N-Partner

# 如何設定 Windows File 事件記錄

**V004**

2019/01/16

## 版權聲明



## 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
1. NXLog ..... 3
1.1 NXLog 架構 ..... 3
1.2 NXLog 安裝 ..... 4
1.3 NXLog 設定檔 ..... 6
1.3.1 Windows 2000 - 2003 ..... 6
1.3.2 Windows 2008 or higher ..... 8
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
6.1.1 組織單位設定 ..... 87
6.1.2 群組原則設定 ..... 91
6.2 工作群組 ..... 96
6.3 稽核資料夾設定 ..... 100
7. N-Reporter ..... 107
7.1 Windows 2000 - 2003 ..... 108
7.2 Windows 2008 or higher ..... 109

# 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。

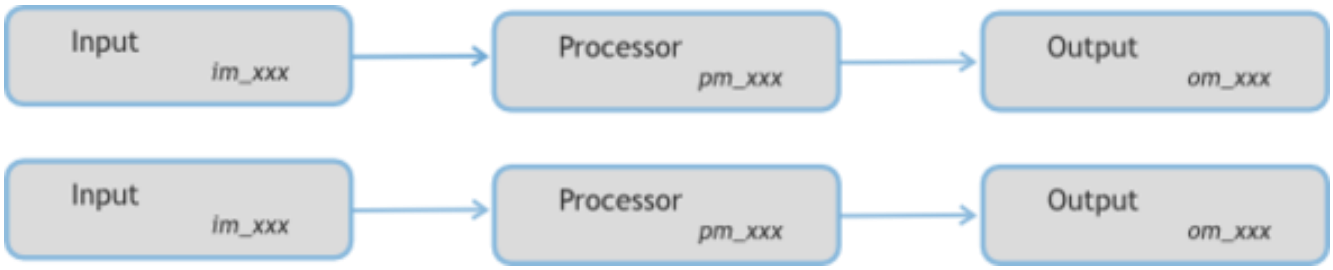
https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

# 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

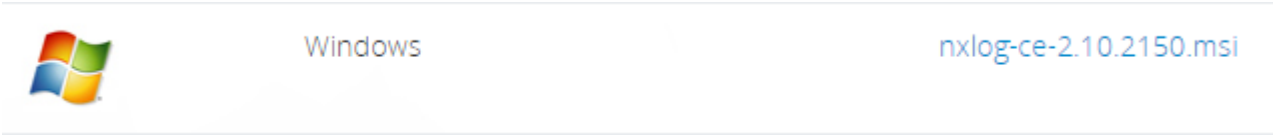


## 1.2 NXLog 安裝

(1) 下載 NXLog

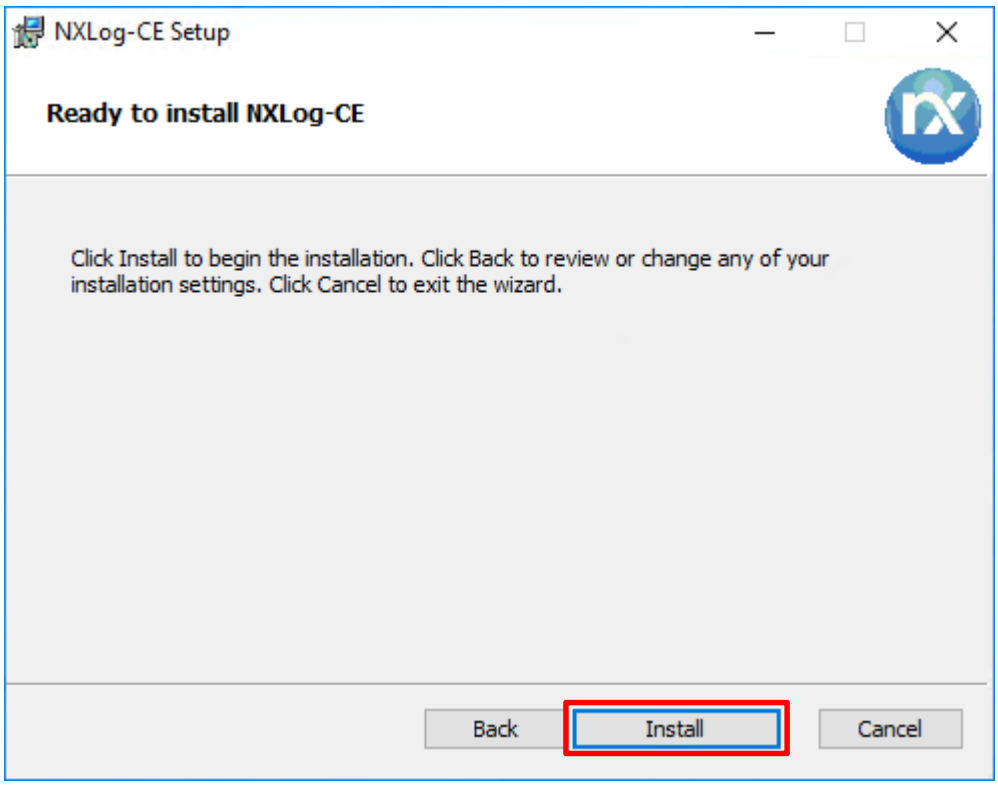
前往網址 https://nxlog.co/products/nxlog-community-edition/download

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]

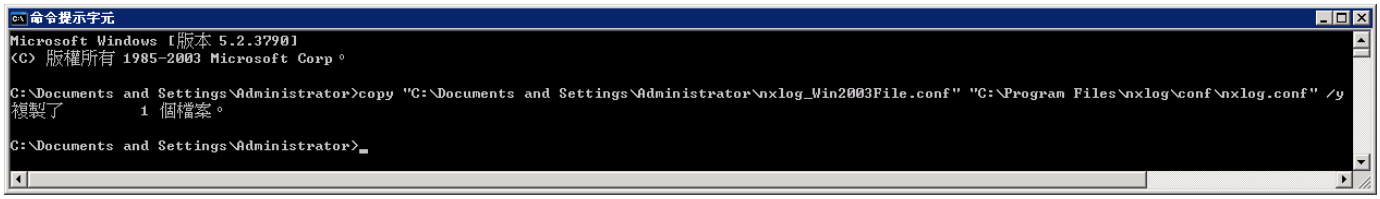


(3) 下載並覆蓋 NXLog 設定檔

(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

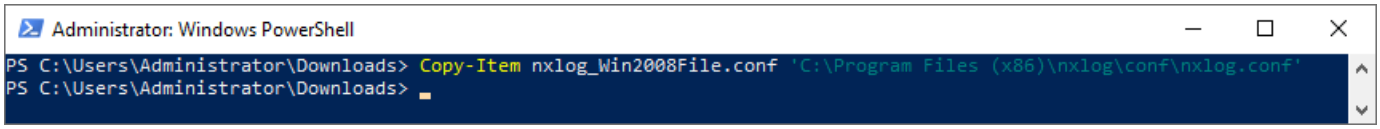
copy "C:\Documents and Settings\Administrator\nxlog_Win2003File.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y 覆蓋 NXLog 設定檔




(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



## 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 ust 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

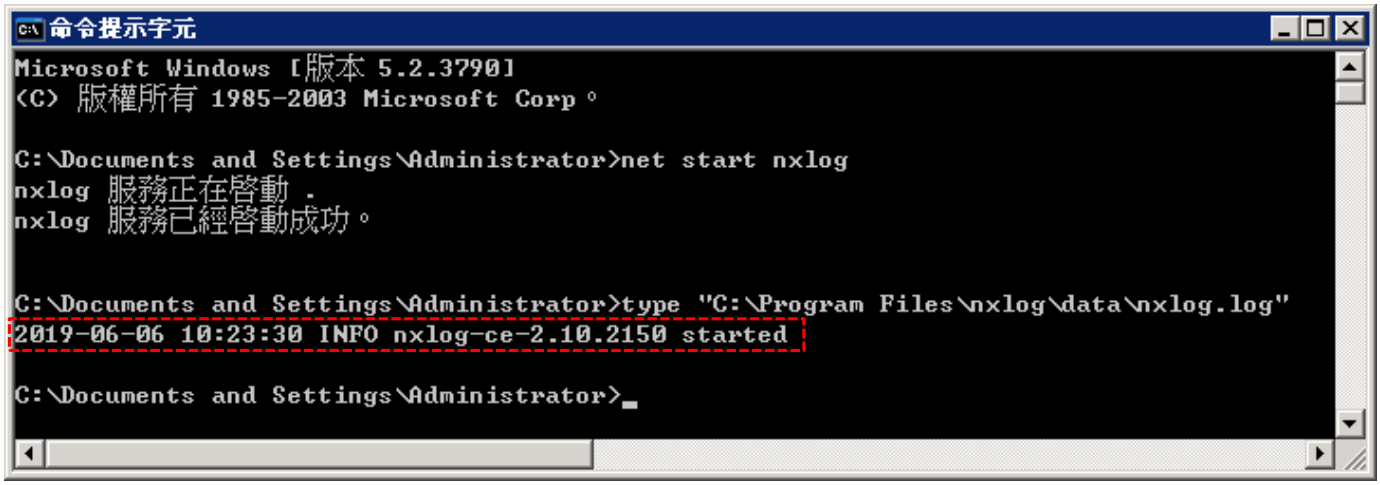
```
define NCloud      192.168.3.51
```

## 1.4 NXLog 啟動服務

### 1.4.1 Windows 2000 - 2003

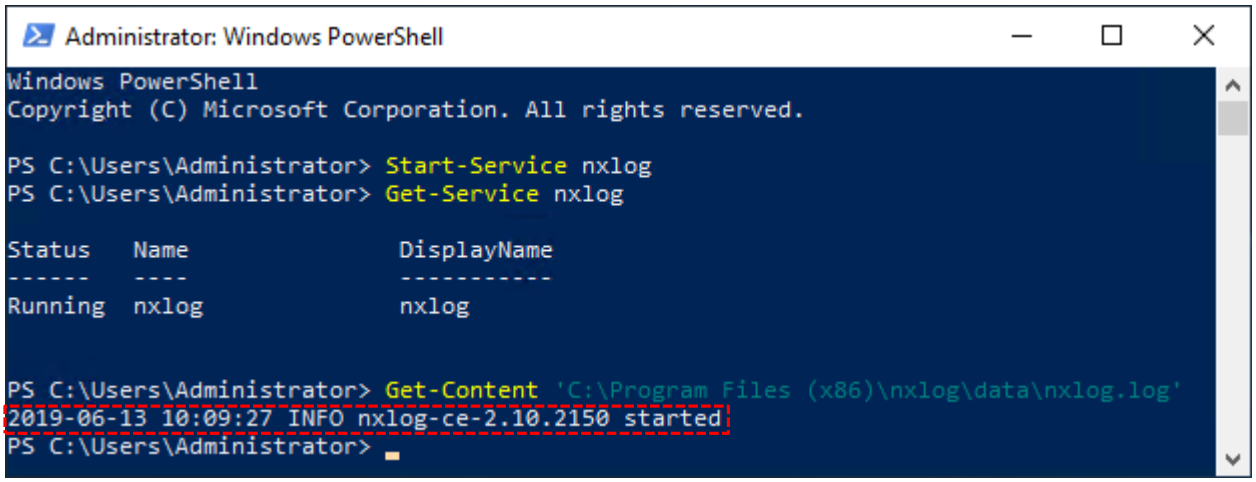
開啟 [命令提示字元] -> 輸入 net start nxlog 啟動 nxlog 服務-> 輸入 type "C:\Program Files\nxlog\data\nxlog.log"

確認沒有錯誤訊息



### 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



# 2. Windows 2003

以下分別為網域和工作群組設定方式。

## 2.1 網域

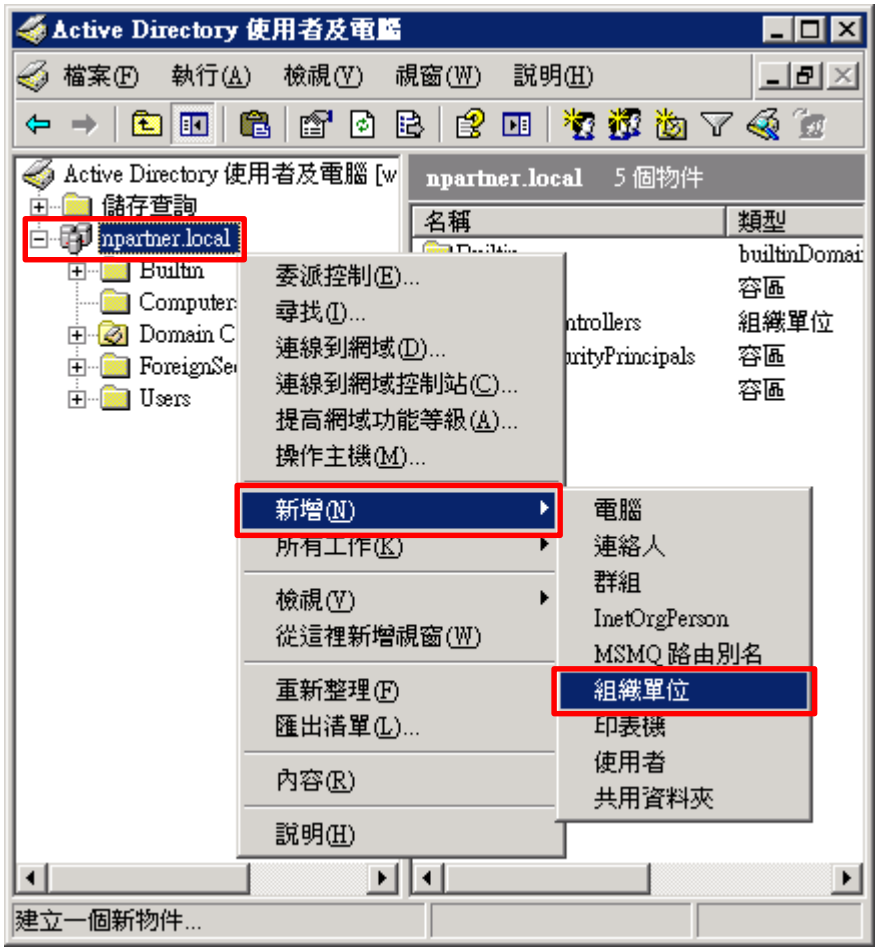
### 2.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

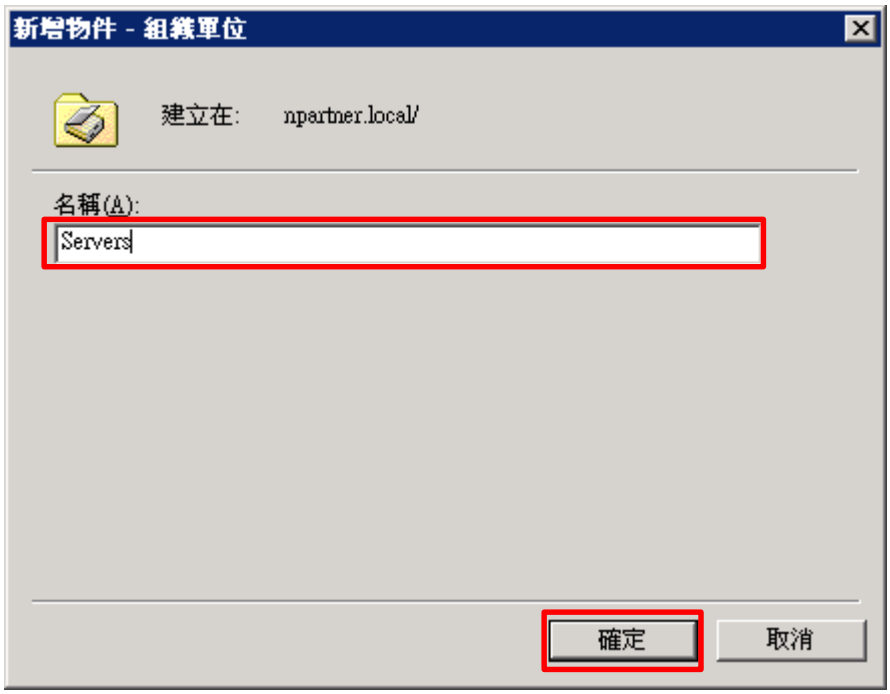

(2) 新增組織單位

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



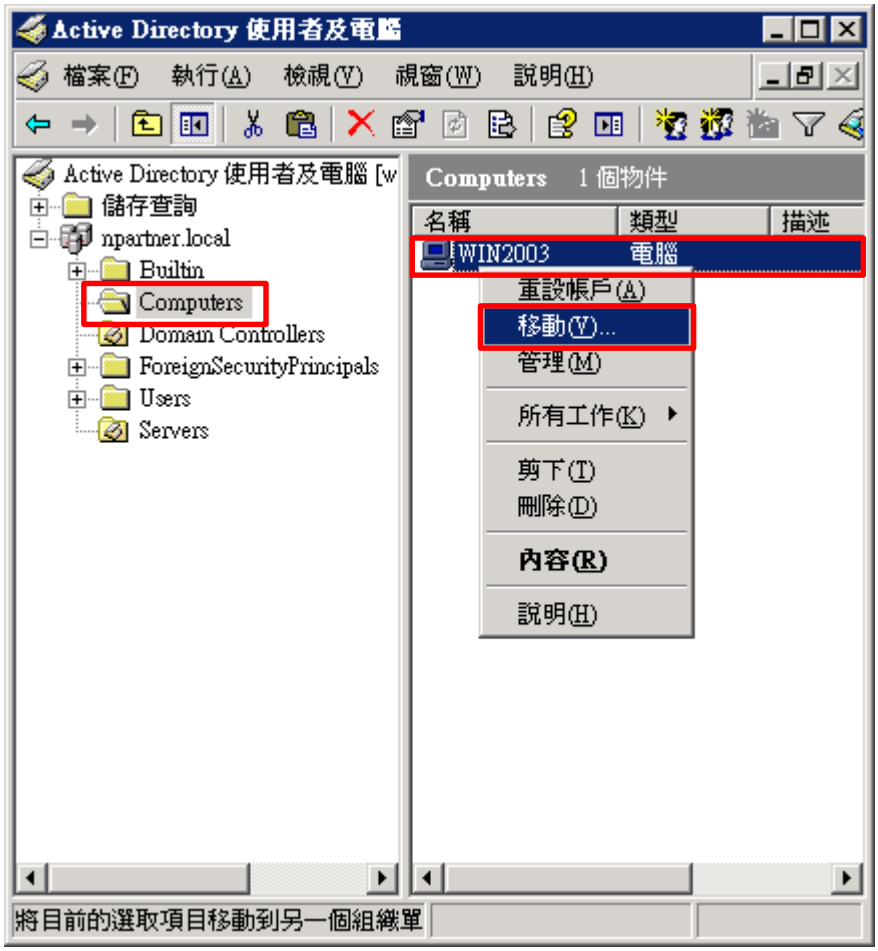
(3) 輸入組織單位名稱

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]

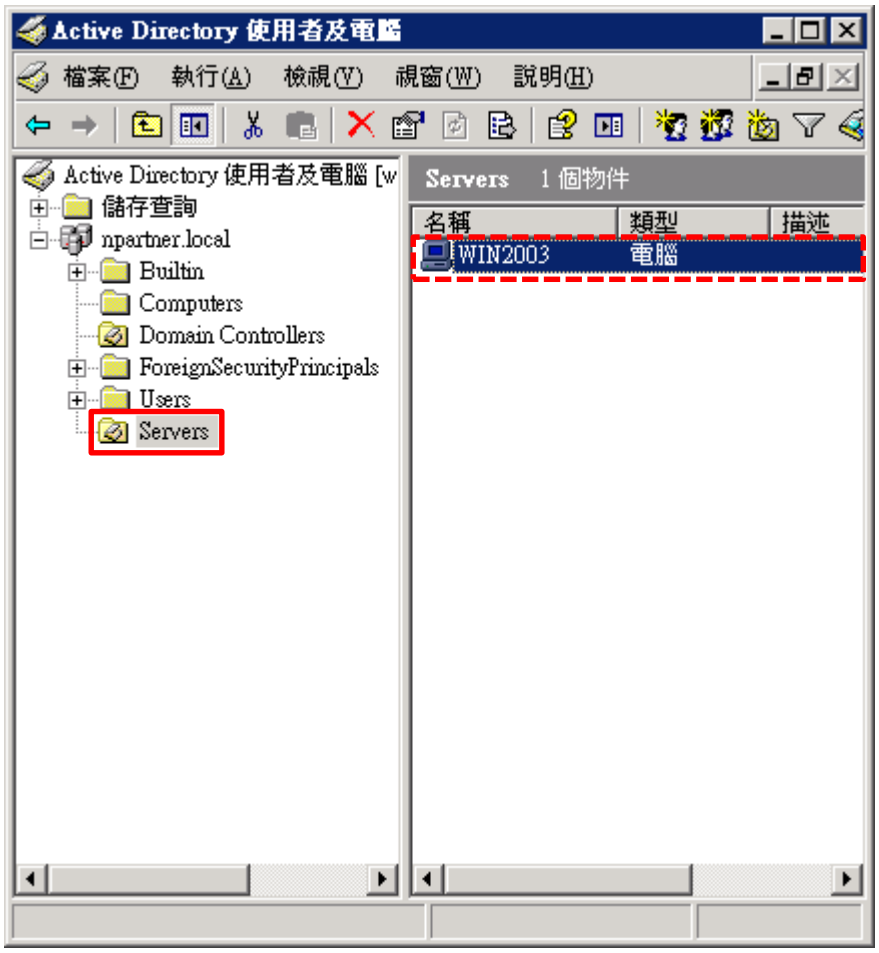


(5) 選擇組織單位

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



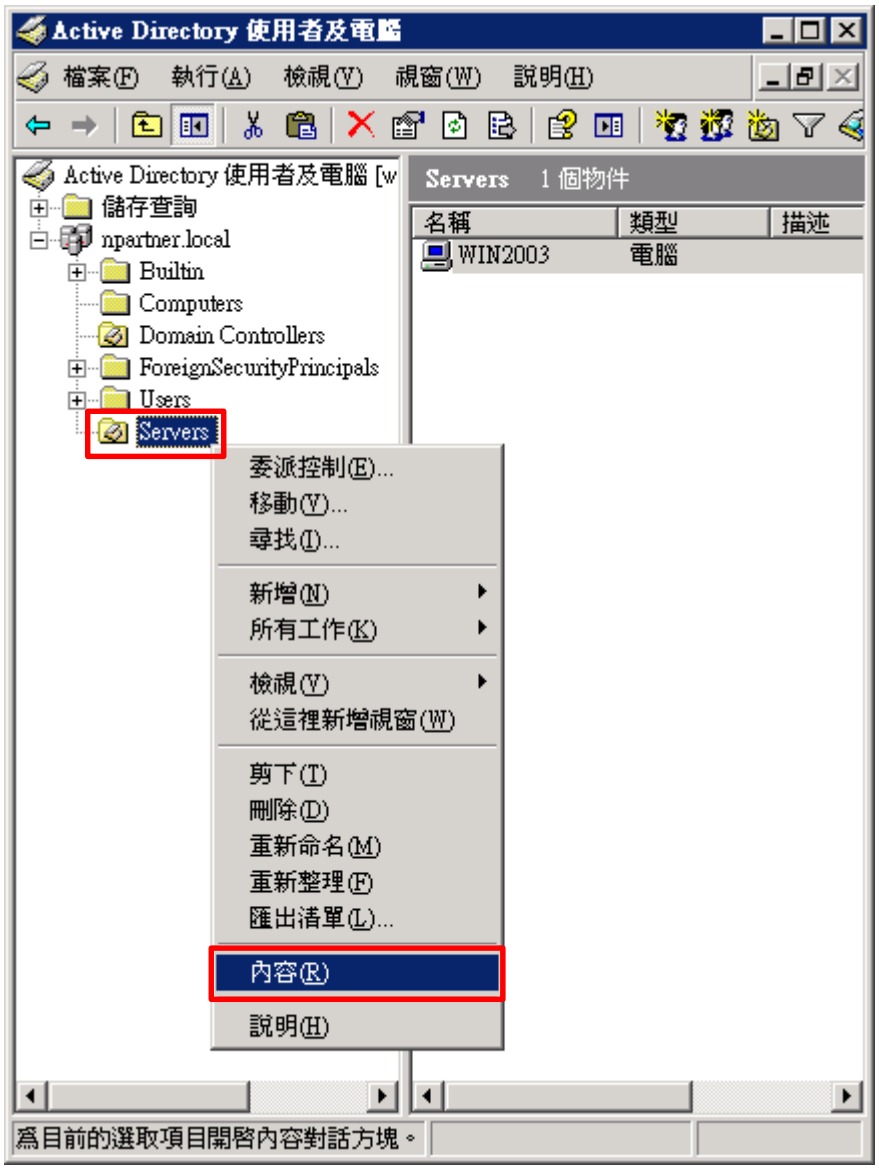
### 2.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

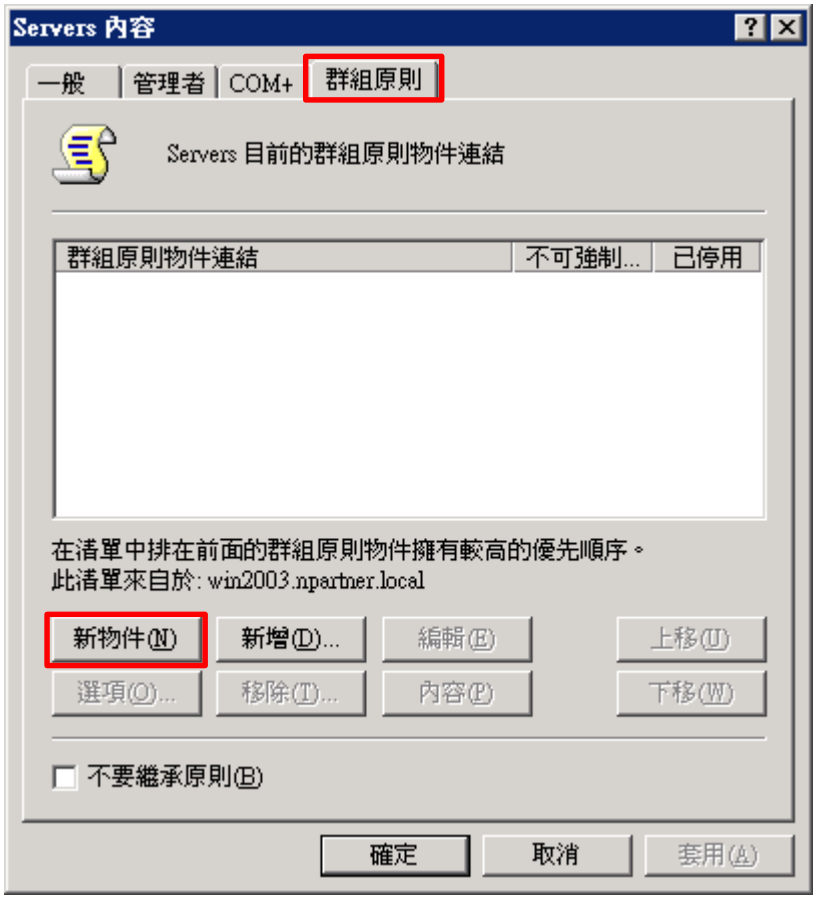

(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]



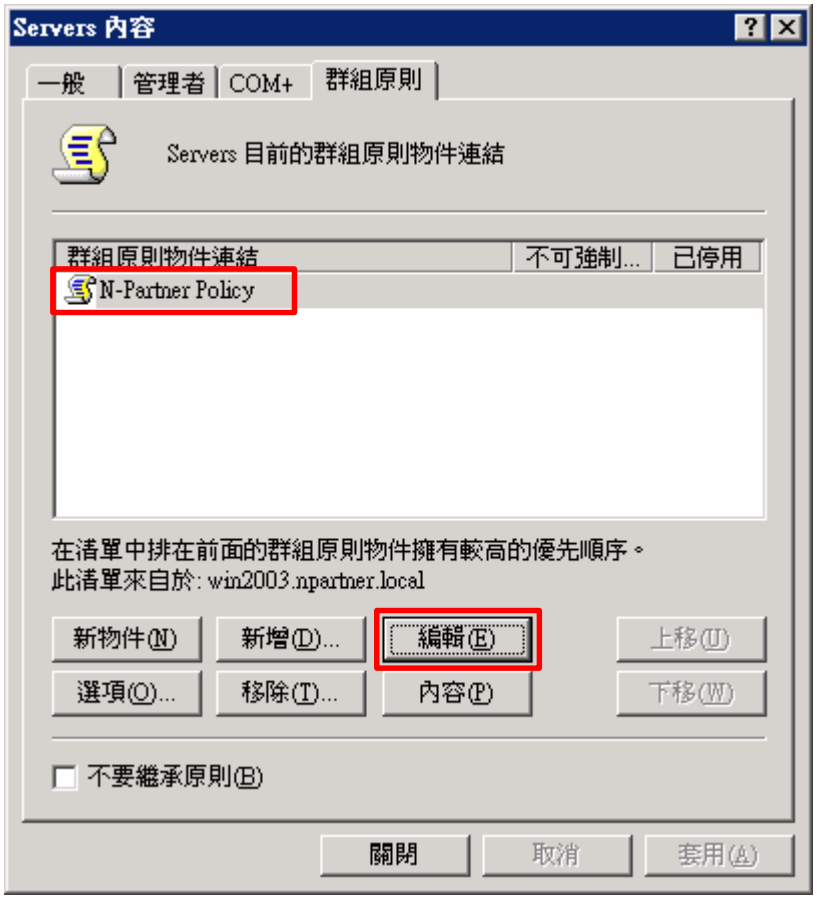
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按下 [新物件]



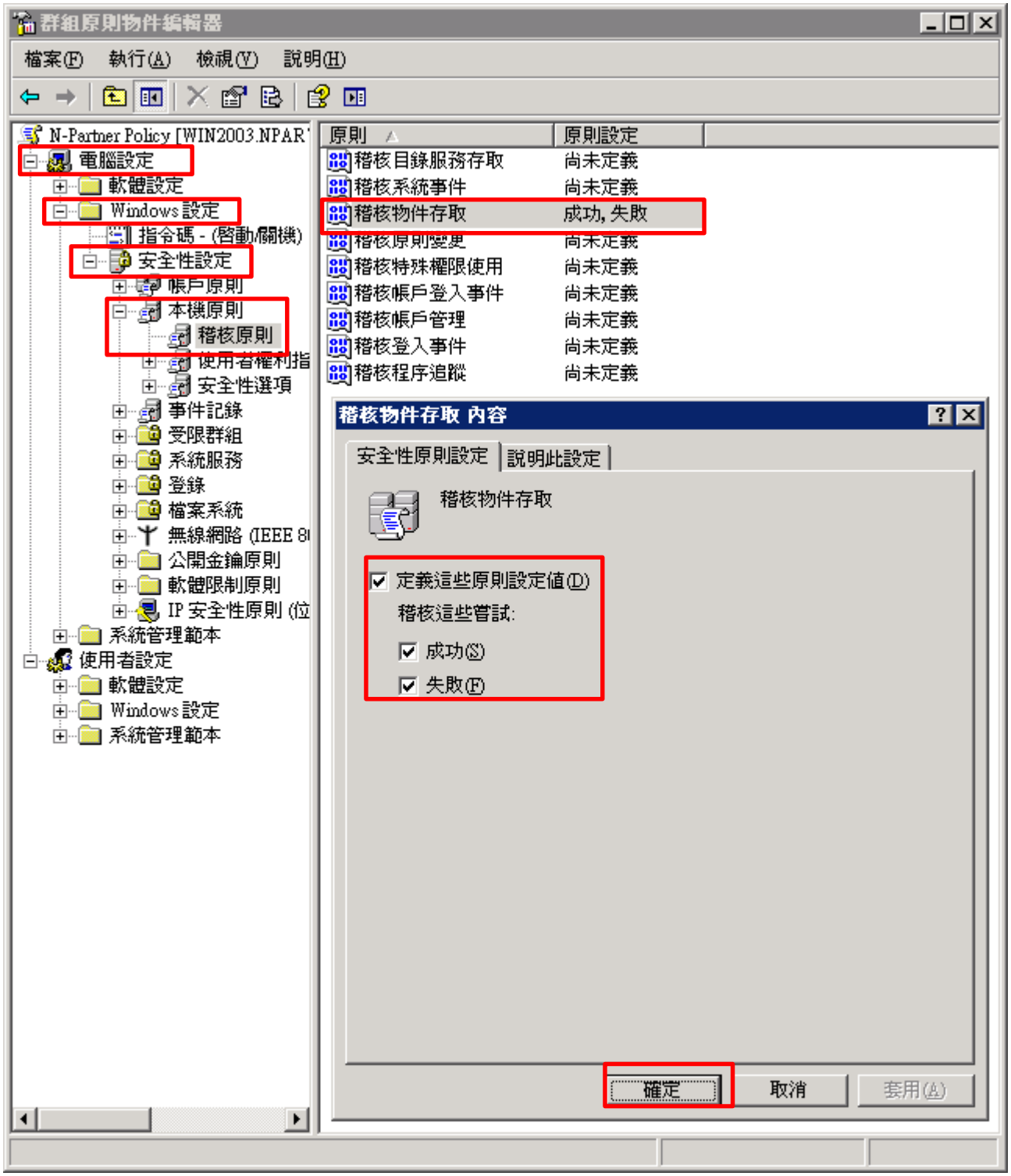
(4) 編輯群組原則物件

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]

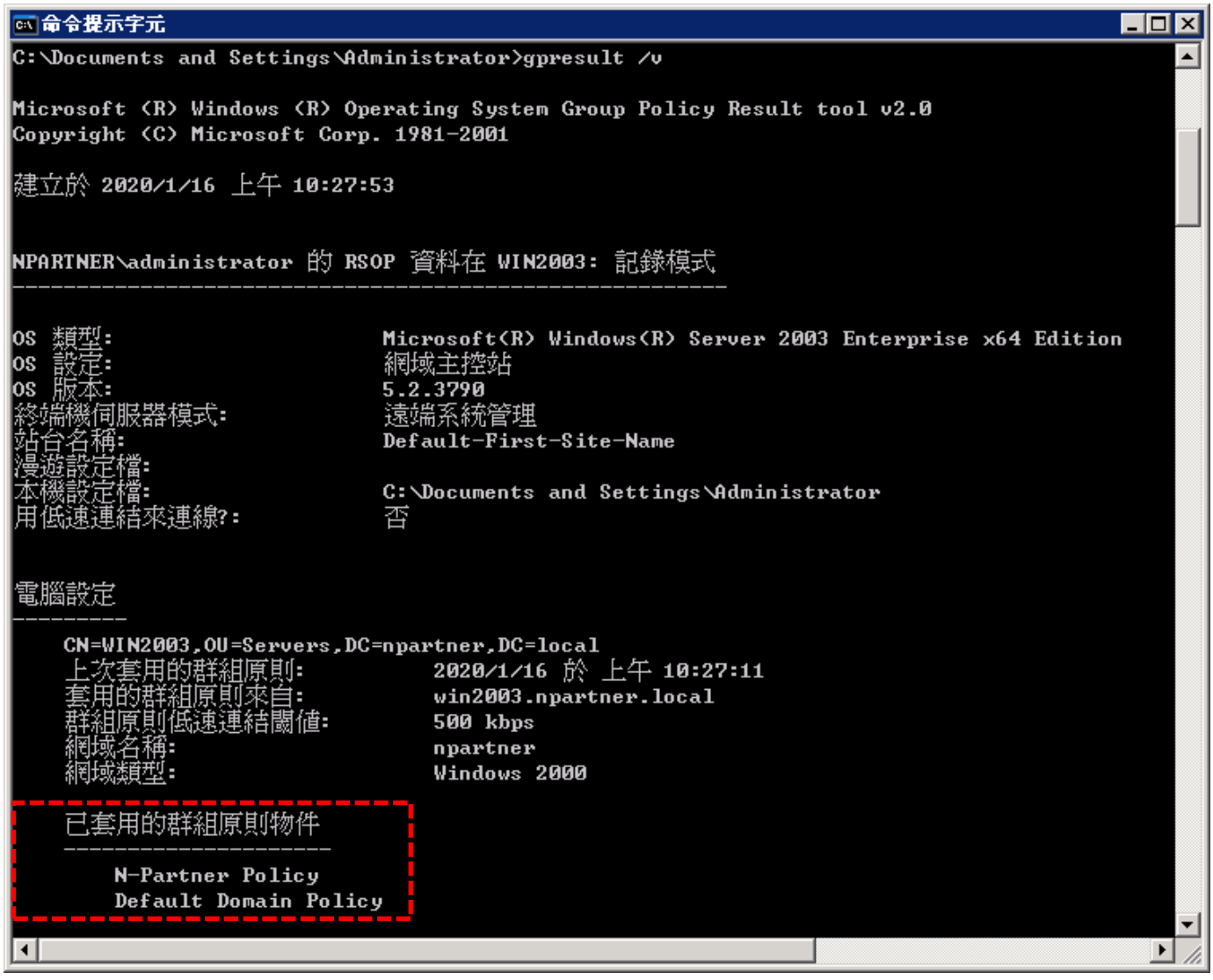


(6) 在 Windows File 伺服器更新群組原則

C:\> gpupdate /force


(7) 查看群組原則套用情形

C:\> gpresult /v



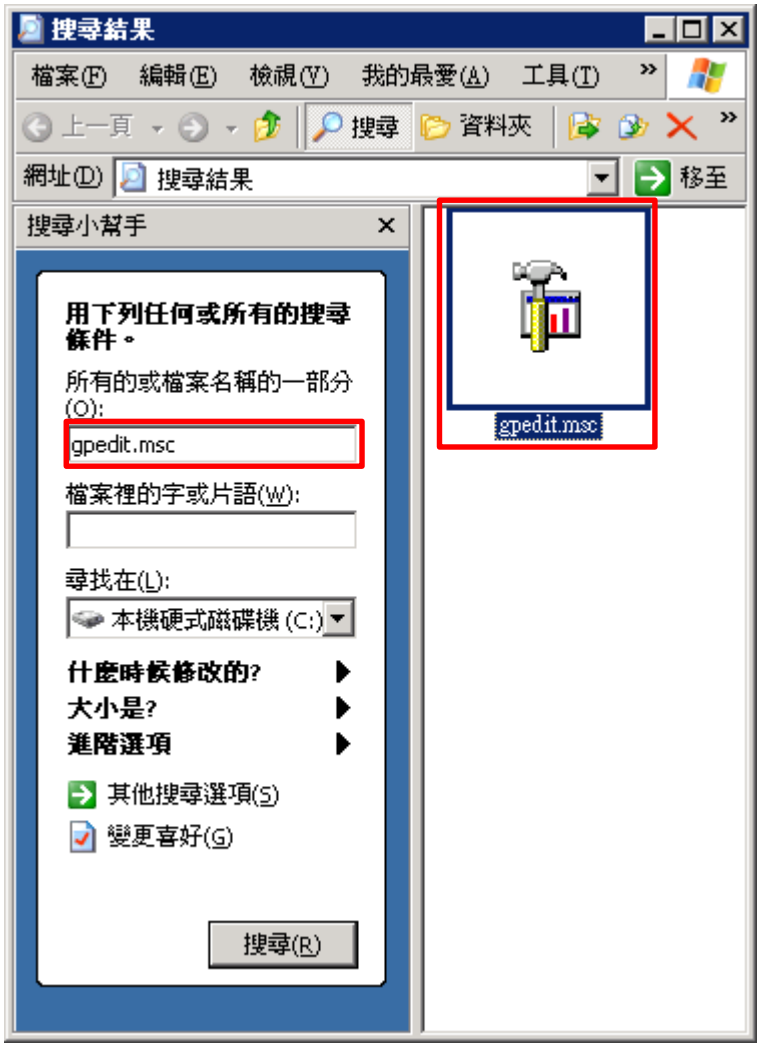
## 2.2 工作群組

(1) 開啟搜尋

點選 [開始] -> 點選 [搜尋]

