

Partner

如何設定

Windows AD 事件記錄

V018

2024/07/10



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	3
1. NXLog	4
1.1 NXLog 安裝.....	4
1.2 NXLog 設定檔下載.....	6
1.2.1 Windows 2003 或之前版本作業系統.....	6
1.2.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄.....	6
1.2.1.2 輸出全部事件記錄.....	7
1.2.2 Windows 2008 或之後版本作業系統.....	8
1.2.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄.....	8
1.2.2.2 輸出應用程式、安全性、系統全部事件記錄.....	9
1.3 NXLog 設定檔.....	10
1.3.1 Windows 2003 或之前版本作業系統.....	10
1.3.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄.....	10
1.3.1.2 輸出全部事件記錄.....	11
1.3.2 Windows 2008 或之後版本作業系統.....	12
1.3.2.1 輸出主機稽核、物件存取、帳戶管理事件記錄.....	12
1.3.2.2 輸出應用程式、安全性、系統全部事件記錄.....	13
1.4 NXLog 啟動服務.....	14
1.4.1 Windows 2003 或之前版本作業系統.....	14
1.4.2 Windows 2008 或之後版本作業系統.....	17
2. Windows 2000	20
2.1 組織單位設定.....	20
2.2 群組原則設定.....	23
2.3 設定 WMI.....	30
2.3.1 新增非管理帳號.....	32
2.3.2 設定 DCOM 權限.....	35
2.3.3 設定 WMI 權限.....	38
2.3.3.1 設定事件日誌權限.....	38
2.3.3.2 設定讀取使用者資料權限.....	42
2.3.4 設定 Event log 讀取權限.....	47
2.3.5 重啟 WMI 服務.....	53
3. Windows 2003	54
3.1 組織單位設定.....	54
3.2 群組原則設定.....	58
3.3 設定 WMI.....	66
3.3.1 新增非管理帳號.....	68
3.3.2 設定 DCOM 權限.....	69
3.3.3 設定 WMI 權限.....	73
3.3.3.1 設定事件日誌權限.....	73
3.3.3.2 設定讀取使用者資料權限.....	78
3.3.4 設定 Event log 讀取權限.....	83
3.3.5 重啟 WMI 服務.....	90
3.3.6 設定防火牆.....	92
4. Windows 2008	94

組織單位設定.....	94
4.2 群組原則設定.....	98
4.3 設定 WMI.....	105
4.3.1 新增非管理帳號.....	106
4.3.2 設定 DCOM 權限.....	107
4.3.3 設定 WMI 權限.....	112
4.3.3.1 設定事件日誌權限.....	112
4.3.3.2 設定讀取使用者資料權限.....	117
4.3.4 設定 Event log 讀取權限.....	122
4.3.5 重啟 WMI 服務.....	127
4.3.6 設定防火牆.....	128
5. Windows 2012	130
5.1 組織單位設定.....	130
5.2 群組原則設定.....	134
5.3 設定 WMI.....	141
5.3.1 新增非管理帳號.....	142
5.3.2 設定 DCOM 權限.....	143
5.3.3 設定 WMI 權限.....	148
5.3.3.1 設定事件日誌權限.....	148
5.3.3.2 設定讀取使用者資料權限.....	153
5.3.4 設定 Event log 讀取權限.....	158
5.3.5 重啟 WMI 服務.....	164
5.3.6 設定防火牆.....	165
6. Windows 2016	166
6.1 組織單位設定.....	166
6.2 群組原則設定.....	170
6.3 設定 WMI.....	177
6.3.1 新增使用者.....	178
6.3.2 設定 DCOM 權限.....	179
6.3.3 設定 WMI 權限.....	184
6.3.3.1 設定事件日誌權限.....	184
6.3.3.2 設定讀取使用者資料權限.....	189
6.3.4 設定 Event log 讀取權限.....	194
6.3.5 重啟 WMI 服務.....	200
6.3.6 設定防火牆.....	201
7. Windows 2019	202
7.1 組織單位設定.....	202
7.2 群組原則設定.....	206
7.3 設定 WMI.....	213
7.3.1 新增非管理帳號.....	214
7.3.2 設定 DCOM 權限.....	215
7.3.3 設定 WMI 權限.....	220
7.3.3.1 設定事件日誌權限.....	220
7.3.3.2 設定讀取使用者資料權限.....	225

7.3.4 設定 Event log 讀取權限	230
7.3.5 重啟 WMI 服務.....	236
7.3.6 設定防火牆.....	237
8. Windows 2022	238
8.1 組織單位設定	238
8.2 群組原則設定	242
8.3 設定 WMI.....	249
8.3.1 新增非管理帳號.....	249
8.3.2 設定 DCOM 權限.....	251
8.3.3 設定 WMI 權限.....	256
8.3.3.1 設定事件日誌權限.....	256
8.3.3.2 設定讀取使用者資料權限.....	261
8.3.4 設定 Event log 讀取權限	266
8.3.5 重啟 WMI 服務.....	272
8.3.6 設定防火牆.....	273
9. N-Reporter	274
9.1 Windows 2003 或之前版本作業系統	275
9.2 Windows 2008 或之後版本作業系統	276
10. 問題排除	277
10.1 WMI Query Language 檢查.....	277
10.1.1 查詢事件日誌.....	278
10.1.2 查詢使用者資料.....	282
10.2 NXLog 安裝問題.....	286

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 AD 事件記錄。

NXLog 工具將 Windows AD 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 AD 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-3.0.2284.msi



(2) 安裝 NXLog

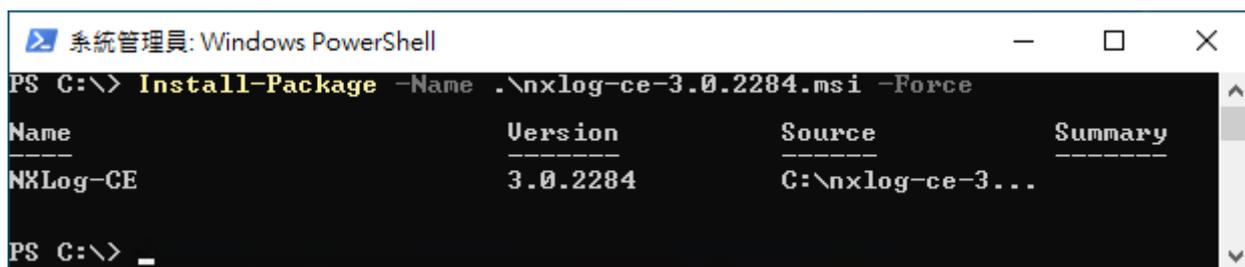
<2.1> Windows 2008 或之後版本作業系統

<2.1.1> 開啟 [Windows PowerShell]



<2.1.2> 安裝 NXLog 軟體

PS C:\> **Install-Package -Name .\nxlog-ce-3.0.2284.msi -Force**

A screenshot of a Windows PowerShell window titled '系統管理員: Windows PowerShell'. The command prompt shows the command 'Install-Package -Name .\nxlog-ce-3.0.2284.msi -Force' being executed. Below the command, a table of installed packages is displayed.

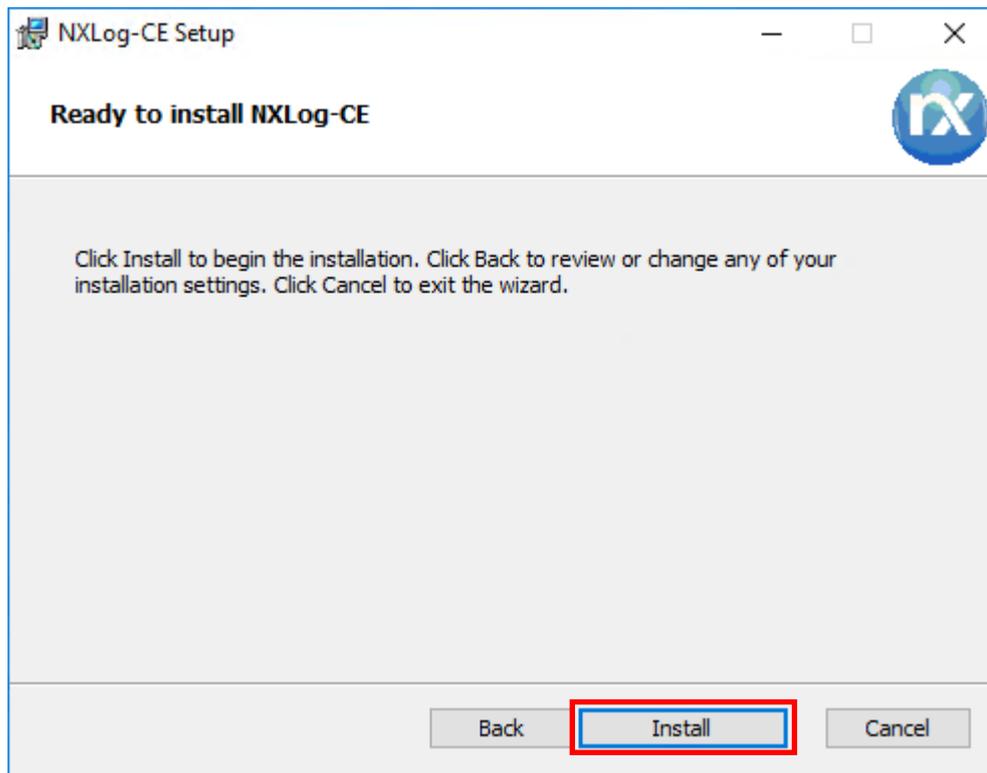
Name	Version	Source	Summary
NXLog-CE	3.0.2284	C:\nxlog-ce-3...	

The prompt ends with 'PS C:\> _'.

紅色文字部位請輸入 NXLog 軟體路徑和檔案

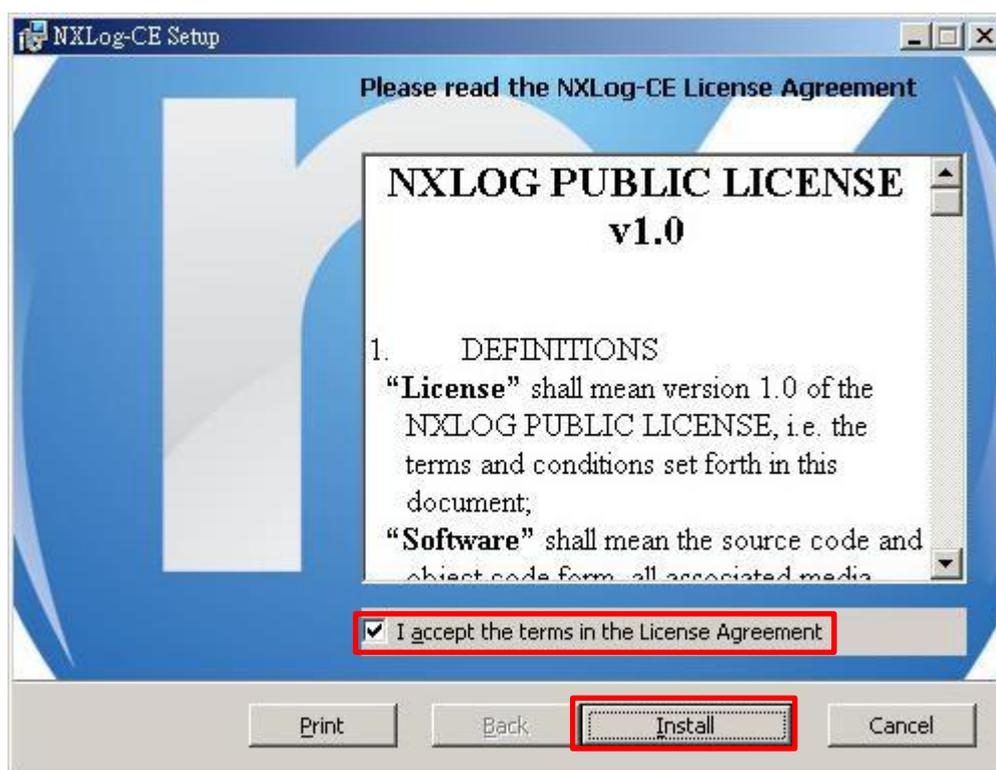
<2.2> Windows 2003

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



<2.3> Windows 2000

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



1.2 NXLog 設定檔下載

1.2.1 Windows 2003 或之前版本作業系統

1.2.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄

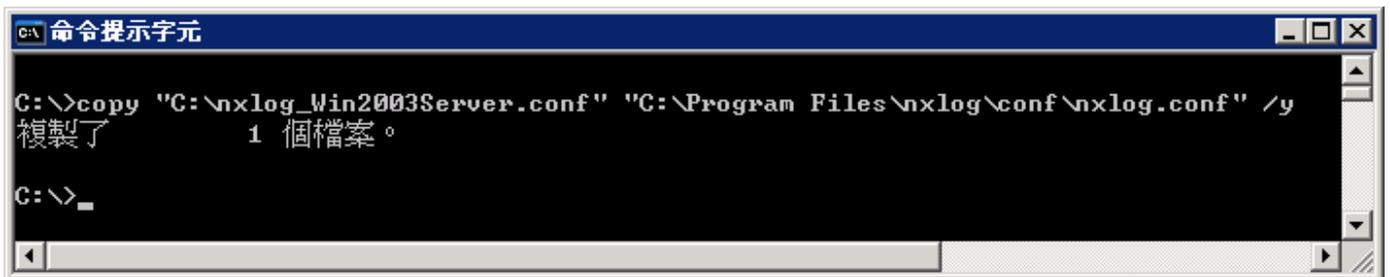
(1) 開啟 [命令提示字元]



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

下載連結：http://www.npartnertech.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

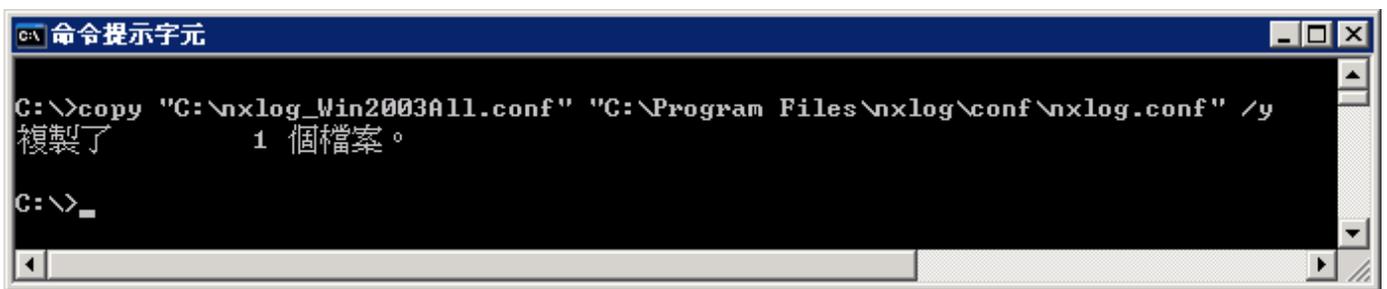
(1) 開啟 [命令提示字元]



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

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

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008Server.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```

A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command prompt shows the execution of the command: `Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008Server.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'`. The command is entered on two lines, with the first line ending in a red prompt character and the second line starting with a red prompt character. The output is not visible.

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.npartnertech.com/download/tech/nxlog_Win2008All.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008All.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The command prompt shows the execution of the command: `Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008All.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'`. The output of the command is not visible, only the prompt `PS C:\> _` is shown.

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 192.168.8.184
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
  Module xm_syslog
</Extension>

## 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 192.168.8.184
```

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

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

1.3.1.2 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      192.168.8.184
define ROOT       C:\Program Files\nxlog
define CERTDIR    %ROOT%\cert
define CONFDIR    %ROOT%\conf
define LOGDIR     %ROOT%\data
define LOGFILE    %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
  Module xm_syslog
</Extension>

## 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 192.168.8.184
```

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

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

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



1.3.2 Windows 2008 或之後版本作業系統

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 192.168.8.184
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
  Module xm_syslog
</Extension>

## 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 192.168.8.184
```

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
```

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



1.4 NXLog 啟動服務

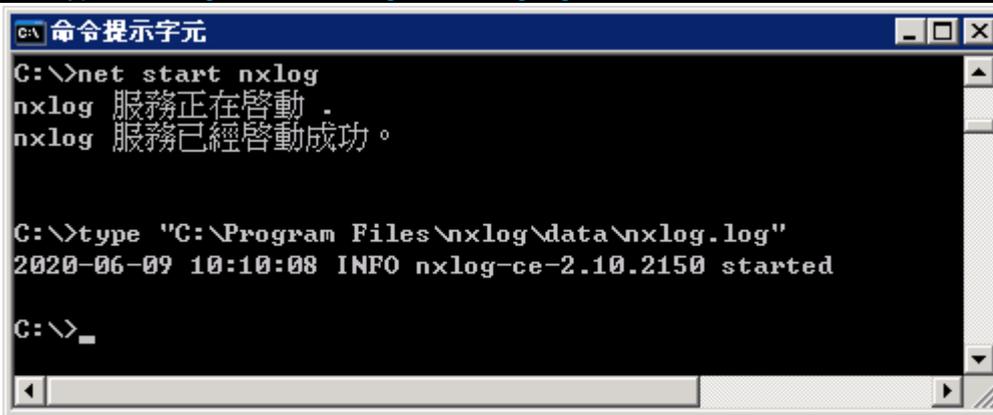
1.4.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]



(2) 啟動 NXLog 服務和確認 NXLog 沒有錯誤訊息

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



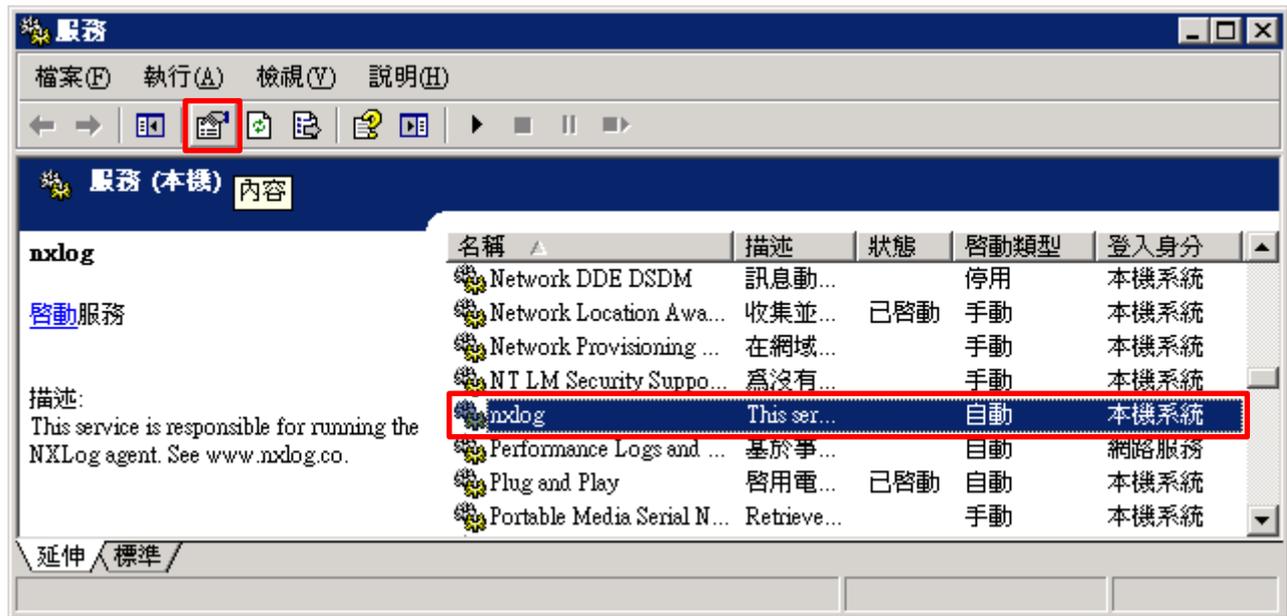
(3) 開啟 [服務] 功能

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

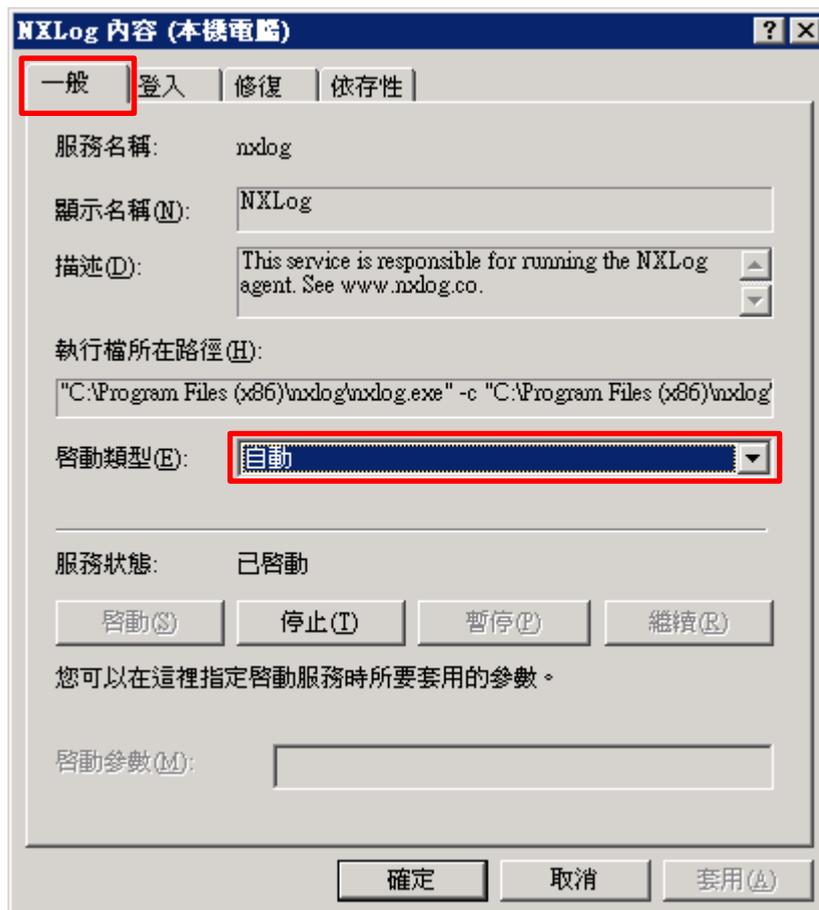


(4) 開啟 NXLog 服務內容

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]

NXLog 內容 (本機電腦)

一般 | 登入 | **修復** | 依存性

如果這項服務執行失敗時，電腦將採取的回應。

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

重設失敗計數於(O): 0 天之後

重新啟動服務於(Y): 1 分鐘之後

執行程式
程式(E):
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)

電腦重新啟動的選項(R)...

確定 取消 套用(A)

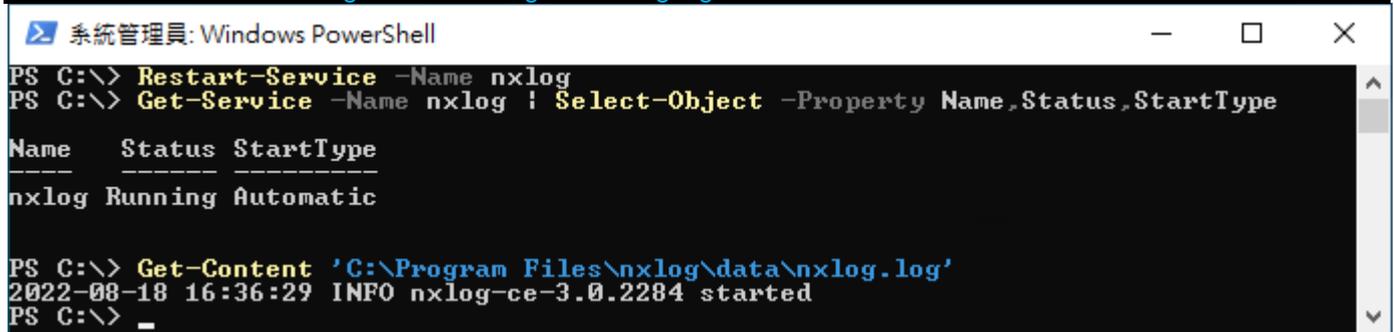
1.4.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]



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

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

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window 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 is a table with columns "Name", "Status", and "StartType", showing "nxlog Running Automatic". The output of the third command is a log entry: "2022-08-18 16:36:29 INFO nxlog-ce-3.0.2284 started".

Name	Status	StartType
nxlog	Running	Automatic

(3) 開啟 [服務] 功能

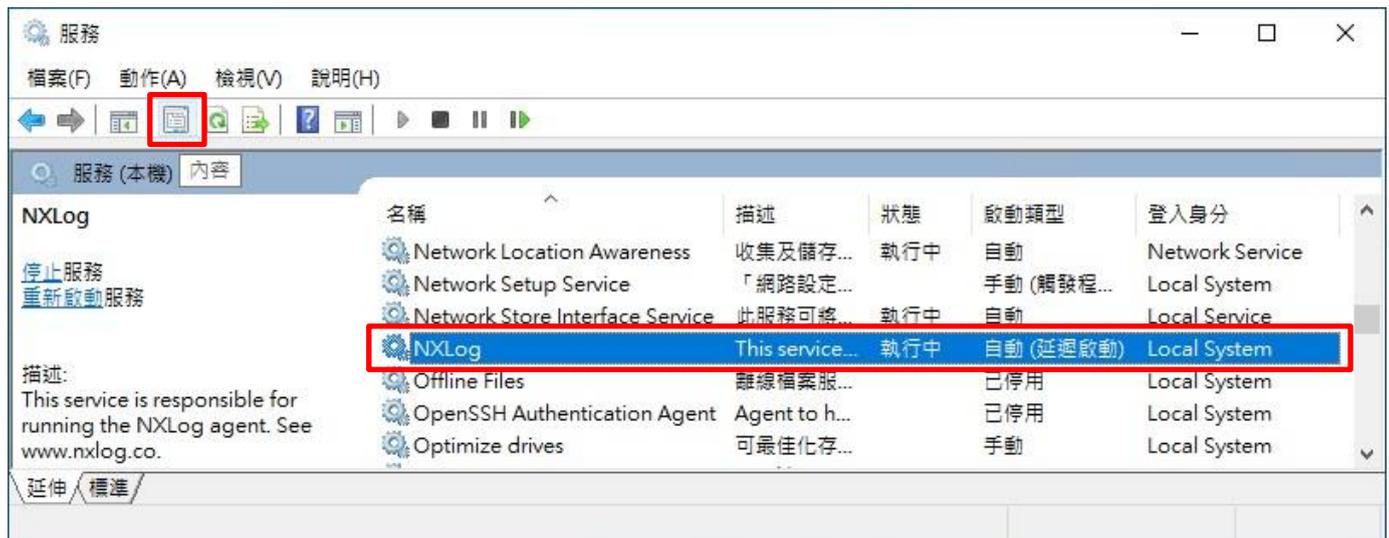
```
PS C:\> Services.msc
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window shows the execution of the command "Services.msc".

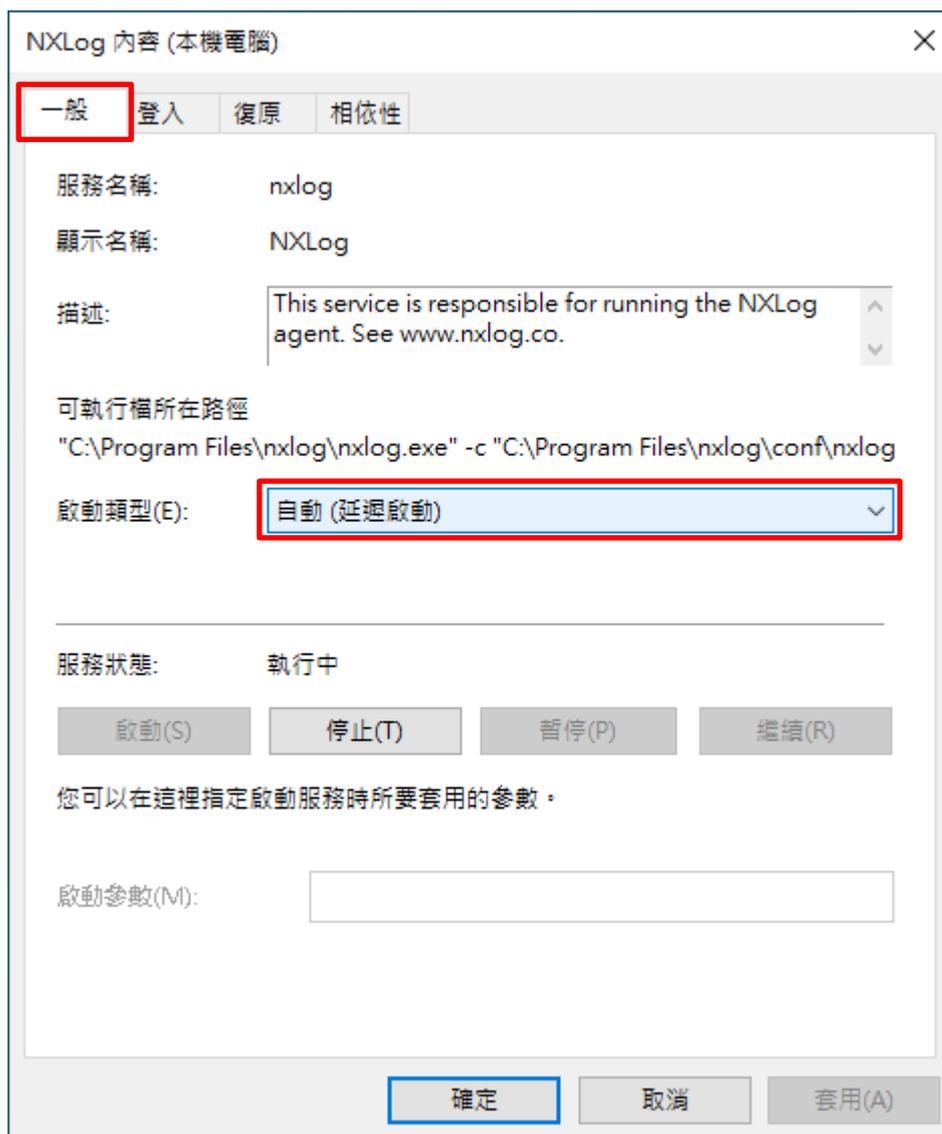
```
PS C:\> Services.msc
PS C:\> _
```

(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認 ; 啟動類型: [自動 (延遲啟動)]



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

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P): 瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%) (E)

確定 取消 套用(A)

2. Windows 2000

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

2.1 組織單位設定

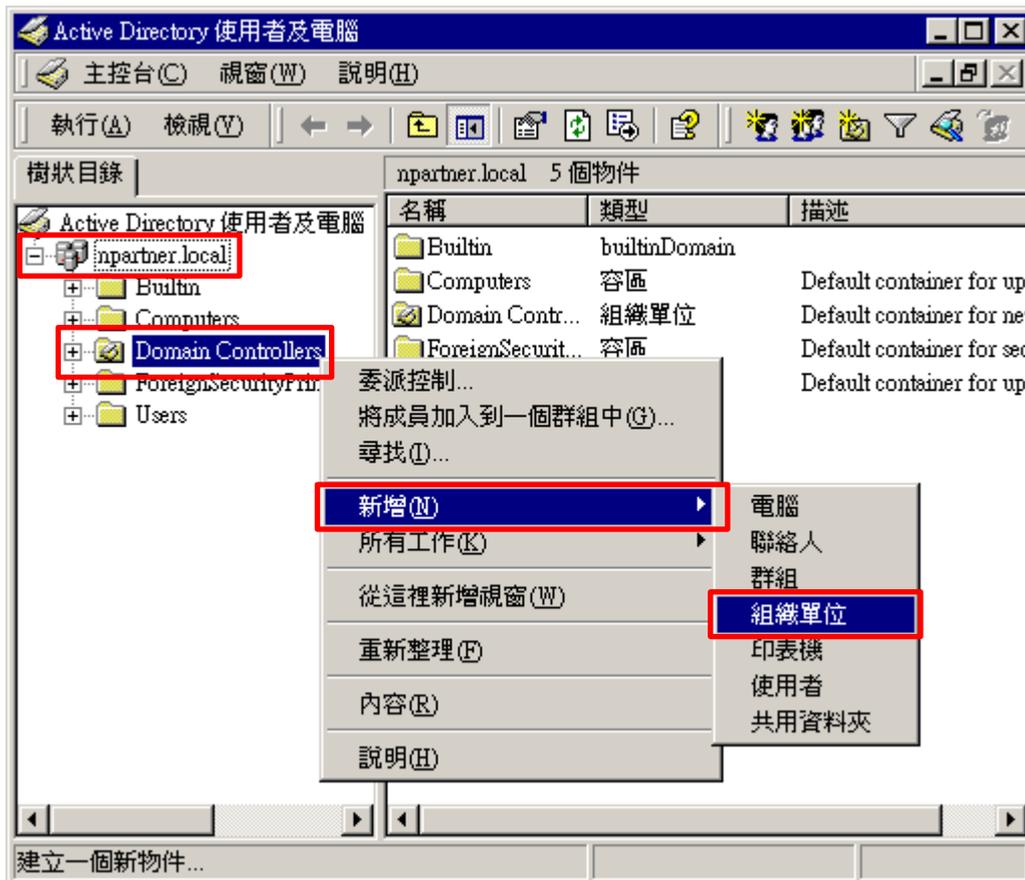
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



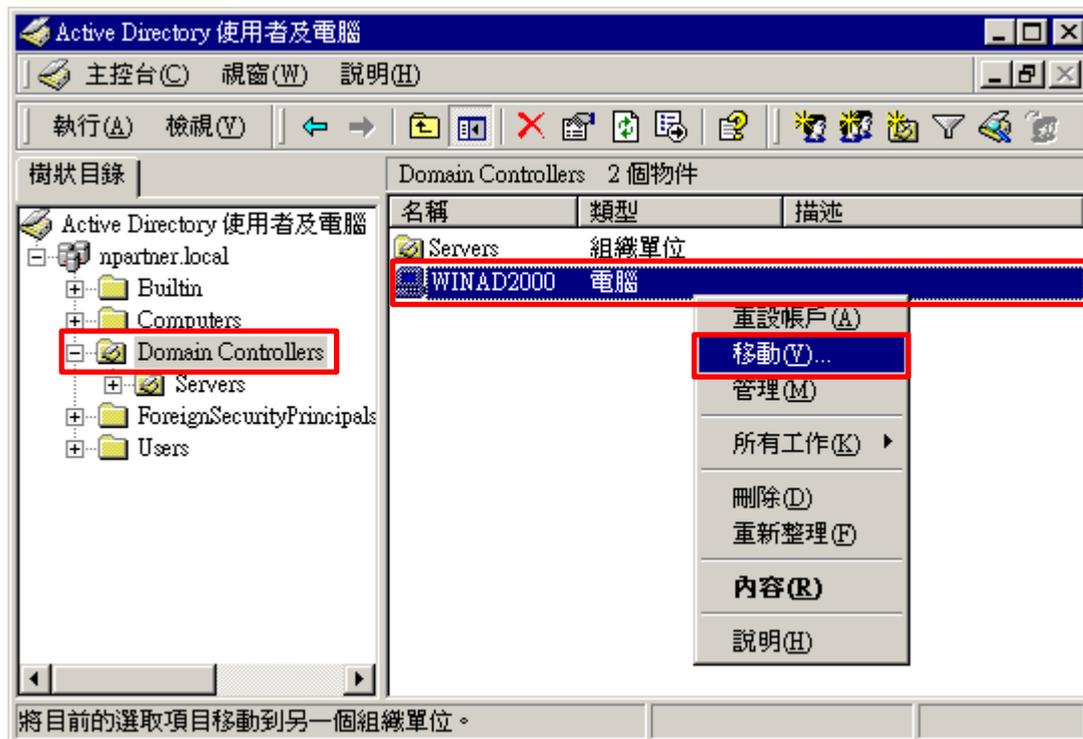
(3) 輸入組織單位名稱

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 [Domain Controllers] 組織單位 -> 在 [WinAD2000] 網域伺服器，按滑鼠右鍵，註: 請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]



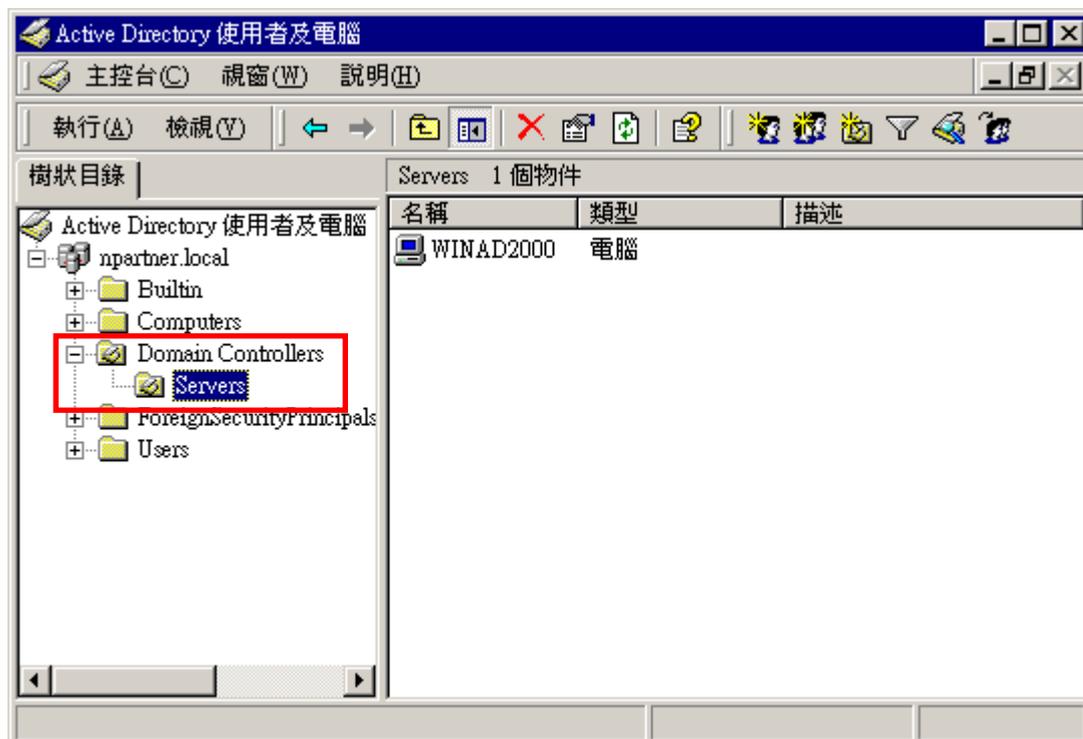
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2000] 網域伺服器已移動。



2.2 群組原則設定

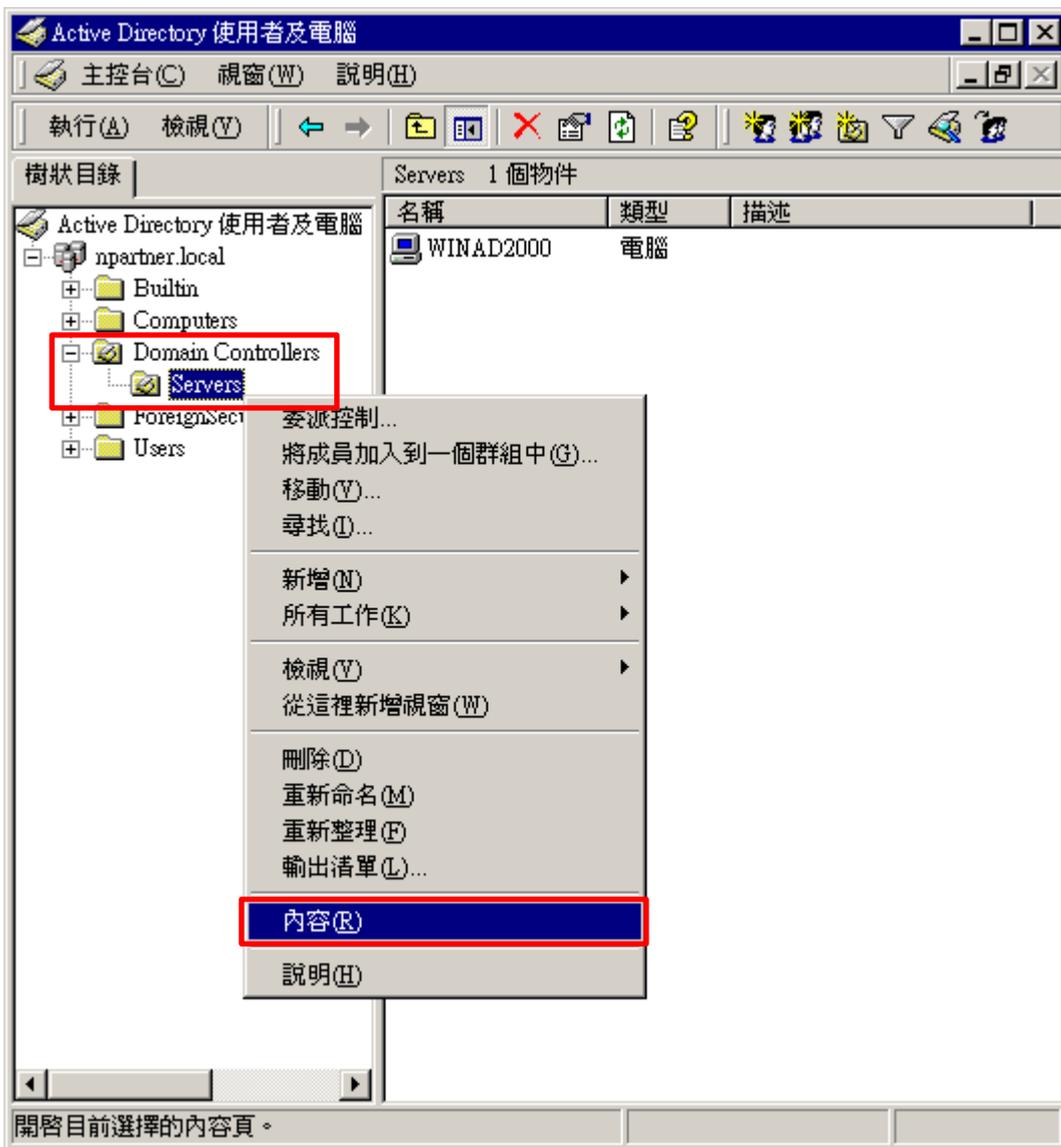
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



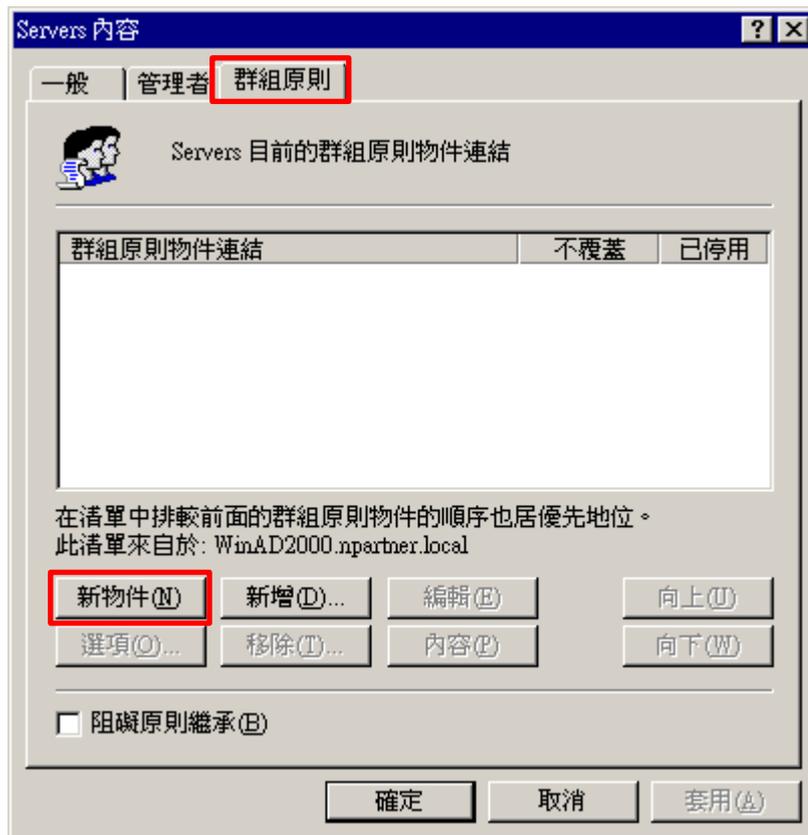
(2) 在 Servers 組織單位，點選內容

展開 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



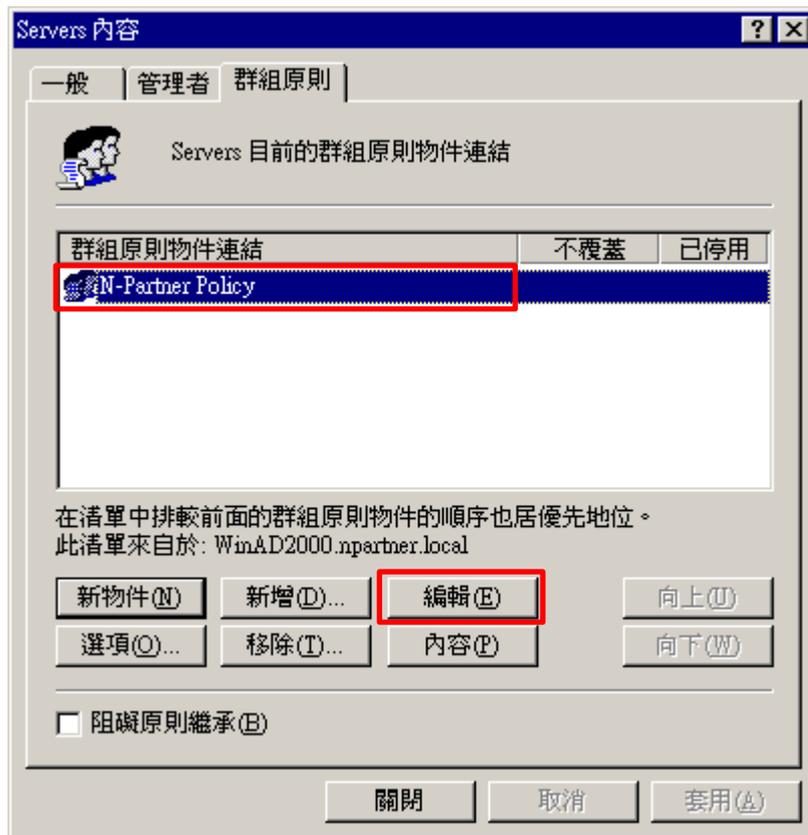
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



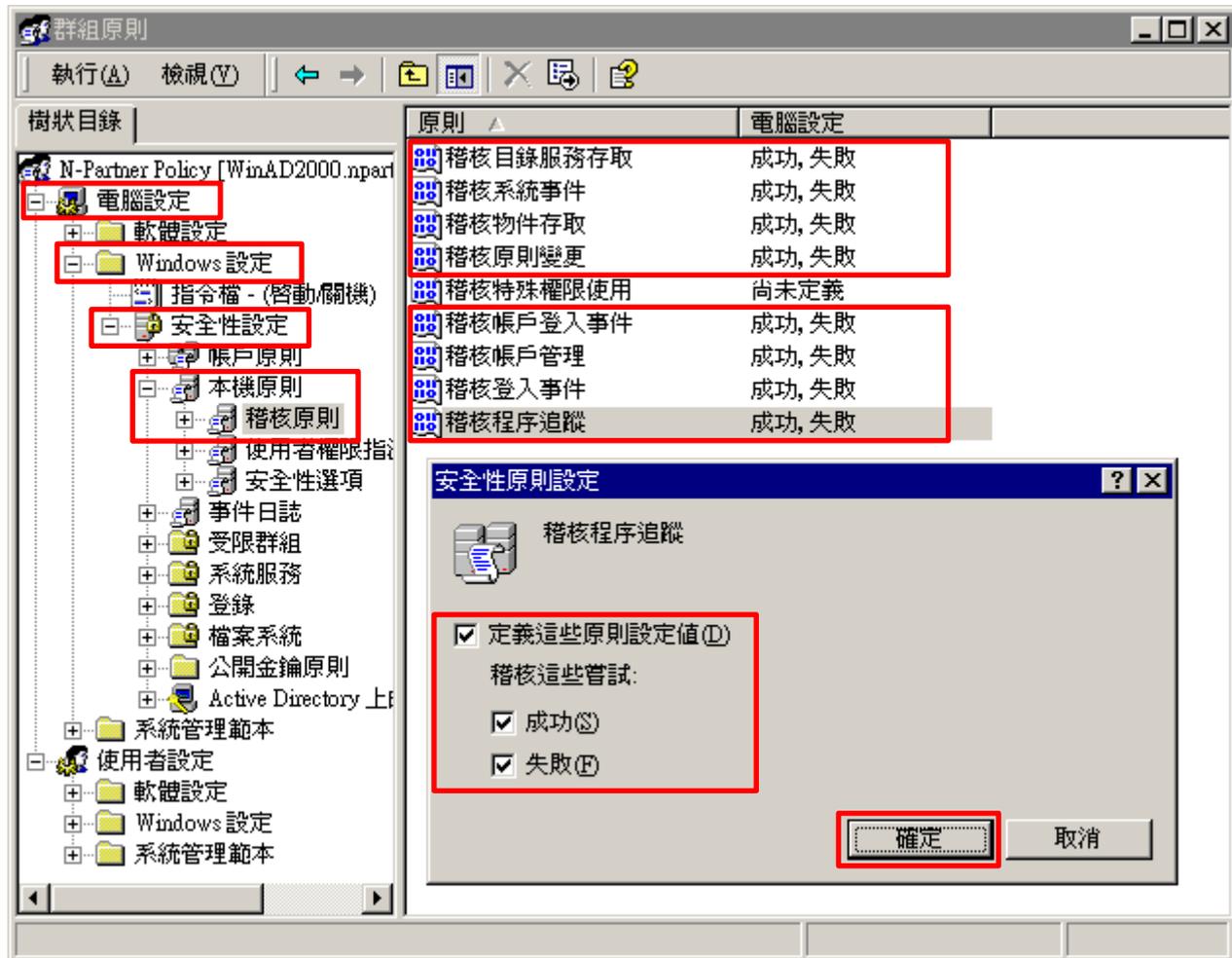
(4) 編輯群組原則物件

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]



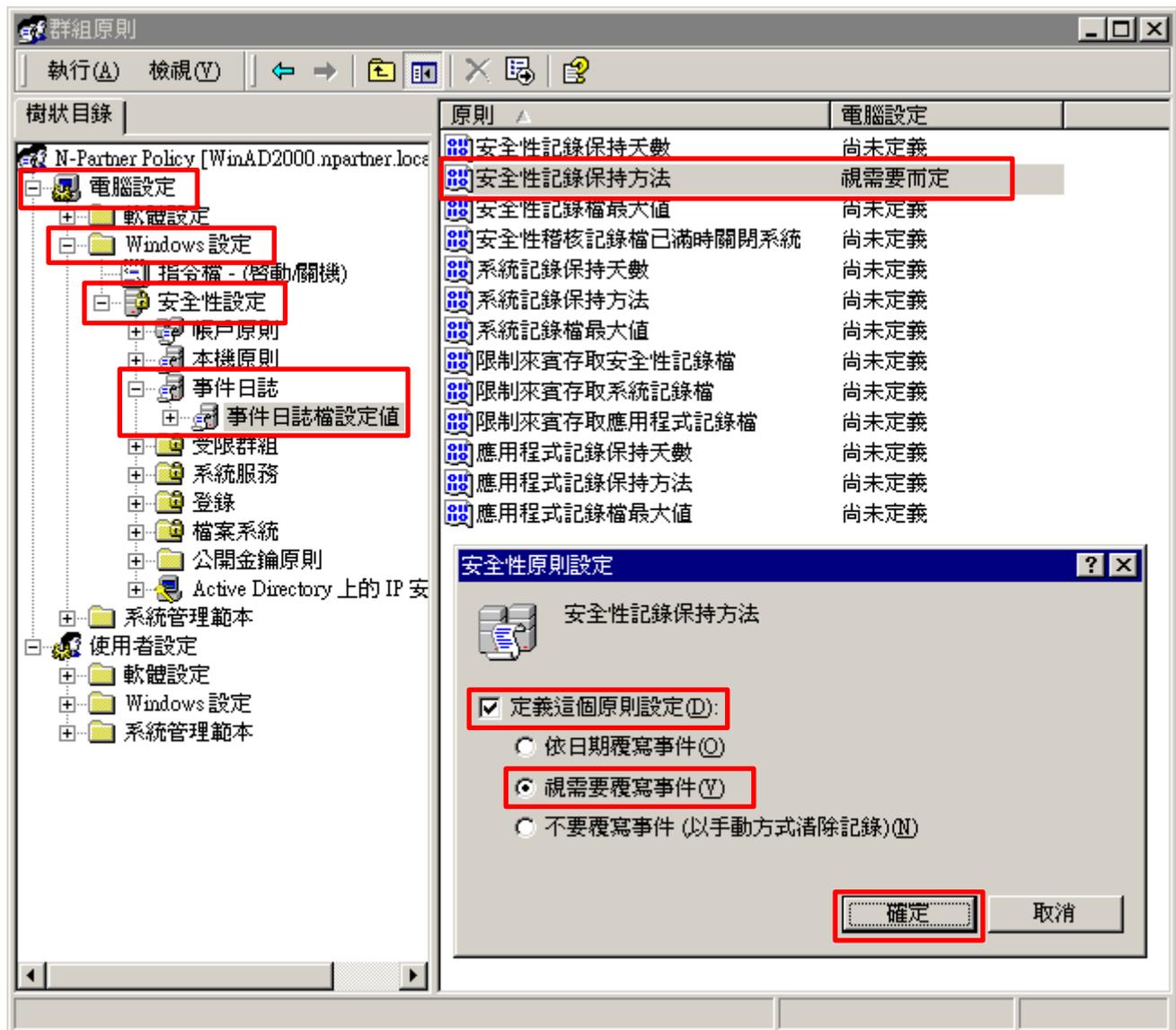
(5) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [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 [定義這些原則設定值] & [成功] & [失敗] -> 按 [確定]



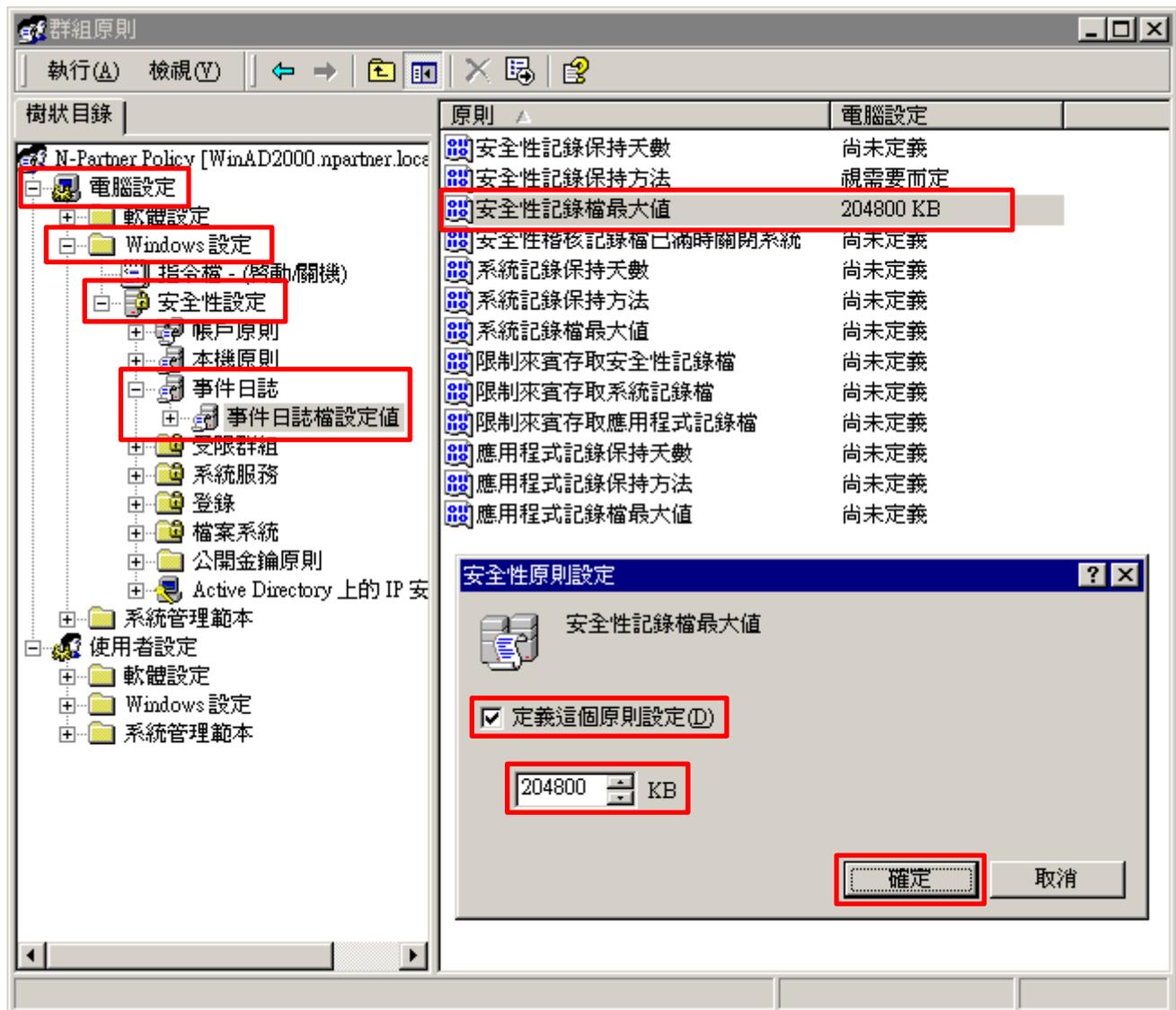
(6) 事件日誌：安全性記錄保持方法

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) 開啟 [命令提示字元]



(9) 更新群組原則。

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



