

# Partner

如何設定

Windows File 事件記錄

V007

2022/03/17



## 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. Windows 2016 .....	104
1. NXLog .....	3	6.1 網域 .....	104
1.1 NXLog 安裝 .....	3	6.1.1 組織單位設定 .....	104
1.2 NXLog 設定檔下載 .....	5	6.1.2 群組原則設定 .....	109
1.2.1 Windows 2003 或之前版本作業系統 .....	5	6.2 工作群組 .....	116
1.2.2 Windows 2008 或之後版本作業系統 .....	6	6.2.1 稽核原則設定 .....	116
1.3 NXLog 設定檔 .....	7	6.2.2 事件檔案設定 .....	120
1.3.1 Windows 2003 或之前版本作業系統 .....	7	6.3 稽核資料夾設定 .....	123
1.3.2 Windows 2008 或之後版本作業系統 .....	8	7. Windows 2019 .....	130
1.4 NXLog 啟動服務 .....	9	7.1 網域 .....	130
1.4.1 Windows 2003 或之前版本作業系統 .....	9	7.1.1 組織單位設定 .....	130
1.4.2 Windows 2008 或之後版本作業系統 .....	12	7.1.2 群組原則設定 .....	135
2. Windows 2000 .....	15	7.2 工作群組 .....	142
2.1 網域 .....	15	7.2.1 稽核原則設定 .....	142
2.1.1 組織單位設定 .....	15	7.2.2 事件檔案設定 .....	146
2.1.2 群組原則設定 .....	19	7.3 稽核資料夾設定 .....	149
2.2 工作群組 .....	25	8. Windows 2022 .....	156
2.2.1 稽核原則設定 .....	25	8.1 網域 .....	156
2.2.2 事件檔案設定 .....	28	8.1.1 組織單位設定 .....	156
2.3 稽核資料夾設定 .....	30	8.1.2 群組原則設定 .....	161
3. Windows 2003 .....	34	8.2 工作群組 .....	168
3.1 網域 .....	34	8.2.1 稽核原則設定 .....	168
3.1.1 組織單位設定 .....	34	8.2.2 事件檔案設定 .....	172
3.1.2 群組原則設定 .....	38	8.3 稽核資料夾設定 .....	175
3.2 工作群組 .....	46	9. N-Reporter .....	182
3.2.1 稽核原則設定 .....	46	9.1 Windows 2003 或之前版本作業系統 .....	183
3.2.2 事件檔案設定 .....	50	9.2 Windows 2008 或之後版本作業系統 .....	184
3.3 稽核資料夾設定 .....	52	10. 故障排除 .....	185
4. Windows 2008 .....	56	10.1 Invoke-GPUUpdate 錯誤 .....	185
4.1 網域 .....	56		
4.1.1 組織單位設定 .....	56		
4.1.2 群組原則設定 .....	59		
4.2 工作群組 .....	66		
4.2.1 稽核原則設定 .....	66		
4.2.2 事件檔案設定 .....	70		
4.3 稽核資料夾設定 .....	73		
5. Windows 2012 .....	78		
5.1 網域 .....	78		
5.1.1 組織單位設定 .....	78		
5.1.2 群組原則設定 .....	83		
5.2 工作群組 .....	90		
5.2.1 稽核原則設定 .....	90		
5.2.2 事件檔案設定 .....	94		
5.3 稽核資料夾設定 .....	97		

## 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 2000 / 2003 / 2008 / 2012 / 2016 / 2019 / 2022 版本。

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

監視的事件：<https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

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

# 1. NXLog

## 1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition)

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

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



Windows

nxlog-ce-3.0.2272.msi

註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

<2.1.1> 開啟 [Windows PowerShell]



<2.1.2> 安裝 NXLog 軟體

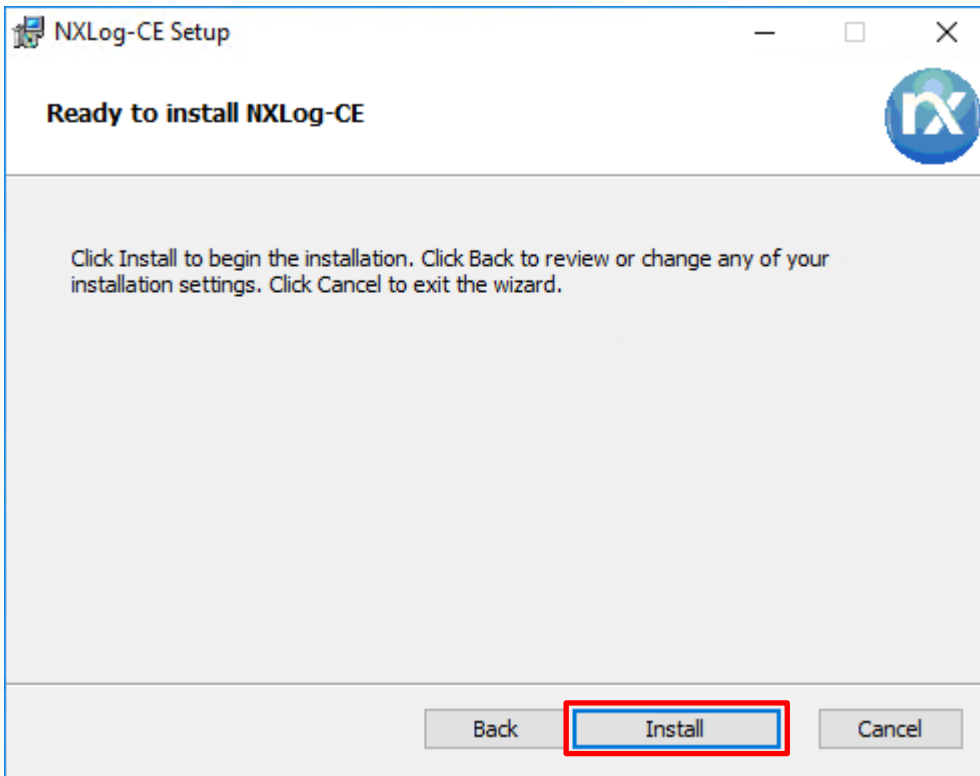
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```

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

紅色文字部位請輸入 NXLog 軟體路徑和檔案

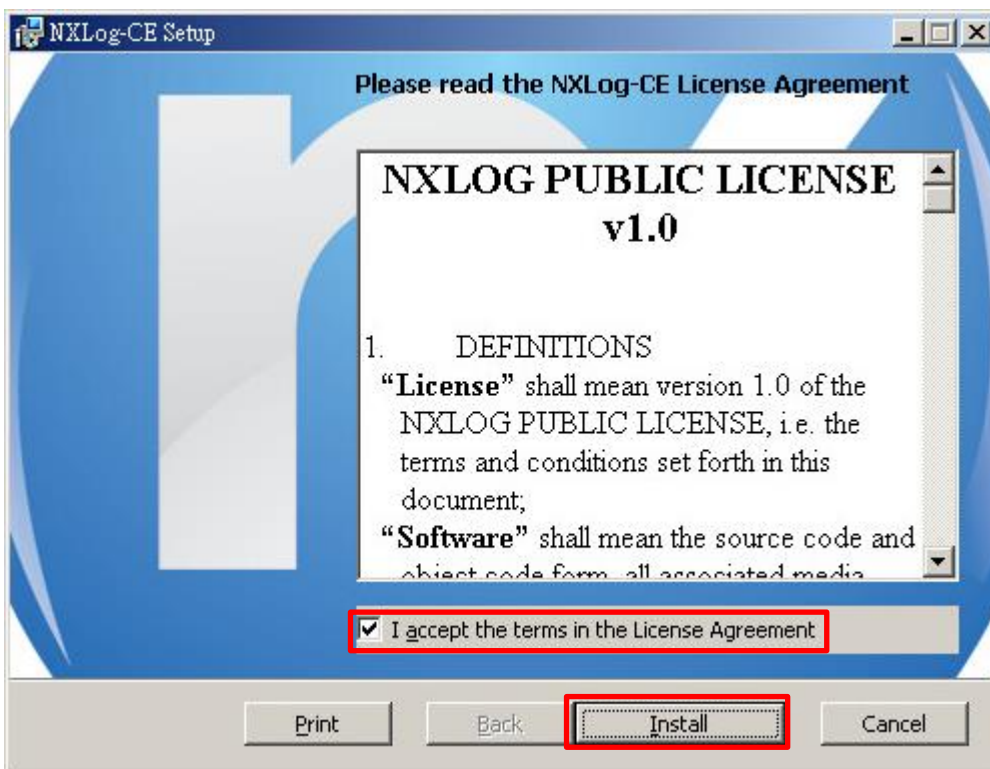
<2.2> Windows 2003

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



<2.3> Windows 2000

點擊 [nxlog-ce-2.9.1716.msi] -> 勾選 [I accept the terms in the License Agreement] -> 按 [Install] 到 [Finish]



## 1.2 NXLog 設定檔下載

### 1.2.1 Windows 2003 或之前版本作業系統

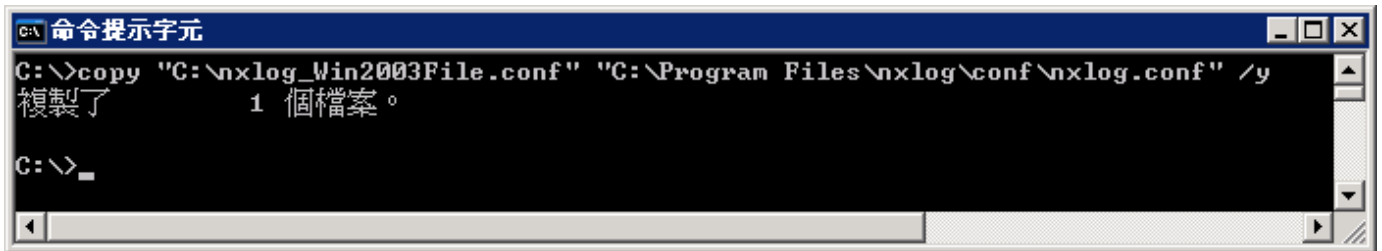
(1) 開啟 [命令提示字元]



(2) 下載 NXLog Windows 2003 File 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_Win2003File.conf](http://www.npartnertech.com/download/tech/nxlog_Win2003File.conf)

```
C:\> copy "C:\nxlog_Win2003File.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



本文件範例環境為 32bit 作業系統，若作業系統環境為 64bit 紅色文字部位請改為以下設定 "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

## 1.2.2 Windows 2008 或之後版本作業系統

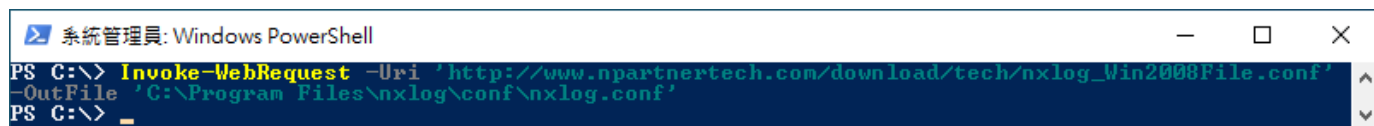
(1) 開啟 [Windows PowerShell]



(2) 下載 NXLog Windows 2008 File 設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_Win2008File.conf](http://www.npartnertech.com/download/tech/nxlog_Win2008File.conf)

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008File.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```



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



## 1.3 NXLog 設定檔

### 1.3.1 Windows 2003 或之前版本作業系統

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
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
==567 or $EventID == 528 or $EventID == 529 or $EventID == 530 or $EventID == 531 or $EventID == 532 or
$EventID == 533 or $EventID == 534 or $EventID == 535 or $EventID == 536 or $EventID == 537 or $EventID ==
538 or $EventID == 539 or $EventID == 540 or $EventID == 551 or $EventID == 552 or $EventID == 682 or
$EventID == 683 or $EventID == 672 or $EventID == 673 or $EventID == 674 or $EventID == 675 or $EventID ==
676 or $EventID == 677 or $EventID == 678 or $EventID == 679 or $EventID == 680 or $EventID == 681)
{ $SyslogFacilityValue = 17; } \
  else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 17; } \
  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 192.168.8.4
```

本文件範例環境為 32bit 作業系統，若作業系統環境為 64bit 請改為以下設定

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

### 1.3.2 Windows 2008 或之後版本作業系統

```
# Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
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 2008 File 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=4656 or EventID=4657 or EventID=4658 or EventID=4659 or
EventID=4660 or EventID=4661 or EventID=4663 or EventID=4664 or EventID=4665 or EventID=4666 or
EventID=4667 or EventID=4668 or EventID=4670 or EventID=4671 or EventID=4690 or EventID=4691 or
EventID=4698 or EventID=4699 or EventID=4700 or EventID=4701 or EventID=4702)]]</Select> \
      <Select Path="Security">*[System[(EventID=5140 or EventID=5142 or EventID=5143 or EventID=5144 or
EventID=5145 or EventID=5148 or EventID=5149 or EventID=5150 or EventID=5151 or EventID=5152 or
EventID=5153 or EventID=5154 or EventID=5155 or EventID=5156 or EventID=5157 or EventID=5158 or
EventID=5159 or EventID=5168 or EventID=5888 or EventID=5889 or EventID=5890)]]</Select> \
      <Select Path="Security">*[System[(EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or
EventID=4772 or EventID=4773 or EventID=4774 or EventID=4775 or EventID=4776 or EventID=4777 or
EventID=4820)]]</Select> \
      <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626 or EventID=4627 or
EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or EventID=4672 or
EventID=4675 or EventID=4778 or EventID=4779 or EventID=4800 or EventID=4801 or EventID=4802 or
EventID=4803 or EventID=4964 or EventID=4976 or EventID=5378 or EventID=5632 or EventID=5633)]]</Select> \
    </Query> \
  </QueryList>
</Input>

<Output out_eventlog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 17;
  Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
    else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route eventlog>
  Path in_eventlog => out_eventlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud 192.168.8.4
```

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

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

## 1.4 NXLog 啟動服務

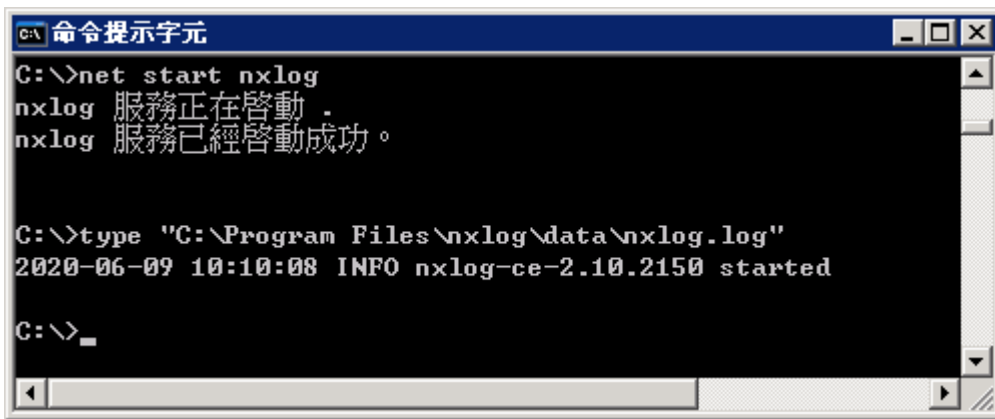
### 1.4.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]



(2) 啟動 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
C:\> net start nxlog  
C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```



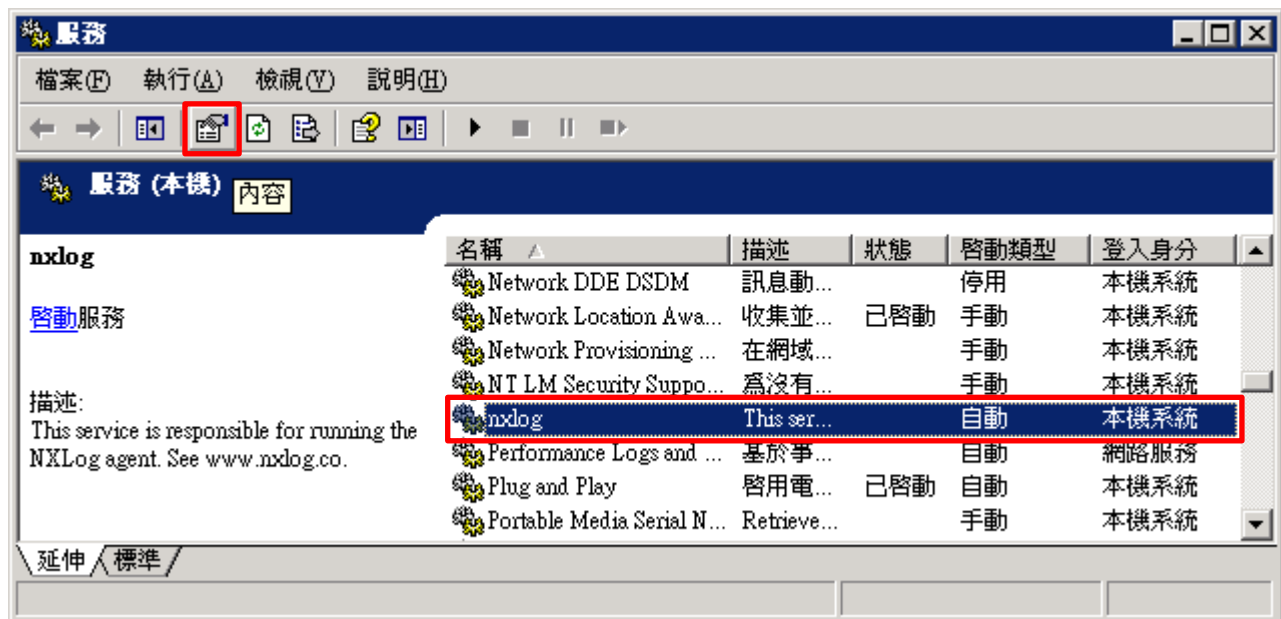
(3) 開啟 [服務] 功能

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

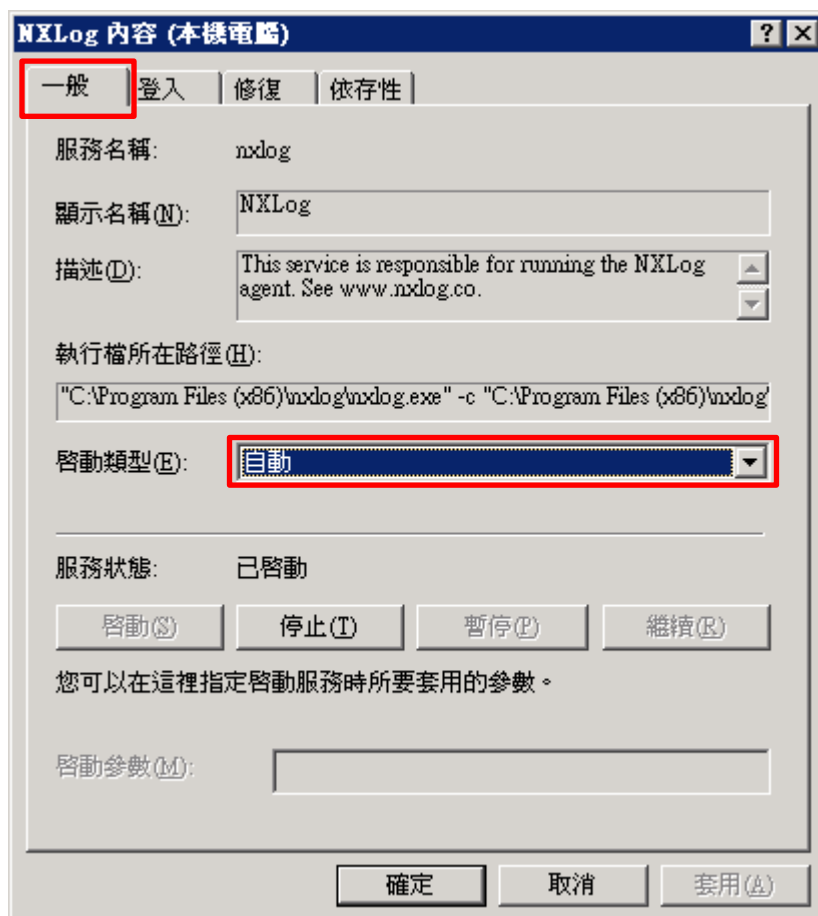


(4) 開啟 NXLog 服務內容

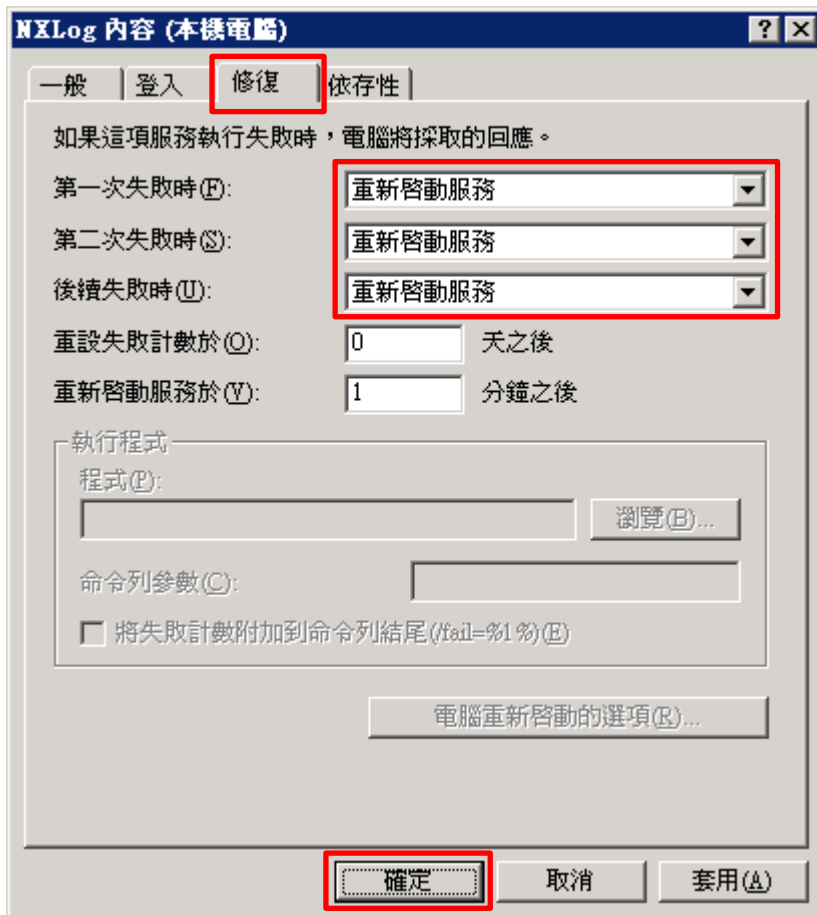
選擇 [nxlog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認 ; 啟動類型: [自動]



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



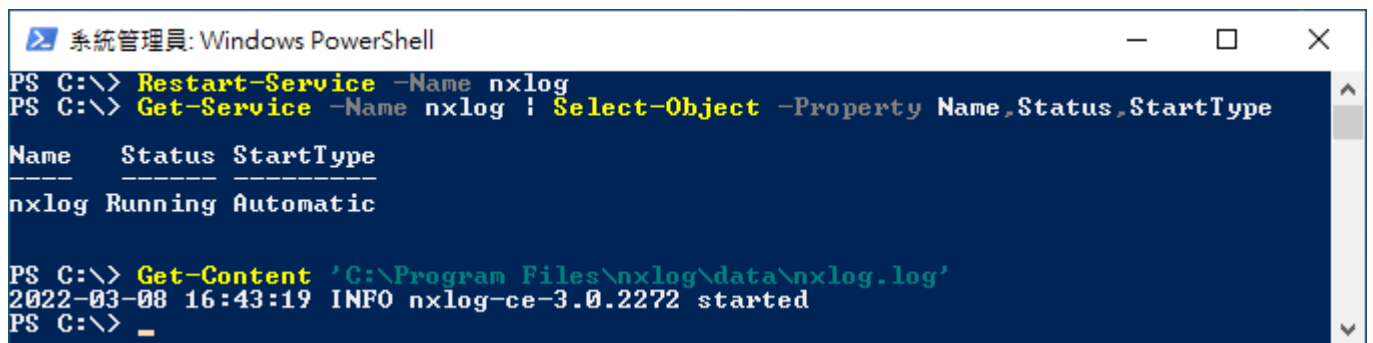
## 1.4.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



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

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

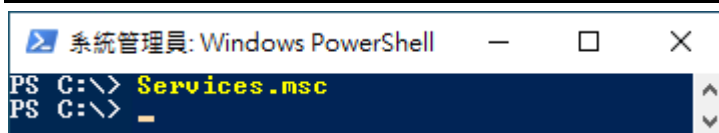
A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has standard Windows window controls (minimize, maximize, close). The command prompt shows the following commands and output:

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

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

(3) 開啟 [服務] 功能

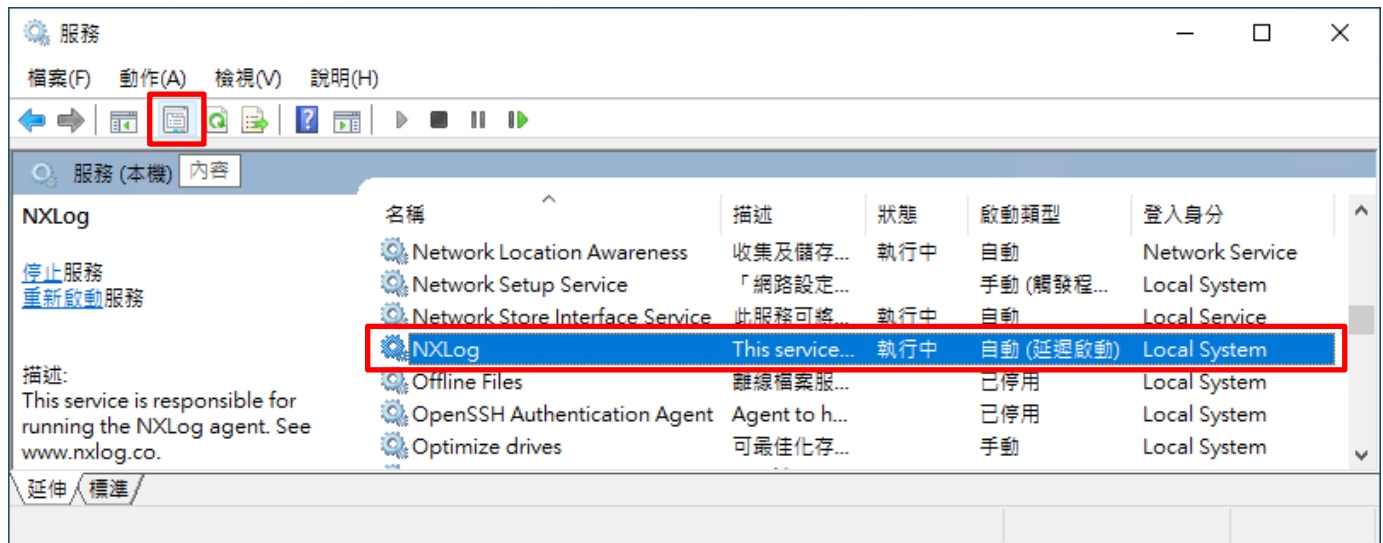
```
PS C:\> Services.msc
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has standard Windows window controls. The command prompt shows the following commands and output:

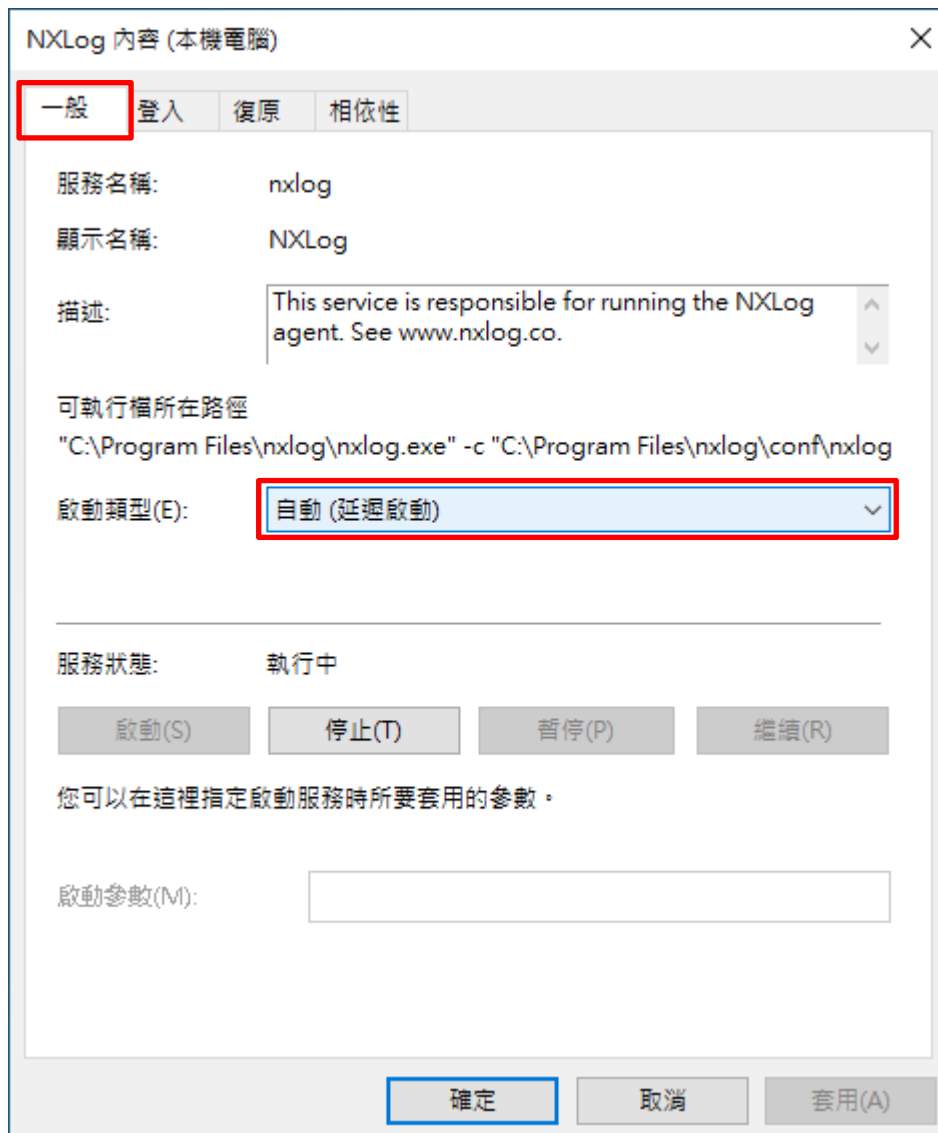
```
PS C:\> Services.msc
PS C:\> _
```

(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (延遲啟動)]





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

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P):  瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%)(E)

確定 取消 套用(A)



## 2. Windows 2000

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

※ 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

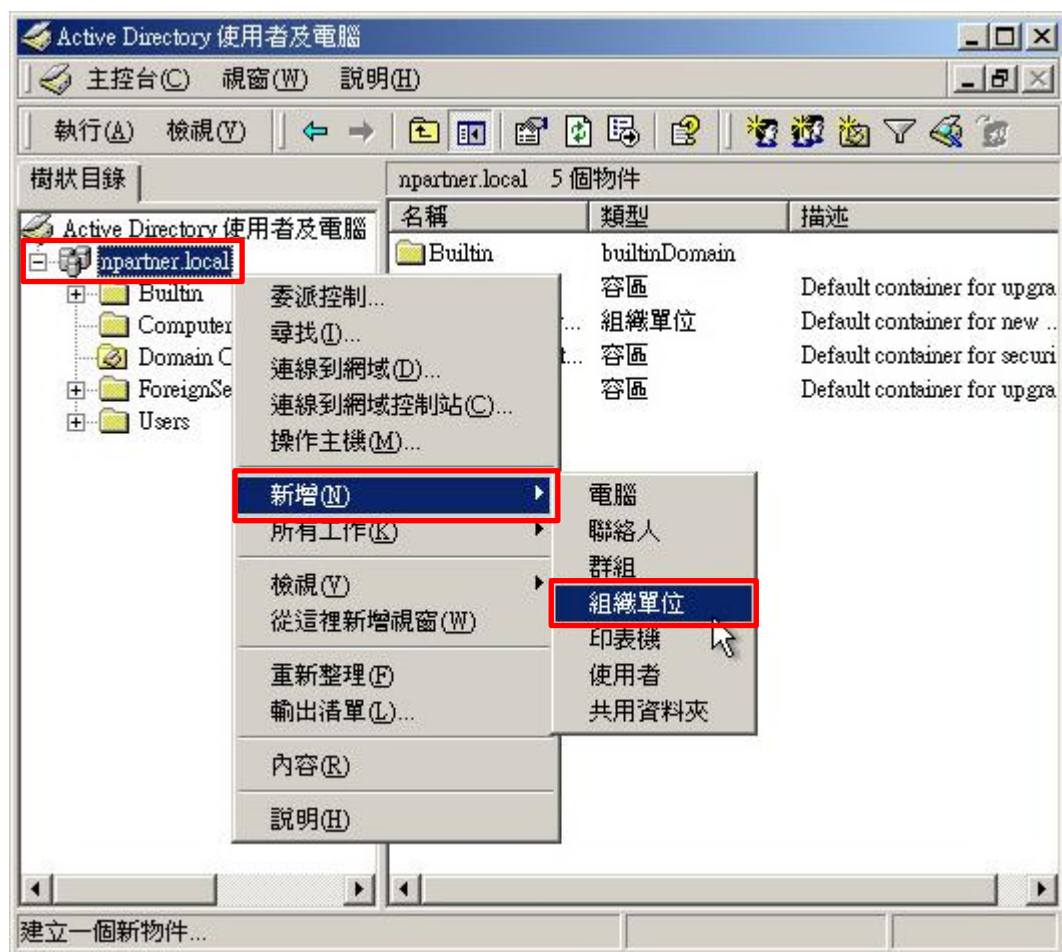
(1) 開啟 AD 使用者和電腦

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]



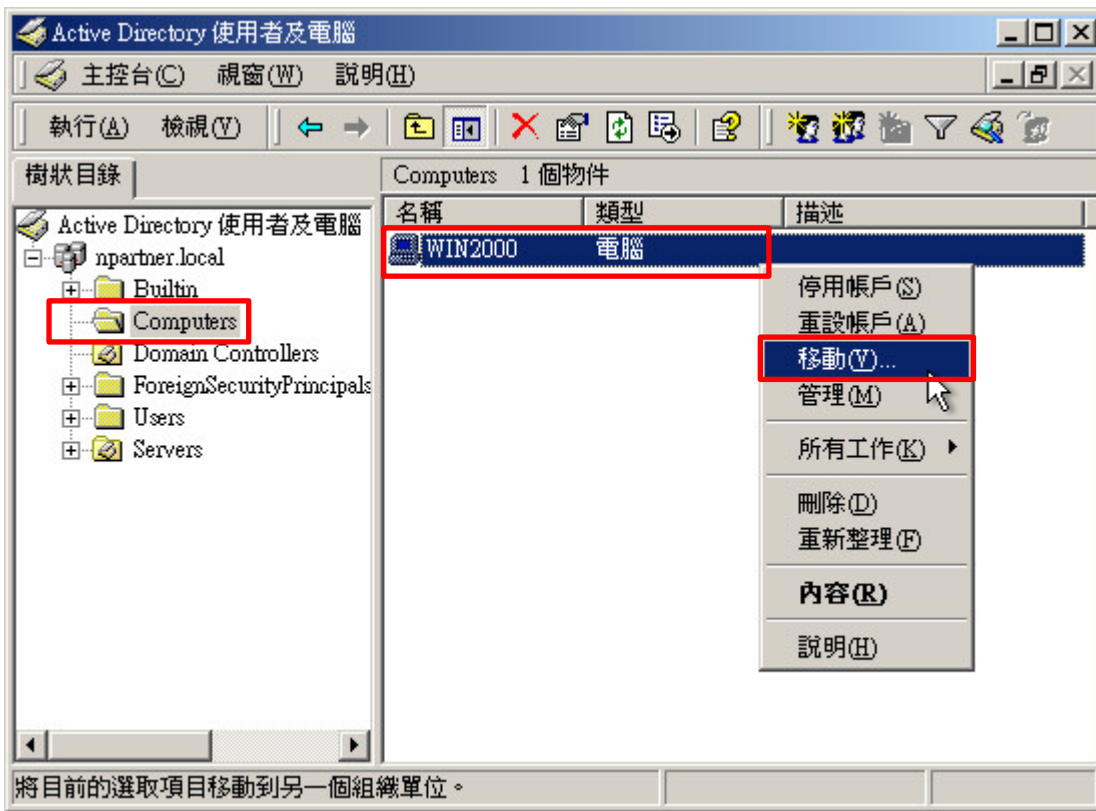
(3) 輸入組織單位名稱

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



(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2000] 伺服器按滑鼠右鍵，註：請依客戶環境選擇 Windows File 伺服器 -> 點選 [移動]



(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [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 Win2000 File 伺服器已移動



## 2.1.2 群組原則設定

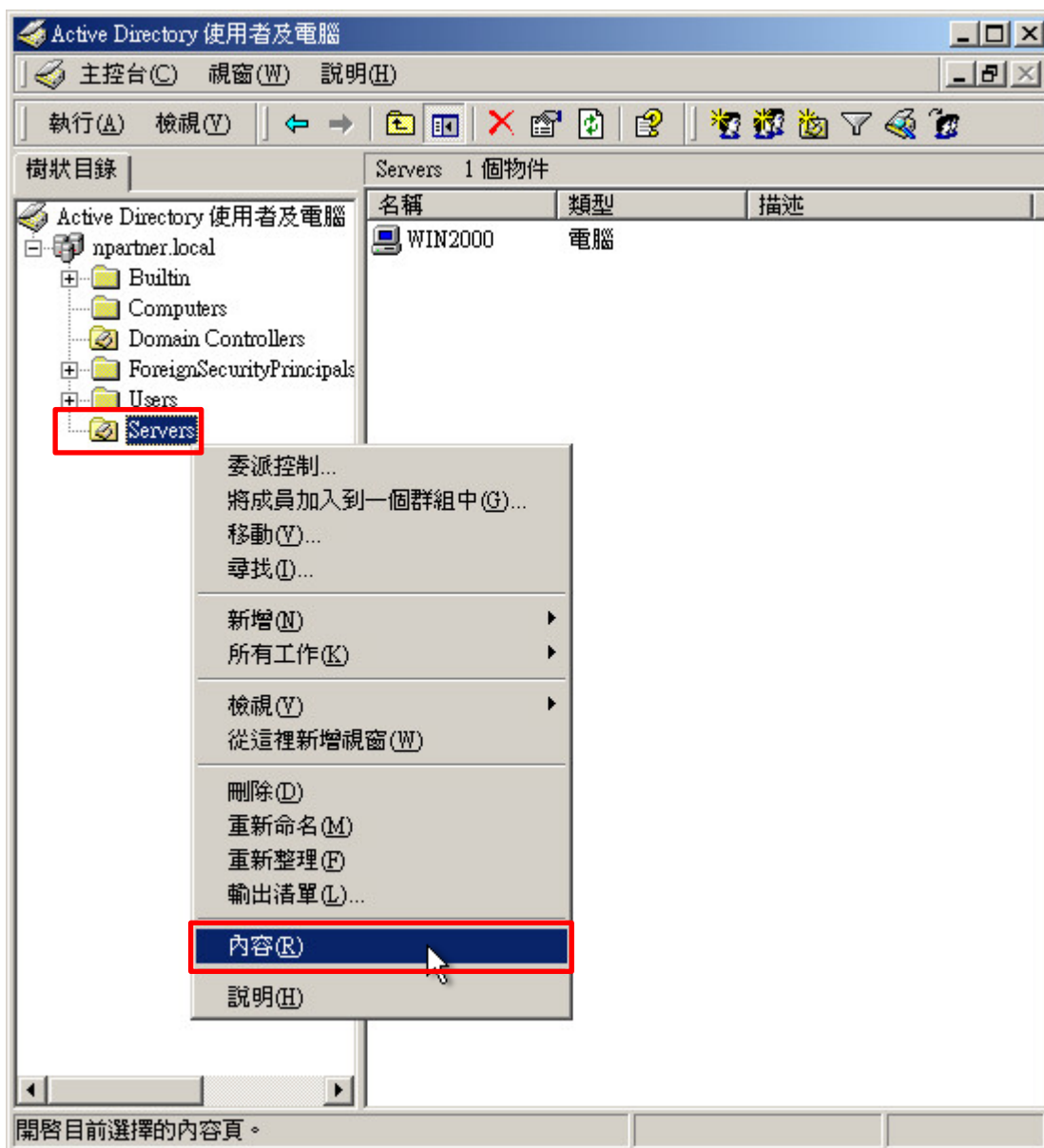
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



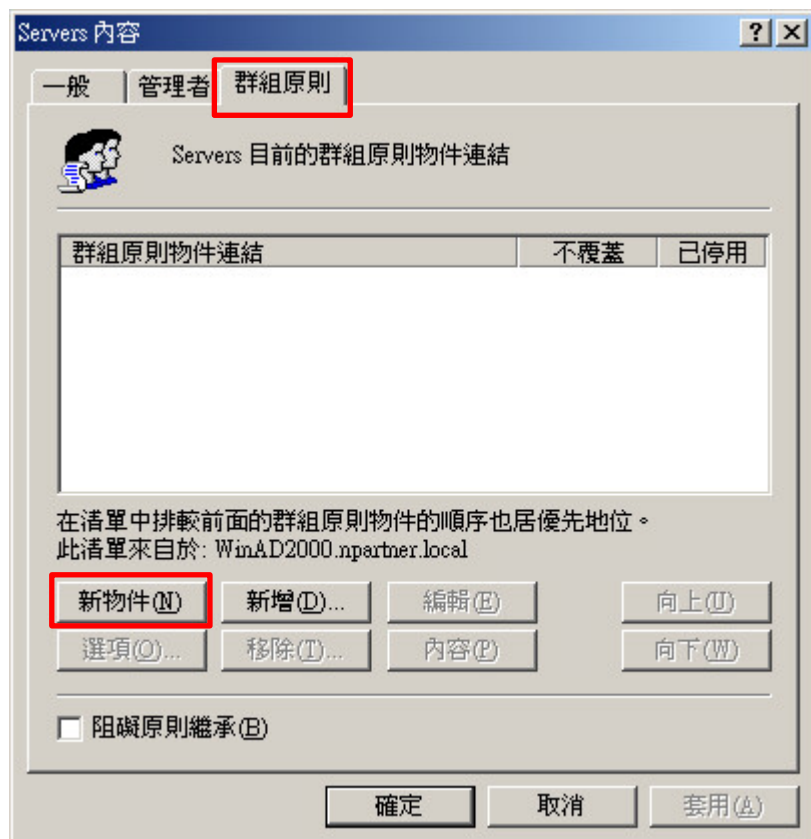
(2) 在 Servers 組織單位，點選內容

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

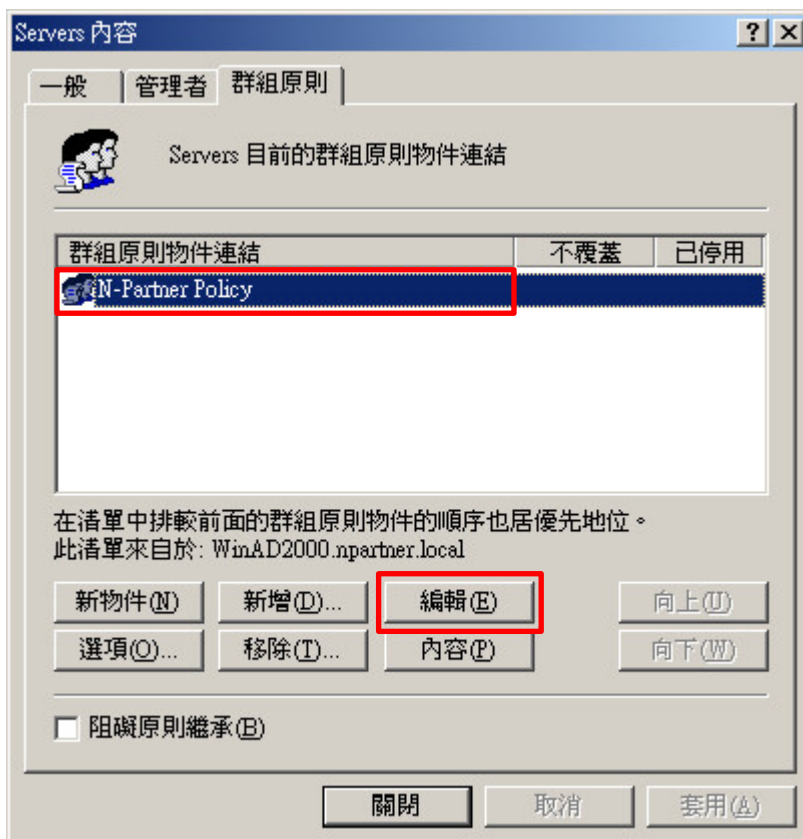
點選 [群組原則] 頁面 -> 按 [新物件]





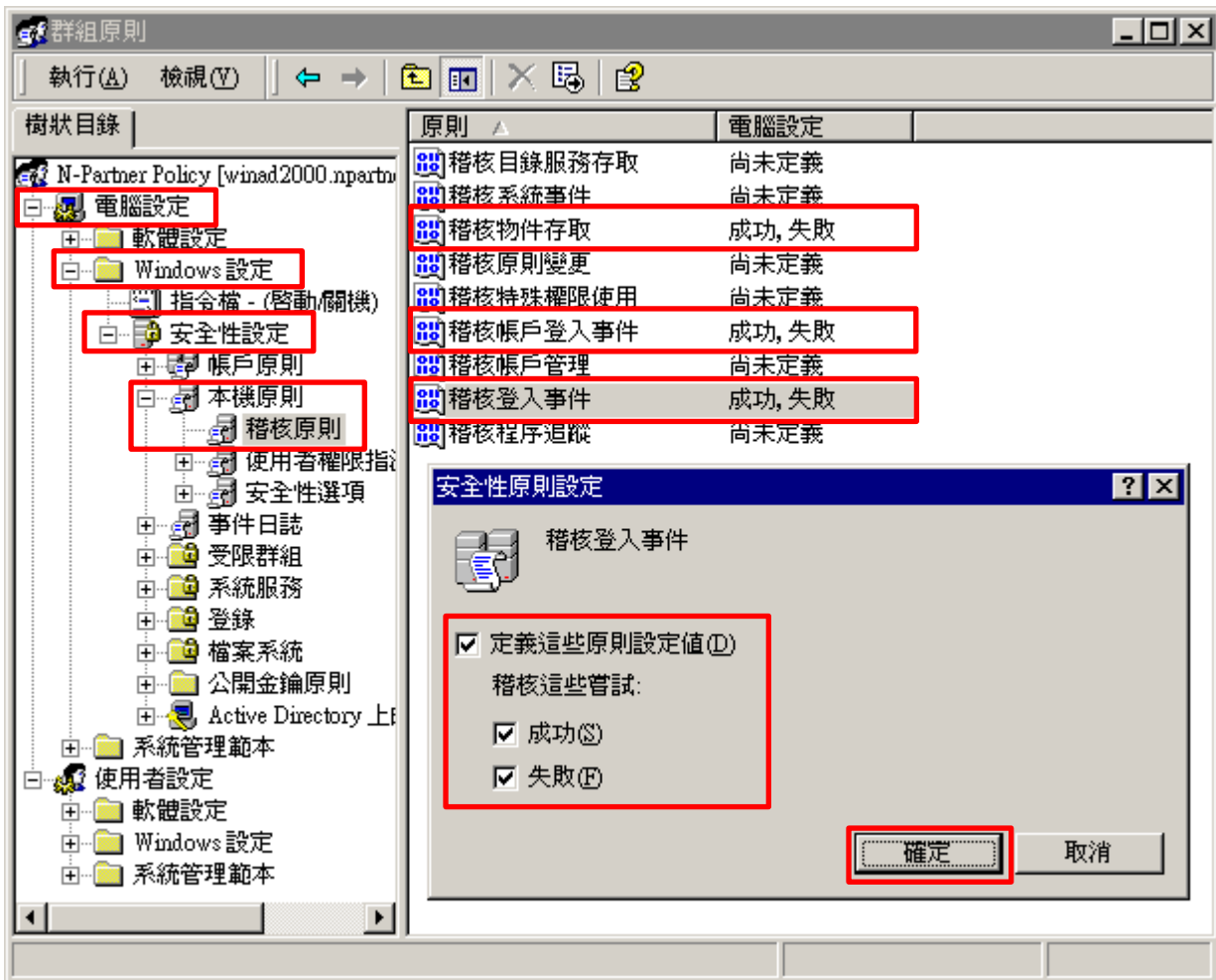
(4) 編輯群組原則物件

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



(5) 本機原則：稽核原則

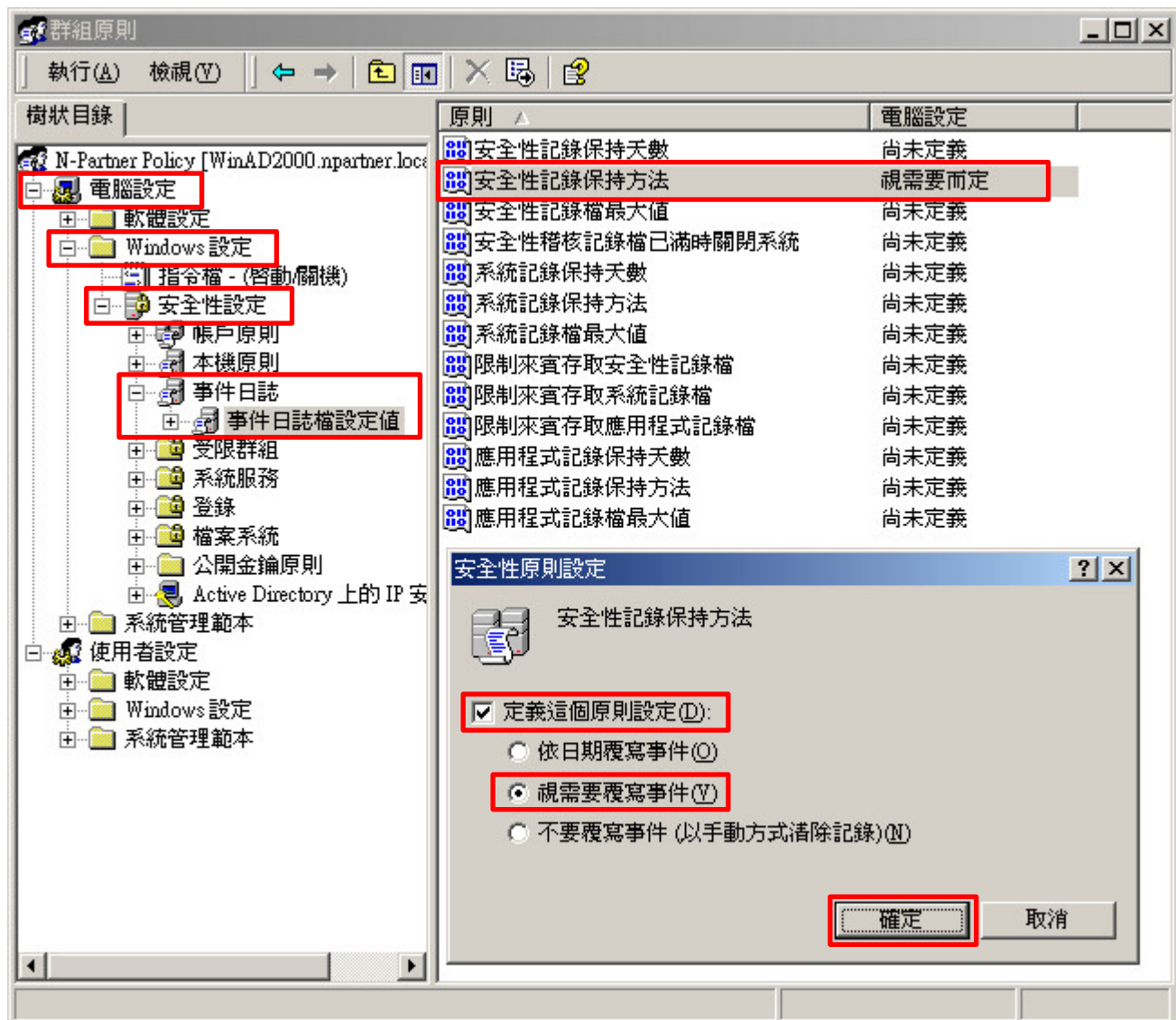
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定值:] & [成功] & [失敗] -> 按 [確定]





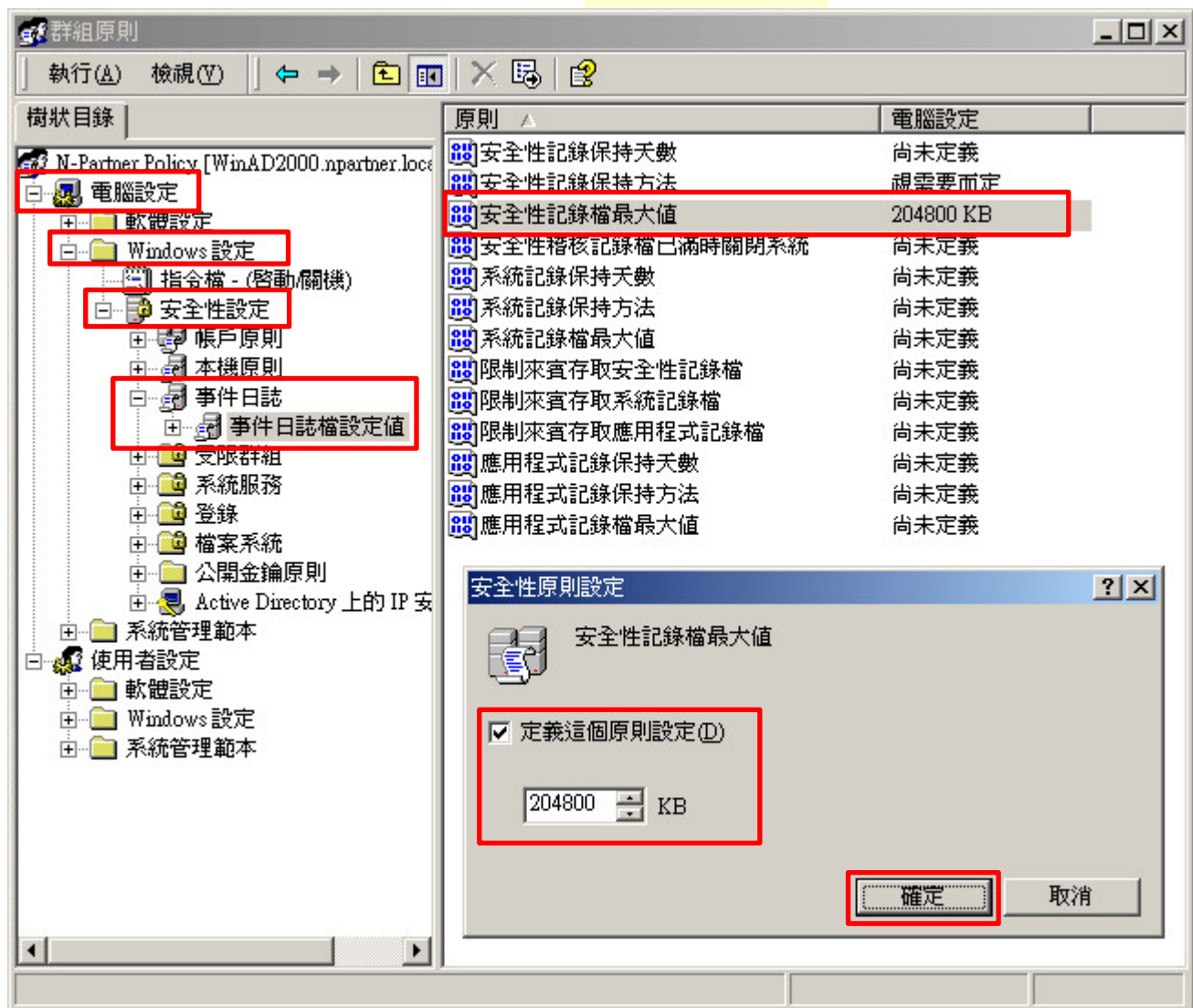
(6) 事件記錄檔：安全性記錄保持方法

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



(7) 事件記錄檔：安全性記錄檔最大值

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

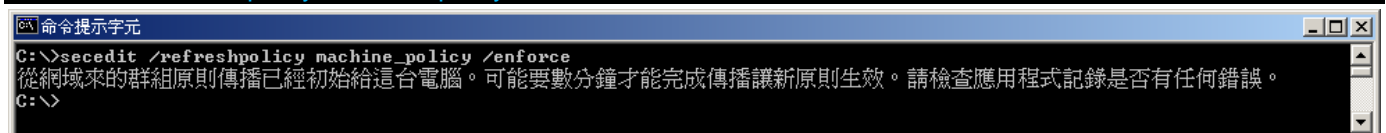


(8) 在 Windows File 伺服器，開啟 [命令提示字元]



(9) 更新群組原則

C:\> secedit /refreshpolicy machine\_policy /enforce

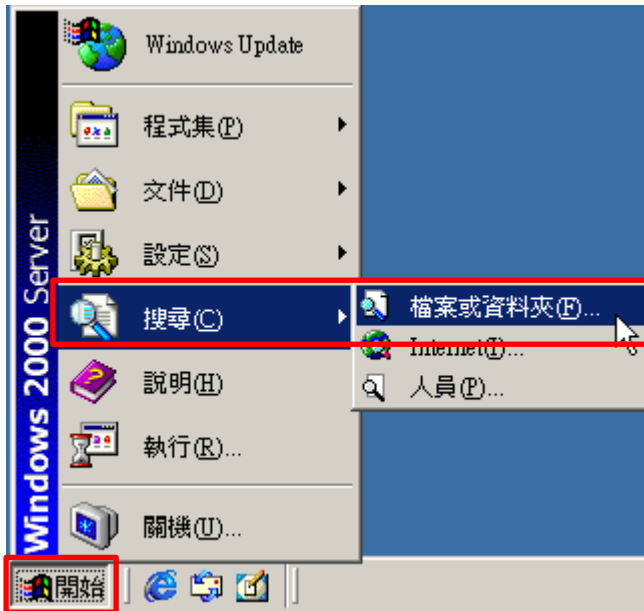


## 2.2 工作群組

### 2.2.1 稽核原則設定

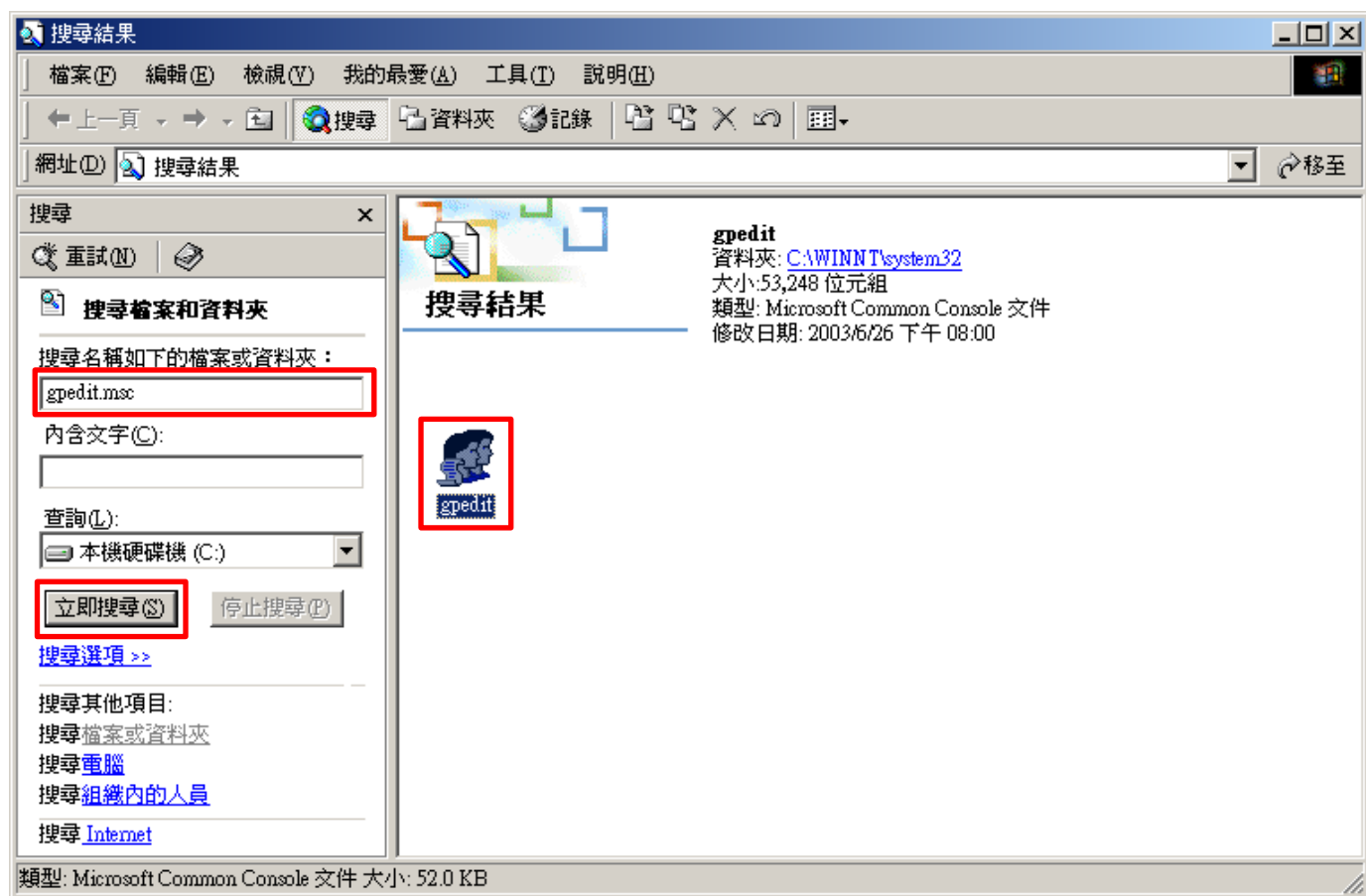
#### (1) 開啟搜尋

按 [開始] -> 點選 [搜尋] -> [檔案或資料夾]



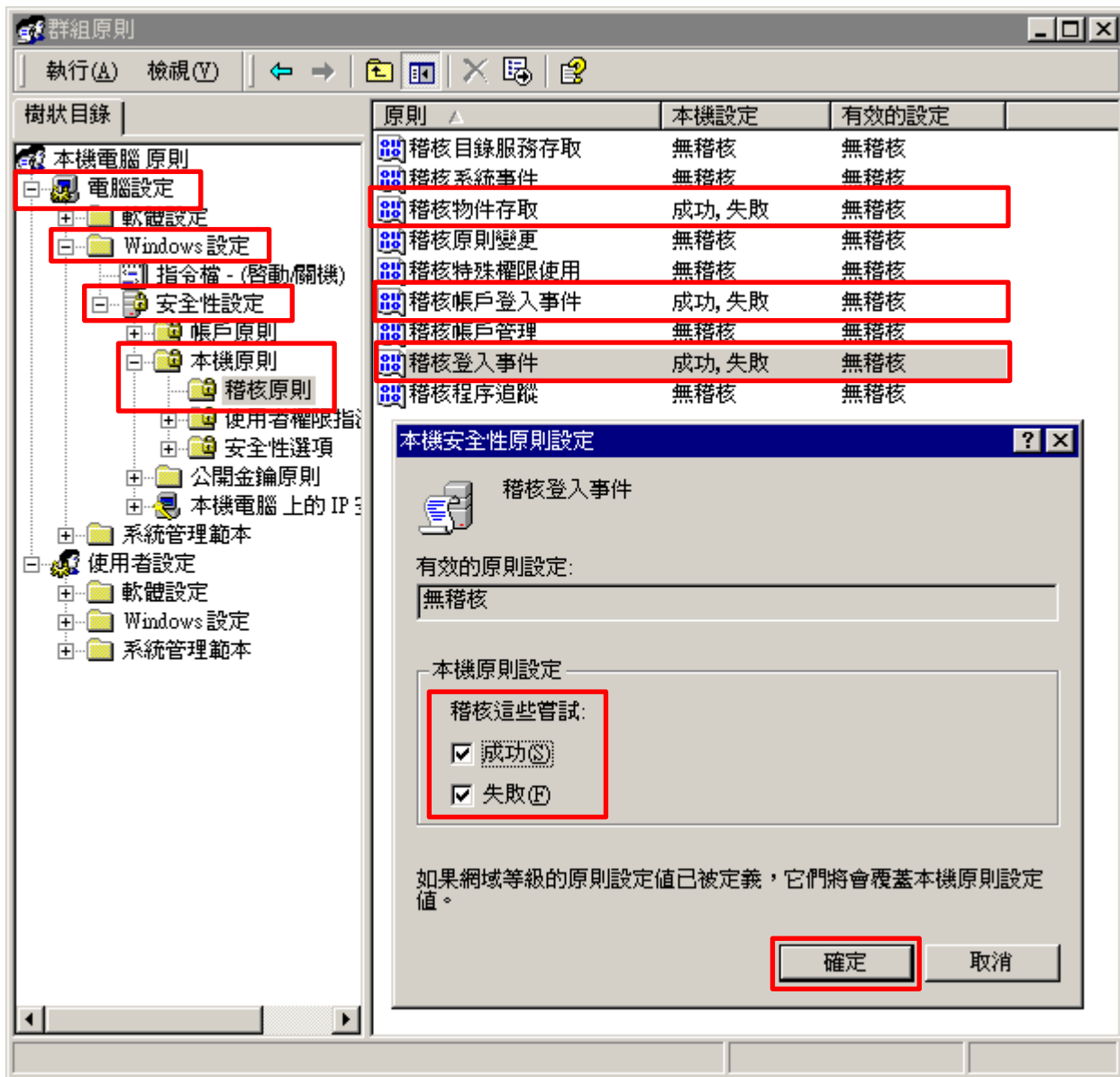
## (2) 搜尋群組原則物件編輯器

輸入 `gpedit.msc` -> 按 [立即搜尋] -> 點選 [gpedit]



(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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(4) 開啟 [命令提示字元]



(5) 更新群組原則

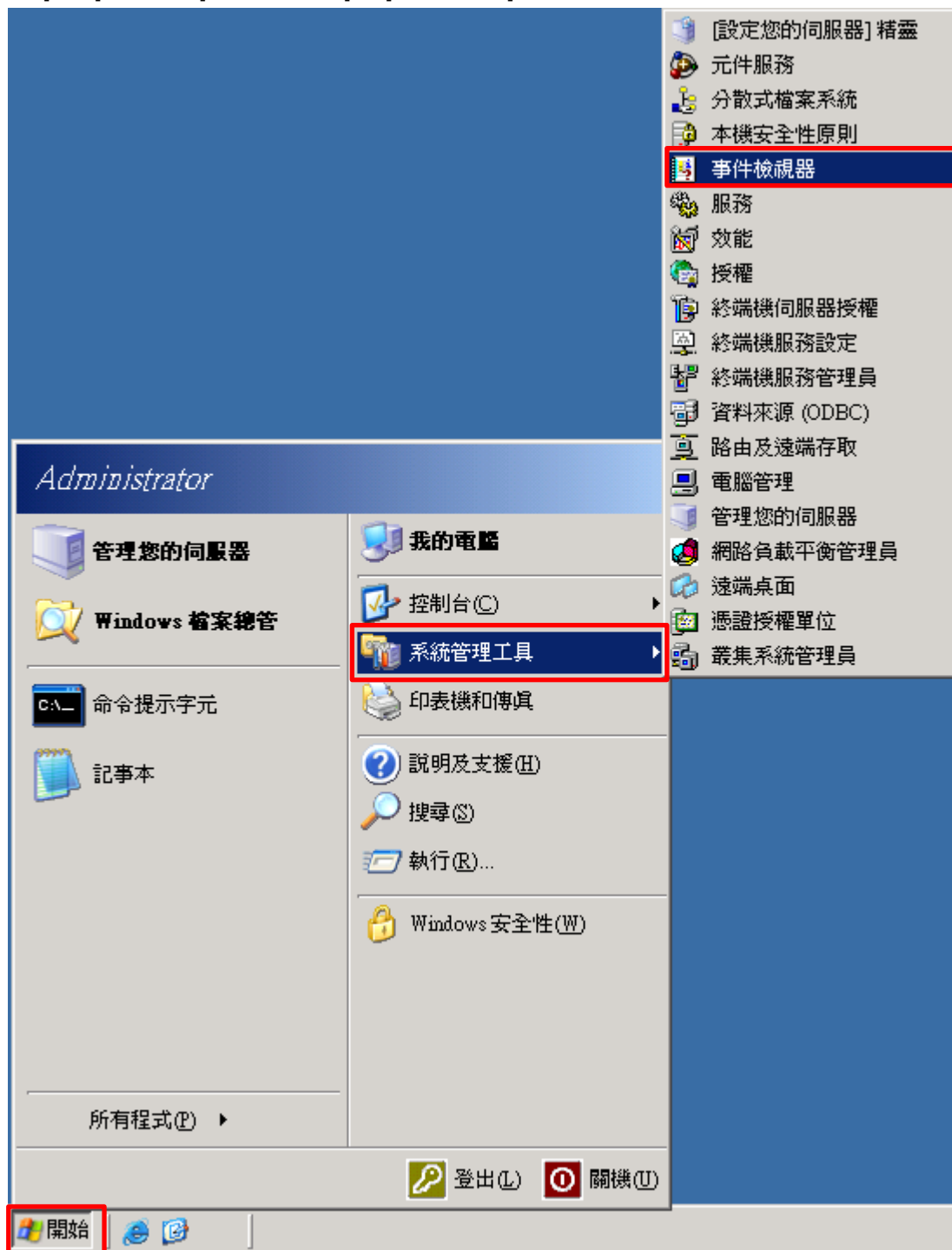
```
C:\> secedit /refreshpolicy machine_policy /enforce
```



## 2.2.2 事件檔案設定

### (1) 開啟事件檢視器

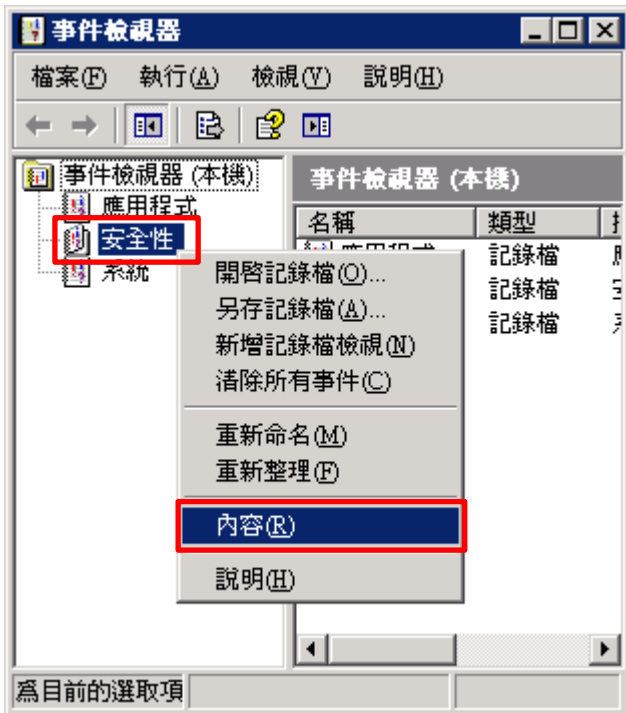
按 [開始] -> 點選 [系統管理工具] -> [事件檢視器]





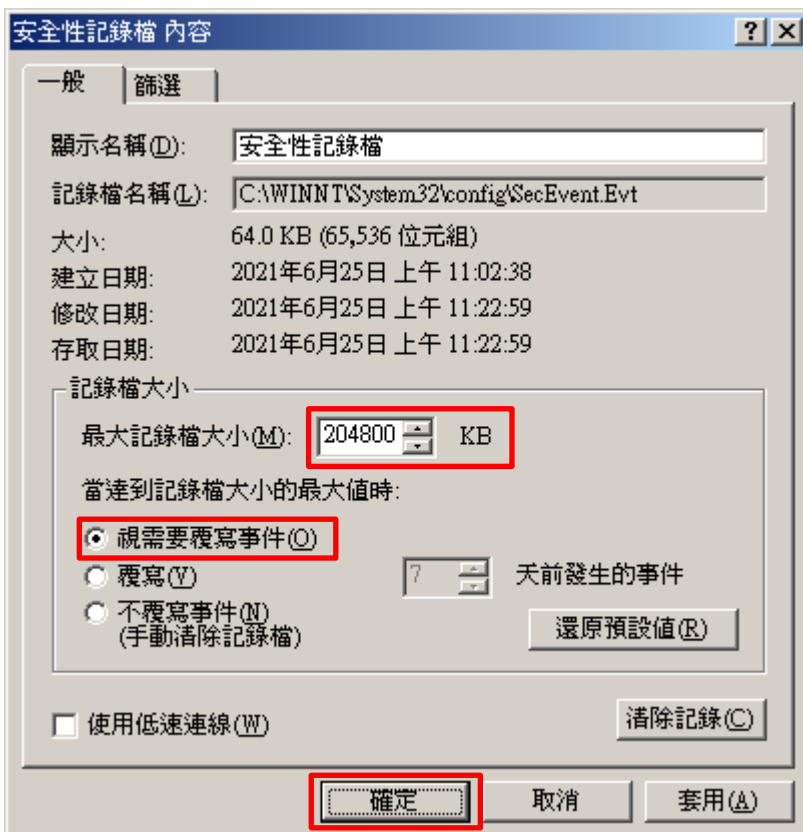
(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



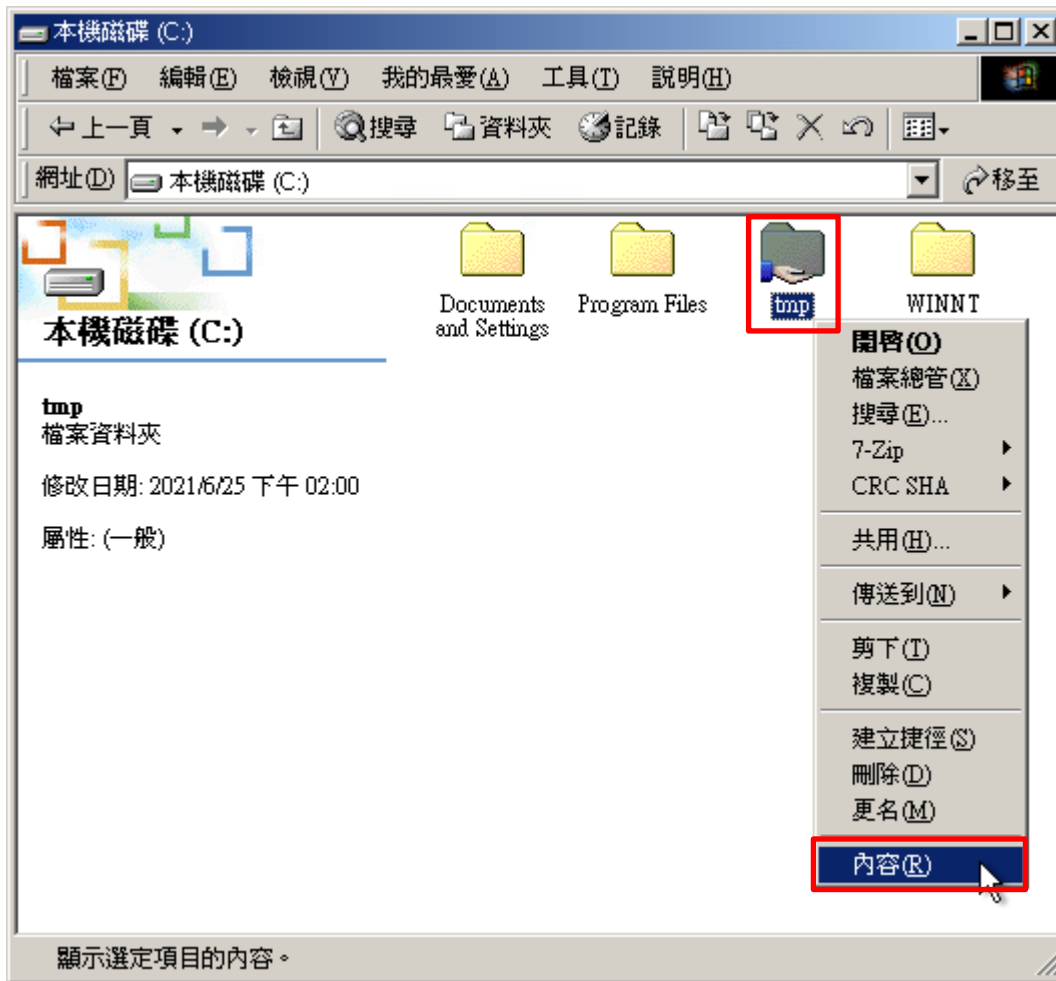
(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]



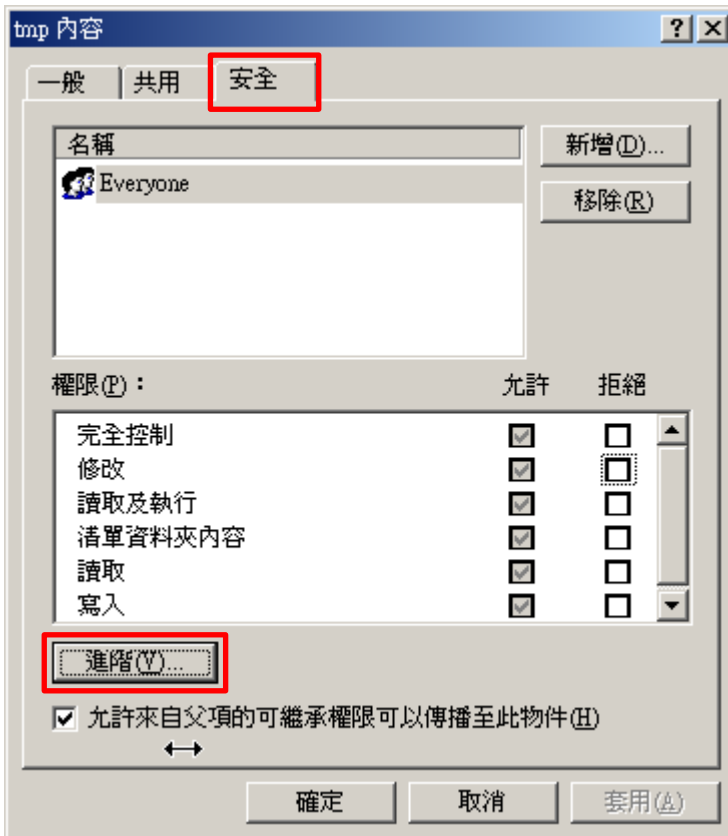
## 2.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]

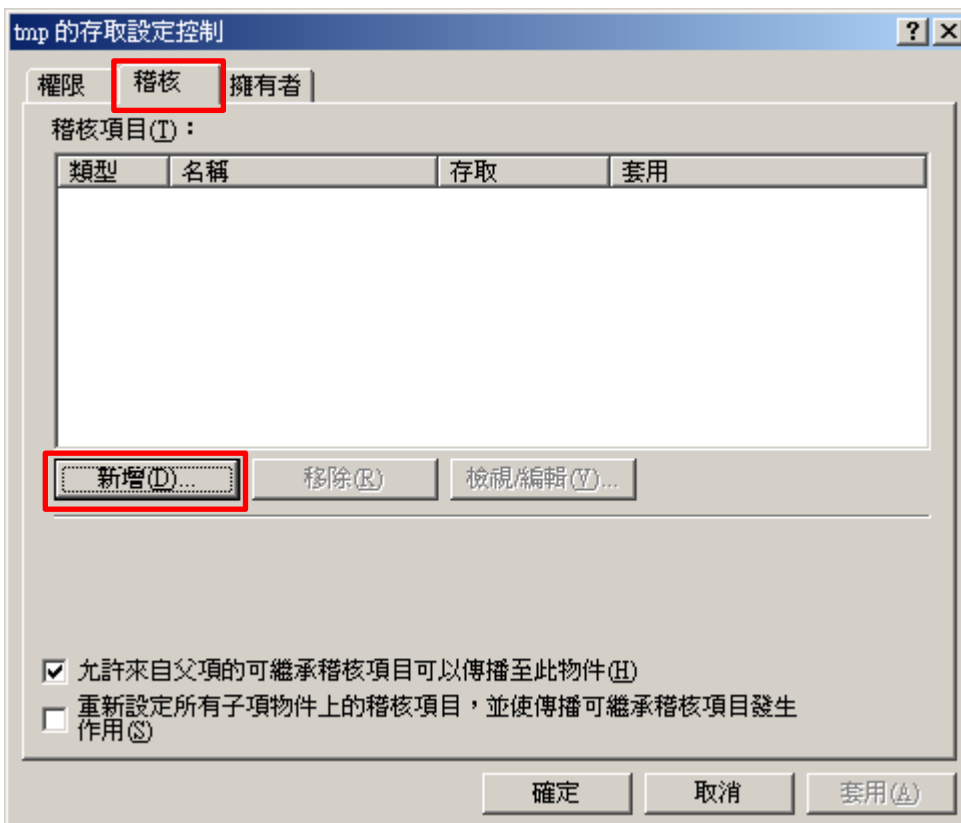




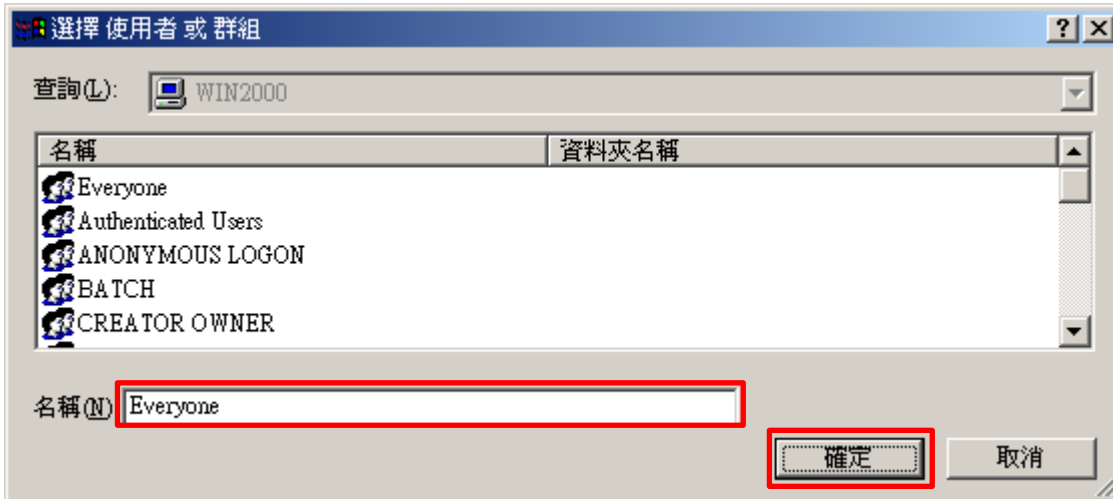
(2) 點選 [安全] 頁面 -> 按 [進階]



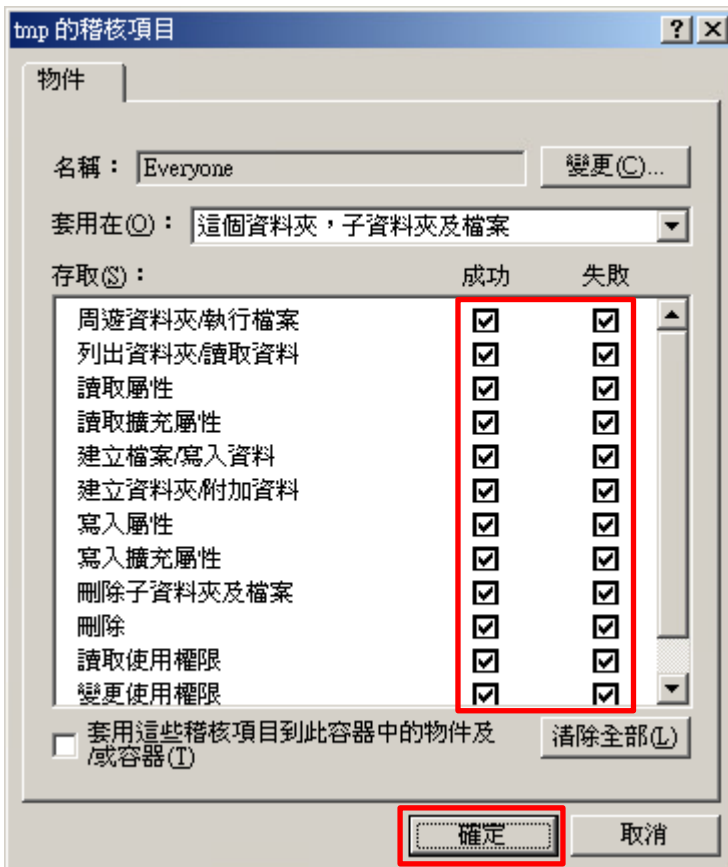
(3) 點選 [稽核] 頁面 -> 按 [新增]



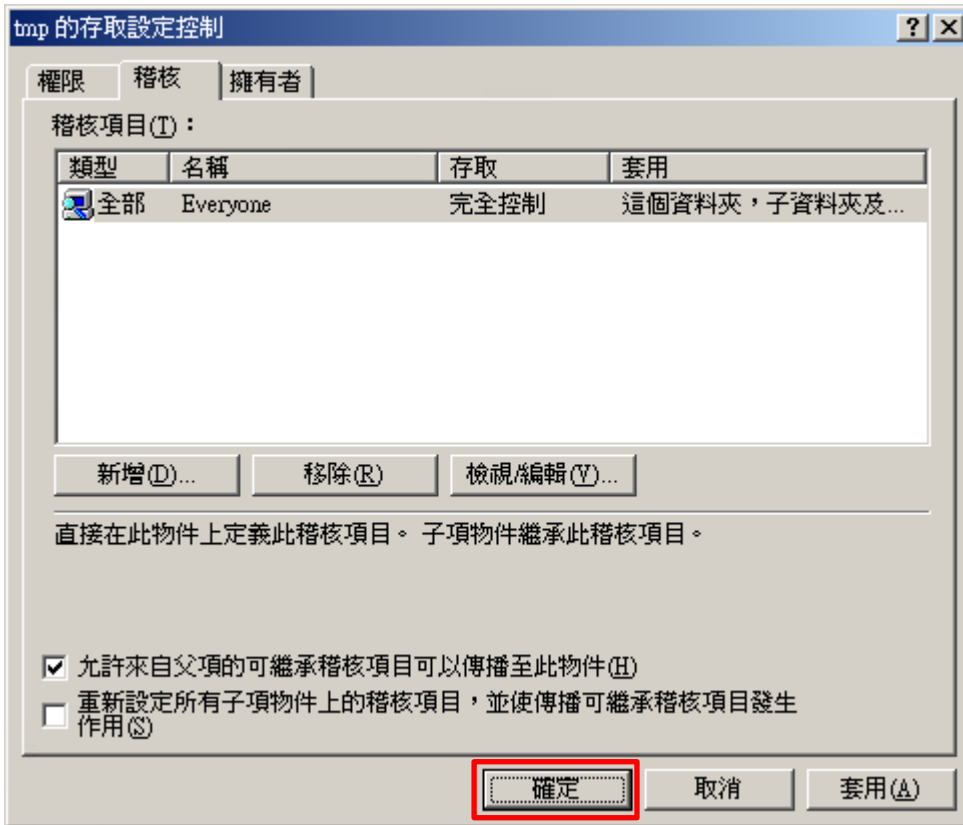
(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [確定]



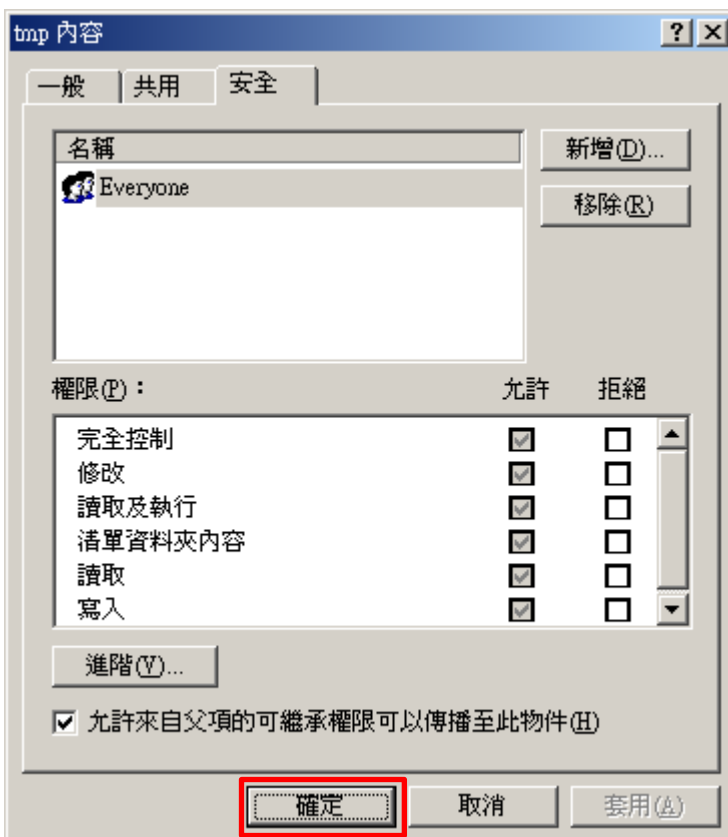
(5) 勾選所有項目存取 [成功] 和 [失敗] -> 按 [確定]



(6) 稽核項目顯示 Everyone 名稱 -> 按 [確定]



(7) 按 [確定]



## 3. Windows 2003

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

※ 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

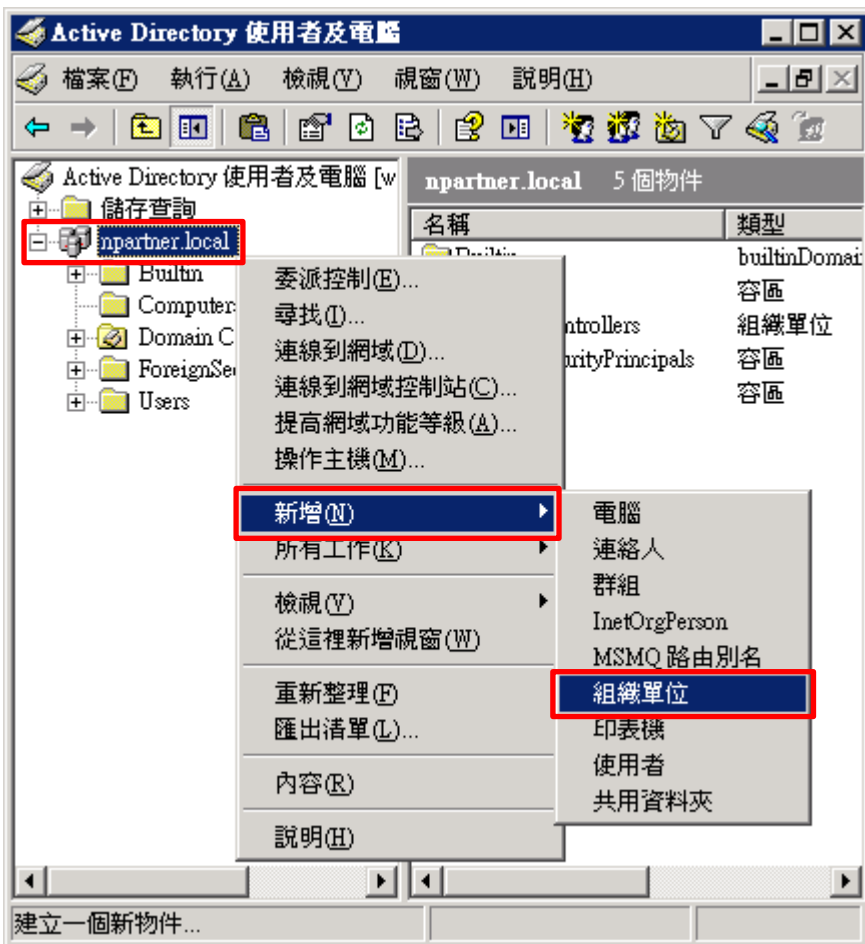
(1) 開啟 AD 使用者和電腦

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]



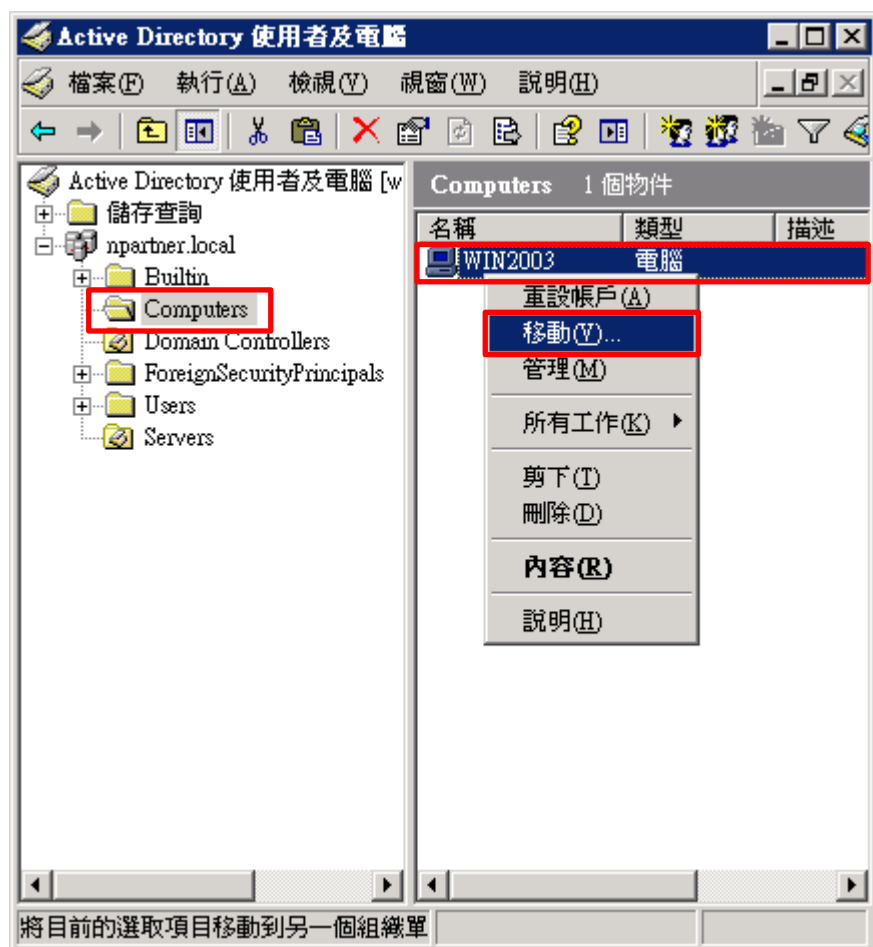
(3) 輸入組織單位名稱

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



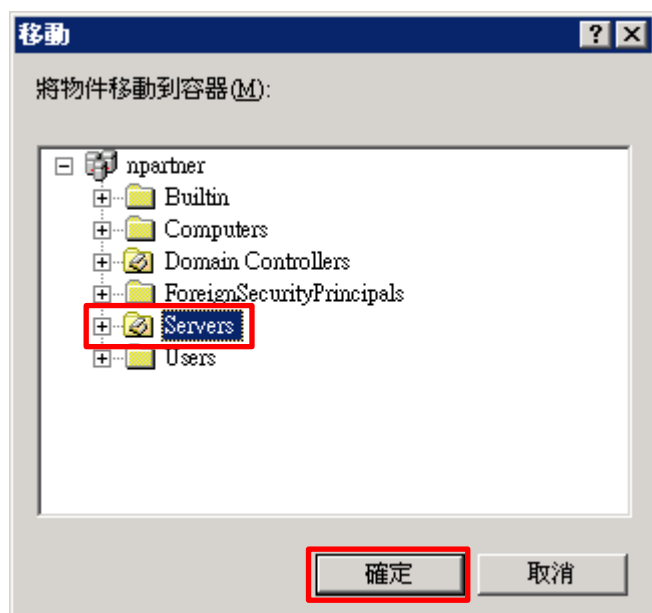
(4) 移動伺服器至新的組織單位

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



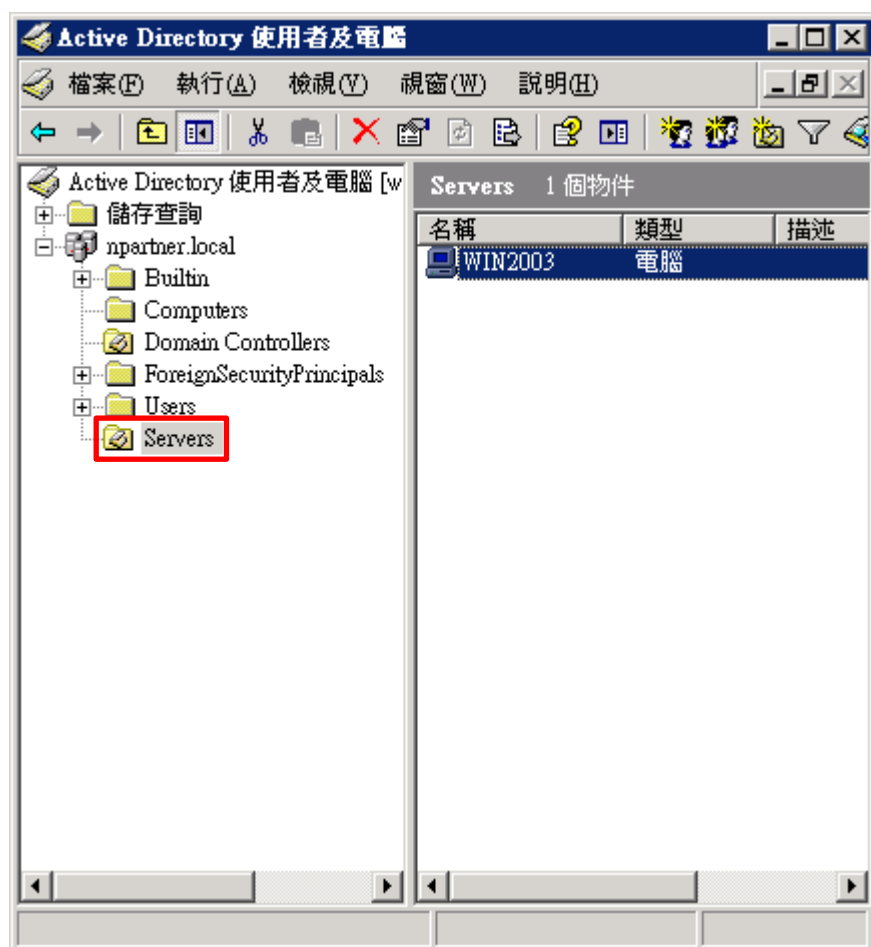
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [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 Win2003 File 伺服器已移動



### 3.1.2 群組原則設定

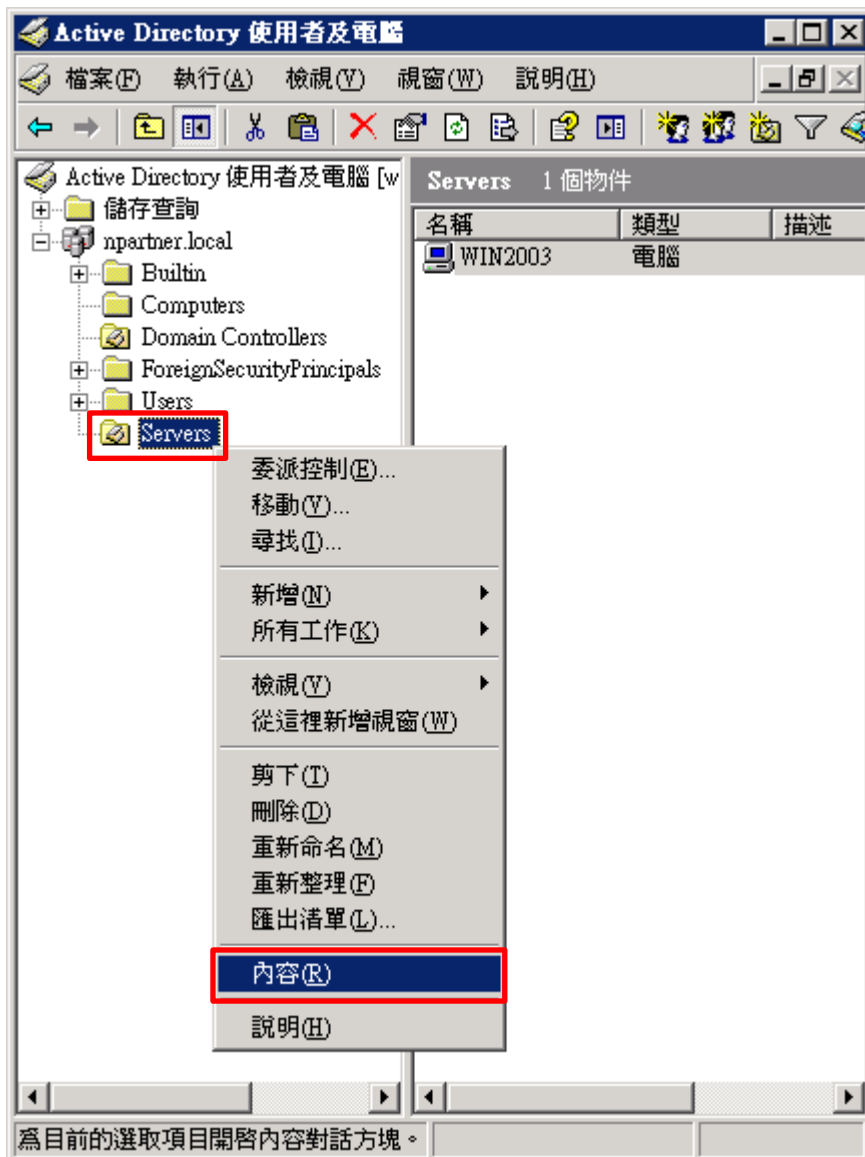
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 在 Servers 組織單位，點選內容

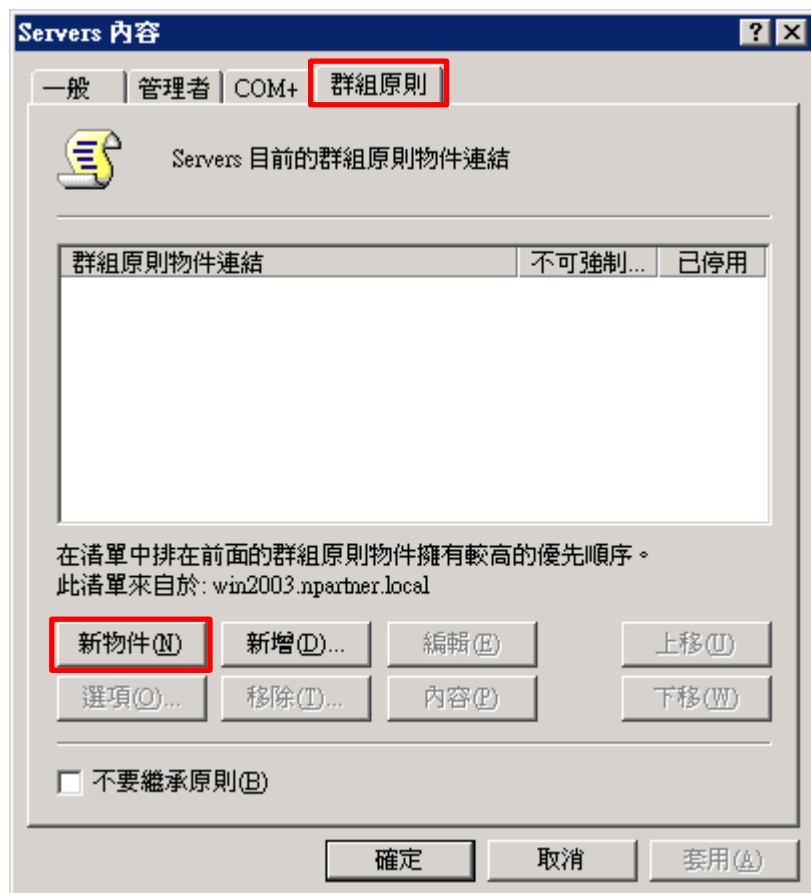
在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]





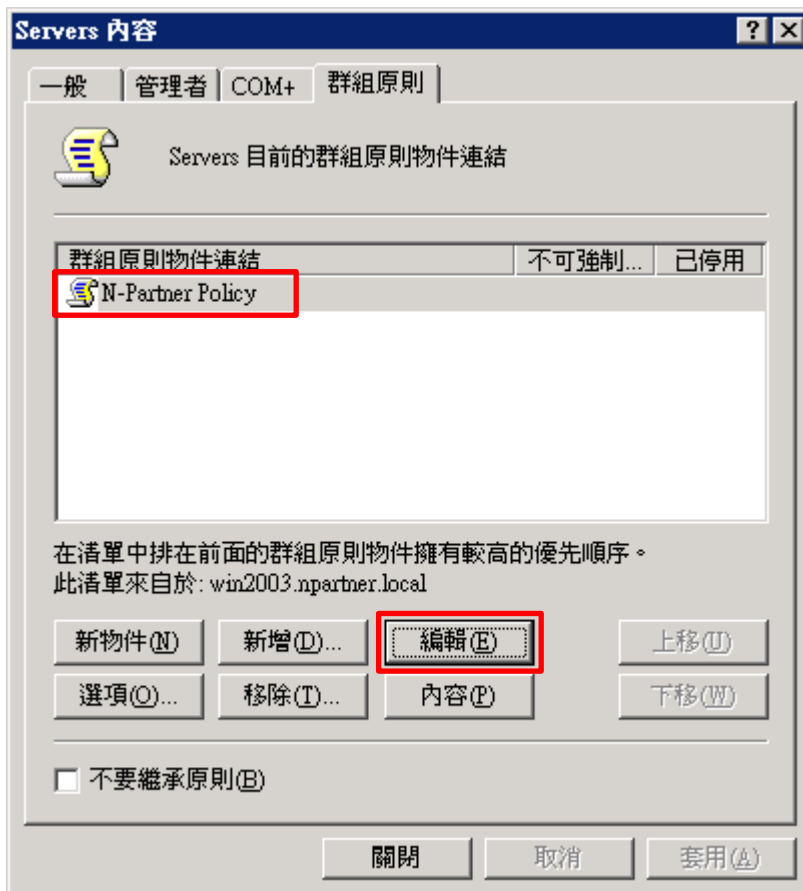
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



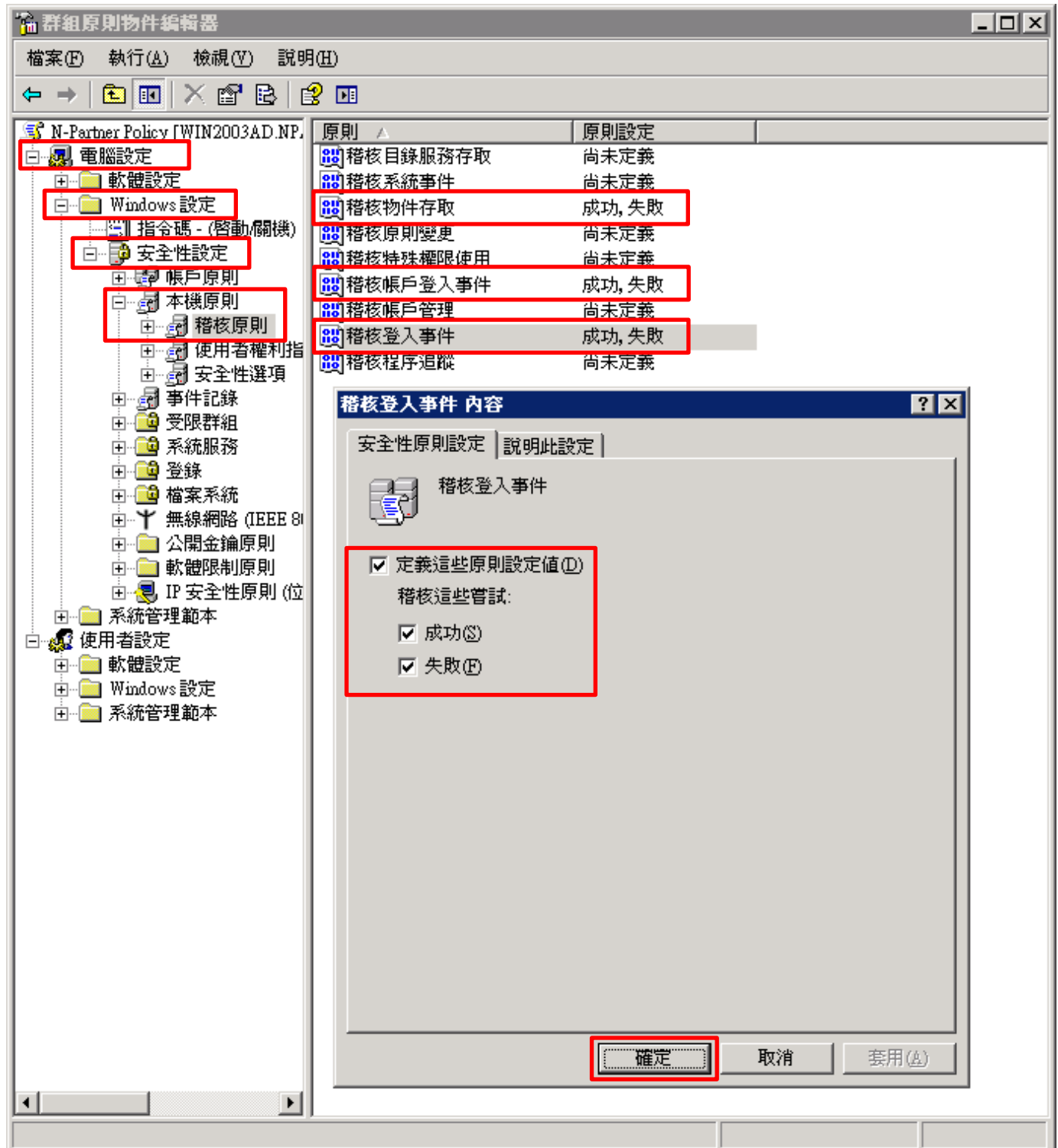
(4) 編輯群組原則物件

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



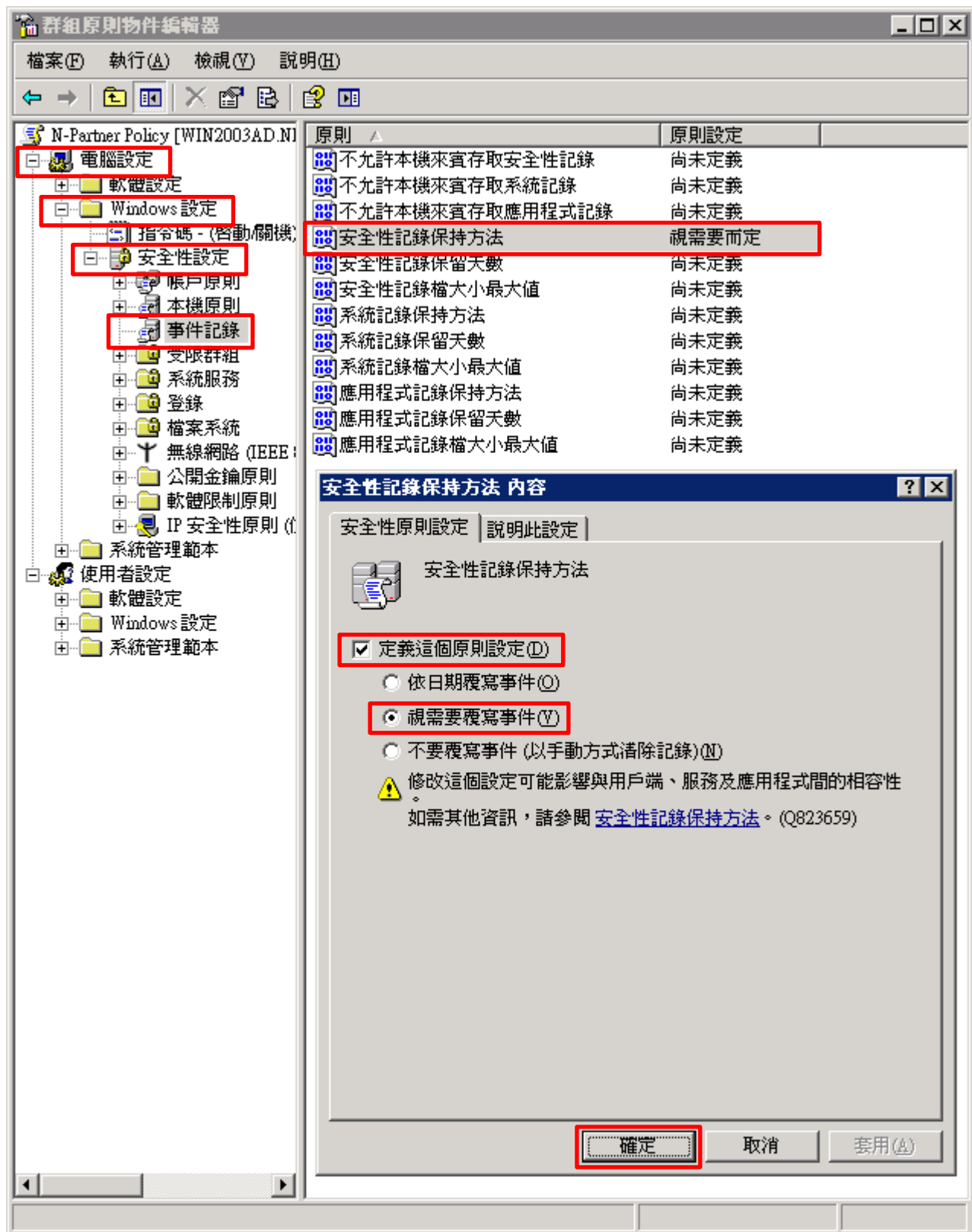
(5) 本機原則：稽核原則

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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定值] & [成功] & [失敗] -> 按 [確定]



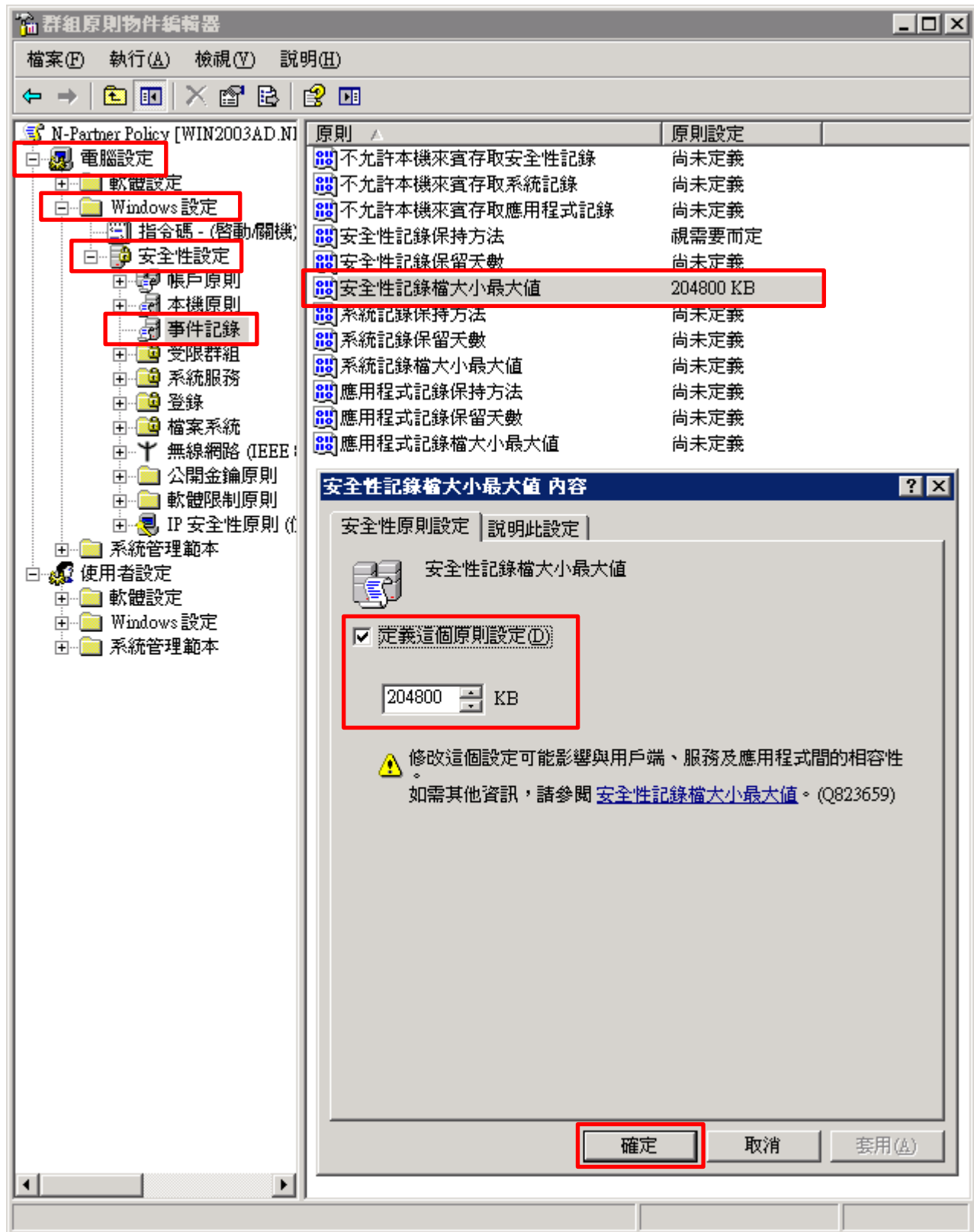
(6) 事件記錄檔：安全性記錄保持方法

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



(7) 事件記錄檔：安全性記錄檔大小最大值

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



(8) 在 Windows File 伺服器，開啟 [命令提示字元]



命令提示字元

(9)更新群組原則，

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



(10) 查看群組原則套用情形

C:\> gpresult /v

```
命令提示字元
C:\>gpresult /v

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

建立於 2021/6/25 上午 09:54:06

WIN2003\Administrator 的 RSOP 資料在 WIN2003: 記錄模式
-----

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

電腦設定
-----
CN=WIN2003,OU=Servers,DC=npartner,DC=local
上次套用的群組原則: 2021/6/25 於 上午 09:51:33
套用的群組原則來自: Win2003AD.npartner.local
群組原則低速連結閾值: 500 kbps
網域名稱: npartner
網域類型: Windows 2000

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

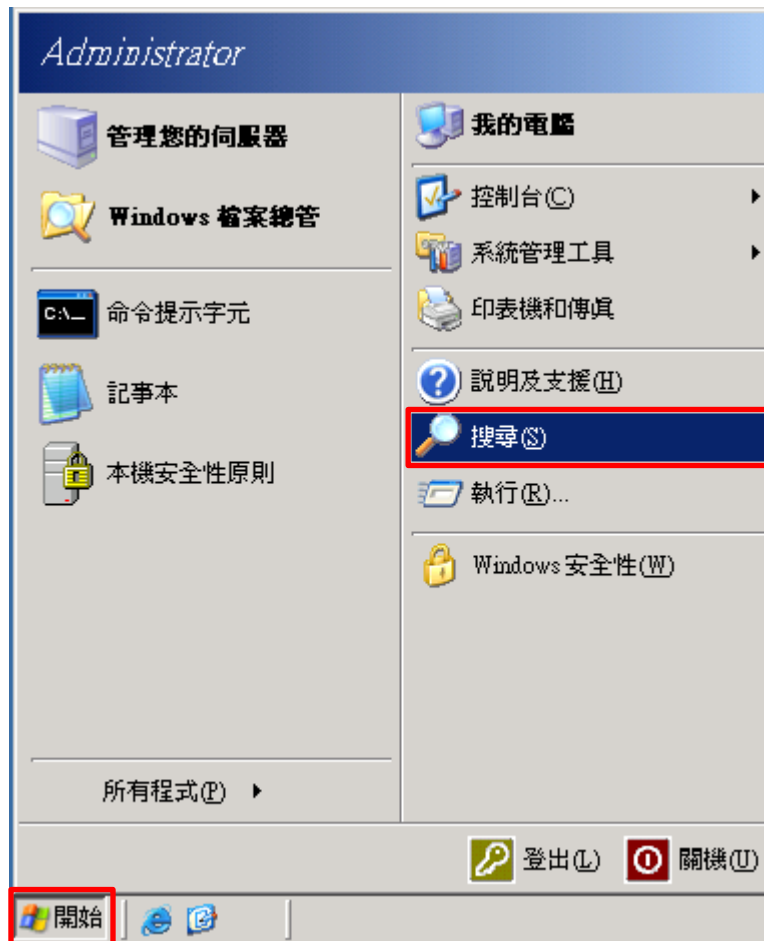


## 3.2 工作群組

### 3.2.1 稽核原則設定

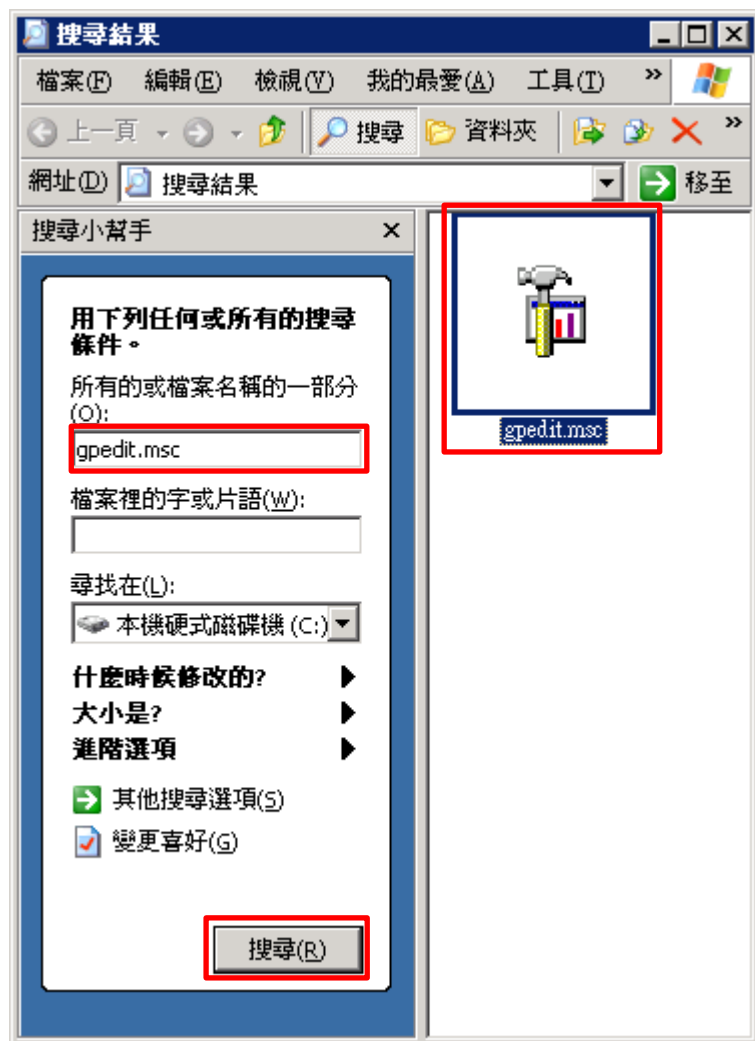
(1) 開啟搜尋

按 [開始] -> 點選 [搜尋]