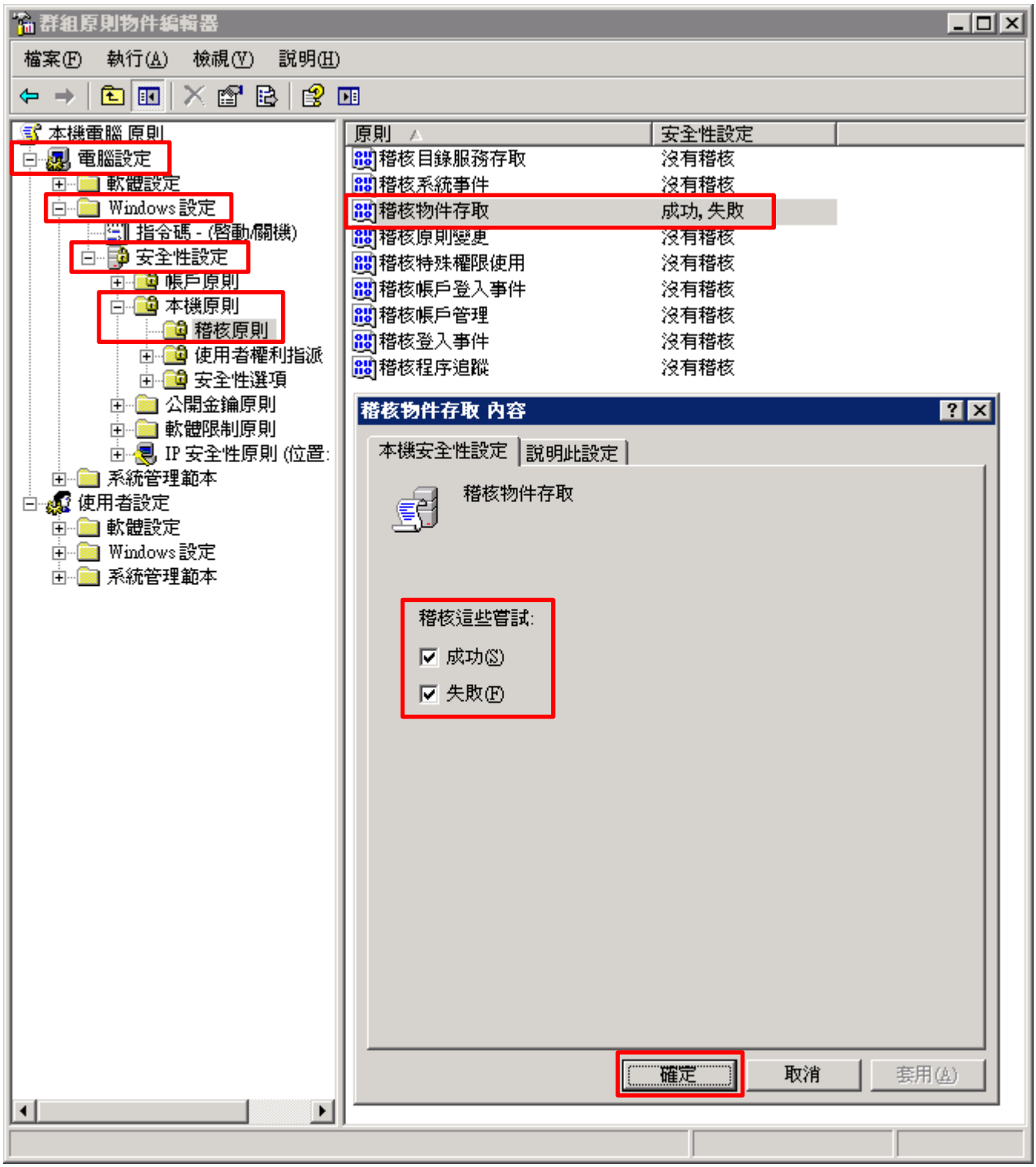
(2) 搜尋群組原則物件編輯器

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]

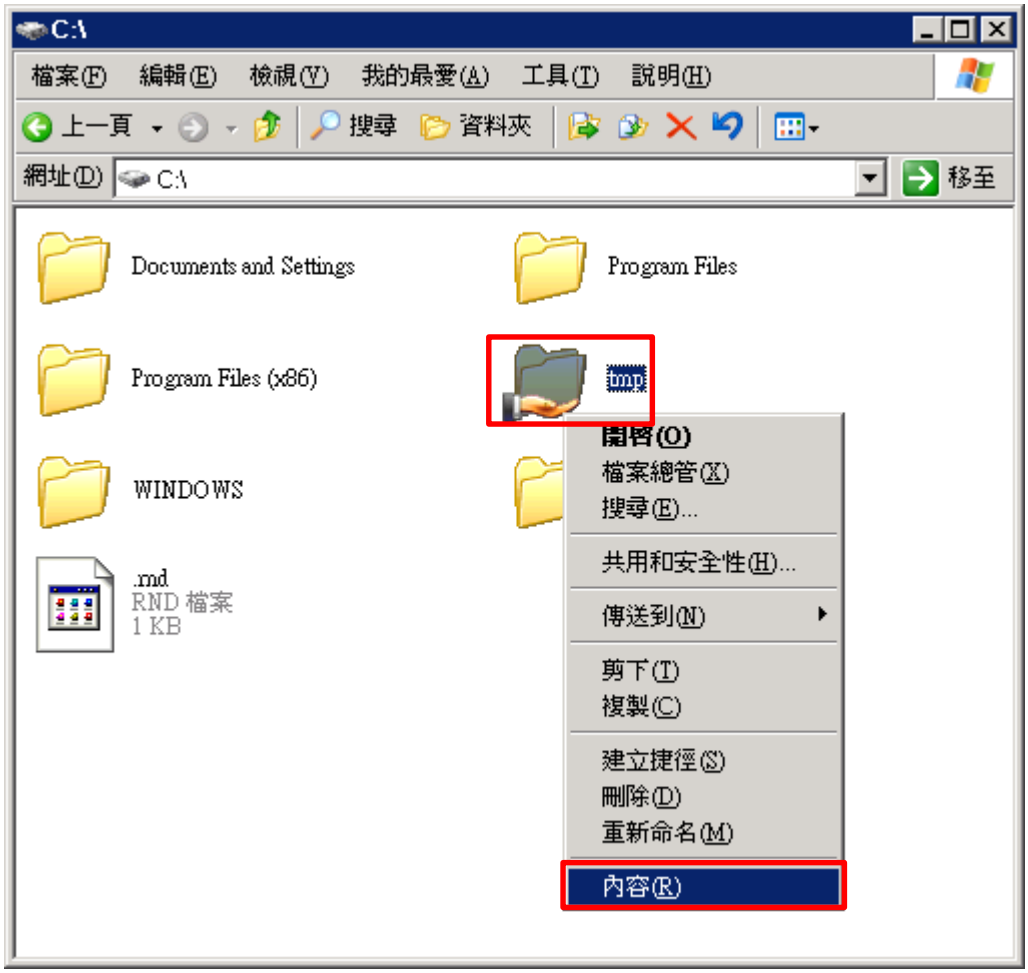


(4) 更新群組原則

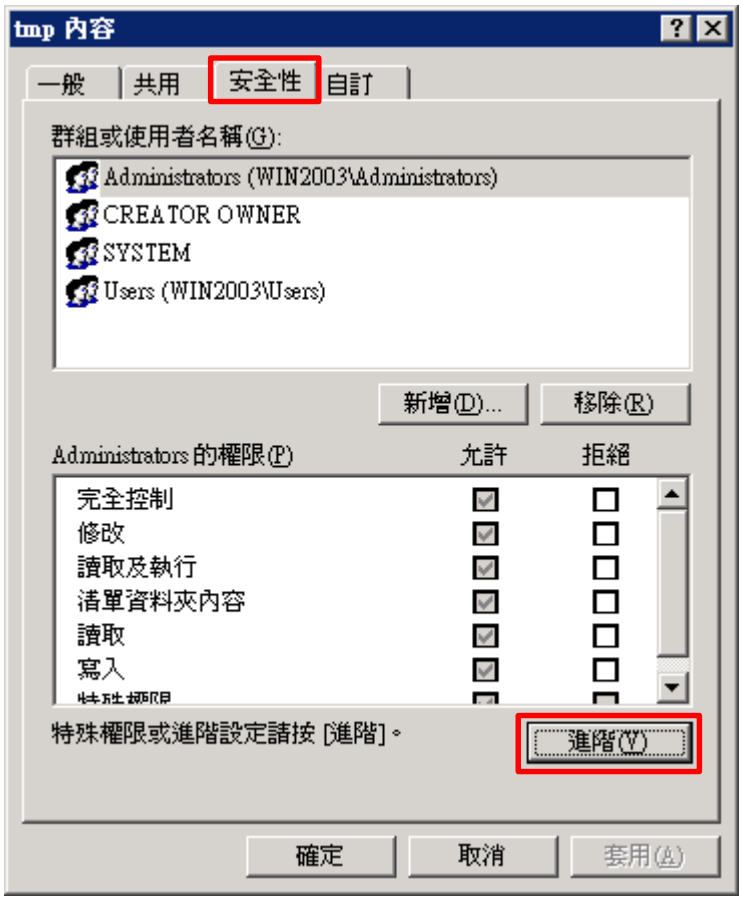
C: \> gpupdate /force

## 2.3 稽核資料夾設定

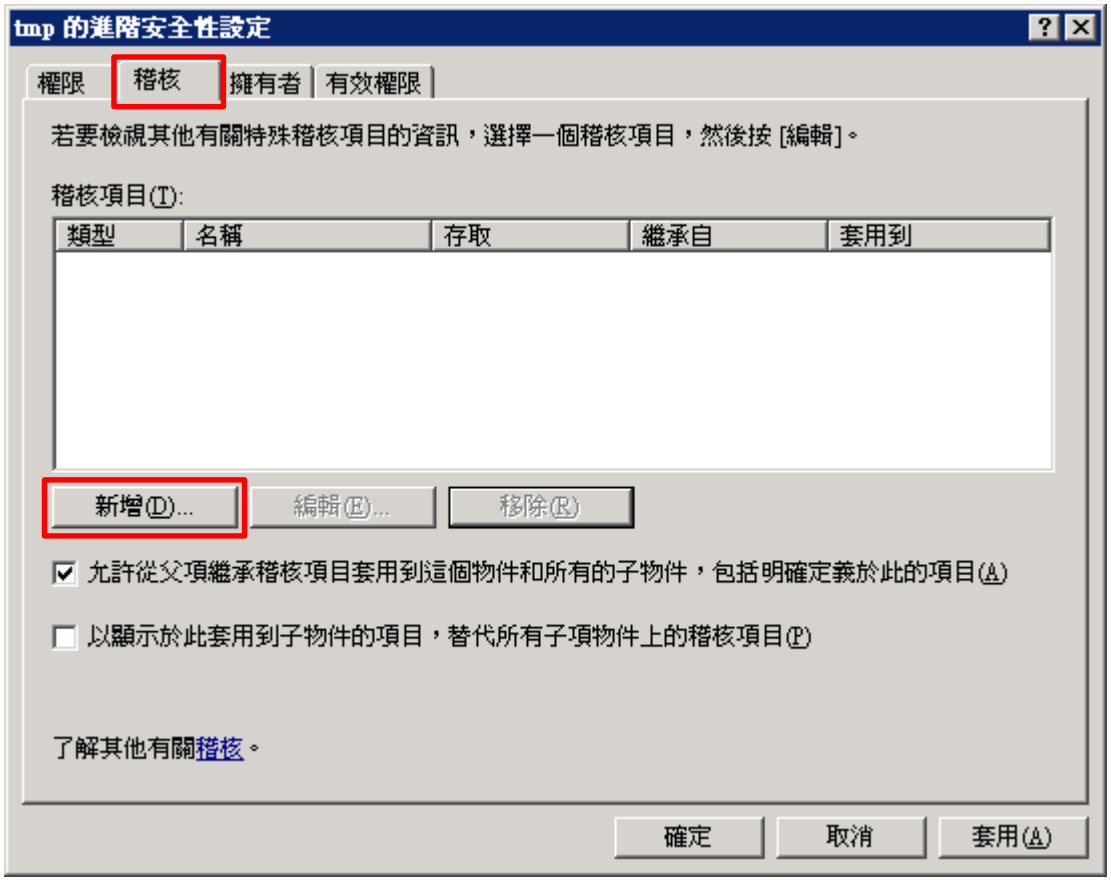
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



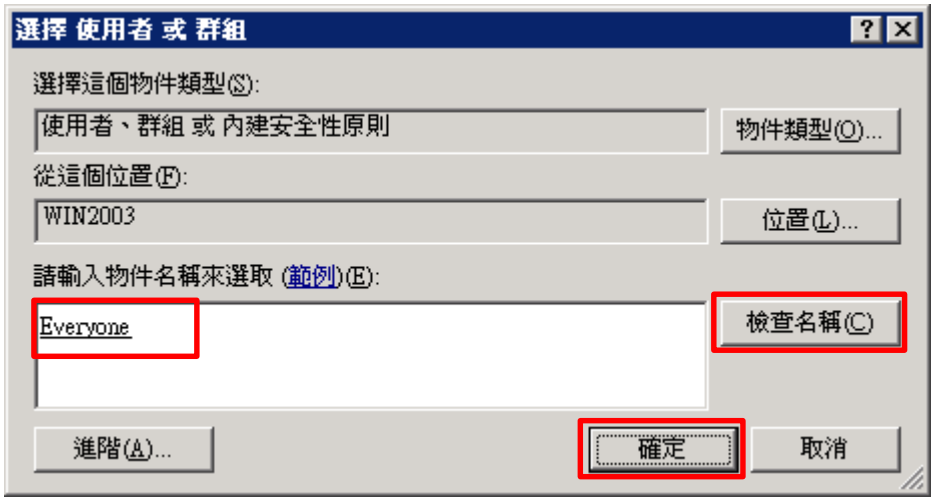
(2) 點選 [安全性] 頁面 -> 按下 [進階]



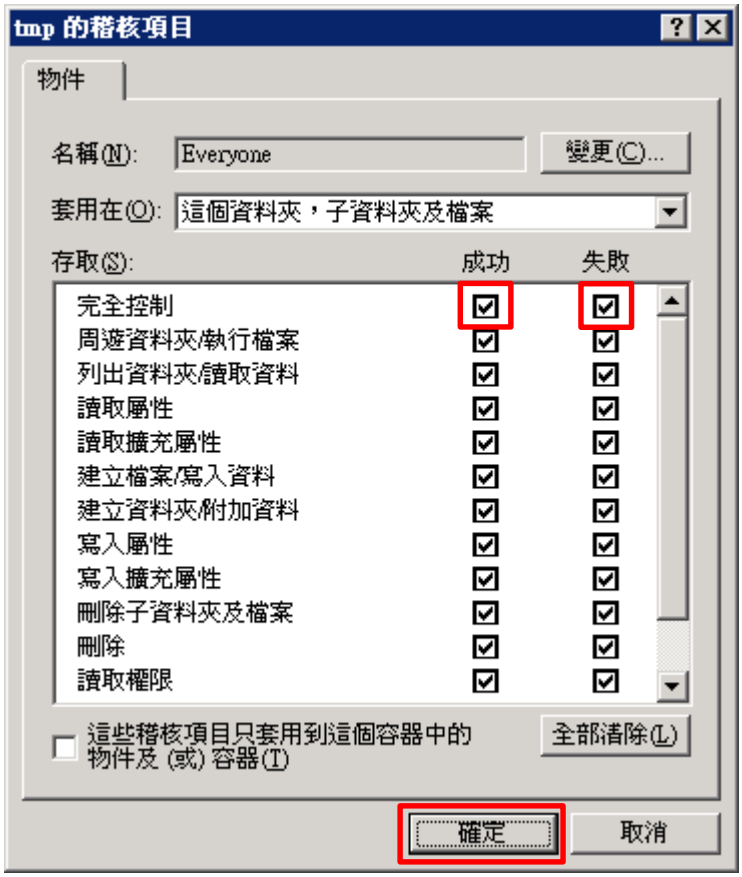

(3) 點選 [稽核] 頁面 -> 按下 [新增]



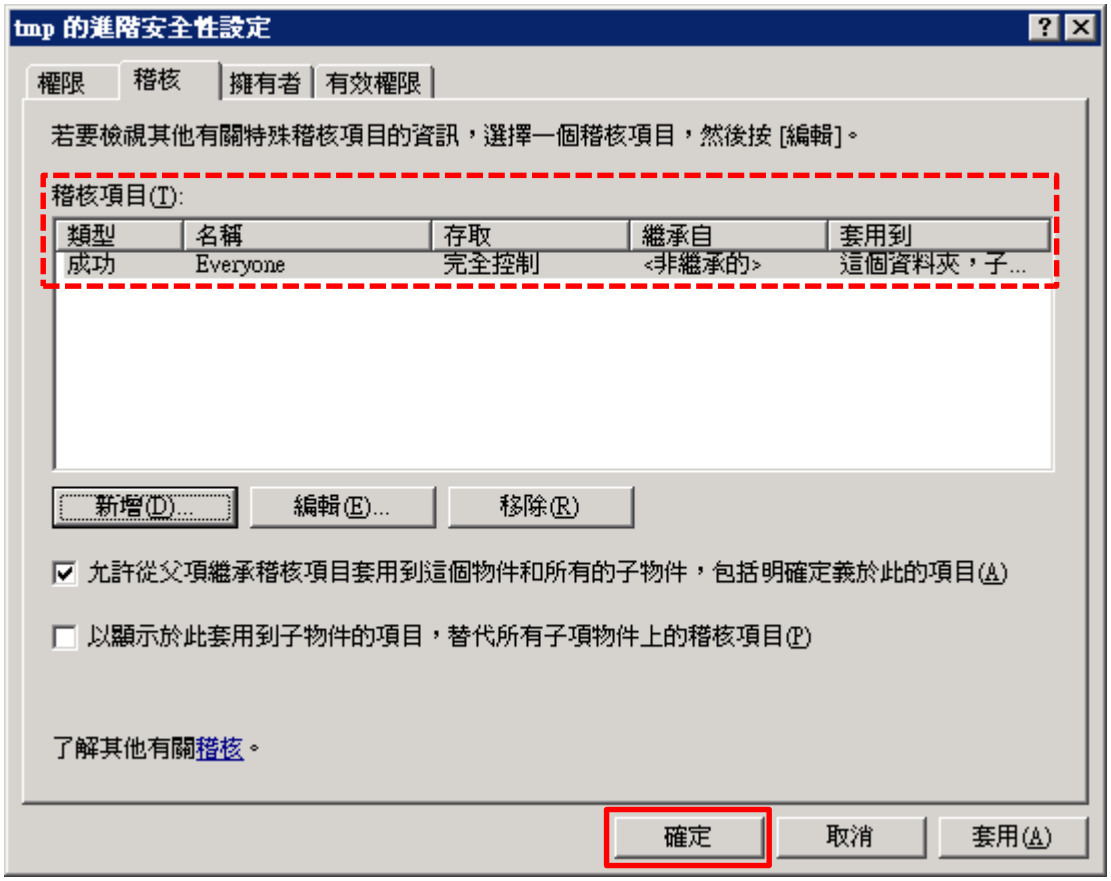
(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]




(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

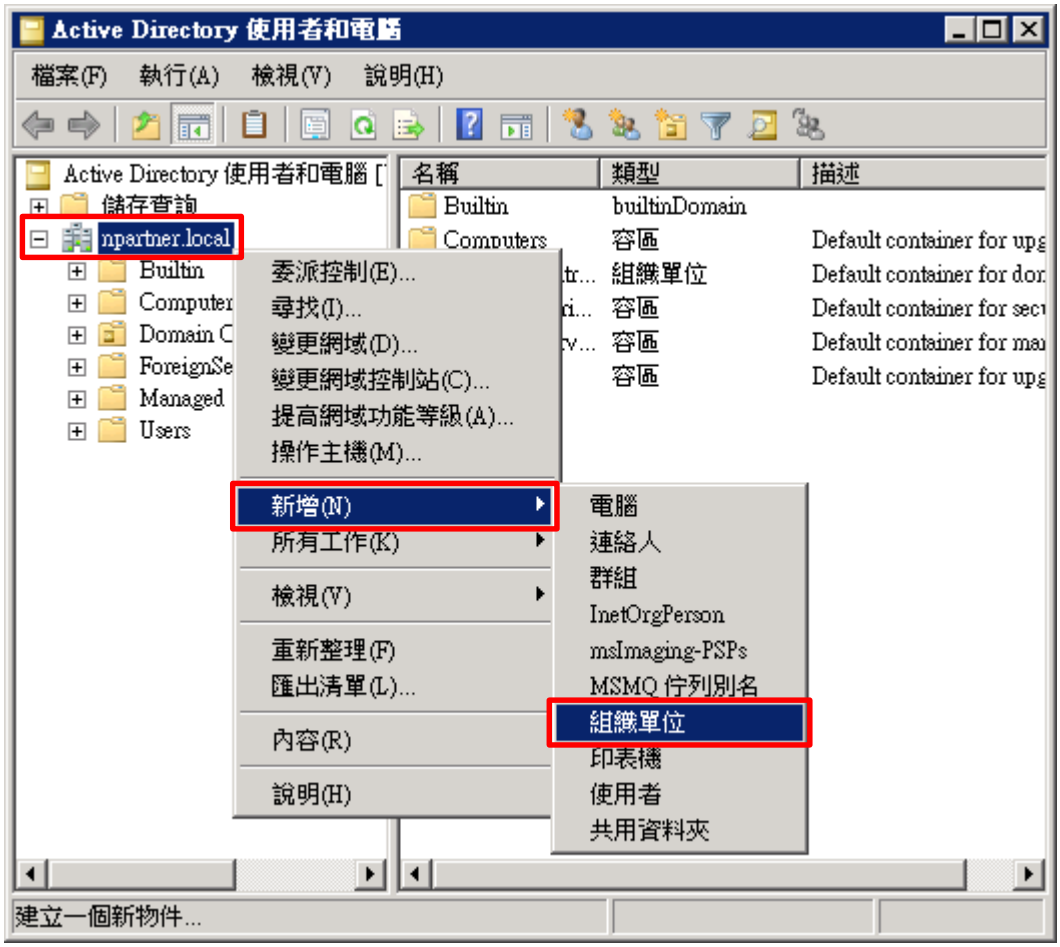
### 3.1.1 組織單位設定

(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]

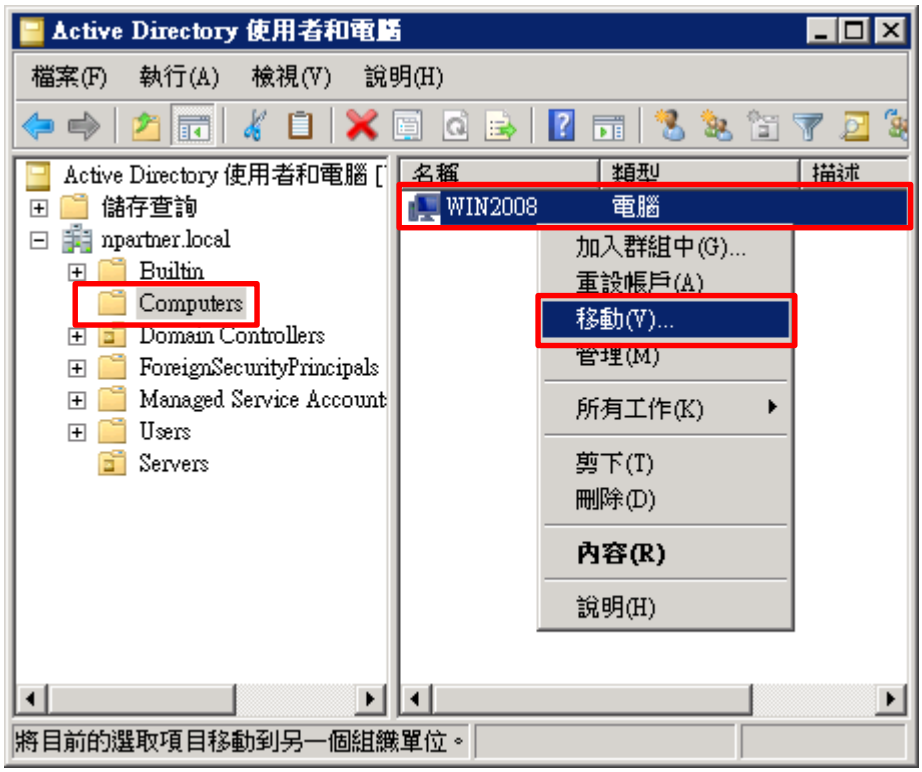


(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]

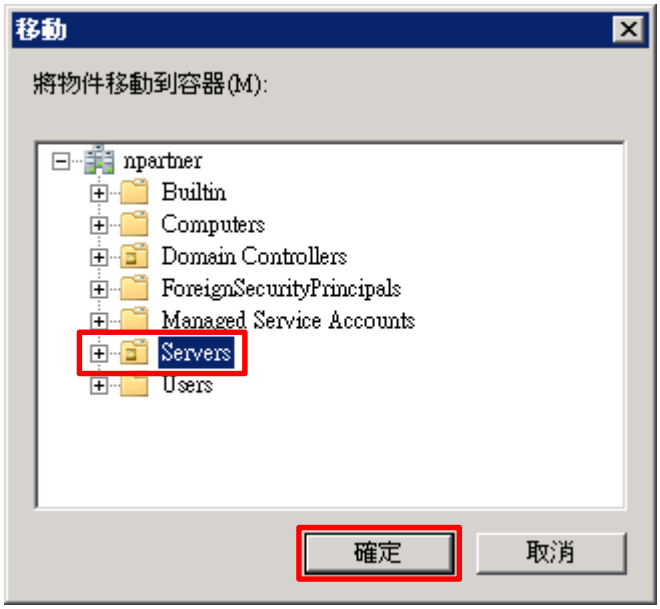

(4) 移動伺服器至新的組織單位

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



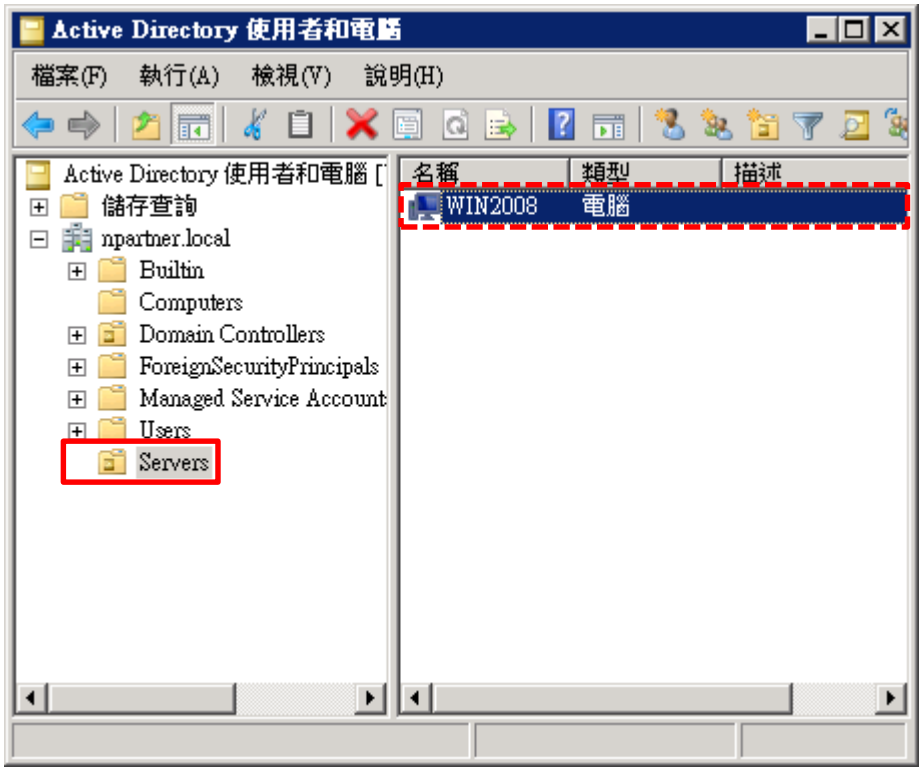
(5) 選擇組織單位

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



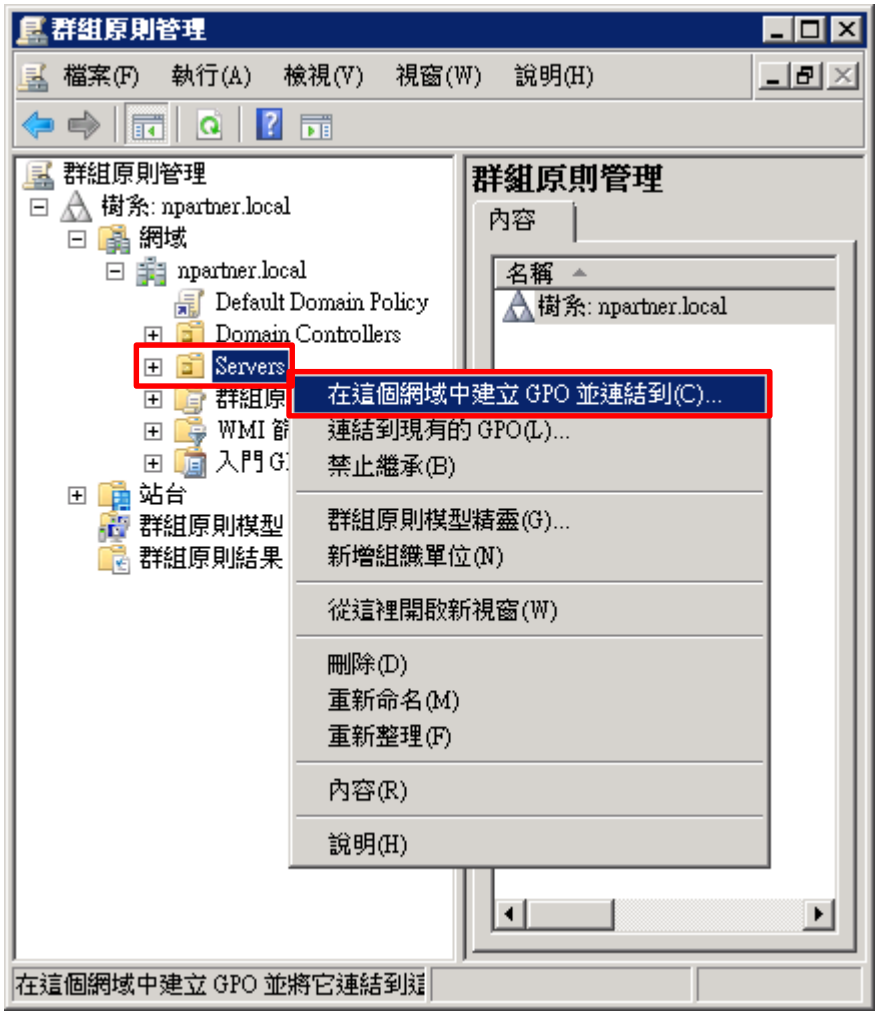
### 3.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

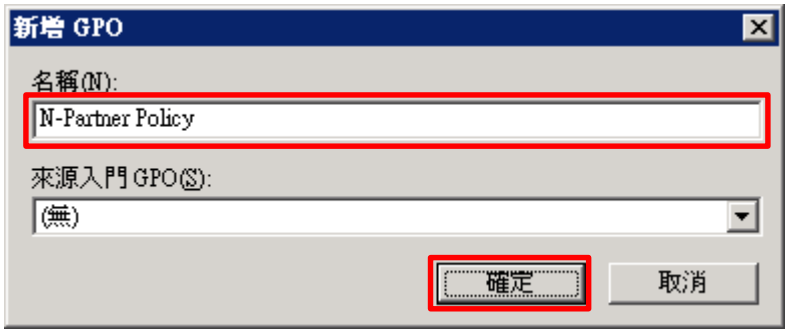

(2) 在 Servers 組織單位，新增群組原則物件

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…]



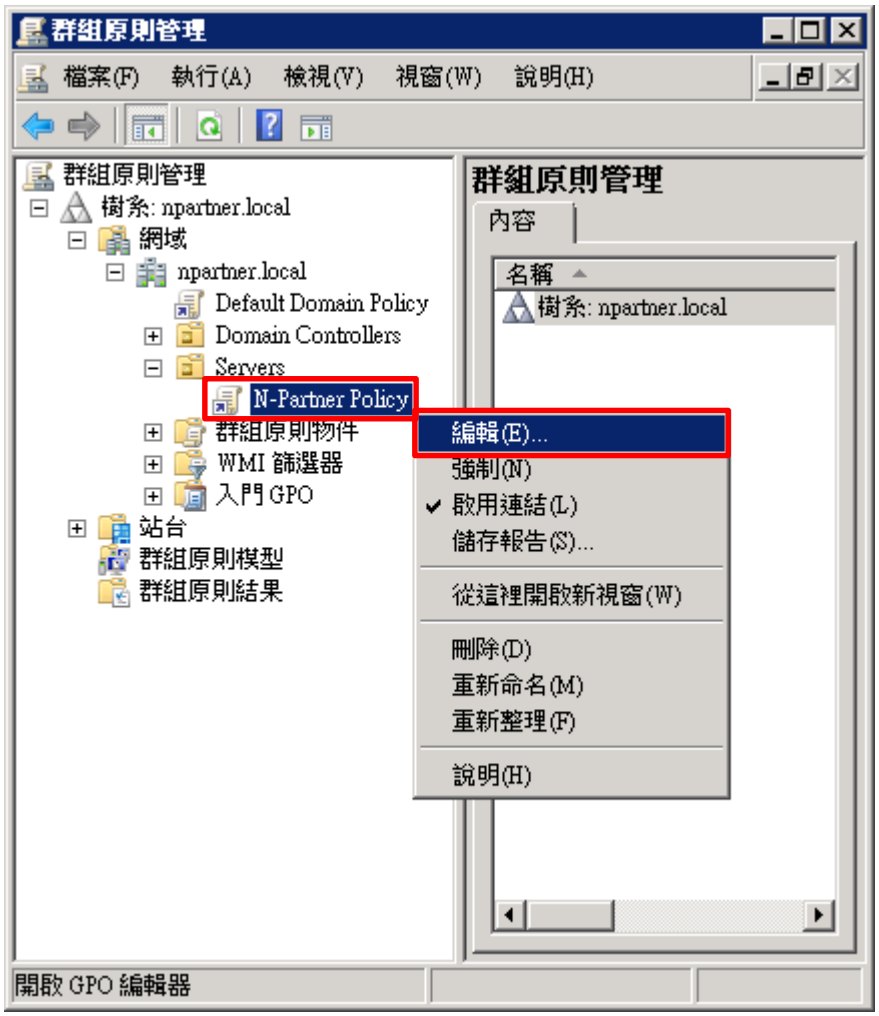
(3) 輸入群組原則物件名稱

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



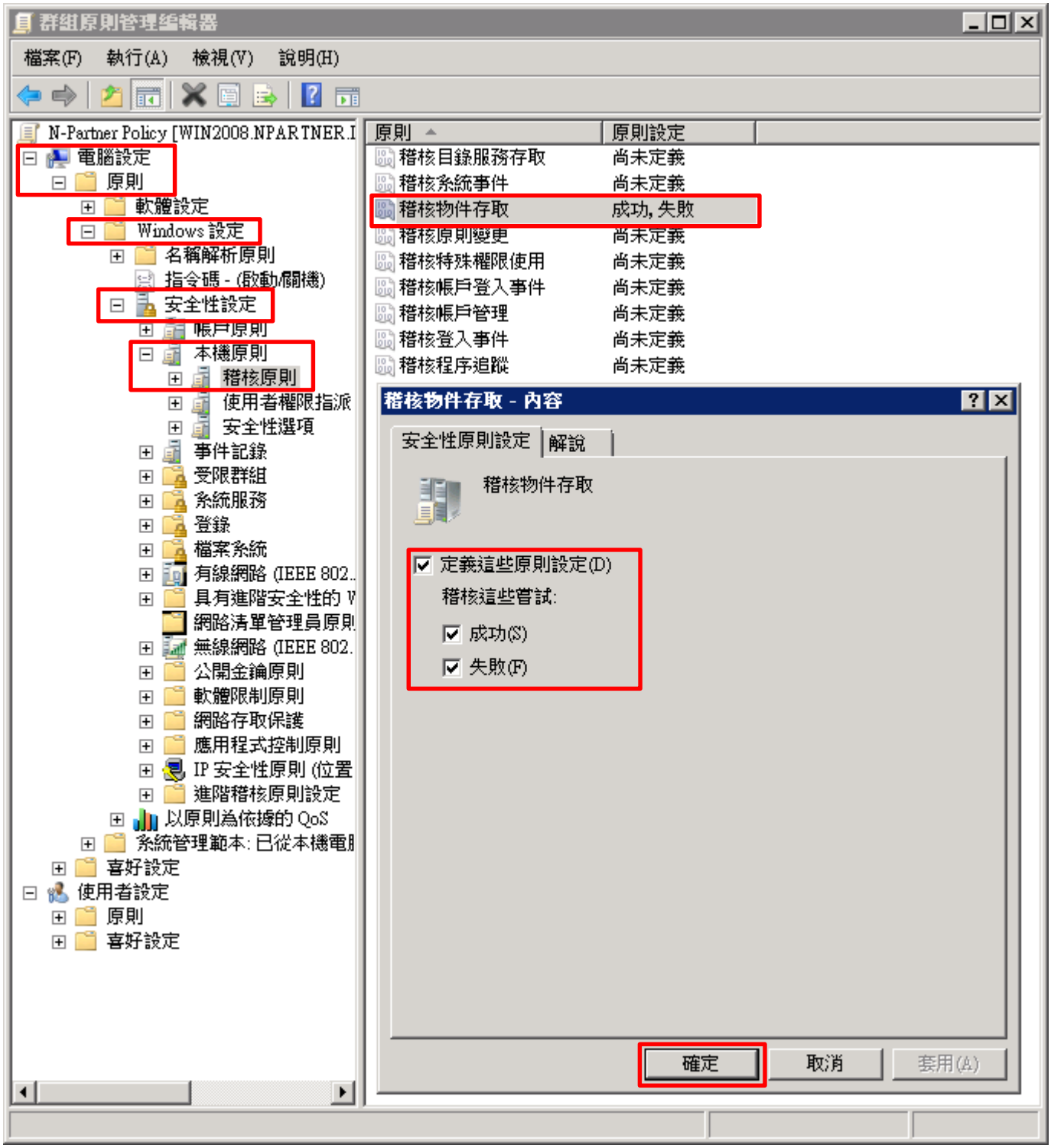

(4) 編輯群組原則物件

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]

