N-Partner

如何設定
Windows AD 事件記錄

V017

2022/12/07

版權聲明

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

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

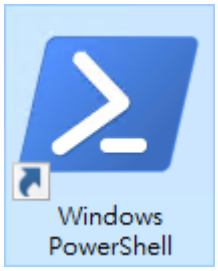
下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.0.2284.msi

	Windows	nxlog-ce-3.0.2284.msi

(2) 安裝 NXLog

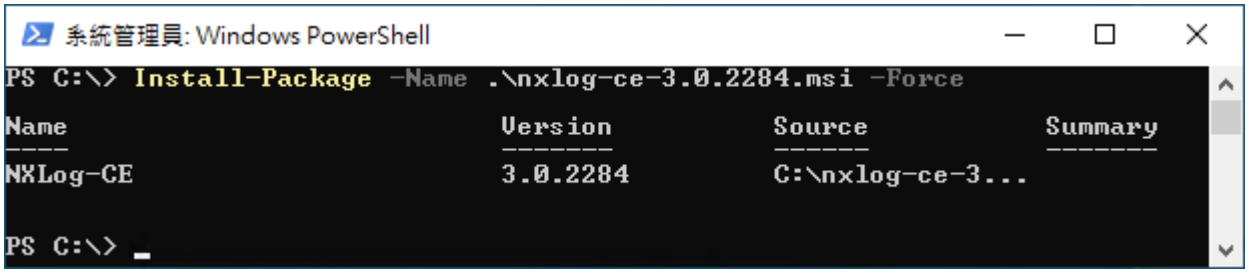
<2.1> Windows 2008 或之後版本作業系統

<2.1.1> 開啟 [Windows PowerShell]



<2.1.2> 安裝 NXLog 軟體

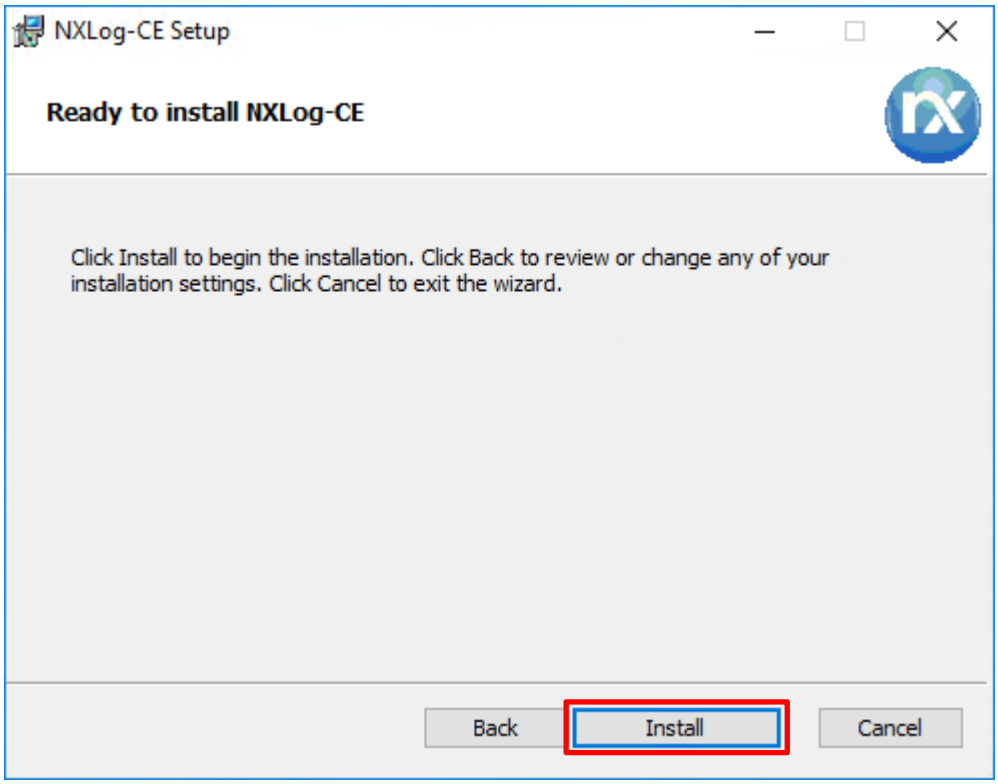
```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2284.msi -Force
```



紅色文字部位請輸入 NXLog 軟體路徑和檔案

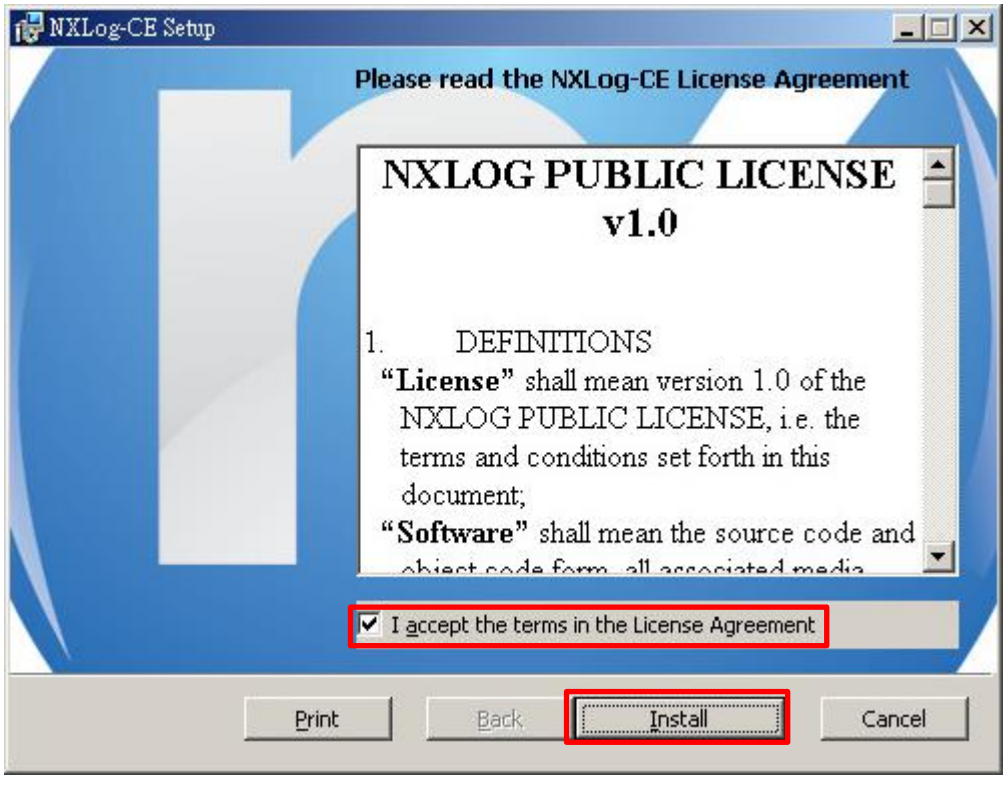
<2.2> Windows 2003

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

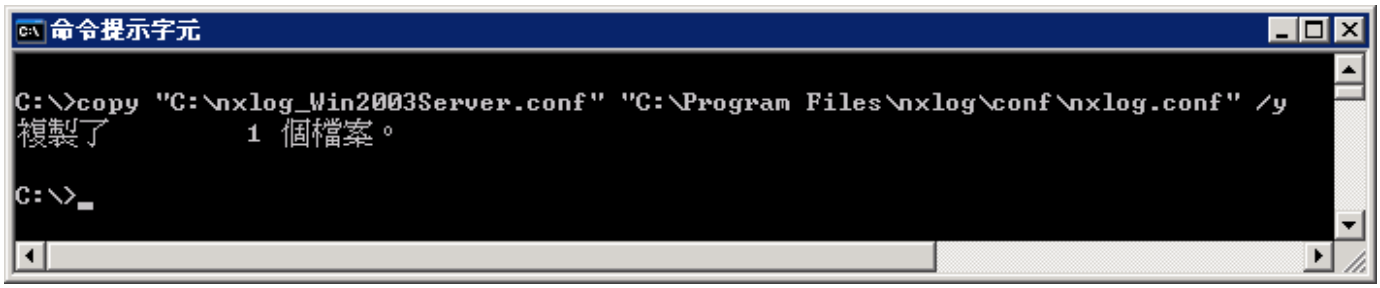
1.2.1.1 輸出主機稽核、物件存取、帳戶管理事件記錄

(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。

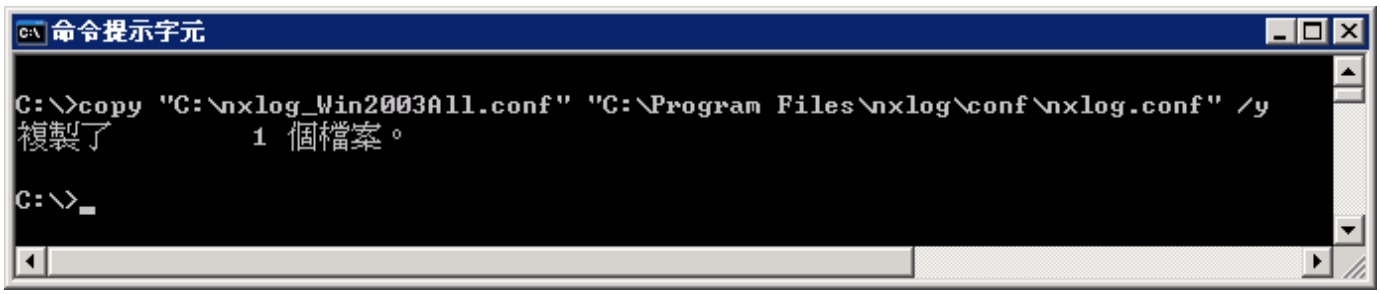
1.2.1.2 輸出全部事件記錄

(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
```



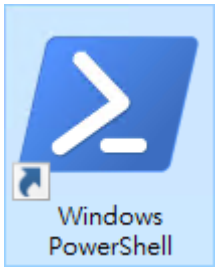
本文件範例是 32 位元作業系統，若作業系統是 64 位元，紅色文字部位請改以下設定 "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

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

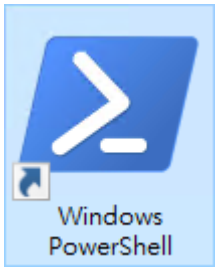
```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_Win2008Server.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```

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'
```

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
```

