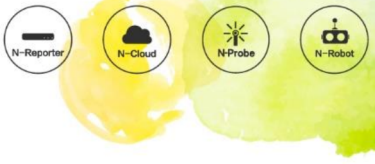
N-Partner

如何設定
Windows File 事件記錄

V009

2024/10/18



版權聲明

商標

目錄

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

監視的事件：https://learn.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

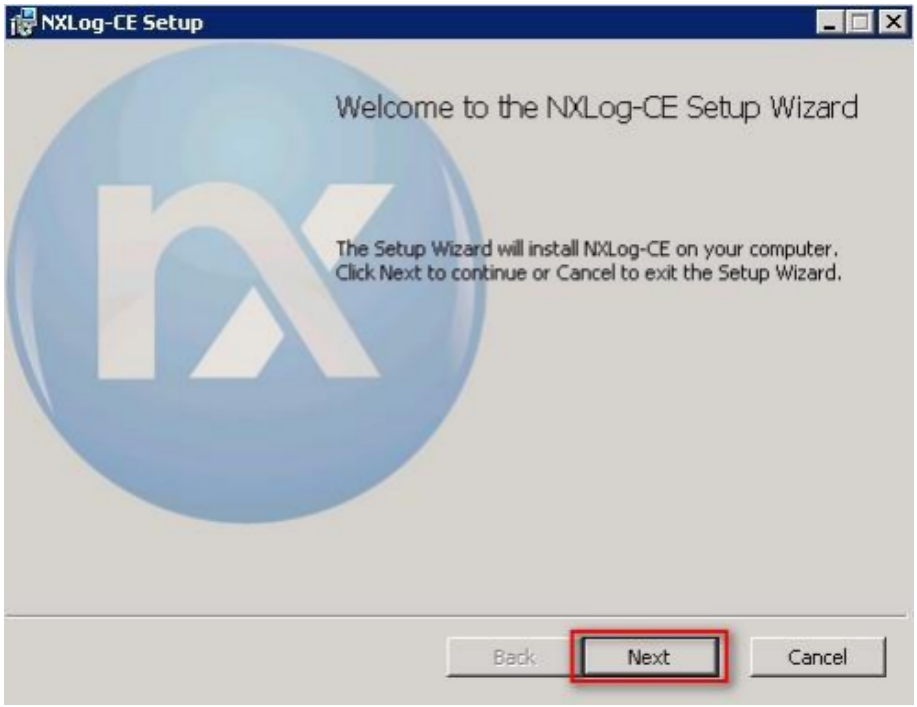
下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.0.2272.msi

註：若需要下載 NXLog 32bit 版本，請與我們連繫。

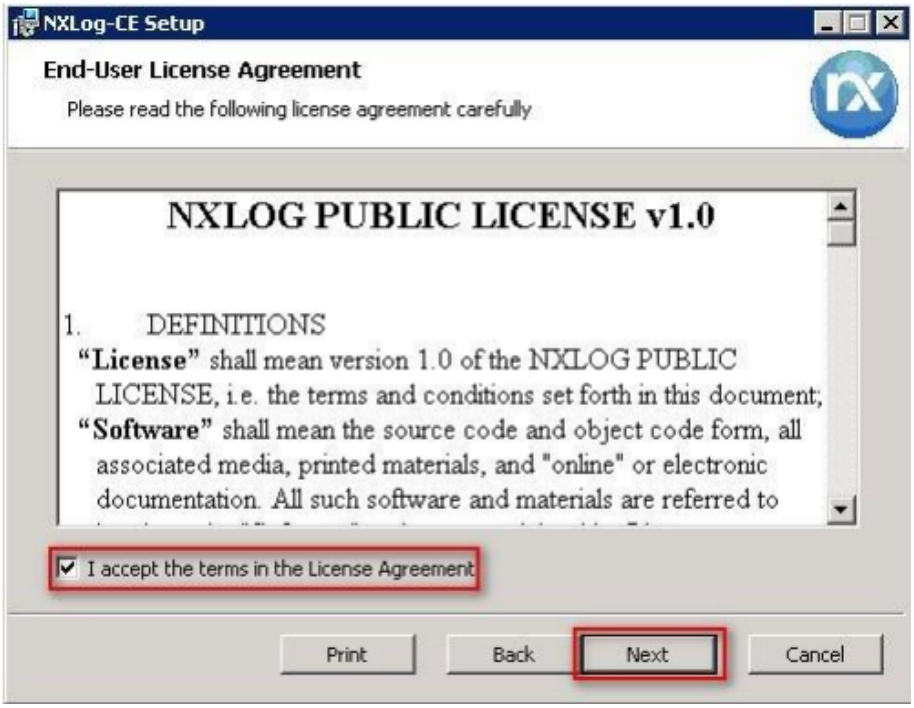
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

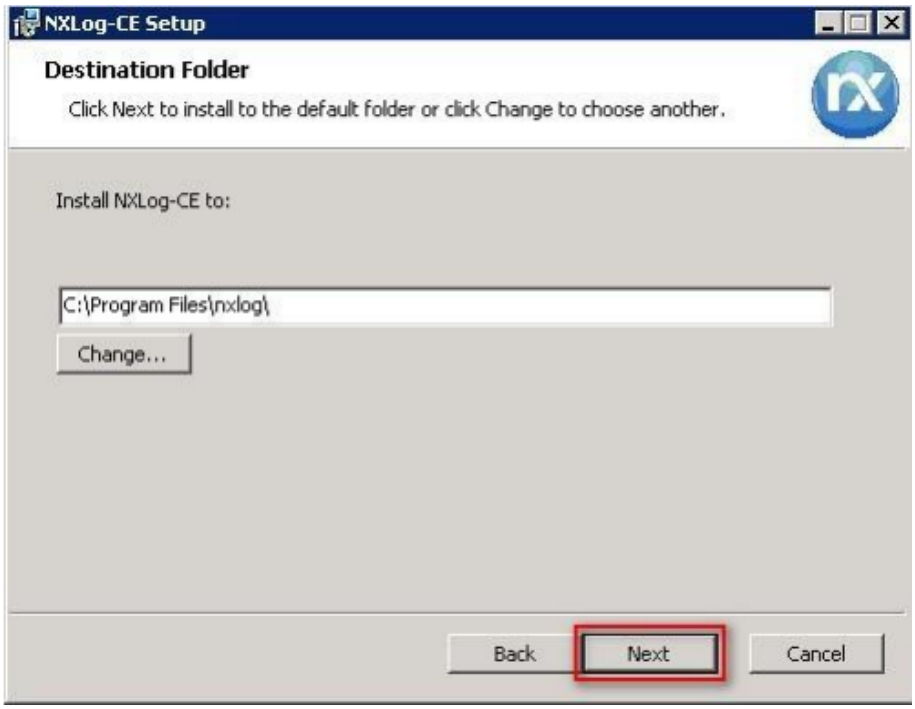
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



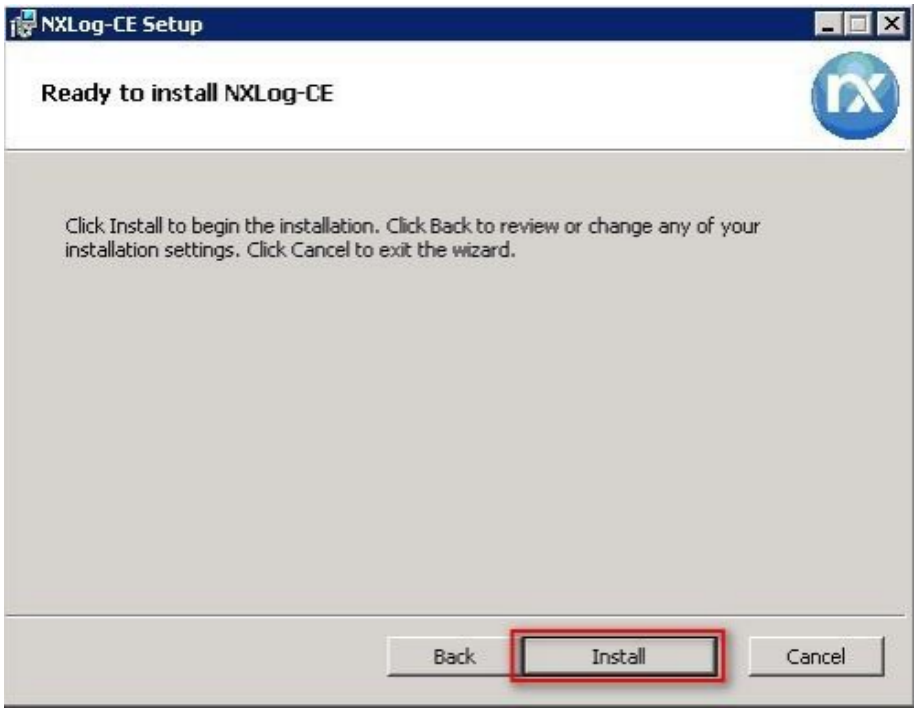
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



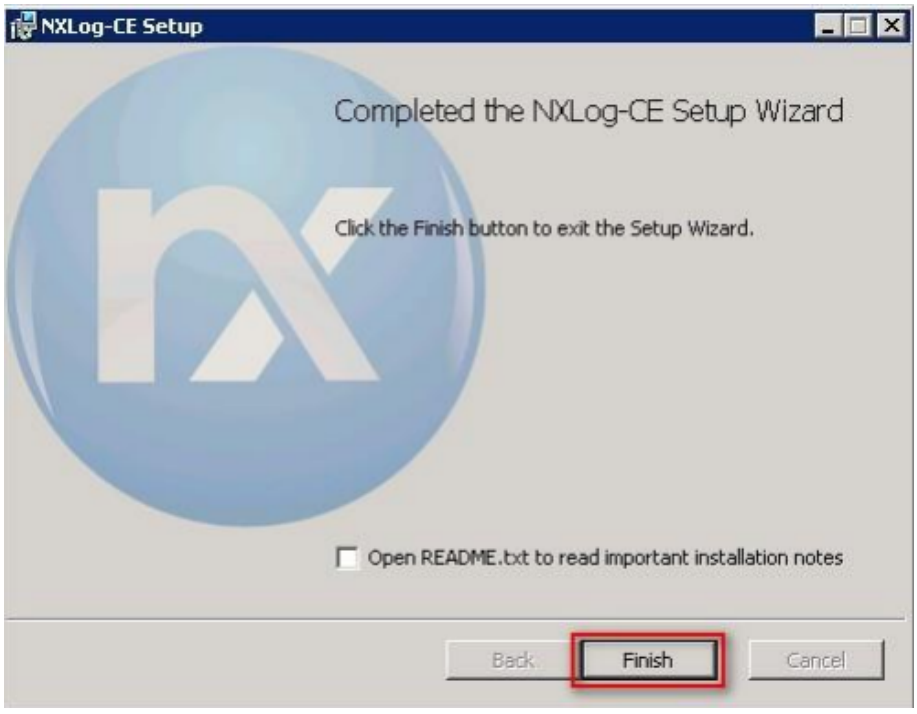
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].

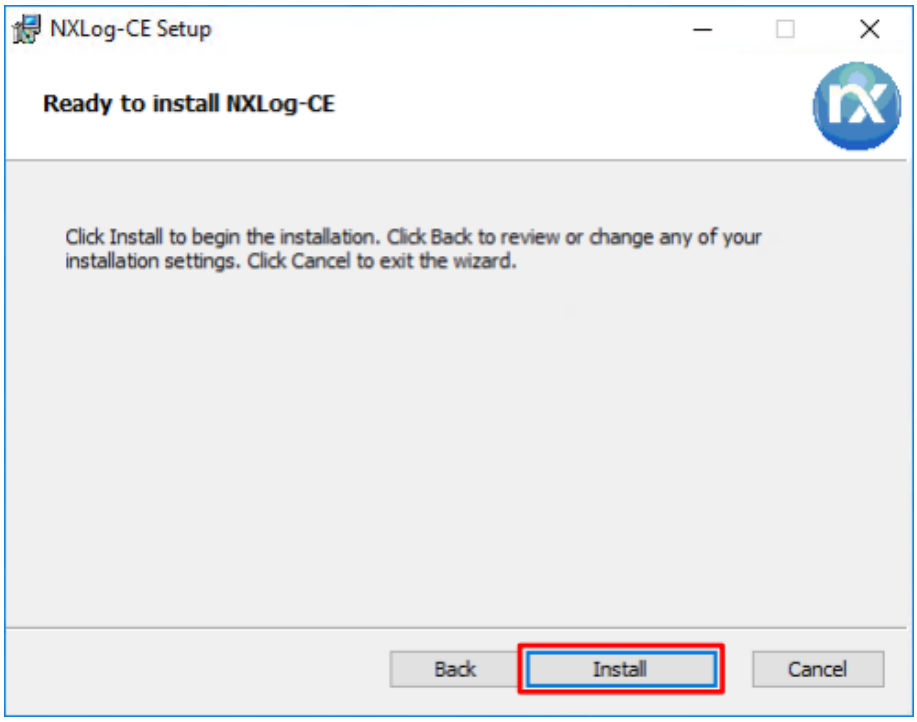


-> 按 [Finish].



<2.2> Windows 2003

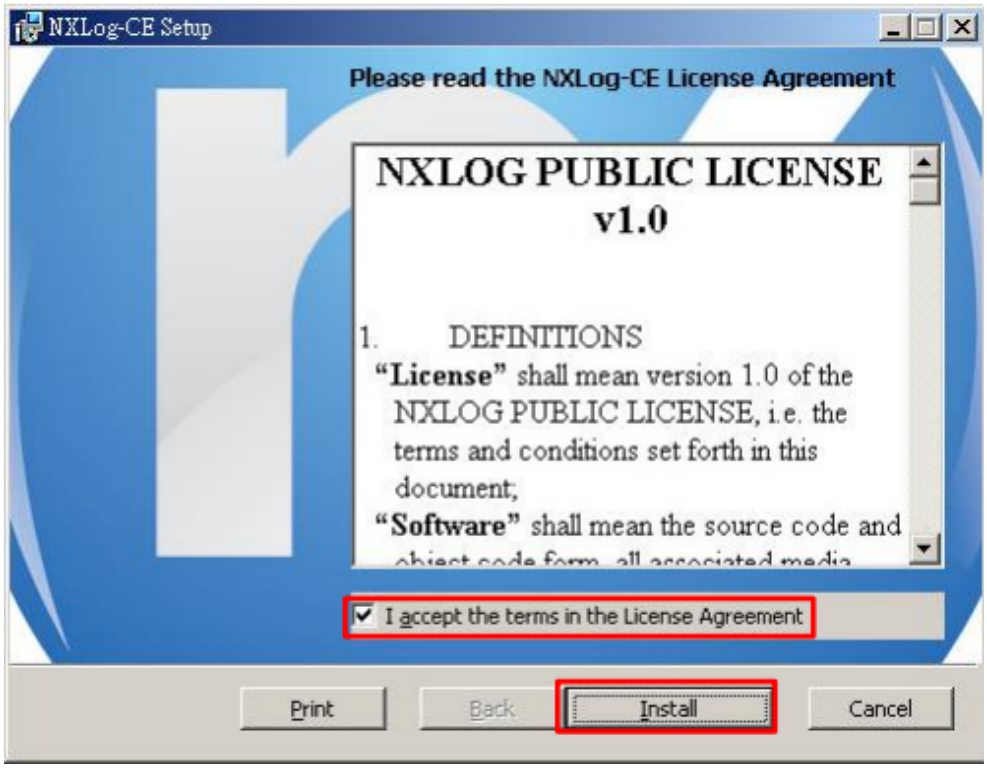
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].



<2.3> Windows 2000

前往 NXLog CE 舊版網址 https://sourceforge.net/projects/nxlog-ce/ , 左點 [See All Activity] , 下載 NXLOG CE 支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.msi] -> 勾選 [I accept the terms in the License Agreement] -> 按 [Install] 到 [Finish].



1.2 NXLog 設定檔下載

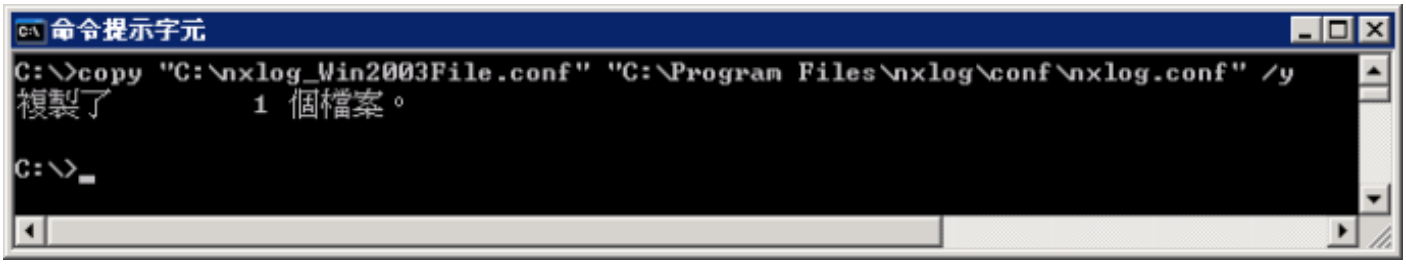
1.2.1 Windows 2003 或之前版本作業系統

(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

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



本文件範例是 64 位元作業系統，若作業系統是 32 位元，紅色文字部位請改以下設定 '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

```
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 64 位元作業系統，若作業系統是 32 位元，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  192.168.3.88
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  192.168.3.88
```

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

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

修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)”，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

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  192.168.3.88
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_mseventlog
    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  192.168.3.88
```

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

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

修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)” ，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

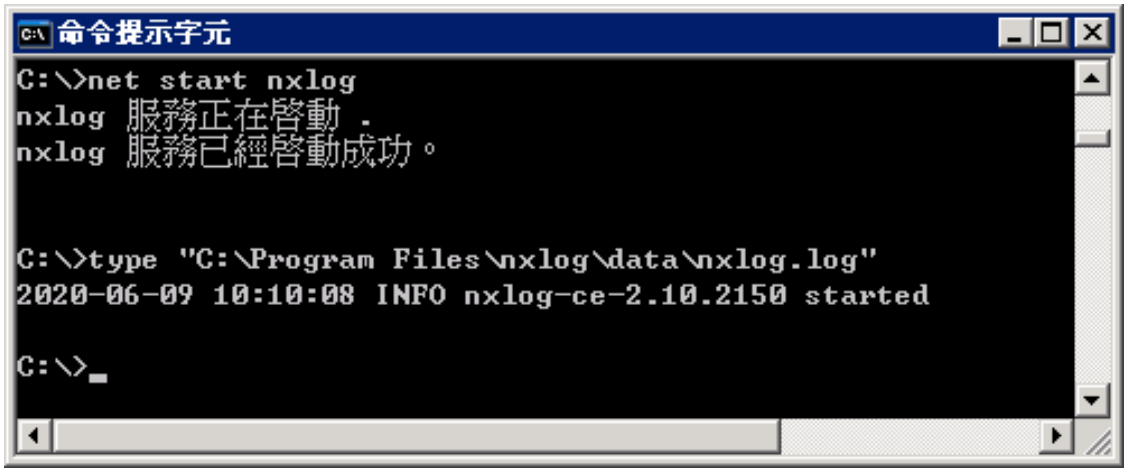
1.4 NXLog 啟動服務

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

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

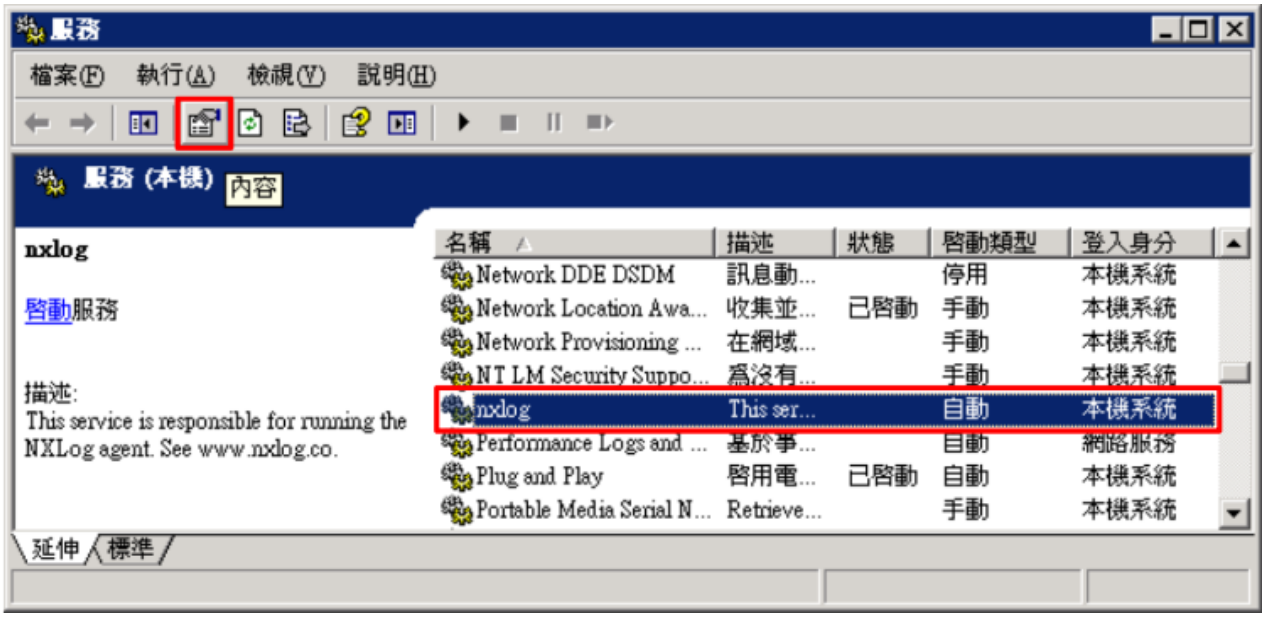


(3) 開啟 [服務] 功能

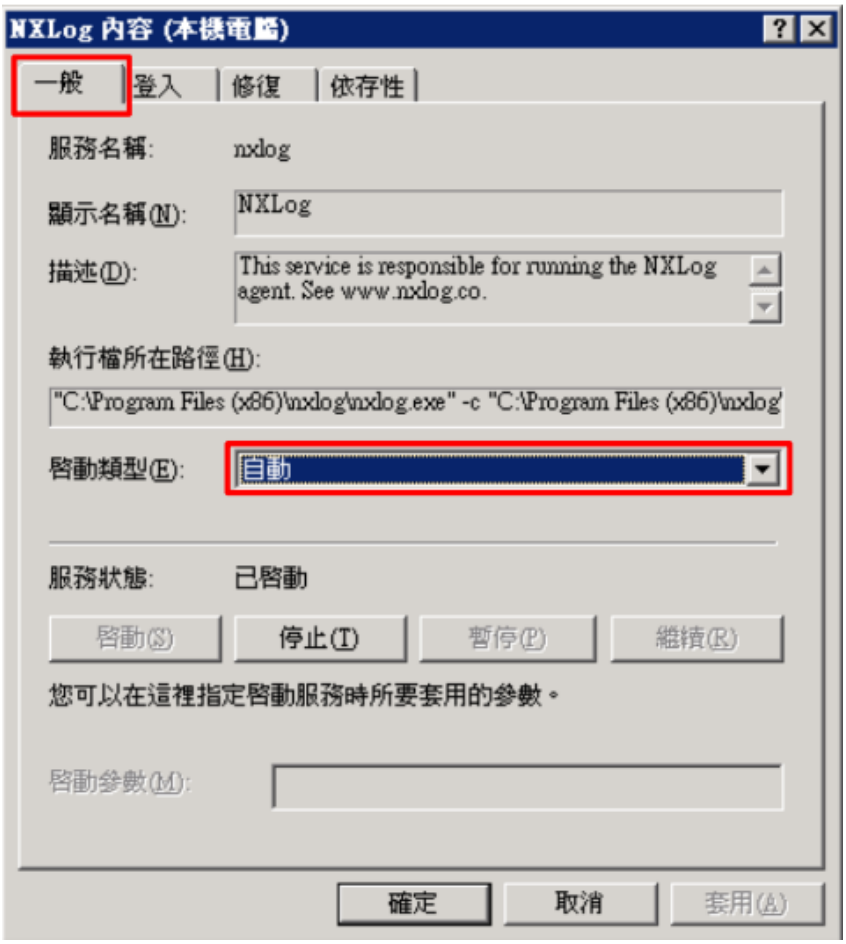
```
PS C:\>  Services.msc
```

(4) 開啟 NXLog 服務內容

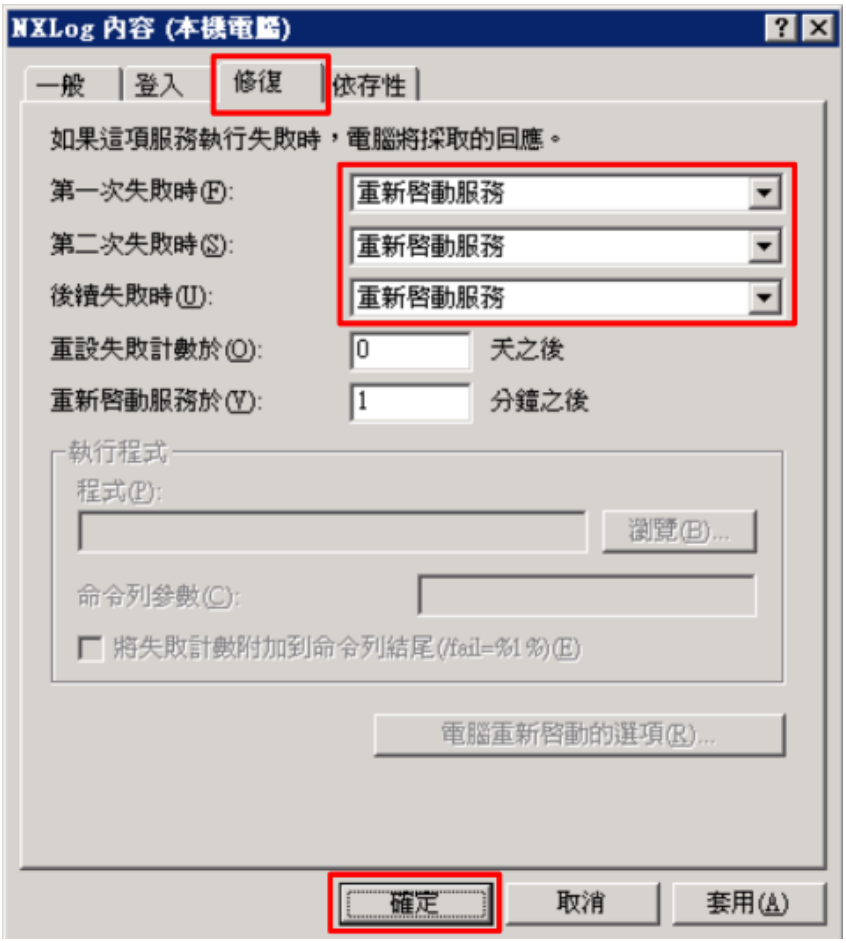
選擇 [NXLog] -> 點選 [內容]



(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]

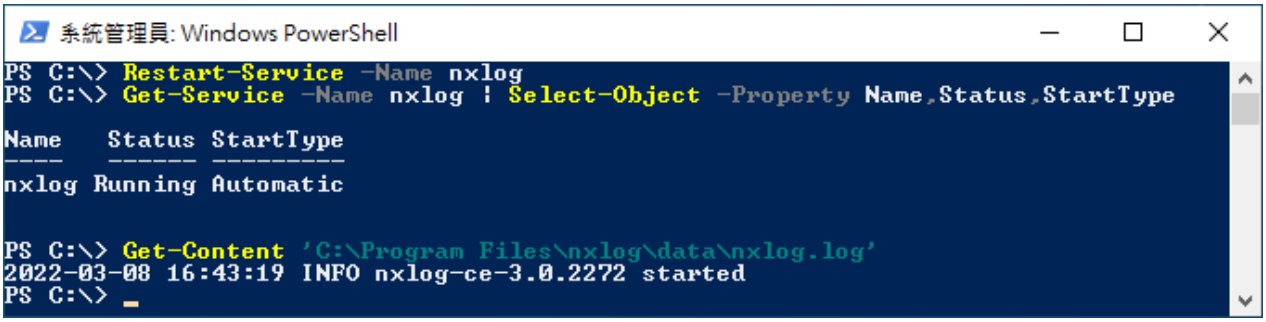


1.4.2 Windows 2008 或之後版本作業系統

(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

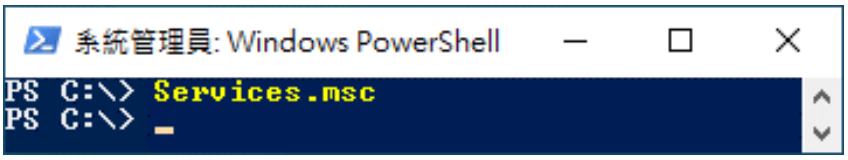
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```



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'`

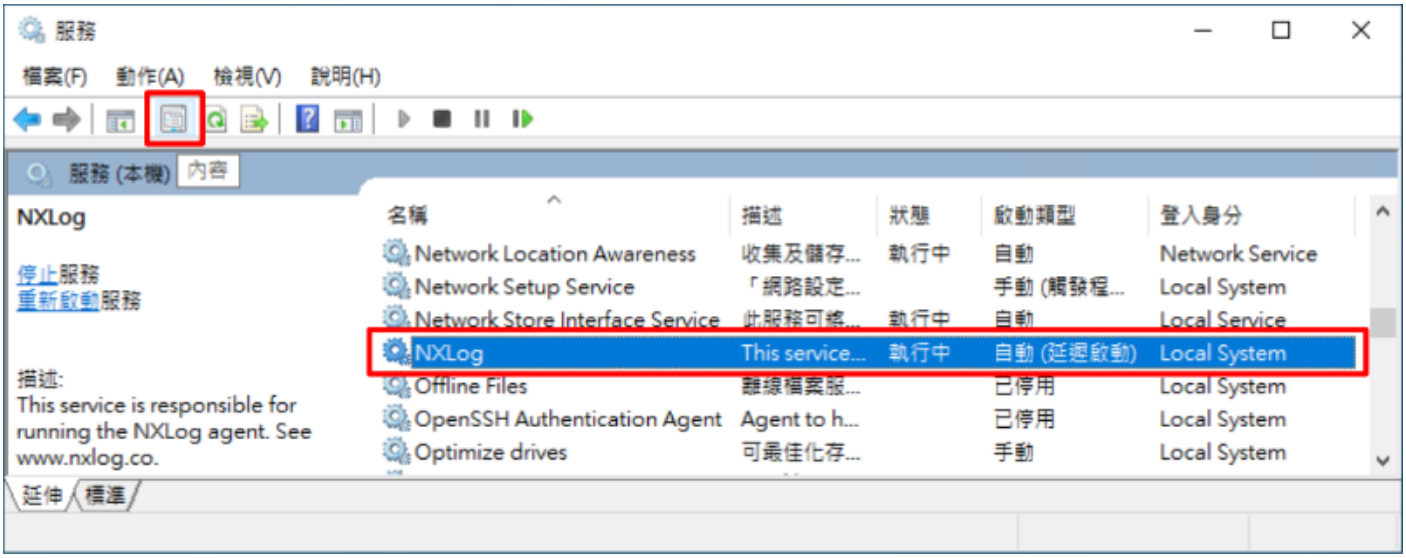
(3) 開啟 [服務] 功能

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

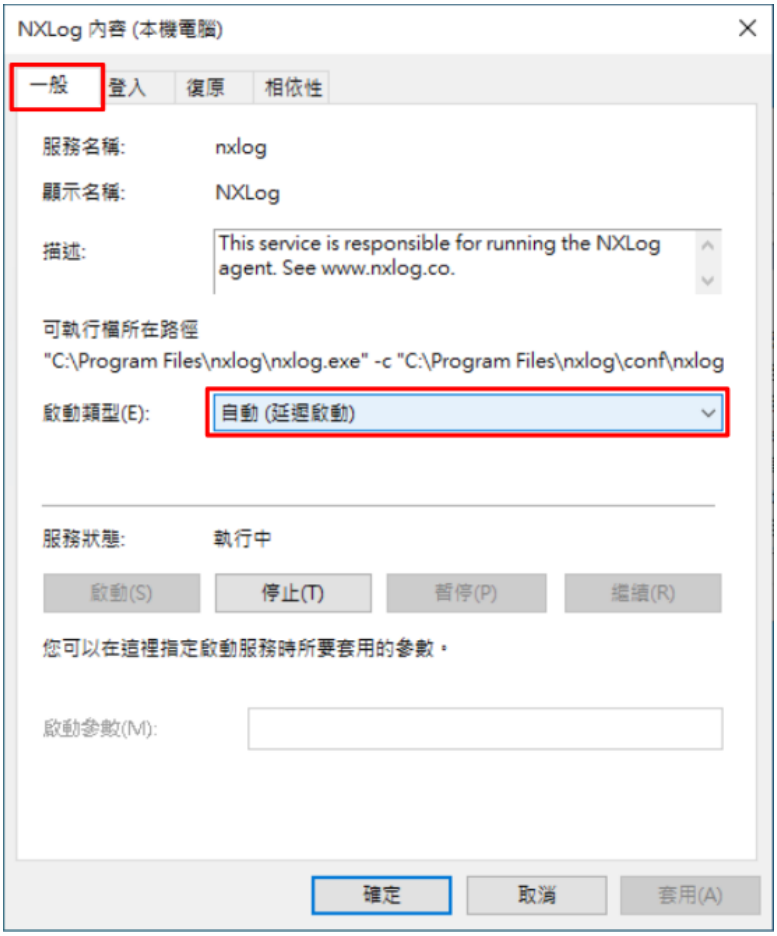


(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選 [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (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]

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

*以下分別為網域或工作群組設定方式。

2.1 網域

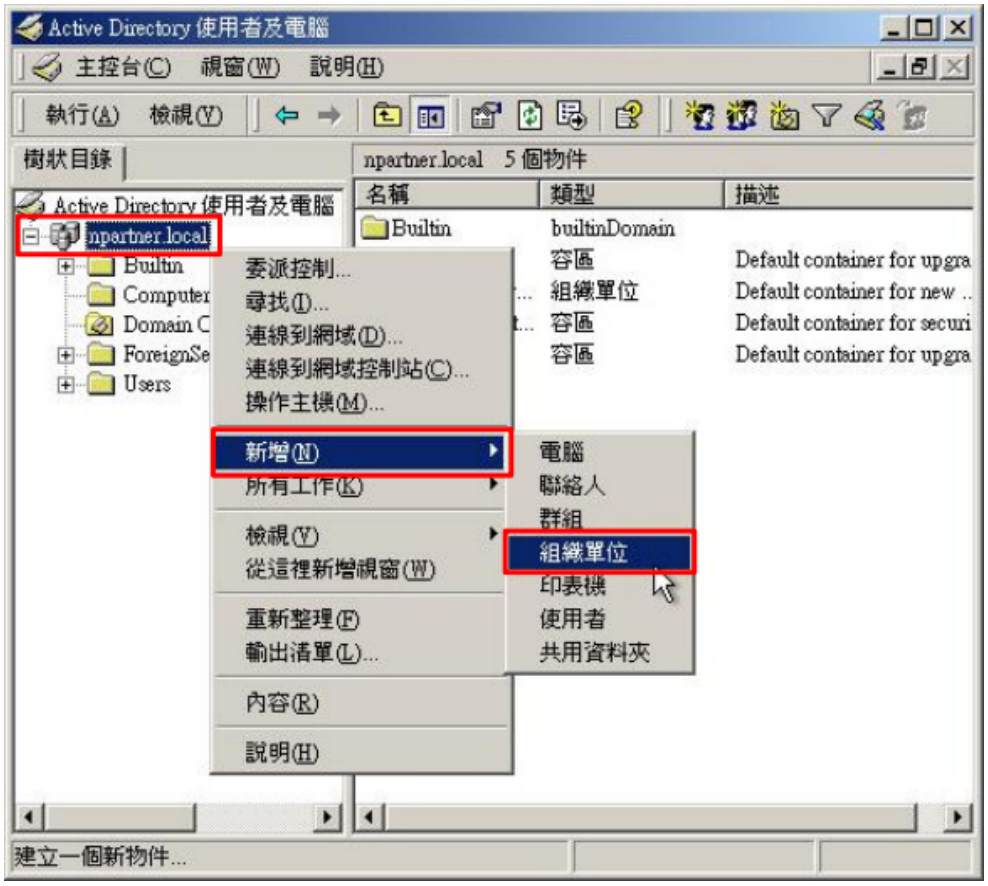
2.1.1 組織單位設定

(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]

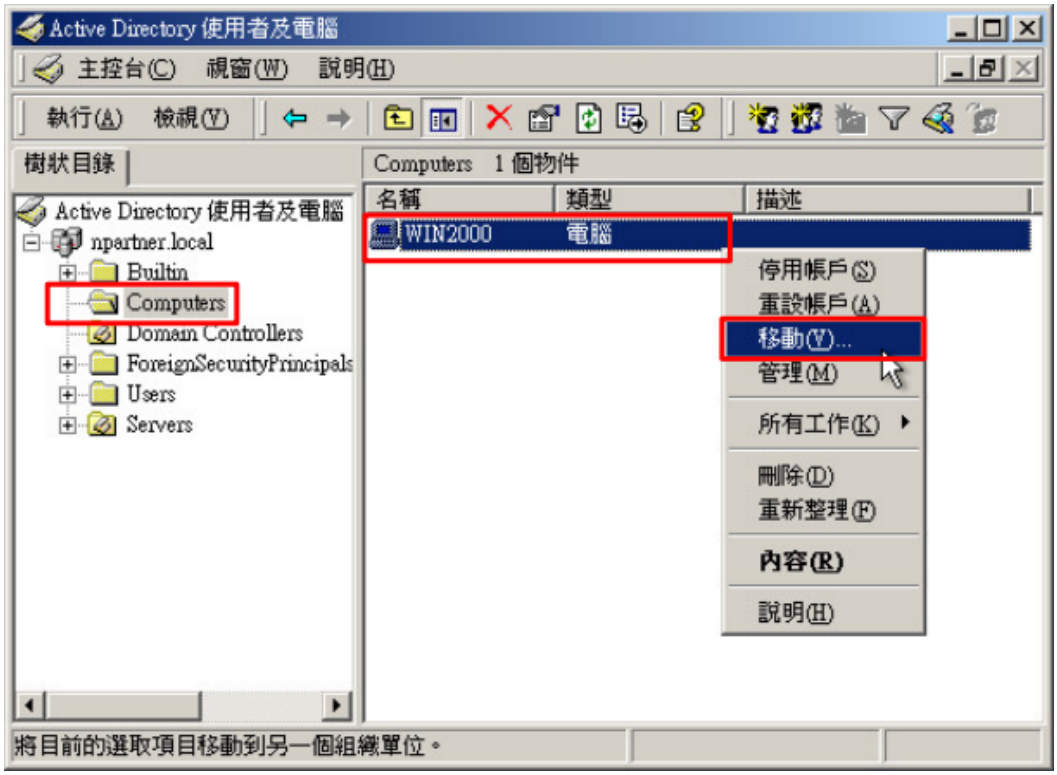


(3) 輸入組織單位名稱

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 主機 -> 點選 [移動]



(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

(6) 確認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。

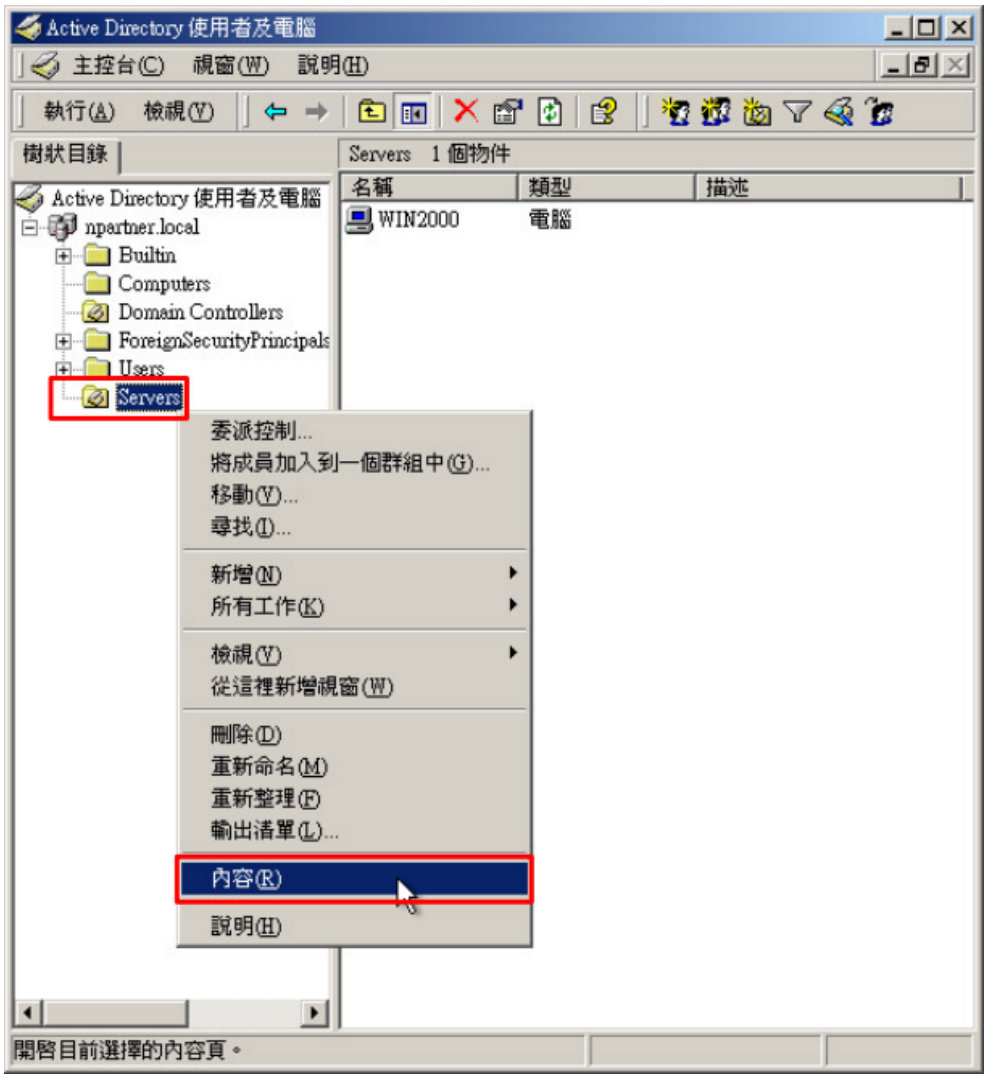
2.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

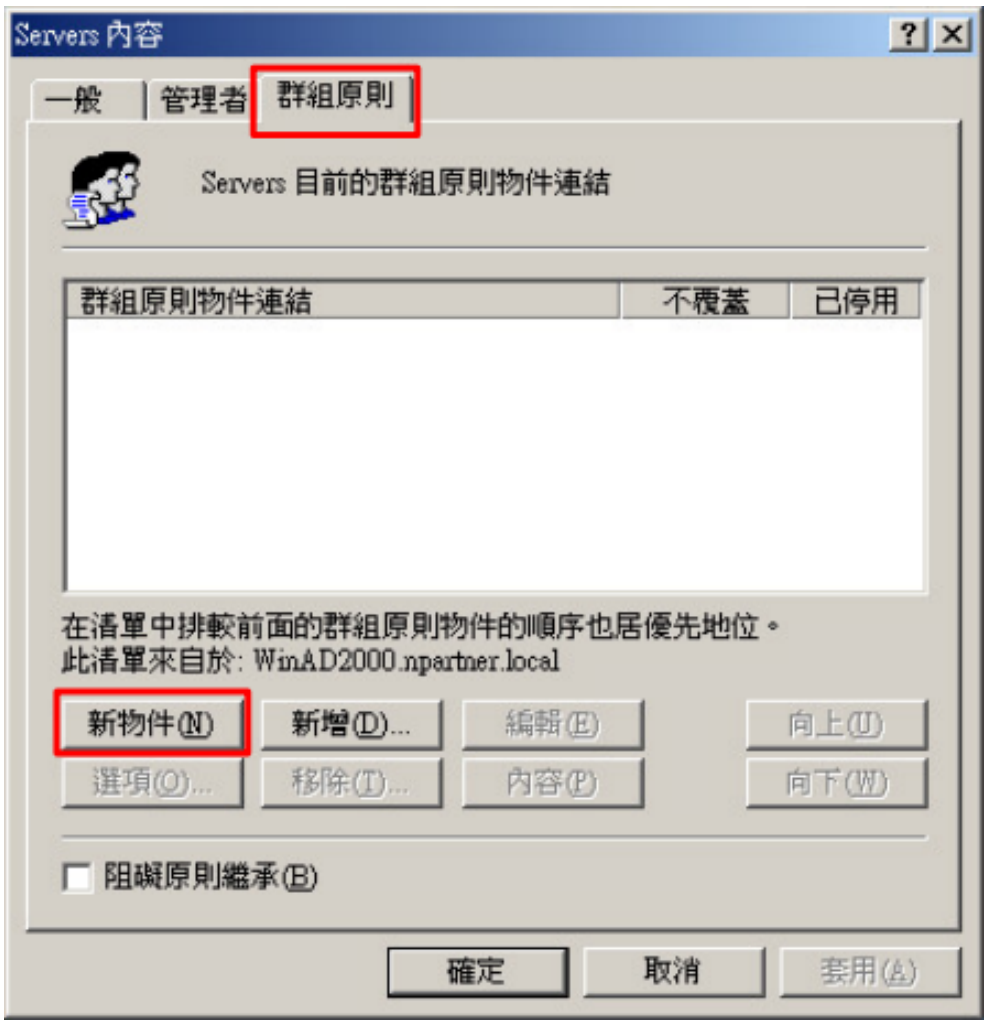
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]



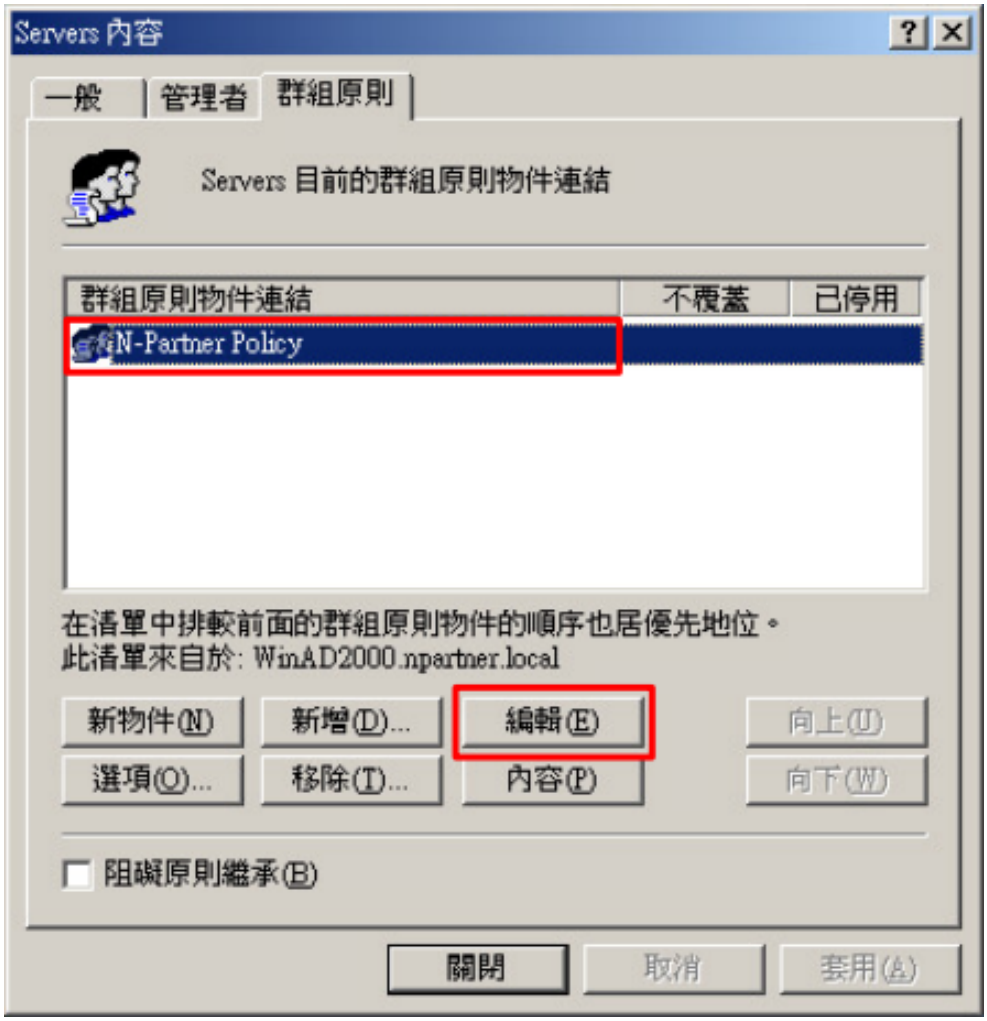
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



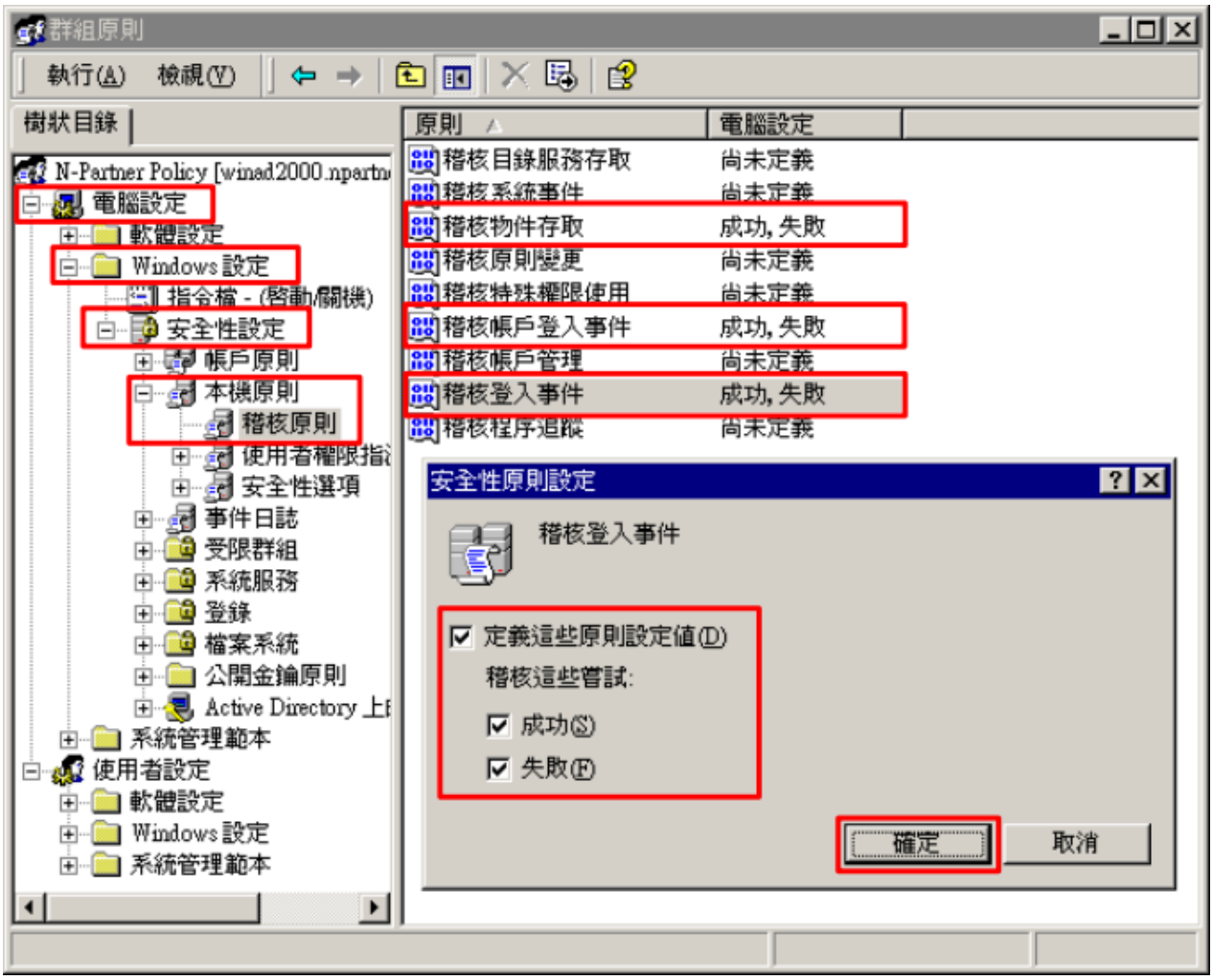
(4) 編輯群組原則物件

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]



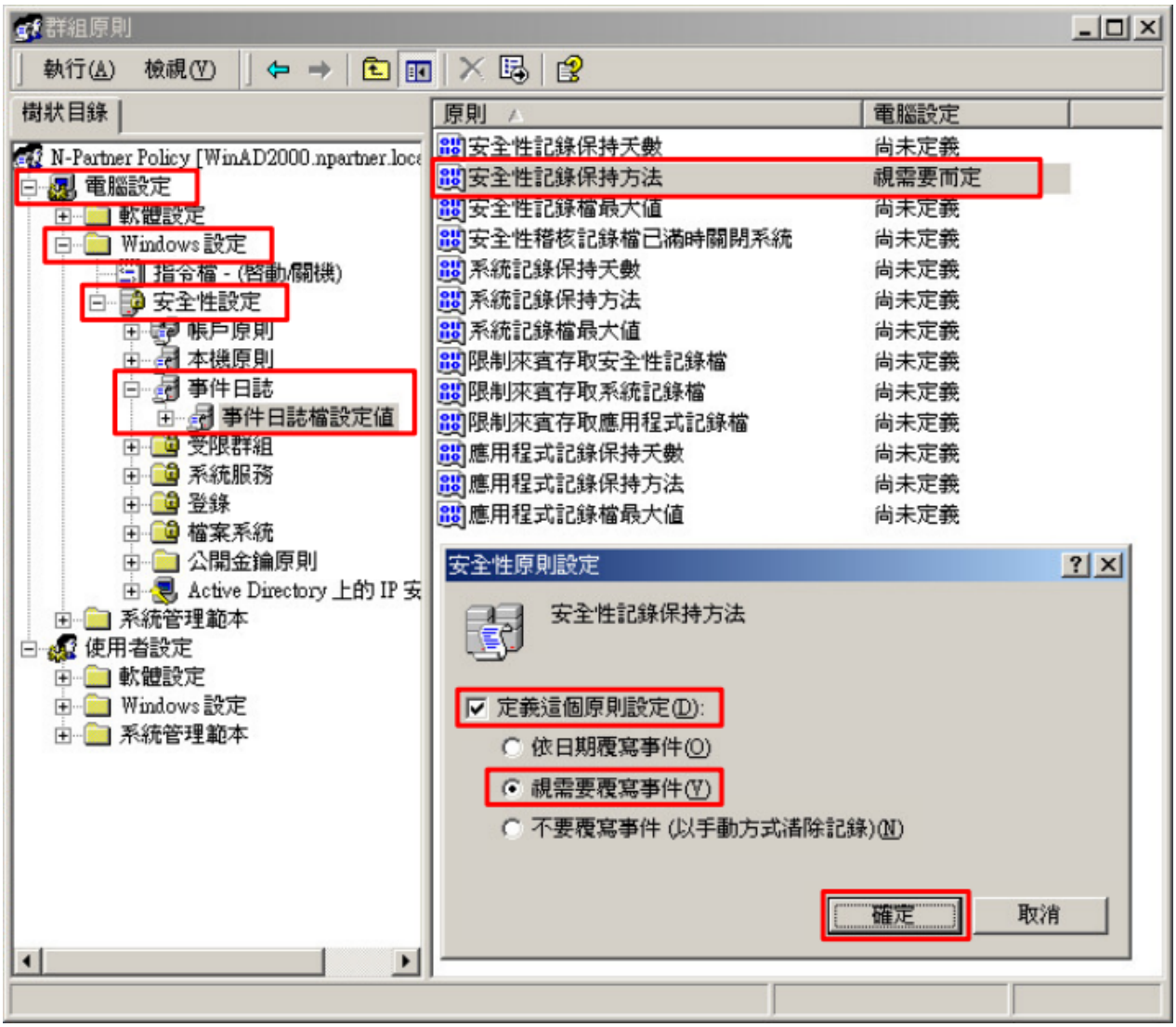
(5) 本機原則：稽核原則

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]



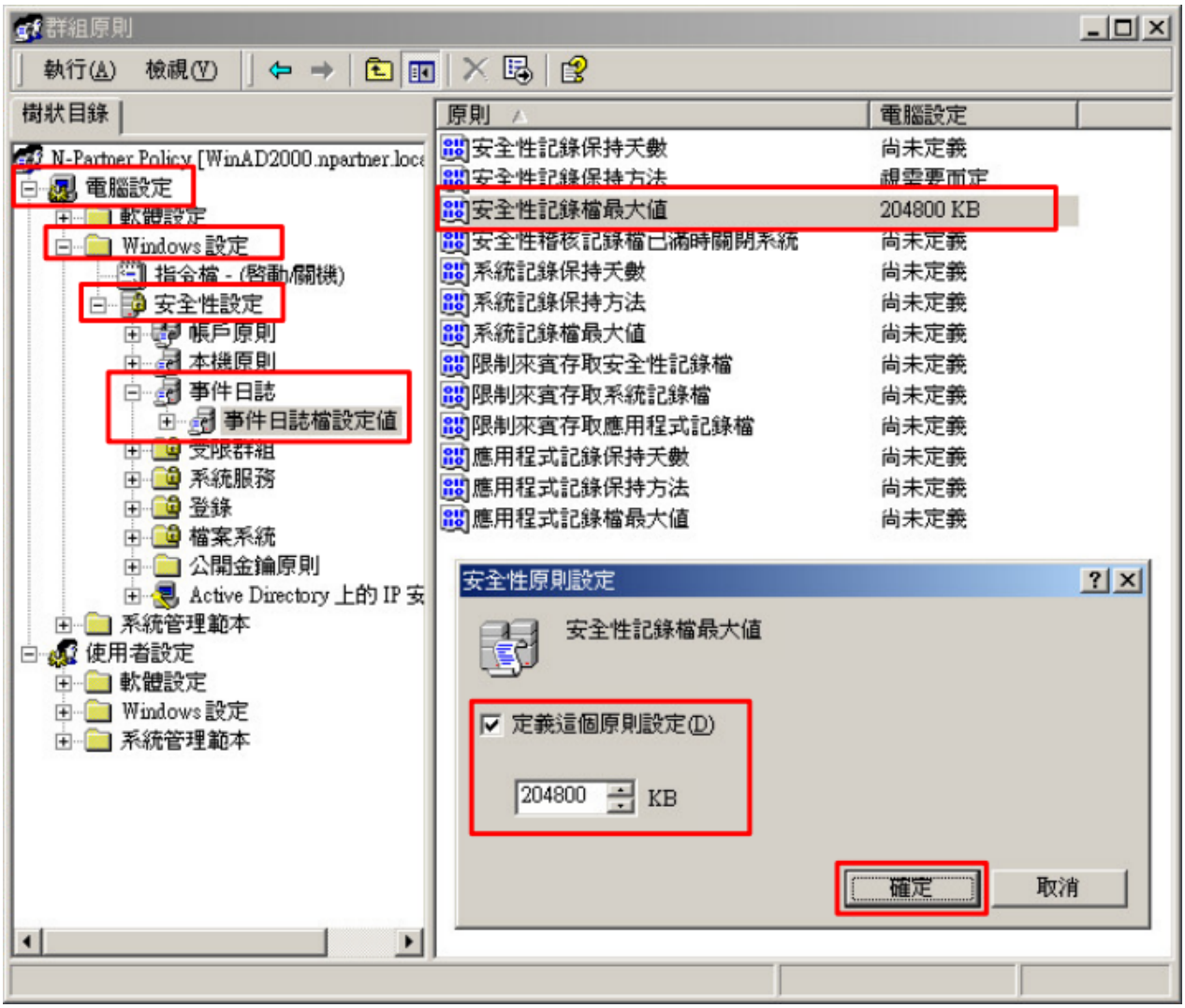
(6)　事件記錄檔：安全性記錄保持方法

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]

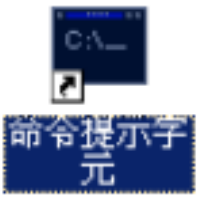


(7) 事件記錄檔：安全性記錄檔最大值

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]



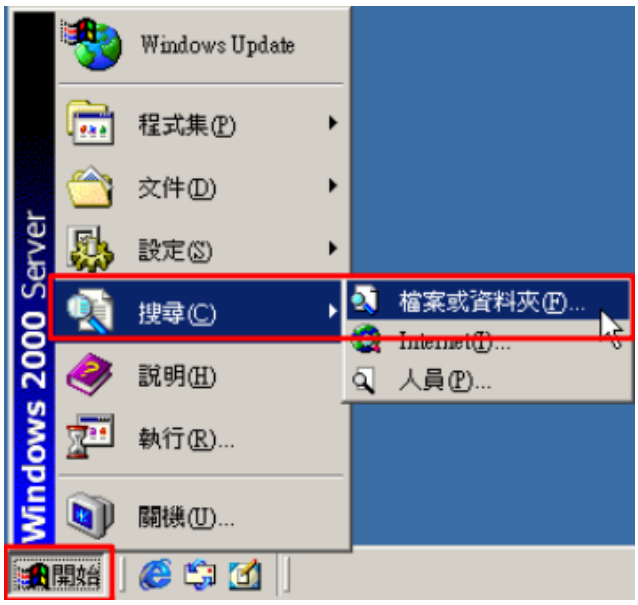
(9) 更新群組原則

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

2.2 工作群組

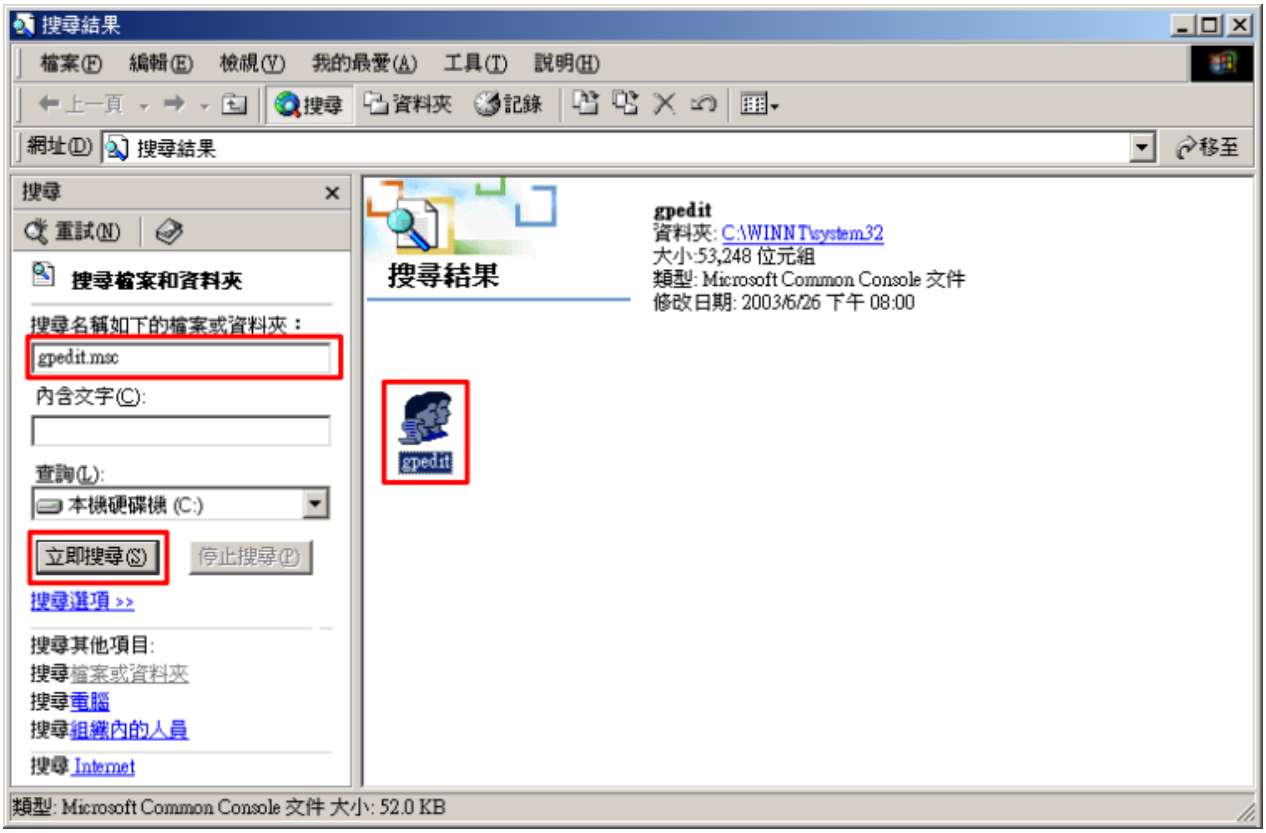
2.2.1 稽核原則設定

(1) 開啟搜尋



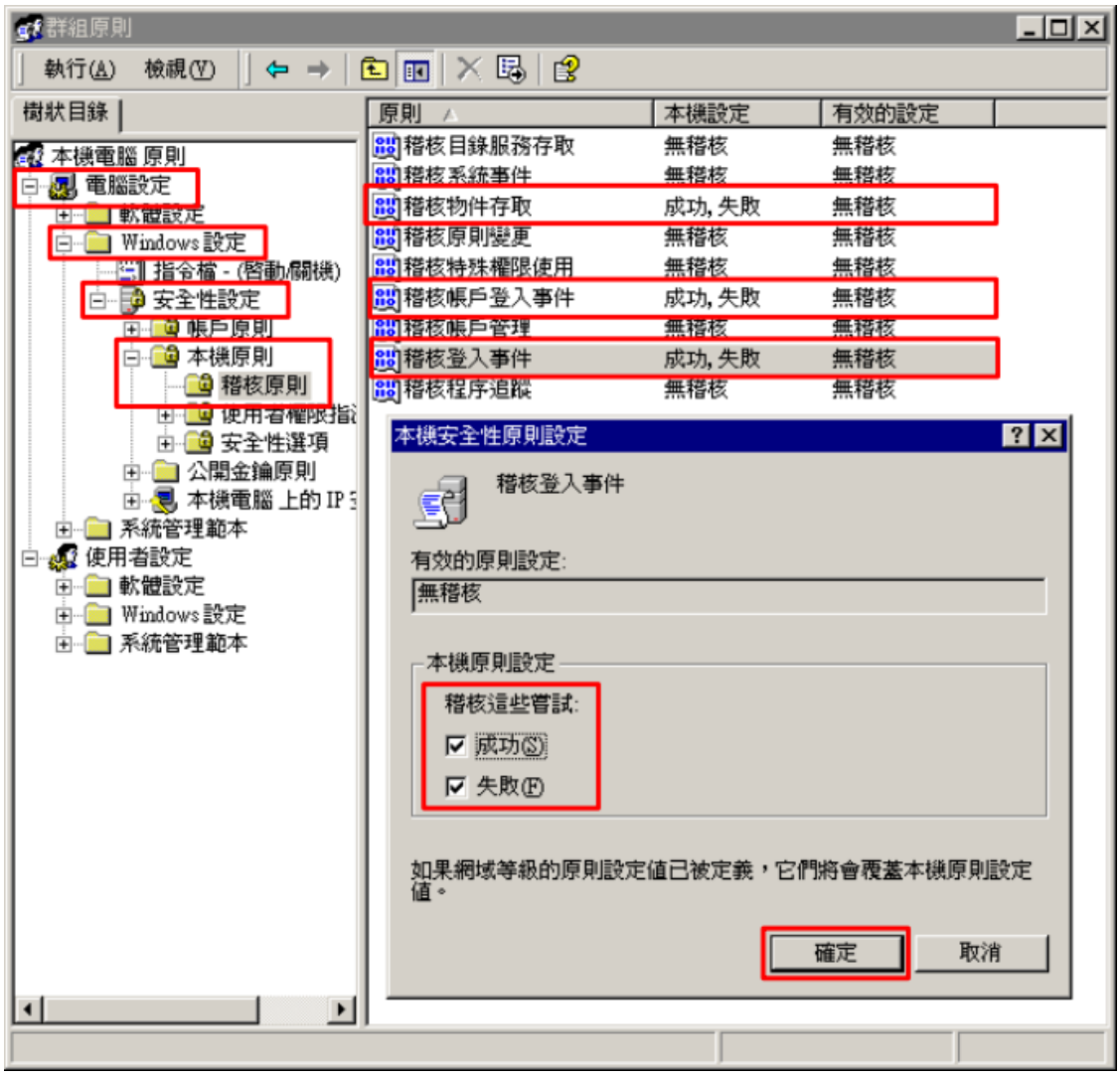
(2) 搜尋群組原則物件編輯器

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]

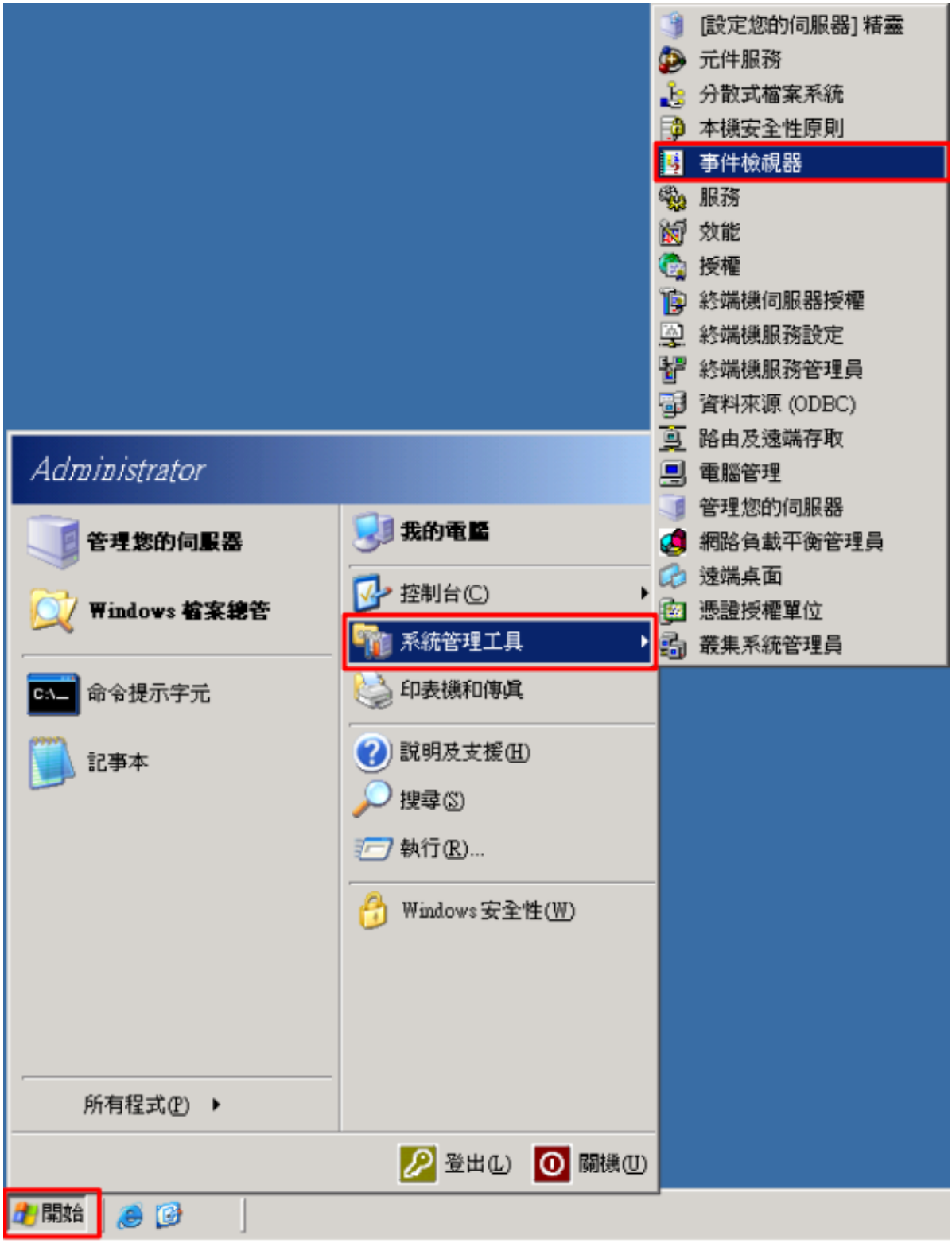
(5) 更新群組原則

