



N-Partner



如何設定 Windows File 事件記錄

V004

2019/01/16



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	6.1.1 組織單位設定	87
1. NXLog.....	3	6.1.2 群組原則設定	91
1.1 NXLog 架構	3	6.2 工作群組.....	96
1.2 NXLog 安裝	4	6.3 稽核資料夾設定	100
1.3 NXLog 設定檔	6	7. N-Reporter.....	107
1.3.1 Windows 2000 – 2003.....	6	7.1 Windows 2000 – 2003.....	108
1.3.2 Windows 2008 or higher.....	8	7.2 Windows 2008 or higher.....	109
1.4 NXLog 啟動服務	10		
1.4.1 Windows 2000 – 2003.....	10		
1.4.2 Windows 2008 or higher.....	11		
2. Windows 2003.....	12		
2.1 網域	12		
2.1.1 組織單位設定	12		
2.1.2 群組原則設定	15		
2.2 工作群組	20		
2.3 稽核資料夾設定	24		
3. Windows 2008.....	28		
3.1 網域	28		
3.1.1 組織單位設定	28		
3.1.2 群組原則設定	31		
3.2 工作群組	36		
3.3 稽核資料夾設定	40		
4. Windows 2012.....	45		
4.1 網域	45		
4.1.1 組織單位設定	45		
4.1.2 群組原則設定	50		
4.2 工作群組	55		
4.3 稽核資料夾設定	59		
5. Windows 2016.....	66		
5.1 網域	66		
5.1.1 組織單位設定	66		
5.1.2 群組原則設定	71		
5.2 工作群組	76		
5.3 稽核資料夾設定	80		
6. Windows 2019.....	87		
6.1 網域	87		



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 Windows File 事件記錄。

NXLog 工具將 Windows 事件記錄轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。

此文件適用於作業系統的 Windows Server 2003 / 2008 / 2012 / 2016 / 2019 版本。

稽核原則建議：Windows 稽核原則設定，協助偵測入侵，SCM(Security Compliance Manager) 基準建議。

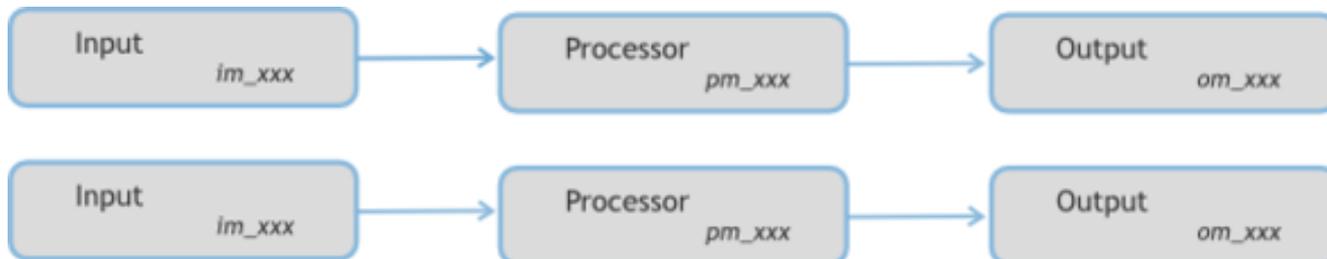
<https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

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>

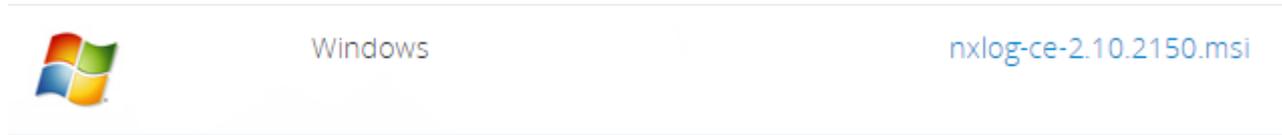


1.2 NXLog 安裝

(1) 下載 NXLog

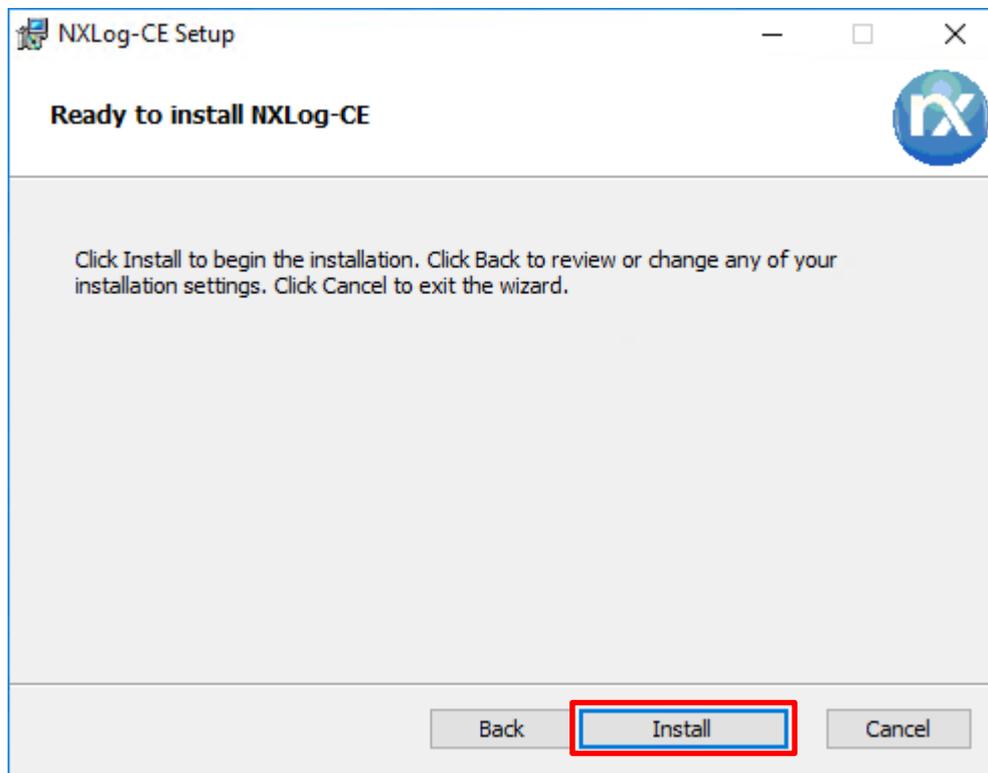
前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 nxlog-ce-x.xx.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]



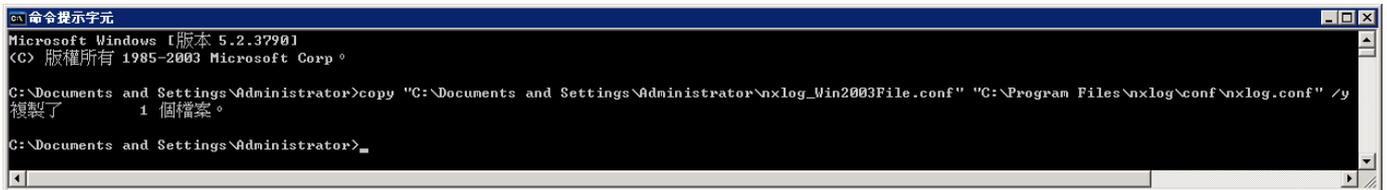
(3) 下載並覆蓋 NXLog 設定檔

(3.1) Windows 2000 - 2003

下載連結 https://www.npartnertech.com/download/tech/nxlog_Win2003File.conf -> 開啟 [命令提示字元] -> 輸入

```
copy "C:\Documents and Settings\Administrator\nxlog_Win2003File.conf" "C:\Program Files\nxlog\conf\nxlog.conf"
```

/y 覆蓋 NXLog 設定檔



```
命令提示字元
Microsoft Windows [版本 5.2.3790.1]
(C) 版權所有 1985-2003 Microsoft Corp.

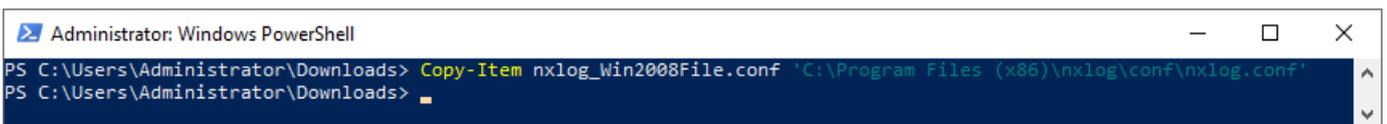
C:\Documents and Settings\Administrator>copy "C:\Documents and Settings\Administrator\nxlog_Win2003File.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
複製了
    1 個檔案。

C:\Documents and Settings\Administrator>
```

(3.2) Windows 2008 or higher

下載連結 https://www.npartnertech.com/download/tech/nxlog_Win2008File.conf -> 開啟 [Windows PowerShell] ->

輸入 `Copy-Item nxlog_Win2008File.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'` 覆蓋 NXLog 設定檔



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads> Copy-Item nxlog_Win2008File.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'
PS C:\Users\Administrator\Downloads>
```

1.3 NXLog 設定檔

1.3.1 Windows 2000 - 2003

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud    192.168.1.184
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 windows File 2000 - 2003 Event Log use the following:
<Input in_eventlog>
  Module im_mseventlog
  ReadFromLast TRUE
  SavePos TRUE Exec parse_syslog_bsd(); \
    if ($EventID == 560 or $EventID == 561 or $EventID == 562 or $EventID == 563 or $EventID == 564 or
$EventID == 565 or $EventID == 566 or $EventID == 567 or $EventID == 568 or $EventID == 569 or $EventID ==
570) { $SyslogFacilityValue = 13; } \
    else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
    else \
    { \
      drop(); \
    }
</Input>

<Output out_eventlog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $Message = string($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>
```



藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud 192.168.3.51
```

本文件範例環境為 32bit 作業系統，若作業系統環境為 64bit 請變更藍色文字部位

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



1.3.2 Windows 2008 or higher

```
# Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.1.184
define ROOT        C:\Program Files (x86)\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 Windows File 2008 or higher 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=5145)]]</Select> \
      <Select Path="Security">*[System[(EventID=5140 or EventID=5142 or EventID=5143 or EventID=5144 or
EventID=5168)]]</Select> \
      <Select Path="Security">*[System[(EventID=4656 or EventID=4658 or EventID=4660 or EventID=4663 or
EventID=4664 or EventID=4985 or EventID=5051 or EventID=4670)]]</Select> \
    </Query> \
  </QueryList>
</Input>

<Output out_eventlog>
  Module om_udp
  Host %NCloud%
  Port 514
  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>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud 192.168.3.51
```

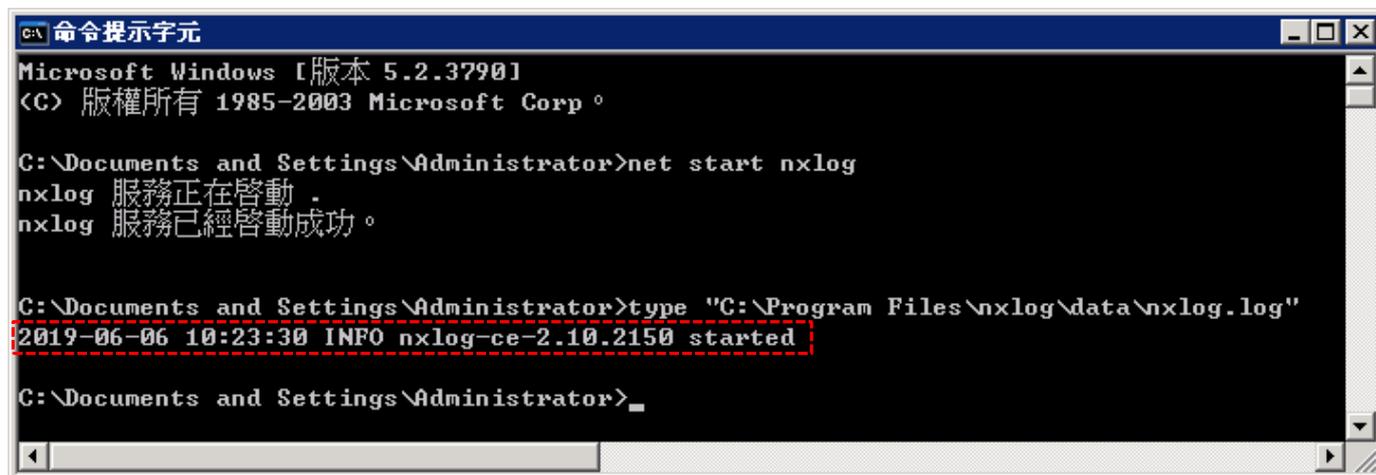


1.4 NXLog 啟動服務

1.4.1 Windows 2000 - 2003

開啟 [命令提示字元] -> 輸入 `net start nxlog` 啟動 nxlog 服務-> 輸入 `type "C:\Program Files\nxlog\data\nxlog.log"`

確認沒有錯誤訊息



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

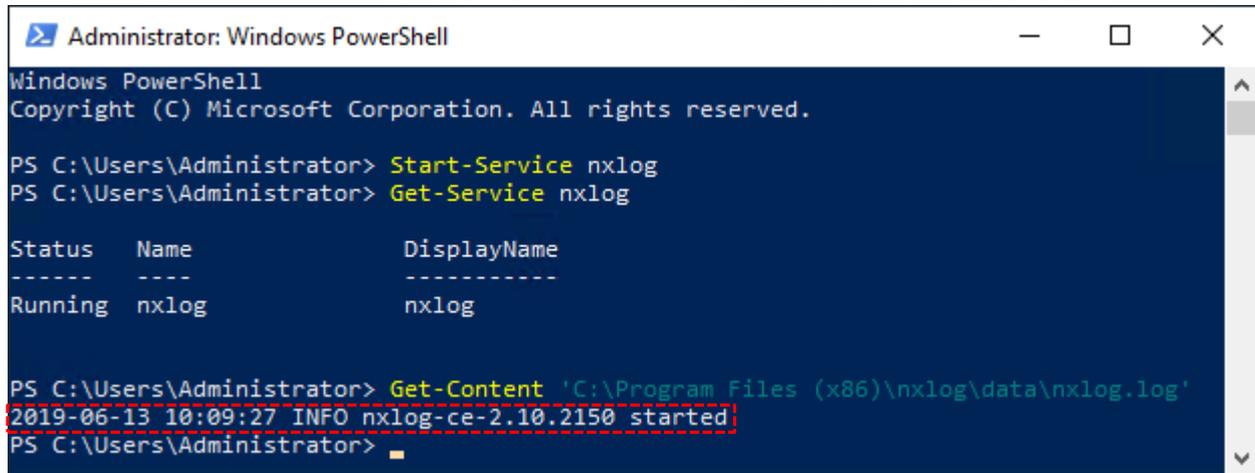
C:\Documents and Settings\Administrator>net start nxlog
nxlog 服務正在啟動。
nxlog 服務已經啟動成功。

C:\Documents and Settings\Administrator>type "C:\Program Files\nxlog\data\nxlog.log"
2019-06-06 10:23:30 INFO nxlog-ce-2.10.2150 started

C:\Documents and Settings\Administrator>
```

1.4.2 Windows 2008 or higher

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 -> 輸入 `Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息



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

PS C:\Users\Administrator> Start-Service nxlog
PS C:\Users\Administrator> Get-Service nxlog

Status      Name          DisplayName
-----
Running     nxlog         nxlog

PS C:\Users\Administrator> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2019-06-13 10:09:27 INFO nxlog-ce-2.10.2150 started
PS C:\Users\Administrator>
```

2. Windows 2003

以下分別為網域和工作群組設定方式。

2.1 網域

2.1.1 組織單位設定

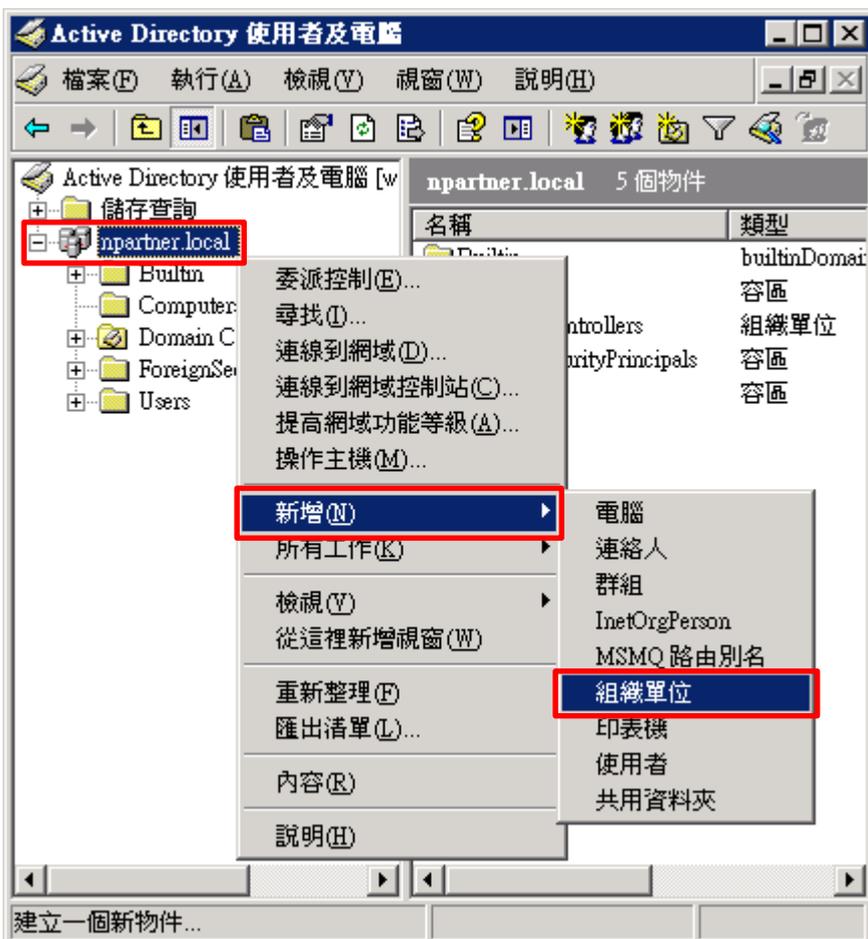
(1) 開啟 AD 使用者和電腦

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]



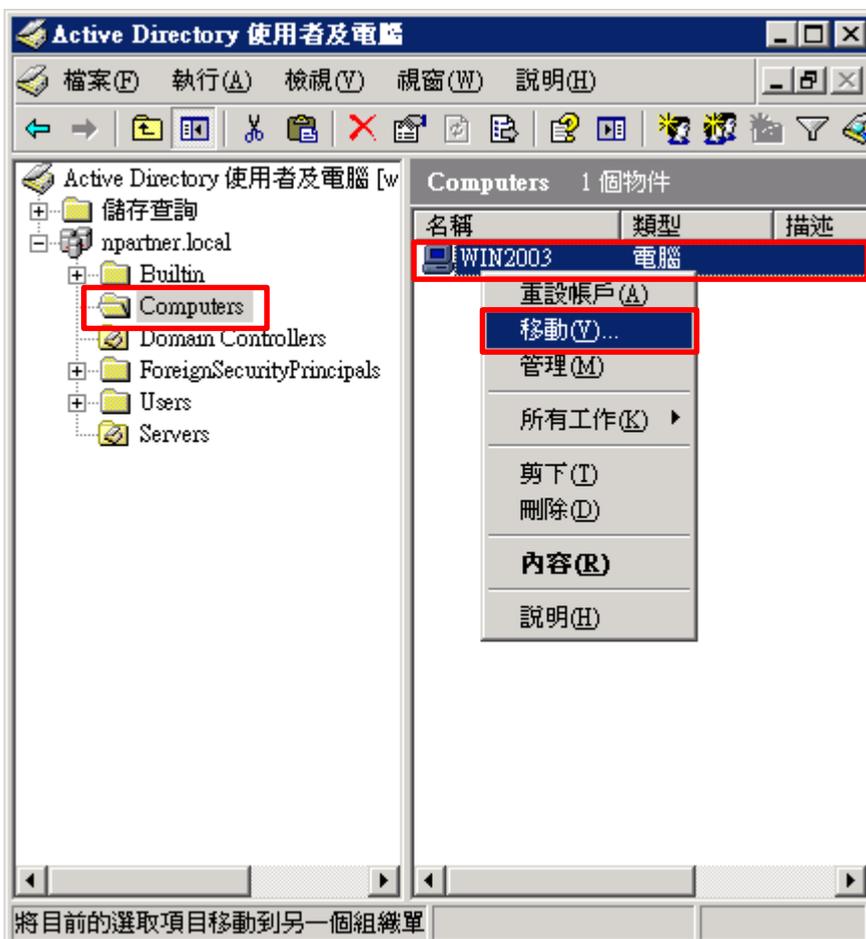
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [電腦名稱(Win2003)] 按滑鼠右鍵 -> 點選 [移動]



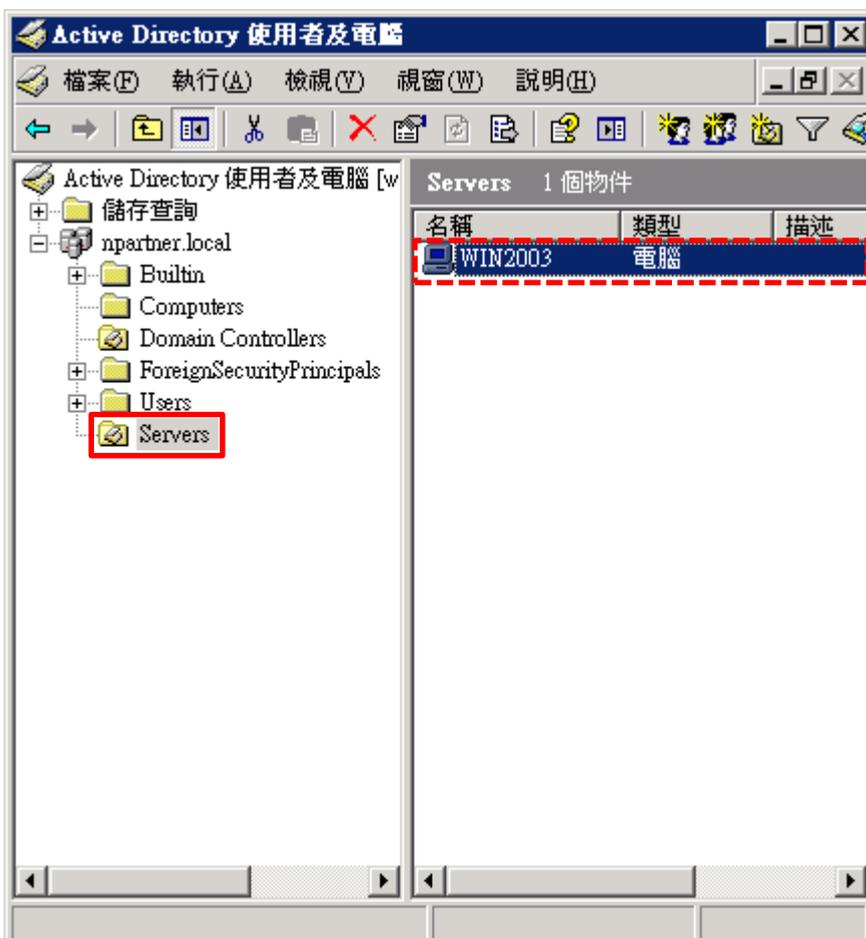
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按下 [確定]



(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位 · 確認 [電腦名稱(Win2003)] 伺服器已移動



2.1.2 群組原則設定

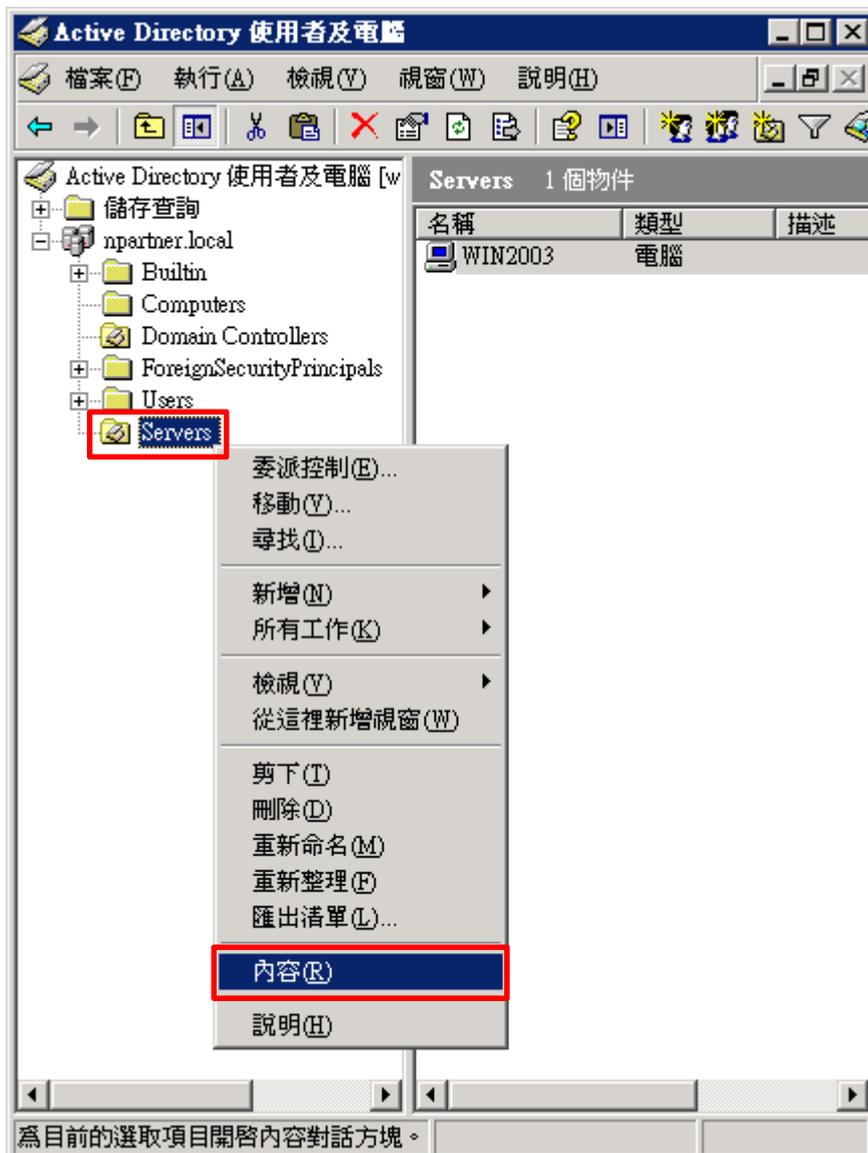
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



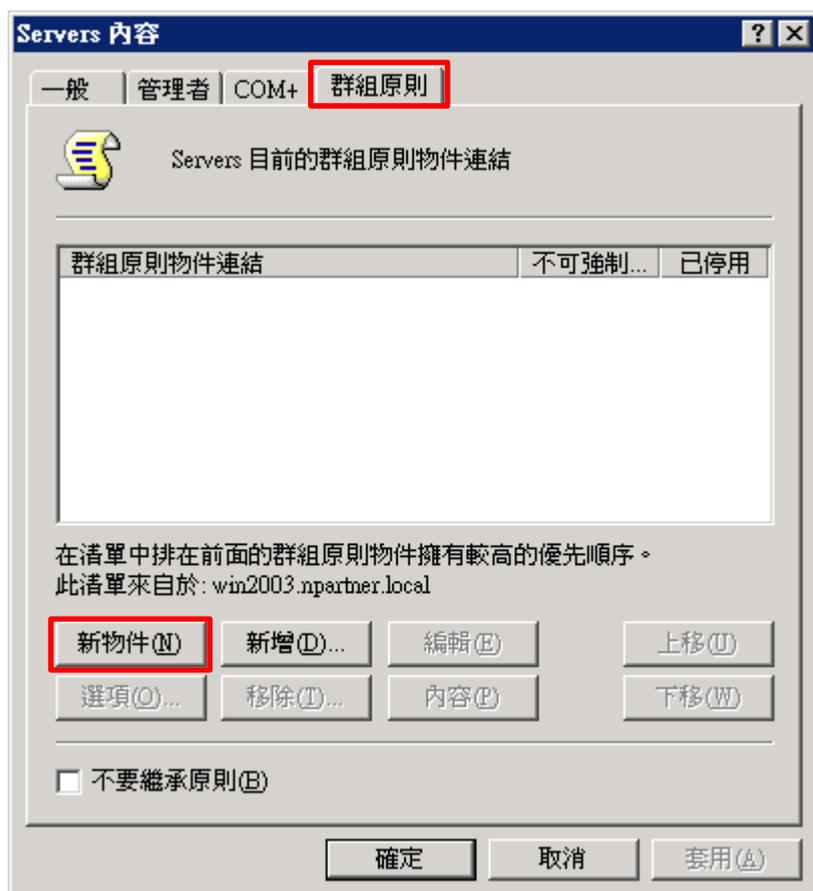
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]



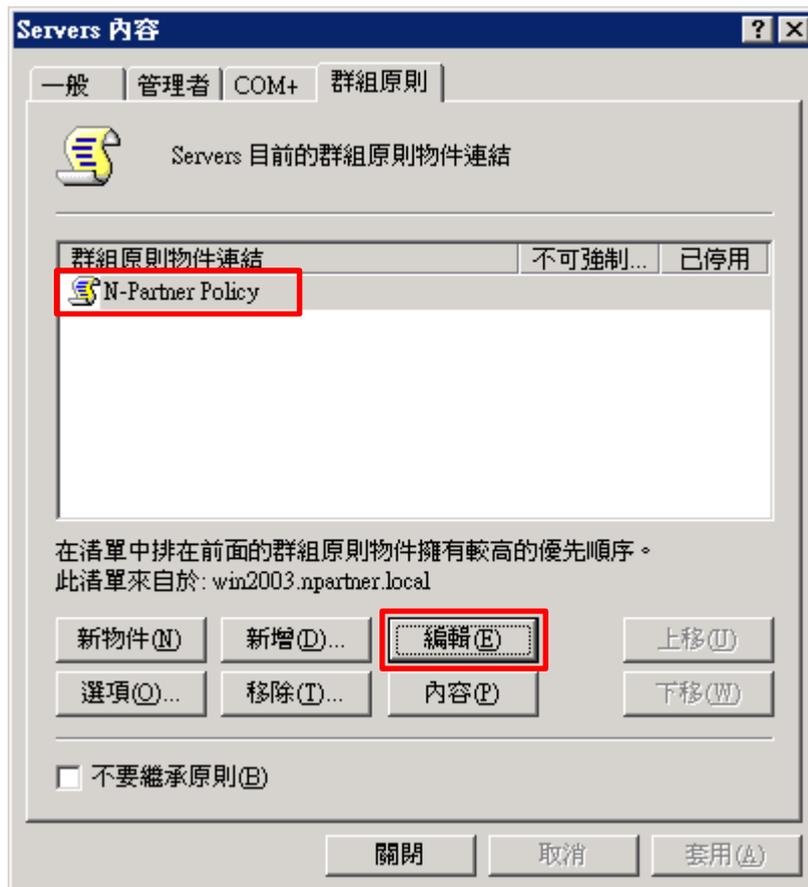
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按下 [新物件]



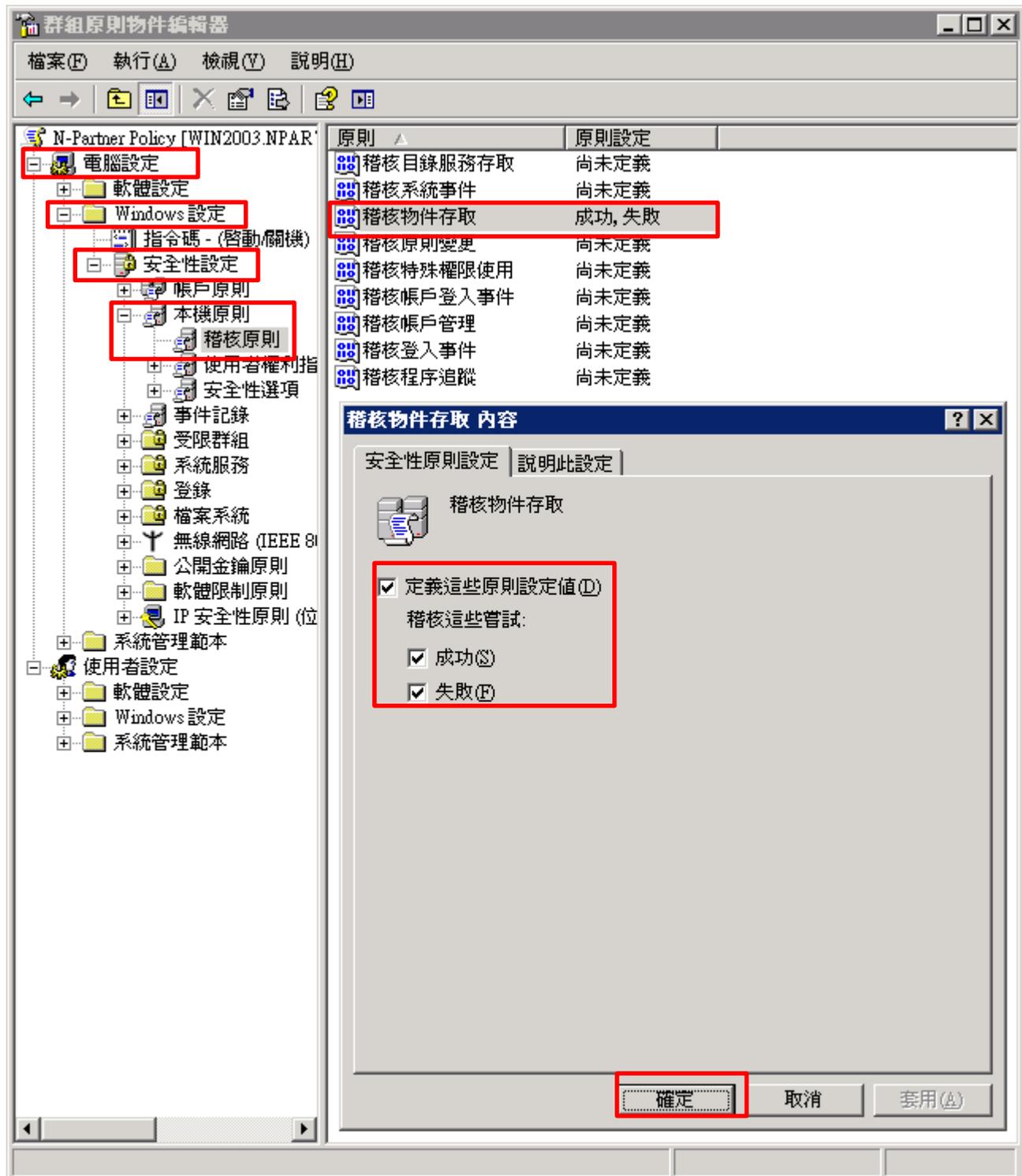
(4) 編輯群組原則物件

輸入群組原則物件名稱 **N-Partner Policy** -> 點選 [編輯]



(5) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按下 [確定]



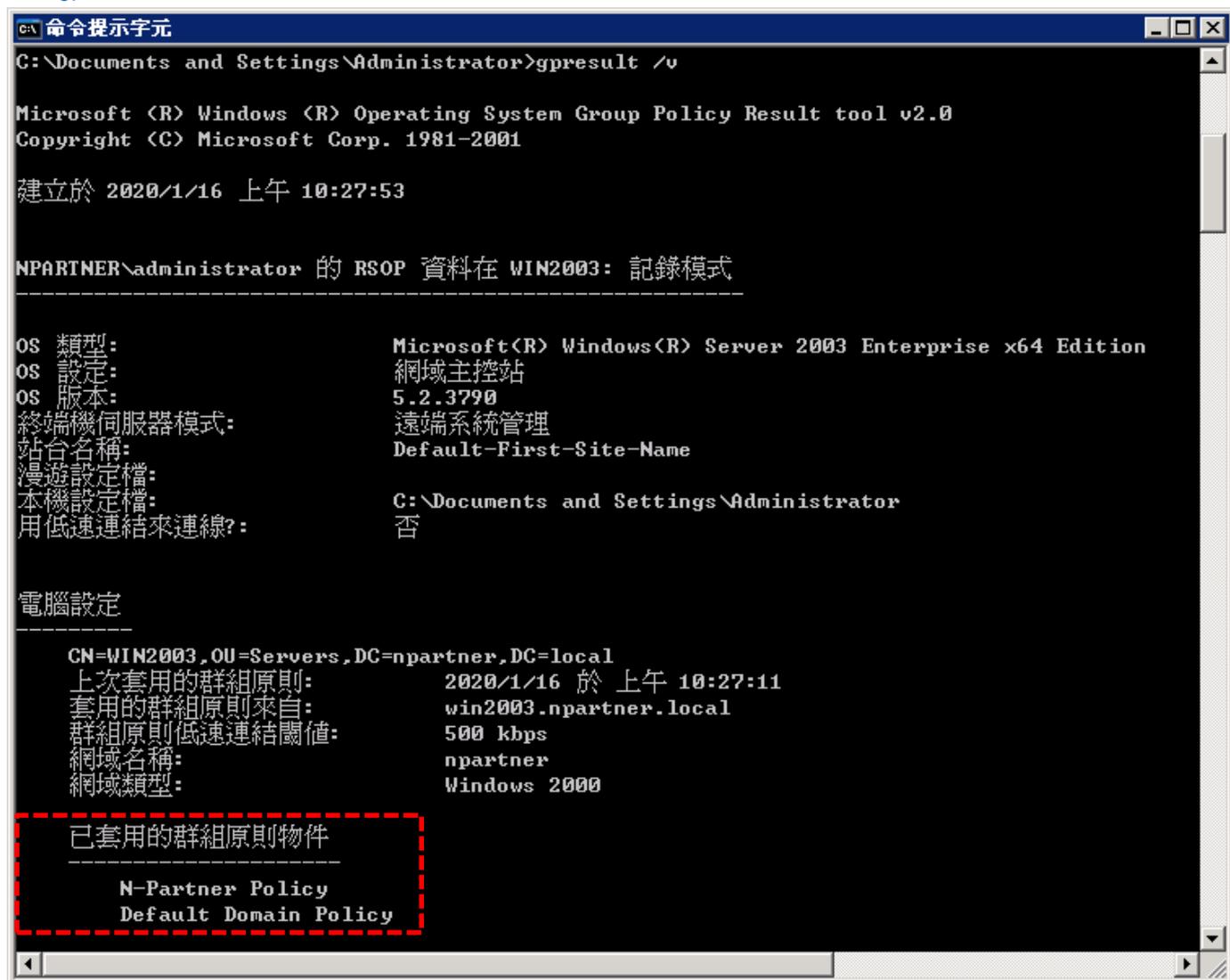
(6) 在 Windows File 伺服器更新群組原則

C:\> gpupdate /force



(7) 查看群組原則套用情形

C:\> gpresult /v



2.2 工作群組

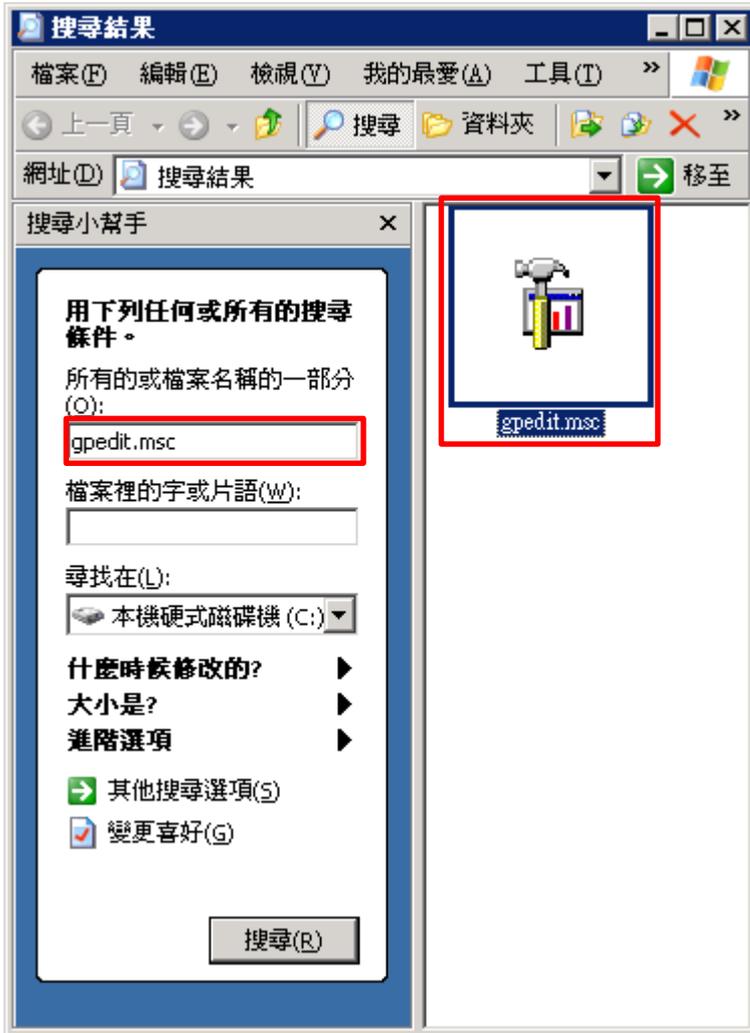
(1) 開啟搜尋

點選 [開始] -> 點選 [搜尋]



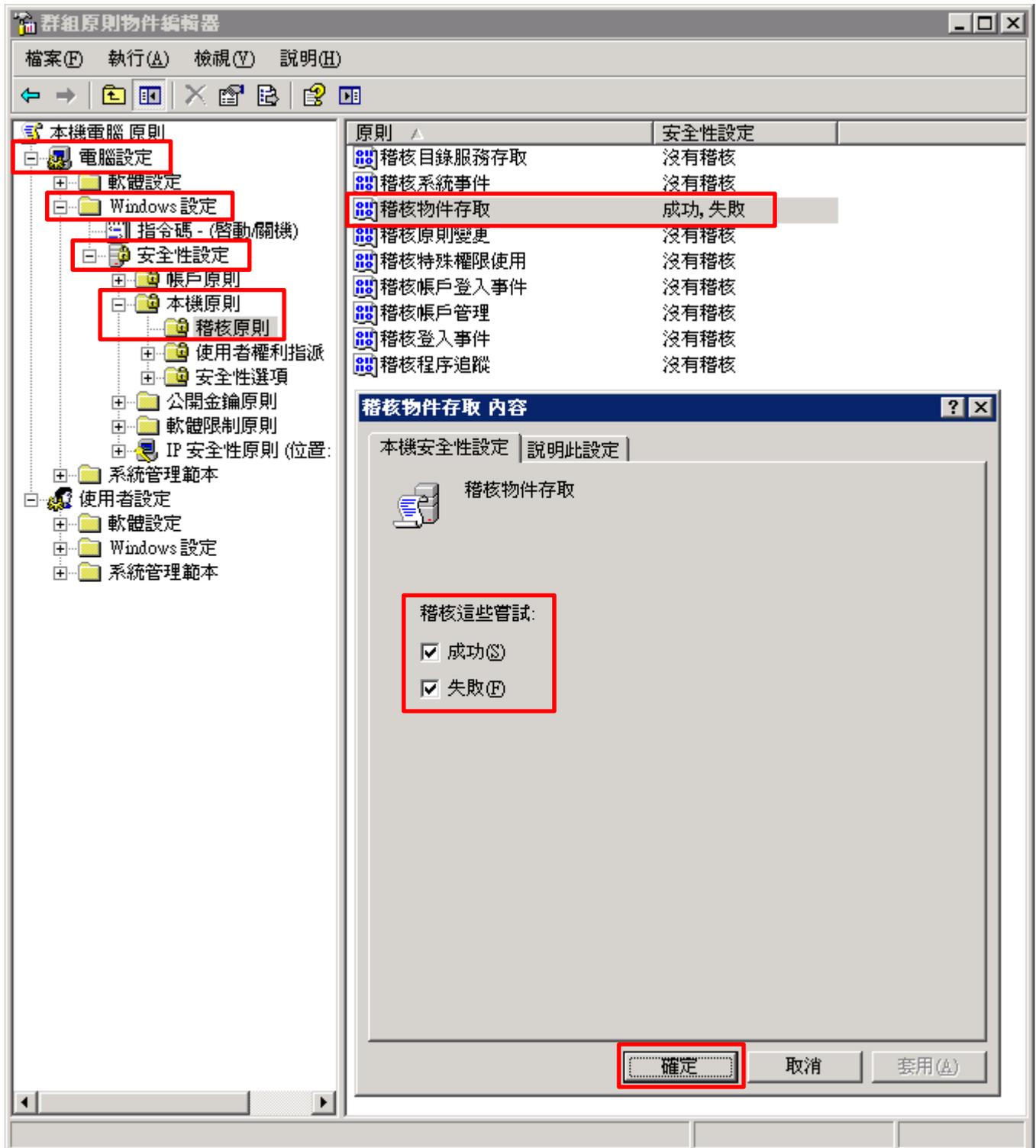
(2) 搜尋群組原則物件編輯器

輸入 `gpedit.msc` -> 執行 `gpedit.msc`



(3) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按下 [確定]



(4) 更新群組原則

C: \> gpupdate /force



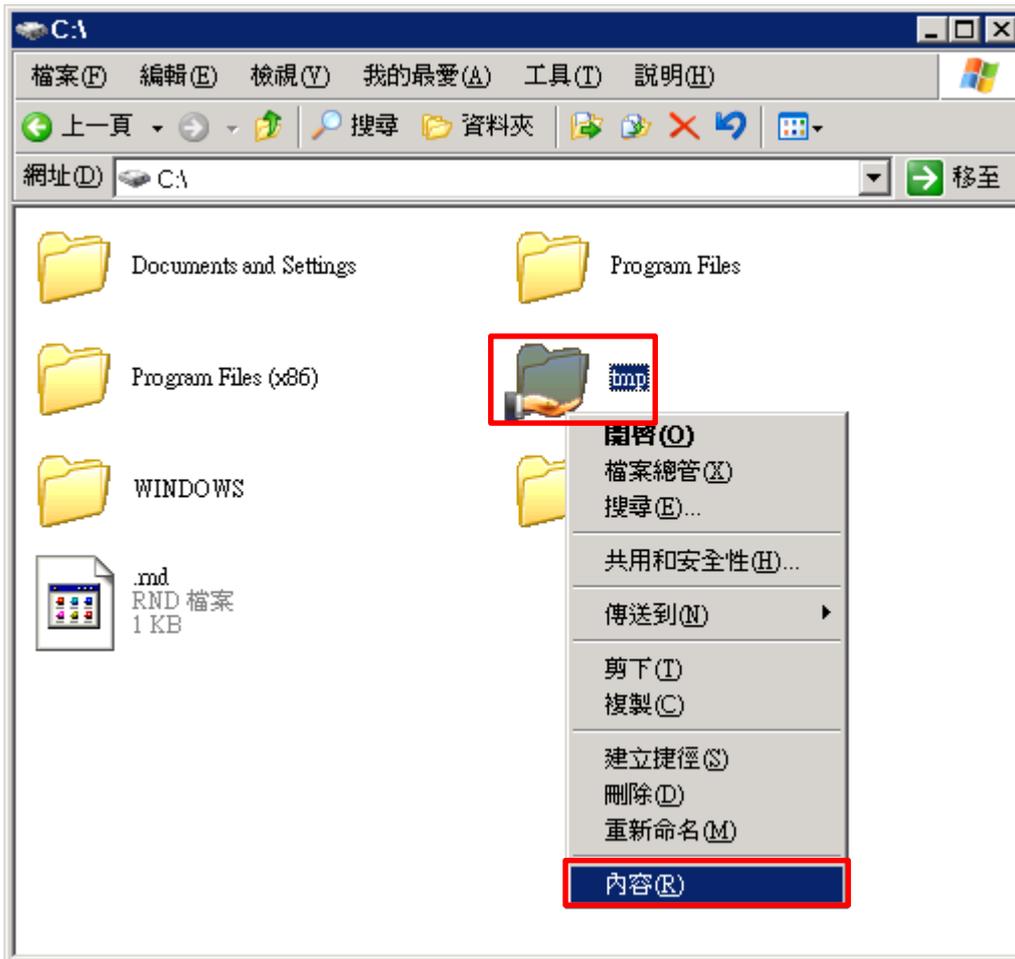
```
命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
正在重新整理原則...
使用者原則重新整理已完成。
電腦原則重新整理已完成。
如果要檢查原則處理中的錯誤，請檢視事件日誌。

