

# Partner

如何設定

Windows Server 事件記錄

V014

2024/04/17



## 版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

## 商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

# 目錄

## 前言 2

## 1. NXLog ..... 3

### 1.1 NXLog 安裝 ..... 3

### 1.2 NXLog 設定檔下載 ..... 8

#### 1.2.1 Windows 2003 或之前版本作業系統 ..... 8

##### 1.2.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄 ..... 8

##### 1.2.1.2 輸出全部事件記錄 ..... 9

#### 1.2.2 Windows 2008 或之後版本作業系統 ..... 10

##### 1.2.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄 ..... 10

##### 1.2.2.2 輸出應用程式、安全性、系統全部事件記錄 ..... 11

### 1.3 NXLog 設定檔 ..... 12

#### 1.3.1 Windows 2003 或之前版本作業系統 ..... 12

##### 1.3.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄 ..... 12

##### 1.3.1.2 輸出全部事件記錄 ..... 13

#### 1.3.2 Windows 2008 或之後版本作業系統 ..... 14

##### 1.3.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄 ..... 14

##### 1.3.2.2 輸出應用程式、安全性、系統全部事件記錄 ..... 15

### 1.4 NXLog 啟動服務 ..... 16

#### 1.4.1 Windows 2003 或之前版本作業系統 ..... 16

#### 1.4.2 Windows 2008 或之後版本作業系統 ..... 19

## 2. Windows 2000 ..... 22

### 2.1 網域 ..... 22

#### 2.1.1 組織單位設定 ..... 22

#### 2.1.2 群組原則設定 ..... 25

### 2.2 工作群組 ..... 32

#### 2.2.1 稽核原則設定 ..... 32

#### 2.2.2 事件檔案設定 ..... 36

## 3. Windows 2003 ..... 39

### 3.1 網域 ..... 39

#### 3.1.1 組織單位設定 ..... 39

#### 3.1.2 群組原則設定 ..... 43

### 3.2 工作群組 ..... 51

#### 3.2.1 稽核原則設定 ..... 51

#### 3.2.2 事件檔案設定 ..... 55

## 4. Windows 2008 ..... 58

### 4.1 網域 ..... 58

#### 4.1.1 組織單位設定 ..... 58

#### 4.1.2 群組原則設定 ..... 61

### 4.2 工作群組 ..... 68

#### 4.2.1 稽核原則設定 ..... 68

#### 4.2.2 事件檔案設定 ..... 72

## 5. Windows 2012 ..... 75

### 5.1 網域 ..... 75

#### 5.1.1 組織單位設定 ..... 75

#### 5.1.2 群組原則設定 ..... 80

### 5.2 工作群組 ..... 87

#### 5.2.1 稽核原則設定 ..... 87

#### 5.2.2 事件檔案設定 ..... 91

## 6. Windows 2016 ..... 94

### 6.1 網域 ..... 94

#### 6.1.1 組織單位設定 ..... 94

#### 6.1.2 群組原則設定 ..... 99

### 6.2 工作群組 ..... 106

#### 6.2.1 稽核原則設定 ..... 106

#### 6.2.2 事件檔案設定 ..... 110

## 7. Windows 2019 ..... 113

### 7.1 網域 ..... 113

#### 7.1.1 組織單位設定 ..... 113

#### 7.1.2 群組原則設定 ..... 118

### 7.2 工作群組 ..... 125

#### 7.2.1 稽核原則設定 ..... 125

#### 7.2.2 事件檔案設定 ..... 129

## 8. Windows 2022 ..... 132

### 8.1 網域 ..... 132

#### 8.1.1 組織單位設定 ..... 132

#### 8.1.2 群組原則設定 ..... 137

### 8.2 工作群組 ..... 144

#### 8.2.1 稽核原則設定 ..... 144

#### 8.2.2 事件檔案設定 ..... 148

## 9. N-Reporter ..... 151

## 10. 問題排除 ..... 158

### 10.1 Invoke-GPUdate 錯誤 ..... 158

### 10.2 NXLog 安裝問題 ..... 160

## 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



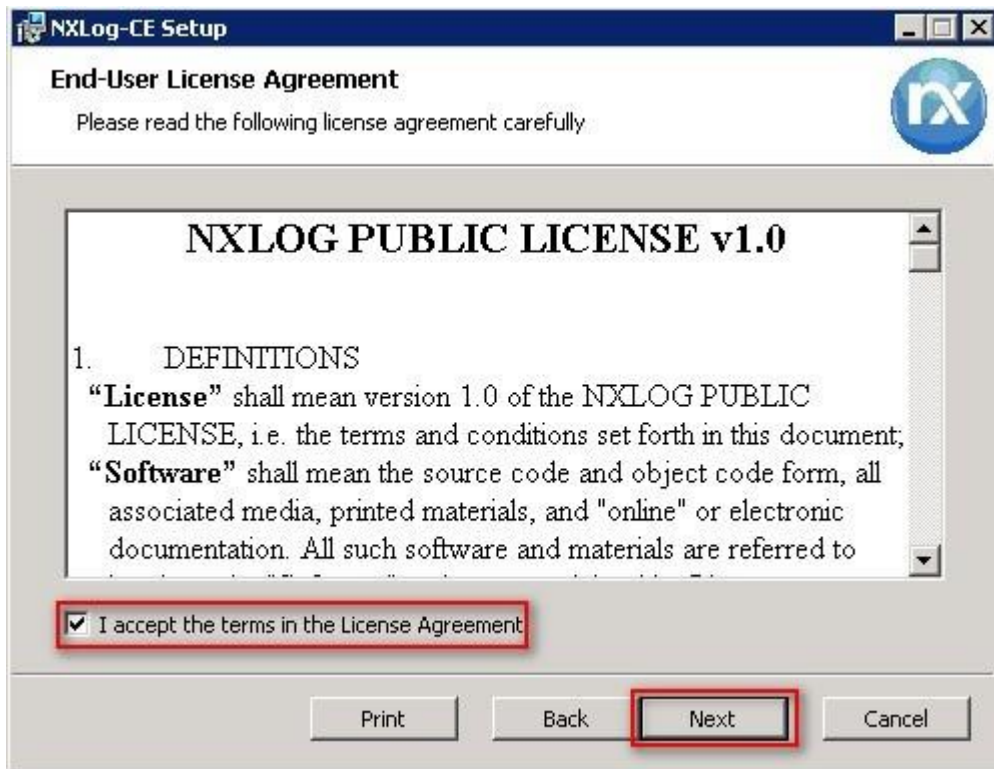
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

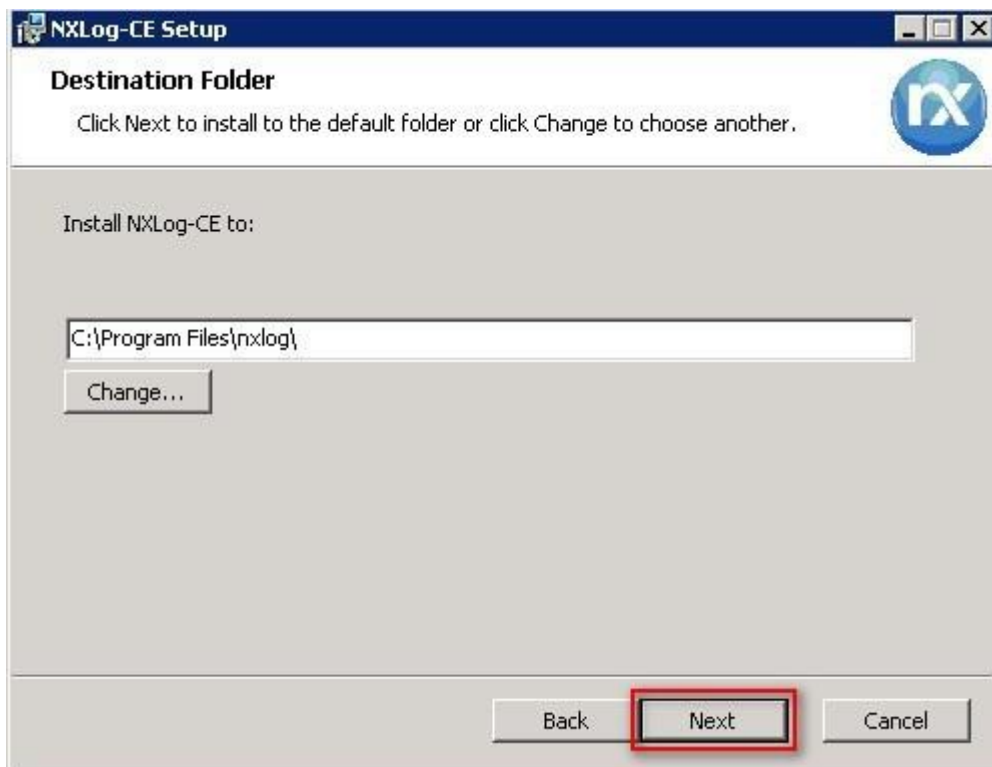
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



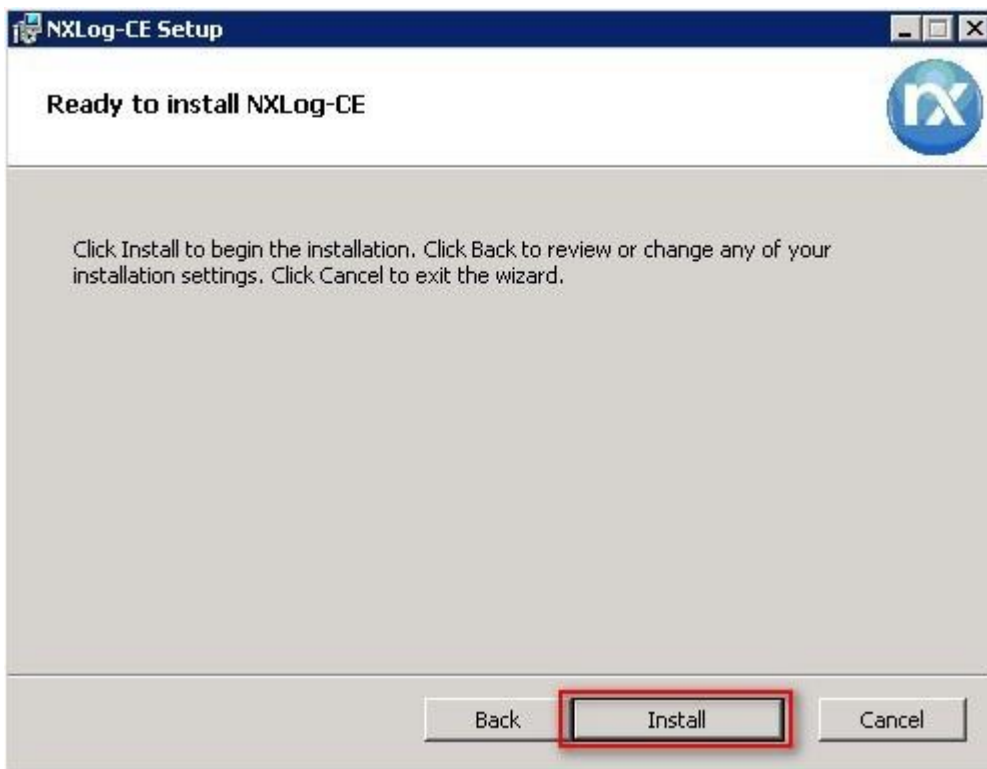
-> 勾选 [I accept the terms in the License Agreement],按 [Next] .



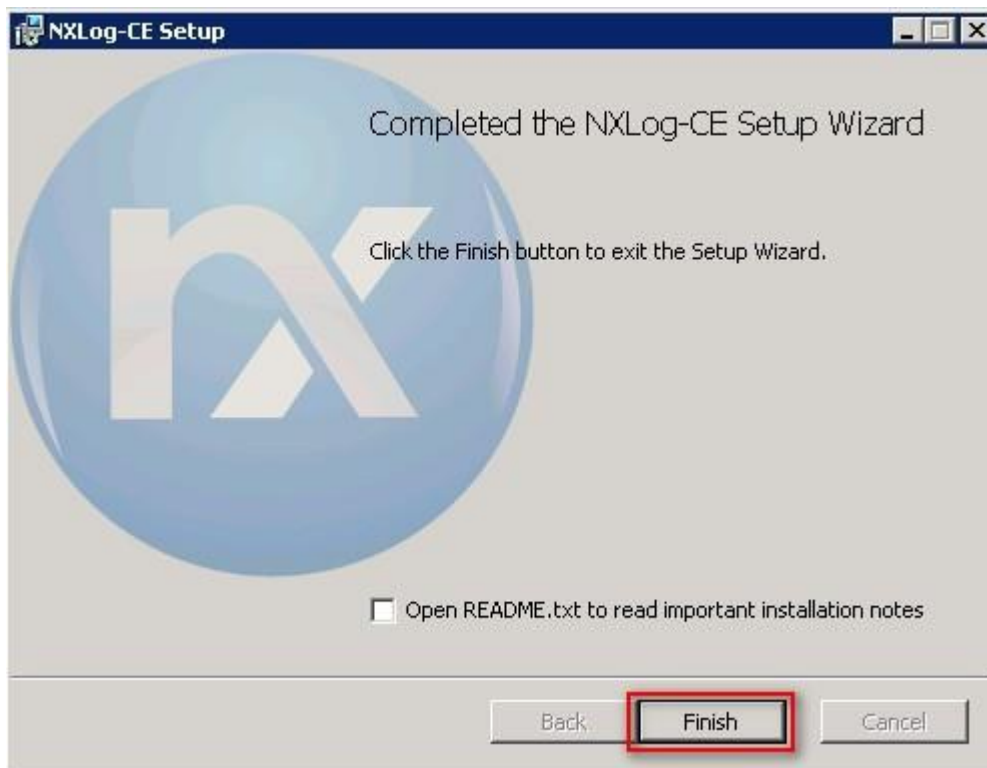
-> 按 [Next].



-> 按 [Install]

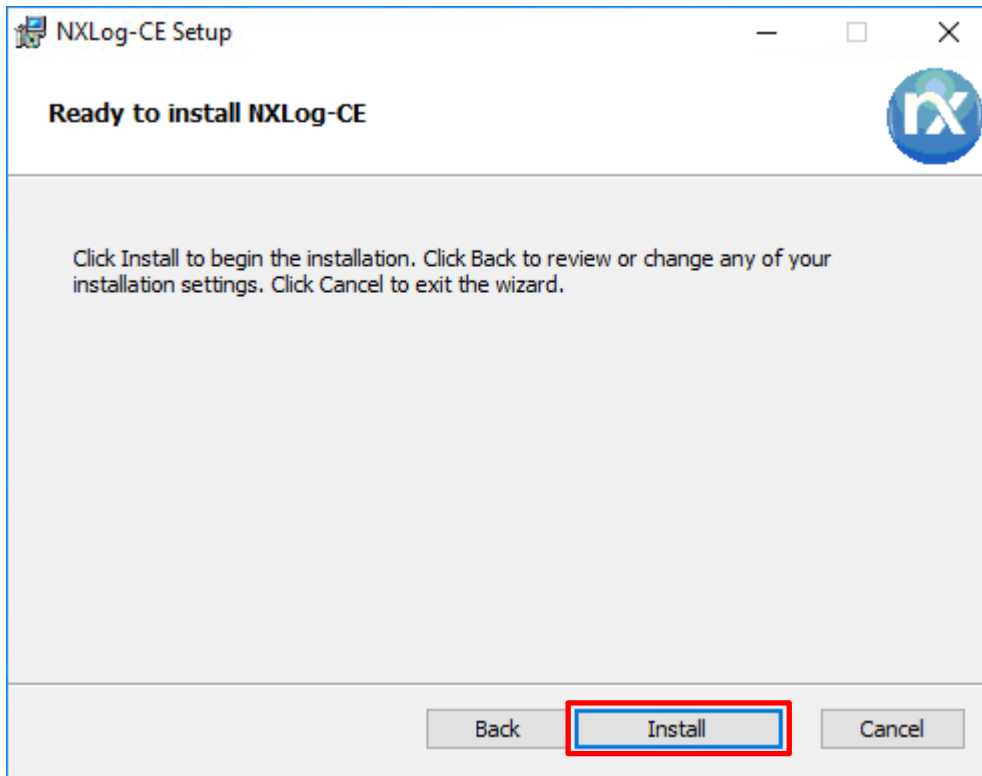


-> 按 [Finish].



<2.2> Windows 2003

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

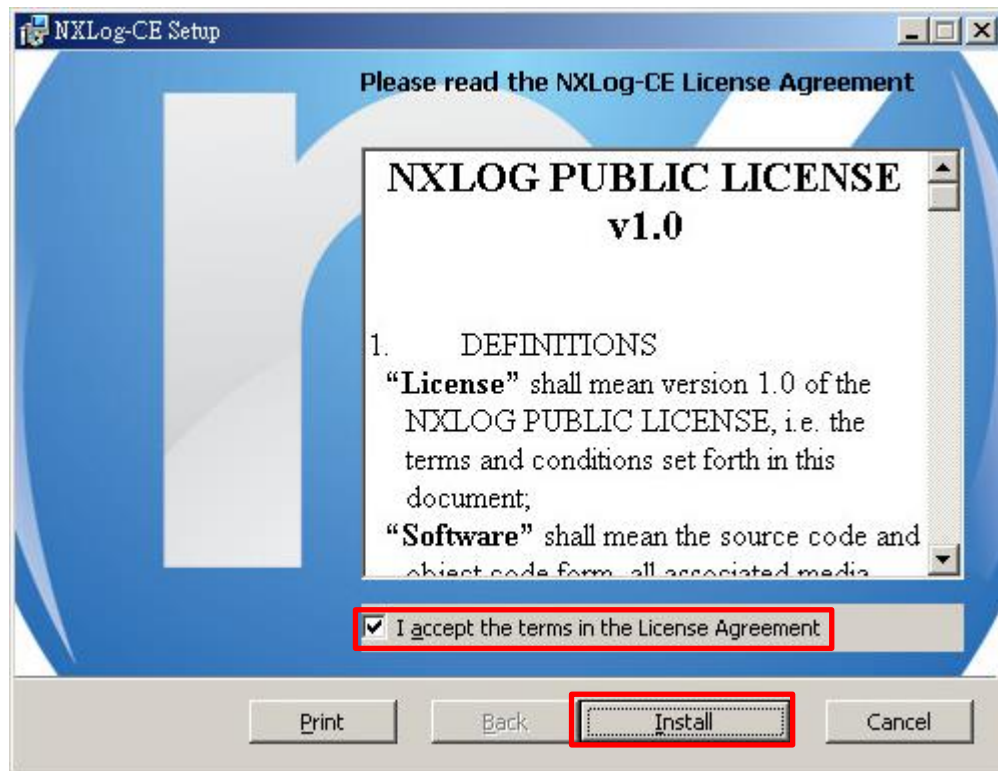




### <2.3> Windows 2000

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

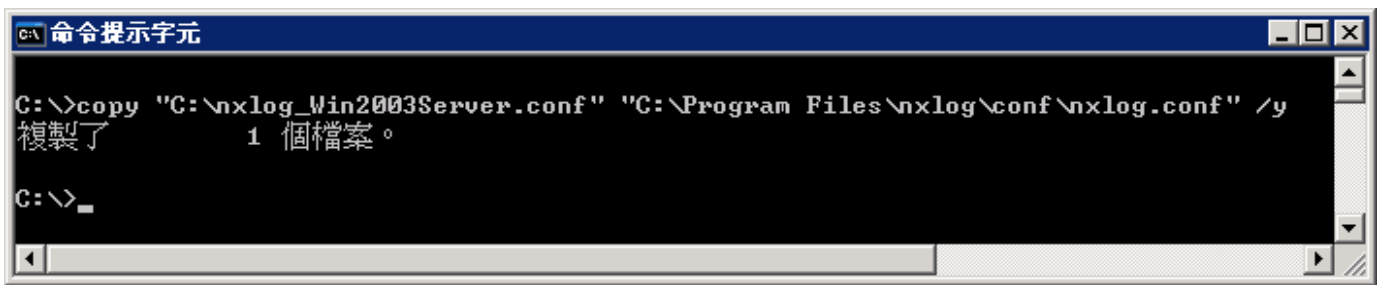
(1) 開啟 [命令提示字元]



(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](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

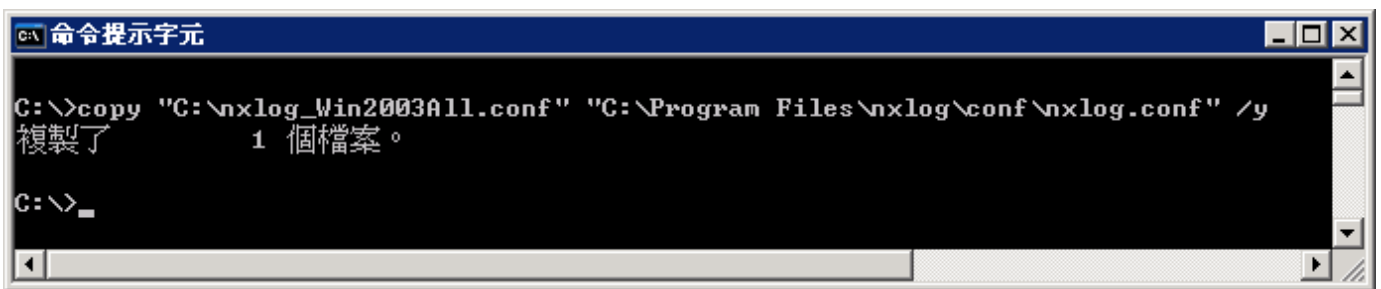
(1) 開啟 [命令提示字元]



(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](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](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](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 $SyslogFacility/Value = 17;
  Exec $Message = string($SourceName) + "-" + string($EventID) + "-" + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverity/Value = 3; } \
    else if ($EventType == 'WARNING') { $SyslogSeverity/Value = 4; } \
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverity/Value = 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"
```



```
C:\> net start nxlog  
nxlog 服務正在啟動。  
nxlog 服務已經啟動成功。  
  
C:\> type "C:\Program Files\nxlog\data\nxlog.log"  
2024-04-17 13:41:41 INFO nxlog-ce-3.2.2329 started  
  
C:\> _
```

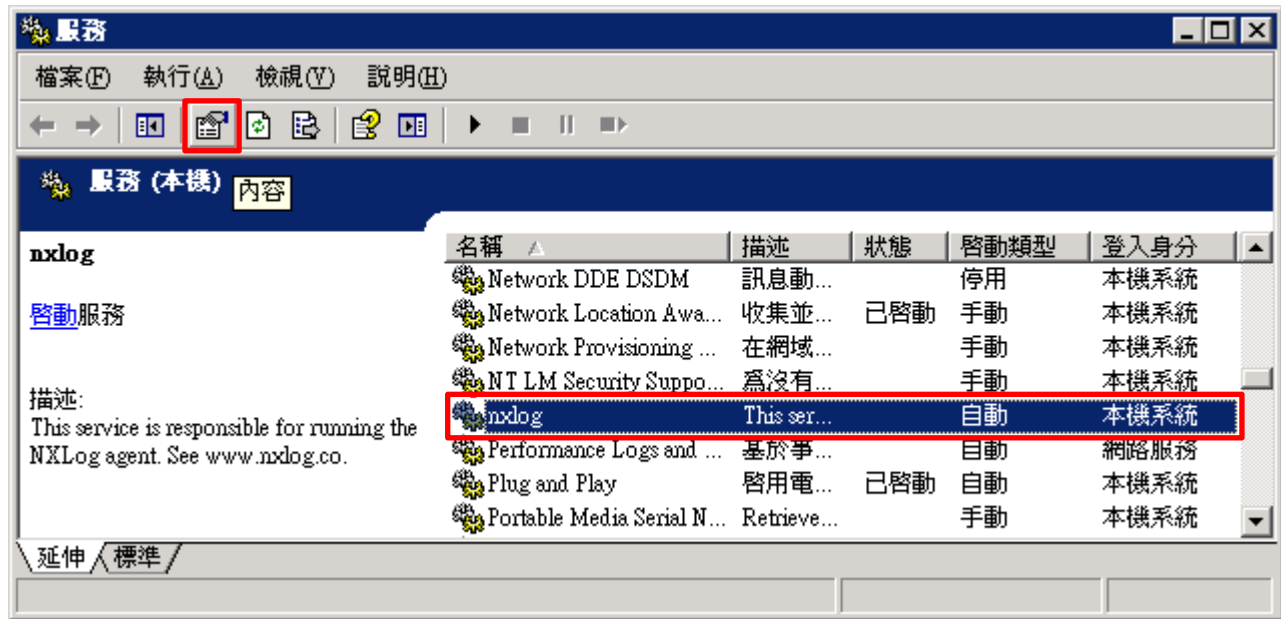
(3) 開啟 [服務] 功能

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

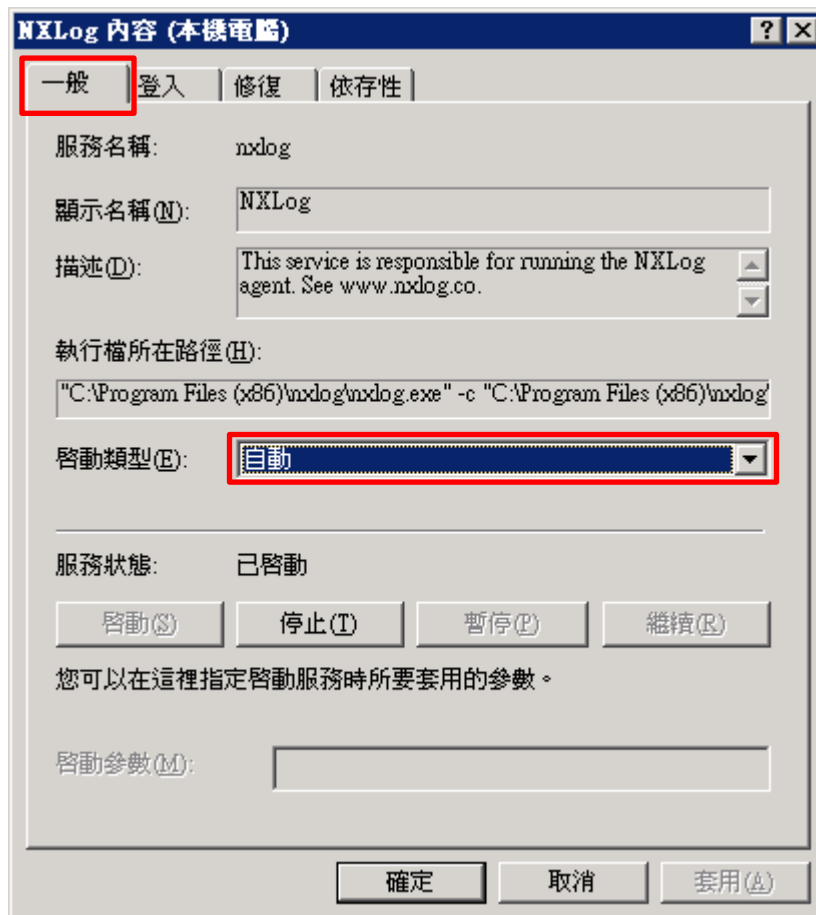


(4) 開啟 NXLog 服務內容

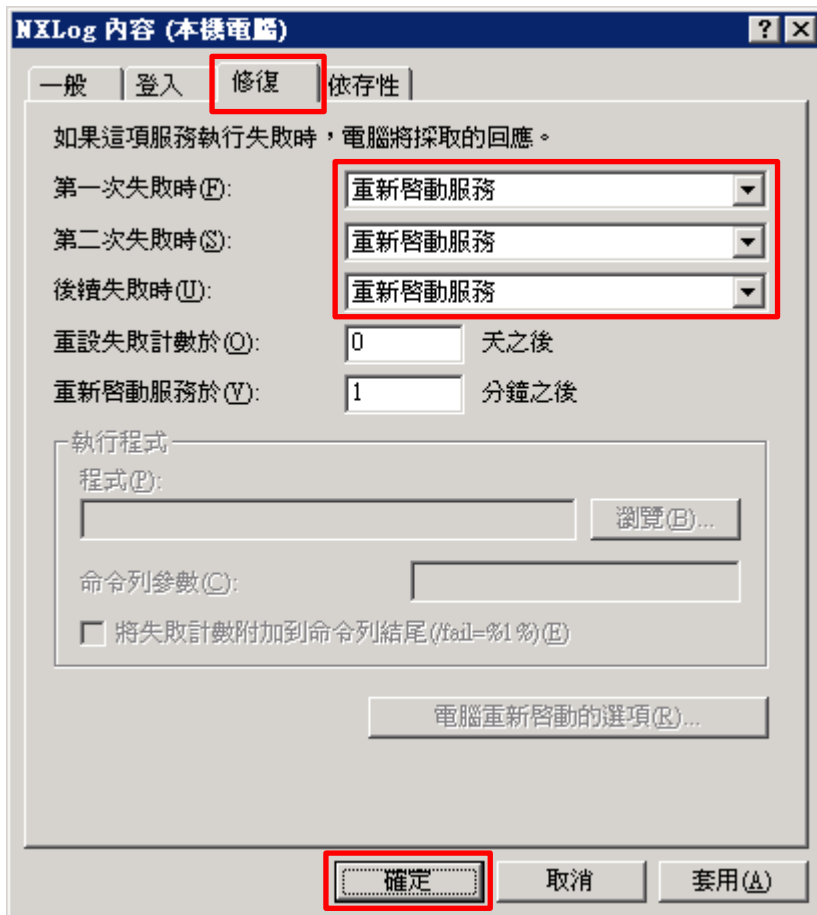
選擇 [nxlog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認 ; 啟動類型: [自動]



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



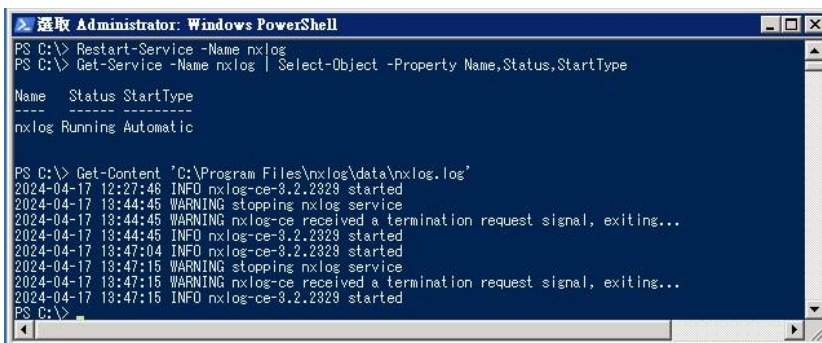
## 1.4.2 Windows 2008 或之後版本作業系統

### (1) 開啟 [Windows PowerShell]



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

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

A screenshot of a Windows PowerShell terminal window titled "選擇 Administrator: Windows PowerShell". The terminal shows the execution of three commands: "Restart-Service -Name nxlog", "Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType", and "Get-Content 'C:\Program Files\nxlog\data\nxlog.log'". The output of the second command shows "nxlog Running Automatic". The output of the third command shows a log file with several entries, including "INFO nxlog-ce-3.2.2329 started", "WARNING stopping nxlog service", and "WARNING nxlog-ce received a termination request signal, exiting...".

```
選擇 Administrator: Windows PowerShell
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name      Status StartType
-----
nxlog     Running Automatic


PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2024-04-17 12:27:46 INFO nxlog-ce-3.2.2329 started
2024-04-17 13:44:45 WARNING stopping nxlog service
2024-04-17 13:44:45 WARNING nxlog-ce received a termination request signal, exiting...
2024-04-17 13:44:45 INFO nxlog-ce-3.2.2329 started
2024-04-17 13:47:04 INFO nxlog-ce-3.2.2329 started
2024-04-17 13:47:15 WARNING stopping nxlog service
2024-04-17 13:47:15 WARNING nxlog-ce received a termination request signal, exiting...
2024-04-17 13:47:15 INFO nxlog-ce-3.2.2329 started
PS C:\>
```

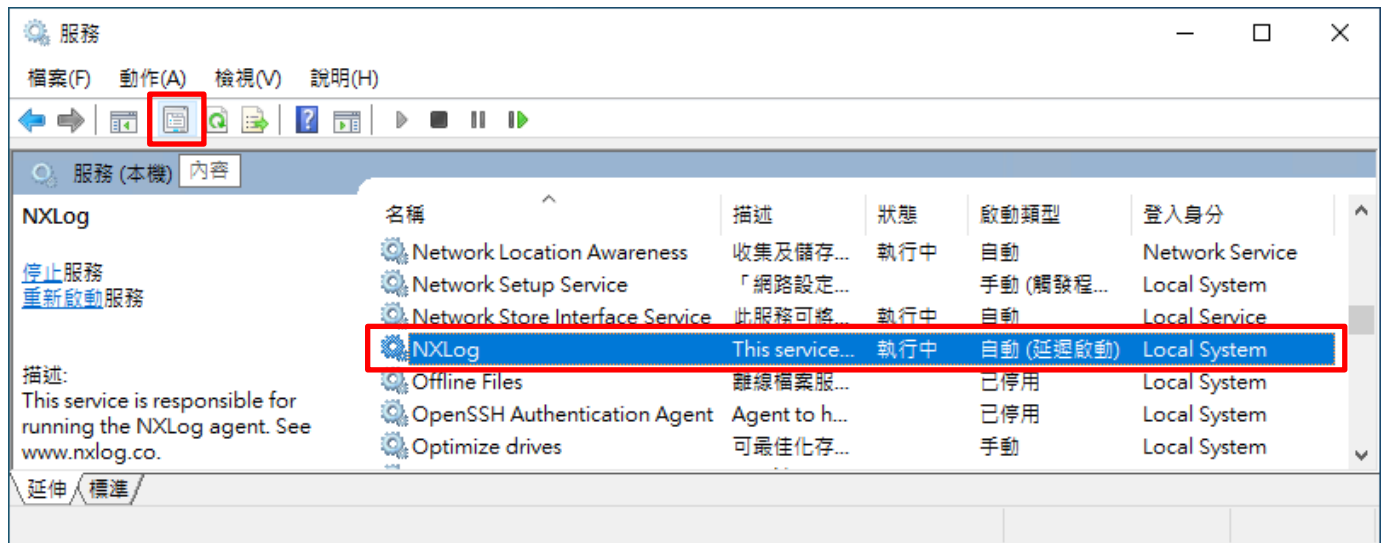
### (3) 開啟 [服務] 功能

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

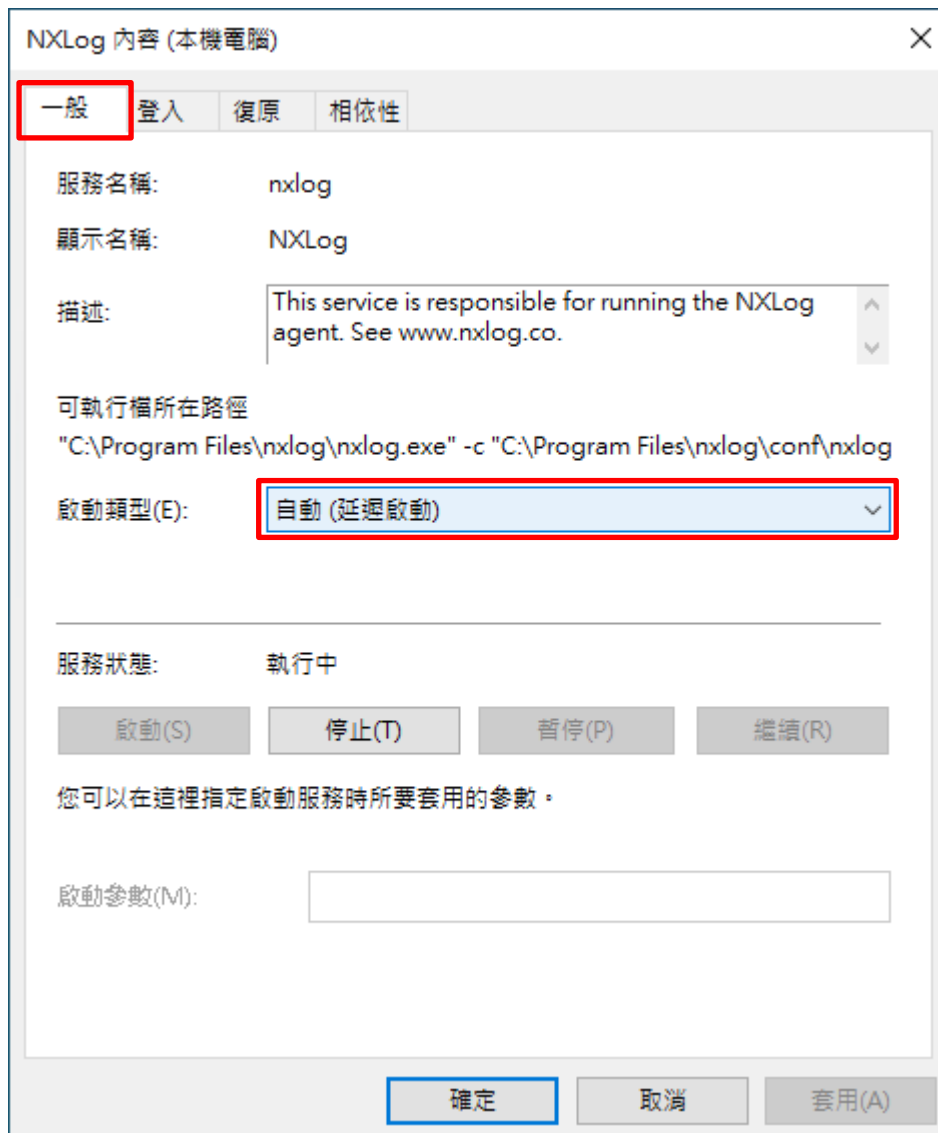


(4) 開啟 NXLog 服務內容

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]

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P):  瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%)(E)

確定 取消 套用(A)

## 2. Windows 2000

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

※ 以下分別為網域和工作群組設定方式。

### 2.1 網域

#### 2.1.1 組織單位設定

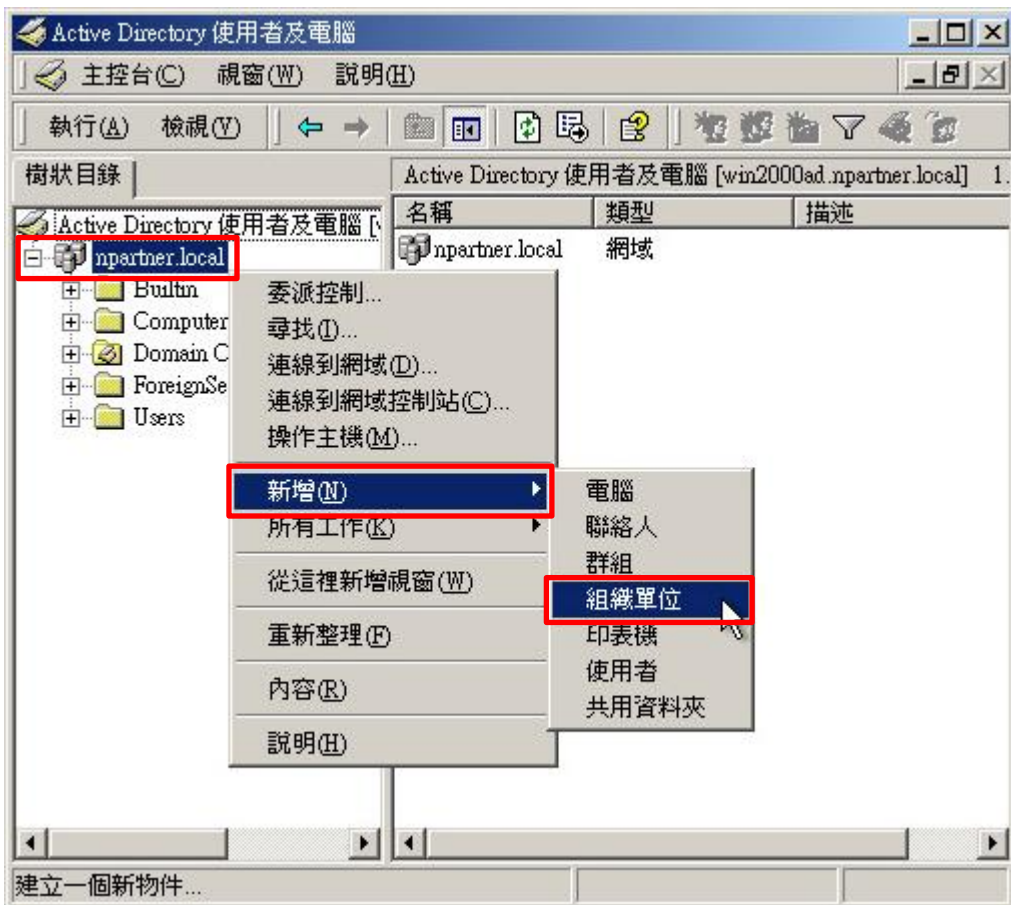
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

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





(3) 輸入組織單位名稱

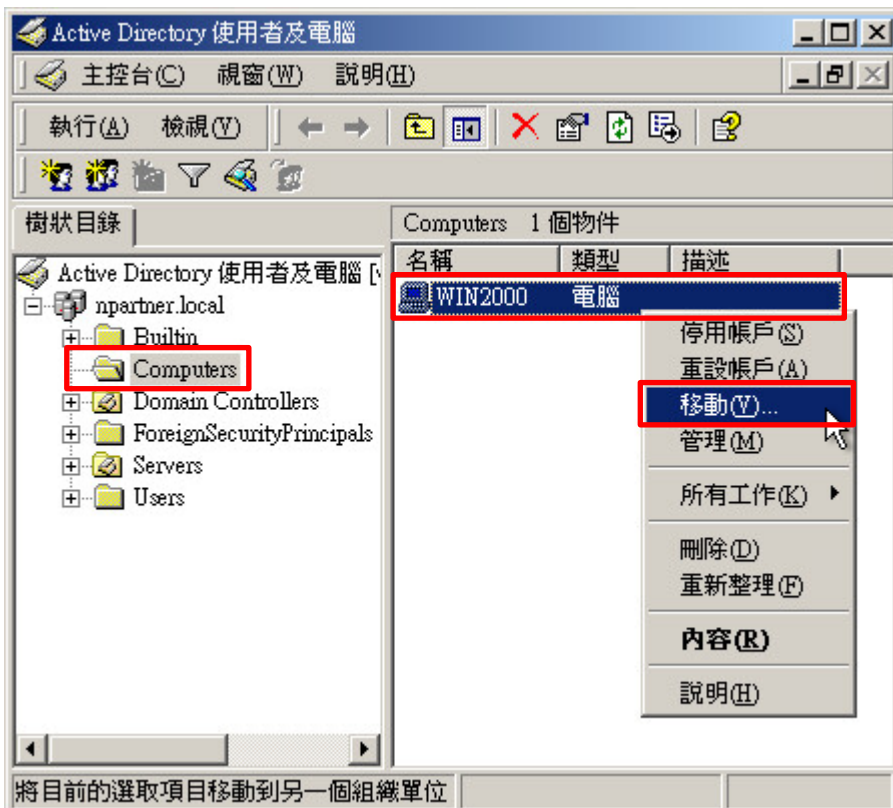
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

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

-> 點選 [移動]



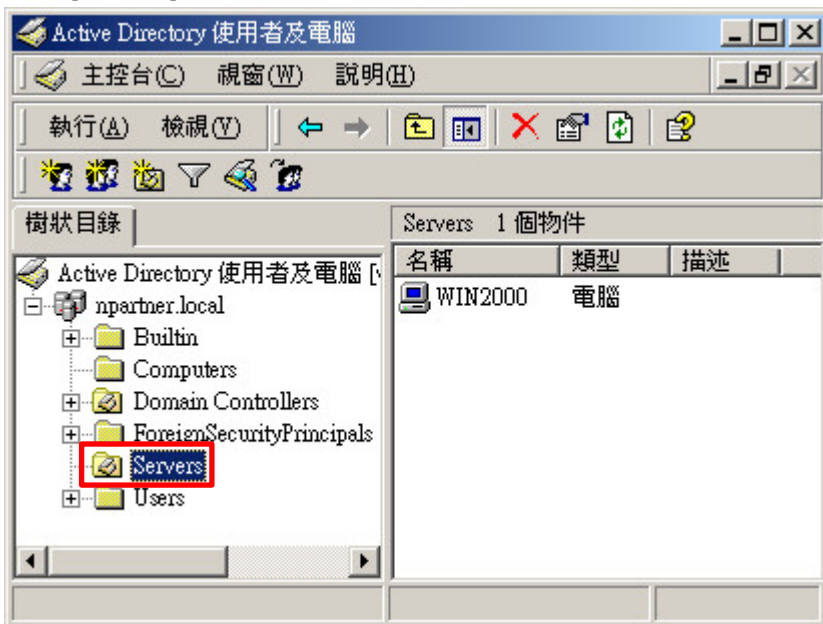
(5) 選擇組織單位

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

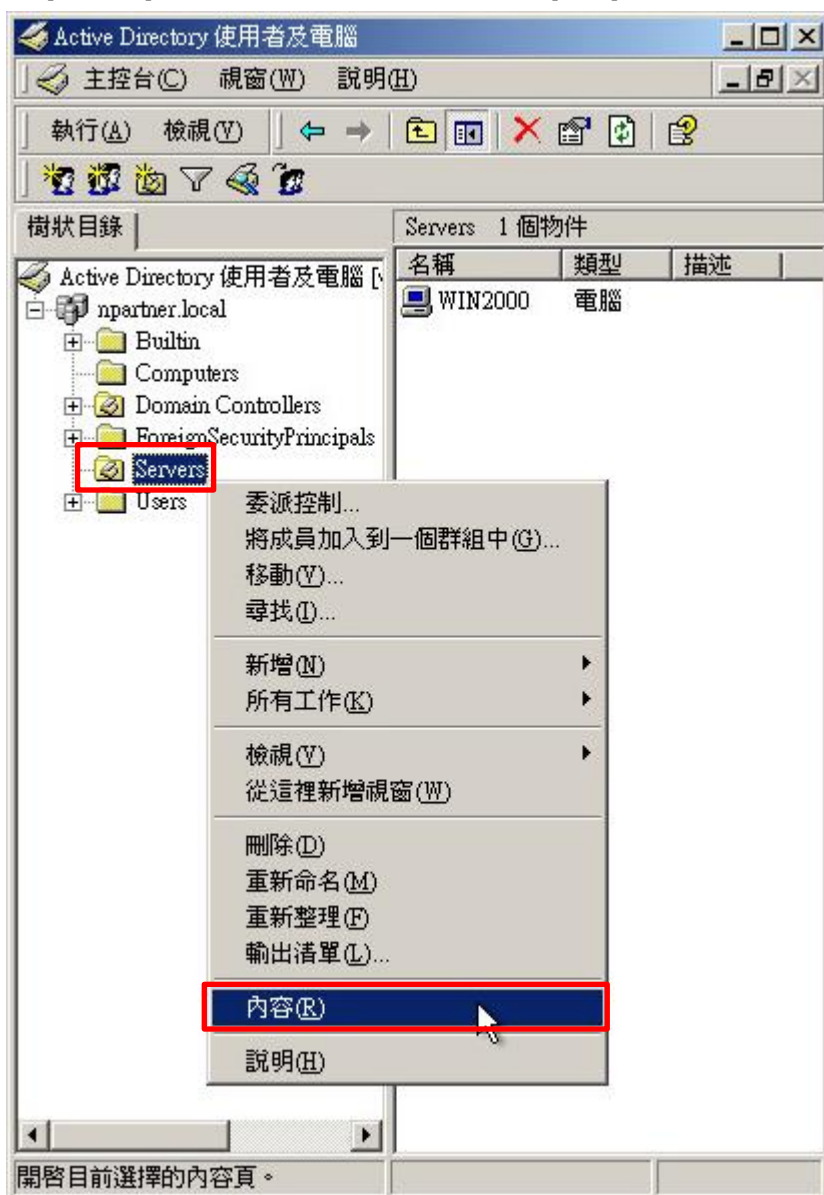
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



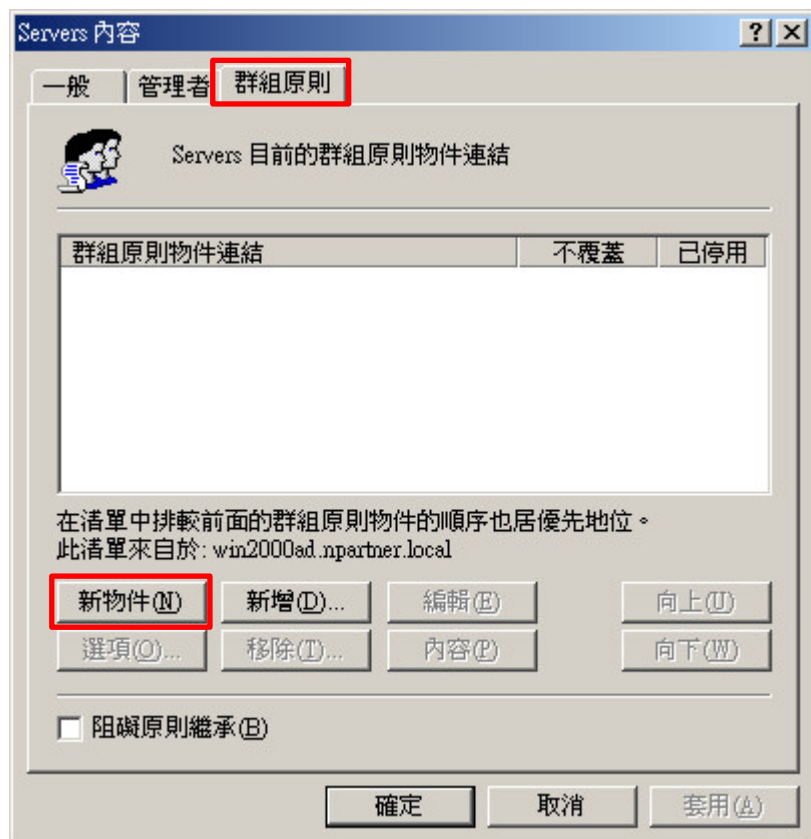
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



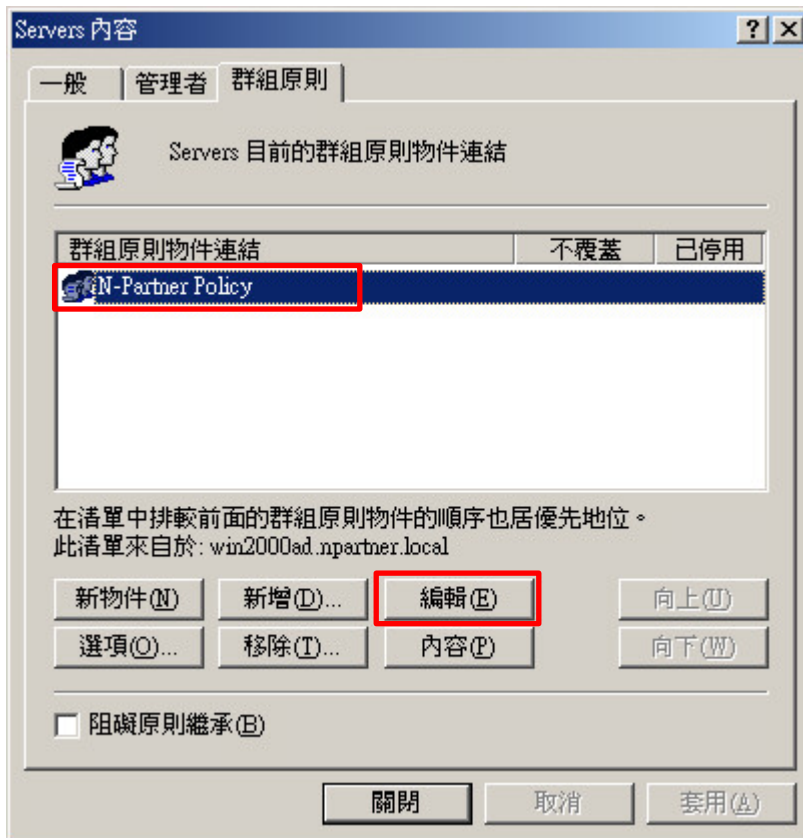
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



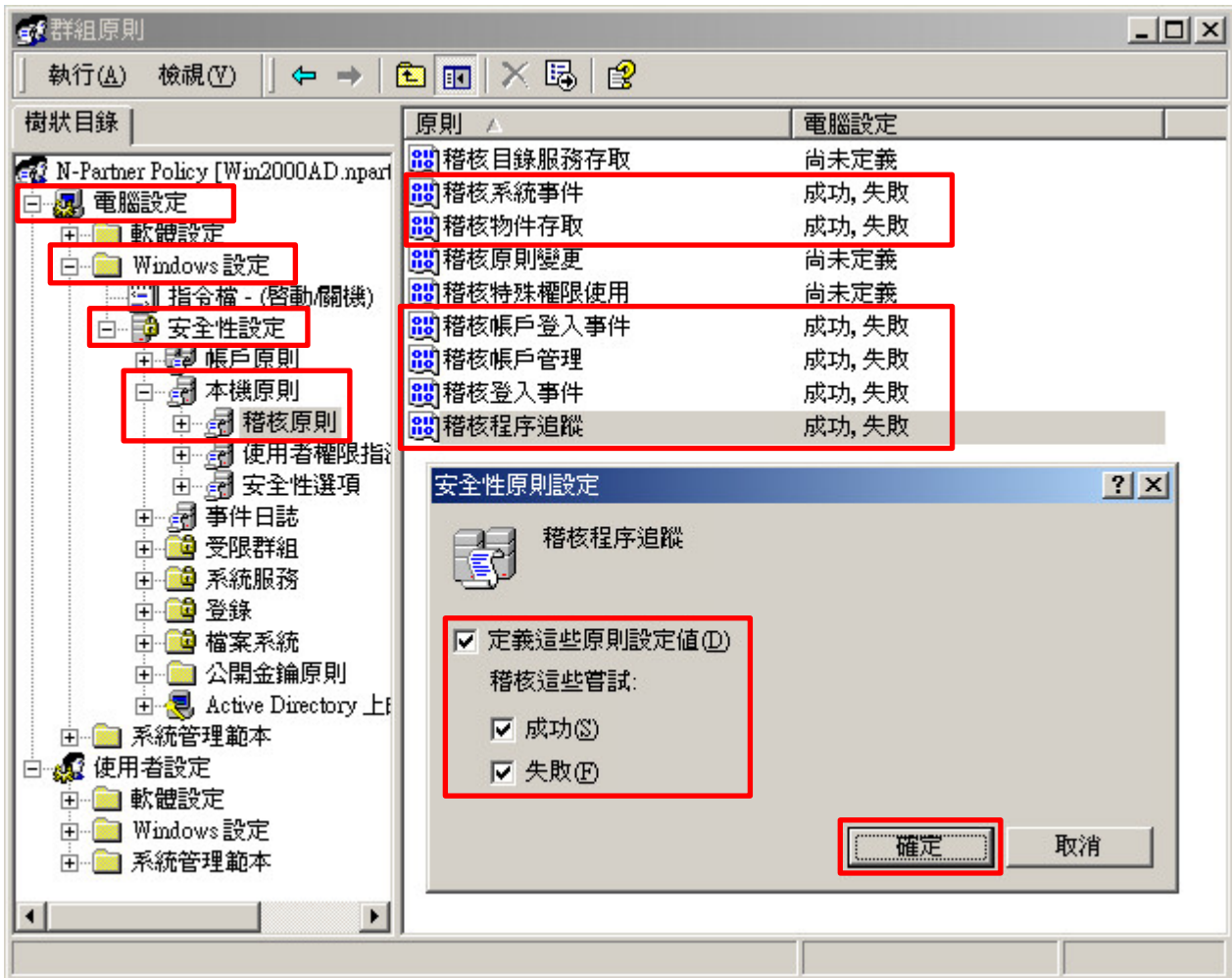
(4) 編輯群組原則物件

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]



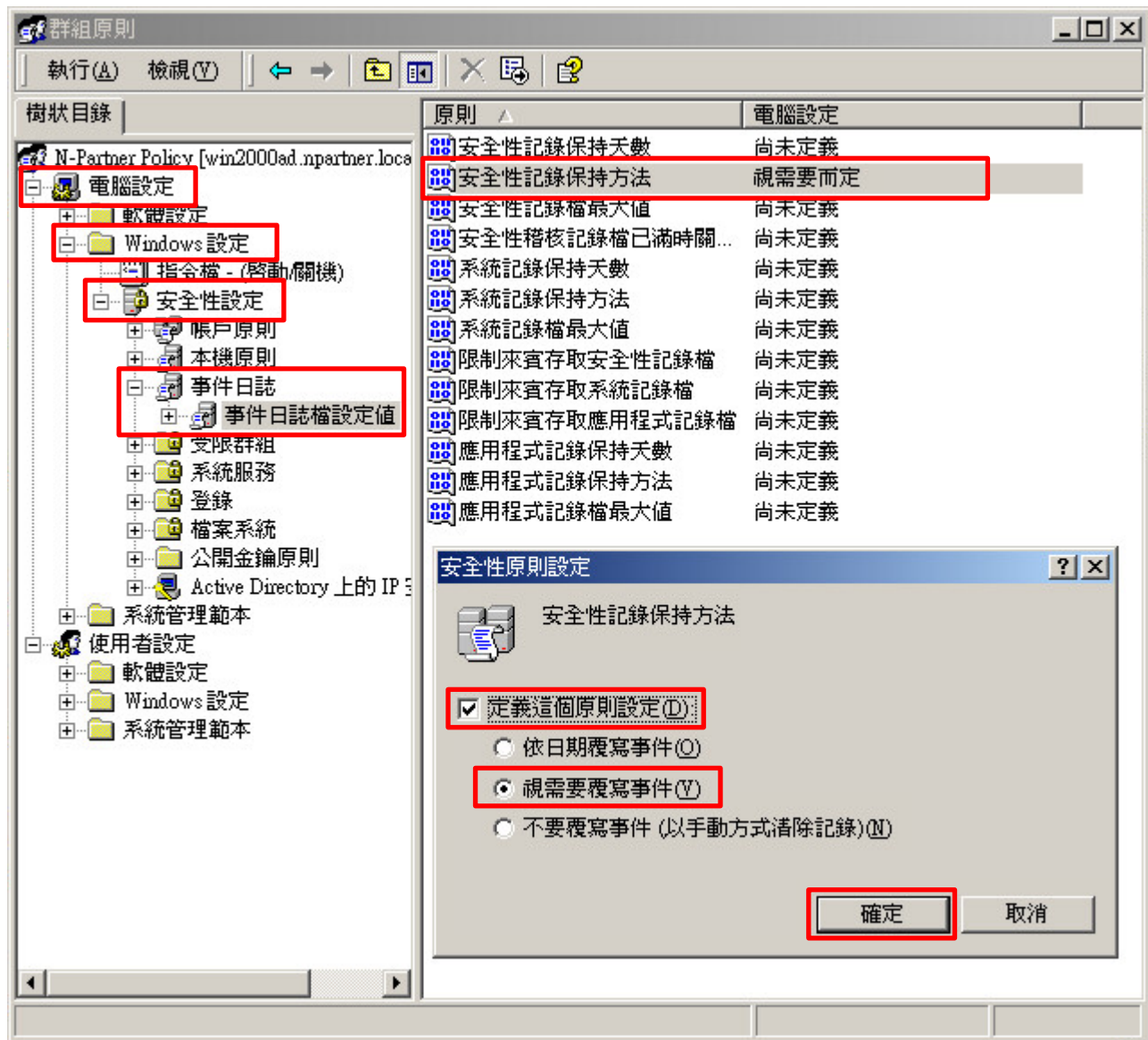
(5) 本機原則：稽核原則

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]



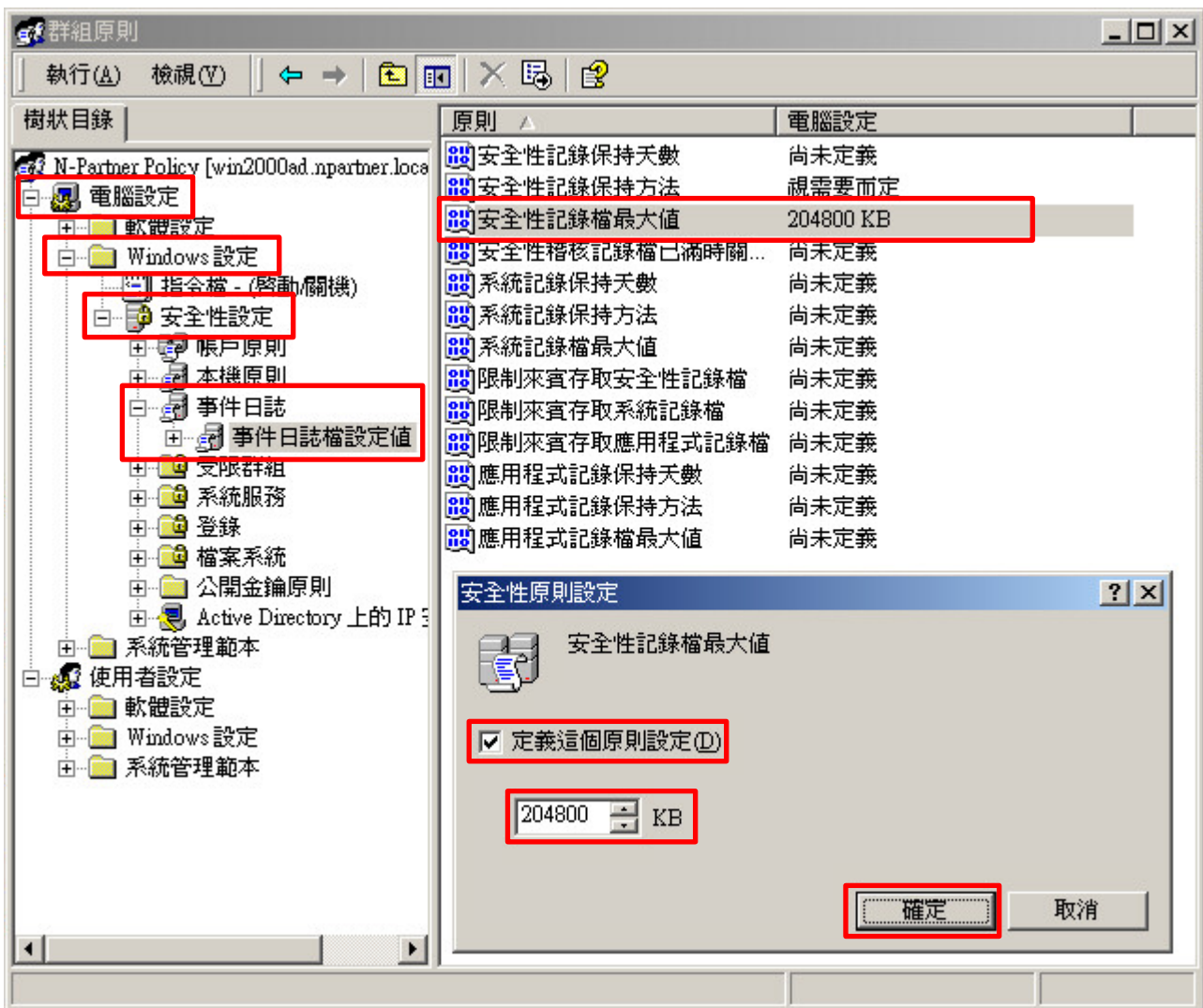
(6) 事件日誌：安全性記錄保持方法

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]

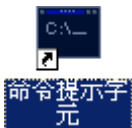


(7) 事件日誌：安全性記錄檔最大值

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



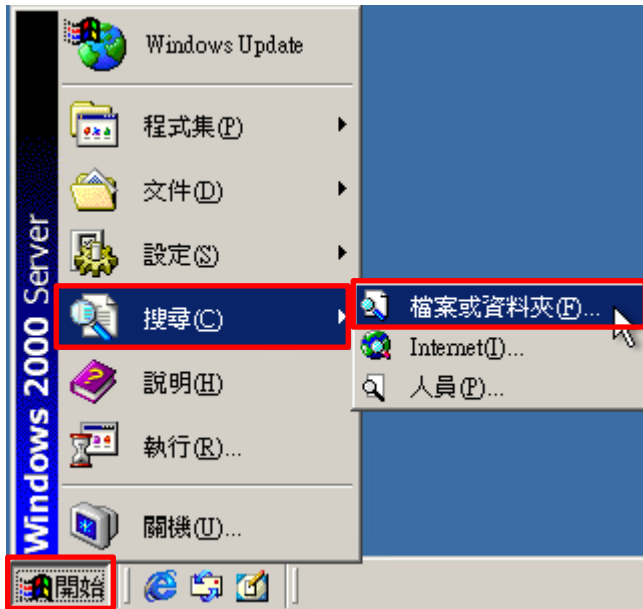
```
命令提示字元
C:\>secedit /refreshpolicy machine_policy /enforce
從網域來的群組原則傳播已經初始給這台電腦。可能要數分鐘才能完成傳播讓新原則生效。
請檢查應用程式記錄是否有任何錯誤。
C:\>_
```

## 2.2 工作群組

### 2.2.1 稽核原則設定

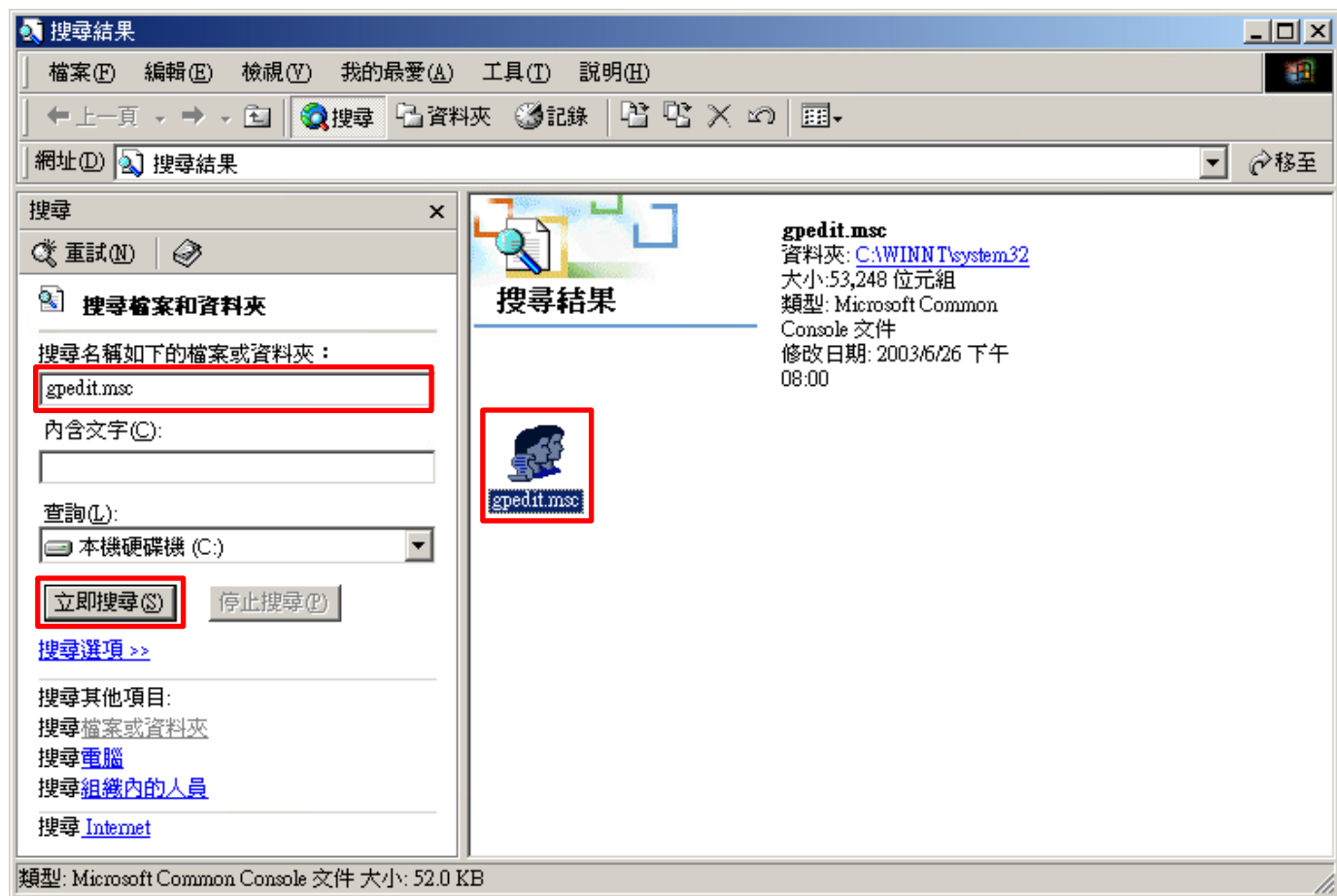
#### (1) 開啟搜尋

點選 [開始] -> [搜尋] -> [檔案或資料夾]



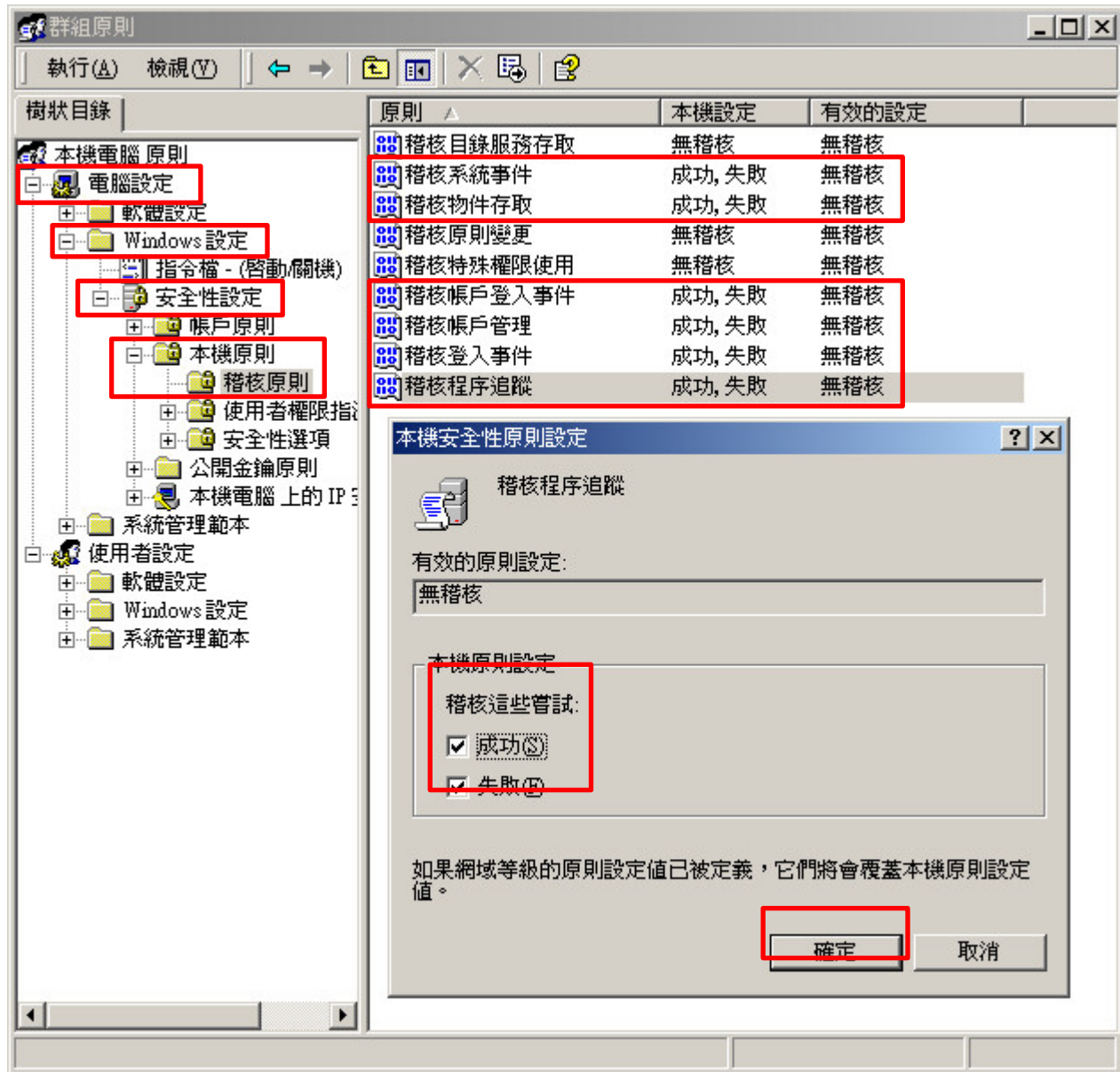
## (2) 搜尋群組原則

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]

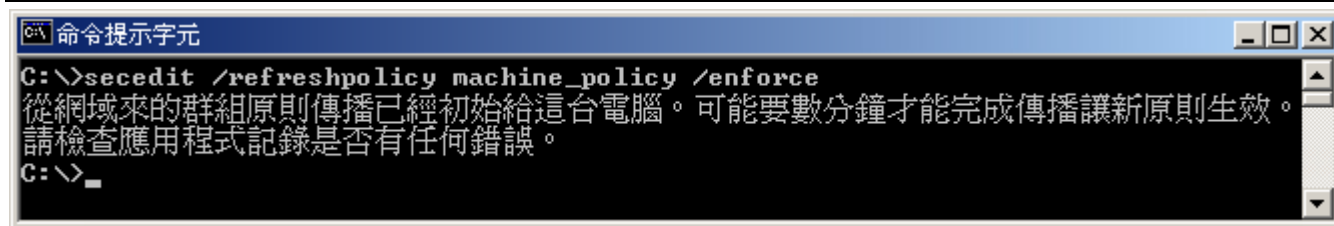


(4) 開啟 [命令提示字元]



(5) 更新群組原則。

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

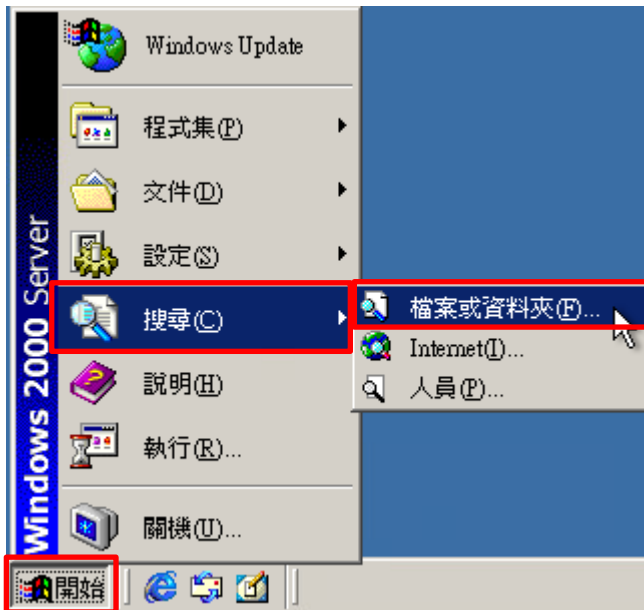