```
命令提示字元
C:\>secdit /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:\>_
```

2.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

KH 內容

撥入	環境	工作階段	遠端控制	終端機服務設定檔		
一般	地址	帳戶	設定檔	電話	組織	成員隸屬

KH

姓氏(L):

名字(F): 英文縮寫(I):

顯示名稱(S):

描述(D):

辦公室(C):

電話號碼(T): 其他(O)...

電子郵件(M):

網頁(W): 其他(R)...

確定 取消 套用(A)

KH 內容

撥入	環境	工作階段	遠端控制	終端機服務設定檔		
一般	地址	帳戶	設定檔	電話	組織	成員隸屬

職稱(T):

部門(D):

公司(C):

主管

名稱(N):

變更(H)... 檢視(V) 清除(L)

屬下(E):

確定 取消 套用(A)

(2) N-Reporter [事件查詢] -> 點選 使用者名稱 

等級	事件	次數	來源使用者名稱	Policy ID	Audit User	來源主機名稱	Ext1	Ext4
Notice	538 User Logoff (AUDIT_SUCCESS 538 NPARTNER\kh)	1	kh 	538	kh	NPARTNER	登入類型:2	登入識別碼: (0x0,0xE8499)

(3) 顯示使用者資料

等級	事件	次數	來源使用者名稱	Policy ID	Audit User	Ext1	Ext4
Notice	538 User Logoff (AUDIT_SUCCESS 538 NPARTNER\kh)	1	kh (KH, TAC, 0032, (Engineer))	538	kh	登入類型:2	登入識別碼: (0x0,0xE8499)

2.3.1 新增非管理帳號

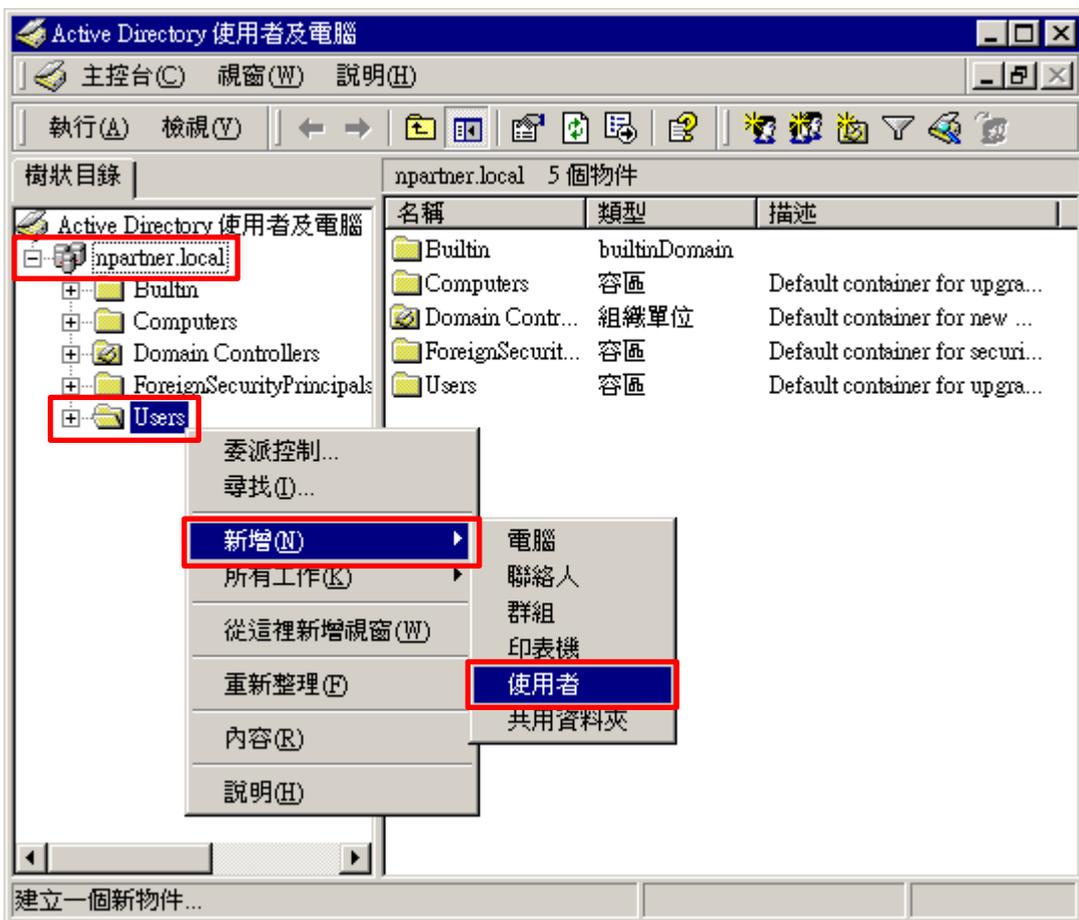
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增帳號

展開 [網域名稱] -> 在 [Users] 組織單位，按滑鼠右鍵 註：請依客戶環境建立使用者 -> 點選 [使用者]



(3) 輸入帳號資訊

輸入使用者名稱 -> 按 [下一步]

新增物件 - 使用者

建立在: npartner.local/Users

姓氏(L):

名字(F): 英文縮寫(I):

全名(A): npartner

使用者登入名稱(U): npartner @npartner.local

使用者登入名稱 (Windows 2000 前版)(W): NPARTNER\ npartner

< 上一步(B) 下一步(N) > 取消

(4) 輸入使用者密碼

輸入兩次相同 [密碼] -> 勾選 [密碼永久有效] -> 按 [下一步]

新增物件 - 使用者

建立在: npartner.local/Users

密碼(P): *****

確認密碼(C): *****

使用者必須在下次登入時變更密碼(M)

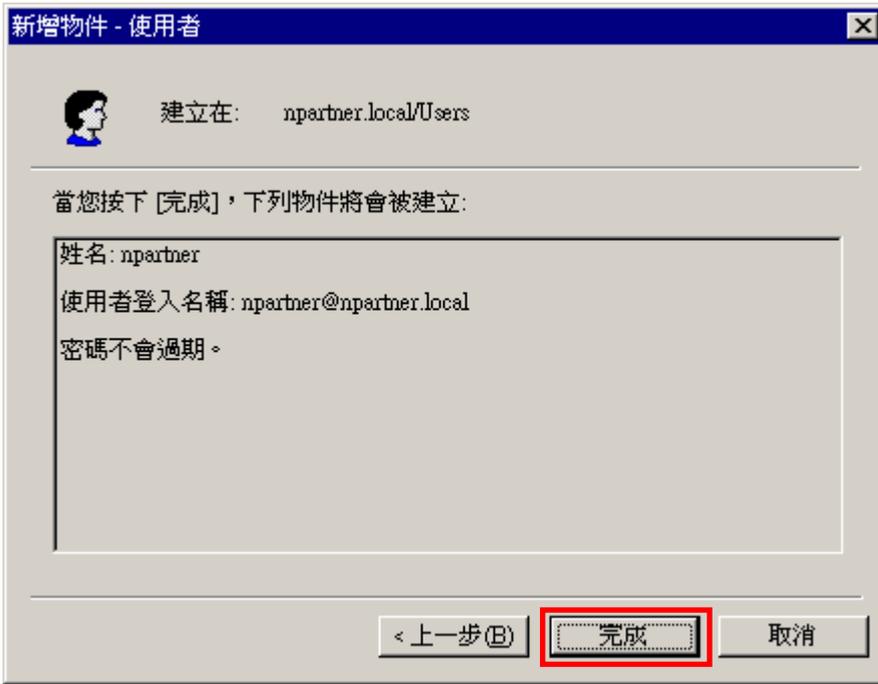
使用者無法變更密碼(S)

密碼永久有效(W)

帳戶已停用(O)

< 上一步(B) 下一步(N) > 取消

(5) 按 [完成]



2.3.2 設定 DCOM 權限

(1) 開啟 [命令提示字元]



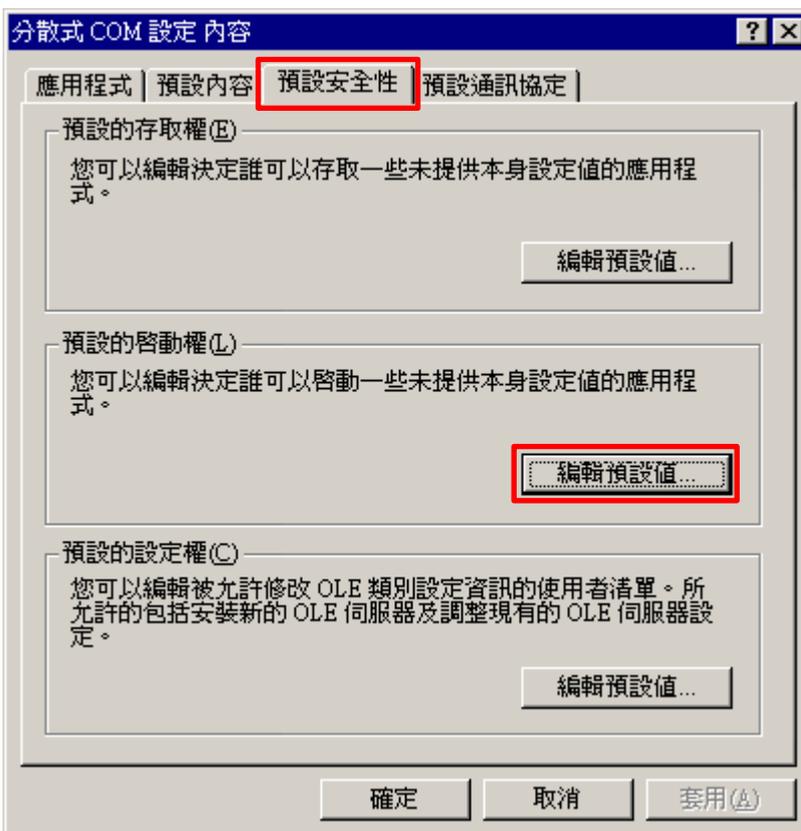
(2) 開啟元件服務

C:\> dcomcnfg.exe



(3) 啟用權限

點選 [預設安全性] 頁面 -> 預設的啟動權，按 [編輯預設值]



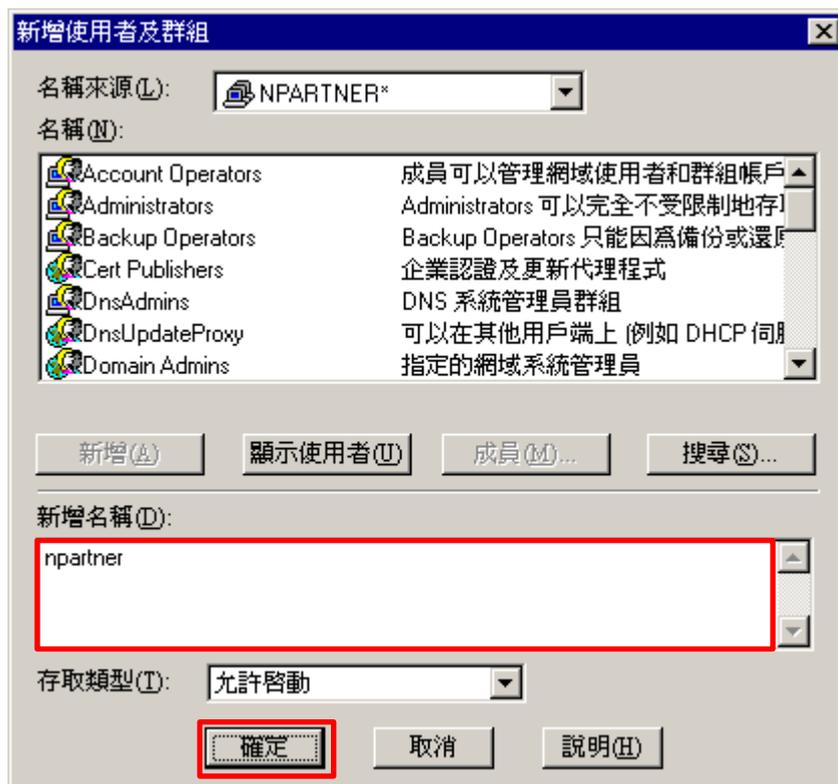
(4) 新增 DCOM 使用者權限

點選 [新增]

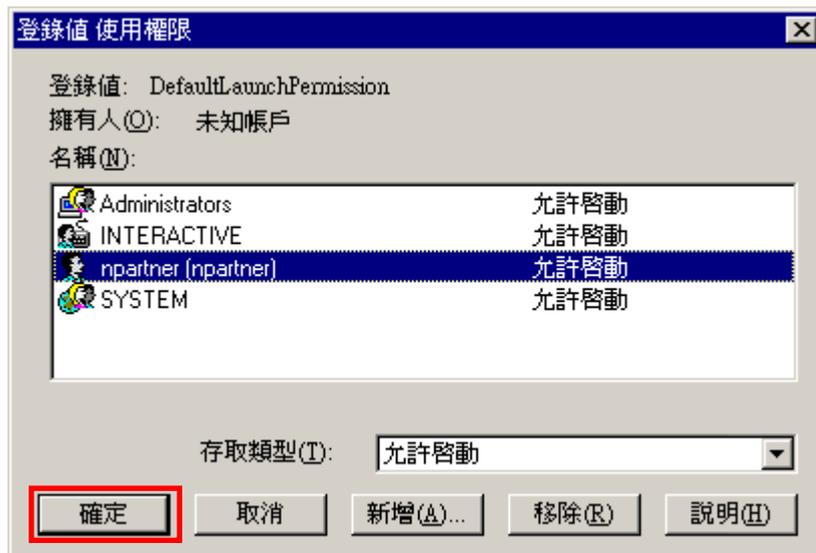


(5) 輸入使用者

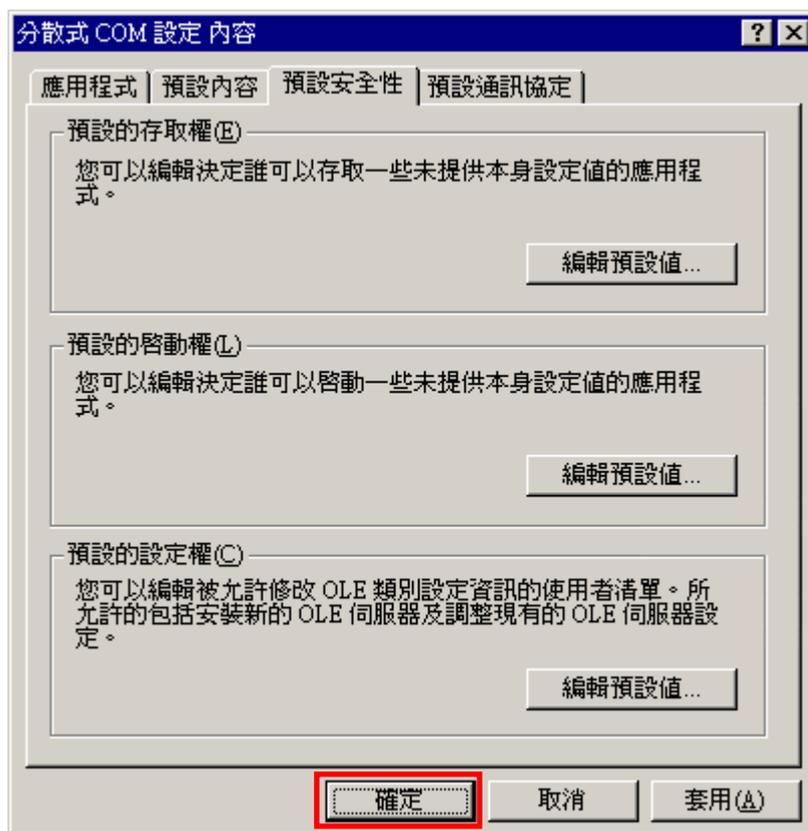
輸入使用者帳號: `npartner` -> 按 [確定]



(6) 按 [確定]



(7)) 按 [確定]



2.3.3 設定 WMI 權限

2.3.3.1 設定事件日誌權限

(1) 開啟 [命令提示字元]



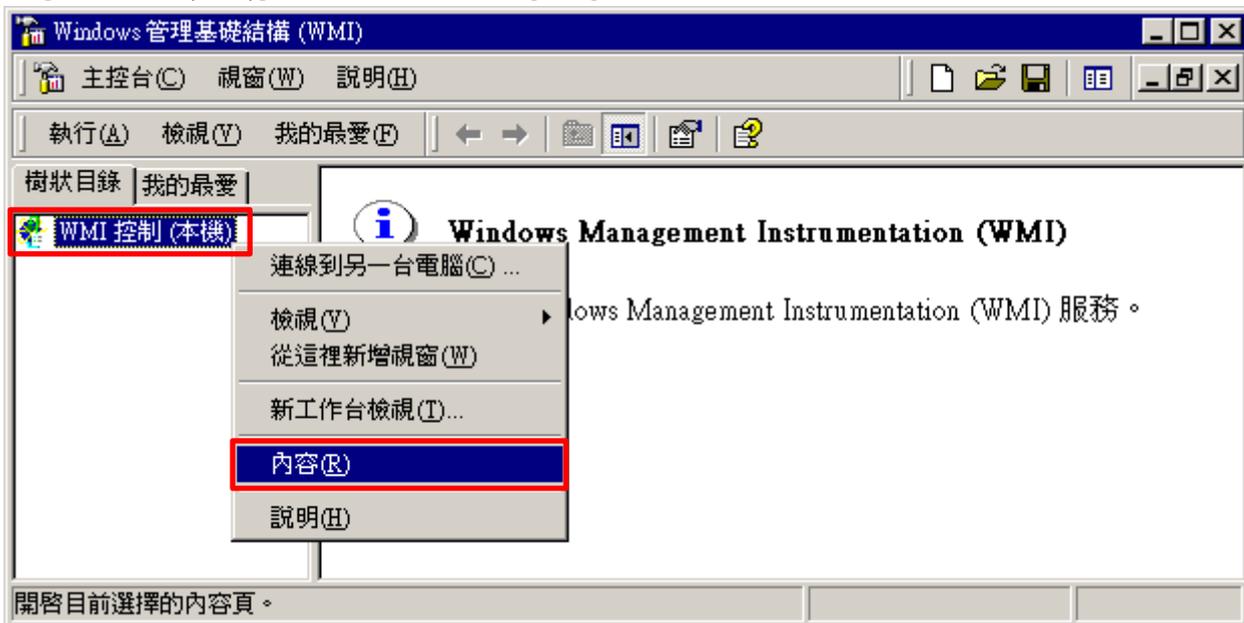
(2) 開啟 WMI 控制

C:\> wmicmgmt.msc



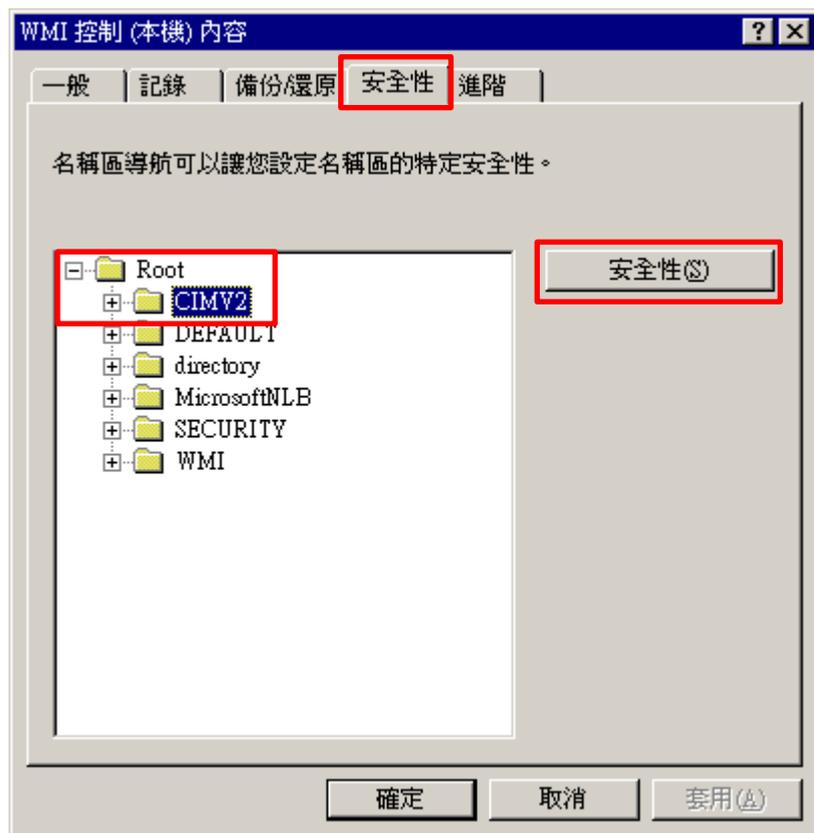
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



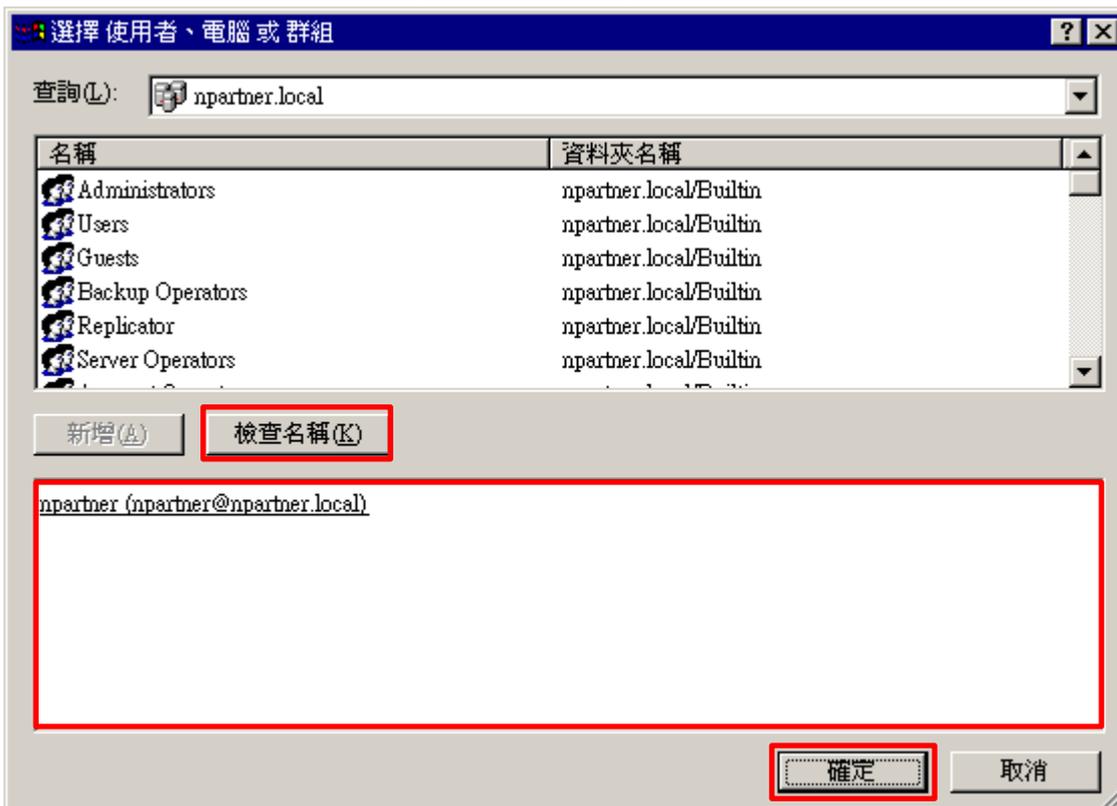
(5) 新增 WMI 使用者權限

按 [新增]



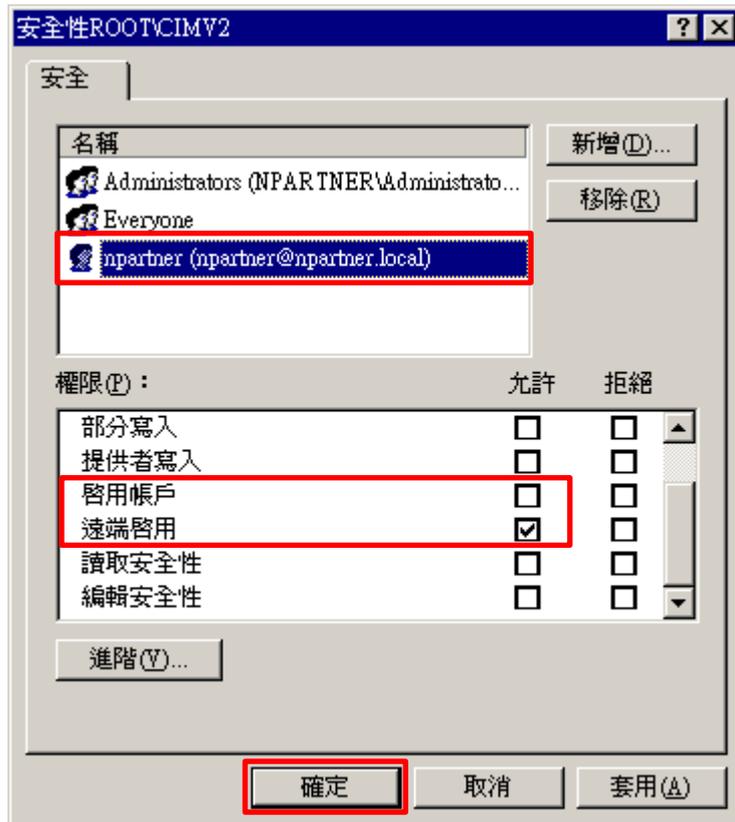
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



2.3.3.2 設定讀取使用者資料權限

(1) 開啟 [命令提示字元]



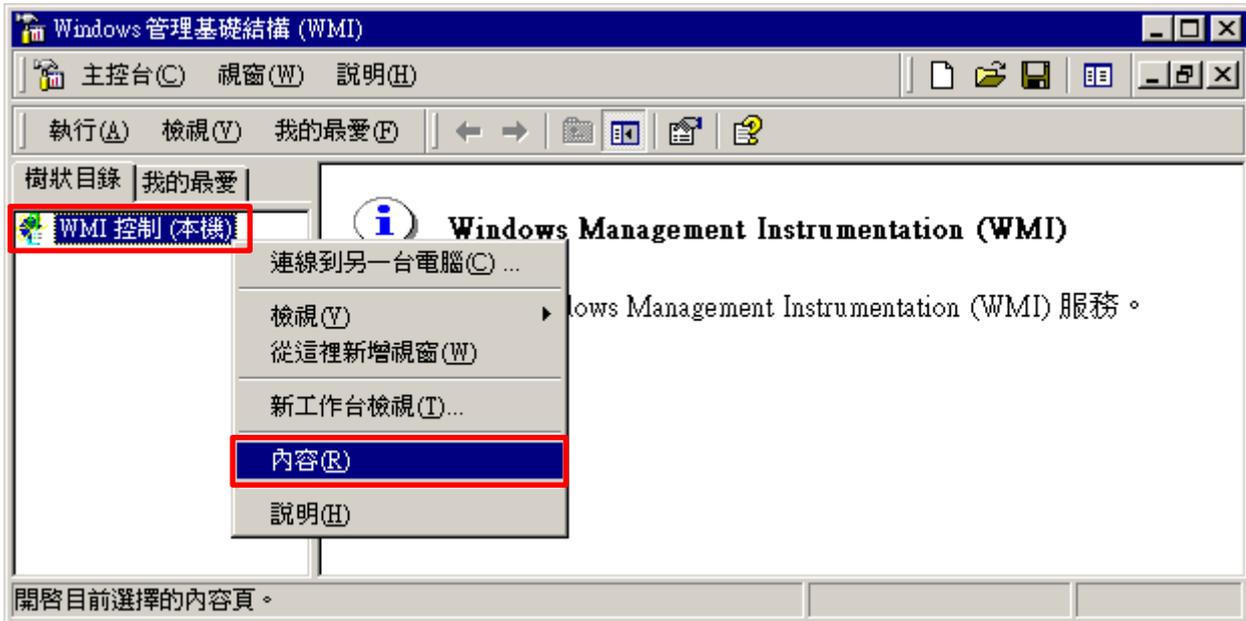
(2) 開啟 WMI 控制

C:\> wmicmgmt.msc



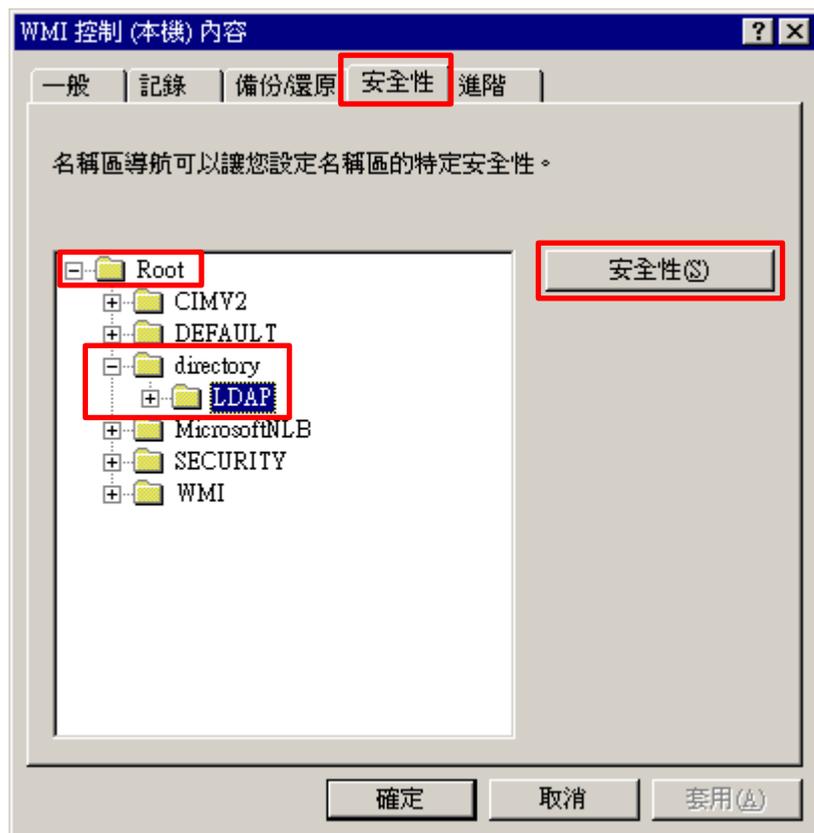
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



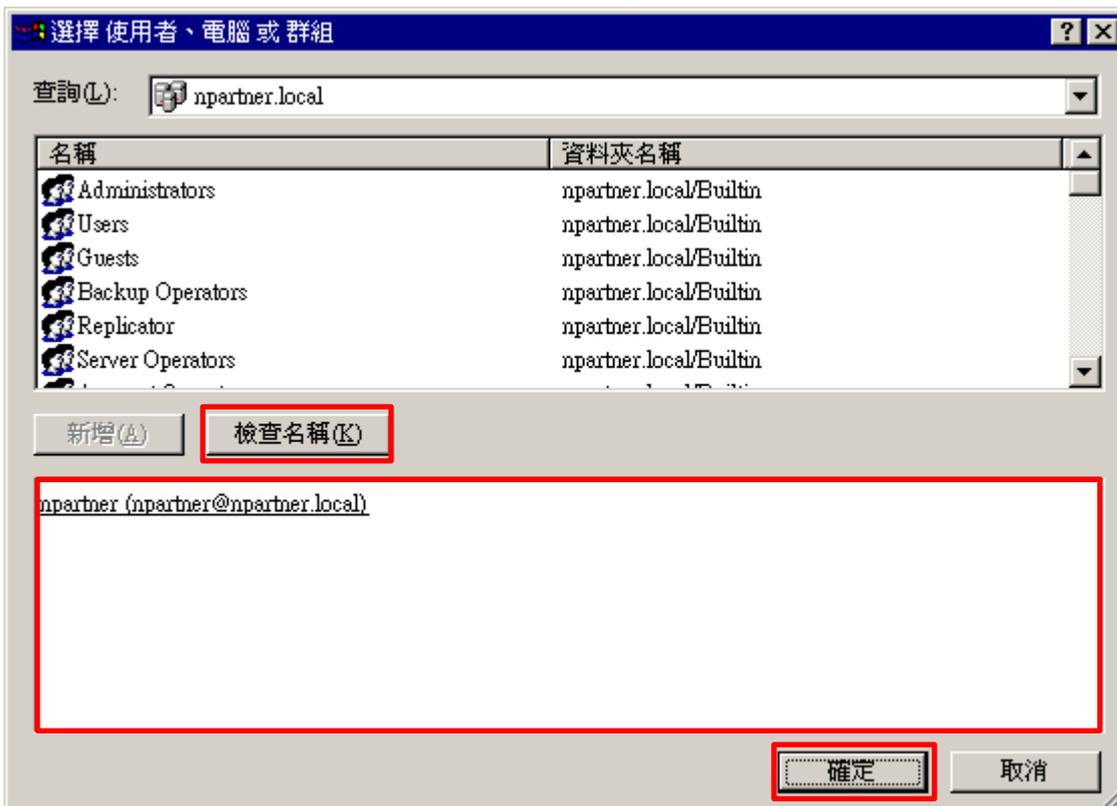
(5) 新增 WMI 使用者權限

按 [新增]



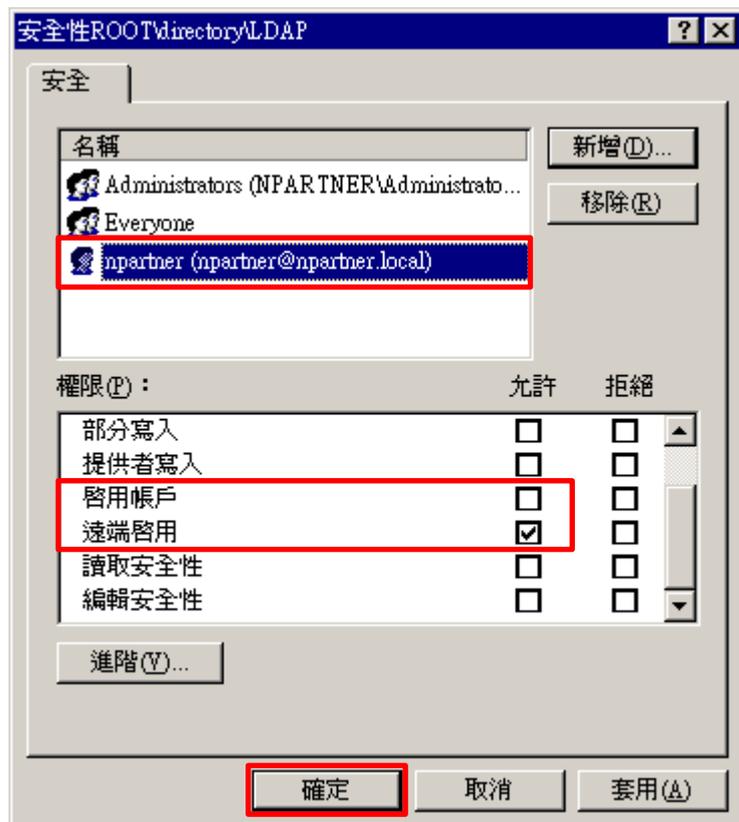
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

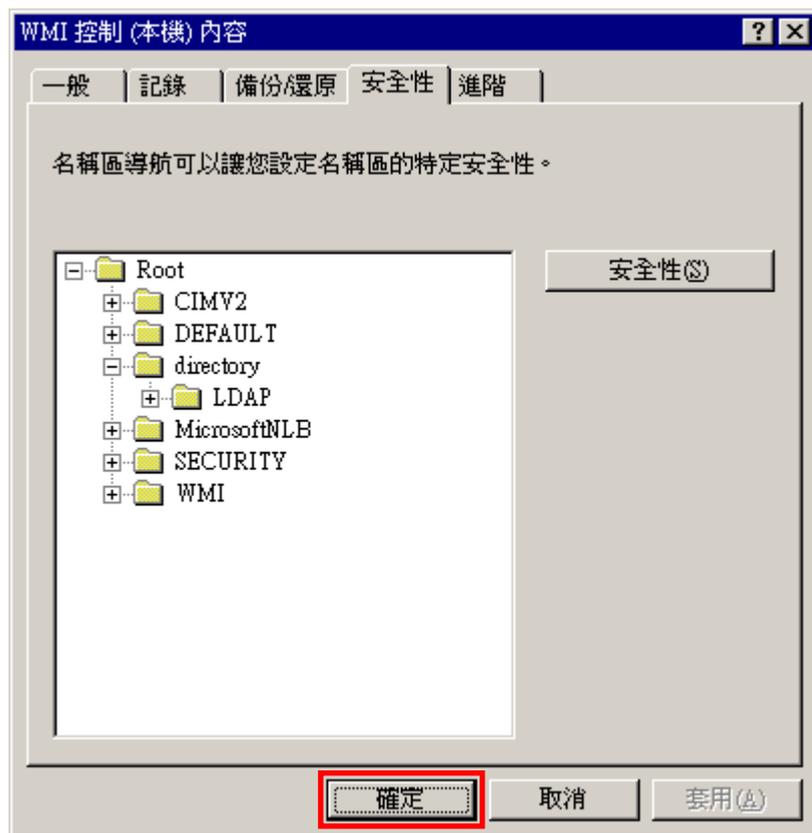


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



2.3.4 設定 Event log 讀取權限

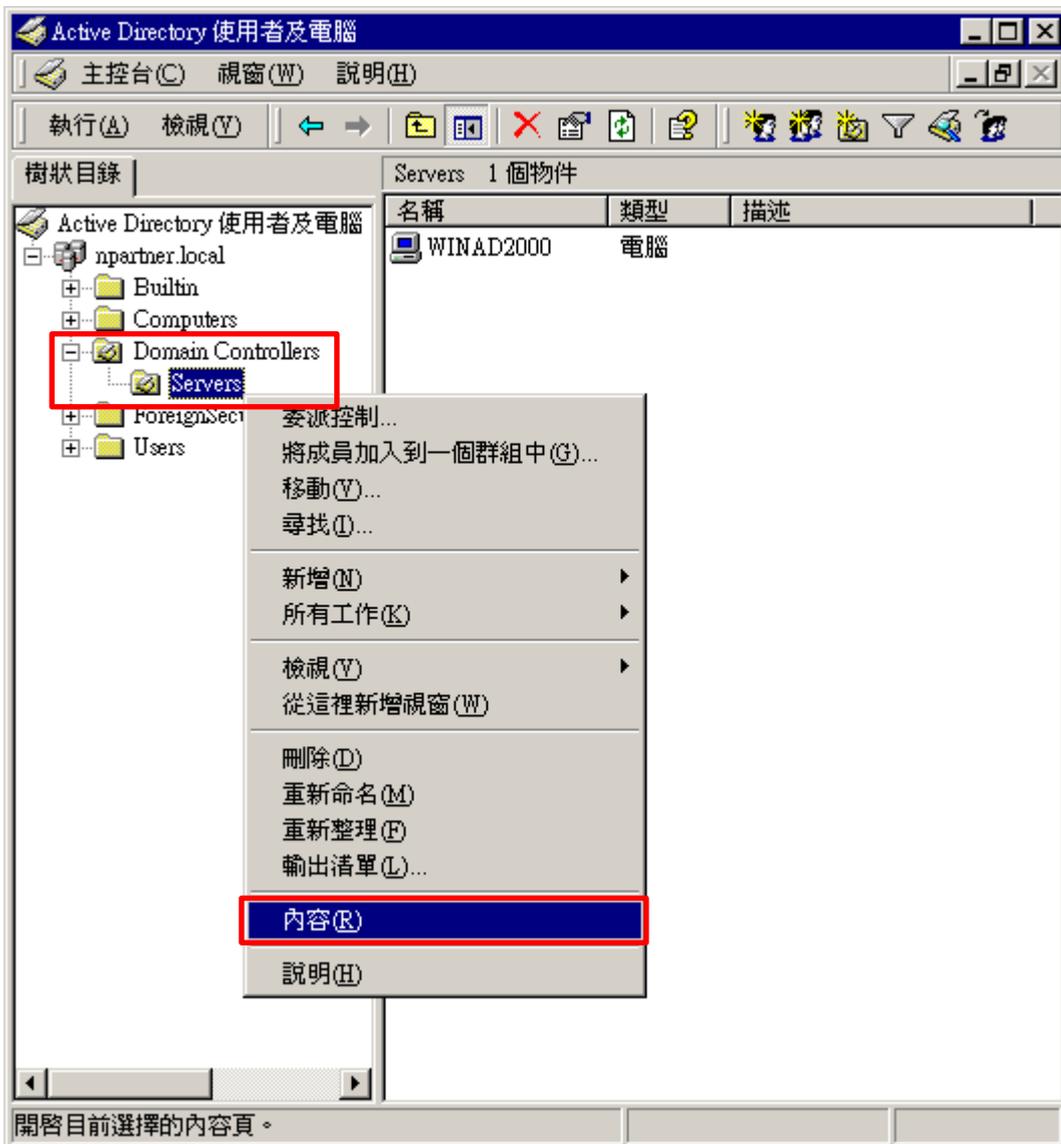
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



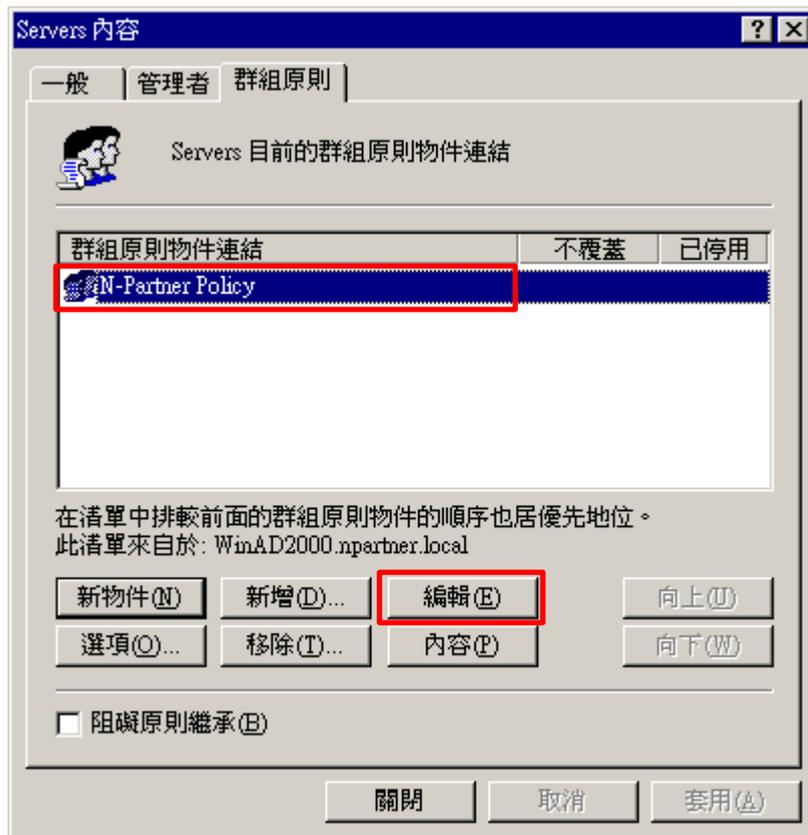
(2) 在 Servers 組織單位，點選內容

展開 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



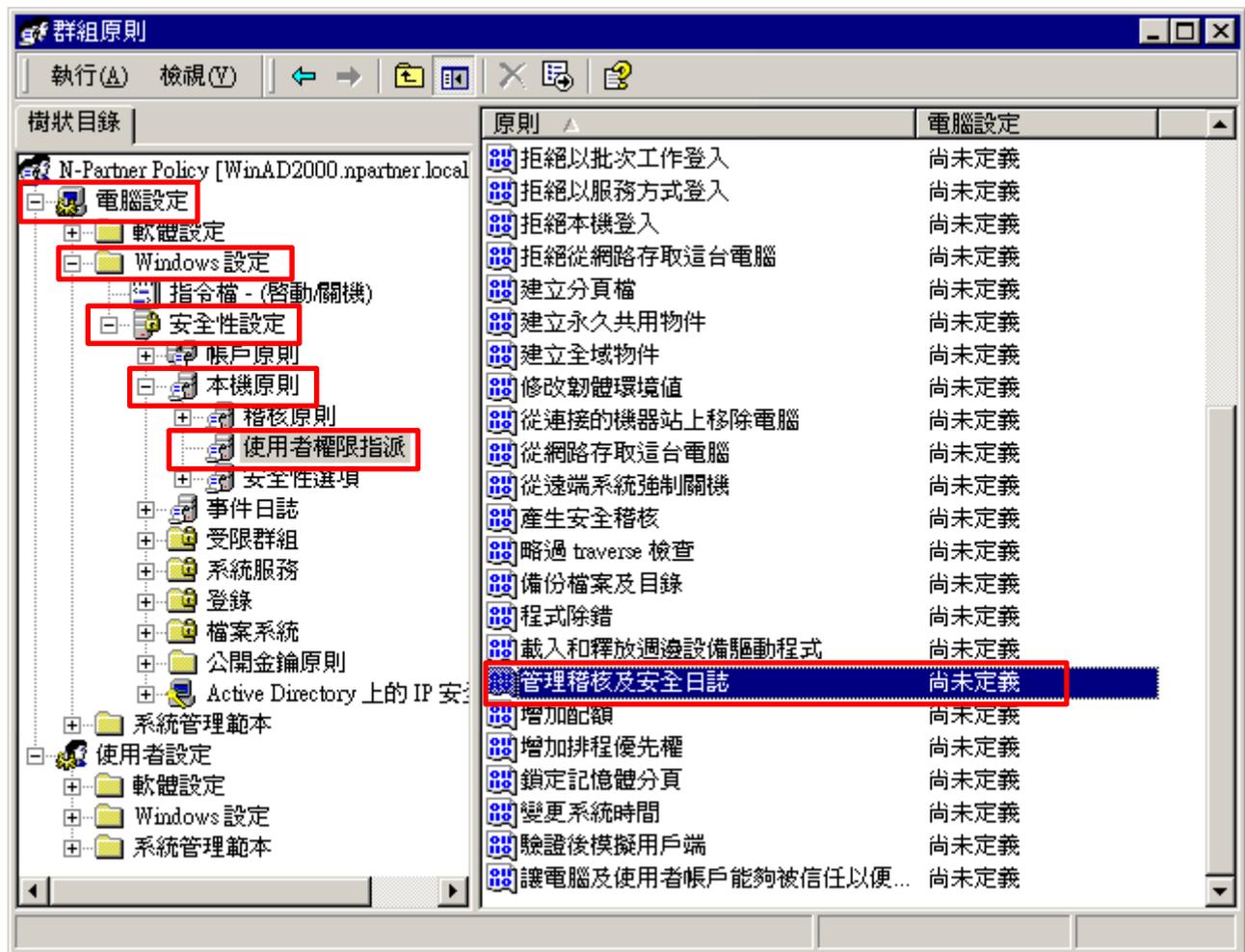
(3) 編輯群組原則物件

點選群組原則物件名稱 [N-Partner Policy] -> 按 [編輯]



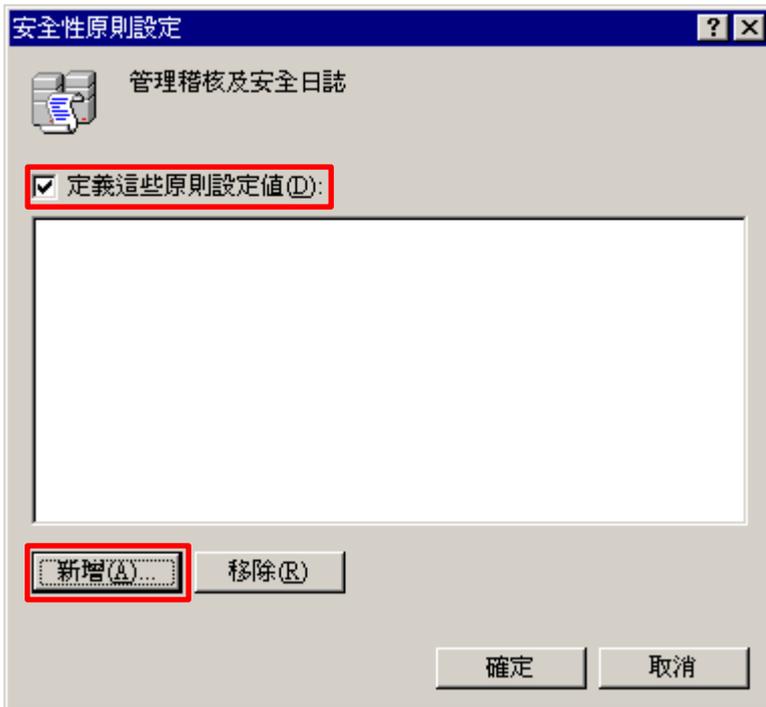
(4) 設定記錄檔

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全日誌] 項目



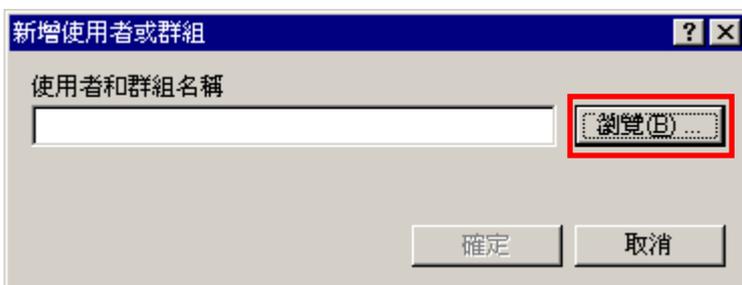
(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增]



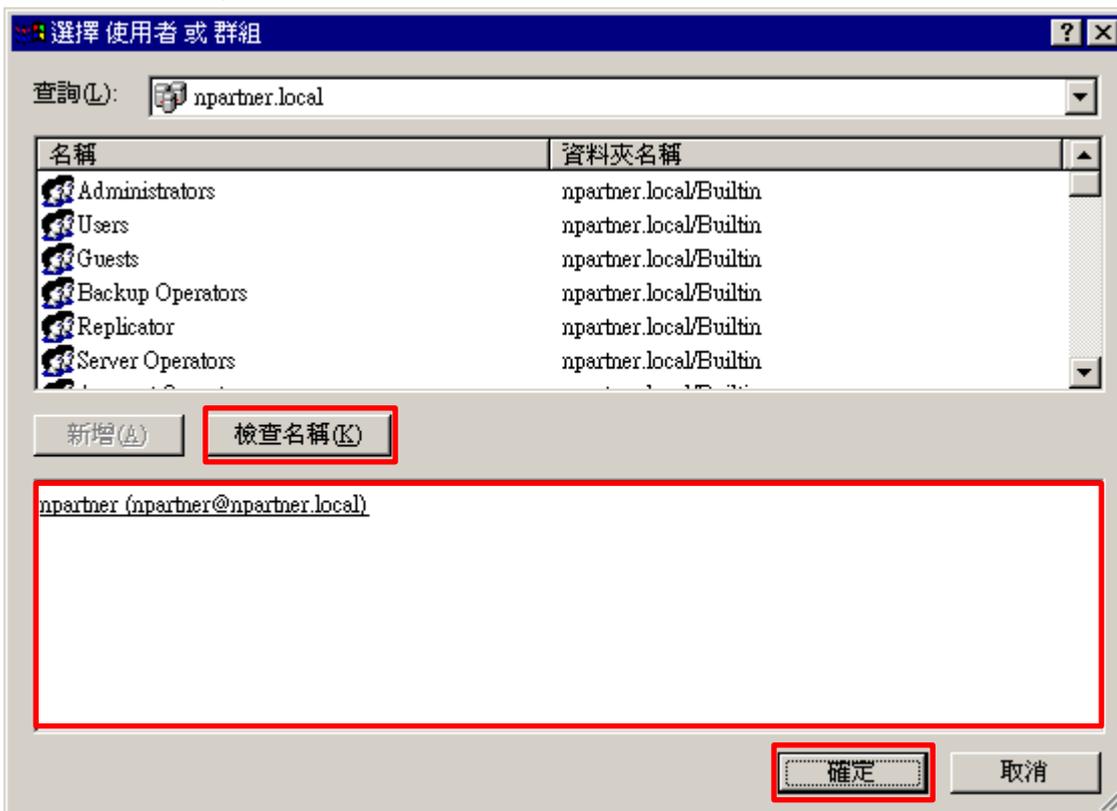
(6) 搜尋使用者

按 [瀏覽]



(7) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



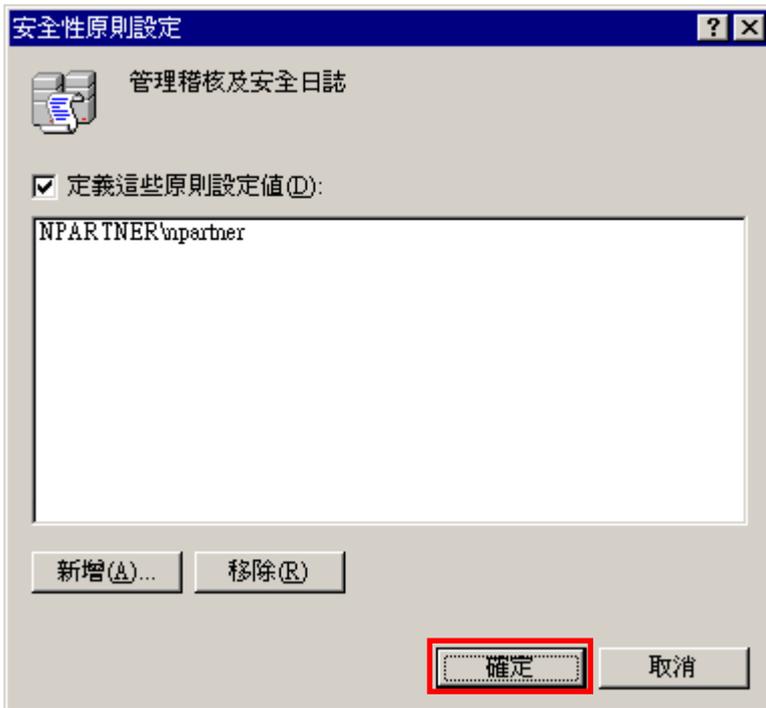
(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

按 [確定]



(10) 開啟 [命令提示字元]



(11) 更新群組原則。

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



2.3.5 重啟 WMI 服務

(1) 開啟 [命令提示字元]



(2) 停用 WMI 服務

C:\> net stop winmgmt



(3) 啟用 WMI 服務

C:\> net start winmgmt



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](#)

3.1 組織單位設定

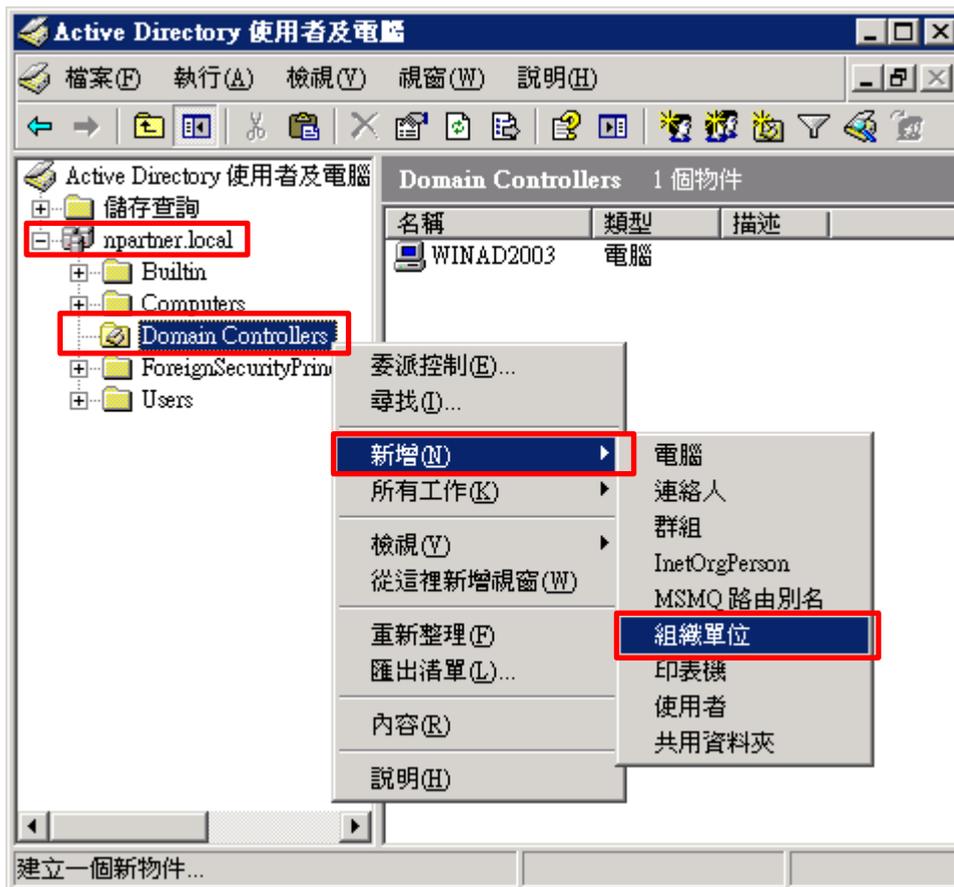
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者及電腦]



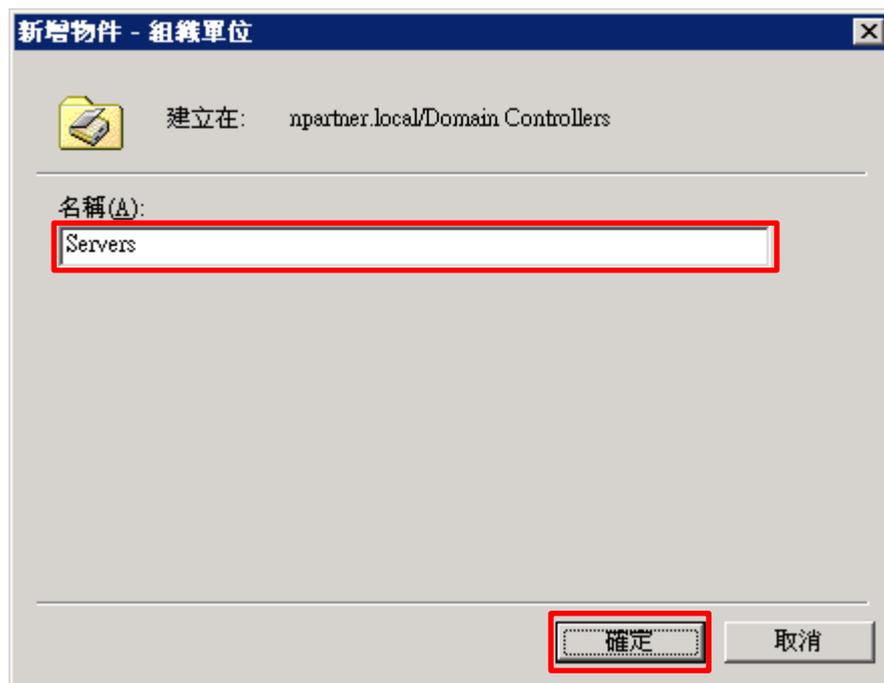
(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]



(3) 輸入組織單位名稱

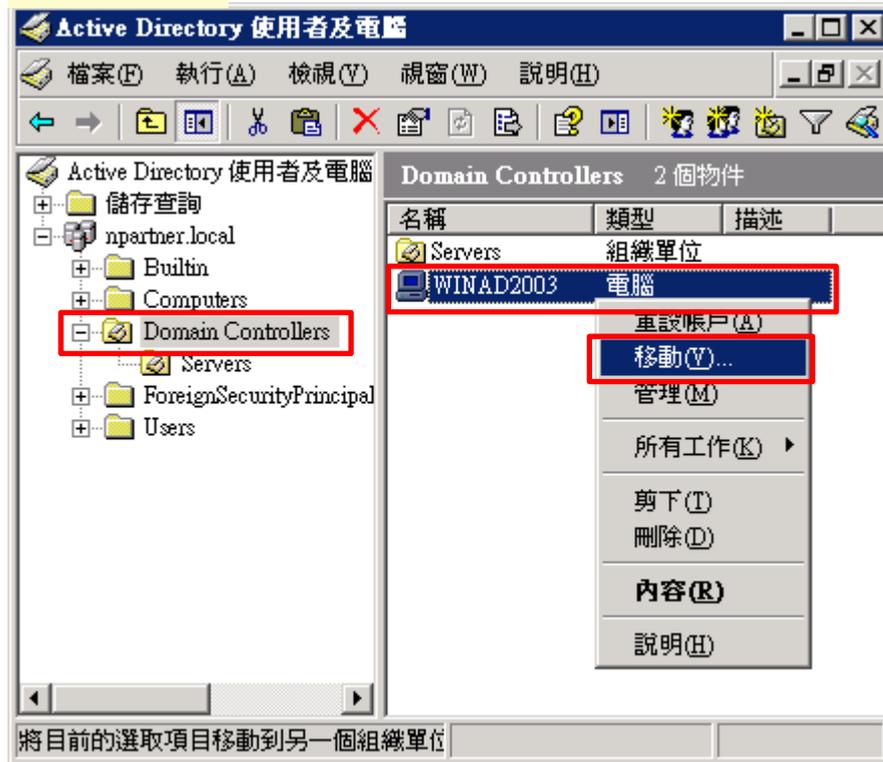
輸入組織單位名稱: Servers 註：請依客戶環境建立組織單位名稱 -> 按 [確定]



(4) 移動網域伺服器至新的組織單位

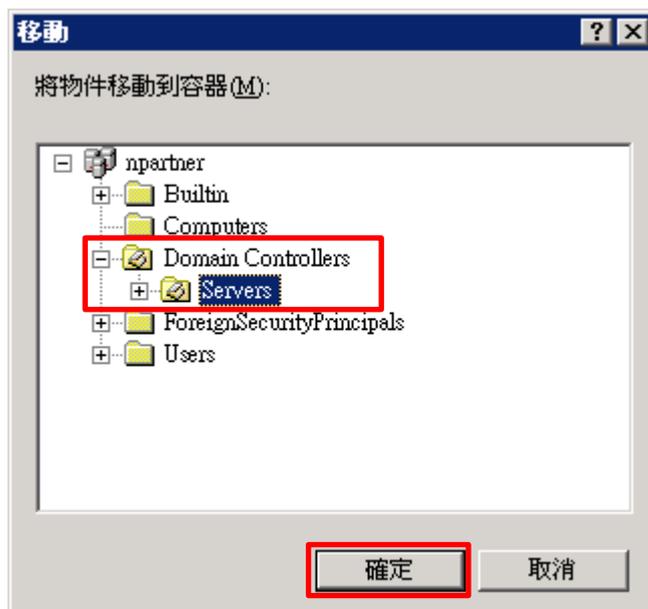
選擇 [Domain Controllers] 組織單位 -> 在 [WinAD2003] 網域伺服器，按滑鼠右鍵，註：請依客戶環境選擇

Windows AD 主機 -> 點選 [移動]



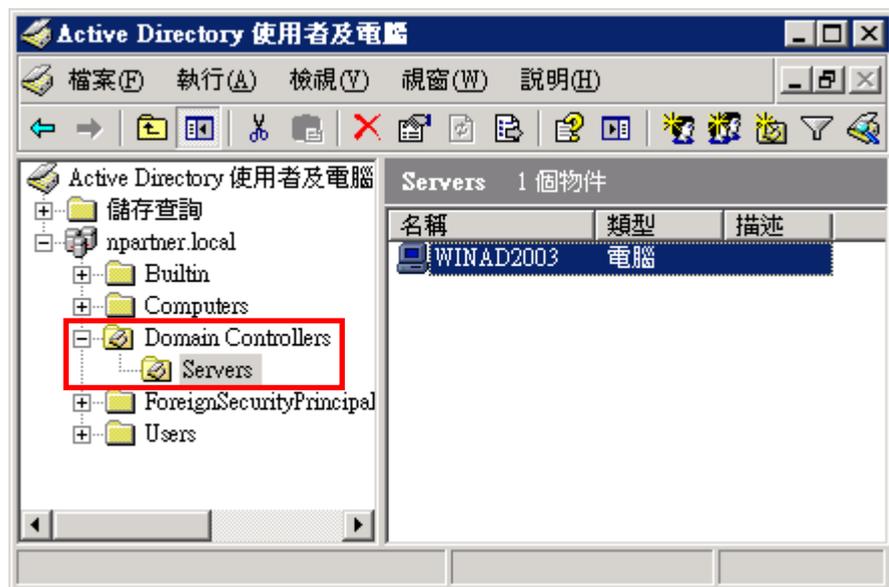
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移至新的組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2003] 網域伺服器已移動。



3.2 群組原則設定

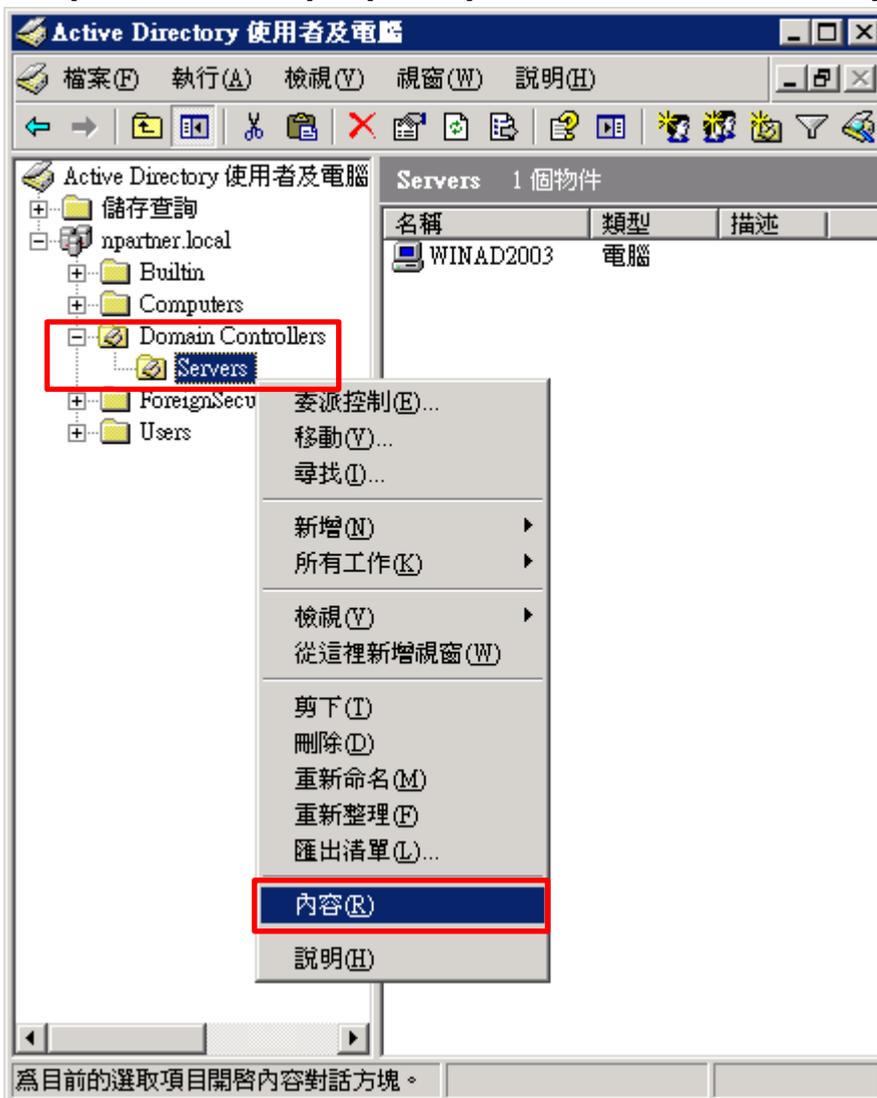
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者及電腦]



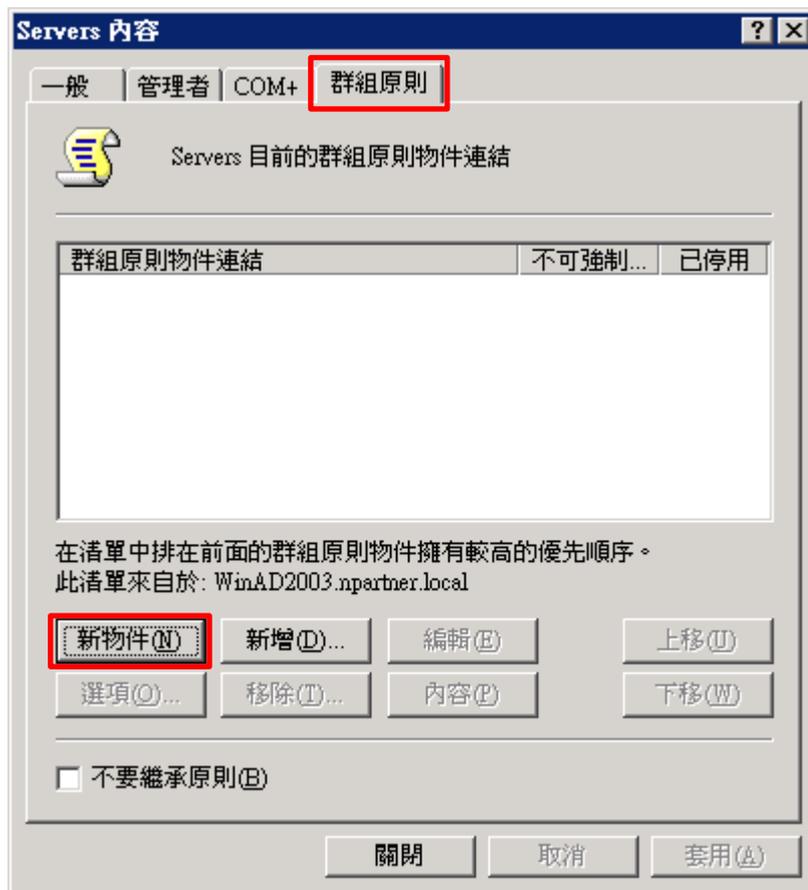
(2) Domain Controllers 的 Servers 組織單位

展開 [Domain Controllers] 的 [Servers] 組織單位 · 按滑鼠右鍵 -> 點選 [內容]



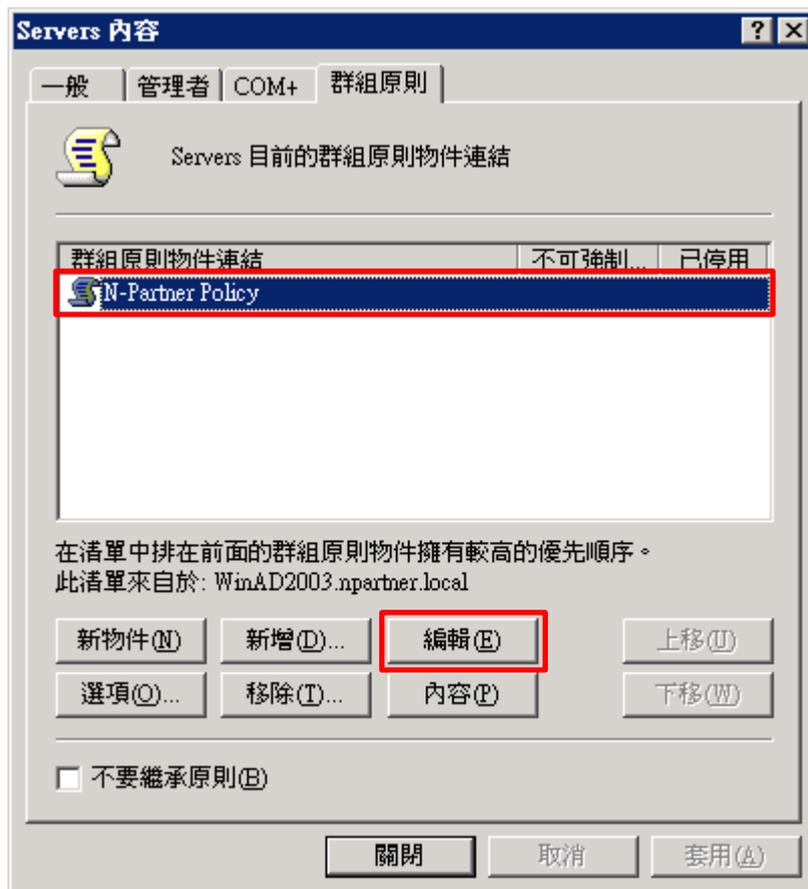
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



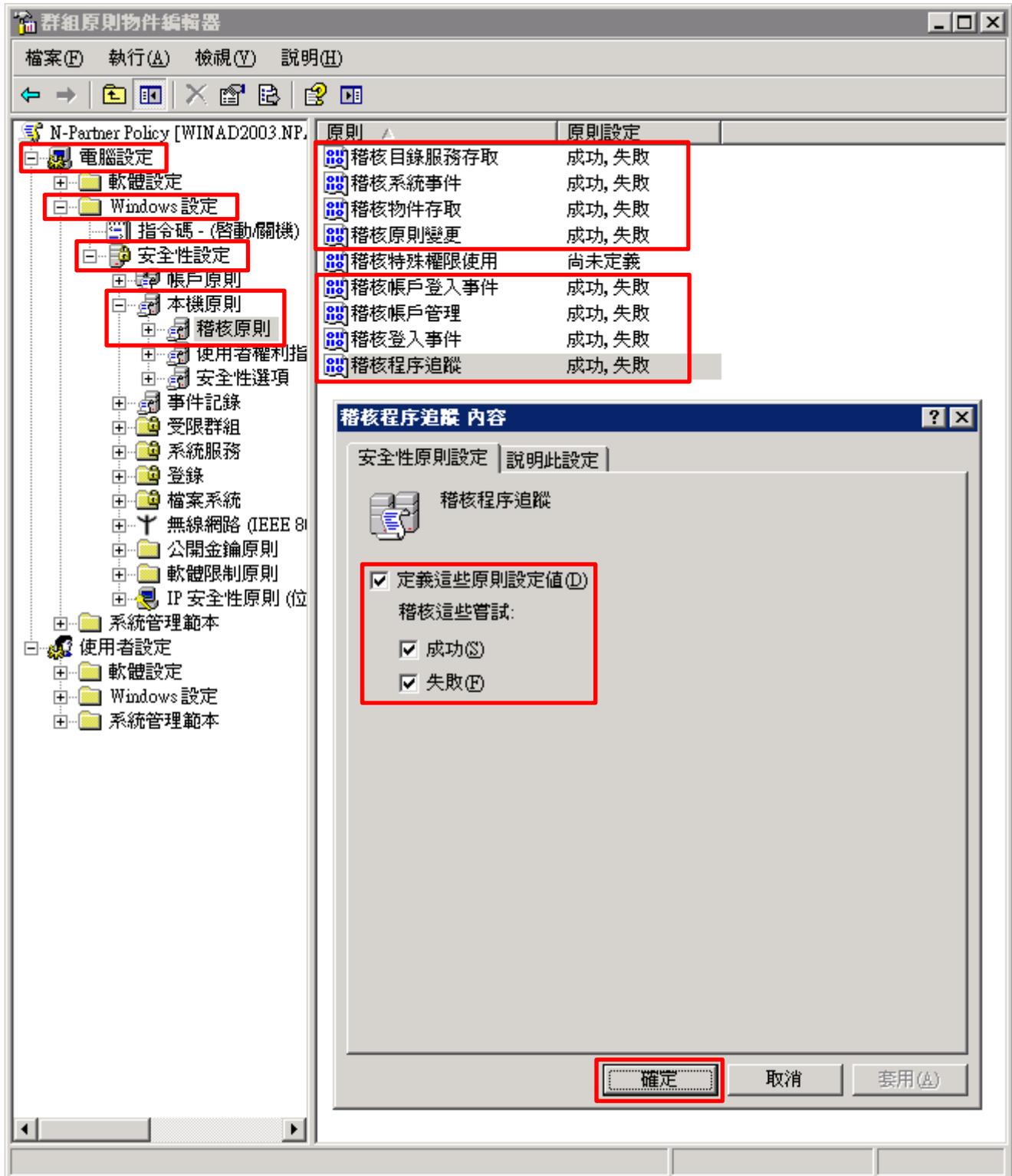
(4) 編輯群組原則物件

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]



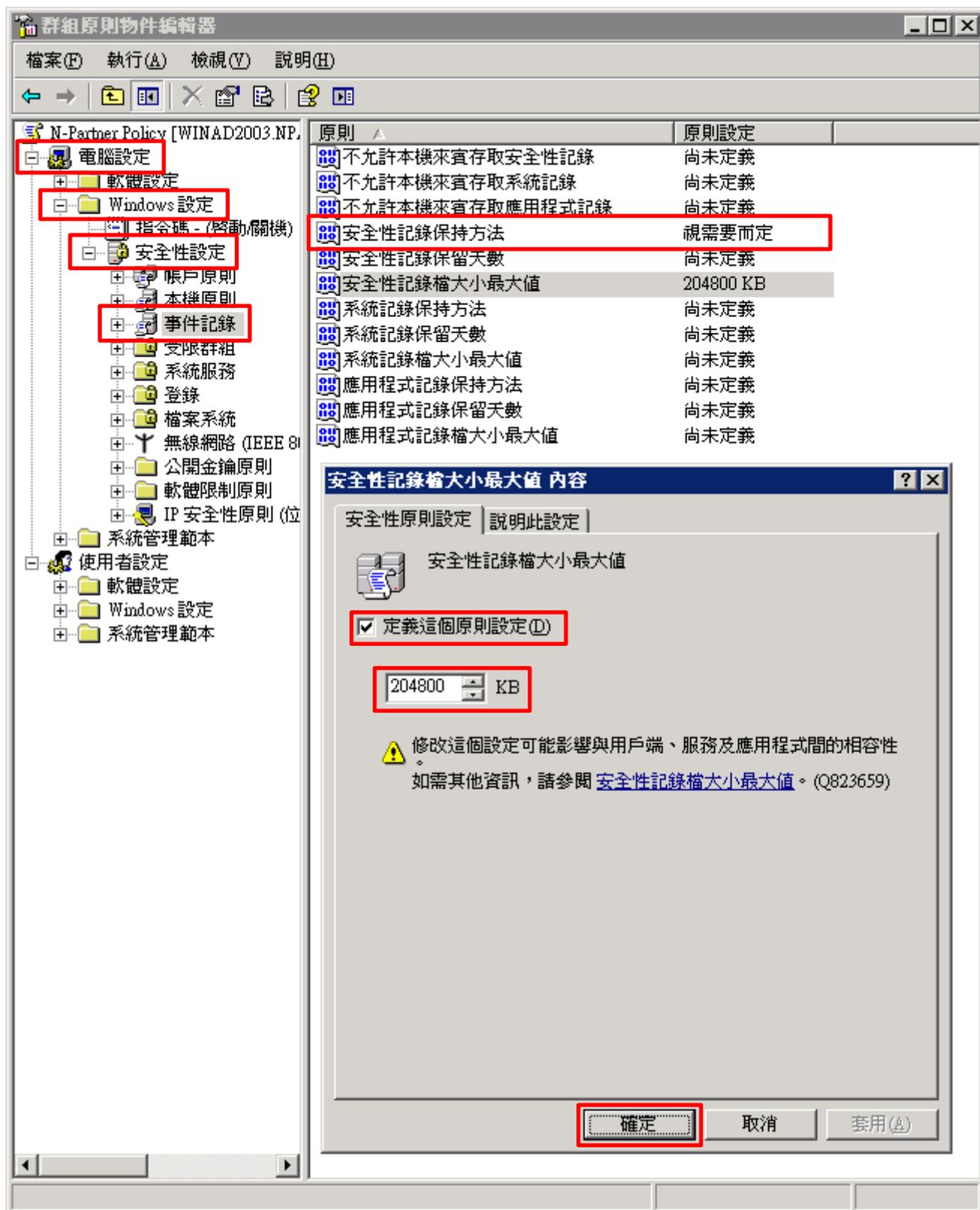
(5) 本機原則：稽核原則

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核目錄服務存取], [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 [定義這些原則設定值] & [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]

The screenshot shows the 'N-Partner Policy [WINAD2003.NP.]' window. The left sidebar shows a tree view with '電腦設定' (Computer Settings) expanded to 'Windows 設定' (Windows Settings) > '安全性設定' (Security Settings) > '事件記錄' (Event Log). The main pane shows a list of policies. The policy '安全性記錄檔大小最大值' (Security Log Size Maximum) is selected and highlighted in red. Its current value is '204800 KB'. A dialog box titled '安全性記錄檔大小最大值 內容' (Security Log Size Maximum Content) is open, showing the '安全性原則設定' (Security Policy Settings) tab. 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'. A warning icon and text are visible below the input field. At the bottom of the dialog, the '確定' (OK) button is highlighted in red.

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

安全性記錄檔大小最大值 內容

安全性原則設定 | 說明此設定

安全性記錄檔大小最大值

定義這個原則設定 (D)

204800 KB

⚠ 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)

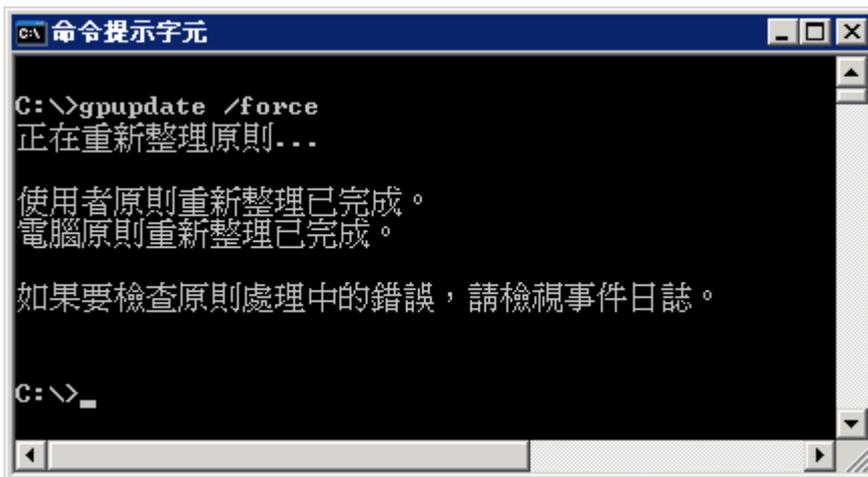
確定 取消 套用 (A)

(8) 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
```

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

建立於 2021/6/29 下午 04:04:36

NPARTNER\administrator 的 RSOP 資料在 WINAD2003: 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=WINAD2003,OU=Servers,OU=Domain Controllers,DC=npartner,DC=local
上次套用的群組原則:    2021/6/29 於 下午 04:01:08
套用的群組原則來自:    WinAD2003.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 Controllers Policy
Default Domain Policy
```

3.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

KH 內容

已發行憑證	成員隸屬	撥入	物件	安全性	環境
工作階段	遠端控制	終端機服務設定檔	COM+		
一般	地址	帳戶	設定檔	電話	組織

KH

姓氏(L):

名字(F): 英文縮寫(I):

顯示名稱(S): KH

描述(D): Engineer

辦公室(O): Taichung Office

電話號碼(T): 其他(O)...

電子郵件(M):

網頁(W): 其他(R)...

確定 取消 套用(A)

KH 內容

已發行憑證	成員隸屬	撥入	物件	安全性	環境
工作階段	遠端控制	終端機服務設定檔	COM+		
一般	地址	帳戶	設定檔	電話	組織

職稱(T):

部門(D): TAC

公司(C):

主管

名稱(N):

變更(B)... 內容(E) 清除(L)

屬下(E):

確定 取消 套用(A)

(2) N-Reporter [事件查詢] -> 點選 使用者名稱 

等級	事件	來源 IP	來源 Port	次數	事件型態	來源使用者名稱	Policy ID	Audit User	Ext1	Ext4
Notice	528 Successful Logon (AUDIT_SUCCESS 528 NPARTNER\kh) (Logon Success)	192.168.5.37	56914	1	audit	kh 	528	kh	登入類型:10	登入識別碼: (0x0,0xB930B)

(3) 顯示使用者資料

等級	事件	來源 IP	來源 Port	次數	事件型態	來源使用者名稱	Policy ID	Audit User	Ext1	Ext4
Notice	528 Successful Logon (AUDIT_SUCCESS 528 NPARTNER\kh) (Logon Success)	192.168.5.37	56914	1	audit	kh (KH. TAC. 0032. (Engineer))	528	kh	登入類型:10	登入識別碼: (0x0,0xB930B)

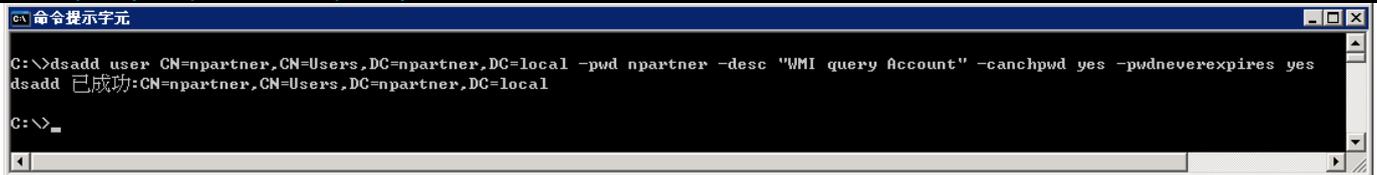
3.3.1 新增非管理帳號

(1) 開啟 [命令提示字元]



(2) 新增帳號

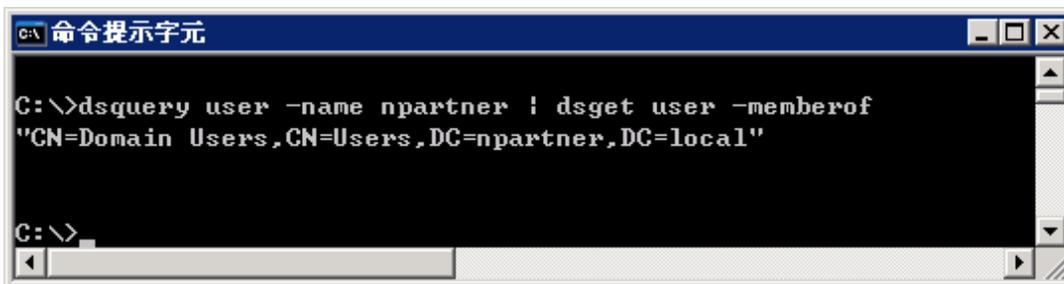
```
C:\> dsadd user CN=npartner,CN=Users,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```



紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
C:\> dsquery user -name npartner | dsget user -memberof
```



3.3.2 設定 DCOM 權限

(1) 開啟 [命令提示字元]



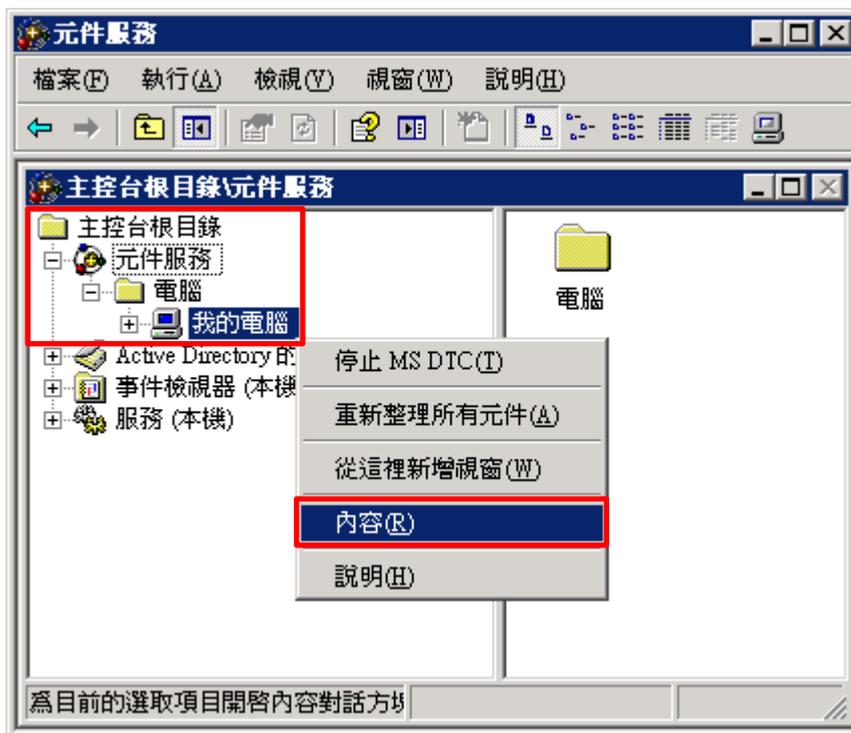
(2) 開啟元件服務

C:\> dcomcnfg.exe



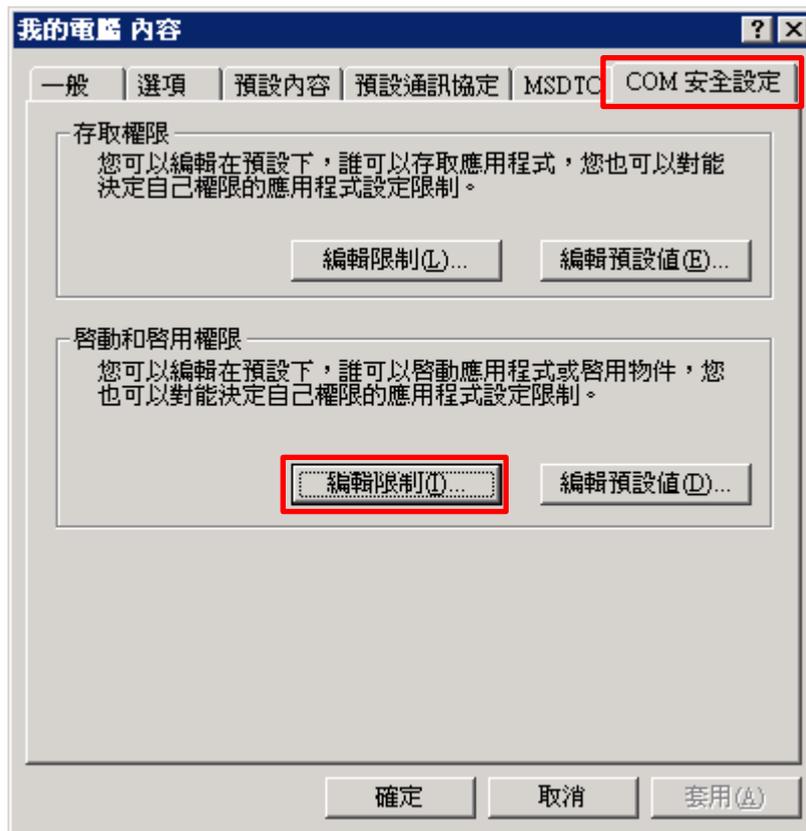
(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



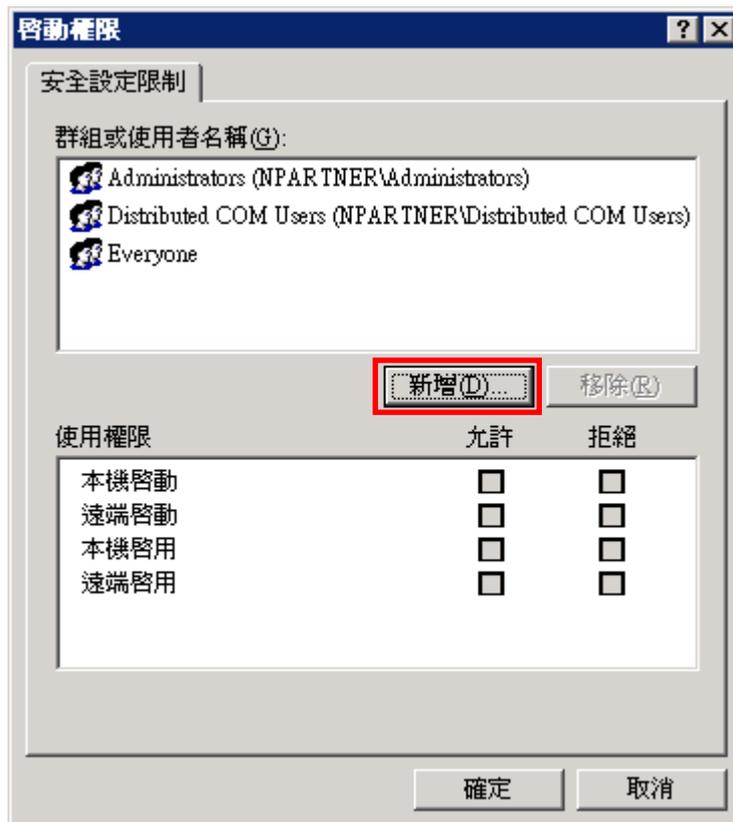
(4) 啟用權限

點選 [COM 安全性設定] 頁面 -> 啟動和啟用權限，按 [編輯限制]



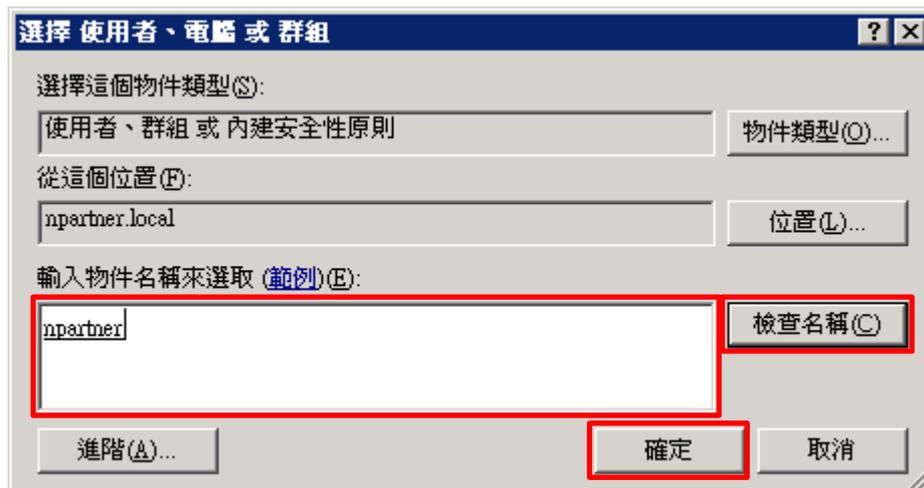
(5) 新增 DCOM 使用者權限

點選 [新增]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

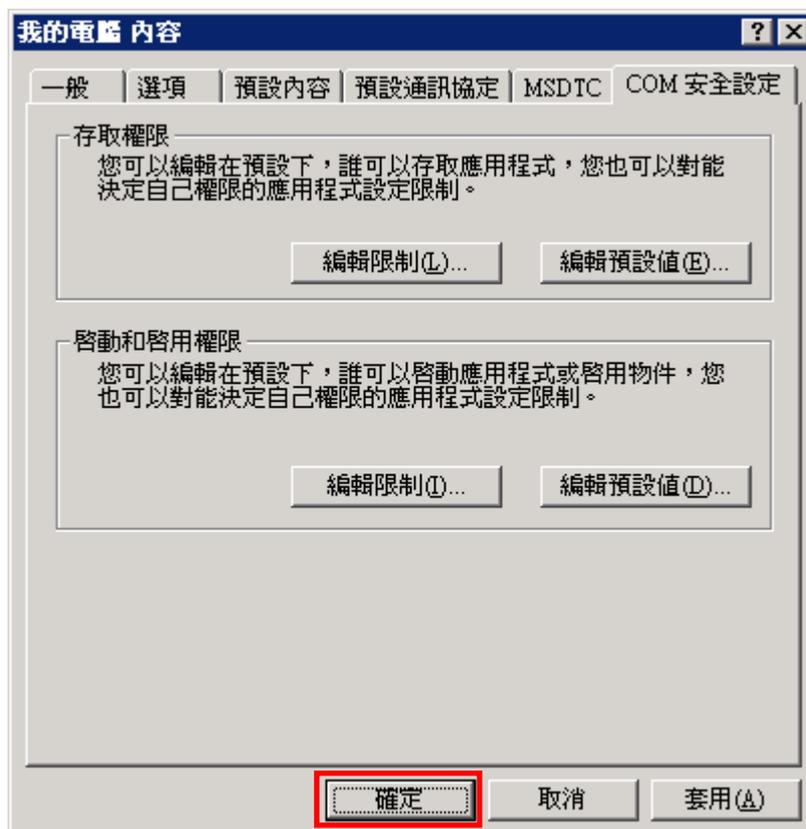


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



3.3.3 設定 WMI 權限

3.3.3.1 設定事件日誌權限

(1) 開啟 [命令提示字元]



(2) 開啟 WMI 控制

C:\> wmicmgmt.msc



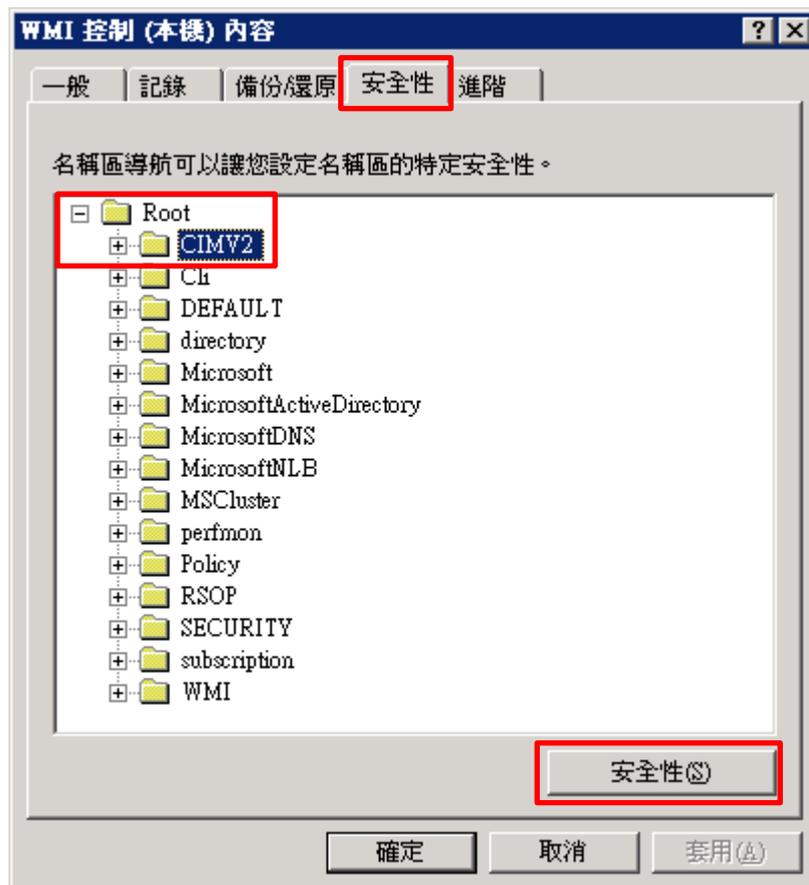
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



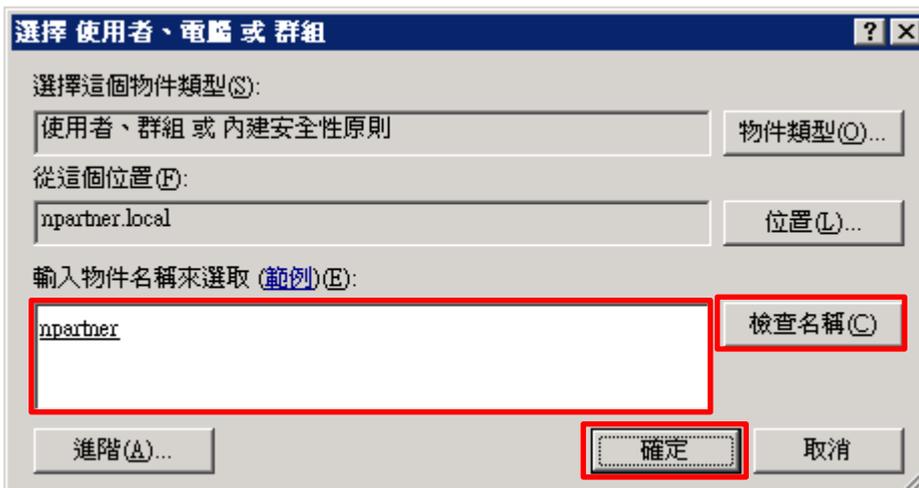
(5) 新增 WMI 使用者權限

按 [新增]



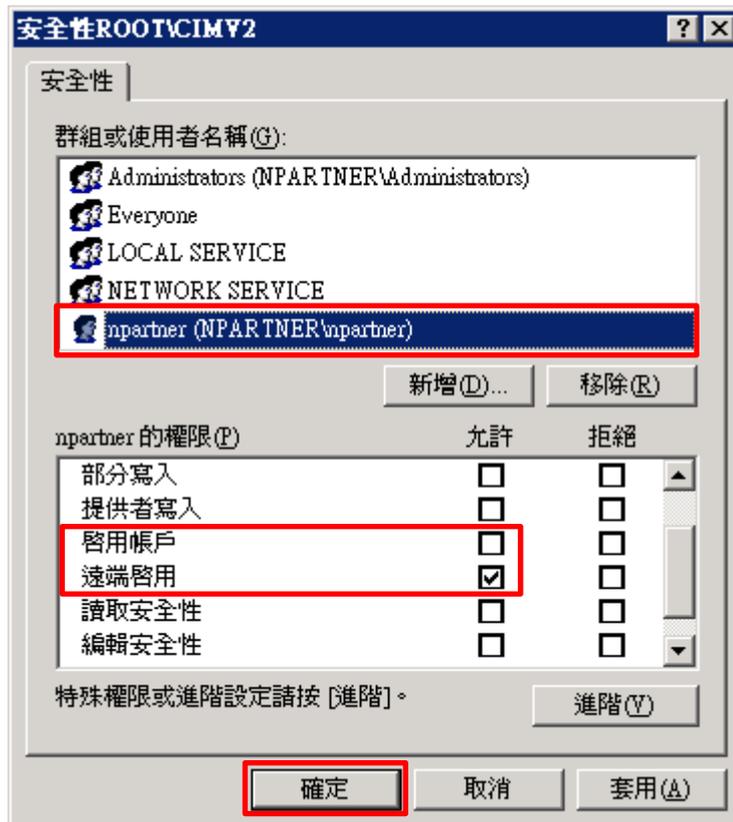
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

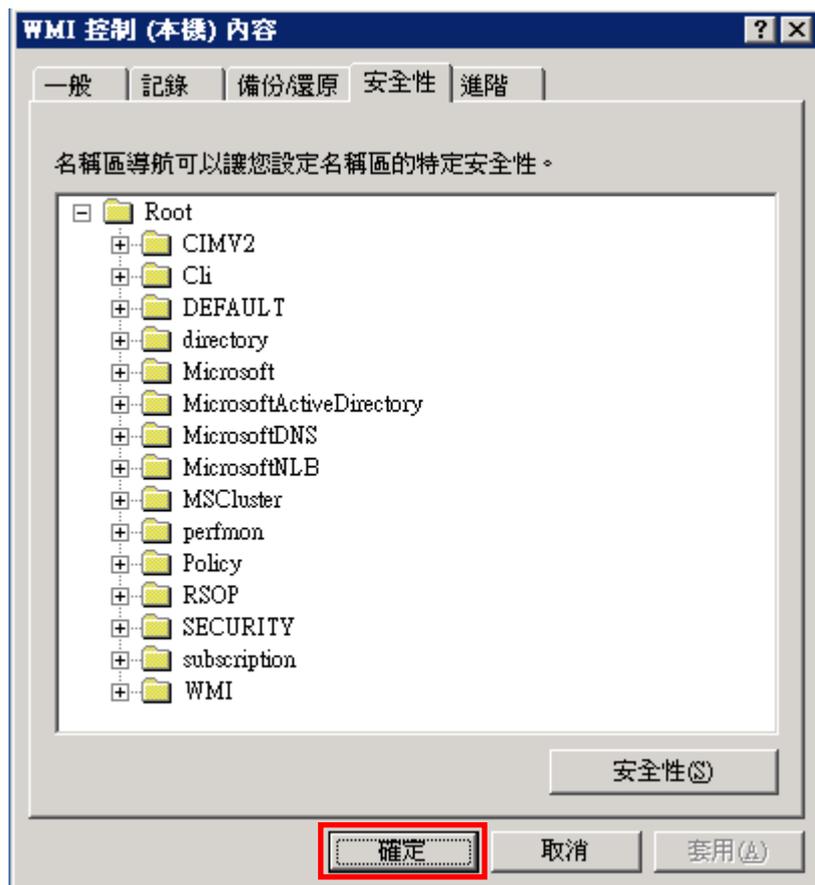


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



3.3.3.2 設定讀取使用者資料權限

(1) 開啟 [命令提示字元]



(2) 開啟 WMI 控制