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
```

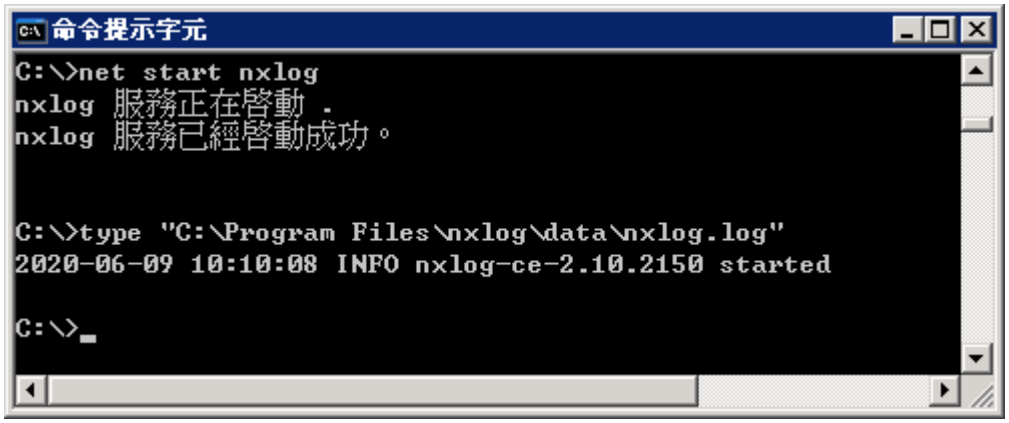
1.4 NXLog 啟動服務

1.4.1 Windows 2003 或之前版本作業系統

(1) 開啟 [命令提示字元]

(2) 啟動 NXLog 服務和確認 NXLog 沒有錯誤訊息

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

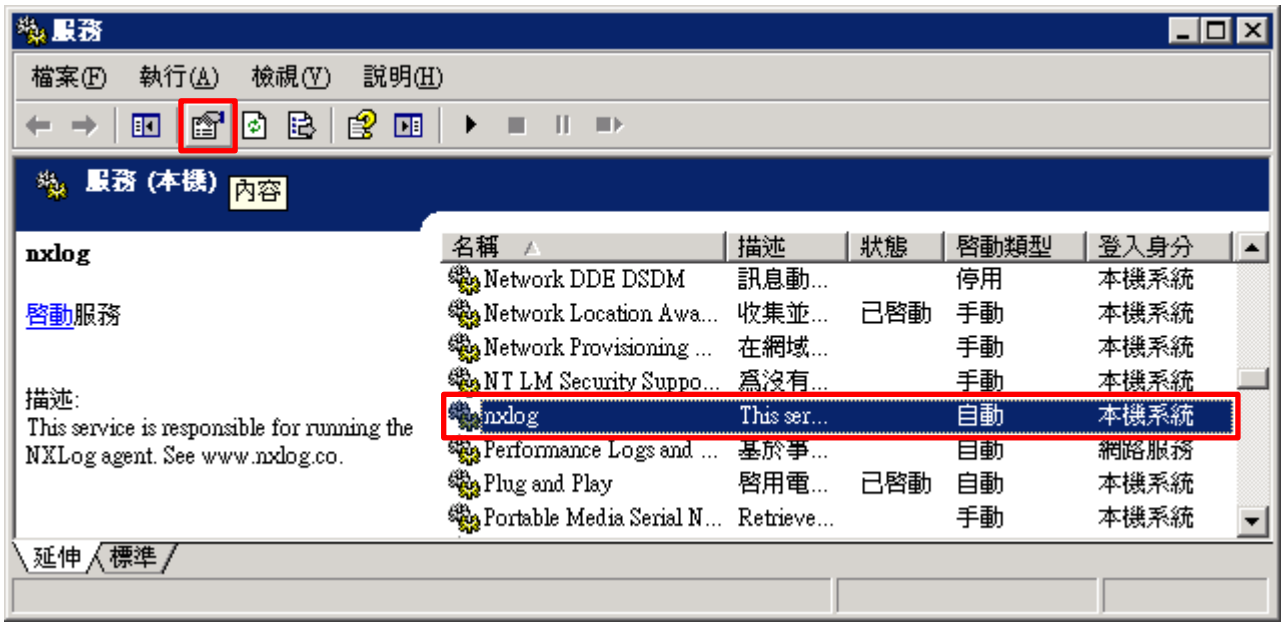


(3) 開啟 [服務] 功能

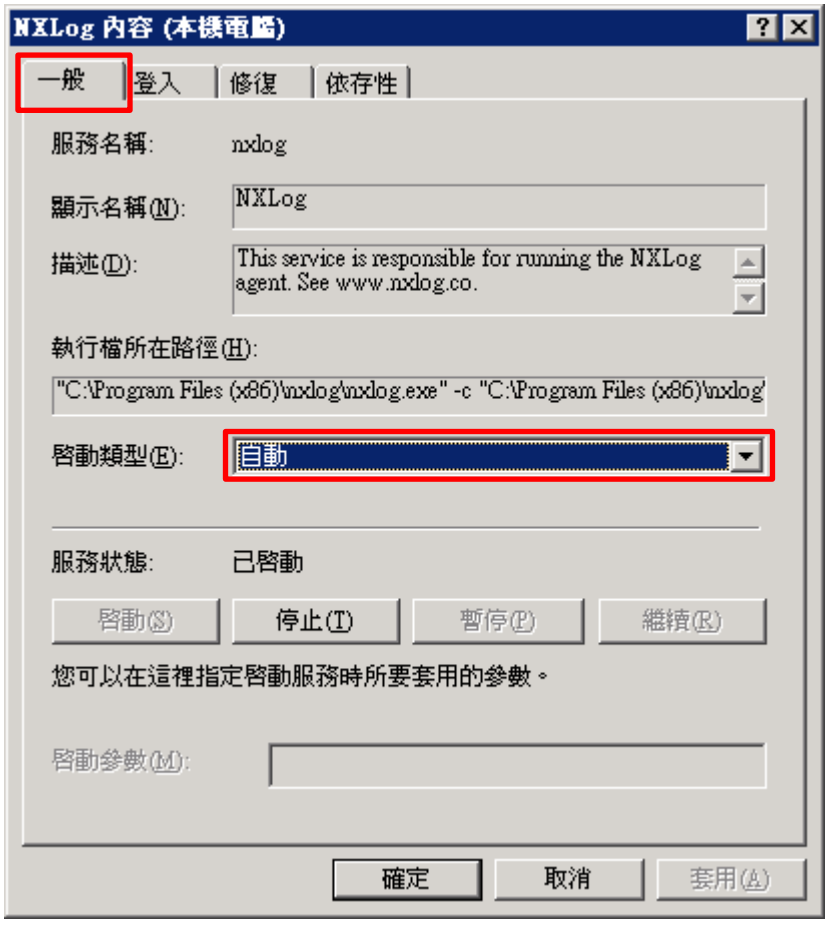
```
C:\> Services.msc
```

(4) 開啟 NXLog 服務內容

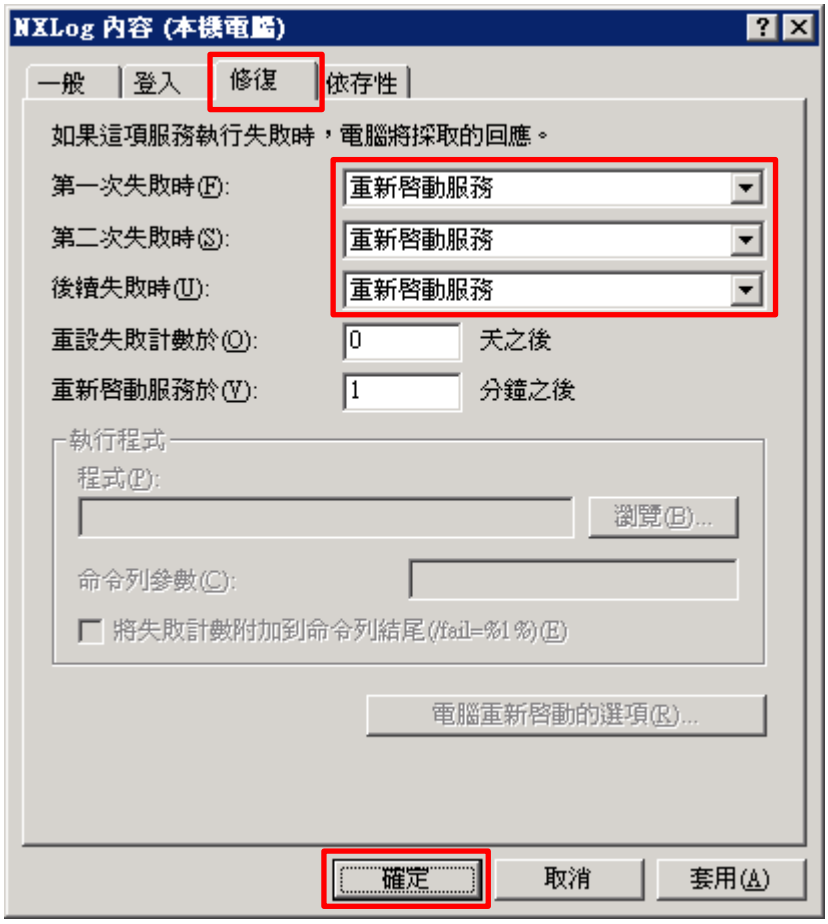
選擇 [nxlog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動]



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

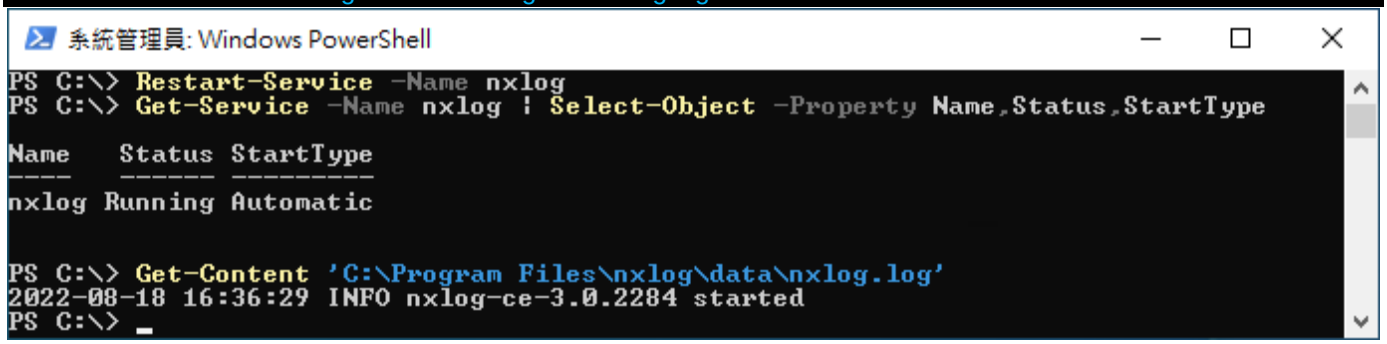


1.4.2 Windows 2008 或之後版本作業系統

(1) 開啟 [Windows PowerShell]

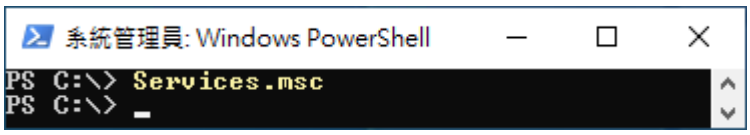
(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

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



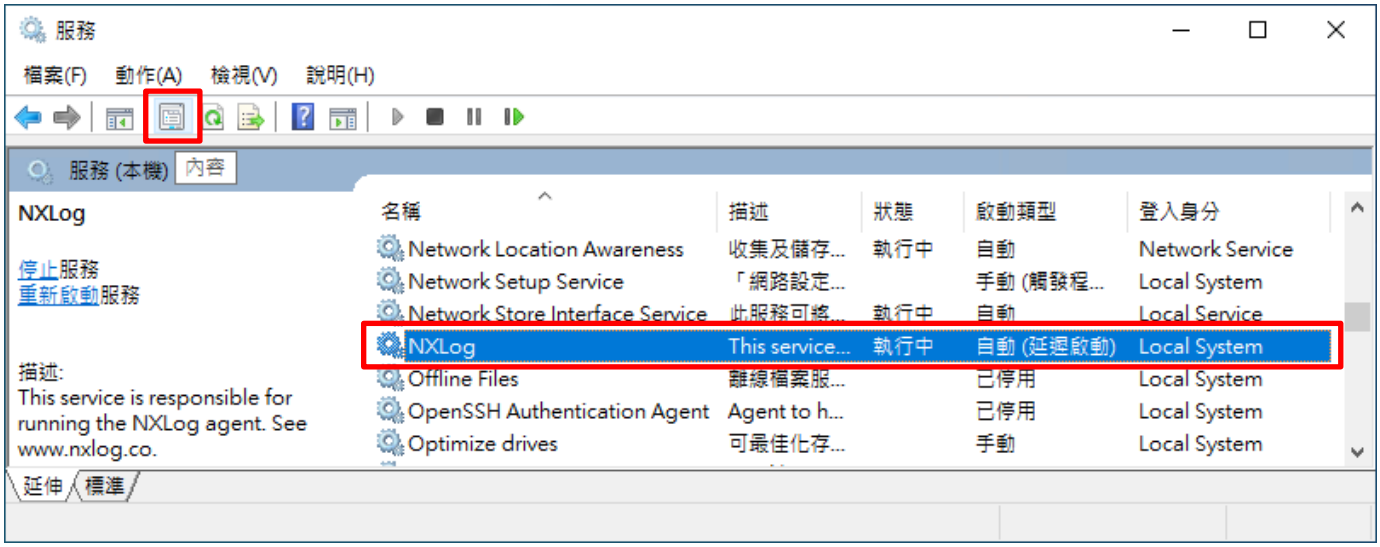
(3) 開啟 [服務] 功能

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

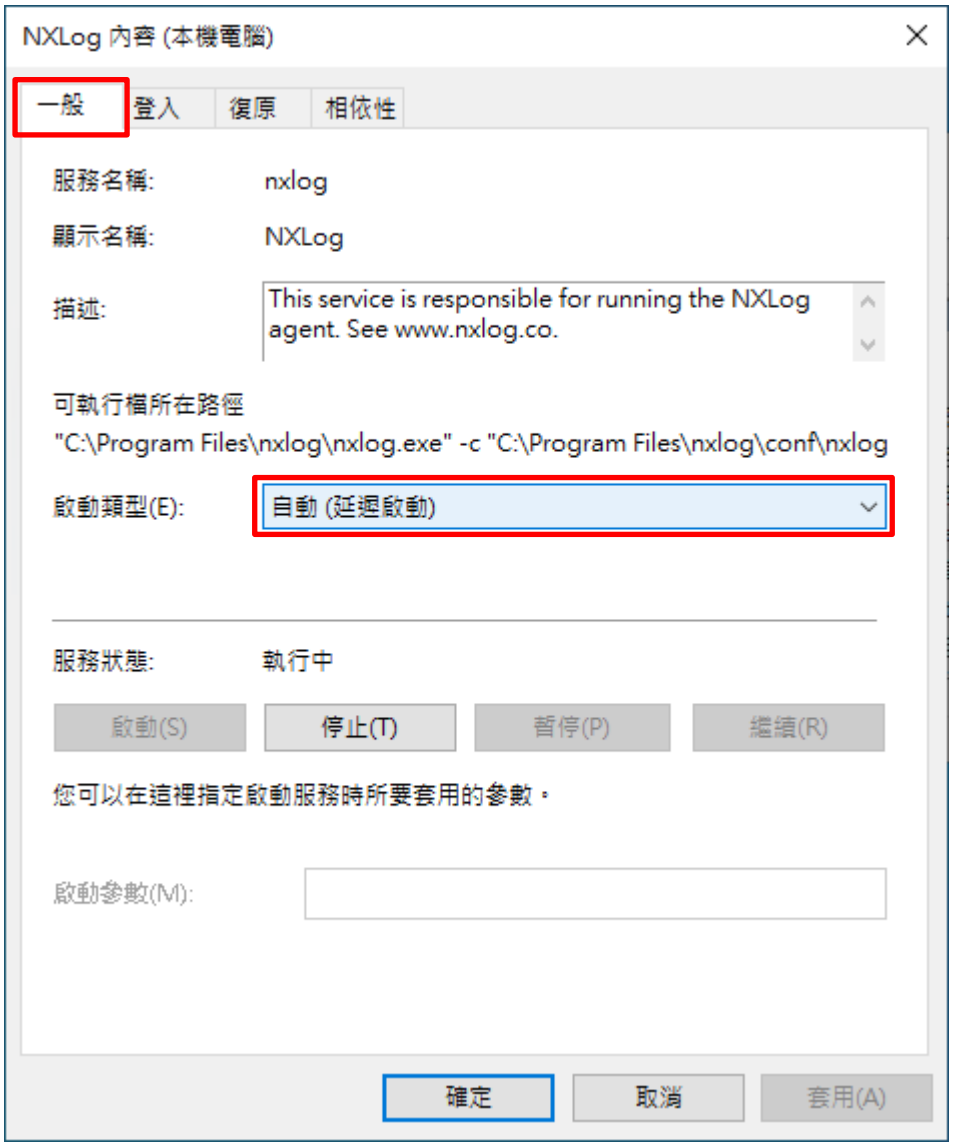


(4) 開啟 NXLog 服務內容

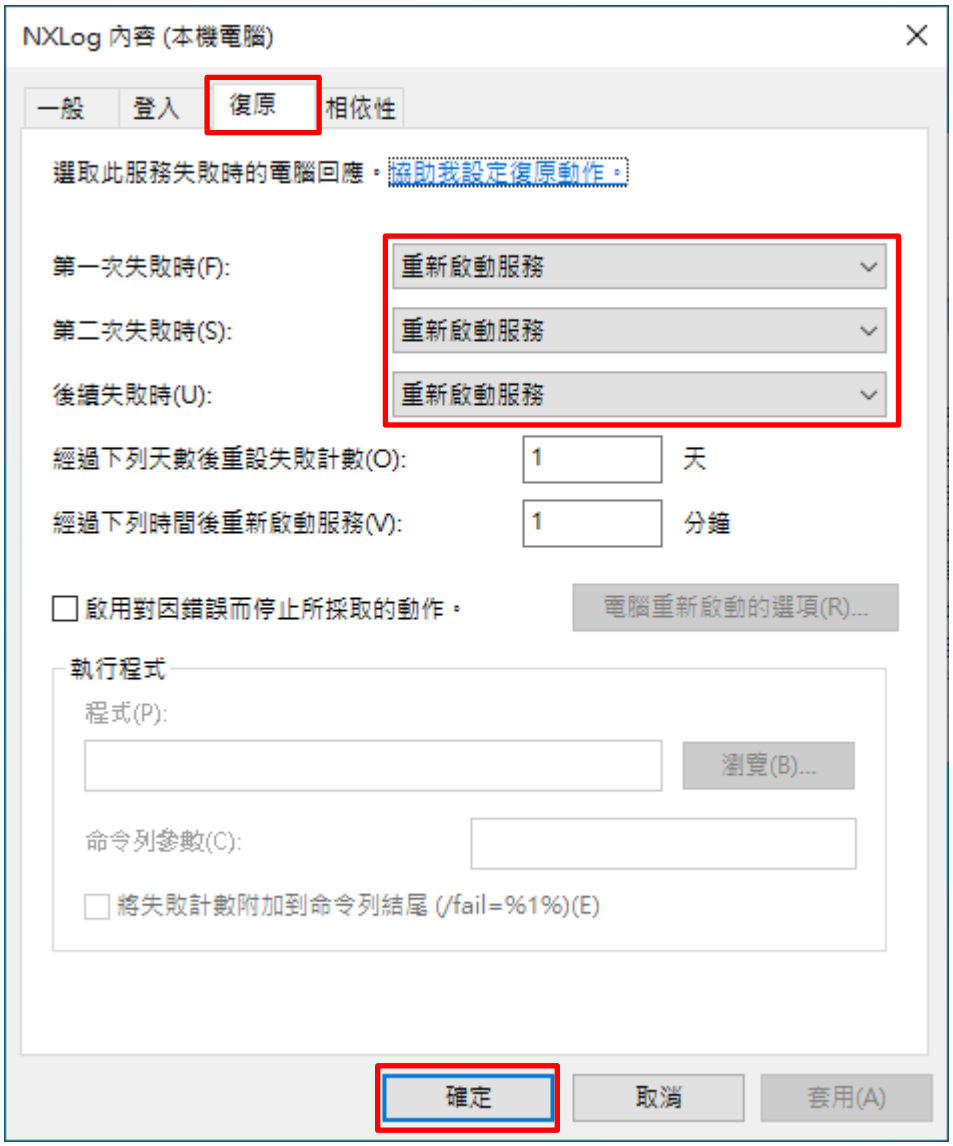
選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (延遲啟動)]



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



2. Windows 2000

Windows 稽核原則設定 詳細說明請參考**前言**的稽核原則建議連結

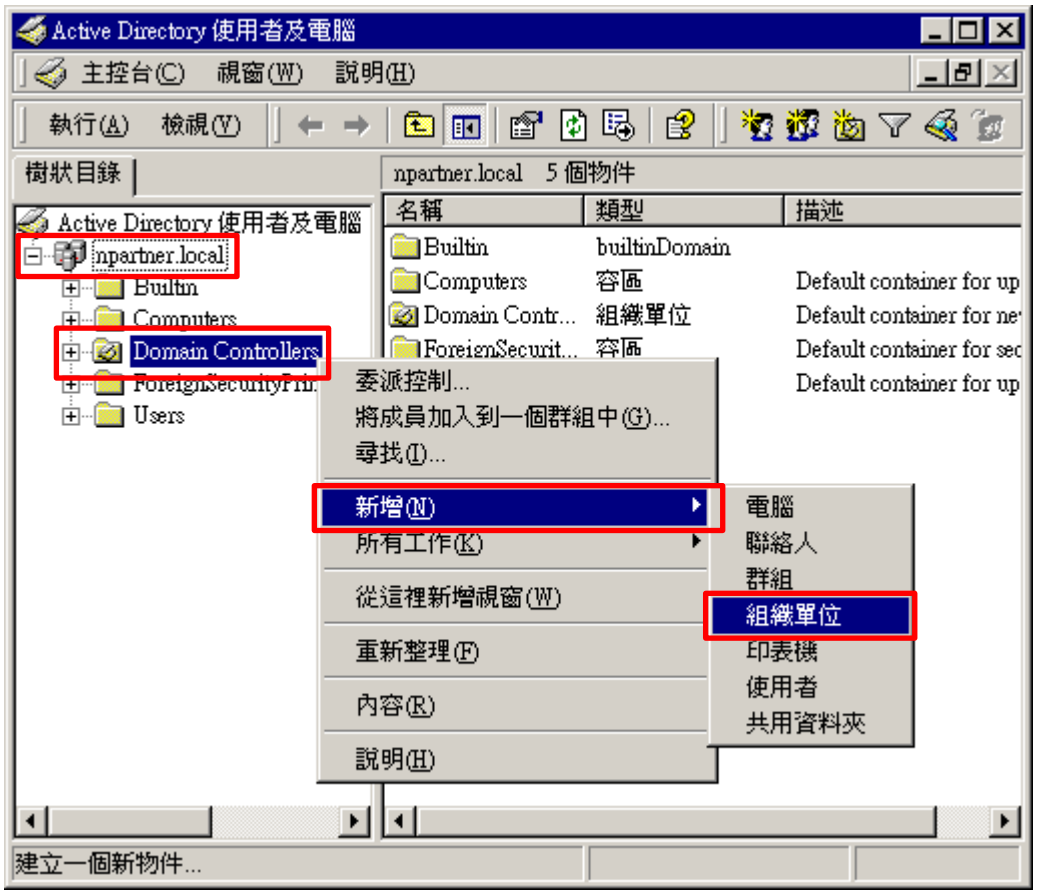
2.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

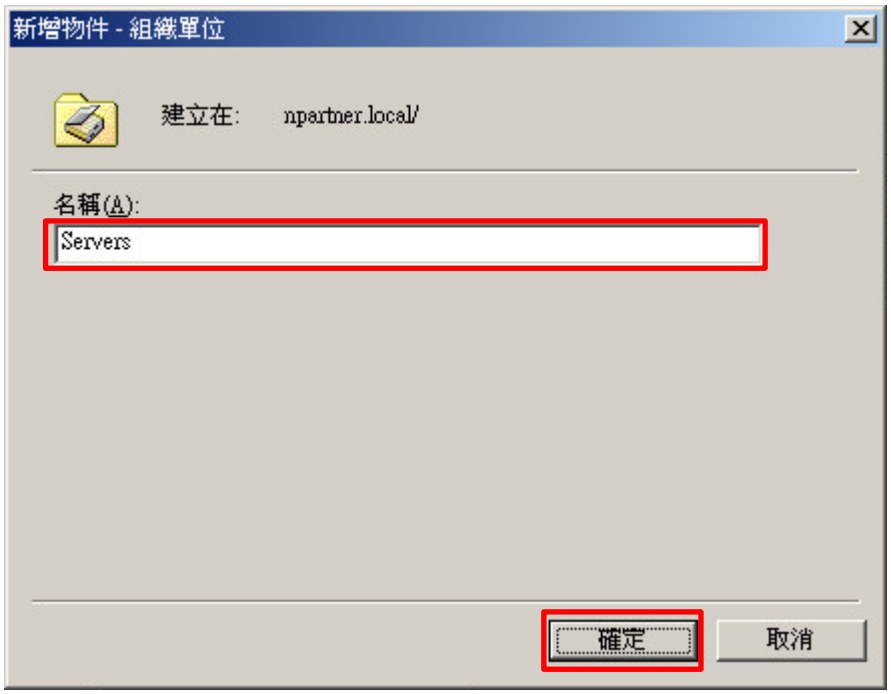
(2) 新增組織單位

[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]



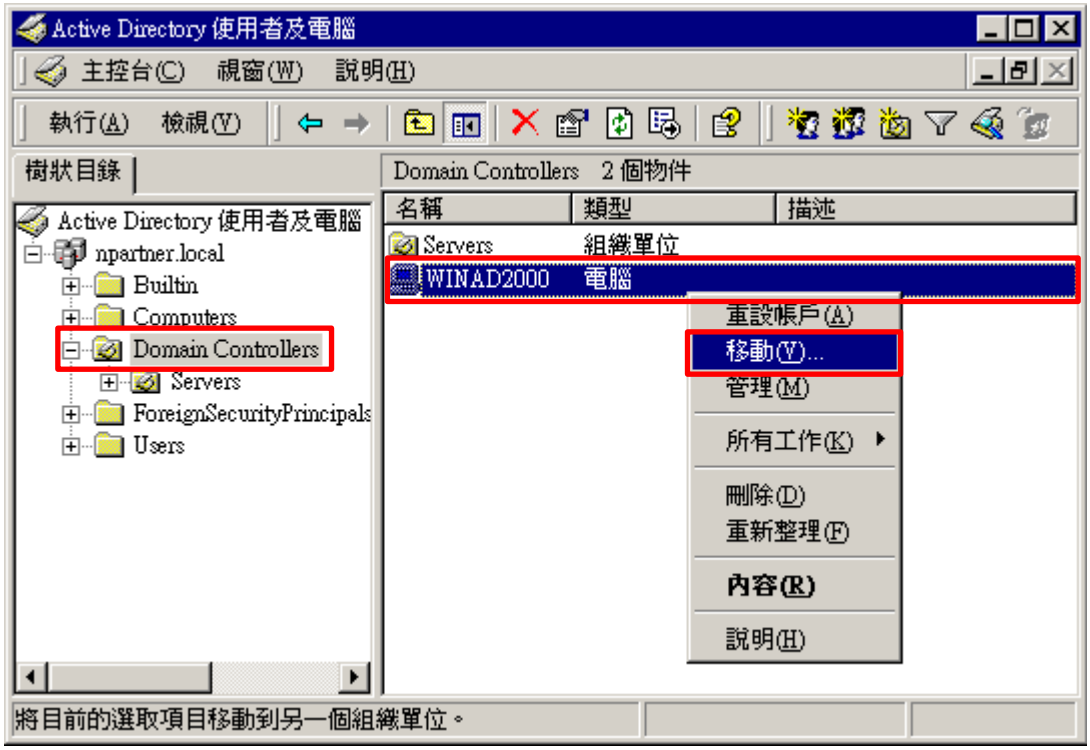
(3) 輸入組織單位名稱

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]

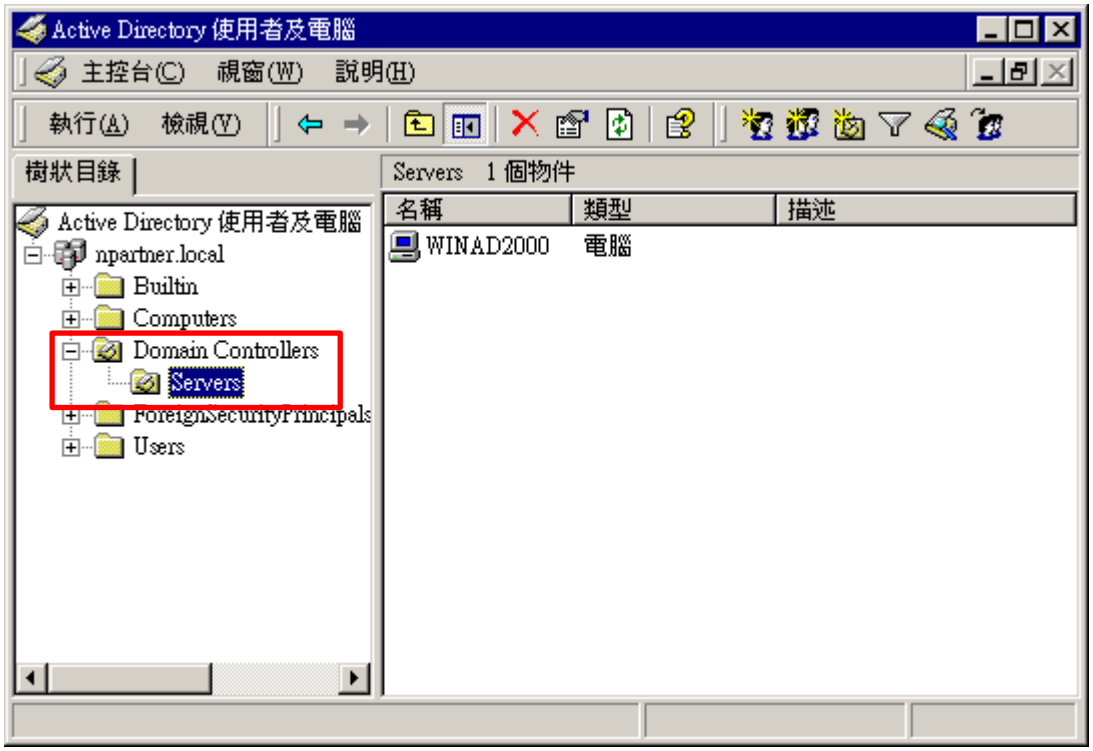


(5) 選擇組織單位

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。



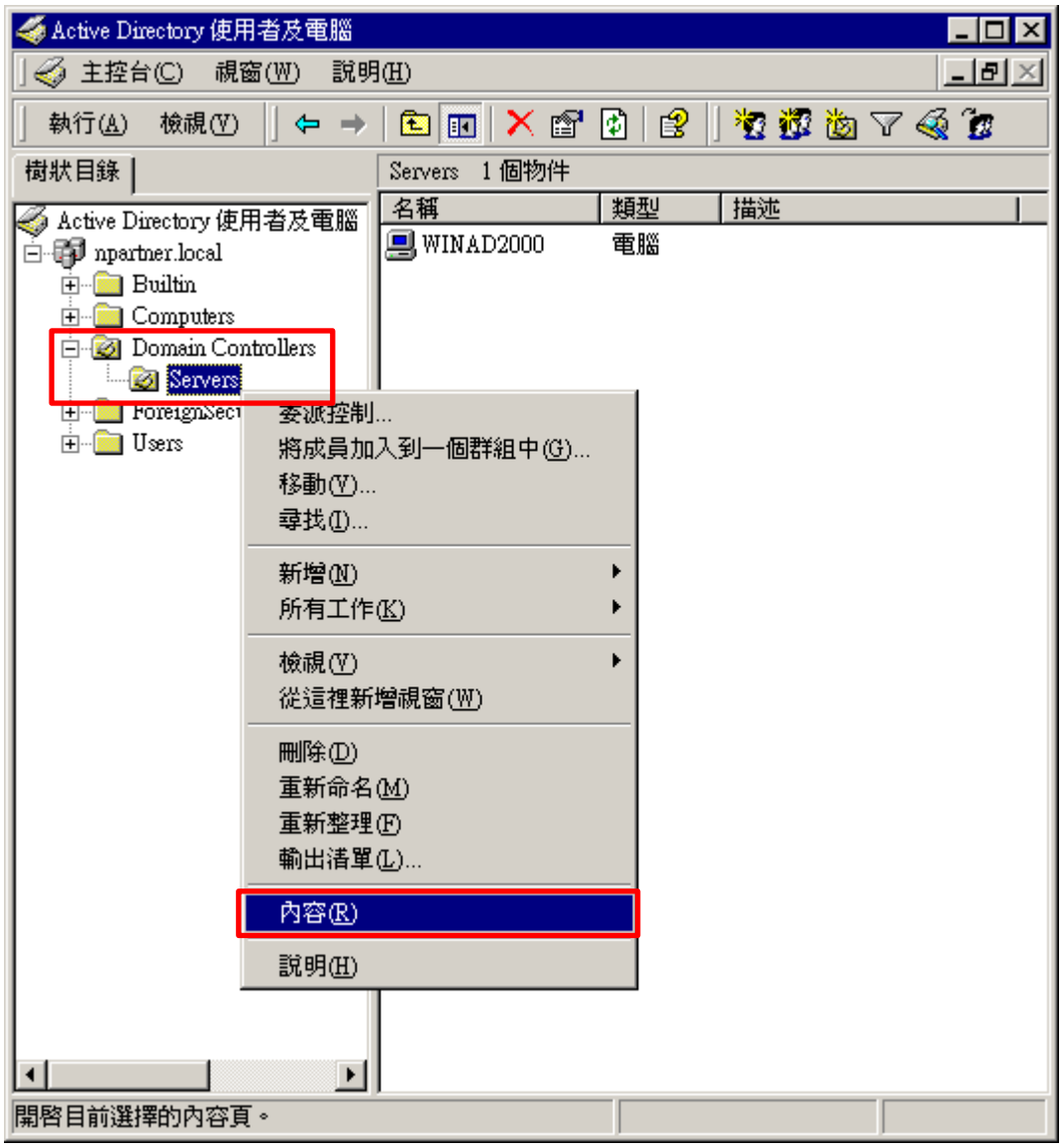
2.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

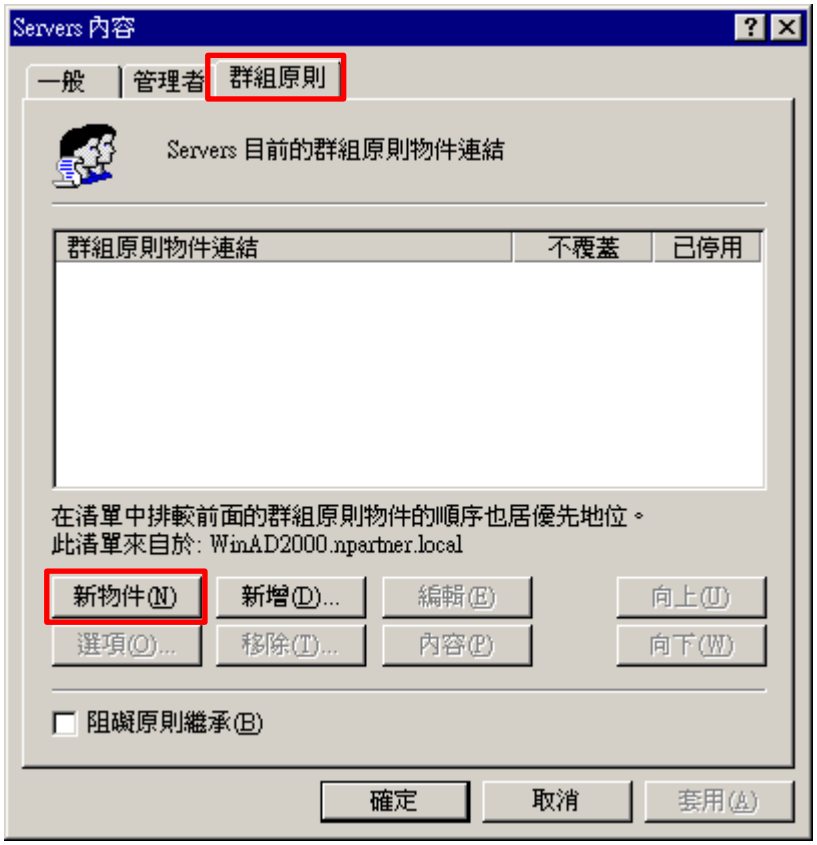
(2) 在 Servers 組織單位，點選內容

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



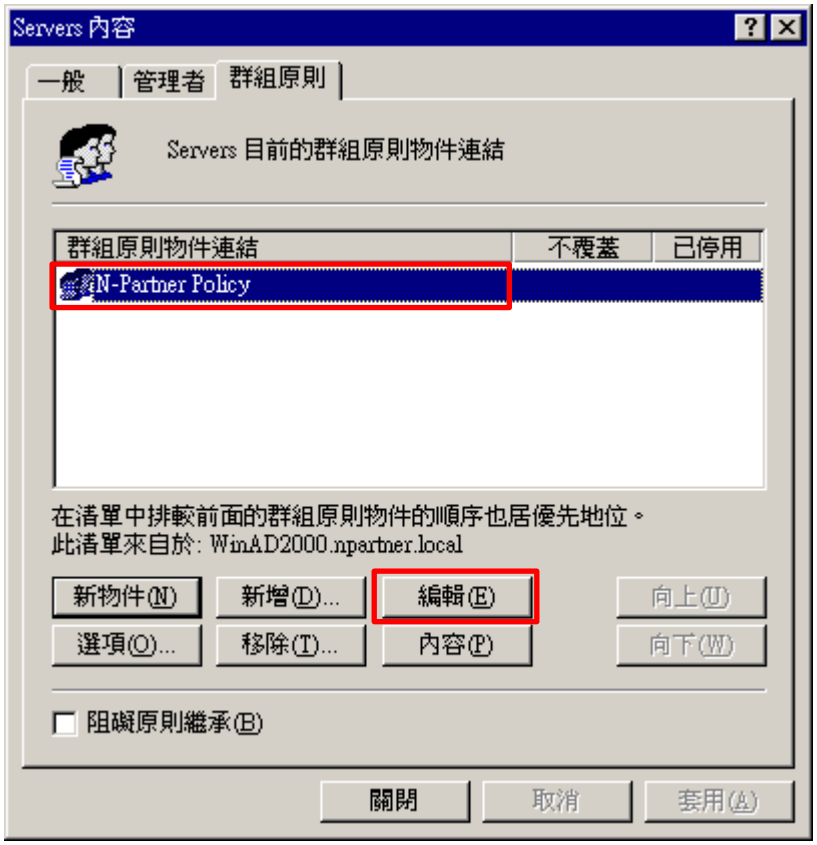
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



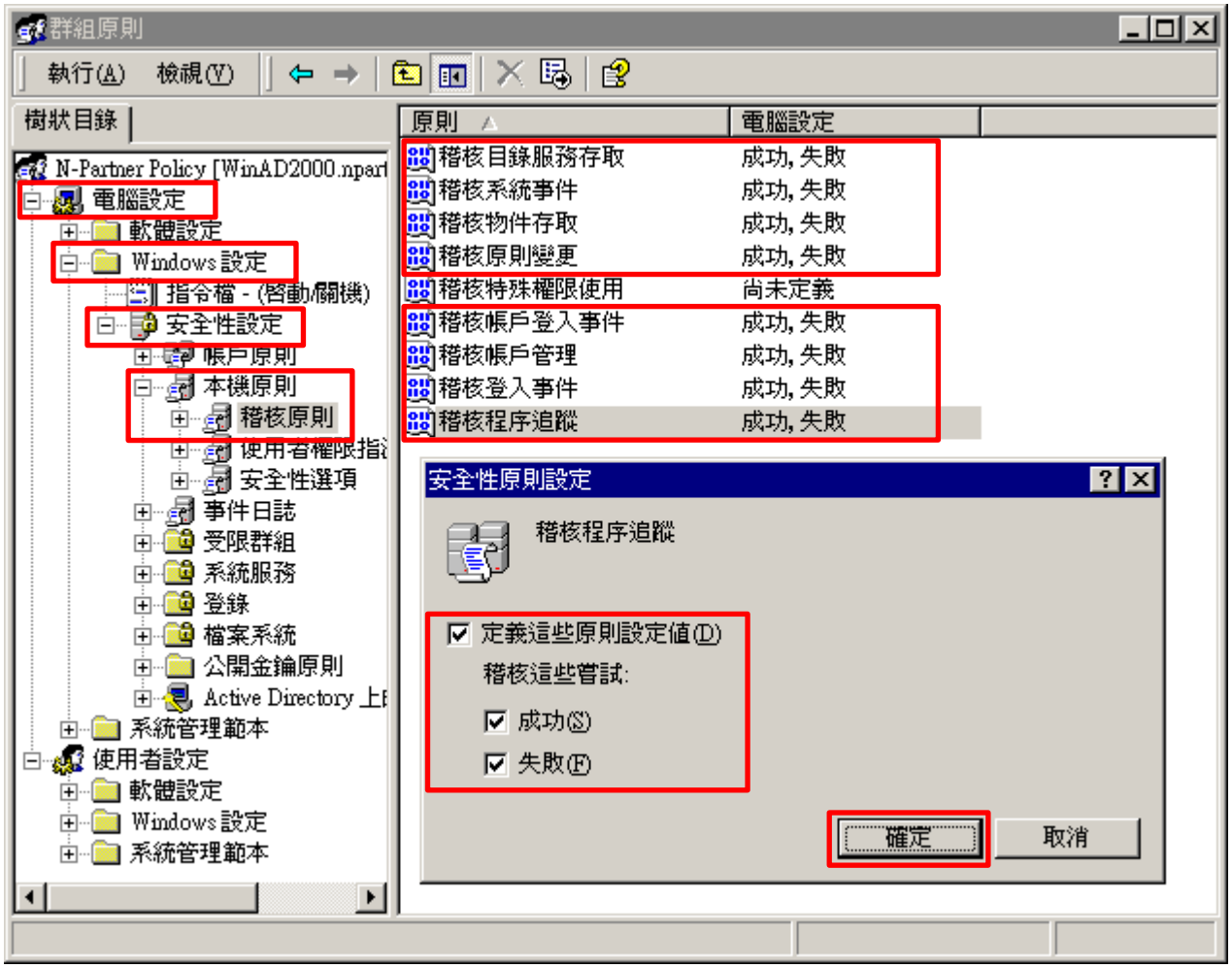
(4) 編輯群組原則物件

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]



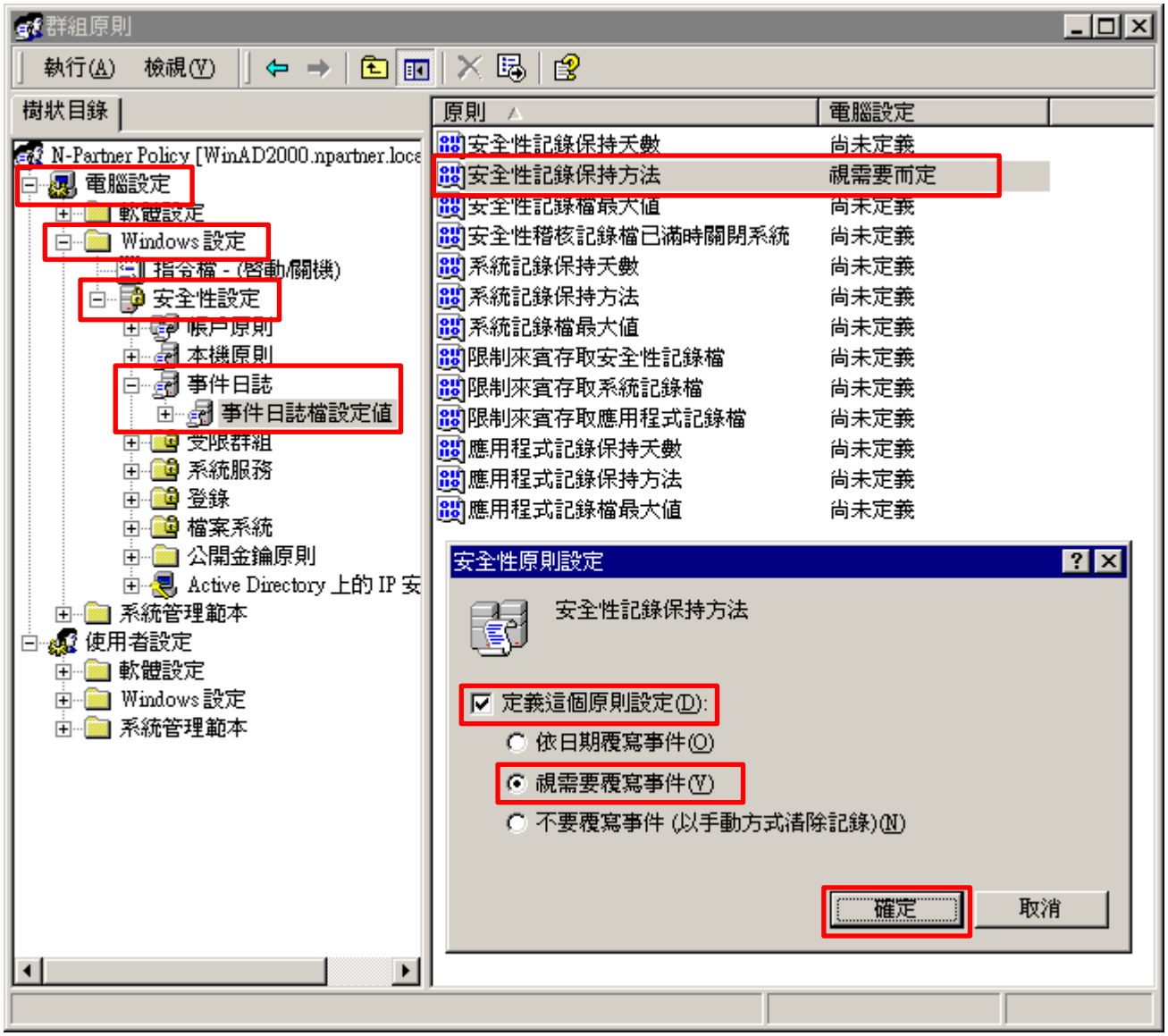
(5) 本機原則：稽核原則

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]



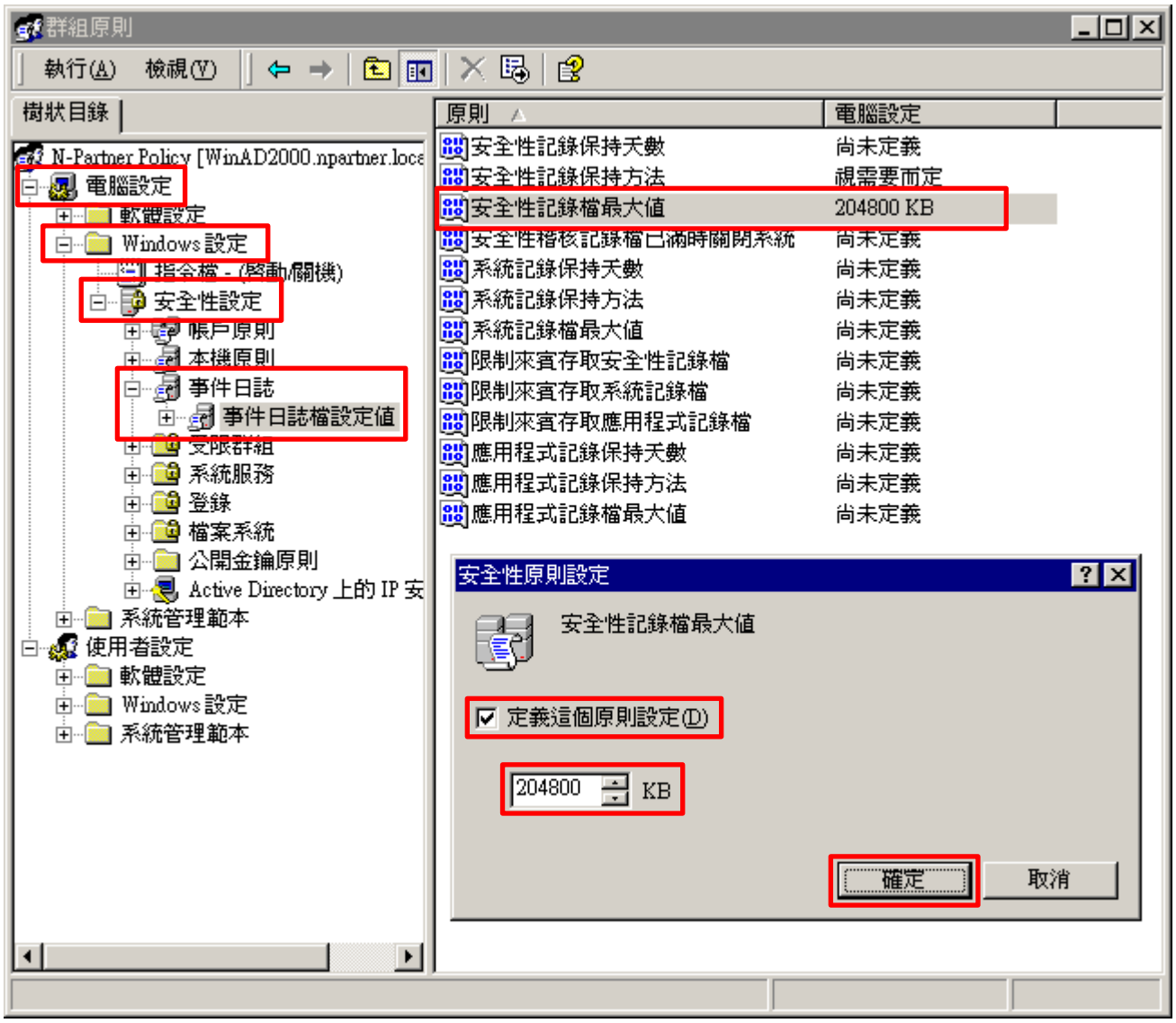
(6) 事件日誌：安全性記錄保持方法

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]

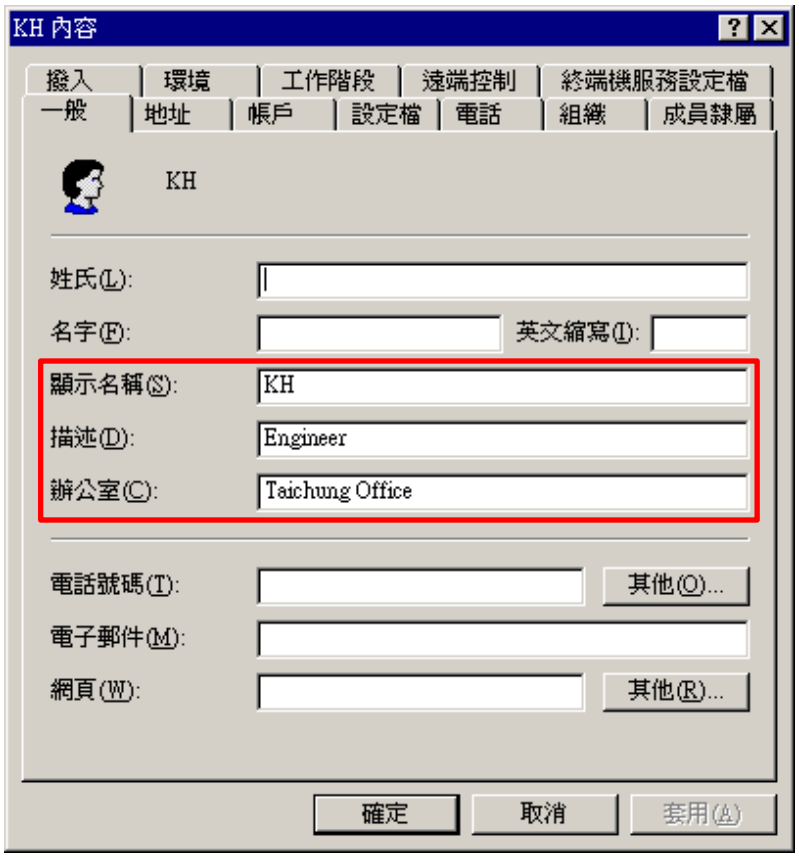
(9) 更新群組原則。

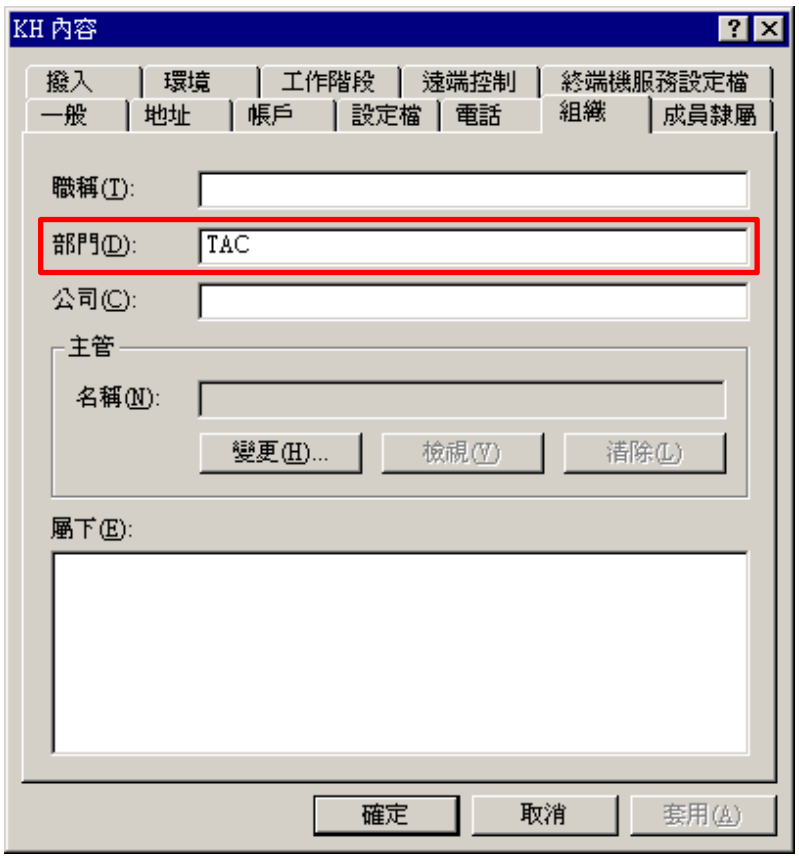
```
C:\> secedit /refreshpolicy machine_policy /enforce
```

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





(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)

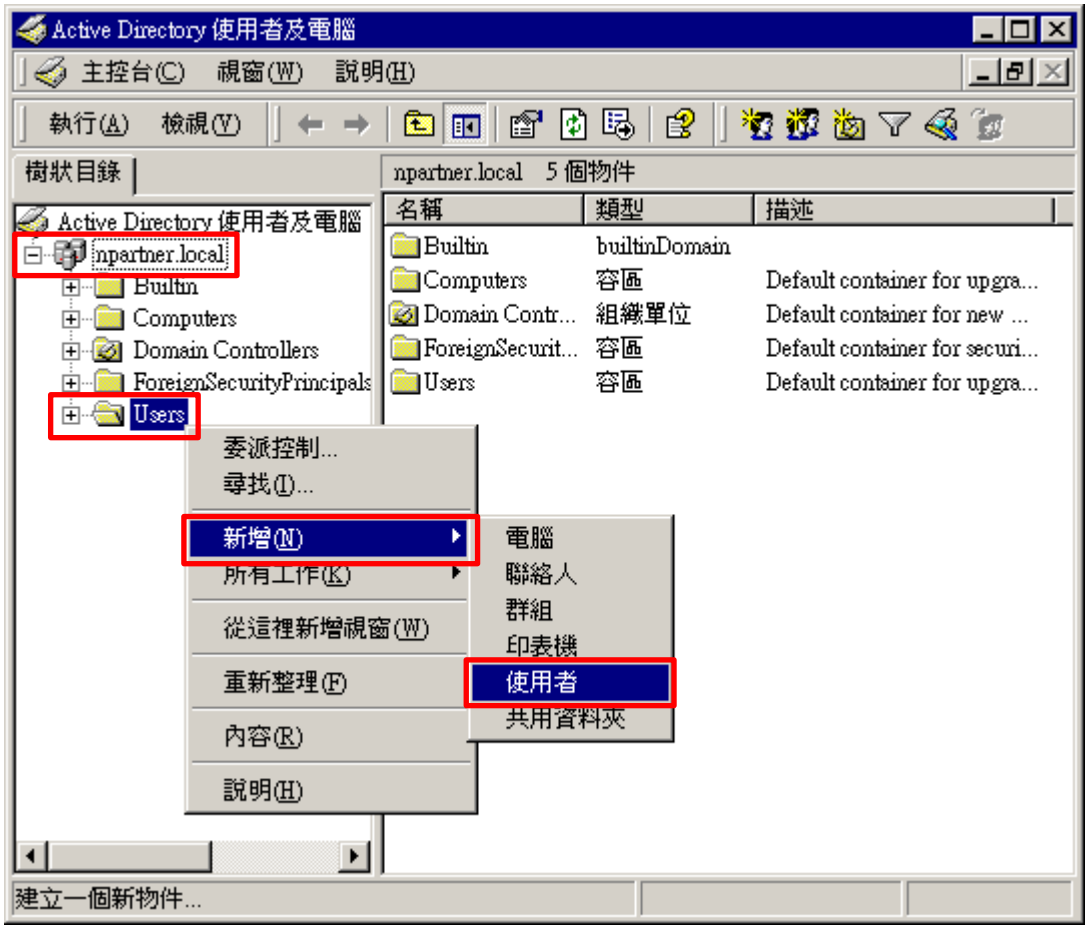
2.3.1 新增非管理帳號

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

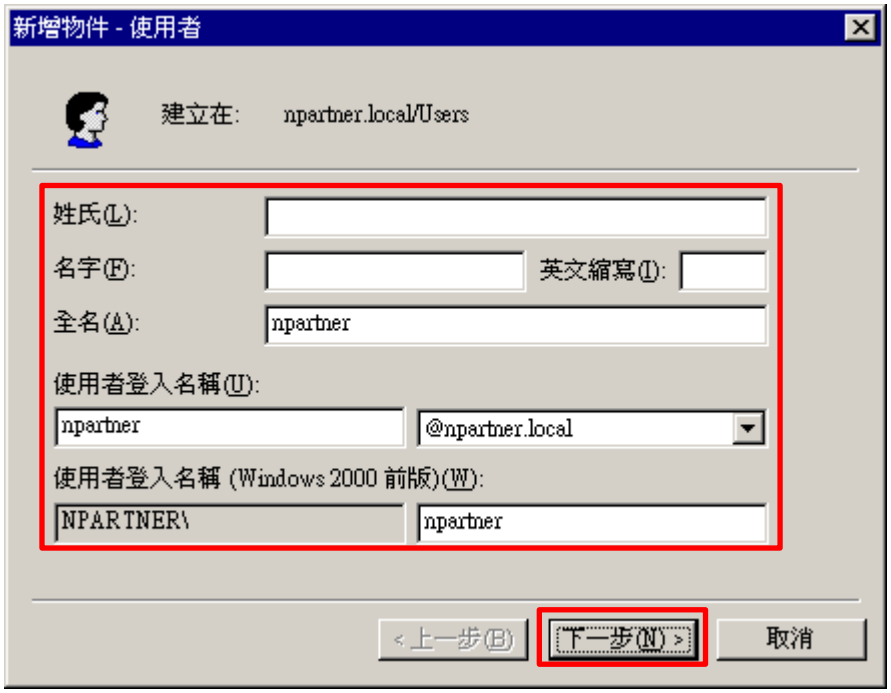
(2) 新增帳號

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]



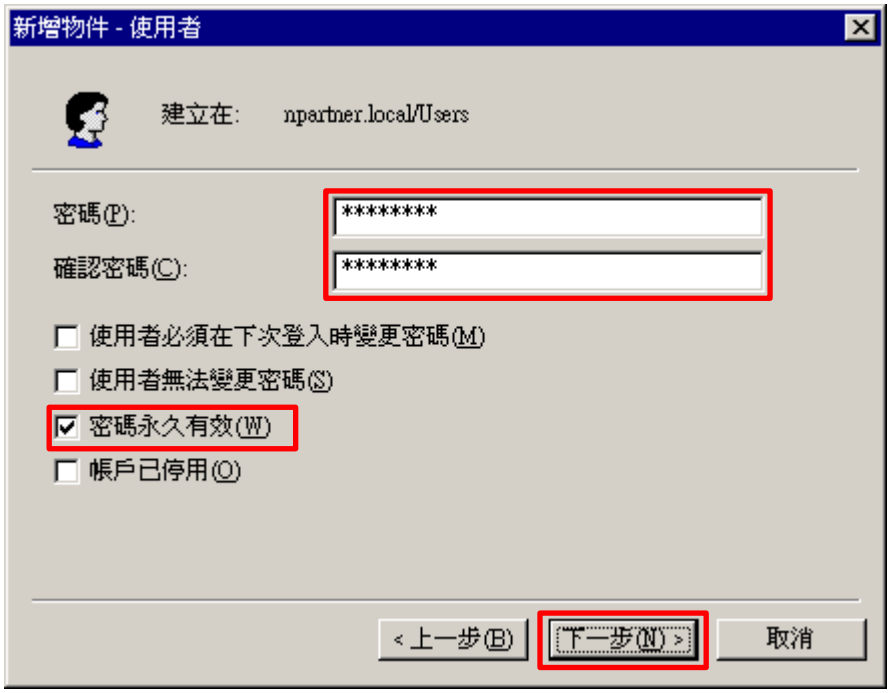
(3) 輸入帳號資訊

輸入使用者名稱 -> 按 [下一步]

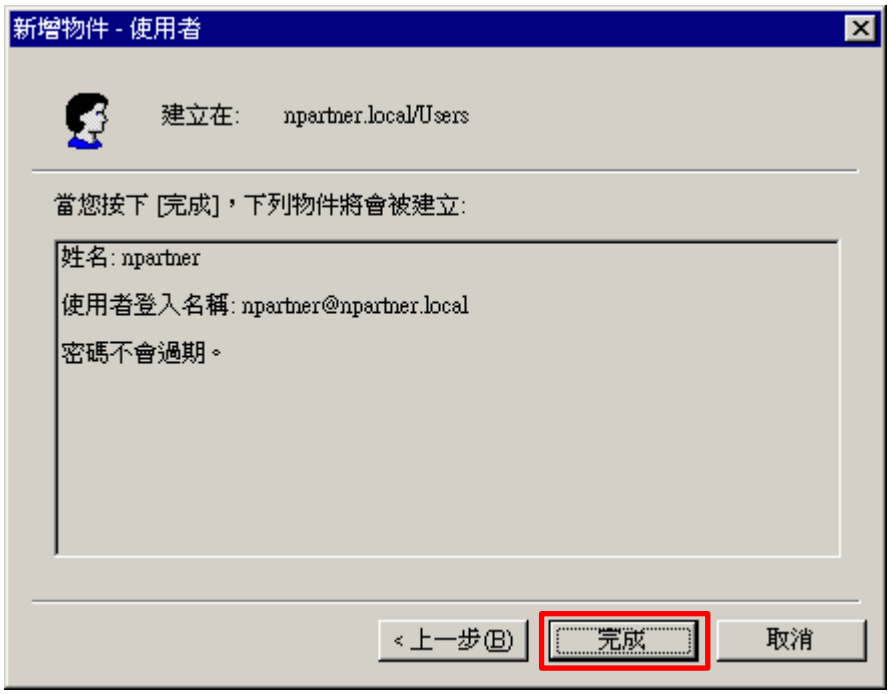


(4) 輸入使用者密碼

輸入兩次相同 [密碼] -> 勾選 [密碼永久有效] -> 按 [下一步]



(5) 按 [完成]



2.3.2 設定 DCOM 權限

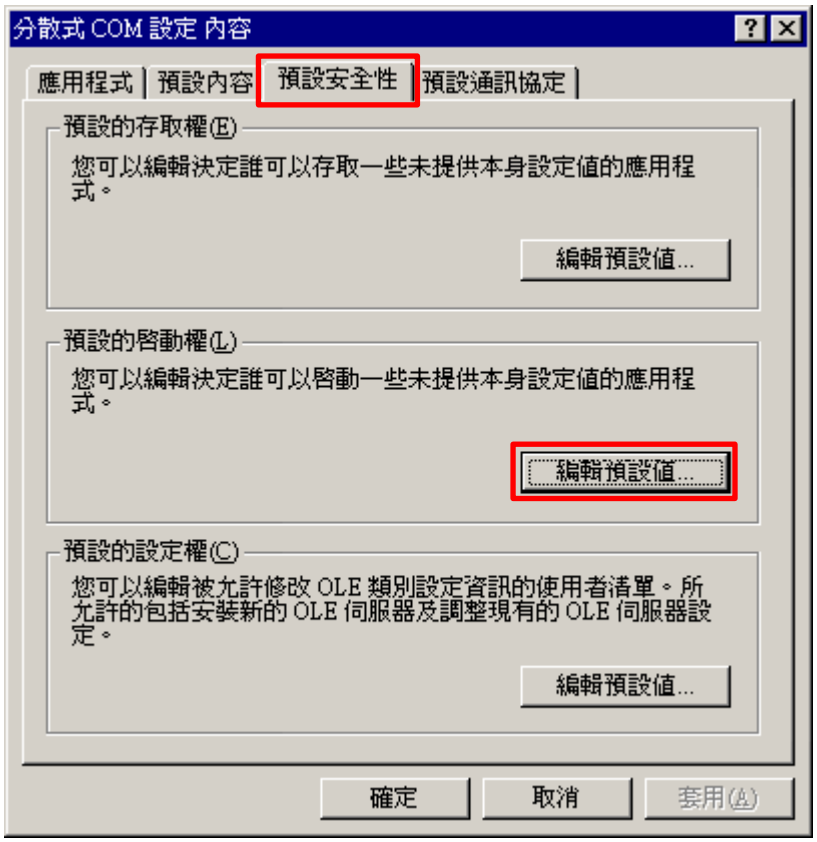
(1) 開啟 [命令提示字元]

(2) 開啟元件服務

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

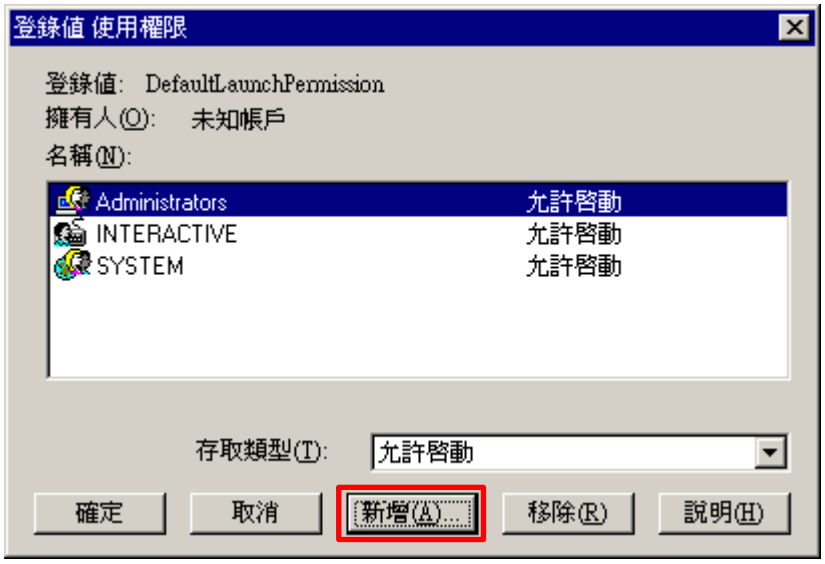
(3) 啟用權限

點選 [預設安全性] 頁面 -> 預設的啟動權，按 [編輯預設值]



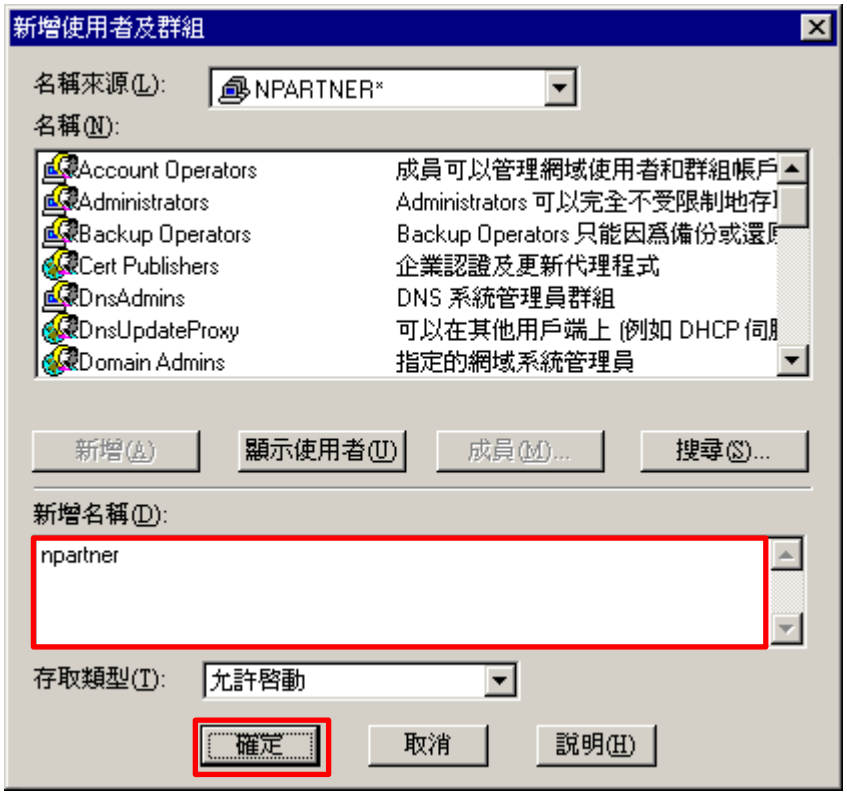
(4) 新增 DCOM 使用者權限

點選 [新增]

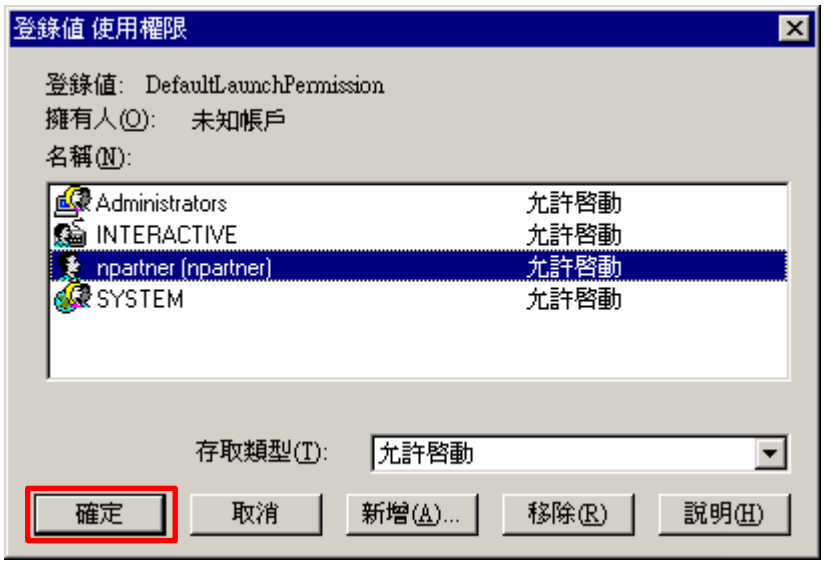


(5) 輸入使用者

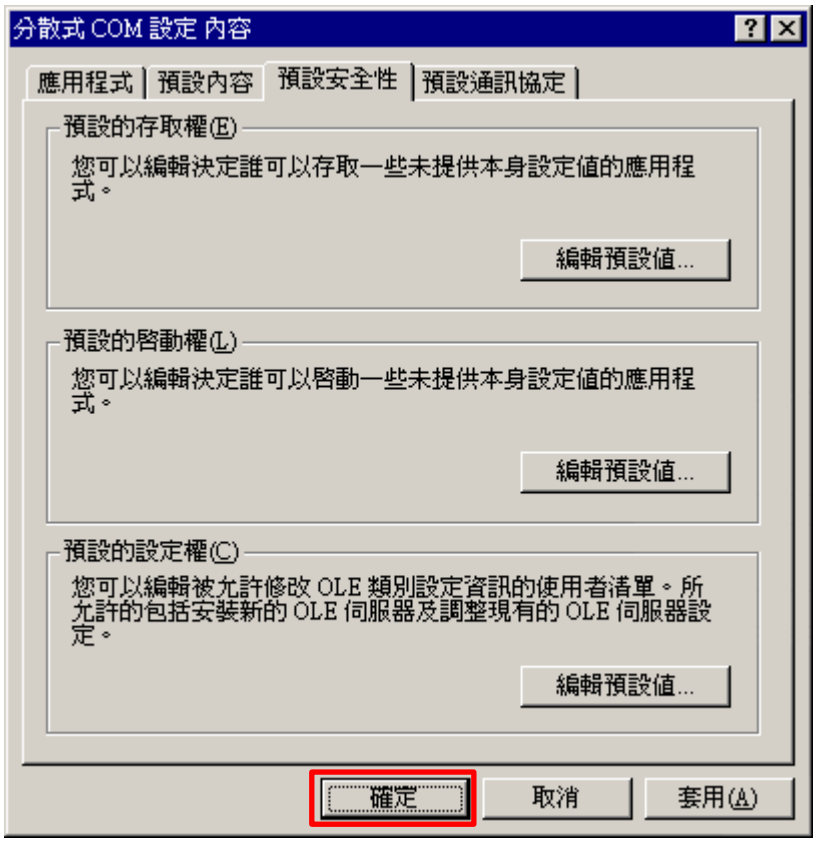
輸入使用者帳號: npartner -> 按 [確定]



(6) 按 [確定]



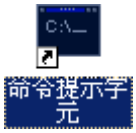
(7) 按 [確定]



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]

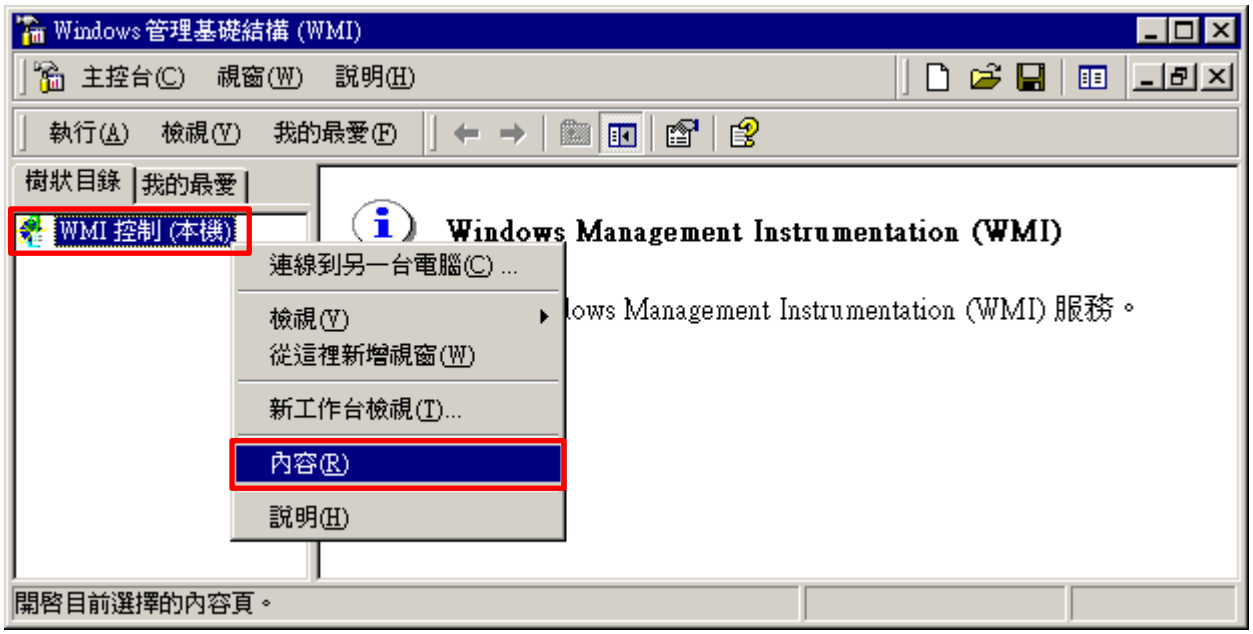


(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

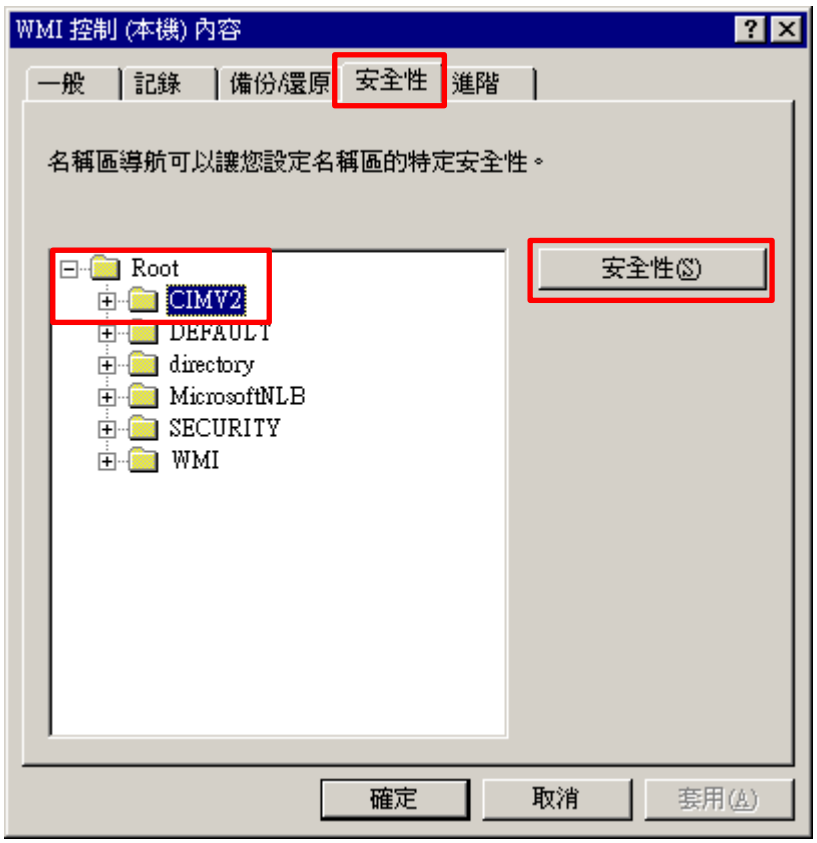
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



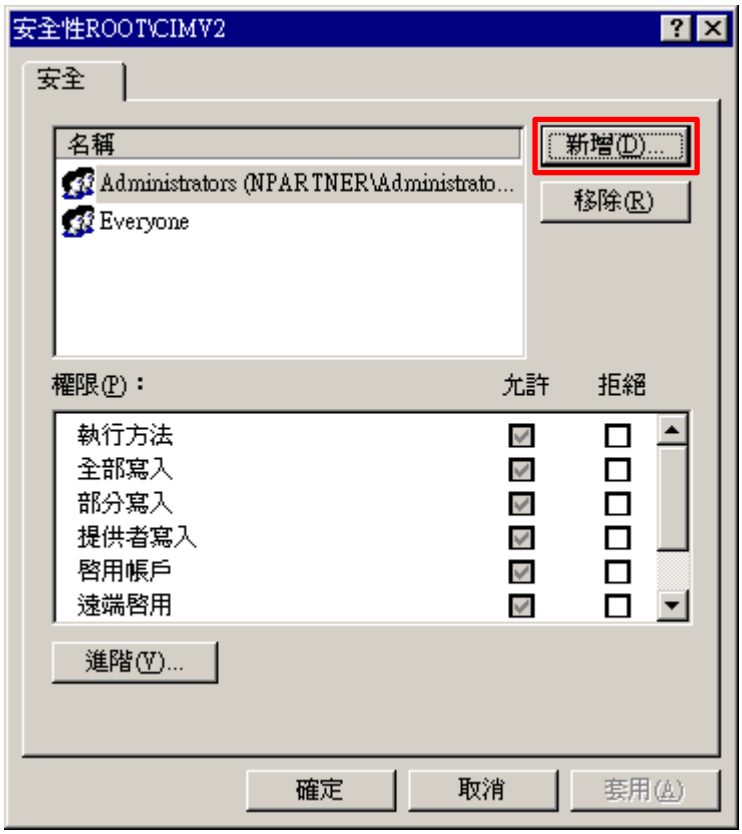
(4) 編輯 CIMV2 安全性

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



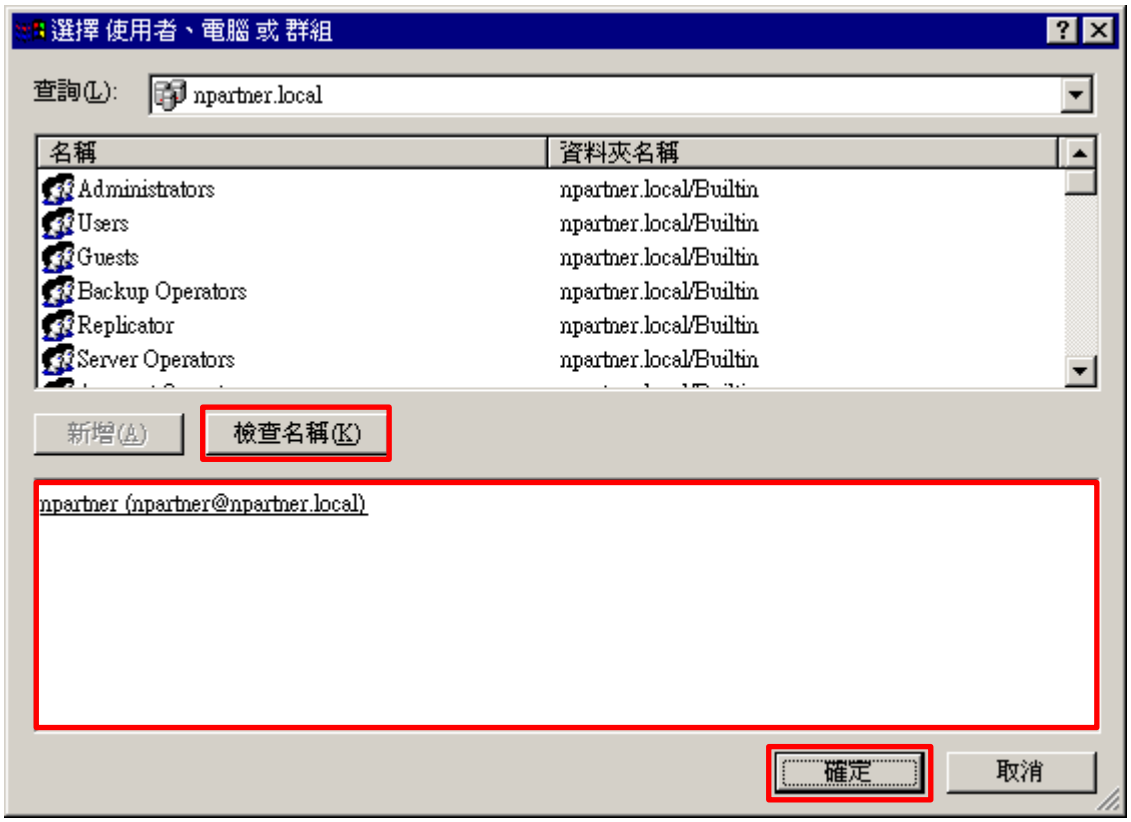
(5) 新增 WMI 使用者權限

按 [新增]



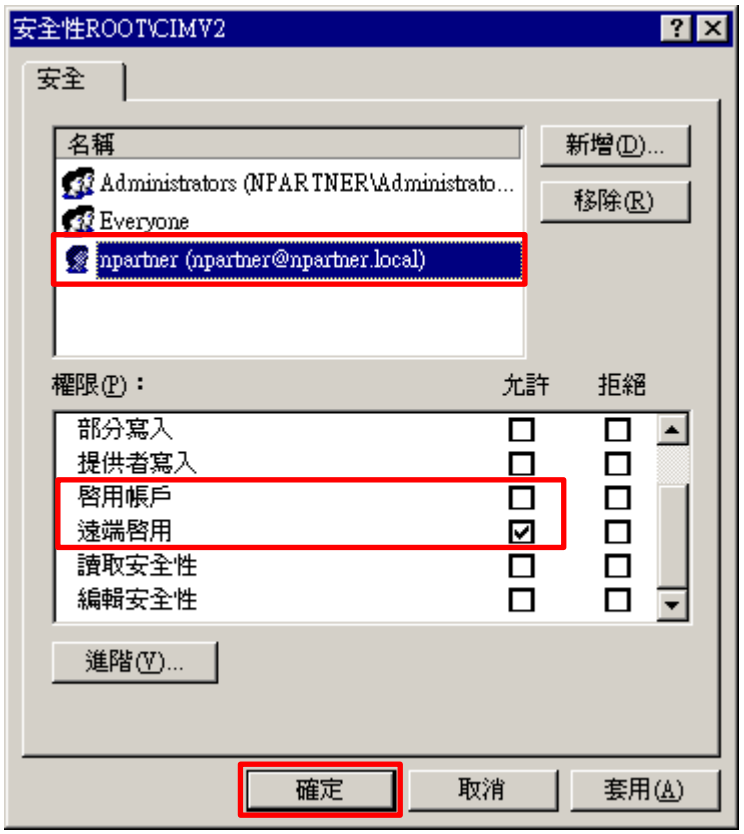
(6) 輸入使用者

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

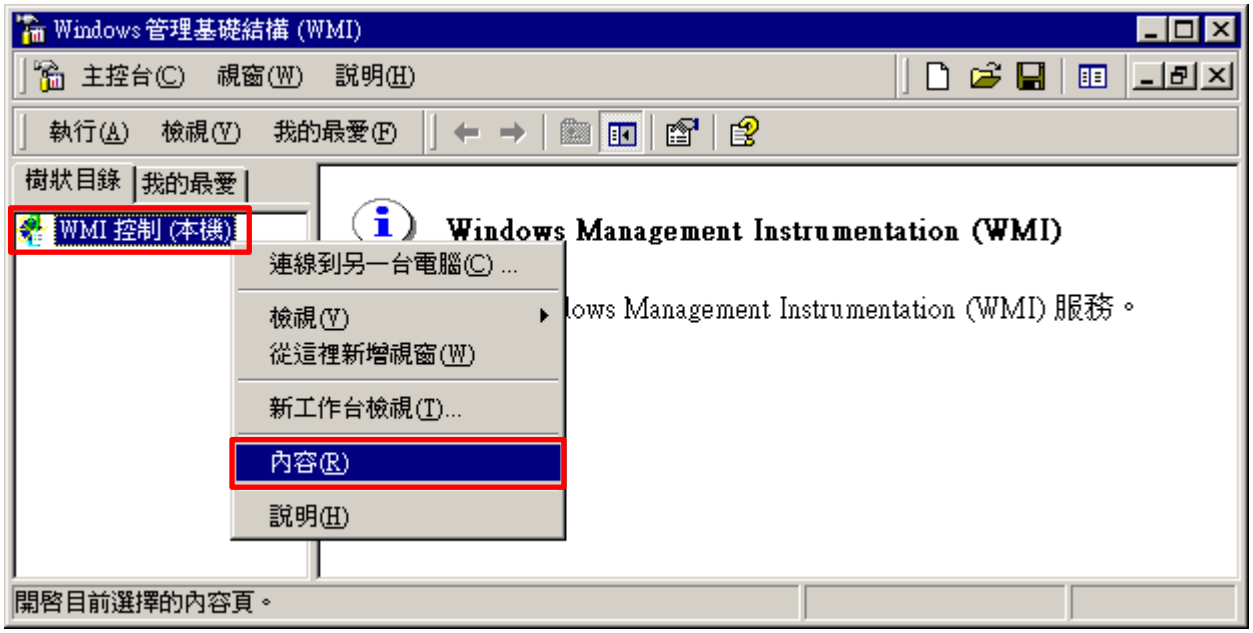
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

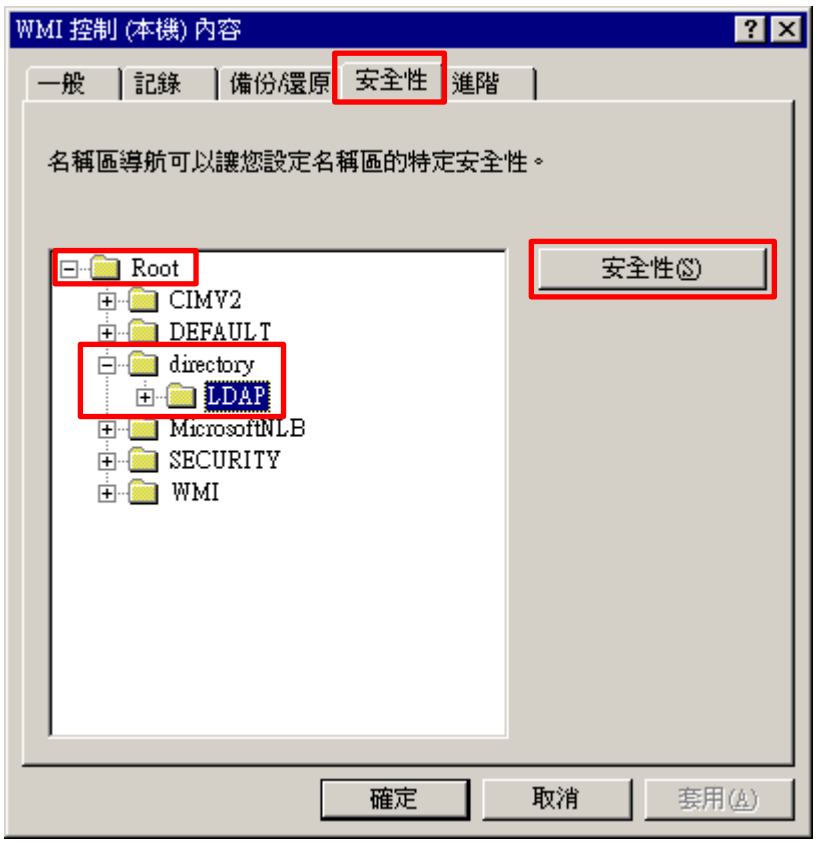
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



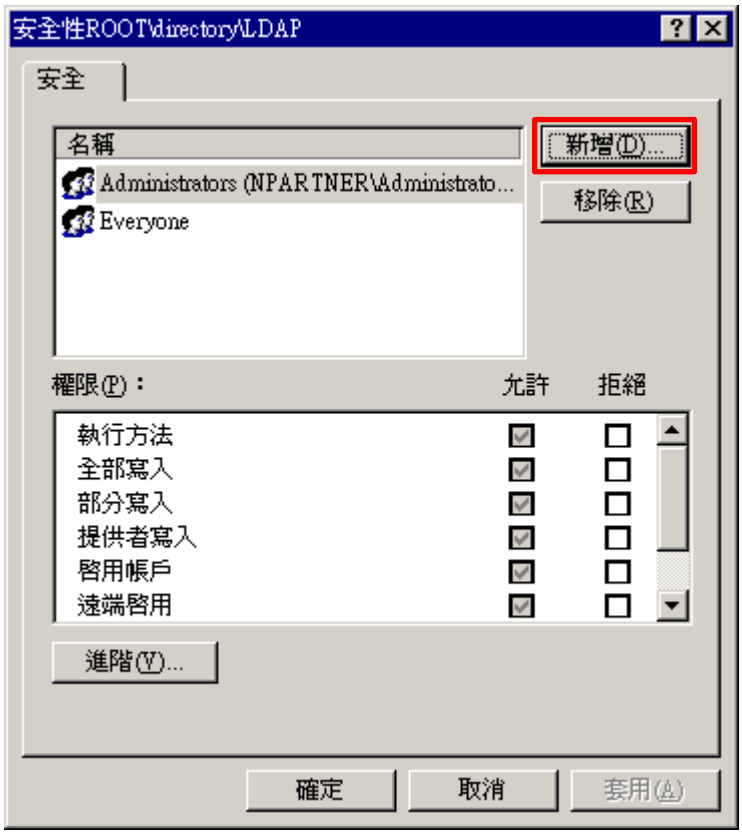
(4) 編輯 LDAP 安全性

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



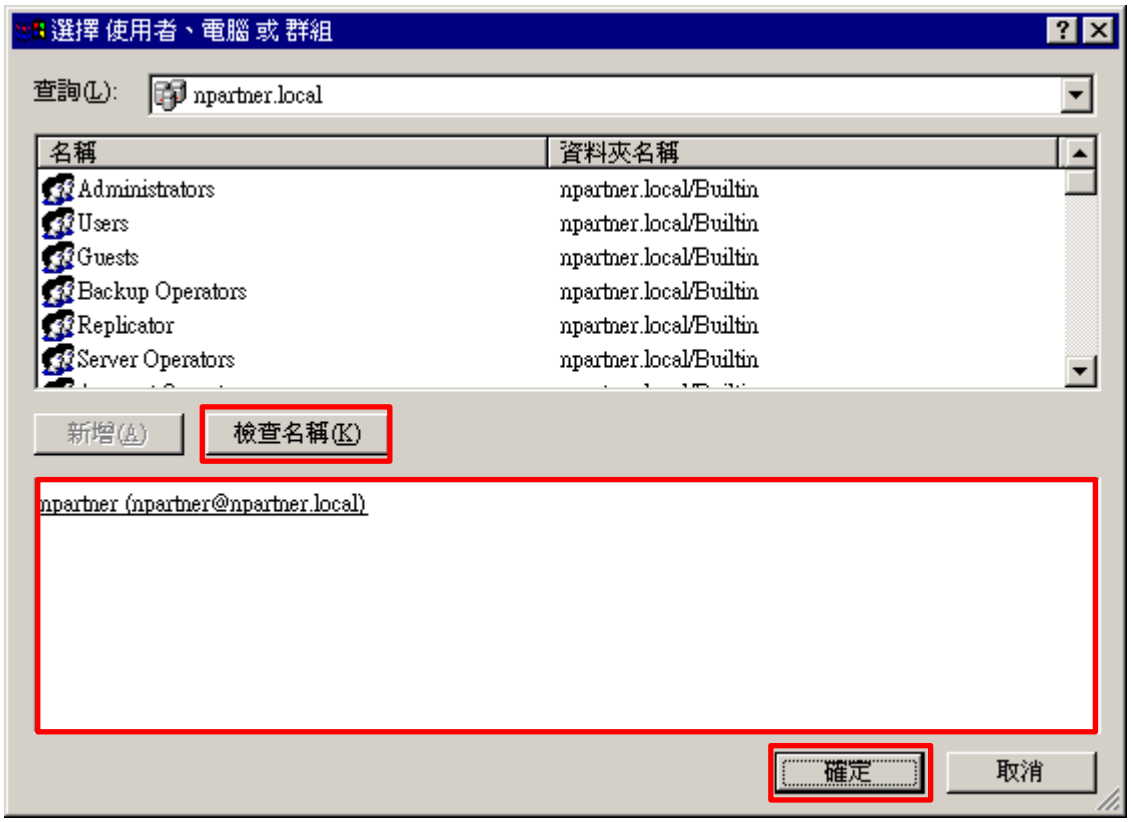
(5) 新增 WMI 使用者權限

按 [新增]



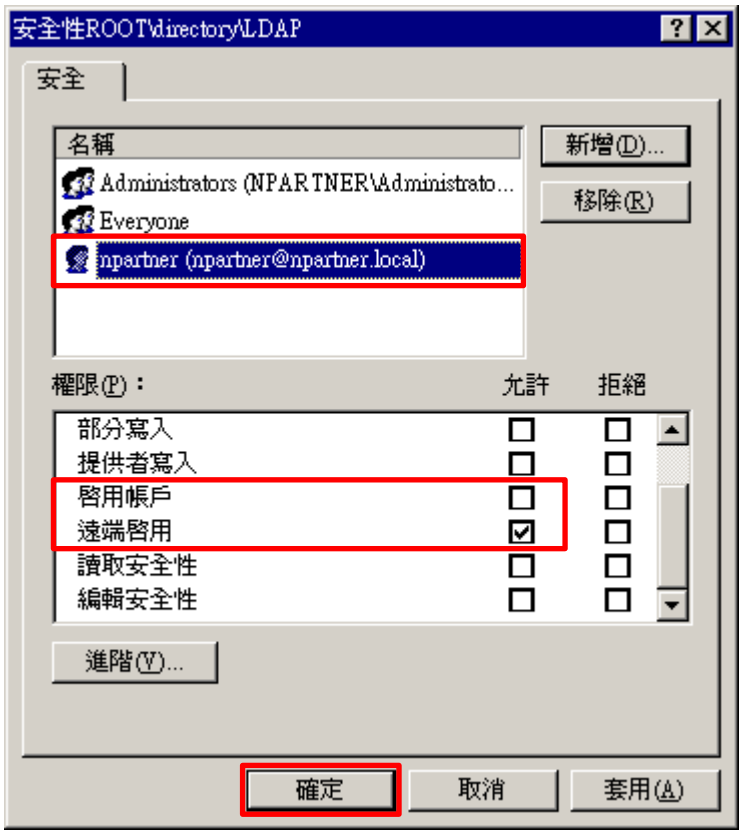
(6) 輸入使用者

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

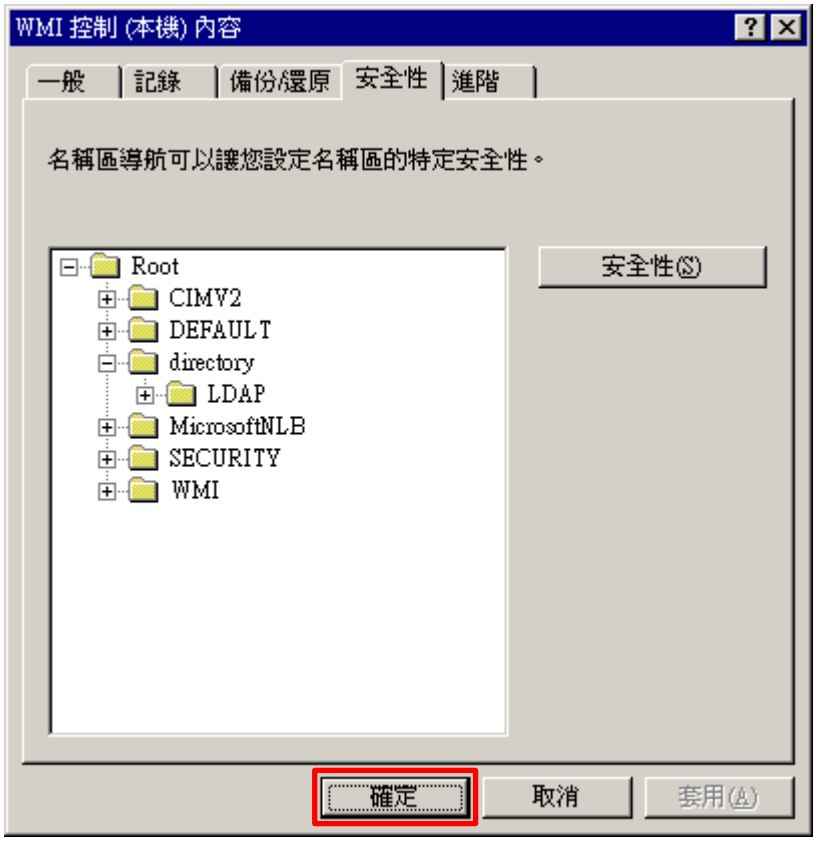


(7) 設定使用者權限

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]



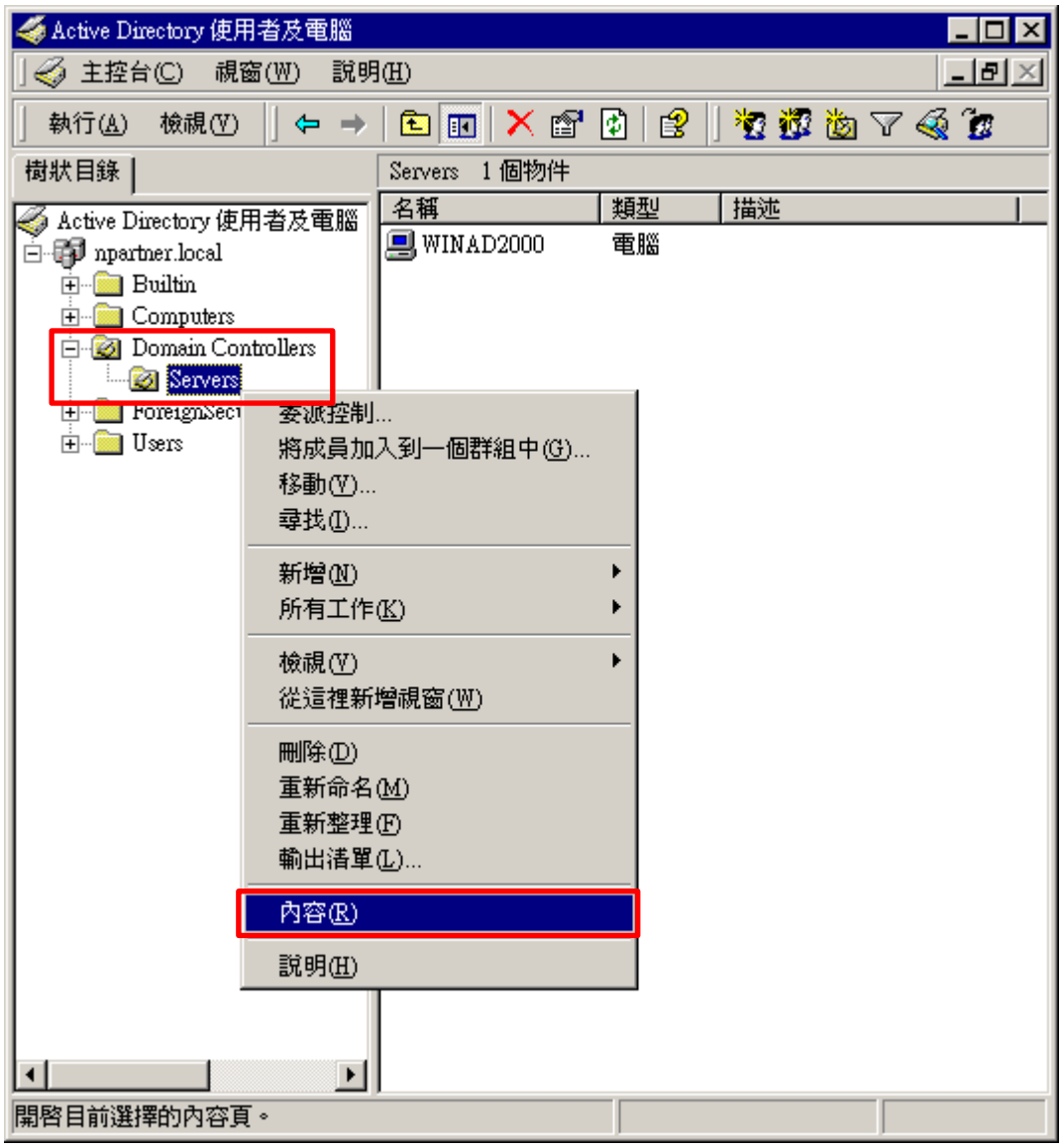
2.3.4 設定 Event log 讀取權限

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

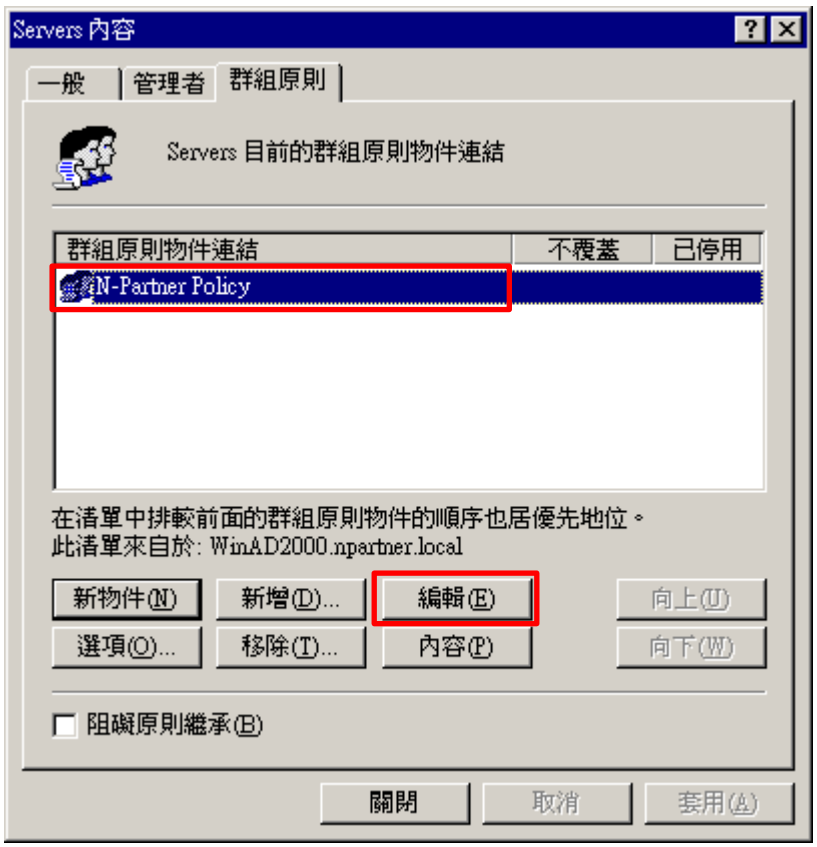
(2) 在 Servers 組織單位，點選內容

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



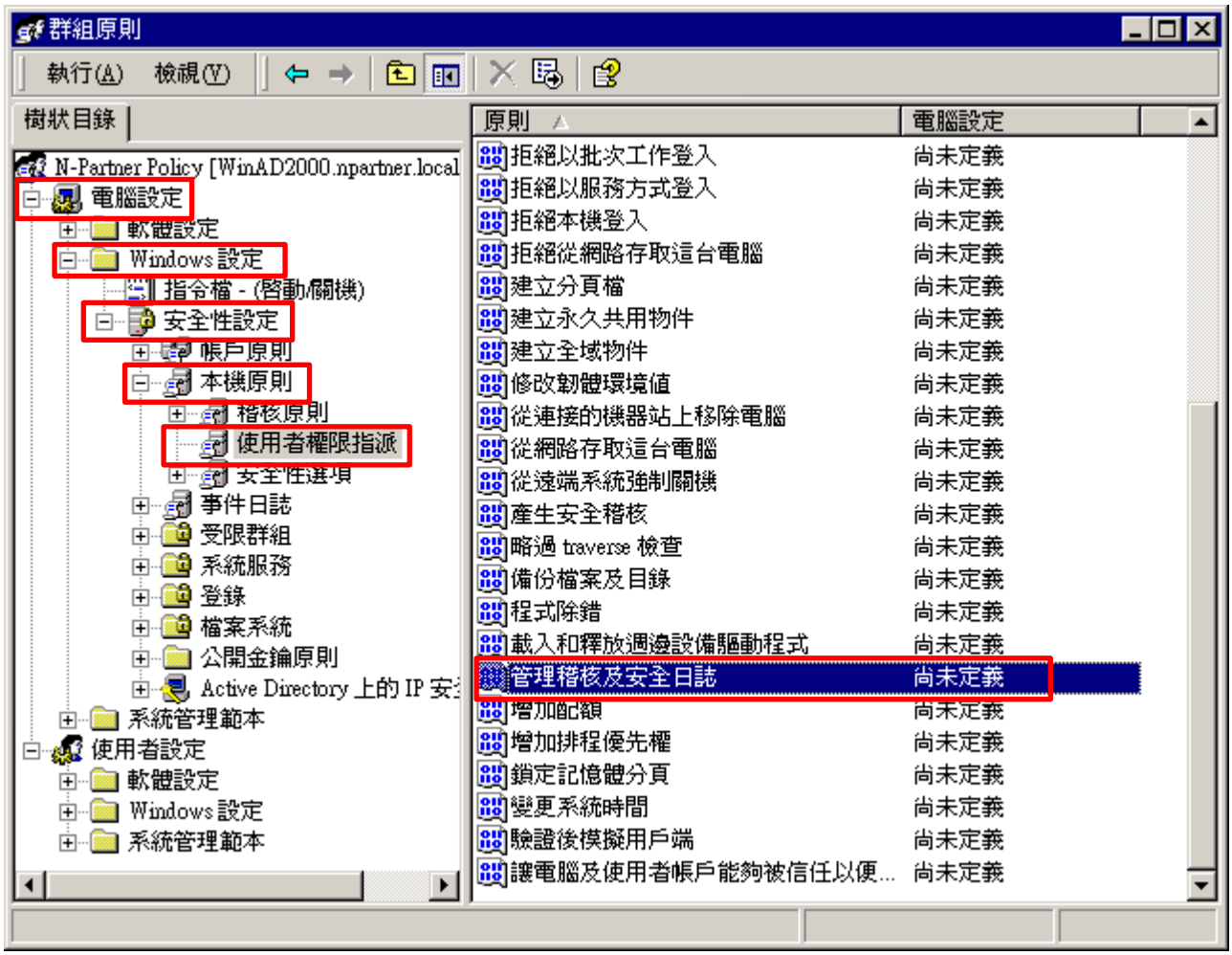
(3) 編輯群組原則物件

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

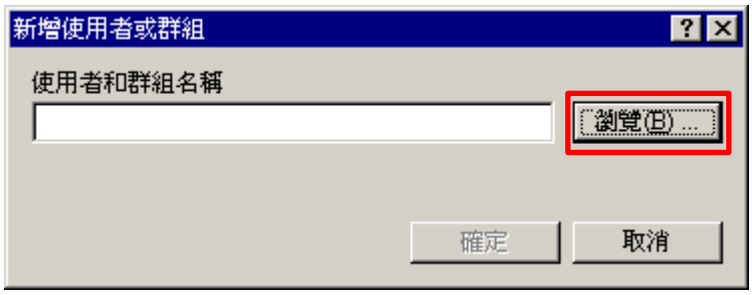


(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增]

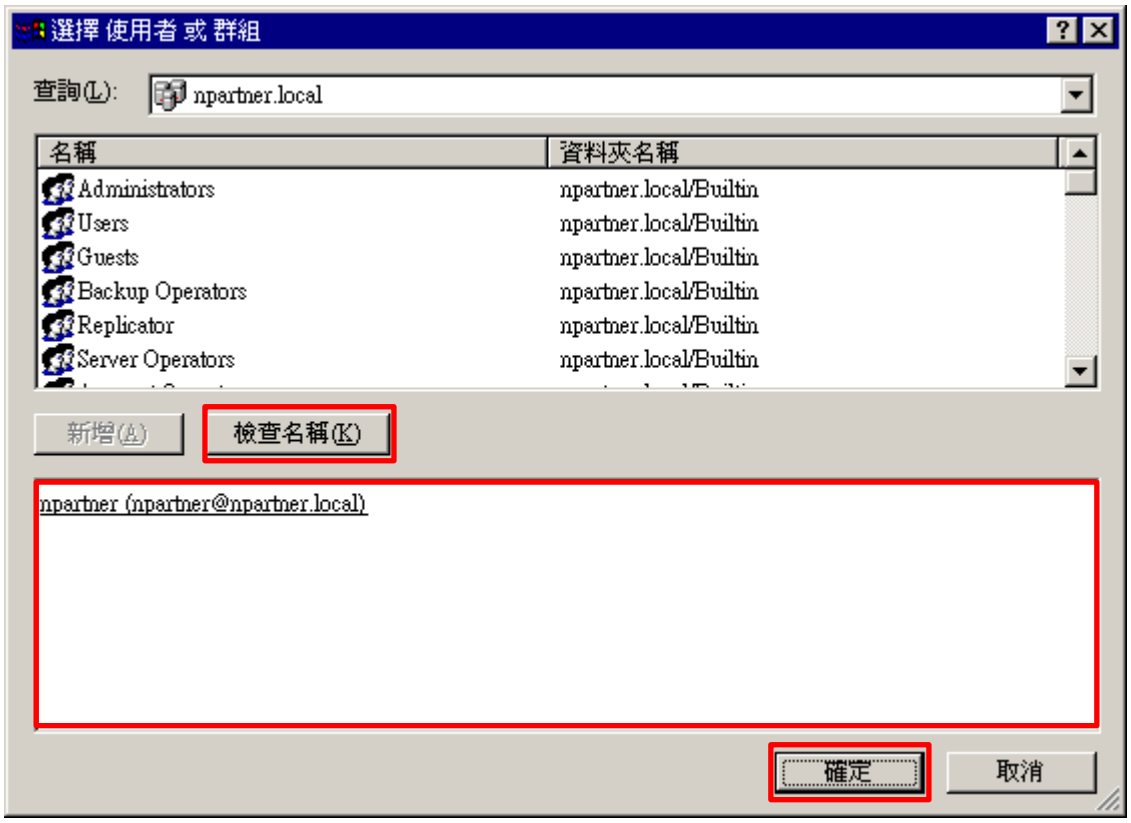
(6) 搜尋使用者

按 [瀏覽]



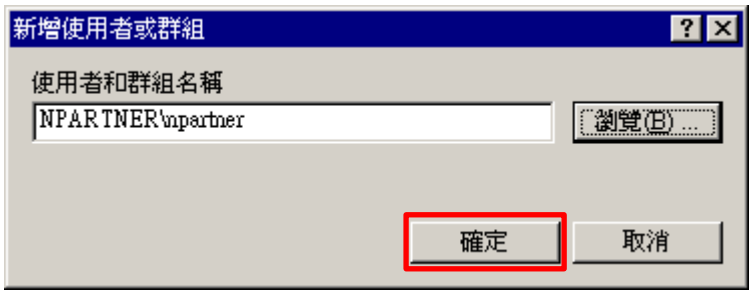
(7) 輸入使用者

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



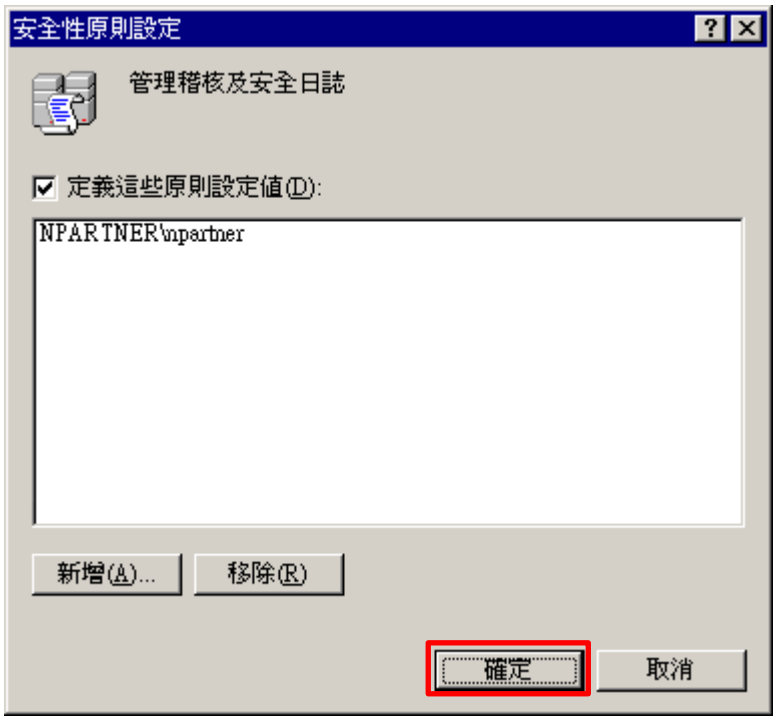
(8) 確定使用者

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:\> secedit /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

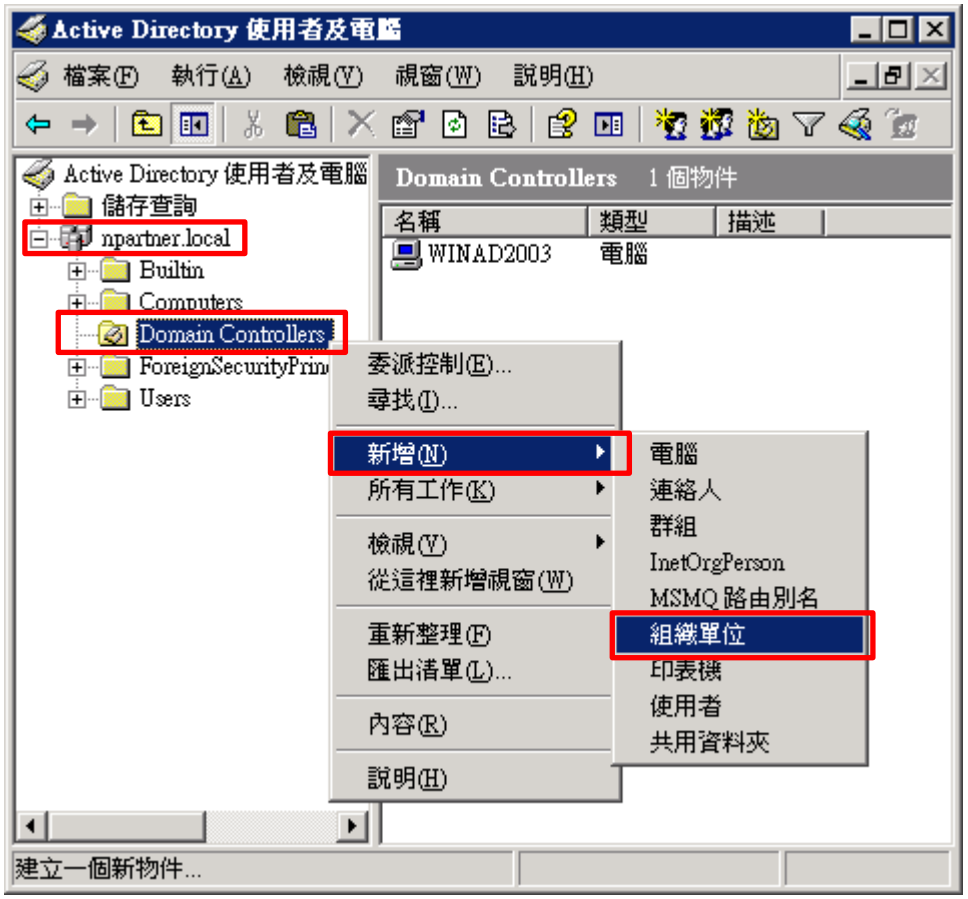
3.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者及電腦]

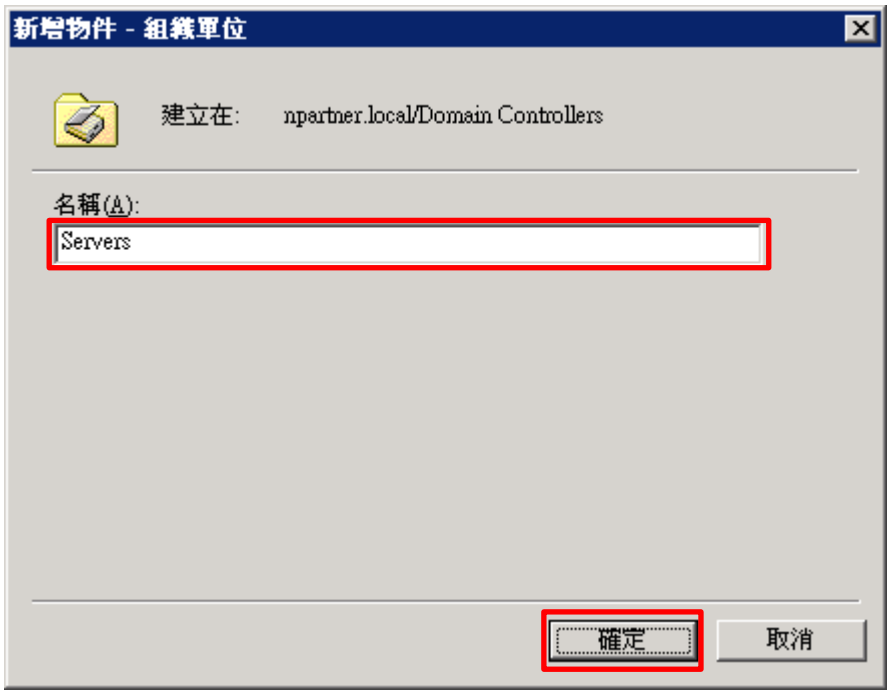
(2) 新增組織單位

[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]



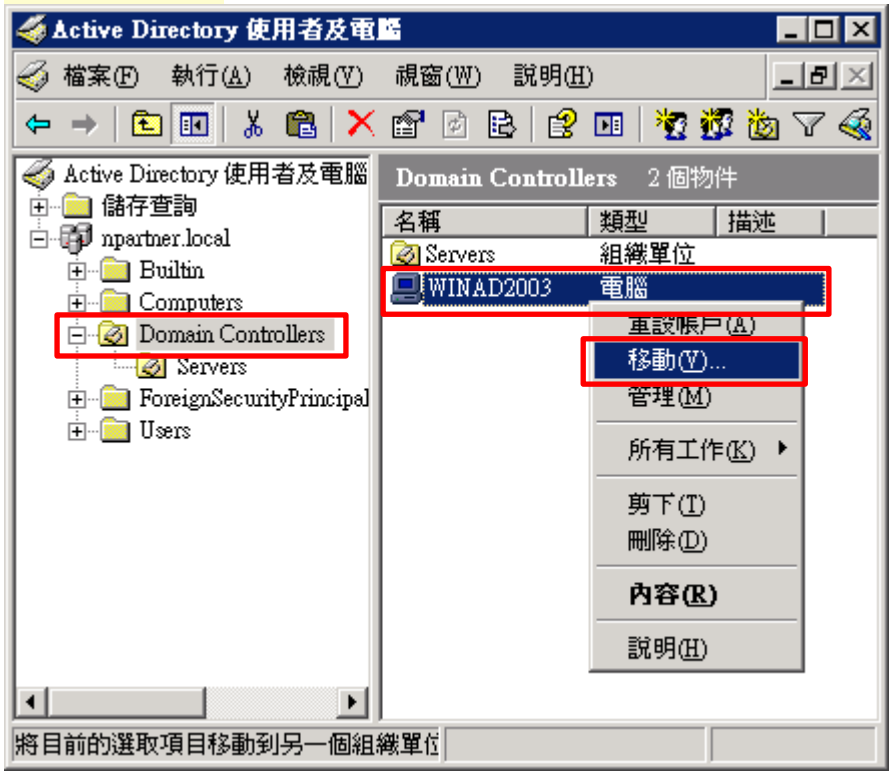
(3) 輸入組織單位名稱

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]

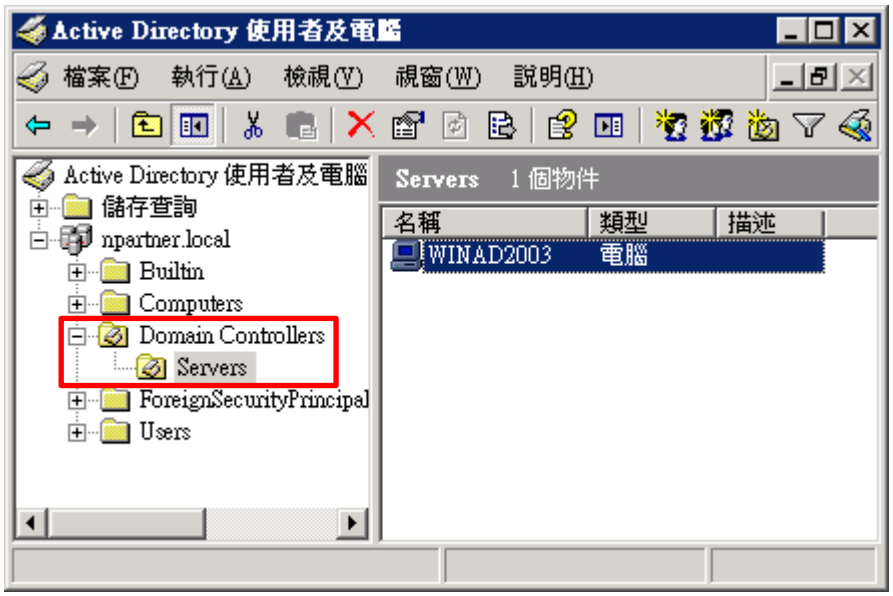


(5) 選擇組織單位

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。



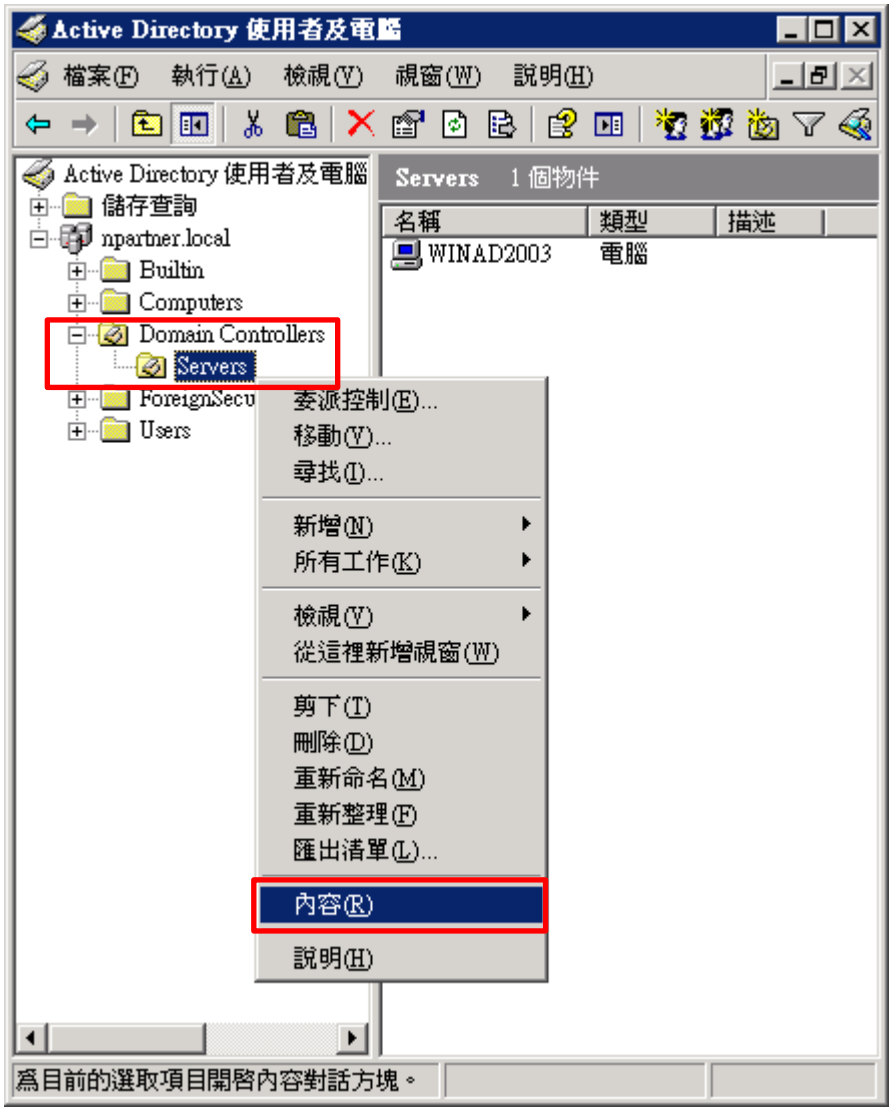
3.2 群組原則設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者及電腦]

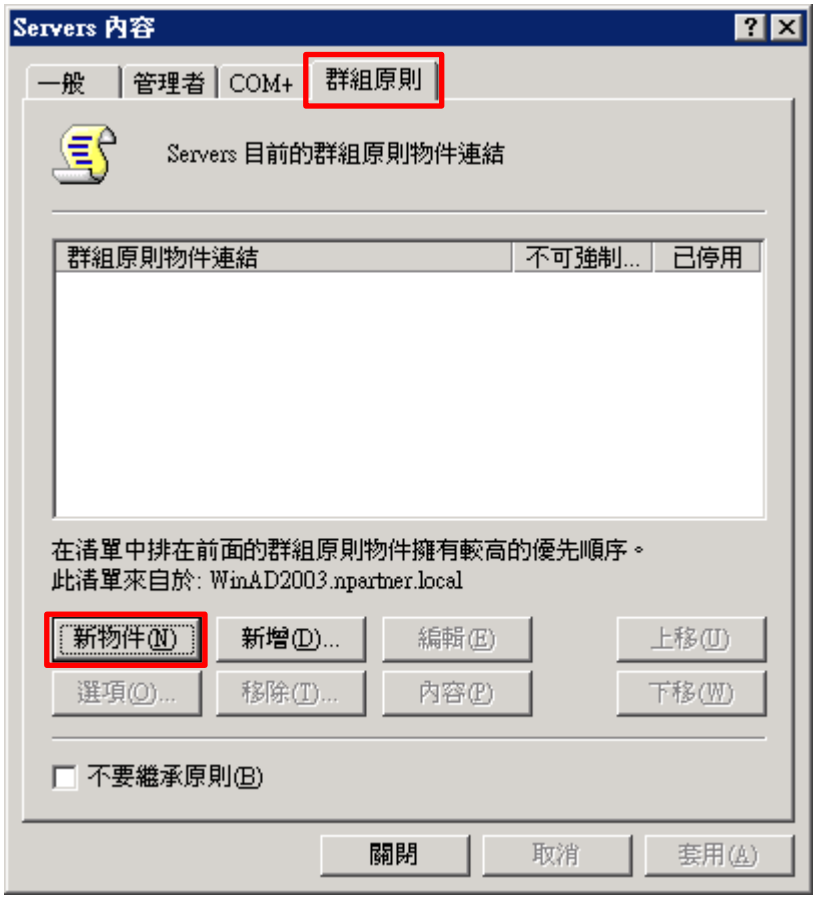
(2) Domain Controllers 的 Servers 組織單位

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



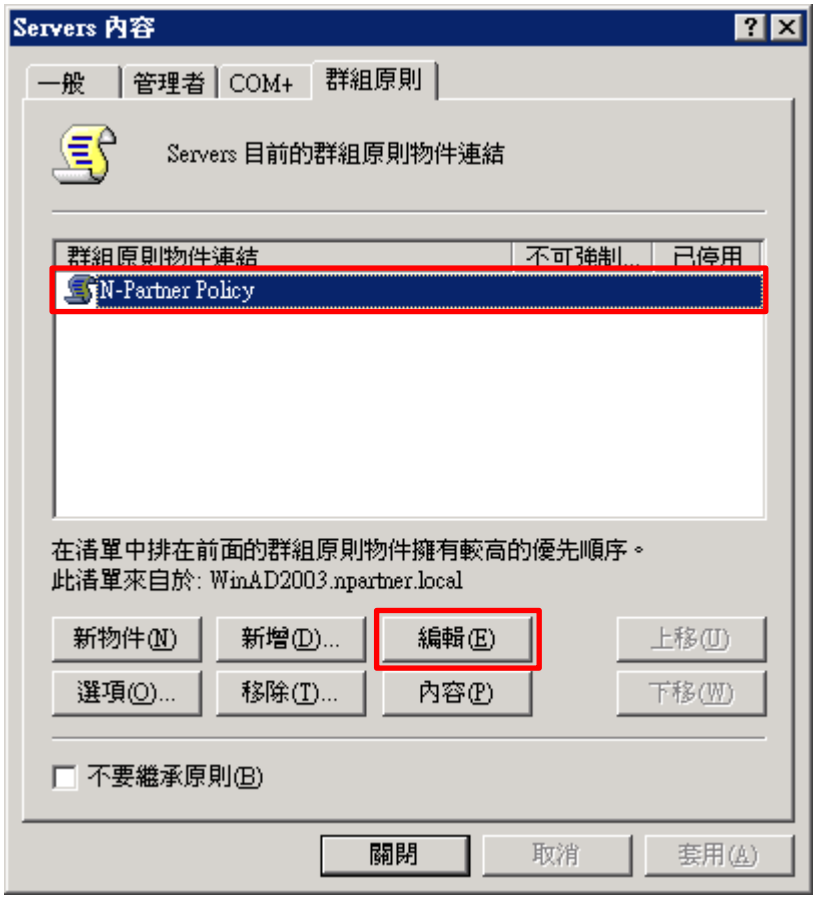
(3) 輸入群組原則物件名稱

點選 [群組原則] 頁面 -> 按 [新物件]



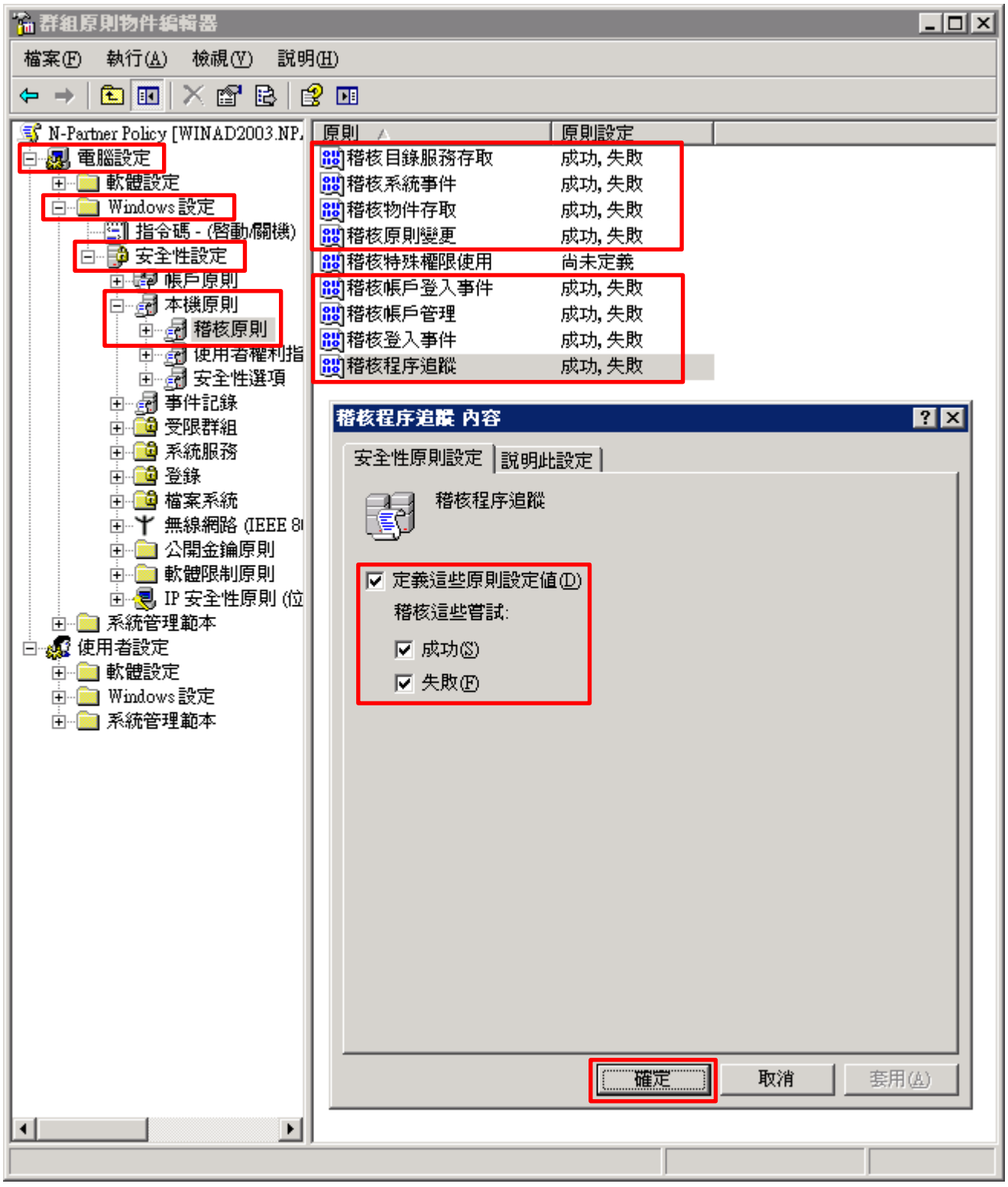
(4) 編輯群組原則物件

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]



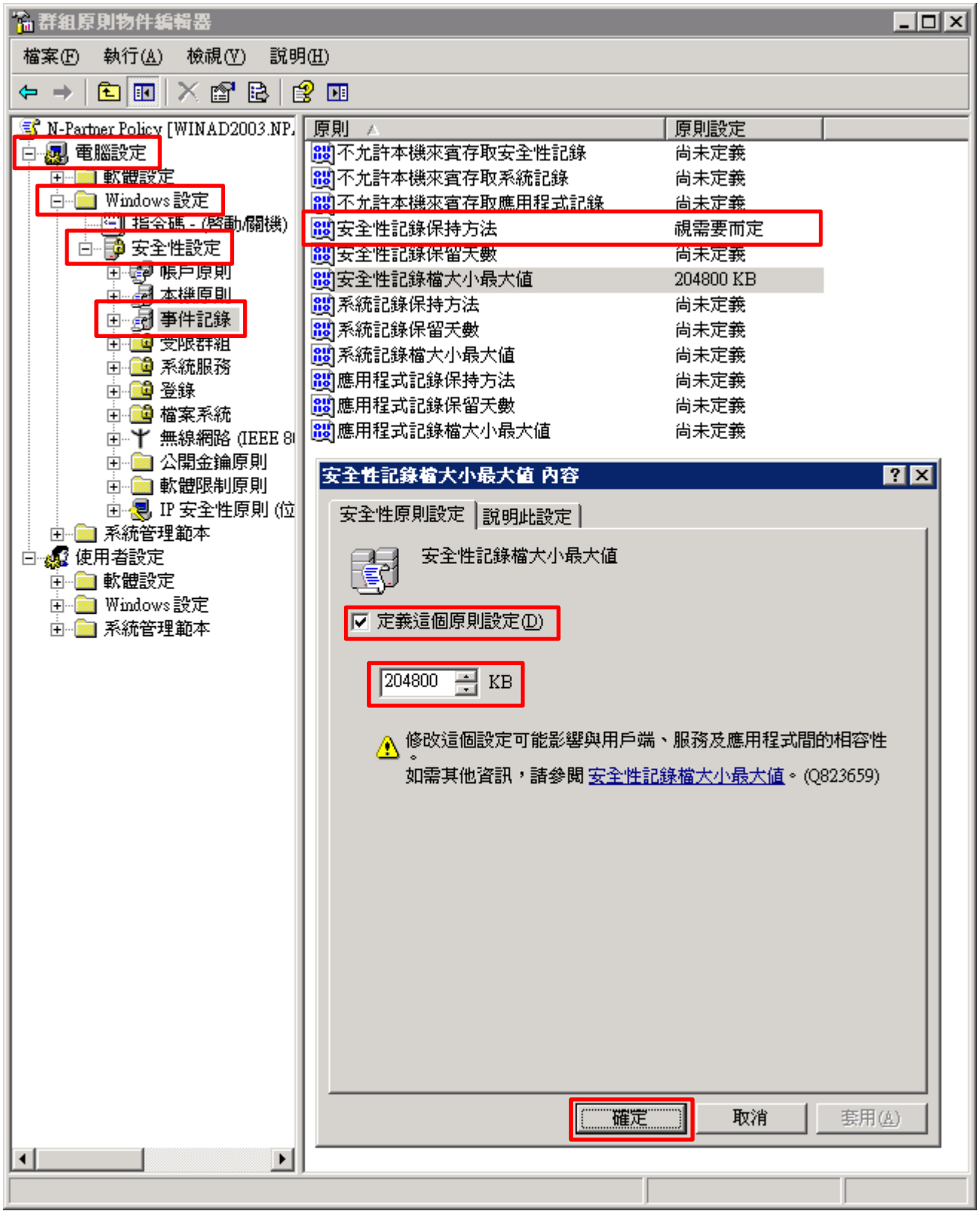
(5) 本機原則：稽核原則

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]



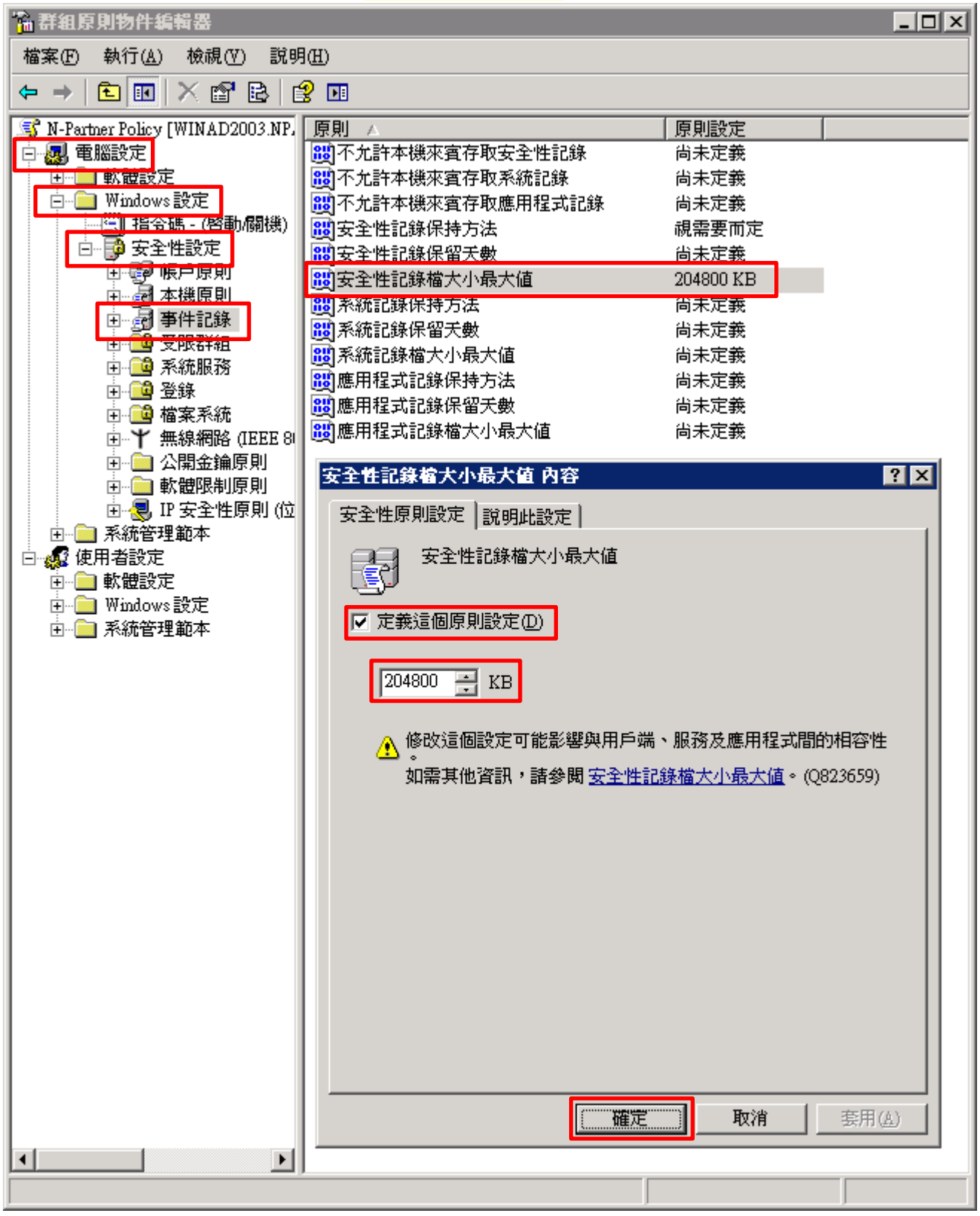
(6) 事件記錄：安全性記錄保持方法

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

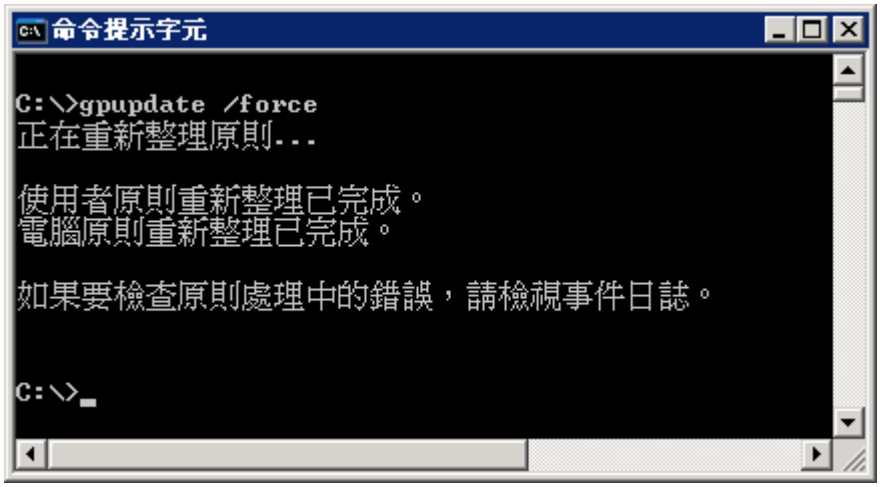
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 點選 [安全性記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]



(8) 開啟 [命令提示字元]

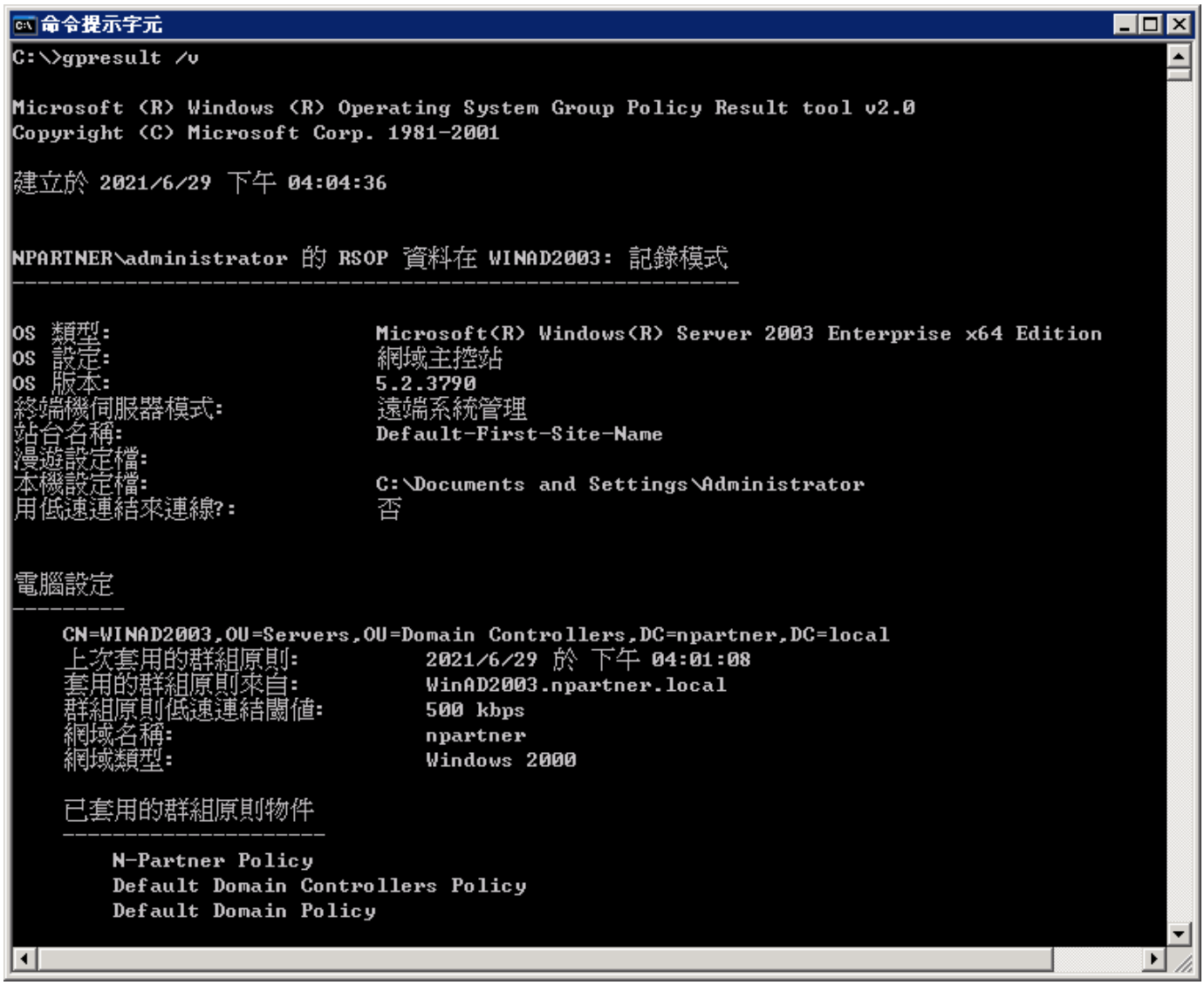
(9) 更新群組原則，

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



(10) 查看群組原則套用情形

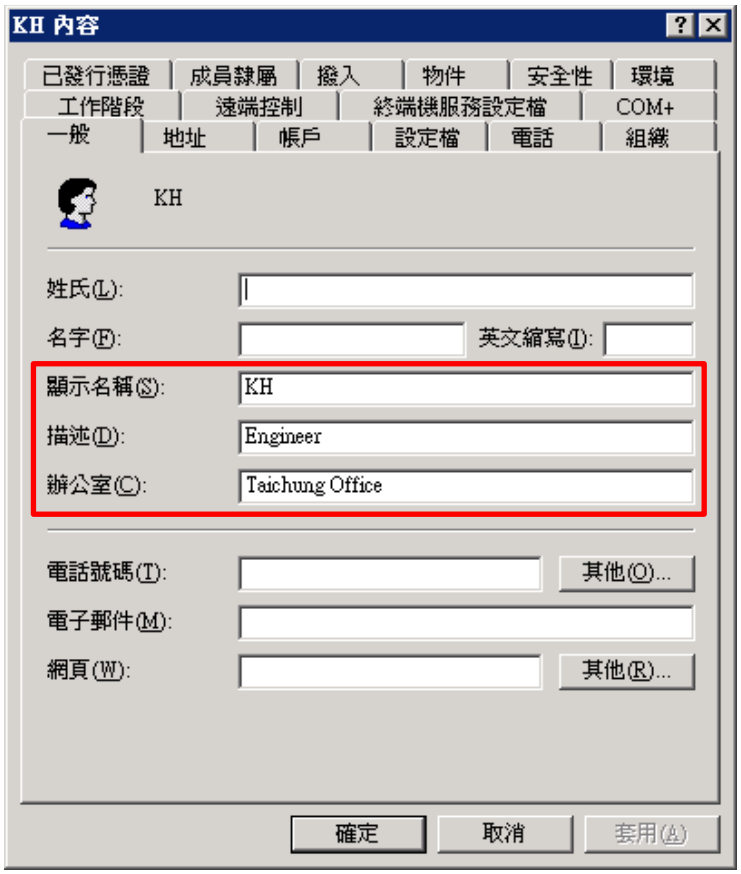
```
C:\> gpresult /v
```

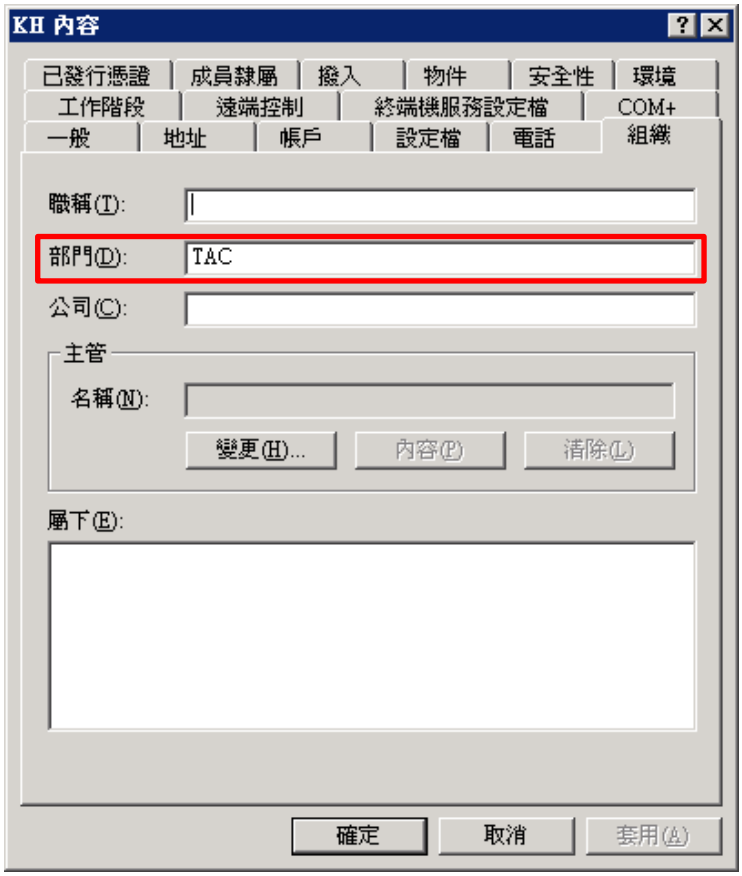


3.3 設定 WMI

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





(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

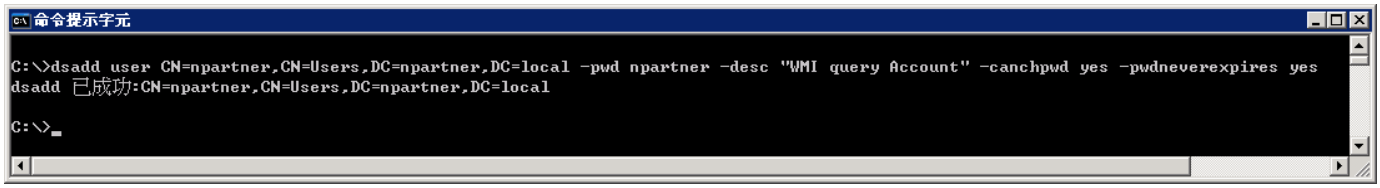
等級	事件	來源 IP	來源 Port	次數	事件型態	來源使用者名稱	Policy ID	Audit User	Ext1	Ext4
Notice	528 Successful Logon (AUDIT_SUCCESS 528 NPARTNER\kh) (Logon Success)	192.168.5.37	56914	1	audit	kh (KH, TAC, 0032, (Engineer))	528	kh	登入類型:10	登入識別碼:(0x0,0xB930B)

3.3.1 新增非管理帳號

(1) 開啟 [命令提示字元]

(2) 新增帳號

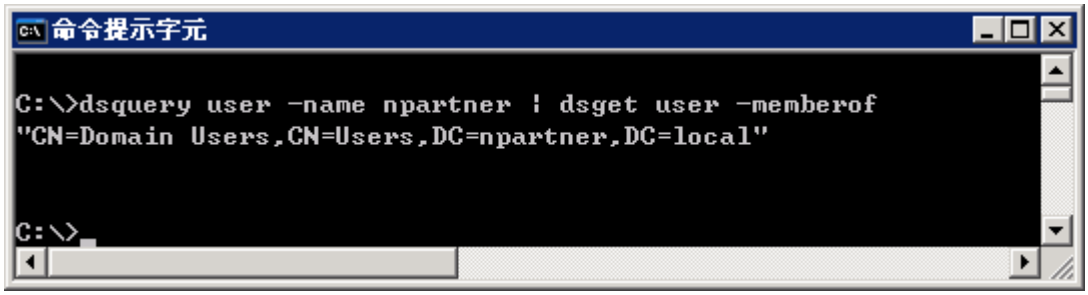
```
C:\> dsadd user CN=npartner,CN=Users,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```