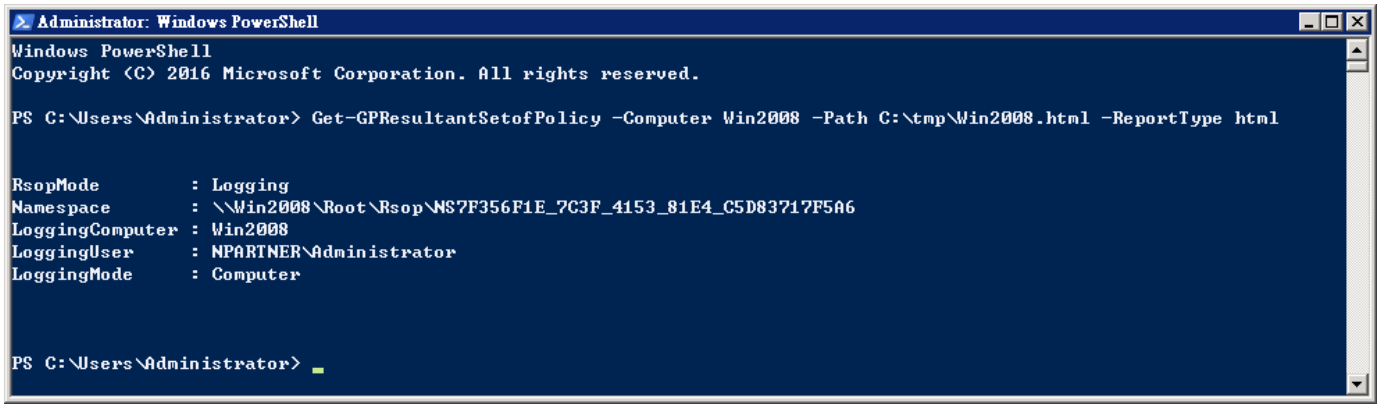


(6) 在 Windows File 伺服器，開啟 [Windows PowerShell]，更新群組原則

PS C:\> gpupdate /force


(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

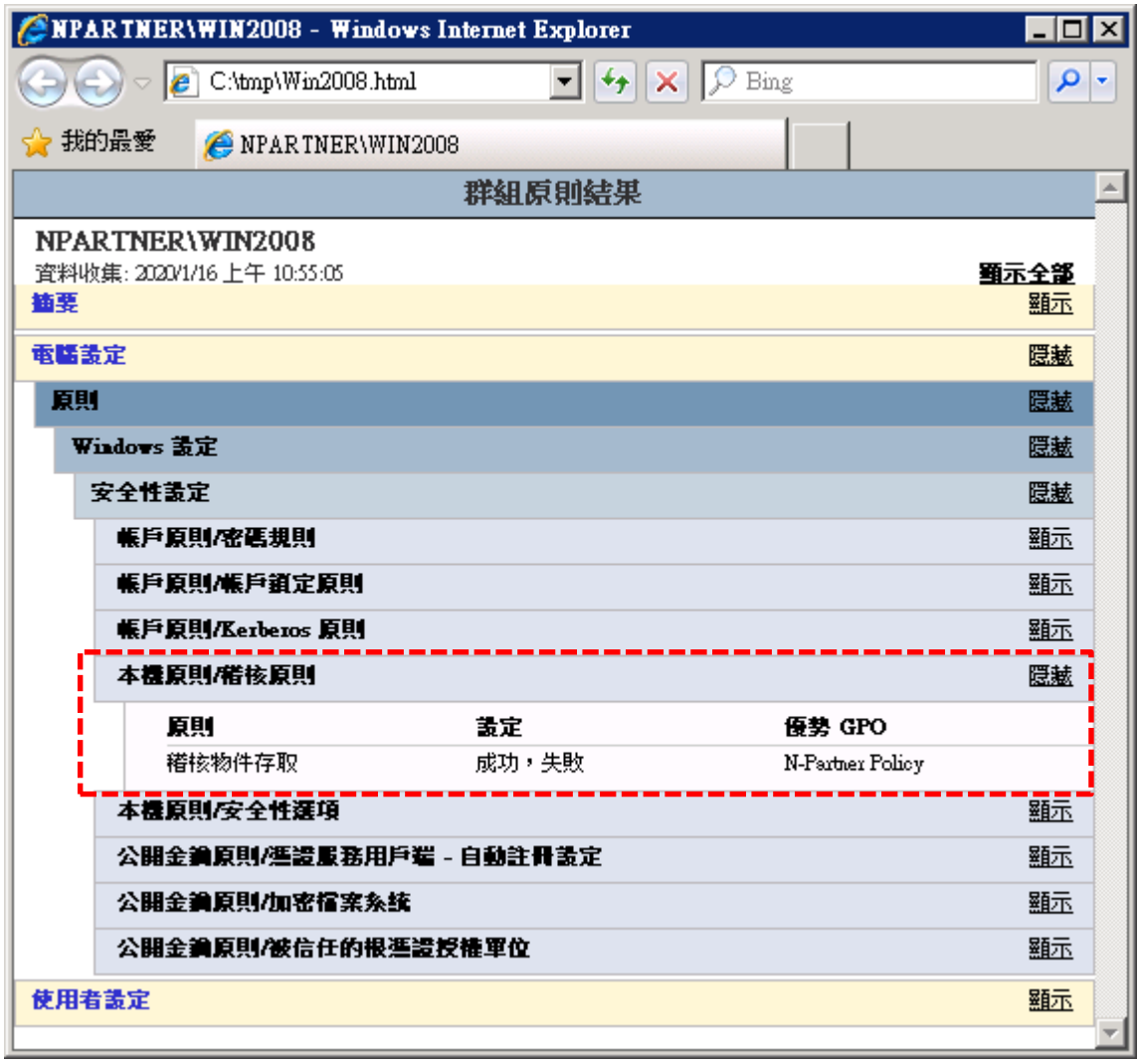
PS C:\> Get-GPResultantSetofPolicy -Computer Win2008 -Path C:\tmp\Win2008.html -ReportType html




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

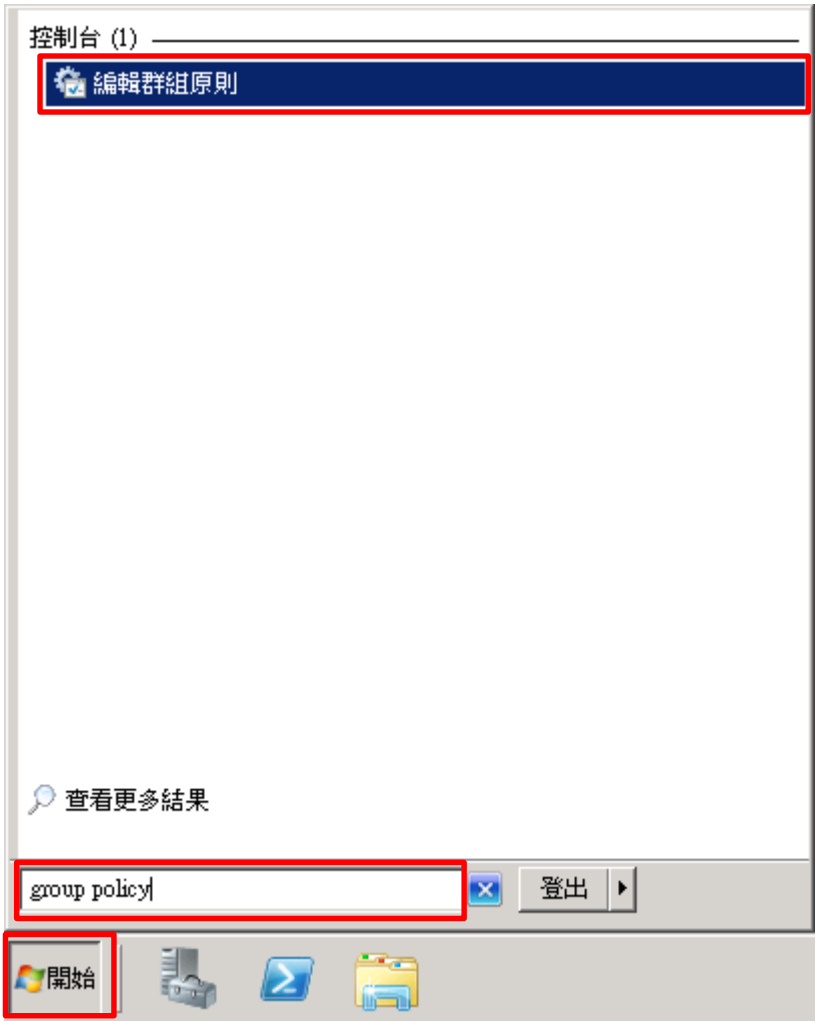
(9) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則



## 3.2 工作群組

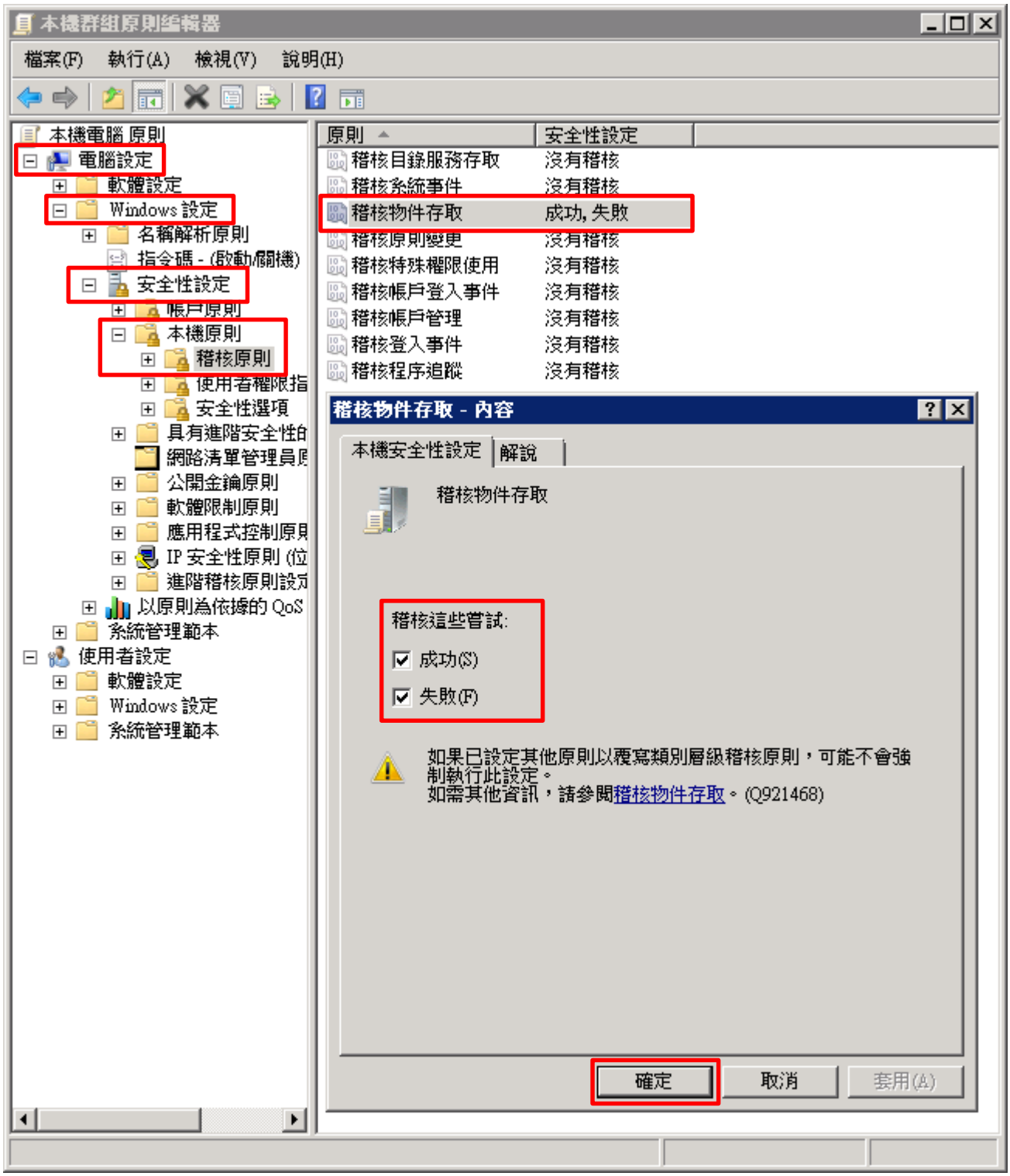
(1) 開啟 [本機群組原則編輯器]

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]



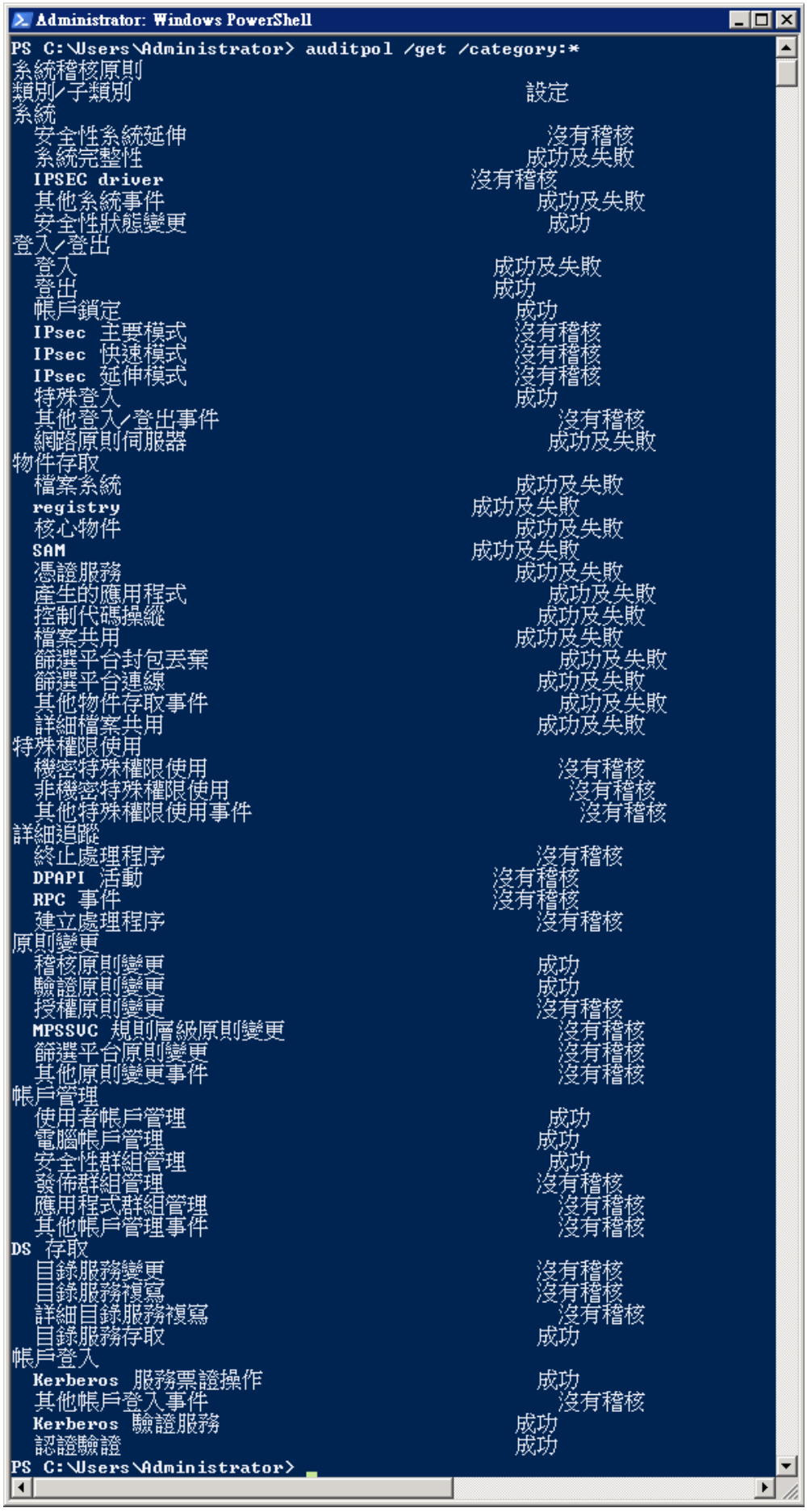
(3) 開啟 [Windows PowerShell]，


(4) 更新群組原則

PS C: \> gpupdate /force

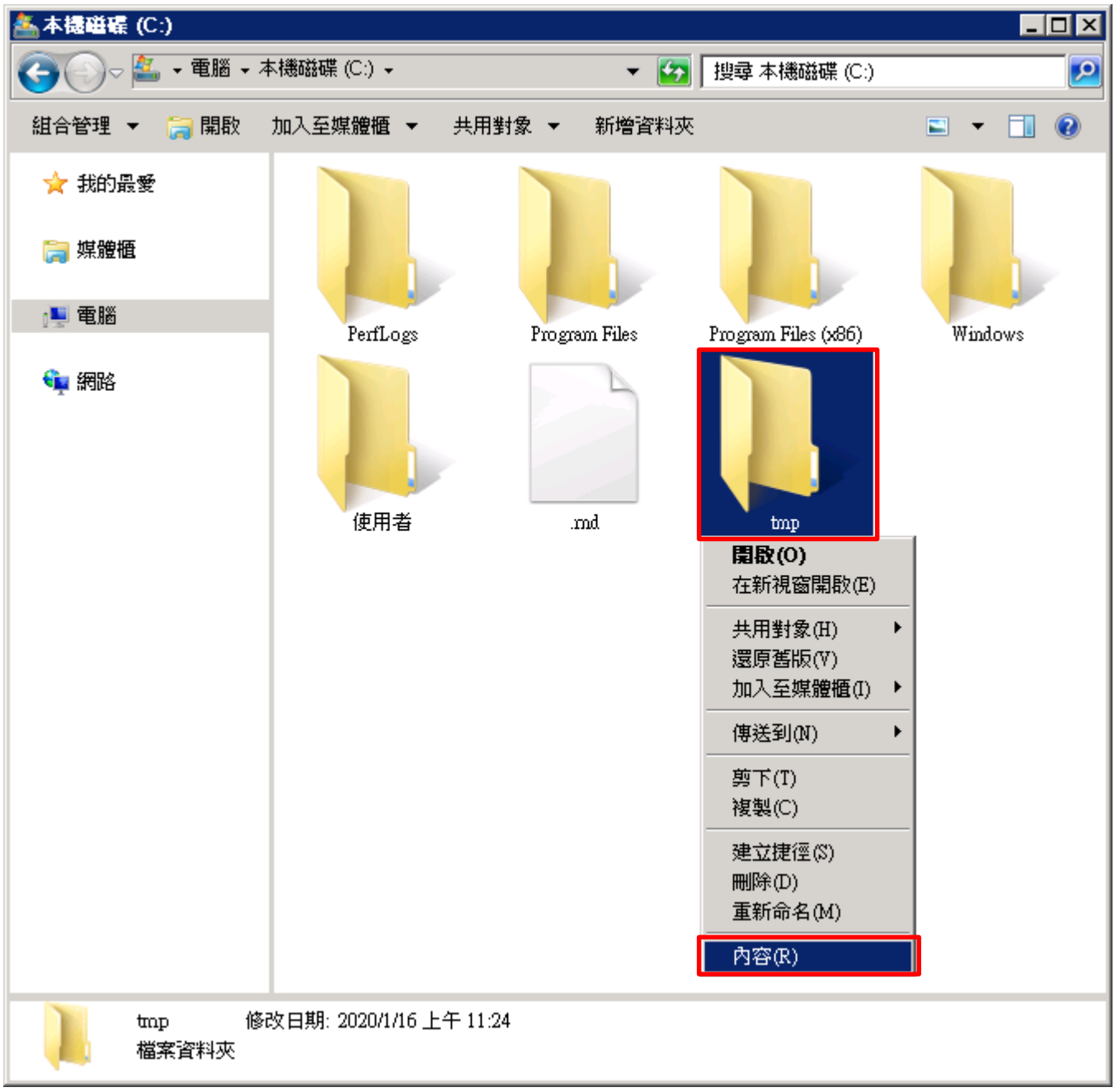
(5) 查看群組原則套用情形

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

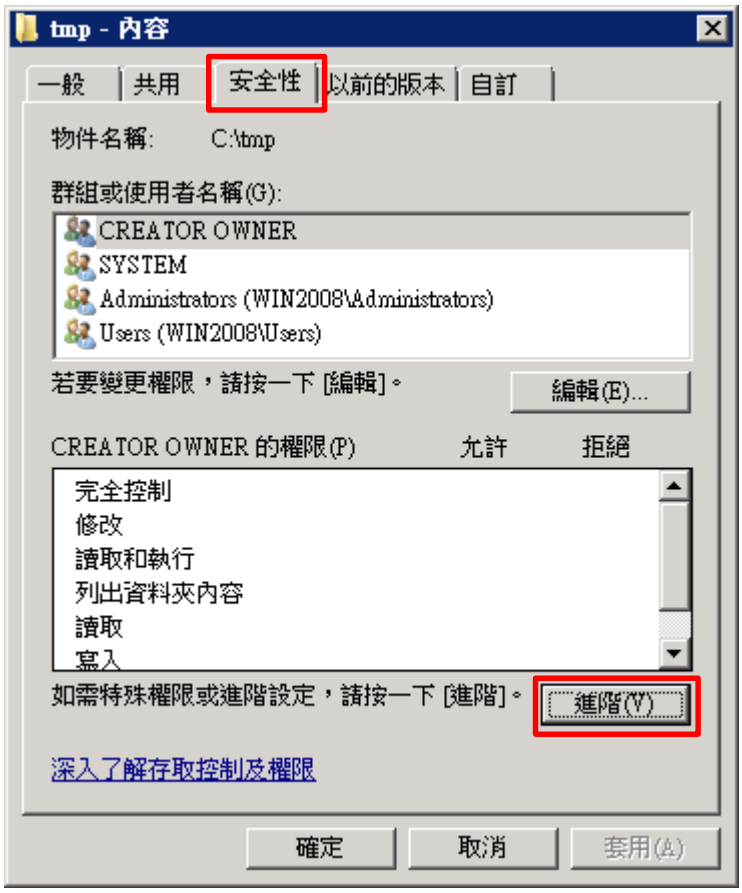


## 3.3 稽核資料夾設定

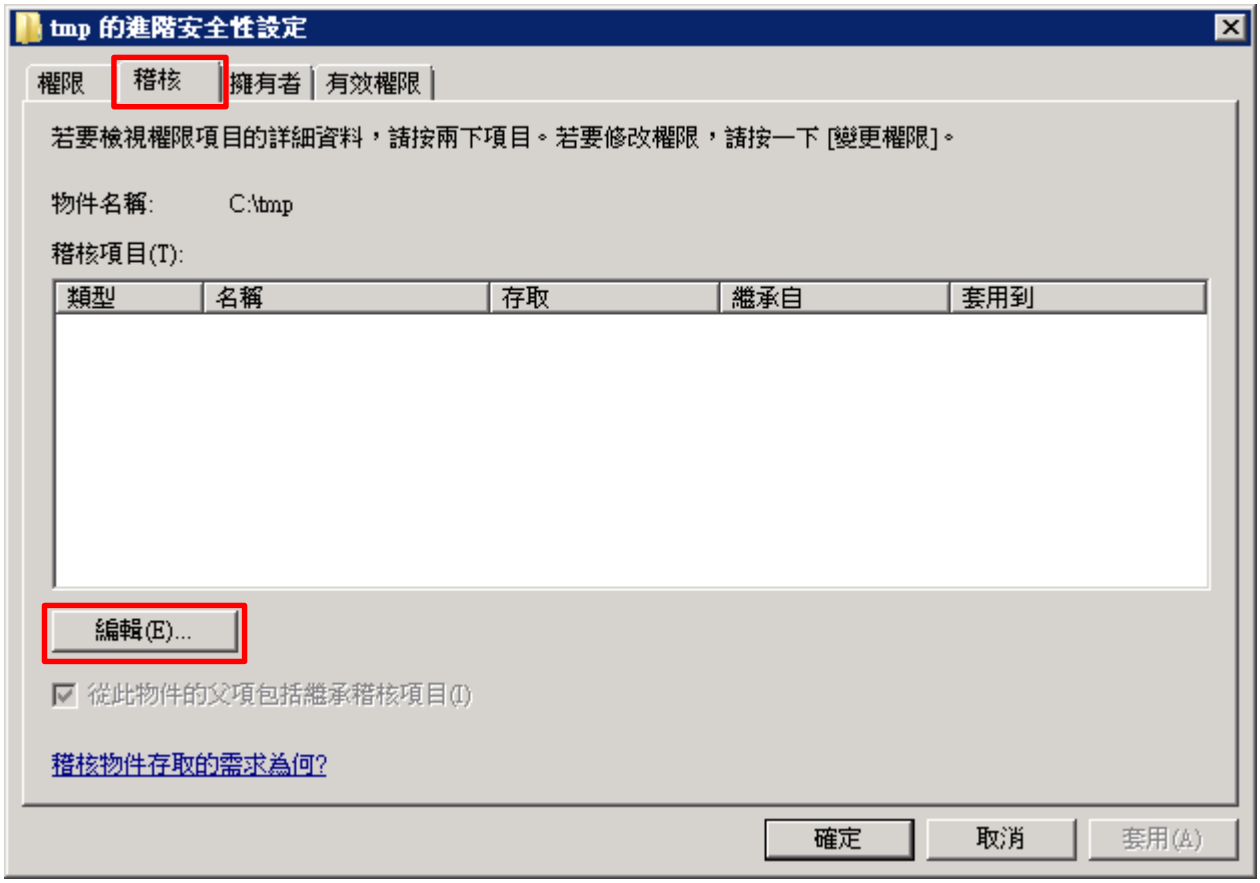
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



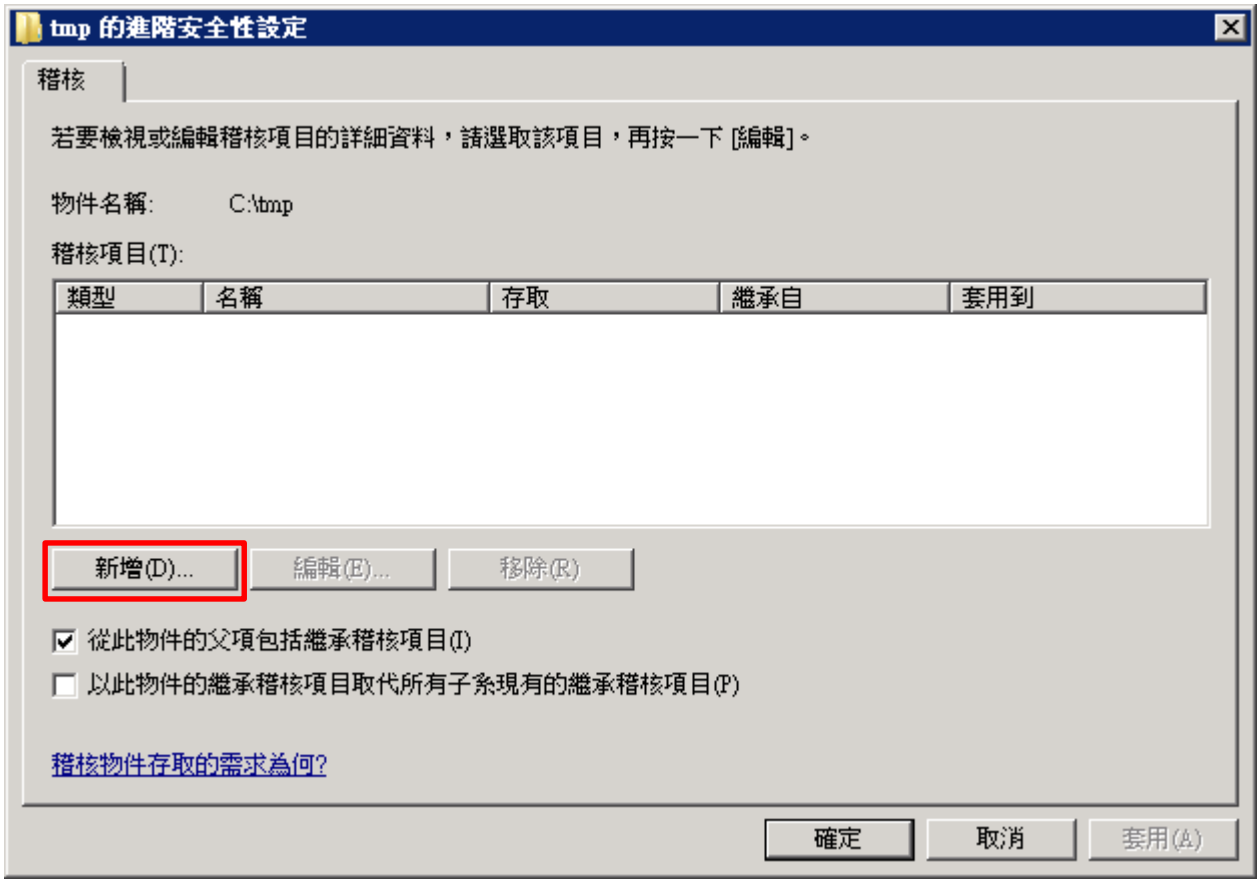
(2) 點選 [安全性] 頁面 -> 按下 [進階]



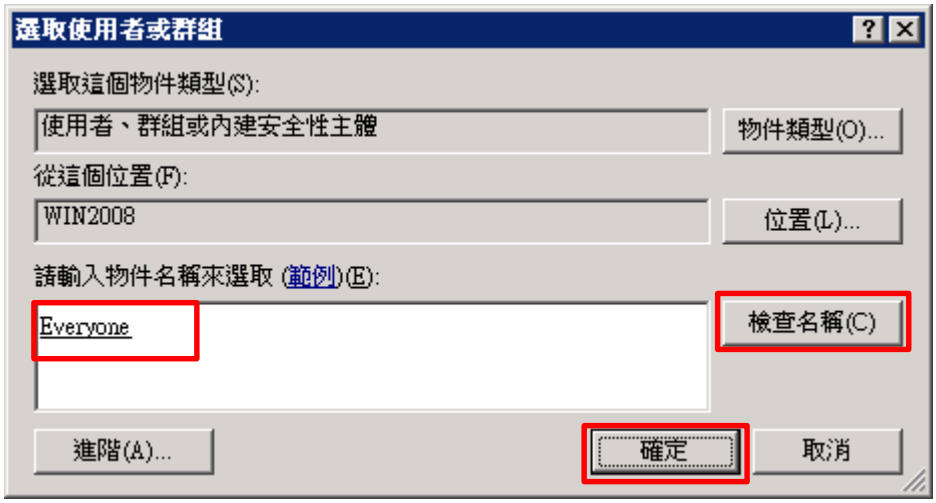

(3) 點選 [稽核] 頁面 -> 按下 [編輯]



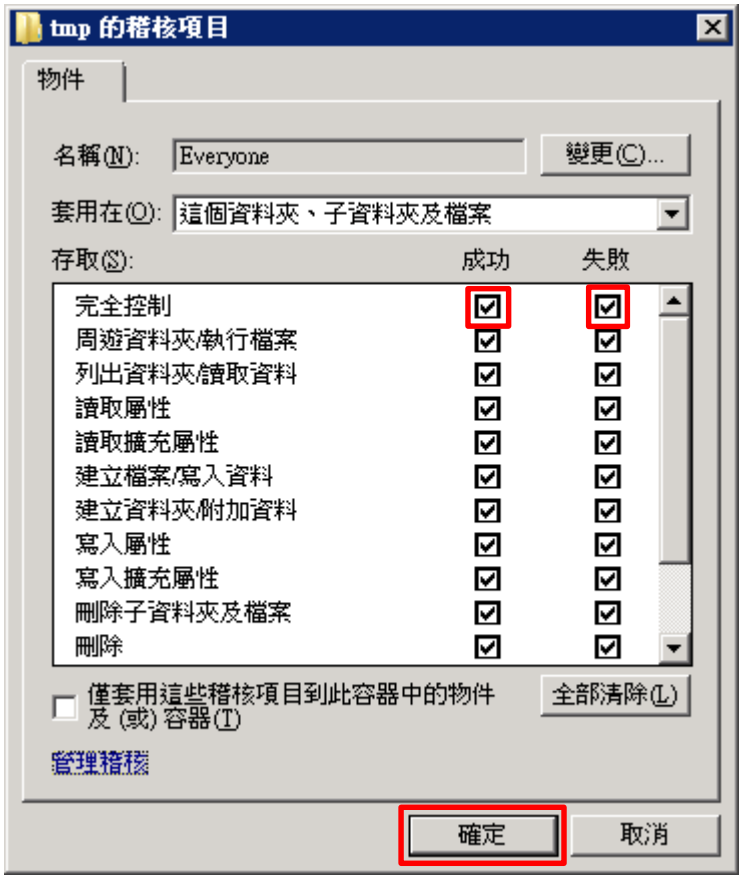
(4) 按下 [新增]



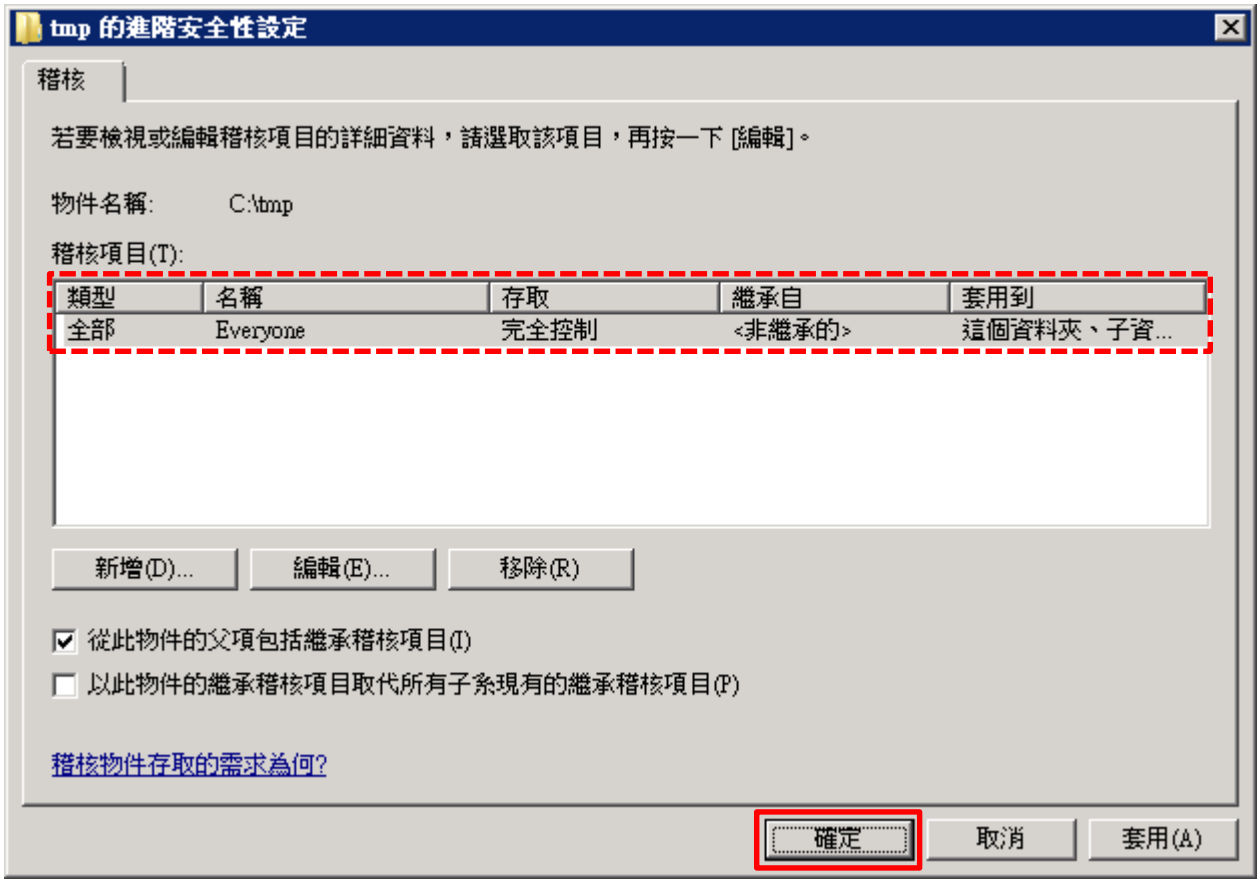

(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



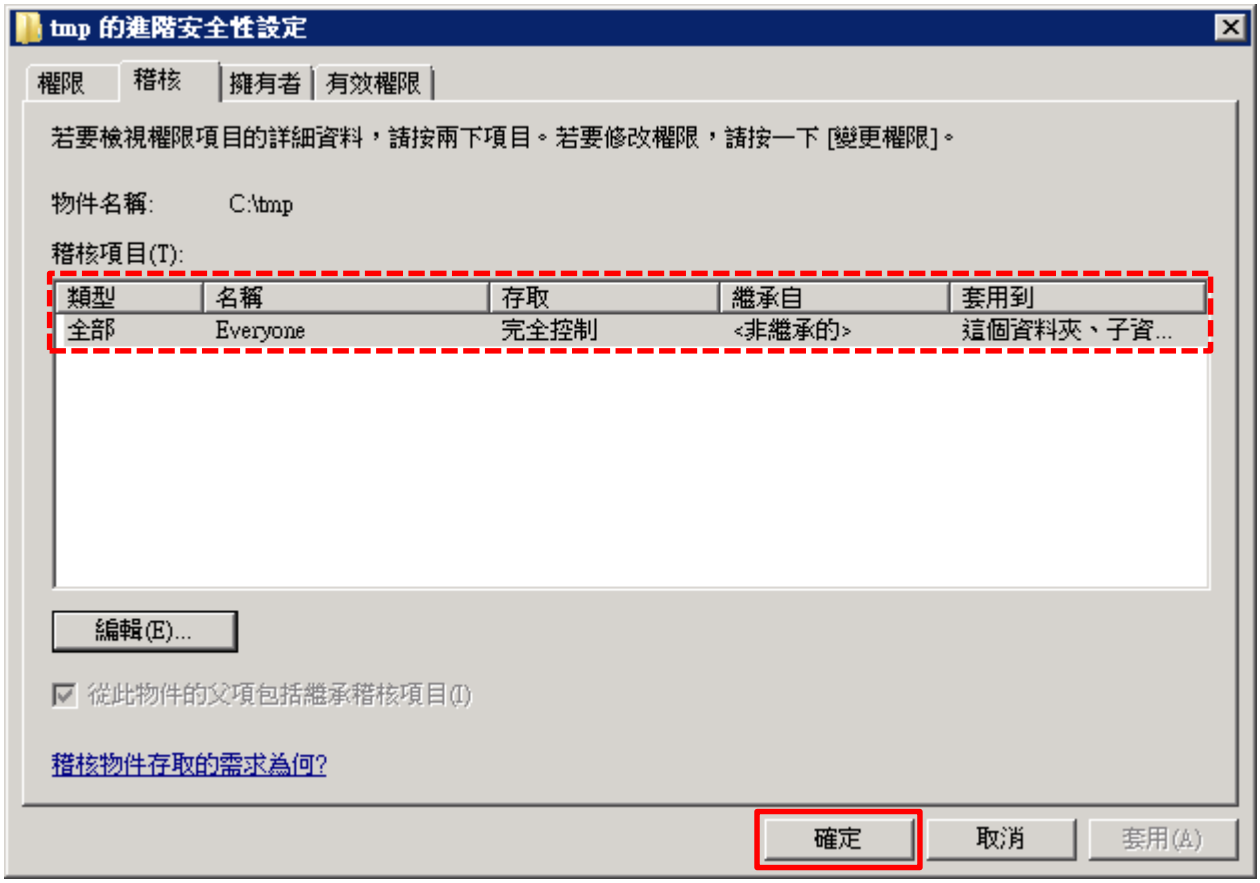
(6) 存取類型 [成功] 和 [失敗] 項目 都勾選 [完全控制] -> 按下 [確定]



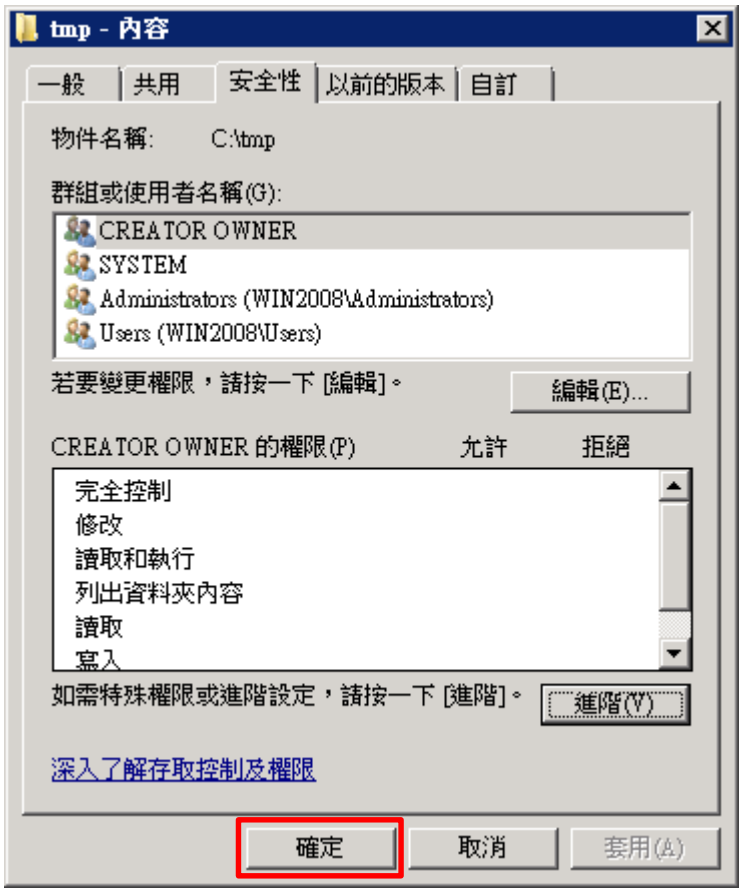

(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(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