```
命令提示字元
C:\>secedit /refreshpolicy machine_policy /enforce
從網域來的群組原則傳播已經初始給這台電腦。可能要數分鐘才能完成傳播讓新原則生效。
請檢查應用程式記錄是否有任何錯誤。
C:\>_
```

## 2.2.2 事件檔案設定

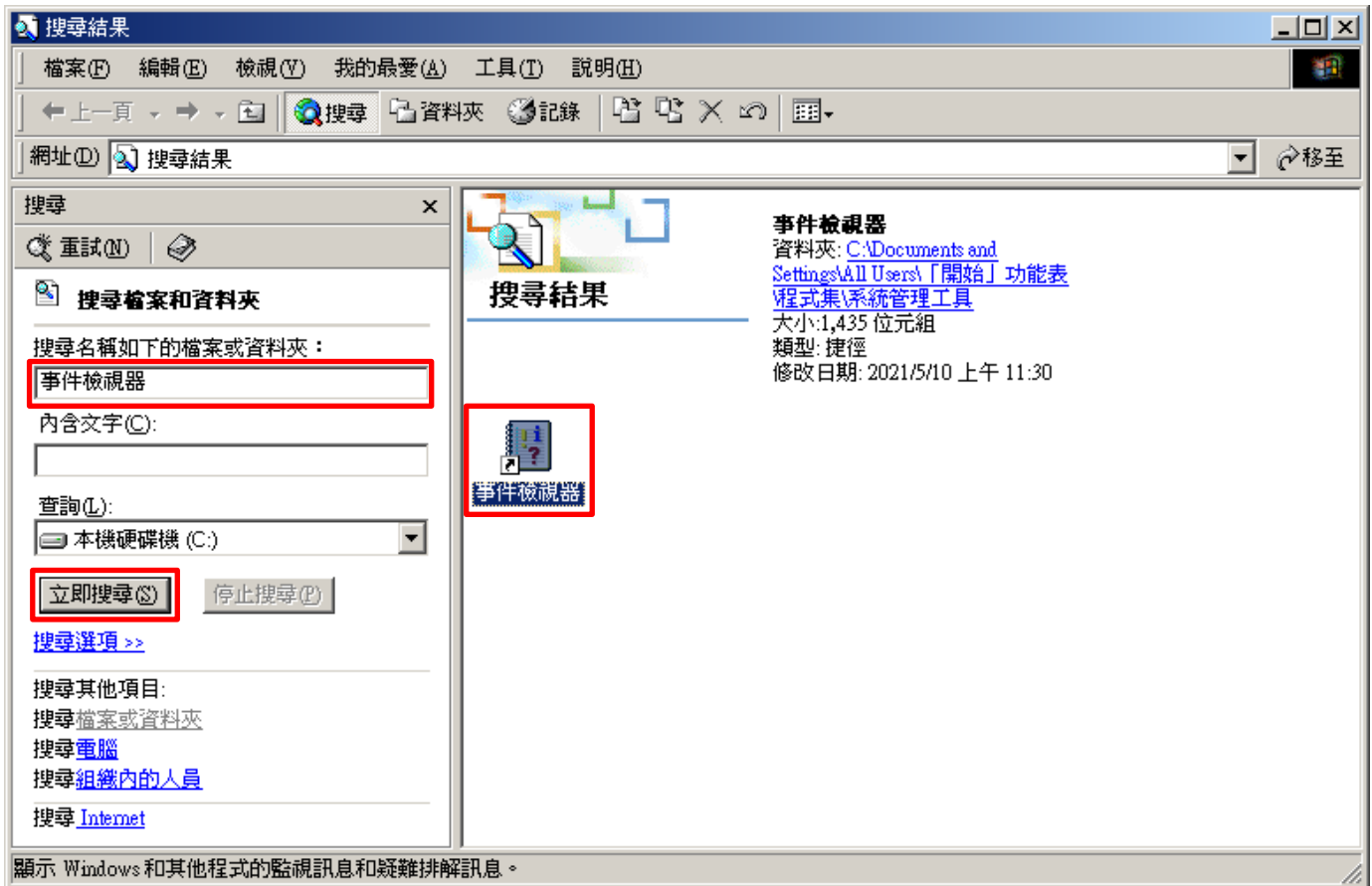
### (1) 開啟搜尋

點選 [開始] -> [搜尋] -> [檔案或資料夾]



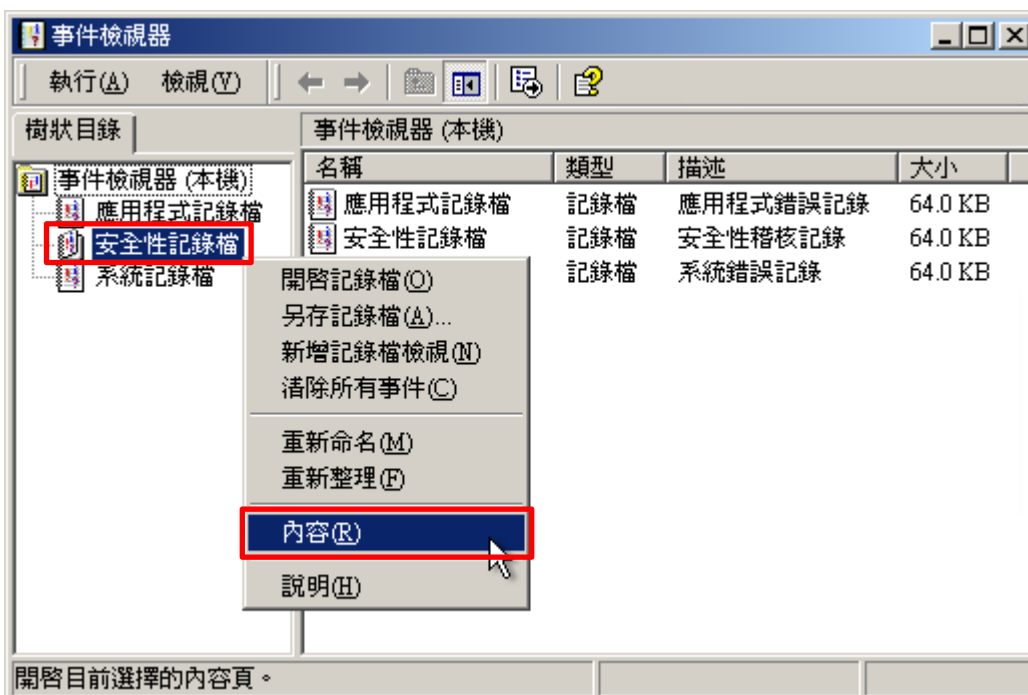
## (2) 搜尋事件檢視器

輸入 **事件檢視器** -> 按 [立即搜尋] -> 點選 [事件檢視器]



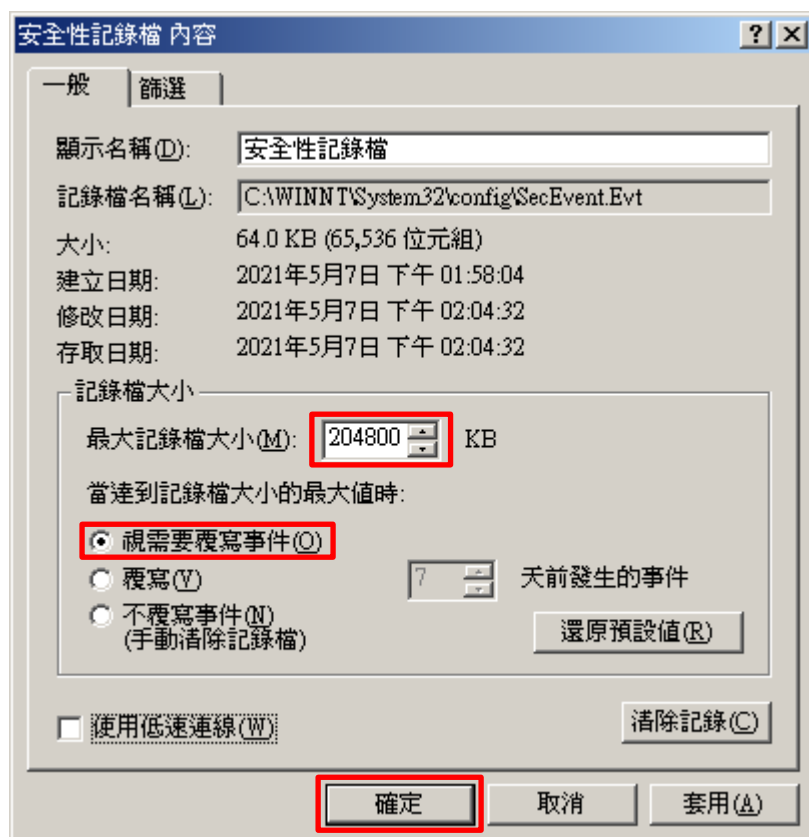
## (3) 編輯安全性記錄檔

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

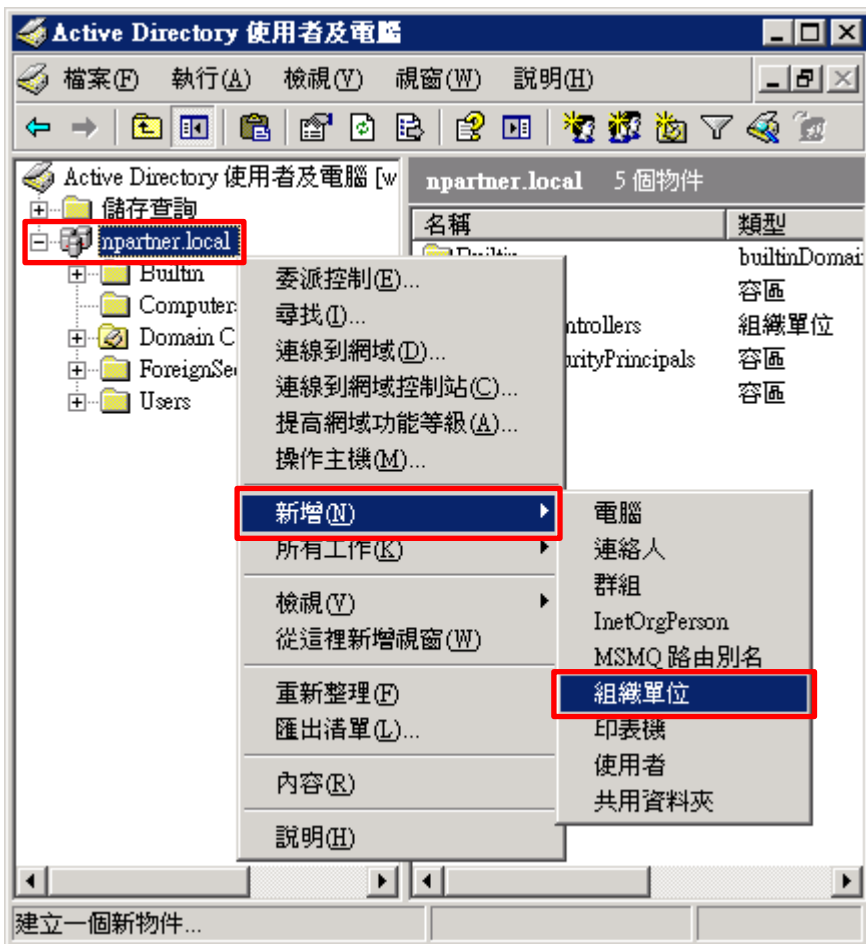
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



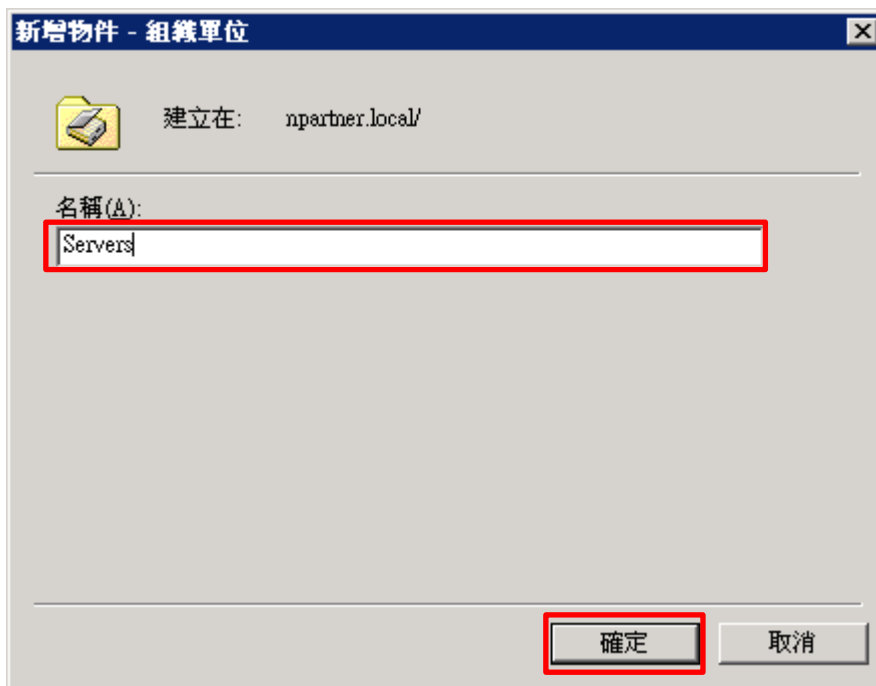
(2) 新增組織單位

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

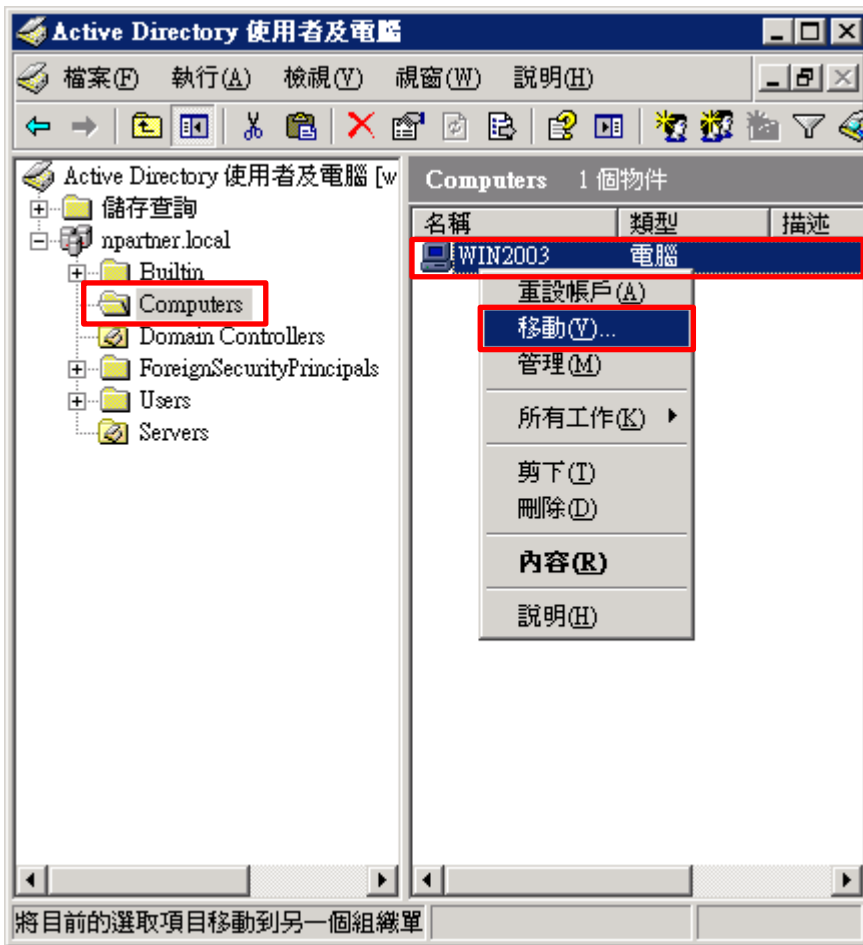
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(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]



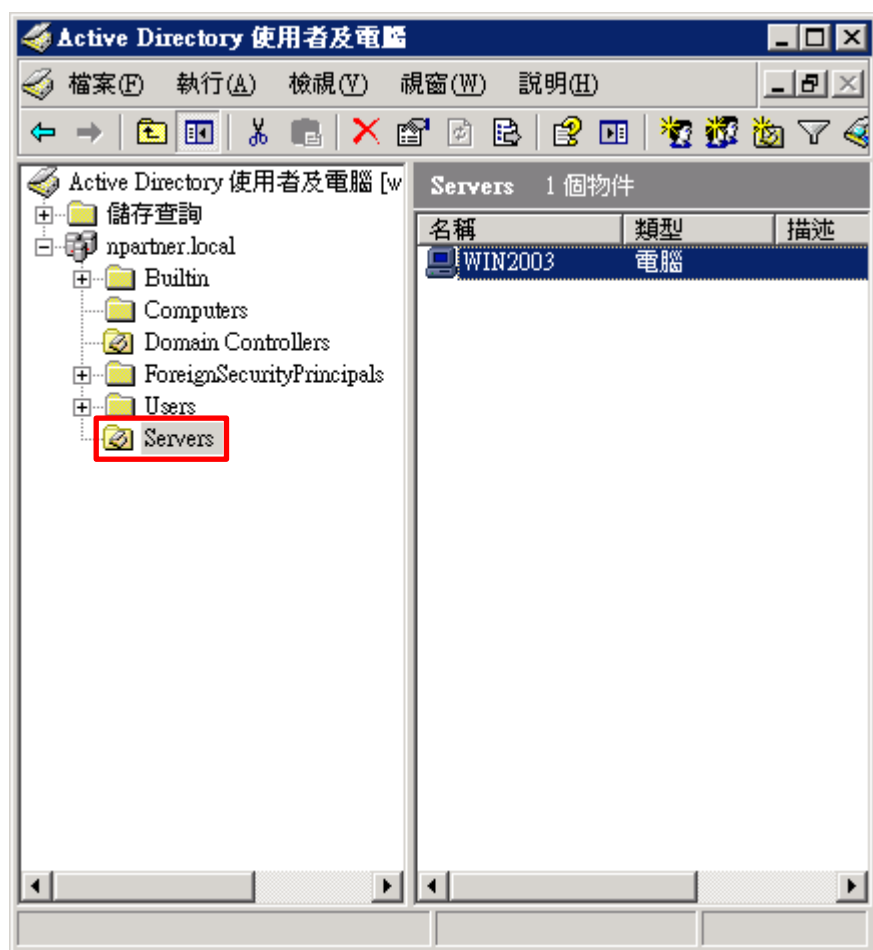
(5) 選擇組織單位

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

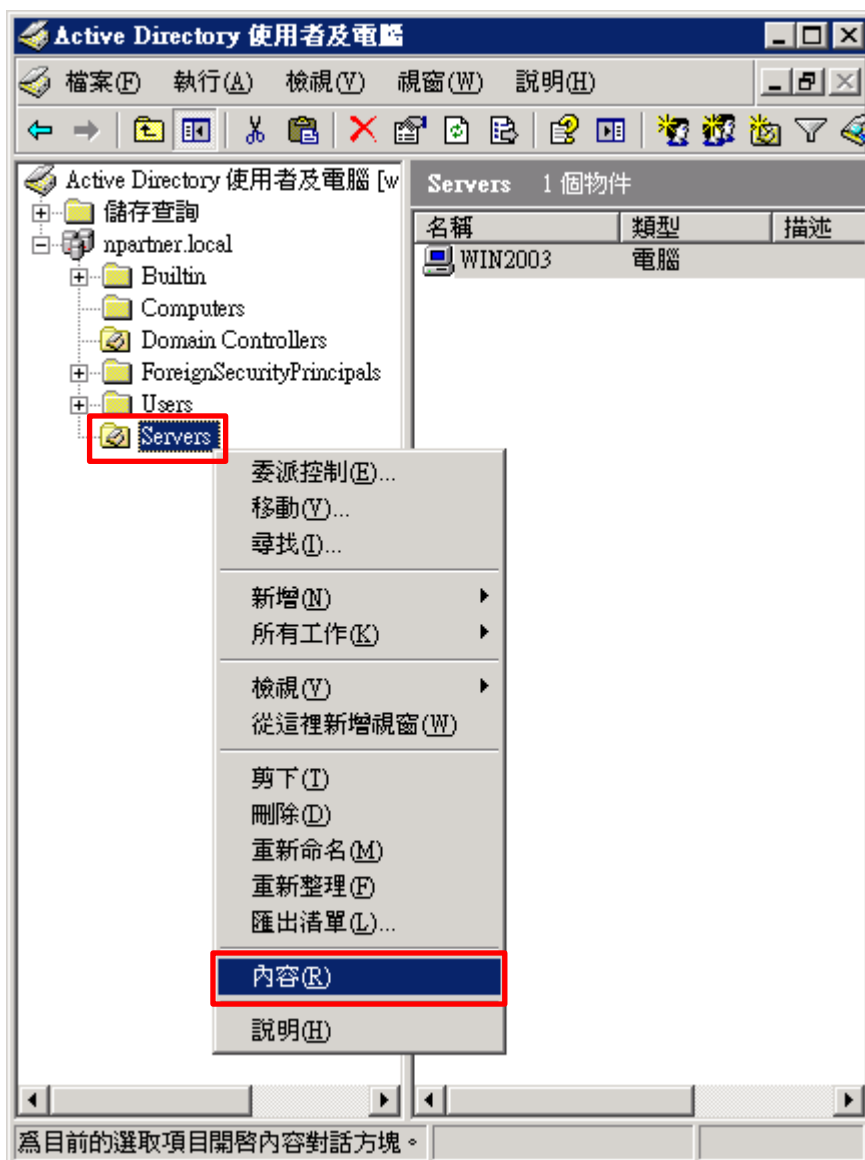
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



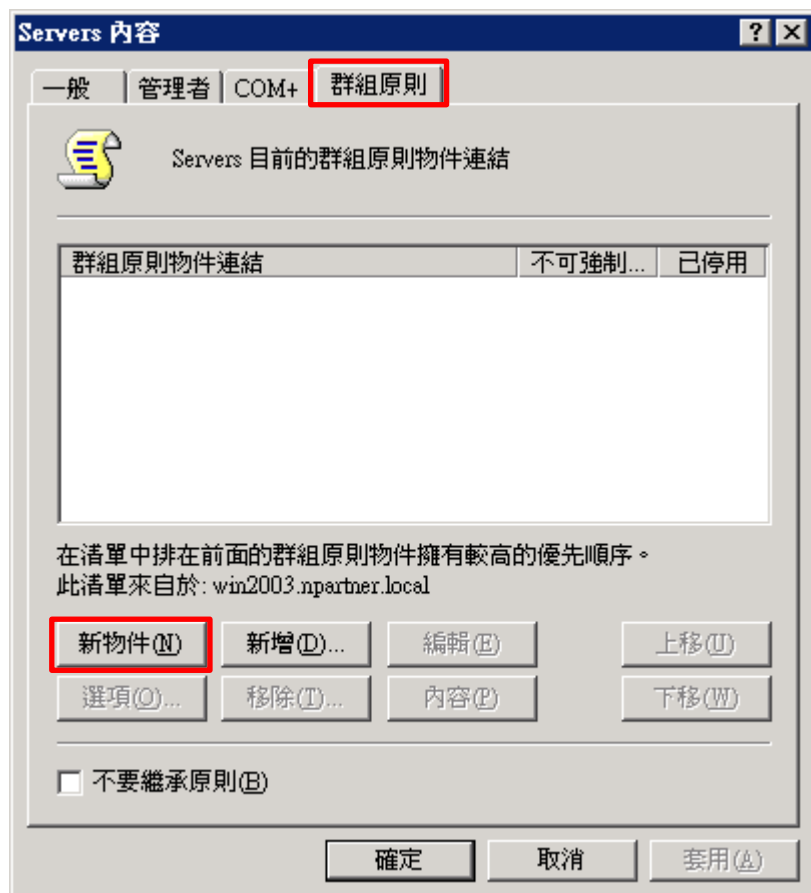
(2) 在 Servers 組織單位，點選內容

在 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



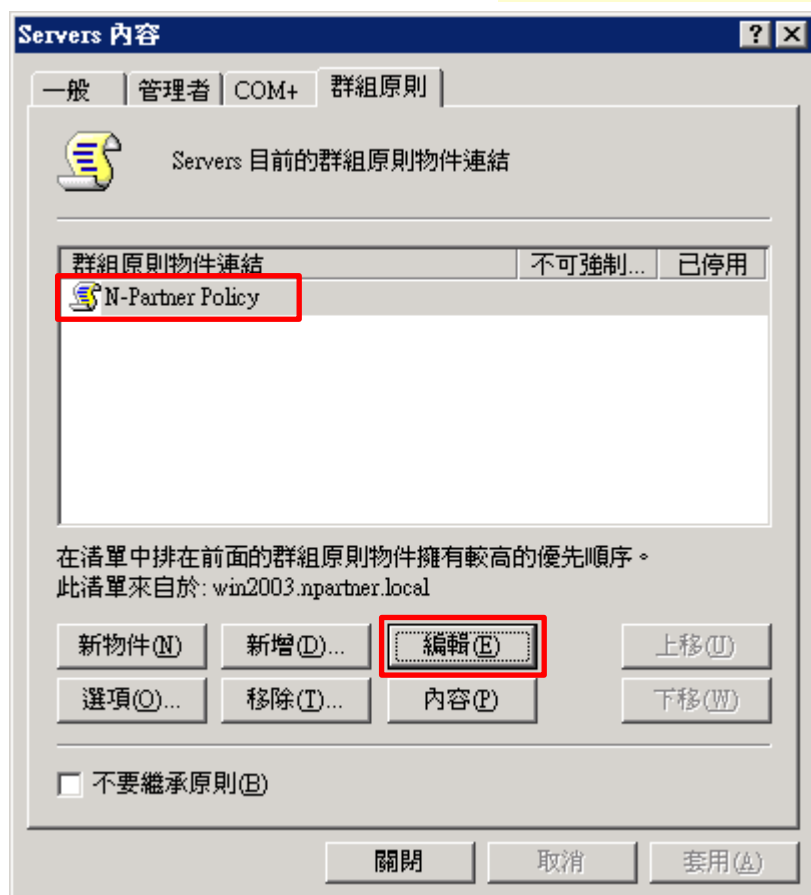
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



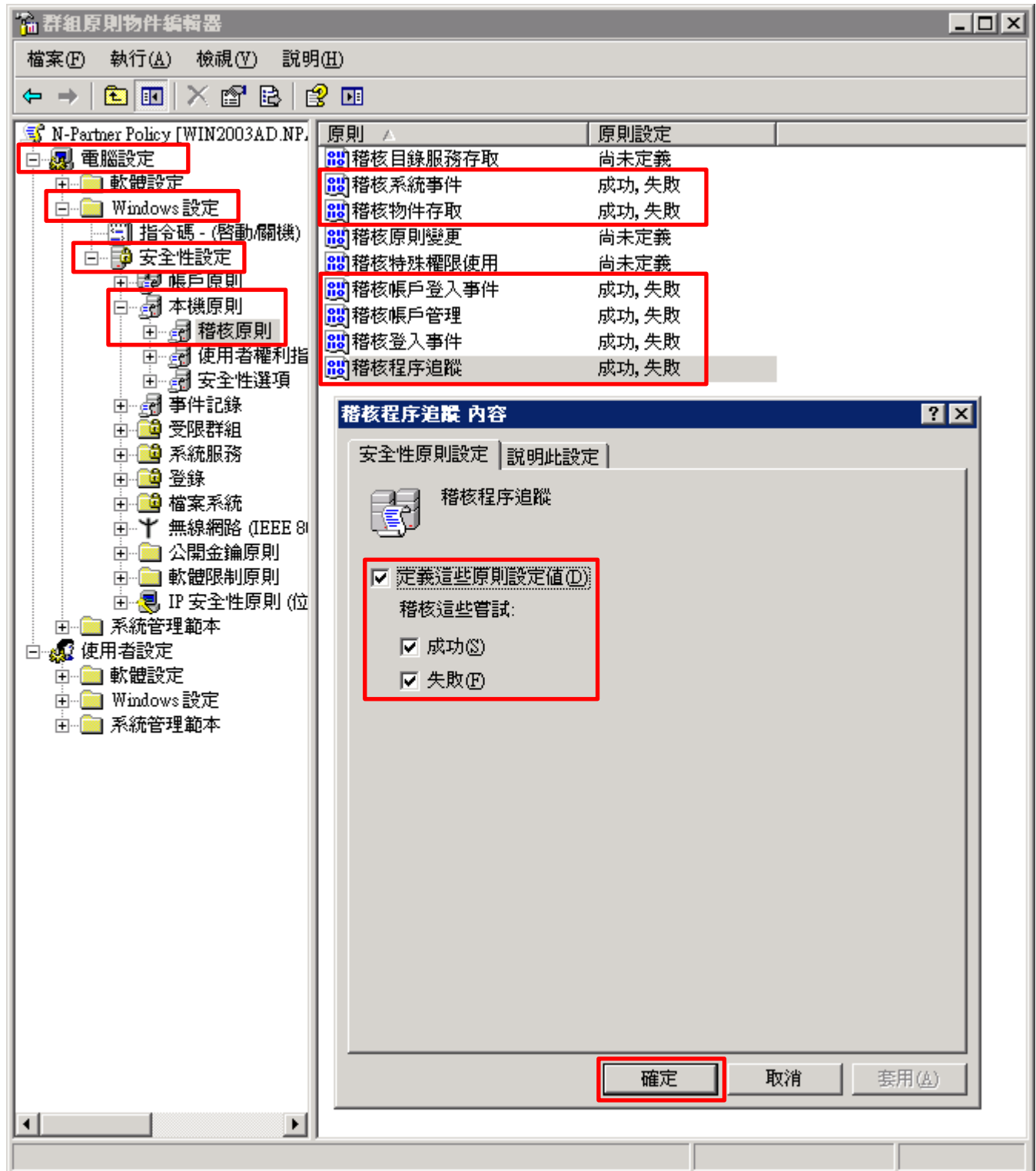
#### (4) 編輯群組原則物件

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

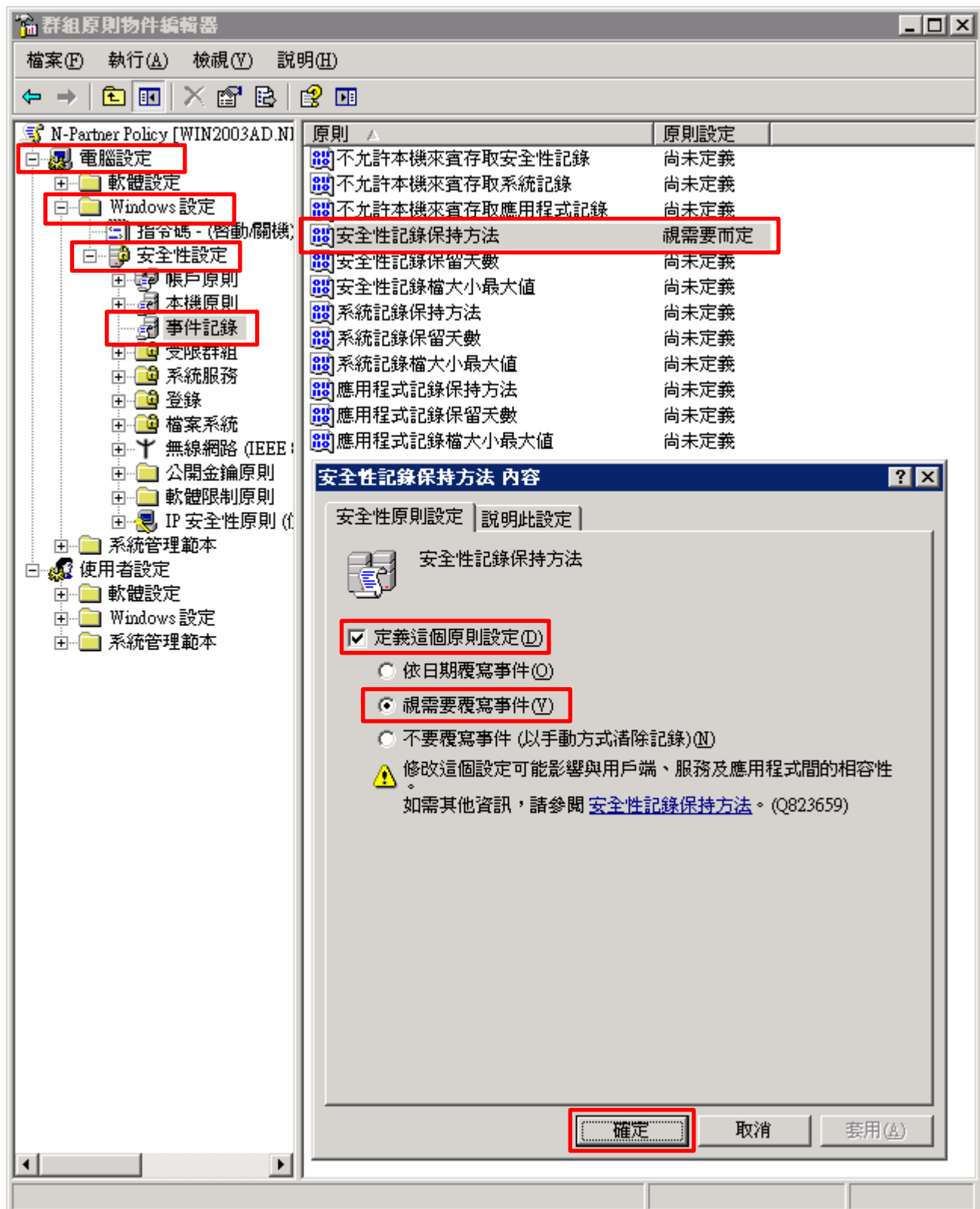
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [稽核物件存取], [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件], [稽核程序追蹤] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





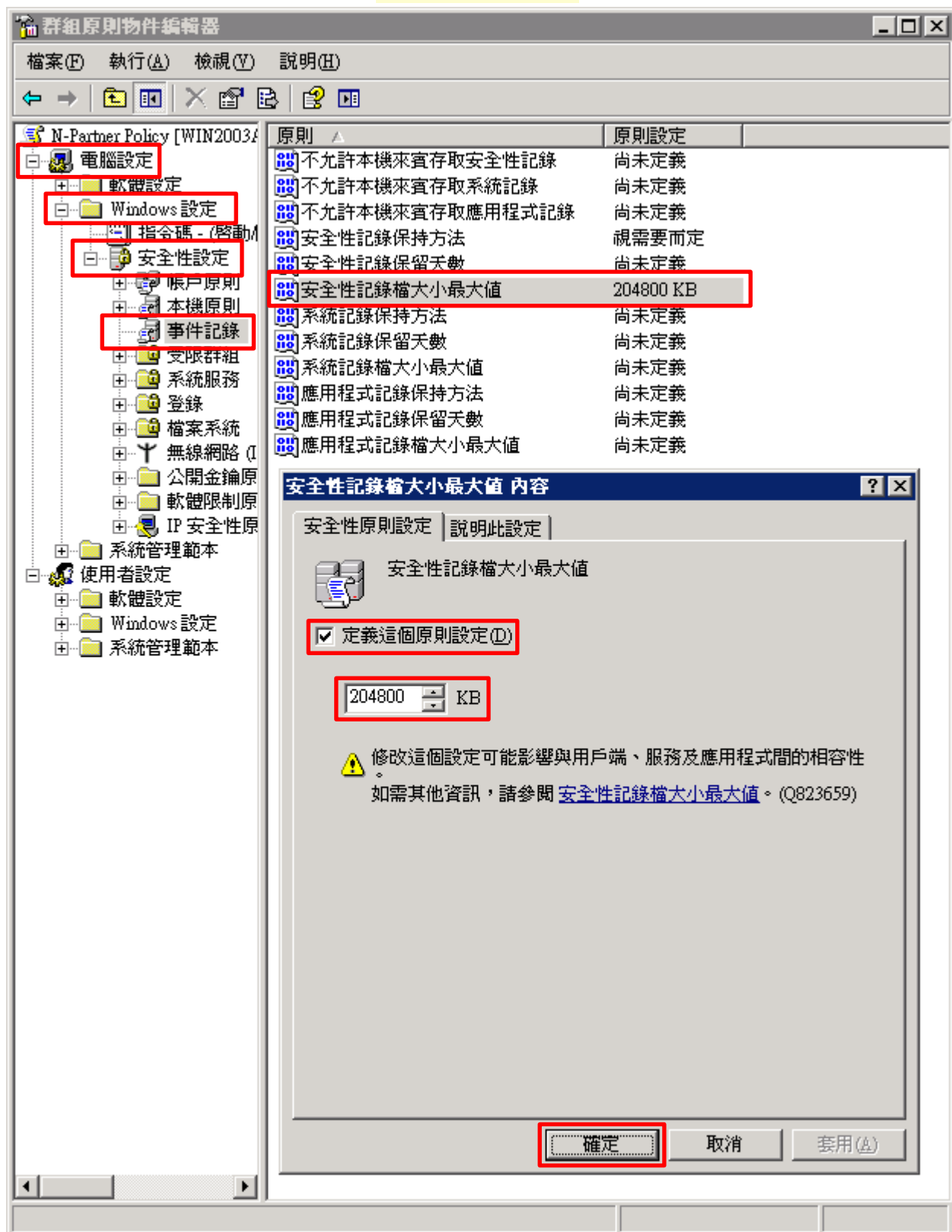
(6) 事件記錄：安全性記錄保持方法

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]



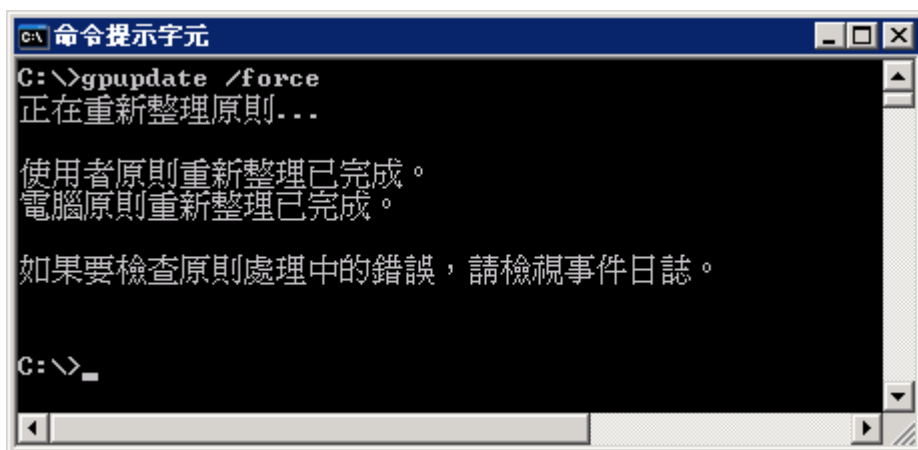
(8) 在 Windows Server 伺服器，開啟 [命令提示字元]



命令提示字元

(9) 更新群組原則。

C:\> gpupdate /force



(10) 查看群組原則套用情形

C:\> gpresult /v

```
命令提示字元
NPARTNER\Administrator 的 RSOP 資料在 WIN2003: 記錄模式
-----
OS 類型:                Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition
OS 設定:                網域主控站
OS 版本:                5.2.3790
終端機伺服器模式:     遠端系統管理
站台名稱:              Default-First-Site-Name
漫遊設定檔:
本機設定檔:            C:\Documents and Settings\Administrator
用低速連結來連線?:    否

電腦設定
-----
CN=WIN2003,OU=Servers,DC=npartner,DC=local
上次套用的群組原則:    2019/6/3 於 上午 10:59:26
套用的群組原則來自:    win2003.npartner.local
群組原則低速連結閾值: 500 kbps
網域名稱:              npartner
網域類型:              Windows 2000