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

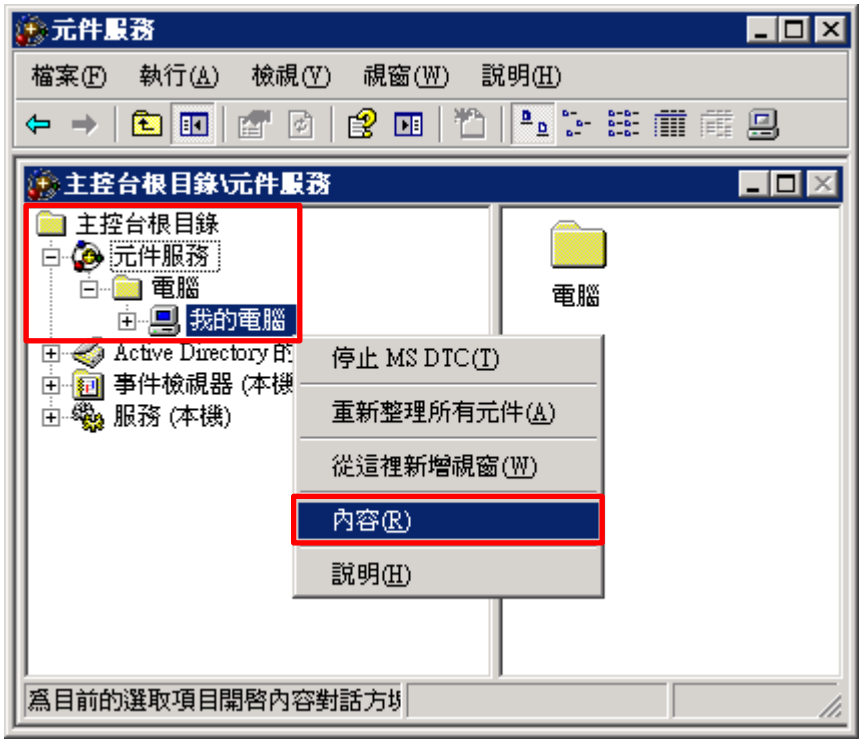
(1) 開啟 [命令提示字元]

(2) 開啟元件服務

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

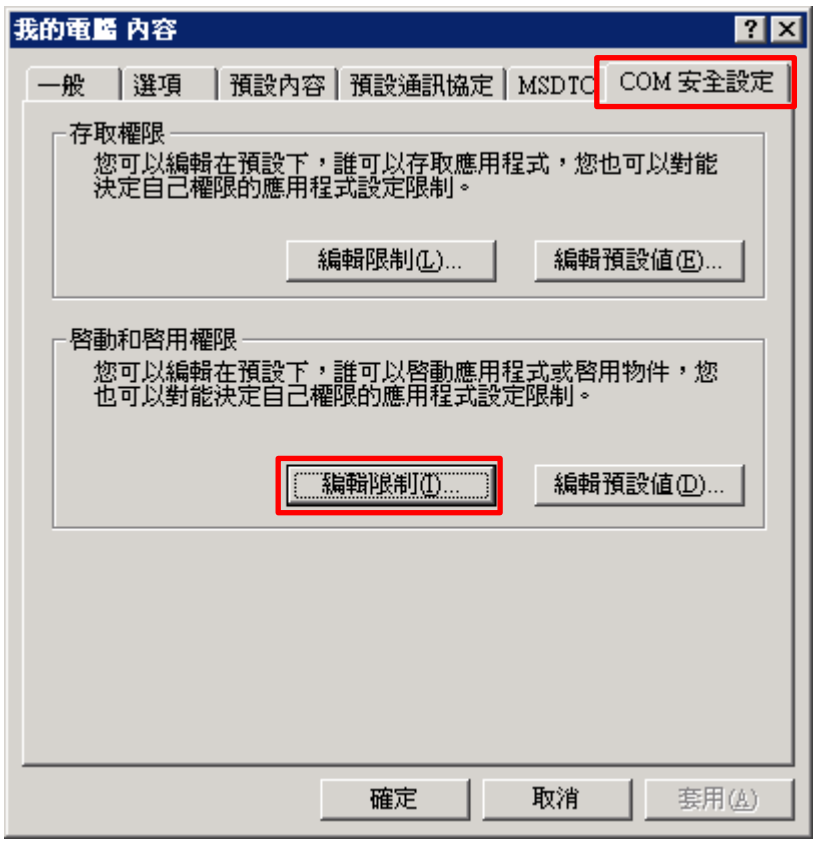
(3) 編輯電腦內容

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]

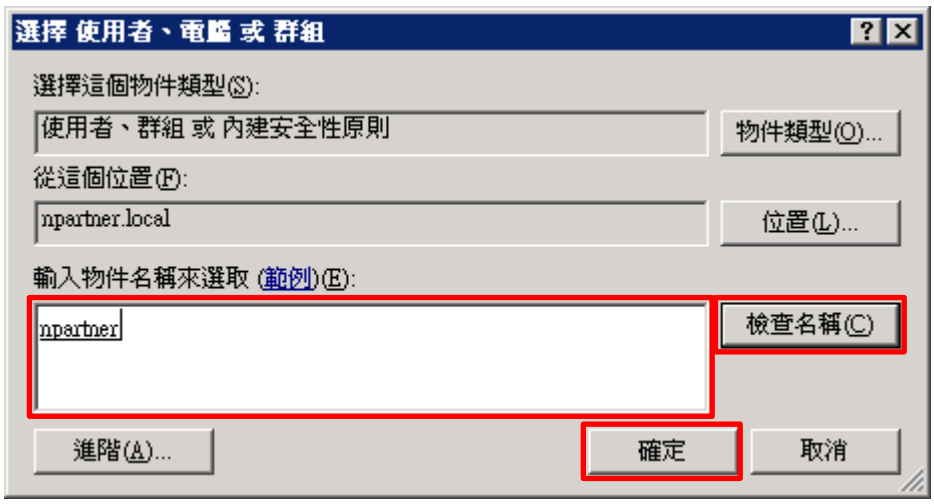


(5) 新增 DCOM 使用者權限

點選 [新增]

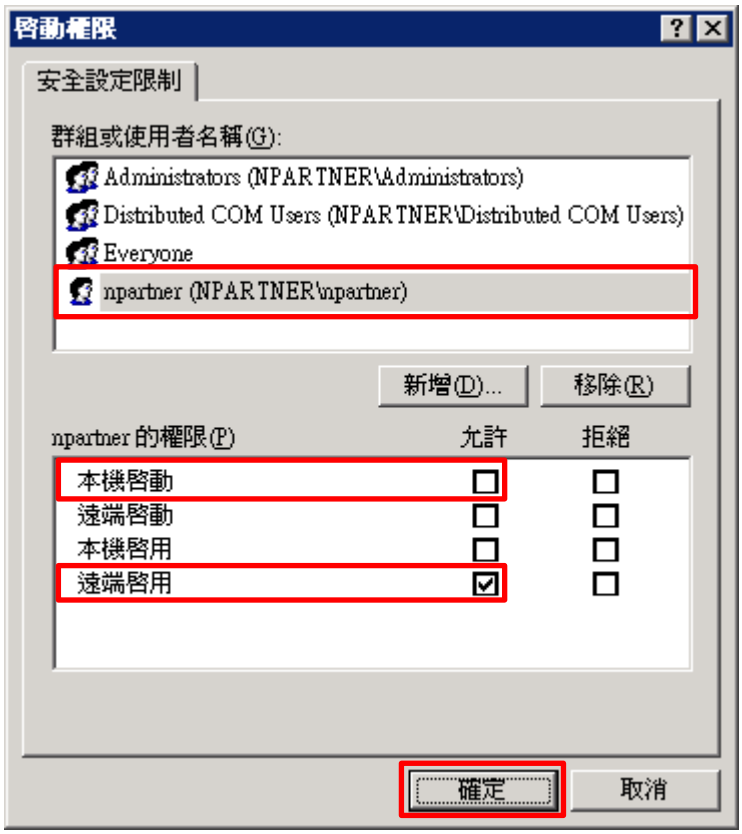
(6) 輸入使用者

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

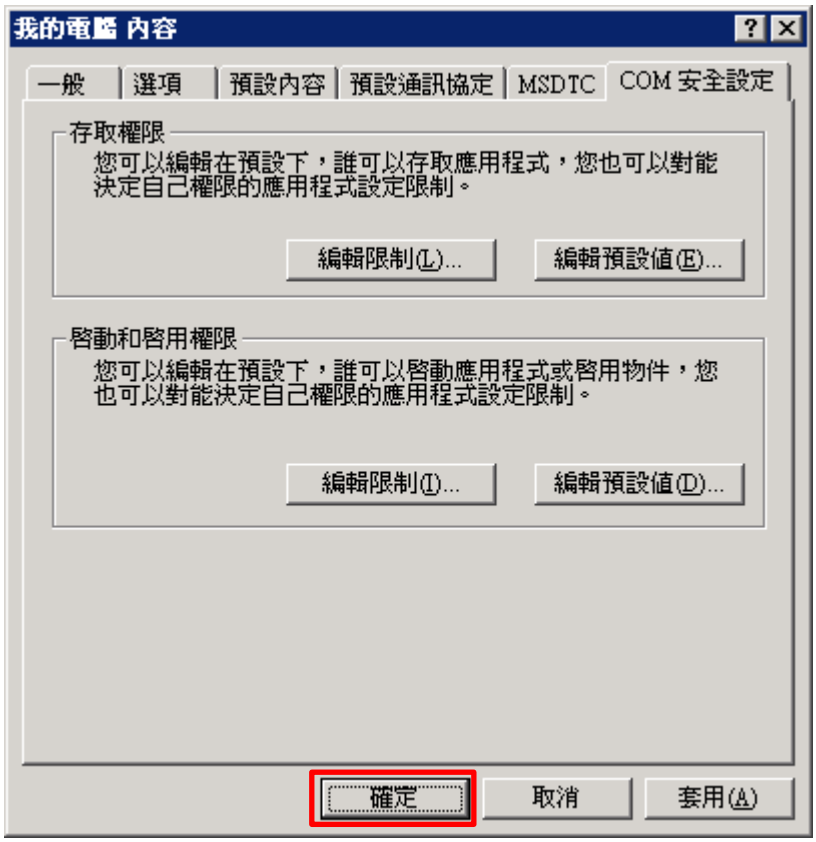


(7) 設定使用者權限

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

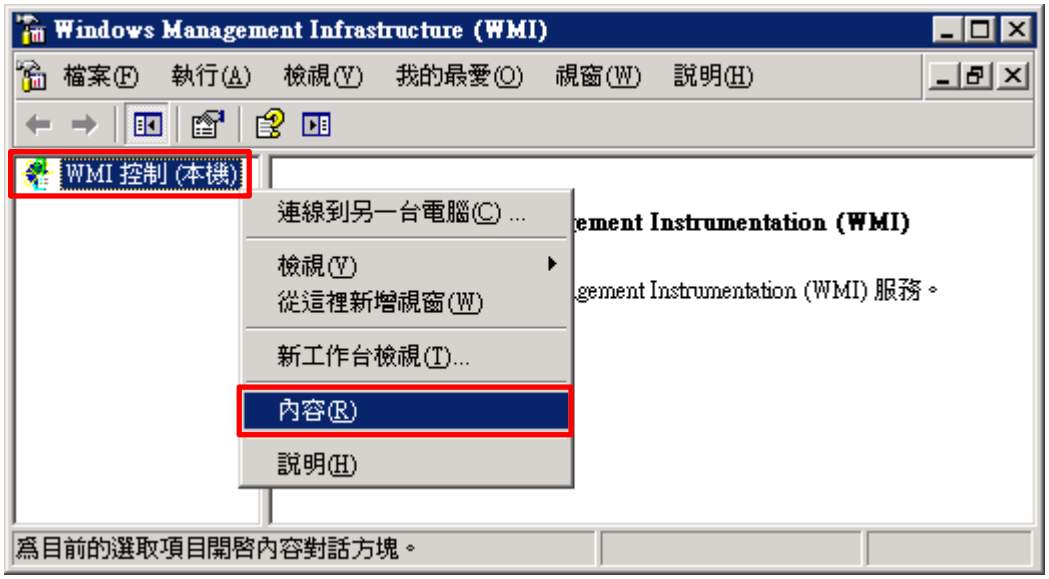
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]