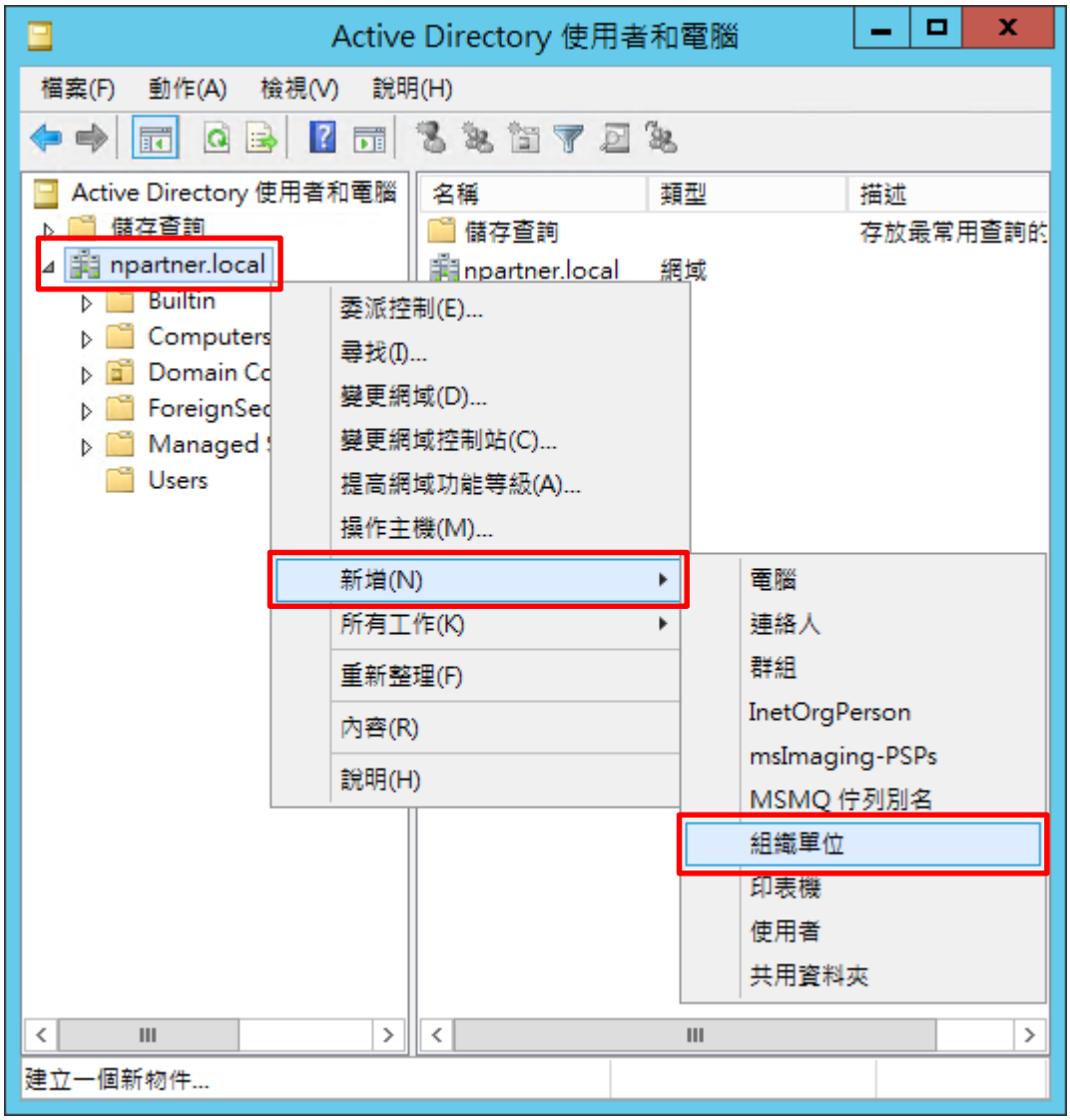
### 4.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

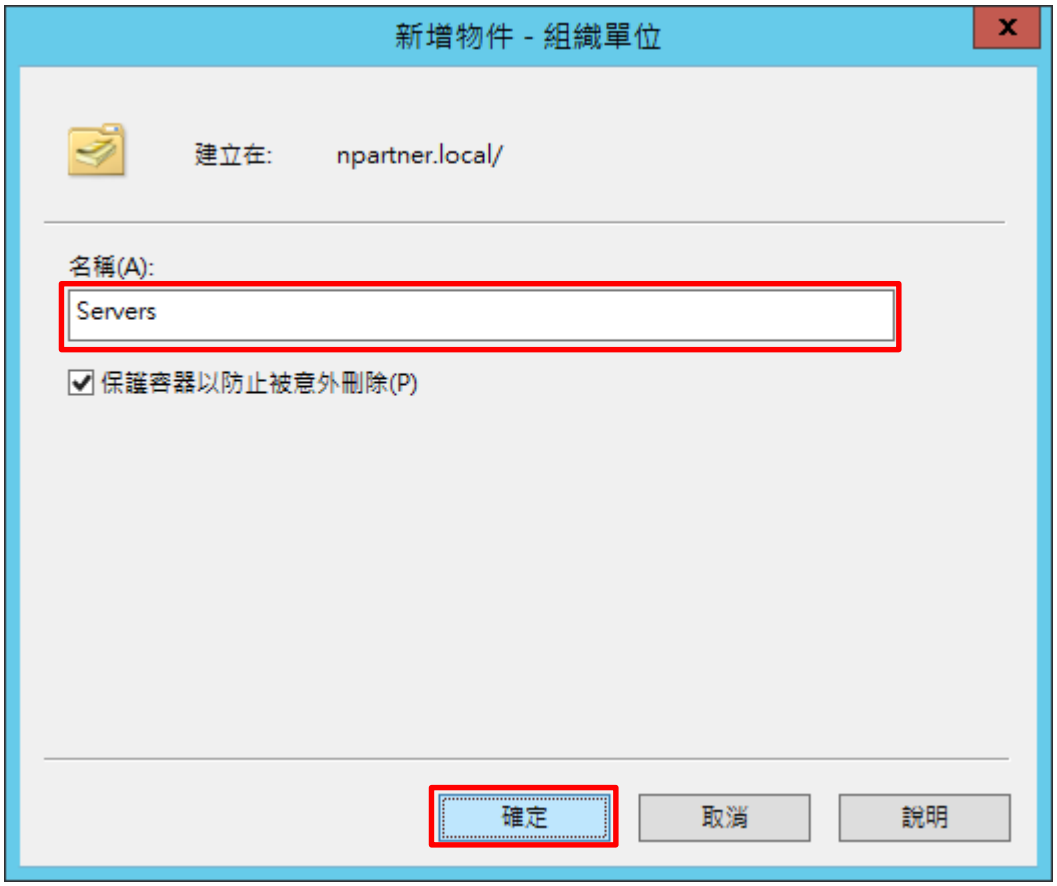
(2) 新增組織單位

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



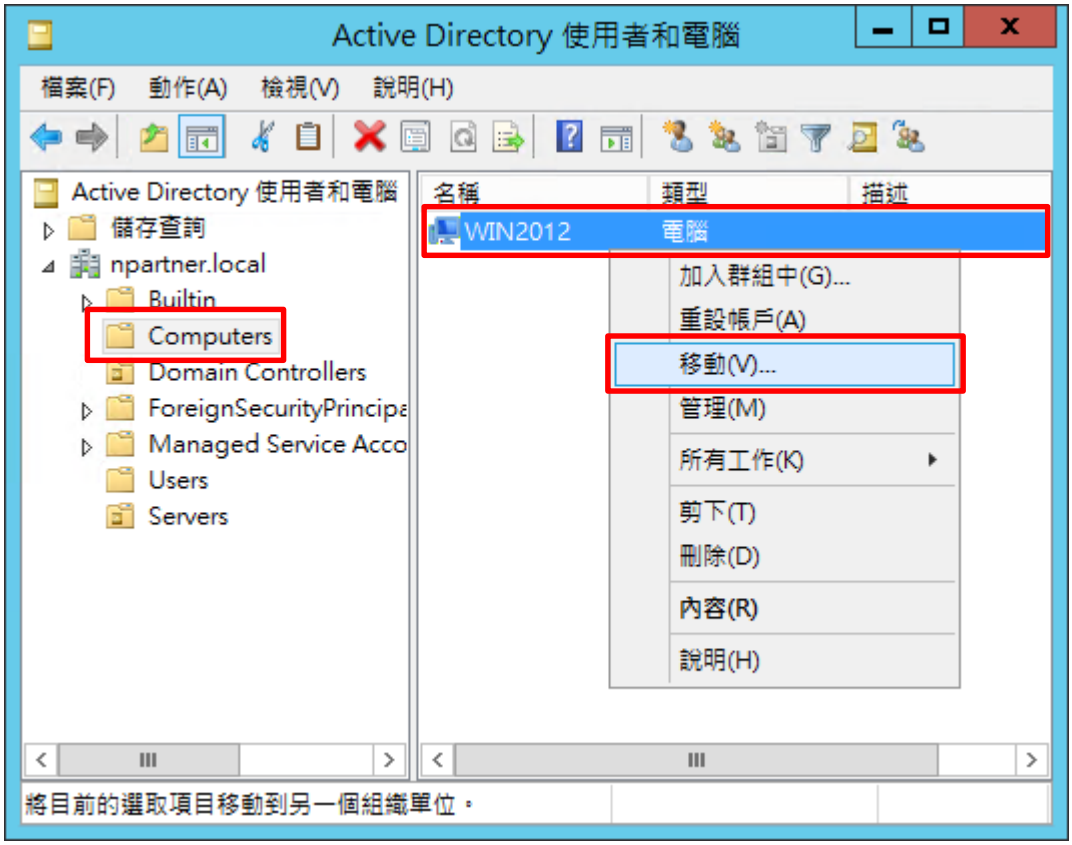
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



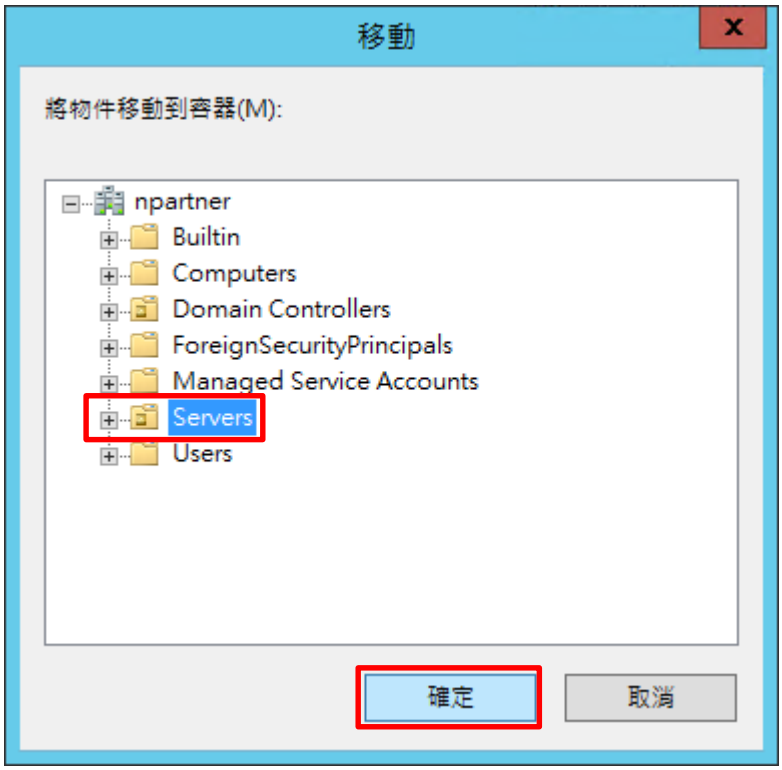
(4) 移動伺服器至新的組織單位

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



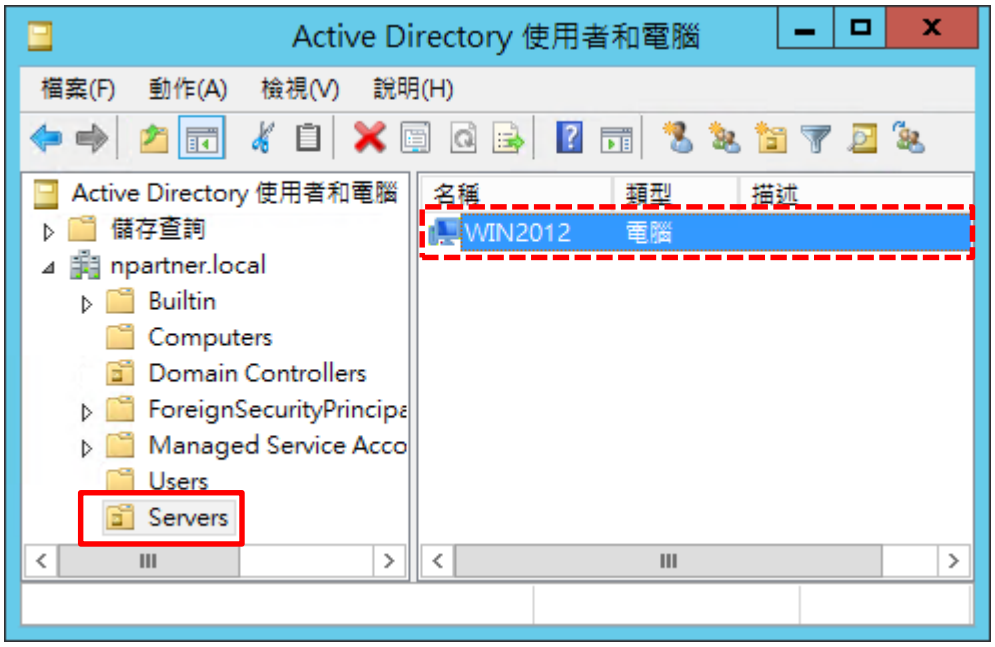

(5) 選擇組織單位

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

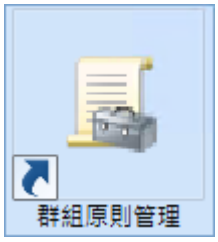
點選 [Servers] 組織單位，確認 [電腦名稱(Win2012)] 伺服器已移動



### 4.1.2 群組原則設定

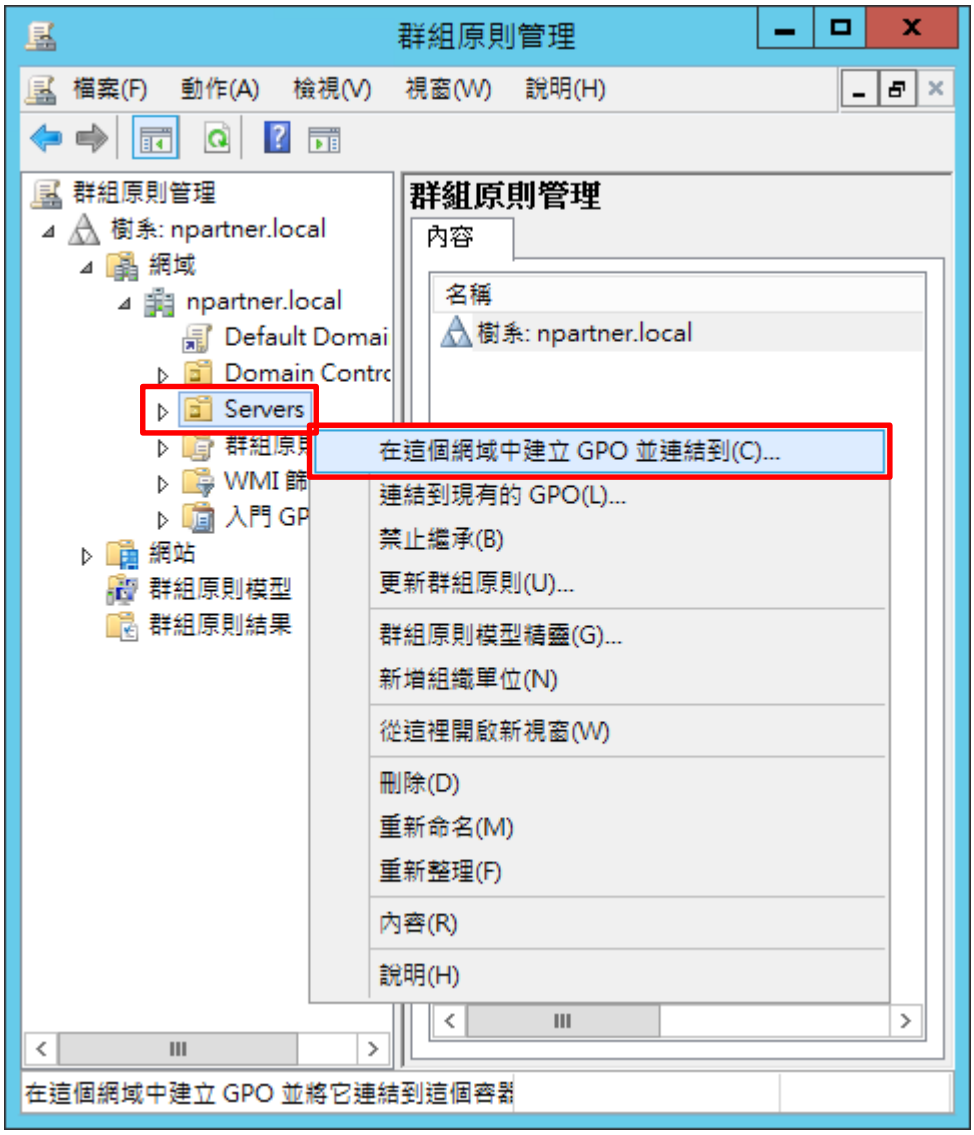
(1) 開啟群組原則管理

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...]

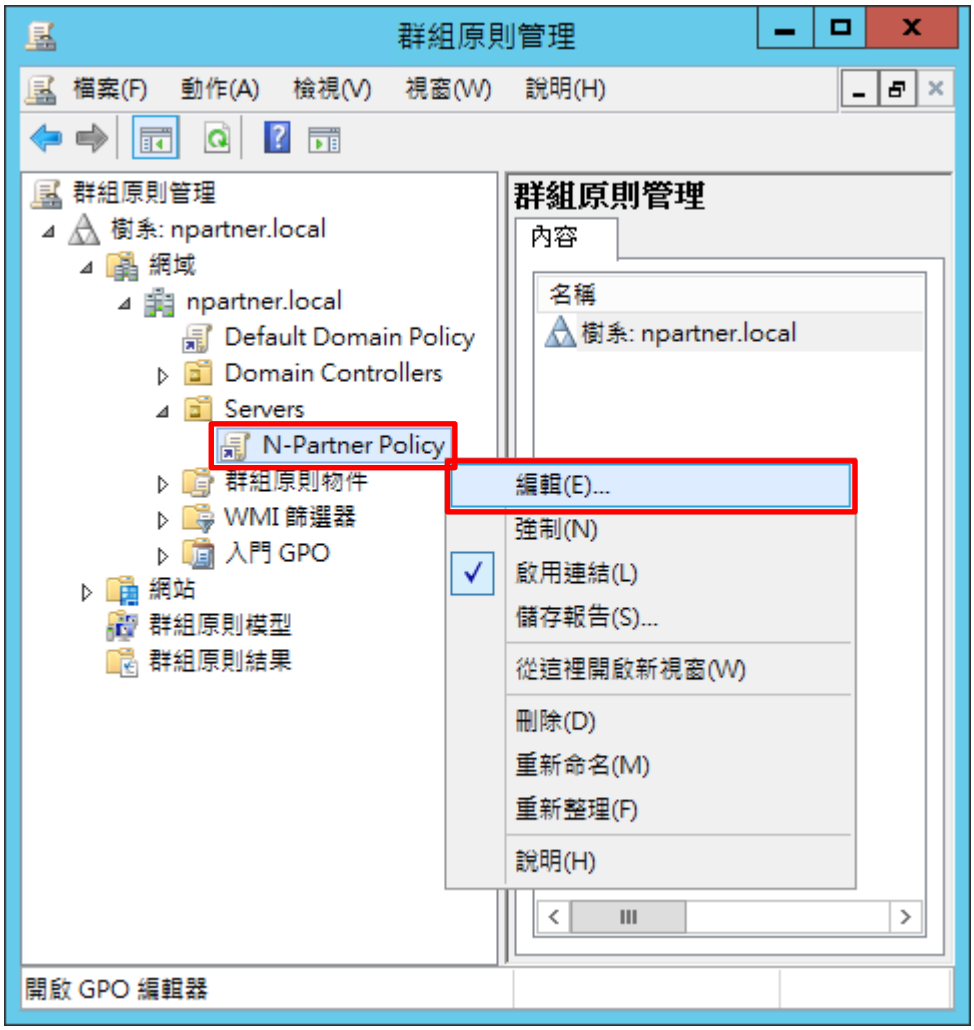


(3) 輸入群組原則物件名稱

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

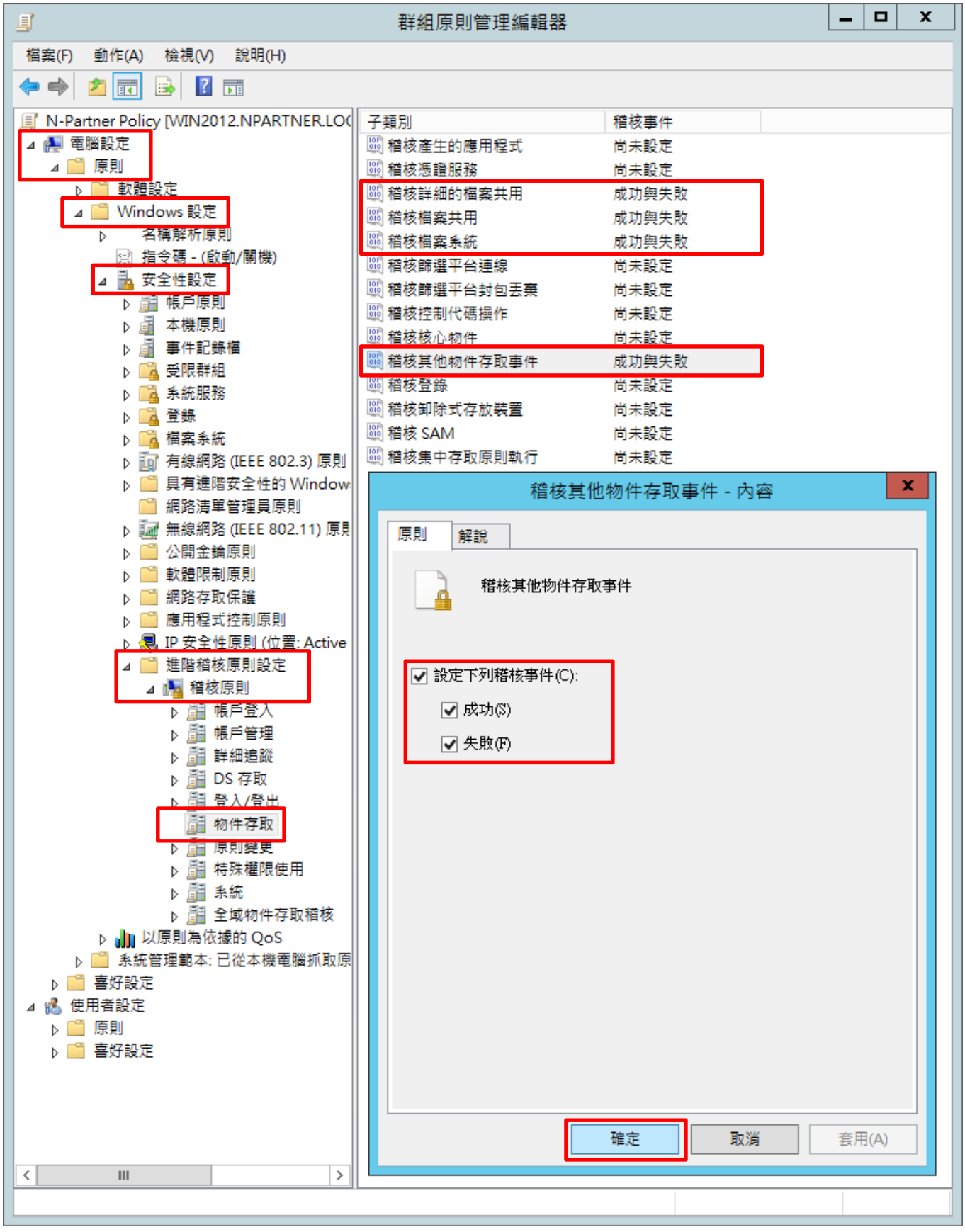

(4) 編輯群組原則物件

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



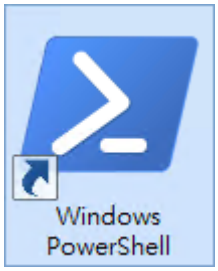
(5) 進階稽核原則：物件存取

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

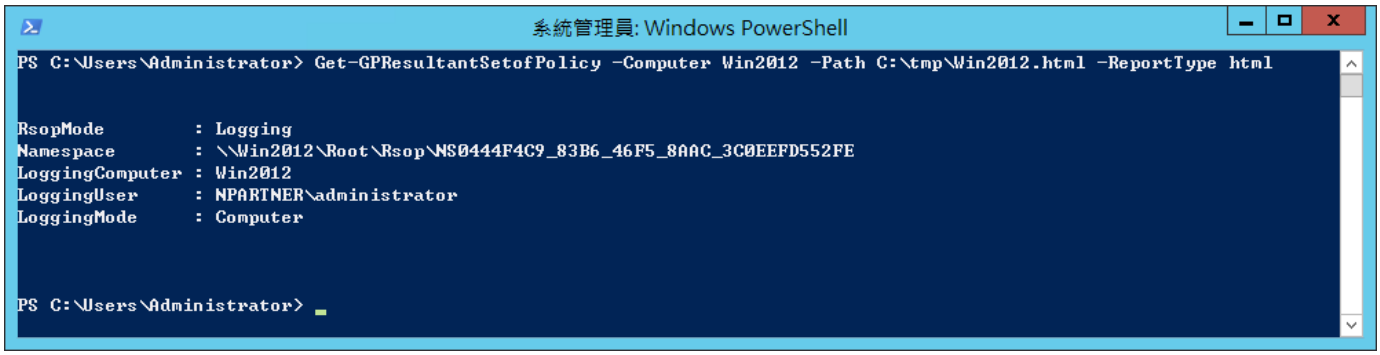
PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force


紅色文字部位請輸入 Windows File 伺服器名稱

Invoke-GPUpdate -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




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

## 4.2 工作群組

(1) 開啟搜尋

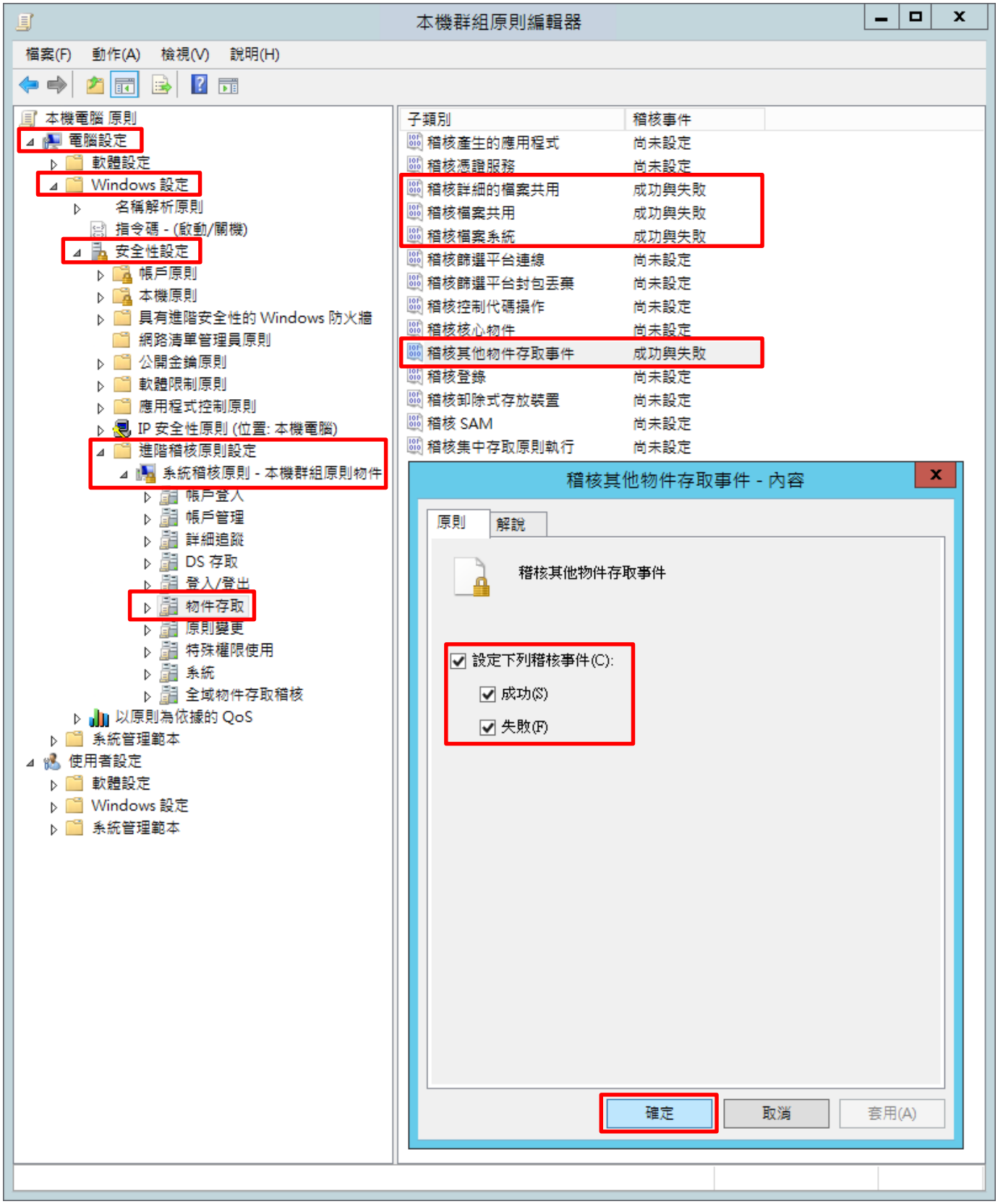
將滑鼠移到右下角點選 [搜尋]


(2) 搜尋群組原則物件編輯器並執行

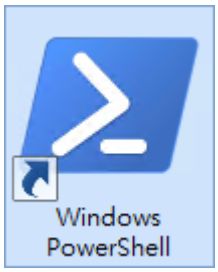
輸入 群組原則 -> 點選 [編輯群組原則]

(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]

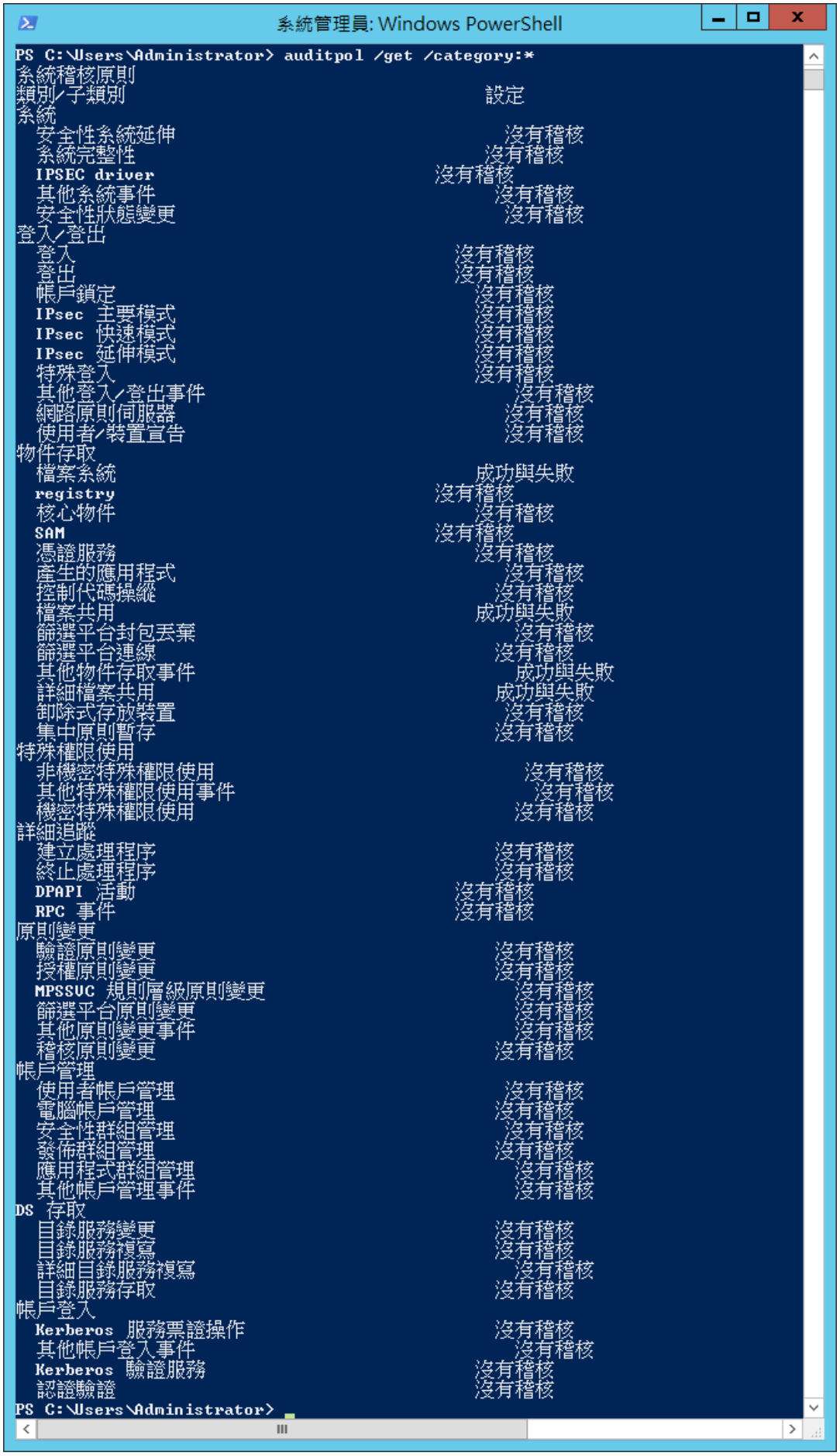



(5) 更新群組原則

PS C: \> gpupdate /force

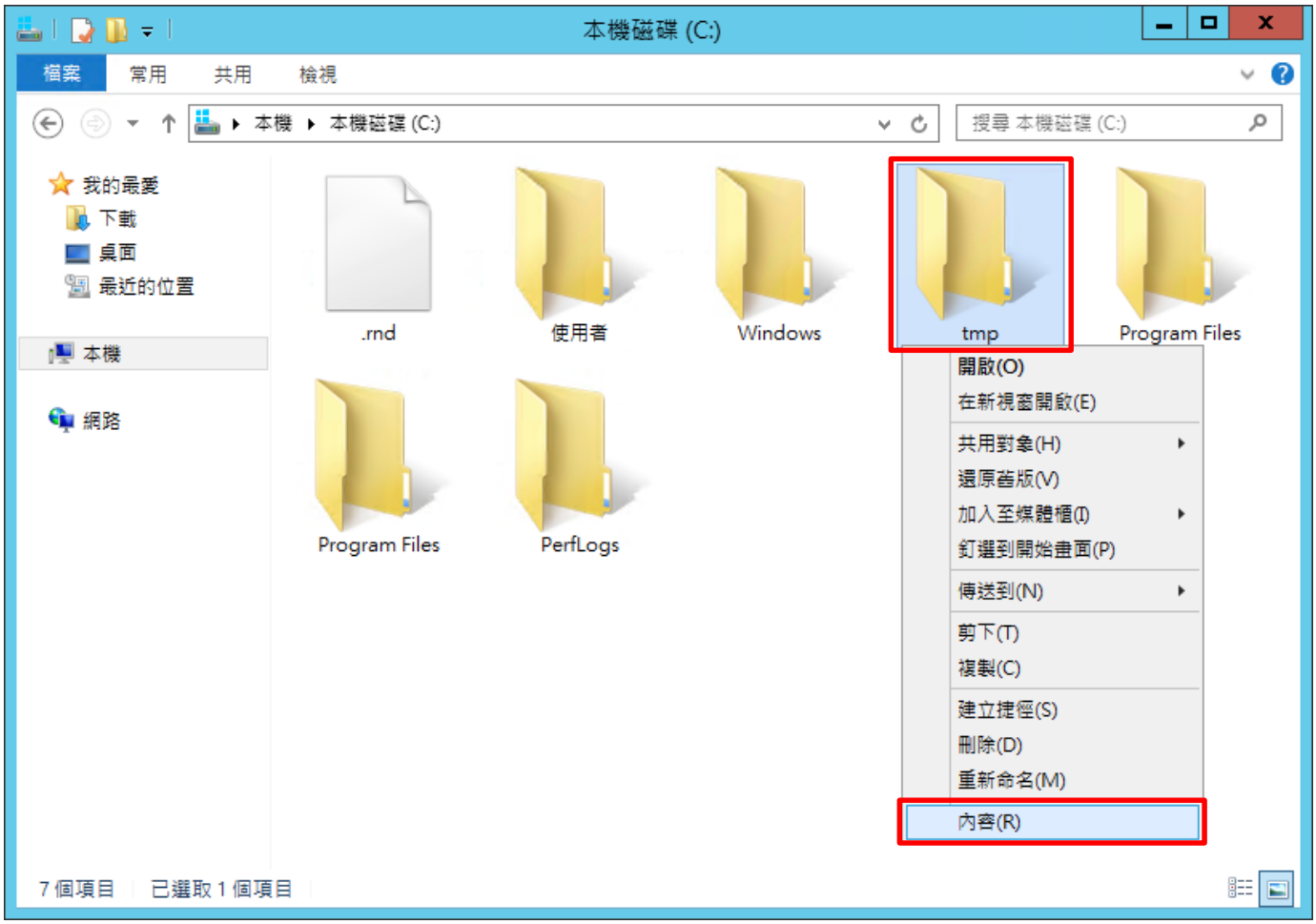
(6) 查看群組原則套用情形

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

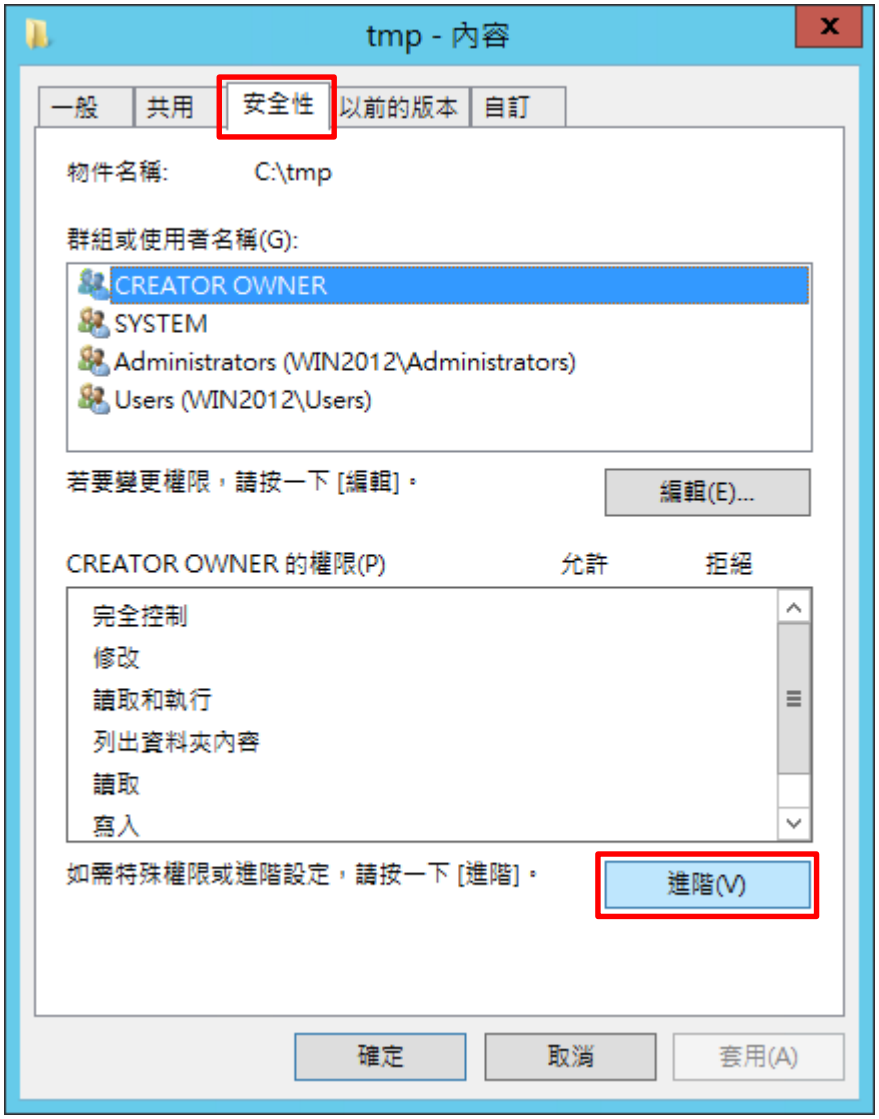


## 4.3 稽核資料夾設定

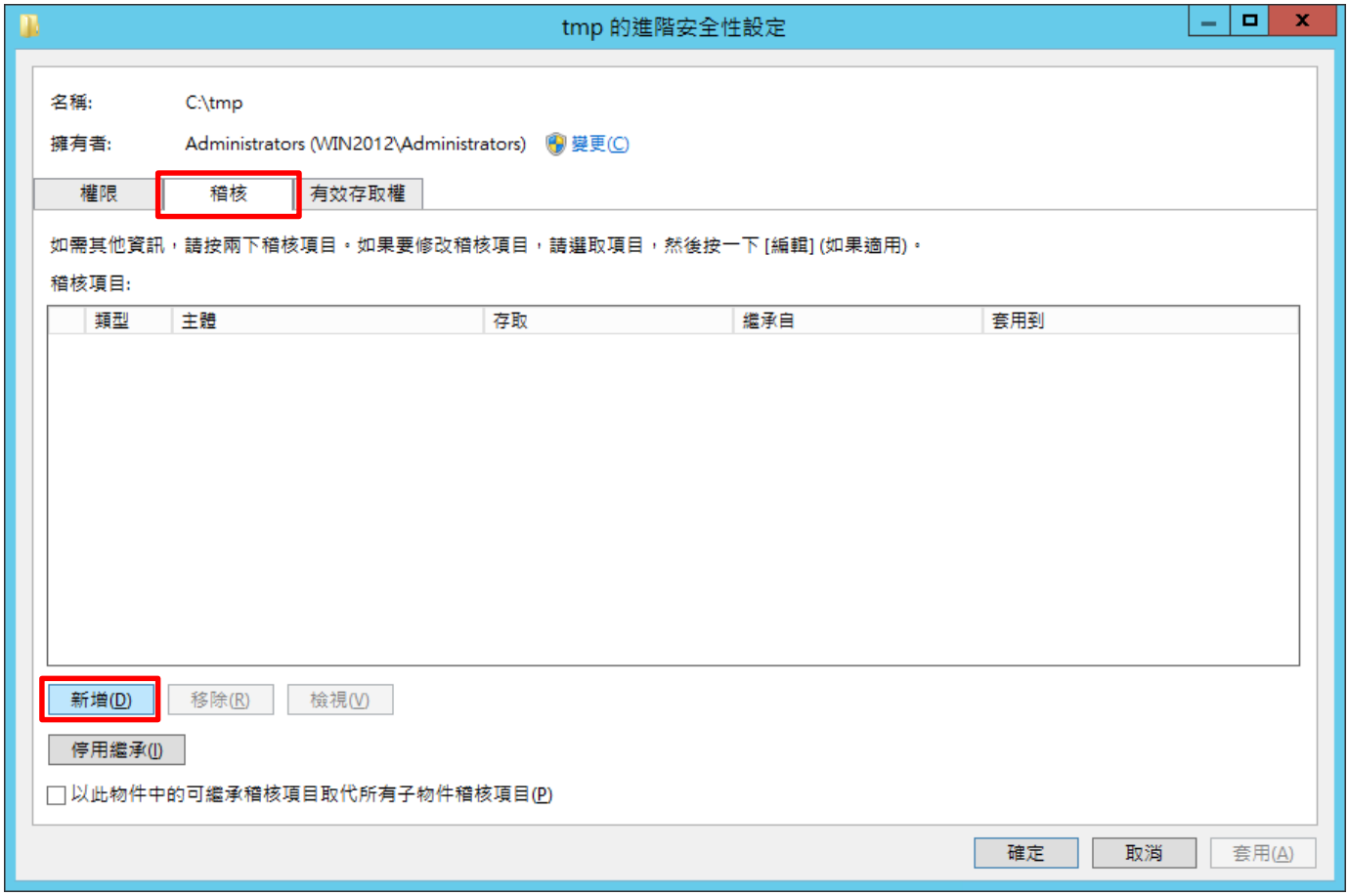
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



