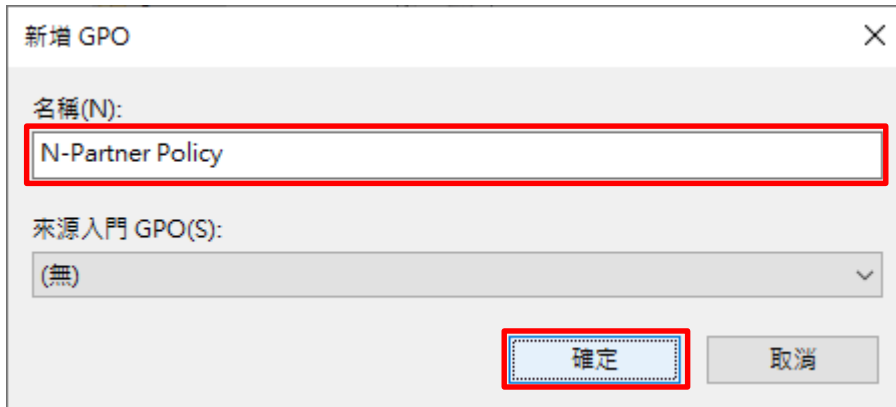
(1) 開啟 [群組原則管理]



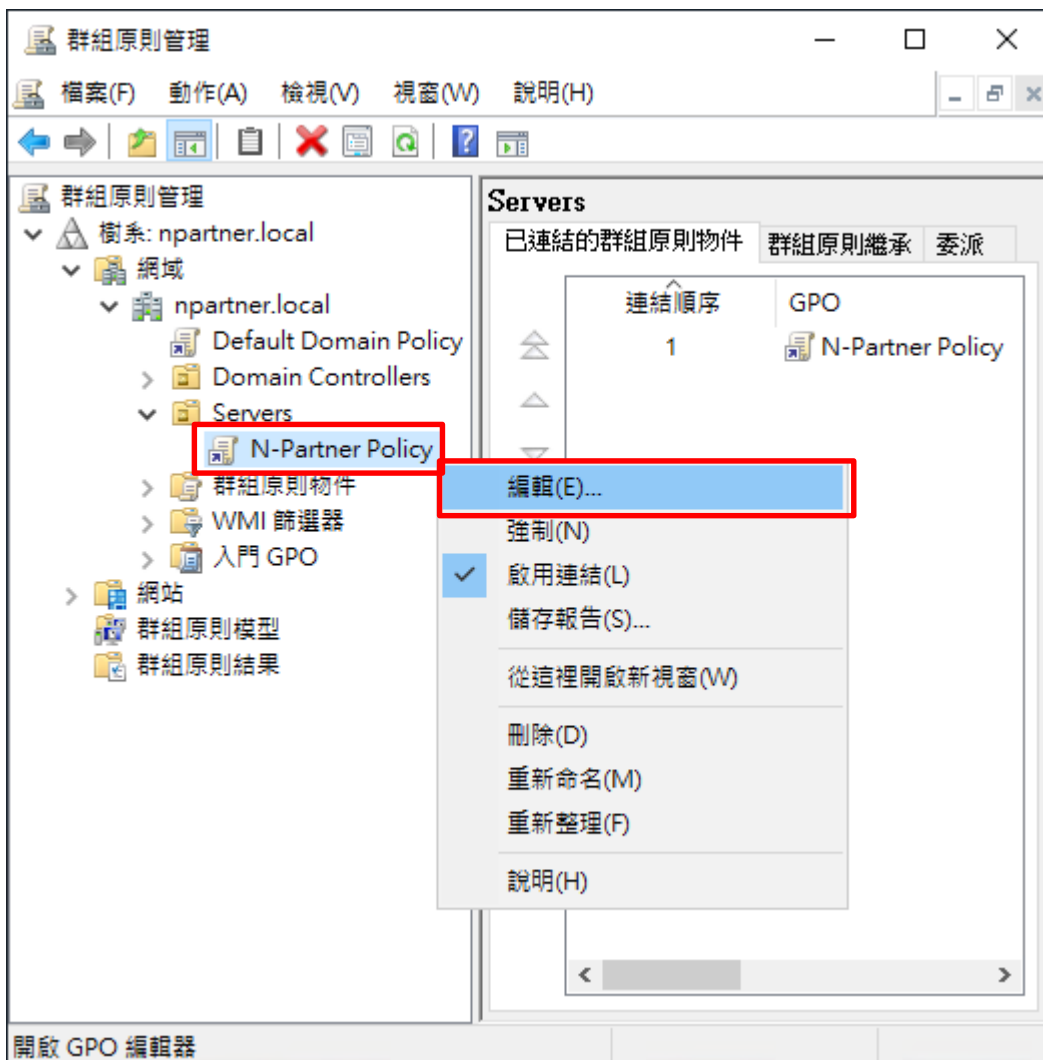
(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到這裡]



