N-Partner

如何設定
Windows Server 事件記錄

V014

2024/04/17

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 Server 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

連線 Windows 安全性事件：https://docs.microsoft.com/zh-tw/azure/sentinel/connect-windows-security-events

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。

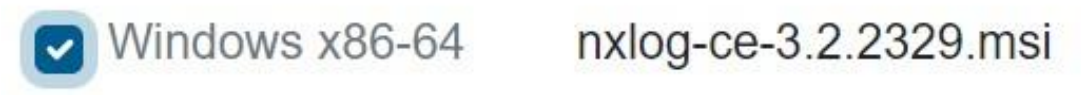
1. NXLog

1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition)

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

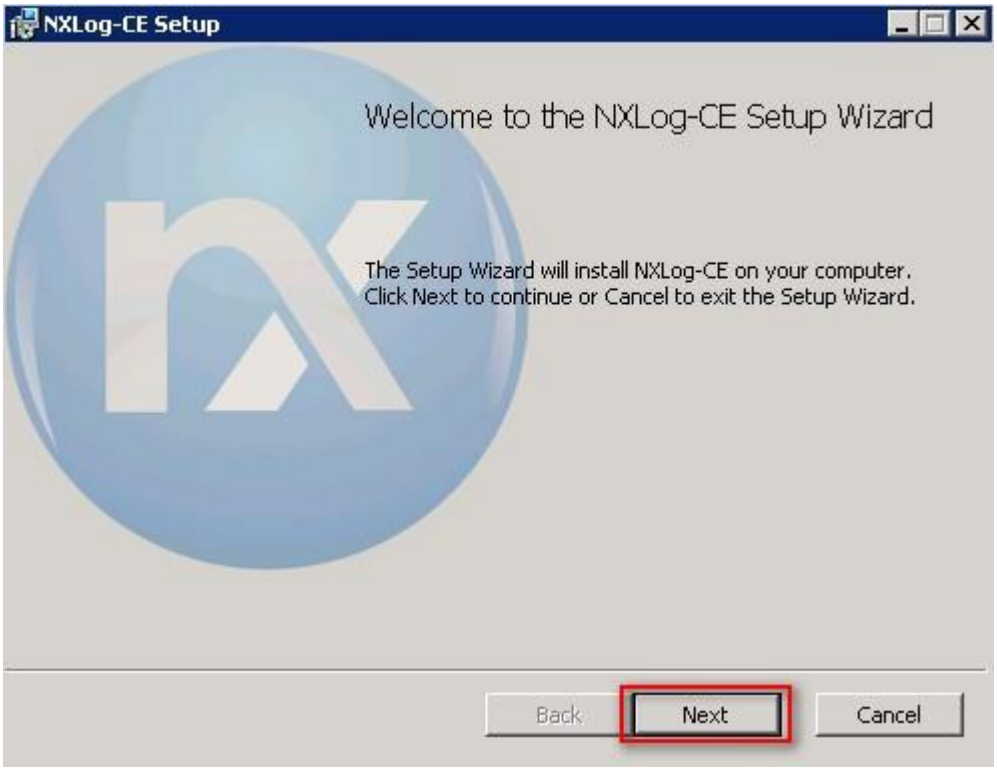
下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.2.2329.msi



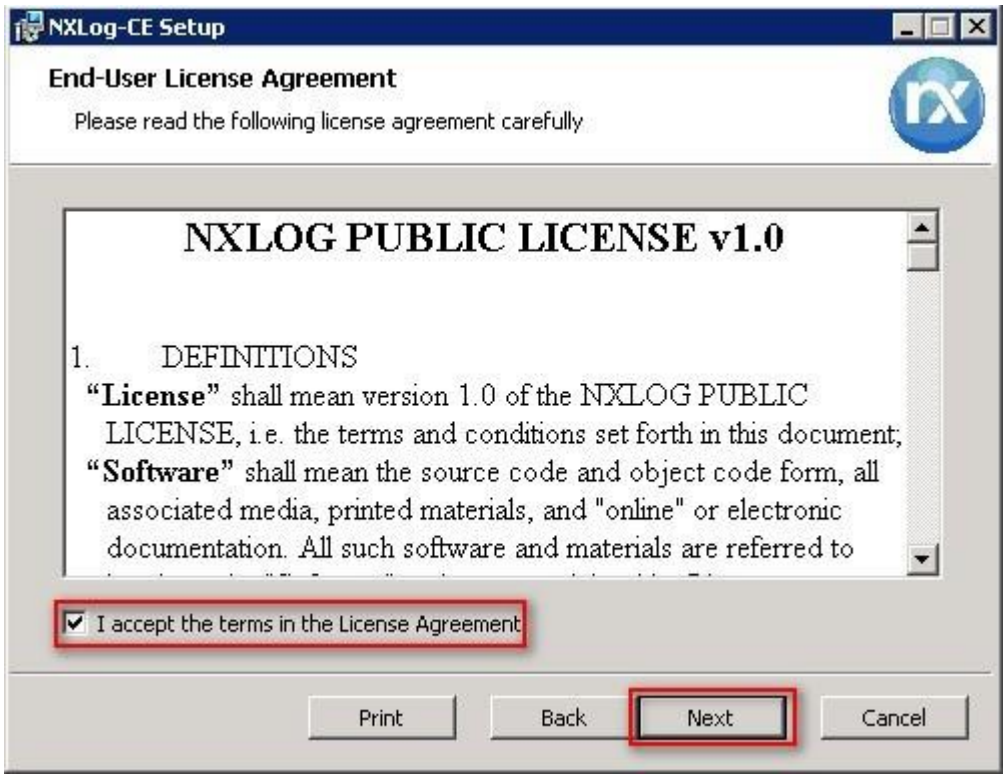
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

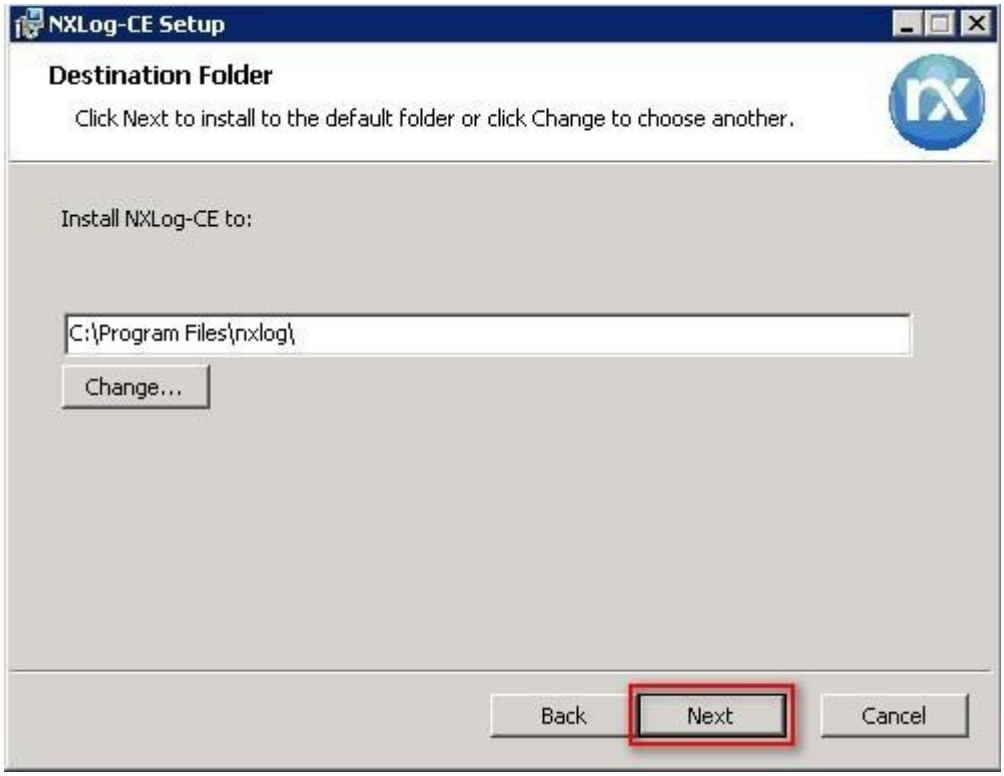
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



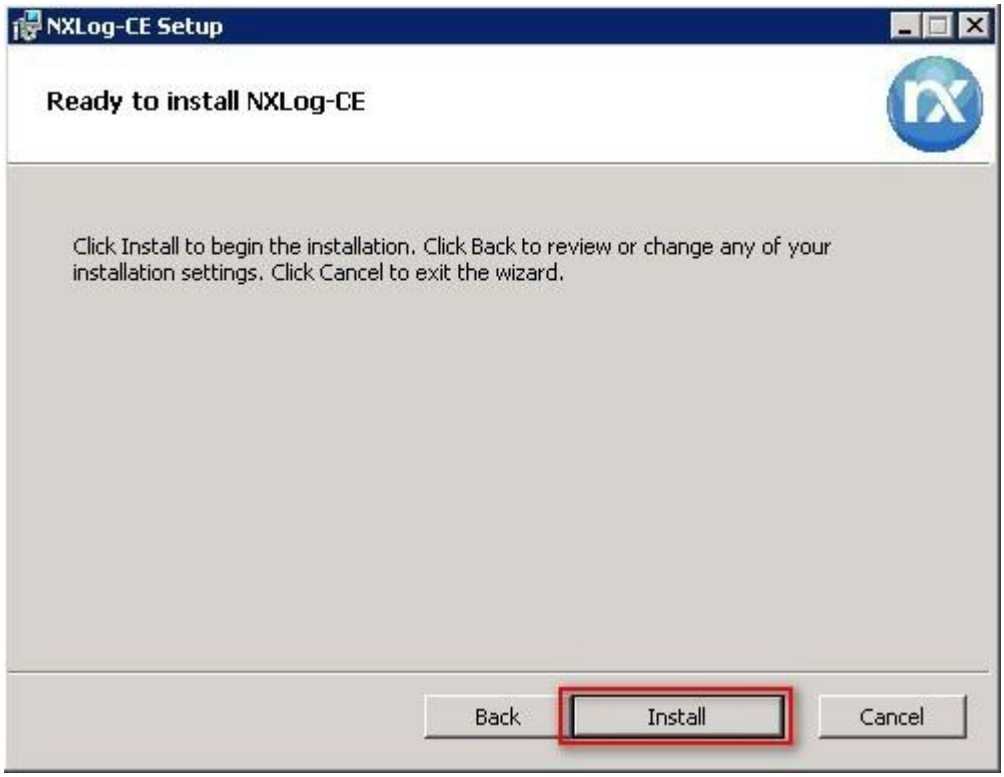
-> 勾選 [I accept the terms in the License Agreement],按 [Next] .



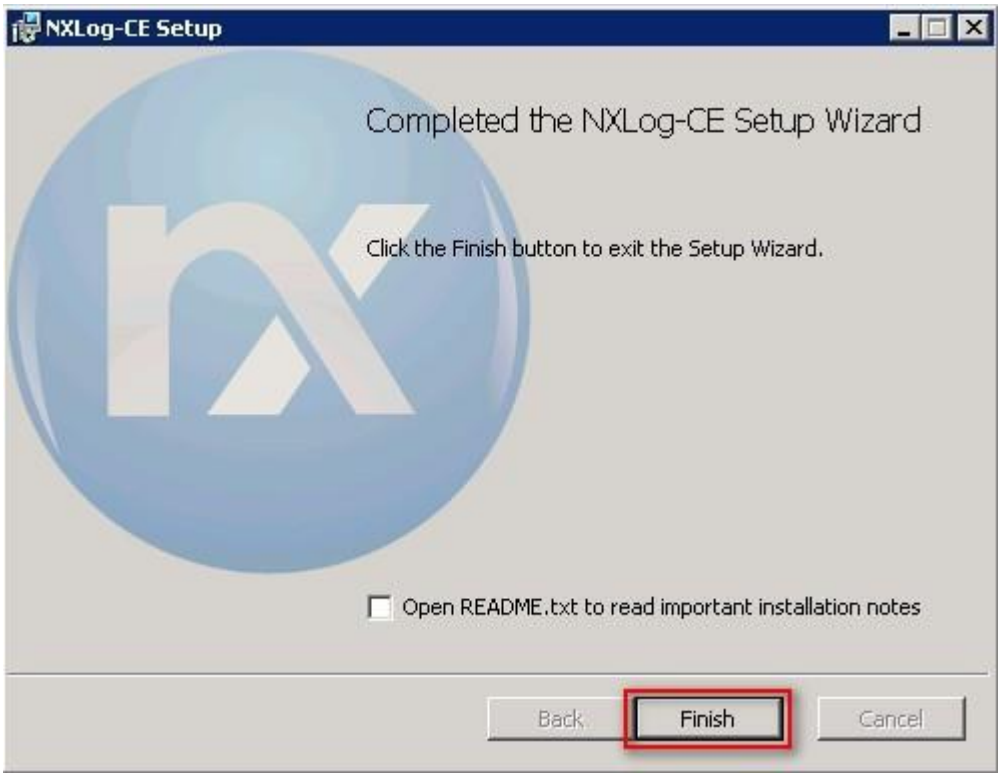
-> 按 [Next].



-> 按 [Install]

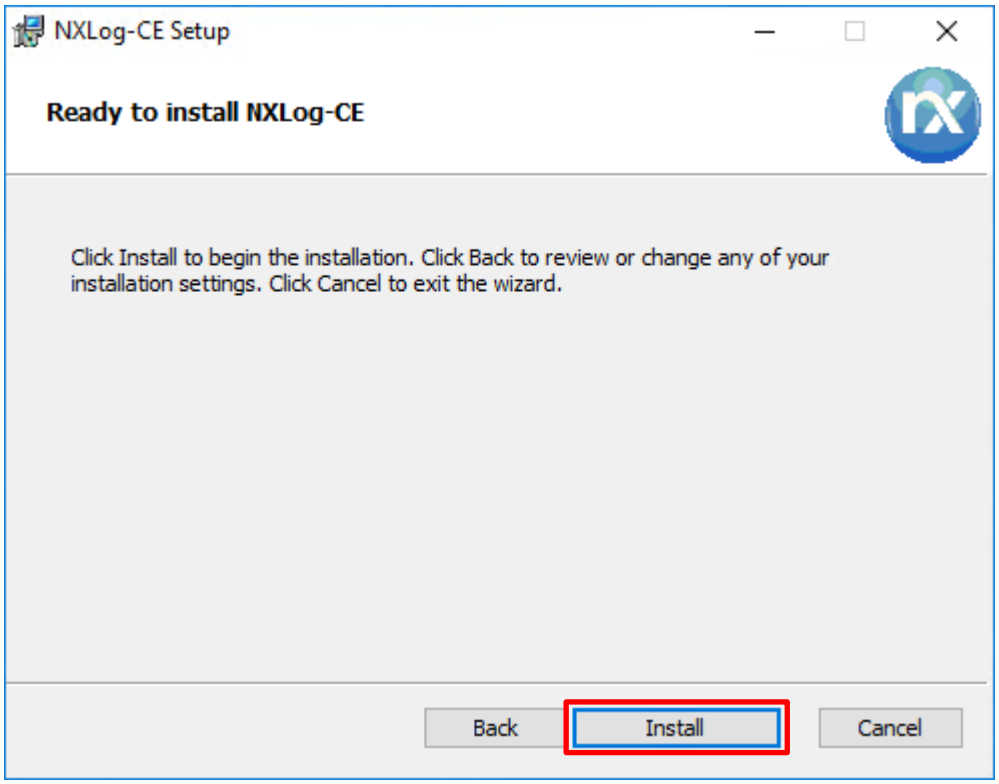


-> 按 [Finish].



<2.2> Windows 2003

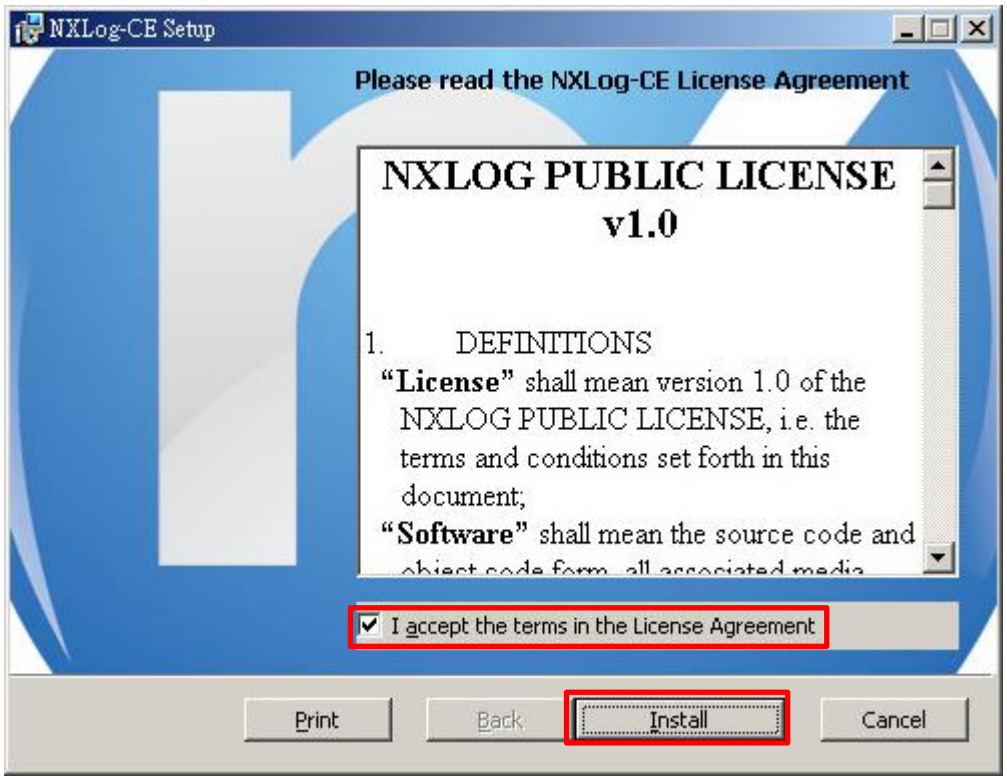
點擊 [nxlog-ce-3.2.2329.msi]] -> 按 [Install] 到 [Finish]



<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

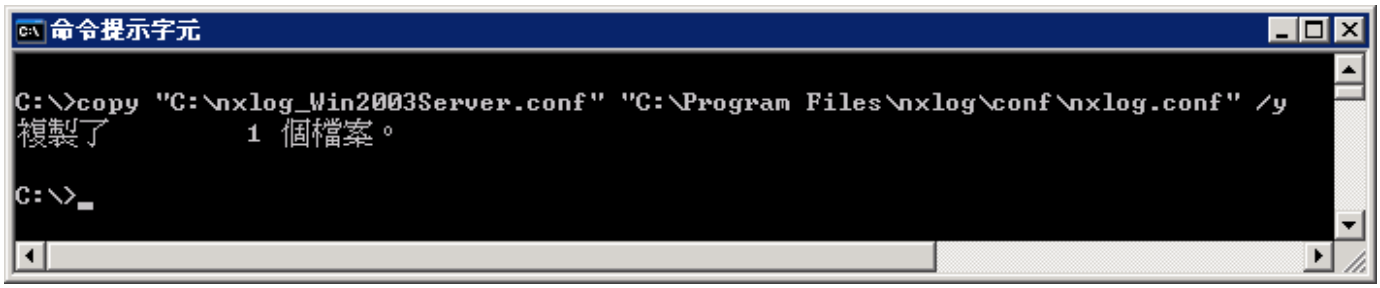
1.2.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄

(1) 開啟 [命令提示字元]

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

下載連結：http://www.npartner.com/download/tech/nxlog_Win2003Server.conf

```
C:\ > copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



本文件範例是 32 位元作業系統，若作業系統是 64 位元，紅色文字部位請改以下設定 "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

註：預設建議採用此設定，此設定檔只輸出主機稽核、物件存取、帳戶管理等事件記錄。減輕 Windows Server 主機效能的負擔。

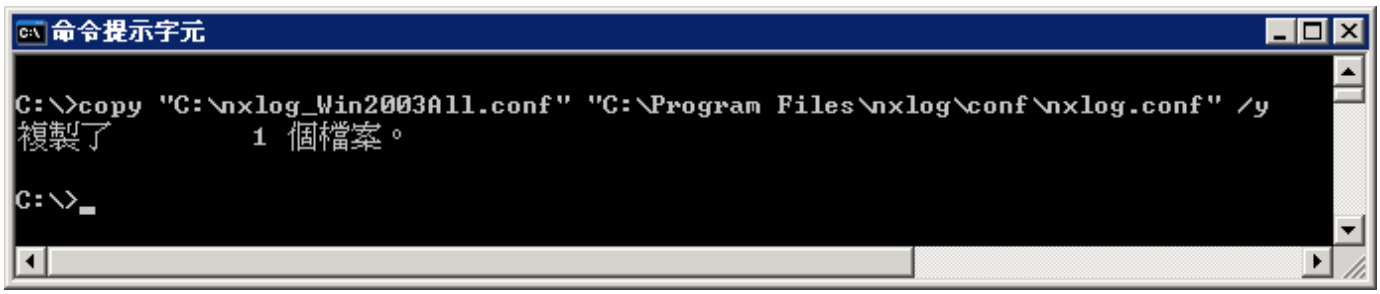
1.2.1.2 輸出全部事件記錄

(1) 開啟 [命令提示字元]

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

下載連結：http://www.npartner.com/download/tech/nxlog_Win2003All.conf

```
C:\ > copy "C:\nxlog_Win2003All.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



本文件範例是 32 位元作業系統，若作業系統是 64 位元，紅色文字部位請改以下設定 "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

註：此設定檔輸出 Windows 所有事件記錄。

1.2.2 Windows 2008 或之後版本作業系統

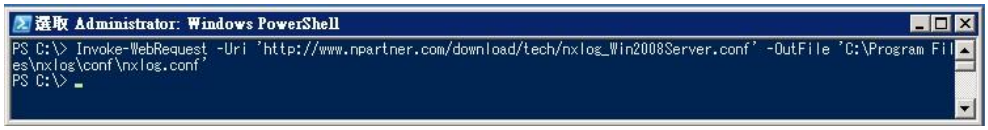
1.2.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄

(1) 開啟 [Windows PowerShell]

(2) 下載 NXLog Windows 2008 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

下載連結：http://www.npartner.com/download/tech/nxlog_Win2008Server.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Win2008Server.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'

註：預設建議採用此設定，此設定檔只輸出主機稽核、物件存取、帳戶管理等事件記錄。減輕 Windows Server 主機效能的負擔。

1.2.2.2 輸出應用程式、安全性、系統全部事件記錄

(1) 開啟 [Windows PowerShell]

(2) 下載 NXLog Windows 2008 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

下載連結：http://www.npartner.com/download/tech/nxlog_Win2008All.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Win2008All.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'

註：此設定檔輸出 Windows 應用程式、安全性、系統所有事件記錄。

1.3 NXLog 設定檔

1.3.1 Windows 2003 或之前版本作業系統

1.3.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.3.50
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>

## Windows Server 2000 - 2003 Event Log use the following:
<Input in_eventlog>
   Module           im_mseventlog
   ReadFromLast TRUE
   SavePos          TRUE
   Exec    parse_syslog_bsd(); \
      if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or
$EventID == 538 or $EventID == 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID ==
624 or $EventID == 626 or $EventID == 627 or $EventID == 628 or $EventID == 629 or $EventID == 630 or
$EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635 or $EventID ==
636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 644 or
$EventID == 645 or $EventID == 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
      else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
      else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
      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      192.168.3.50
```

本文件範例是 32bit 作業系統，若作業系統是 64bit 請改為以下設定

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

1.3.1.2 輸出全部事件記錄

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud         192.168.3.50
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>

## Windows Server 2000 - 2003 Event Log use the following:
<Input in_eventlog>
   Module           im_mseventlog
   ReadFromLast TRUE
   SavePos          TRUE
   Exec parse_syslog_bsd();
</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      192.168.3.50
```

本文件範例是 32bit 作業系統，若作業系統是 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

1.3.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud     192.168.3.50
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>

## define Security Events
define SecurityEvents 1100, 1102, 4768, 4769, 4771, 4616, 4657, 4624, \
4625, 4634, 4647, 4648, 5140, 5142, 5143, 5144, \
5145, 5168, 4656, 4658, 4660, 4663, 4664, 4688, \
4985, 5051, 4670, 4719, 4739, 4720, 4722, 4723, \
4724, 4725, 4726, 4738, 4740, 4767, 4727, 4728, \
4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, \
4764, 4741, 4742, 4743, 4744, 4745, 4748, 4749, \
4750, 4753, 4754, 4755, 4756, 4758, 4759, 4760, \
4763, 4778, 4783, 4800, 4801
## define Other Events
define OtherEvents 7036

## Windows Server 2008 or higher Event Log use the following:
<Input in_eventlog>
   Module            im_msvistalog
   ReadFromLast TRUE
   SavePos           TRUE
   Query             <QueryList> \
      <Query Id="0"> \
         <Select Path="Security">*</Select> \
         <Select Path="System">*</Select> \
      </Query> \
   </QueryList>
   Exec if ($EventID NOT IN (%SecurityEvents%)) and \
              ($EventID NOT IN (%OtherEvents%)) drop();
</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     192.168.3.50
```

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
```

1.3.2.2 輸出應用程式、安全性、系統全部事件記錄

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.3.50
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>

## Windows Server 2008 or higher Event Log use the following:
<Input in_eventlog>
   Module           im_msvistalog
   ReadFromLast TRUE
   SavePos          TRUE
   Query <QueryList>\
                <Query Id="0">\
                    <Select Path="Application">*</Select>\
                    <Select Path="Security">*</Select>\
                    <Select Path="System">*</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      192.168.3.50
```

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
```

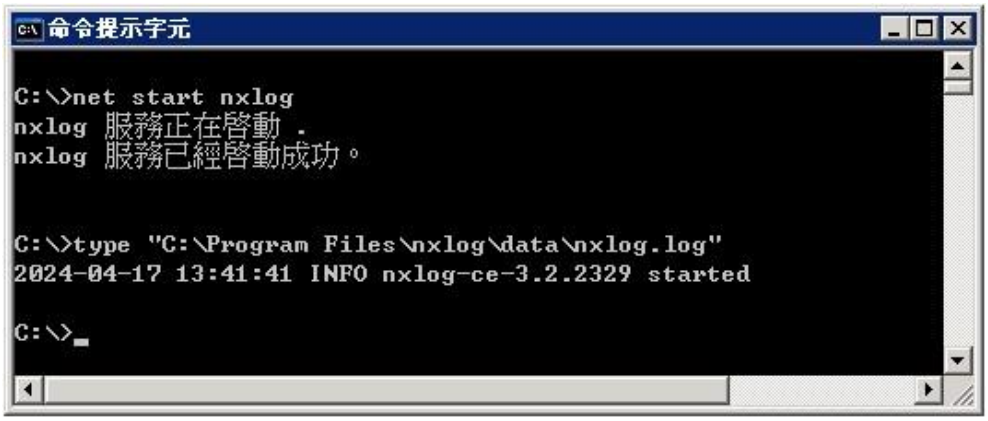
1.4 NXLog 啟動服務

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"
```

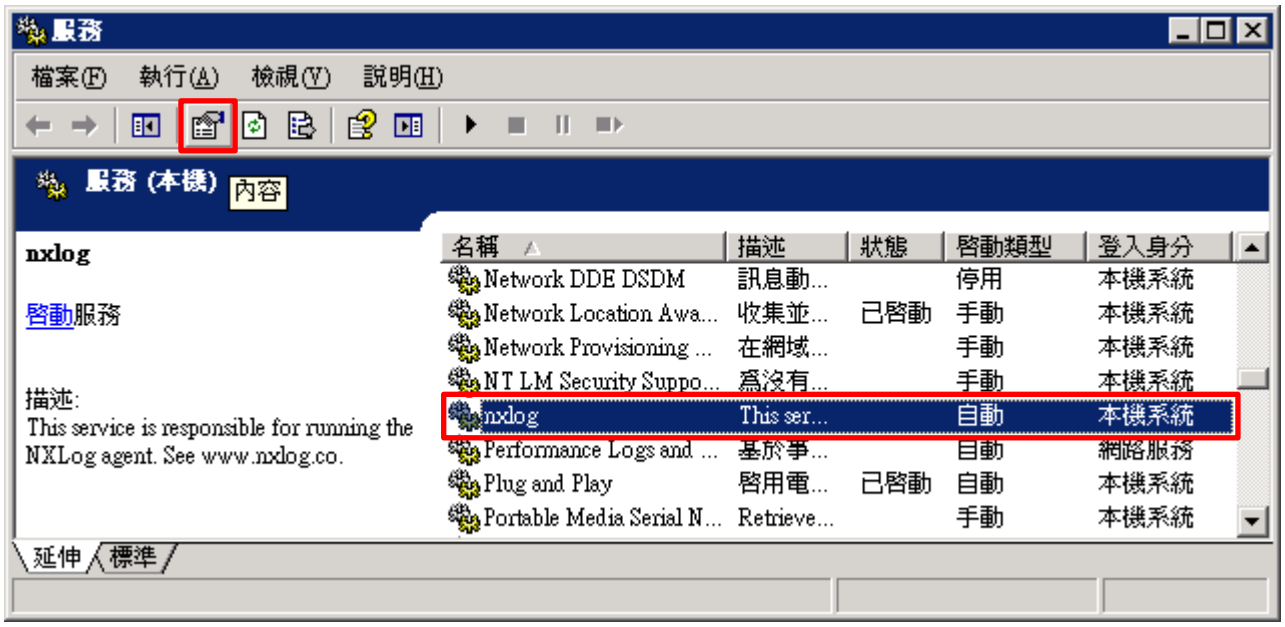


(3) 開啟 [服務] 功能

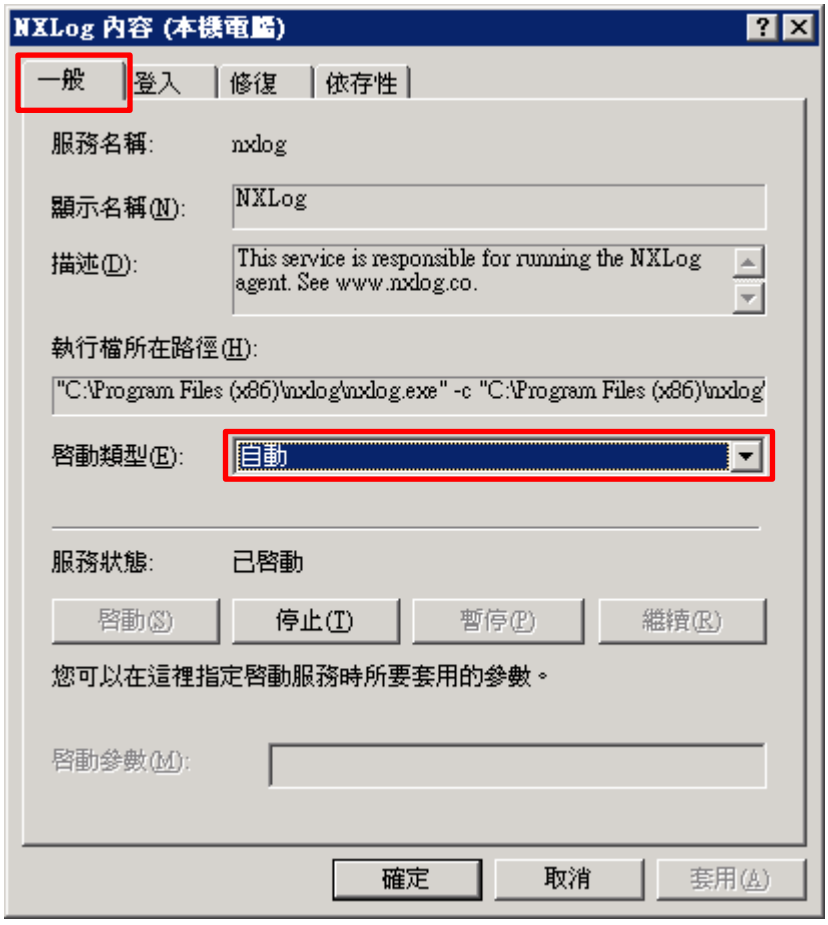
```
C:\> Services.msc
```

(4) 開啟 NXLog 服務內容

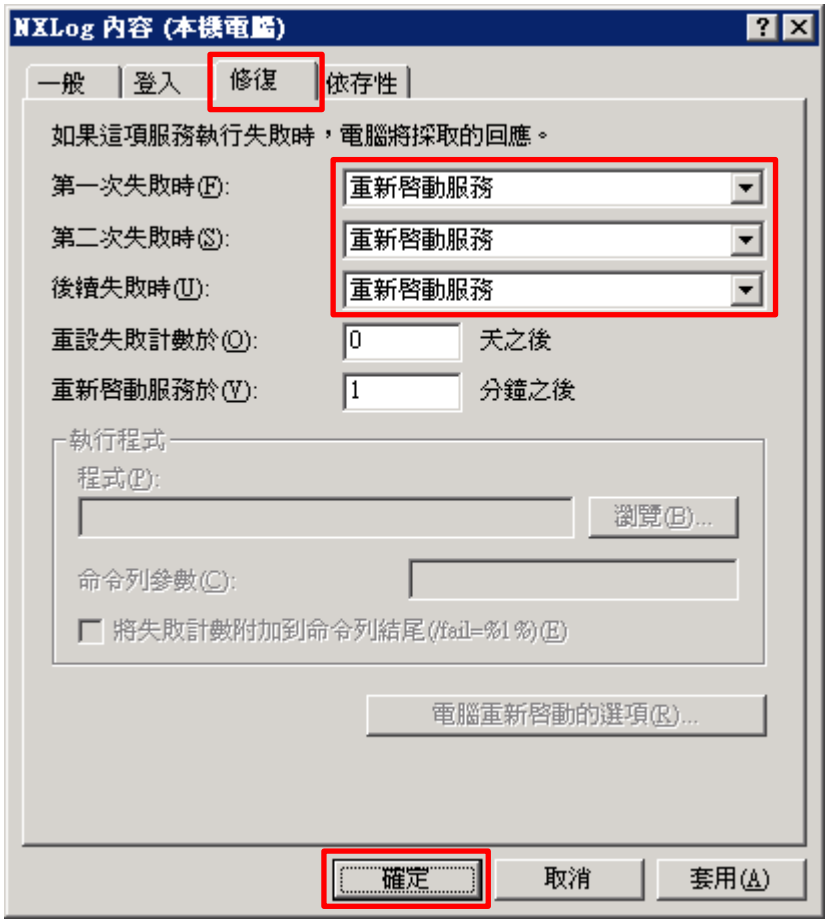
選擇 [nxlog] -> 點選  [內容]



(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]

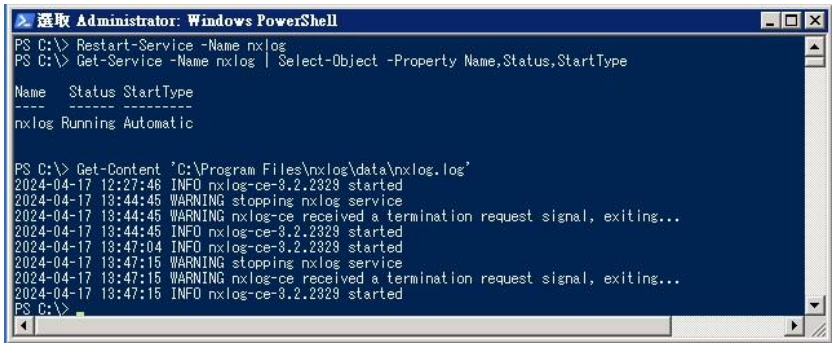


1.4.2 Windows 2008 或之後版本作業系統

(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'
```

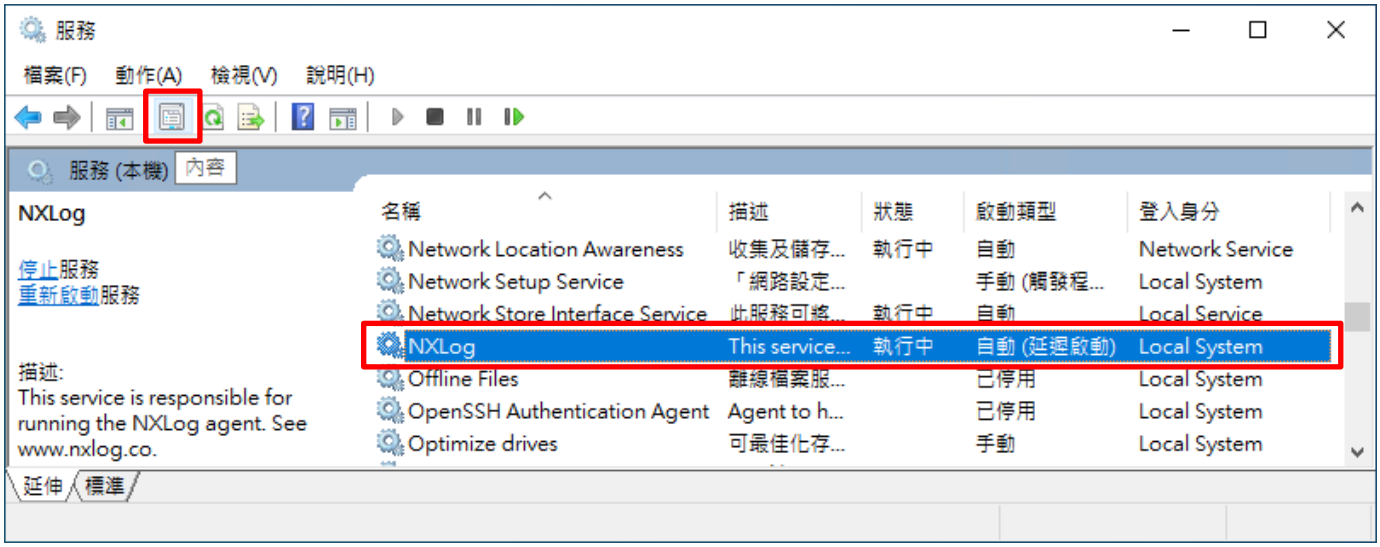


(3) 開啟 [服務] 功能

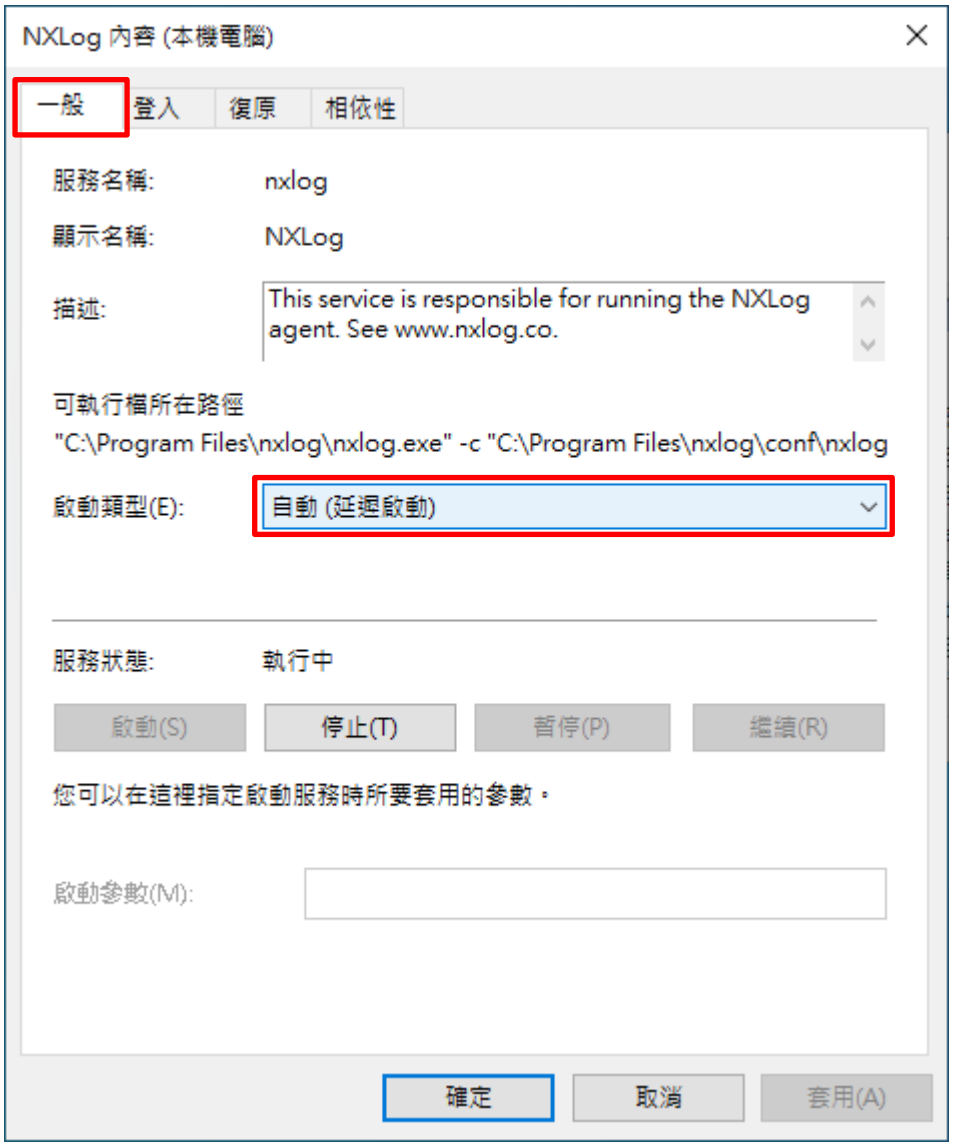
```
PS C:\> Services.msc
```

(4) 開啟 NXLog 服務內容

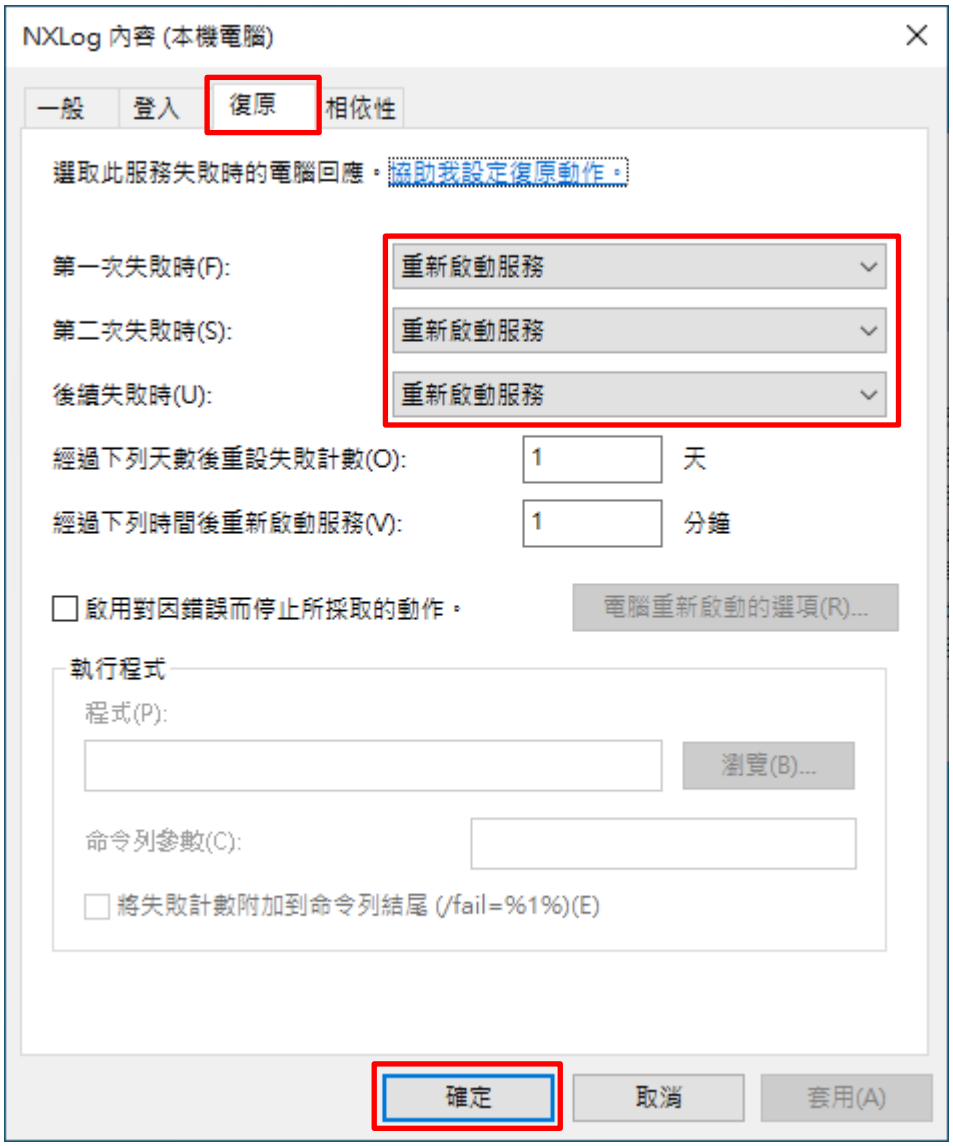
選擇 [NXLog] -> 點選  [內容]



(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

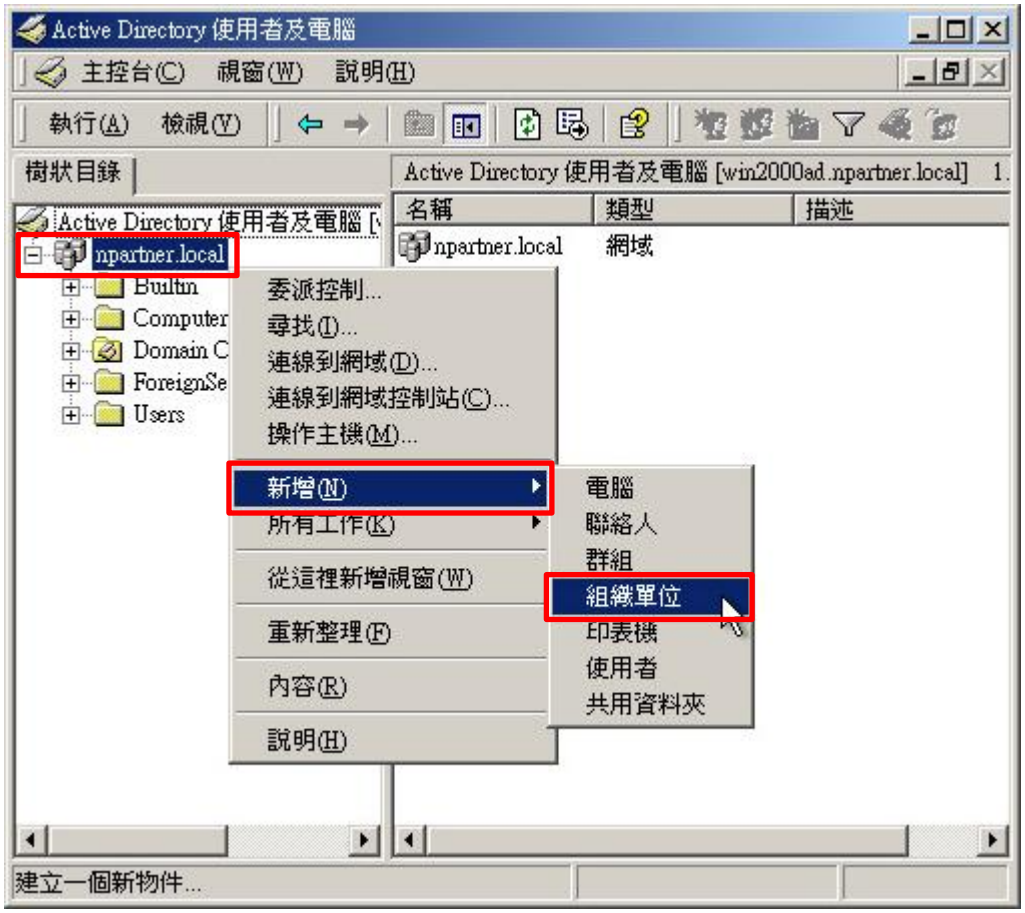
2.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

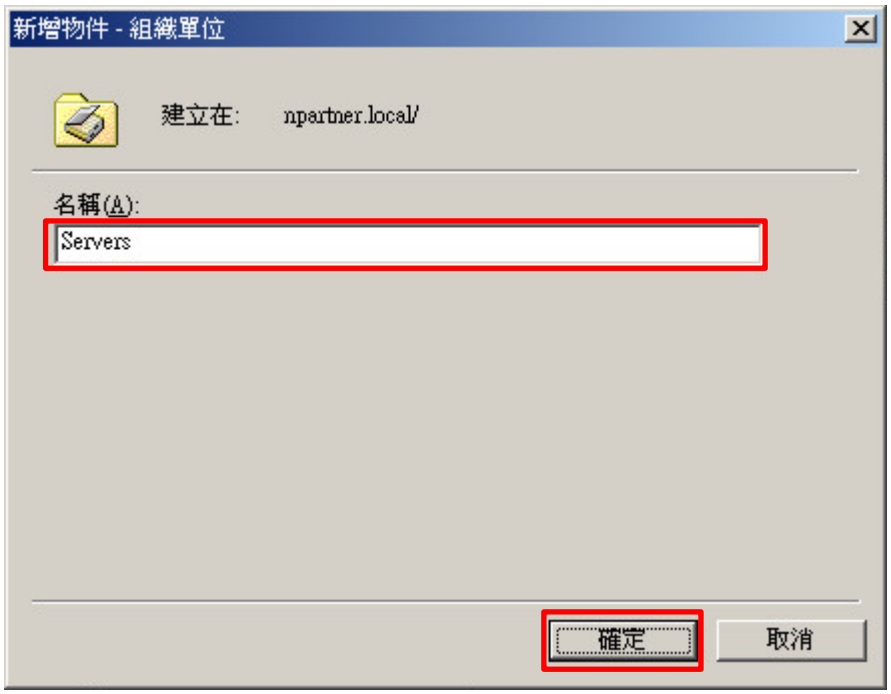
(2) 新增組織單位

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

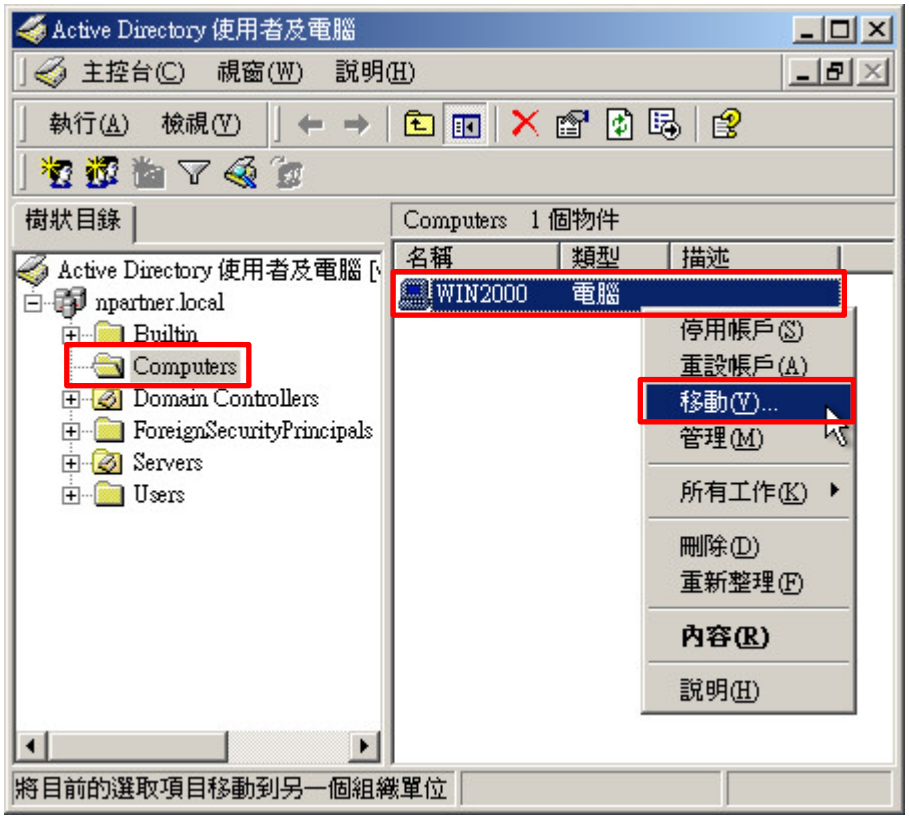
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(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 Server 主機

-> 點選 [移動]

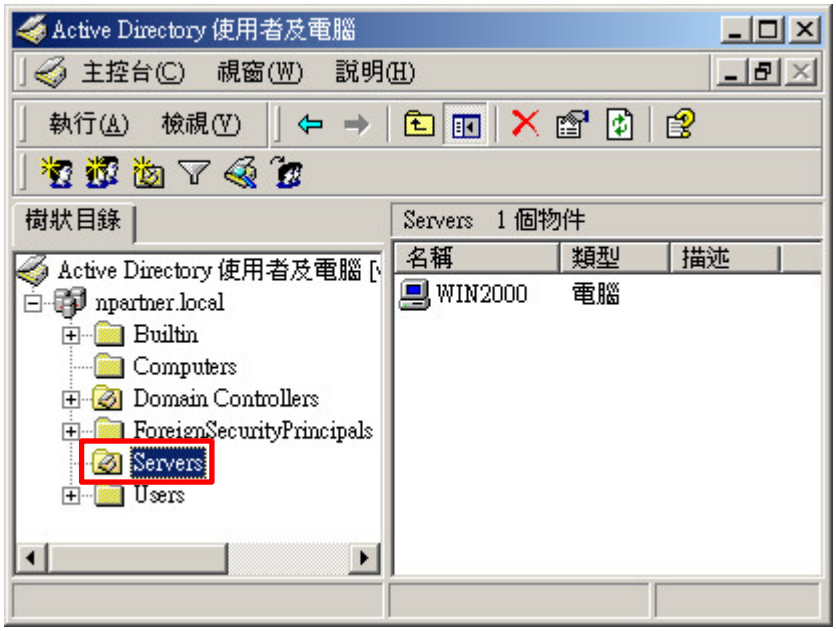


(5) 選擇組織單位

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 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