```
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]

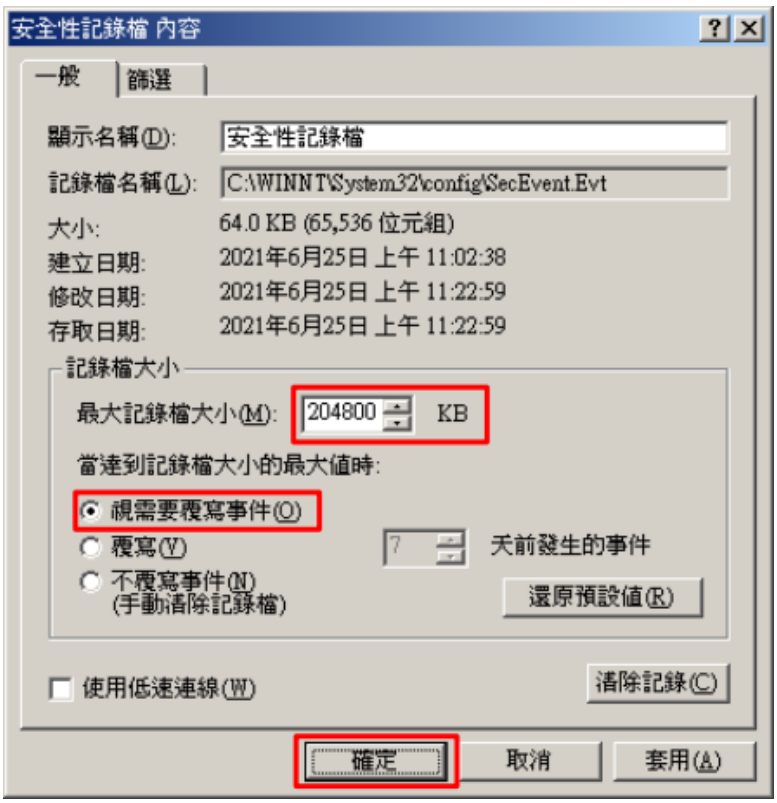


(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]

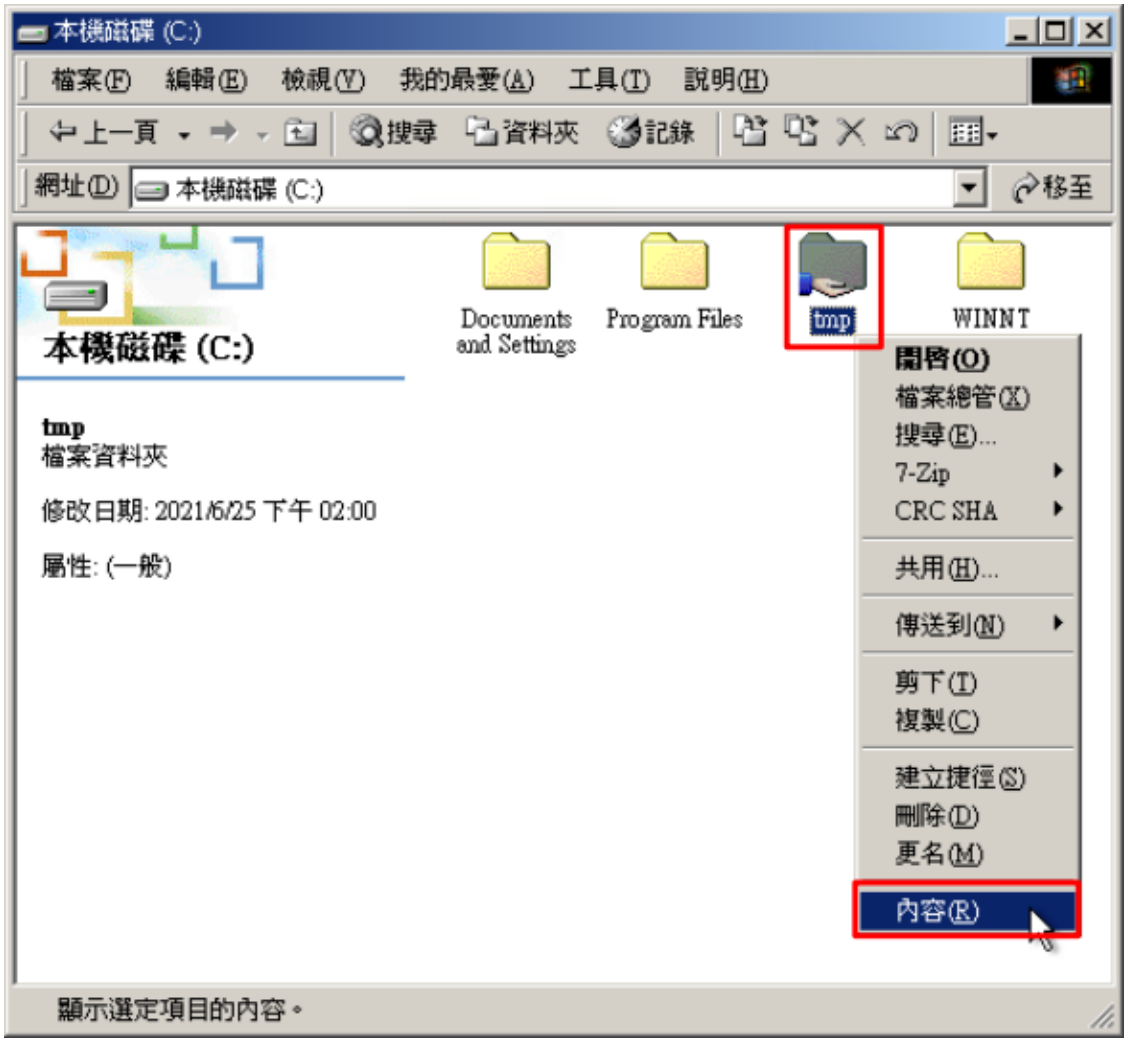
(3) 設定安全性記錄檔

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]

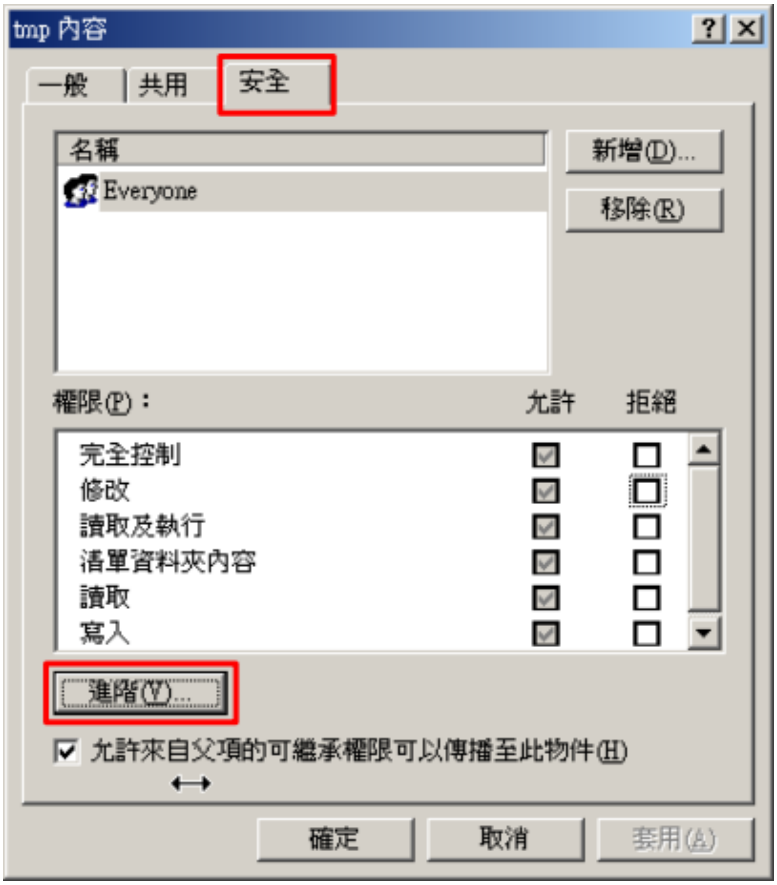


2.3 稽核資料夾設定

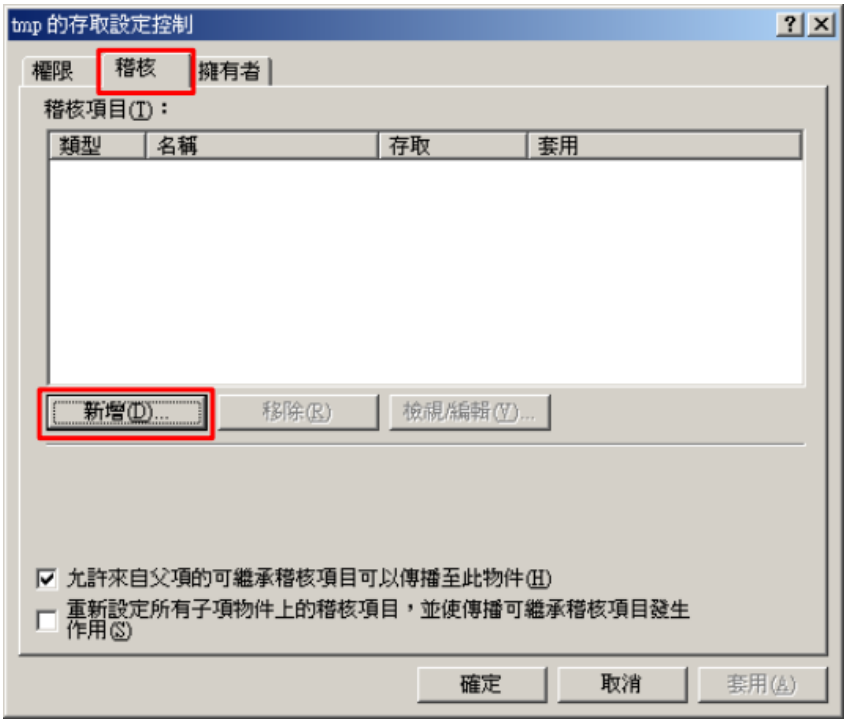
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



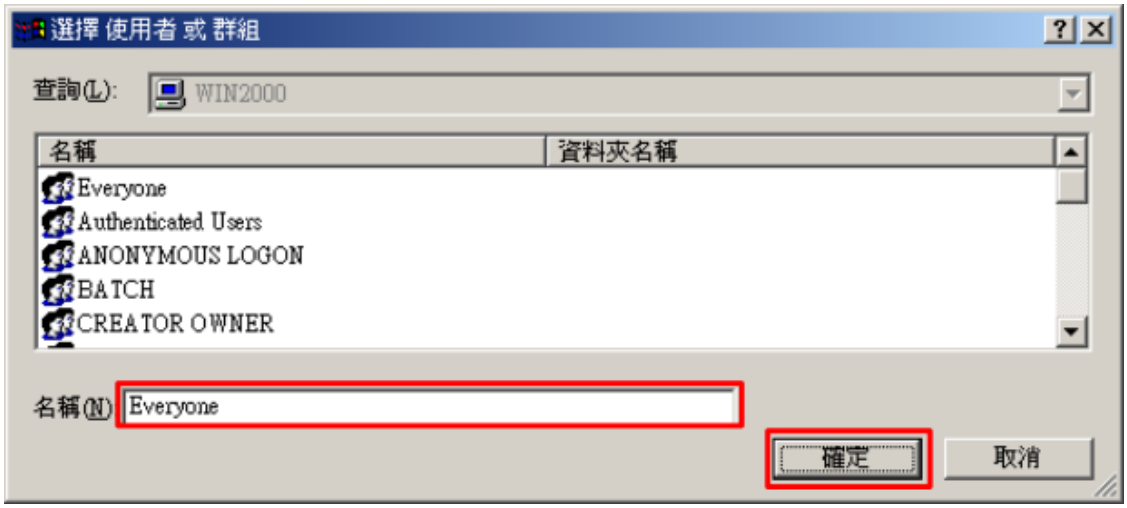
(2) 點選 [安全] 頁面 -> 按 [進階]



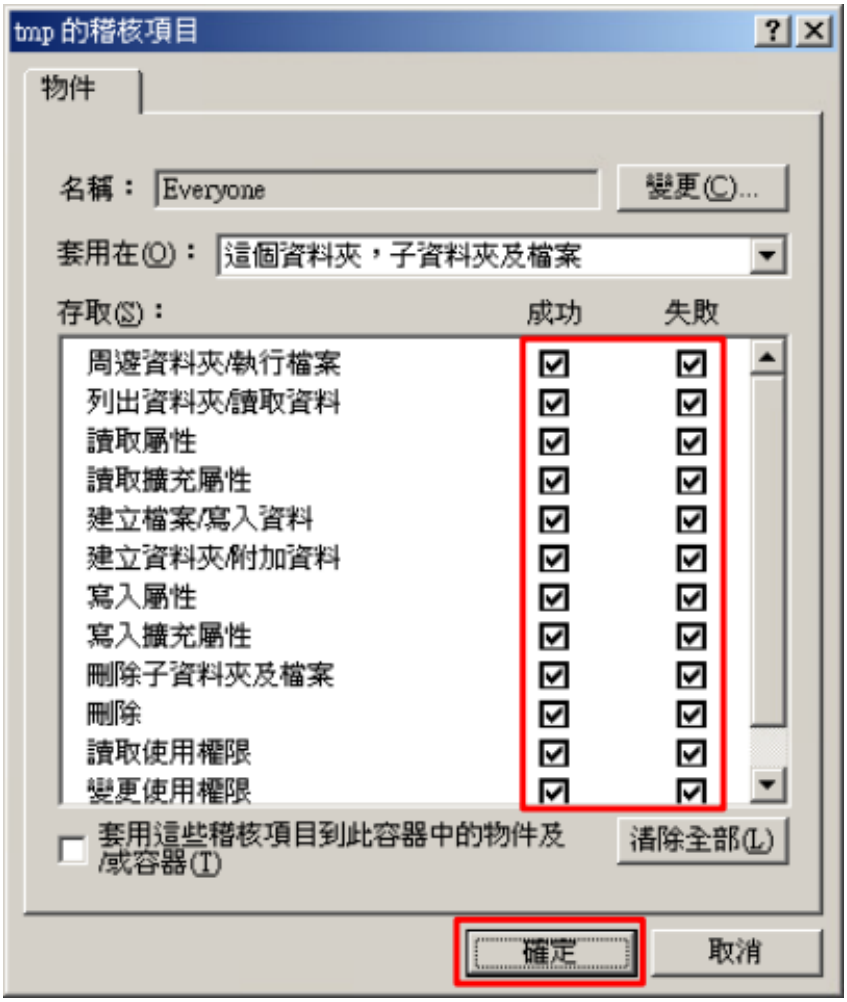
(3) 點選 [稽核] 頁面 -> 按 [新增]



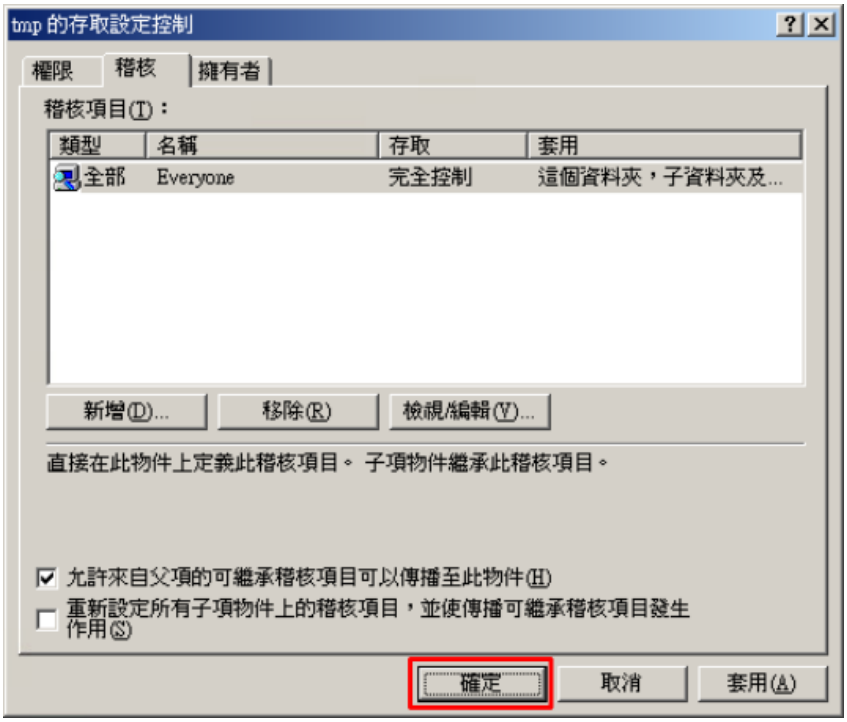
(4) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [確定]



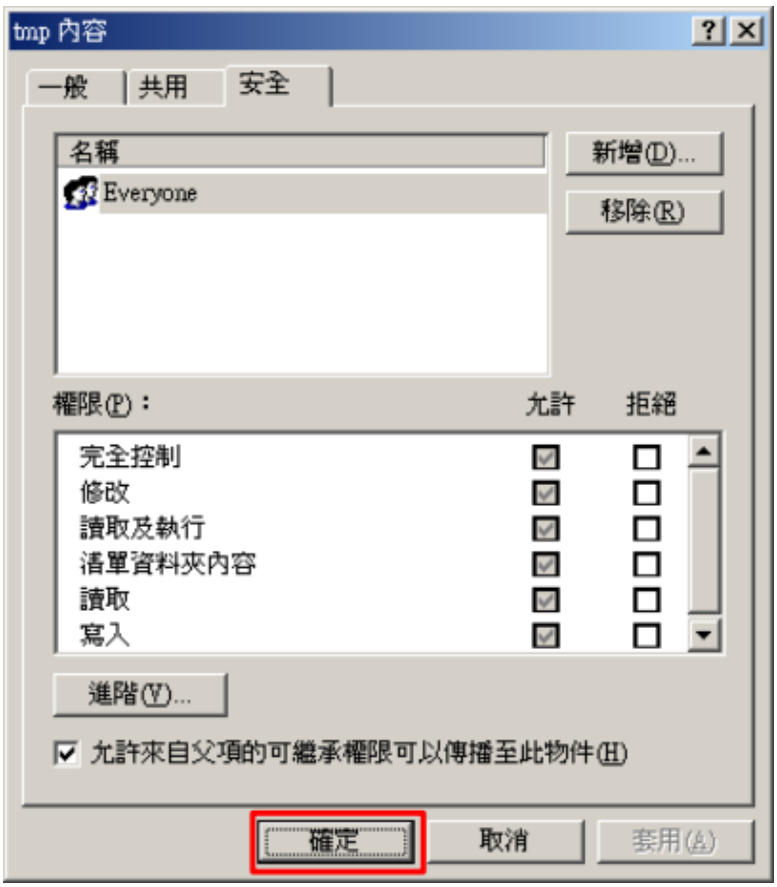
(5) 勾選所有項目存取 [成功] 和 [失敗] -> 按 [確定]



(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

*以下分別為網域或工作群組設定方式。

3.1 網域

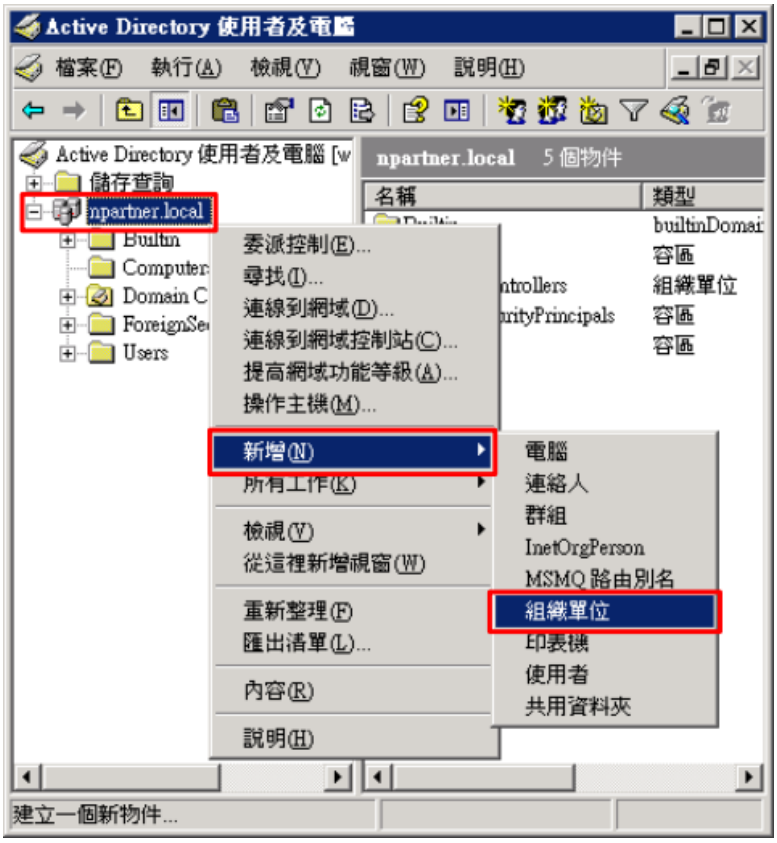
3.1.1 組織單位設定

(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]

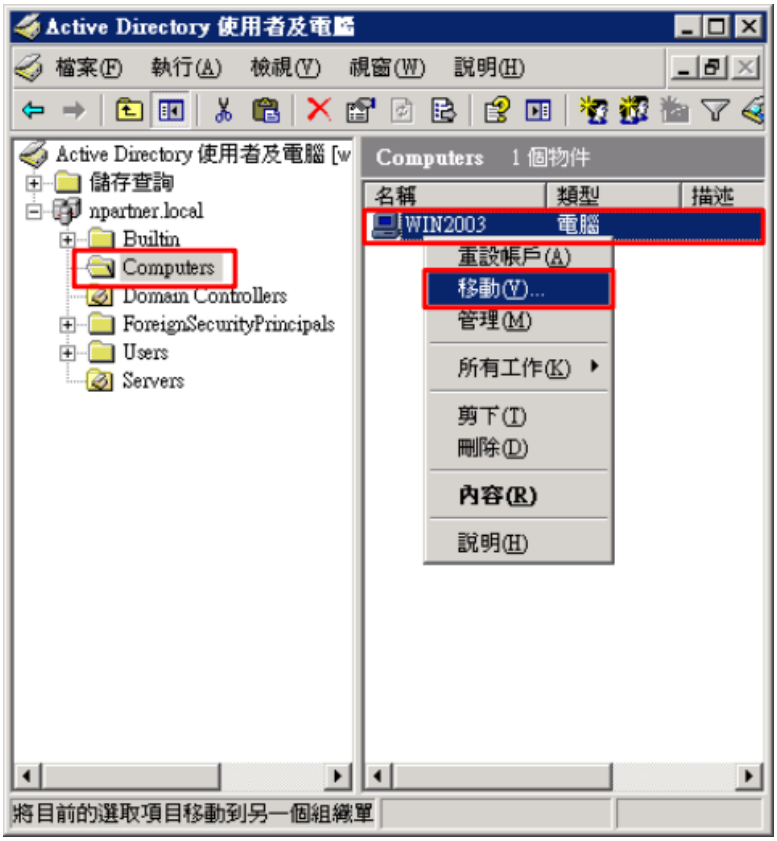


(3) 輸入組織單位名稱

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 主機 -> 點選 [移動]

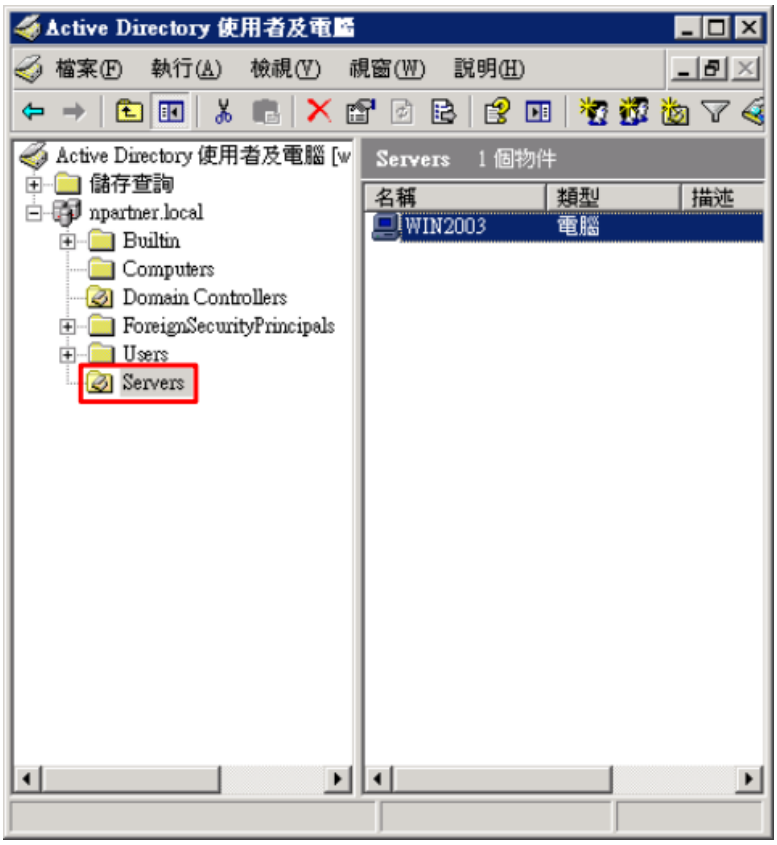


(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

(6) 確認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。



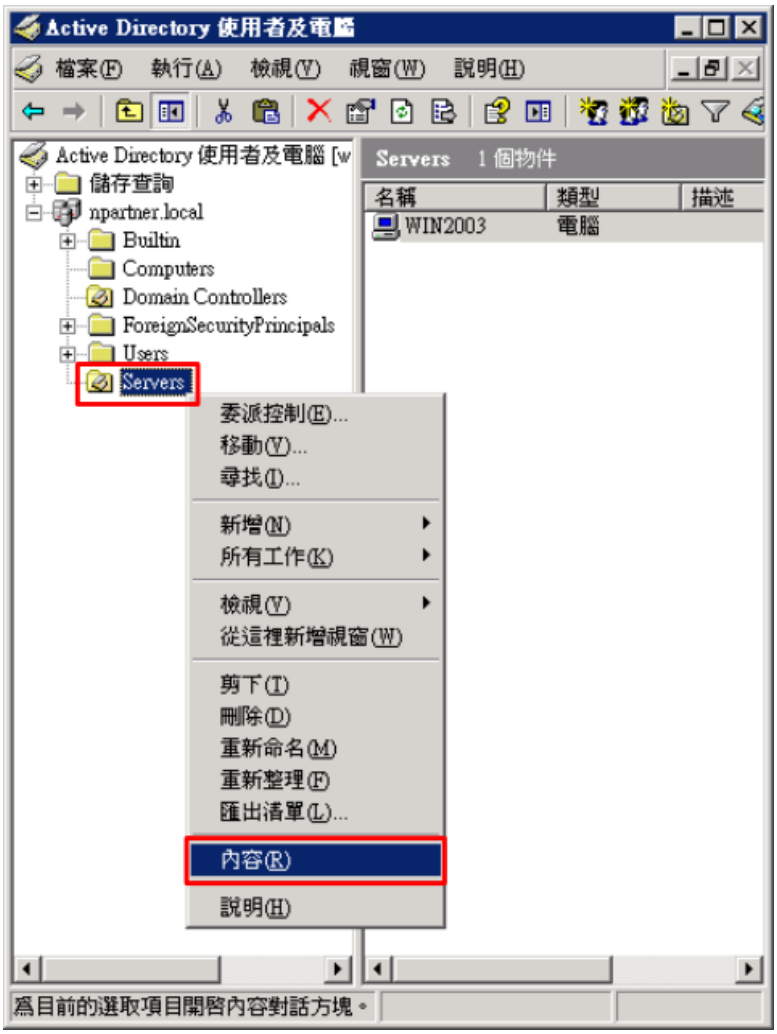
3.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

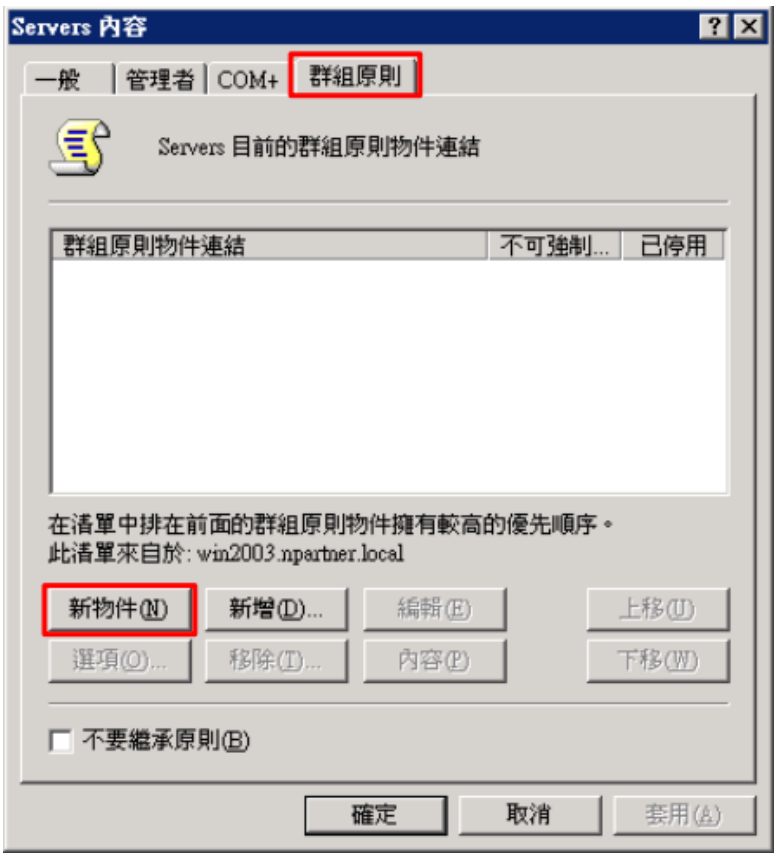
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位按滑鼠右鍵 -> 點選 [內容]



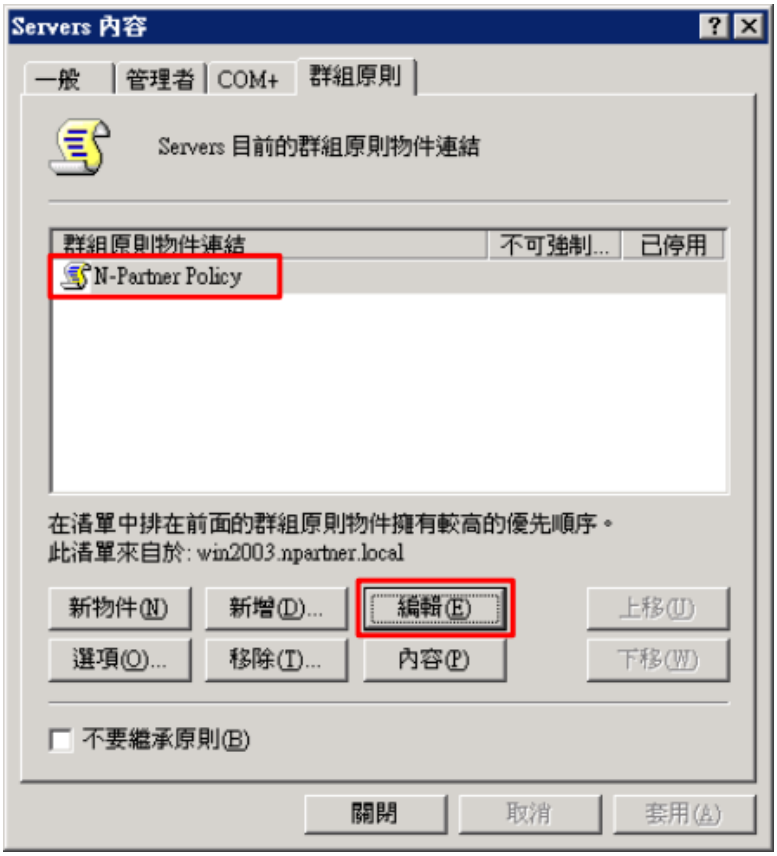
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



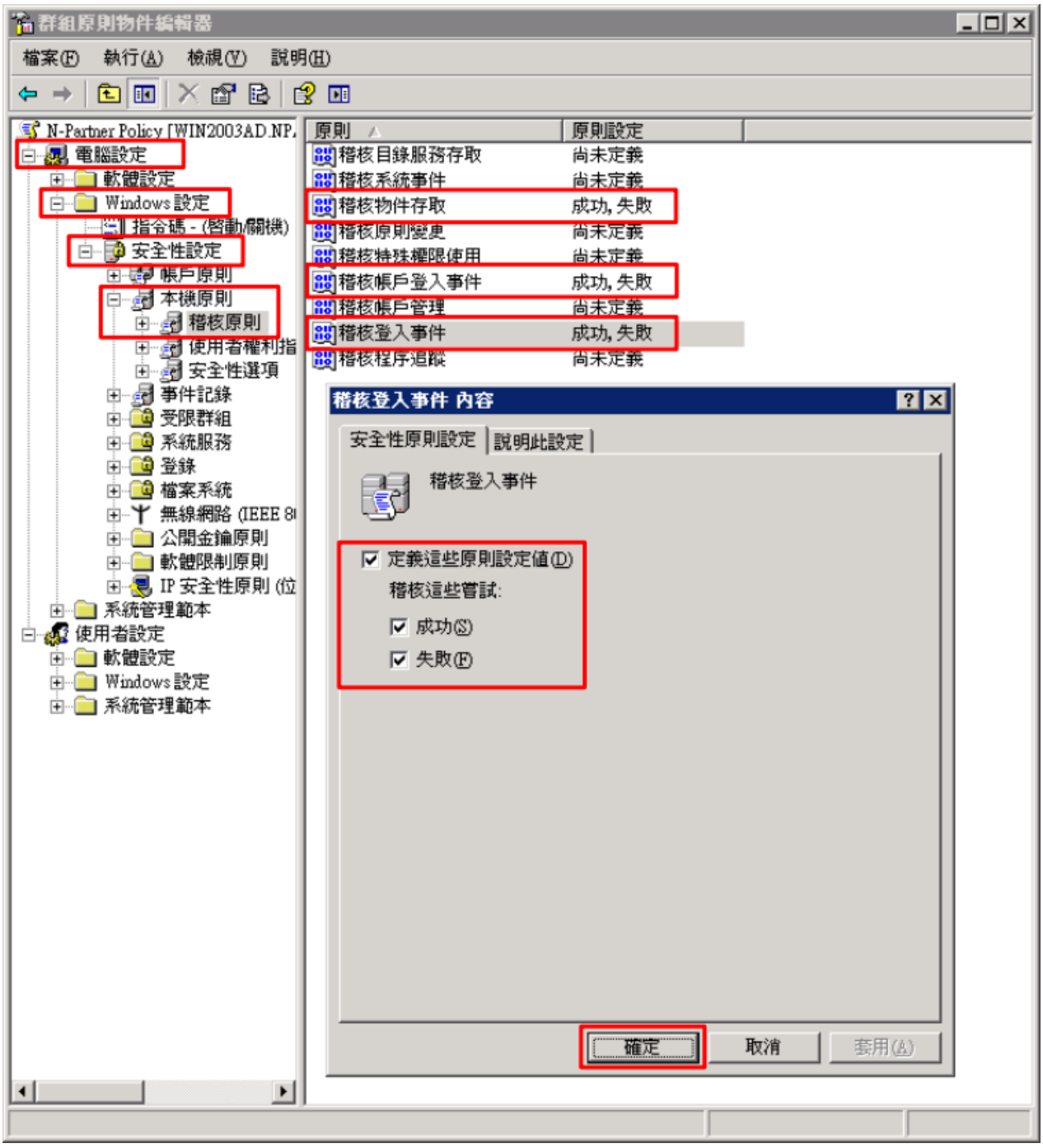
(4)　編輯群組原則物件

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]



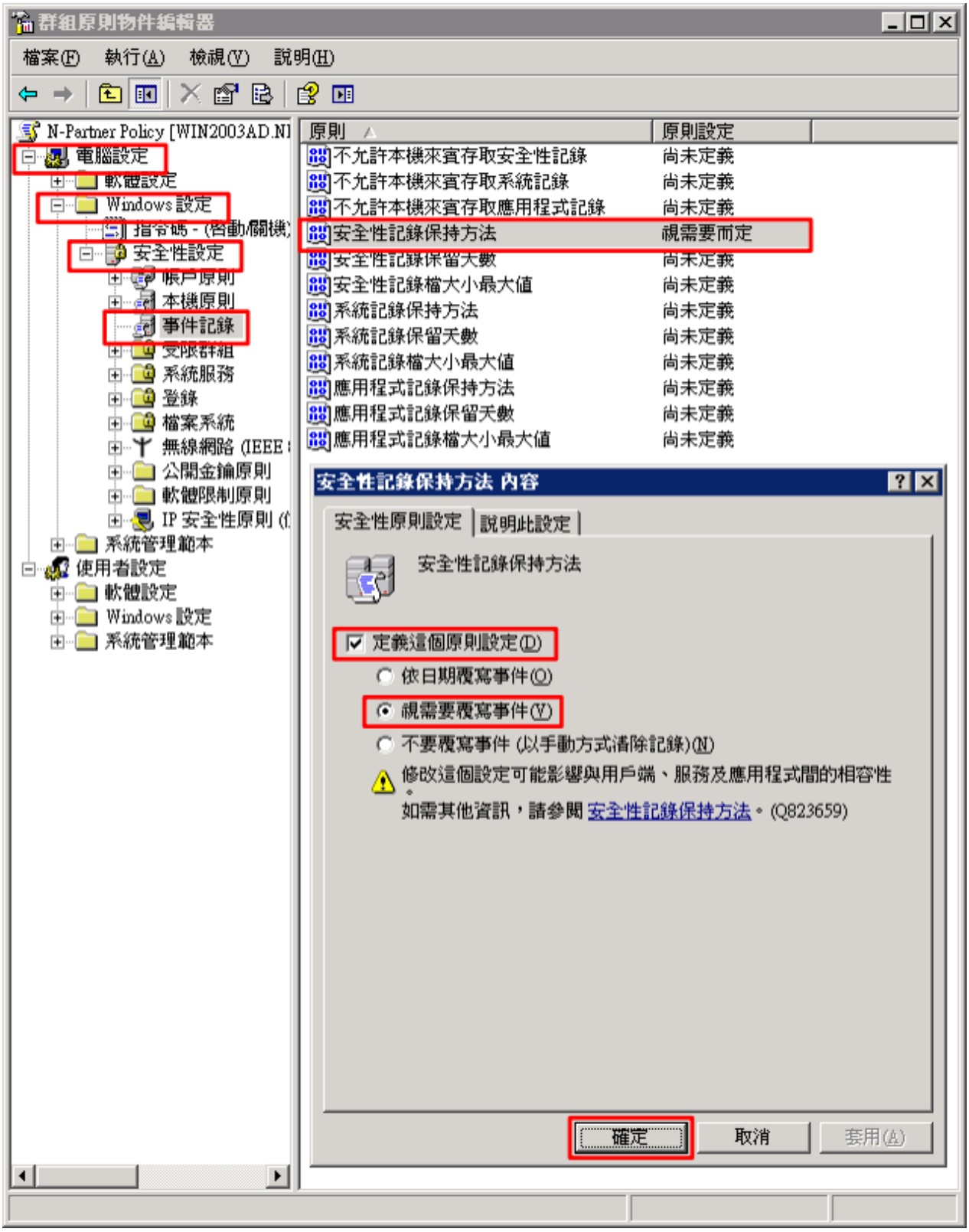
(5) 本機原則：稽核原則

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]



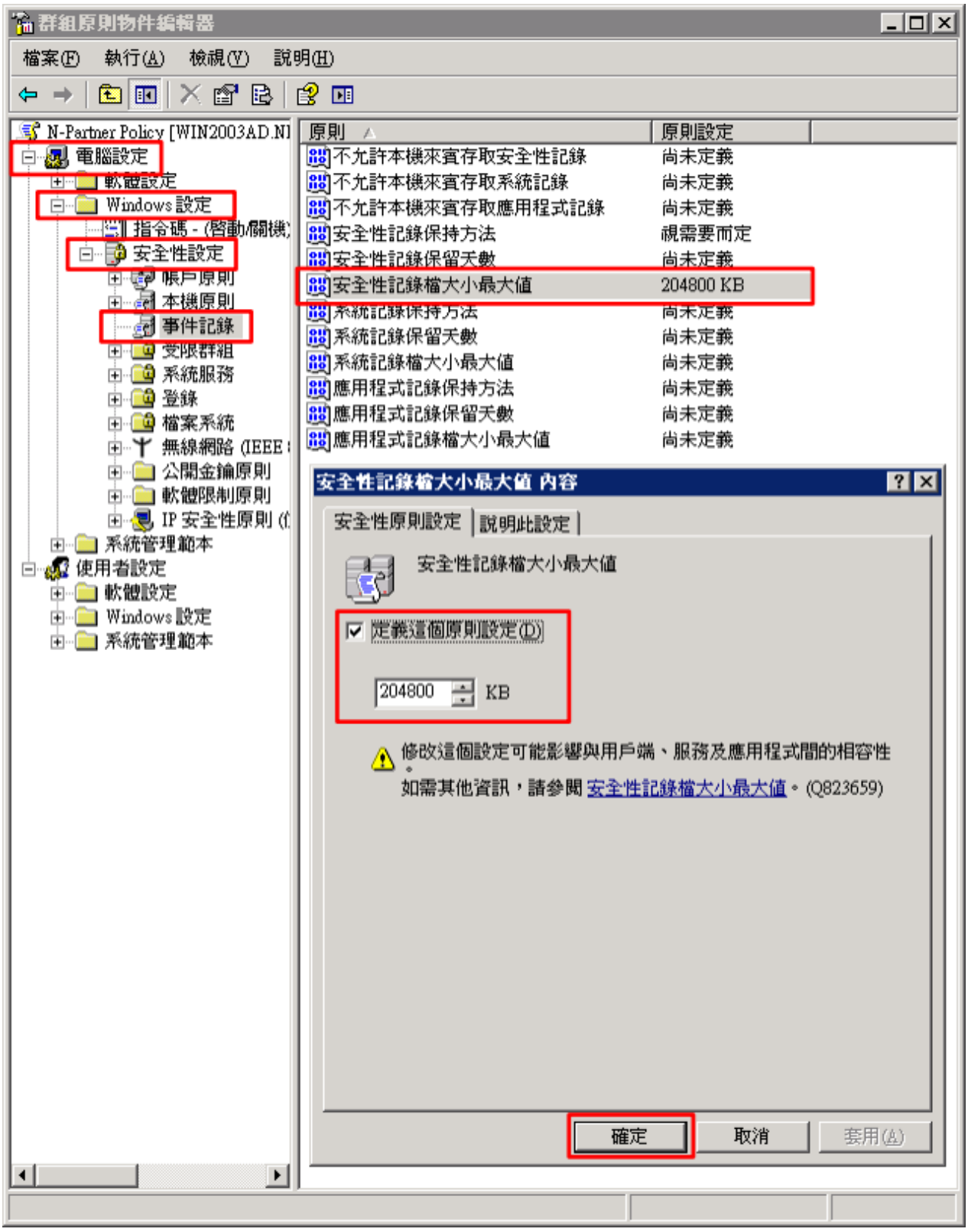
(6)　事件記錄檔：安全性記錄保持方法

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

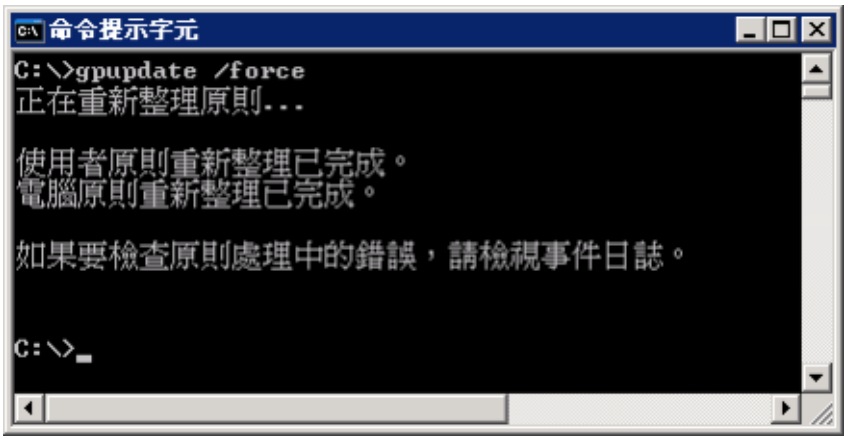
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8)　在 Windows File 伺服器，開啟 [命令提示字元]

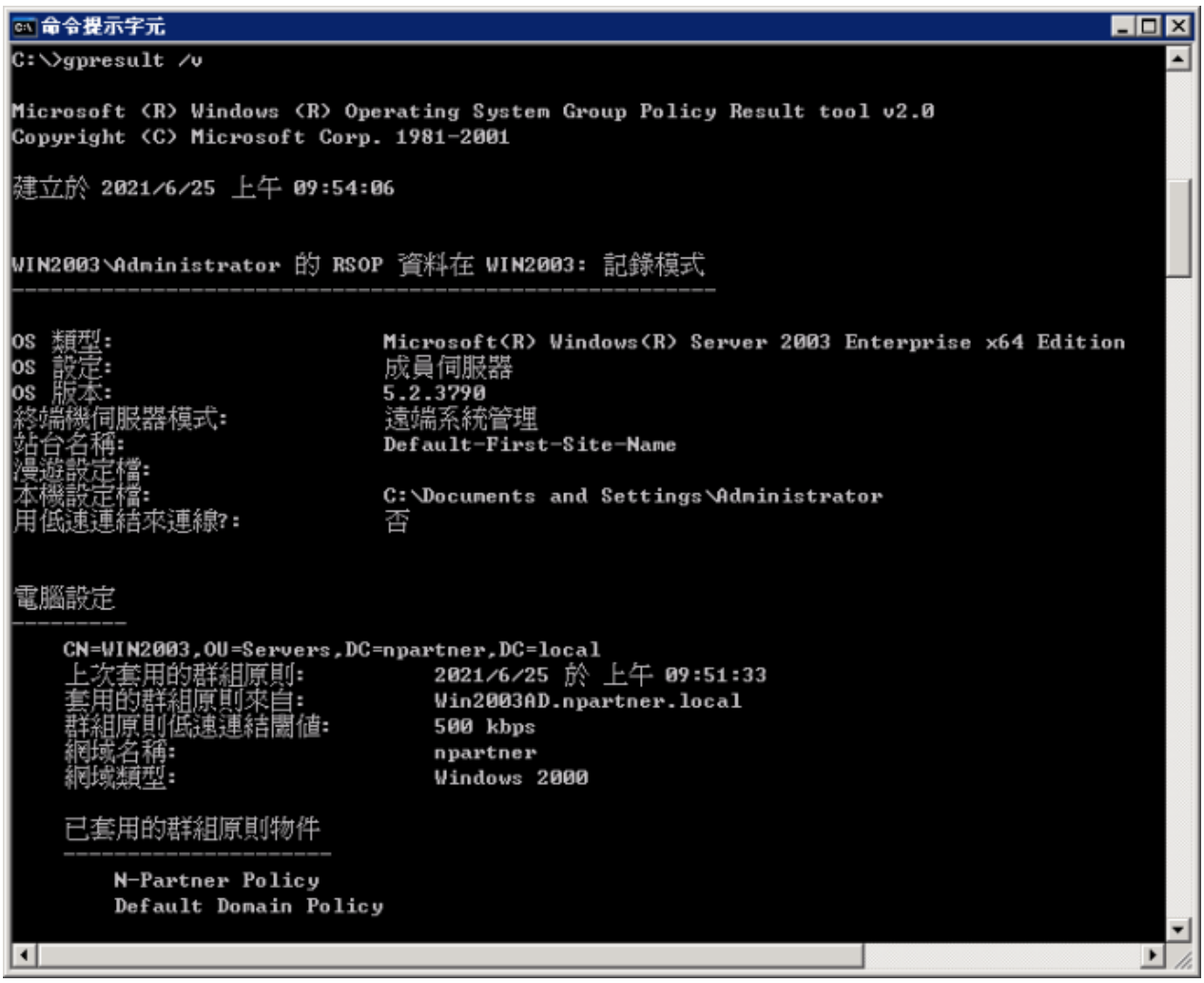
(9)　更新群組原則

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



(10) 查看群組原則套用情形

```
C:\> gpresult /v
```



3.2 工作群組

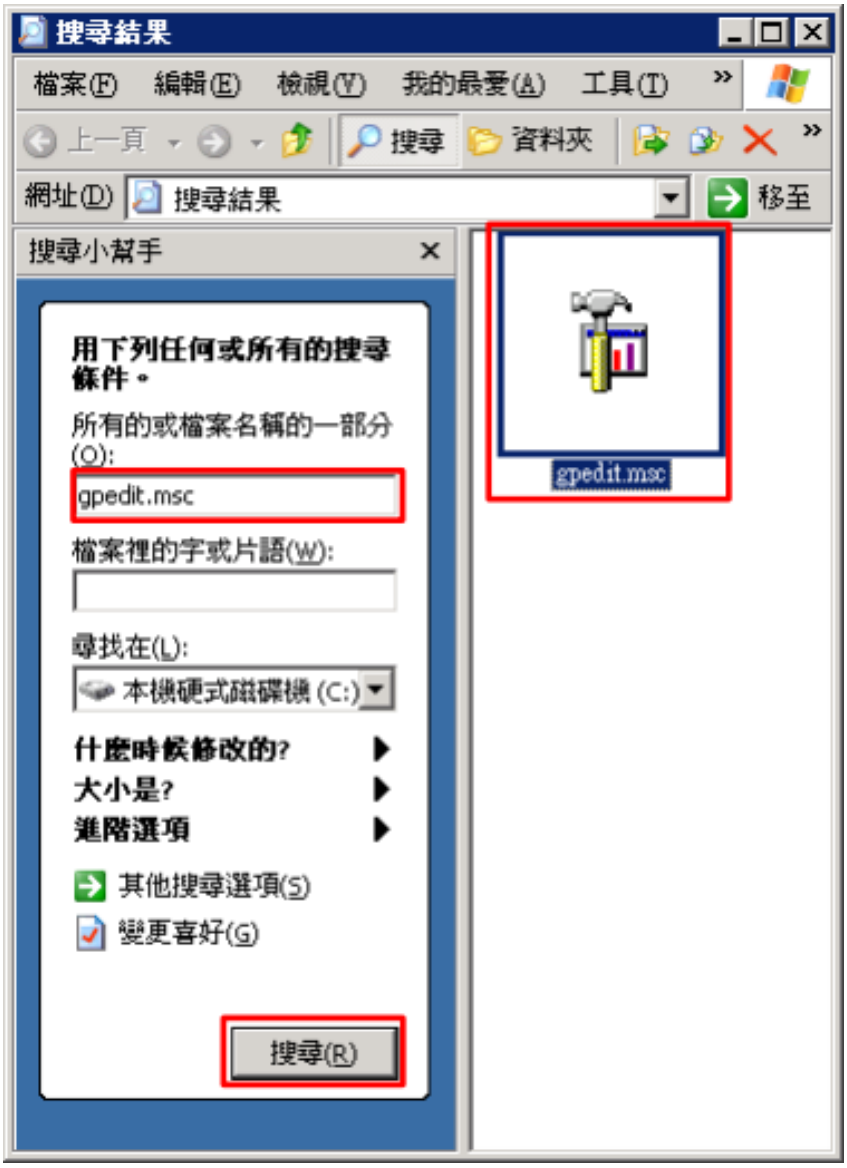
3.2.1 稽核原則設定

(1) 開啟搜尋

按 [開始] -> 點選 [搜尋]

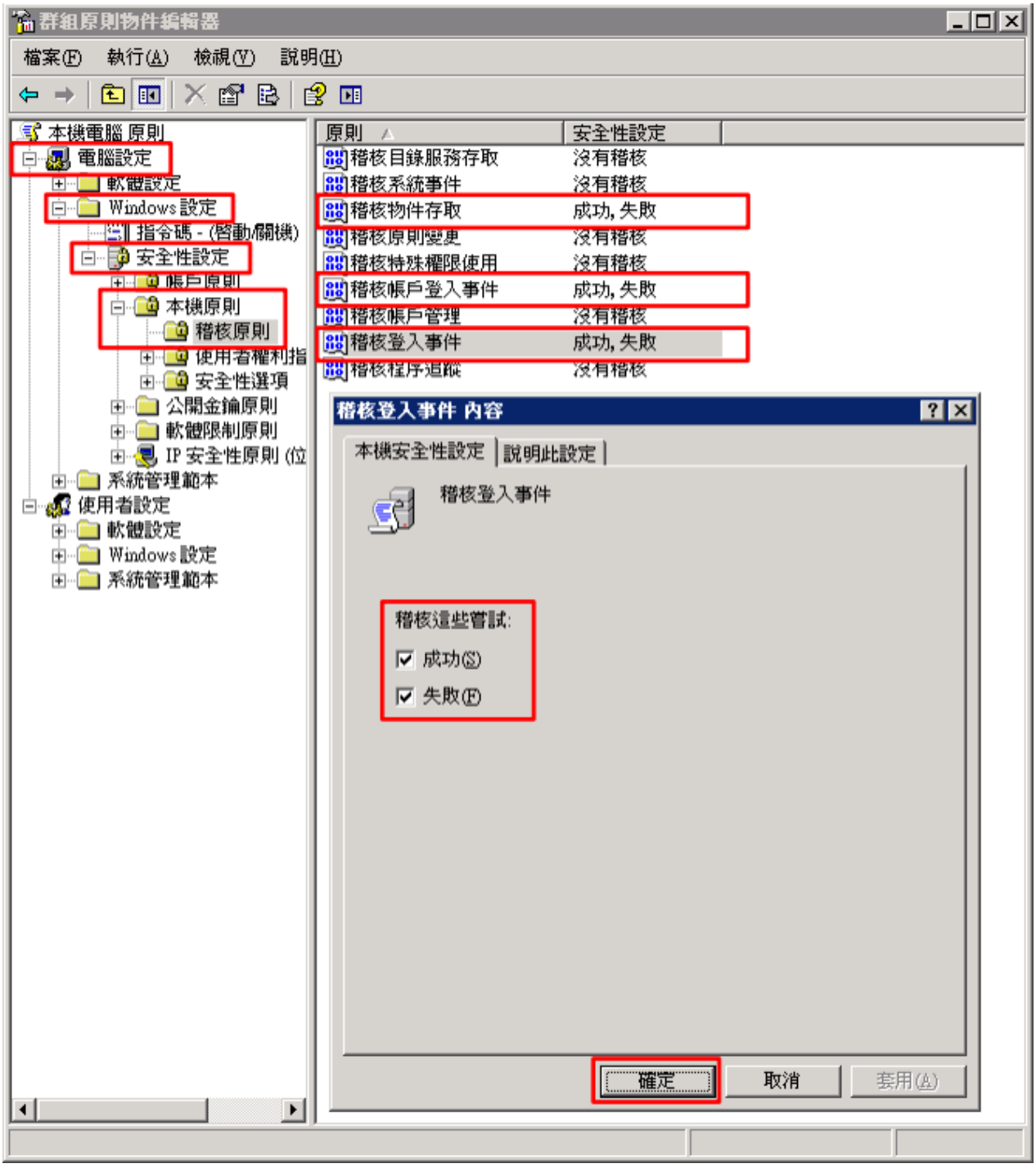
(2) 搜尋群組原則物件編輯器

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



(3) 本機原則：稽核原則

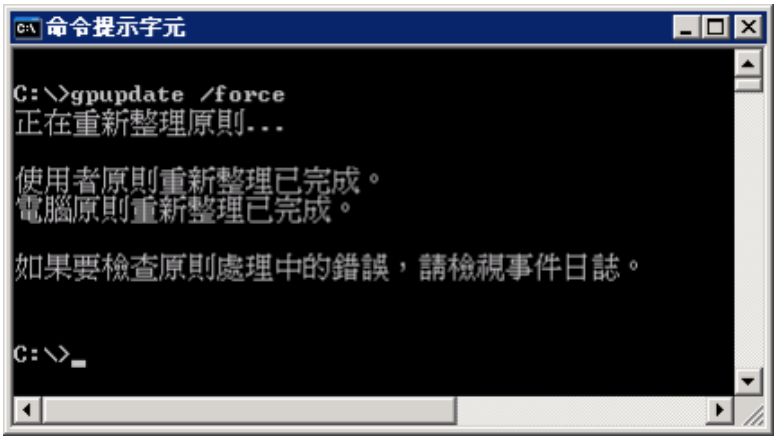
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(4) 開啟 [命令提示字元]

(5) 更新群組原則

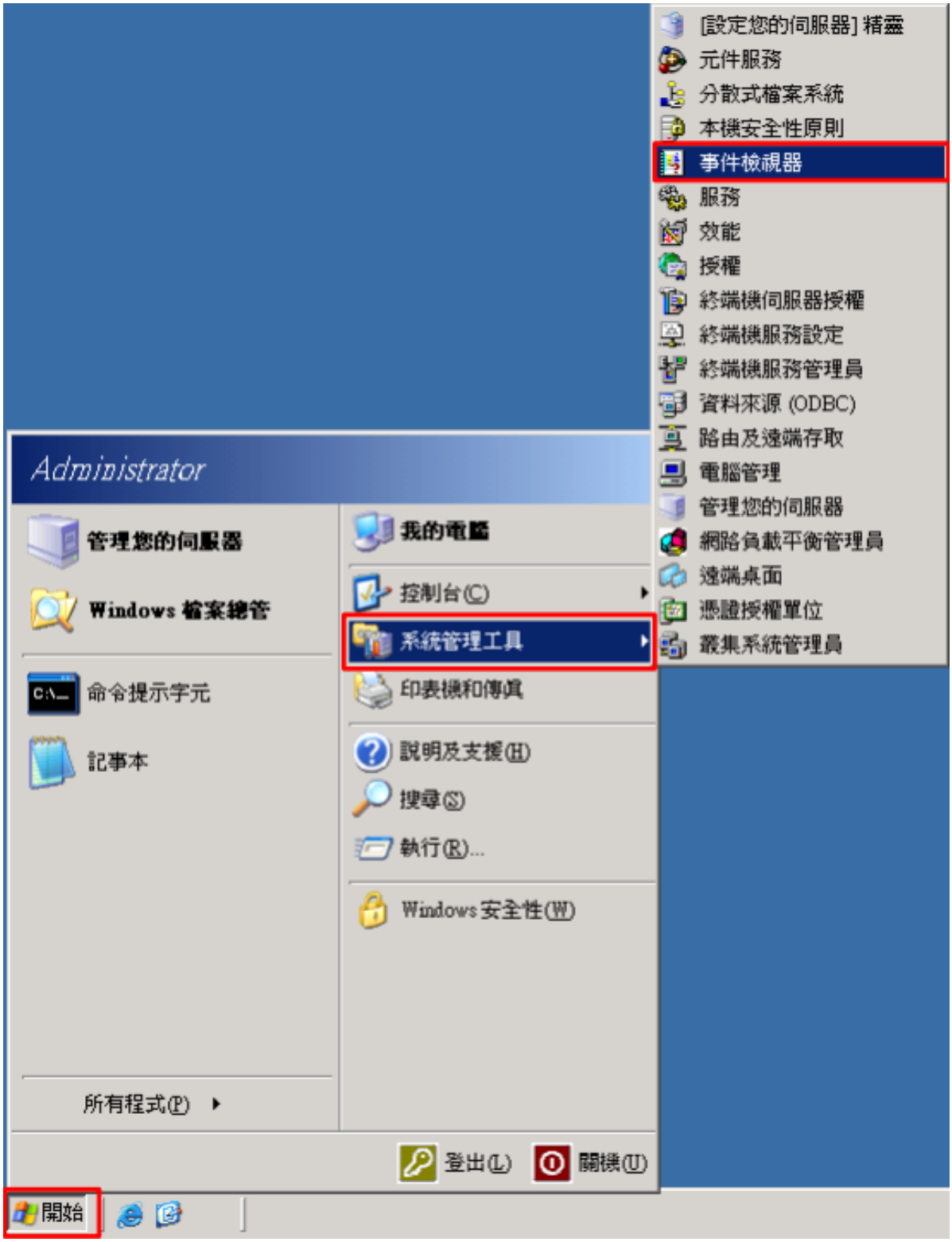
```
C:\> gpupdate /force
```



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]

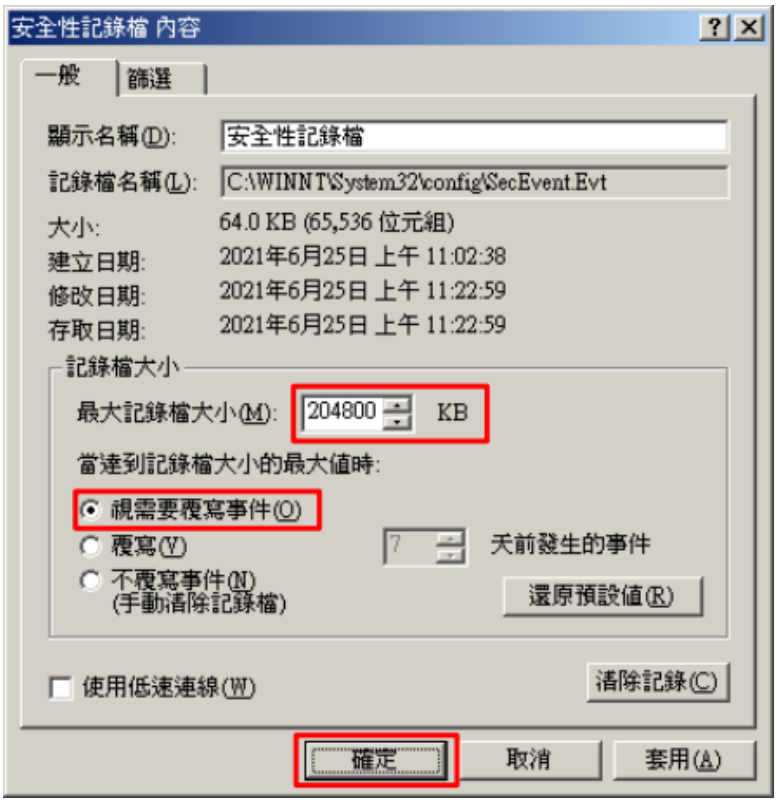


(2) 編輯安全性記錄

在 [安全性] 按滑鼠右鍵 -> 點選 [內容]