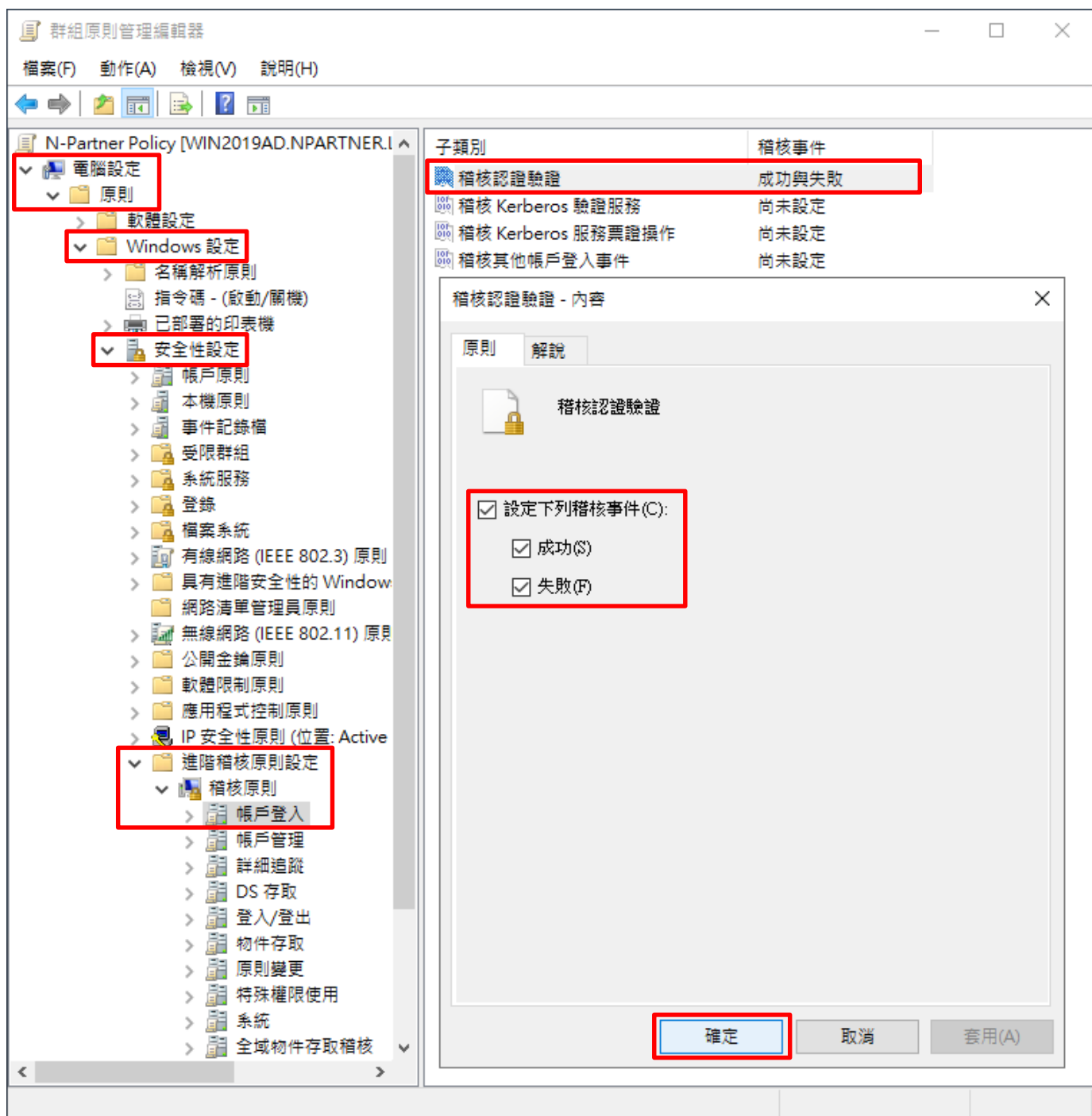
(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]