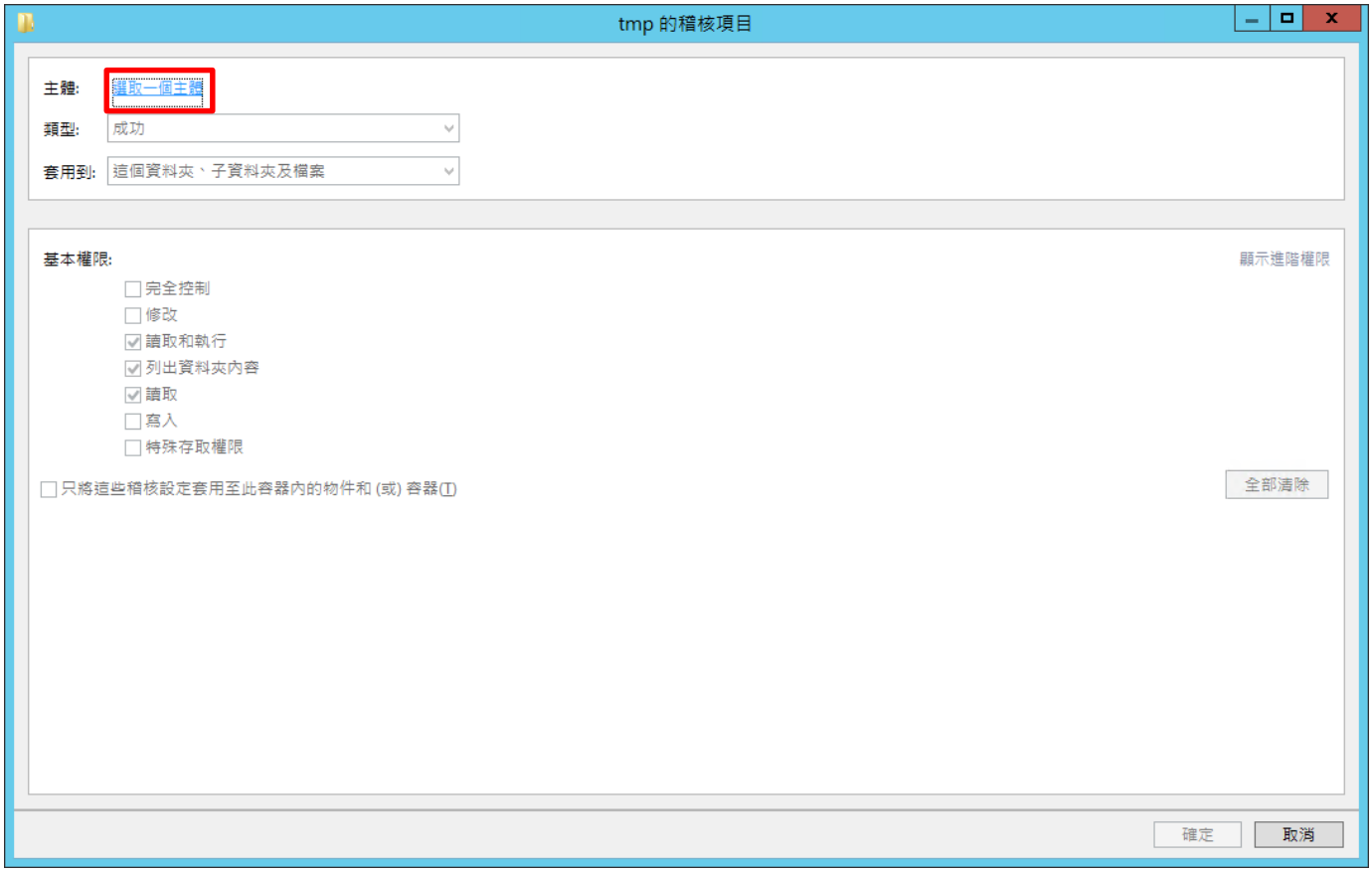
(2) 點選 [安全性] 頁面 -> 按下 [進階]



(3) 點選 [稽核] 頁面 -> 按下 [新增]

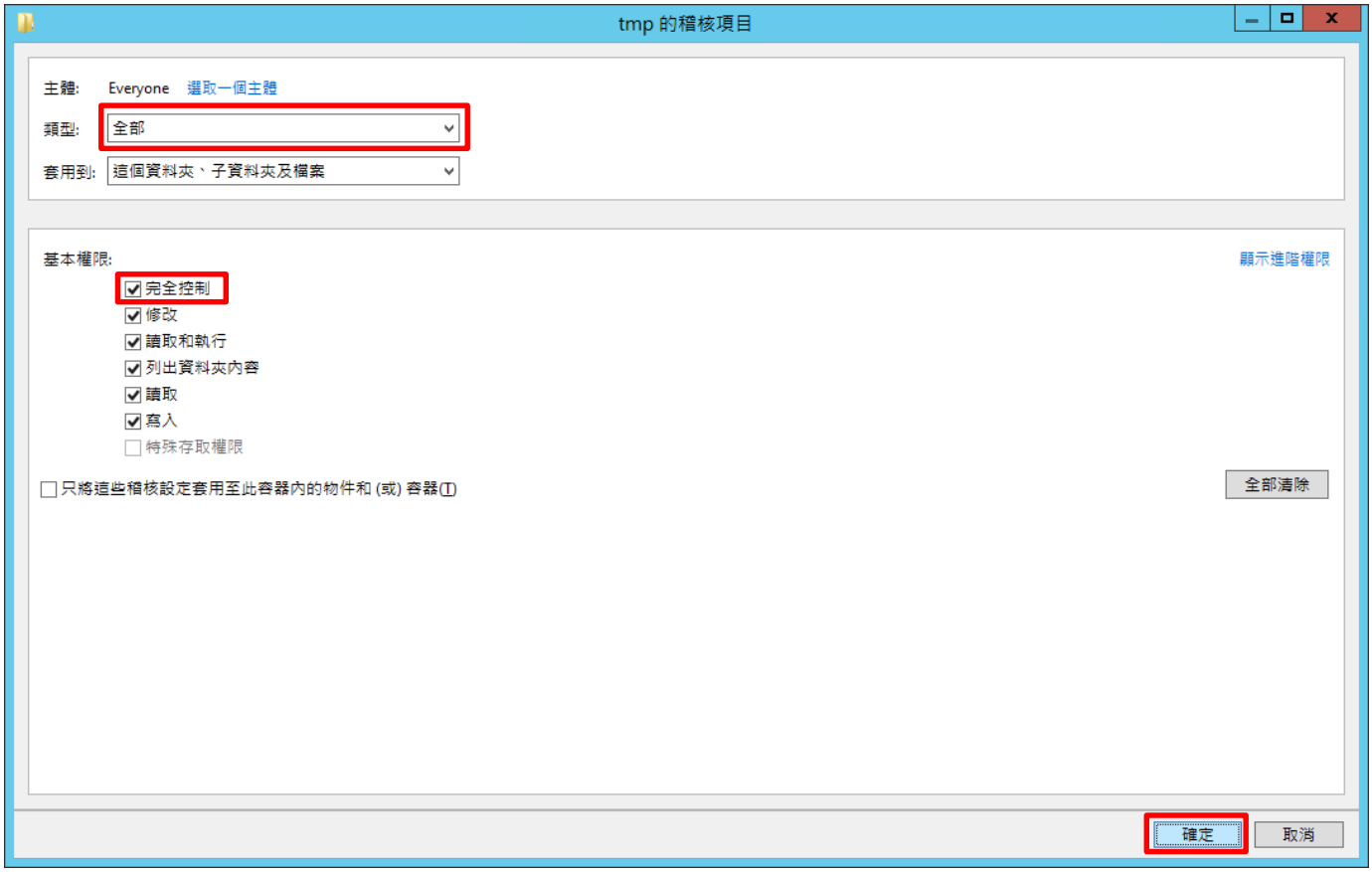


(4) 點選 [選取一個主體]

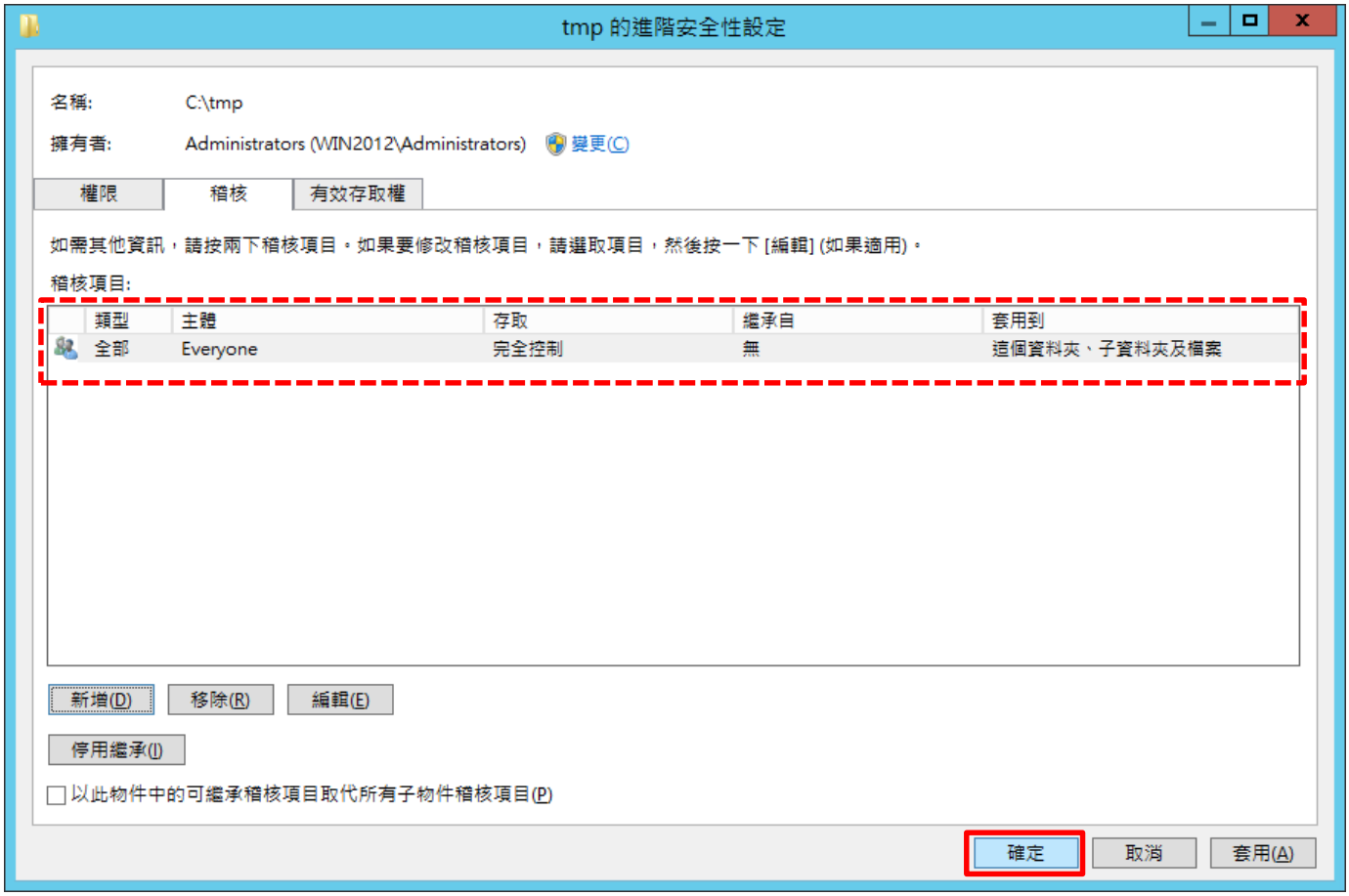



(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]

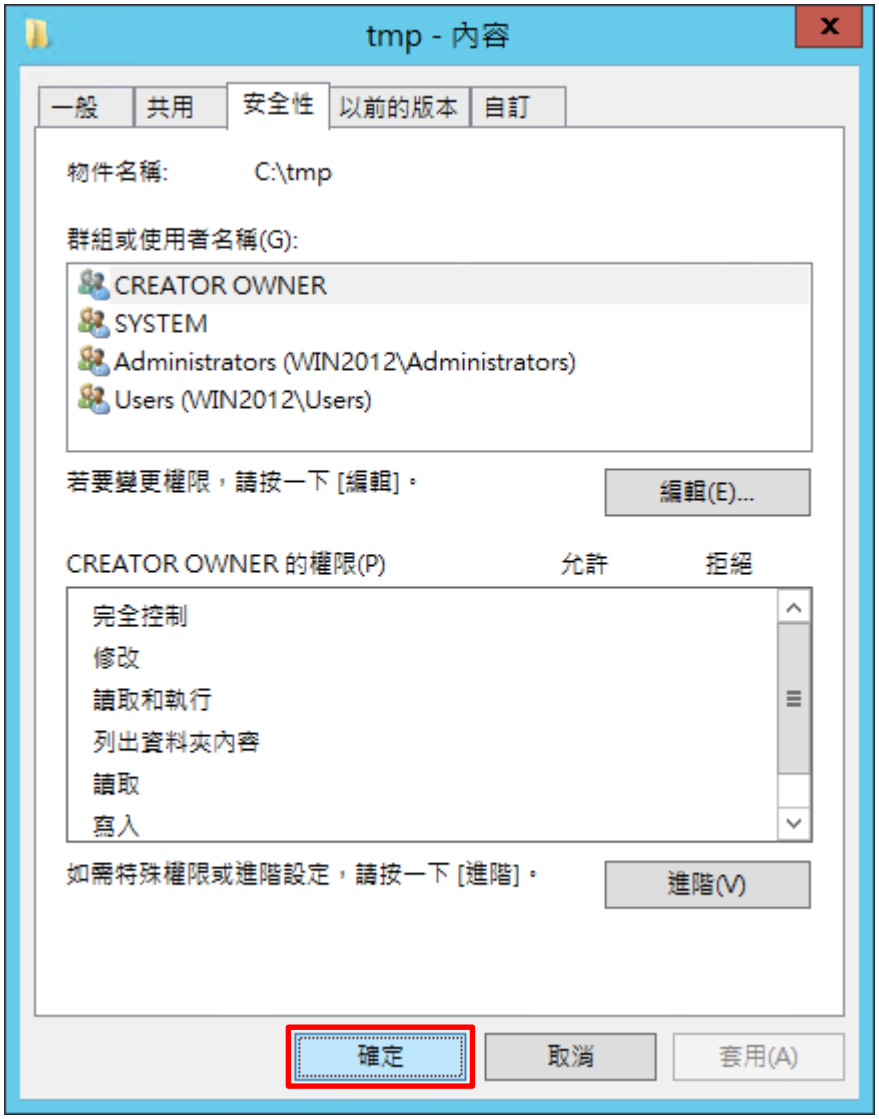
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 按下 [確定]



# 5. Windows 2016

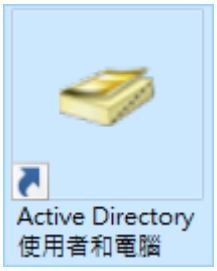
以下分別為網域和工作群組設定方式。

## 5.1 網域

### 5.1.1 組織單位設定

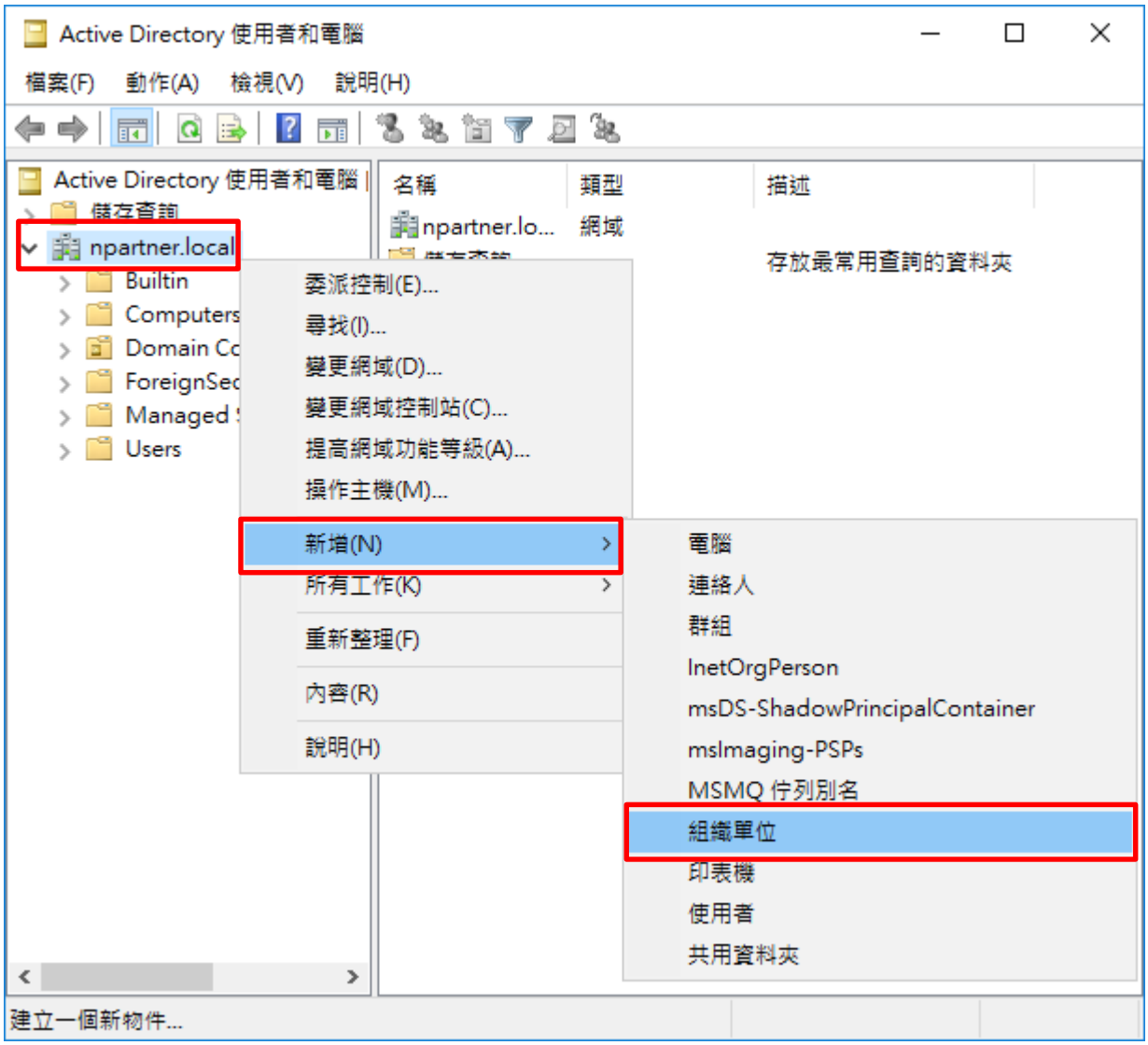
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



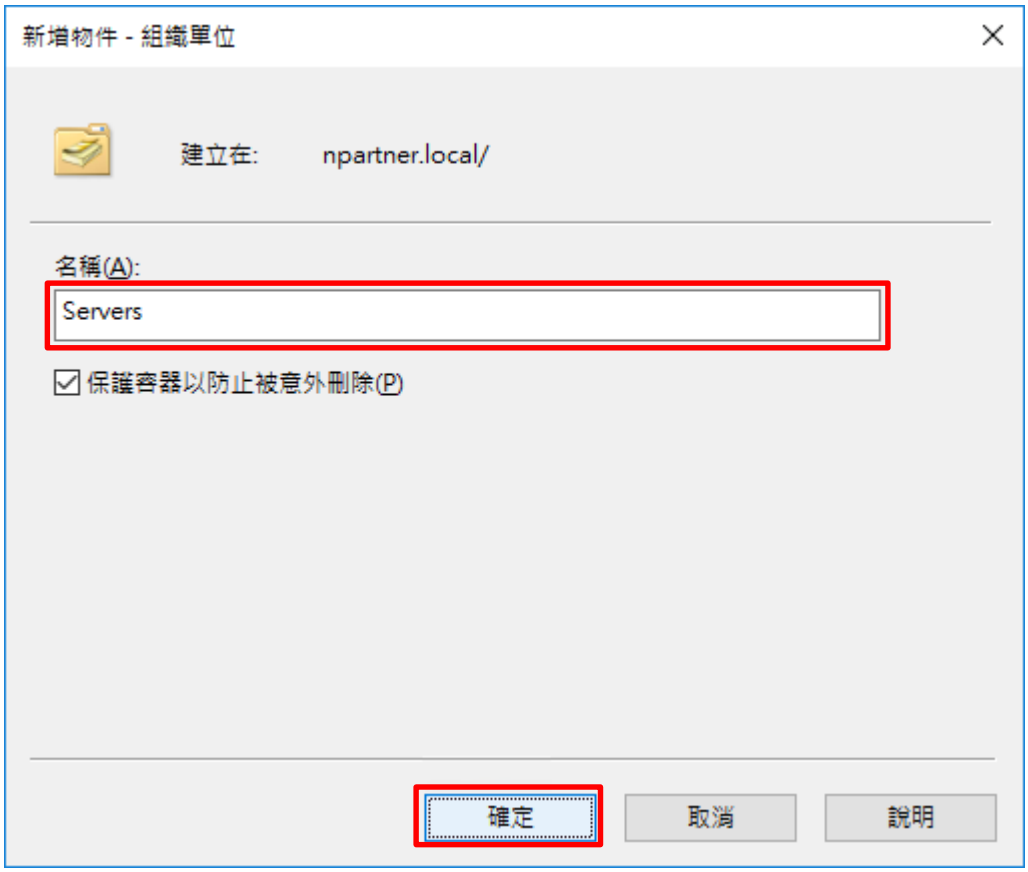
(2) 新增組織單位

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



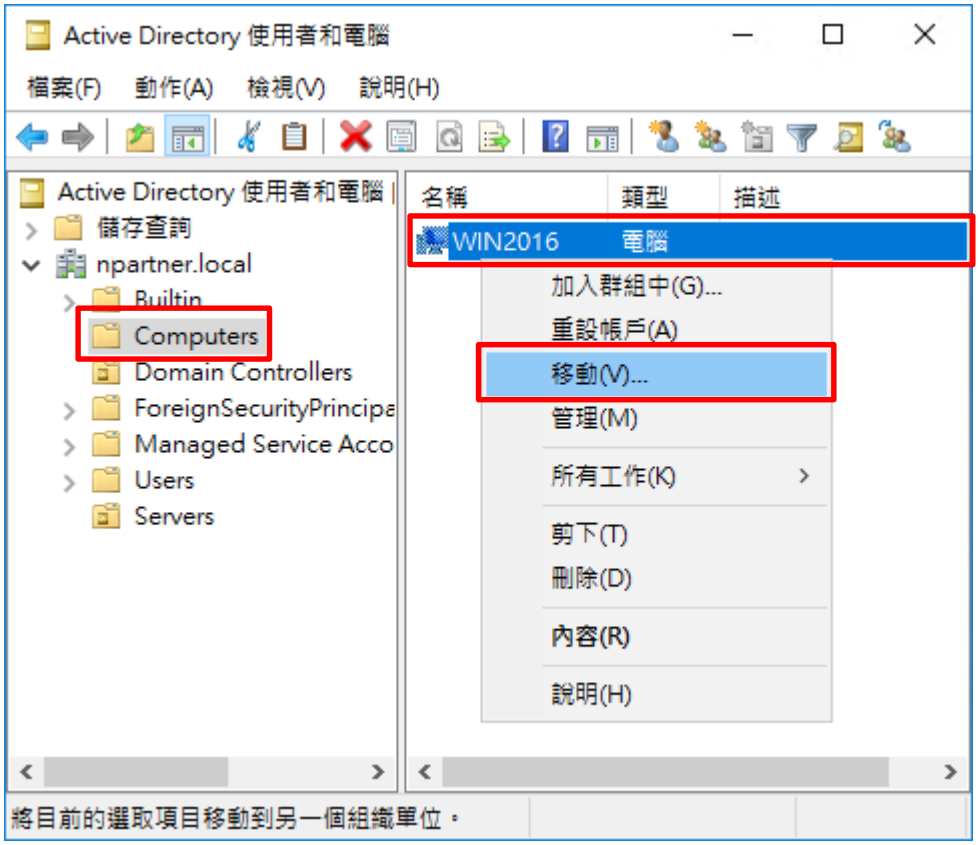
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



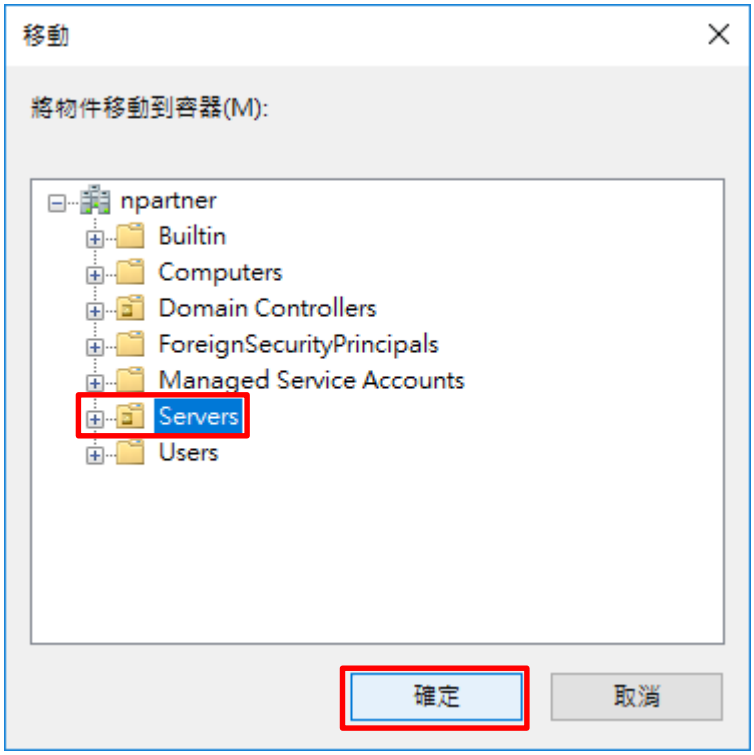
(4) 移動伺服器至新的組織單位

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



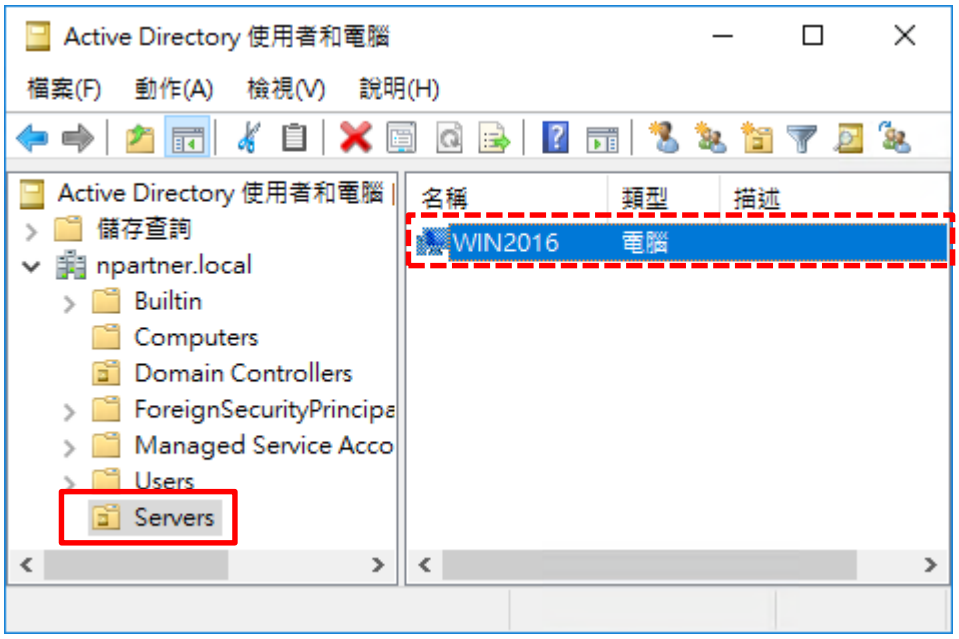

(5) 選擇組織單位

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

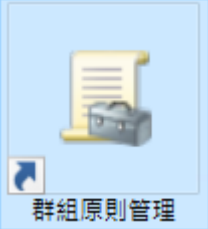
點選 [Servers] 組織單位，確認 [電腦名稱(Win2016)] 伺服器已移動



### 5.1.2 群組原則設定

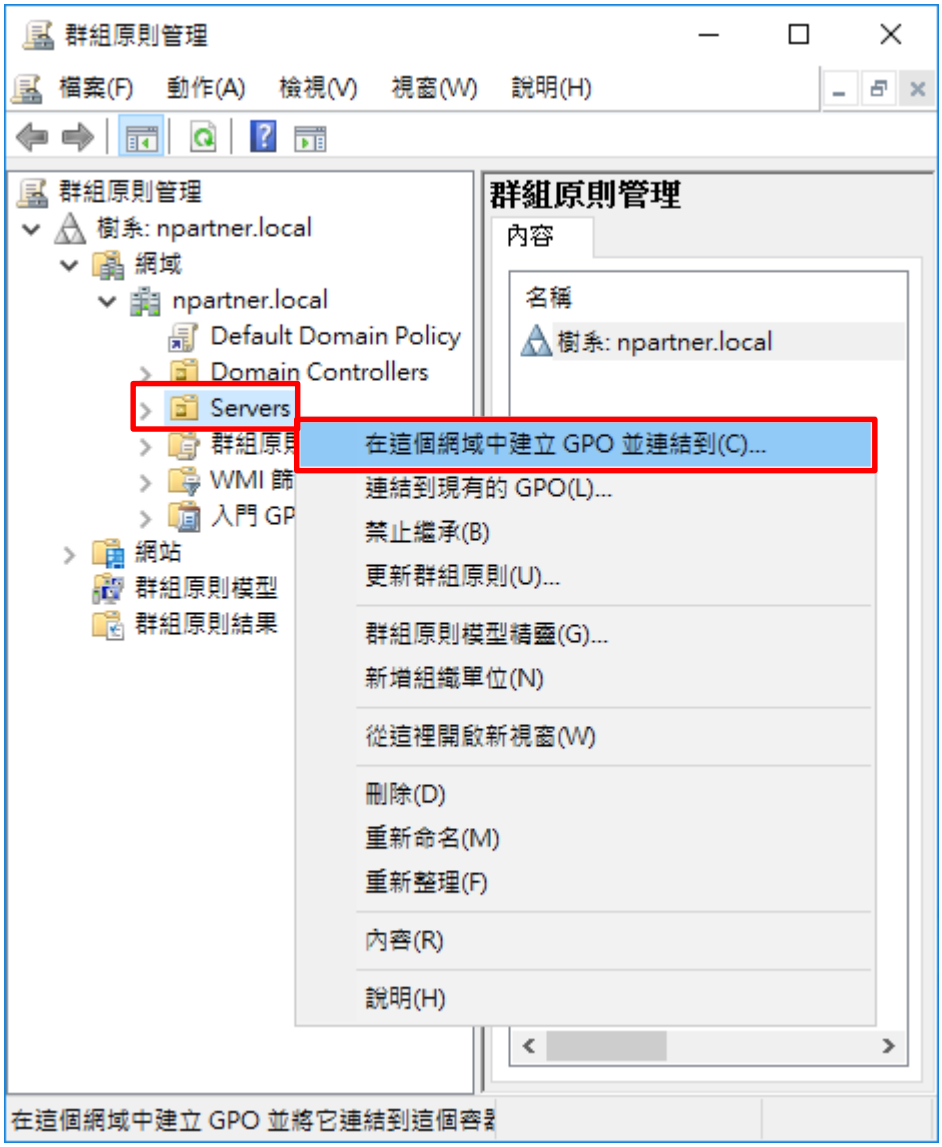
(1) 開啟群組原則管理

開啟 [群組原則管理]



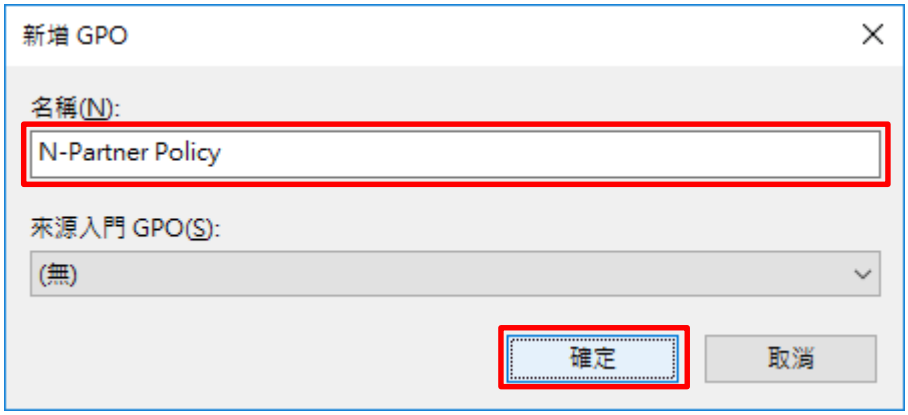

(2) 在 Servers 組織單位，新增群組原則物件

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...]