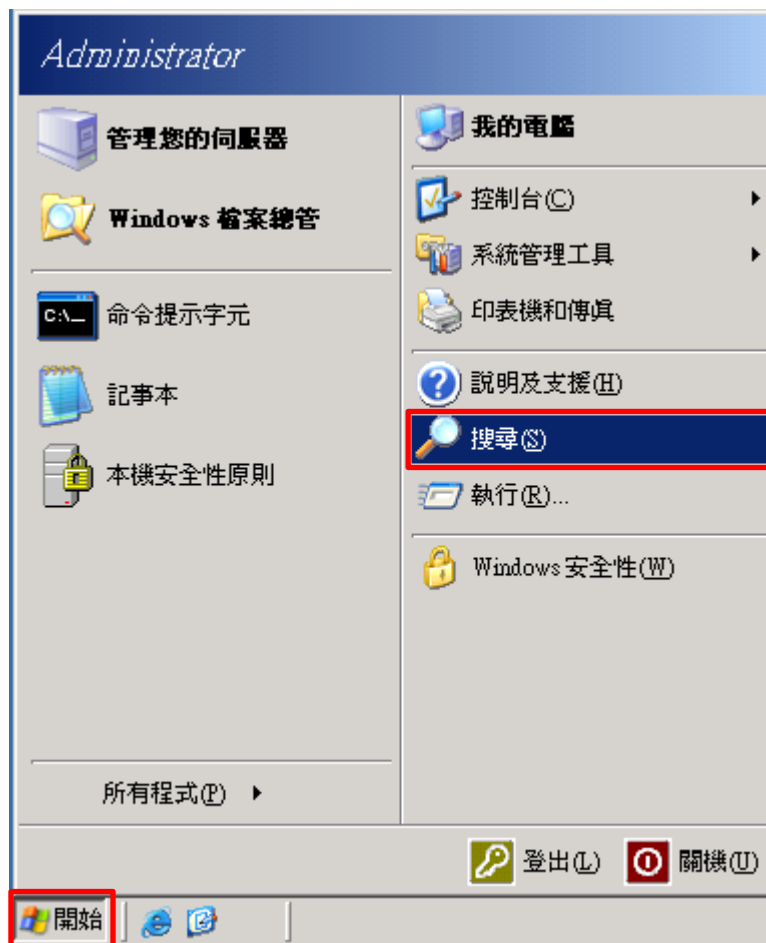
已套用的群組原則物件
-----
N-Partner Policy
Default Domain Policy
```

## 3.2 工作群組

### 3.2.1 稽核原則設定

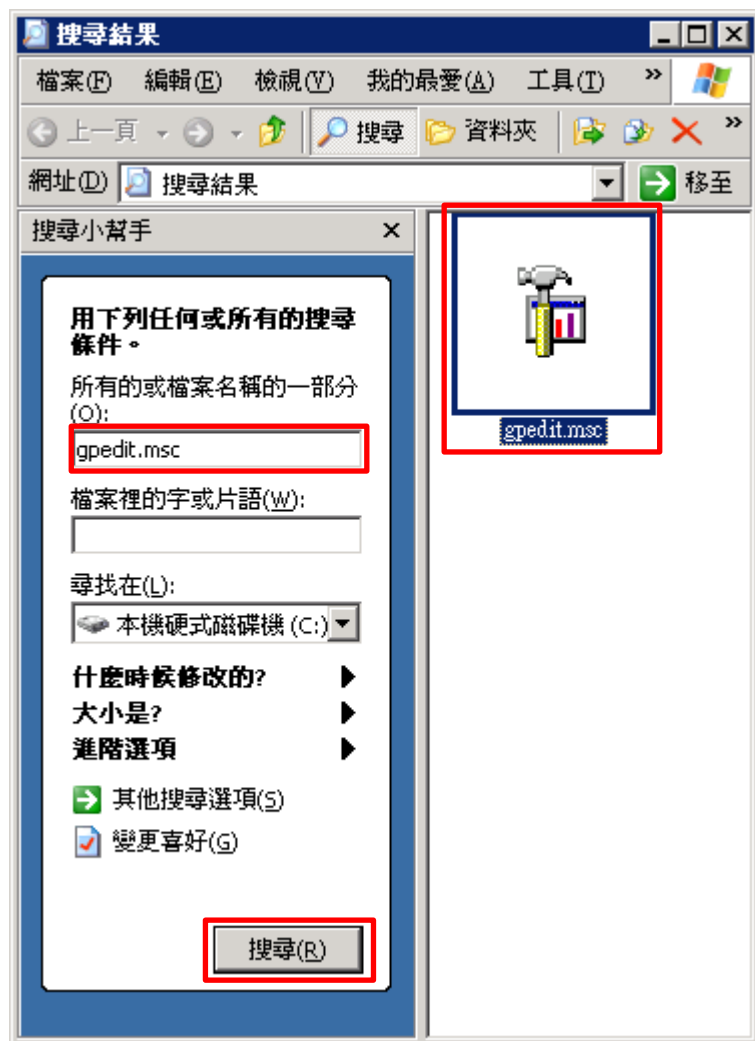
(1) 開啟搜尋

點選 [開始] -> [搜尋]



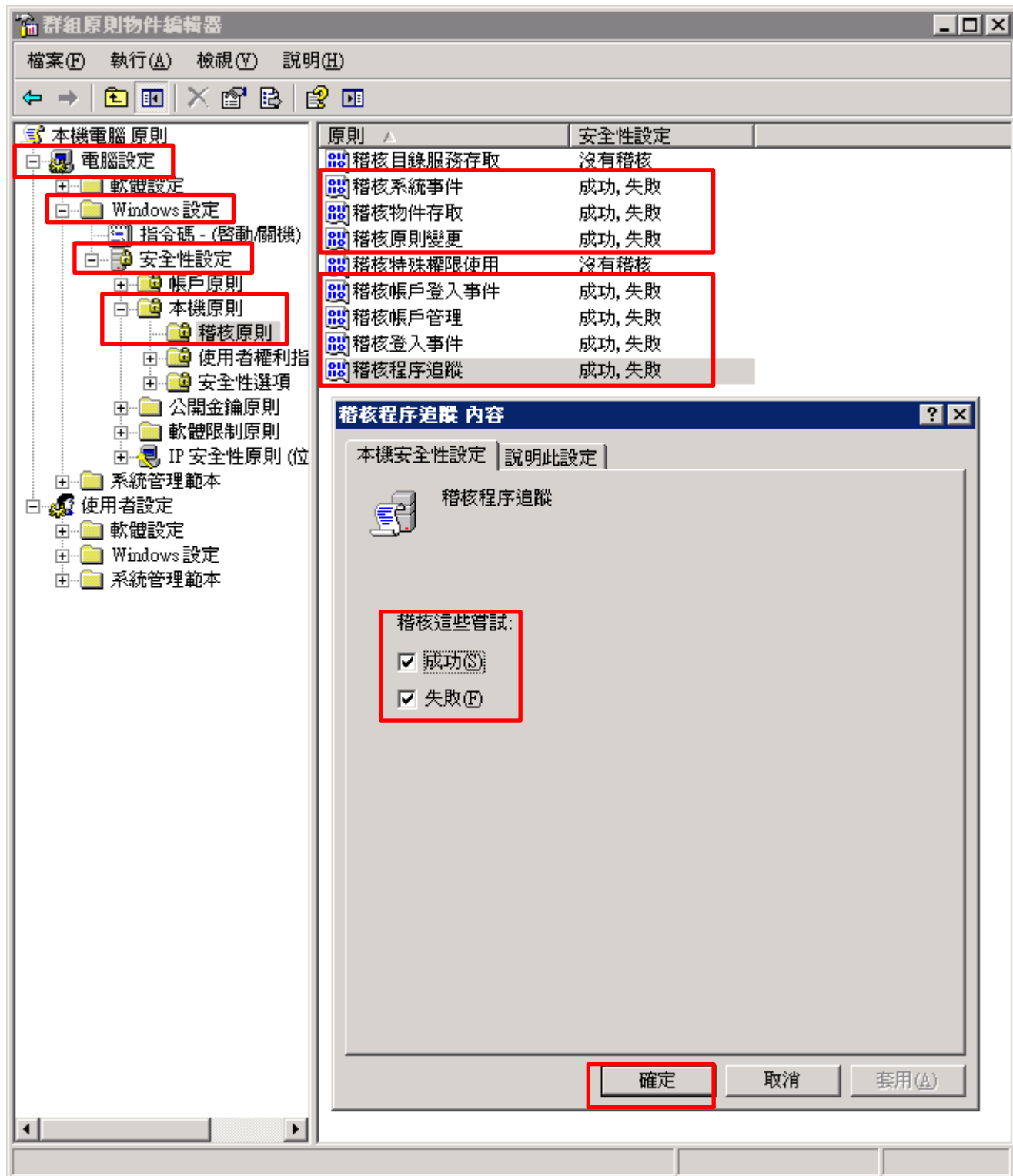
(2) 搜尋群組原則物件編輯器

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]



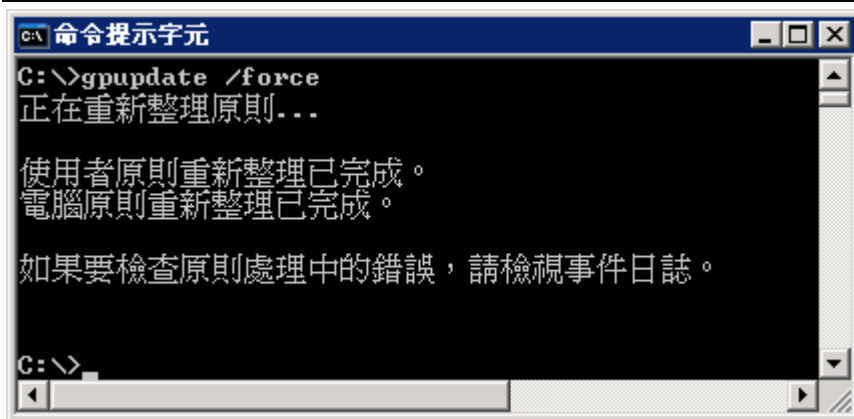
(4) 開啟 [命令提示字元]



命令提示字元

(5) 更新群組原則 .

C:\> gpupdate /force

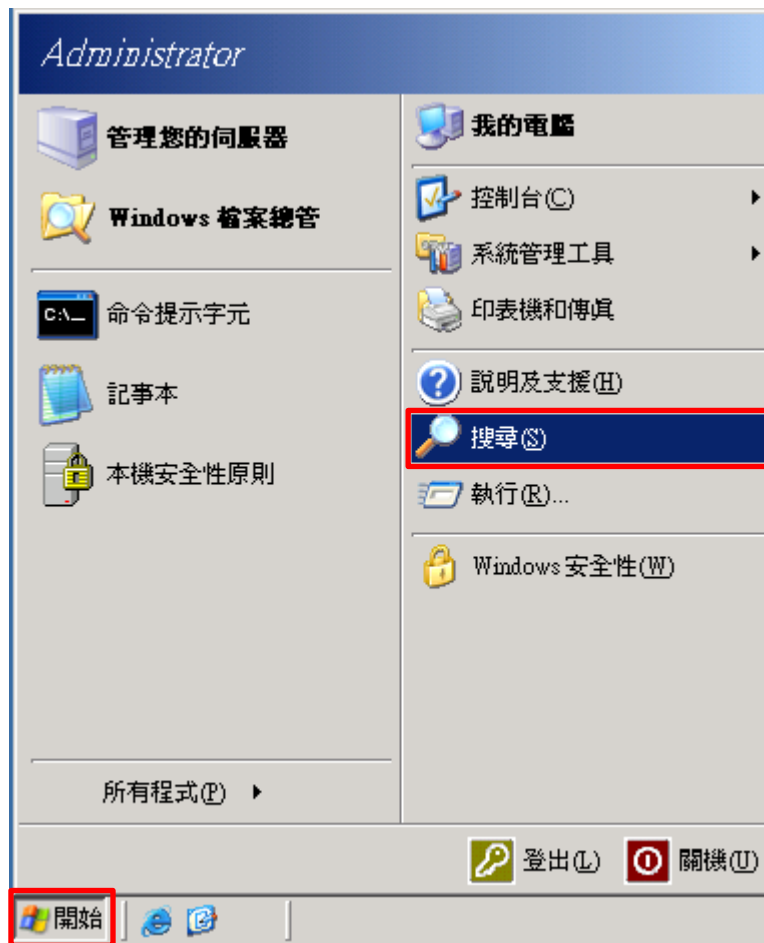




### 3.2.2 事件檔案設定

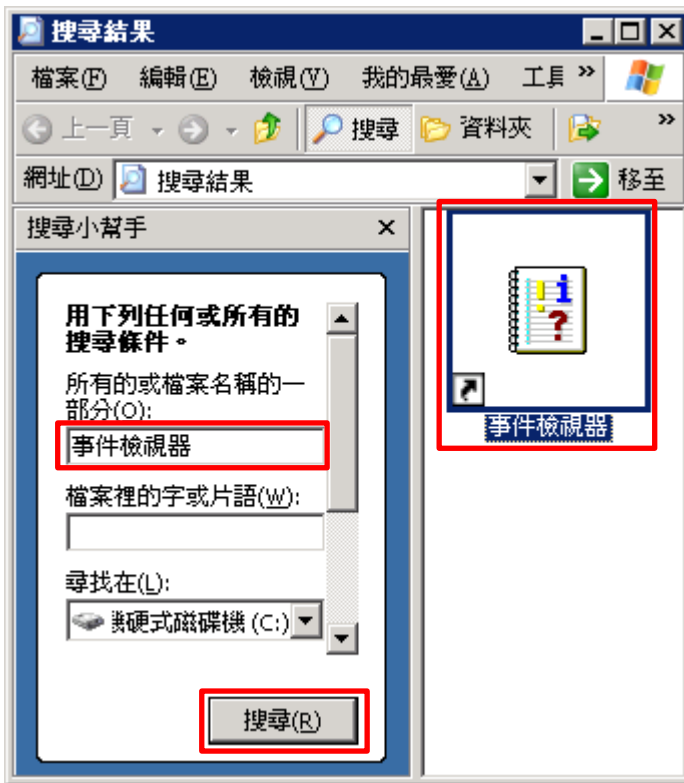
#### (1) 開啟搜尋

點選 [開始] -> [搜尋]



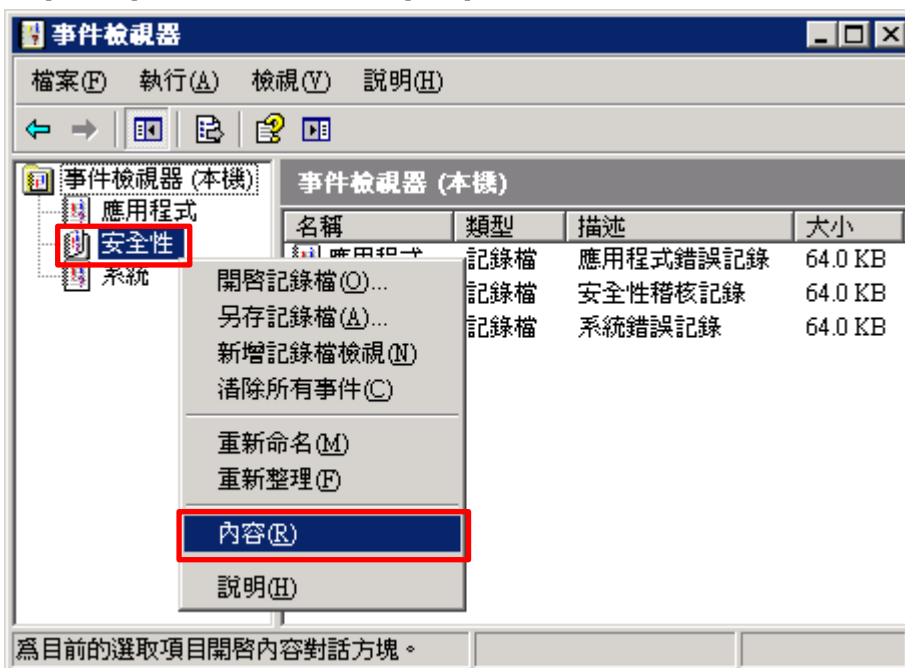
(2) 搜尋事件檢視器

輸入 **事件檢視器** -> 按 [搜尋] -> 點選 [事件檢視器]



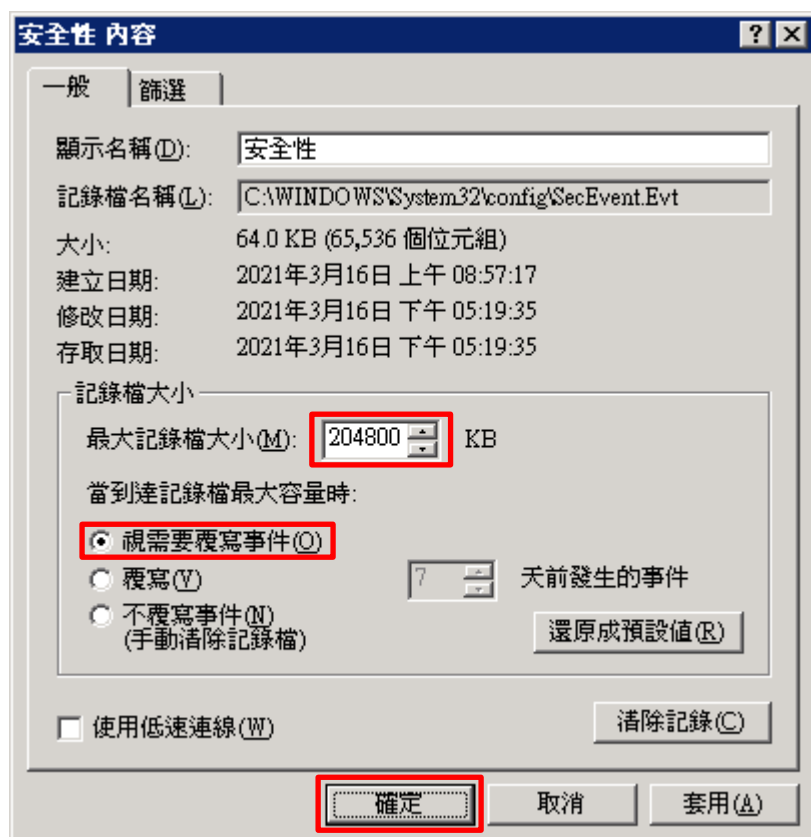
(3) 編輯安全性記錄

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

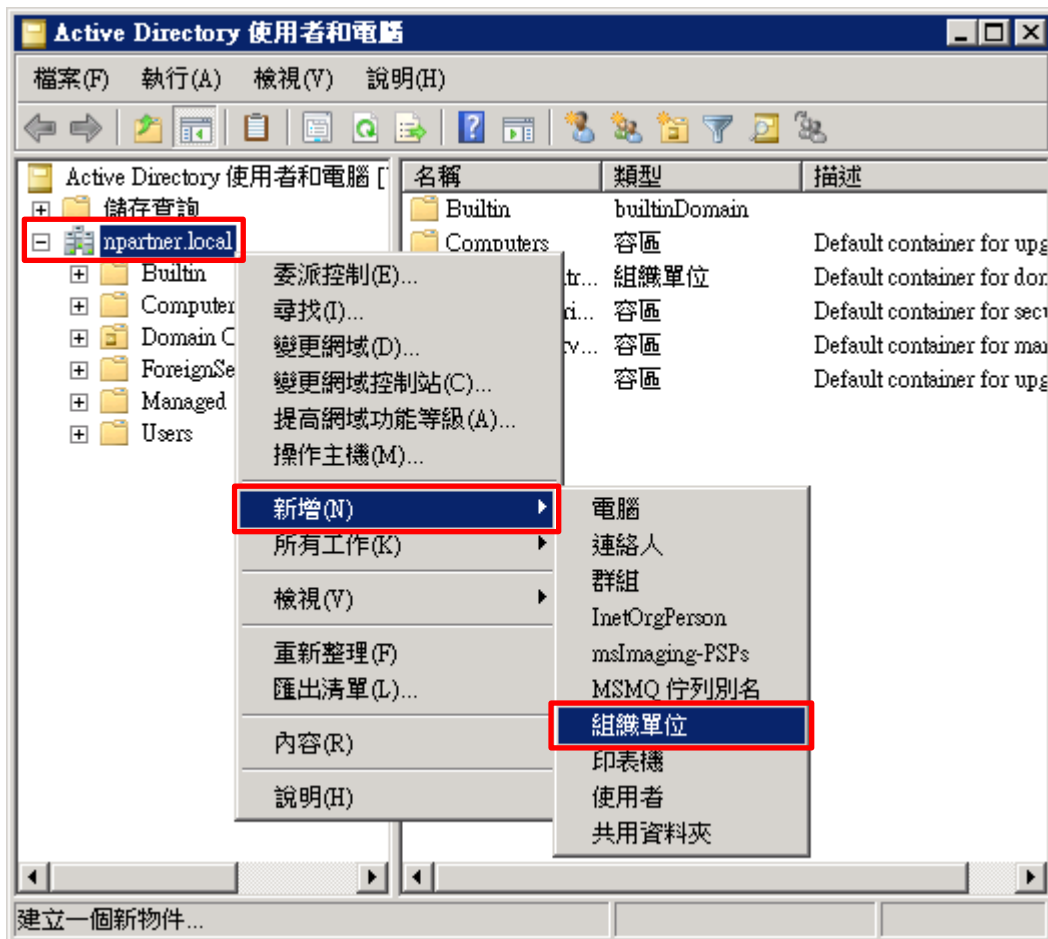
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



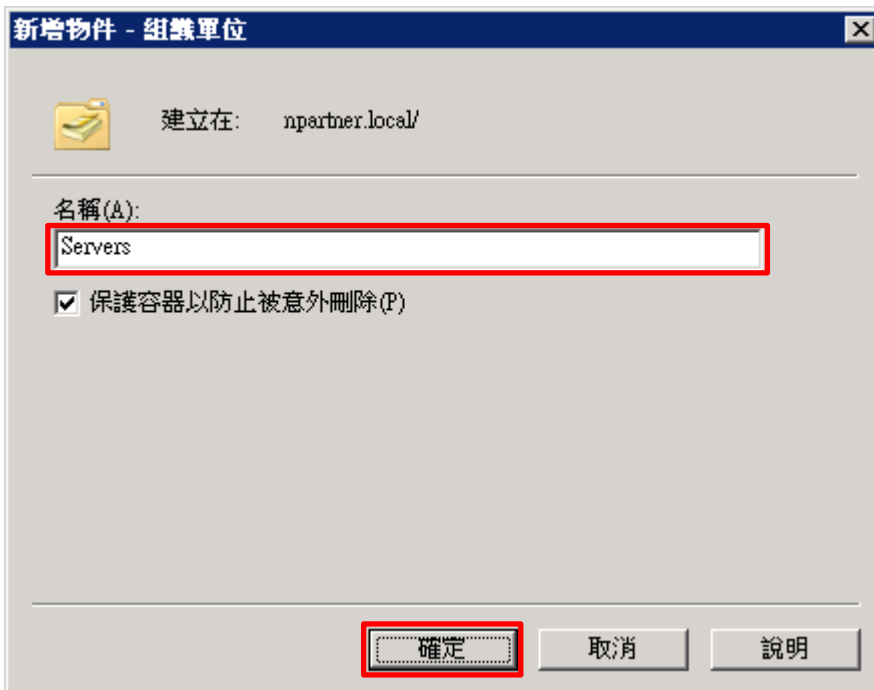
(2) 新增組織單位

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

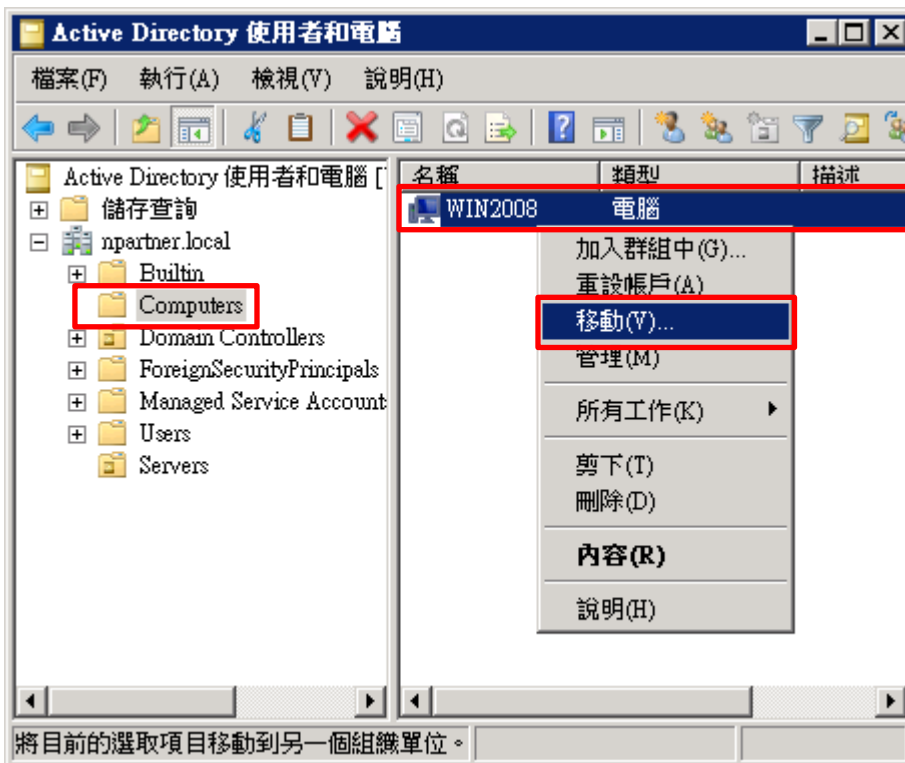
輸入組織單位名稱: Servers 註: 請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動伺服器至新的組織單位

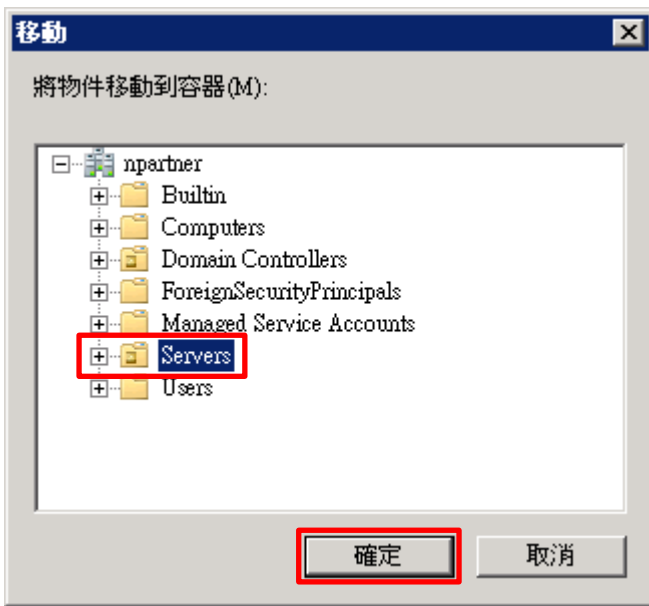
選擇 [Computers] 組織單位 -> 在 [Win2008] 伺服器, 按滑鼠右鍵, 註: 請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



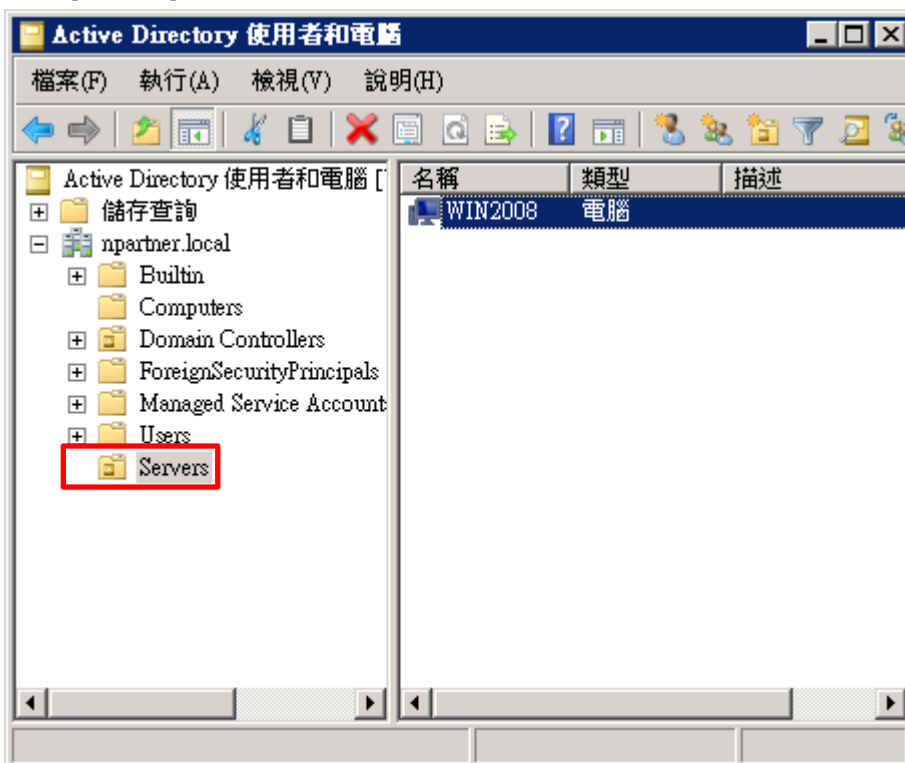
(5) 選擇組織單位

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

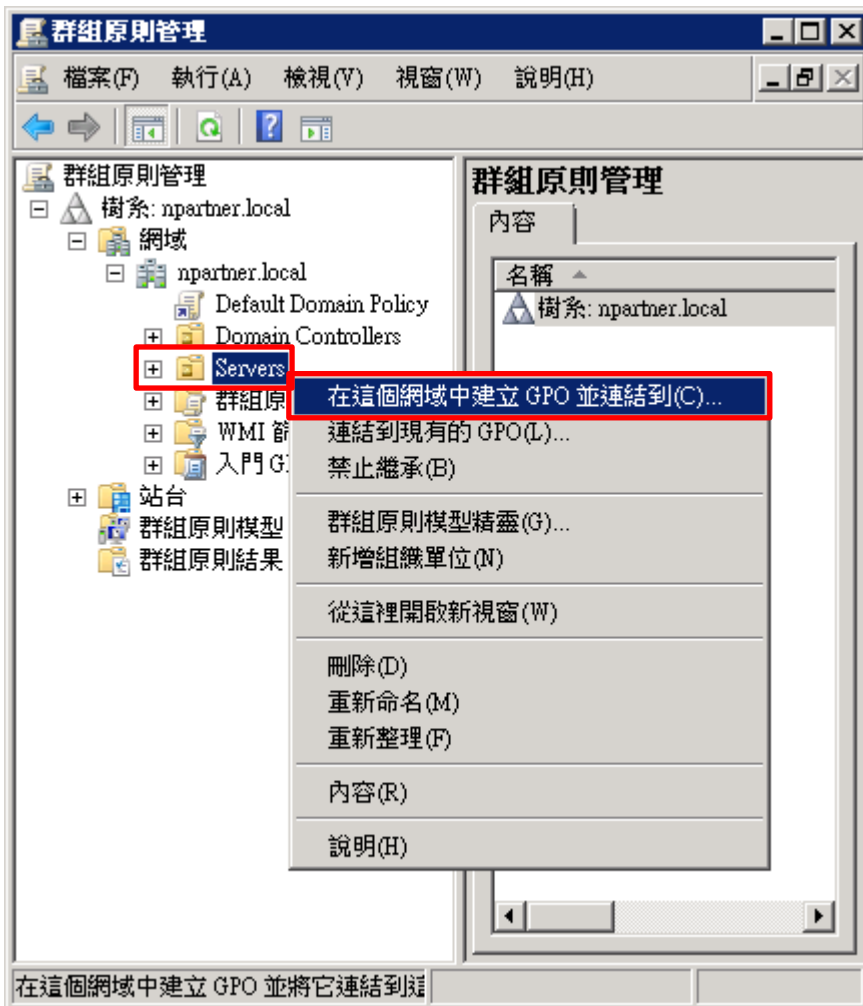
### (1) 開啟群組原則管理

開啟 [群組原則管理]



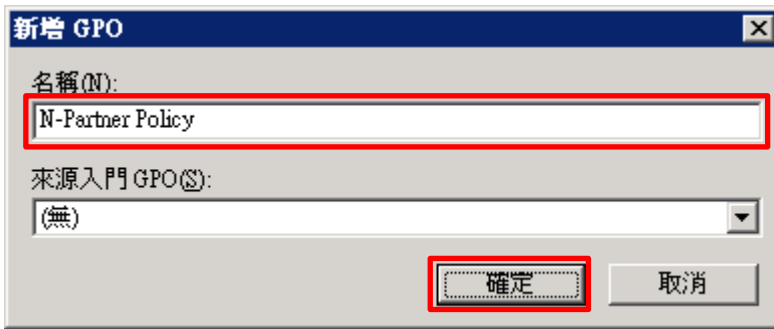
### (2) 在 Servers 組織單位，新增群組原則物件

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...]



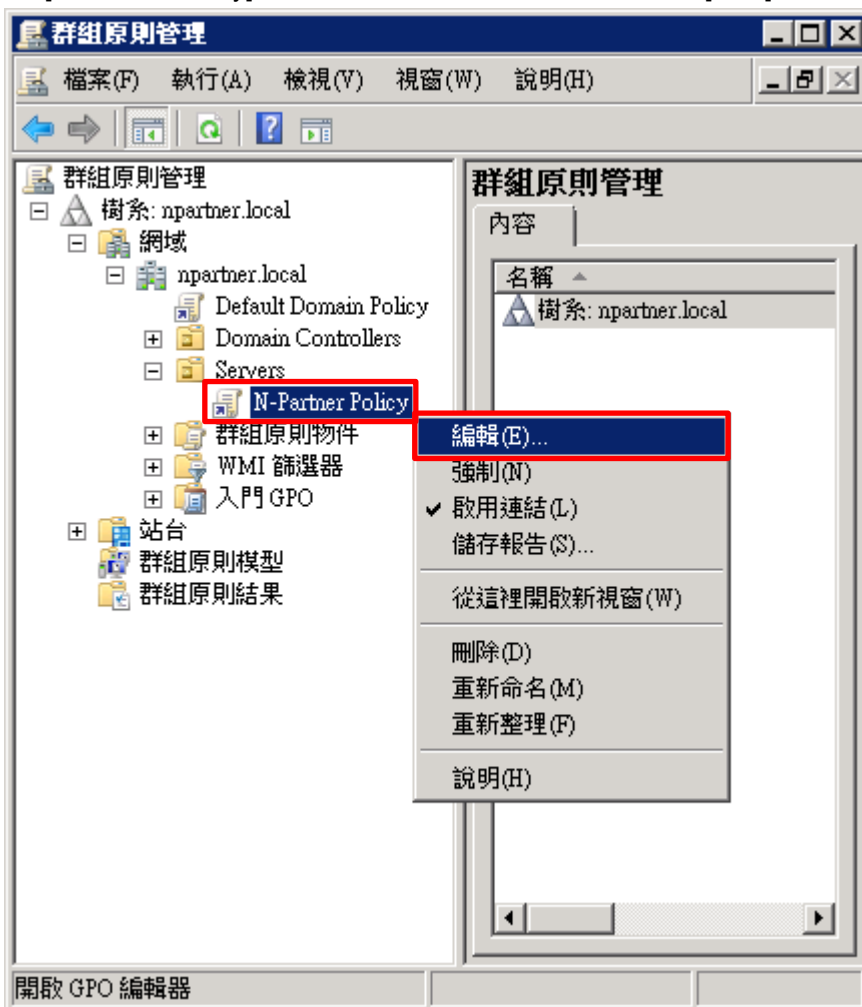
(3) 輸入群組原則物件名稱

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

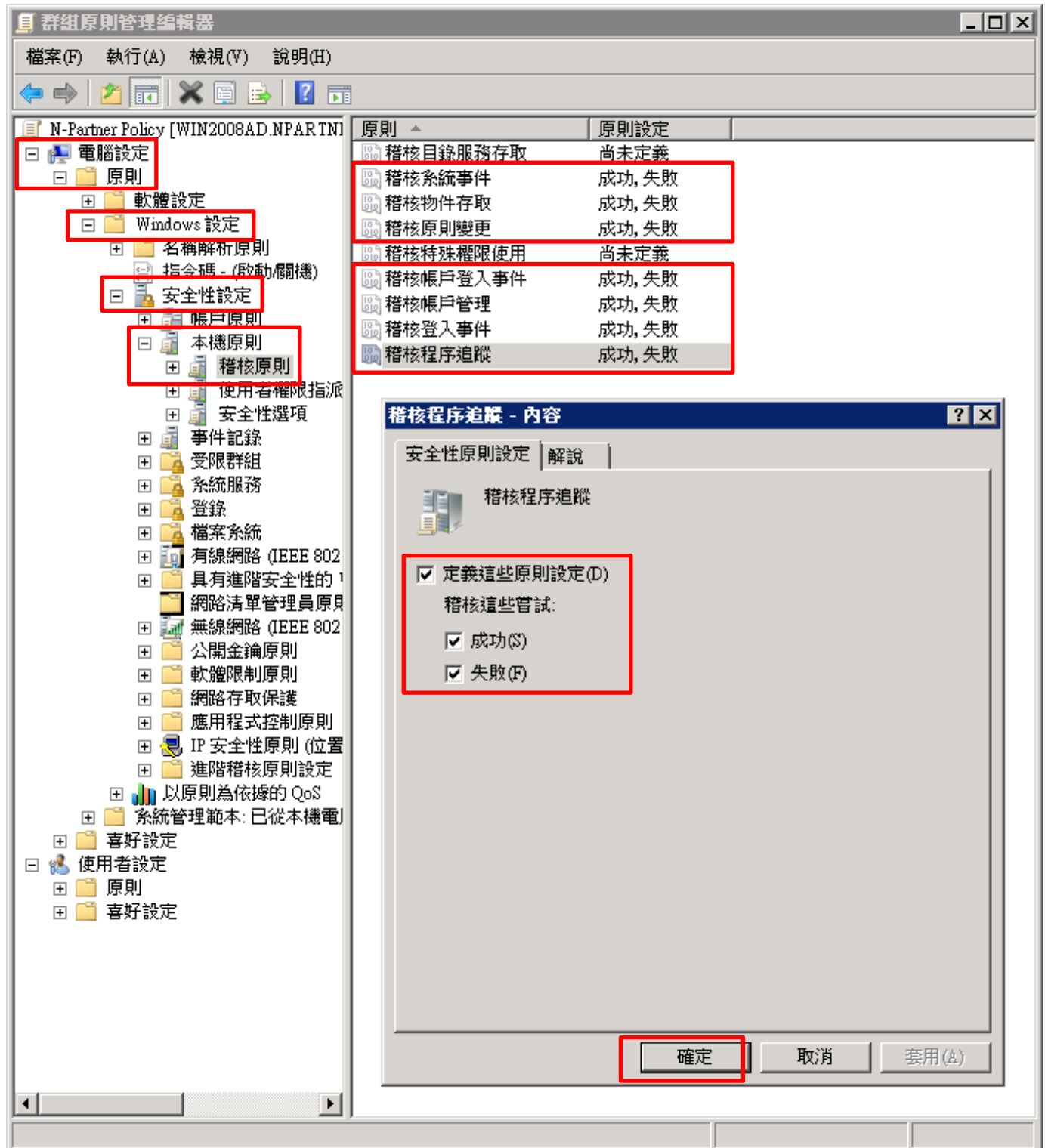
在 [N-Partner Policy] 群組原則物件，按滑鼠右鍵 -> 點選 [編輯]





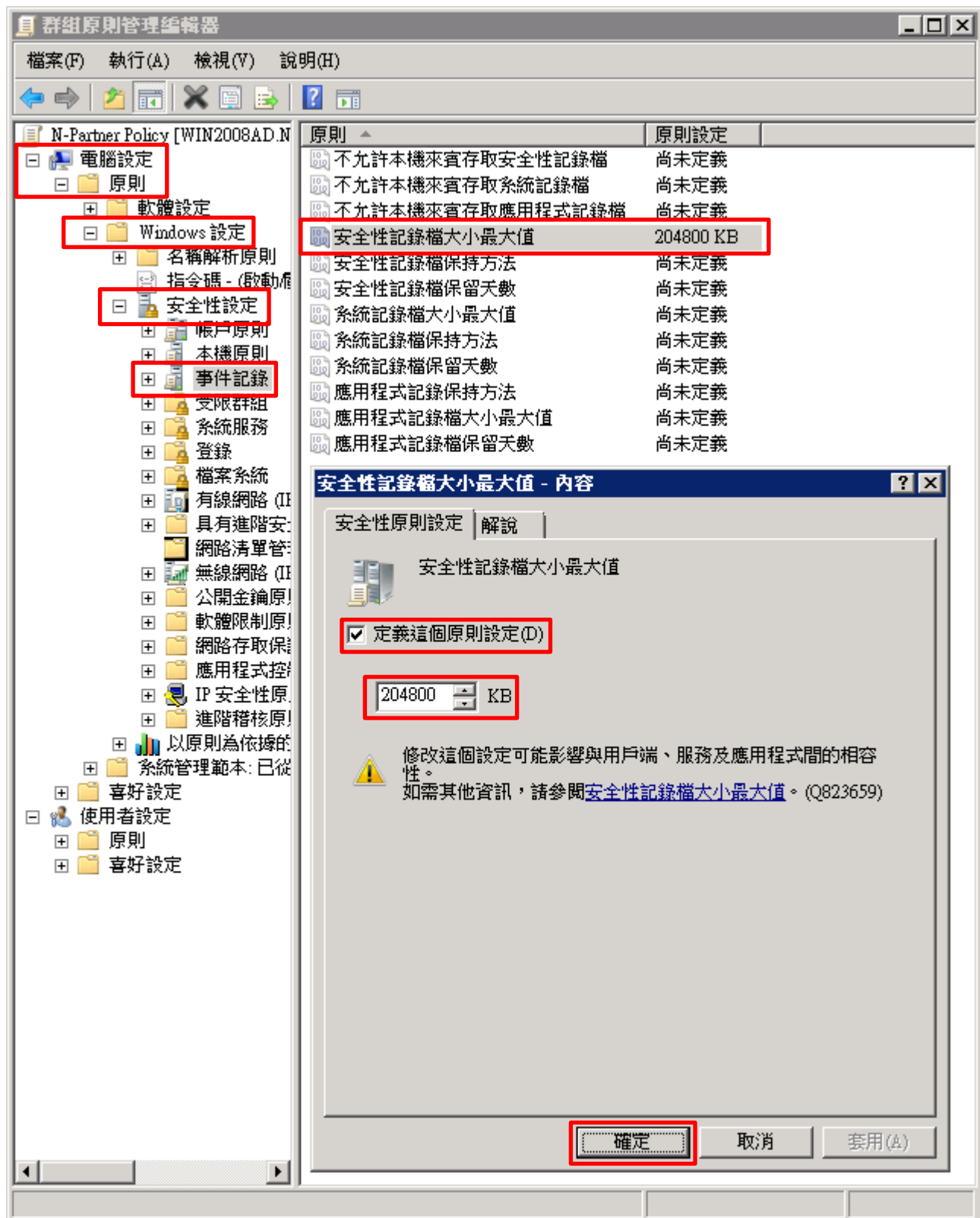
(5) 本機原則：稽核原則

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]



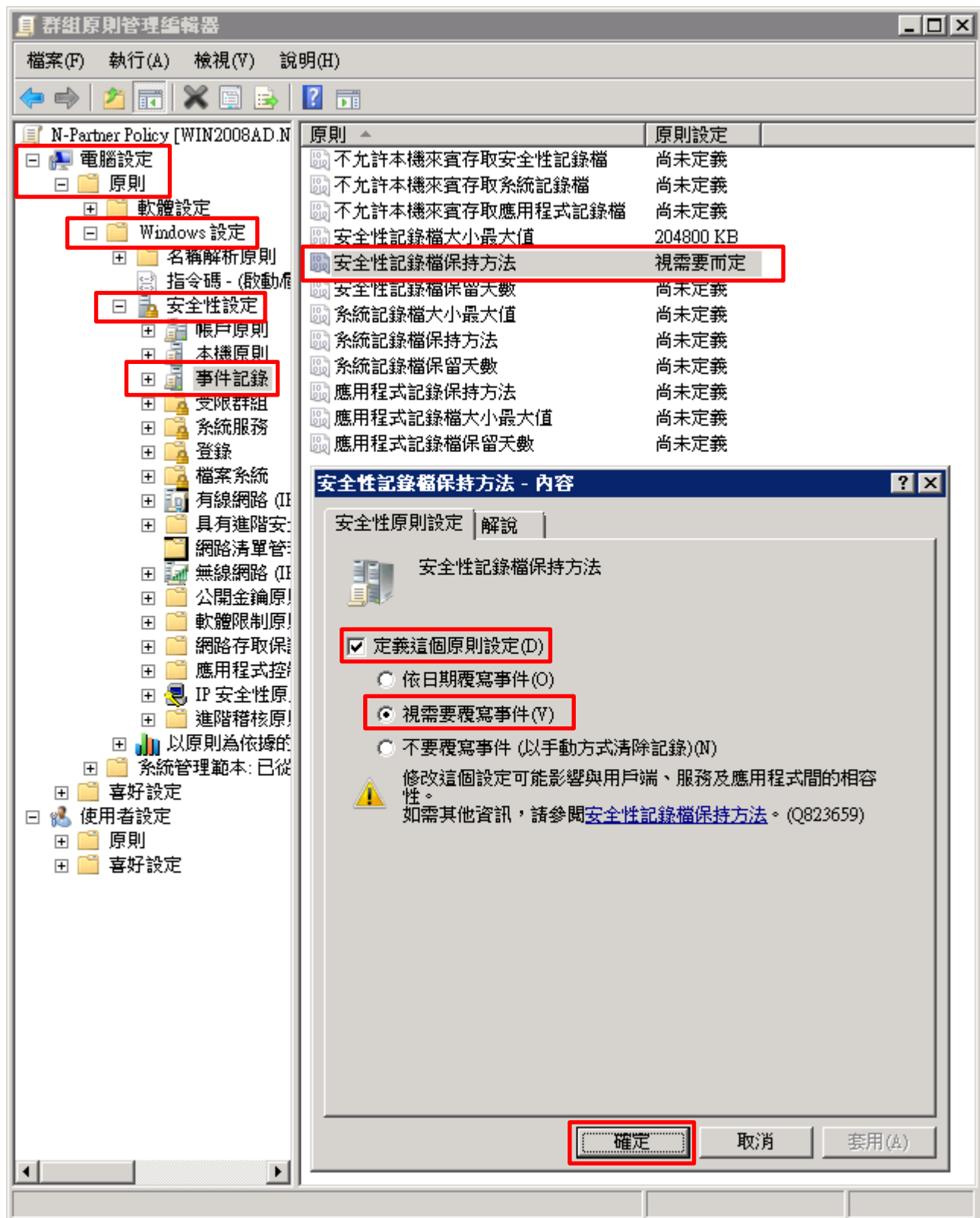
(6) 事件記錄：安全性記錄檔大小最大值

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

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

(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

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command "PS C:\> Get-GPResultantSetofPolicy -Computer Win2008 -Path C:\tmp\Win2008.html -ReportType html" being entered. The output is a list of properties: "RsopMode : Logging", "Namespace : \\Win2008\Root\Rsop\NSF08D1398\_6CC3\_45C1\_8274\_5DD9E6292858", "LoggingComputer : Win2008", "LoggingUser : NPARTNER\administrator", and "LoggingMode : Computer". The prompt "PS C:\> " is visible at the bottom of the terminal.

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

**群組原則結果**

**NPARTNER\WIN2008**  
資料收集: 2022/8/18 下午 01:28:52

**摘要** 顯示全部

**電腦設定** 隱藏

**原則** 隱藏

**Windows 設定** 隱藏

**安全性設定** 隱藏

**帳戶原則/密碼規則** 顯示

**帳戶原則/帳戶鎖定原則** 顯示

**本機原則/稽核原則** 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy

**本機原則/安全性選項** 顯示

**事件記錄檔** 隱藏

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

**公開金鑰原則/憑證服務用戶端 - 自動註冊設定** 顯示

**公開金鑰原則/加密檔案系統** 顯示

**公開金鑰原則/被信任的根憑證授權單位** 顯示

**使用者設定** 顯示

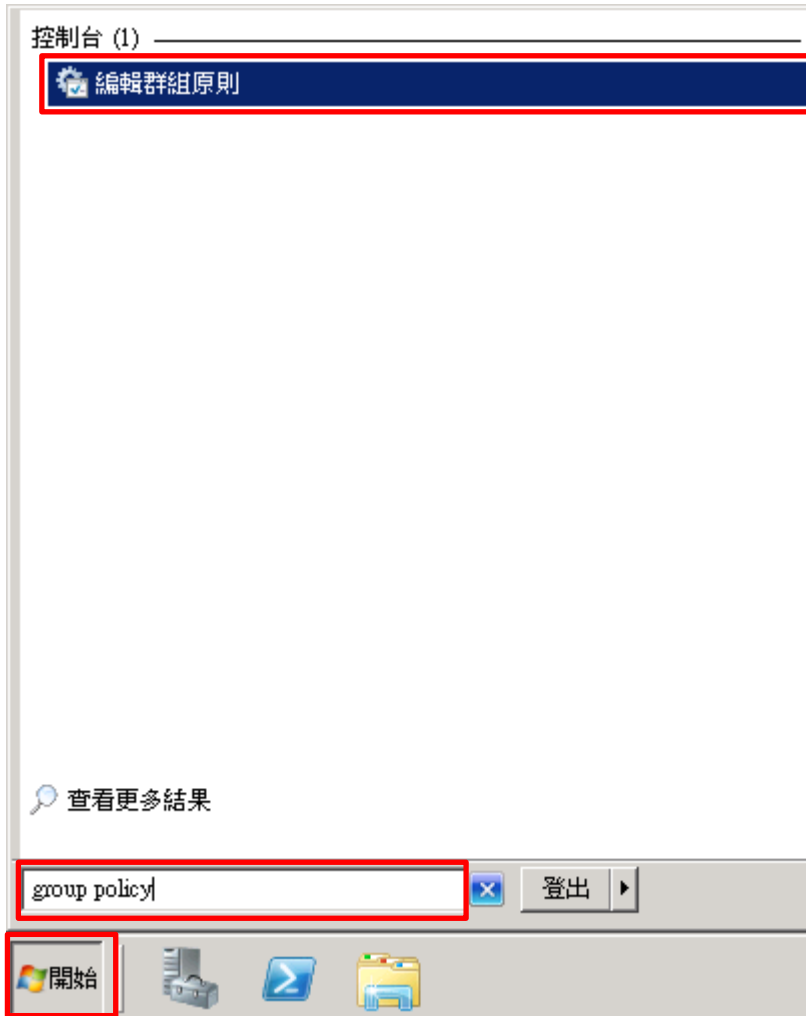
電腦 | 受保護模式: 關閉

## 4.2 工作群組

### 4.2.1 稽核原則設定

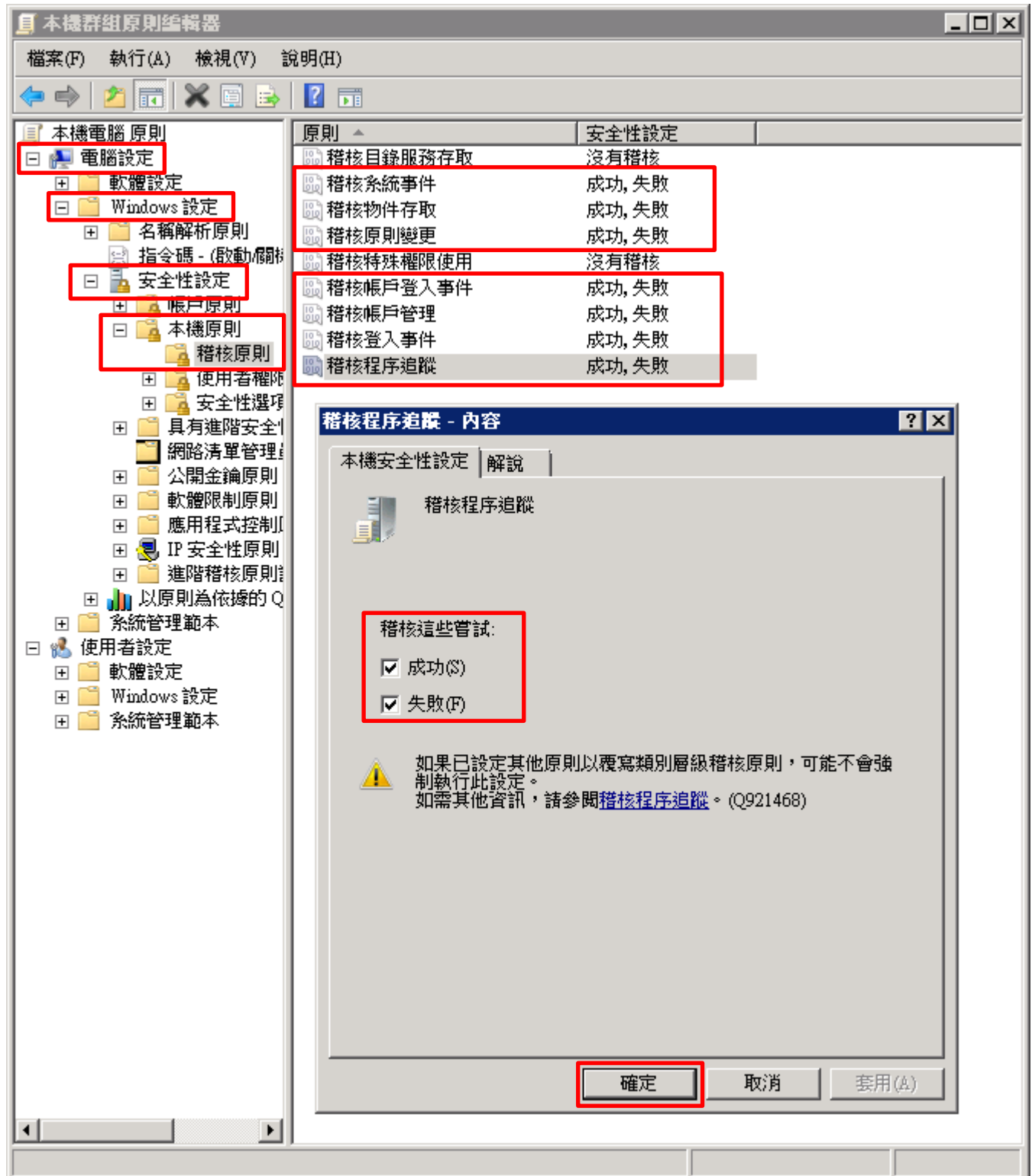
(1) 開啟 [本機群組原則編輯器]

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

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

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

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

使用者原則更新已成功完成。
電腦原則更新已成功完成。

PS C:\Users\Administrator> _
```