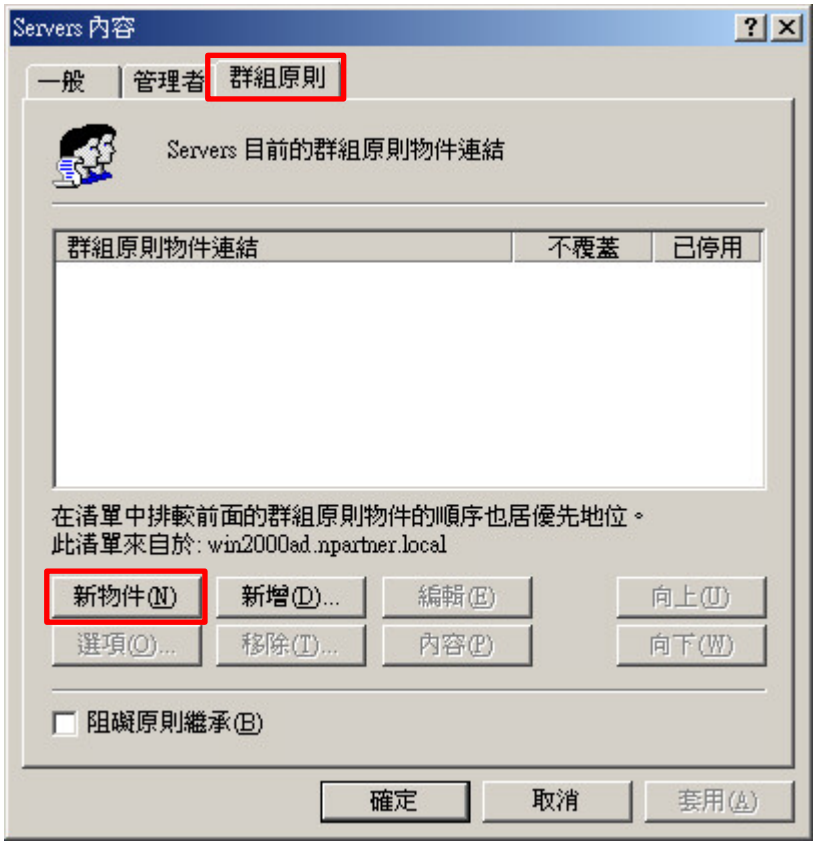
開啟 [Active Directory 使用者和電腦]

(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]

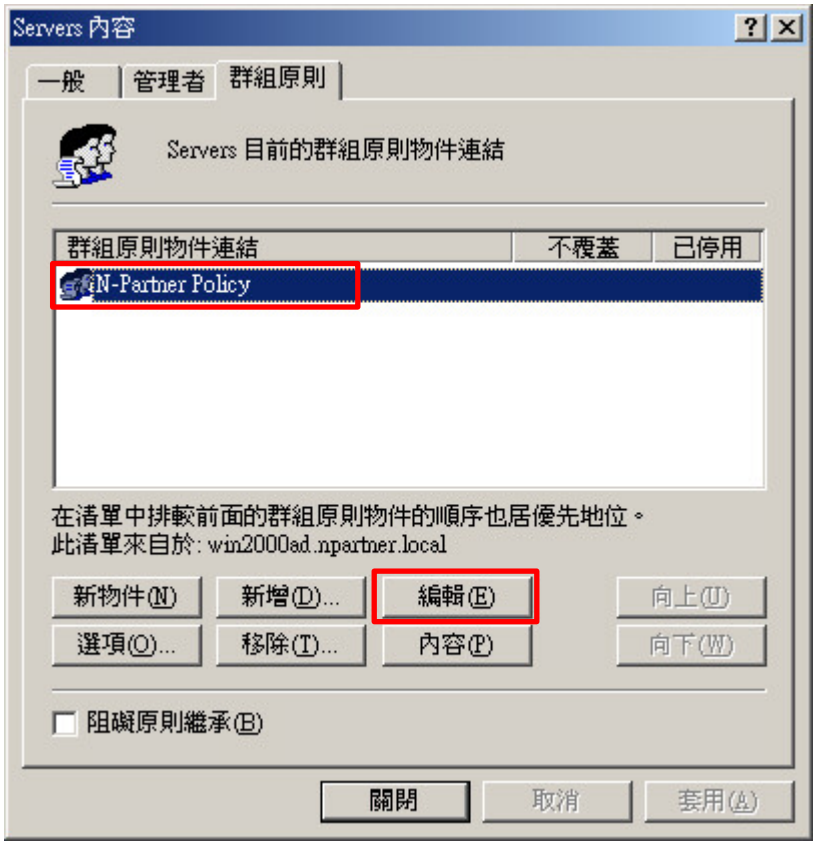
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



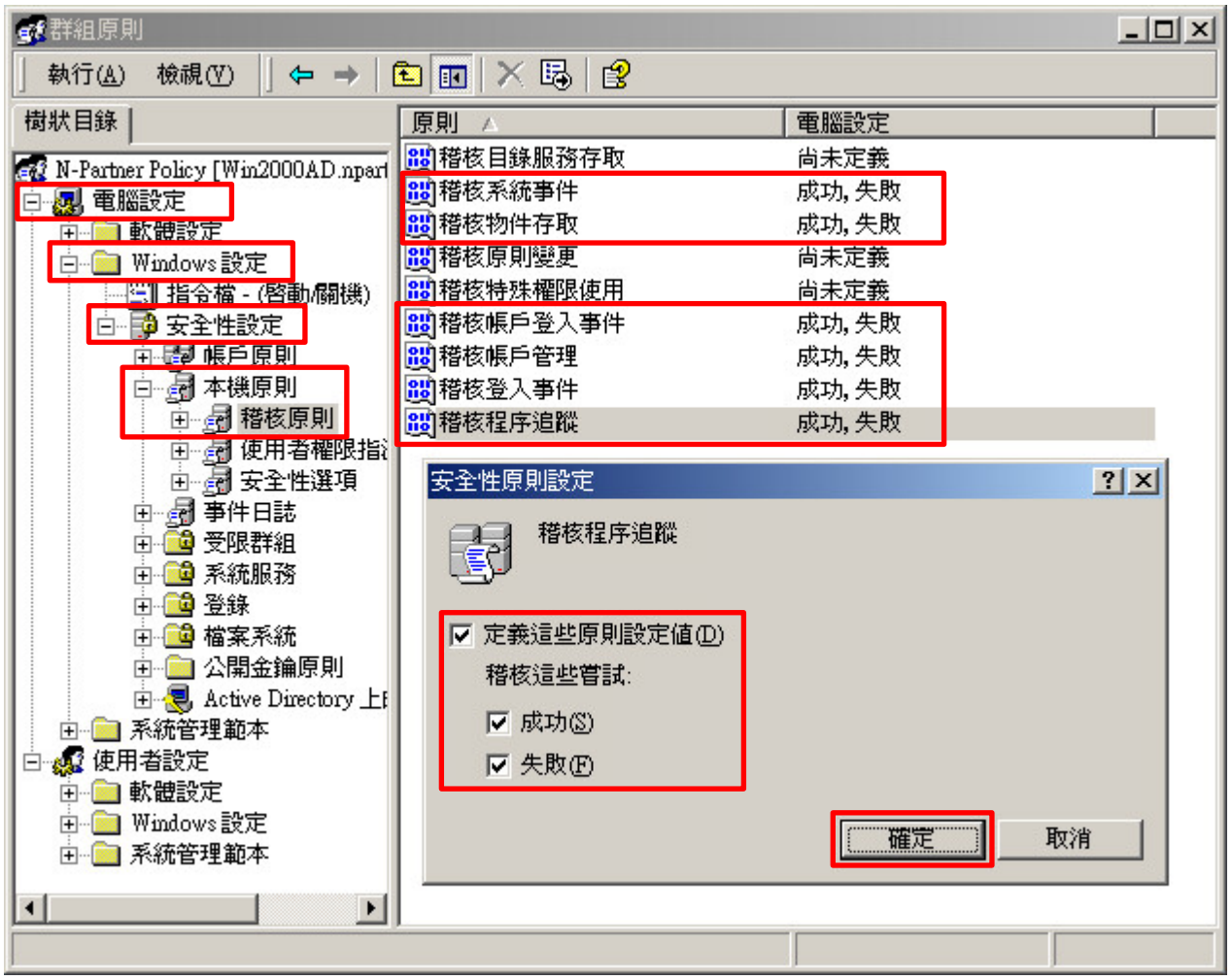
(4) 編輯群組原則物件

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]



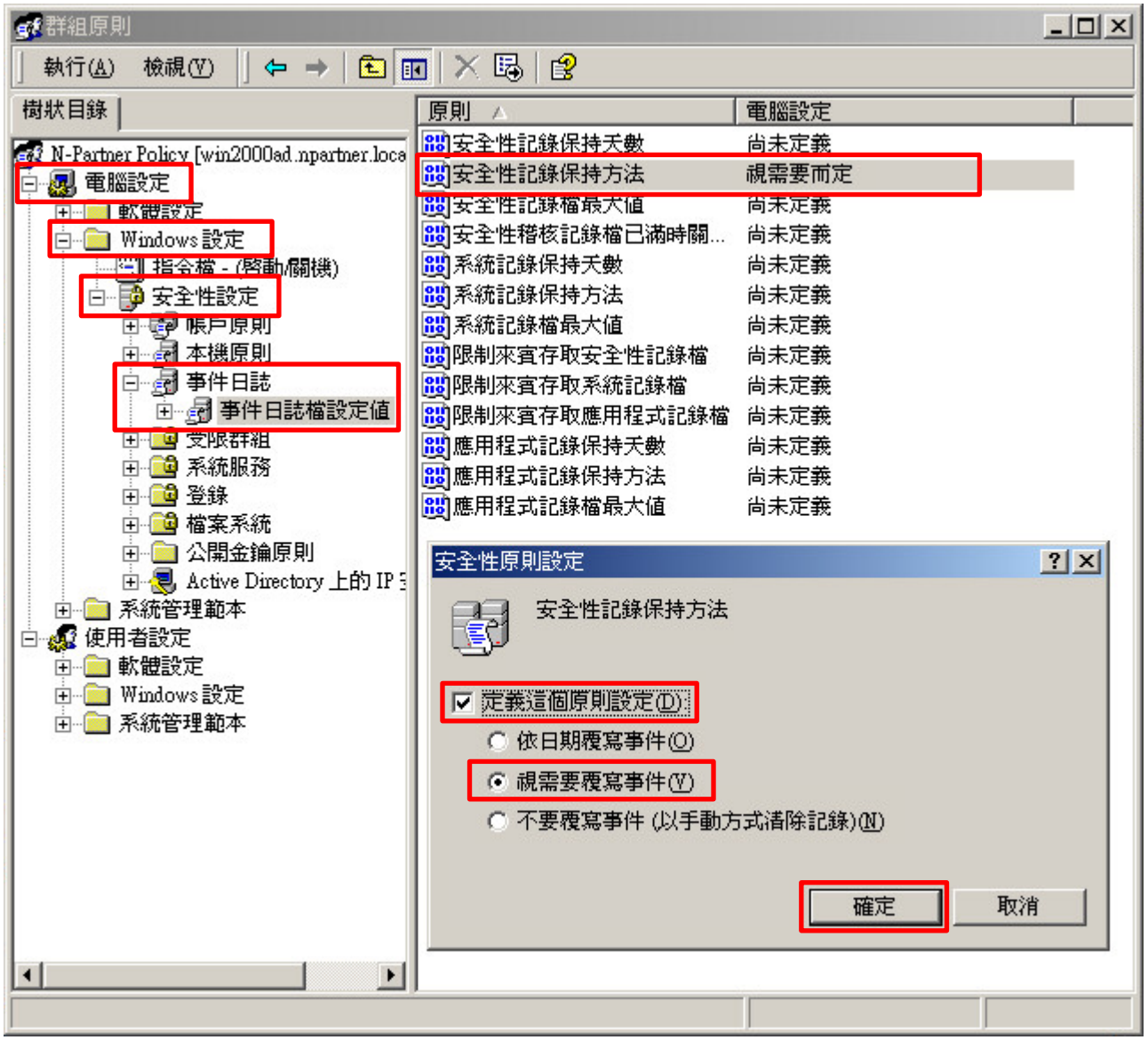
(5) 本機原則：稽核原則

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



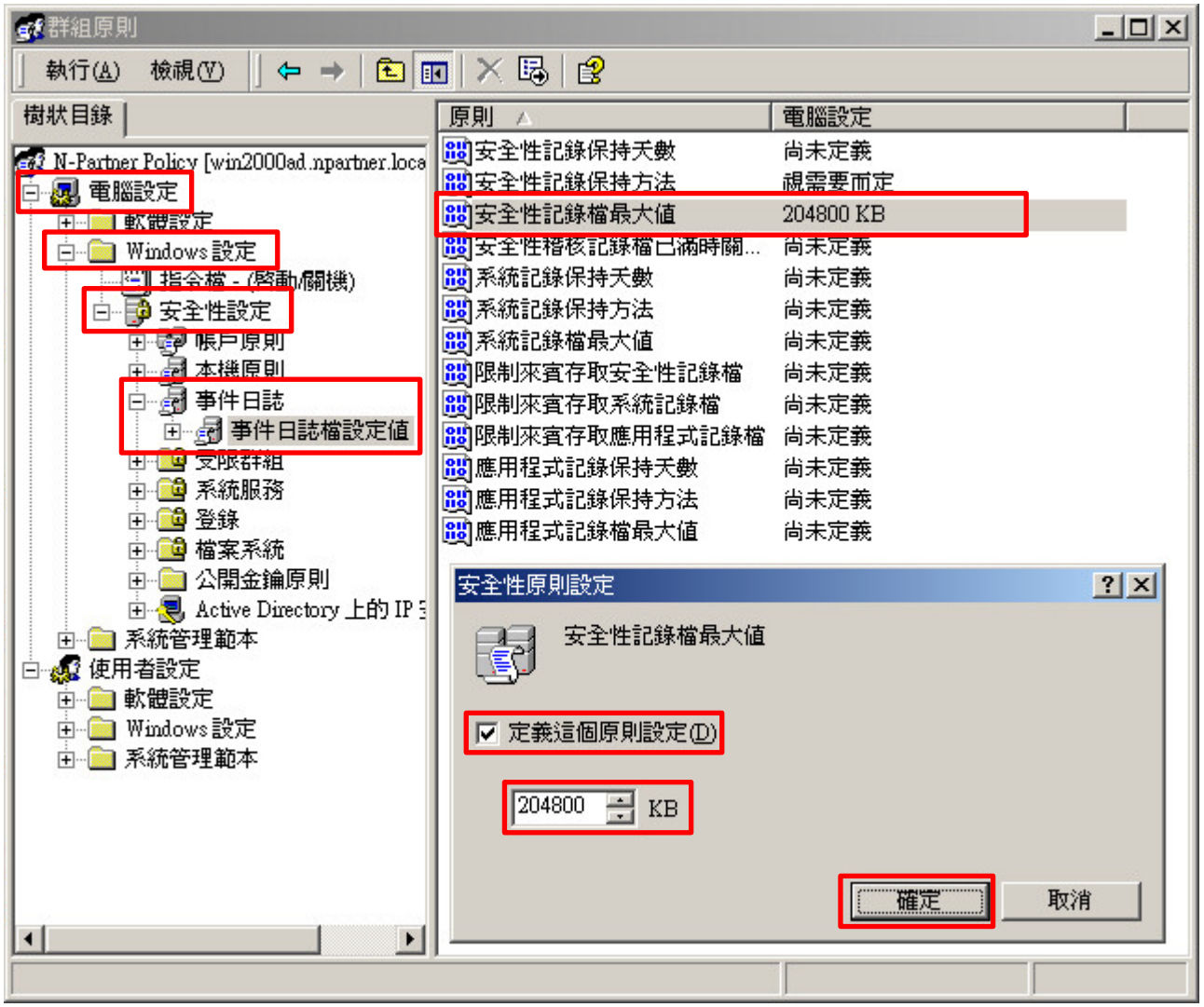
(6) 事件日誌：安全性記錄保持方法

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] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(7) 事件日誌：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] 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]



(8) 在 Windows Server 伺服器，開啟 [命令提示字元]

(9) 更新群組原則。

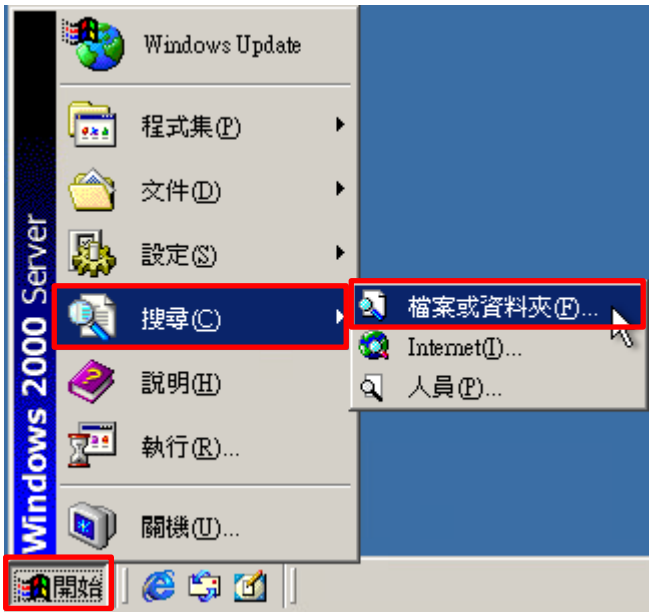
```
C:\> secedit /refreshpolicy machine_policy /enforce
```

2.2 工作群組

2.2.1 稽核原則設定

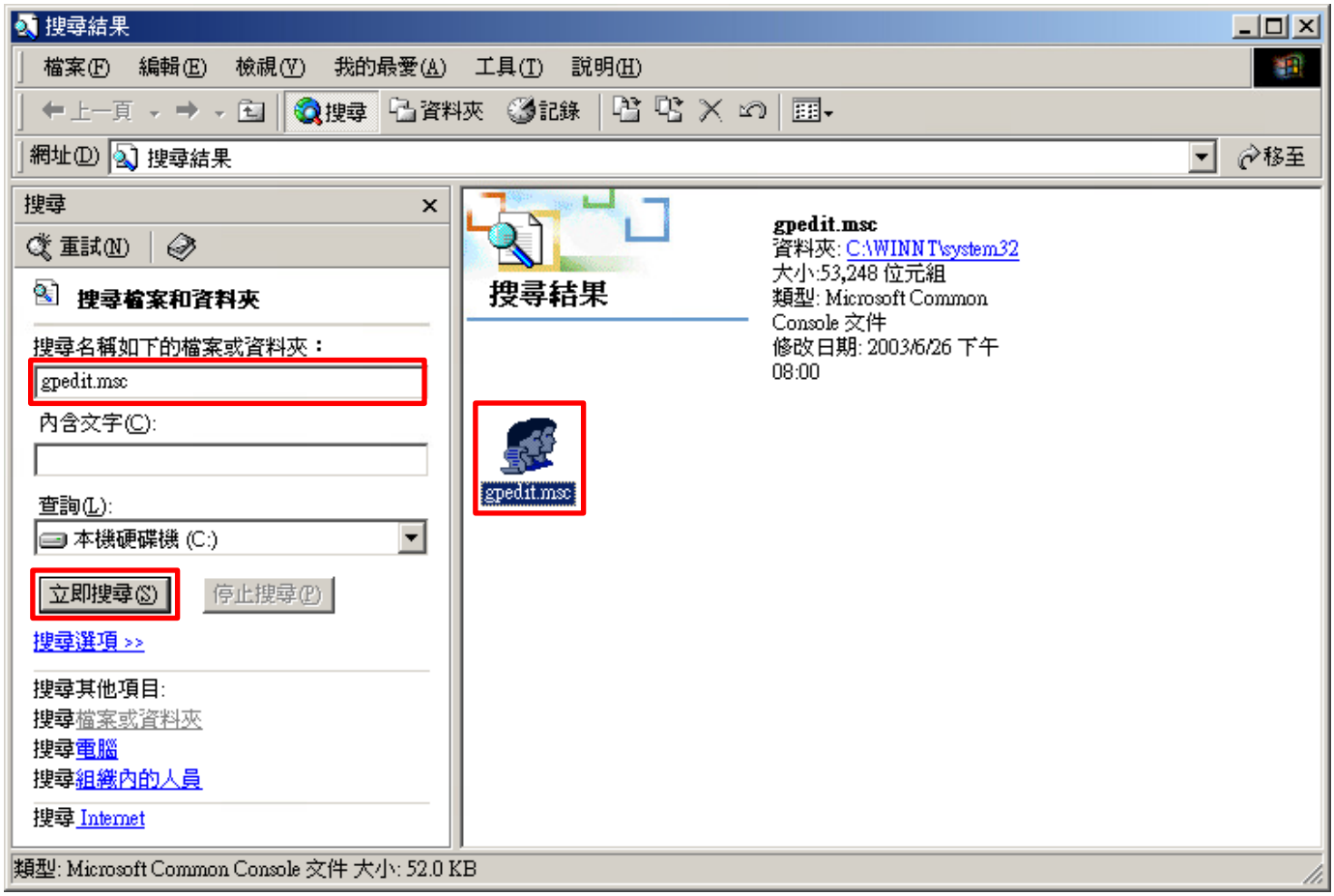
(1) 開啟搜尋

點選 [開始] -> [搜尋] -> [檔案或資料夾]



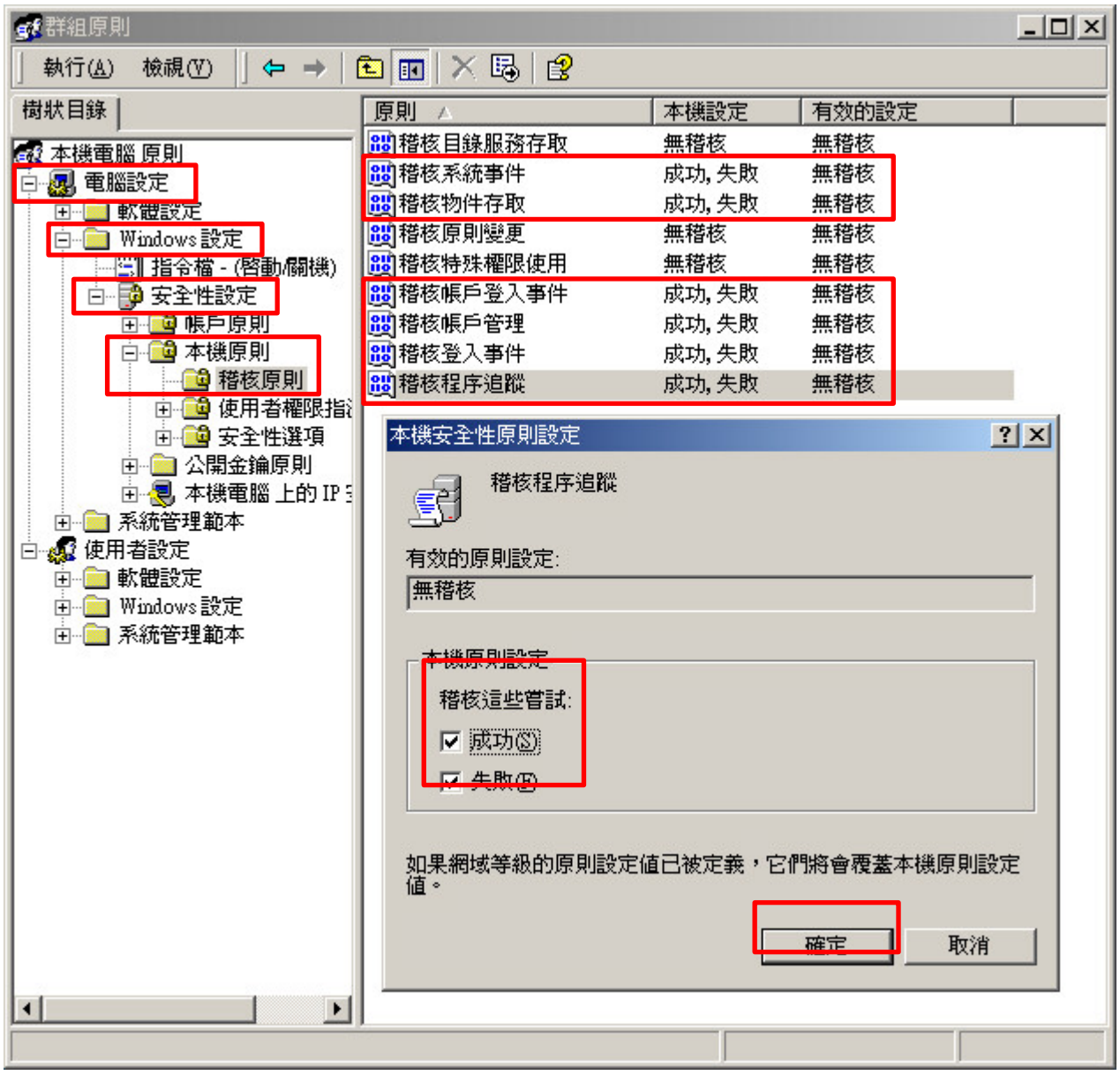
(2) 搜尋群組原則

輸入 gpedit.msc -> 按 [立即搜尋] -> 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 [稽核系統事件], [稽核物件存取], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 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]

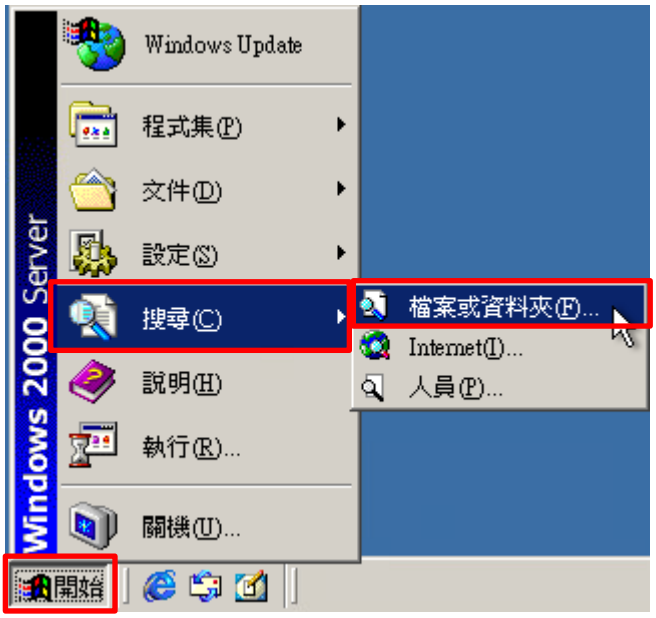
(5) 更新群組原則，

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

2.2.2 事件檔案設定

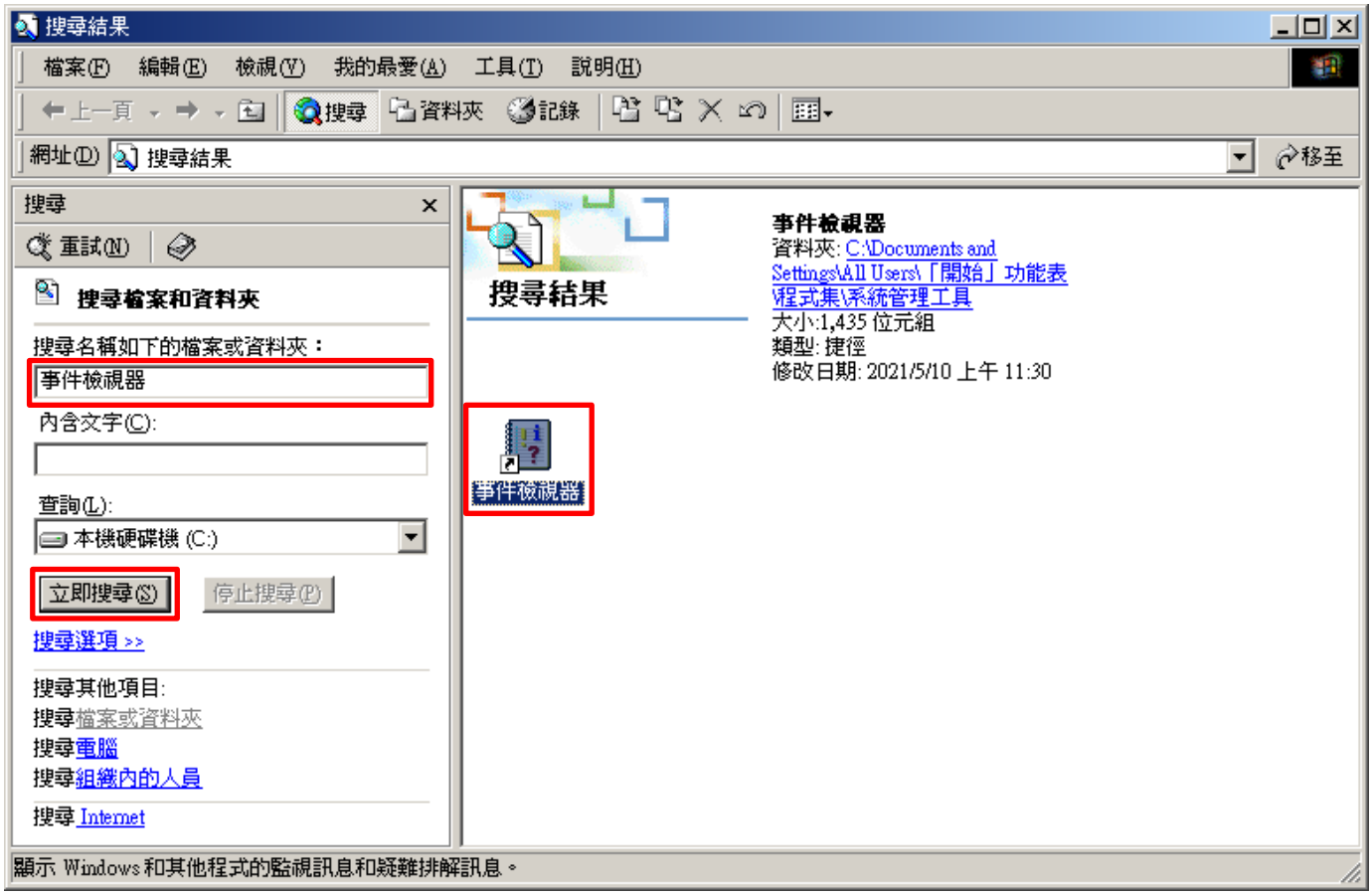
(1) 開啟搜尋

點選 [開始] -> [搜尋] -> [檔案或資料夾]



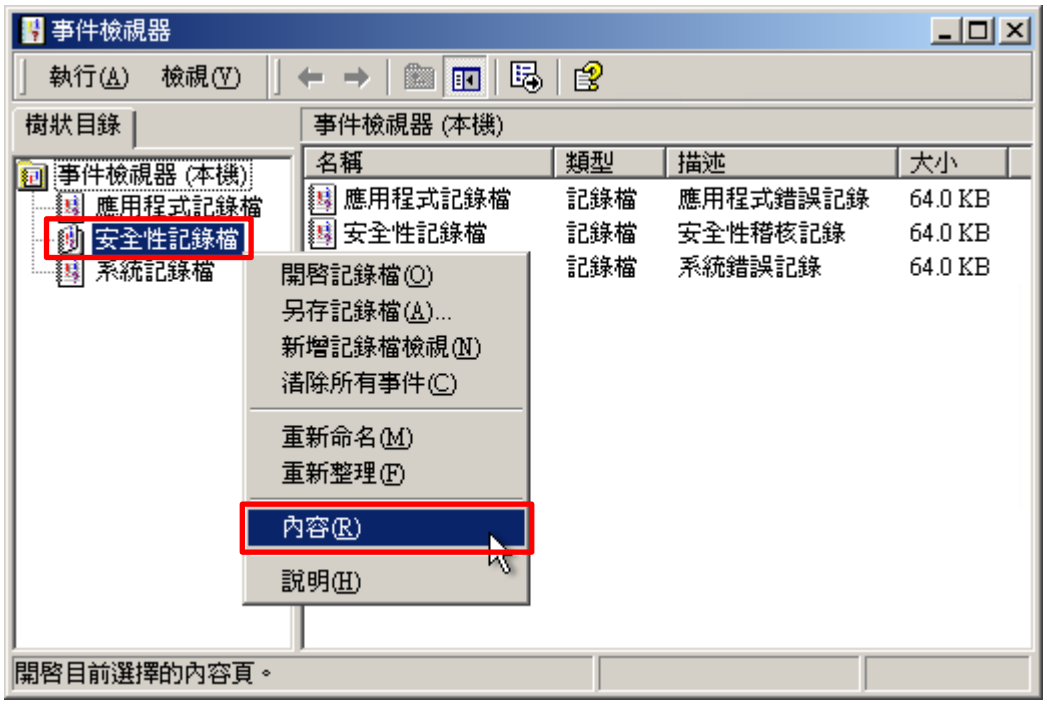
(2) 搜尋事件檢視器

輸入事件檢視器 -> 按 [立即搜尋] -> 點選 [事件檢視器]



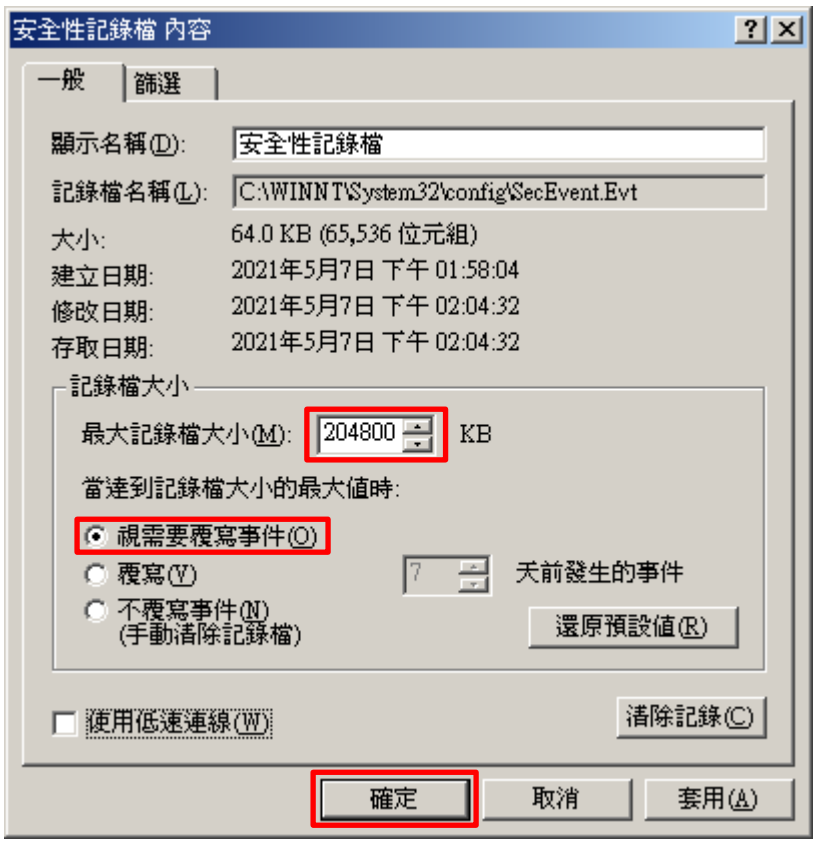
(3) 編輯安全性記錄檔

在 [安全性記錄檔] 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]



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

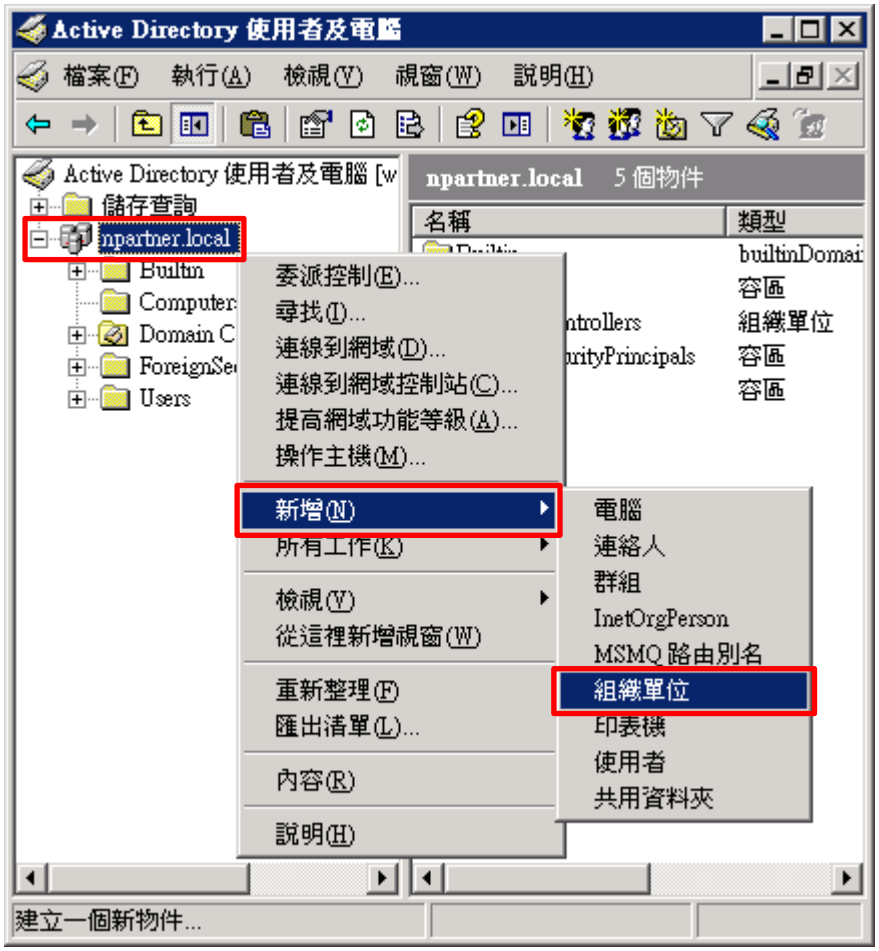
3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

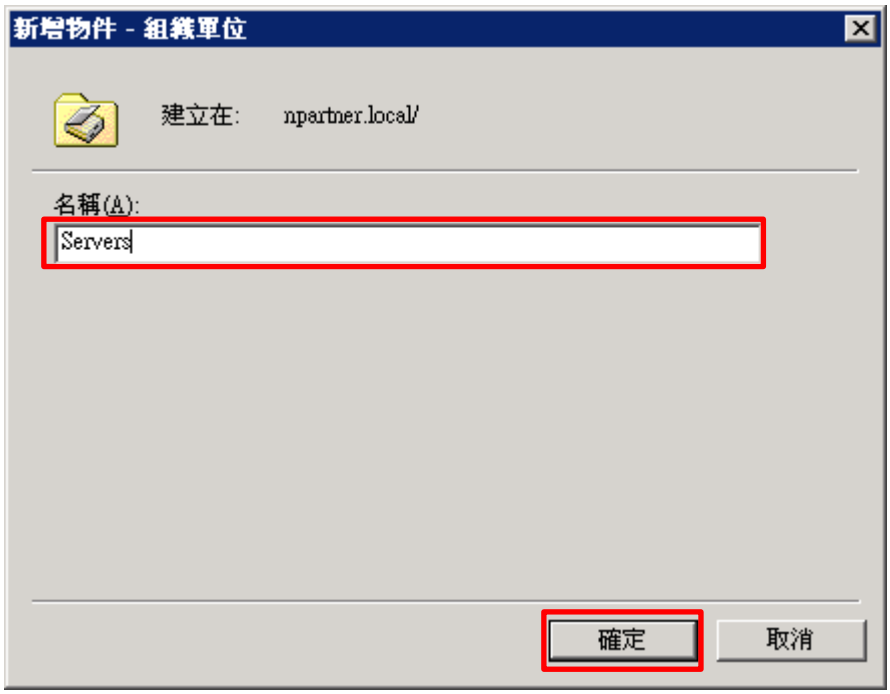
(2) 新增組織單位

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

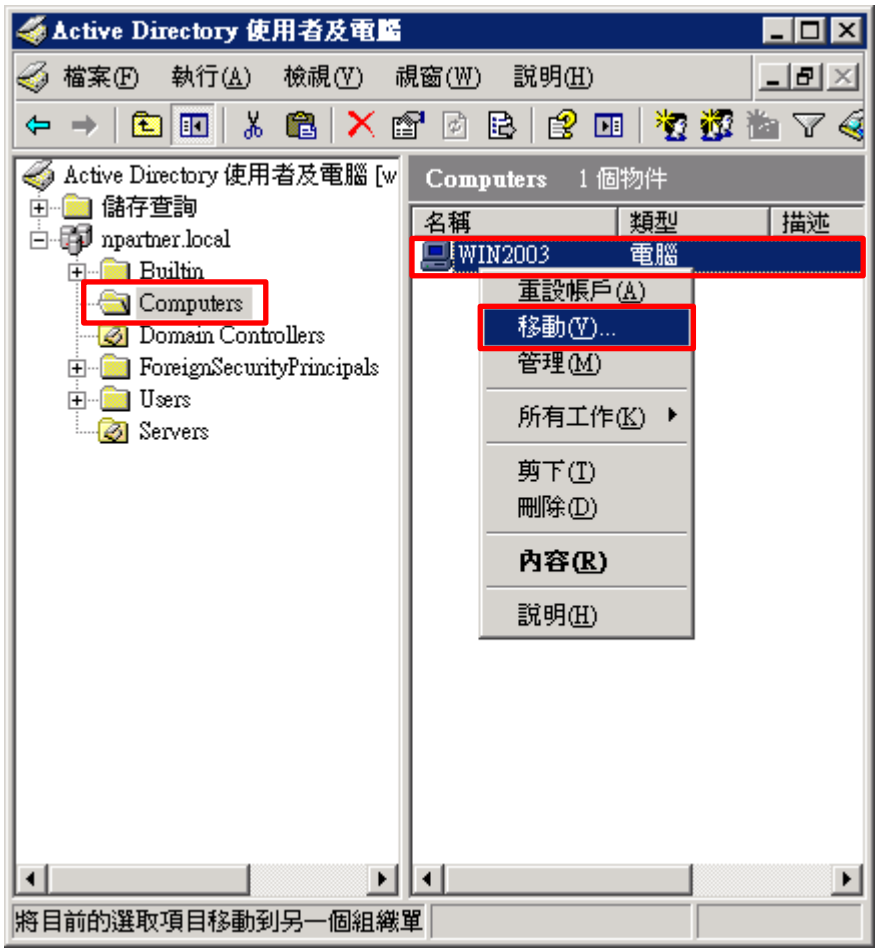
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

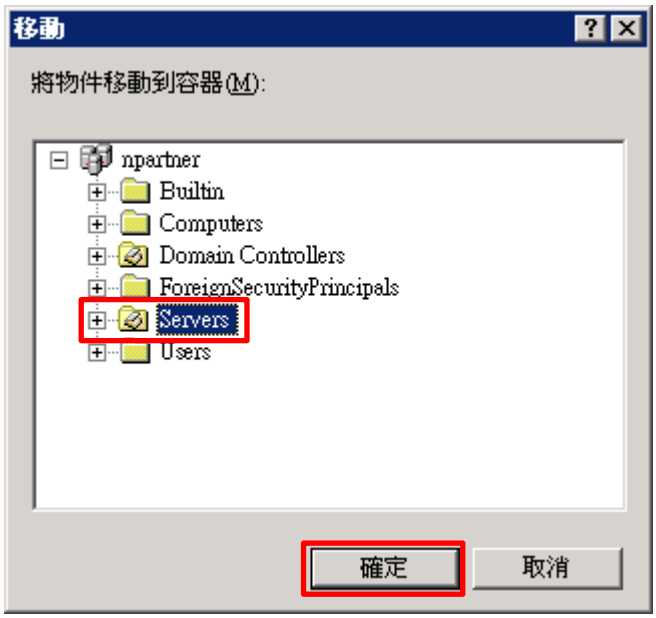
選擇 [Computers] 組織單位 -> 在 [Win2003] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



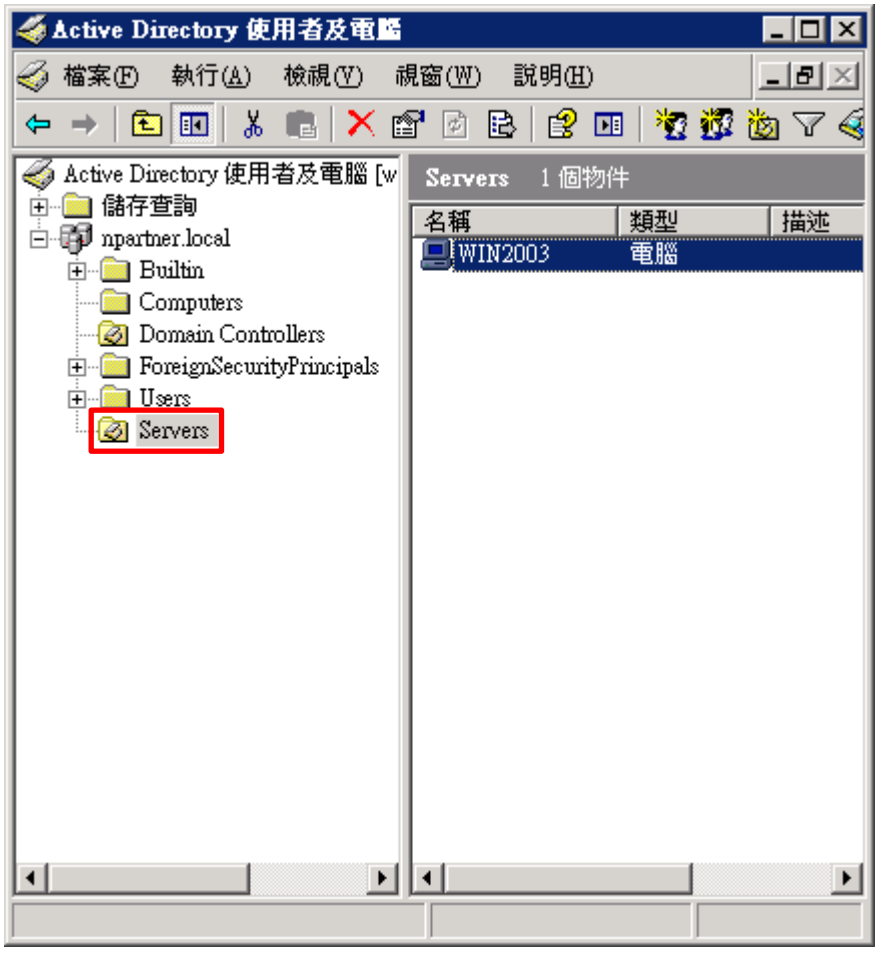
(5) 選擇組織單位

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 伺服器已移動。



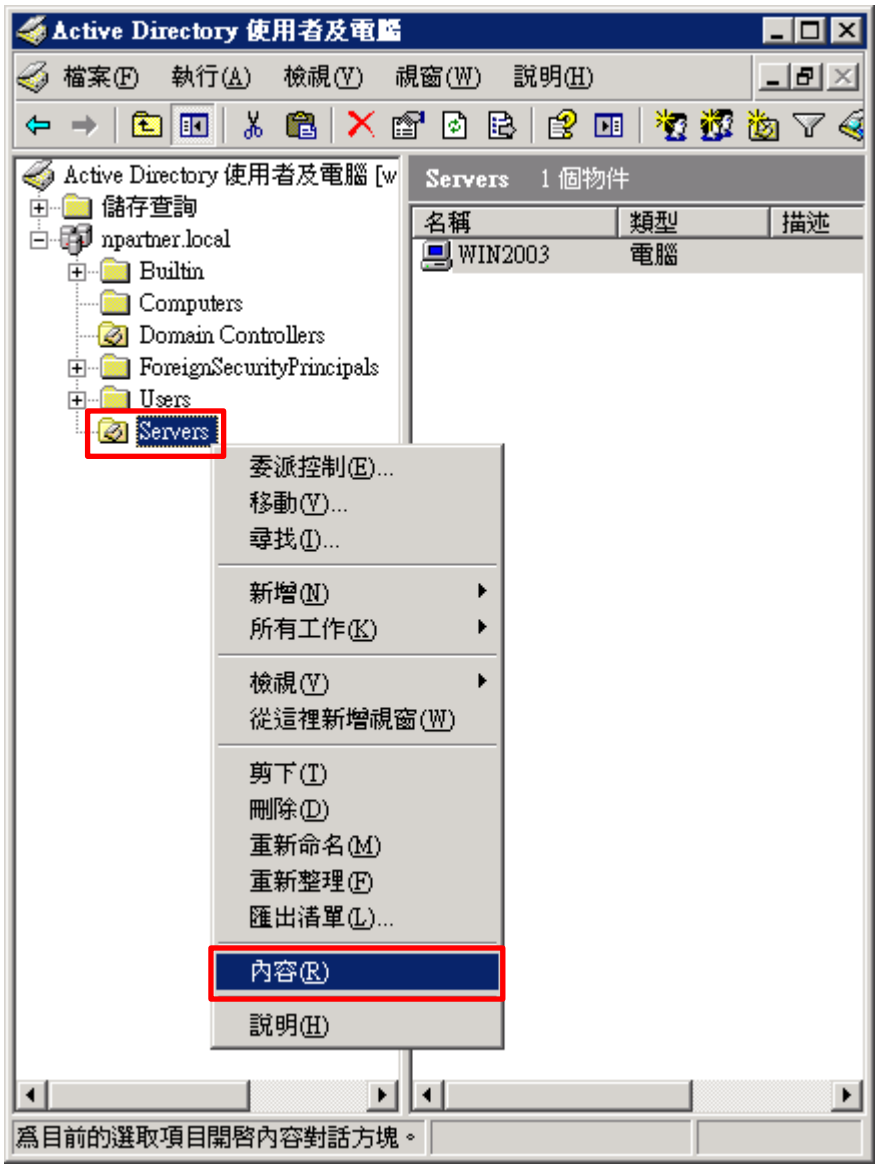
3.1.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

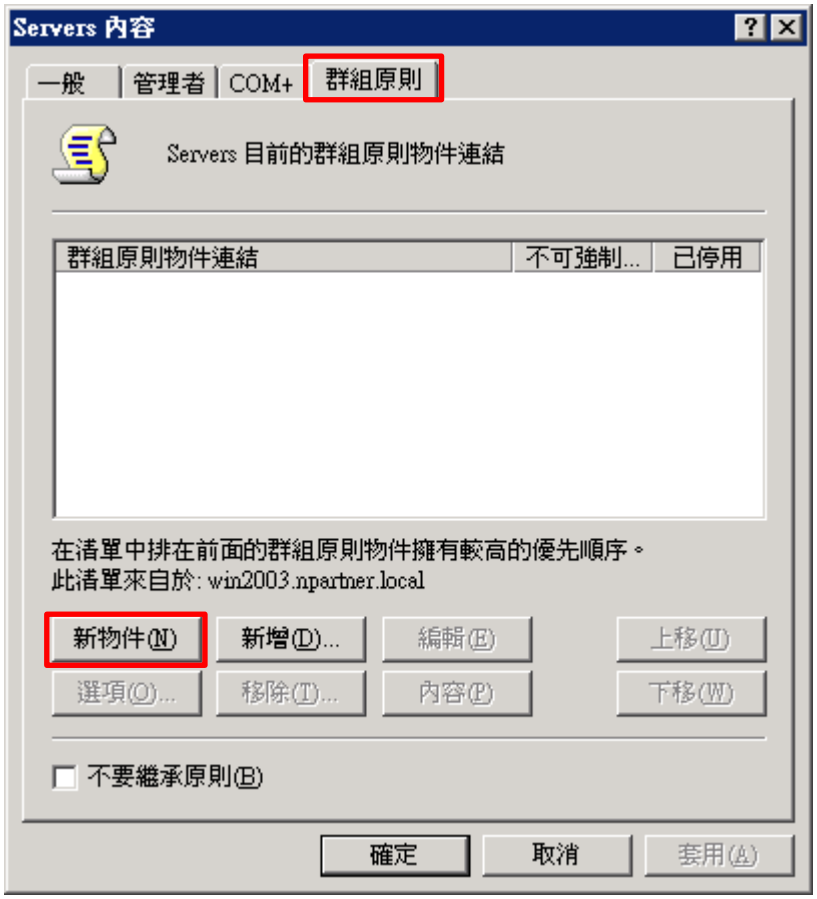
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



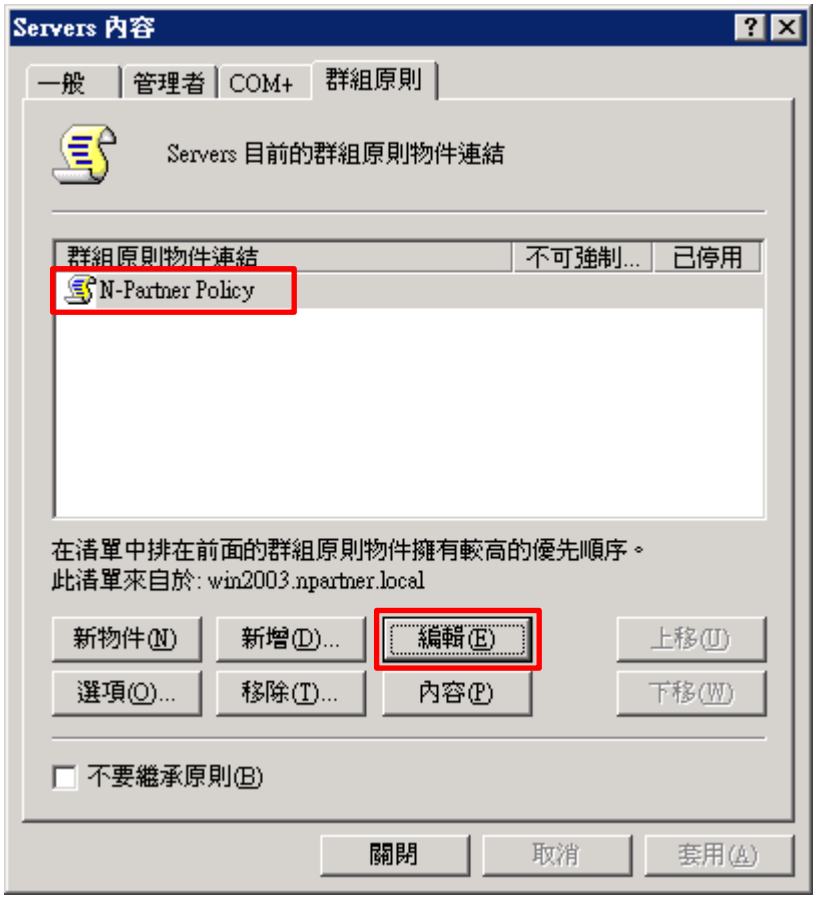
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