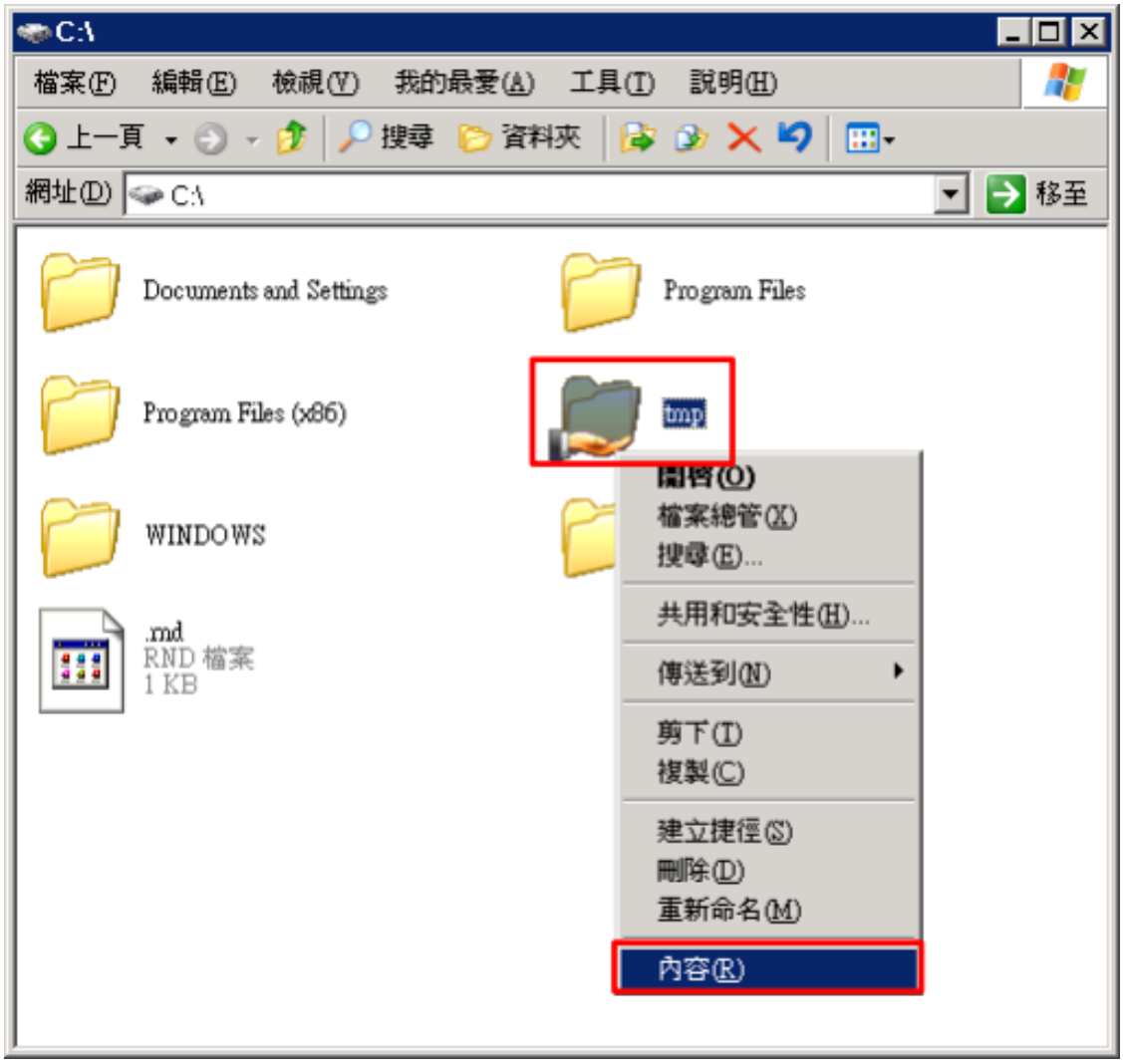
(3) 設定安全性記錄檔

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]

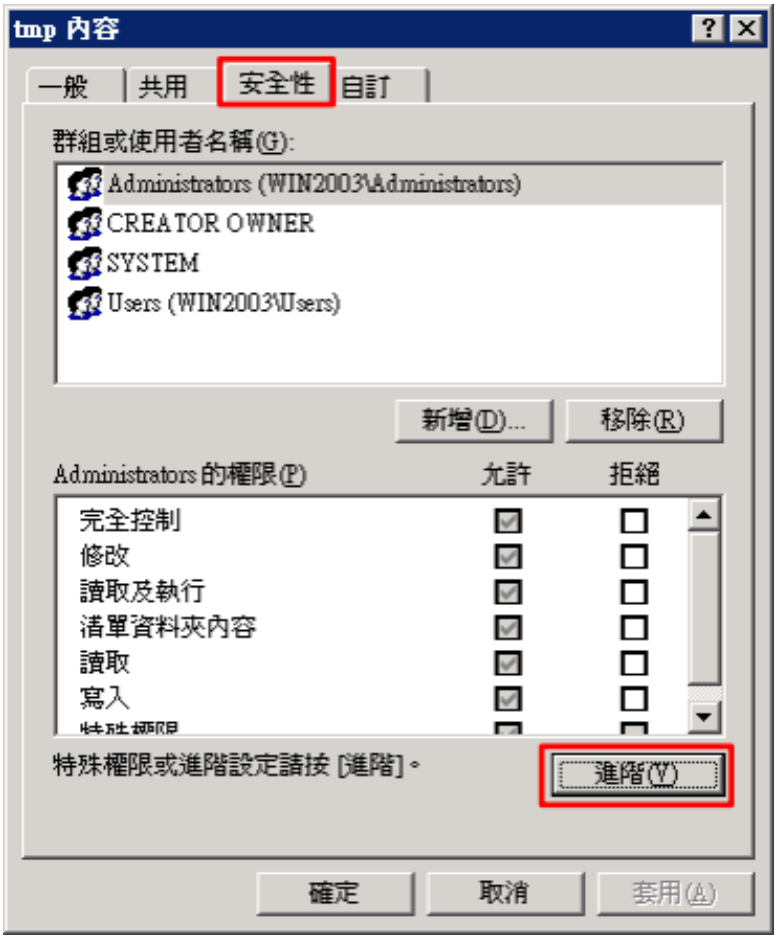


3.3 稽核資料夾設定

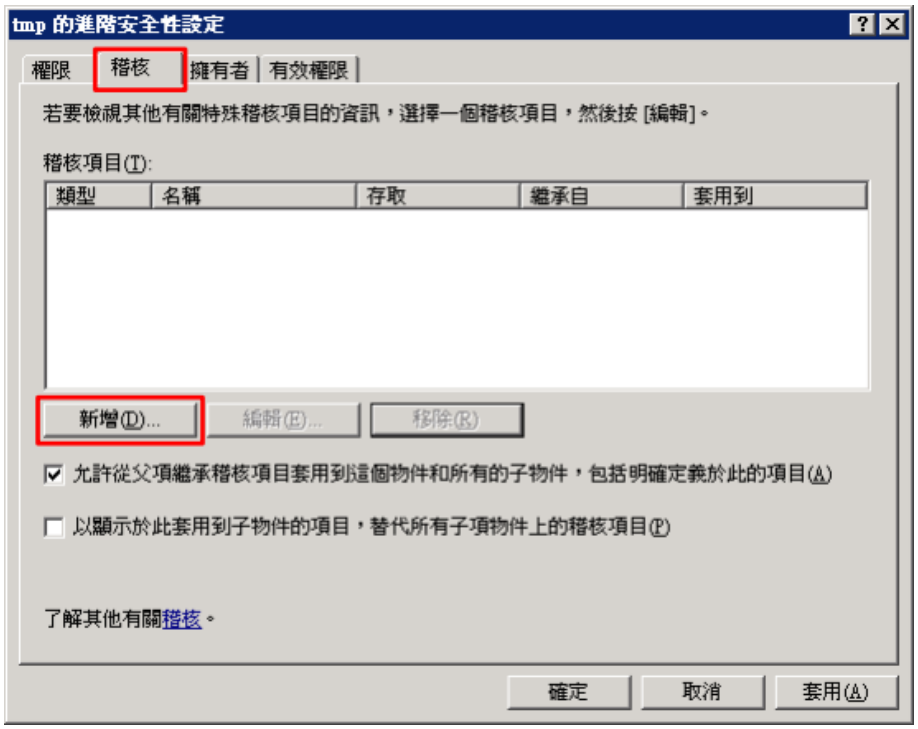
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



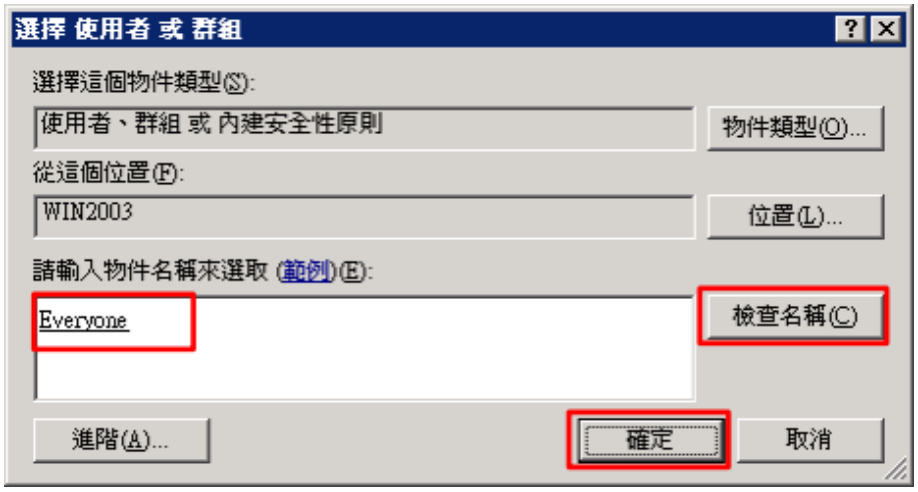
(2) 點選 [安全性] 頁面 -> 按 [進階]



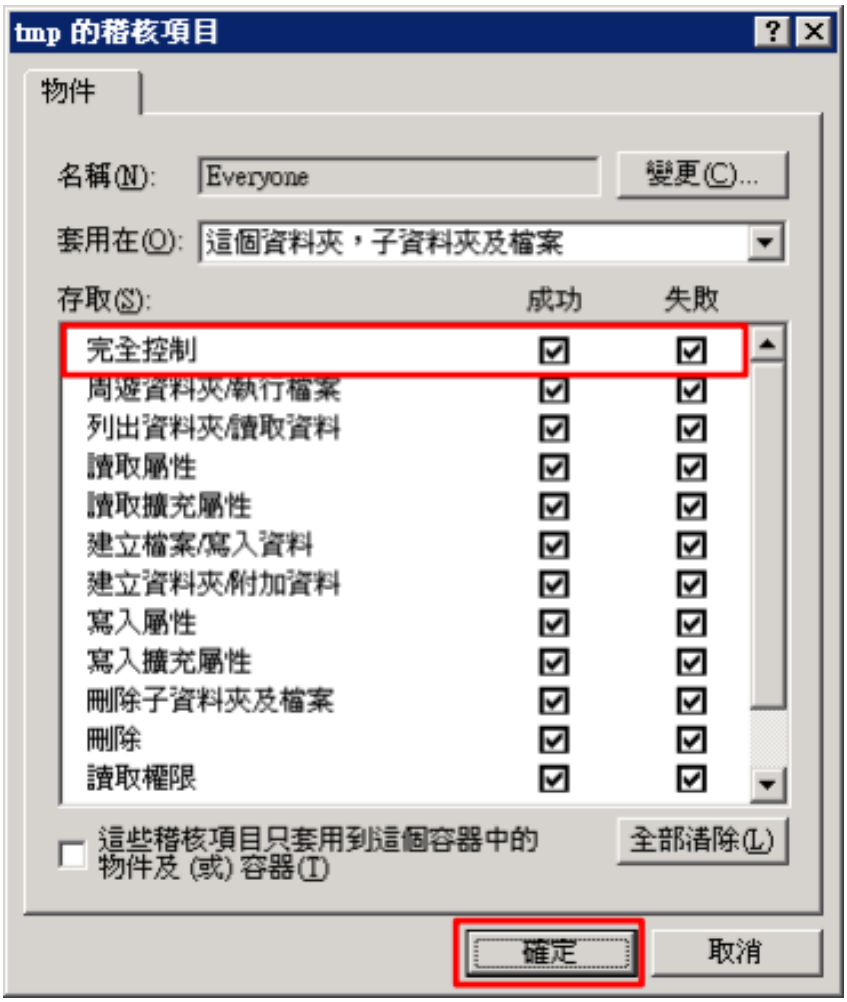
(3) 點選 [稽核] 頁面 -> 按 [新增]



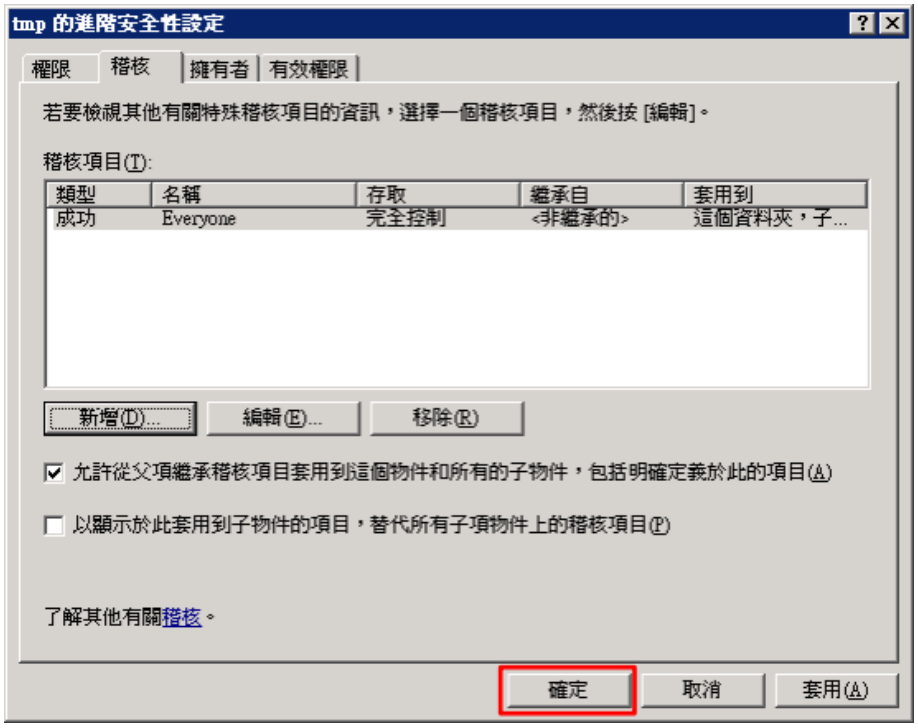
(4)　物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



(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

*以下分別為網域或工作群組設定方式。

4.1 網域

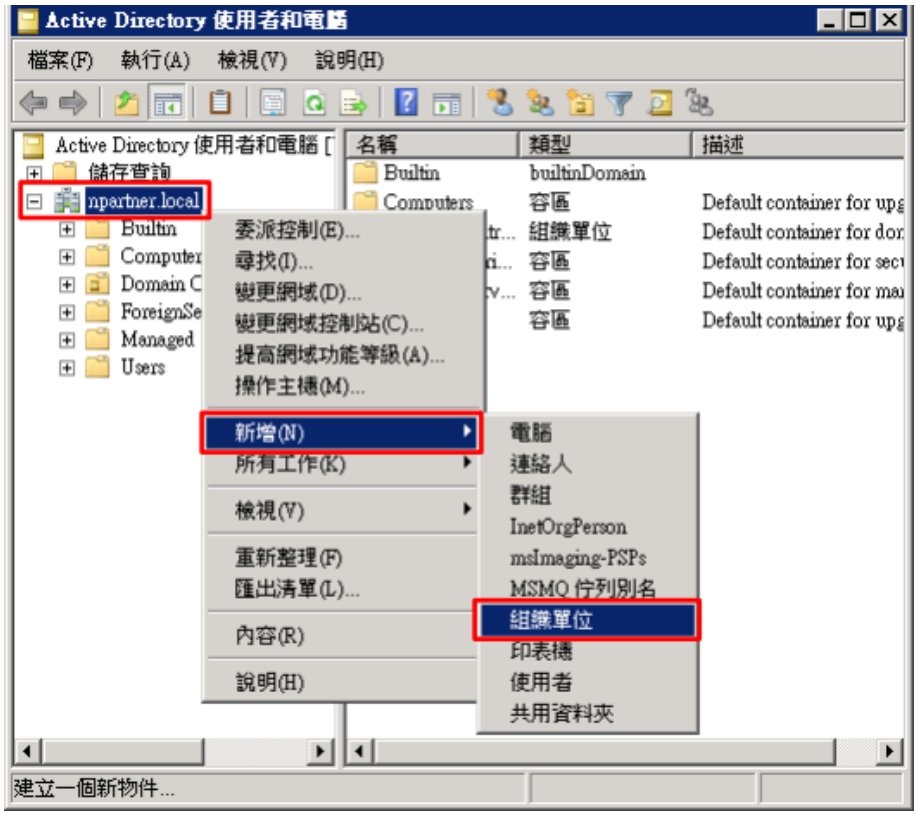
4.1.1 組織單位設定

(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]

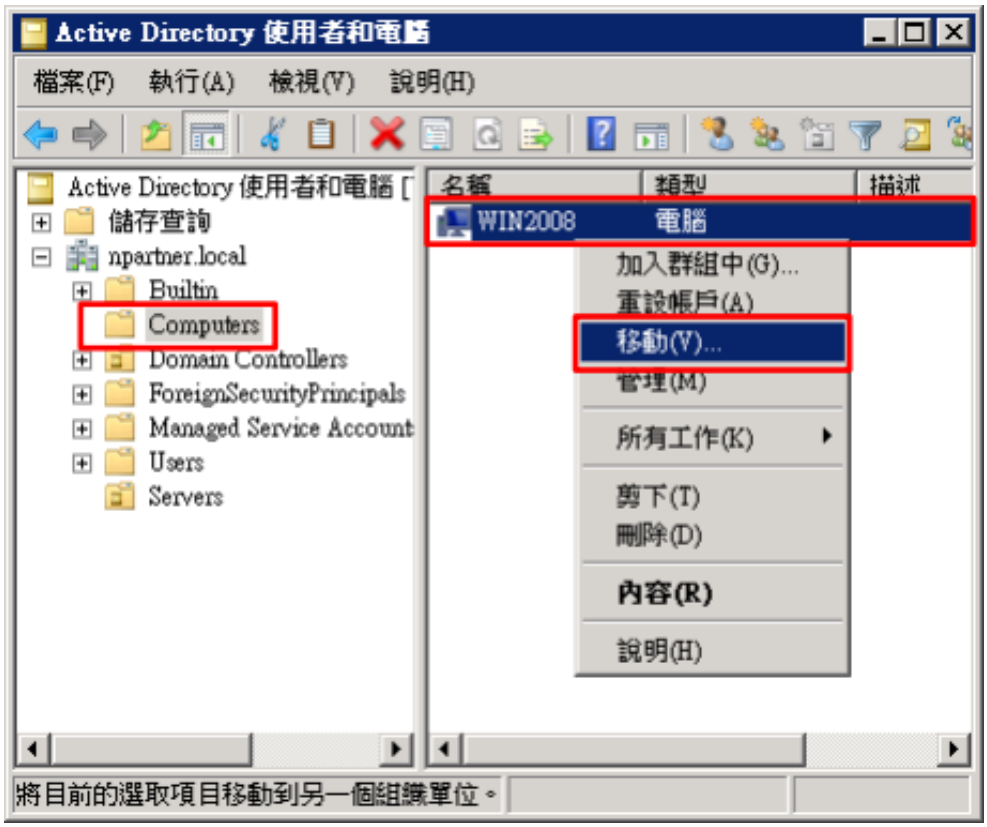


(3) 輸入組織單位名稱

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]

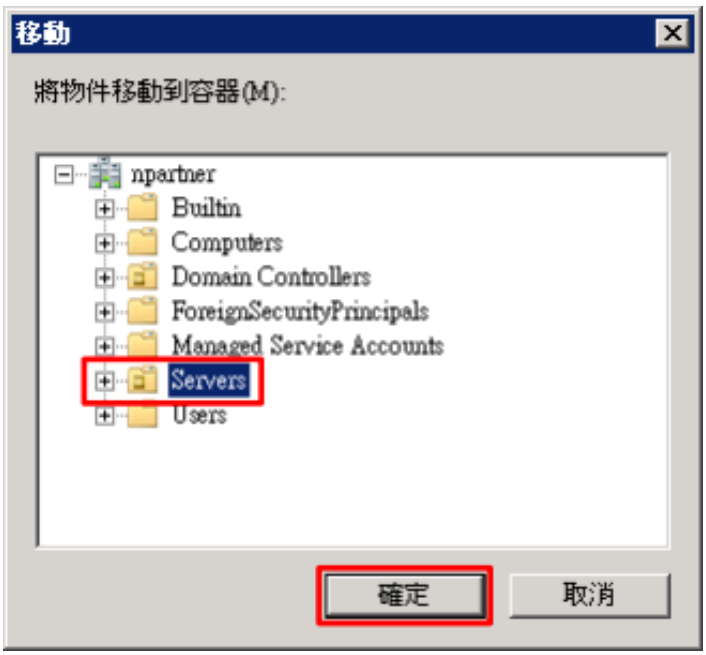
(4) 移動伺服器至新的組織單位

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 主機 -> 點選 [移動]



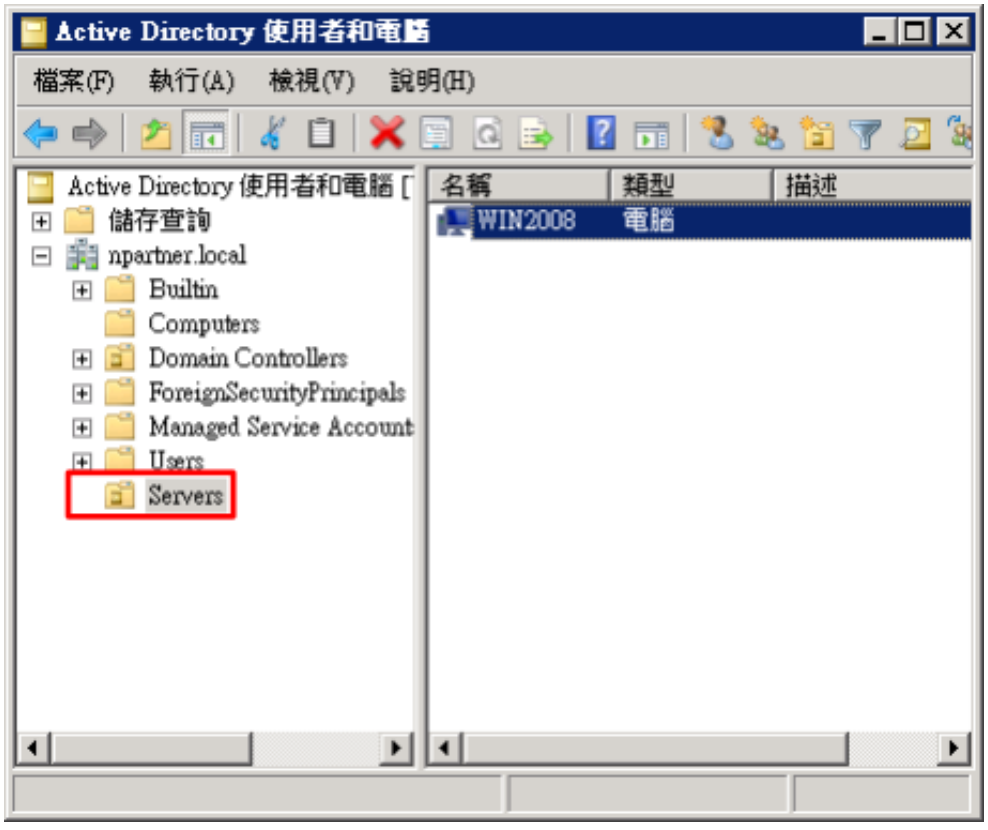
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認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。



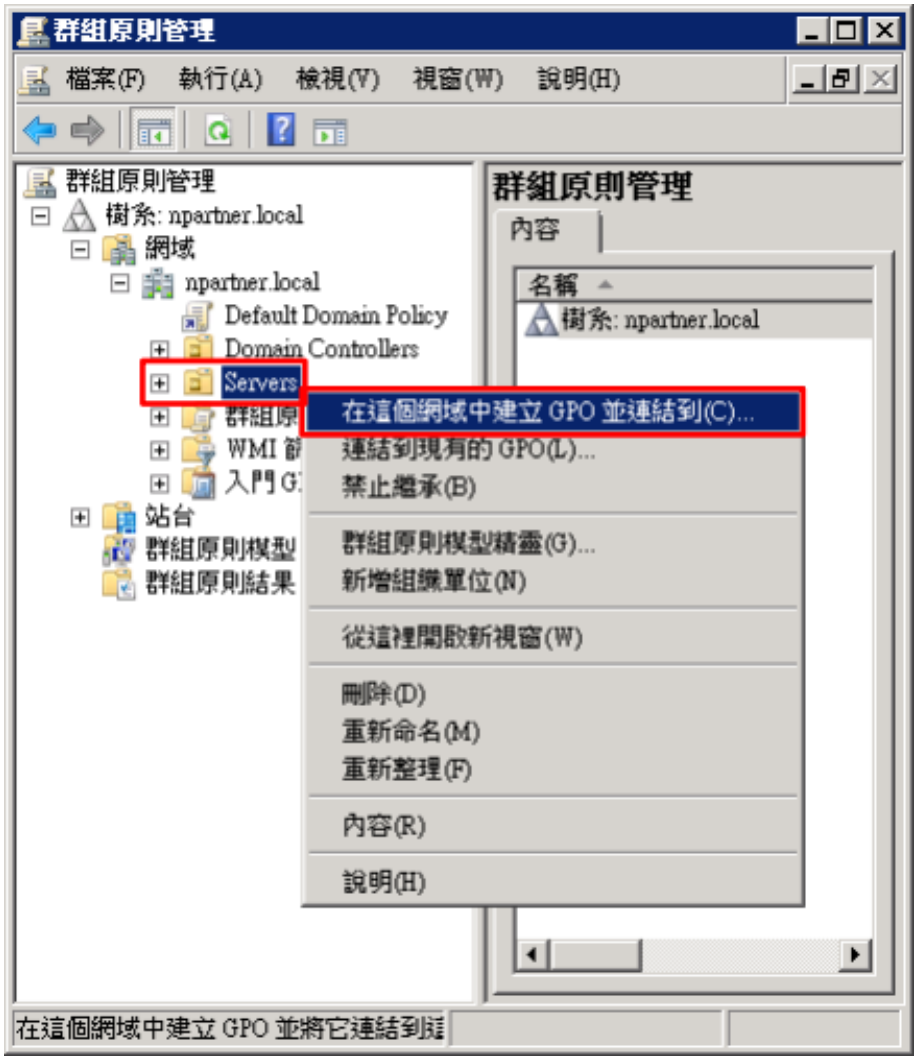
4.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

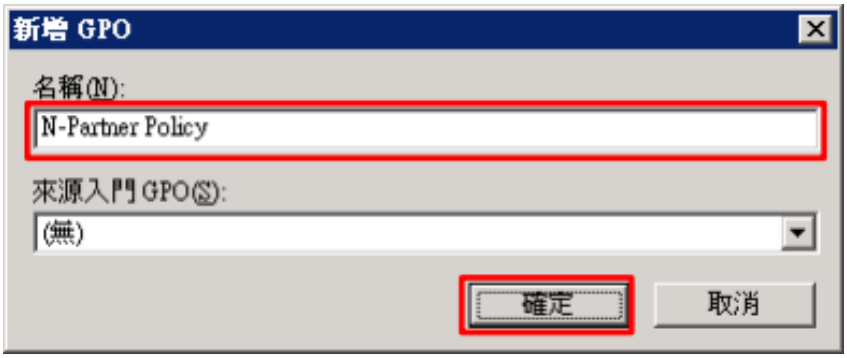
(2) 在 Servers 組織單位，新增群組原則物件

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...]



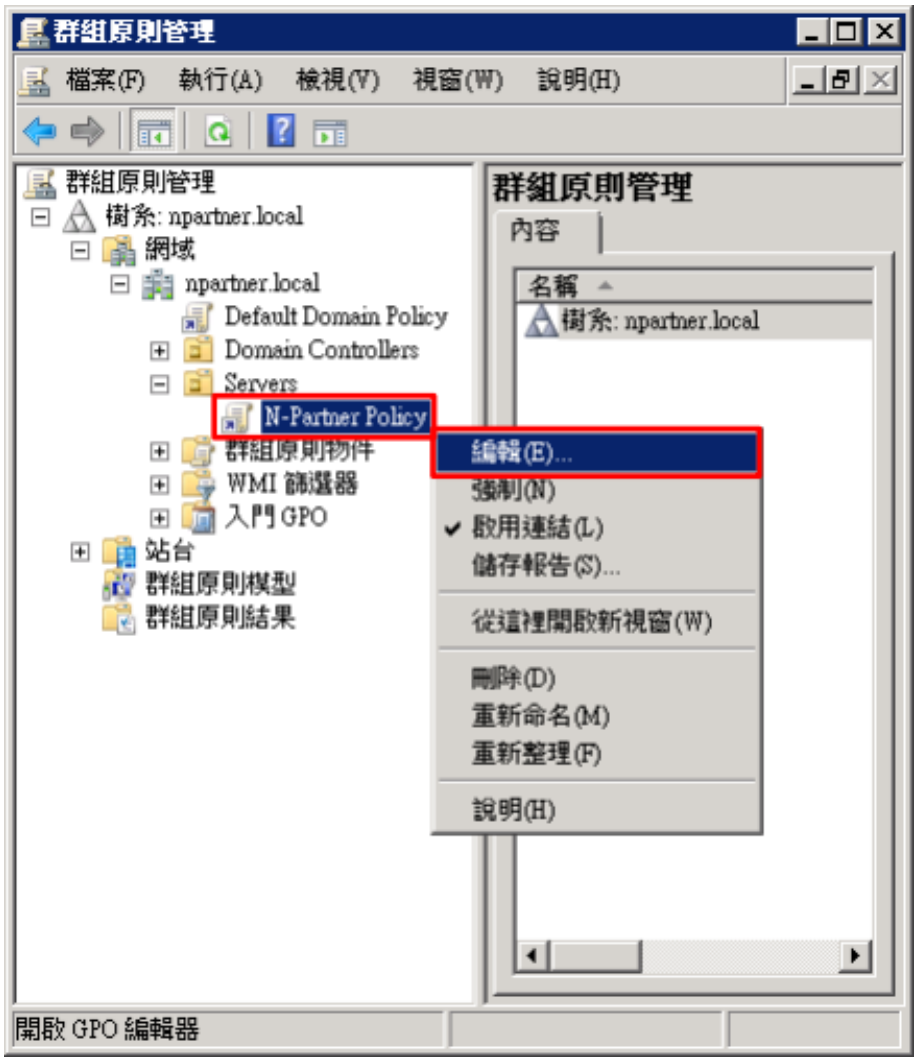
(3) 輸入群組原則物件名稱

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]



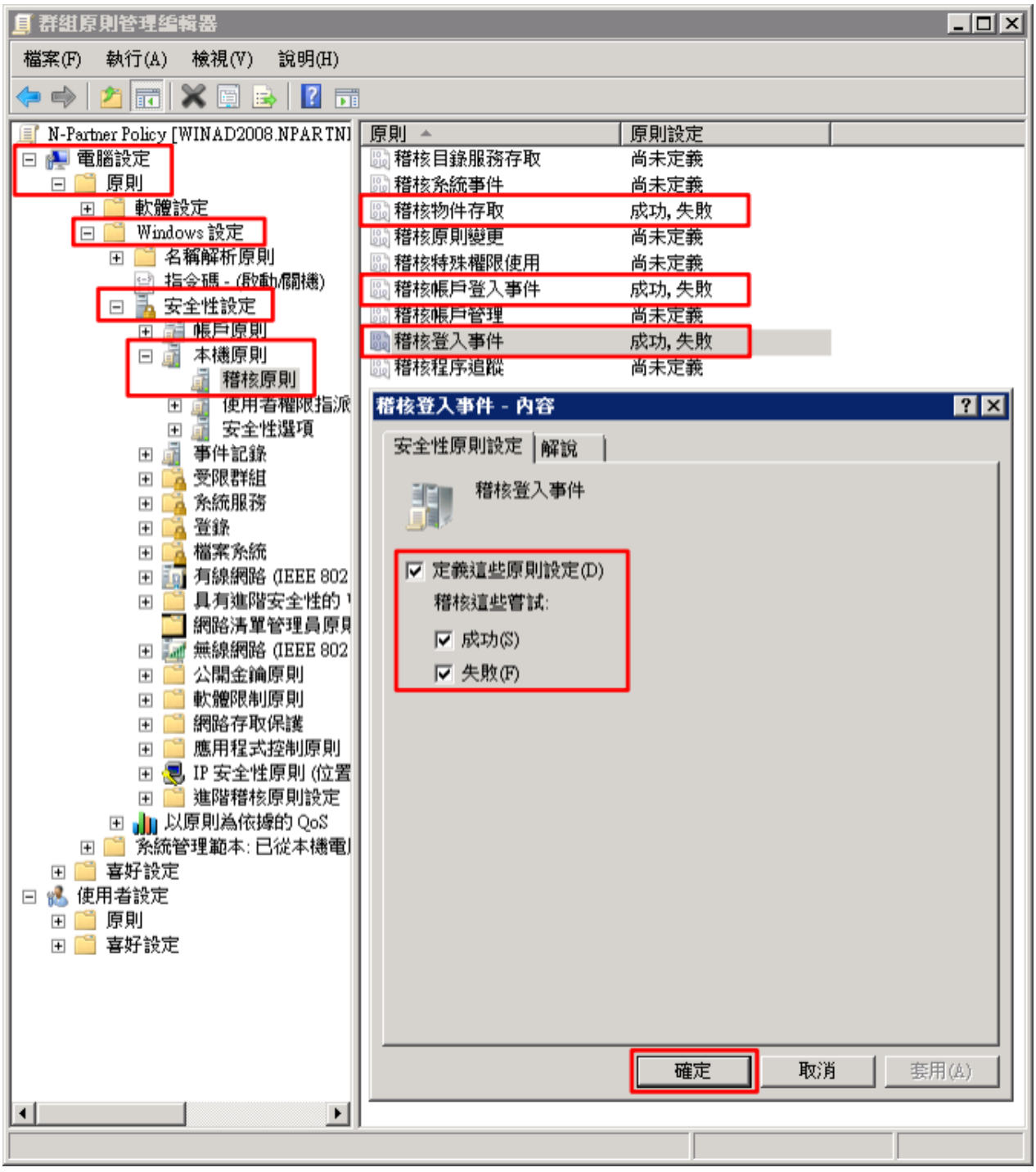
(4) 編輯群組原則物件

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



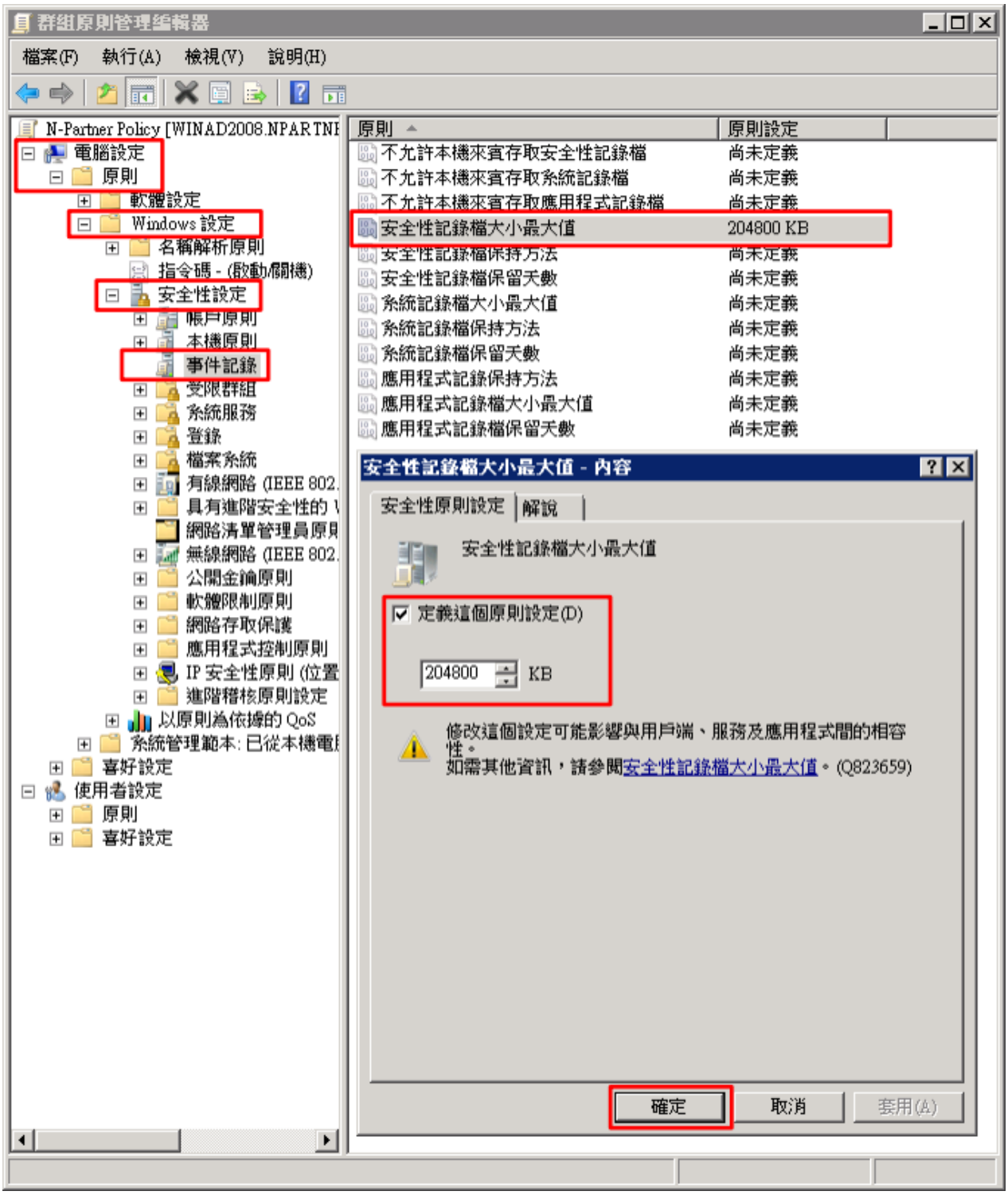
(5) 本機原則：稽核原則

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]



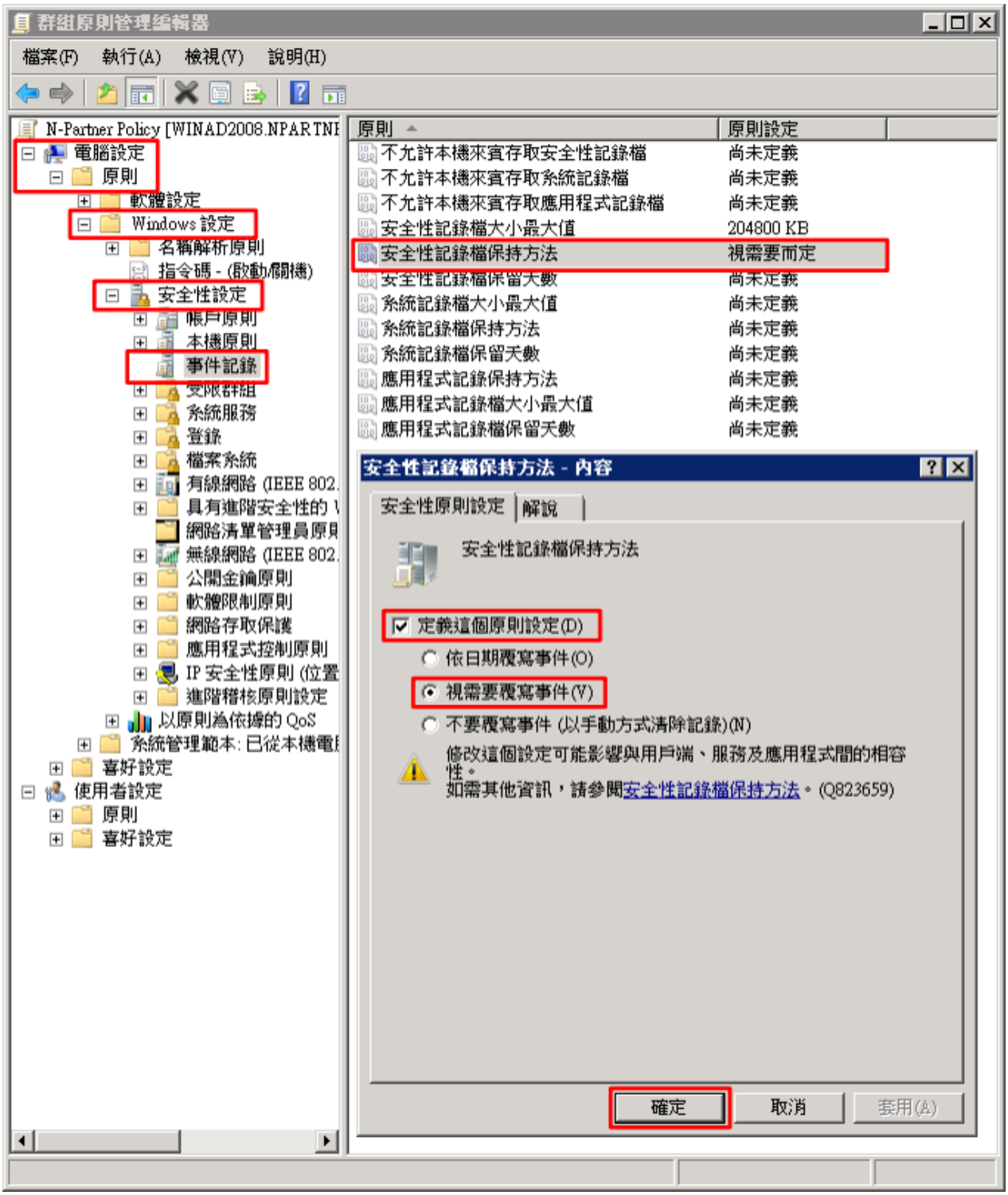
(6) 事件記錄檔：安全性記錄檔大小最大值

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]



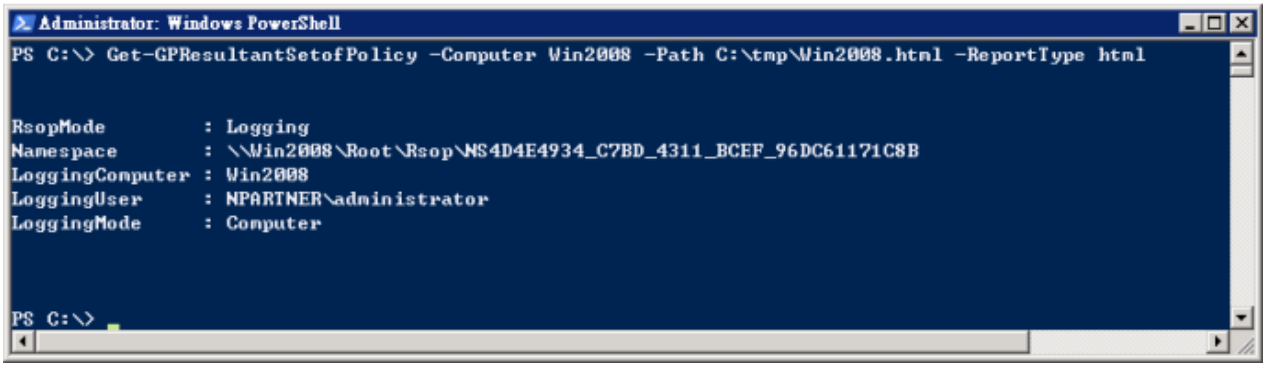
(8)　在 Windows File 伺服器 -> 開啟 [Windows PowerShell]

(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

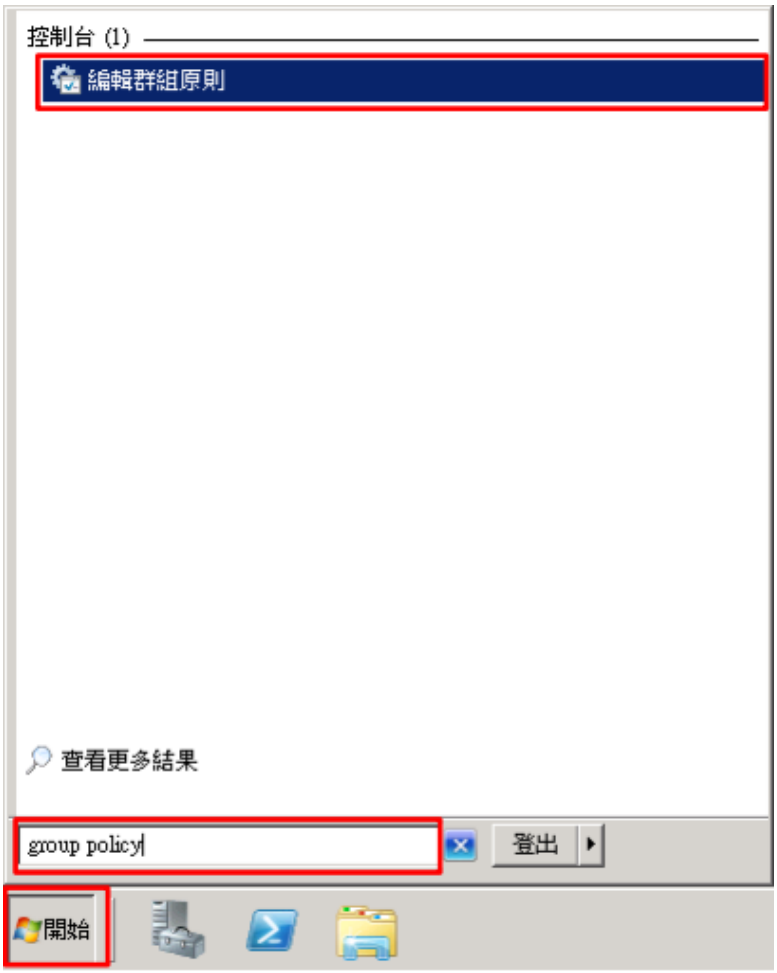
(11)　開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則

4.2 工作群組

4.2.1 稽核原則設定

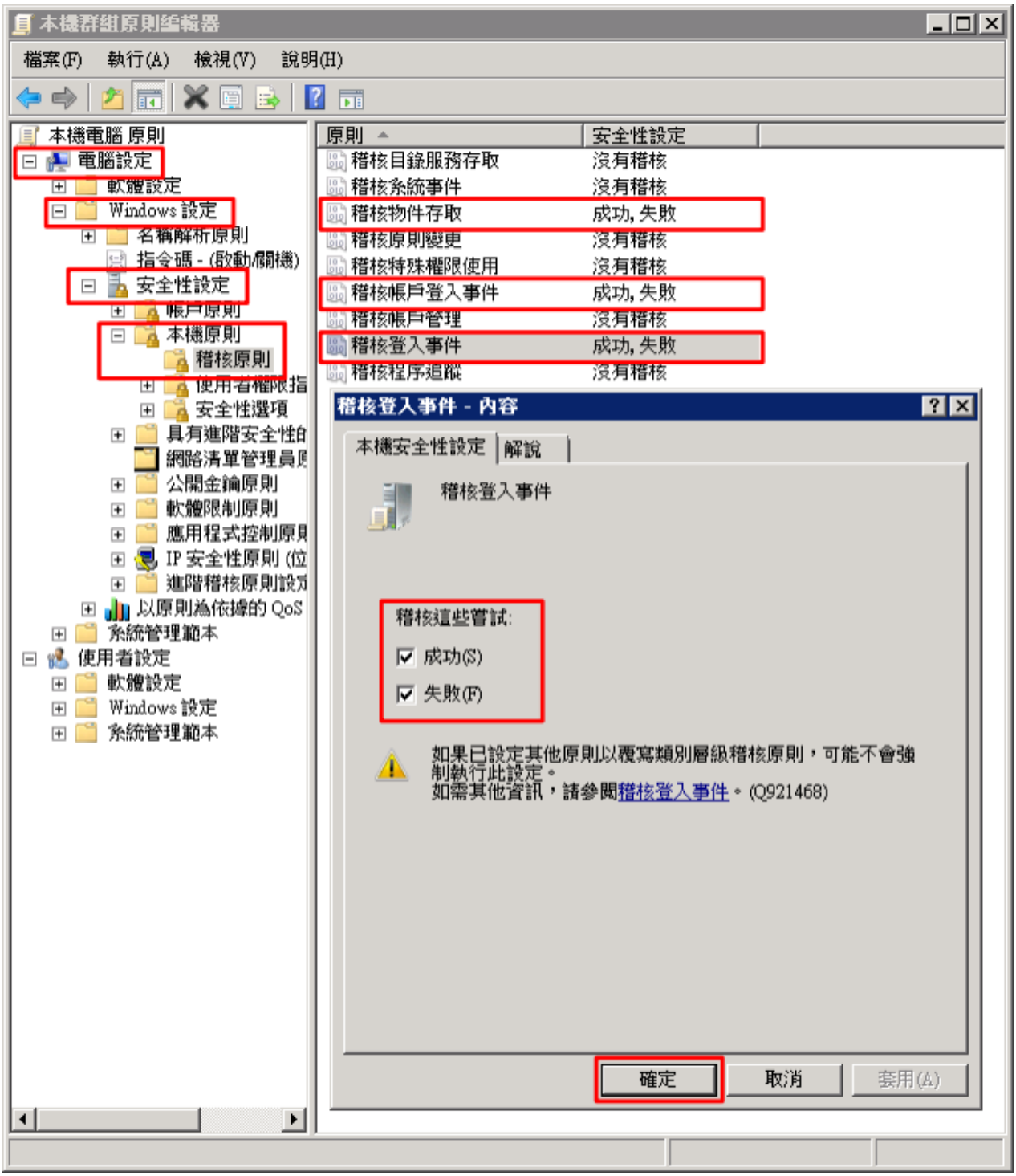
(1) 開啟 [本機群組原則編輯器]

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]



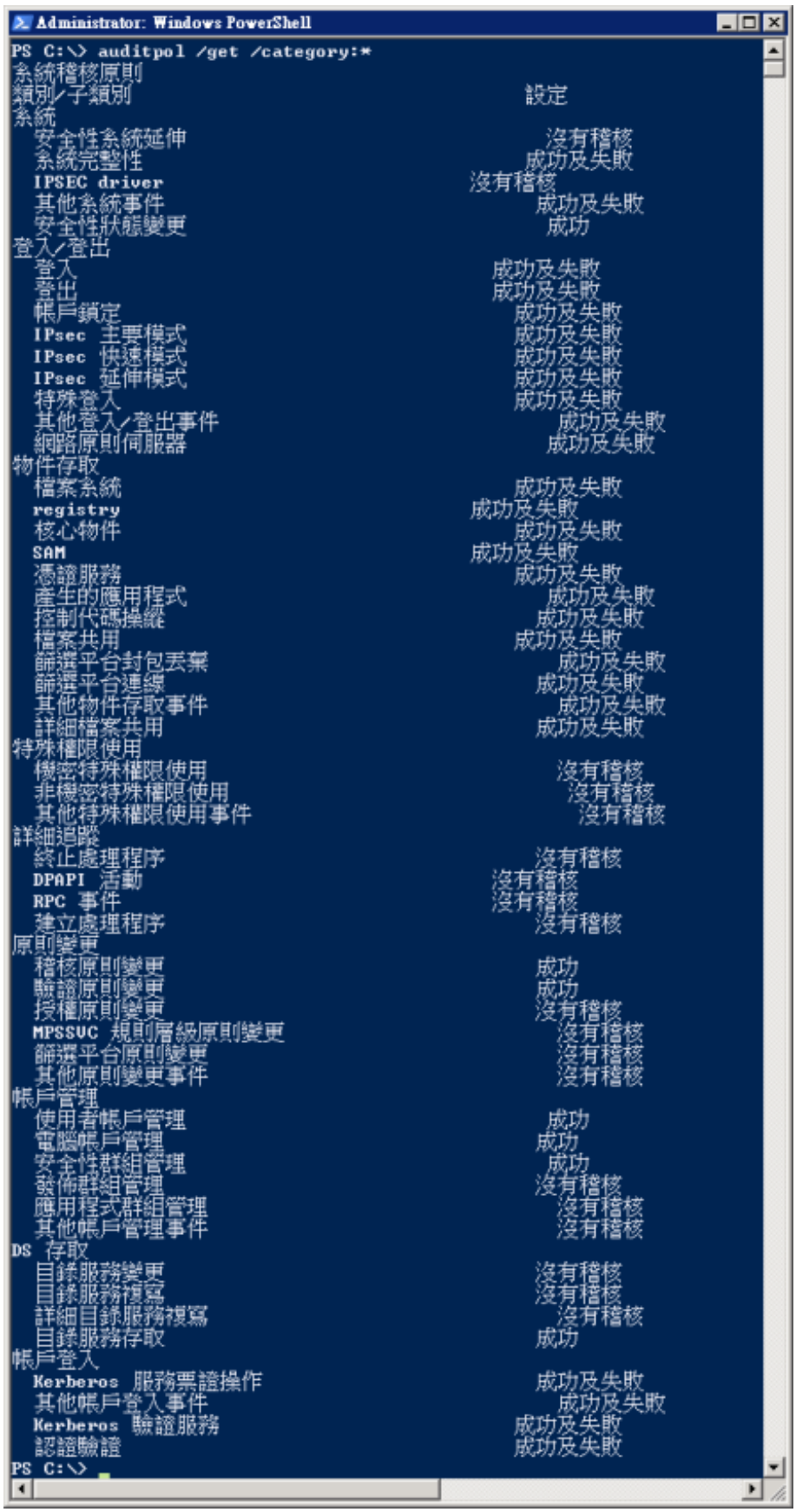
(3) 開啟 [Windows PowerShell]

(4) 更新群組原則

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

(5) 查看群組原則套用情形

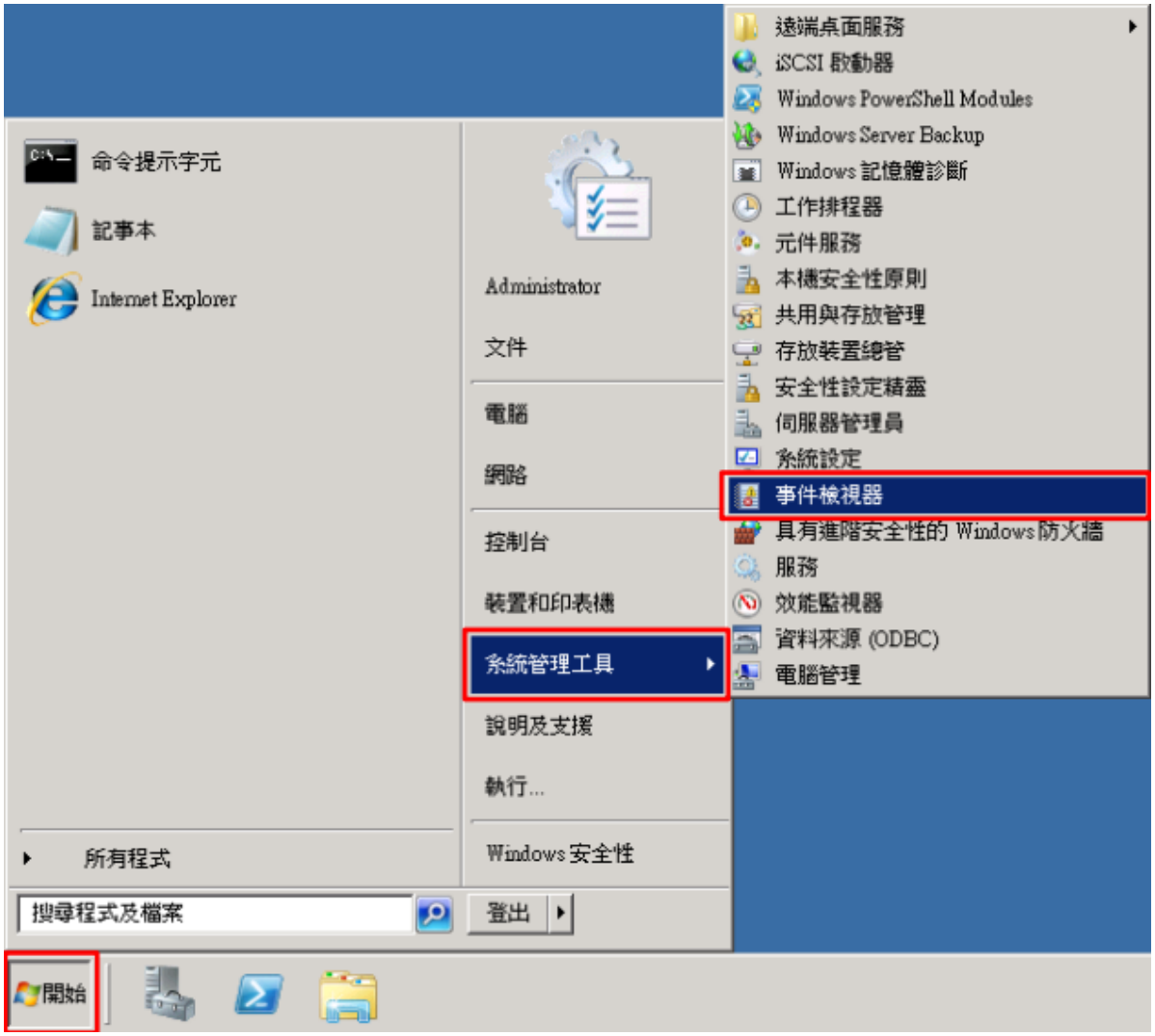
```
PS C:\> auditpol /get /category:*
```



4.2.2 事件檔案設定

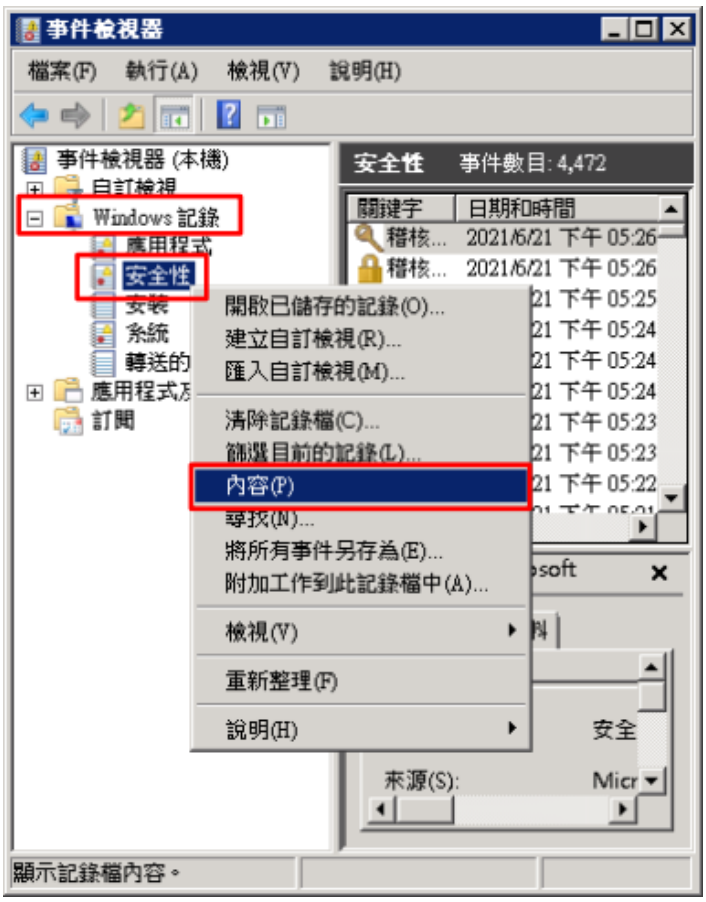
(1) 開啟事件檢視器

按 [開始] -> 點選 [系統管理工具] -> [事件檢視器]



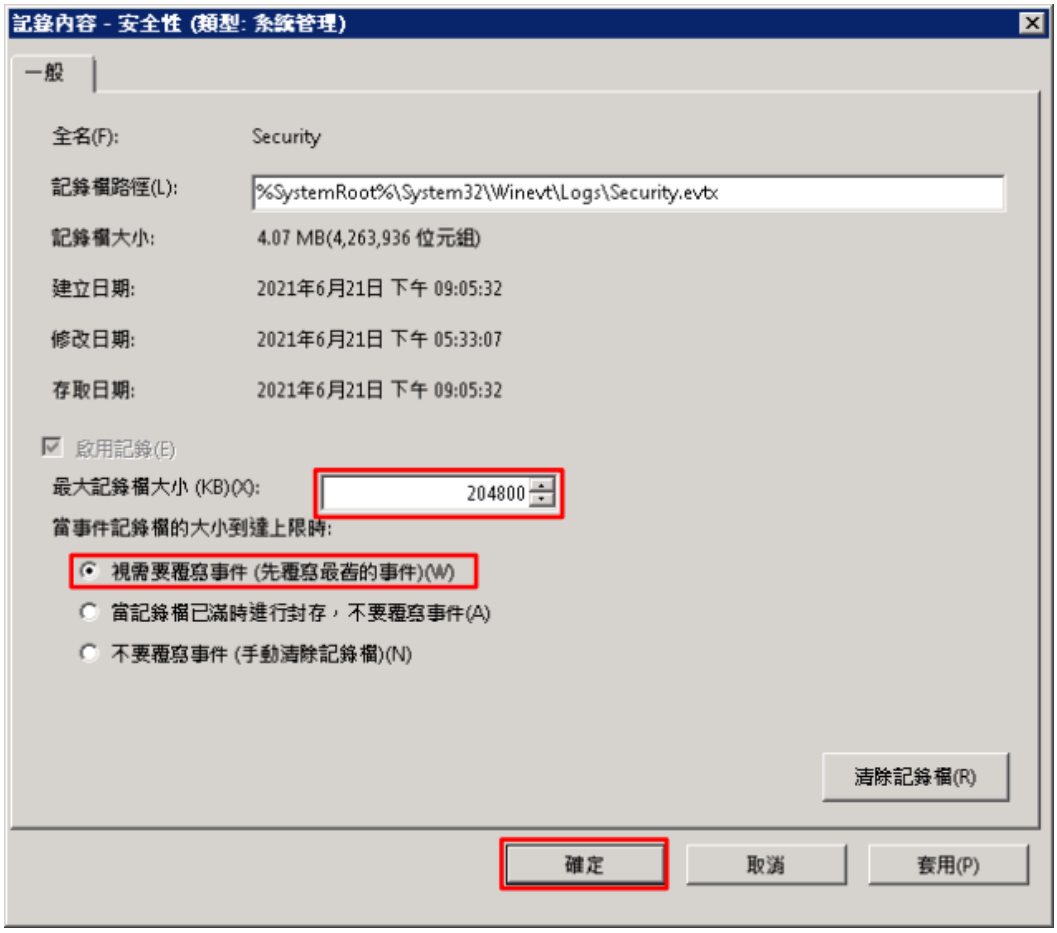
(2) 編輯安全性記錄

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



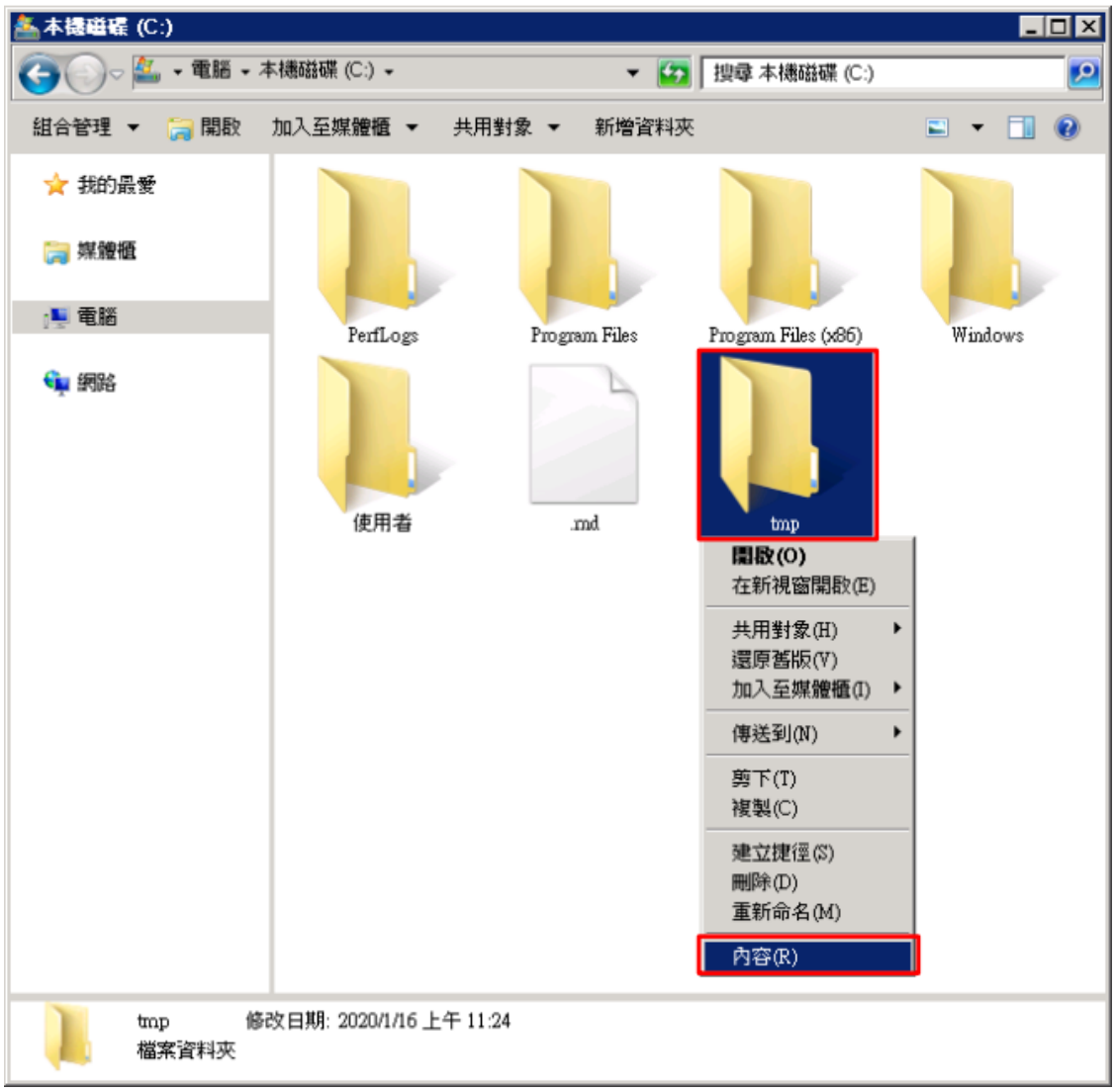
(3) 設定安全性記錄檔

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]