```
C:\> wimgmt.msc
```



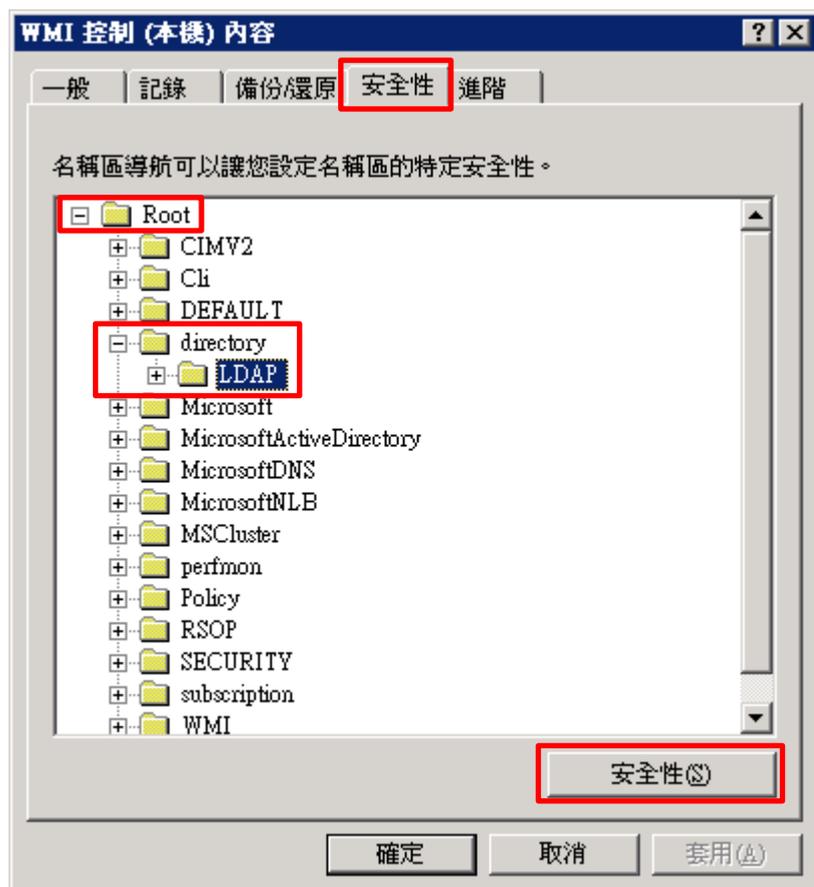
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



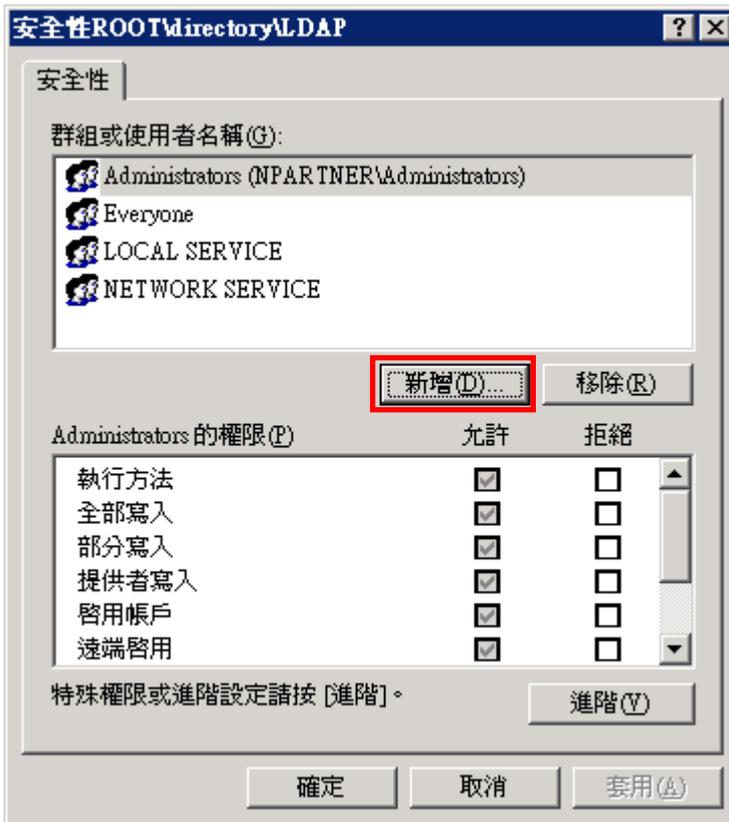
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



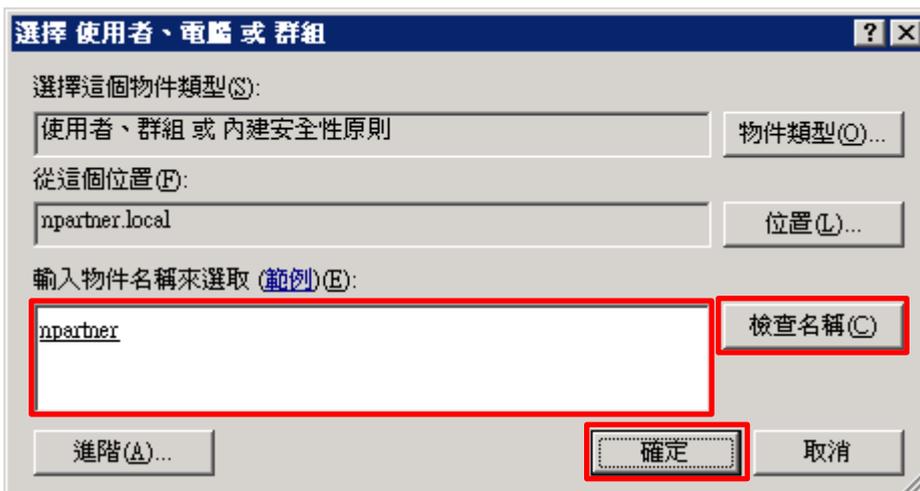
(5) 新增 WMI 使用者權限

按 [新增]



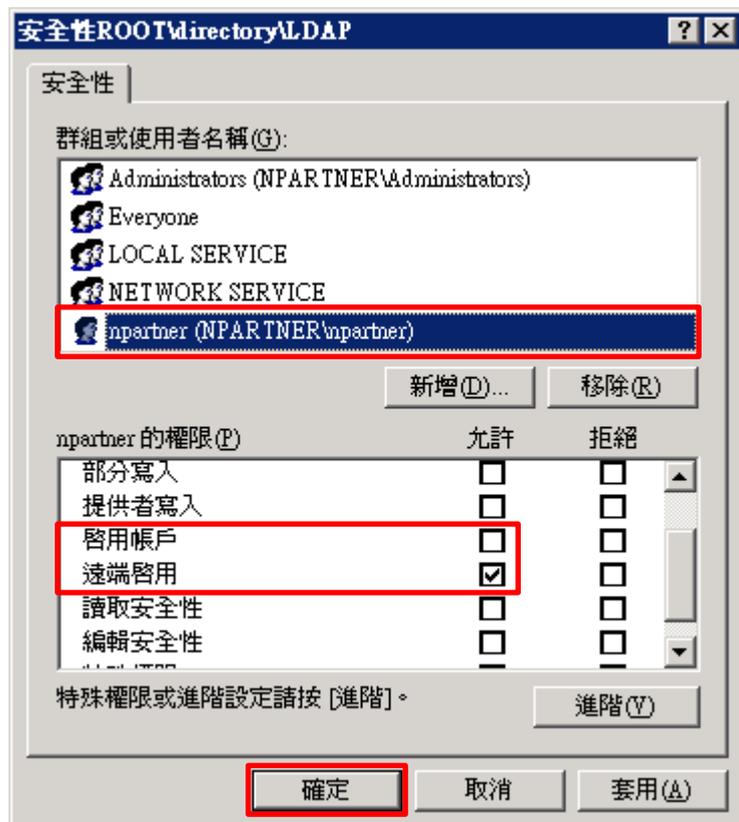
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

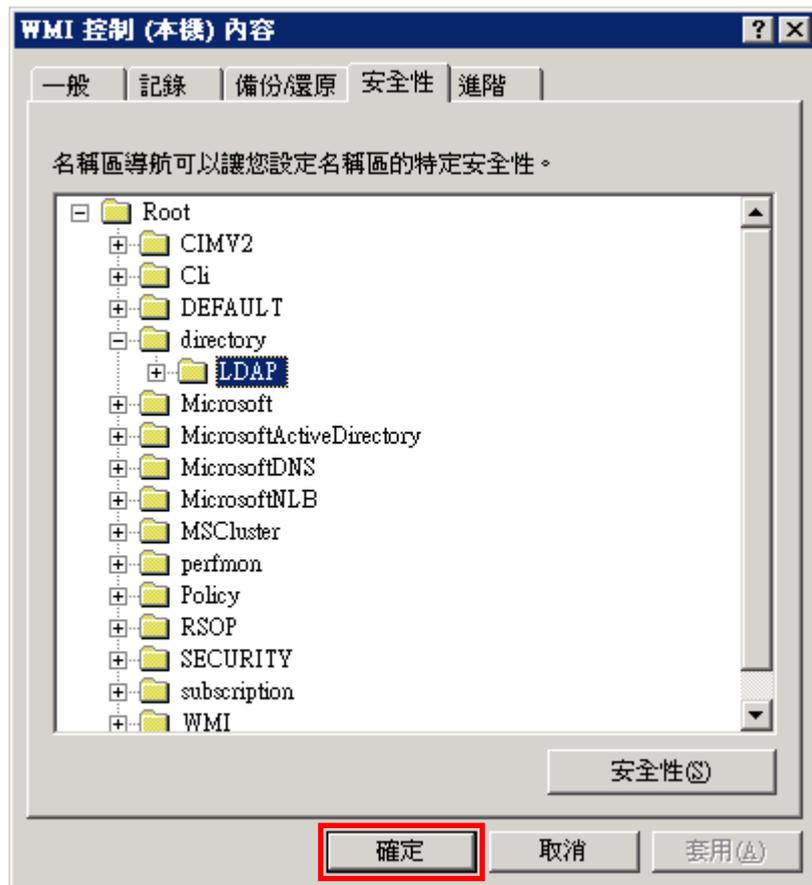


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



3.3.4 設定 Event log 讀取權限

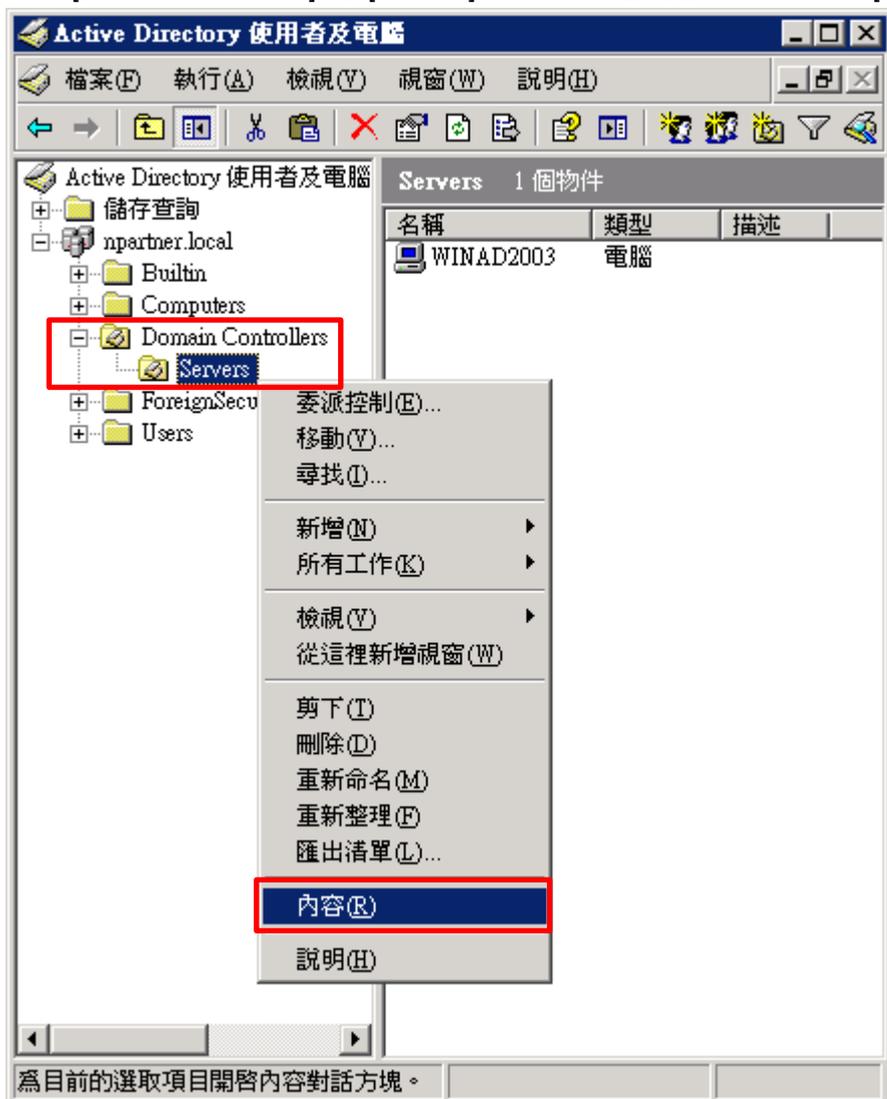
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



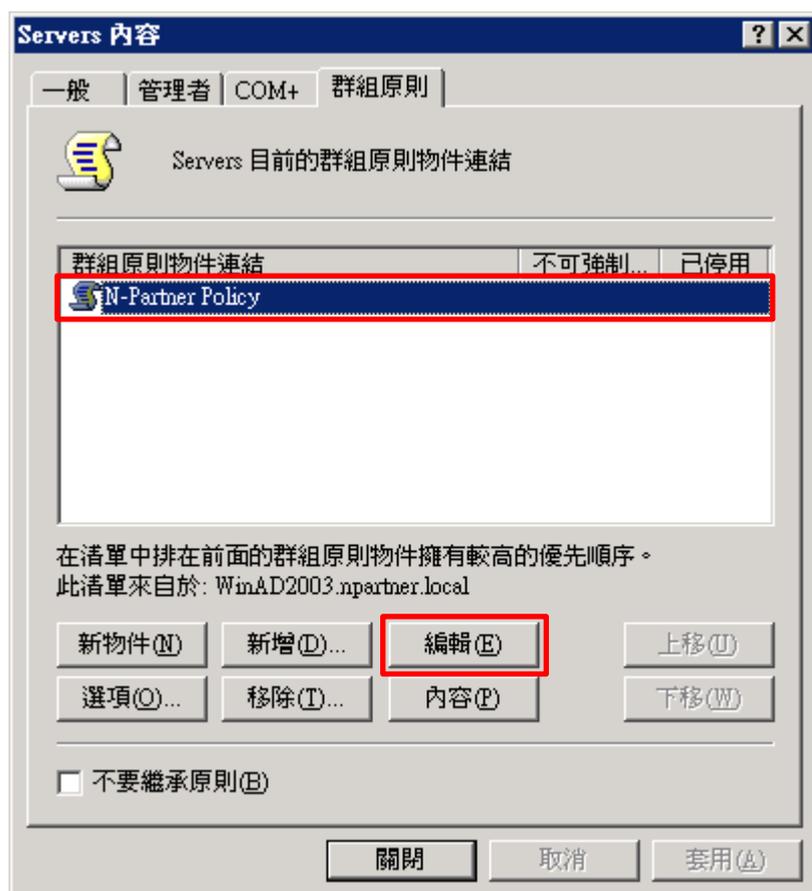
(2) Domain Controllers 的 Servers 組織單位，點選內容

選擇 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [內容]



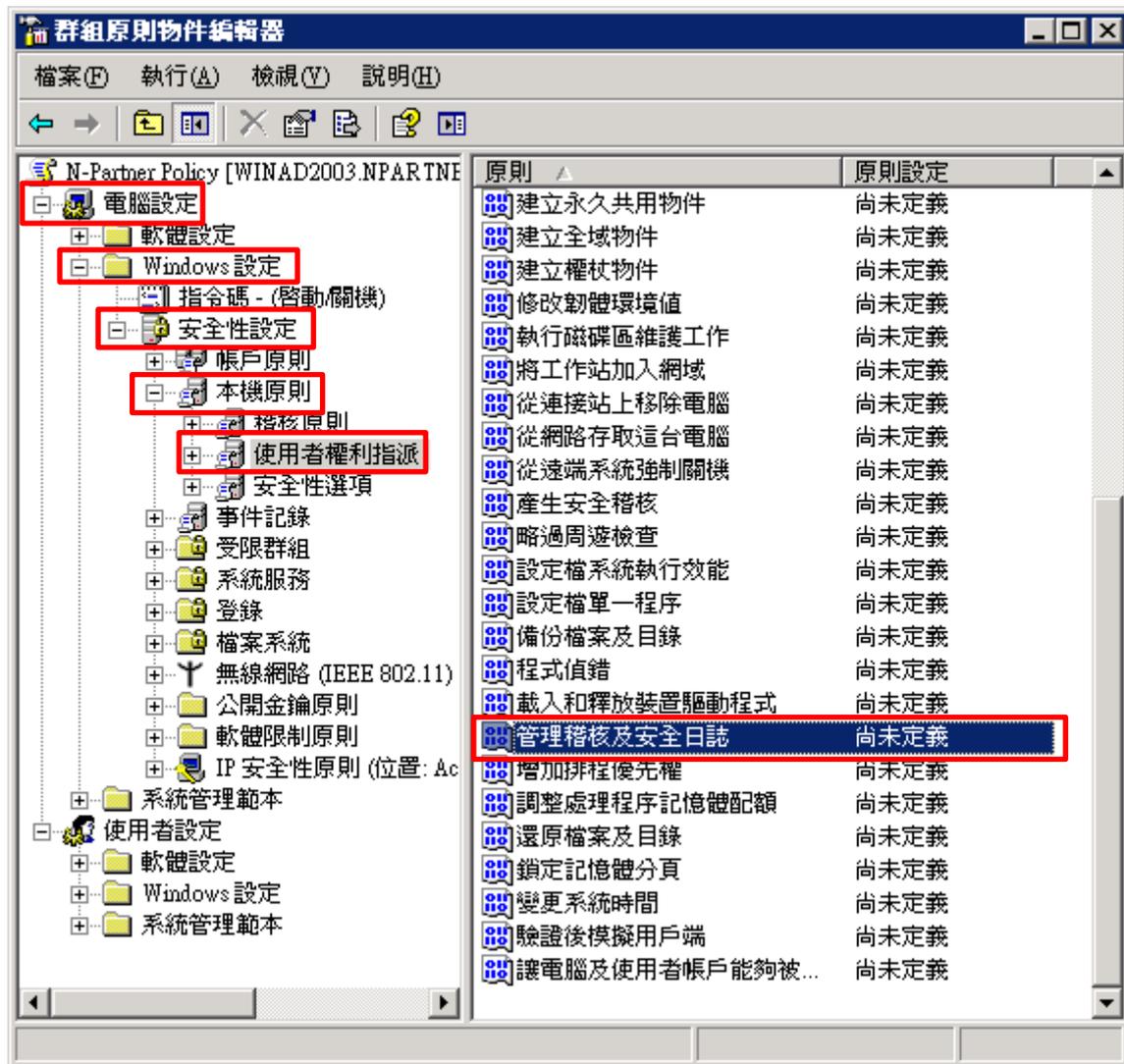
(3) 編輯群組原則物件

點選群組原則物件名稱 [N-Partner Policy] -> 按 [編輯]



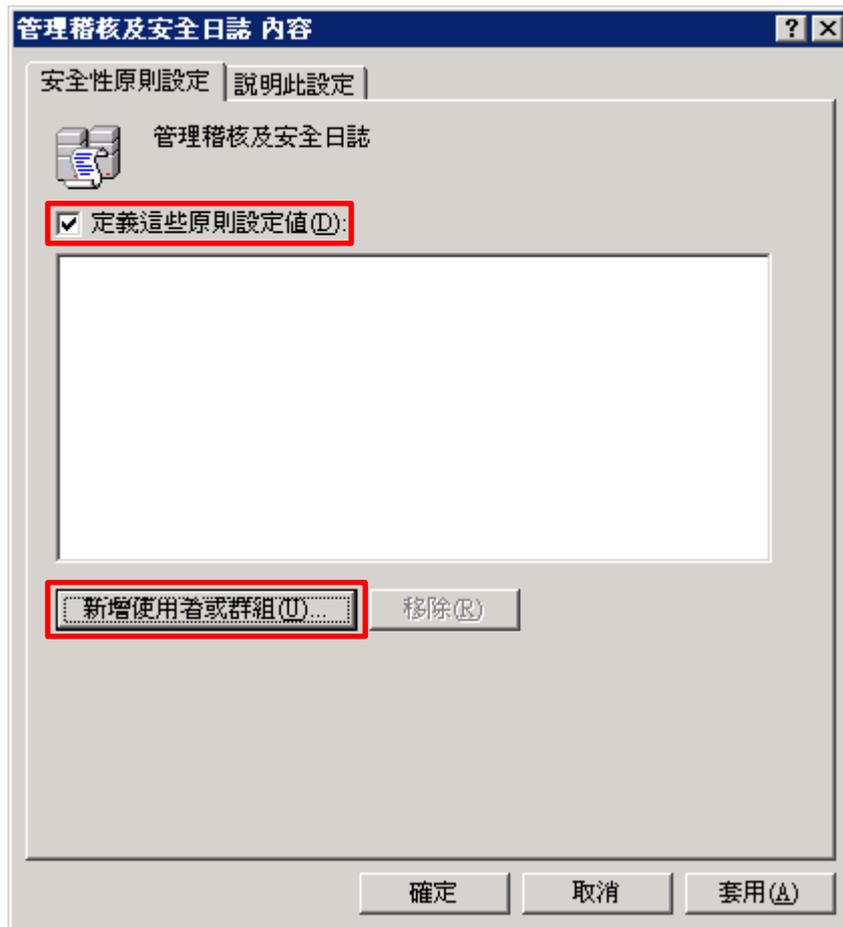
(4) 設定記錄檔

展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權利指派] -> 點選 [管理稽核及安全性日誌] 項目



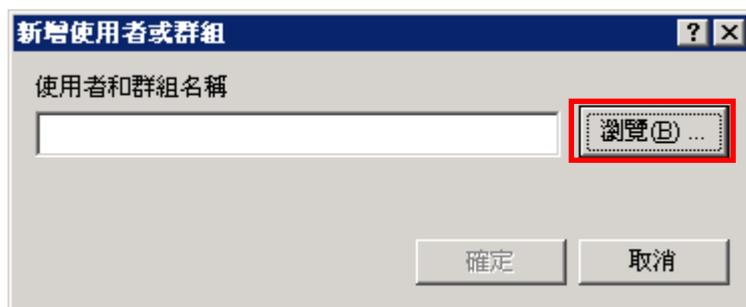
(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



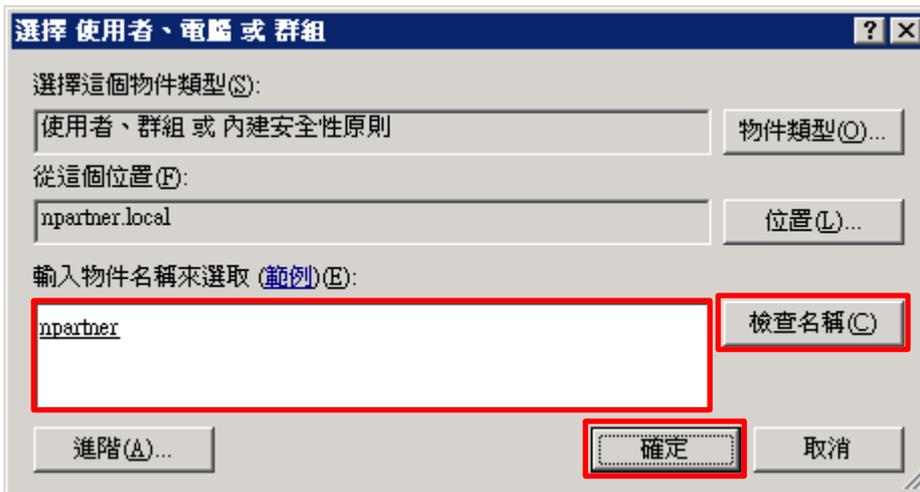
(6) 搜尋使用者

按 [瀏覽]



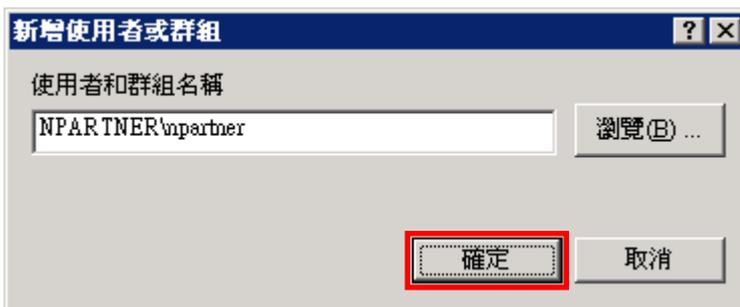
(7) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



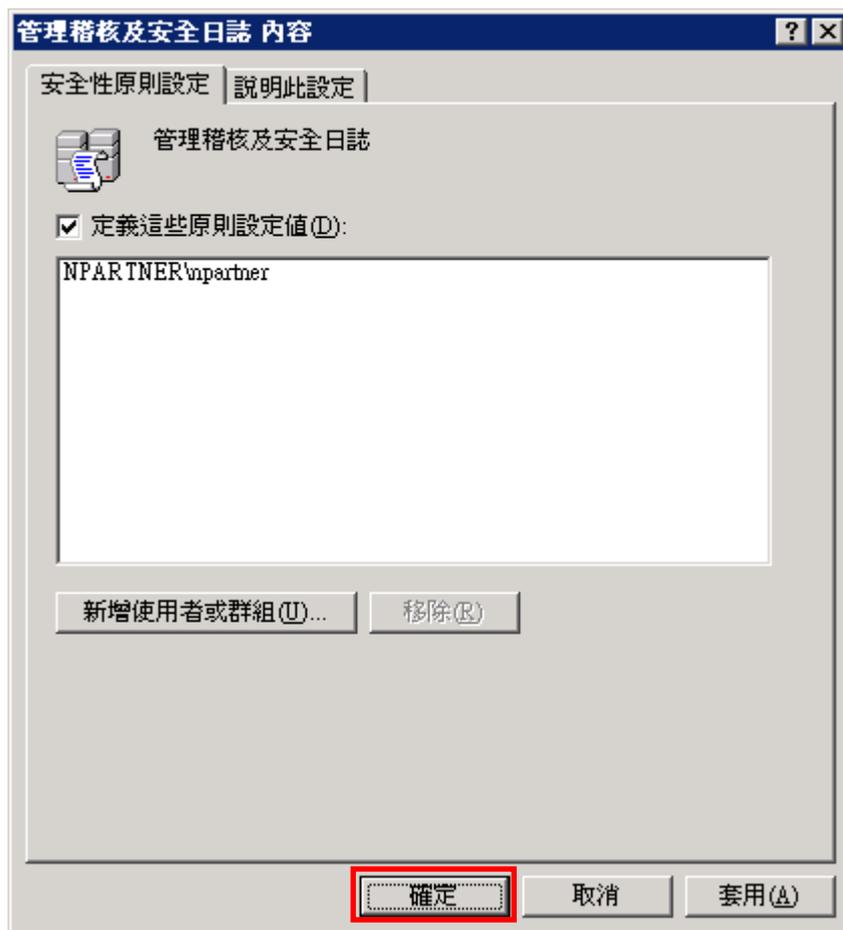
(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

按 [確定]



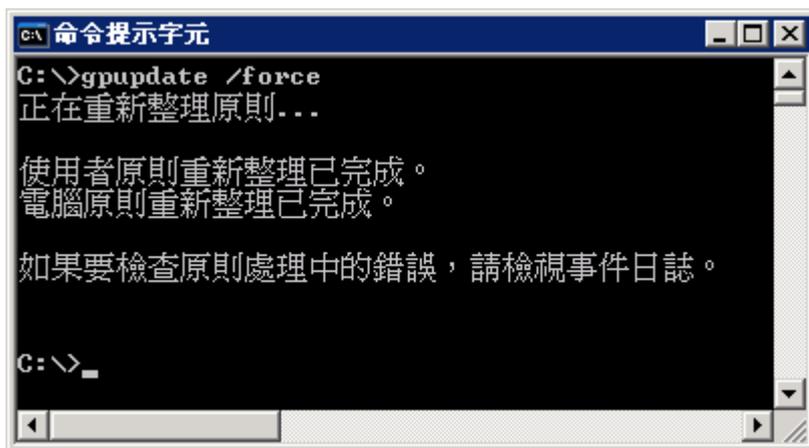
(10) 開啟 [命令提示字元]



命令提示字元

(11) 更新群組原則

C:\> gpupdate /force



```
C:\> gpupdate /force
正在重新整理原則...

使用者原則重新整理已完成。
電腦原則重新整理已完成。

如果要檢查原則處理中的錯誤，請檢視事件日誌。

C:\> _
```

3.3.5 重啟 WMI 服務

(1) 開啟 [命令提示字元]



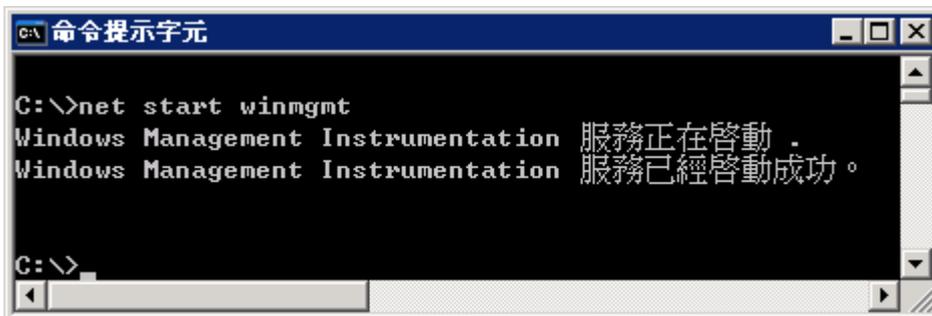
(2) 停用 WMI 服務

C:\> net stop winmgmt



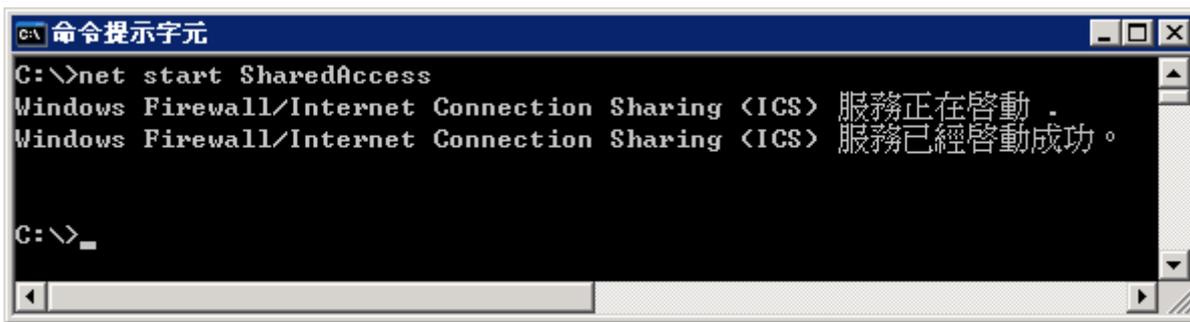
(3) 啟用 WMI 服務

C:\> net start winmgmt



(4) 啟用 Firewall 服務

C:\> net start SharedAccess



```
C:\> net start SharedAccess
Windows Firewall/Internet Connection Sharing (ICS) 服務正在啓動。
Windows Firewall/Internet Connection Sharing (ICS) 服務已經啓動成功。

C:\> _
```

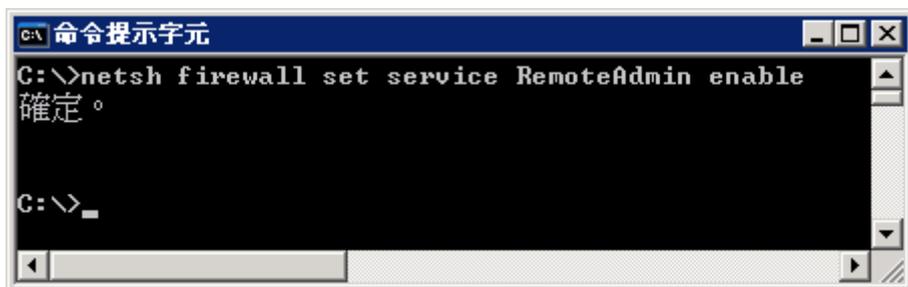
3.3.6 設定防火牆

(1) 開啟 [命令提示字元]



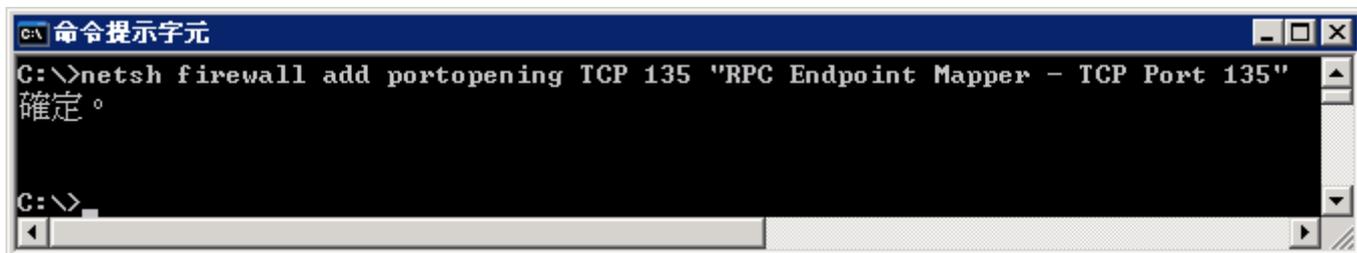
(2) 允許 WMI 通過防火牆

```
C:\> netsh firewall set service RemoteAdmin enable
```



(3) 允許 TCP 135 Port 通過防火牆

```
C:\> netsh firewall add portopening TCP 135 "RPC Endpoint Mapper - TCP Port 135"
```



(4) 查看防火牆設定

C:\> netsh firewall show config

```
C:\> netsh firewall show config

網域 設定檔組態:
-----
操作模式                = 啓用
例外模式                = 啓用
多點傳送/廣播回應模式  = 啓用
通知模式                = 啓用

標準 設定檔組態 <目前的>:
-----
操作模式                = 啓用
例外模式                = 啓用
多點傳送/廣播回應模式  = 啓用
通知模式                = 啓用

標準 設定檔的服務設定:
-----
模式      自訂      名稱
-----
啓用      否      遠端桌面
啓用      否      遠端系統管理

標準 設定檔的連接埠設定:
-----
連接埠 通訊協定 模式      名稱
-----
135     TCP      啓用      RPC Endpoint Mapper - TCP Port 135
3389    TCP      啓用      遠端桌面

記錄設定:
-----
檔案位置          = C:\tmp\pf firewall.log
最大檔案大小      = 4096 KB
丟棄的封包        = 停用
連線              = 啓用

區域連線 防火牆設定:
-----
操作模式                = 啓用

C:\>
```

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](#)

4.1 組織單位設定

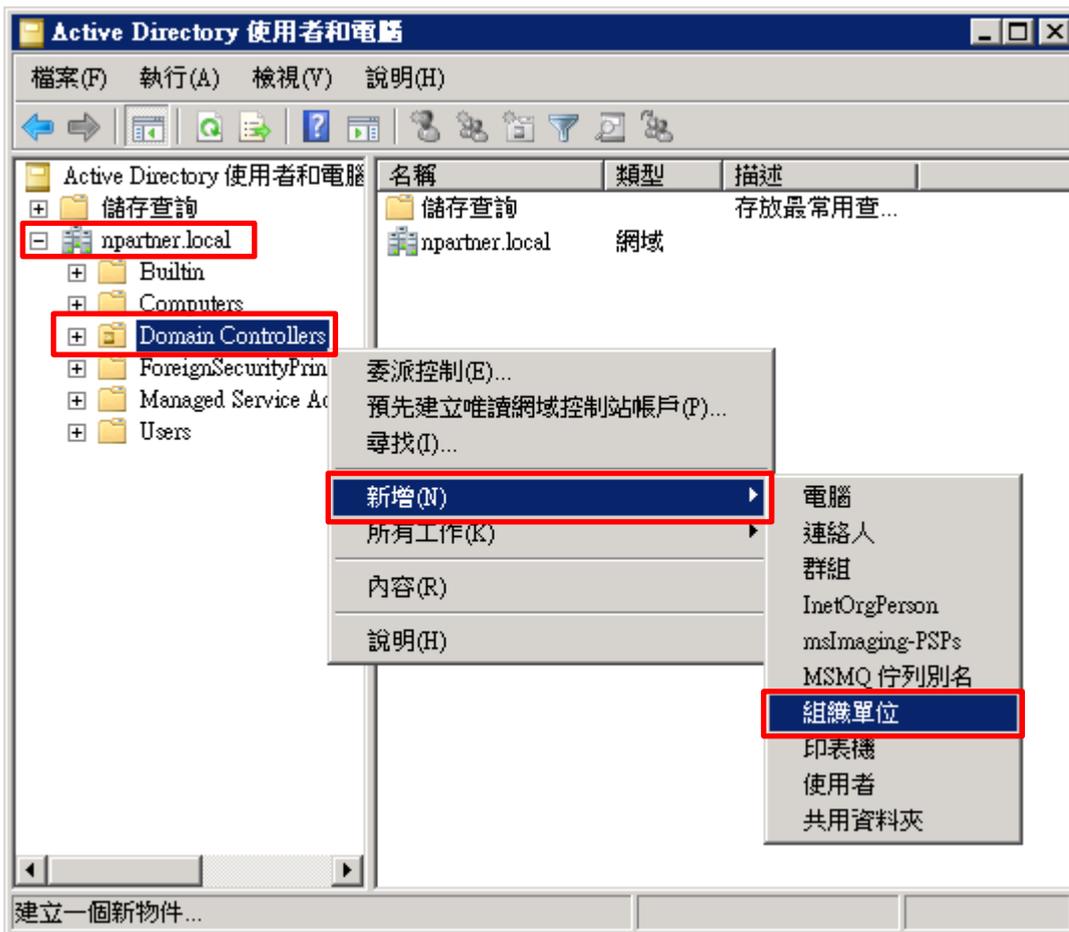
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

[網域名稱] 的 [Domain Controllers] 組織單位，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/Domain Controllers

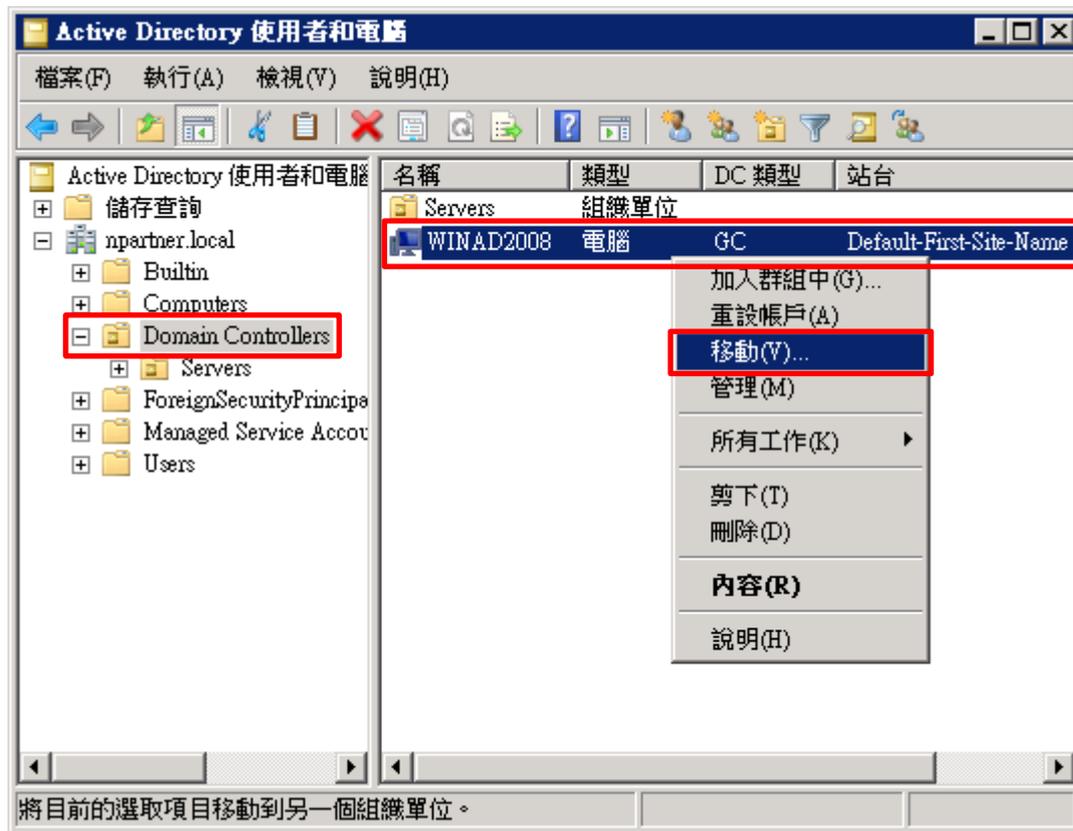
名稱(A):
Servers

保護容器以防止被意外刪除(O)

確定 取消 說明

(4) 移動伺服器至新的組織單位

選擇 [Domain Controllers] 組織單位 -> 在 [WinAD2008] 網域伺服器，按滑鼠右鍵，註：請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]



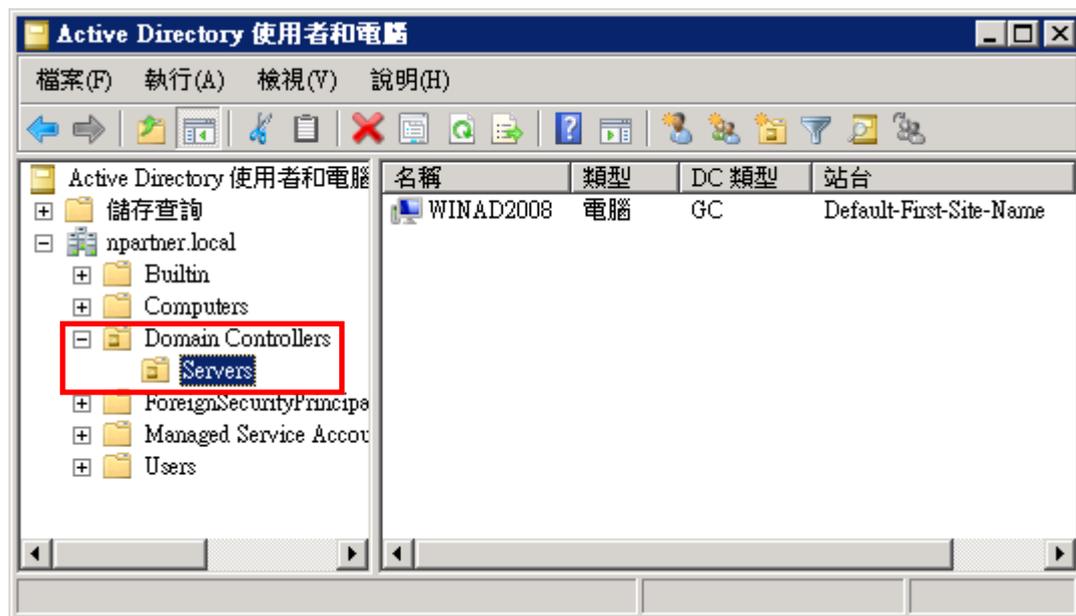
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [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 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2008] 網域伺服器已移動。



4.2 群組原則設定

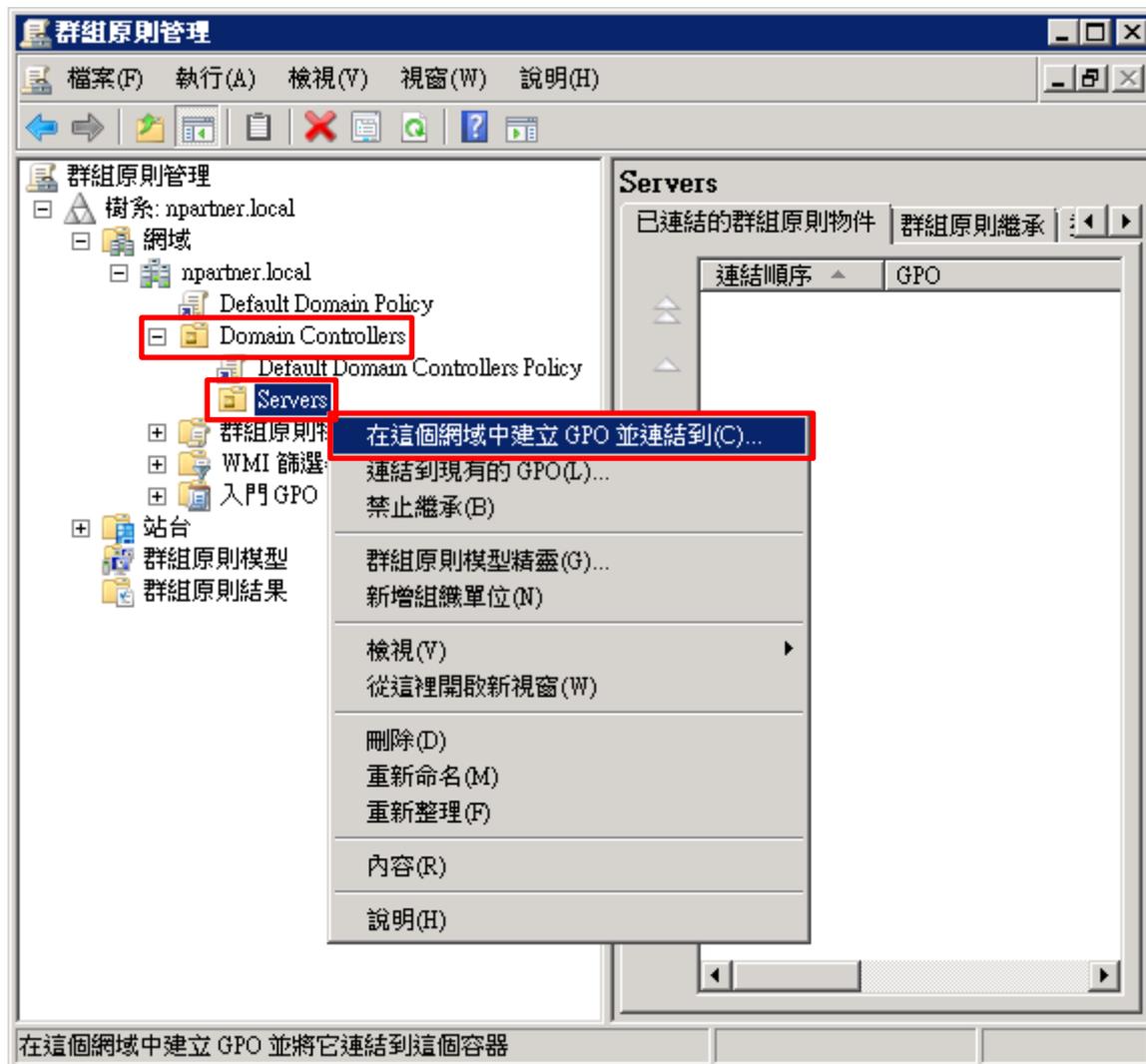
(1) 開啟群組原則管理

開啟 [群組原則管理]



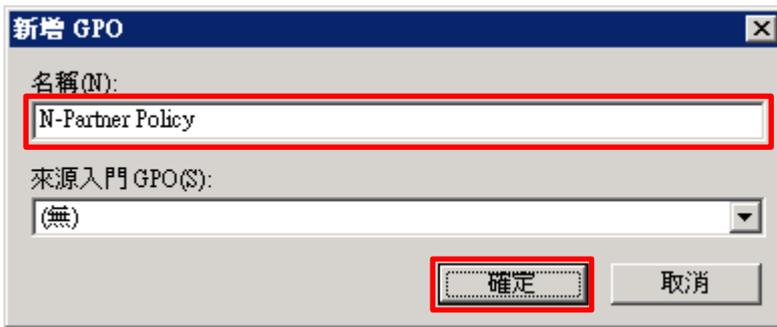
(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [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...]



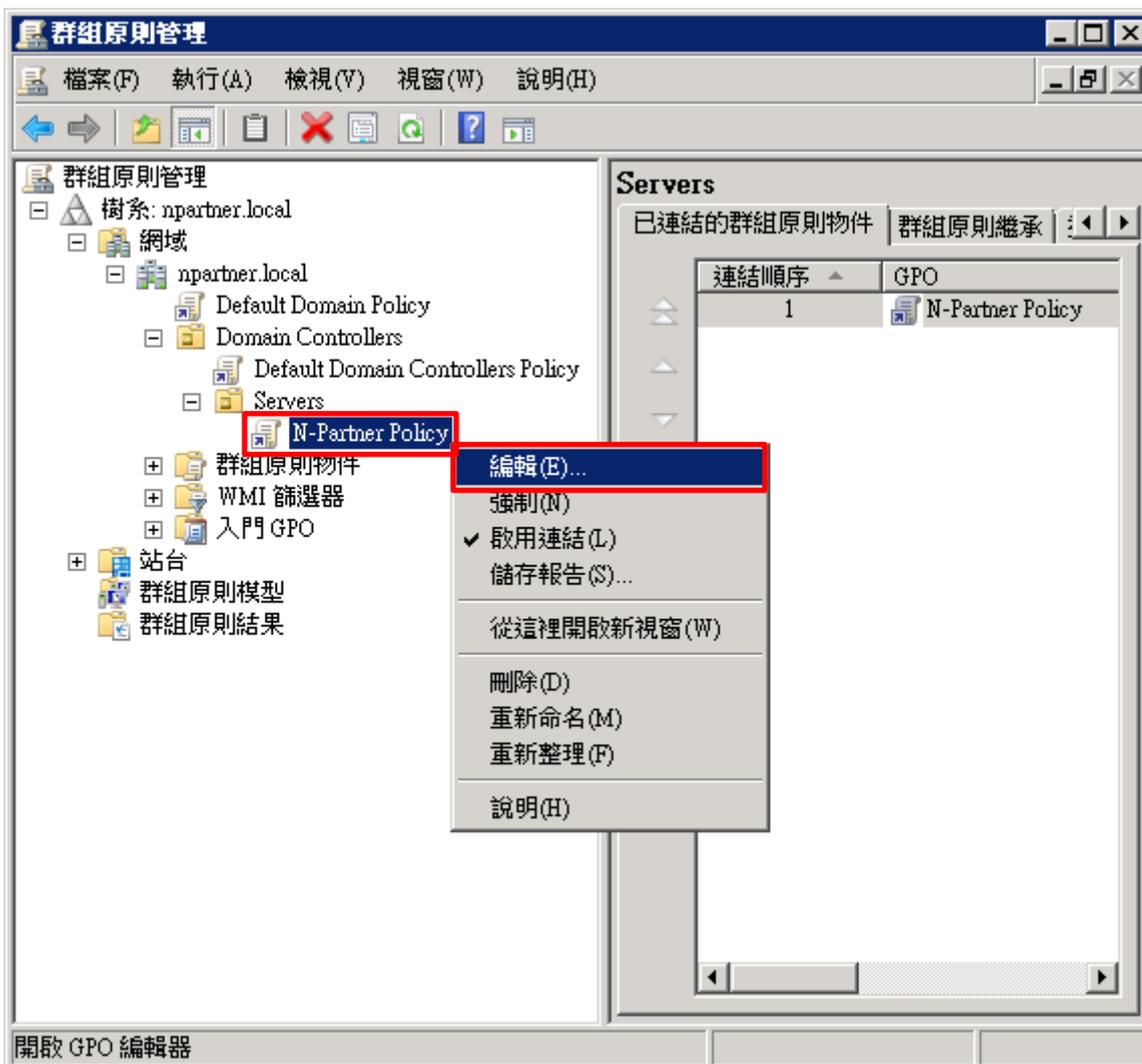
(3) 輸入群組原則物件名稱

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]



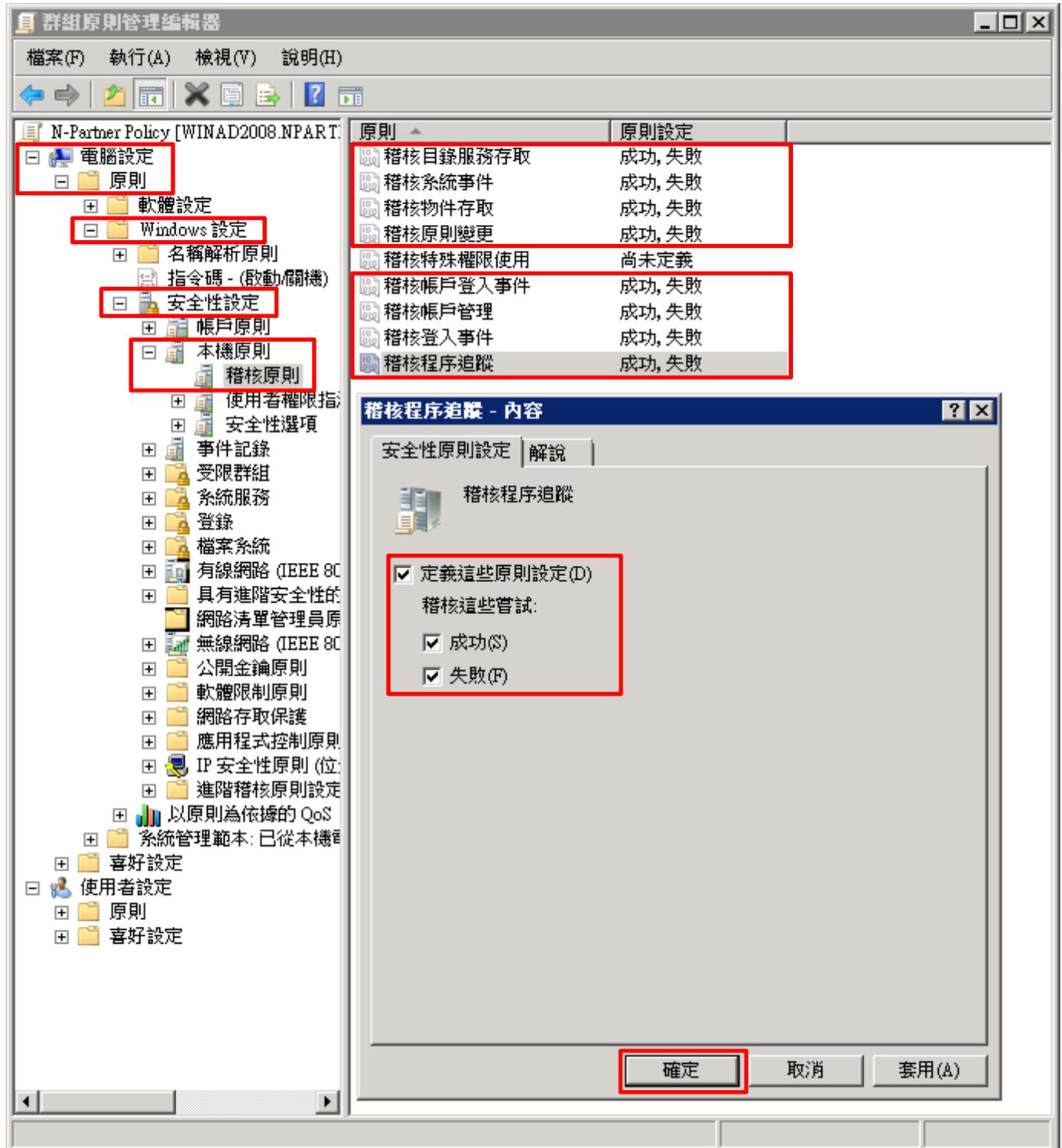
(4) 編輯群組原則物件

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



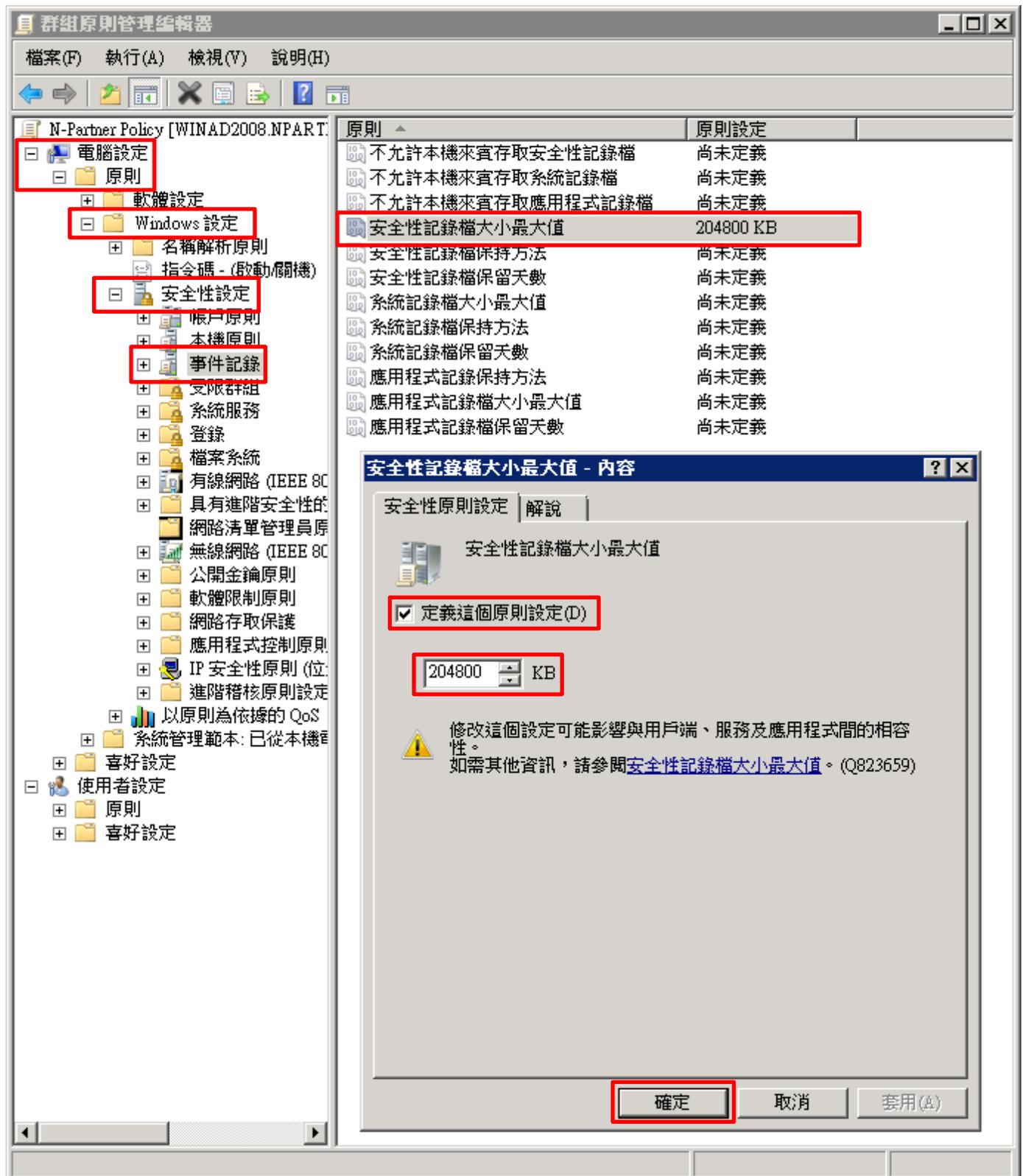
(5) 本機原則：稽核原則

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 [稽核目錄服務存取], [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]



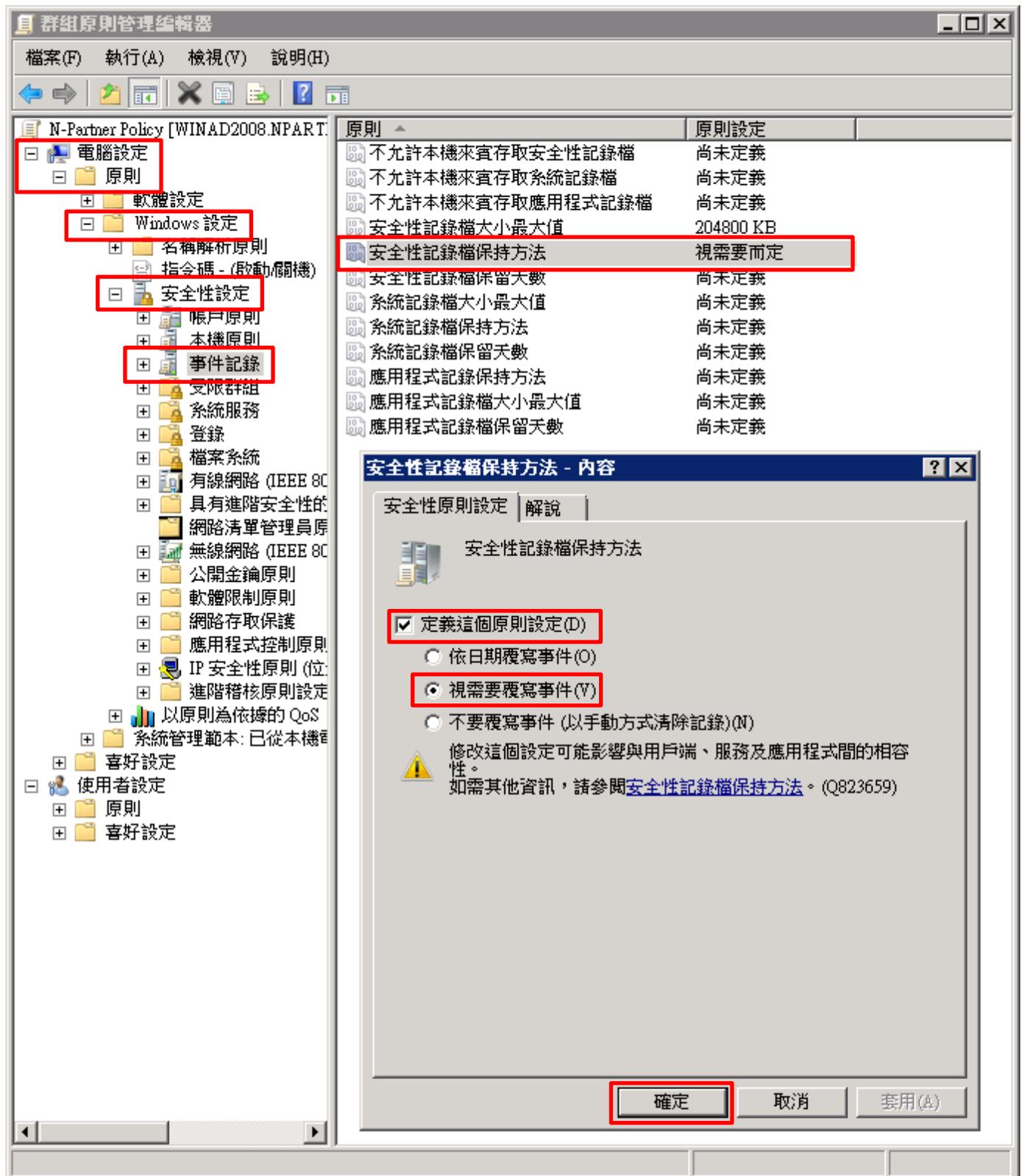
(6) 事件記錄：安全性記錄檔大小最大值

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) 開啟 [Windows PowerShell]



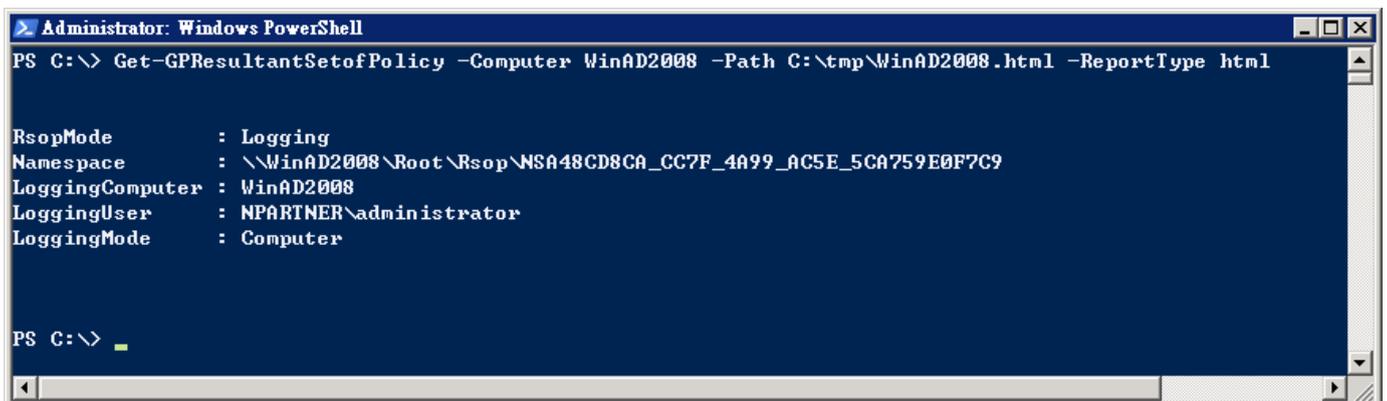
(9) 更新群組原則

PS C:\> gpupdate /force



(10) 產生伺服器群組原則報表

PS C:\> Get-GPResultantSetofPolicy -Computer WinAD2008 -Path C:\tmp\WinAD2008.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 AD 2008 伺服器，套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WINAD2008
資料收集: 2021/6/30 上午 10:07:42

摘要 [顯示全部](#)
[顯示](#)

電腦設定 [隱藏](#)

原則 [隱藏](#)

Windows 設定 [隱藏](#)

安全性設定 [隱藏](#)

帳戶原則/密碼規則 [顯示](#)

帳戶原則/帳戶鎖定原則 [顯示](#)

帳戶原則/Kerberos 原則 [顯示](#)

本機原則/稽核原則 [隱藏](#)

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
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/使用者權限指派 [顯示](#)

本機原則/安全性選項 [顯示](#)

事件記錄檔 [隱藏](#)

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 [顯示](#)

公開金鑰原則/加密檔案系統 [顯示](#)

公開金鑰原則/被信任的根憑證授權單位 [顯示](#)

使用者設定 [顯示](#)

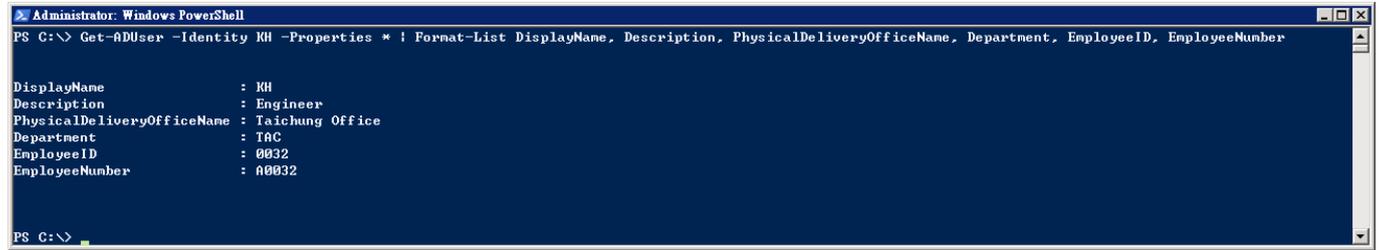
電腦 | 受保護模式: 關閉 | 100%

4.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



紅色文字部位請依客戶環境輸入使用者名稱

(2) N-Reporter [事件查詢] -> 點選 使用者名稱

等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh	4724	Administrator	User Management

(3) 顯示使用者資料

事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh (KH, TAC, 0032, (Engineer))	4724	Administrator	User Management

4.3.1 新增非管理帳號

(1) 開啟 [Active Directory PowerShell Snap-In]



(2) 新增帳號

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell 的 Active Directory 模組". The console shows the execution of the command: `New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True`. The command is executed successfully, and the prompt returns to `PS C:\>`.

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell 的 Active Directory 模組". The console shows the execution of the command: `Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled`. The output is as follows:
`DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local`
`Enabled : True`
`GivenName :`
`MemberOf : {}`
`Name : npartner`
`ObjectClass : user`
`ObjectGUID : 72bca9e-46db-42e4-aae6-597e8c33cd73`
`PasswordNeverExpires : True`
`SamAccountName : npartner`
`SID : S-1-5-21-2487502702-2233515932-3288244281-1106`
`Surname :`
`UserPrincipalName : npartner@npartner.local`
The prompt returns to `PS C:\>`.

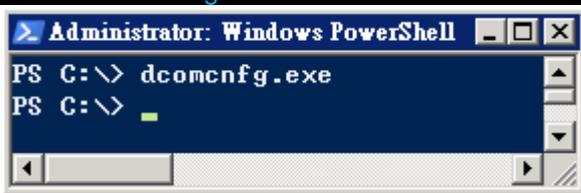
4.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



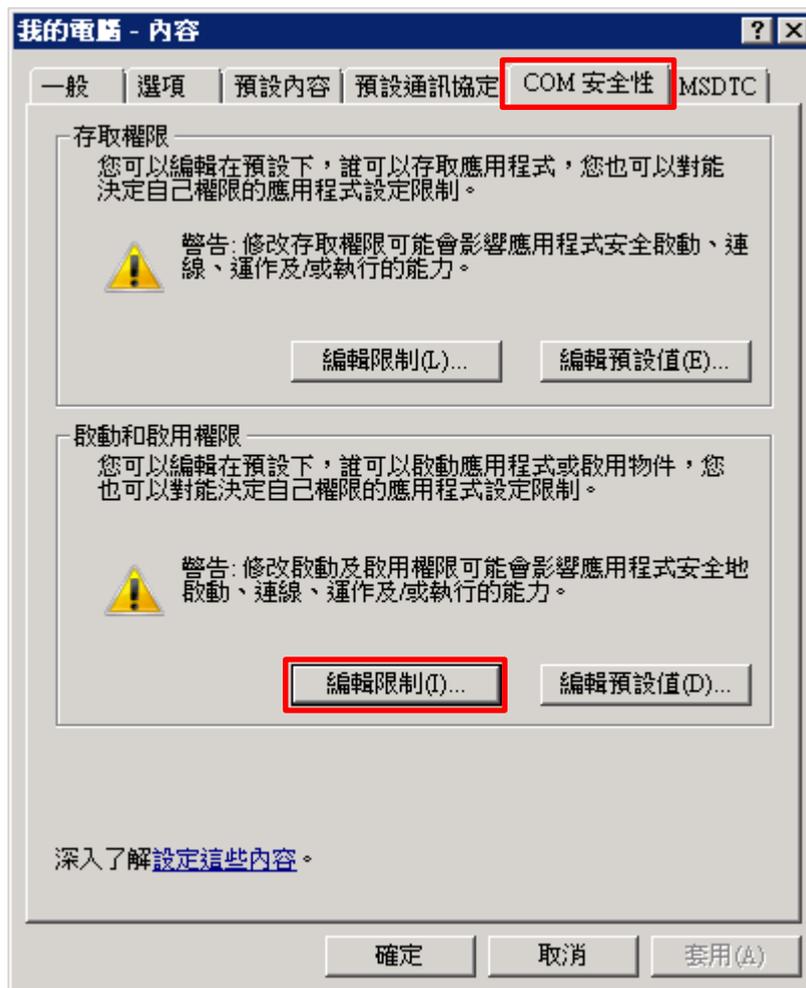
(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



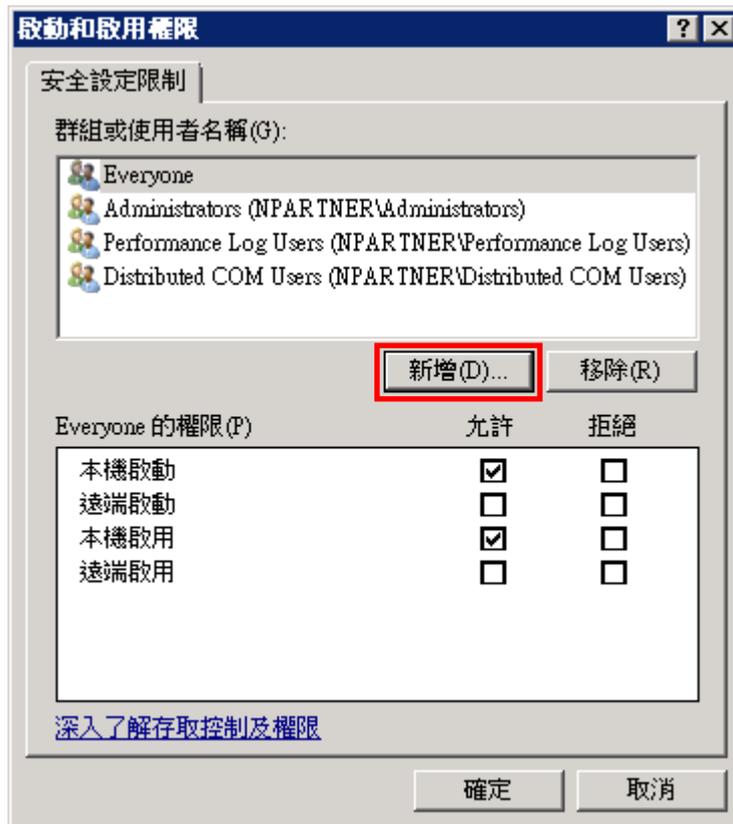
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



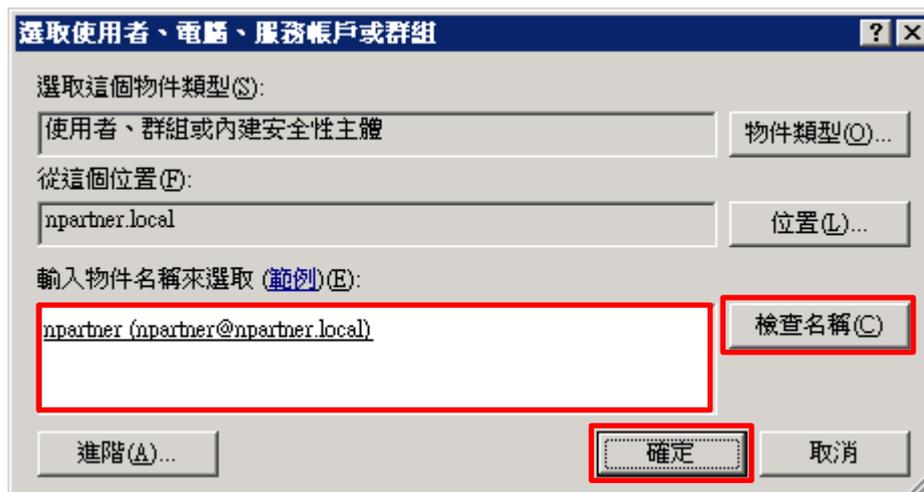
(5) 新增 DCOM 使用者權限

點選 [新增]



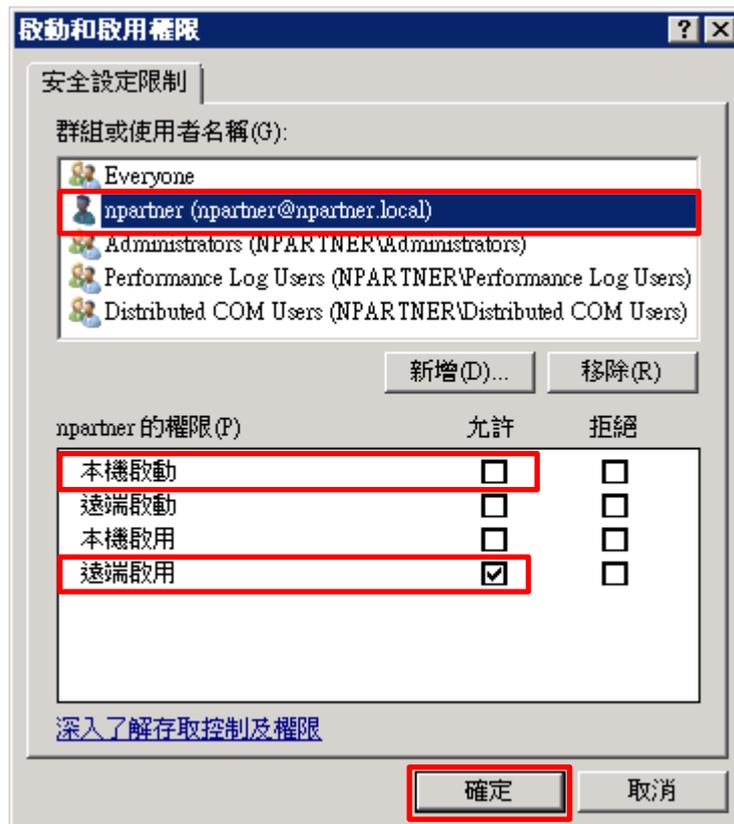
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

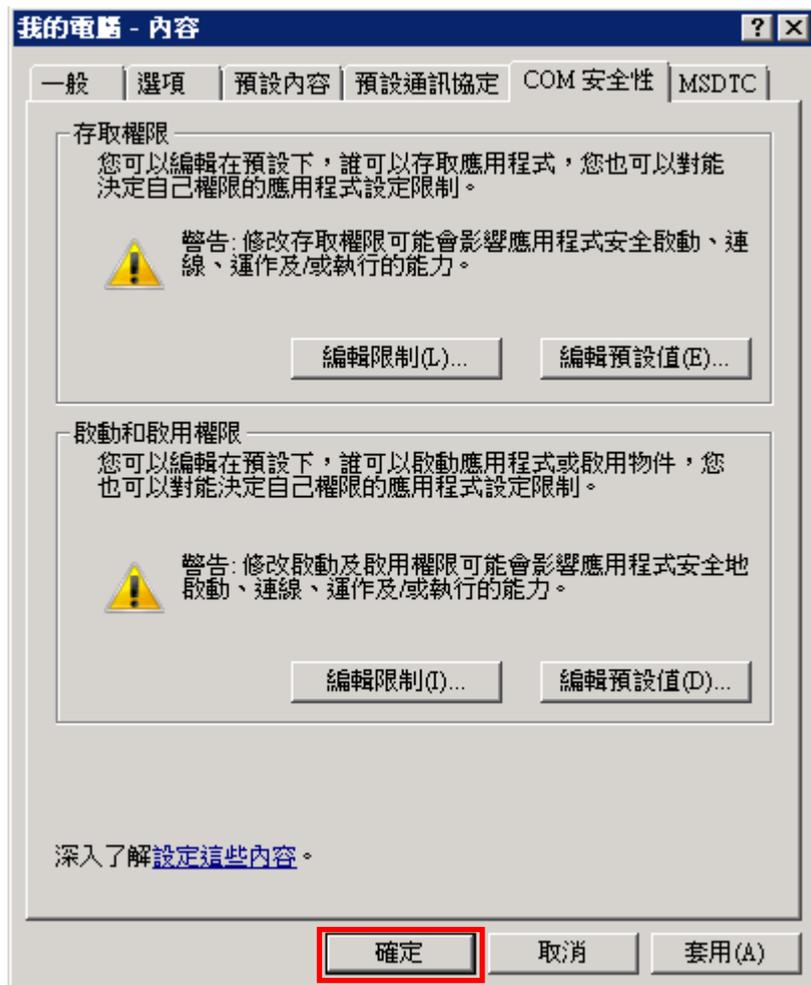


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



4.3.3 設定 WMI 權限

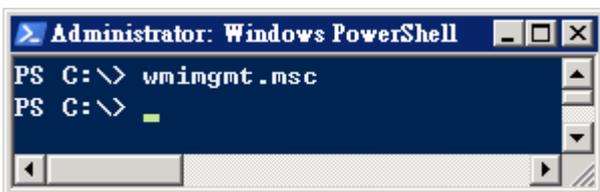
4.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



(2) 開啟 WMI 控制

PS C:\> `wimgmt.msc`



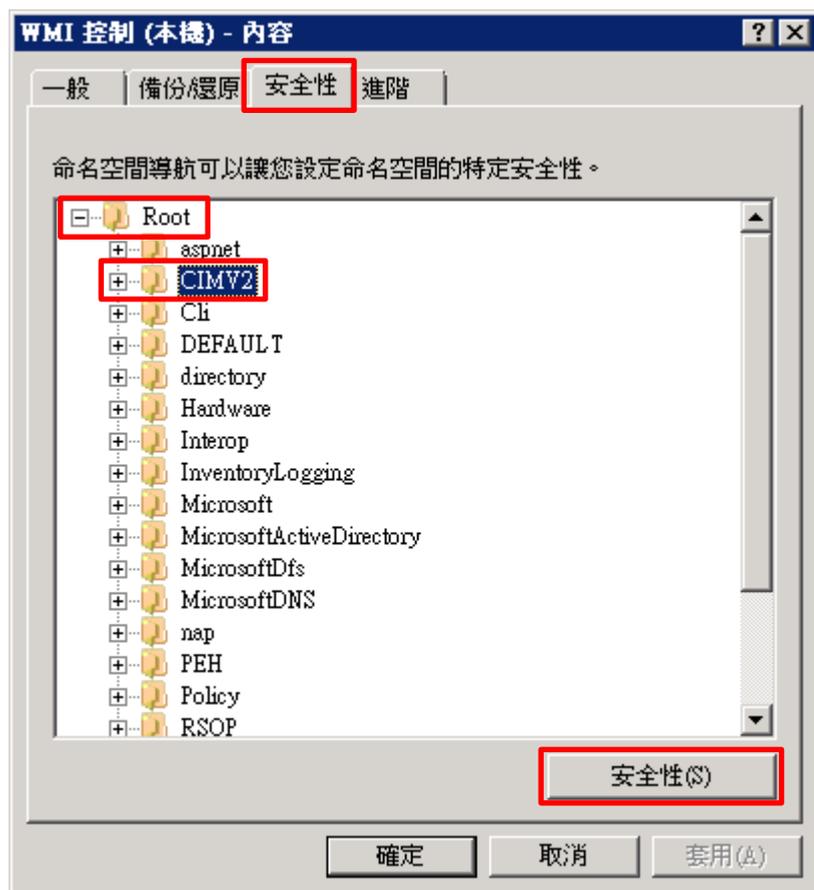
(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]



(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



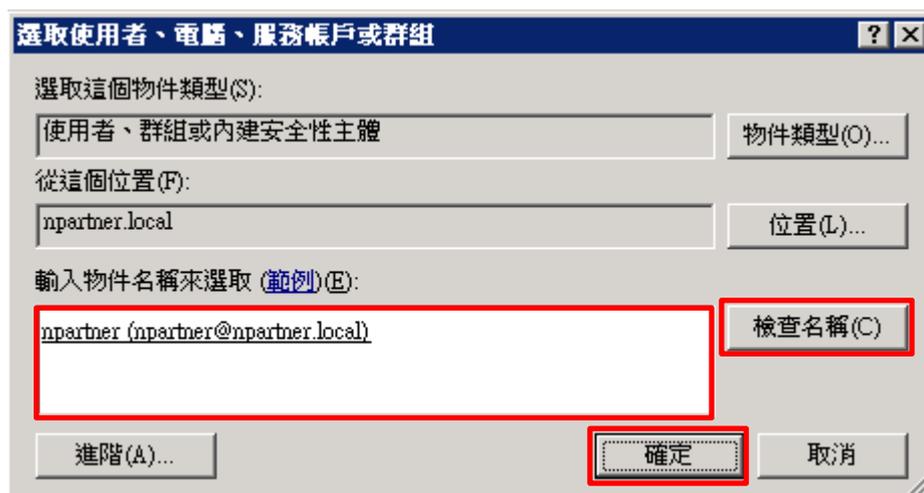
(5) 新增 WMI 使用者權限

按 [新增]



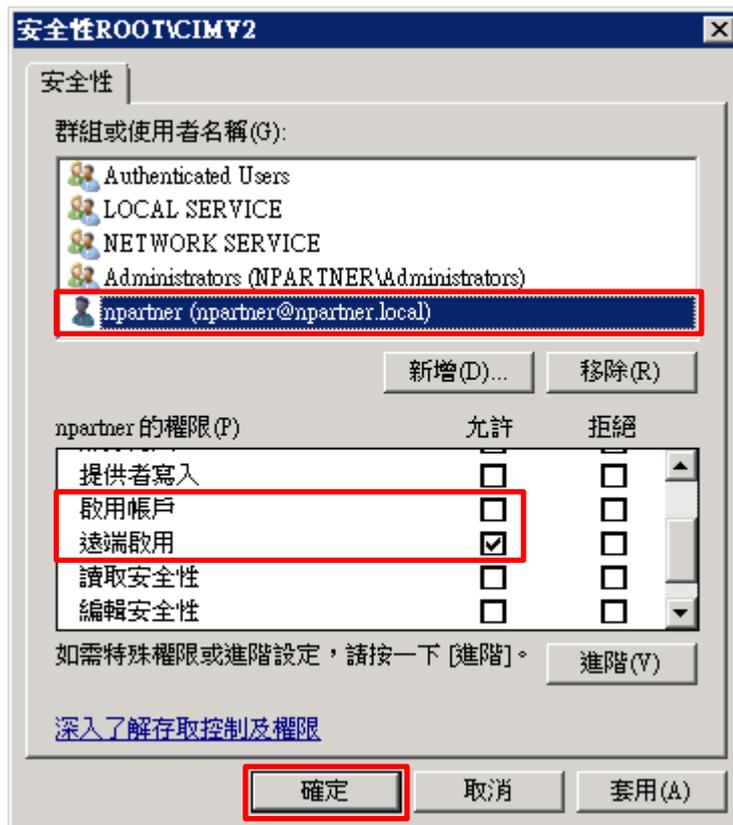
(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

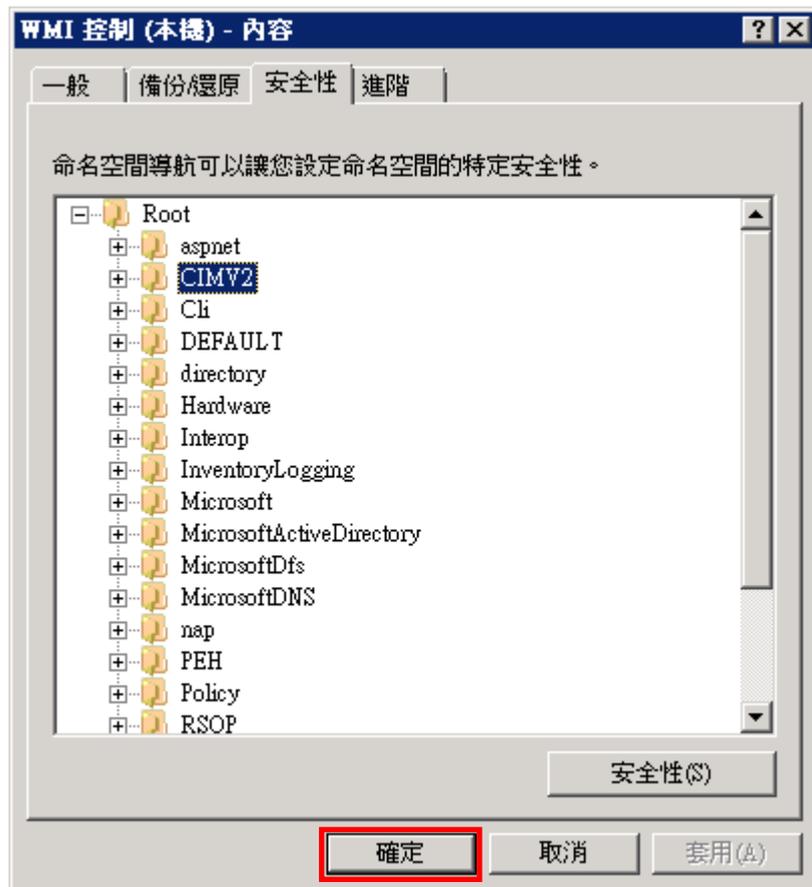


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



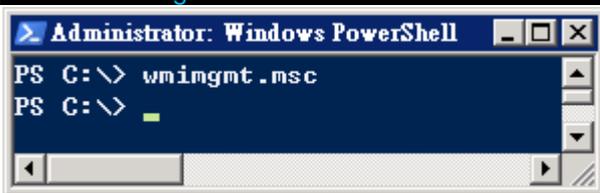
4.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



(2) 開啟元件服務

PS C:\> wmicmgmt.msc



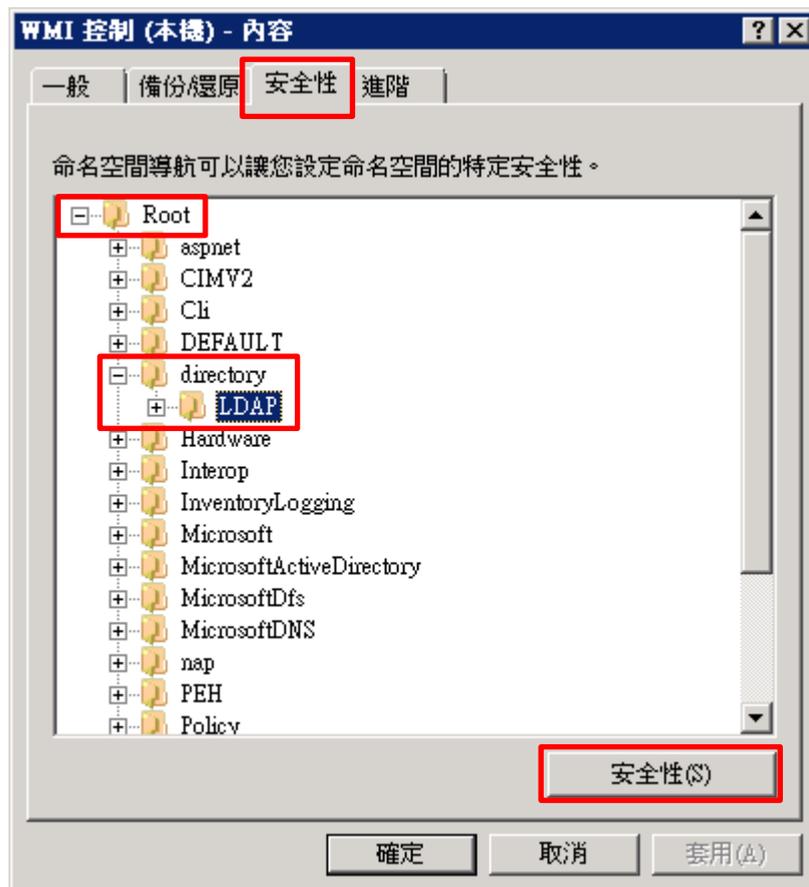
(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]



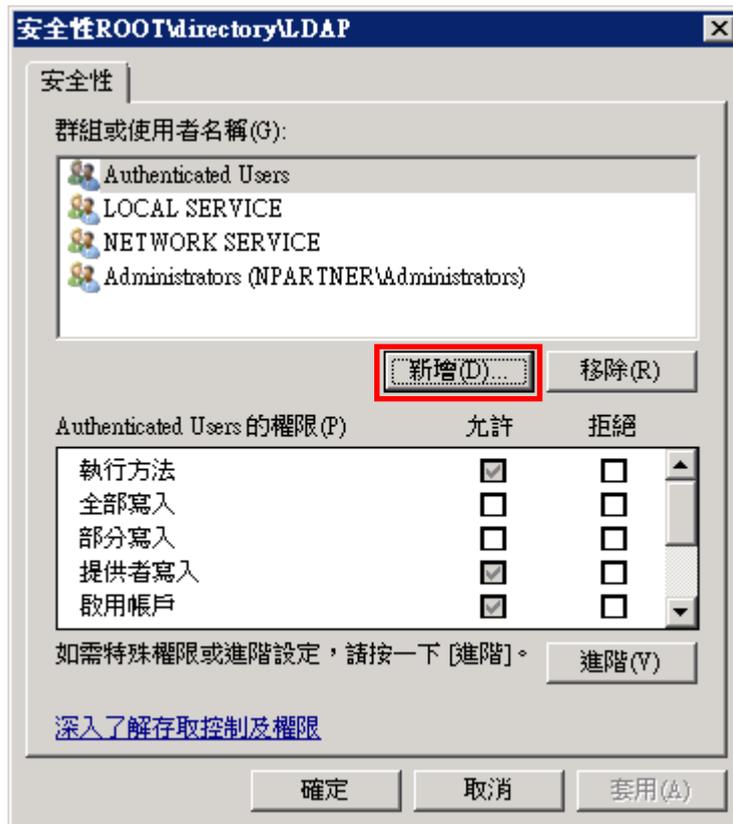
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



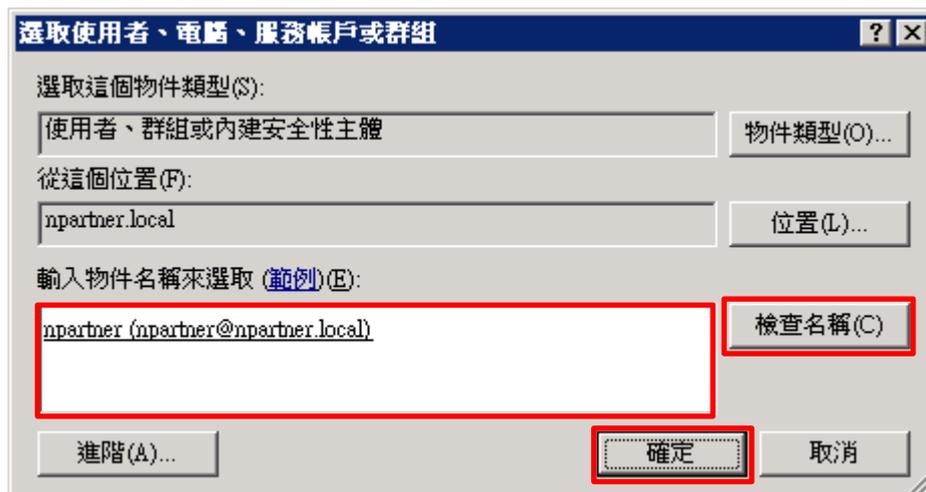
(5) 新增 WMI 使用者權限

按 [新增]



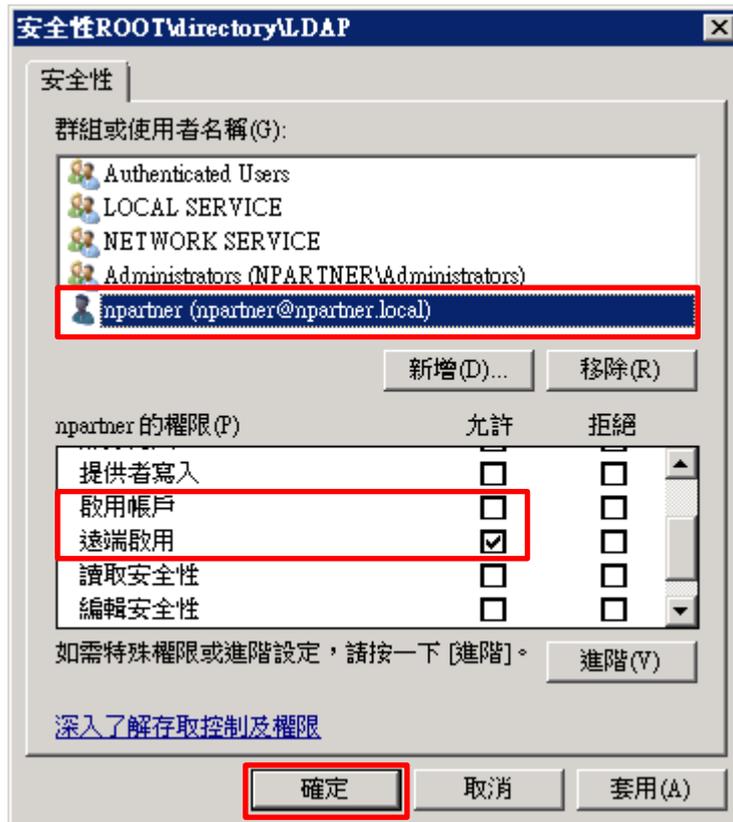
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

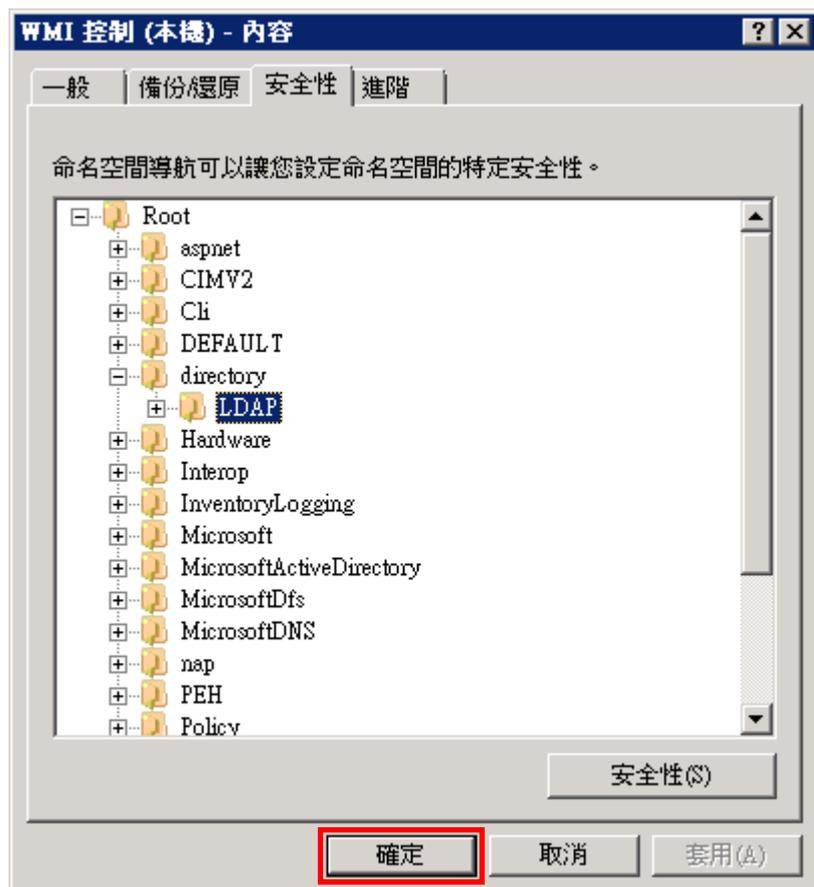


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



4.3.4 設定 Event log 讀取權限

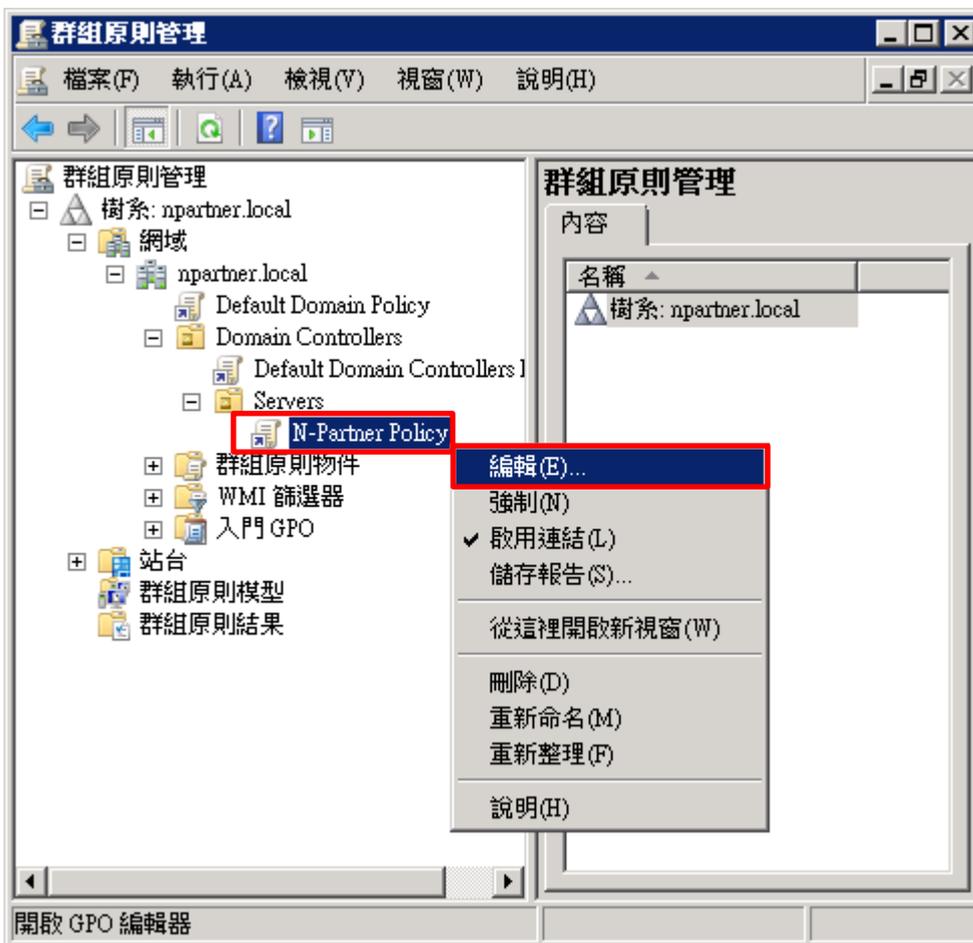
(1) 開啟群組原則管理

開啟 [群組原則管理]



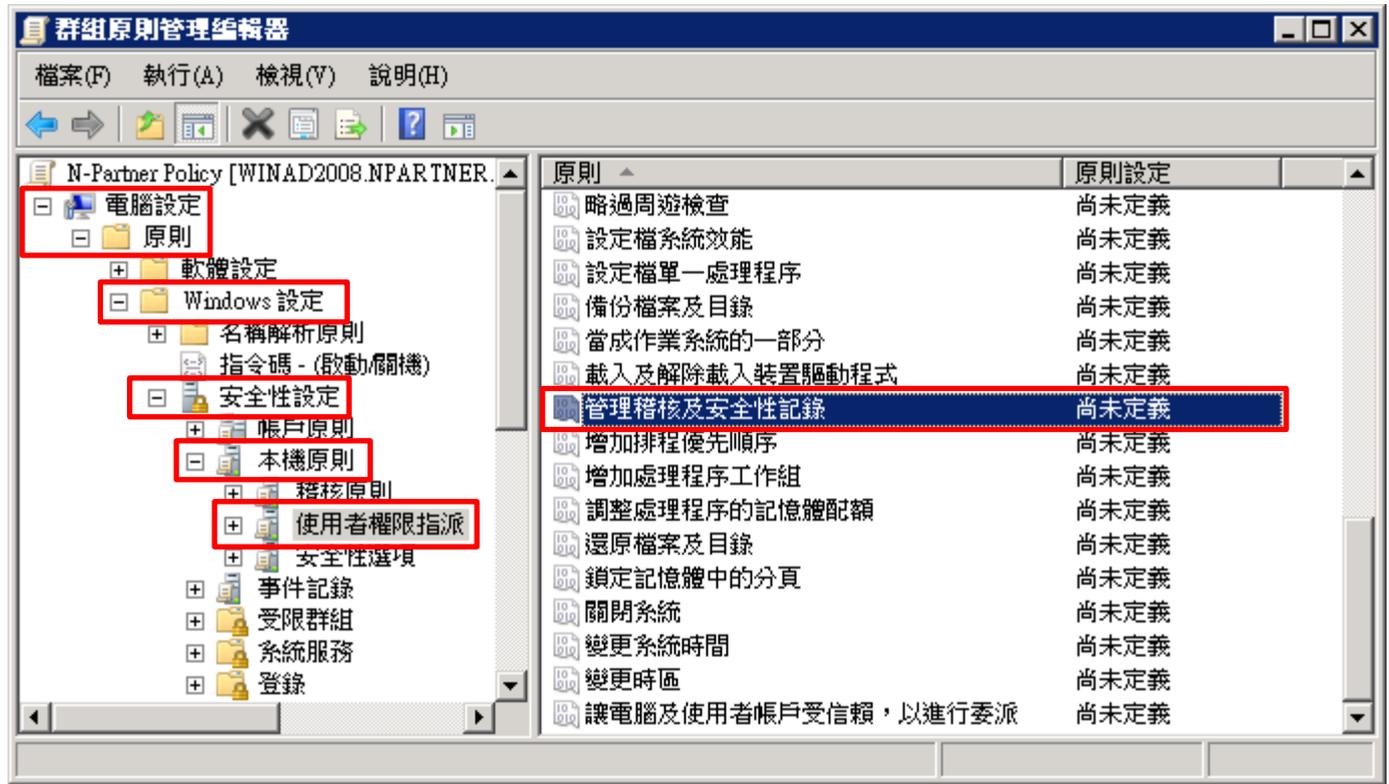
(2) 編輯群組原則物件

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



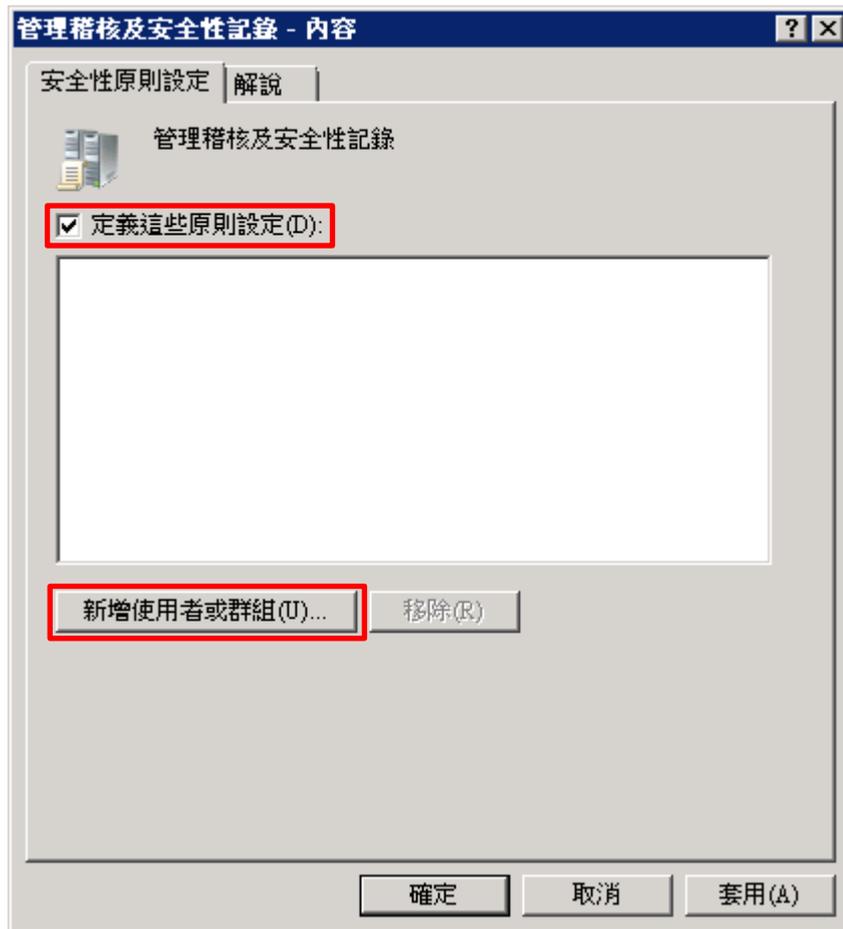
(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全性記錄] 項目



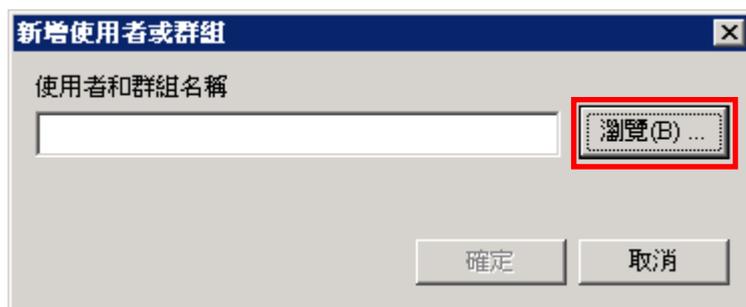
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



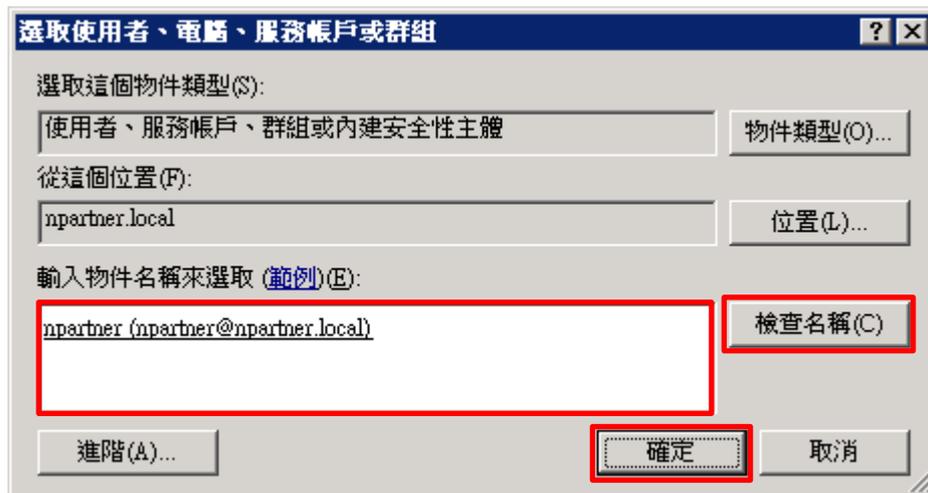
(5) 搜尋使用者

按 [瀏覽]



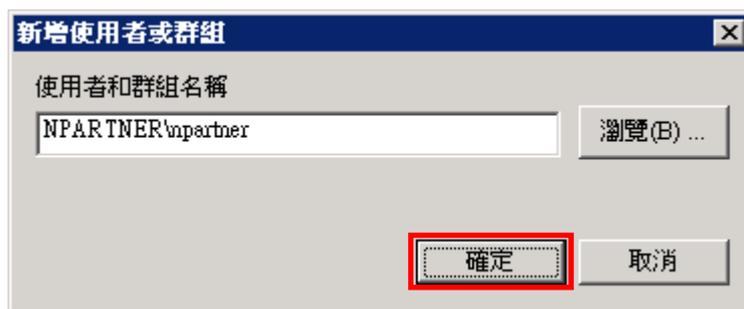
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



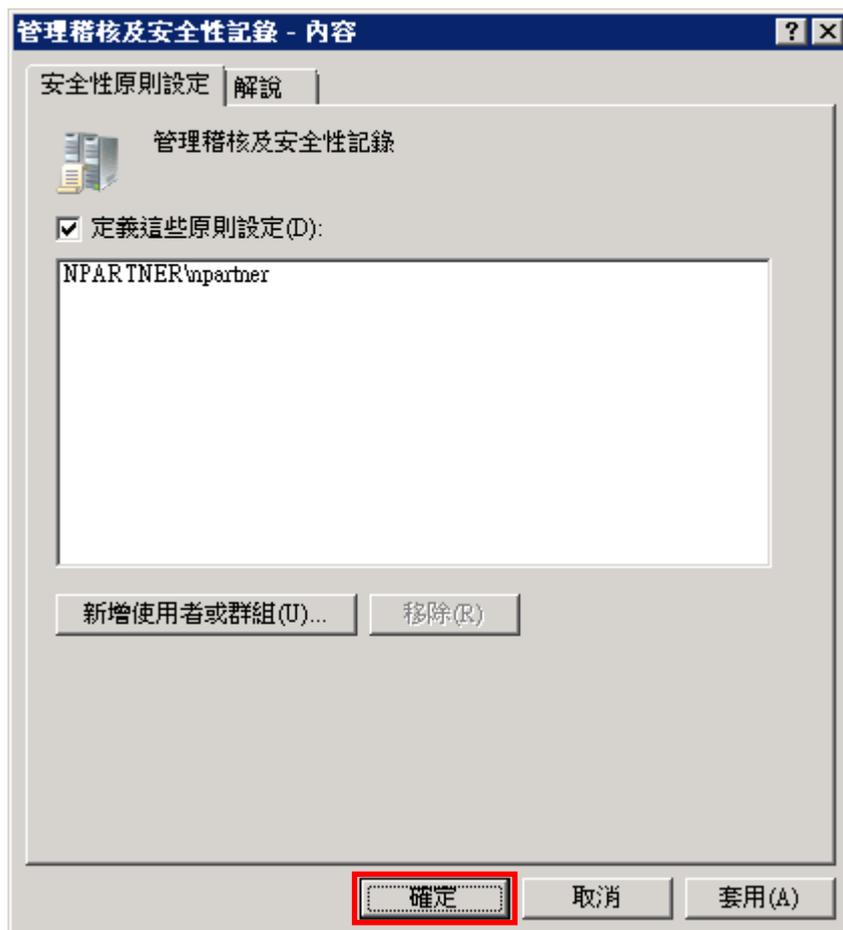
(7) 確定使用者

按 [確定]



(8) 確定設定記錄檔

按 [確定]



(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

PS C:\> gpupdate /force



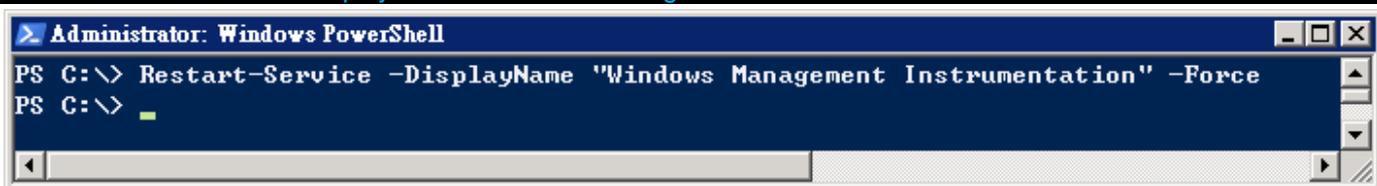
4.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



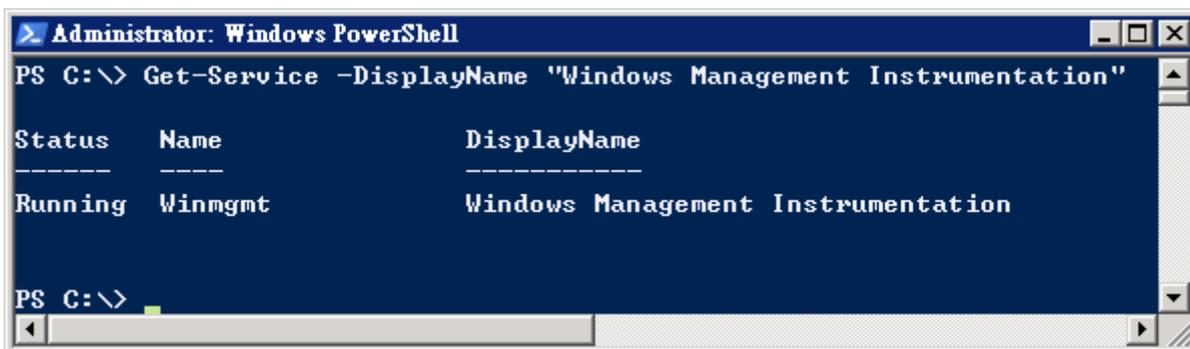
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



4.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 允許 WMI 通過防火牆