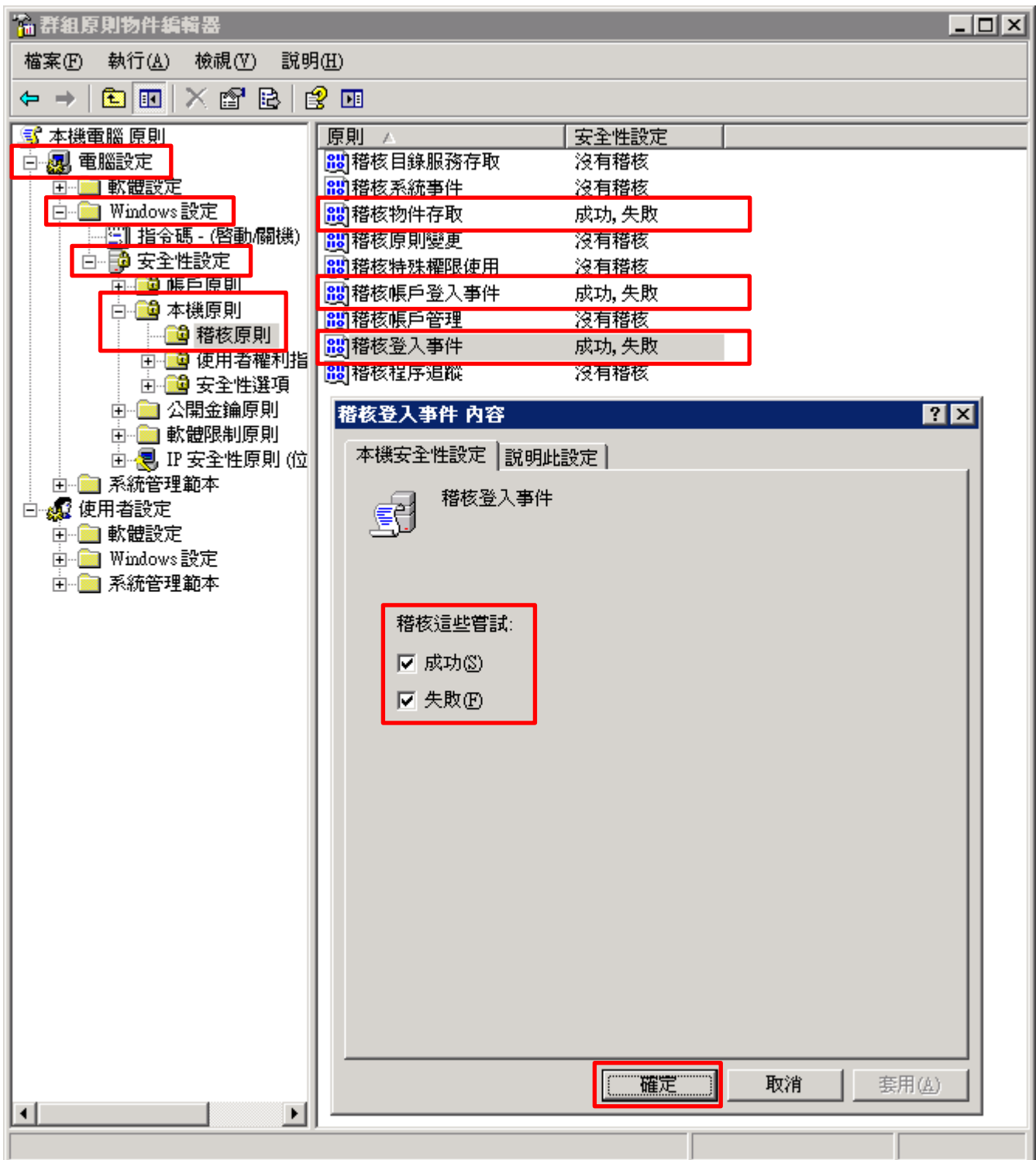
(2) 搜尋群組原則物件編輯器

輸入 `gpedit.msc` -> 按 [搜尋] -> 點選 [`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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



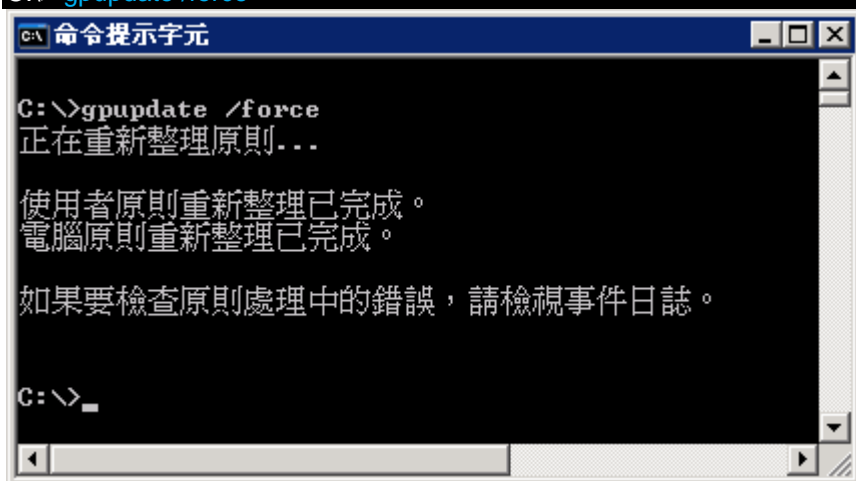
(4) 開啟 [命令提示字元]



命令提示字元

(5) 更新群組原則

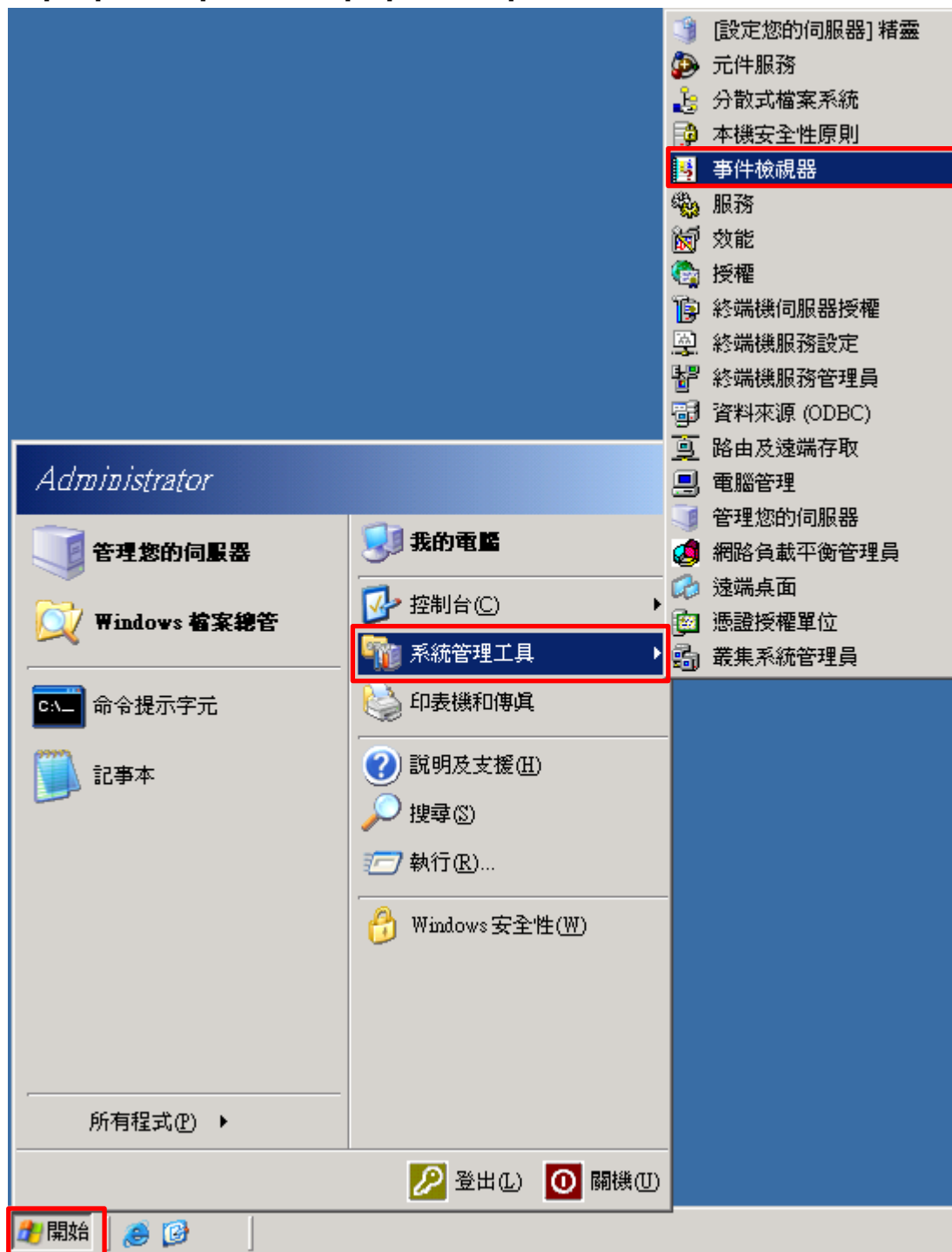
C:\> gpupdate /force



### 3.2.2 事件檔案設定

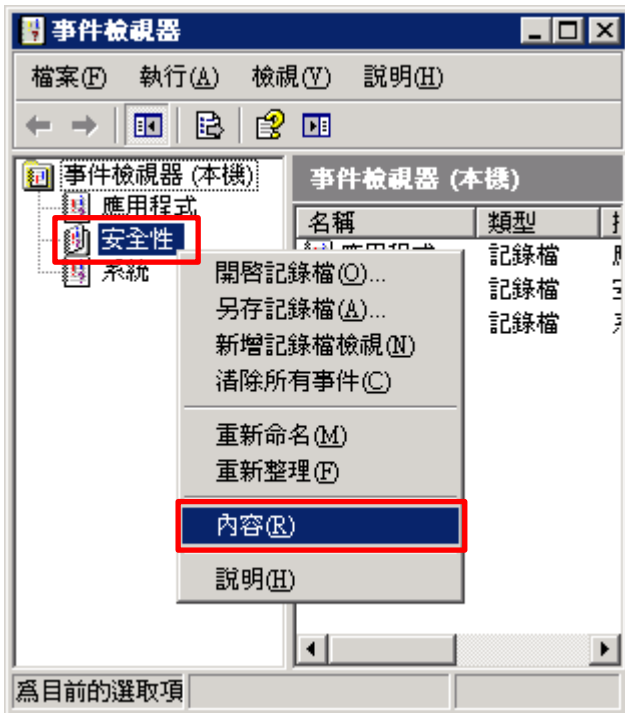
#### (1) 開啟事件檢視器

按 [開始] -> 點選 [系統管理工具] -> [事件檢視器]



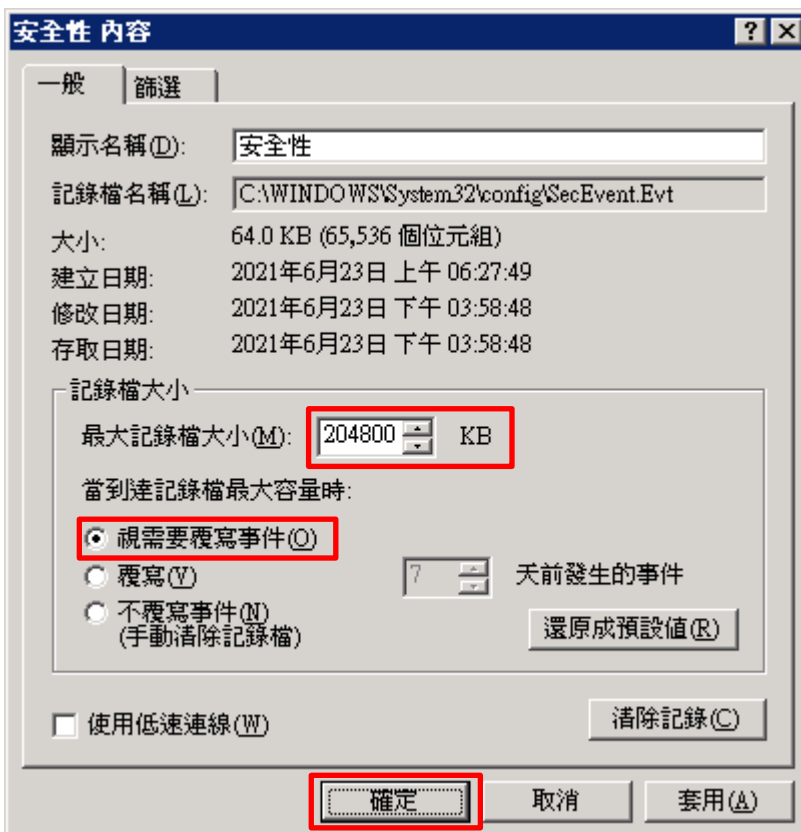
(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



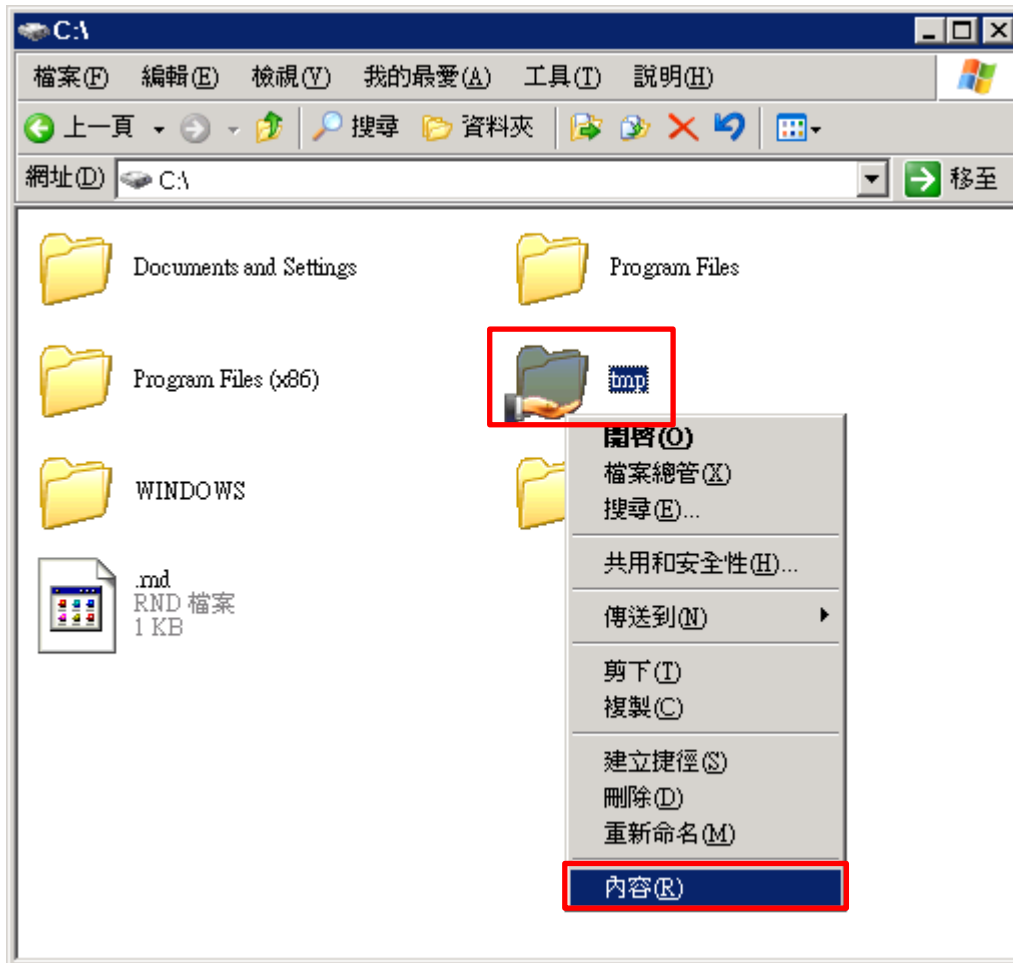
(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]



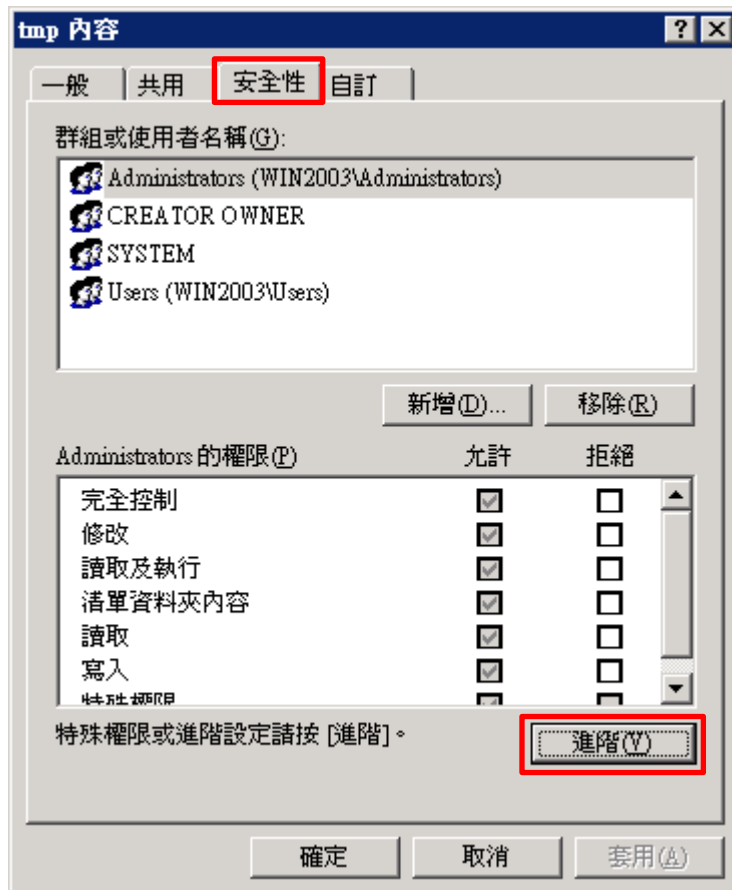
### 3.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]

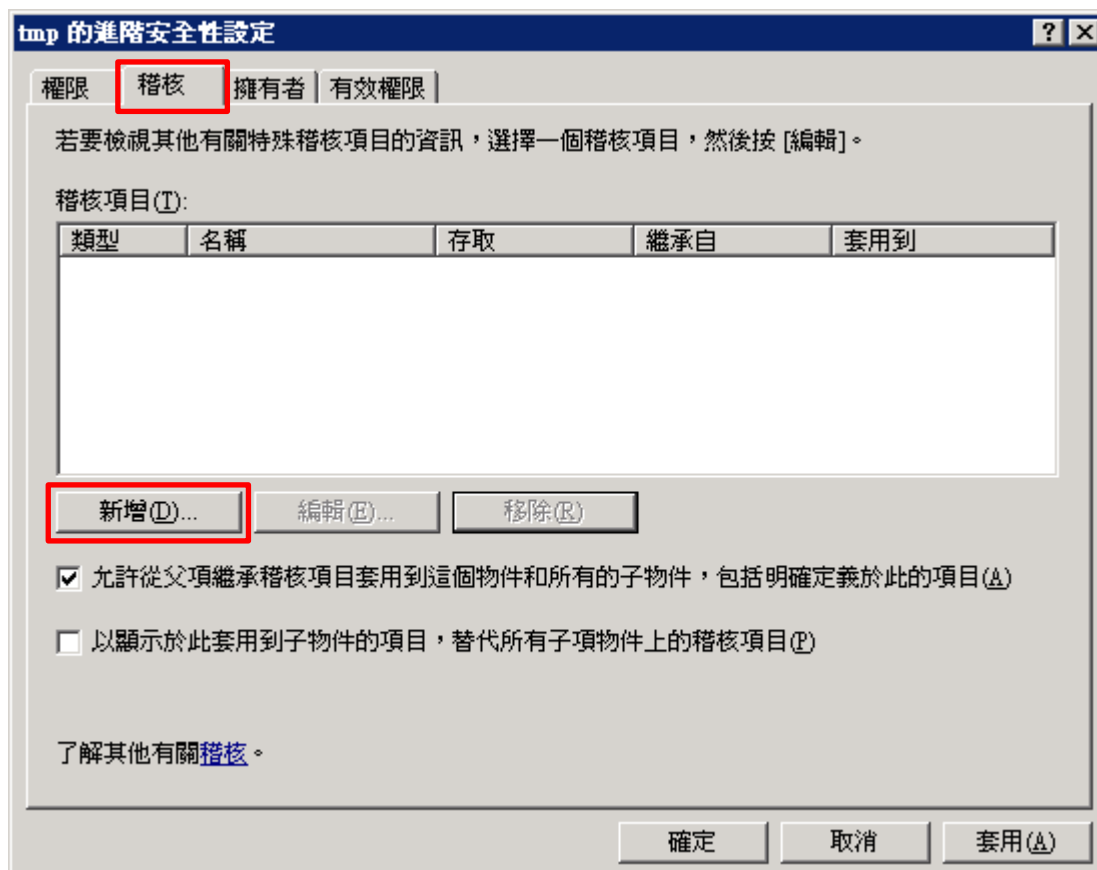




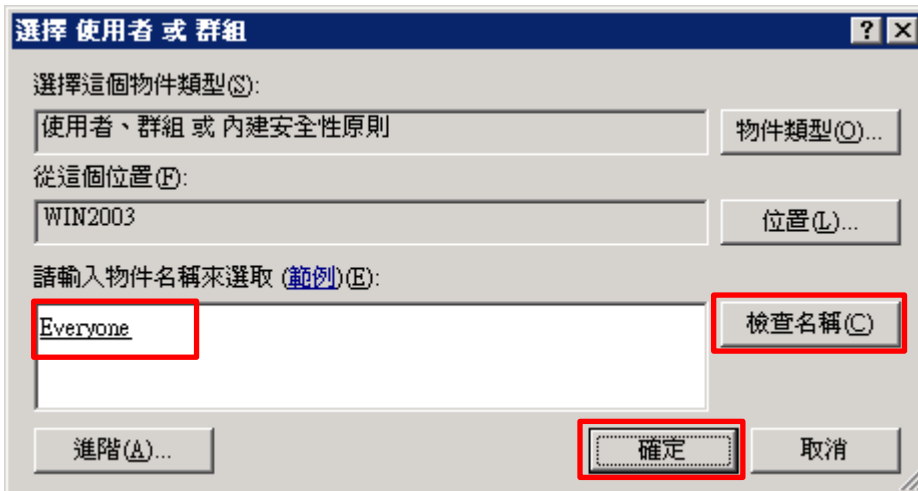
(2) 點選 [安全性] 頁面 -> 按 [進階]



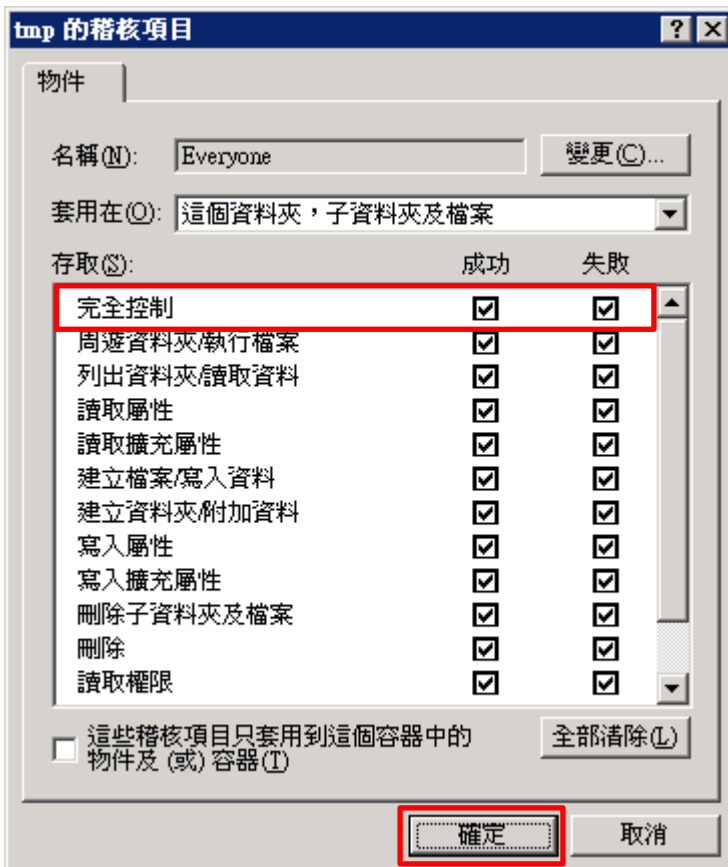
(3) 點選 [稽核] 頁面 -> 按 [新增]



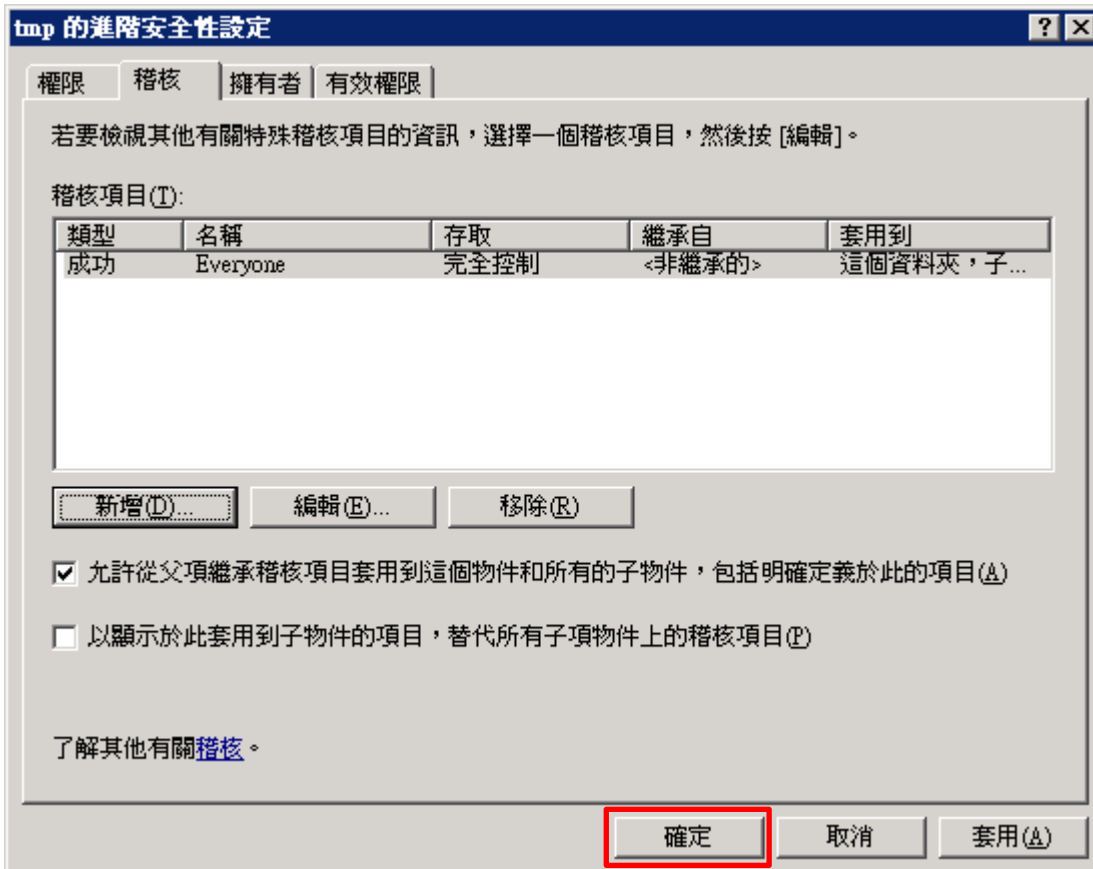
(4) 物件名稱輸入 **Everyone** 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



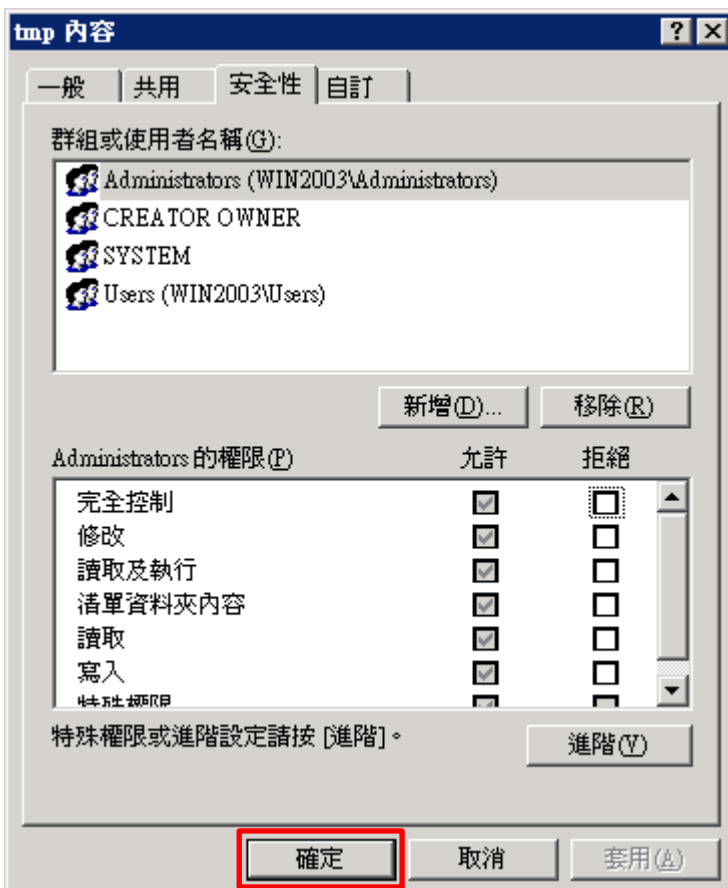
(5) 存取類型 [成功] 和 [失敗] 項目都勾選 [完全控制] -> 按 [確定]



(6) 稽核項目顯示 Everyone 名稱 -> 按 [確定]



(7) 按 [確定]



## 4. Windows 2008

Windows 稽核原則設定 詳細說明請參考前言的[稽核原則建議連結](#)

※ 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

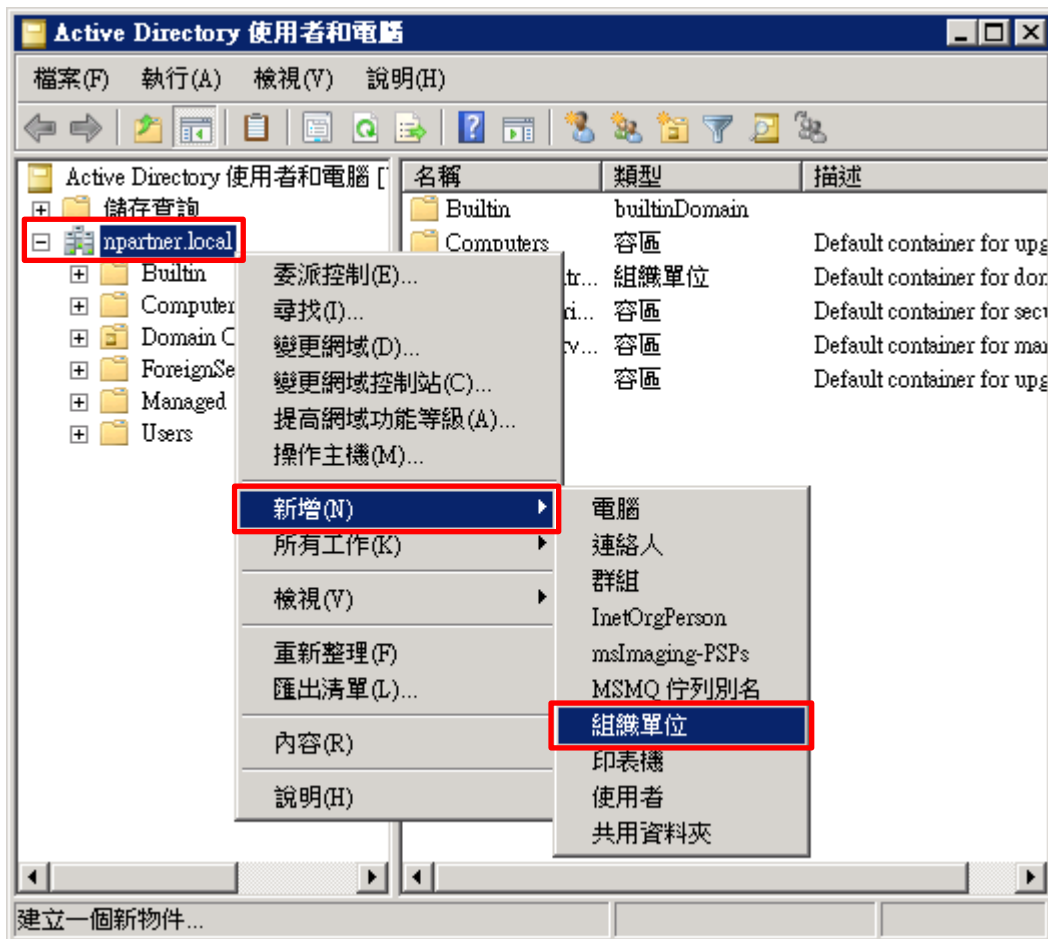
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



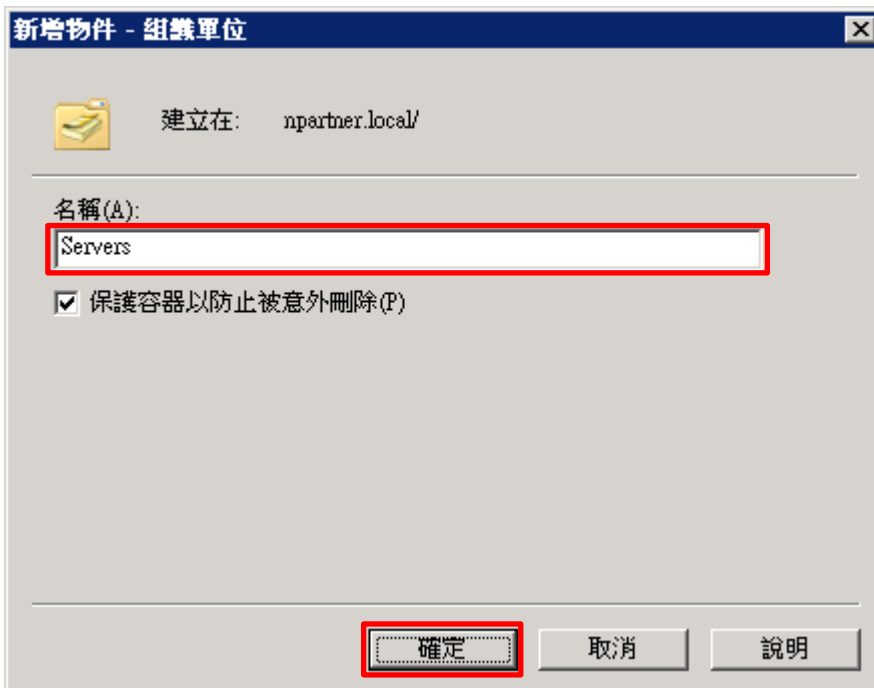
(2) 新增組織單位

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



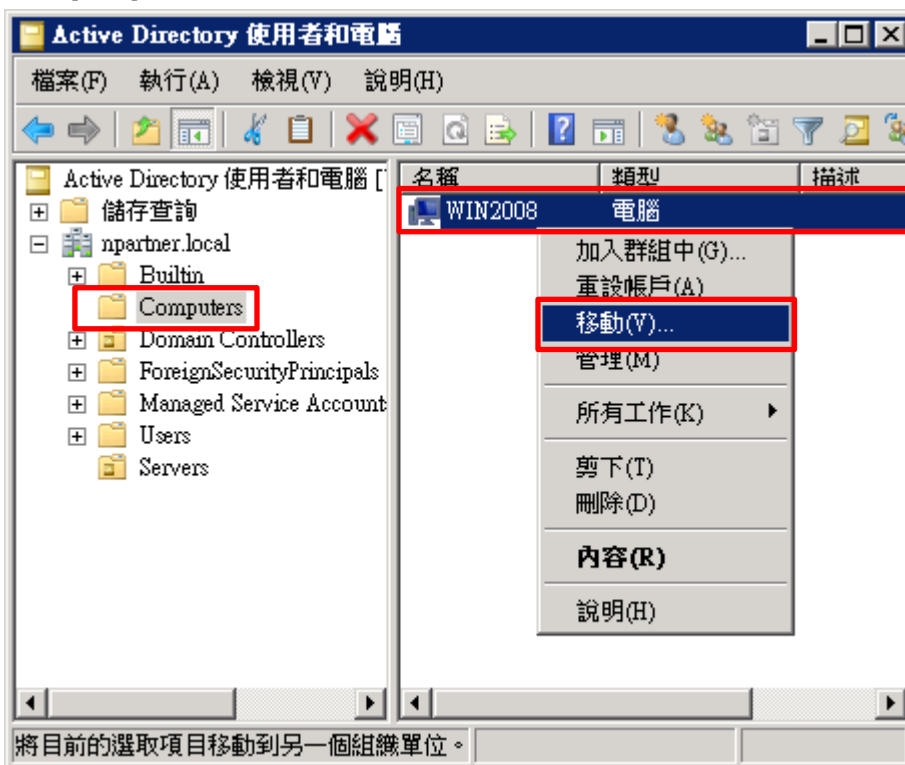
### (3) 輸入組織單位名稱

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



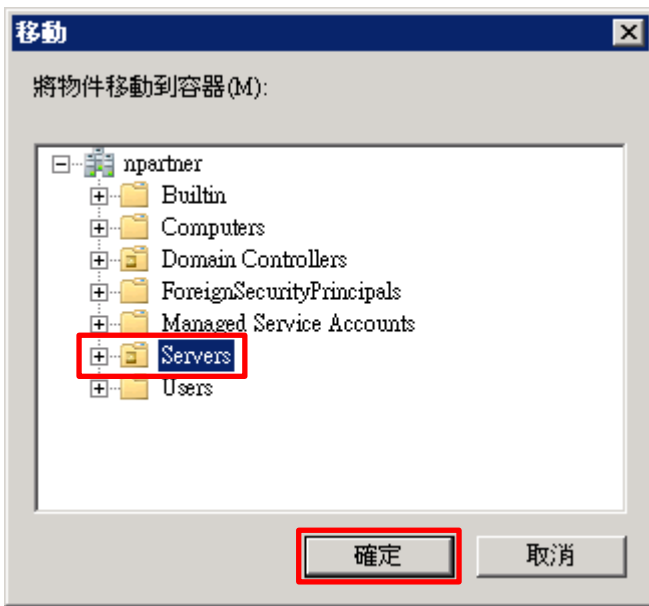
### (4) 移動伺服器至新的組織單位

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



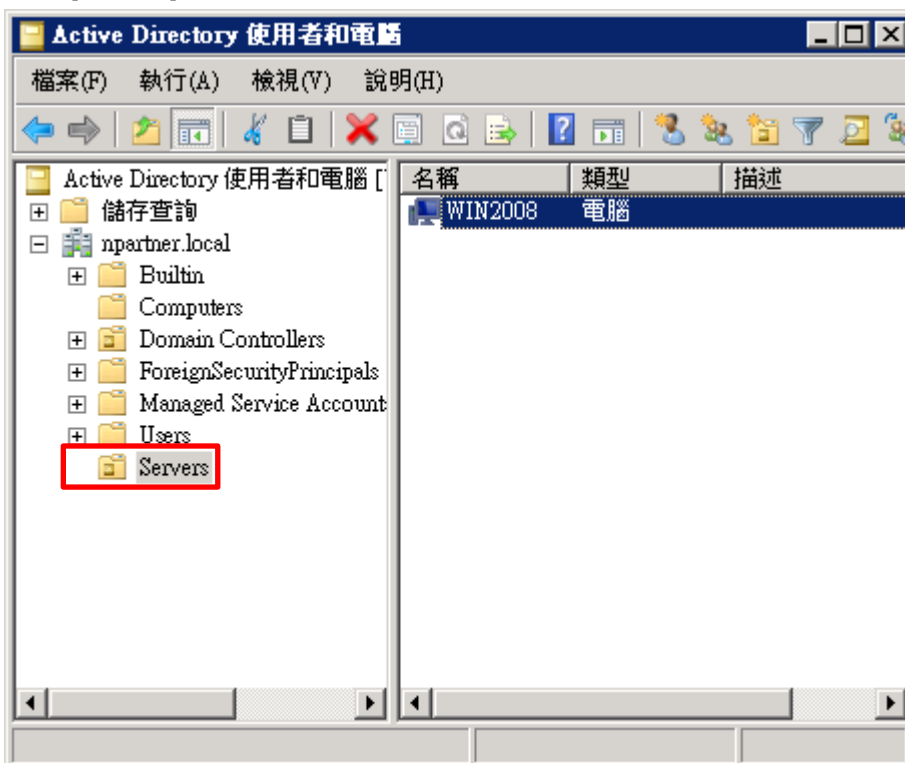
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [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 Win2008 File 伺服器已移動



## 4.1.2 群組原則設定

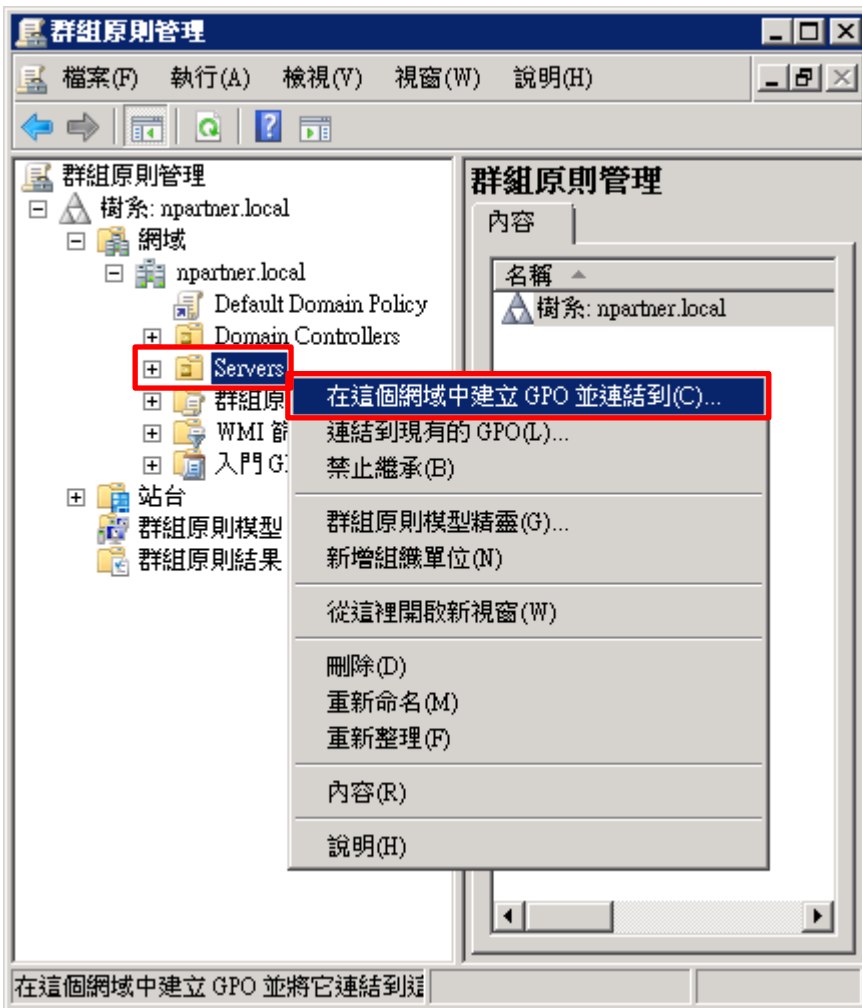
### (1) 開啟群組原則管理

開啟 [群組原則管理]



### (2) 在 Servers 組織單位，新增群組原則物件

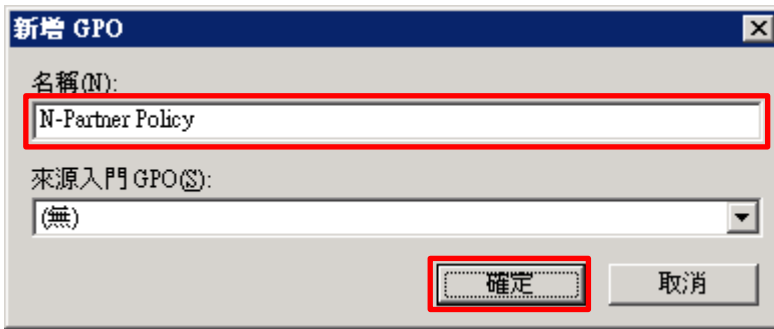
在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





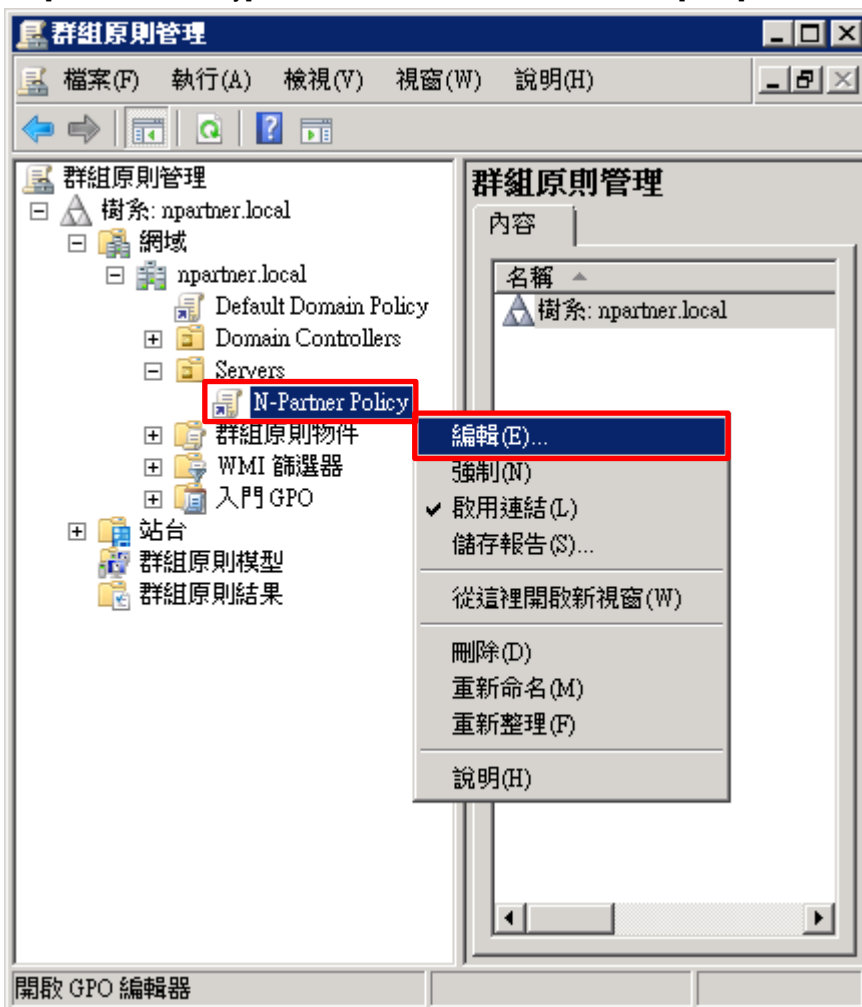
(3) 輸入群組原則物件名稱

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



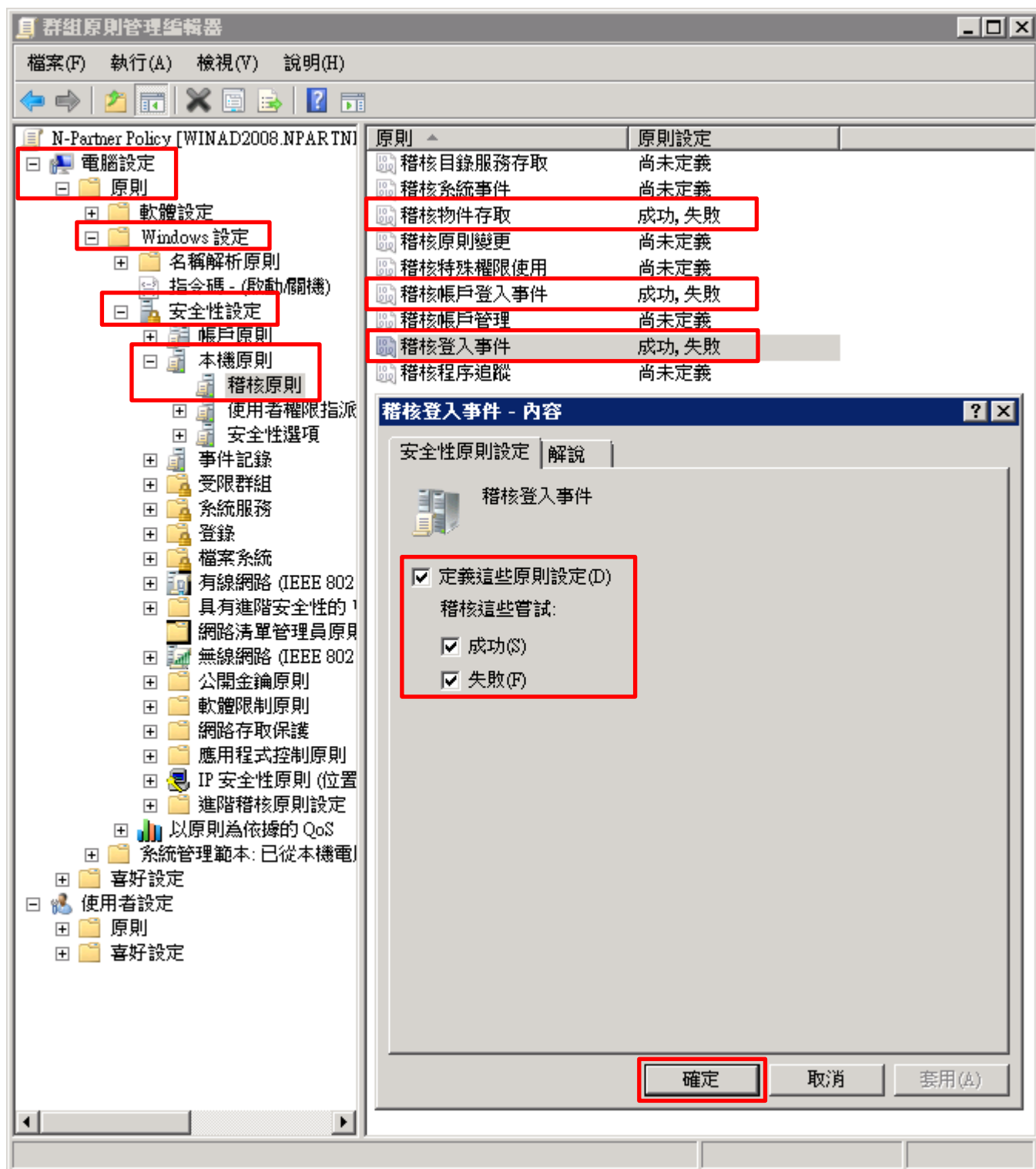
(4) 編輯群組原則物件

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



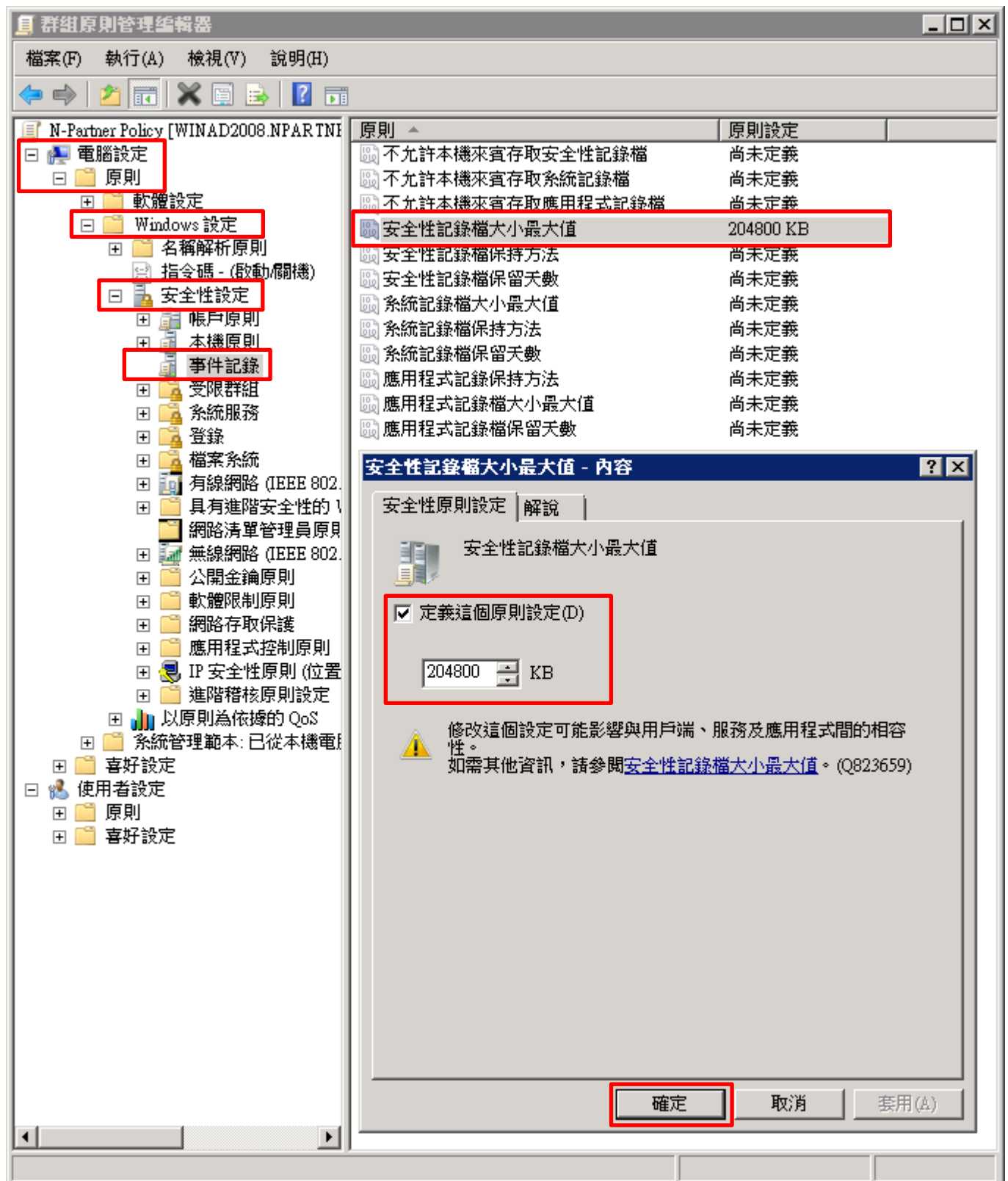
(5) 本機原則：稽核原則

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



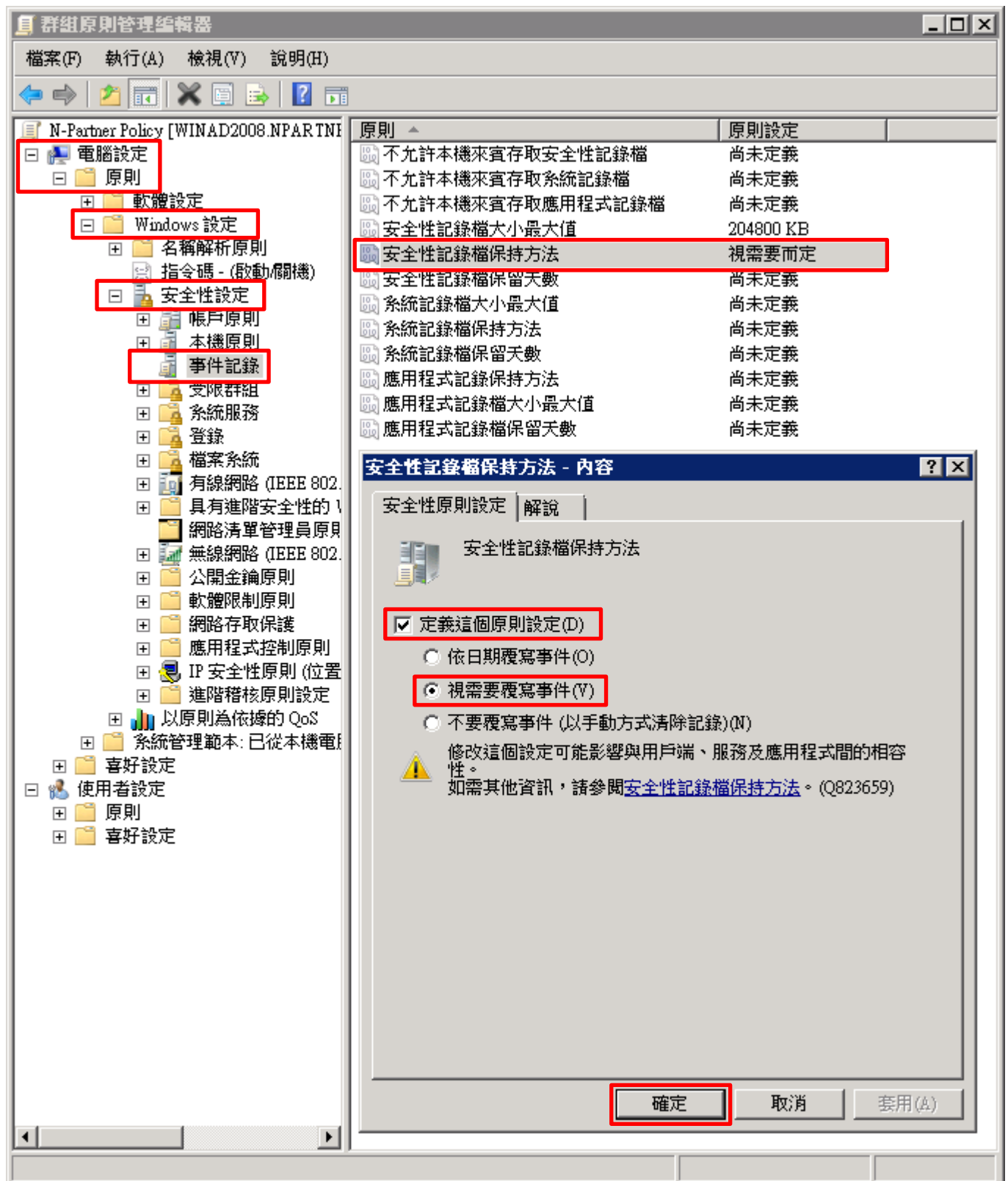
(6) 事件記錄檔：安全性記錄檔大小最大值

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



(7) 事件記錄檔：安全性記錄檔保持方法

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



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



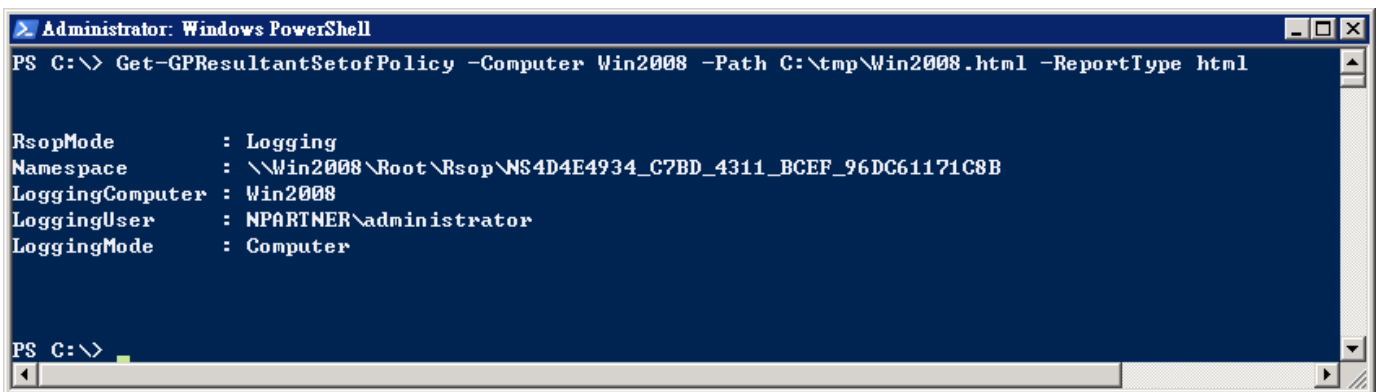
(9) 更新群組原則

PS C:\> gpupdate /force



(10) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell] -> 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 Windows File 伺服器名稱和資料夾路徑檔案名稱