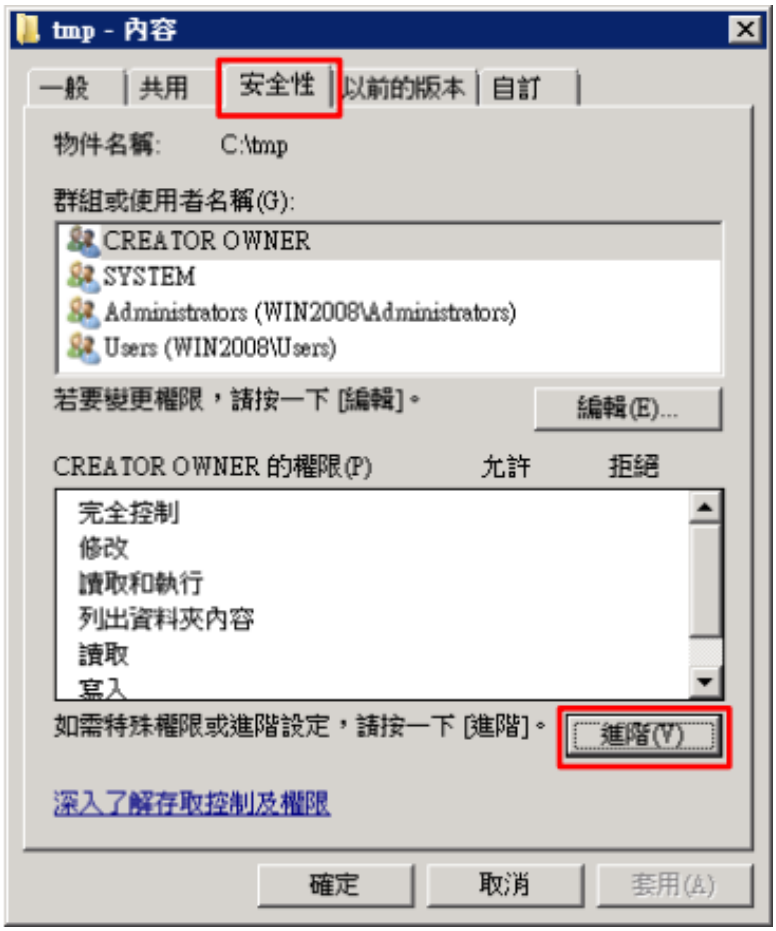


4.3 稽核資料夾設定

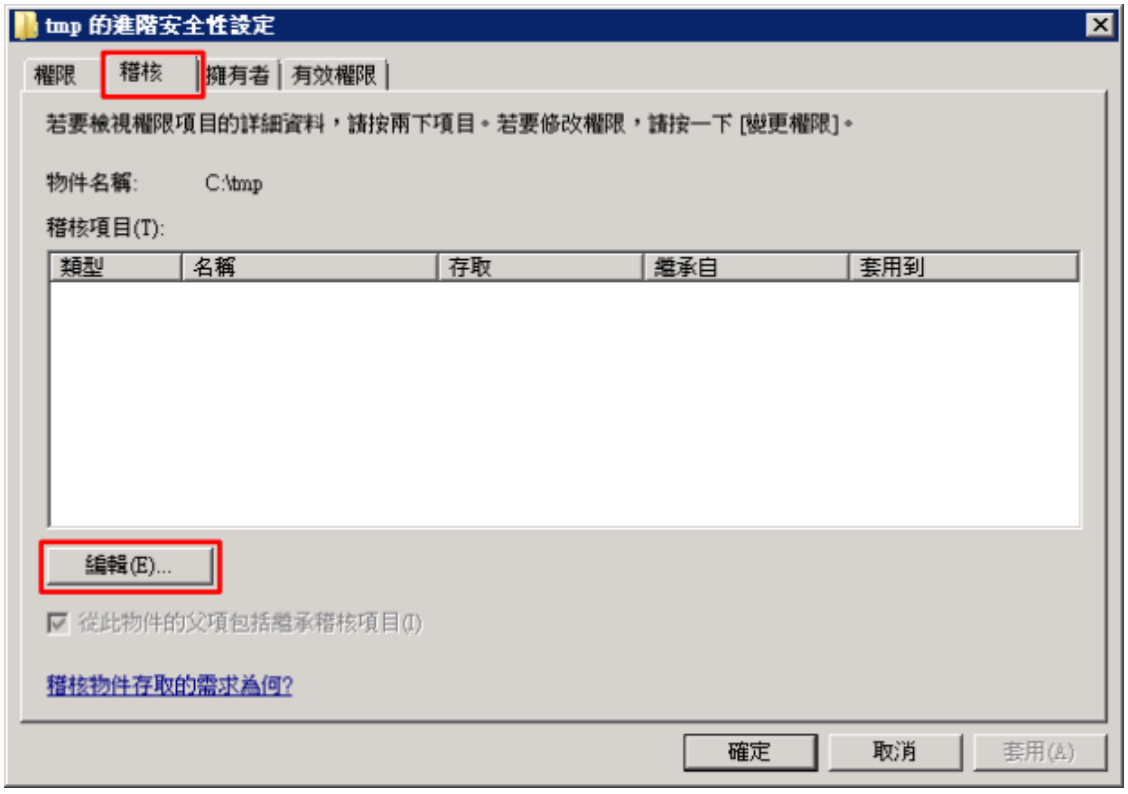
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



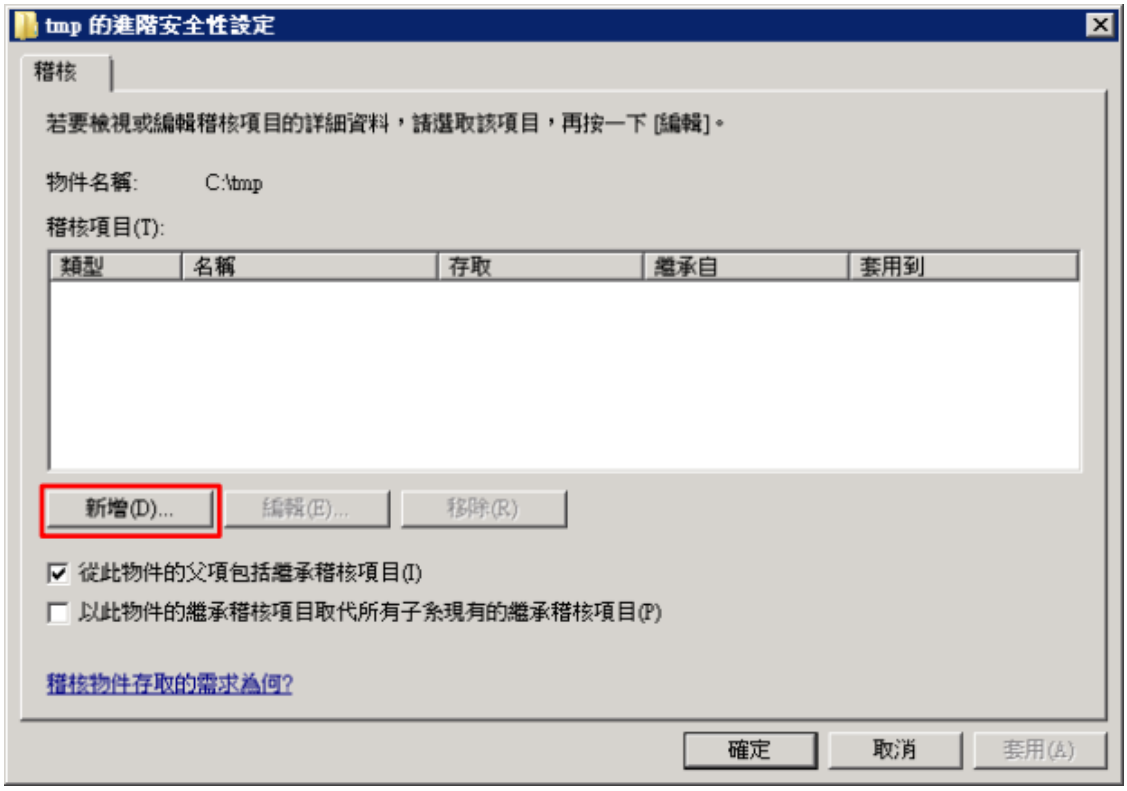
(2) 點選 [安全性] 頁面 -> 按 [進階]



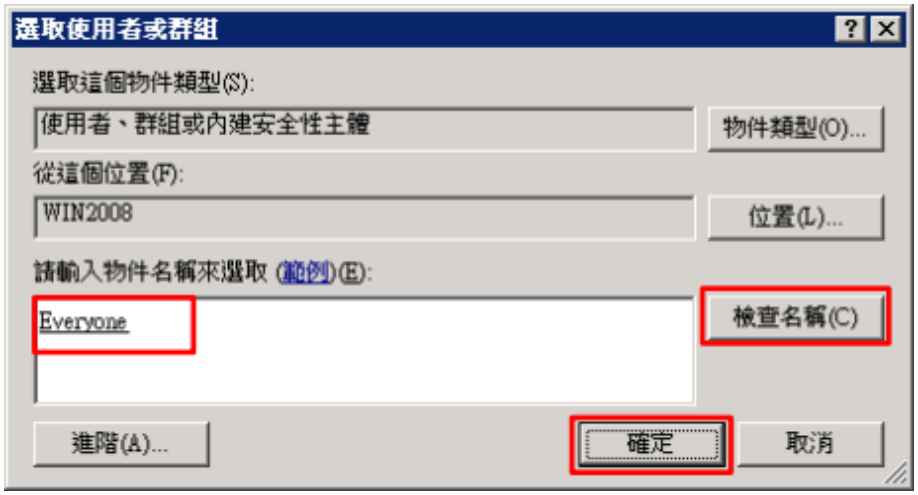
(3) 點選 [稽核] 頁面 -> 按 [新增]



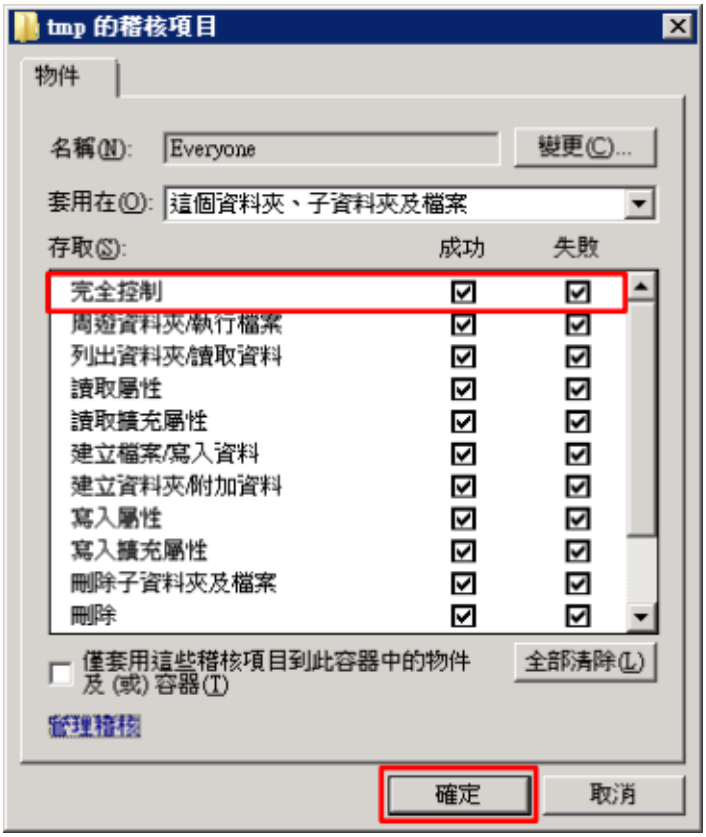
(4) 按 [新增]



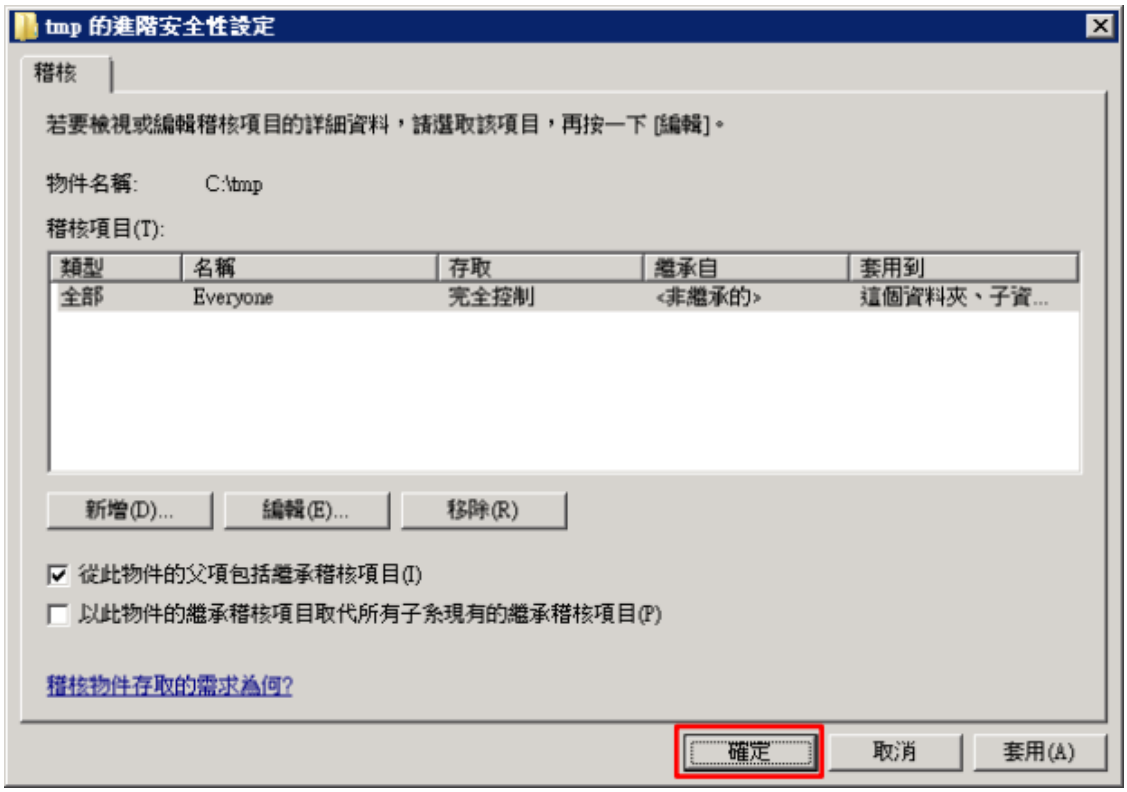
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



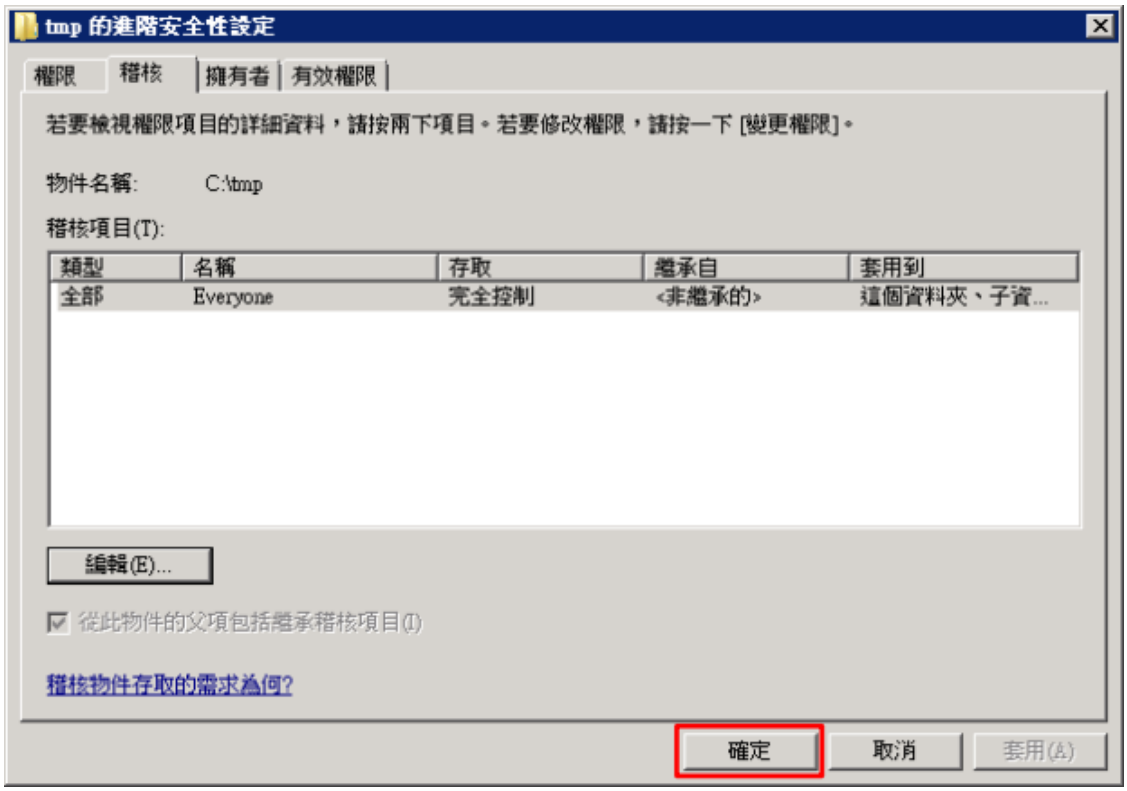
(6)　存取類型 [成功] 和 [失敗] 項目都勾選 [完全控制] -> 按 [確定]



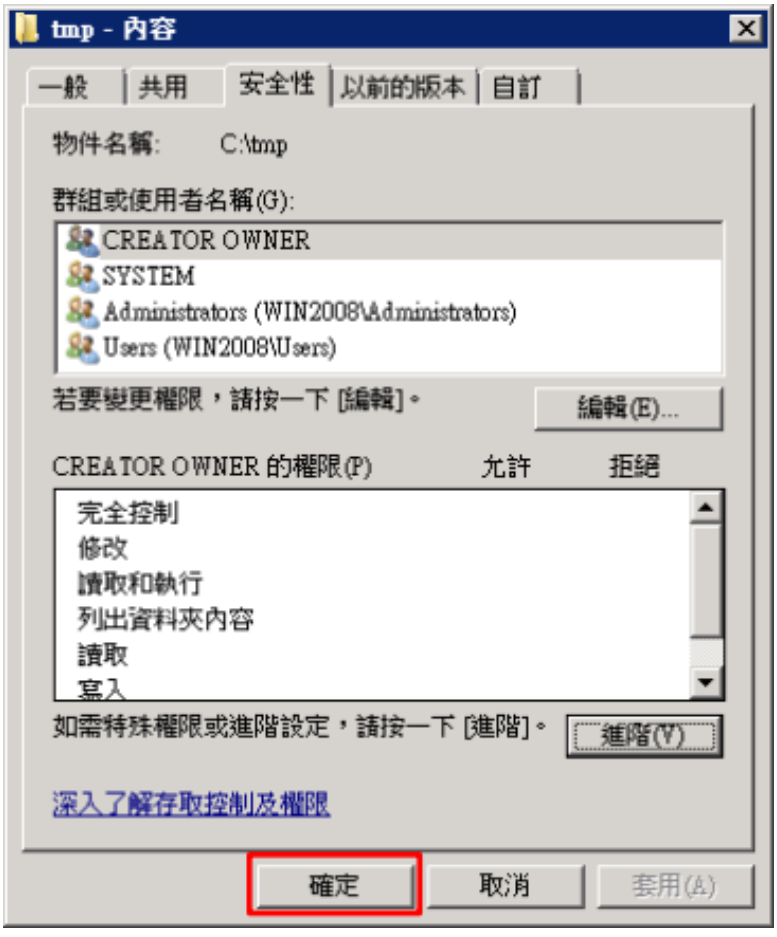
(7)　稽核項目顯示 Everyone 名稱 -> 按 [確定]



(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

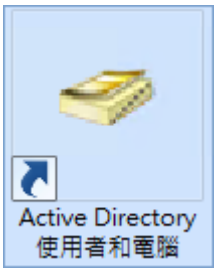
*以下分別為網域或工作群組設定方式。

5.1 網域

5.1.1 組織單位設定

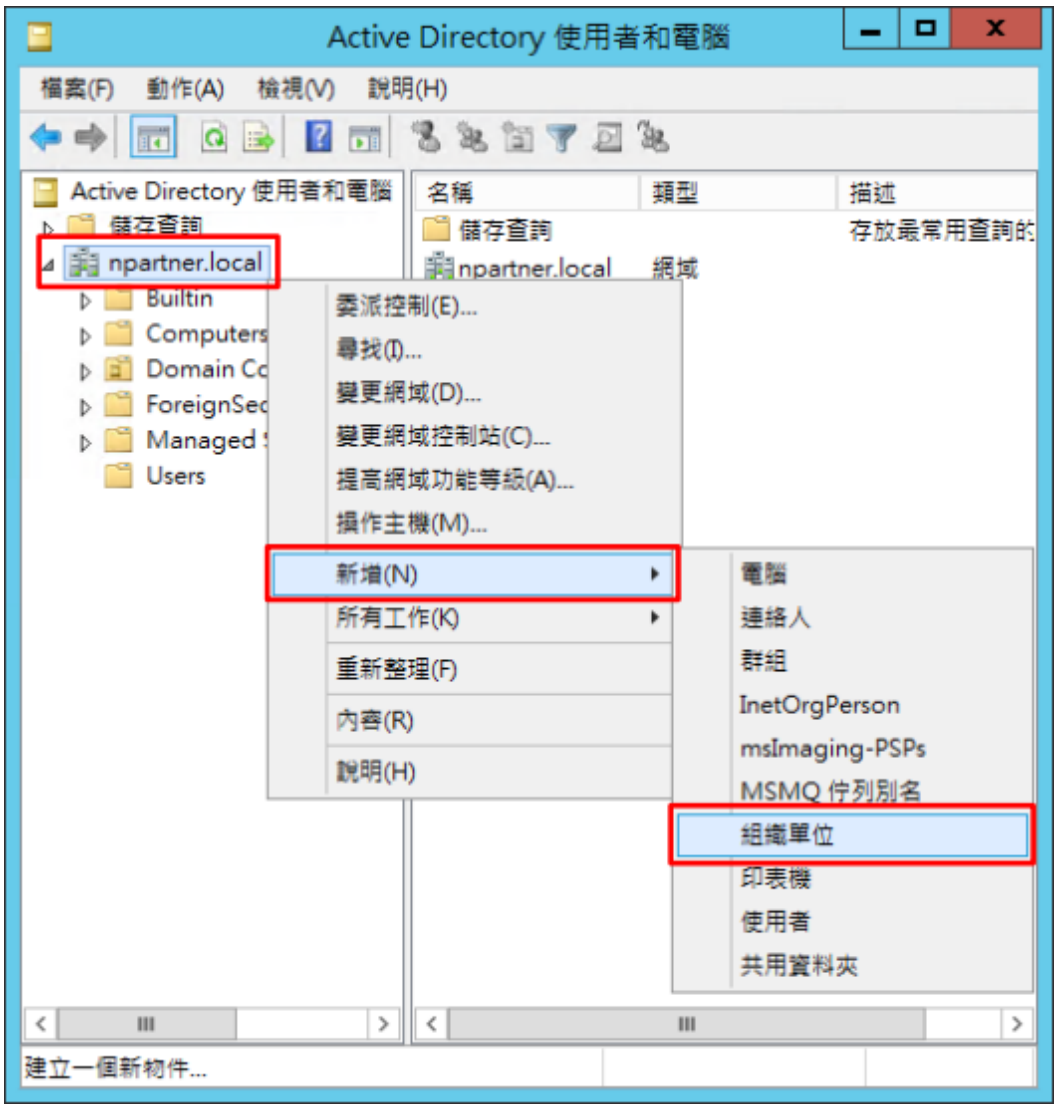
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



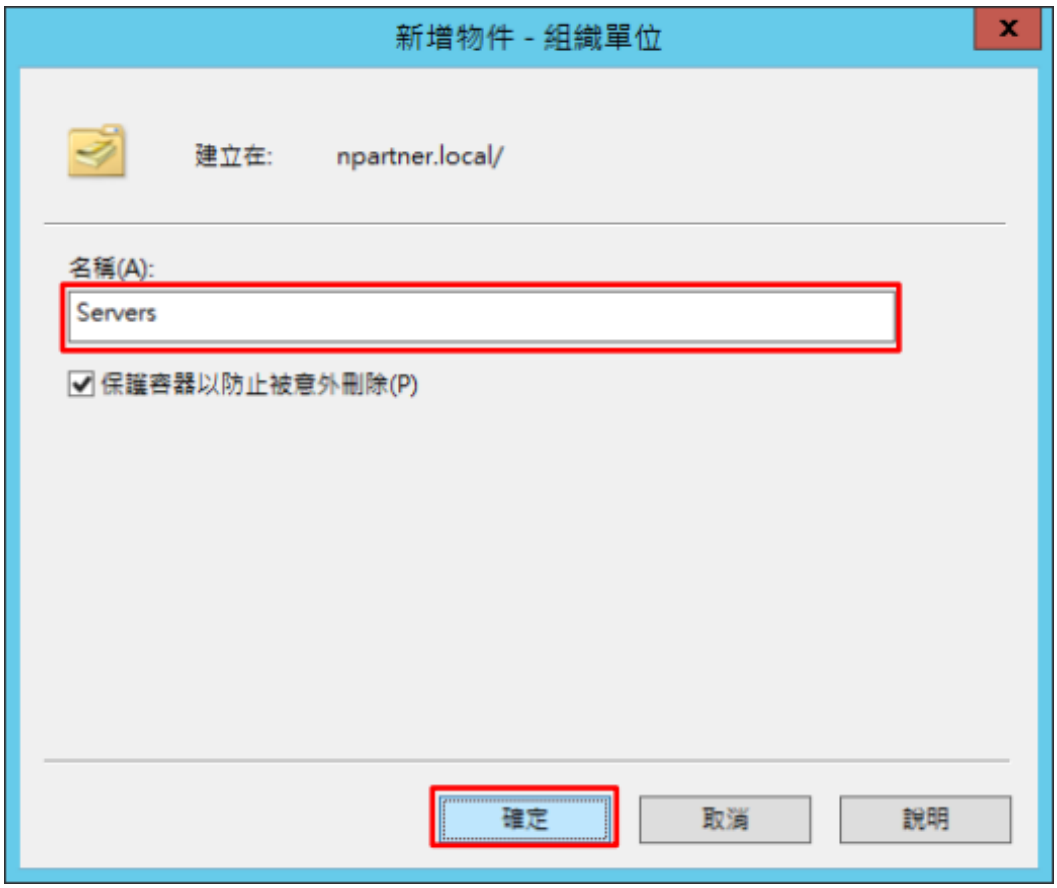
(2) 新增組織單位

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



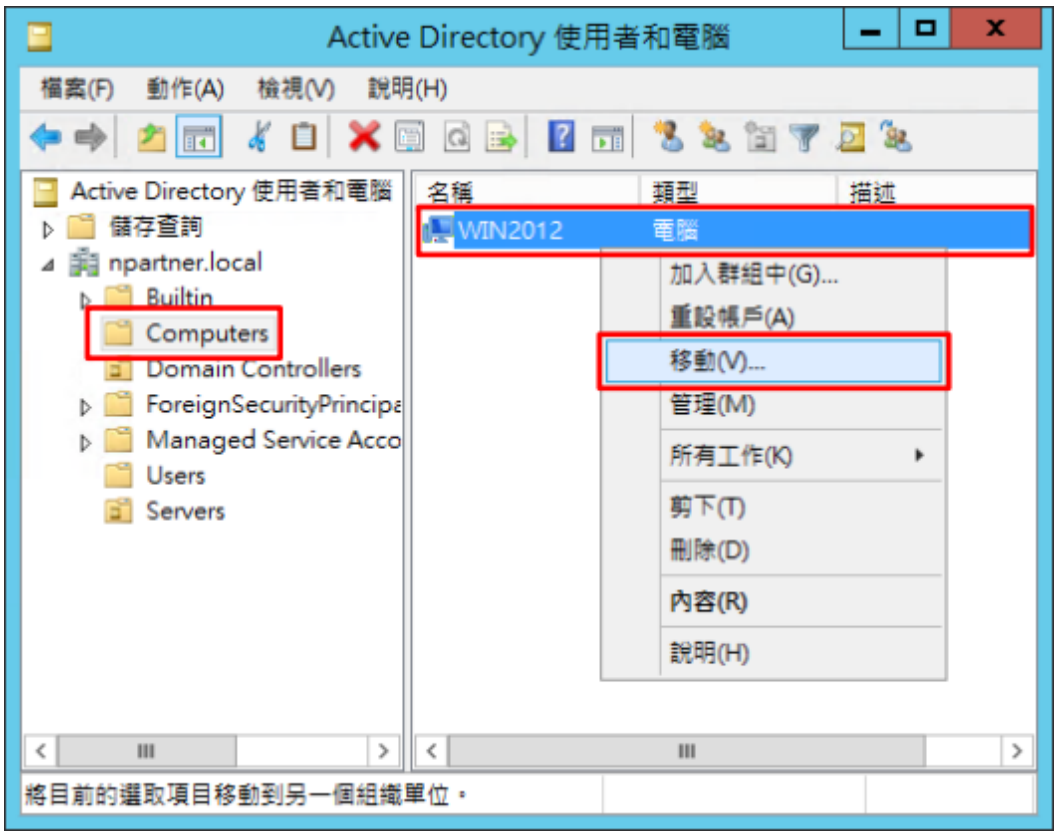
(3)　輸入組織單位名稱

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]



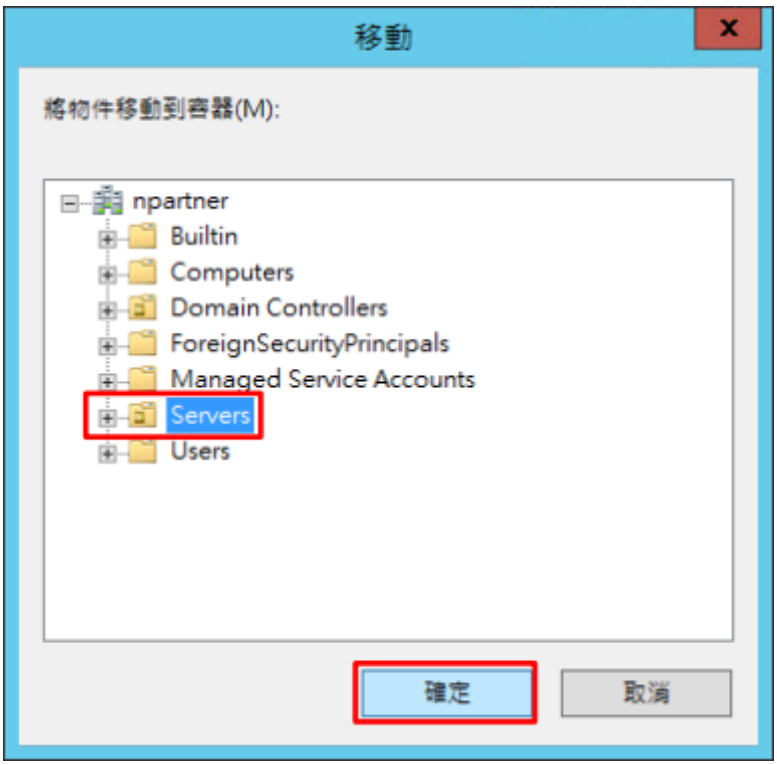
(4) 移動伺服器至新的組織單位

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 主機 -> 點選 [移動]



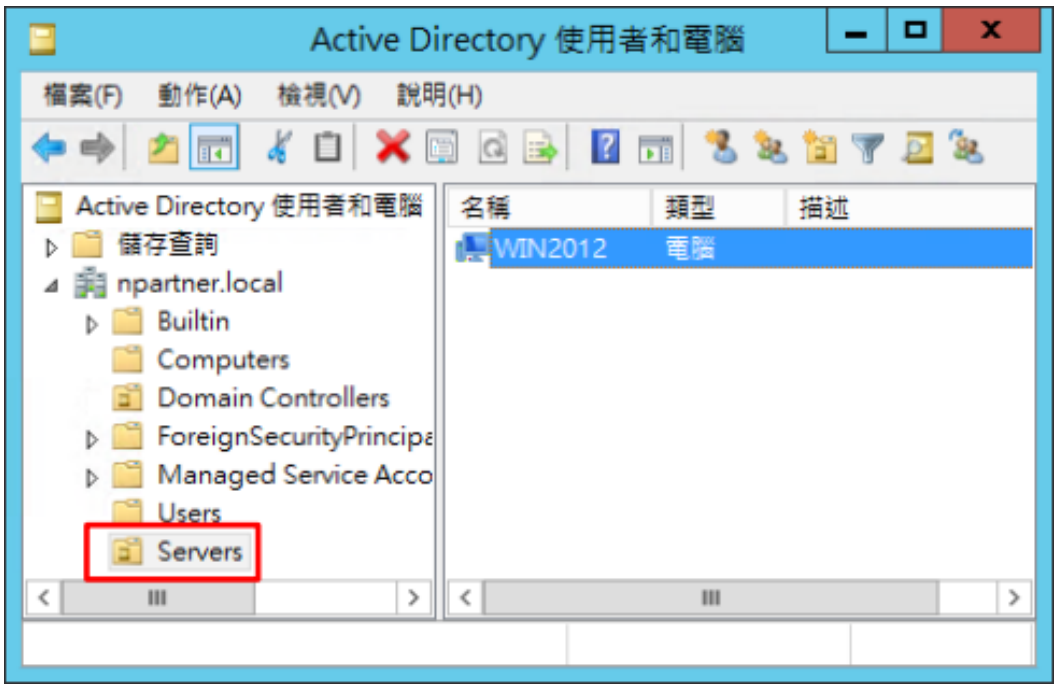
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

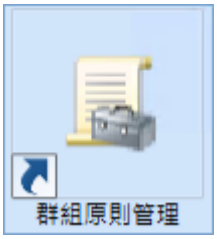
點選 [Servers] 組織單位，確認 Win2012 File 伺服器已移動。



5.1.2 群組原則設定

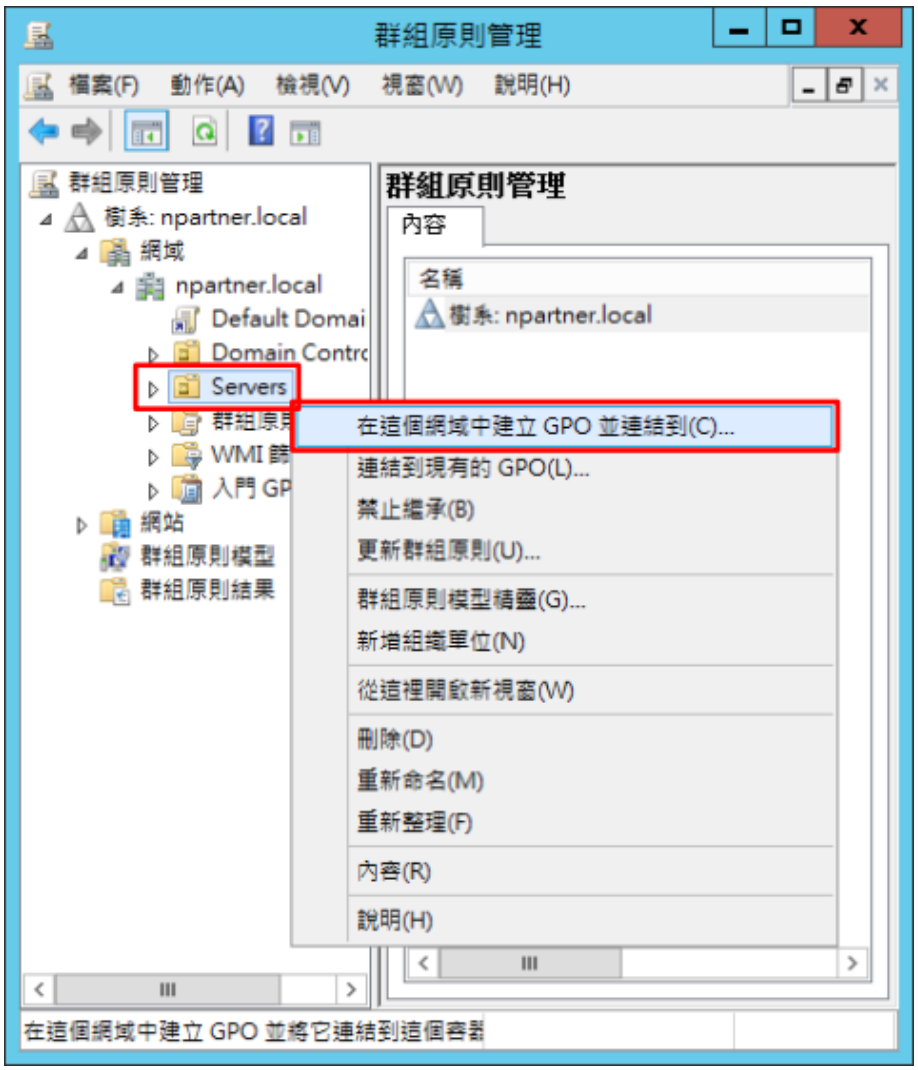
(1) 開啟群組原則管理

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...]

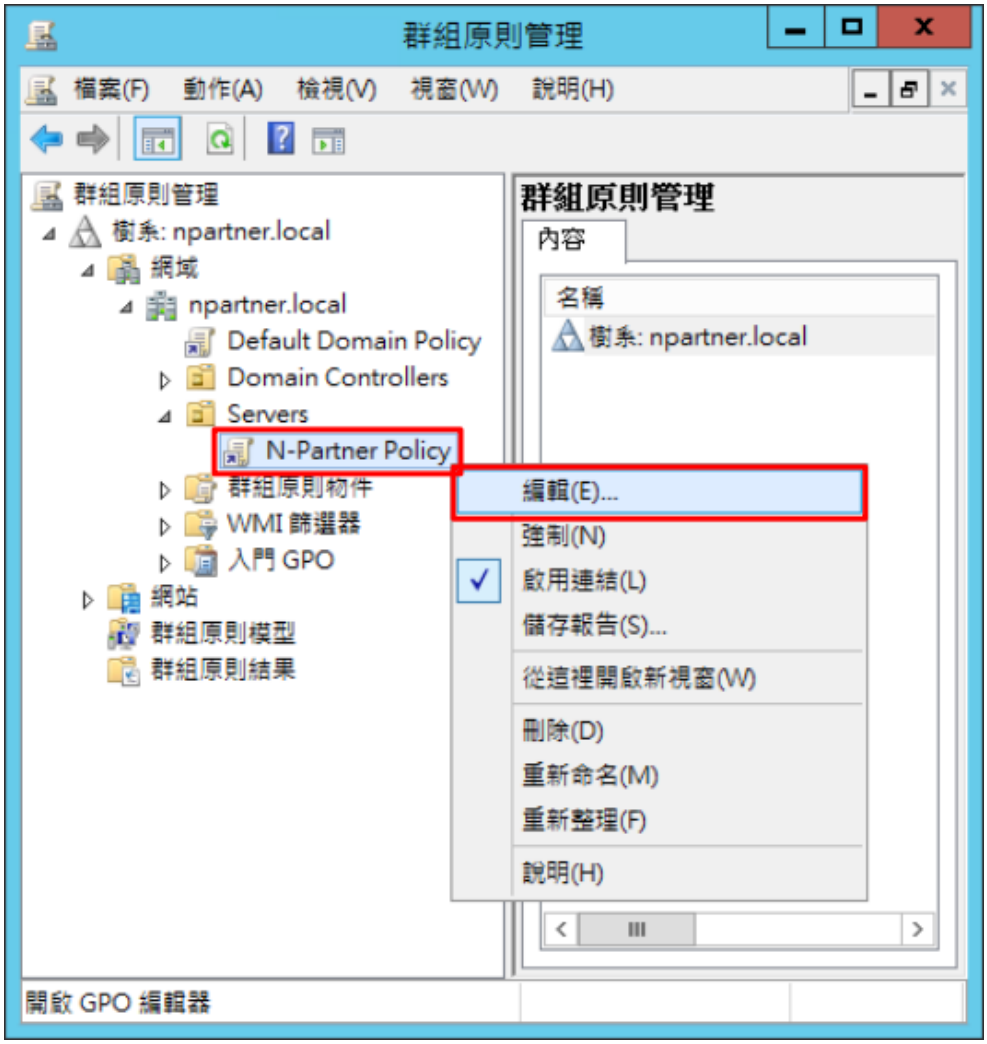


(3) 輸入群組原則物件名稱

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]

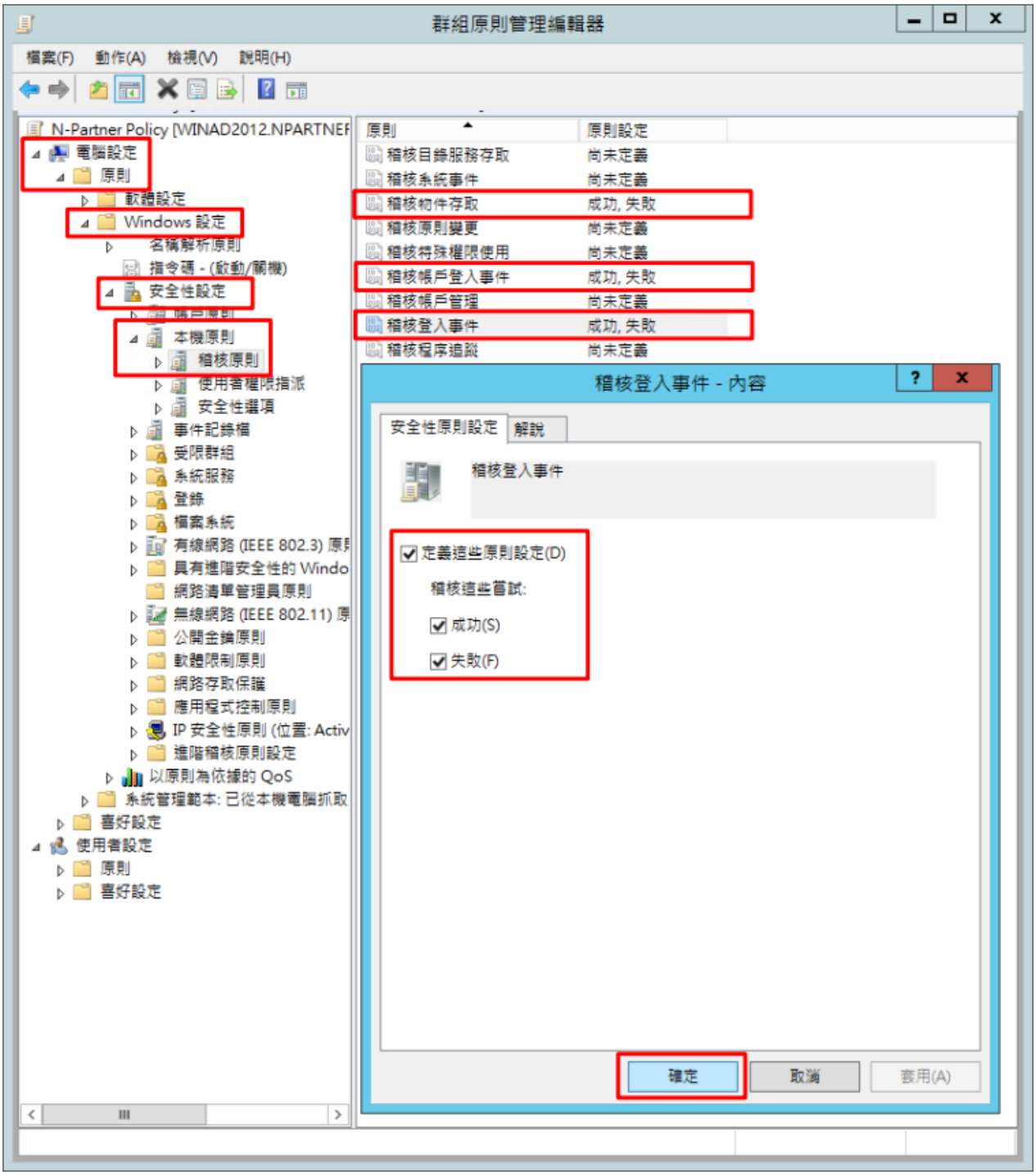
(4) 編輯群組原則物件

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



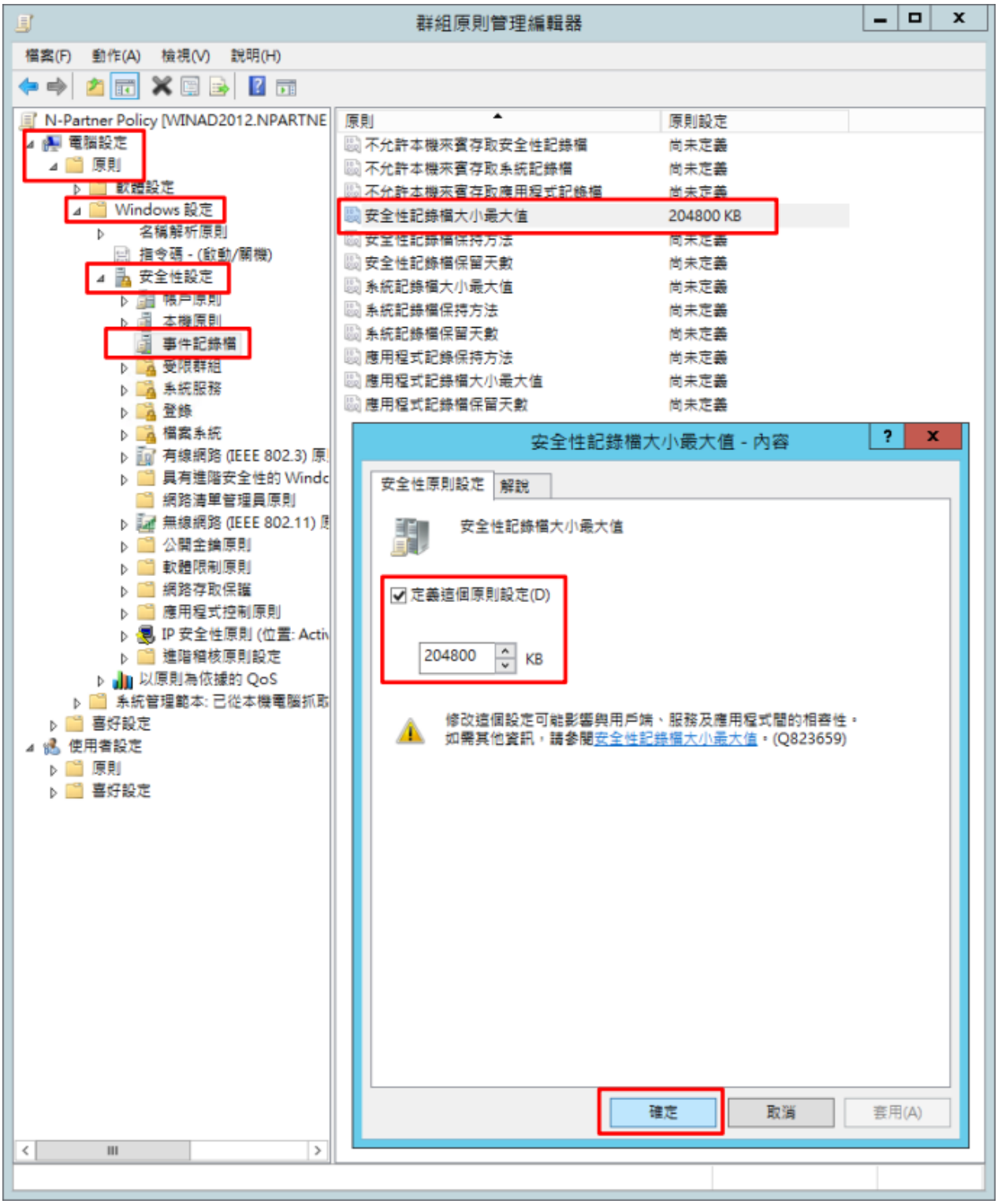
(5) 本機原則：稽核原則

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]



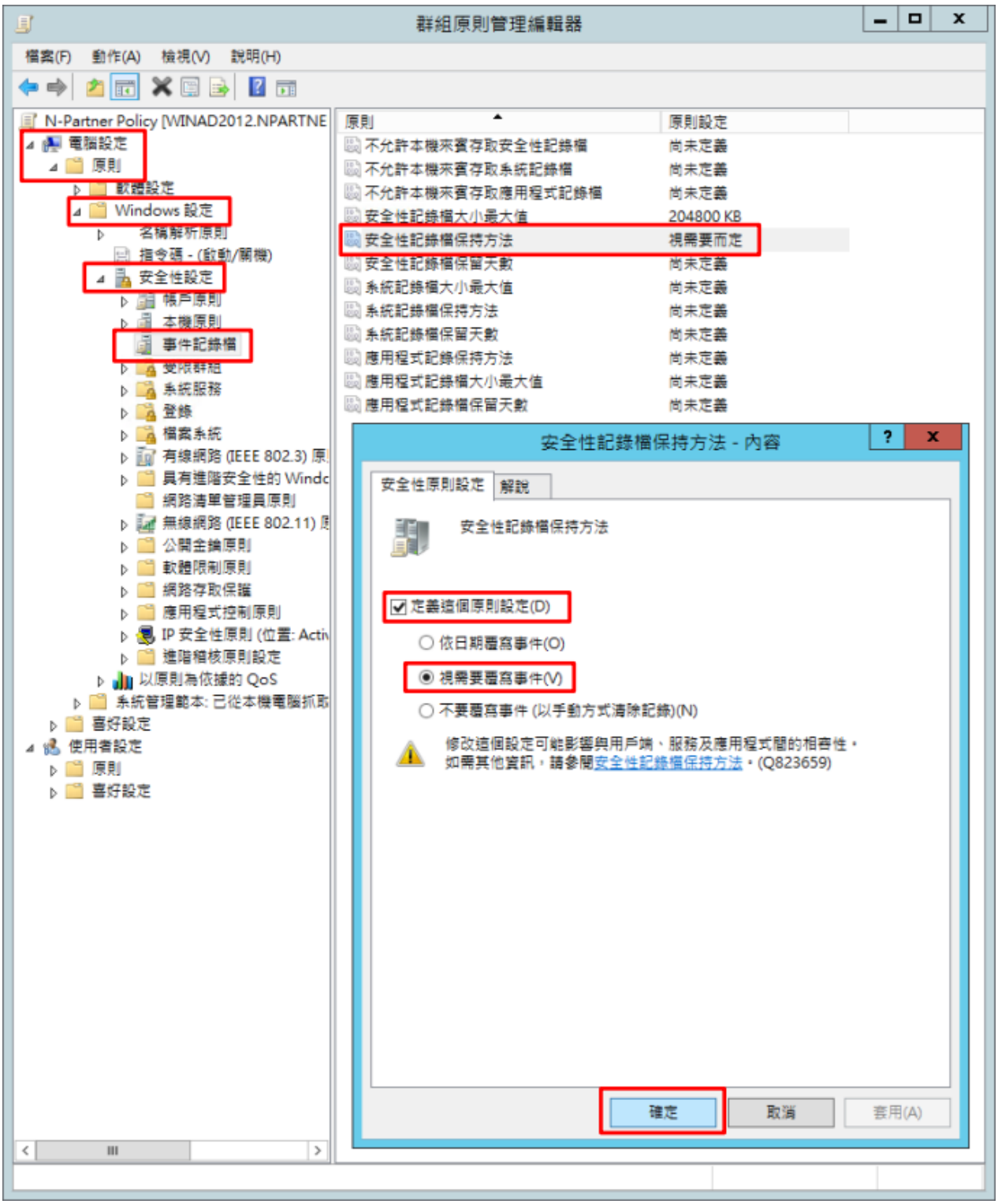
(6)　事件記錄檔：安全性記錄檔大小最大值

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]

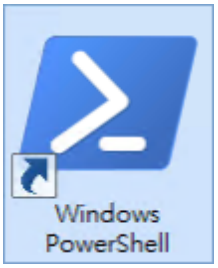


(7) 事件記錄檔：安全性記錄檔保持方法

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]

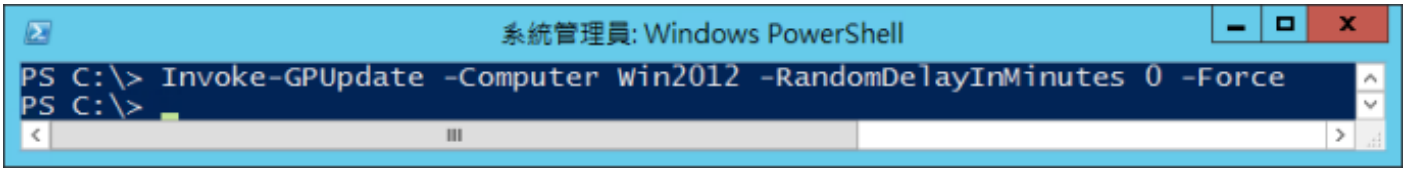


(8) 在 Windows File 伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows File 伺服器群組原則

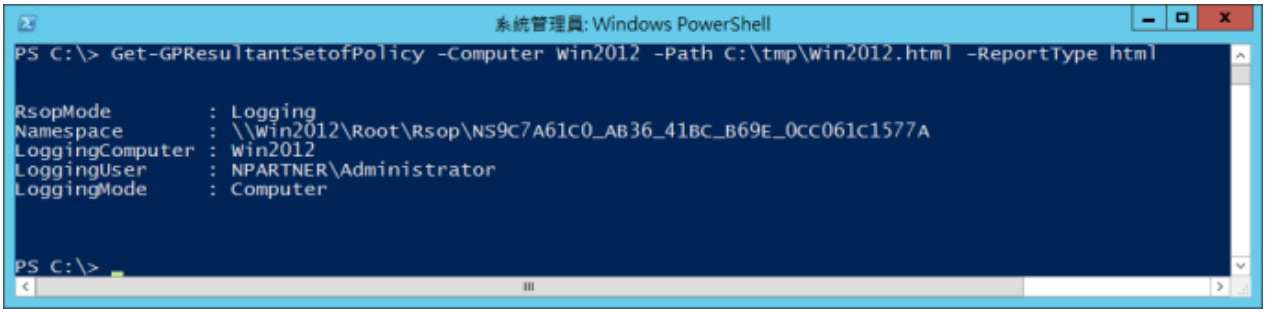
```
PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows File 伺服器名

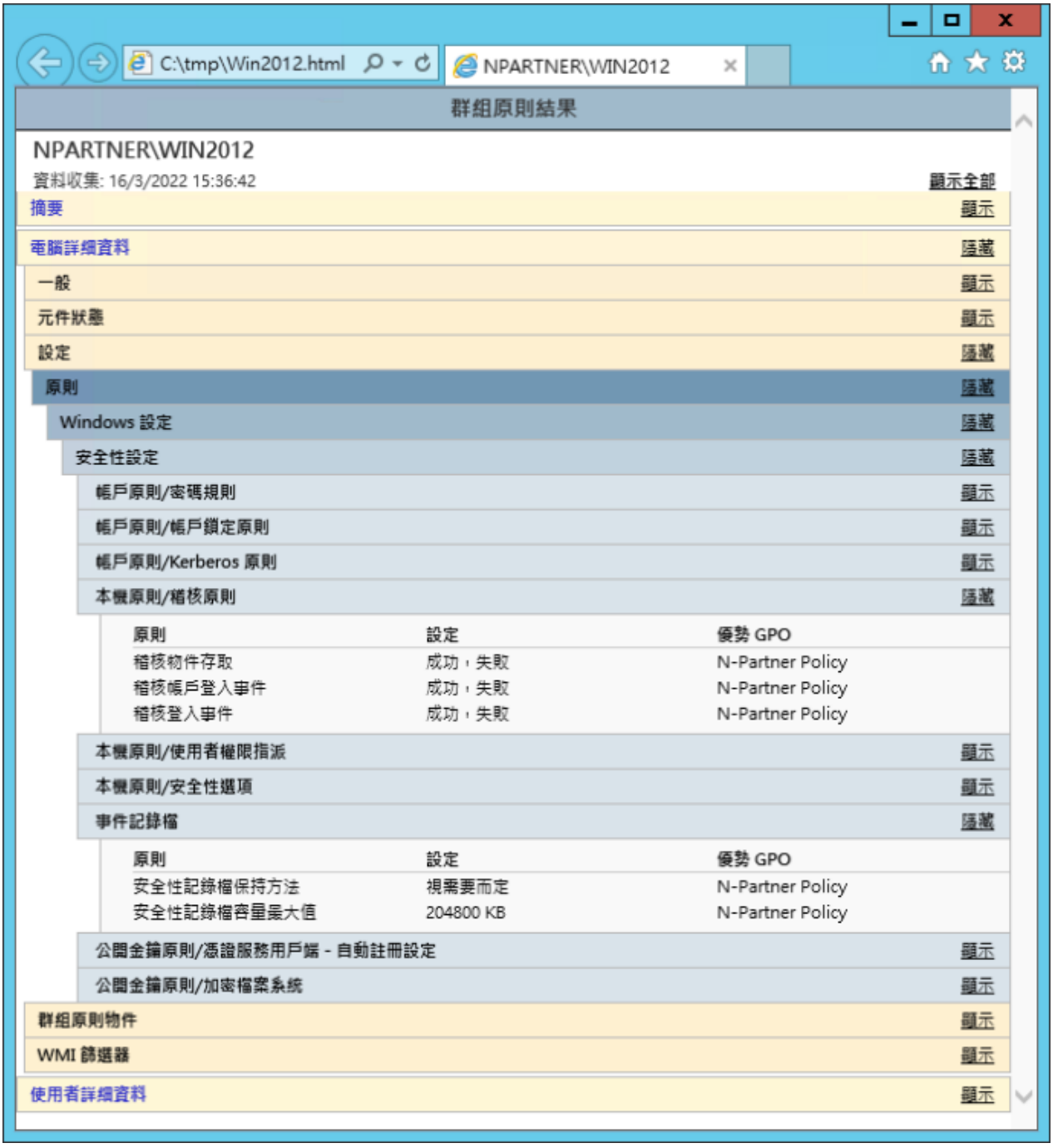
(10) 產生 Windows File 伺服器群組原則報表

```
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

(11) 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

5.2.1 稽核原則設定

(1) 開啟搜尋

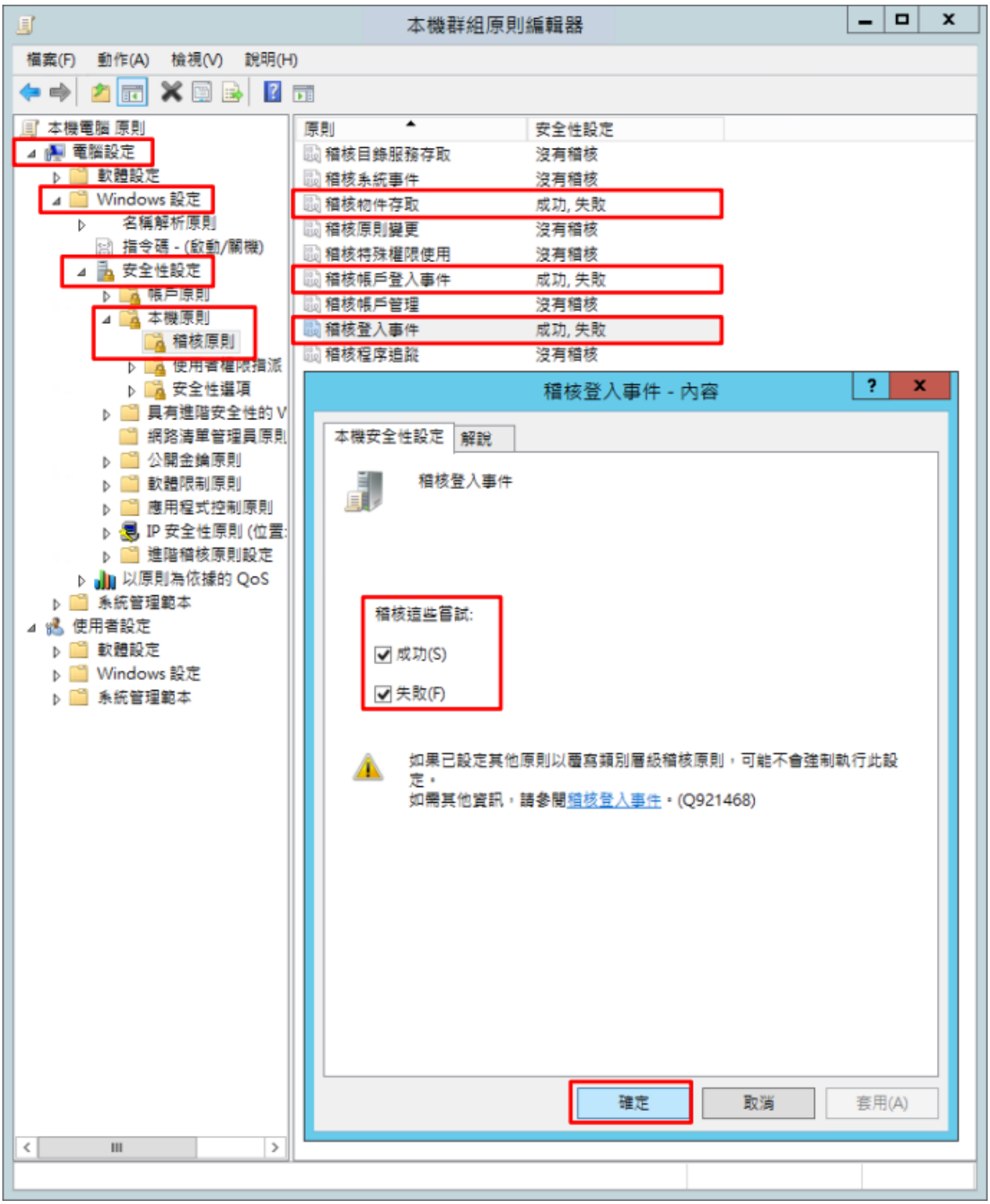
將滑鼠移到右下角點選 [搜尋]

(2) 搜尋群組原則物件編輯並執行

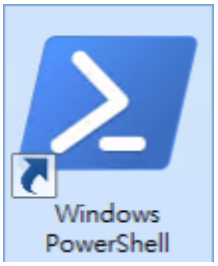
輸入 群組原則 -> 點選 [編輯群組原則]

(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]

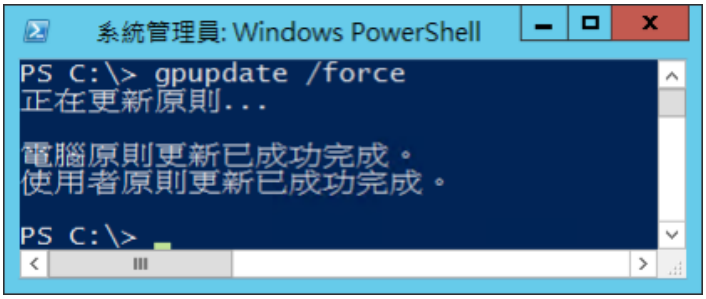


(4) 開啟 [Windows PowerShell]



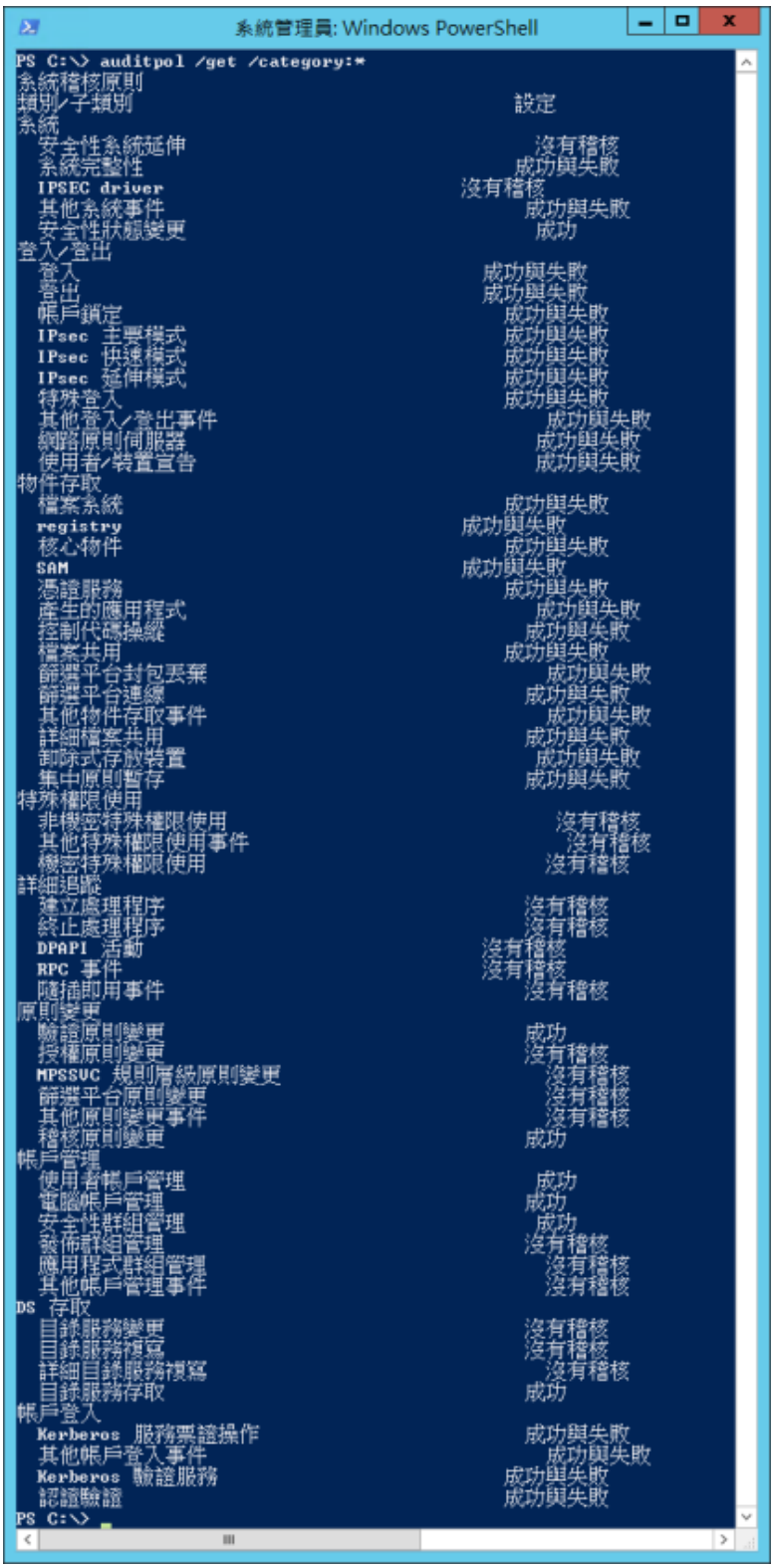
(5) 更新群組原則

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



(6) 查看群組原則套用情形

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



5.2.2 事件檔案設定

(1) 開啟搜尋

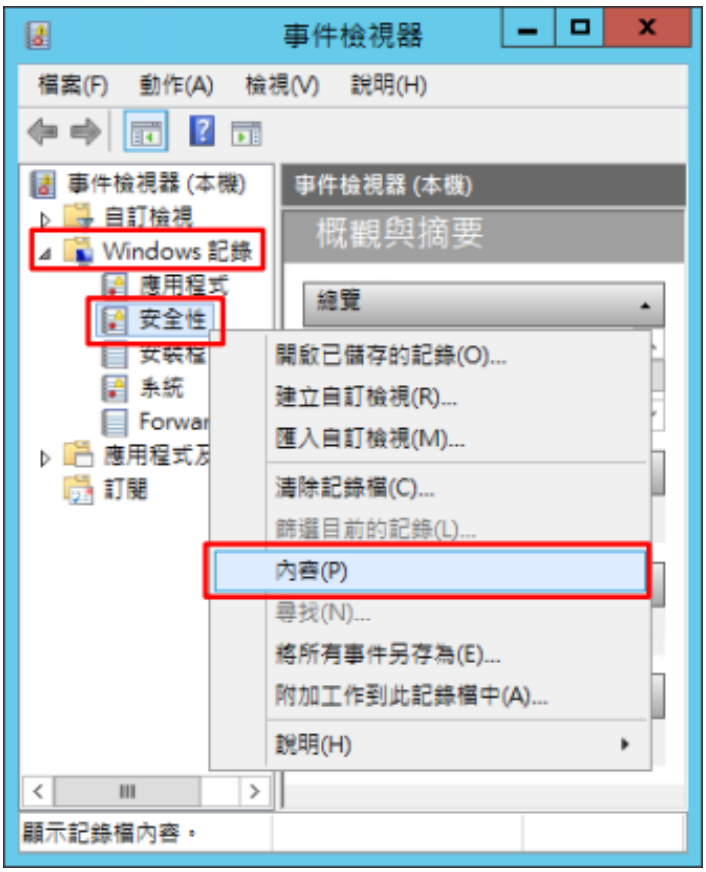
將滑鼠移到右下角點選 [搜尋]

(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]