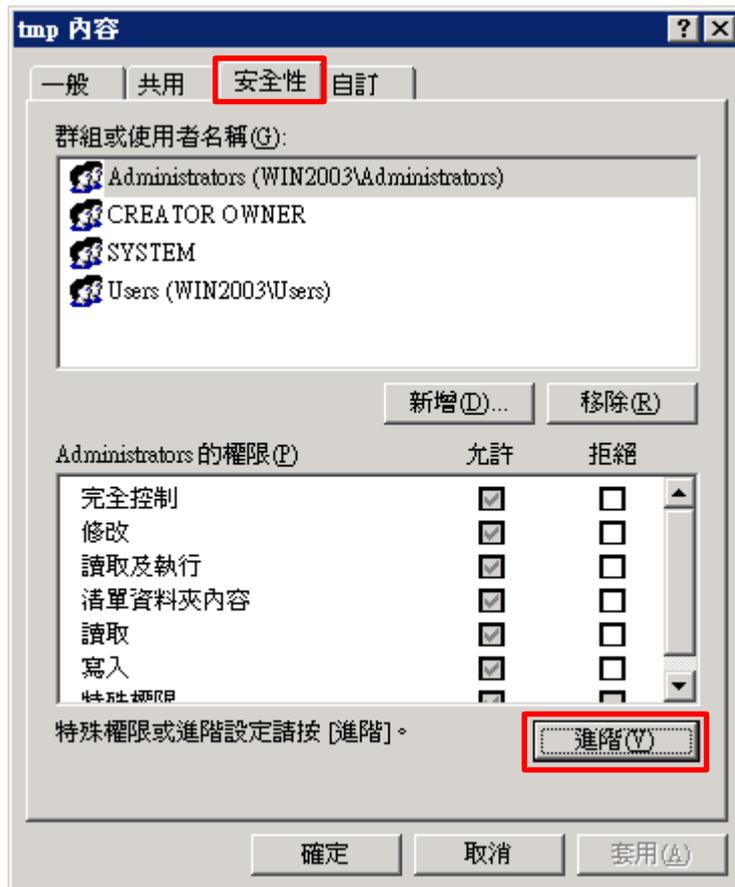
C:\Documents and Settings\Administrator>
```

2.3 稽核資料夾設定

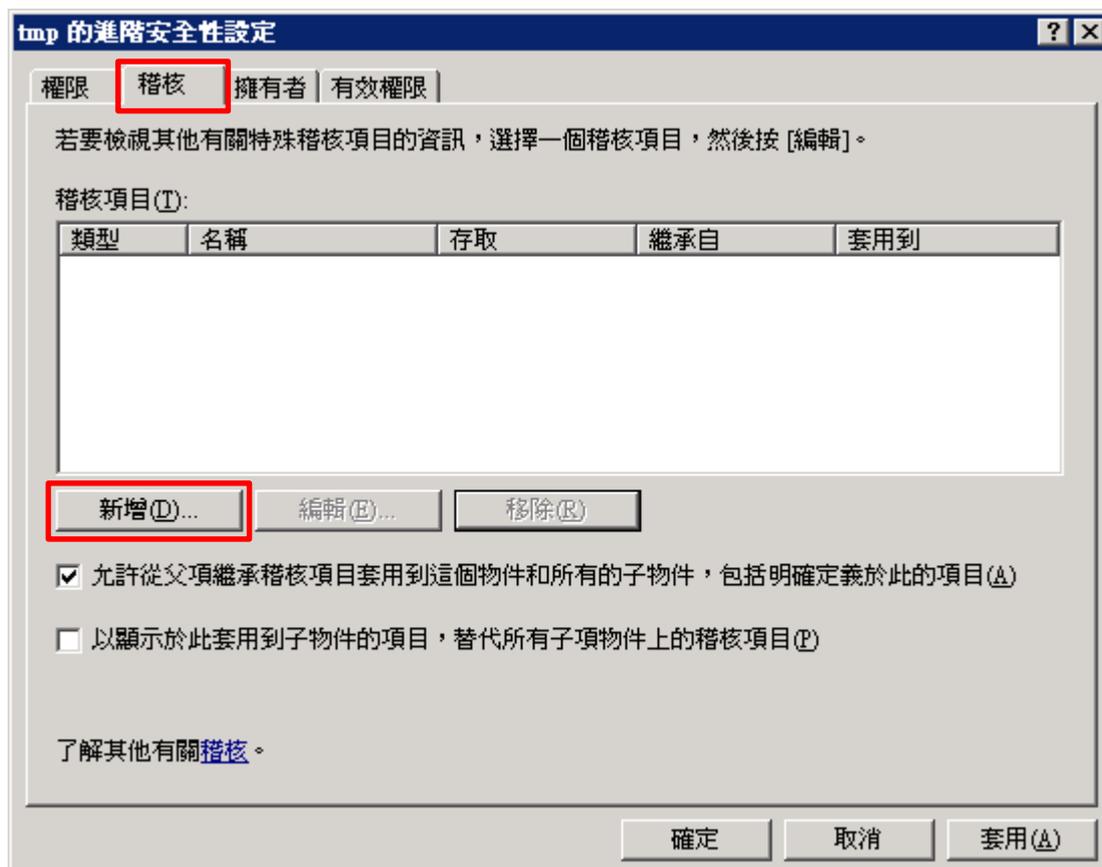
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



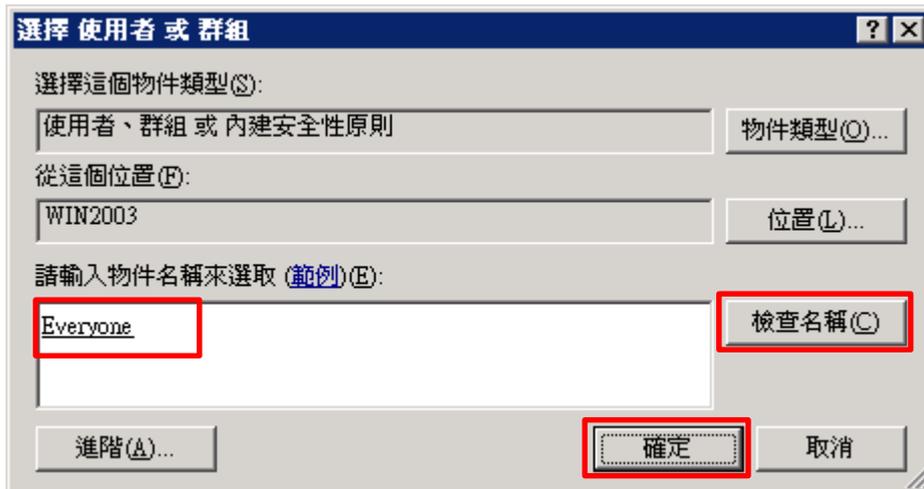
(2) 點選 [安全性] 頁面 -> 按下 [進階]



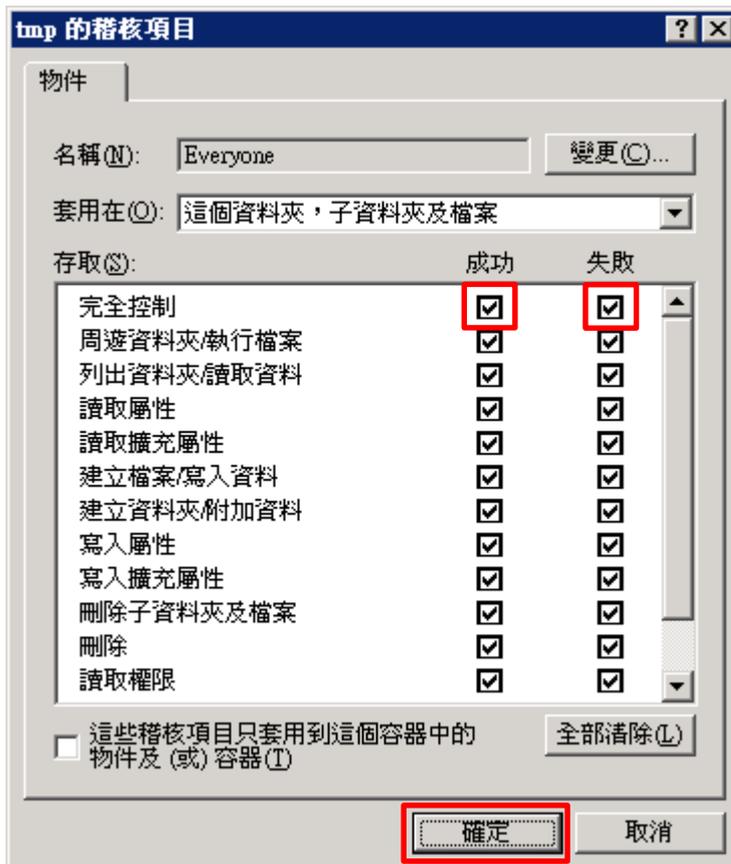
(3) 點選 [稽核] 頁面 -> 按下 [新增]



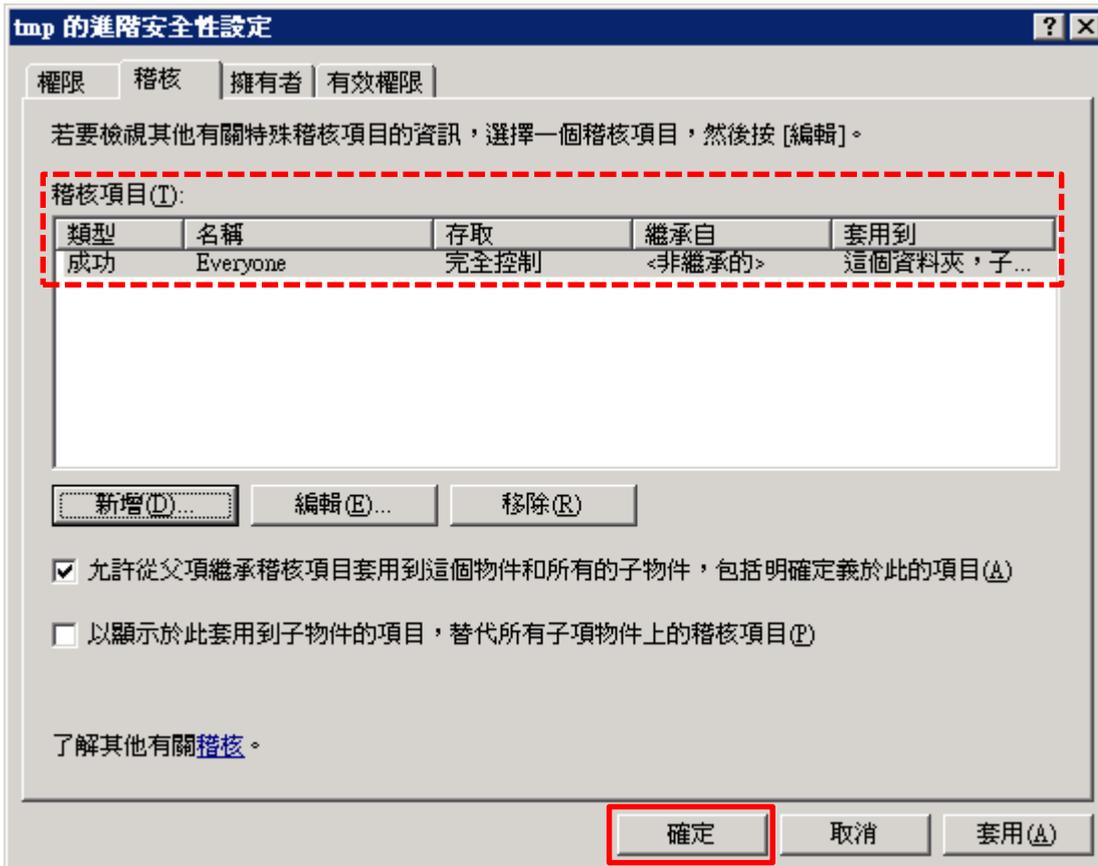
(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



(5) 存取類型 [成功] 和 [失敗] 項目都勾選 [完全控制] -> 按下 [確定]



(6) 稽核項目顯示 Everyone 名稱 -> 按下 [確定]



3. Windows 2008

以下分別為網域和工作群組設定方式。

3.1 網域

3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



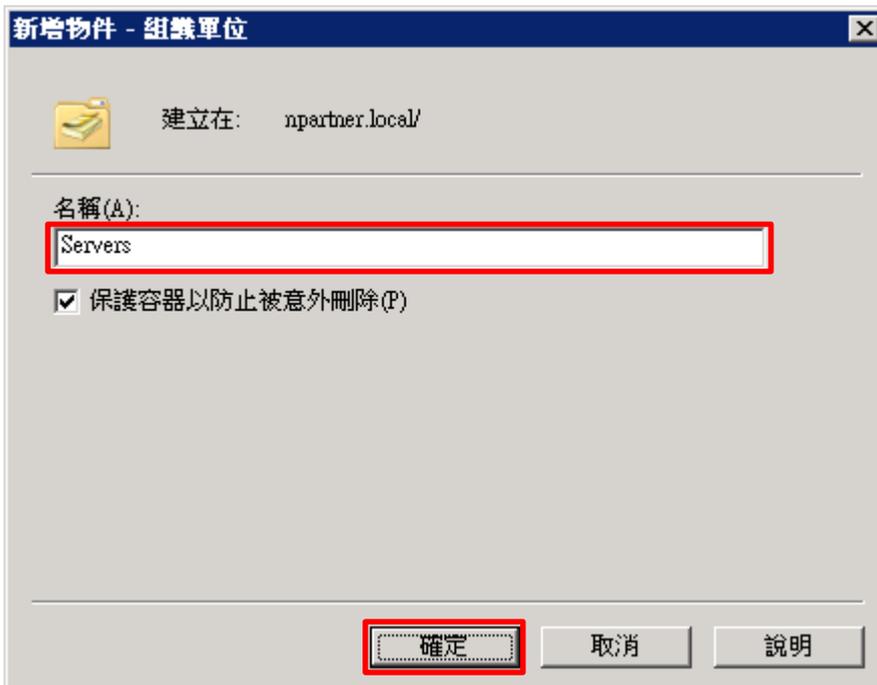
(2) 新增組織單位

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



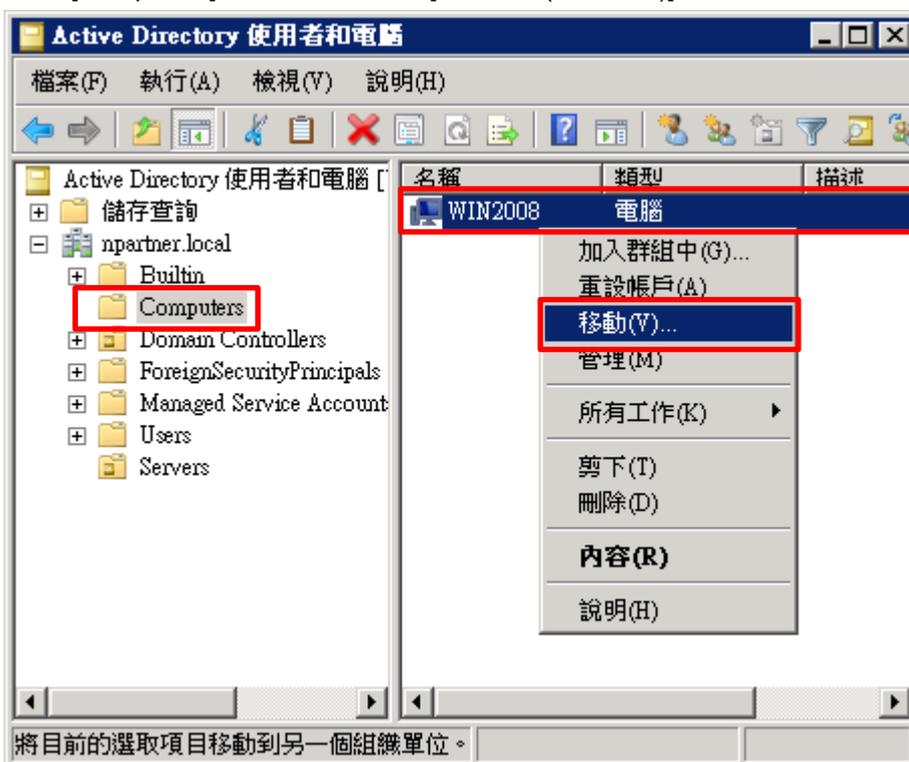
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



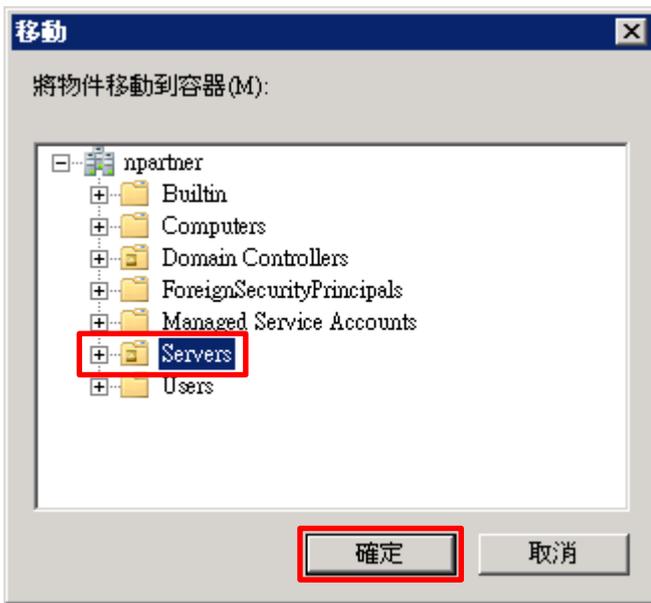
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [電腦名稱(Win2008)] 按滑鼠右鍵 -> 點選 [移動]



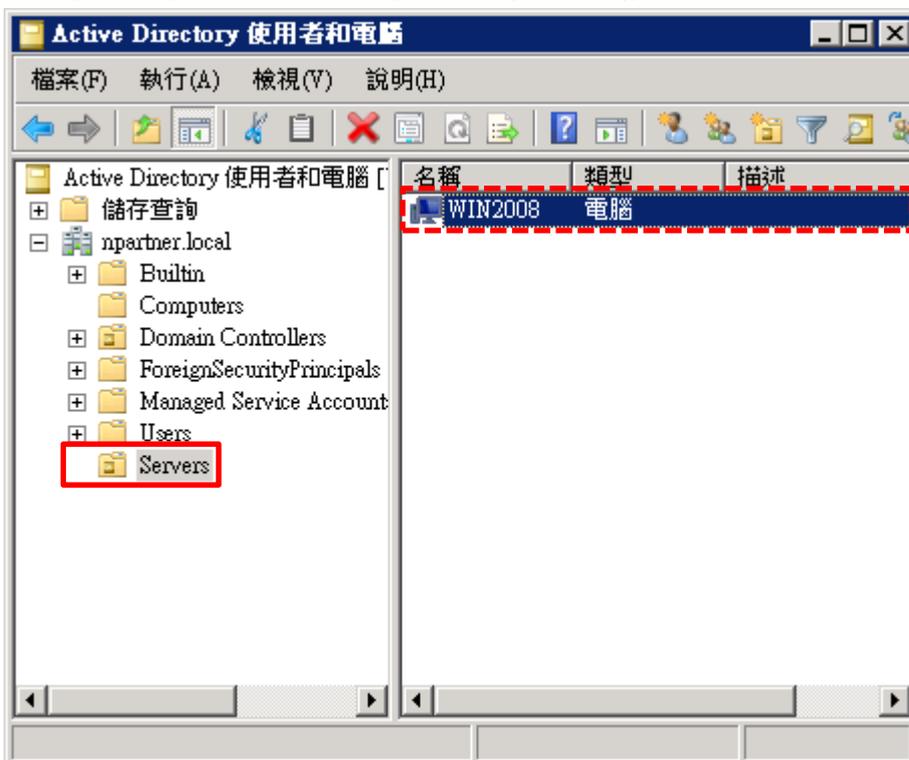
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按下 [確定]



(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位 · 確認 [電腦名稱(Win2008)] 伺服器已移動



3.1.2 群組原則設定

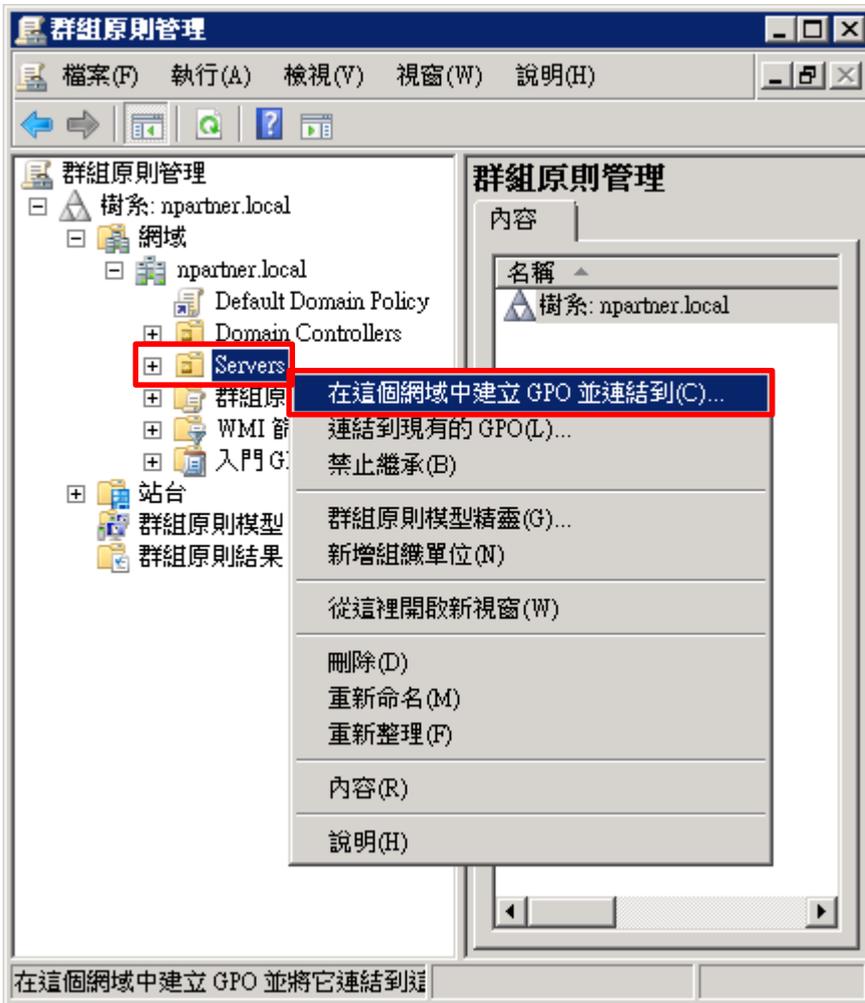
(1) 開啟群組原則管理

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...]



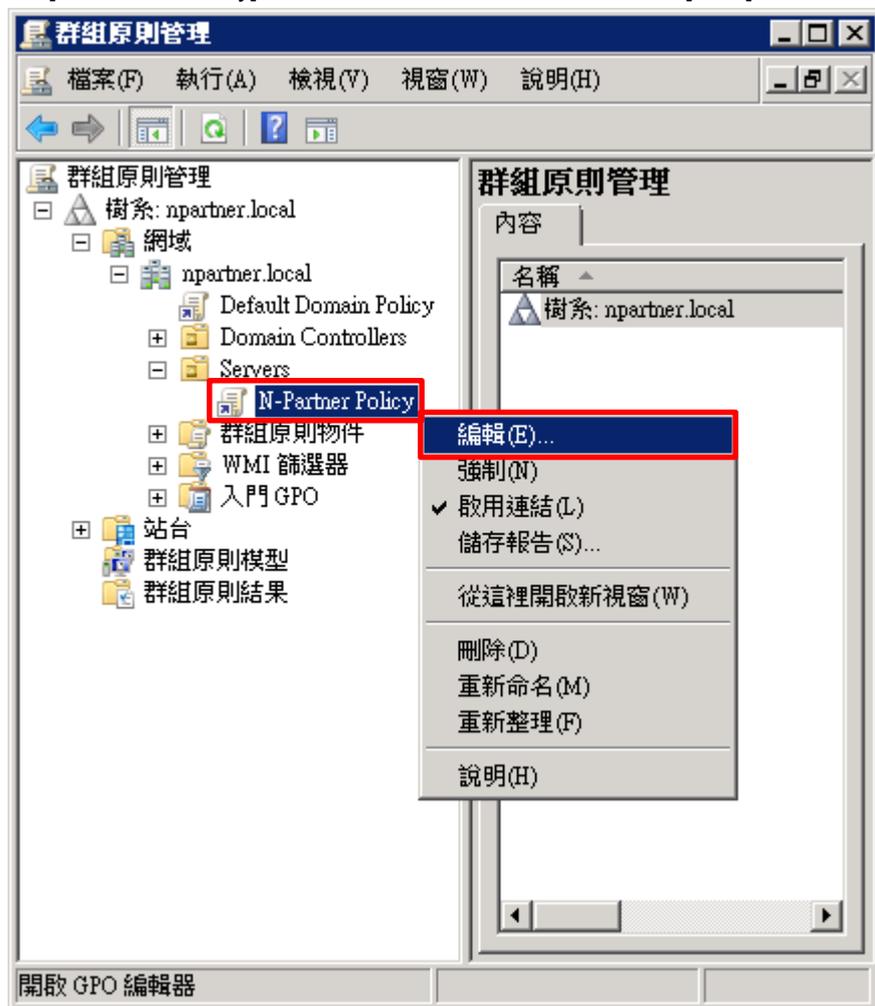
(3) 輸入群組原則物件名稱

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



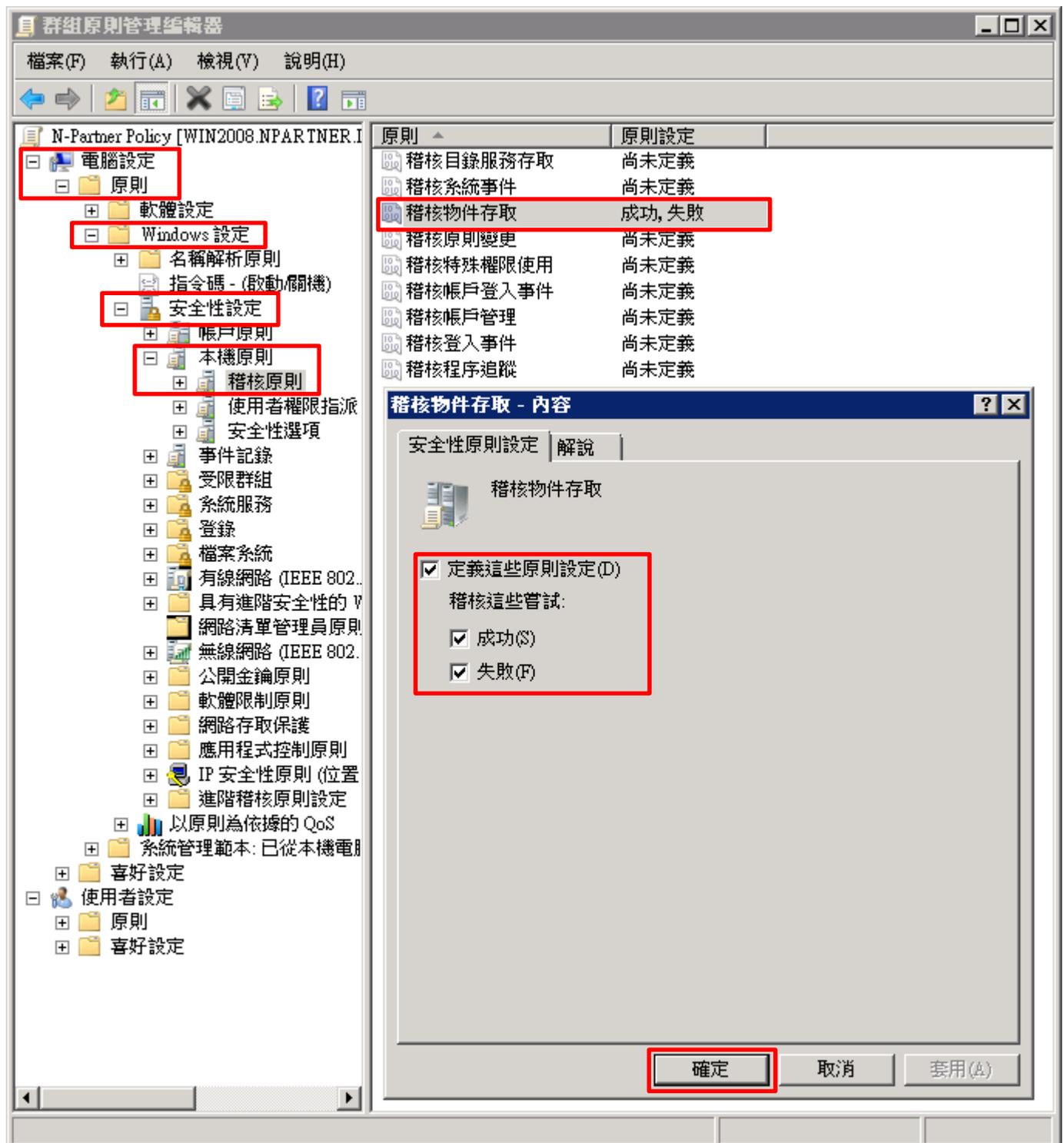
(4) 編輯群組原則物件

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] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取] 項目 -> 勾選 [定義這些原則設定:] & [成功] & [失敗] -> 按下 [確定]



(6) 在 Windows File 伺服器，開啟 [Windows PowerShell]，更新群組原則

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



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

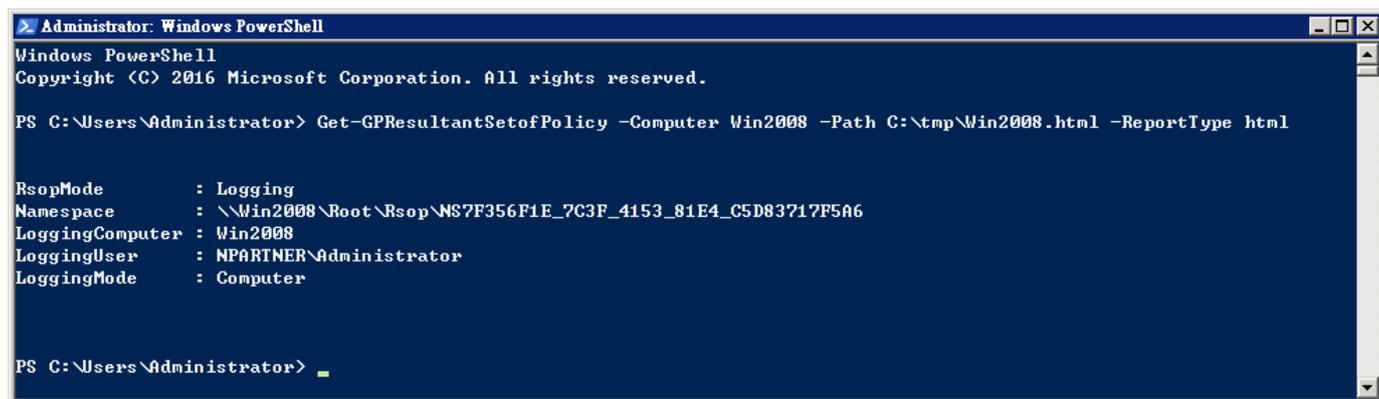
PS C:\Users\Administrator> gpupdate /force
正在更新原則...

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> █
```