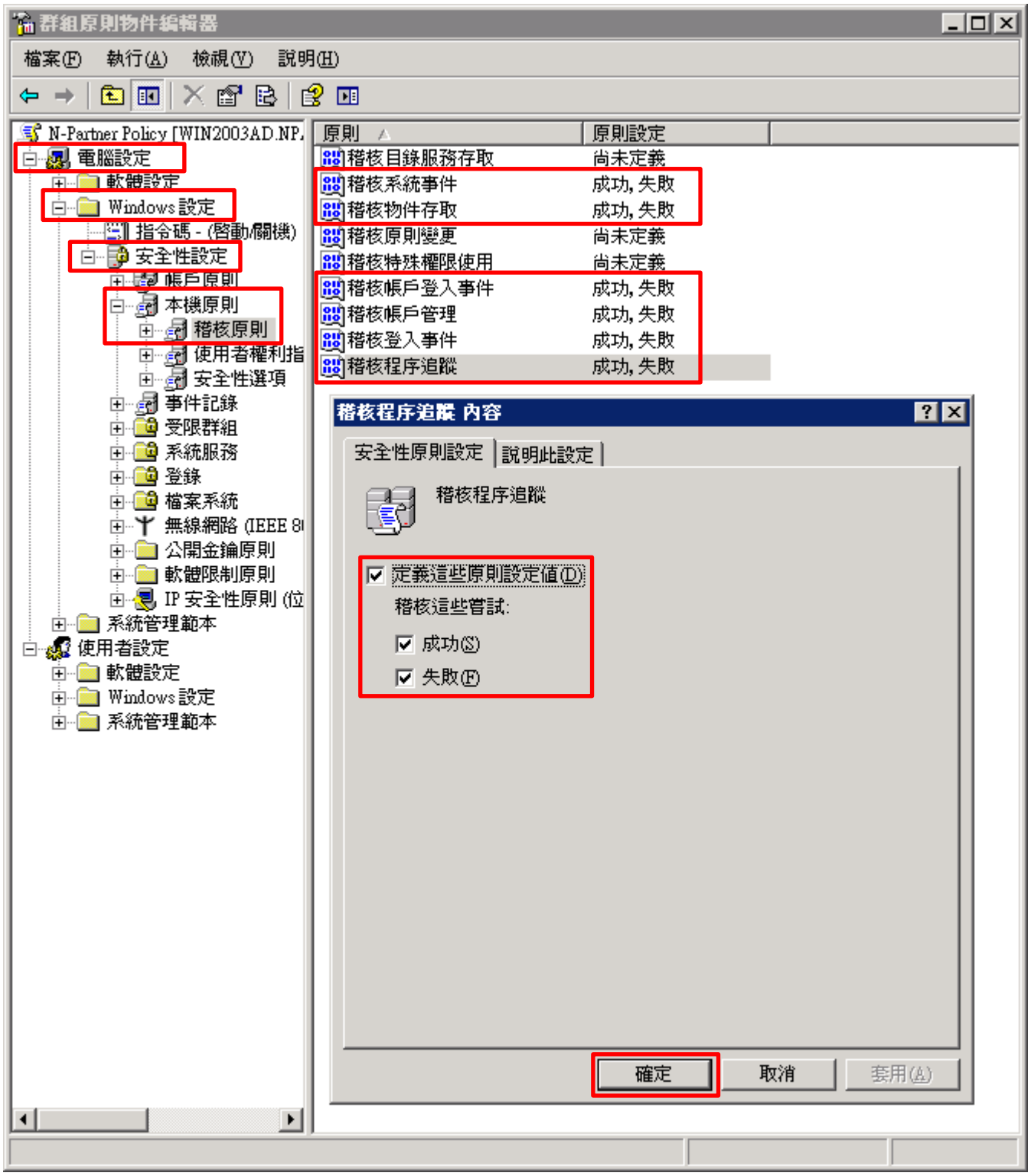
(4) 編輯群組原則物件

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]



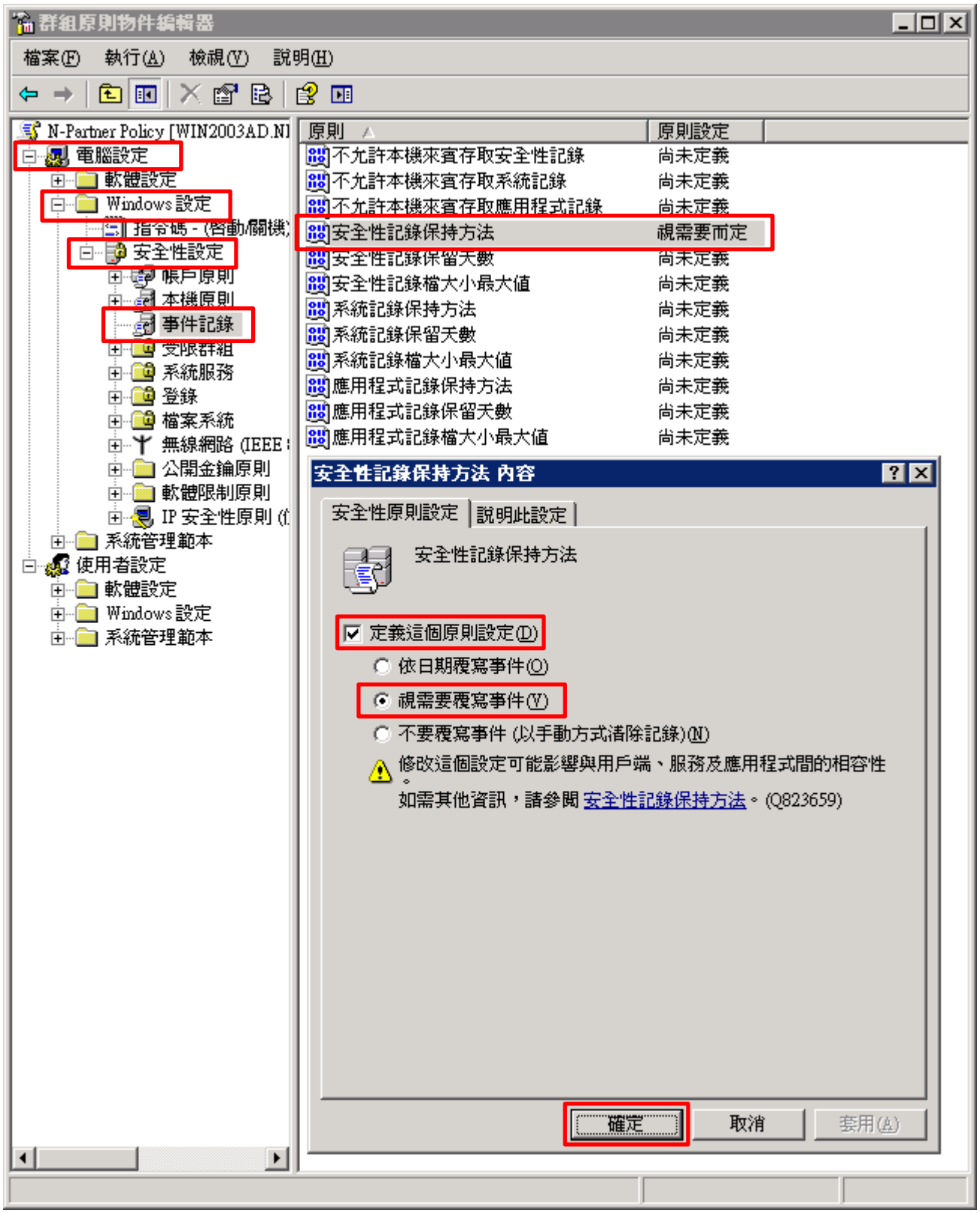
(5) 本機原則：稽核原則

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



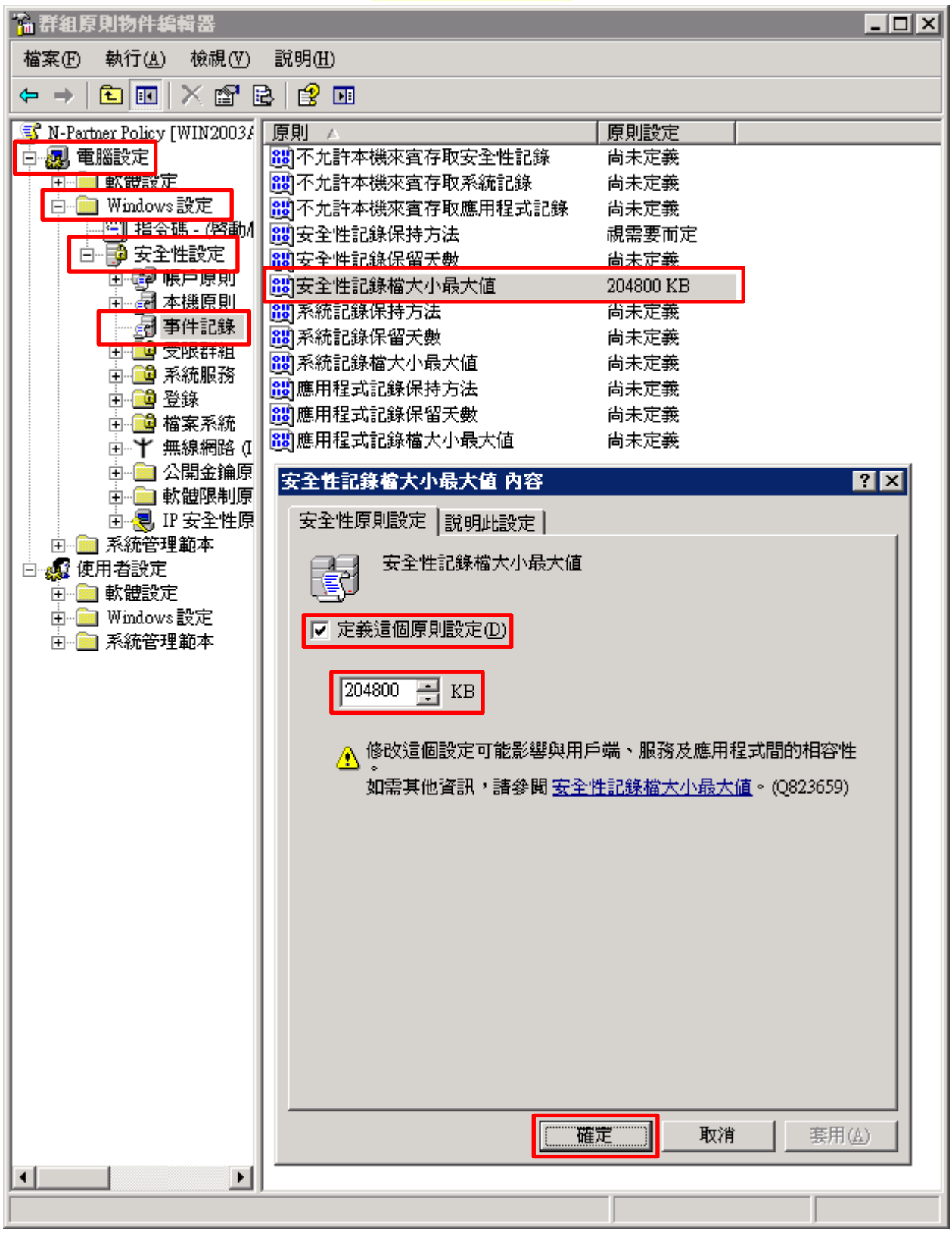
(6) 事件記錄：安全性記錄保持方法

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] 項目 -> 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：安全性記錄檔大小最大值

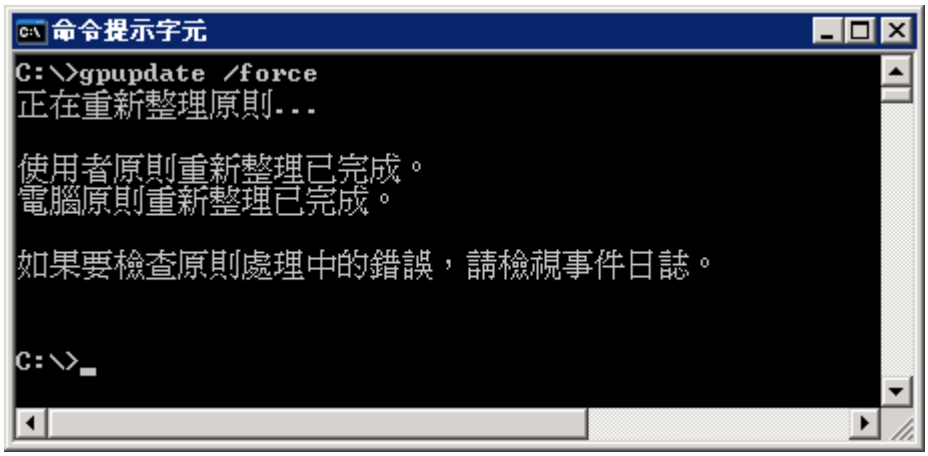
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8) 在 Windows Server 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

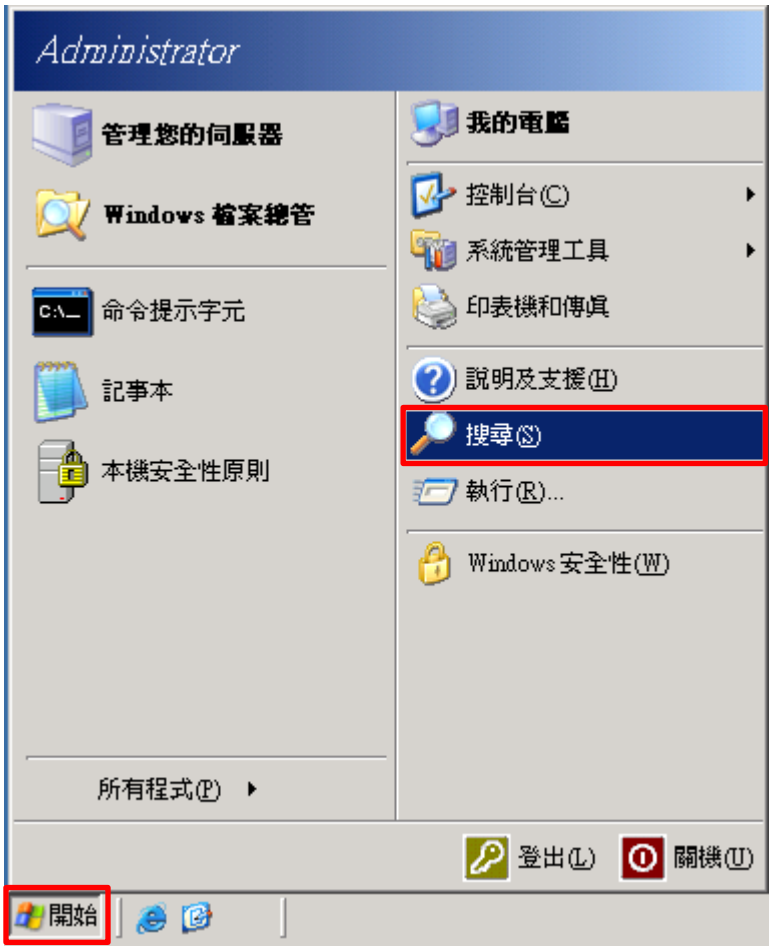
```
C:\> gpresult /v
```

3.2 工作群組

3.2.1 稽核原則設定

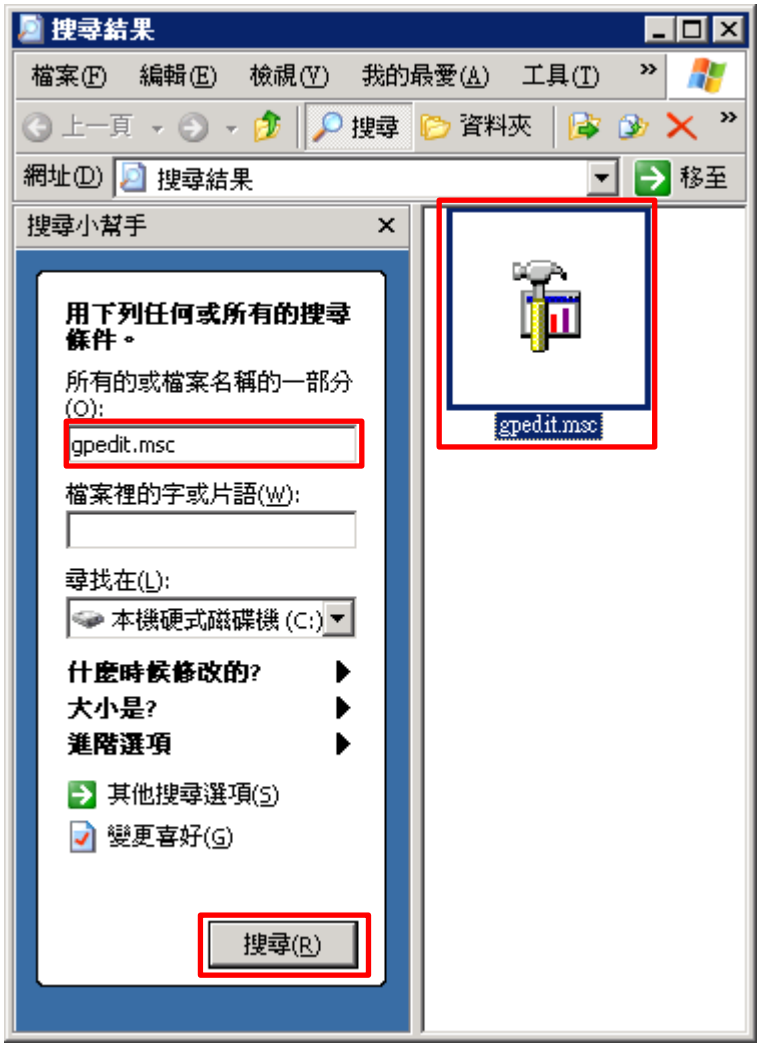
(1) 開啟搜尋

點選 [開始] -> [搜尋]



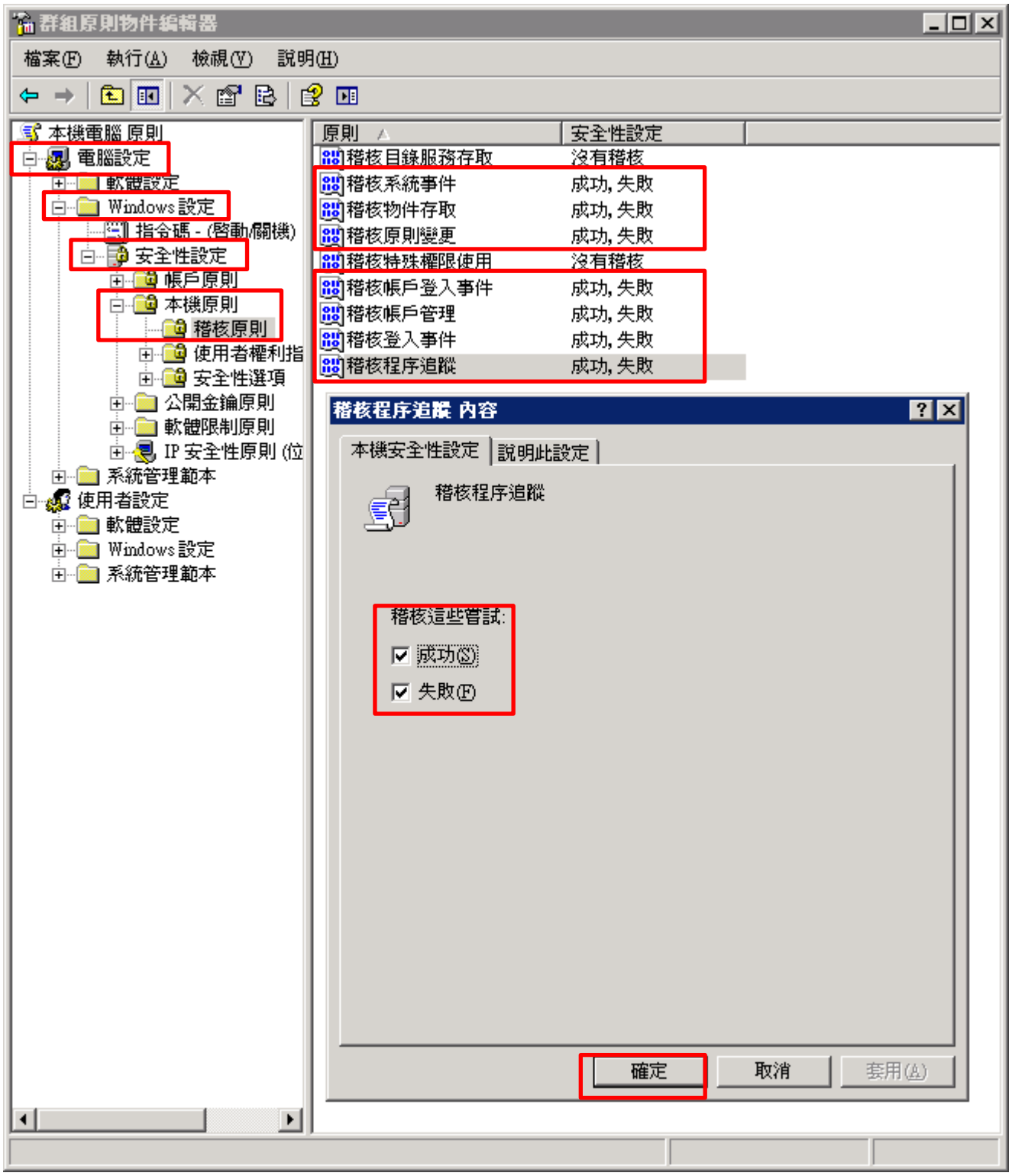
(2) 搜尋群組原則物件編輯器

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



(3) 本機原則：稽核原則

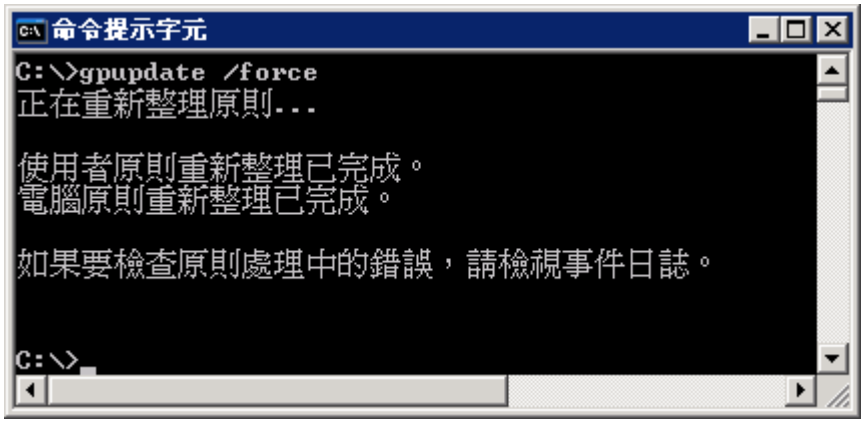
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(4) 開啟 [命令提示字元]

(5) 更新群組原則，

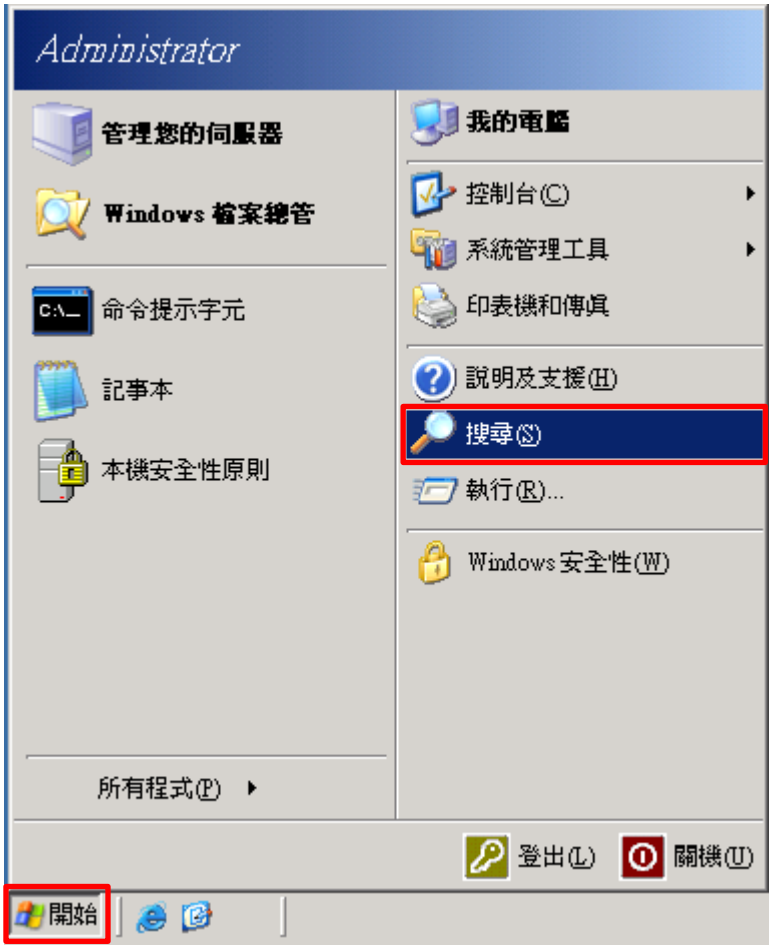
```
C:\> gpupdate /force
```



3.2.2 事件檔案設定

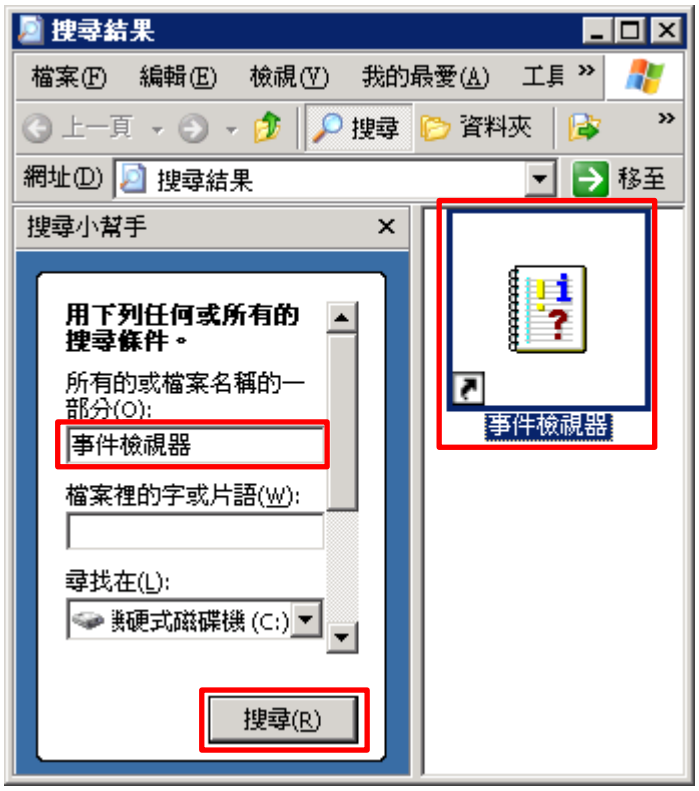
(1) 開啟搜尋

點選 [開始] -> [搜尋]



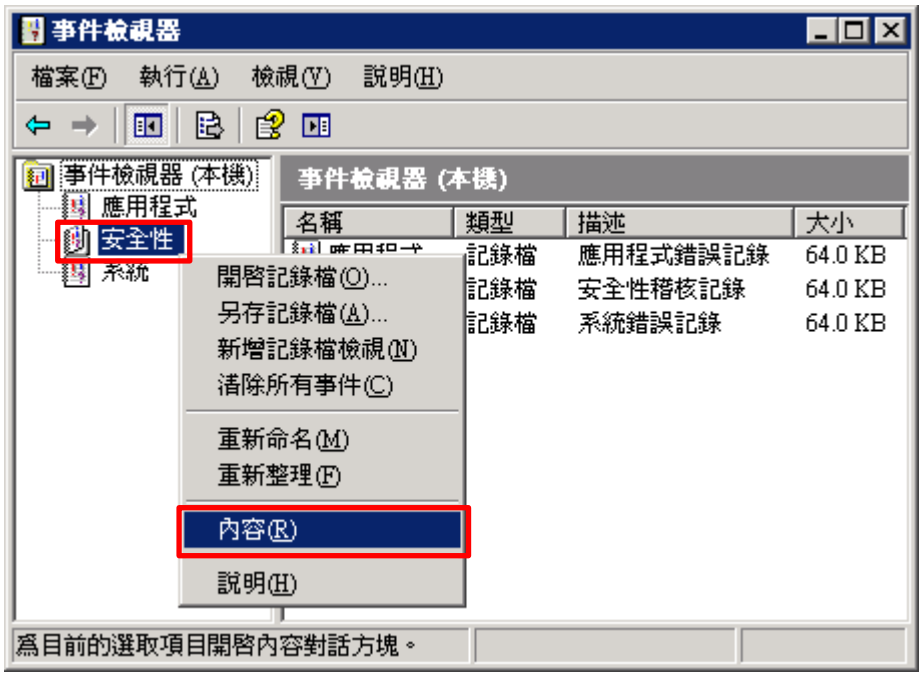
(2) 搜尋事件檢視器

輸入事件檢視器 -> 按 [搜尋] -> 點選 [事件檢視器]



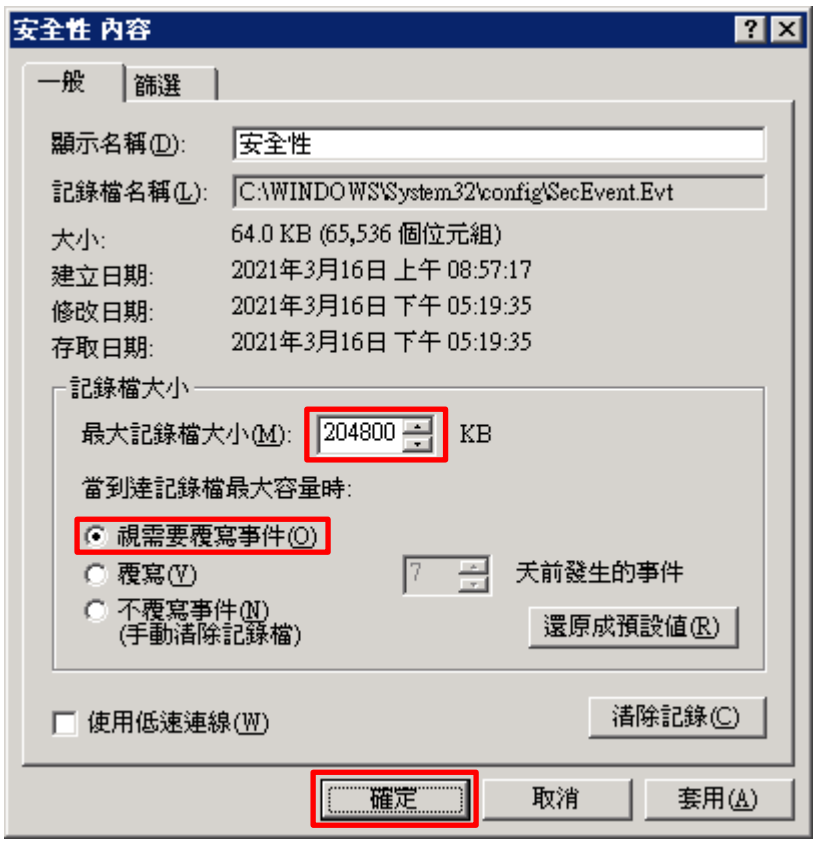
(3) 編輯安全性記錄

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]



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

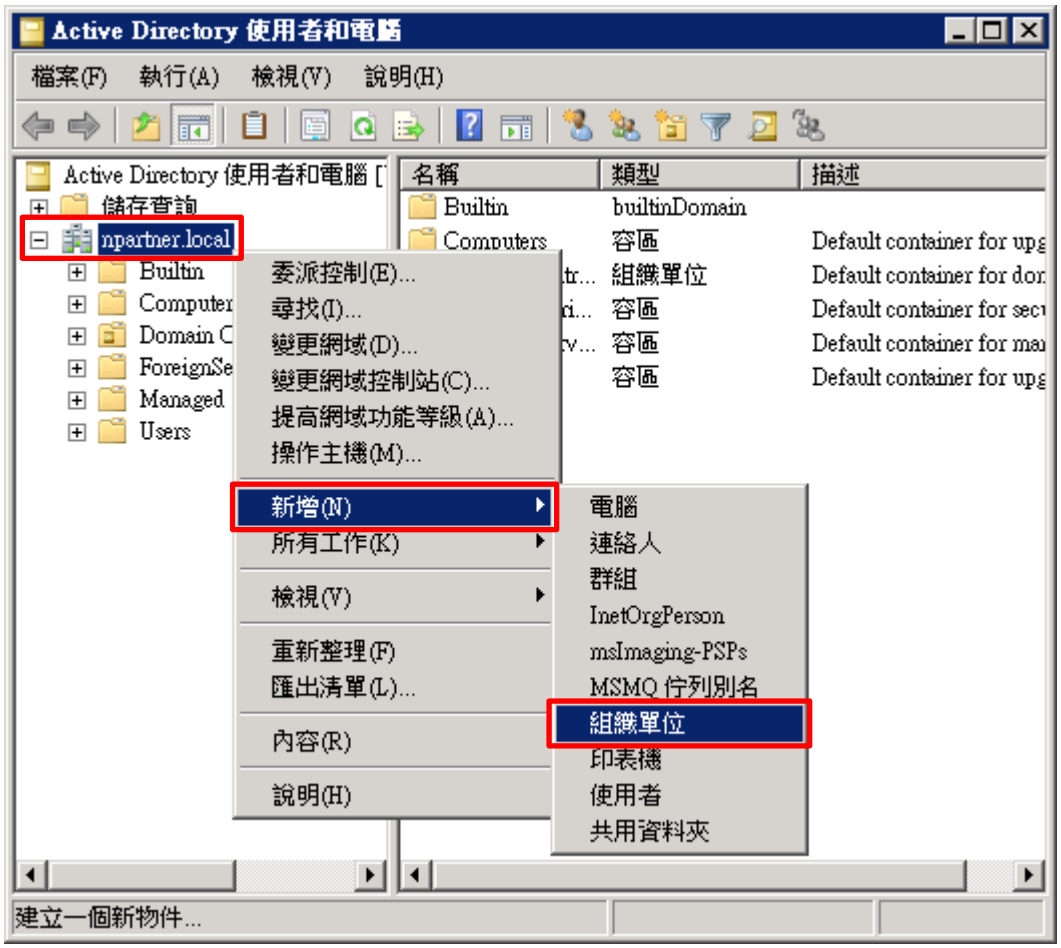
4.1.1 組織單位設定

(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]



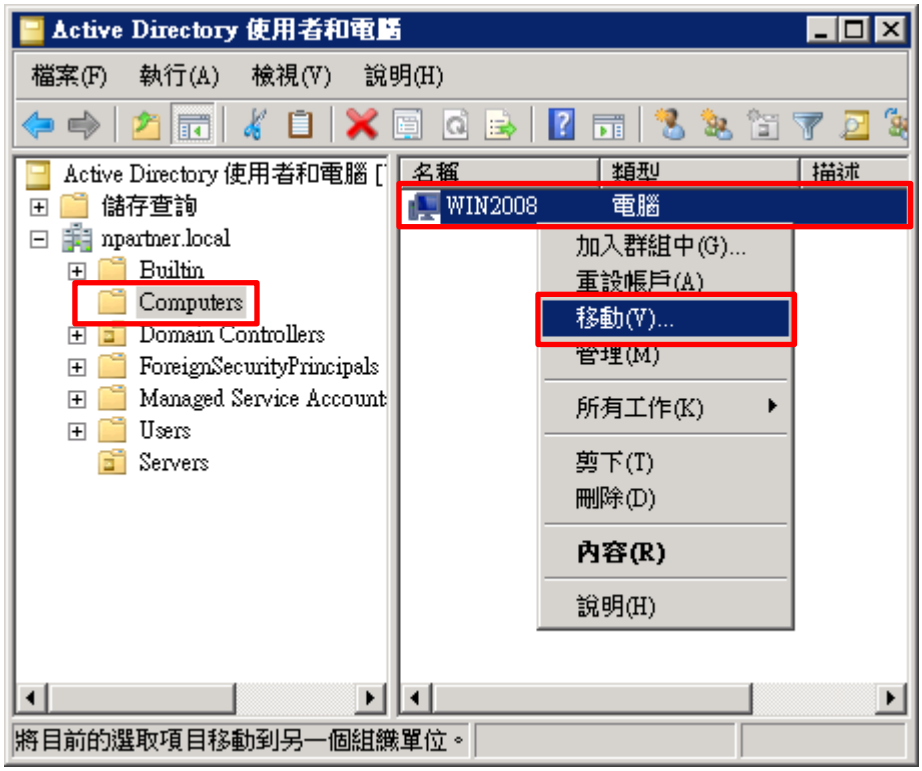
(3) 輸入組織單位名稱

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

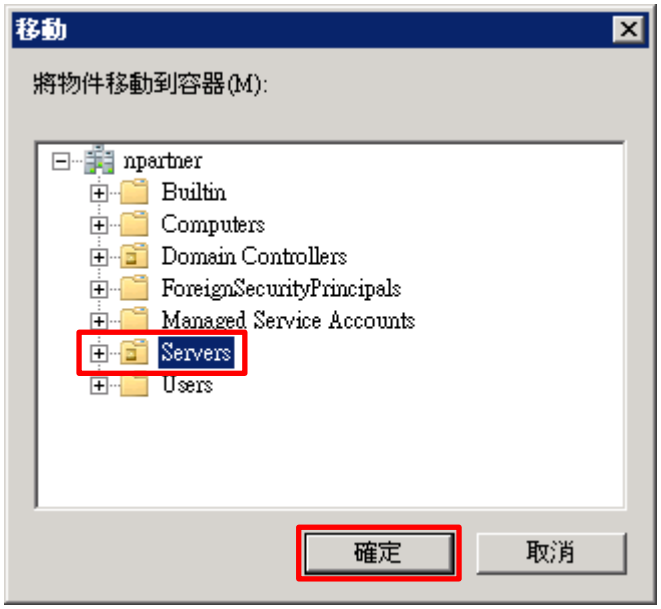
選擇 [Computers] 組織單位 -> 在 [Win2008] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



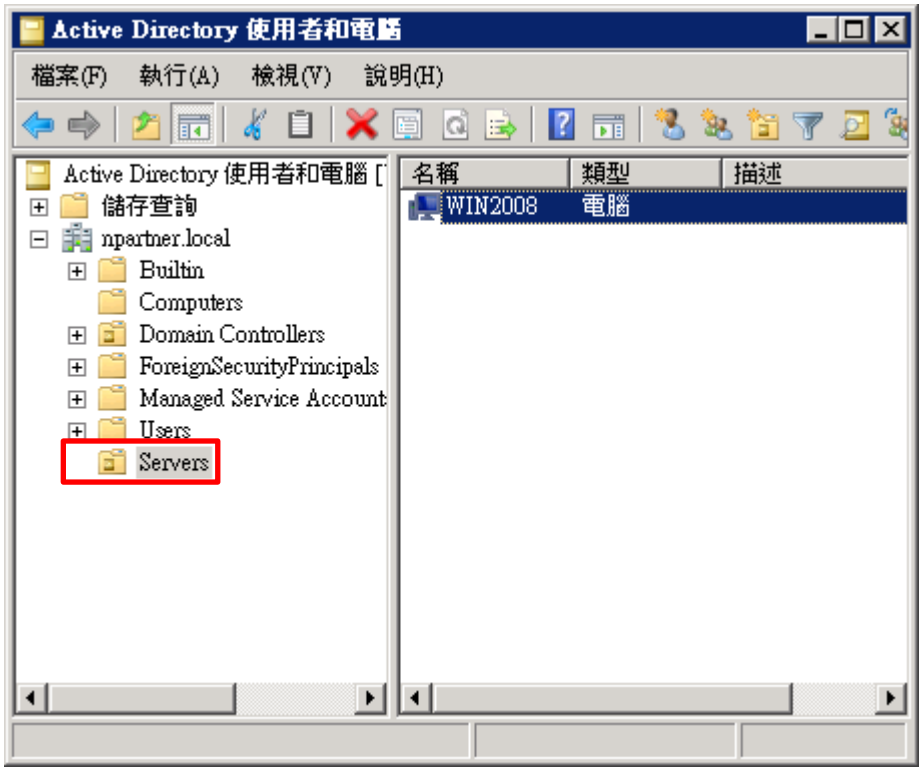
(5) 選擇組織單位

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 伺服器已移動。



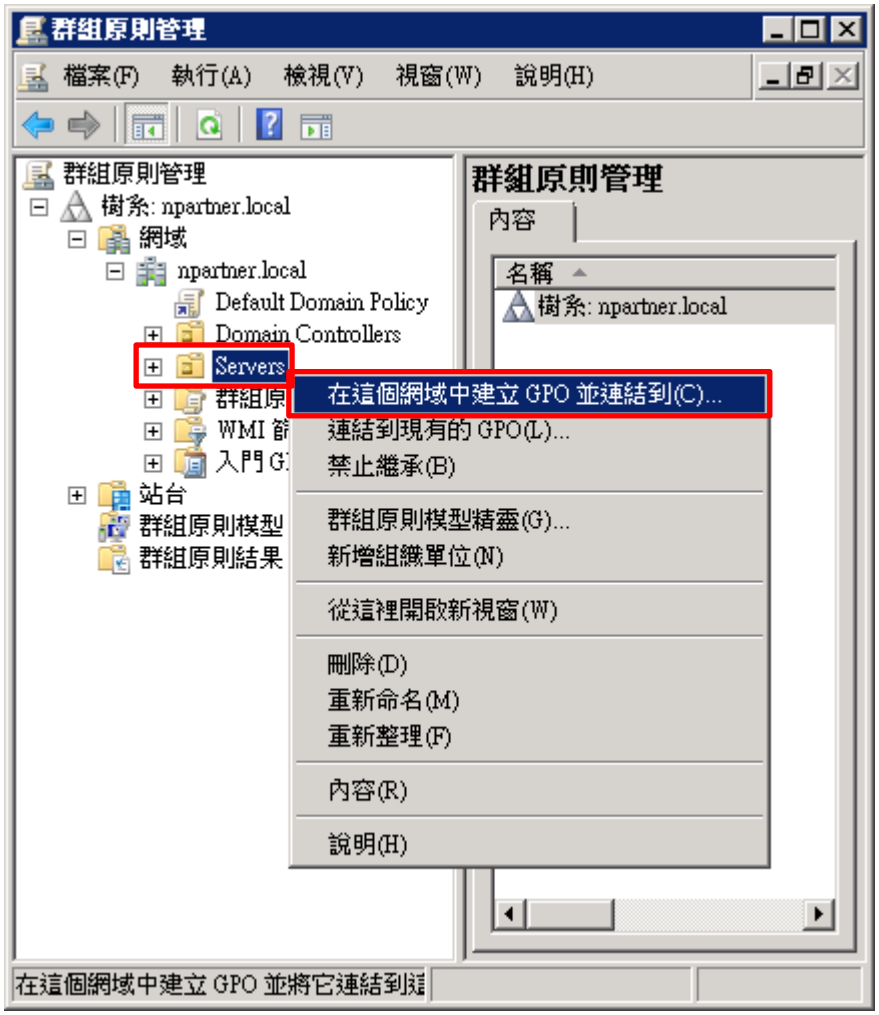
4.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

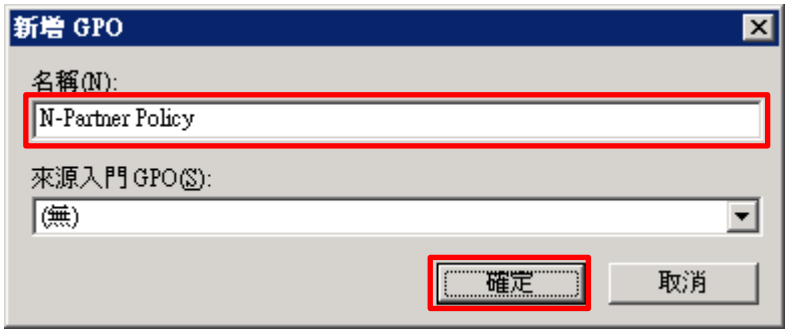
(2) 在 Servers 組織單位，新增群組原則物件

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...]



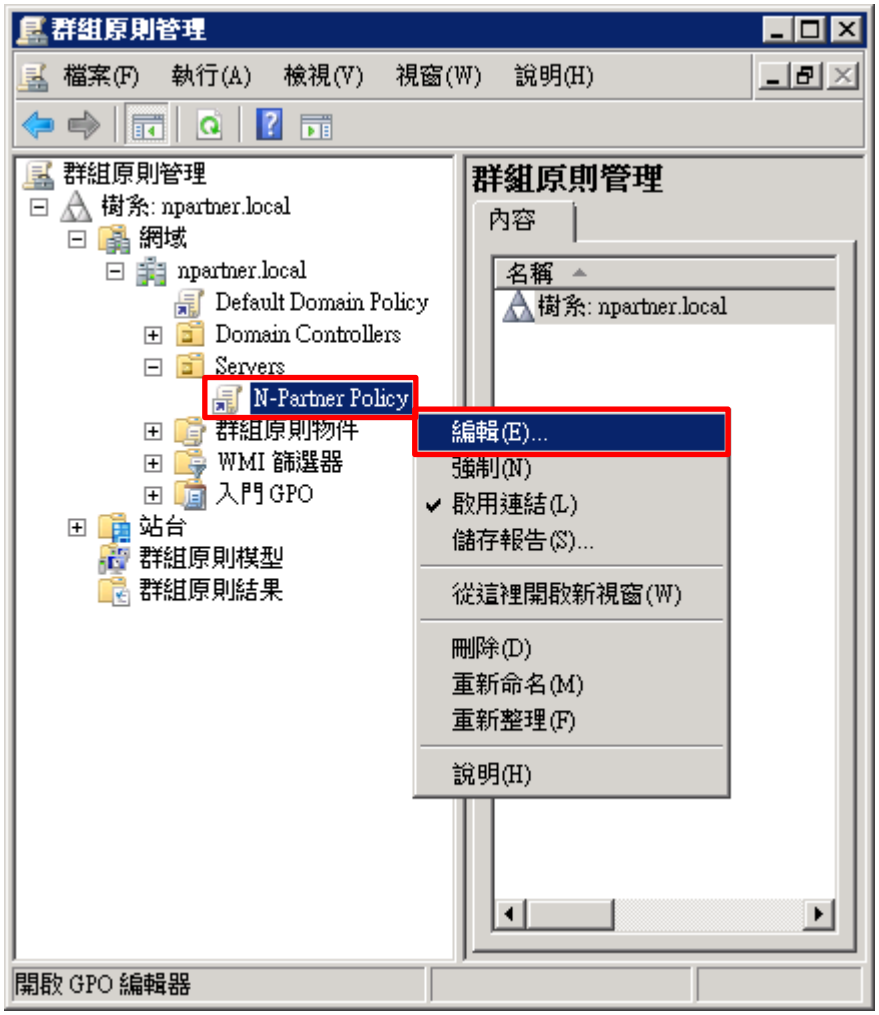
(3) 輸入群組原則物件名稱

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]



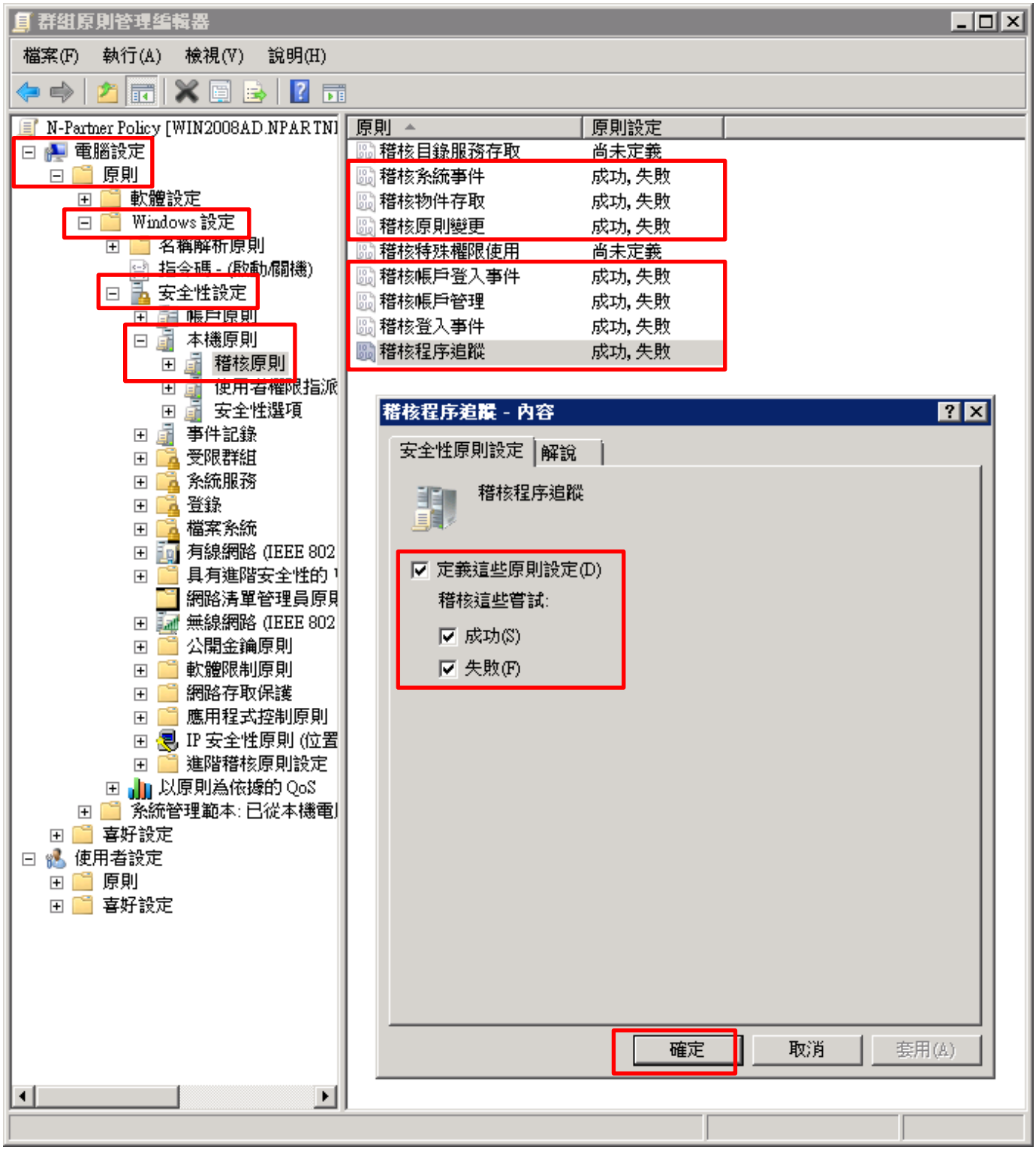
(4) 編輯群組原則物件

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



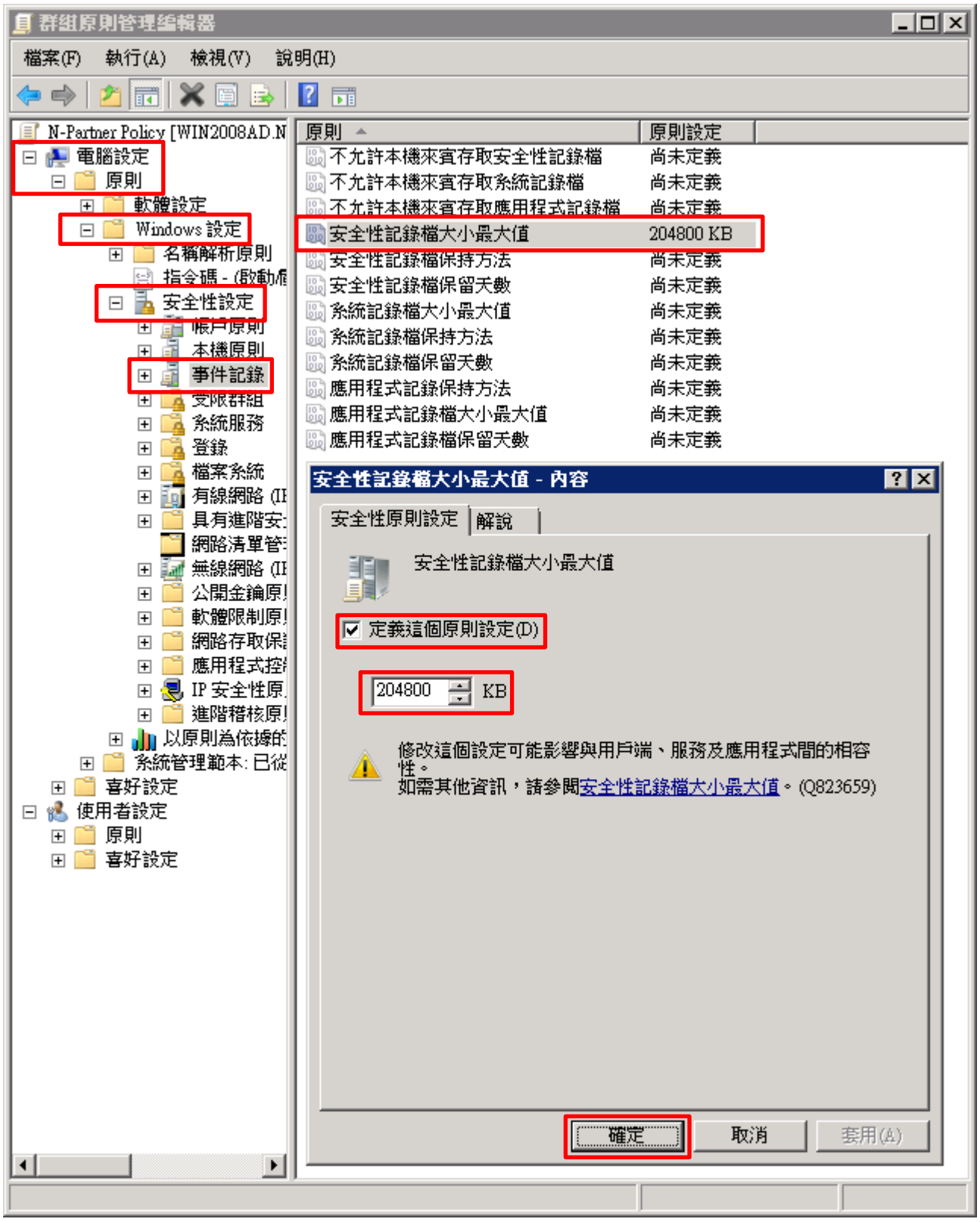
(5) 本機原則：稽核原則

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



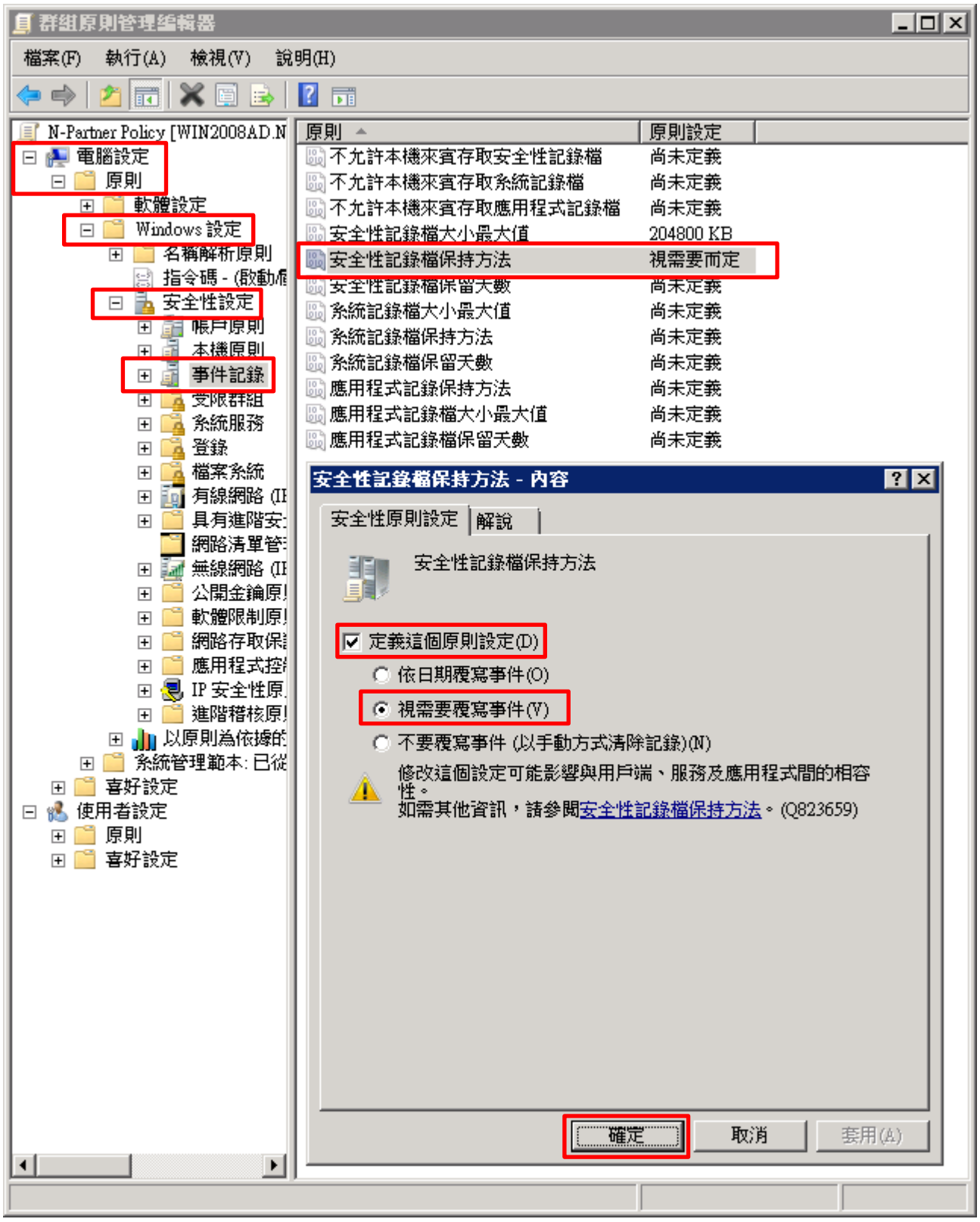
(6) 事件記錄：安全性記錄檔大小最大值

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] 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：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] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