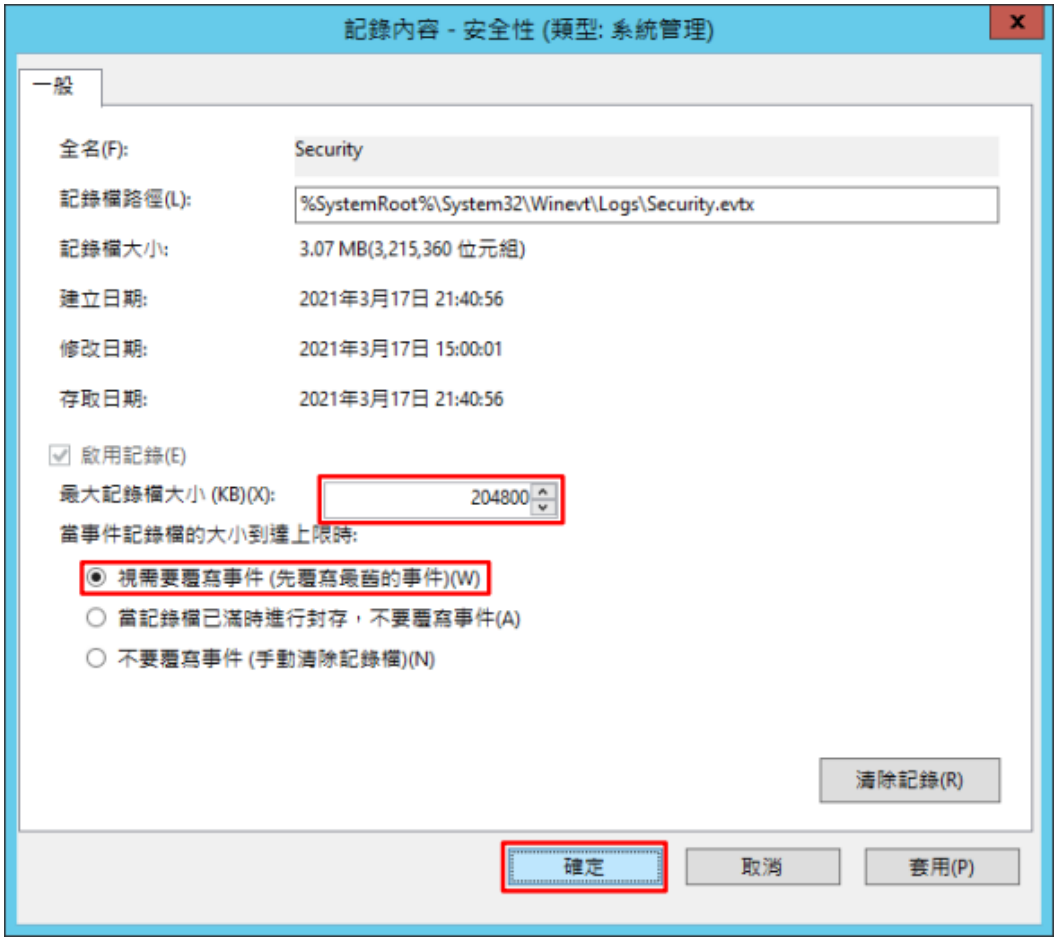
(3) 編輯安全性記錄

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



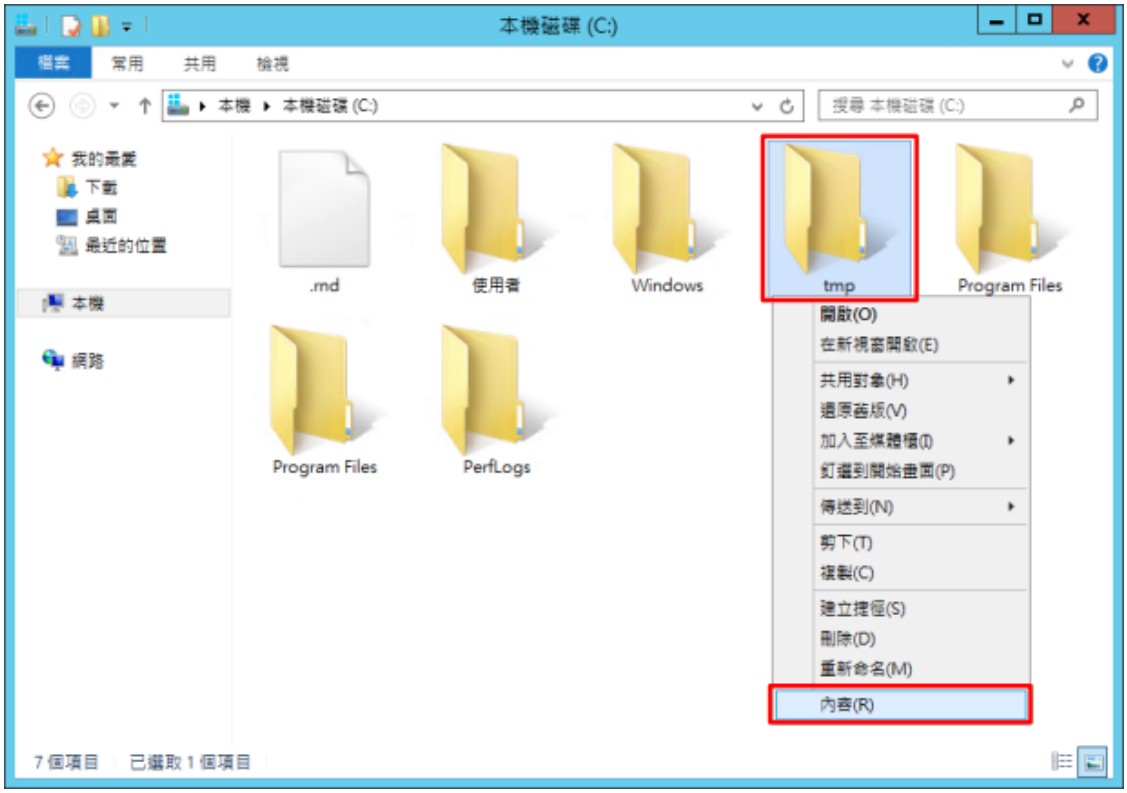
(4) 設定安全性記錄檔

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]

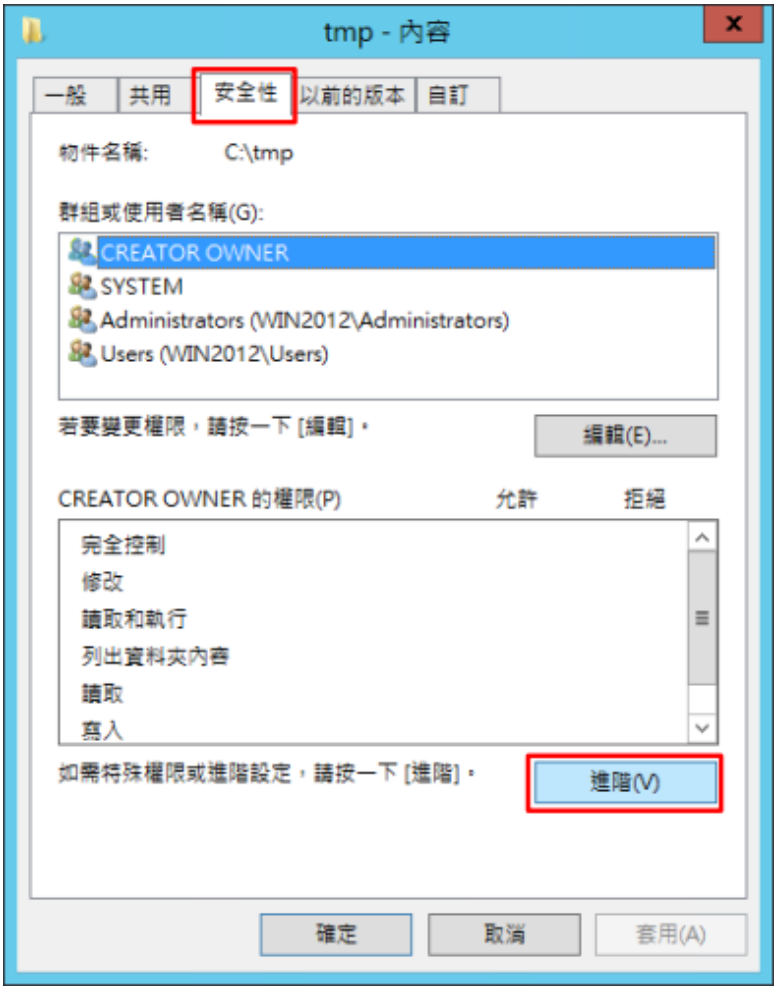


5.3 稽核資料夾設定

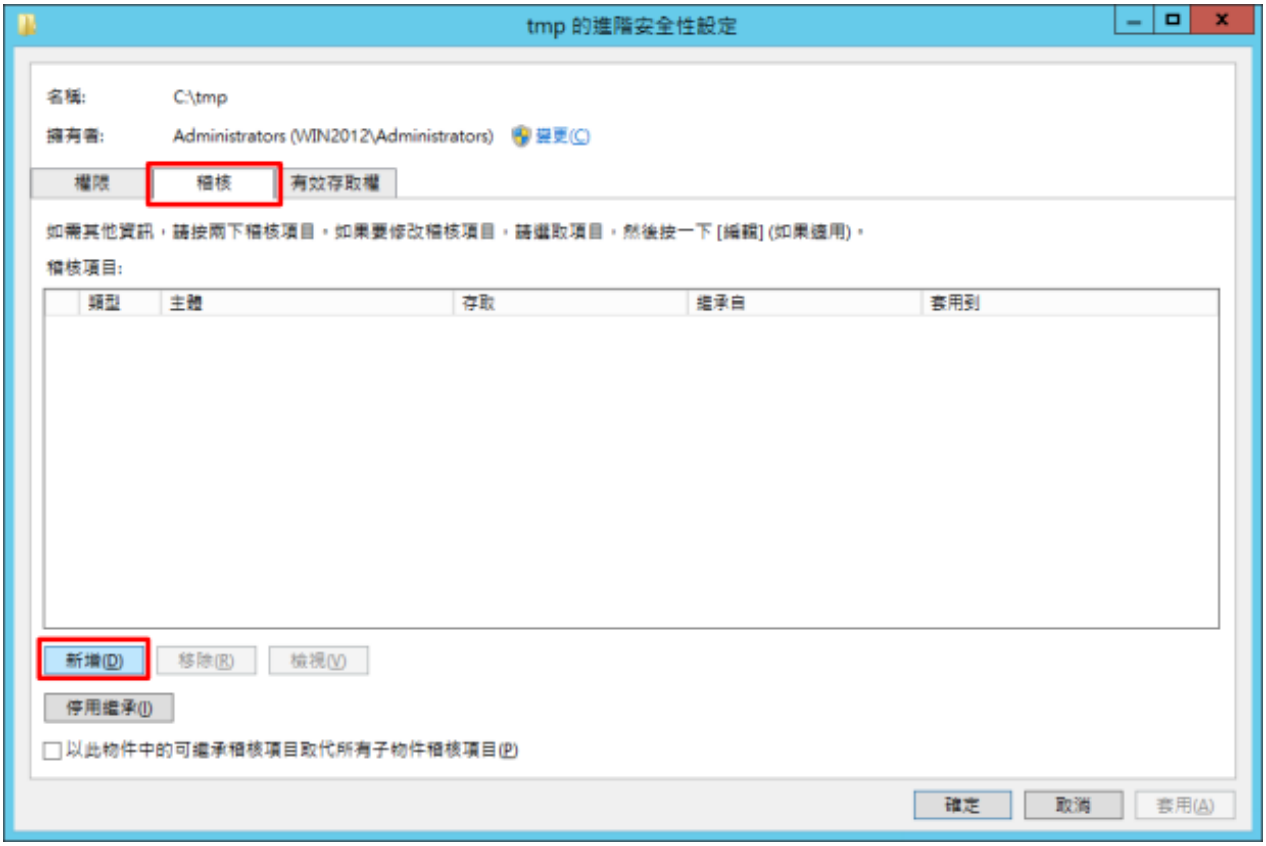
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



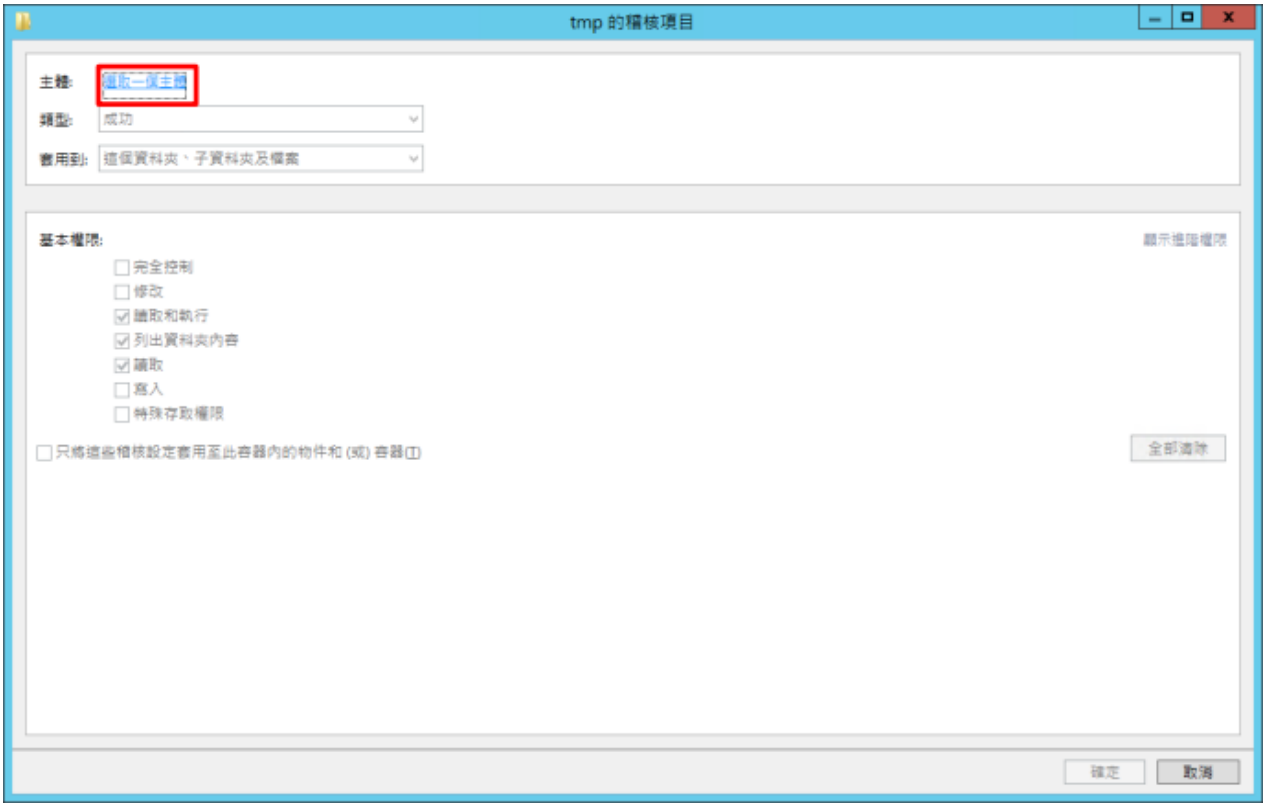
(2) 點選 [安全性] 頁面 -> 按 [進階]



(3) 點選 [稽核] 頁面 -> 按 [新增]

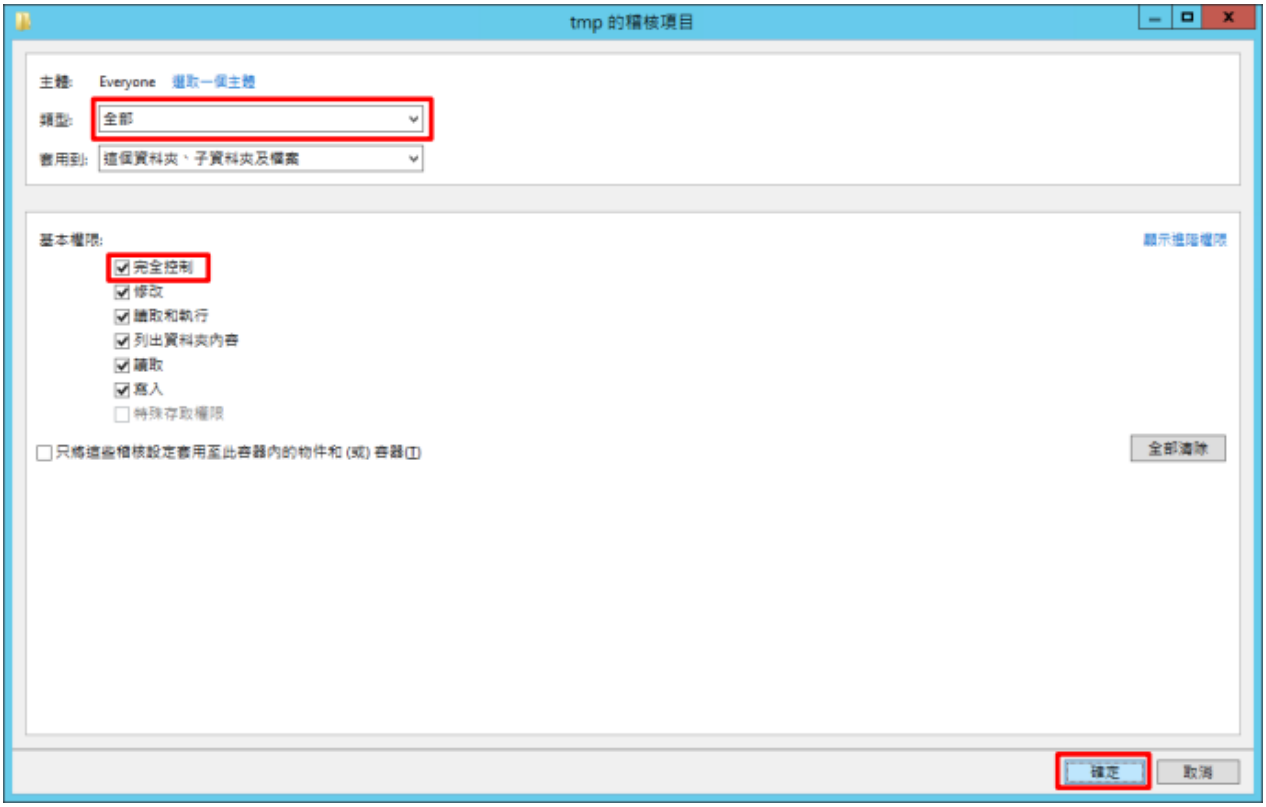


(4) 點選 [選取一個主體]

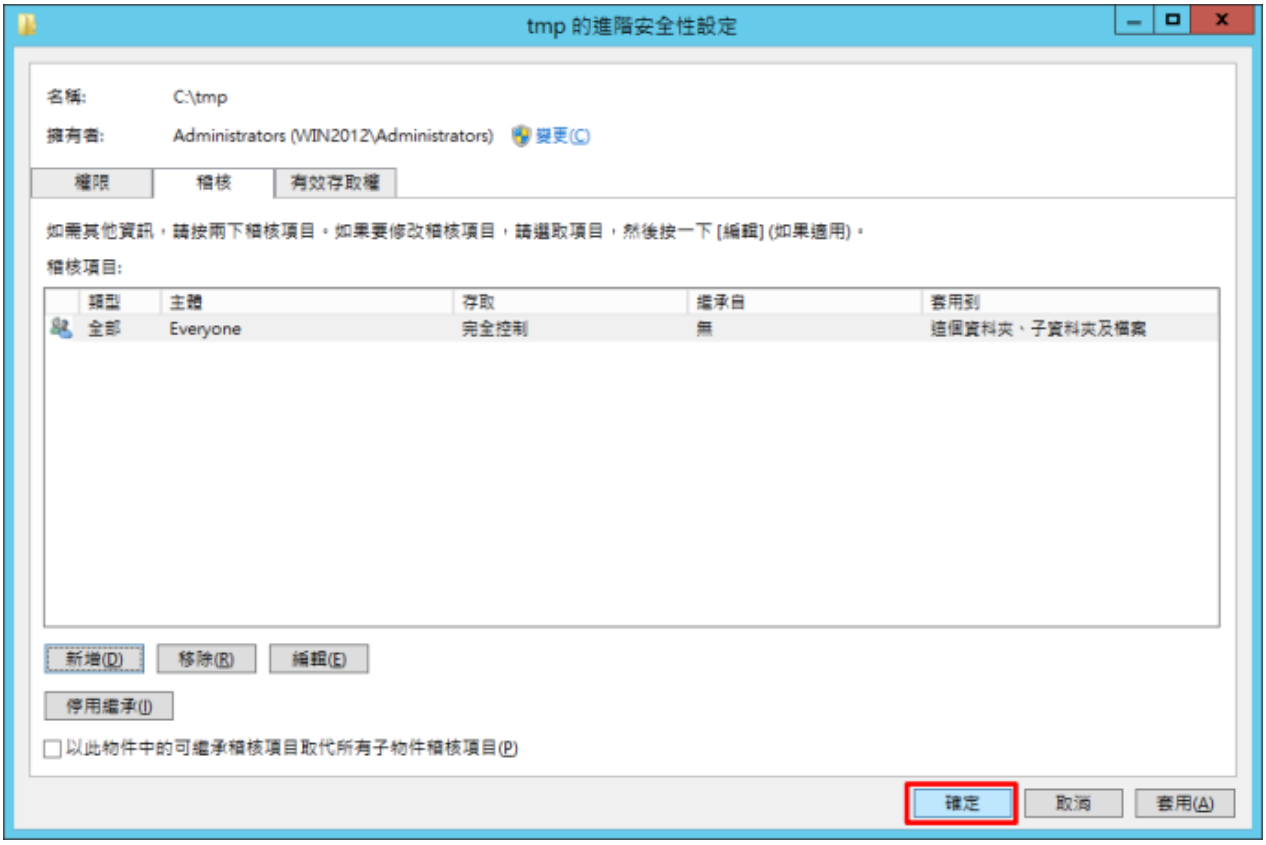


(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

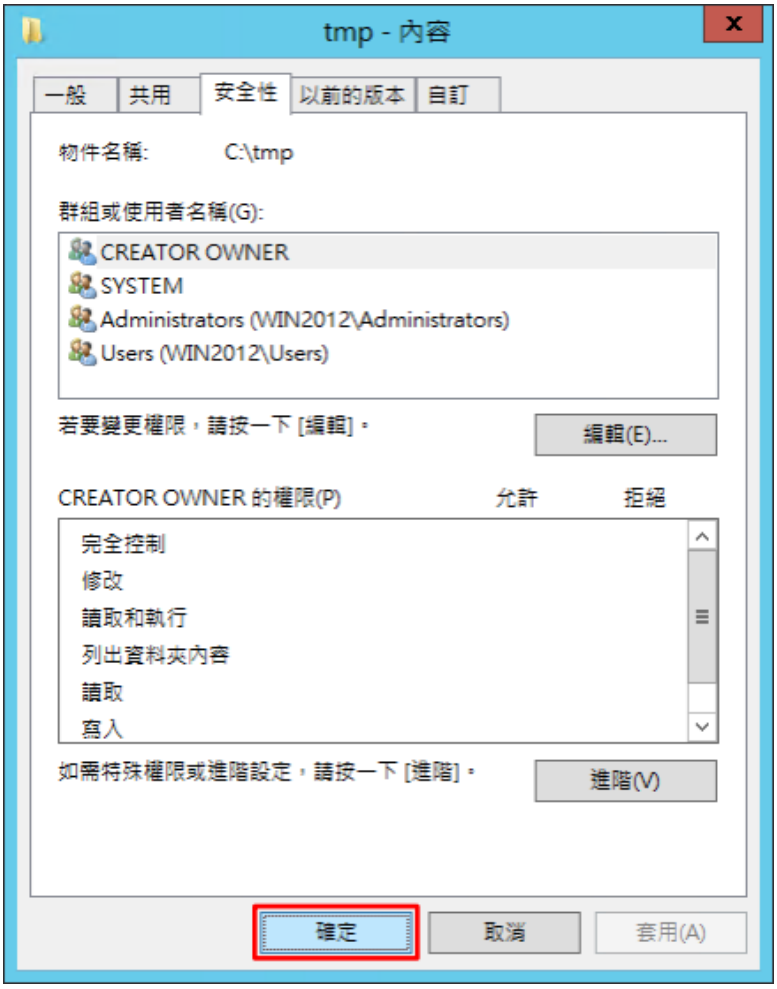
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(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

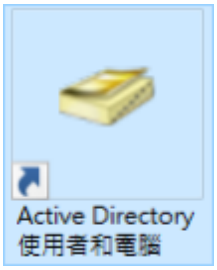
*以下分別為網域和工作群組設定方式。

6.1 網域

6.1.1 組織單位設定

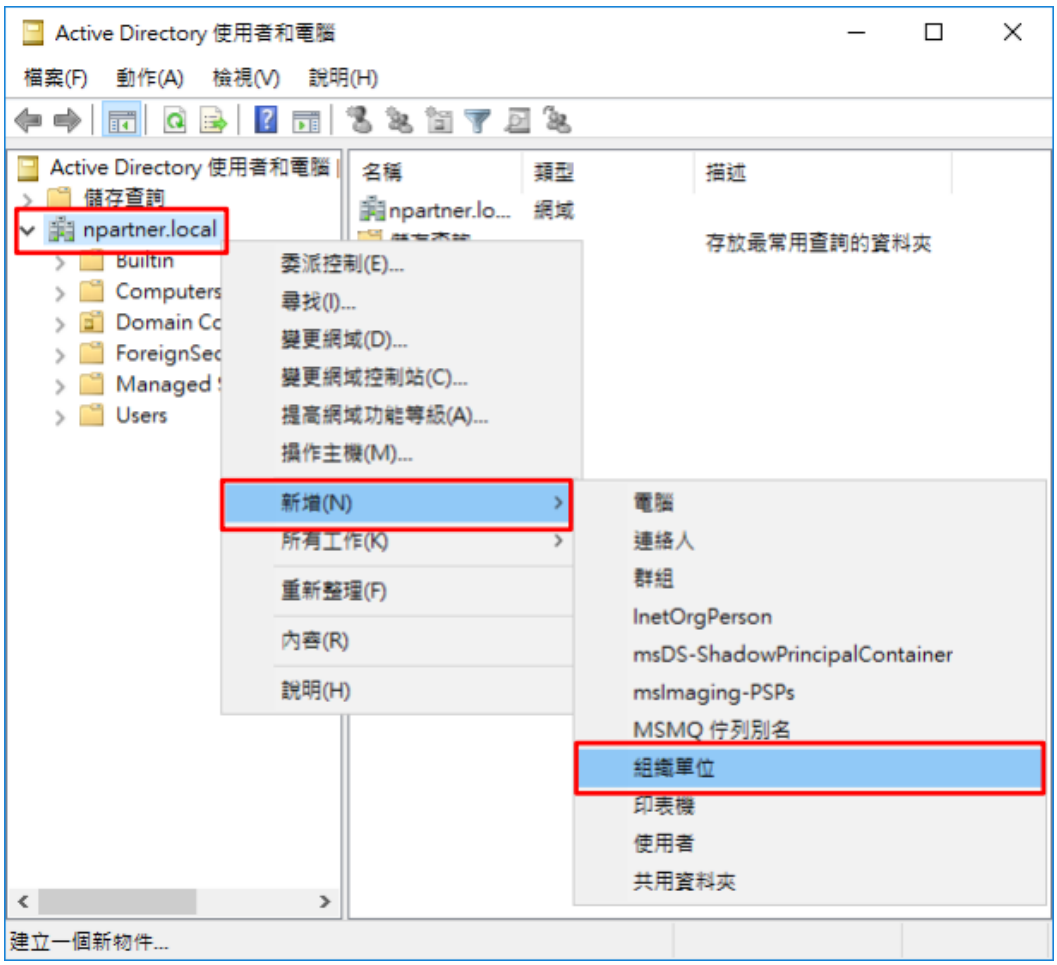
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



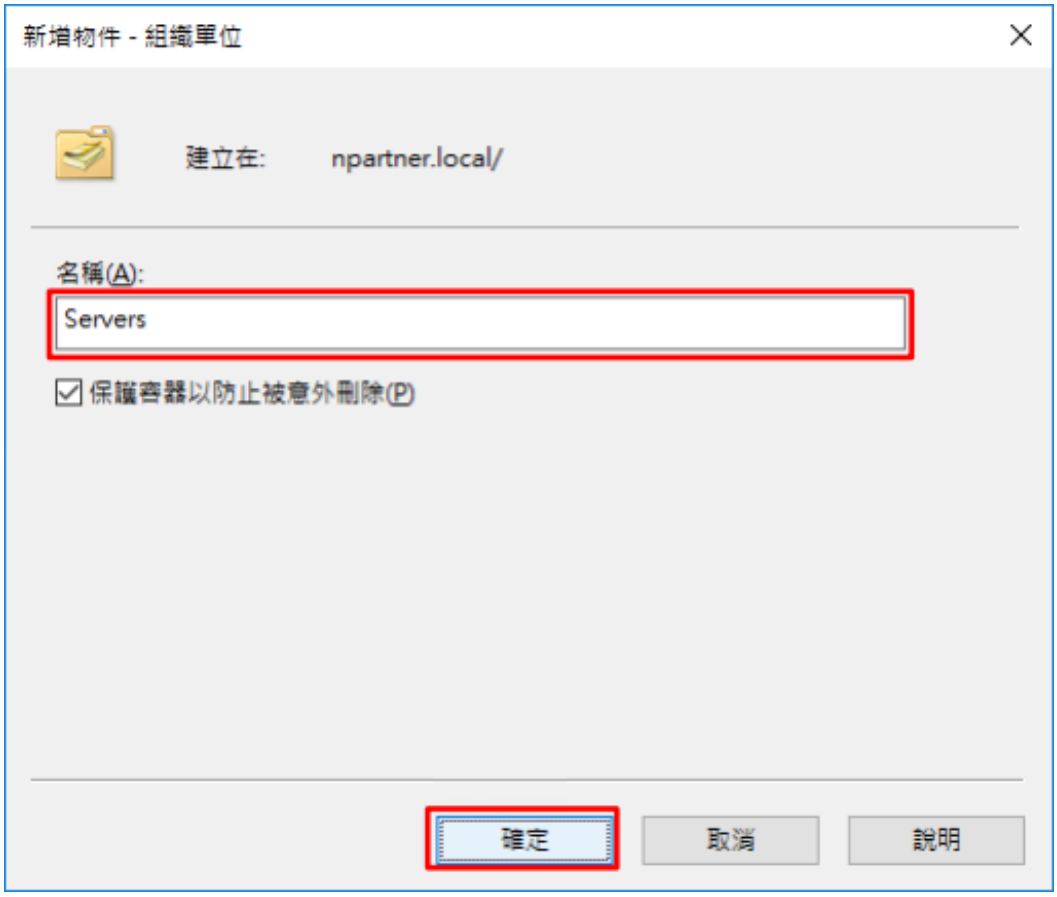
(2) 新增組織單位

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



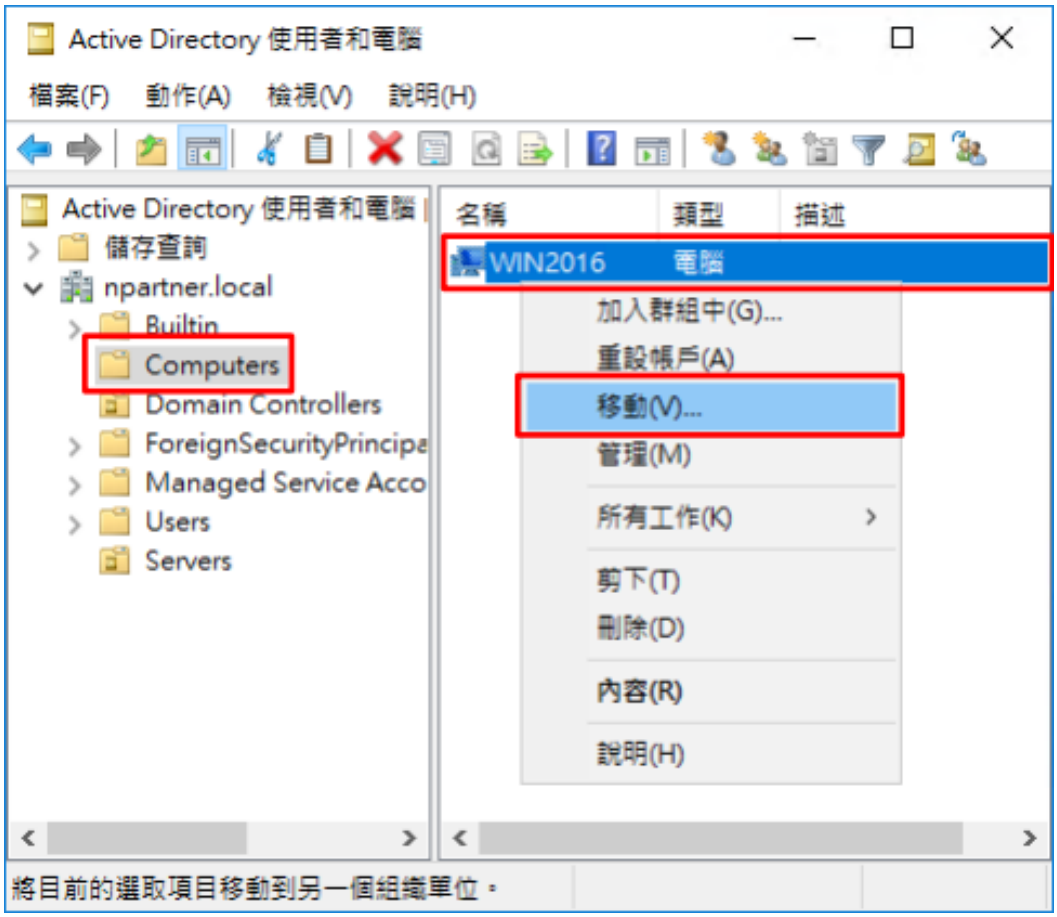
(3)　輸入組織單位名稱

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]



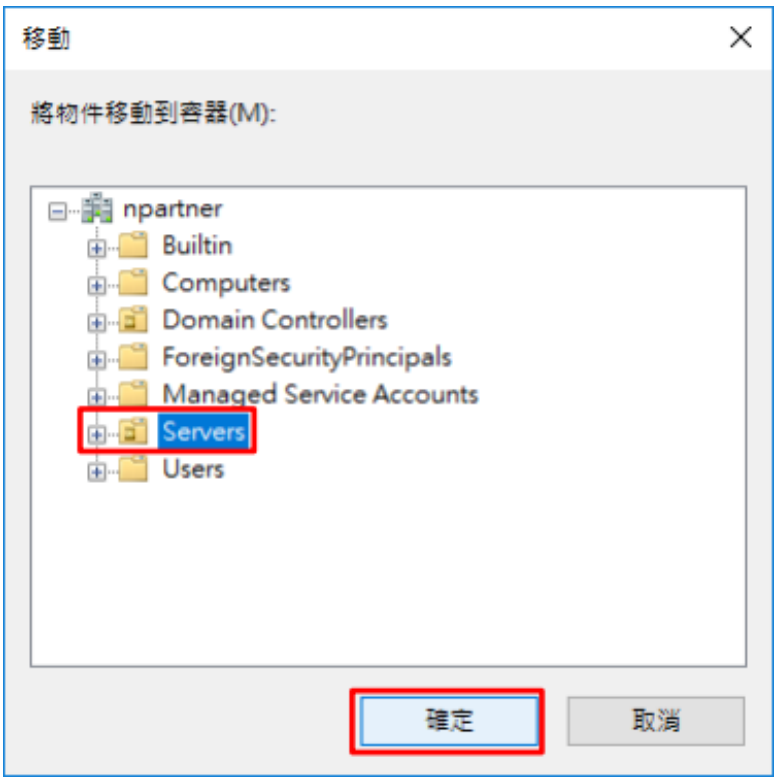
(4) 移動伺服器至新的組織單位

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 主機 -> 點選 [移動]



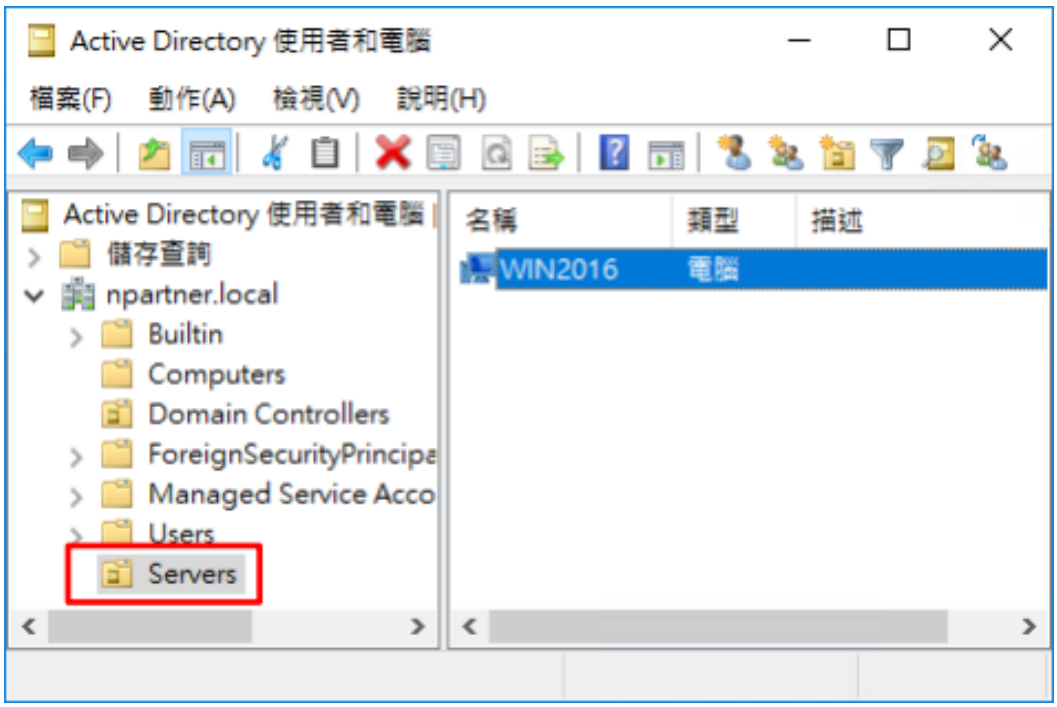
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

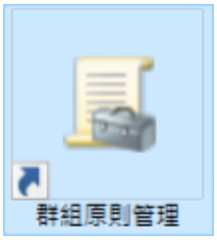
點選 [Servers] 組織單位，確認 Win2016 File 伺服器已移動。



6.1.2 群組原則設定

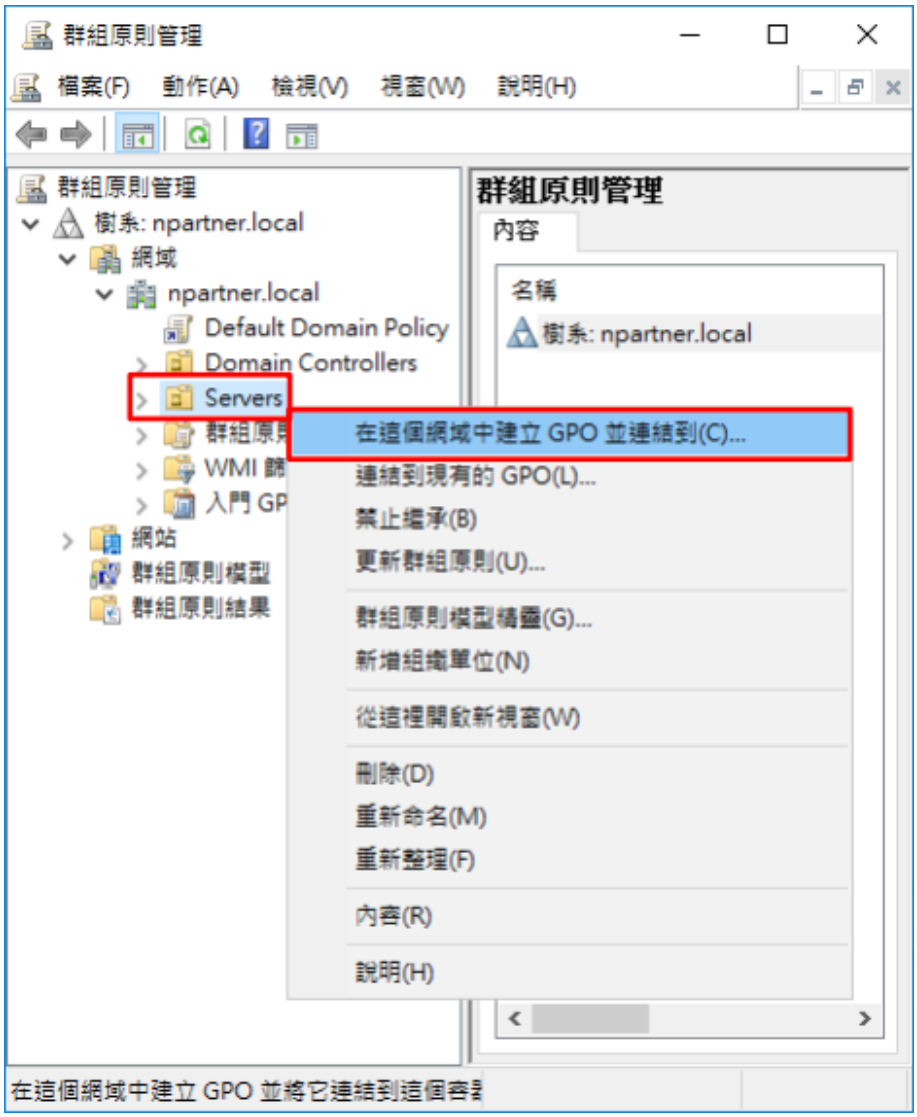
(1) 開啟群組原則管理

開啟 [群組原則管理]



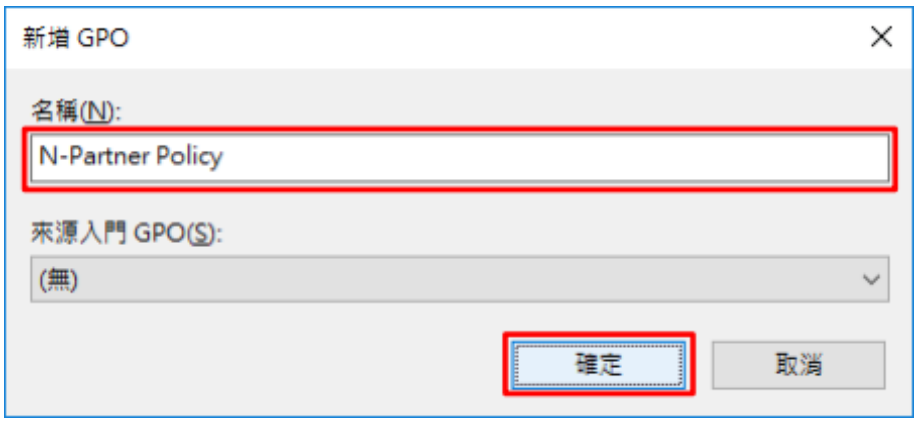
(2) 在 Servers 組織單位，新增群組原則物件

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...]



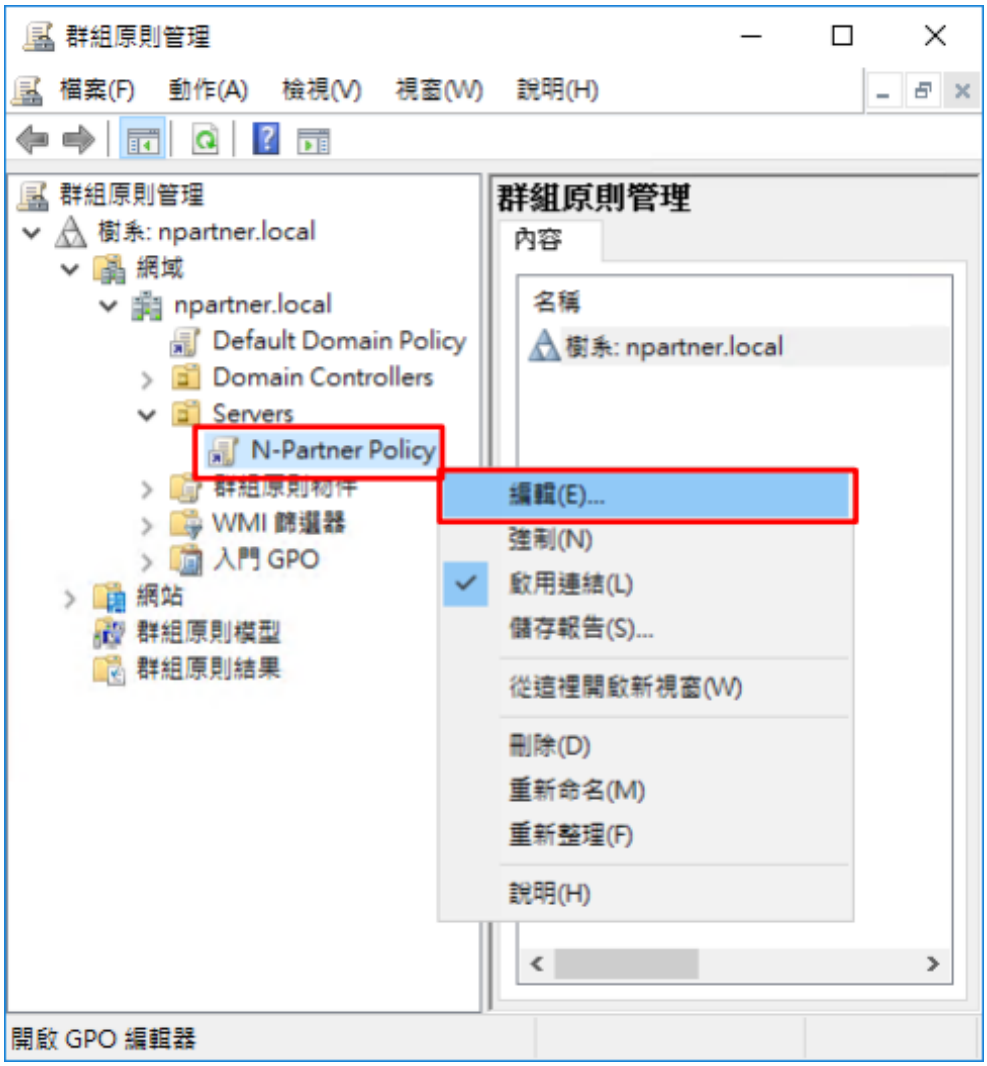
(3) 輸入群組原則物件名稱

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]



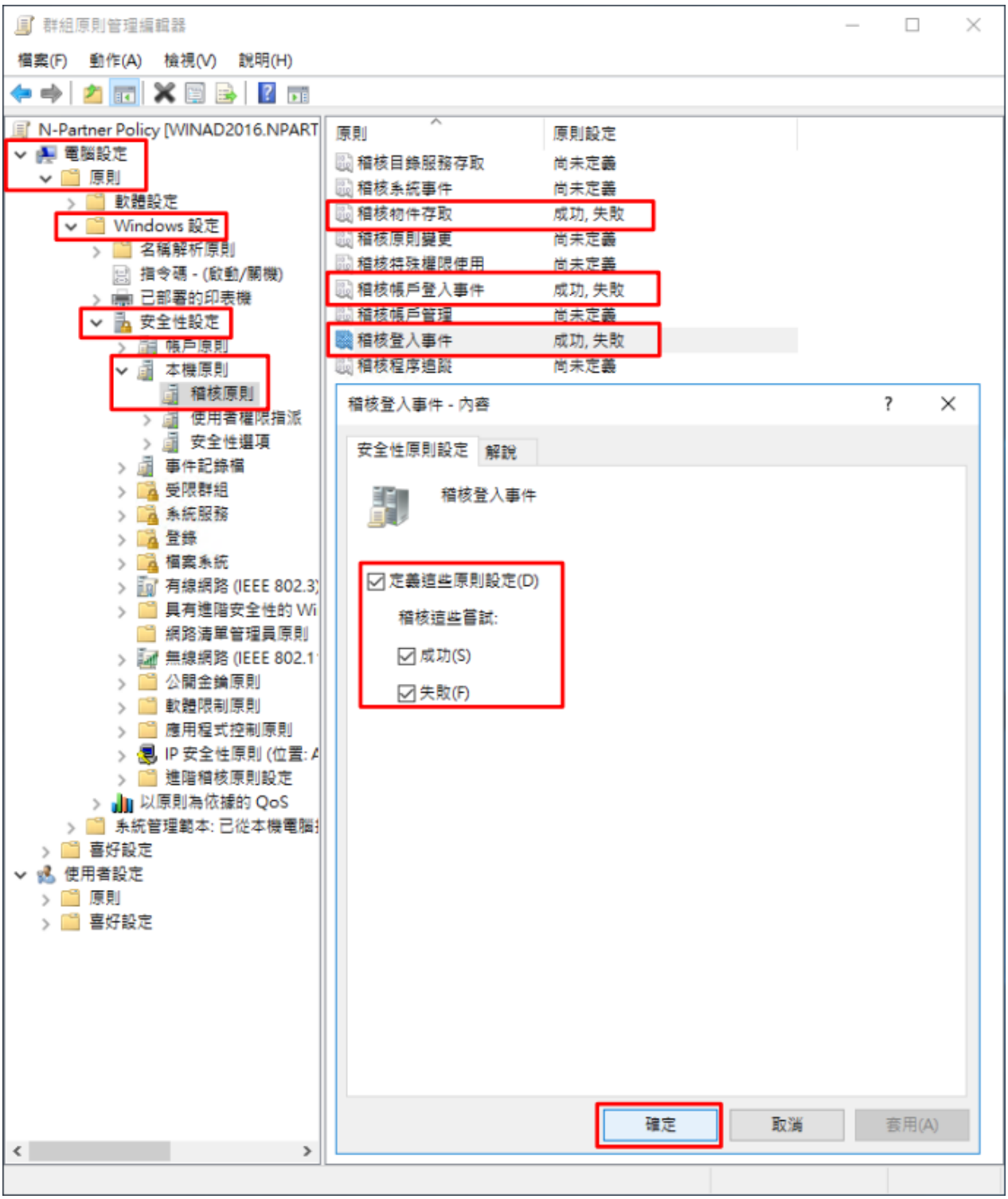
(4) 編輯群組原則物件

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



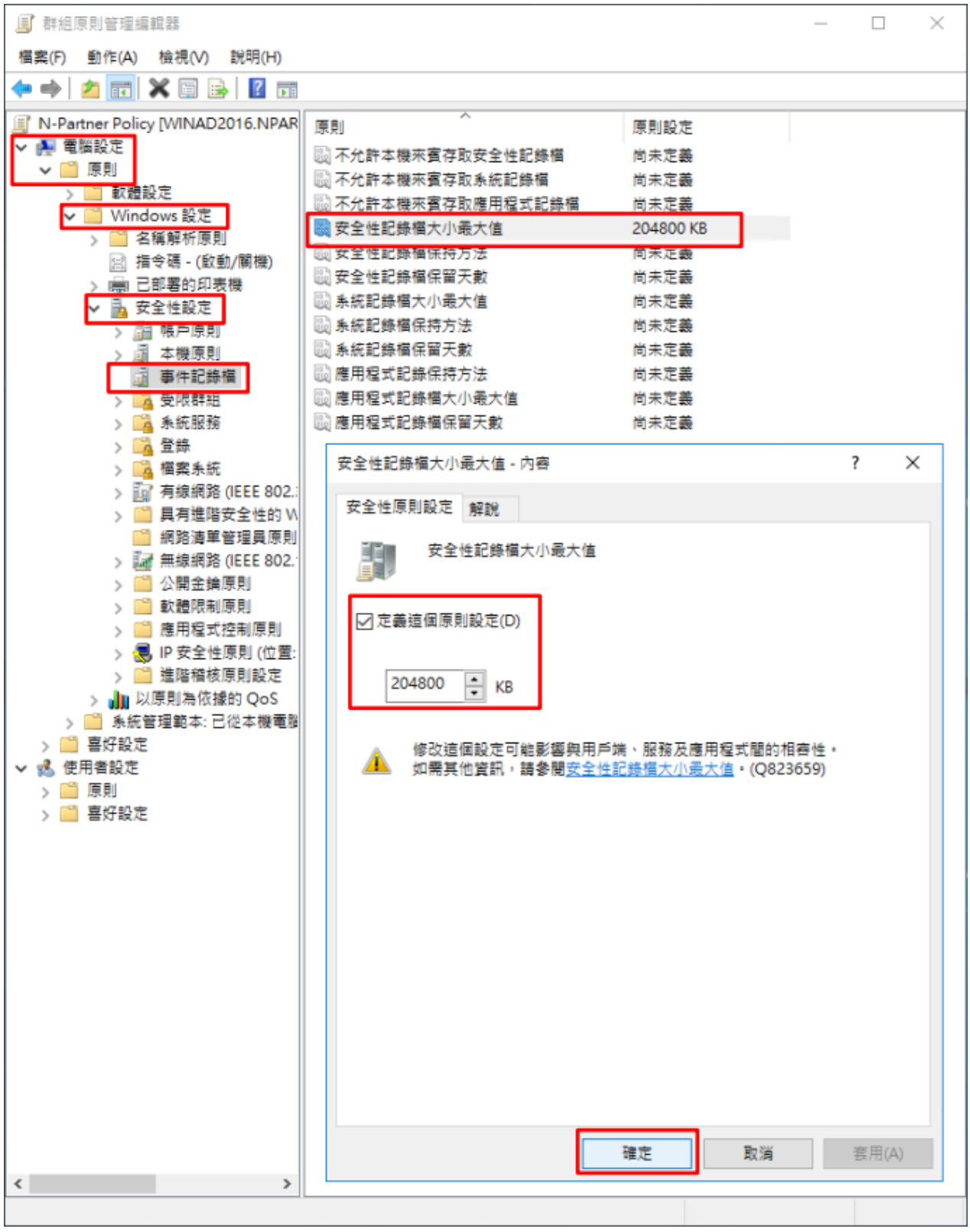
(5) 本機原則：稽核原則

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]



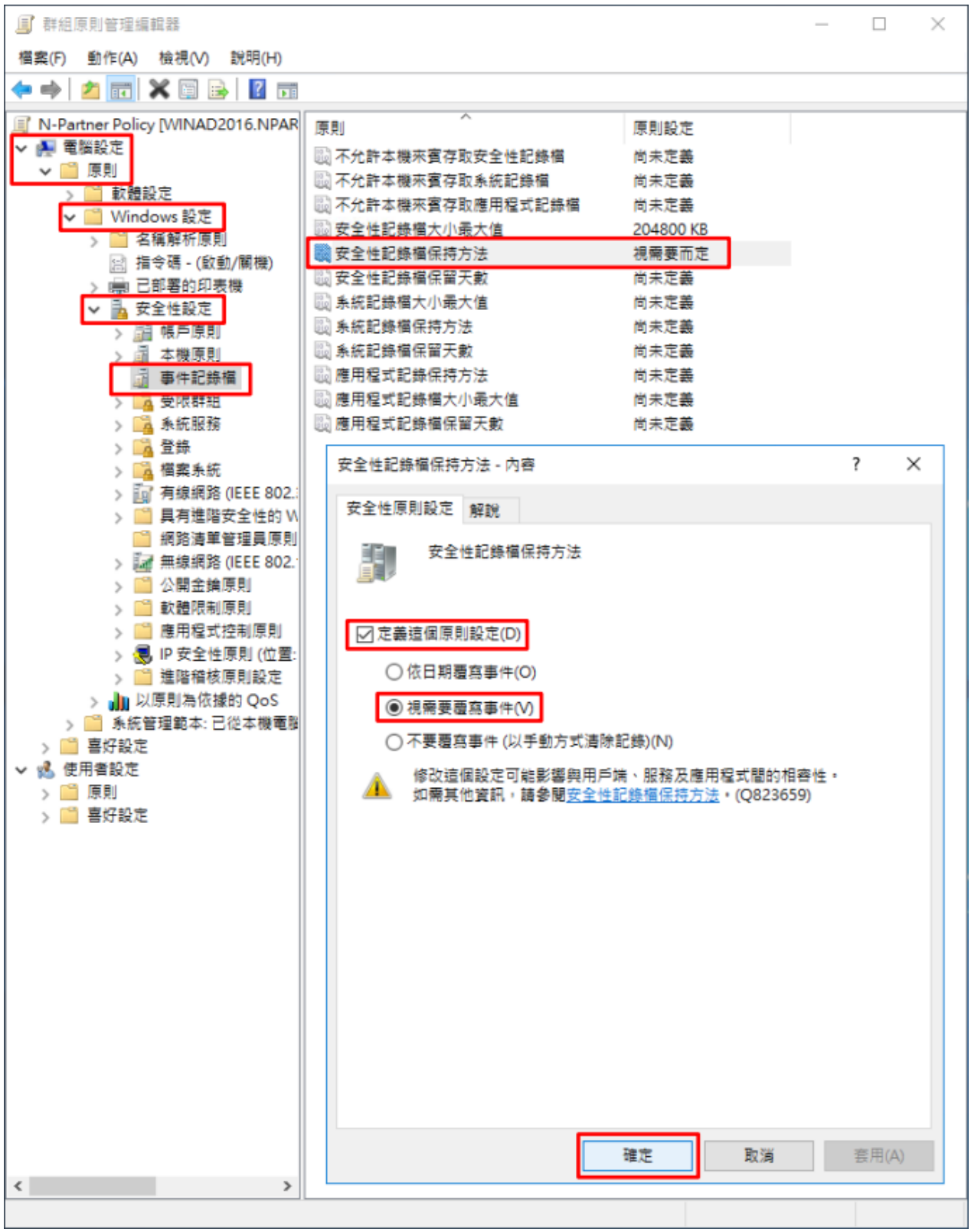
(6)　事件記錄檔：安全性記錄檔大小最大值

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]

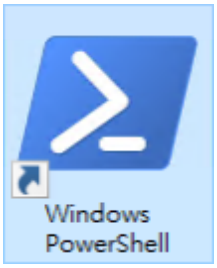


(7) 事件記錄檔：安全性記錄檔保持方法

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]

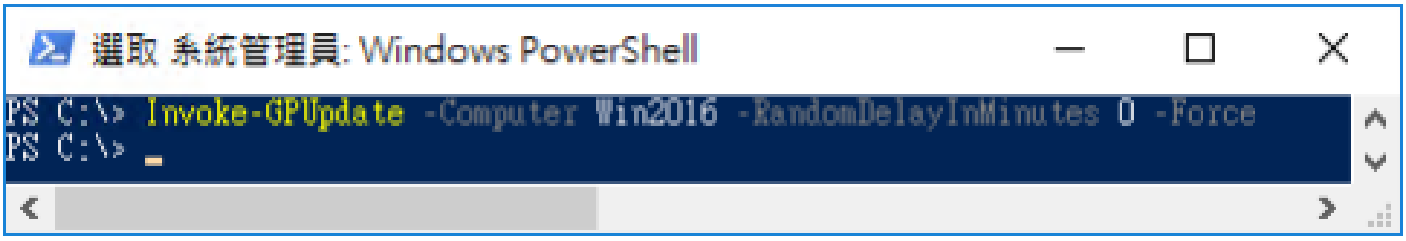


(8) 在 Windows File 伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows File 伺服器群組原則