(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]



- (5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]



- (6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -> 點選 [稽核其他帳戶管理事件], [稽核使用者帳戶管理] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

子類別	稽核事件
稽核應用程式群組管理	尚未設定
稽核電腦帳戶管理	尚未設定
稽核發佈群組管理	尚未設定
稽核其他帳戶管理事件	成功與失敗
稽核安全性群組管理	尚未設定
稽核使用者帳戶管理	成功與失敗

稽核使用者帳戶管理 - 內容

原則 解說

稽核使用者帳戶管理

設定下列稽核事件(C):

- 成功(S)
- 失敗(F)

確定 取消 套用(A)

- (7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -> 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

The screenshot displays the Group Policy Management console for the 'N-Partner Policy [WIN2019AD.NPARTNER.LOC]'. The left-hand navigation pane shows the following path: **電腦設定** (Computer Settings) > **原則** (Policies) > **軟體設定** (Software Settings) > **Windows 設定** (Windows Settings) > **名稱解析原則** (Name Resolution Policies) > **指令碼 - (啟動/關機)** (Scripts - (Startup/Shutdown)) > **已部署的印表機** (Deployed Printers) > **安全性設定** (Security Settings) > **帳戶原則** (Account Policies) > **本機原則** (Local Policies) > **事件記錄檔** (Event Logs) > **受限群組** (Restricted Groups) > **系統服務** (System Services) > **登錄** (Logon) > **檔案系統** (File System) > **有線網路 (IEEE 802.3) 原則** (Wired Network (IEEE 802.3) Policies) > **具有進階安全性的 Windows D** (Windows Defender) > **網路清單管理員原則** (Network List Management Policies) > **無線網路 (IEEE 802.11) 原則** (Wireless Network (IEEE 802.11) Policies) > **公開金鑰原則** (Public Key Policies) > **軟體限制原則** (Software Restriction Policies) > **應用程式控制原則** (Application Control Policies) > **IP 安全性原則 (位置: Active Dir** (IP Security Policies (Location: Active Directory)) > **進階稽核原則設定** (Advanced Audit Policy Settings) > **稽核原則** (Audit Policies) > **登入/登出** (Logon/Logoff).

The right-hand pane shows the 'Logon' policy configuration. The '子類別' (Subcategory) column lists various audit events, and the '稽核事件' (Audit Events) column shows their status. The following events are checked (indicated by a blue icon):

子類別	稽核事件
稽核帳戶鎖定	成功與失敗
稽核使用者/裝置宣告	尚未設定
稽核群組成員資格	尚未設定
稽核 IPsec 延伸模式	尚未設定
稽核 IPsec 主要模式	尚未設定
稽核 IPsec 快速模式	尚未設定
稽核登出	成功與失敗
稽核登入	成功與失敗
稽核網路原則伺服器	尚未設定
稽核其他登入/登出事件	尚未設定
稽核特殊登入	尚未設定