(8) 在 AD 網域伺服器，開啟 [Windows PowerShell]，產生 Windows File 伺服器群組原則報表

```
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\NS7F356F1E_7C3F_4153_81E4_C5D83717F5A6
LoggingComputer : Win2008
LoggingUser    : NPARTNER\Administrator
LoggingMode    : Computer

PS C:\Users\Administrator> █
```

紅色文字部位請輸入 File 伺服器名稱和資料夾路徑檔案名稱

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

(9) 開啟報表 · 確認 Windows File 伺服器 · 套用 N-Partner Policy 群組原則

群組原則結果

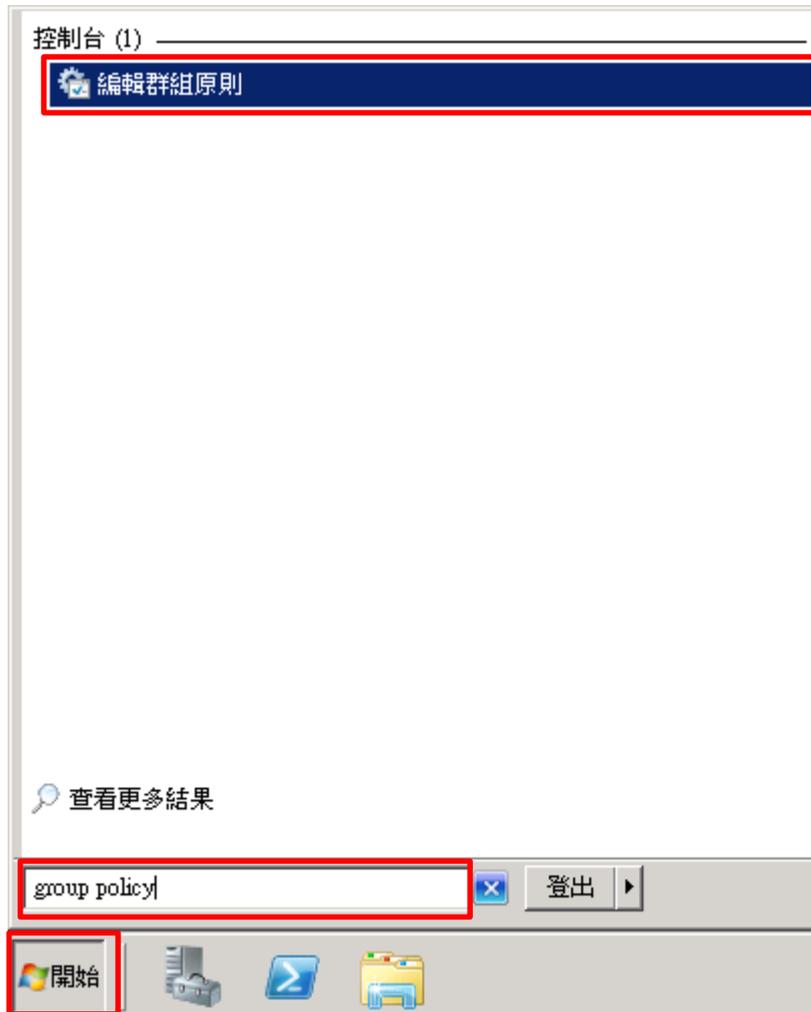
NPARTNER\WIN2008
資料收集: 2020/1/16 上午 10:55:05

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						
<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>稽核物件存取</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	原則	設定	優勢 GPO	稽核物件存取	成功, 失敗	N-Partner Policy	
原則	設定	優勢 GPO					
稽核物件存取	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	顯示						

3.2 工作群組

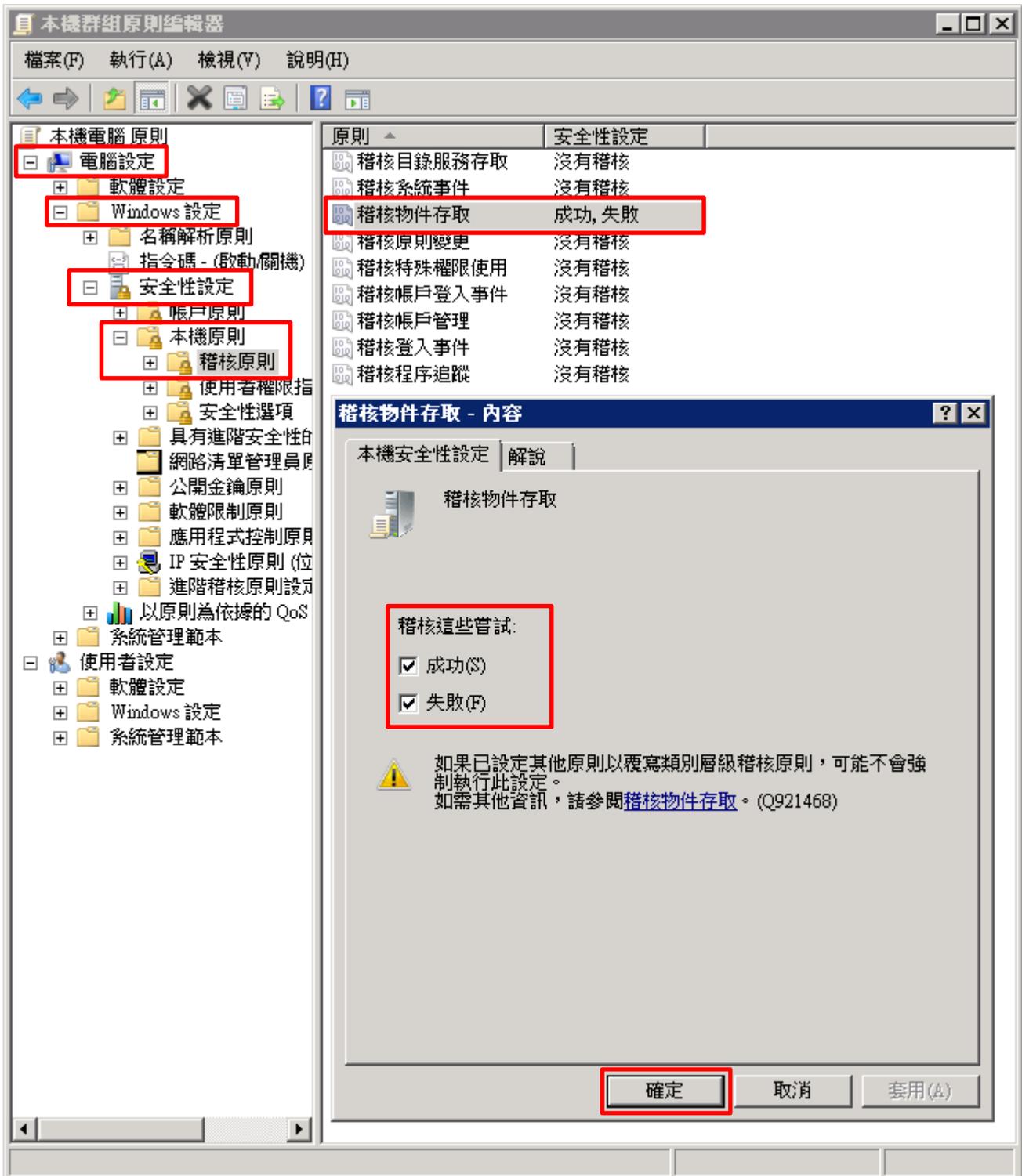
(1) 開啟 [本機群組原則編輯器]

點選 [開始] -> 在 [搜尋] 欄位 · 輸入 `group policy` -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按下 [確定]



(3) 開啟 [Windows PowerShell] ·



(4) 更新群組原則

PS C:\> gpupdate /force

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command "gpupdate /force" being executed, followed by the output: "正在更新原則...", "使用者原則更新已成功完成。", and "電腦原則更新已成功完成。". The prompt "PS C:\Users\Administrator>" is visible at the end of the output.

```
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> _
```

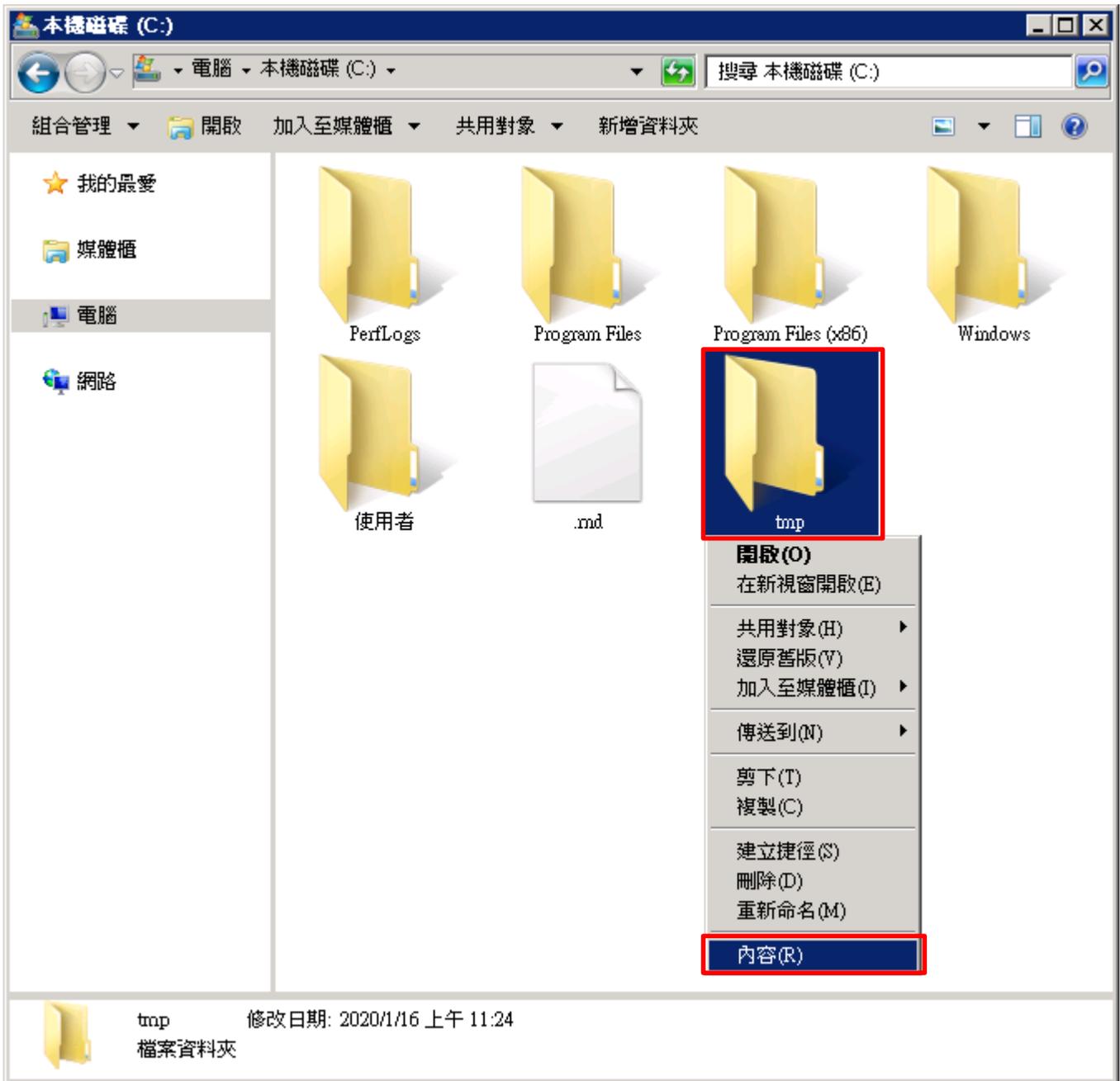
(5) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