(11) 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: 2022/3/15 下午 04:22:27 顯示全部

**摘要** 顯示

**電腦設定** 隱藏

**原則** 隱藏

**Windows 設定** 隱藏

**安全性設定** 隱藏

帳戶原則/密碼規則		顯示
帳戶原則/帳戶鎖定原則		顯示
帳戶原則/Kerberos 原則		顯示
本機原則/稽核原則		隱藏

原則	設定	優勢 GPO
稽核物件存取	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/使用者權限指派		顯示
本機原則/安全性選項		顯示
事件記錄檔		隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定		顯示
公開金鑰原則/加密檔案系統		顯示
公開金鑰原則/被信任的根憑證授權單位		顯示

**使用者設定** 顯示

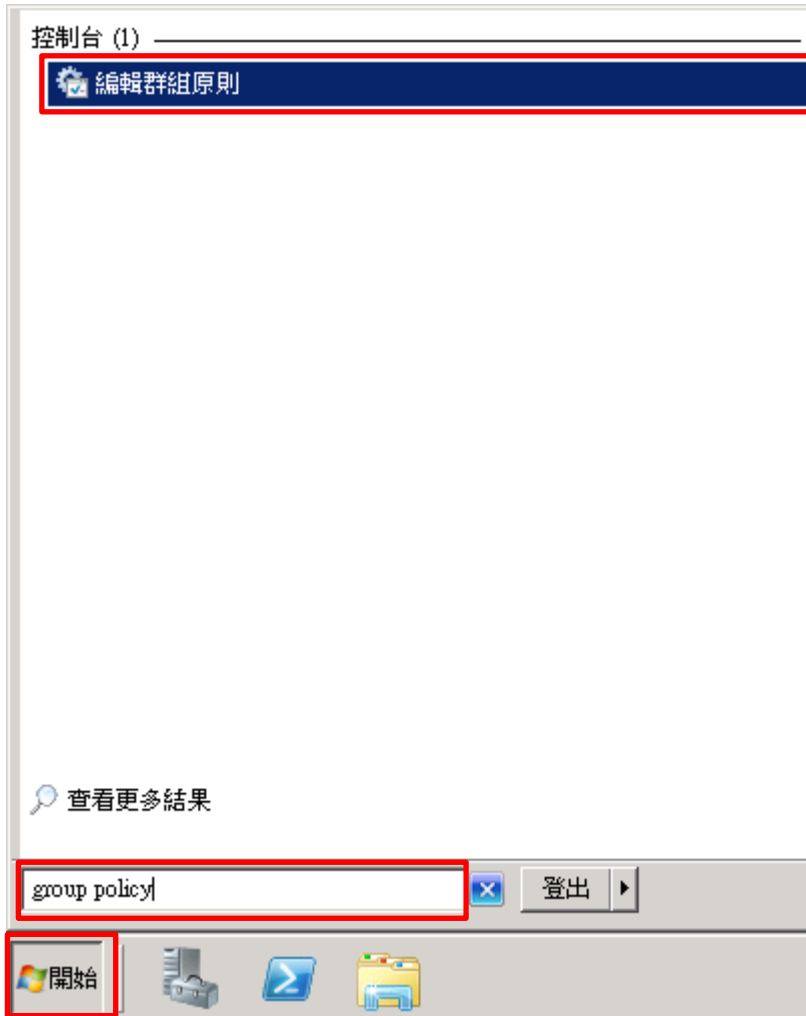
電腦 | 受保護模式: 關閉 | 100%

## 4.2 工作群組

### 4.2.1 稽核原則設定

(1) 開啟 [本機群組原則編輯器]

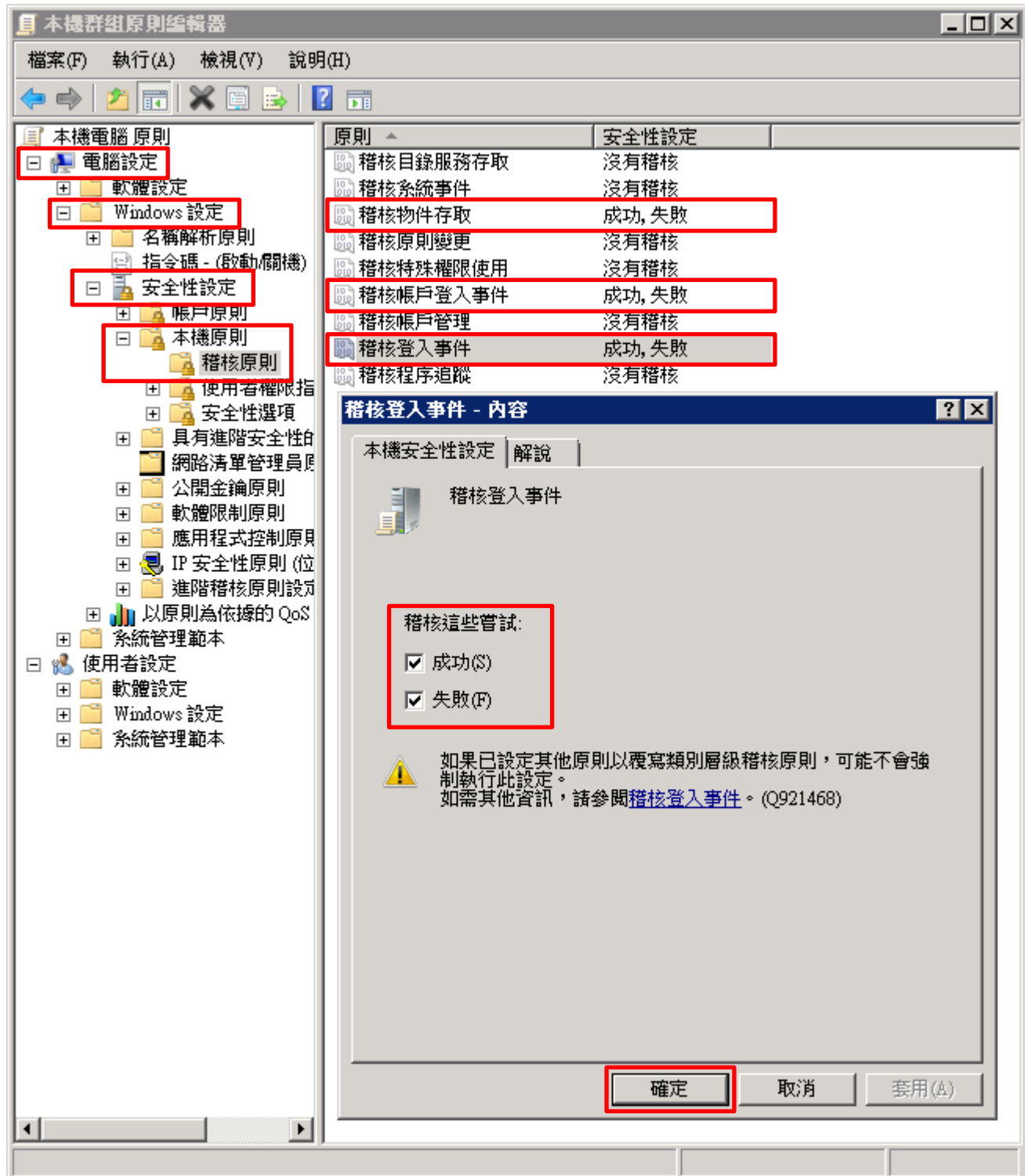
點選 [開始] -> 在 [搜尋] 欄位，輸入 `group policy` -> 點選 [編輯群組原則]





(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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

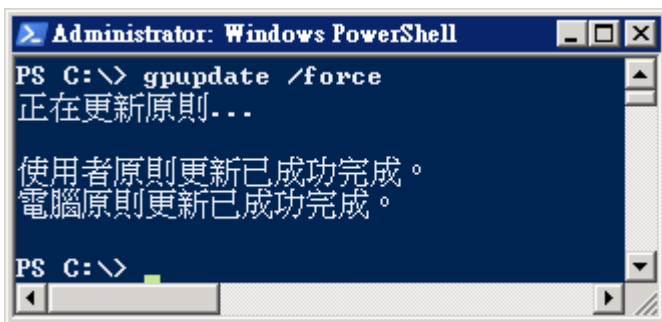


(3) 開啟 [Windows PowerShell] .



(4) 更新群組原則

PS C:\> gpupdate /force



(5) 查看群組原則套用情形

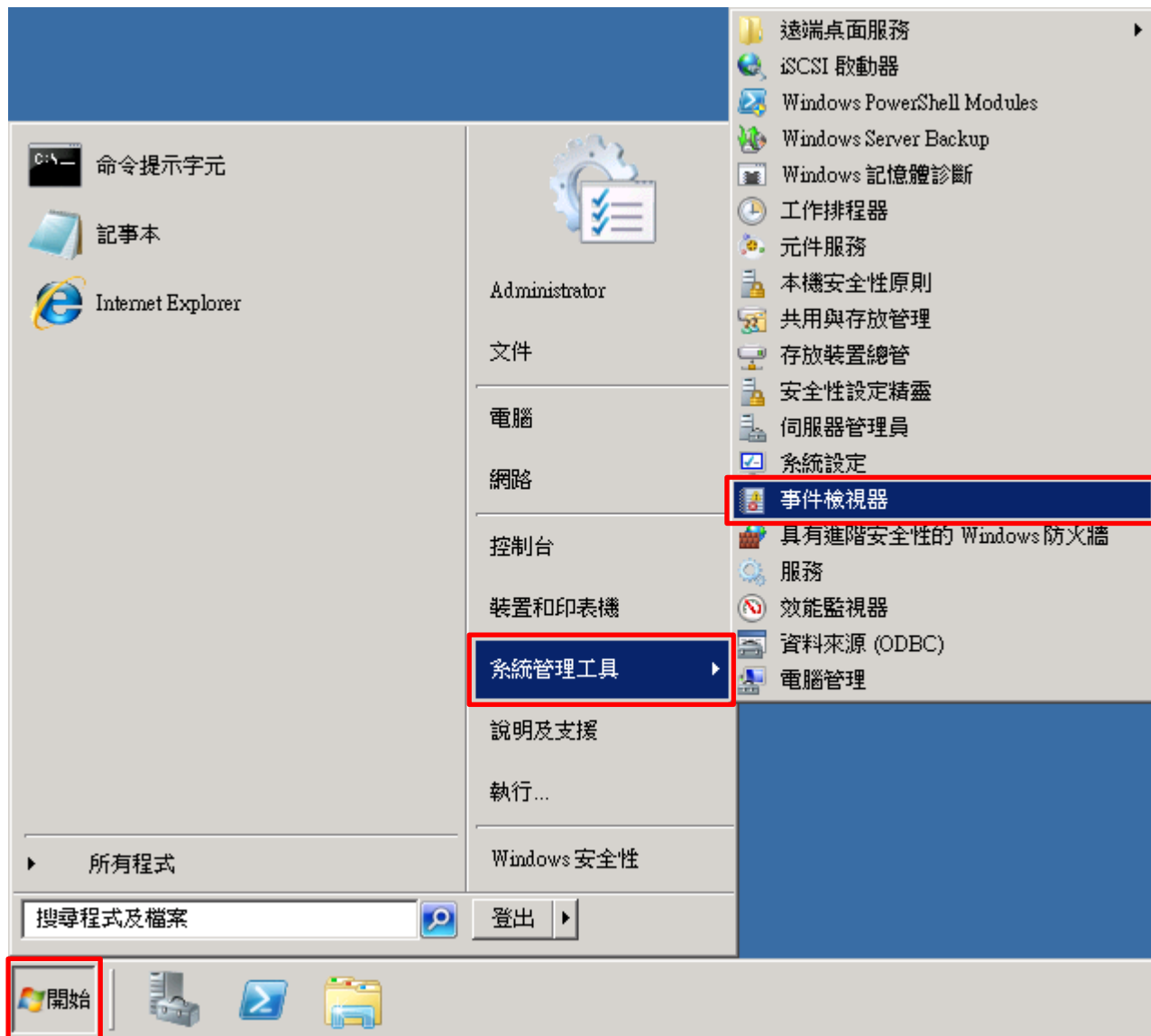
PS C:\> auditpol /get /category:\*

```
Administrator: Windows PowerShell
PS C:\> 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                成功及失敗
帳戶鎖定            成功及失敗
IPsec 主要模式      成功及失敗
IPsec 快速模式      成功及失敗
IPsec 延伸模式      成功及失敗
特殊登入            成功及失敗
其他登入/登出事件  成功及失敗
網路原則伺服器      成功及失敗
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 成功及失敗
其他帳戶登入事件    成功及失敗
Kerberos 驗證服務    成功及失敗
認證驗證            成功及失敗
PS C:\>
```

### 3.2.2 事件檔案設定

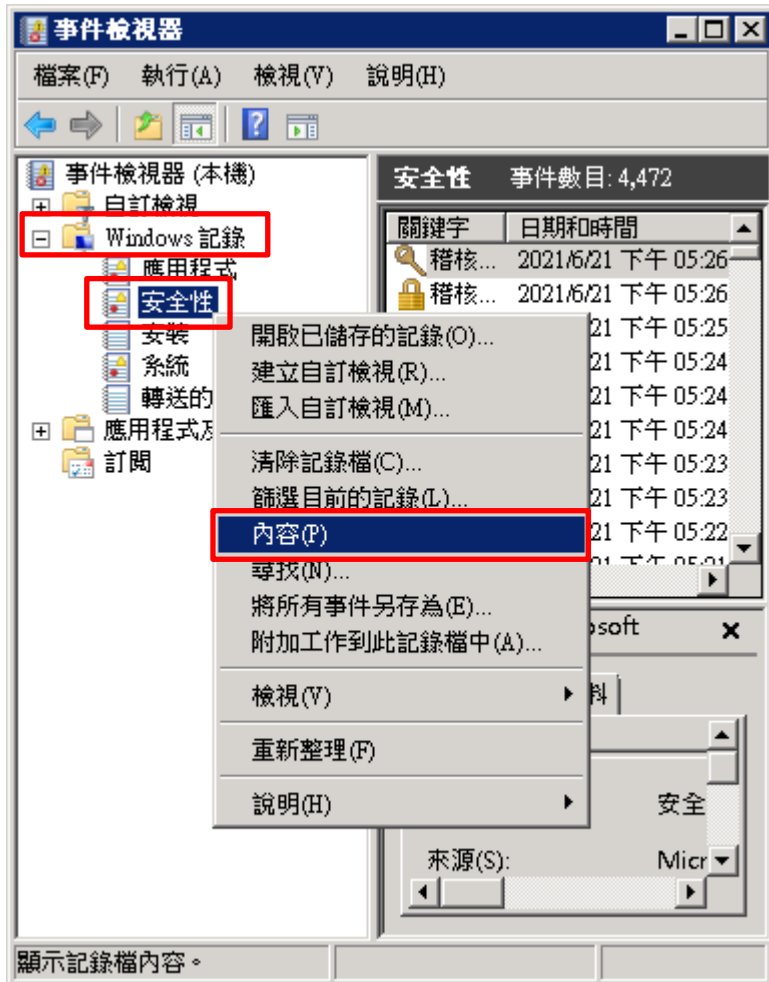
#### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



(2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx

記錄檔大小: 4.07 MB(4,263,936 位元組)

建立日期: 2021年6月21日 下午 09:05:32

修改日期: 2021年6月21日 下午 05:33:07

存取日期: 2021年6月21日 下午 09:05:32

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

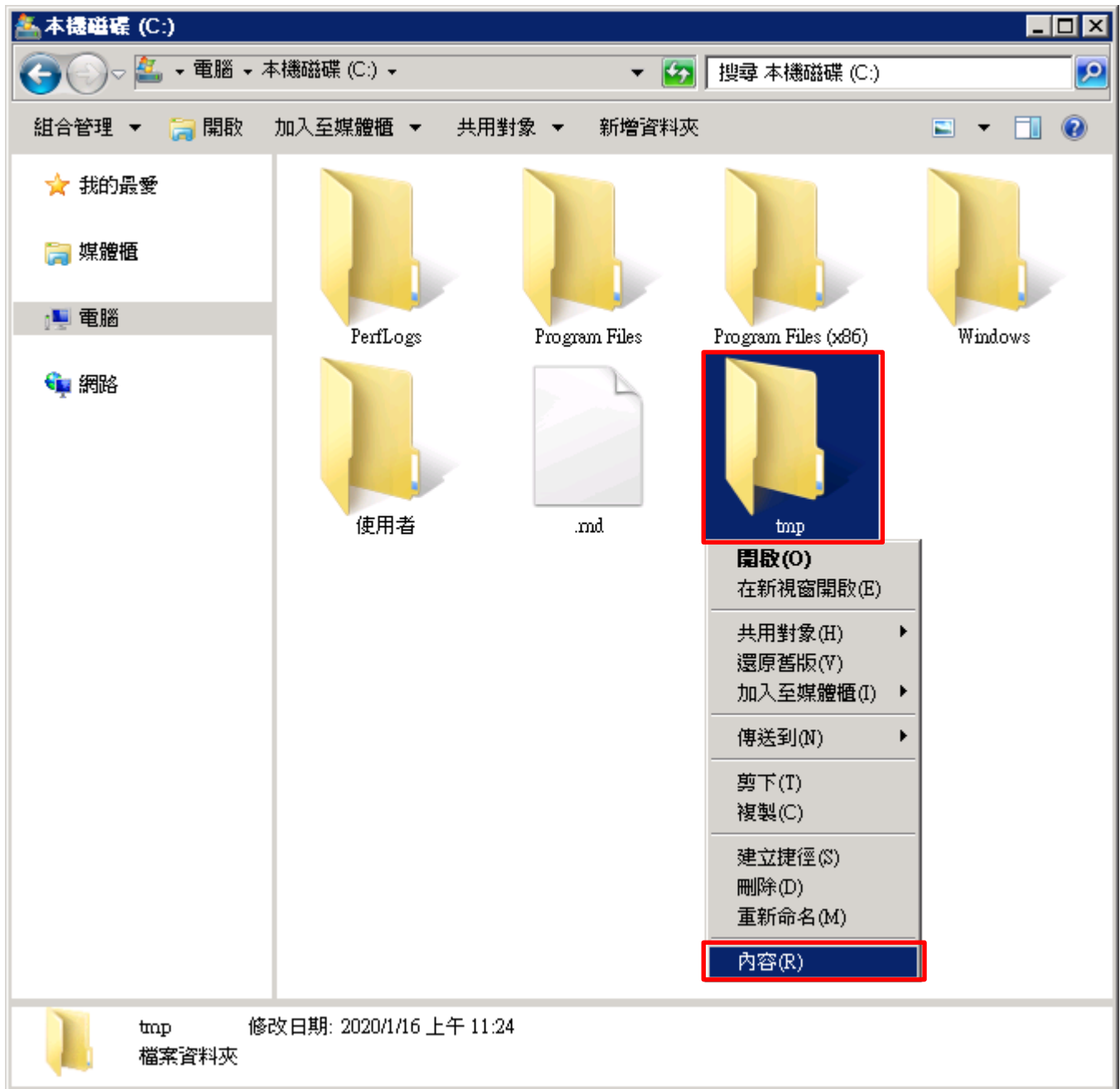
不要覆寫事件 (手動清除記錄檔)(N)

清除記錄檔(R)

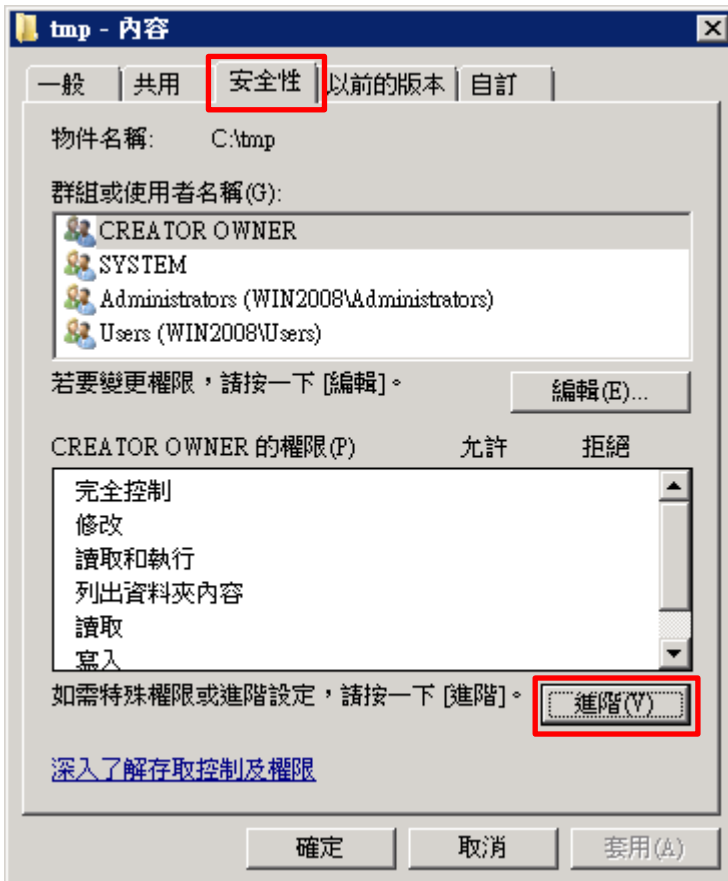
確定 取消 套用(P)

### 3.3 稽核資料夾設定

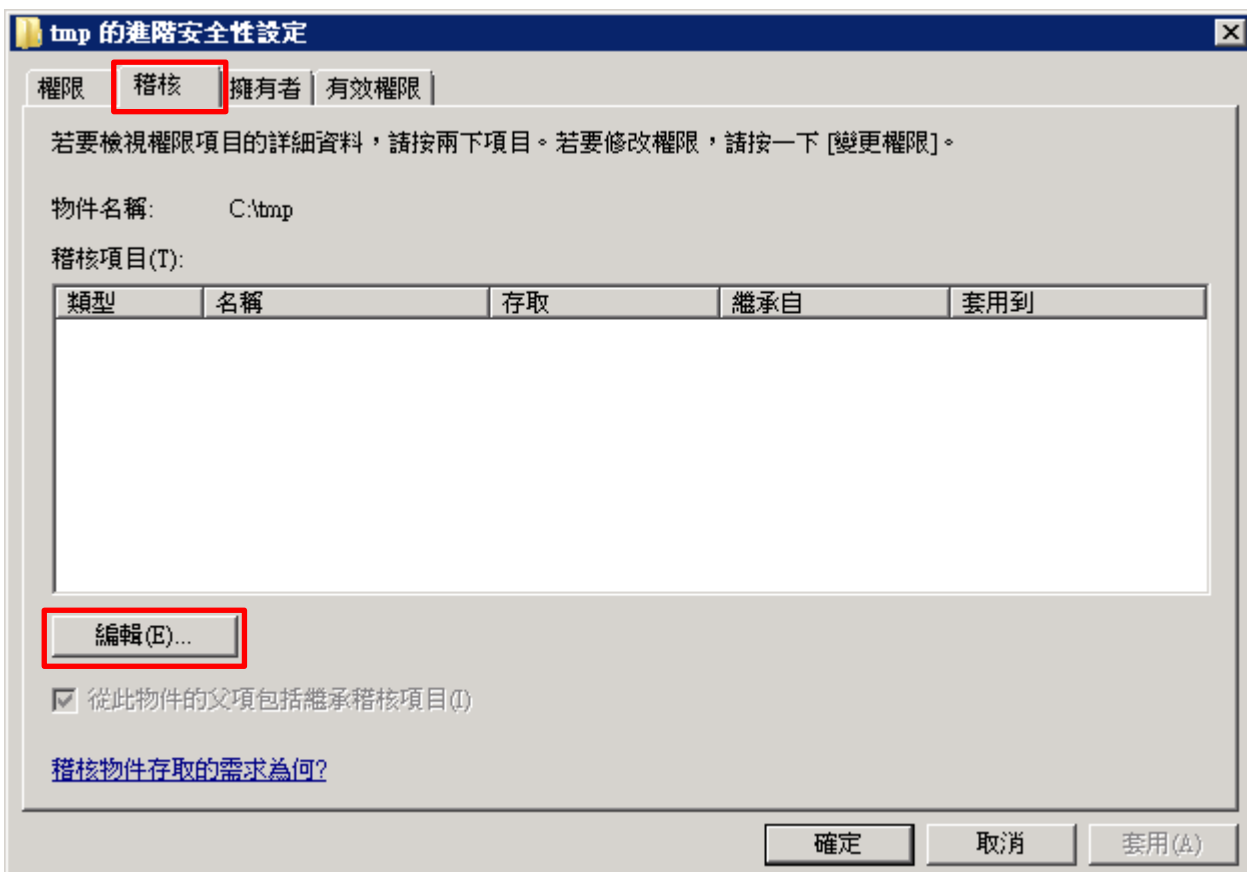
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



(2) 點選 [安全性] 頁面 -> 按 [進階]

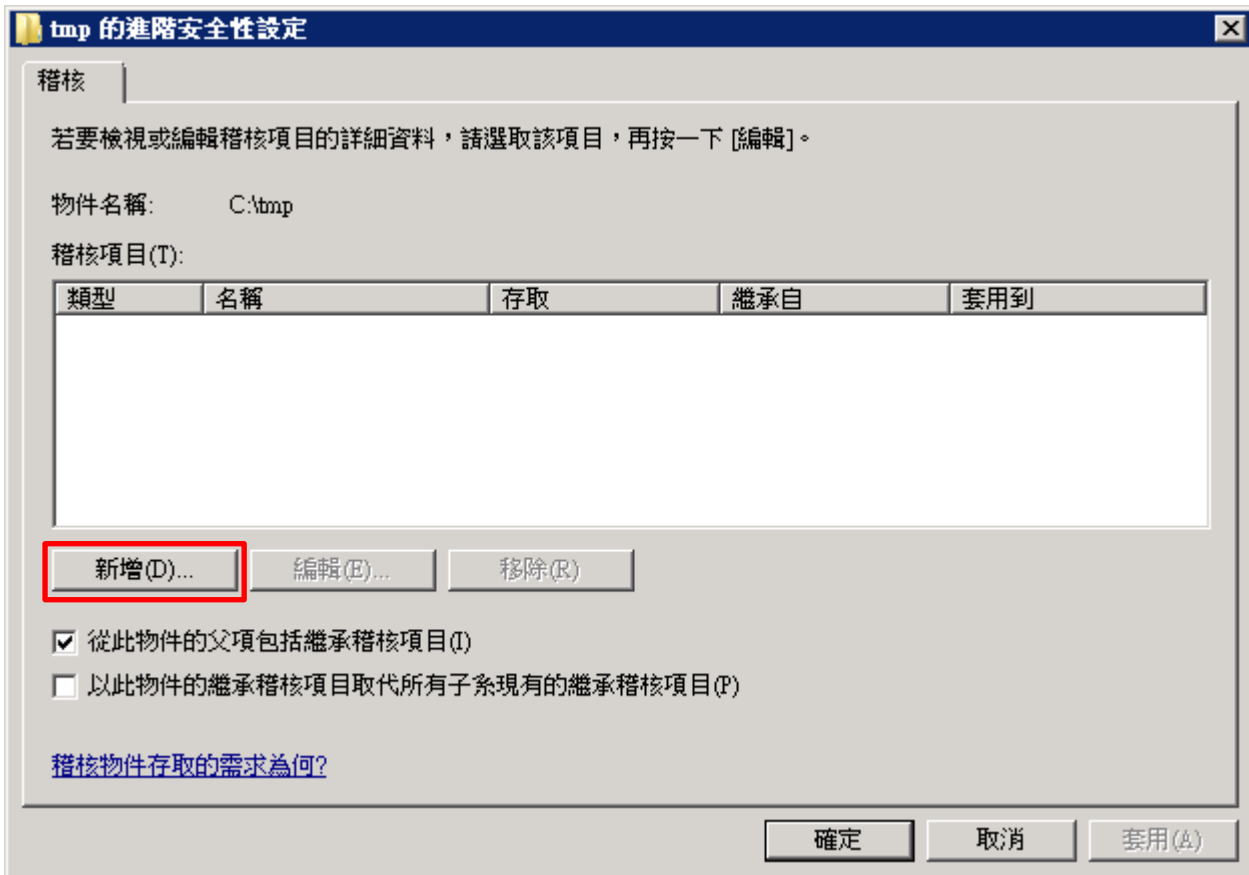


(3) 點選 [稽核] 頁面 -> 按 [編輯]

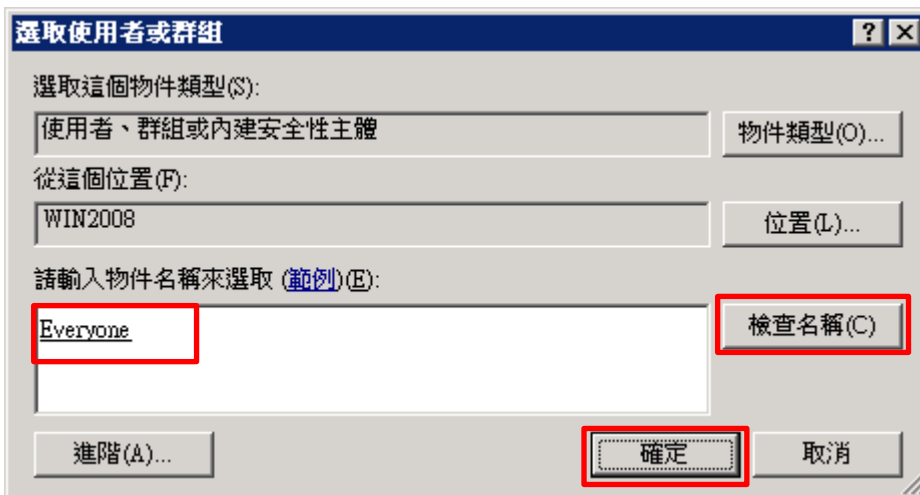




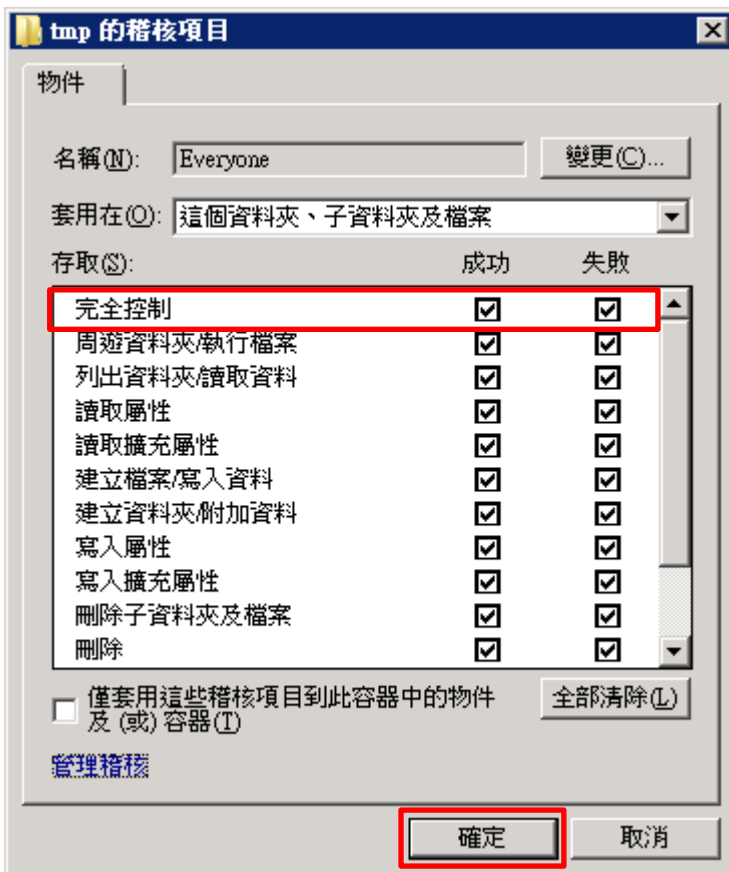
(4) 按 [新增]



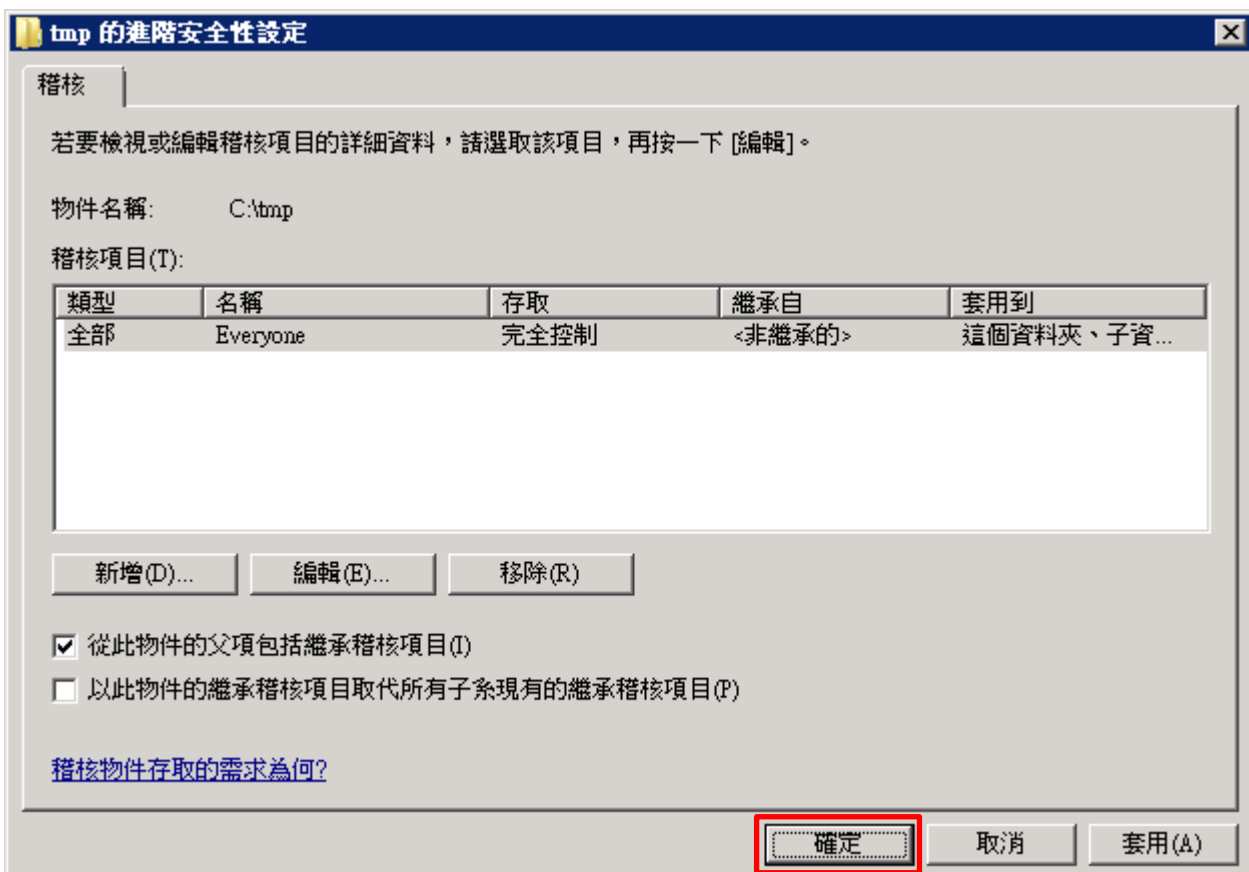
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



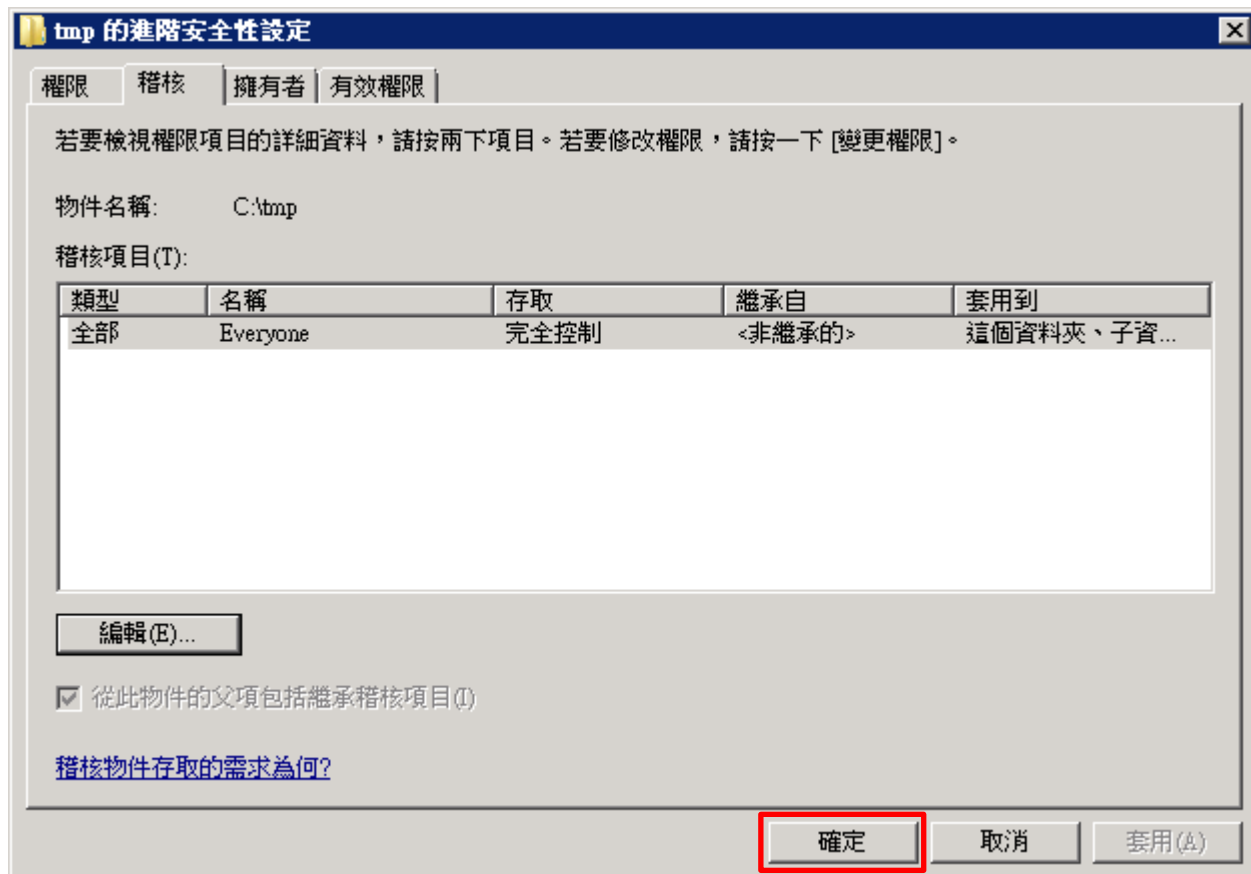
(6) 存取類型 [成功] 和 [失敗] 項目 都勾選 [完全控制] -> 按 [確定]



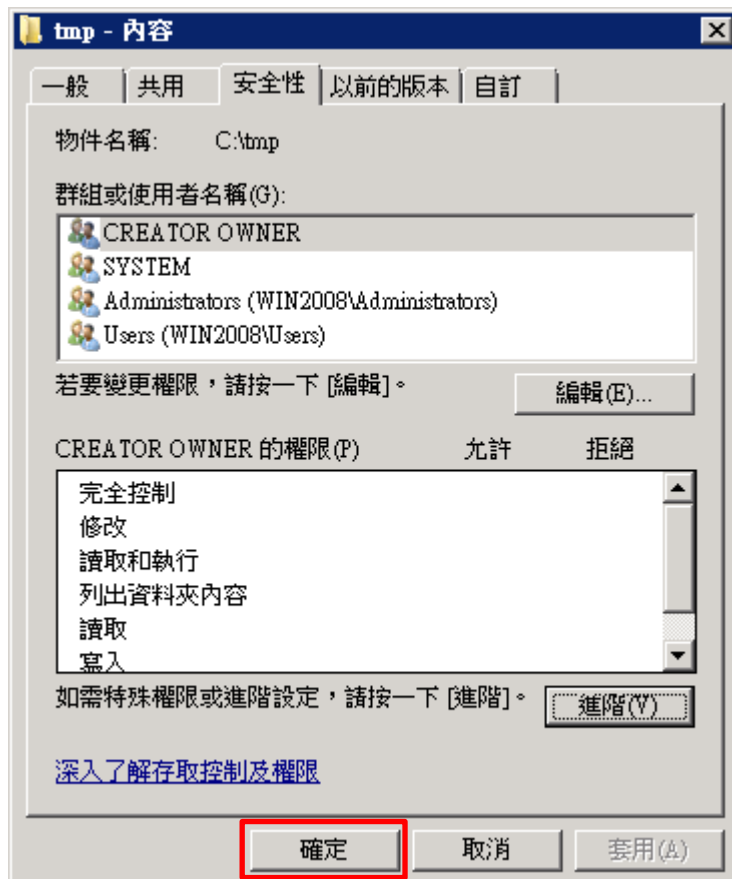
(7) 稽核項目顯示 Everyone 名稱 -> 按 [確定]



(8) 稽核項目顯示 Everyone 名稱 -> 按 [確定]



(9) 按 [確定]



## 5. Windows 2012

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

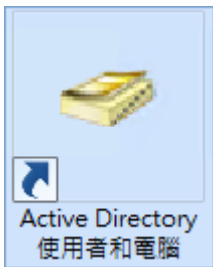
※ 以下分別為網域和工作群組設定方式。

### 5.1 網域

#### 5.1.1 組織單位設定

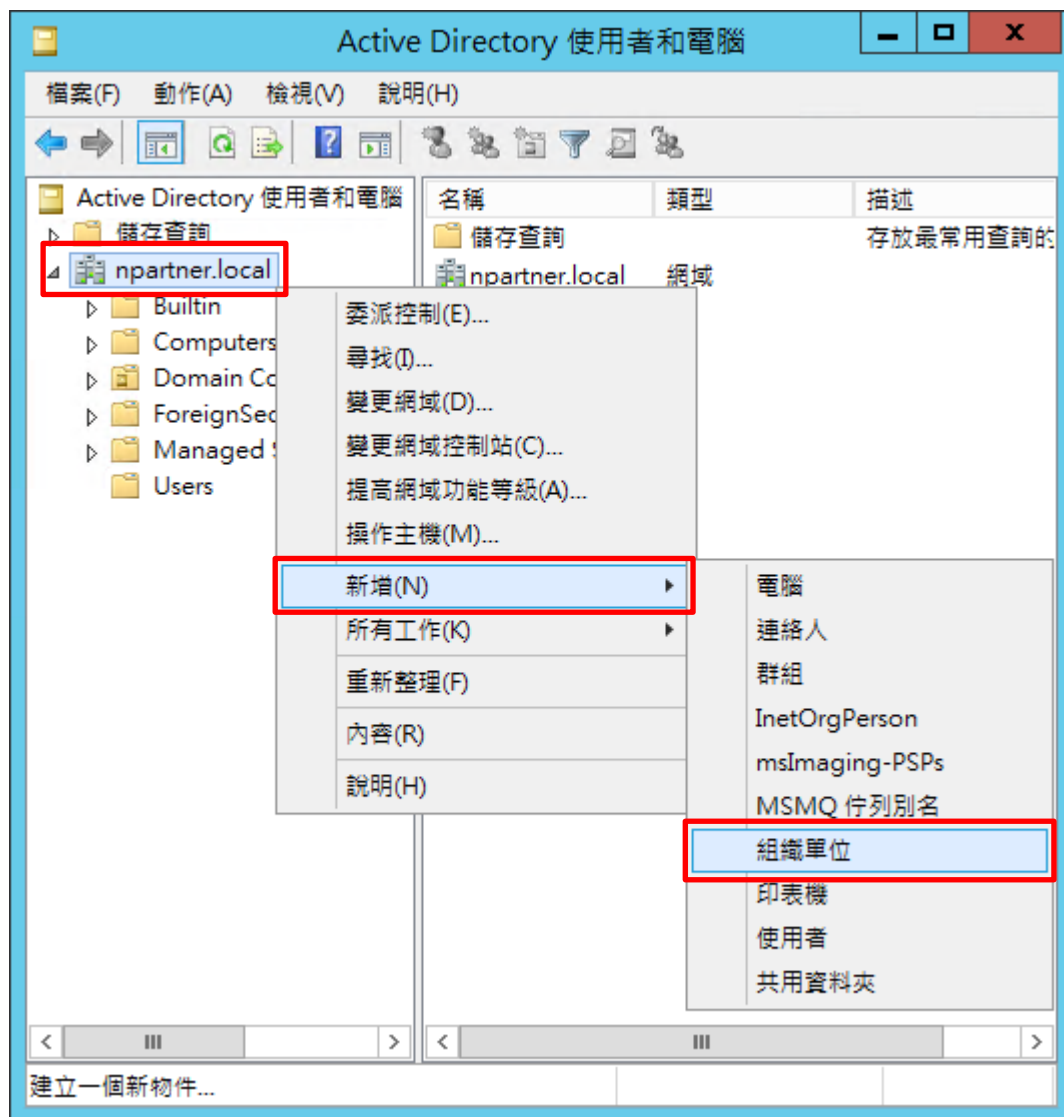
(1) 開啟 AD 使用者和電腦

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 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/

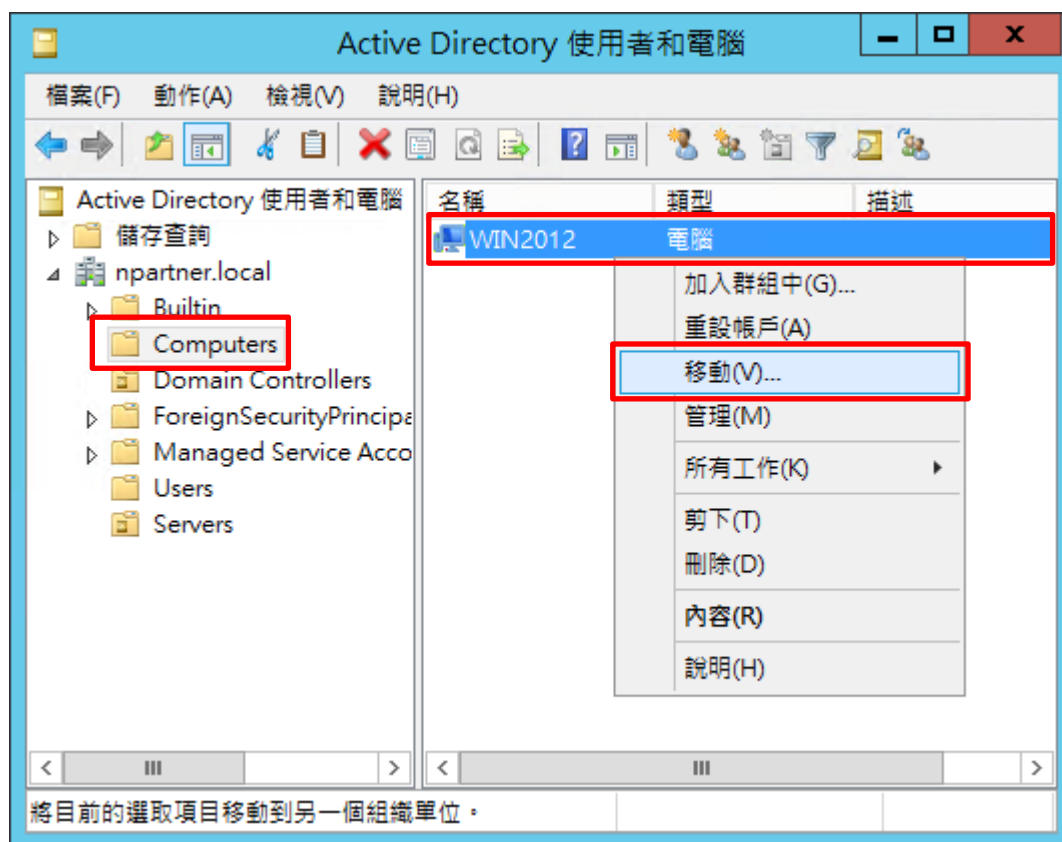
名稱(A):  
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

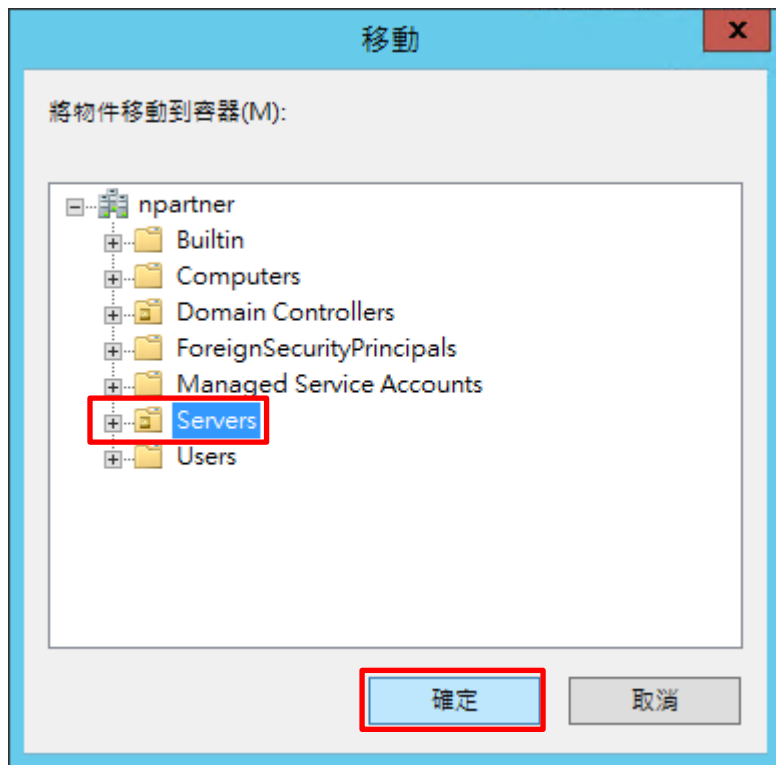
(4) 移動伺服器至新的組織單位

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



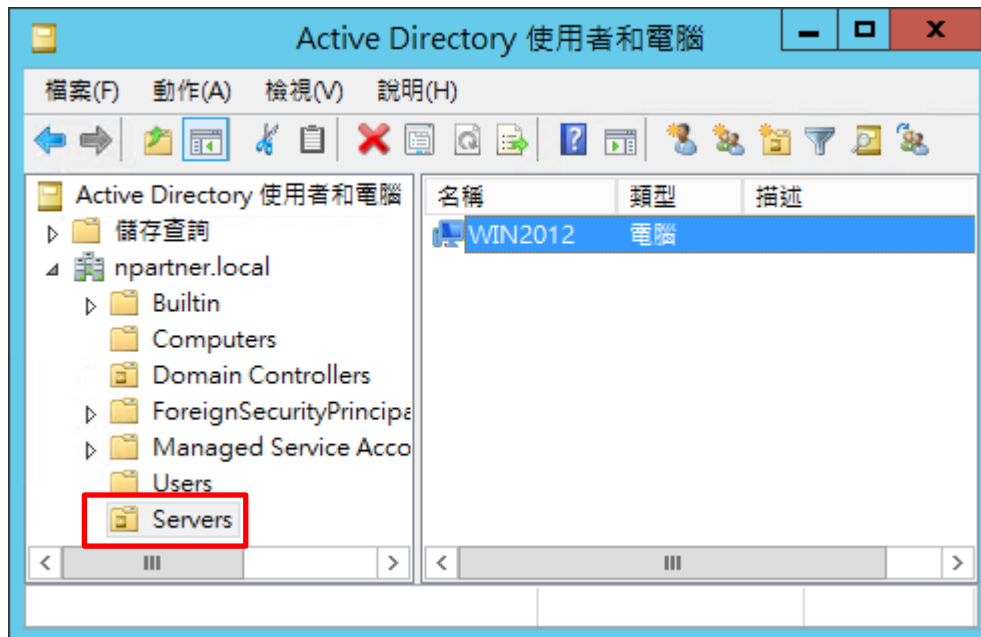
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [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 Win2012 File 伺服器已移動

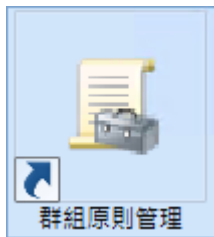




## 5.1.2 群組原則設定

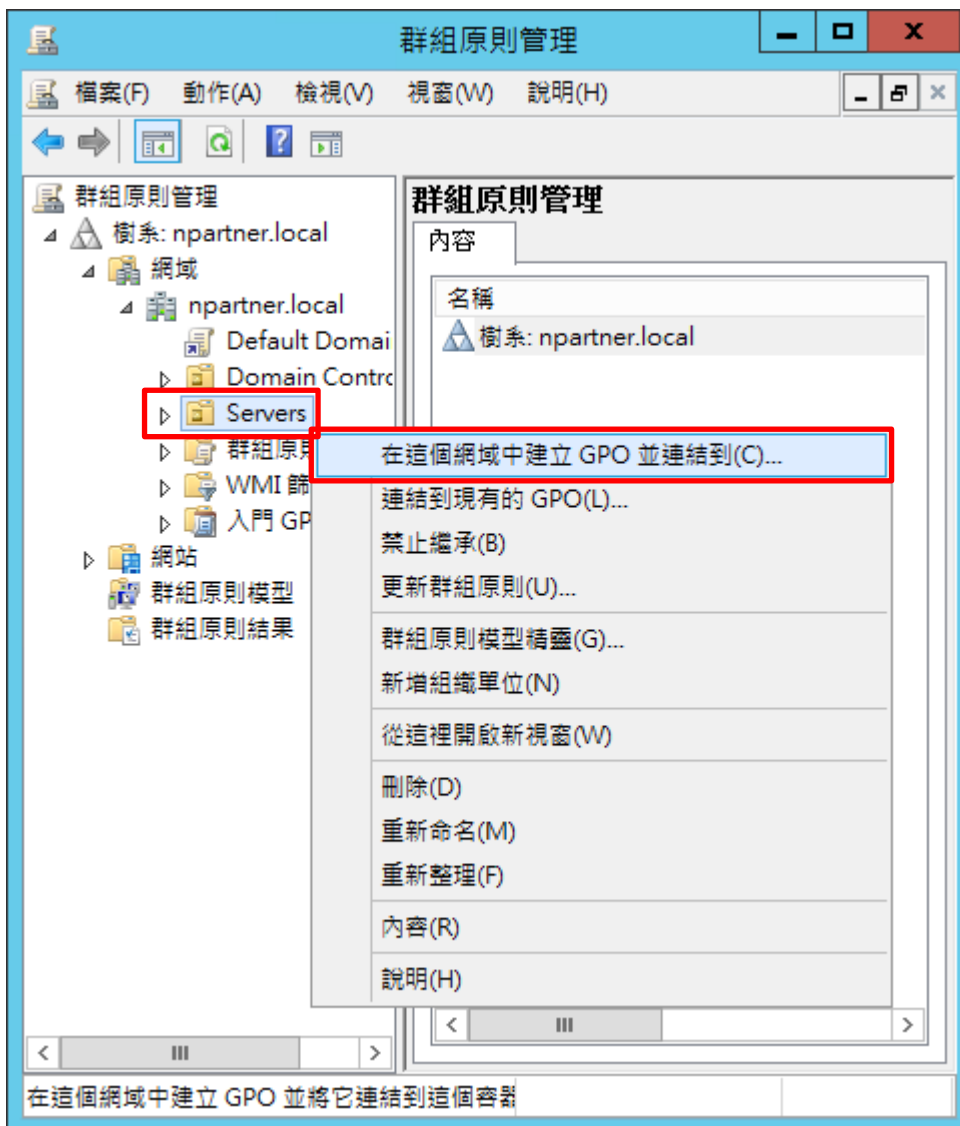
### (1) 開啟群組原則管理

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...]