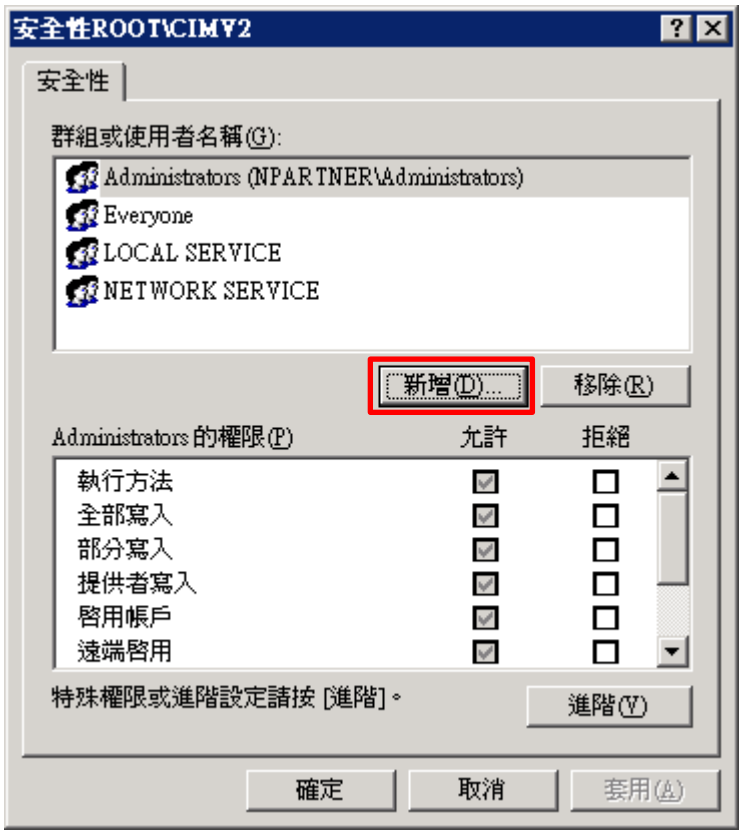


(4) 編輯 CIMV2 安全性

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

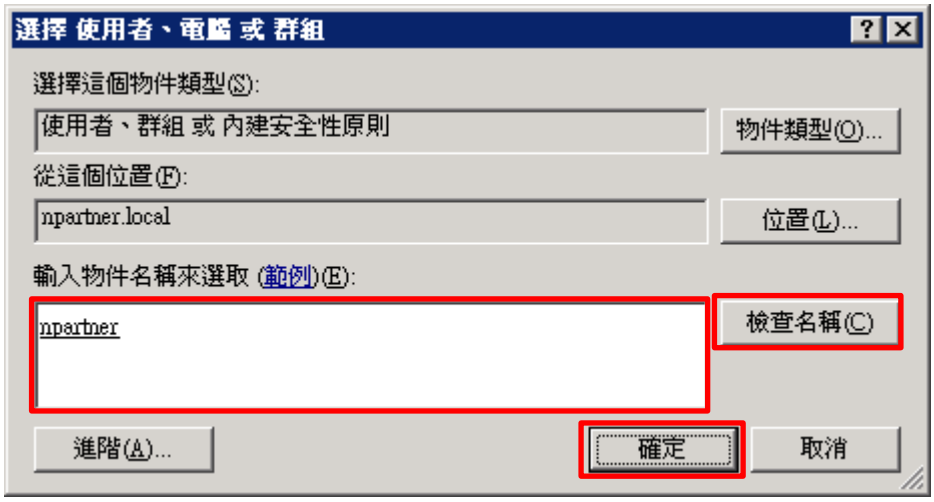
(5) 新增 WMI 使用者權限

按 [新增]



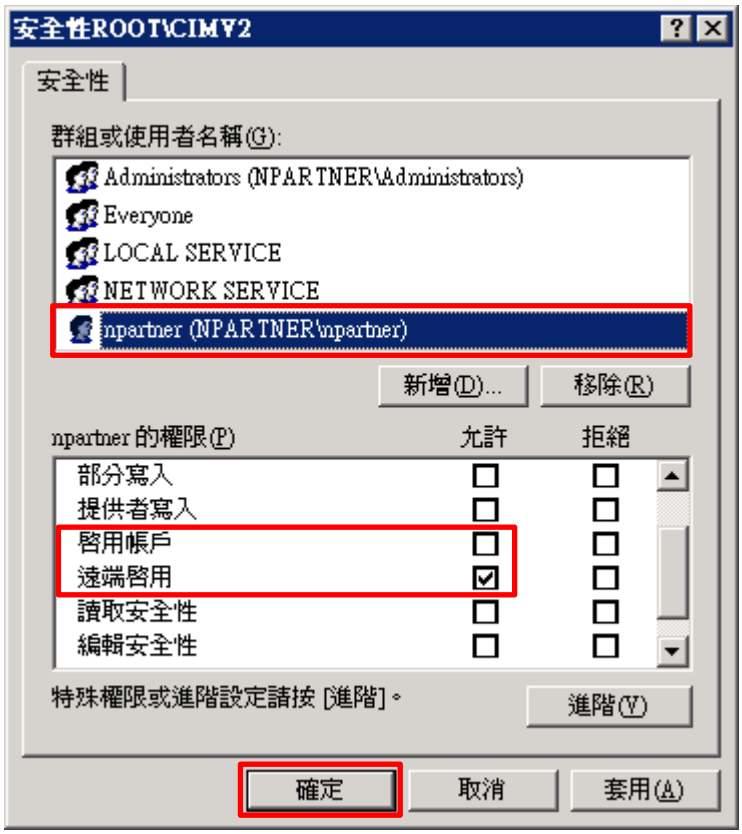
(6) 輸入使用者

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

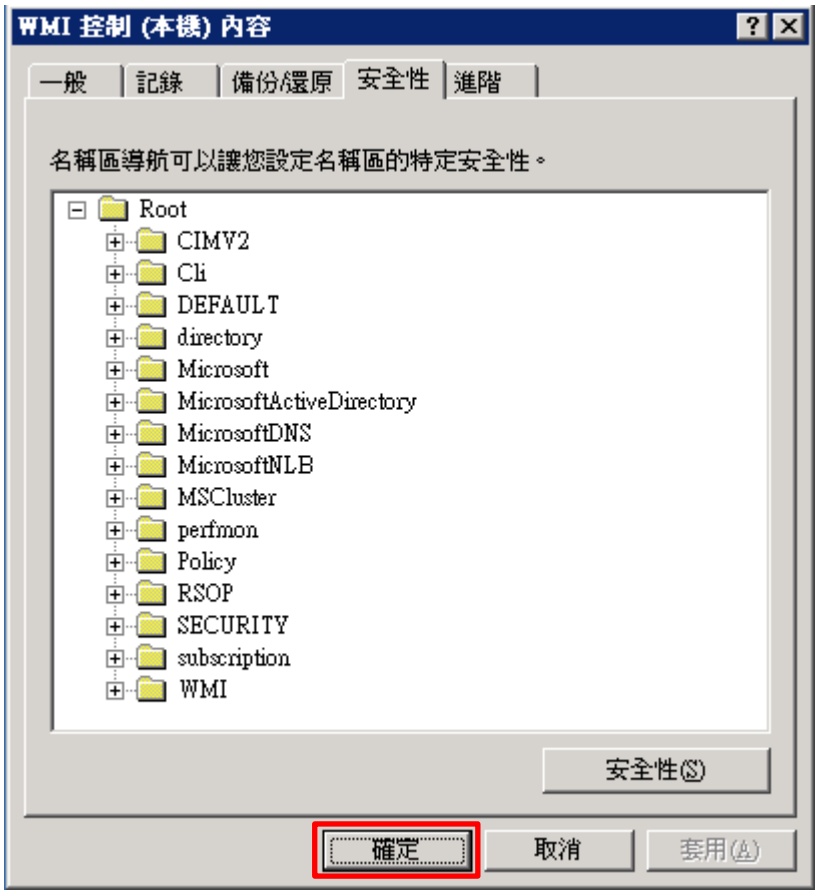


(7) 設定使用者權限

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

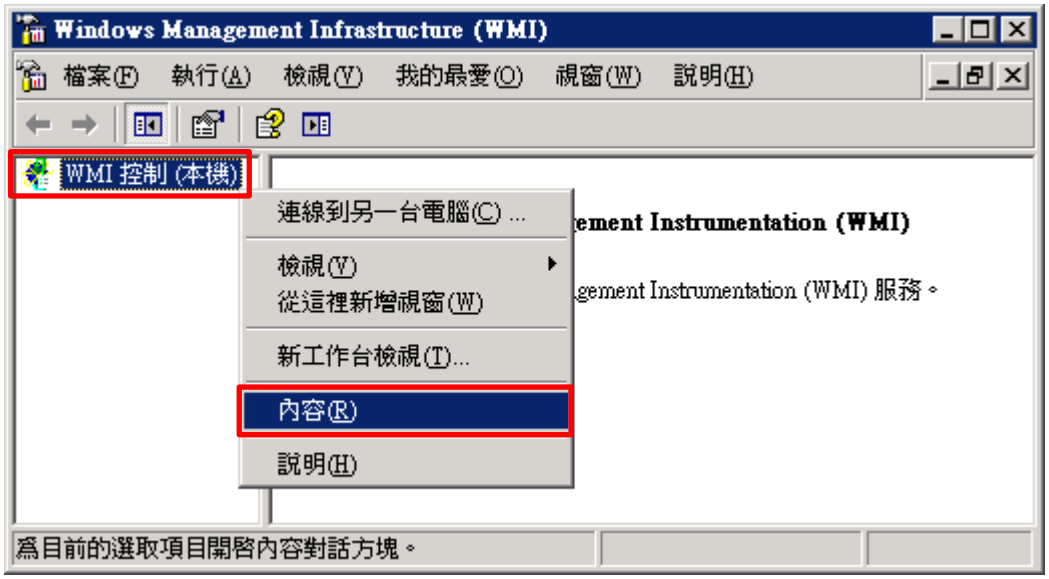
(1) 開啟 [命令提示字元]

(2) 開啟 WMI 控制

```
C:\> wmimgmt.msc
```

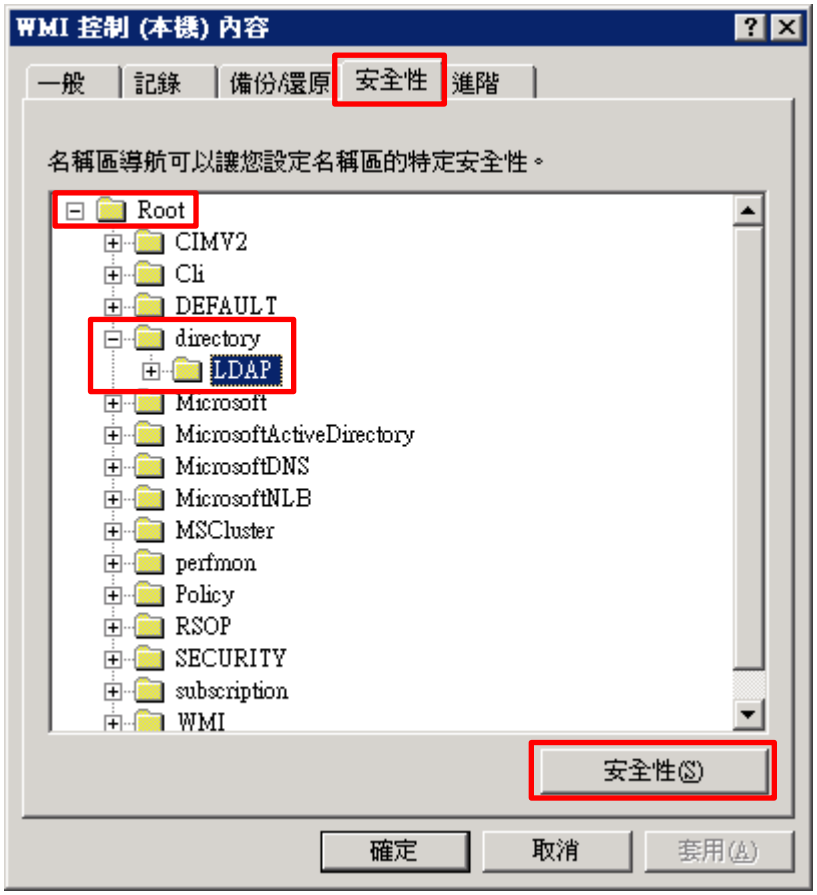
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



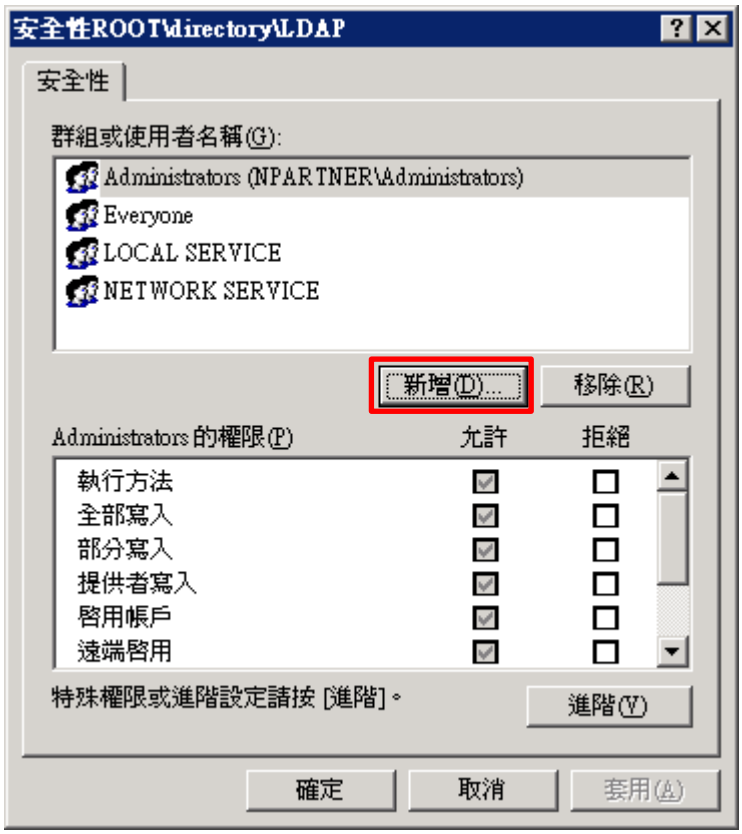
(4) 編輯 LDAP 安全性

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



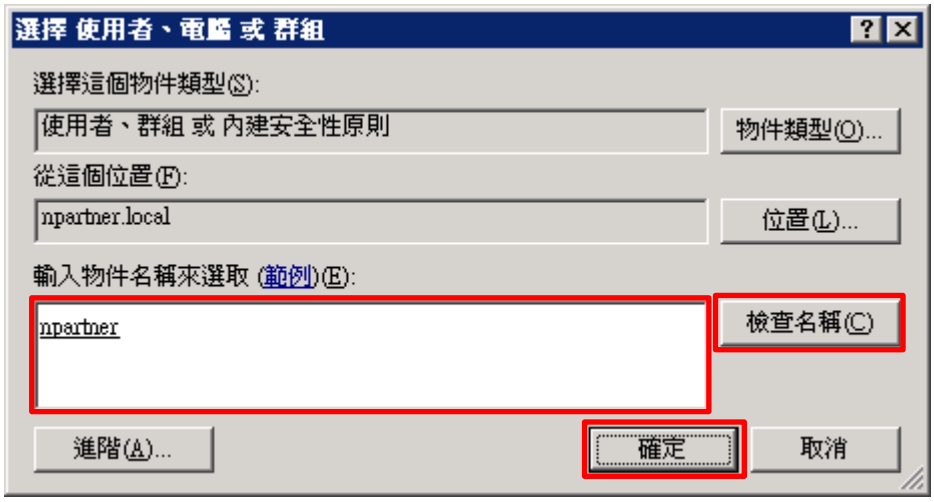
(5) 新增 WMI 使用者權限

按 [新增]



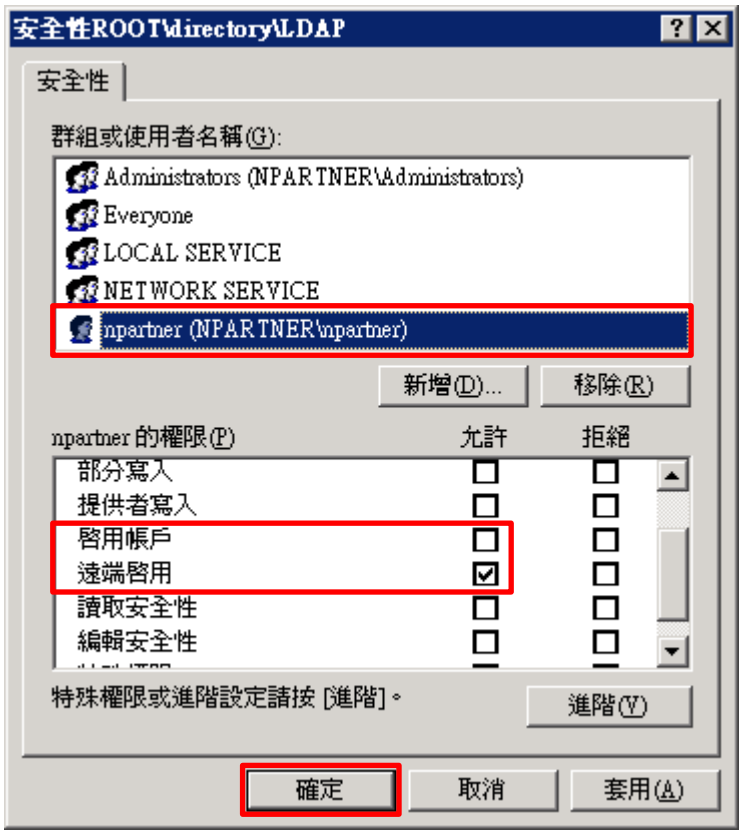
(6) 輸入使用者

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

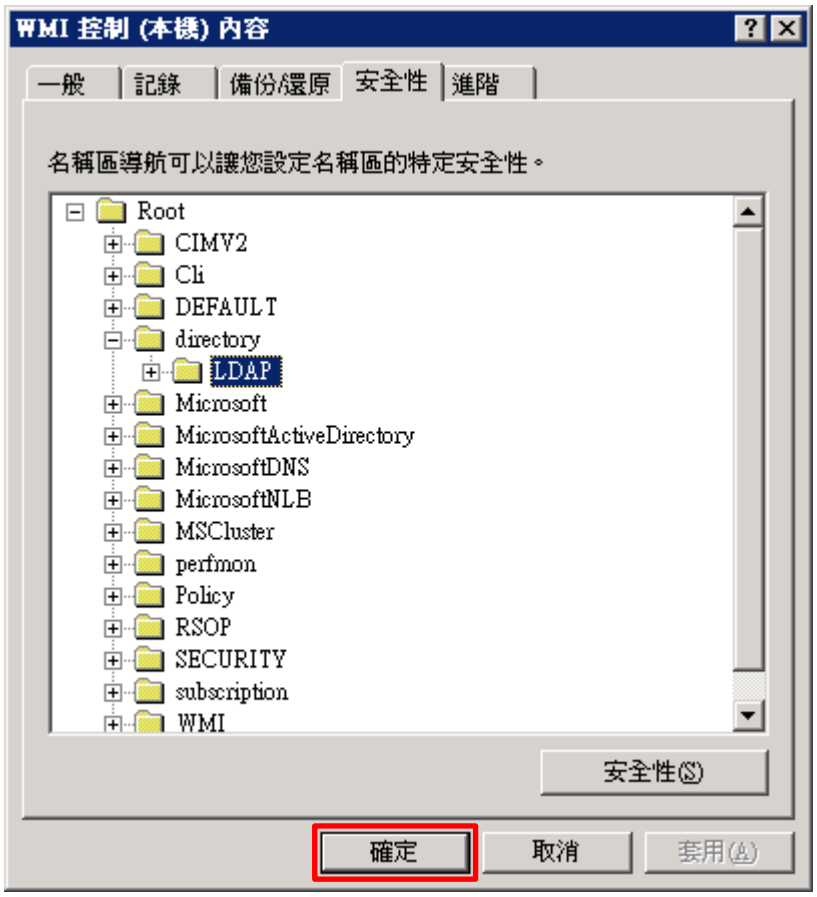


(7) 設定使用者權限

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]



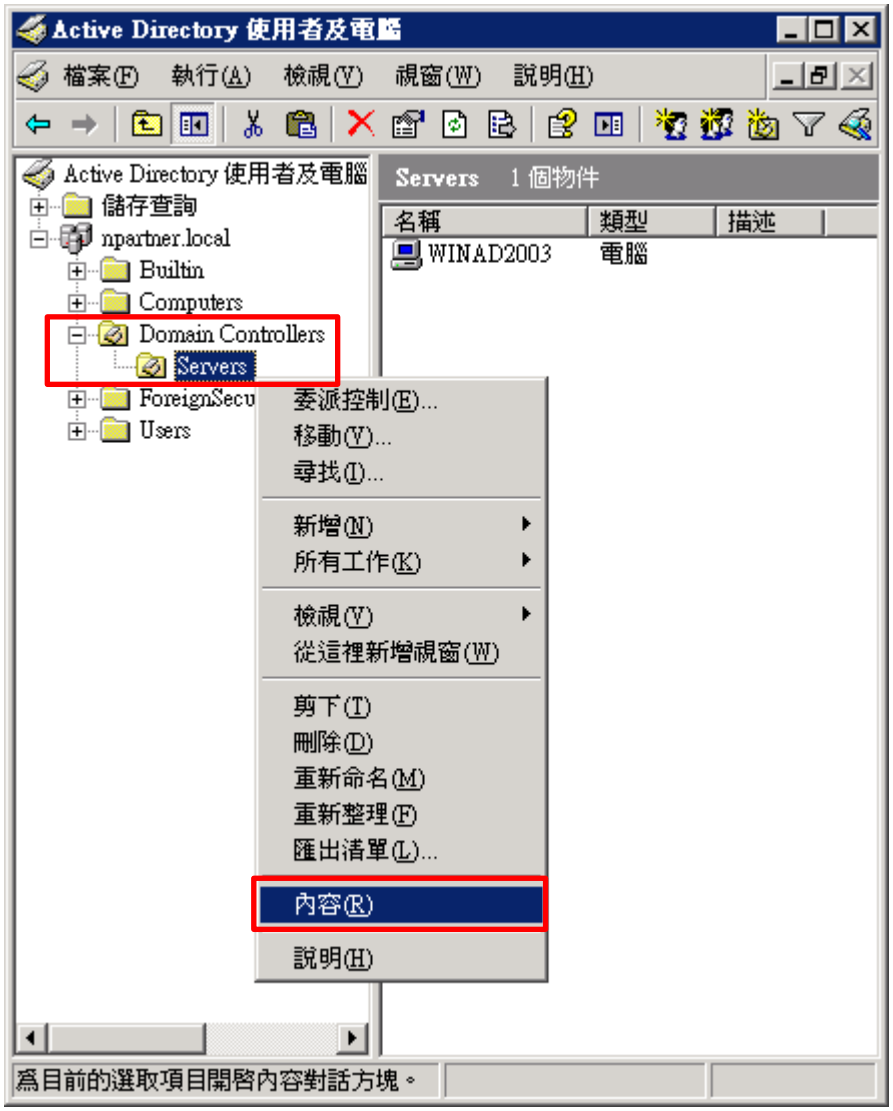
3.3.4 設定 Event log 讀取權限

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

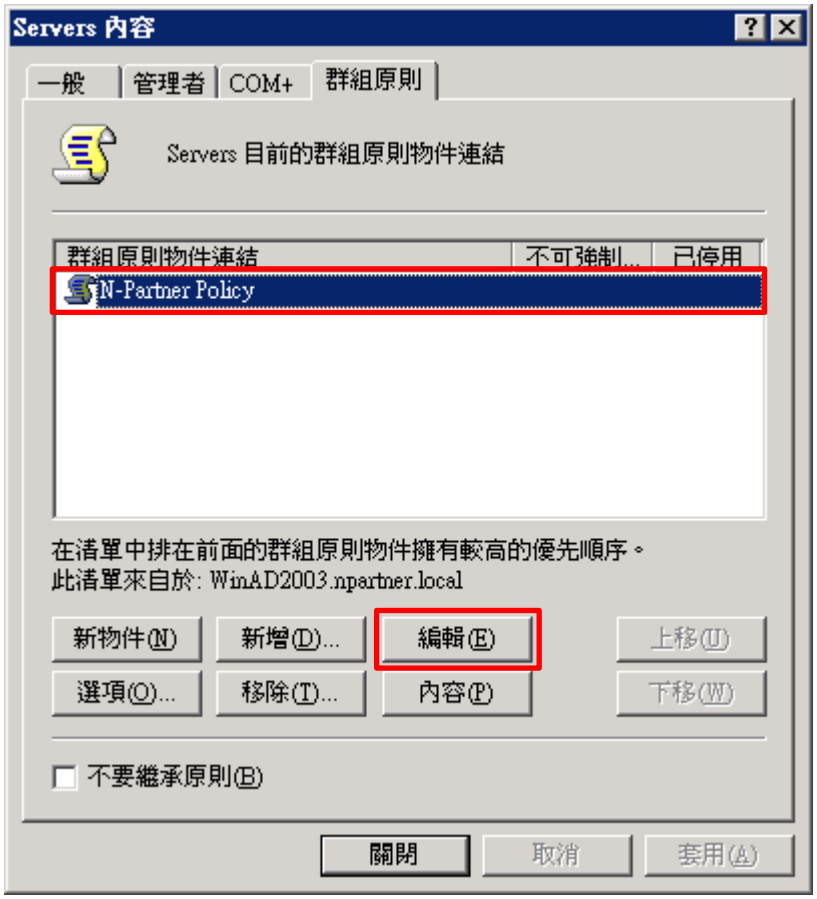
(2) Domain Controllers 的 Servers 組織單位，點選內容

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



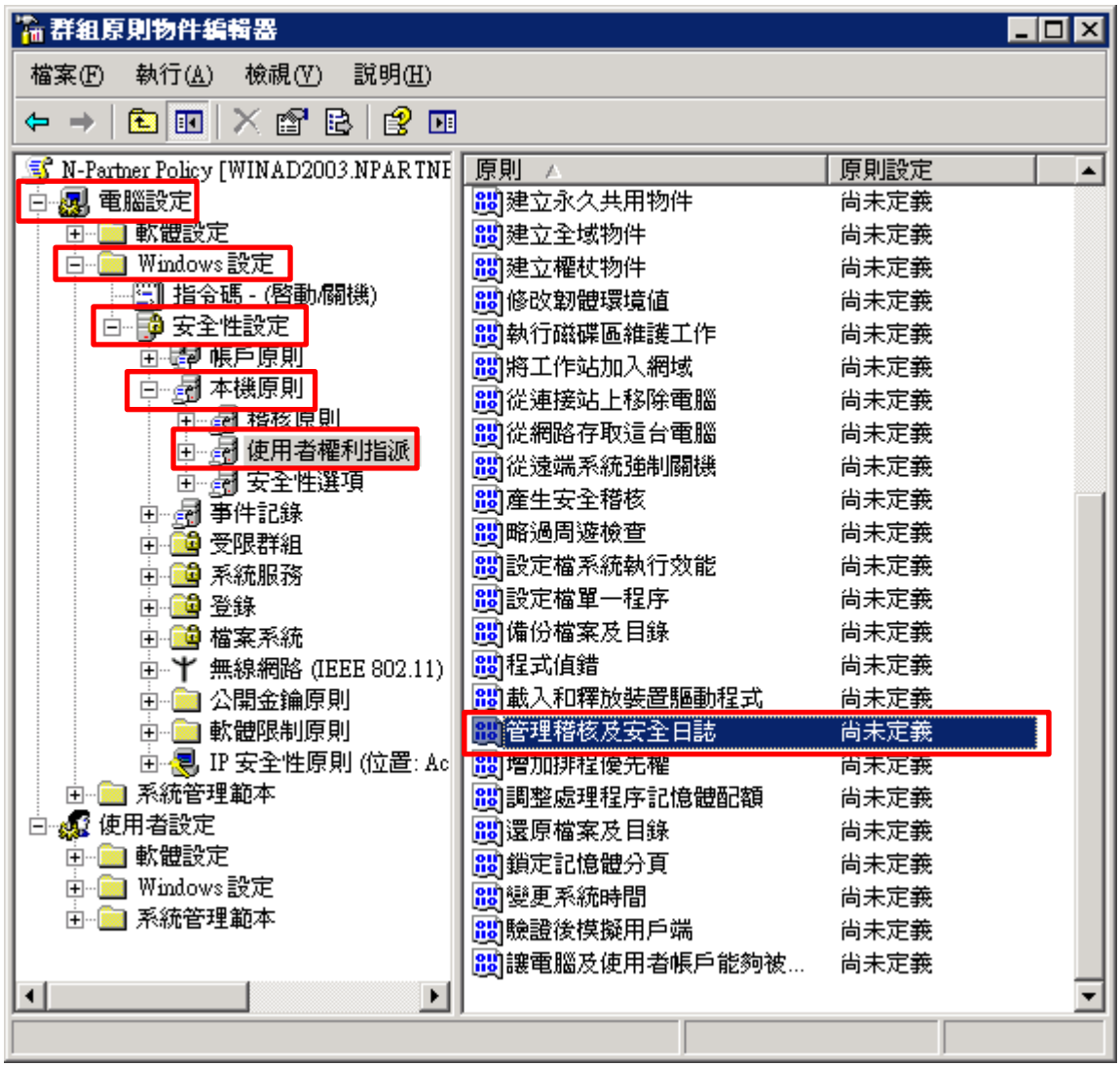
(3) 編輯群組原則物件

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



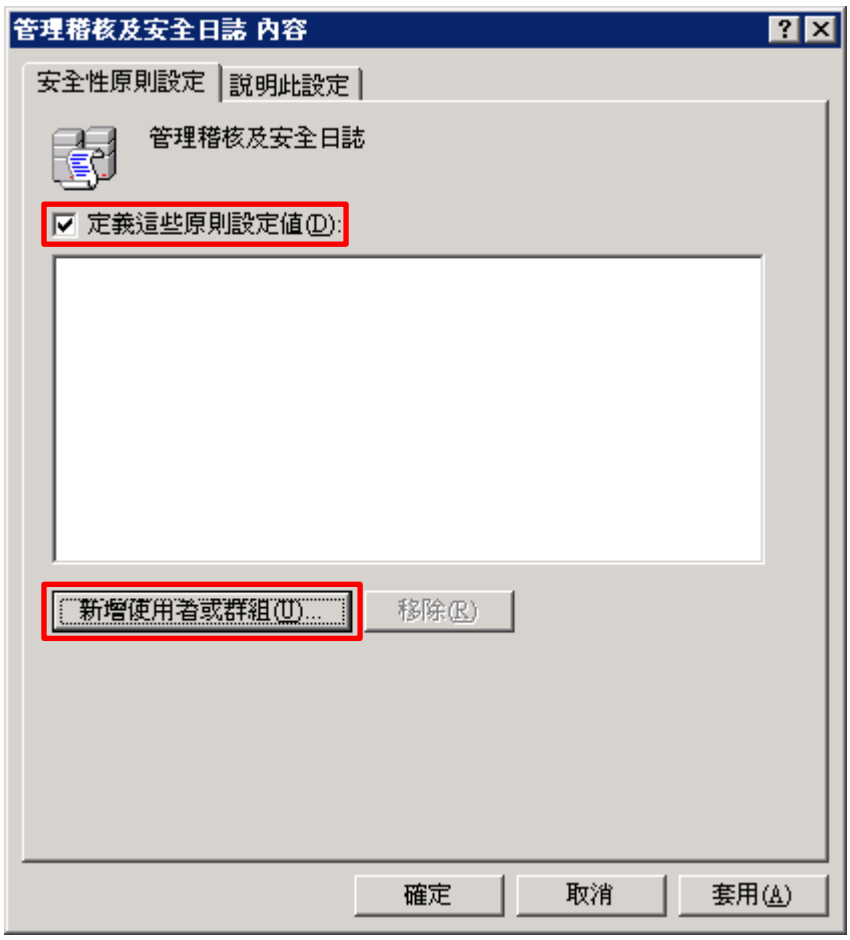
(4) 設定記錄檔

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



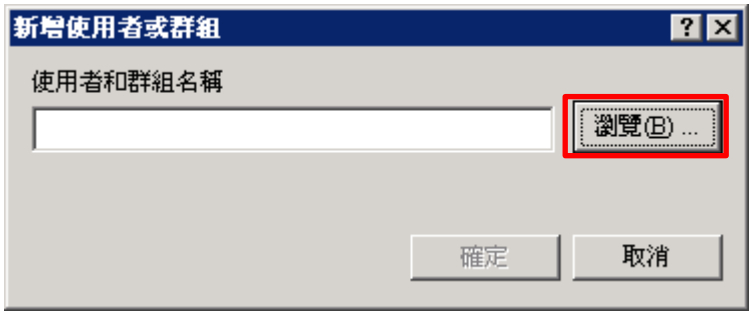
(5) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



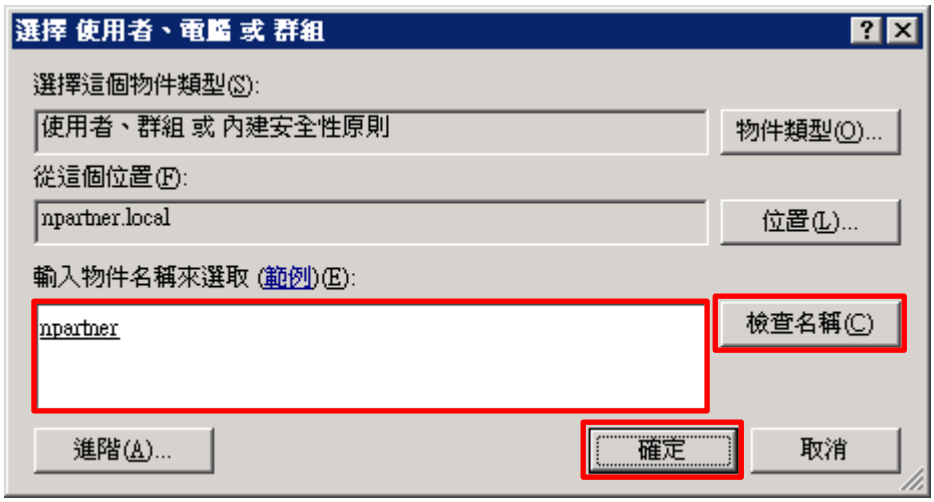
(6) 搜尋使用者

按 [瀏覽]



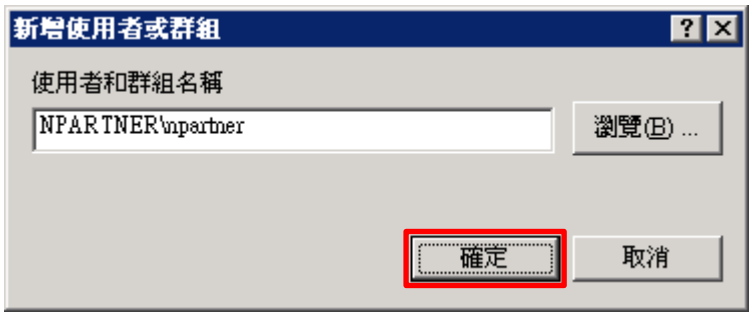
(7) 輸入使用者

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



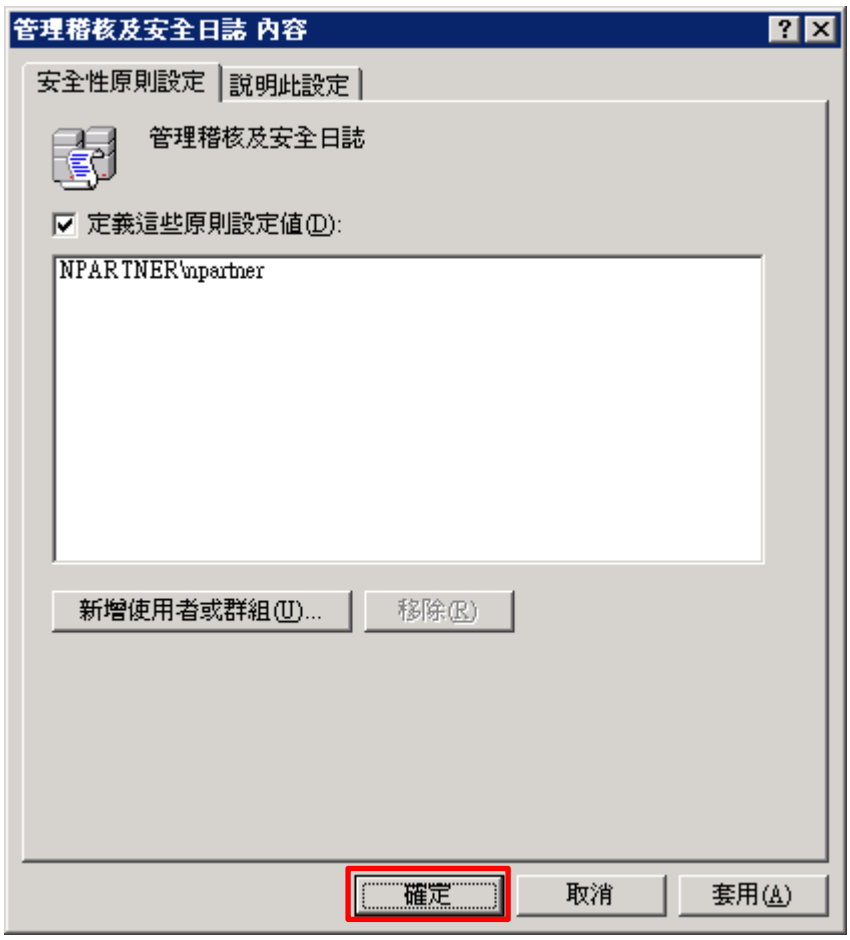
(8) 確定使用者

按 [確定]



(9) 確定設定記錄檔

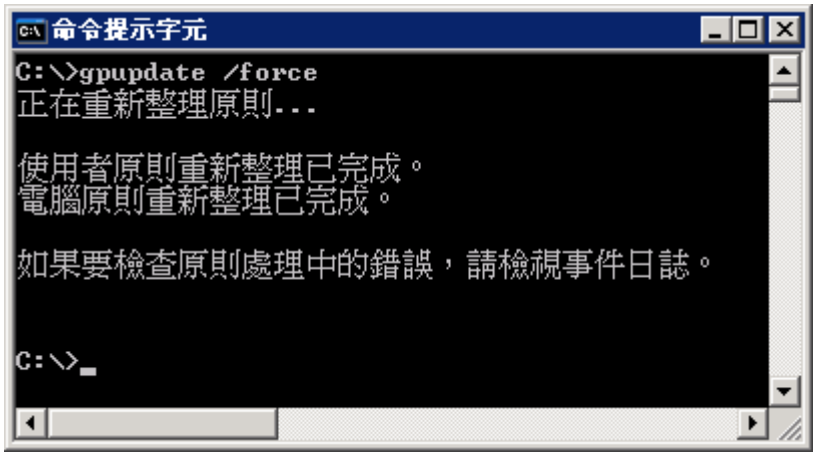
按 [確定]



(10) 開啟 [命令提示字元]

(11) 更新群組原則

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



3.3.5 重啟 WMI 服務

(1) 開啟 [命令提示字元]

(2) 停用 WMI 服務

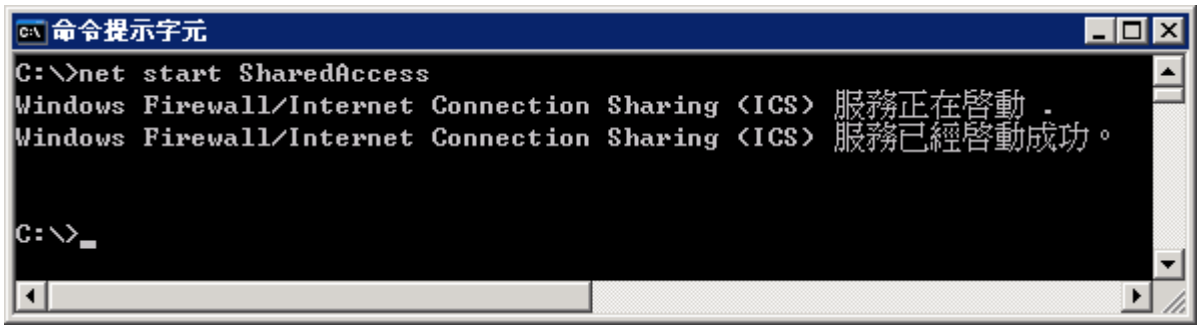
```
C:\> net stop winmgmt
```

(3) 啟用 WMI 服務

```
C:\> net start winmgmt
```

(4) 啟用 Firewall 服務

```
C:\> net start SharedAccess
```

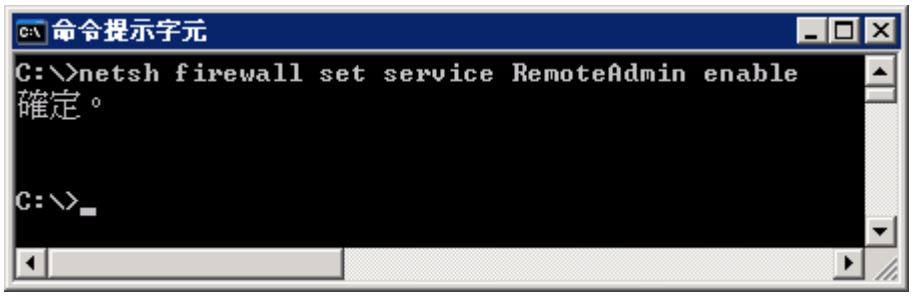


3.3.6 設定防火牆

(1) 開啟 [命令提示字元]

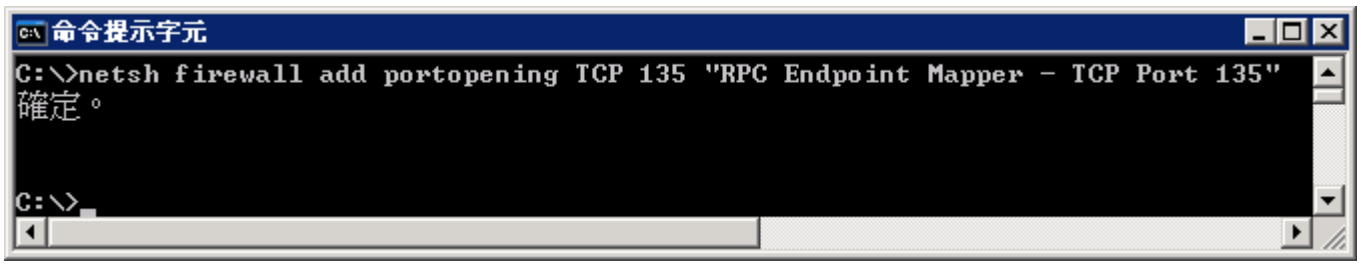
(2) 允許 WMI 通過防火牆

```
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
```

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

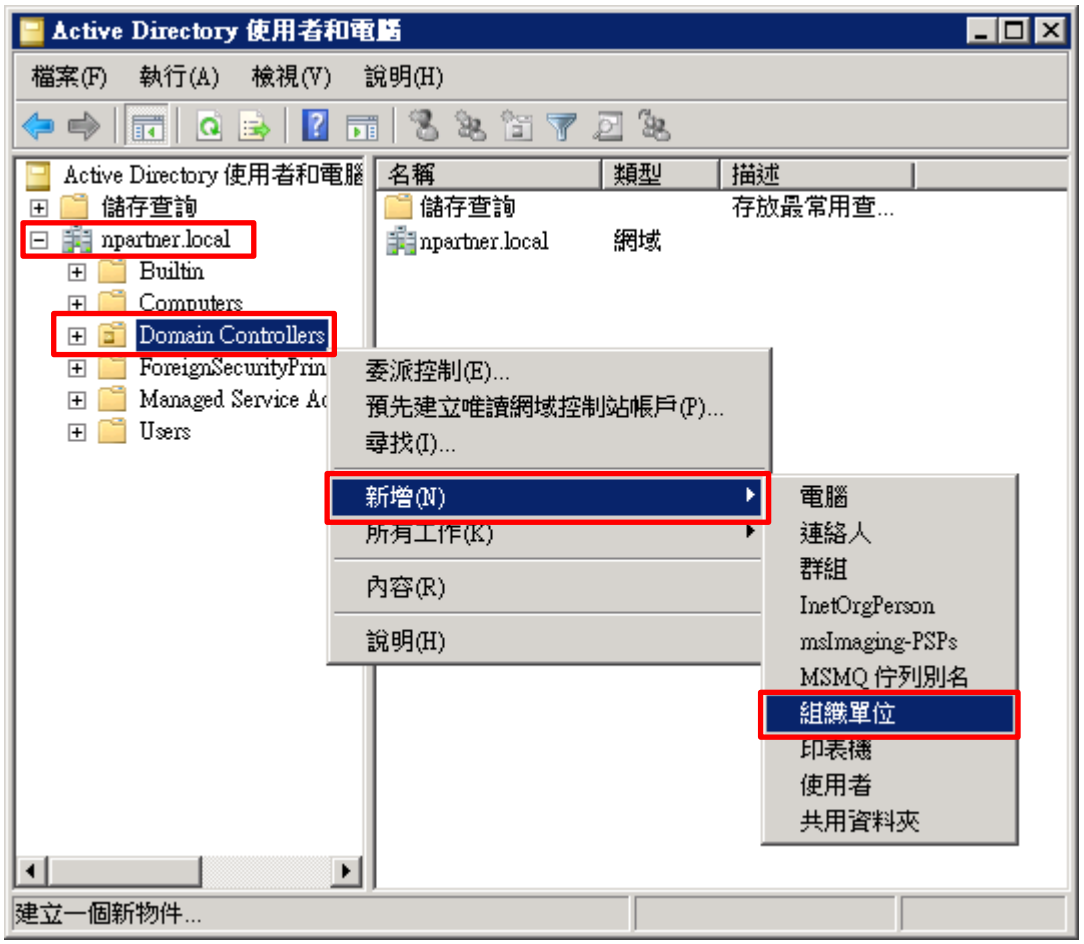
4.1 組織單位設定

(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]

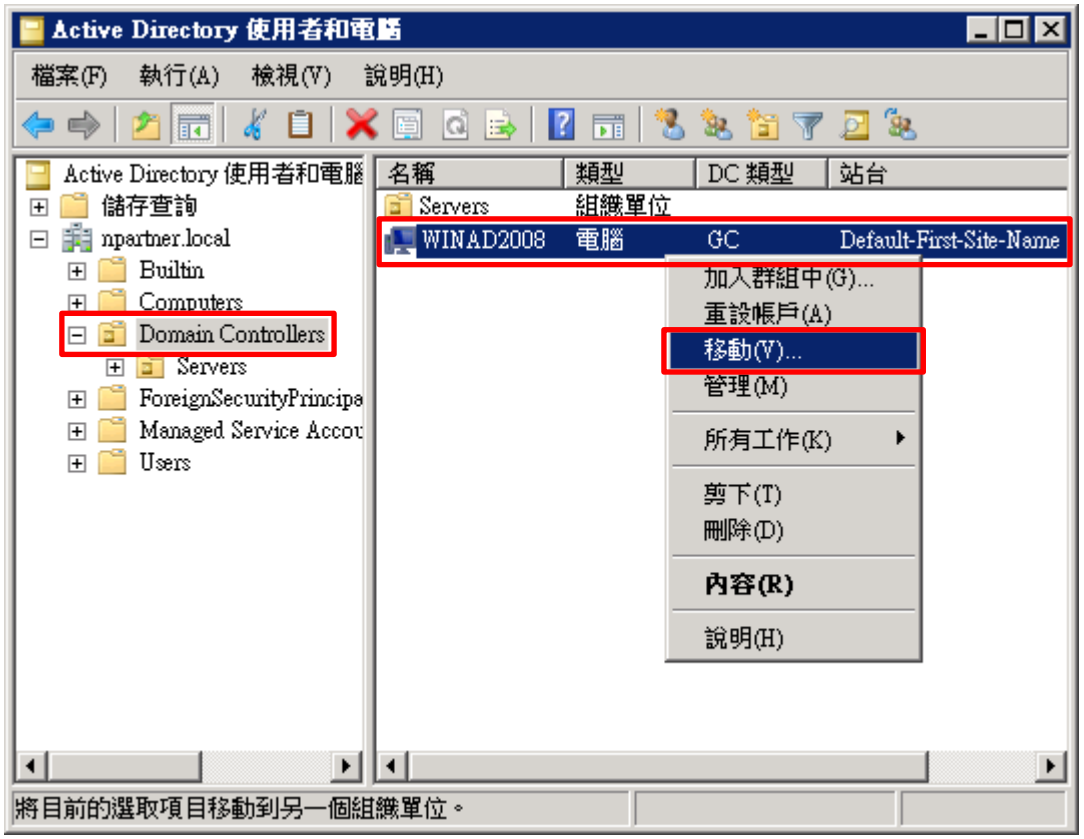


(3) 輸入組織單位名稱

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]

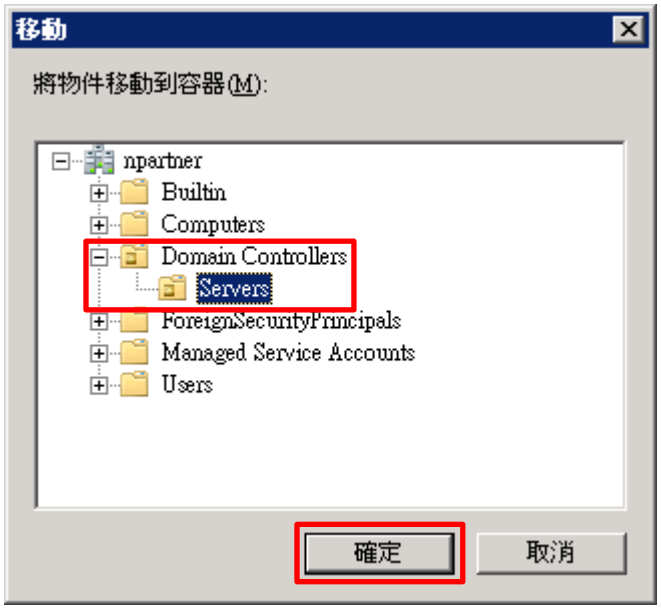
(4) 移動伺服器至新的組織單位

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]



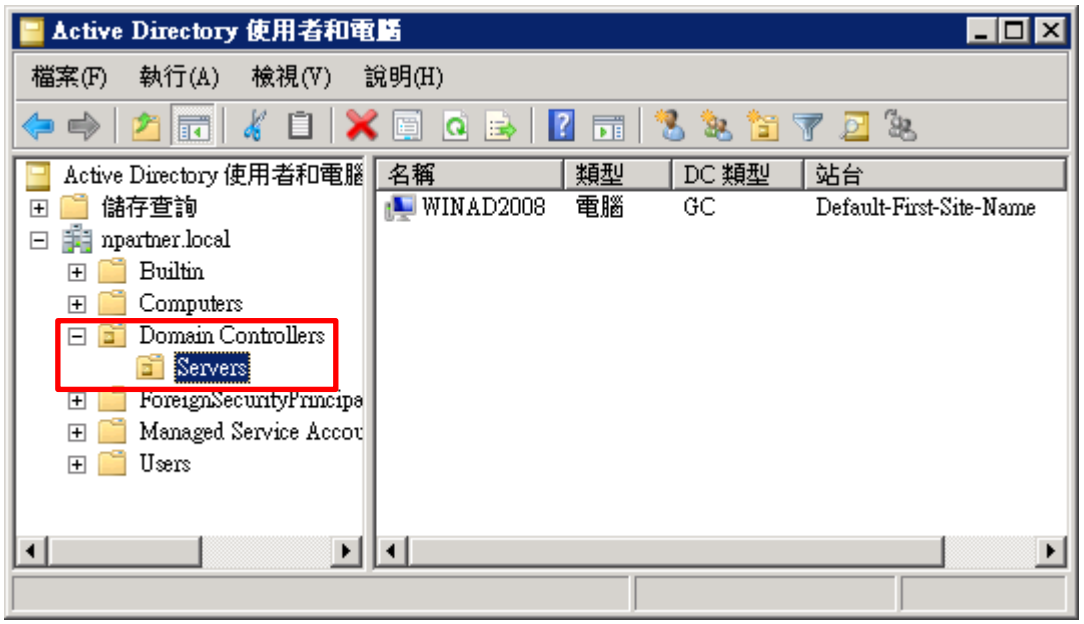
(5) 選擇組織單位

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。



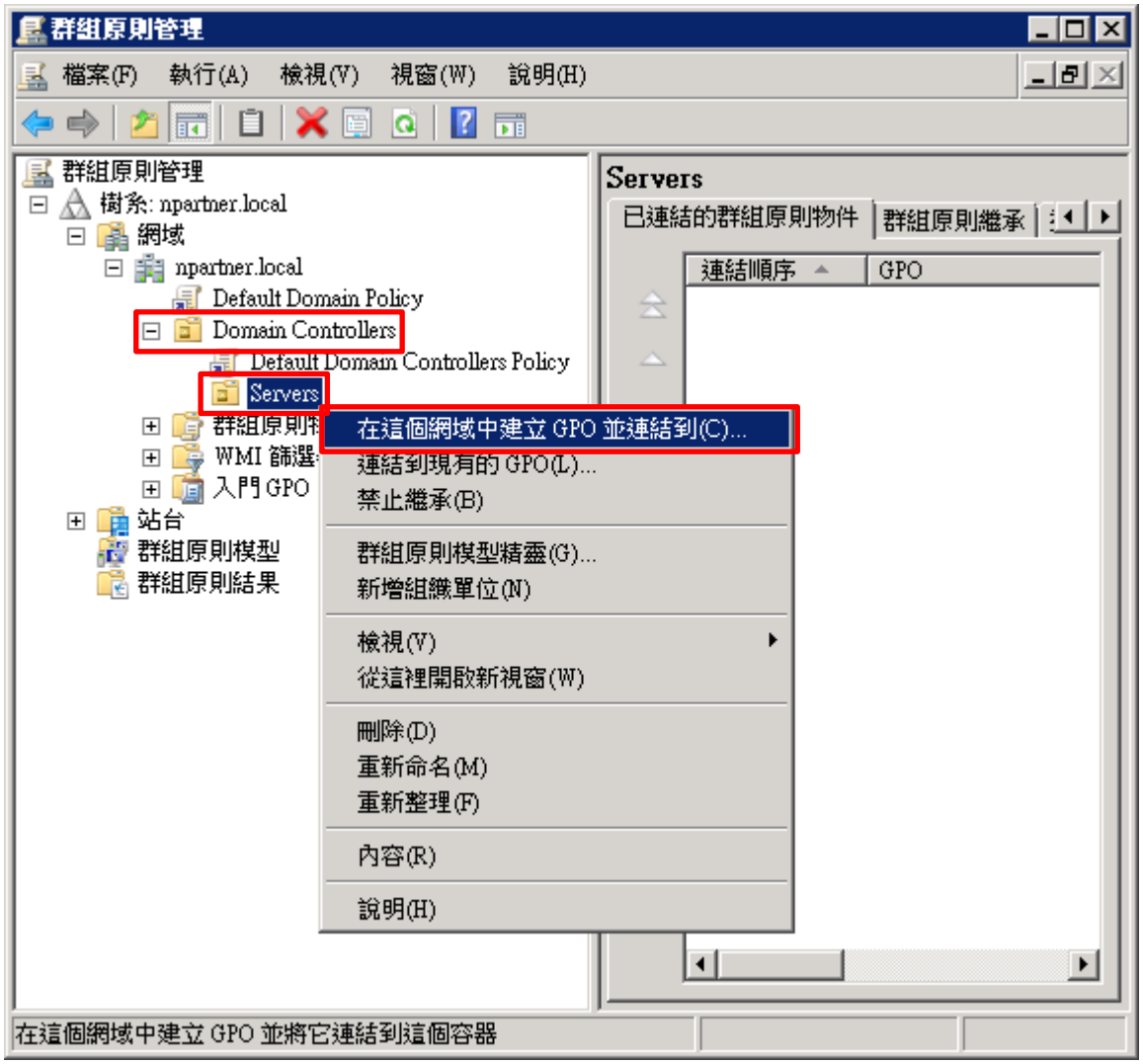
4.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

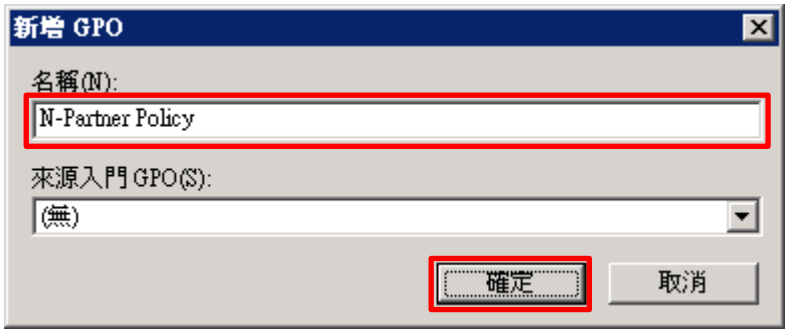
(2) 在 Servers 組織單位，新增群組原則物件

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...]