```
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes` being executed. The output is "已經更新 4 規則。" followed by "確定。" on the next line. The prompt `PS C:\>` is visible at the bottom.

```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
已經更新 4 規則。
確定。
PS C:\>
```

(3) 查看防火牆 WMI 啟用狀態

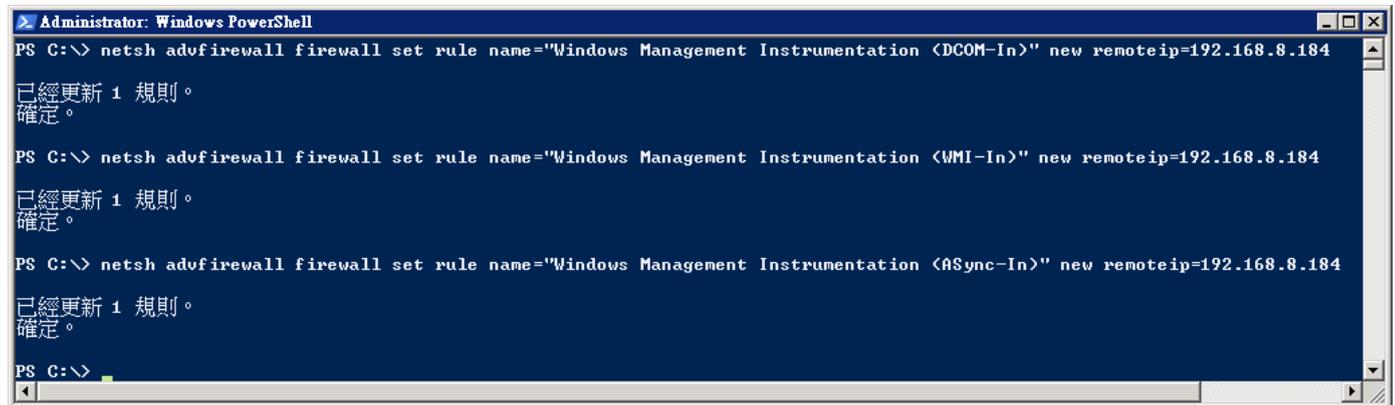
```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2` being executed. The output lists five firewall rules, all with "啟用:" (Enabled) set to "是" (Yes). The rules are: "Windows Management Instrumentation (DCOM-In)", "Windows Management Instrumentation (WMI)", "Windows Management Instrumentation (WMI-In)", "Windows Management Instrumentation (WMI-Out)", and "Windows Management Instrumentation (ASync-In)". Each rule entry shows its name, enabled status, group, local IP, and remote IP.

```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
> 規則名稱: Windows Management Instrumentation (DCOM-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 任一
> 規則名稱: Windows Management Instrumentation (WMI-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 任一
> 規則名稱: Windows Management Instrumentation (WMI-Out)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 任一
> 規則名稱: Windows Management Instrumentation (ASync-In)
-----
  啟用: 是
  群組: Windows Management Instrumentation (WMI)
  LocalIP: 任一
  RemoteIP: 任一
PS C:\>
```

(4) 設定防火牆 · 只允許 N-Reporter IP query WMI

```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)" new remoteip=192.168.8.184
```

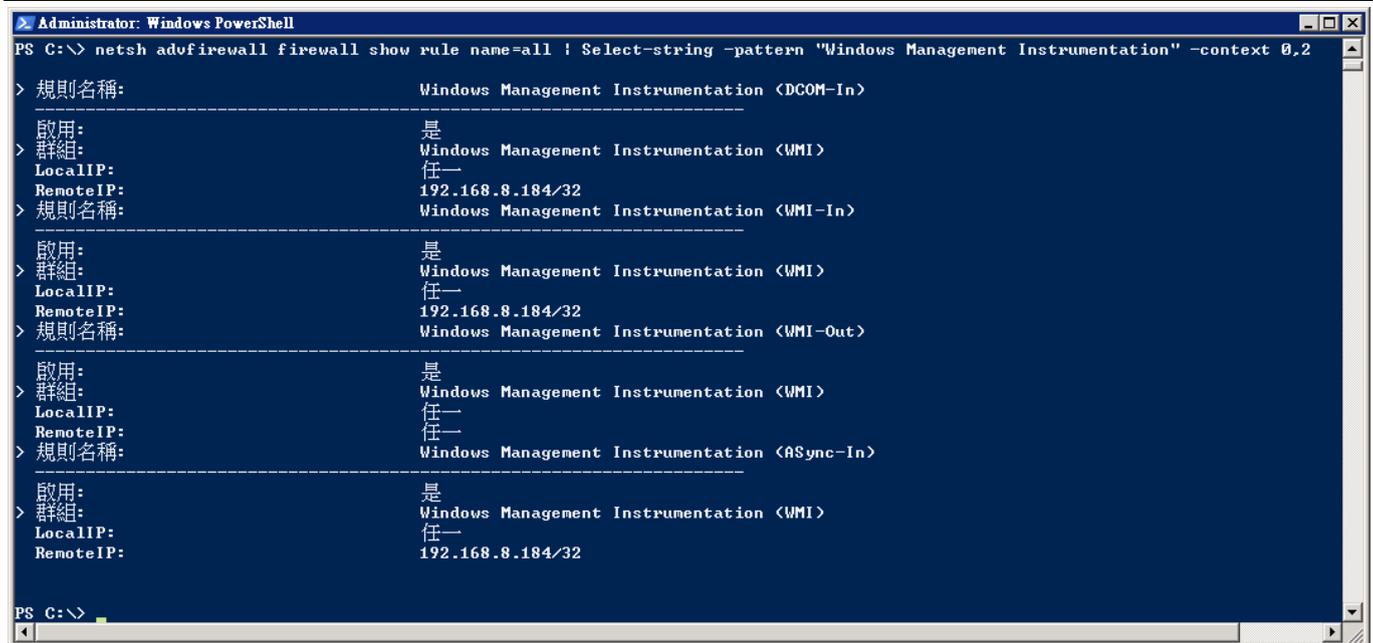


```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation <DCOM-In>" new remoteip=192.168.8.184
已經更新 1 規則。
確定。
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation <WMI-In>" new remoteip=192.168.8.184
已經更新 1 規則。
確定。
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation <ASync-In>" new remoteip=192.168.8.184
已經更新 1 規則。
確定。
PS C:\>
```

紅色文字部位請輸入 N-Reporter IP address

(5) 查看防火牆 WMI 設定狀態

```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```



```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all ! Select-string -pattern "Windows Management Instrumentation" -context 0,2
> 規則名稱: Windows Management Instrumentation <DCOM-In>
-----
  啟用: 是
  群組: Windows Management Instrumentation <WMI>
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32
> 規則名稱: Windows Management Instrumentation <WMI-In>
-----
  啟用: 是
  群組: Windows Management Instrumentation <WMI>
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32
> 規則名稱: Windows Management Instrumentation <WMI-Out>
-----
  啟用: 是
  群組: Windows Management Instrumentation <WMI>
  LocalIP: 任一
  RemoteIP: 任一
> 規則名稱: Windows Management Instrumentation <ASync-In>
-----
  啟用: 是
  群組: Windows Management Instrumentation <WMI>
  LocalIP: 任一
  RemoteIP: 192.168.8.184/32
PS C:\>
```

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](#)

5.1 組織單位設定

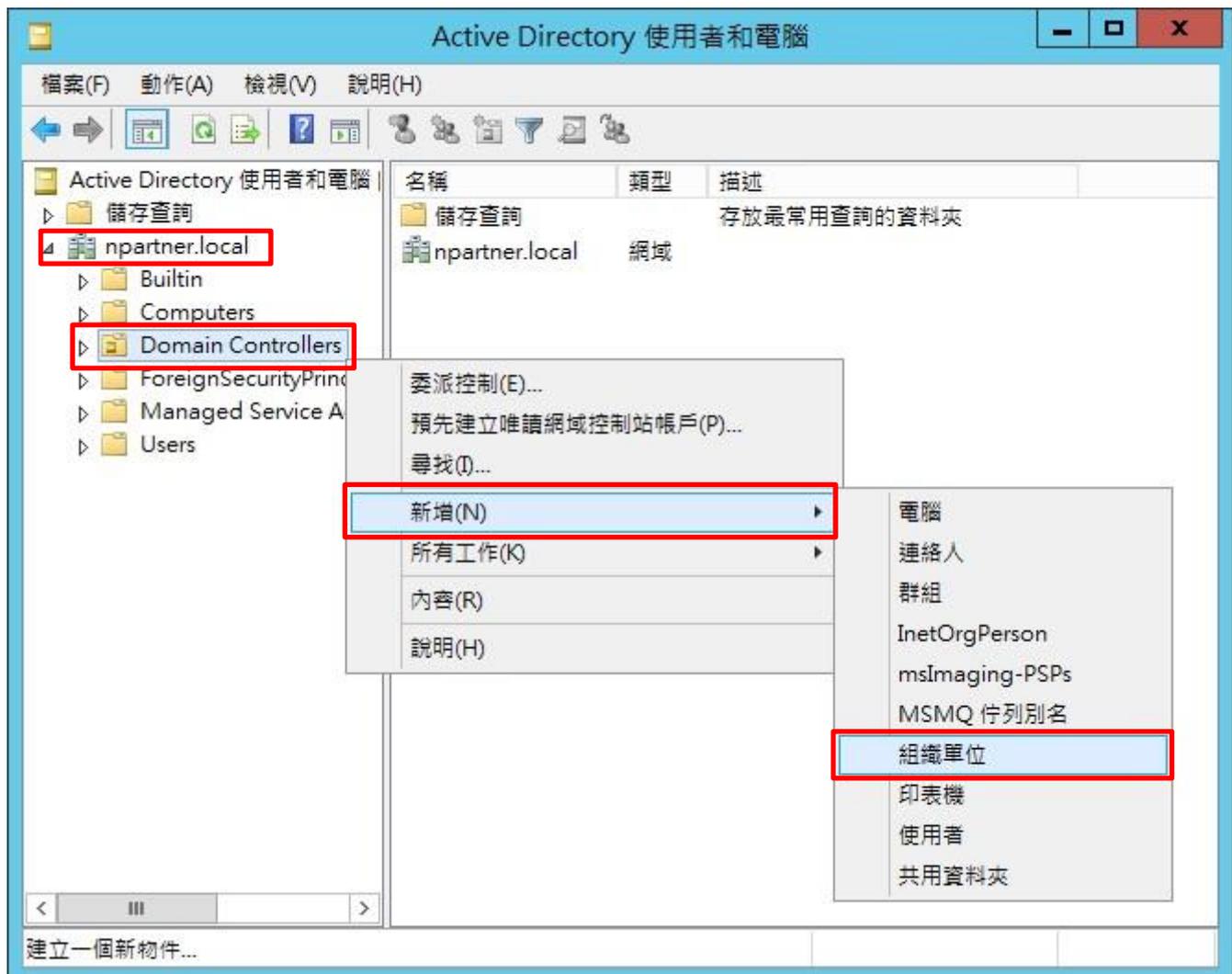
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 的 [Domain Controllers] 組織單位，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/Domain Controllers

名稱(A):
Servers

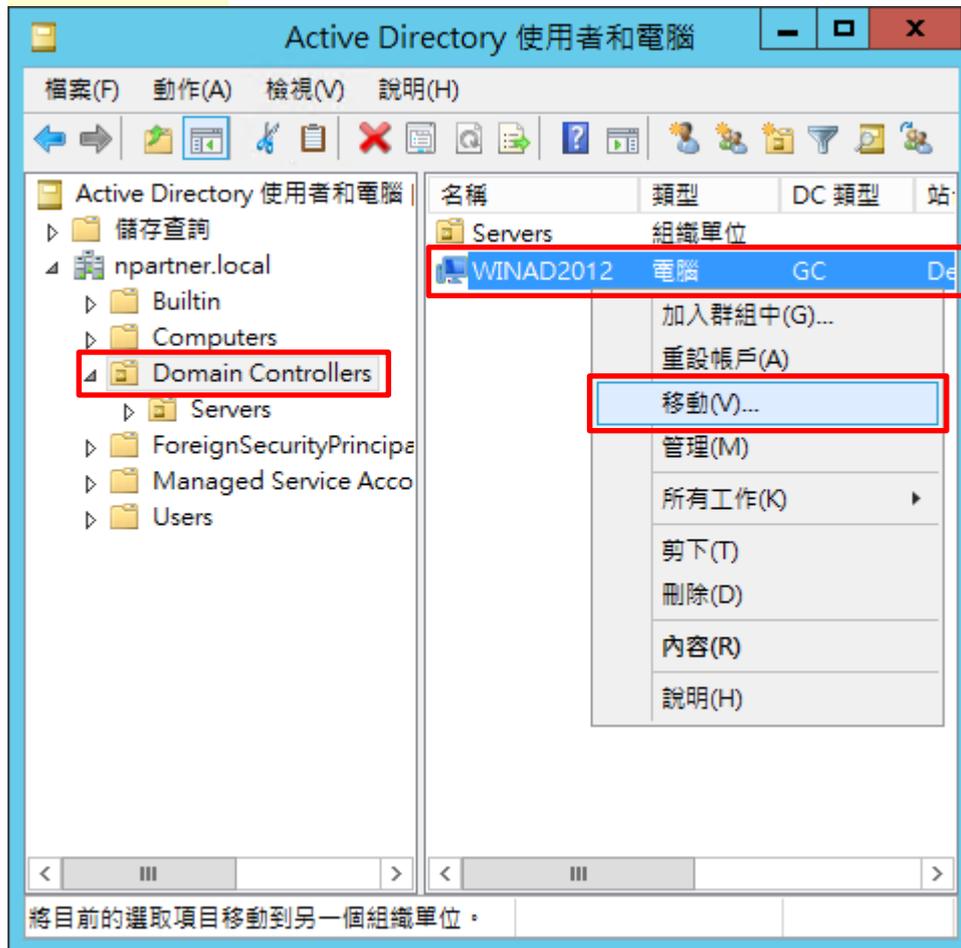
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

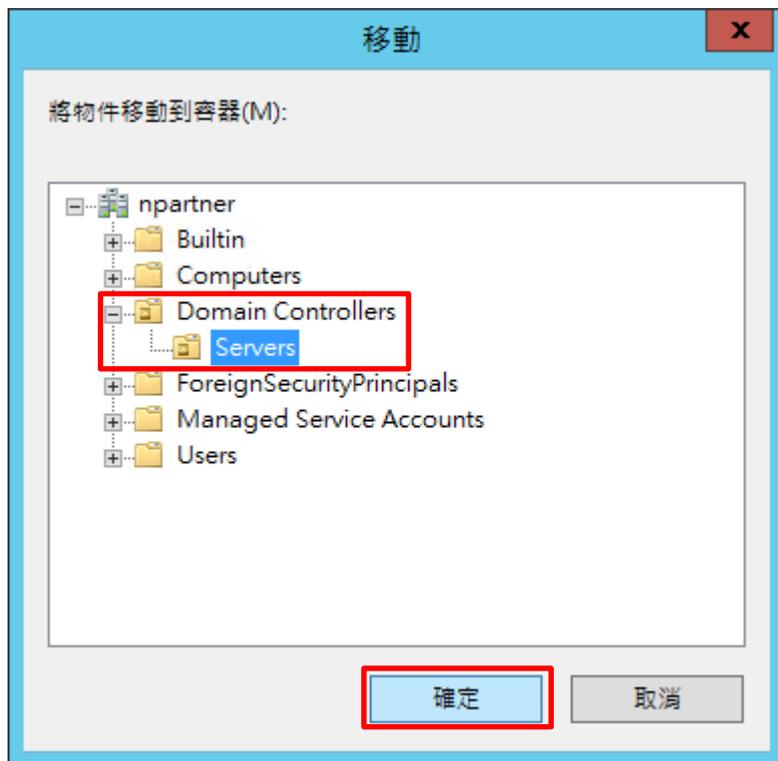
選擇 [Domain Controllers] 組織單位 -> 在 [WinAD2012] 網域伺服器，按滑鼠右鍵，註：請依客戶環境選擇

Windows AD 主機 -> 點選 [移動]



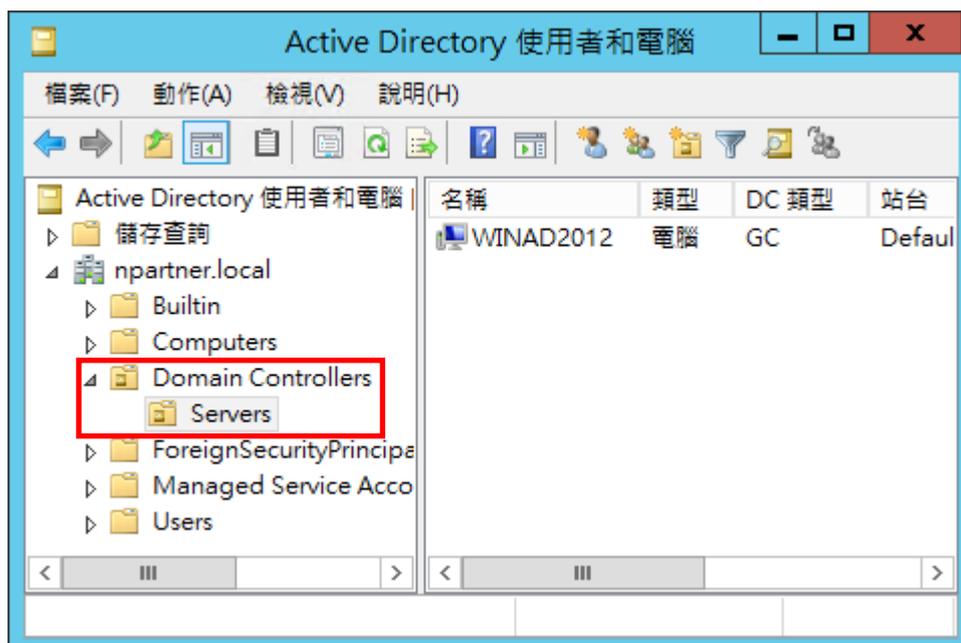
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [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 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2012] 網域伺服器已移動。



5.2 群組原則設定

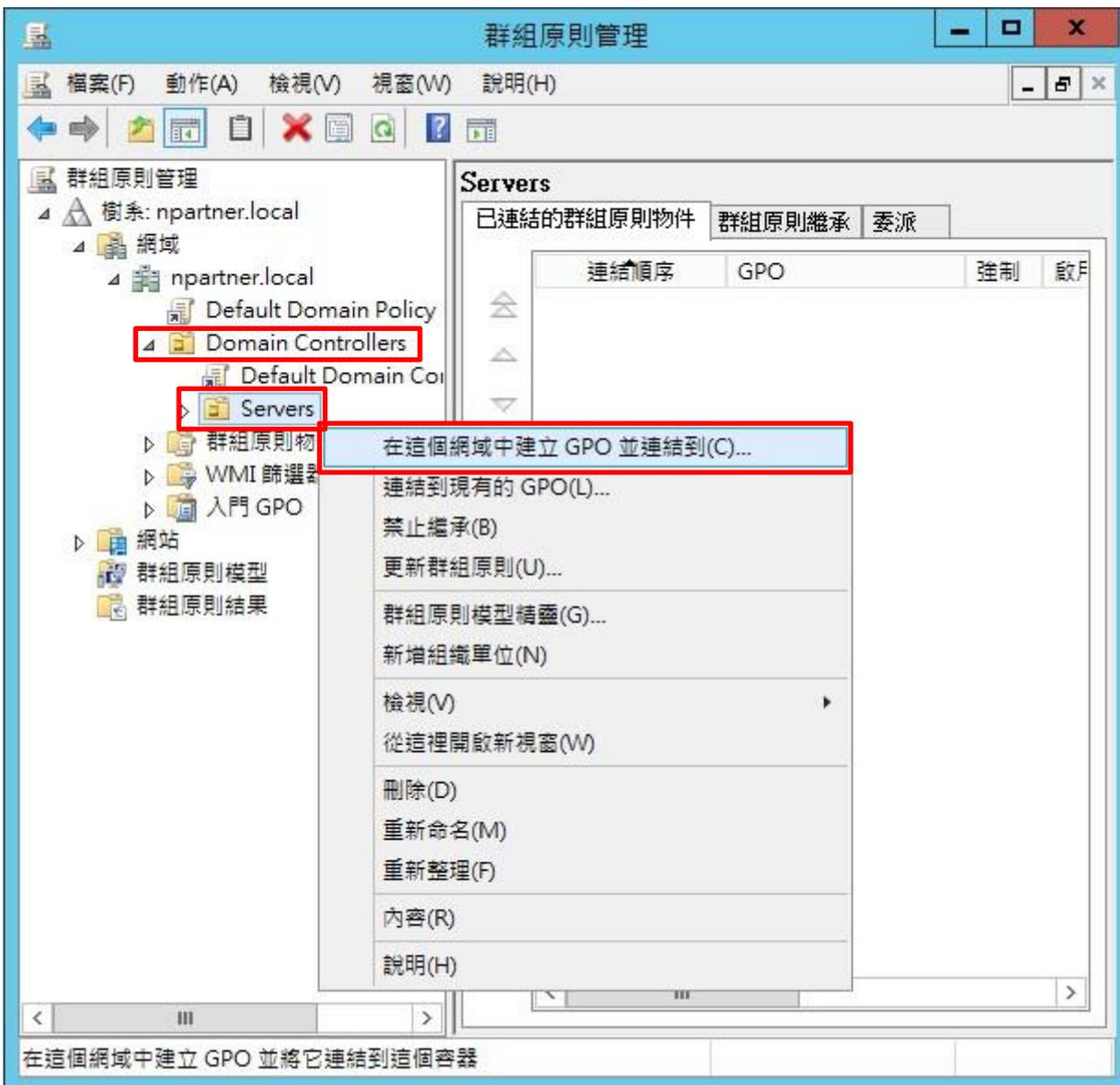
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [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...]



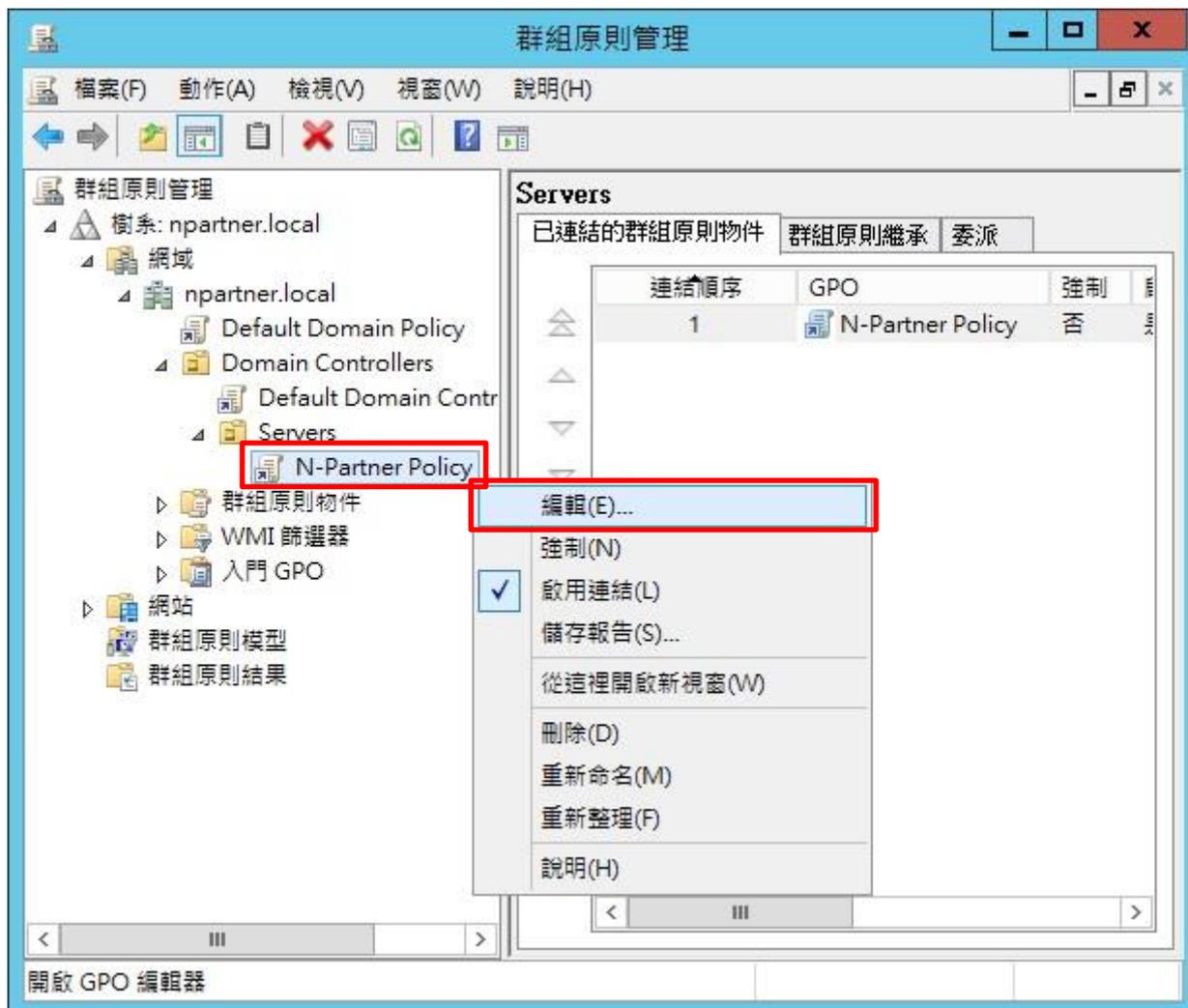
(3) 輸入群組原則物件名稱

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]



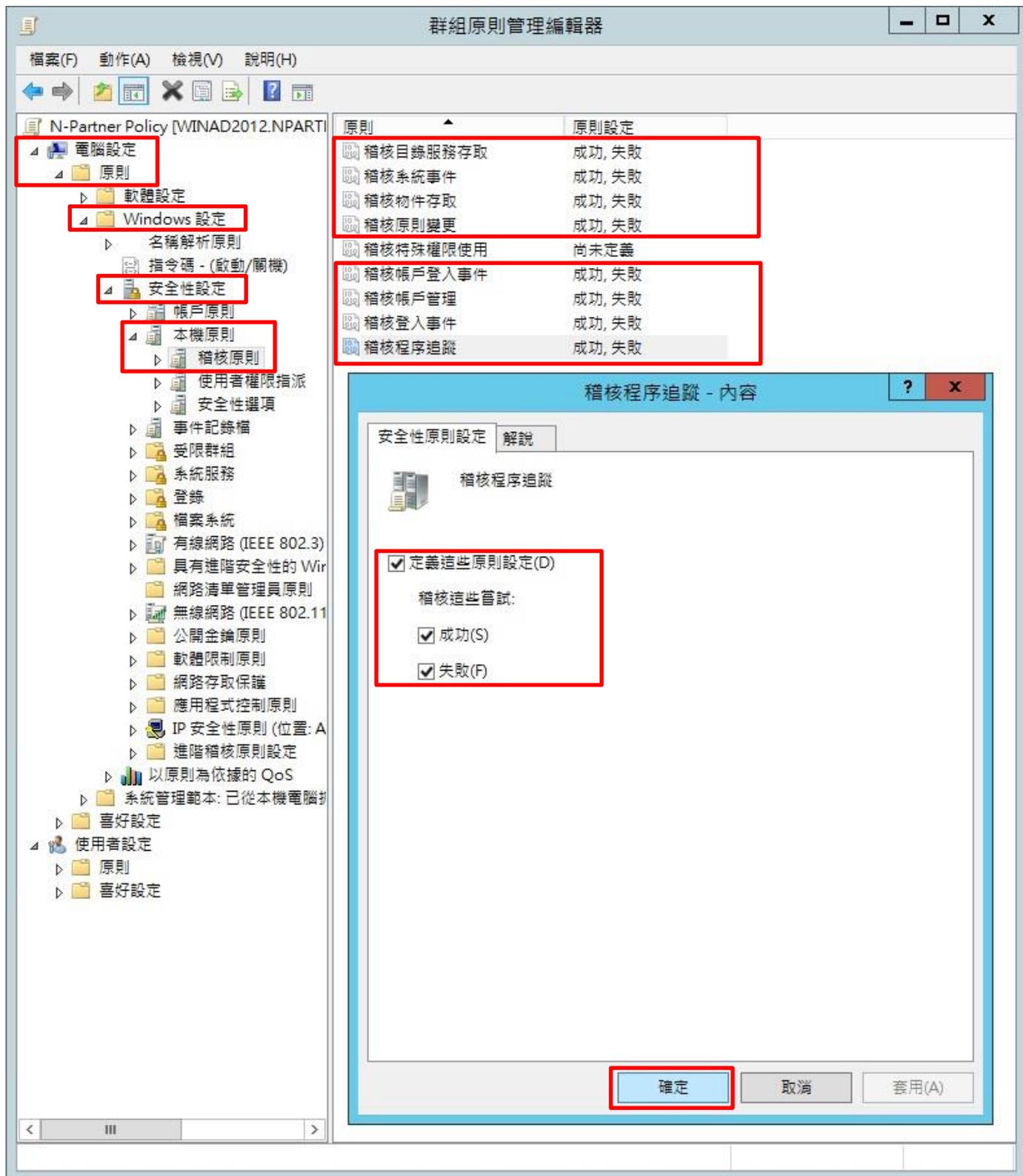
(4) 編輯群組原則物件

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 [稽核目錄服務存取], [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 '群組原則管理編輯器' (Group Policy Management Editor) window. The left pane shows the tree structure with '電腦設定' (Computer Configuration) expanded to '事件記錄檔' (Event Log). The right pane shows a list of policies, with '安全性記錄檔大小最大值' (Maximum Security Log File Size) selected and its value set to 204800 KB. A dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum Security Log File Size - Content) is open, showing the '安全性原則設定' (Policy Settings) tab. The checkbox '定義這個原則設定(D)' (Define this policy setting) is checked, and the value '204800 KB' is entered in the text box. A warning message is displayed below the input field. The '確定' (OK) button is highlighted with a red box.

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

安全性記錄檔大小最大值 - 內容

安全性原則設定 解說

安全性記錄檔大小最大值

定義這個原則設定(D)

204800 KB

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)

確定 取消 套用(A)

(7) 事件記錄檔：安全性記錄檔保持方法

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

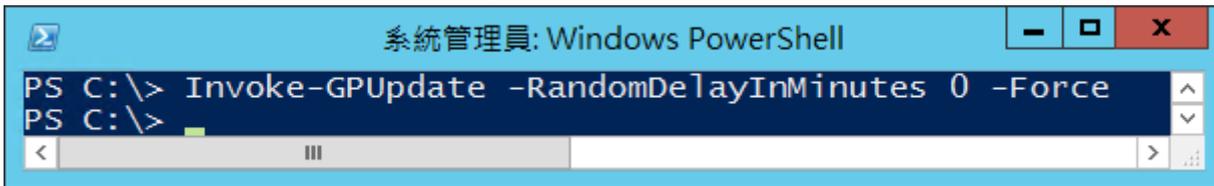


(8) 開啟 [Windows PowerShell]



(9) 更新群組原則

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



(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer WinAD2012 -Path C:\tmp\WinAD2012.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表，確認 Windows AD 2012 伺服器，套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WINAD2012
資料收集: 30/6/2021 11:13:19 顯示全部

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

帳戶原則/Kerberos 原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
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/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

5.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

```
PS C:\> Get-ADUser -Filter 'Name -like "*KH"' -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```

```

系統管理員: Windows PowerShell
PS C:\> Get-ADUser -Filter 'Name -like "*KH"' -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber

DisplayName           : KH
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department            : TAC
EmployeeID            : 0032
EmployeeNumber        : A0032
  
```

紅色文字部位請依客戶環境輸入使用者名稱

(2) N-Reporter [事件查詢] -> 點選 使用者名稱

等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh	4724	Administrator	User Management

(3) 顯示使用者資料

事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh (KH, TAC, 0032, (Engineer))	4724	Administrator	User Management

5.3.1 新增非管理帳號

(1) 開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

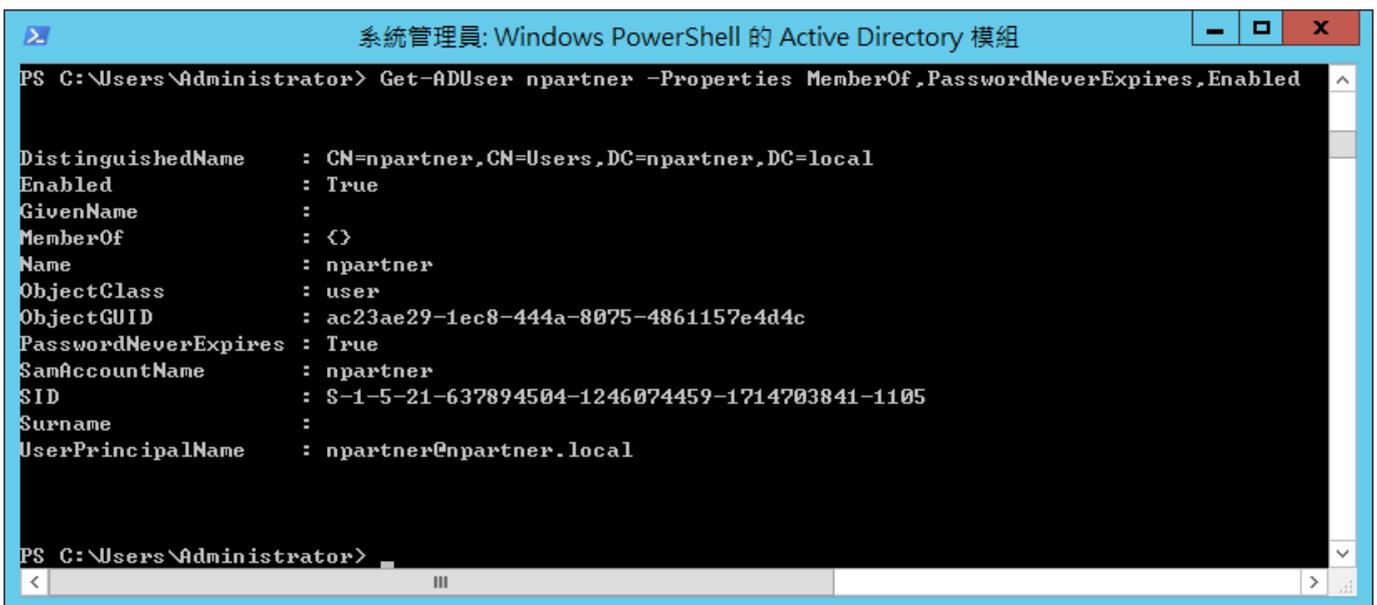
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```



紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```



```
DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                : True
GivenName              :
MemberOf               : {}
Name                   : npartner
ObjectClass             : user
ObjectGUID             : ac23ae29-1ec8-444a-8075-4861157e4d4c
PasswordNeverExpires   : True
SamAccountName         : npartner
SID                    : S-1-5-21-637894504-1246074459-1714703841-1105
Surname                :
UserPrincipalName      : npartner@npartner.local