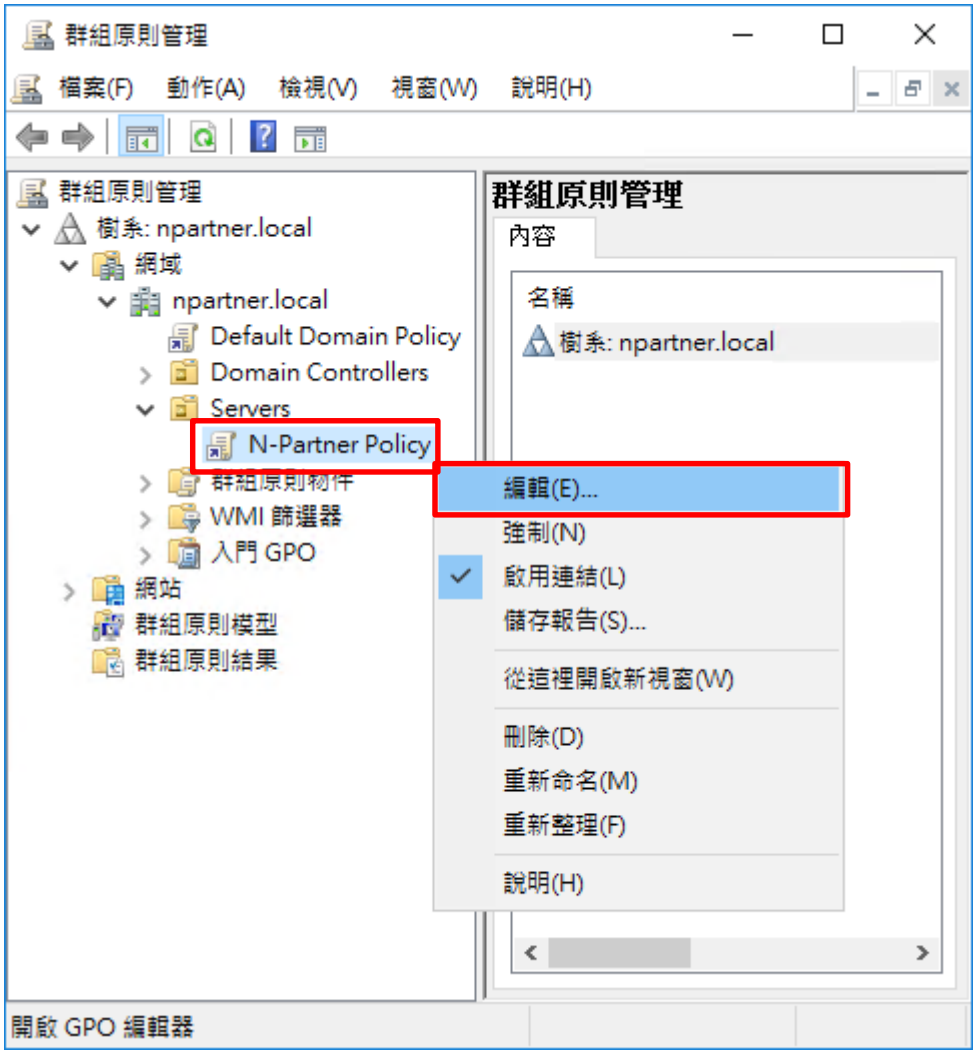
(3) 輸入群組原則物件名稱

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



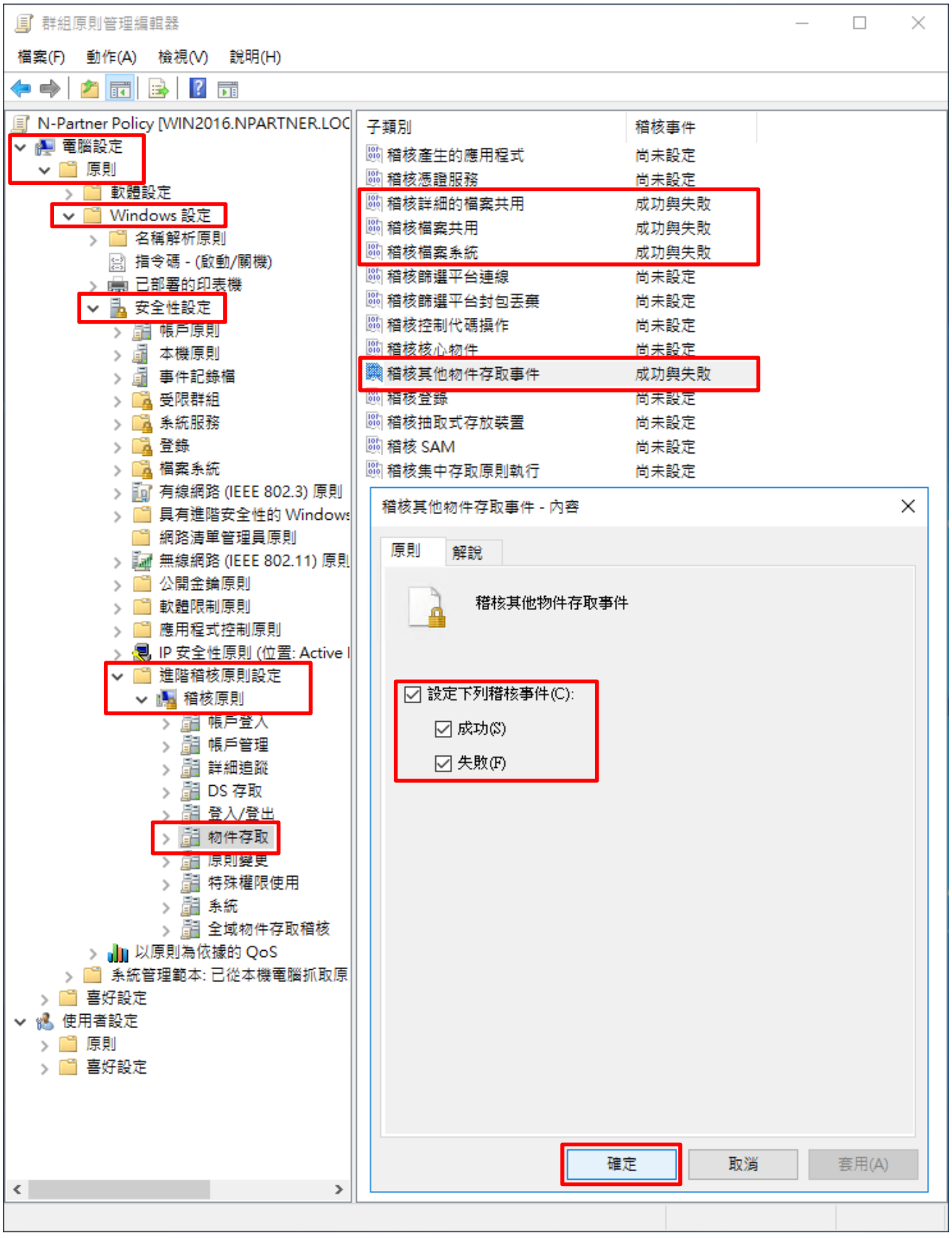

(4) 編輯群組原則物件

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



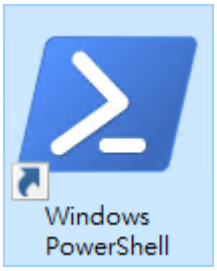
(5) 進階稽核原則：物件存取

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]



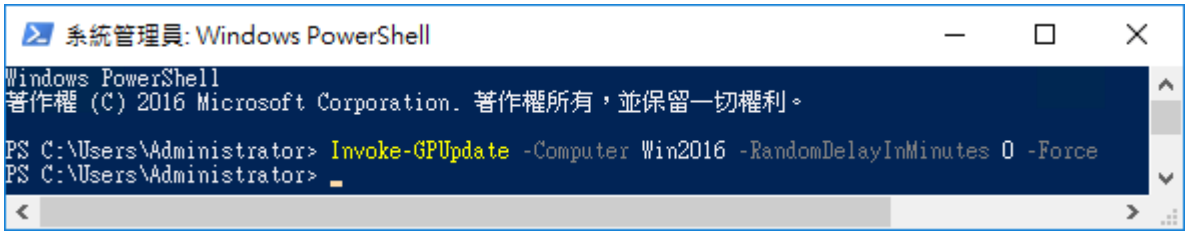
(6) 在 AD 網域伺服器，開啟 Windows PowerShell

開啟 [Windows PowerShell]




(7) 更新 Windows File 伺服器群組原則

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

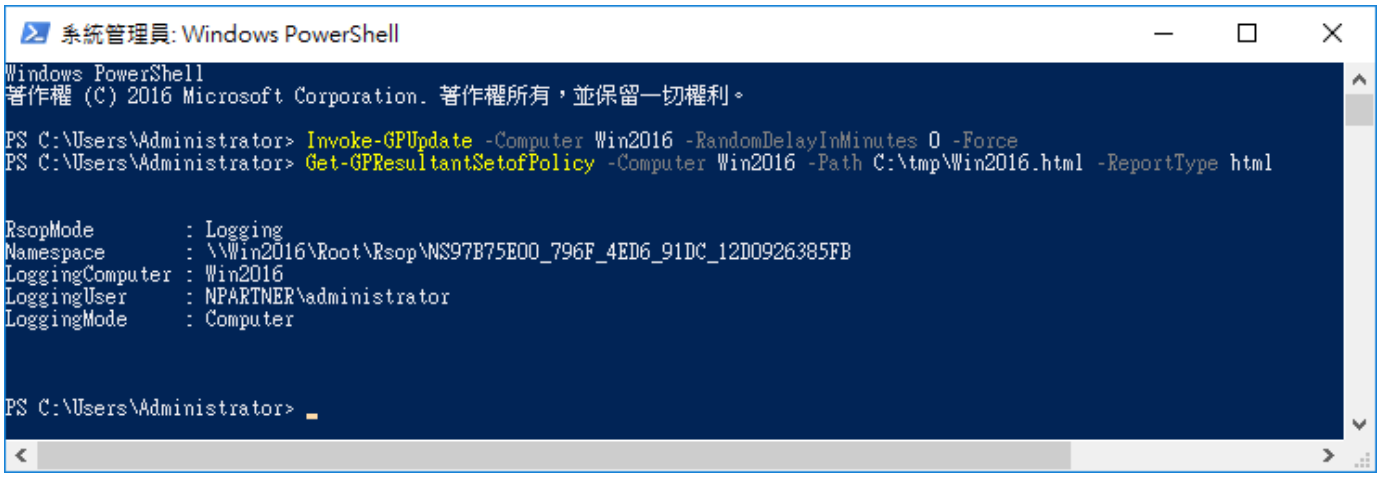



紅色文字部位請輸入 Windows File 伺服器名稱

Invoke-GPUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force

(8) 產生 Windows File 伺服器群組原則報表

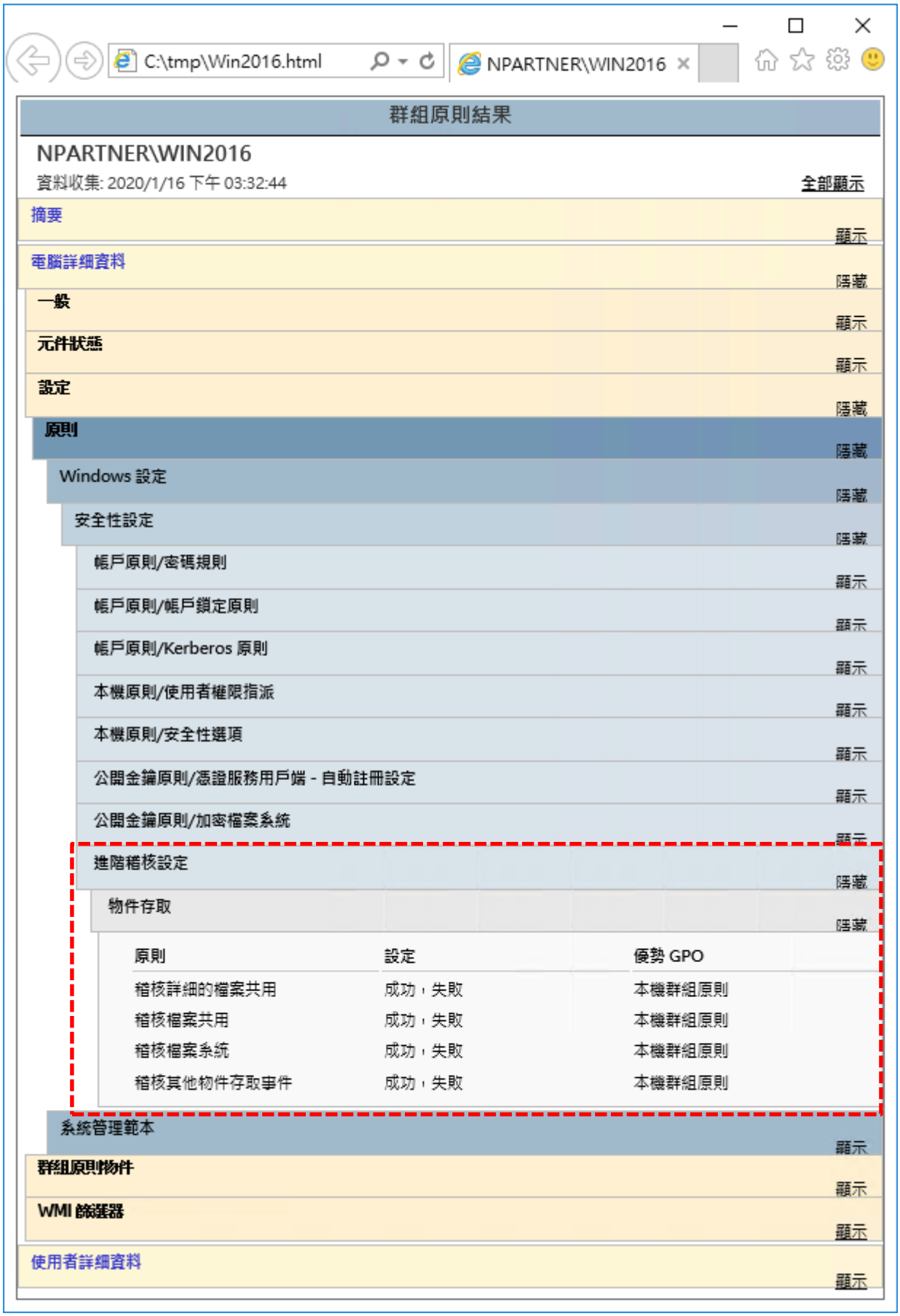
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016 -Path C:\tmp\Win2016.html -ReportType html




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

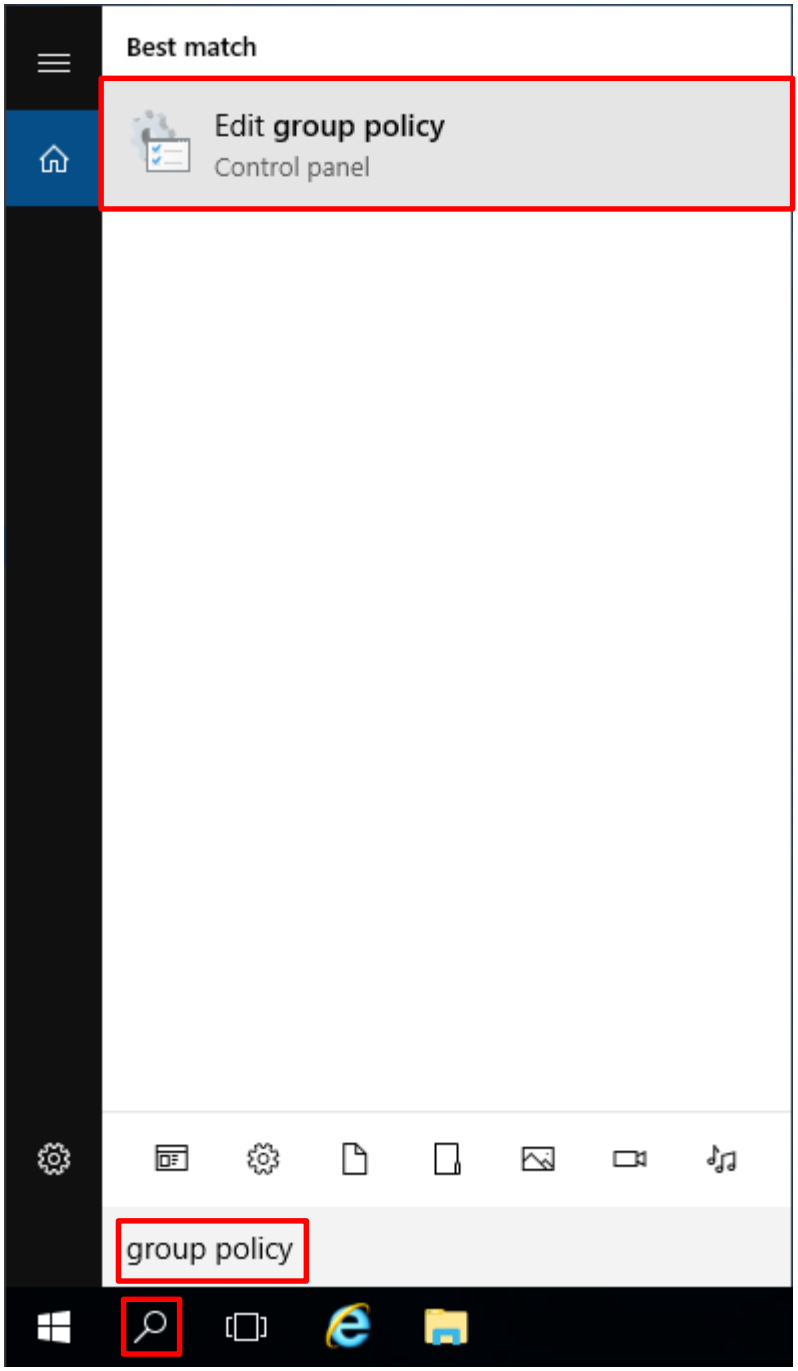
(9) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則



## 5.2 工作群組

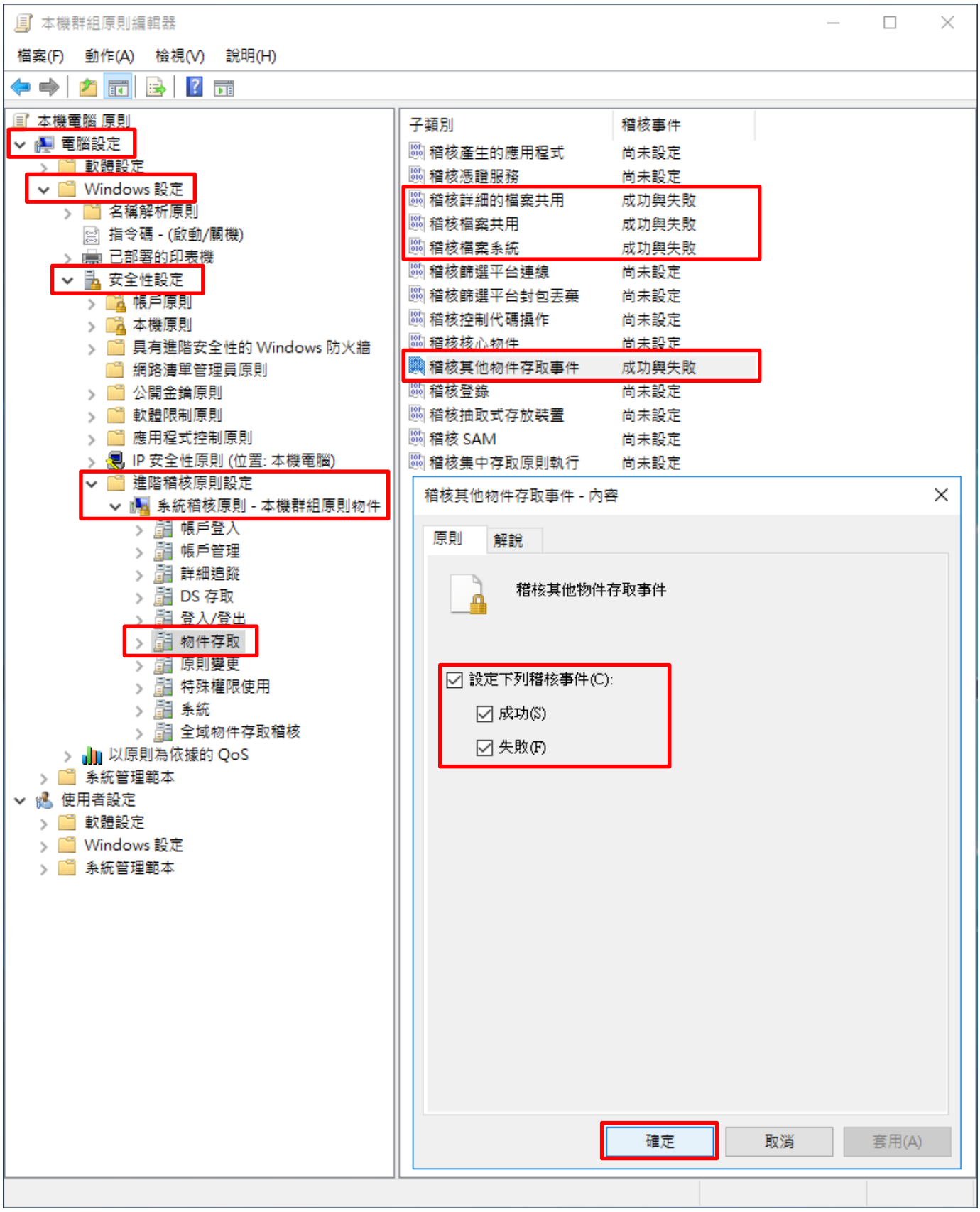
(1) 開啟本機群組原則編輯器

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

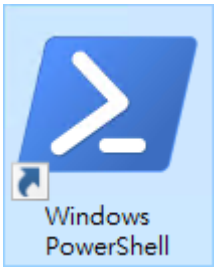


(2) 進階稽核原則：物件存取

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]

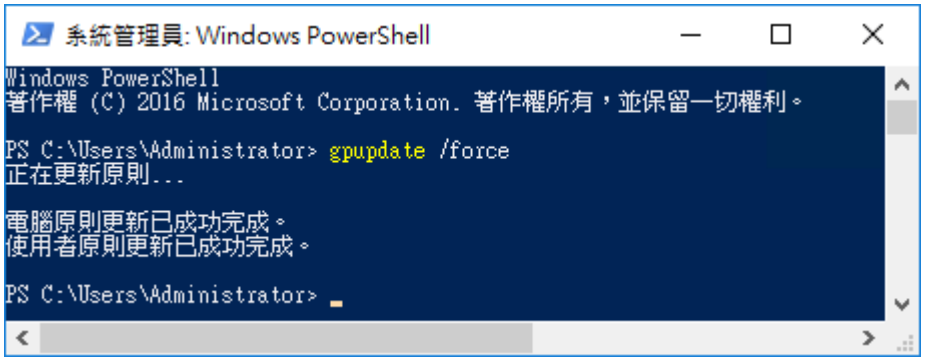


(4) 開啟 [Windows PowerShell]



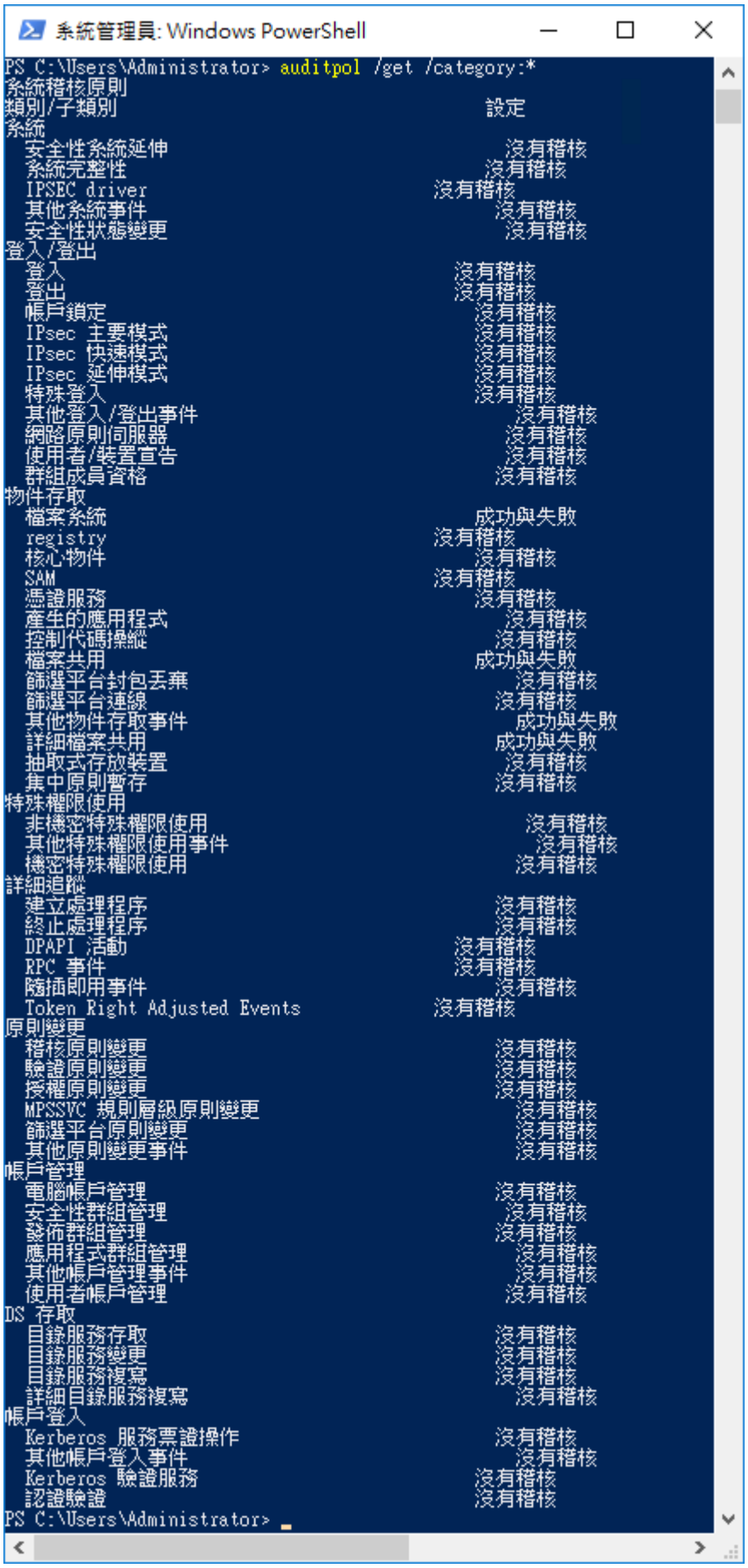

(5) 更新群組原則

PS C: \> gpupdate /force



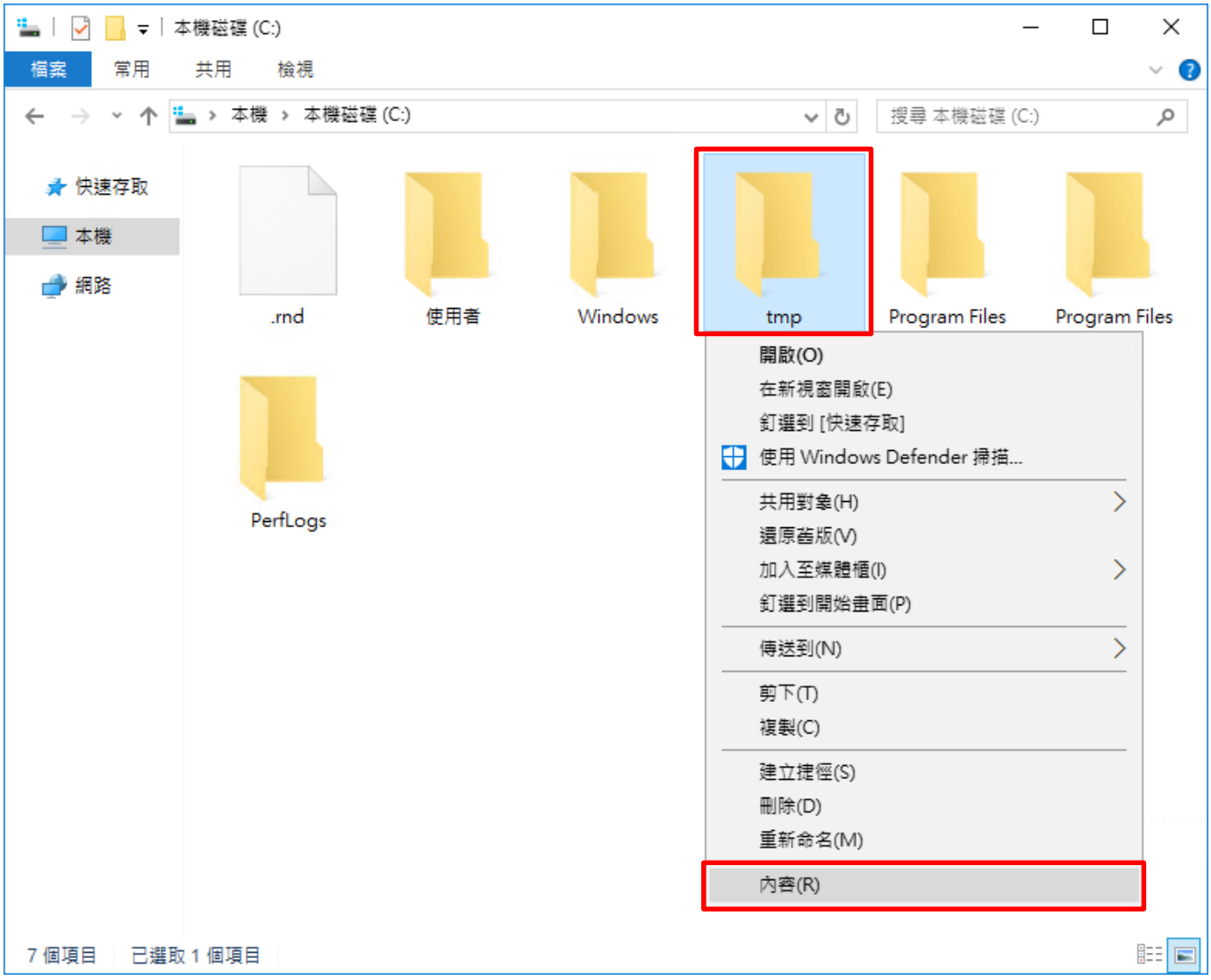
(6) 查看群組原則套用情形

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

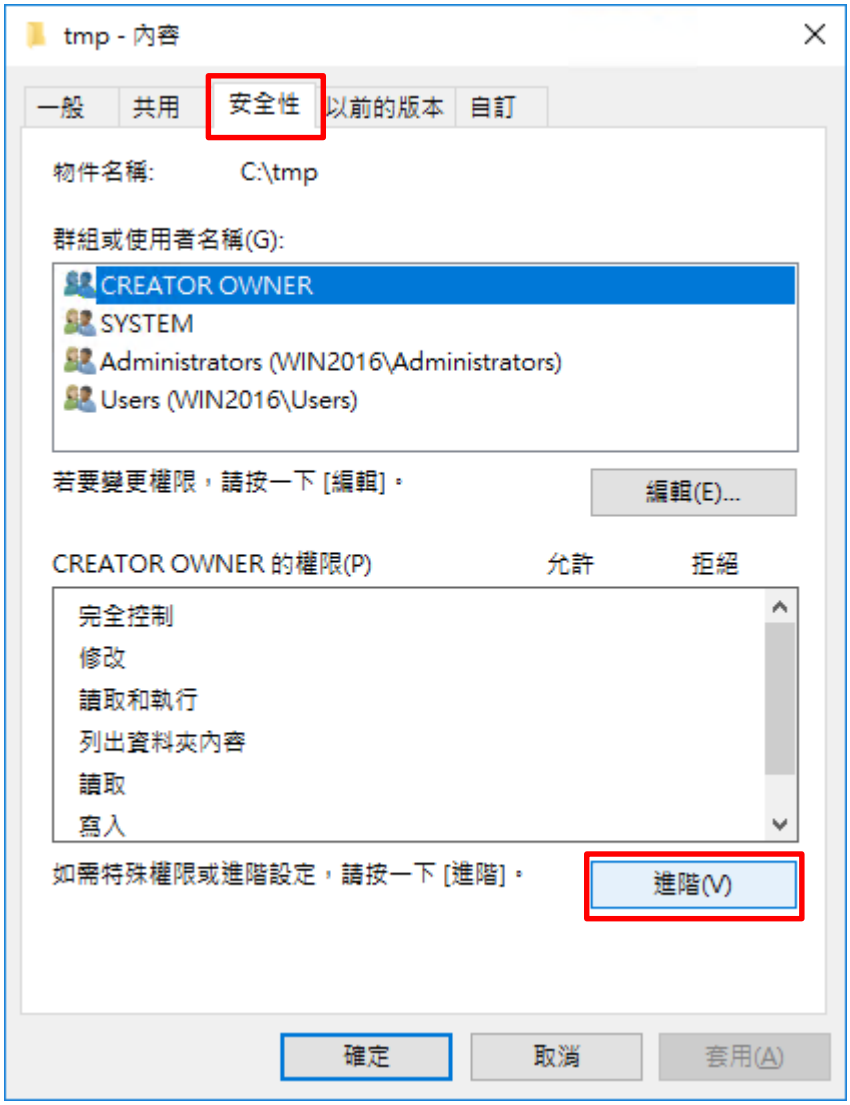


## 5.3 稽核資料夾設定

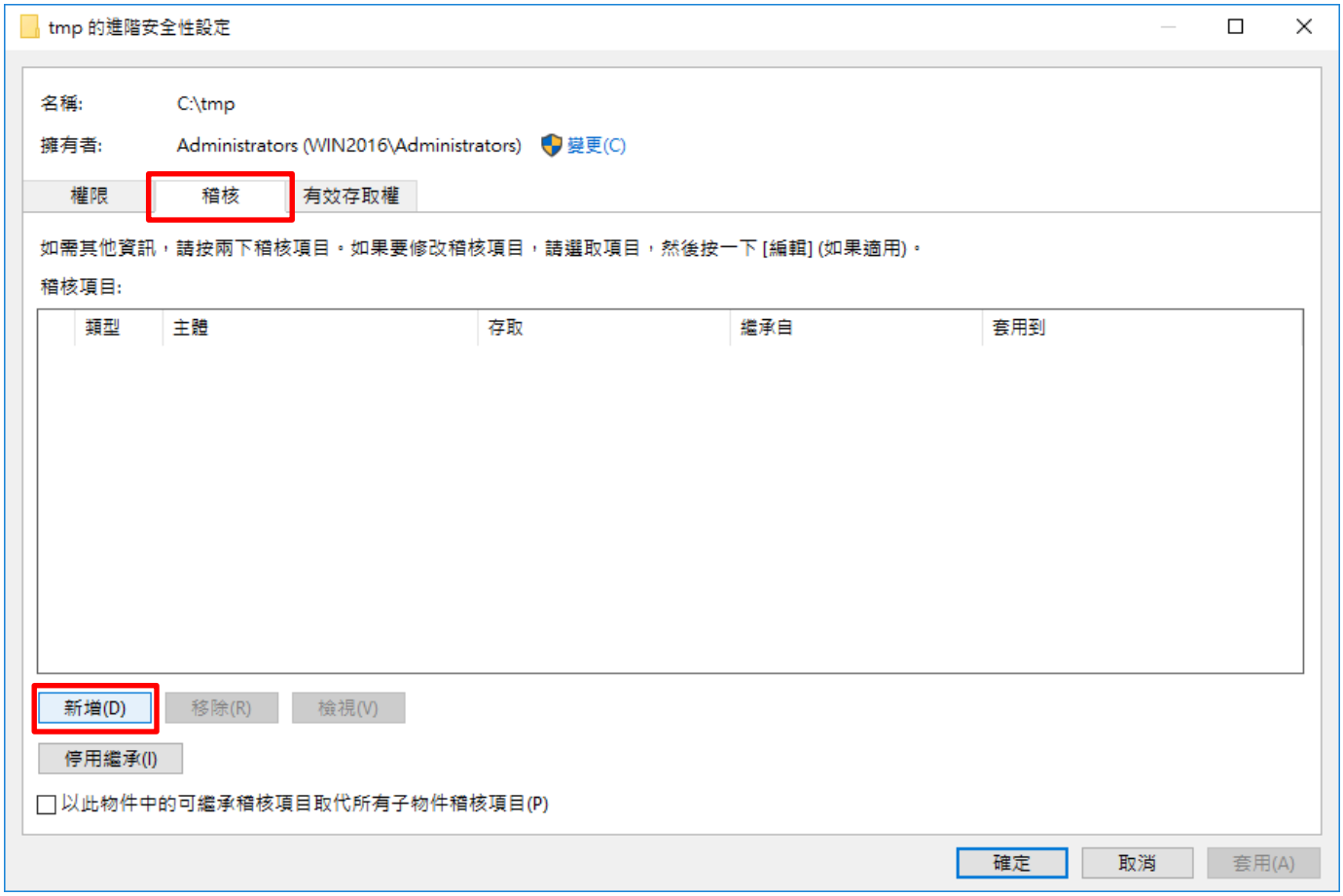
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



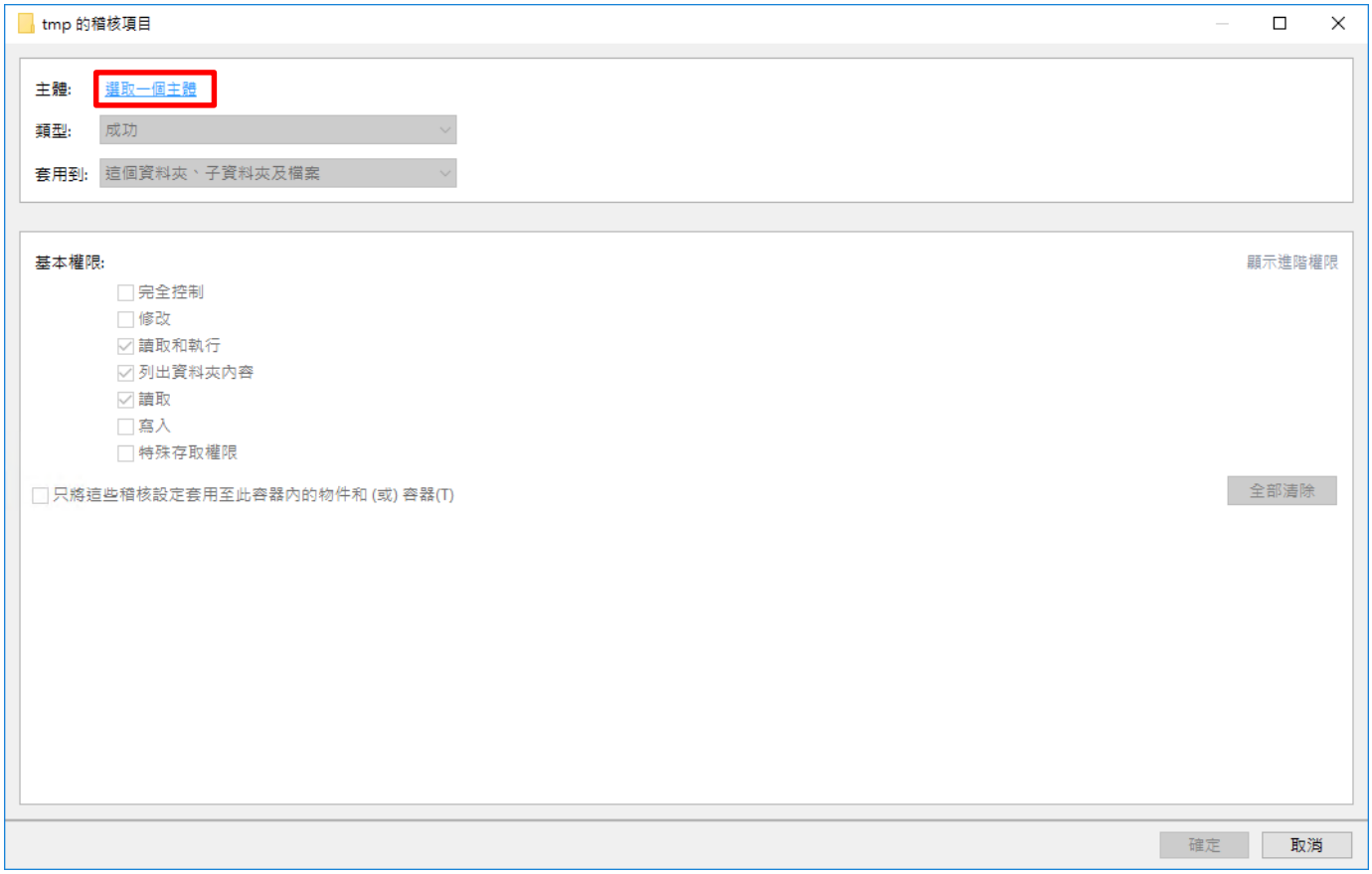
(2) 點選 [安全性] 頁面 -> 按下 [進階]



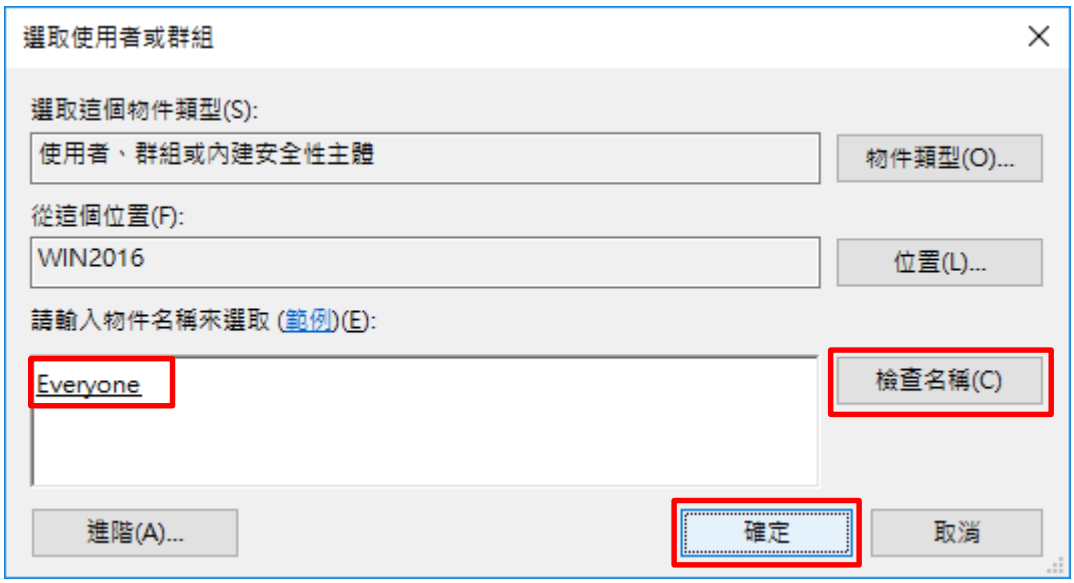
(3) 點選 [稽核] 頁面 -> 按下 [新增]