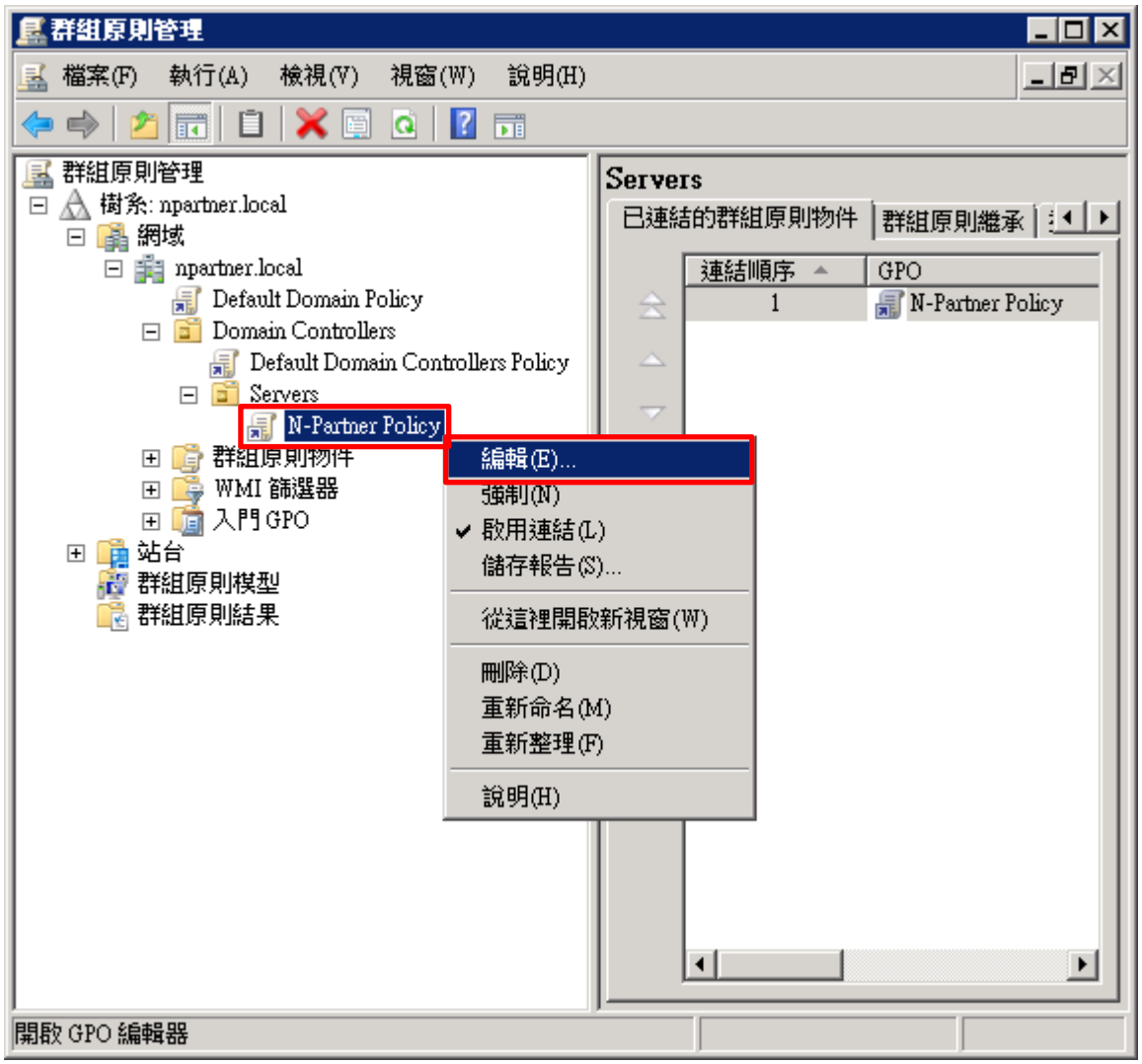
(3) 輸入群組原則物件名稱

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]



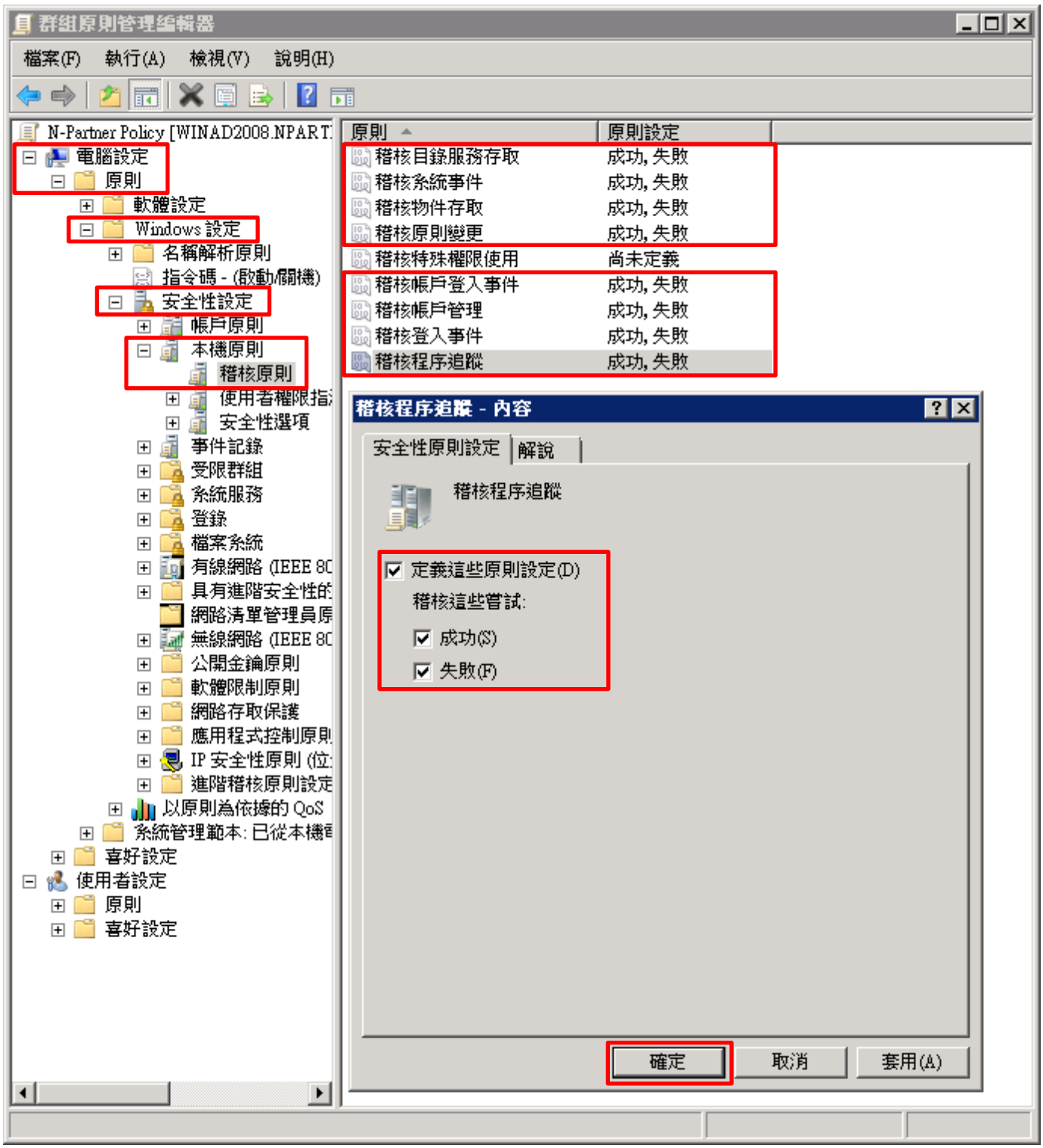
(4) 編輯群組原則物件

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



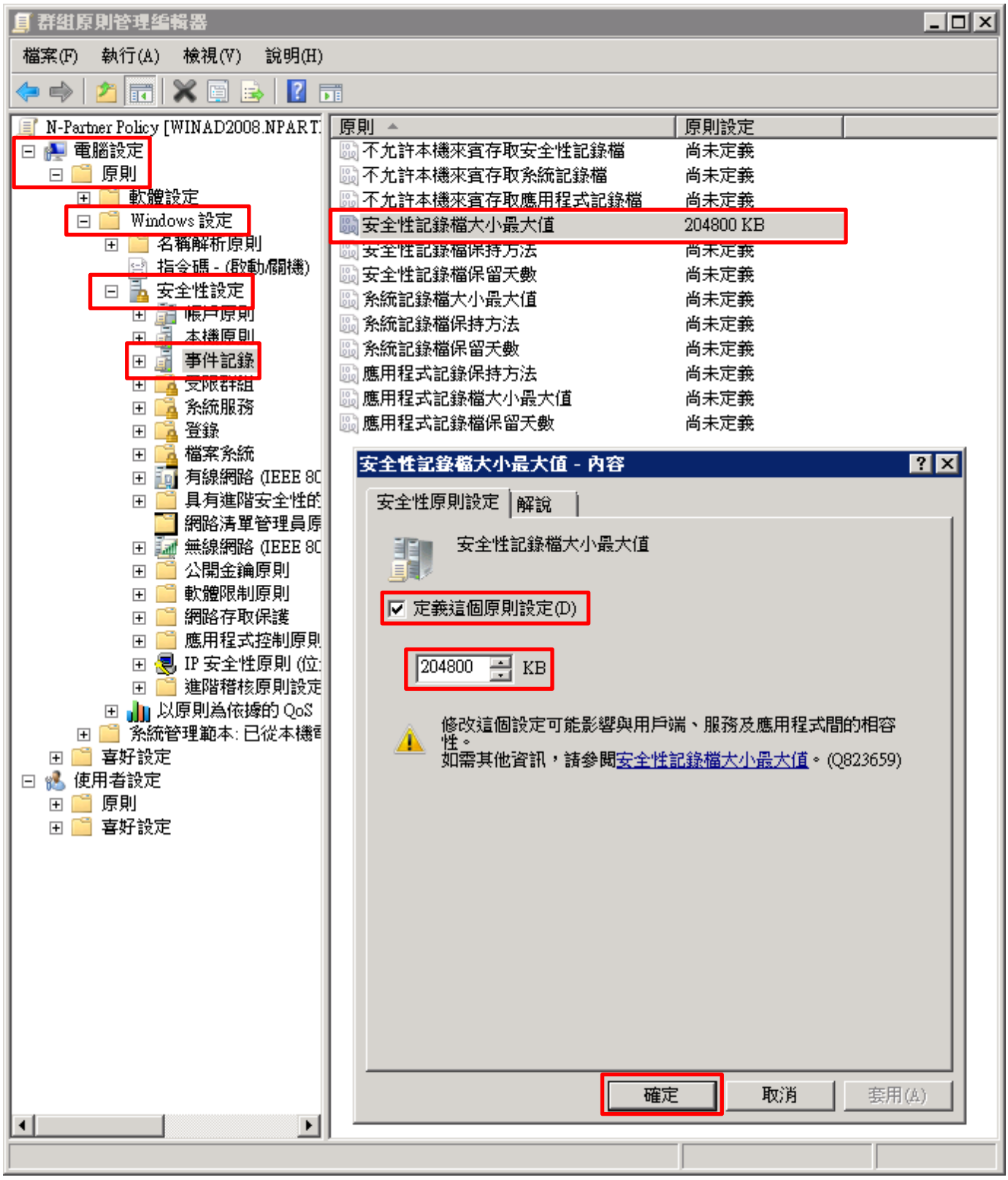
(5) 本機原則：稽核原則

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]



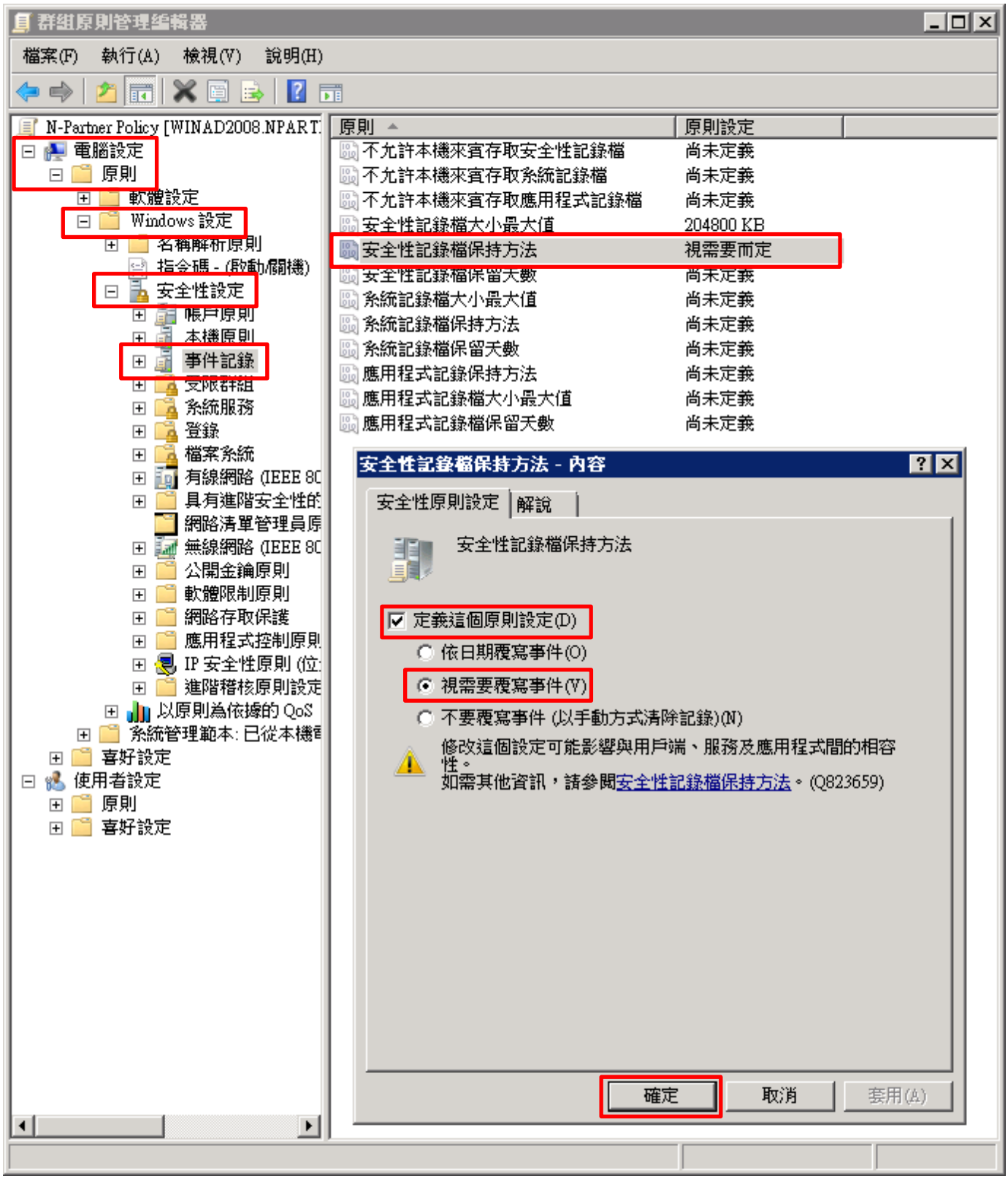
(6) 事件記錄：安全性記錄檔大小最大值

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]



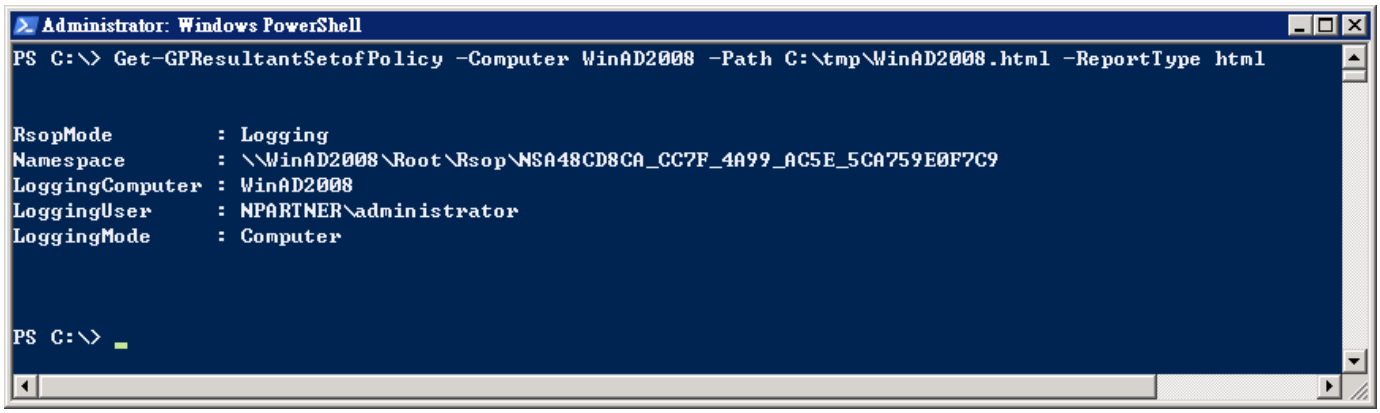
(8) 開啟 [Windows PowerShell]

(9) 更新群組原則

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

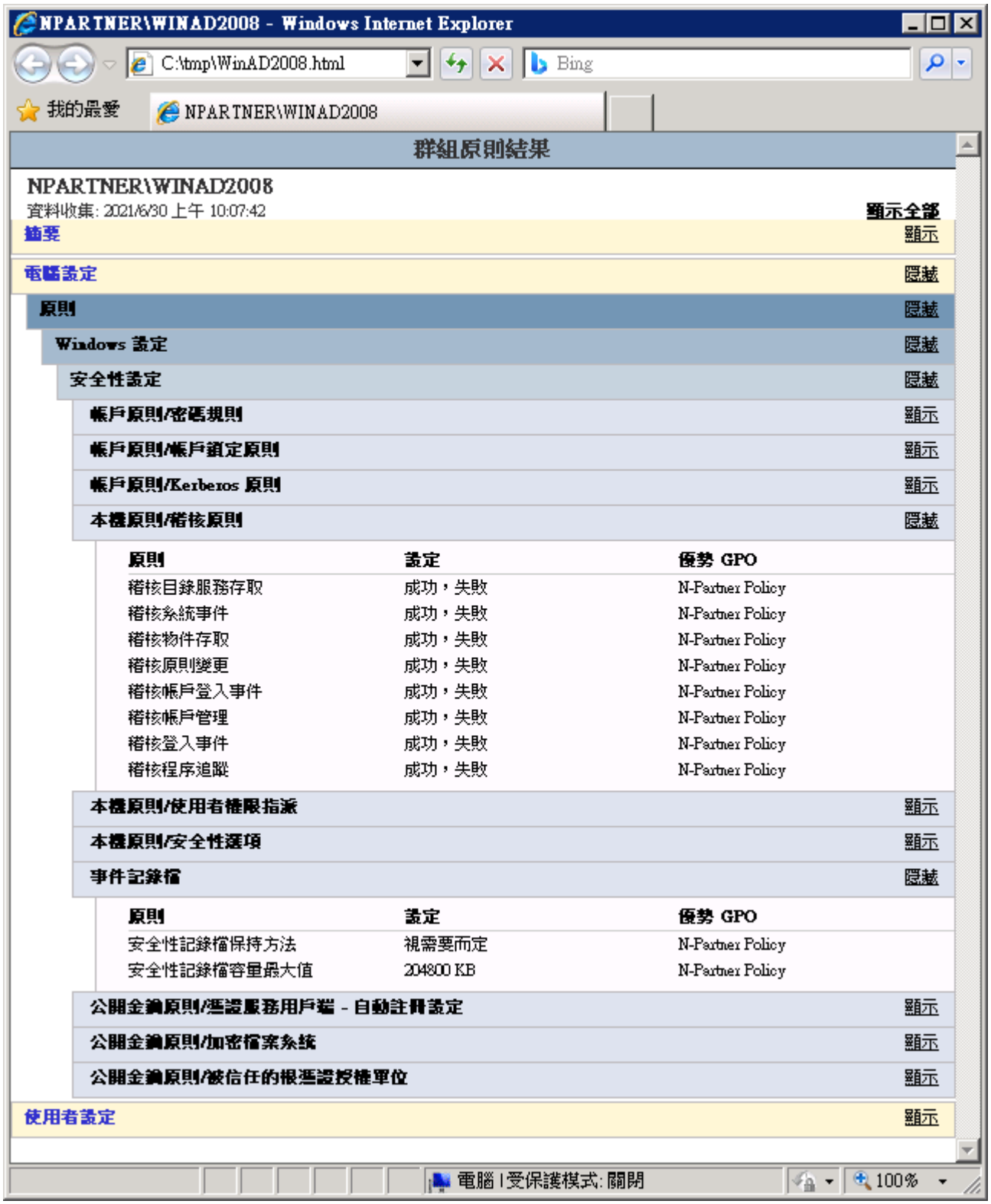
(10) 產生伺服器群組原則報表

```
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

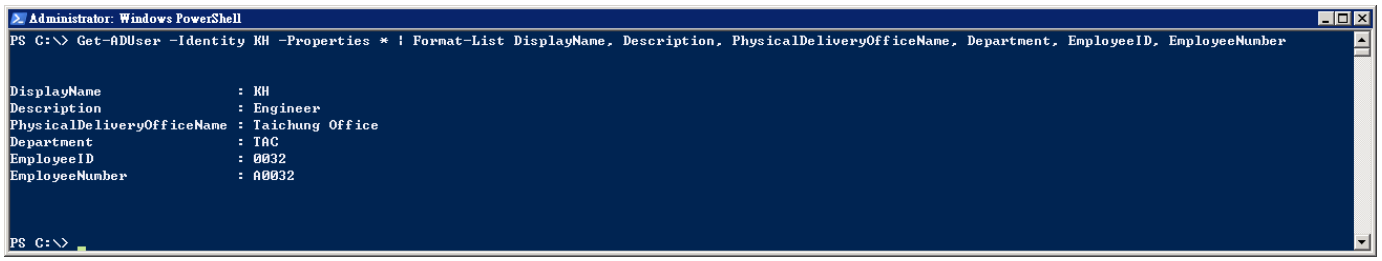


4.3 設定 WMI

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

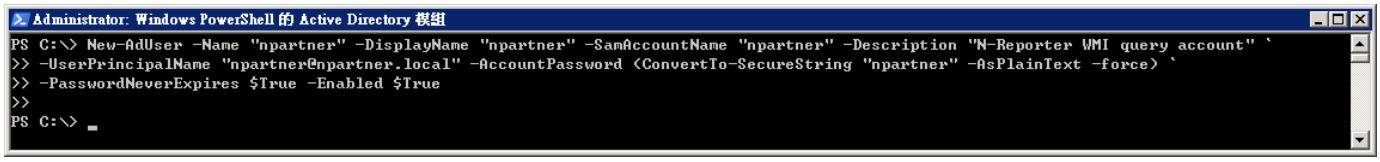
事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 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

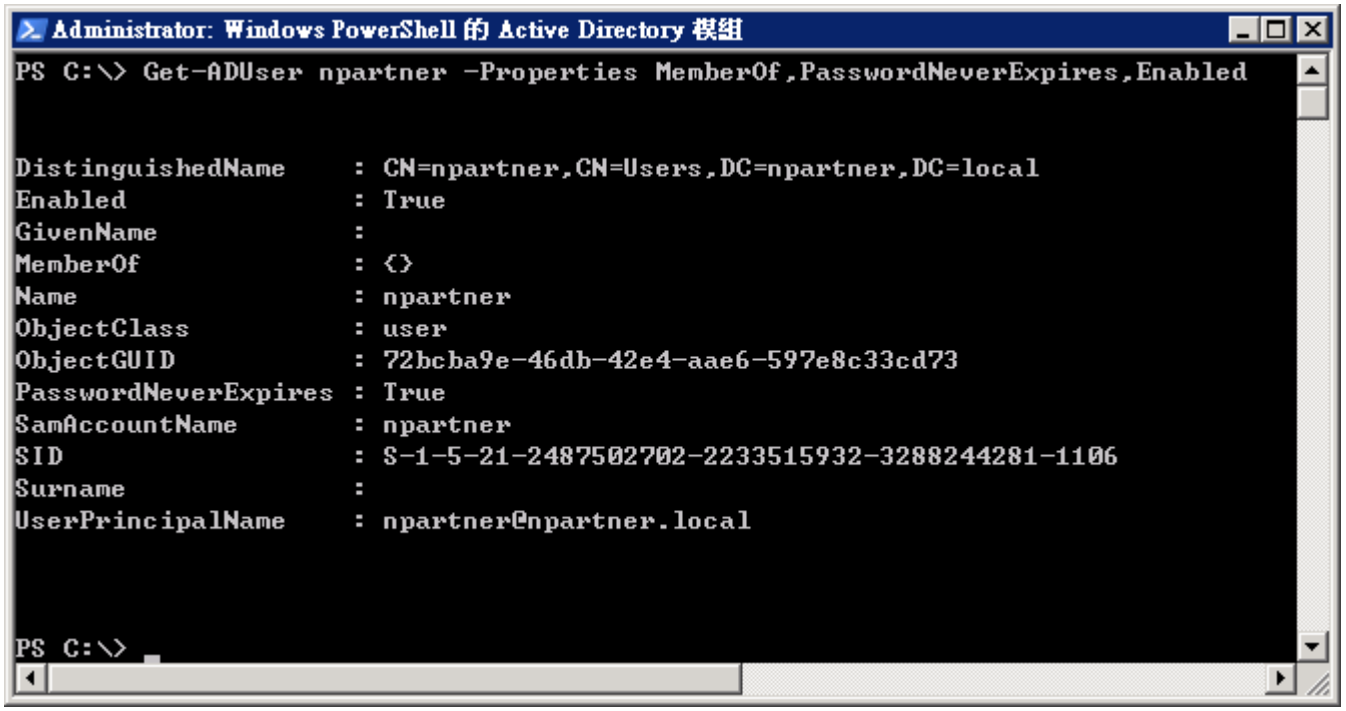
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

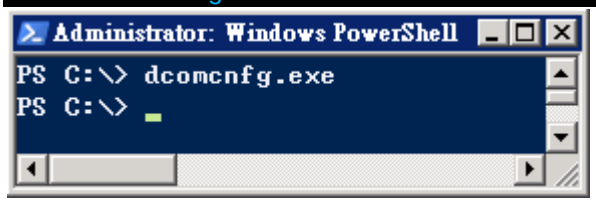


4.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

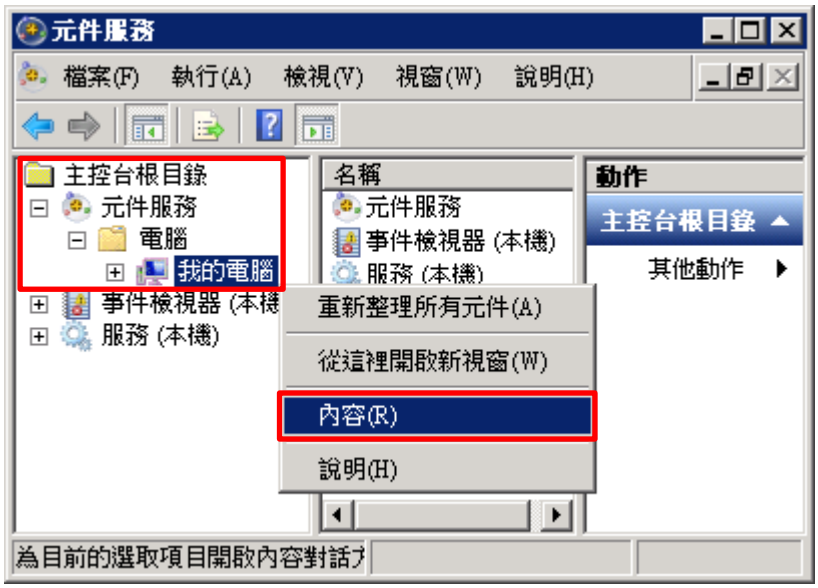
(2) 開啟元件服務

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



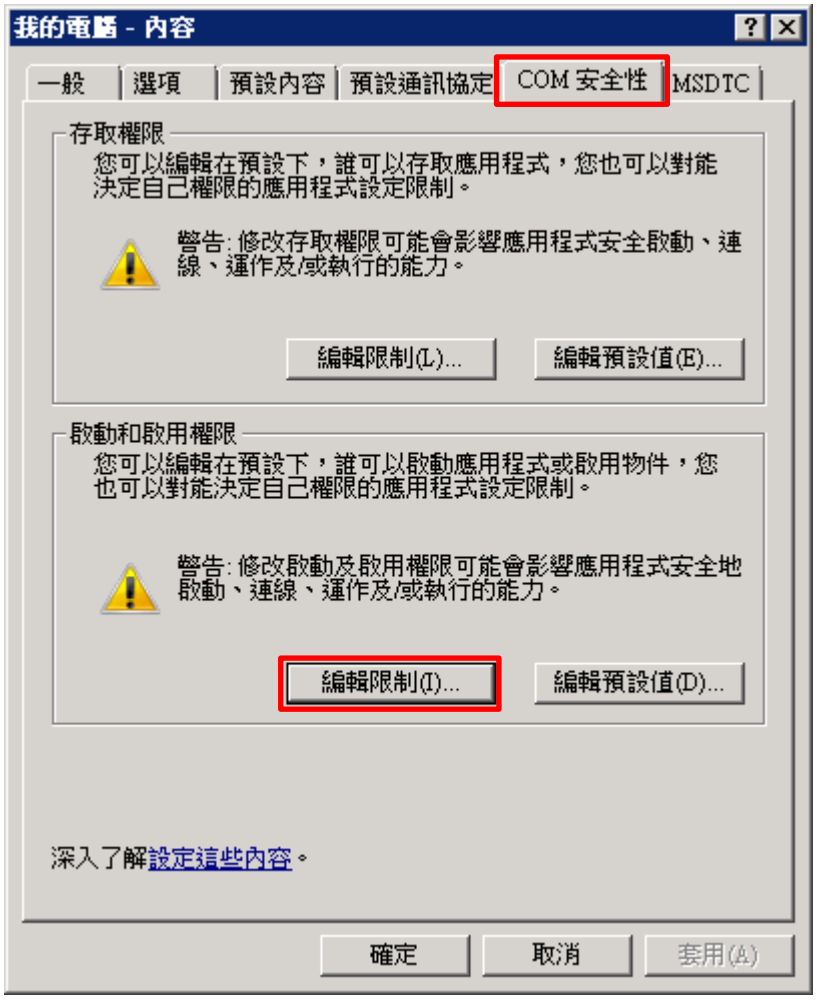
(3) 編輯電腦內容

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]



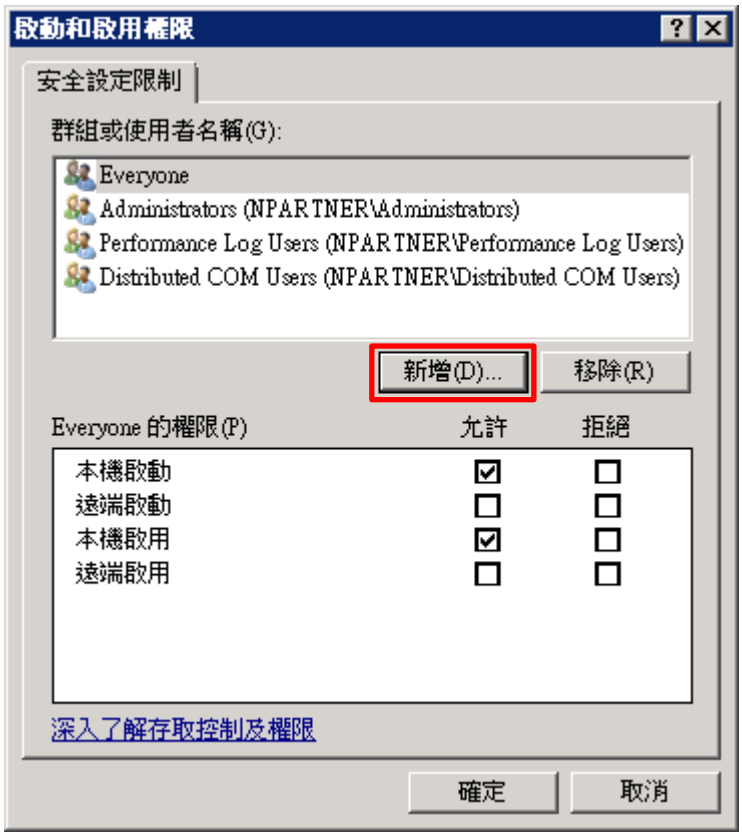
(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]



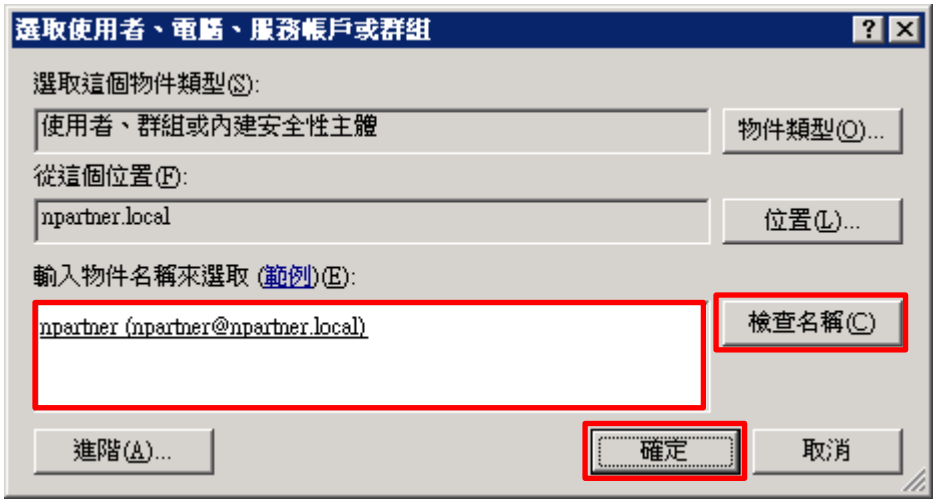
(5) 新增 DCOM 使用者權限

點選 [新增]



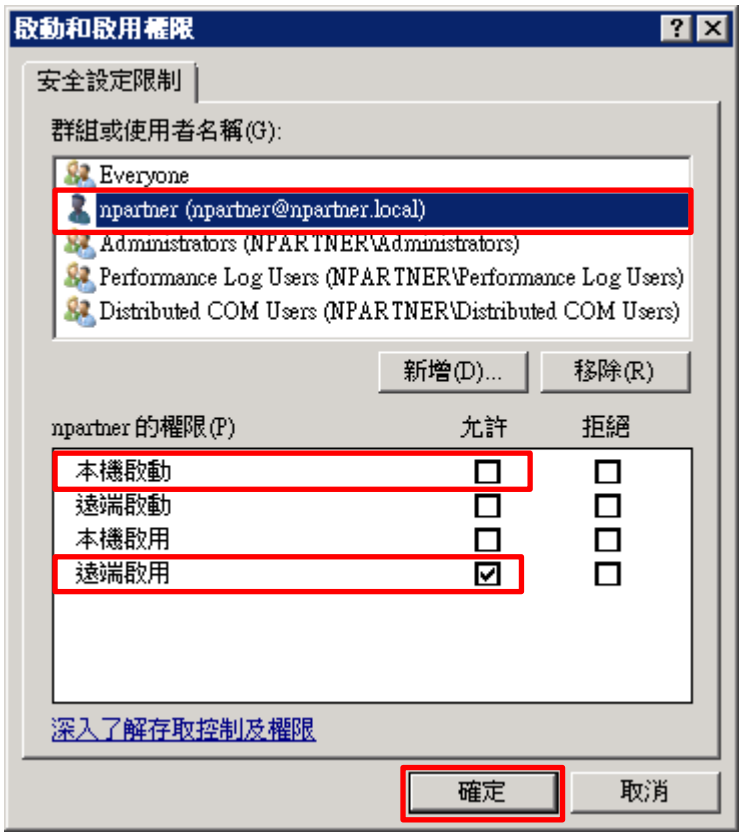
(6) 輸入使用者

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

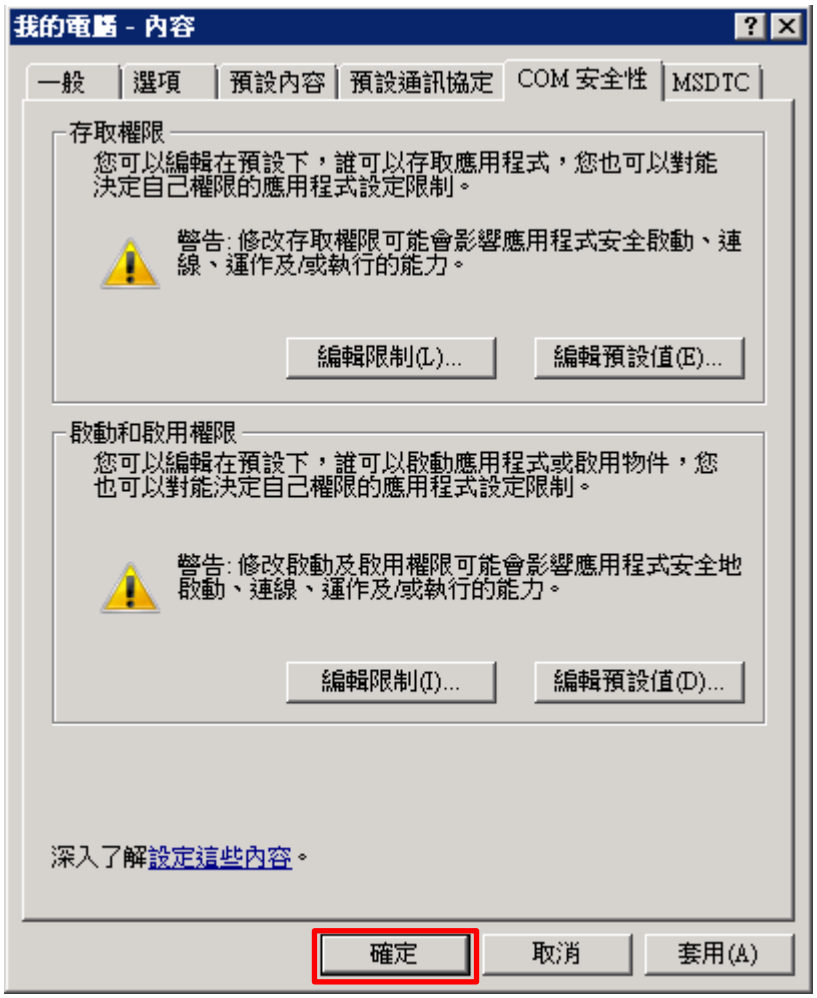


(7) 設定使用者權限

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]



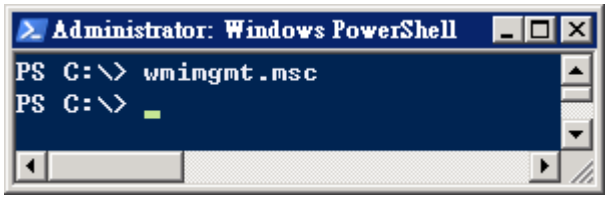
4.3.3 設定 WMI 權限

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:\> wmimgmt.msc
```

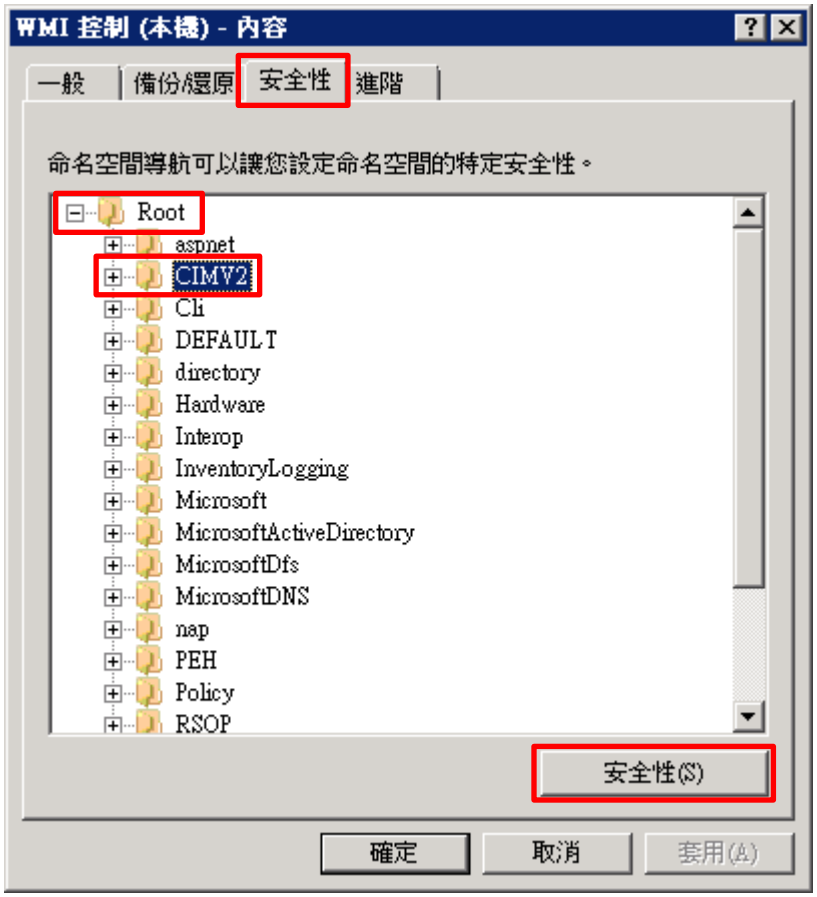


(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]

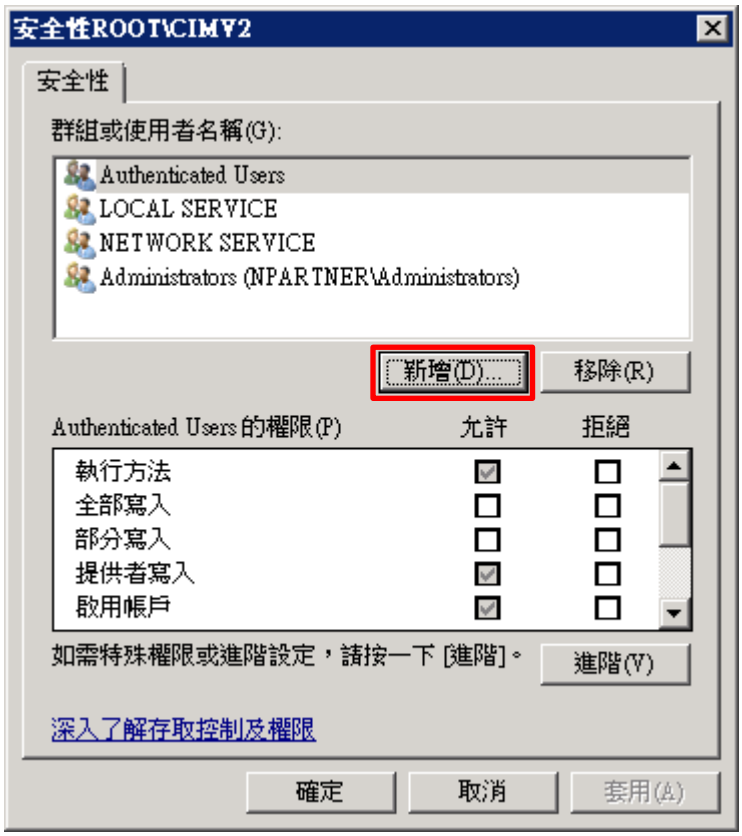
(4) 編輯 CIMV2 安全性

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



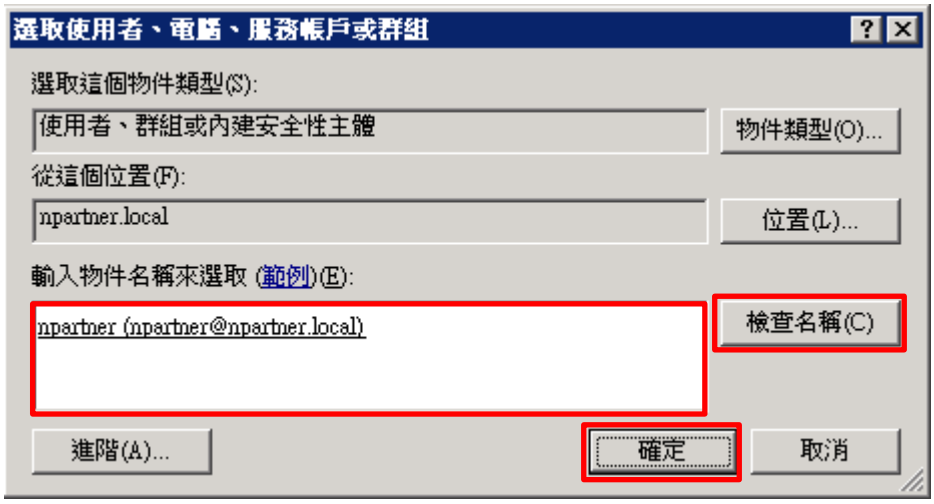
(5) 新增 WMI 使用者權限

按 [新增]



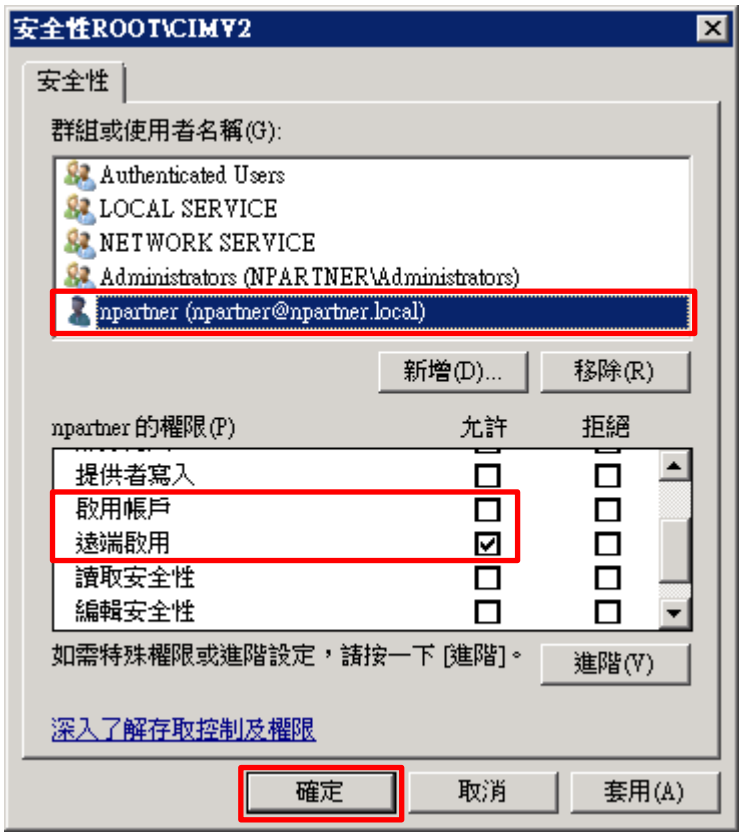
(6) 輸入使用者

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

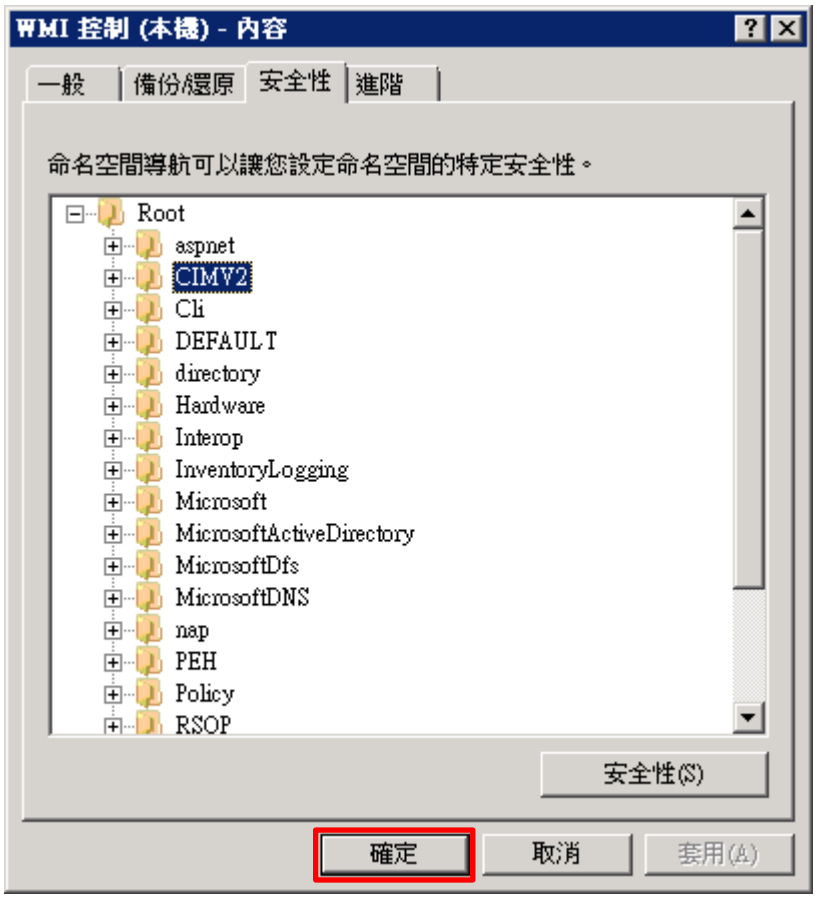


(7) 設定使用者權限

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]

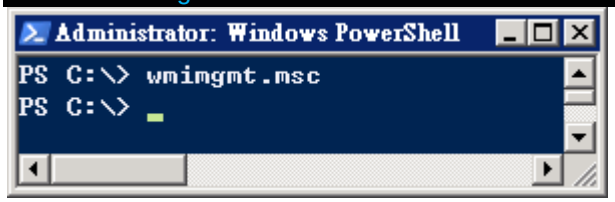


4.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

(2) 開啟元件服務

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

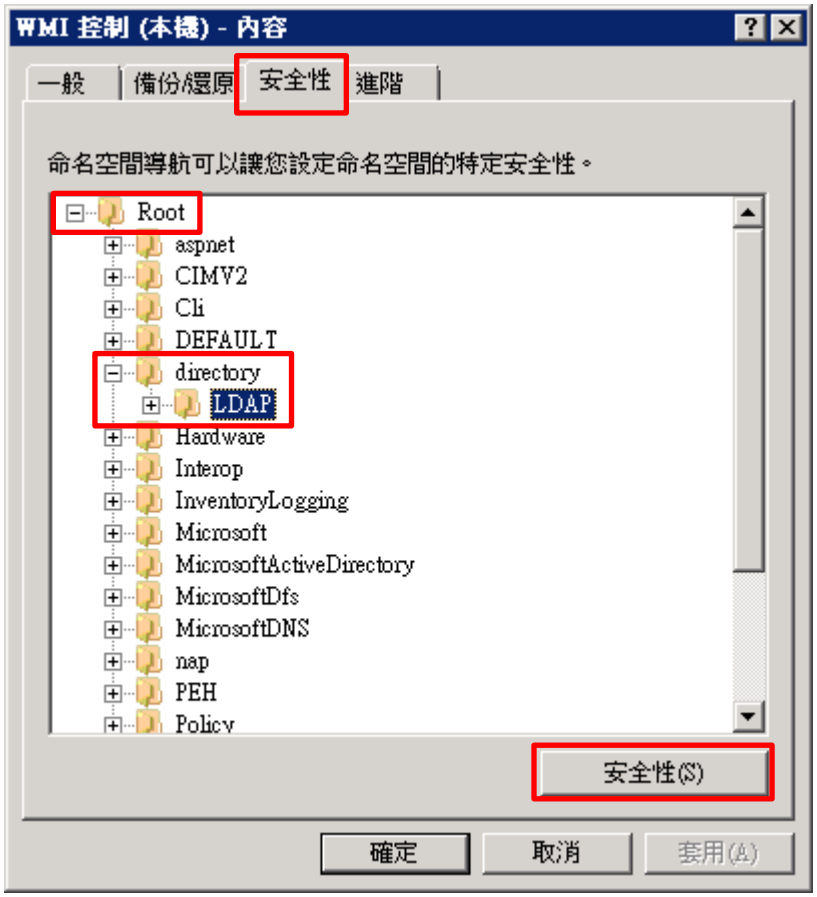


(3) 編輯 WMI 控制

點選 [WMI 控制 (本機)] -> 按  [內容]

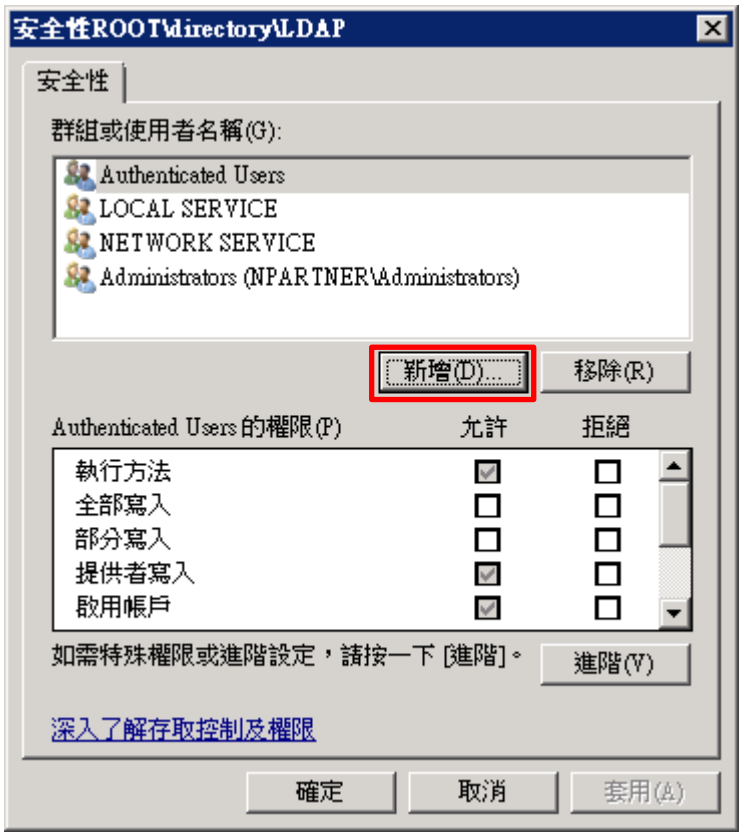
(4) 編輯 LDAP 安全性

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



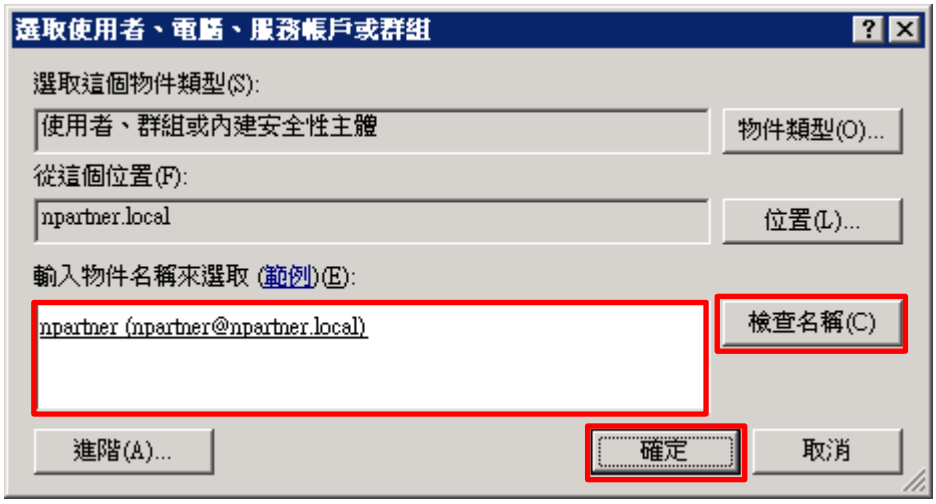
(5) 新增 WMI 使用者權限

按 [新增]



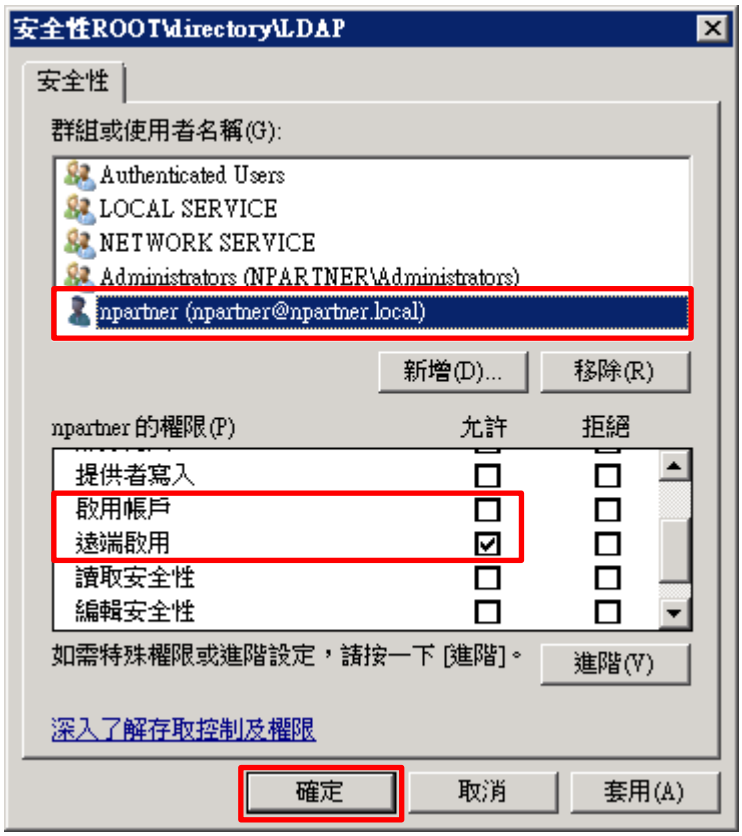
(6) 輸入使用者

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

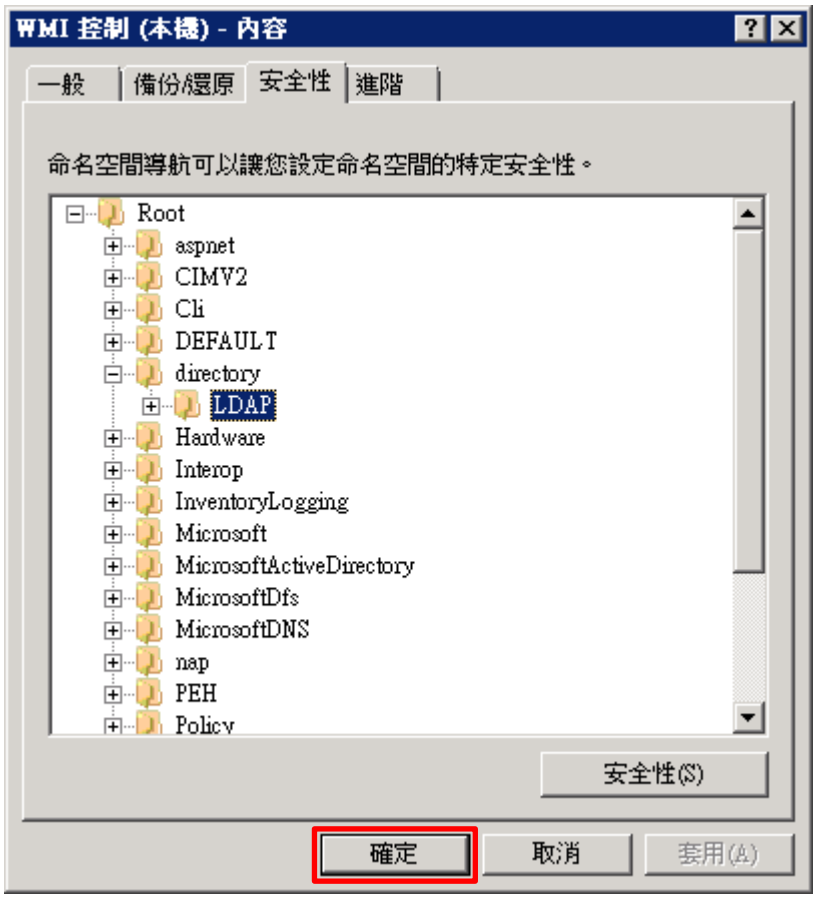


(7) 設定使用者權限

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]