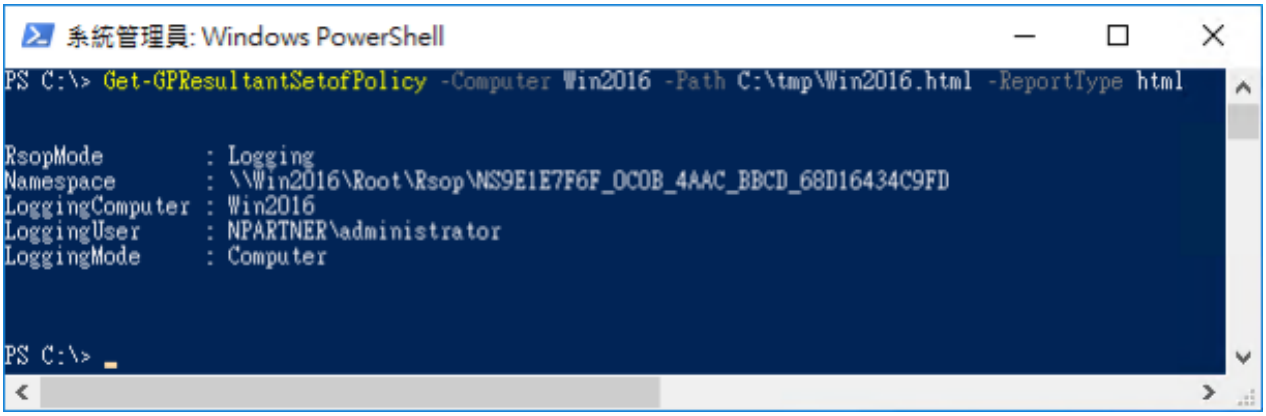
```
PS C:\> Invoke-GPUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows File 伺服器名

(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

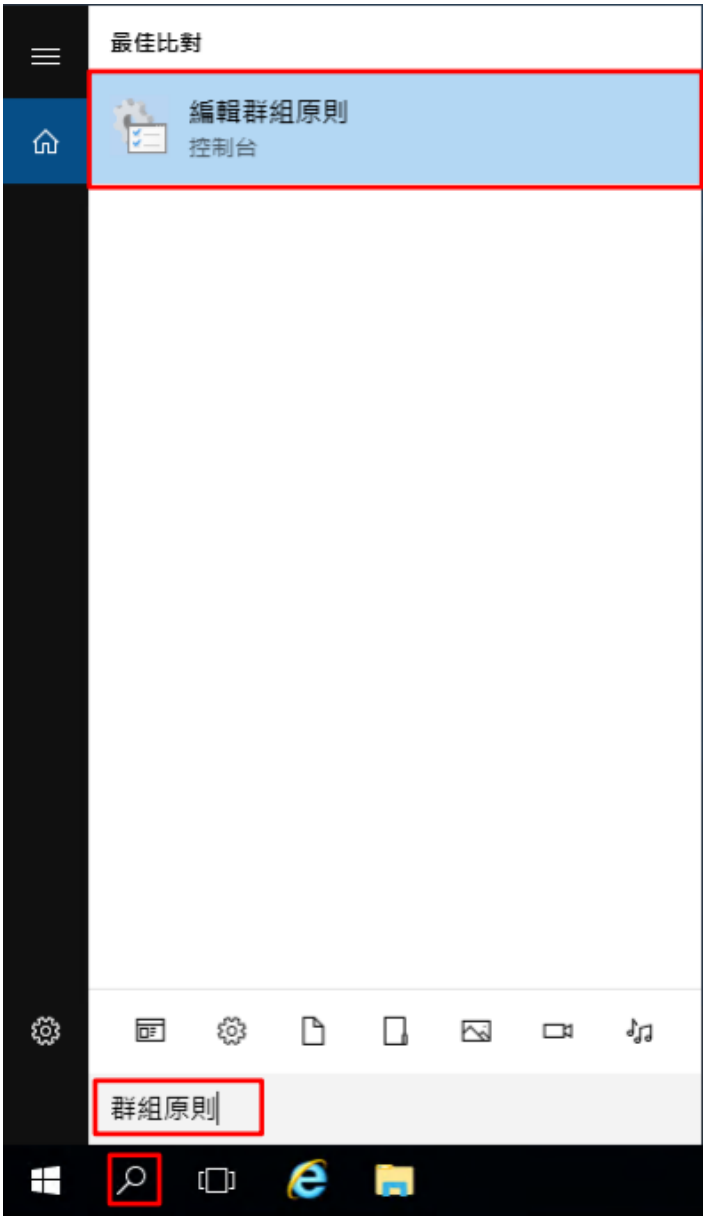
(11) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則

6.2 工作群組

6.2.1 稽核原則設定

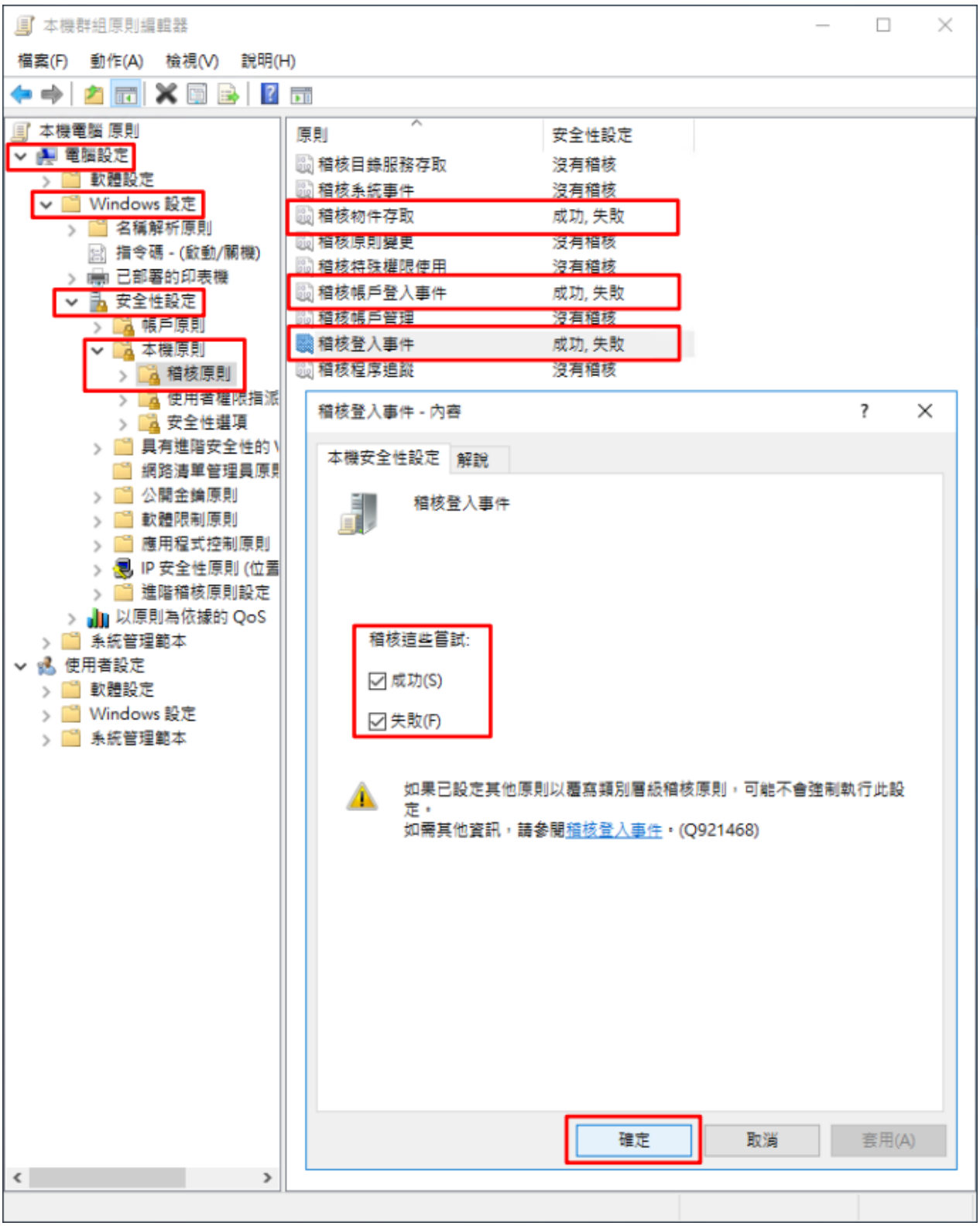
(1) 開啟本機群組原則編輯器

點選 -> 輸入 群組原則 -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

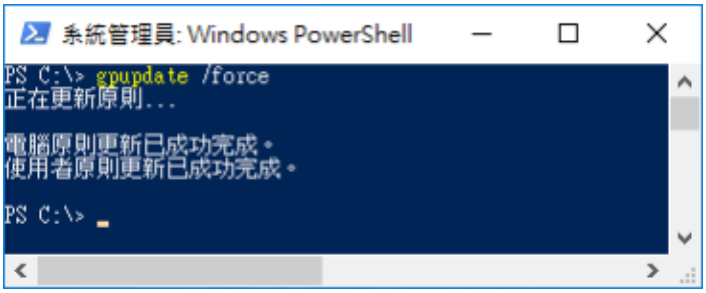
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

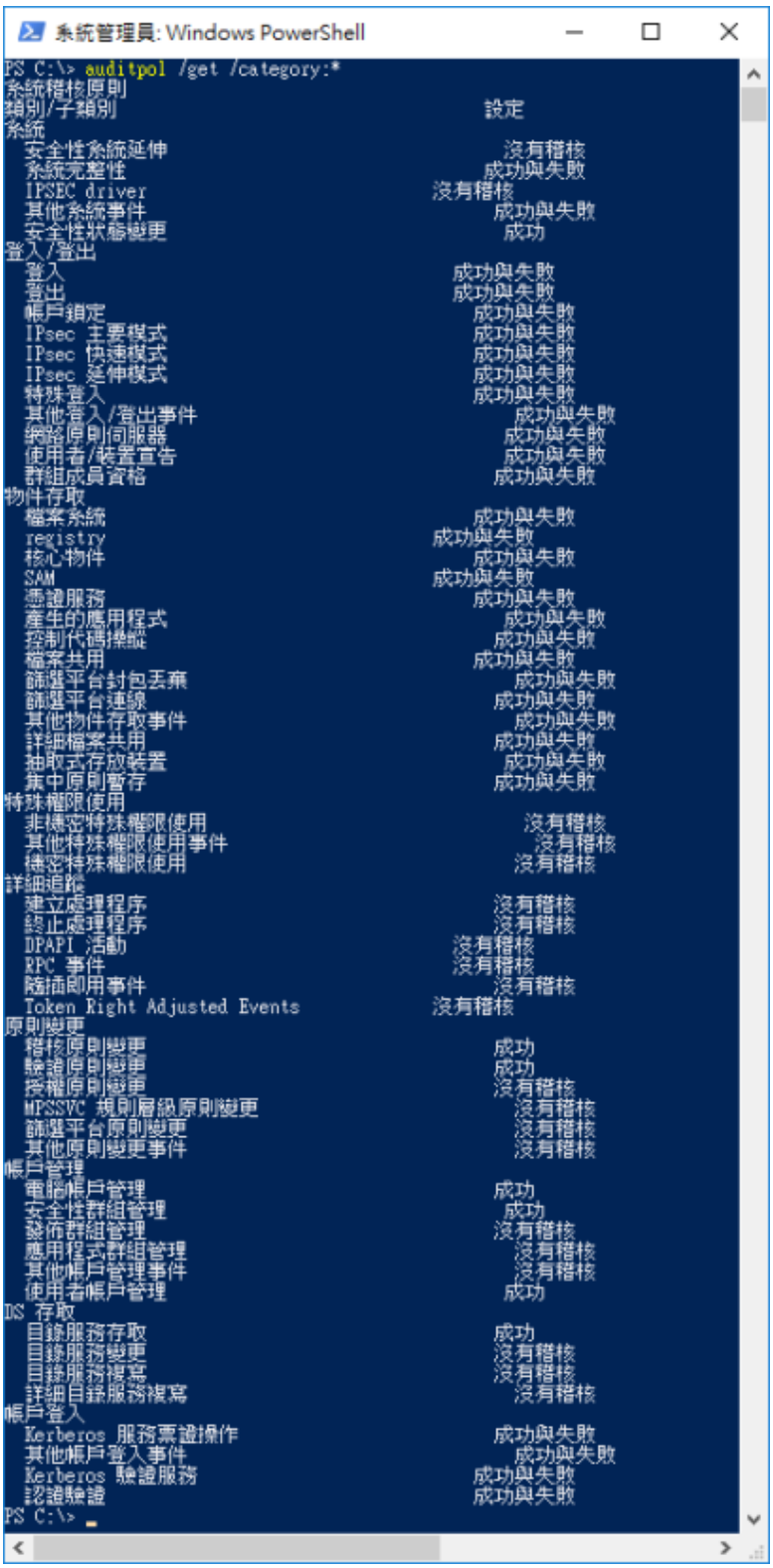
(4) 更新群組原則

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



(5) 查看群組原則套用情形

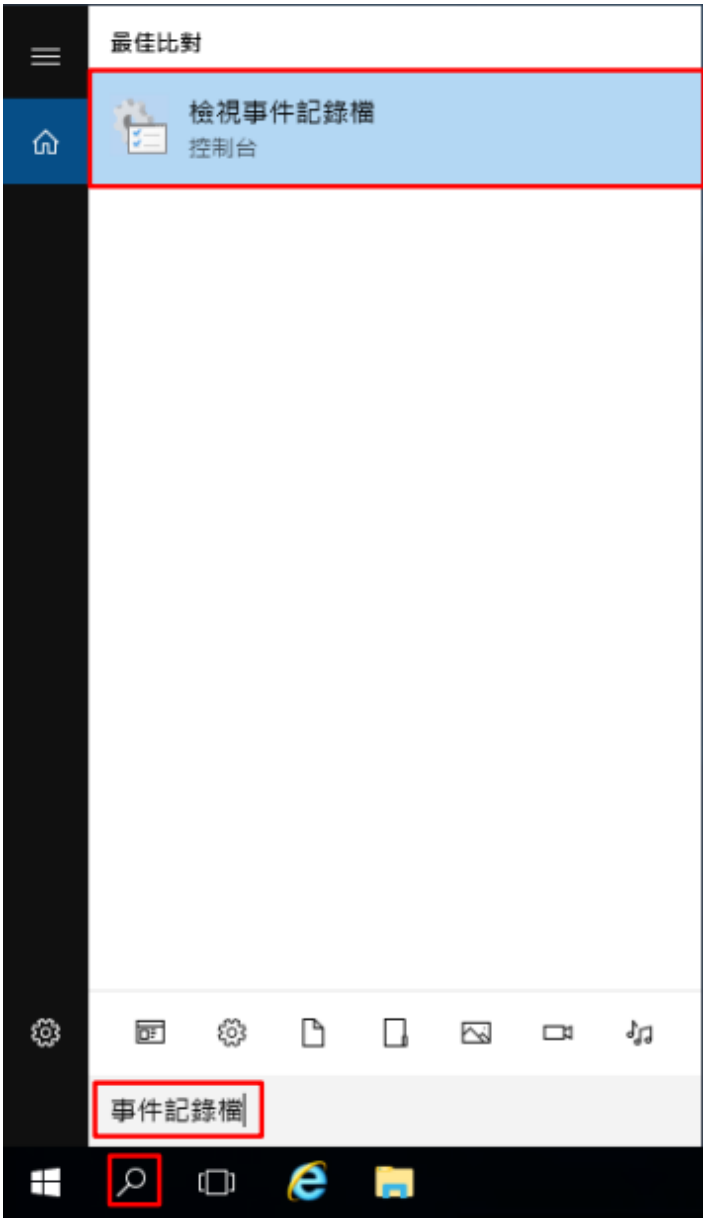
```
PS C:\> auditpol /get /category:*
```



6.2.2 事件檔案設定

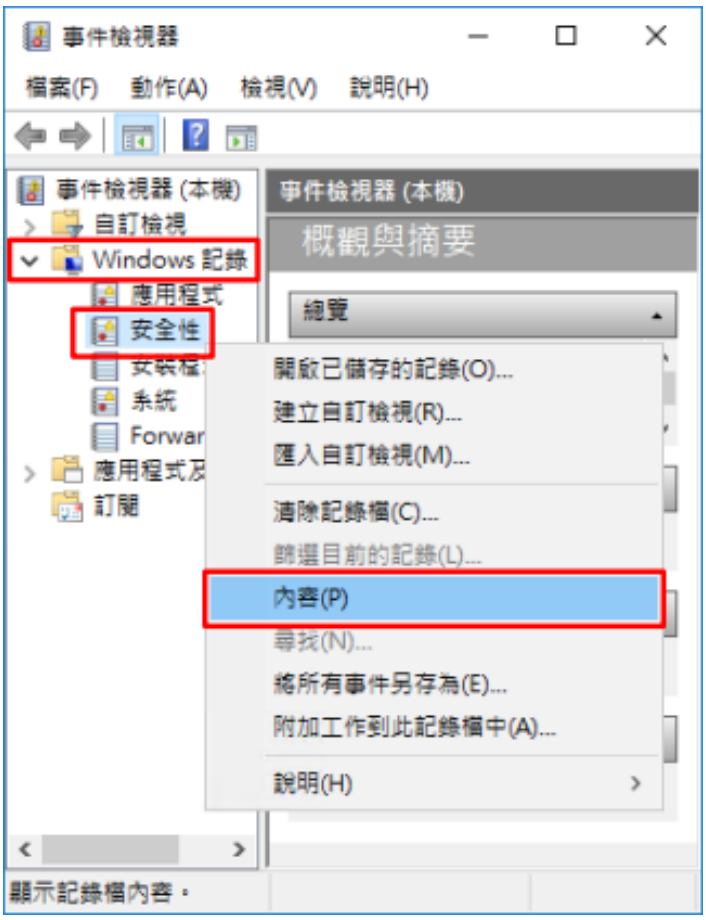
(1) 開啟 [檢視事件記錄檔]

點選 -> 輸入 事件記錄檔 -> 點選 [檢視事件記錄檔]



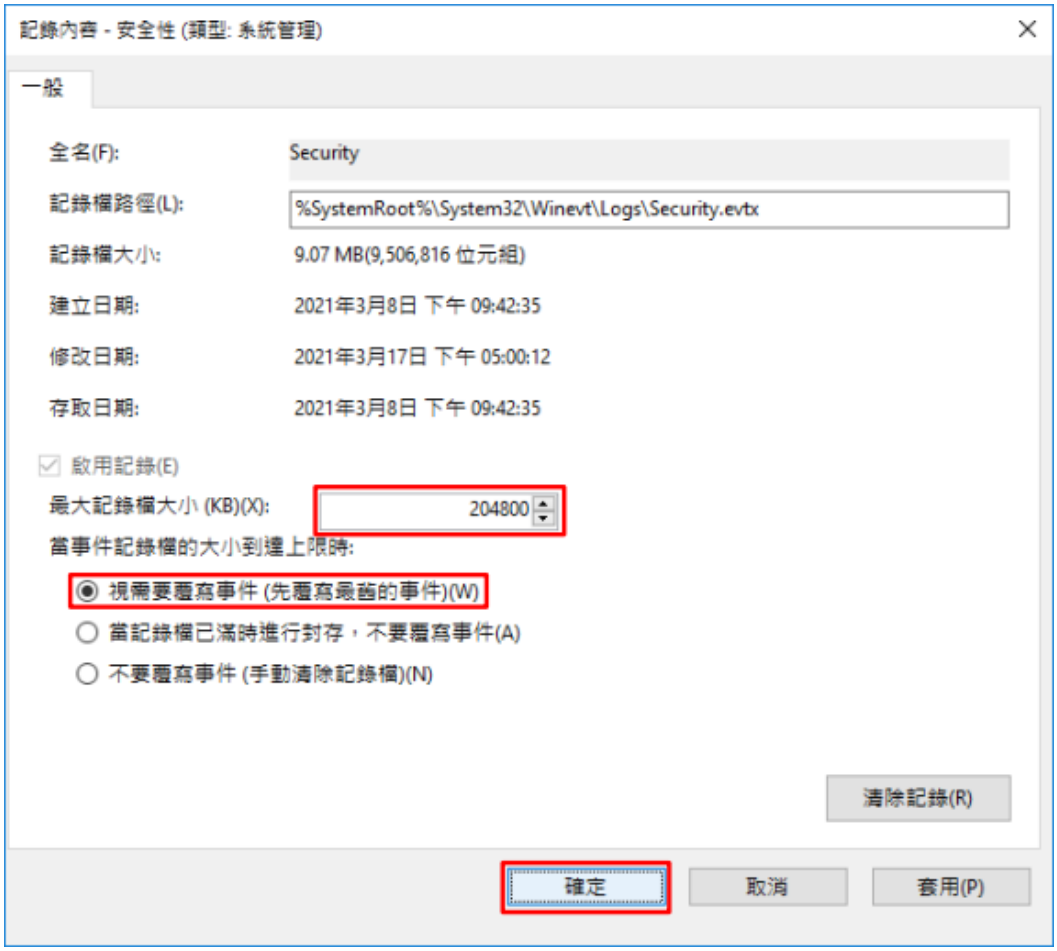
(2) 編輯安全性記錄

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



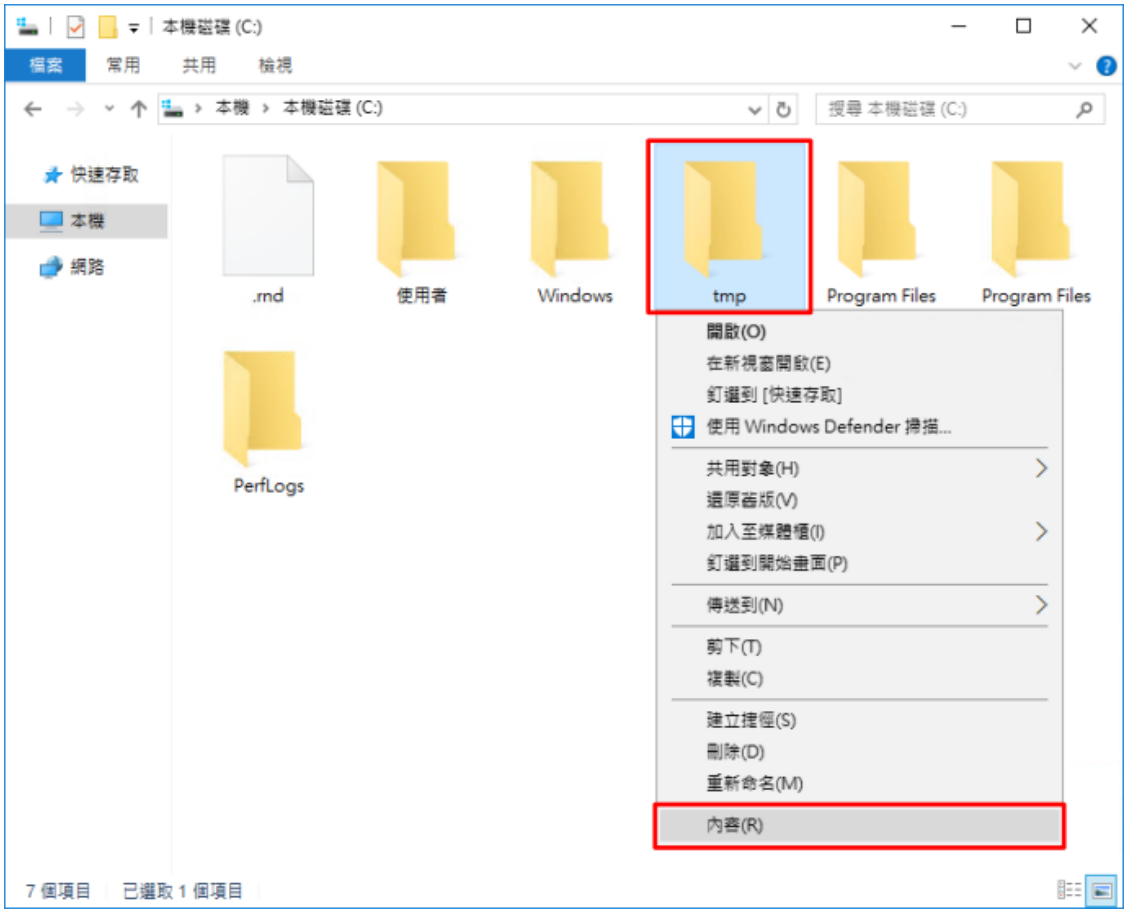
(3) 設定安全性記錄檔

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]

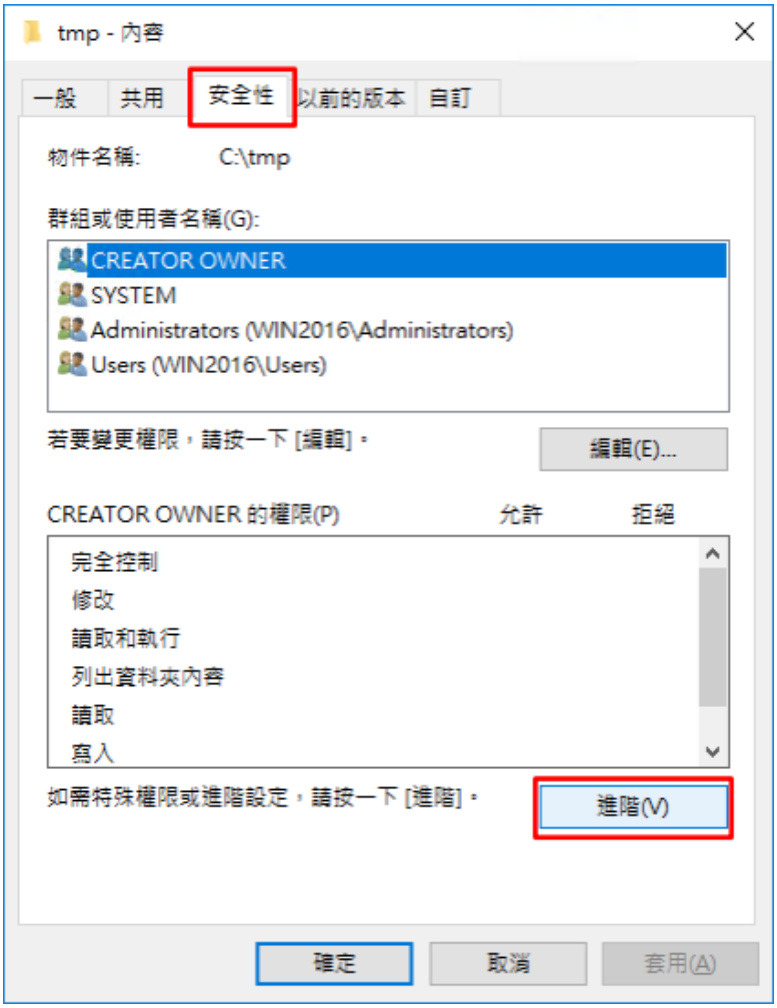


6.3 稽核資料夾設定

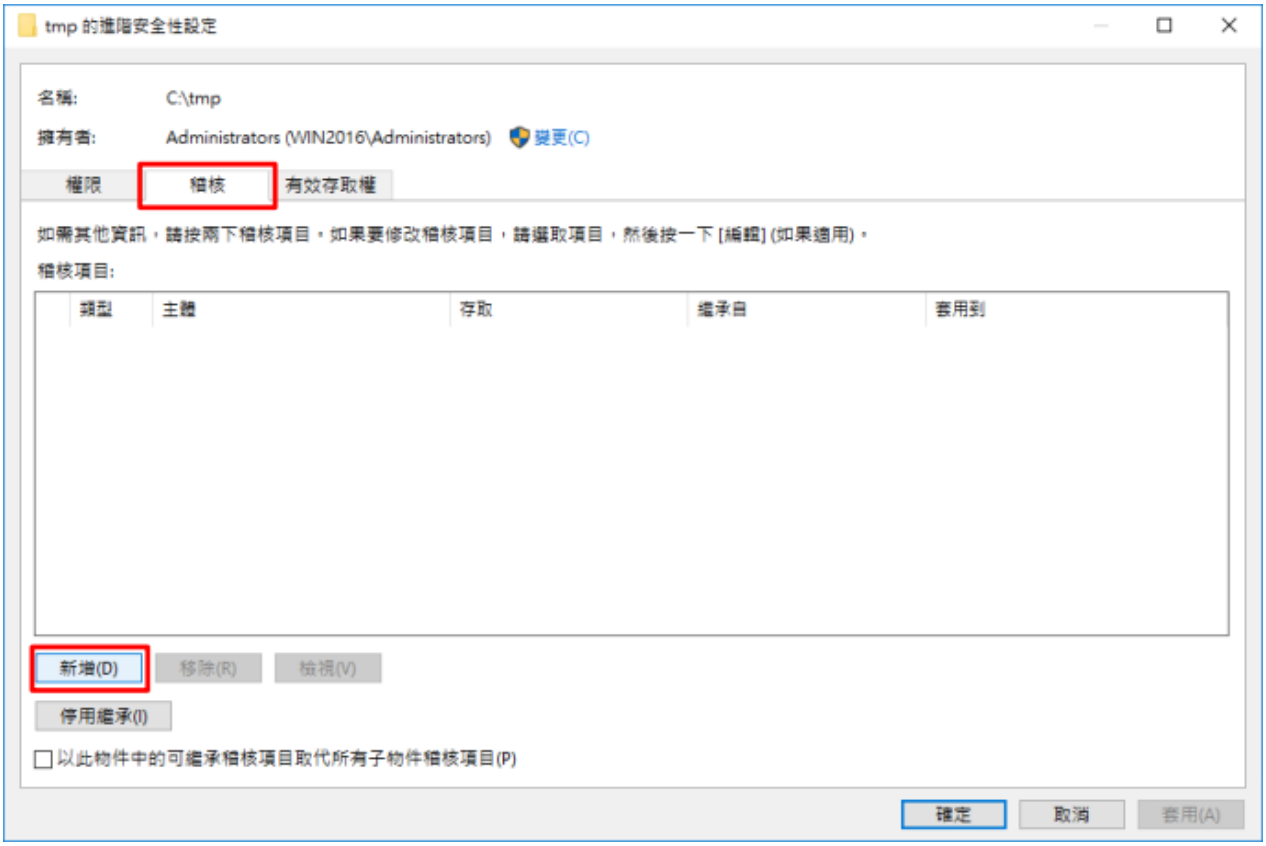
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



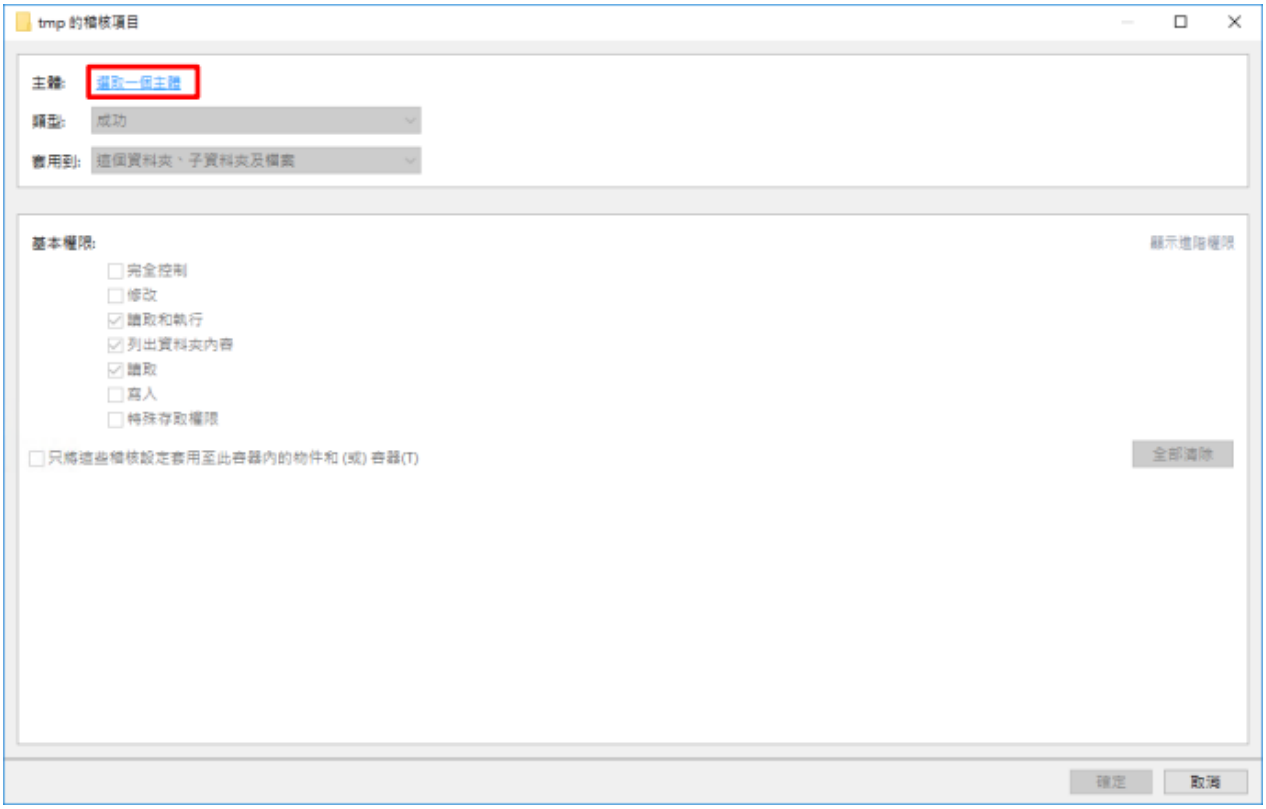
(2) 點選 [安全性] 頁面 -> 按 [進階]



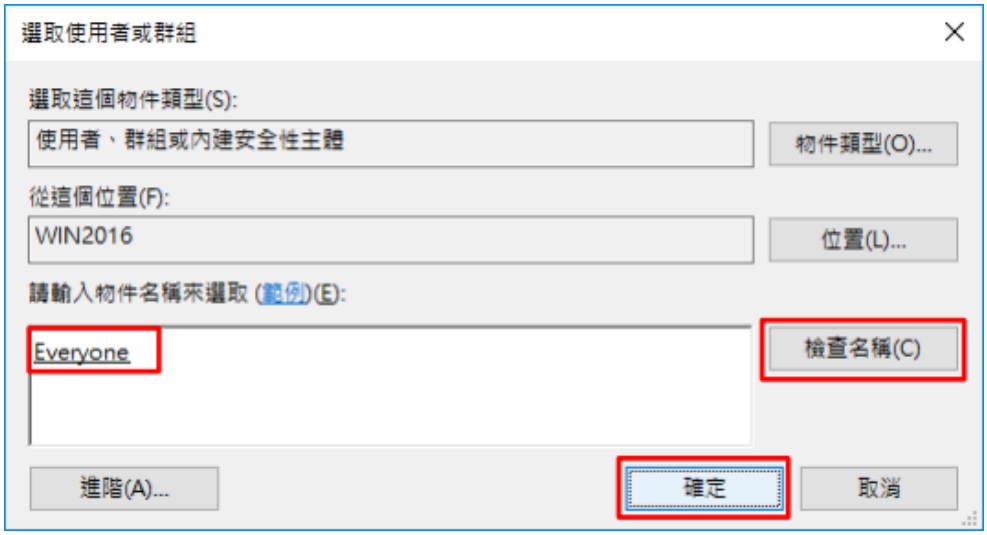
(3) 點選 [稽核] 頁面 -> 按 [新增]



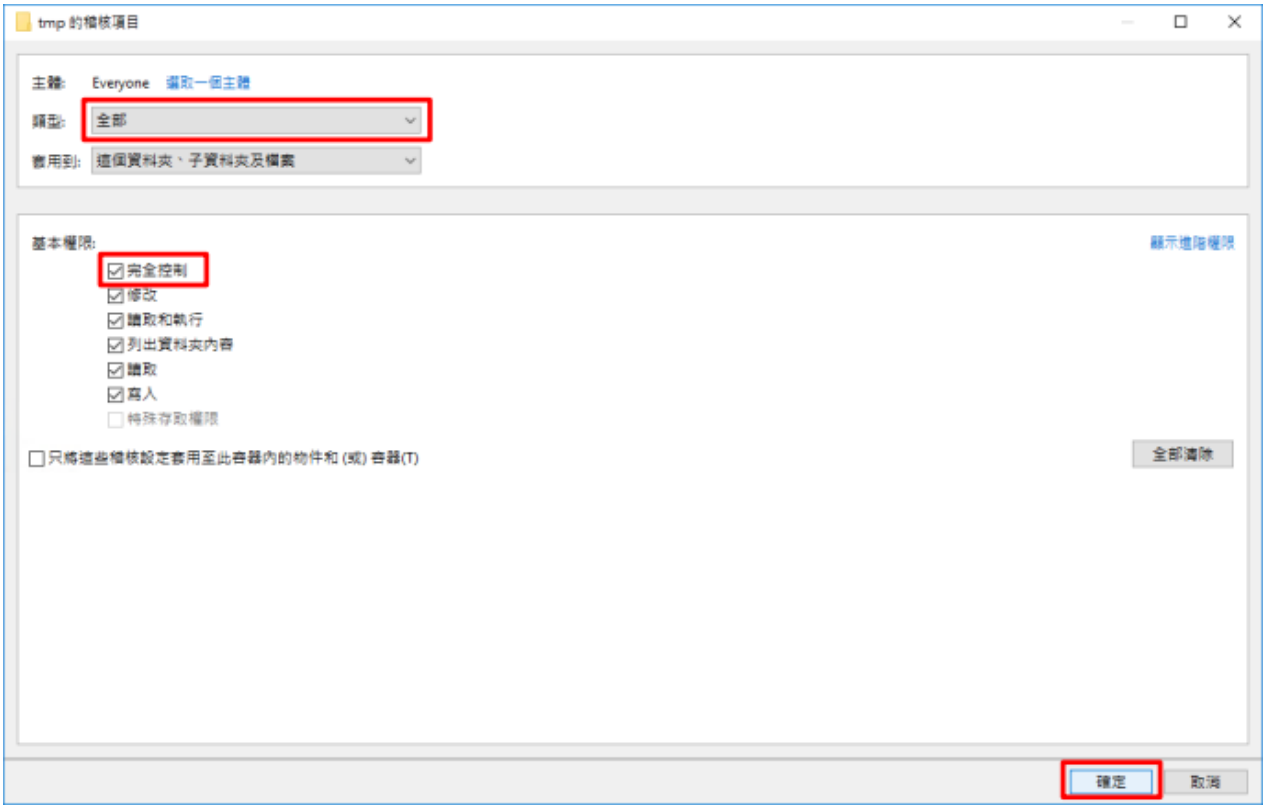
(4) 點選 [選取一個主體]



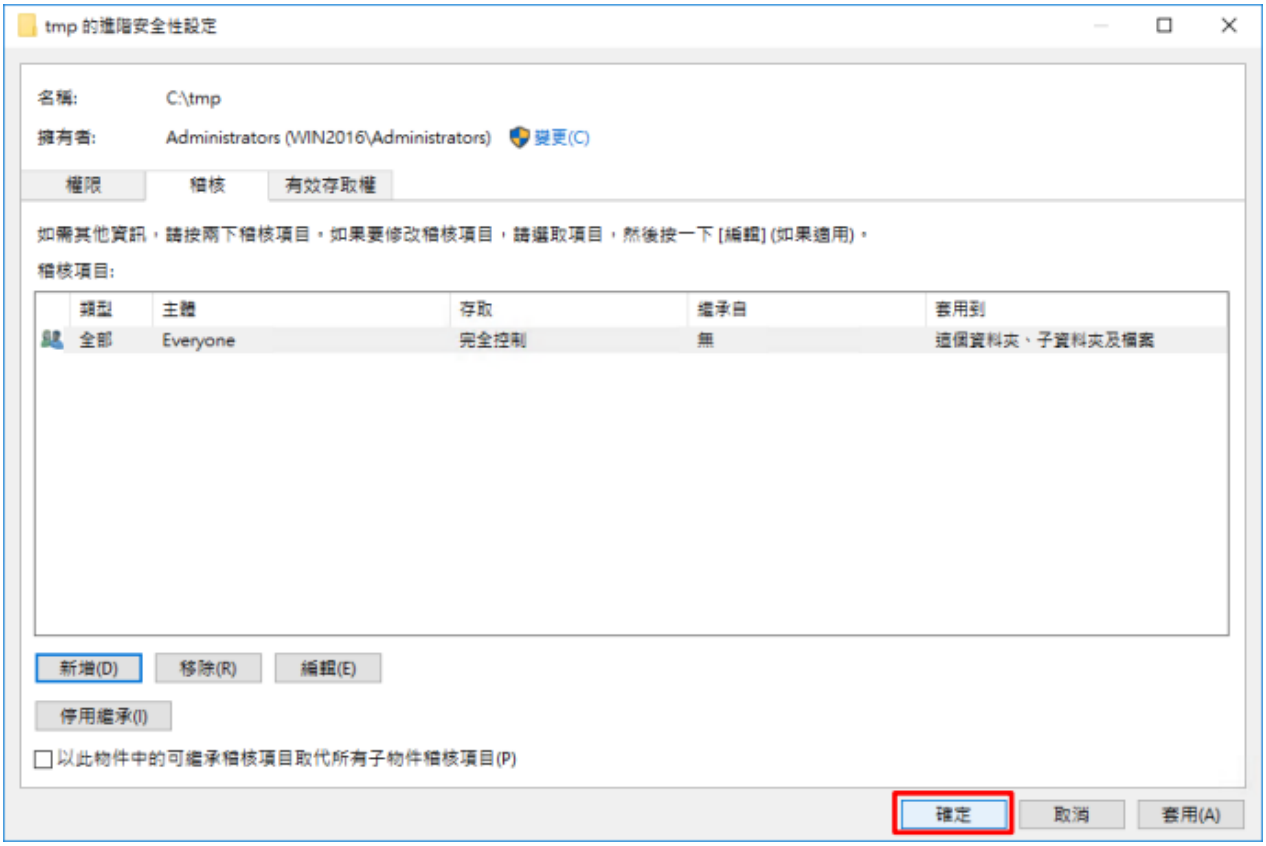
(5) 物件名稱輸入 `Everyone` 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]



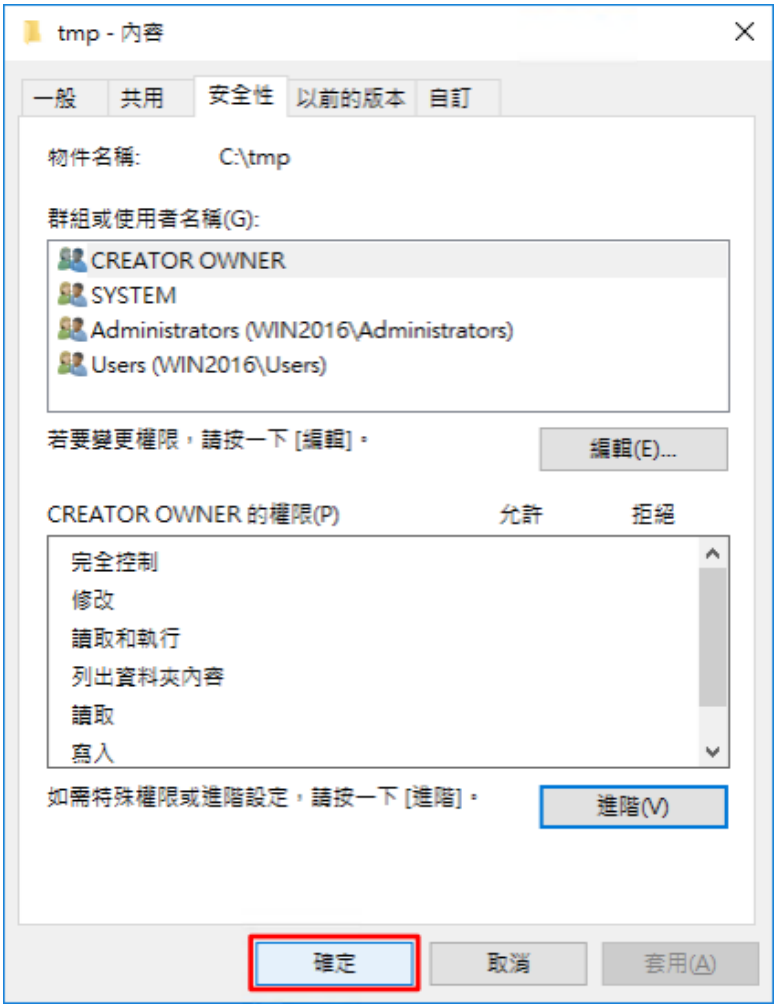
(6) 類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(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

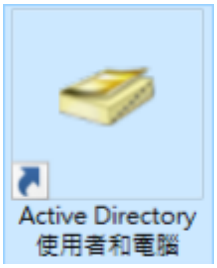
*以下分別為網域和工作群組設定方式。

7.1 網域

7.1.1 組織單位設定

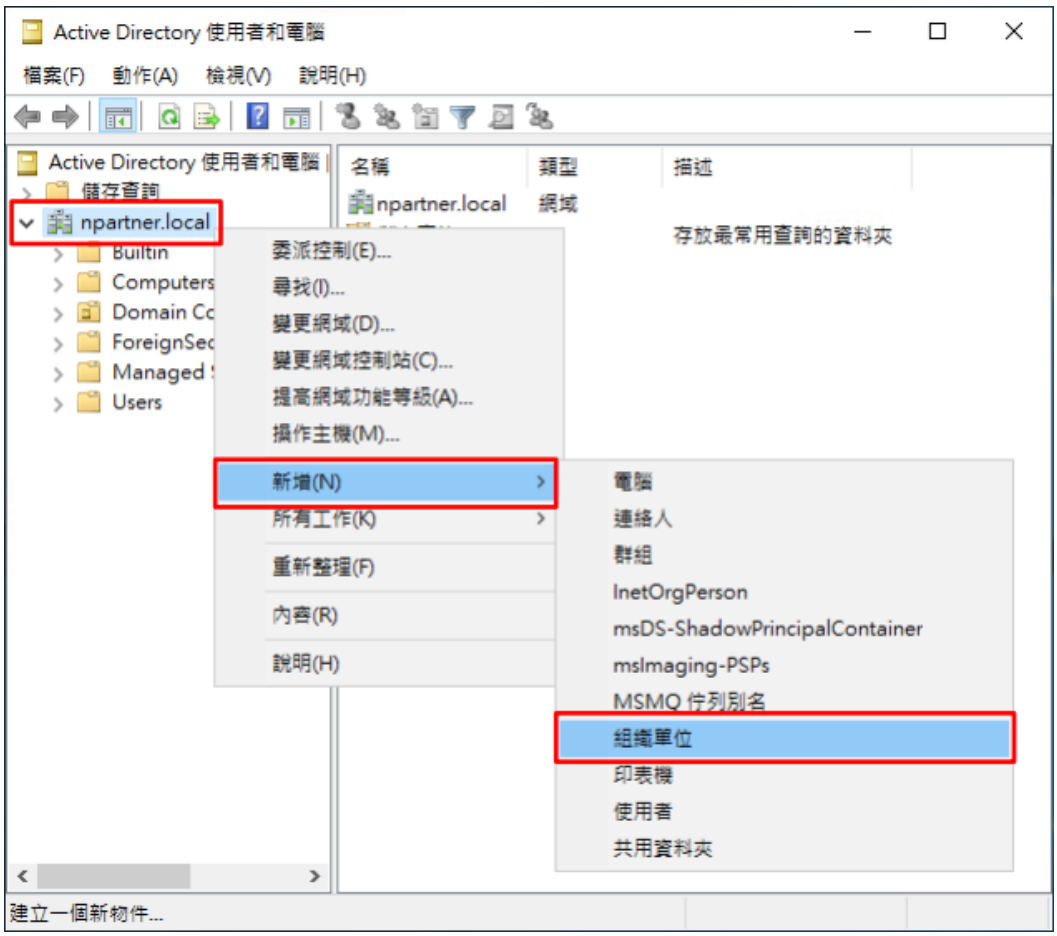
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



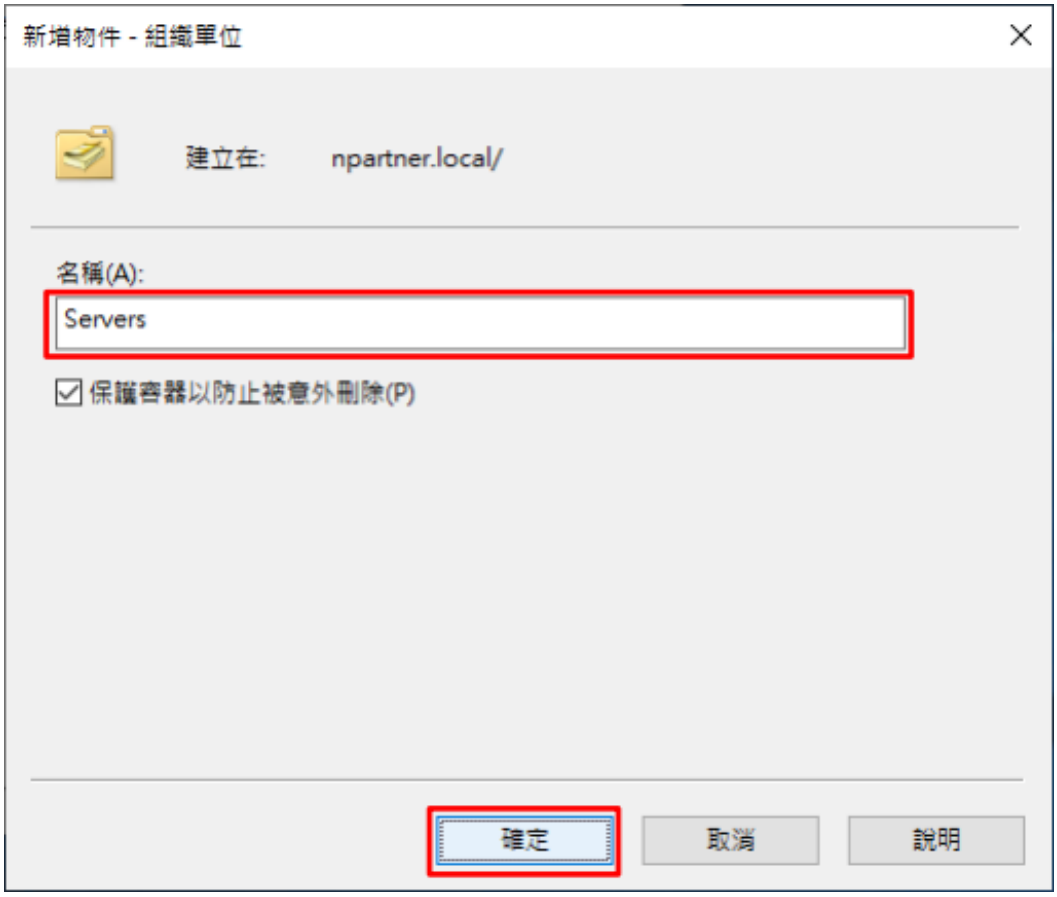
(2) 新增組織單位

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



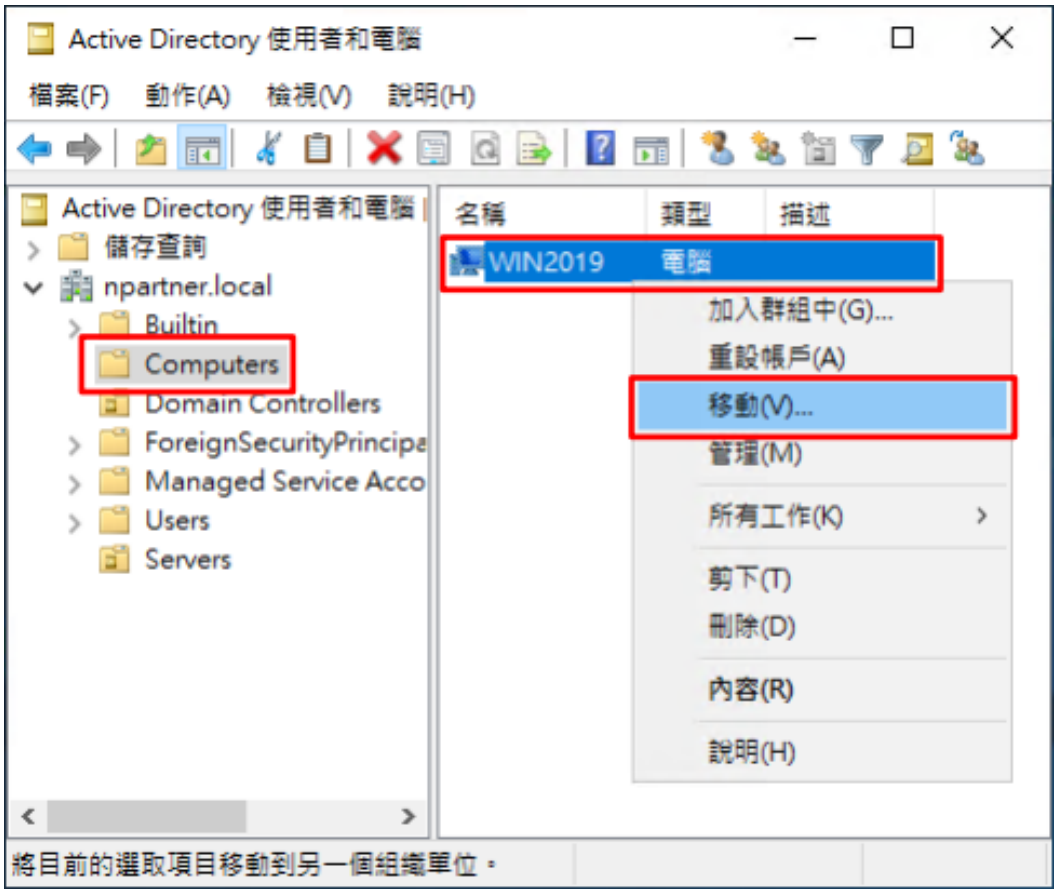
(3)　輸入組織單位名稱

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]



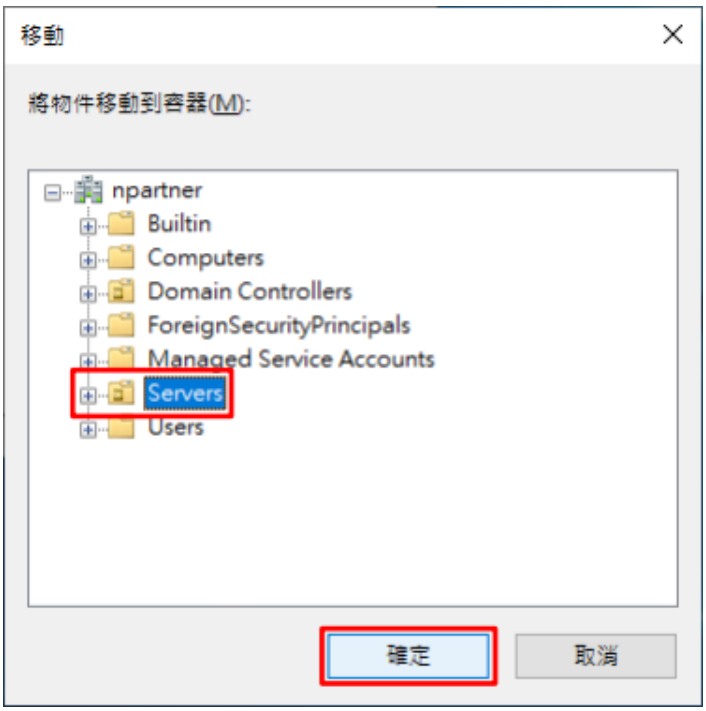
(4) 移動伺服器至新的組織單位

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 主機 -> 點選 [移動]



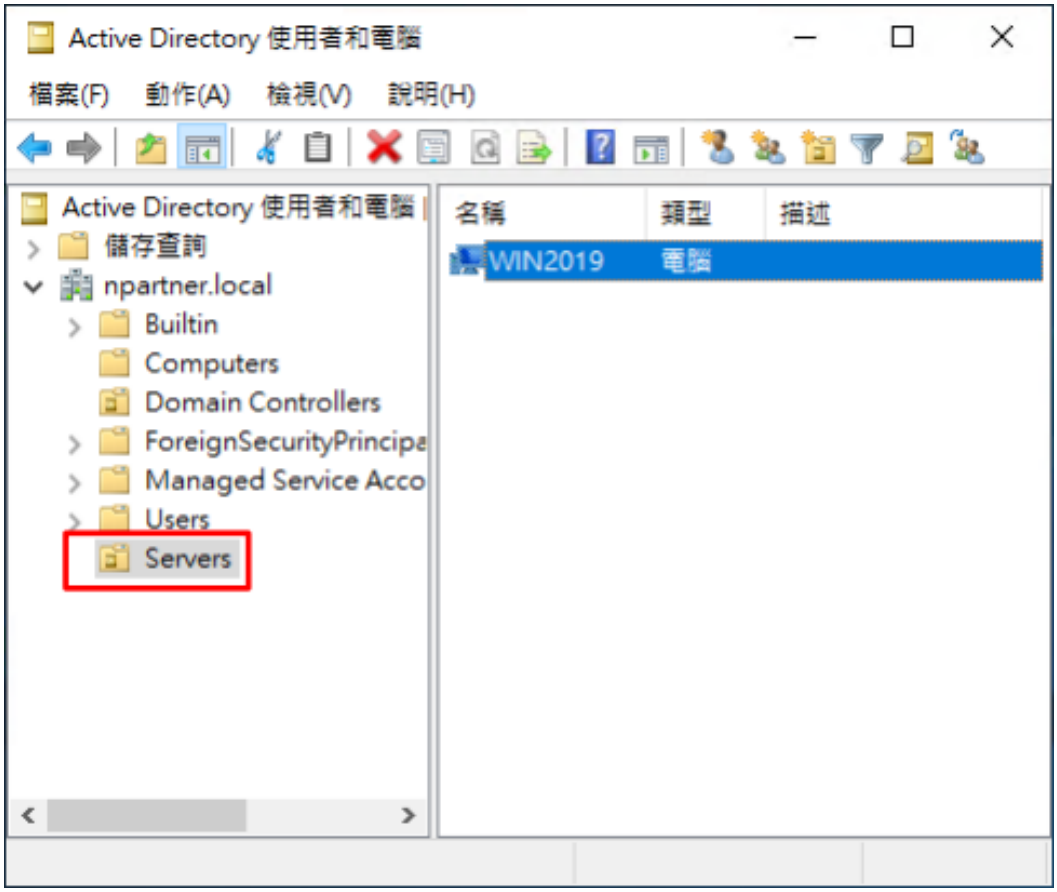
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

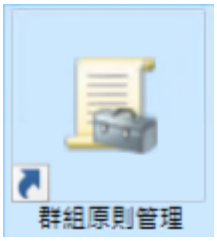
點選 [Servers] 組織單位，確認 Win2019 File 伺服器已移動。



7.1.2 群組原則設定

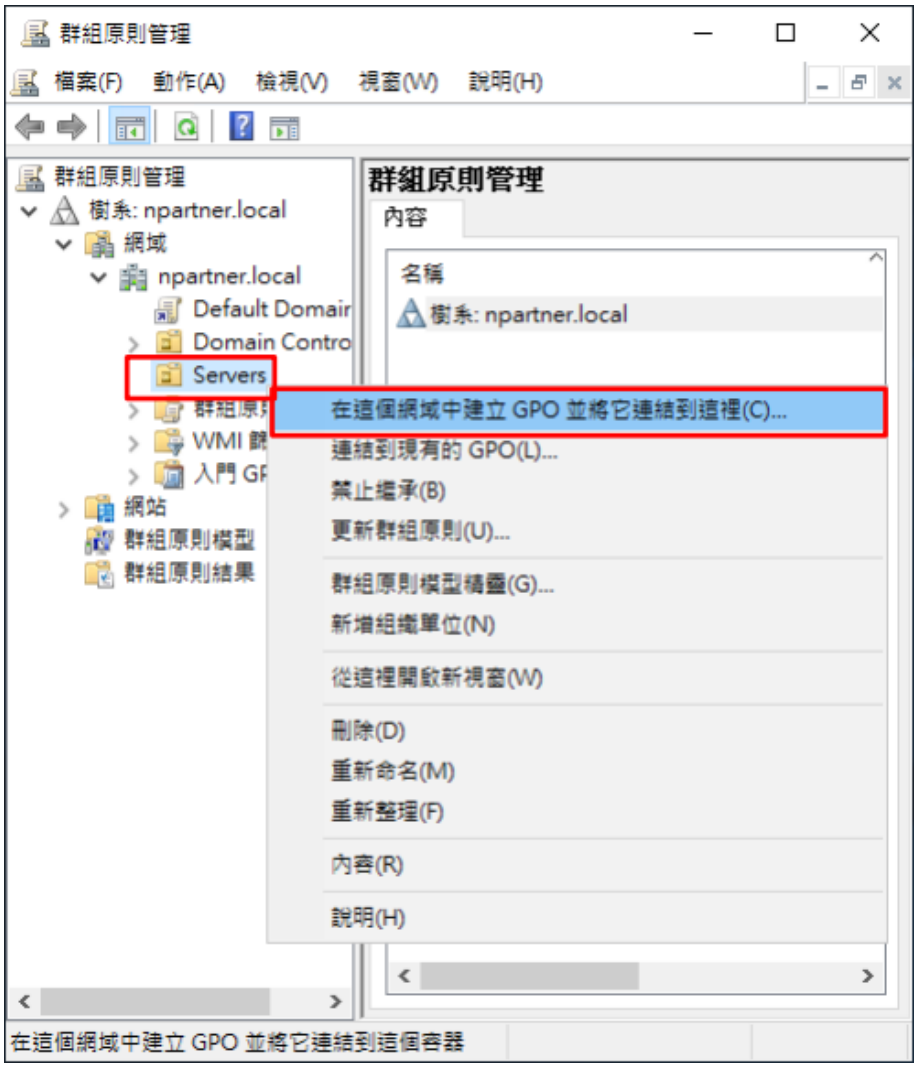
(1) 開啟群組原則管理

開啟 [群組原則管理]



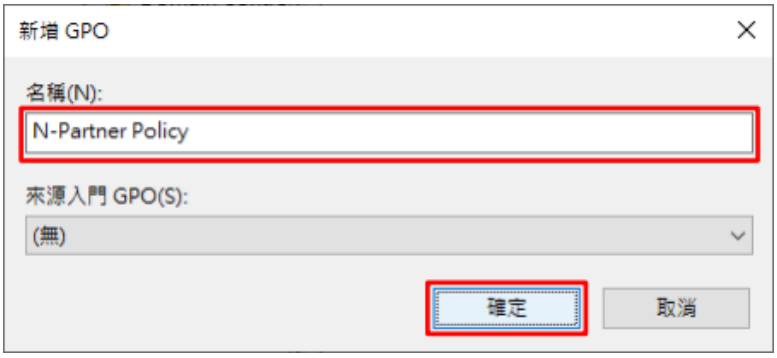
(2) 在 Servers 組織單位，新增群組原則物件

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...]



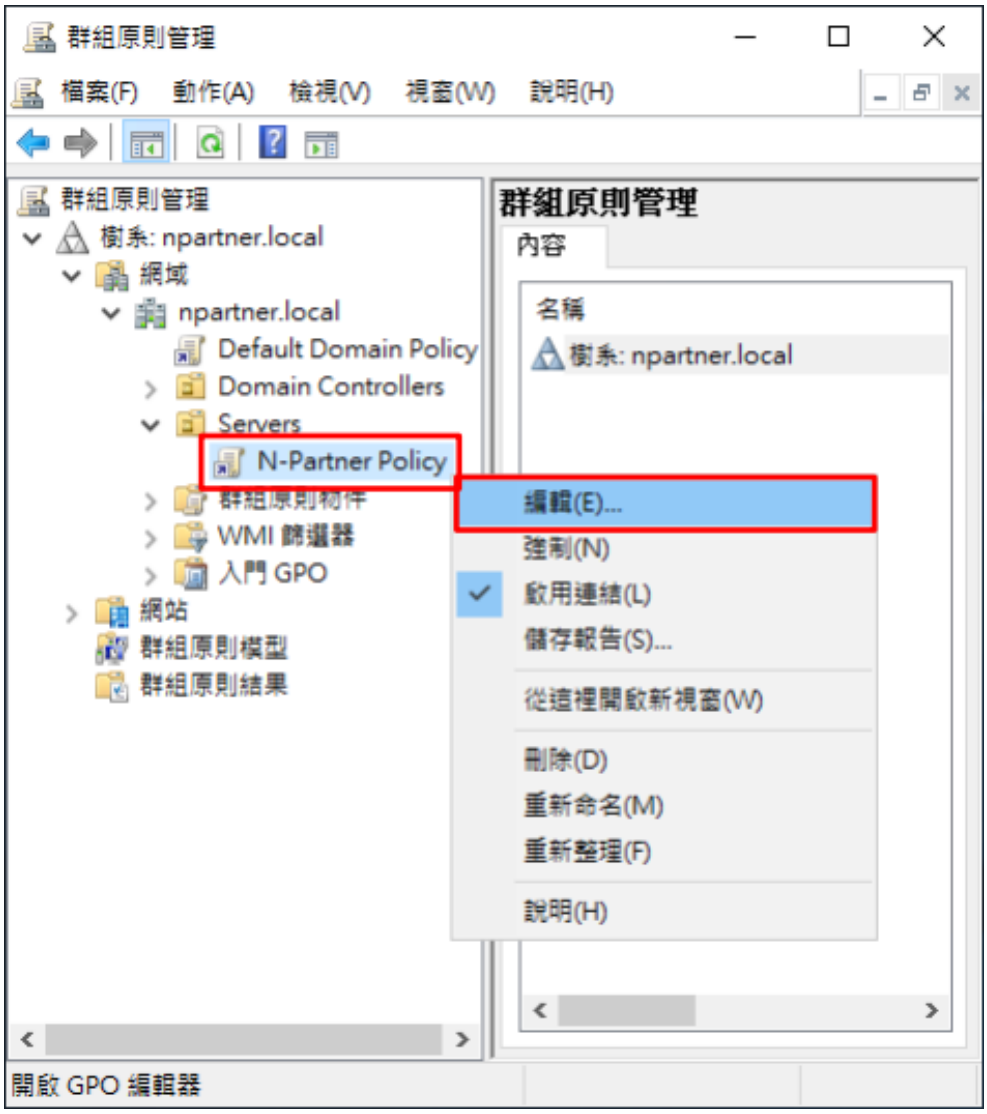
(3) 輸入群組原則物件名稱

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]



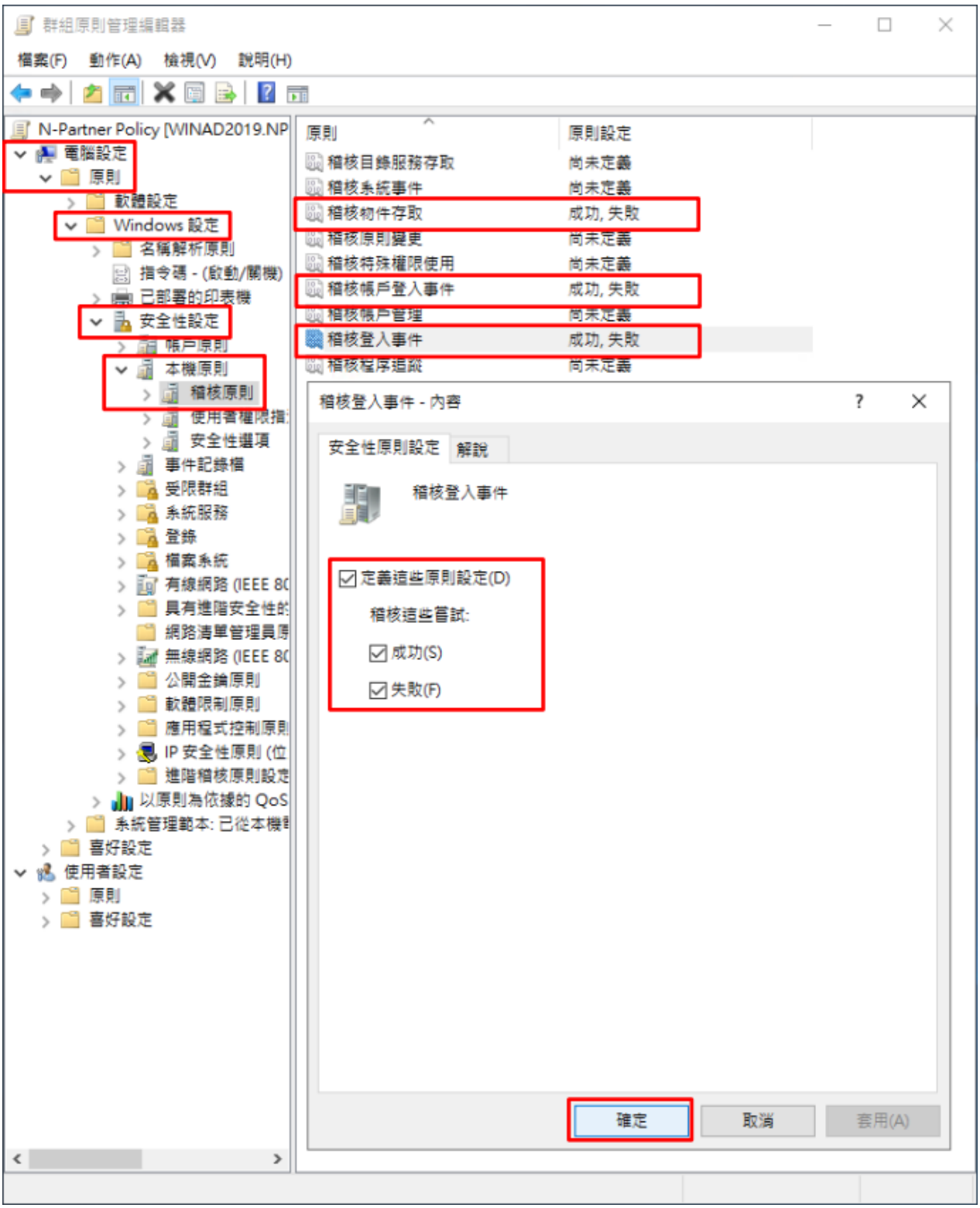
(4) 編輯群組原則物件

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



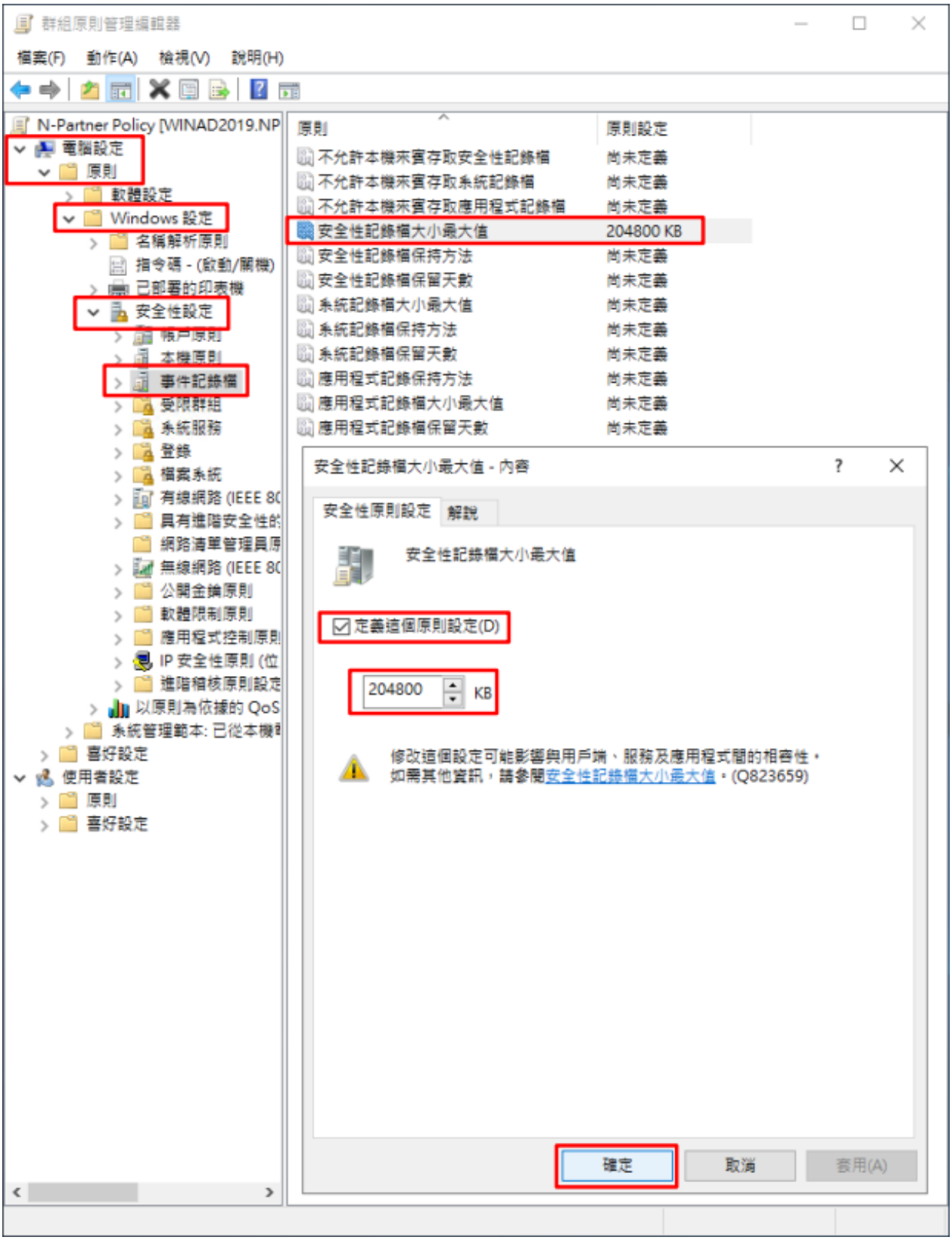
(5) 本機原則：稽核原則

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]



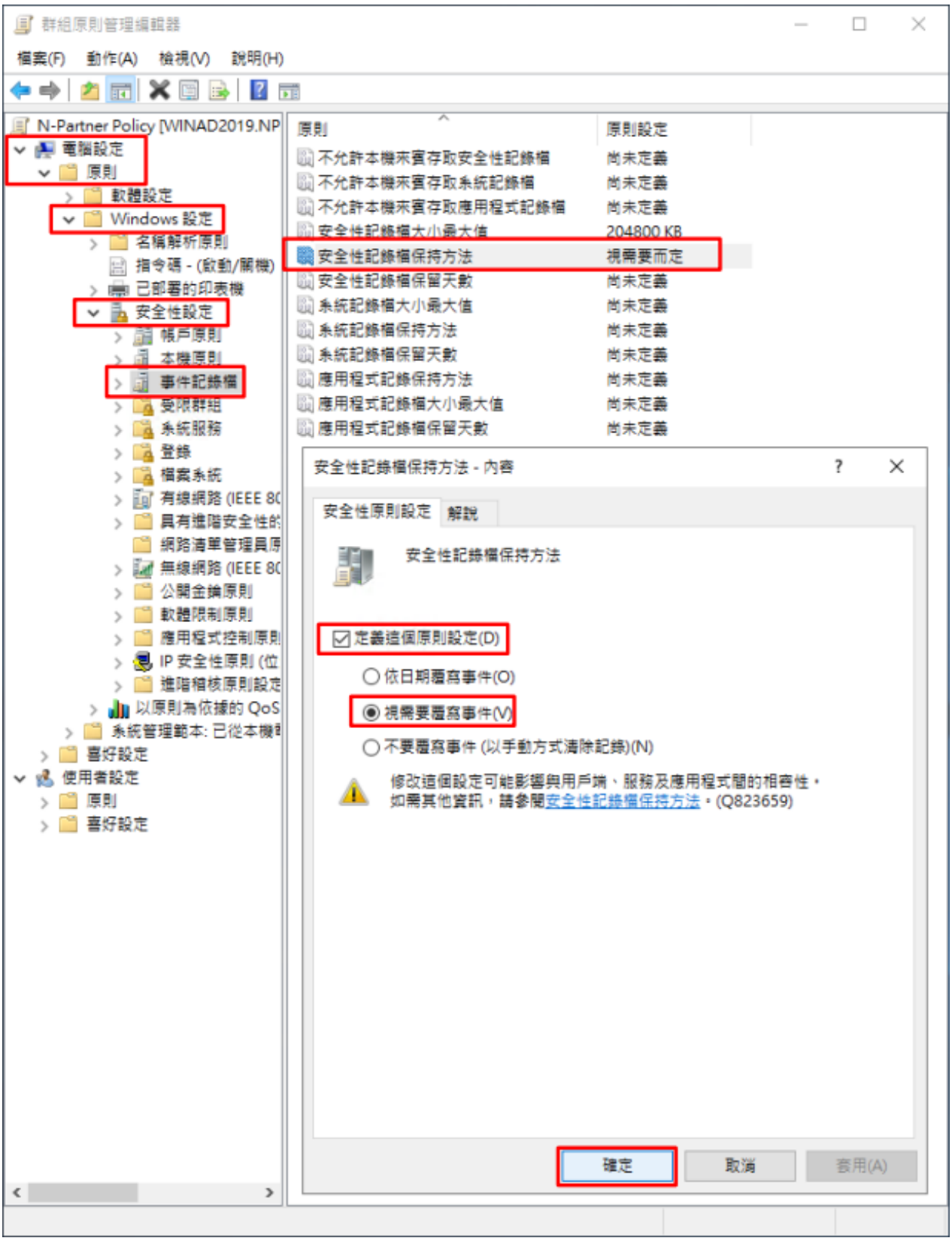
(6)　事件記錄檔：安全性記錄檔大小最大值

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]

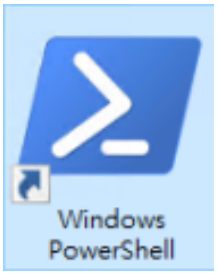


(7) 事件記錄檔：安全性記錄檔保持方法

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]



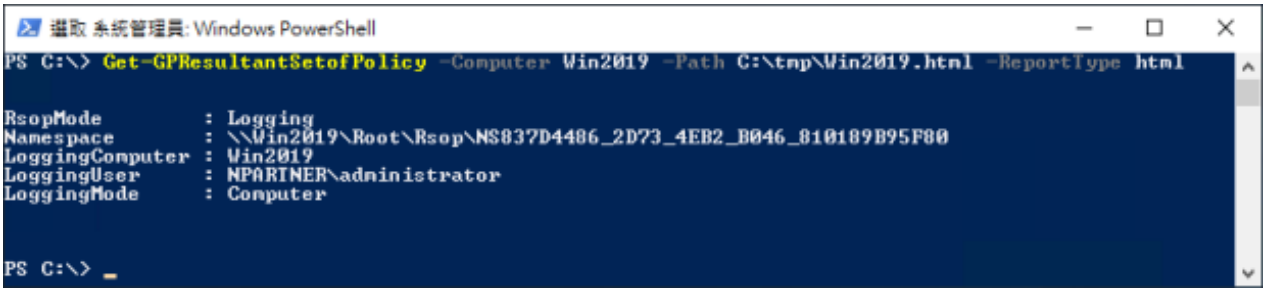
(9) 更新 Windows File 伺服器群組原則

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

紅色文字部位請輸入 Windows File 伺服器名

(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
```