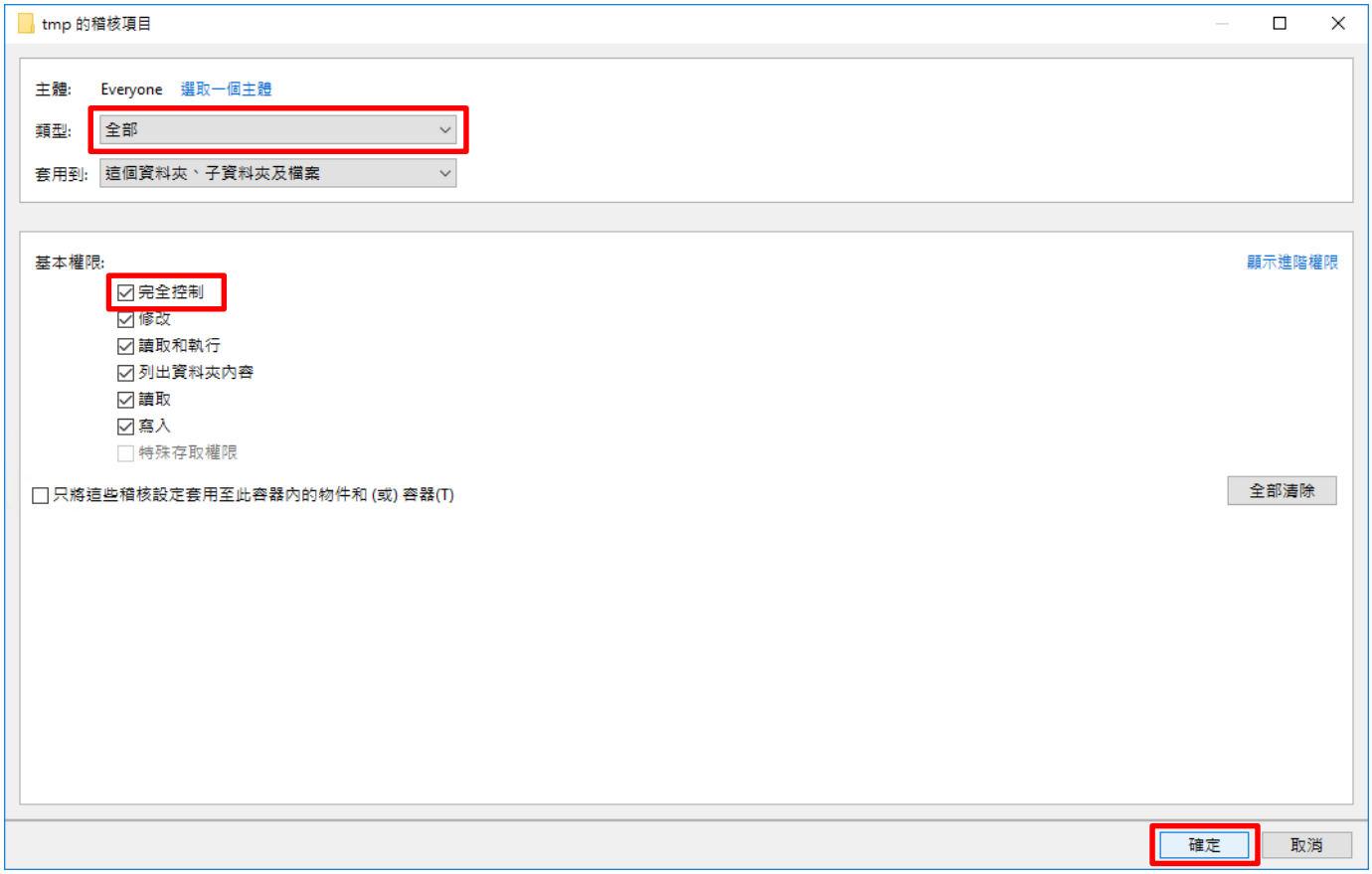
(4) 點選 [選取一個主體]



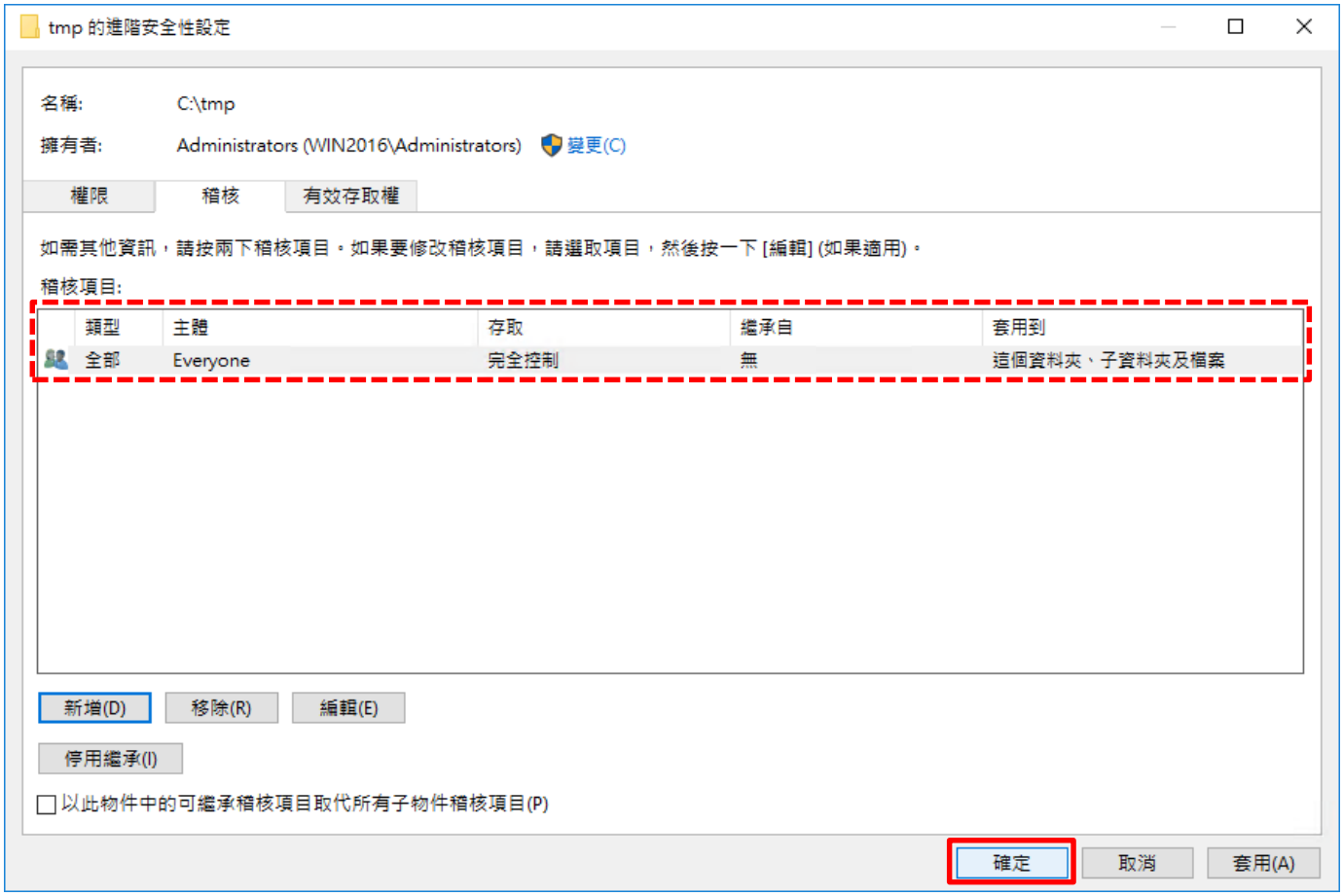

(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按下 [檢查名稱] -> 按下 [確定]



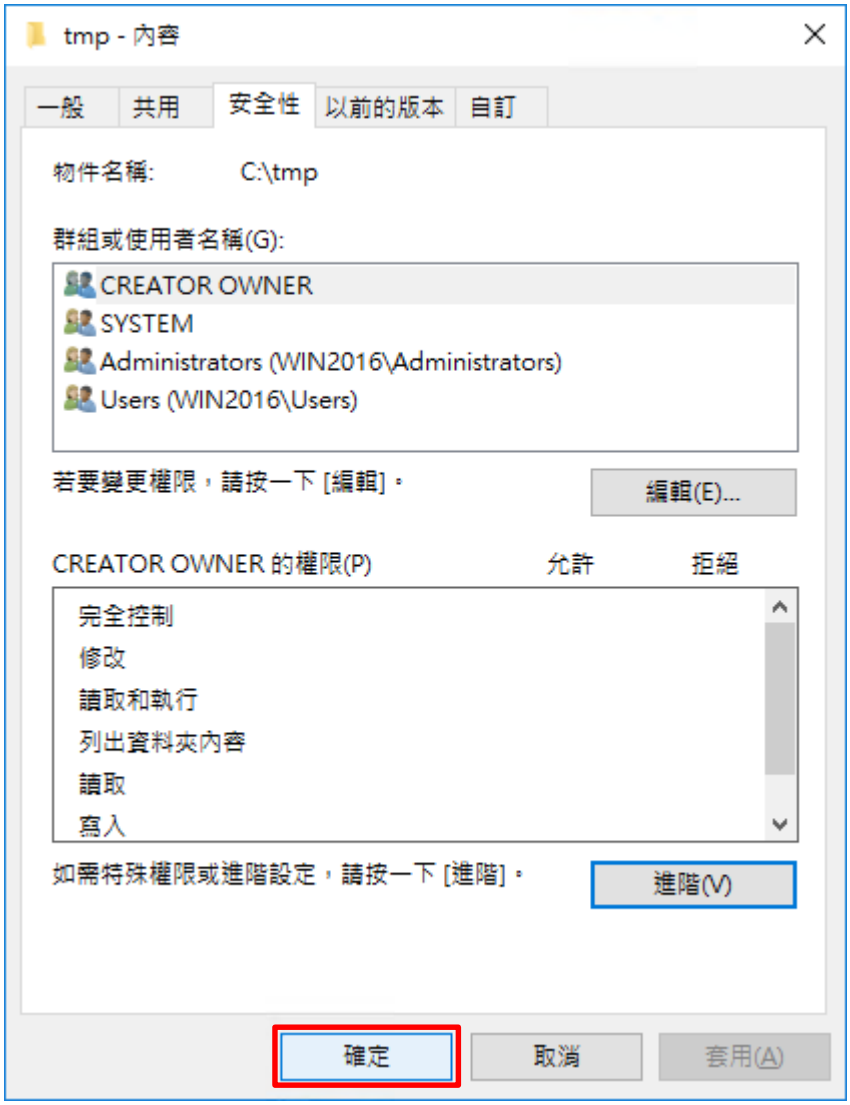
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



(8) 按下 [確定]



# 6. Windows 2019

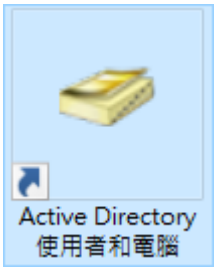
以下分別為網域和工作群組設定方式。

## 6.1 網域

### 6.1.1 組織單位設定

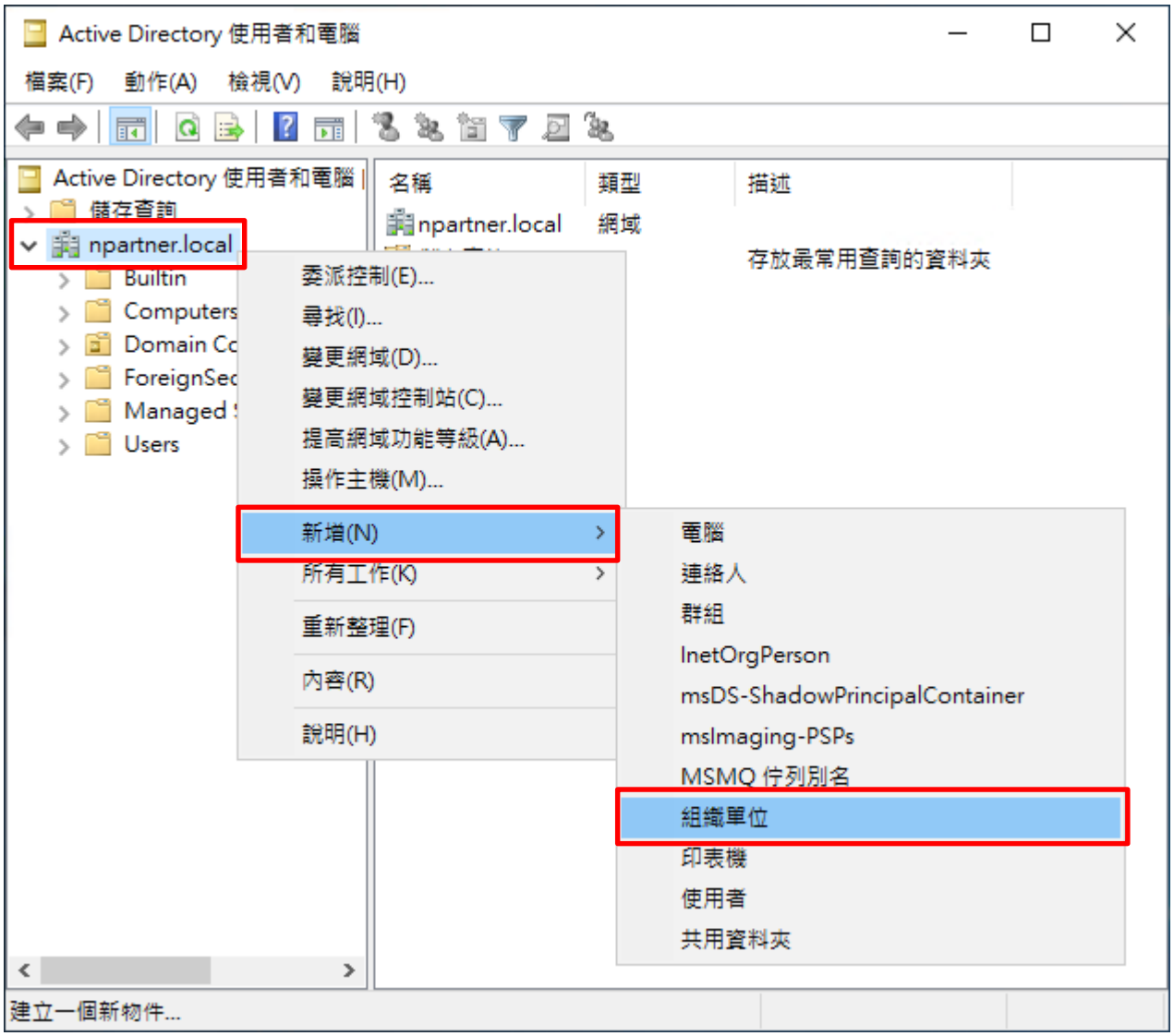
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



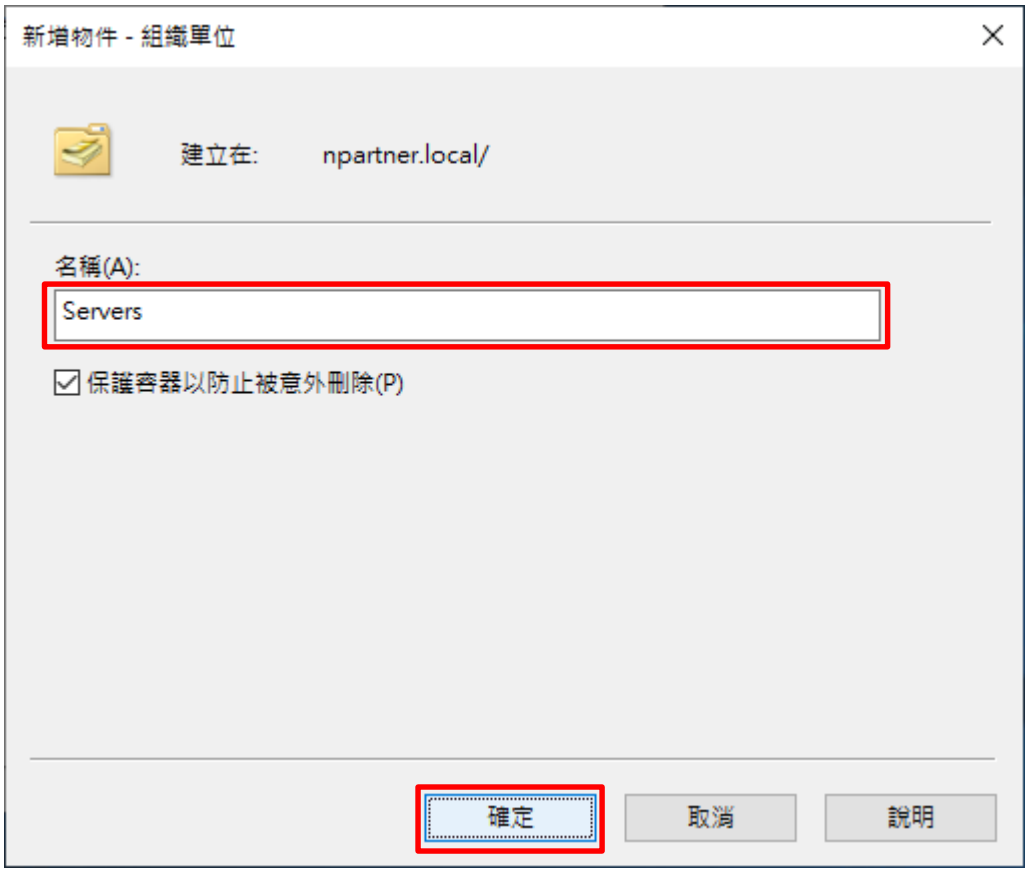
(2) 新增組織單位

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



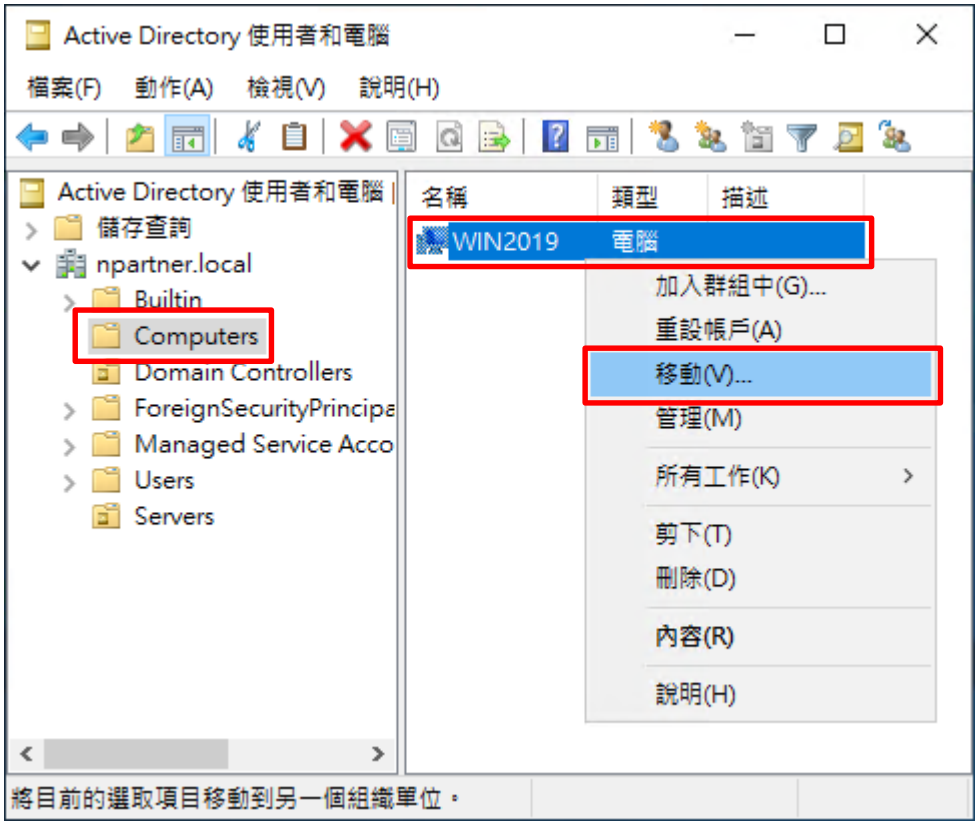
(3) 輸入組織單位名稱

輸入組織單位名稱: Servers -> 按下 [確定]



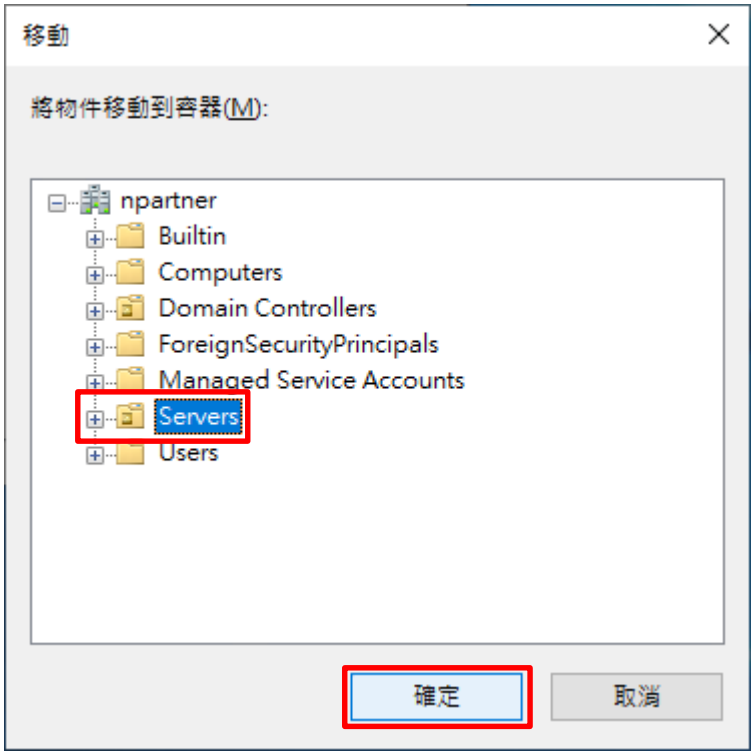

(4) 移動伺服器至新的組織單位

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



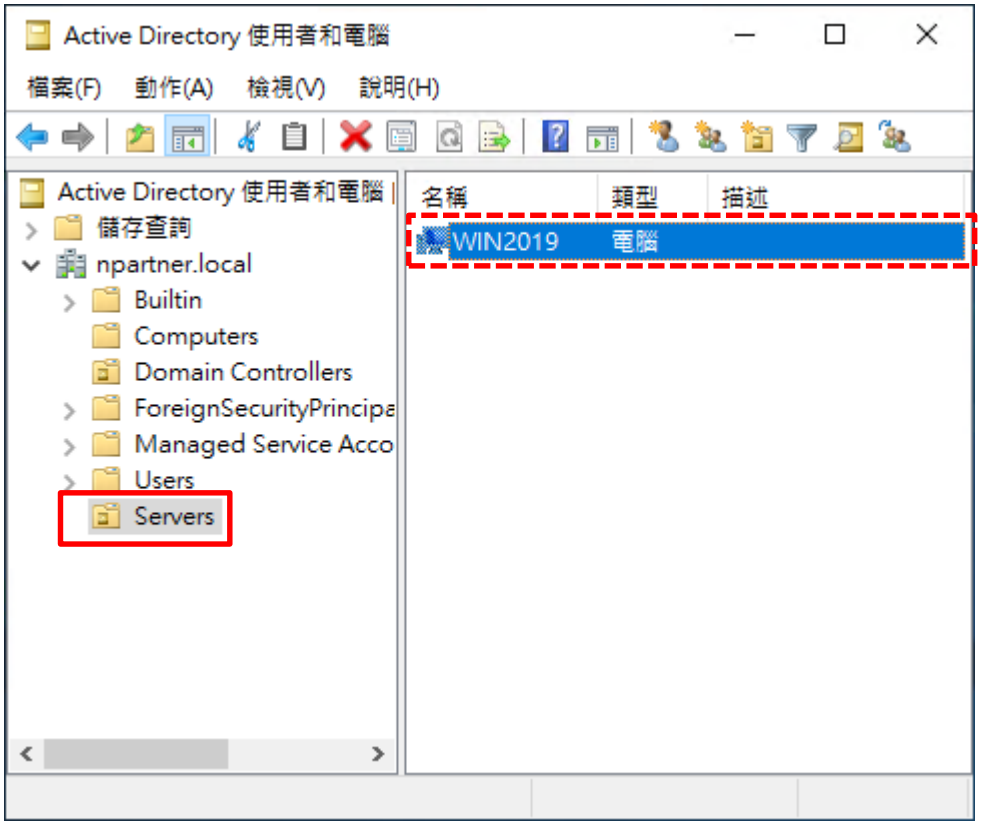
(5) 選擇組織單位

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

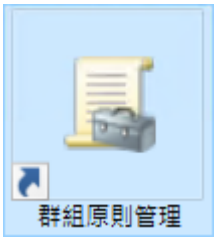
點選 [Servers] 組織單位，確認 [電腦名稱(Win2019)] 伺服器已移動



### 6.1.2 群組原則設定

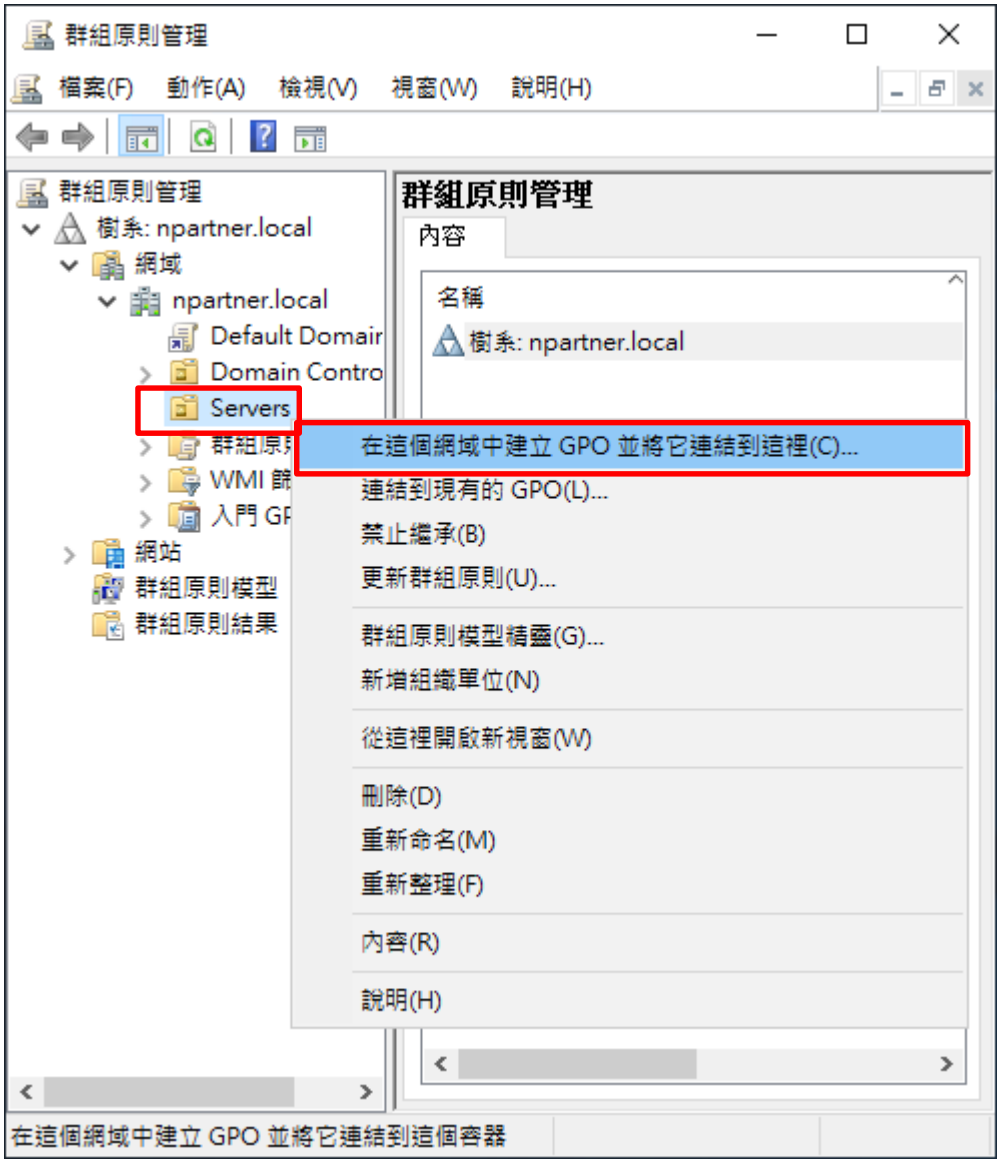
(1) 開啟群組原則管理

開啟 [ Group Policy Management(群組原則管理) ]



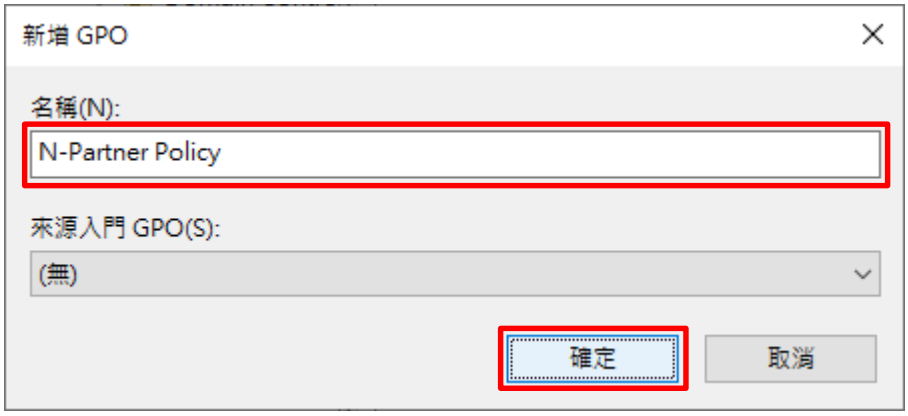

(2) 在 Servers 組織單位，新增群組原則物件

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...]



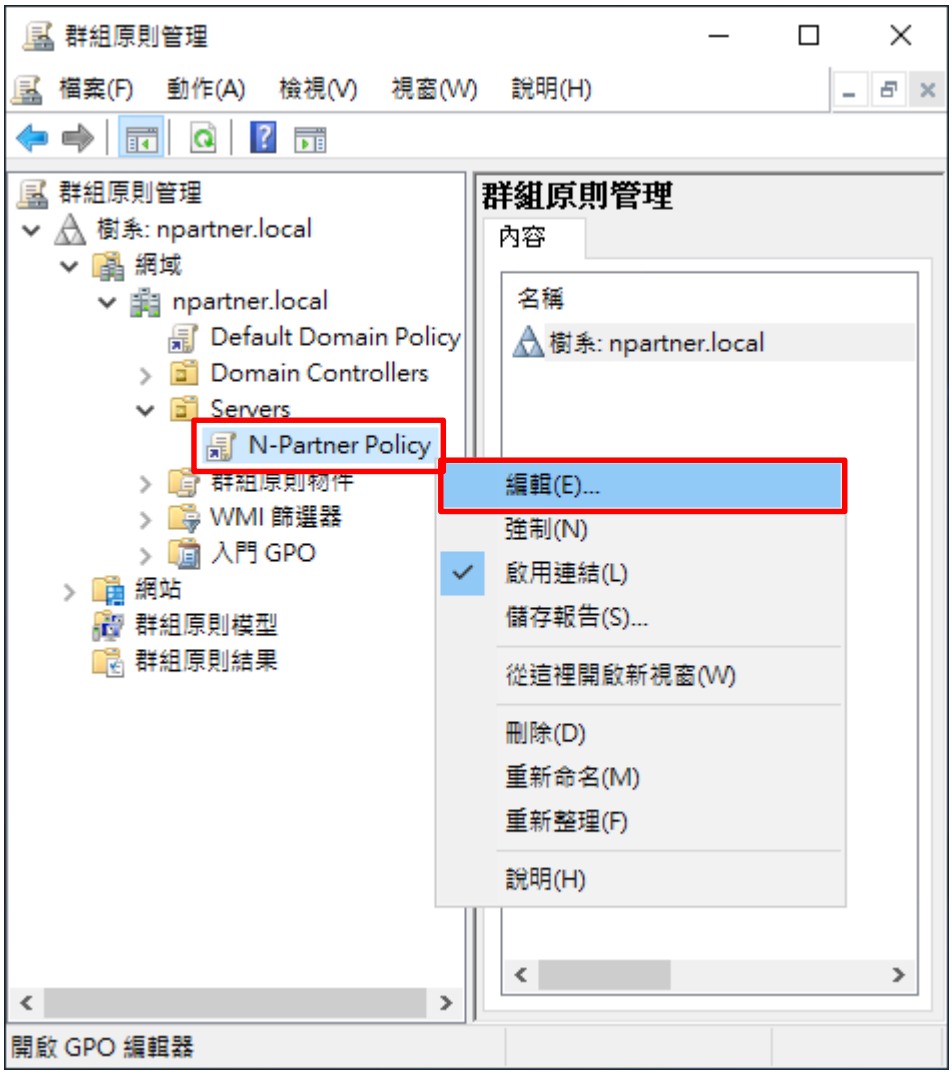
(3) 輸入群組原則物件名稱

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



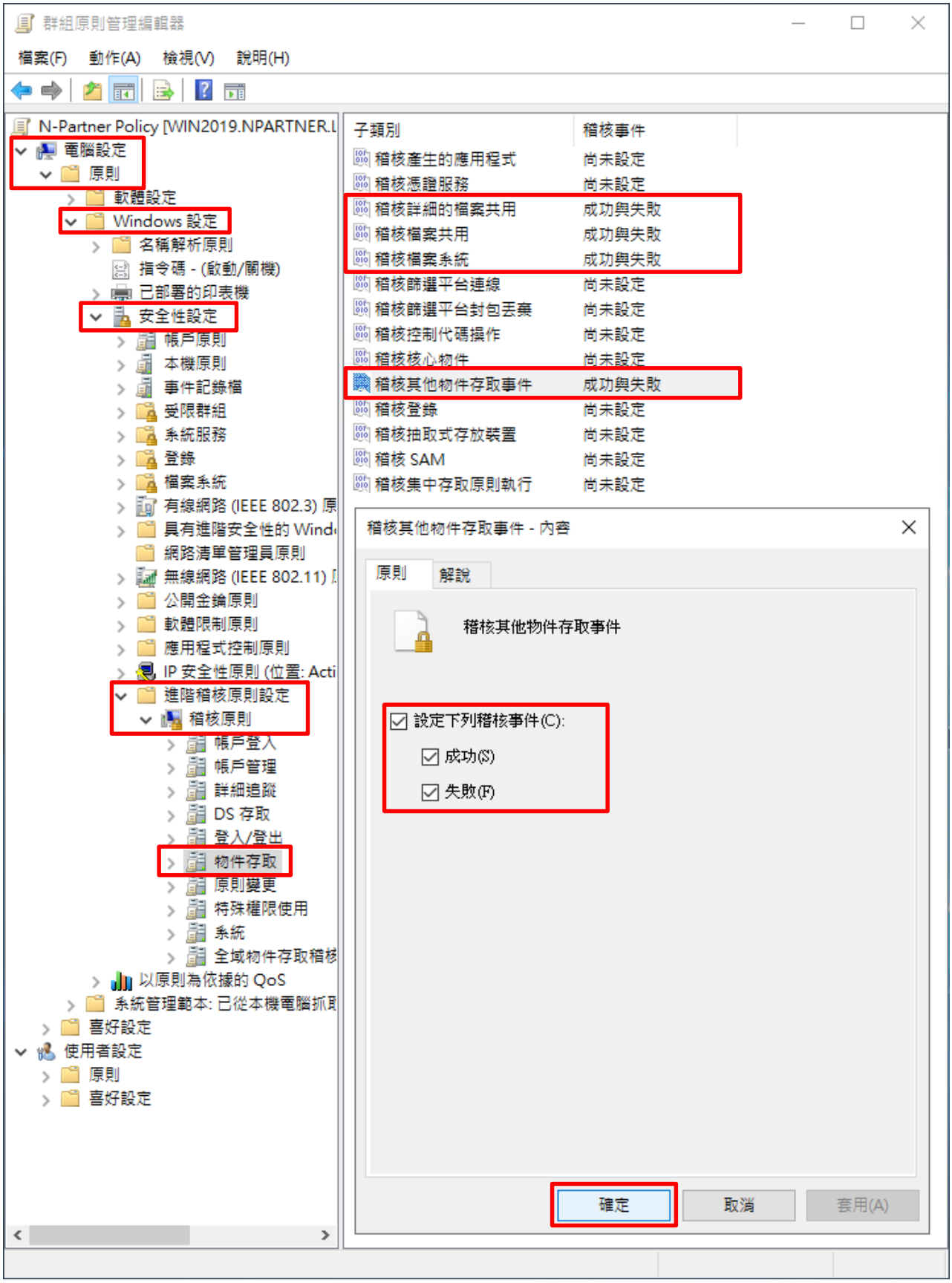

(4) 編輯群組原則物件

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



(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]

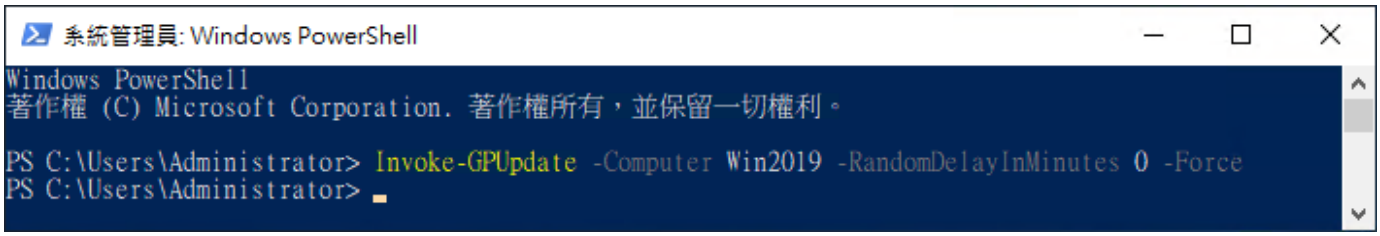


(6) 在 AD 網域伺服器，開啟 Windows PowerShell

開啟 [Windows PowerShell]