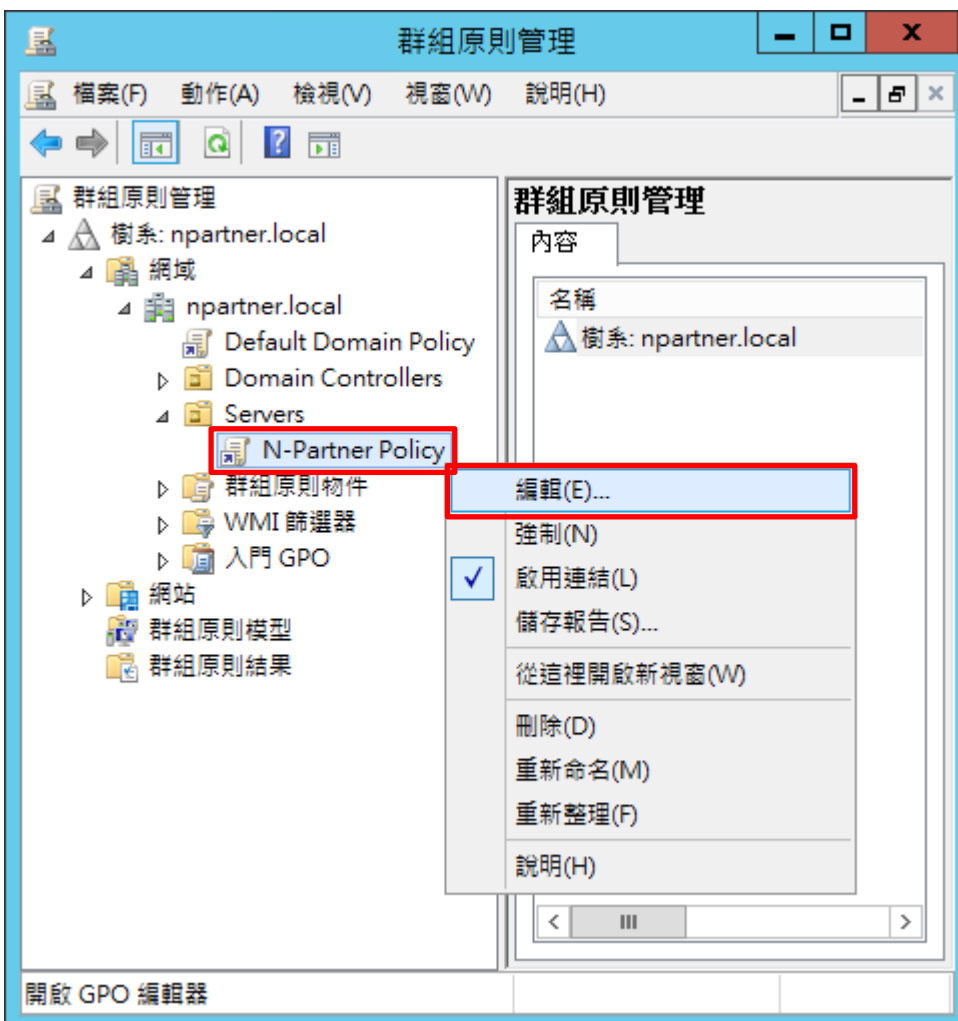
(3) 輸入群組原則物件名稱

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



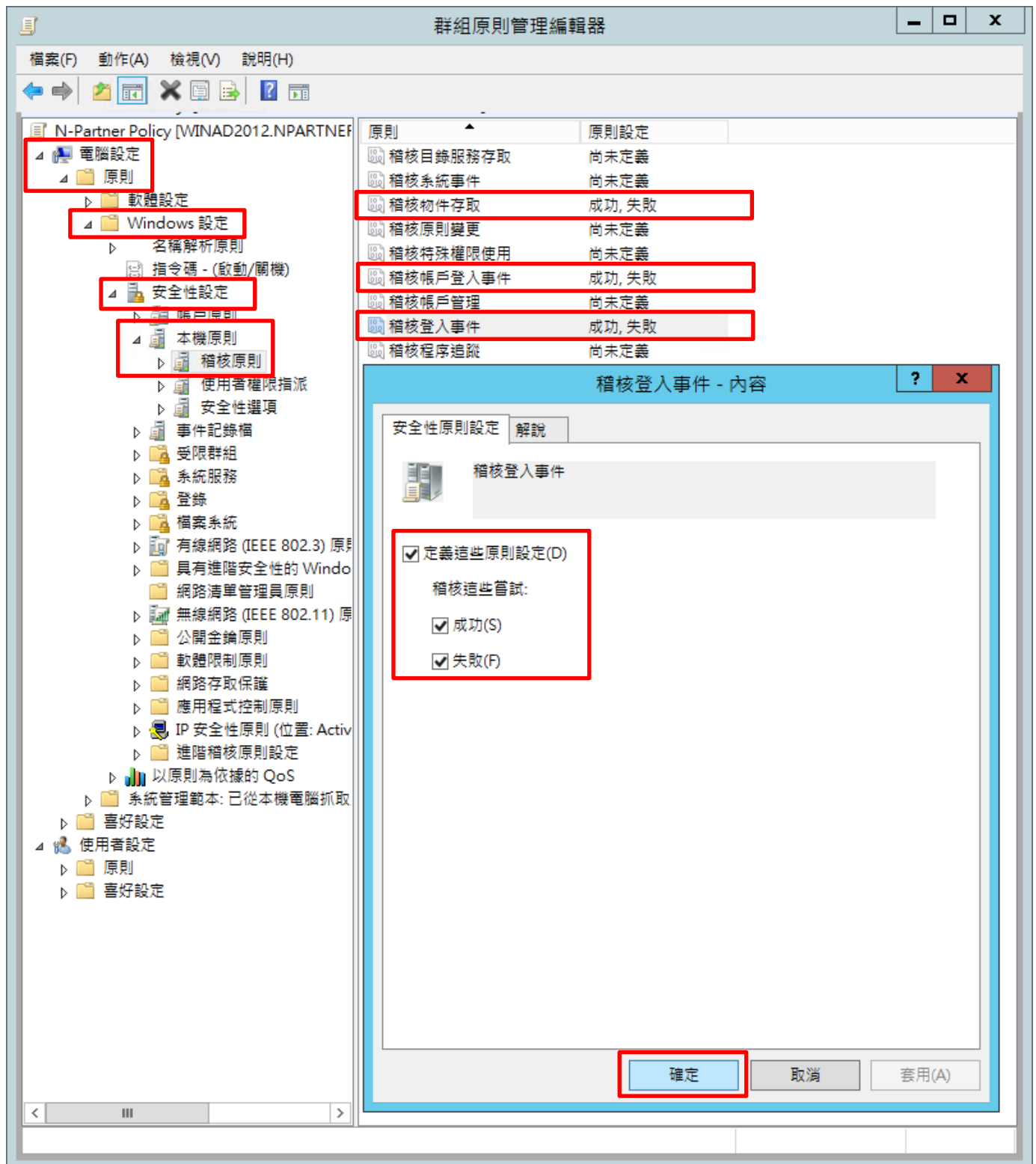
(4) 編輯群組原則物件

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



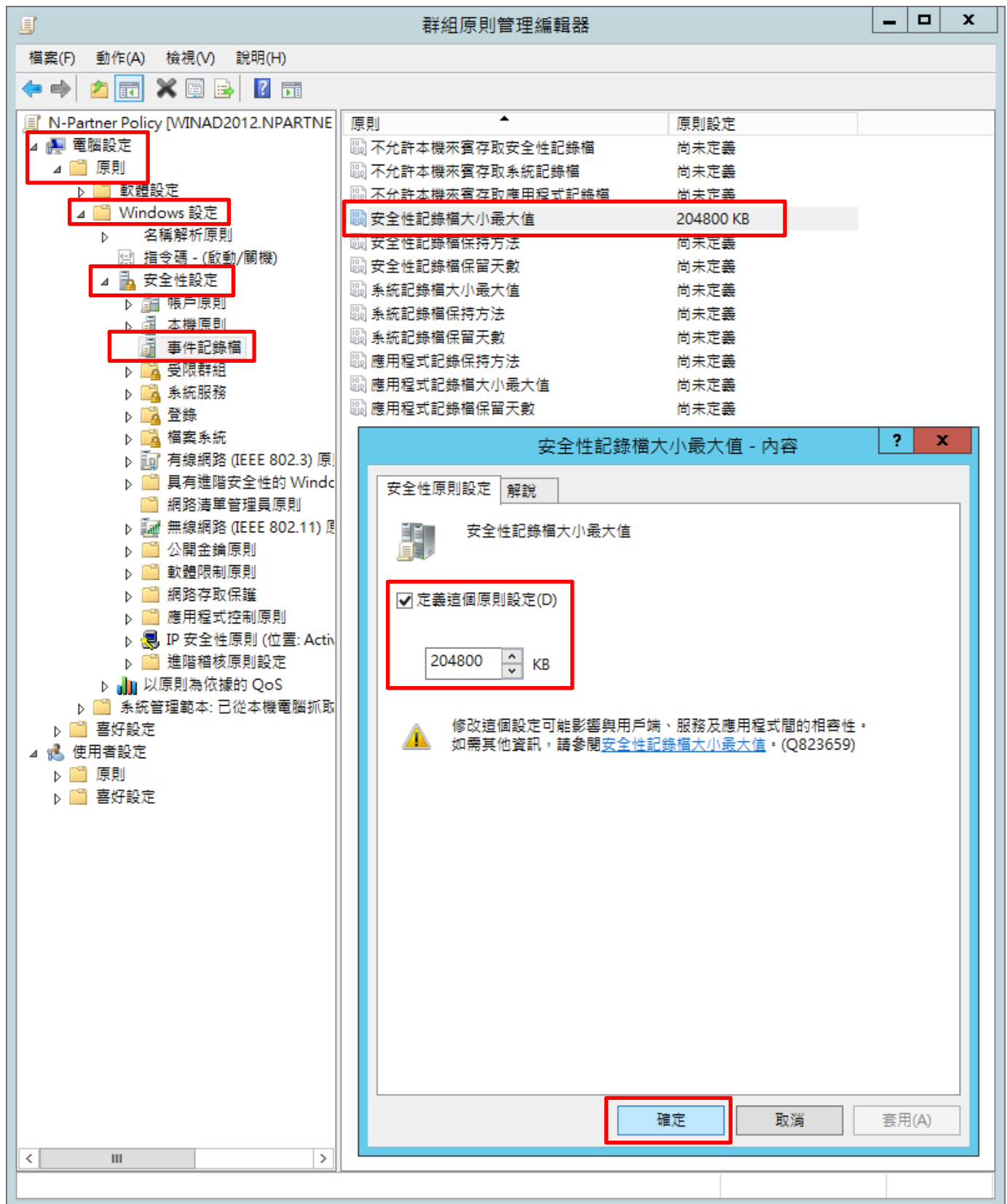
(5) 本機原則：稽核原則

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



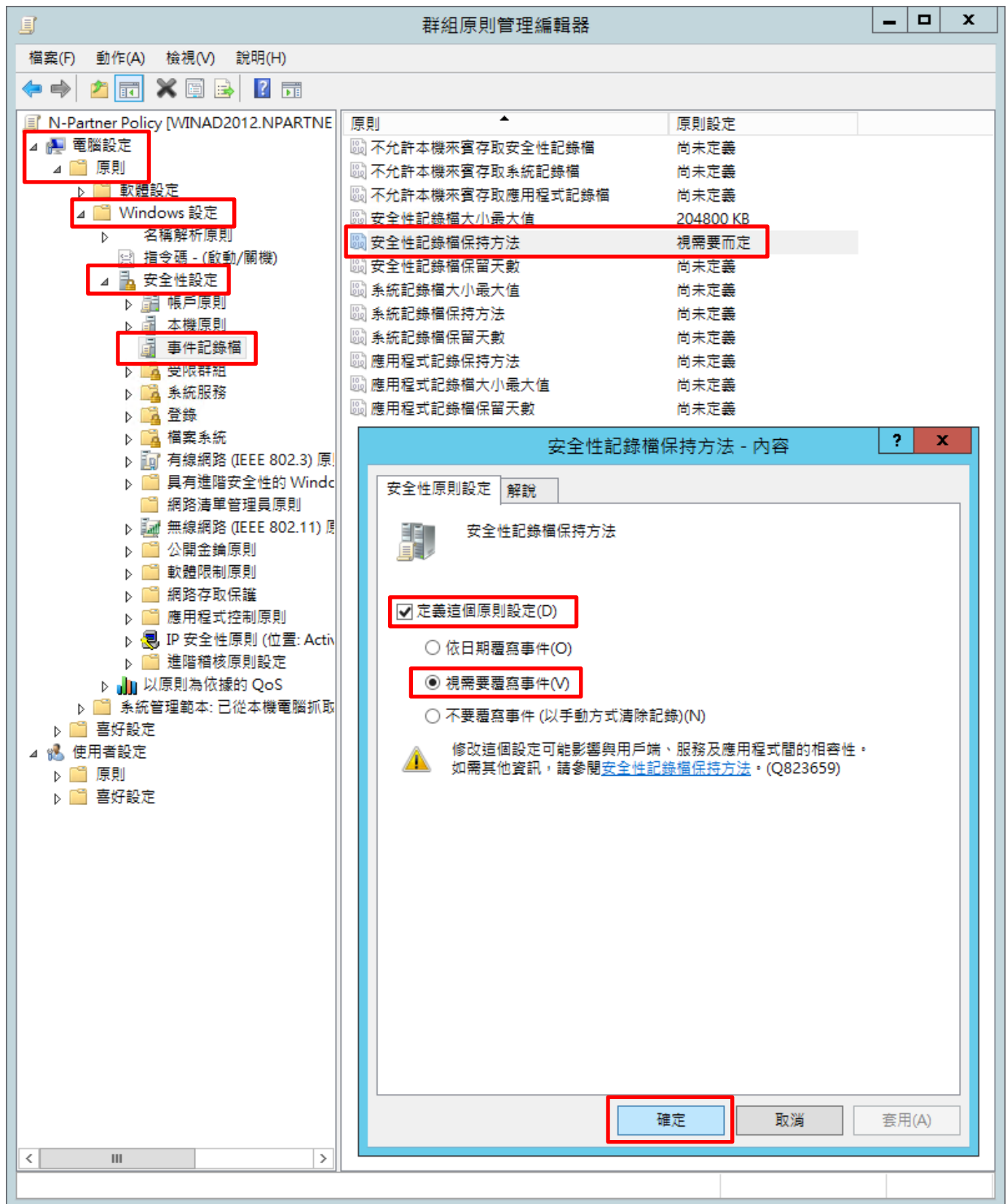
(6) 事件記錄檔：安全性記錄檔大小最大值

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

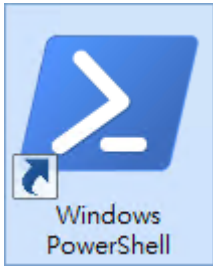


(7) 事件記錄檔：安全性記錄檔保持方法

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

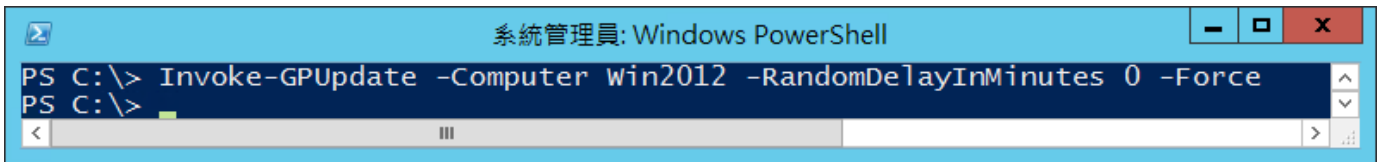


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(7) 更新 Windows File 伺服器群組原則

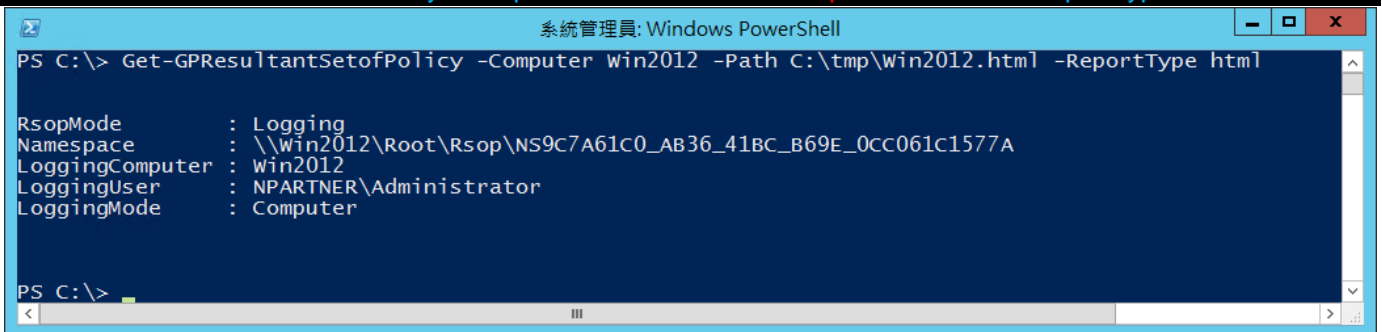
```
PS C:\> Invoke-GPUUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command: `PS C:\> Invoke-GPUUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force`. The prompt then returns to `PS C:\>`. The text "Win2012" in the command is highlighted in red in the original image.

紅色文字部位請輸入 Windows File 伺服器名稱

(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 terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command: `PS C:\> Get-GPResultantSetofPolicy -Computer Win2012 -Path C:\tmp\Win2012.html -ReportType html`. The output is as follows:  
`RsopMode : Logging  
Namespace : \\win2012\Root\Rsop\NS9C7A61C0_AB36_41BC_B69E_0CC061C1577A  
LoggingComputer : win2012  
LoggingUser : NPARTNER\Administrator  
LoggingMode : Computer`  
The prompt then returns to `PS C:\>`. The text "Win2012" and "C:\tmp\Win2012.html" in the command are highlighted in red in the original image.

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



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

The screenshot shows a web browser window with the address bar displaying 'C:\tmp\Win2012.html' and 'NPARTNER\WIN2012'. The main content area is titled '群組原則結果' (Group Policy Results) and shows the following structure:

- NPARTNER\WIN2012** (資料收集: 16/3/2022 15:36:42)
  - 摘要 (顯示全部 / 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/稽核原則 (隱藏)
 

原則	設定	優勢 GPO
稽核物件存取	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
          - 本機原則/使用者權限指派 (顯示)
          - 本機原則/安全性選項 (顯示)
          - 事件記錄檔 (隱藏)
 

原則	設定	優勢 GPO
安全性記錄檔保持方法	視需要而定	N-Partner Policy
安全性記錄檔容量最大值	204800 KB	N-Partner Policy
          - 公開金鑰原則/憑證服務用戶端 - 自動註冊設定 (顯示)
          - 公開金鑰原則/加密檔案系統 (顯示)
  - 群組原則物件 (顯示)
  - WMI 篩選器 (顯示)
  - 使用者詳細資料 (顯示)

## 5.2 工作群組

### 5.2.1 稽核原則設定

#### (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

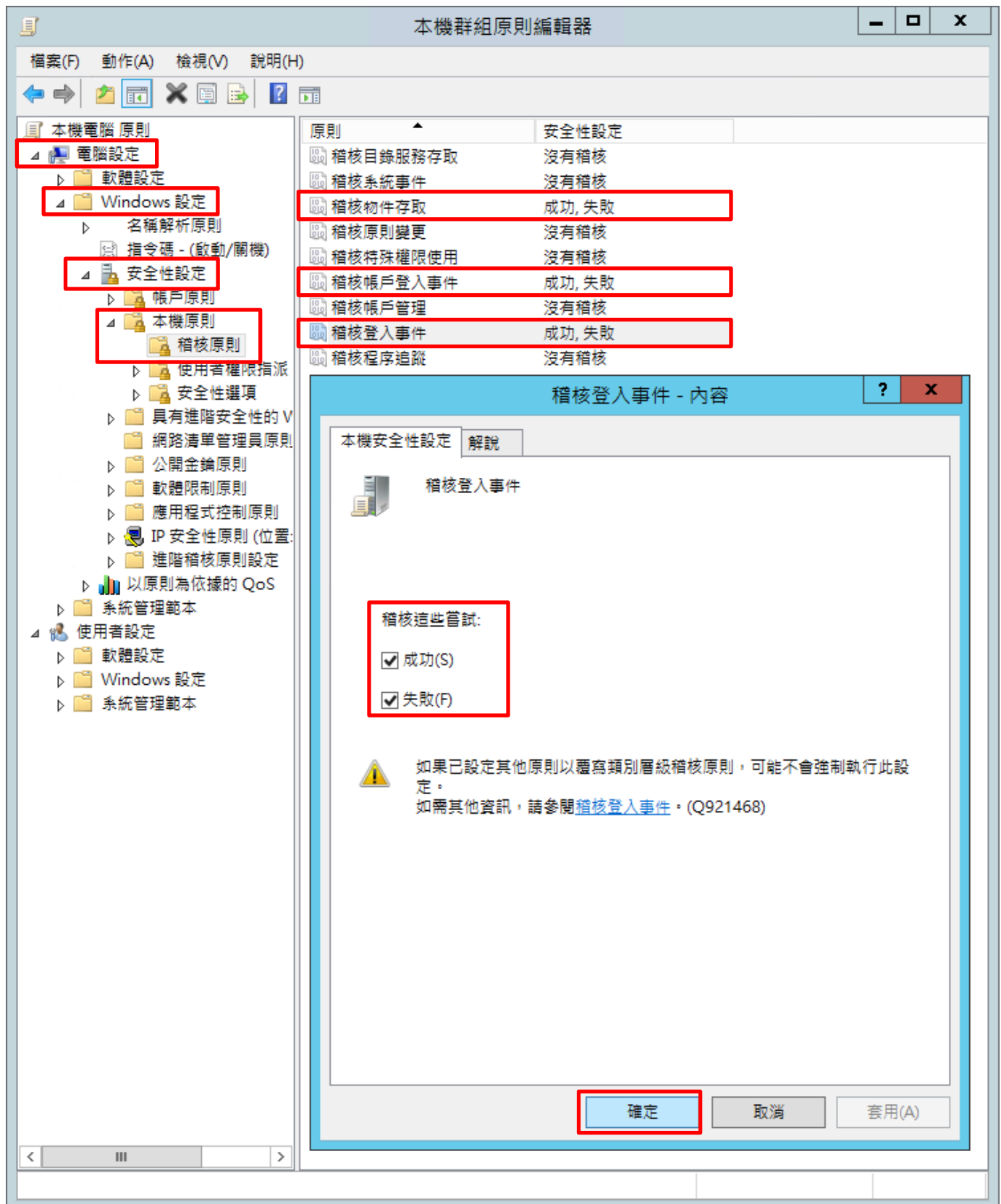
輸入 [群組原則](#) -> 點選 [編輯群組原則]



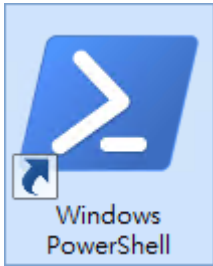


(3) 本機原則：稽核原則

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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

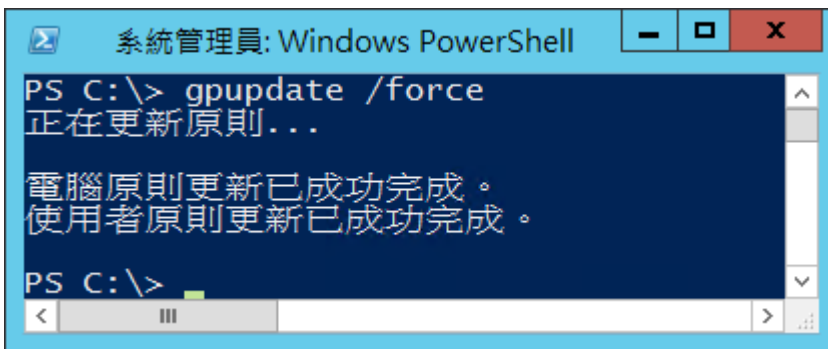


(4) 開啟 [Windows PowerShell]



(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:\> 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          成功與失敗
  IPSEC driver        沒有稽核
  其他系統事件        成功與失敗
  安全性狀態變更      成功
登入/登出
  登入                成功與失敗
  登出                成功與失敗
  帳戶鎖定            成功與失敗
  IPsec 主要模式      成功與失敗
  IPsec 快速模式      成功與失敗
  IPsec 延伸模式      成功與失敗
  特殊登入            成功與失敗
  其他登入/登出事件    成功與失敗
網路原則伺服器
  使用者/裝置宣告      成功與失敗
物件存取
  檔案系統            成功與失敗
  registry            成功與失敗
  核心物件            成功與失敗
  SAM                成功與失敗
  憑證服務            成功與失敗
  產生的應用程式      成功與失敗
  控制代碼操縱        成功與失敗
  檔案共用            成功與失敗
  篩選平台封包丟棄    成功與失敗
  篩選平台連線        成功與失敗
  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      成功與失敗
  集中原則暫存        成功與失敗
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
原則變更
  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
  稽核原則變更        成功
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 成功與失敗
  其他帳戶登入事件    成功與失敗
  Kerberos 驗證服務    成功與失敗
  認證驗證            成功與失敗
PS C:\>
```

## 5.2.2 事件檔案設定

### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



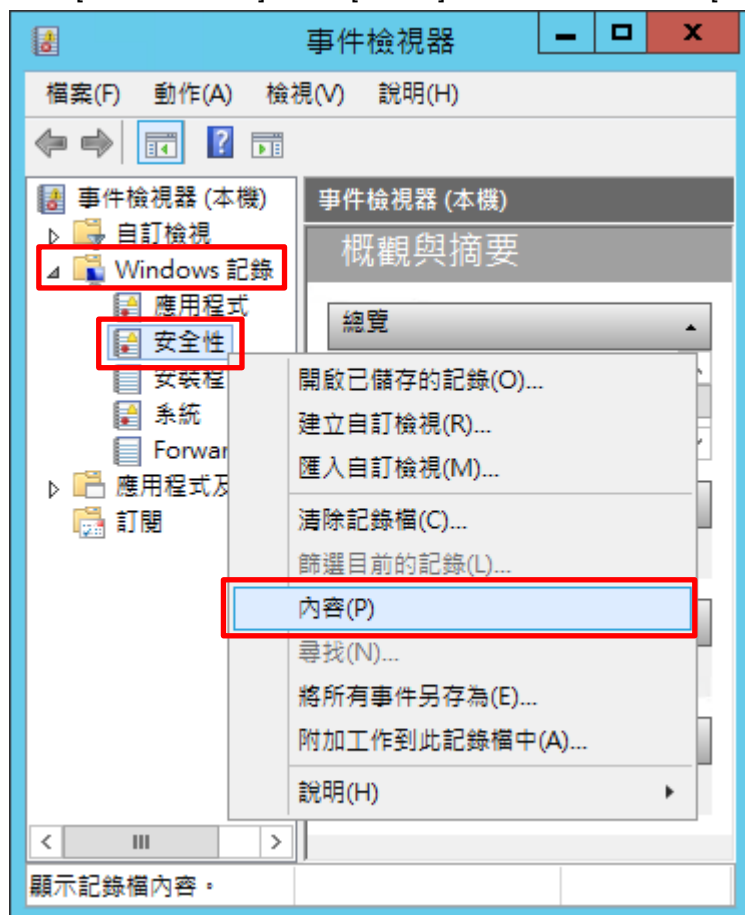
### (2) 搜尋事件檢視器並執行

輸入事件檢視器 -> 點選 [事件檢視器]



### (3) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(4) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx

記錄檔大小: 3.07 MB(3,215,360 位元組)

建立日期: 2021年3月17日 21:40:56

修改日期: 2021年3月17日 15:00:01

存取日期: 2021年3月17日 21:40:56

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

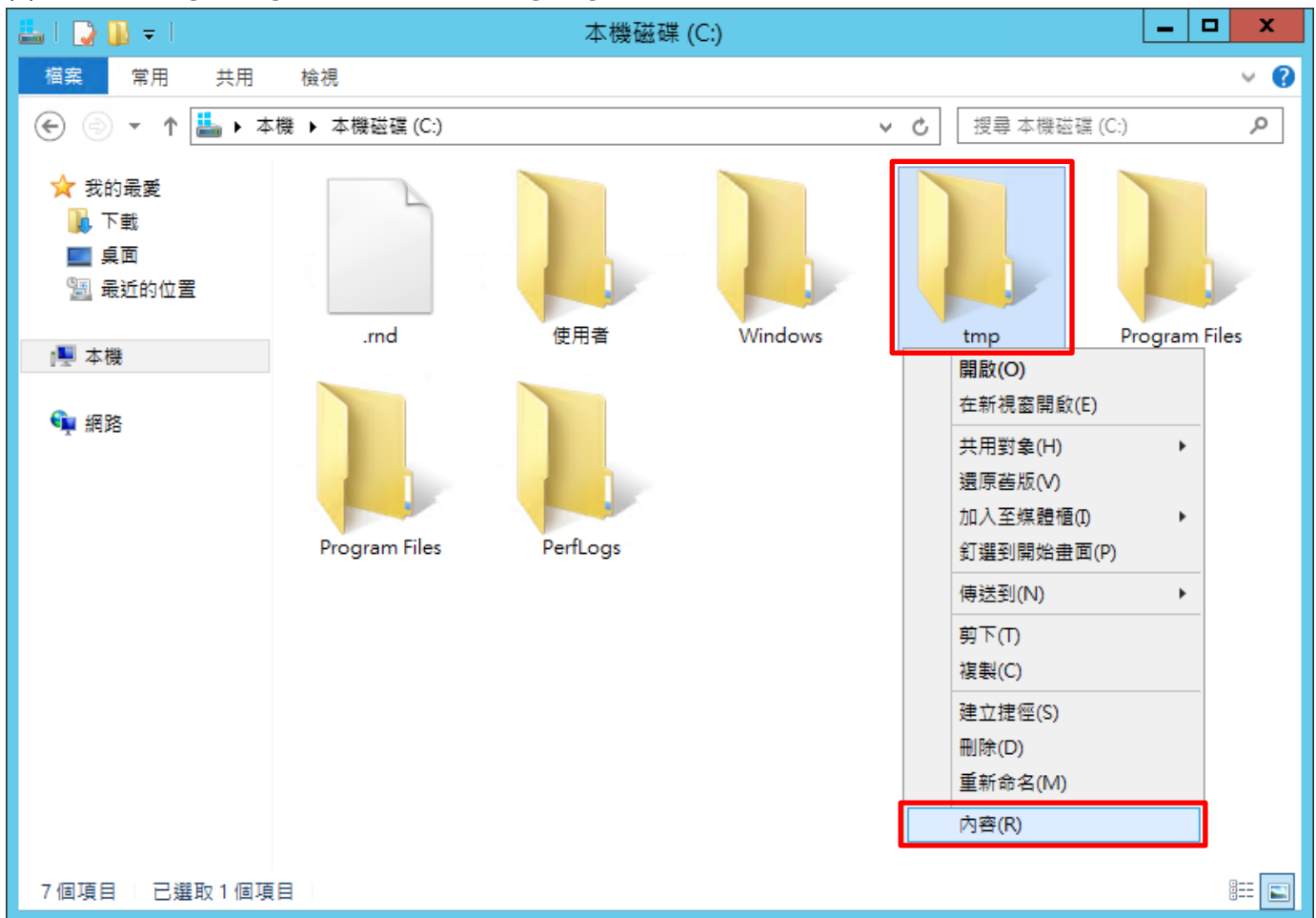
不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

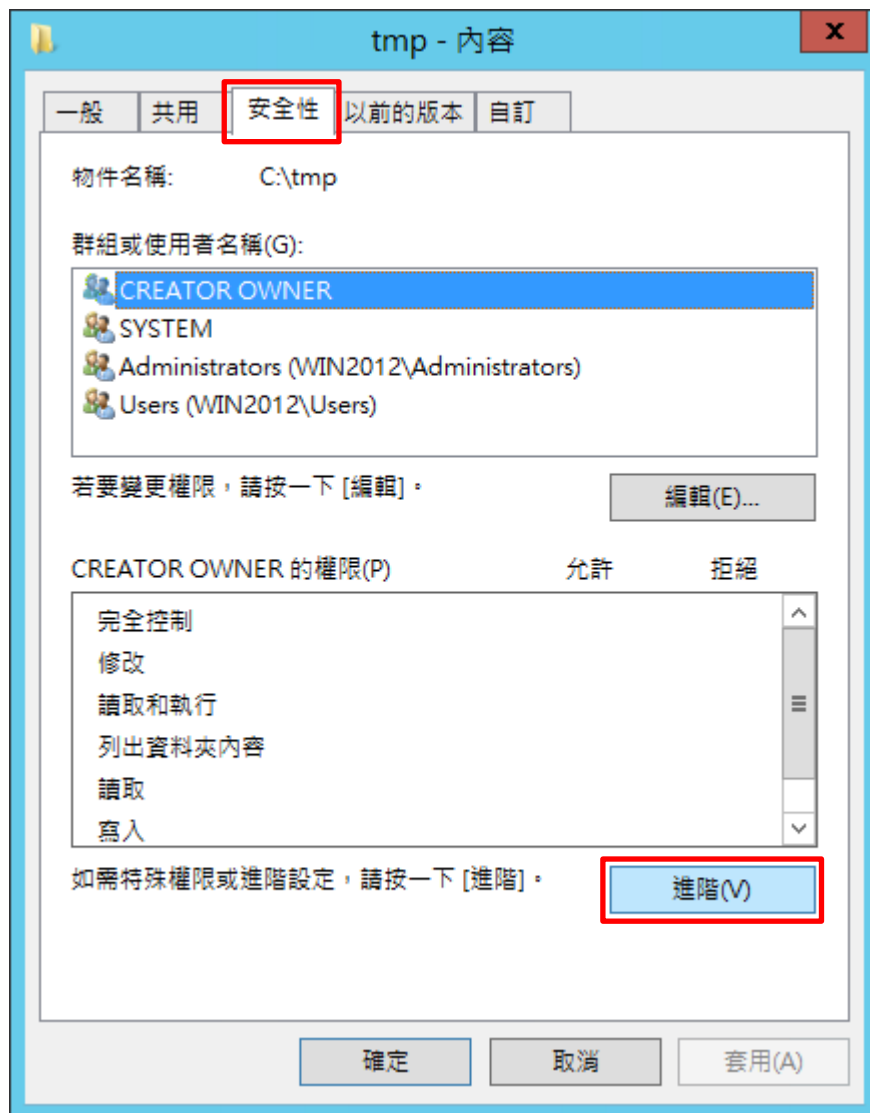
確定 取消 套用(P)

## 5.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]

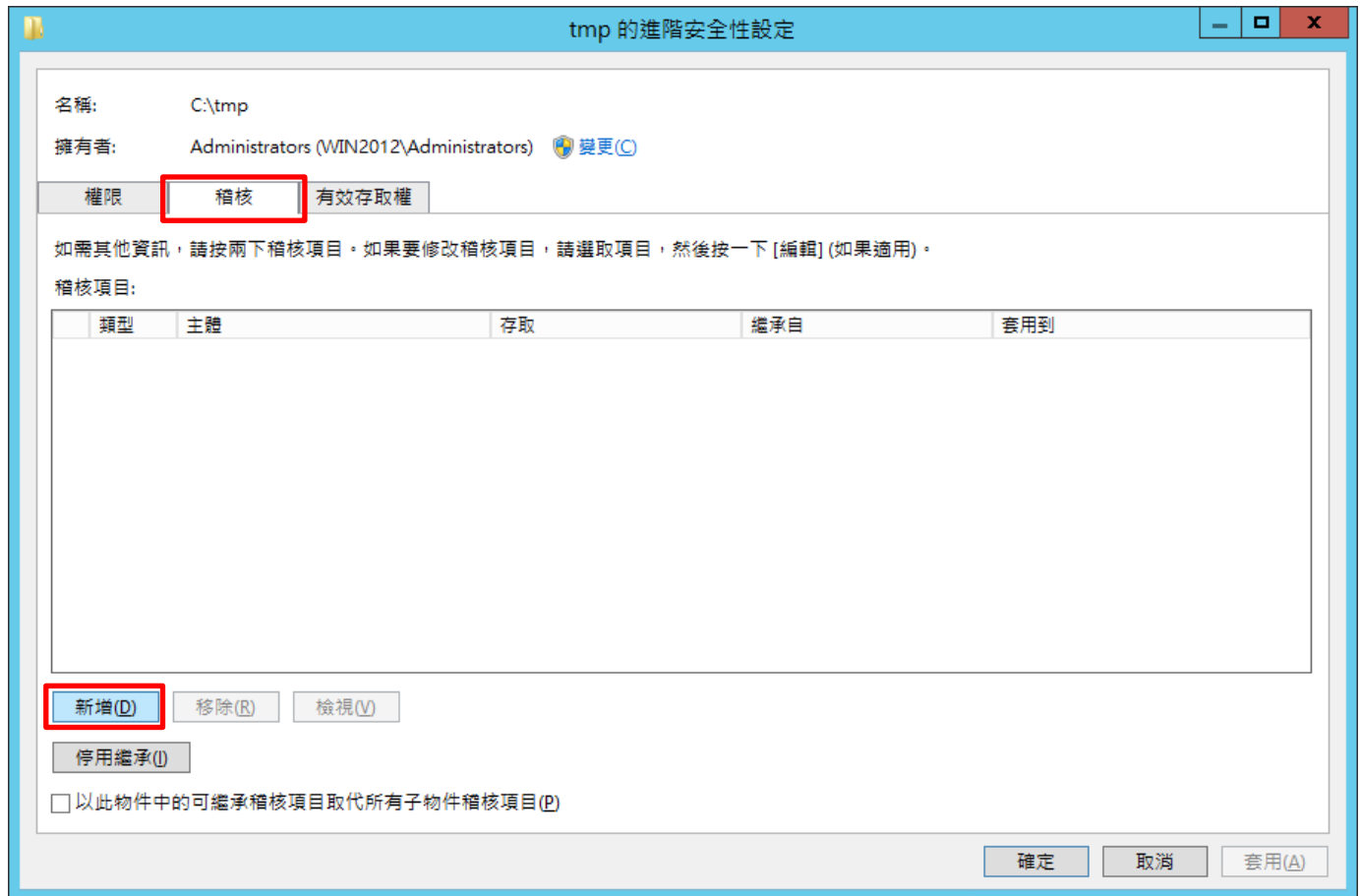


(2) 點選 [安全性] 頁面 -> 按 [進階]

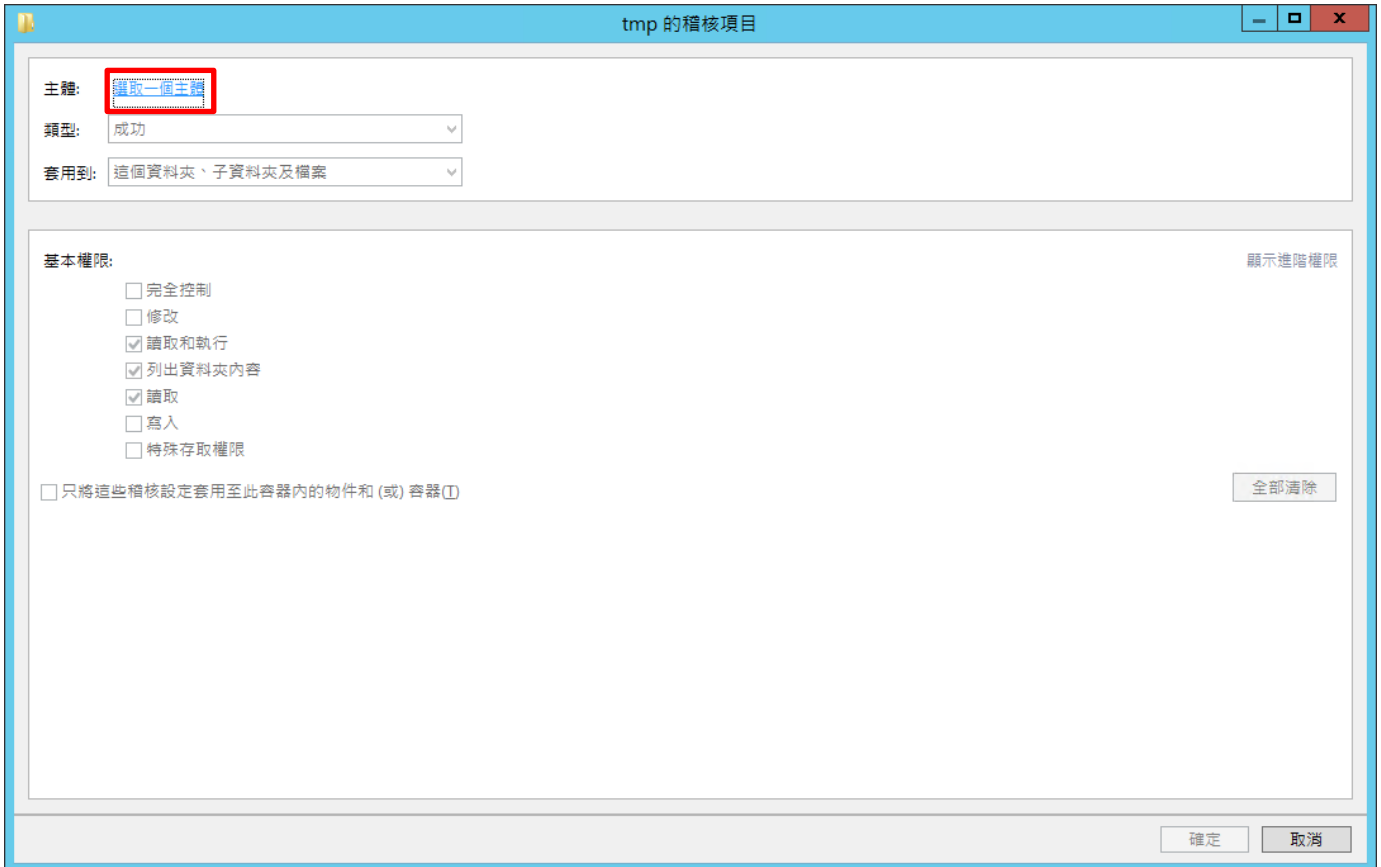




(3) 點選 [稽核] 頁面 -> 按 [新增]



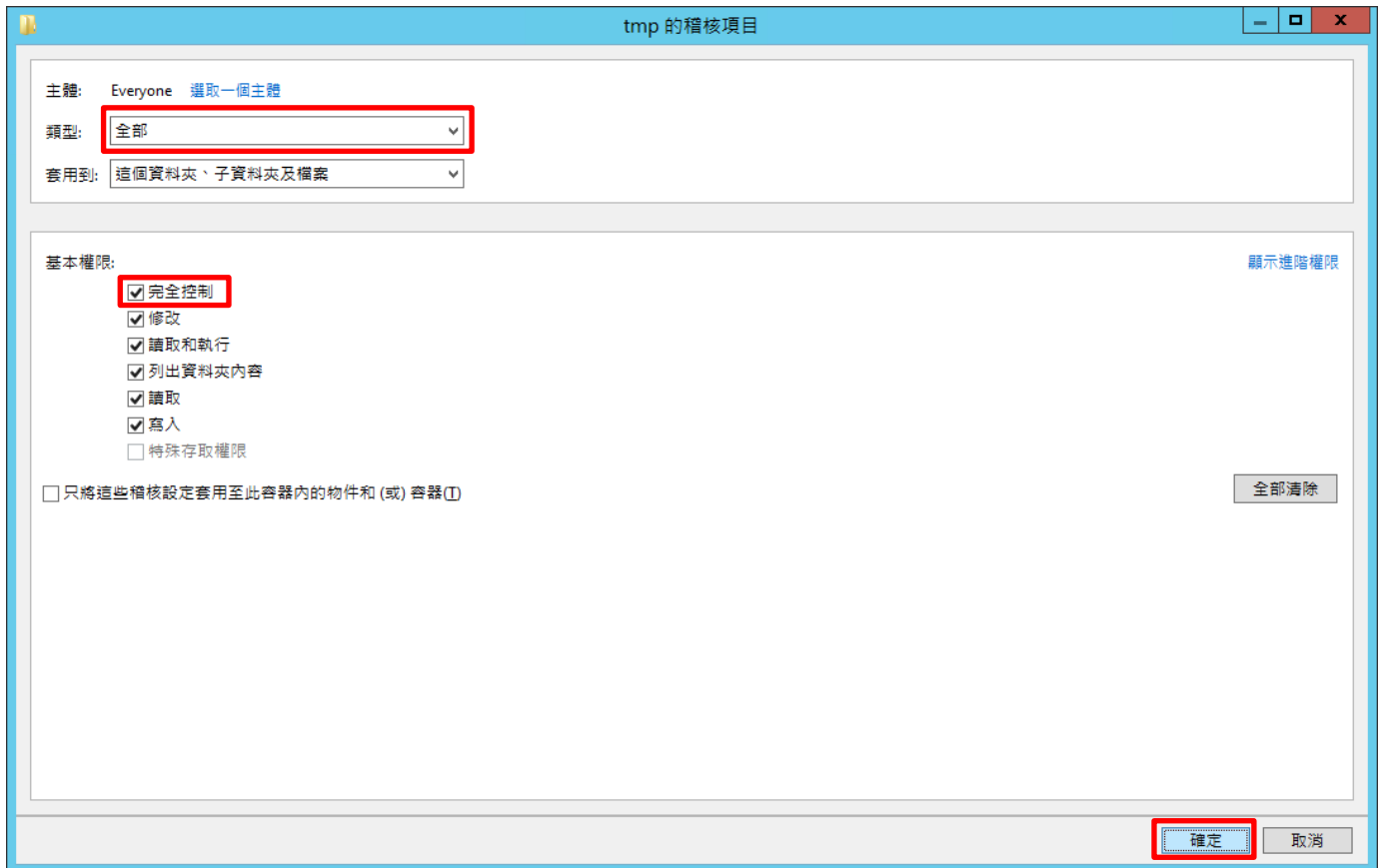
(4) 點選 [選取一個主體]



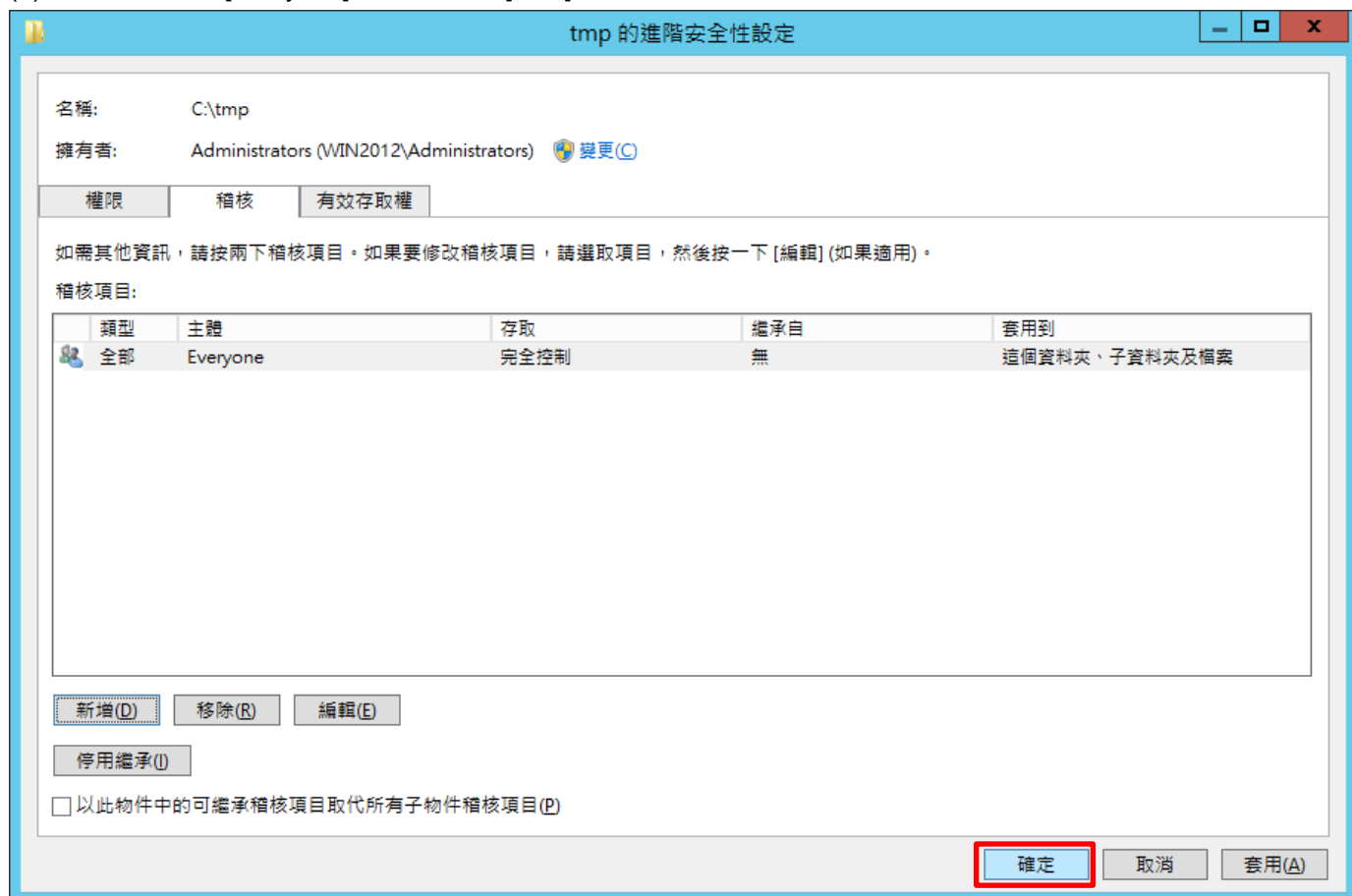
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



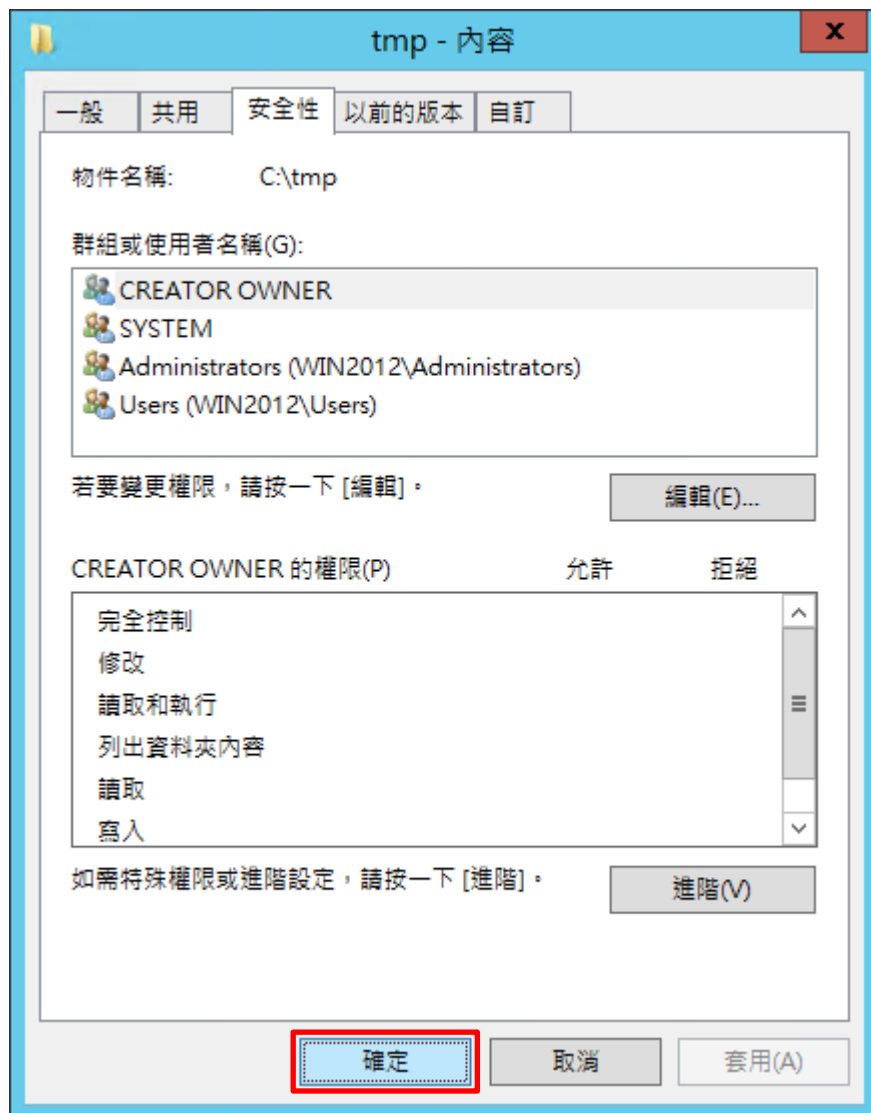
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(7) 稽核項目顯示 [Everyone] 名稱 -> 按 [確定]



(8) 按 [確定]



## 6. Windows 2016

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

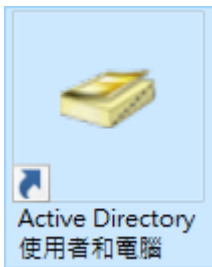
※ 以下分別為網域和工作群組設定方式。

### 6.1 網域

#### 6.1.1 組織單位設定

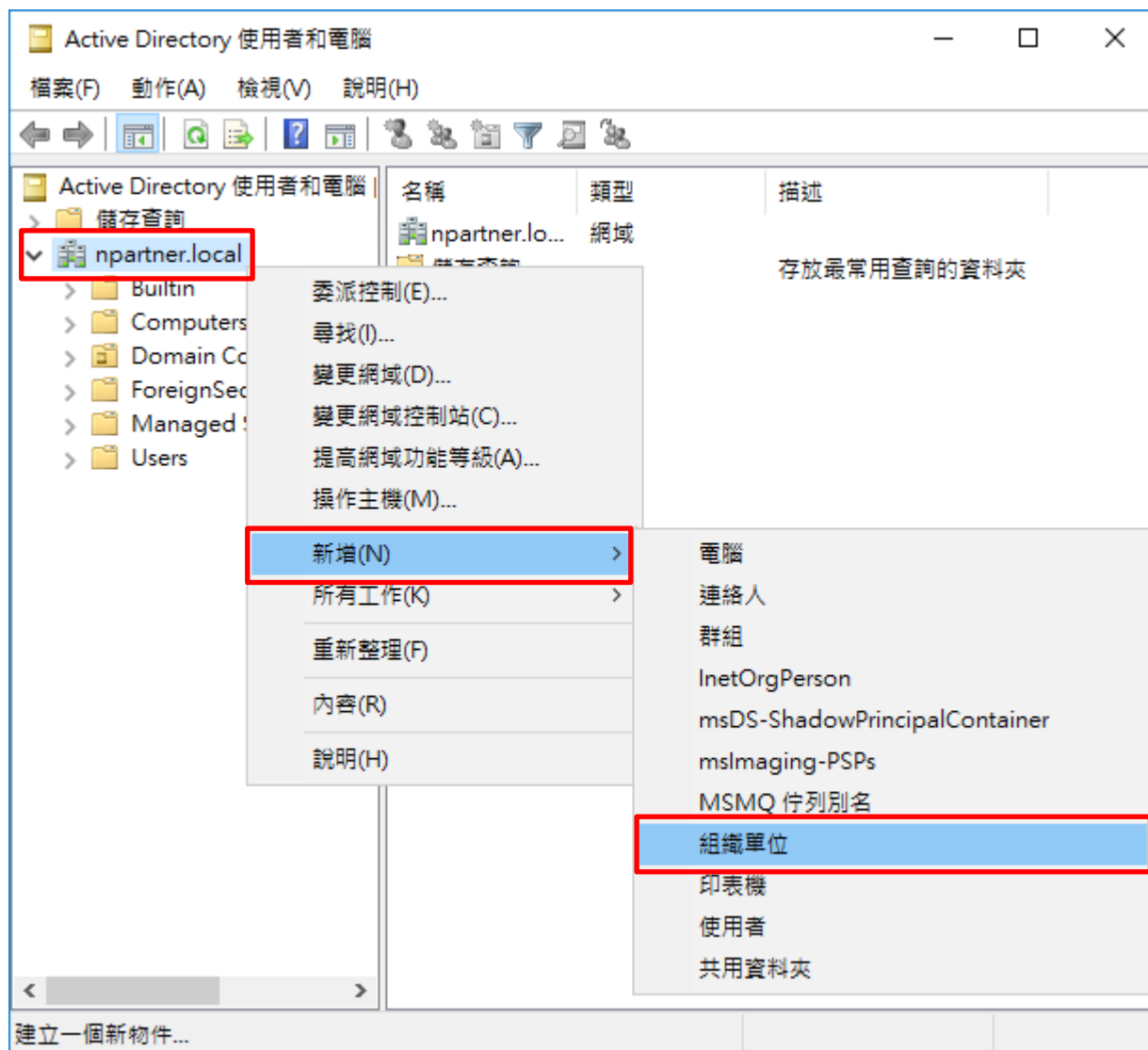
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



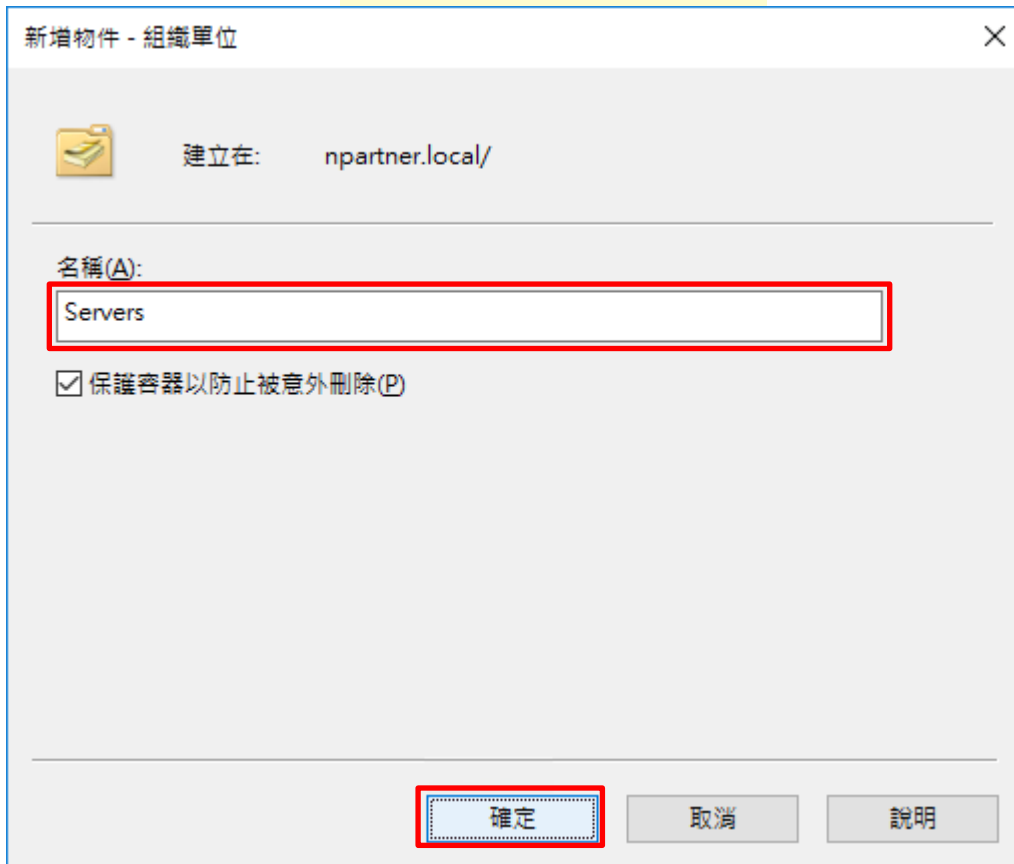
## (2) 新增組織單位

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 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/

名稱(A):  
Servers

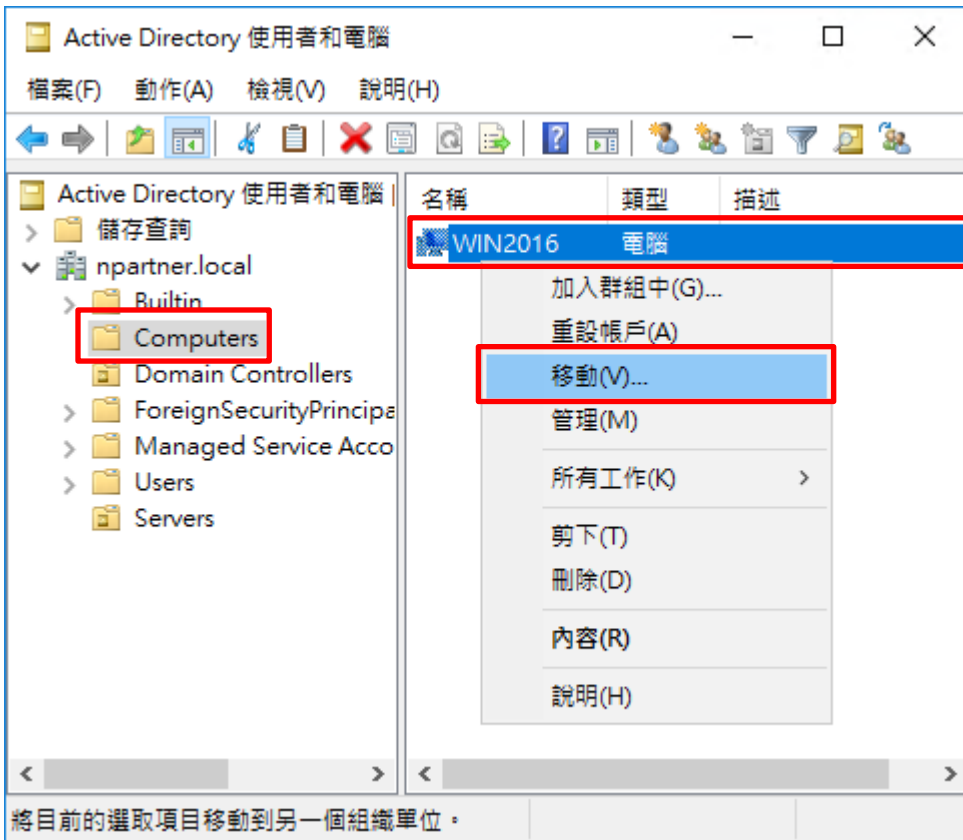
保護容器以防止被意外刪除(P)