PS C:\Users\Administrator>
```

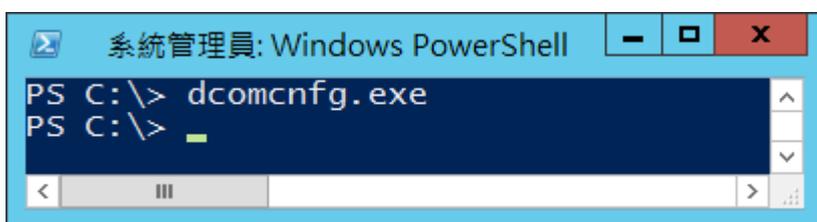
5.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



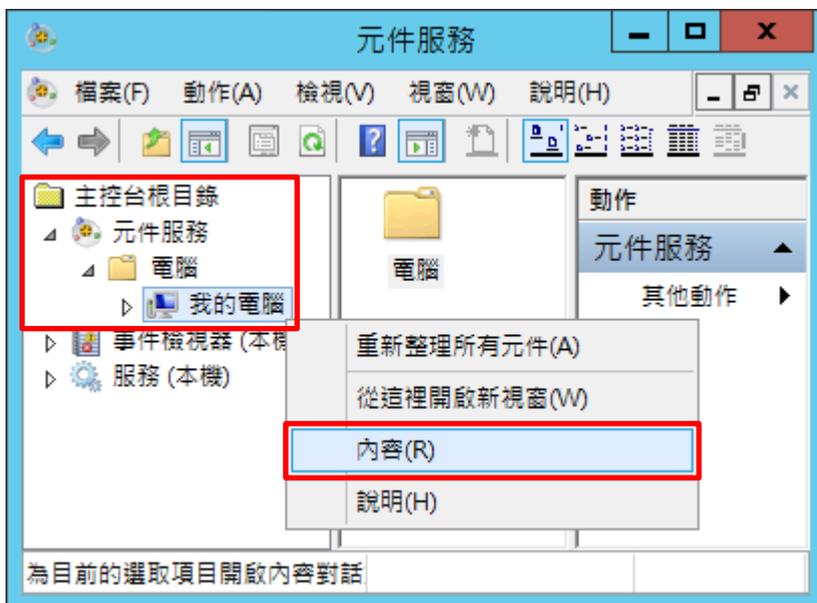
(2) 開啟元件服務

PS C:\> dcomcnfg.exe



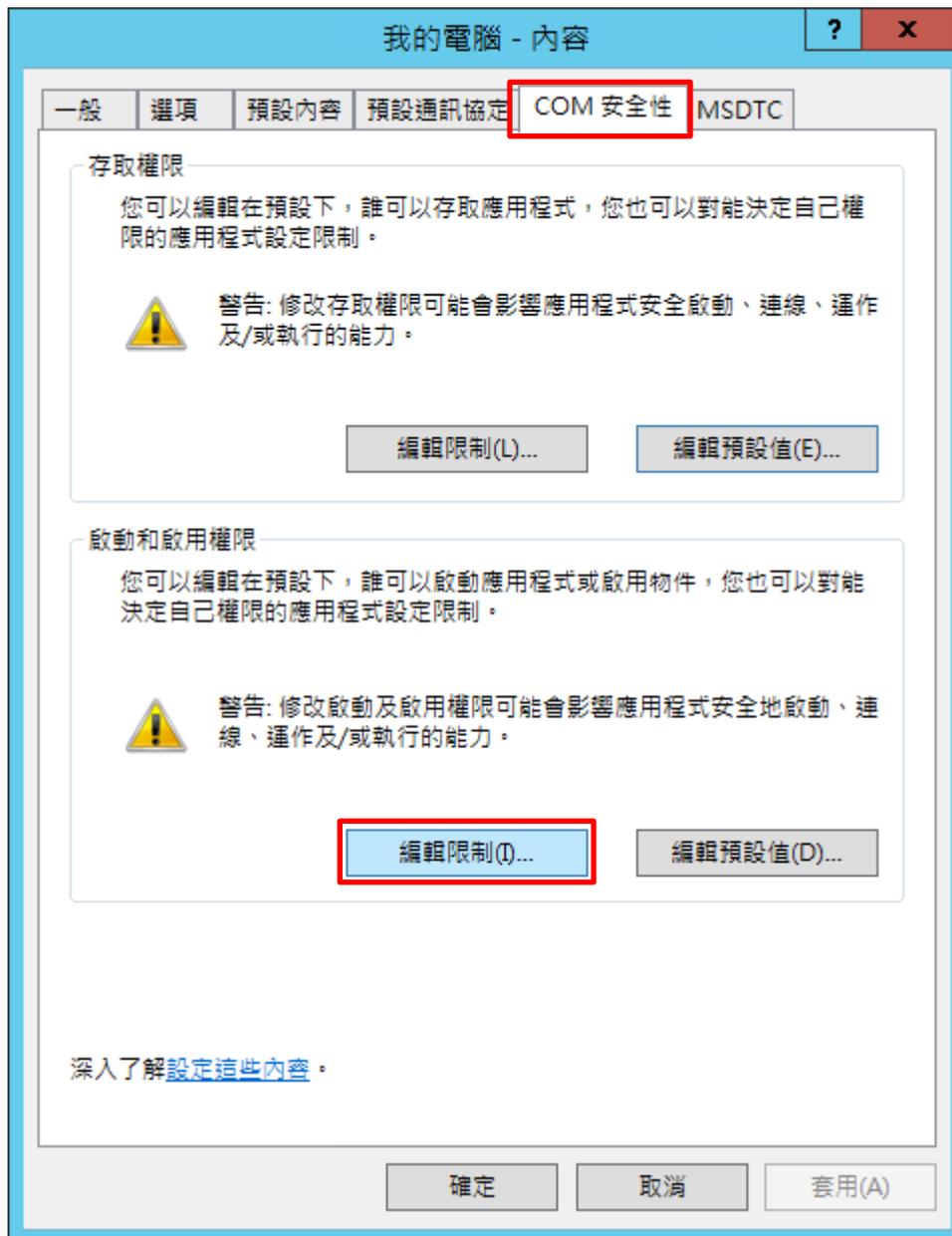
(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



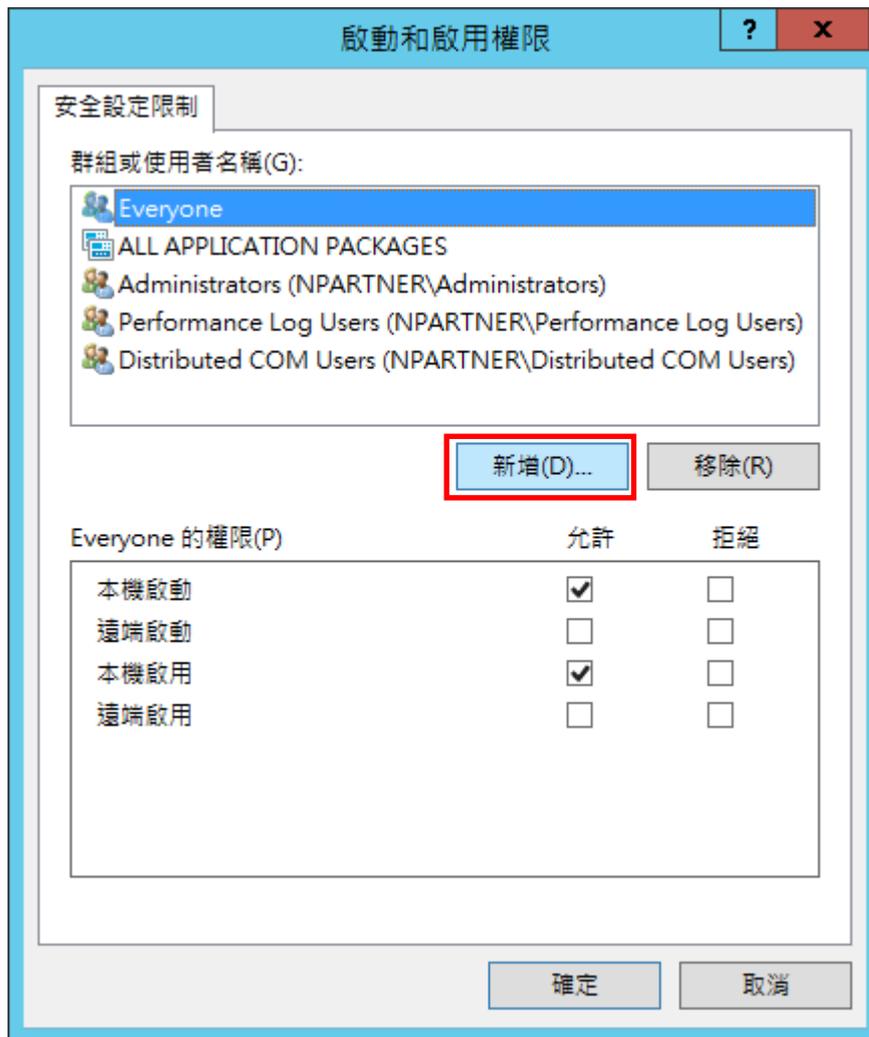
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



(5) 新增 DCOM 使用者權限

點選 [新增]



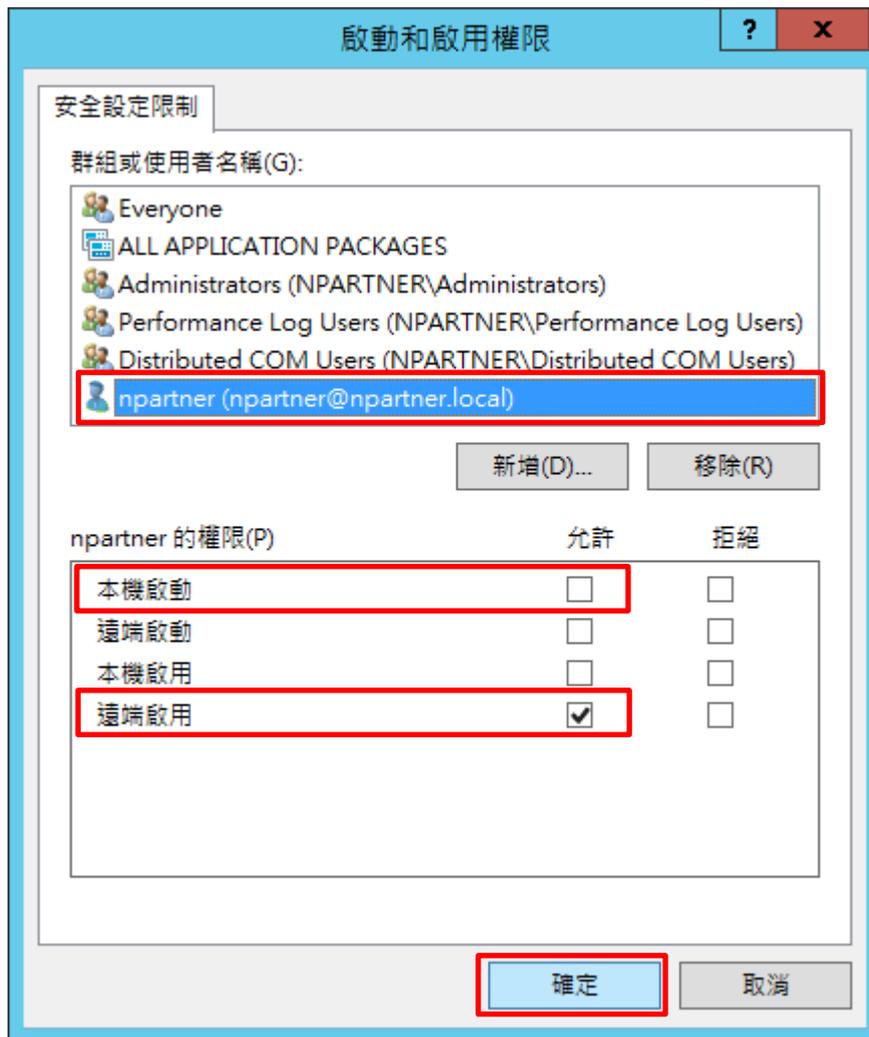
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



5.3.3 設定 WMI 權限

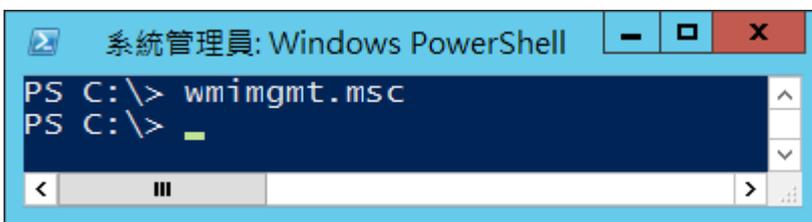
5.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



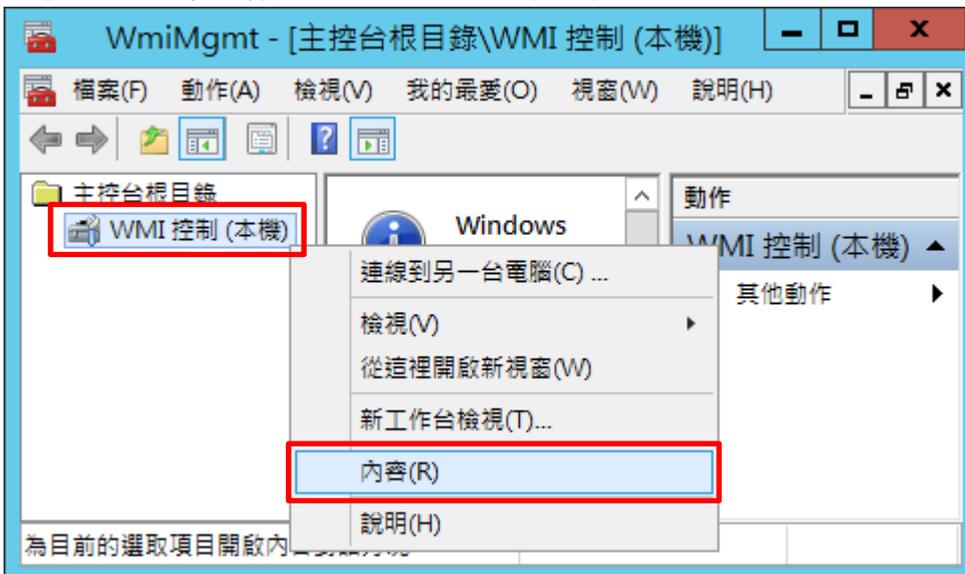
(2) 開啟元件服務

PS C:\> wmicgmt.msc



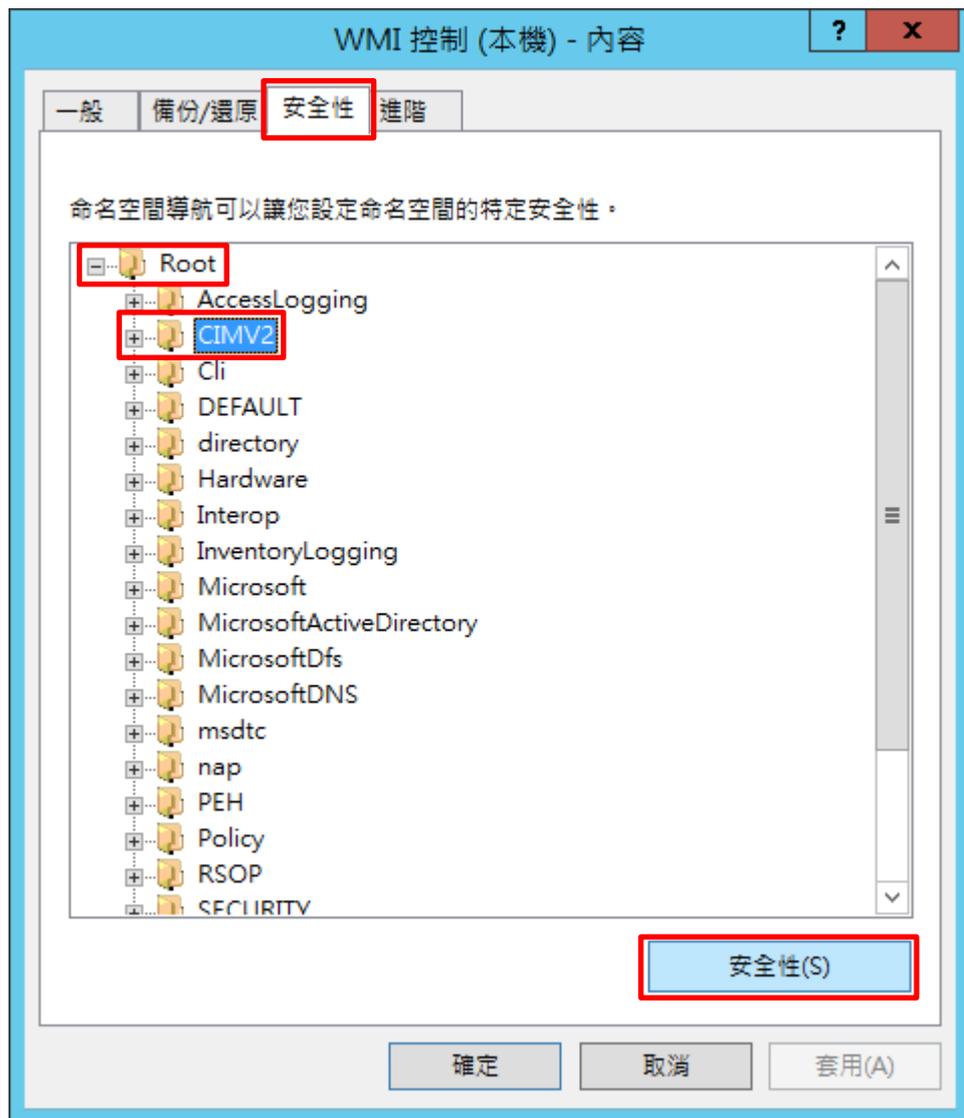
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



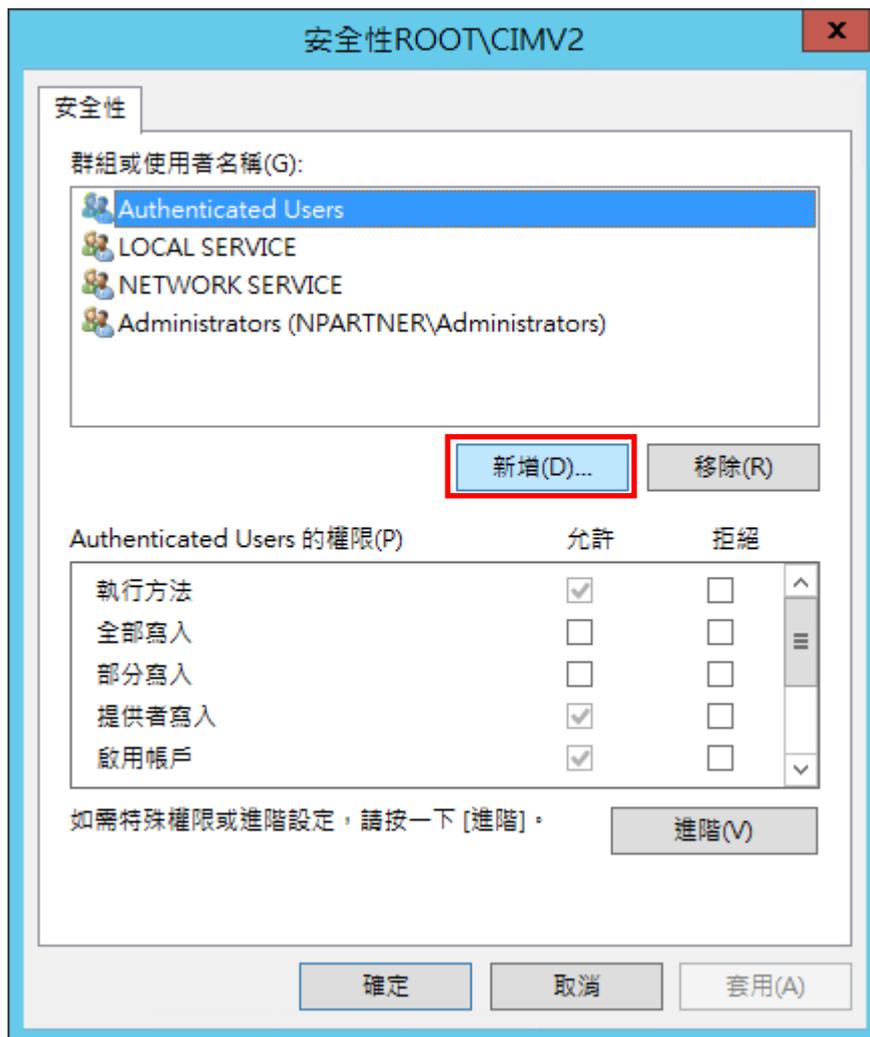
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



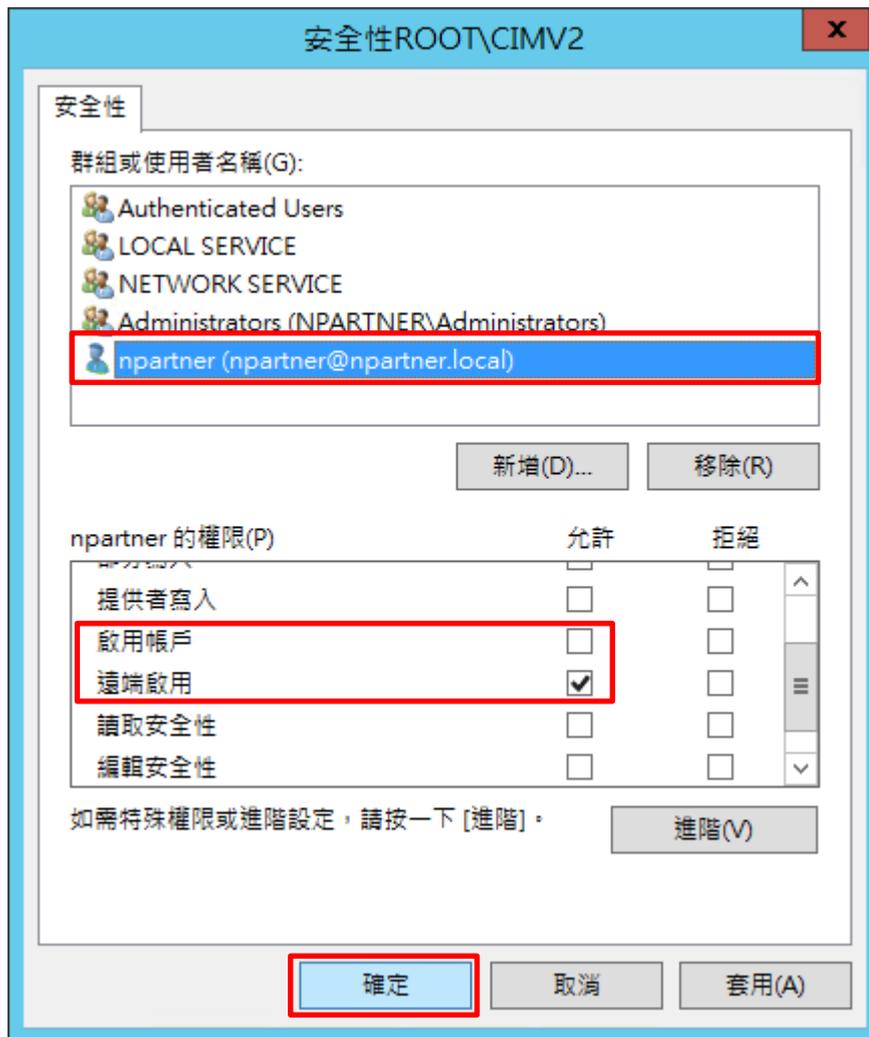
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

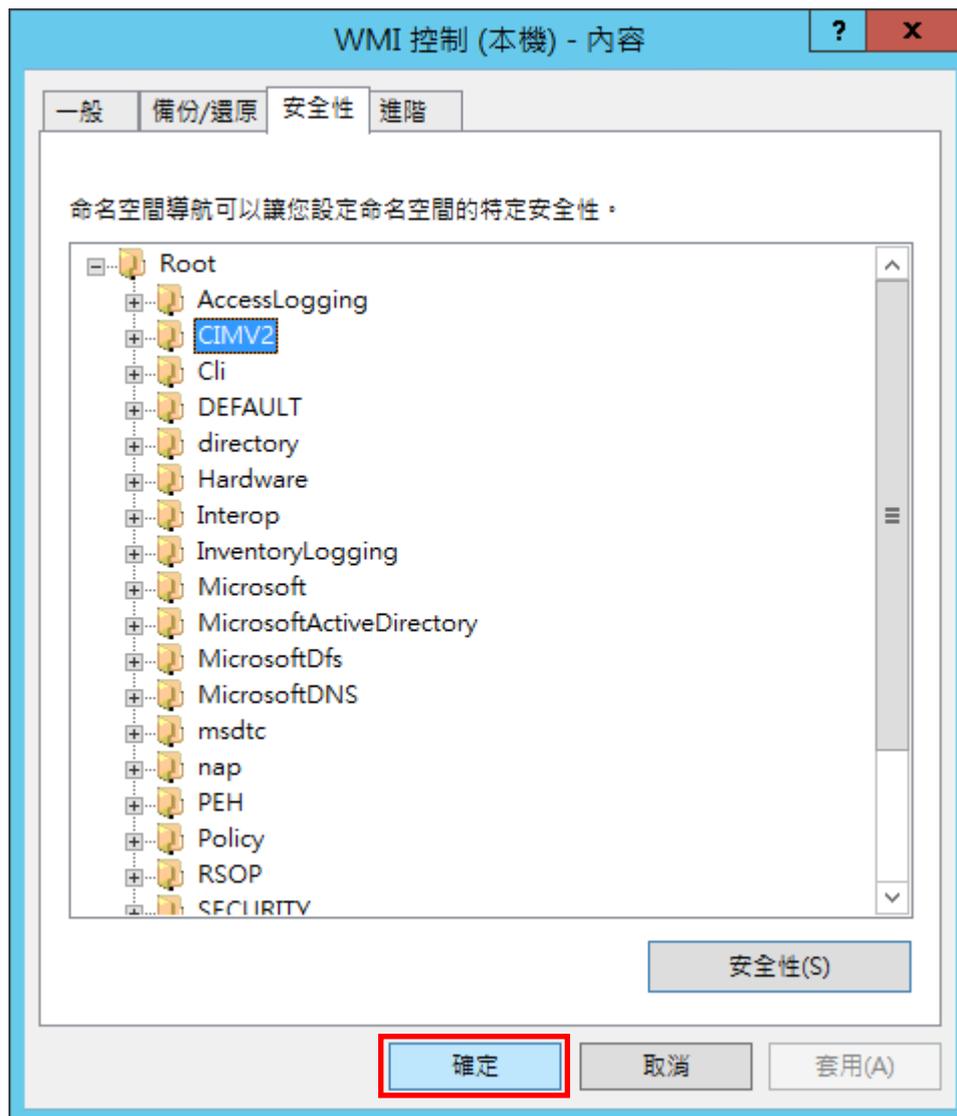


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



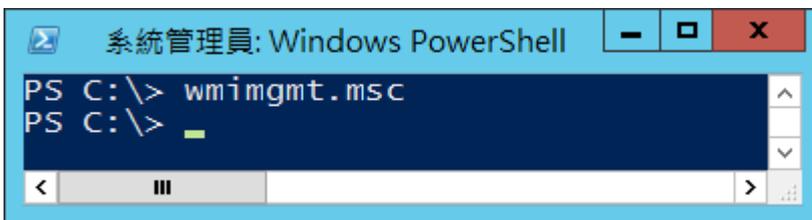
5.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



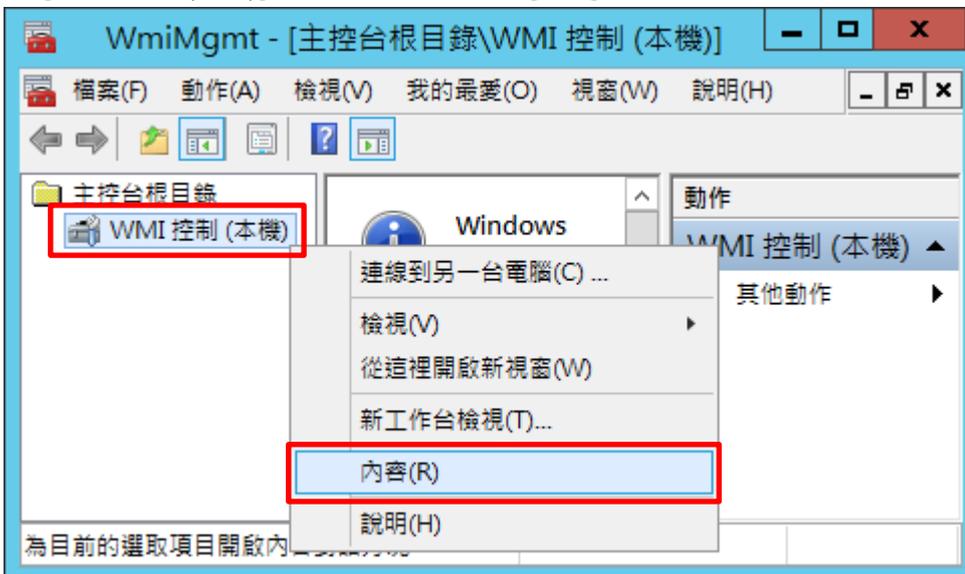
(2) 開啟元件服務

PS C:\> wimgmt.msc



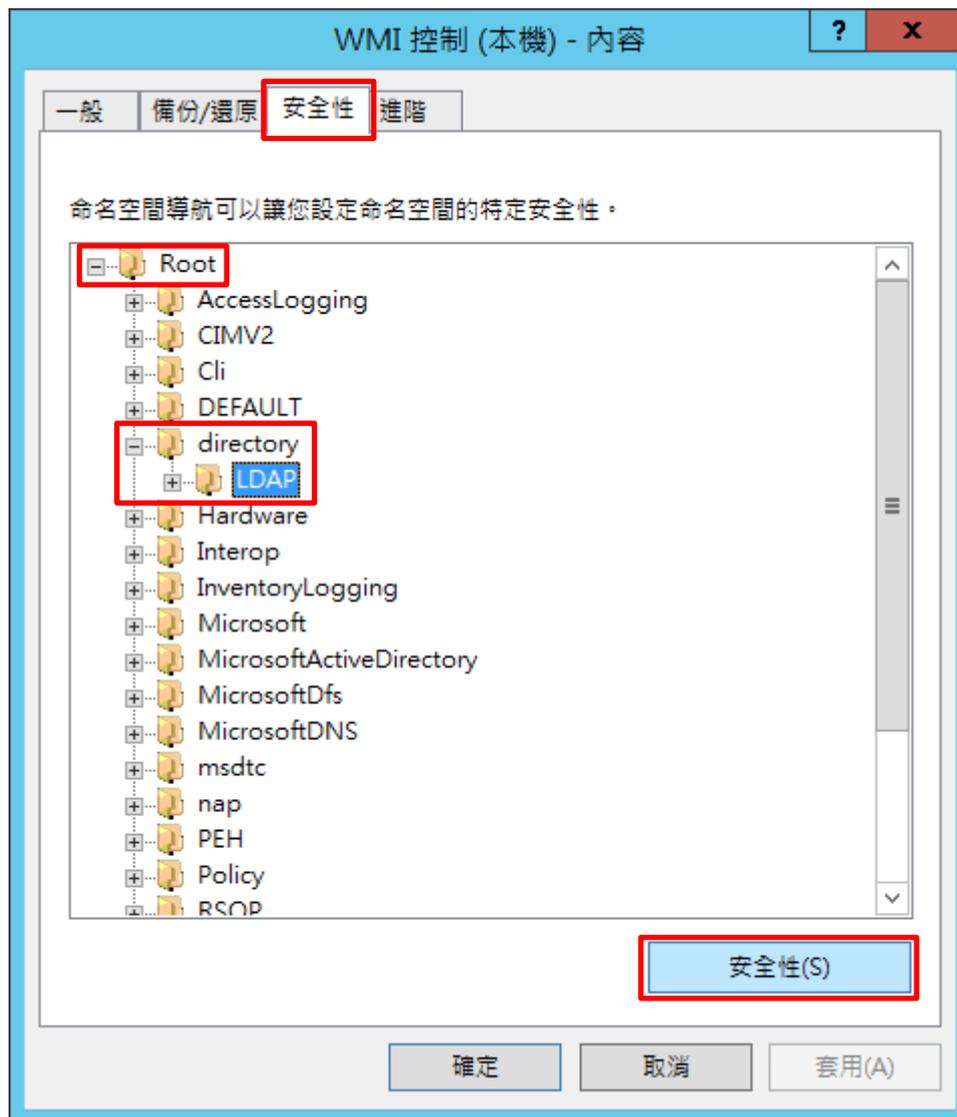
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



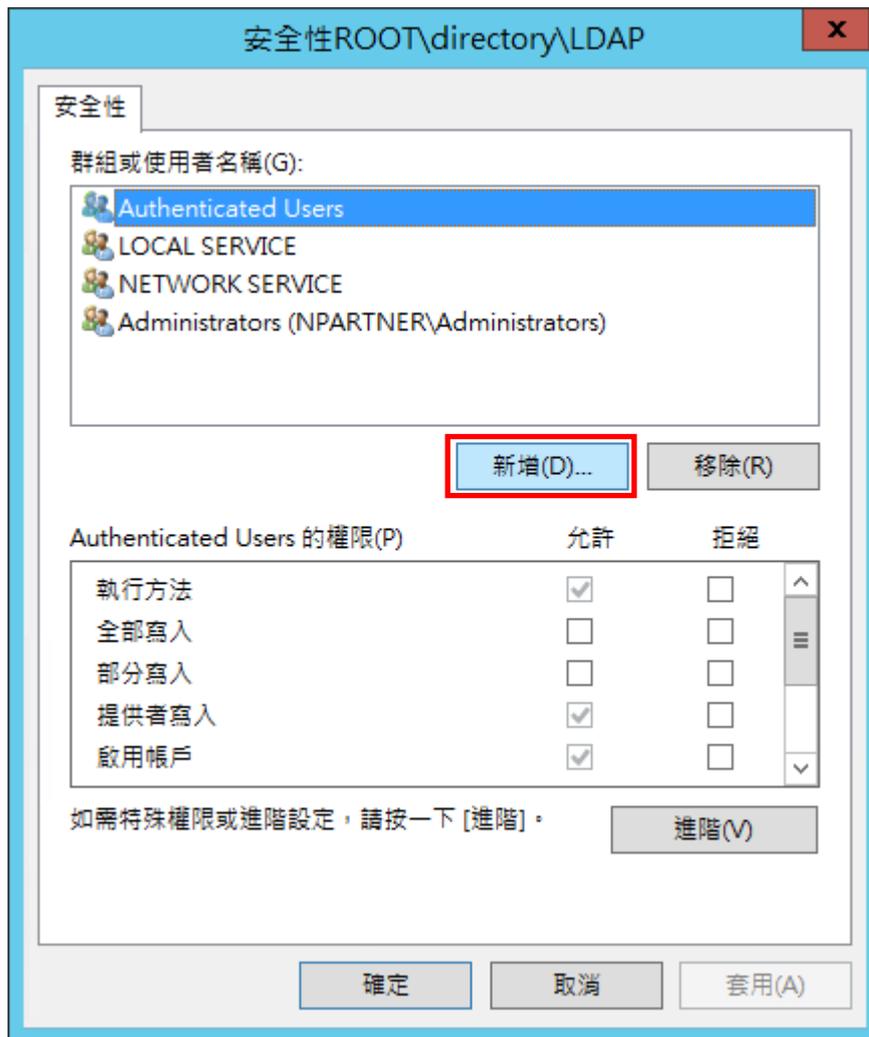
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



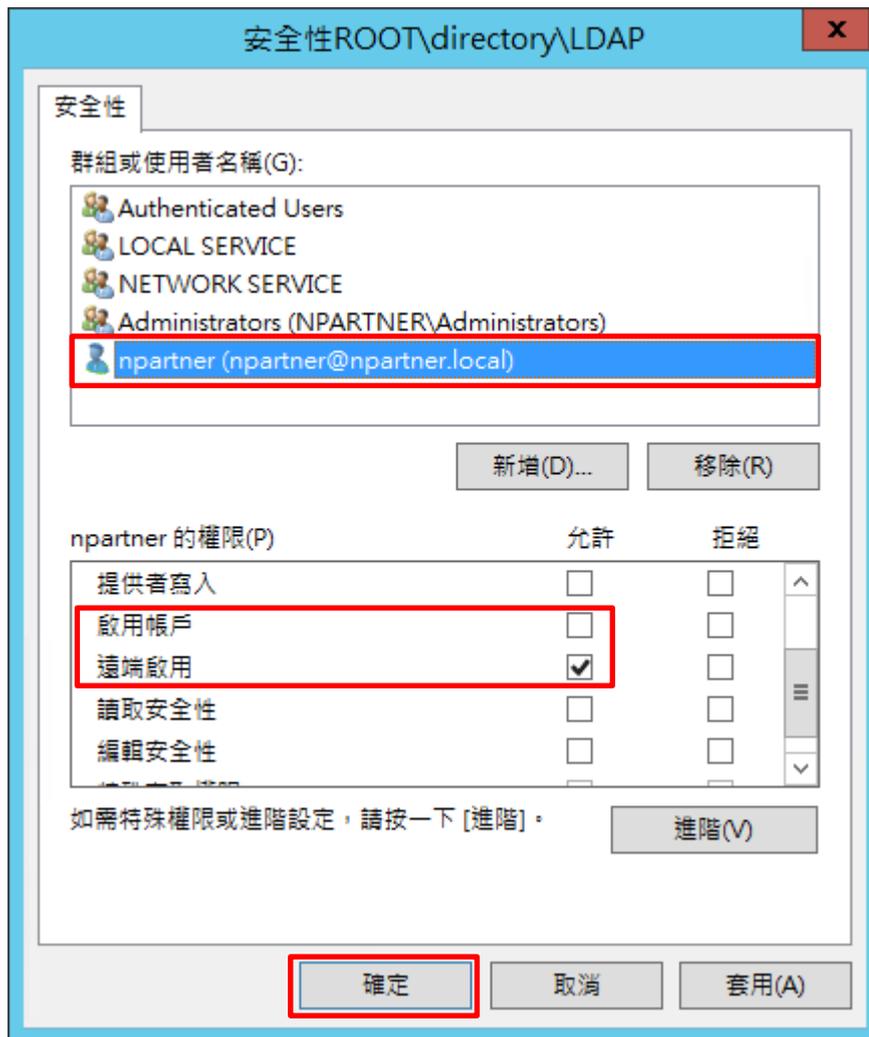
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

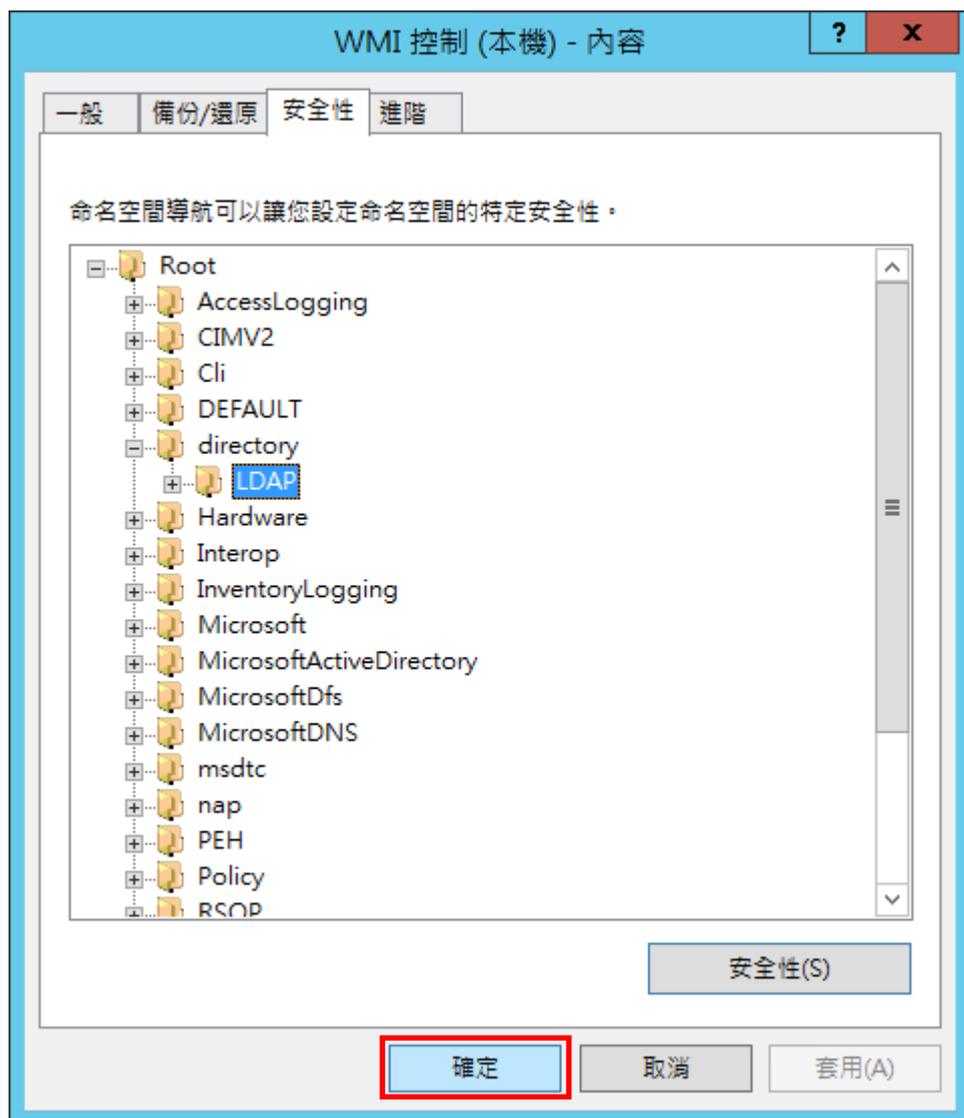


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



5.3.4 設定 Event log 讀取權限

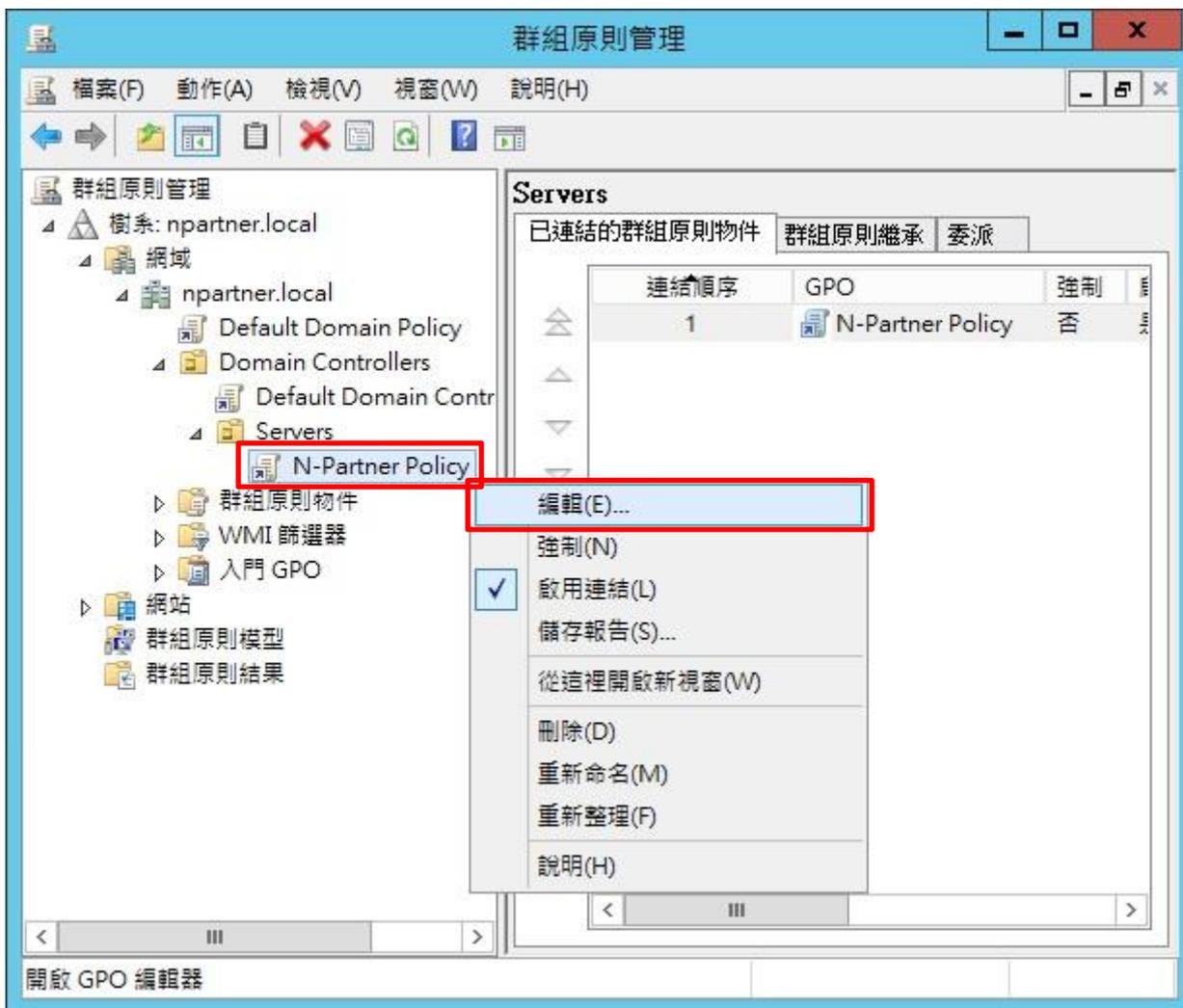
(1) 開啟群組原則管理

開啟 [群組原則管理]



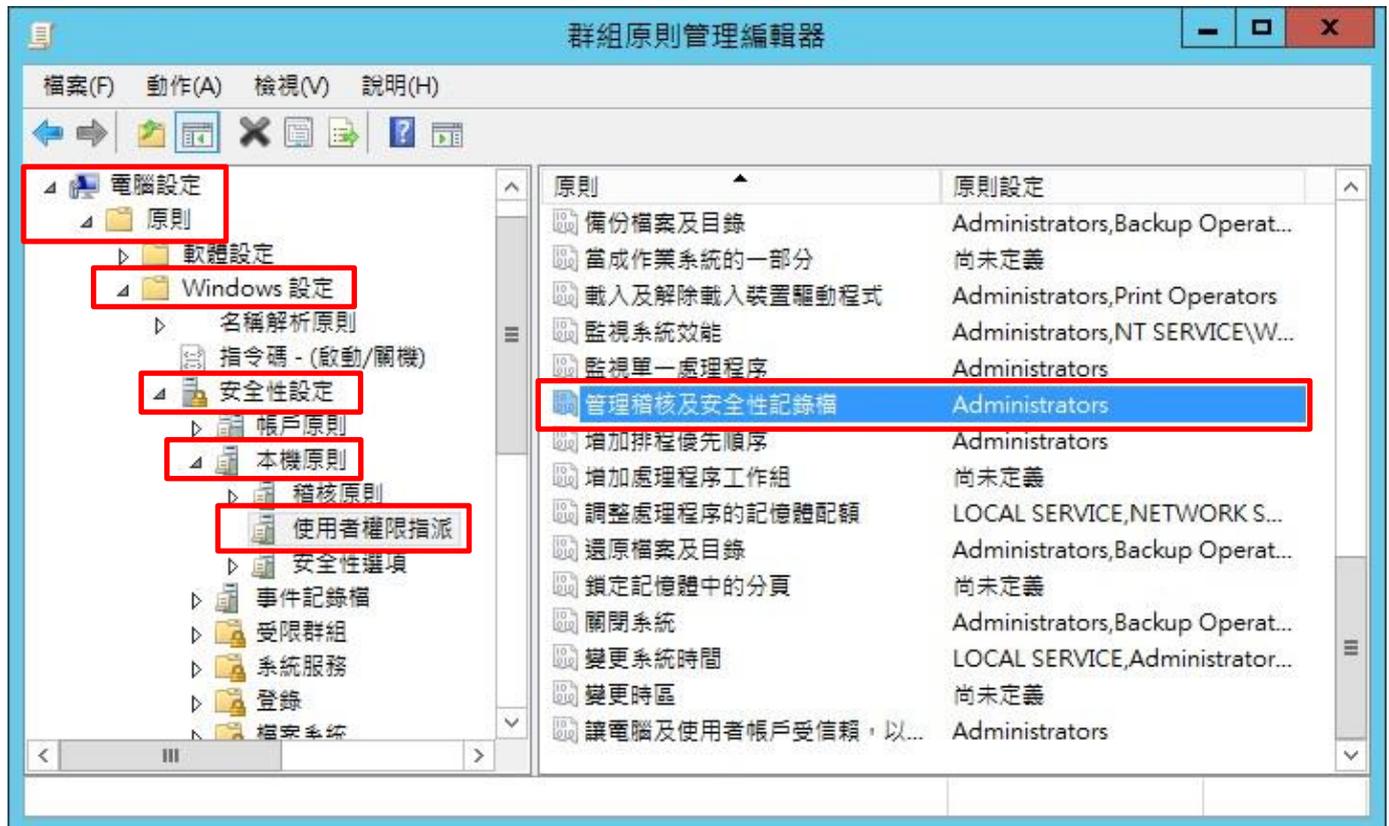
(2) 編輯群組原則物件

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



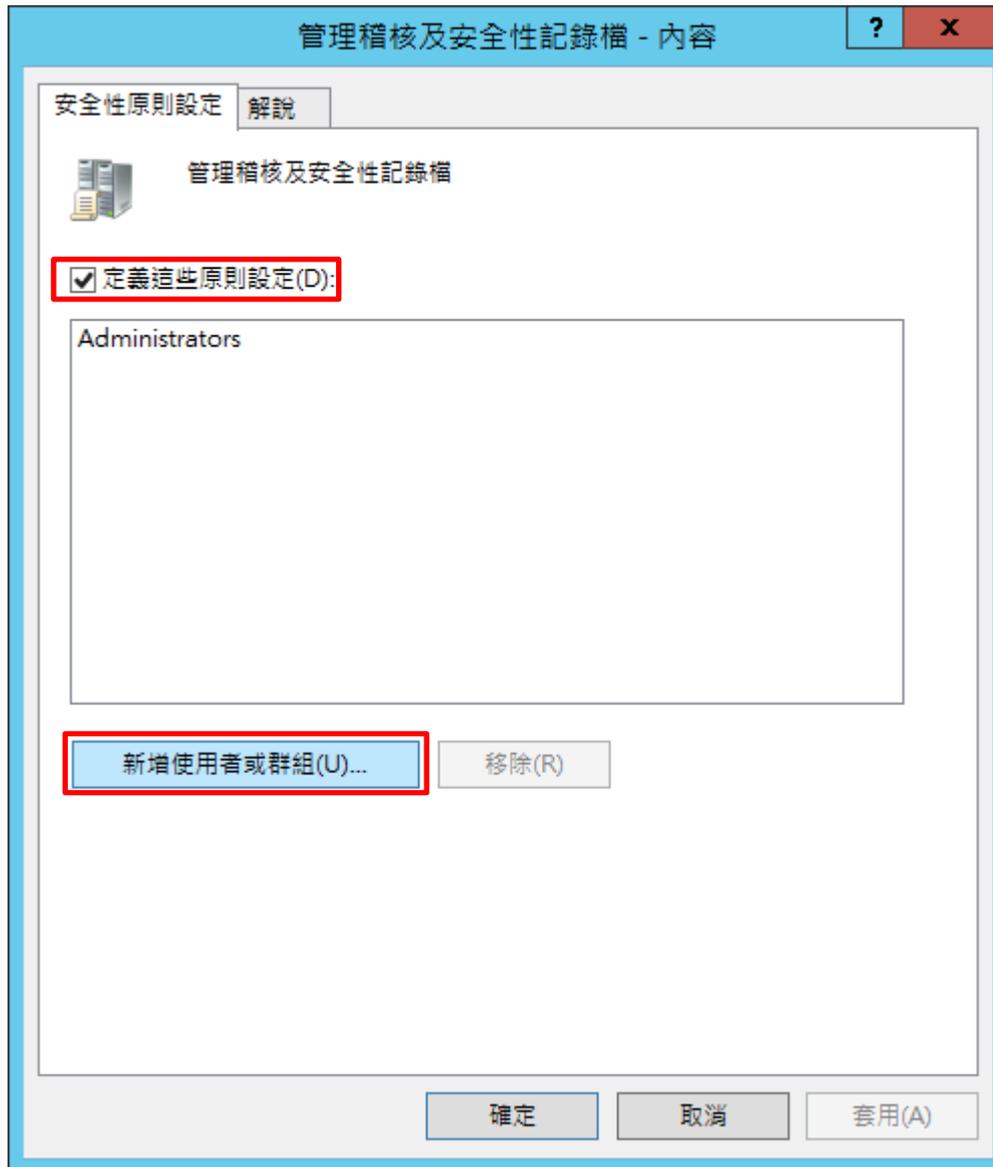
(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 選擇 [管理稽核及安全性記錄檔] 項目



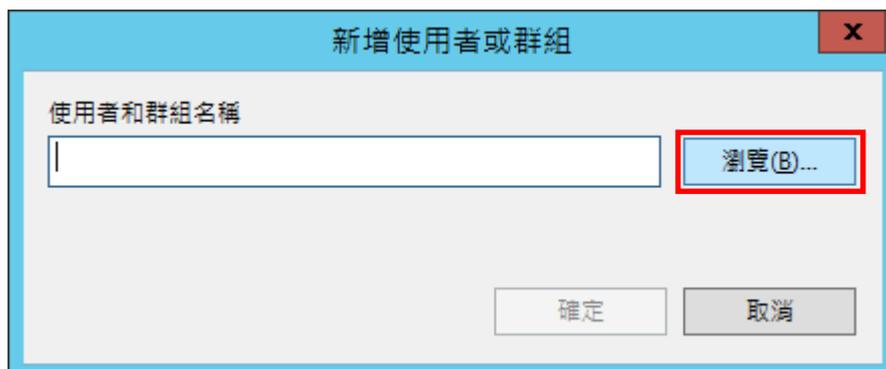
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、群組或內建安全性主體 物件類型(O)...

從這個位置(F):
npartner.local 位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local) 檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

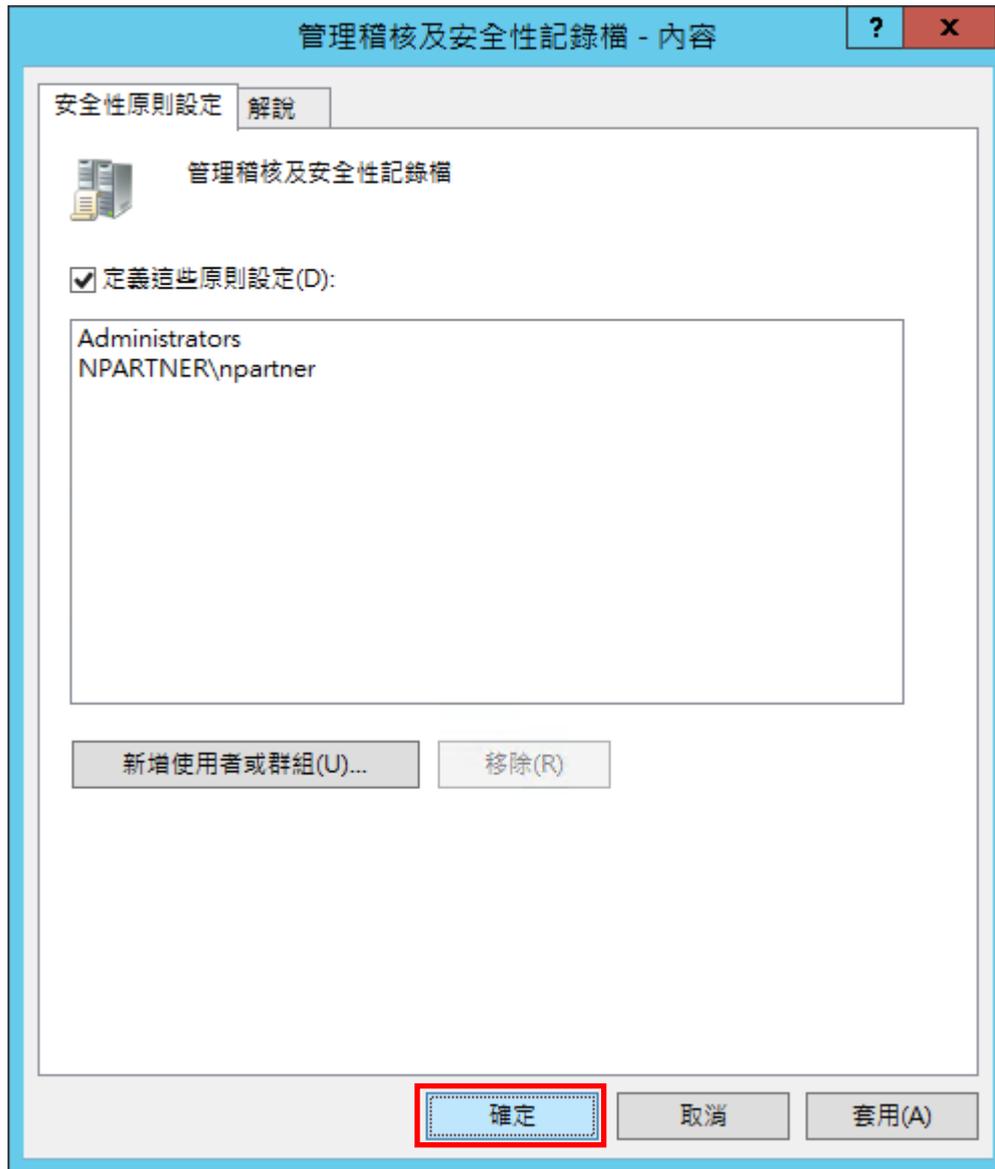
新增使用者或群組

使用者和群組名稱
NPARTNER\partner 瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]

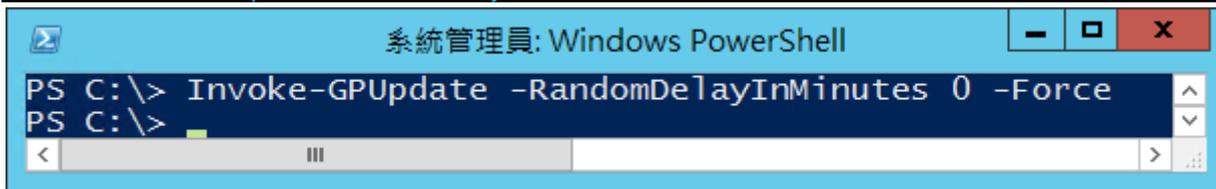


(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force



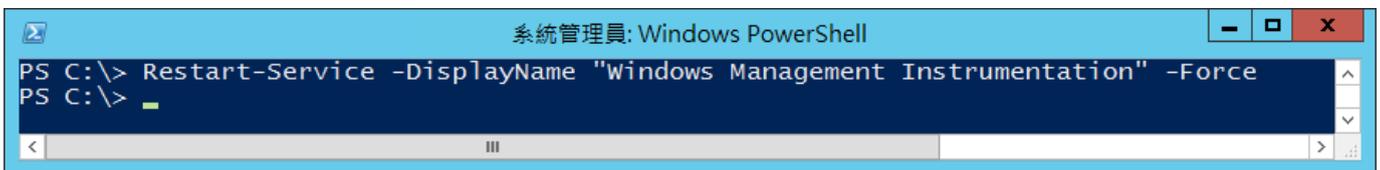
5.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



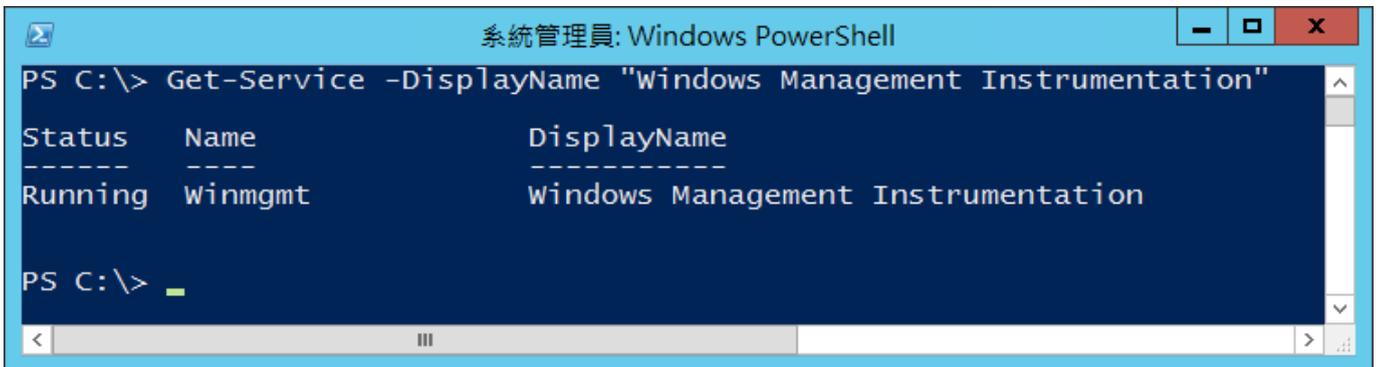
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



5.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



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](#)

6.1 組織單位設定

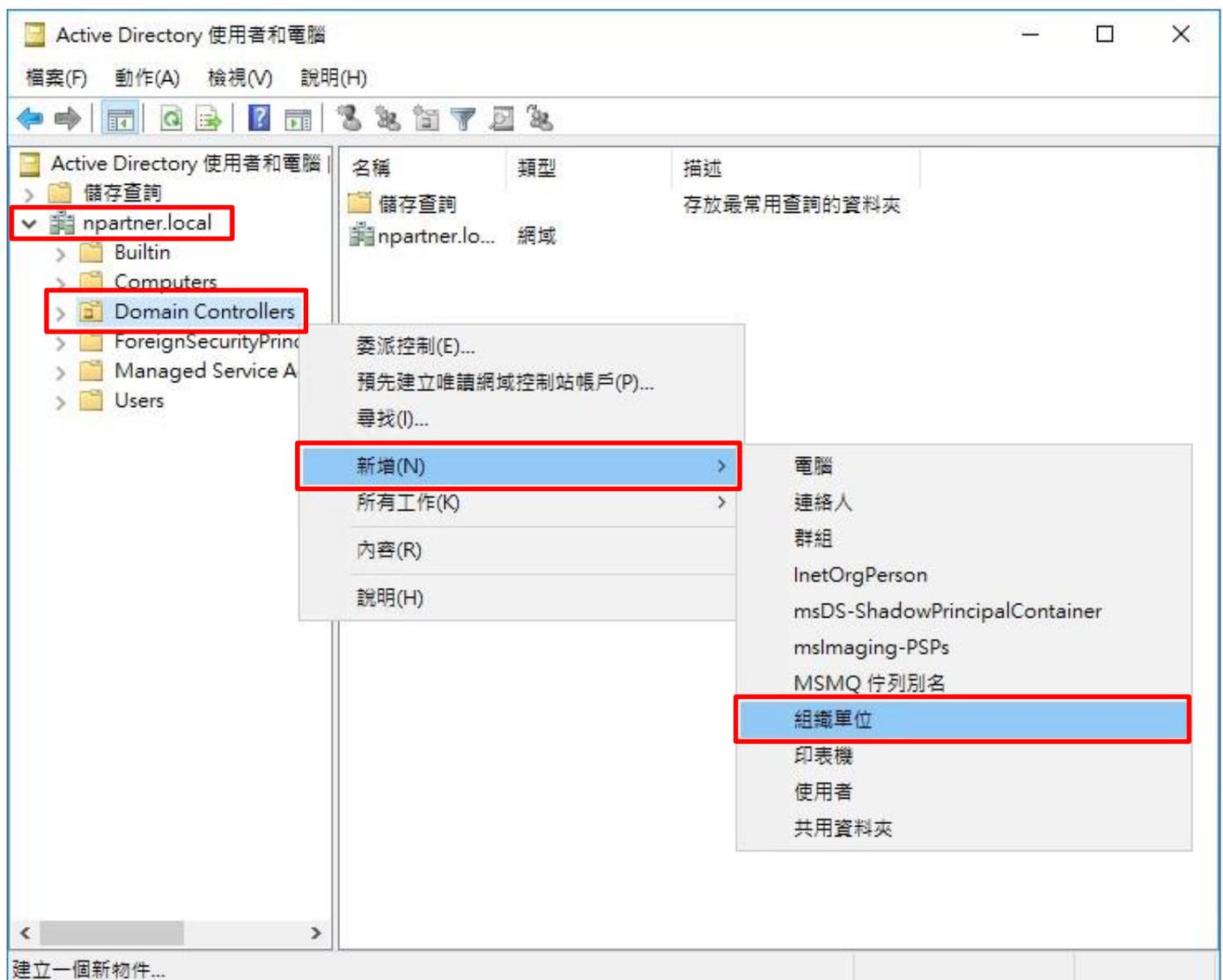
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 的 [Domain Controllers] 組織單位，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/Domain Controllers

名稱(A):
Servers

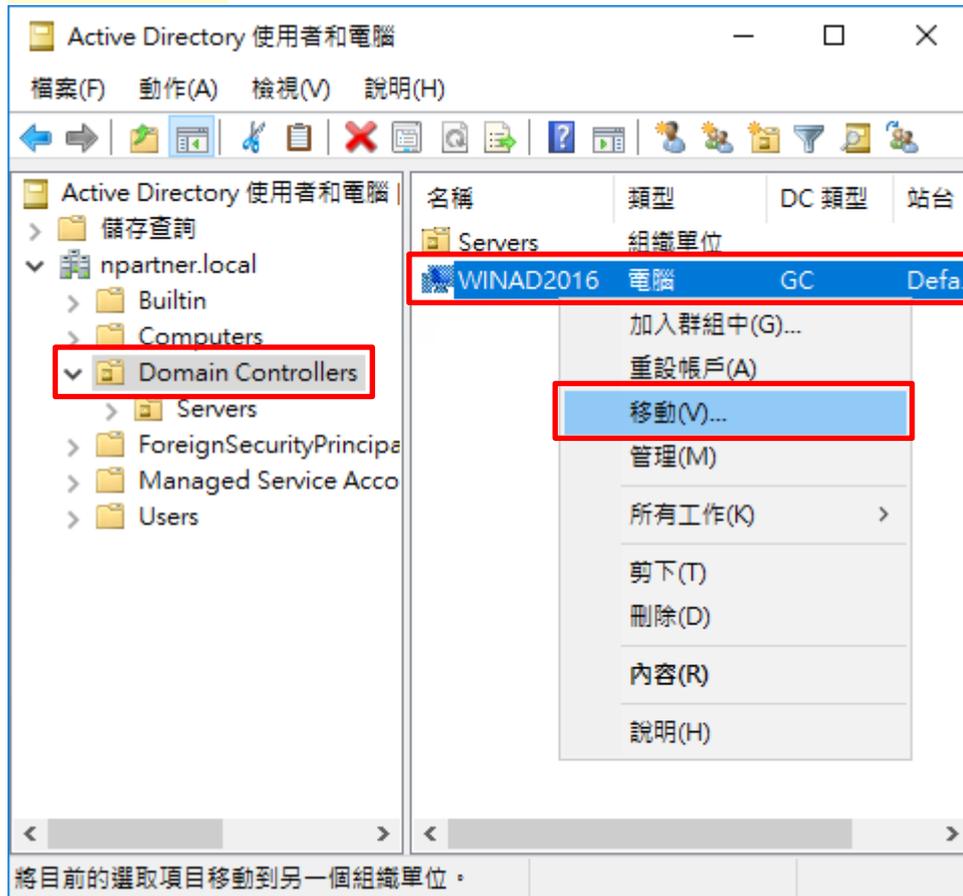
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

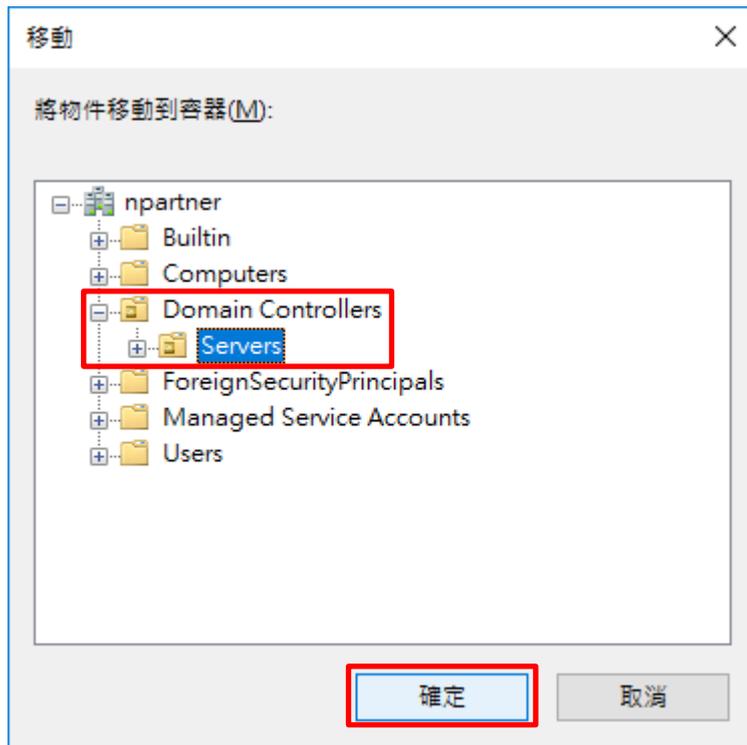
選擇 [Domain Controllers] 組織單位 -> 在 [WinAD2016] 網域伺服器，按滑鼠右鍵，註：請依客戶環境選擇

Windows AD 主機 -> 點選 [移動]



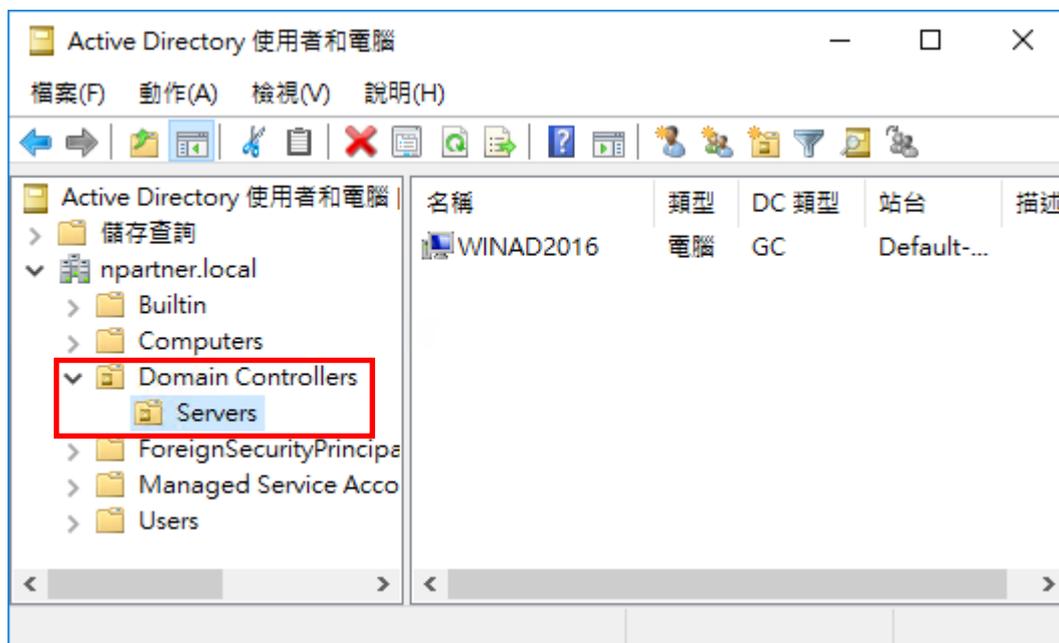
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [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 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2016] 網域伺服器已移動。



6.2 群組原則設定

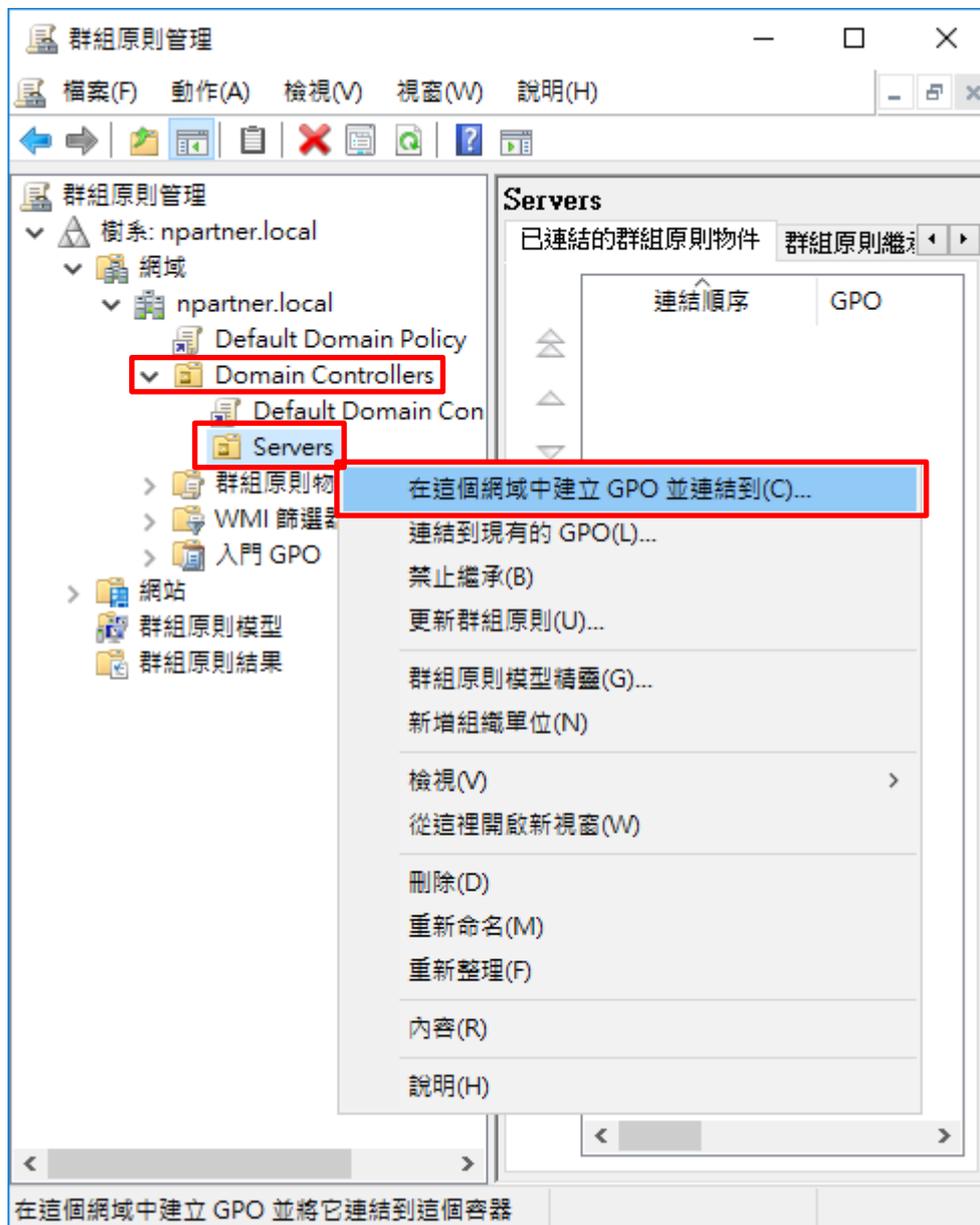
(1) 開啟群組原則管理

開啟 [群組原則管理]



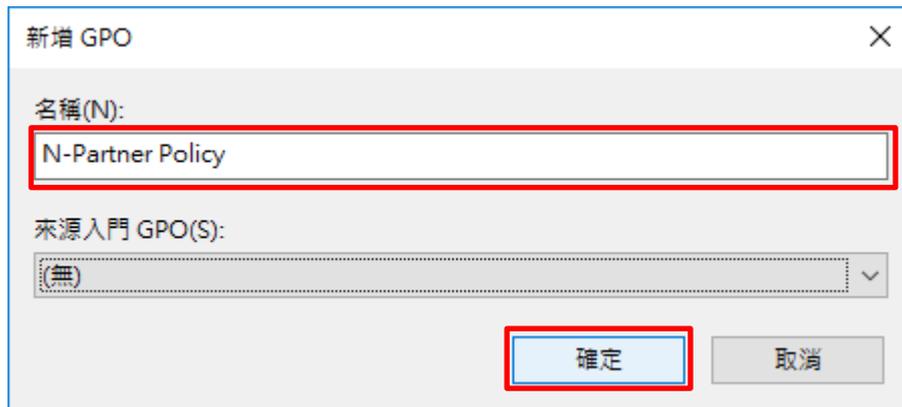
(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [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...]



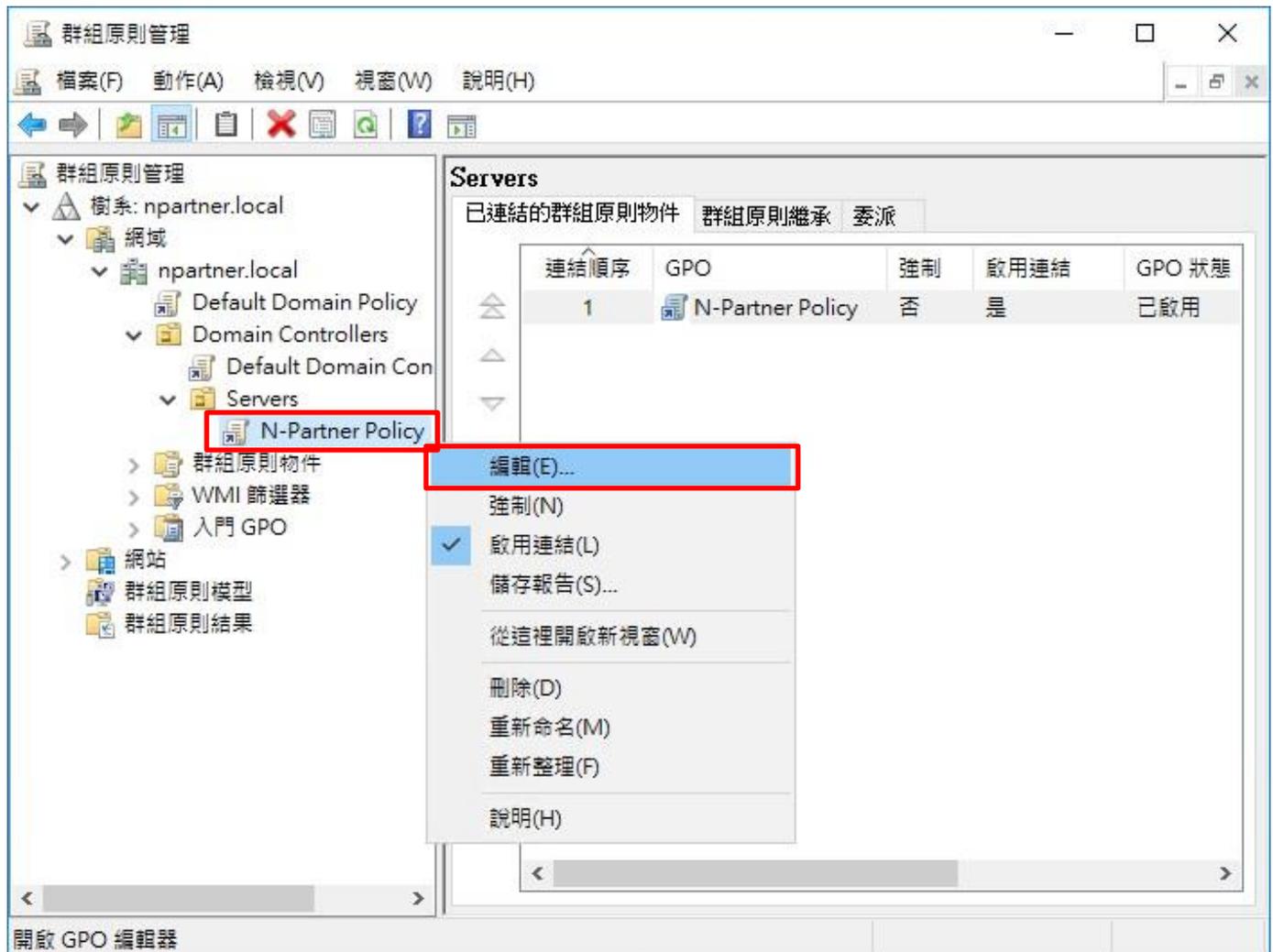
(3) 輸入群組原則物件名稱

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]



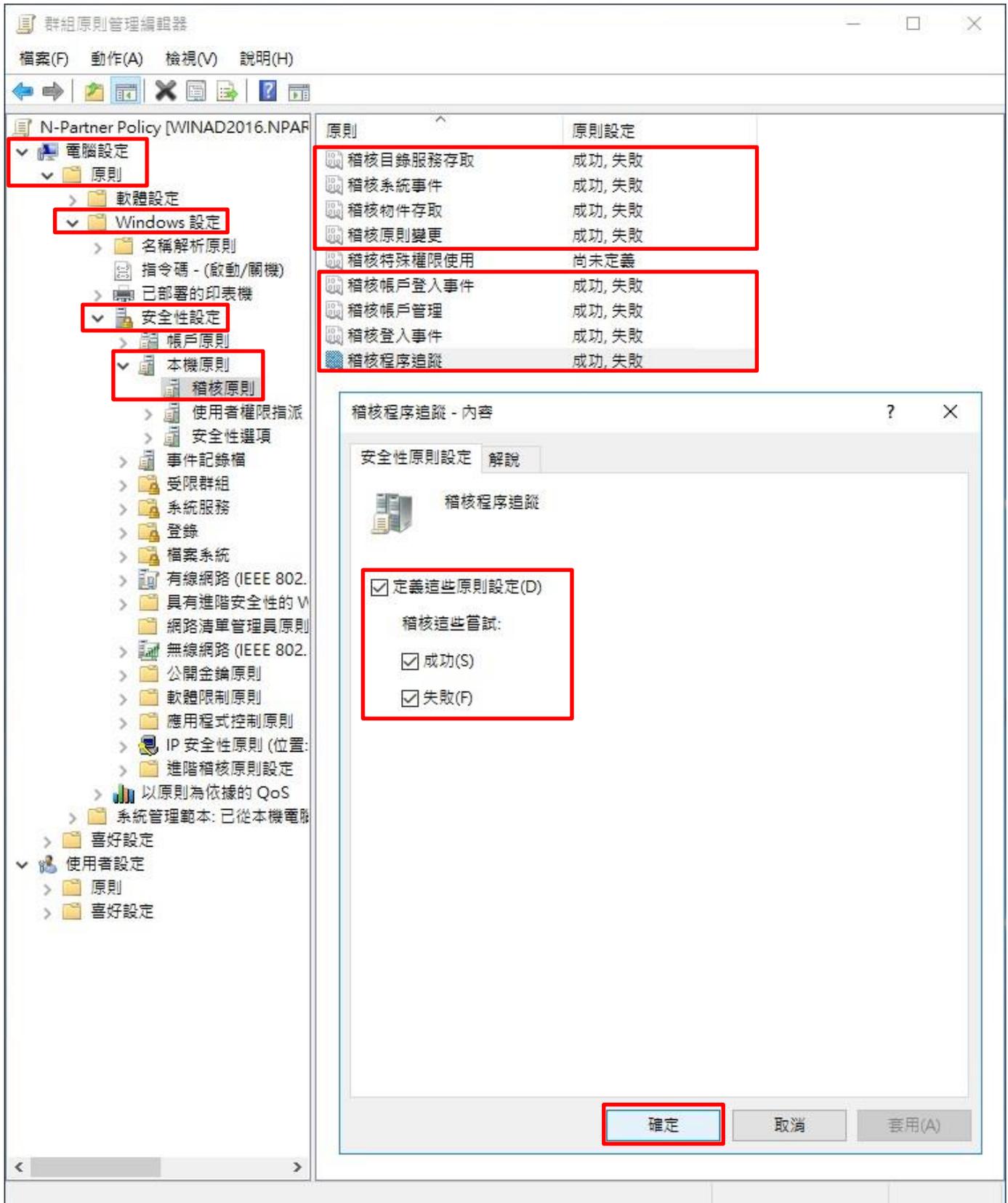
(4) 編輯群組原則物件

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 [稽核目錄服務存取], [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]



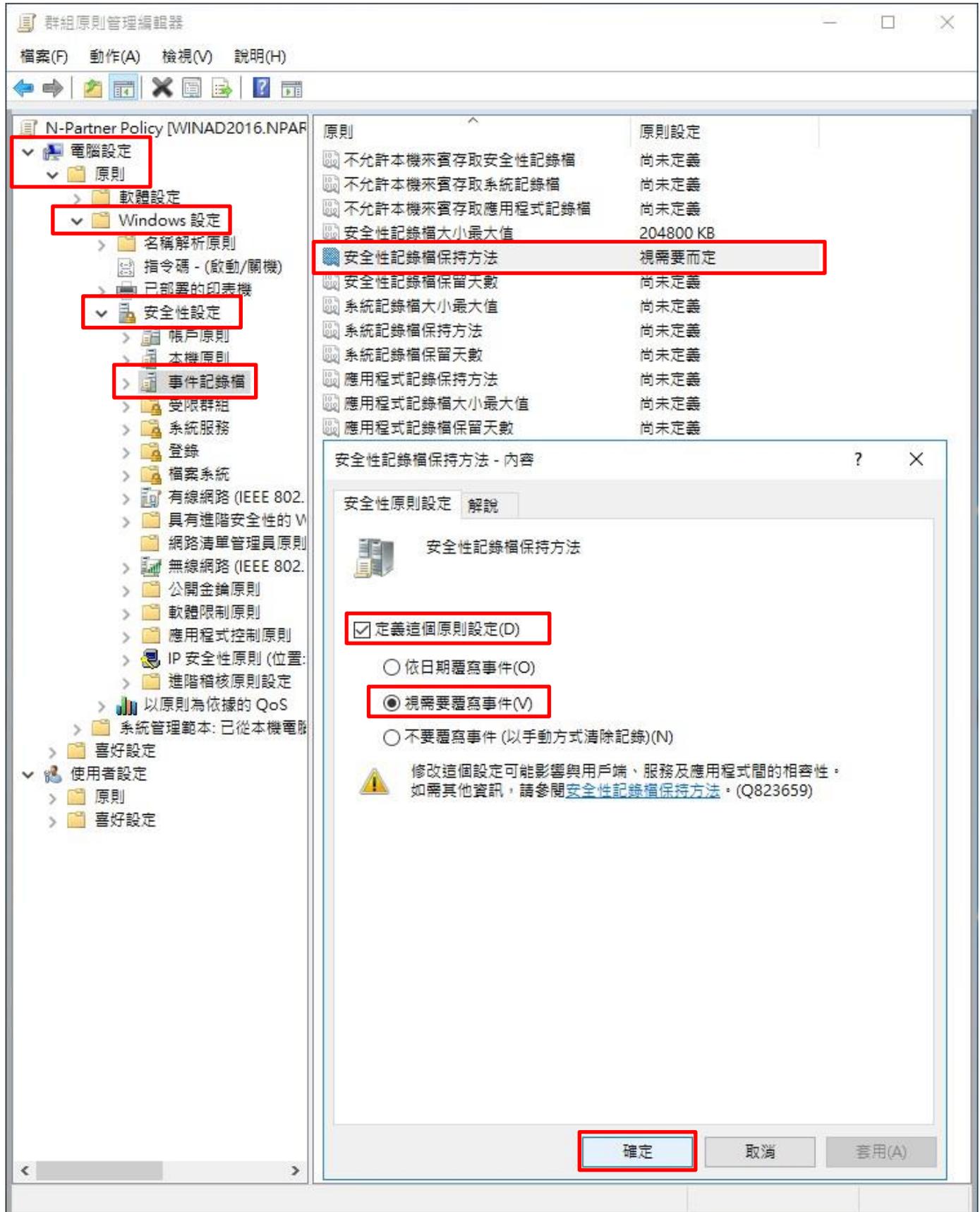
(6) 事件記錄檔：安全性記錄檔大小最大值

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 console for the 'N-Partner Policy [WINAD2016.NPAR]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (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' (Maximum size of security event logs) selected and highlighted in red. The value for this policy is set to 204800 KB. A dialog box titled '安全性記錄檔大小最大值 - 內容' (Maximum size of security event logs - Content) is open in the foreground, showing the '安全性原則設定' (Security Policy Settings) tab. In this dialog, the checkbox '定義這個原則設定(D)' (Define this policy setting) is checked and highlighted in red. Below the checkbox, the value '204800' is entered in a text box, followed by a dropdown menu set to 'KB', which is also highlighted in red. At the bottom of the dialog, the '確定' (OK) button is highlighted in red. A warning icon and text are visible in the dialog, 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)'

(7) 事件記錄檔：安全性記錄檔保持方法

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

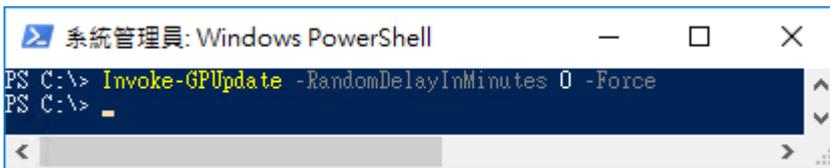


(8) 開啟 [Windows PowerShell]



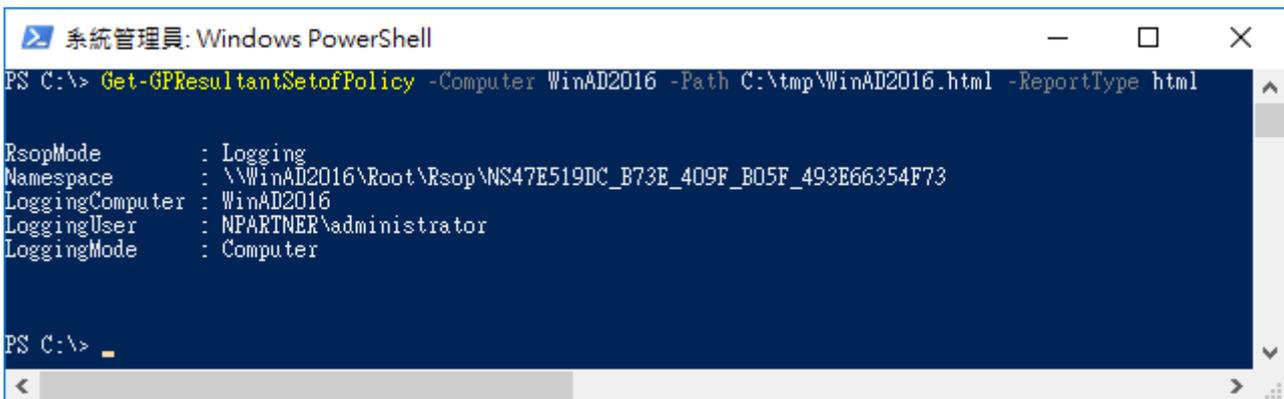
(9) 更新群組原則

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



(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer WinAD2016 -Path C:\tmp\WinAD2016.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表 · 確認 Windows AD 2016 伺服器 · 套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WINAD2016
資料收集: 2021/6/30 下午 02:09:43 全部顯示

- 摘要 顯示
- 電腦詳細資料 隱藏
- 一般 顯示
- 元件狀態 顯示
- 設定 隱藏
- 原則** 隱藏
 - Windows 設定 隱藏
 - 安全性設定 隱藏
 - 帳戶原則/密碼規則 顯示
 - 帳戶原則/帳戶鎖定原則 顯示
 - 帳戶原則/Kerberos 原則 顯示
 - 本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
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/使用者權限指派 顯示
 - 本機原則/安全性選項 顯示
 - 事件記錄檔 隱藏

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

6.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```

```

系統管理員: Windows PowerShell
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber

DisplayName           : KH
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department            : TAC
EmployeeID            : 0032
EmployeeNumber        : A0032
    