(5) 查看群組原則套用情形

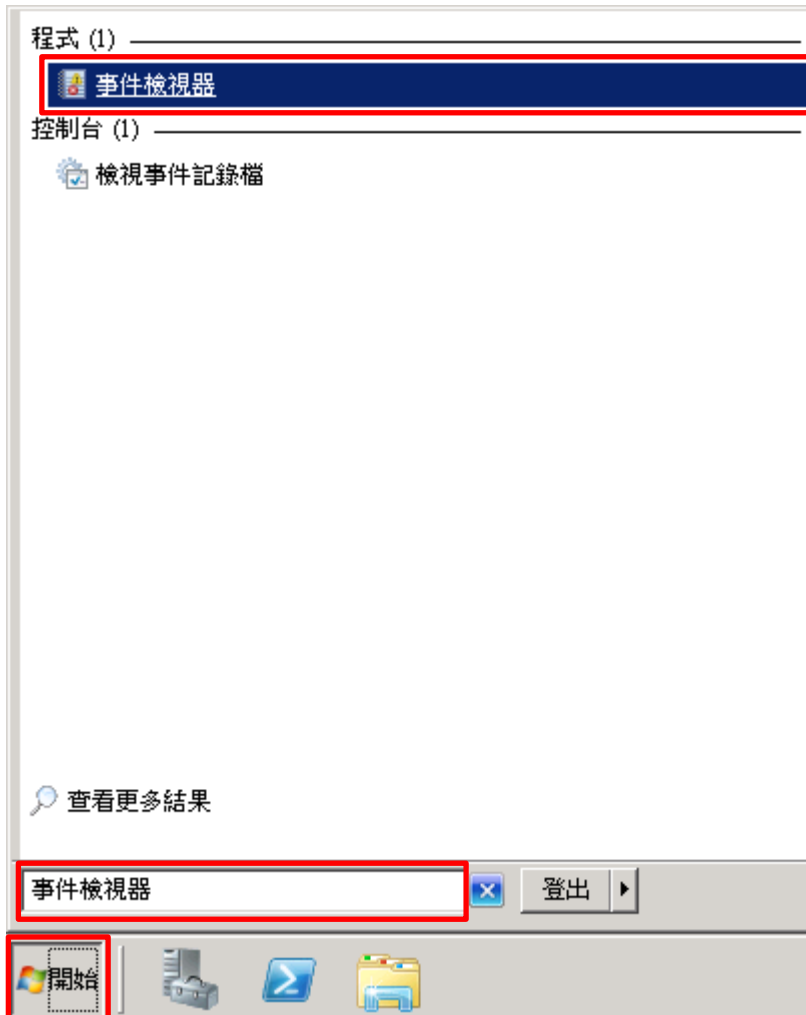
PS C:\> auditpol /get /category:\*

```
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
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
  MPSSUC 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

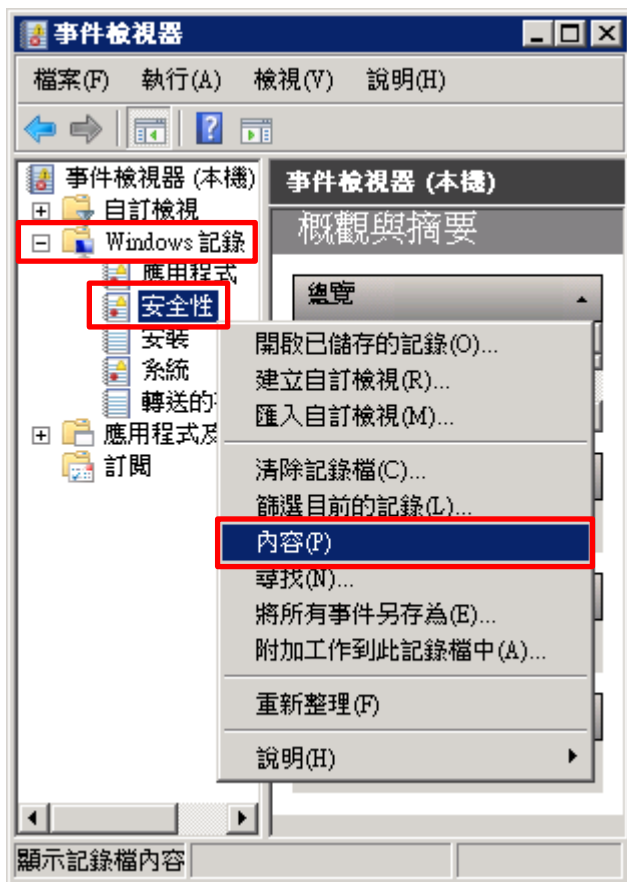
(1) 開啟 [事件檢視器]

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]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

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

記錄檔大小: 3.07 MB(3,215,360 位元組)

建立日期: 2021年3月17日 下午 06:23:54

修改日期: 2021年3月17日 上午 11:42:37

存取日期: 2021年3月17日 下午 06:23:54

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄檔(R)

確定 取消 套用(P)

## 5. Windows 2012

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

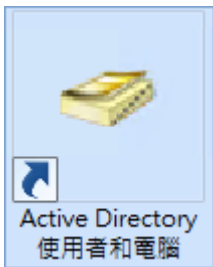
※ 以下分別為網域和工作群組設定方式。

### 5.1 網域

#### 5.1.1 組織單位設定

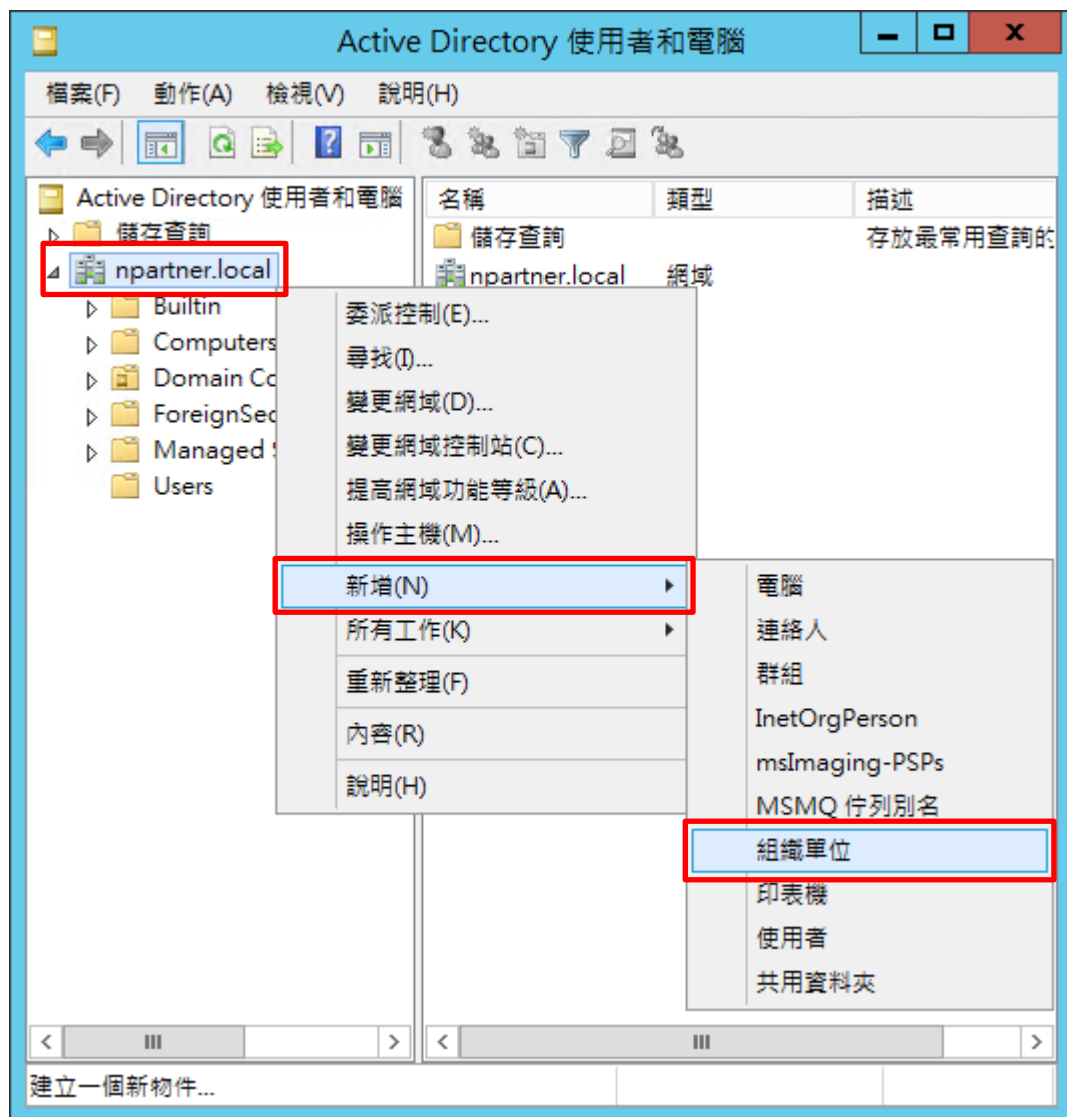
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



## (2) 新增組織單位

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



(3) 輸入組織單位名稱

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

新增物件 - 組織單位

建立於: npartner.local/

名稱(A):  
Servers

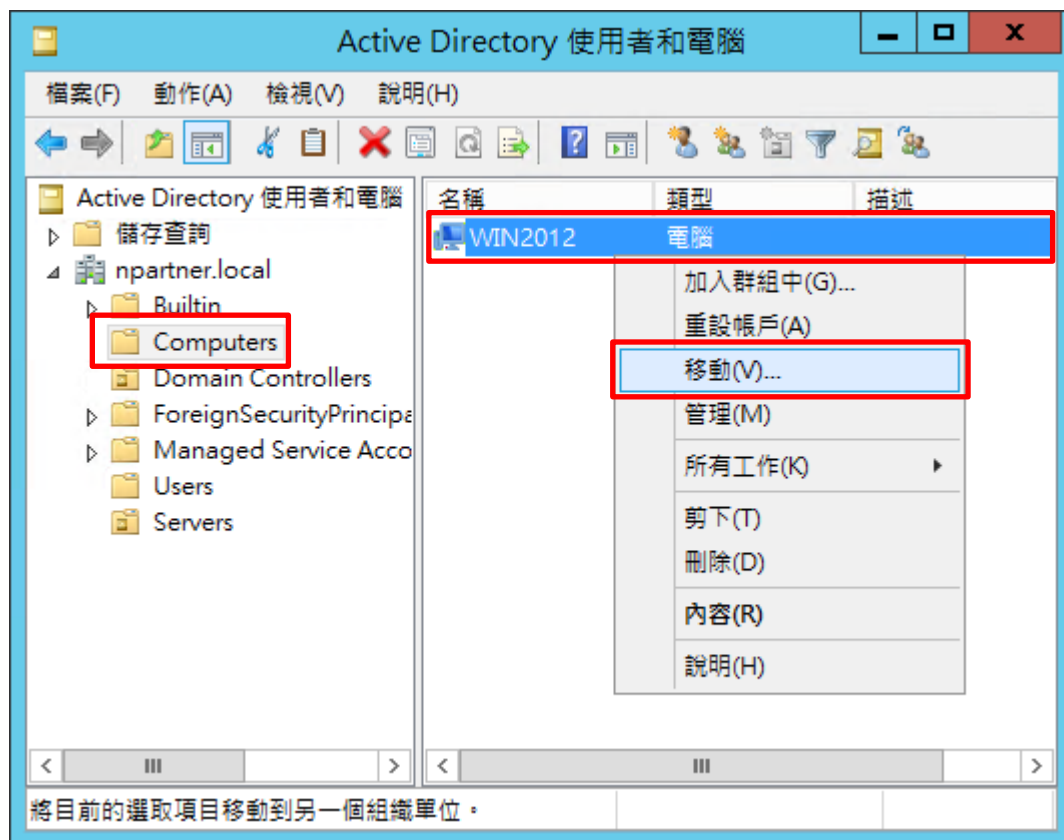
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

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

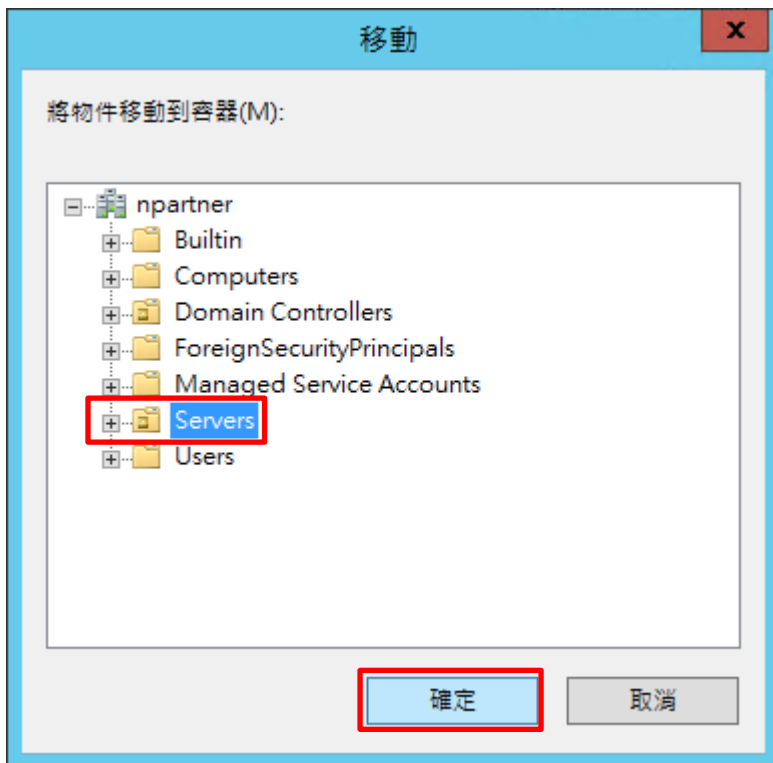
-> 點選 [移動]





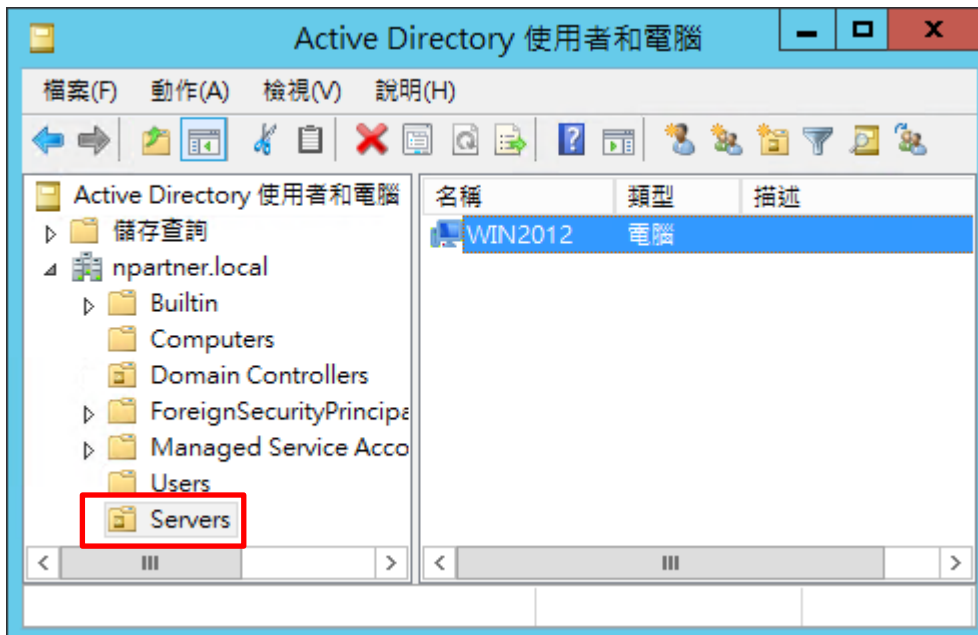
(5) 選擇組織單位

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

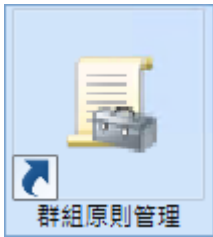
點選 [Servers] 組織單位，確認 Win2012 伺服器已移動。



## 5.1.2 群組原則設定

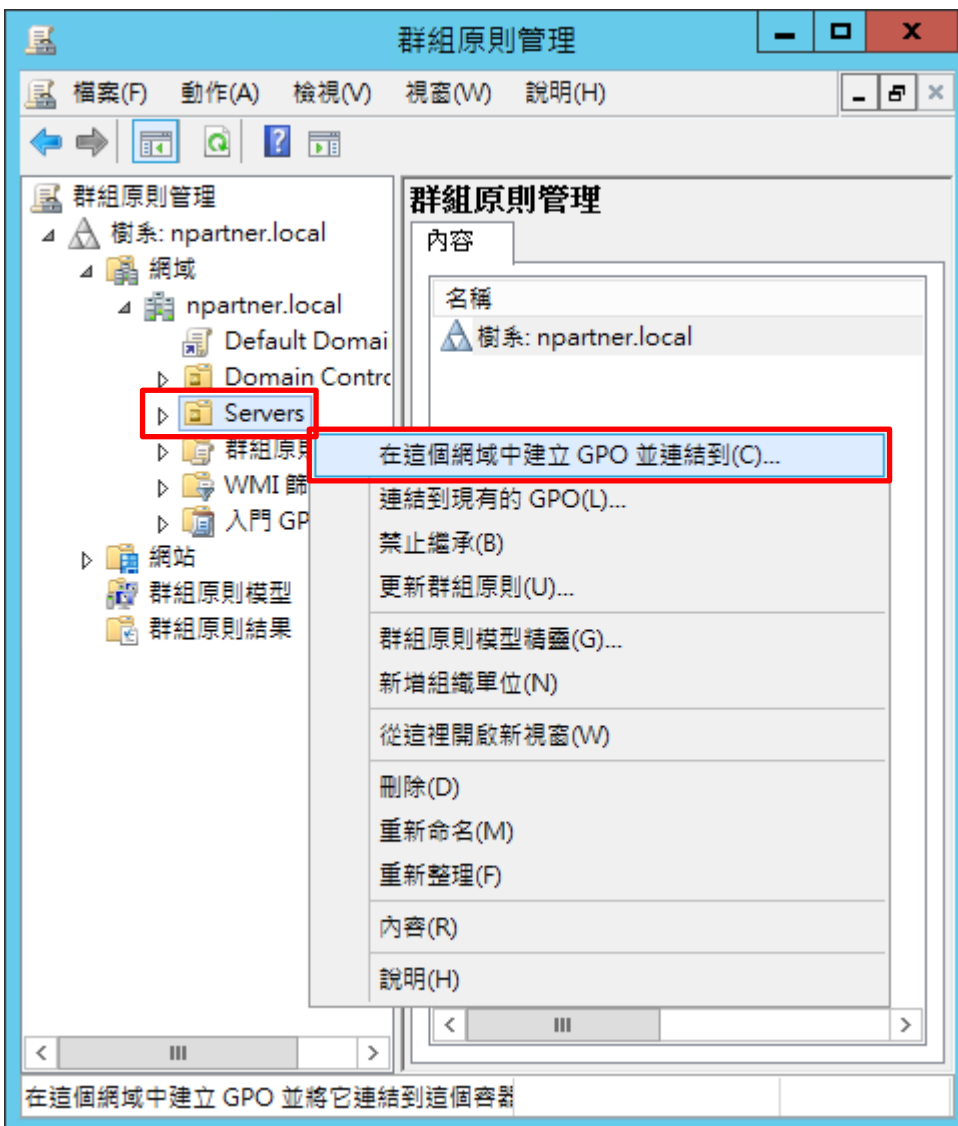
### (1) 開啟群組原則管理

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...]



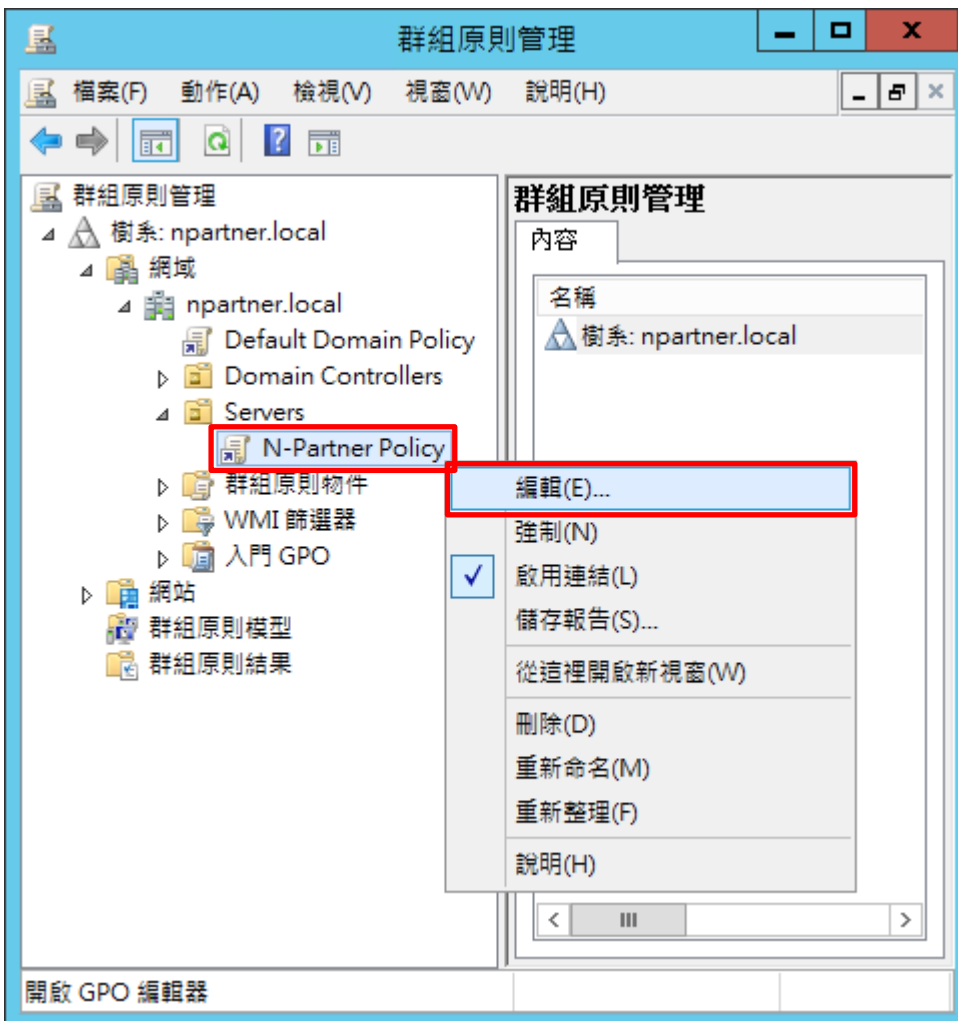
(3) 輸入群組原則物件名稱

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]



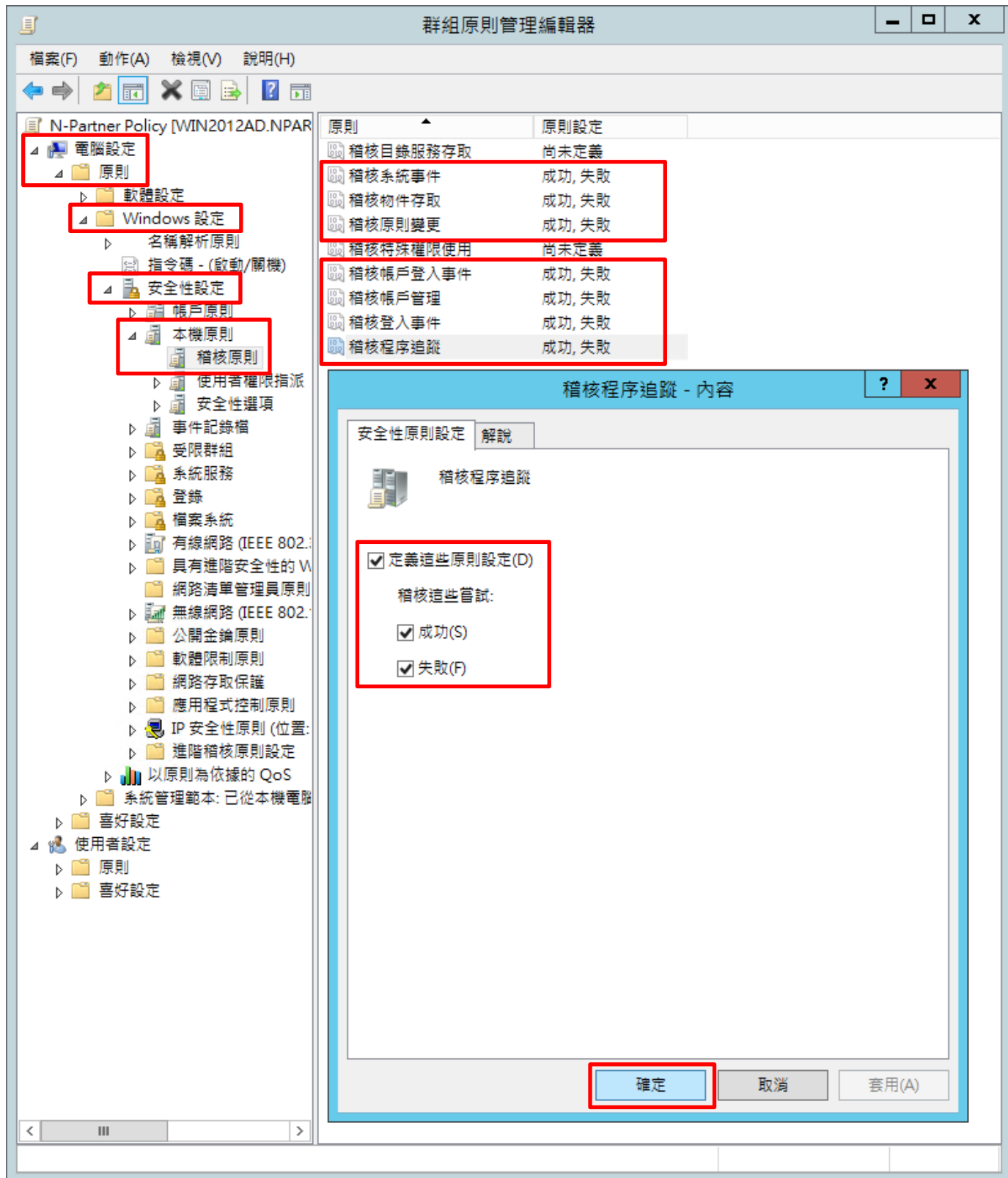
(4) 編輯群組原則物件

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



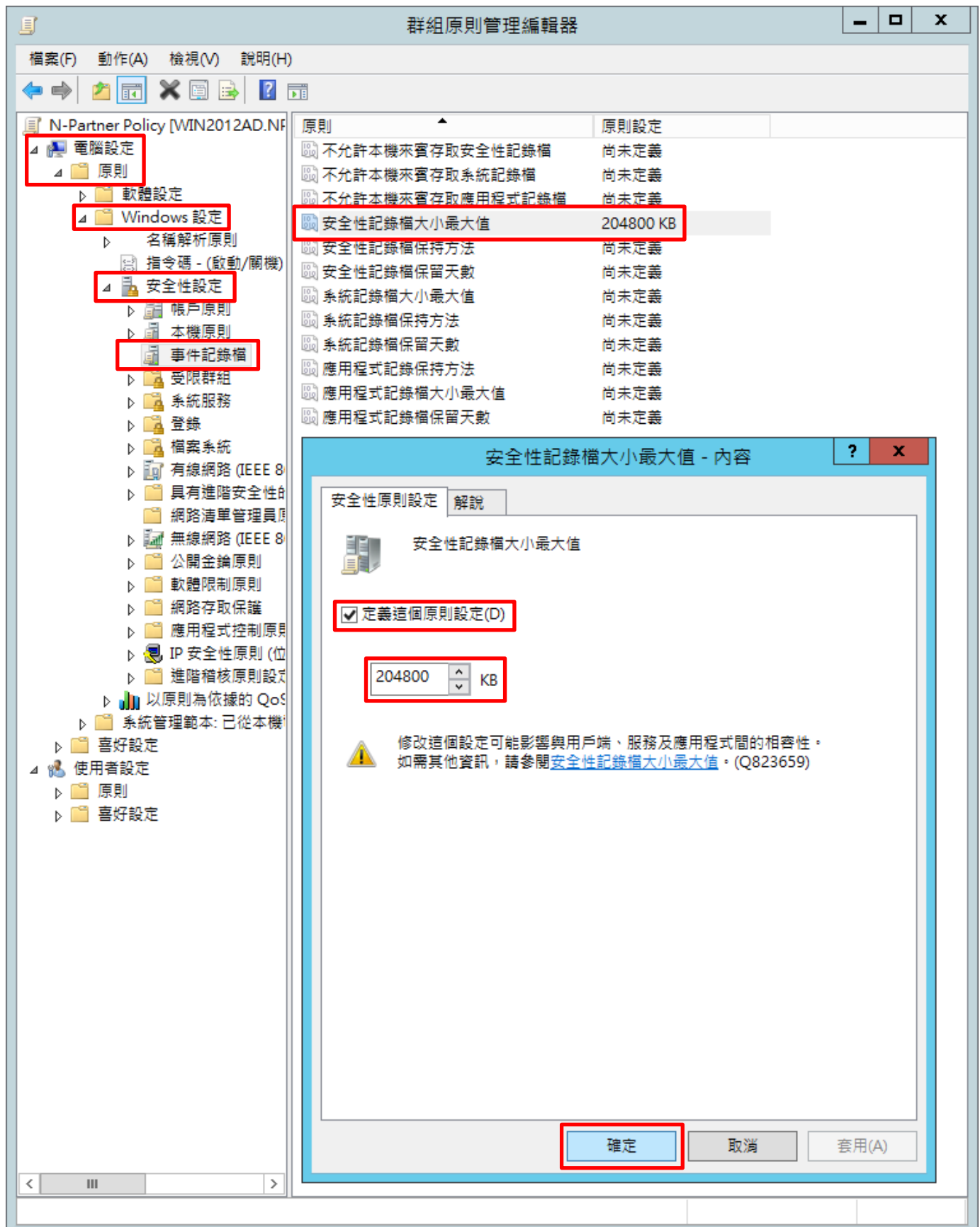
(5) 本機原則：稽核原則

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]



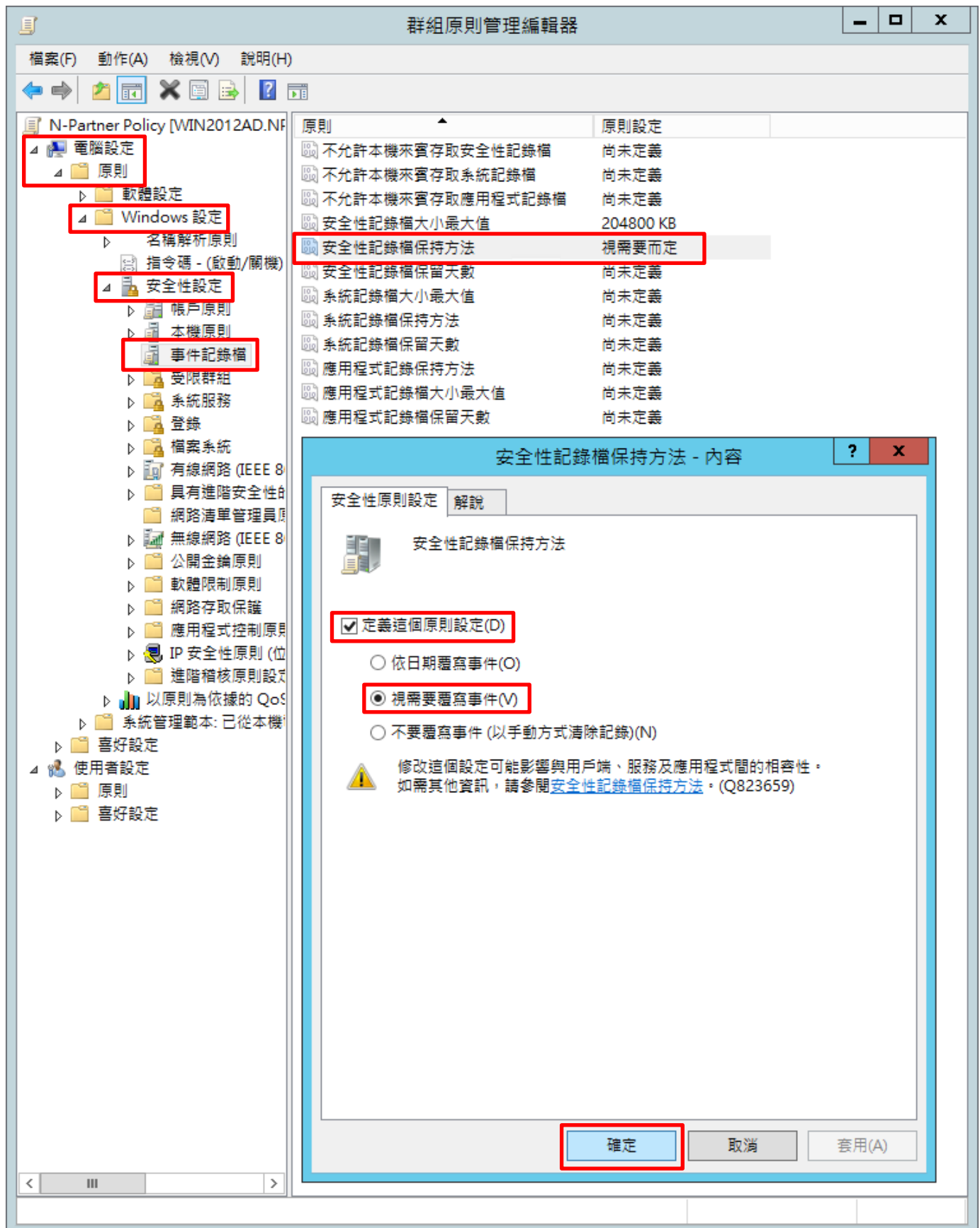
(6) 事件記錄檔：安全性記錄檔大小最大值

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]

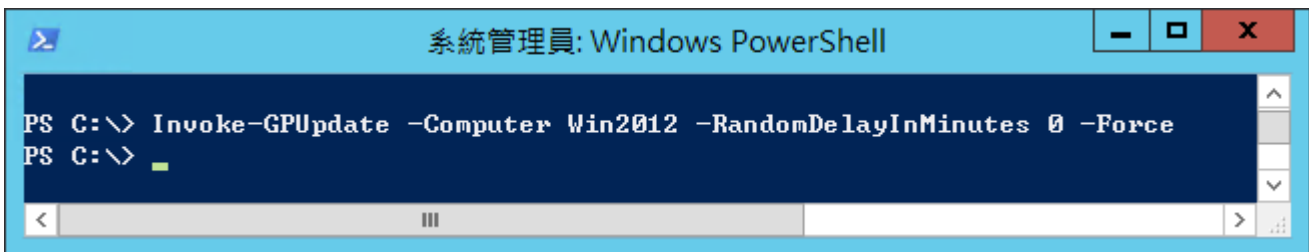


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



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

```
PS C:\> Invoke-GPUdate -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

**群組原則結果**

**NPARTNER\WIN2012**  
資料收集: 2022/8/18 下午 12:15:02

**摘要** 顯示全部

**電腦詳細資料** 顯示

- 一般 顯示
- 元件狀態 顯示
- 設定 隱藏
- 原則** 隱藏
  - Windows 設定** 隱藏
    - 安全性設定** 隱藏
      - 帳戶原則/密碼規則 顯示
      - 帳戶原則/帳戶鎖定原則 顯示
      - 本機原則/稽核原則** 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy
      - 本機原則/安全性選項** 顯示
      - 事件記錄檔** 隱藏

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



## 5.2 工作群組

### 5.2.1 稽核原則設定

#### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



#### (2) 搜尋群組原則物件編輯器並執行

輸入 群組原則 -> 點選 [編輯群組原則]



### (3) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [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]

The screenshot shows the Windows Security application with the 'Local Policies' section expanded. The 'Audit Policy' folder is selected, and the following policies are listed in the main pane:

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

The 'Audit Program Tracking - Content' dialog box is open, showing the 'Audit these attempts' section with the following options checked:

- 成功(S)
- 失敗(F)

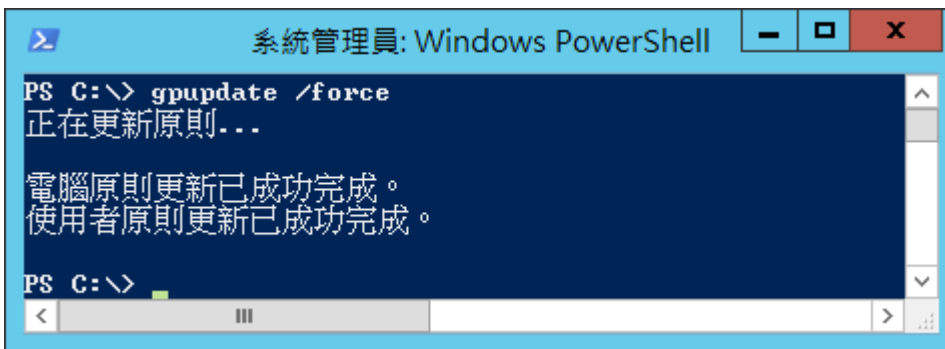
The 'Confirm' button is highlighted in red.

(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

PS C:\> gpupdate /force



(6) 查看群組原則套用情形

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

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

## 5.2.2 事件檔案設定

### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



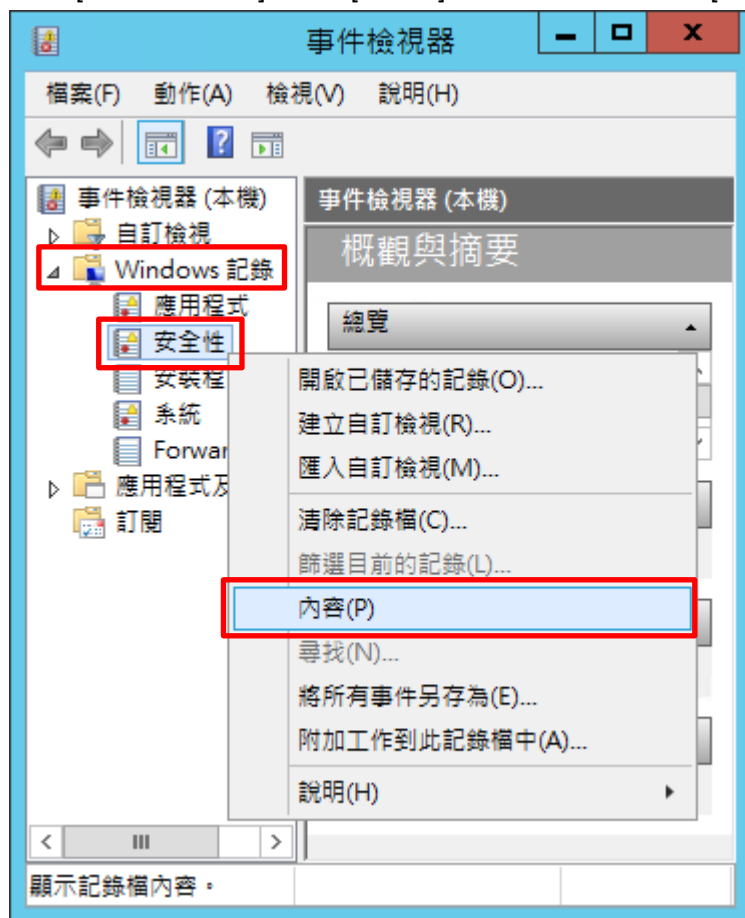
### (2) 搜尋事件檢視器並執行

輸入事件檢視器 -> 點選 [事件檢視器]



### (3) 編輯安全性記錄

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



(4) 設定安全性記錄檔

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

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

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

記錄檔大小: 3.07 MB(3,215,360 位元組)

建立日期: 2021年3月17日 21:40:56

修改日期: 2021年3月17日 15:00:01

存取日期: 2021年3月17日 21:40:56

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

確定 取消 套用(P)

## 6. Windows 2016

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

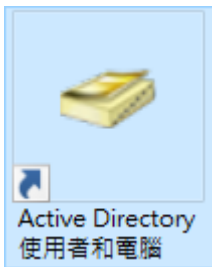
※ 以下分別為網域和工作群組設定方式。

### 6.1 網域

#### 6.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

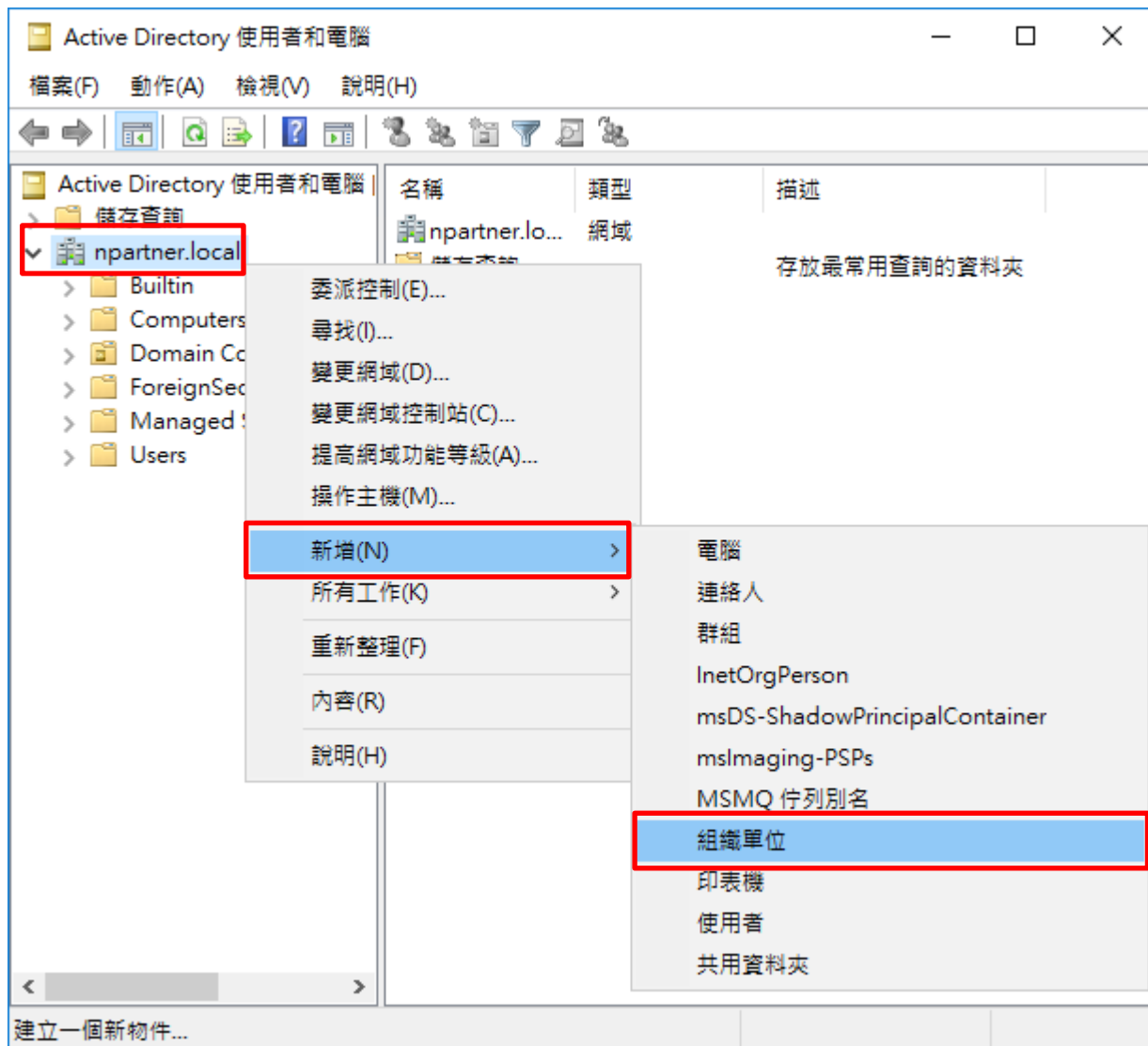
開啟 [Active Directory 使用者和電腦]





## (2) 新增組織單位

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



(3) 輸入組織單位名稱

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

新增物件 - 組織單位

建立在: npartner.local/

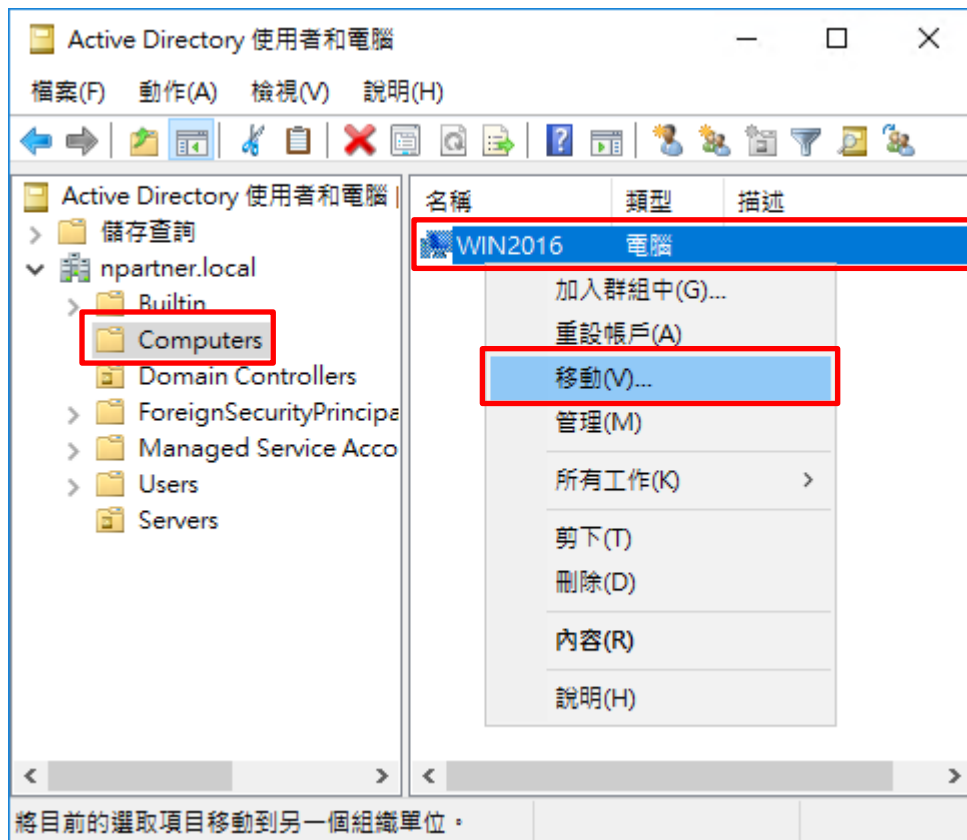
名稱(A):  
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

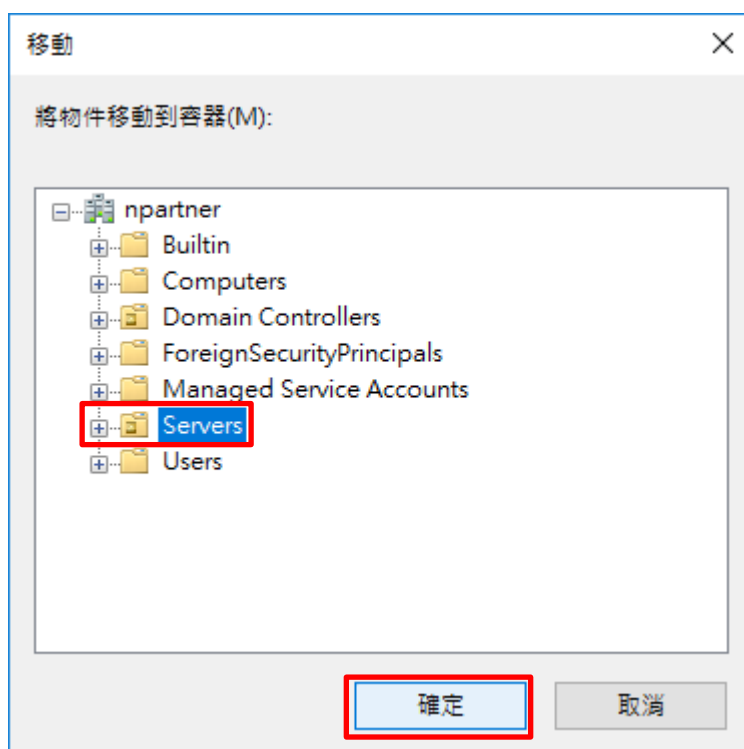
(4) 移動伺服器至新的組織單位

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



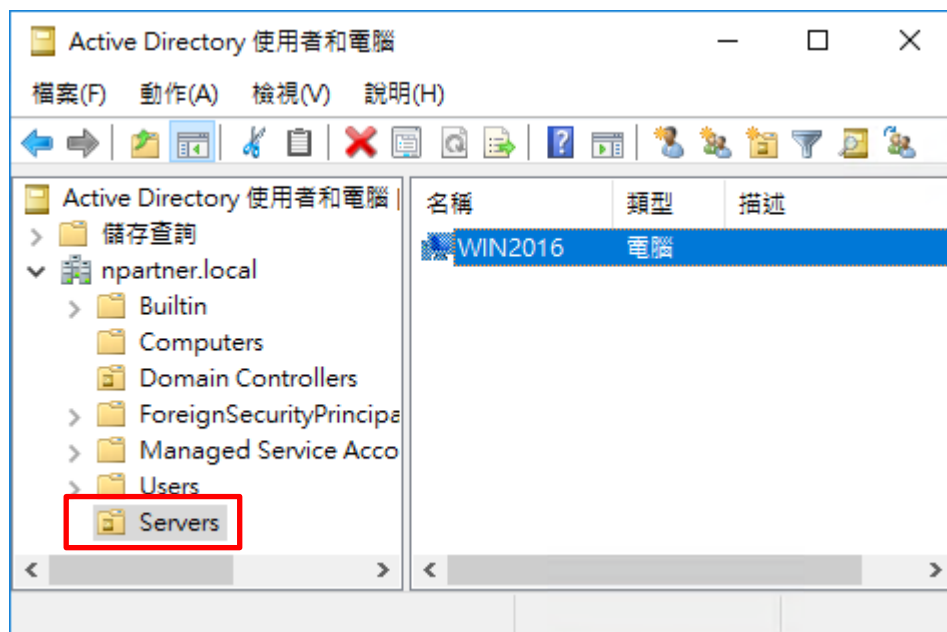
(5) 選擇組織單位

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

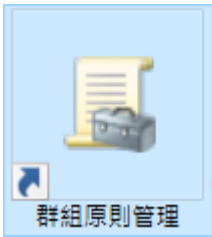
點選 [Servers] 組織單位，確認 Win2016 伺服器已移動。



## 6.1.2 群組原則設定

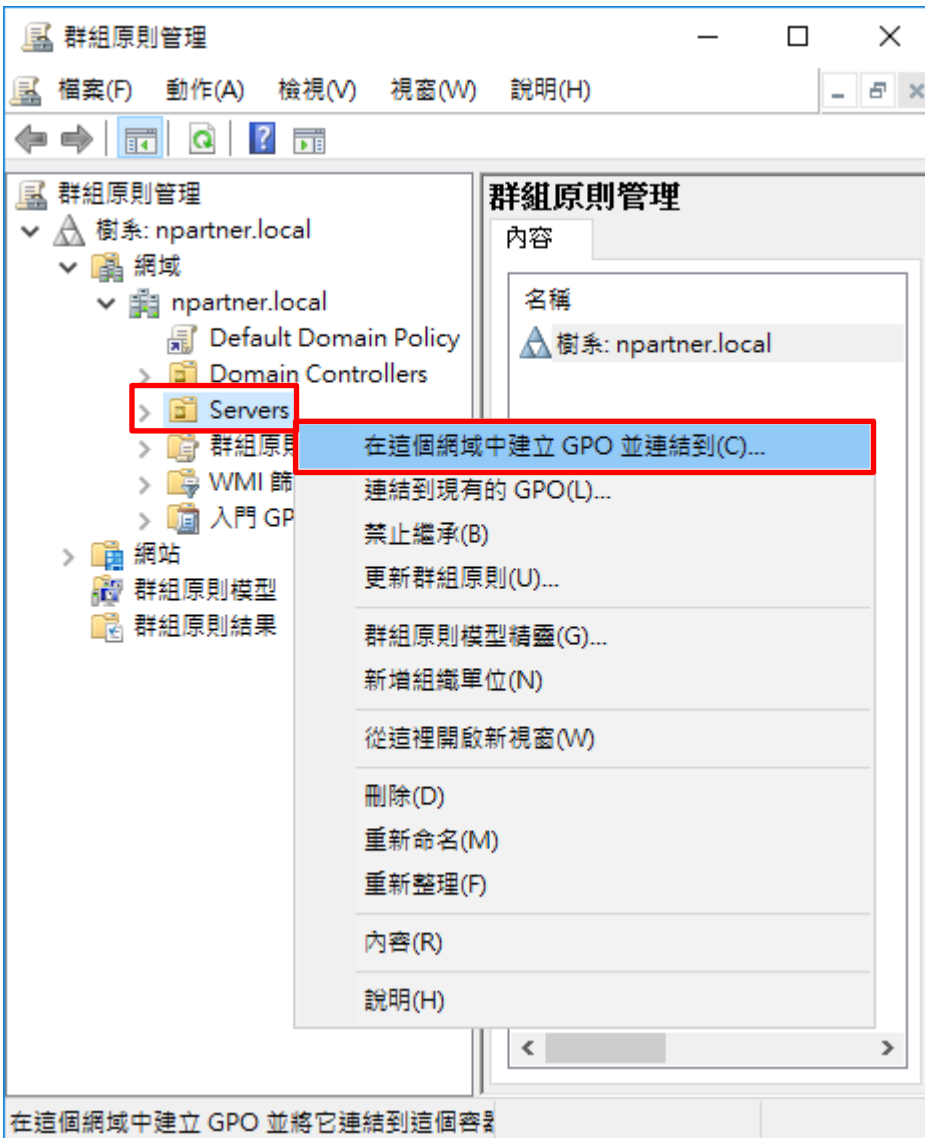
### (1) 開啟群組原則管理

開啟 [群組原則管理]



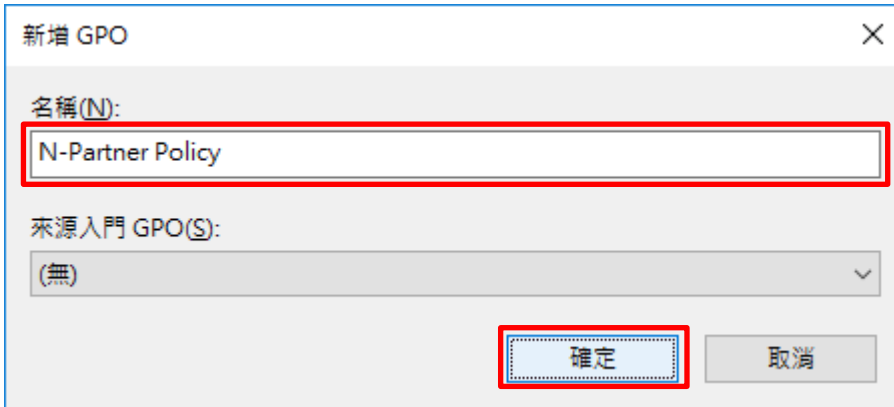
### (2) 在 Servers 組織單位，新增群組原則物件

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...]