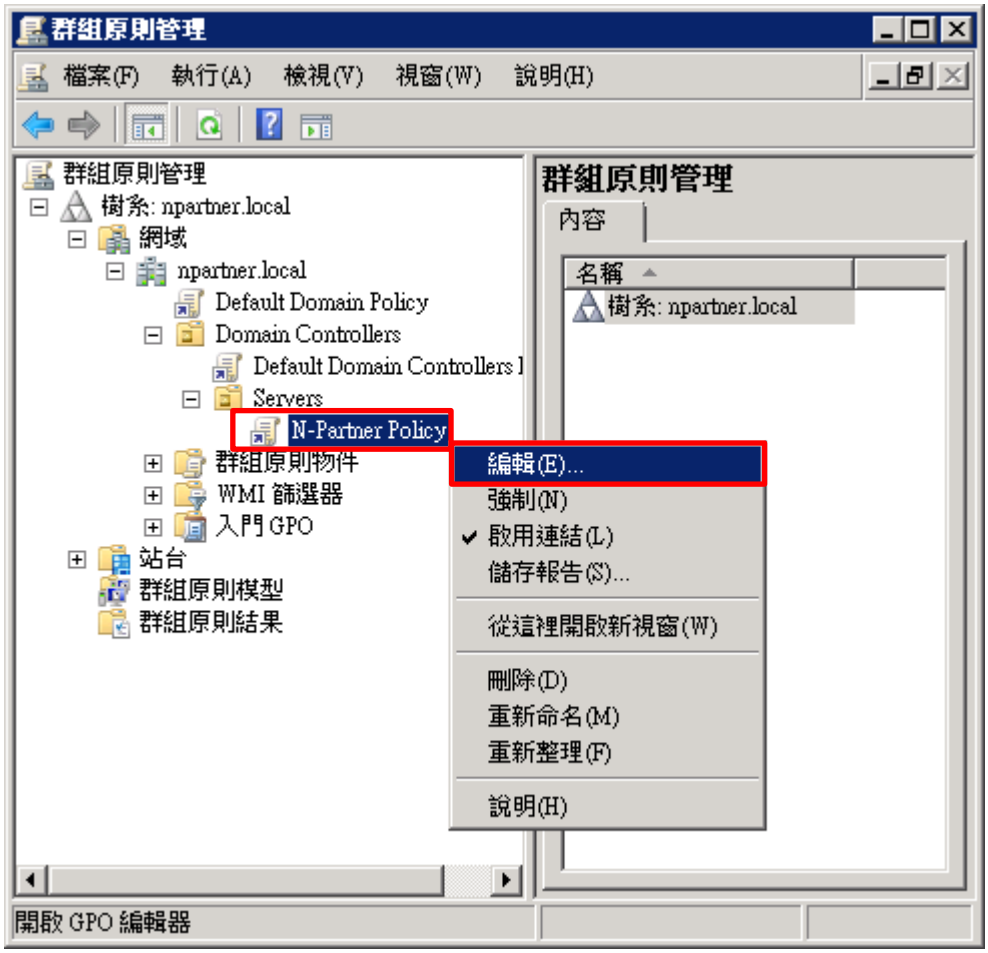
4.3.4 設定 Event log 讀取權限

(1) 開啟群組原則管理

開啟 [群組原則管理]

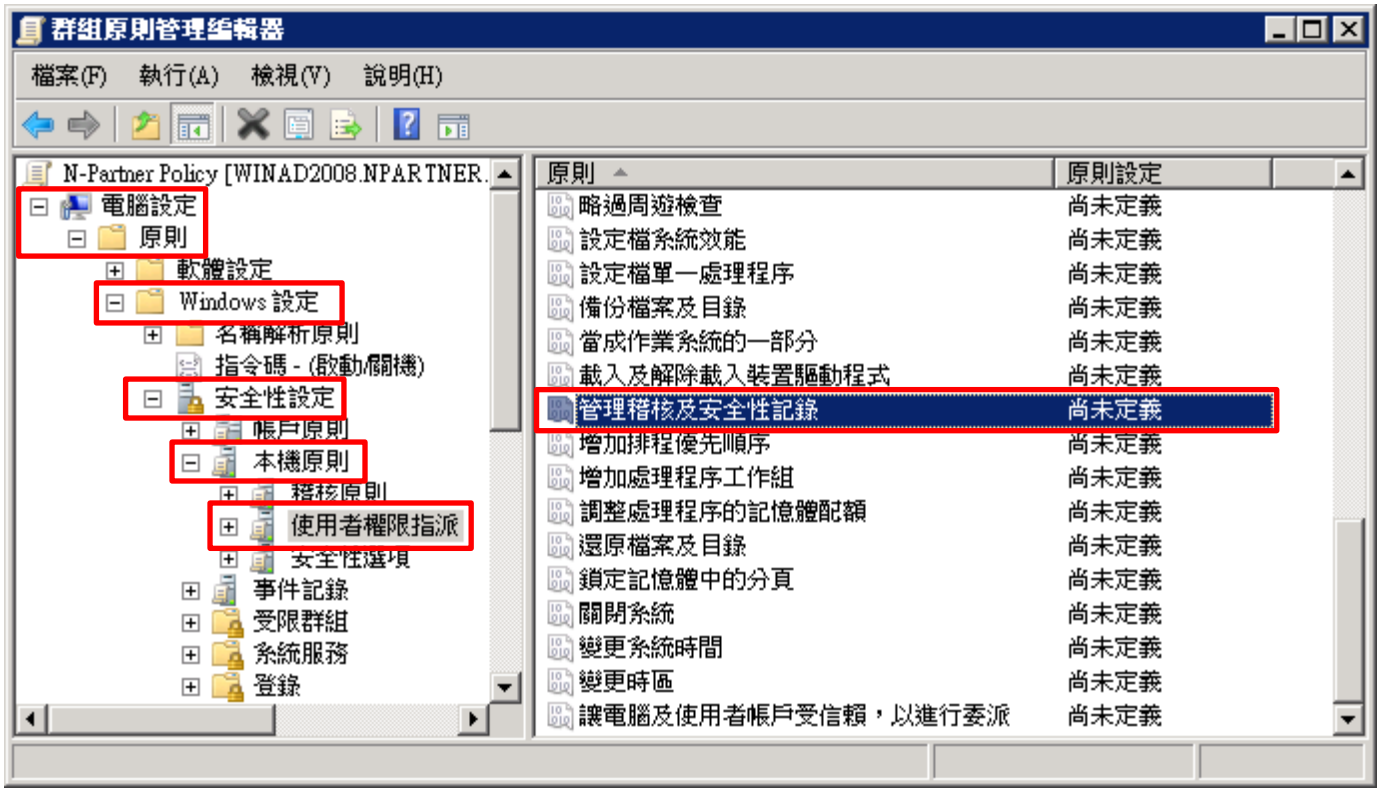
(2) 編輯群組原則物件

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



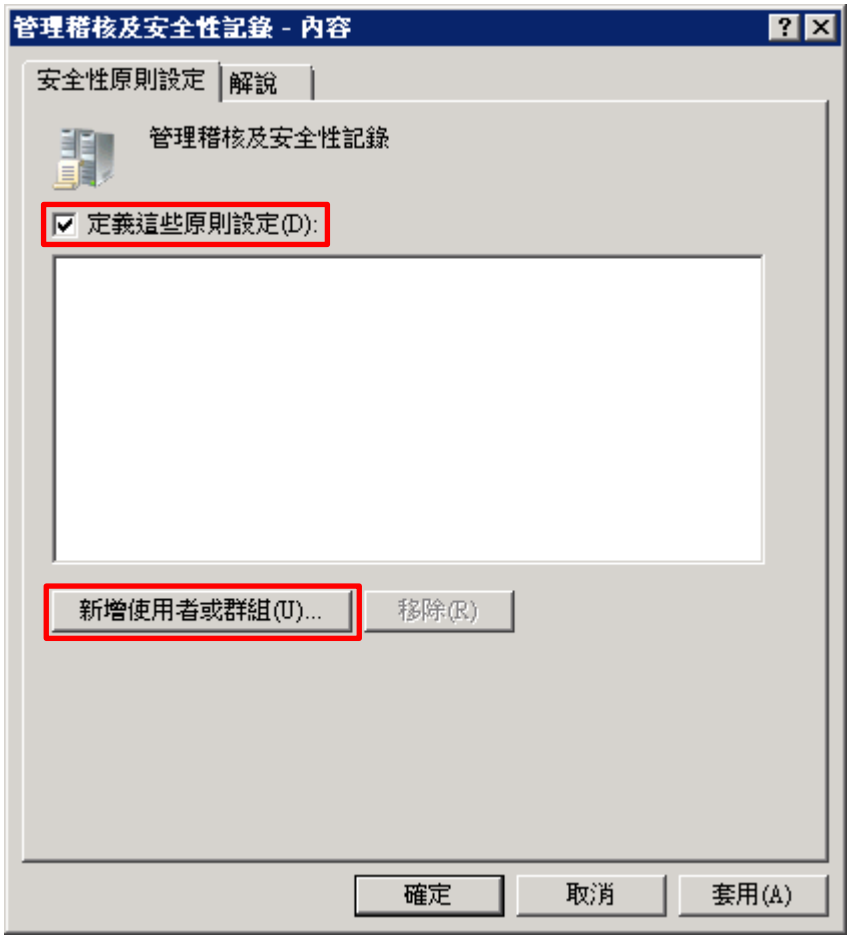
(3) 設定記錄檔

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



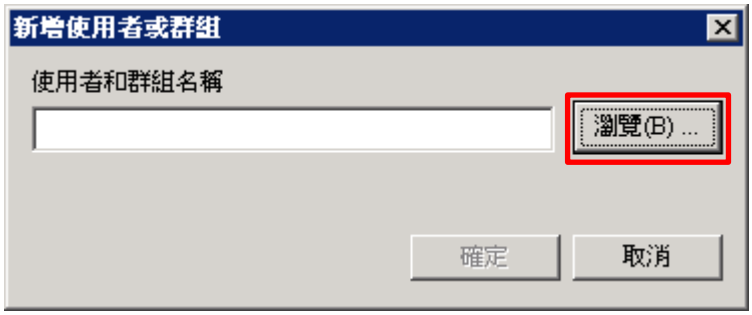
(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]



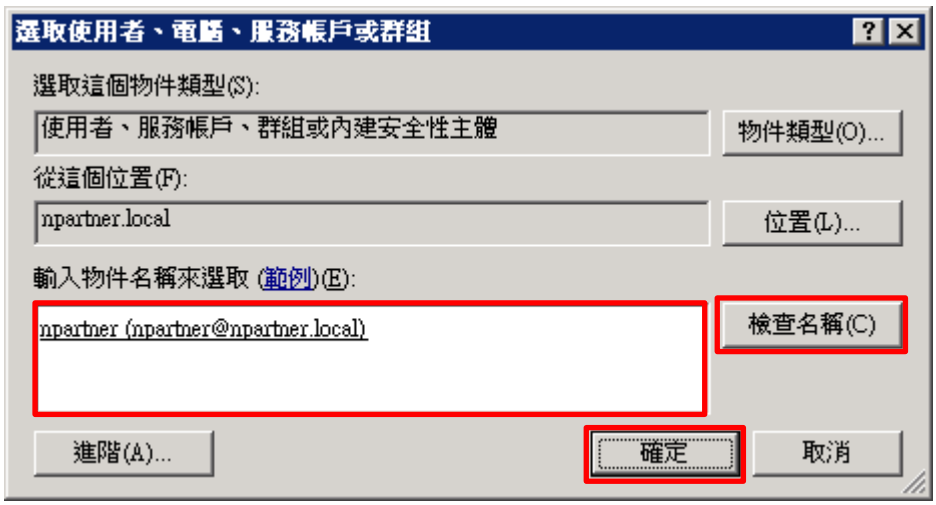
(5) 搜尋使用者

按 [瀏覽]



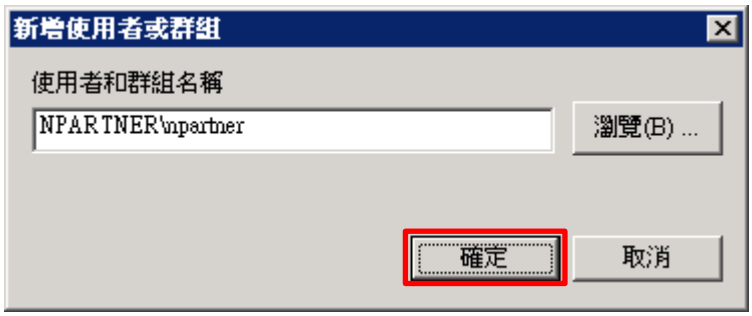
(6) 輸入使用者

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



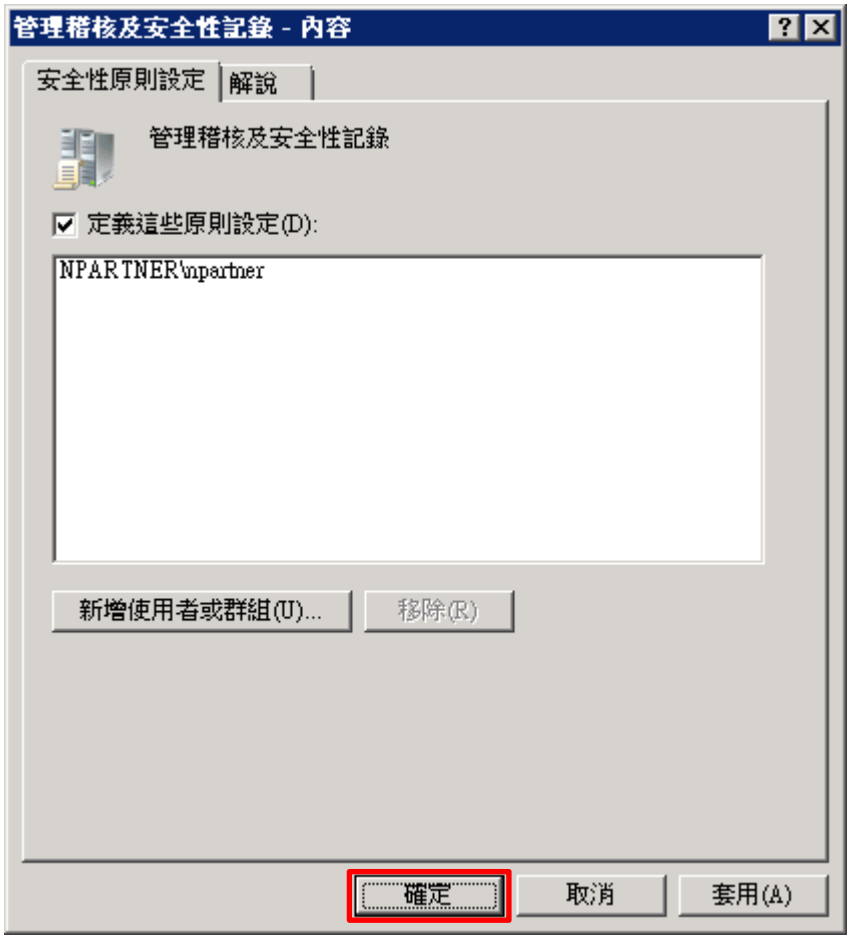
(7) 確定使用者

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

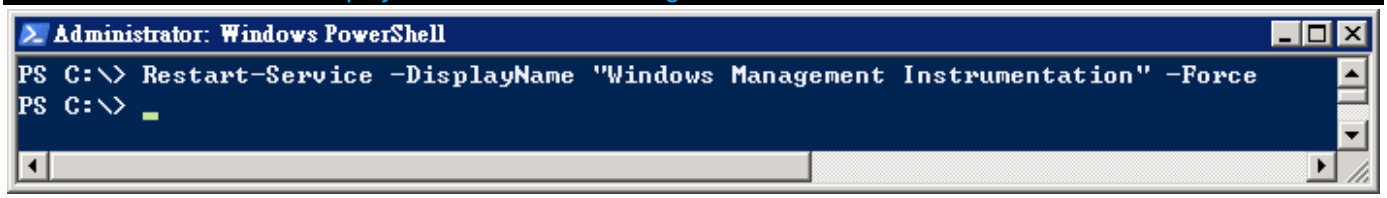
```
PS C:\> gpupdate /force
```

4.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

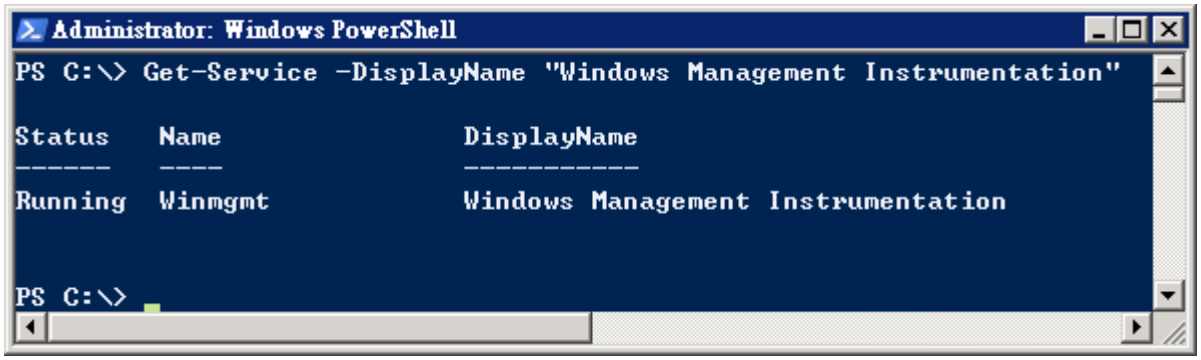
(2) 重啟 WMI 服務

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



(3) 查看 WMI 服務

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

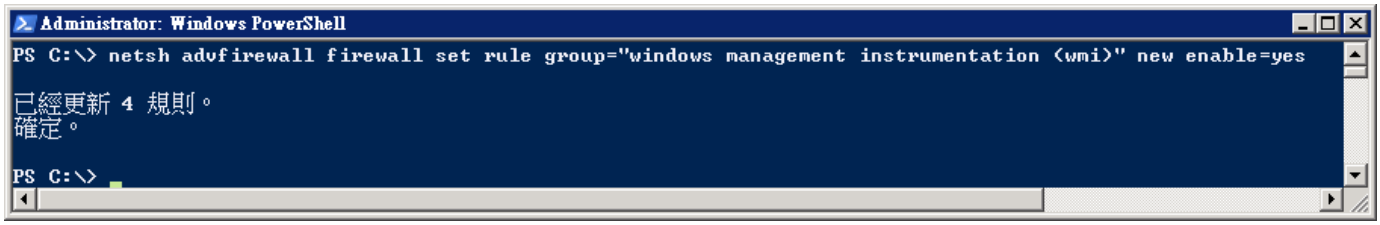


4.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]

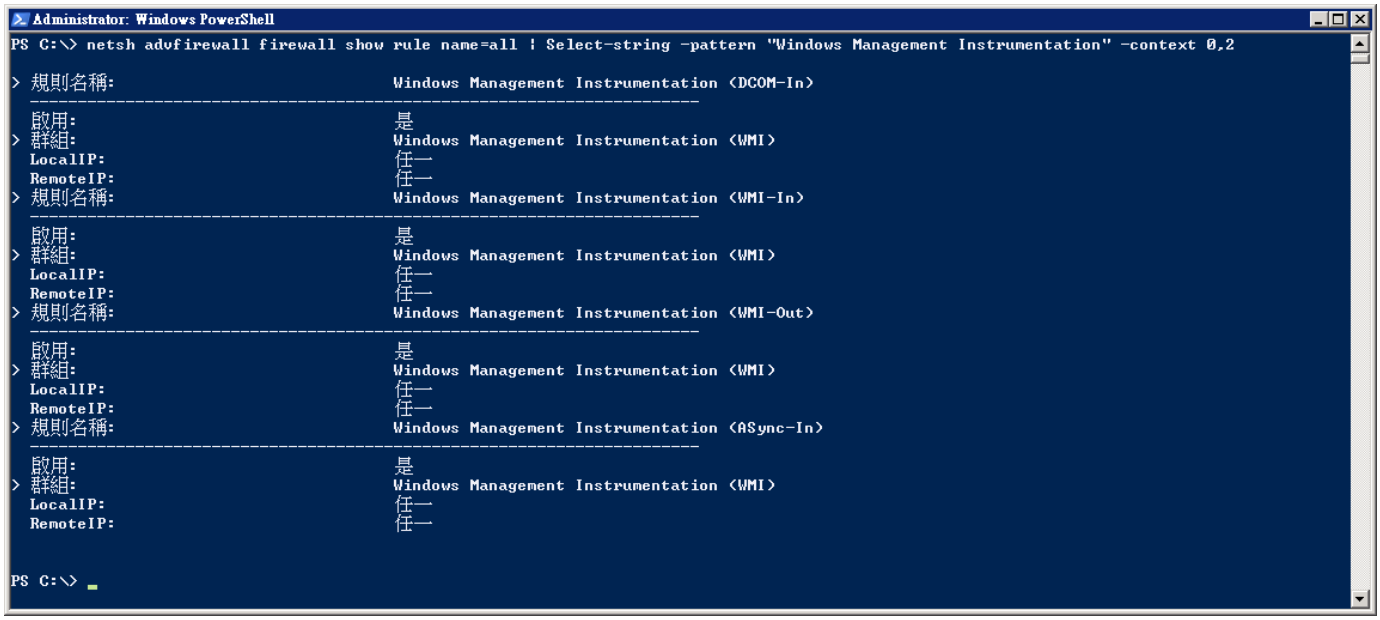
(2) 允許 WMI 通過防火牆

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



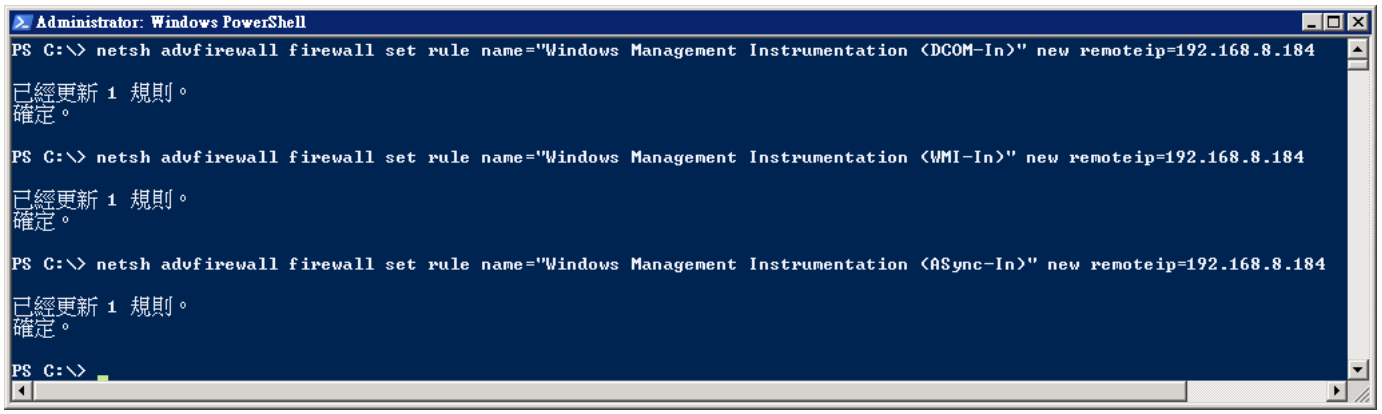
(3) 查看防火牆 WMI 啟用狀態

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



(4) 設定防火牆，只允許 N-Reporter IP query WMI

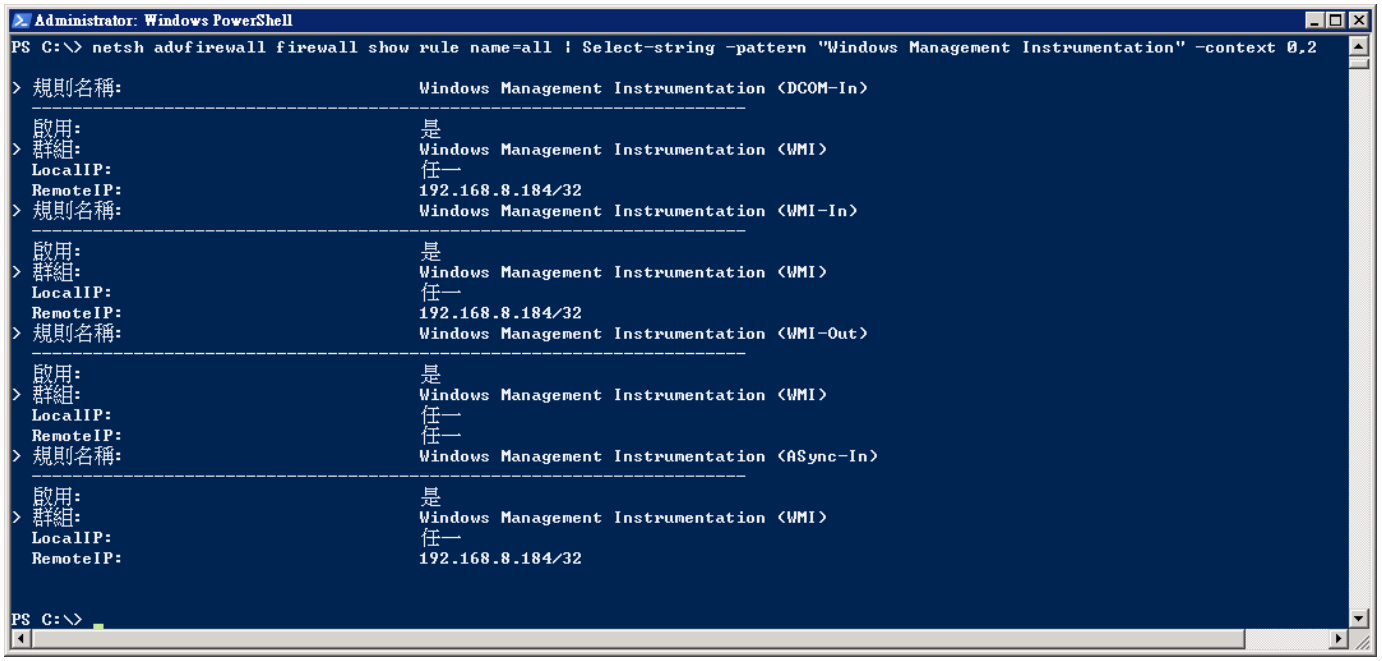
```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows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



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
```



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

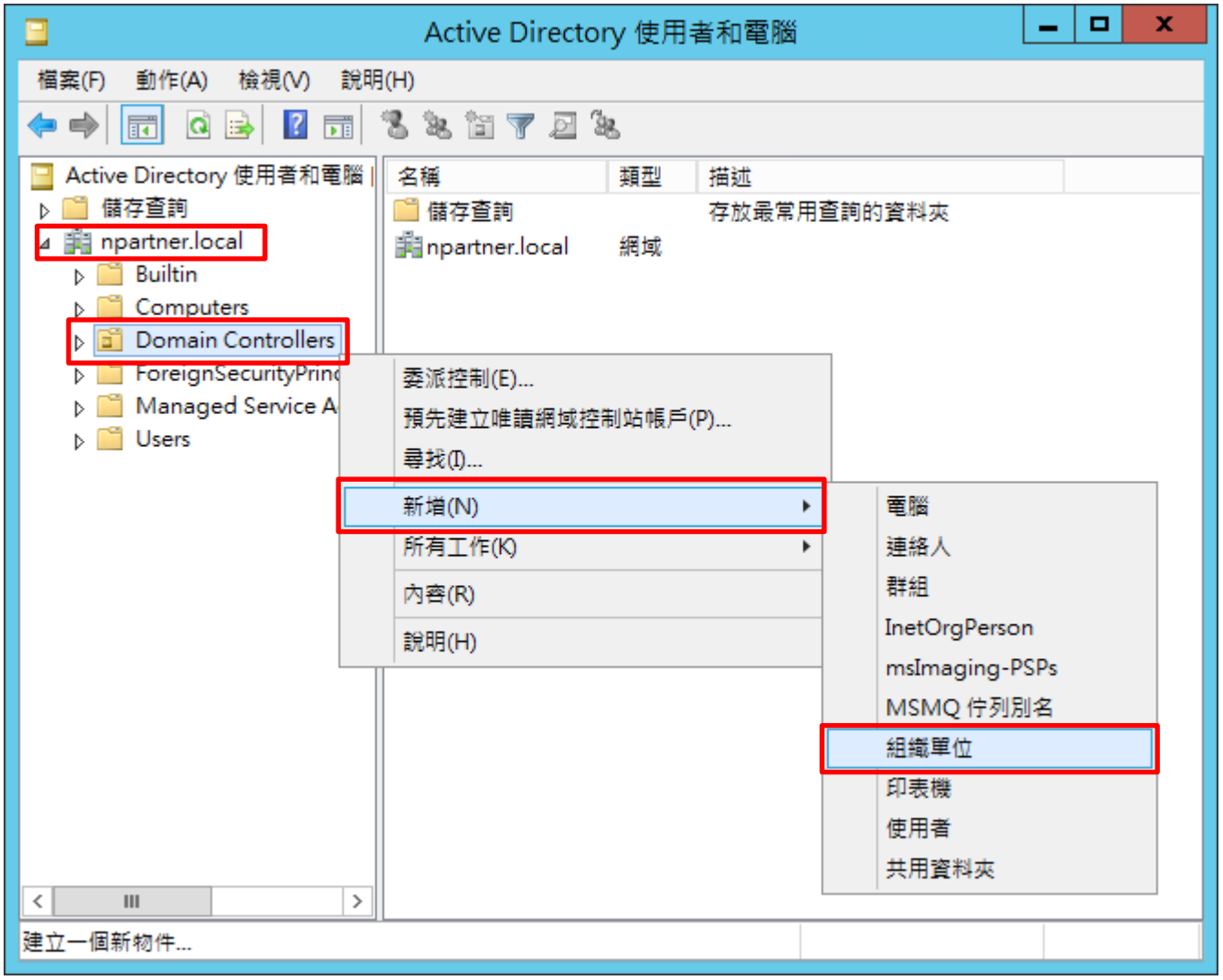
5.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

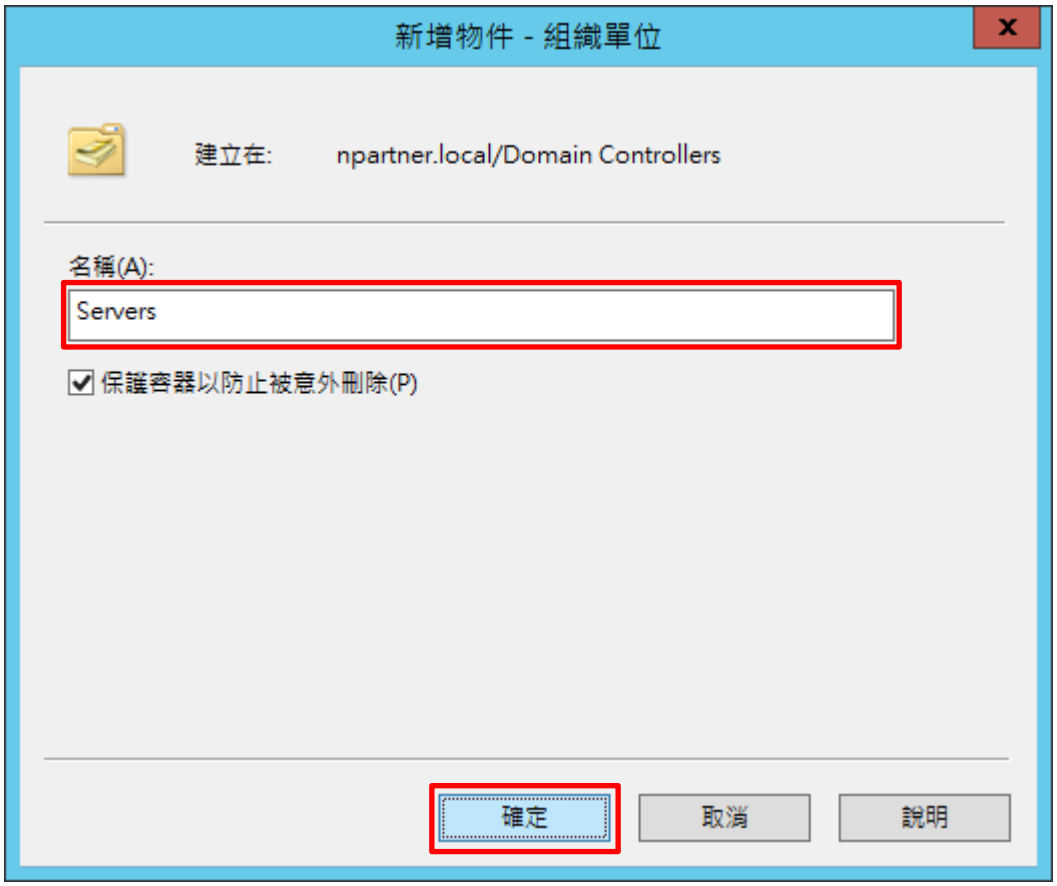
(2) 新增組織單位

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]



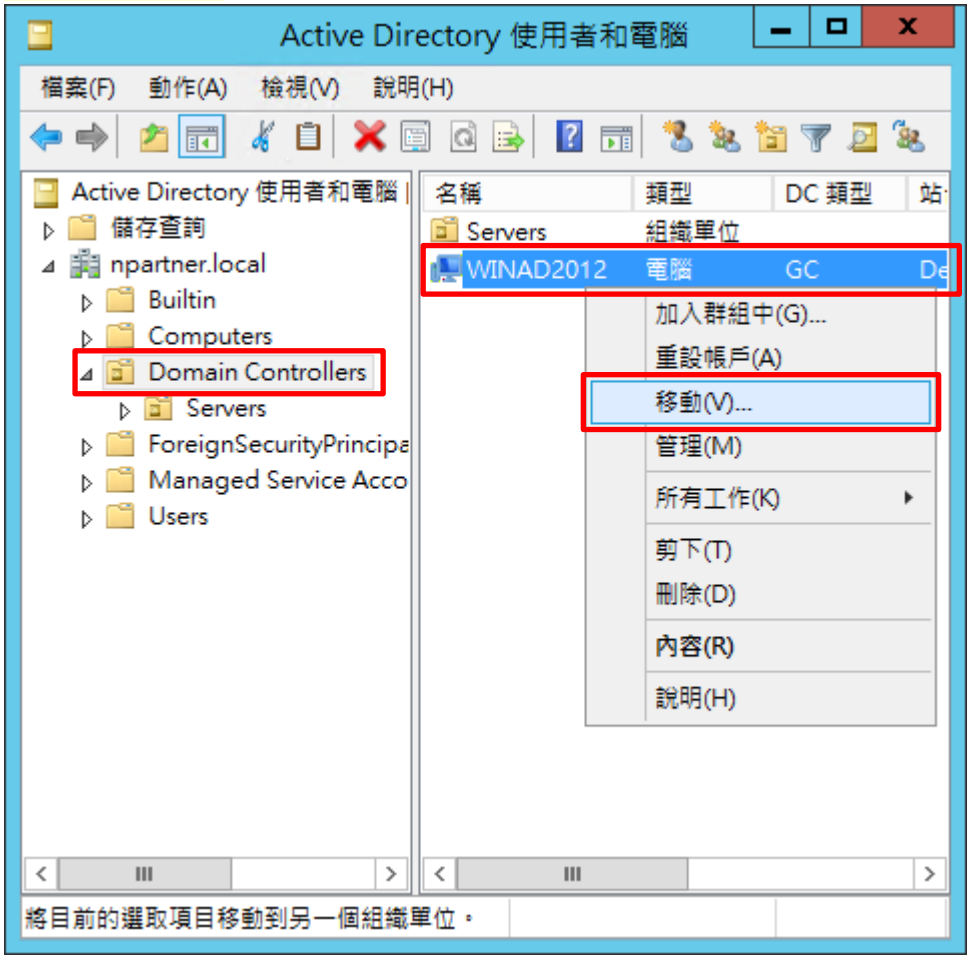
(3) 輸入組織單位名稱

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]



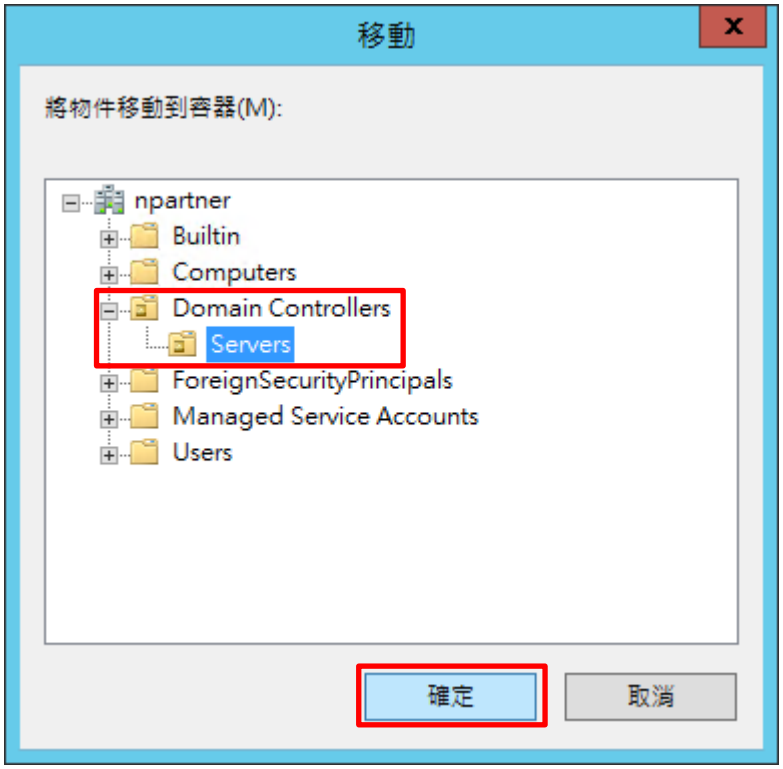
(4) 移動伺服器至新的組織單位

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]



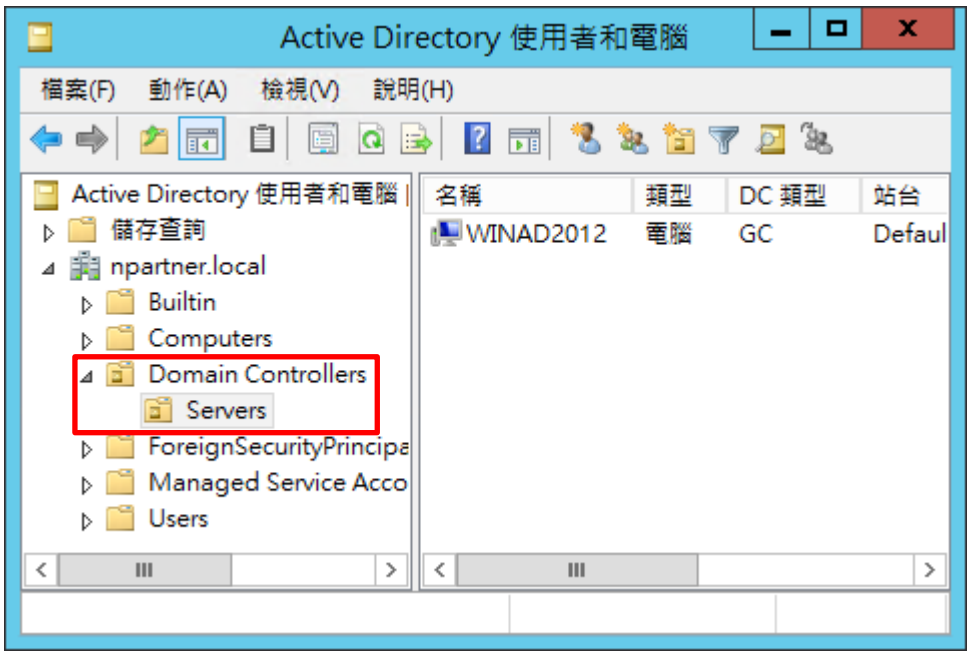
(5) 選擇組織單位

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

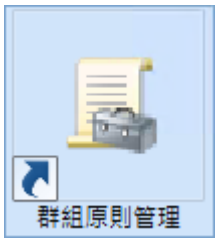
點選 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2012] 網域伺服器已移動。



5.2 群組原則設定

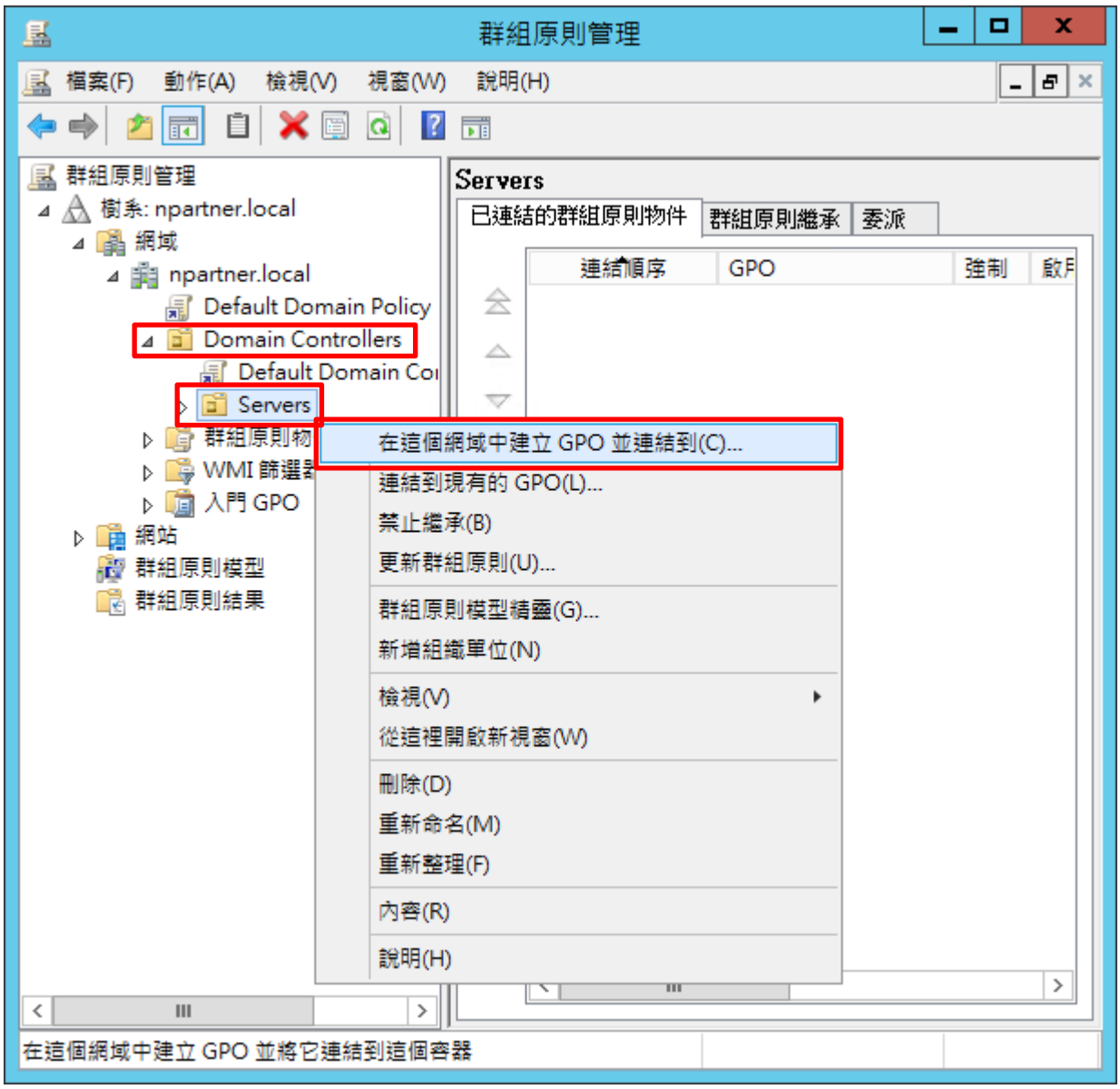
(1) 開啟群組原則管理

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

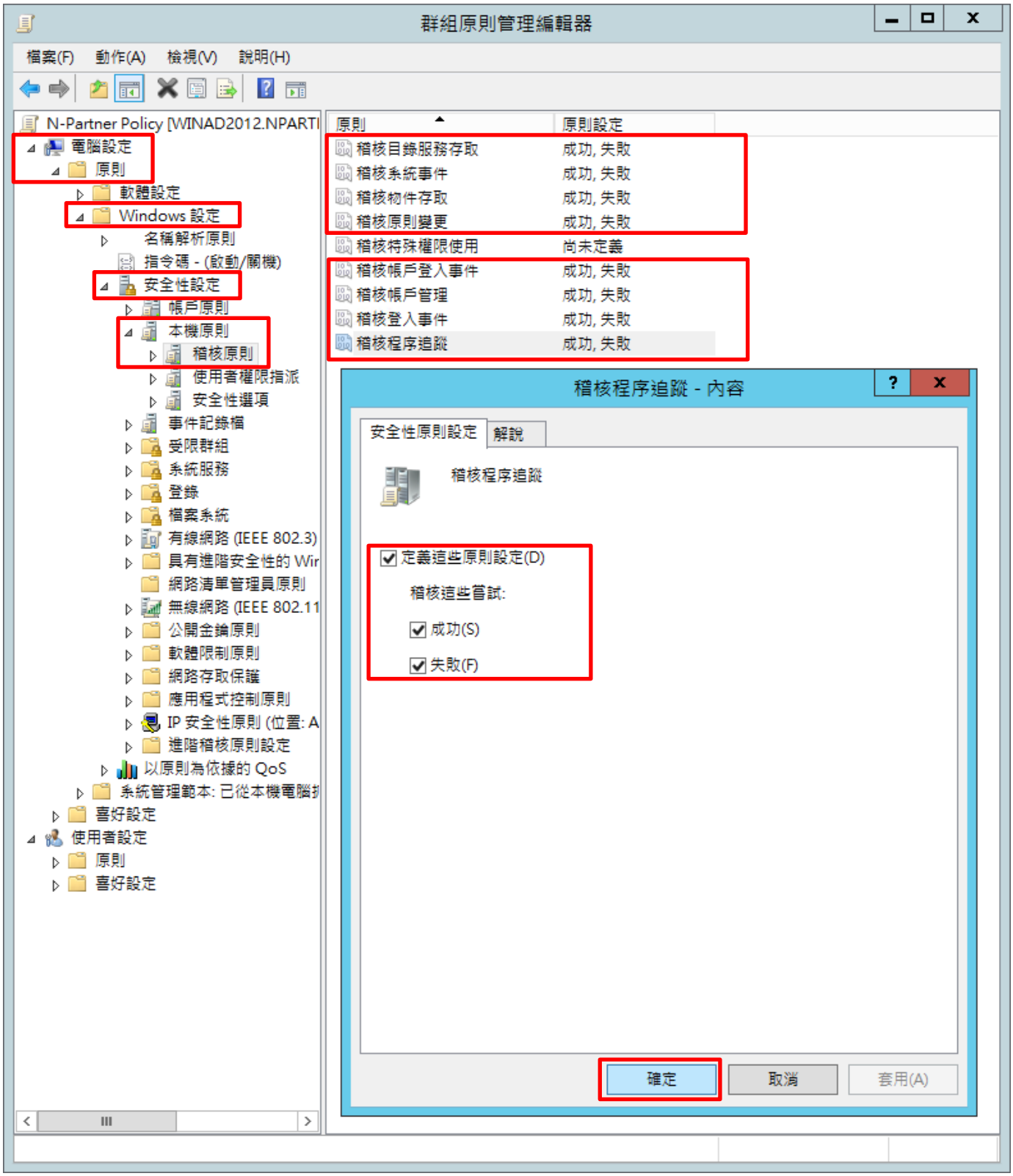
輸入群組原則物件名稱: N-Partner Policy 註：請依客戶環境建立群組物件名稱 -> 按 [確定]

(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]

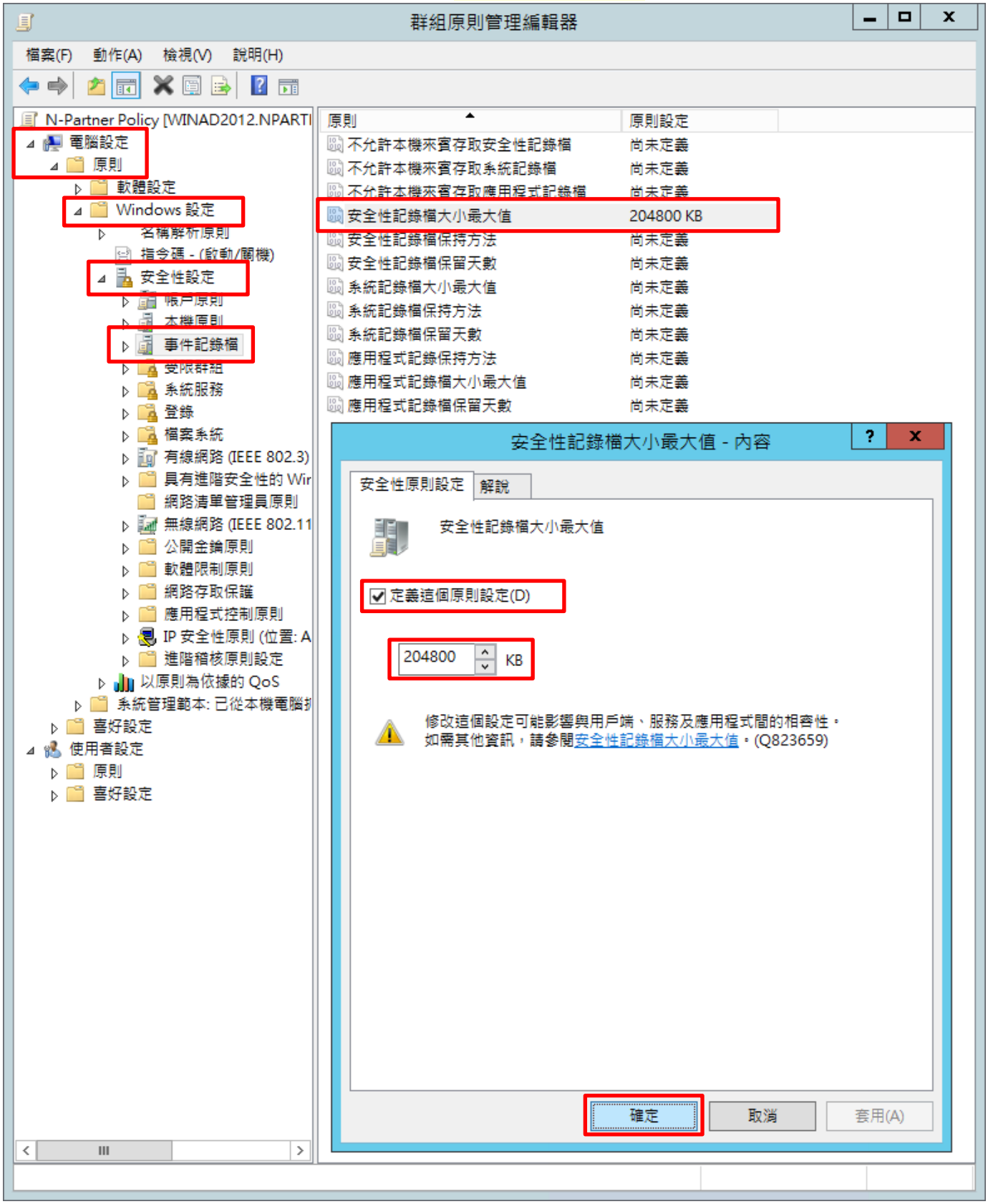
(5) 本機原則：稽核原則

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]



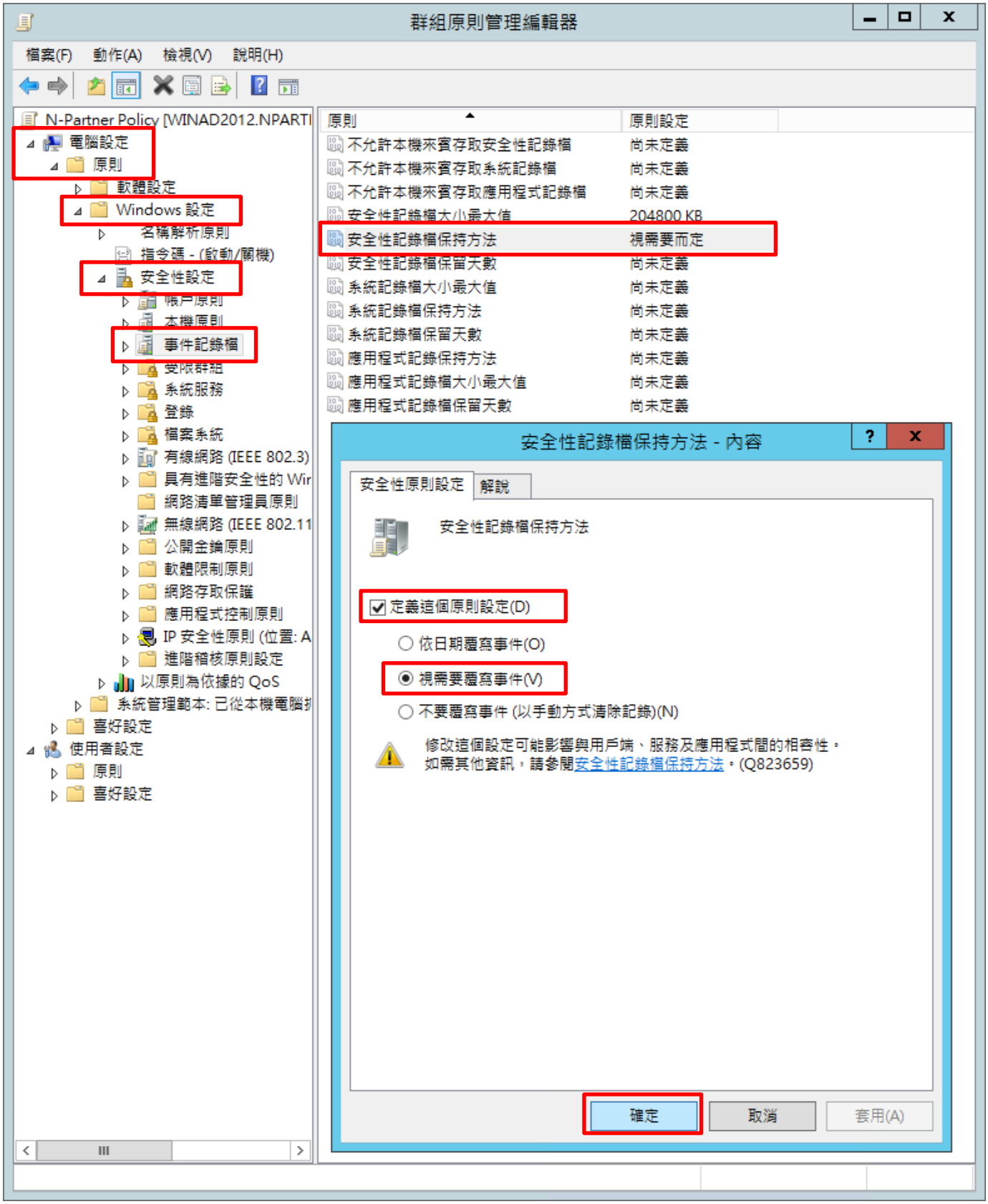
(6) 事件記錄檔：安全性記錄檔大小最大值

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]



(7) 事件記錄檔：安全性記錄檔保持方法

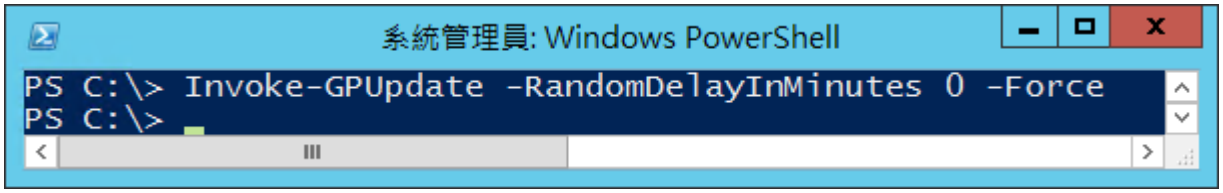
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