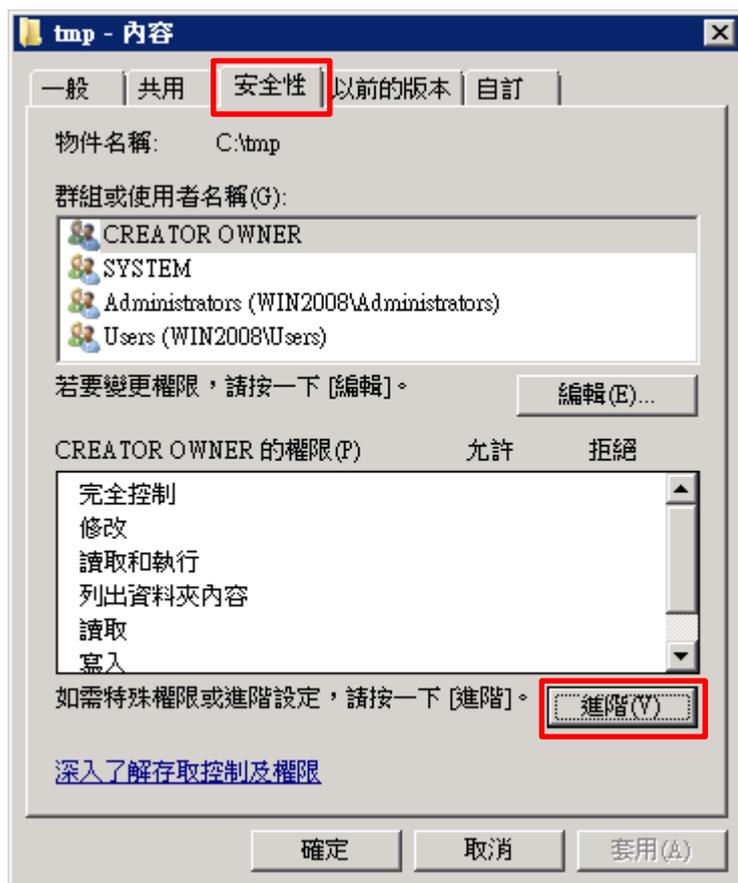
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
  安全性系統延伸      沒有稽核
  系統完整性          成功及失敗
  IPSEC driver        沒有稽核
  其他系統事件        成功及失敗
  安全性狀態變更      成功
登入/登出
  登入                成功及失敗
  登出                成功
  帳戶鎖定            成功
  IPsec 主要模式      沒有稽核
  IPsec 快速模式      沒有稽核
  IPsec 延伸模式      沒有稽核
  特殊登入            成功
  其他登入/登出事件  沒有稽核
網路原則/伺服器
物件存取
  檔案系統            成功及失敗
  registry            成功及失敗
  核心物件            成功及失敗
  SAM                 成功及失敗
  憑證服務            成功及失敗
  產生的應用程式      成功及失敗
  控制代碼操縱        成功及失敗
  檔案共用            成功及失敗
  篩選平台封包丟棄    成功及失敗
  篩選平台連線        成功及失敗
  其他物件存取事件    成功及失敗
  詳細檔案共用        成功及失敗
特殊權限使用
  機密特殊權限使用    沒有稽核
  非機密特殊權限使用  沒有稽核
  其他特殊權限使用事件 沒有稽核
詳細追蹤
  終止處理程序        沒有稽核
  DPAPI 活動          沒有稽核
  RPC 事件            沒有稽核
  建立處理程序        沒有稽核
原則變更
  稽核原則變更        成功
  驗證原則變更        成功
  授權原則變更        沒有稽核
  MPSSUC 規則層級原則變更 沒有稽核
  篩選平台原則變更    沒有稽核
  其他原則變更事件    沒有稽核
帳戶管理
  使用者帳戶管理      成功
  電腦帳戶管理        成功
  安全性群組管理      成功
  發佈群組管理        沒有稽核
  應用程式群組管理    沒有稽核
  其他帳戶管理事件    沒有稽核
DS 存取
  目錄服務變更        沒有稽核
  目錄服務複寫        沒有稽核
  詳細目錄服務複寫    沒有稽核
  目錄服務存取        成功
帳戶登入
  Kerberos 服務票證操作 成功
  其他帳戶登入事件    沒有稽核
  Kerberos 驗證服務    成功
  認證驗證            成功
PS C:\Users\Administrator>
```

3.3 稽核資料夾設定

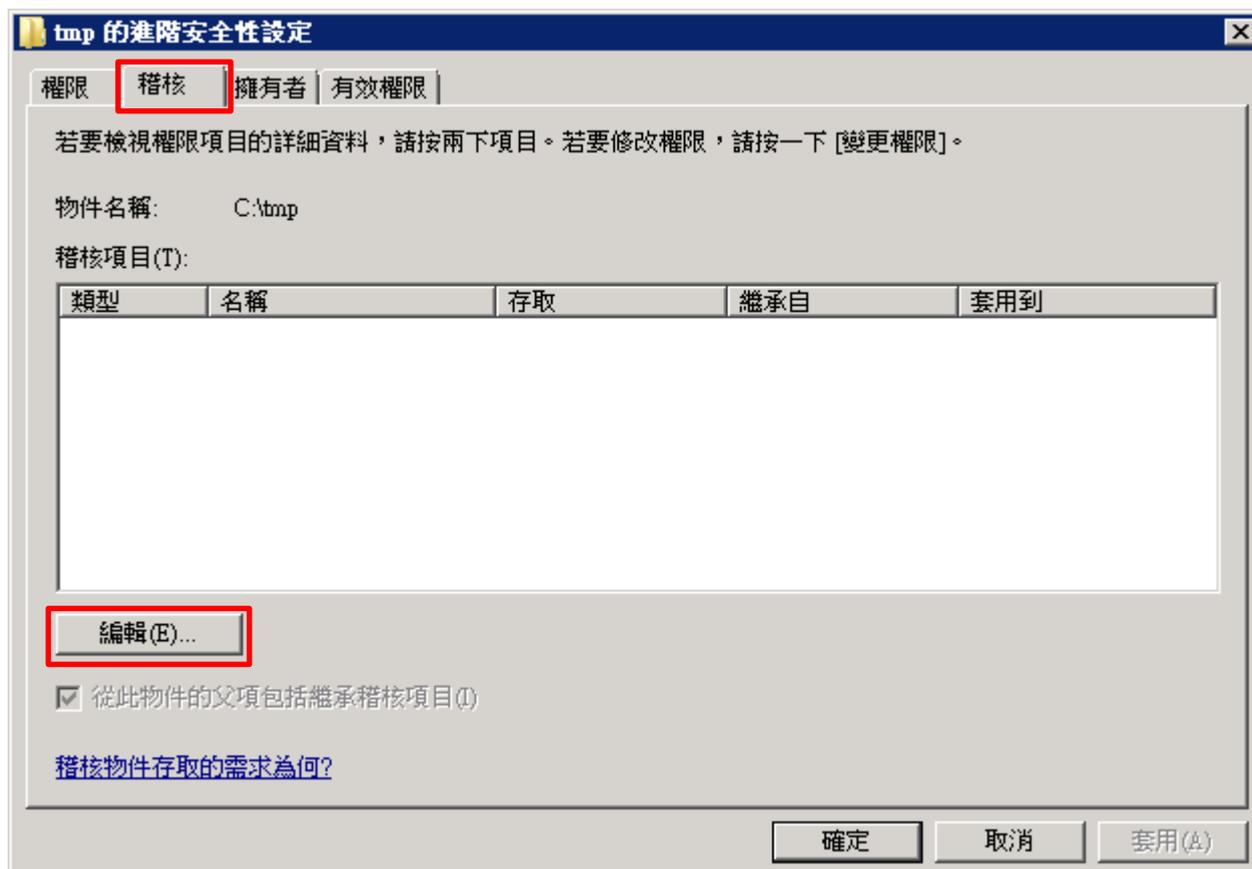
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



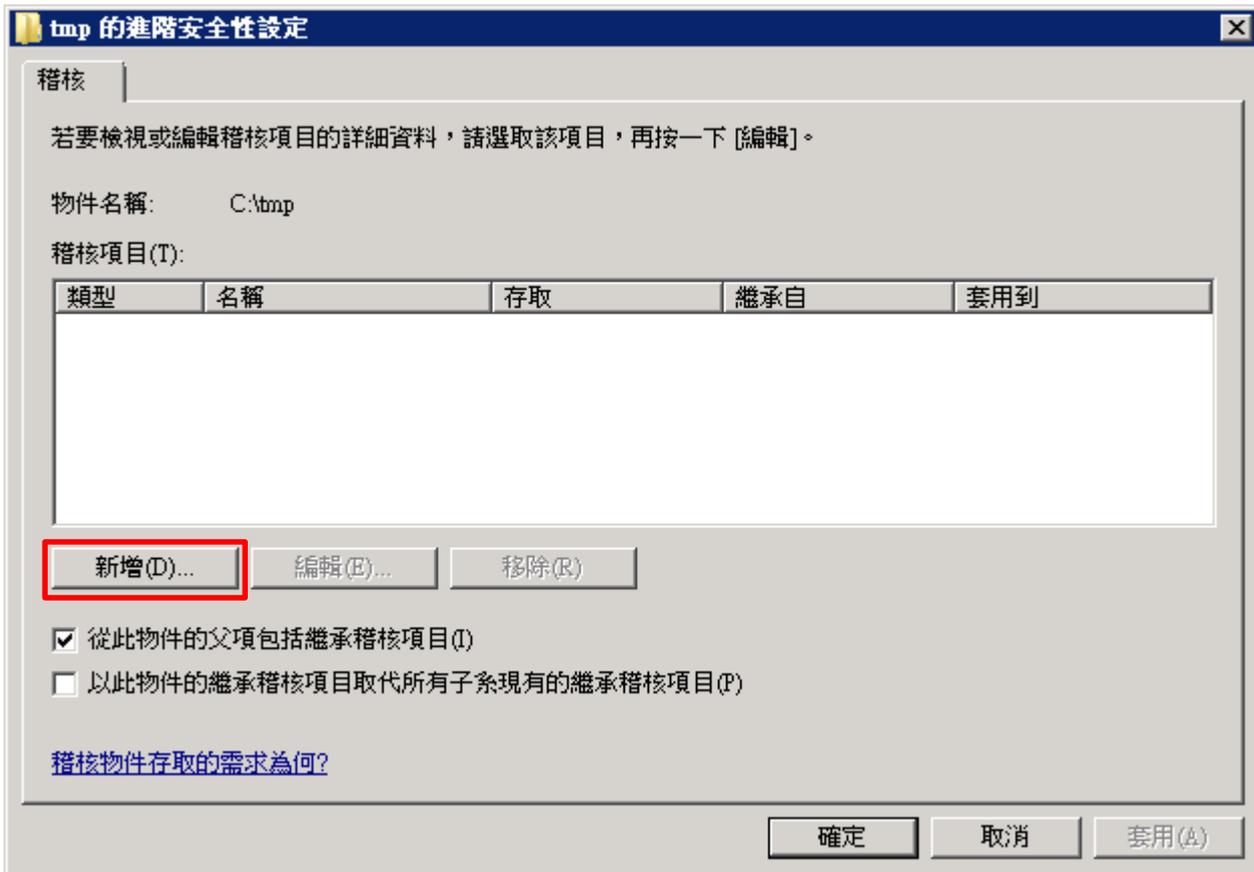
(2) 點選 [安全性] 頁面 -> 按下 [進階]



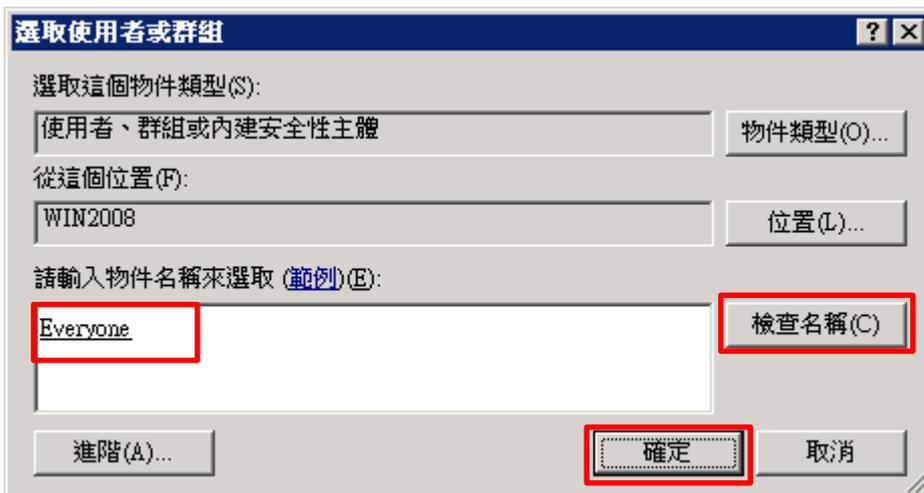
(3) 點選 [稽核] 頁面 -> 按下 [編輯]



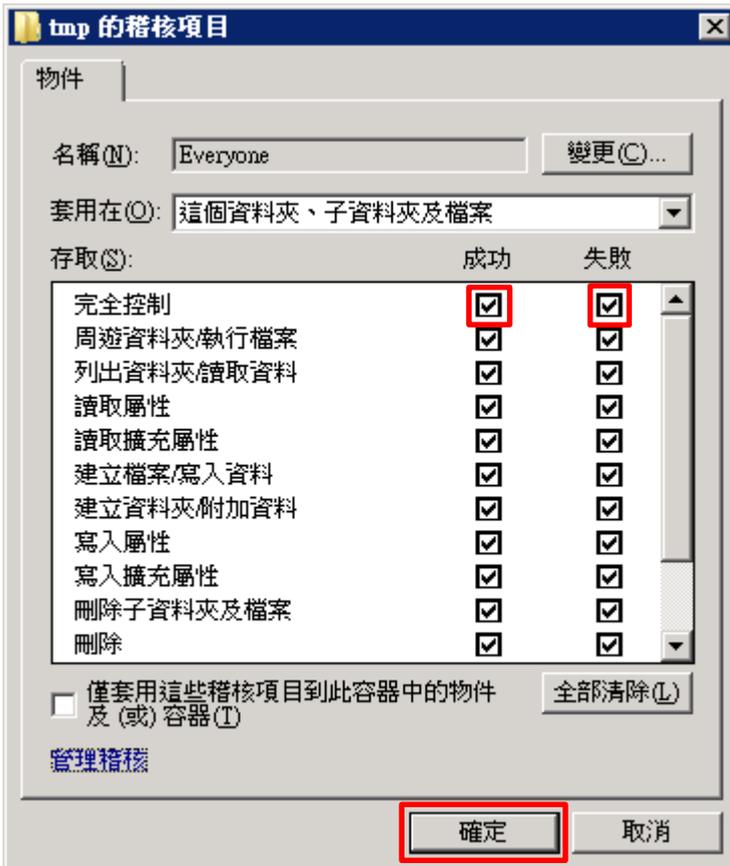
(4) 按下 [新增]



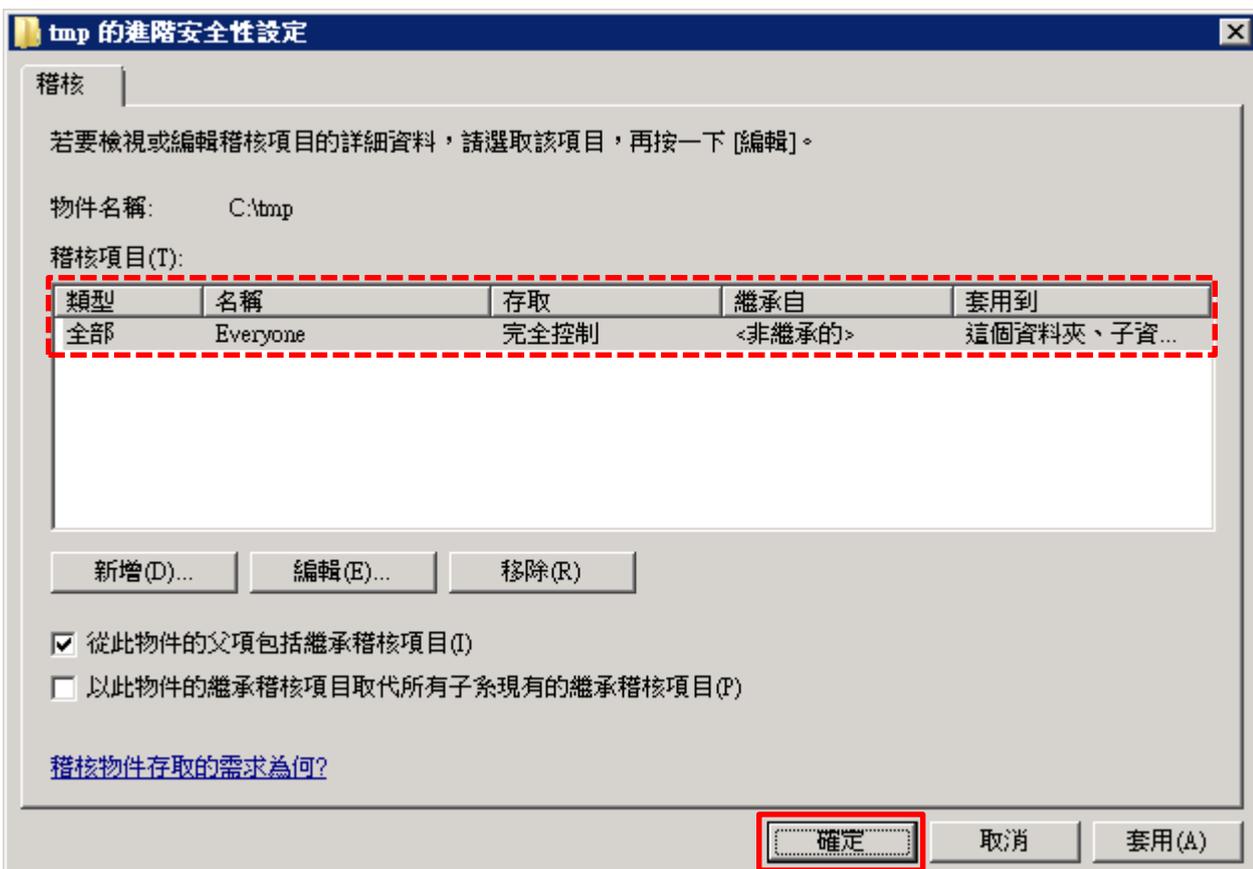
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



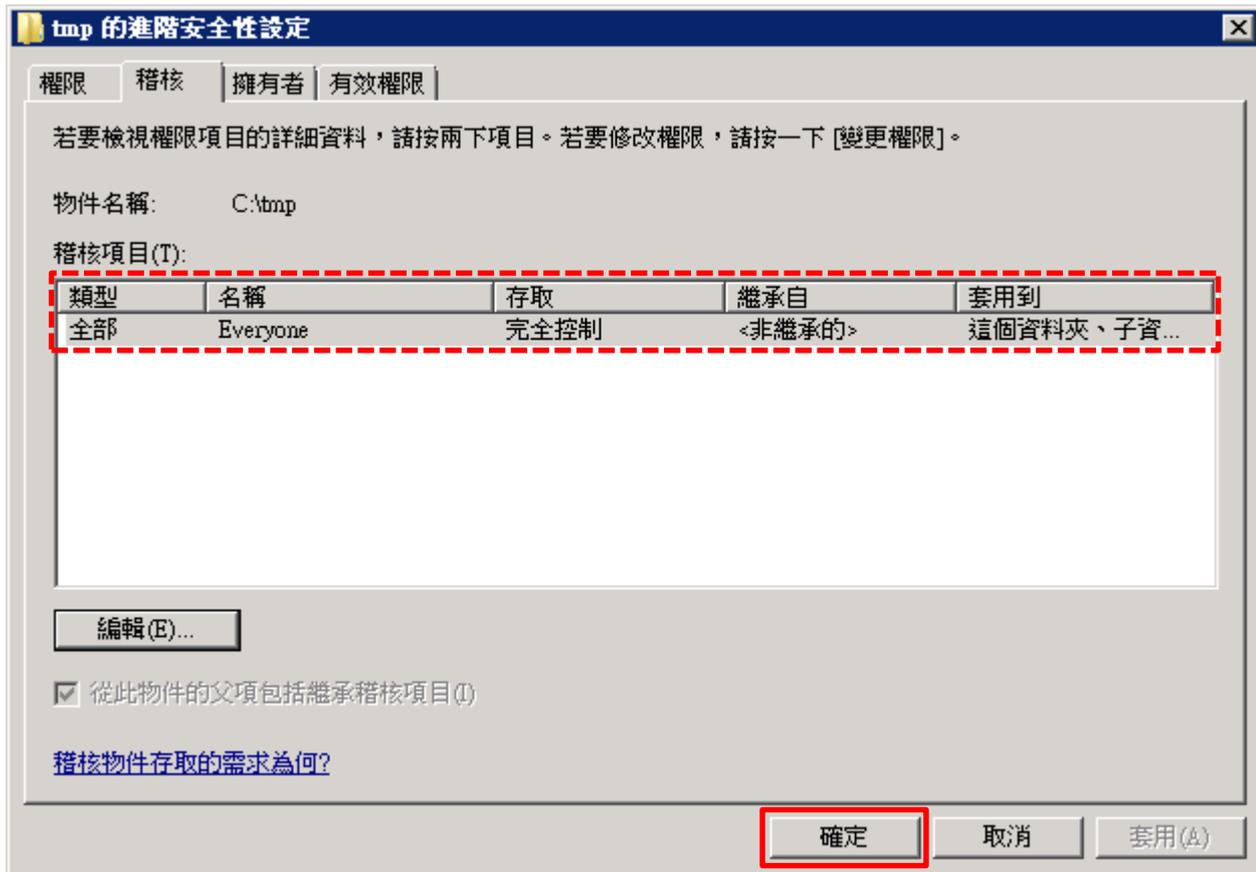
(6) 存取類型 [成功] 和 [失敗] 項目 都勾選 [完全控制] -> 按下 [確定]



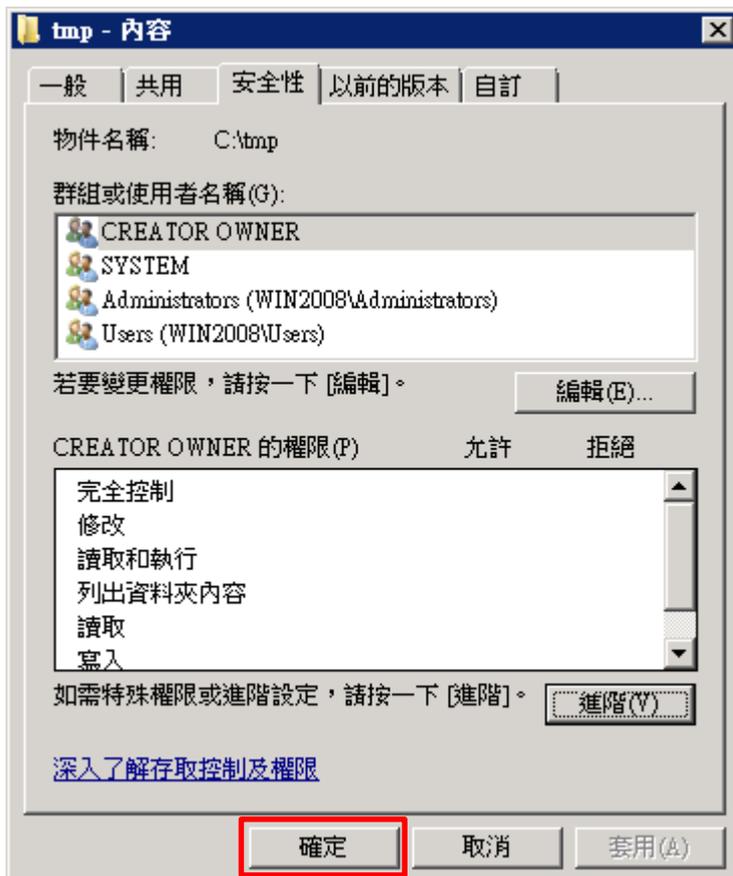
(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(9) 按下 [確定]



4. Windows 2012

以下分別為網域和工作群組設定方式。

4.1 網域

4.1.1 組織單位設定

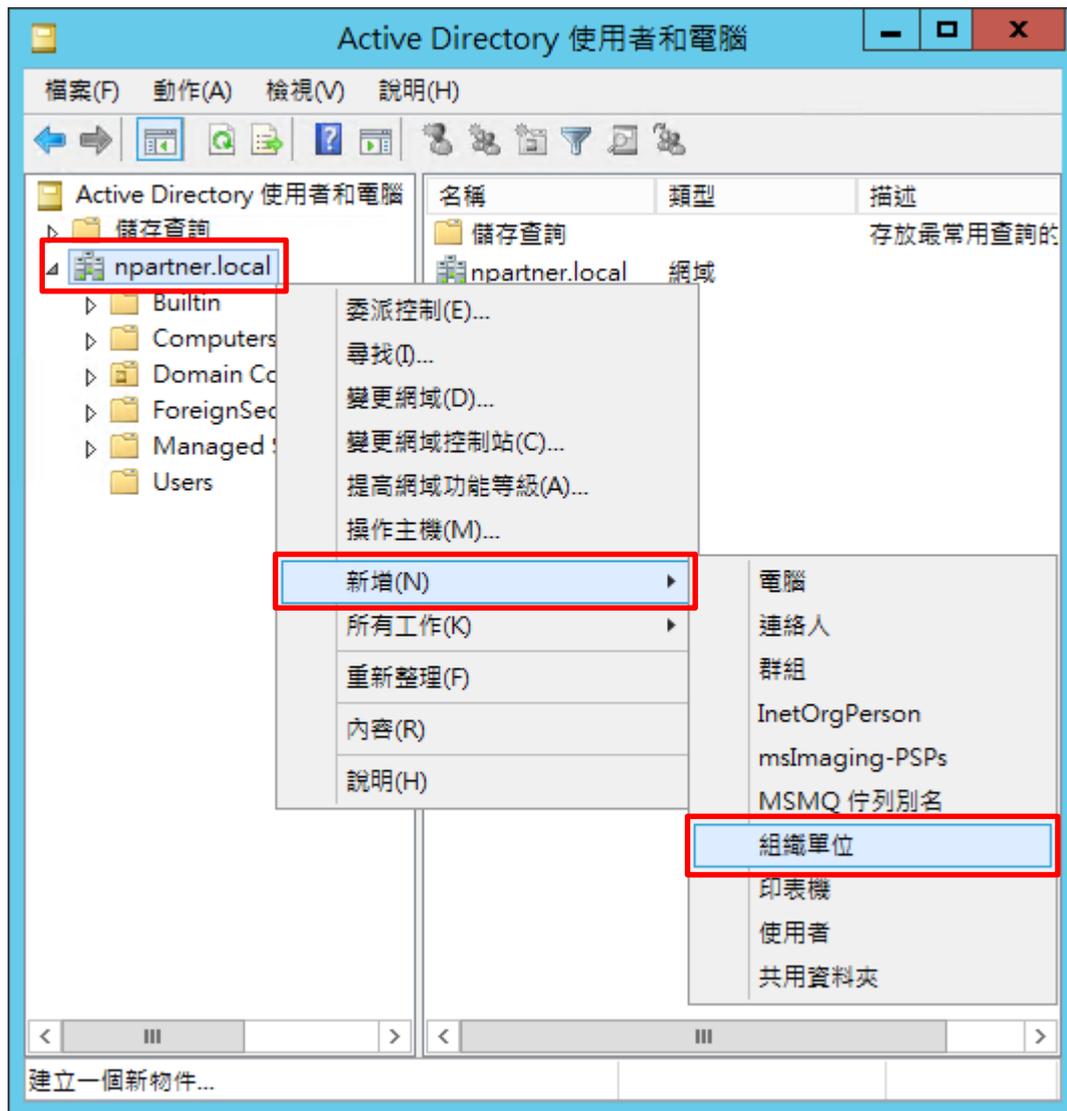
(1) 開啟 AD 使用者和電腦

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 -> 按下 [確定]

新增物件 - 組織單位

建立於: npartner.local/

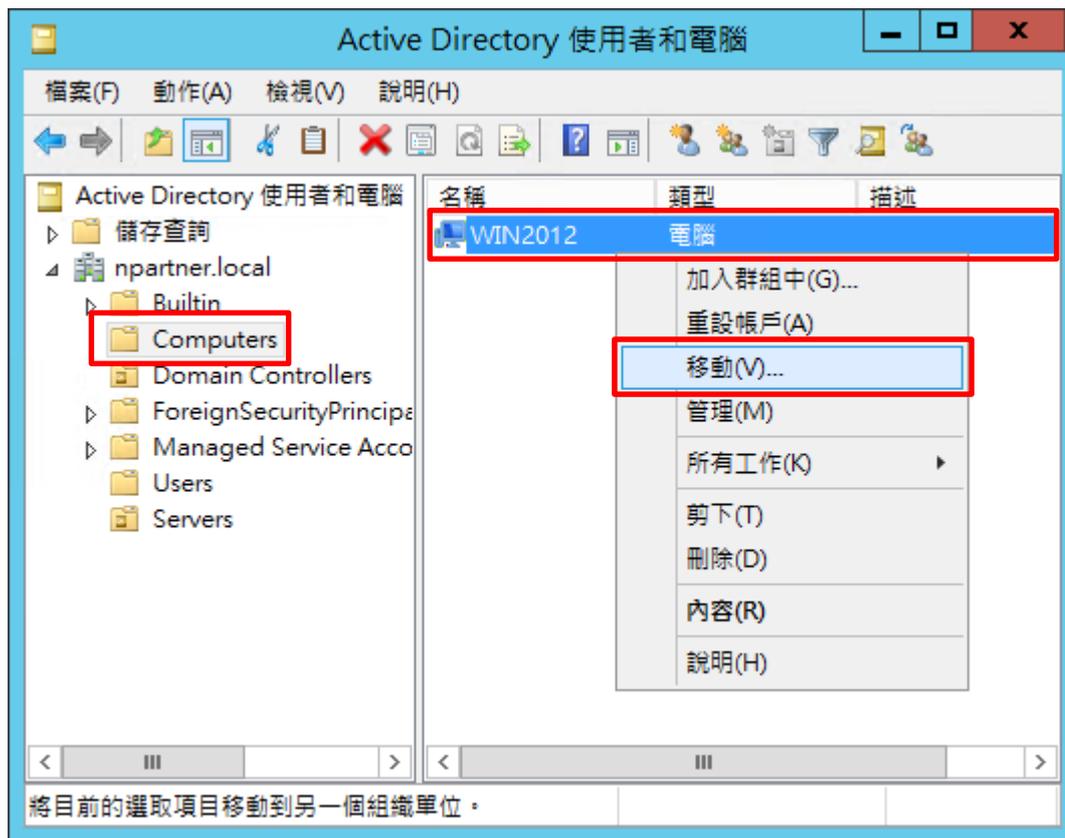
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

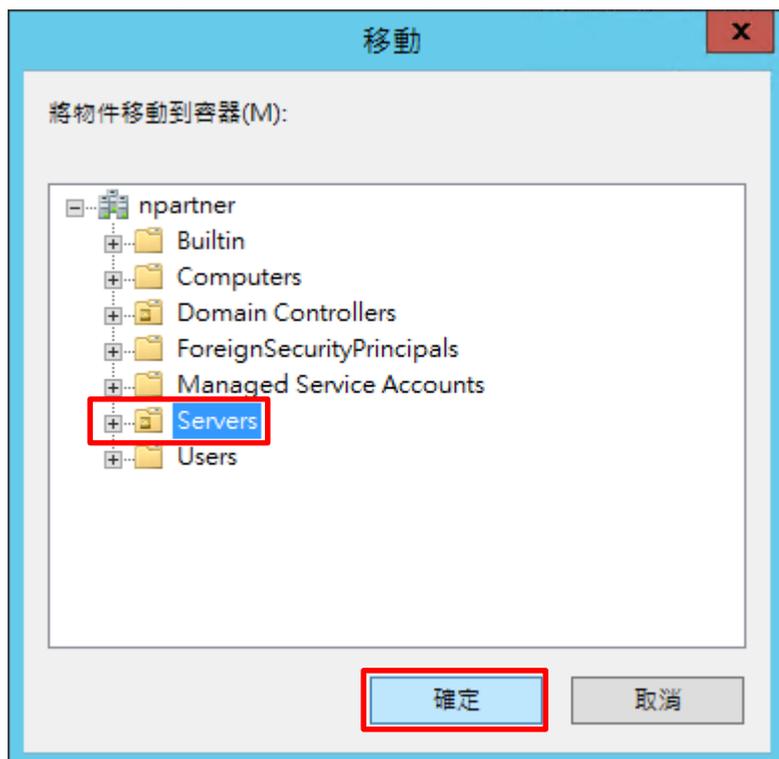
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [電腦名稱(Win2012)] 按滑鼠右鍵 -> 點選 [移動]



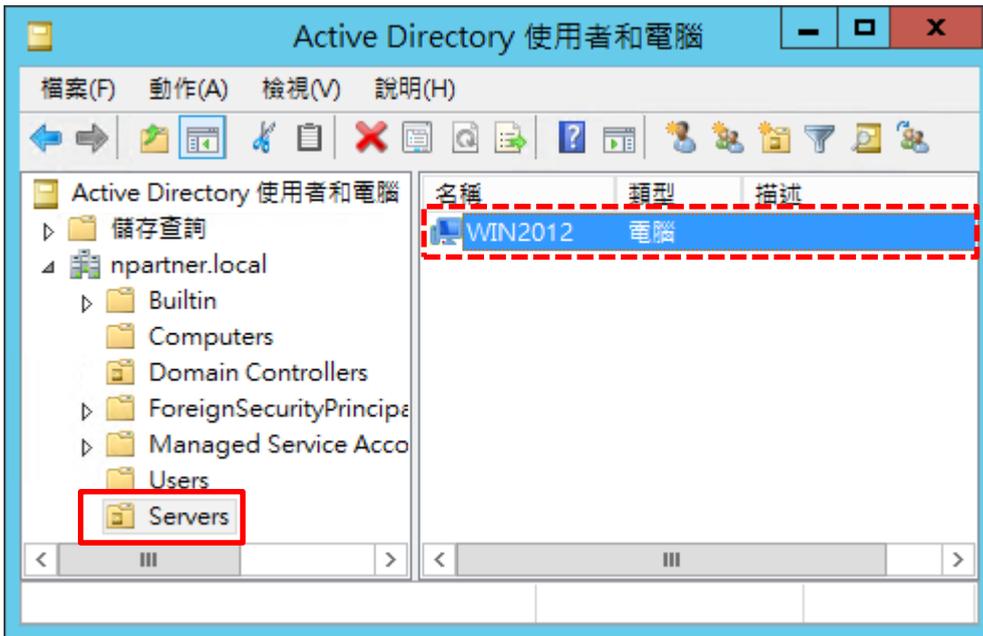
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按下 [確定]



(6) 確認伺服器已移動至新的組織單位

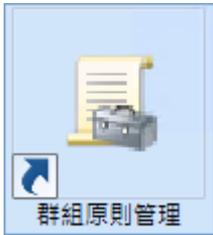
點選 [Servers] 組織單位，確認 [電腦名稱(Win2012)] 伺服器已移動



4.1.2 群組原則設定

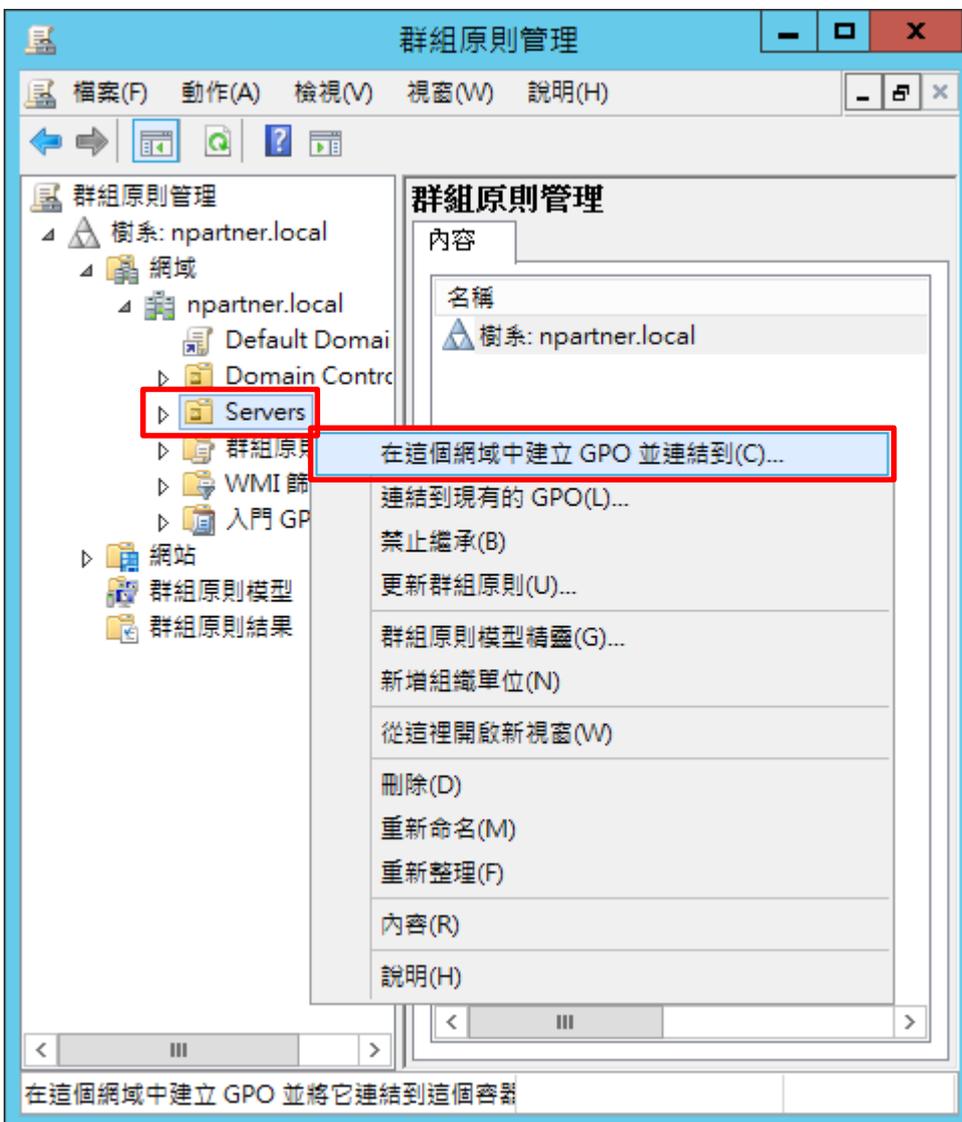
(1) 開啟群組原則管理

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...]



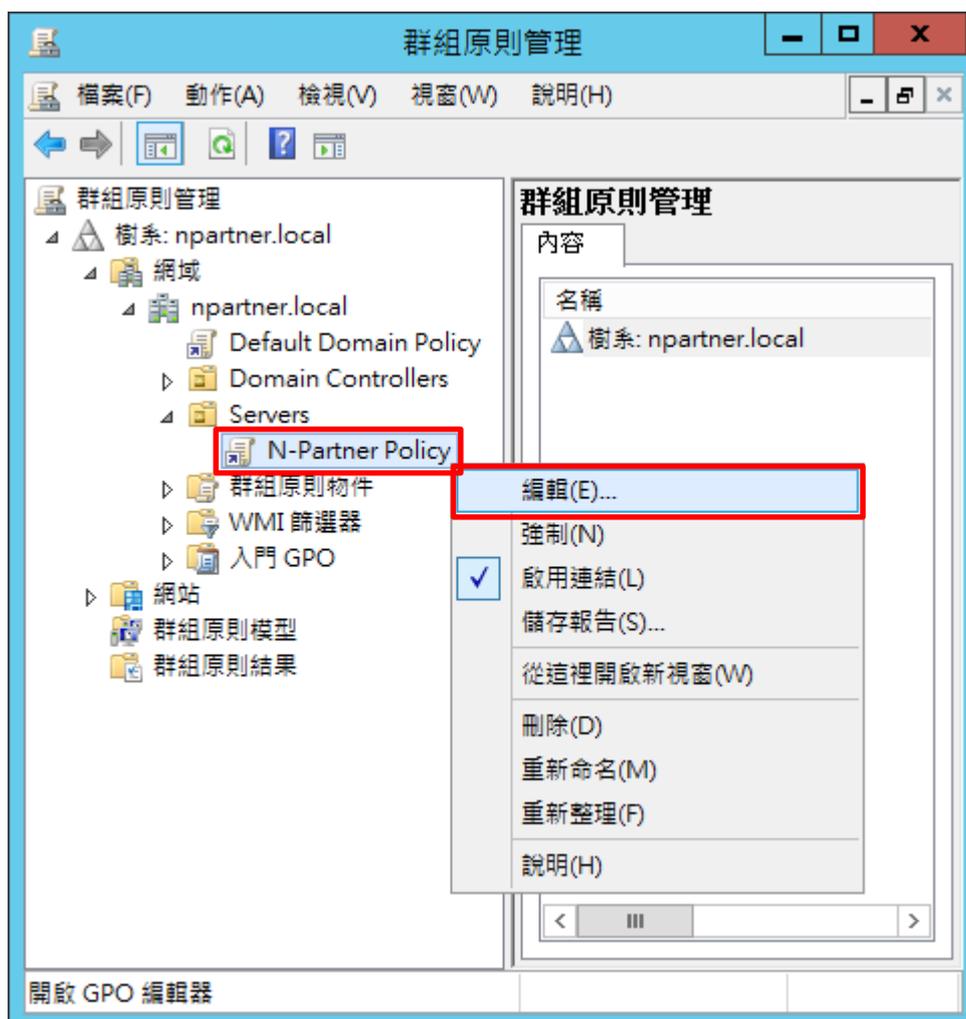
(3) 輸入群組原則物件名稱

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



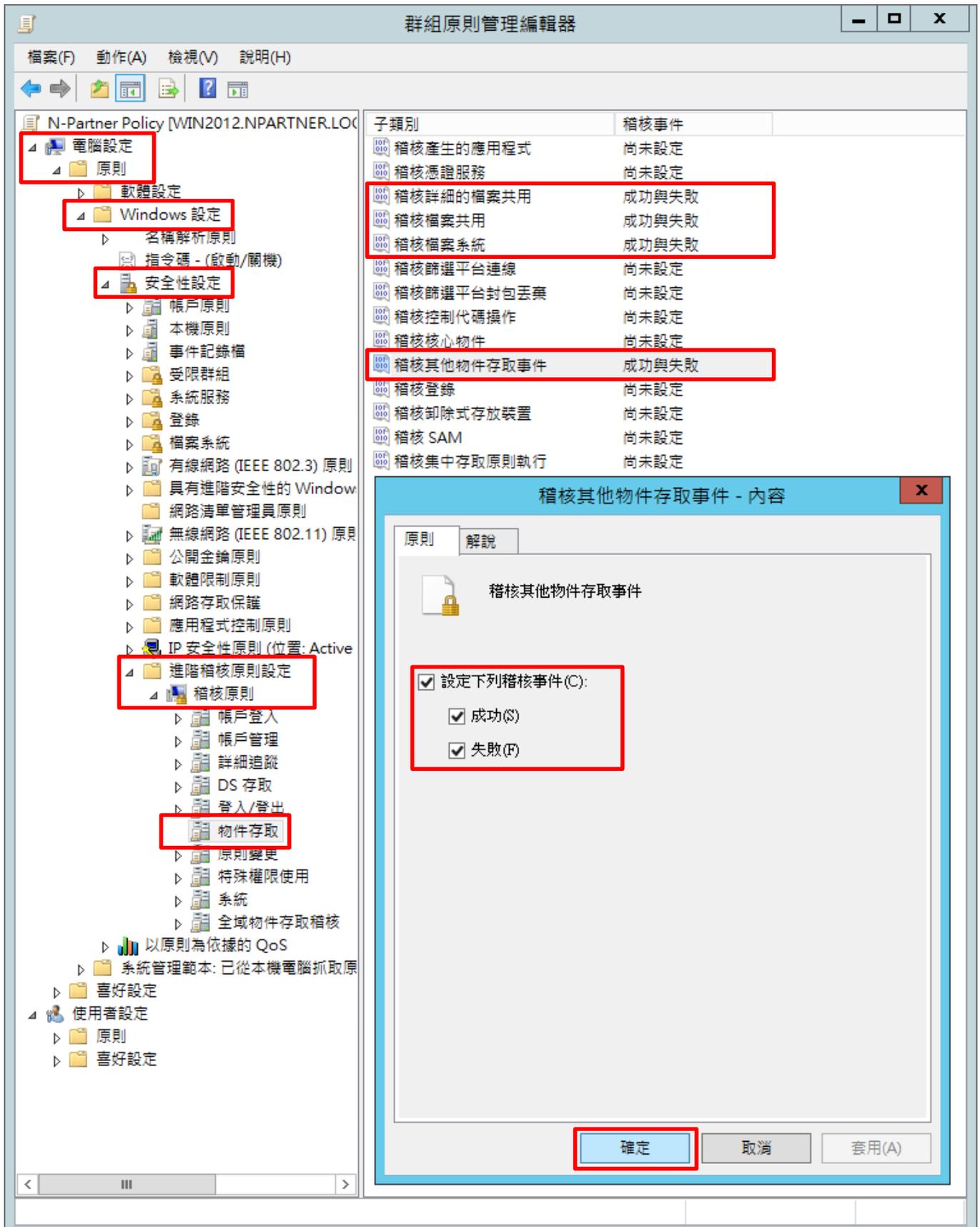
(4) 編輯群組原則物件

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



(5) 進階稽核原則：物件存取

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [進階稽核原則設定] -> [稽核原則] -> [物件存取] -> 點選 [稽核詳細的檔案共用], [稽核檔案共用], [稽核檔案系統], [稽核其他物件存取事件] 項目 -> 勾選 [設定下列稽核事件:] & [成功] & [失敗] -> 按下 [確定]



(6) 在 AD 網域伺服器，開啟 Windows PowerShell

開啟 [Windows PowerShell]



(7) 更新 Windows File 伺服器群組原則

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

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has a dark blue background. The text inside shows the command prompt "PS C:\Users\Administrator>" followed by the command `Invoke-GPUdate -Computer Win2012 -RandomDelayInMinutes 0 -Force`. The output shows the copyright notice for Microsoft Corporation and the command prompt again.