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

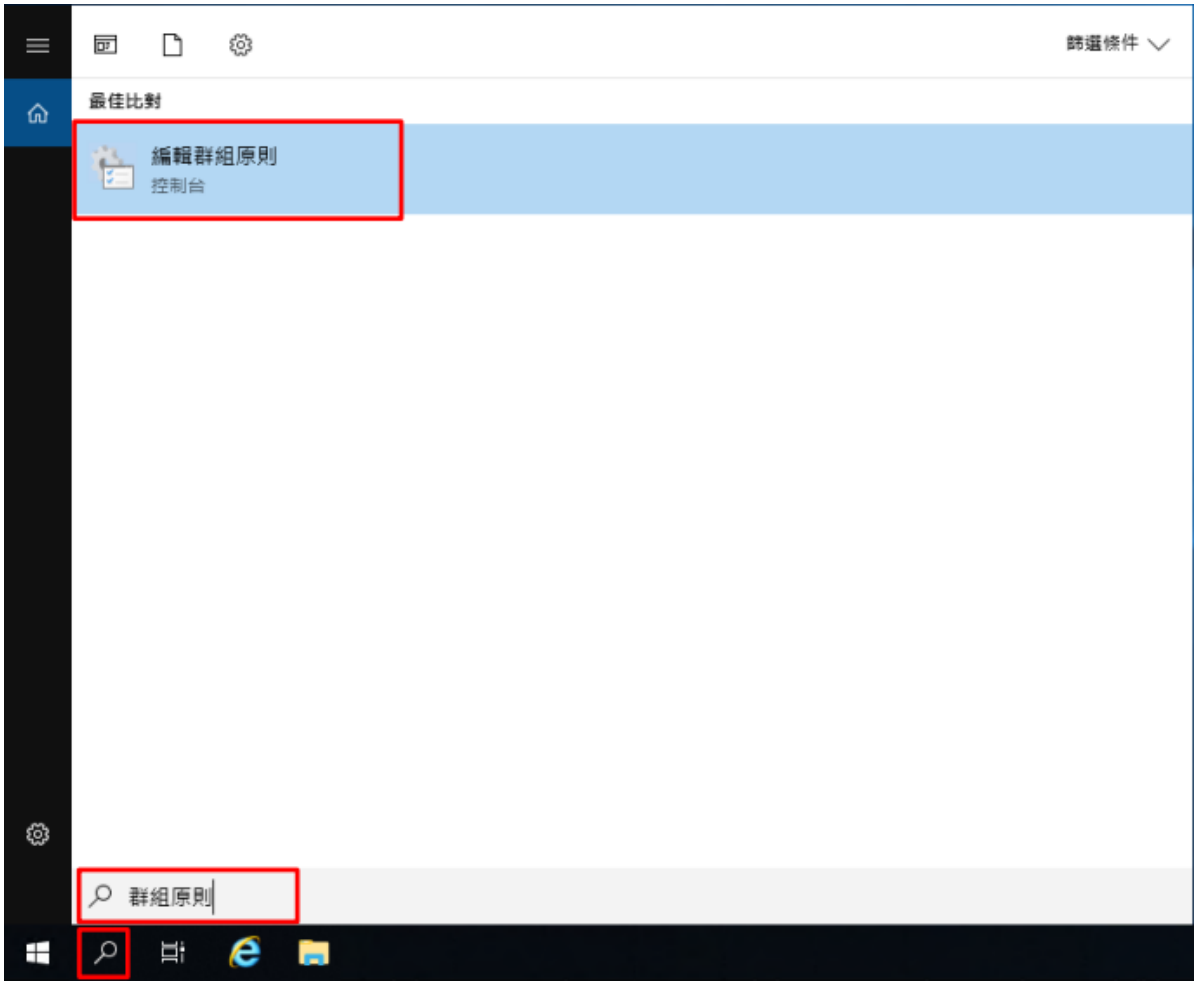
(11) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則

7.2 工作群組

7.2.1 稽核原則設定

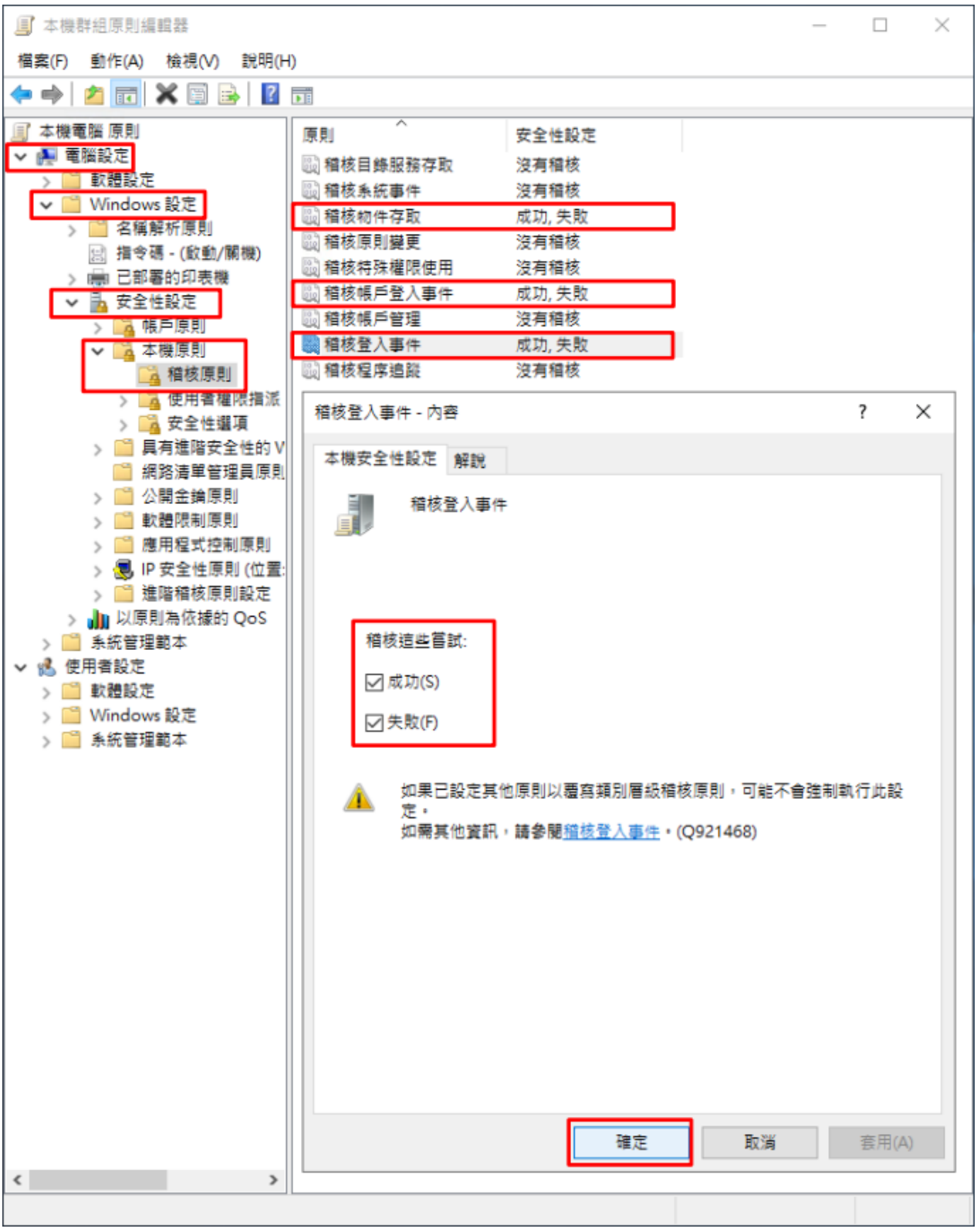
(1) 開啟本機群組原則編輯器

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

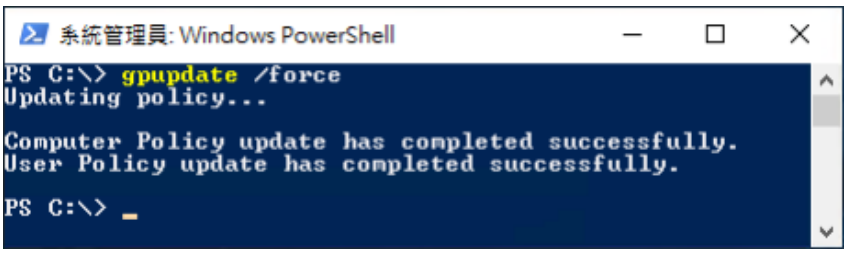
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核物件存取], [稽核帳戶登入事件], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

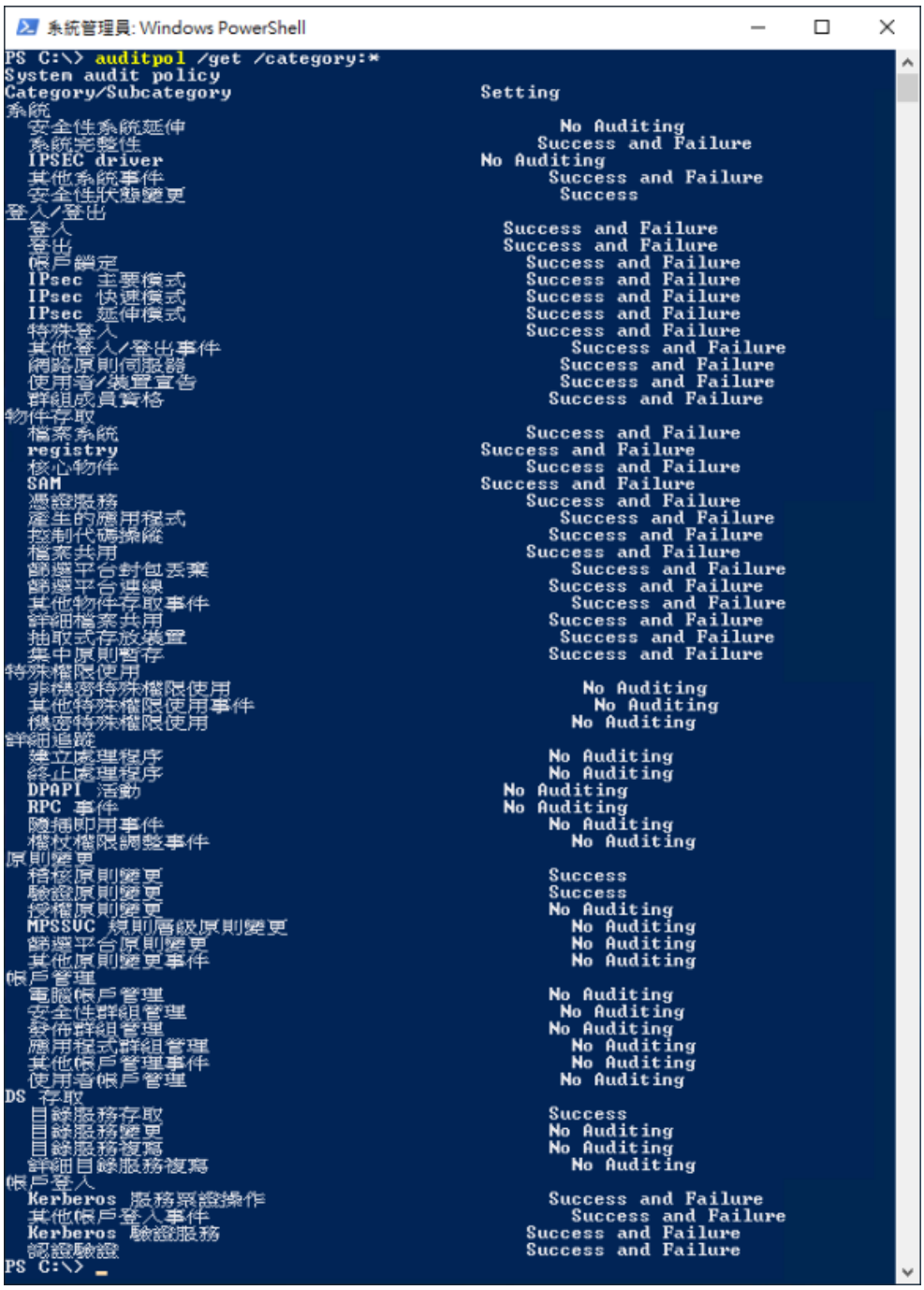
(4) 更新群組原則

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



(5) 查看群組原則套用情形

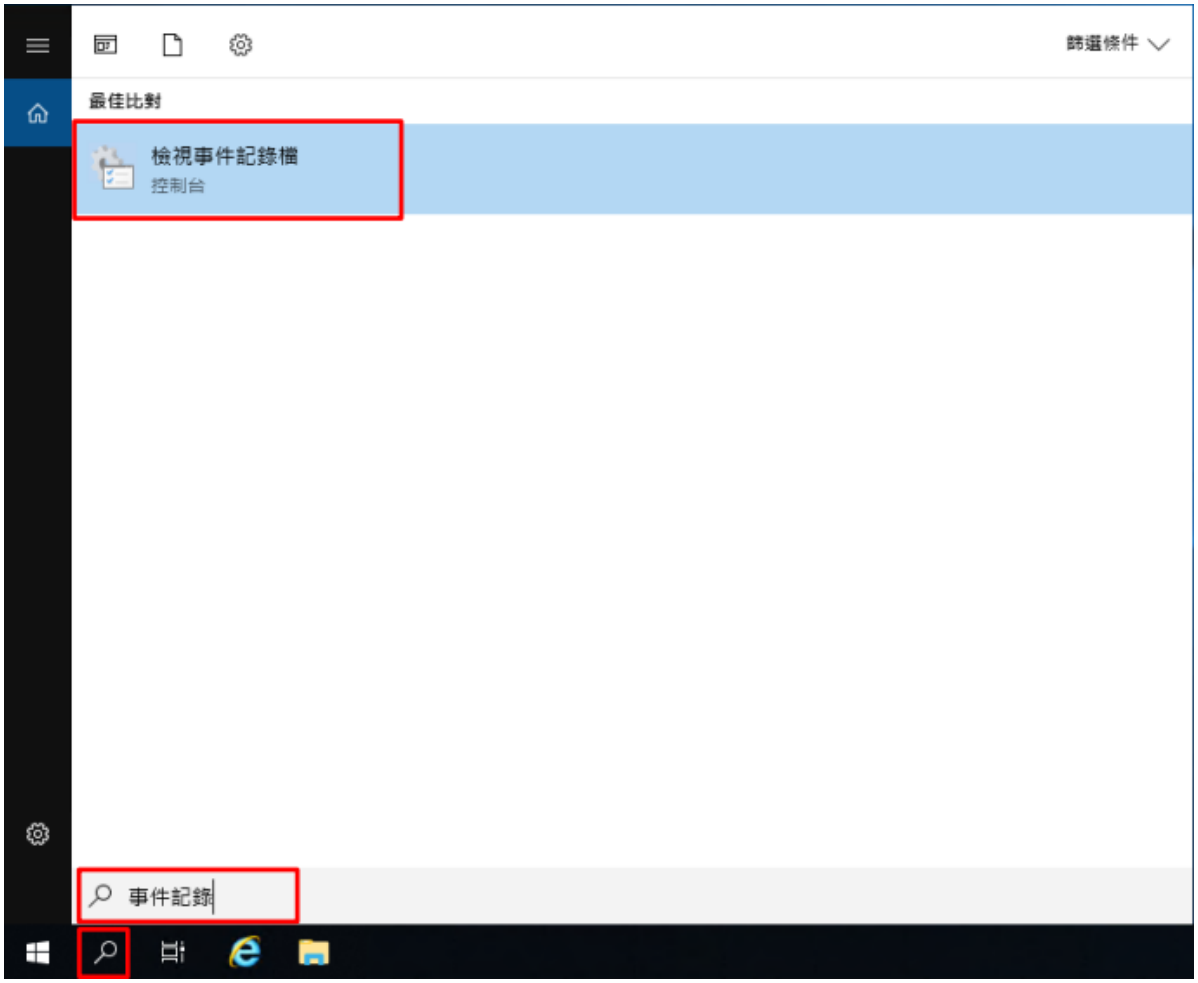
```
PS C:\> auditpol /get /category:*
```



7.2.2 事件檔案設定

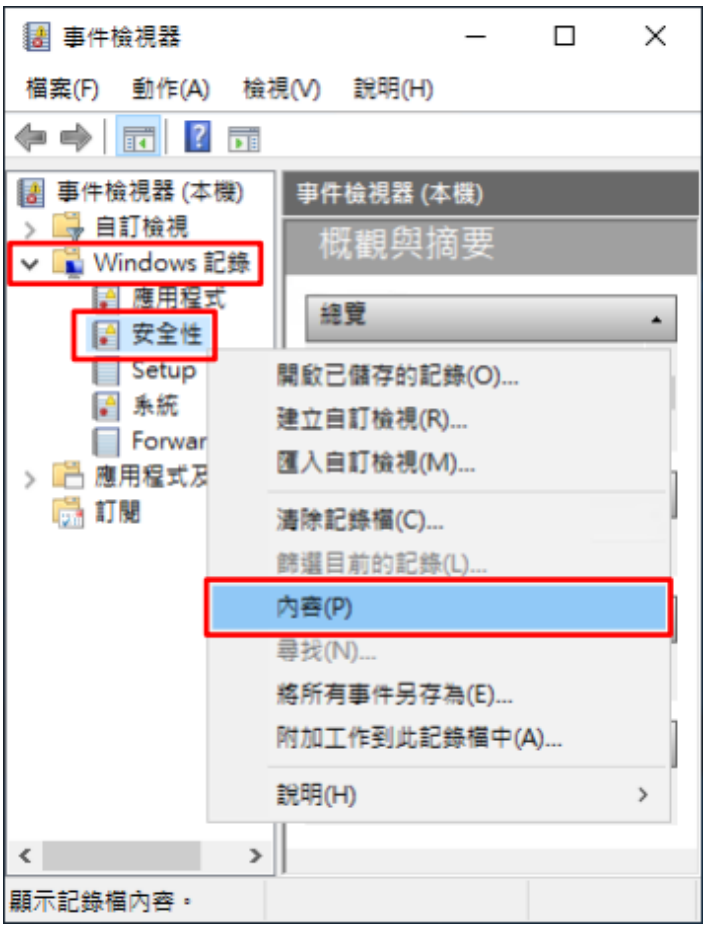
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入 事件記錄 -> 點選 [檢視事件記錄檔]



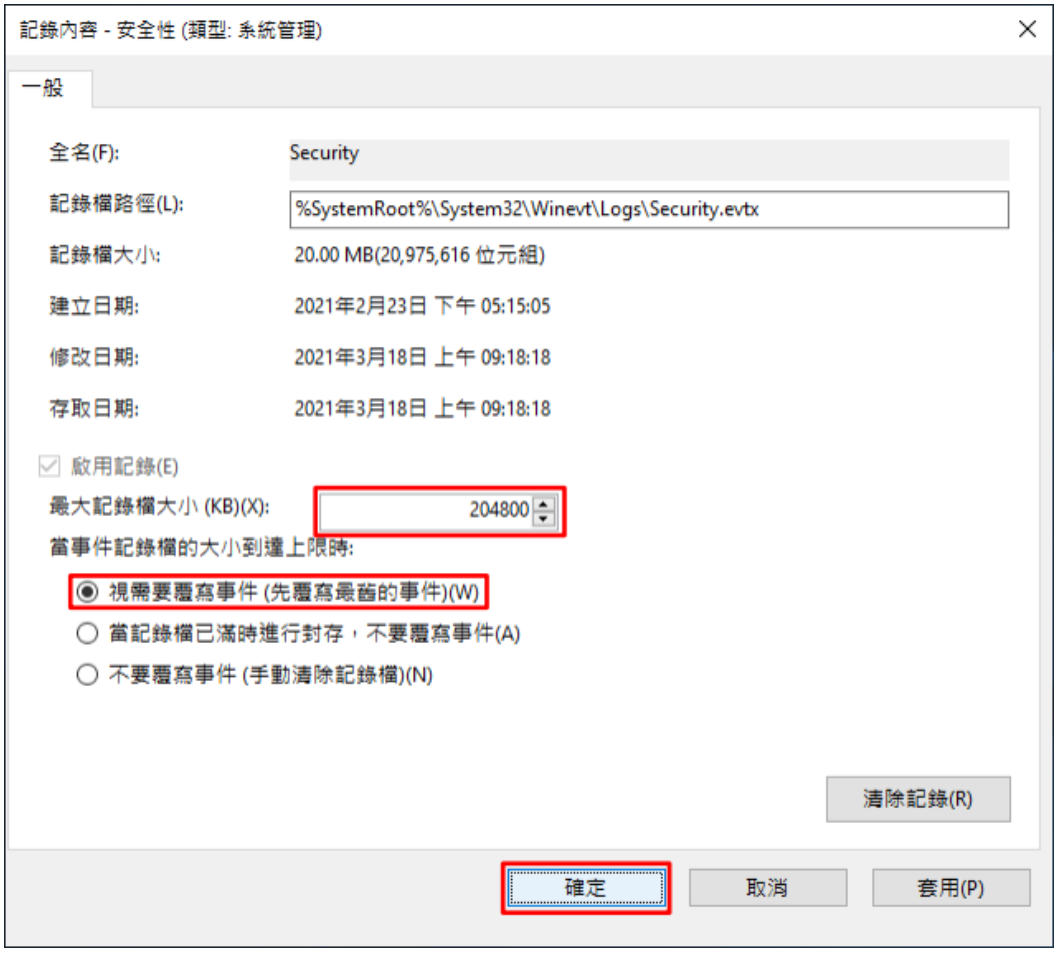
(2) 編輯安全性記錄

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



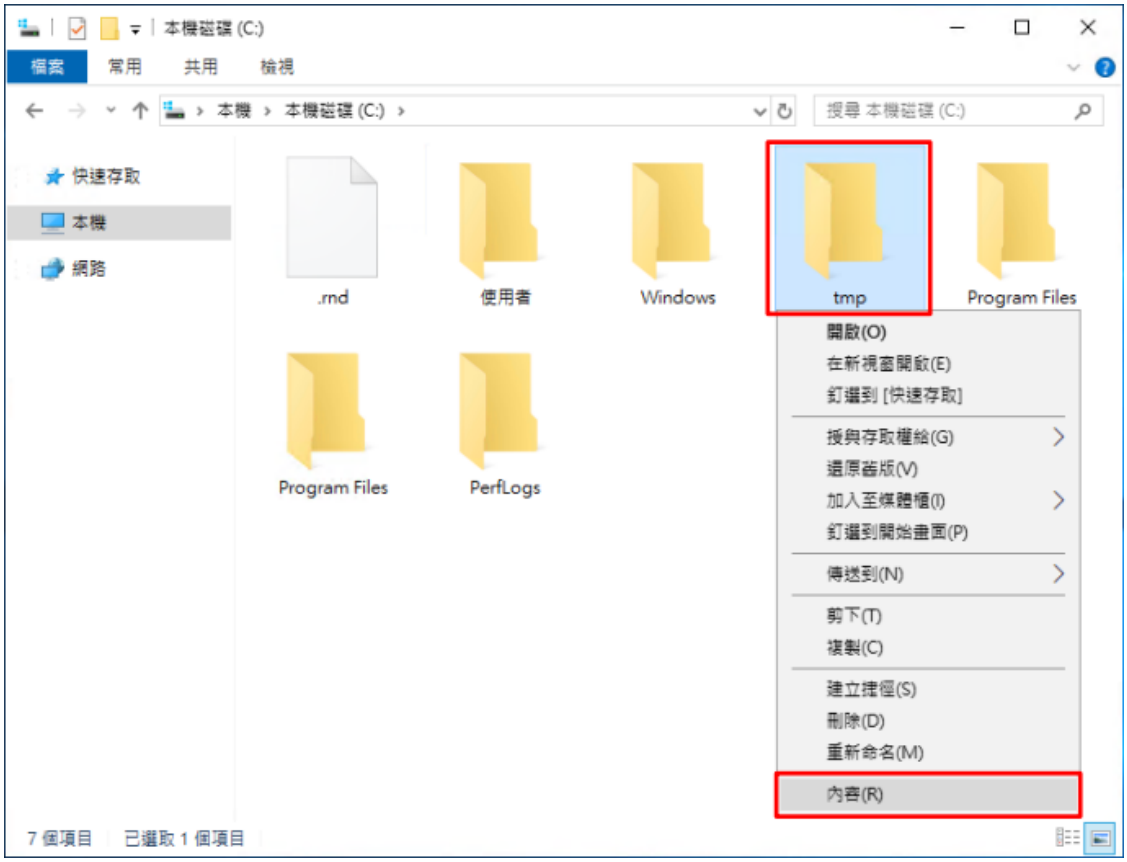
(3) 設定安全性記錄檔

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]

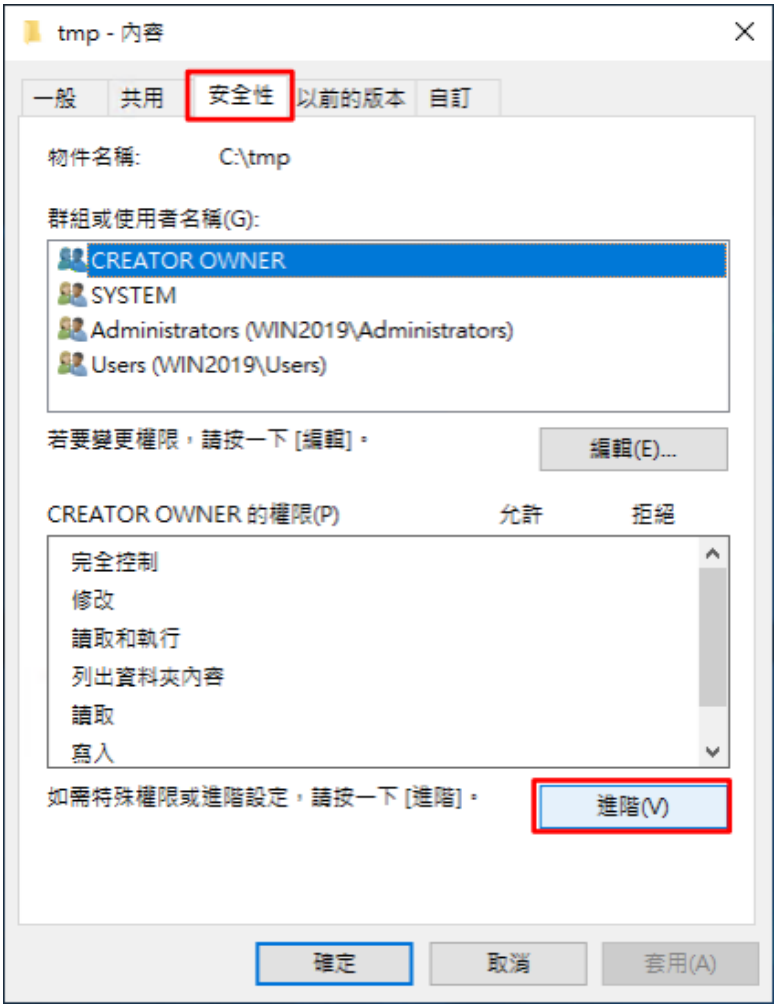


7.3 稽核資料夾設定

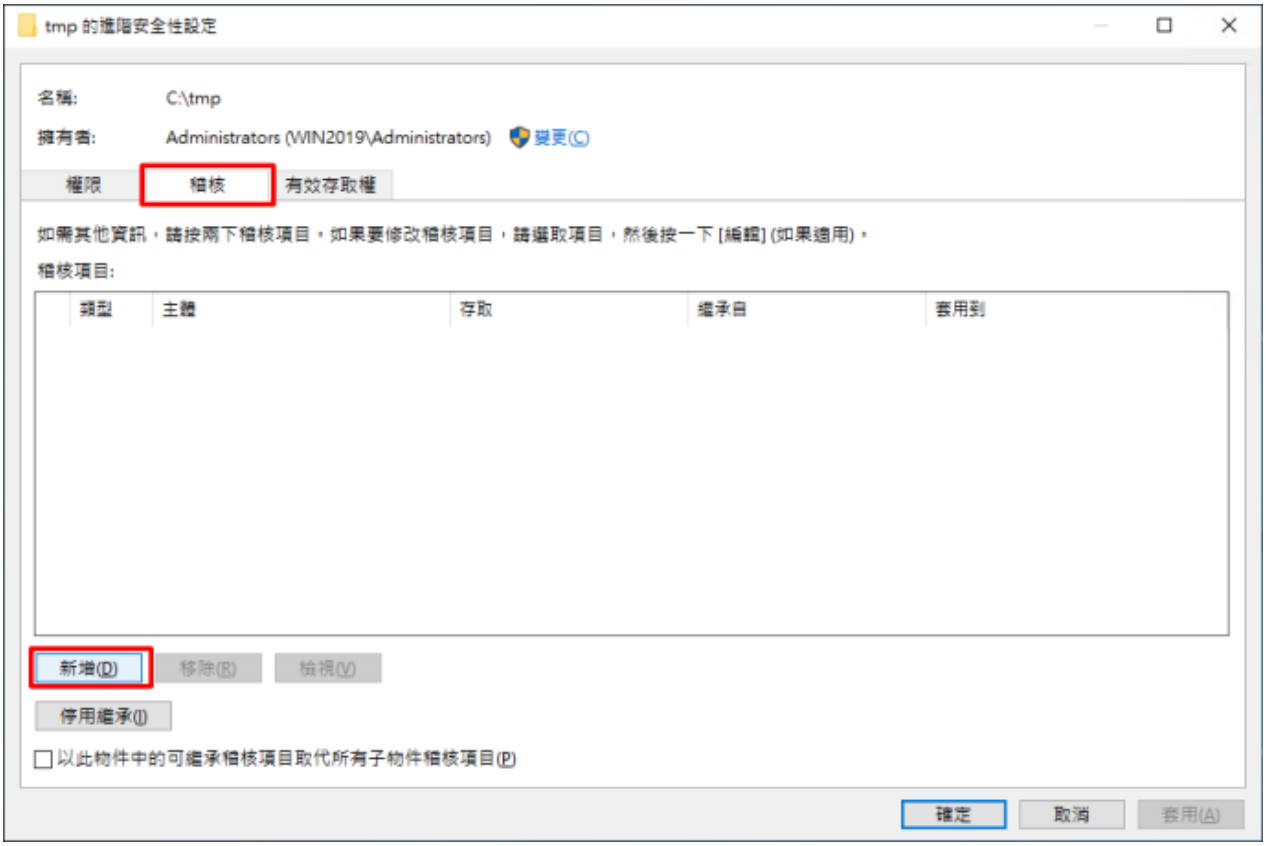
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



(2) 點選 [安全性] 頁面 -> 按 [進階]



(3) 點選 [稽核] 頁面 -> 按 [新增]

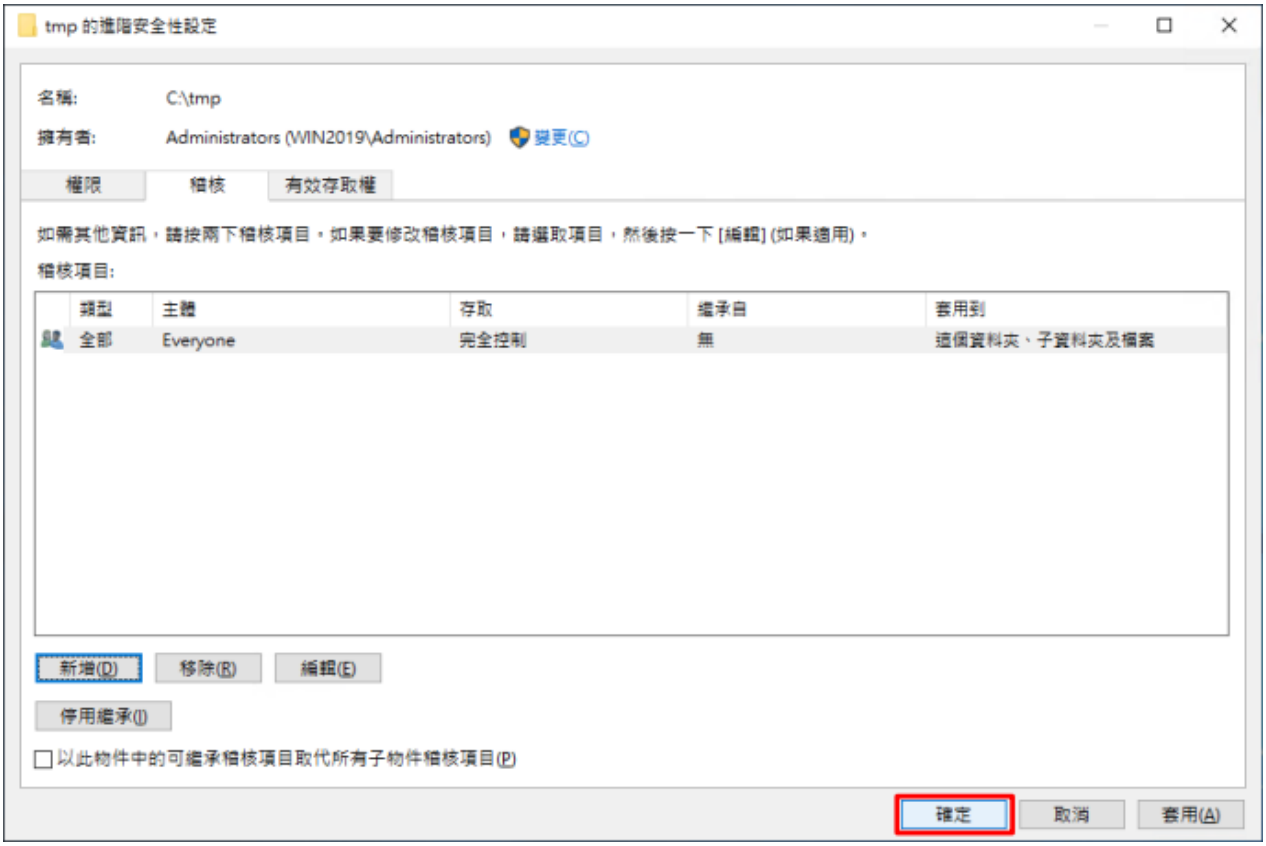


(4) 點選 [選取一個主體]

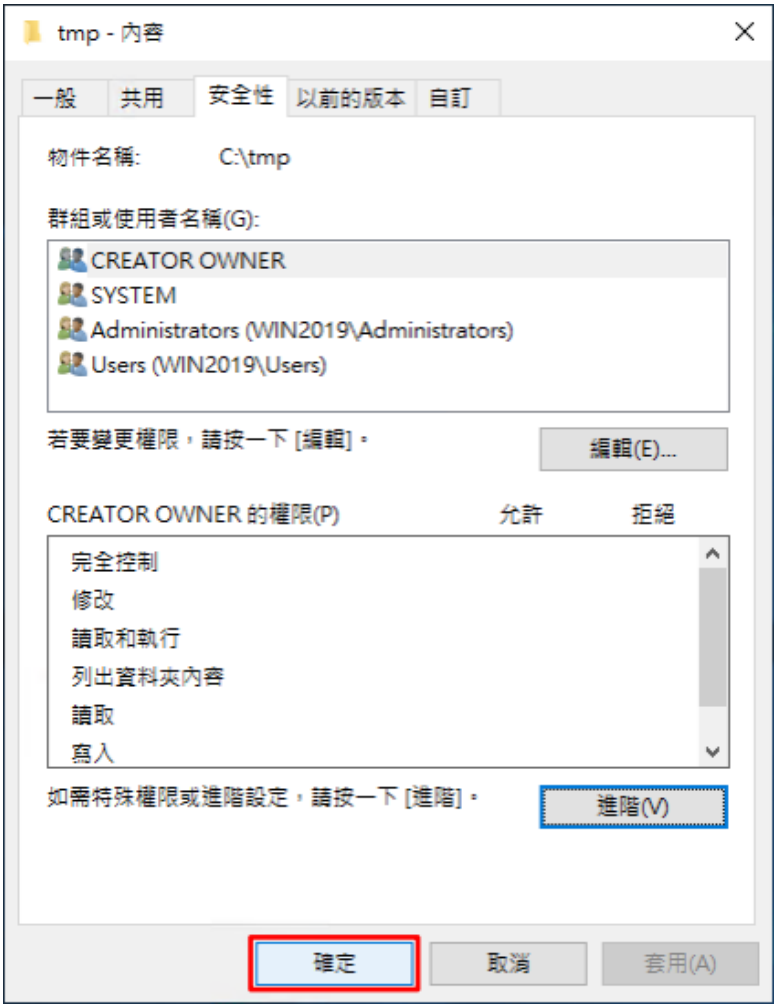
(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

(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

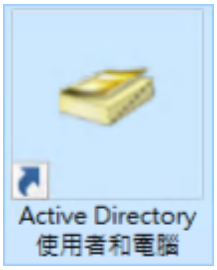
*以下分別為網域和工作群組設定方式。

8.1 網域

8.1.1 組織單位設定

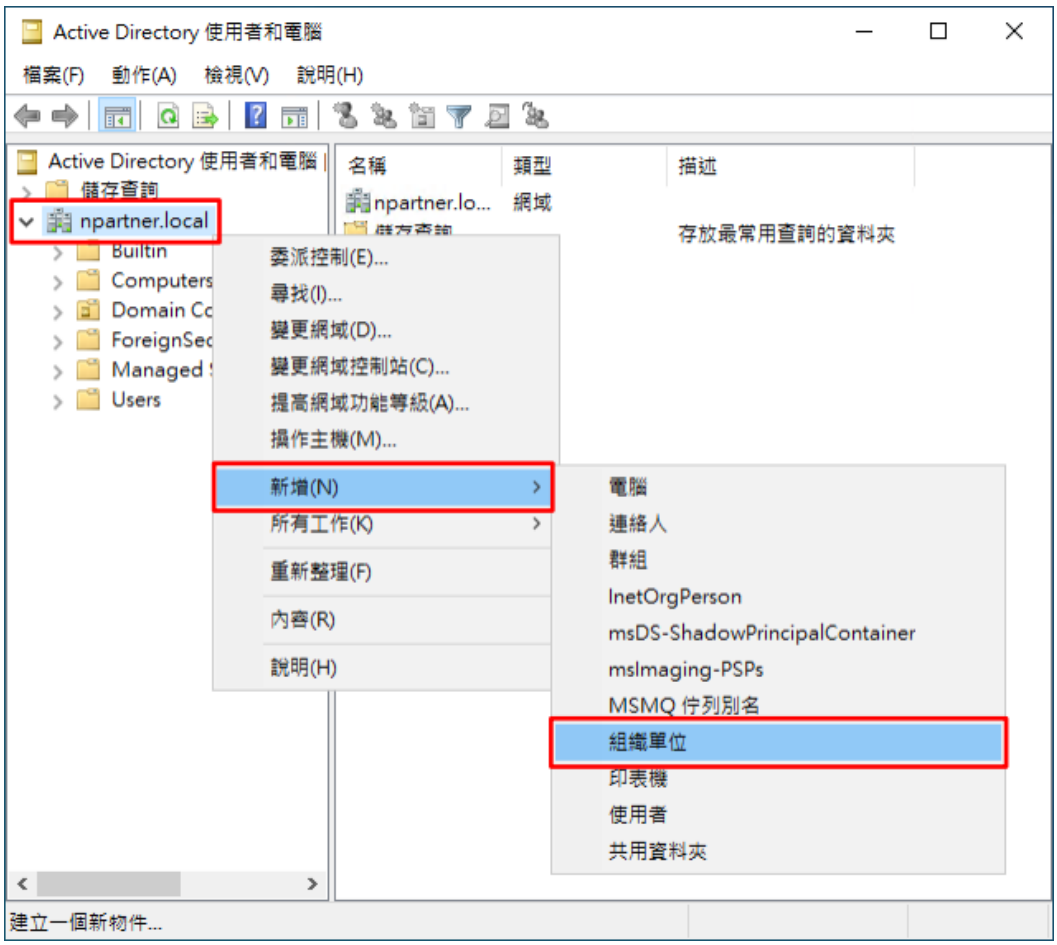
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



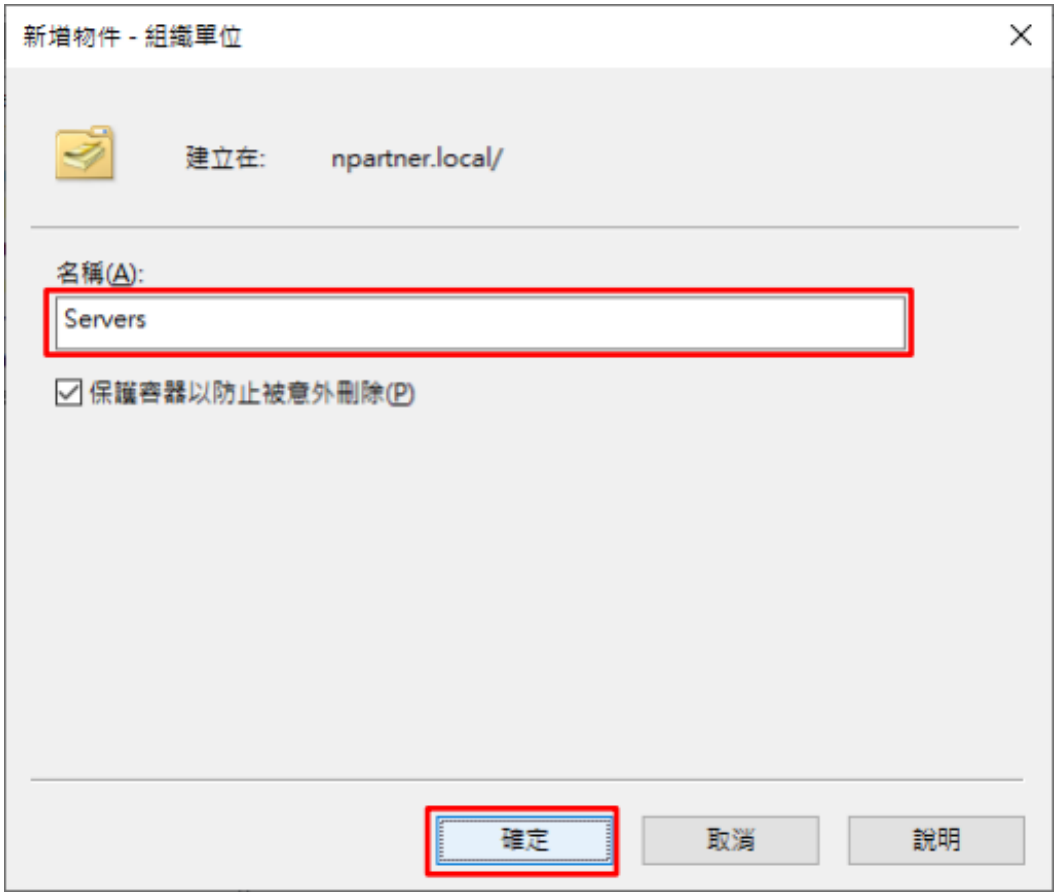
(2) 新增組織單位

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



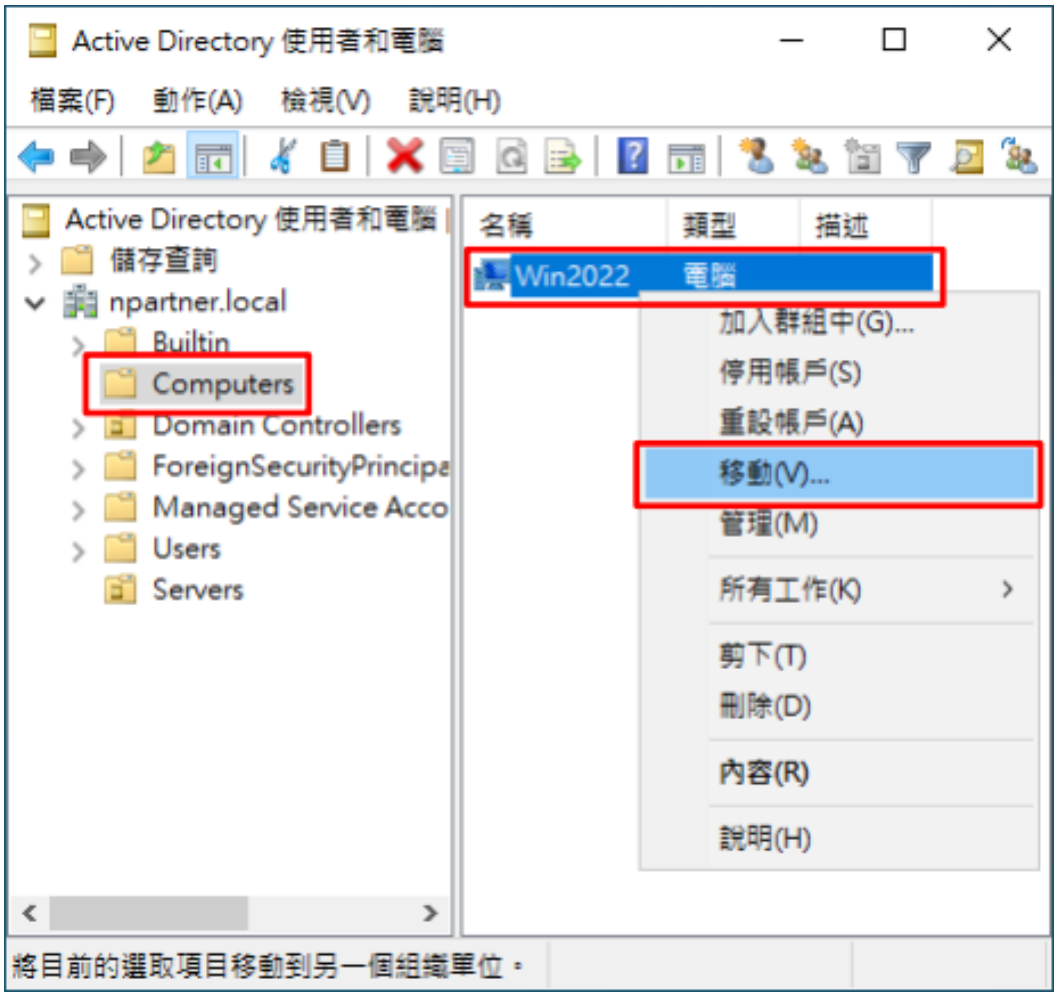
(3)　輸入組織單位名稱

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]



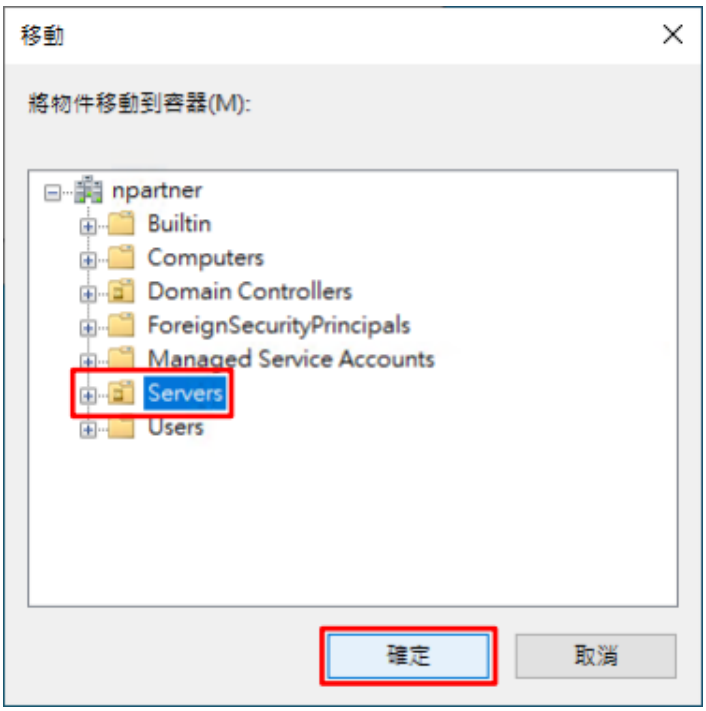
(4) 移動伺服器至新的組織單位

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 主機 -> 點選 [移動]



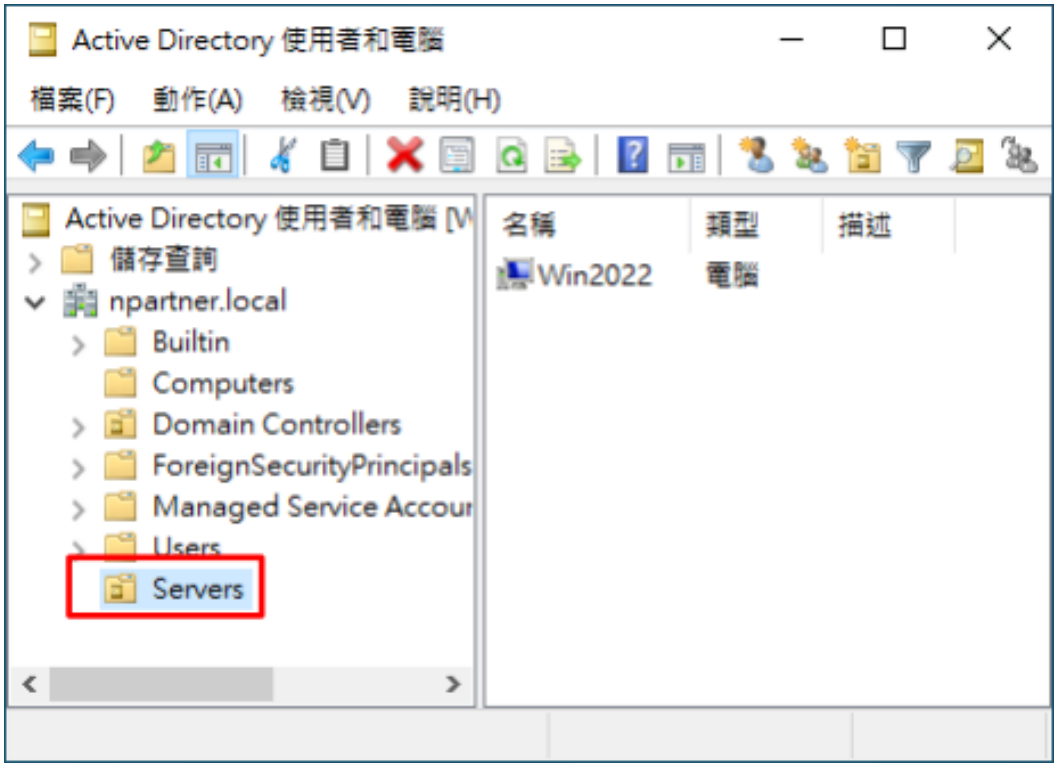
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

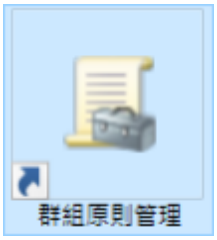
點選 [Servers] 組織單位，確認 Win2022 File 伺服器已移動。



8.1.2 群組原則設定

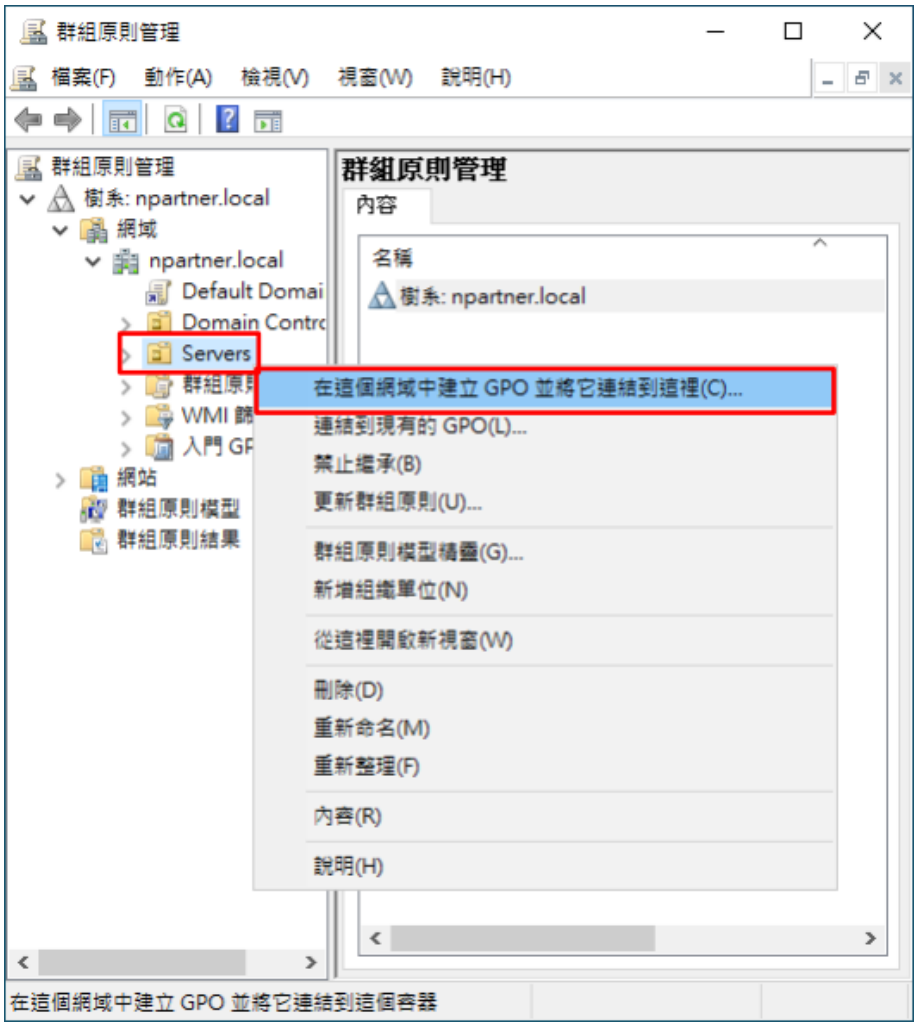
(1) 開啟群組原則管理

開啟 [群組原則管理]



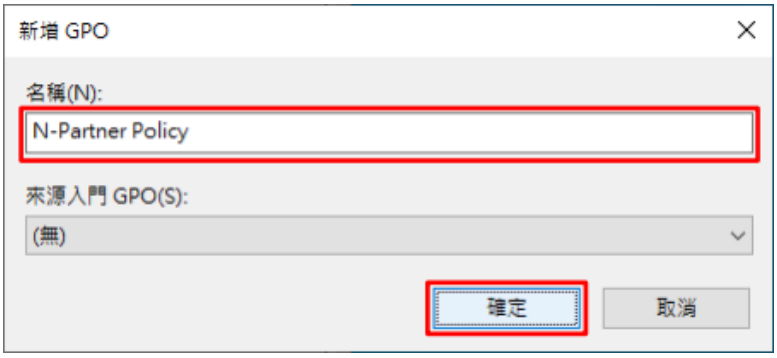
(2) 在 Servers 組織單位，新增群組原則物件

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...]



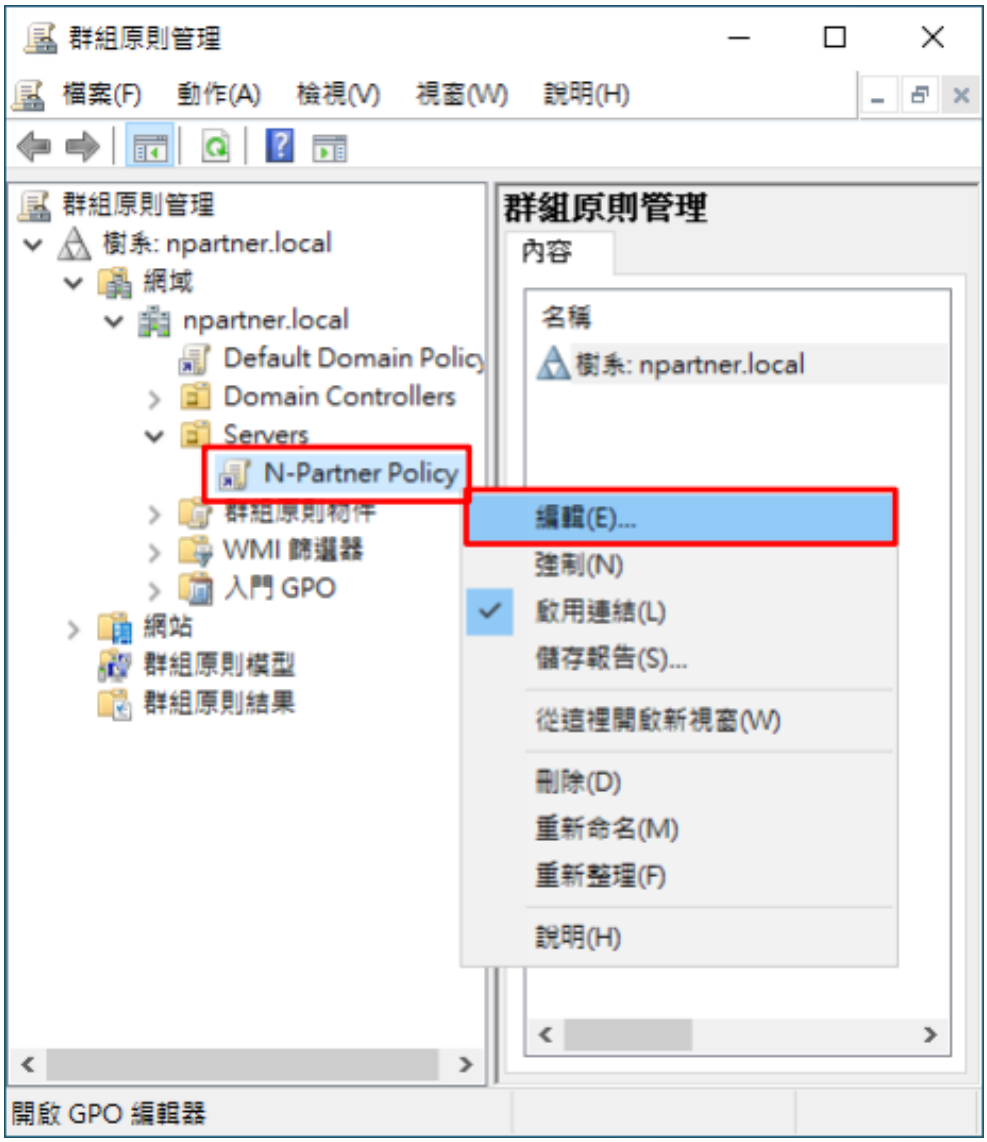
(3) 輸入群組原則物件名稱

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]



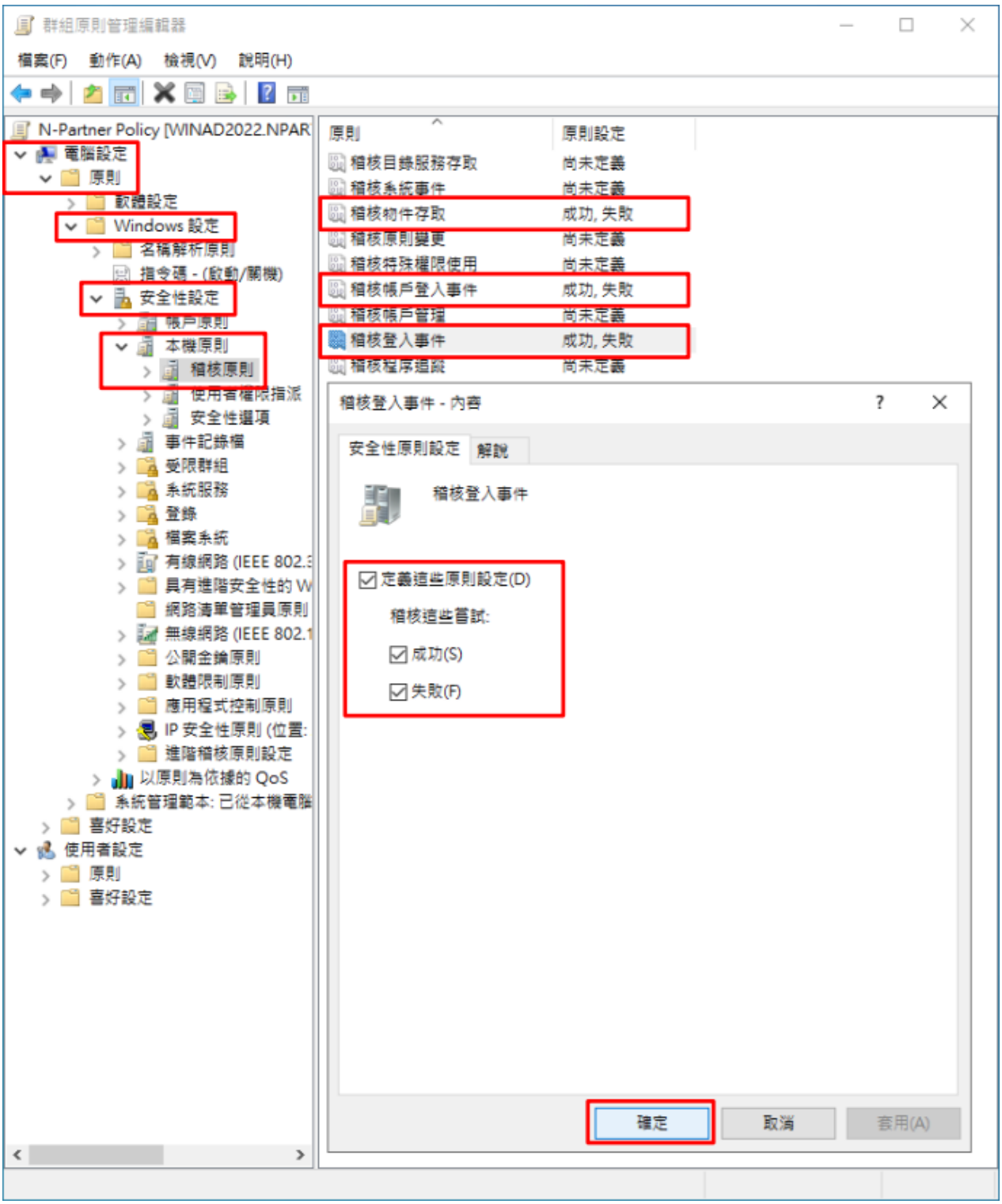
(4) 編輯群組原則物件

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



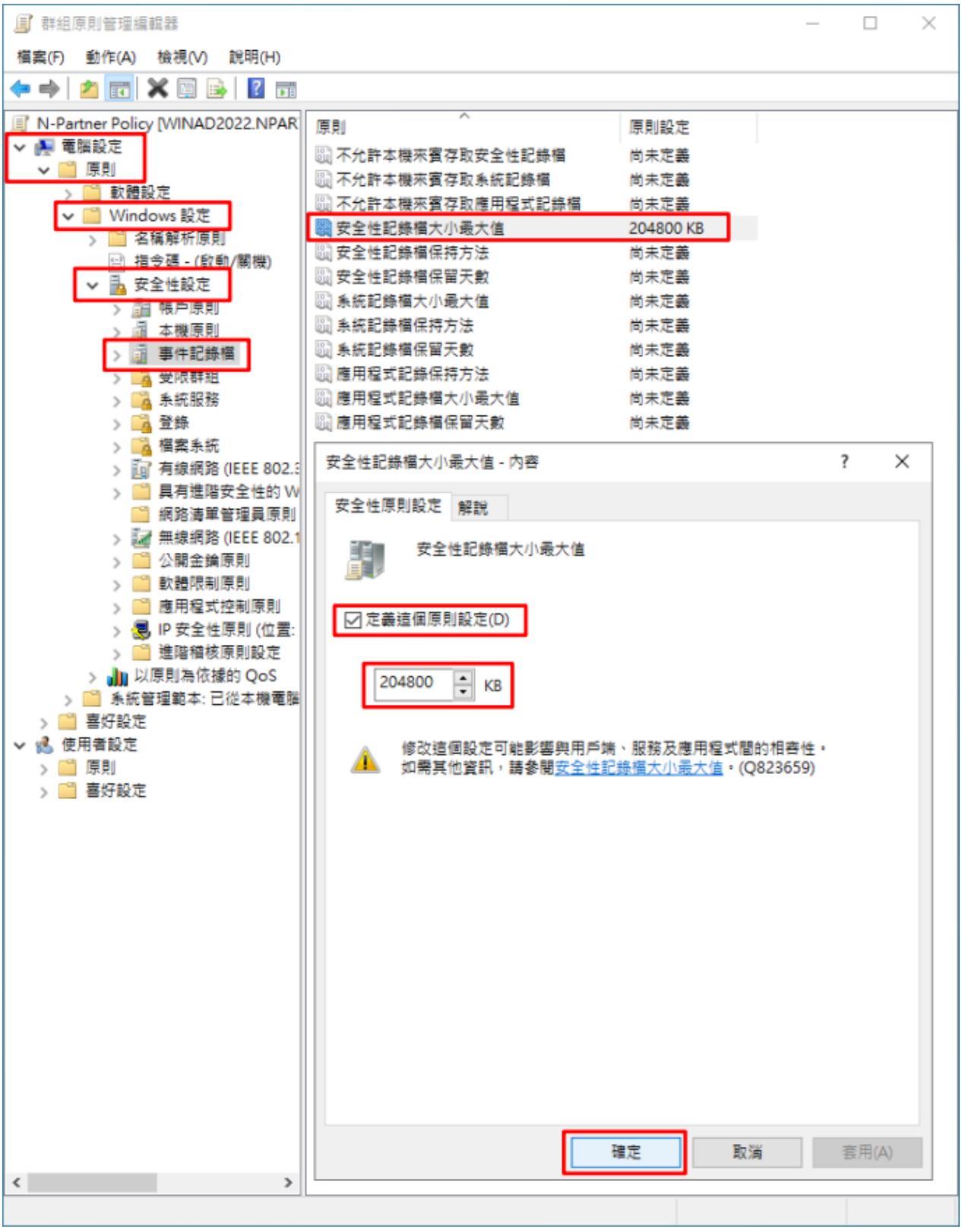
(5) 本機原則：稽核原則

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]