確定 取消 說明



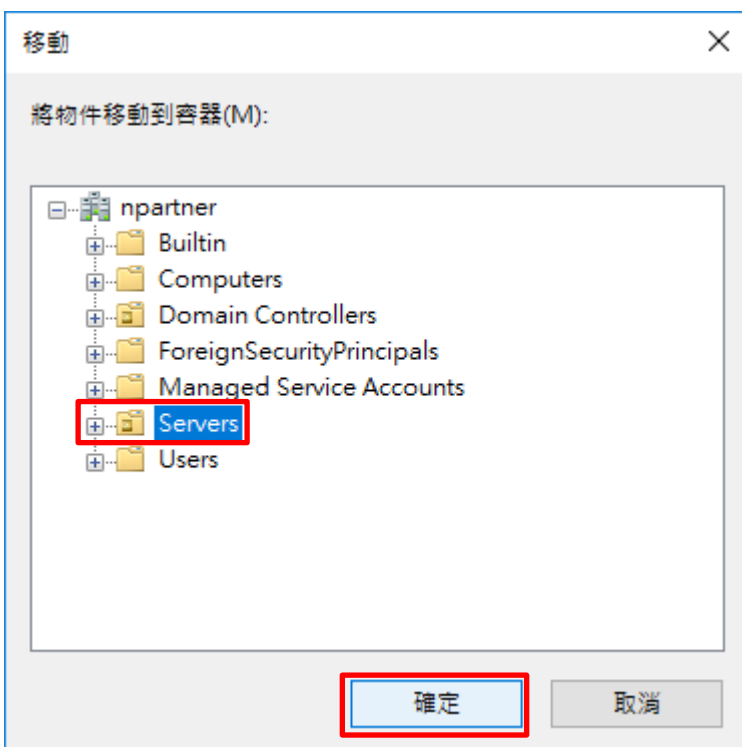
(4) 移動伺服器至新的組織單位

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



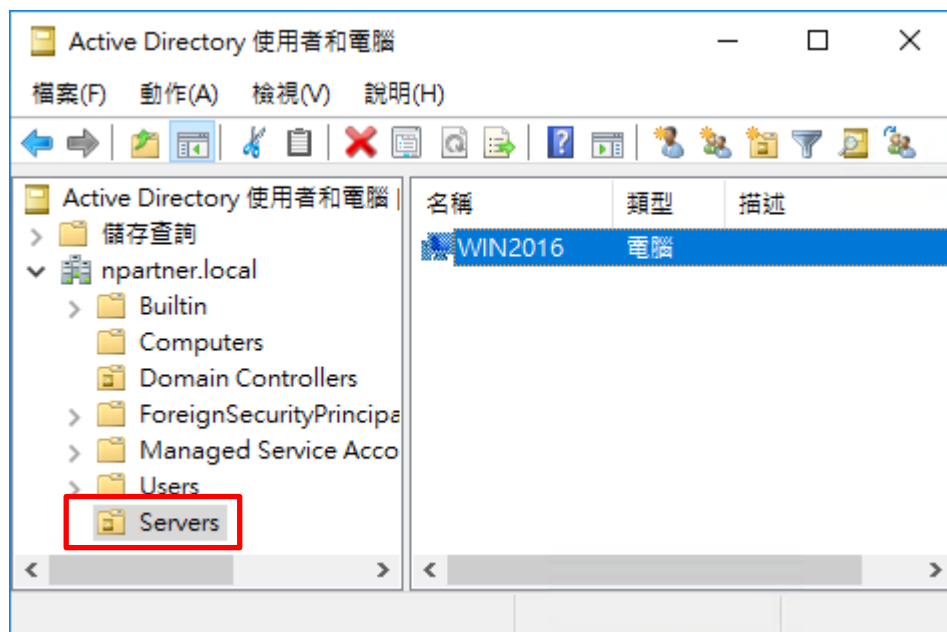
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

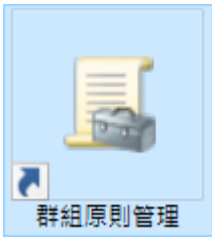
點選 [Servers] 組織單位，確認 Win2016 File 伺服器已移動



## 6.1.2 群組原則設定

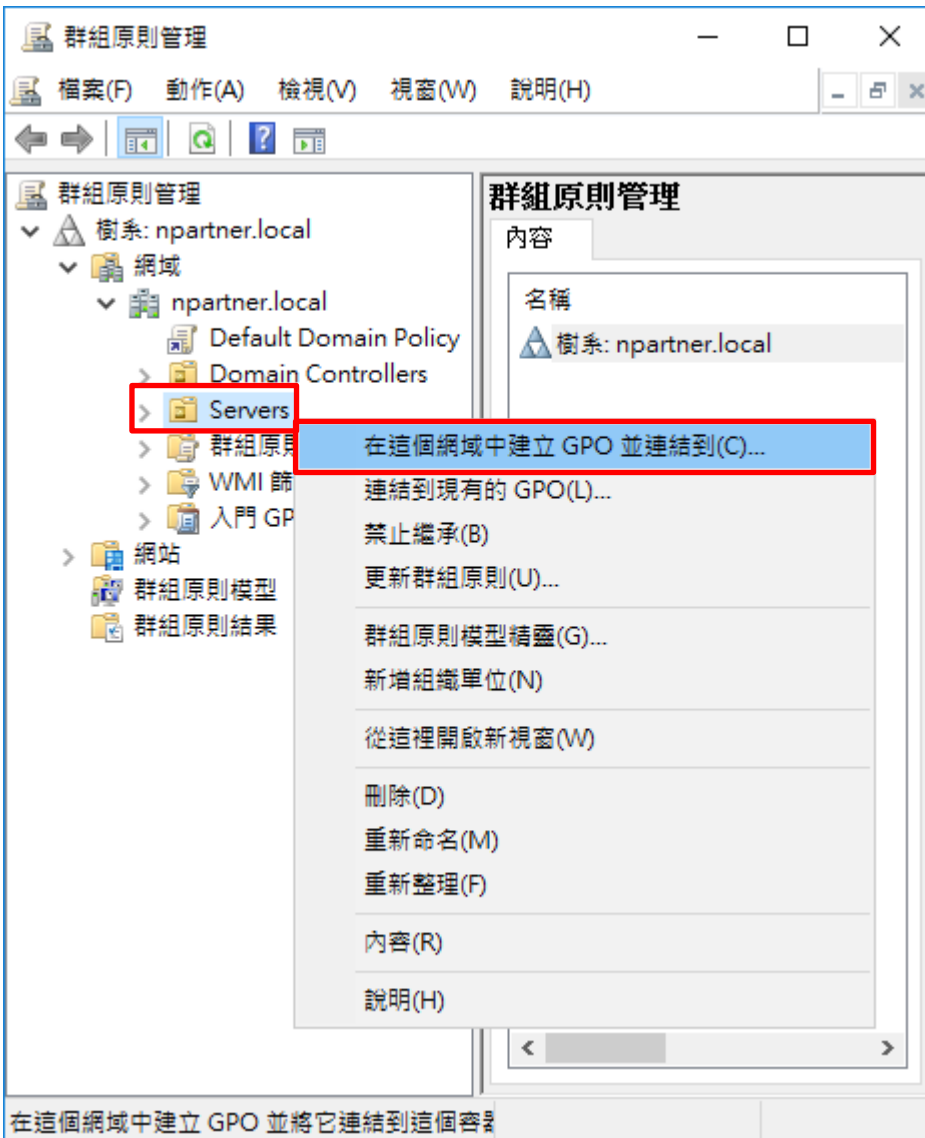
### (1) 開啟群組原則管理

開啟 [群組原則管理]



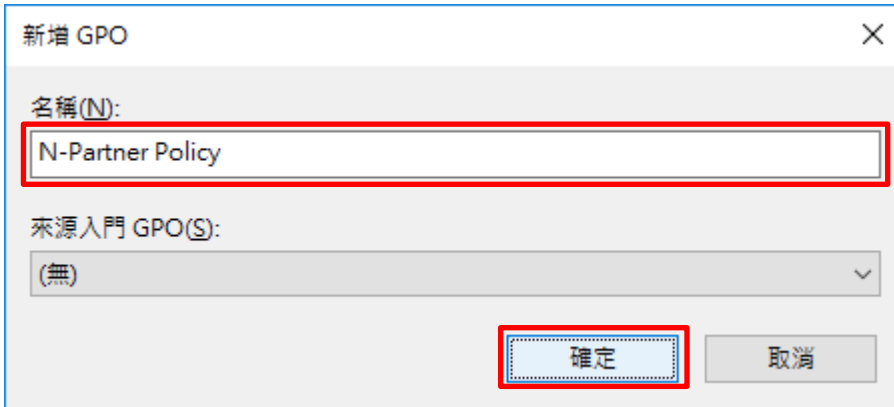
### (2) 在 Servers 組織單位，新增群組原則物件

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



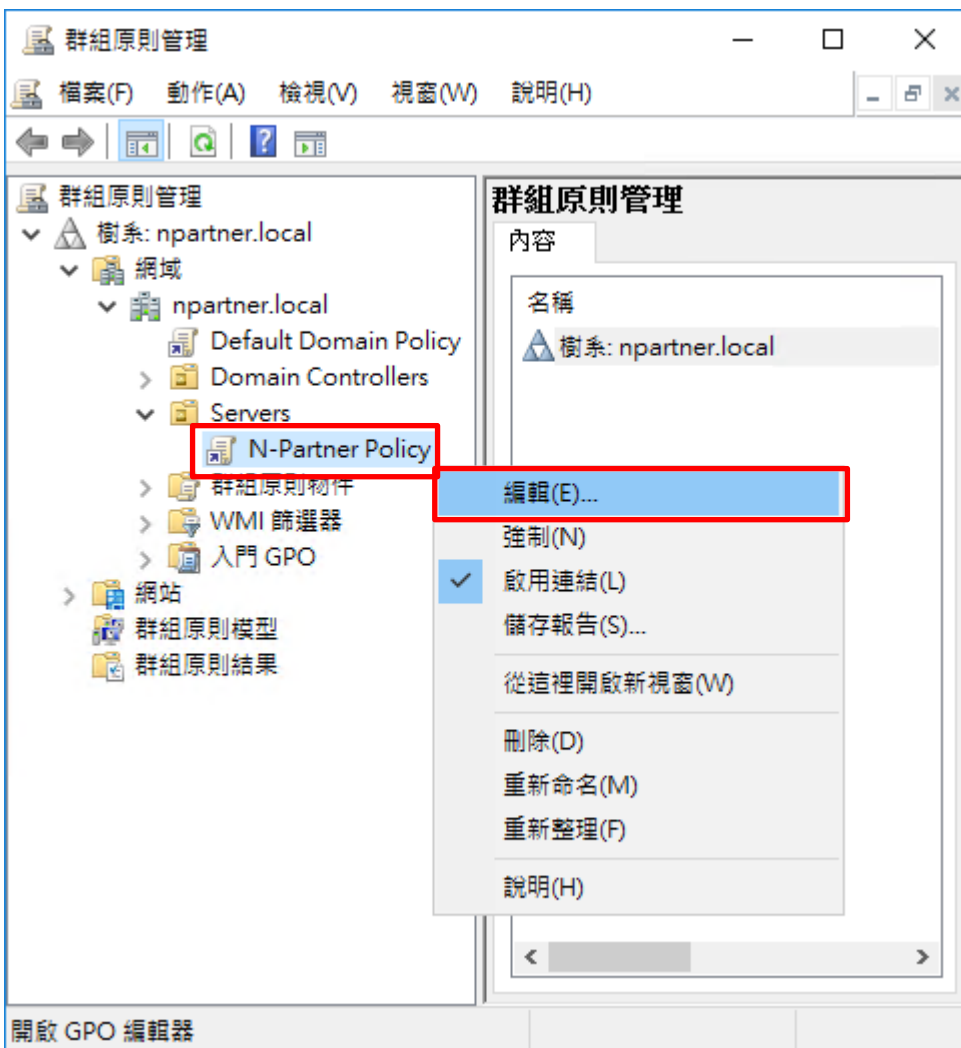
(3) 輸入群組原則物件名稱

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



(4) 編輯群組原則物件

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



(5) 本機原則：稽核原則

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

群組原則管理編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

N-Partner Policy [WINAD2016.NPART]

原則	原則設定
稽核目錄服務存取	尚未定義
稽核系統事件	尚未定義
稽核物件存取	成功, 失敗
稽核原則變更	尚未定義
稽核特殊權限使用	尚未定義
稽核帳戶登入事件	成功, 失敗
稽核帳戶管理	尚未定義
稽核登入事件	成功, 失敗
稽核程序追蹤	尚未定義

稽核登入事件 - 內容

安全性原則設定 解說

稽核登入事件

定義這些原則設定(D)

稽核這些嘗試:

成功(S)

失敗(F)

確定 取消 套用(A)

(6) 事件記錄檔：安全性記錄檔大小最大值

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

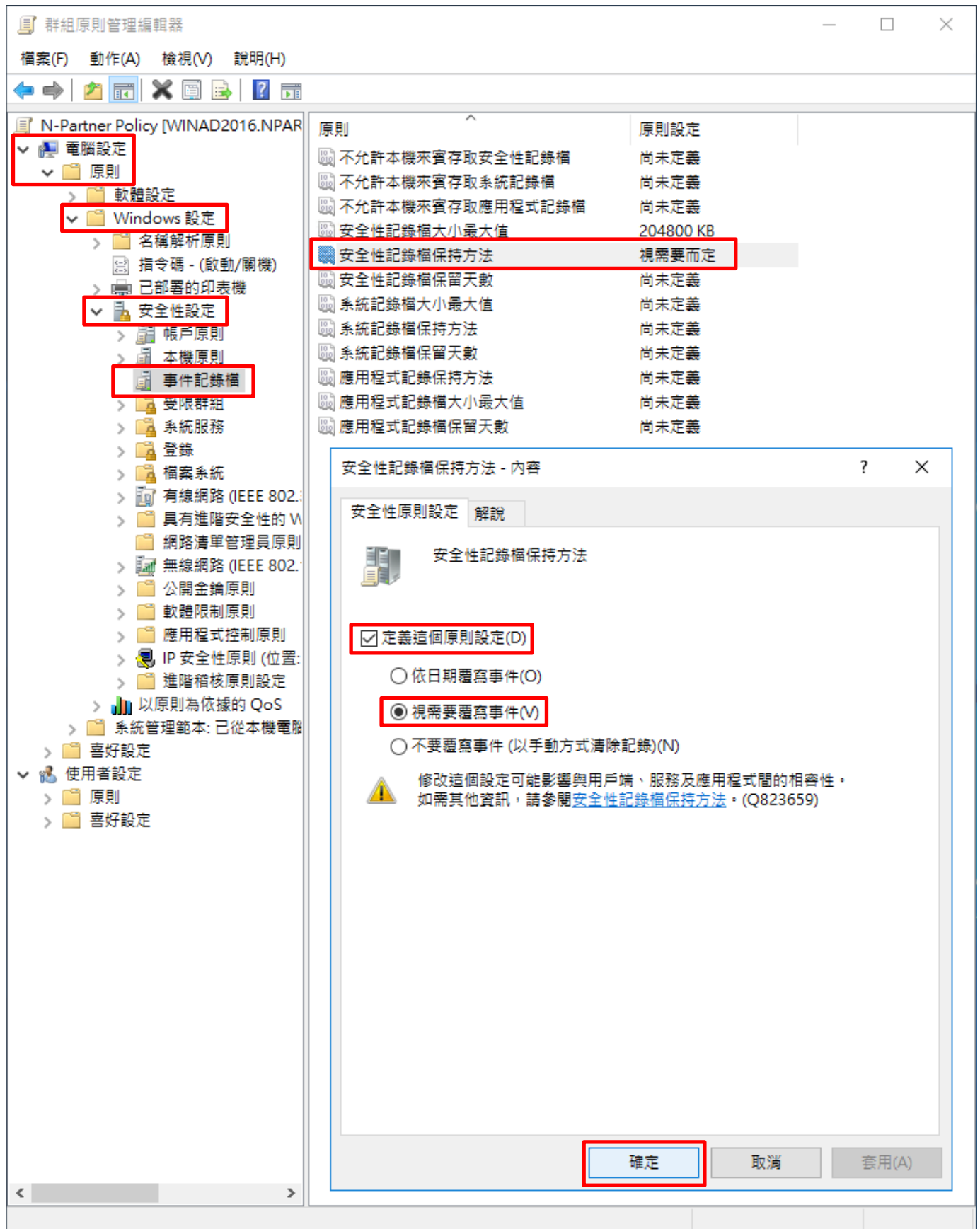
The screenshot shows the Group Policy Management console for 'N-Partner Policy [WINAD2016.NPAR]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Logs). The 'Maximum size of security event logs' policy is selected and highlighted in red. The right-hand pane shows a list of policies with their current settings. The selected policy is set to '204800 KB'. Below this, a dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum size of security event logs - Content) is open. In this dialog, the '定義這個原則設定(D)' (Define this policy setting) checkbox is checked and highlighted in red. The value '204800' is entered in the text box, followed by a dropdown menu set to 'KB'. A warning icon and text are visible below the input field. At the bottom of the dialog, the '確定' (OK) button is highlighted in red.

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



(7) 事件記錄檔：安全性記錄檔保持方法

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

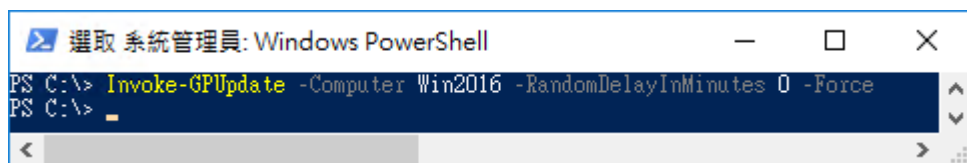


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows File 伺服器群組原則

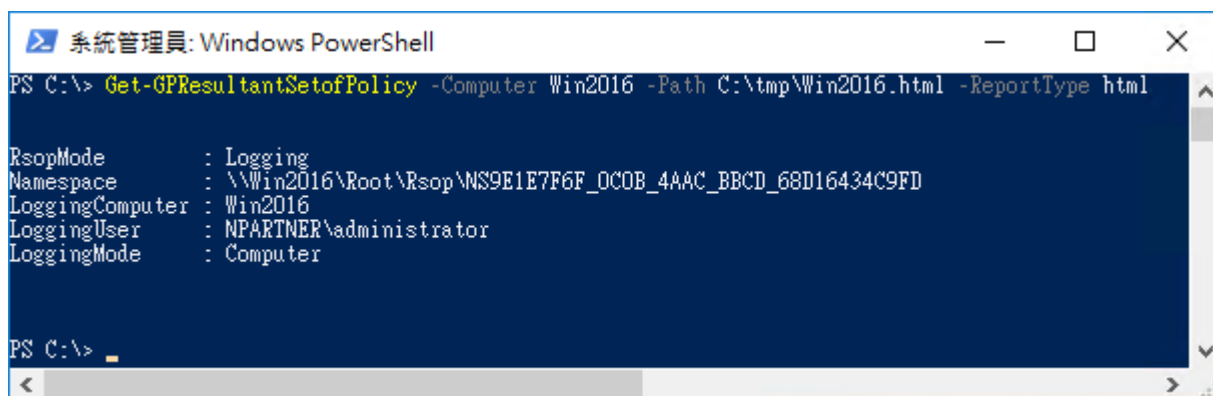
```
PS C:\> Invoke-GPUUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows File 伺服器名稱

(10) 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



(11) 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\WIN2016  
資料收集: 2022/3/16 下午 04:33:56 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/稽核原則 隱藏

原則	設定	優勢 GPO
稽核物件存取	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

## 6.2 工作群組

### 6.2.1 稽核原則設定

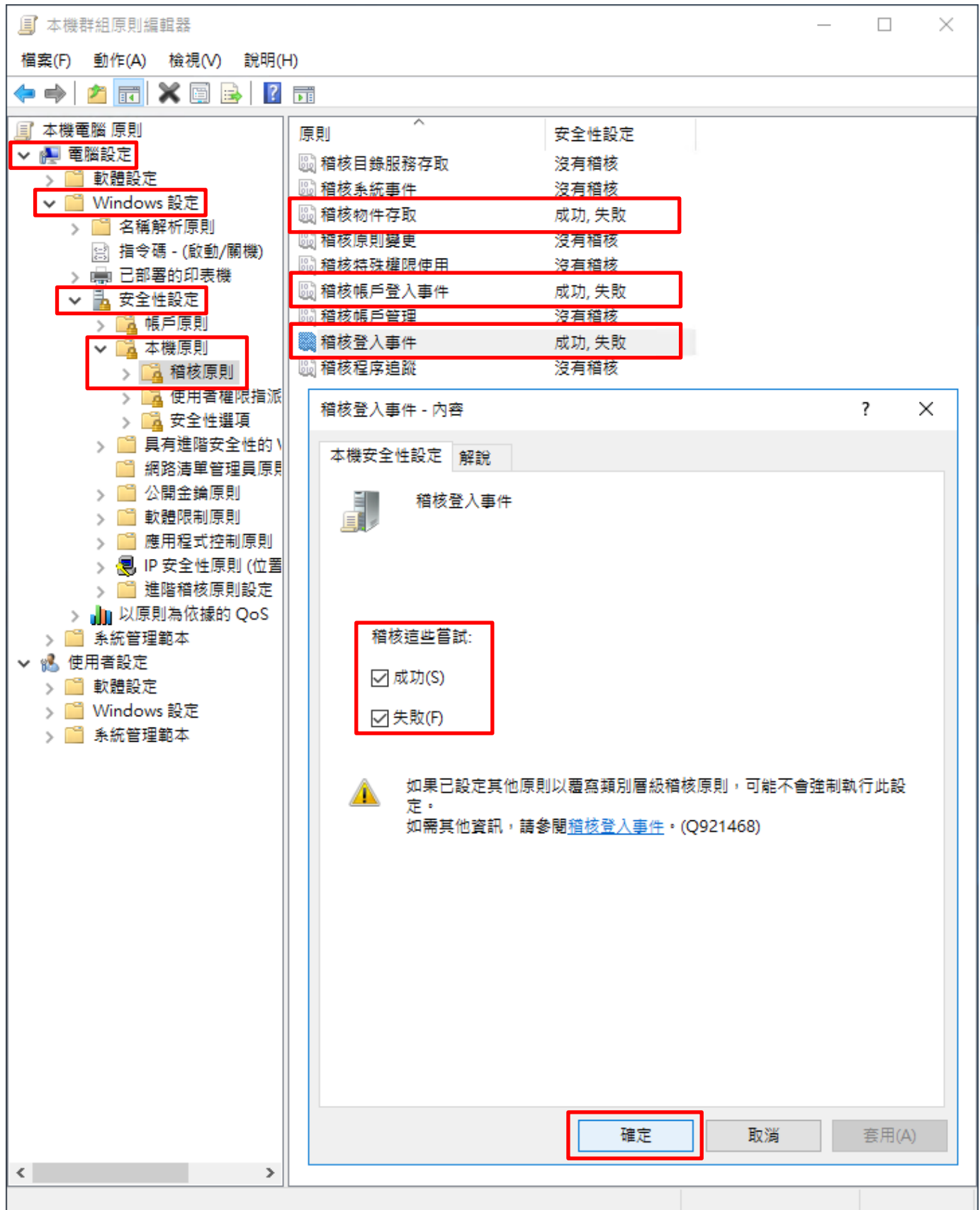
(1) 開啟本機群組原則編輯器

點選  [搜尋] -> 輸入 **群組原則** -> 點選 [編輯群組原則]



(2) 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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

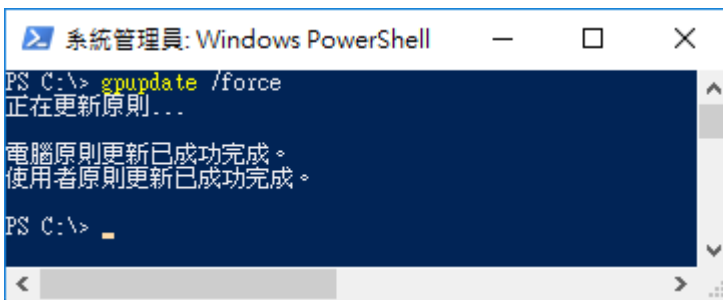


(3) 開啟 [Windows PowerShell]



(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:\*

```
系統管理員: Windows PowerShell
PS C:\> 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          成功與失敗
IPSEC driver        沒有稽核
其他系統事件        成功與失敗
安全性狀態變更      成功
登入/登出
登入                成功與失敗
登出                成功與失敗
帳戶鎖定            成功與失敗
IPsec 主要模式      成功與失敗
IPsec 快速模式      成功與失敗
IPsec 延伸模式      成功與失敗
特殊登入            成功與失敗
其他登入/登出事件  成功與失敗
網路原則伺服器      成功與失敗
使用者/裝置宣告    成功與失敗
群組成員資格        成功與失敗
物件存取
檔案系統            成功與失敗
registry            成功與失敗
核心物件            成功與失敗
SAM                 成功與失敗
憑證服務            成功與失敗
產生的應用程式      成功與失敗
控制代碼操縱        成功與失敗
檔案共用            成功與失敗
篩選平台封包丟棄    成功與失敗
篩選平台連線        成功與失敗
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      成功與失敗
集中原則暫存        成功與失敗
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        成功
驗證原則變更        成功
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        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
使用者帳戶管理      成功
DS 存取
目錄服務存取        成功
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 成功與失敗
其他帳戶登入事件    成功與失敗
Kerberos 驗證服務    成功與失敗
認證驗證            成功與失敗
PS C:\>
```

## 6.2.2 事件檔案設定

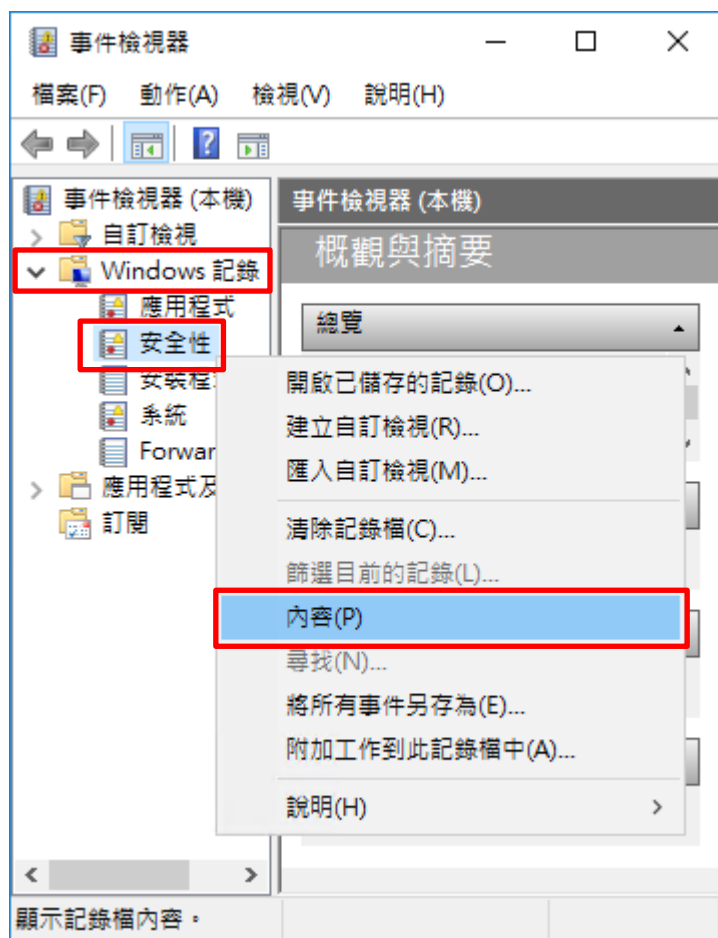
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入 [事件記錄檔](#) -> 點選 [檢視事件記錄檔]



## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(4) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx

記錄檔大小: 9.07 MB(9,506,816 位元組)

建立日期: 2021年3月8日 下午 09:42:35

修改日期: 2021年3月17日 下午 05:00:12

存取日期: 2021年3月8日 下午 09:42:35

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

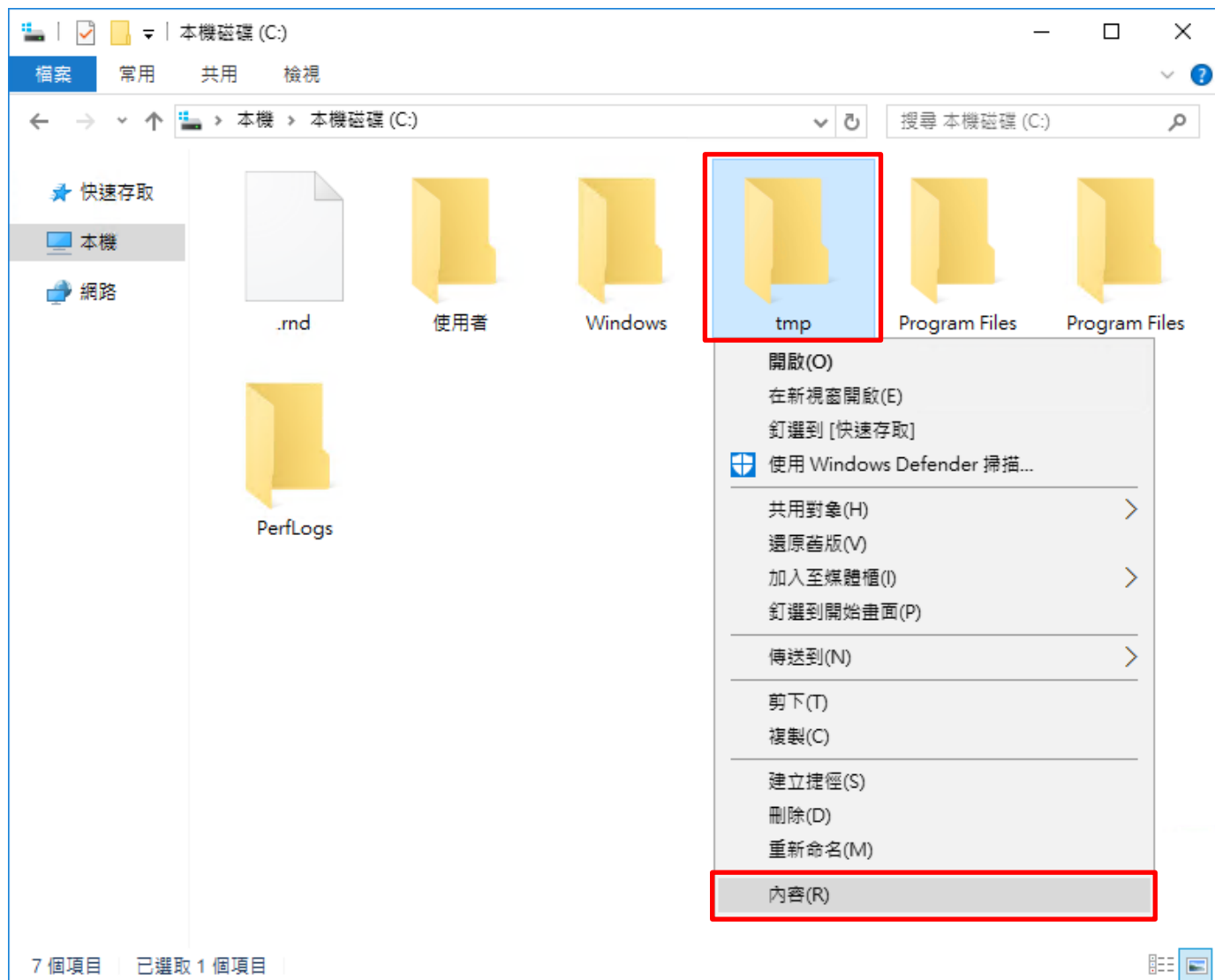
清除記錄(R)

確定 取消 套用(P)

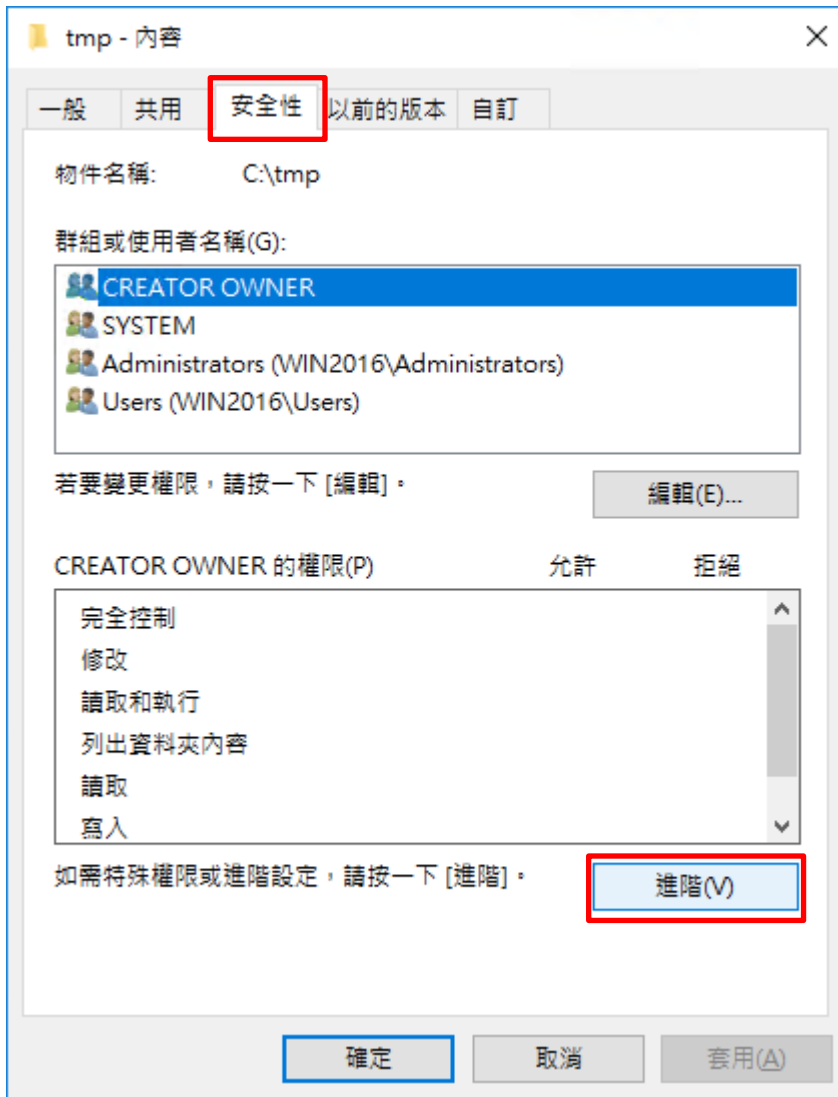


## 6.3 稽核資料夾設定

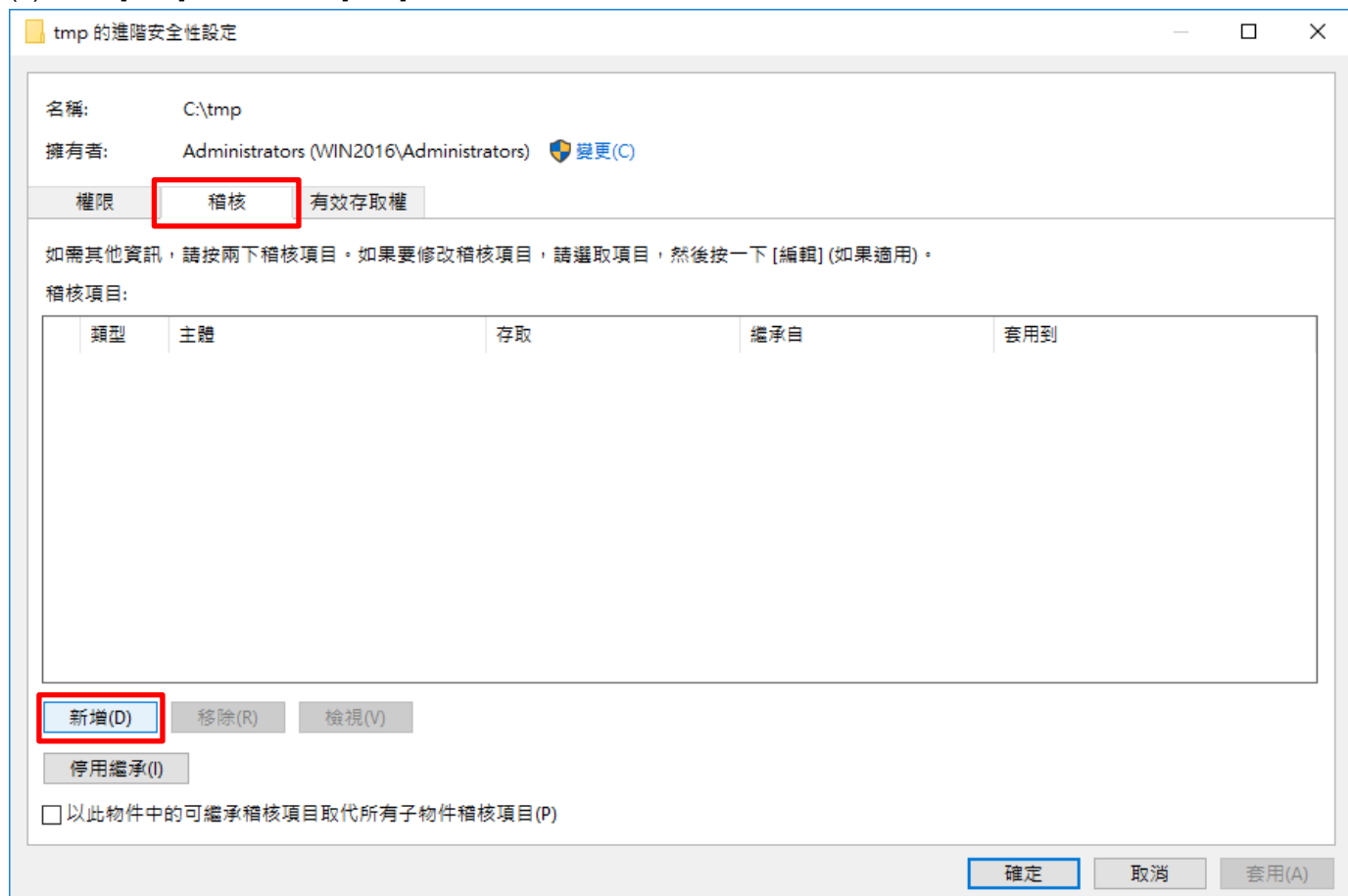
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



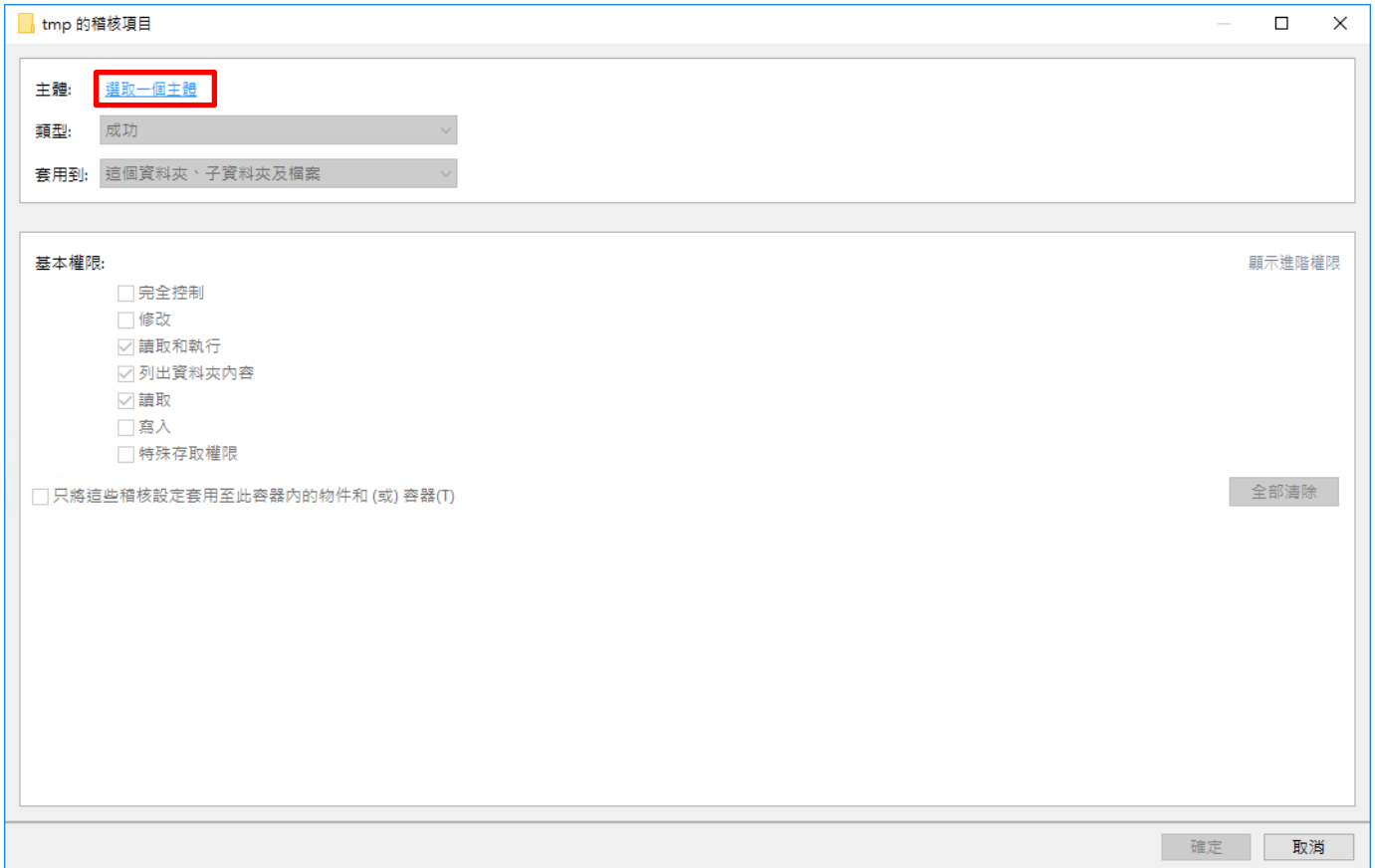
(2) 點選 [安全性] 頁面 -> 按 [進階]



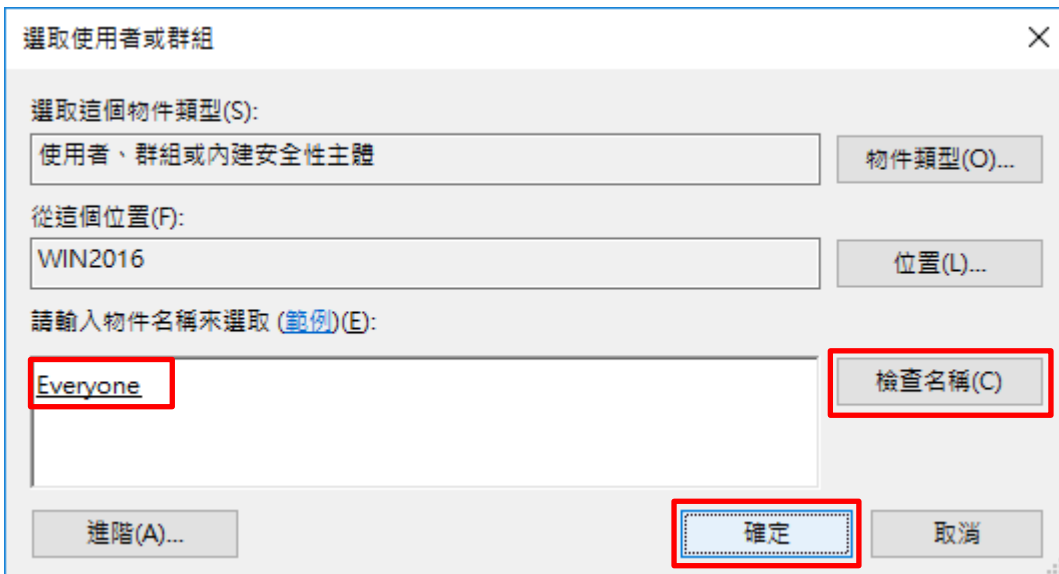
(3) 點選 [稽核] 頁面 -> 按 [新增]



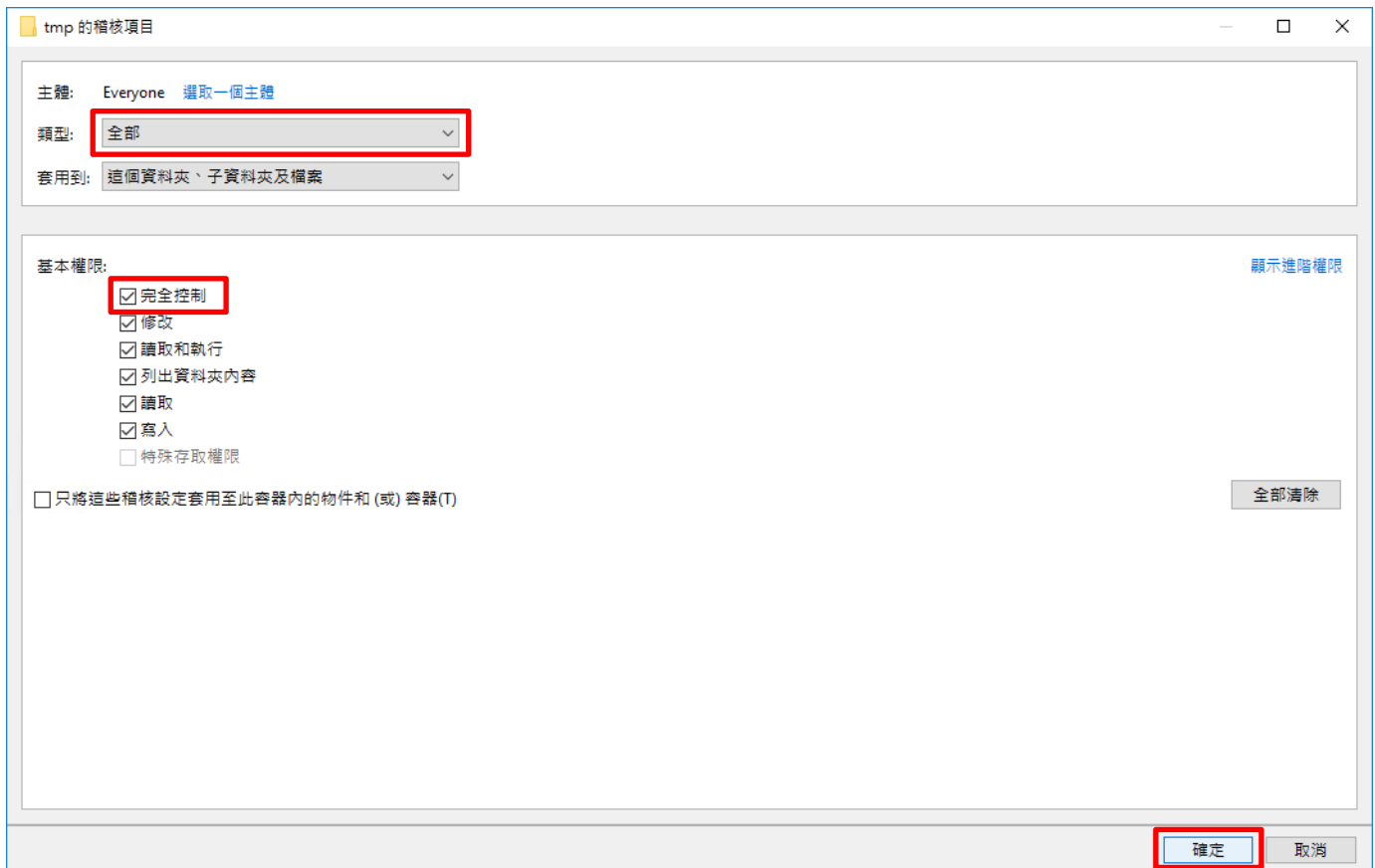
(4) 點選 [選取一個主體]



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



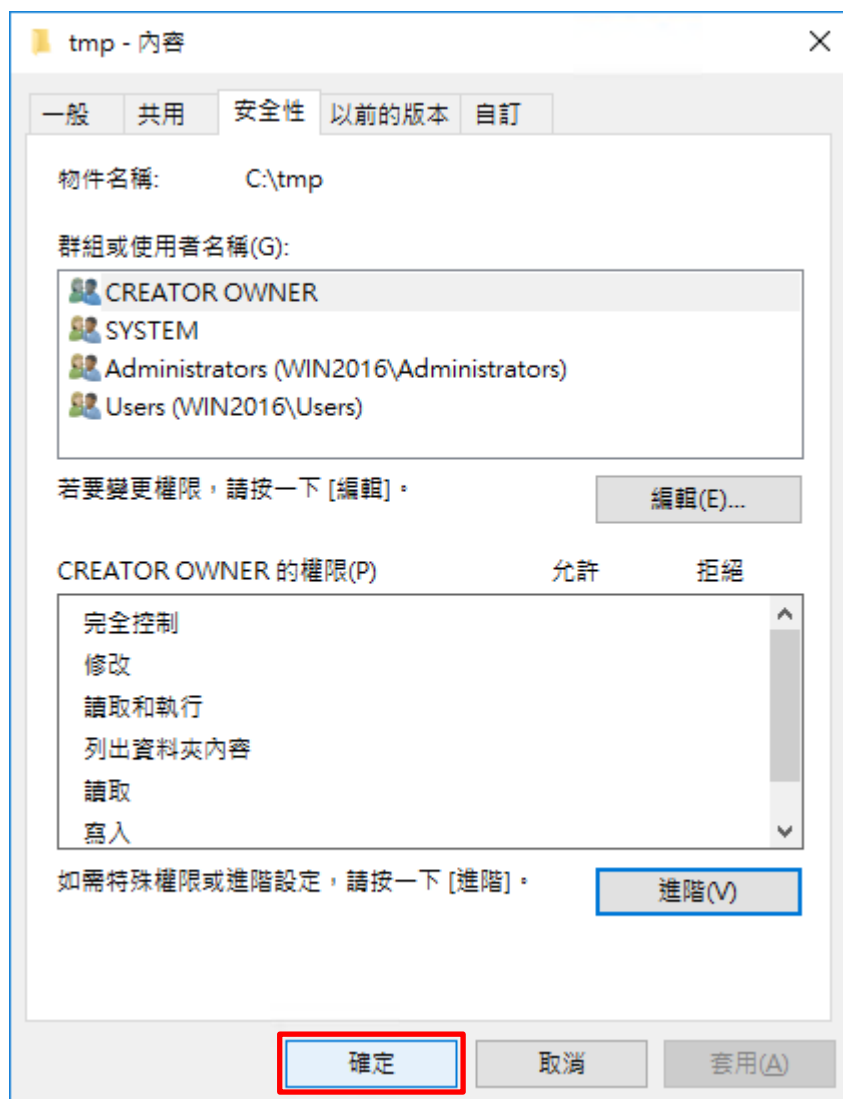
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(7) 顯示稽核主體 [Everyone] -> 按 [確定]



(8) 按 [確定]



## 7. Windows 2019

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

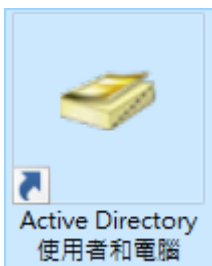
※ 以下分別為網域和工作群組設定方式。

### 7.1 網域

#### 7.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

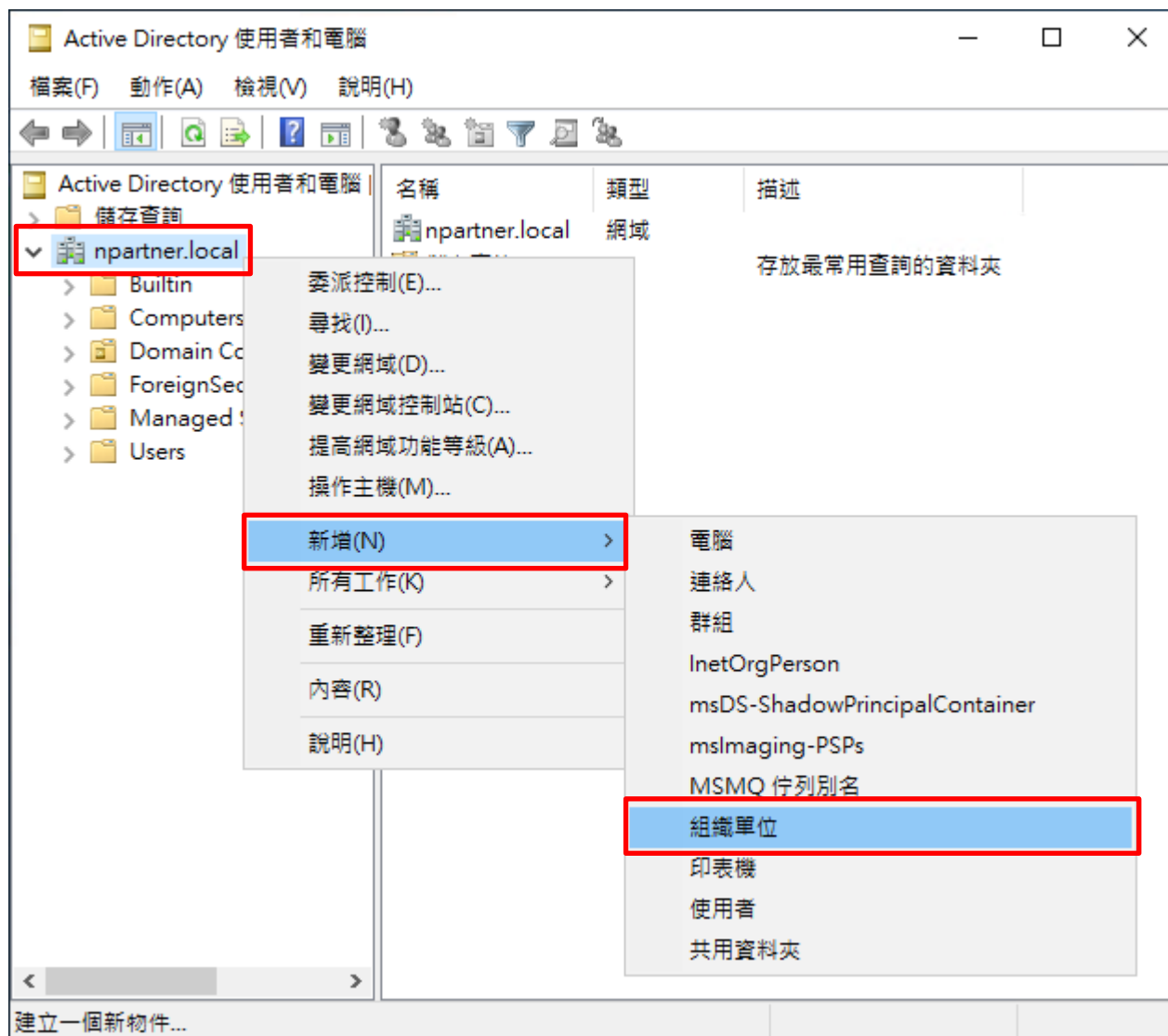
開啟 [Active Directory 使用者和電腦]





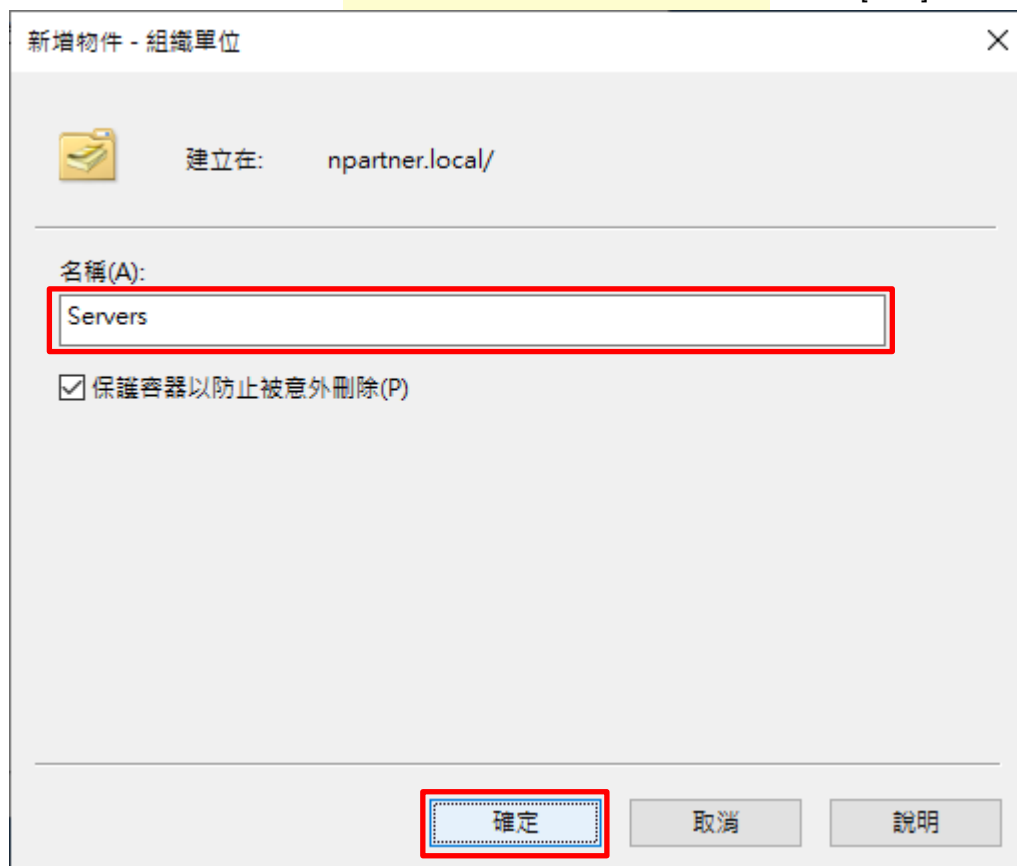
## (2) 新增組織單位

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 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/

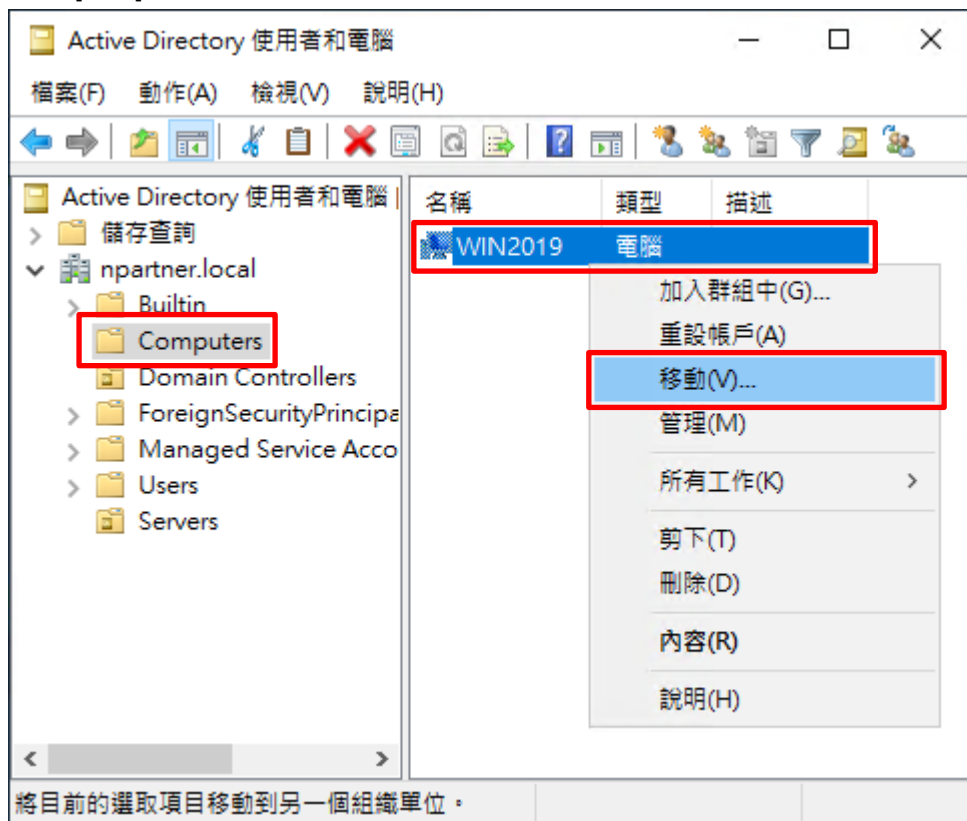
名稱(A):  
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

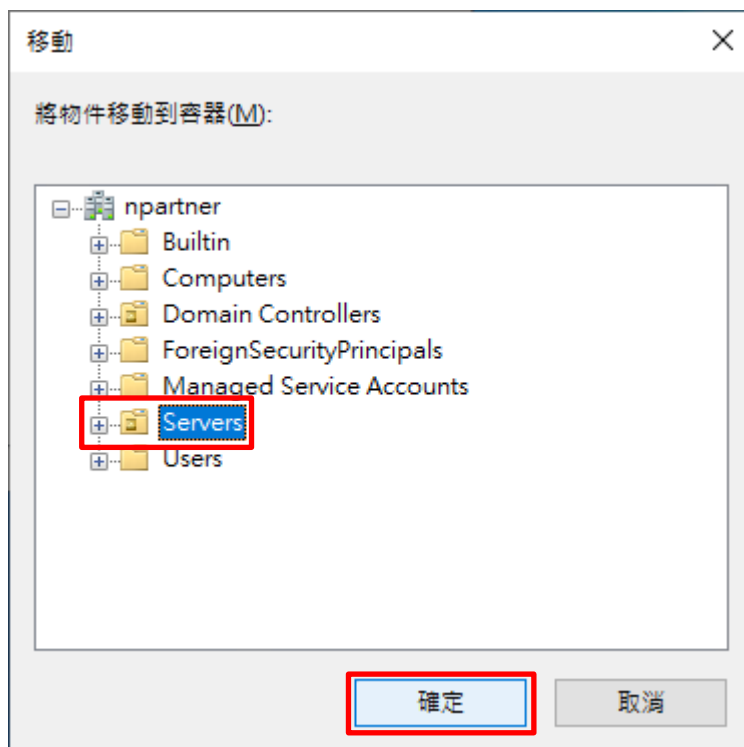
(4) 移動伺服器至新的組織單位

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



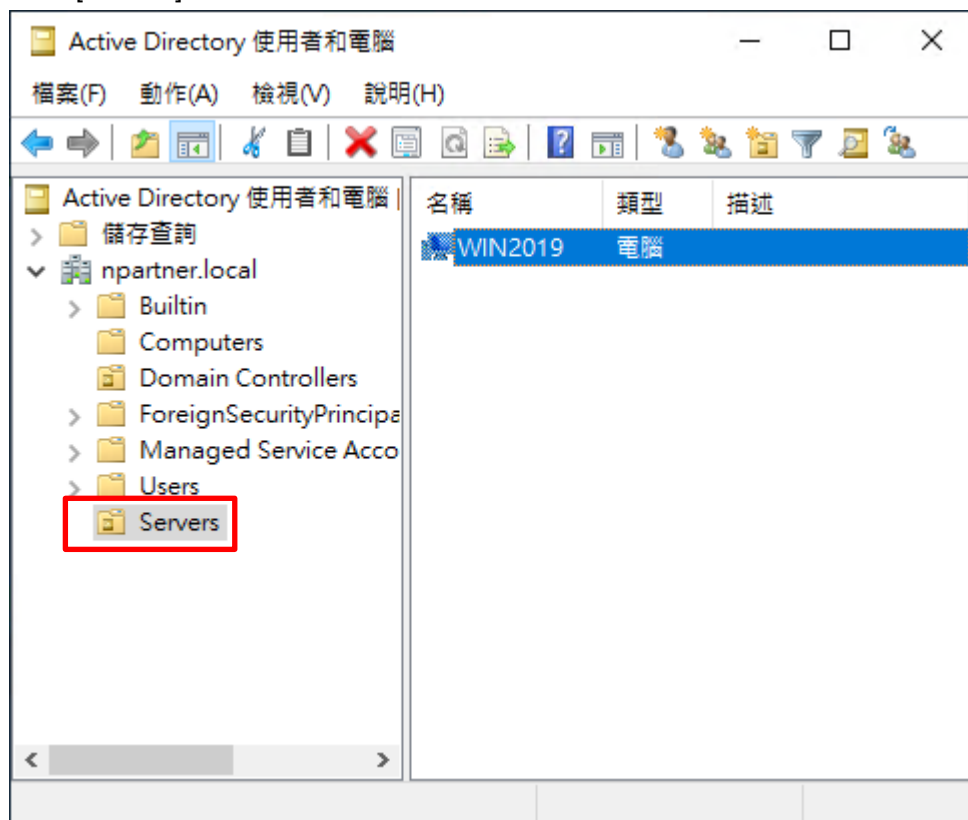
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

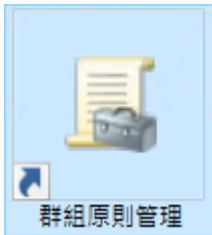
點選 [Servers] 組織單位，確認 Win2019 伺服器已移動



## 7.1.2 群組原則設定

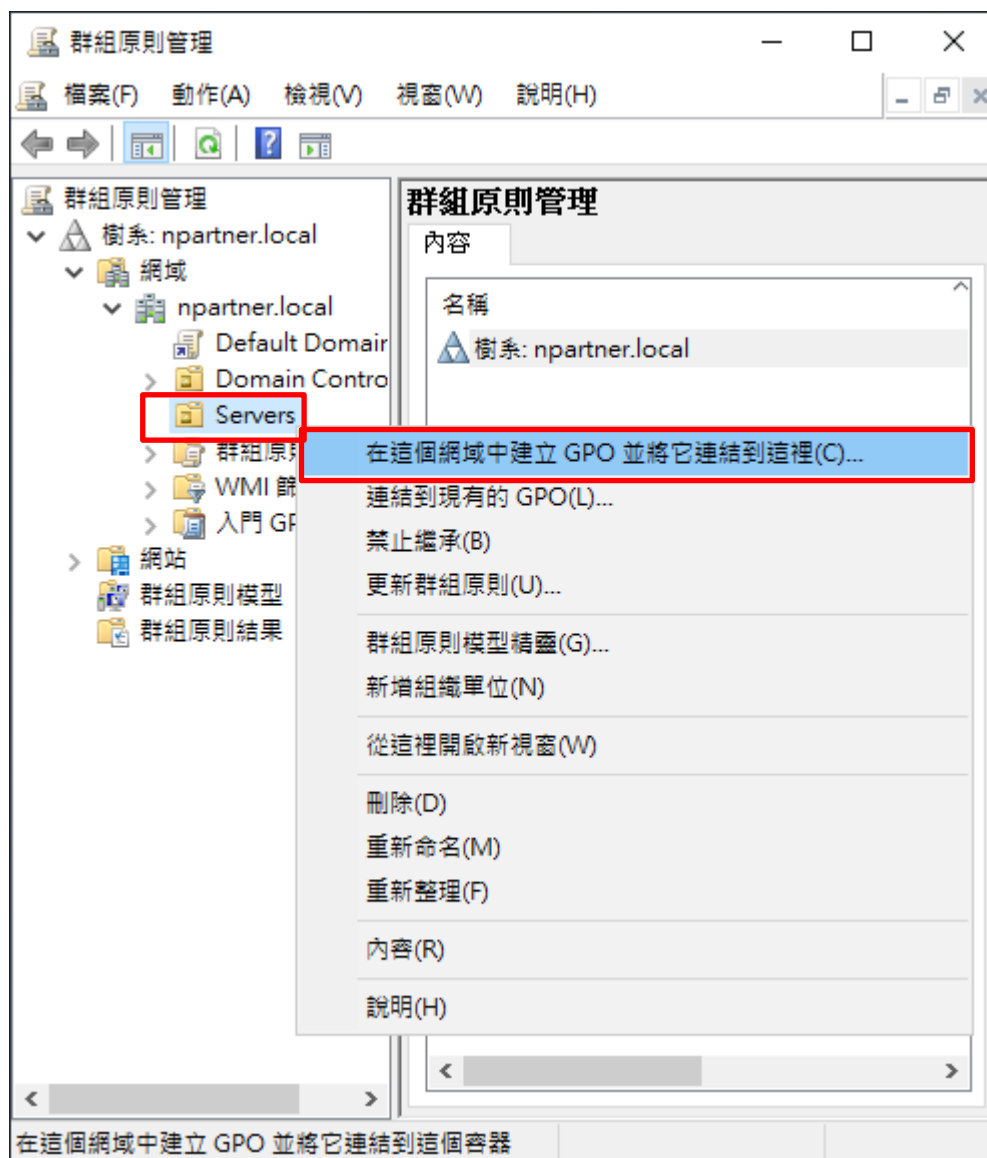
### (1) 開啟群組原則管理

開啟 [群組原則管理]



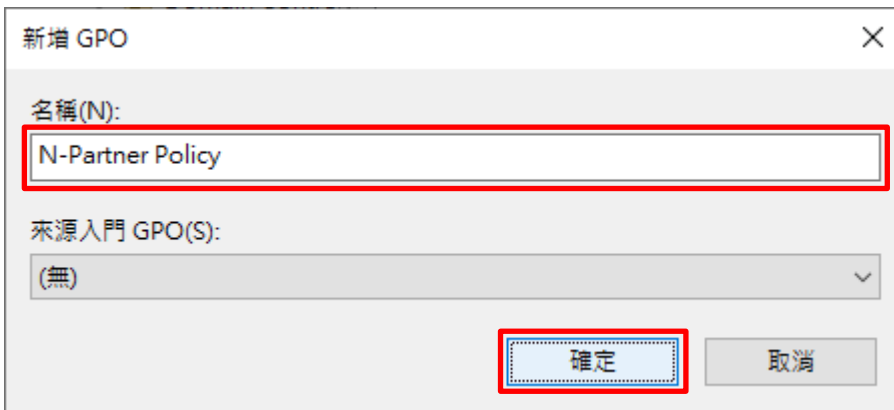
### (2) 在 Servers 組織單位，新增群組原則物件

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...]



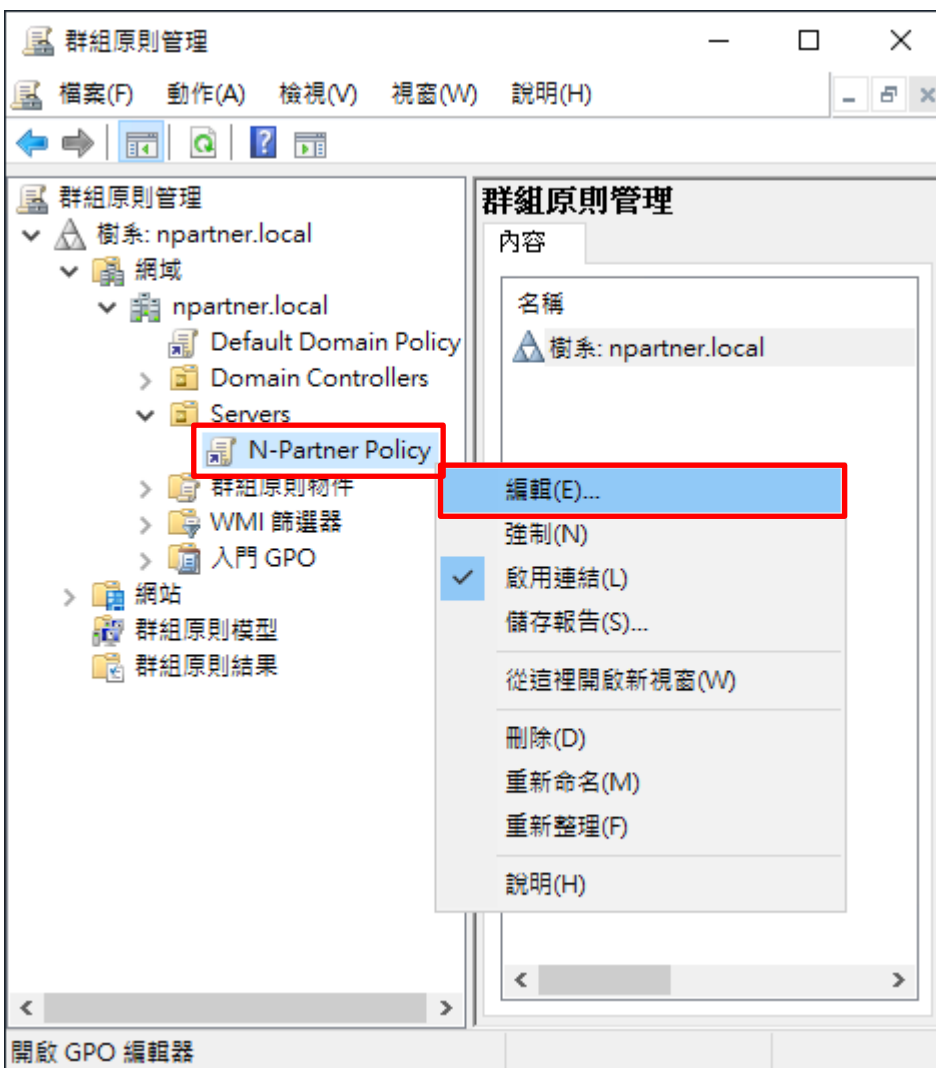
(3) 輸入群組原則物件名稱

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



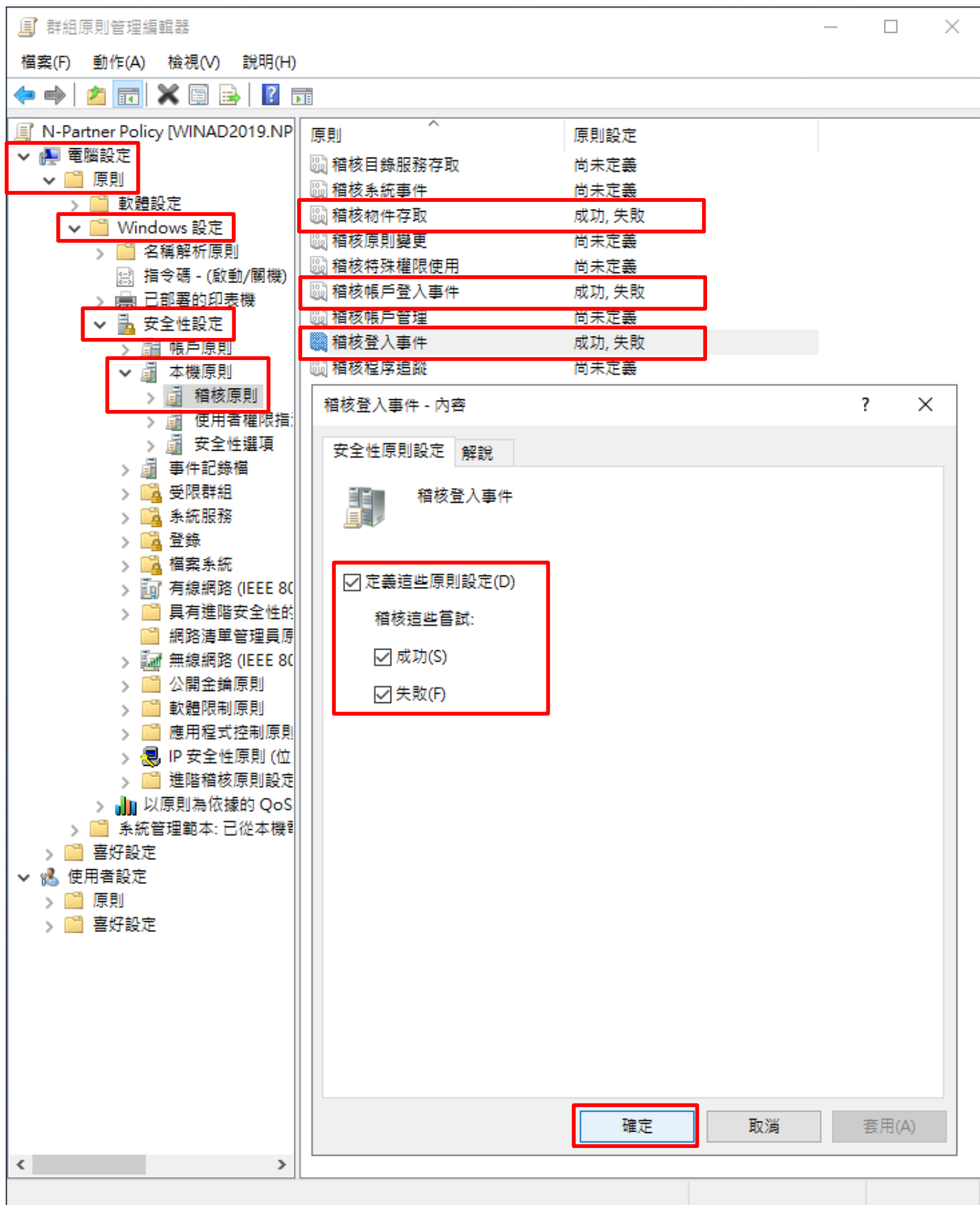
(4) 編輯群組原則物件

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



(5) 本機原則：稽核原則

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





(6) 事件記錄檔：安全性記錄檔大小最大值

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

The screenshot shows the Group Policy Editor window titled "群組原則管理編輯器". The left-hand navigation pane is expanded to show the following path: "電腦設定" (Computer Configuration) > "原則" (Policies) > "Windows 設定" (Windows Settings) > "安全性設定" (Security Settings) > "事件記錄檔" (Event Log). The right-hand pane displays a list of policies. The policy "安全性記錄檔大小最大值" (Maximum size of security log) is selected and highlighted. Its current value is "204800 KB".

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

An inset dialog box titled "安全性記錄檔大小最大值 - 內容" (Maximum size of security log - Content) is open. It shows the "安全性原則設定" (Security Policy Setting) tab. The "定義這個原則設定(D)" (Define this policy setting) checkbox is checked. Below it, the value "204800" is entered in a text box, followed by a dropdown menu set to "KB". A warning icon and text are present: "修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)". At the bottom of the dialog, the "確定" (OK) button is highlighted.



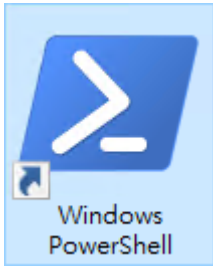
(7) 事件記錄檔：安全性記錄檔保持方法

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

The screenshot shows the Group Policy Editor window for 'N-Partner Policy [WINAD2019.NP]'. The left-hand navigation pane is expanded to show the path: 電腦設定 (Computer Configuration) > 原則 (Policy) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies. The policy '安全性記錄檔保持方法' (Security Log Retention Method) is selected and highlighted. Below this, a dialog box titled '安全性記錄檔保持方法 - 內容' (Security Log Retention Method - Content) is open. In this dialog, the '安全性原則設定' (Security Policy Settings) tab is active. The '定義這個原則設定(D)' (Define this policy setting) checkbox is checked. Underneath, the radio button for '視需要覆寫事件(V)' (Override based on requirements) is selected. A warning icon and text are visible at the bottom of the dialog, stating that changes may affect compatibility. At the bottom of the dialog, the '確定' (OK) button is highlighted with a red box.

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

(8) 開啟 [Windows PowerShell]



(9) 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 titled "系統管理員: Windows PowerShell". The terminal shows the command `Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force` being entered and executed. The output is a single underscore character `_`. The text "Win2019" in the command is highlighted in red in the original image.

紅色文字部位請輸入 Windows File 伺服器名稱

(10) 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 titled "選取 系統管理員: Windows PowerShell". The terminal 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\MS837D4486_2D73_4EB2_B046_810189B95F80`, `LoggingComputer : Win2019`, `LoggingUser : NPARTNER\administrator`, and `LoggingMode : Computer`. The text "Win2019" in the command is highlighted in red in the original image.

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

(11) 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: 2022/3/17 上午 09:56:51 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/稽核原則 隱藏

原則	設定	優勢 GPO
稽核物件存取	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy

本機原則/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

**群組原則物件** 顯示

**WMI 篩選器** 顯示

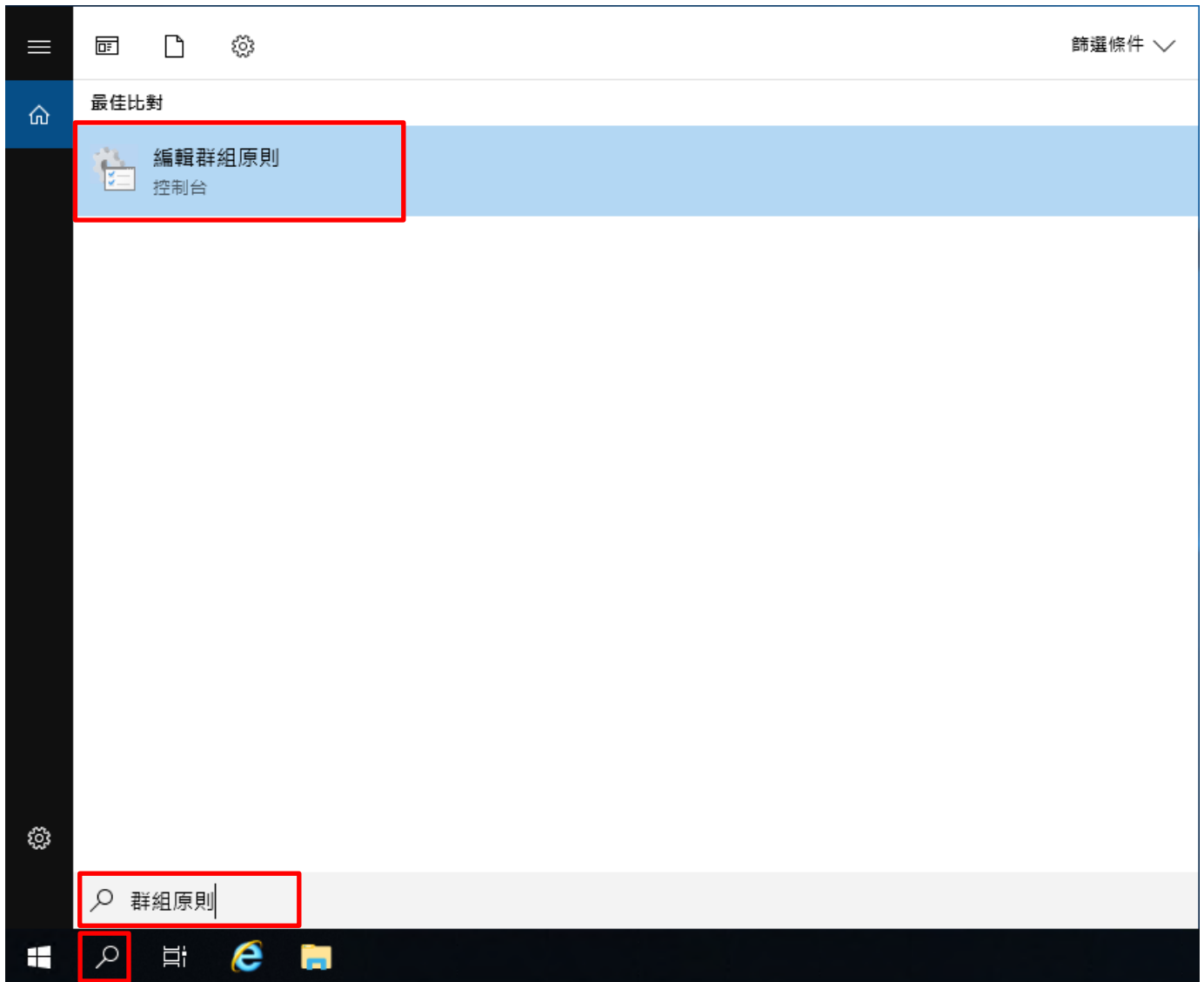
**使用者詳細資料** 顯示

## 7.2 工作群組

### 7.2.1 稽核原則設定

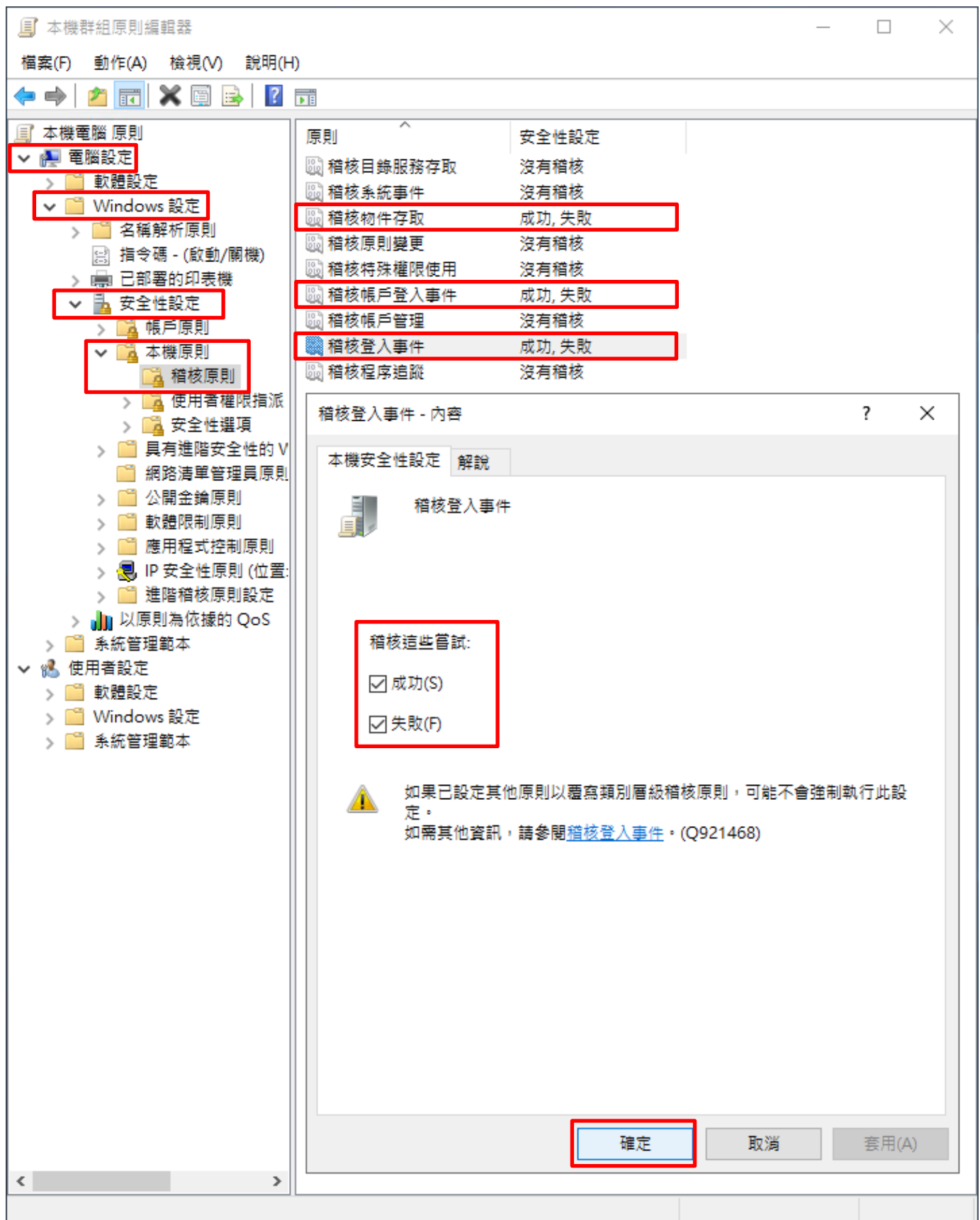
(1) 開啟本機群組原則編輯器

點選  [搜尋] -> 輸入 **群組原則** -> 點選 [編輯群組原則]

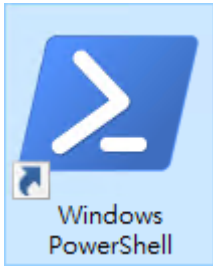


(2) 本機原則：稽核原則

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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

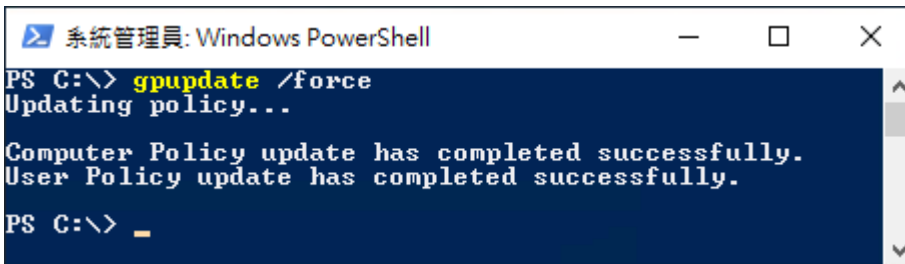


(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The terminal content shows the command "gpupdate /force" being executed, followed by "Updating policy...", "Computer Policy update has completed successfully.", and "User Policy update has completed successfully.". The prompt "PS C:\>" is visible at the bottom.