```
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> Invoke-GPUdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
PS C:\Users\Administrator>
```

紅色文字部位請輸入 Windows File 伺服器名稱

`Invoke-GPUdate -Computer Win2012 -RandomDelayInMinutes 0 -Force`

(8) 產生 Windows File 伺服器群組原則報表

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

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has a dark blue background. The text inside shows the command prompt "PS C:\Users\Administrator>" followed by the command `Get-GPResultantSetofPolicy -Computer Win2012 -Path C:\tmp\Win2012.html -ReportType html`. The output shows several properties: RsopMode, Namespace, LoggingComputer, LoggingUser, and LoggingMode.

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

RsopMode       : Logging
Namespace      : \\Win2012\Root\Rsop\NS0444F4C9_83B6_46F5_8AAC_3C0EEFD52FE
LoggingComputer : Win2012
LoggingUser    : NPARTNER\administrator
LoggingMode    : Computer

PS C:\Users\Administrator>
```

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

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

(9) 開啟報表 · 確認 Windows File 伺服器 · 套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WIN2012
資料收集: 2020/1/16 下午 02:35:26 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

帳戶原則/Kerberos 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

物件存取 隱藏

原則	設定	優勢 GPO
稽核詳細的檔案共用	成功, 失敗	N-Partner Policy
稽核檔案共用	成功, 失敗	N-Partner Policy
稽核檔案系統	成功, 失敗	N-Partner Policy
稽核其他物件存取事件	成功, 失敗	N-Partner Policy

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

4.2 工作群組

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



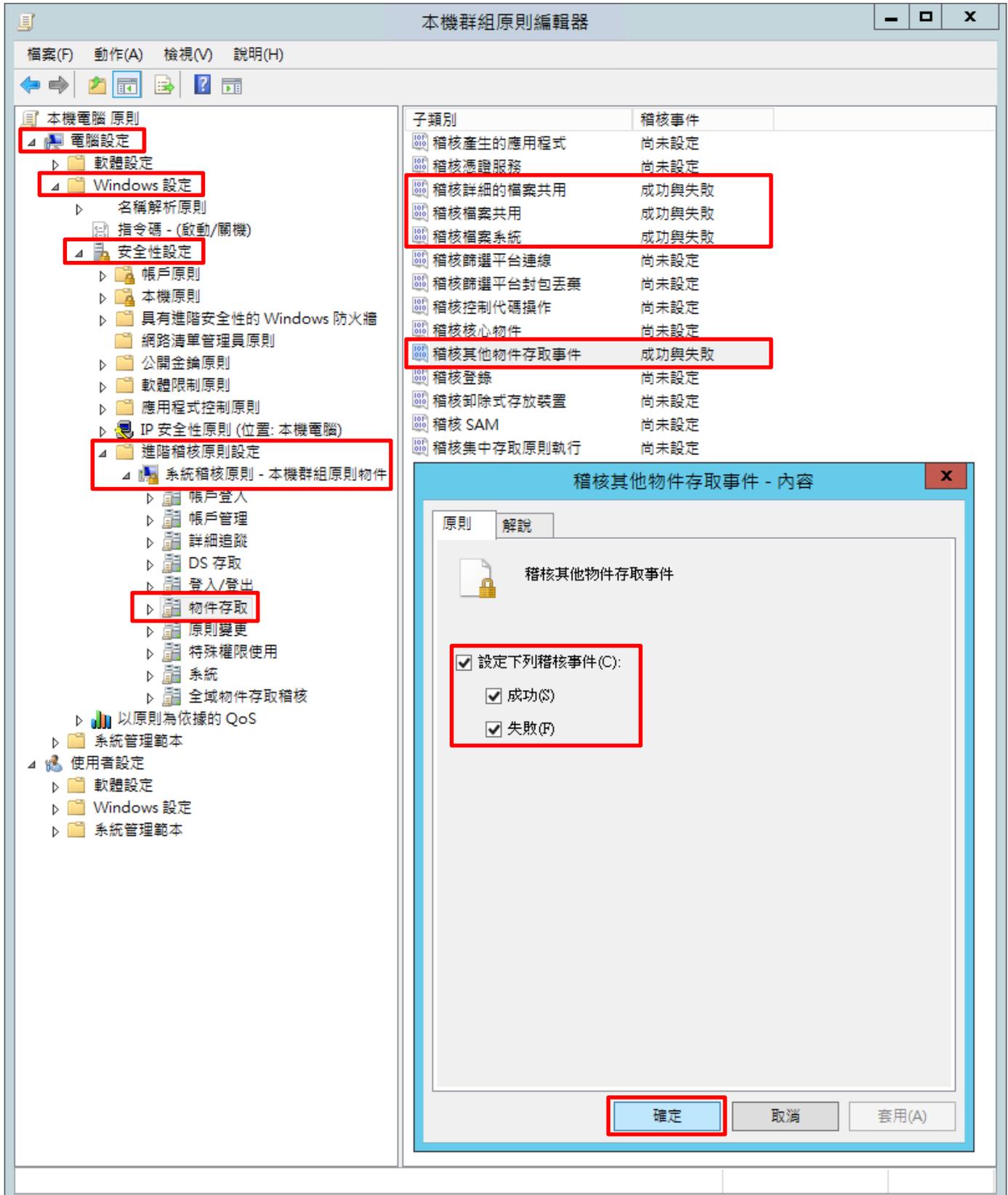
(2) 搜尋群組原則物件編輯器並執行

輸入 群組原則 -> 點選 [編輯群組原則]



(3) 進階稽核原則：物件存取

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [系統稽核原則 - 本機群組原則物件] -> [物件存取] -> 點選 [稽核詳細的檔案共用], [稽核檔案共用], [稽核檔案系統], [稽核其他物件存取事件] 項目 -> 勾選 [設定下列稽核事件:] & [成功] & [失敗] -> 按下 [確定]



(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

PS C:\> gpupdate /force



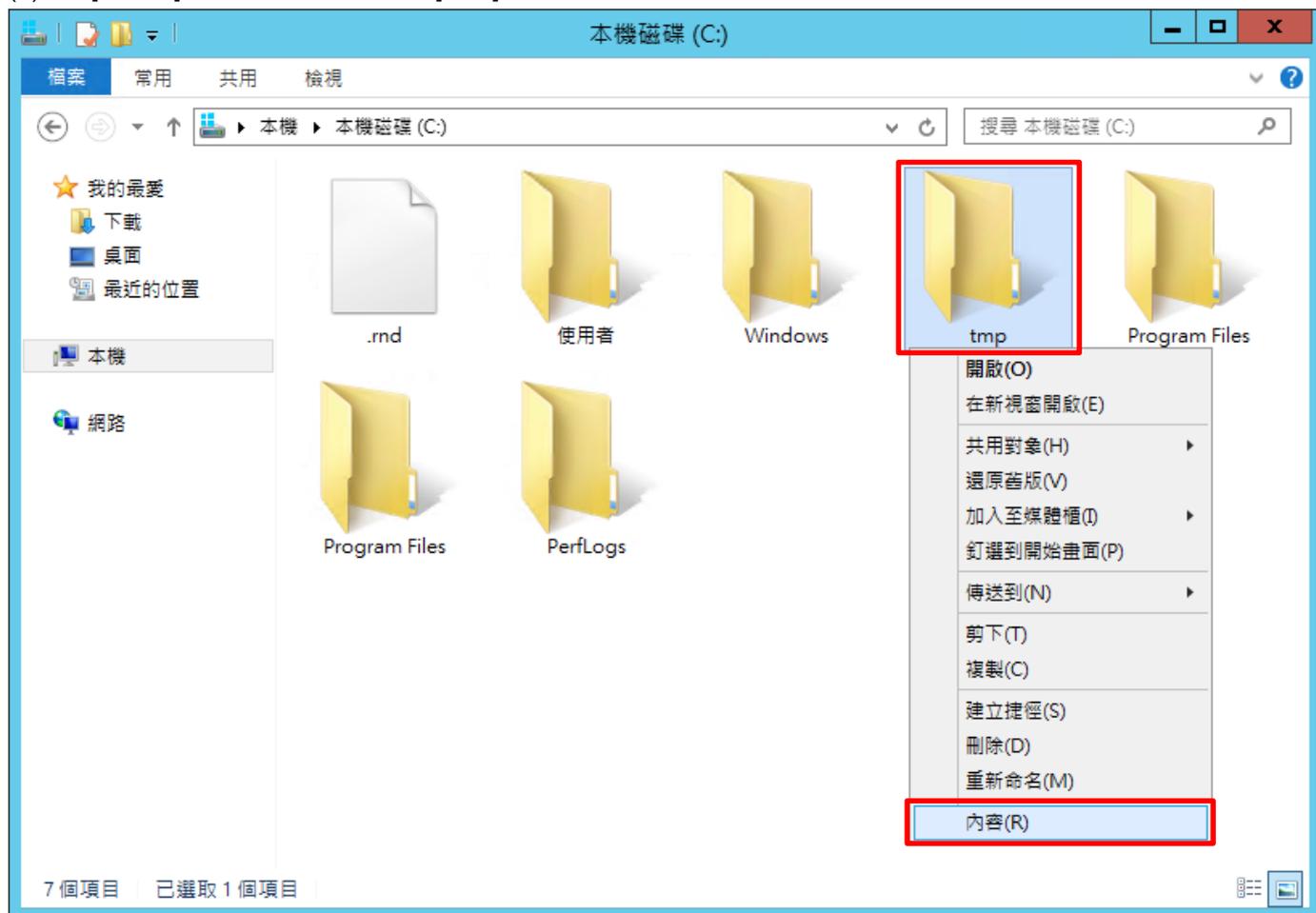
(6) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

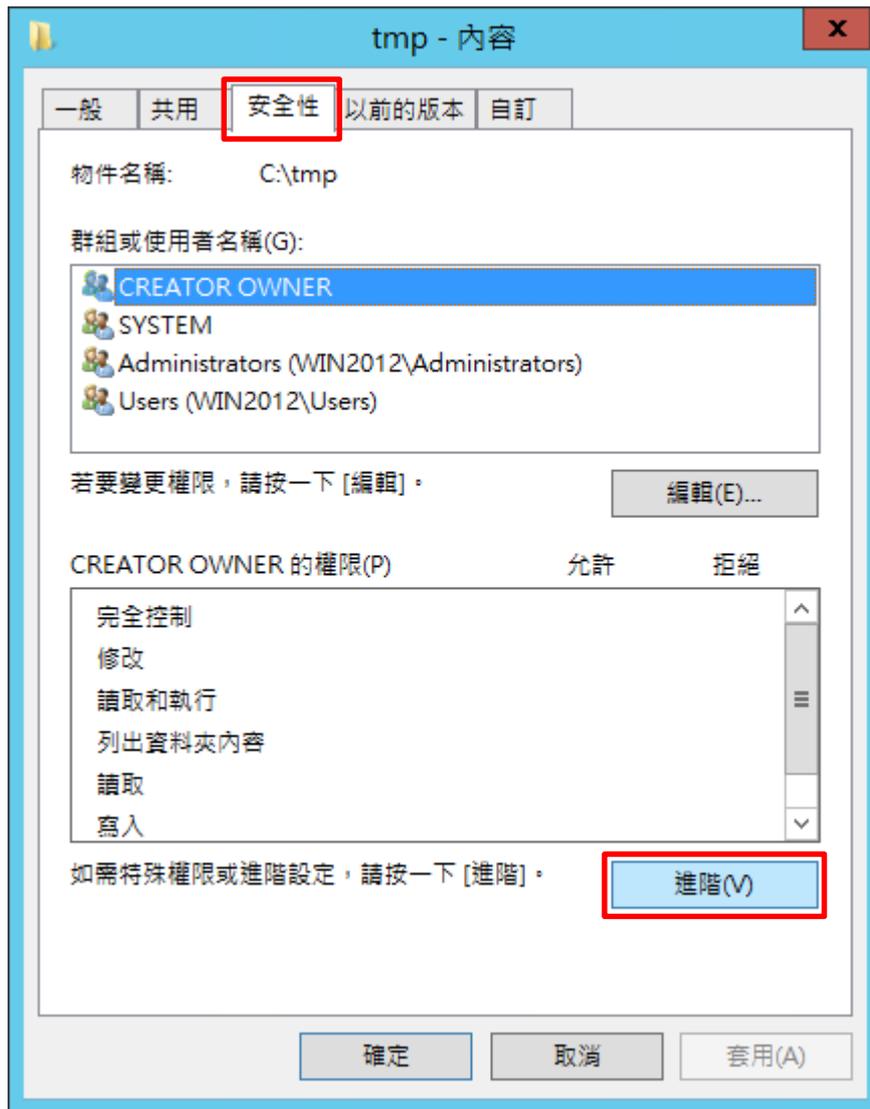
```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
  安全性系統延伸      沒有稽核
  系統完整性          沒有稽核
  IPSEC driver        沒有稽核
  其他系統事件        沒有稽核
  安全性狀態變更      沒有稽核
登入/登出
  登入                沒有稽核
  登出                沒有稽核
  帳戶鎖定            沒有稽核
  IPsec 主要模式      沒有稽核
  IPsec 快速模式      沒有稽核
  IPsec 延伸模式      沒有稽核
  特殊登入            沒有稽核
  其他登入/登出事件  沒有稽核
網路原則伺服器
  使用者/裝置宣告    沒有稽核
物件存取
  檔案系統            成功與失敗
  registry            沒有稽核
  核心物件            沒有稽核
  SAM                 沒有稽核
  憑證服務            沒有稽核
  產生的應用程式    沒有稽核
  控制代碼操縱        沒有稽核
  檔案共用            成功與失敗
  篩選平台封包丟棄    沒有稽核
  篩選平台連線        沒有稽核
  其他物件存取事件    成功與失敗
  詳細檔案共用        成功與失敗
  卸除式存放裝置      沒有稽核
  集中原則暫存        沒有稽核
特殊權限使用
  非機密特殊權限使用  沒有稽核
  其他特殊權限使用事件 沒有稽核
  機密特殊權限使用    沒有稽核
詳細追蹤
  建立處理程序        沒有稽核
  終止處理程序        沒有稽核
  DPAPI 活動          沒有稽核
  RPC 事件            沒有稽核
原則變更
  驗證原則變更        沒有稽核
  授權原則變更        沒有稽核
  MPSSUC 規則層級原則變更 沒有稽核
  篩選平台原則變更    沒有稽核
  其他原則變更事件    沒有稽核
  稽核原則變更        沒有稽核
帳戶管理
  使用者帳戶管理      沒有稽核
  電腦帳戶管理        沒有稽核
  安全性群組管理      沒有稽核
  發佈群組管理        沒有稽核
  應用程式群組管理    沒有稽核
  其他帳戶管理事件    沒有稽核
DS 存取
  目錄服務變更        沒有稽核
  目錄服務複寫        沒有稽核
  詳細目錄服務複寫    沒有稽核
  目錄服務存取        沒有稽核
帳戶登入
  Kerberos 服務票證操作 沒有稽核
  其他帳戶登入事件    沒有稽核
  Kerberos 驗證服務    沒有稽核
  認證驗證            沒有稽核
PS C:\Users\Administrator>
```

4.3 稽核資料夾設定

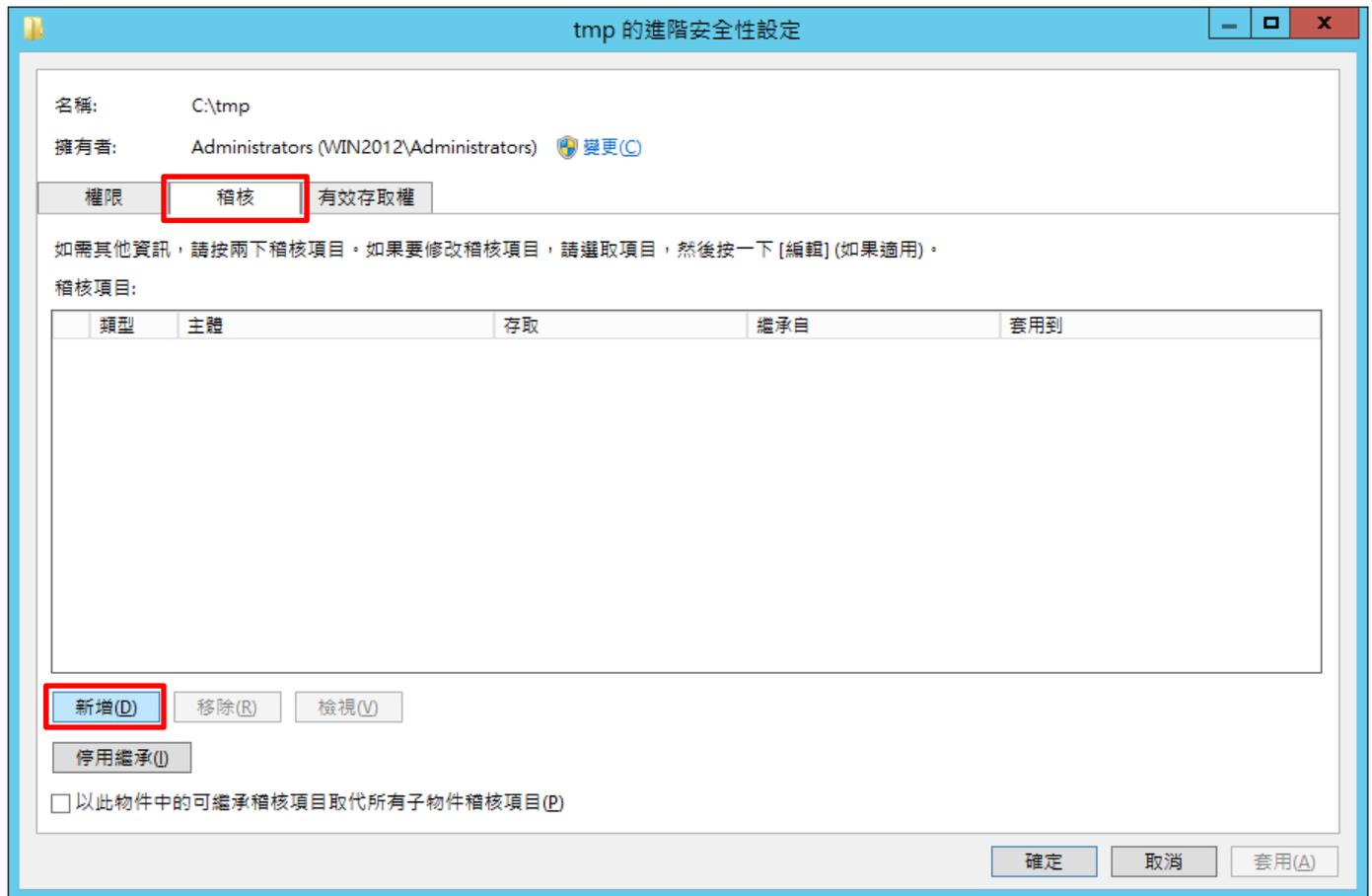
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



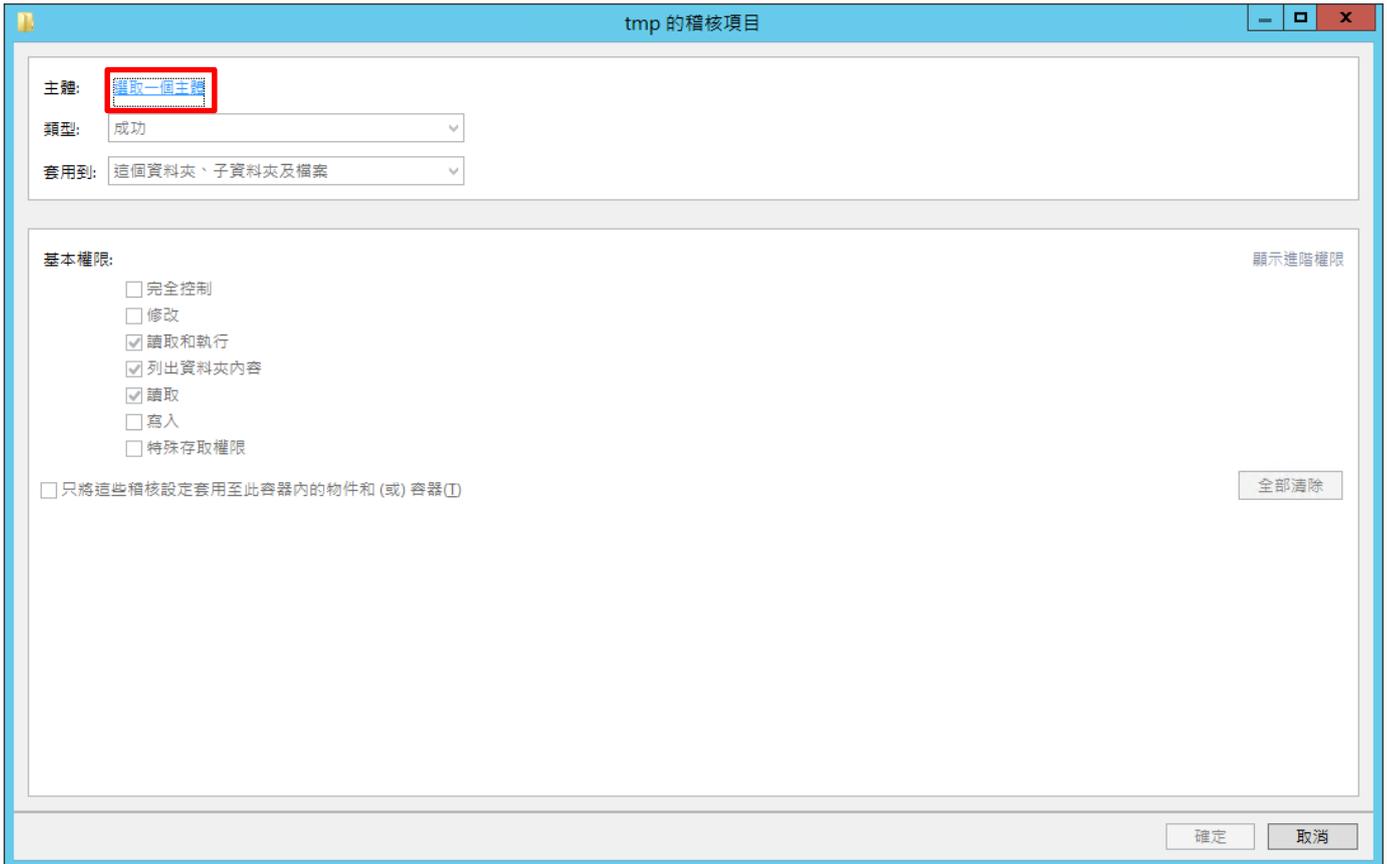
(2) 點選 [安全性] 頁面 -> 按下 [進階]



(3) 點選 [稽核] 頁面 -> 按下 [新增]



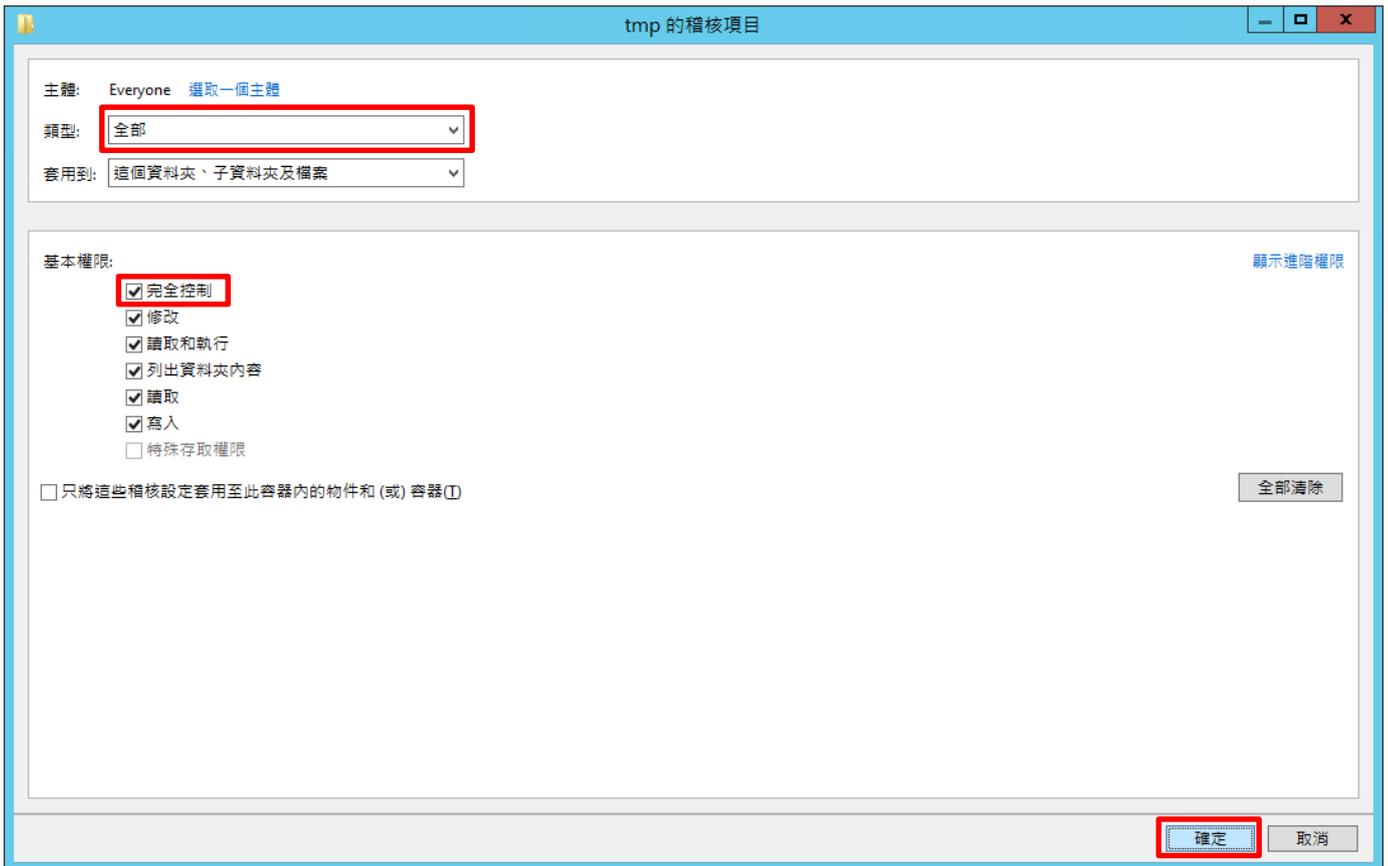
(4) 點選 [選取一個主體]



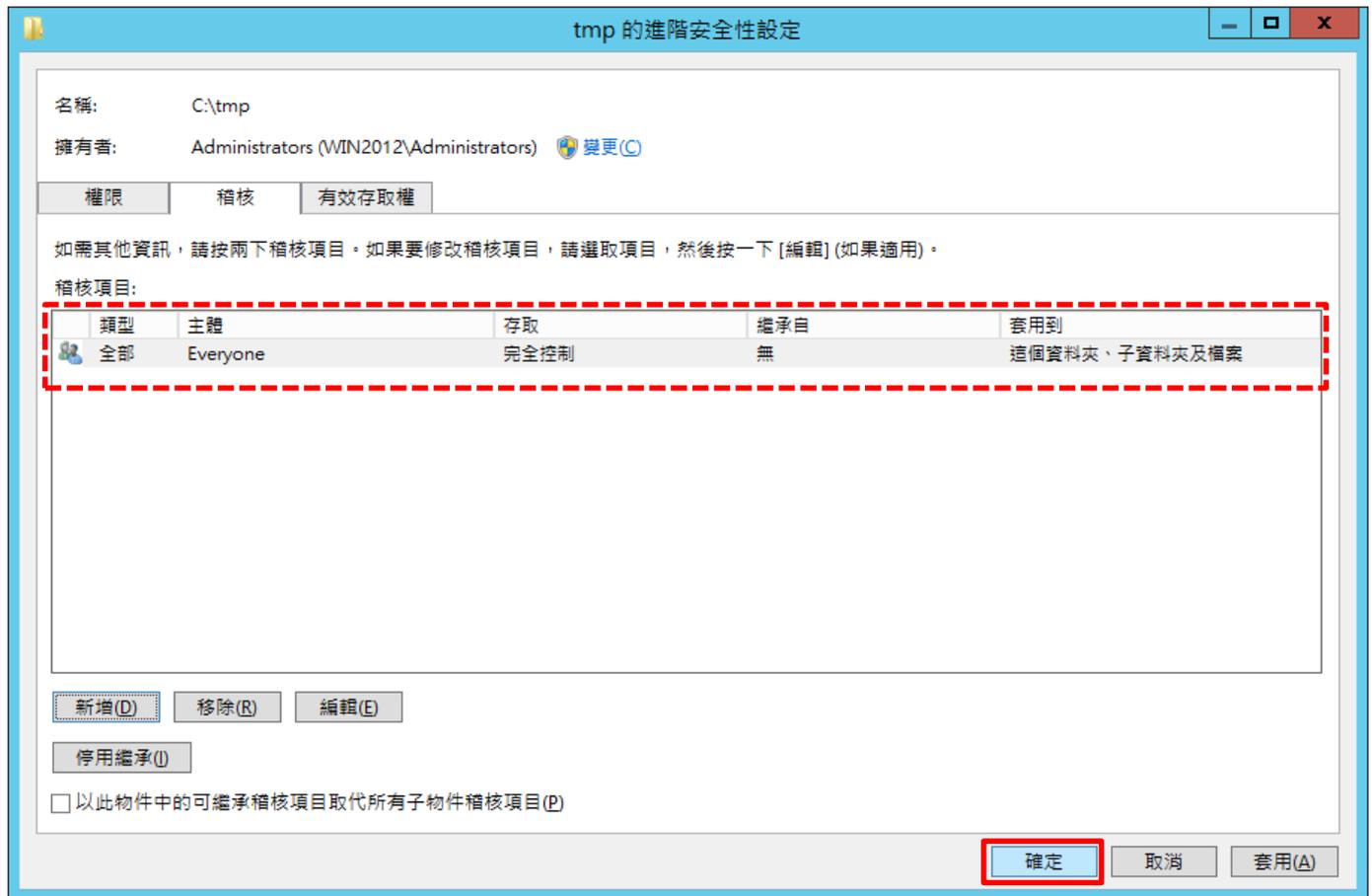
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



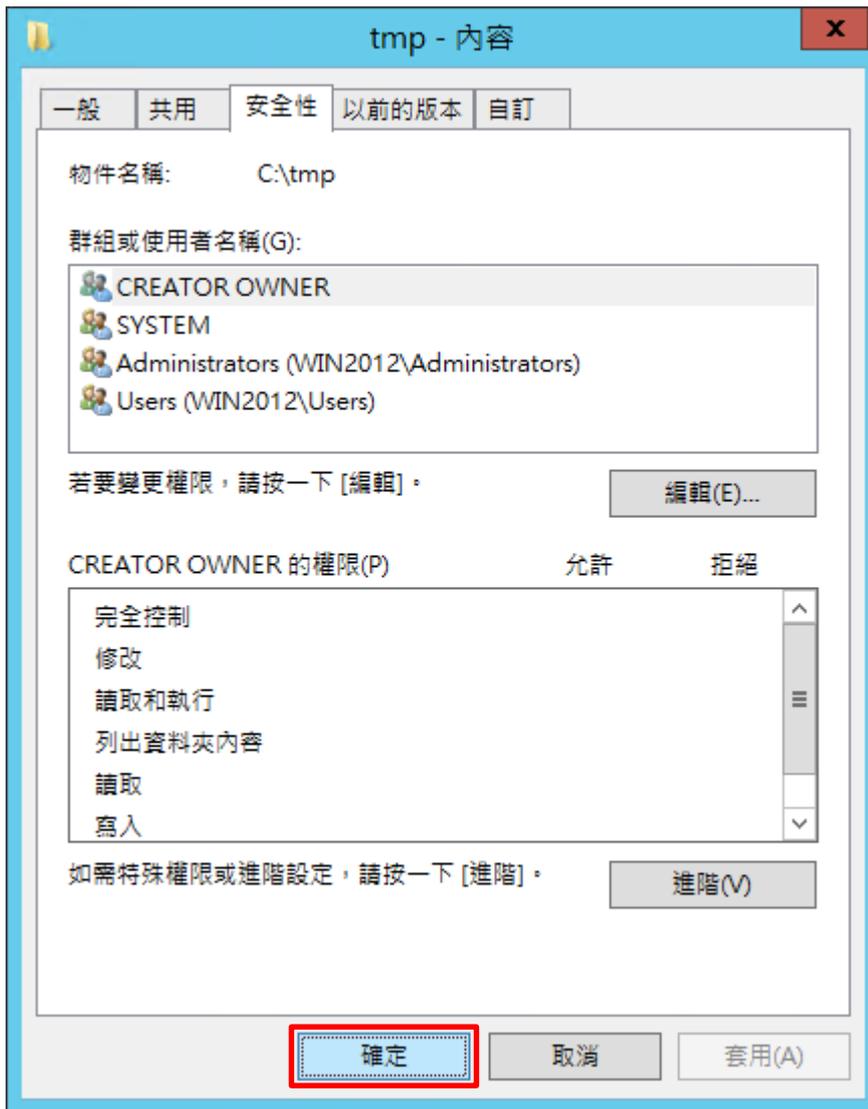
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 按下 [確定]





5. Windows 2016

以下分別為網域和工作群組設定方式。

5.1 網域

5.1.1 組織單位設定

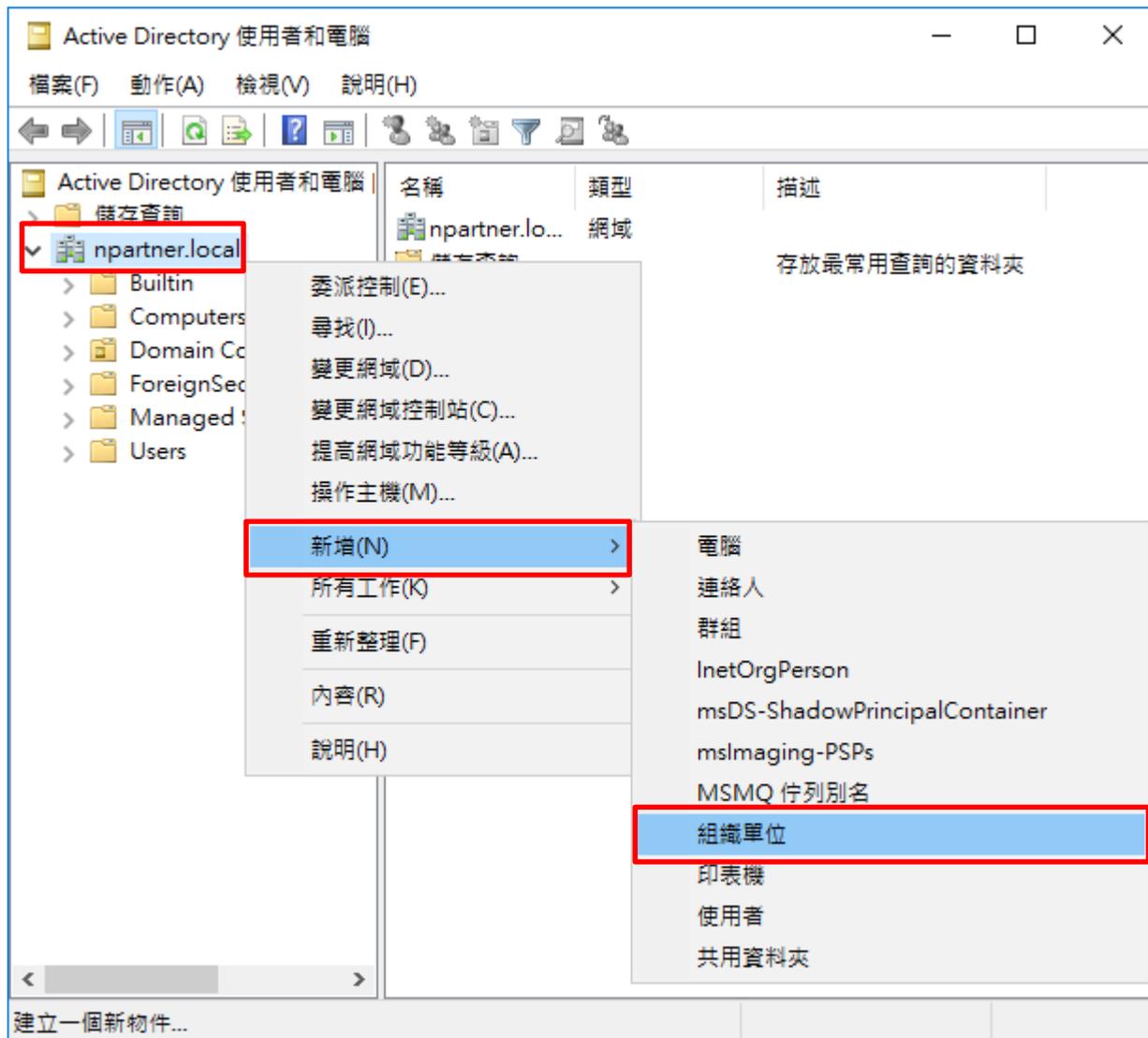
(1) 開啟 AD 使用者和電腦

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 -> 按下 [確定]

新增物件 - 組織單位

建立在: npartner.local/

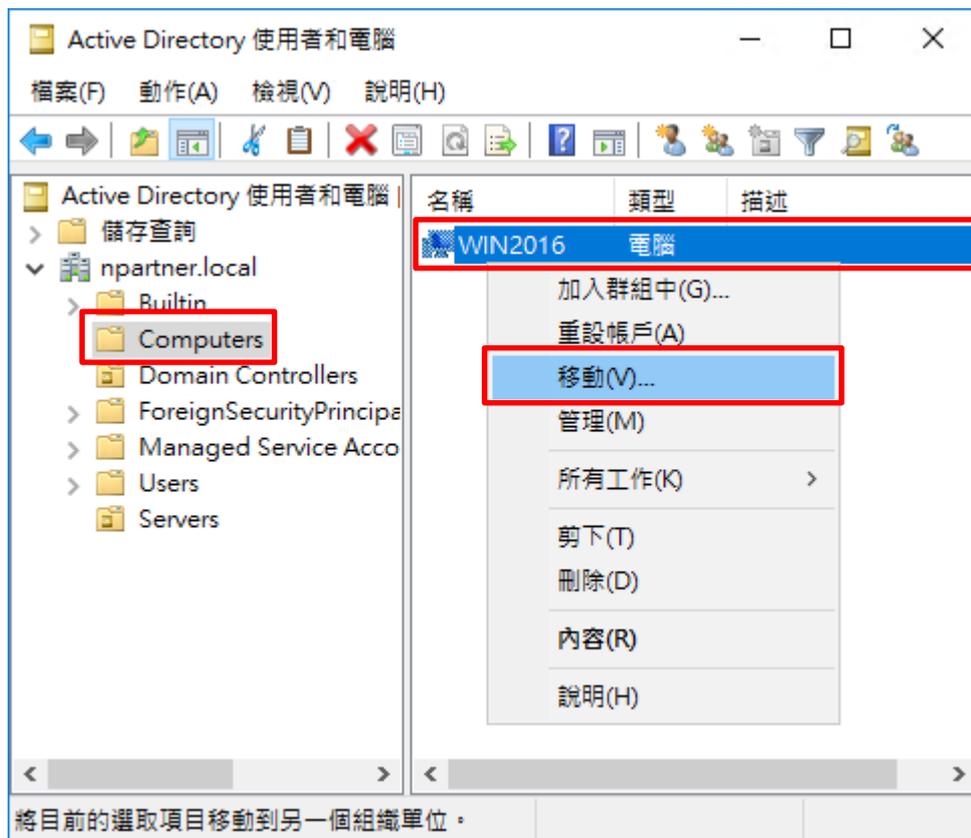
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