(7) 更新 Windows File 伺服器群組原則

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

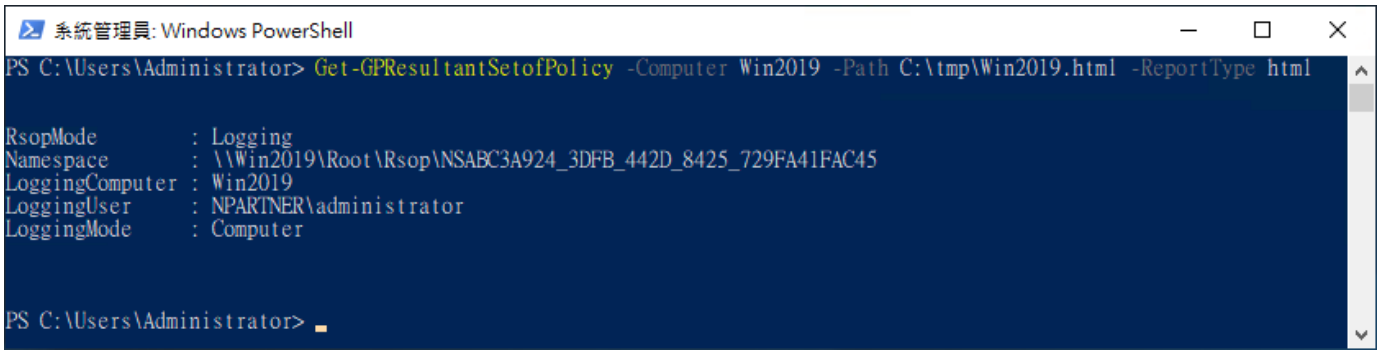



紅色文字部位請輸入 Windows File 伺服器名稱

Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force

(8) 產生 Windows File 伺服器群組原則報表

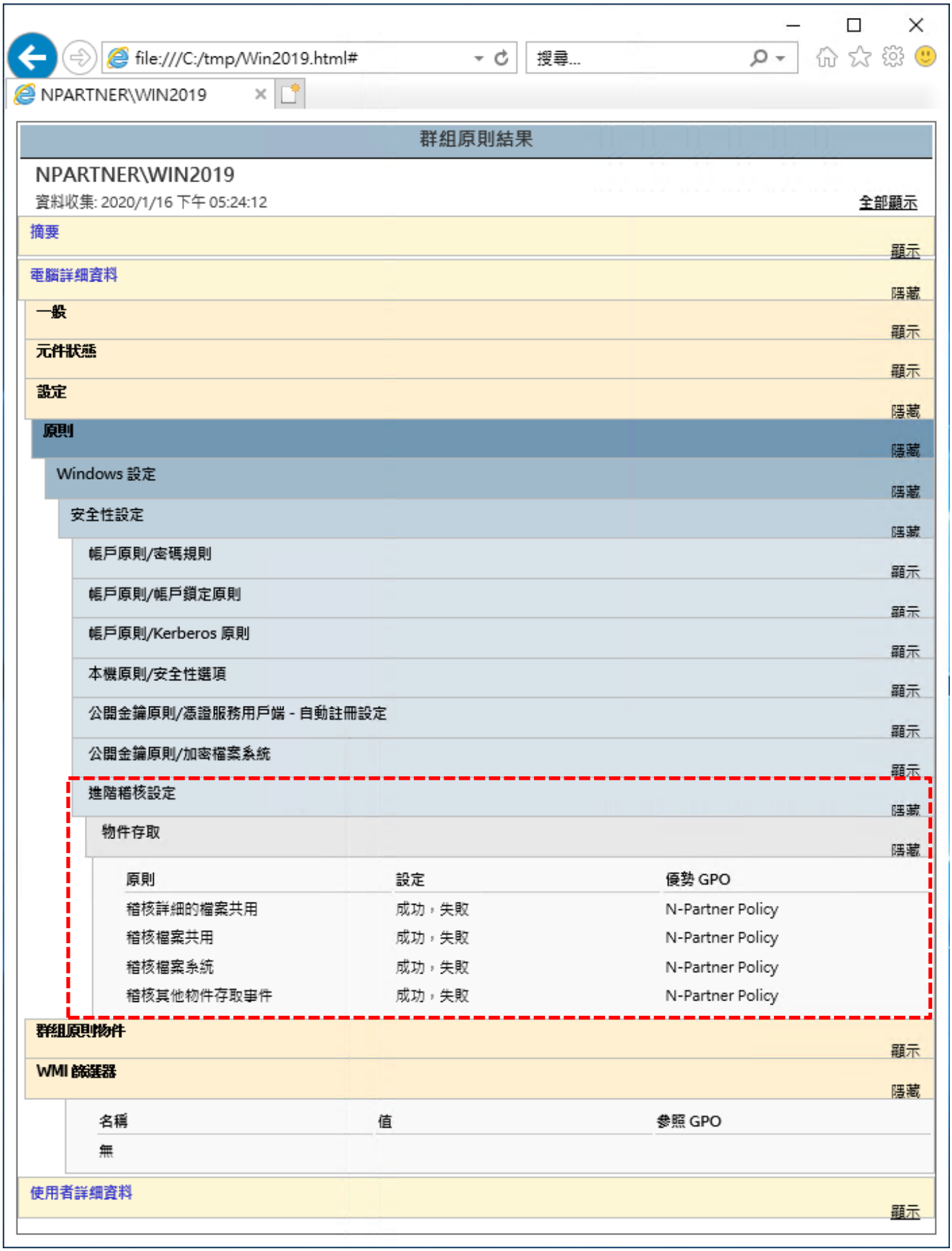
PS C:\> Get-GPResultantSetofPolicy -Computer Win2019 -Path C:\tmp\Win2019.html -ReportType html




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

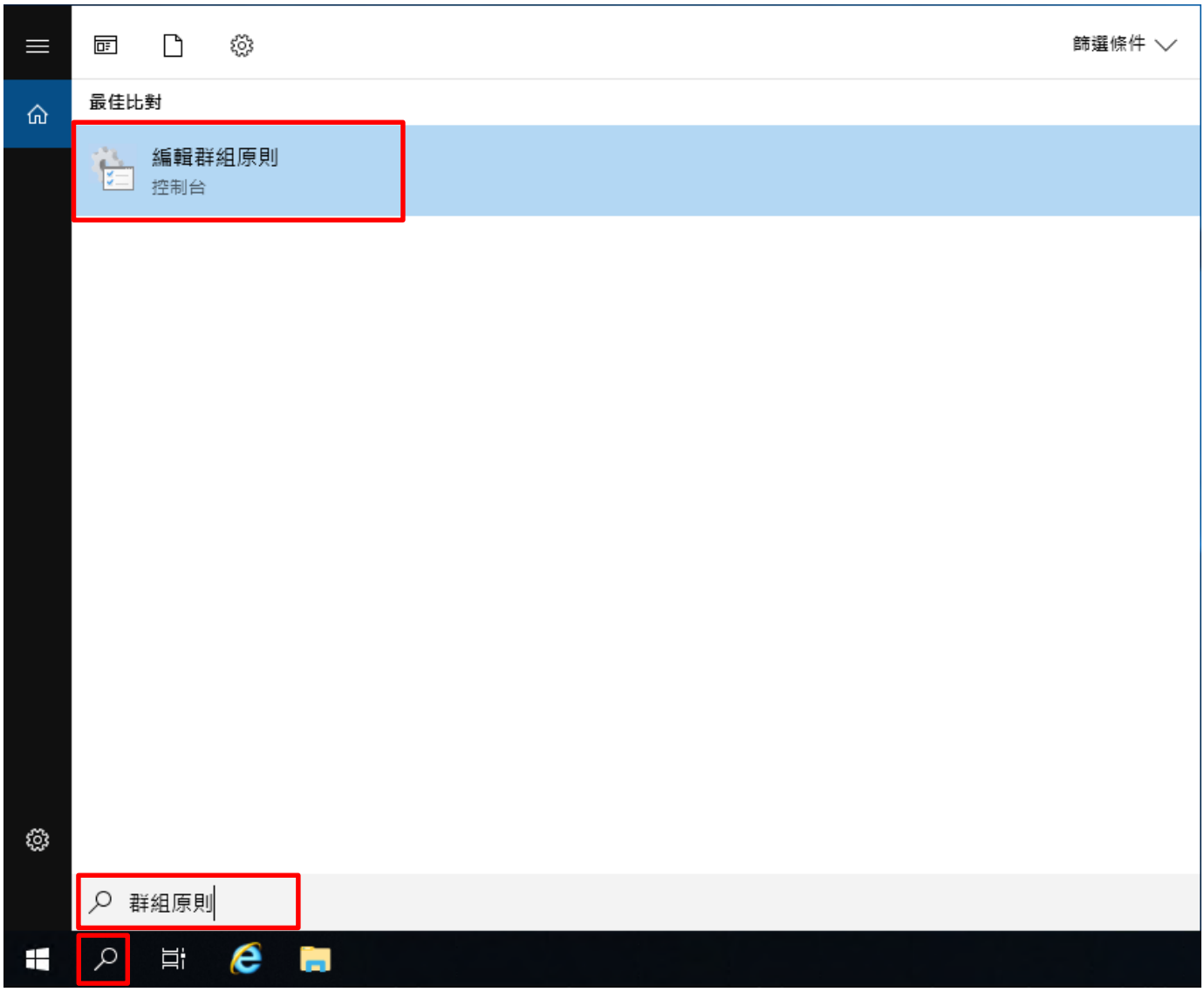
(9) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則



## 6.2 工作群組

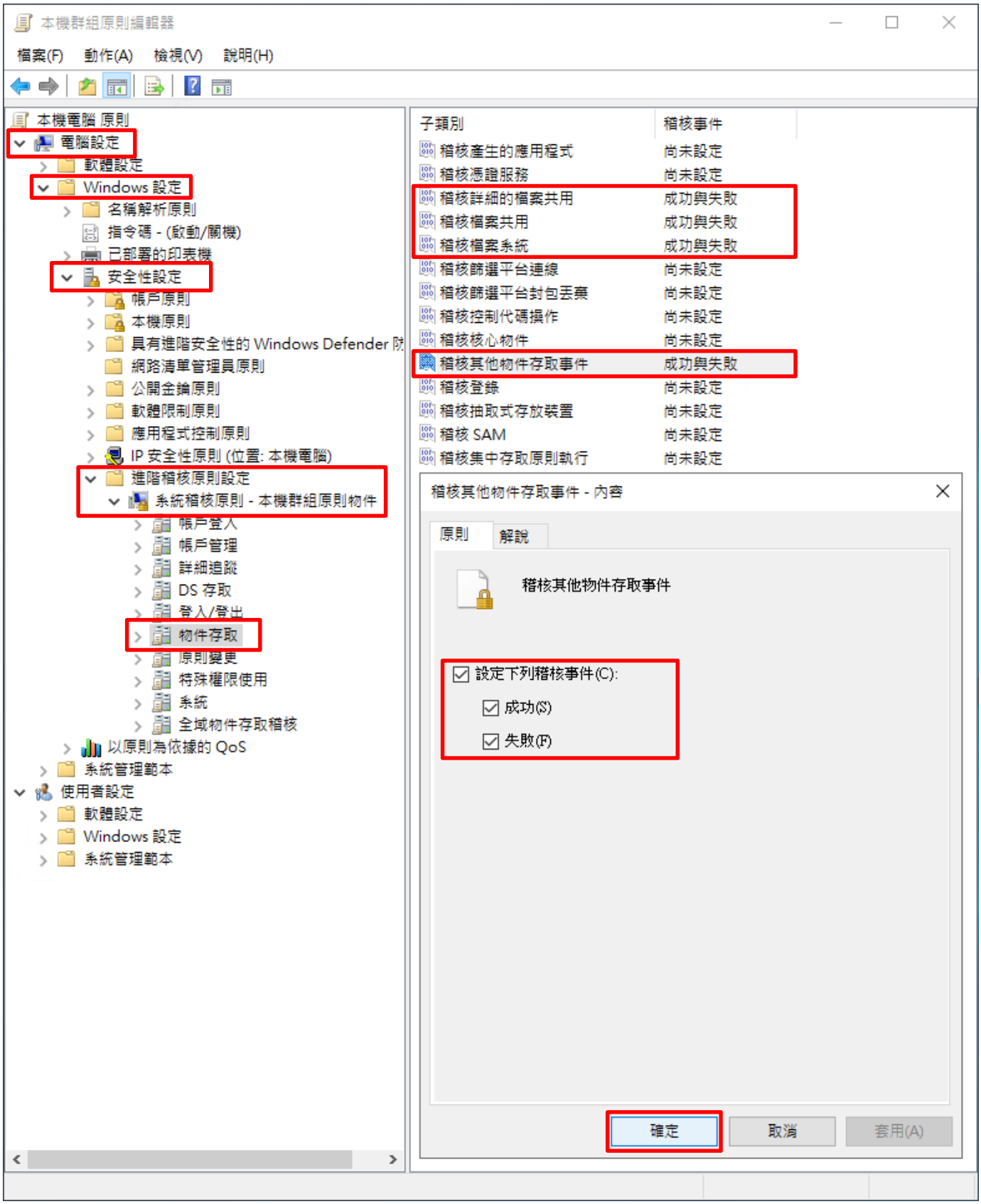
(1) 開啟本機群組原則編輯器

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]



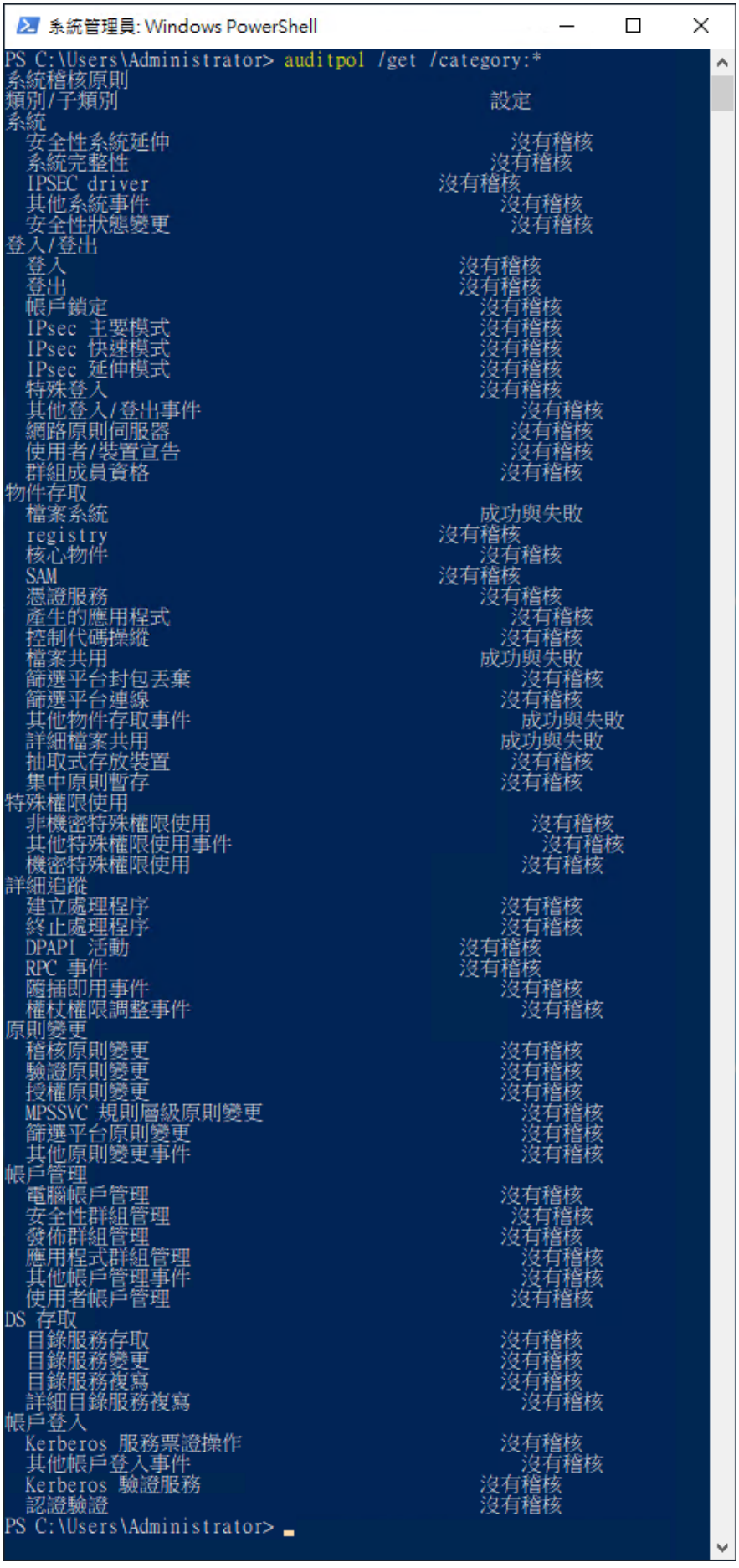
(4) 開啟 [Windows PowerShell]


(5) 更新群組原則

PS C: \> gpupdate /force

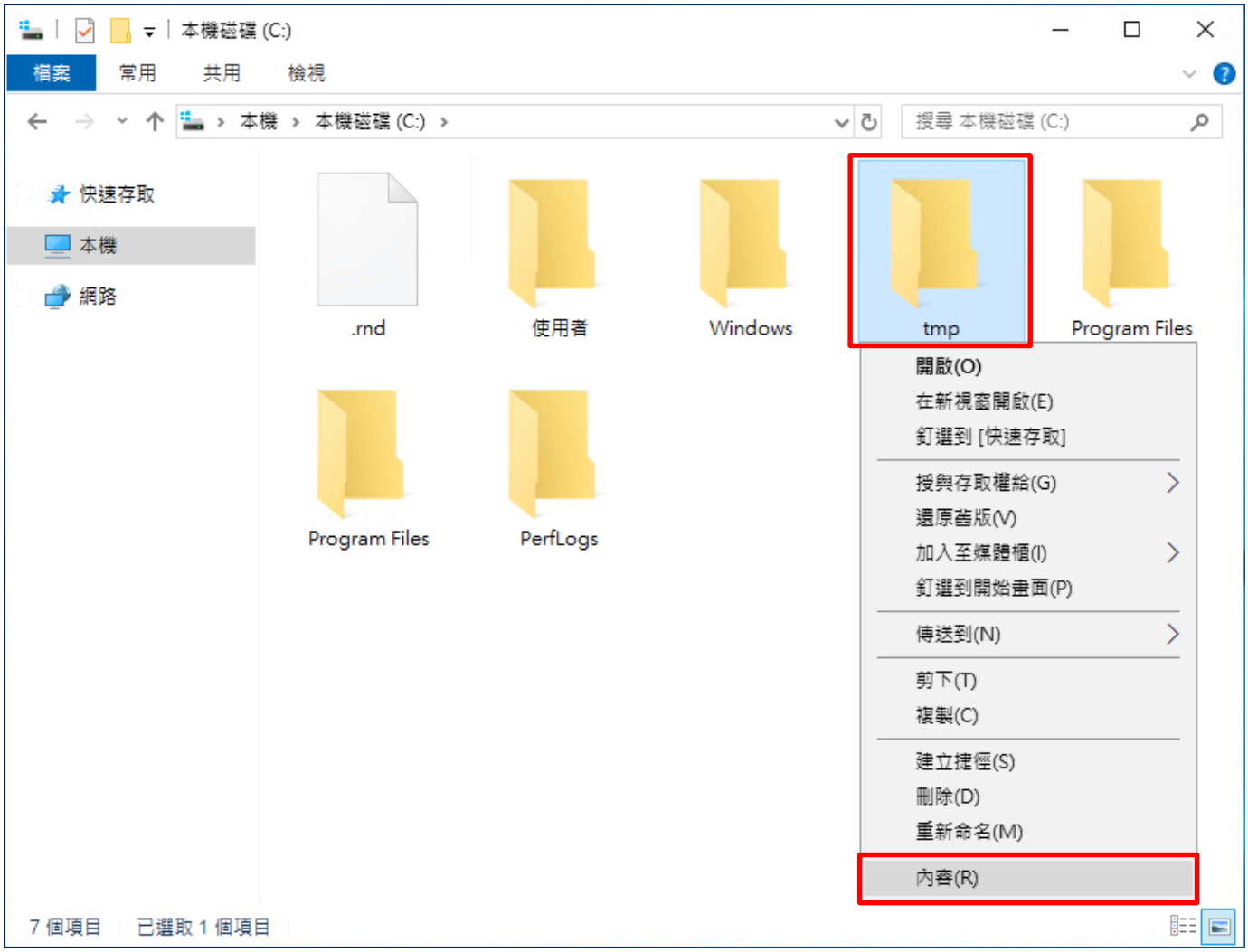
(6) 查看群組原則套用情形

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

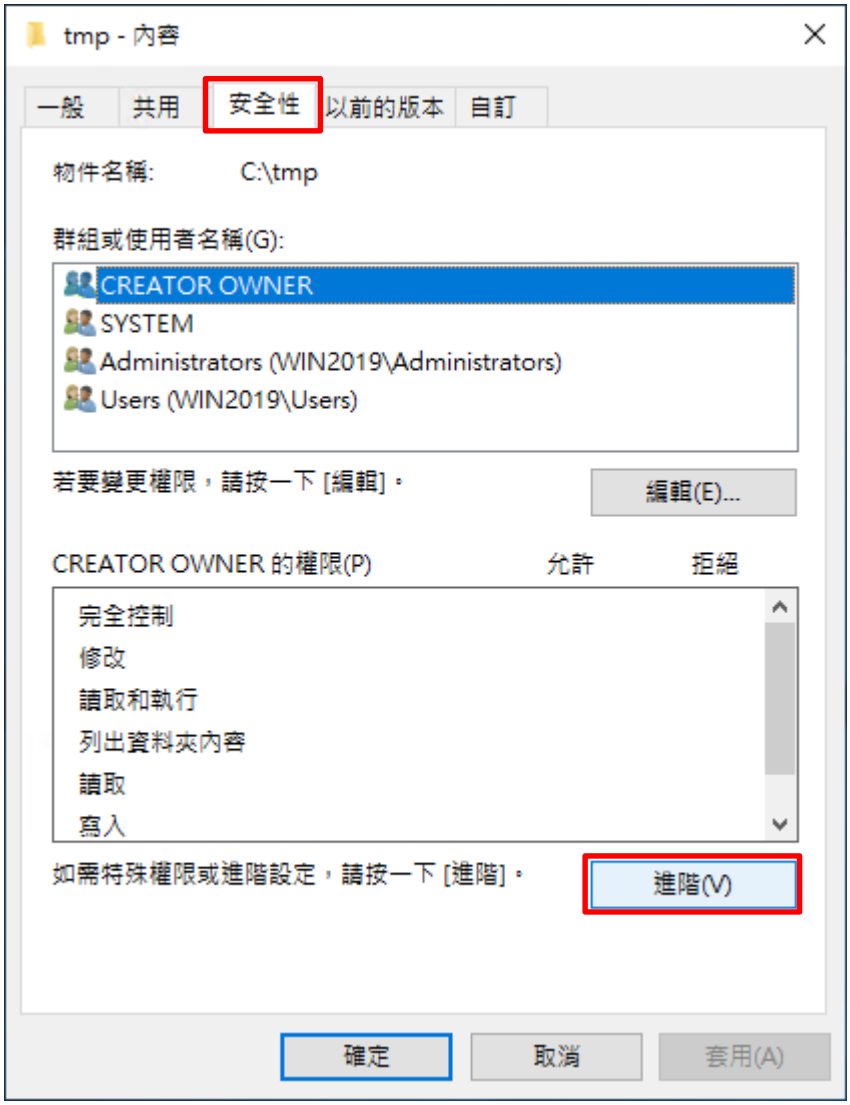


## 6.3 稽核資料夾設定

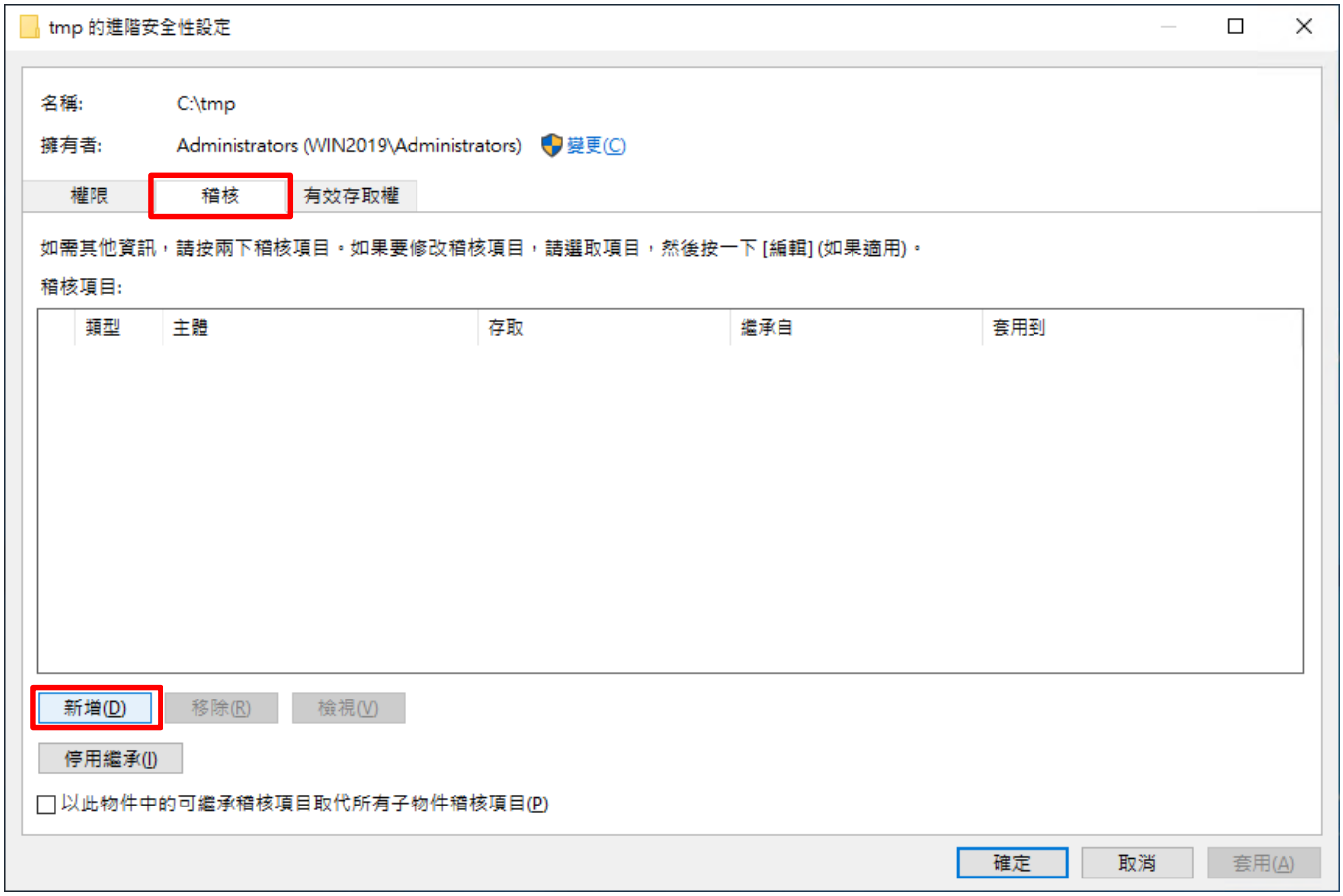
(1) 在 [資料夾] 按滑鼠右鍵 -> 選擇 [內容]



(2) 點選 [安全性] 頁面 -> 按下 [進階]



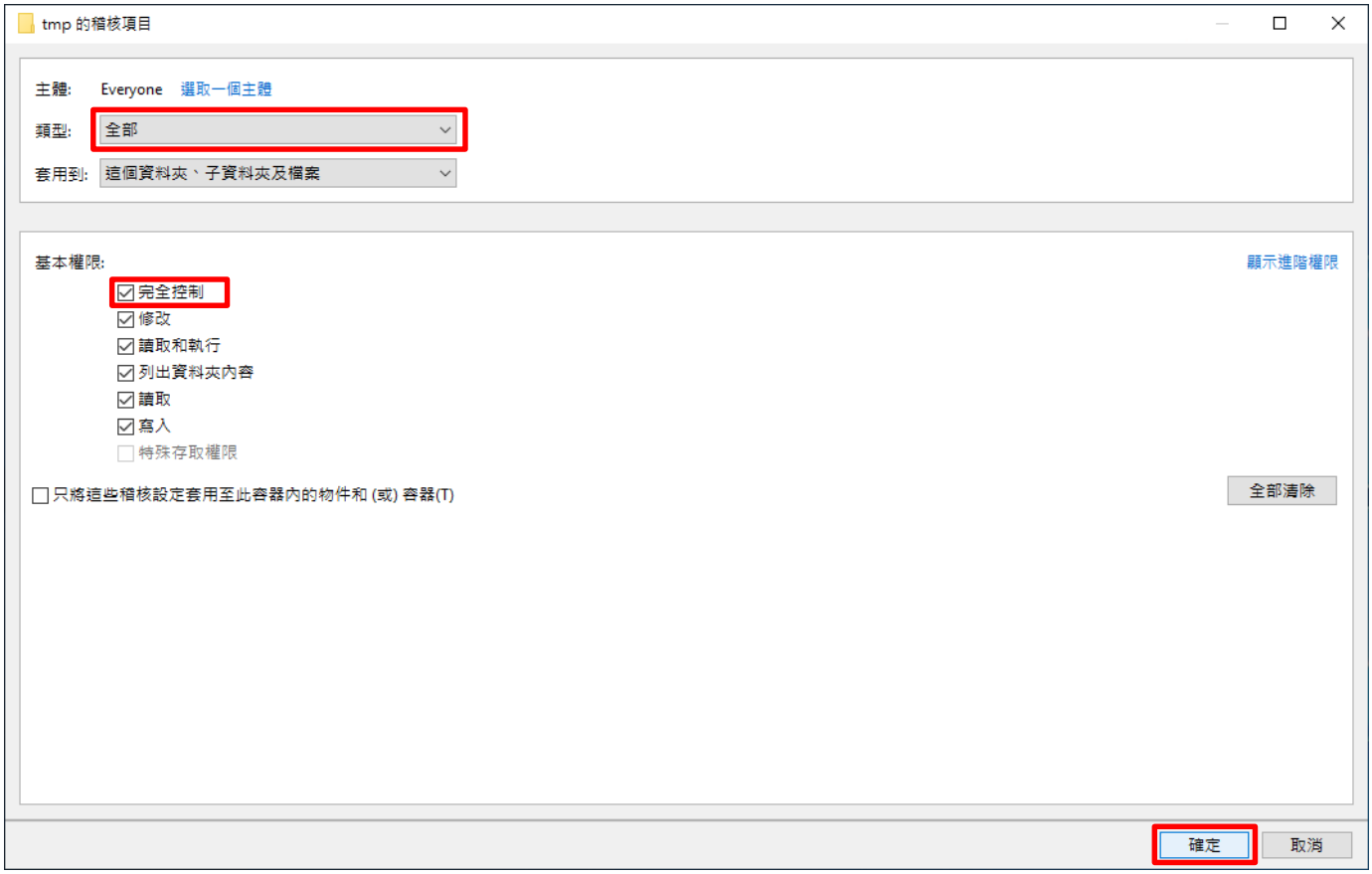
(3) 點選 [稽核] 頁面 -> 按下 [新增]



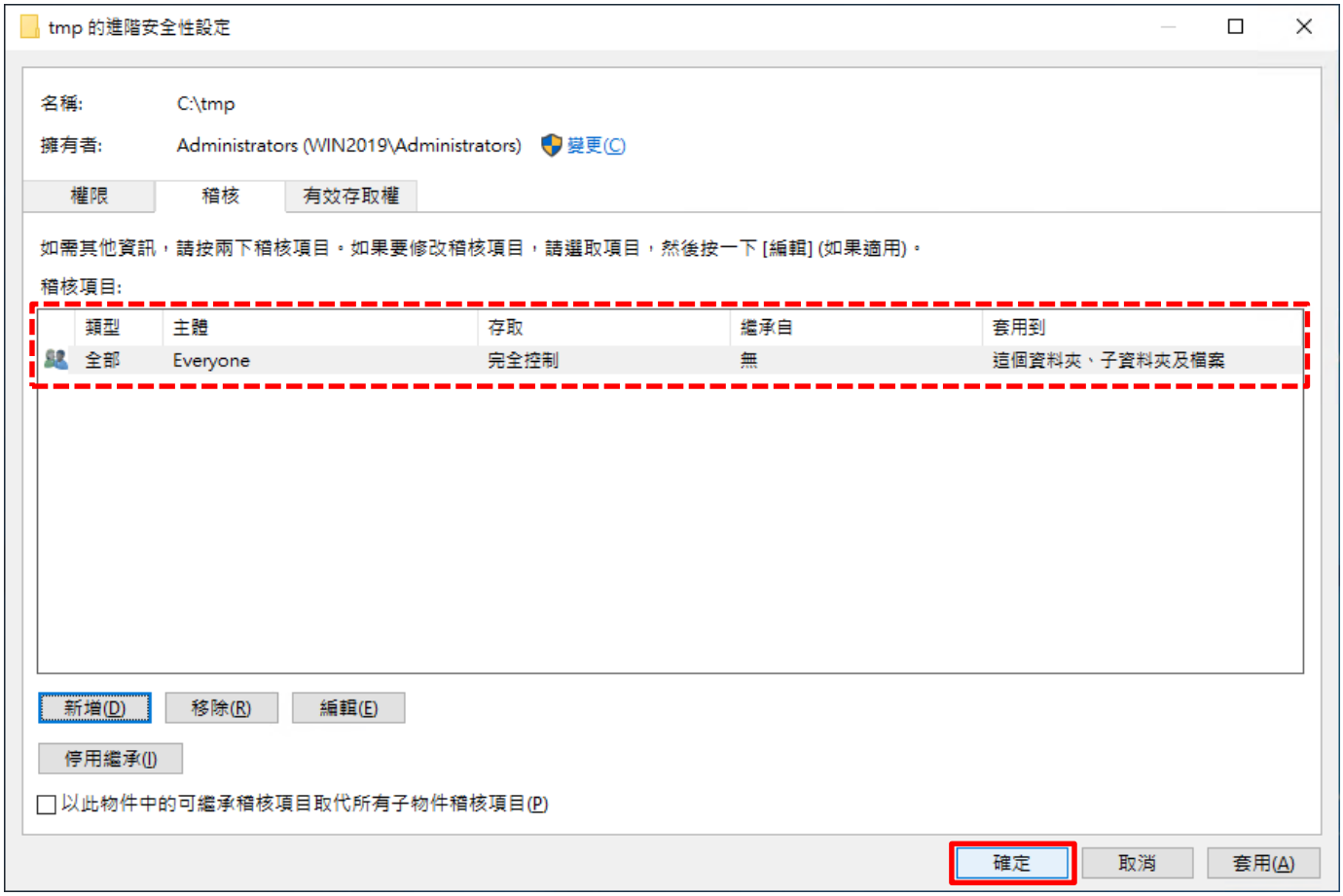
(4) 點選 [選取一個主體]


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

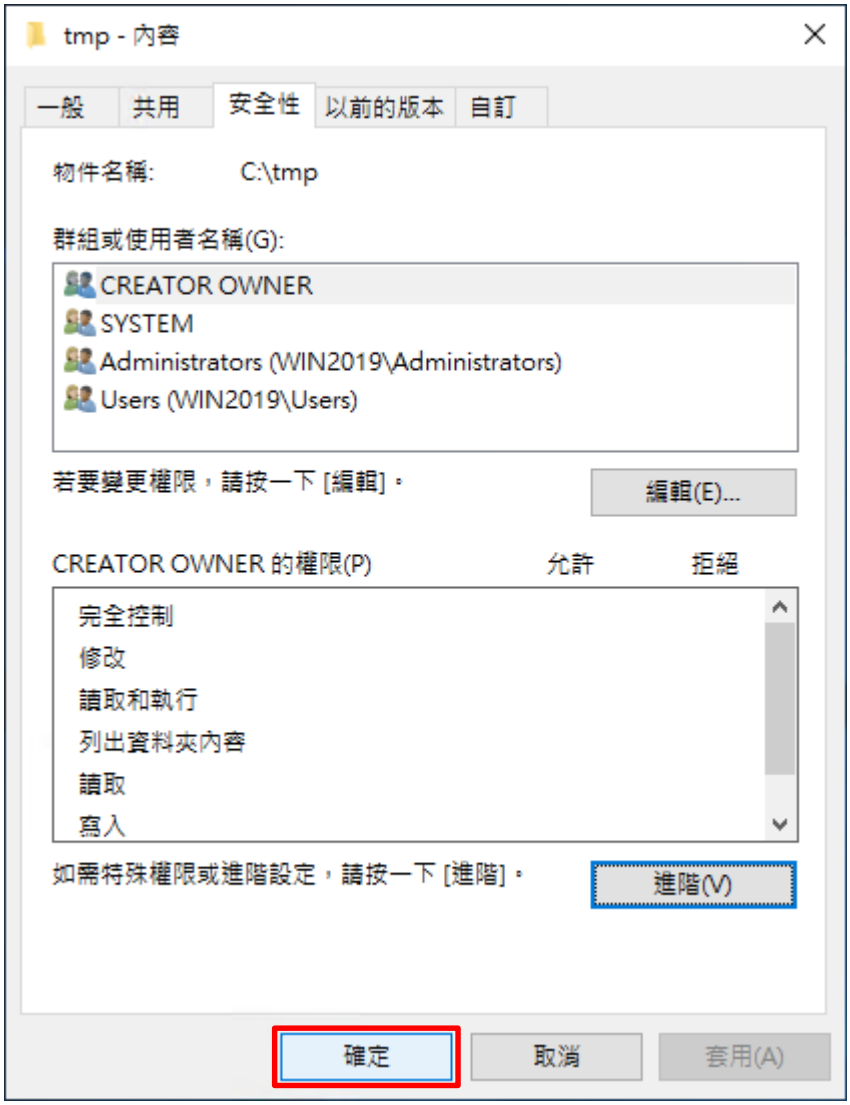
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按下 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按下 [確定]



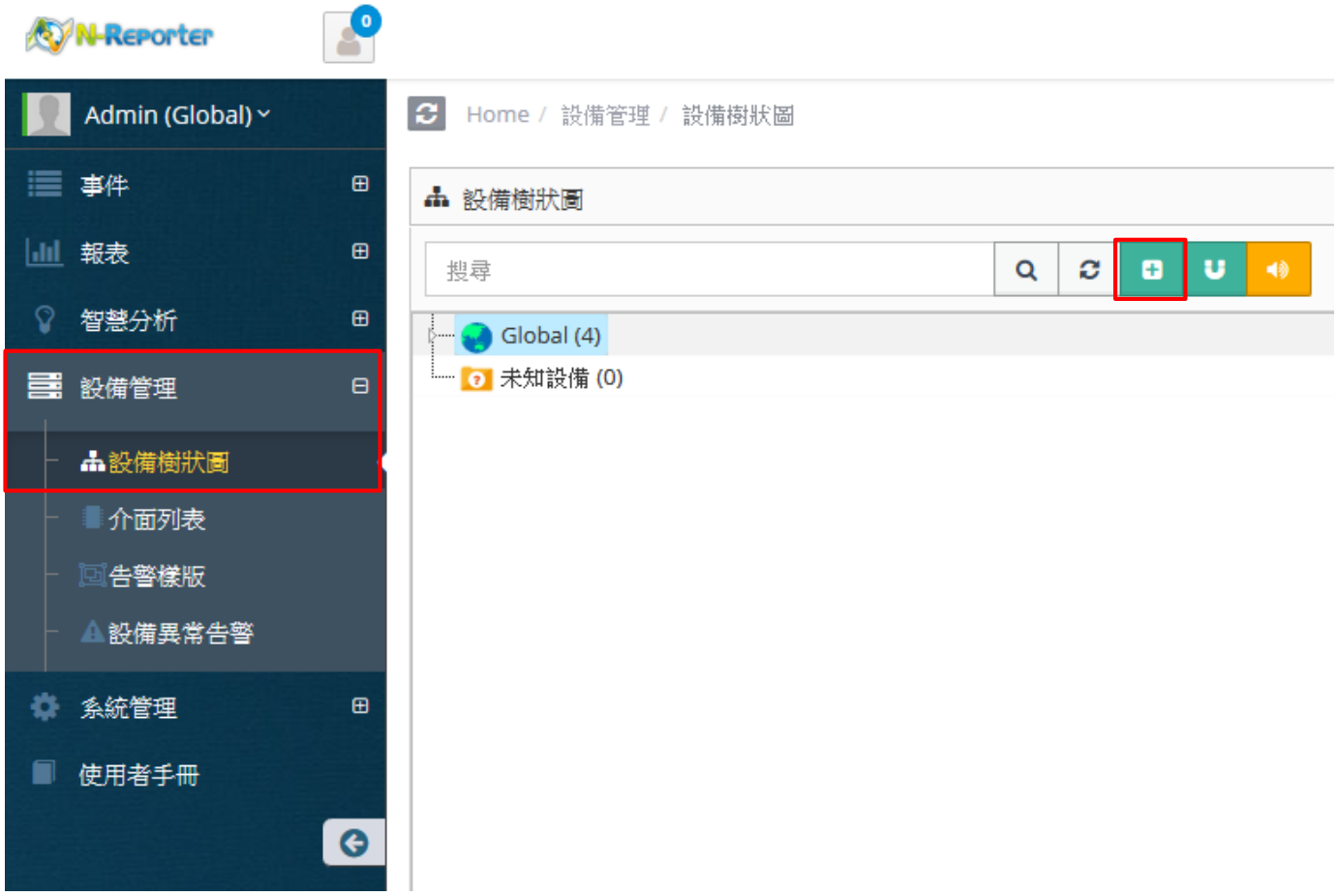
(8) 按下 [確定]



# 7. N-Reporter

(1) 新增 Windows File 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



## 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]

## 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]

## 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

業 務 相 關 請 洽 :

Email: sales@npartnertech.com