```

紅色文字部位請依客戶環境輸入使用者名稱

(2) N-Reporter [事件查詢] -> 點選 使用者名稱

等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh	4724	Administrator	User Management

(3) 顯示使用者資料

事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh (KH, TAC, 0032, (Engineer))	4724	Administrator	User Management

6.3.1 新增使用者

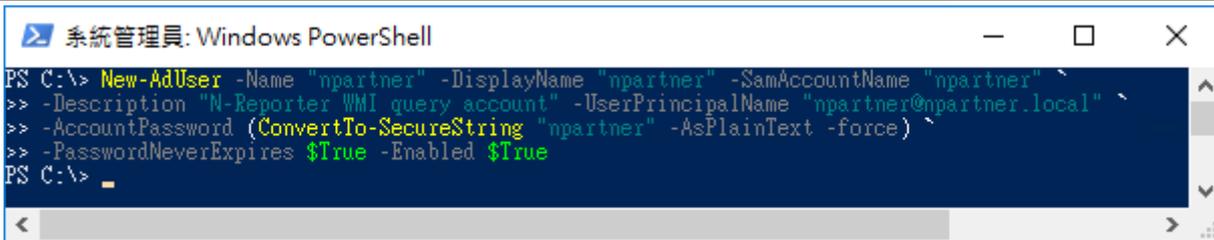
(1) 開啟 AD 使用者和電腦

開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

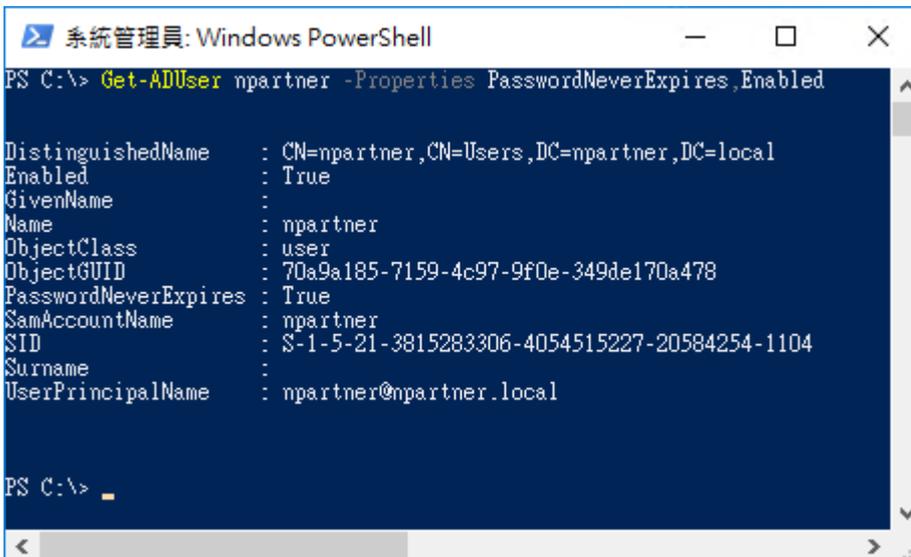
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```



紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```



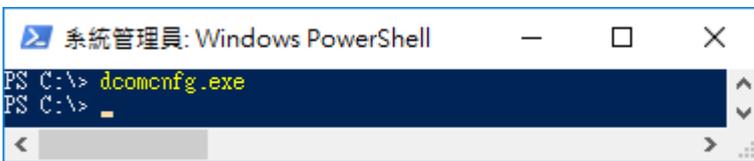
6.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



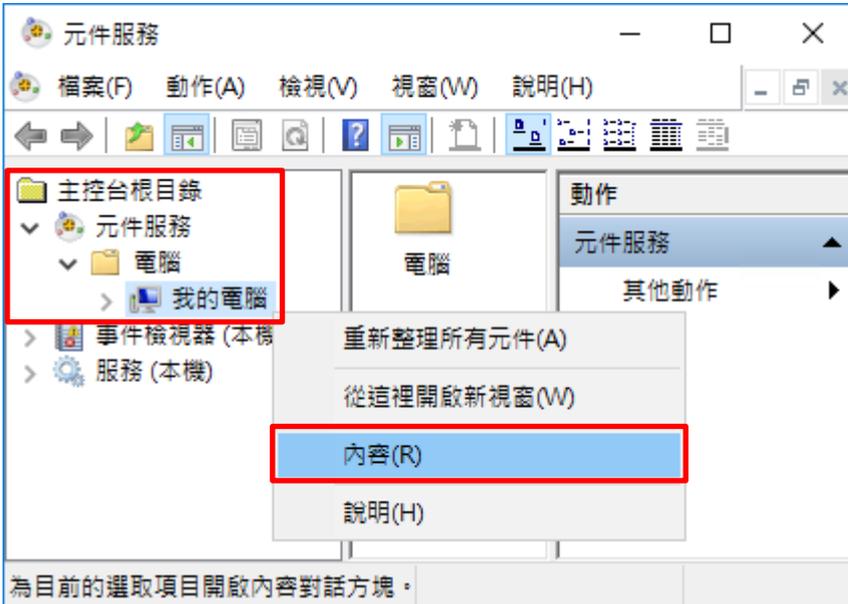
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



(3) 編輯電腦內容

展開 [主控台根目錄] -> [元件服務] -> [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



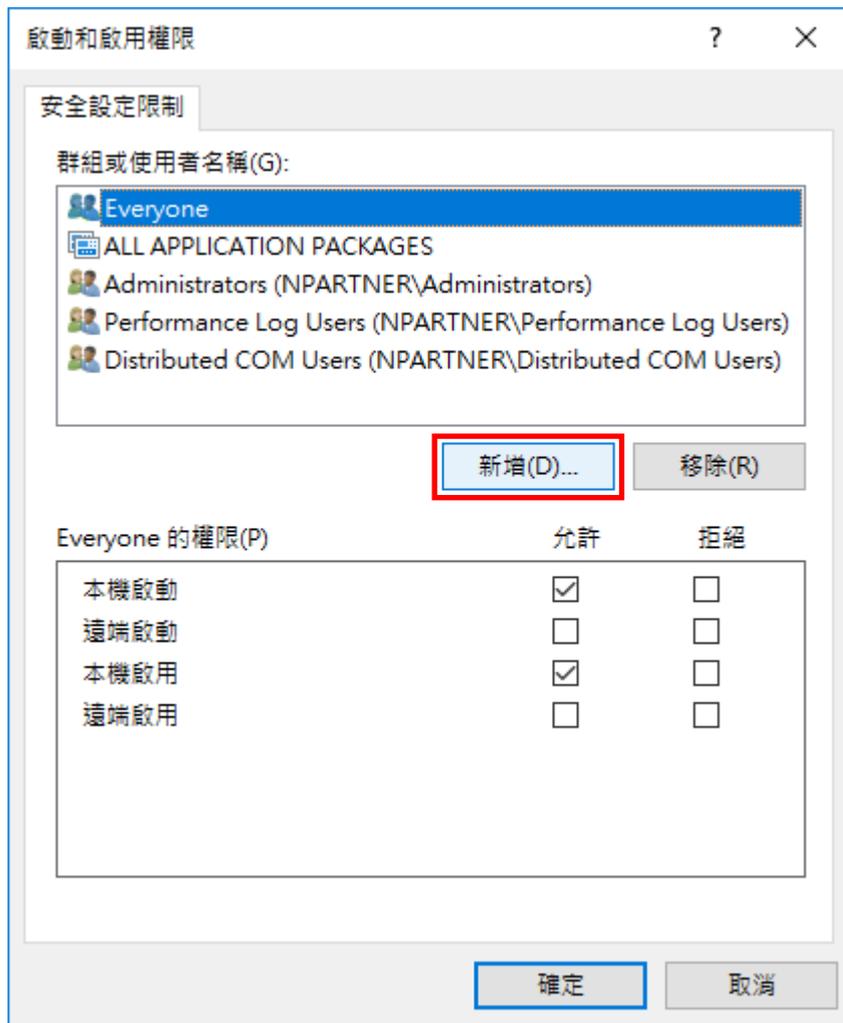
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



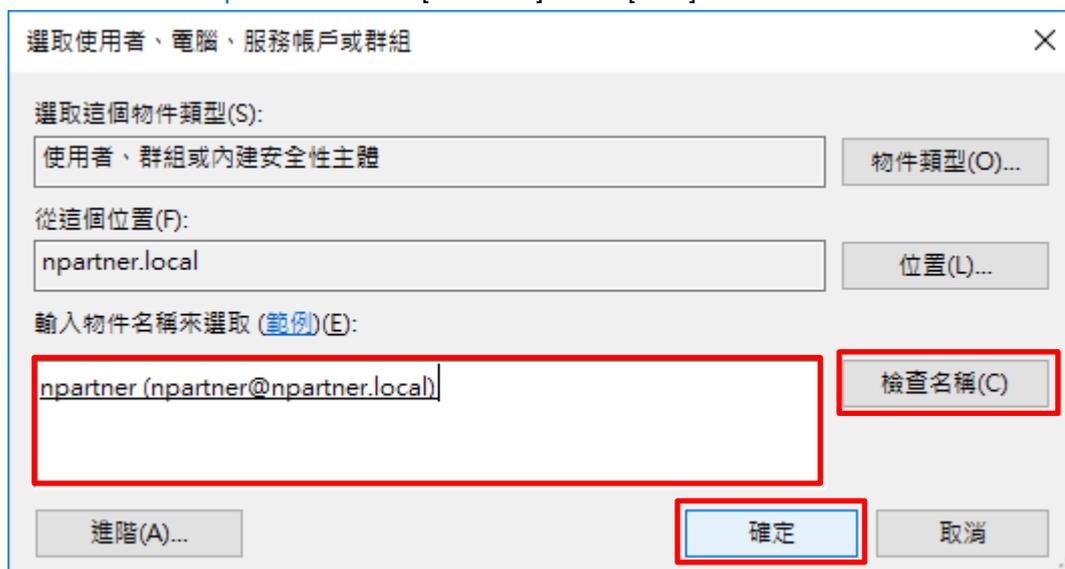
(5) 新增 DCOM 使用者權限

點選 [新增]



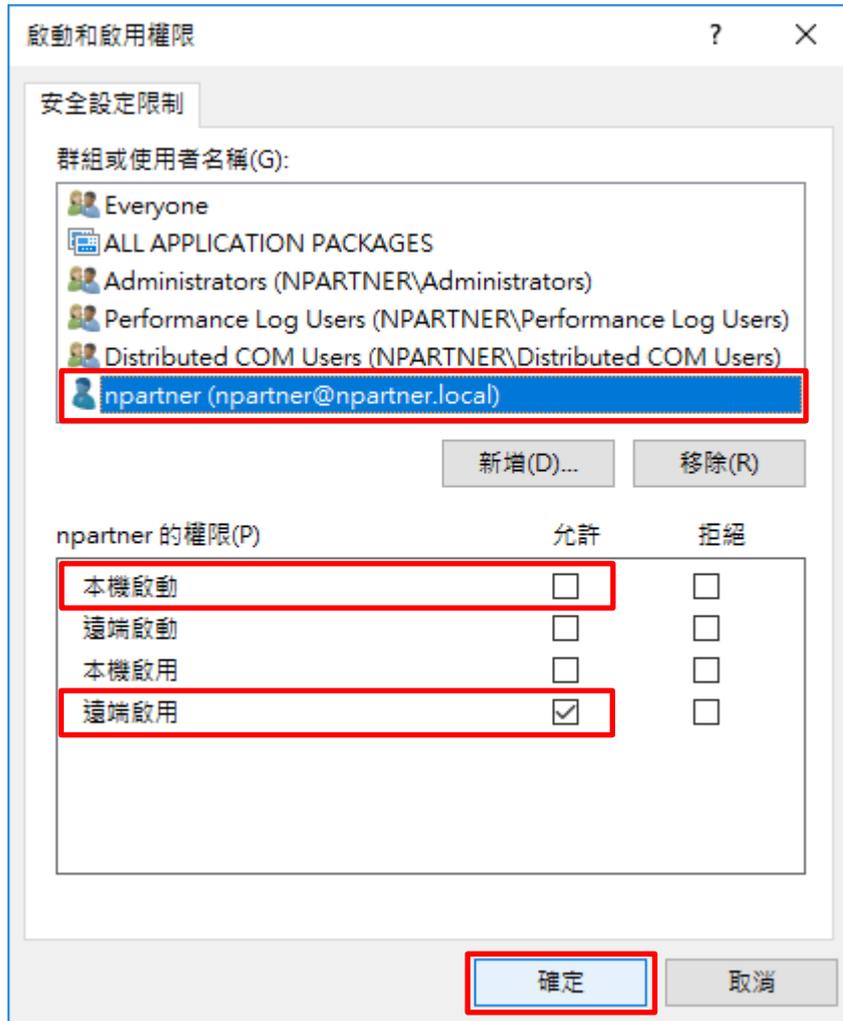
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



6.3.3 設定 WMI 權限

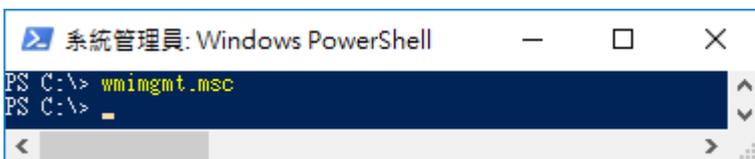
6.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



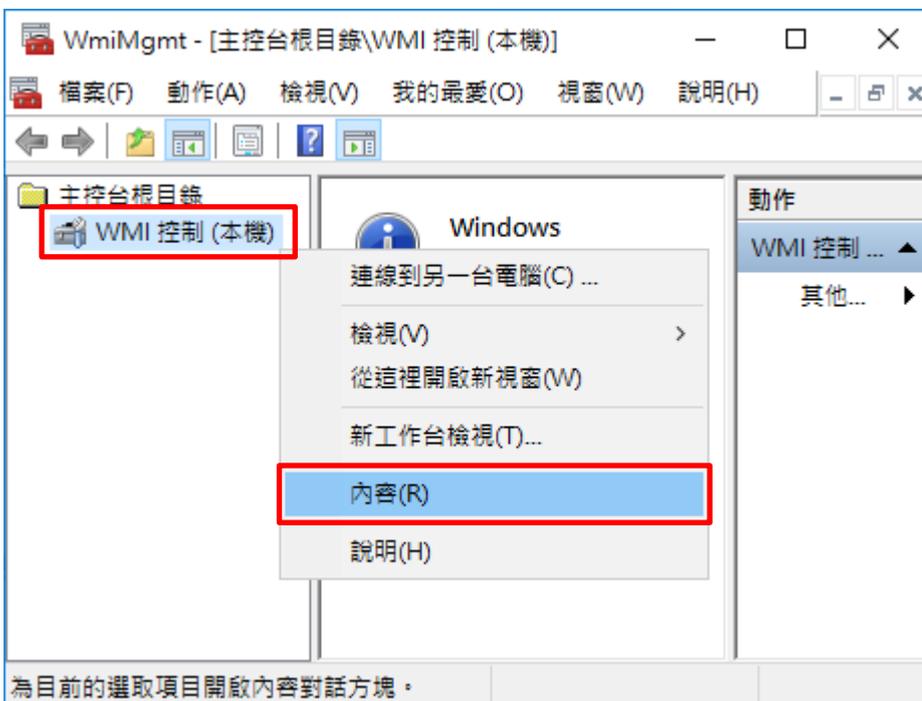
(2) 開啟元件服務

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



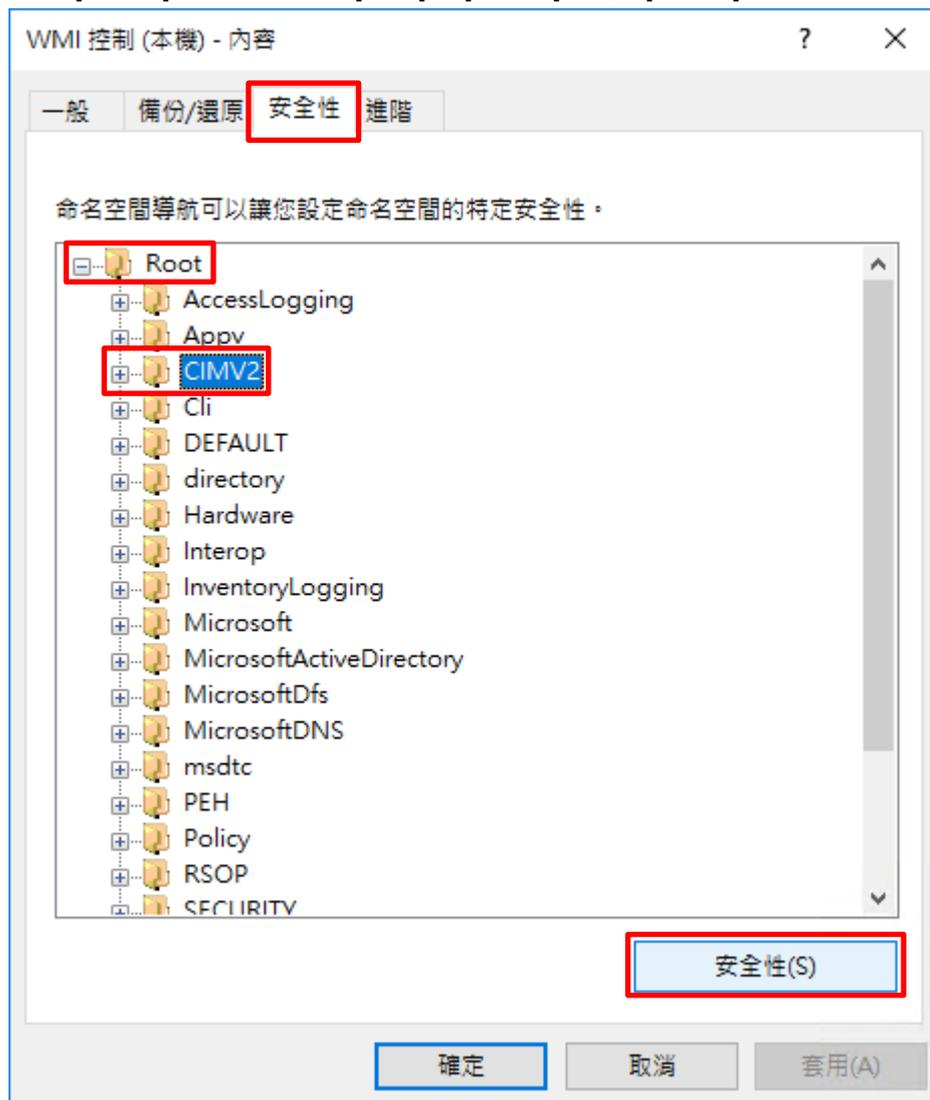
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



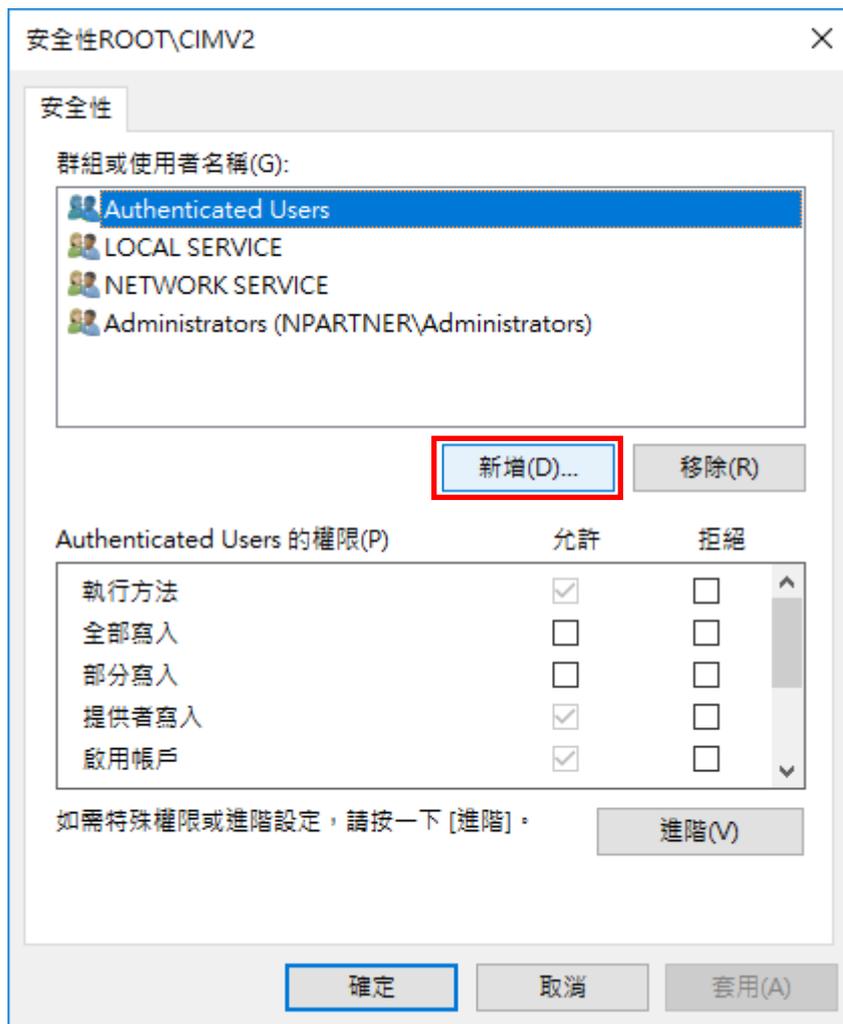
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



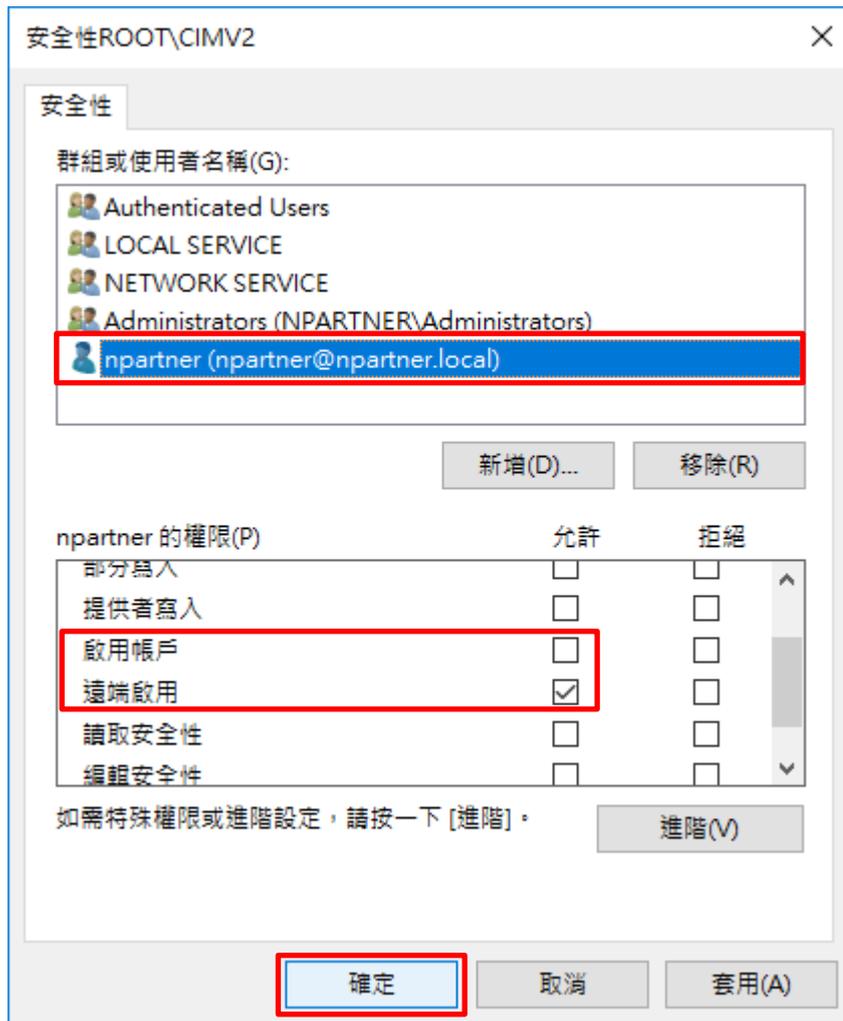
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

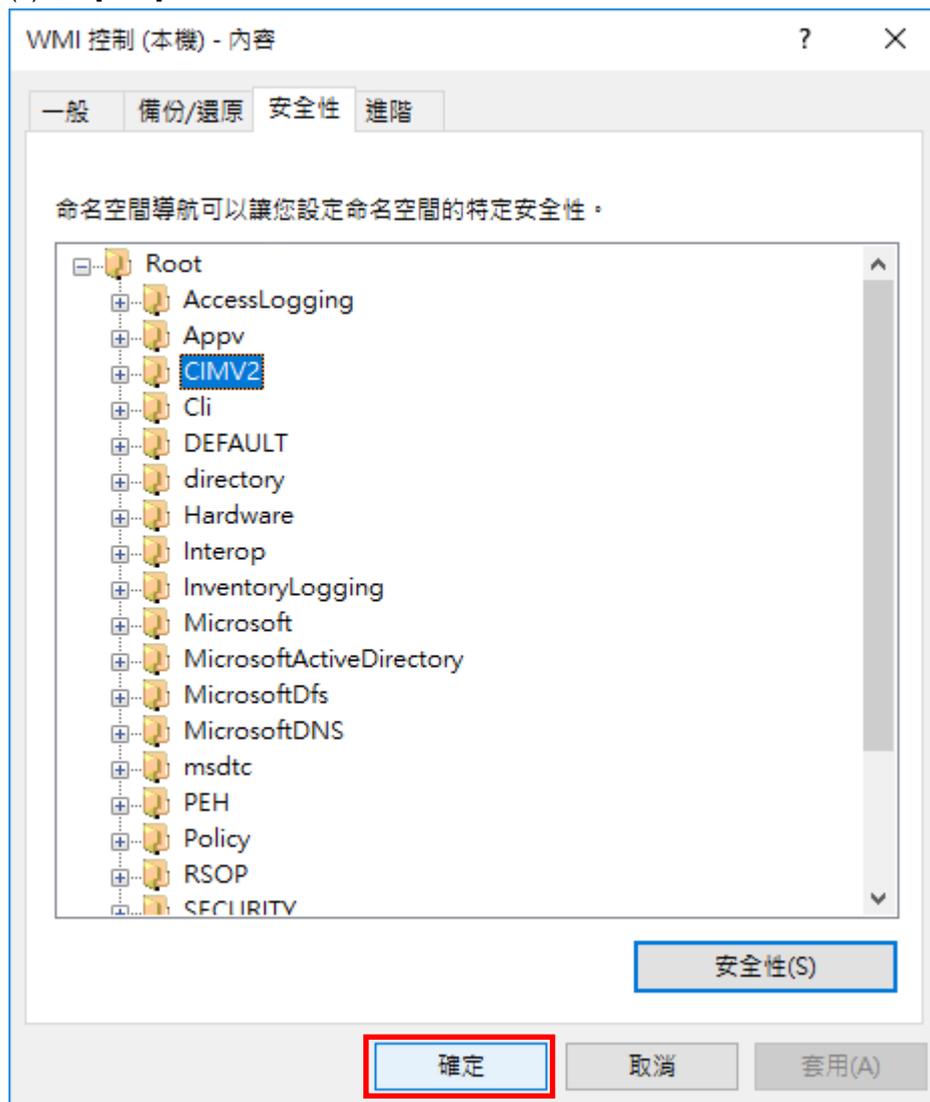


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



6.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



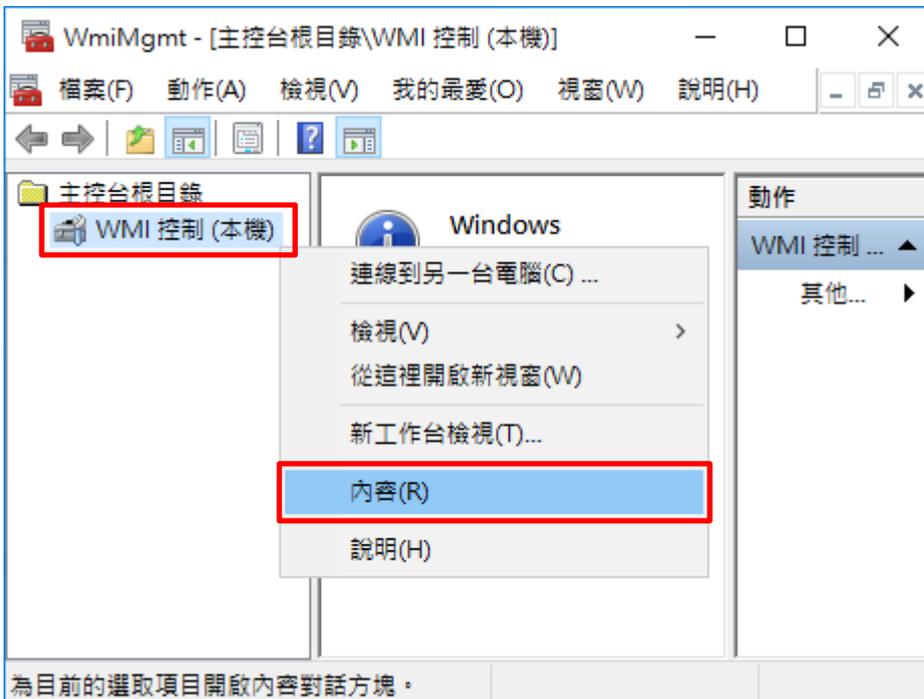
(2) 開啟元件服務

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



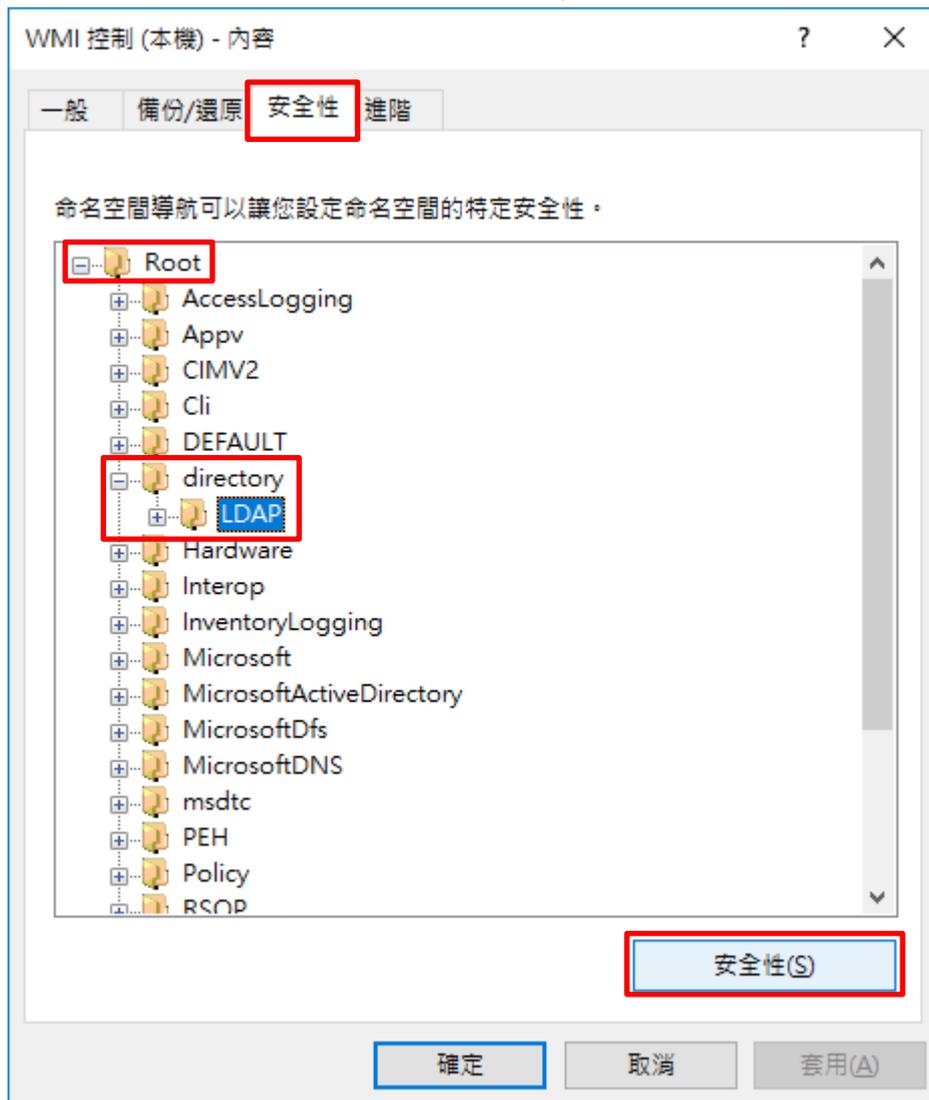
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



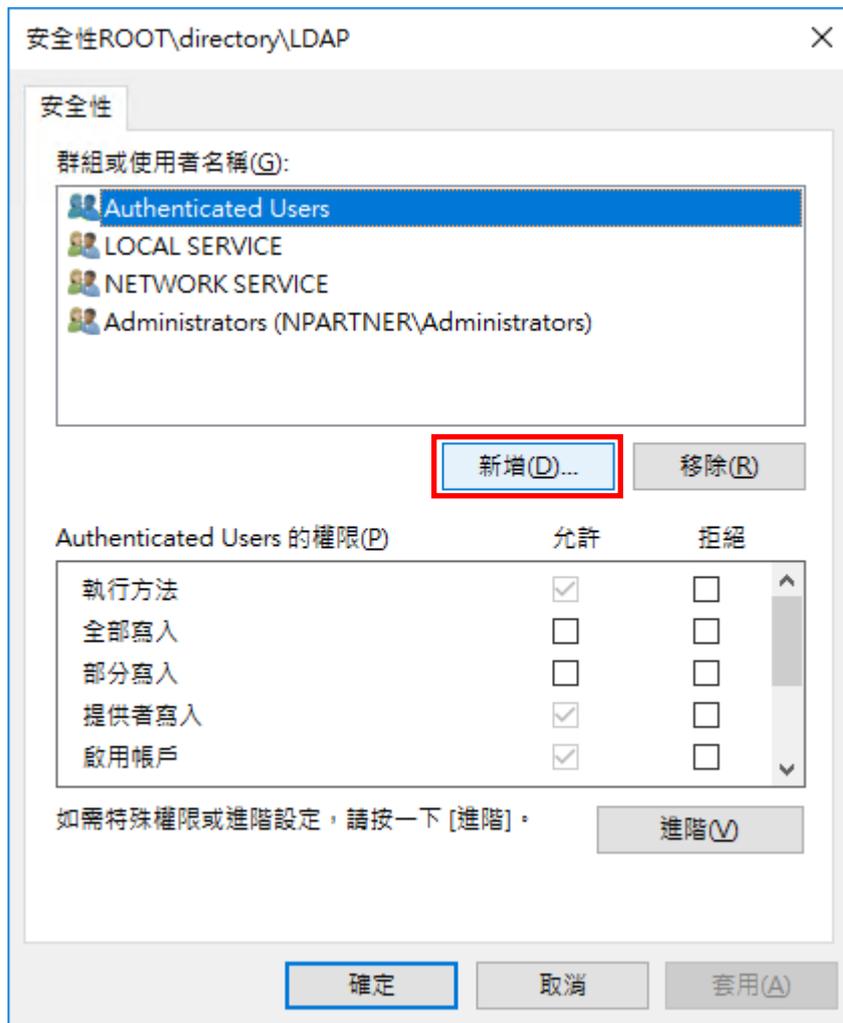
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



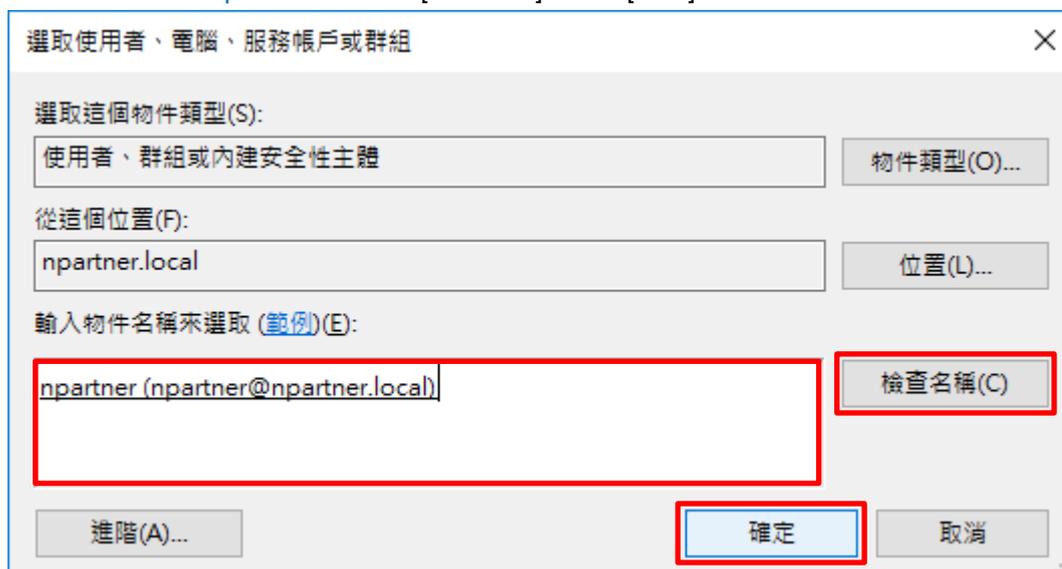
(5) 新增 WMI 使用者權限

按 [新增]



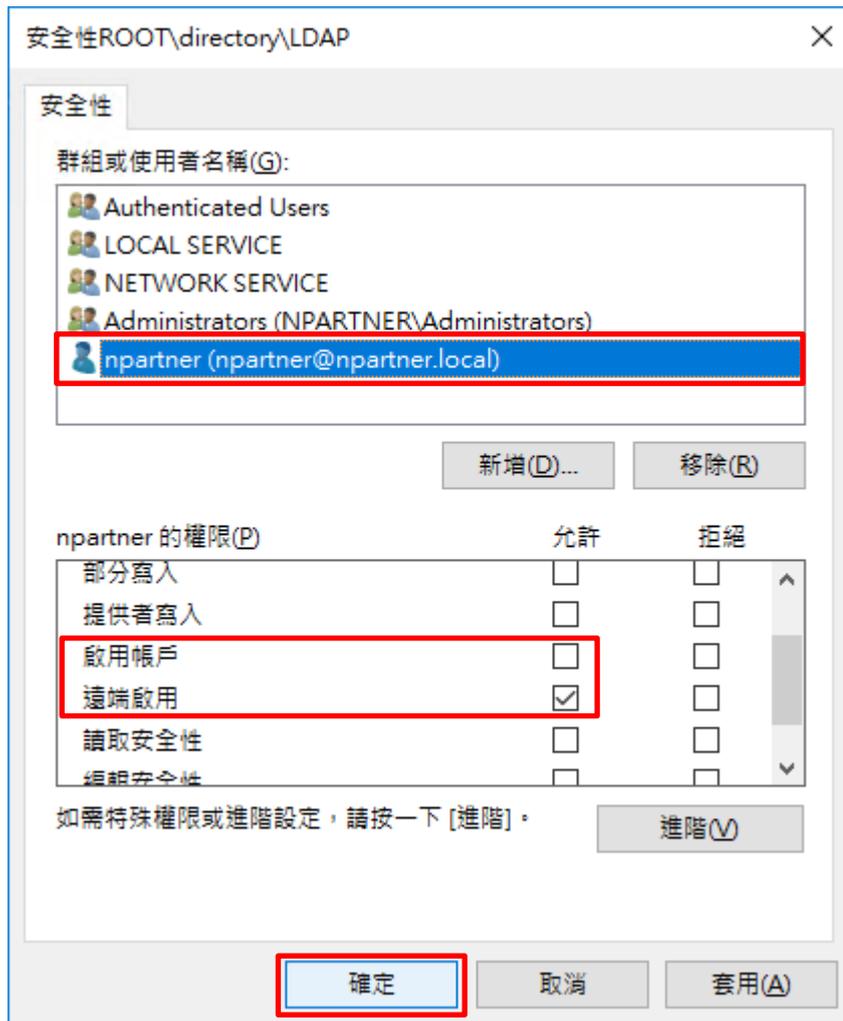
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

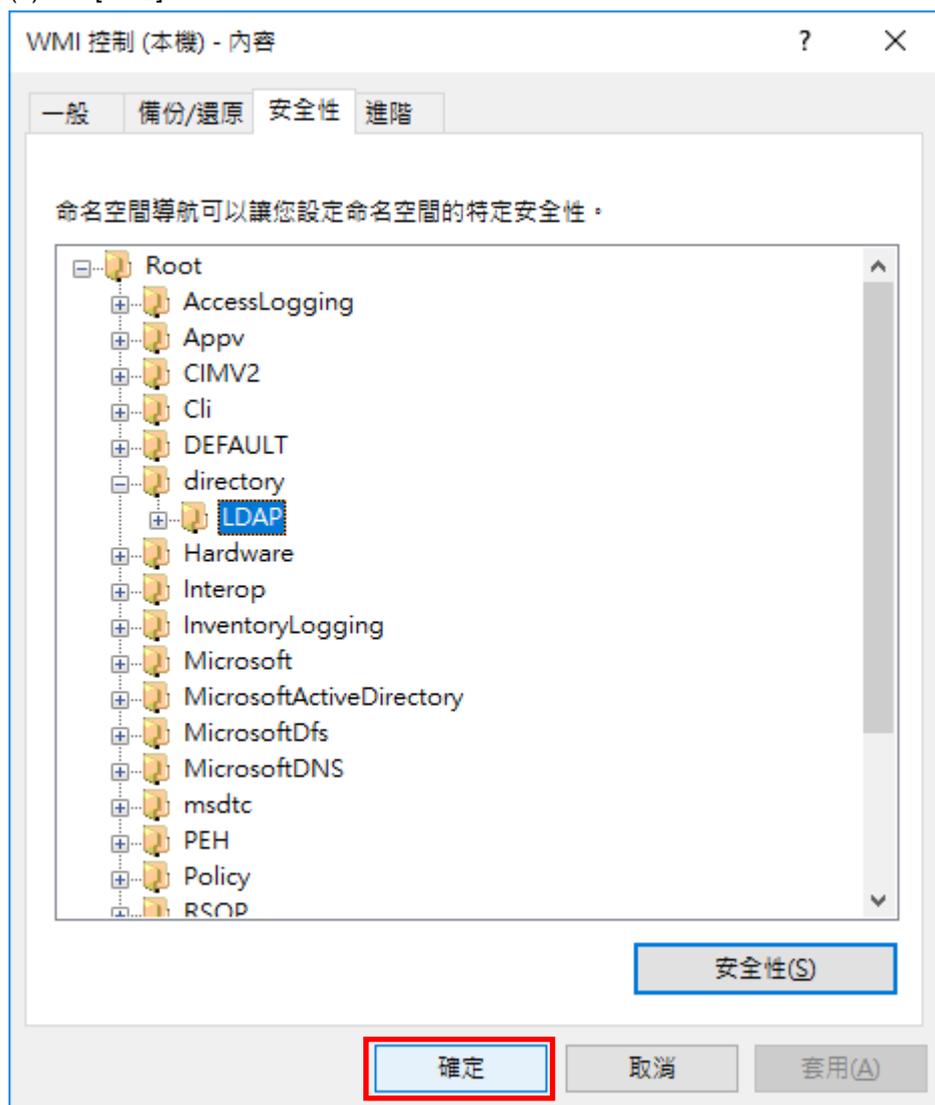


(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 按 [確定]



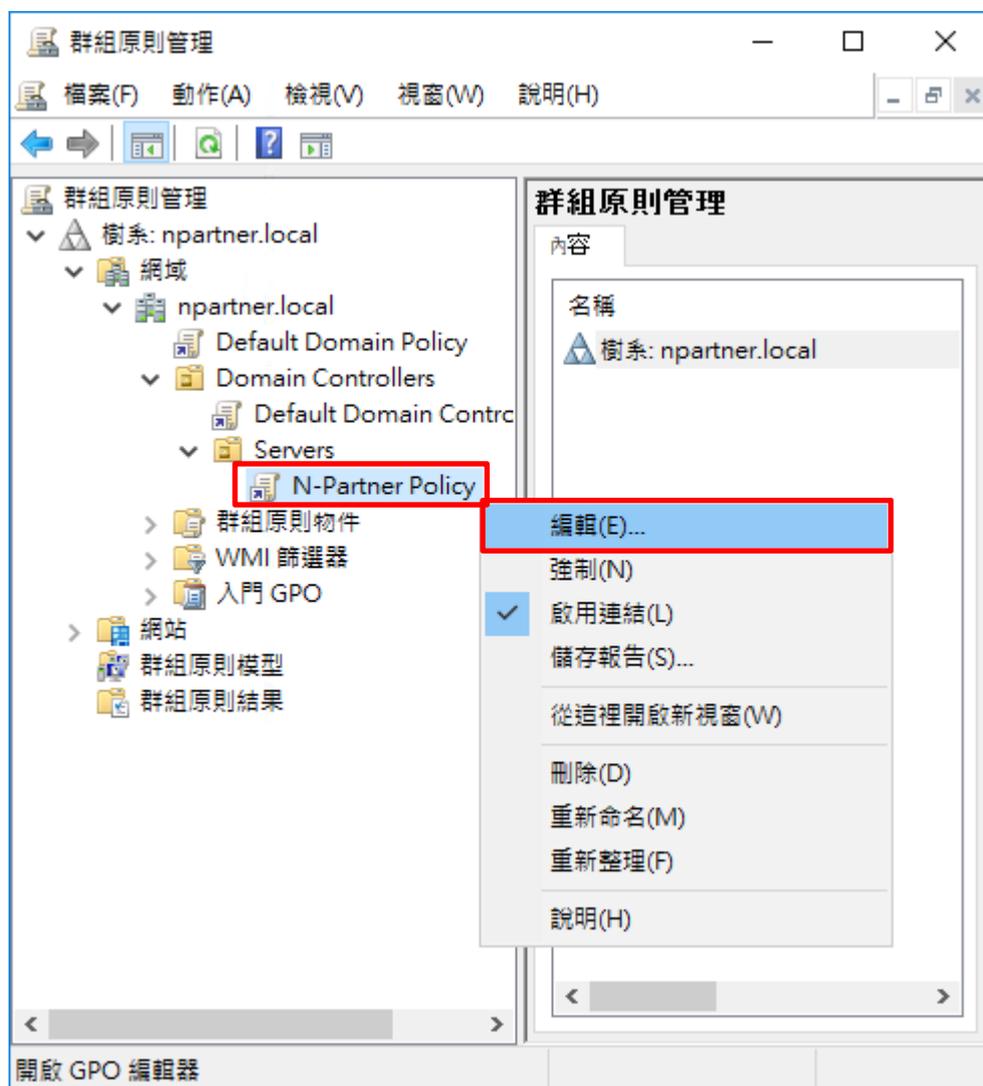
6.3.4 設定 Event log 讀取權限

(1) 開啟 [群組原則管理]



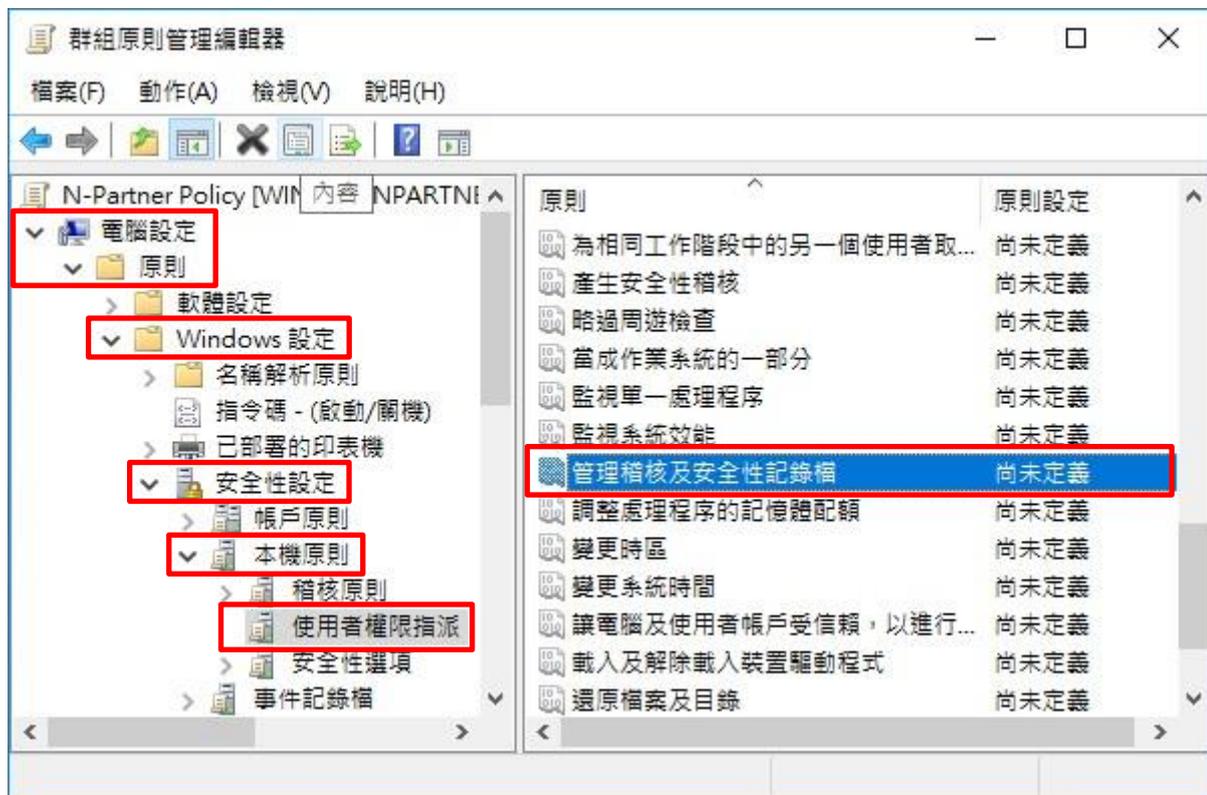
(2) 編輯群組原則物件

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



(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全性記錄檔] 項目



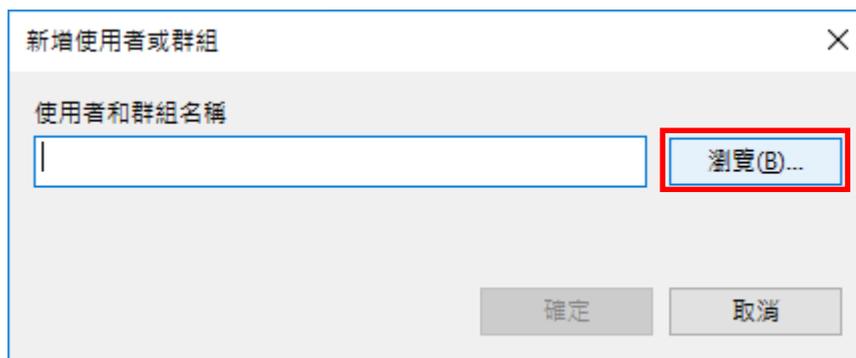
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

選擇使用者、電腦、服務帳戶或群組

選擇這個物件類型(S):
使用者、服務帳戶、群組或內建安全性主體 物件類型(O)...

從這個位置(F):
npartner.local 位置(L)...

輸入物件名稱來選擇 (範例)(E):
npartner (npartner@npartner.local) 檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

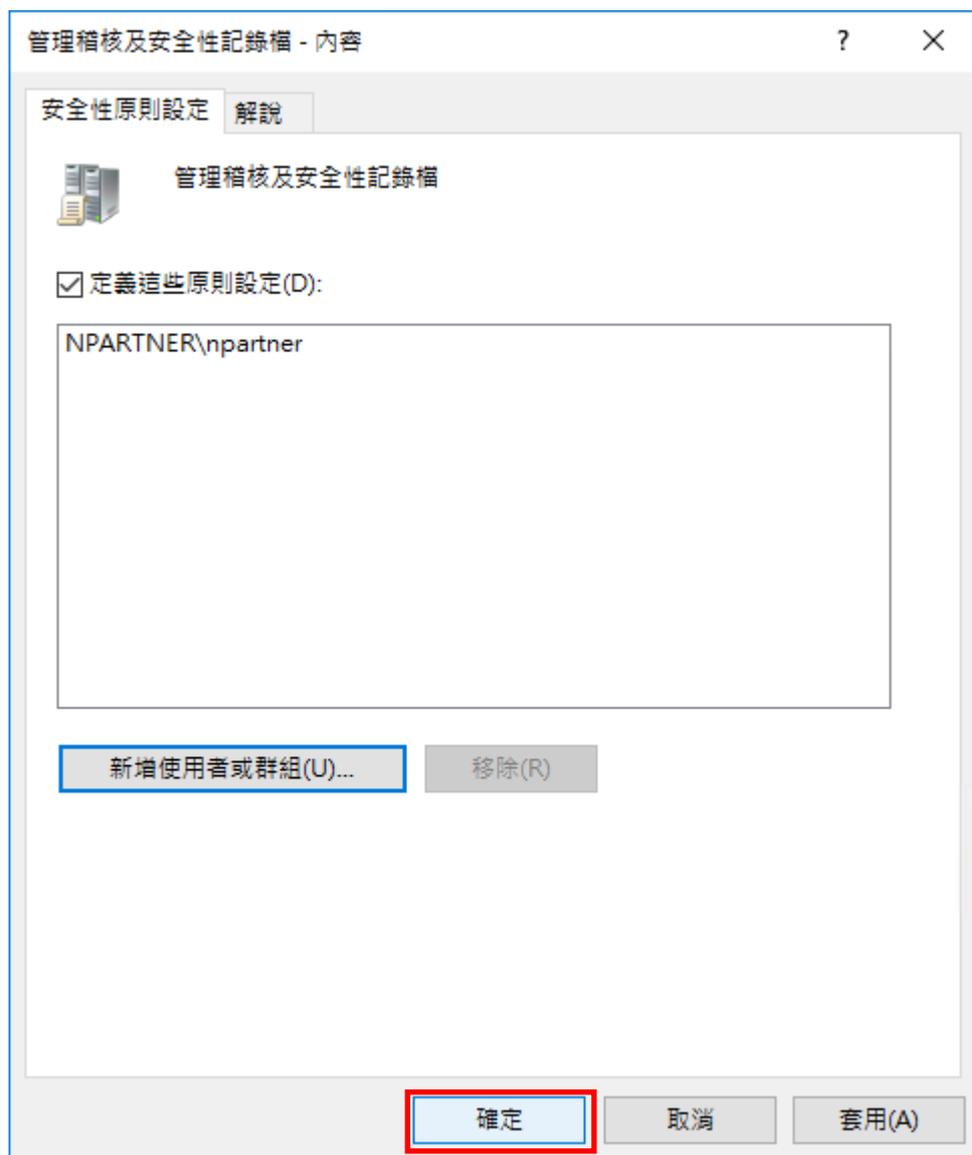
新增使用者或群組

使用者和群組名稱
NPARTNER\npartner 瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]

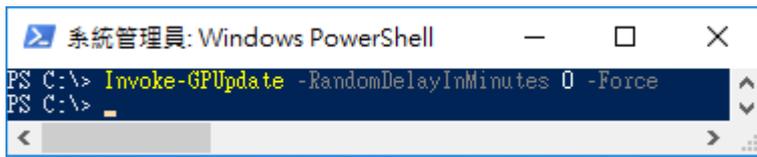


(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

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



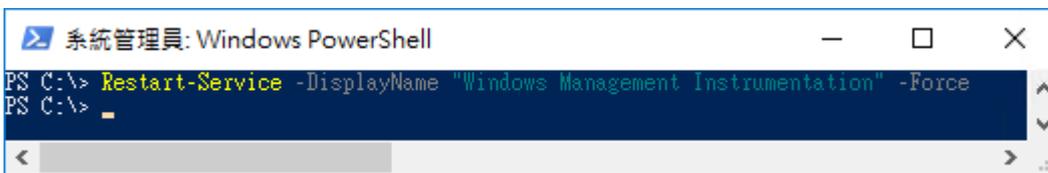
6.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



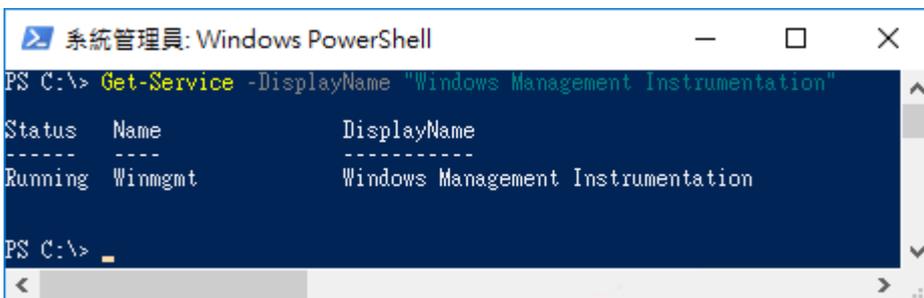
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



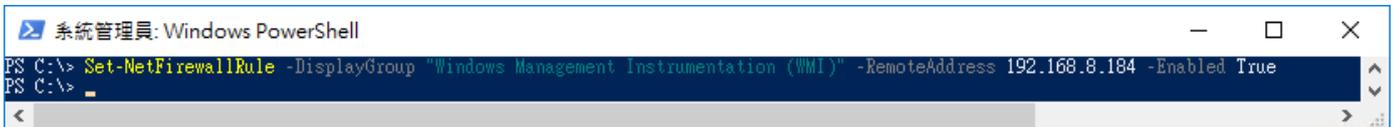
6.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

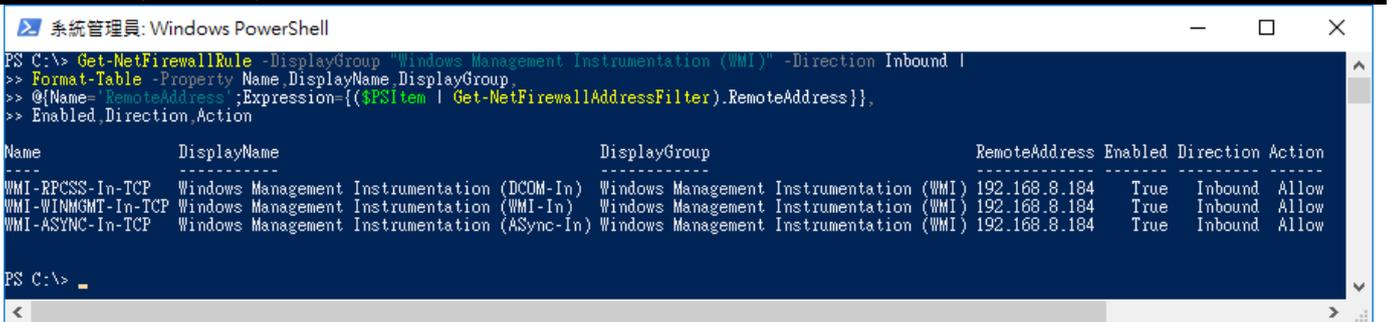
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



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](#)

7.1 組織單位設定

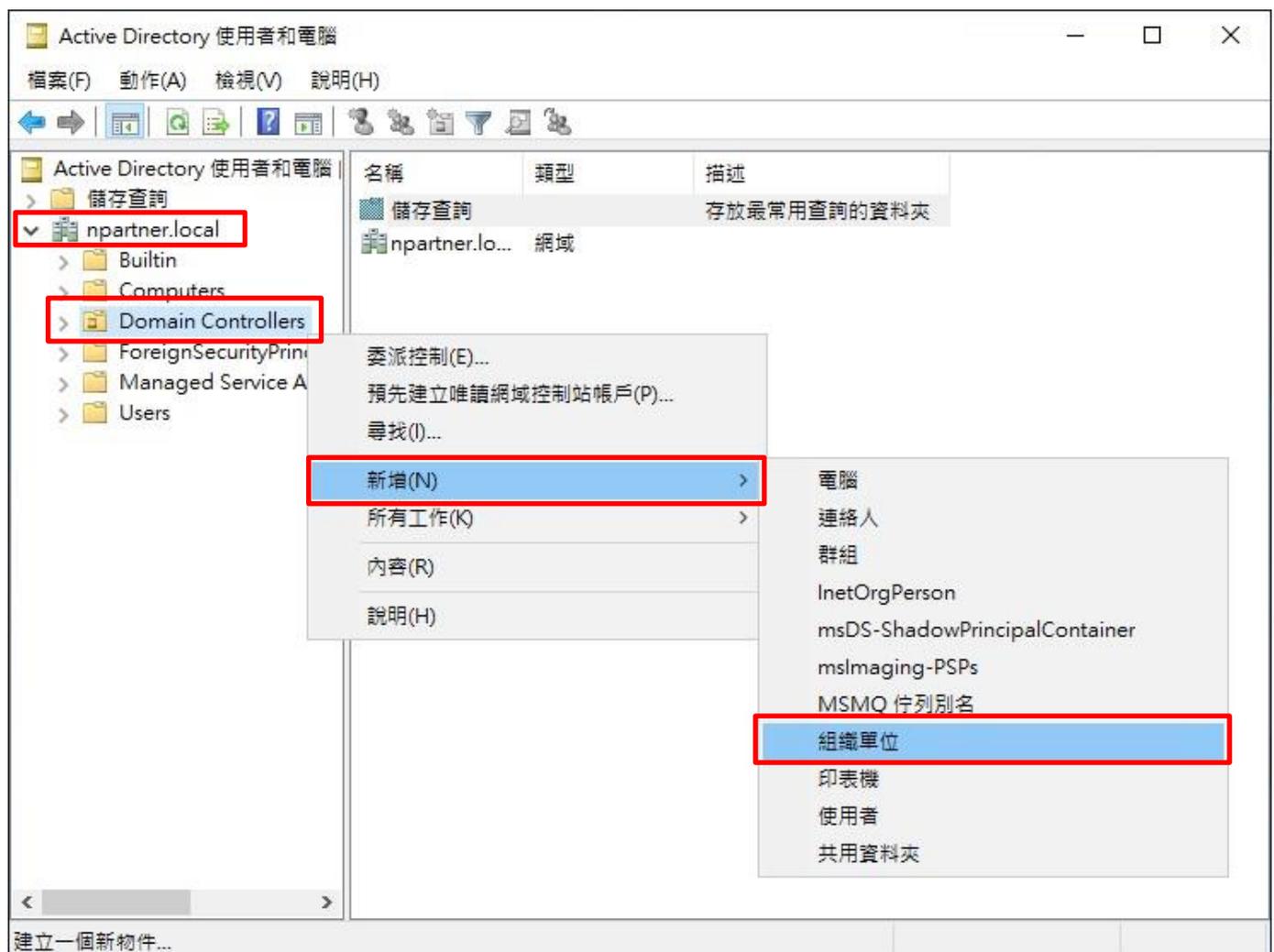
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 的 [Domain Controllers] 組織單位，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/Domain Controllers

名稱(A):
Servers

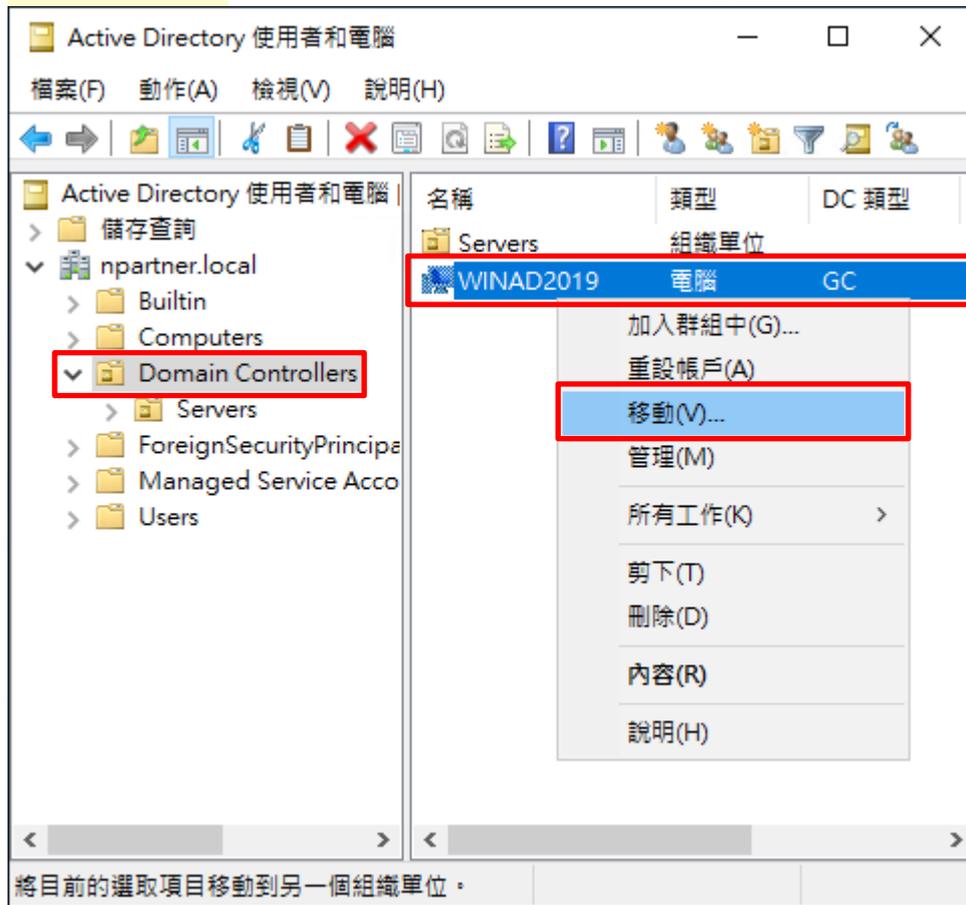
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

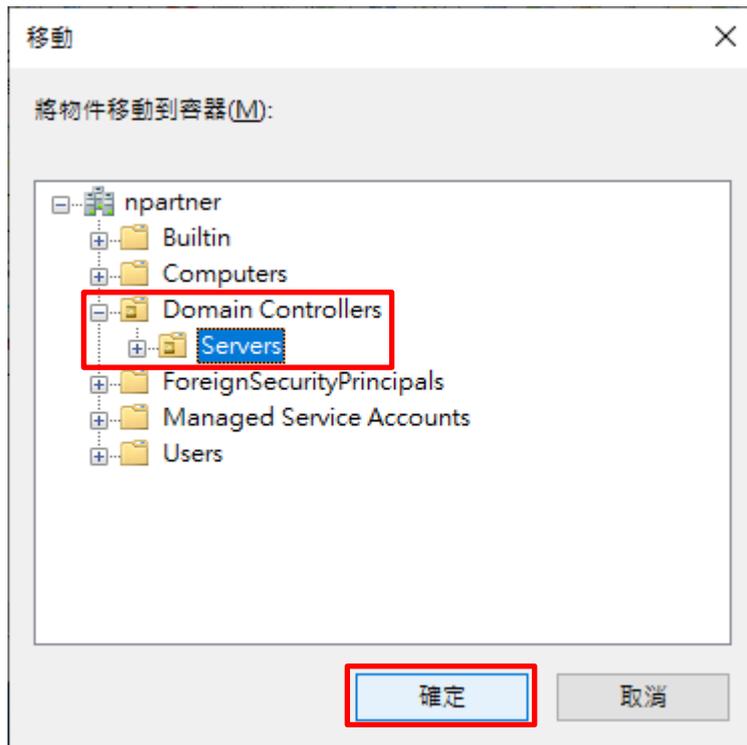
選擇 [Domain Controllers] 組織單位 -> 在 [WinAD2019] 網域伺服器，按滑鼠右鍵註：請依客戶環境選擇

Windows AD 主機 -> 點選 [移動]



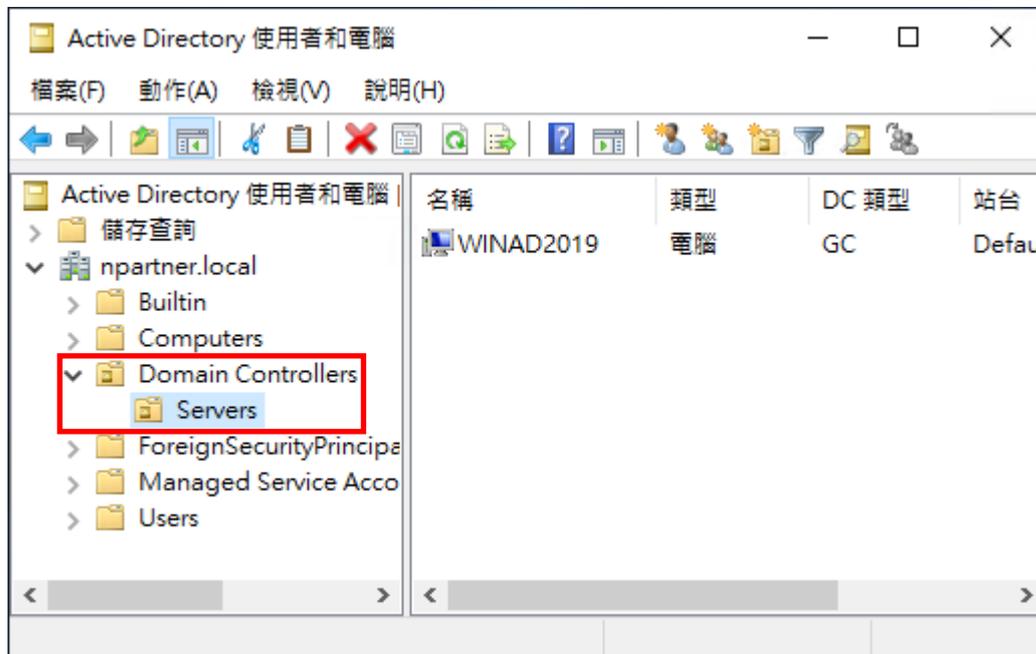
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [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 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2019] 網域伺服器已移動。



7.2 群組原則設定

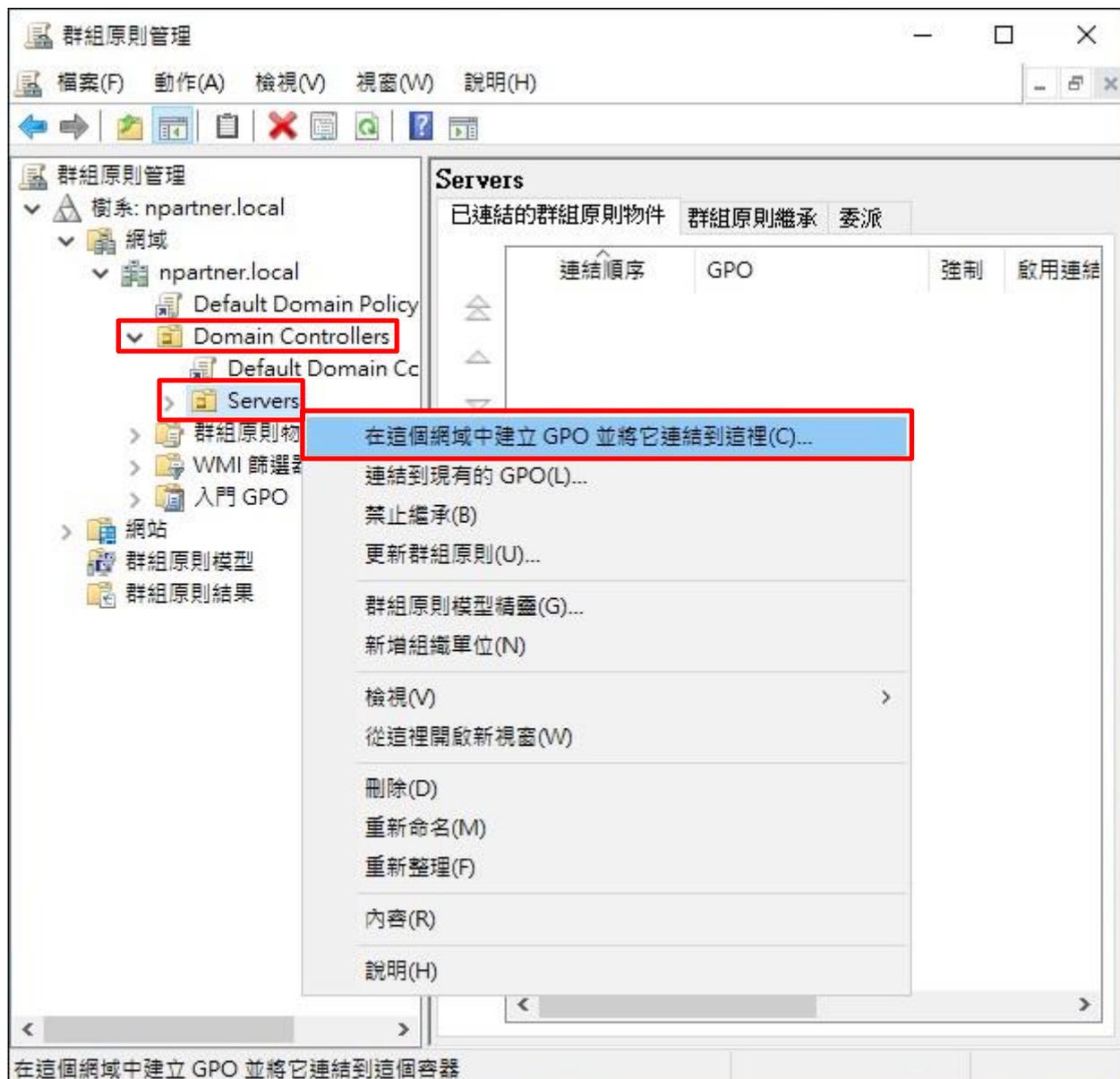
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並將它連結到這裡...]



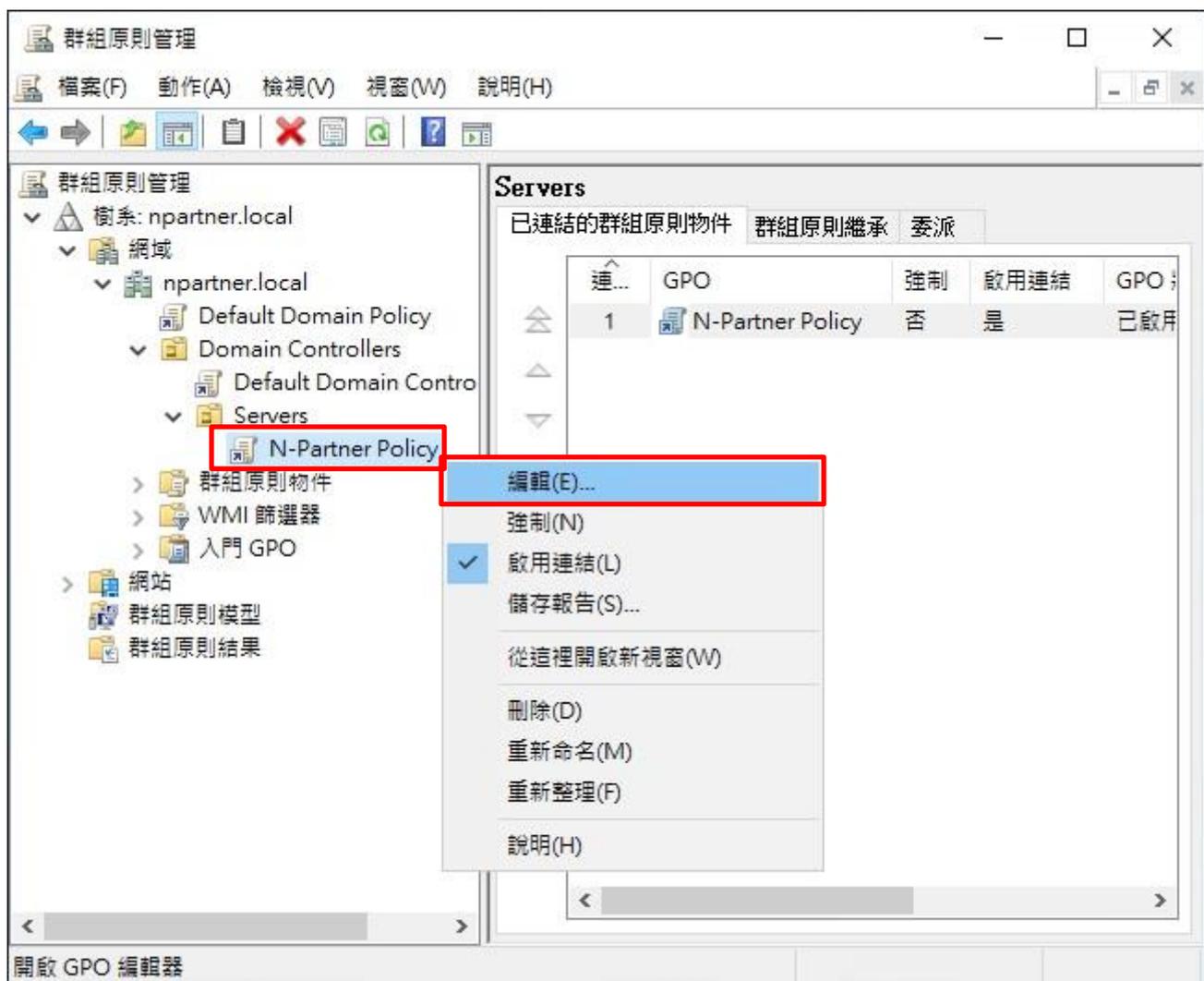
(3) 輸入群組原則物件名稱

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 [稽核目錄服務存取], [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]

原則	原則設定
稽核目錄服務存取	成功, 失敗
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	尚未定義
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

安全性原則設定 解說

稽核程序追蹤

定義這些原則設定(D)

稽核這些嘗試:

成功(S)

失敗(F)

確定 取消 套用(A)

(6) 事件記錄檔：安全性記錄檔大小最大值

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

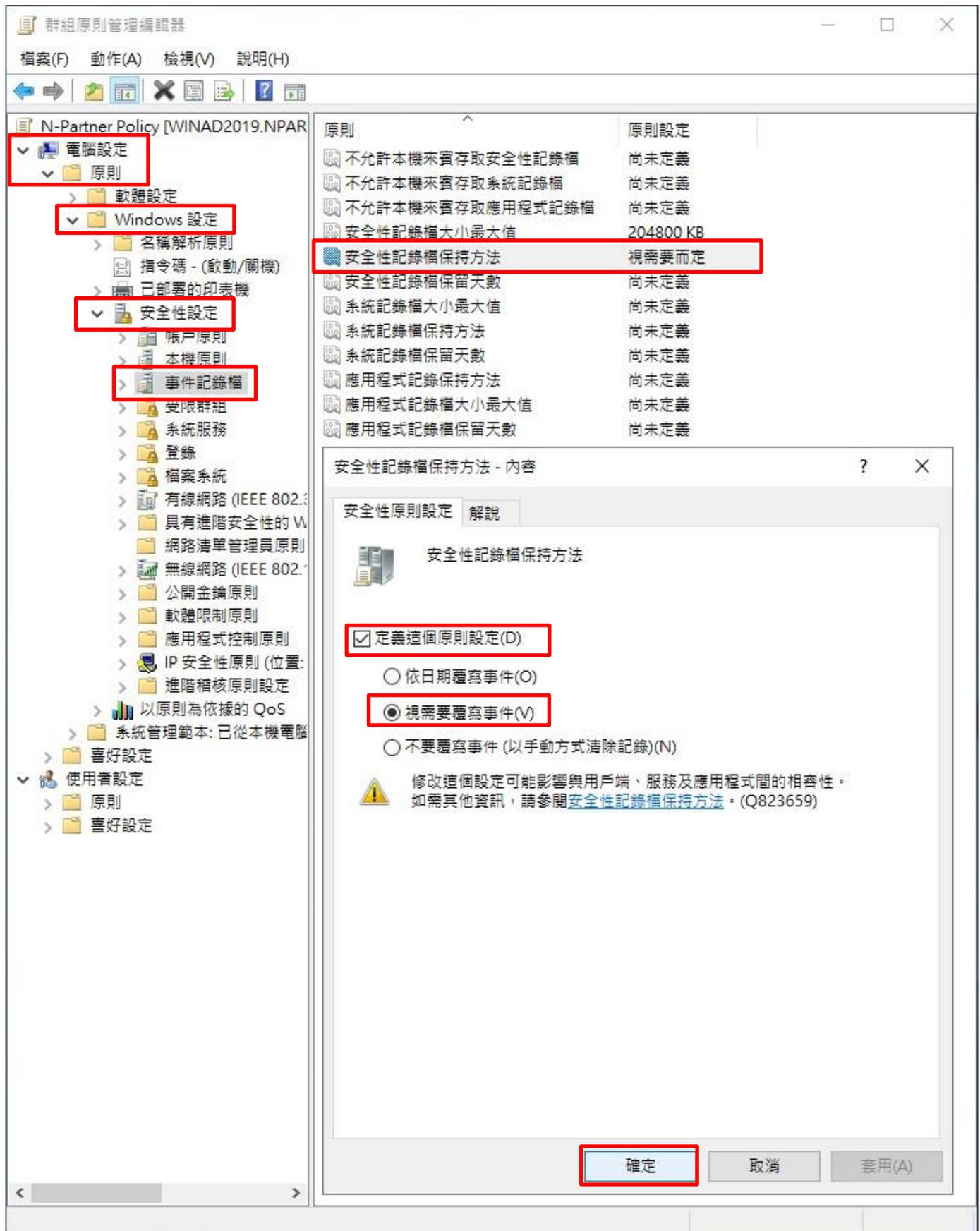
The screenshot shows the Group Policy Editor window titled "群組原則管理編輯器". The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Logs). The right-hand pane displays a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

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

A dialog box titled "安全性記錄檔大小最大值 - 內容" (Maximum size of security event logs - Content) is open in the foreground. It shows the "安全性原則設定" (Security Policy Setting) tab. The policy name "安全性記錄檔大小最大值" is displayed. The checkbox "定義這個原則設定(D)" (Define this policy setting) is checked. Below it, the value "204800" is entered in a text box, followed by a dropdown menu set to "KB". A warning icon and text are present at the bottom of the dialog: "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 right of the dialog, the "確定" (OK) button is highlighted.

(7) 事件記錄檔：安全性記錄檔保持方法

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



(8) 開啟 [Windows PowerShell]



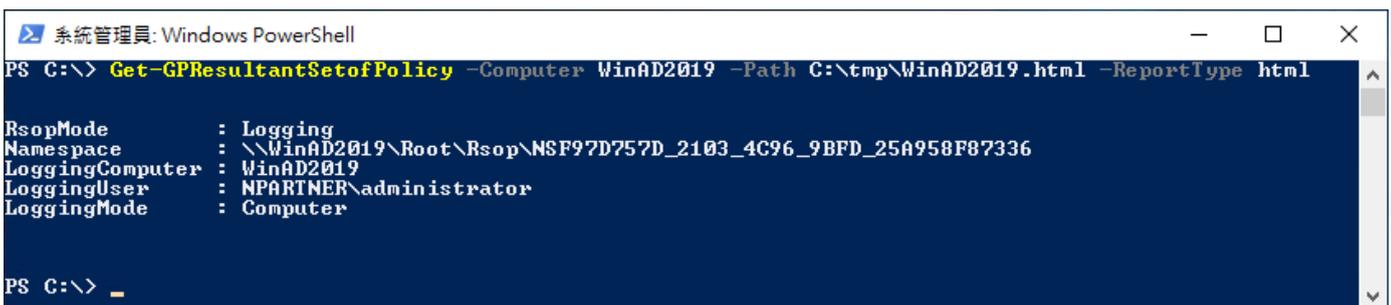
(9) 更新群組原則

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



(10) 產生 Windows AD 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer WinAD2019 -Path C:\tmp\WinAD2019.html -ReportType html
```



紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表，確認 Windows AD 2019 伺服器，套用 N-Partner Policy 群組原則

群組原則結果

NPARTNER\WINAD2019
資料收集: 2021/6/30 下午 02:49:24 全部顯示

摘要 顯示

電腦詳細資料 隱藏

一般 顯示

元件狀態 顯示

設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

帳戶原則/Kerberos 原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
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/使用者權限指派 顯示

本機原則/安全性選項 顯示

事件記錄檔 隱藏

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

公開金鑰原則/憑證服務用戶端 - 自動註冊設定 顯示

公開金鑰原則/加密檔案系統 顯示

群組原則物件 顯示

WMI 篩選器 顯示

使用者詳細資料 顯示

7.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```

```

系統管理員: Windows PowerShell
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
DisplayName           : KH
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department            : TAC
EmployeeID            : 0032
EmployeeNumber        : A0032
PS C:\> _
    
```

紅色文字部位請依客戶環境輸入使用者名稱

(2) N-Reporter [事件查詢] -> 點選 使用者名稱 

等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator 	kh 	4724	Administrator	User Management

(3) 顯示使用者資料

事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator 	kh (KH, TAC, 0032, (Engineer))	4724	Administrator	User Management