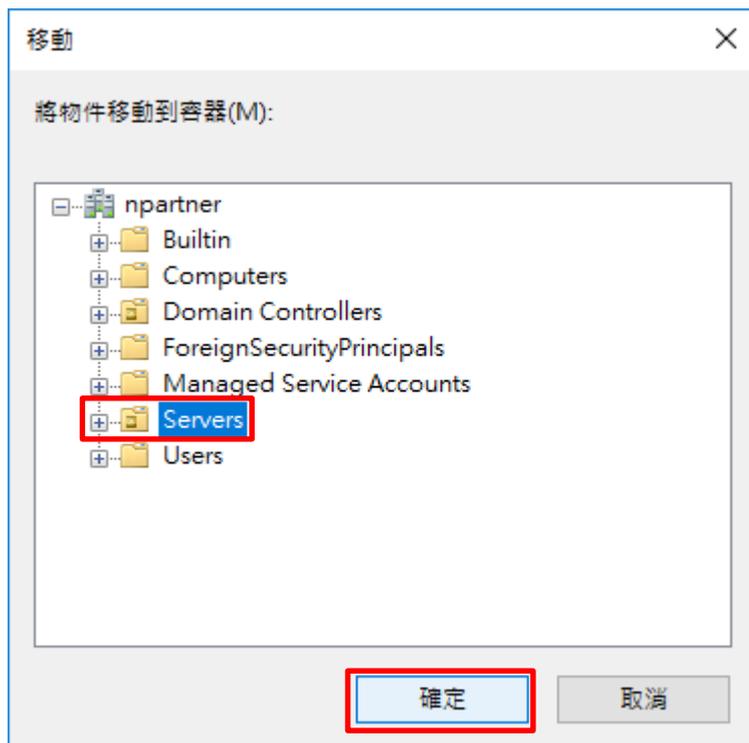
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [電腦名稱(Win2016)] 按滑鼠右鍵 -> 點選 [移動]



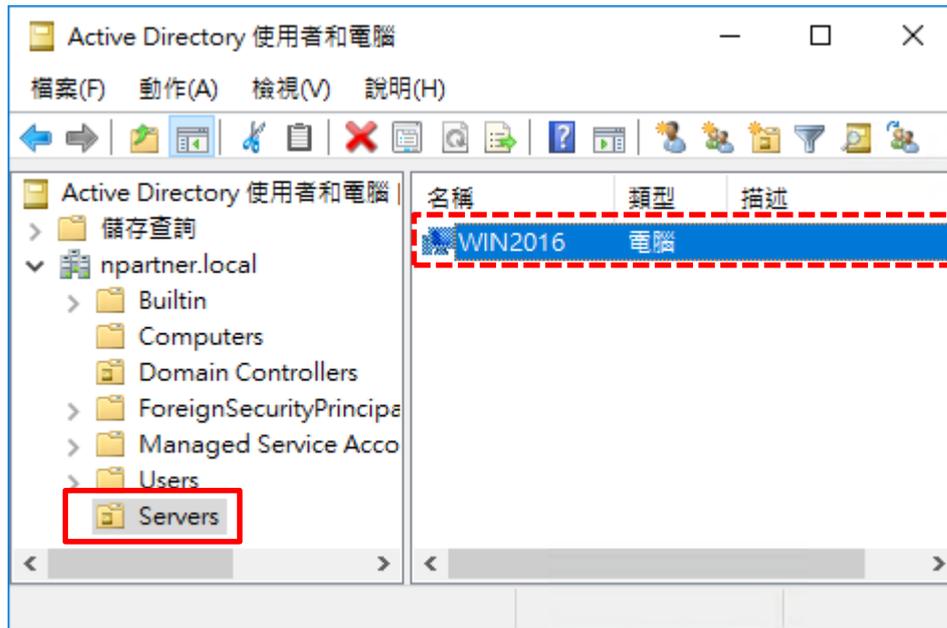
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按下 [確定]



(6) 確認伺服器已移動至新的組織單位

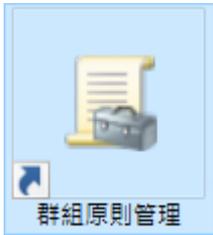
點選 [Servers] 組織單位，確認 [電腦名稱(Win2016)] 伺服器已移動



5.1.2 群組原則設定

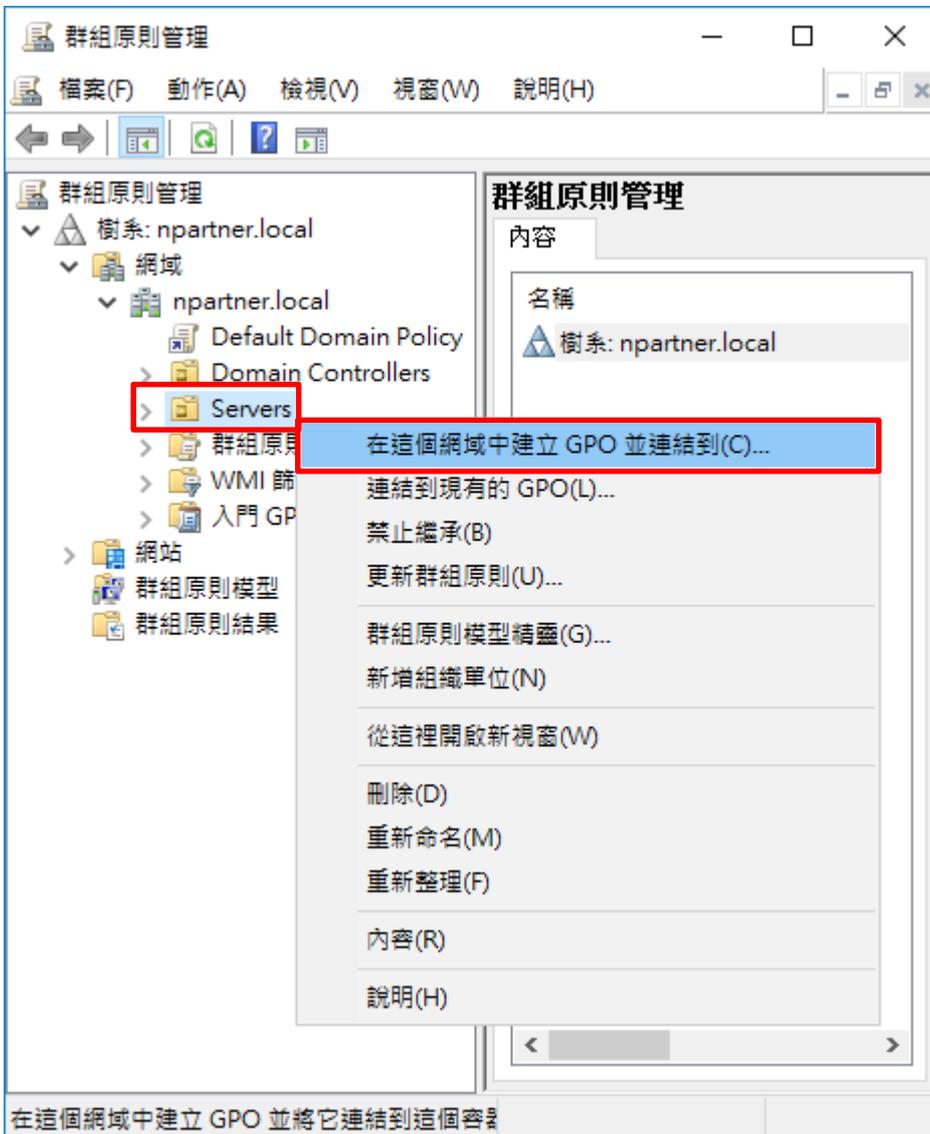
(1) 開啟群組原則管理

開啟 [群組原則管理]



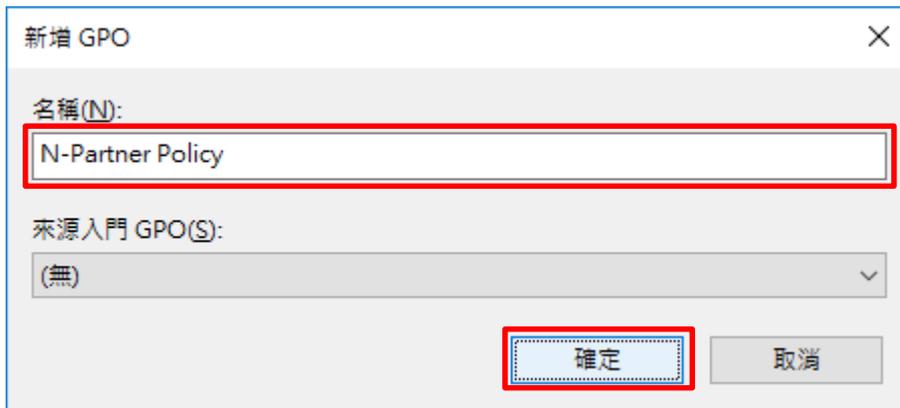
(2) 在 Servers 組織單位，新增群組原則物件

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...]



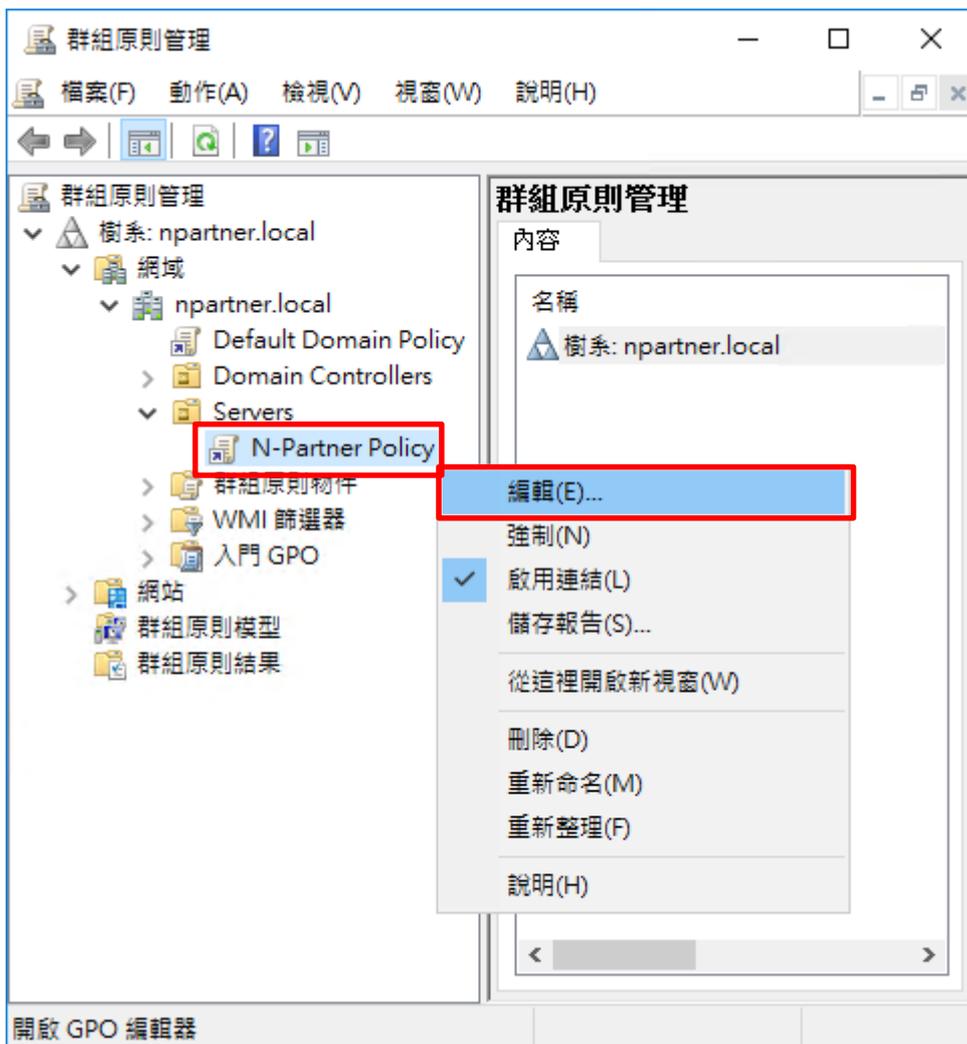
(3) 輸入群組原則物件名稱

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



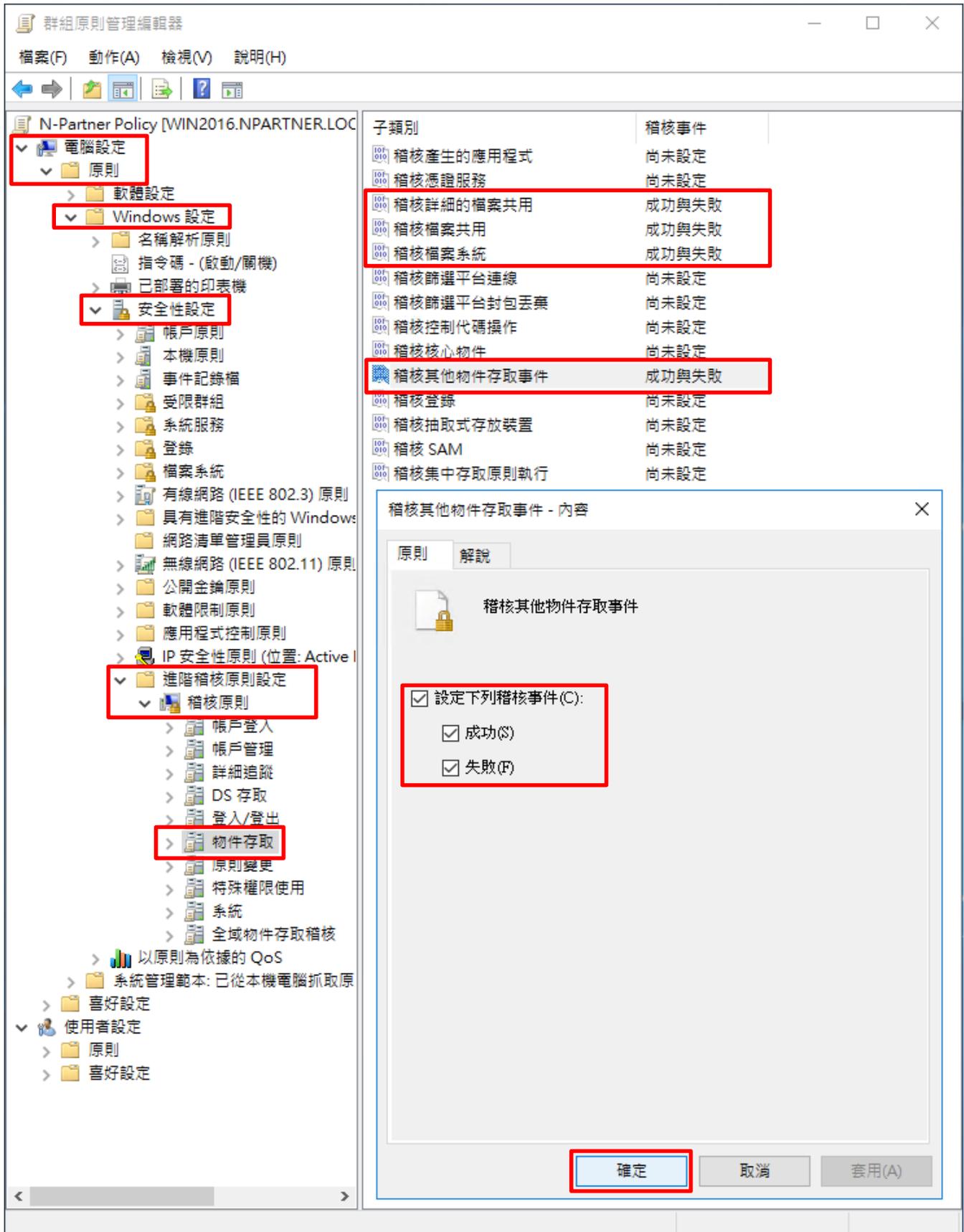
(4) 編輯群組原則物件

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



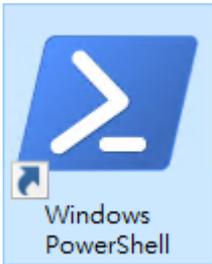
(5) 進階稽核原則：物件存取

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [進階稽核原則設定] -> [稽核原則] -> [物件存取] -> 點選 [稽核詳細的檔案共用], [稽核檔案共用], [稽核檔案系統], [稽核其他物件存取事件] 項目 -> 勾選 [設定下列稽核事件:] & [成功] & [失敗] -> 按下 [確定]



(6) 在 AD 網域伺服器，開啟 Windows PowerShell

開啟 [Windows PowerShell]



(7) 更新 Windows File 伺服器群組原則

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

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Invoke-GPUUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force` being entered and executed. The output is not visible, only the prompt `PS C:\Users\Administrator>` is shown after the command.

紅色文字部位請輸入 Windows File 伺服器名稱

`Invoke-GPUUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force`

(8) 產生 Windows File 伺服器群組原則報表

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

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Get-GPResultantSetofPolicy -Computer Win2016 -Path C:\tmp\Win2016.html -ReportType html` being entered and executed. The output is a list of properties: `RsopMode : Logging`, `Namespace : \\Win2016\Root\Rsop\NS97B75E00_796F_4ED6_91DC_12D0926385FB`, `LoggingComputer : Win2016`, `LoggingUser : NPARTNER\administrator`, and `LoggingMode : Computer`. The prompt `PS C:\Users\Administrator>` is shown at the bottom.

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

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

5.2 工作群組

(1) 開啟本機群組原則編輯器

點選 [搜尋] -> 輸入 `group policy` -> 點選 [Edit group policy]



(2) 進階稽核原則：物件存取

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [系統稽核原則 - 本機群組原則物件] -> [物件存取] -> 點選 [稽核詳細的檔案共用], [稽核檔案共用], [稽核檔案系統], [稽核其他物件存取事件] 項目 -> 勾選 [設定下列稽核事件:] & [成功] & [失敗] -> 按下 [確定]

The screenshot displays the Windows Group Policy Editor interface. The left-hand navigation pane shows the hierarchy: Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Objects > Object Access. The right-hand pane shows a list of audit policies, with 'Audit Other Object Access Events' selected. Below this, a dialog box titled 'Audit Other Object Access Events - Content' is open, showing the configuration for this policy. The 'Principle' tab is active, and the 'Audit Other Object Access Events' policy is listed. Under the 'Audit the following events (C):' section, both 'Success (S)' and 'Failure (F)' are checked. The 'OK' button is highlighted.

子類別	稽核事件
稽核產生的應用程式	尚未設定
稽核憑證服務	尚未設定
稽核詳細的檔案共用	成功與失敗
稽核檔案共用	成功與失敗
稽核檔案系統	成功與失敗
稽核篩選平台連線	尚未設定
稽核篩選平台封包丟棄	尚未設定
稽核控制代碼操作	尚未設定
稽核核心物件	尚未設定
稽核其他物件存取事件	成功與失敗
稽核登錄	尚未設定
稽核抽取式存放裝置	尚未設定
稽核 SAM	尚未設定
稽核集中存取原則執行	尚未設定

稽核其他物件存取事件 - 內容

原則 解說

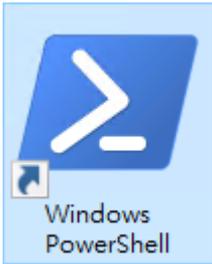
稽核其他物件存取事件

設定下列稽核事件(C):

- 成功(S)
- 失敗(F)

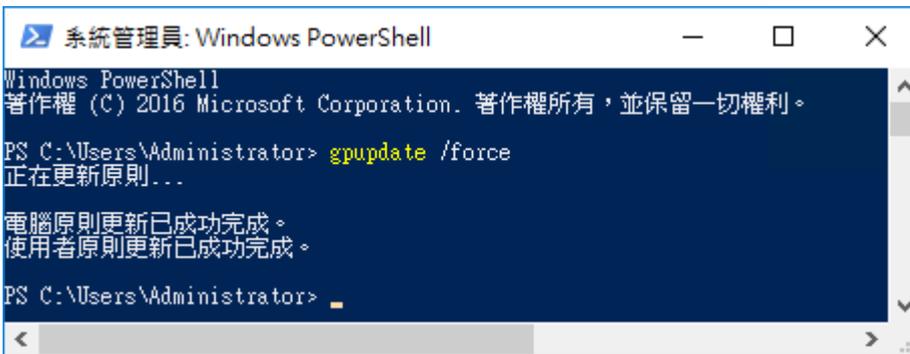
確定 取消 套用(A)

(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

PS C:\> gpupdate /force



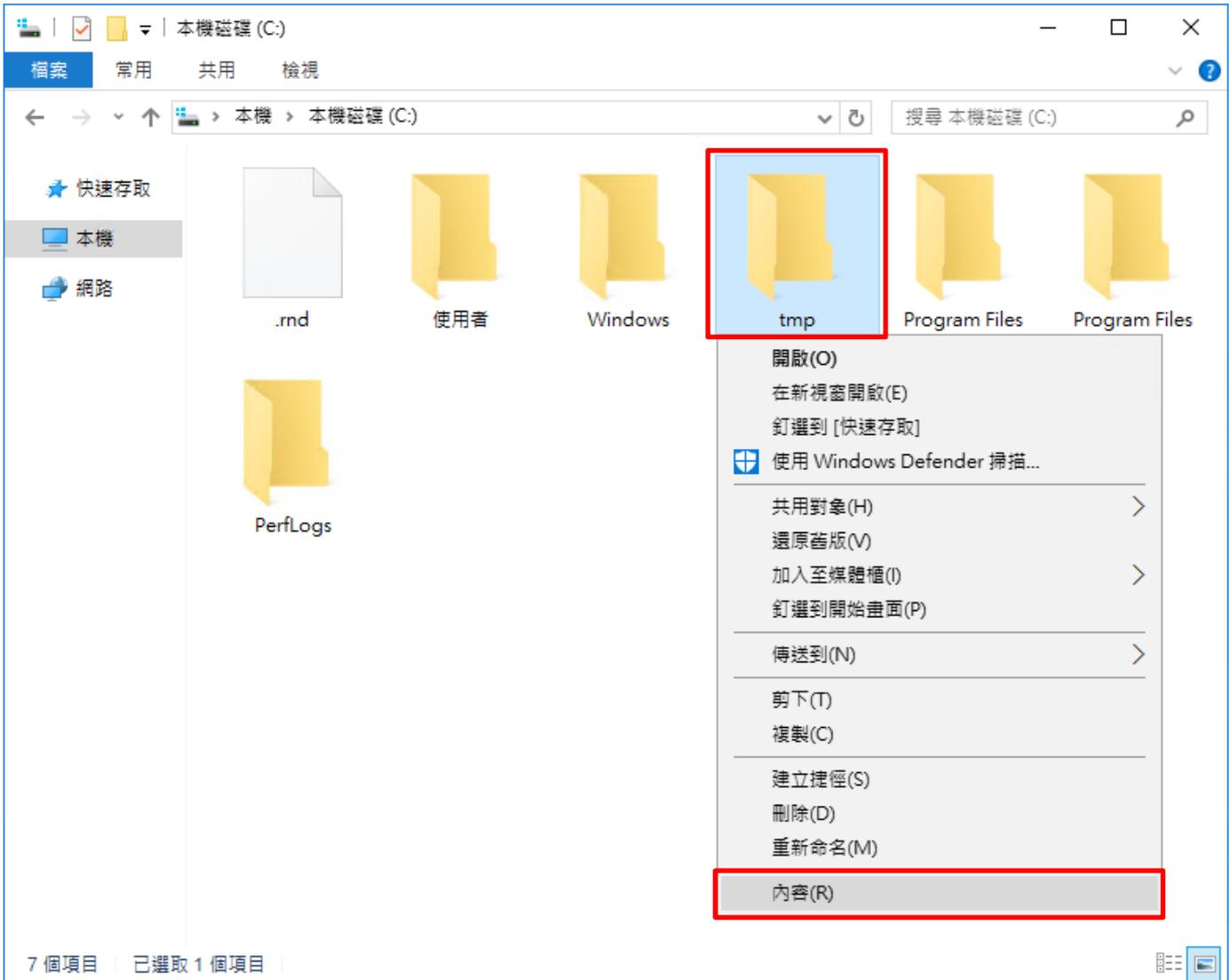
(6) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

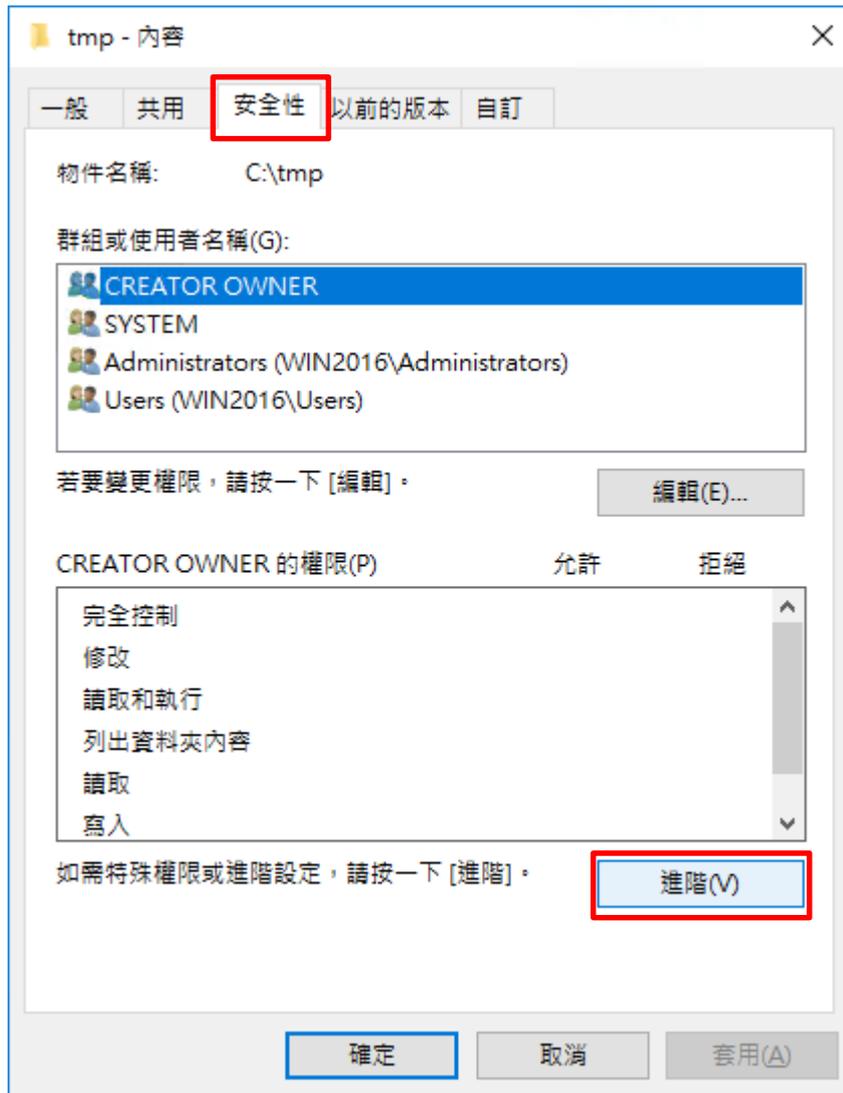
```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
安全性系統延伸      沒有稽核
系統完整性          沒有稽核
IPSEC driver        沒有稽核
其他系統事件        沒有稽核
安全性狀態變更      沒有稽核
登入/登出
登入                沒有稽核
登出                沒有稽核
帳戶鎖定            沒有稽核
IPsec 主要模式      沒有稽核
IPsec 快速模式      沒有稽核
IPsec 延伸模式      沒有稽核
特殊登入            沒有稽核
其他登入/登出事件  沒有稽核
網際原則伺服器      沒有稽核
使用者/裝置宣告    沒有稽核
群組成員資格        沒有稽核
物件存取
檔案系統            成功與失敗
registry            沒有稽核
核心物件            沒有稽核
SAM                 沒有稽核
憑證服務            沒有稽核
產生的應用程式      沒有稽核
控制代碼操縱        沒有稽核
檔案共用            成功與失敗
篩選平台封包丟棄    沒有稽核
篩選平台連線        沒有稽核
其他物件存取事件    成功與失敗
詳細檔案共用        成功與失敗
抽取式存放裝置      沒有稽核
集中原則暫存        沒有稽核
特殊權限使用
非機密特殊權限使用  沒有稽核
其他特殊權限使用事件 沒有稽核
機密特殊權限使用    沒有稽核
詳細追蹤
建立處理程序        沒有稽核
終止處理程序        沒有稽核
DPAPI 活動          沒有稽核
RPC 事件            沒有稽核
隨插即用事件        沒有稽核
Token Right Adjusted Events 沒有稽核
原則變更
稽核原則變更        沒有稽核
驗證原則變更        沒有稽核
授權原則變更        沒有稽核
MPSSVC 規則層級原則變更 沒有稽核
篩選平台原則變更    沒有稽核
其他原則變更事件    沒有稽核
帳戶管理
電腦帳戶管理        沒有稽核
安全性群組管理      沒有稽核
發佈群組管理        沒有稽核
應用程式群組管理    沒有稽核
其他帳戶管理事件    沒有稽核
使用者帳戶管理      沒有稽核
DS 存取
目錄服務存取        沒有稽核
目錄服務變更        沒有稽核
目錄服務複寫        沒有稽核
詳細目錄服務複寫    沒有稽核
帳戶登入
Kerberos 服務票證操作 沒有稽核
其他帳戶登入事件    沒有稽核
Kerberos 驗證服務    沒有稽核
認證驗證            沒有稽核
PS C:\Users\Administrator>
```

5.3 稽核資料夾設定

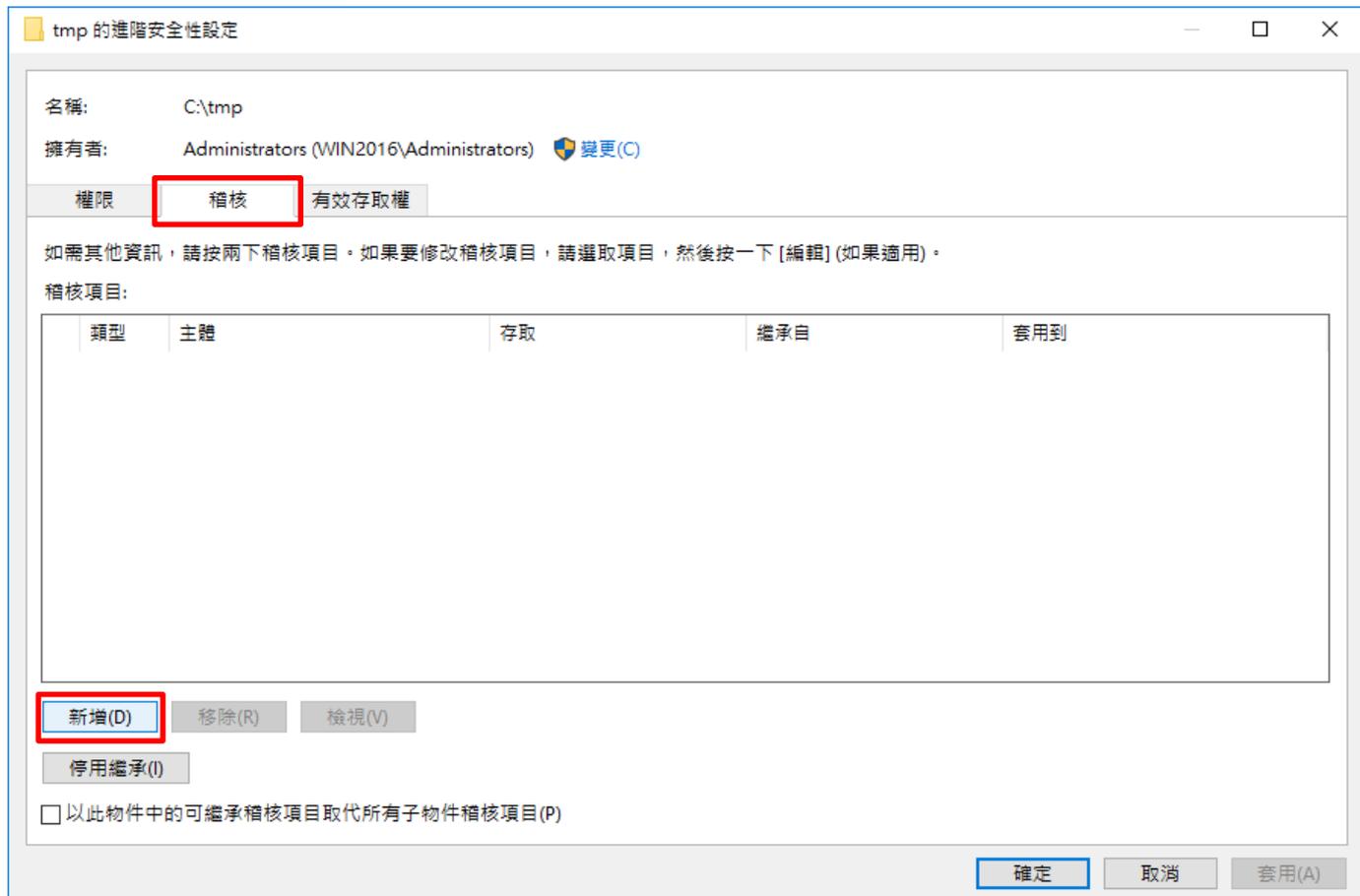
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



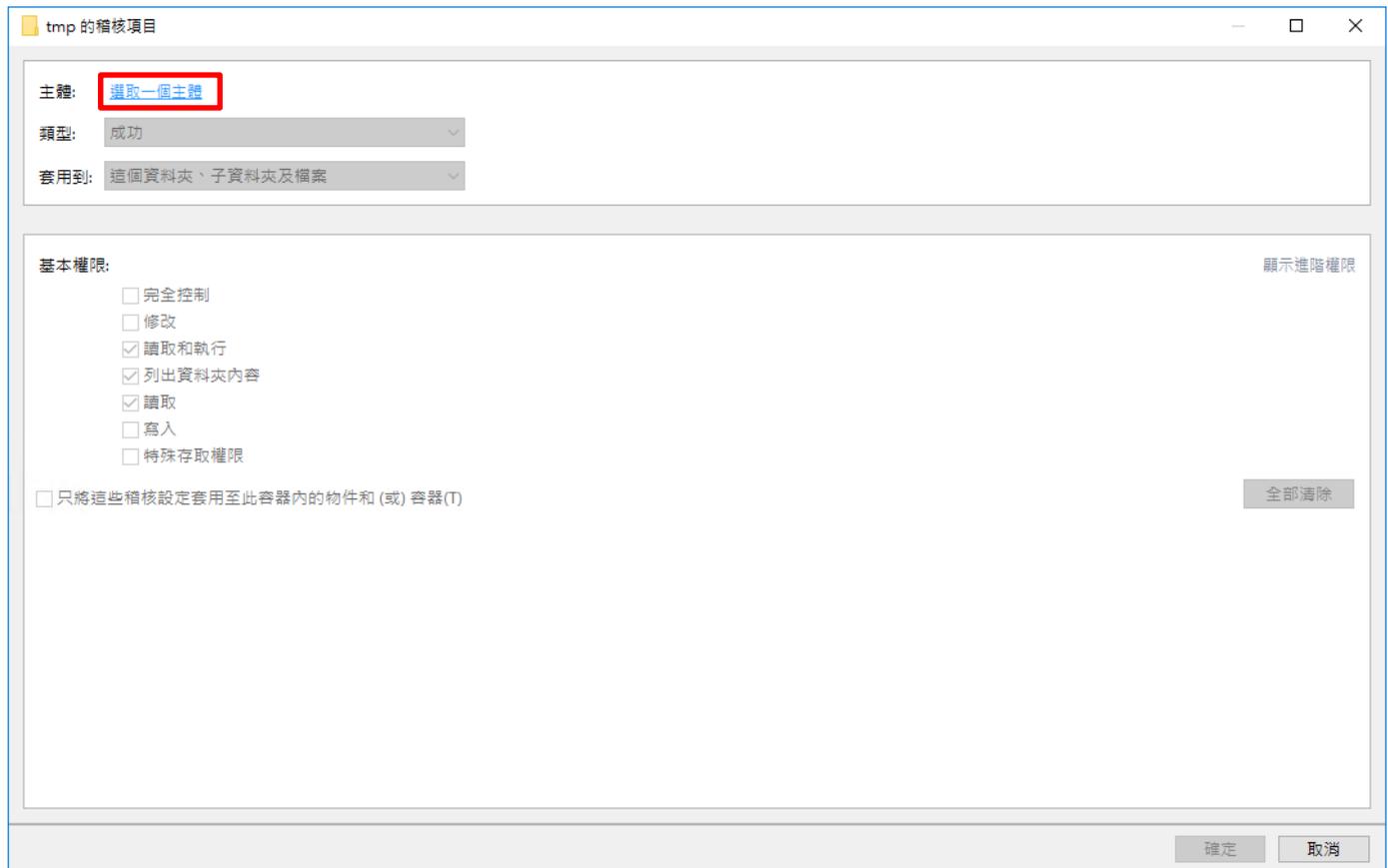
(2) 點選 [安全性] 頁面 -> 按下 [進階]