```
系統管理員: Windows PowerShell
PS C:\> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\> _
```

(5) 查看群組原則套用情形

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

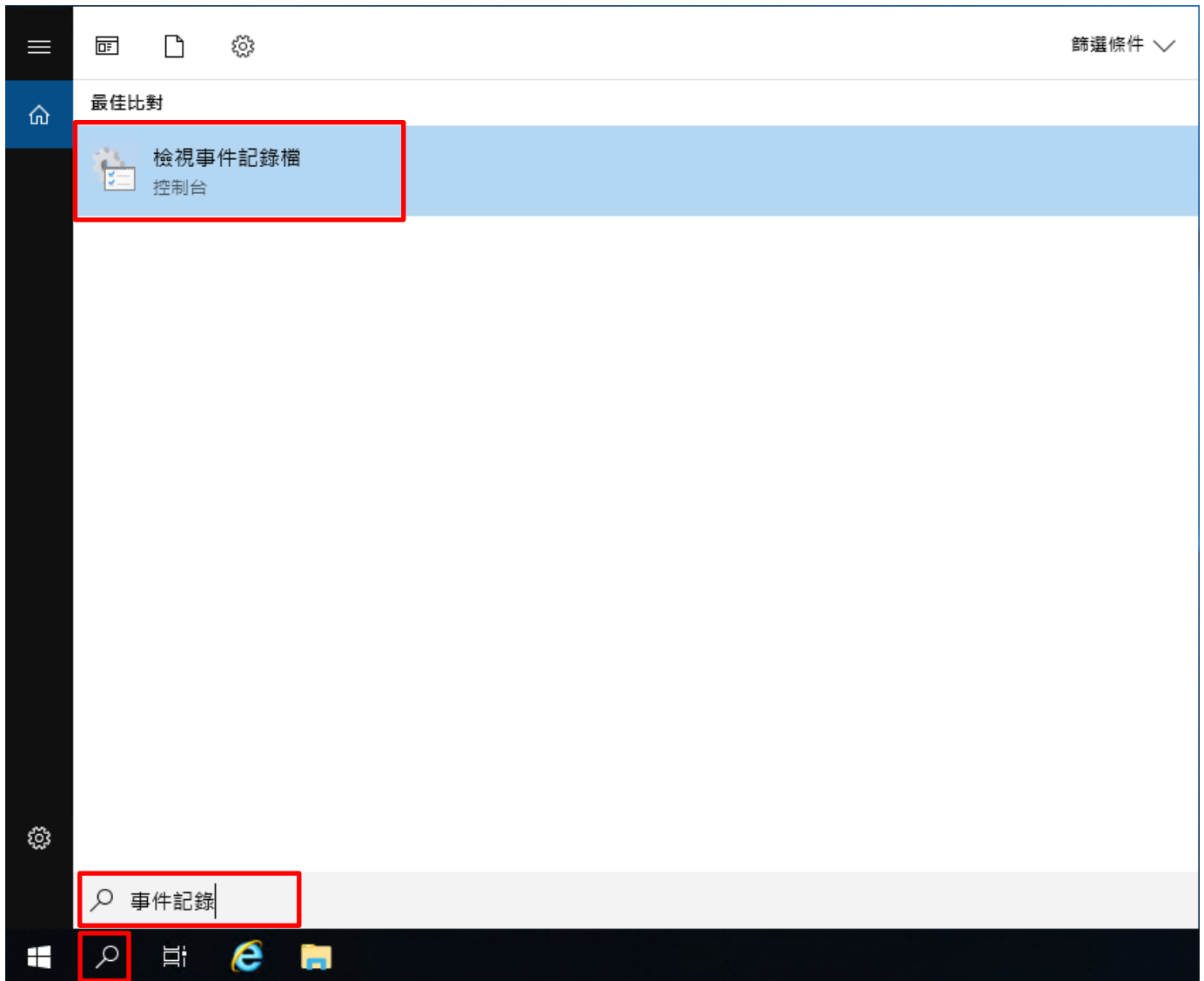
```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
系統
  安全性系統延伸          No Auditing
  系統完整性              Success and Failure
  IPSEC driver             No Auditing
  其他系統事件            Success and Failure
  安全性狀態變更          Success
登入/登出
  登入                    Success and Failure
  登出                    Success and Failure
  帳戶鎖定                Success and Failure
  IPsec 主要模式          Success and Failure
  IPsec 快速模式          Success and Failure
  IPsec 延伸模式          Success and Failure
  特殊登入                Success and Failure
  其他登入/登出事件      Success and Failure
  網路原則伺服器          Success and Failure
  使用者/裝置宣告        Success and Failure
  群組成員資格            Success and Failure
物件存取
  檔案系統                Success and Failure
  registry                 Success and Failure
  核心物件                Success and Failure
  SAM                     Success and Failure
  憑證服務                Success and Failure
  產生的應用程式          Success and Failure
  控制代碼操縱            Success and Failure
  檔案共用                Success and Failure
  篩選平台封包丟棄        Success and Failure
  篩選平台連線            Success and Failure
  其他物件存取事件        Success and Failure
  詳細檔案共用            Success and Failure
  抽取式存放裝置          Success and Failure
  集中原則暫存            Success and Failure
特殊權限使用
  非機密特殊權限使用      No Auditing
  其他特殊權限使用事件    No Auditing
  機密特殊權限使用        No Auditing
詳細追蹤
  建立處理程序            No Auditing
  終止處理程序            No Auditing
  DPAPI 活動                No Auditing
  RPC 事件                 No Auditing
  隨插即用事件            No Auditing
  權杖權限調整事件        No Auditing
原則變更
  稽核原則變更            Success
  驗證原則變更            Success
  授權原則變更            No Auditing
  MPSSUC 規則層級原則變更 No Auditing
  篩選平台原則變更        No Auditing
  其他原則變更事件        No Auditing
帳戶管理
  電腦帳戶管理            No Auditing
  安全性群組管理          No Auditing
  發佈群組管理            No Auditing
  應用程式群組管理        No Auditing
  其他帳戶管理事件        No Auditing
  使用者帳戶管理          No Auditing
DS 存取
  目錄服務存取            Success
  目錄服務變更            No Auditing
  目錄服務複寫            No Auditing
  詳細目錄服務複寫        No Auditing
帳戶登入
  Kerberos 服務票證操作    Success and Failure
  其他帳戶登入事件        Success and Failure
  Kerberos 驗證服務        Success and Failure
  認證驗證                Success and Failure
PS C:\>
```



## 7.2.2 事件檔案設定

(1) 開啟 [檢視事件記錄檔]

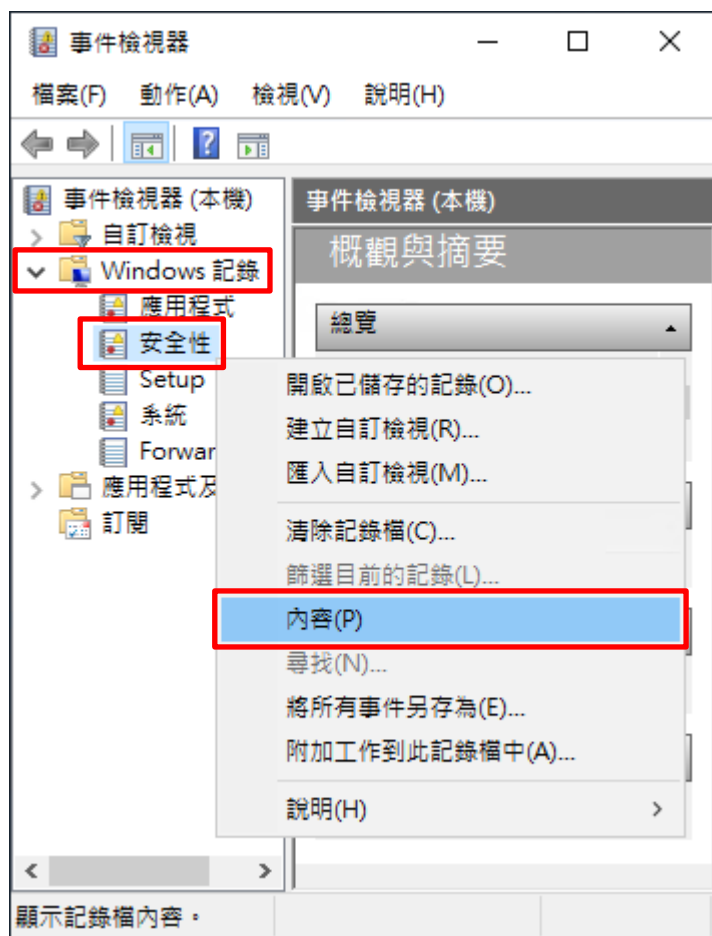
點選 [搜尋] -> 輸入事件記錄 -> 點選 [檢視事件記錄檔]





## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx

記錄檔大小: 20.00 MB(20,975,616 位元組)

建立日期: 2021年2月23日 下午 05:15:05

修改日期: 2021年3月18日 上午 09:18:18

存取日期: 2021年3月18日 上午 09:18:18

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

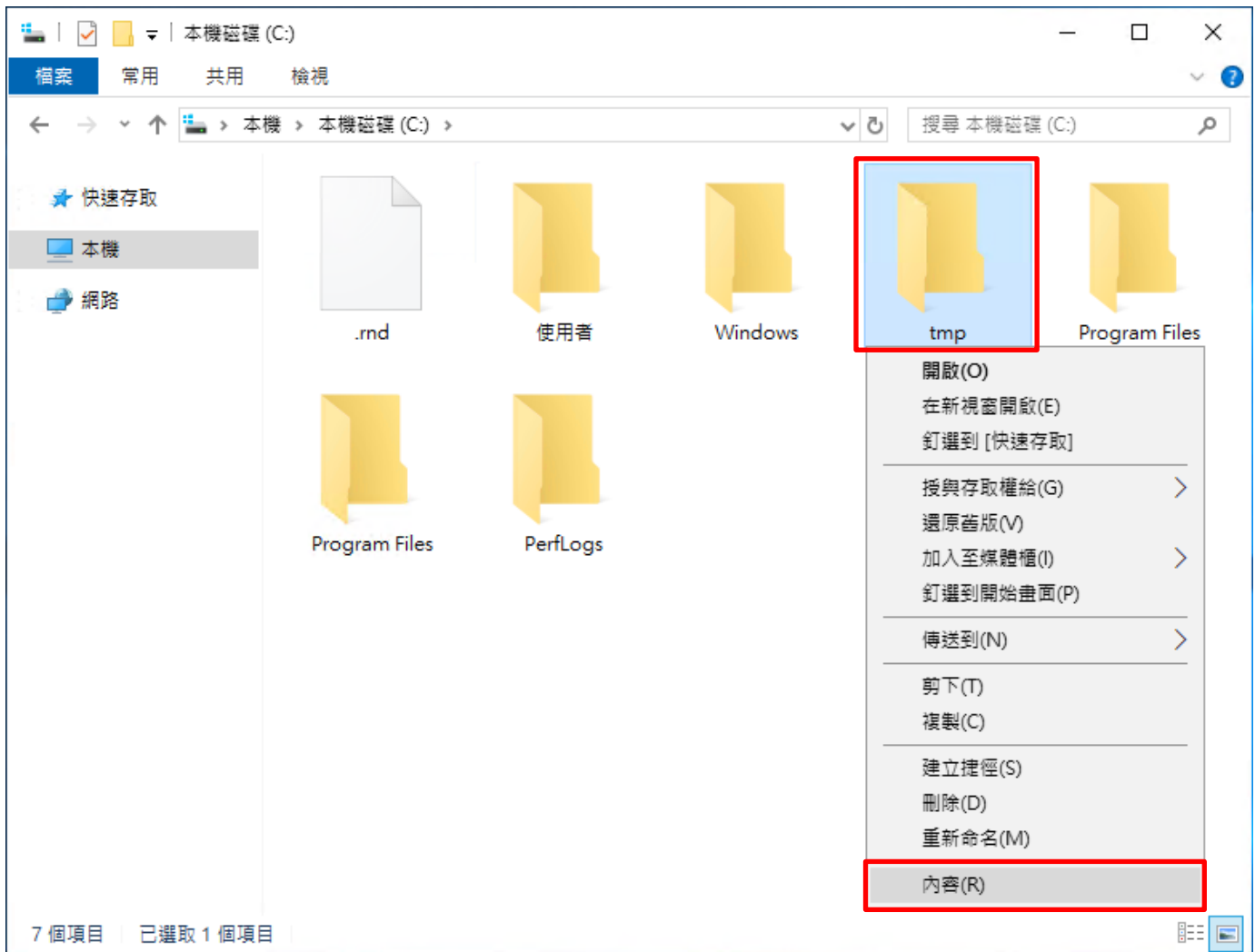
不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

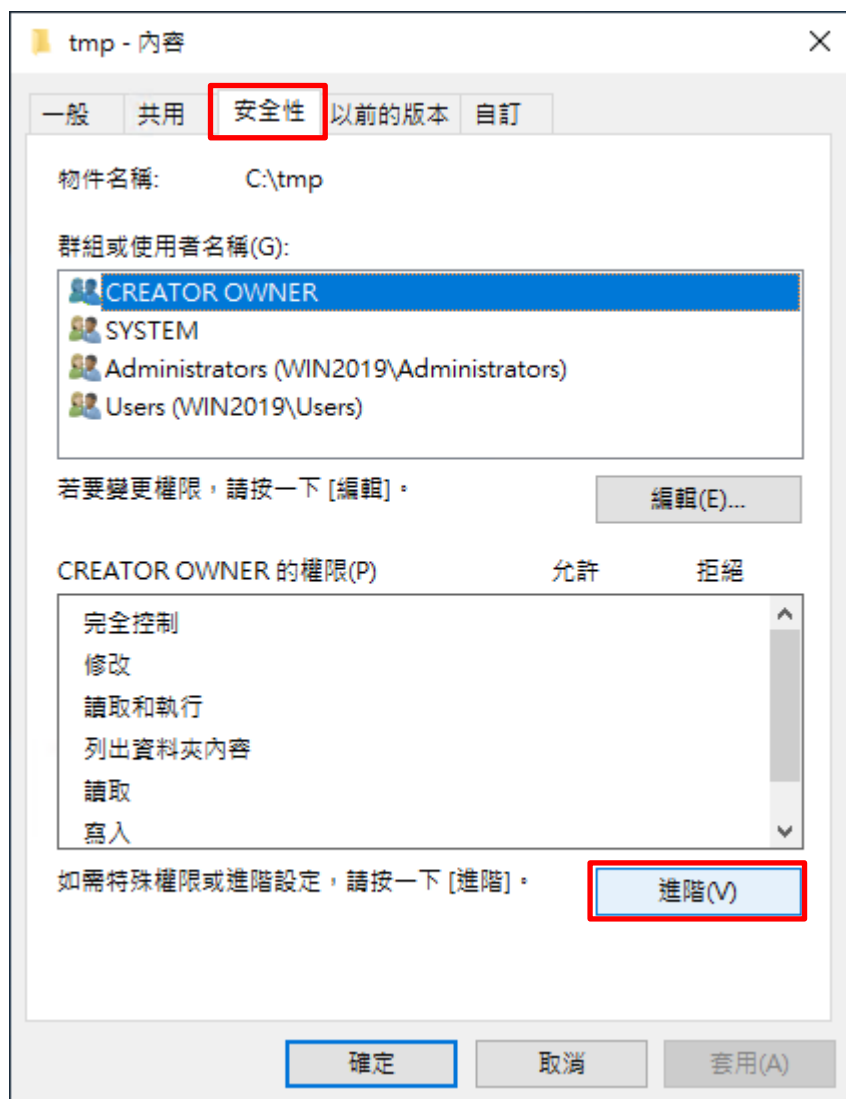
確定 取消 套用(P)

## 7.3 稽核資料夾設定

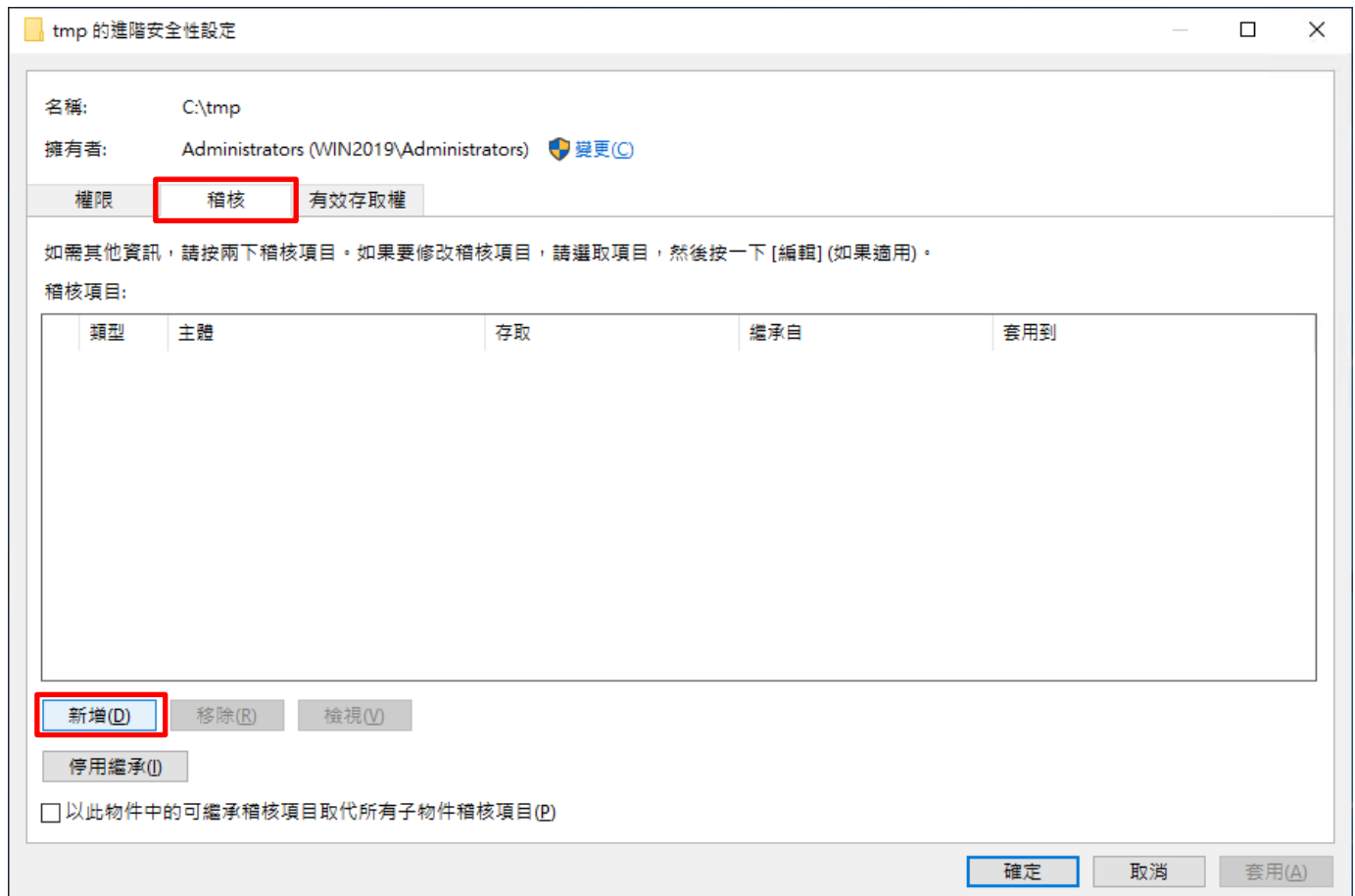
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



(2) 點選 [安全性] 頁面 -> 按 [進階]



(3) 點選 [稽核] 頁面 -> 按 [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 [檢查名稱] -> 按 [確定]



(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]

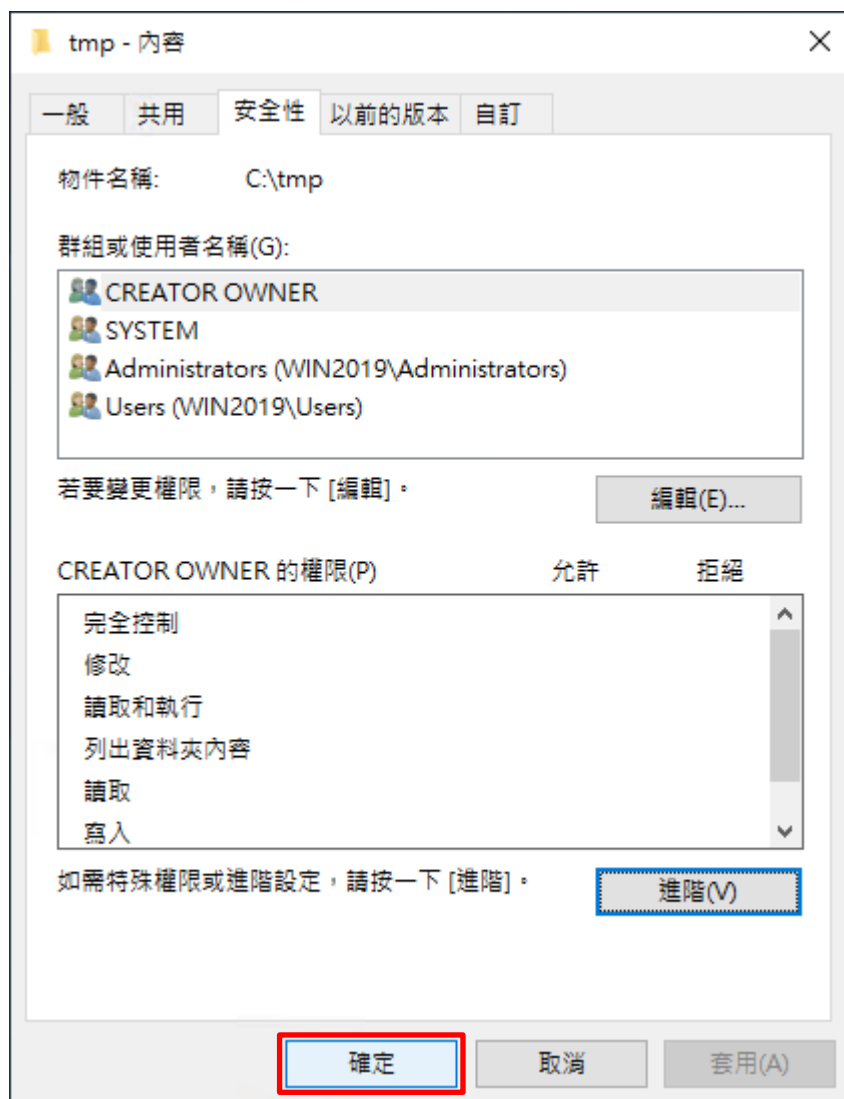


(7) 顯示稽核主體 [Everyone] -> 按 [確定]





(8) 按 [確定]



## 8. Windows 2022

Windows 稽核原則設定 [詳細說明請參考前言的稽核原則建議連結](#)

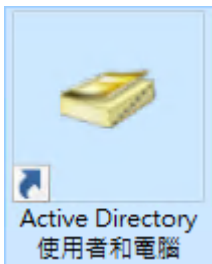
※ 以下分別為網域和工作群組設定方式。

### 8.1 網域

#### 8.1.1 組織單位設定

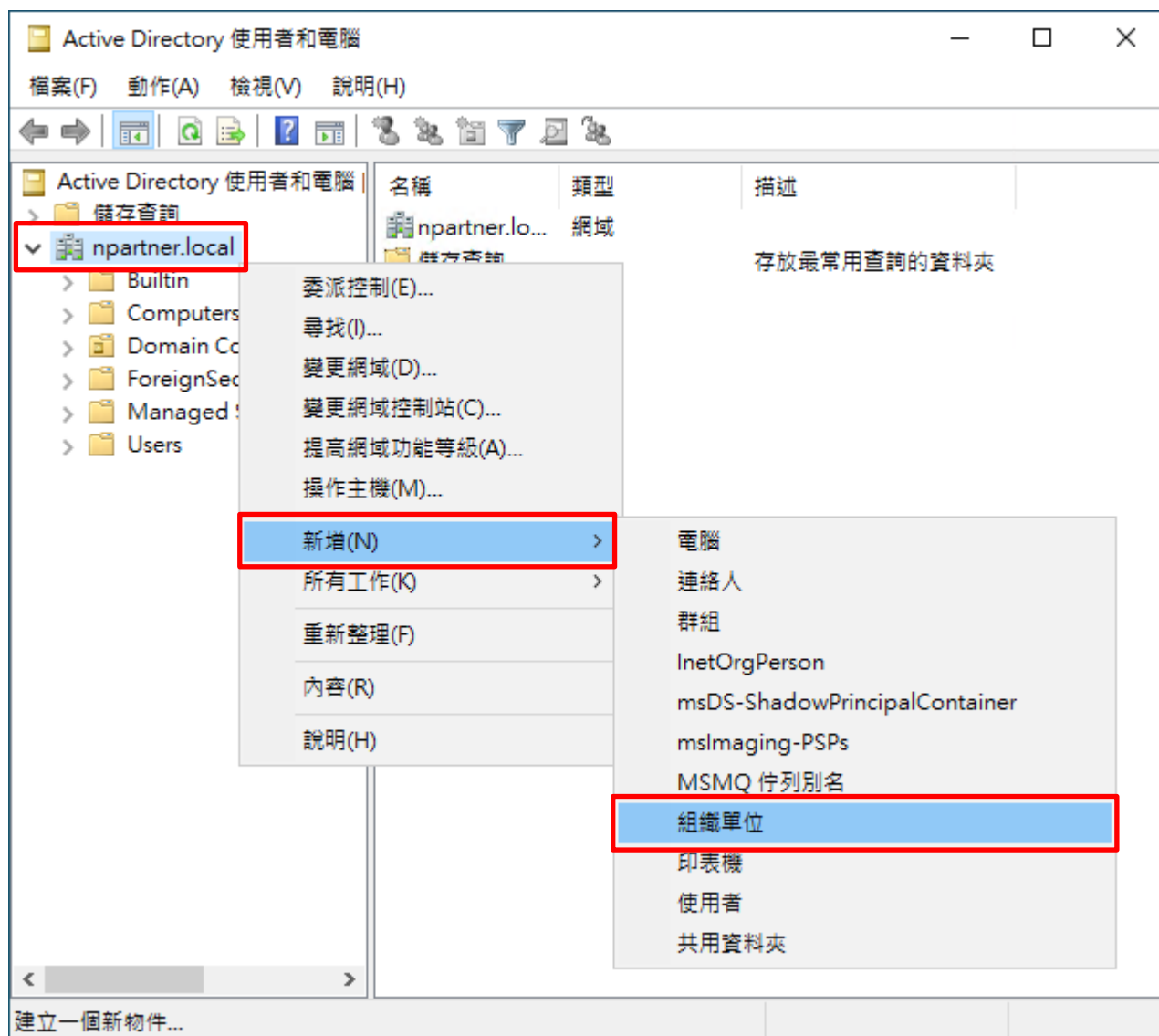
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



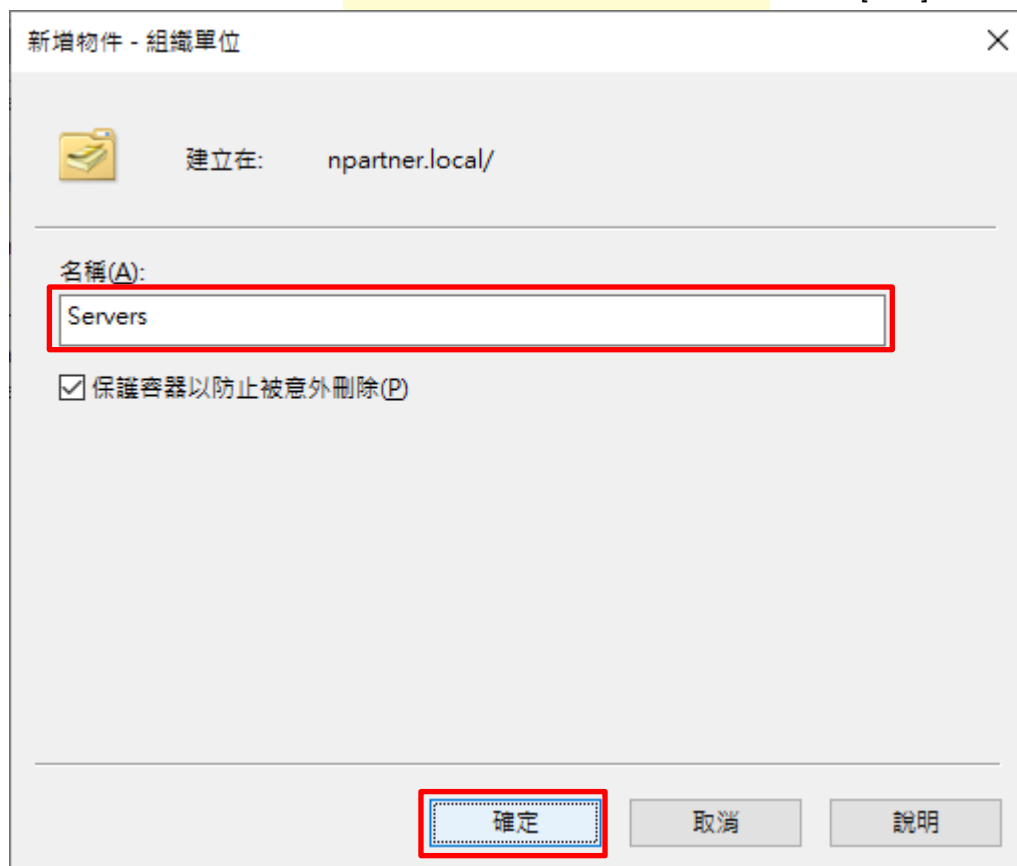
## (2) 新增組織單位

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 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



新增物件 - 組織單位

建立在: npartner.local/

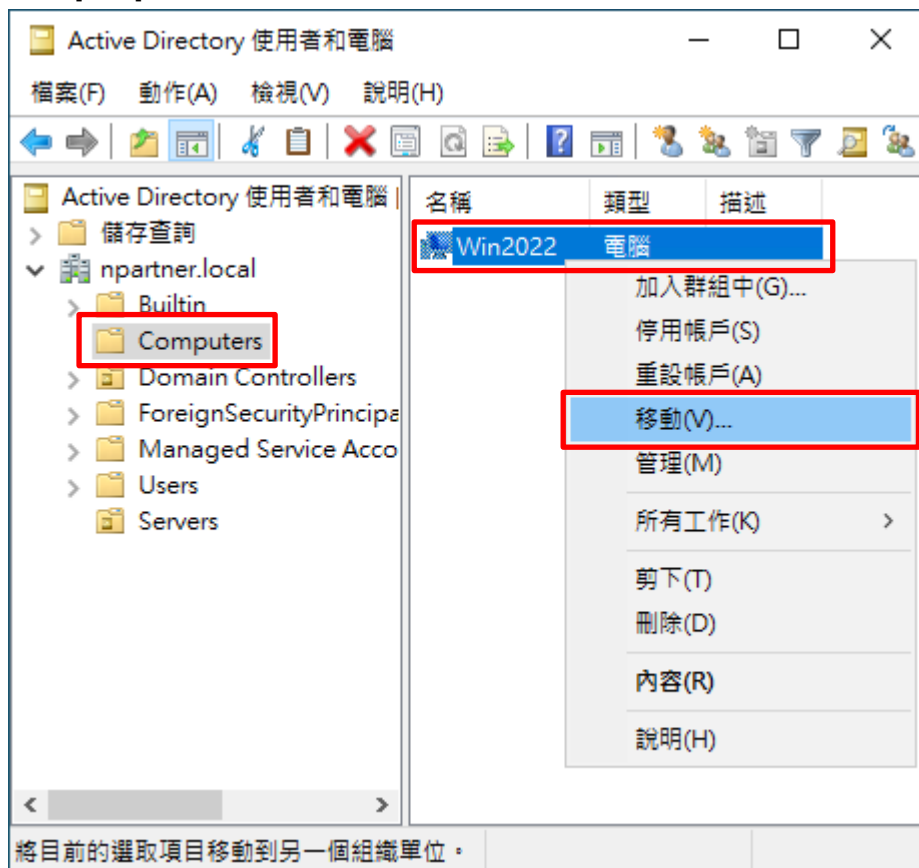
名稱(A):  
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

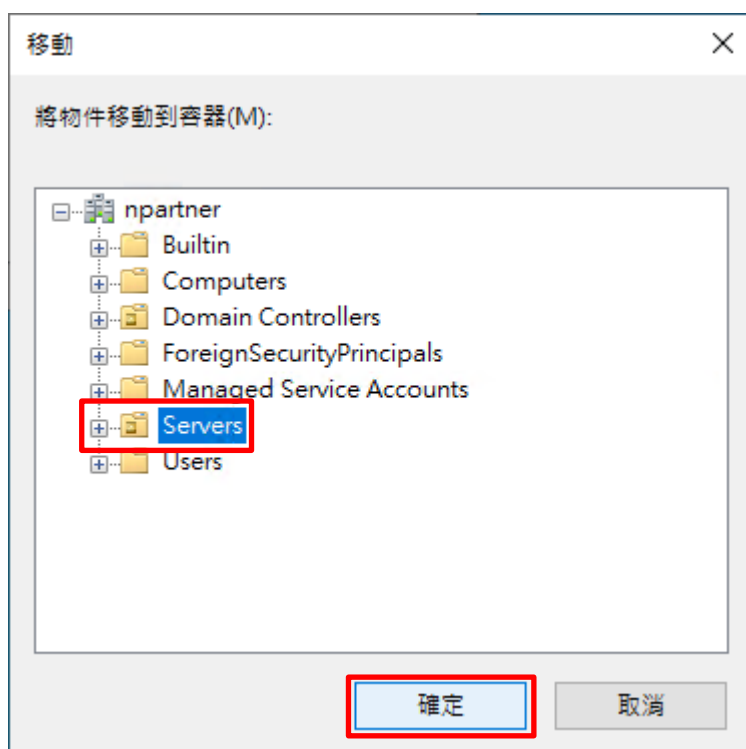
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [Win2022] 伺服器按滑鼠右鍵，註：請依客戶環境選擇 Windows File 伺服器 -> 點選 [移動]



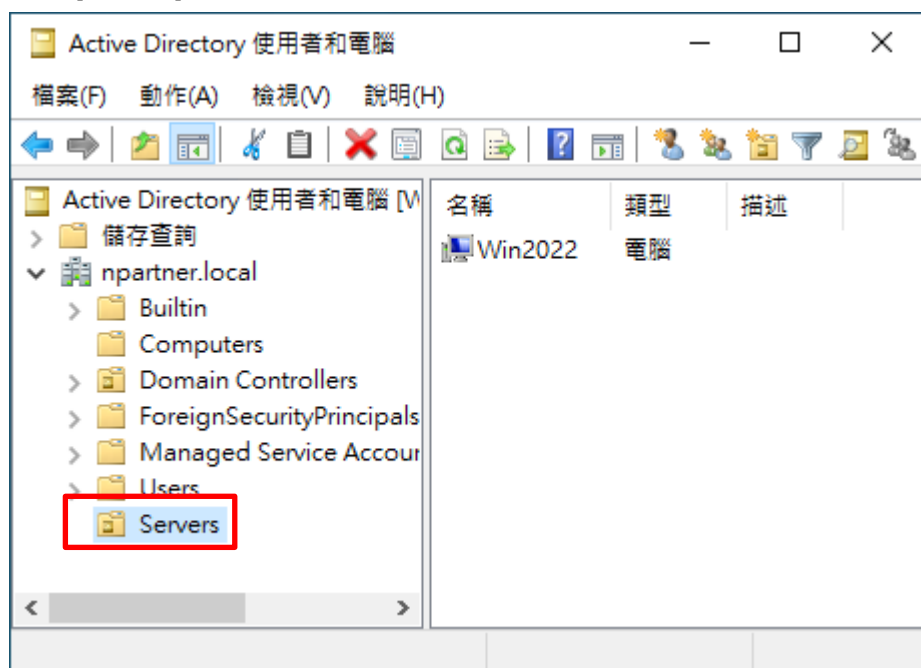
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

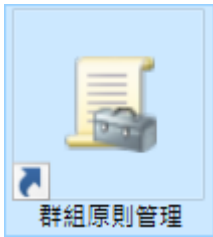
點選 [Servers] 組織單位，確認 Win2022 File 伺服器已移動



## 8.1.2 群組原則設定

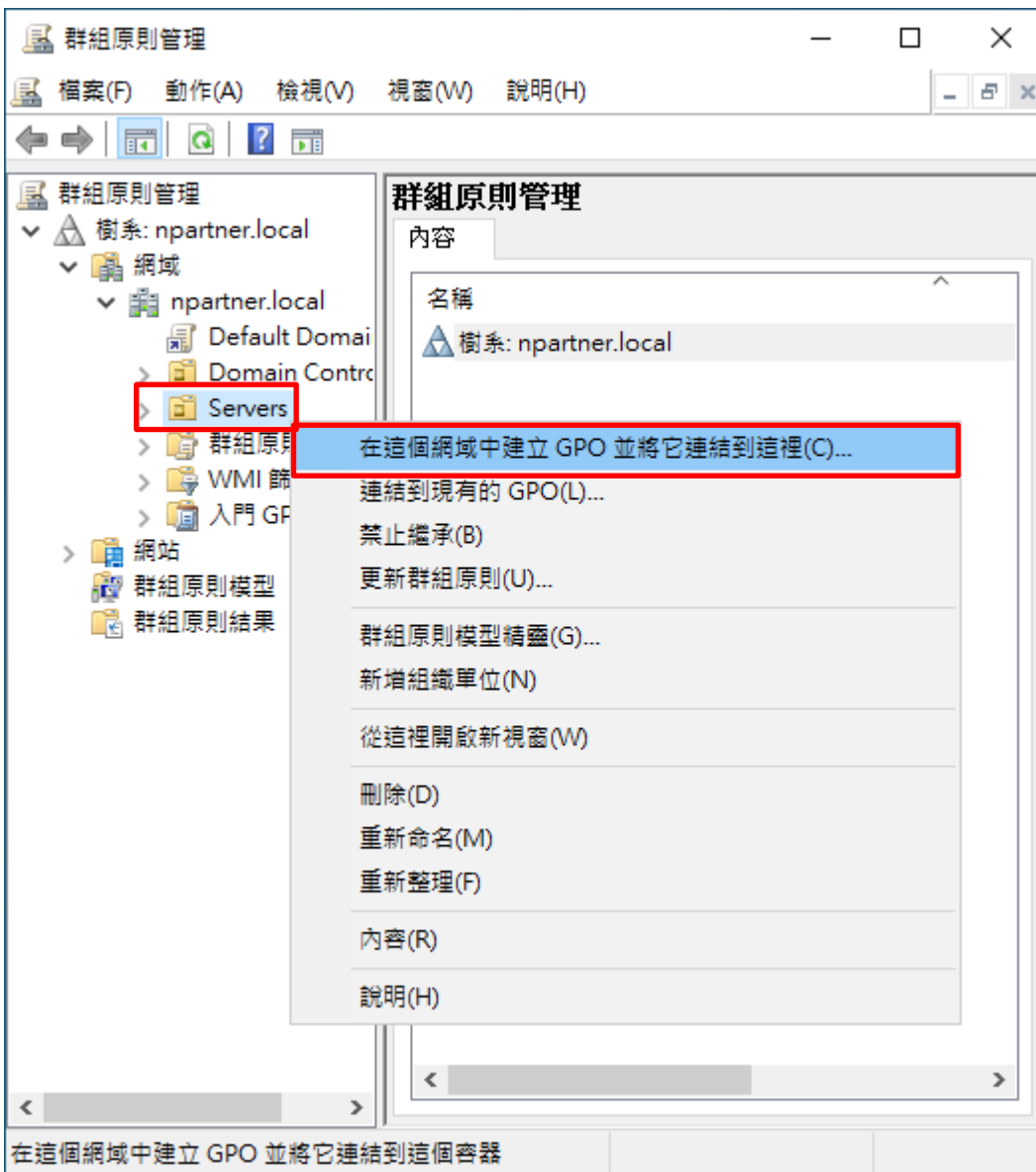
### (1) 開啟群組原則管理

開啟 [群組原則管理]



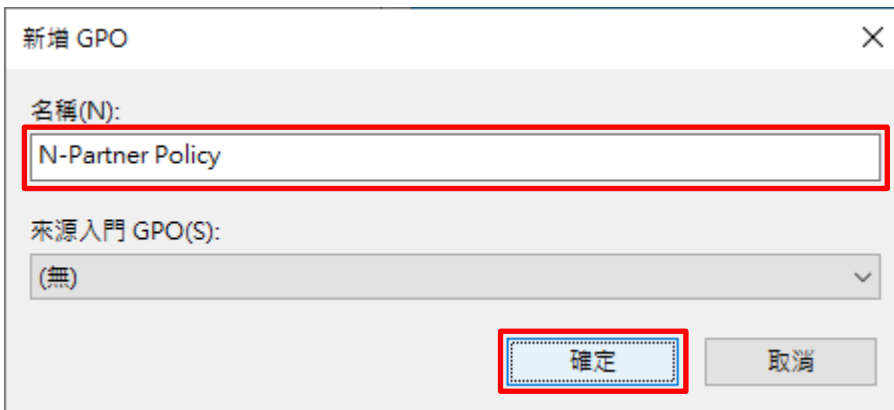
### (2) 在 Servers 組織單位，新增群組原則物件

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...]



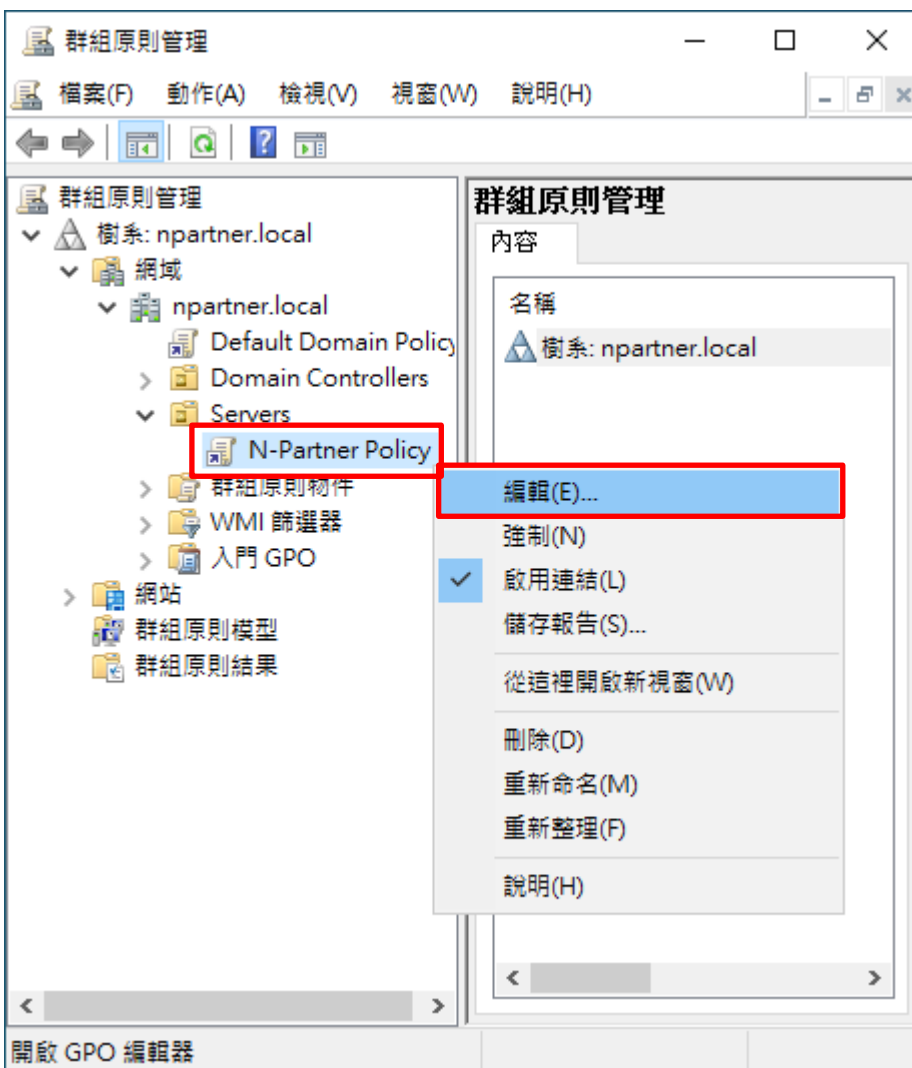
(3) 輸入群組原則物件名稱

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



(4) 編輯群組原則物件

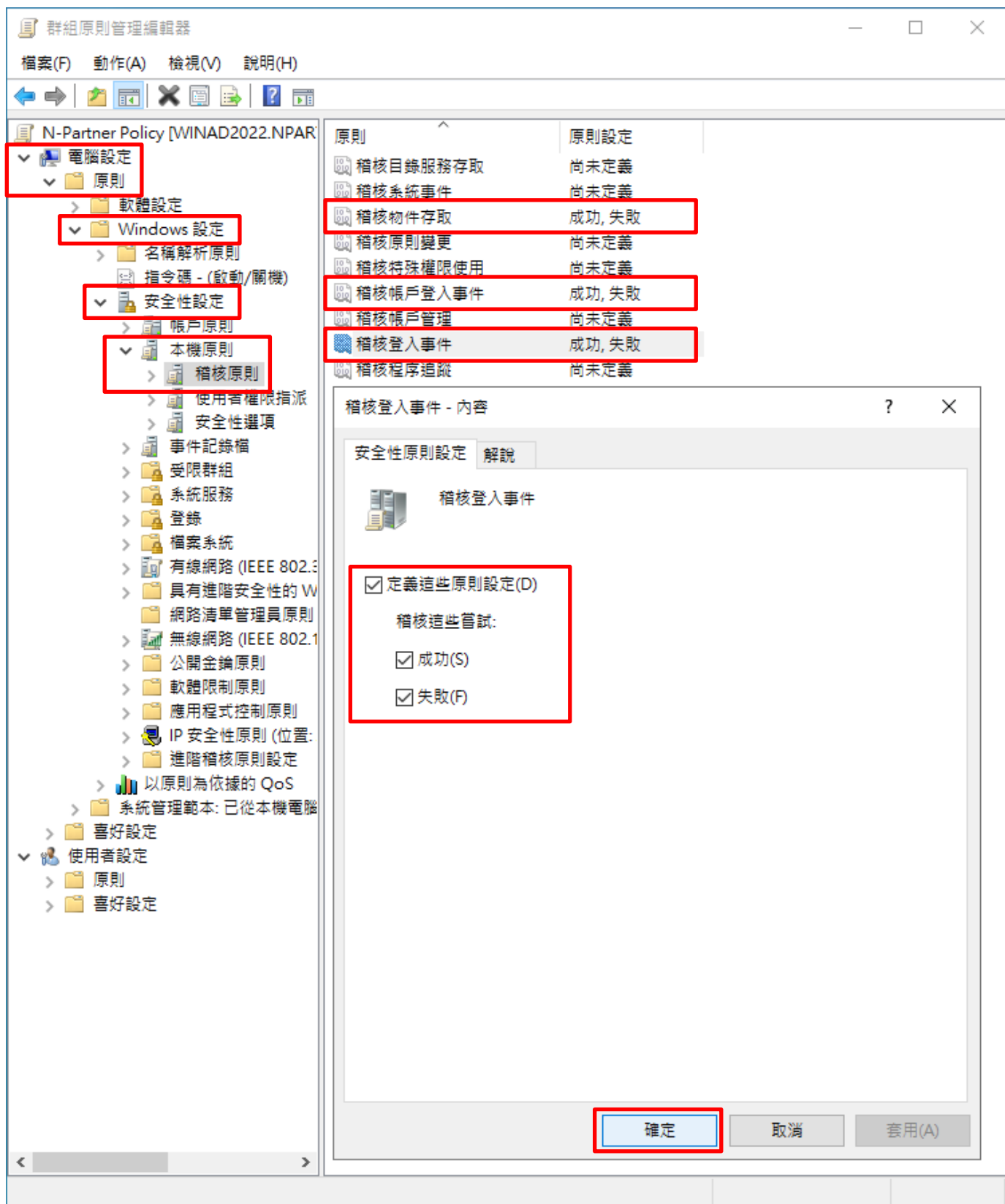
在 [N-Partner Policy] 群組原則物件按滑鼠右鍵 -> 點選 [編輯]





(5) 本機原則：稽核原則

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



(6) 事件記錄檔：安全性記錄檔大小最大值

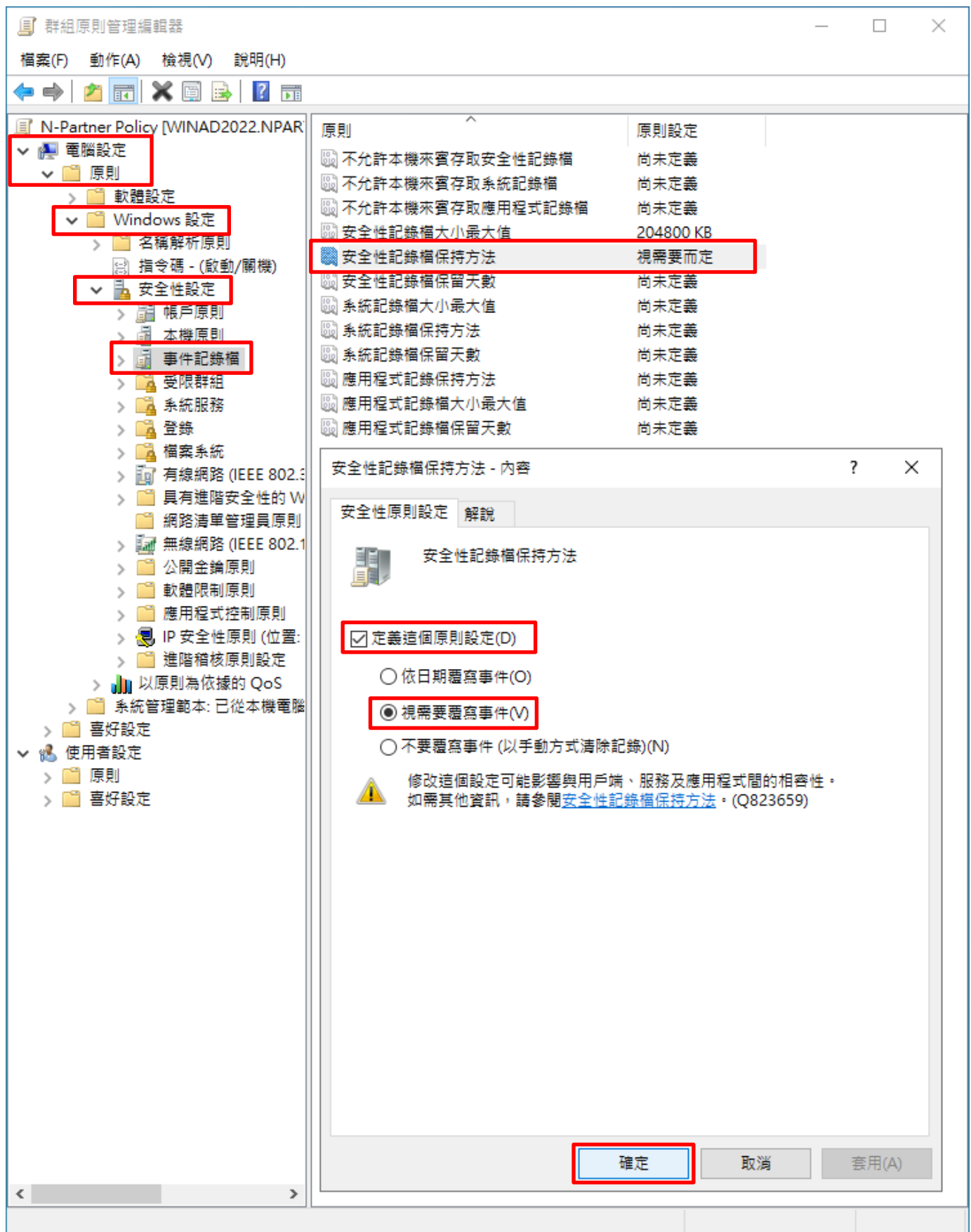
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定]: -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Management Editor window for 'N-Partner Policy [WINAD2022.NPAR]'. The left-hand tree view is expanded to '電腦設定' (Computer Configuration) > '原則' (Policies) > 'Windows 設定' (Windows Settings) > '安全性設定' (Security Settings) > '事件記錄檔' (Event Logs). The right-hand pane displays a list of policies, with '安全性記錄檔大小最大值' (Maximum size of security event logs) selected and highlighted in red. The value is set to '204800 KB'. A dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum size of security event logs - Content) is open, showing the '安全性原則設定' (Security Policy Settings) tab. The checkbox '定義這個原則設定(D)' (Define this policy setting) is checked. The value '204800' is entered in the text box, followed by 'KB' in the dropdown menu. A warning icon and text are visible below the input field, stating: '修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)'. The '確定' (OK) button is highlighted in red at the bottom of the dialog box.

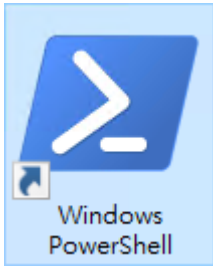
原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	204800 KB
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	尚未定義
應用程式記錄檔大小最大值	尚未定義
應用程式記錄檔保留天數	尚未定義

(7) 事件記錄檔：安全性記錄檔保持方法

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

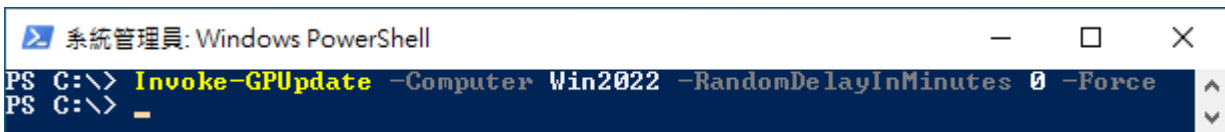


(8) 開啟 [Windows PowerShell]



(9) 更新 Windows File 伺服器群組原則

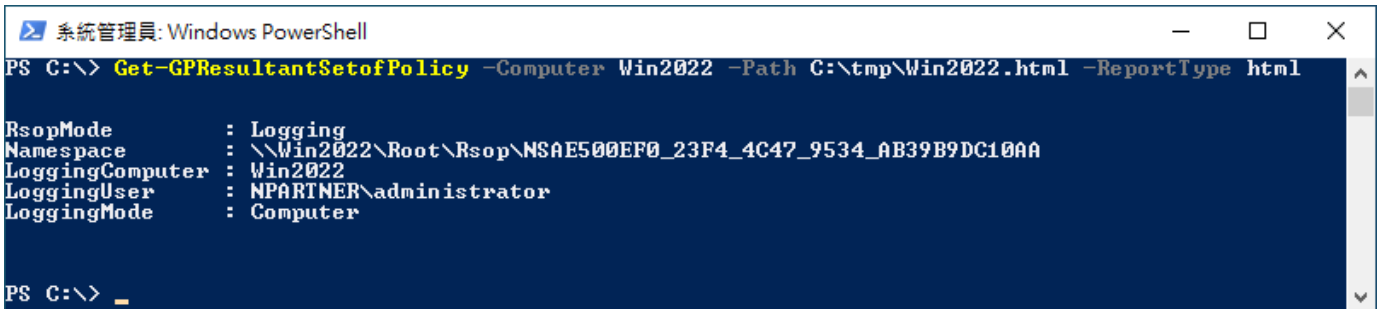
```
PS C:\> Invoke-GPUdate -Computer Win2022 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows File 伺服器名稱