7.3.1 新增非管理帳號

(1) 開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\Users\Administrator> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
PS C:\Users\Administrator> _
```

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\Users\Administrator> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
Name                    : npartner
ObjectClass             : user
ObjectGUID              : c82573b6-9946-45ab-94ff-d1c7fe6409fe
PasswordNeverExpires   : True
SamAccountName         : npartner
SID                     : S-1-5-21-3442889578-203786663-490607469-1104
Surname                 :
UserPrincipalName      : npartner@npartner.local

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

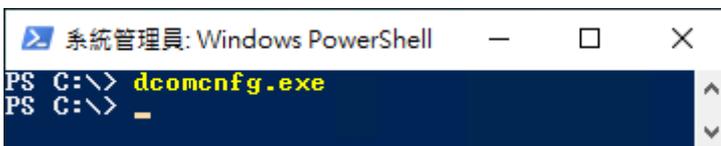
7.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



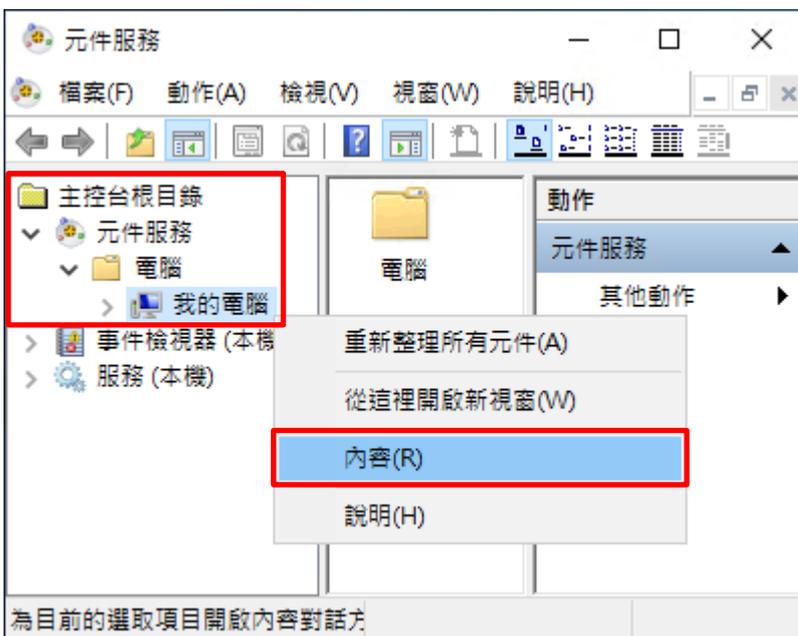
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



(3) 編輯電腦內容

展開 [主控台根目錄], [元件服務], [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



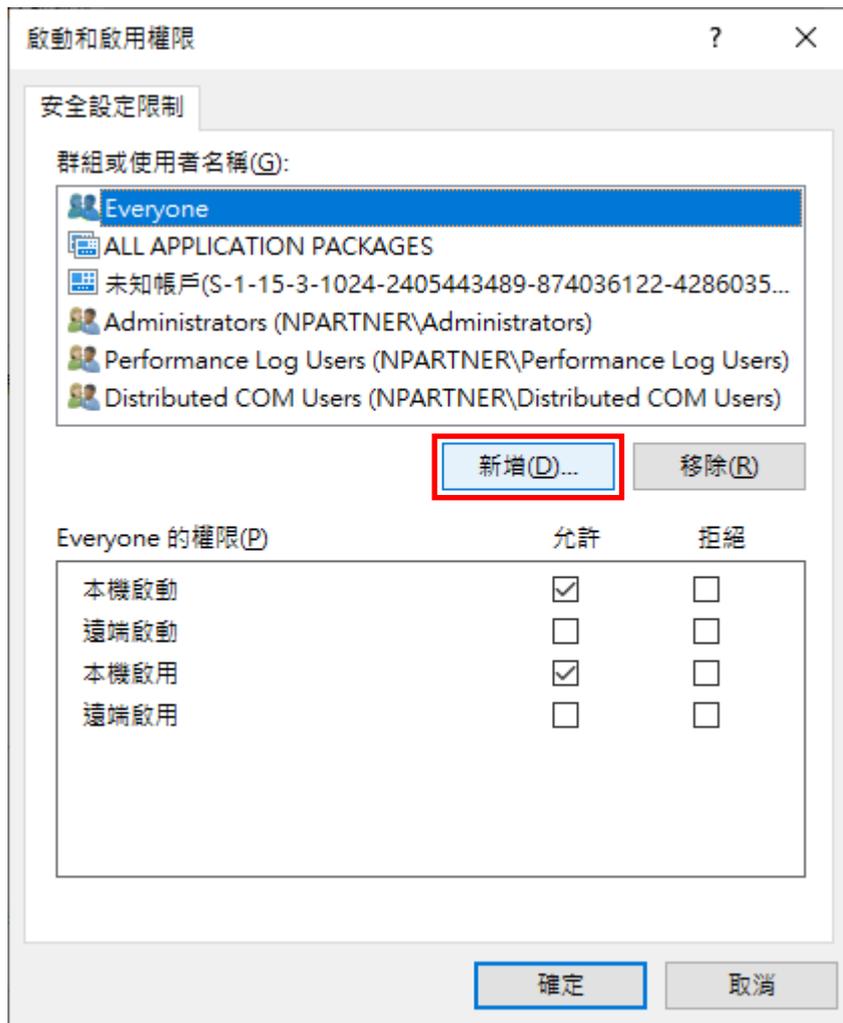
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



(5) 新增 DCOM 使用者權限

點選 [新增]



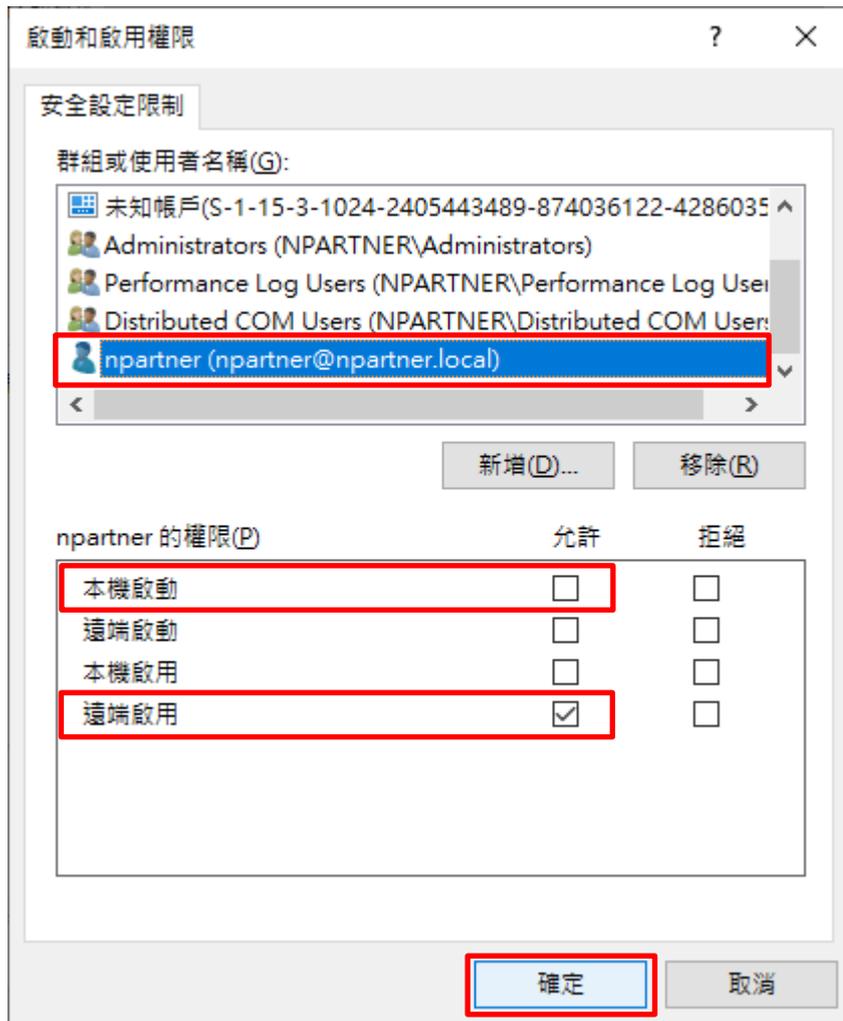
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



7.3.3 設定 WMI 權限

7.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



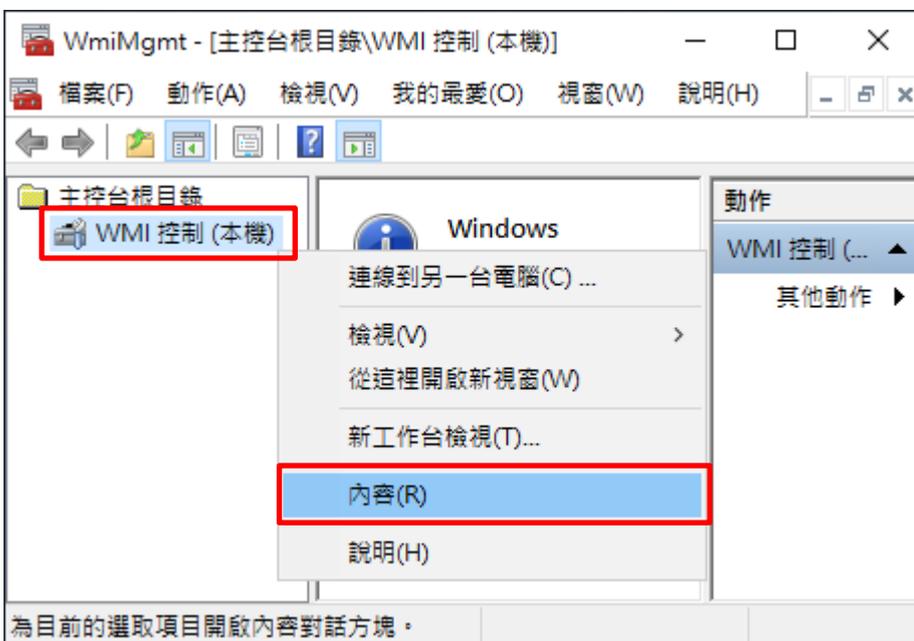
(2) 開啟元件服務

PS C:\> `wimgmt.msc`



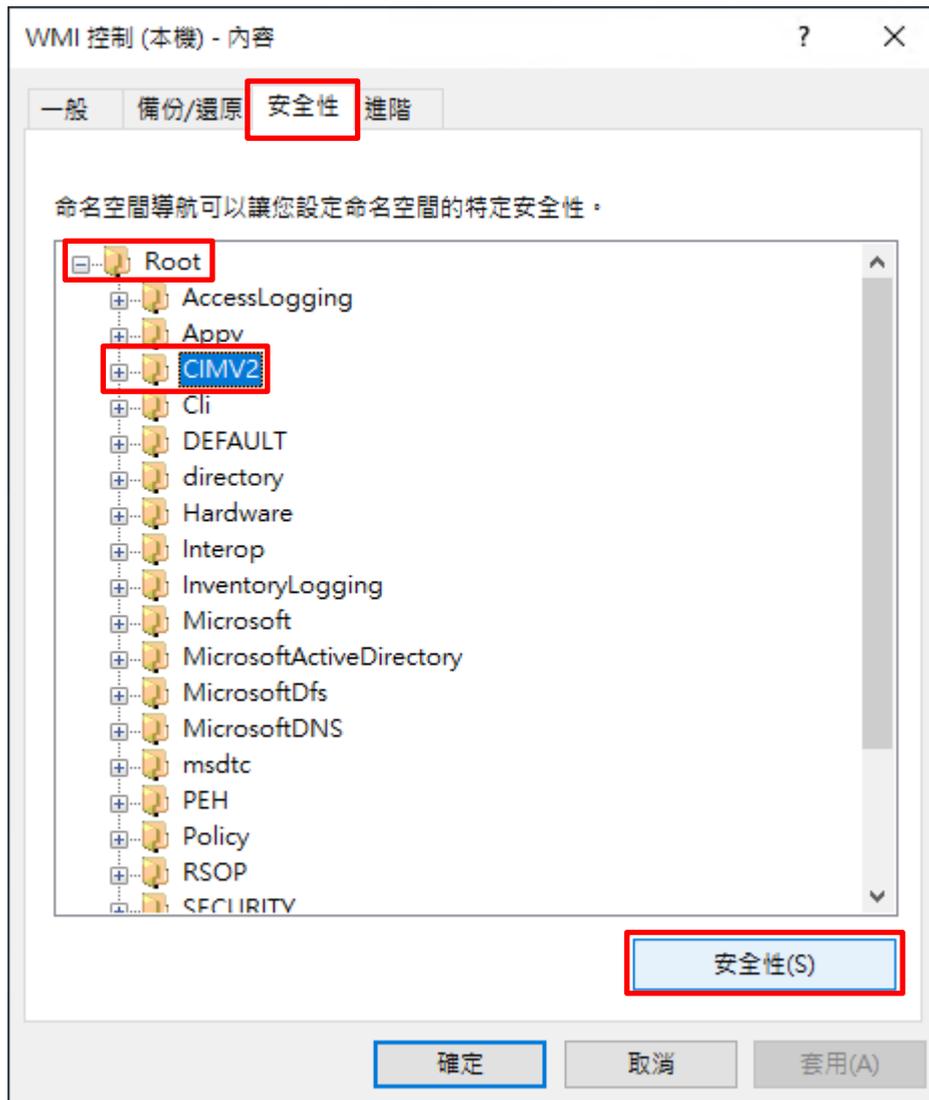
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



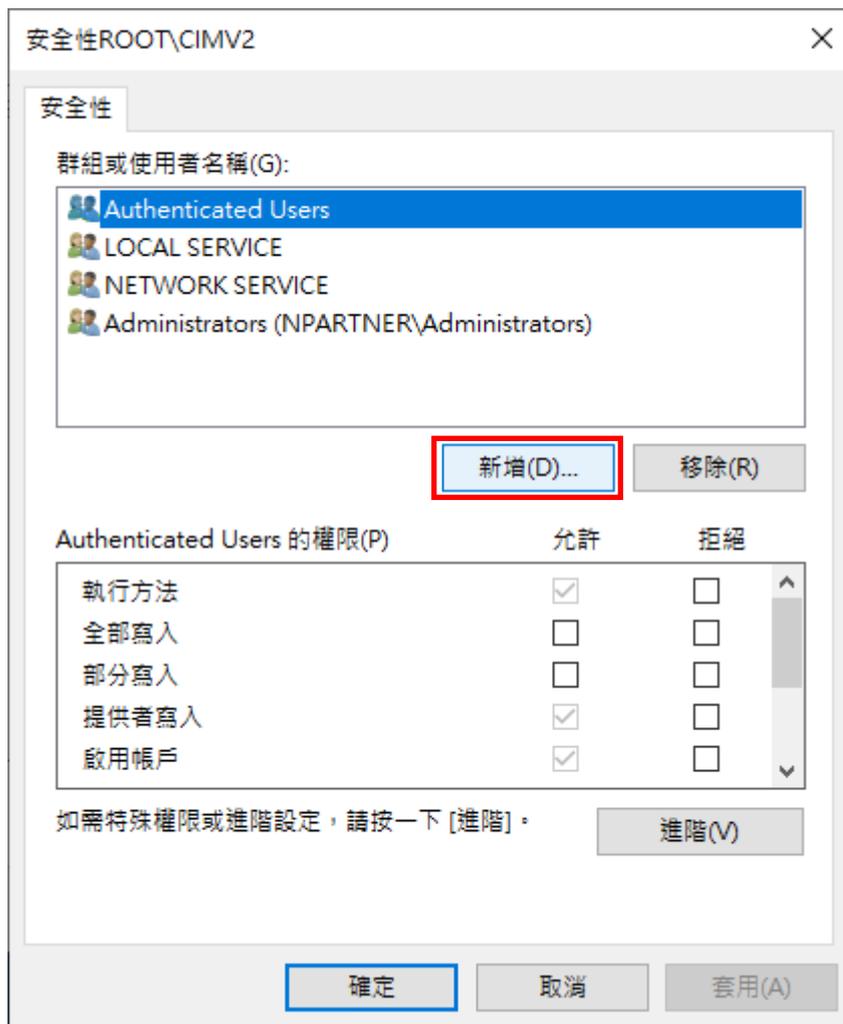
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [CIMV2] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



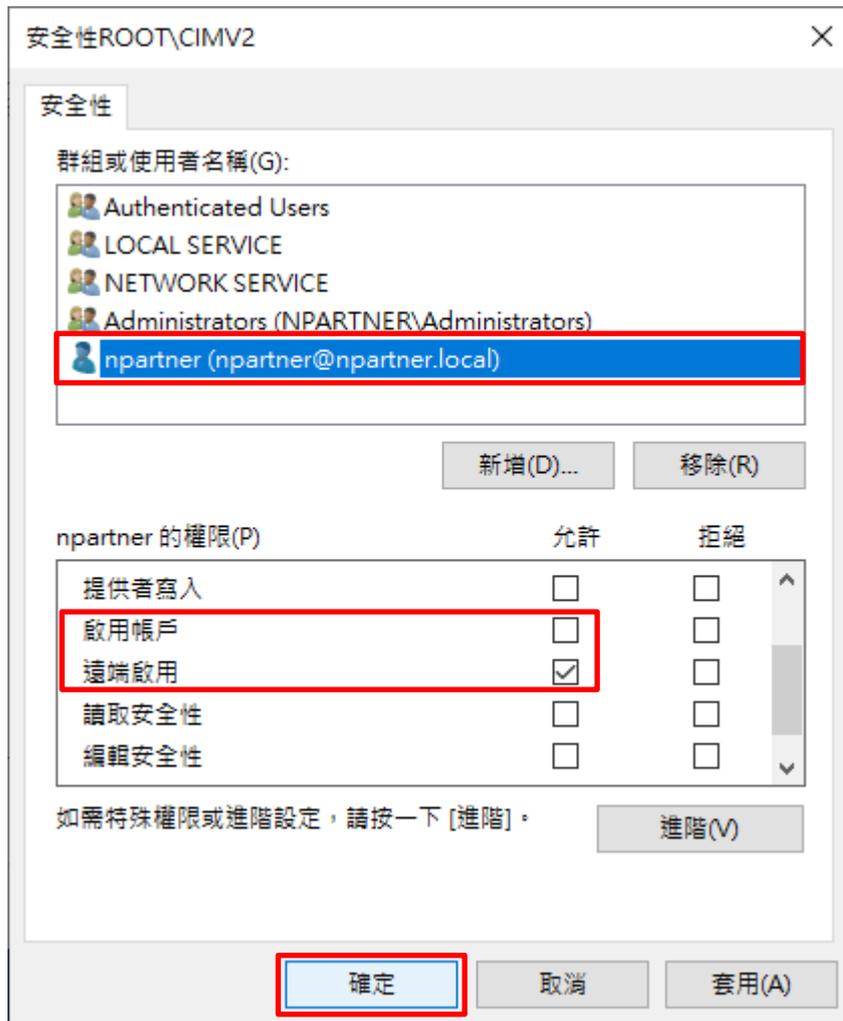
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



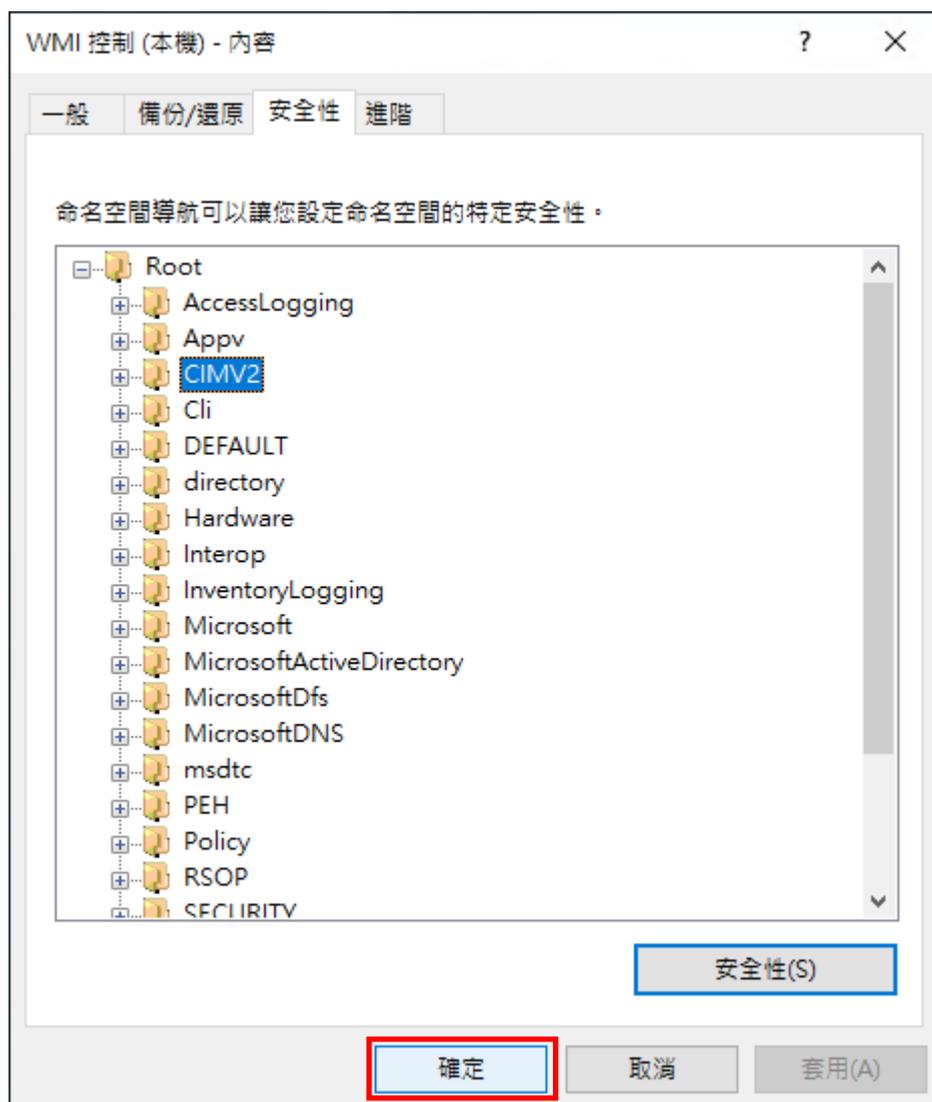
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



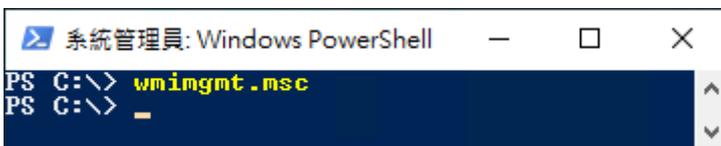
7.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



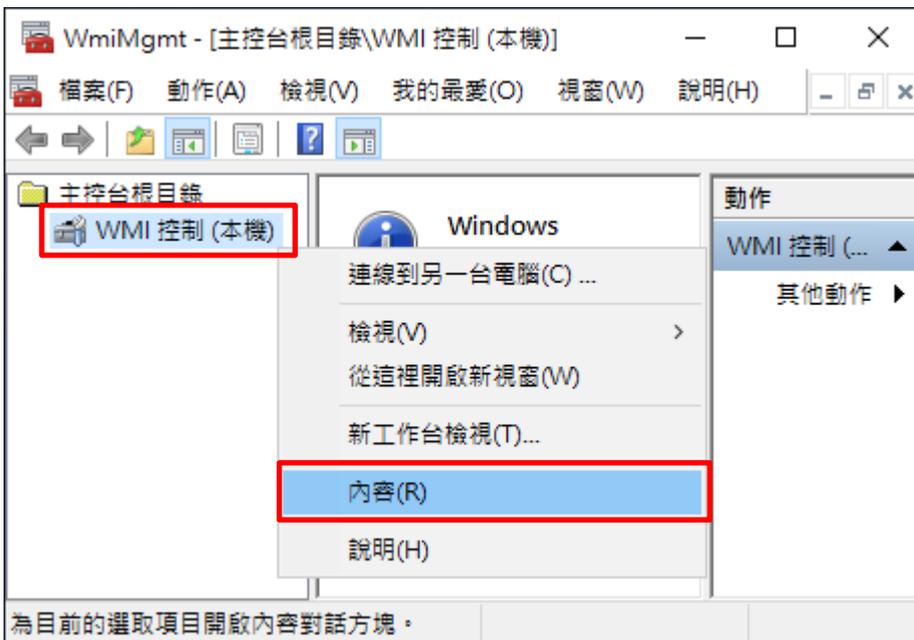
(2) 開啟元件服務

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



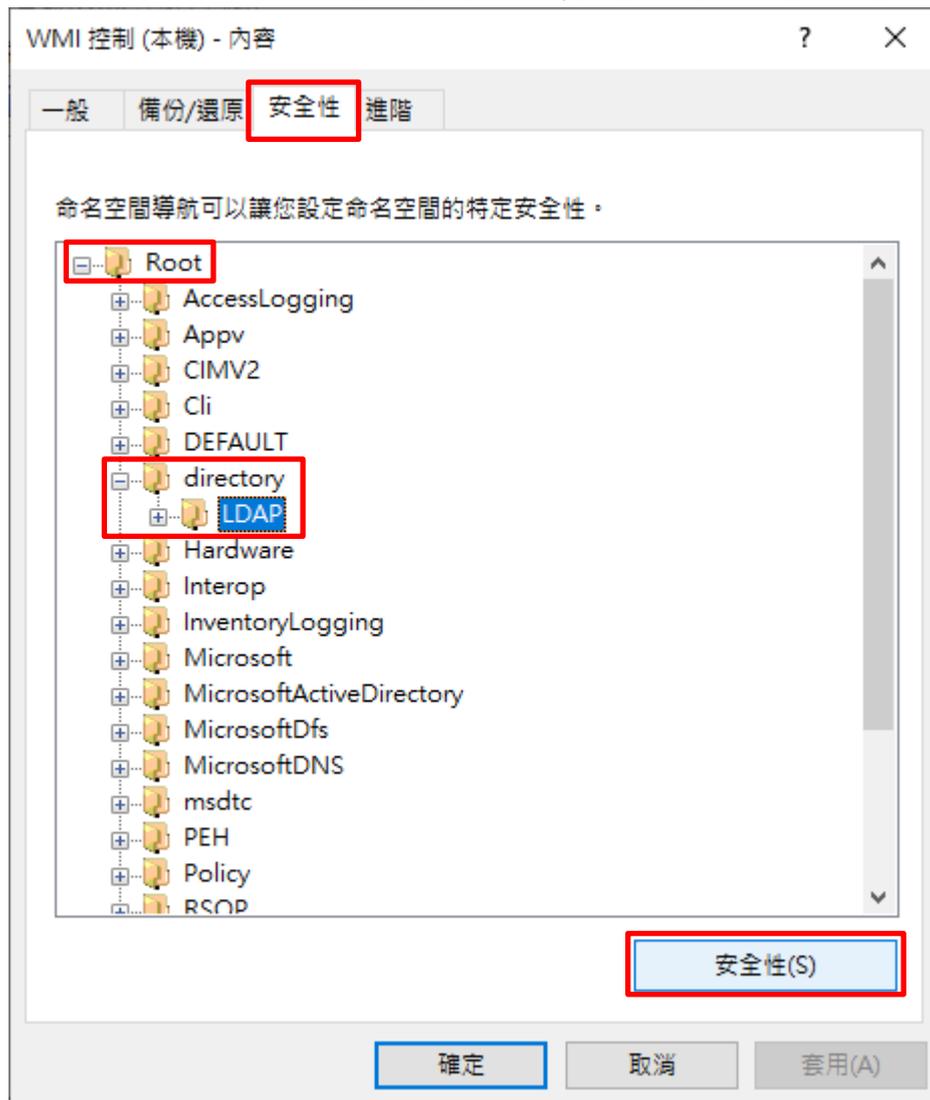
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



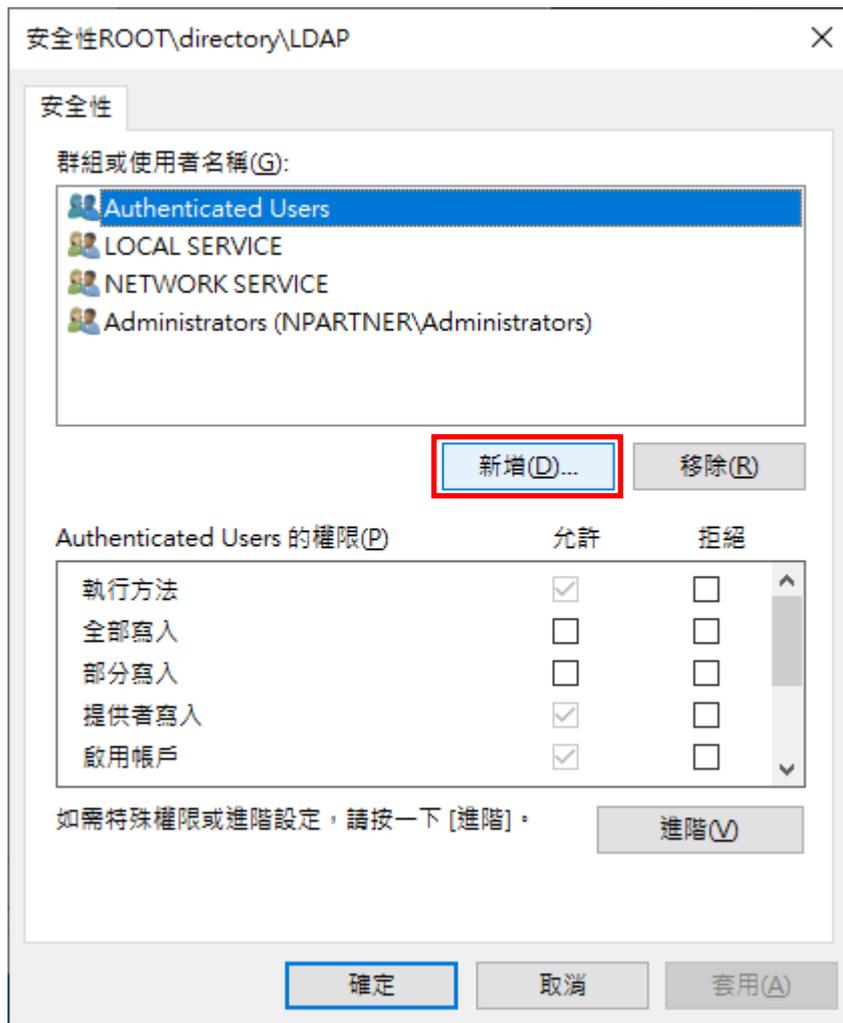
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



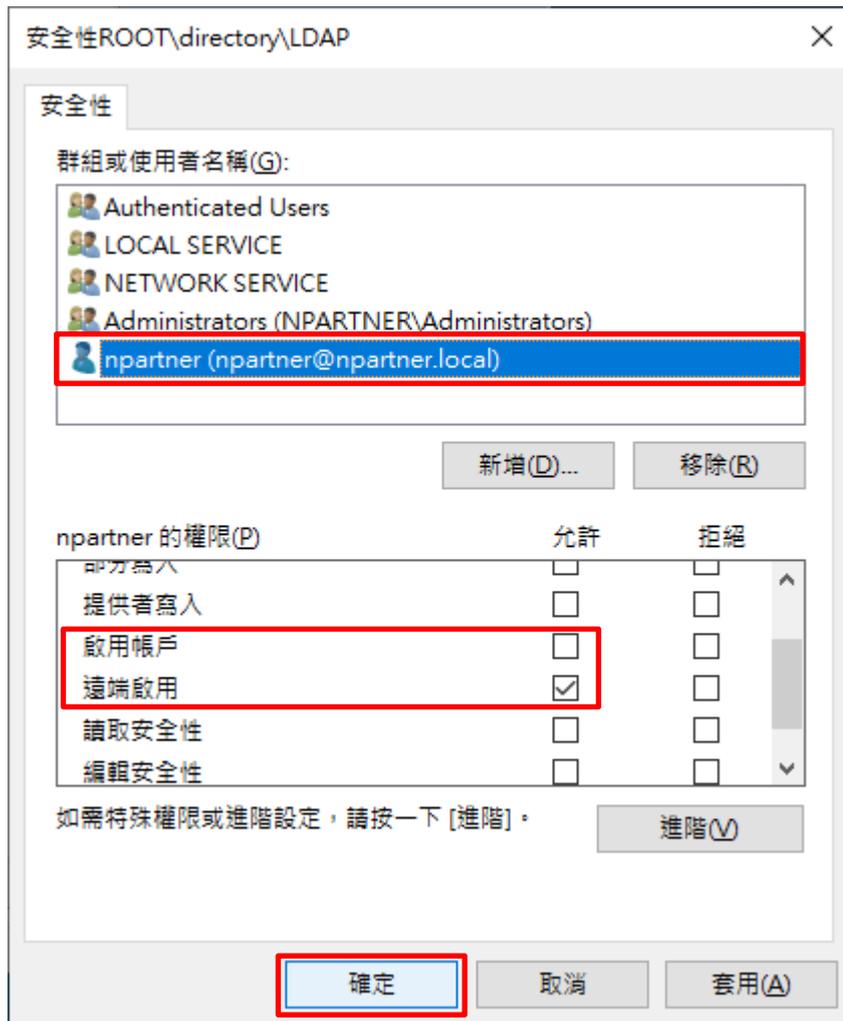
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



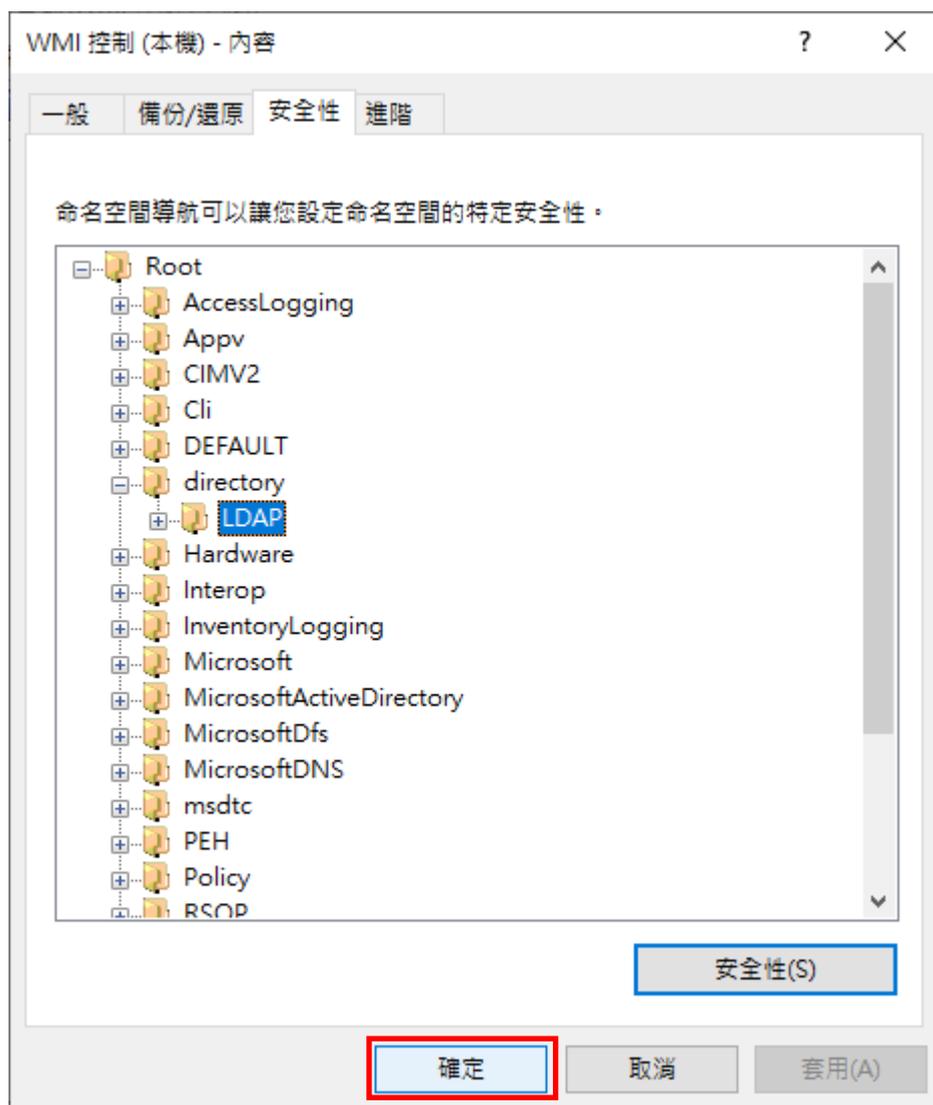
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



7.3.4 設定 Event log 讀取權限

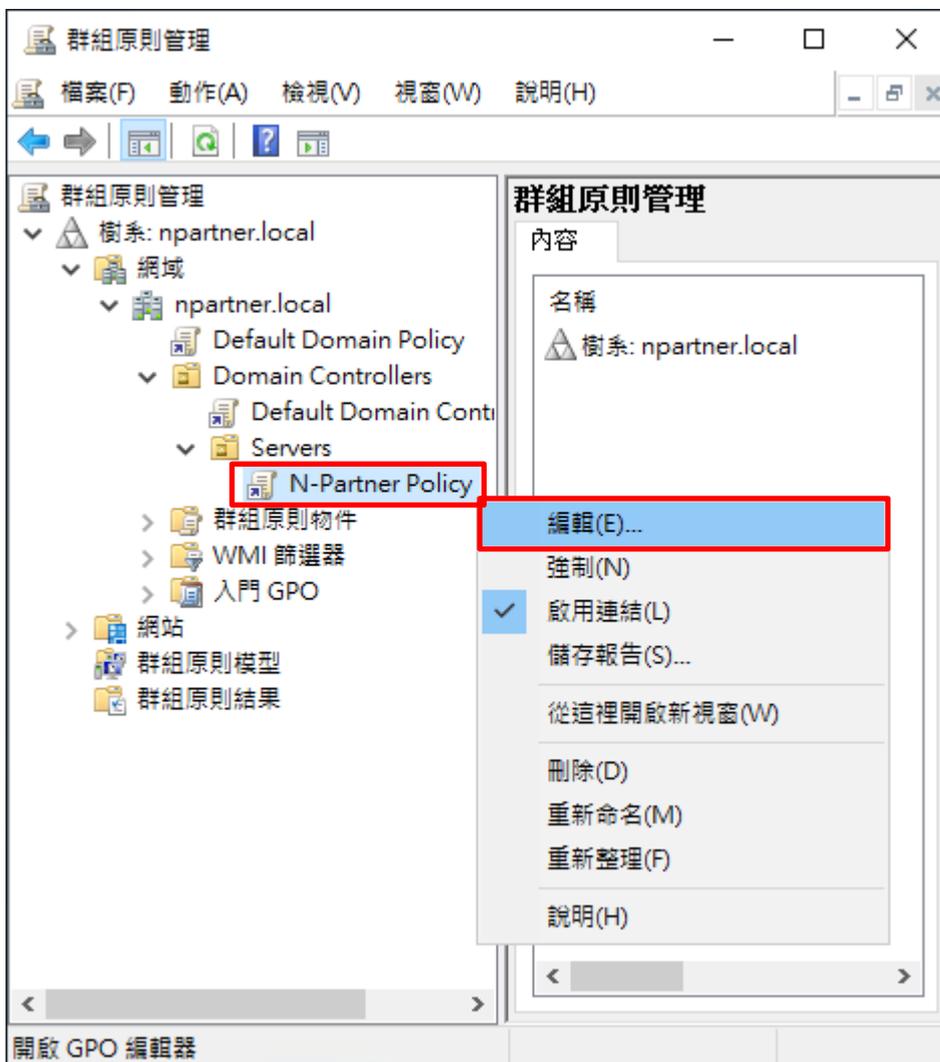
(1) 開啟群組原則管理

開啟 [群組原則管理]



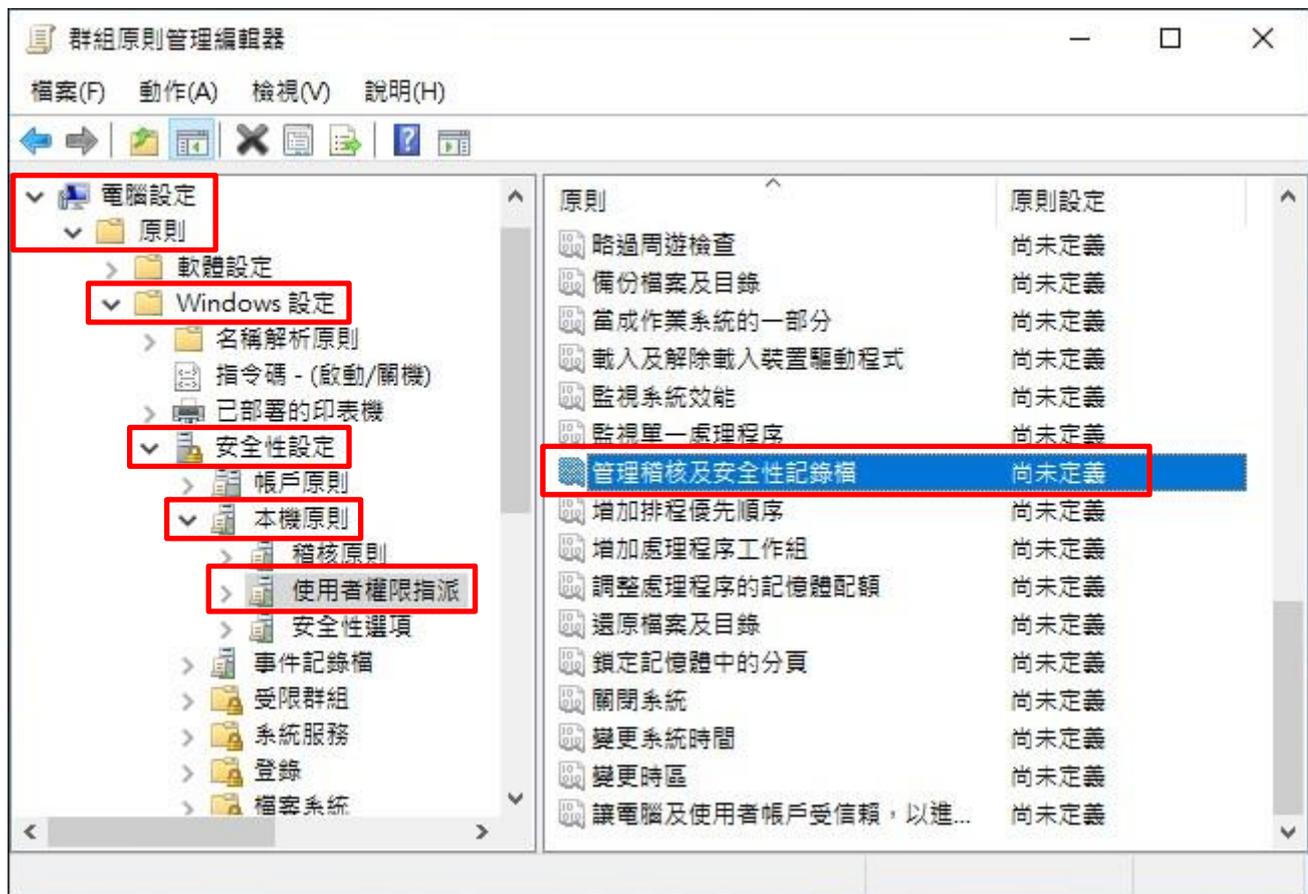
(2) 編輯群組原則物件

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



(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全性記錄檔] 項目



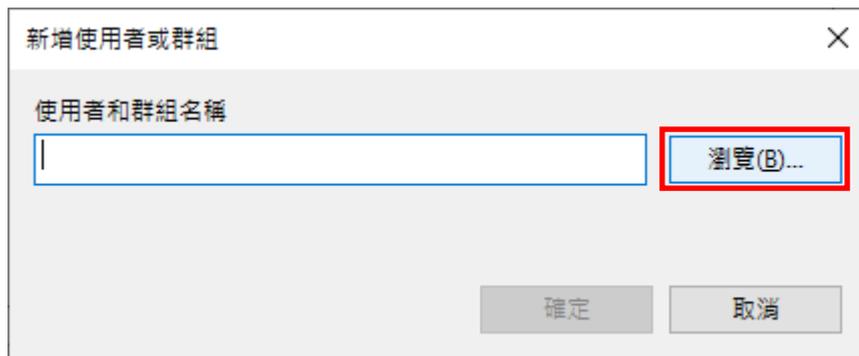
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、服務帳戶、群組或內建安全性主體 物件類型(O)...

從這個位置(F):
npartner.local 位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local) 檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

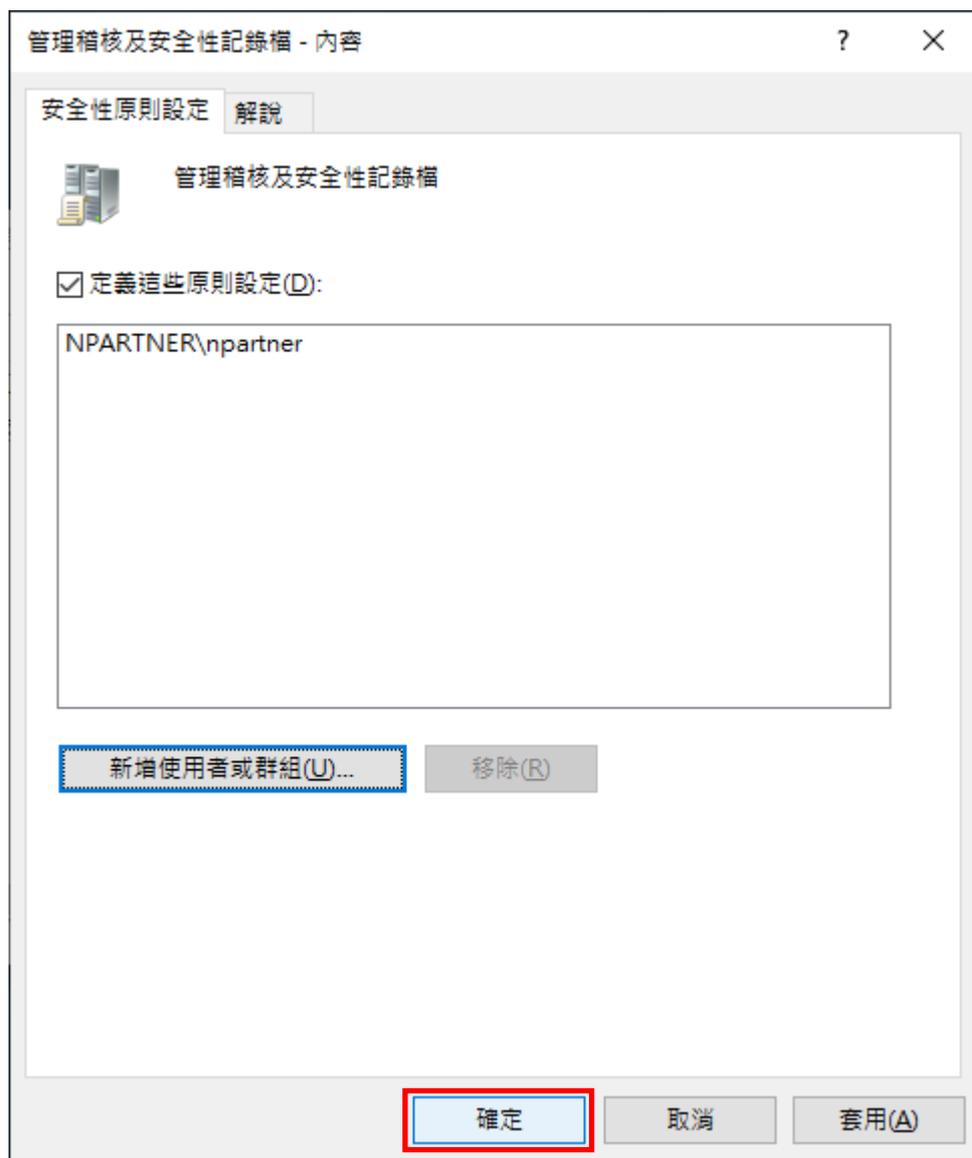
新增使用者或群組

使用者和群組名稱
NPARTNER\npartner 瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]



(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

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



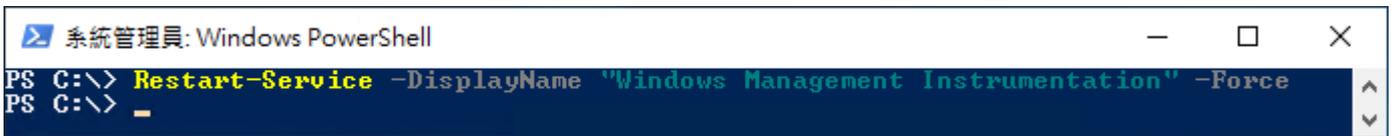
7.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



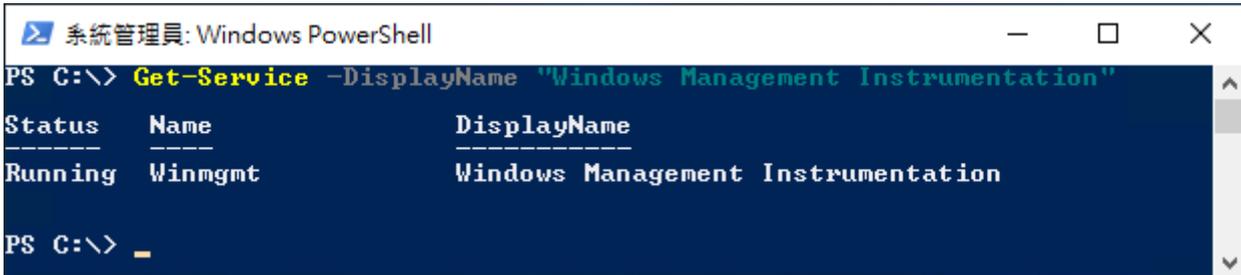
(2) 重啟 WMI 服務

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



7.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

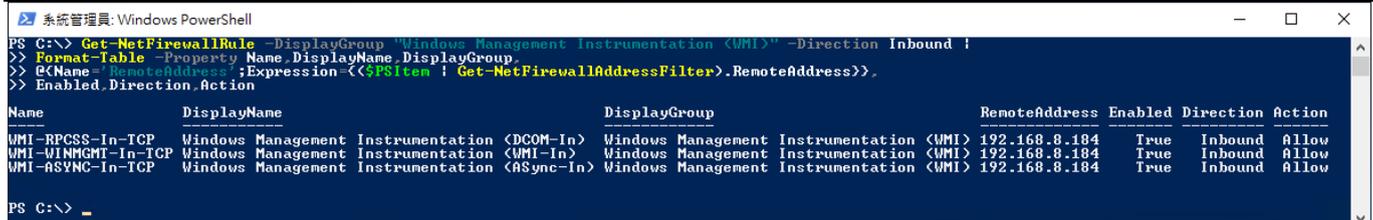
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```

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: `Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True`. The output is a single line: `PS C:\> _`.

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |  
>> Format-Table -Property Name,DisplayName,DisplayGroup,  
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},  
>> Enabled,Direction,Action
```

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-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound | Format-Table -Property Name,DisplayName,DisplayGroup, @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}}, Enabled,Direction,Action`. The output is a table with the following data:

Name	DisplayName	DisplayGroup	RemoteAddress	Enabled	Direction	Action
WMI-RPCSS-In-TCP	Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow
WMI-WINMGMT-In-TCP	Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow
WMI-ASYNC-In-TCP	Windows Management Instrumentation (ASync-In)	Windows Management Instrumentation (WMI)	192.168.8.184	True	Inbound	Allow

The terminal prompt ends with `PS C:\> _`.

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](#)

8.1 組織單位設定

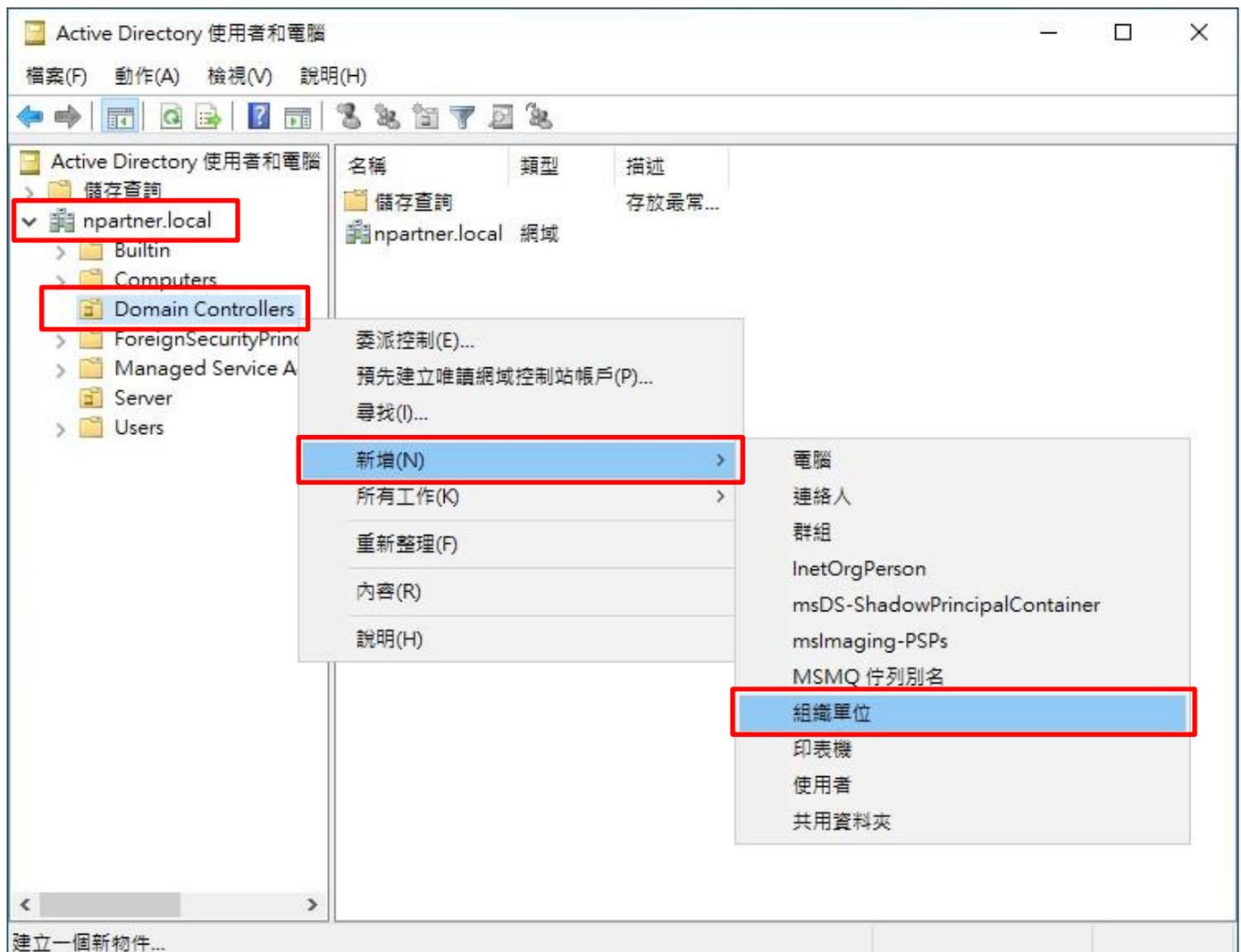
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



(2) 新增組織單位

在 [網域名稱] 的 [Domain Controllers] 組織單位，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/Domain Controllers

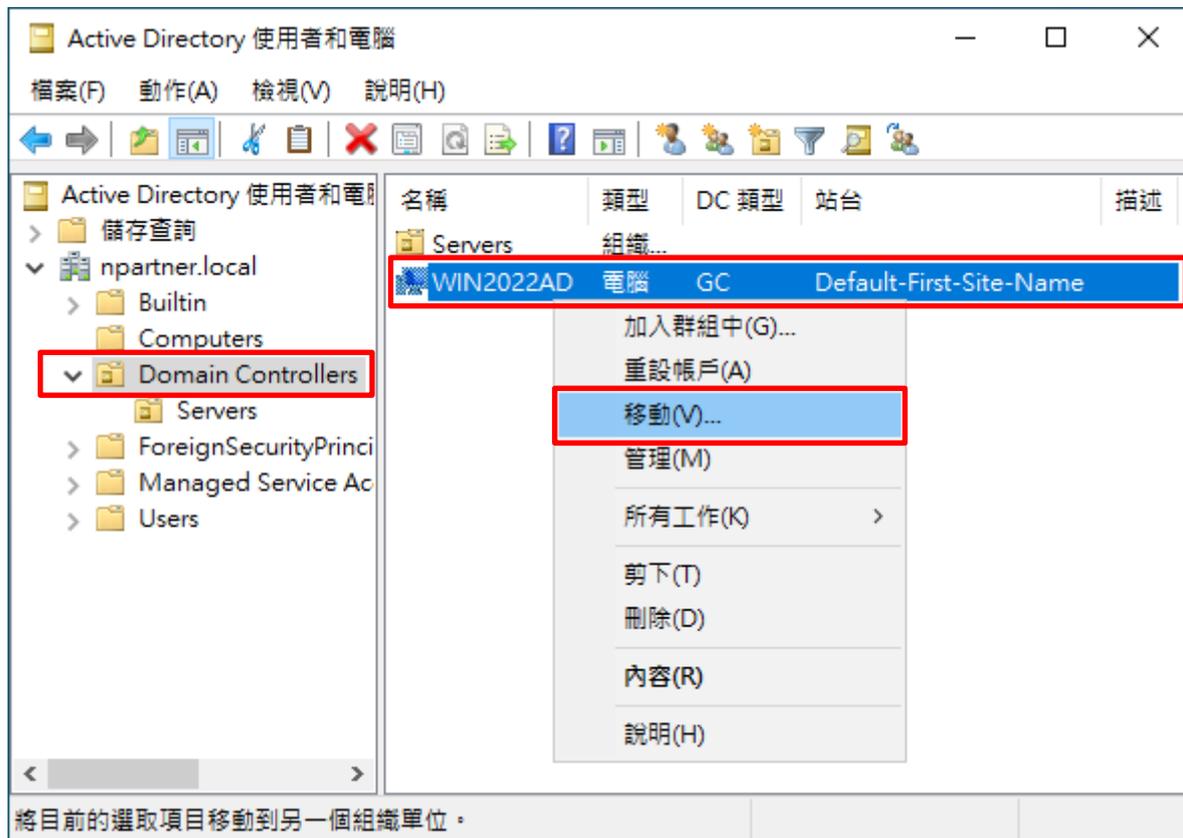
名稱(A):
Servers

保護容器以防止被意外刪除(P)

確定 取消 說明

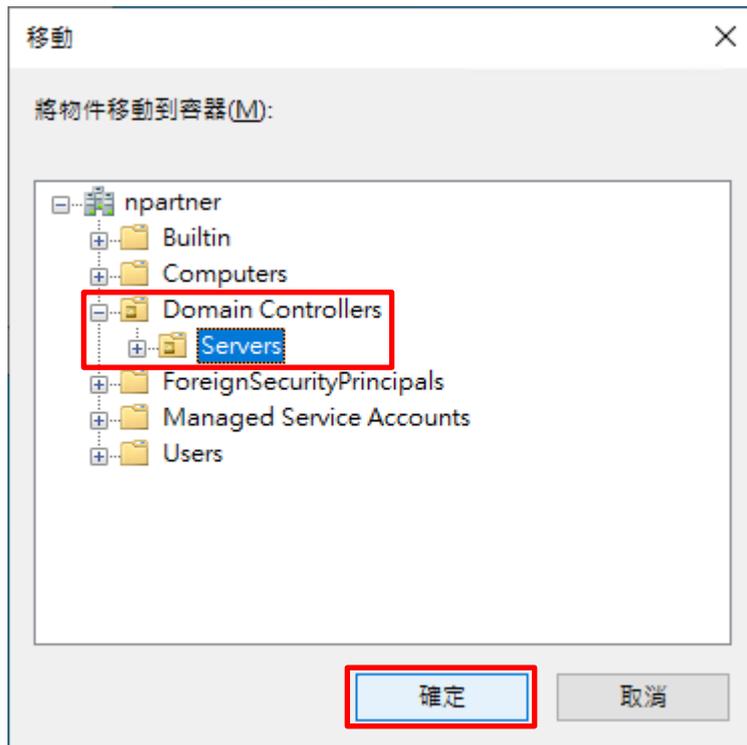
(4) 移動伺服器至新的組織單位

選擇 [Domain Controllers] 組織單位 -> 在 [Win2022AD] 網域伺服器，按滑鼠右鍵註：請依客戶環境選擇 Windows AD 主機 -> 點選 [移動]



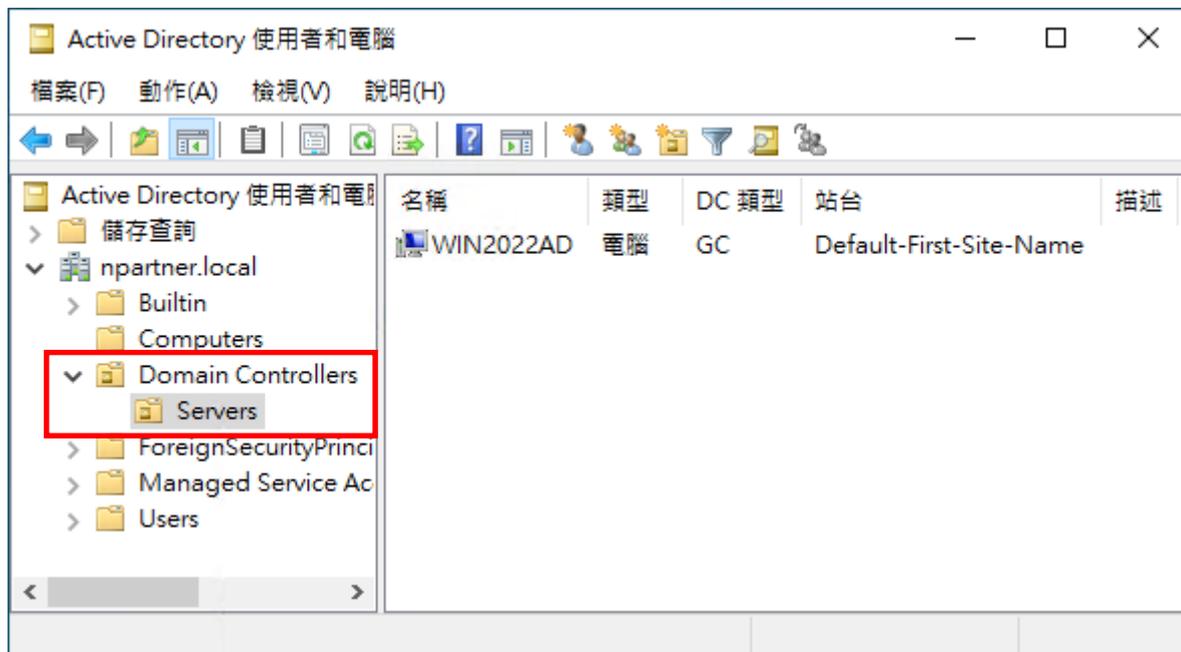
(5) 選擇組織單位

選擇 [Domain Controllers] 的 [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 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2022AD] 網域伺服器已移動。



8.2 群組原則設定

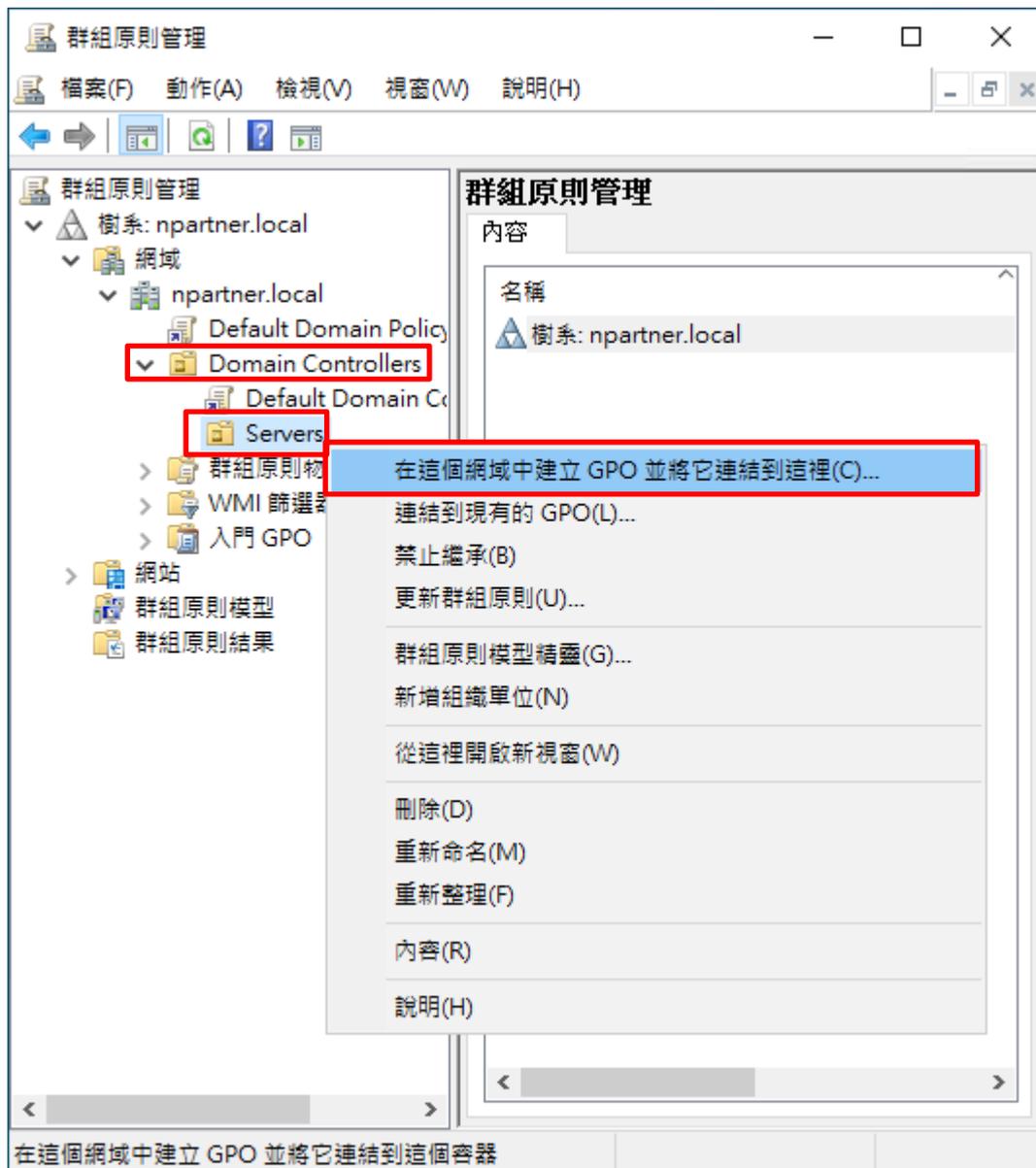
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

在 [Domain Controllers] 的 [Servers] 組織單位，按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並將它連結到這裡...]



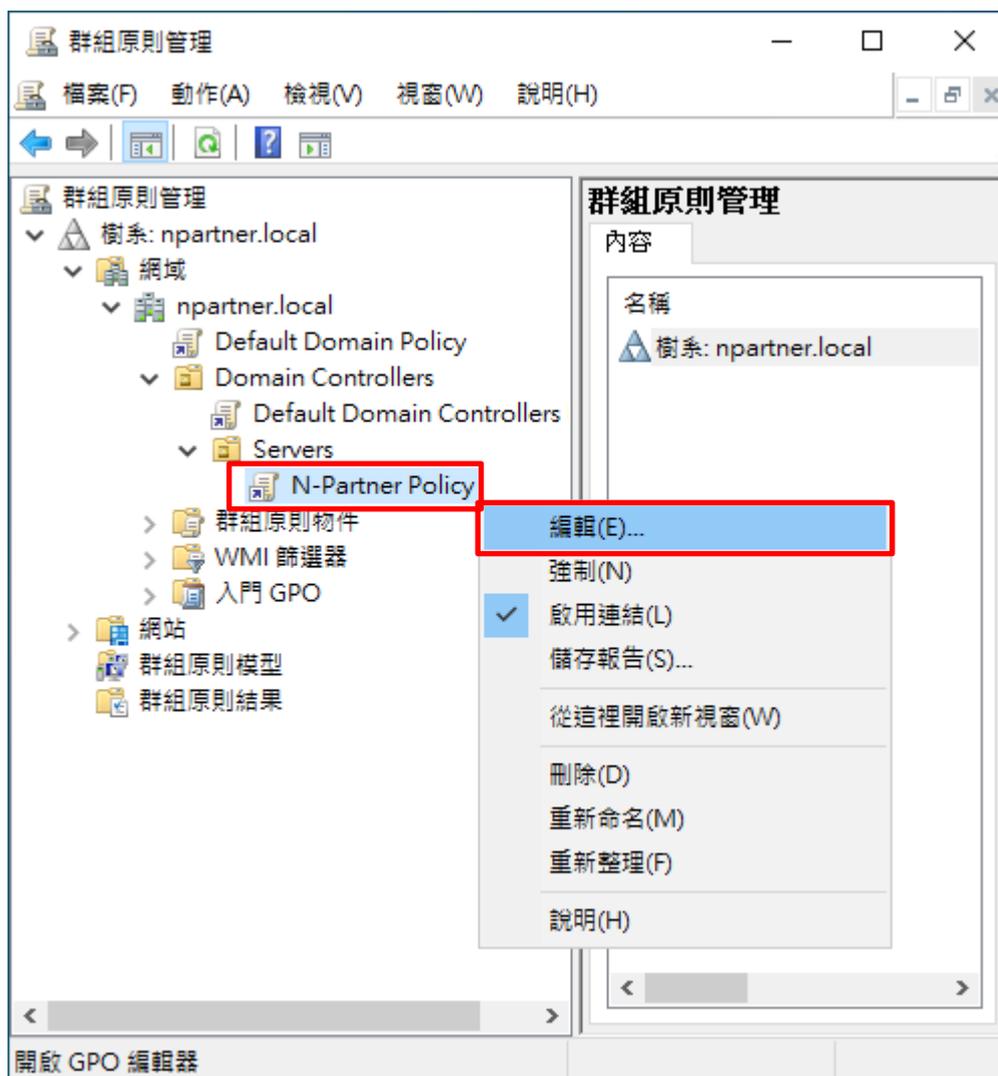
(3) 輸入群組原則物件名稱

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]



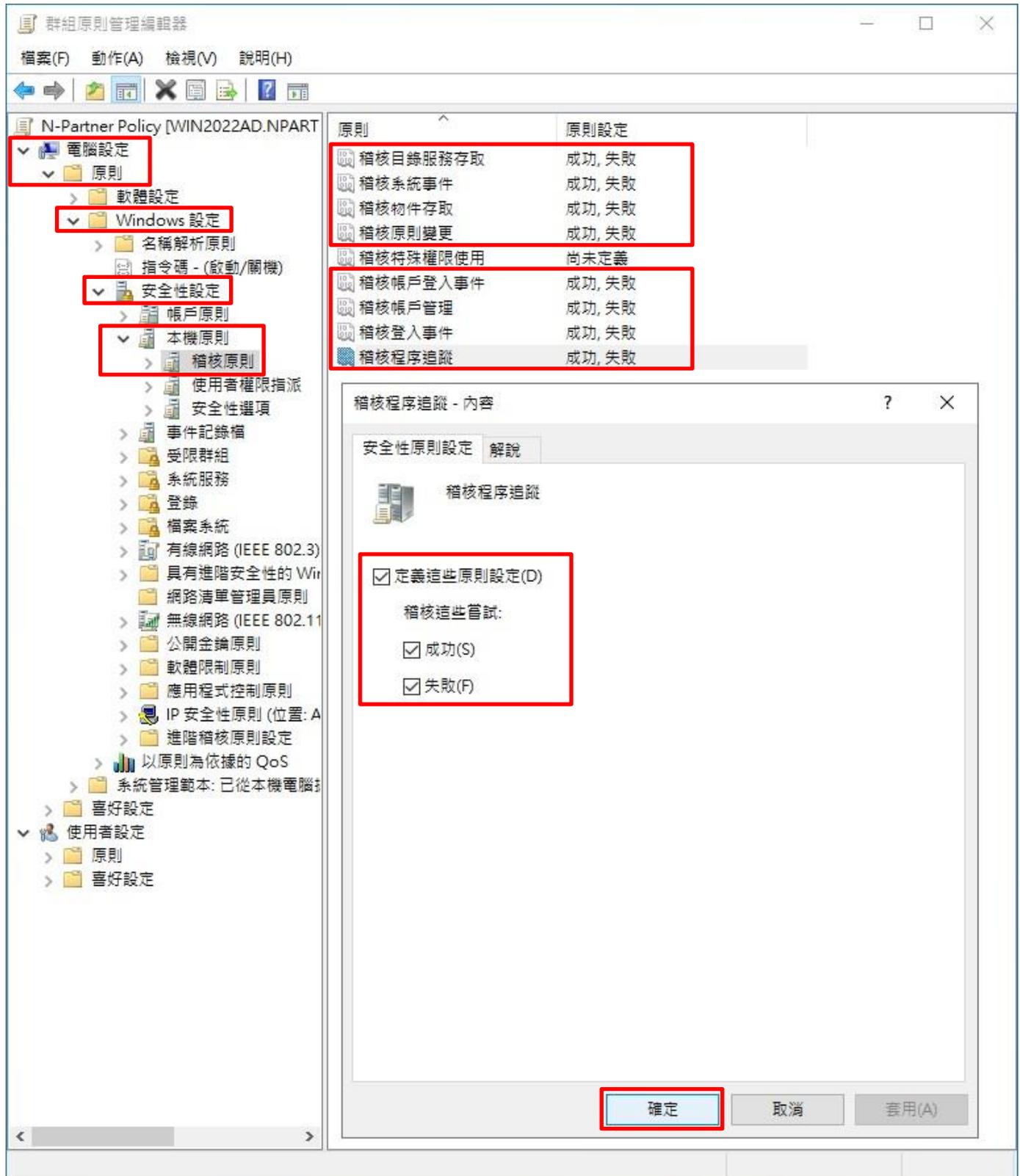
(4) 編輯群組原則物件

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 [稽核目錄服務存取], [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]

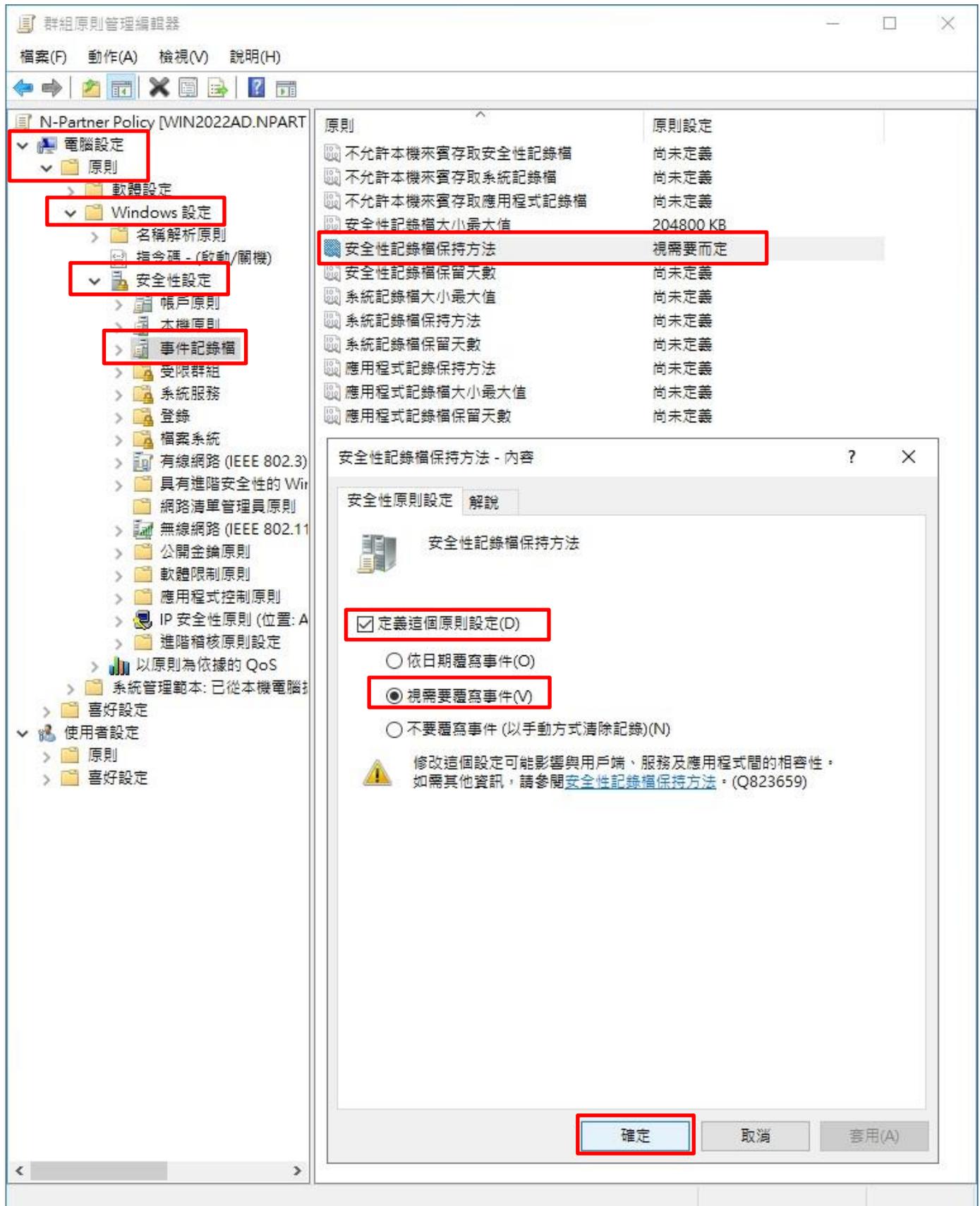
The screenshot shows the Group Policy Management Editor window for 'N-Partner Policy [WIN2022AD.NPART]'. The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log Settings). The 'Maximum size of security event logs' policy is selected and highlighted in red. The right-hand pane shows the policy details, with the value '204800 KB' also highlighted in red.

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

The 'Maximum size of security event logs - Content' dialog box is open, showing the 'Security Policy Settings' tab. The 'Define this policy setting (D)' checkbox is checked and highlighted in red. The value '204800' is entered in the text box, with 'KB' selected in the units dropdown, also highlighted in red. A warning icon and text are visible below the input field: '修改這個設定可能影響與用戶端、服務及應用程式間的相容性。如需其他資訊，請參閱[安全性記錄檔大小最大值](#)。(Q823659)'. The '確定' (OK) button is highlighted in red at the bottom of the dialog.