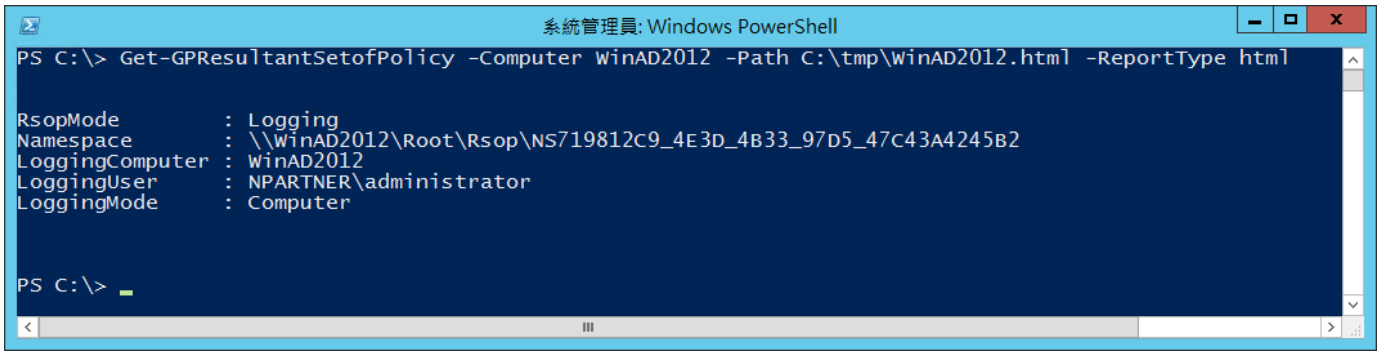
(9) 更新群組原則

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



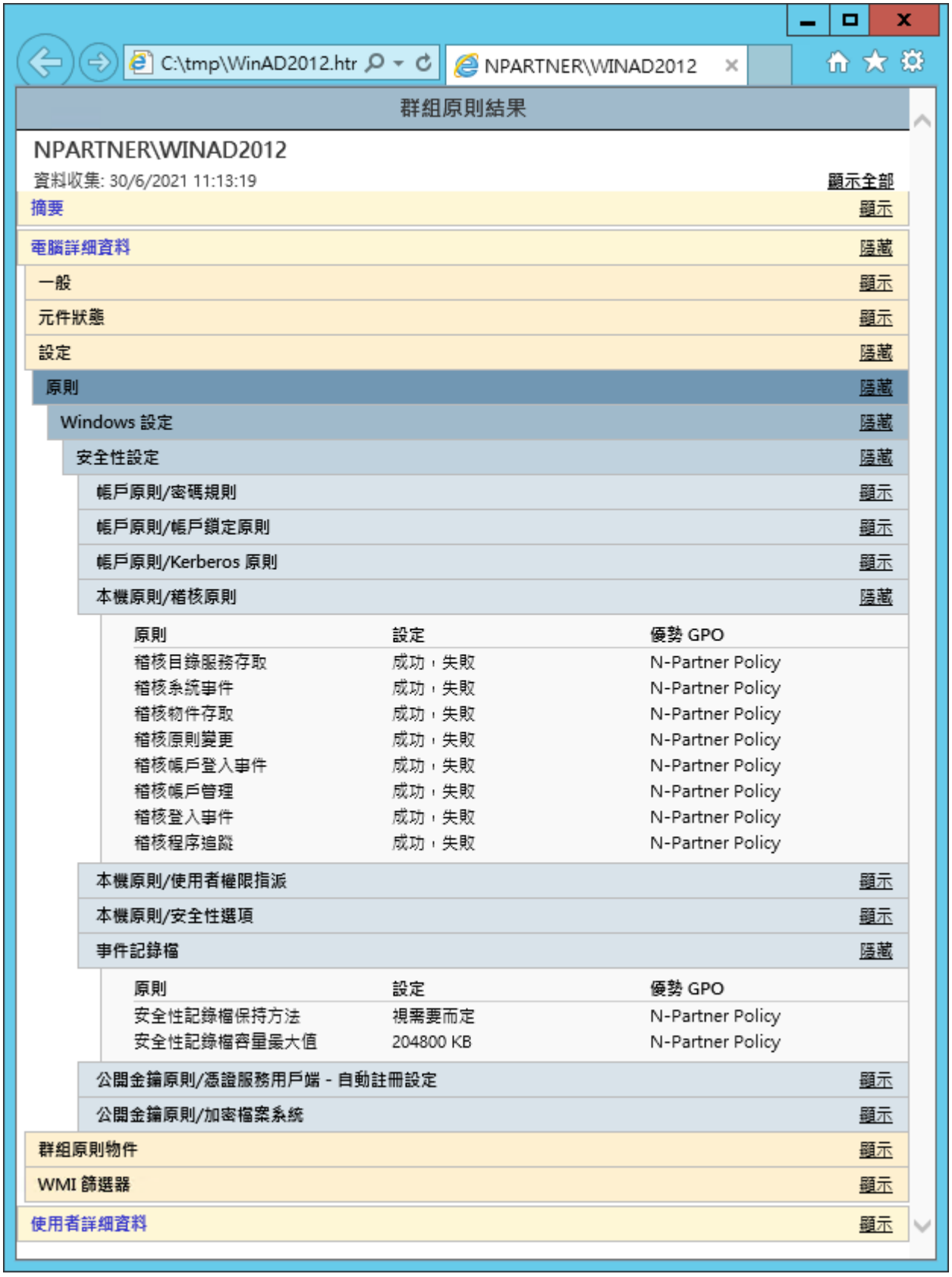
(10) 產生伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer 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

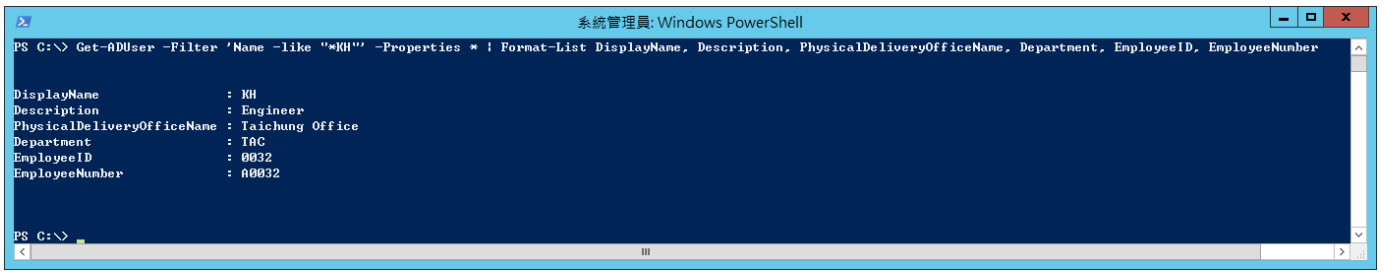


5.3 設定 WMI

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
```



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

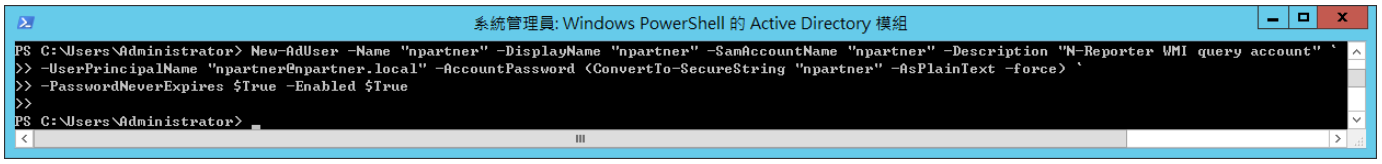
事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500 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

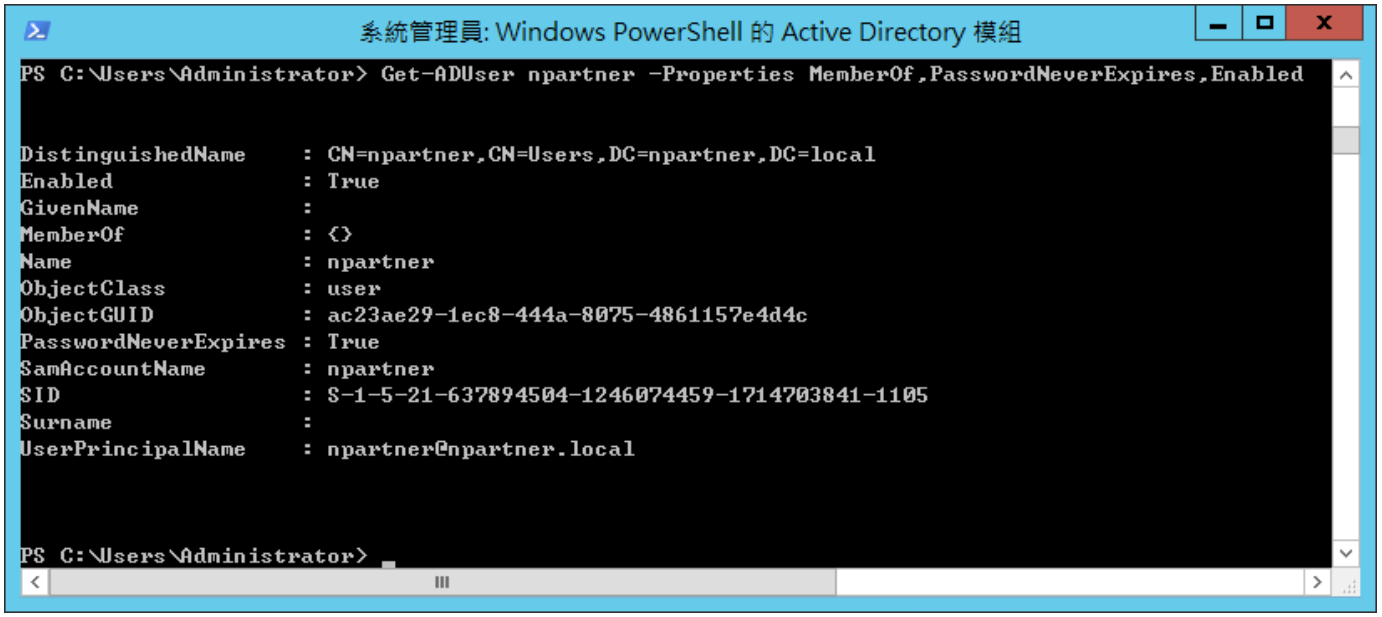
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

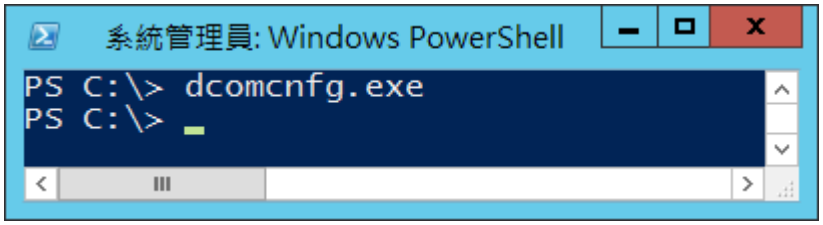


5.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

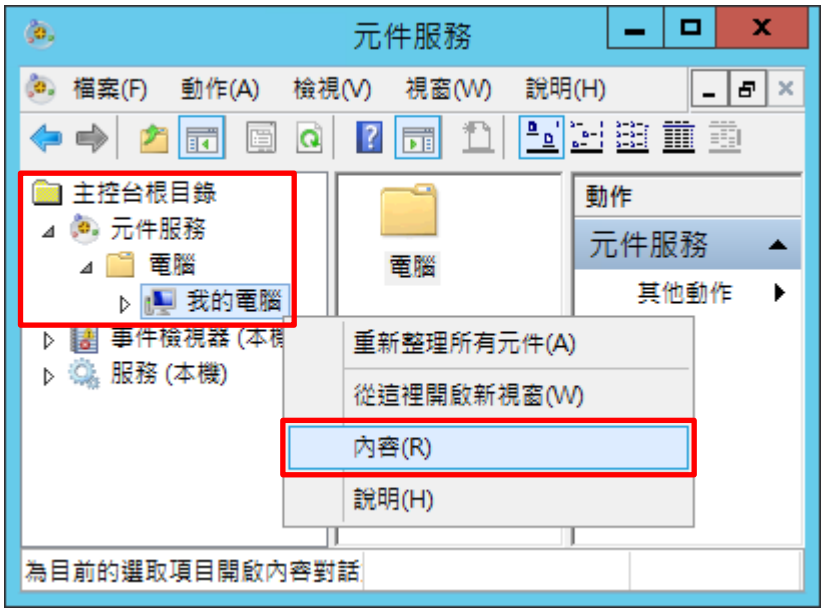
(2) 開啟元件服務

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



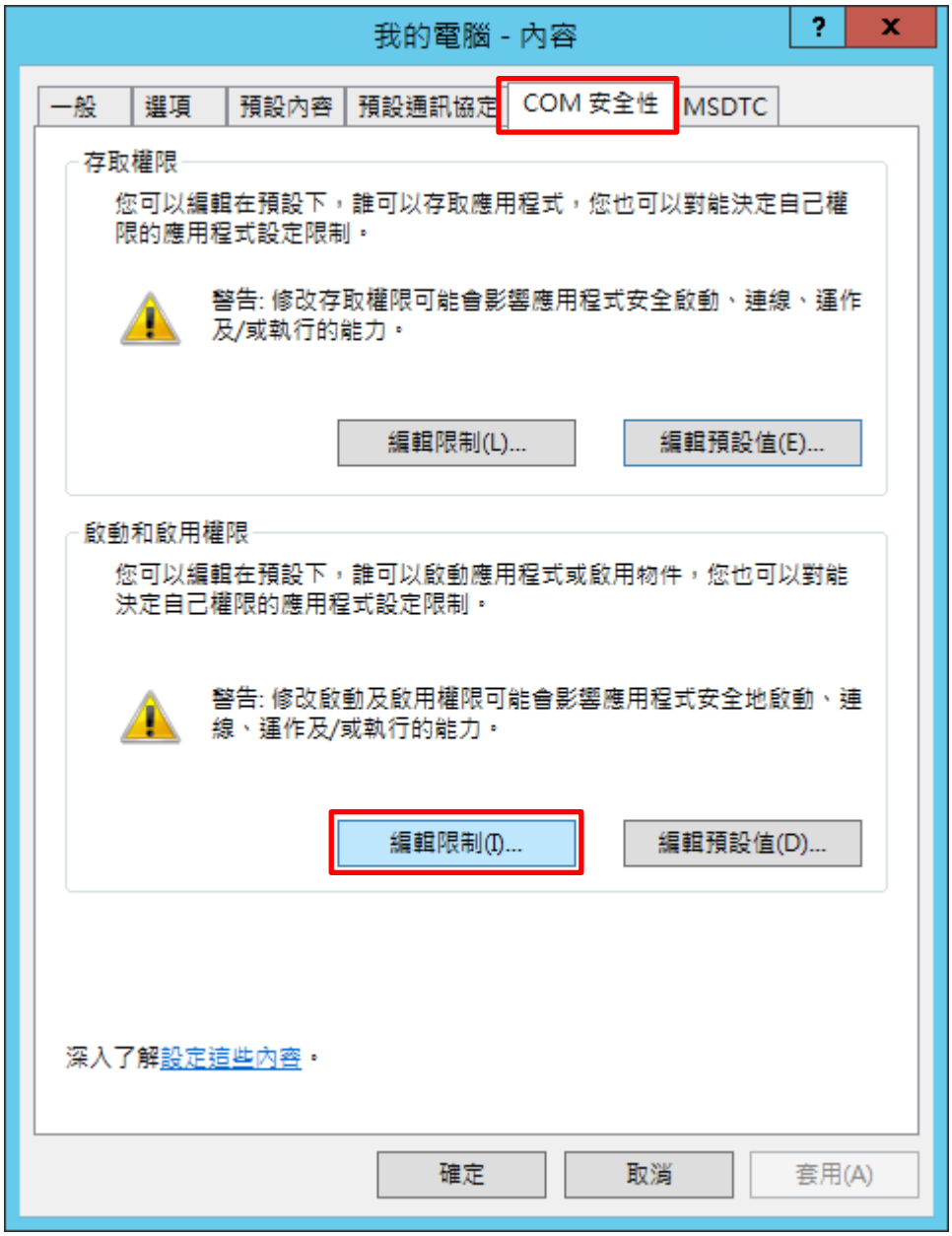
(3) 編輯電腦內容

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]



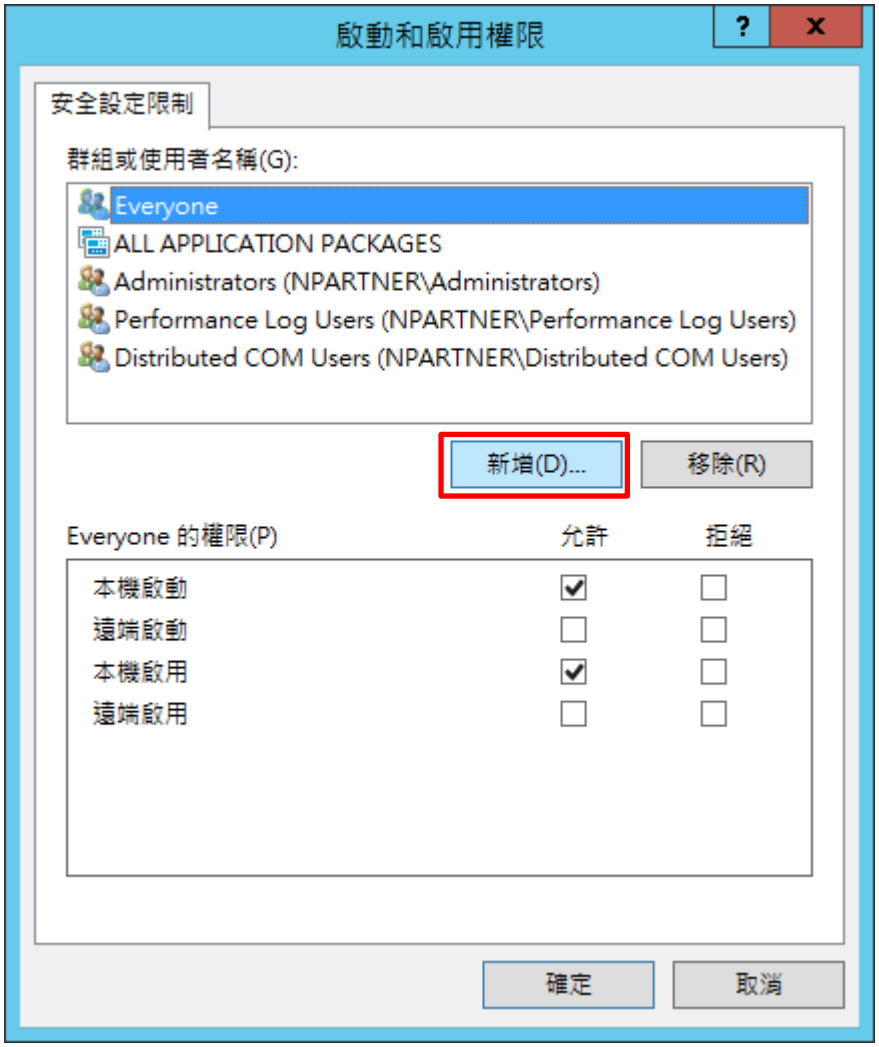
(4) 啟用權限

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]

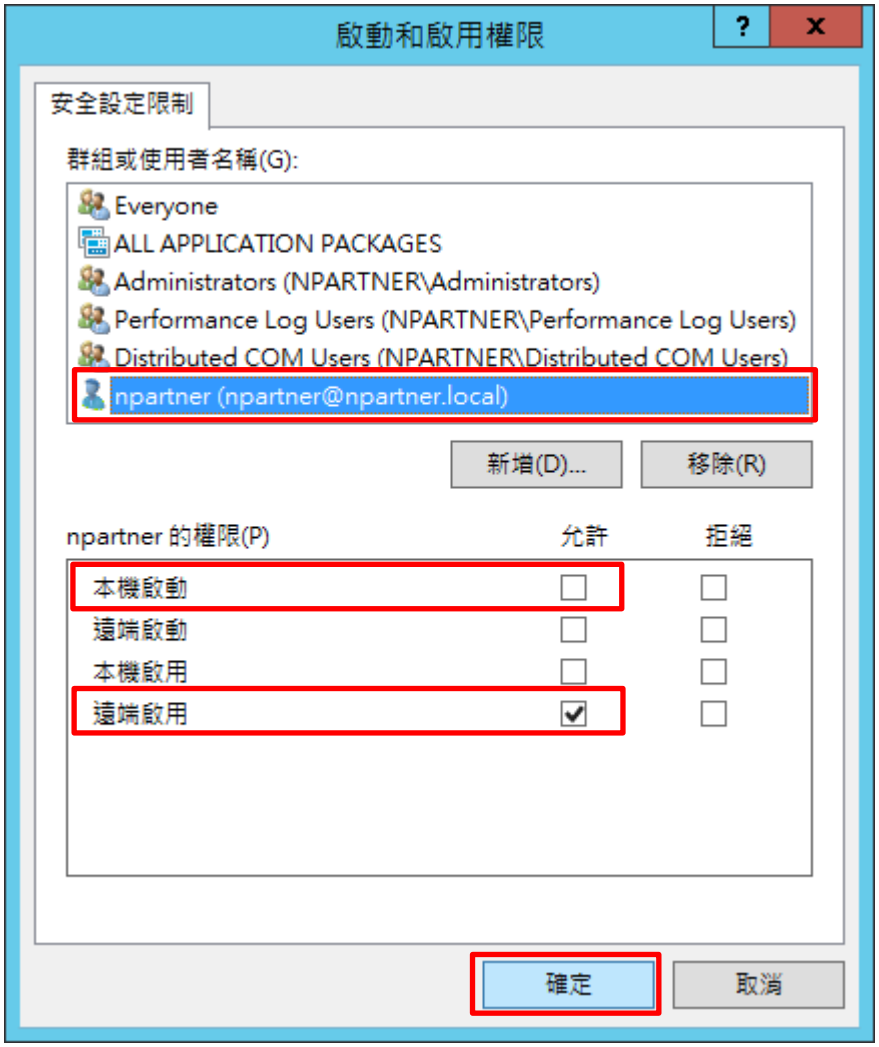


(6) 輸入使用者

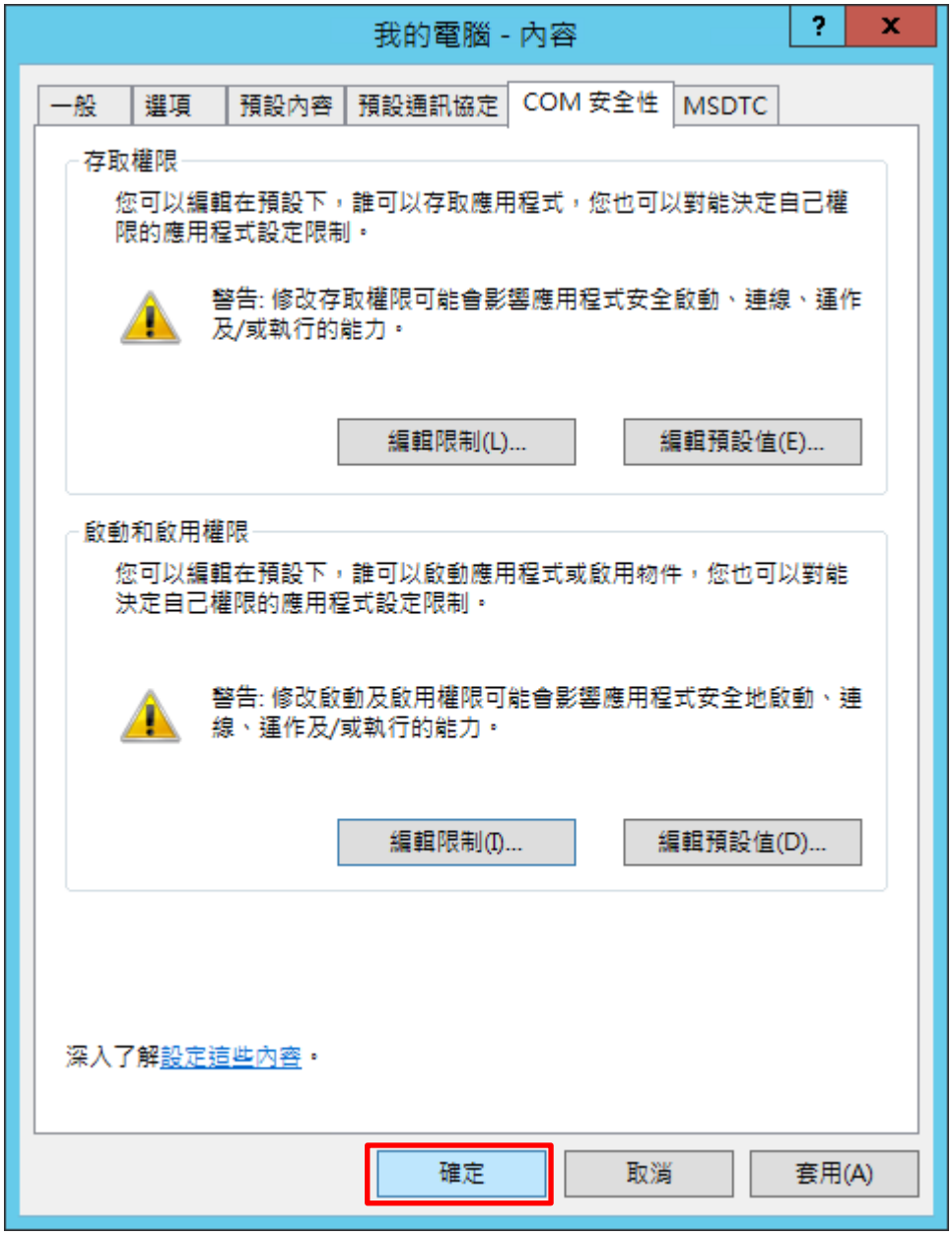
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]



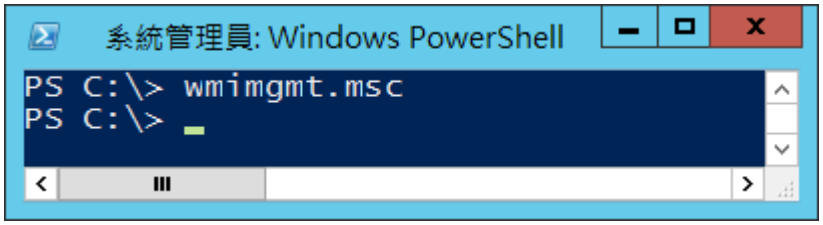
5.3.3 設定 WMI 權限

5.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]

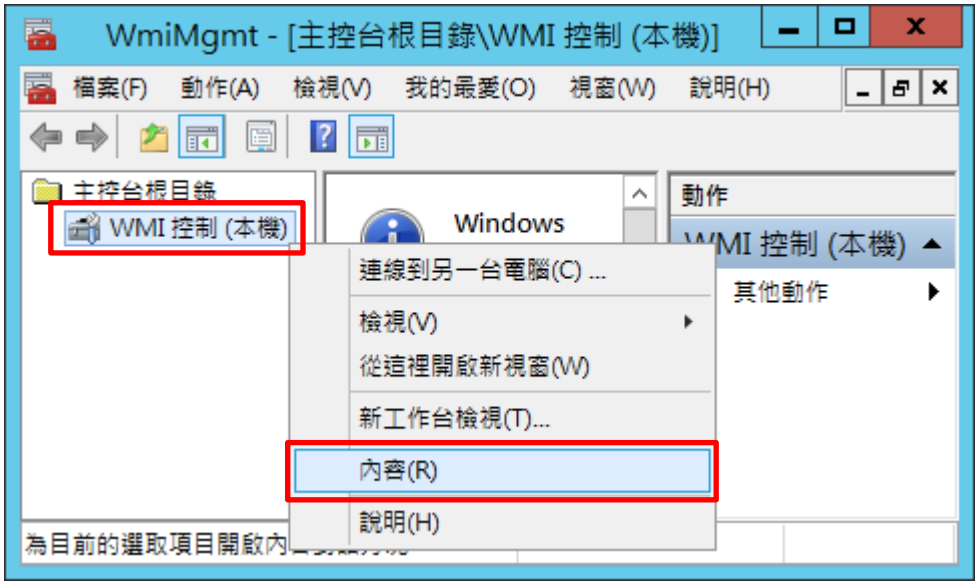
(2) 開啟元件服務

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



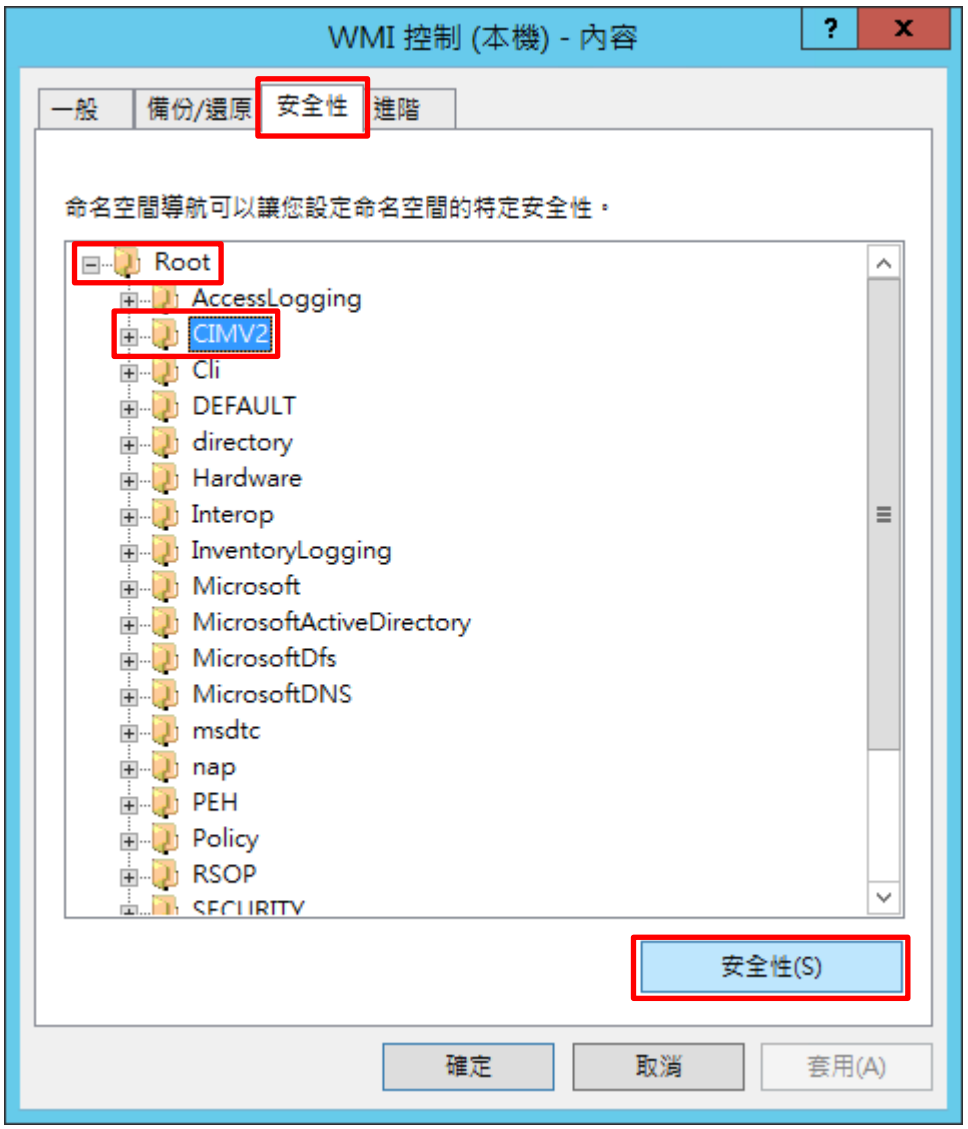
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



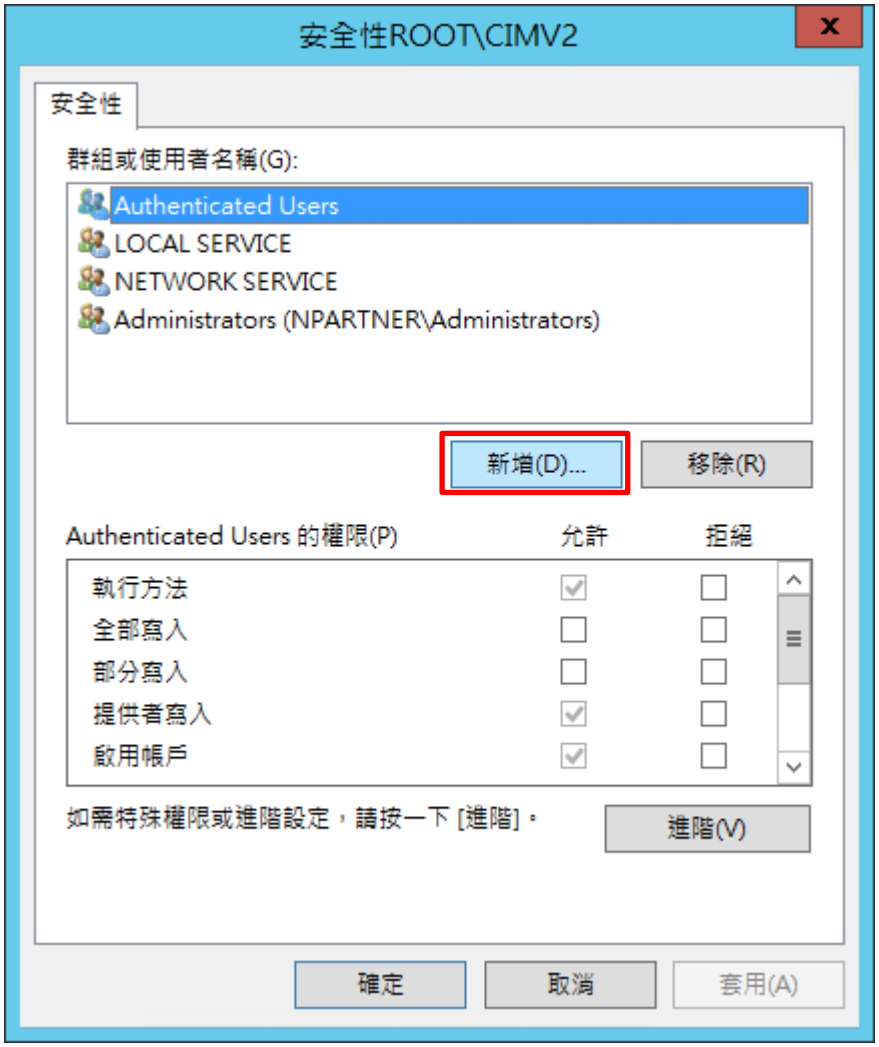
(4) 編輯 CIMV2 安全性

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]

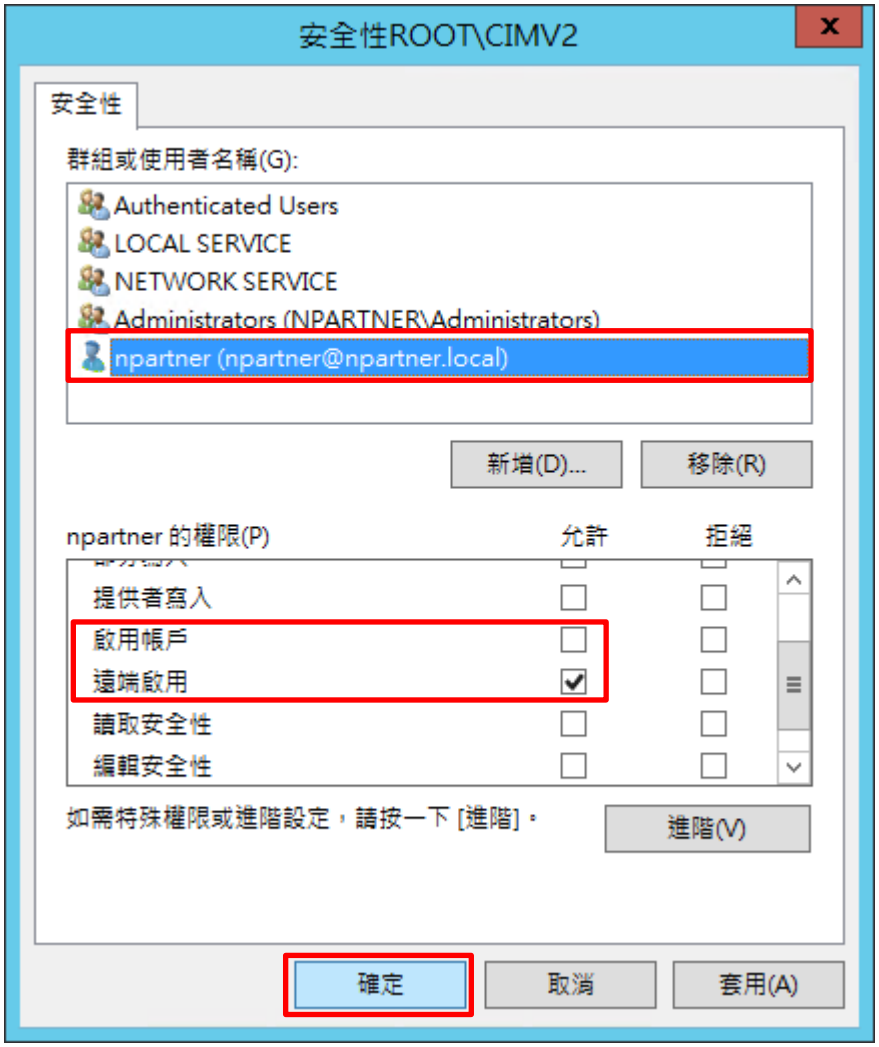


(6) 輸入使用者

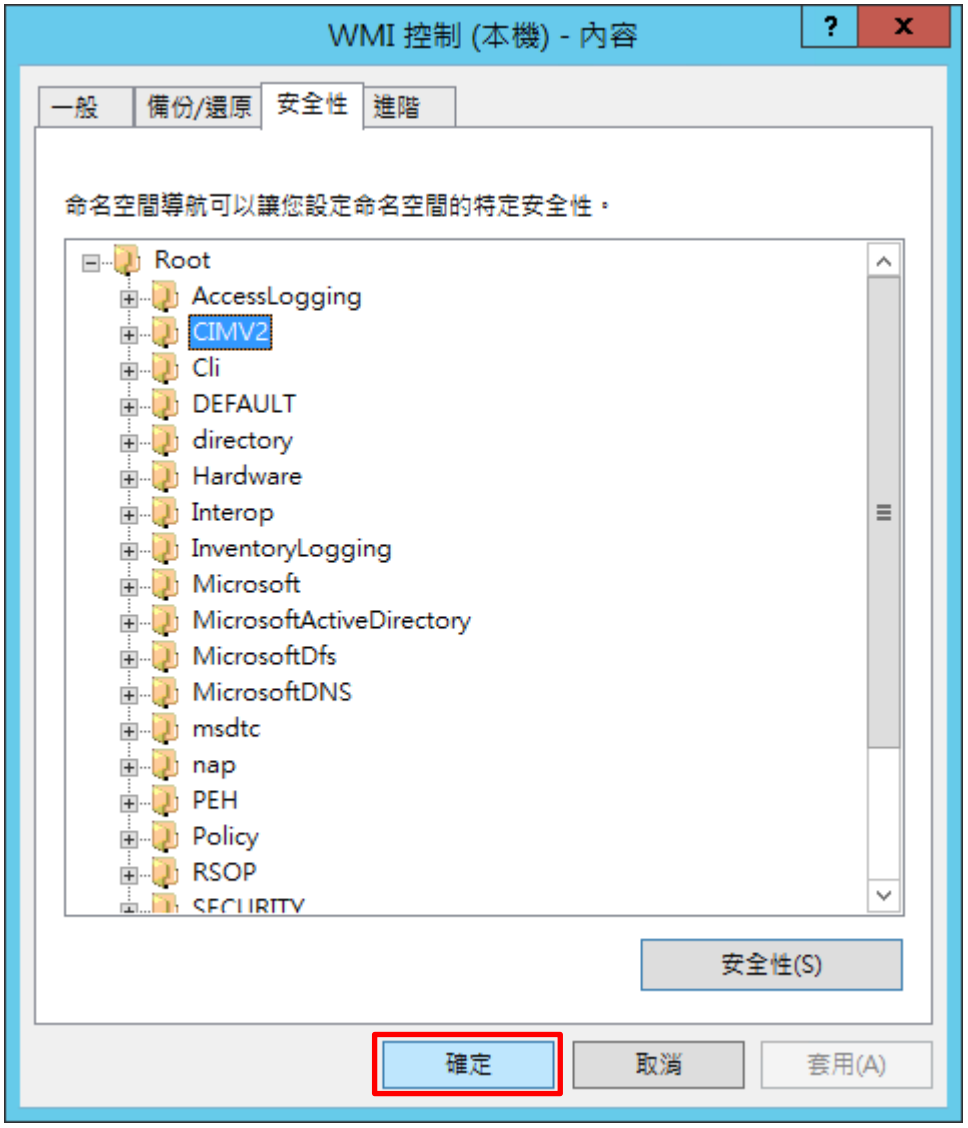
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]

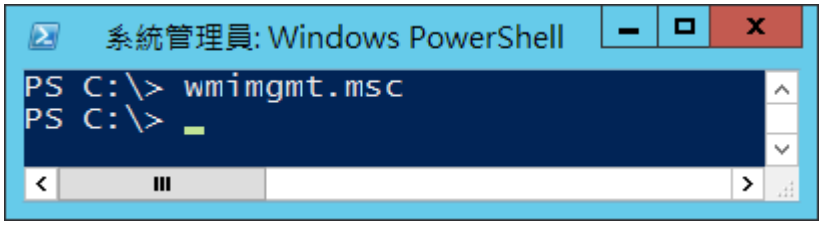


5.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

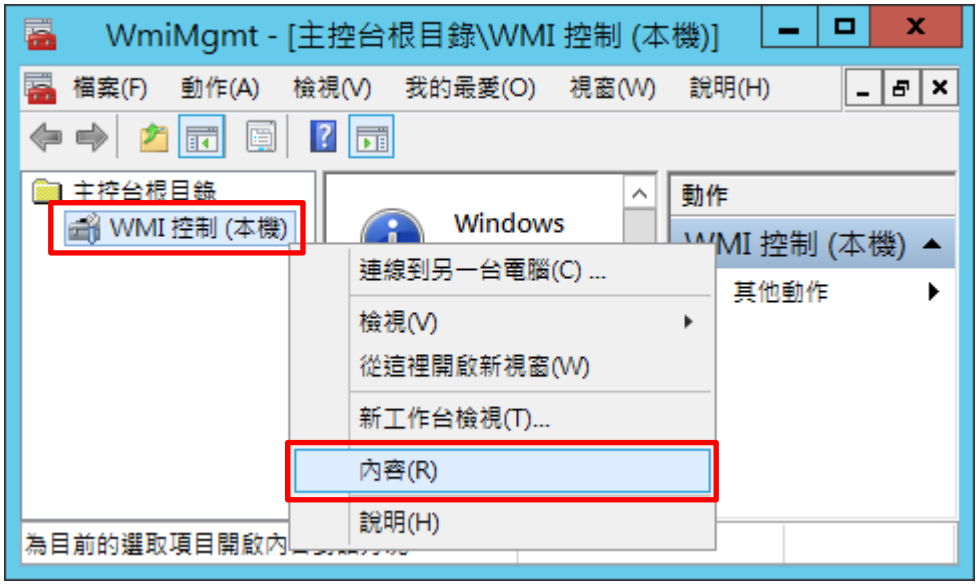
(2) 開啟元件服務

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



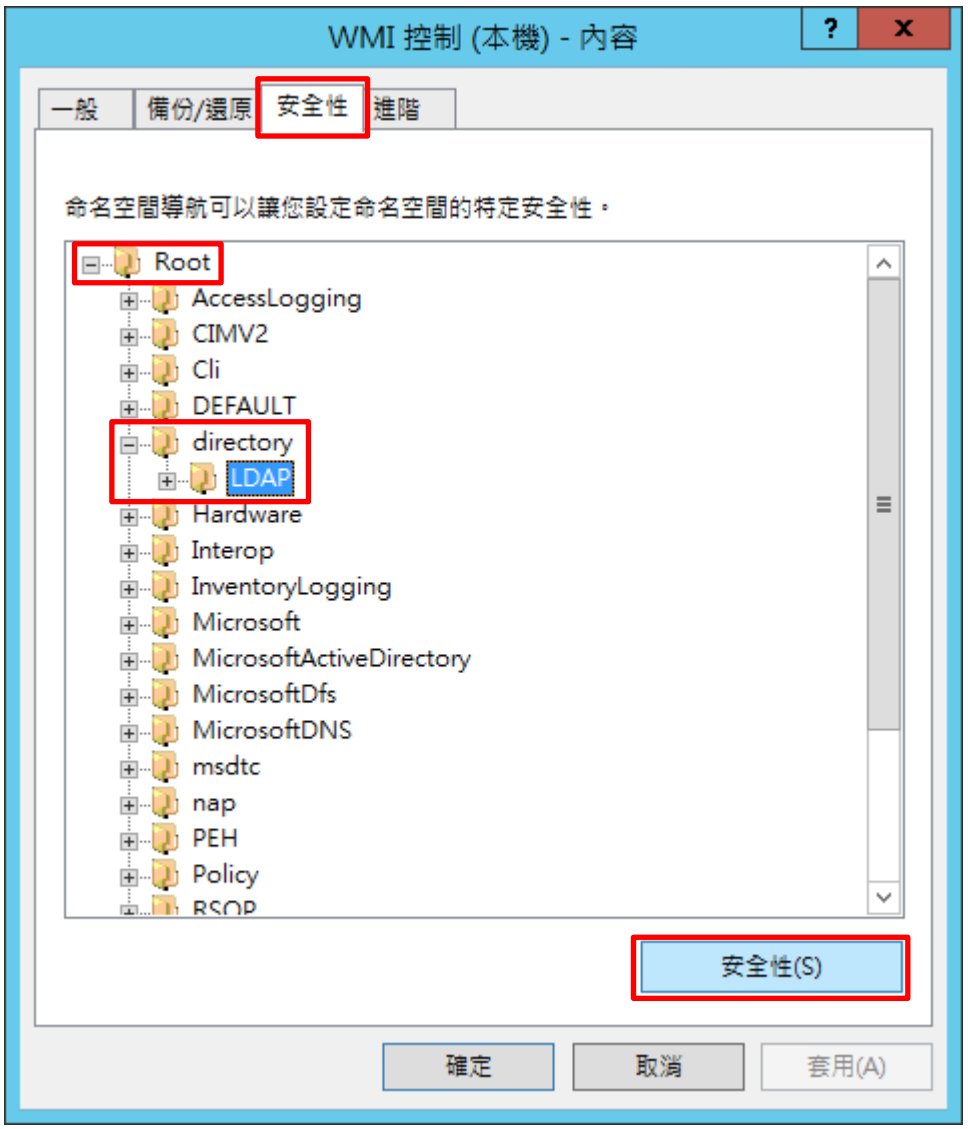
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



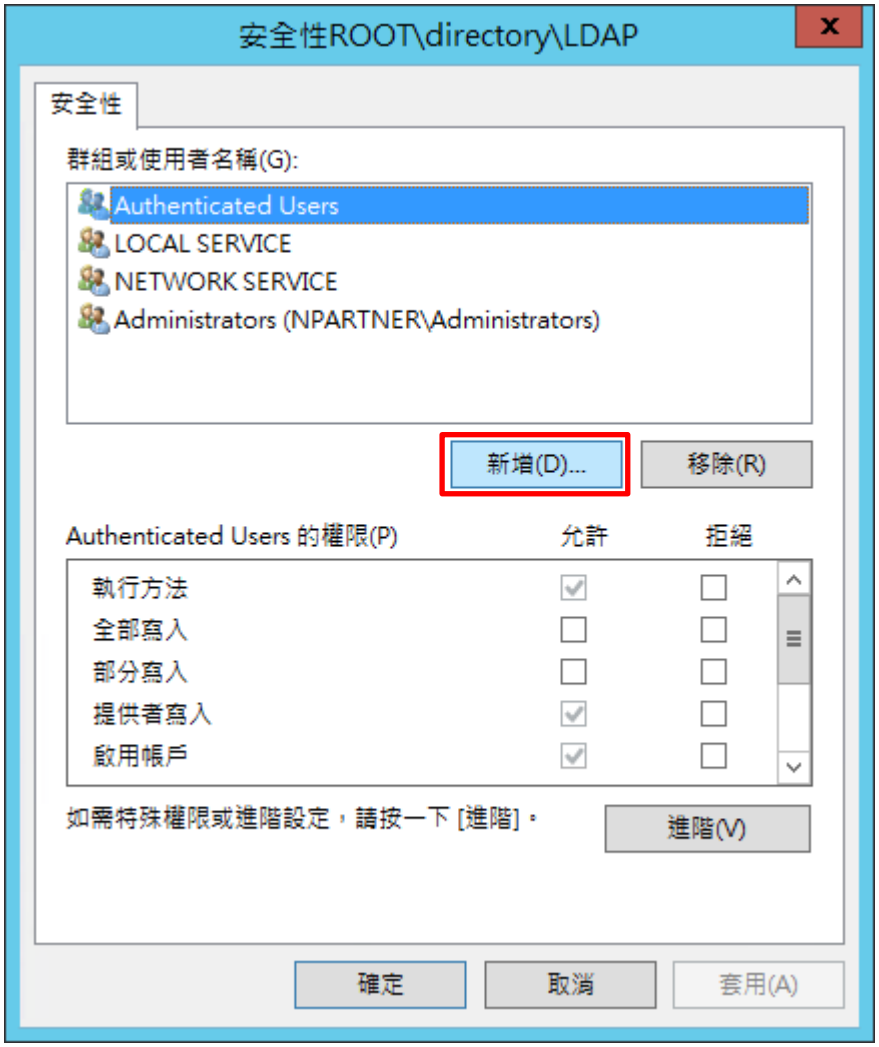
(4) 編輯 LDAP 安全性

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]

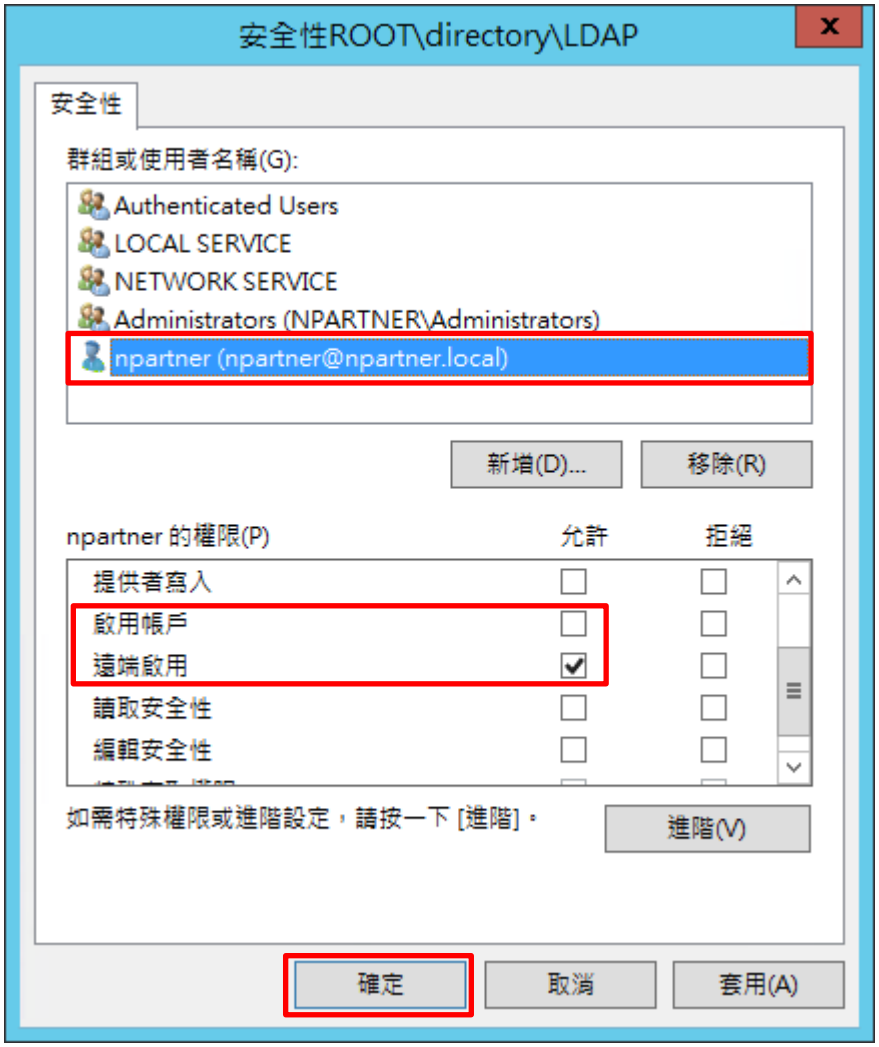


(6) 輸入使用者

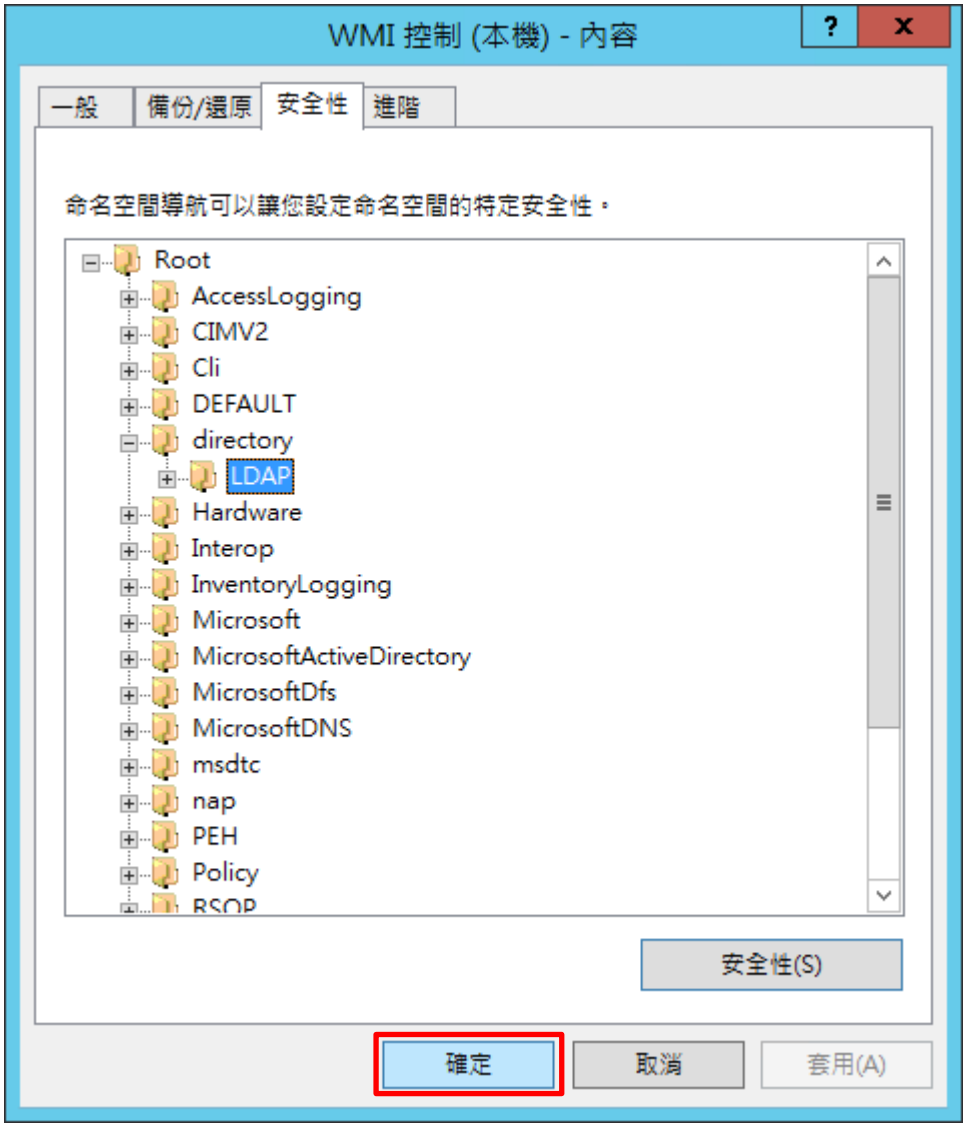
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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]



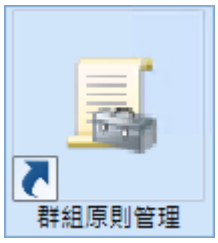
(8) 按 [確定]



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]

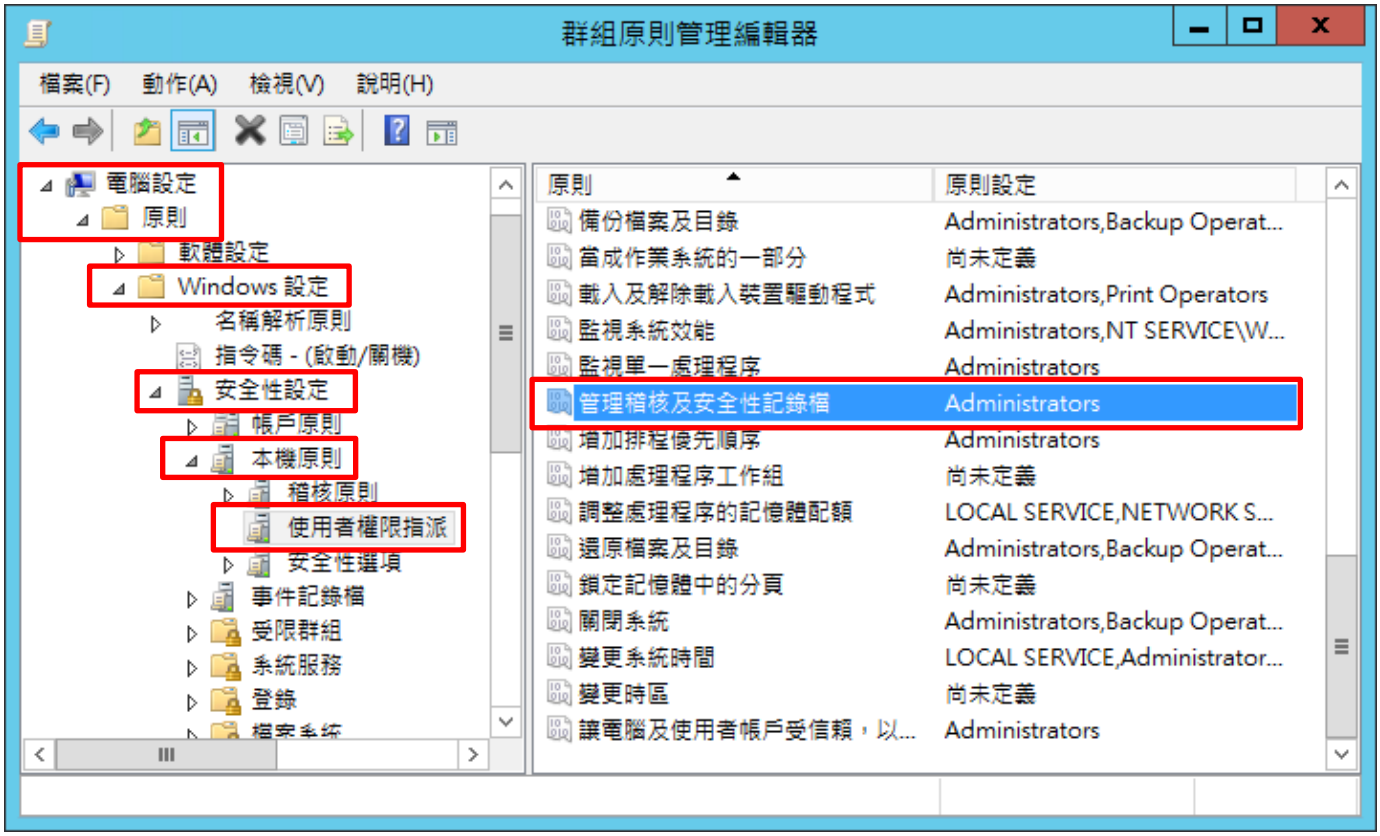


(2) 編輯群組原則物件

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

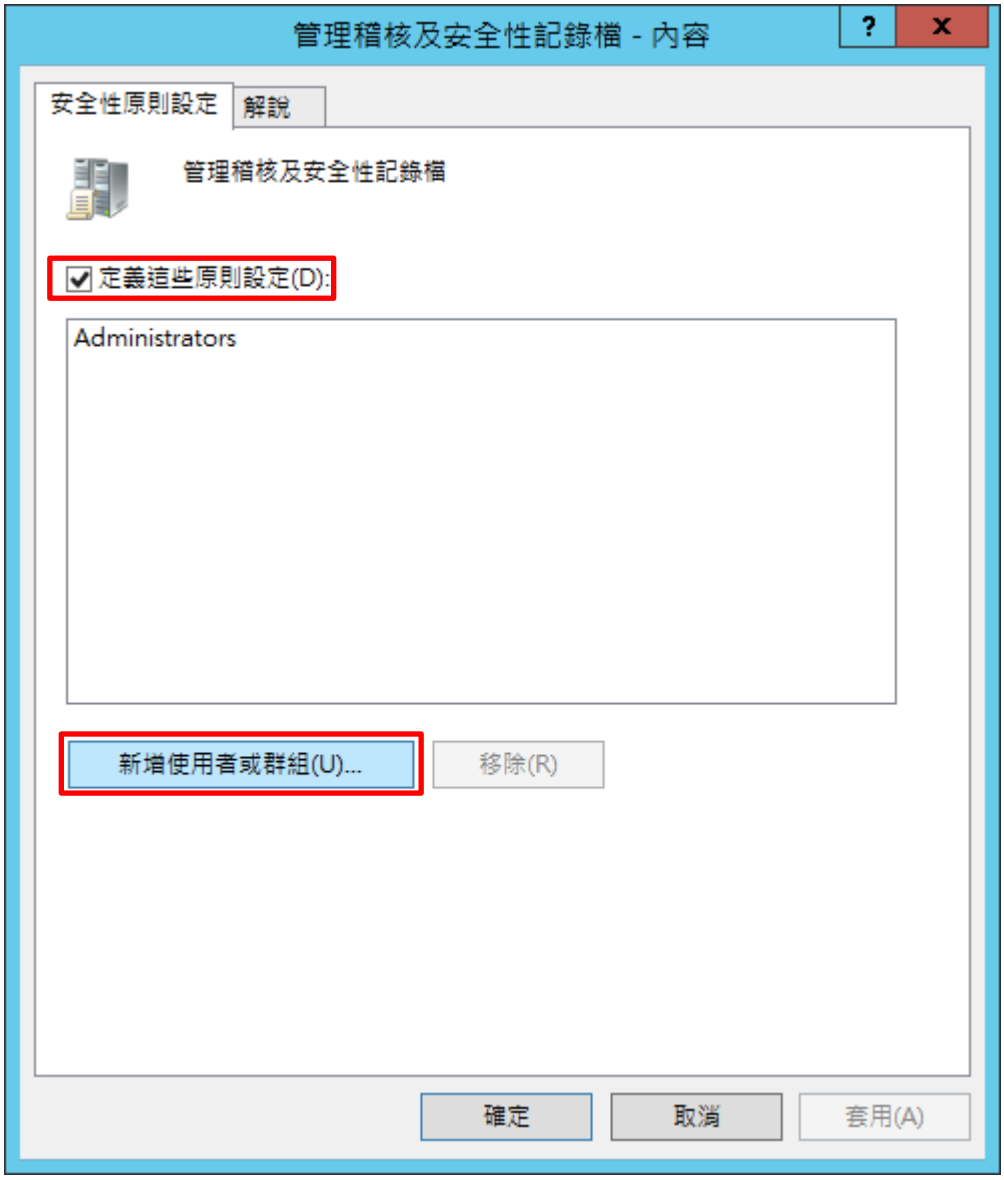
(3) 設定記錄檔

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



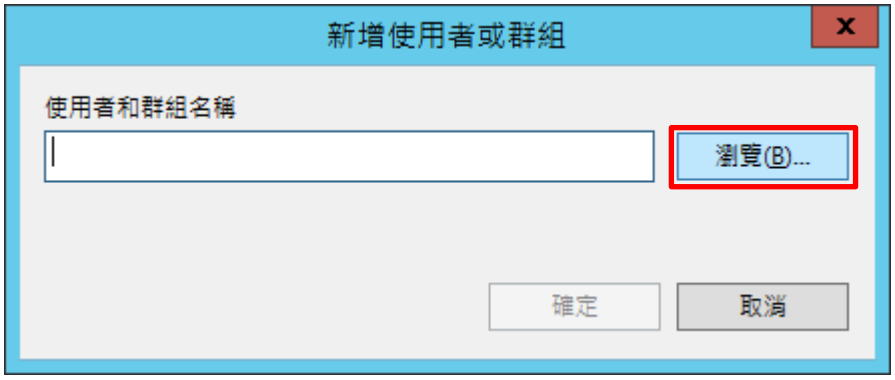
(4) 新增管理稽核使用者

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

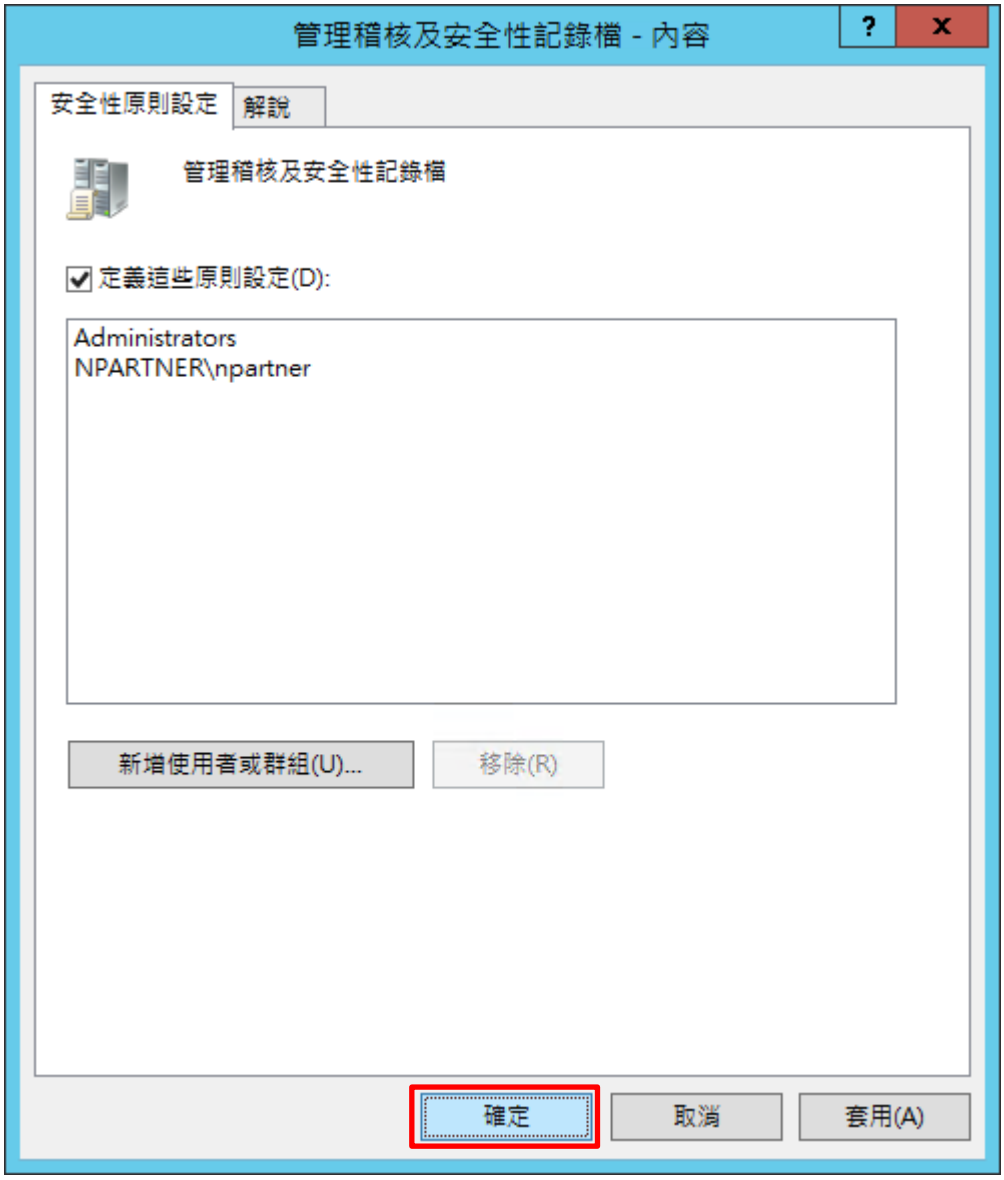
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(7) 確定使用者

按 [確定]

(8) 確定設定記錄檔

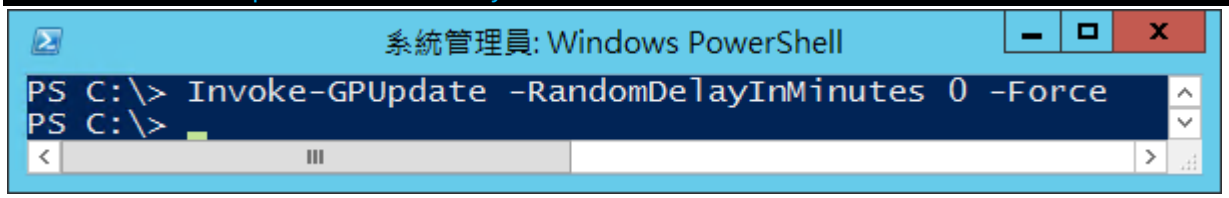
按 [確定]



(9) 開啟 [Windows PowerShell]

(10) 更新群組原則

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

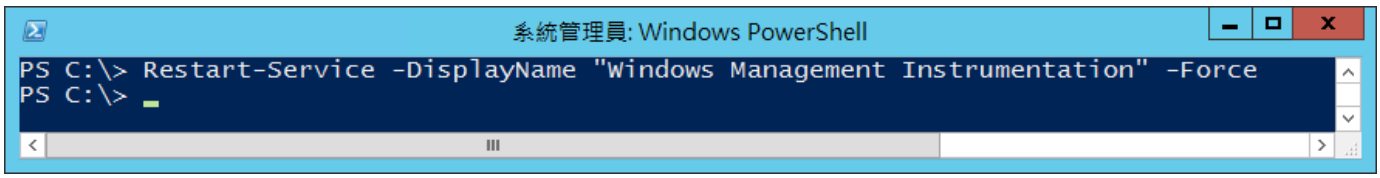


5.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

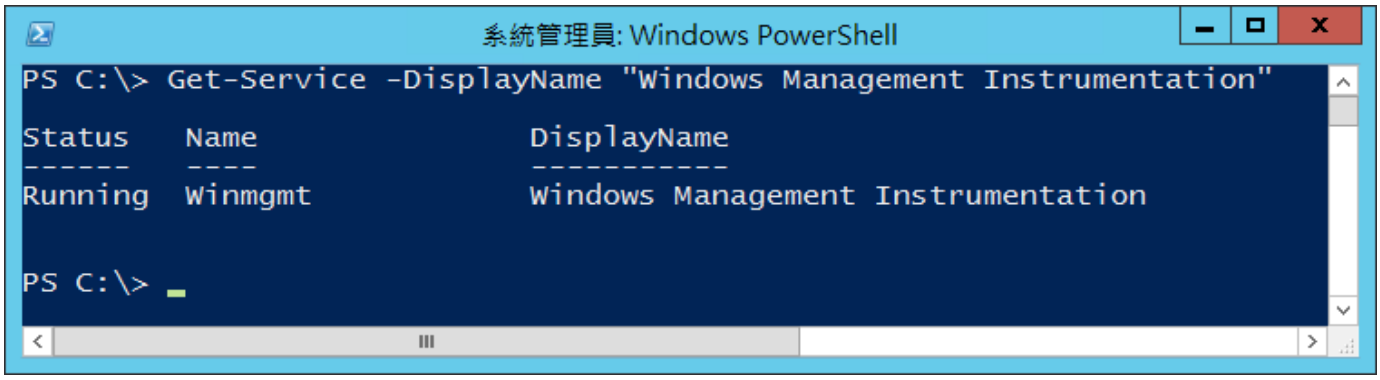
(2) 重啟 WMI 服務

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



(3) 查看 WMI 服務

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

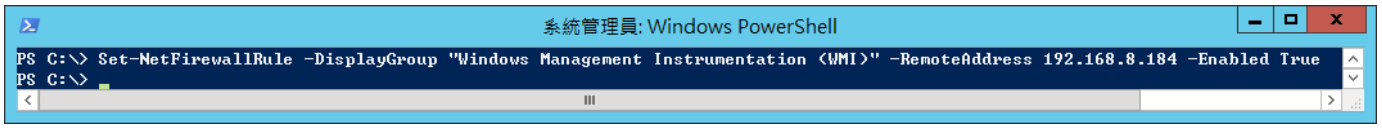


5.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]

(2) 設定防火牆，只允許 N-Reporter IP query WMI

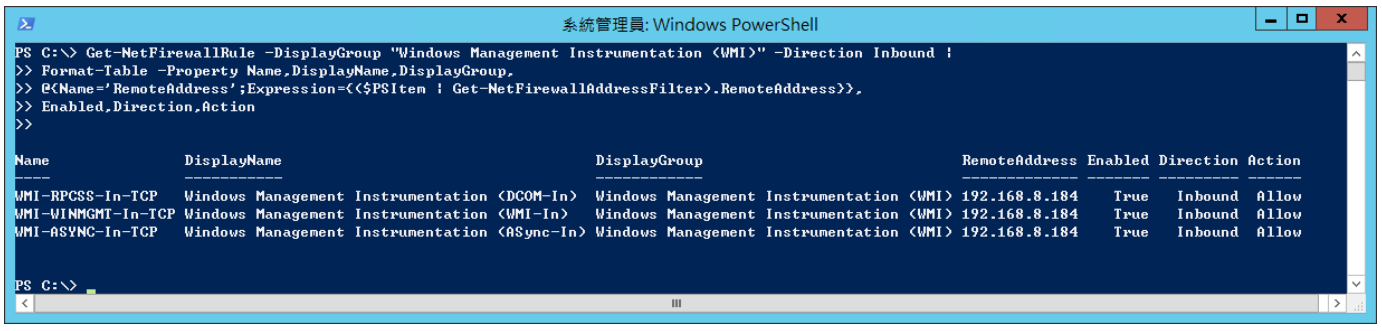
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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
```