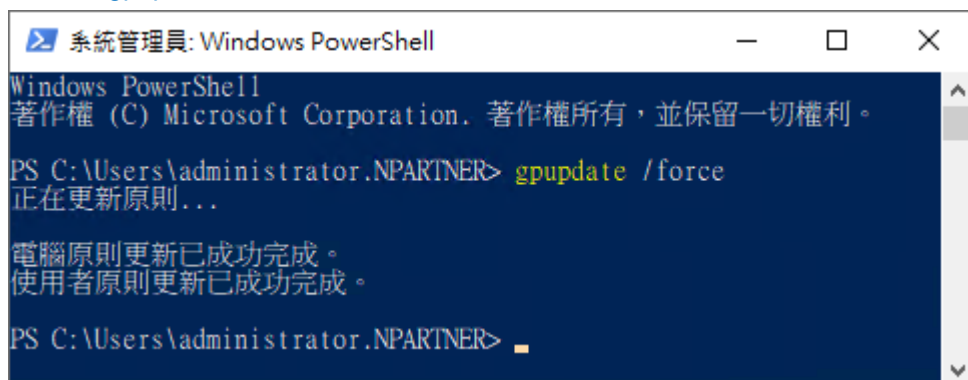
The '稽核登入 - 內容' (Logon - Content) dialog box is open, showing the '原則' (Policy) tab. It displays the '稽核登入' (Logon) policy and the following checked events:

- 設定下列稽核事件(C):
 - 成功(S)
 - 失敗(F)

The '確定' (OK) button is highlighted with a red box.

(8) 在 Exchange Server 伺服器更新群組原則

PS C:\> gpupdate /force



```
系統管理員: Windows PowerShell
Windows PowerShell
著作權 (C) Microsoft Corporation. 著作權所有，並保留一切權利。
PS C:\Users\administrator.NPARTNER> gpupdate /force
正在更新原則...
電腦原則更新已成功完成。
使用者原則更新已成功完成。
PS C:\Users\administrator.NPARTNER> █
```

(9) 在 AD 網域伺服器，產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱，-Path 指定報告文件的路徑和檔名。

PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2019.html -ReportType html -Computer EXCH2019



```
系統管理員: Windows PowerShell
Windows PowerShell
著作權 (C) Microsoft Corporation. 著作權所有，並保留一切權利。
PS C:\Users\Administrator> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2019.html -ReportType html -Computer EXCH2019
RsopMode       : Logging
Namespace      : \\EXCH2019\Root\Rsop\NSFE6A5754_9EF2_44F0_9F17_56276496BB40
LoggingComputer : EXCH2019
LoggingUser    : NPARTNER\administrator
LoggingMode     : Computer
PS C:\Users\Administrator> █
```

(10) 開啟 [C:\tmp\EXCH2019.html] 確認啟用 [N-Partner Policy]

群組原則結果

NPARTNER\EXCH2019
資料收集: 2019/9/4 上午 11:59:15 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/安全性選項 顯示

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

進階稽核設定 隱藏

帳戶登入 隱藏

原則	設定	優勢 GPO
稽核認證驗證	成功, 失敗	N-Partner Policy

帳戶管理 隱藏

原則	設定	優勢 GPO
稽核其他帳戶管理事件	成功, 失敗	N-Partner Policy
稽核使用者帳戶管理	成功, 失敗	N-Partner Policy

登入/登出 隱藏

原則	設定	優勢 GPO
稽核帳戶鎖定	成功, 失敗	N-Partner Policy
稽核登出	成功, 失敗	N-Partner Policy
稽核登入	成功, 失敗	N-Partner Policy

7. N-Reporter

7.1 Exchange Message Tracking log

(1) 新增 Exchange Server 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]