(7) 事件記錄檔：安全性記錄檔保持方法

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



(8) 開啟 [Windows PowerShell]



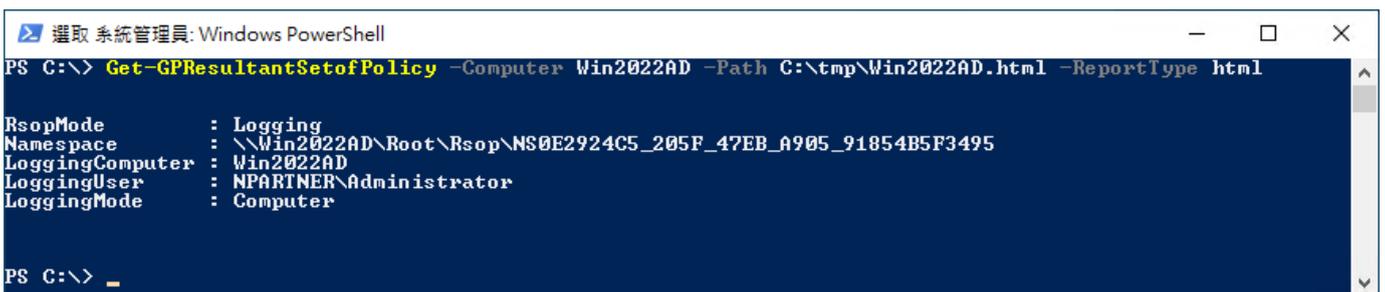
(9) 更新群組原則

```
PS C:\> Invoke-GPUUpdate -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-GPUUpdate -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt returns to `PS C:\>`.

(10) 產生 Windows AD 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2022AD -Path C:\tmp\Win2022AD.html -ReportType html
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "選取 系統管理員: Windows PowerShell". The command prompt shows the command `Get-GPResultantSetofPolicy -Computer Win2022AD -Path C:\tmp\Win2022AD.html -ReportType html` being entered and executed. The output is as follows:
`RsopMode : Logging`
`Namespace : \\Win2022AD\Root\Rsop\NS0E2924C5_205F_47EB_A905_91854B5F3495`
`LoggingComputer : Win2022AD`
`LoggingUser : NPARTNER\Administrator`
`LoggingMode : Computer`
The prompt returns to `PS C:\>`.

紅色文字部位請輸入 Windows AD 伺服器名稱和資料夾路徑檔案名稱

(11) 開啟報表，確認 Windows AD 2022 伺服器，套用 N-Partner Policy 群組原則

群組原則結果

群組: NPARTNER\WIN2022AD

資料收集: 2022/3/9 下午 04:26:05

電腦詳細資料

全部顯示

一般

元件狀態

設定

原則

Windows 設定

安全性設定

帳戶原則/密碼規則

帳戶原則/帳戶鎖定原則

帳戶原則/Kerberos 原則

本機原則/稽核原則

原則	設定	優勢 GPO
稽核目錄服務存取	成功, 失敗	N-Partner Policy
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/使用者權限指派

本機原則/安全性選項

事件記錄檔

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

公開金鑰原則/加密檔案系統

群組原則物件

WMI 篩選器

使用者詳細資料

8.3 設定 WMI

註：設定 WMI 是在 N-Reporter [事件查詢] 的 [使用者名稱] 欄位關聯 Windows 帳號相關資訊

(1) 查看 N-Reporter 會關聯 Windows AD 是否有使用者資料

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```

```

系統管理員: Windows PowerShell
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
DisplayName           : KH
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department            : TAC
EmployeeID            : 0032
EmployeeNumber        : A0032
PS C:\> _
    
```

紅色文字部位請依客戶環境輸入使用者名稱

(2) N-Reporter [事件查詢] -> 點選 使用者名稱

等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh	4724	Administrator	User Management

(3) 顯示使用者資料

事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 Account Name: Administrator Account Domain: NPARTNER0 Logon ID: 0x1A7B03 Target Account: Security ID: S-1-5-21-3283165886-1174691238-2893489689-1105 Account Name: kh Account Domain: NPARTNER0	1	audit	Administrator	kh (KH, TAC, 0032, (Engineer))	4724	Administrator	User Management

8.3.1 新增非管理帳號

(1) 開啟 [Windows PowerShell 的 Active Directory 模組]



(2) 新增帳號

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner"
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local"
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force)
>> -PasswordNeverExpires $True -Enabled $True
PS C:\> _
```

紅色文字部位請輸入帳號密碼及網域資訊

(3) 查看帳號狀態

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

```
系統管理員: Windows PowerShell 的 Active Directory 模組
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
Name                    : npartner
ObjectClass              : user
ObjectGUID              : ce1fc82b-b66f-4888-a69d-119979335279
PasswordNeverExpires    : True
SamAccountName          : npartner
SID                     : S-1-5-21-2041781864-1685919884-1961877824-1105
Surname                 :
UserPrincipalName       : npartner@npartner.local

PS C:\> _
```

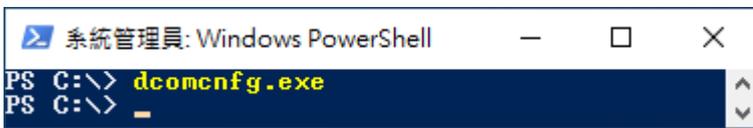
8.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



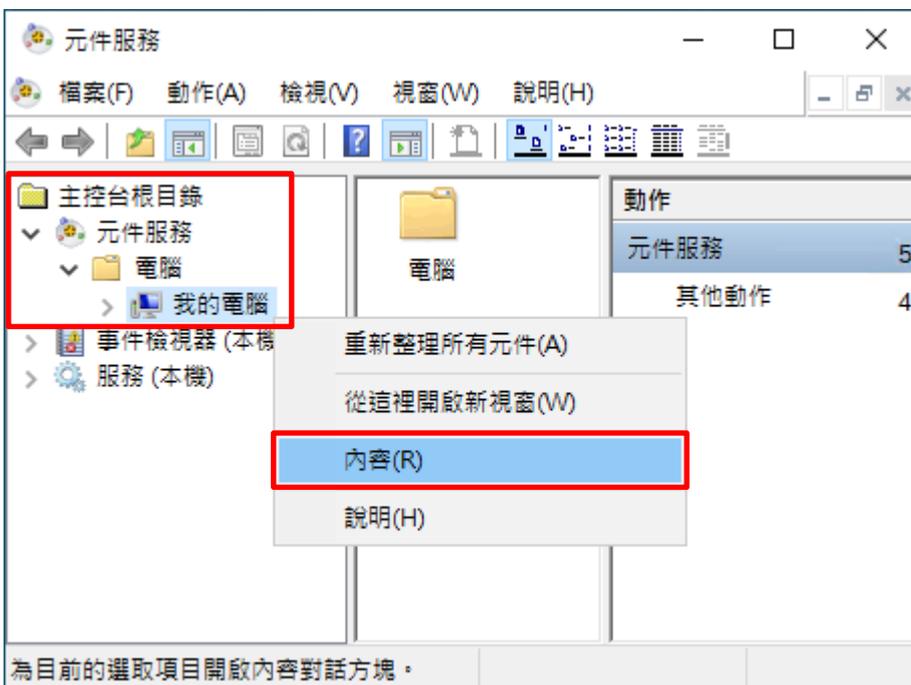
(2) 開啟元件服務

```
PS C:\> dcomcnfg.exe
```



(3) 編輯電腦內容

展開 [主控台根目錄], [元件服務], [電腦] -> 在 [我的電腦] 按滑鼠右鍵 -> 點選 [內容]



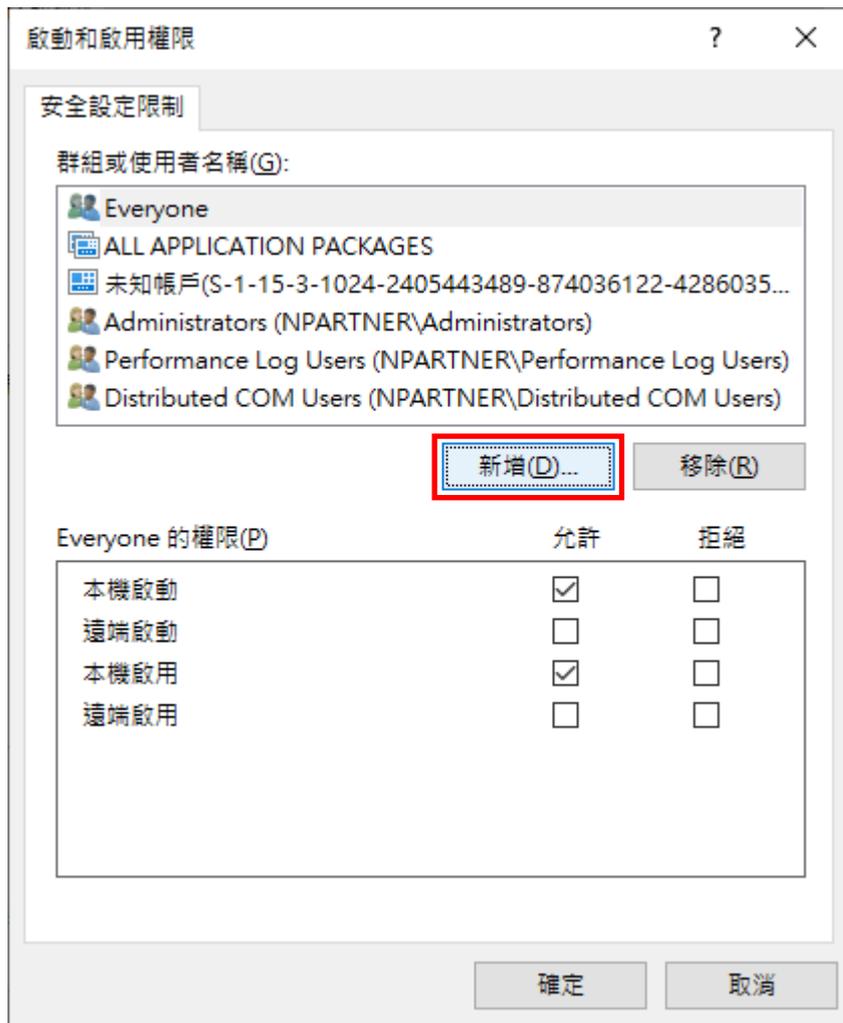
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



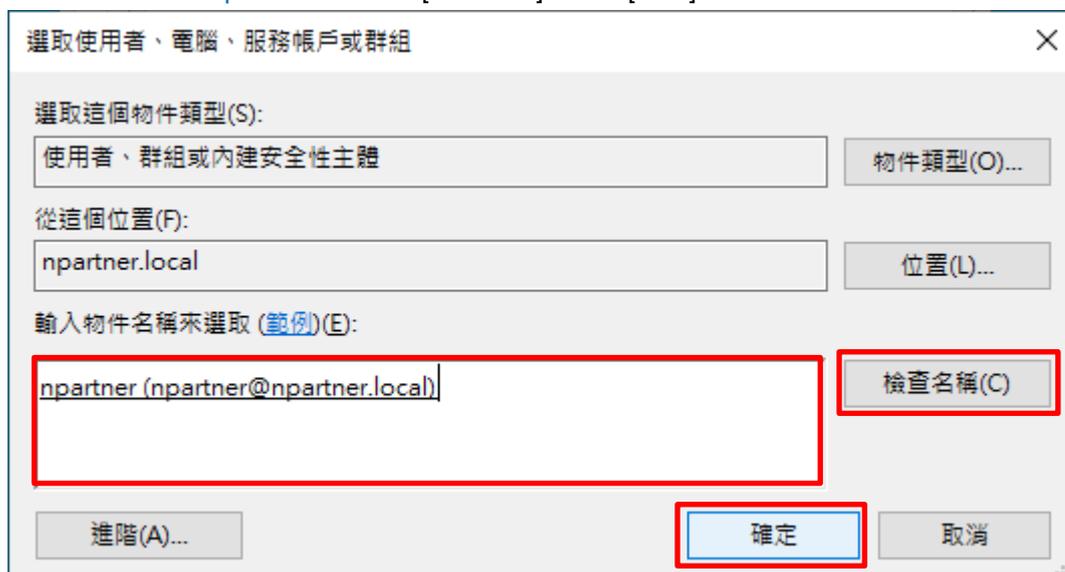
(5) 新增 DCOM 使用者權限

按 [新增]



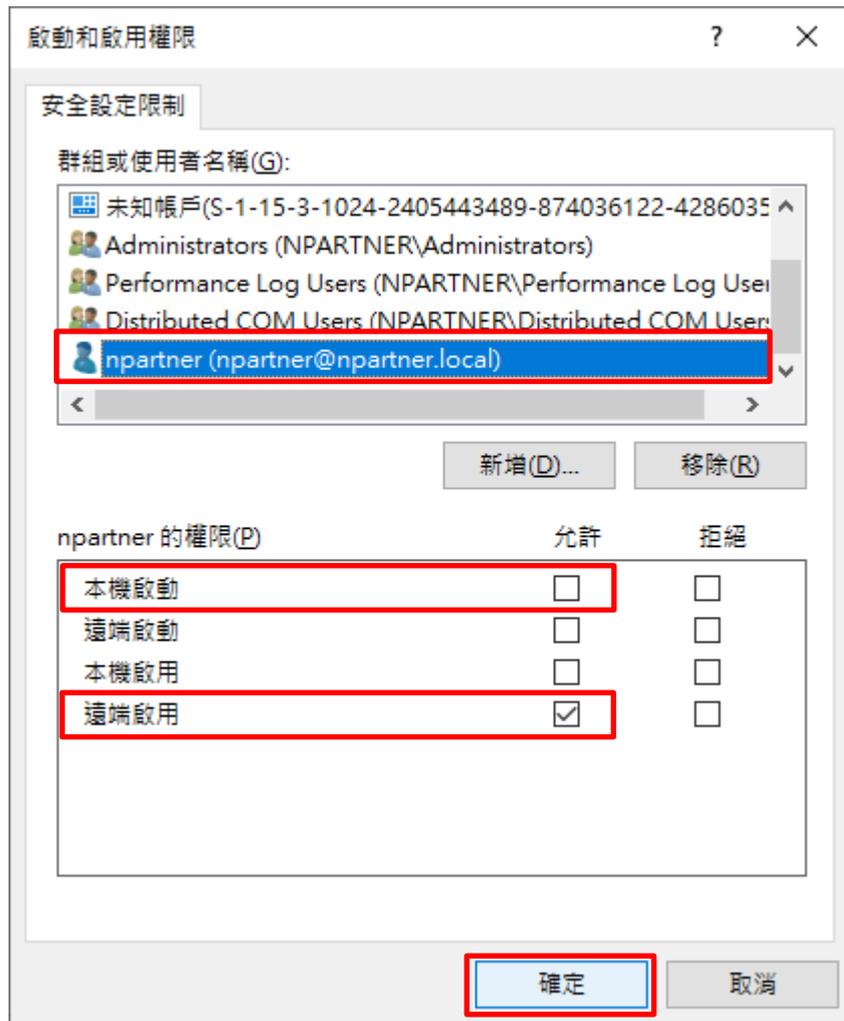
(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [本機啟動:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



8.3.3 設定 WMI 權限

8.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



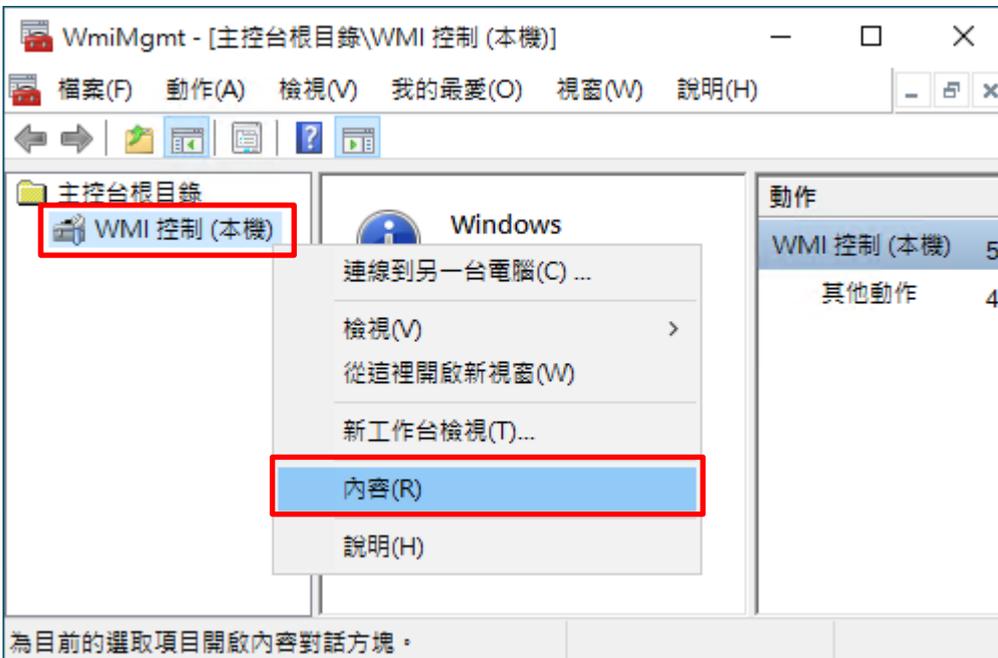
(2) 開啟元件服務

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



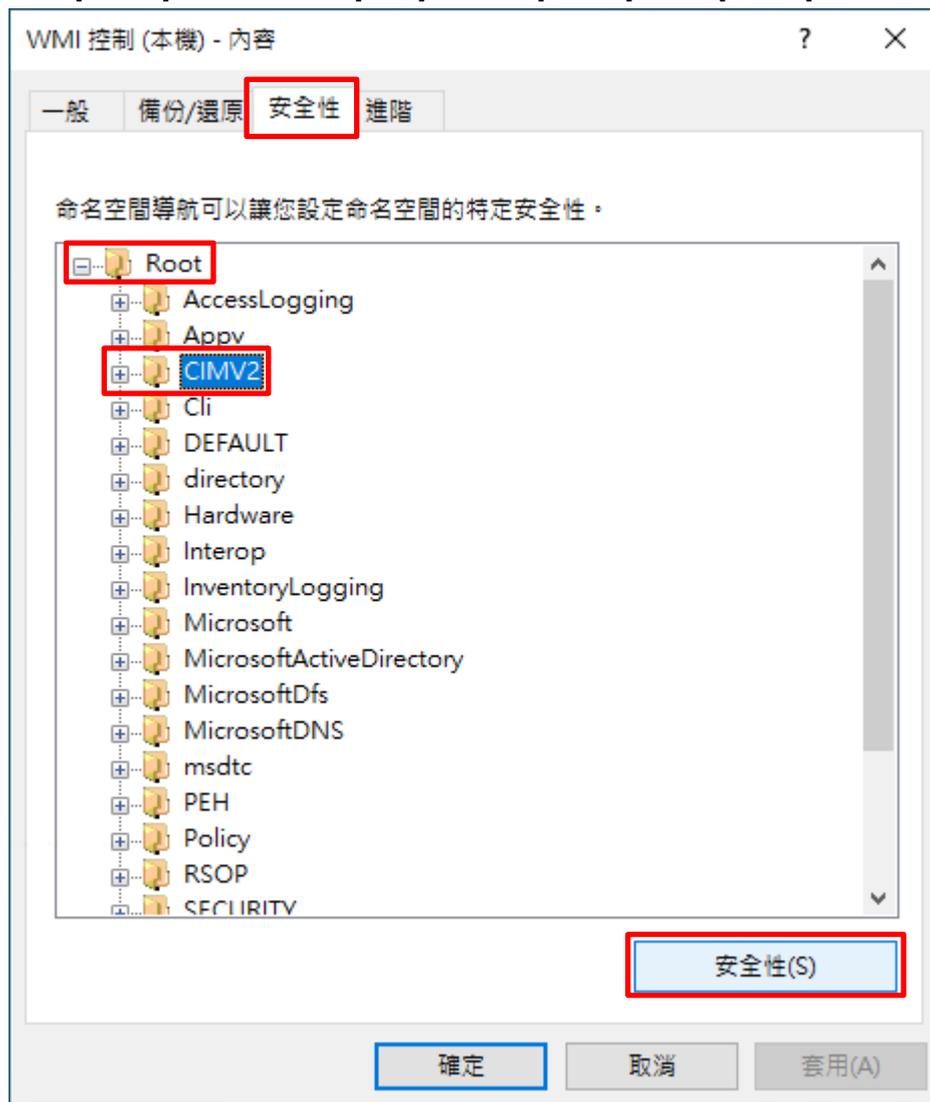
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



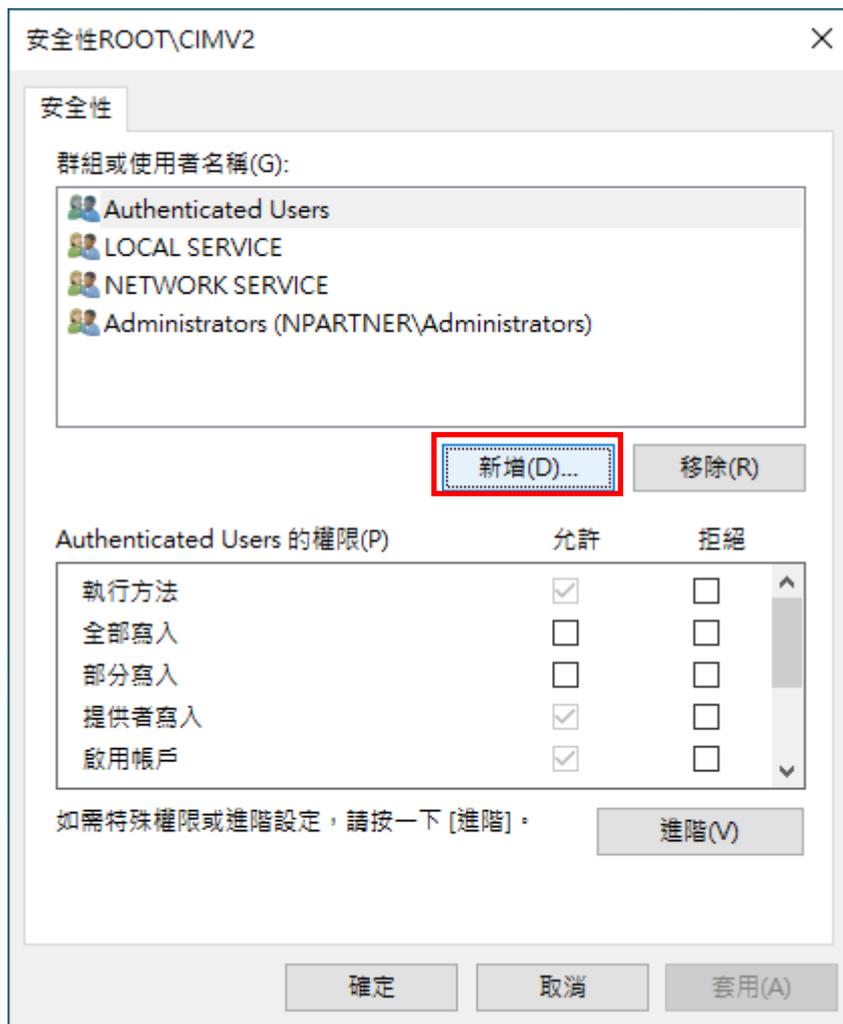
(4) 編輯 CIMV2 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> 點選 [CIMV2] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



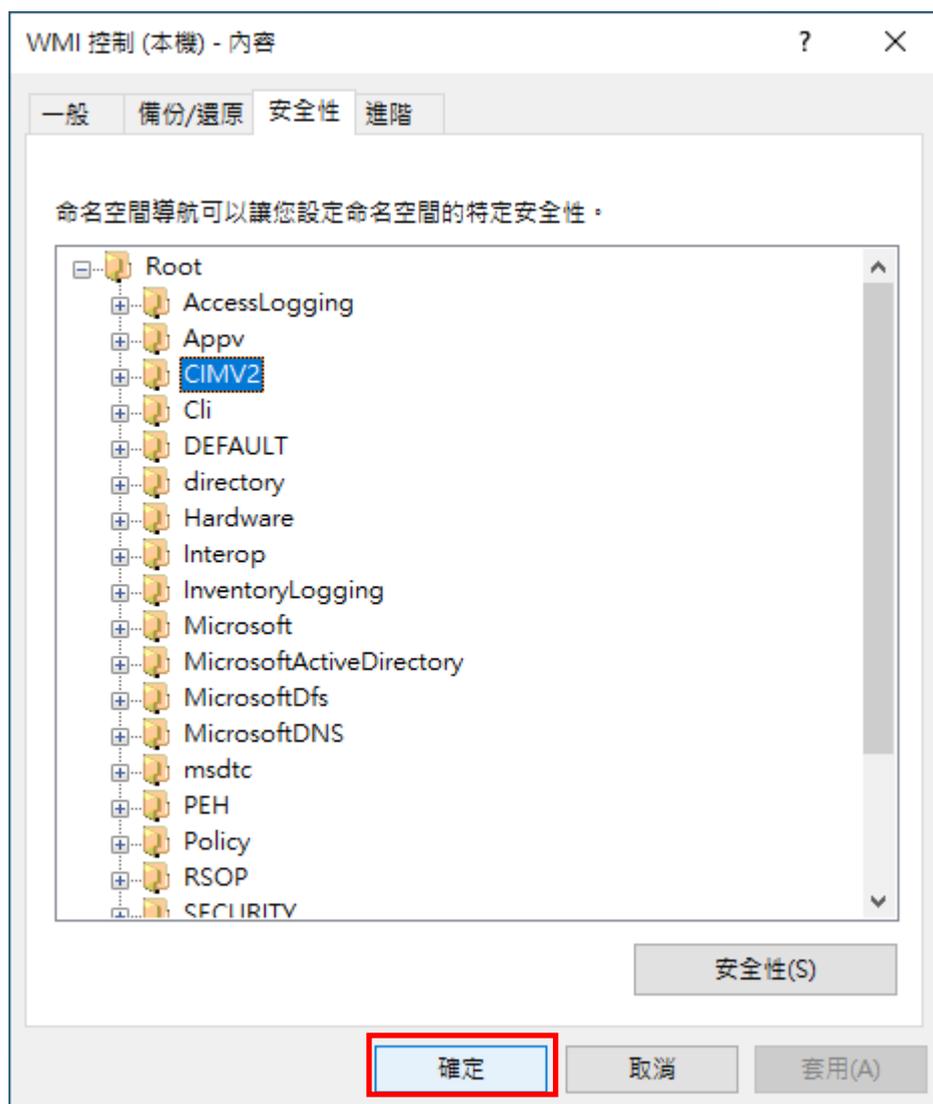
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



8.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



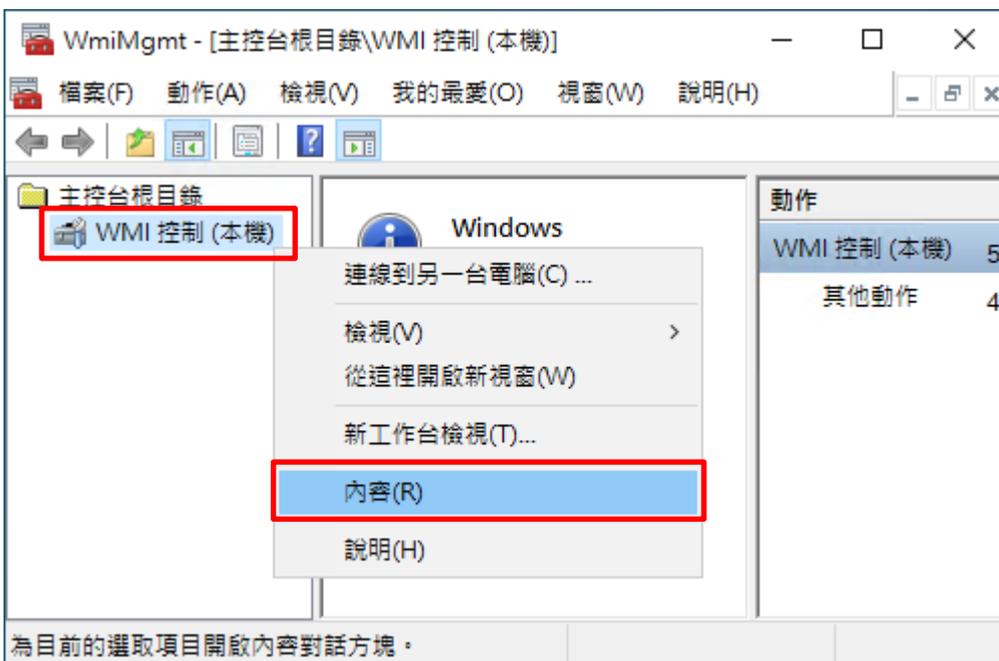
(2) 開啟元件服務

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



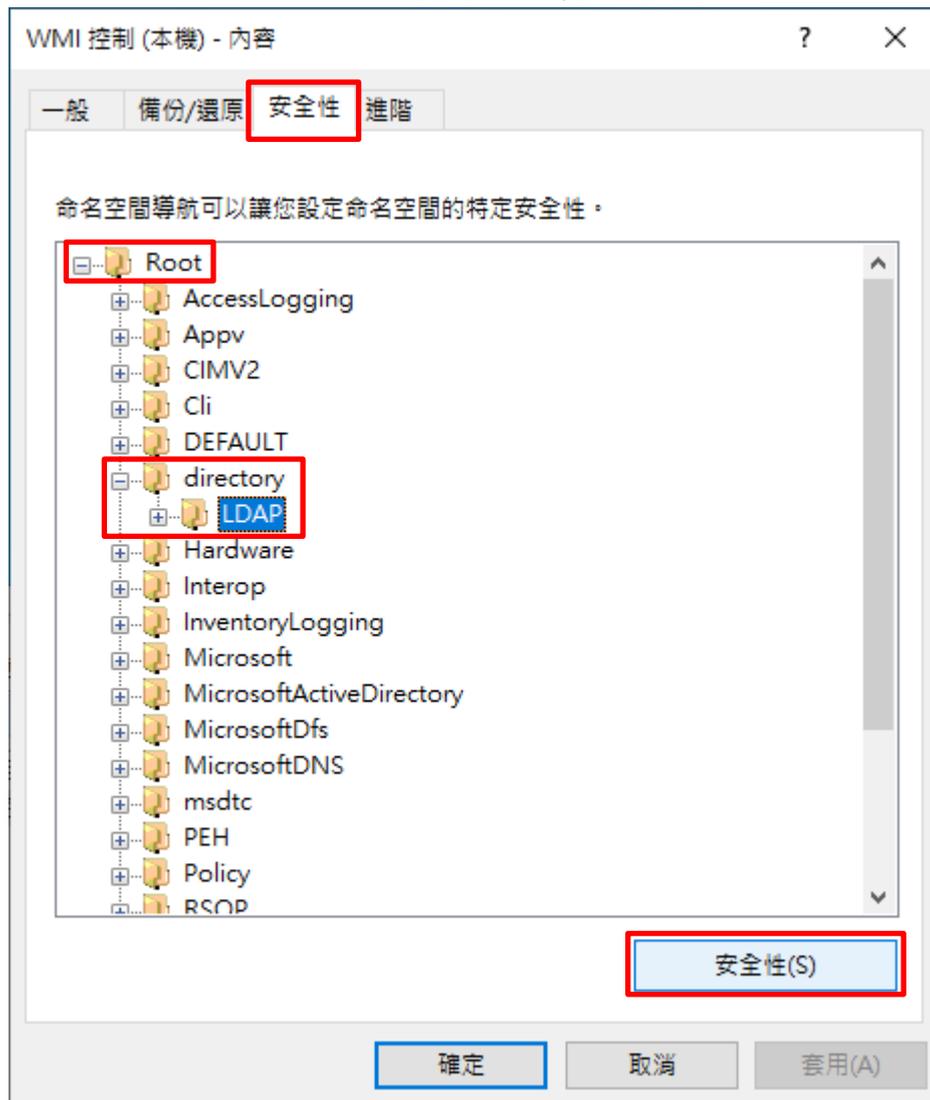
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



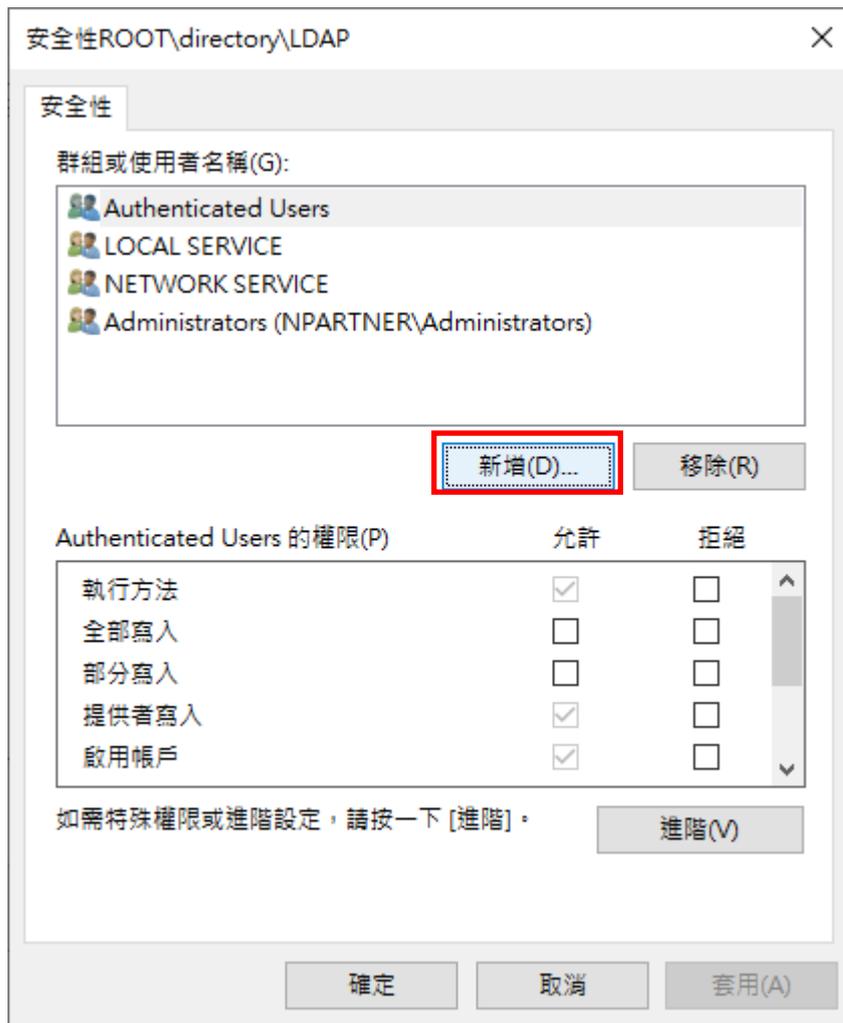
(4) 編輯 LDAP 安全性

點選 [安全性] 頁面 -> 展開 [Root] -> [directory] -> [LDAP] -> 按 [安全性]



(5) 新增 WMI 使用者權限

按 [新增]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]



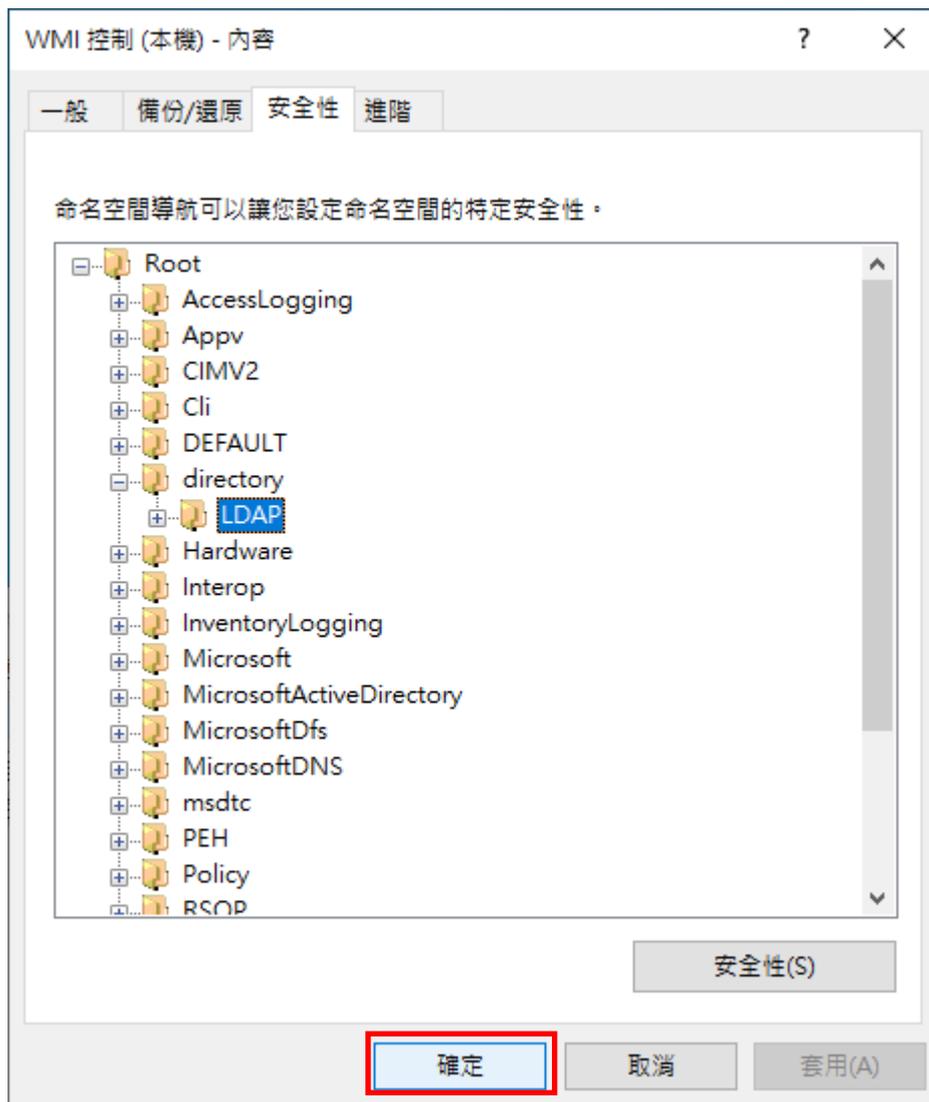
(7) 設定使用者權限

點選使用者帳號: [npartner] -> 取消勾選 [啟用帳號:允許] -> 勾選 [遠端啟用:允許] -> 按 [確定]



(8) 確定使用者權限

按 [確定]



8.3.4 設定 Event log 讀取權限

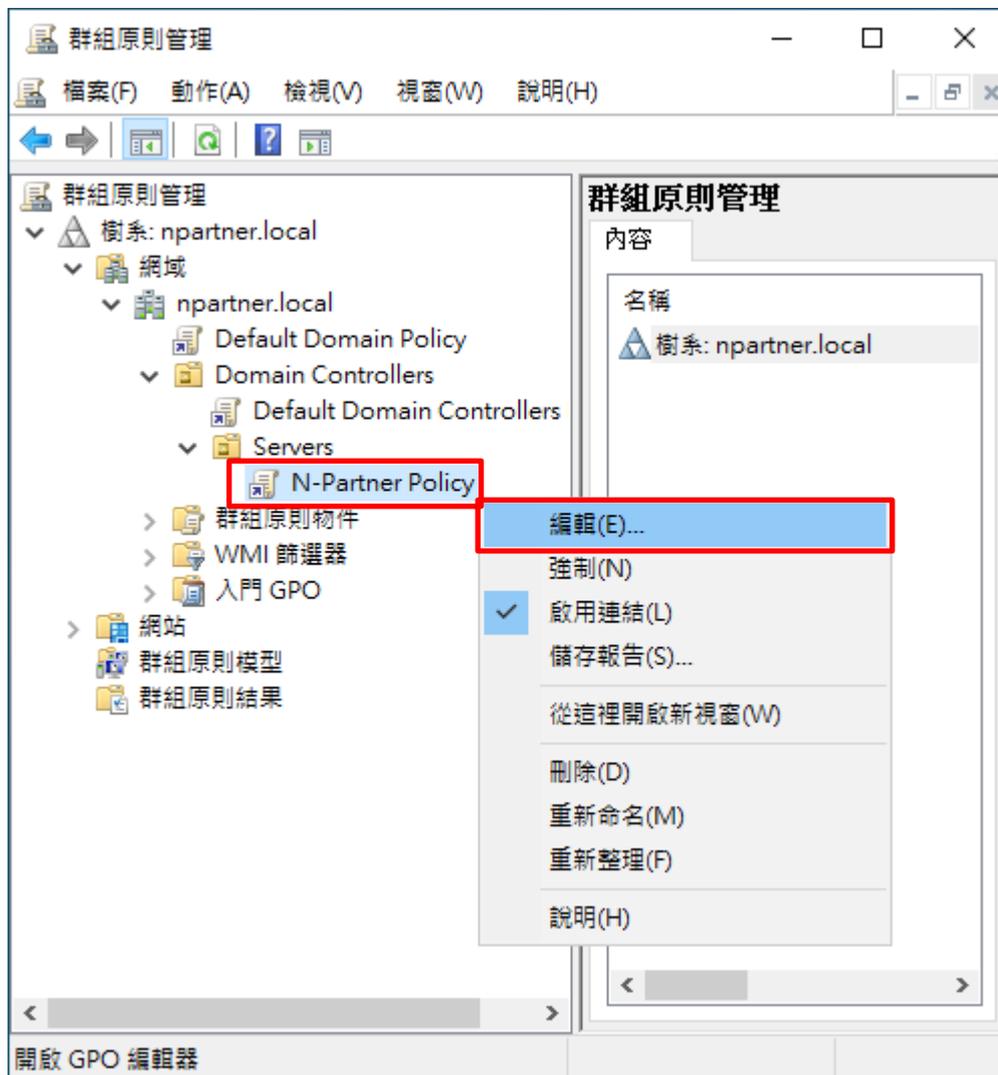
(1) 開啟群組原則管理

開啟 [群組原則管理]



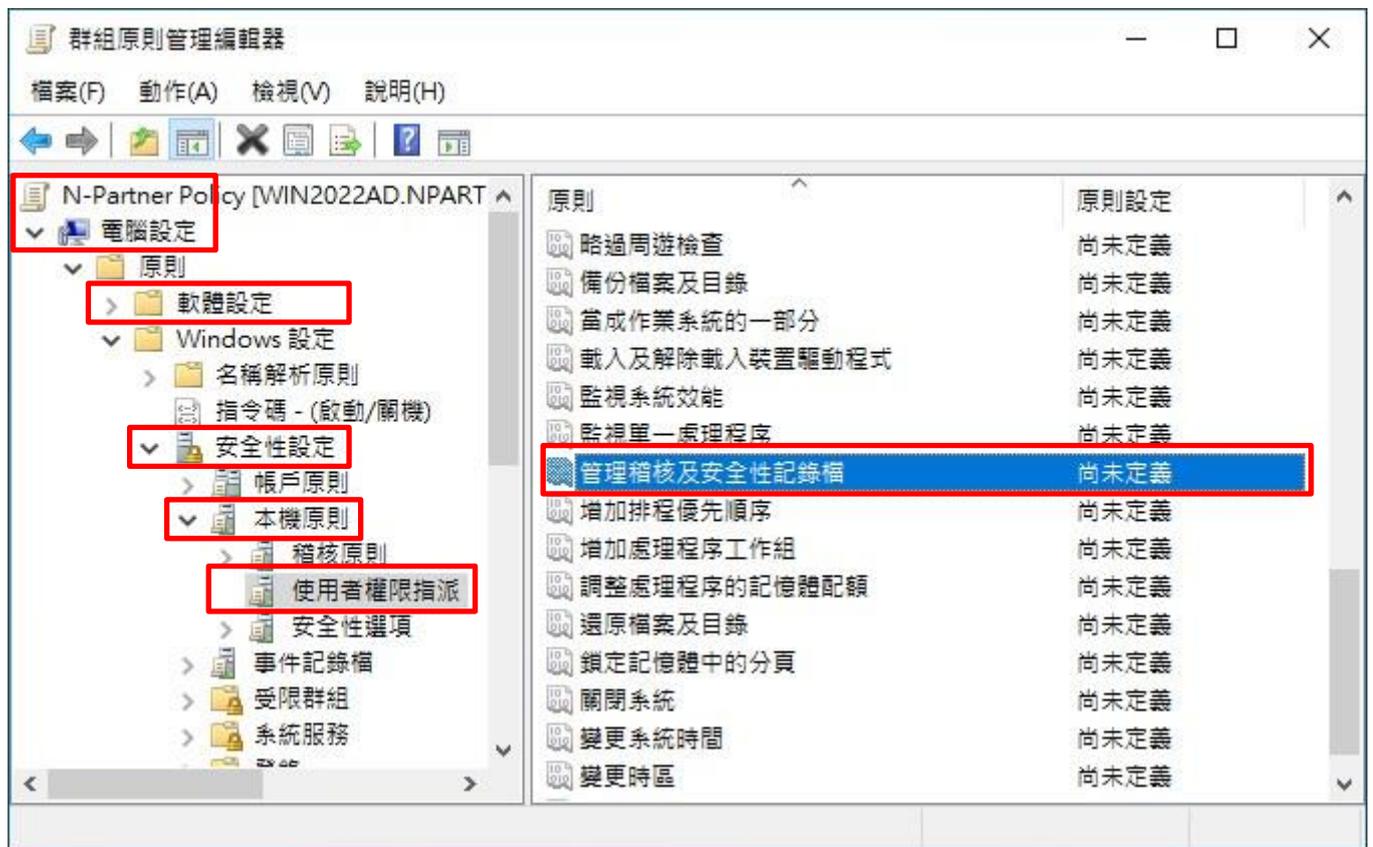
(2) 編輯群組原則物件

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



(3) 設定記錄檔

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [使用者權限指派] -> 點選 [管理稽核及安全性記錄檔] 項目



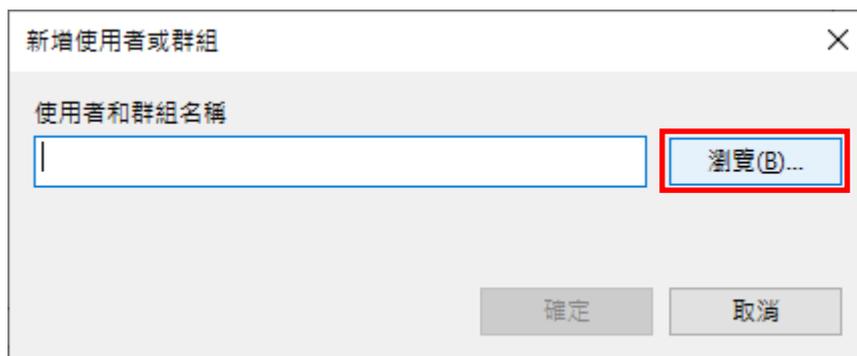
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



(5) 搜尋使用者

按 [瀏覽]



(6) 輸入使用者

輸入使用者帳號: `npartner` -> 點選 [檢查名稱] -> 按 [確定]

選取使用者、電腦、服務帳戶或群組

選取這個物件類型(S):
使用者、服務帳戶、群組或內建安全性主體 物件類型(O)...

從這個位置(F):
npartner.local 位置(L)...

輸入物件名稱來選取 (範例)(E):
npartner (npartner@npartner.local) 檢查名稱(C)

進階(A)... 確定 取消

(7) 確定使用者

按 [確定]

新增使用者或群組

使用者和群組名稱
NPARTNER\npartner 瀏覽(B)...

確定 取消

(8) 確定設定記錄檔

按 [確定]



(9) 開啟 [Windows PowerShell]



(10) 更新群組原則

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



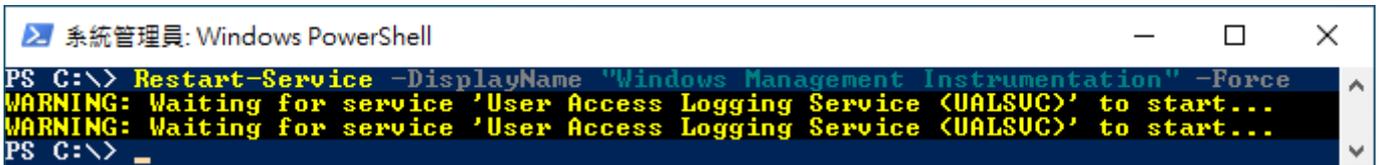
8.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



(2) 重啟 WMI 服務

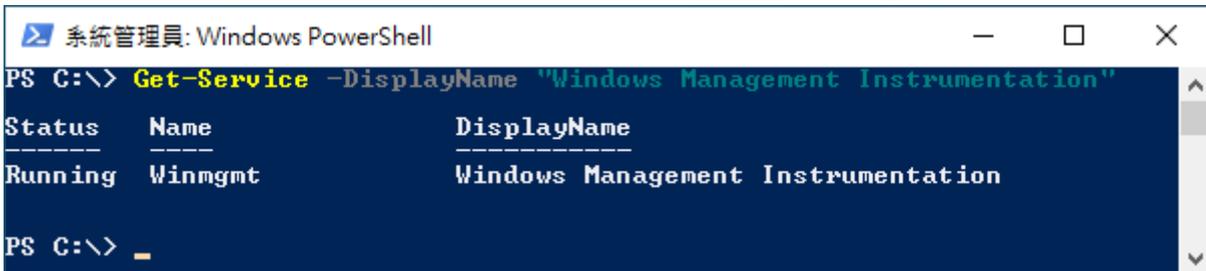
```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Restart-Service -DisplayName "Windows Management Instrumentation" -Force` being executed. The output consists of two yellow warning messages: `WARNING: Waiting for service 'User Access Logging Service (UALSUC)' to start...` followed by a blank line and another identical warning message. The prompt `PS C:\> _` is visible at the bottom.

```
系統管理員: Windows PowerShell
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
WARNING: Waiting for service 'User Access Logging Service (UALSUC)' to start...
WARNING: Waiting for service 'User Access Logging Service (UALSUC)' to start...
PS C:\> _
```

(3) 查看 WMI 服務

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Get-Service -DisplayName "Windows Management Instrumentation"` being executed. The output is a table with three columns: `Status`, `Name`, and `DisplayName`. The first row shows the service is `Running`, with `Winmgmt` as the name and `Windows Management Instrumentation` as the display name. The prompt `PS C:\> _` is visible at the bottom.

```
系統管理員: Windows PowerShell
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
Status      Name          DisplayName
-----
Running     Winmgmt       Windows Management Instrumentation
PS C:\> _
```

8.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆 · 只允許 N-Reporter IP query WMI

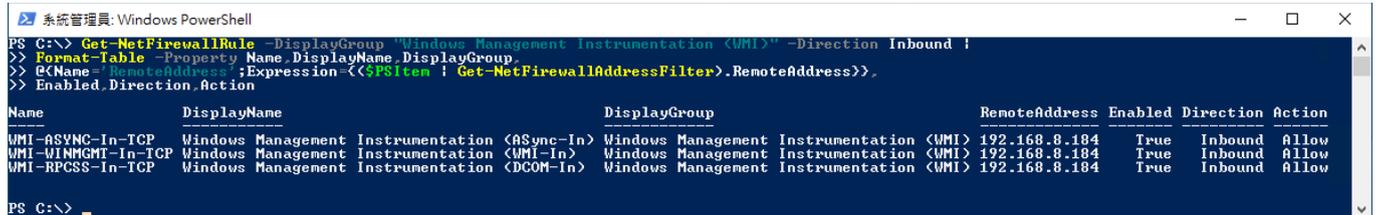
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 查看防火牆 WMI 啟用狀態

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |  
>> Format-Table -Property Name,DisplayName,DisplayGroup,  
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},  
>> Enabled,Direction,Action
```



9. N-Reporter

(1) 新增 Windows AD 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]

The screenshot displays the N-Reporter 7 web application interface. On the left is a dark sidebar menu with the following items: 事件, 報表, 智慧分析, Dashboard, 設備管理 (highlighted with a red box), 設備資產樹狀圖, 設備批次管理, 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, 效能監控, 系統管理, and 使用者手冊. The main content area shows the breadcrumb 'Home / 設備管理 / 設備資產樹狀圖' and the title '設備資產樹狀圖'. Below the title is a search bar with the text '搜尋', a '重新輸入' (Refresh) button, a '啟動查詢' (Start Query) button, and a red-bordered '+' button. The main content area shows a tree structure with 'Global (10/10)' and a sub-item '未知設備 (0/3)'.

(2) 選擇設備種類

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



9.1 Windows 2003 或之前版本作業系統

(1) 設備基本設定

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

新增設備 - 設備基本設定

設備基本設定

設備名稱 *

WindowsAD-192.168.8.195

IP *

192.168.8.195

所屬領域 *

Global

Syslog 資料格式 ⓘ

Windows AD

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

Host Mib

Web 監控 ⓘ

啟用網頁監控功能

上一步 下一步 取消

(2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)]->編碼方式選擇[BIG5]-> 點選 [下一步]

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

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ

(17) local use 1 (local1)

編碼方式

BIG5

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

(3) 其他

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



新增設備 - 其它

其它

設備 Icon 

Host

接收狀態

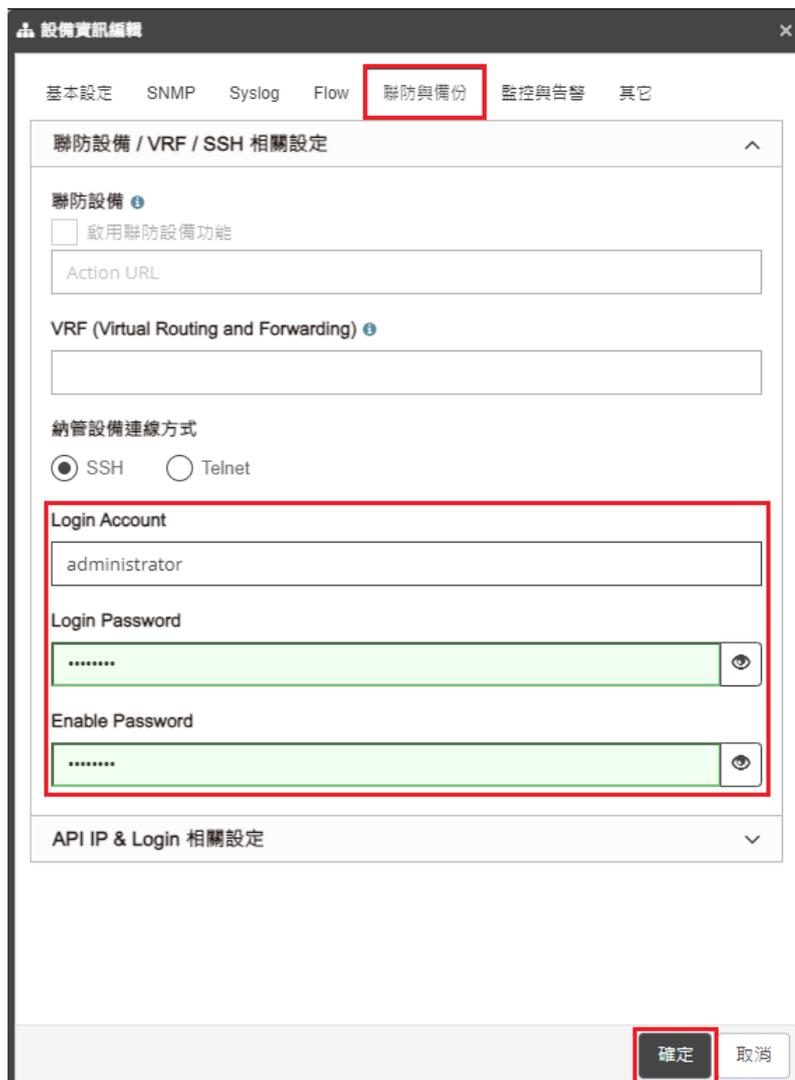
啟用 停用

經緯度

緯度 經度

(4) WMI設定

輸入 Windows AD 的 WMI Login Account 和 Login Password ，若沒設定 WMI 可以不用輸入帳密



設備資訊編輯

基本設定 SNMP Syslog Flow **聯防與備份** 監控與告警 其它

聯防設備 / VRF / SSH 相關設定

聯防設備

啟用聯防設備功能

Action URL

VRF (Virtual Routing and Forwarding)

納管設備連線方式

SSH Telnet

Login Account

administrator

Login Password

.....

Enable Password

.....

API IP & Login 相關設定

確定 取消

9.2 Windows 2008 或之後版本作業系統

(1) 設備基本設定

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

新增設備 - 設備基本設定

設備基本設定

設備名稱 *

WindowsAD-192.168.8.195

IP *

192.168.8.195

所屬領域 *

Global

Syslog 資料格式 ⓘ

Windows AD

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

Host Mib

Web 監控 ⓘ

啟用網頁監控功能

上一步 下一步 取消

(2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)]->編碼方式選擇[UTF-8]-> 點選 [下一步]
(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ
(17) local use 1 (local1) ▼

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

(3) 其他

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



新增設備 - 其它

其它

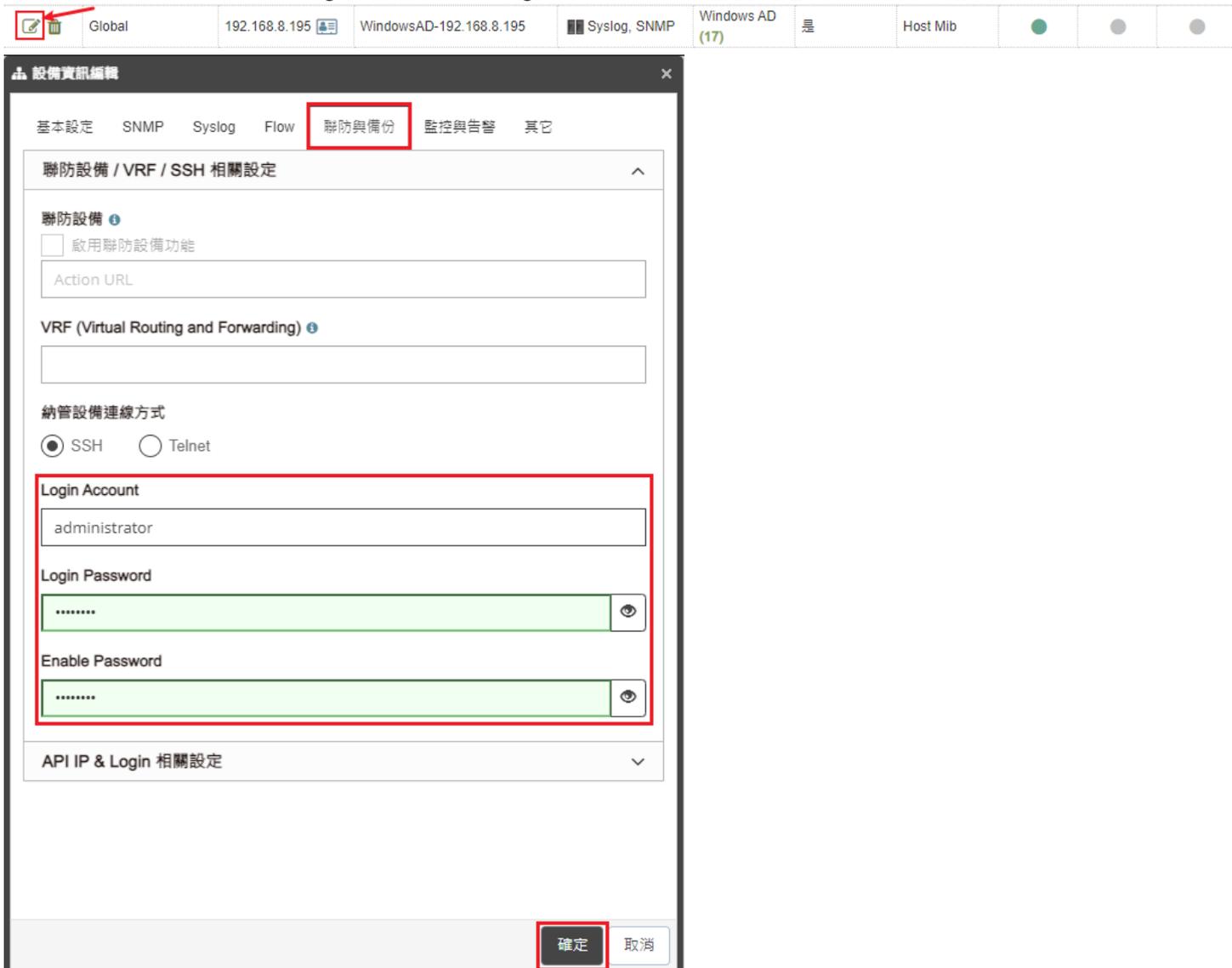
設備 Icon

接收狀態
 啟用 停用

經緯度
緯度 經度

(4) WMI設定

輸入 Windows AD 的 WMI Login Account 和 Login Password，若沒設定 WMI 可以不用輸入帳密



Global 192.168.8.195 WindowsAD-192.168.8.195 Syslog, SNMP Windows AD (17) Host Mib

設備資訊編輯

基本設定 SNMP Syslog Flow 聯防與備份 監控與告警 其它

聯防設備 / VRF / SSH 相關設定

聯防設備
 啟用聯防設備功能
Action URL

VRF (Virtual Routing and Forwarding)

納管設備連線方式
 SSH Telnet

Login Account
administrator

Login Password
.....

Enable Password
.....

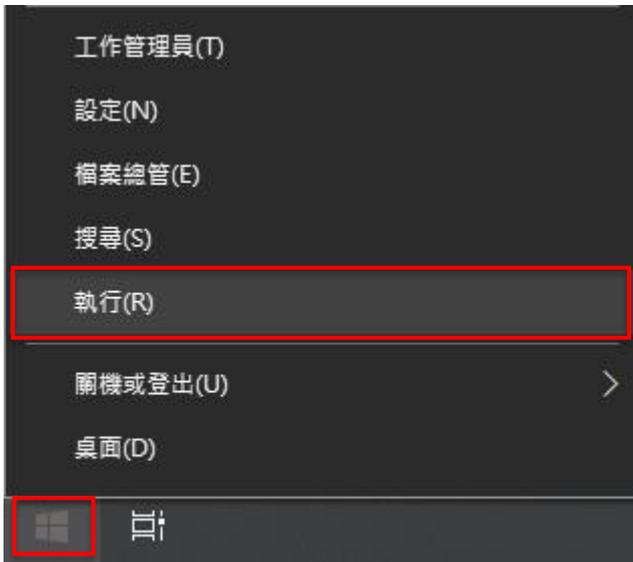
API IP & Login 相關設定

確定 取消

10. 問題排除

10.1 WMI Query Language 檢查

(1) 按  -> 點選 [執行]

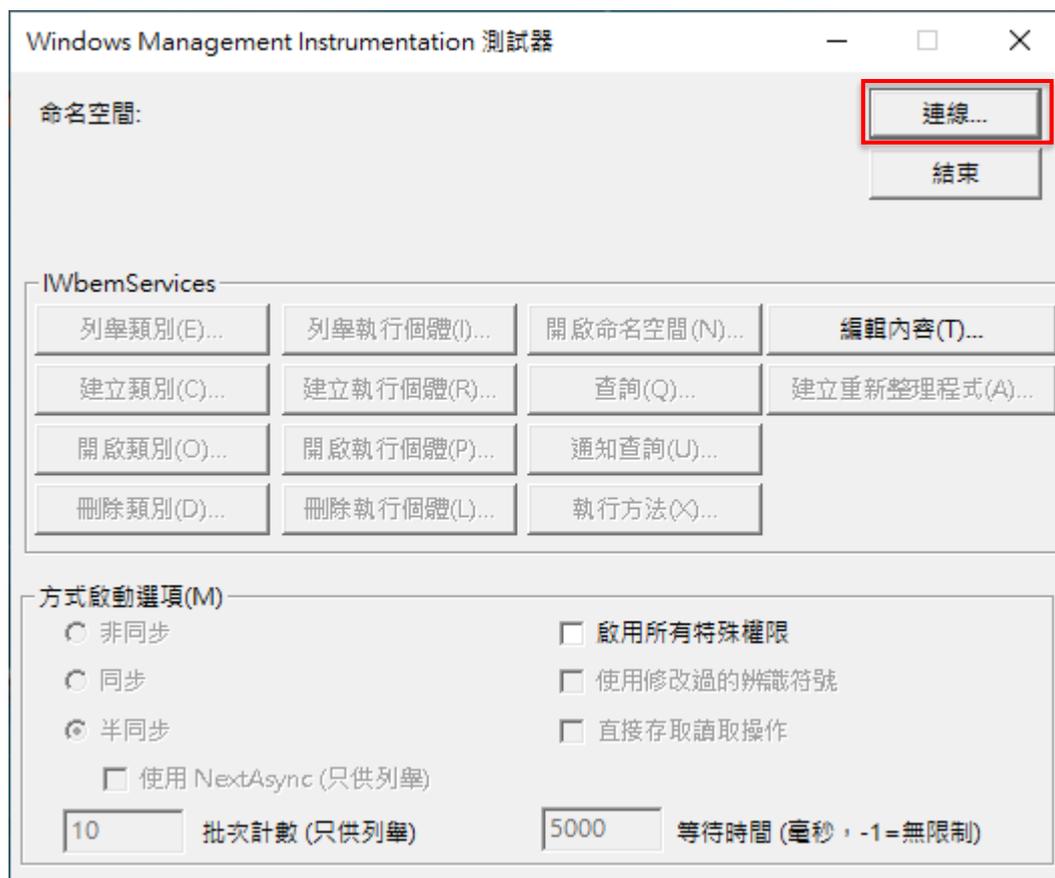


(2) 輸入 `wbemtest` -> 按 [確定]



10.1.1 查詢事件日誌

(1) 按 [連線]



(2) 輸入命名空間 \\<Windows AD IP>\root\cimv2 -> 使用者帳號和密碼 -> 按 [連線]

連線

命名空間: \\192.168.1.183\root\cimv2

連線: 使用: IWbemLocator (Namespaces) 傳回: IWbemServices 完成: Synchronous

認證: 使用者(U): npartner 密碼(P): ***** 授權(A):

地區設定(L):

如何解譯空白密碼(H): NULL 空白

模擬等級(I): 識別 模擬 委派

驗證等級(V): 無 封包 連線 封包完整性 呼叫 封包私密性

(3) 按 [查詢]

Windows Management Instrumentation 測試器

命名空間:
\\192.168.1.183\root\cimv2

連線...
結束

IWbemServices

列舉類別(E)...	列舉執行個體(I)...	開啟命名空間(N)...	編輯內容(T)...
建立類別(C)...	建立執行個體(R)...	查詢(Q)...	建立重新整理程式(A)...
開啟類別(O)...	開啟執行個體(P)...	通知查詢(U)...	
刪除類別(D)...	刪除執行個體(L)...	執行方法(X)...	

方式啟動選項(M)

非同步 啟用所有特殊權限
 同步 使用修改過的辨識符號
 半同步 直接存取讀取操作
 使用 NextAsync (只供列舉)

10 批次計數 (只供列舉) 5000 等待時間 (毫秒, -1=無限制)

(4) 輸入查詢 `Select * FROM Win32_NTLogEvent` -> 按 [套用]

查詢

輸入查詢

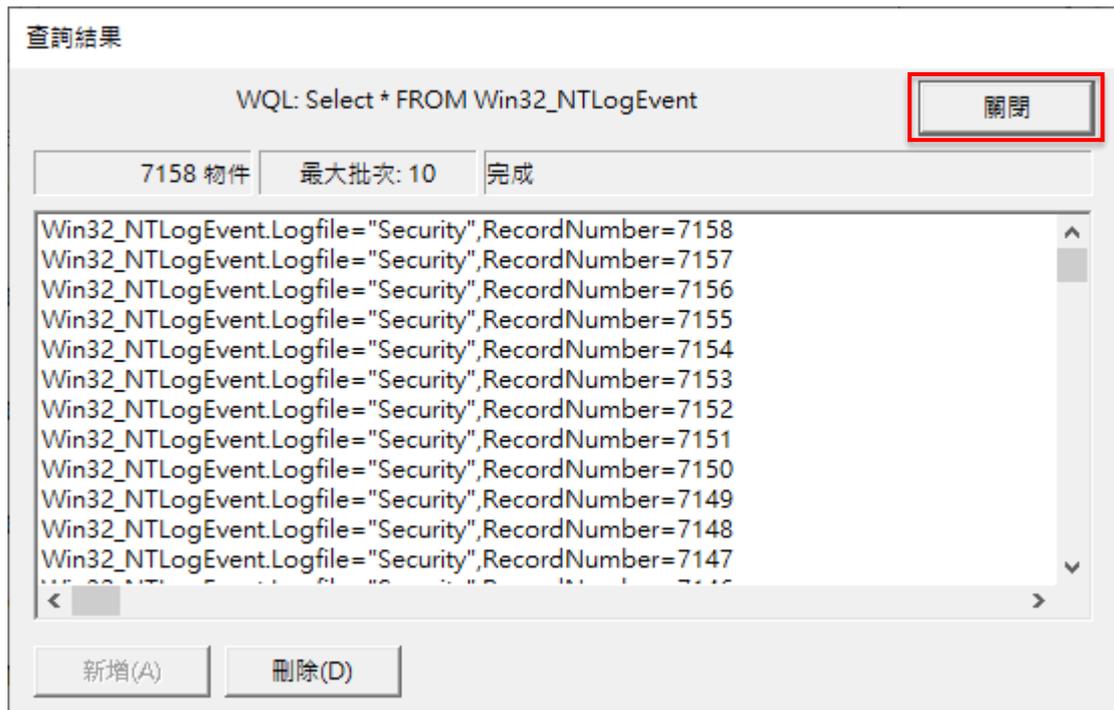
Select * FROM Win32_NTLogEvent

查詢類型

WQL 抓取類別原型

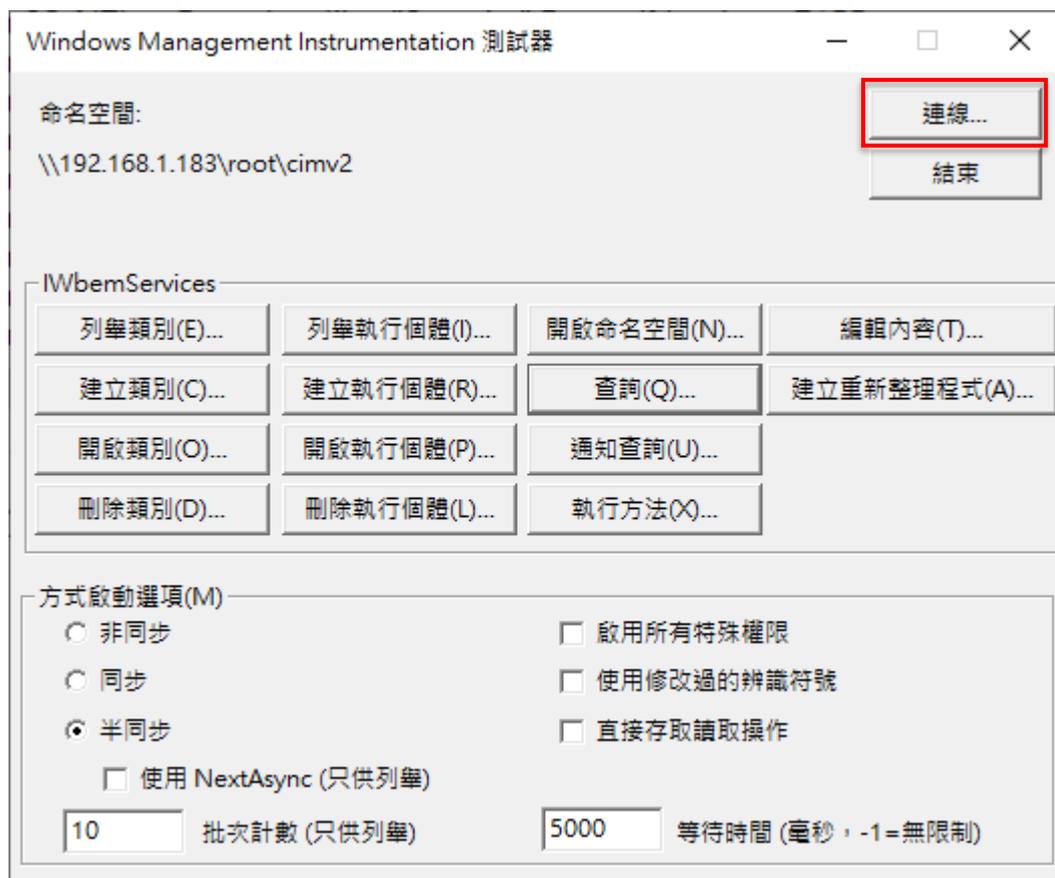
套用
取消

(5) 顯示查詢到資料 -> 按 [關閉]



10.1.2 查詢使用者資料

(1) 按 [連線]



(2) 檢查使用者資料；輸入命名空間 \\<Windows AD IP>\root\directory\LDAP -> 使用者帳號和密碼 -> 按 [連線]

連線

命名空間
\\192.168.1.183\root\directory\LDAP

連線

取消

連線:
使用: IWbemLocator (Namespaces)
傳回: IWbemServices 完成: Synchronous

認證
使用者(U): npartner
密碼(P): *****
授權(A):

地區設定(L)

如何解譯空白密碼(H)
 NULL 空白

模擬等級(I)
 識別
 模擬
 委派

驗證等級(V)
 無 封包
 連線 封包完整性
 呼叫 封包私密性

(3) 按 [查詢]

Windows Management Instrumentation 測試器

命名空間:
\\192.168.1.183\root\directory\LDAP

連線...
結束

IWbemServices

列舉類別(E)... 列舉執行個體(I)... 開啟命名空間(N)... 編輯內容(T)...
建立類別(C)... 建立執行個體(R)... 查詢(Q)... 建立重新整理程式(A)...
開啟類別(O)... 開啟執行個體(P)... 通知查詢(U)...
刪除類別(D)... 刪除執行個體(L)... 執行方法(X)...

方式啟動選項(M)

非同步 啟用所有特殊權限
 同步 使用修改過的辨識符號
 半同步 直接存取讀取操作
 使用 NextAsync (只供列舉)

10 批次計數 (只供列舉) 5000 等待時間 (毫秒, -1=無限制)

(4) 輸入查詢 `Select * FROM ds_user` -> 按 [套用]

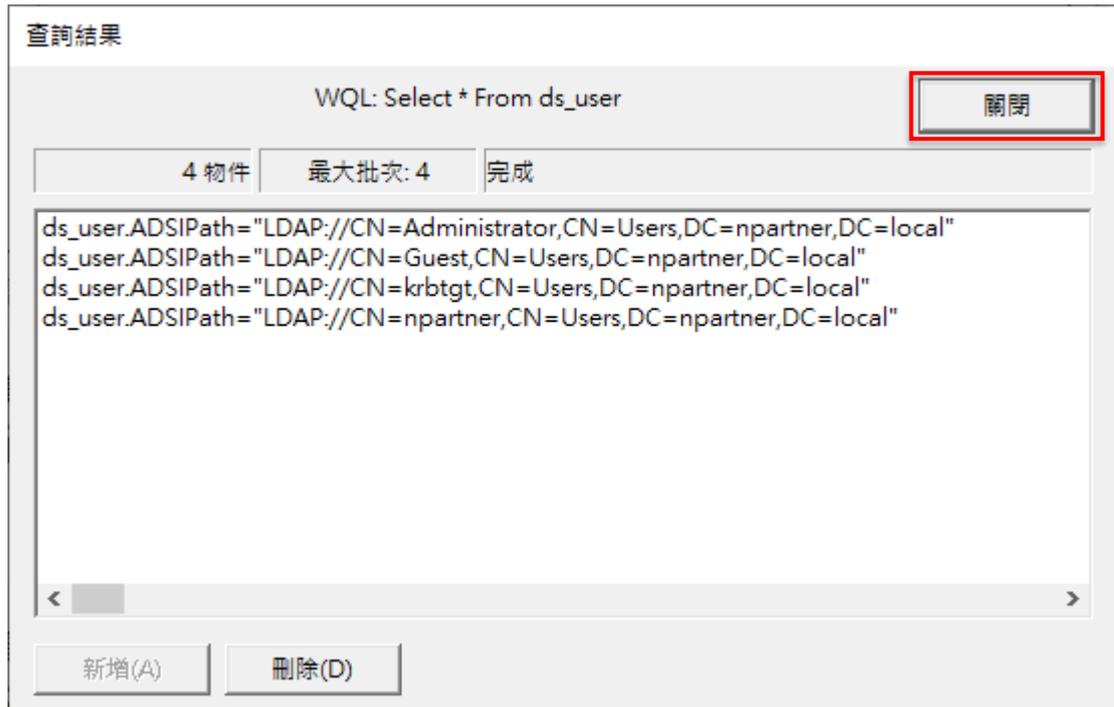
查詢

輸入查詢
Select * FROM ds_user

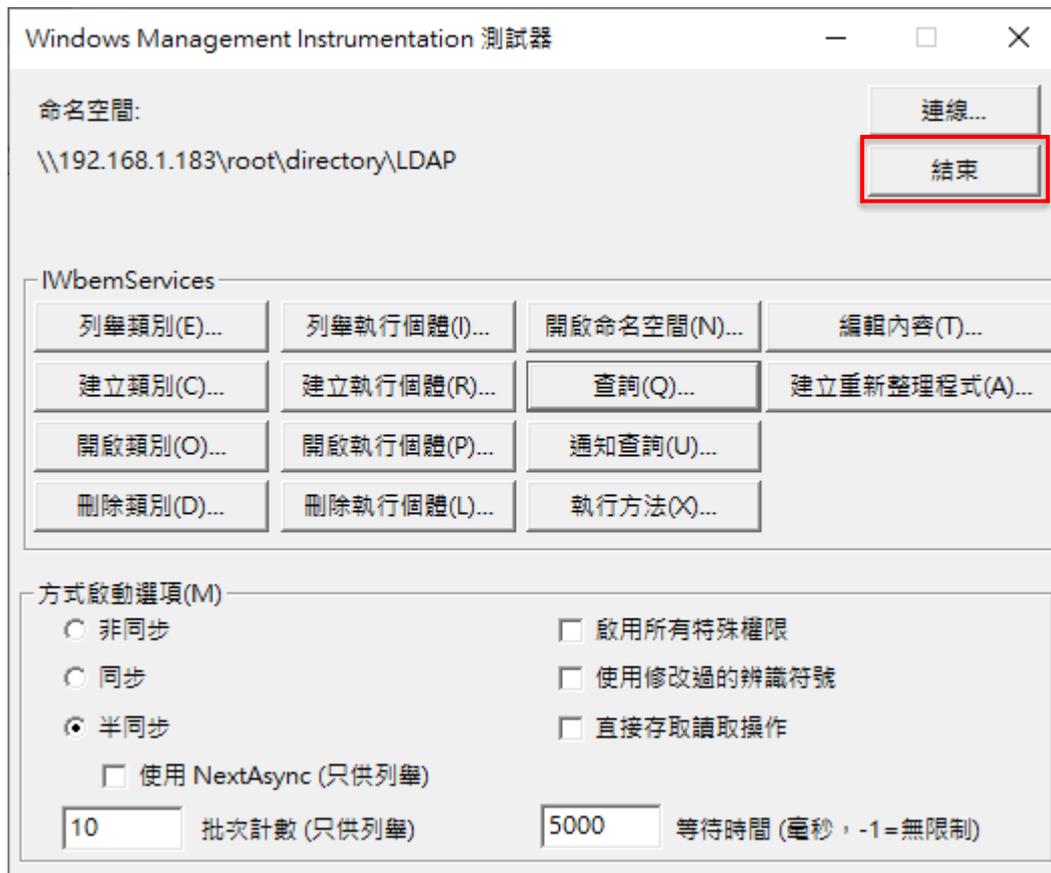
查詢類型
WQL 抓取類別原型

套用
取消

(5) 顯示查詢到資料 -> 按 [關閉]

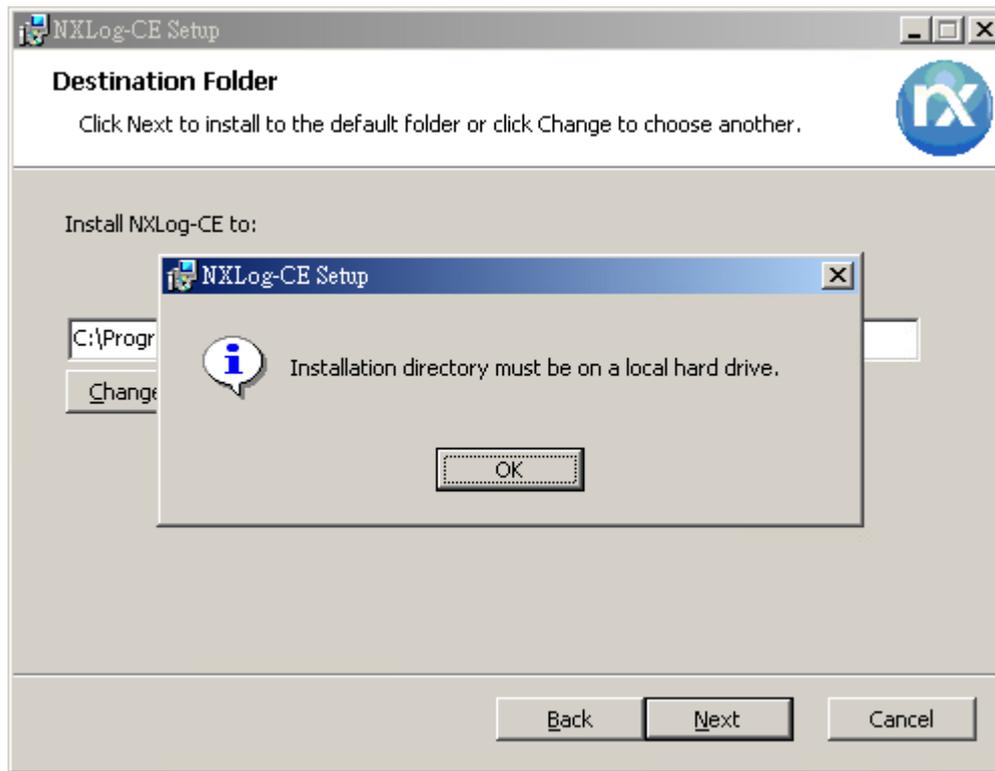


(6) 使用者帳號密碼可以查詢到資料；按 [結束] 關閉 WMI 測試器



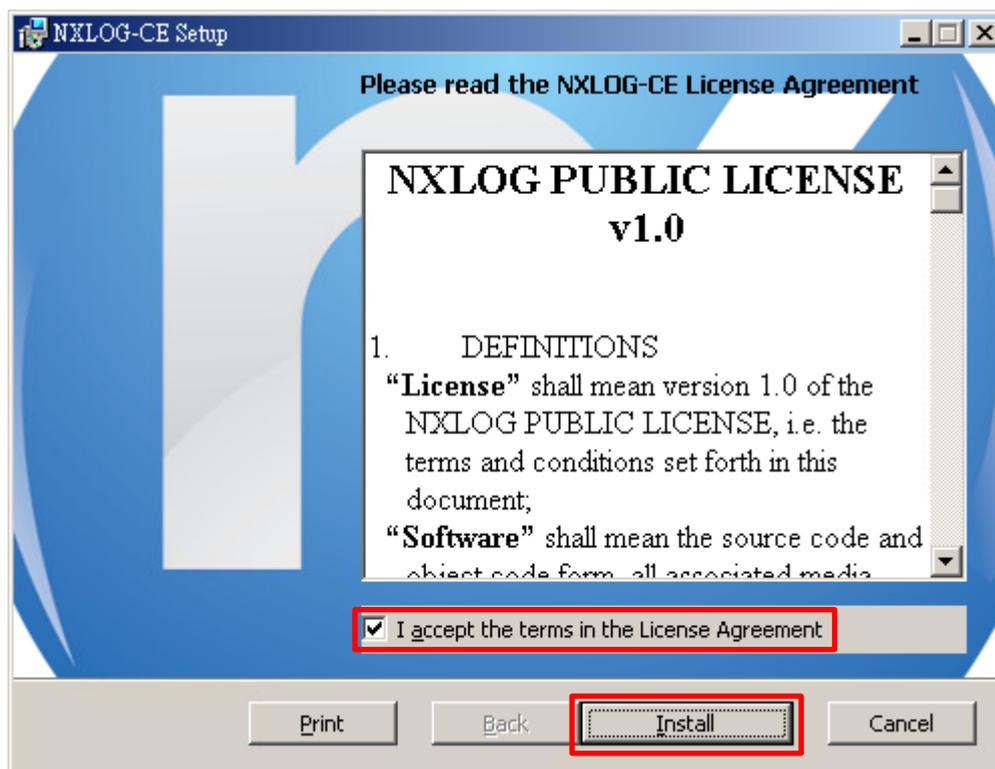
10.2 NXLog 安裝問題

(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@npartnertech.com
技術詢問 / support@npartnertech.com