(3) 點選 [稽核] 頁面 -> 按下 [新增]



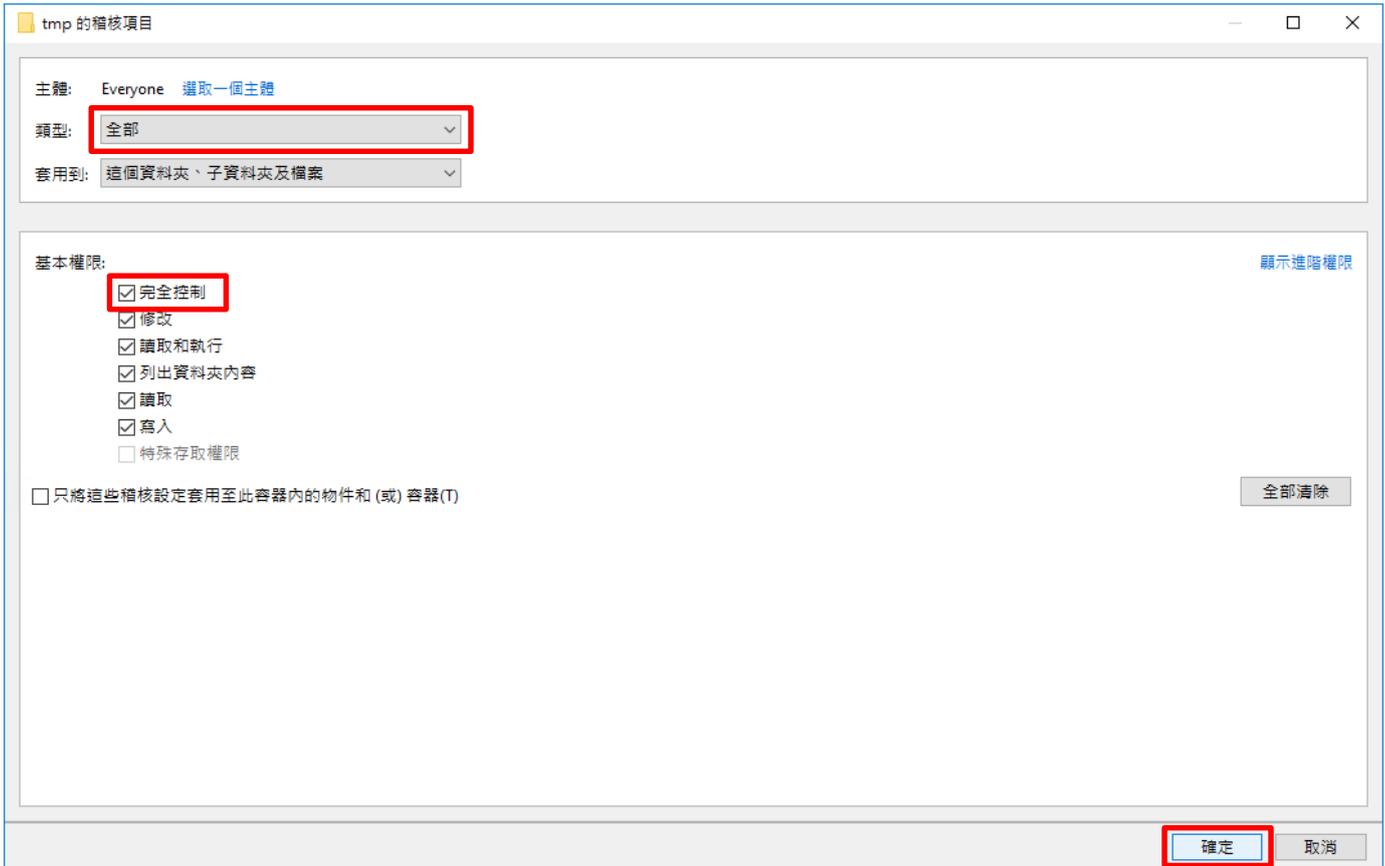
(4) 點選 [選取一個主體]



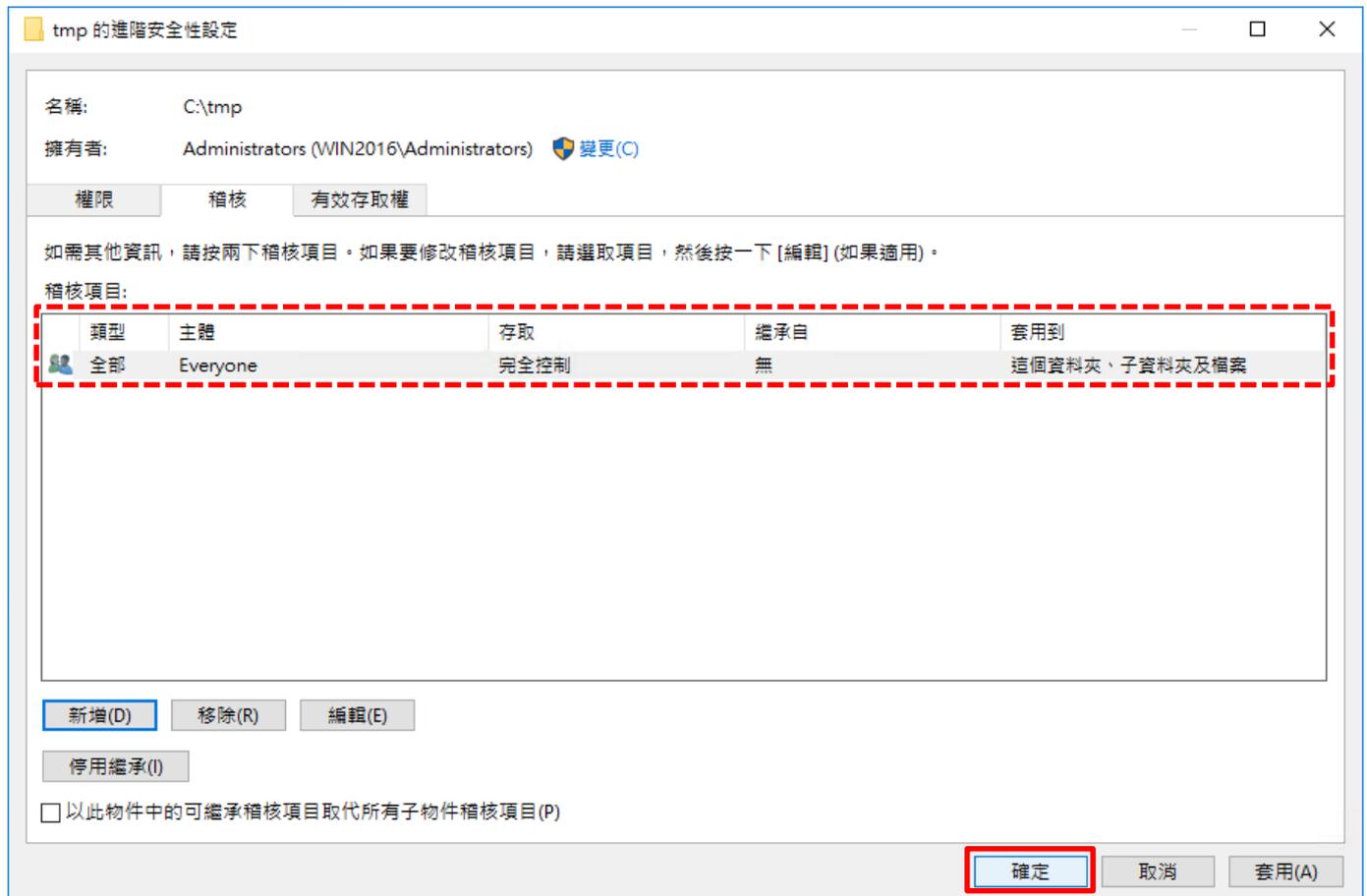
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



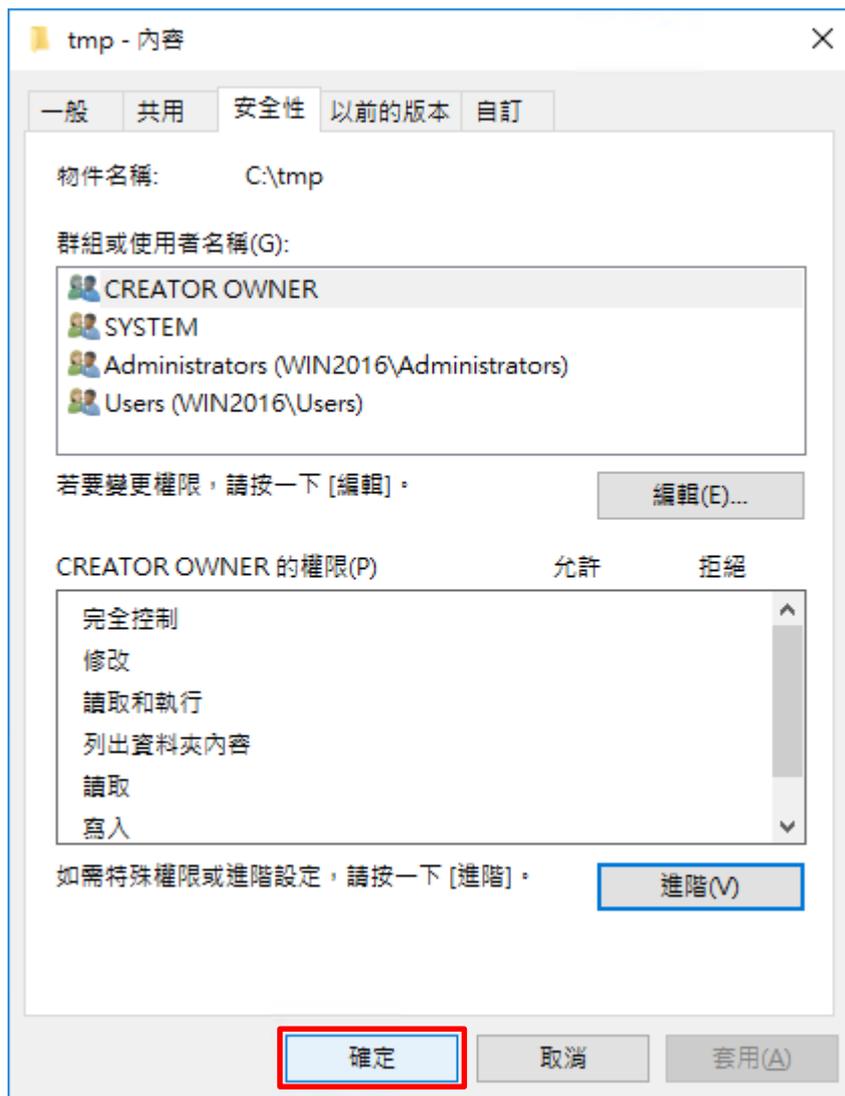
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 按下 [確定]



6. Windows 2019

以下分別為網域和工作群組設定方式。

6.1 網域

6.1.1 組織單位設定

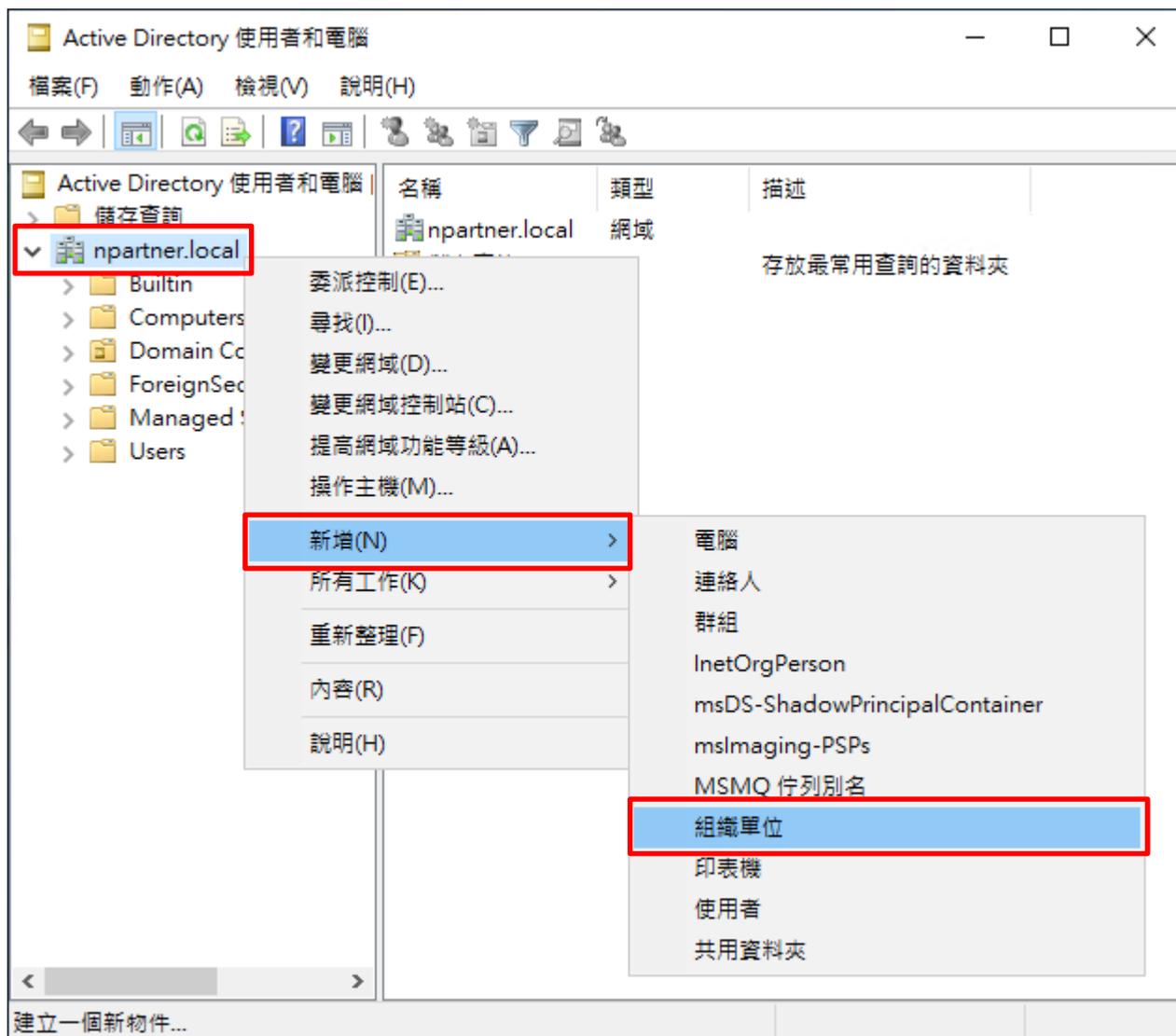
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



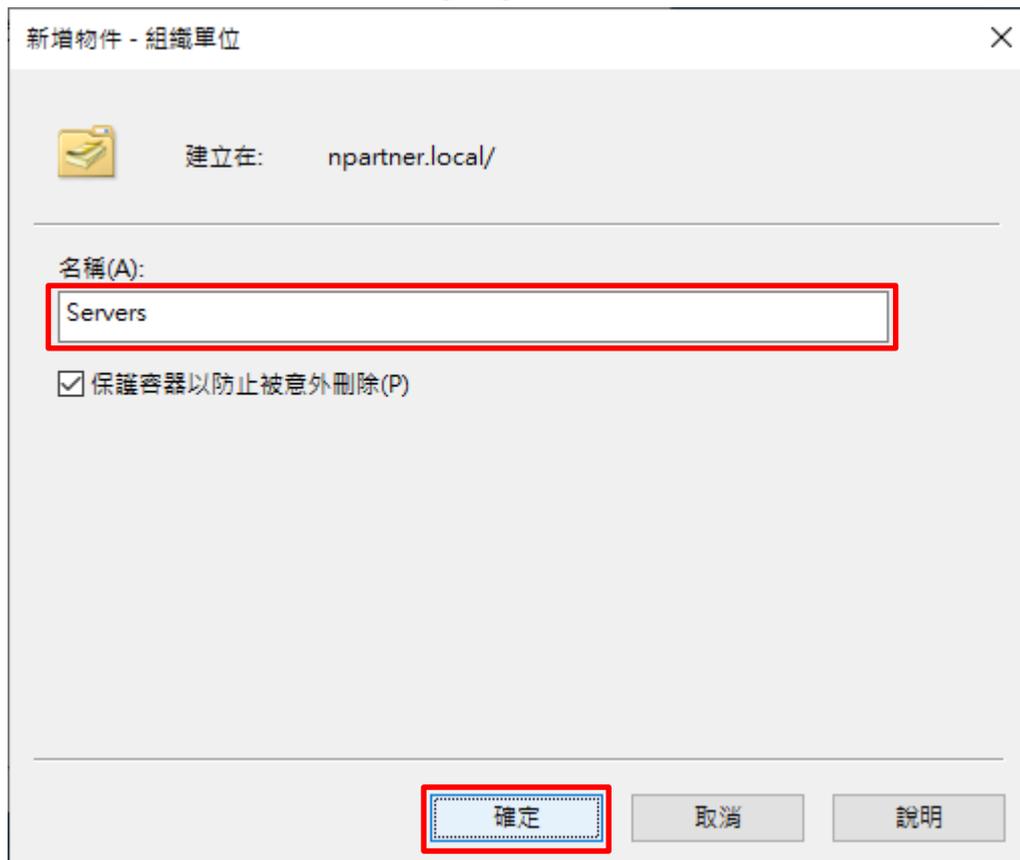
(2) 新增組織單位

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



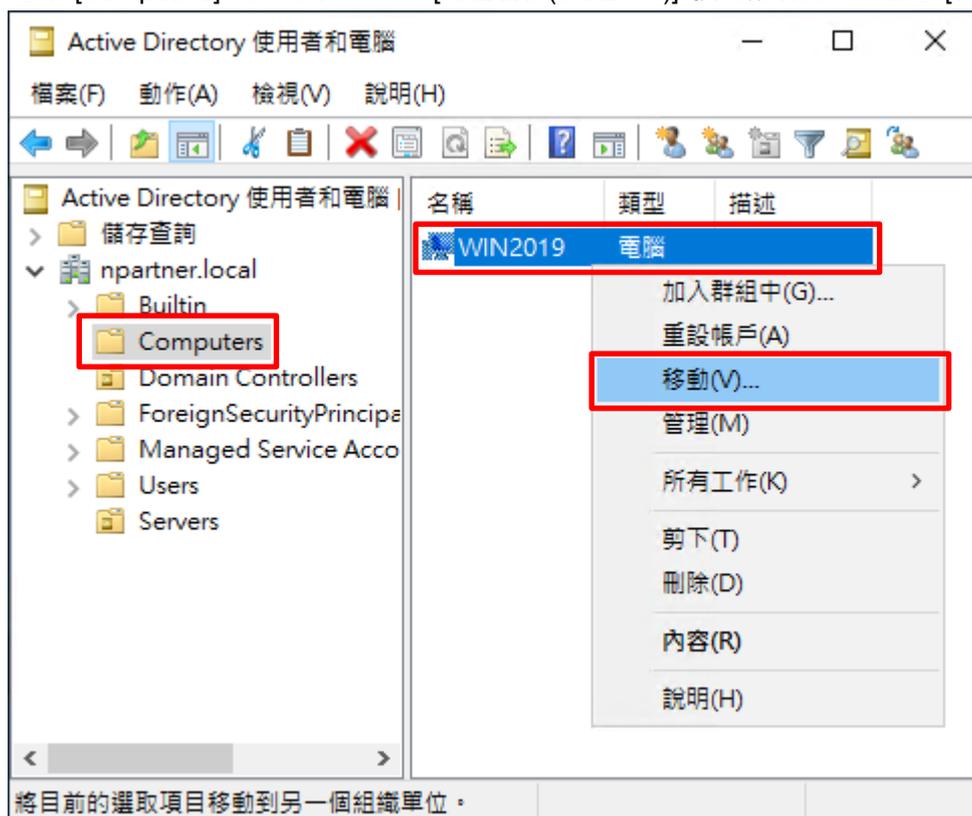
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



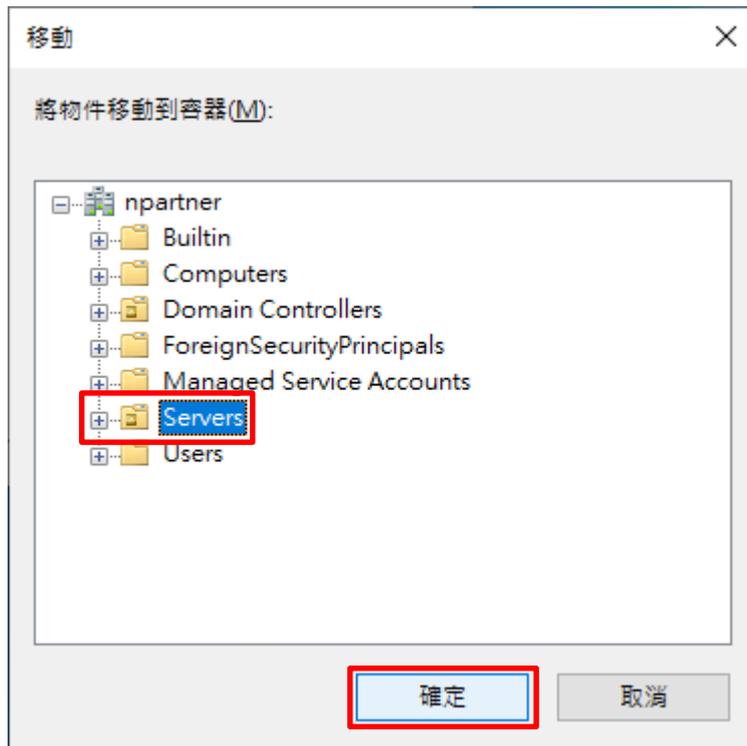
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [電腦名稱(Win2019)] 按滑鼠右鍵 -> 點選 [移動]



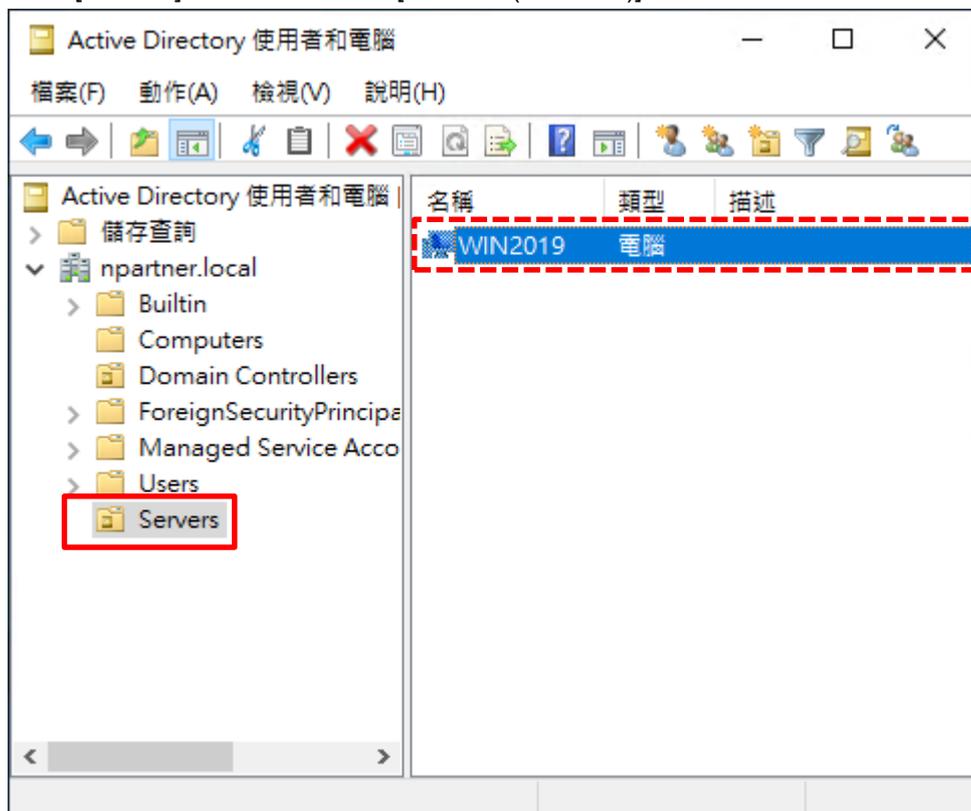
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按下 [確定]



(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位，確認 [電腦名稱(Win2019)] 伺服器已移動



6.1.2 群組原則設定

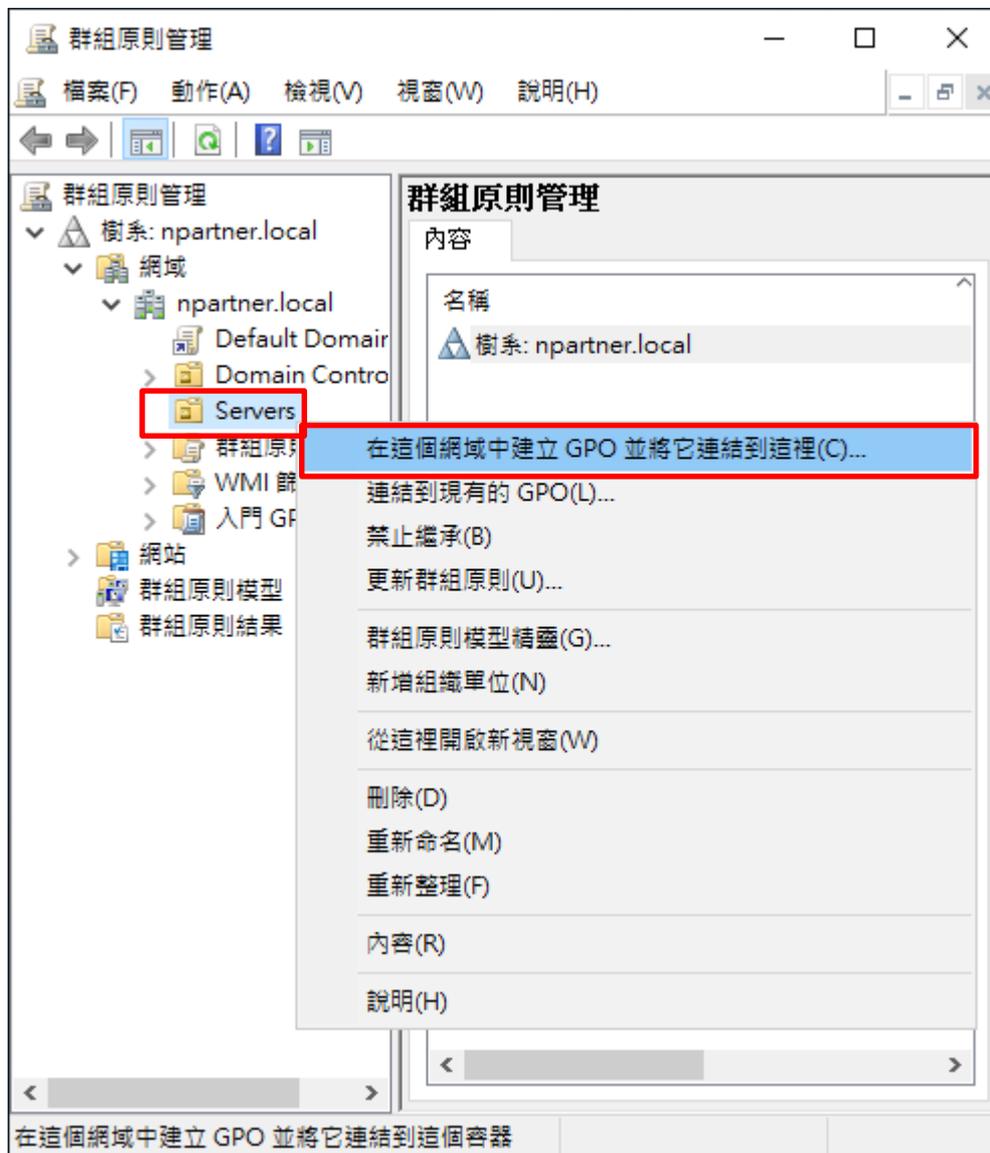
(1) 開啟群組原則管理

開啟 [Group Policy Management(群組原則管理)]



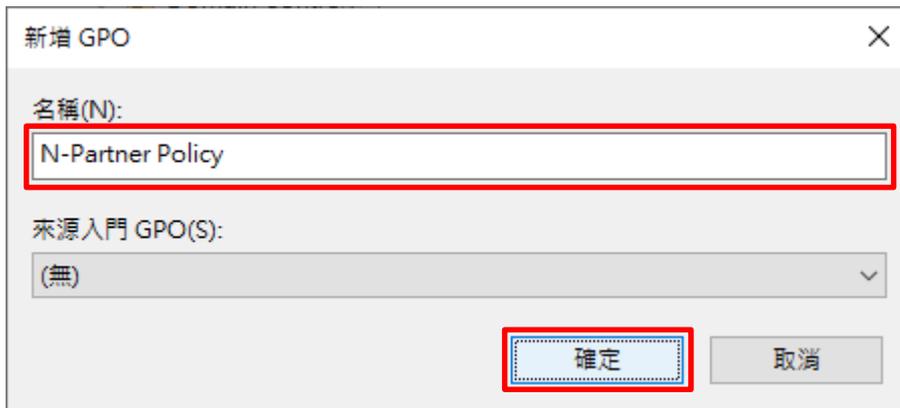
(2) 在 Servers 組織單位，新增群組原則物件

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...]



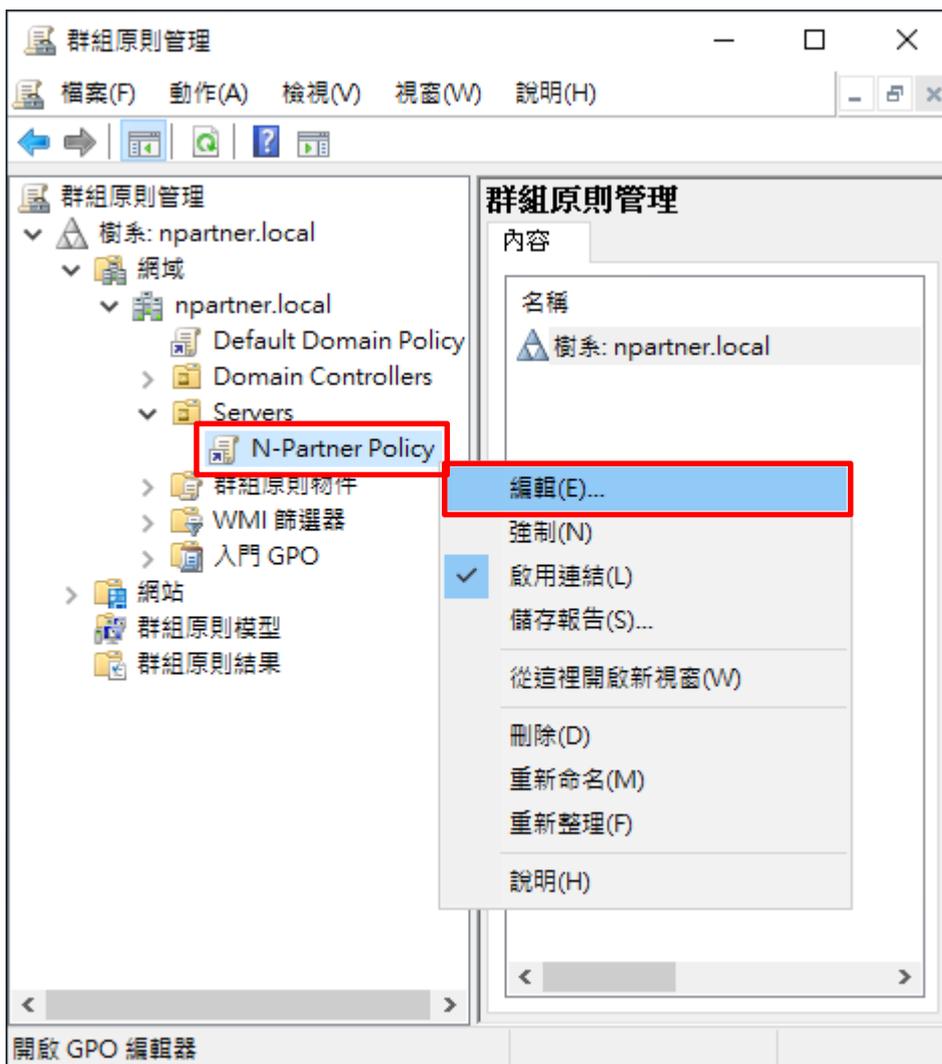
(3) 輸入群組原則物件名稱

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



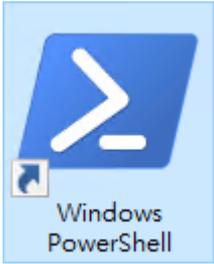
(4) 編輯群組原則物件

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



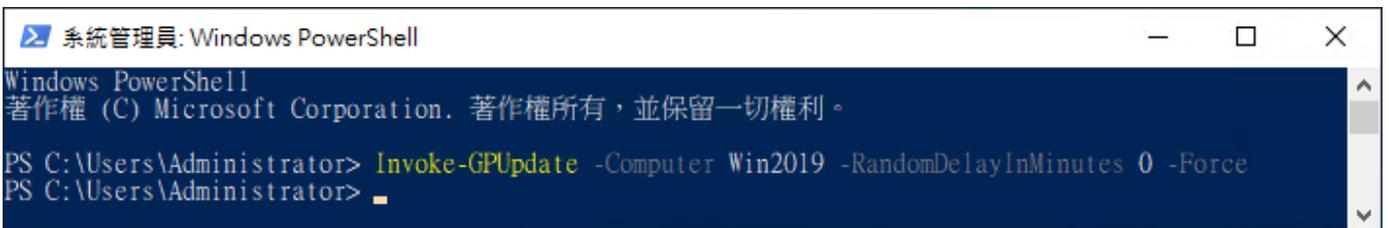
(6) 在 AD 網域伺服器，開啟 Windows PowerShell

開啟 [Windows PowerShell]



(7) 更新 Windows File 伺服器群組原則

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

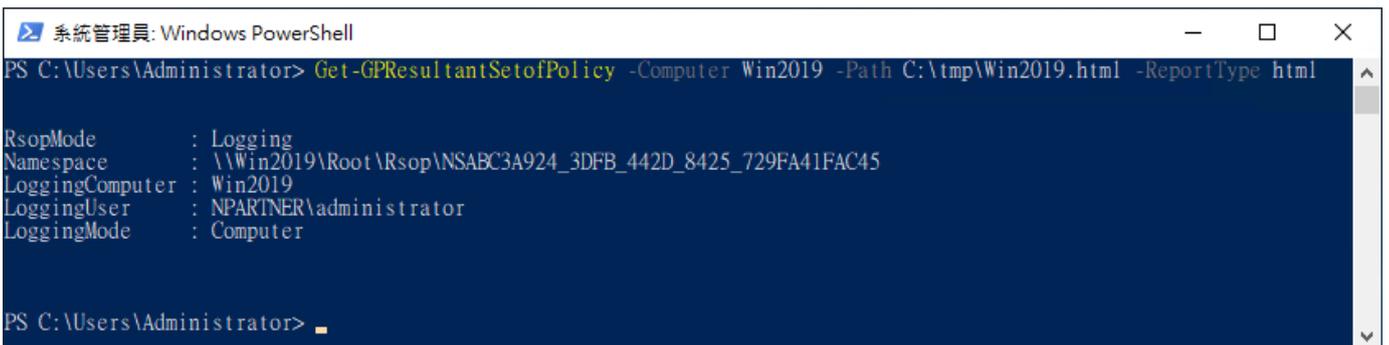
A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The terminal content shows the command `Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force` being entered and executed. The output is blank, indicating the command ran successfully. The prompt is `PS C:\Users\Administrator>`.