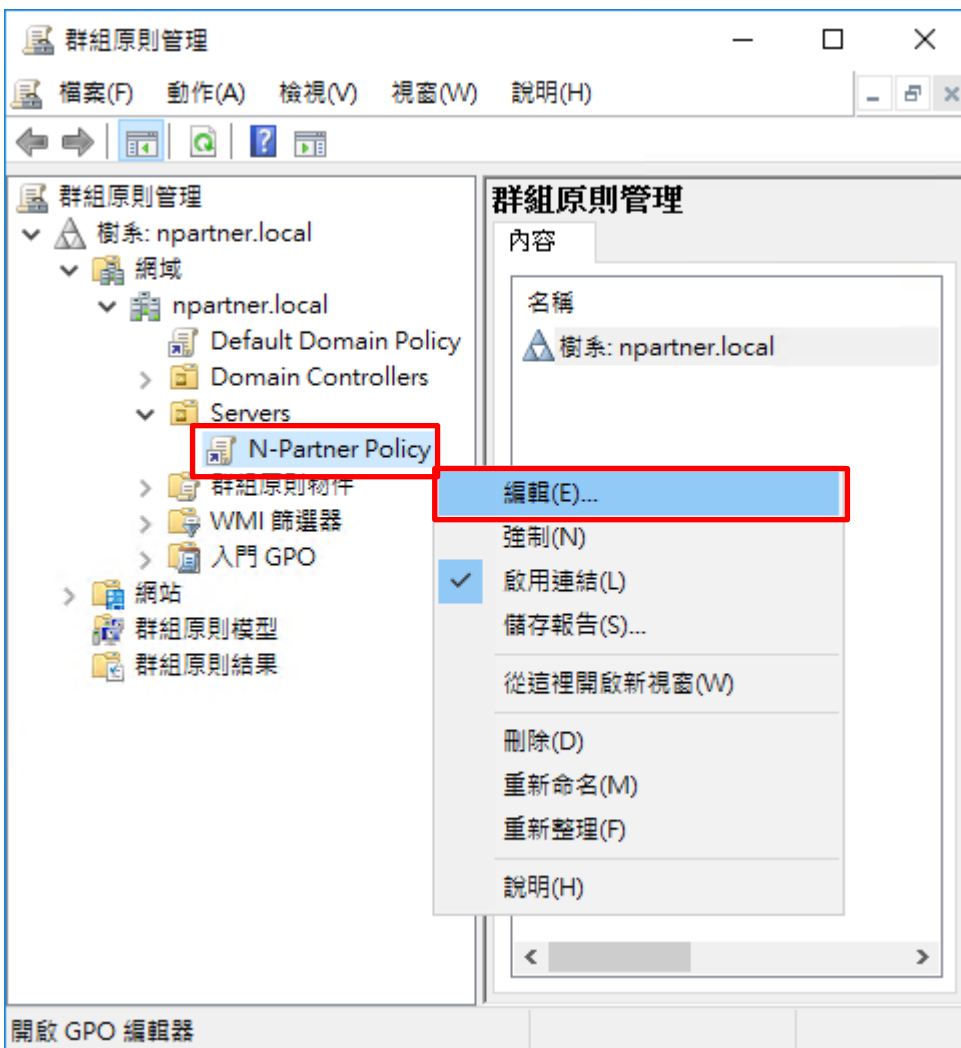
(3) 輸入群組原則物件名稱

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]



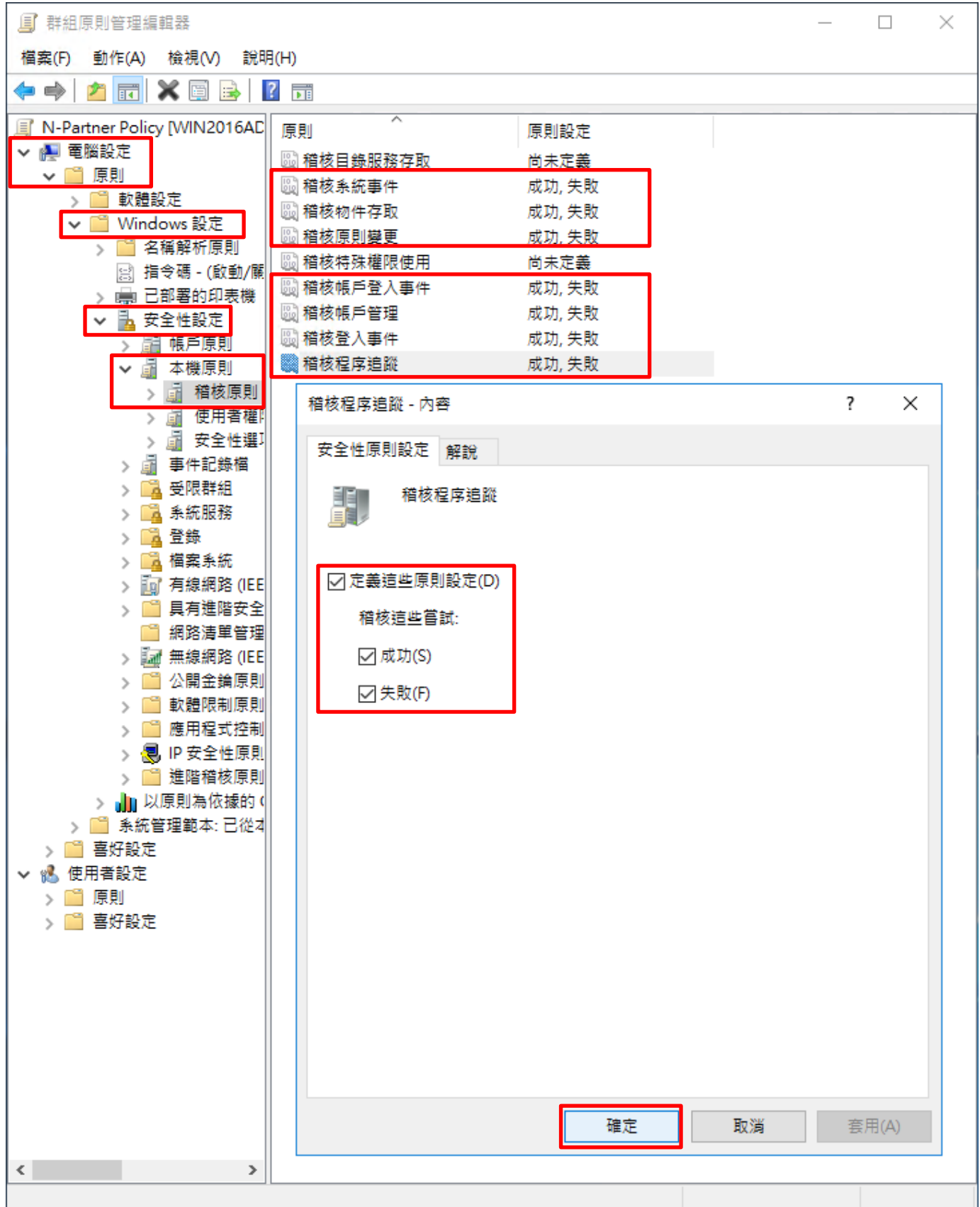
(4) 編輯群組原則物件

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

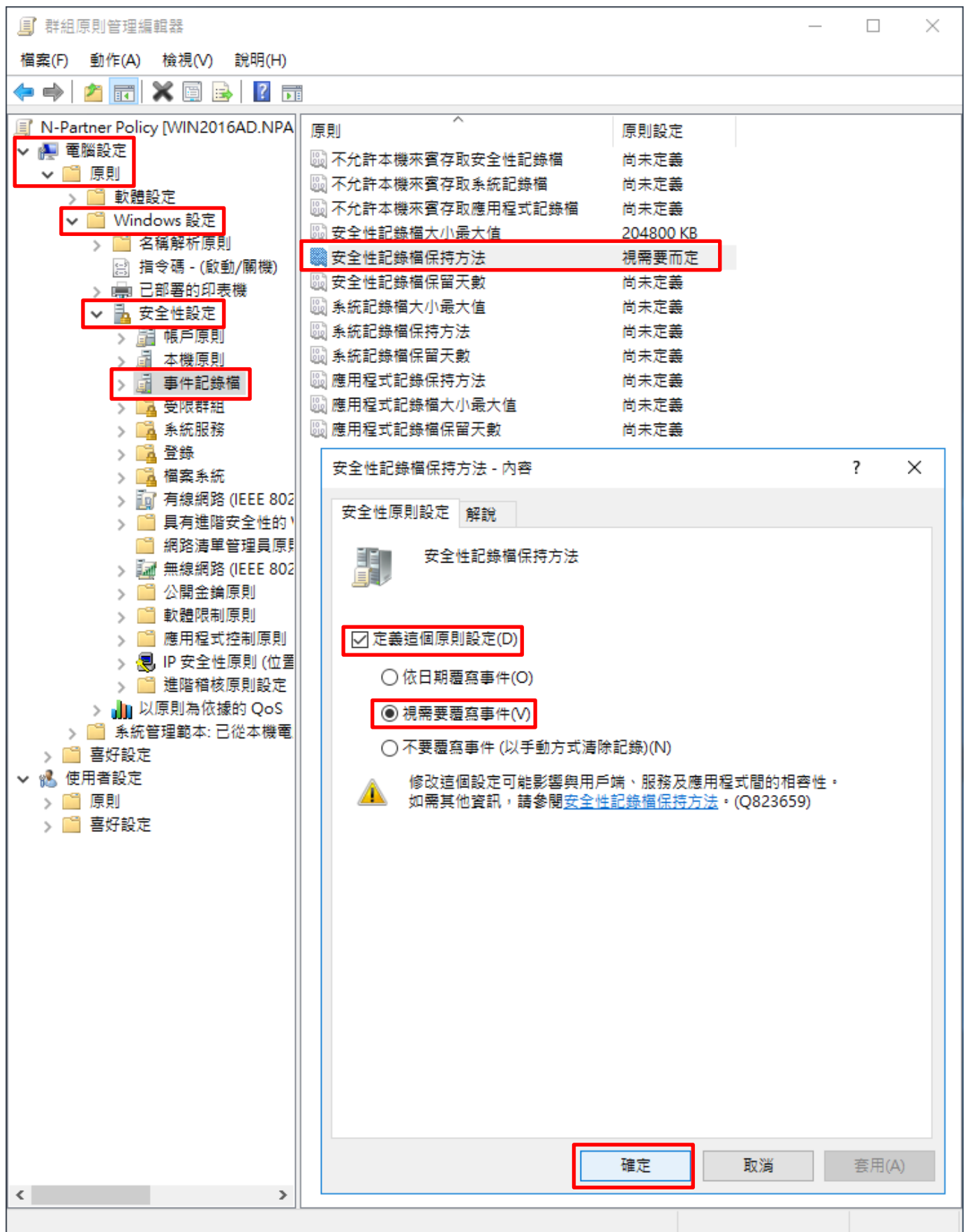
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Editor window for 'N-Partner Policy [WIN2016AD.NPA]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policy) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies, with '安全性記錄檔大小最大值' (Security Log Size Maximum) selected and highlighted in red. The value for this policy is set to '204800 KB'. Below the policy list, a dialog box titled '安全性記錄檔大小最大值 - 內容' (Security Log Size Maximum - Content) is open. In this dialog, the '定義這個原則設定(D)' (Define this policy setting) checkbox is checked and highlighted in red. The value '204800' is entered in the text box, followed by 'KB'. A warning icon and text are visible below the input field, stating: '修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)'. At the bottom of the dialog, the '確定' (OK) button is highlighted in red.



(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]

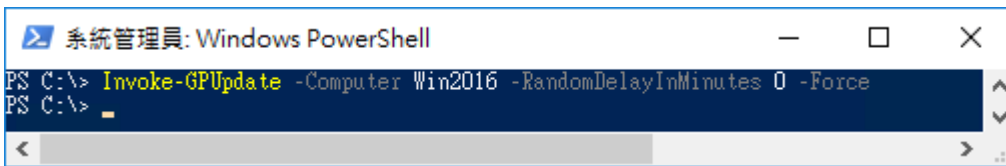


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 Windows Server 群組原則

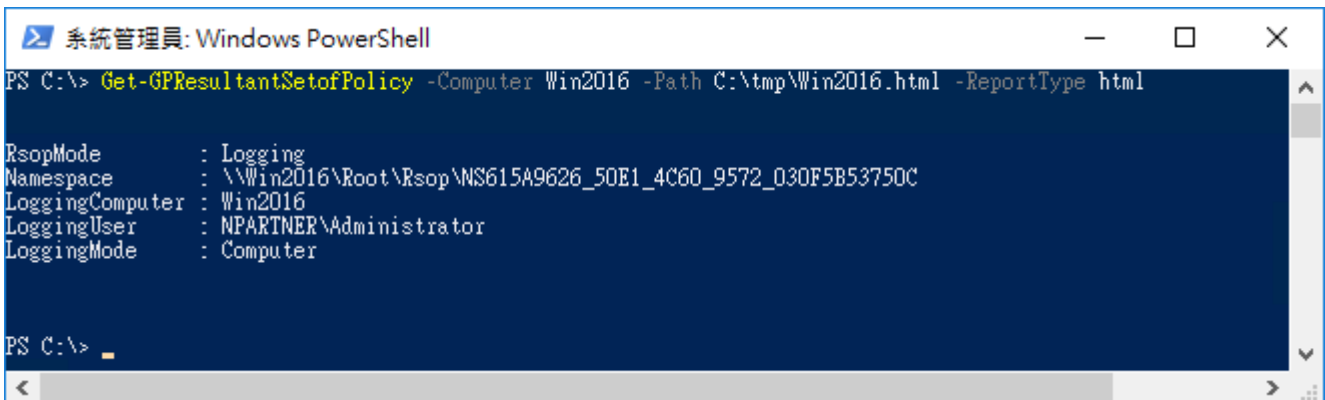
```
PS C:\> Invoke-GPUdate -Computer Win2016 -RandomDelayInMinutes 0 -Force
```



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

- □ ×
← → file:///C:/tmp/Win2016.htmr NPARTNER\WIN2016

**群組原則結果**

**NPARTNER\WIN2016**  
資料收集: 2022/8/18 下午 02:53:57 全部顯示

摘要	顯示																								
電腦詳細資料	隱藏																								
一般	顯示																								
元件狀態	顯示																								
設定	隱藏																								
<b>原則</b>	隱藏																								
Windows 設定	隱藏																								
安全性設定	隱藏																								
帳戶原則/密碼規則	顯示																								
帳戶原則/帳戶鎖定原則	顯示																								
本機原則/稽核原則	隱藏																								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">原則</th> <th style="width: 30%;">設定</th> <th style="width: 40%;">優勢 GPO</th> </tr> </thead> <tbody> <tr><td>稽核系統事件</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核物件存取</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核原則變更</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核帳戶登入事件</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核帳戶管理</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核登入事件</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> <tr><td>稽核程序追蹤</td><td>成功, 失敗</td><td>N-Partner Policy</td></tr> </tbody> </table>	原則	設定	優勢 GPO	稽核系統事件	成功, 失敗	N-Partner Policy	稽核物件存取	成功, 失敗	N-Partner Policy	稽核原則變更	成功, 失敗	N-Partner Policy	稽核帳戶登入事件	成功, 失敗	N-Partner Policy	稽核帳戶管理	成功, 失敗	N-Partner Policy	稽核登入事件	成功, 失敗	N-Partner Policy	稽核程序追蹤	成功, 失敗	N-Partner Policy	
原則	設定	優勢 GPO																							
稽核系統事件	成功, 失敗	N-Partner Policy																							
稽核物件存取	成功, 失敗	N-Partner Policy																							
稽核原則變更	成功, 失敗	N-Partner Policy																							
稽核帳戶登入事件	成功, 失敗	N-Partner Policy																							
稽核帳戶管理	成功, 失敗	N-Partner Policy																							
稽核登入事件	成功, 失敗	N-Partner Policy																							
稽核程序追蹤	成功, 失敗	N-Partner Policy																							
本機原則/安全性選項	顯示																								
事件記錄檔	隱藏																								
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">原則</th> <th style="width: 30%;">設定</th> <th style="width: 40%;">優勢 GPO</th> </tr> </thead> <tbody> <tr><td>安全性記錄檔保持方法</td><td>視需要而定</td><td>N-Partner Policy</td></tr> <tr><td>安全性記錄檔容量最大值</td><td>204800 KB</td><td>N-Partner Policy</td></tr> </tbody> </table>	原則	設定	優勢 GPO	安全性記錄檔保持方法	視需要而定	N-Partner Policy	安全性記錄檔容量最大值	204800 KB	N-Partner Policy																
原則	設定	優勢 GPO																							
安全性記錄檔保持方法	視需要而定	N-Partner Policy																							
安全性記錄檔容量最大值	204800 KB	N-Partner Policy																							
公開金鑰原則/憑證服務用戶端 - 自動註冊設定	顯示																								
公開金鑰原則/加密檔案系統	顯示																								
<b>群組原則物件</b>	顯示																								
<b>WMI 篩選器</b>	顯示																								
使用者詳細資料	顯示																								

## 6.2 工作群組

### 6.2.1 稽核原則設定

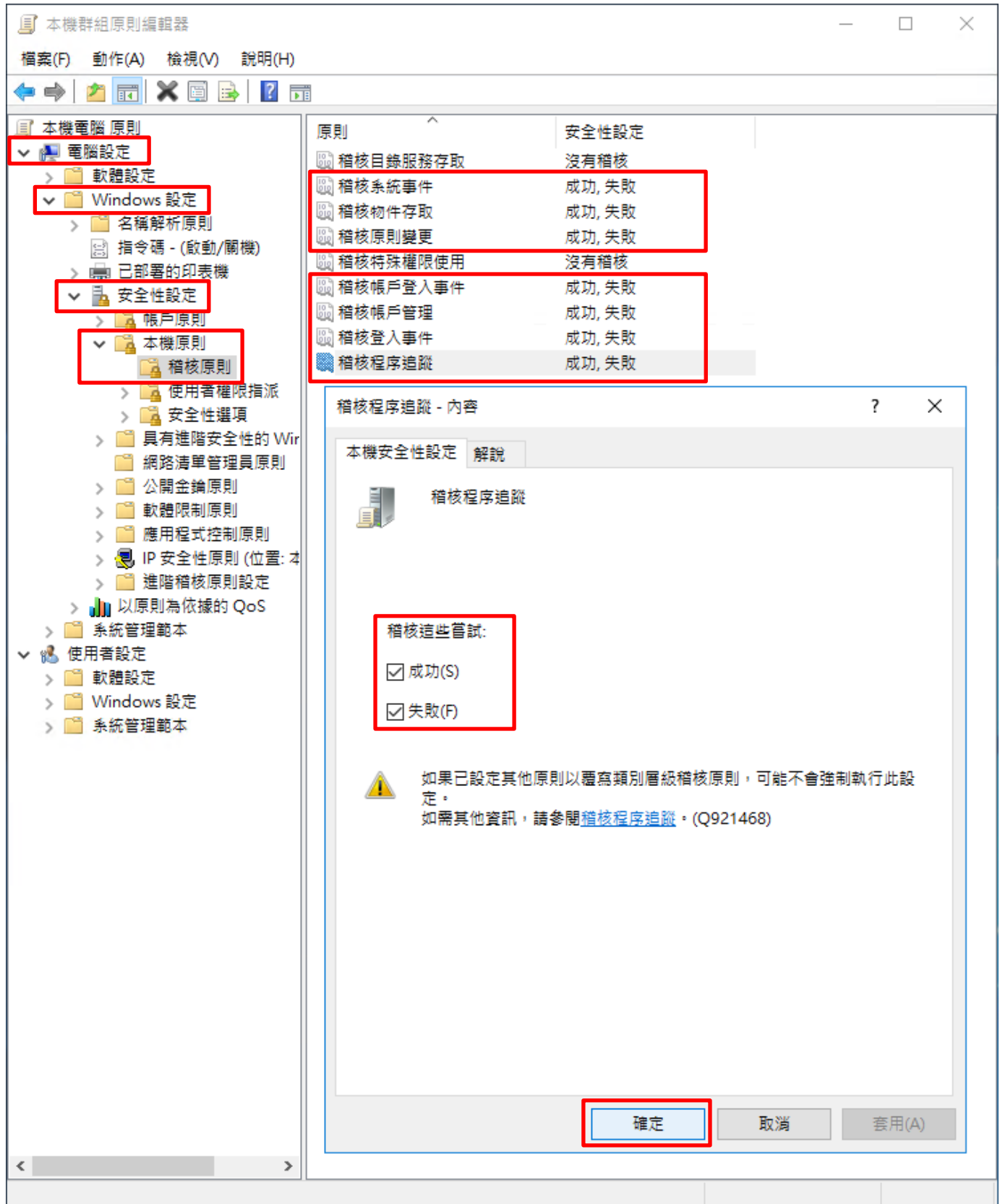
(1) 開啟 [本機群組原則編輯器]

點選 [搜尋] -> 輸入 群組原則 -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [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]

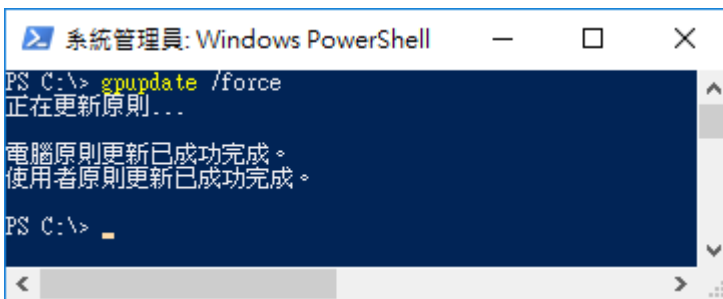


(3) 開啟 [Windows PowerShell]



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

## 6.2.2 事件檔案設定

(1) 開啟 [檢視事件記錄檔]

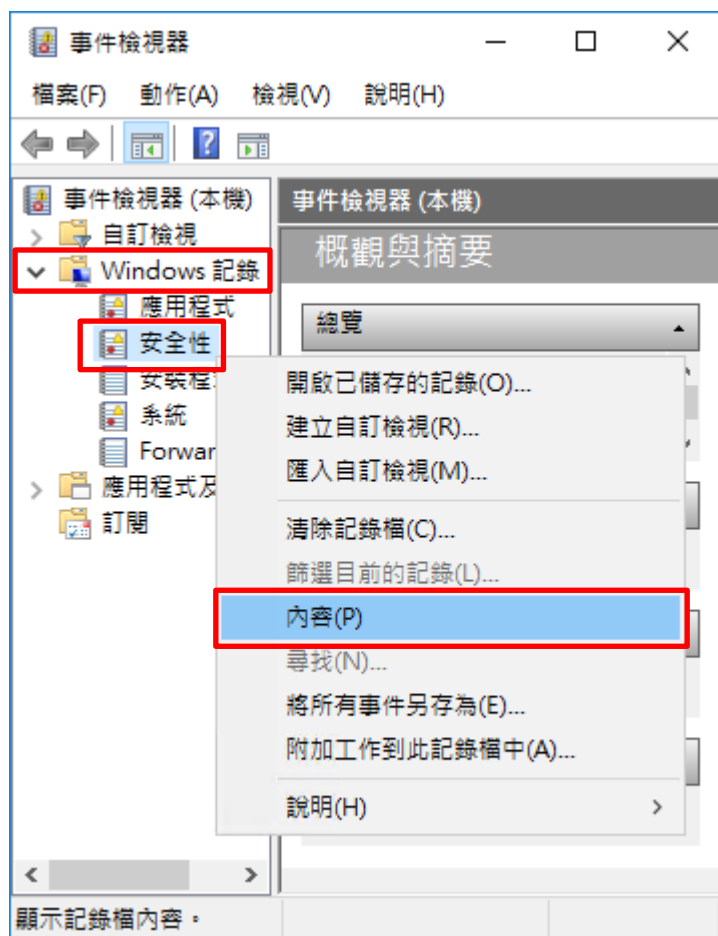
點選 [搜尋] -> 輸入 [事件記錄檔](#) -> 點選 [檢視事件記錄檔]





## (2) 編輯安全性記錄

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



#### (4) 設定安全性記錄檔

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

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

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

記錄檔大小: 9.07 MB(9,506,816 位元組)

建立日期: 2021年3月8日 下午 09:42:35

修改日期: 2021年3月17日 下午 05:00:12

存取日期: 2021年3月8日 下午 09:42:35

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

確定 取消 套用(P)

## 7. Windows 2019

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

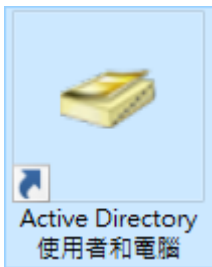
※ 以下分別為網域和工作群組設定方式。

### 7.1 網域

#### 7.1.1 組織單位設定

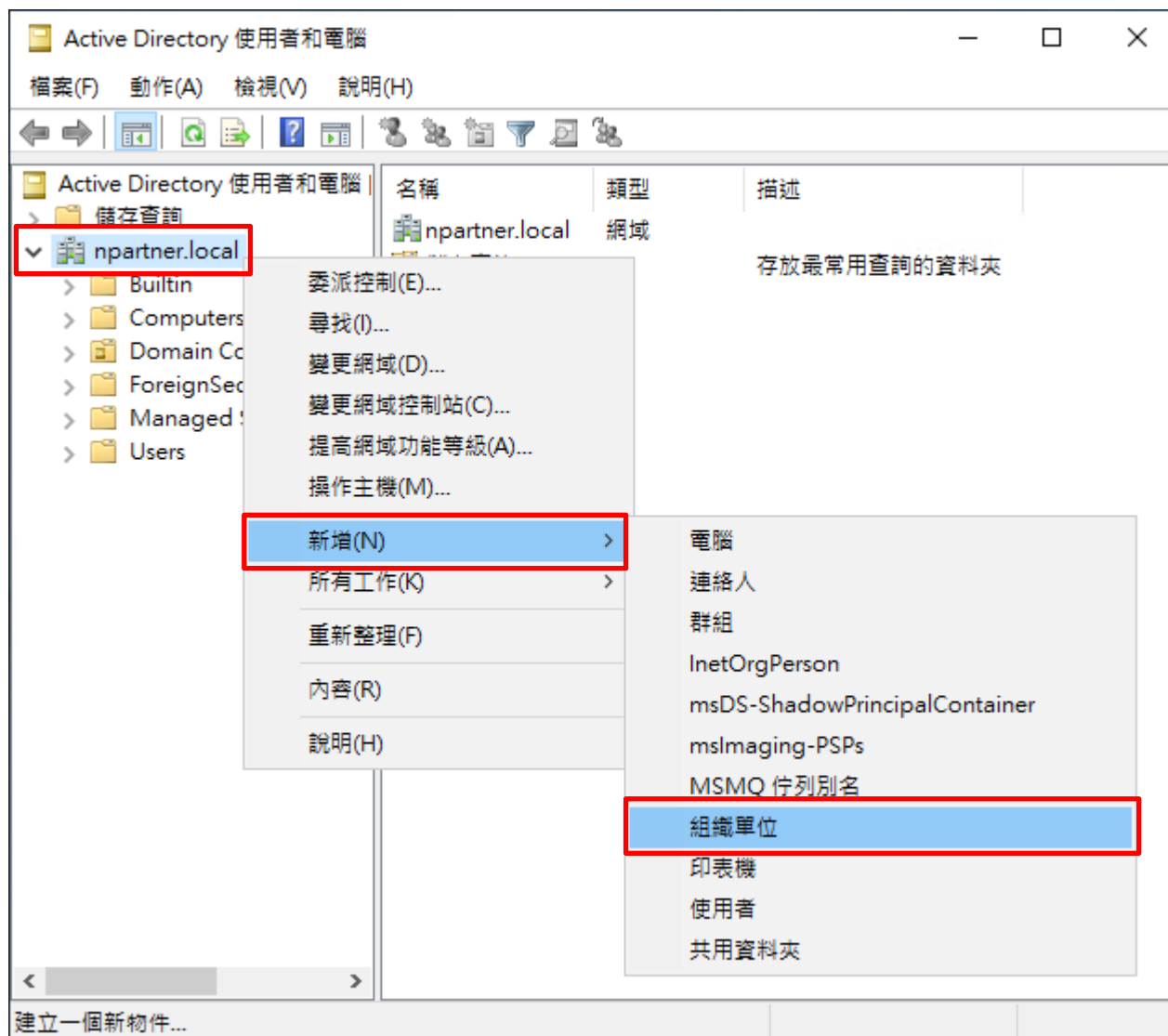
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



## (2) 新增組織單位

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



(3) 輸入組織單位名稱

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

新增物件 - 組織單位

建立在: npartner.local/

名稱(A):  
Servers

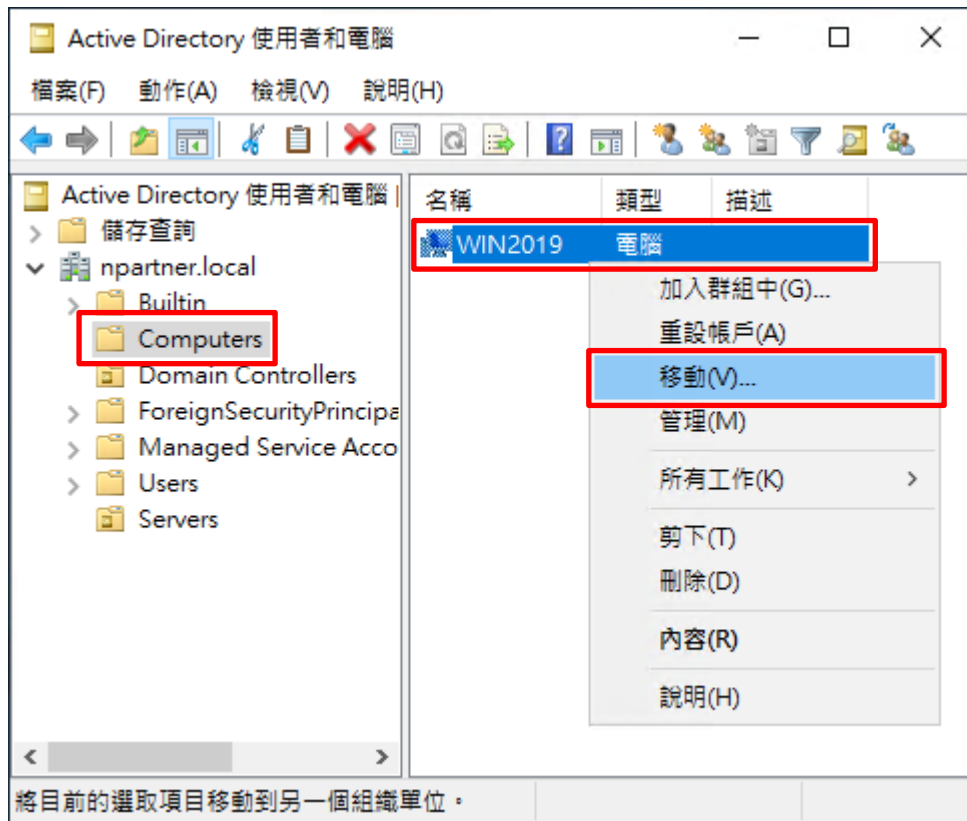
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

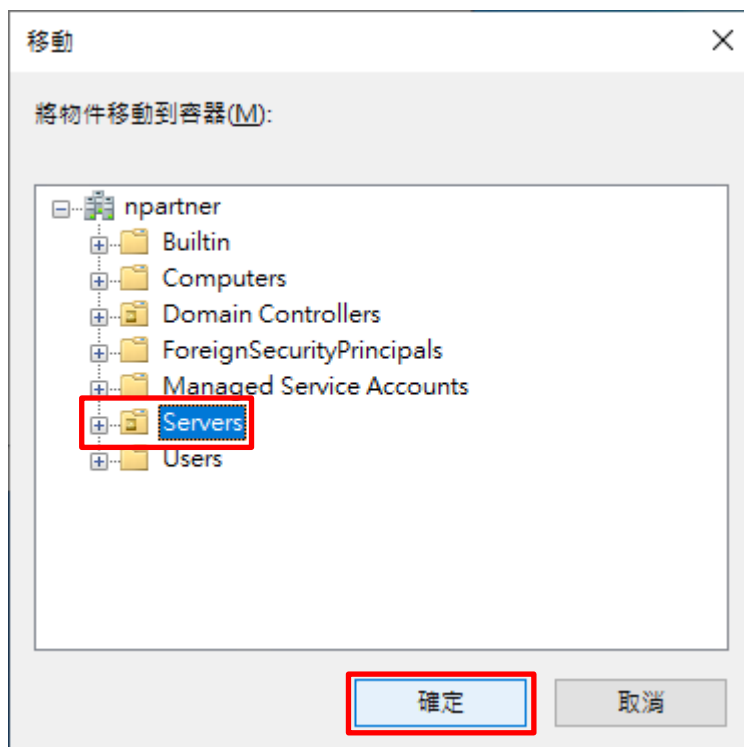
選擇 [Computers] 組織單位 -> 在 [Win2019] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



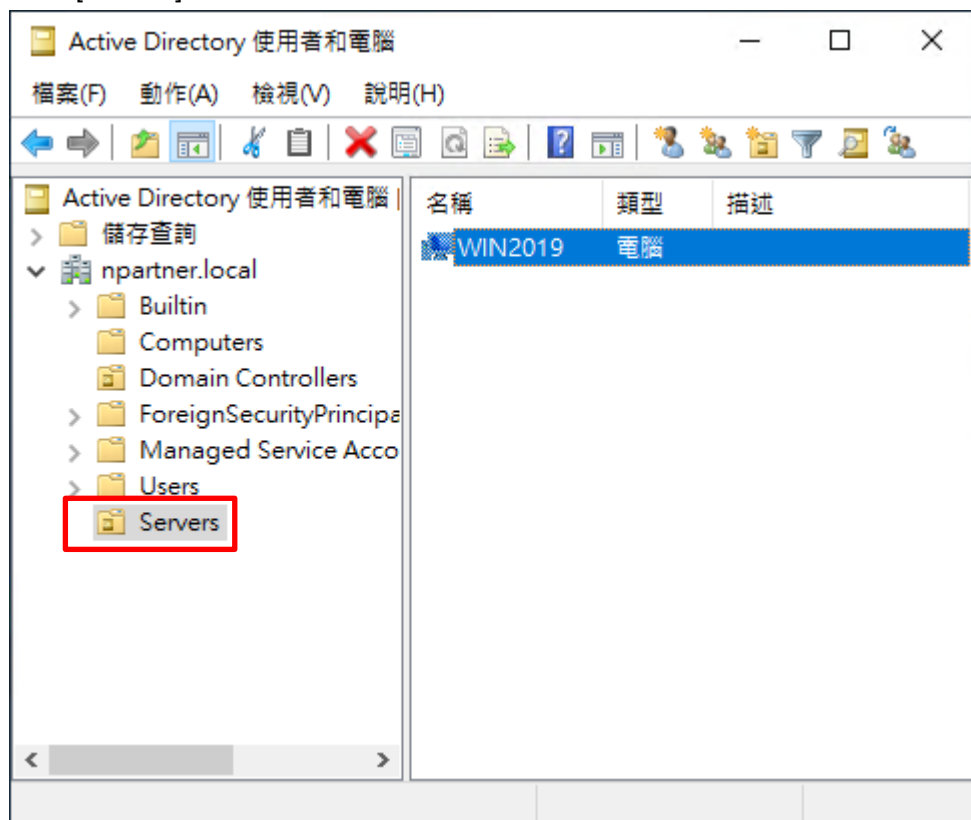
(5) 選擇組織單位

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

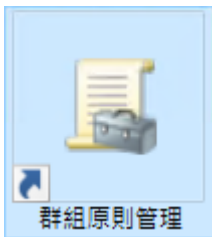
點選 [Servers] 組織單位，確認 Win2019 伺服器已移動。



## 7.1.2 群組原則設定

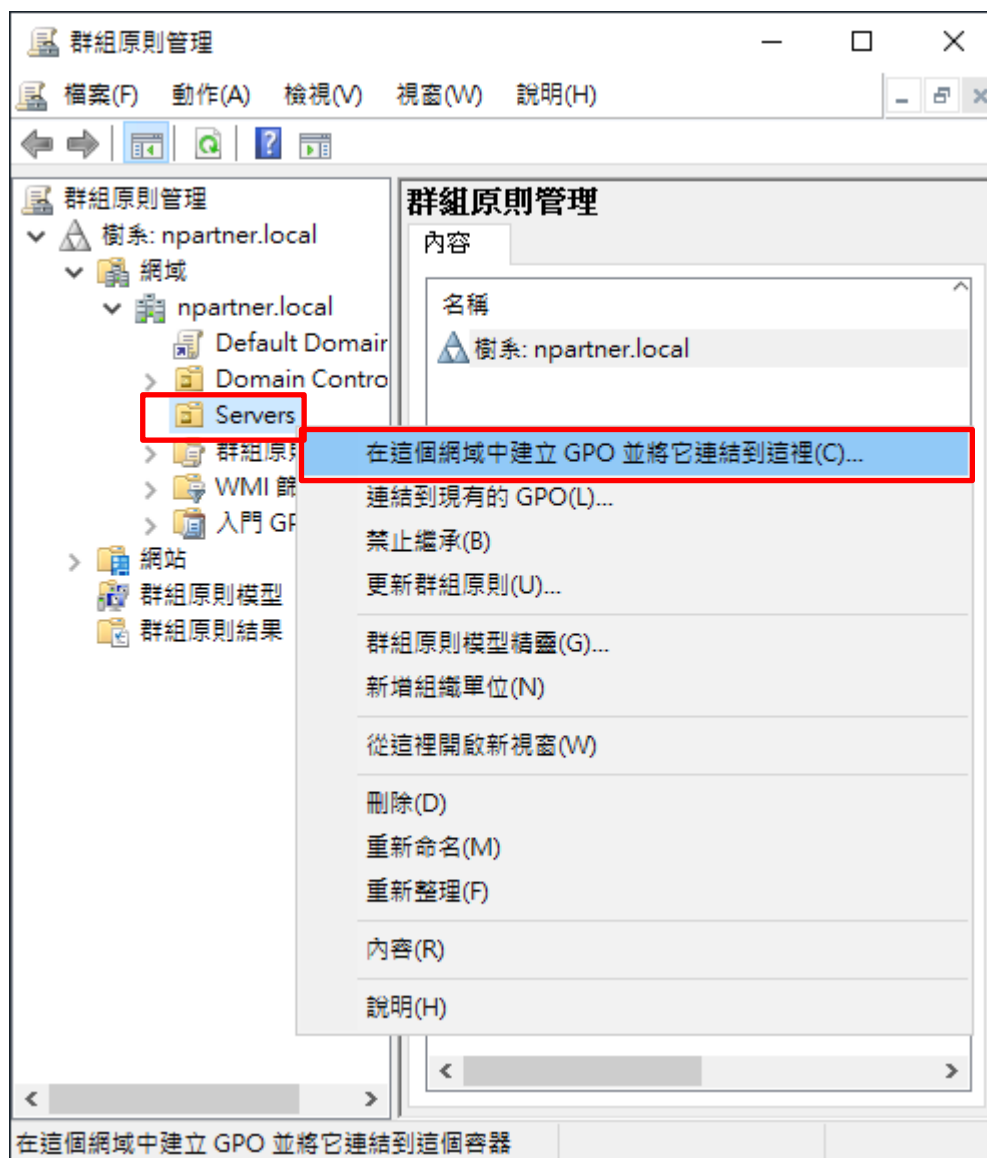
### (1) 開啟群組原則管理

開啟 [群組原則管理]



### (2) 在 Servers 組織單位，新增群組原則物件

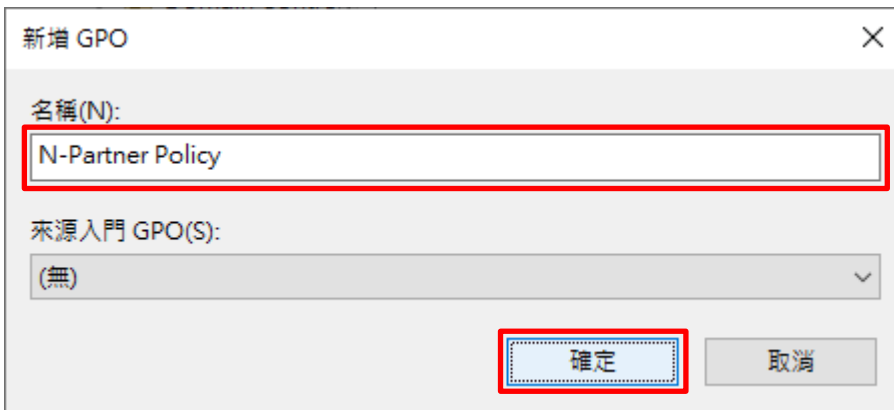
在 [Servers] 組織單位上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到...]