The screenshot displays the N-Reporter web interface. On the left, a dark blue sidebar contains a menu with '設備管理' (Device Management) highlighted, and a sub-menu where '設備樹狀圖' (Device Tree) is selected. The main content area shows the '設備樹狀圖' page with a search bar and a table. The table has a header with columns: '操作', '所屬領域', 'IP', '設備名稱', '設備種類', '資料格式', 'Model', '狀態', '介面', '硬碟', '建立時間', and '瀏覽'. The table body is empty, displaying '未知設備 (0)' and 'No data!'. A red box highlights the '新增' (Add) button in the table's toolbar. At the bottom, there is a pagination bar showing '25' items per page, '第 0 共 0 頁', and a footer with 'Copyright © 2009 N-Partner. All rights reserved.' and '上次登錄時間 2019-08-16 10:15:00'.

(2) 設定 Exchange message tracking 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] 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
Exchange_Mail-192.168.1.183

IP
192.168.1.183

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Exchange 2013

Facility
(2) mail system

編碼方式
UTF-8

設備進階設定

設備 Icon
icon-host

Login Account

Login Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

確定 取消

7.2 Exchange Event log

(1) 新增 Exchange Event 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]

The screenshot shows the N-Partner web interface. On the left sidebar, the '設備管理' (Device Management) menu is highlighted with a red box, and its sub-menu '設備樹狀圖' (Device Tree) is also highlighted. The main content area displays the '設備樹狀圖' page. At the top of this page, there is a search bar and a set of action buttons. The '新增' (Add) button, which is a green square with a white plus sign, is highlighted with a red box. Below the search bar, there is a table with columns: '操作', '所屬領域', 'IP', '設備名稱', '設備種類', '資料格式', 'Model', '狀態', '介面', '硬碟', '建立時間', and '瀏覽'. The table currently shows 'Global (0)' and '未知設備 (0)'. The status 'No data!' is displayed in the table area. At the bottom of the page, there is a pagination bar showing '25' items per page, '第 0 共 0 頁', and a footer with 'Copyright © 2009 N-Partner. All rights reserved.' and '上次登錄時間 © 2019-08-16 10:15:00'.

(2) 設定 Exchange event 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: [(20) local use 4 (local4)] -

> 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

Exchange_Event-192.168.1.183

IP

192.168.1.183

設備種類

Syslog Flow SNMP

Syslog 相關設定

資料格式

Windows

Facility

(20) local use 4 (local4)

編碼方式

UTF-8

設備進階設定

設備 Icon

icon-host

Login Account

Login Password

接收狀態

啟用 停用

暫無資料告警

啟用 Syslog/Flow 暫無資料告警

確定 **取消**

7.3 Exchange IIS log

(1) 新增 Exchange IIS 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]

The screenshot displays the N-Partner management interface. On the left, a navigation menu is visible with '設備管理' (Device Management) selected, and its sub-menu '設備樹狀圖' (Device Tree) highlighted with a red box. The main content area shows the '設備樹狀圖' page with a search bar and a table. The table has a header row with columns: '操作', '所屬領域', 'IP', '設備名稱', '設備種類', '資料格式', 'Model', '狀態', '介面', '硬碟', '建立時間', and '瀏覽'. Below the header, there is a row for 'Global (0)' and a row for '未知設備 (0)'. The table body is empty, displaying 'No data!'. A red box highlights the '新增' (Add) button in the top right corner of the table area. The footer of the page contains the copyright information 'Copyright © 2009 N-Partner. All rights reserved.' and the login time '上次登錄時間 2019-08-16 10:15:00'.

(2) 設定 Exchange IIS 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
Exchange_IIS-192.168.1.183

IP
192.168.1.183

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
IIS

Facility
(22) local use 6 (local6)

編碼方式
UTF-8

設備進階設定

設備 Icon
icon-host

Login Account

Login Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

確定 **取消**



連絡資訊

TEL: +886-4-23752865

FAX: +886-4-23757458

技術問題請洽：

Email: support@npartnertech.com

Skype: [support@npartnertech.com](https://www.skype.com/en/contacts/skype/support@npartnertech.com)

業務相關請洽：

Email: sales@npartnertech.com