紅色文字部位請輸入 Windows File 伺服器名稱

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

(8) 產生 Windows File 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 terminal content shows the command `Get-GPResultantSetofPolicy -Computer Win2019 -Path C:\tmp\Win2019.html -ReportType html` being entered and executed. The output is a list of properties: `RsopMode : Logging`, `Namespace : \\Win2019\Root\Rsop\NSABC3A924_3DFB_442D_8425_729FA41FAC45`, `LoggingComputer : Win2019`, `LoggingUser : NPARTNER\administrator`, and `LoggingMode : Computer`. The prompt is `PS C:\Users\Administrator>`.

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

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

(9) 開啟報表 · 確認 Windows File 伺服器 · 套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WIN2019
資料收集: 2020/1/16 下午 05:24:12 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

帳戶原則/Kerberos 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

物件存取 隱藏

原則	設定	優勢 GPO
稽核詳細的檔案共用	成功, 失敗	N-Partner Policy
稽核檔案共用	成功, 失敗	N-Partner Policy
稽核檔案系統	成功, 失敗	N-Partner Policy
稽核其他物件存取事件	成功, 失敗	N-Partner Policy

群組原則物件 顯示

WMI 篩選器 隱藏

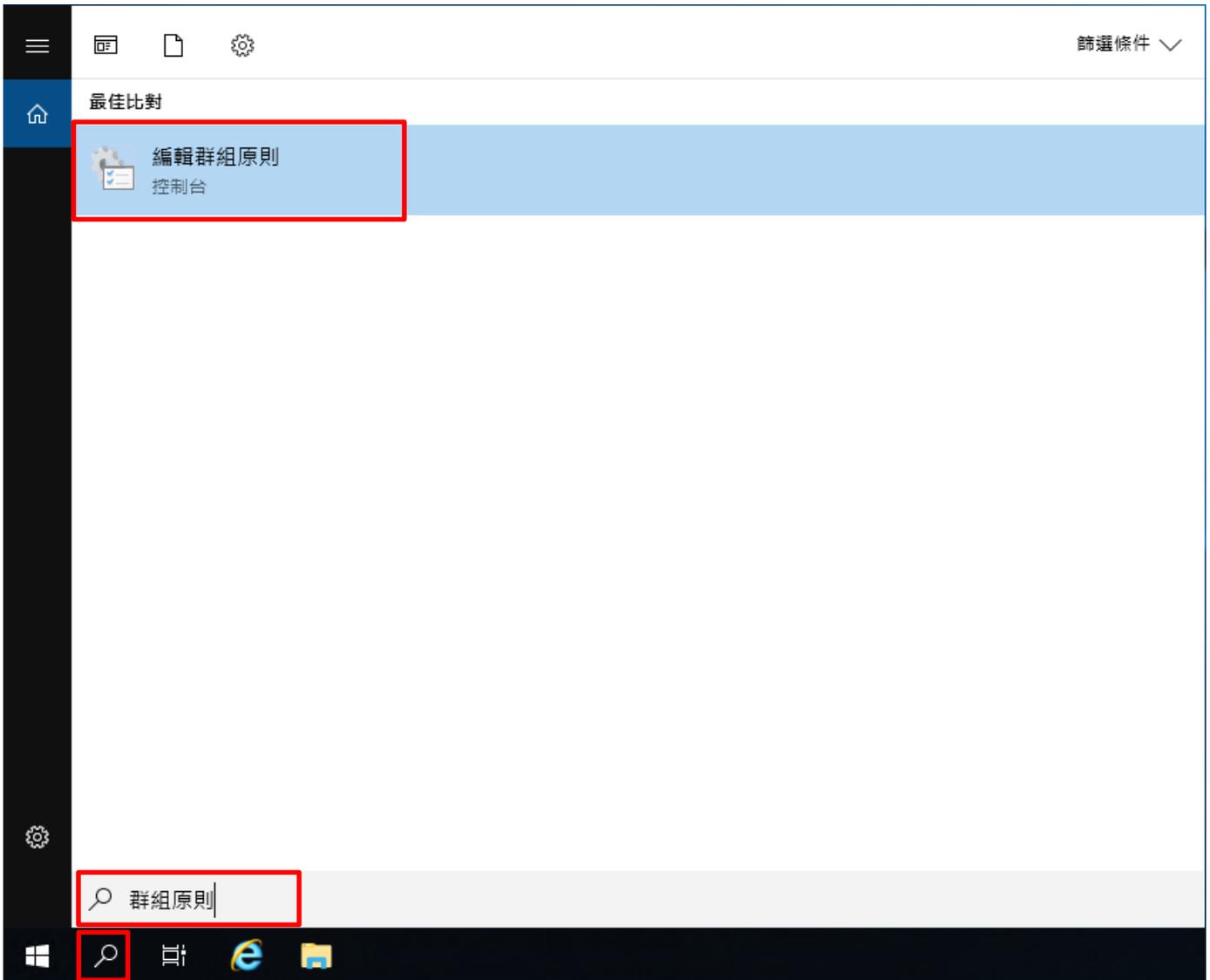
名稱	值	參照 GPO
無		

使用者詳細資料 顯示

6.2 工作群組

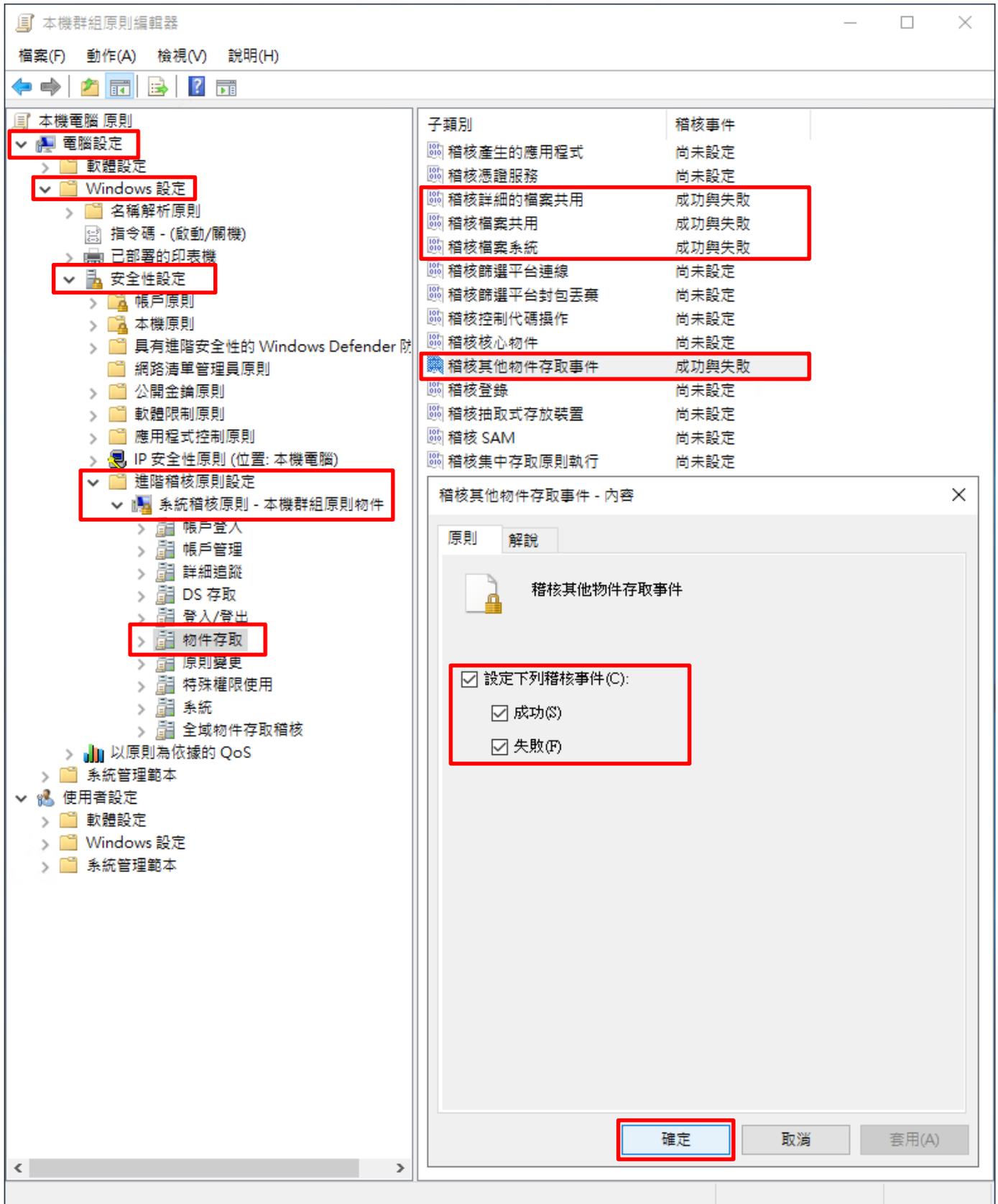
(1) 開啟本機群組原則編輯器

點選 [搜尋] -> 輸入群組原則-> 點選 [編輯群組原則]

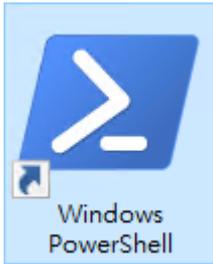


(2) 進階稽核原則：物件存取

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [系統稽核原則 - 本機群組原則物件] -> [物件存取] -> 點選 [稽核詳細的檔案共用], [稽核檔案共用], [稽核檔案系統], [稽核其他物件存取事件] 項目 -> 勾選 [設定下列稽核事件:] & [成功] & [失敗] -> 按下 [確定]



(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

PS C:\> gpupdate /force



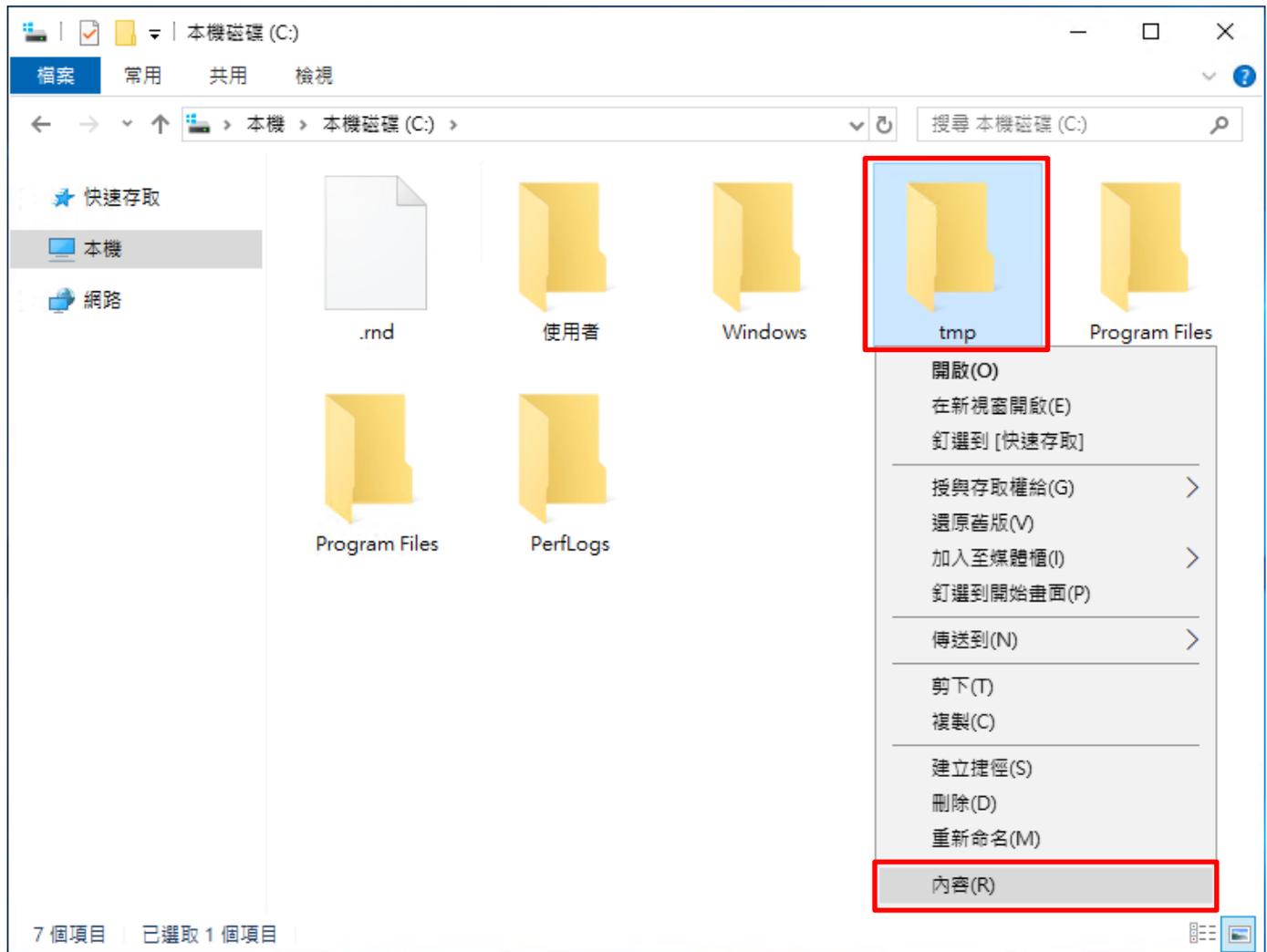
(6) 查看群組原則套用情形

PS C:\> auditpol /get /category:*

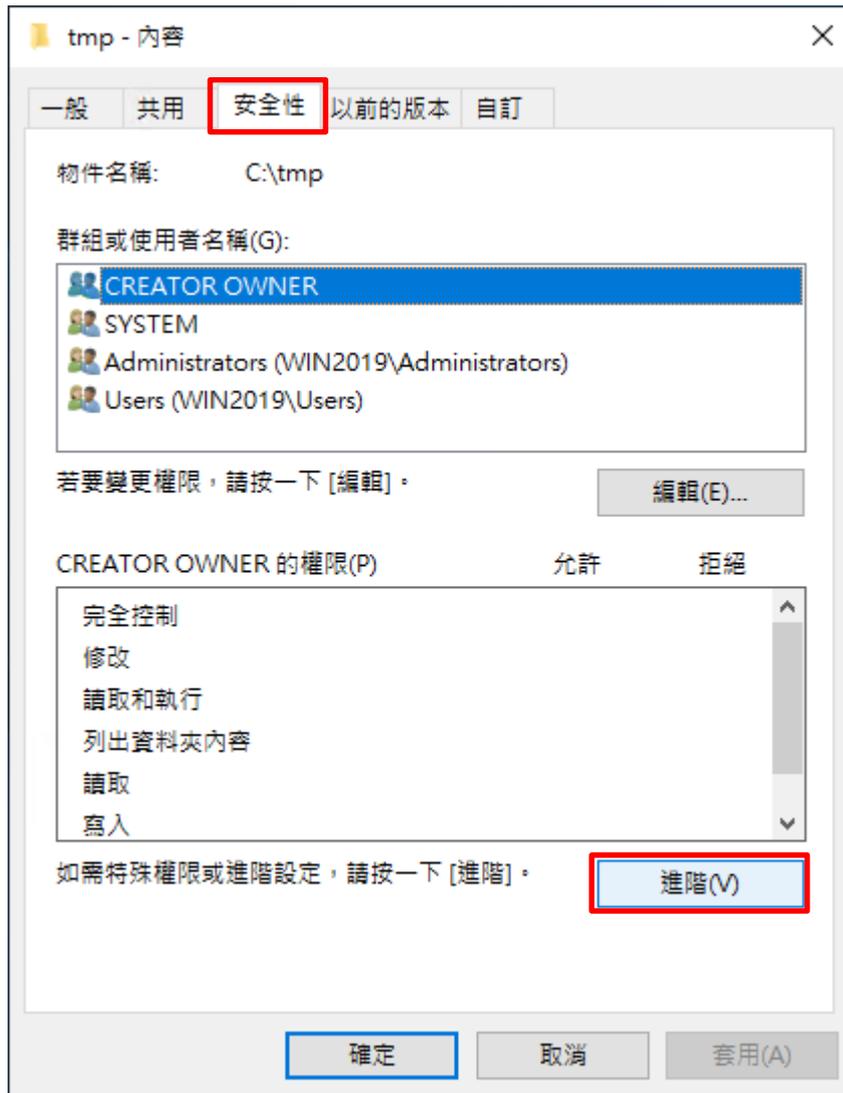
```
系統管理員: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
  安全性系統延伸      沒有稽核
  系統完整性          沒有稽核
  IPSEC driver        沒有稽核
  其他系統事件        沒有稽核
  安全性狀態變更      沒有稽核
登入/登出
  登入                沒有稽核
  登出                沒有稽核
  帳戶鎖定            沒有稽核
  IPsec 主要模式      沒有稽核
  IPsec 快速模式      沒有稽核
  IPsec 延伸模式      沒有稽核
  特殊登入            沒有稽核
  其他登入/登出事件    沒有稽核
  網路原則伺服器      沒有稽核
  使用者/裝置宣告      沒有稽核
  群組成員資格        沒有稽核
物件存取
  檔案系統            成功與失敗
  registry            沒有稽核
  核心物件            沒有稽核
  SAM                沒有稽核
  憑證服務            沒有稽核
  產生的應用程式      沒有稽核
  控制代碼操縱        沒有稽核
  檔案共用            成功與失敗
  篩選平台封包丟棄    沒有稽核
  篩選平台連線        沒有稽核
  其他物件存取事件    成功與失敗
  詳細檔案共用        成功與失敗
  抽取式存放裝置      沒有稽核
  集中原則暫存        沒有稽核
特殊權限使用
  非機密特殊權限使用  沒有稽核
  其他特殊權限使用事件 沒有稽核
  機密特殊權限使用    沒有稽核
詳細追蹤
  建立處理程序        沒有稽核
  終止處理程序        沒有稽核
  DPAPI 活動          沒有稽核
  RPC 事件            沒有稽核
  隨插即用事件        沒有稽核
  權杖權限調整事件    沒有稽核
原則變更
  稽核原則變更        沒有稽核
  驗證原則變更        沒有稽核
  授權原則變更        沒有稽核
  MPSSVC 規則層級原則變更 沒有稽核
  篩選平台原則變更    沒有稽核
  其他原則變更事件    沒有稽核
帳戶管理
  電腦帳戶管理        沒有稽核
  安全性群組管理      沒有稽核
  發佈群組管理        沒有稽核
  應用程式群組管理    沒有稽核
  其他帳戶管理事件    沒有稽核
  使用者帳戶管理      沒有稽核
DS 存取
  目錄服務存取        沒有稽核
  目錄服務變更        沒有稽核
  目錄服務複寫        沒有稽核
  詳細目錄服務複寫    沒有稽核
帳戶登入
  Kerberos 服務票證操作 沒有稽核
  其他帳戶登入事件    沒有稽核
  Kerberos 驗證服務    沒有稽核
  認證驗證            沒有稽核
PS C:\Users\Administrator>
```

6.3 稽核資料夾設定

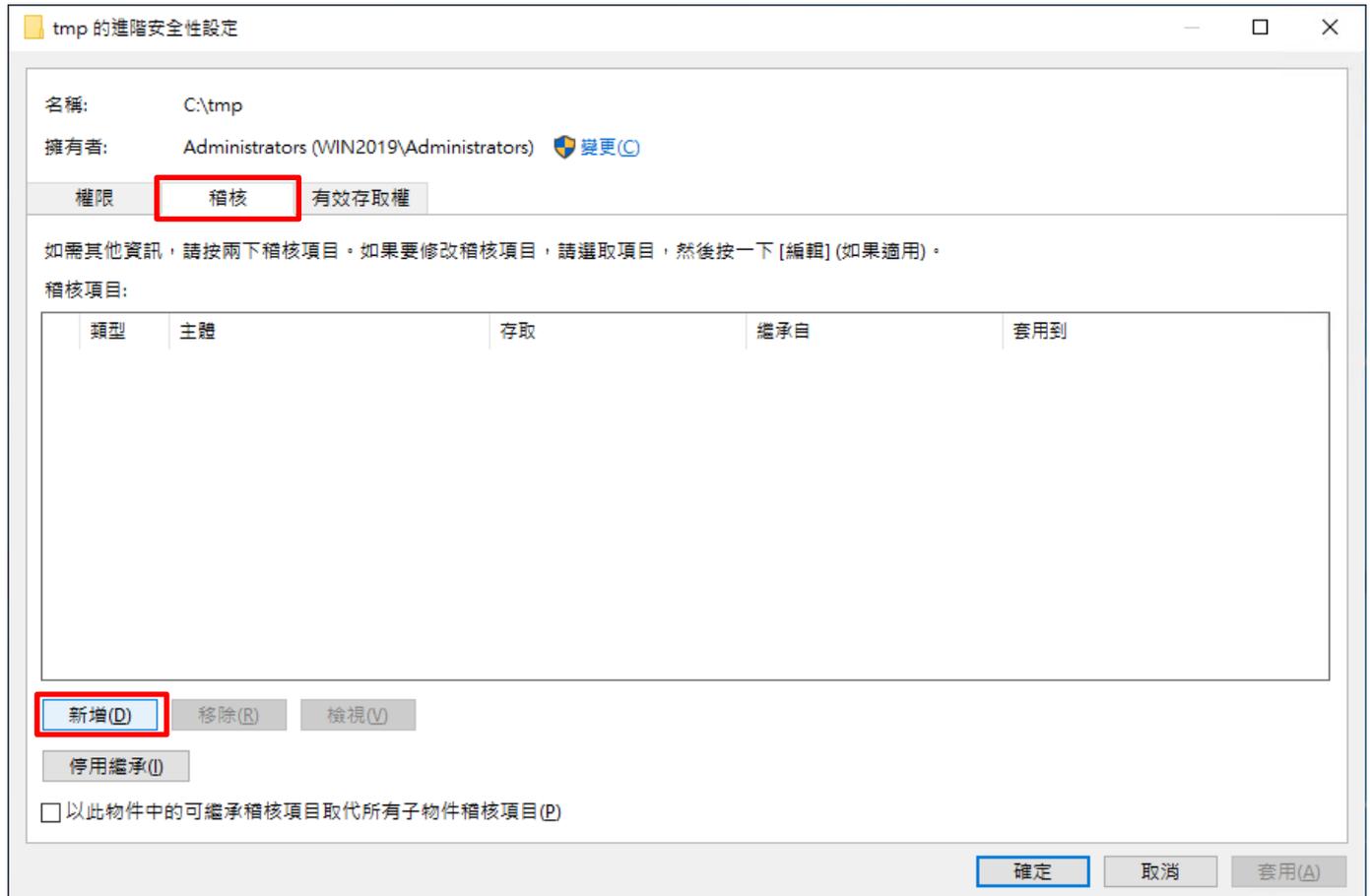
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



(2) 點選 [安全性] 頁面 -> 按下 [進階]



(3) 點選 [稽核] 頁面 -> 按下 [新增]



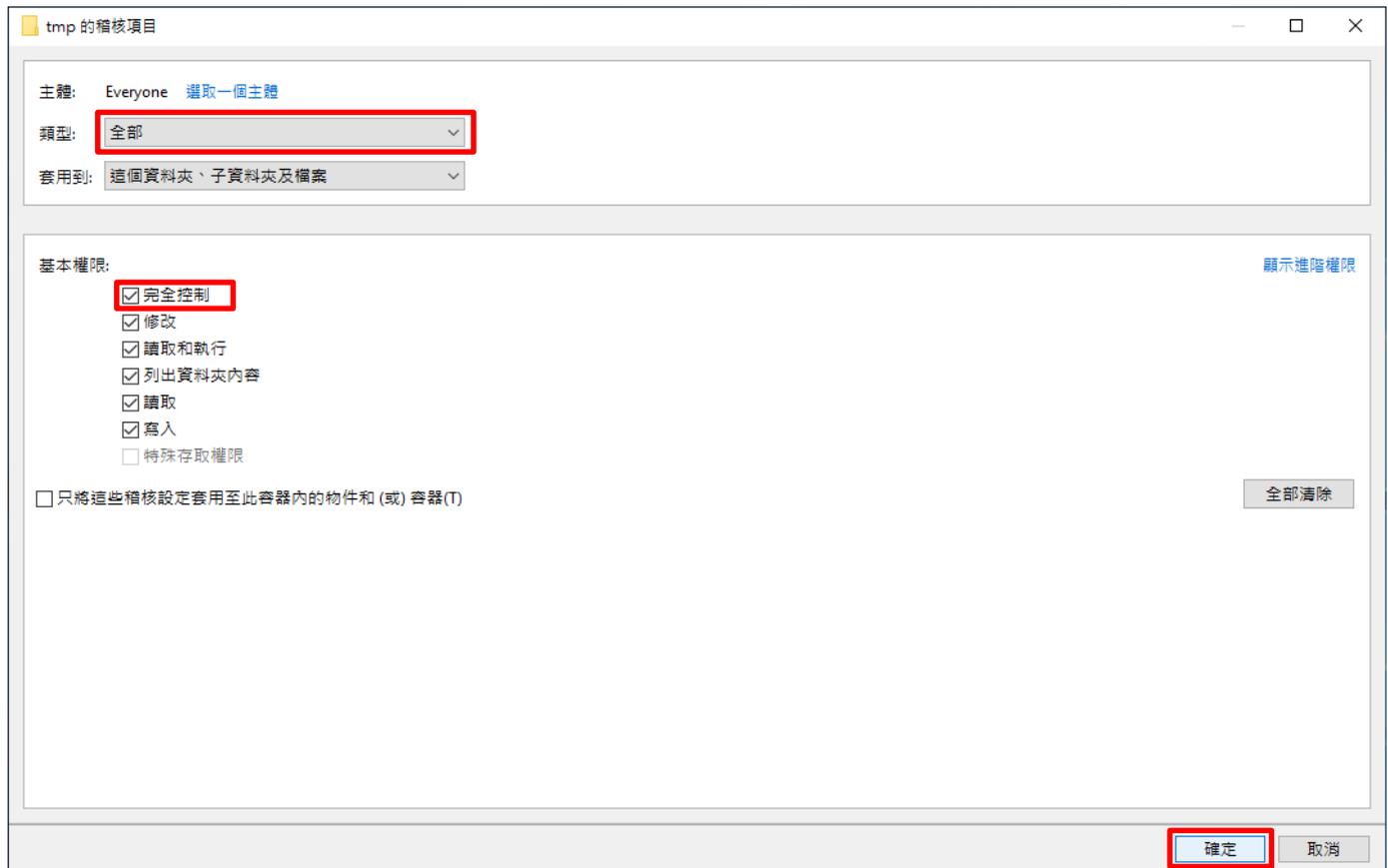
(4) 點選 [選取一個主體]



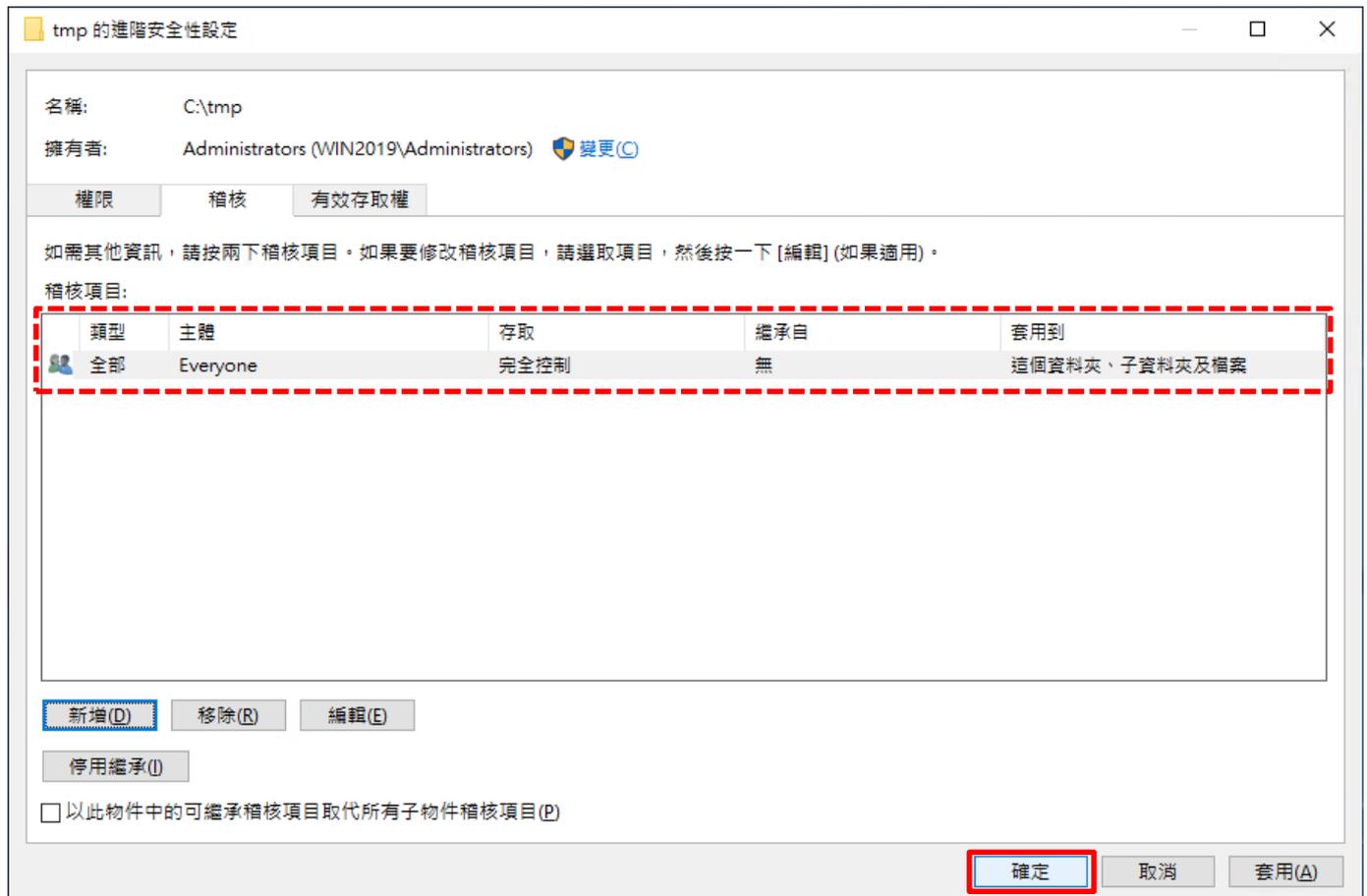
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



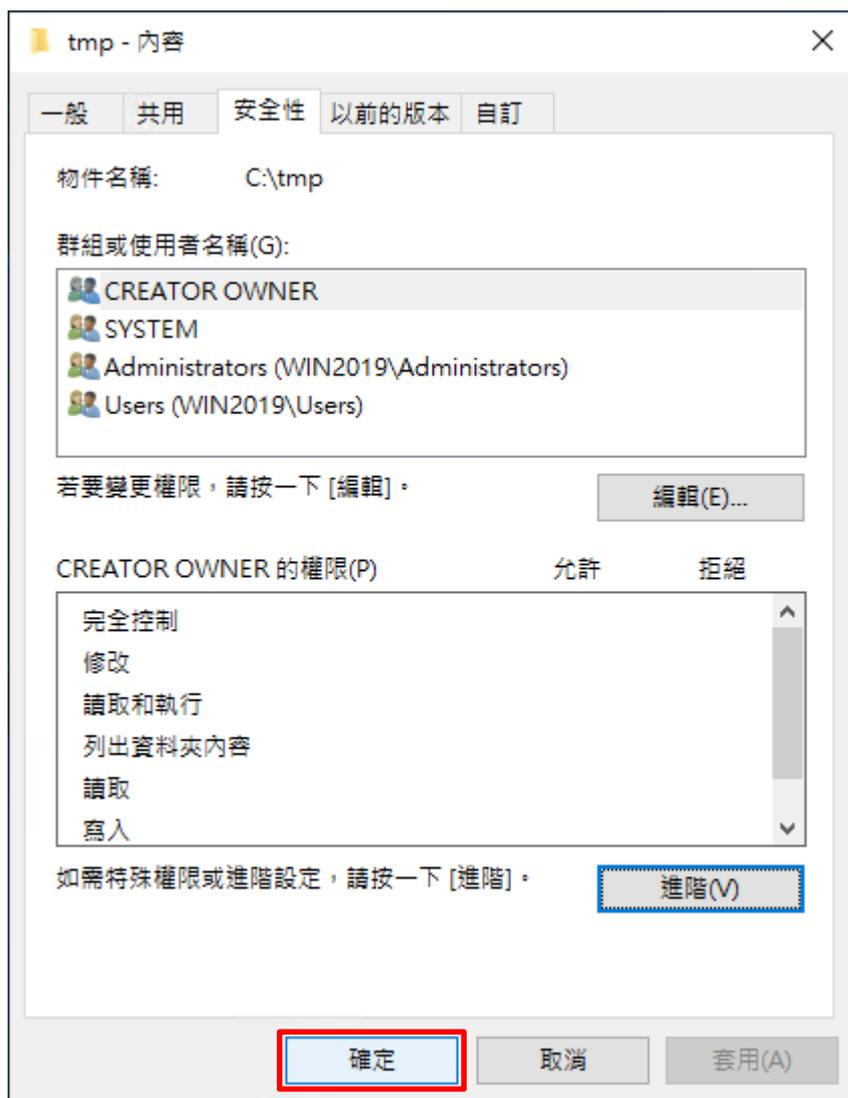
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 按下 [確定]



7. N-Reporter

(1) 新增 Windows File 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' (Events), '報表' (Reports), '智慧分析' (Smart Analysis), '設備管理' (Device Management), '設備樹狀圖' (Device Tree View), '介面列表' (Interface List), '告警樣版' (Alert Templates), '設備異常告警' (Device Abnormal Alerts), '系統管理' (System Management), and '使用者手冊' (User Manual). The '設備管理' and '設備樹狀圖' items are highlighted with a red box. 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 blue 'U' button, and a yellow speaker icon. The main content area lists 'Global (4)' and '未知設備 (0)' (Unknown Devices (0)).

7.1 Windows 2000 - 2003

(2) 設定 Windows File 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] -> 編碼方式: [BIG5] -> 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
Windows_Files-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

編碼方式
BIG5

設備進階設定

ICMP 告警樣板
----- N/A -----

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

資料保留天數

確定 取消

7.2 Windows 2008 or higher

(2) 設定 Windows File 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] -> 編碼方式: [UTF-8] -> 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
Windows_Files-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

編碼方式
UTF-8

設備進階設定

ICMP 告警樣板
----- N/A -----

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

資料保留天數

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/voice/support@npartnertech.com)

業務相關請洽：

Email: sales@npartnertech.com