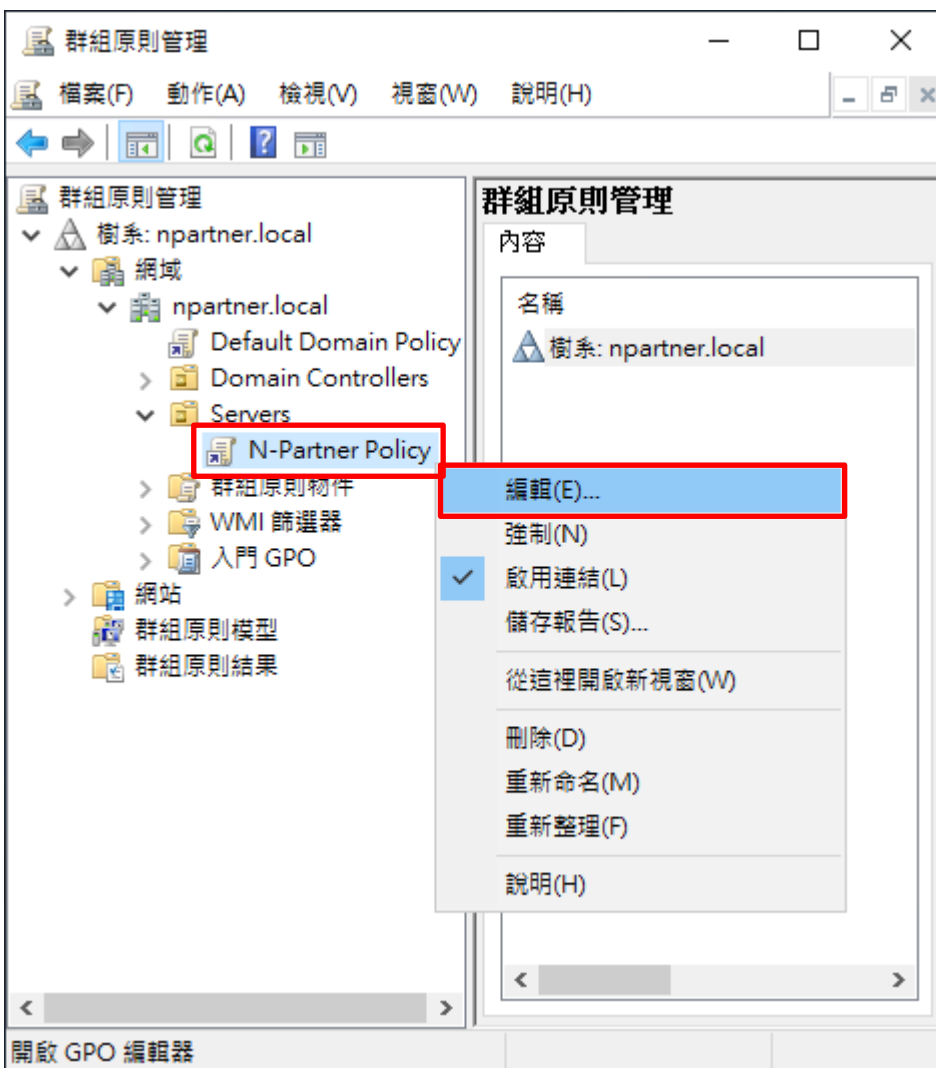
(3) 輸入群組原則物件名稱

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]



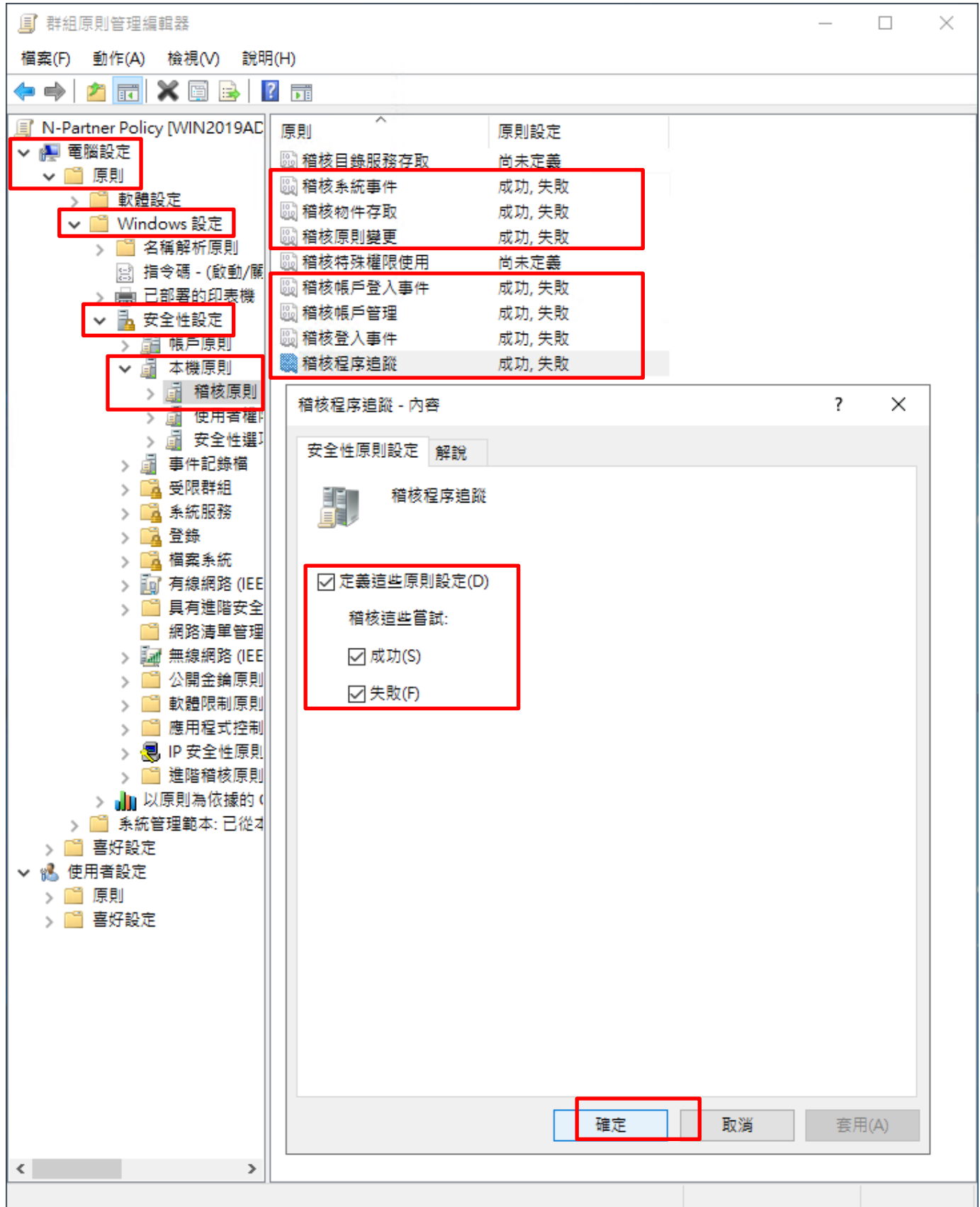
(4) 編輯群組原則物件

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

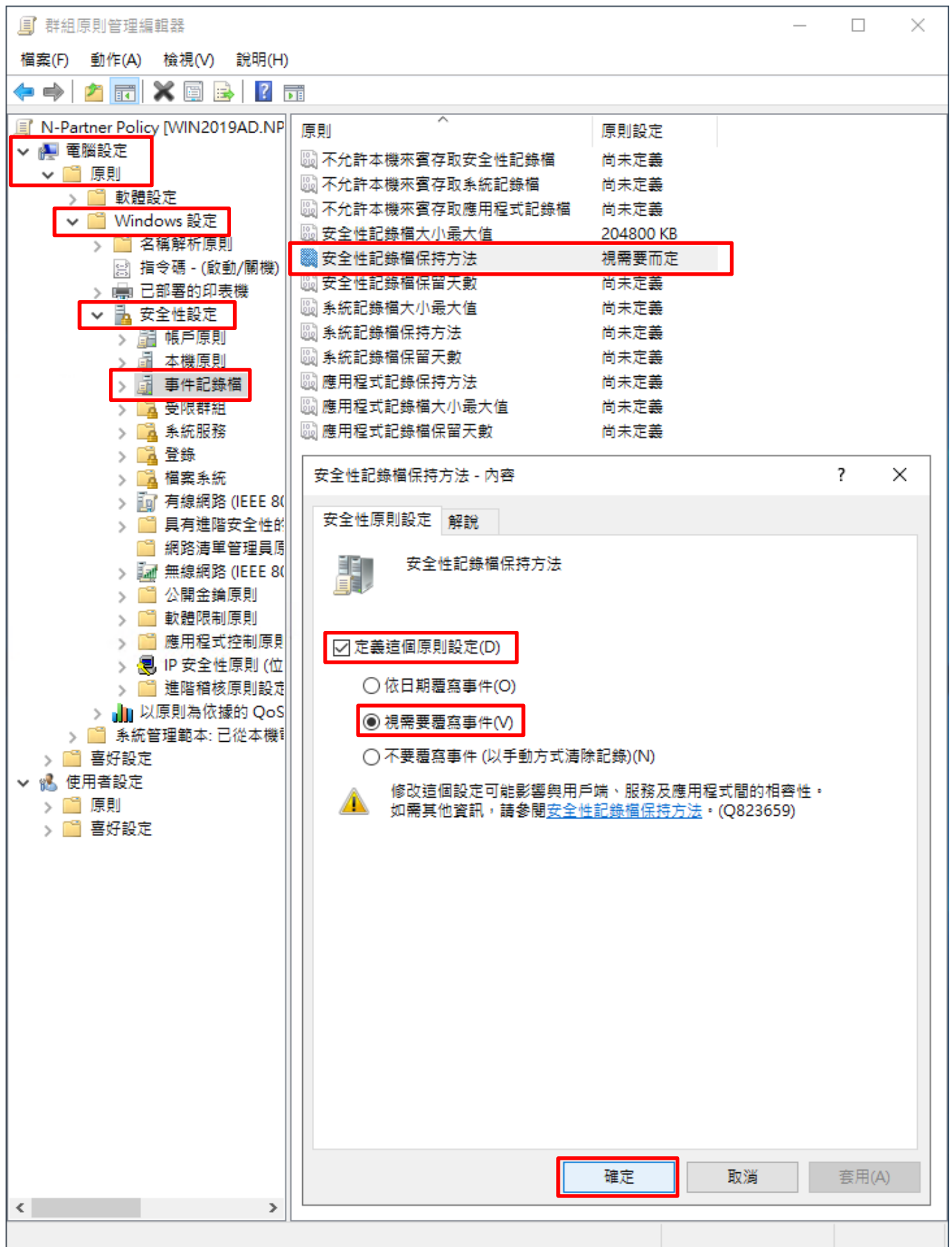
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定]: -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Management Editor window for 'N-Partner Policy [WIN2019AD.NP]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policy) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies, with '安全性記錄檔大小最大值' (Security Log Size Maximum) selected and highlighted. Below this, a dialog box titled '安全性記錄檔大小最大值 - 內容' (Security Log Size Maximum - Content) is open. In this dialog, the '定義這個原則設定(D)' (Define this policy setting) checkbox is checked. The value '204800' is entered in the text box, followed by 'KB' in the dropdown menu. A warning icon and text at the bottom of the dialog state: '修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)'. The '確定' (OK) button is highlighted with a red box.

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

(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]

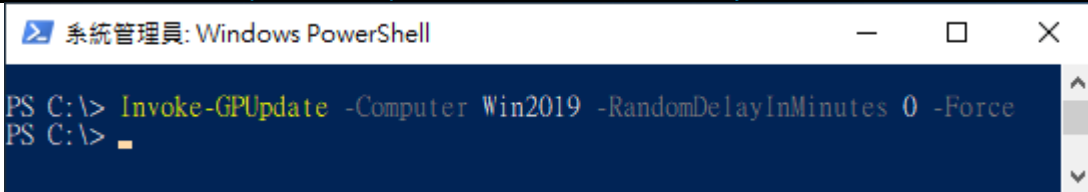


(8) 開啟 [Windows PowerShell]



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

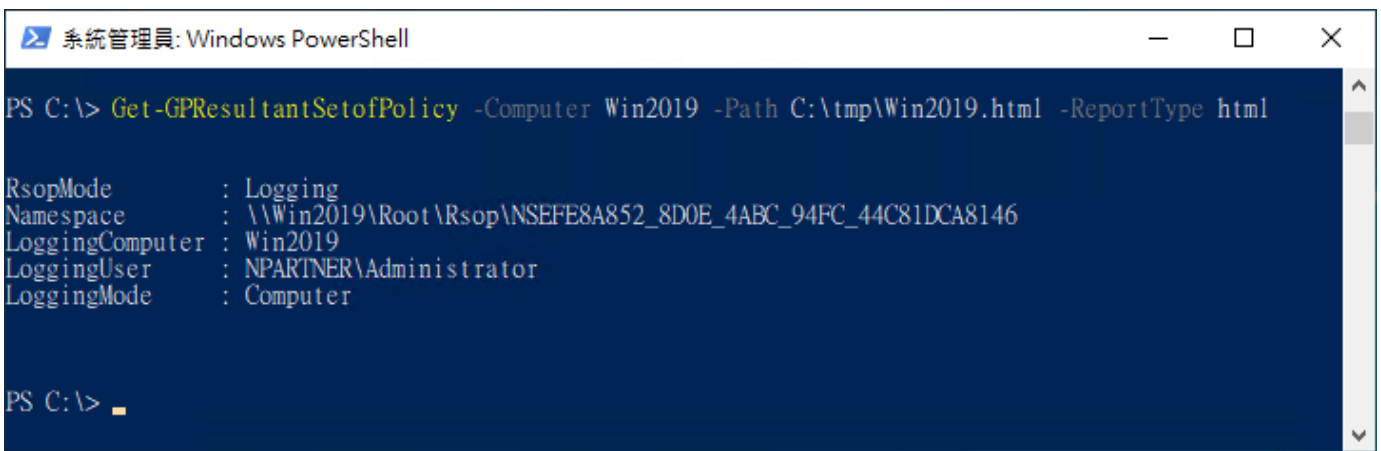
```
PS C:\> Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



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

file:///C:/tmp/Win2019.html# 搜尋...

NPARTNER\WIN2019

### 群組原則結果

NPARTNER\WIN2019  
資料收集: 2022/8/18 下午 03:45:06 全部顯示

**摘要** 顯示

**電腦詳細資料** 隱藏

**一般** 顯示

**元件狀態** 顯示

**設定** 隱藏

**原則** 隱藏

**Windows 設定** 隱藏

**安全性設定** 隱藏

**帳戶原則/密碼規則** 顯示

**帳戶原則/帳戶鎖定原則** 顯示

**本機原則/稽核原則** 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy

**本機原則/安全性選項** 顯示

**事件記錄檔** 隱藏

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

**公開金鑰原則/憑證服務用戶端 - 自動註冊設定** 顯示

**公開金鑰原則/加密檔案系統** 顯示

**群組原則物件** 顯示

**WMI 篩選器** 顯示

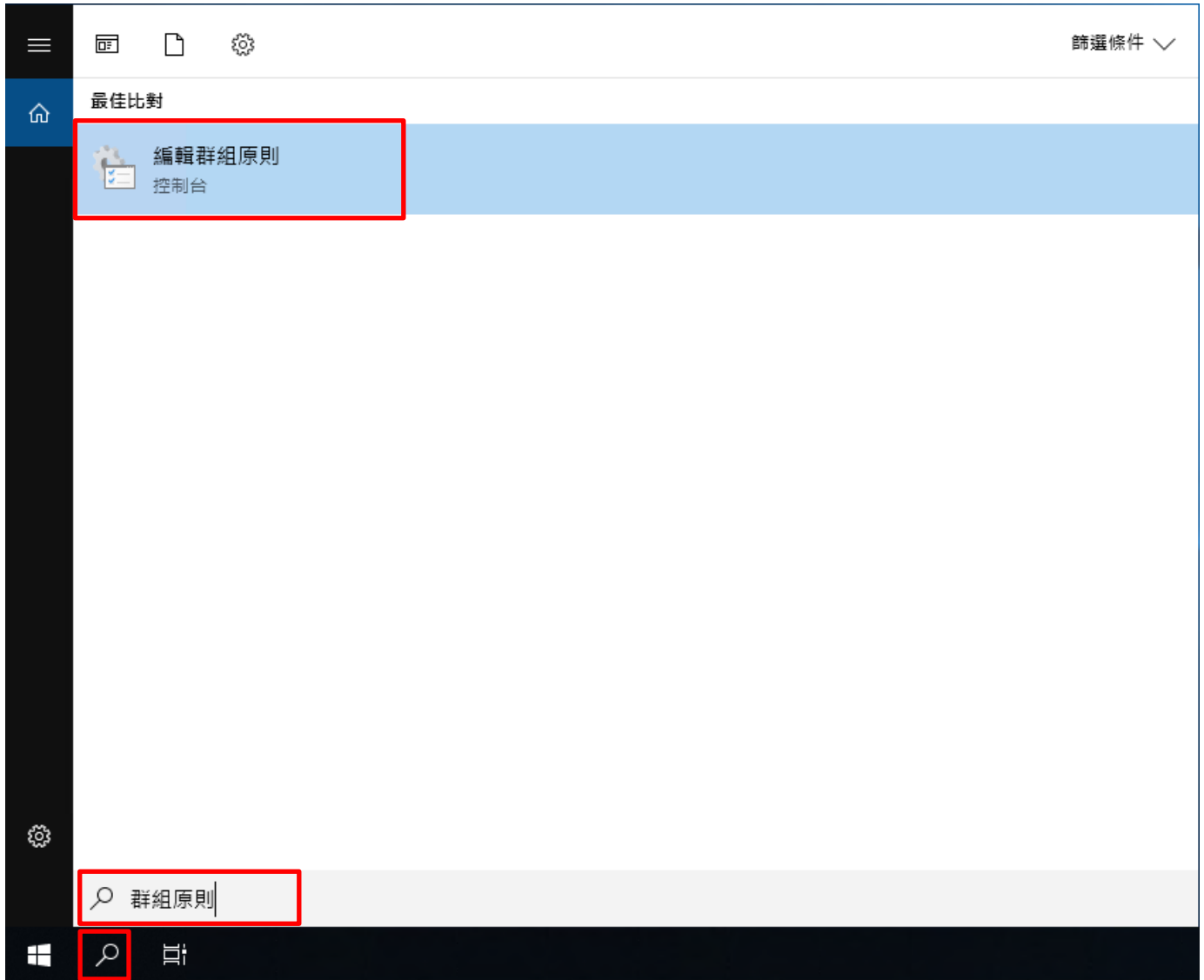
**使用者詳細資料** 顯示

## 7.2 工作群組

### 7.2.1 稽核原則設定

(1) 開啟本機群組原則編輯器

點選 [搜尋] -> 輸入 **群組原則** -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [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]

本機群組原則編輯器

檔案(F) 動作(A) 檢視(V) 說明(H)

本機電腦 原則

- 電腦設定
  - 軟體設定
  - Windows 設定
    - 名稱解析原則
    - 指令碼 - (啟動/關機)
    - 已部署的印表機
    - 安全性設定
      - 帳戶原則
      - 本機原則
        - 稽核原則
    - 使用者權限指派
    - 安全性選項
    - 具有進階安全性的 Windows
    - 網路清單管理員原則
    - 公開金鑰原則
    - 軟體限制原則
    - 應用程式控制原則
    - IP 安全性原則 (位置: 本機)
    - 進階稽核原則設定
  - 以原則為依據的 QoS
  - 系統管理範本
- 使用者設定
  - 軟體設定
  - Windows 設定
  - 系統管理範本

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

稽核程序追蹤 - 內容

本機安全性設定 解說

稽核程序追蹤

稽核這些嘗試:

- 成功(S)
- 失敗(F)

⚠ 如果已設定其他原則以覆寫類別層級稽核原則, 可能不會強制執行此設定。  
如需其他資訊, 請參閱[稽核程序追蹤](#)。(Q921468)

確定 取消 套用(A)

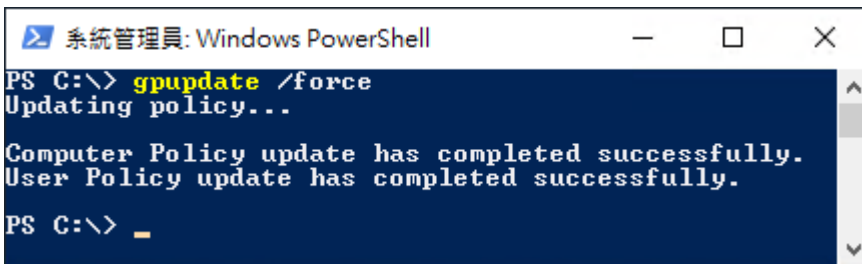


(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force



(5) 查看群組原則套用情形

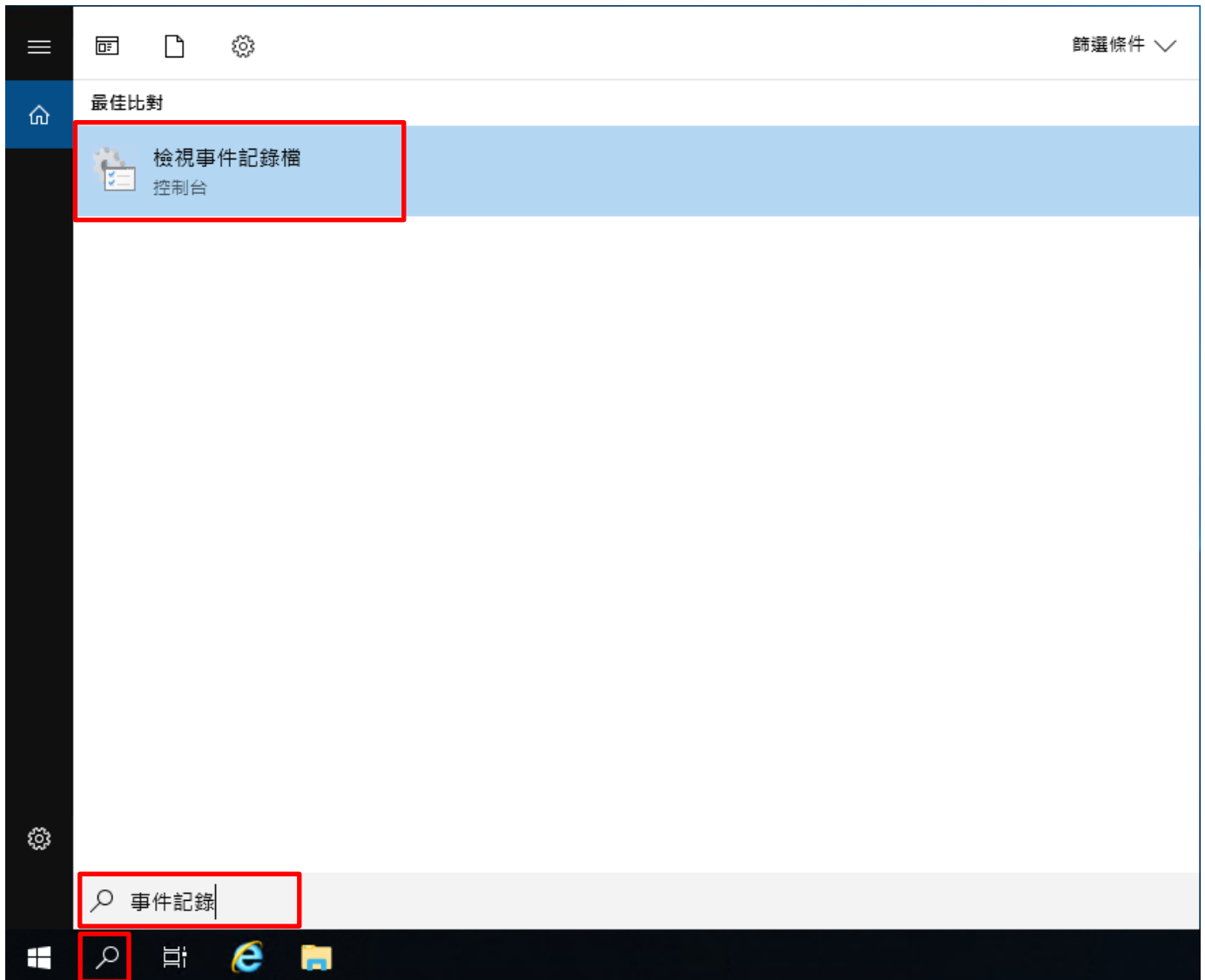
PS C:\> auditpol /get /category:\*

```
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
  MPSSUC 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

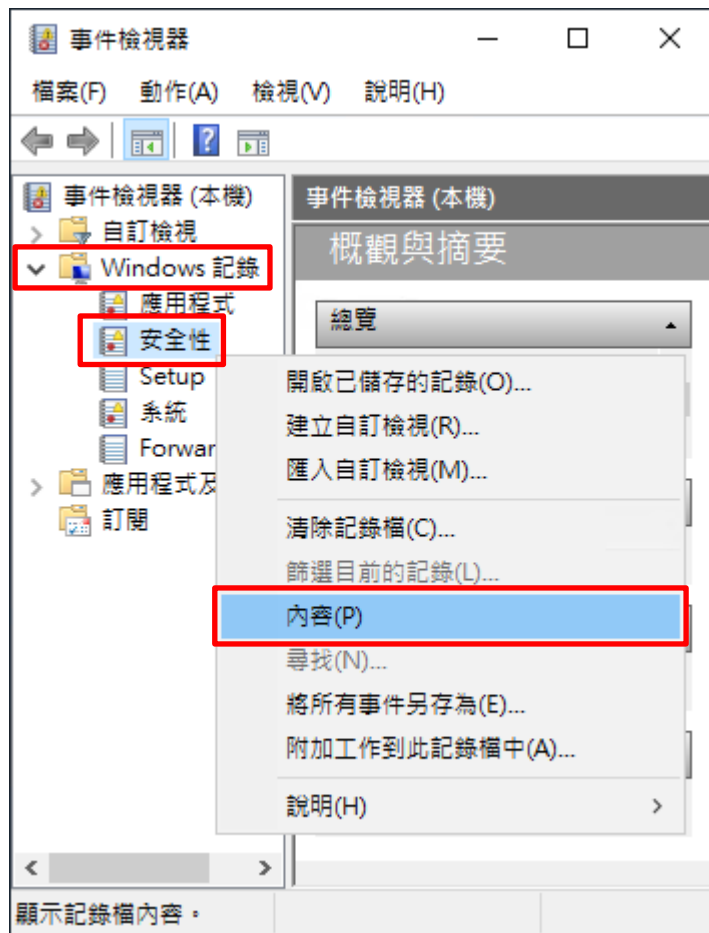
(1) 開啟 [檢視事件記錄檔]

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]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

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

記錄檔大小: 20.00 MB(20,975,616 位元組)

建立日期: 2021年2月23日 下午 05:15:05

修改日期: 2021年3月18日 上午 09:18:18

存取日期: 2021年3月18日 上午 09:18:18

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

確定 取消 套用(P)

## 8. Windows 2022

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

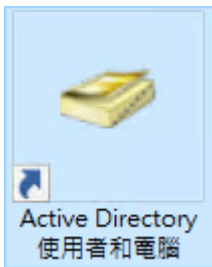
※ 以下分別為網域和工作群組設定方式。

### 8.1 網域

#### 8.1.1 組織單位設定

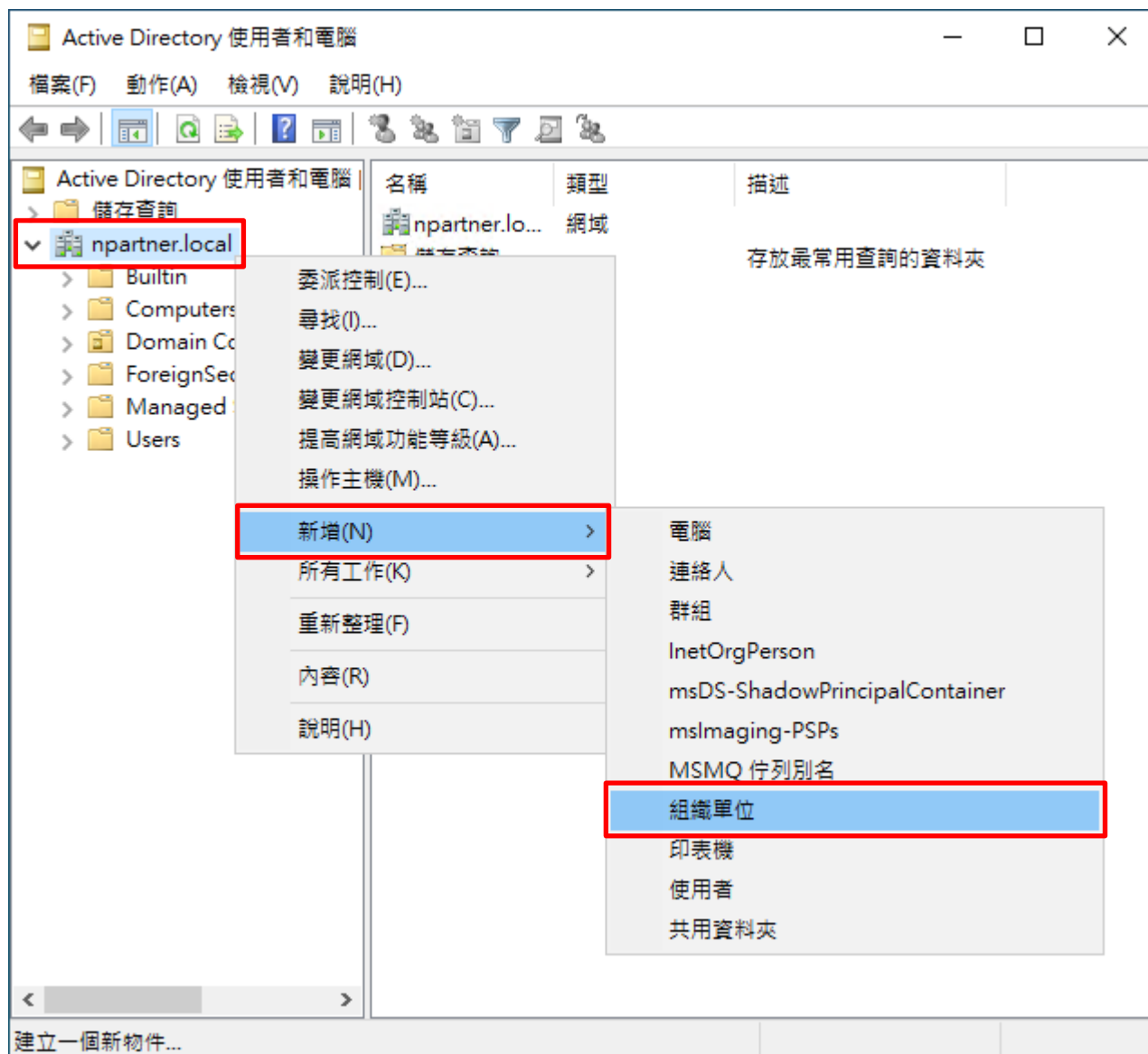
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



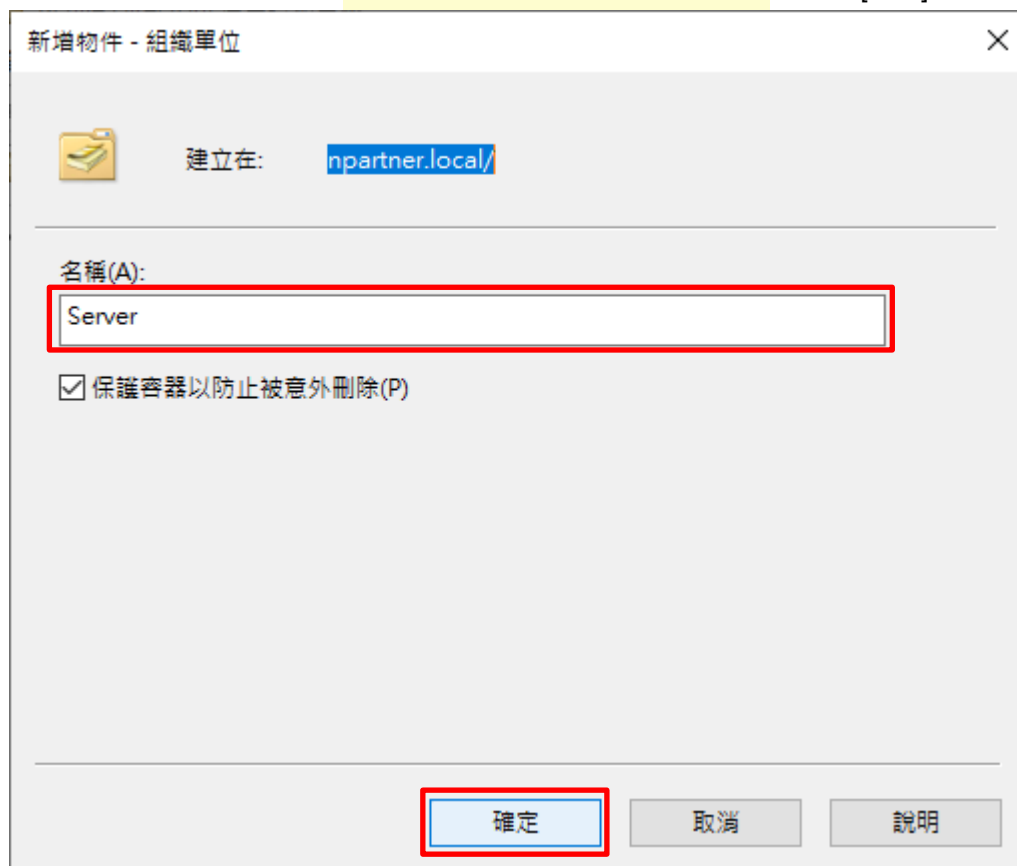
## (2) 新增組織單位

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



(3) 輸入組織單位名稱

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



新增物件 - 組織單位

建立在: npartner.local/

名稱(A):  
Server

保護容器以防止被意外刪除(P)

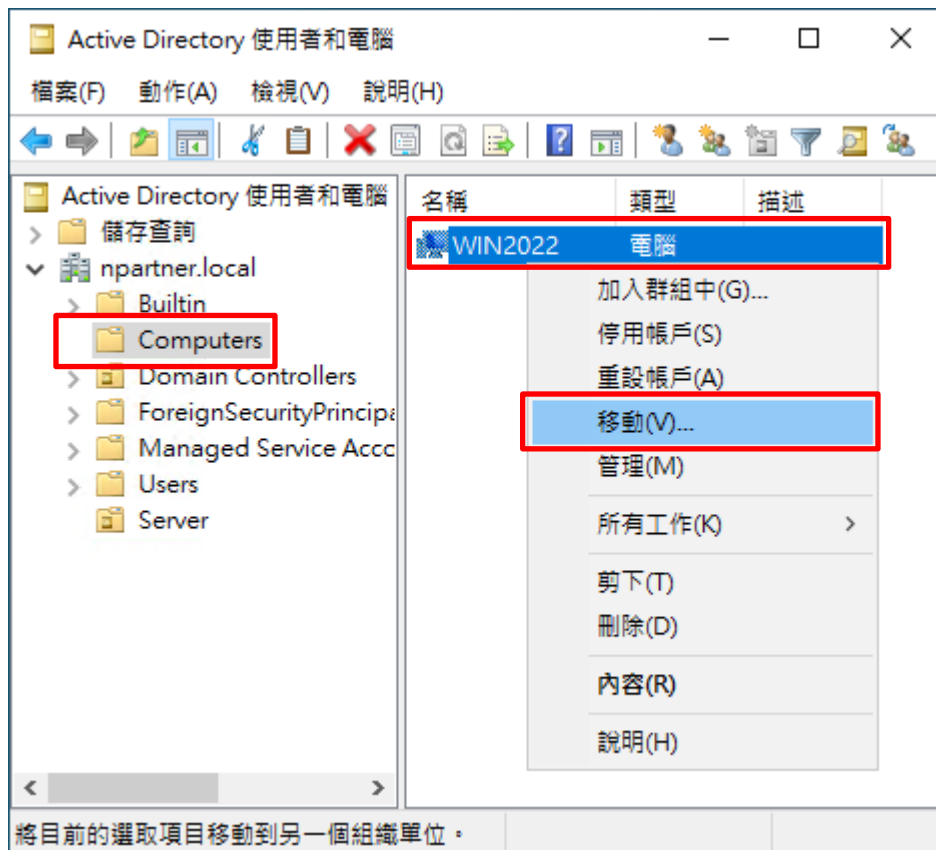
確定 取消 說明



(4) 移動伺服器至新的組織單位

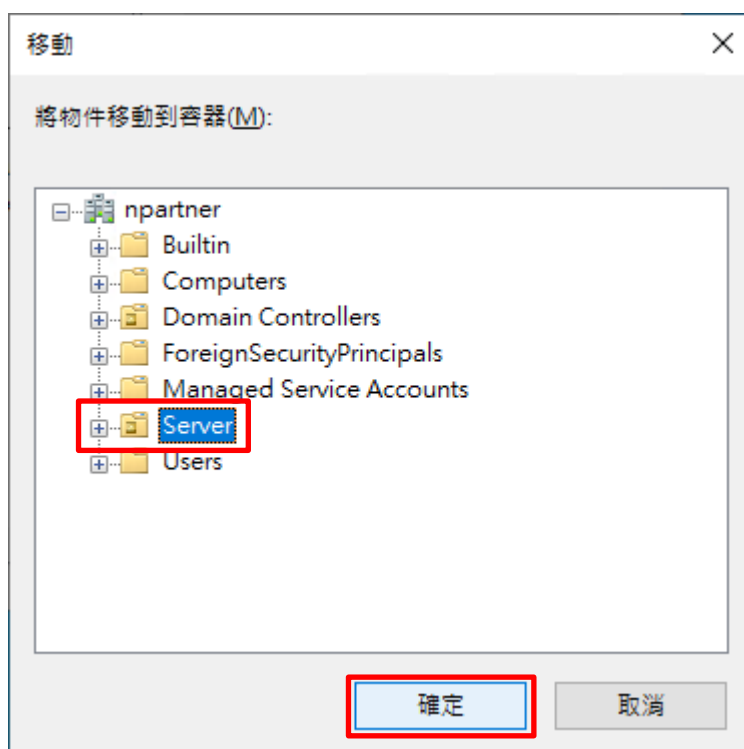
選擇 [Computers] 組織單位 -> 在 [Win2022] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows Server 主機

-> 點選 [移動]



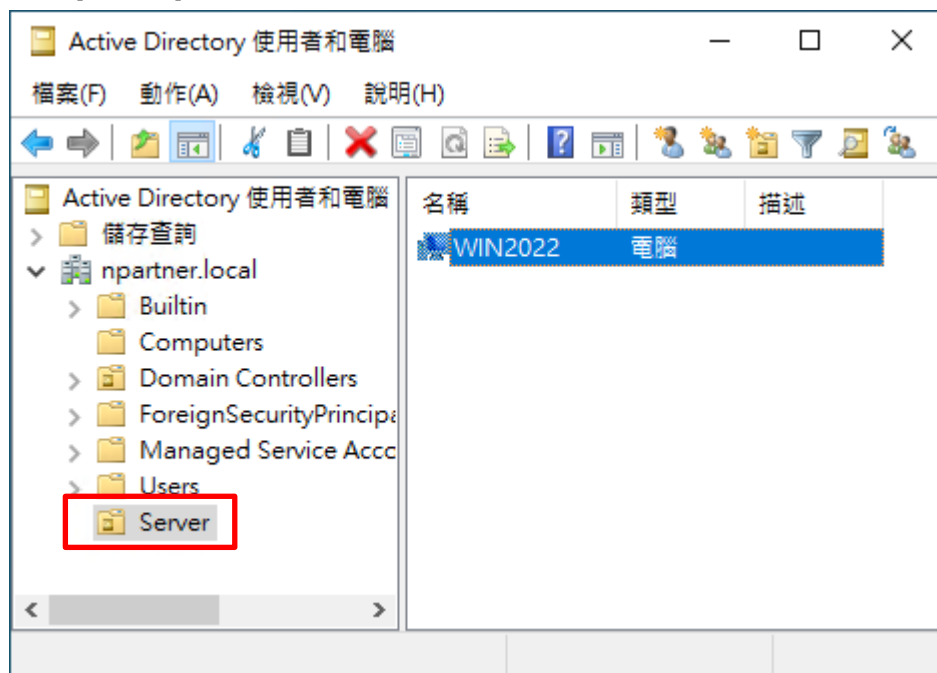
(5) 選擇組織單位

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

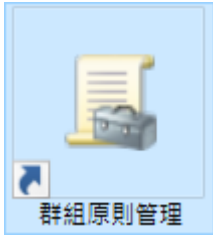
點選 [Servers] 組織單位，確認 Win2022 伺服器已移動。



## 8.1.2 群組原則設定

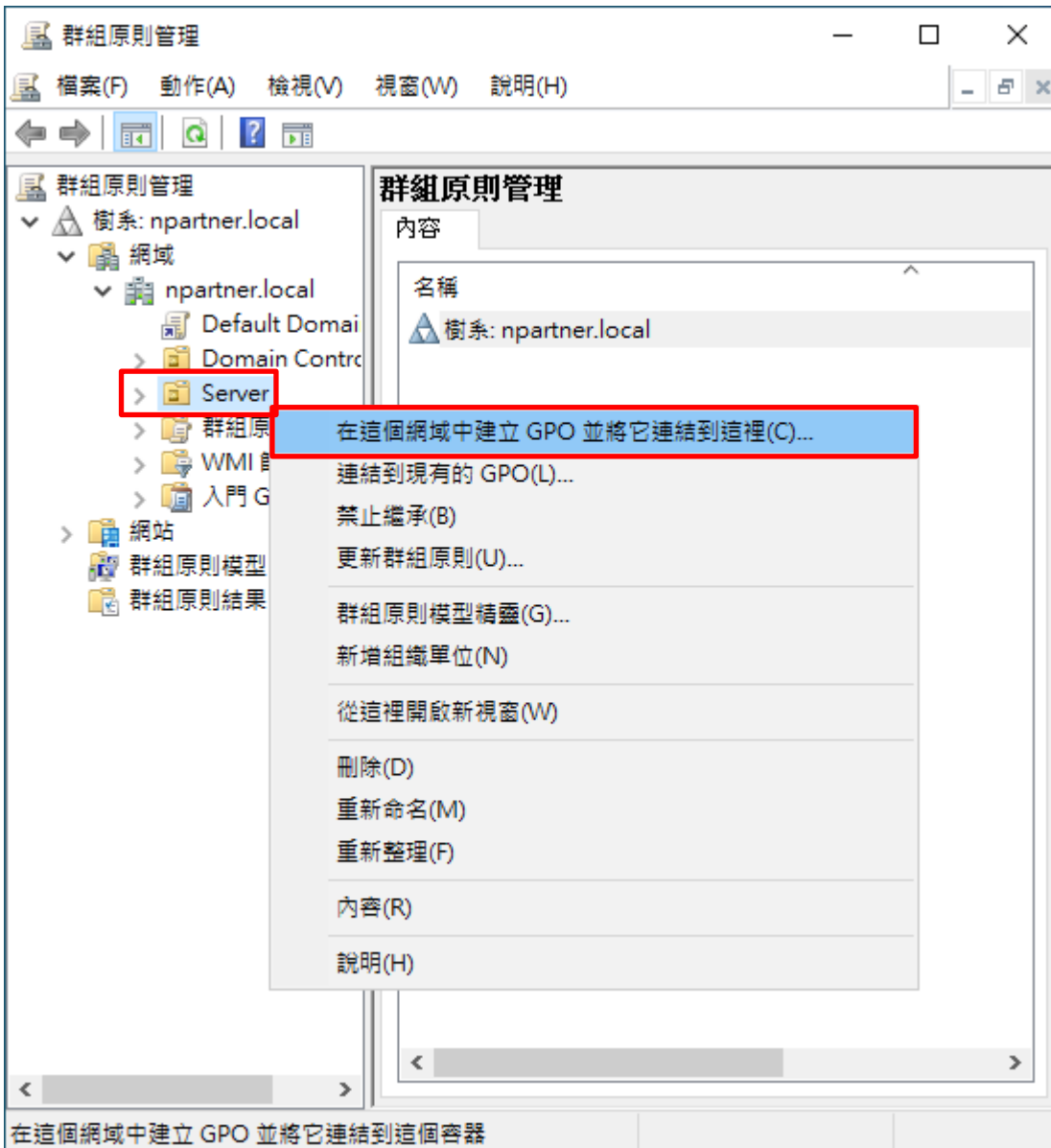
### (1) 開啟群組原則管理

開啟 [群組原則管理]



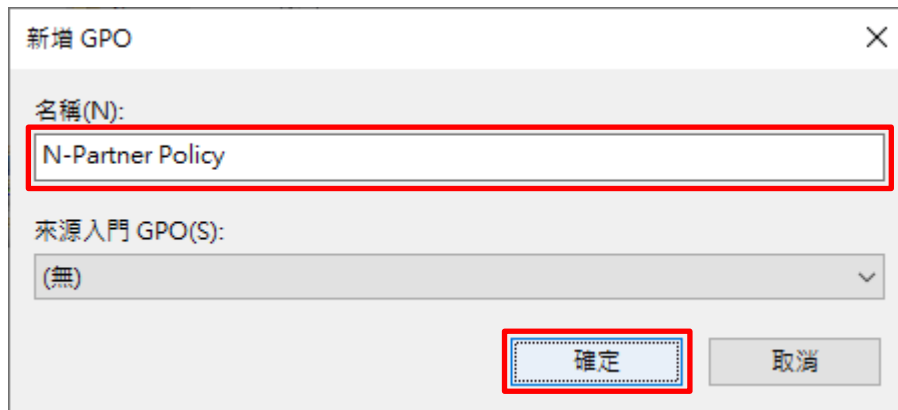
### (2) 在 Servers 組織單位，新增群組原則物件

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...]