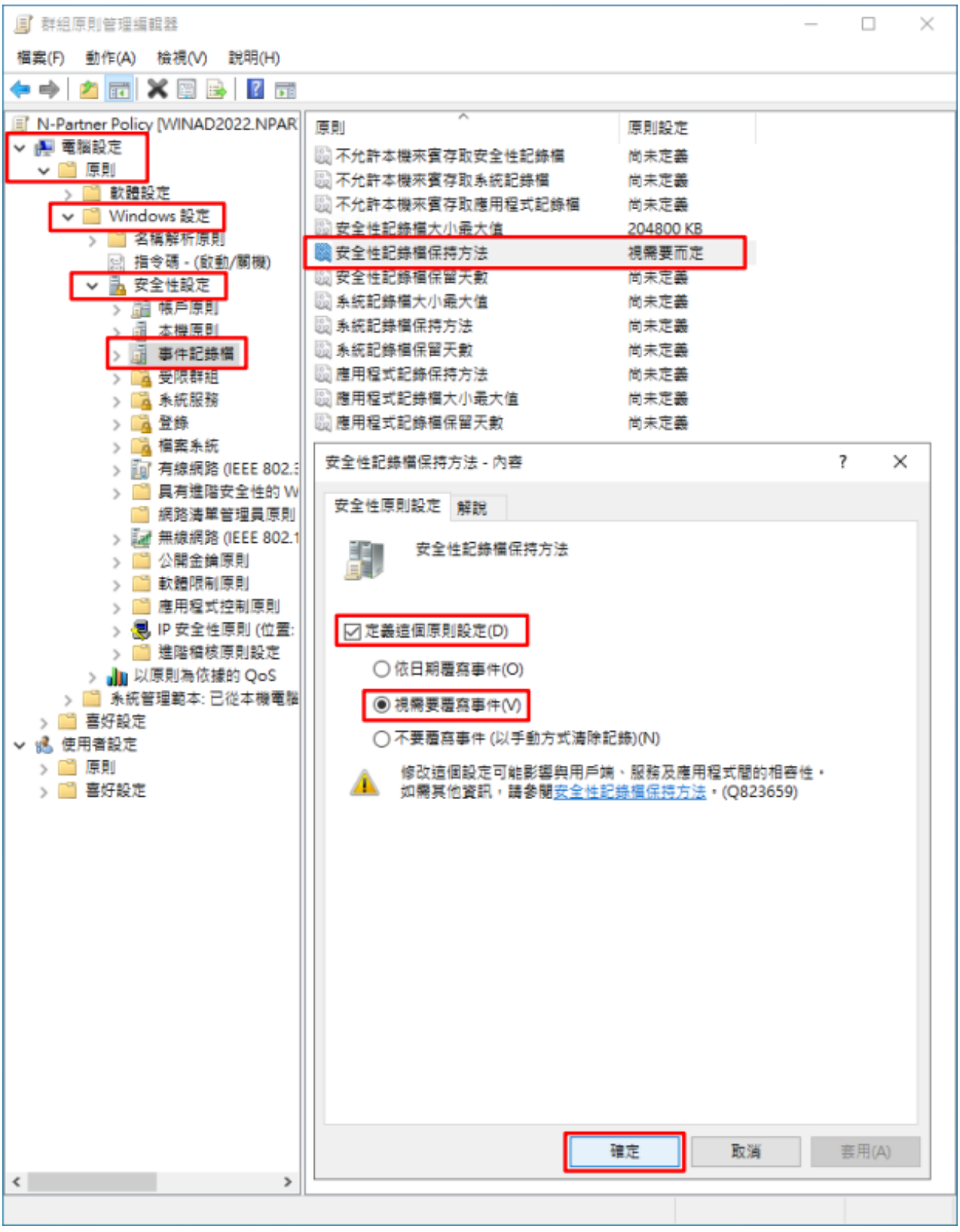
(6) 事件記錄檔：安全性記錄檔大小最大值

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]



(7) 事件記錄檔：安全性記錄檔保持方法

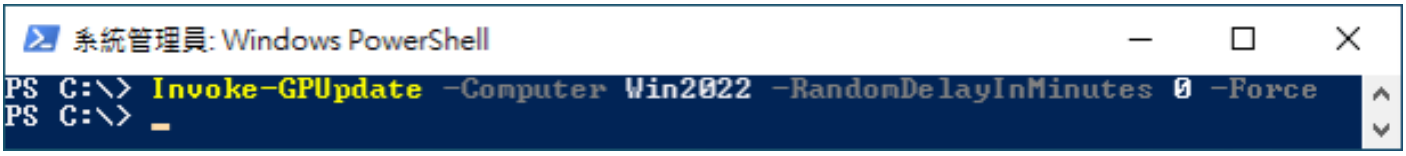
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

(9) 更新 Windows File 伺服器群組原則

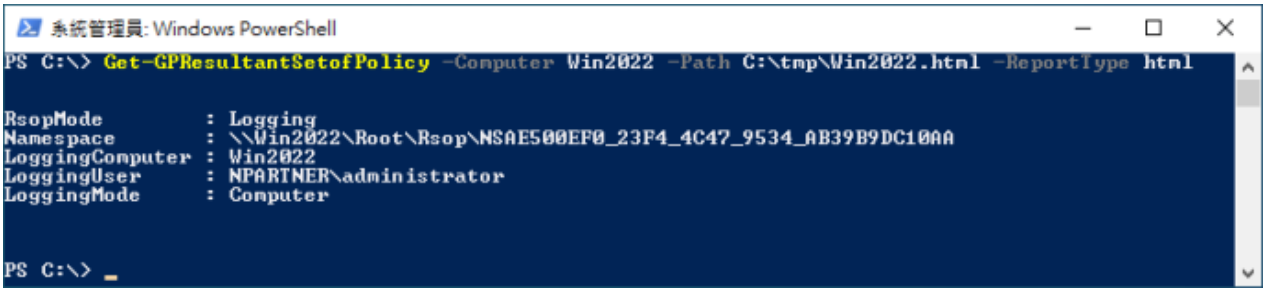
```
PS C:\> Invoke-GPUpdate -Computer Win2022 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows File 伺服器名

(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

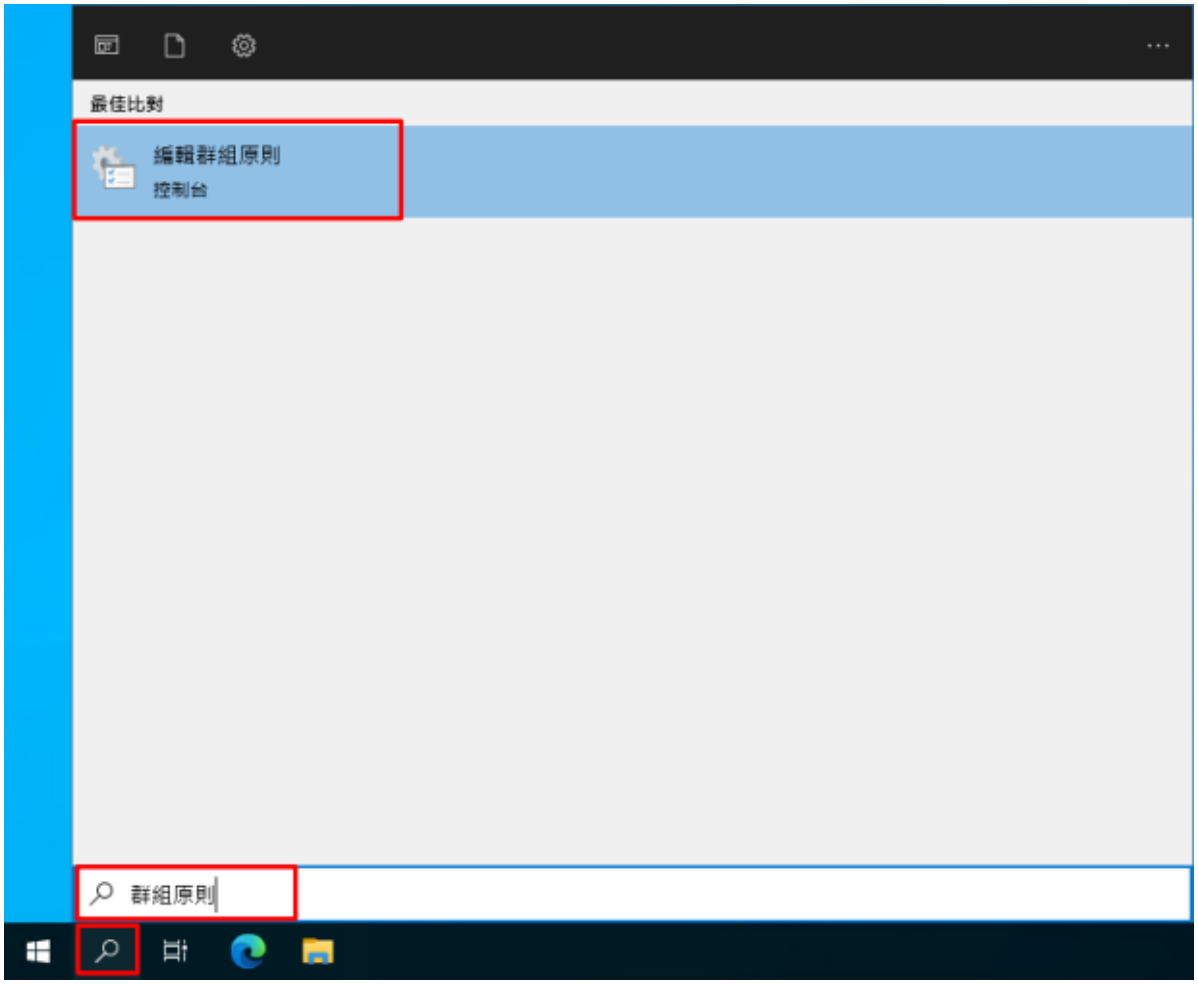
(11) 開啟報表，確認 Windows File 伺服器，套用 N-Partner Policy 群組原則

8.2 工作群組

8.2.1 稽核原則設定

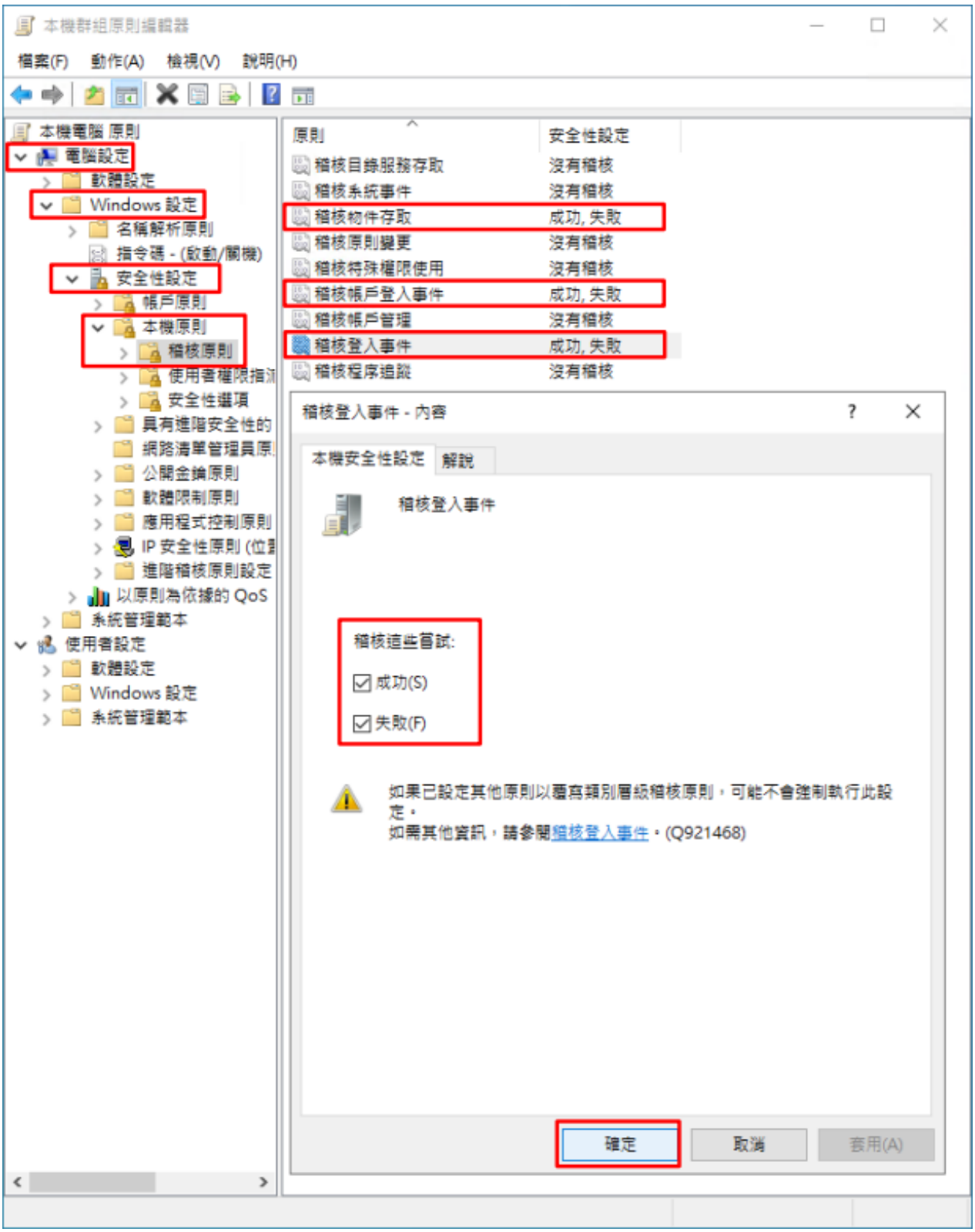
(1) 開啟本機群組原則編輯器

點選 [搜尋] -> 輸入 群組原則 -> 點選 [編輯群組原則]

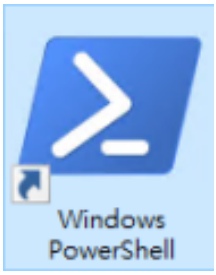


(2) 本機原則：稽核原則

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]

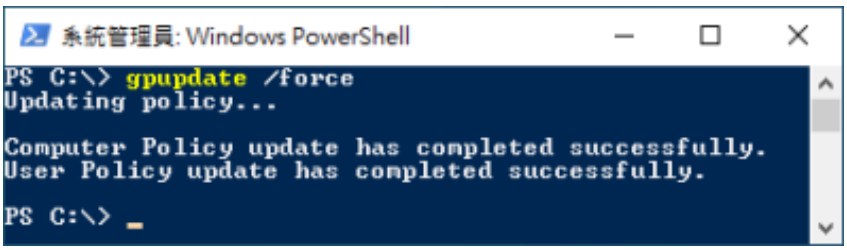


(3) 開啟 [Windows PowerShell]



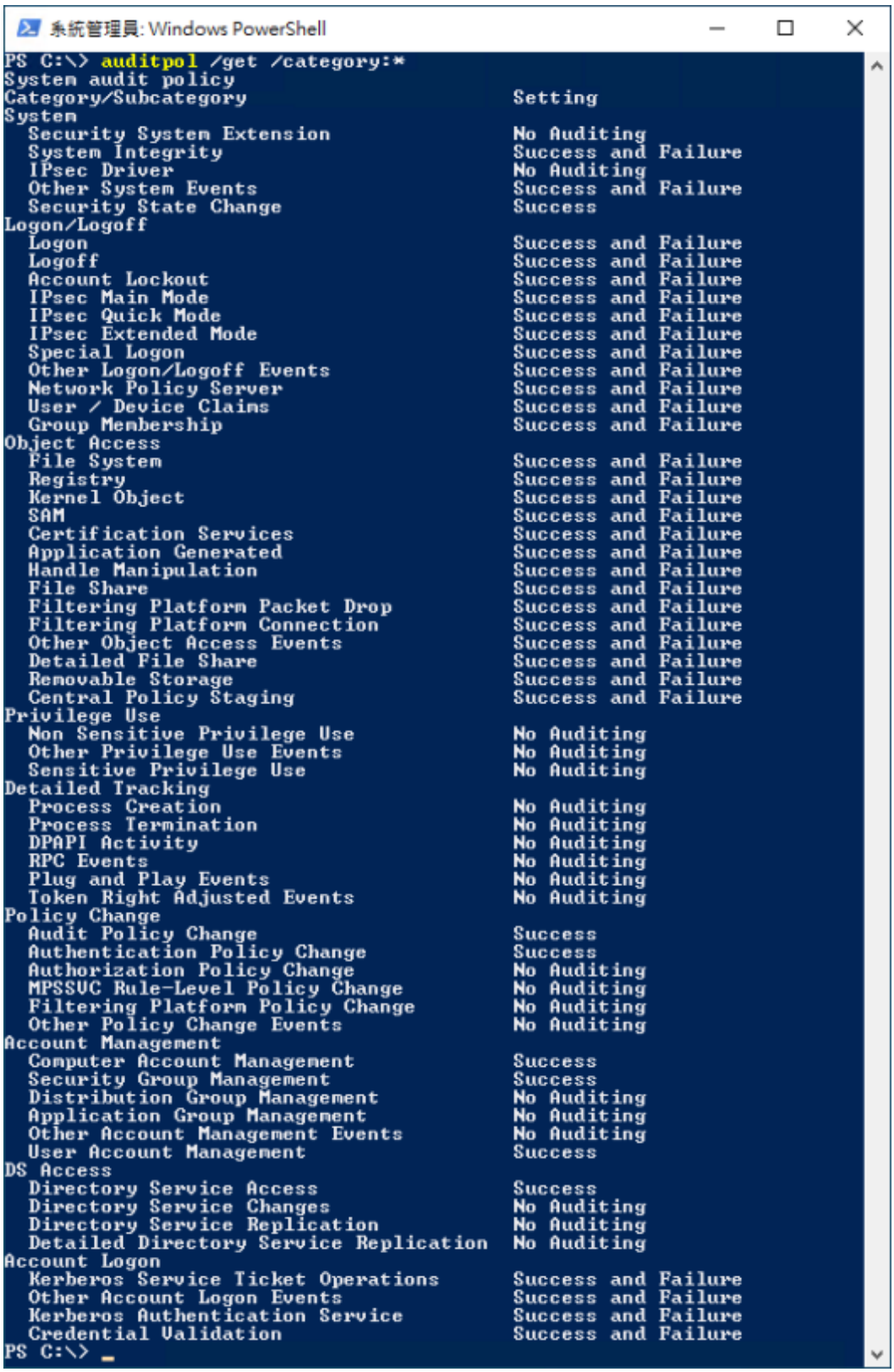
(4) 更新群組原則

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



(5) 查看群組原則套用情形

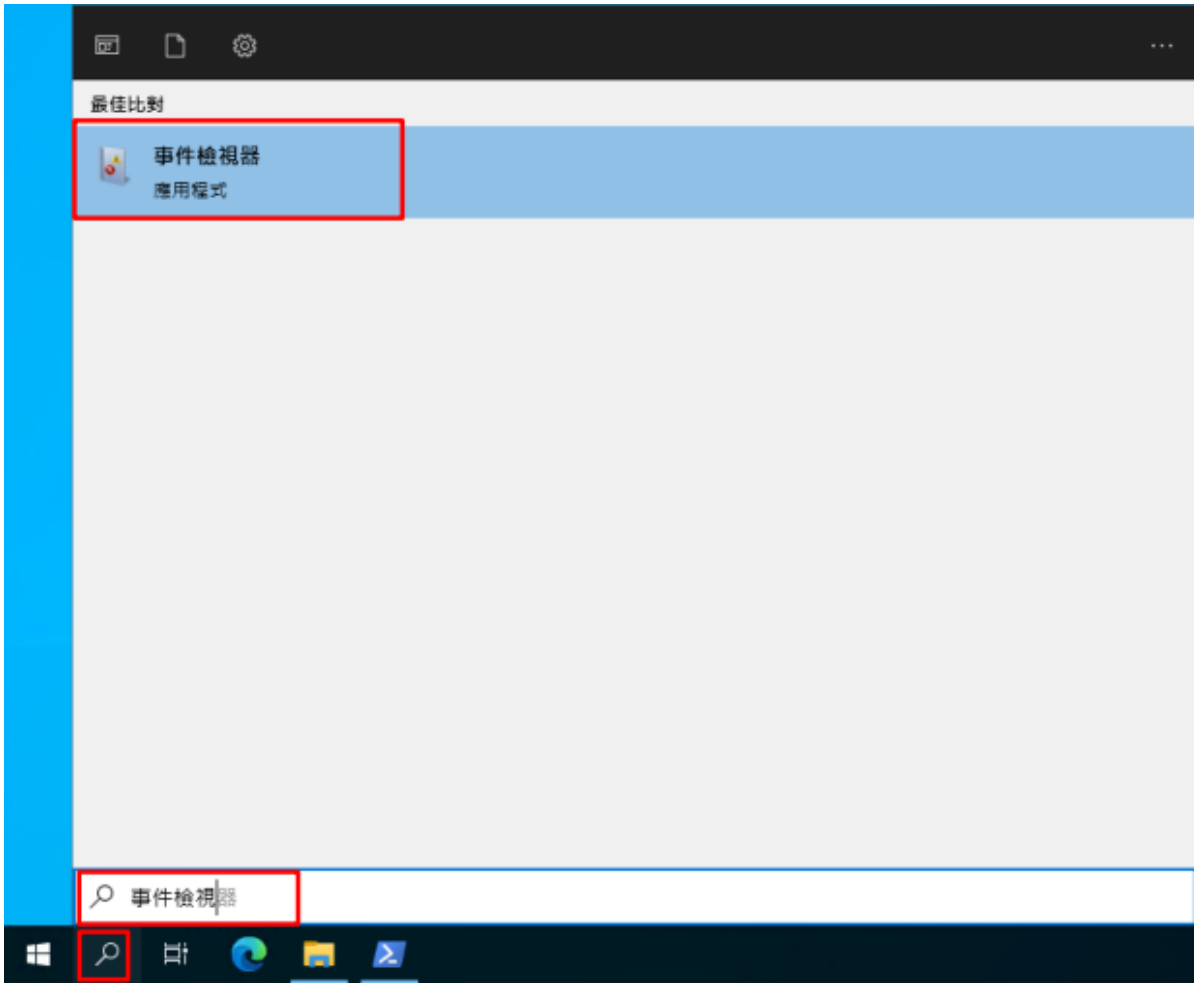
```
PS C:\> auditpol /get /category:*
```



8.2.2 事件檔案設定

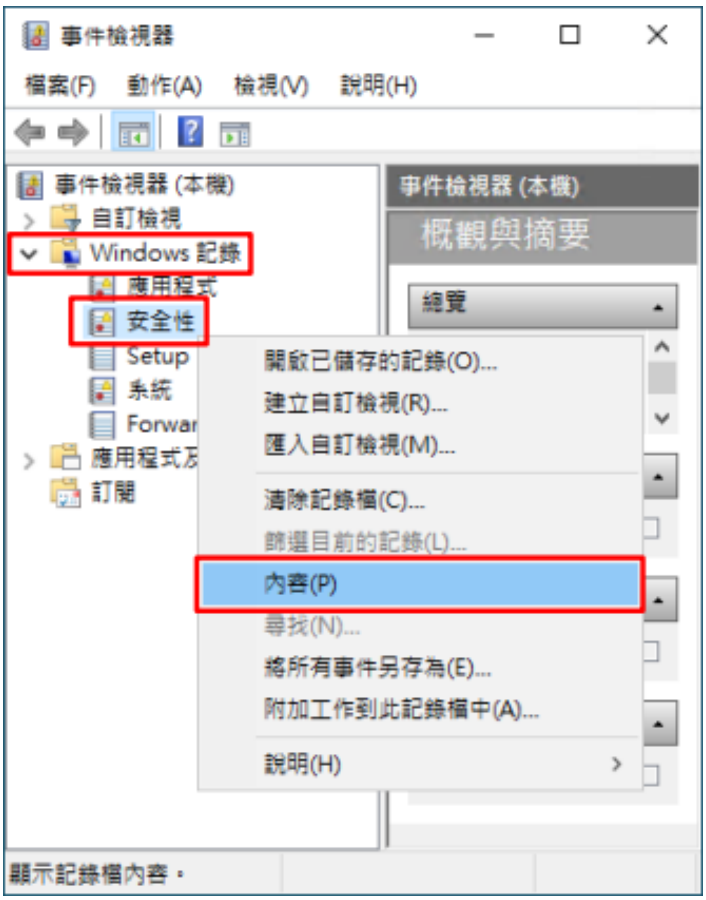
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入 事件檢視 -> 點選 [事件檢視器]



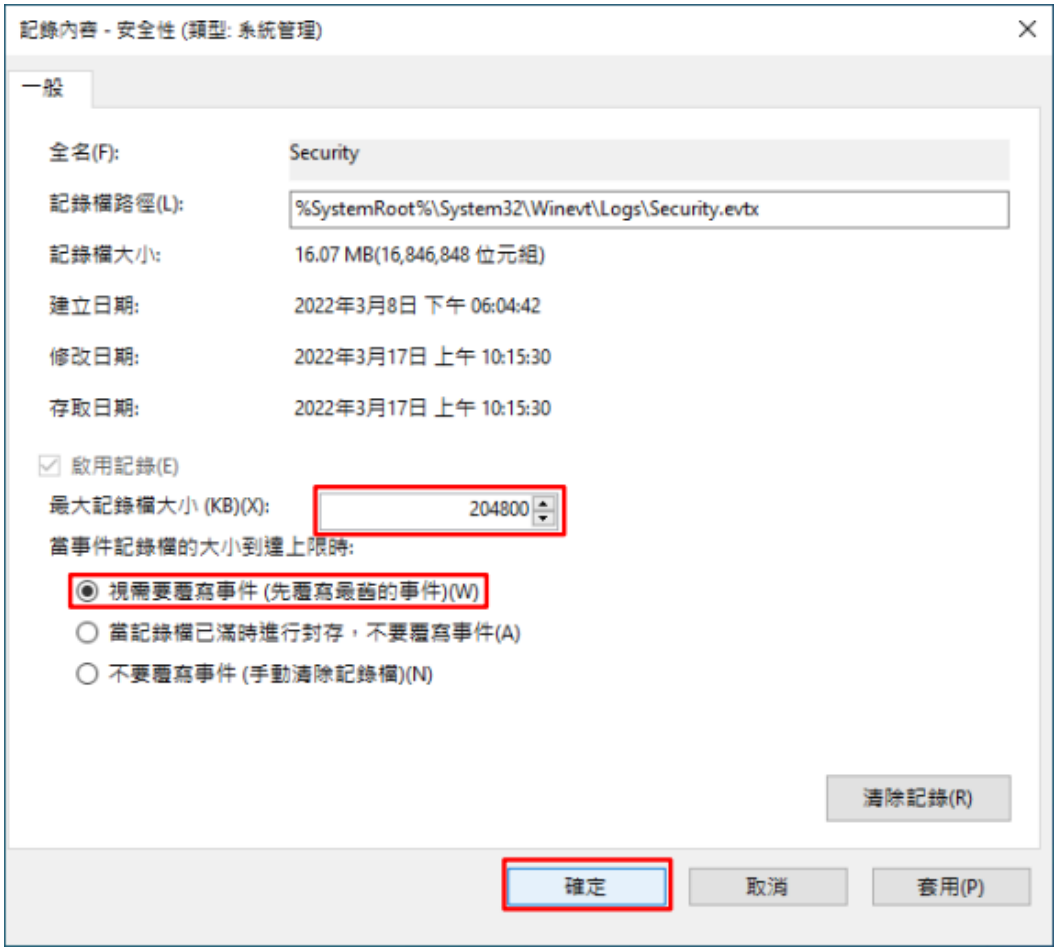
(2) 編輯安全性記錄

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



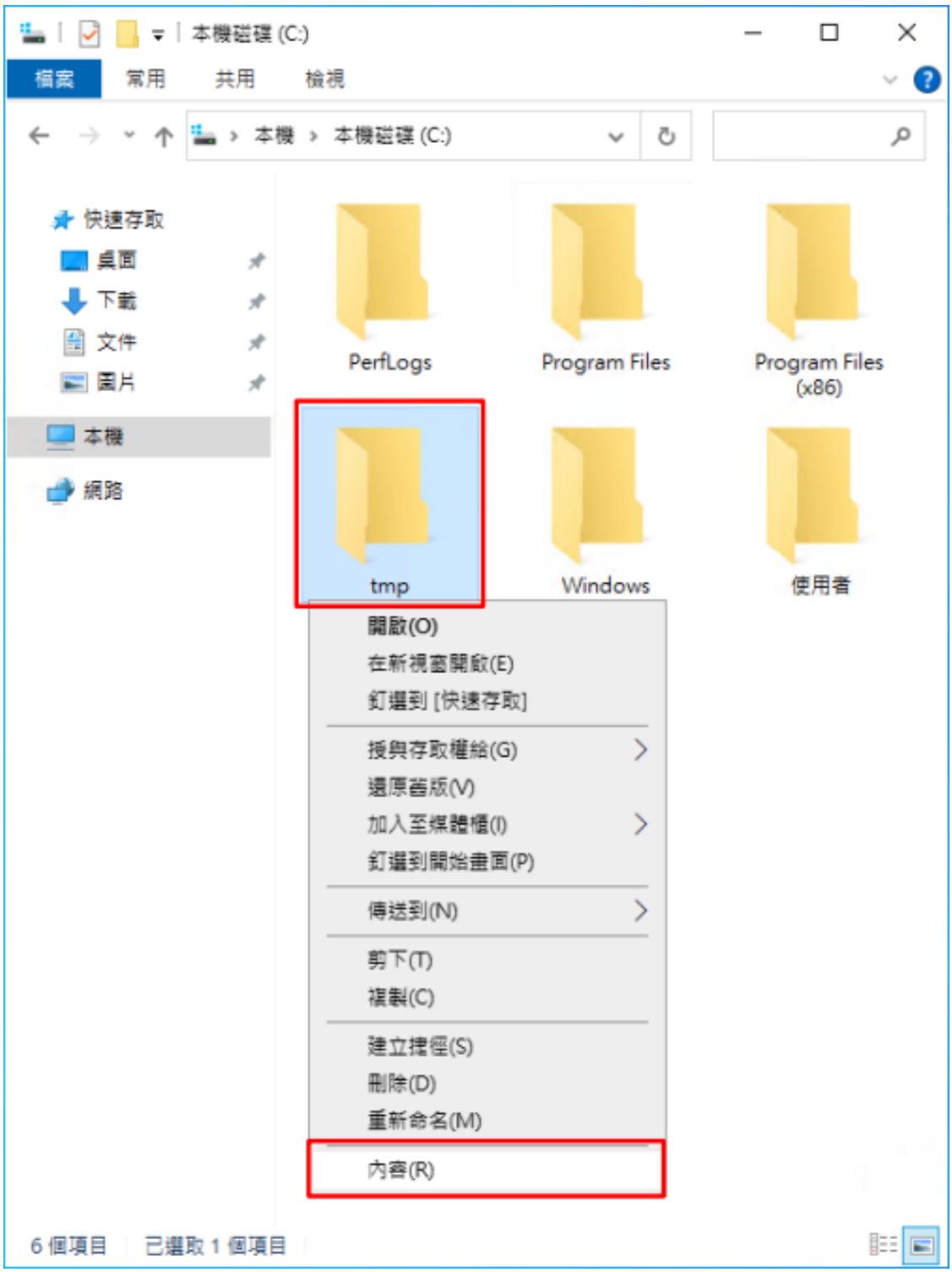
(3) 設定安全性記錄檔

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]

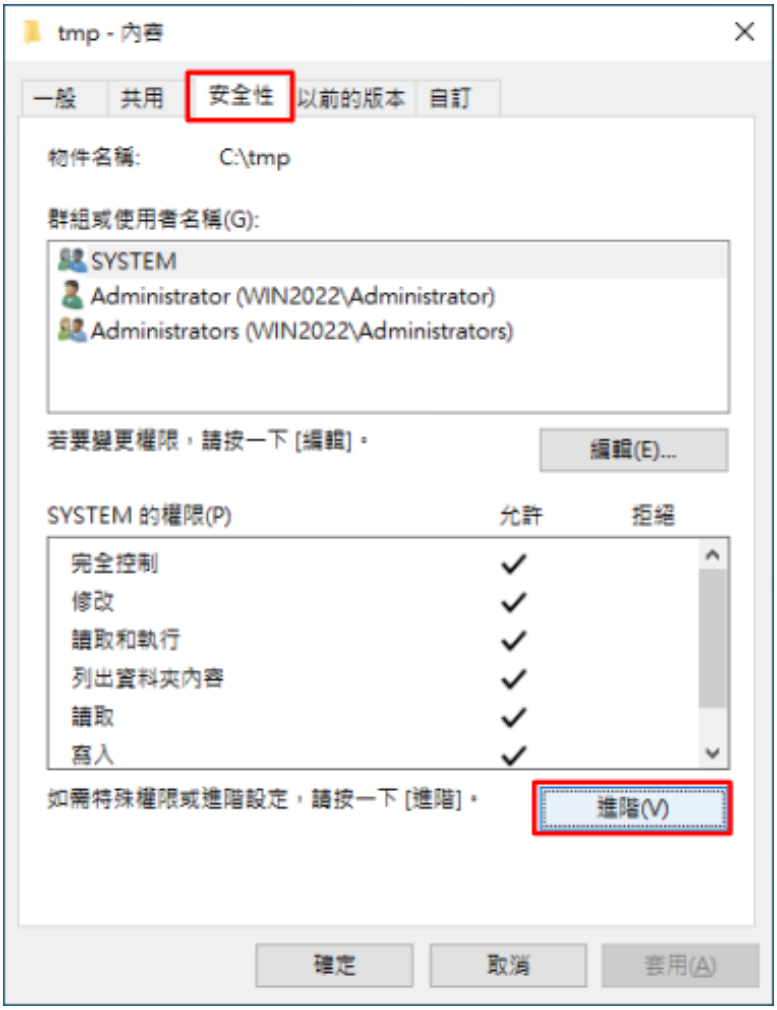


8.3 稽核資料夾設定

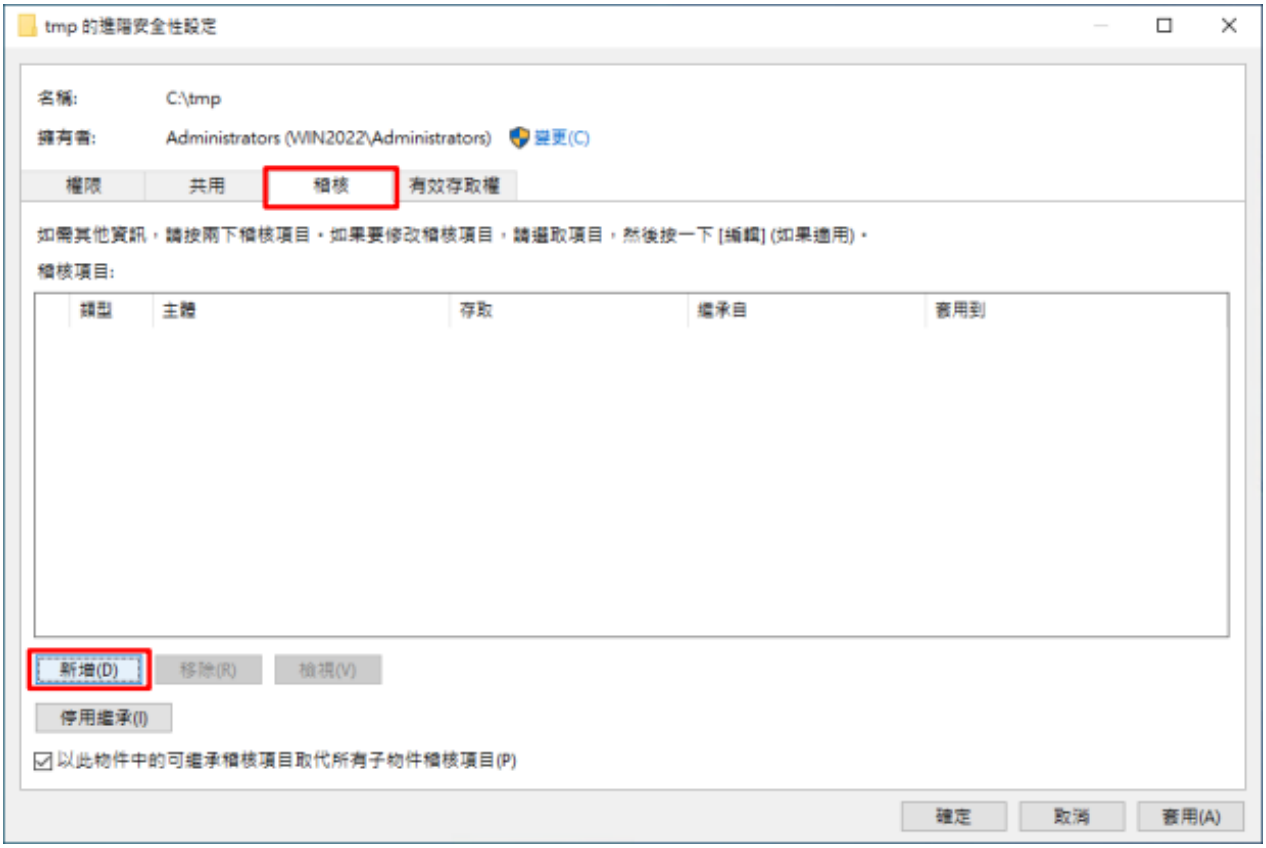
(1) 選擇要稽核 [資料夾] 按滑鼠右鍵 -> 點選 [內容]



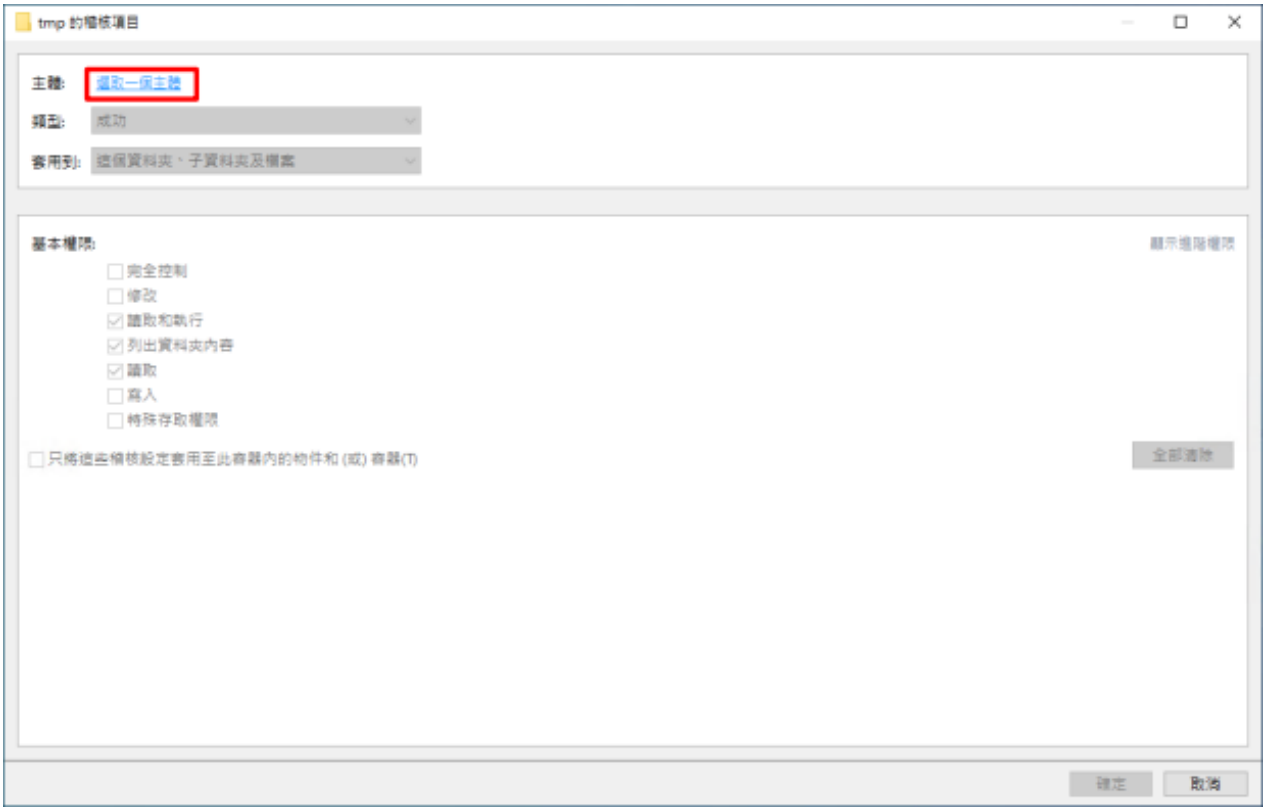
(2) 點選 [安全性] 頁面 -> 按 [進階]



(3) 點選 [稽核] 頁面 -> 按 [新增]

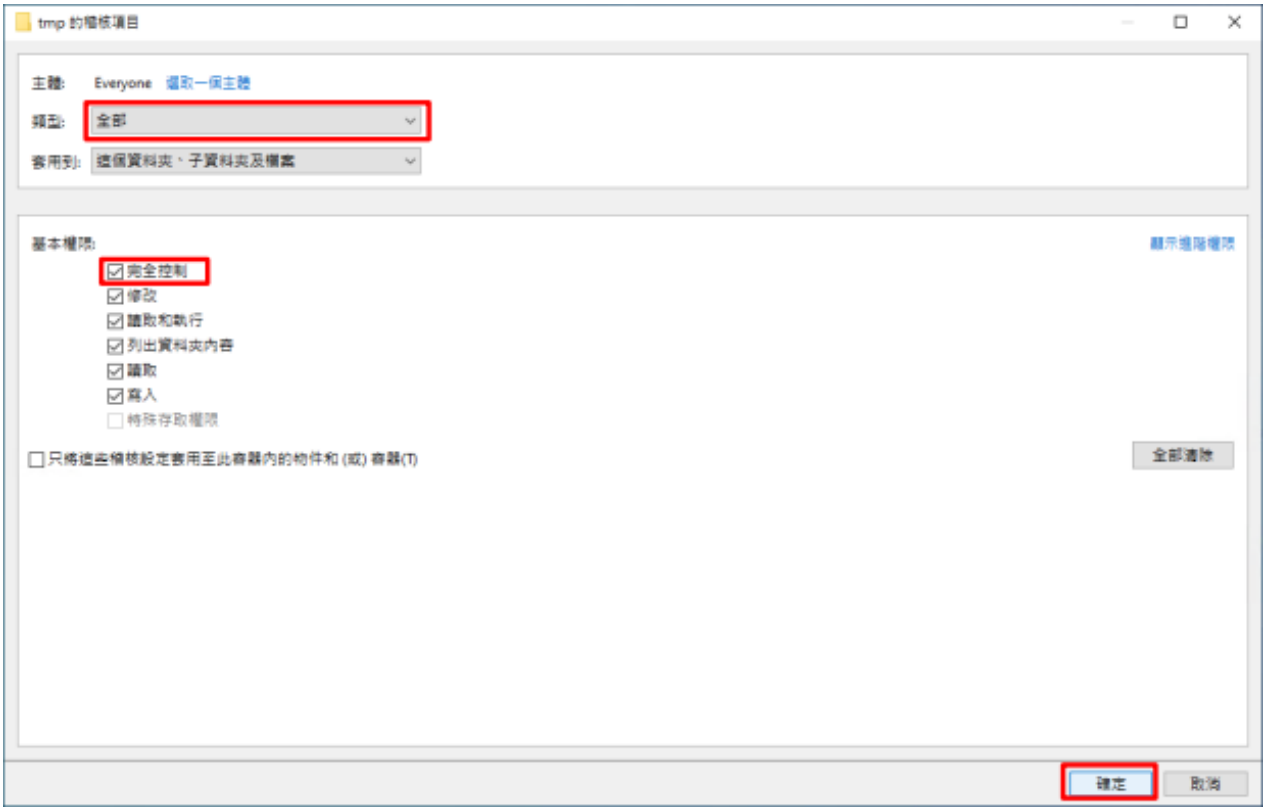


(4) 點選 [選取一個主體]

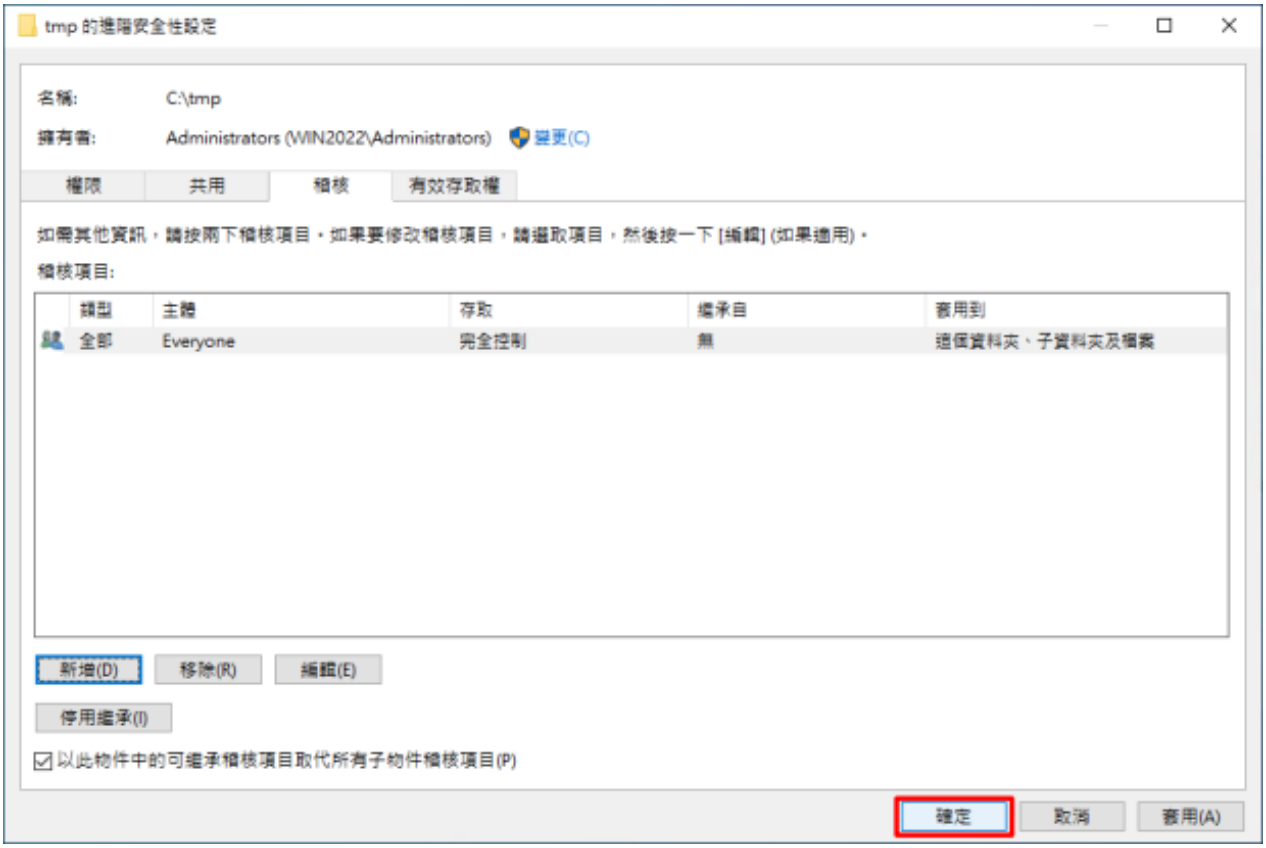


(5) 物件名稱輸入 Everyone 稽核所有用戶 -> 按 [檢查名稱] -> 按 [確定]

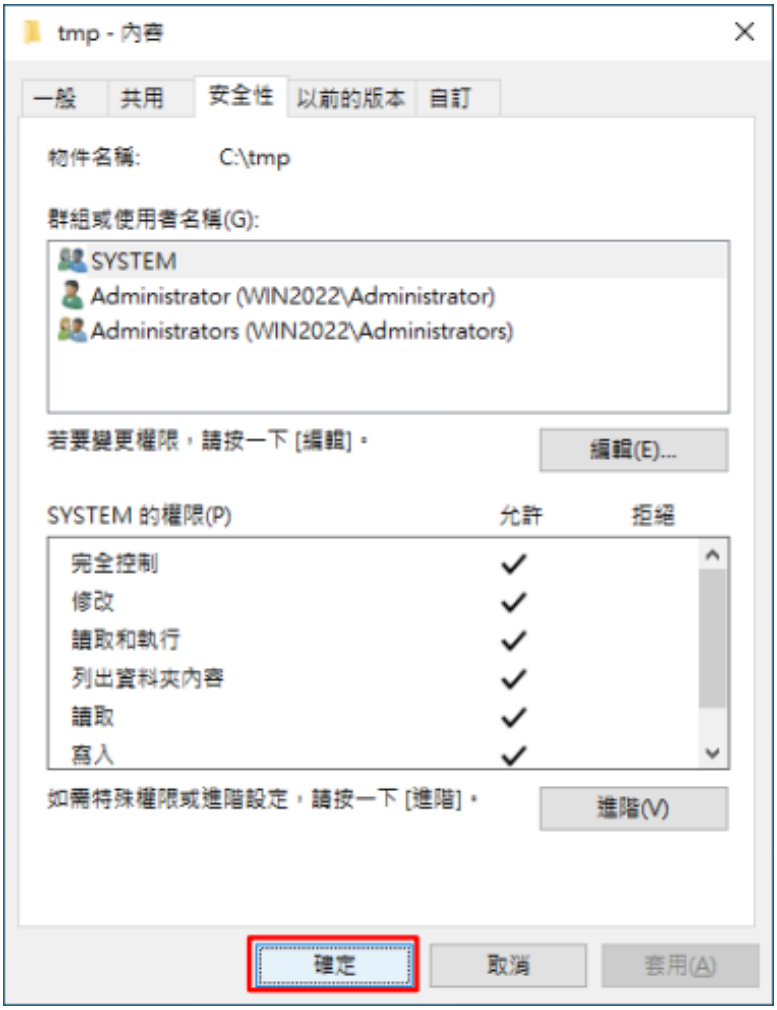
(6)　類型選擇 [全部] -> 勾選 [完全控制] -> 按 [確定]



(7) 顯示稽核主體 [Everyone] -> 按 [確定]



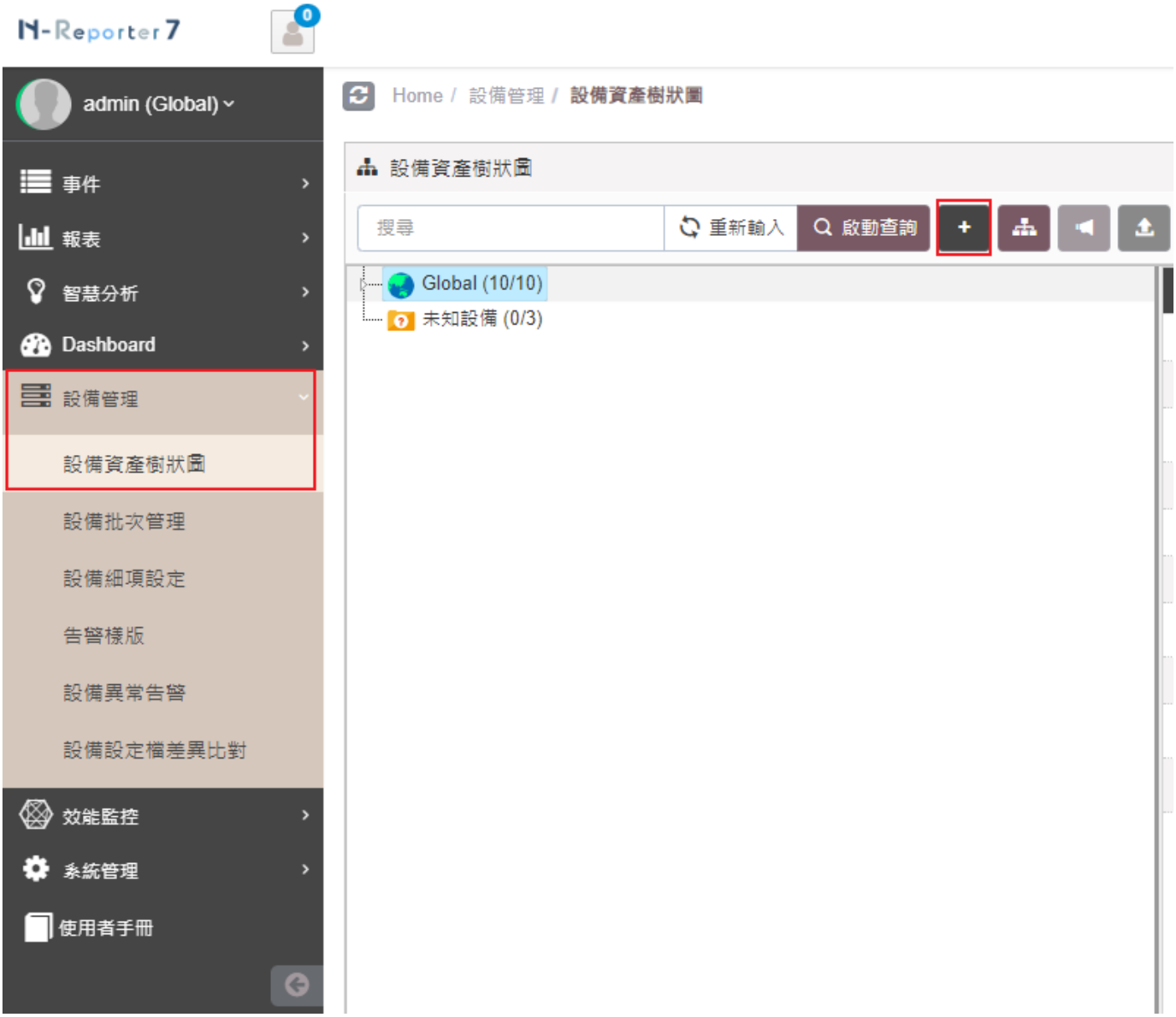
(8) 按 [確定]



9 N-Reporter

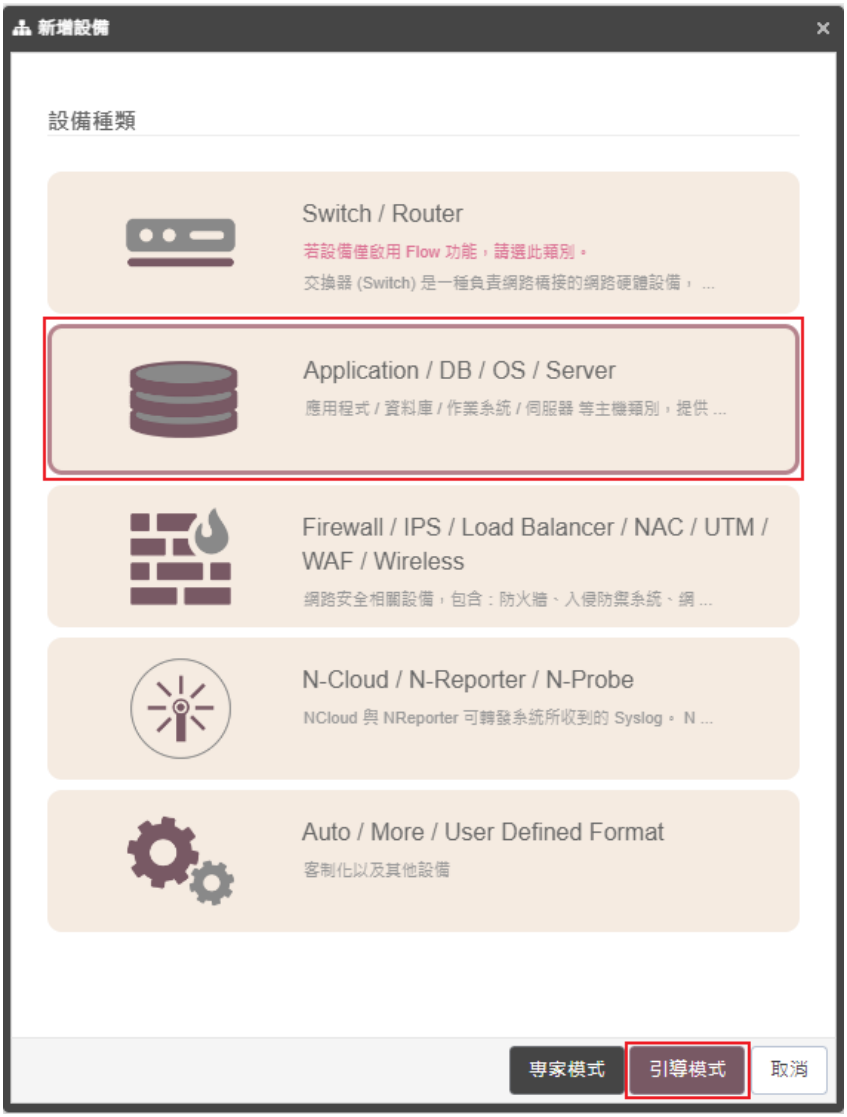
(1) 新增 Windows File 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

選擇 [Application/DB/OS/Server]-> 點選 [引導模式]



9.1 Windows 2003 或之前版本作業系統

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows]-> 點選 [下一步]

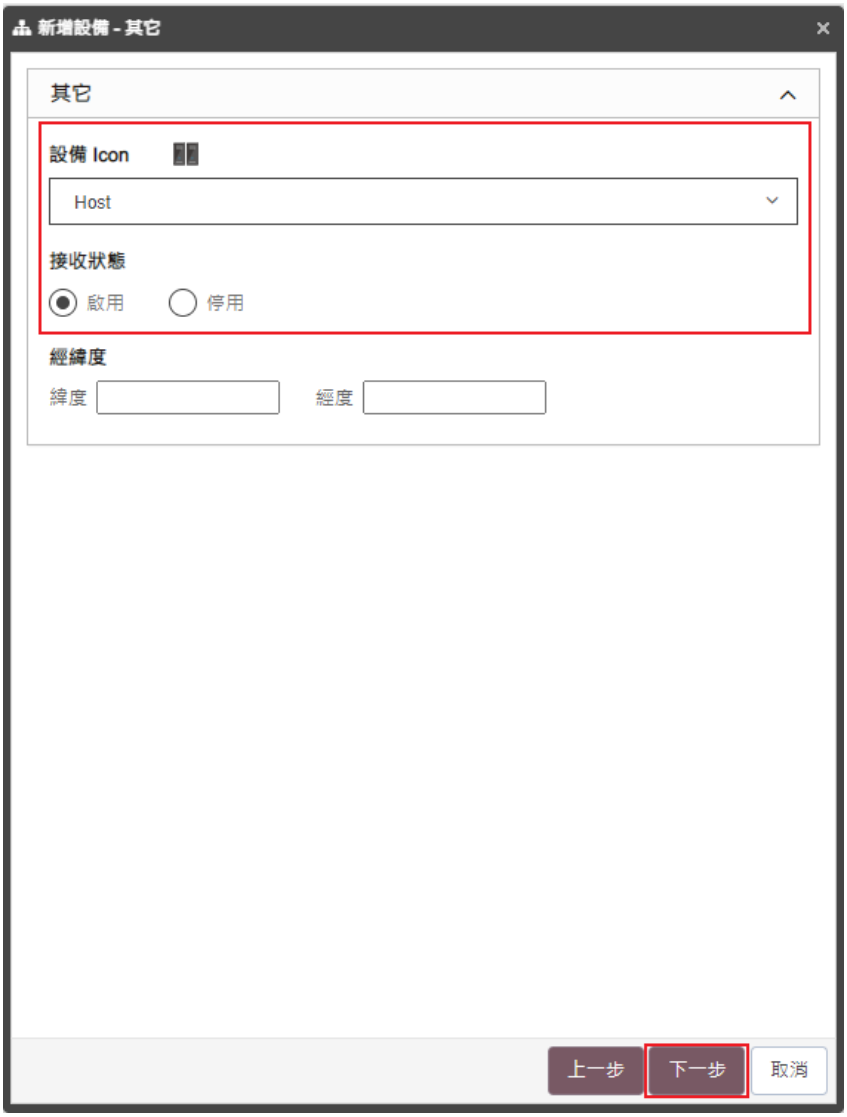
(2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)] 和編碼方式: [BIG 5] -> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]



是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]

9.2 Windows 2008 或之後版本作業系統

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows]-> 點選 [下一步]

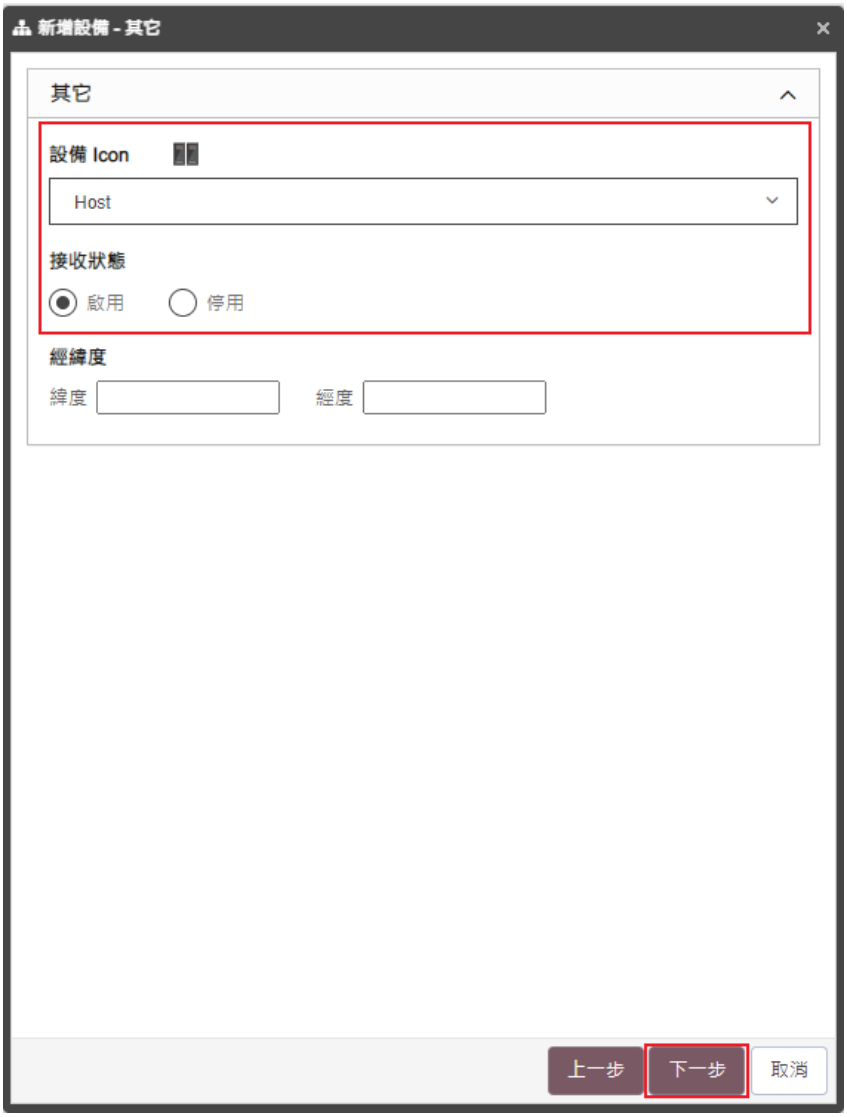
(2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)] 和編碼方式: [UTF-8] -> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

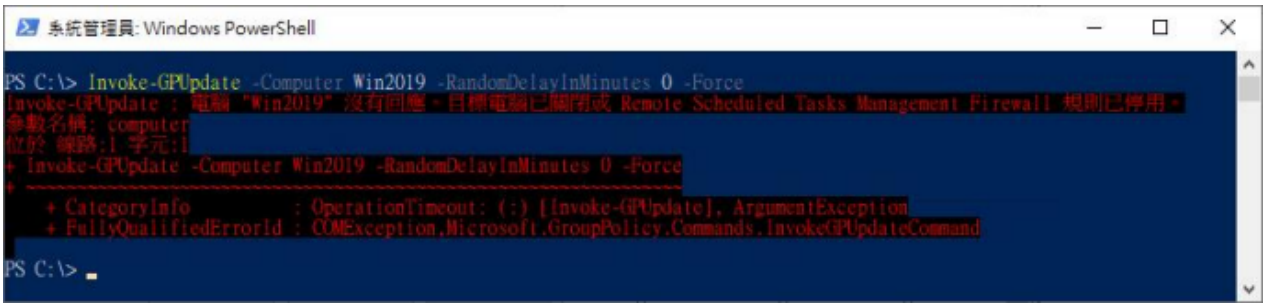


是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]

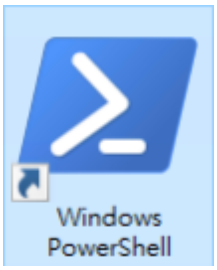
10 問題排除

10.1 Invoke-GPUpdate 錯誤

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

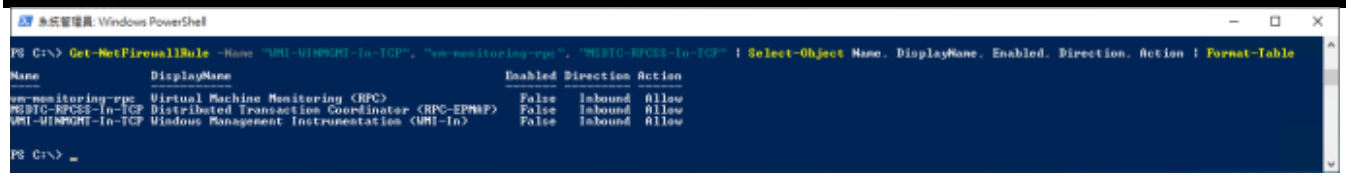


(2) 在 Windows File 伺服器，開啟 [Windows PowerShell]



(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
```

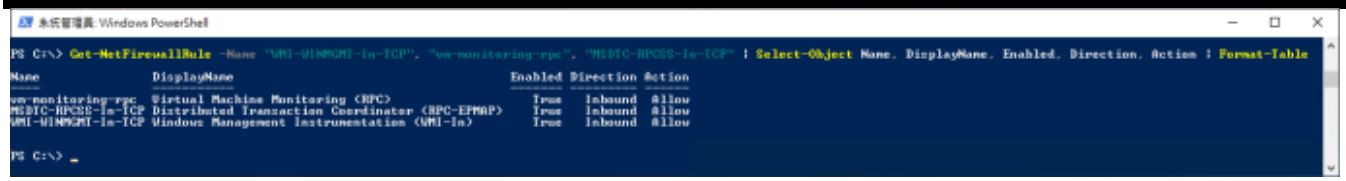


(4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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

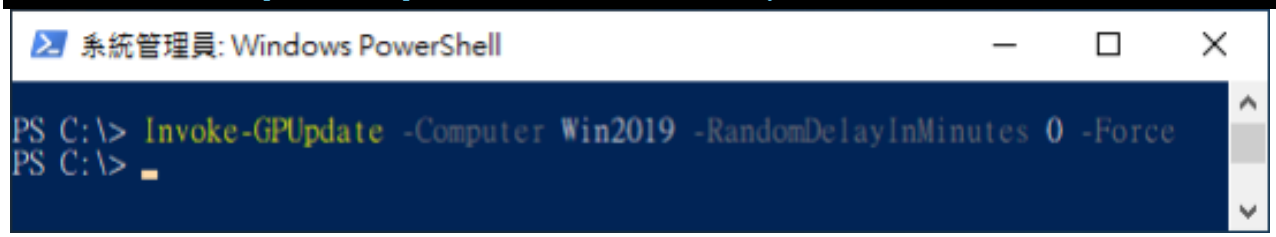
(5) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
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
```

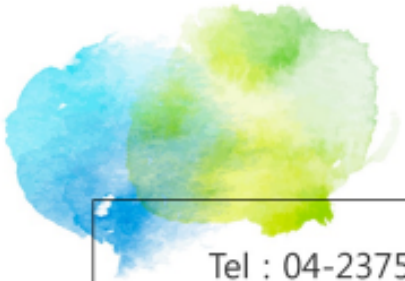


(6) 在 AD 網域伺服器 -> 更新 Windows File 群組原則

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



紅色文字部位請輸入 Windows Server 伺服器名稱



Tel：04-23752865　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com