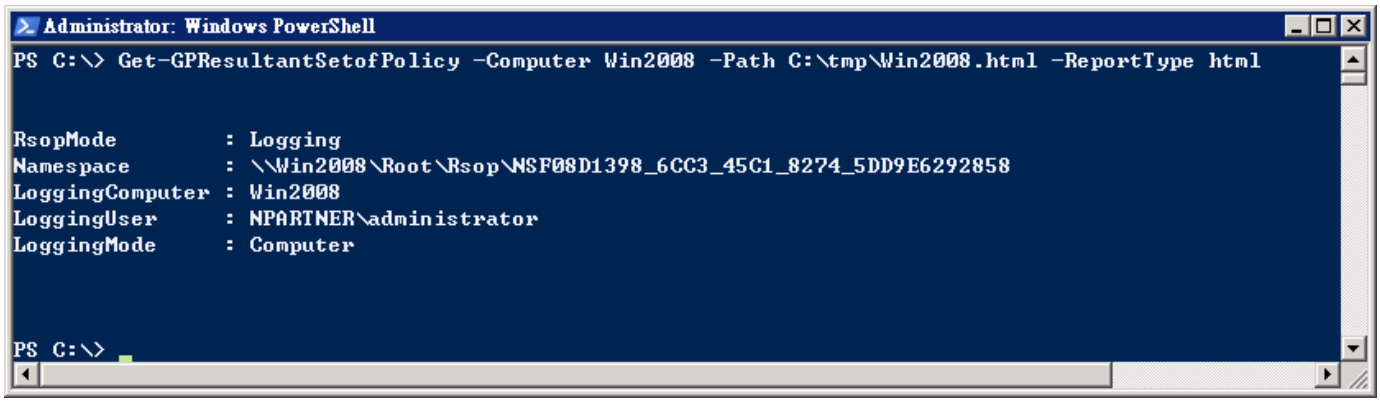
(8) 在 Windows Server 伺服器 -> 開啟 [Windows PowerShell]

(9) 更新群組原則

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

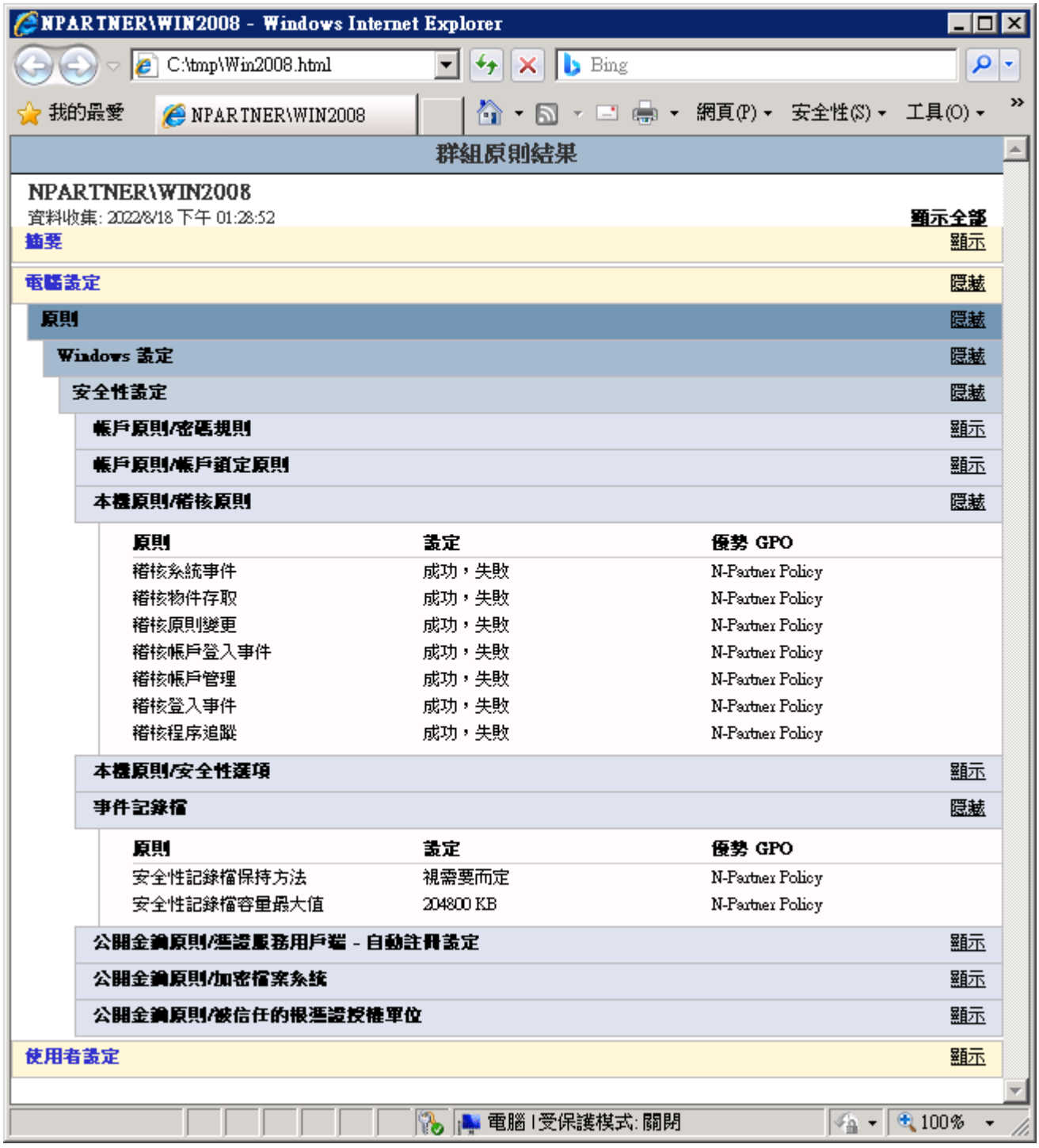
(10) 在 AD 網域伺服器 -> 產生 Windows Server 伺服器群組原則報表

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



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

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

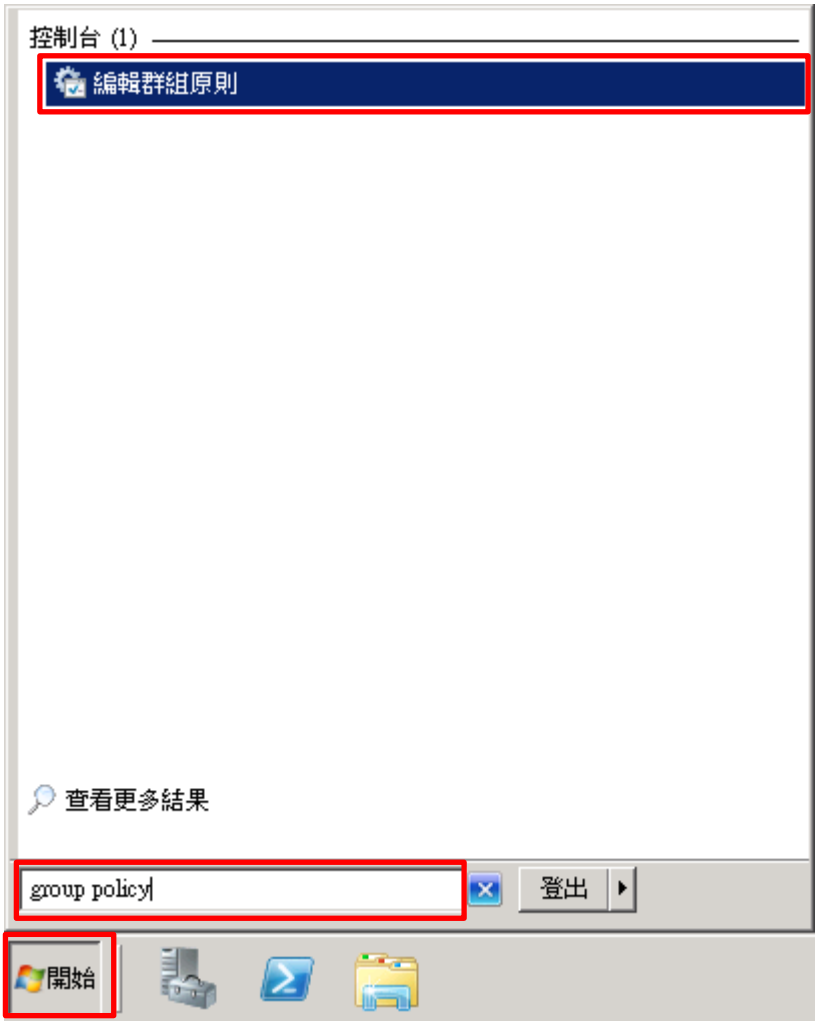


4.2 工作群組

4.2.1 稽核原則設定

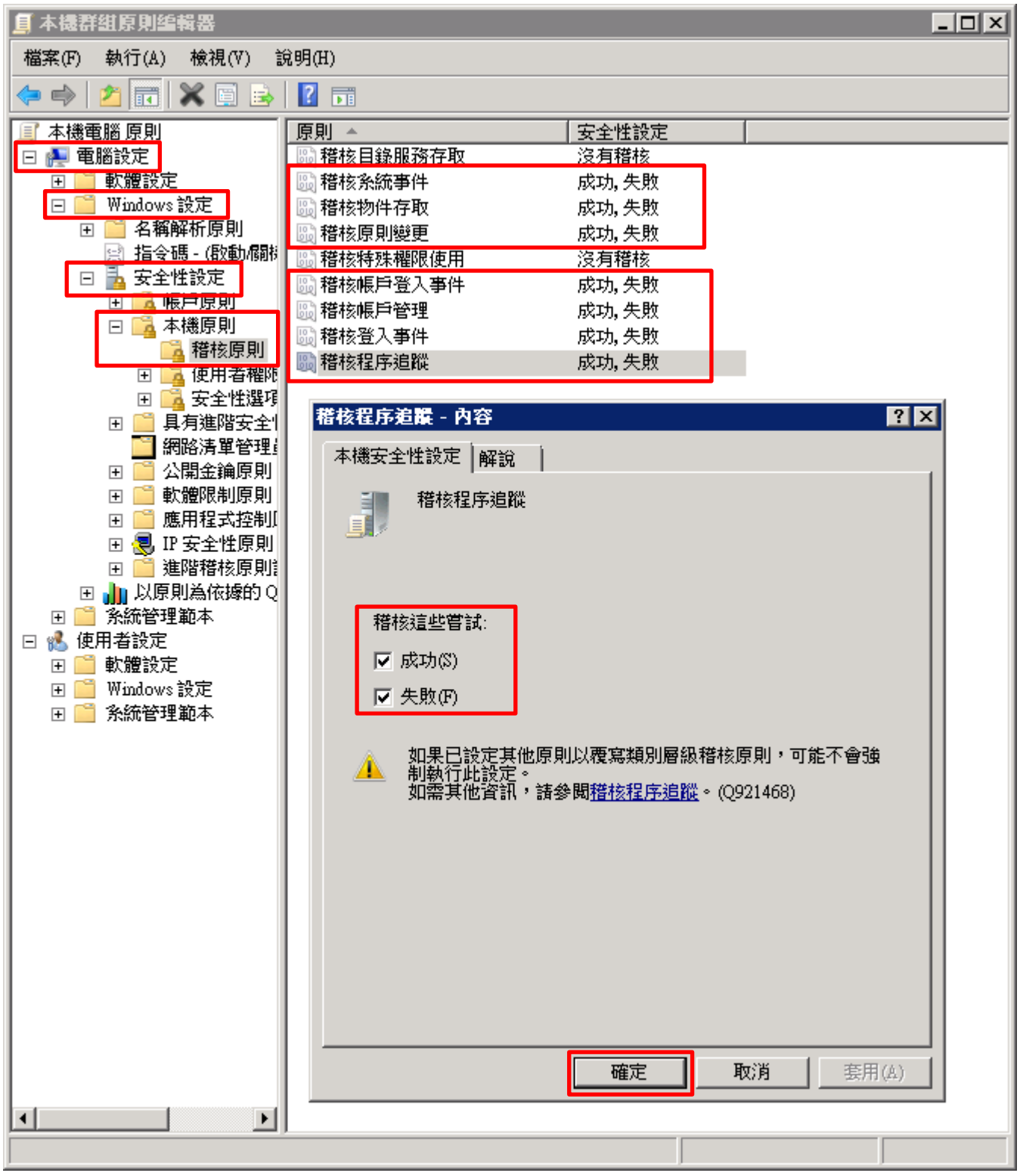
(1) 開啟 [本機群組原則編輯器]

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



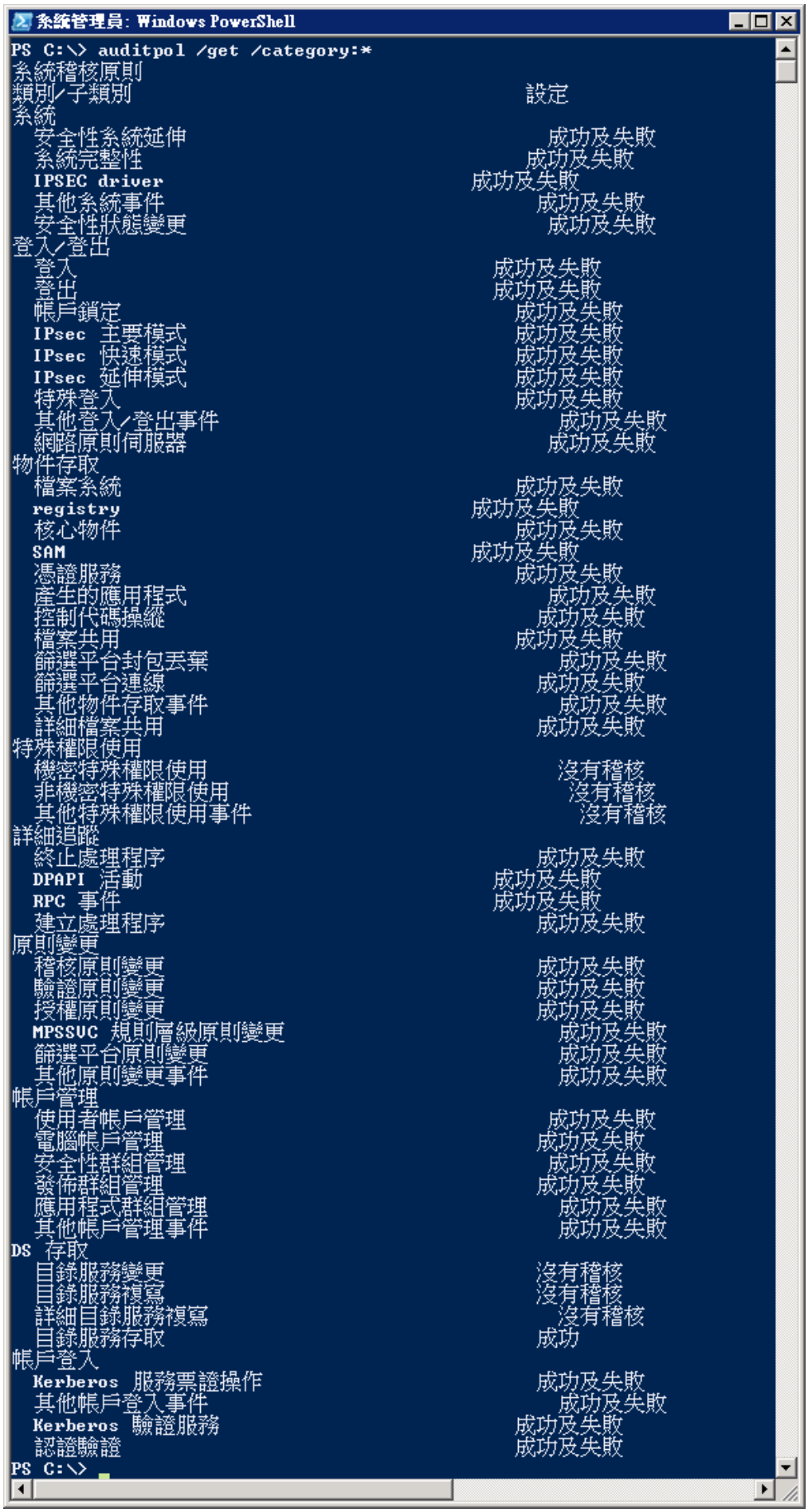
(3) 開啟 [Windows PowerShell]

(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:*
```

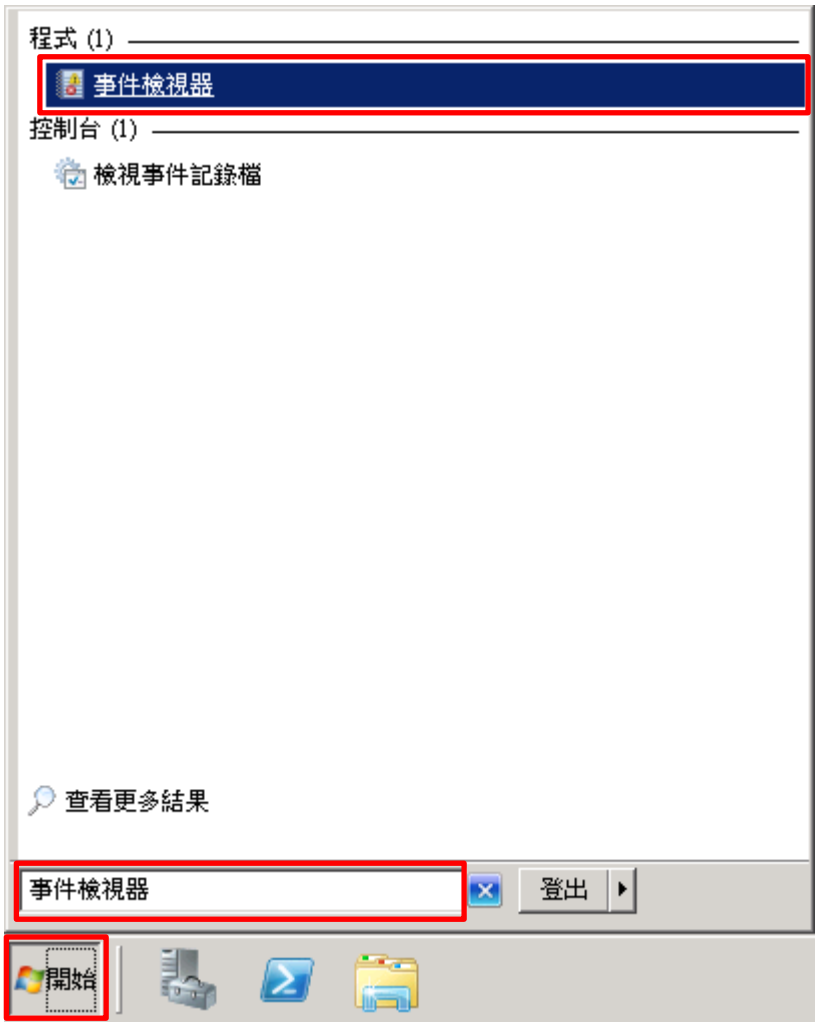


```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
系統稽核原則
類別/子類別                                    設定
系統
  安全性系統延伸                                成功及失敗
  系統完整性                                    成功及失敗
  IPSEC driver                                  成功及失敗
  其他系統事件                                  成功及失敗
  安全性狀態變更                                成功及失敗
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                                  成功及失敗
  DPAPI 活動                                    成功及失敗
  RPC 事件                                      成功及失敗
  建立處理程序                                  成功及失敗
原則變更
  稽核原則變更                                  成功及失敗
  驗證原則變更                                  成功及失敗
  授權原則變更                                  成功及失敗
  MPSSVC 規則層級原則變更                       成功及失敗
  篩選平台原則變更                              成功及失敗
  其他原則變更事件                              成功及失敗
帳戶管理
  使用者帳戶管理                                成功及失敗
  電腦帳戶管理                                  成功及失敗
  安全性群組管理                                成功及失敗
  發佈群組管理                                  成功及失敗
  應用程式群組管理                              成功及失敗
  其他帳戶管理事件                              成功及失敗
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:\>
```

4.2.2 事件檔案設定

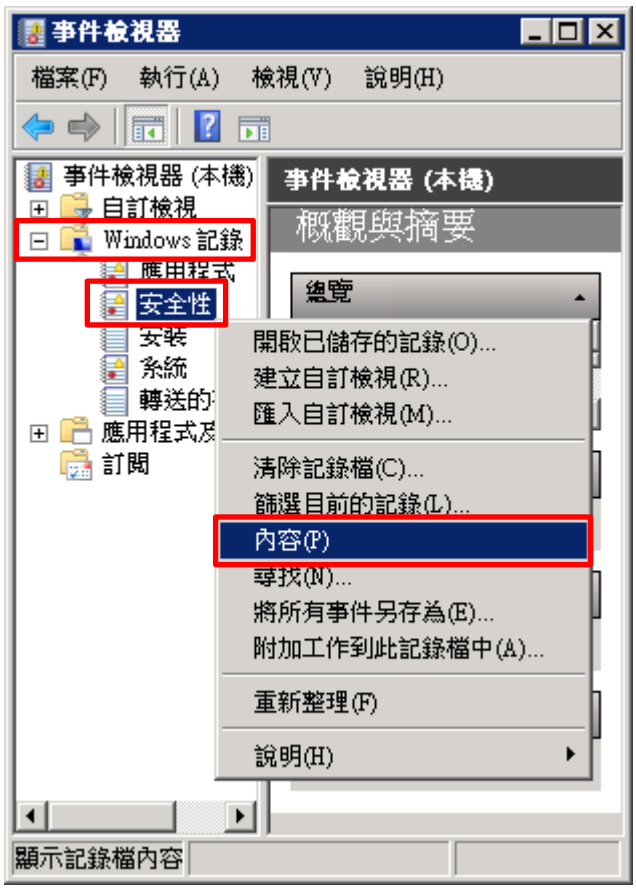
(1) 開啟 [事件檢視器]

點選 [開始] -> 在 [搜尋] 欄位，輸入事件檢視器 -> 點選 [事件檢視器]



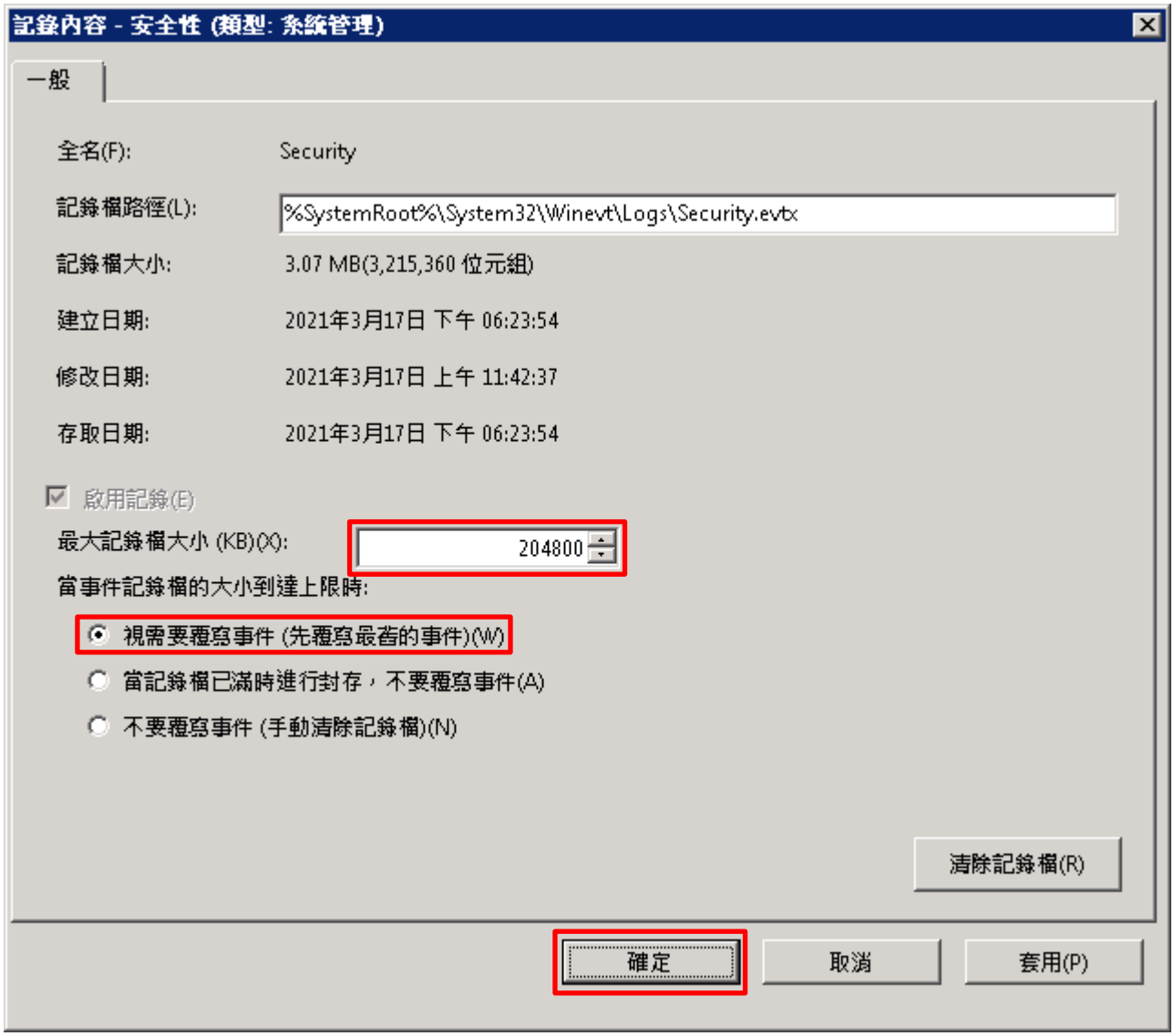
(2) 編輯安全性記錄

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]



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

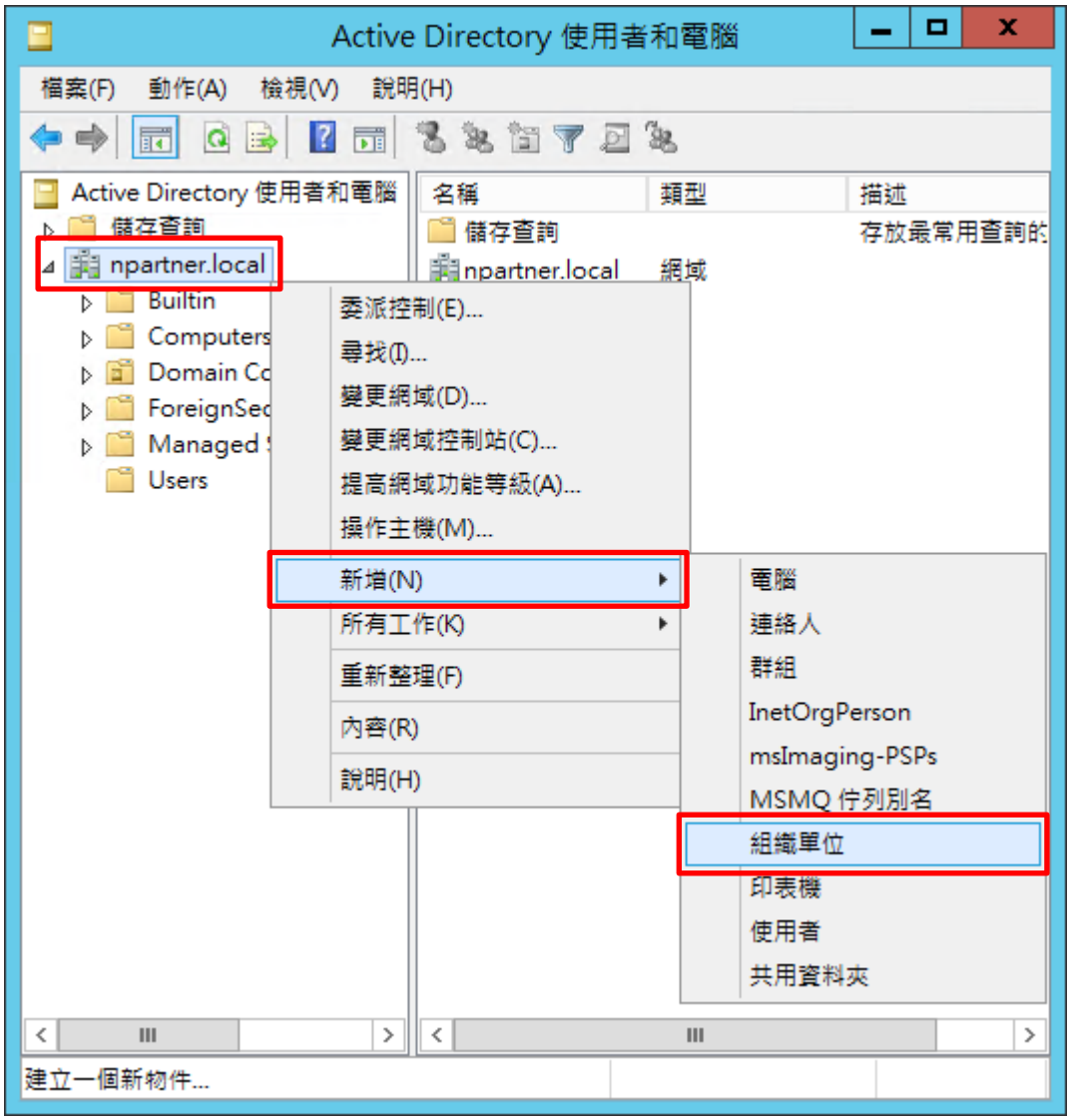
5.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

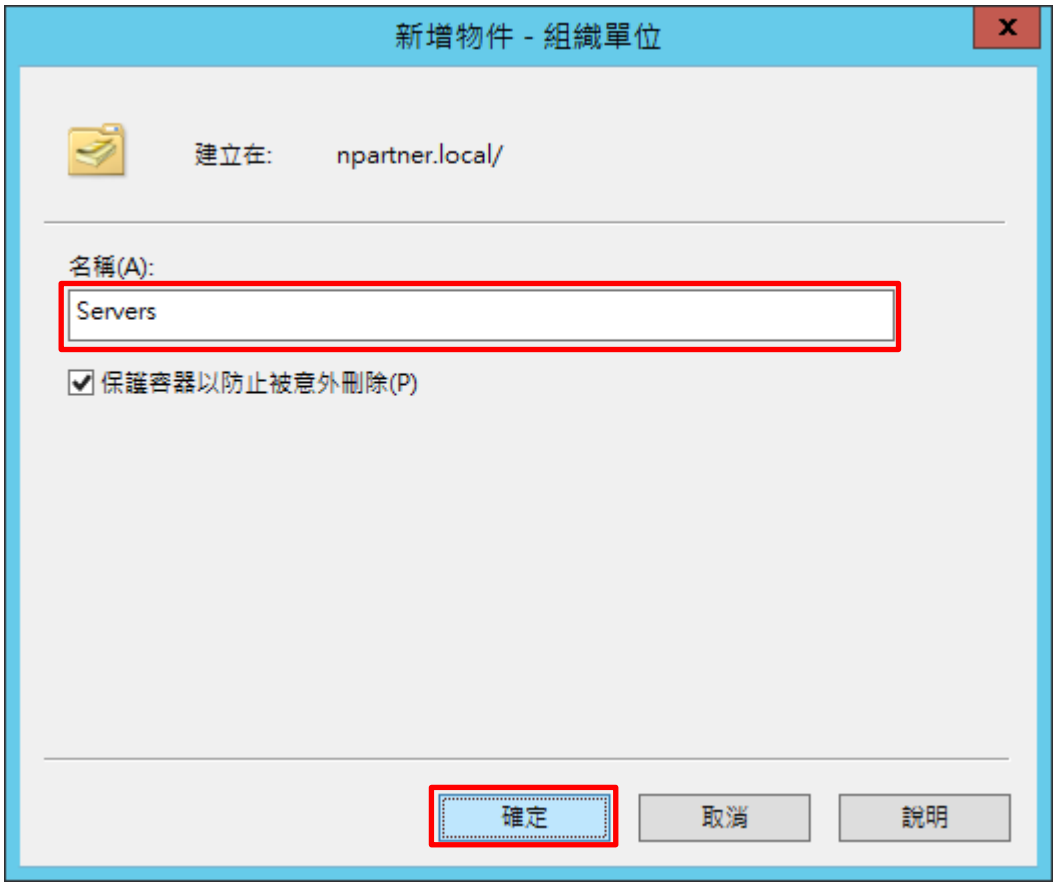
(2) 新增組織單位

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

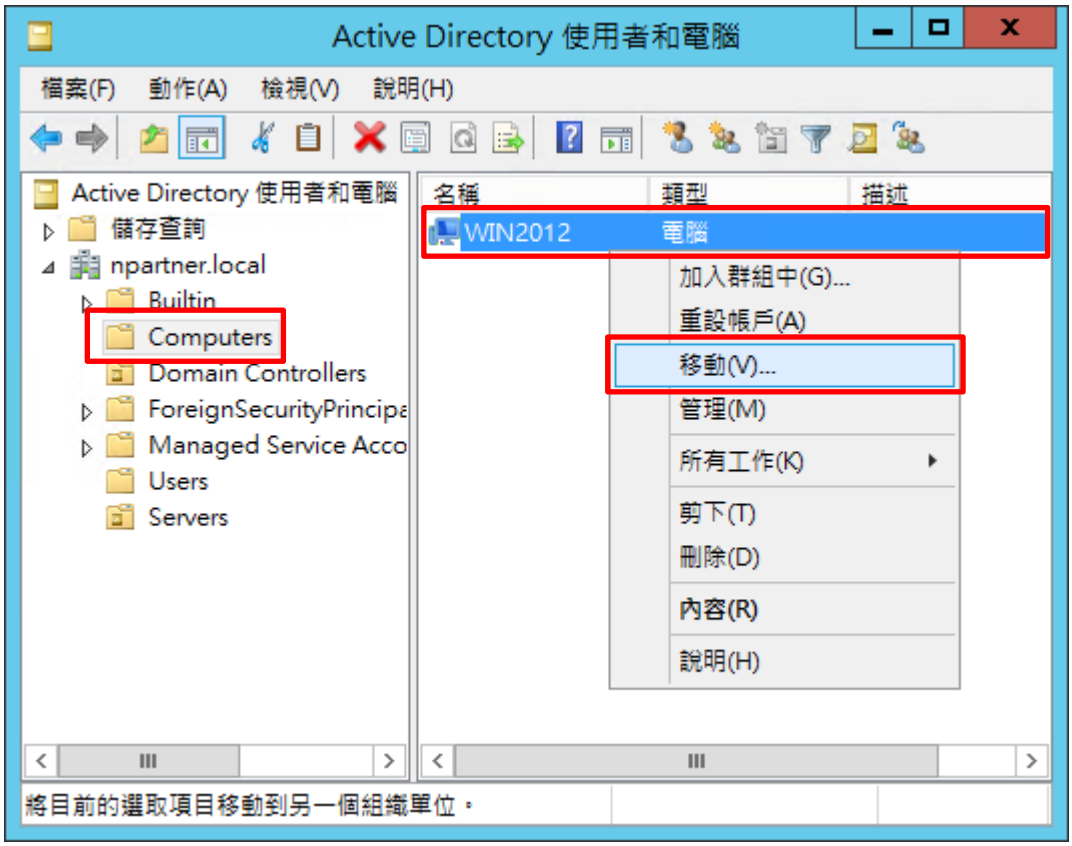
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

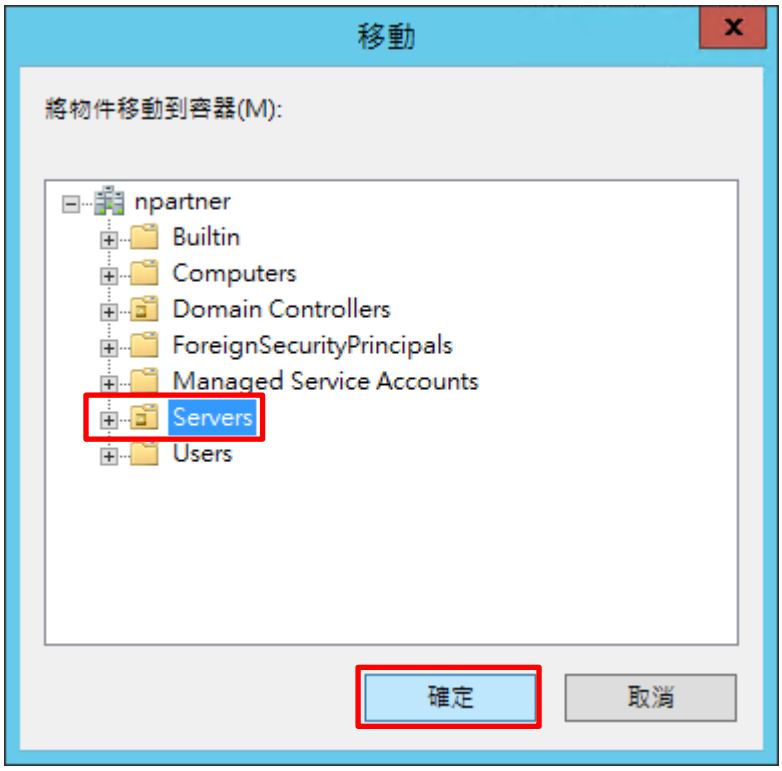
選擇 [Computers] 組織單位 -> 在 [Win2012] 伺服器，按滑鼠右鍵 註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



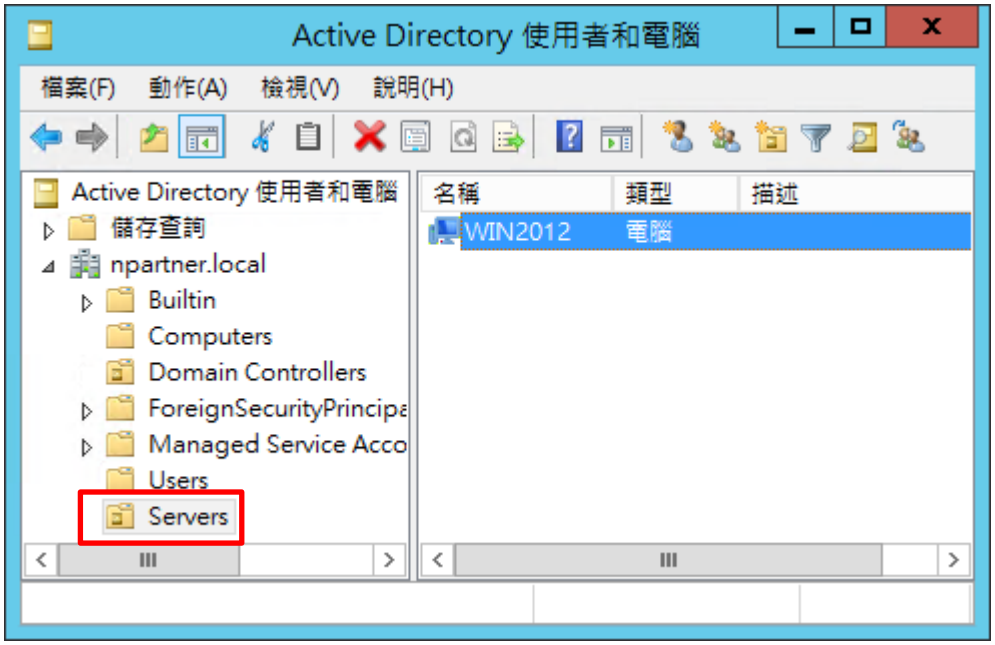
(5) 選擇組織單位

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

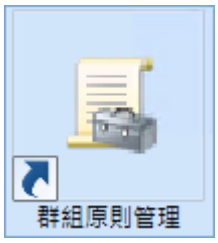
點選 [Servers] 組織單位，確認 Win2012 伺服器已移動。



5.1.2 群組原則設定

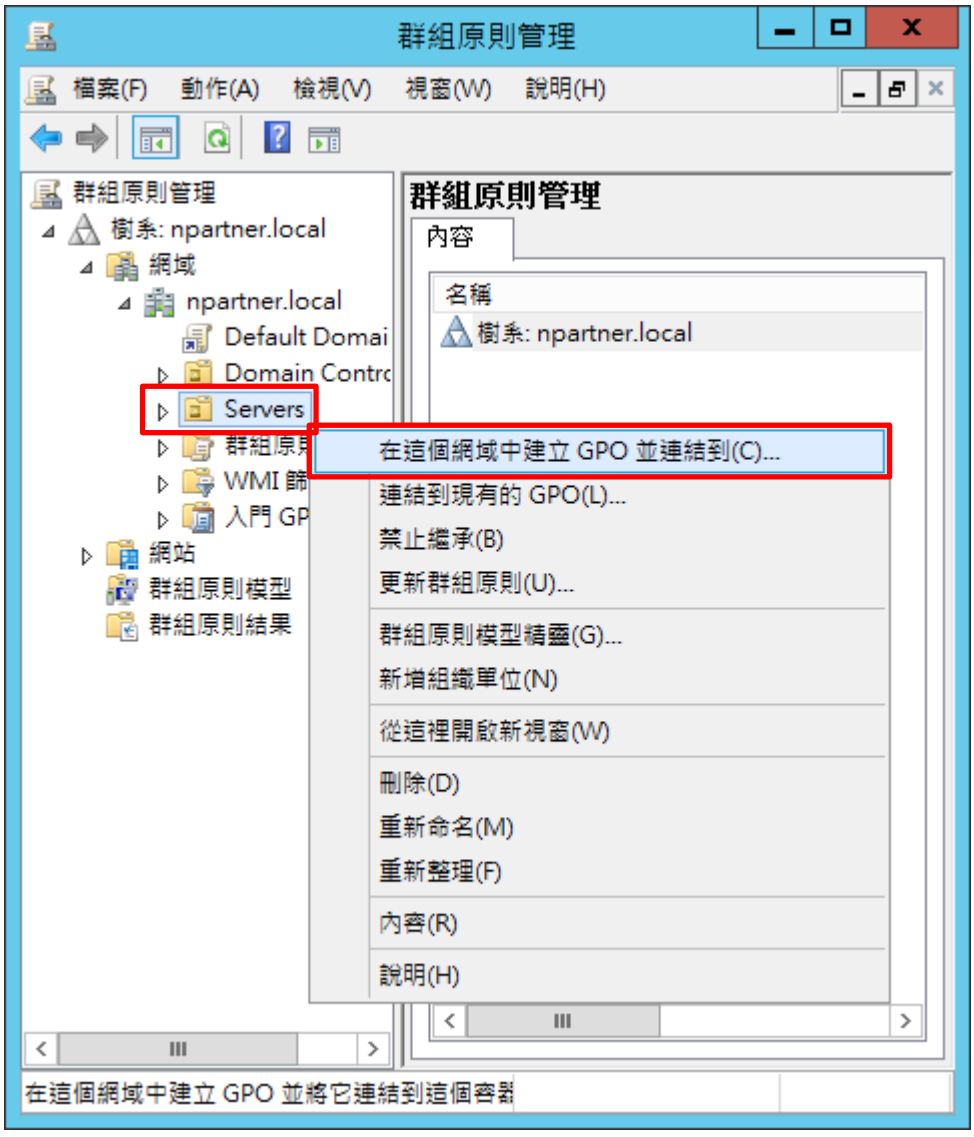
(1) 開啟群組原則管理

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...]

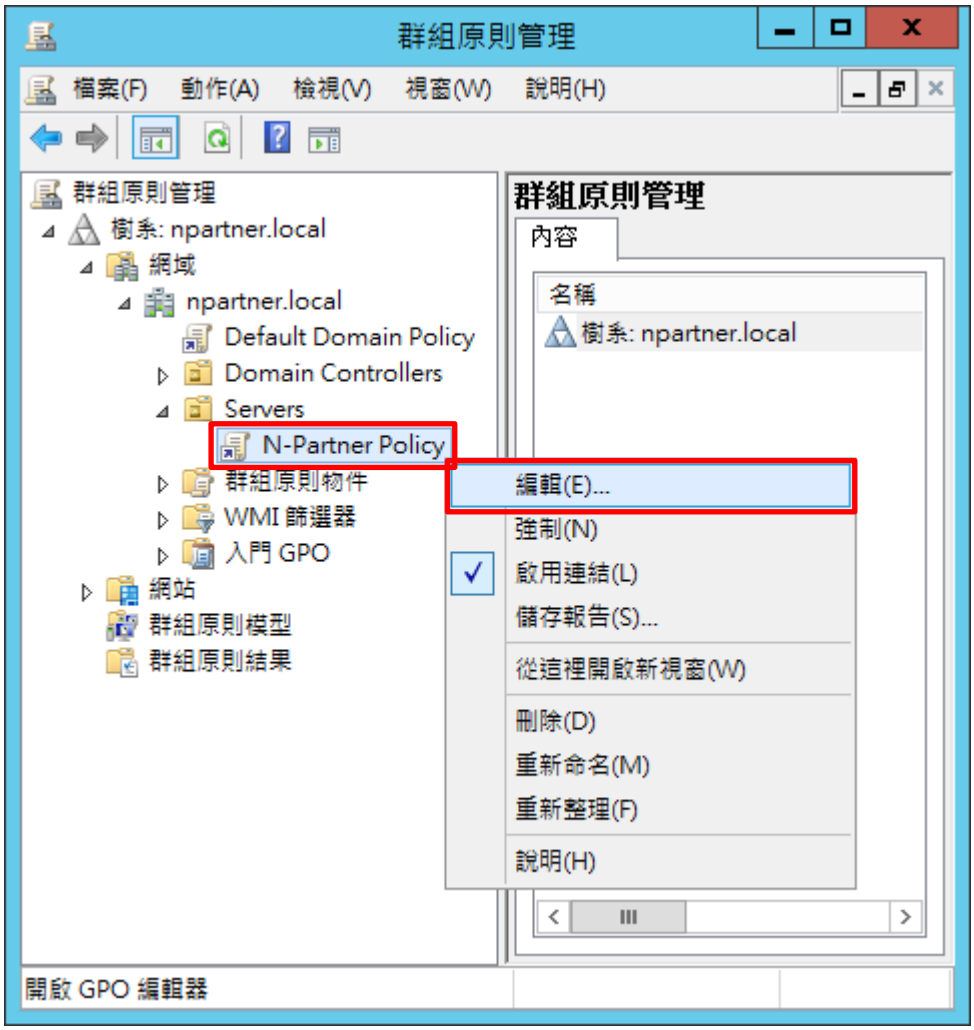


(3) 輸入群組原則物件名稱

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]

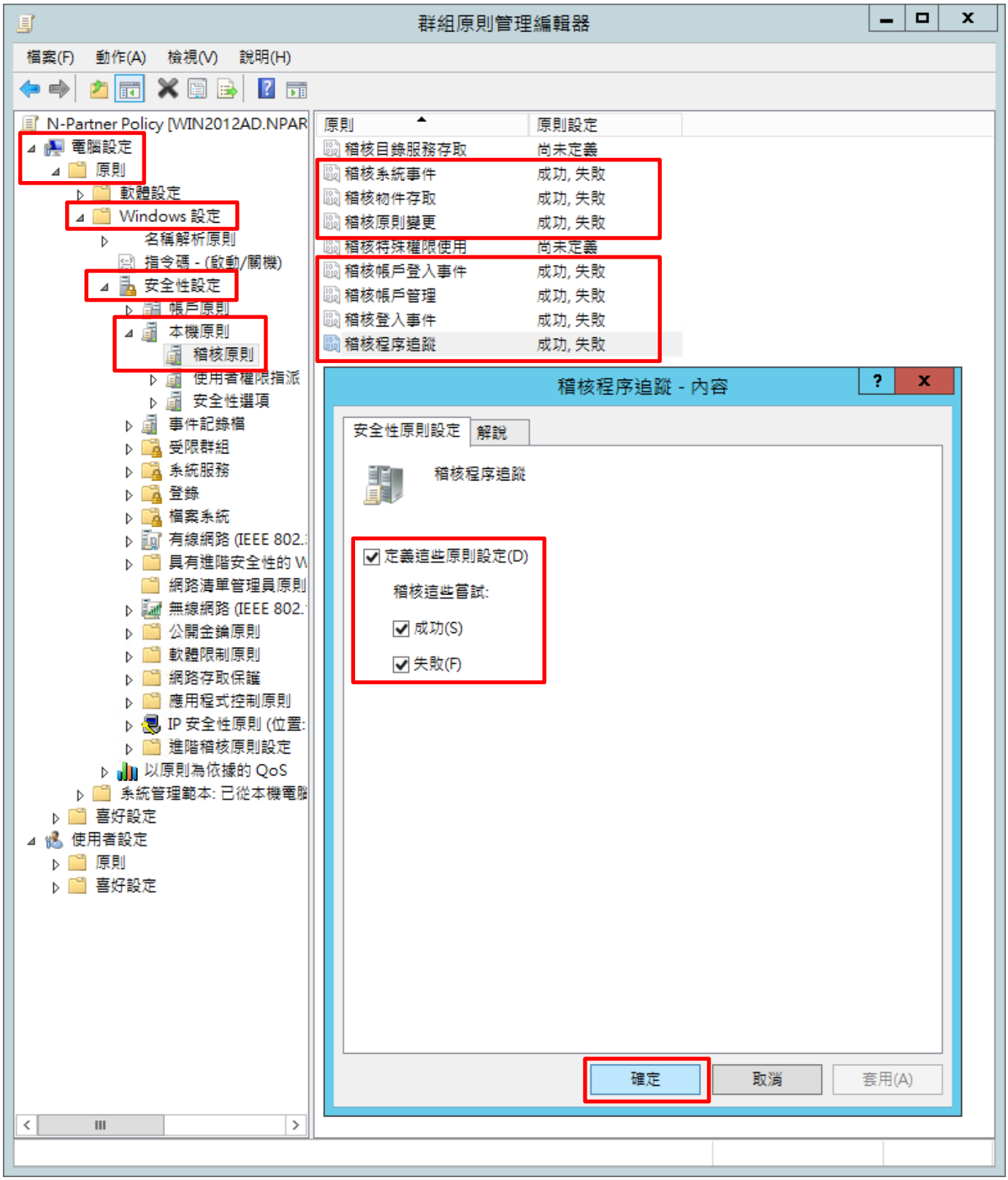
(4) 編輯群組原則物件

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



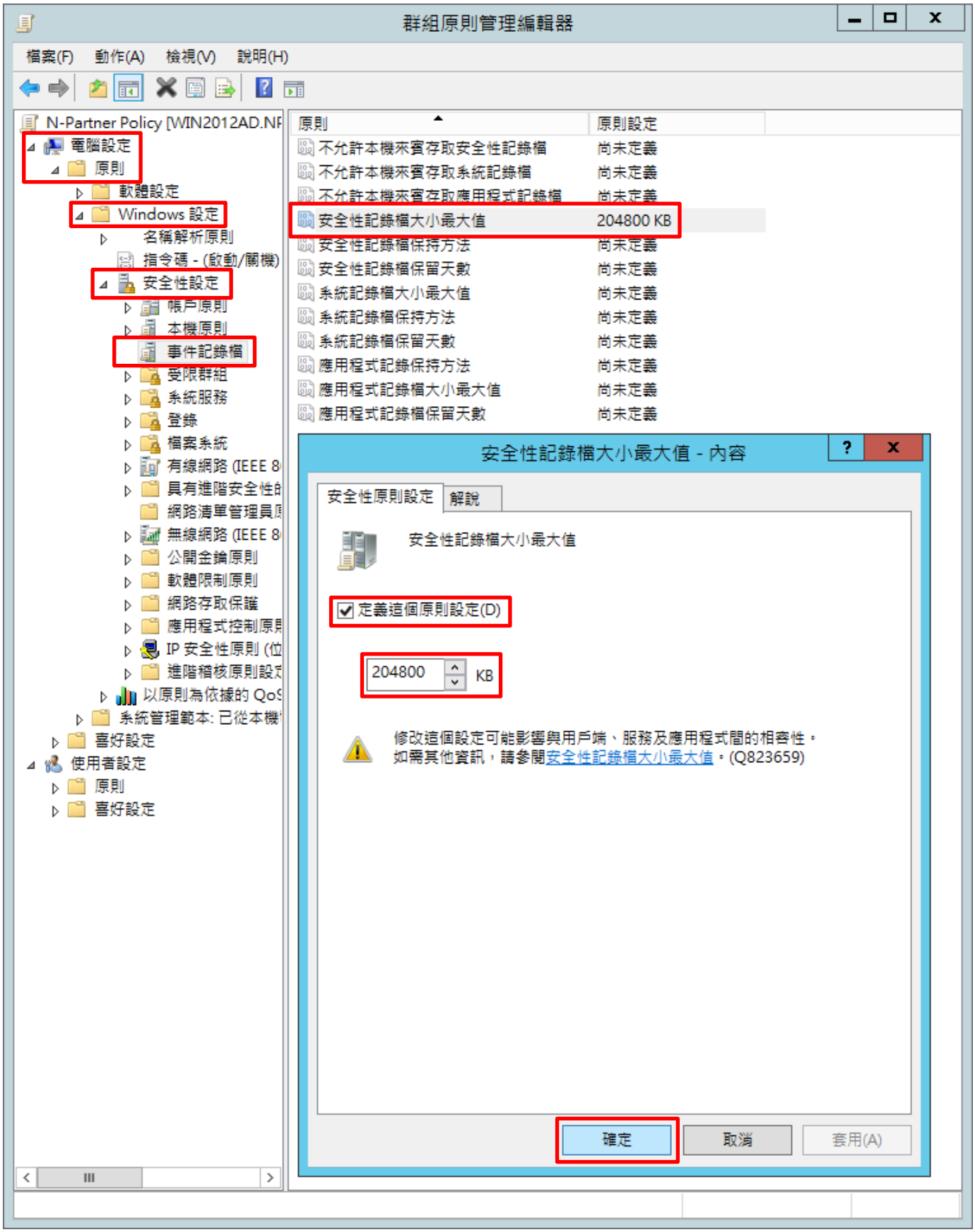
(5) 本機原則：稽核原則

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



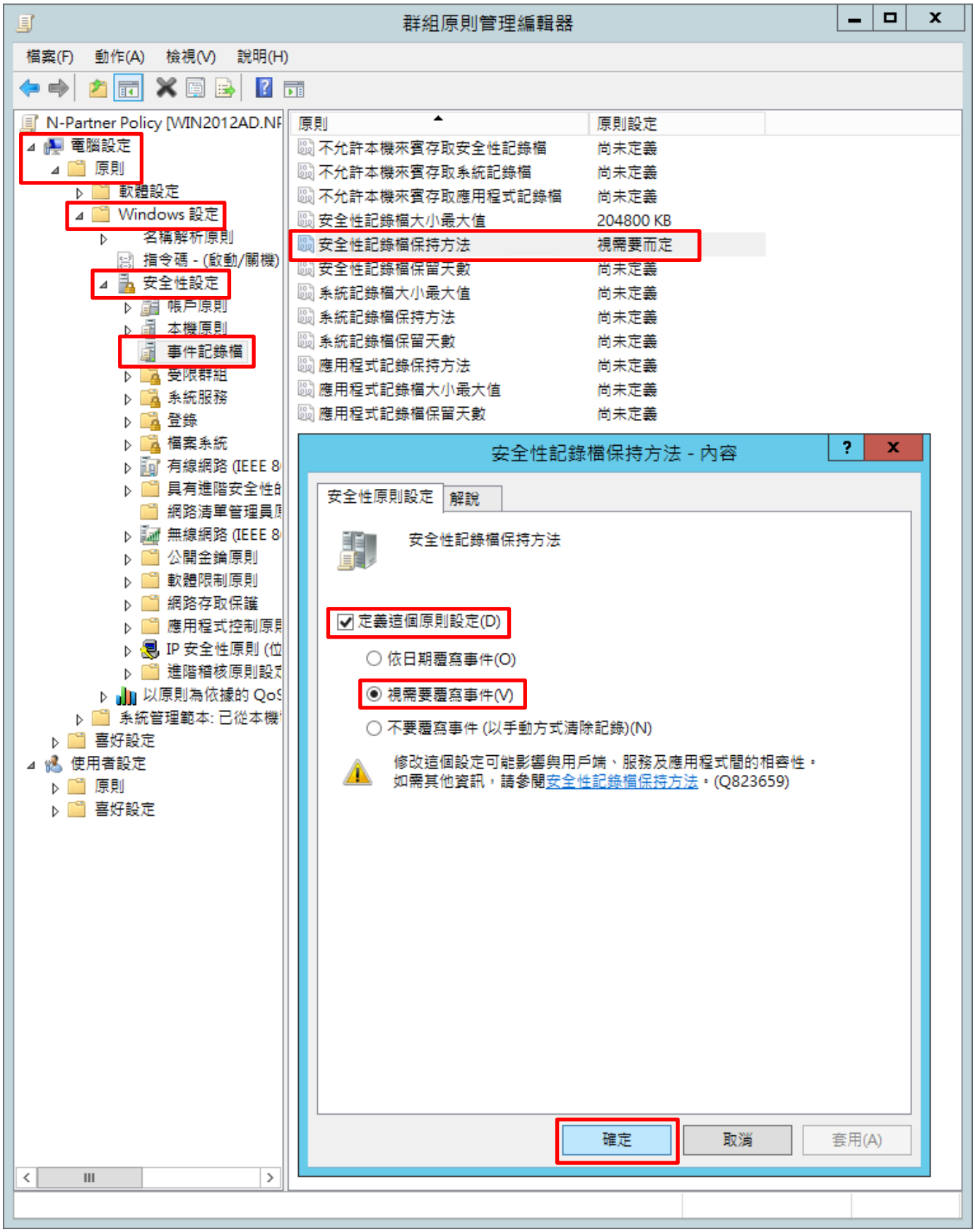
(6) 事件記錄檔：安全性記錄檔大小最大值

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

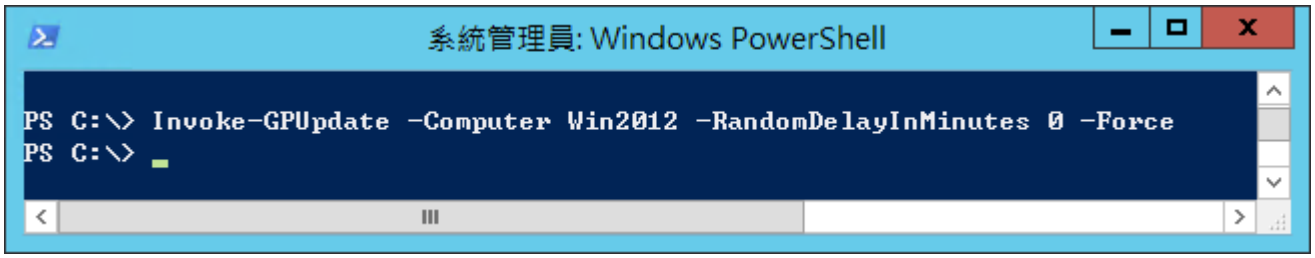
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] -> 勾選 [定義這個原則設定] -> 點選 [視需要覆寫事件] -> 按 [確定]



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

(9) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

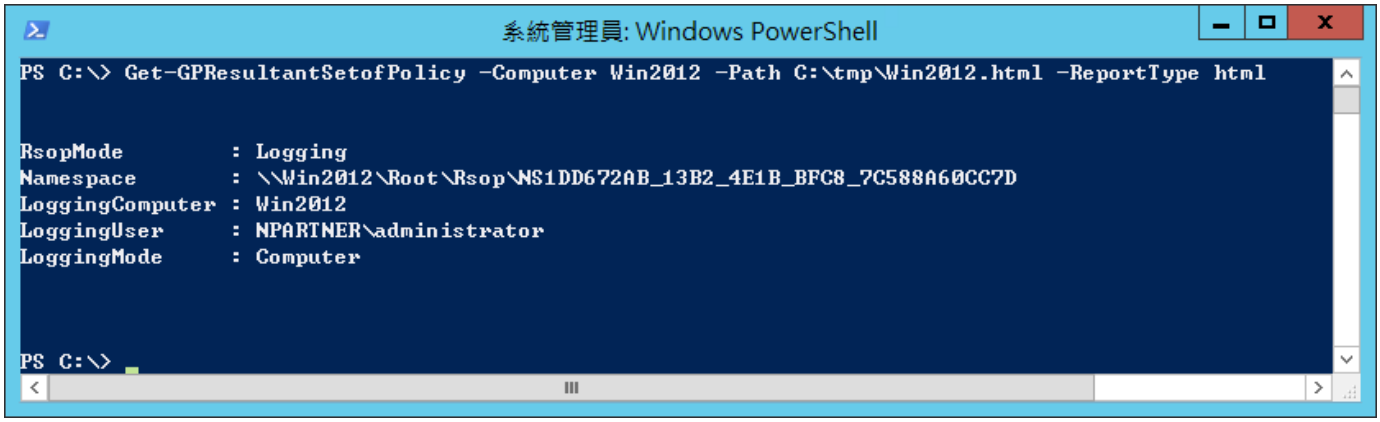
```
PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱

(10) 在 AD 網域伺服器 -> 產生 Windows Server 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 Server 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 -> 確認 Windows Server 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

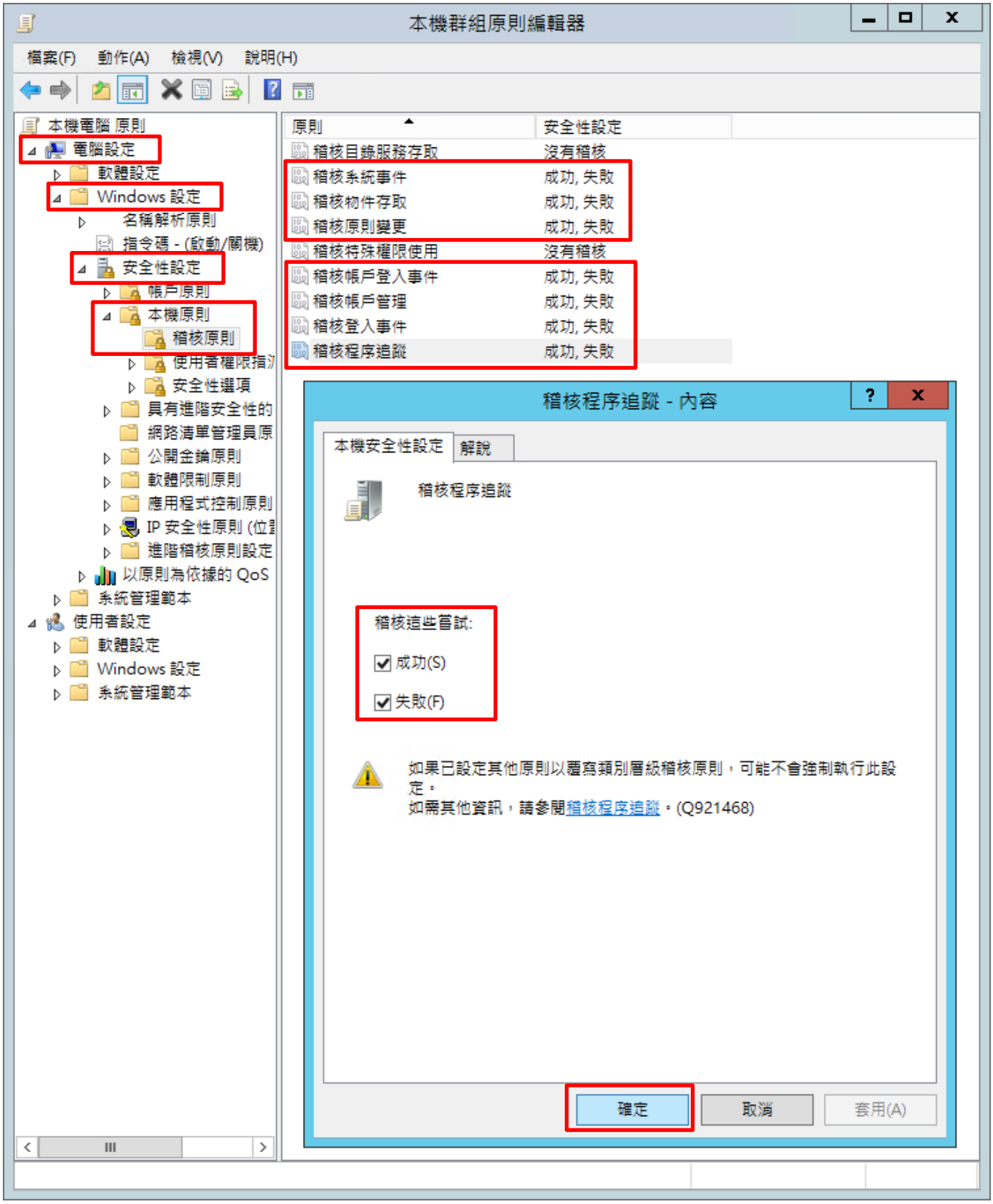
將滑鼠移到右下角點選 [搜尋]

(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

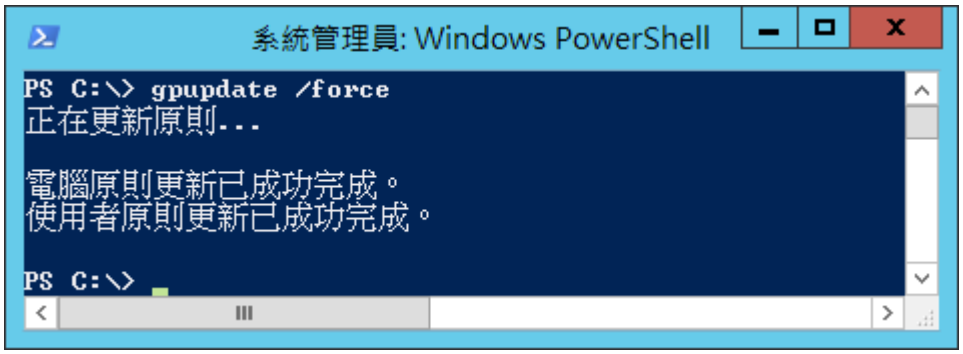
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(4) 開啟 [Windows PowerShell]

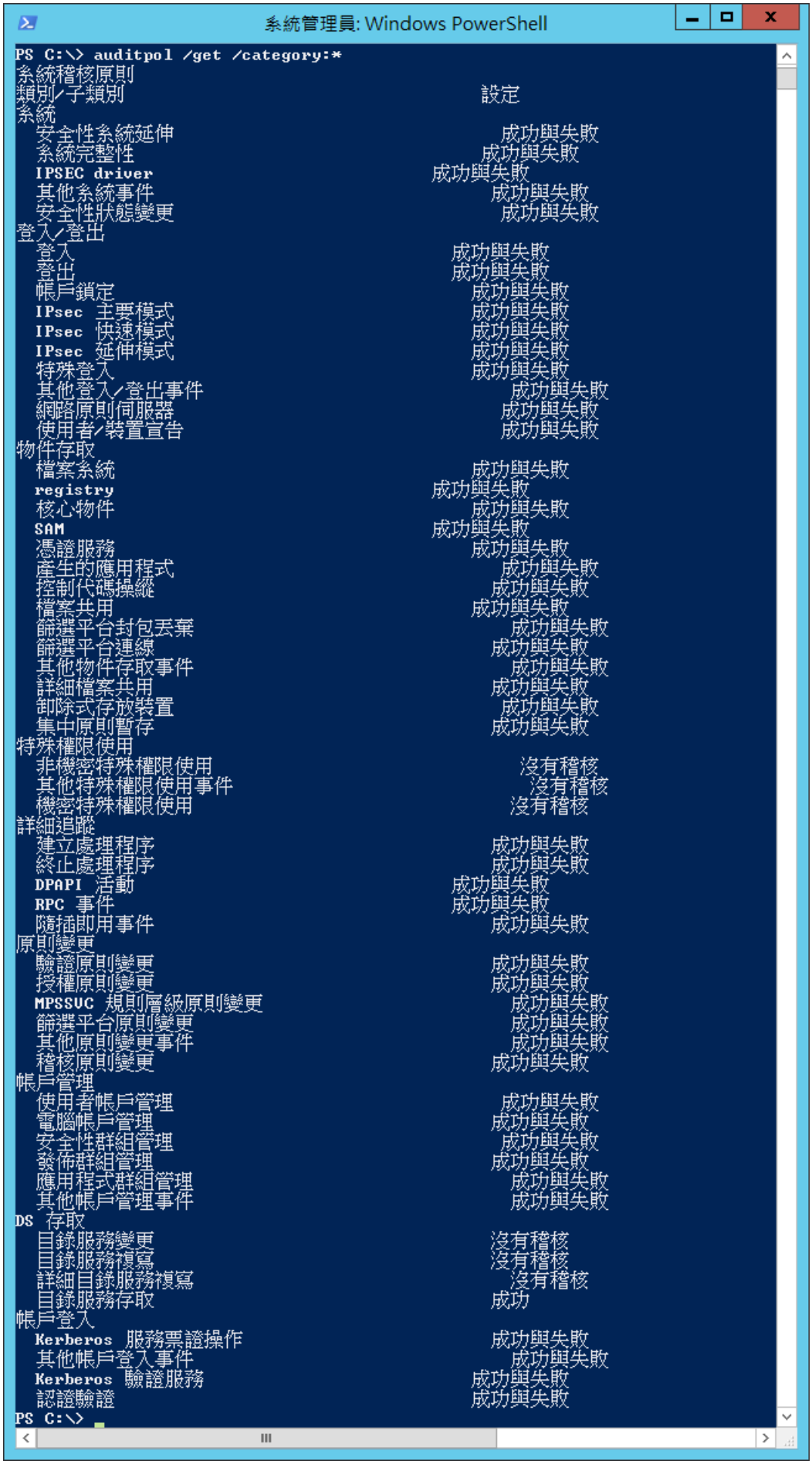
(5) 更新群組原則

```
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

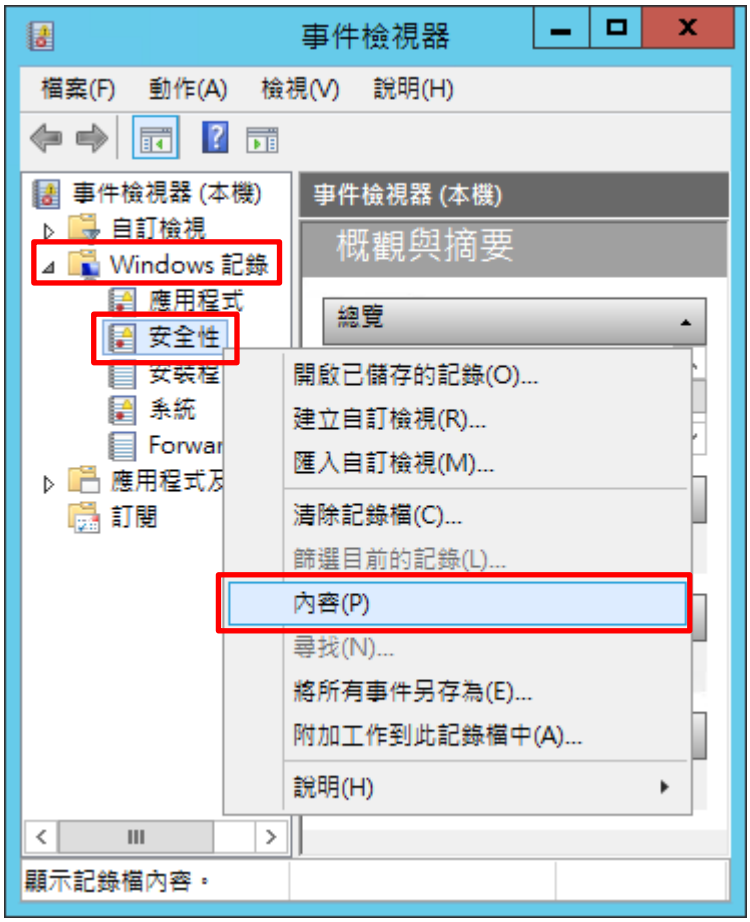
將滑鼠移到右下角點選 [搜尋]

(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]

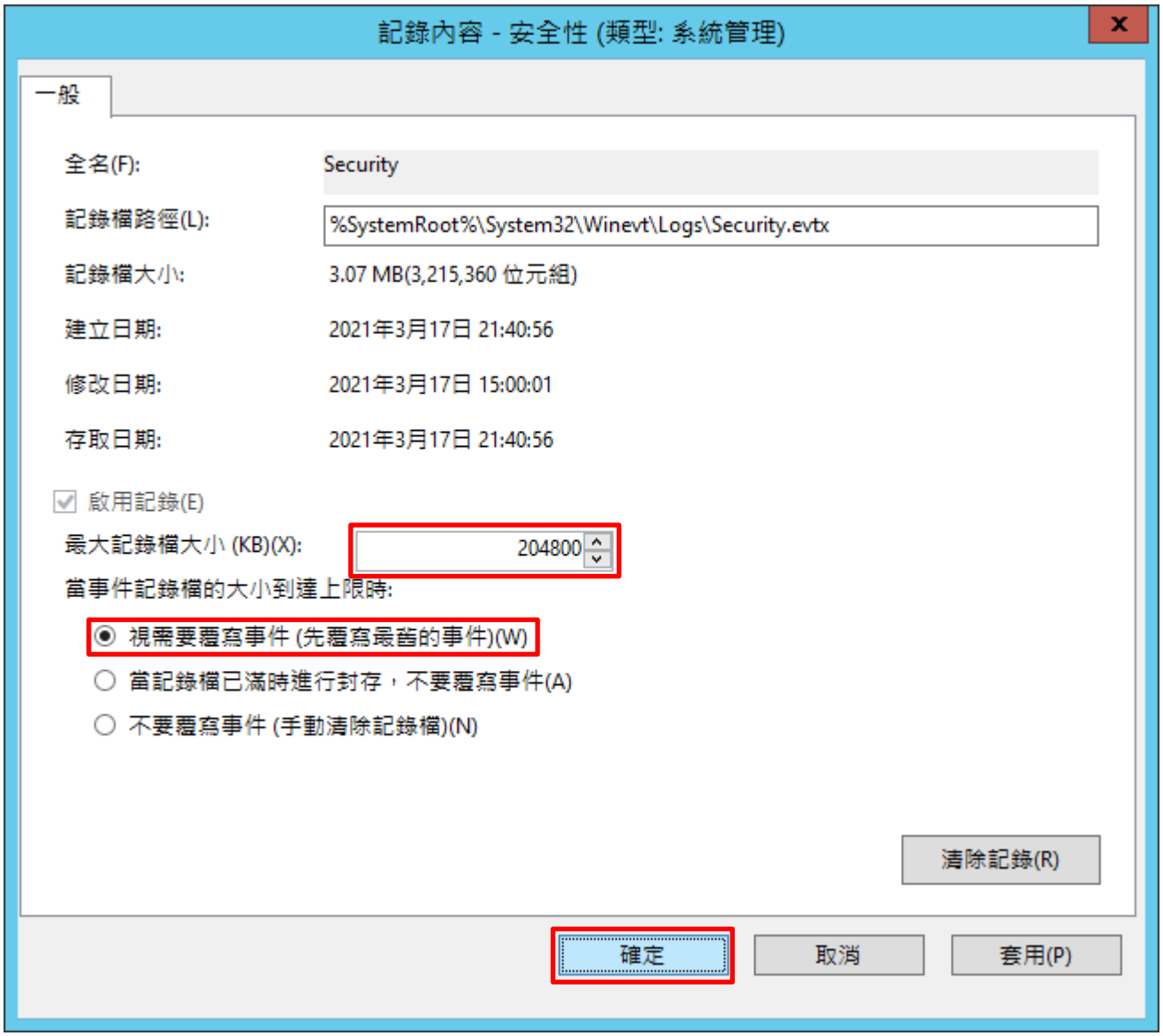
(3) 編輯安全性記錄

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]



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

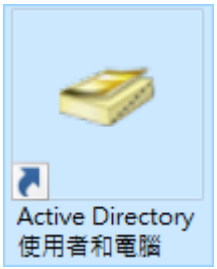
※ 以下分別為網域和工作群組設定方式。

6.1 網域

6.1.1 組織單位設定

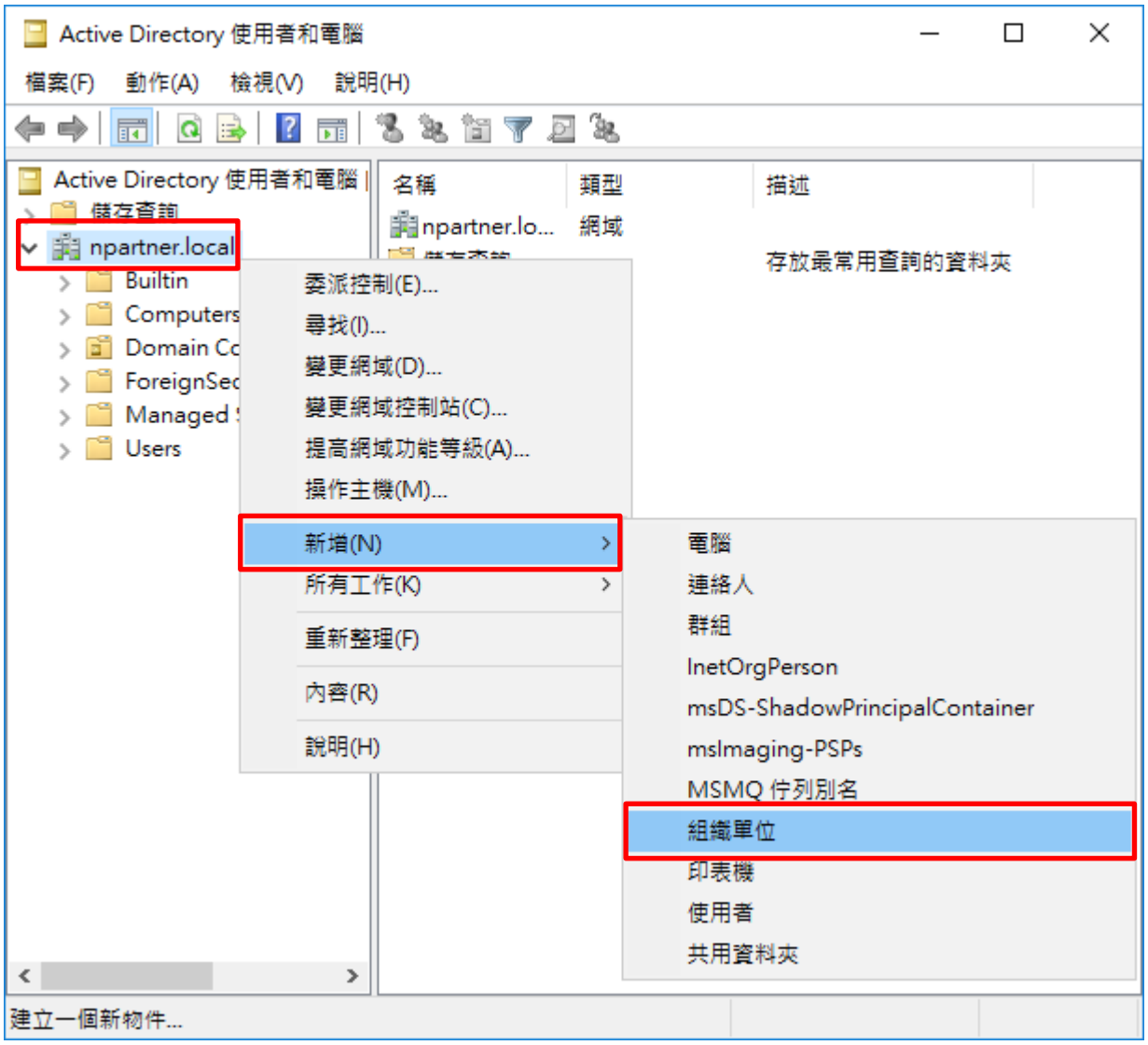
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



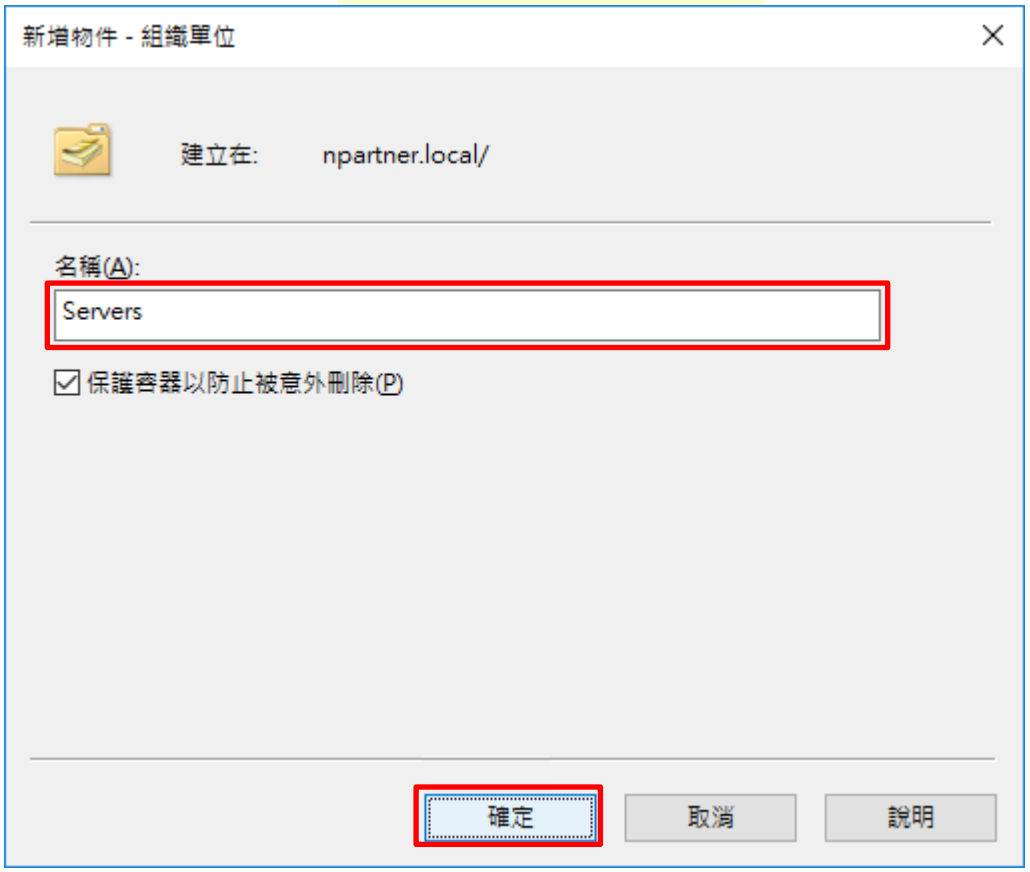
(2) 新增組織單位

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



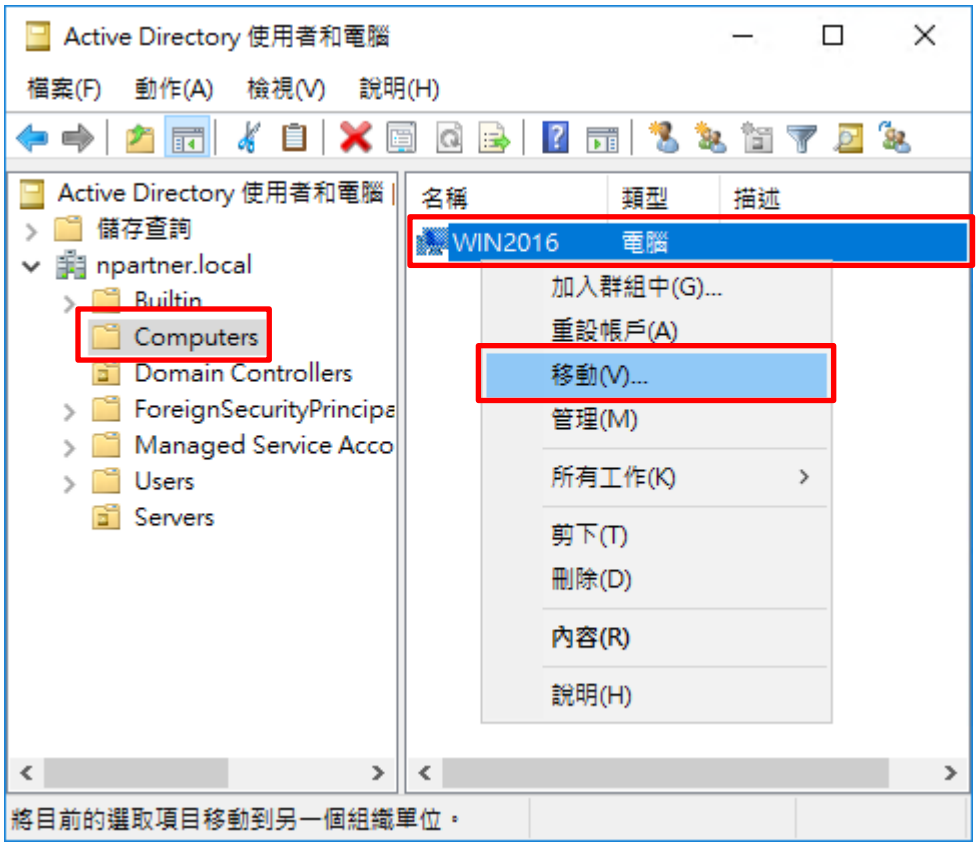
(3) 輸入組織單位名稱

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]



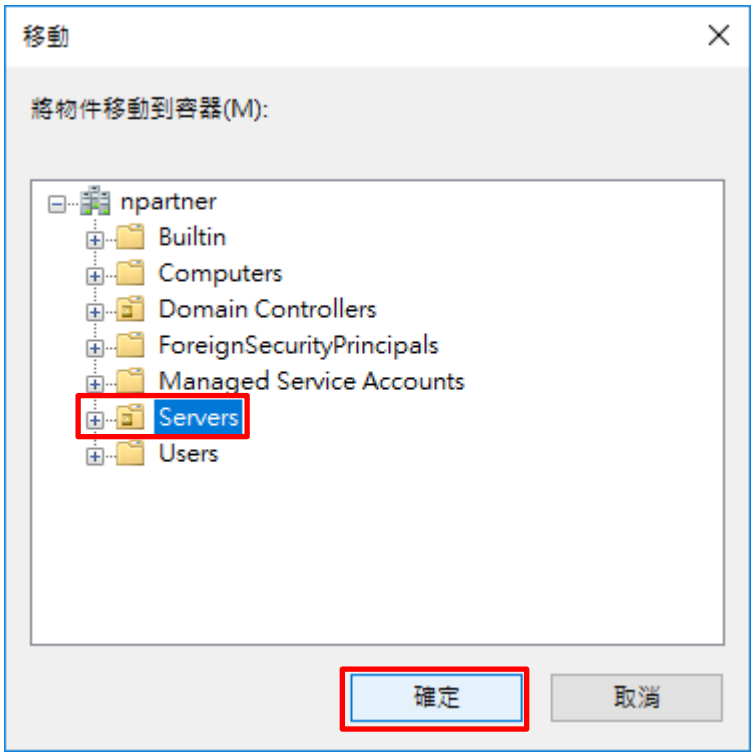
(4) 移動伺服器至新的組織單位

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 Server 主機 -> 點選 [移動]



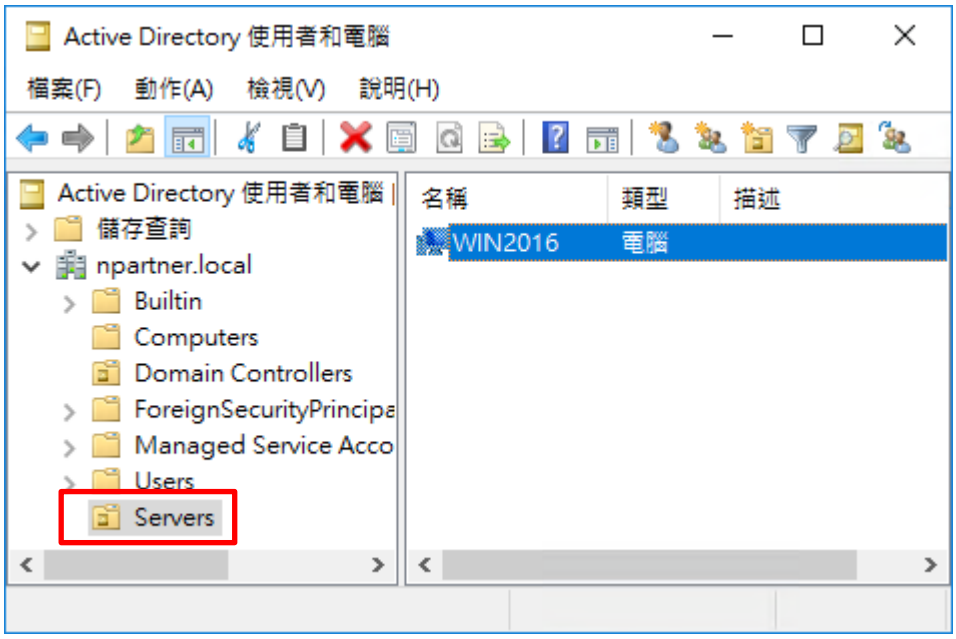
(5) 選擇組織單位

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

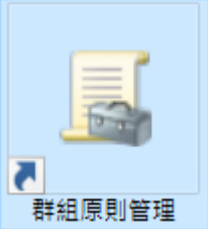
點選 [Servers] 組織單位，確認 Win2016 伺服器已移動。



6.1.2 群組原則設定

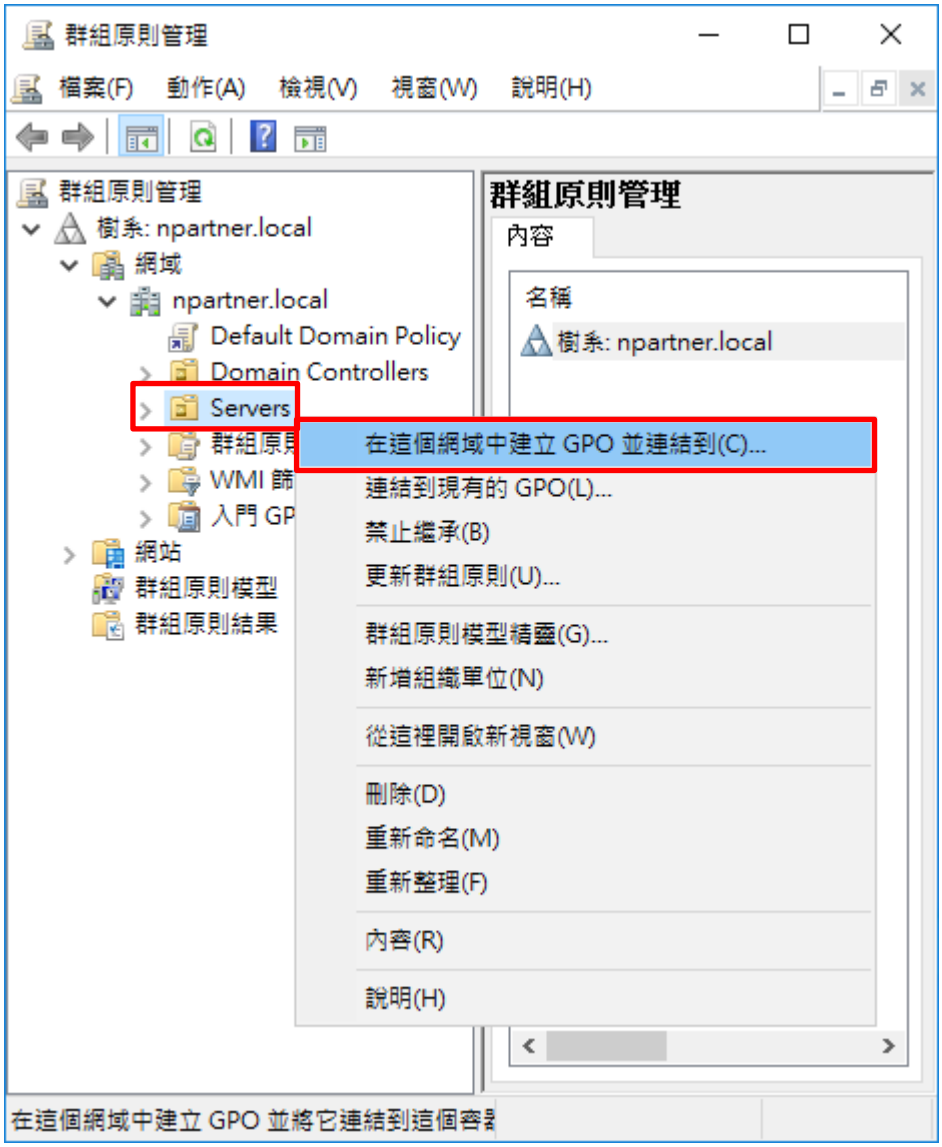
(1) 開啟群組原則管理

開啟 [群組原則管理]



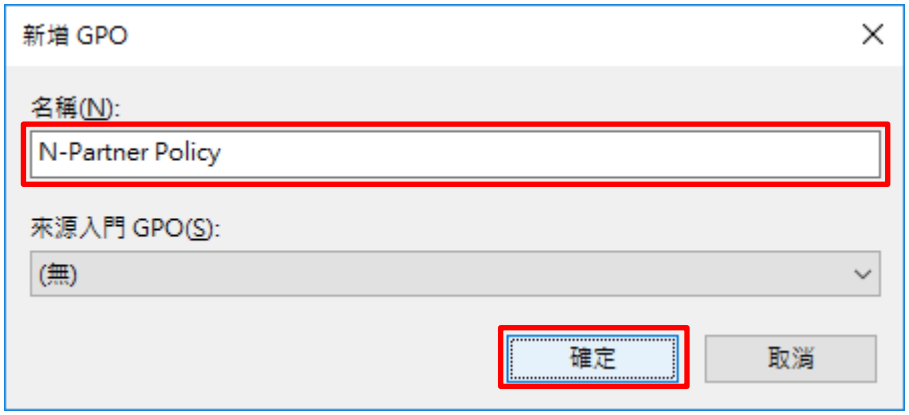
(2) 在 Servers 組織單位，新增群組原則物件

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



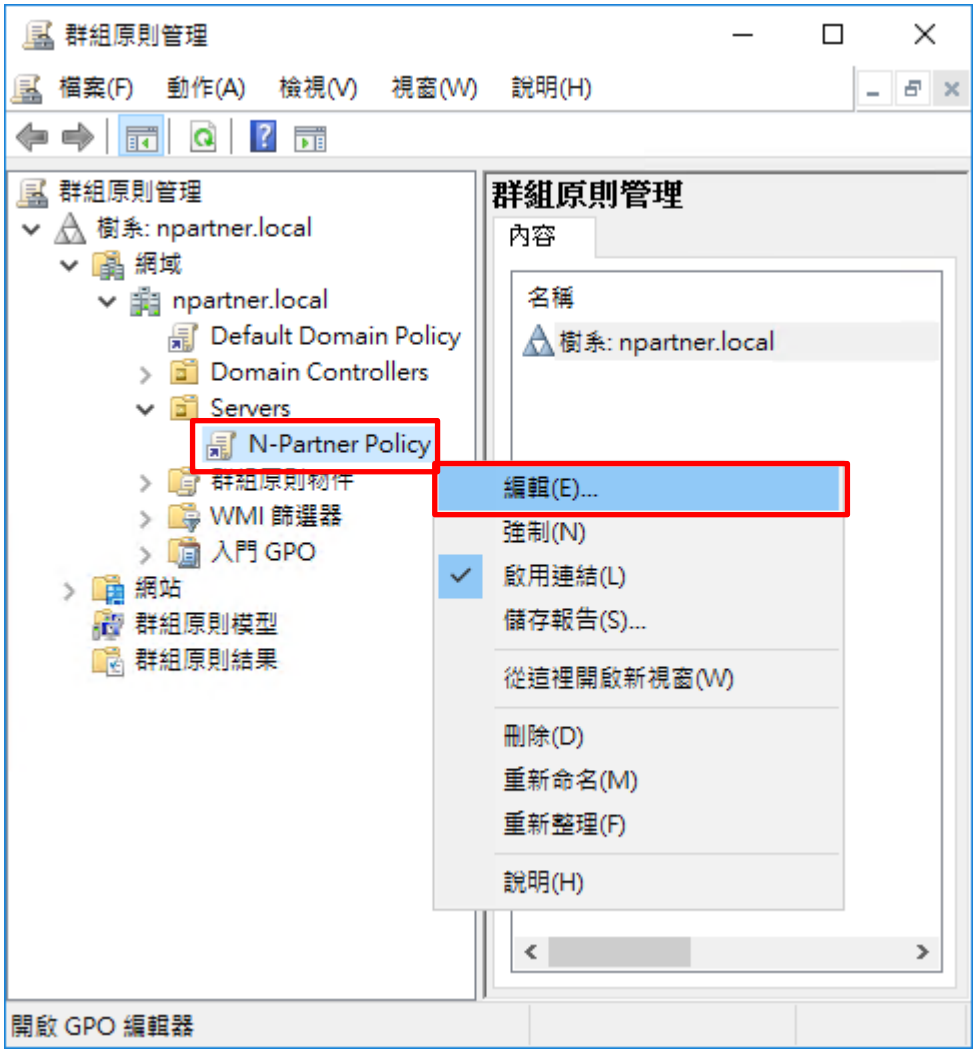
(3) 輸入群組原則物件名稱

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]



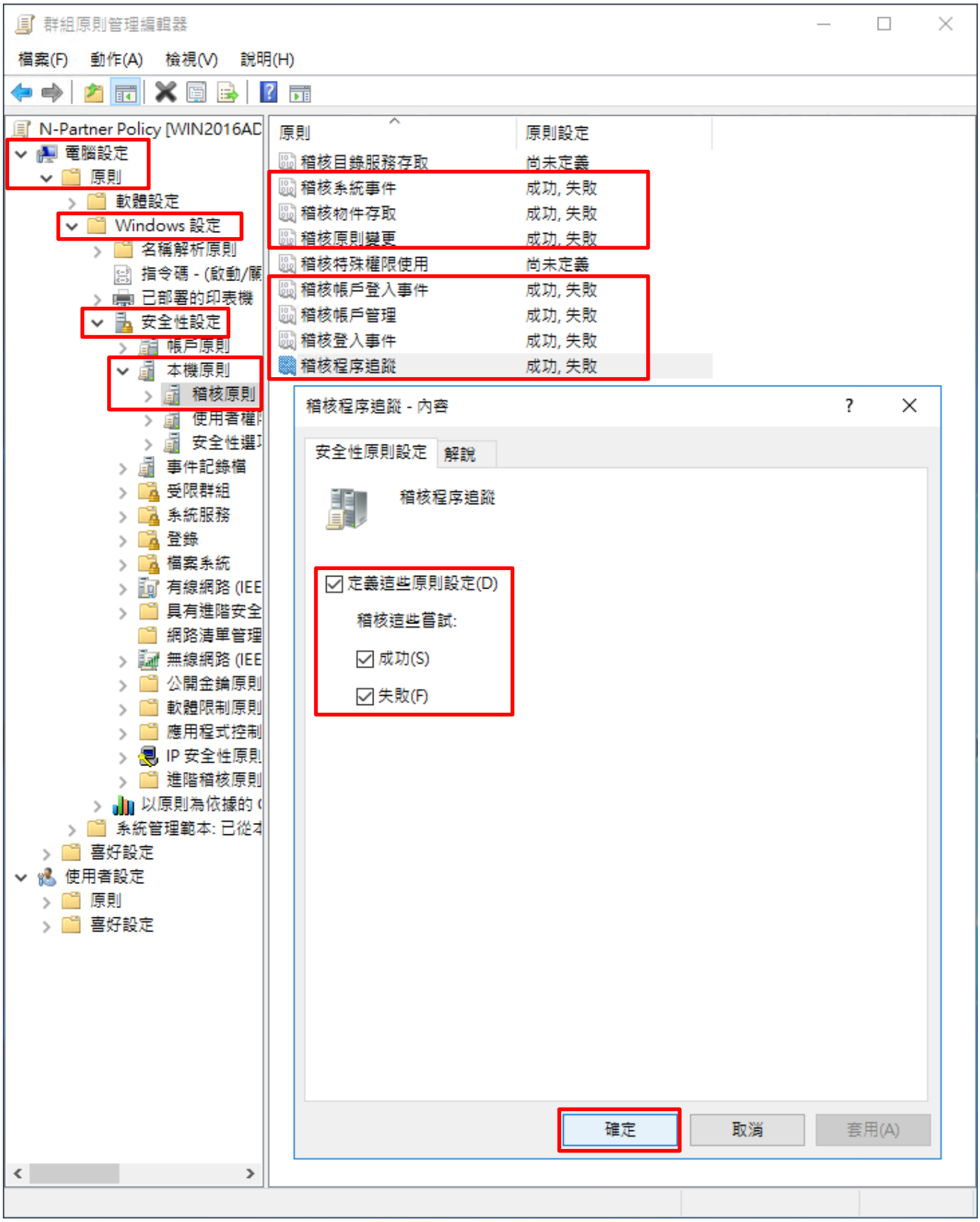
(4) 編輯群組原則物件

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



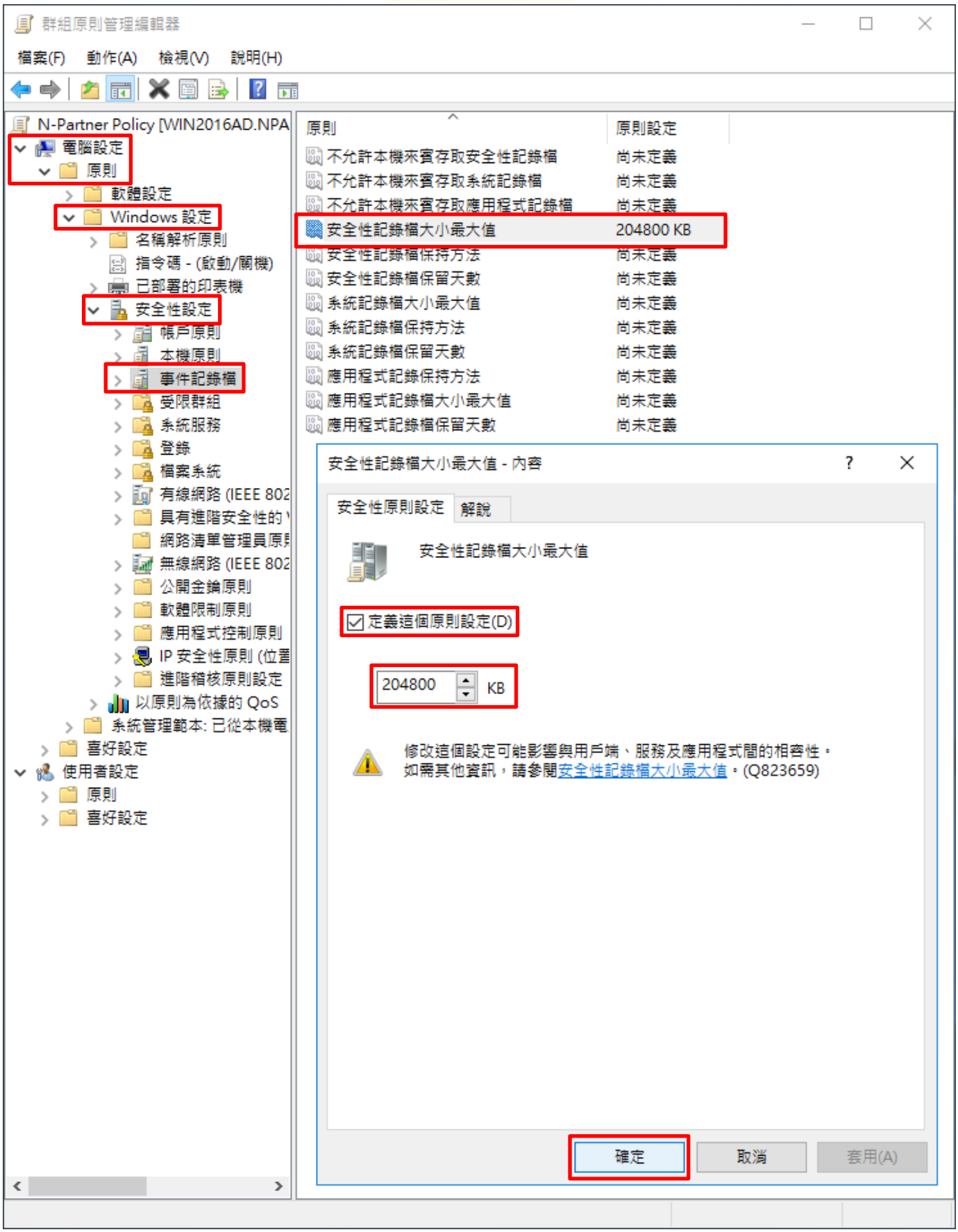
(5) 本機原則：稽核原則

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



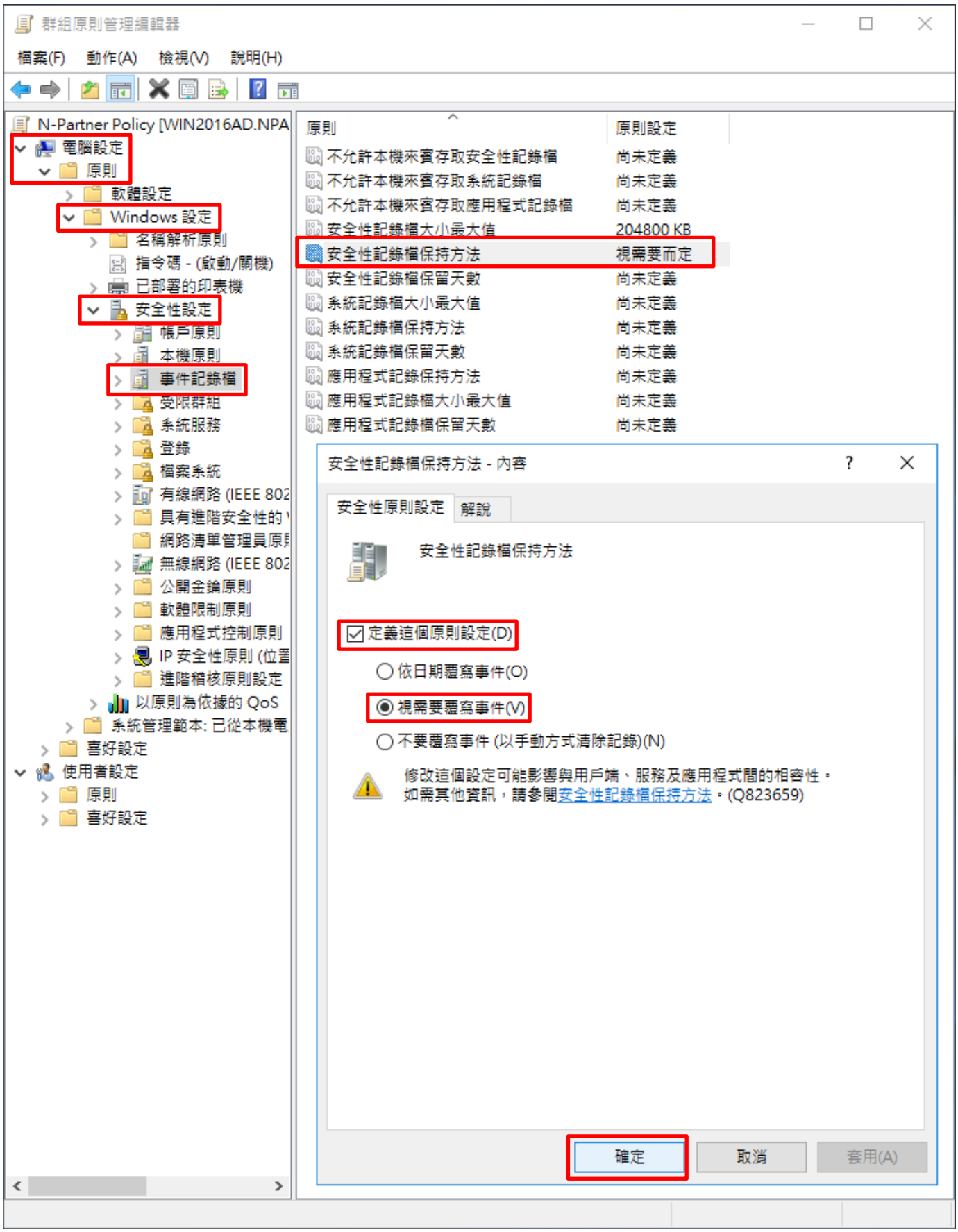
(6) 事件記錄檔：安全性記錄檔大小最大值

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]

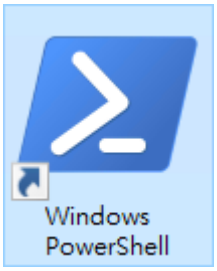


(7) 事件記錄檔：安全性記錄檔保持方法

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]

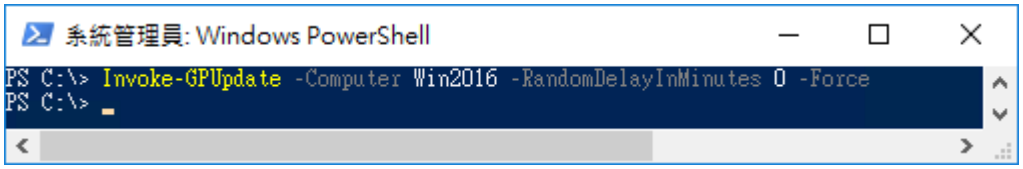


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows Server 群組原則

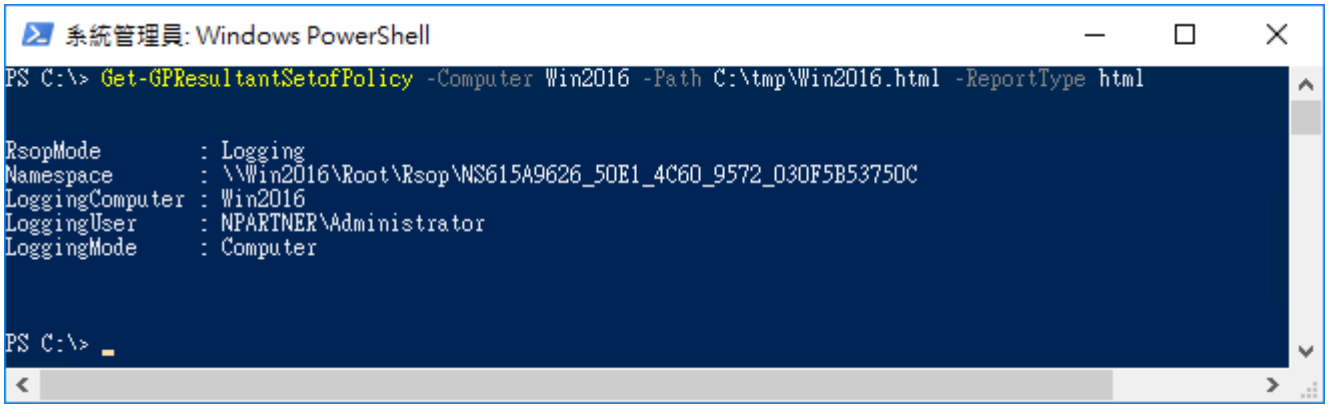
```
PS C:\> Invoke-GPUpdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱

(10) 在 AD 網域伺服器 -> 產生 Windows Server 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 Server 伺服器名稱和資料夾路徑檔案名稱

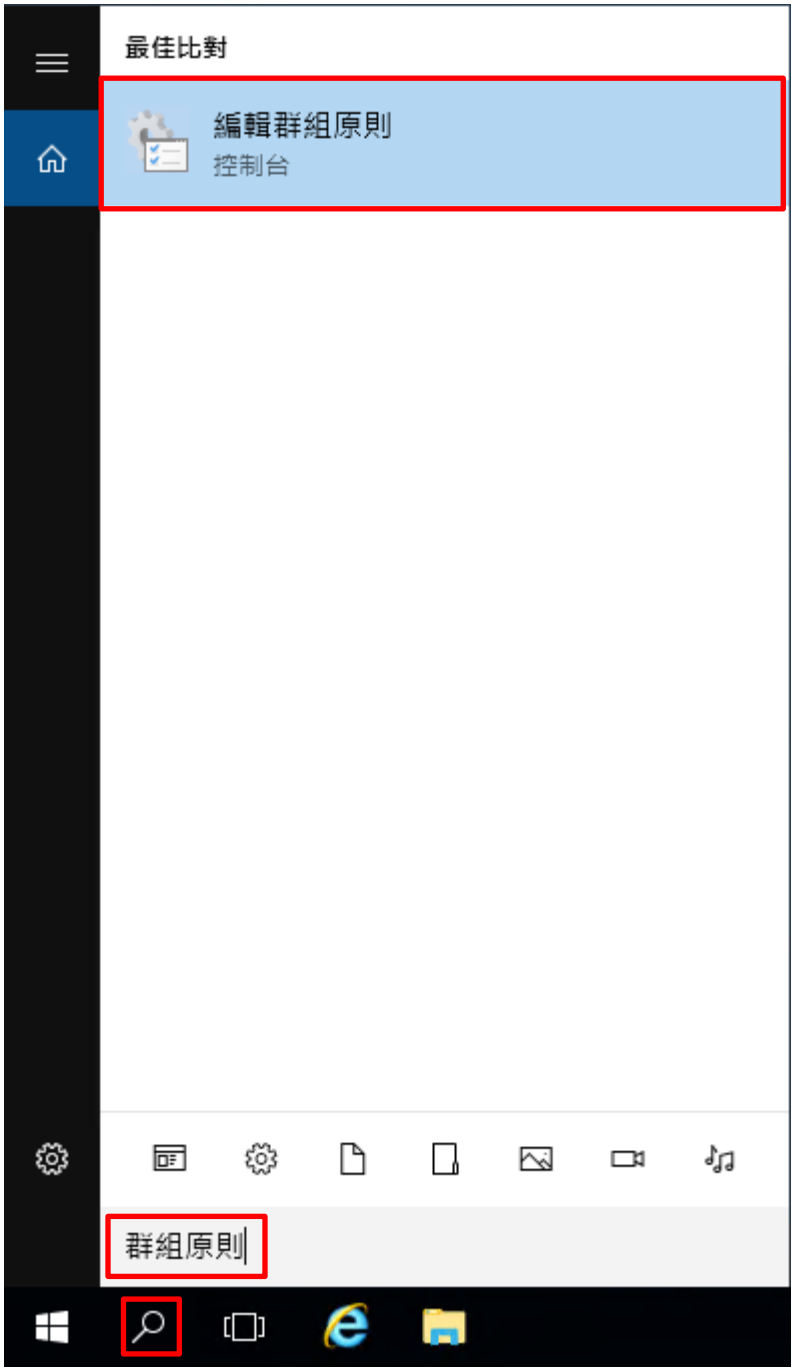
(11) 開啟報表 -> 確認 Windows Server 伺服器 -> 套用 N-Partner Policy 群組原則

6.2 工作群組

6.2.1 稽核原則設定

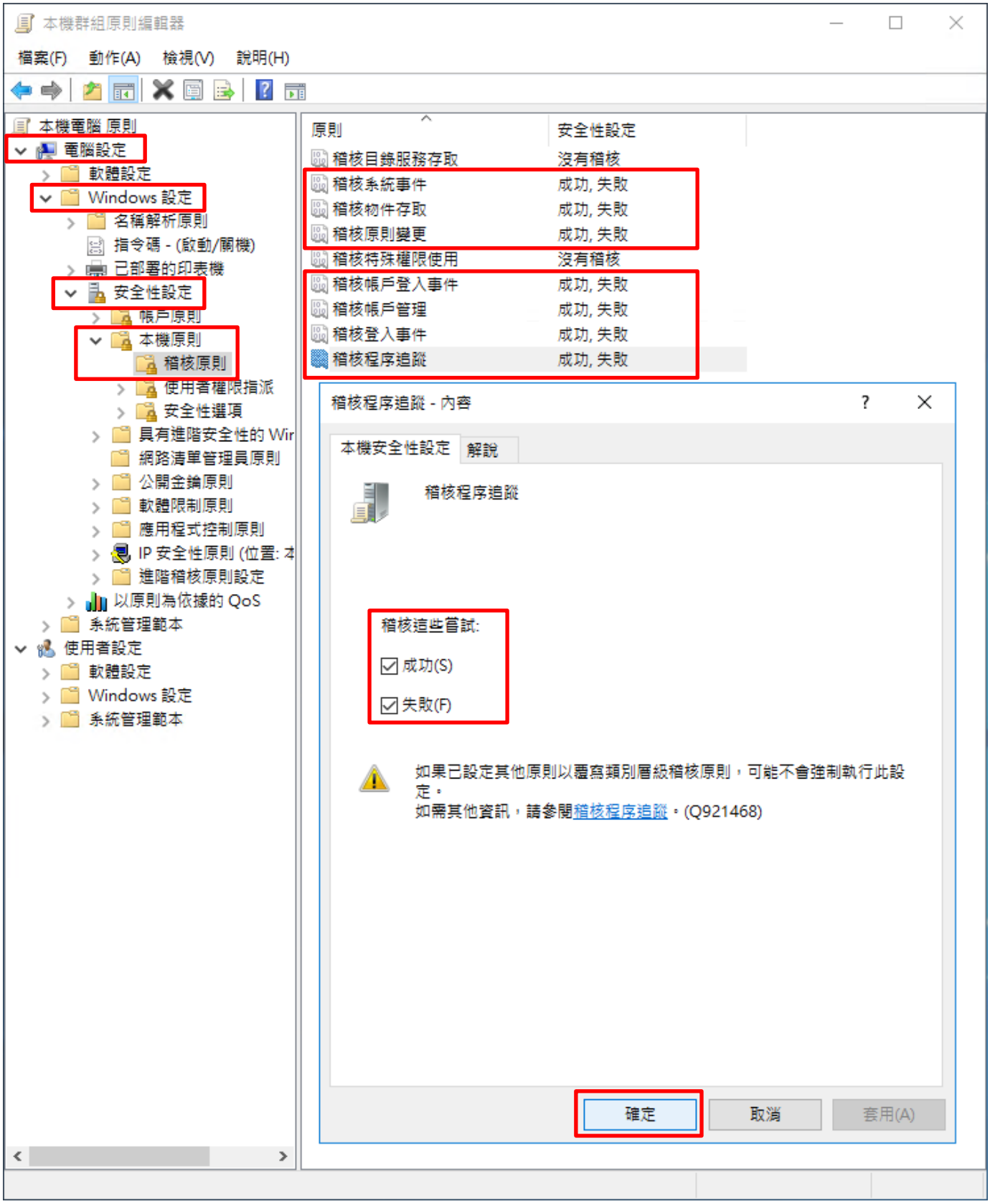
(1) 開啟 [本機群組原則編輯器]

點選 [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

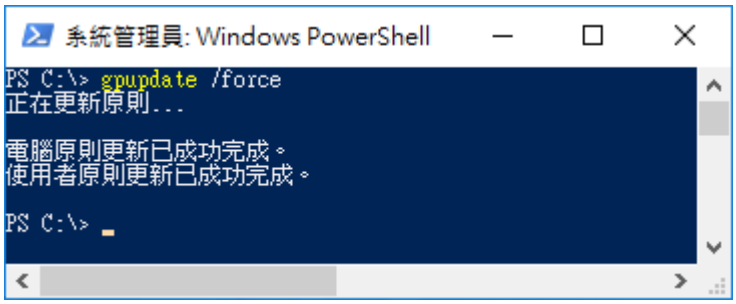
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

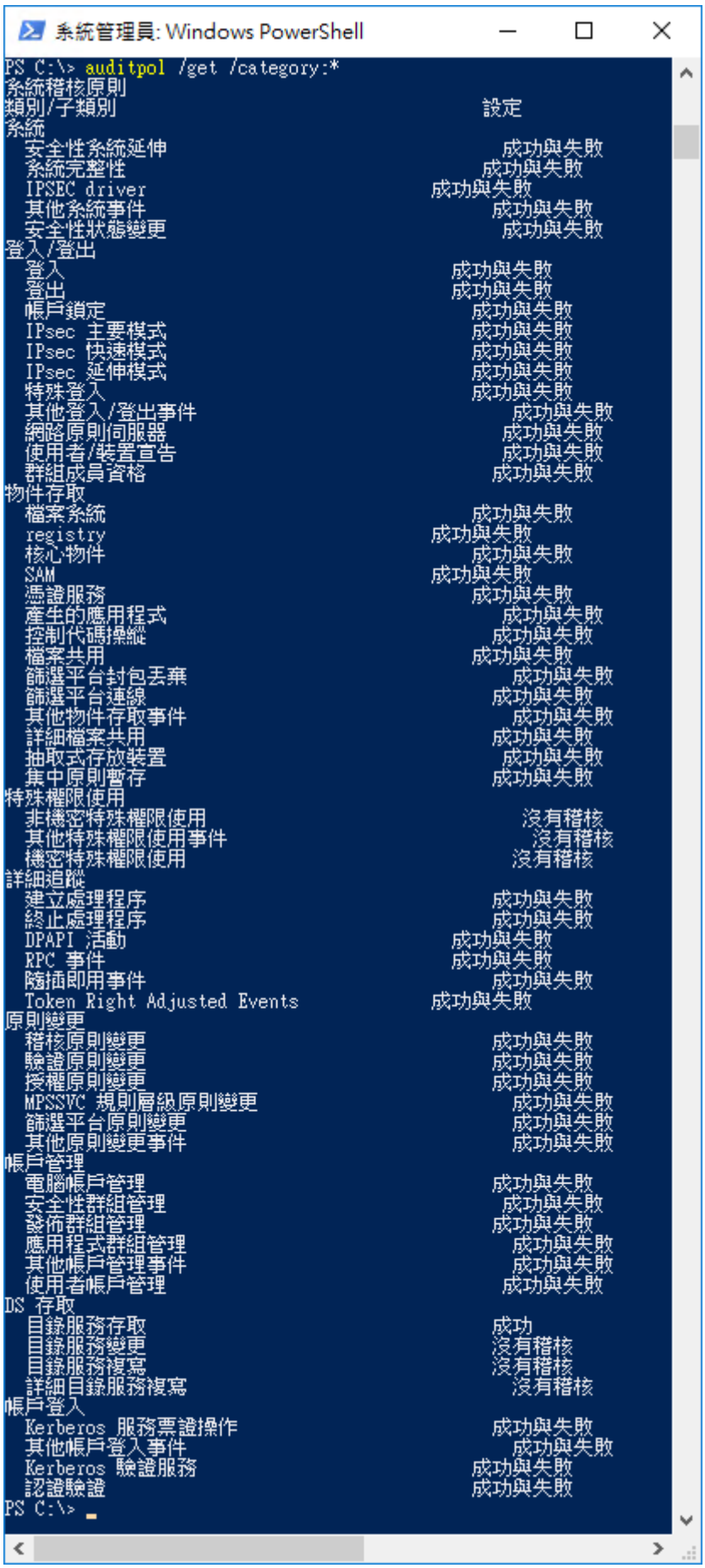
(4) 更新群組原則

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



(5) 查看群組原則套用情形

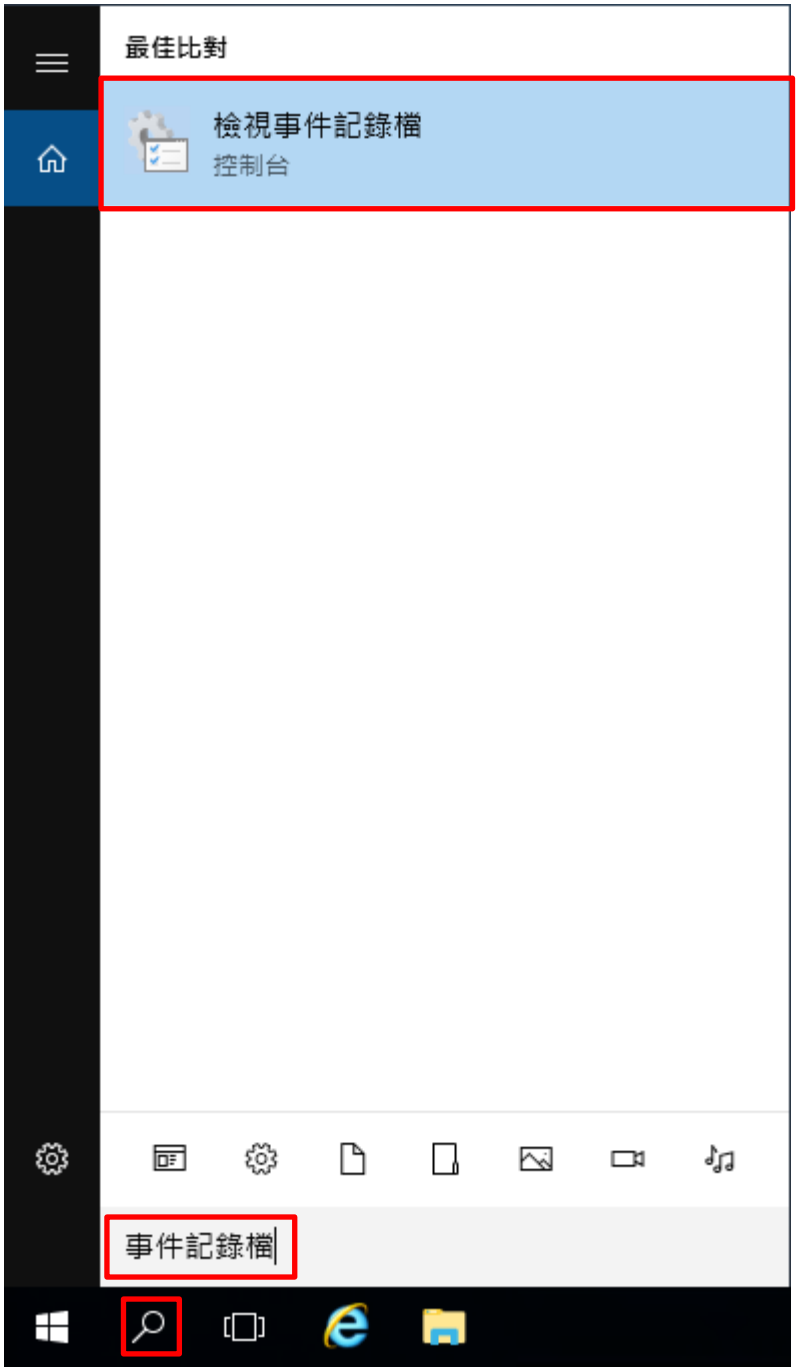
```
PS C: \> auditpol /get /category:*
```



6.2.2 事件檔案設定

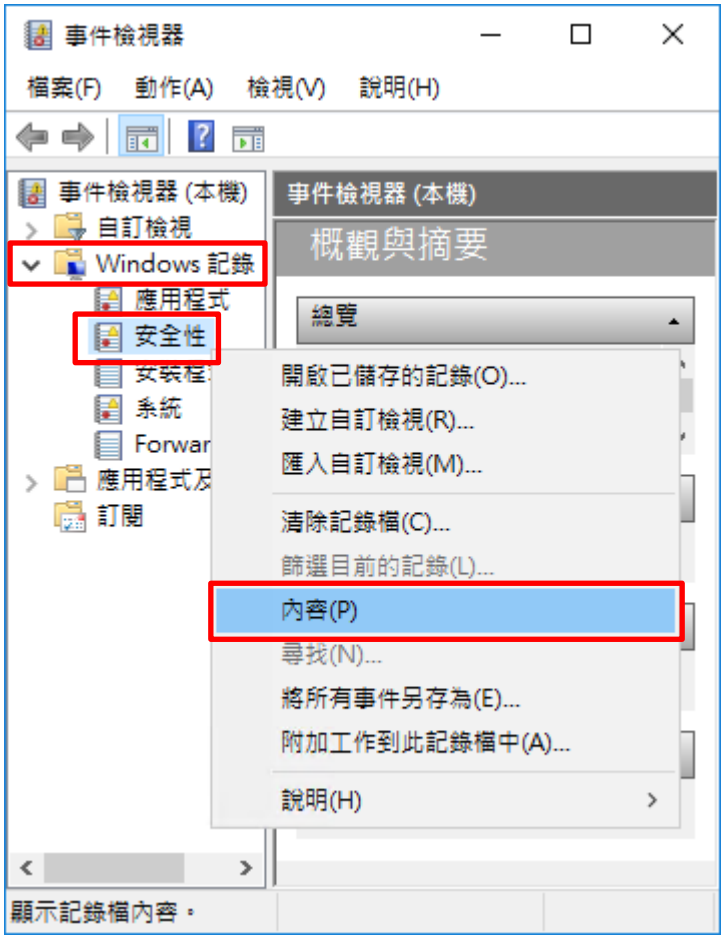
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入事件記錄檔 -> 點選 [檢視事件記錄檔]



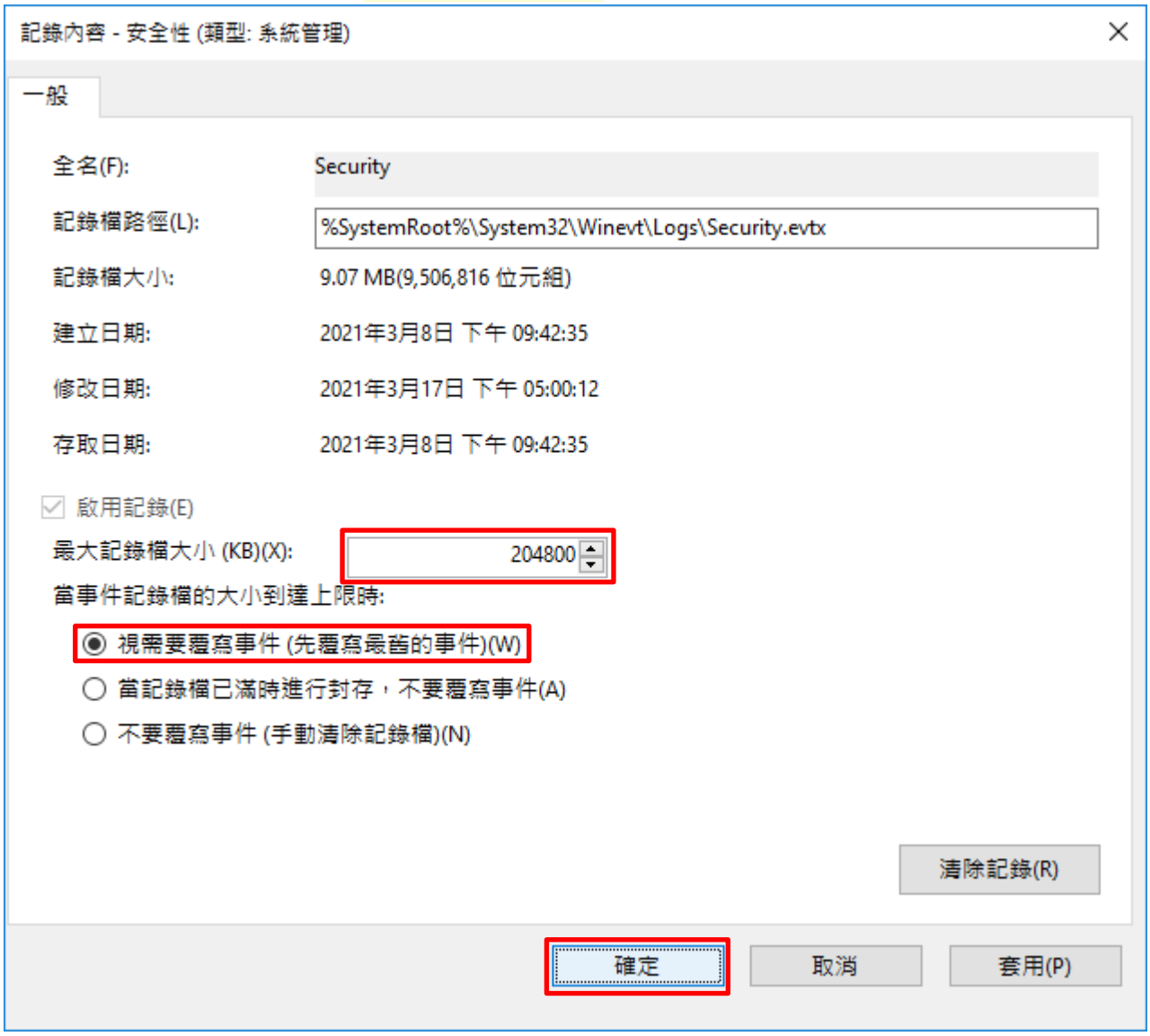
(2) 編輯安全性記錄

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]



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

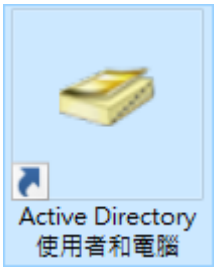
※ 以下分別為網域和工作群組設定方式。

7.1 網域

7.1.1 組織單位設定

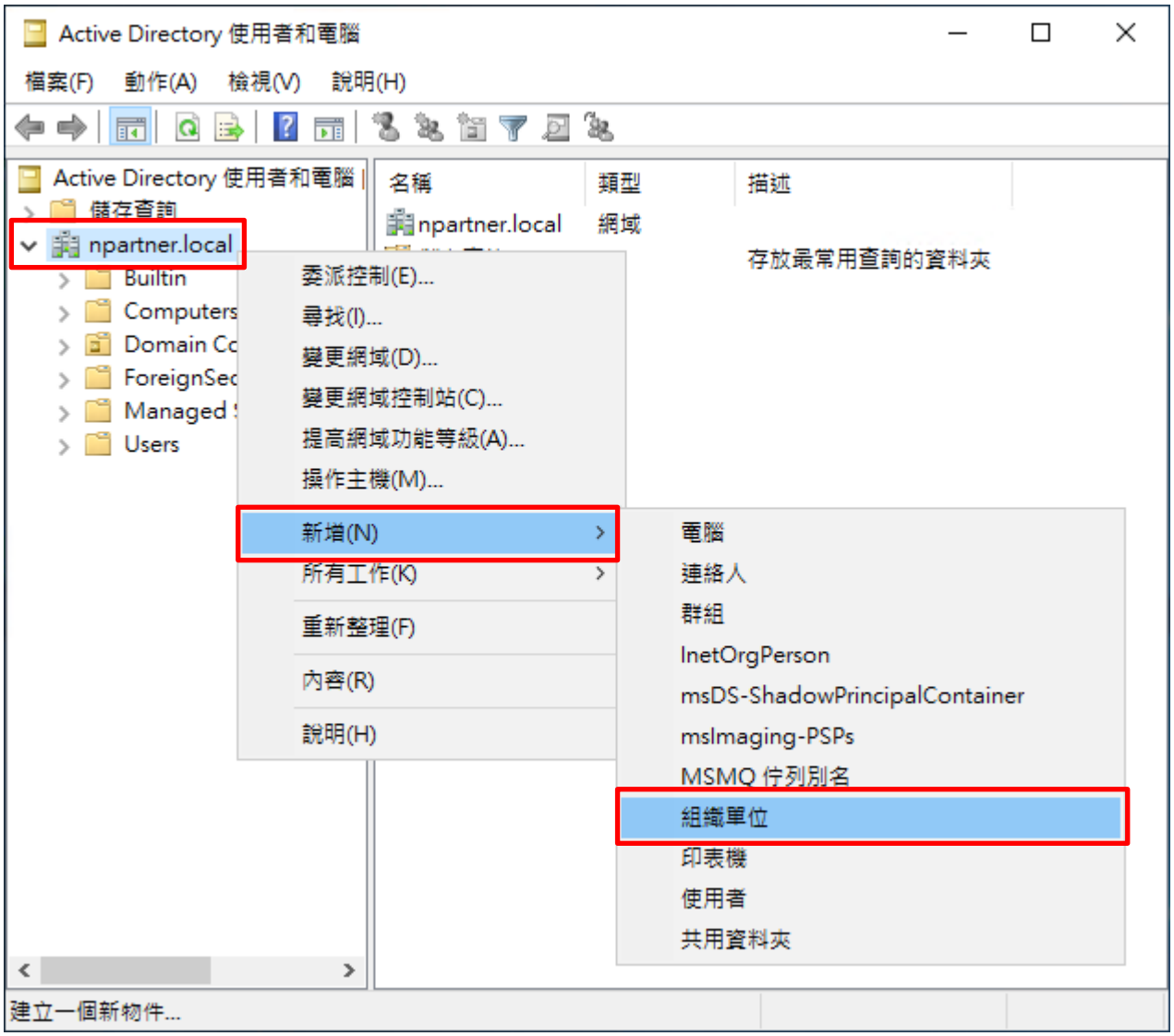
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



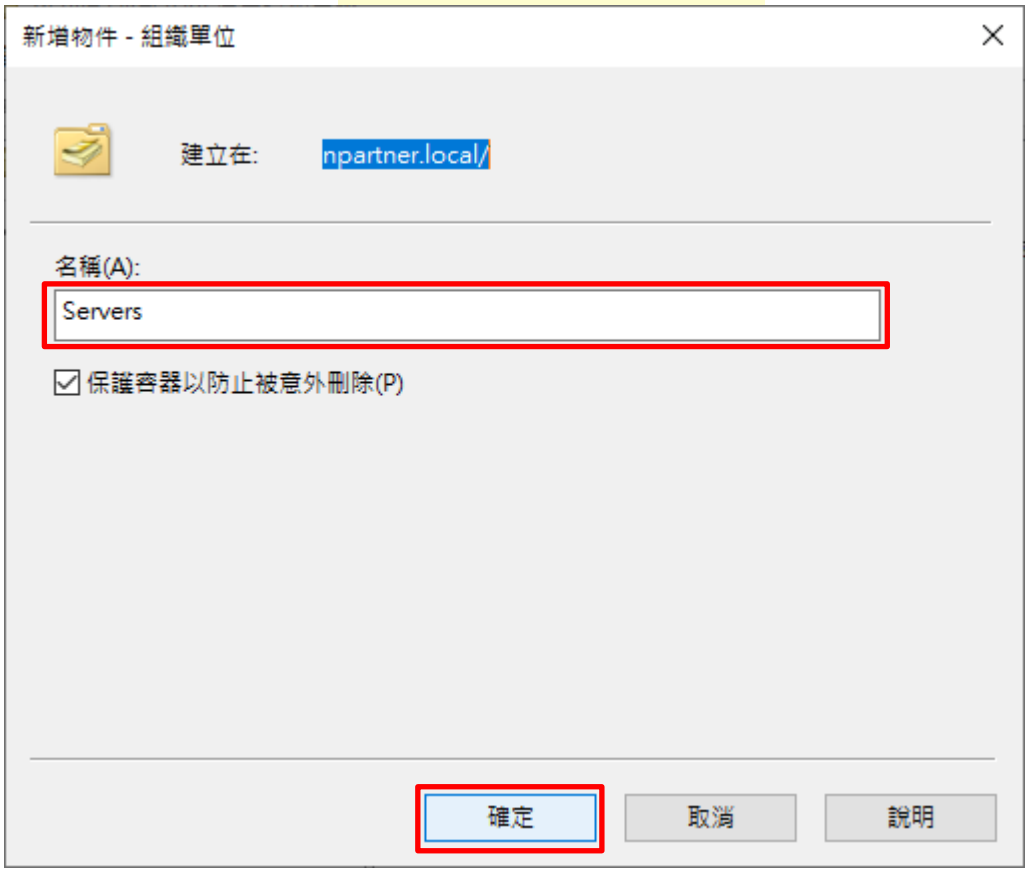
(2) 新增組織單位

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

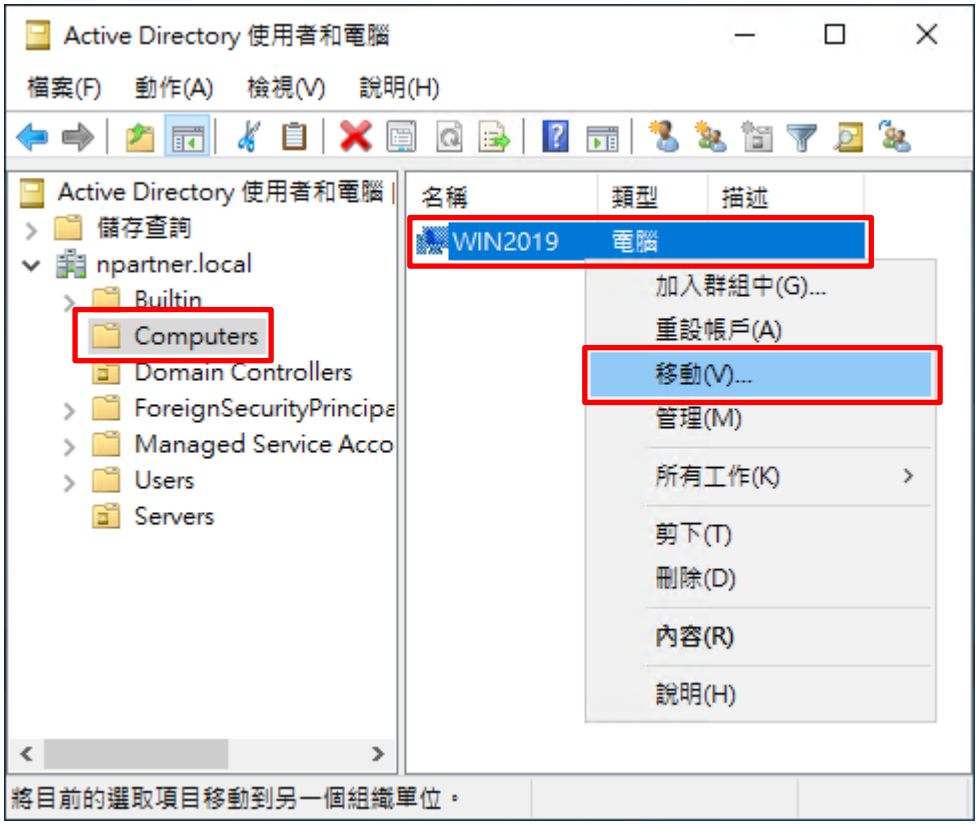
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

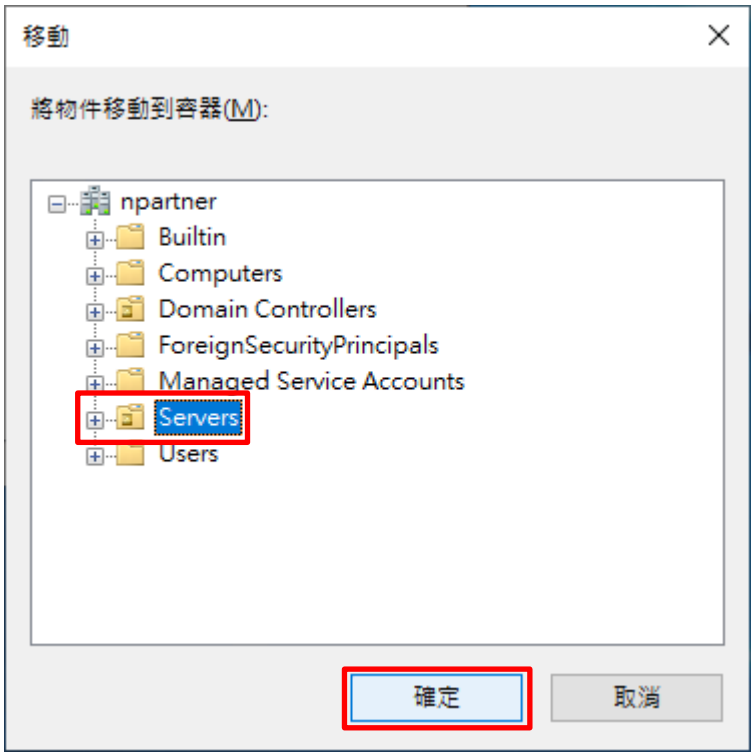
選擇 [Computers] 組織單位 -> 在 [Win2019] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



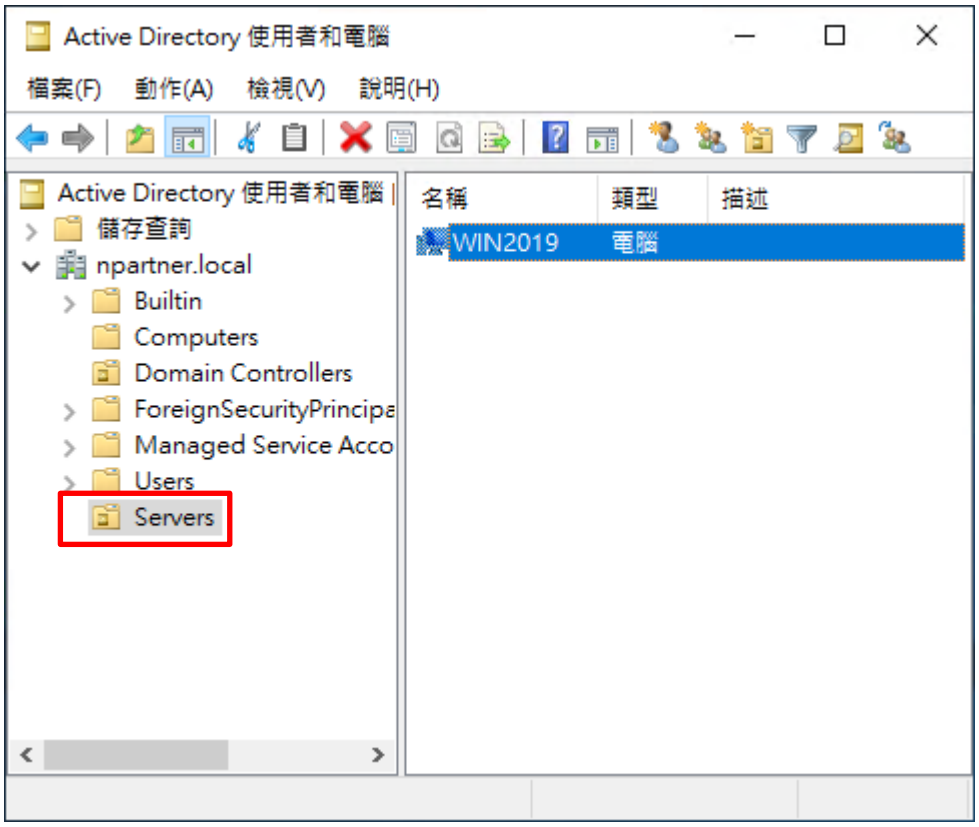
(5) 選擇組織單位

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

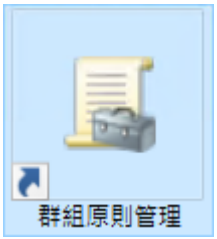
點選 [Servers] 組織單位，確認 Win2019 伺服器已移動。



7.1.2 群組原則設定

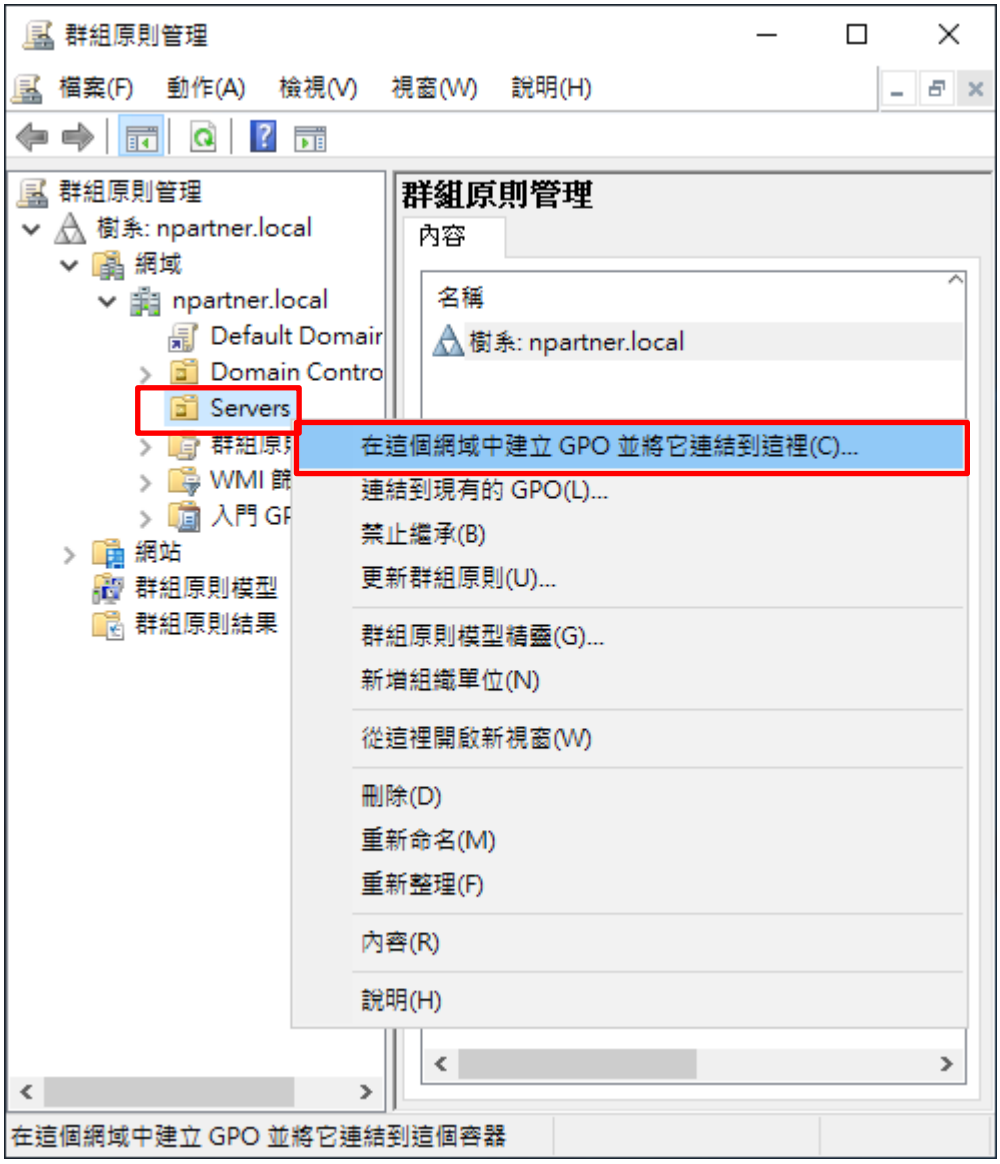
(1) 開啟群組原則管理

開啟 [群組原則管理]



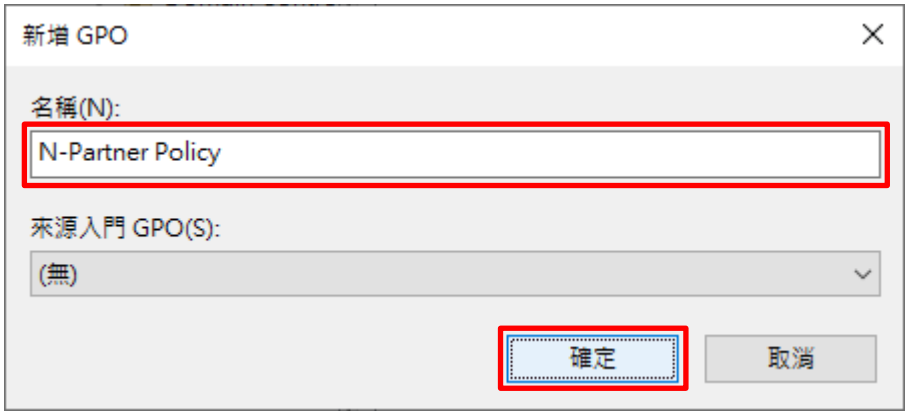
(2) 在 Servers 組織單位，新增群組原則物件

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



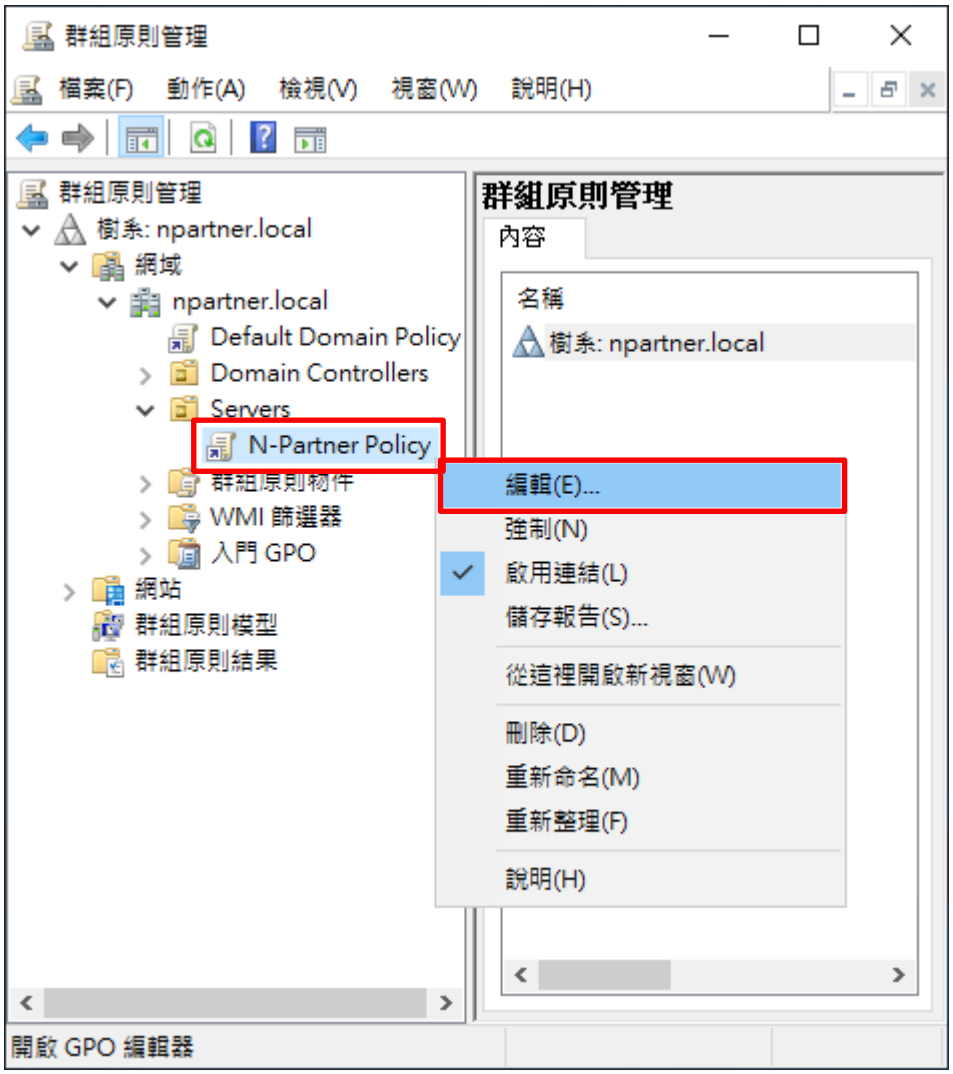
(3) 輸入群組原則物件名稱

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]