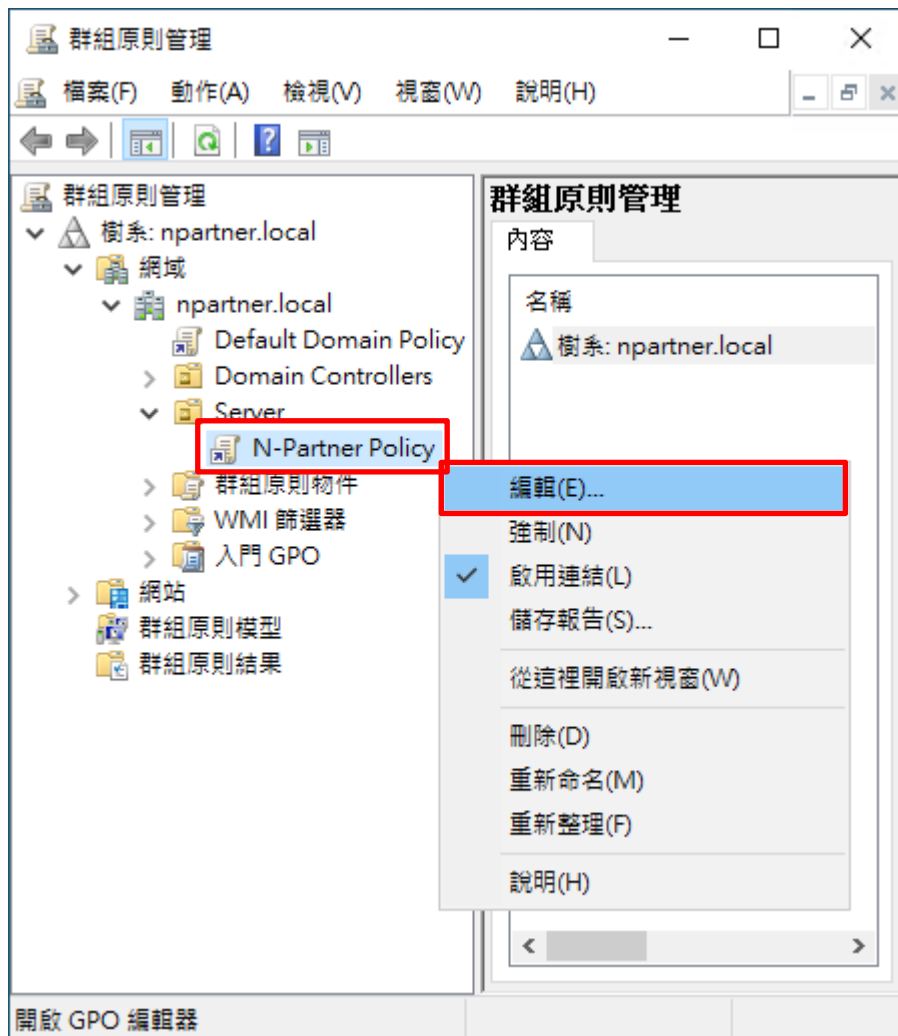
(3) 輸入群組原則物件名稱

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]



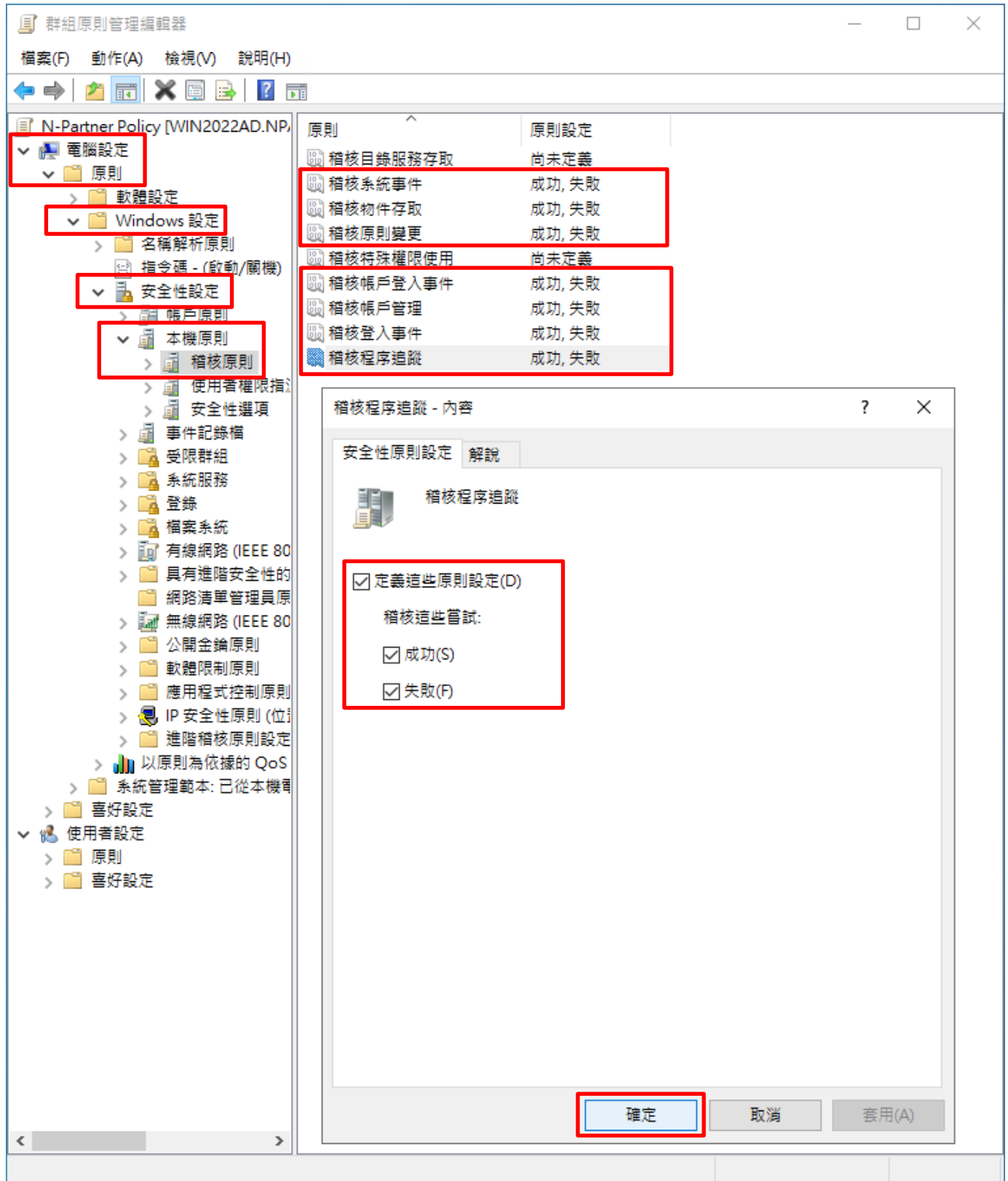
(4) 編輯群組原則物件

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



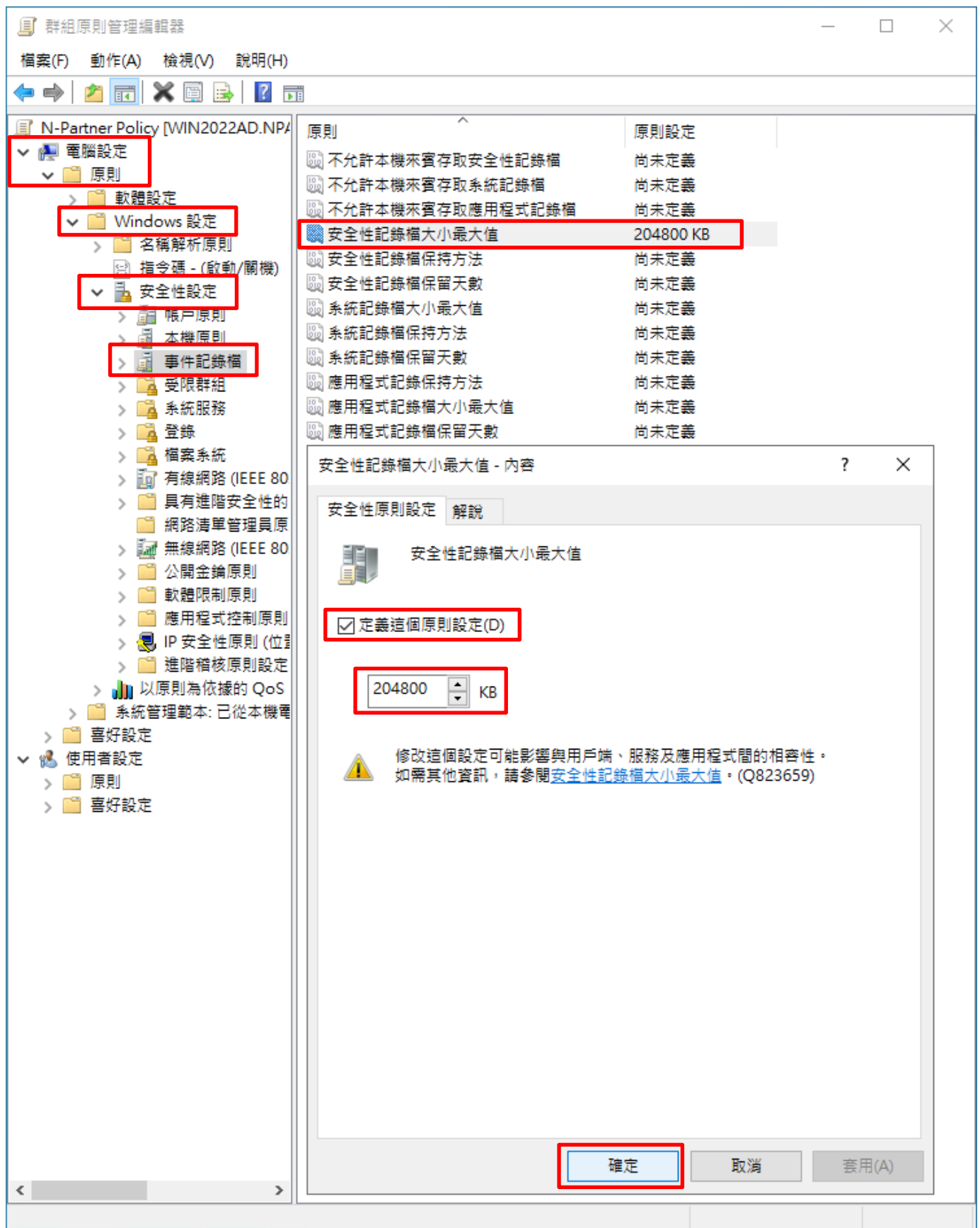
(5) 本機原則：稽核原則

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]



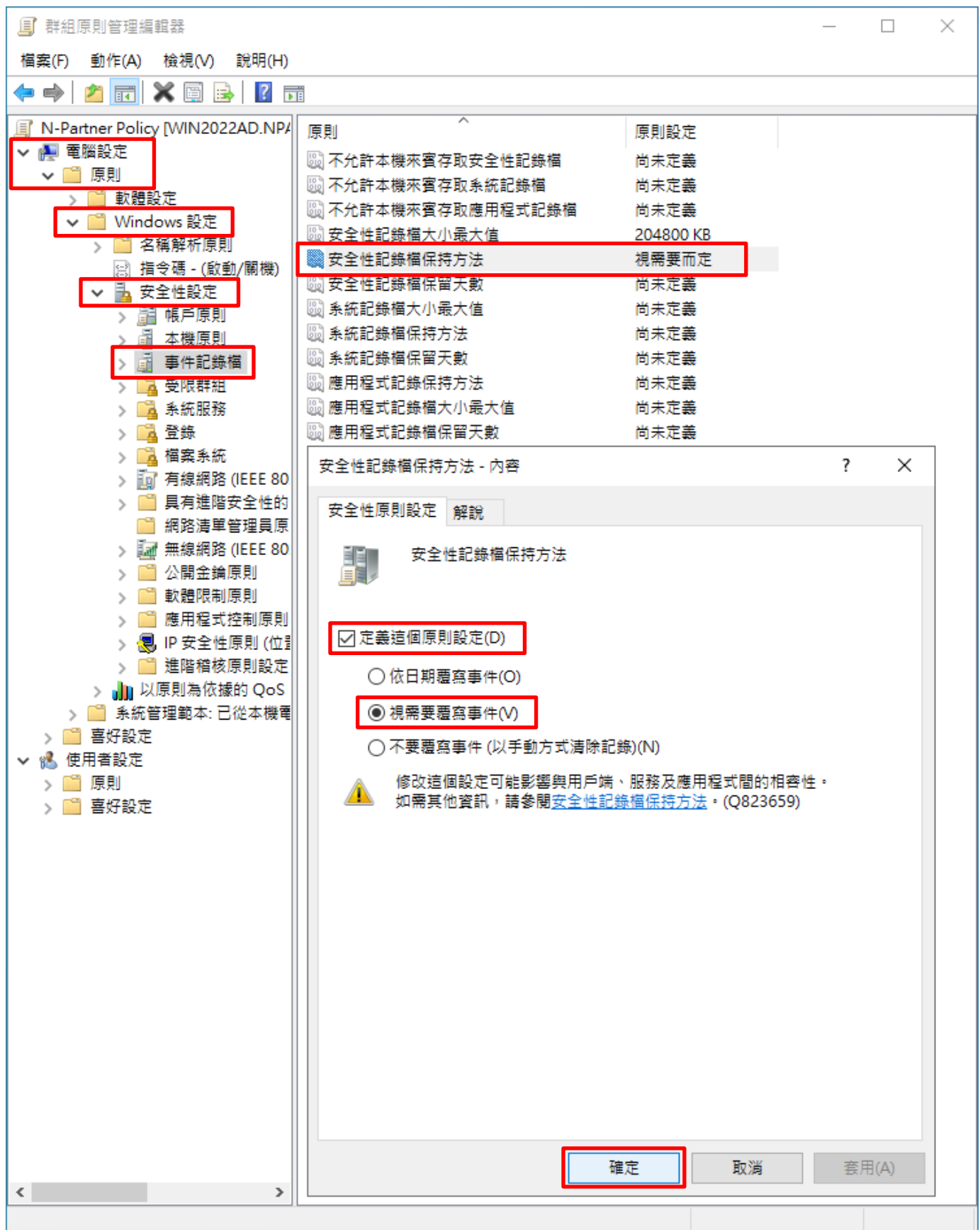
(6) 事件記錄檔：安全性記錄檔大小最大值

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-GPUdate -Computer Win2022 -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command `Invoke-GPUdate -Computer Win2022 -RandomDelayInMinutes 0 -Force` being entered. The output shows the command has executed successfully, with a cursor on the next line.

```
系統管理員: Windows PowerShell
PS C:\> Invoke-GPUdate -Computer Win2022 -RandomDelayInMinutes 0 -Force
PS C:\> _
```

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
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the command `Get-GPResultantSetofPolicy -Computer Win2022 -Path C:\tmp\Win2022.html -ReportType html` being entered. The output displays the following information:

```
系統管理員: Windows PowerShell
PS C:\> Get-GPResultantSetofPolicy -Computer Win2022 -Path C:\tmp\Win2022.html -ReportType html

RsopMode           : Logging
Namespace          : \\Win2022\Root\Rsop\NSE59DD34B_FD2A_4E78_88DF_7717ADA12057
LoggingComputer   : Win2022
LoggingUser        : NPARTNER\administrator
LoggingMode        : Computer

PS C:\> _
```

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

**群組原則結果**

**NPARTNER\WIN2022**  
資料收集: 2022/8/18 下午 04:10:30 全部顯示

**摘要** 顯示

**電腦詳細資料** 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

**原則** 隱藏

Windows 設定 隱藏

安全性設定 隱藏

    帳戶原則/密碼規則 顯示

    帳戶原則/帳戶鎖定原則 顯示

    本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核系統事件	成功, 失敗	N-Partner Policy
稽核物件存取	成功, 失敗	N-Partner Policy
稽核原則變更	成功, 失敗	N-Partner Policy
稽核帳戶登入事件	成功, 失敗	N-Partner Policy
稽核帳戶管理	成功, 失敗	N-Partner Policy
稽核登入事件	成功, 失敗	N-Partner Policy
稽核程序追蹤	成功, 失敗	N-Partner Policy

本機原則/安全性選項 顯示

事件記錄檔 隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

**群組原則物件** 顯示

**WMI 篩選器** 顯示

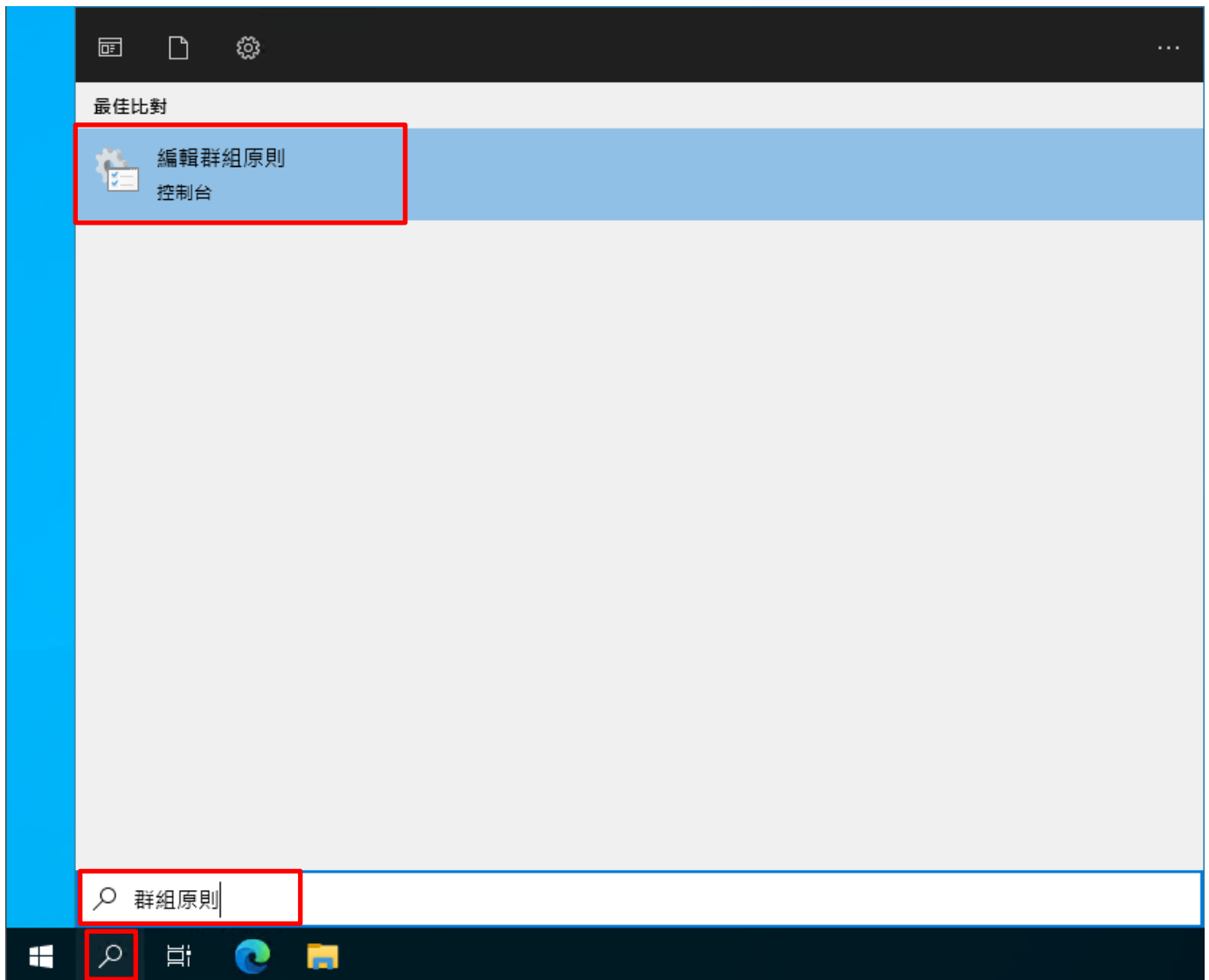
**使用者詳細資料** 顯示

## 8.2 工作群組

### 8.2.1 稽核原則設定

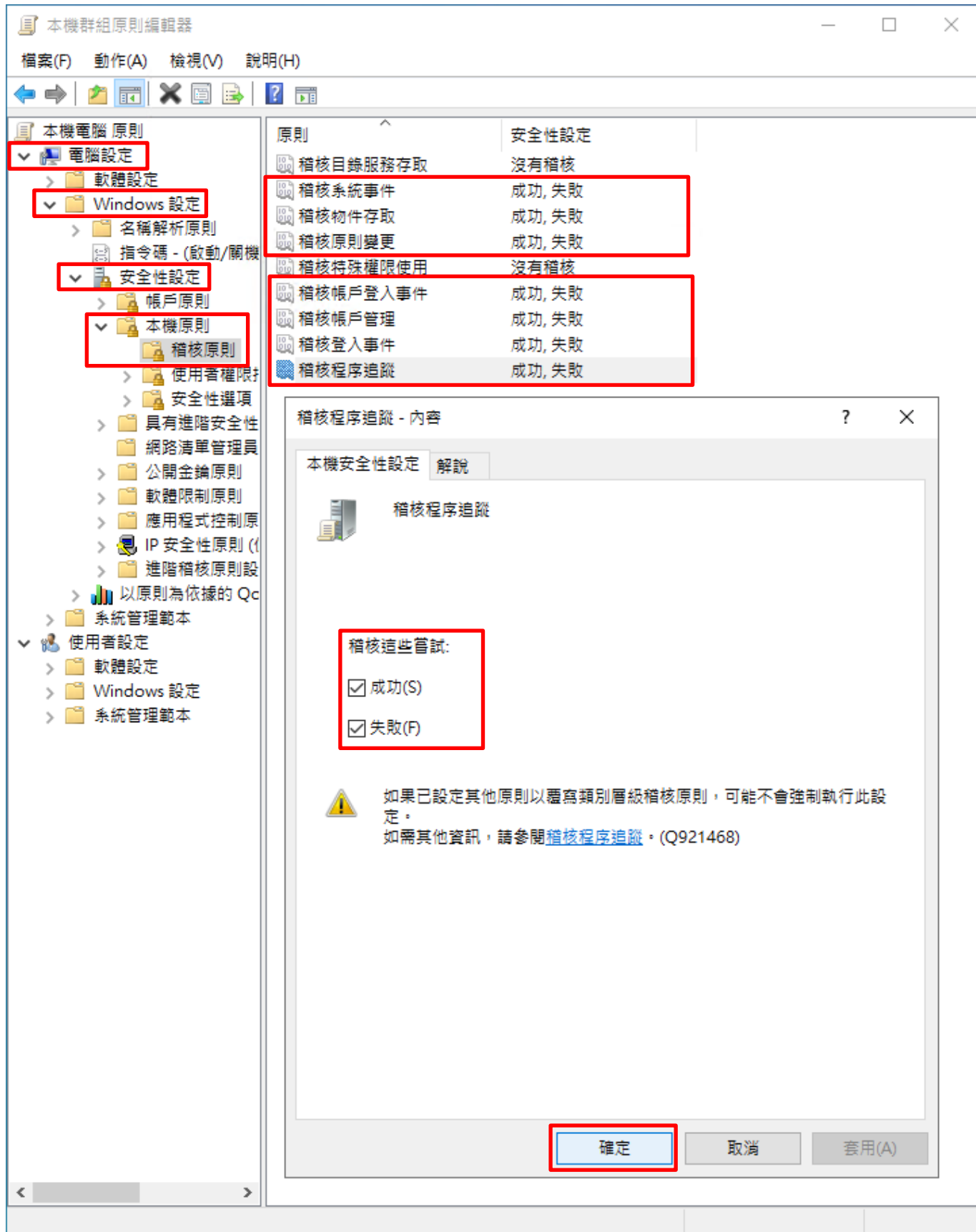
(1) 開啟本機群組原則編輯器

點選  [搜尋] -> 輸入 群組原則 -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核系統事件], [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]

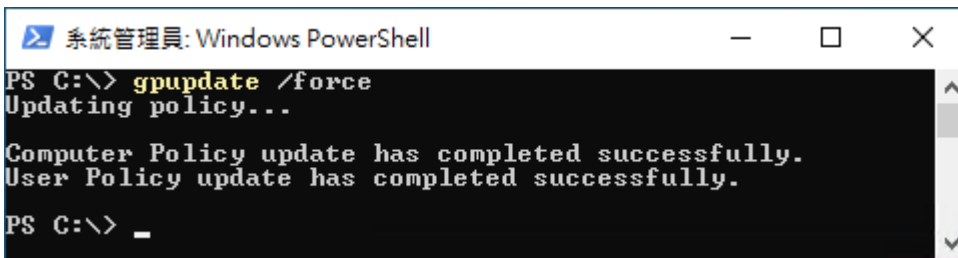


(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force



(5) 查看群組原則套用情形

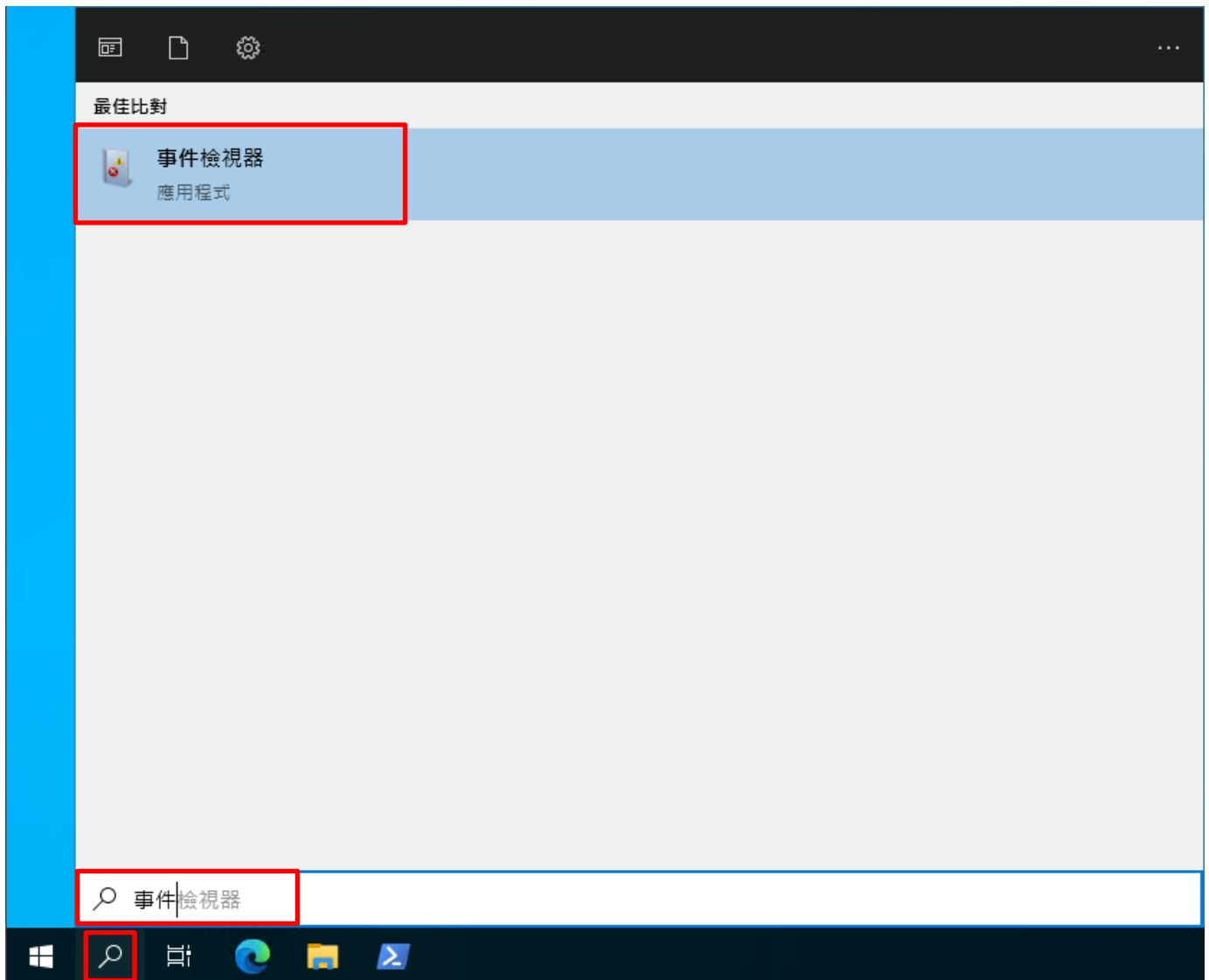
PS C:\> auditpol /get /category:\*

```
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
  MPSSUC 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:\>
```

## 8.2.2 事件檔案設定

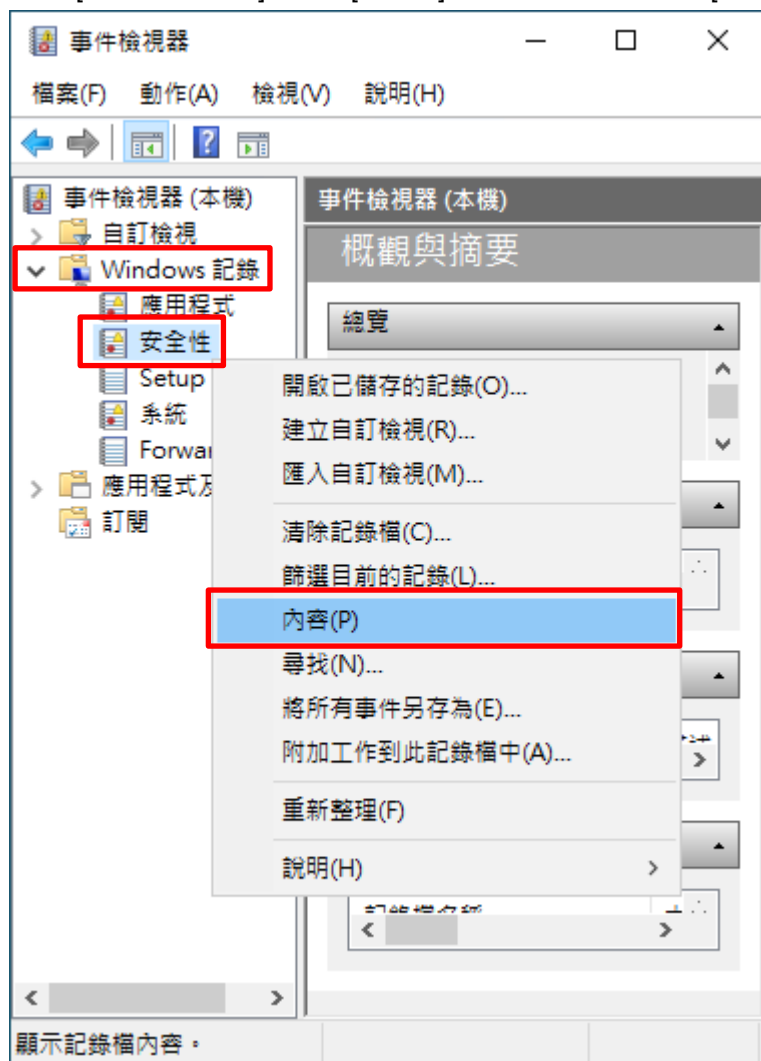
(1) 開啟 [事件檢視器]

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]

記錄內容 - 安全性 (類型: 系統管理)

一般

全名(F): Security

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

記錄檔大小: 16.07 MB(16,846,848 位元組)

建立日期: 2022年3月8日 下午 06:04:42

修改日期: 2022年3月9日 上午 11:20:31

存取日期: 2022年3月9日 上午 11:20:31

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

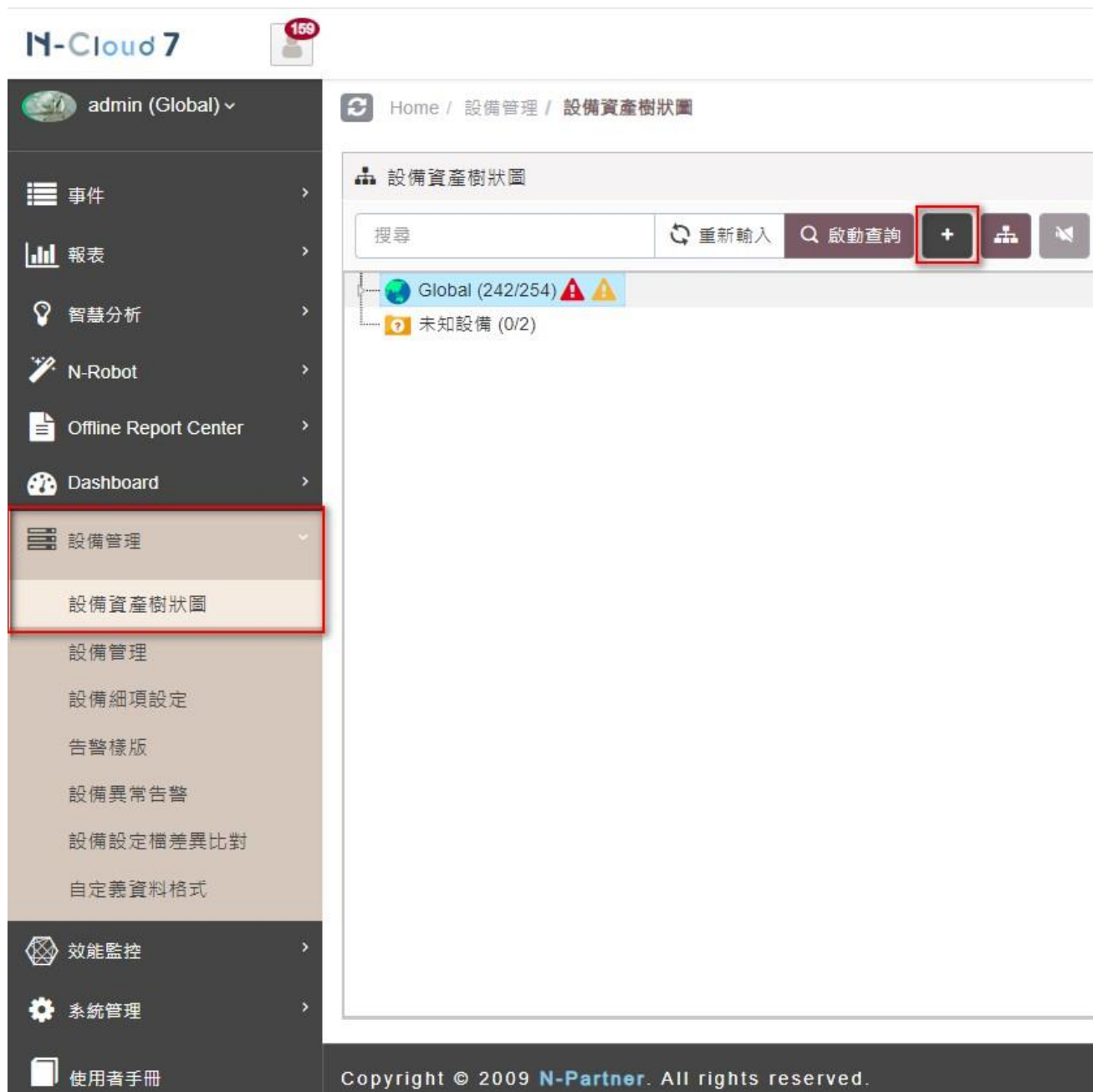
確定 取消 套用(P)



## 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].



The screenshot displays the N-Reporter web interface. On the left is a dark sidebar menu with the user 'admin (Global)' at the top. The '設備管理' (Equipment Management) menu item is highlighted with a red box, and its sub-menu is expanded, also with a red box around it. The sub-menu items include '設備資產樹狀圖' (Equipment Asset Tree View), '設備管理', '設備細項設定', '告警樣版', '設備異常告警', '設備設定檔差異比對', and '自定義資料格式'. The main content area shows the breadcrumb 'Home / 設備管理 / 設備資產樹狀圖'. Below this is a search bar with a '搜尋' (Search) button, a '重新輸入' (Refresh) button, and a '啟動查詢' (Start Query) button. A red box highlights a '+' button next to the search bar. Below the search bar, there is a tree view showing 'Global (242/254)' with two warning icons and '未知設備 (0/2)' (Unknown Equipment (0/2)). At the bottom of the page, there is a copyright notice: 'Copyright © 2009 N-Partner. All rights reserved.'

(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 ].

### 新增設備 - 設備基本設定

設備基本設定

設備名稱 \*

Win2008 CHT 192.168.14.86

IP \*

192.168.14.86

所屬領域 \*

Global

Syslog 資料格式 ⓘ 

Windows

自定義資料格式 ⓘ 

請選擇...

SNMP Model ⓘ

請選擇...

Web 監控 ⓘ

啟用網頁監控功能

上一步 下一步 取消

左點[ 下一步 ]。

### 新增設備 - SNMP 相關設定

#### SNMP 相關設定

SNMP IP

Version

V2C

Read Community

public

Write Community

SNMP Timeout(秒)

5

編碼方式

UTF-8

設備 (介面與磁碟分割區) 搜尋 Timeout (秒)

120

SNMP V3

上一步 下一步 取消

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**。

**新增設備 - Syslog 相關設定**

**Syslog 相關設定**

**Facility** ⓘ

-----

**編碼方式**

UTF-8

**Syslog 正規化資料保留天數上限** ⓘ

-----

**Raw Data 保留與轉發**

Raw Data 保留

本設備於分時監控報表啟動 Syslog 轉發時，採用 Raw Data 格式

轉發方式將使用來源設備的 IP

上一步 下一步 取消

左點[ 下一步 ]。

### 新增設備 - 監控與告警

告警樣版 ^

ICMP 告警樣版

請選擇... v

設備告警樣版

請選擇... v

程序告警樣版

請選擇... v

自訂 OID 樣版

NTP 告警樣版

請選擇... v

監控與連線測試 v

告警通報設定 v

告警細項設定 v

上一步 下一步 取消

左點[ 下一步 ]。

新增設備 - 其它

其它

設備 Icon 

Host

經緯度

緯度, 經度

接收狀態

啟用  停用

設備共享 

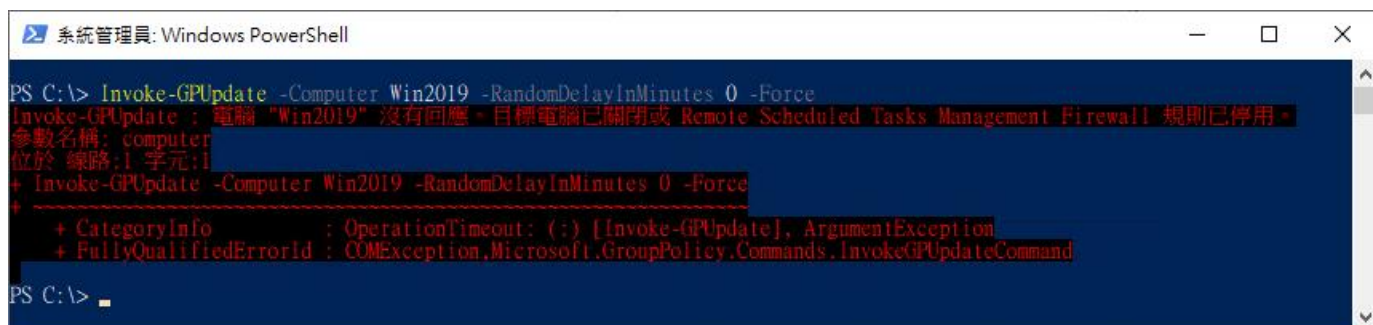
設備共享

上一步 下一步 取消

## 10. 問題排除

### 10.1 Invoke-GPUdate 錯誤

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



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

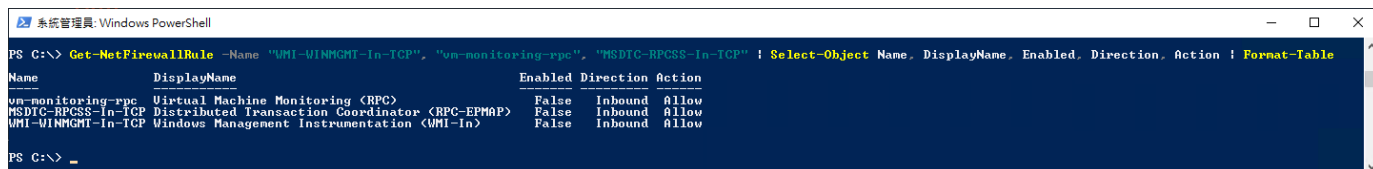
PS C:\> _
```

(2) 在 Windows 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
```



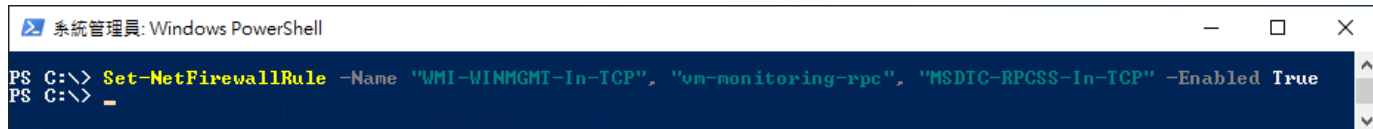
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```

Name	DisplayName	Enabled	Direction	Action
vm-monitoring-rpc	Virtual Machine Monitoring (RPC)	False	Inbound	Allow
MSDTC-RPCSS-In-TCP	Distributed Transaction Coordinator (RPC-EPMAP)	False	Inbound	Allow
WMI-WINMGMT-In-TCP	Windows Management Instrumentation (WMI-In)	False	Inbound	Allow

```
PS C:\> _
```

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

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

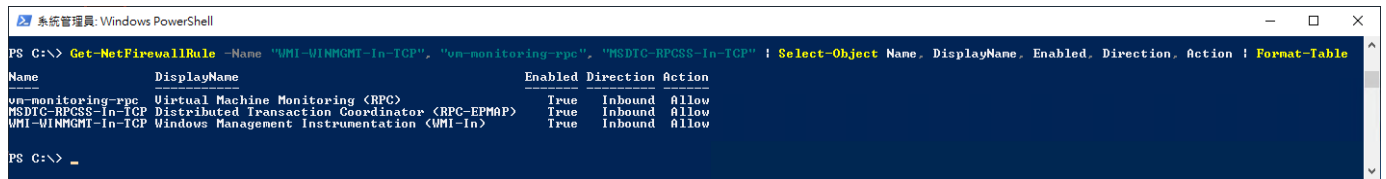


```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
PS C:\> _
```



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

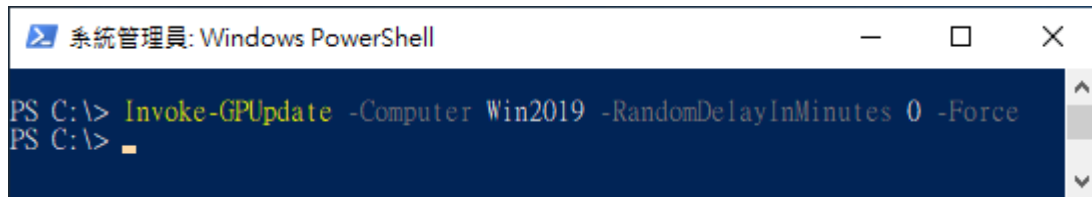
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |  
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



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

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

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

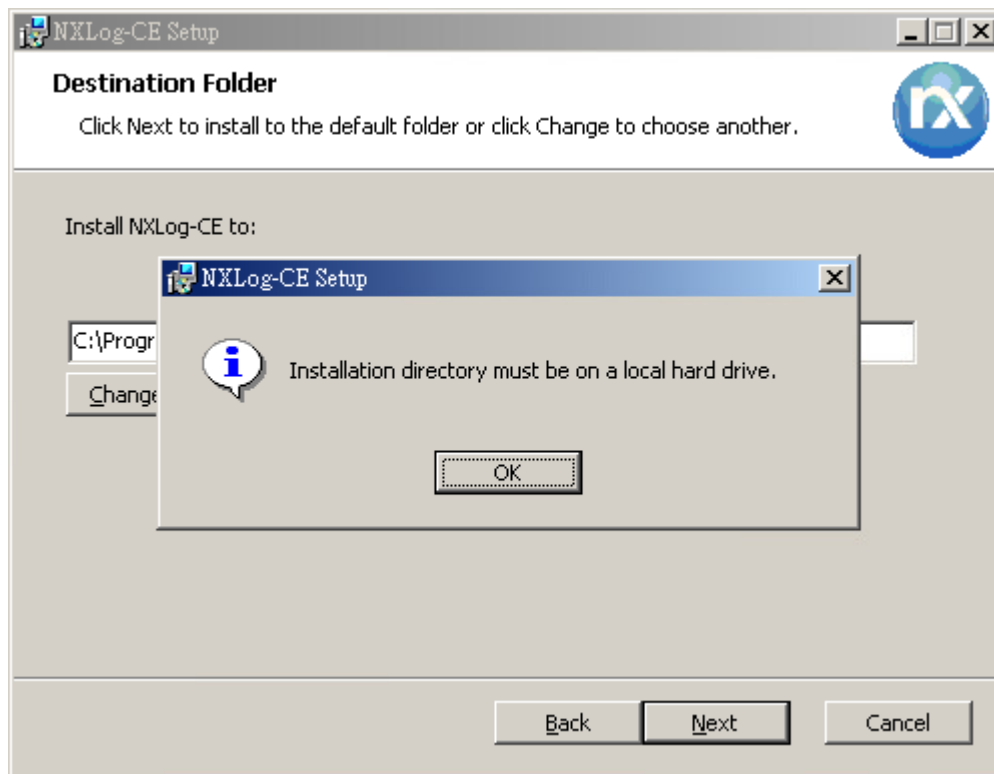


```
系統管理員: Windows PowerShell  
PS C:\> Invoke-GPUdate -Computer Win2019 -RandomDelayInMinutes 0 -Force  
PS C:\> _
```

紅色文字部位請輸入 Windows Server 伺服器名稱

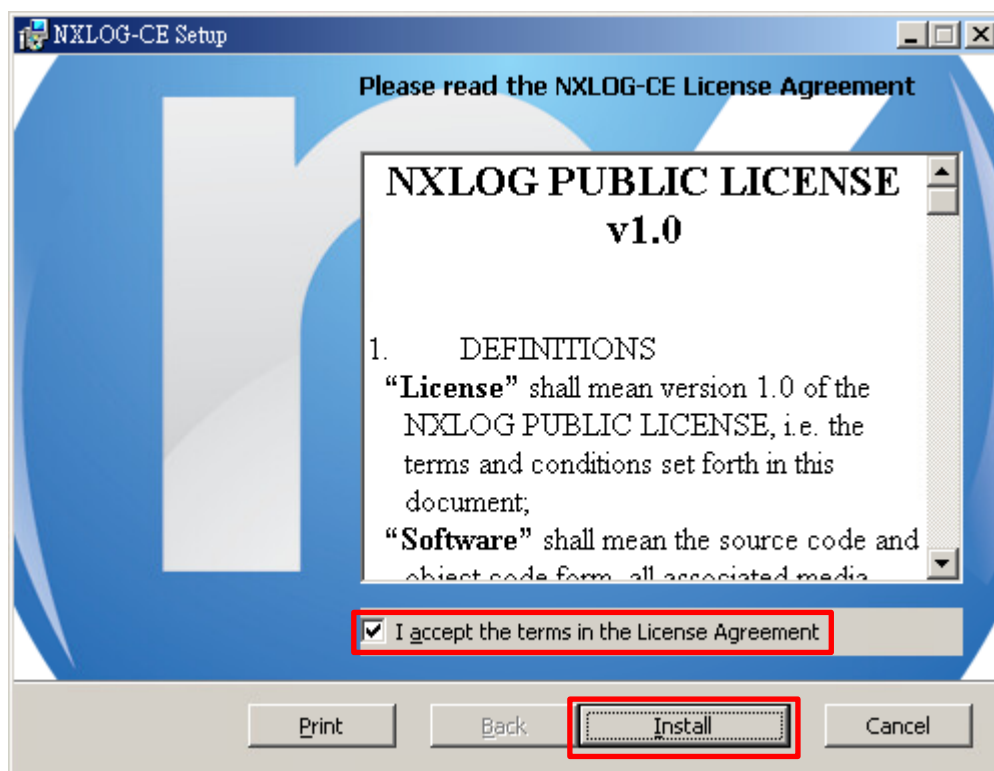
## 10.2 NXLog 安裝問題

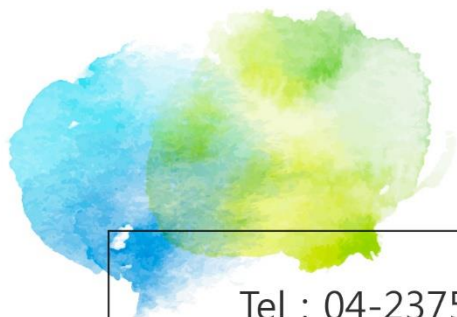
(1) 安裝 NXLog(2.10.2150) 顯示 Installation directory must be on a local hard drive.



(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](mailto:sales@npartner.com)

技術詢問 : [support@npartner.com](mailto:support@npartner.com)