(10) 產生 Windows File 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2022 -Path C:\tmp\Win2022.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

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

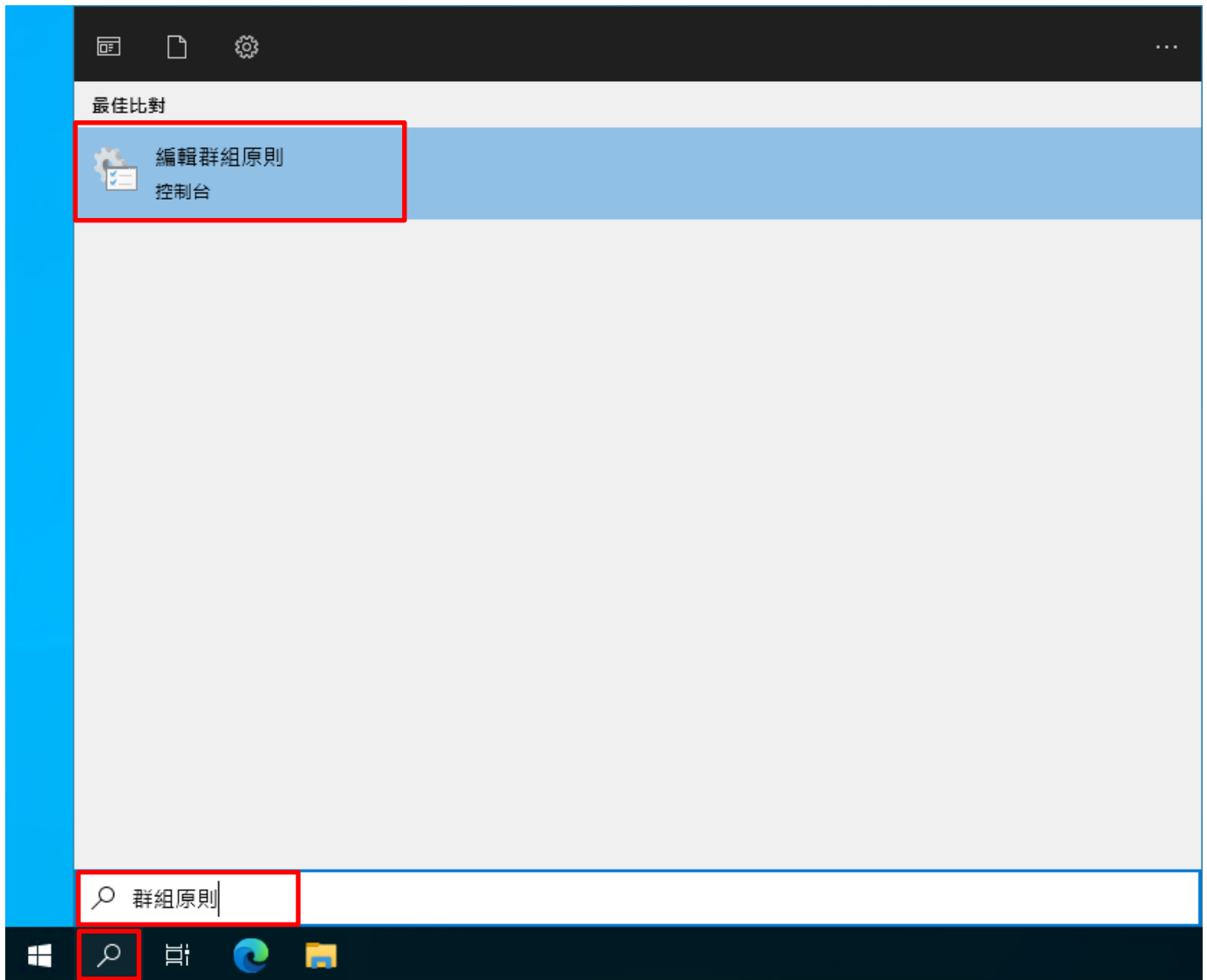
群組原則結果			
<b>群組 NPARTNER\WIN2022</b>			
資料收集: 2022/3/17 上午 11:55:26 電腦詳細資料			全部顯示
一般			隱藏
元件狀態			顯示
設定			顯示
<b>原則</b>			隱藏
<b>Windows 設定</b>			隱藏
<b>安全性設定</b>			隱藏
帳戶原則/密碼規則			顯示
帳戶原則/帳戶鎖定原則			顯示
帳戶原則/Kerberos 原則			顯示
本機原則/稽核原則			隱藏
原則	設定	優勢 GPO	
稽核物件存取	成功, 失敗	N-Partner Policy	
稽核帳戶登入事件	成功, 失敗	N-Partner Policy	
稽核登入事件	成功, 失敗	N-Partner Policy	
本機原則/使用者權限指派			顯示
本機原則/安全性選項			顯示
事件記錄檔			隱藏
原則	設定	優勢 GPO	
安全性記錄檔保持方法	視需要而定	N-Partner Policy	
安全性記錄檔容量最大值	204800 KB	N-Partner Policy	
公開金鑰原則/憑證服務用戶端 - 自動註冊設定			顯示
公開金鑰原則/加密檔案系統			顯示
群組原則物件			顯示
WMI 篩選器			顯示
使用者詳細資料			顯示

## 8.2 工作群組

### 8.2.1 稽核原則設定

(1) 開啟本機群組原則編輯器

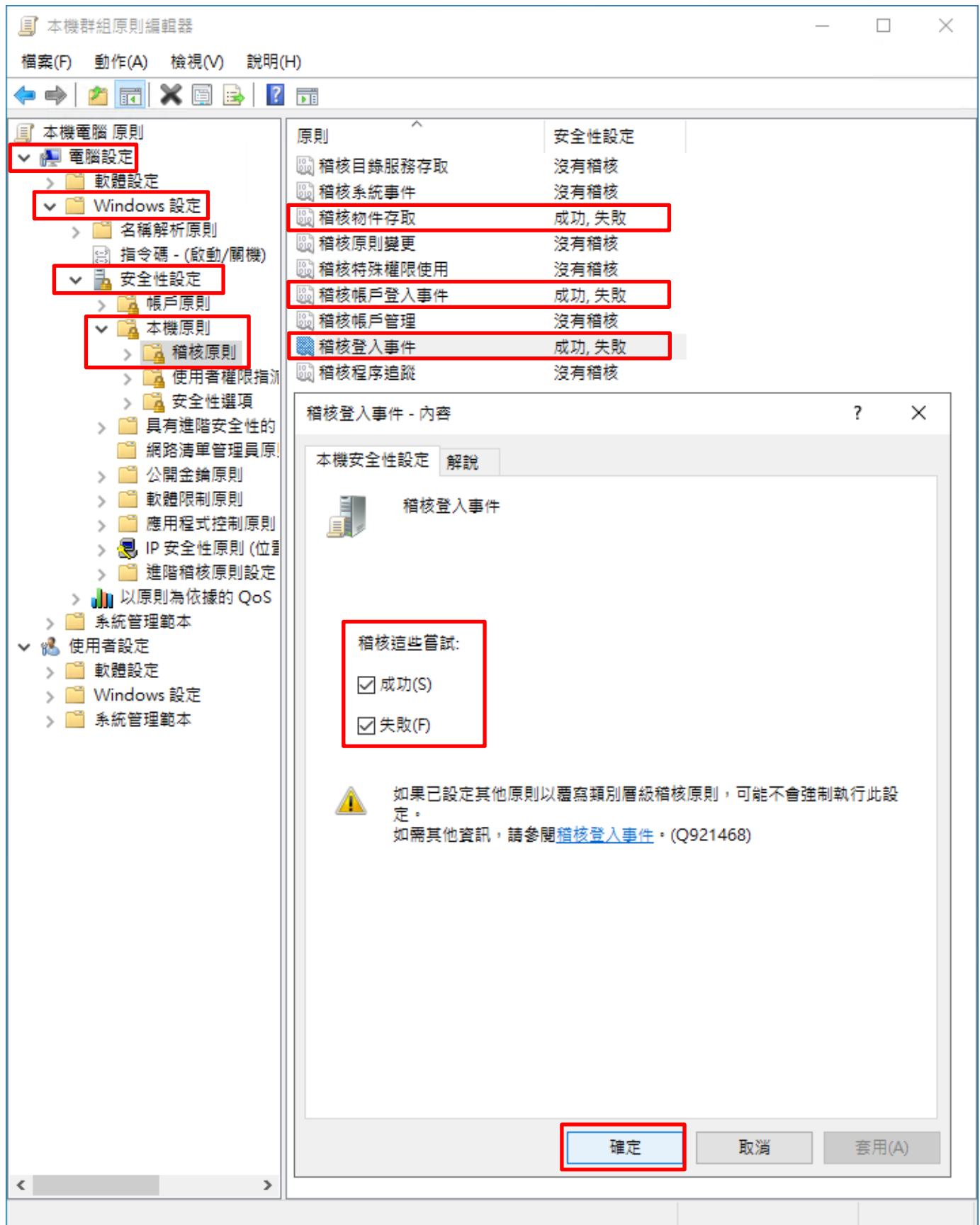
點選  [搜尋] -> 輸入 **群組原則** -> 點選 [編輯群組原則]





(2) 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], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]

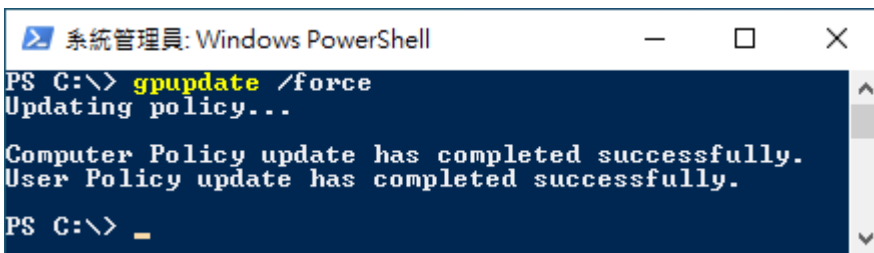


(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

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





(5) 查看群組原則套用情形

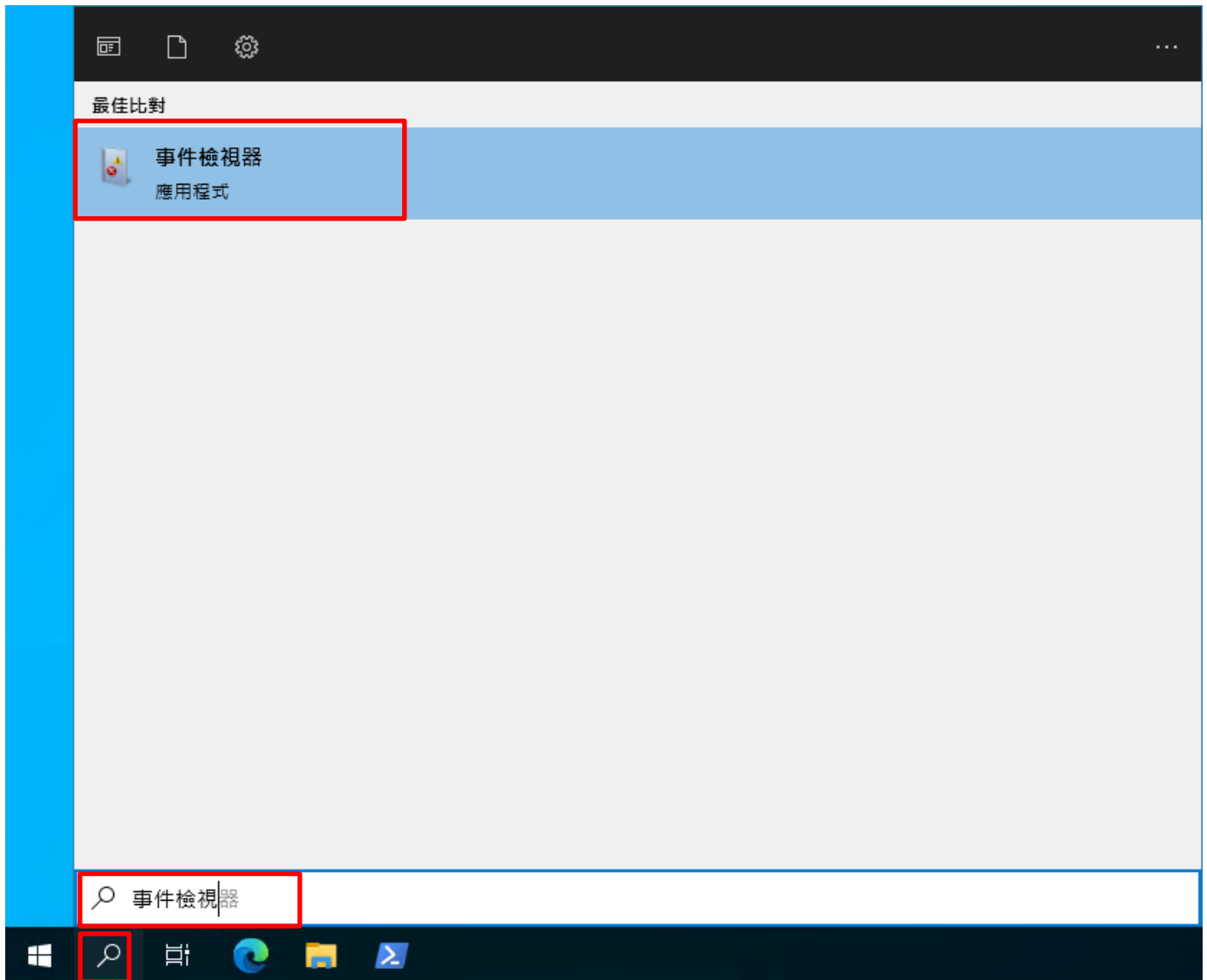
PS C:\> auditpol /get /category:\*

```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension No Auditing
  System Integrity        Success and Failure
  IPsec Driver             No Auditing
  Other System Events     Success and Failure
  Security State Change   Success
Logon/Logoff
  Logon                    Success and Failure
  Logoff                   Success and Failure
  Account Lockout         Success and Failure
  IPsec Main Mode         Success and Failure
  IPsec Quick Mode        Success and Failure
  IPsec Extended Mode     Success and Failure
  Special Logon           Success and Failure
  Other Logon/Logoff Events Success and Failure
  Network Policy Server   Success and Failure
  User / Device Claims    Success and Failure
  Group Membership        Success and Failure
Object Access
  File System             Success and Failure
  Registry                Success and Failure
  Kernel Object           Success and Failure
  SAM                    Success and Failure
  Certification Services  Success and Failure
  Application Generated   Success and Failure
  Handle Manipulation     Success and Failure
  File Share              Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events Success and Failure
  Detailed File Share     Success and Failure
  Removable Storage       Success and Failure
  Central Policy Staging  Success and Failure
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events No Auditing
  Sensitive Privilege Use   No Auditing
Detailed Tracking
  Process Creation        No Auditing
  Process Termination     No Auditing
  DPAPI Activity          No Auditing
  RPC Events              No Auditing
  Plug and Play Events    No Auditing
  Token Right Adjusted Events No Auditing
Policy Change
  Audit Policy Change     Success
  Authentication Policy Change Success
  Authorization Policy Change No Auditing
  MPSSUC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events No Auditing
Account Management
  Computer Account Management Success
  Security Group Management Success
  Distribution Group Management No Auditing
  Application Group Management No Auditing
  Other Account Management Events No Auditing
  User Account Management Success
DS Access
  Directory Service Access Success
  Directory Service Changes No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation   Success and Failure
PS C:\>
```

## 8.2.2 事件檔案設定

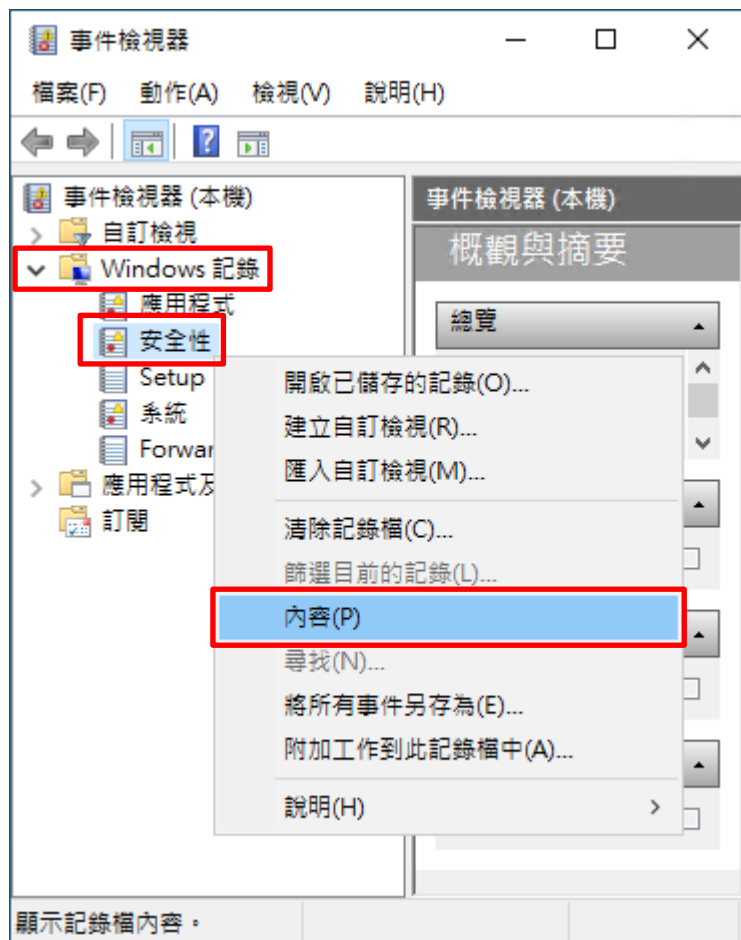
(1) 開啟 [檢視事件記錄檔]

點選  [搜尋] -> 輸入事件檢視 -> 點選 [事件檢視器]



## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [安全性] 按滑鼠右鍵 -> 點選 [內容]



(3) 設定安全性記錄檔

輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

記錄檔路徑(L): %SystemRoot%\System32\Winevt\Logs\Security.evtx

記錄檔大小: 16.07 MB(16,846,848 位元組)

建立日期: 2022年3月8日 下午 06:04:42

修改日期: 2022年3月17日 上午 10:15:30

存取日期: 2022年3月17日 上午 10:15:30

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

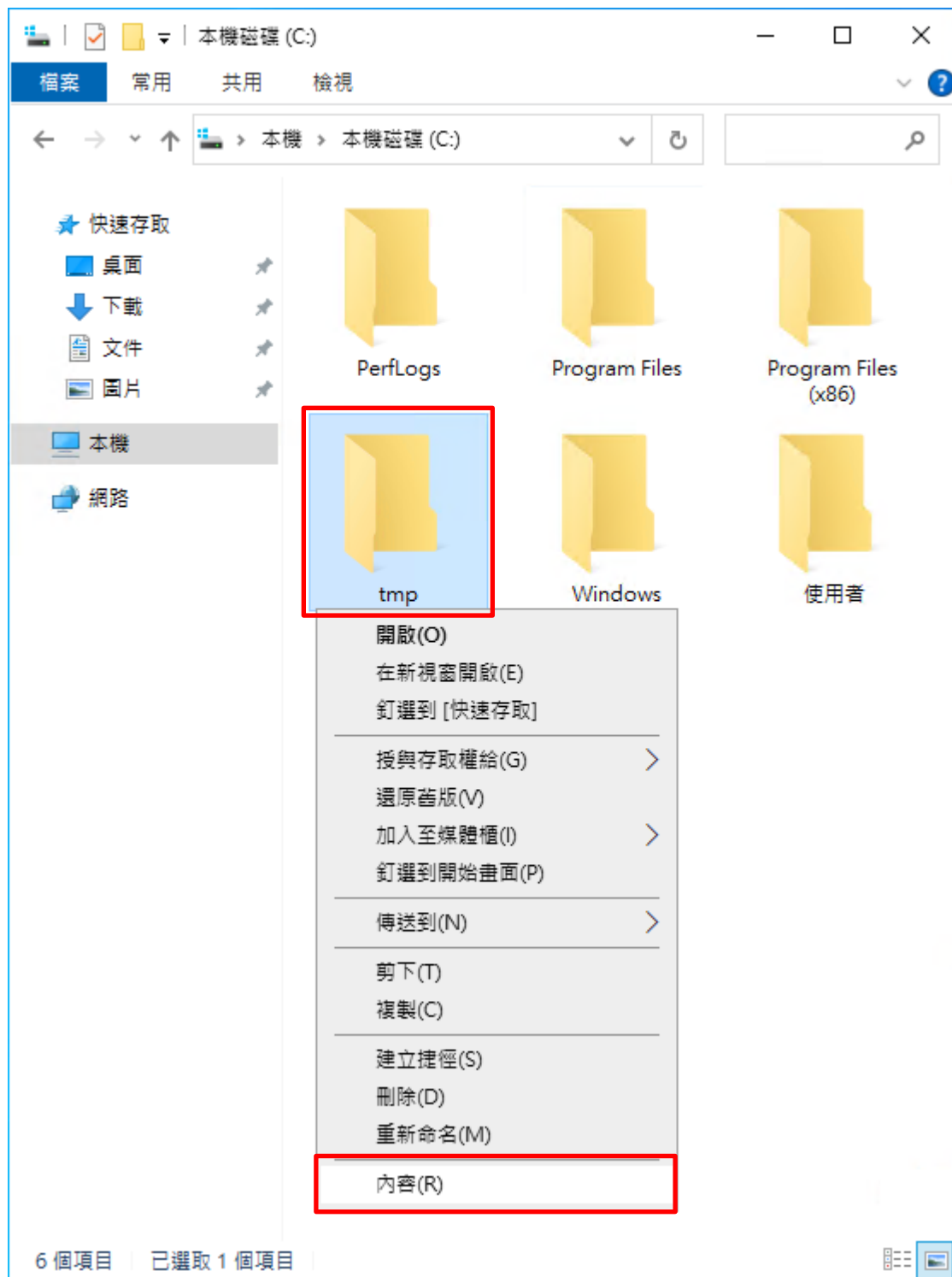
不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

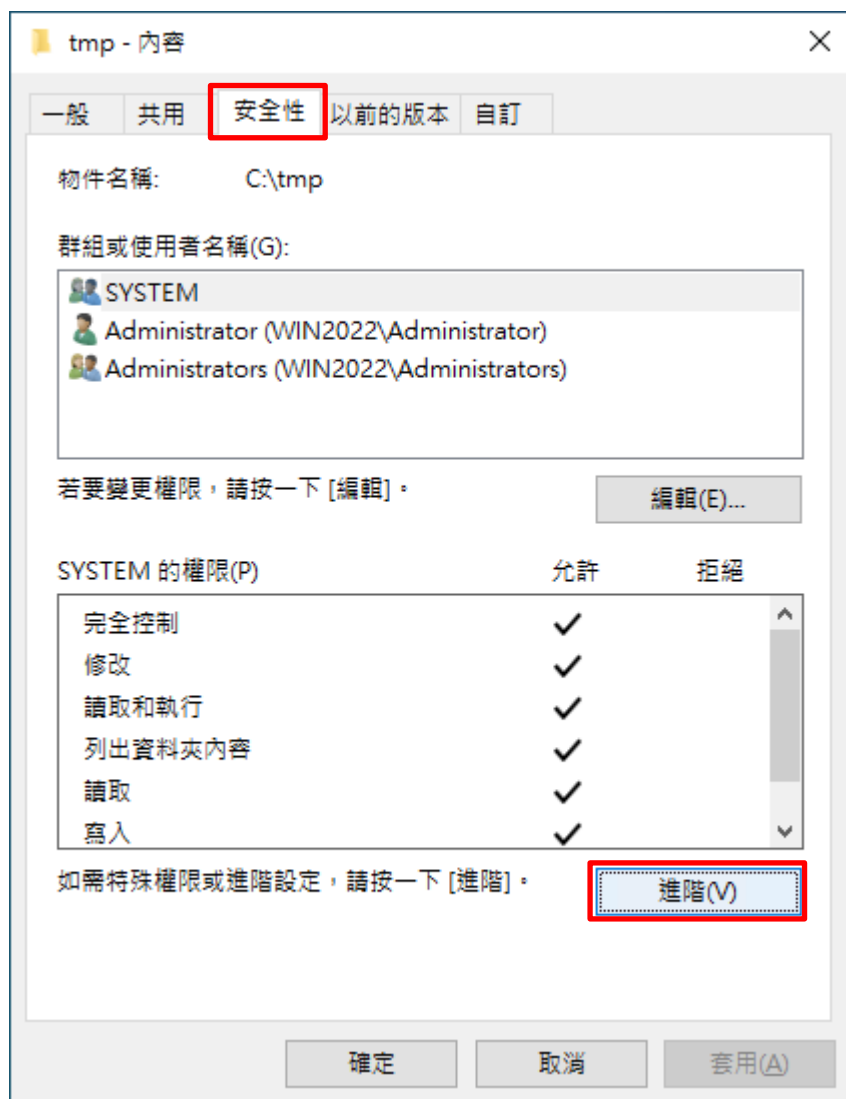
確定 取消 套用(P)

## 8.3 稽核資料夾設定

(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



(2) 點選 [安全性] 頁面 -> 按 [進階]



(3) 點選 [稽核] 頁面 -> 按 [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 [檢查名稱] -> 按 [確定]





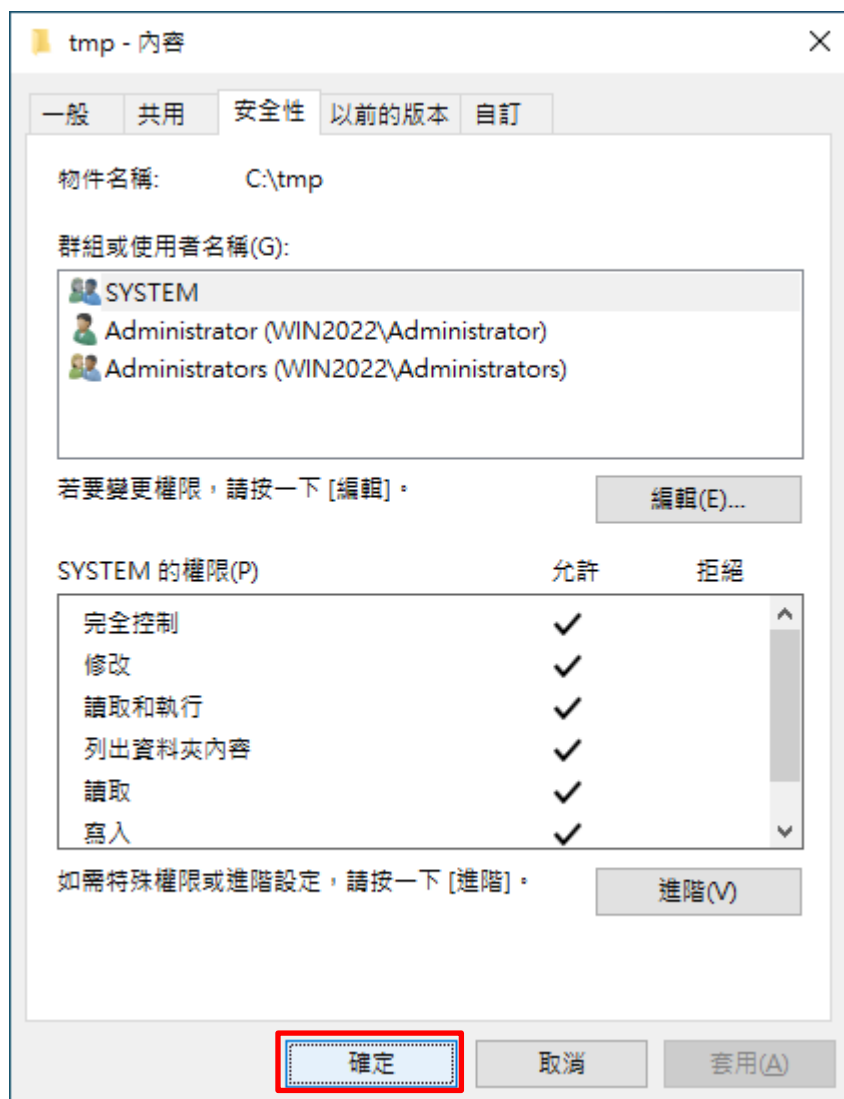
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(7) 顯示稽核主體 [Everyone] -> 按 [確定]



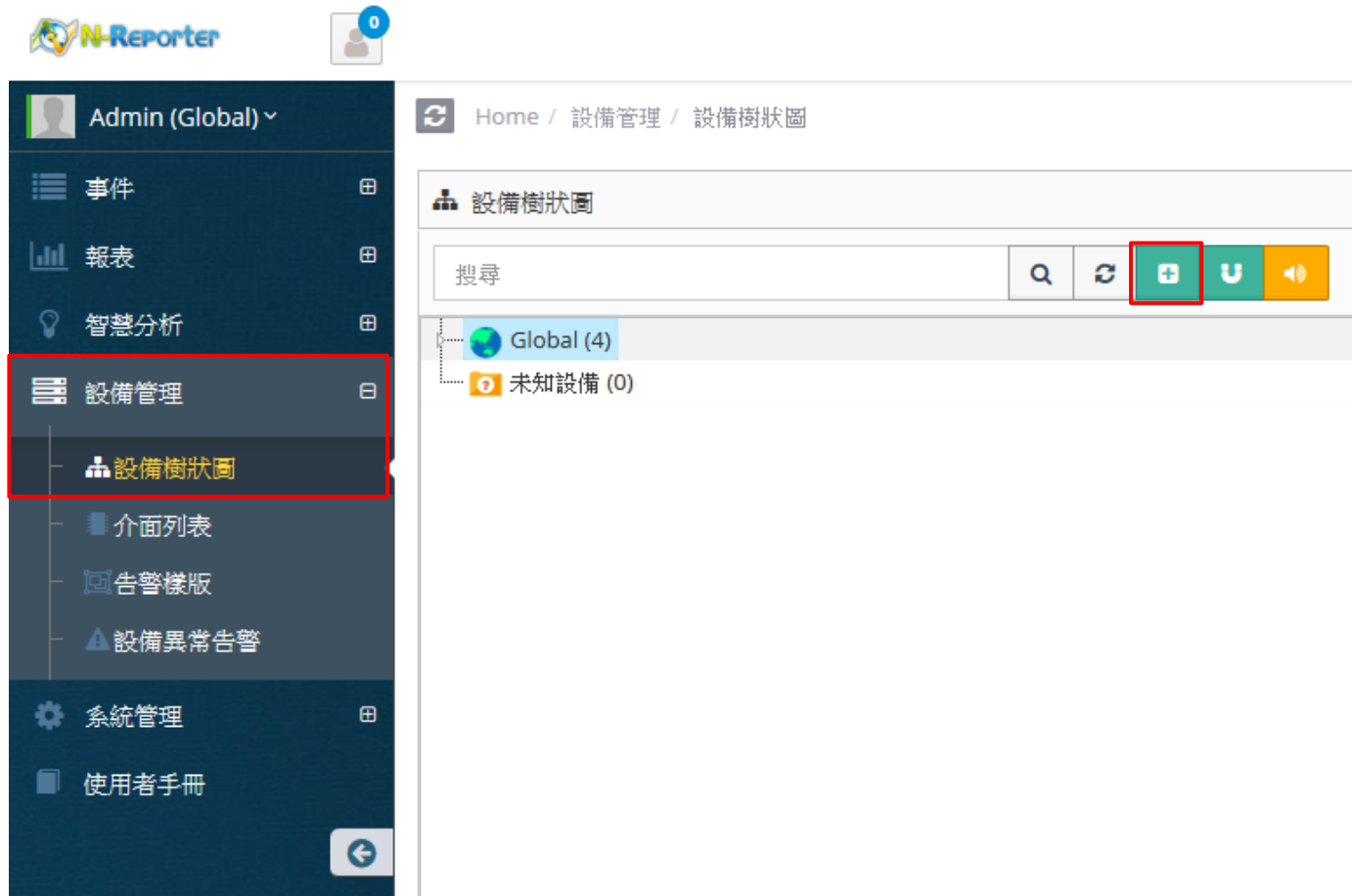
(8) 按 [確定]



## 9. 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', '報表', '智慧分析', '設備管理' (highlighted with a red box), '設備樹狀圖' (highlighted with a red box), '介面列表', '告警樣版', '設備異常告警', '系統管理', and '使用者手冊'. The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖' and the title '設備樹狀圖'. Below the title is a search bar with a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a green 'U' button, and a yellow speaker icon. The device tree shows a 'Global (4)' folder containing '未知設備 (0)'.

## 9.1 Windows 2003 或之前版本作業系統

(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] 和 Facility: [(17) local user 1 (local1)] 和編碼方式: [BIG5] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

新增設備

設備基本設定

名稱  
WinFiles-192.168.8.183

IP  
192.168.8.183

設備種類  
 Syslog  Flow  SNMP  PM

Syslog 相關設定

資料格式  
Windows

使用自定義資料格式

Facility  
(17) local use 1 (local1)

編碼方式  
BIG5

日誌保留 Raw Data  Raw Data

本設備於分時監控報表啟動Syslog轉發時， Raw Data

設備進階設定

ICMP 告警樣版  
N/A

設備 Icon  
icon-host

Login Account

Login Password

Enable Password

接收狀態  
 啟用  停用

暫無資料告警  
 啟用 Syslog 暫無資料告警

告警通報設定  
預設

資料保留天數

經緯度  
緯度 經度

確定 取消

若勾選 [日誌保留 Raw Date] ·

[事件查詢] 顯示 Raw Data 資訊

## 9.2 Windows 2008 或之後版本作業系統

(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] 和 Facility: [(17) local user 1 (local1)] 和編碼方式: [UTF-8] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

新增設備

設備基本設定

名稱  
WinFiles-192.168.8.183

IP  
192.168.8.183

設備種類  
 Syslog  Flow  SNMP  PM

Syslog 相關設定

資料格式  
Windows

使用自定義資料格式

Facility  
(17) local use 1 (local1)

編碼方式  
UTF-8

日誌保留 Raw Data  Raw Data

設備進階設定

ICMP 告警樣版  
N/A

設備 Icon  
icon-host

Login Account

Login Password

Enable Password

接收狀態  
 啟用  停用

暫無資料告警  
 啟用 Syslog 暫無資料告警

告警通報設定  
預設

資料保留天數

經緯度  
緯度 經度

確定 取消

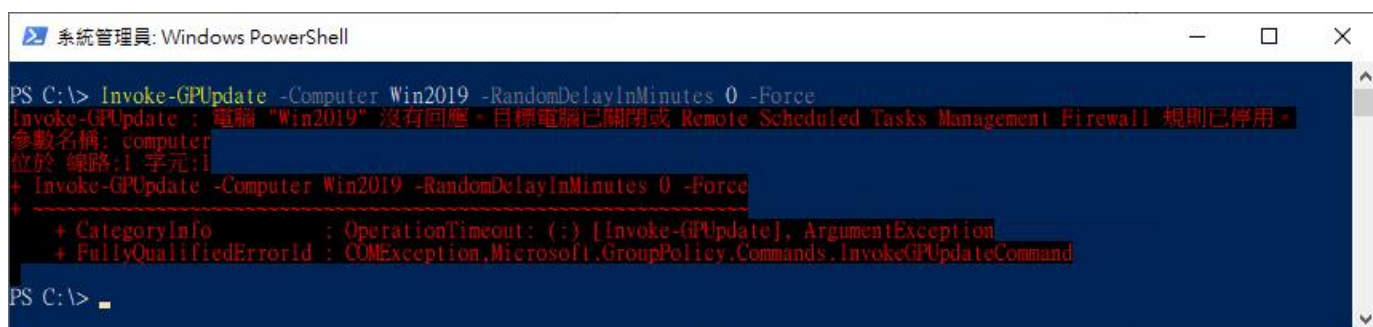
若勾選 [日誌保留 Raw Date] ,

[事件查詢] 顯示 Raw Data 資訊

## 10. 故障排除

### 10.1 Invoke-GPUdate 錯誤

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



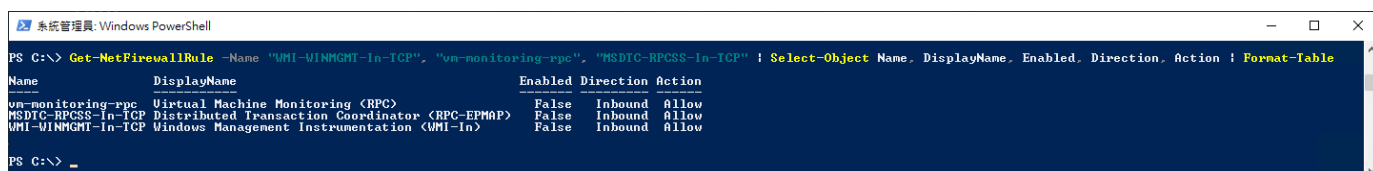
```
PS C:\> Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
Invoke-GPUdate : 電腦 "Win2019" 沒有回應。目標電腦已關閉或 Remote Scheduled Tasks Management Firewall 規則已停用。
參數名稱: computer
位於 線路:1 字元:1
+ Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
+ ~~~~~
+ CategoryInfo          : OperationTimeout: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

(2) 在 Windows File 伺服器 · 開啟 [Windows PowerShell]



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

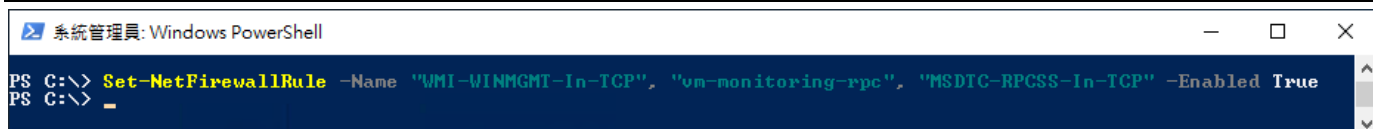
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



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

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

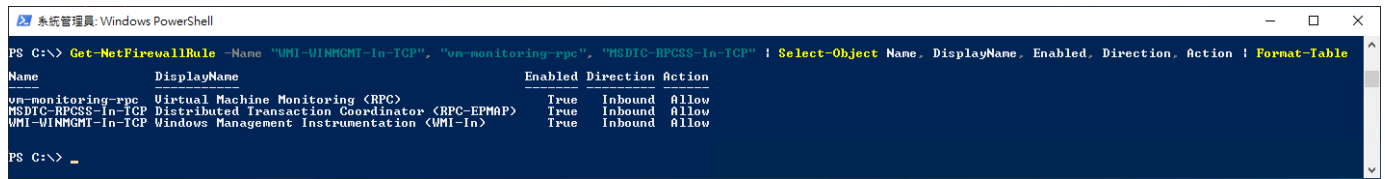
```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -
Enabled True
```



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

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

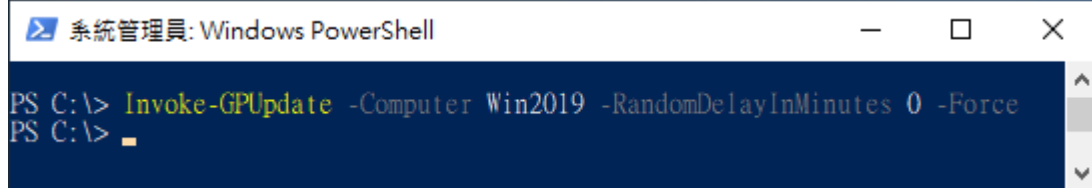
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |  
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
系統管理員: Windows PowerShell  
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table  
Name                DisplayName          Enabled Direction Action  
-----  
vm-monitoring-rpc   Virtual Machine Monitoring (RPC)      True    Inbound  Allow  
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP) True    Inbound  Allow  
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In) True    Inbound  Allow  
PS C:\> _
```

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

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



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

紅色文字部位請輸入 Windows File 伺服器名稱





Tel / 04-23752865    Fax / 04-23757458  
業務詢問 / [sales@npartnertech.com](mailto:sales@npartnertech.com)  
技術詢問 / [support@npartnertech.com](mailto:support@npartnertech.com)