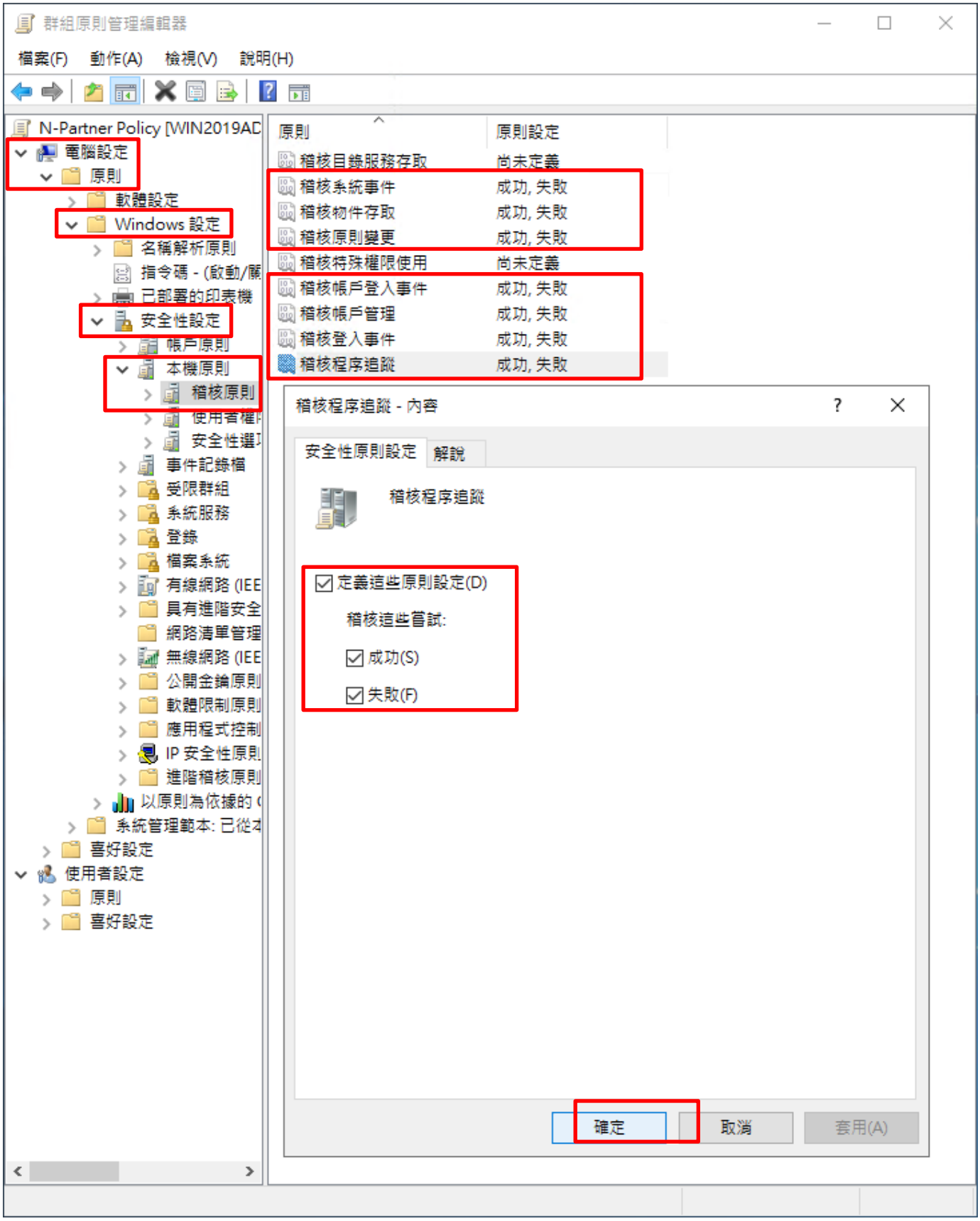
(4) 編輯群組原則物件

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



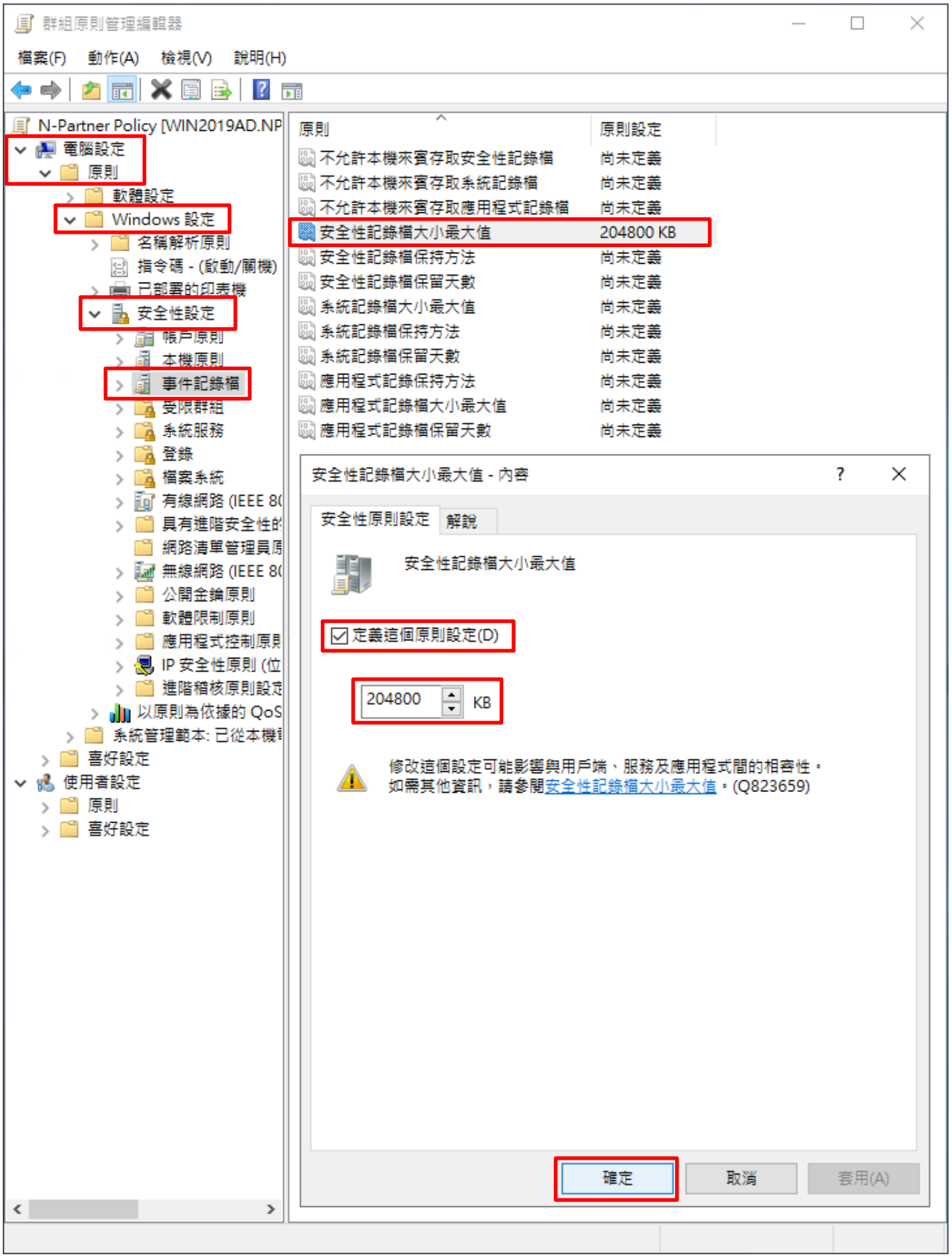
(5) 本機原則：稽核原則

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



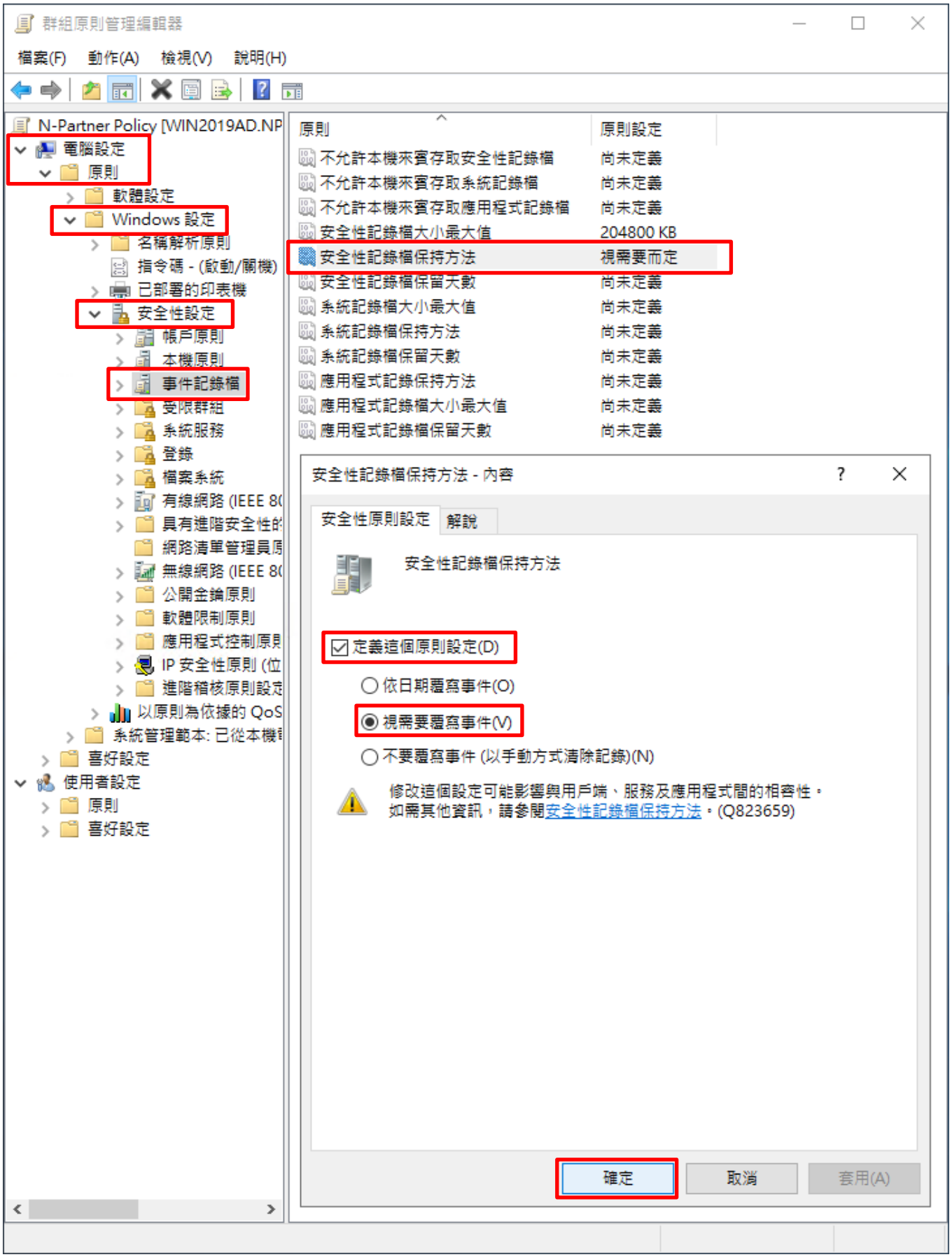
(6) 事件記錄檔：安全性記錄檔大小最大值

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

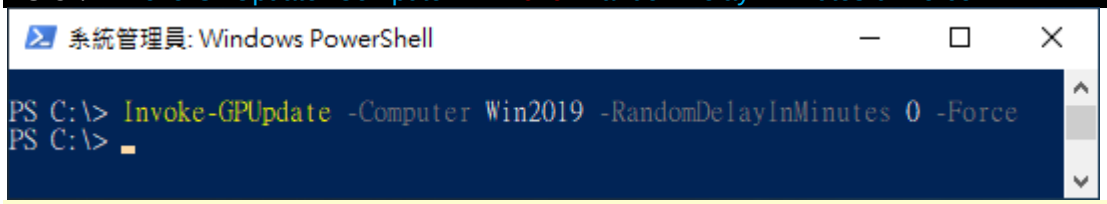
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

(9) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

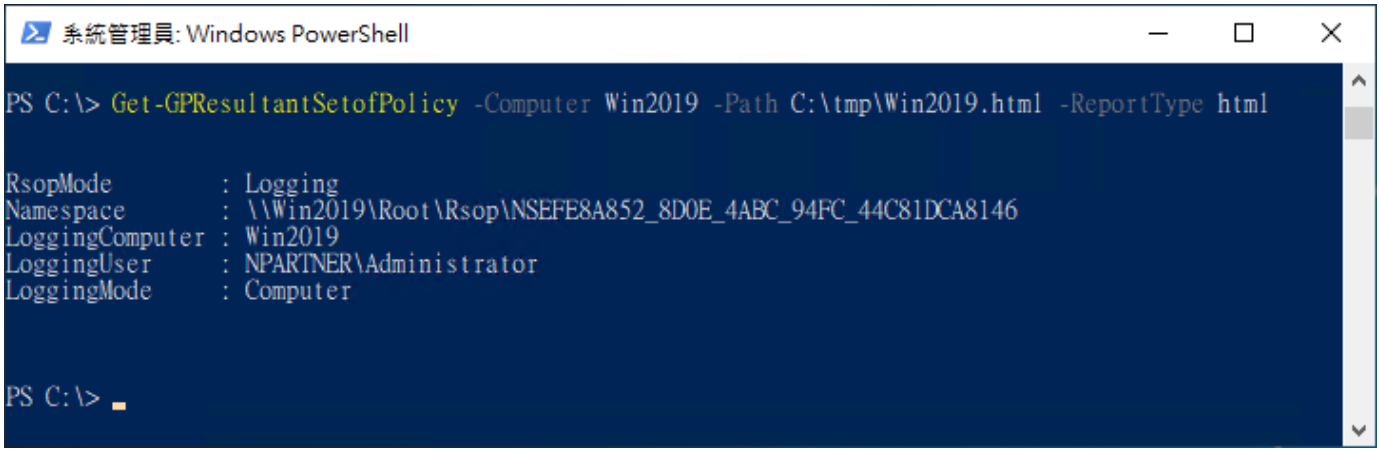
```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱

(10) 在 AD 網域伺服器 -> 產生 Windows Server 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 Server 伺服器名稱和資料夾路徑檔案名稱

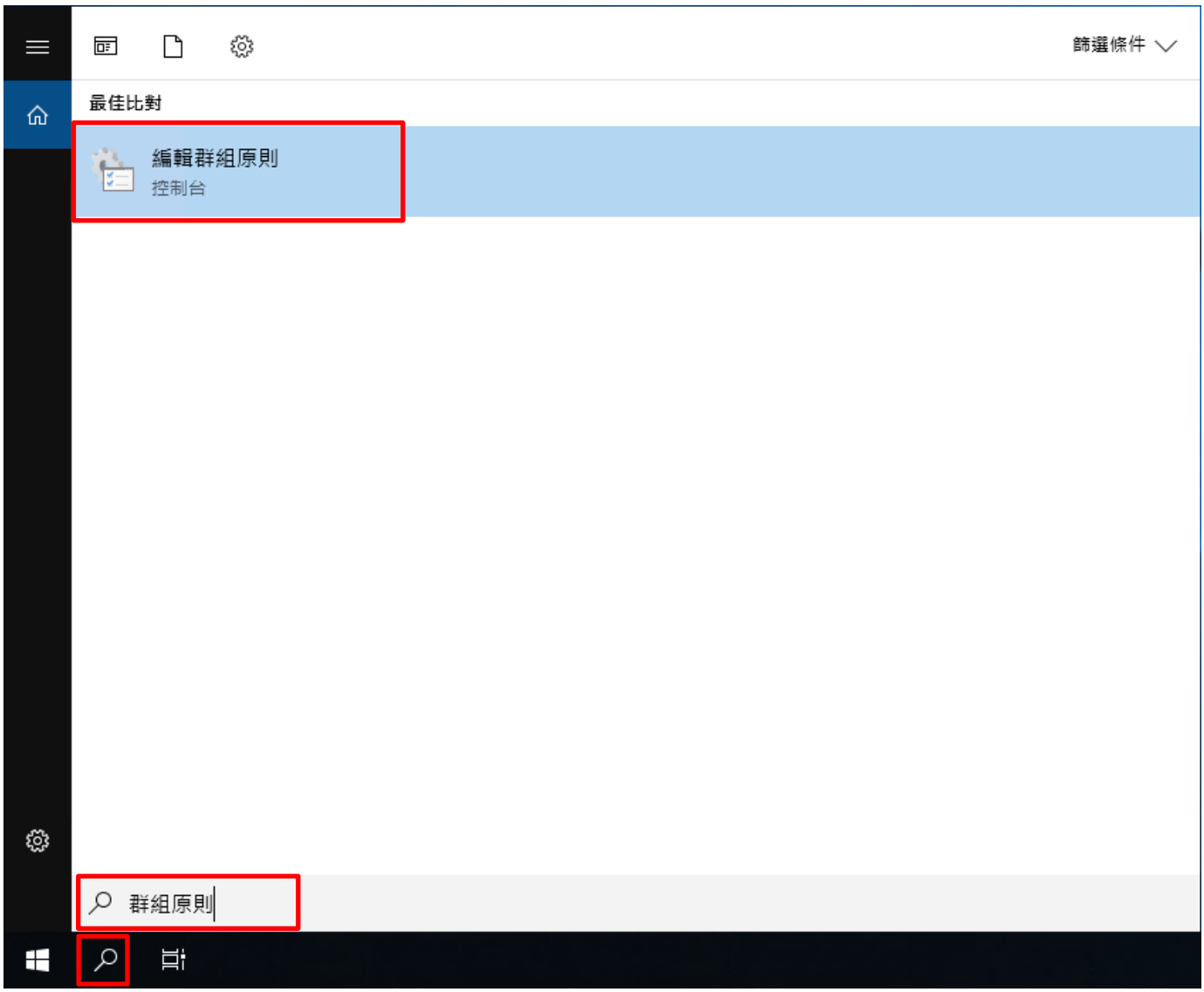
(11) 開啟報表 -> 確認 Windows Server 伺服器 -> 套用 N-Partner Policy 群組原則

7.2 工作群組

7.2.1 稽核原則設定

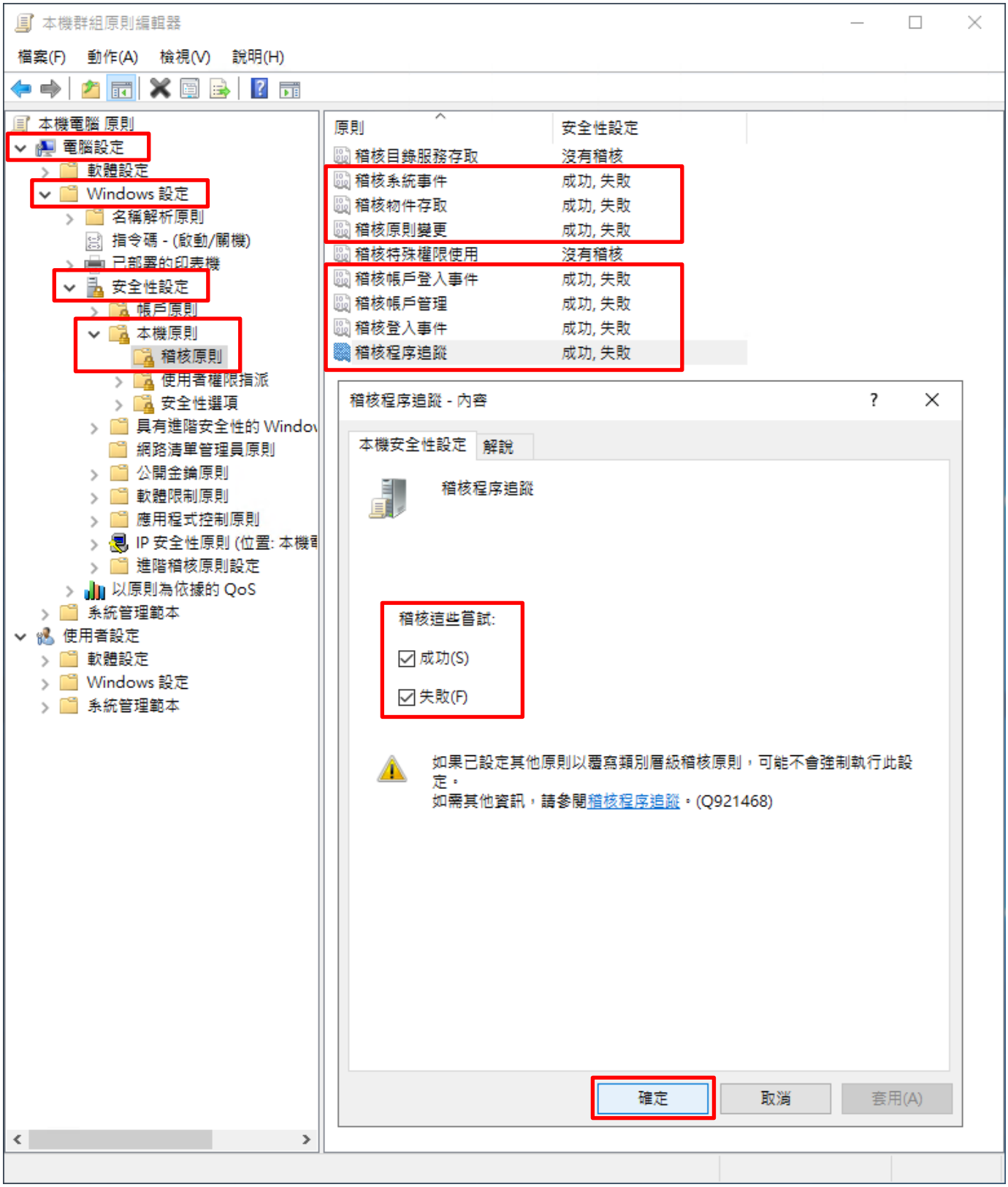
(1) 開啟本機群組原則編輯器

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

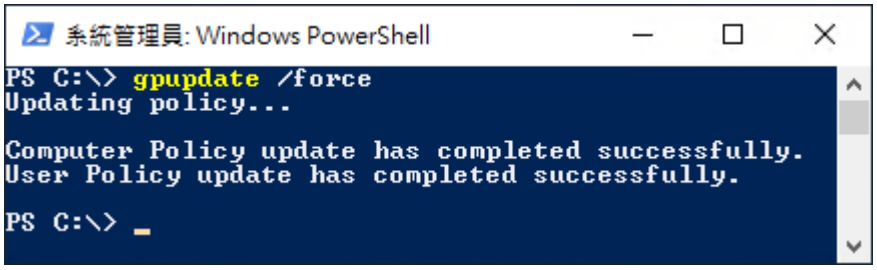
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(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:*
```

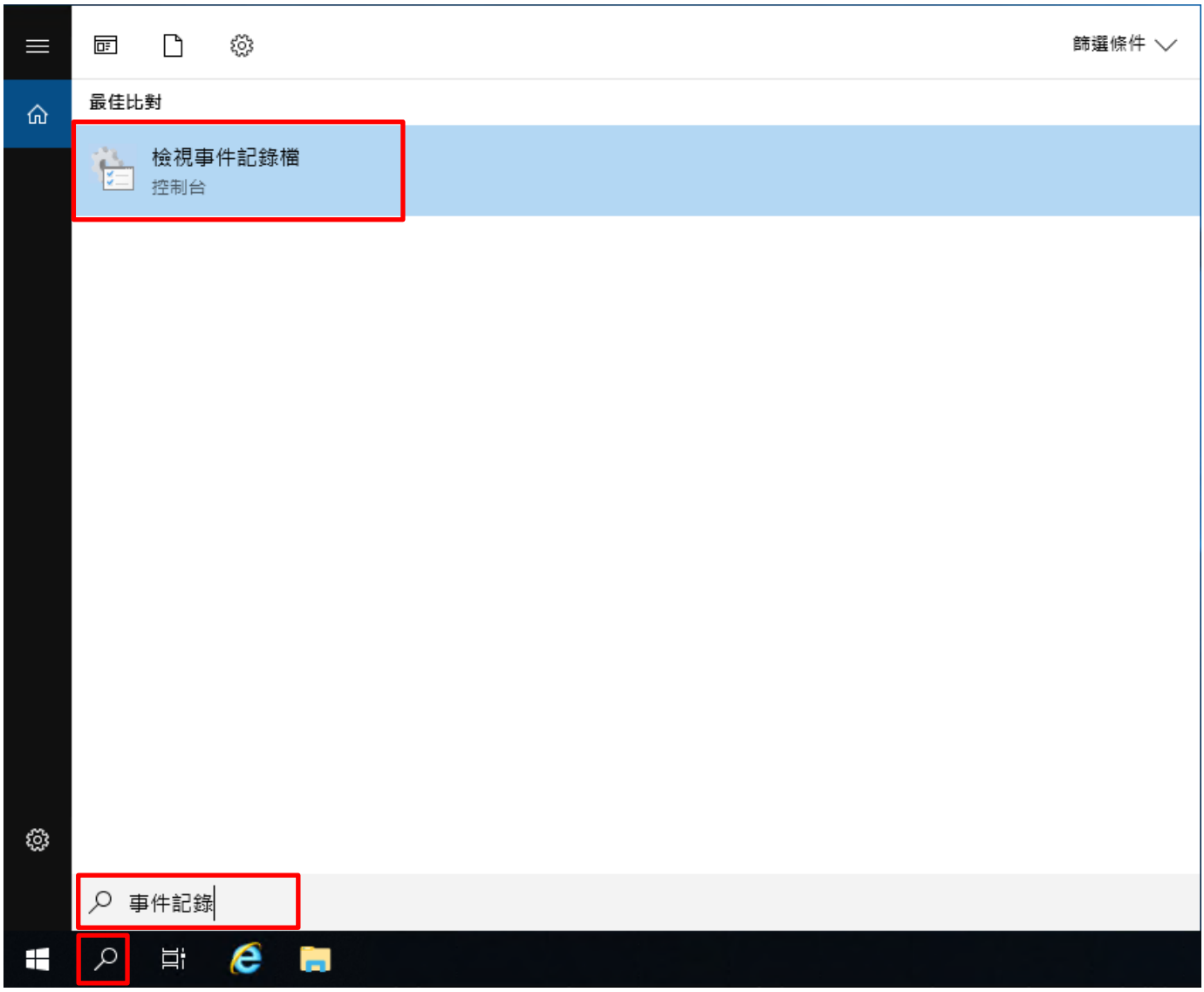
系統管理員: Windows PowerShell

```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
系統
  安全性系統延伸                          Success and Failure
  系統完整性                            Success and Failure
  IPSEC driver                          Success and Failure
  其他系統事件                            Success and Failure
  安全性狀態變更                           Success and Failure
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                            Success and Failure
  終止處理程序                            Success and Failure
  DPAPI 活動                            Success and Failure
  RPC 事件                              Success and Failure
  隨插即用事件                            Success and Failure
  權杖權限調整事件                          Success and Failure
原則變更
  稽核原則變更                            Success and Failure
  驗證原則變更                            Success and Failure
  授權原則變更                            Success and Failure
  MPSSVC 規則層級原則變更                    Success and Failure
  篩選平台原則變更                          Success and Failure
  其他原則變更事件                          Success and Failure
帳戶管理
  電腦帳戶管理                            Success and Failure
  安全性群組管理                           Success and Failure
  發佈群組管理                            Success and Failure
  應用程式群組管理                          Success and Failure
  其他帳戶管理事件                          Success and Failure
  使用者帳戶管理                           Success and Failure
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

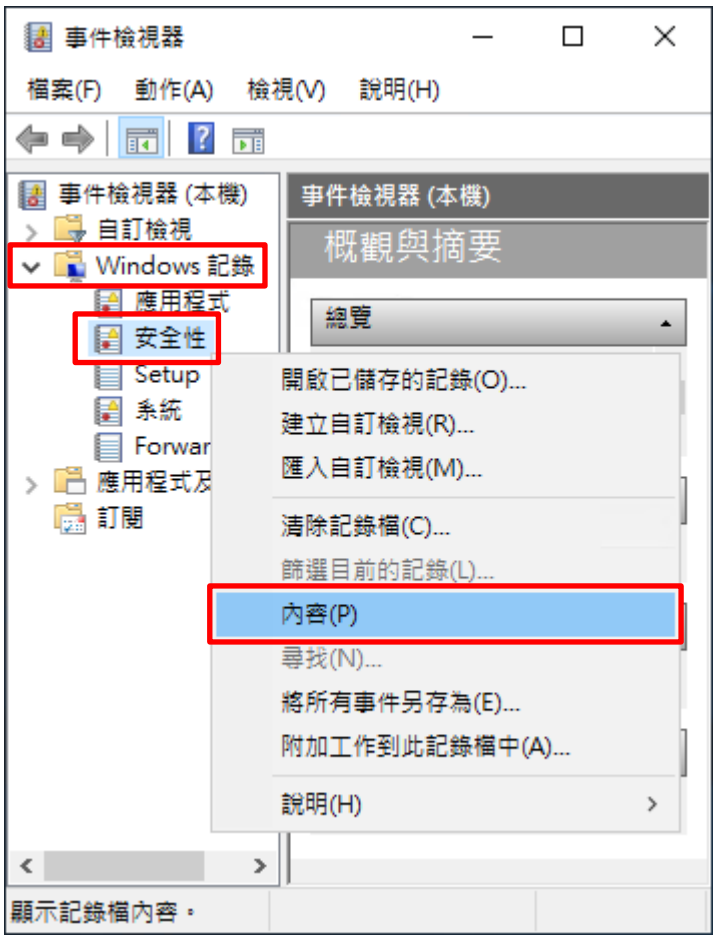
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入事件記錄 -> 點選 [檢視事件記錄檔]



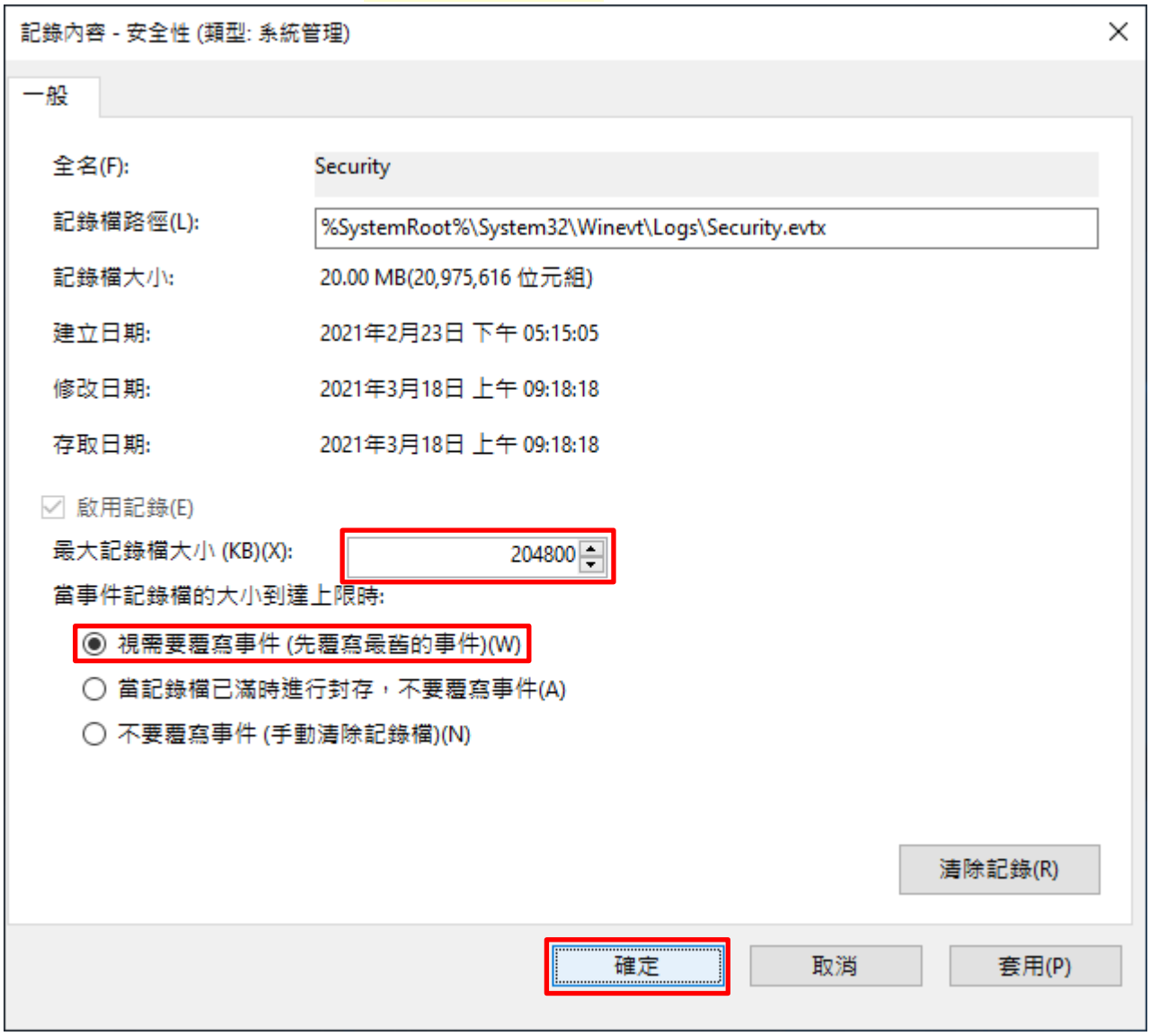
(2) 編輯安全性記錄

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



(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]



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

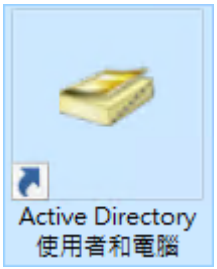
※ 以下分別為網域和工作群組設定方式。

8.1 網域

8.1.1 組織單位設定

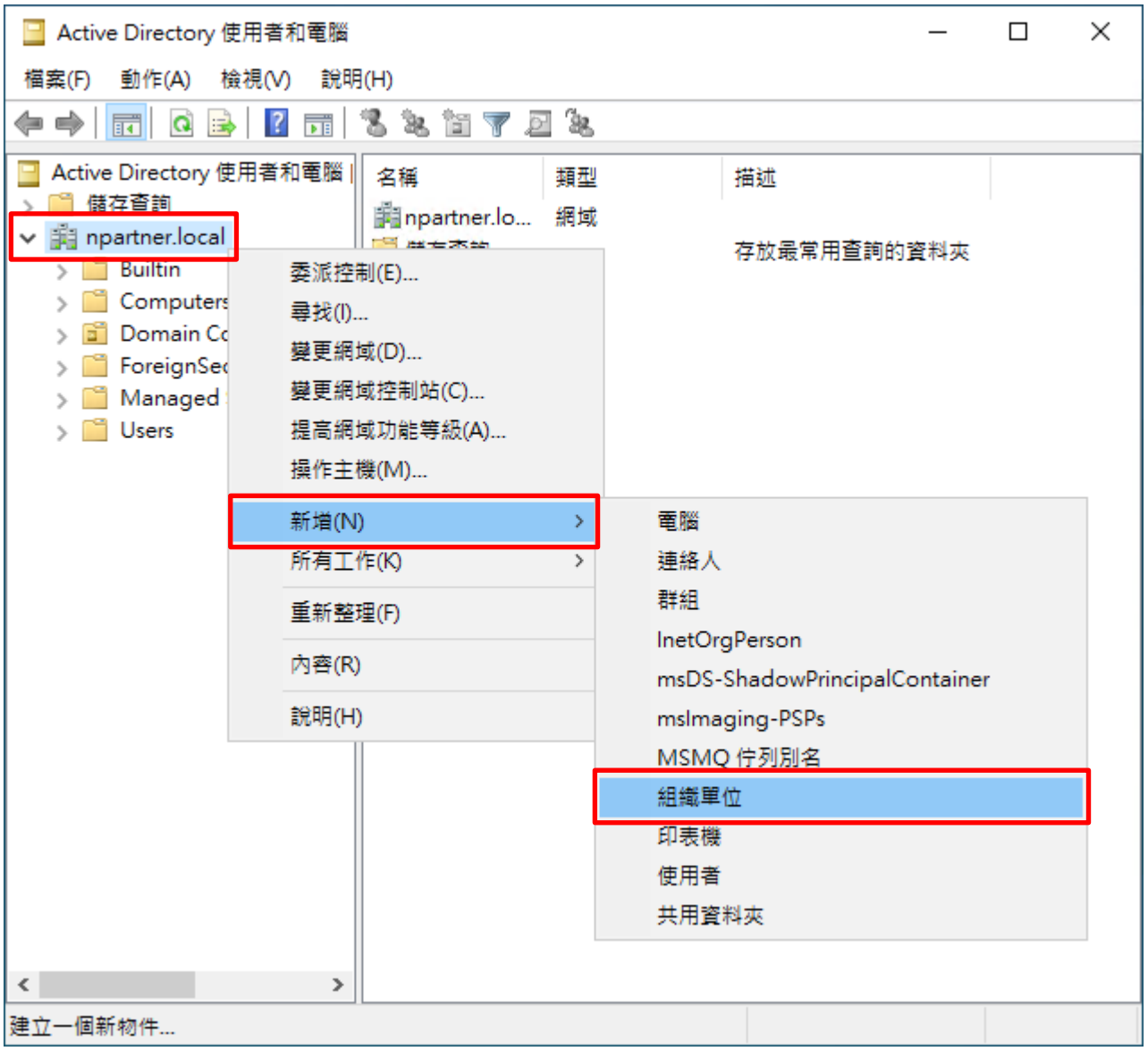
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



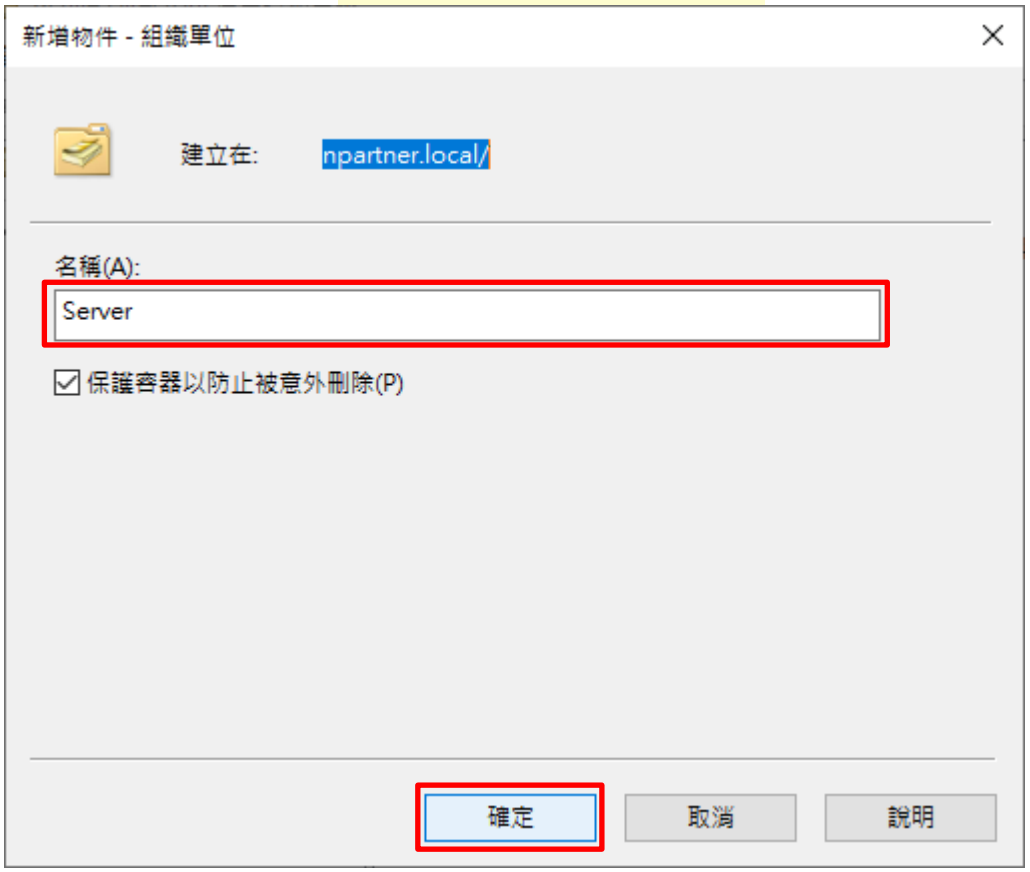
(2) 新增組織單位

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

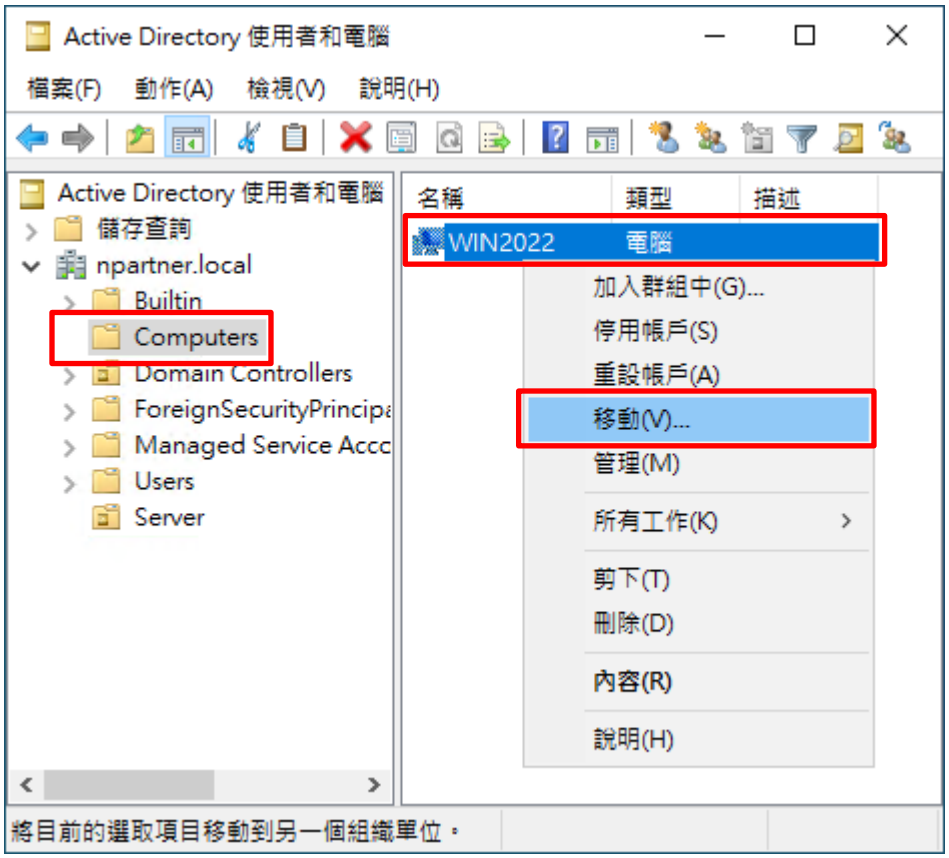
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

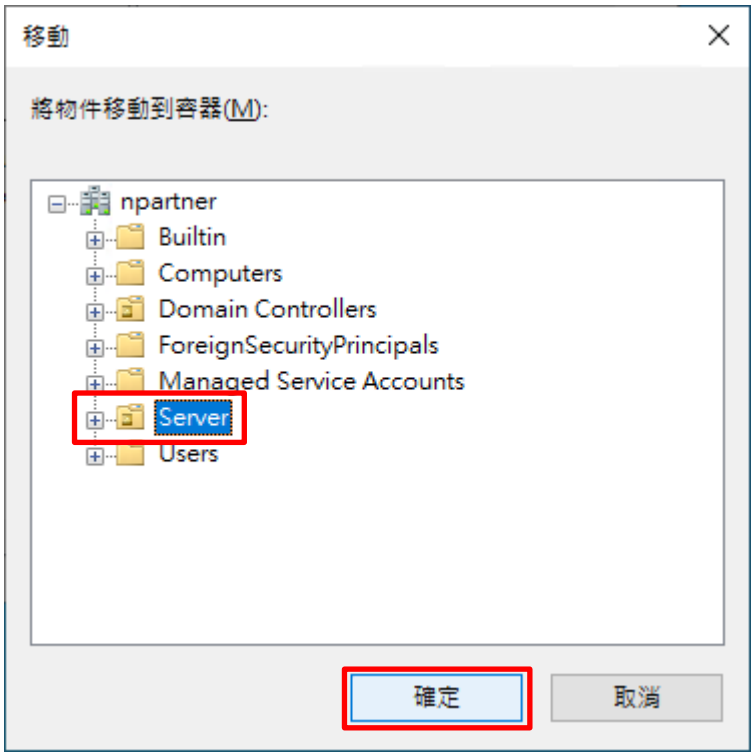
選擇 [Computers] 組織單位 -> 在 [Win2022] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



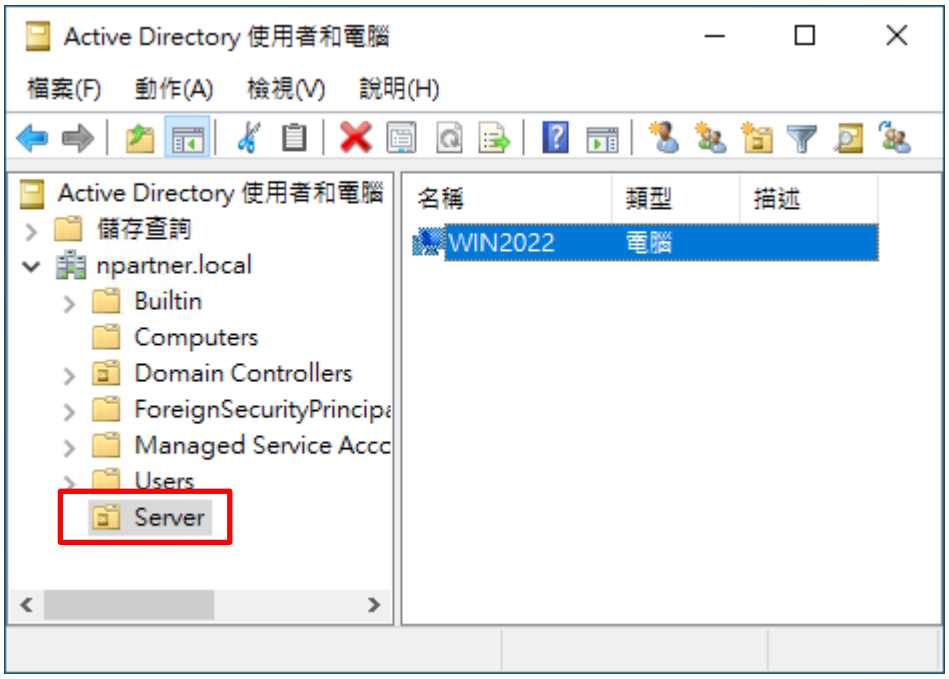
(5) 選擇組織單位

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

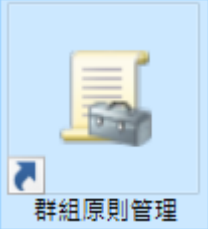
點選 [Servers] 組織單位，確認 Win2022 伺服器已移動。



8.1.2 群組原則設定

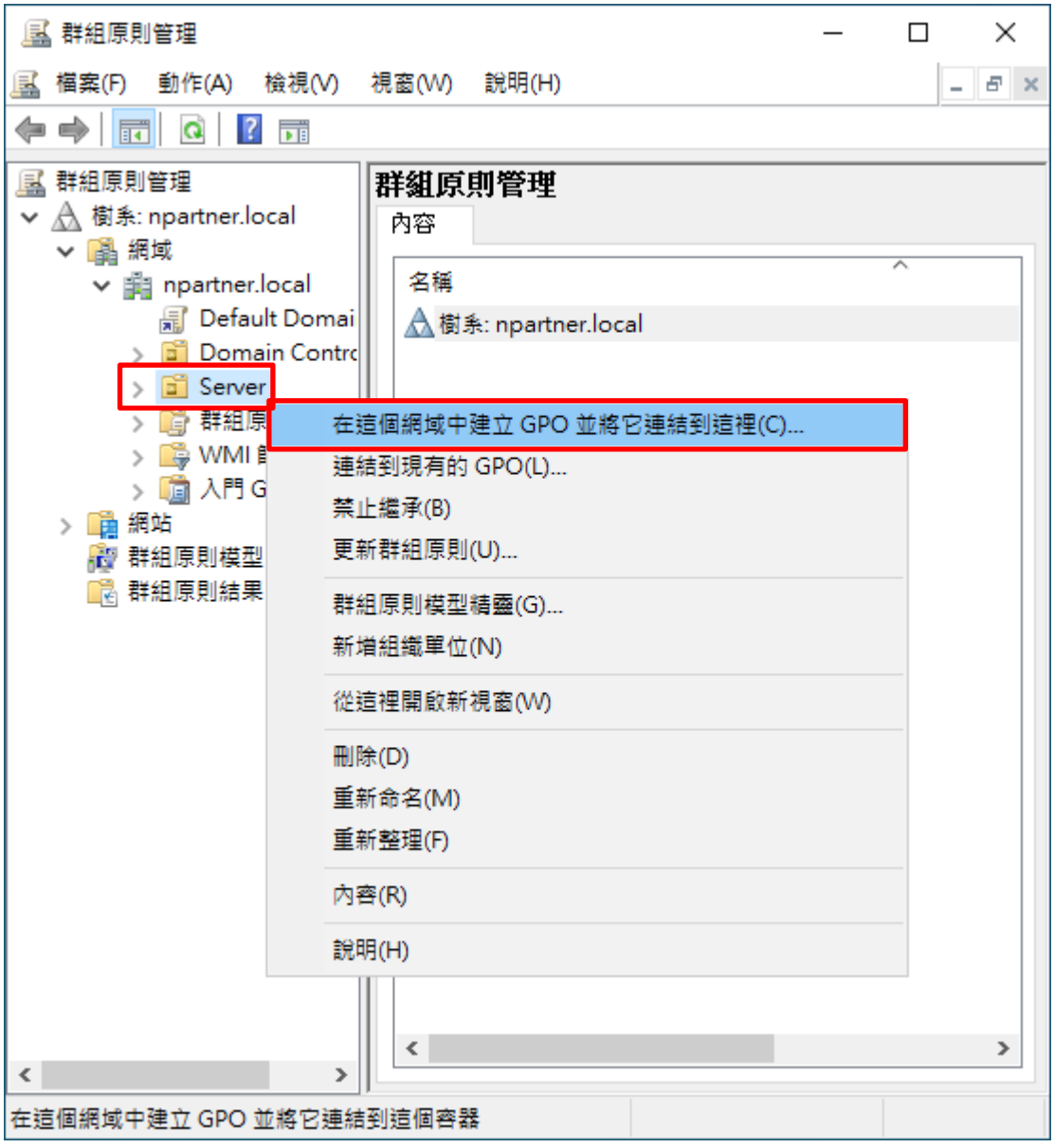
(1) 開啟群組原則管理

開啟 [群組原則管理]



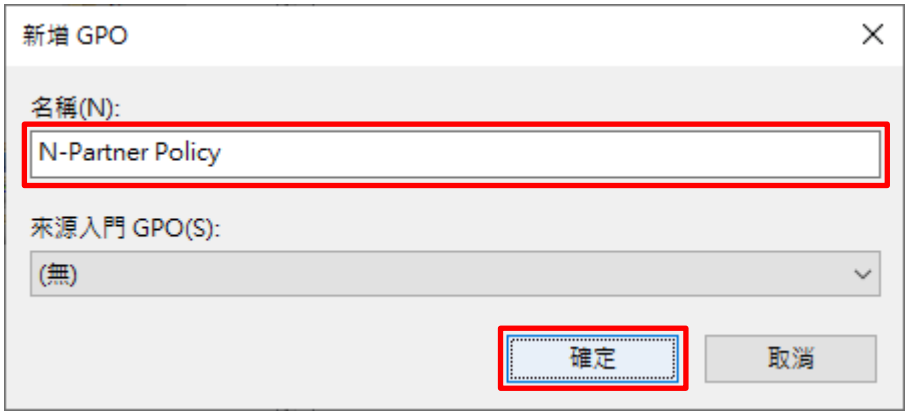
(2) 在 Servers 組織單位，新增群組原則物件

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



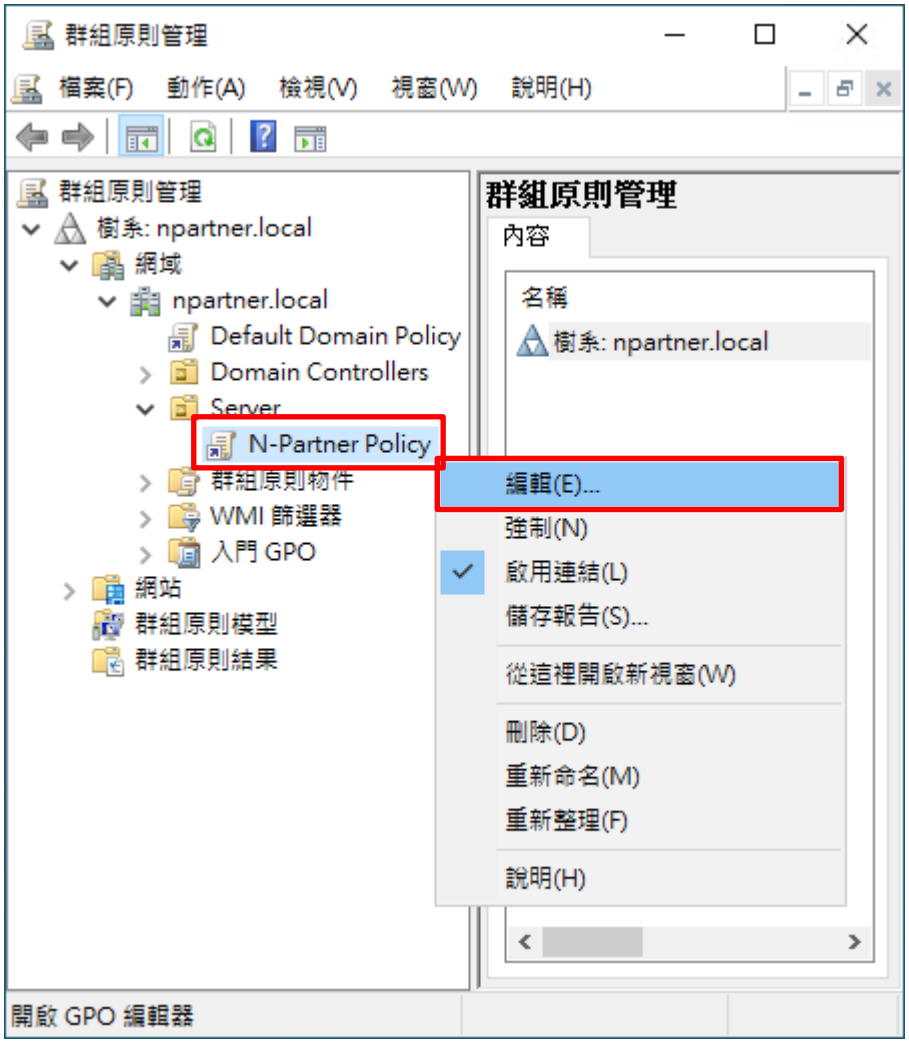
(3) 輸入群組原則物件名稱

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]



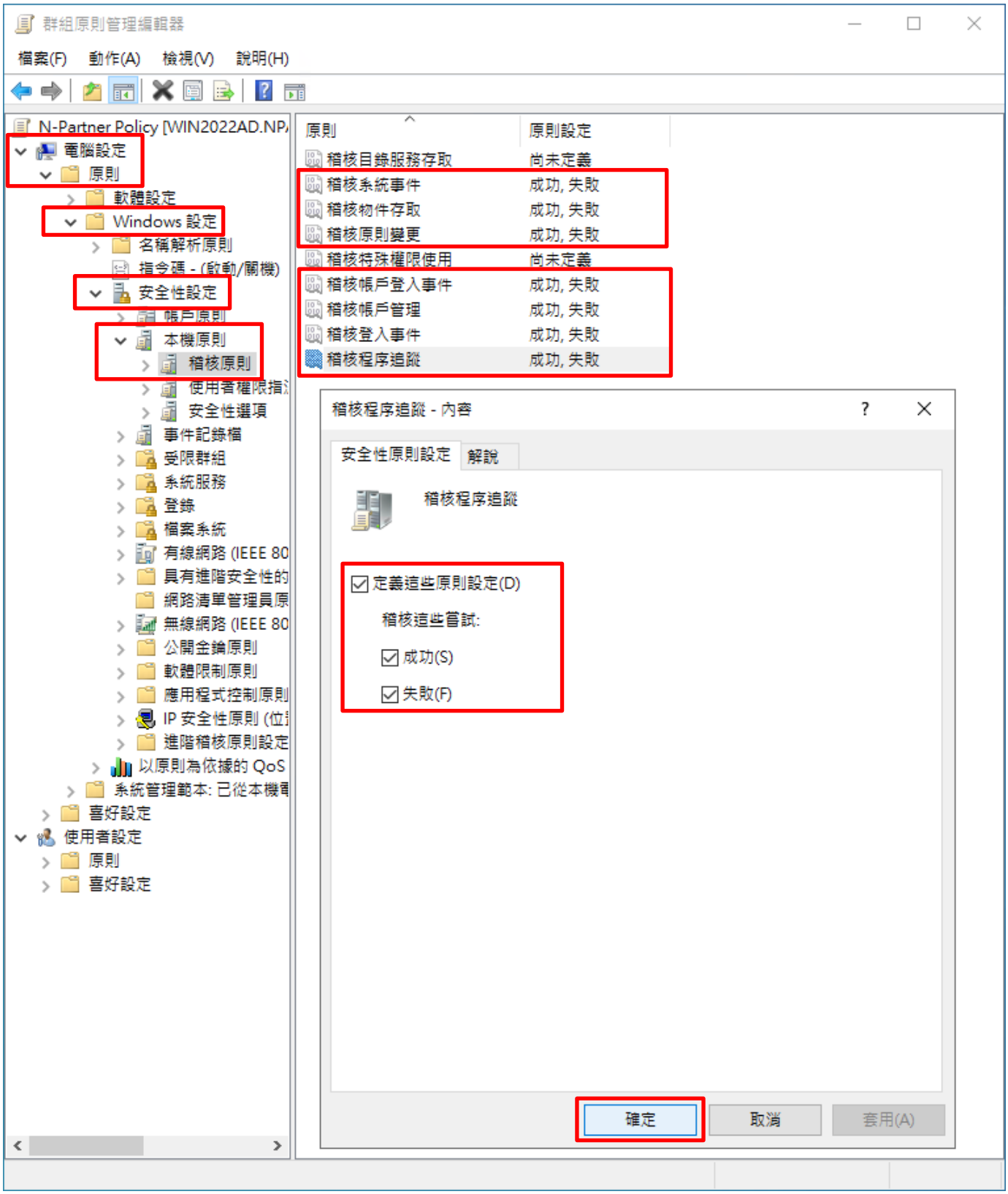
(4) 編輯群組原則物件

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



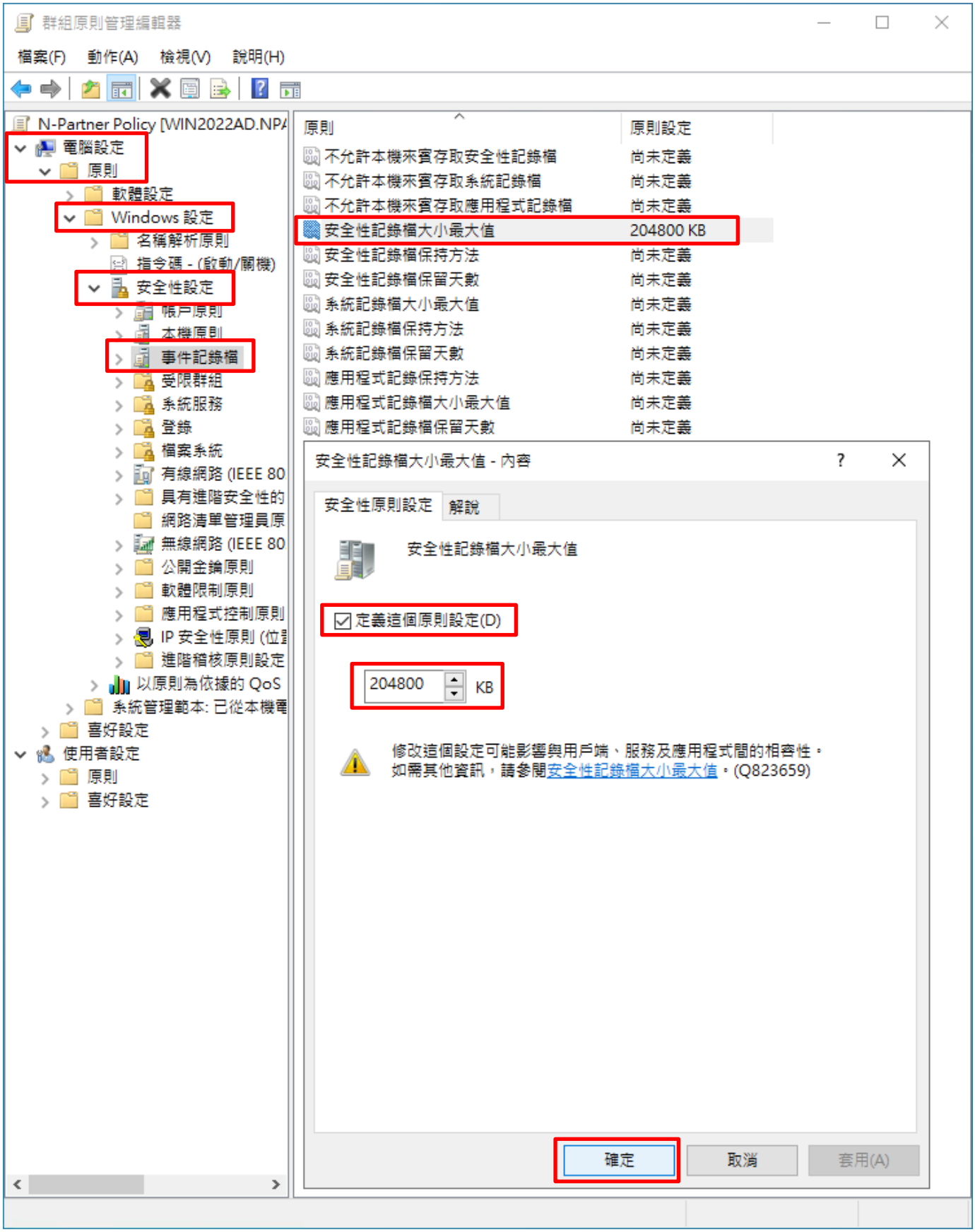
(5) 本機原則：稽核原則

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 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



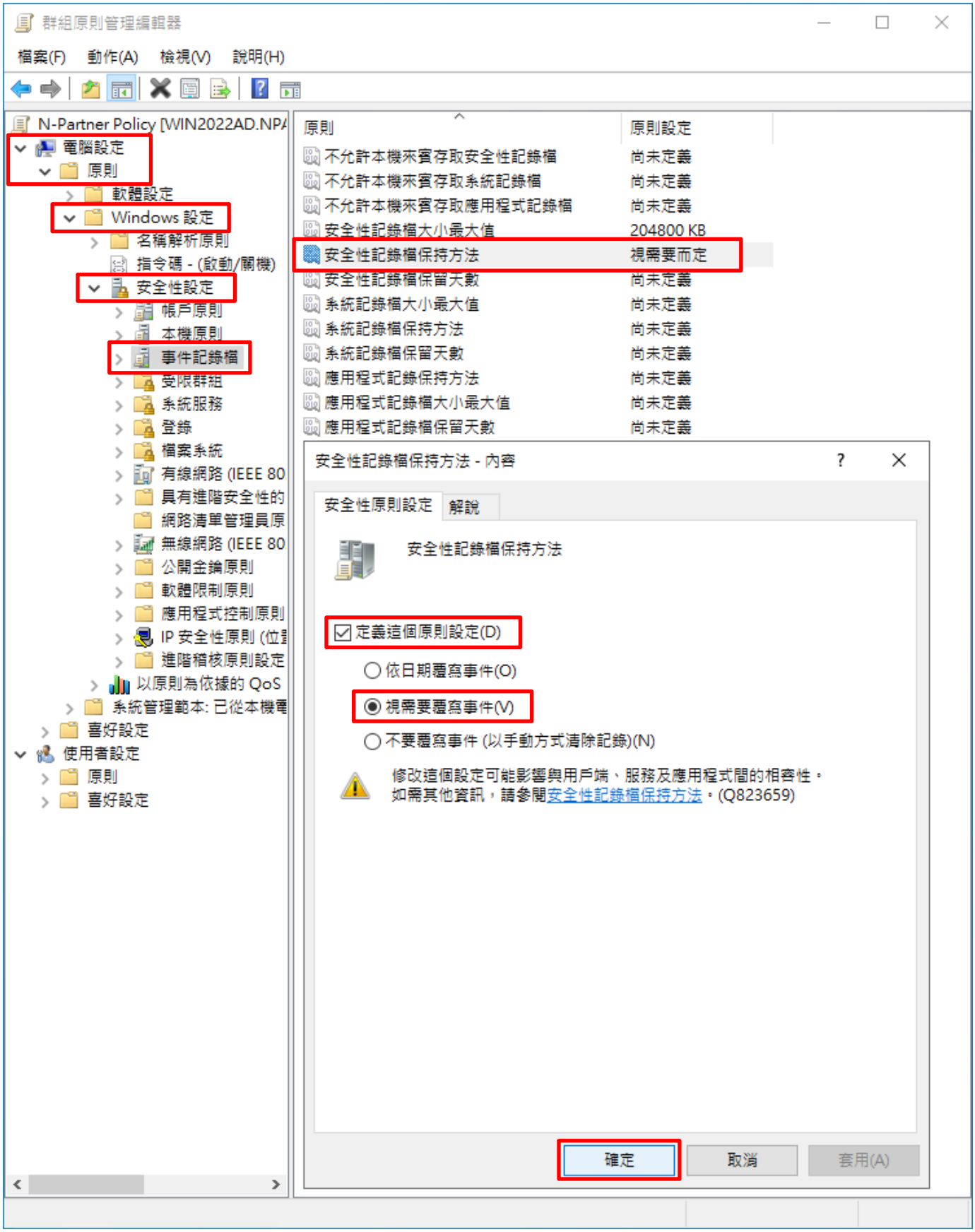
(6) 事件記錄檔：安全性記錄檔大小最大值

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

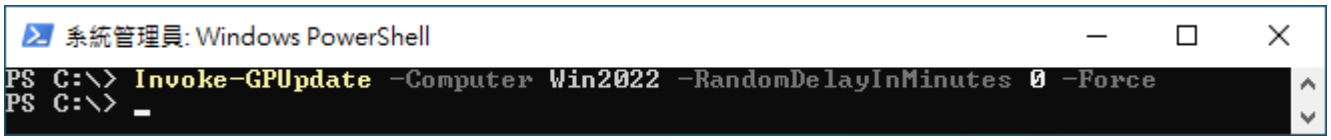
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

(9) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

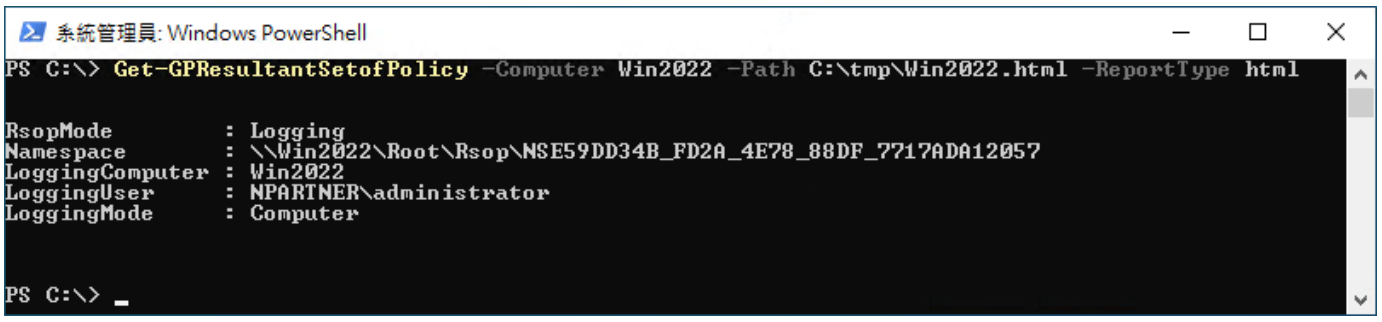
```
PS C:\> Invoke-GPUpdate -Computer Win2022 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱

(10) 在 AD 網域伺服器 -> 產生 Windows Server 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 Server 伺服器名稱和資料夾路徑檔案名稱

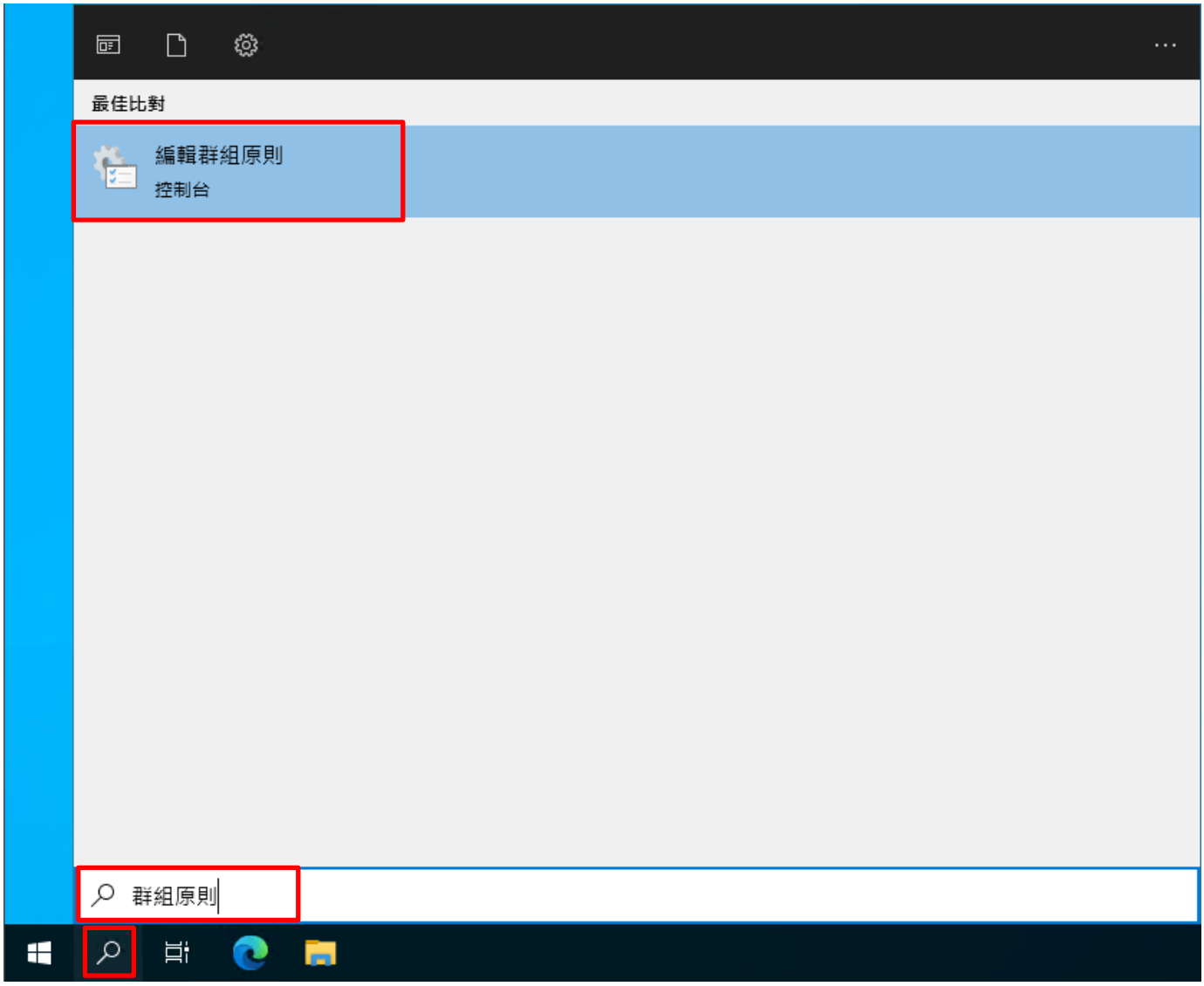
(11) 開啟報表 -> 確認 Windows Server 伺服器 -> 套用 N-Partner Policy 群組原則

8.2 工作群組

8.2.1 稽核原則設定

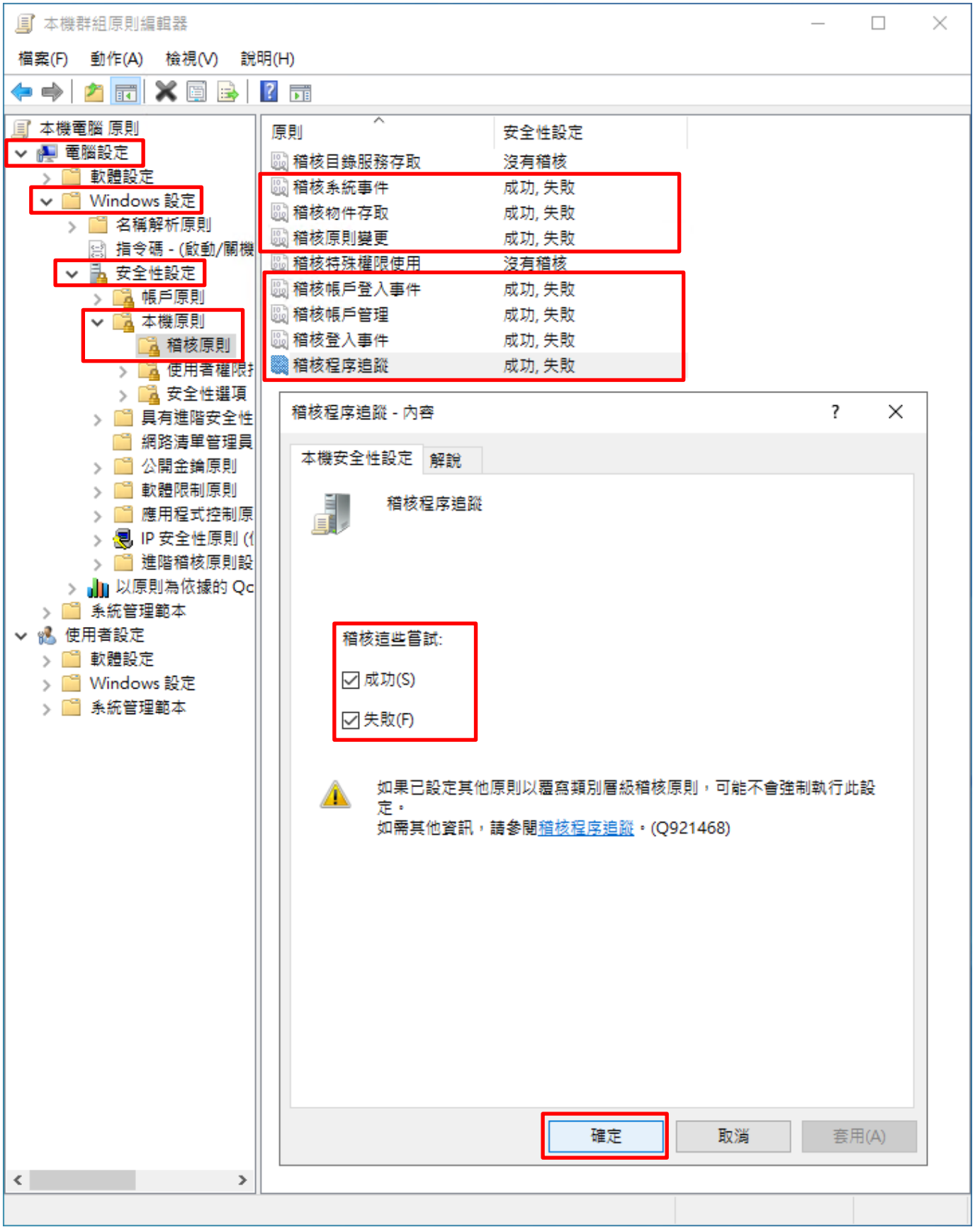
(1) 開啟本機群組原則編輯器

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

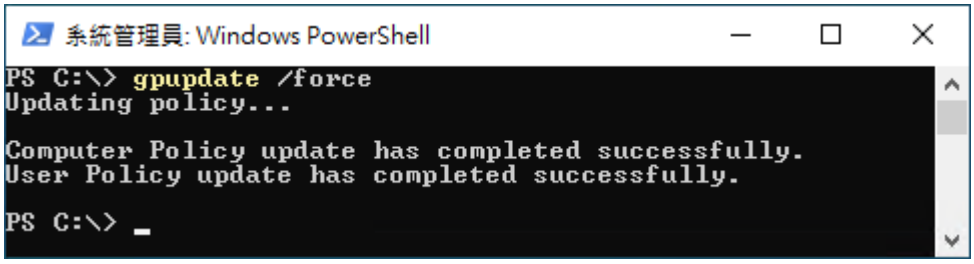
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核原則變更], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

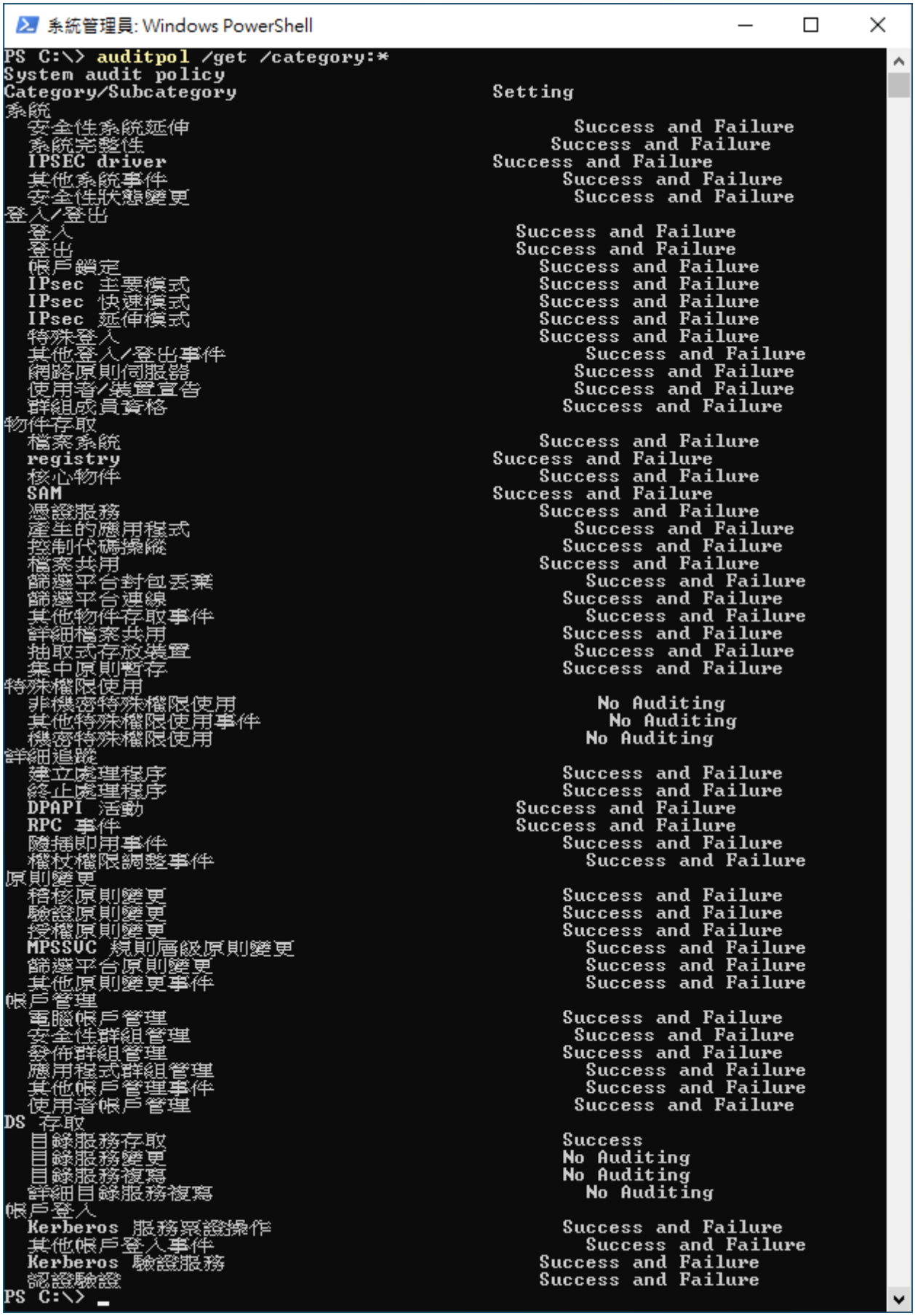
(4) 更新群組原則

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



(5) 查看群組原則套用情形

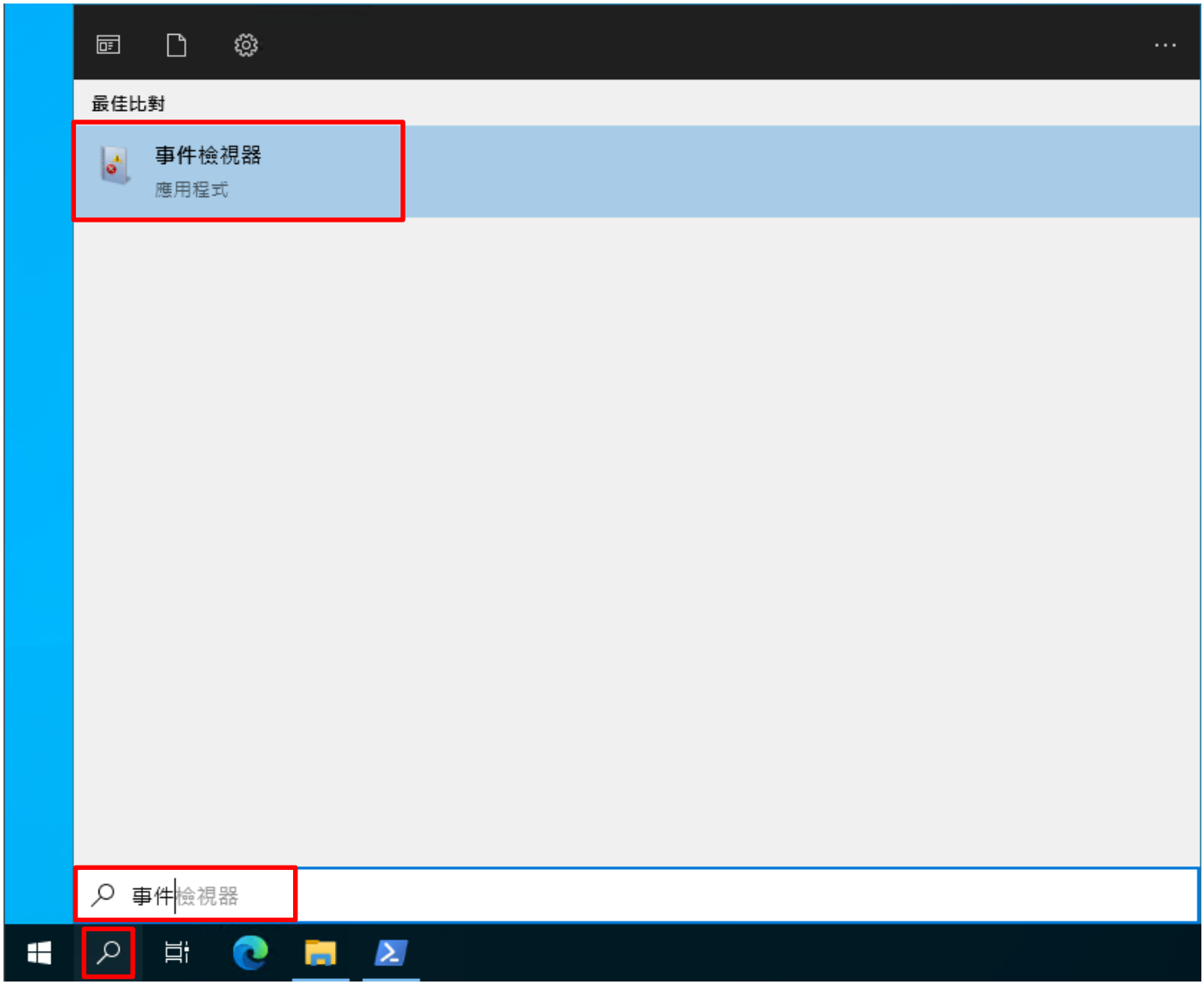
```
PS C: \> auditpol /get /category:*
```



8.2.2 事件檔案設定

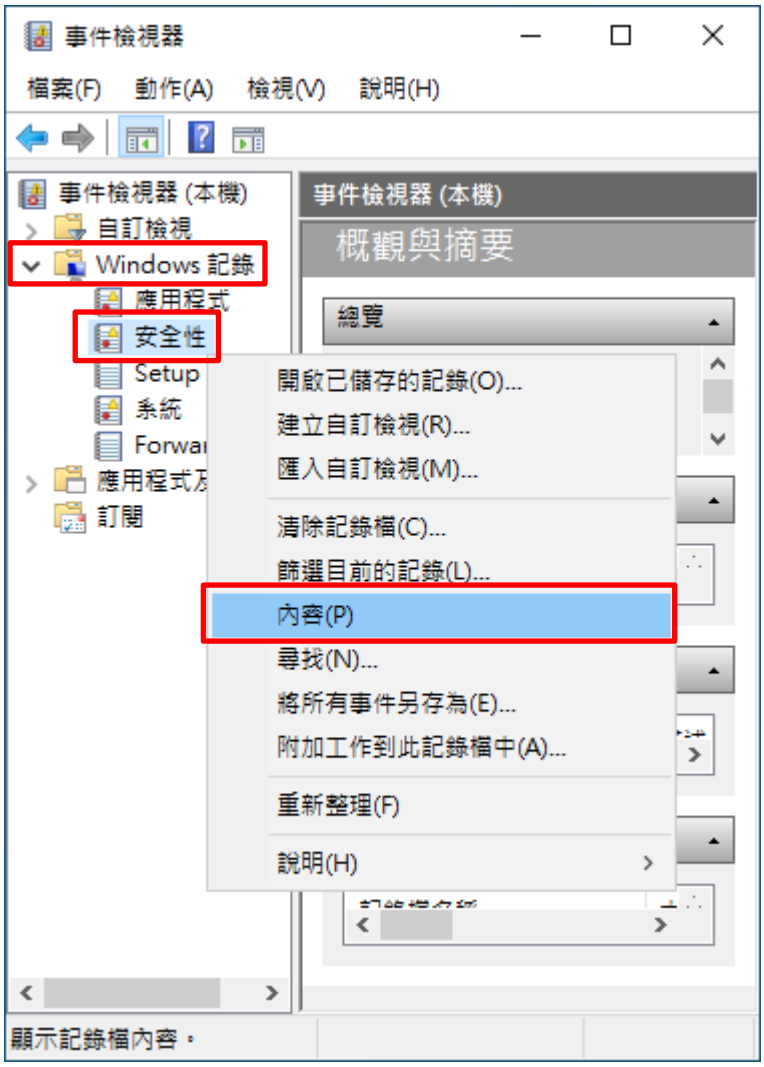
(1) 開啟 [事件檢視器]

點選  [搜尋] -> 輸入事件 -> 點選 [事件檢視器]



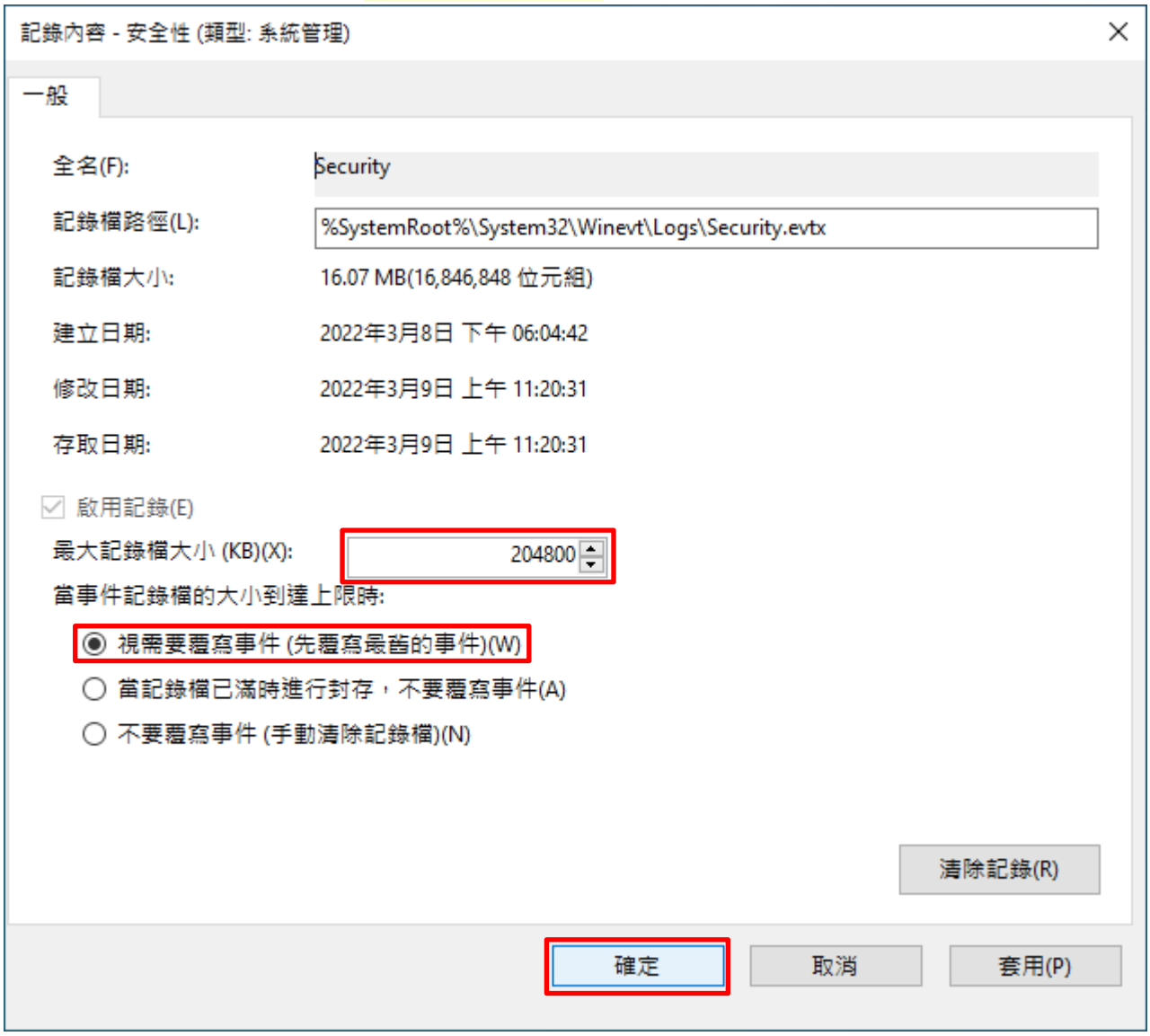
(2) 編輯安全性記錄

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



(4) 設定安全性記錄檔

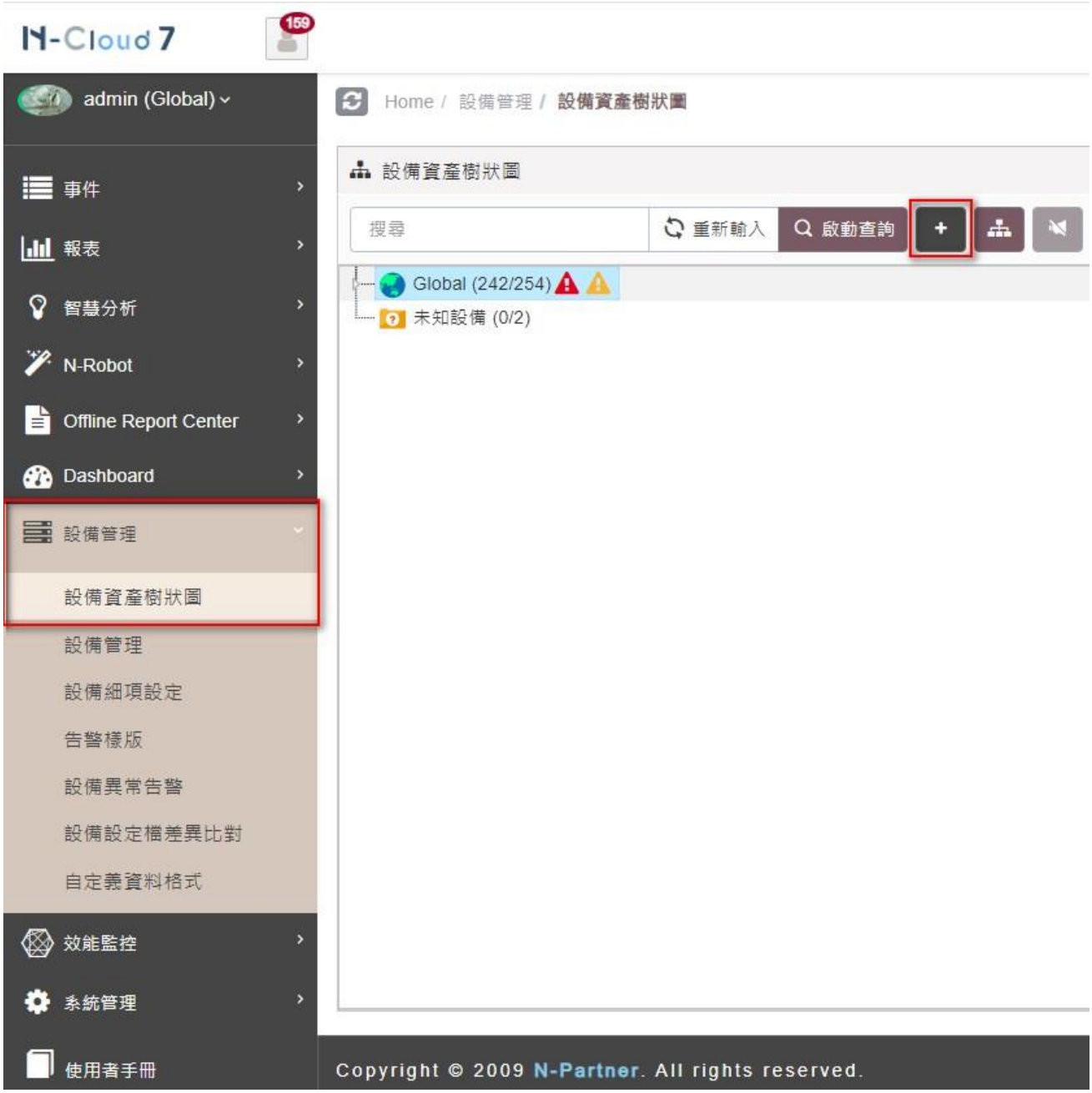
輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]



9. N-Reporter

(1) 新增 Windows Server 設備

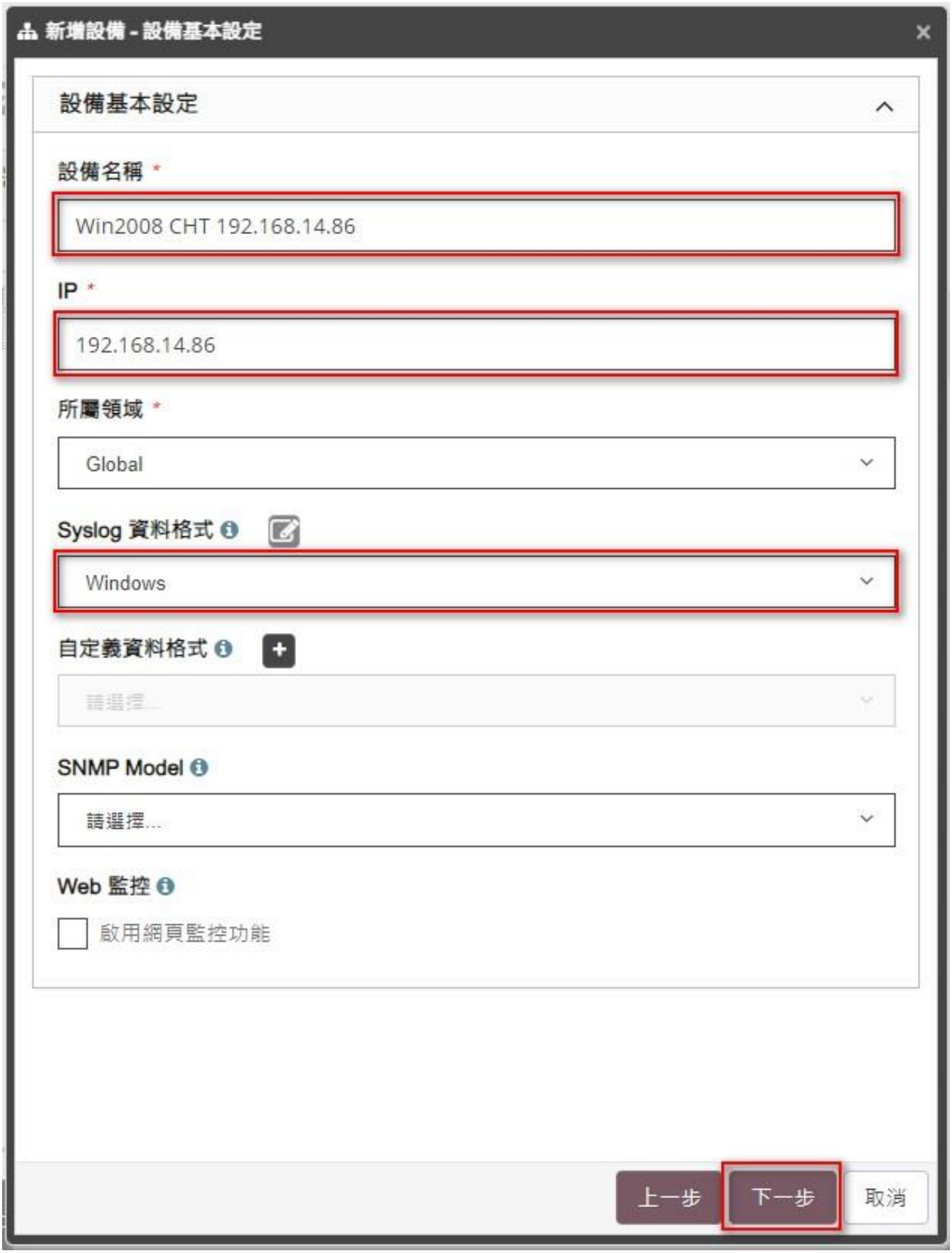
[設備管理] -> [設備資產樹狀圖] -> 點選 [新增] .



(2) 設定 Windows Server 設備的資料格式

左點[Application / DB / OS / Server],左點[引導模式] .

輸入設備名稱和 IP. Syslog Data Type 選擇 Windows or Windows (Raw).左點[下一步] .



左點[下一步].

編碼方式 選擇 [UTF-8],左點[下一步] .

註：Windows2000、WindowsXP、Windows2003 繁體版 編碼方式 請選擇 BIG5 .

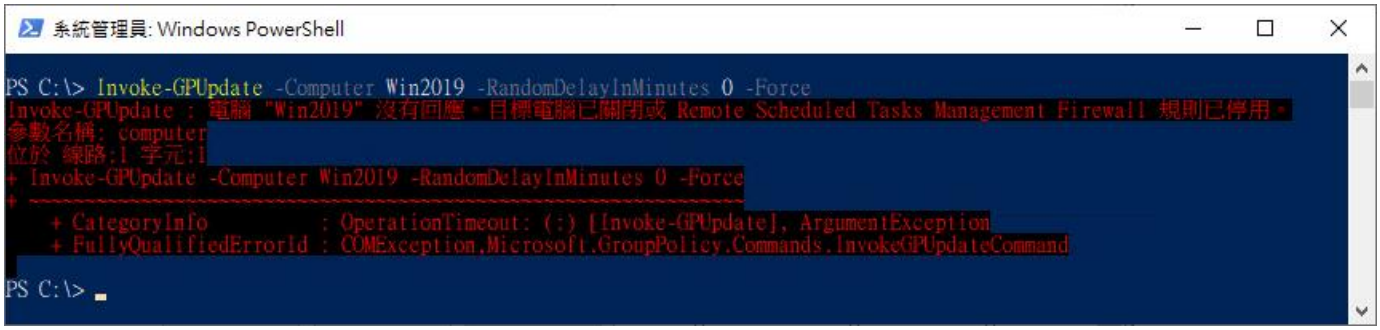
左點[下一步].

左點[下一步].

10. 問題排除

10.1 Invoke-GPUpdate 錯誤

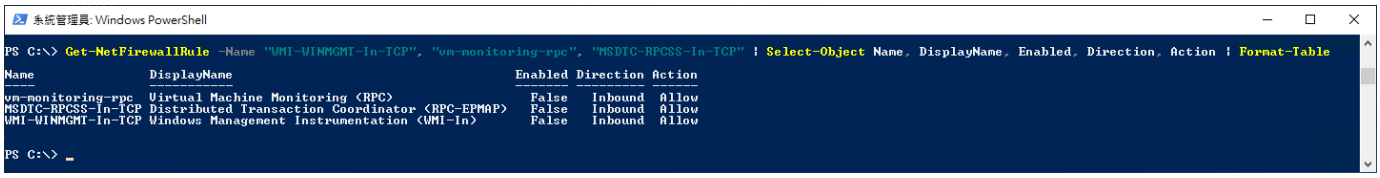
(1) 在 AD 網域伺服器 -> 執行 Invoke-GPUpdate 更新 Windows Server 群組原則出現錯誤訊息



(2) 在 Windows Server 開啟 [Windows PowerShell]

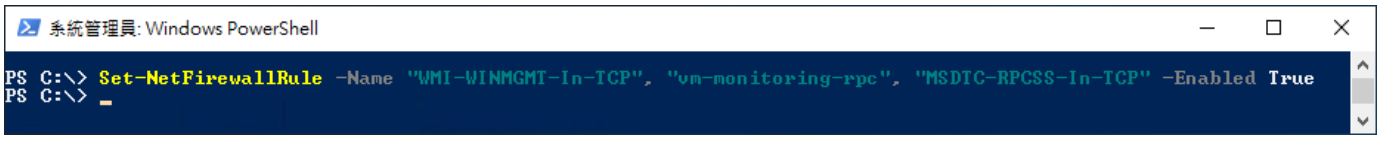
(3) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
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
```



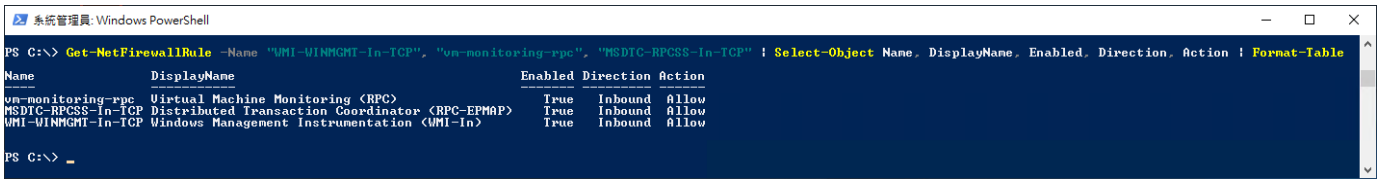
(4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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



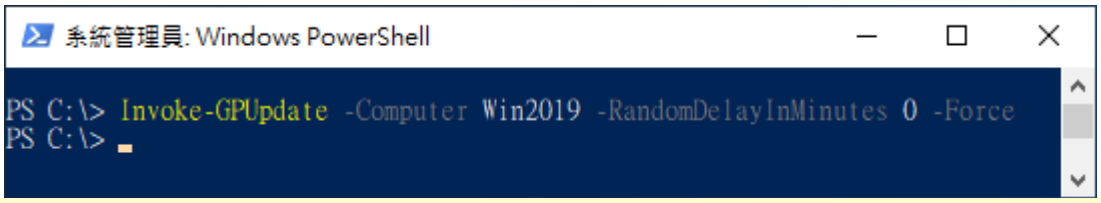
(5) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

```
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 Server 群組原則

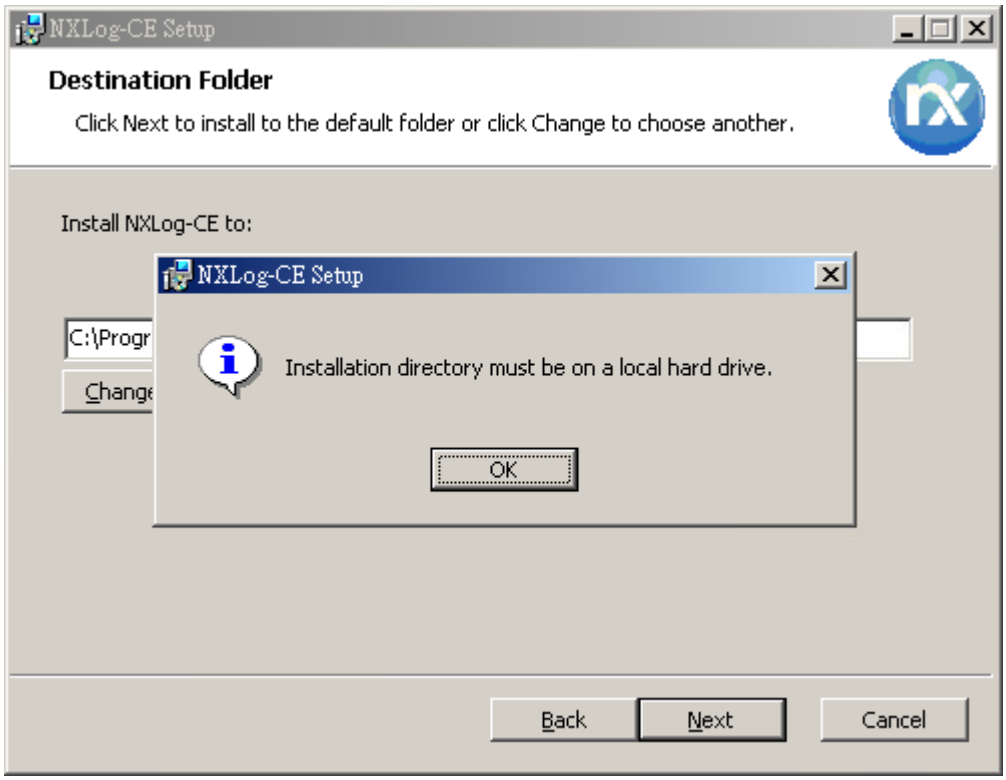
```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 Windows Server 伺服器名稱

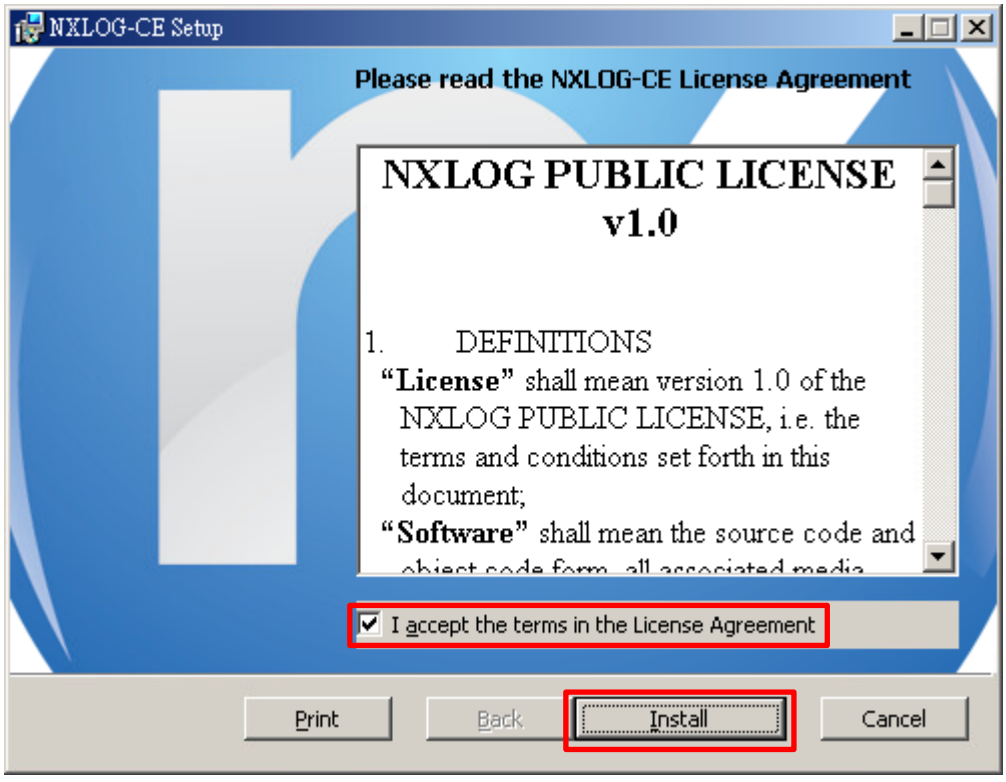
10.2 NXLog 安裝問題

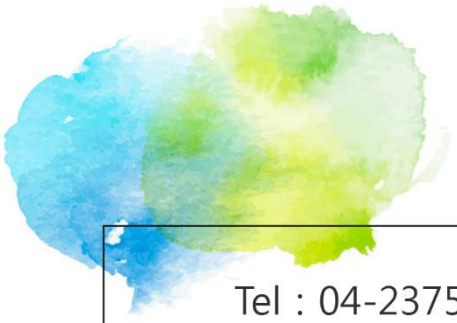
(1) 安裝 NXLog(2.10.2150) 顯示 Installation directory must be on a local hard drive.



(2) 安裝 NXLog 之前版本

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





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