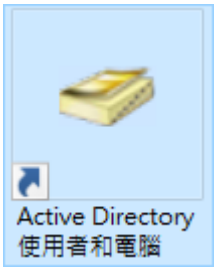
6. Windows 2016

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

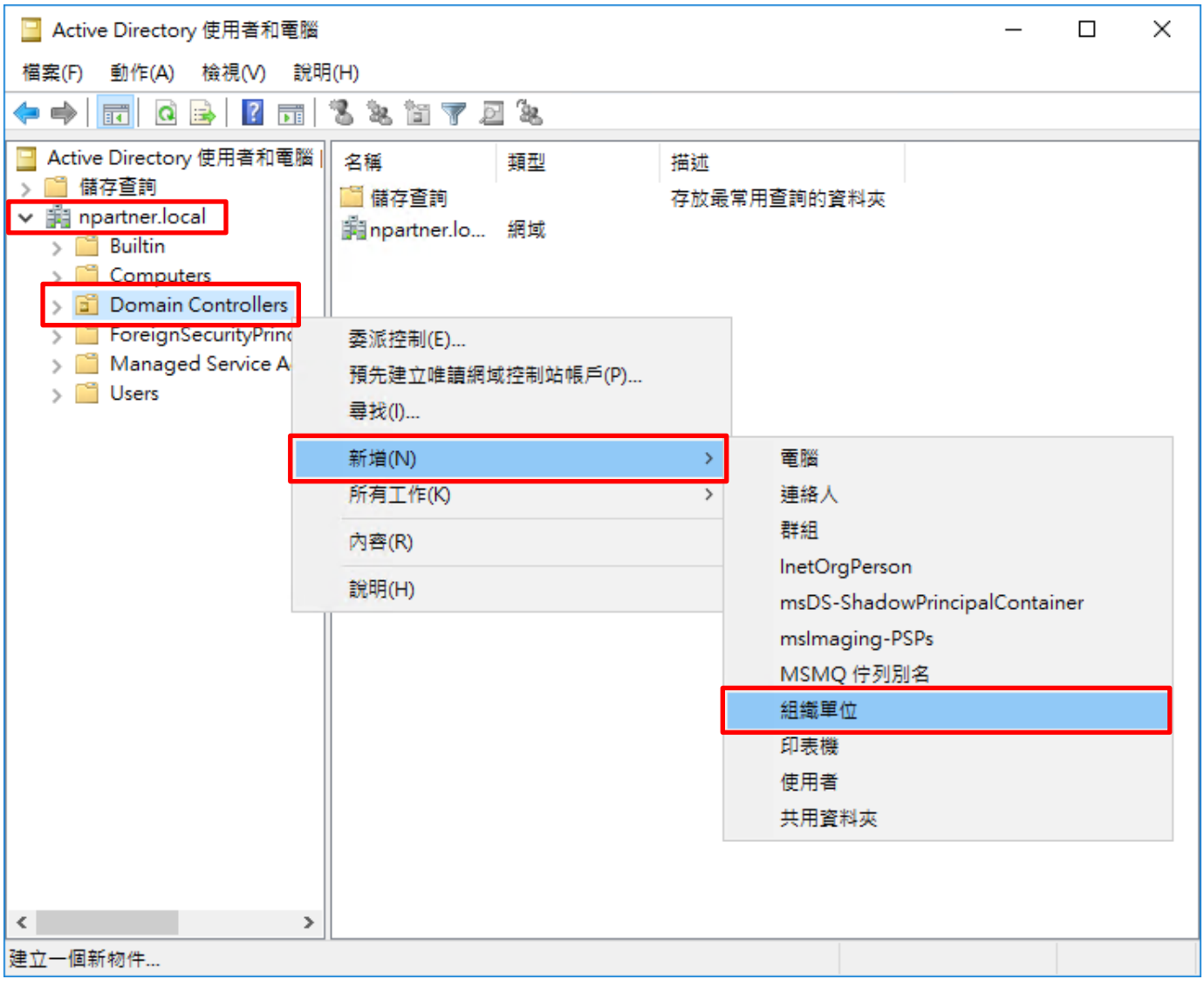
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



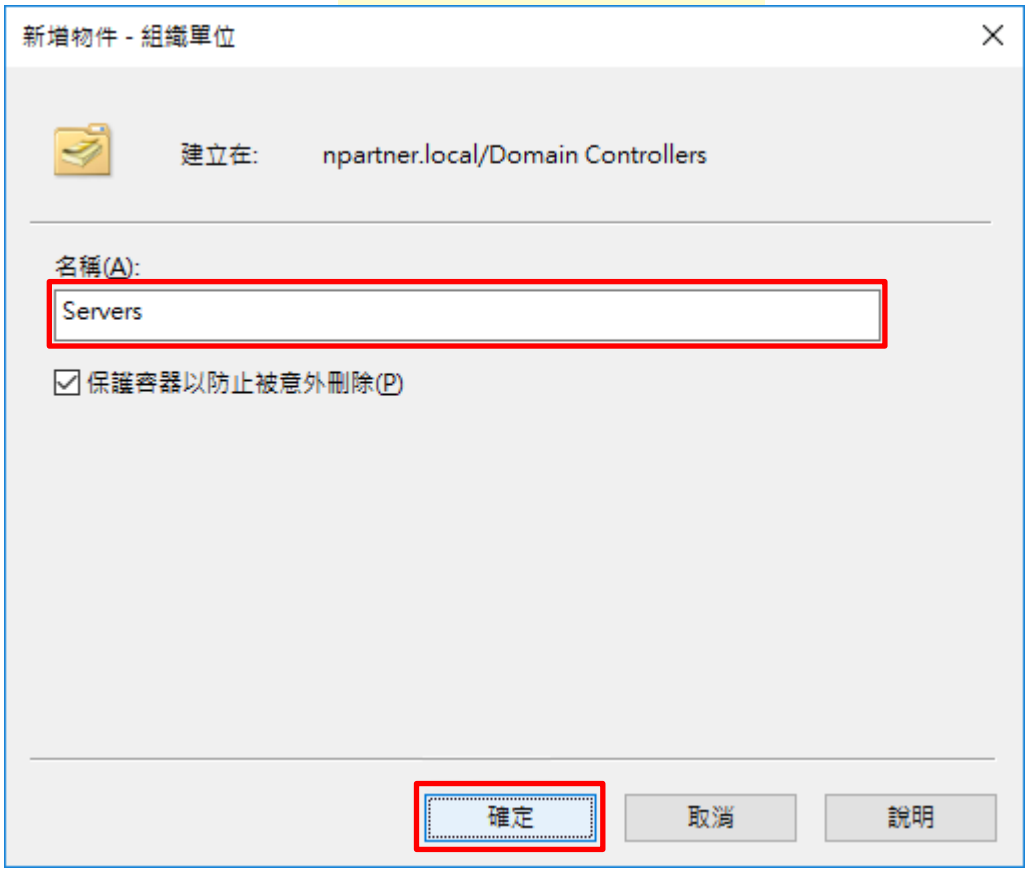
(2) 新增組織單位

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]



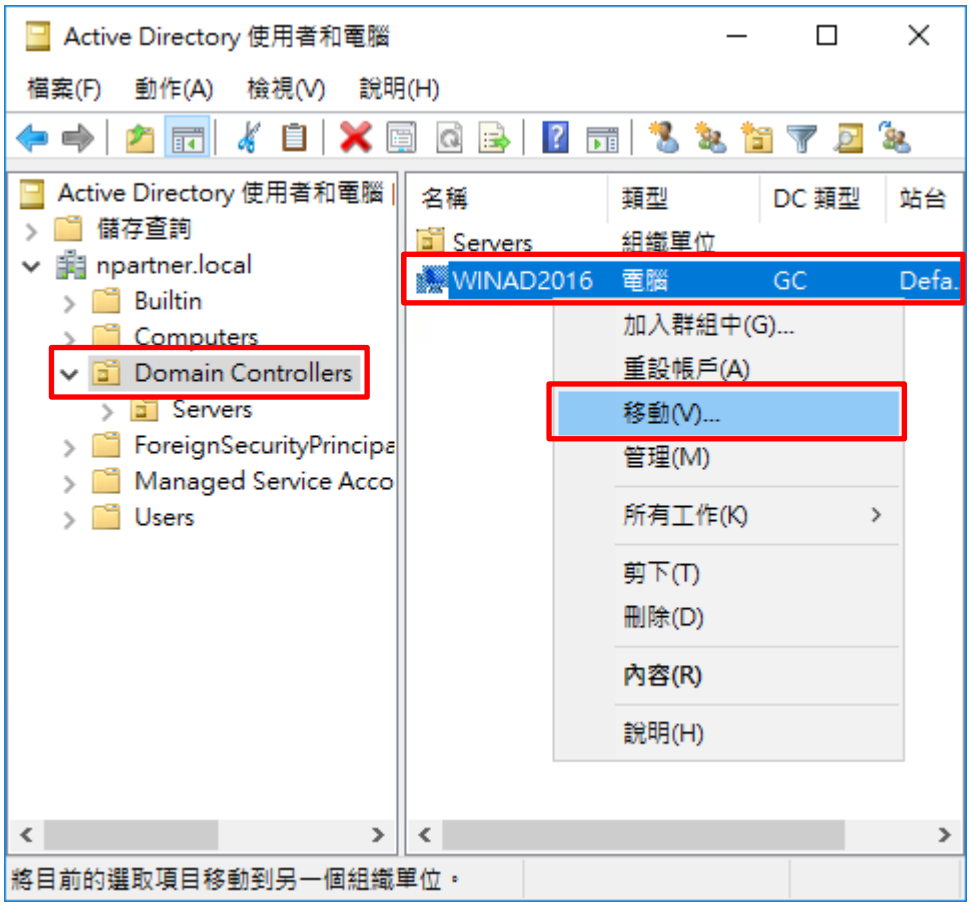
(3) 輸入組織單位名稱

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]



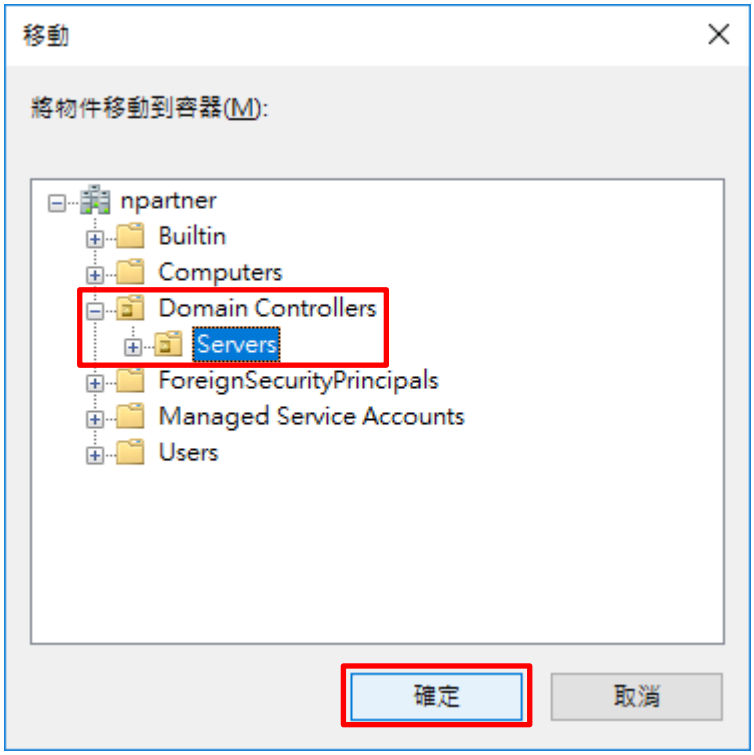
(4) 移動伺服器至新的組織單位

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]



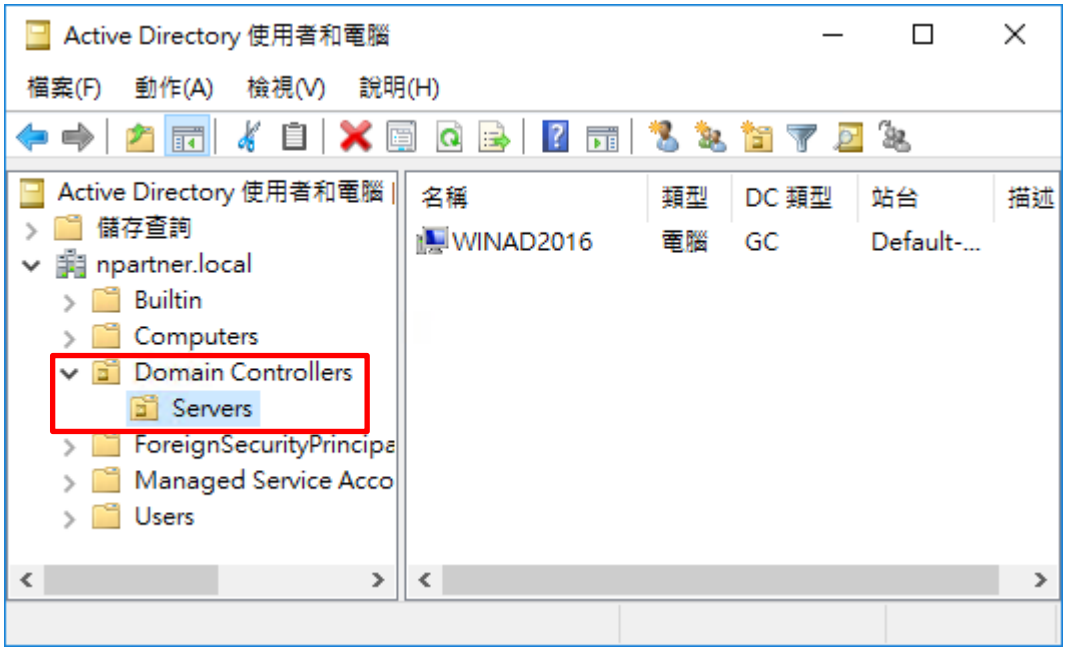
(5) 選擇組織單位

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

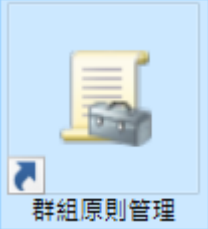
點選 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2016] 網域伺服器已移動。



6.2 群組原則設定

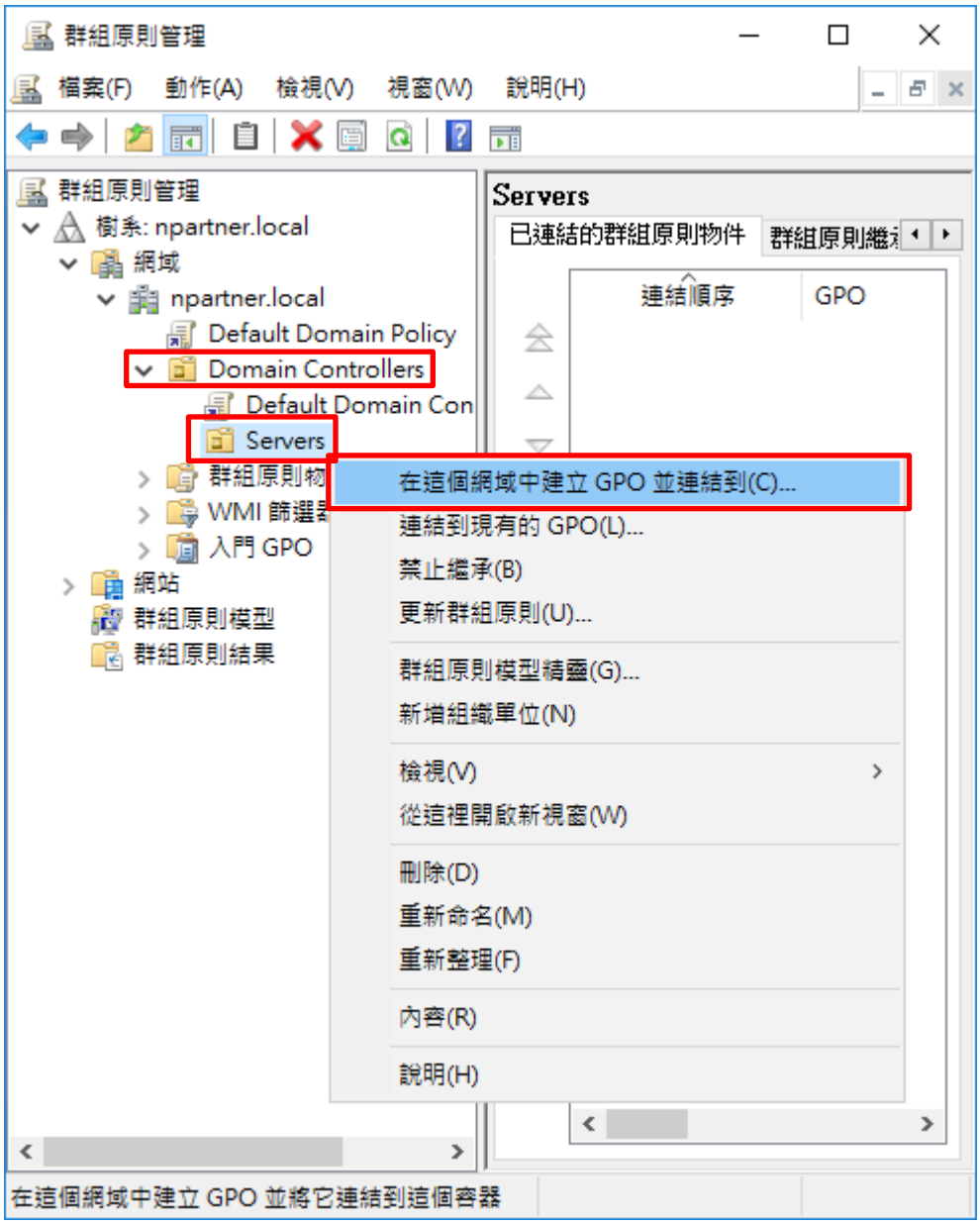
(1) 開啟群組原則管理

開啟 [群組原則管理]



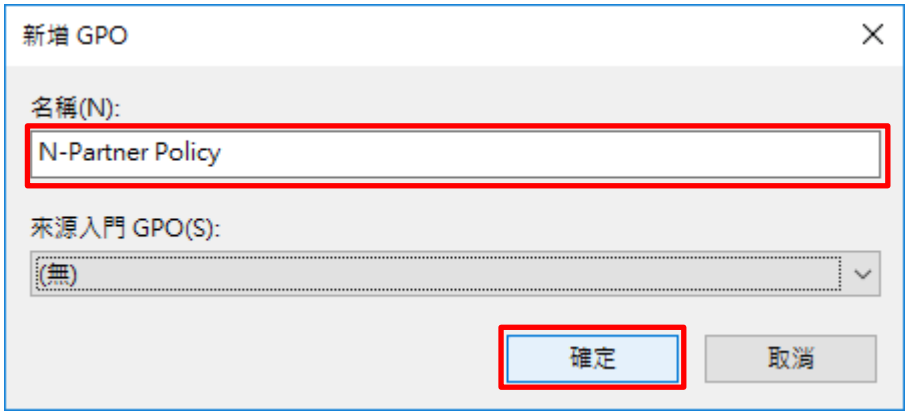
(2) 在 Servers 組織單位，新增群組原則物件

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...]



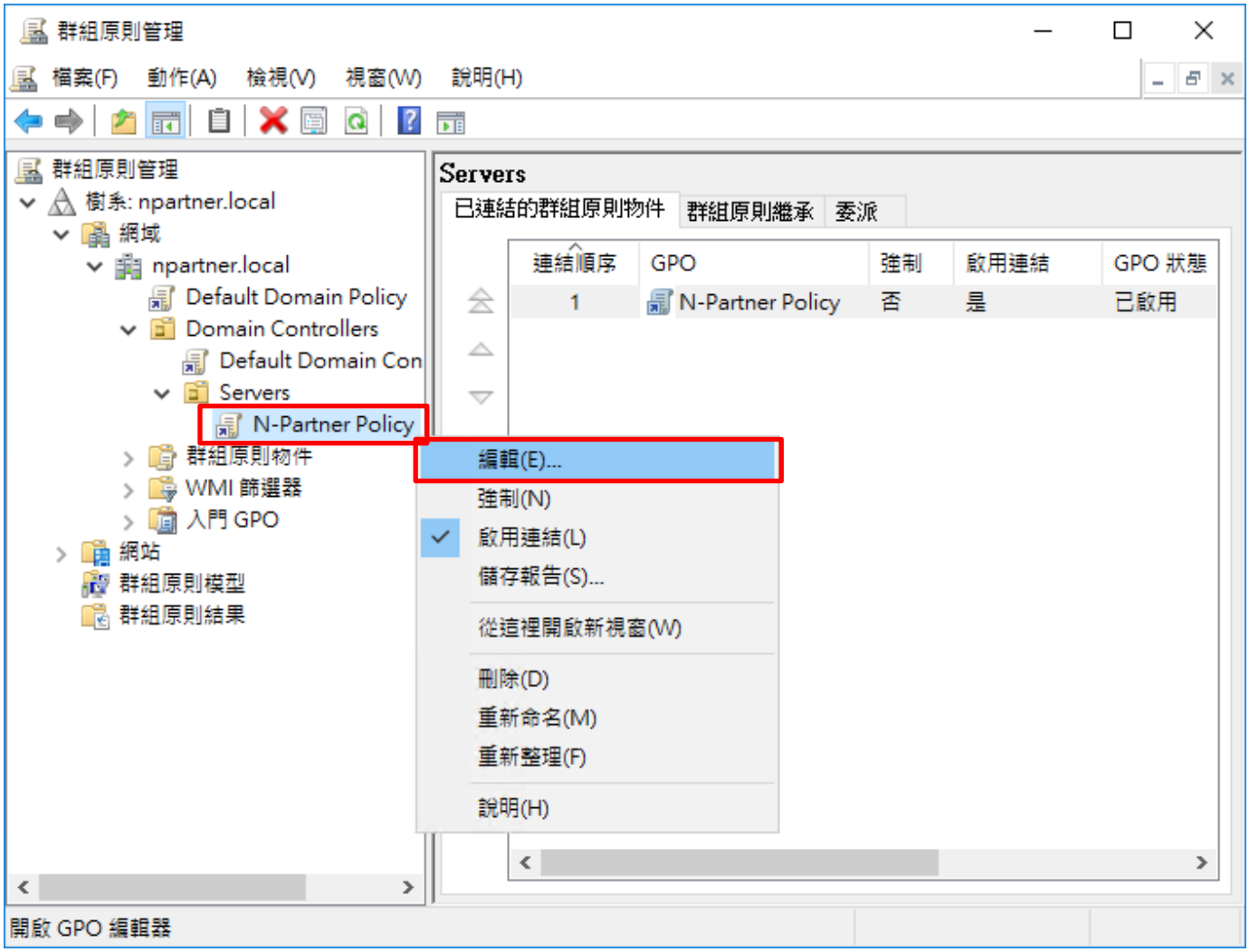
(3) 輸入群組原則物件名稱

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]



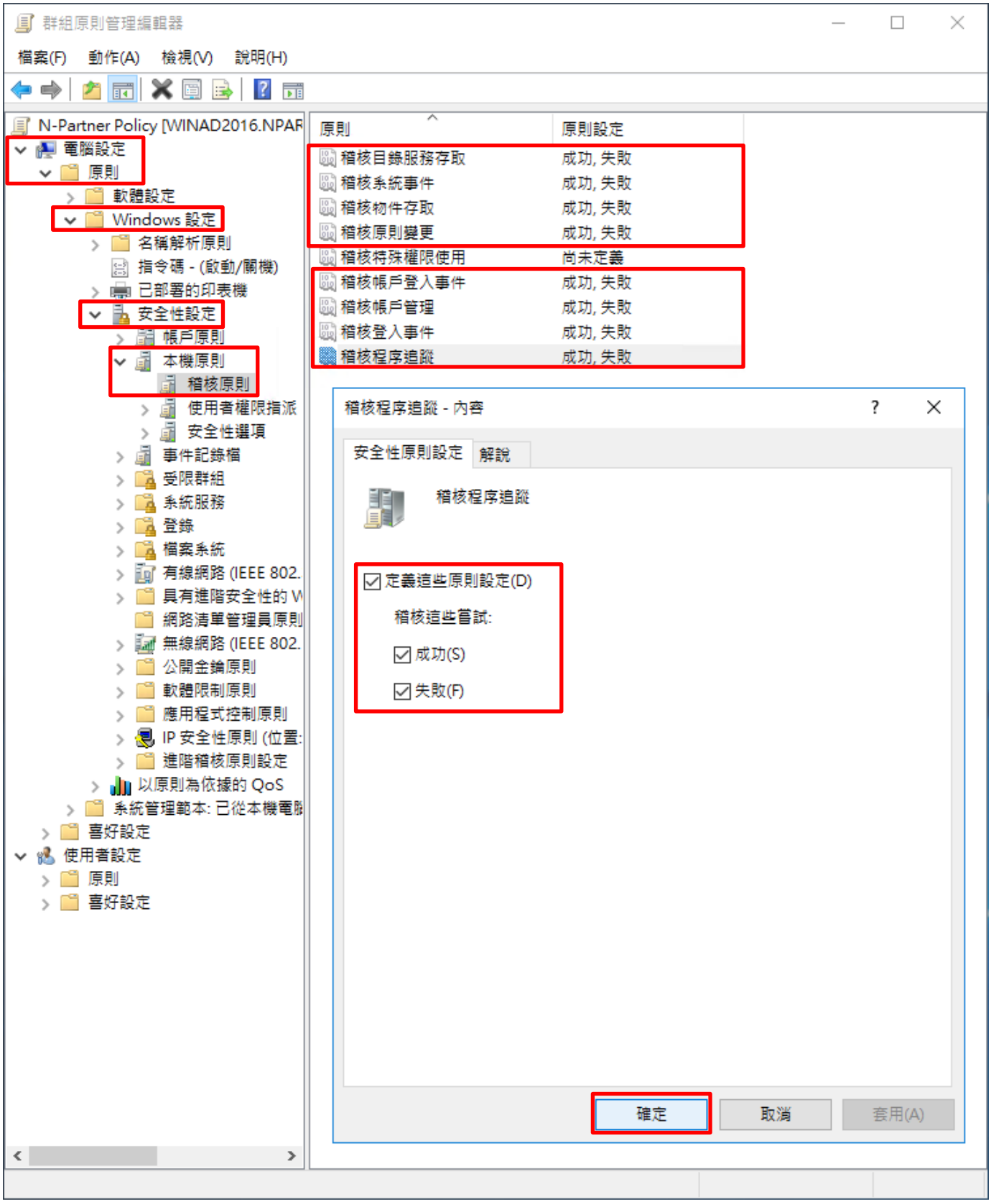
(4) 編輯群組原則物件

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



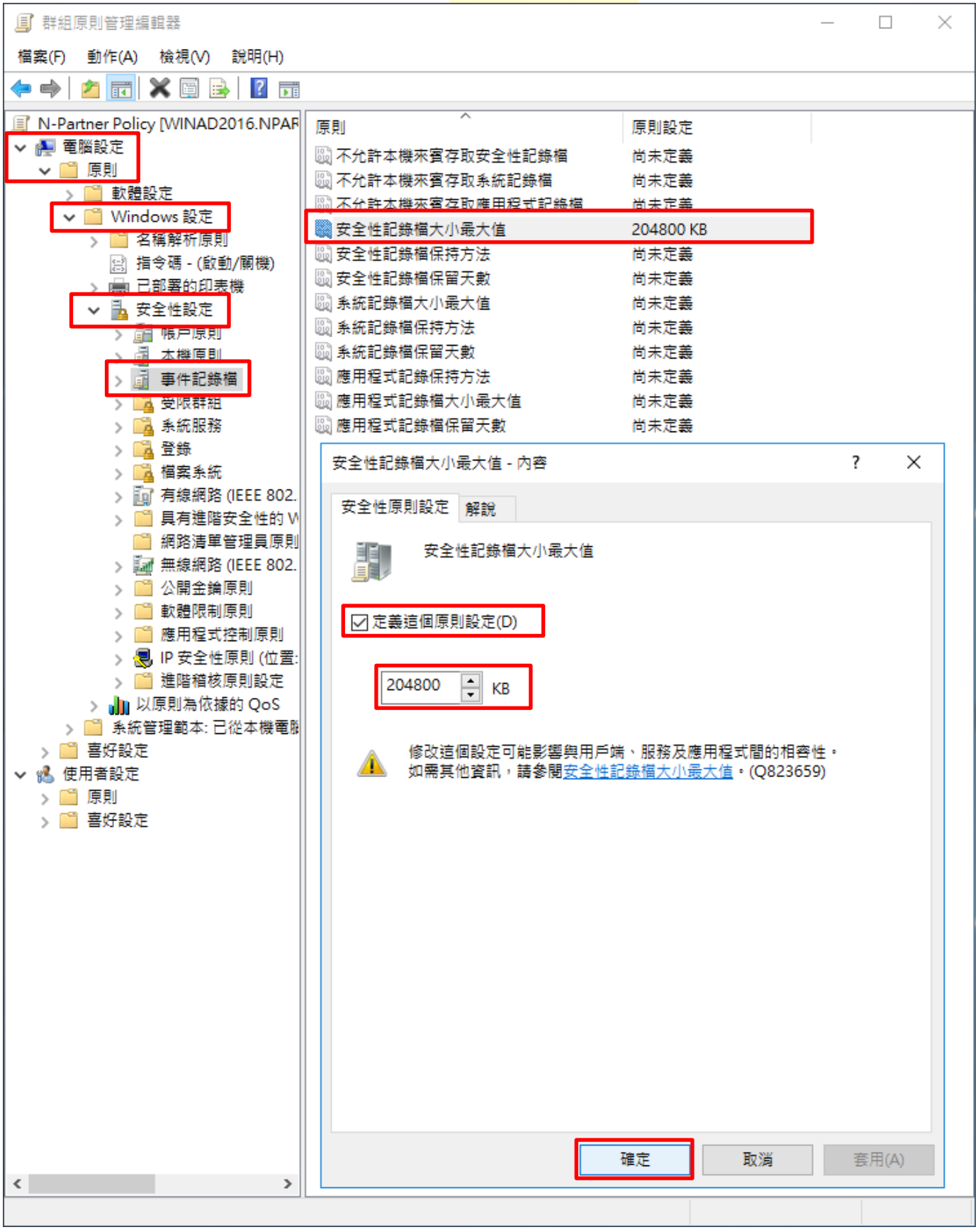
(5) 本機原則：稽核原則

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]



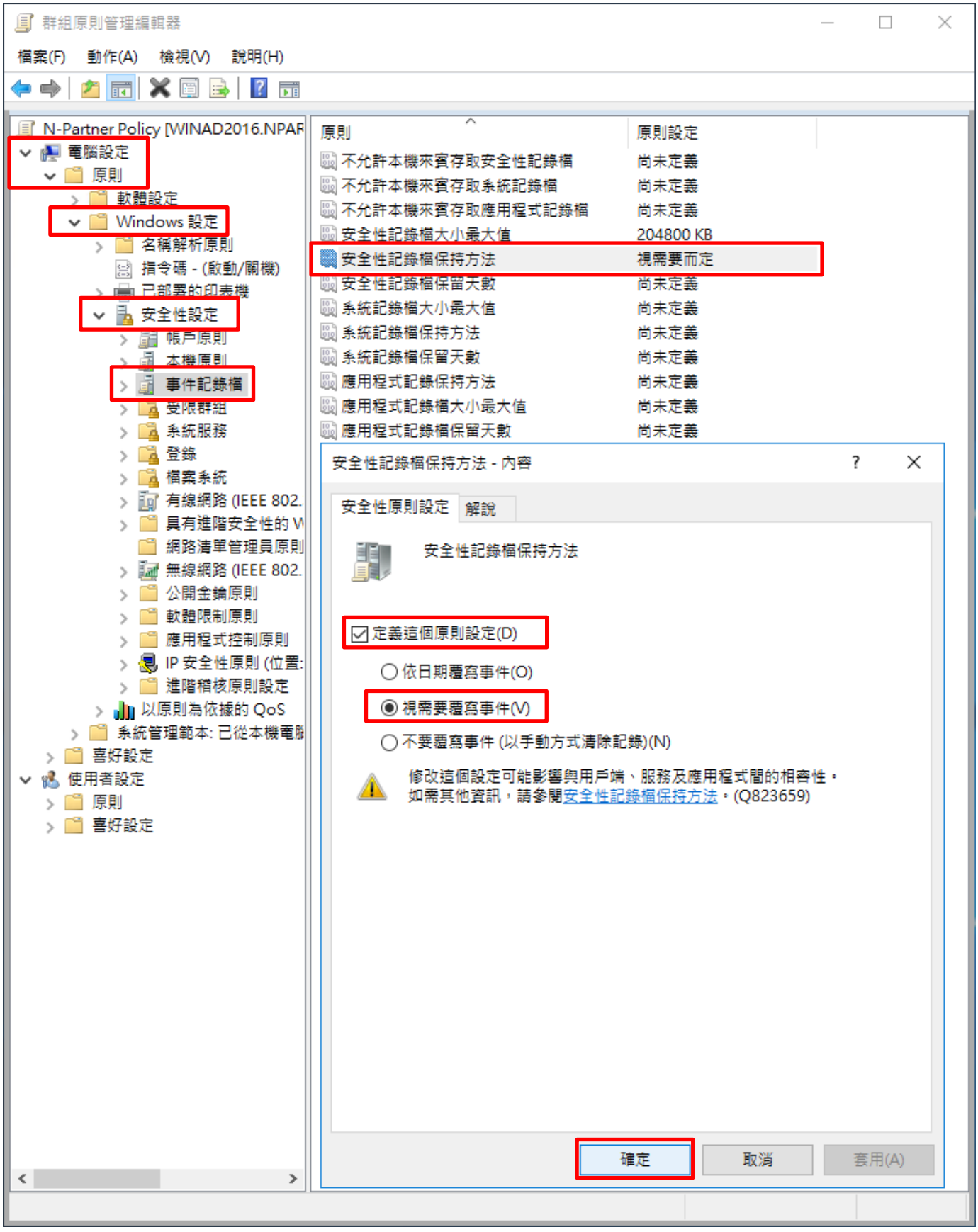
(6) 事件記錄檔：安全性記錄檔大小最大值

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]

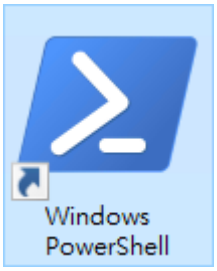


(7) 事件記錄檔：安全性記錄檔保持方法

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]

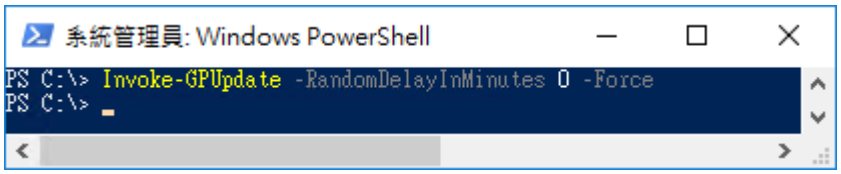


(8) 開啟 [Windows PowerShell]



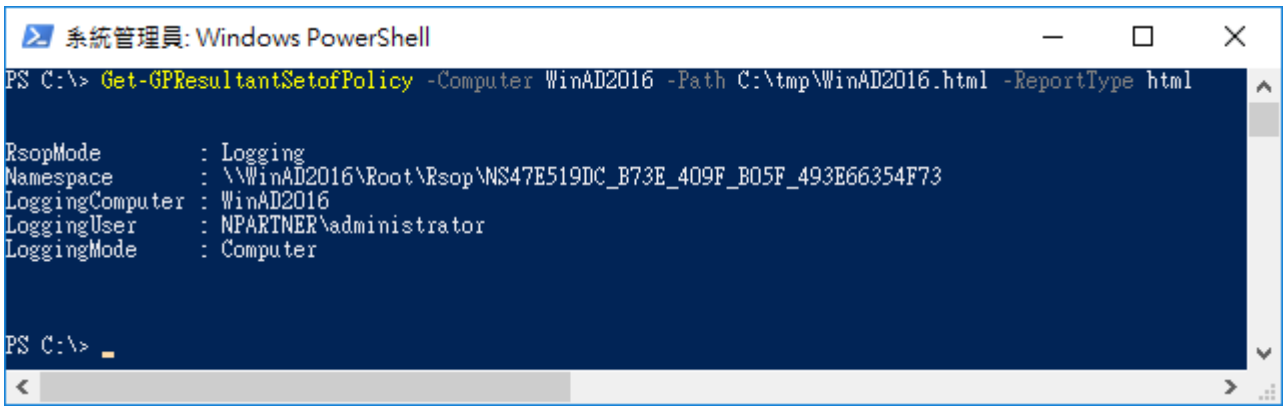
(9) 更新群組原則

```
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

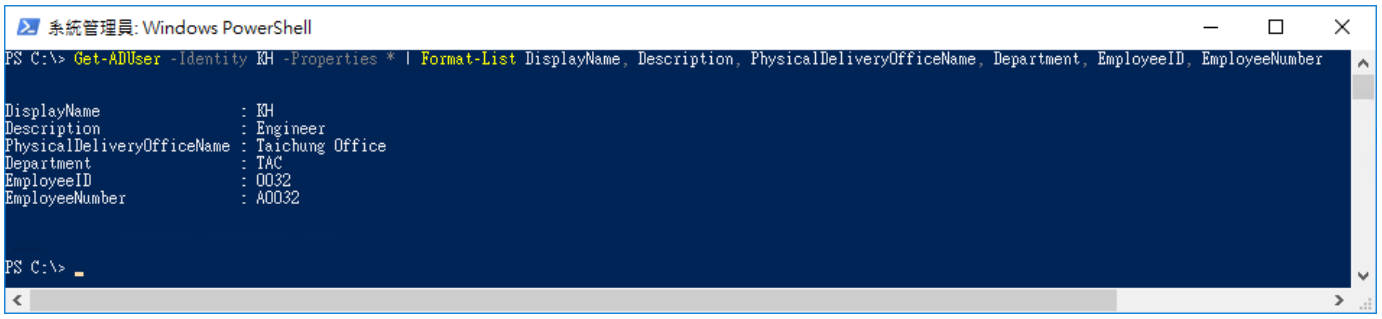
(11) 開啟報表，確認 Windows AD 2016 伺服器，套用 N-Partner Policy 群組原則

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
```



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

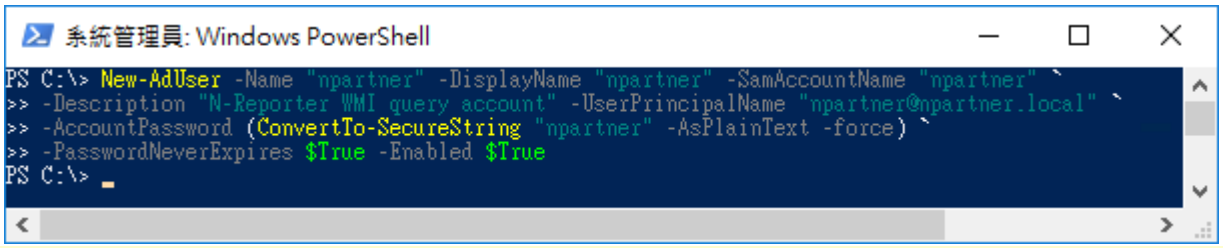
6.3.1 新增使用者

(1) 開啟 AD 使用者和電腦

開啟 [Windows PowerShell 的 Active Directory 模組]

(2) 新增帳號

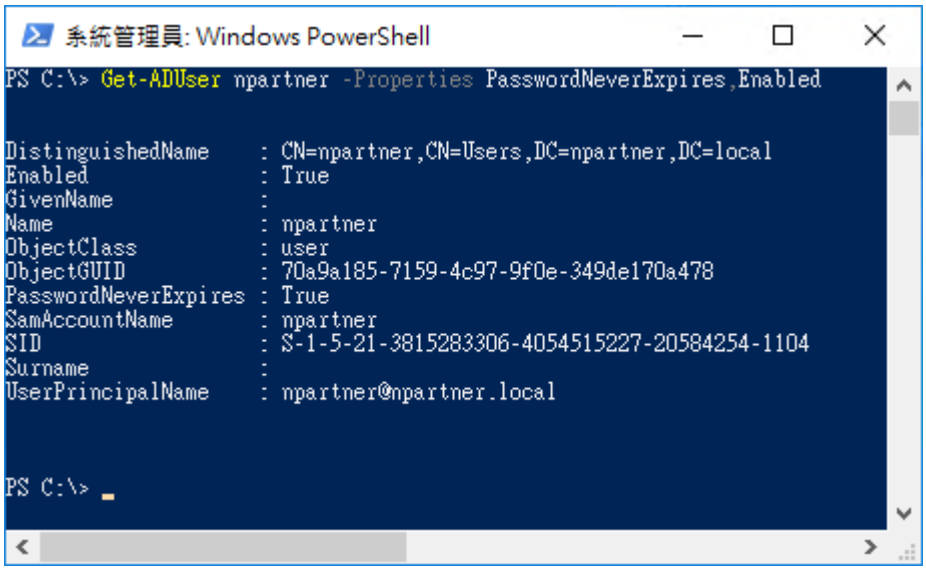
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



紅色文字部位請輸入帳號密碼及網域資訊

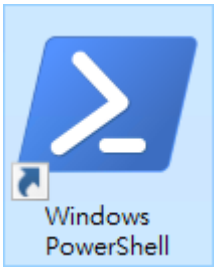
(3) 查看帳號狀態

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



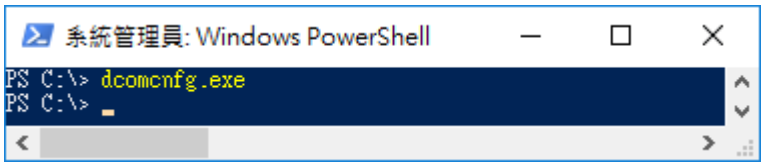
6.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]



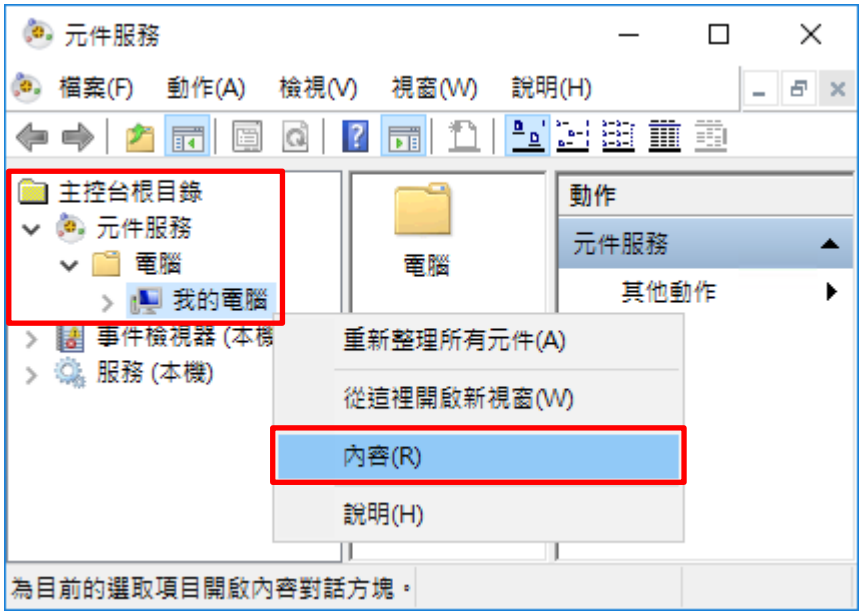
(2) 開啟元件服務

```
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]

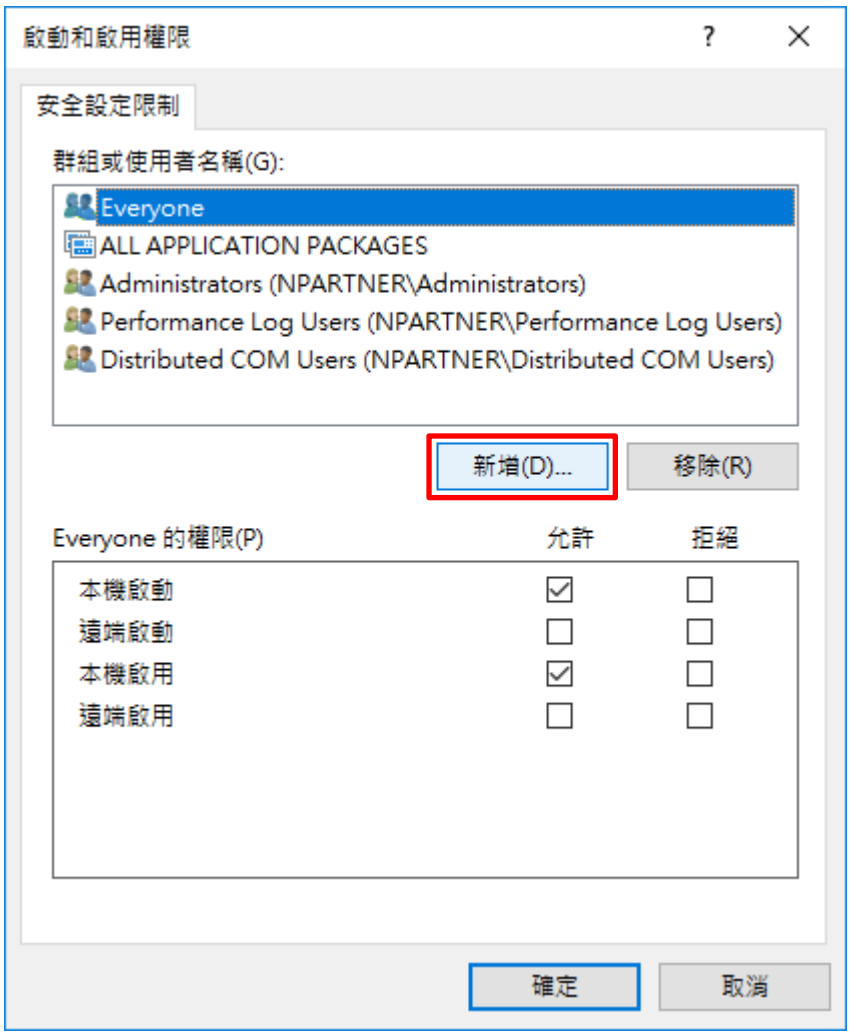


(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]

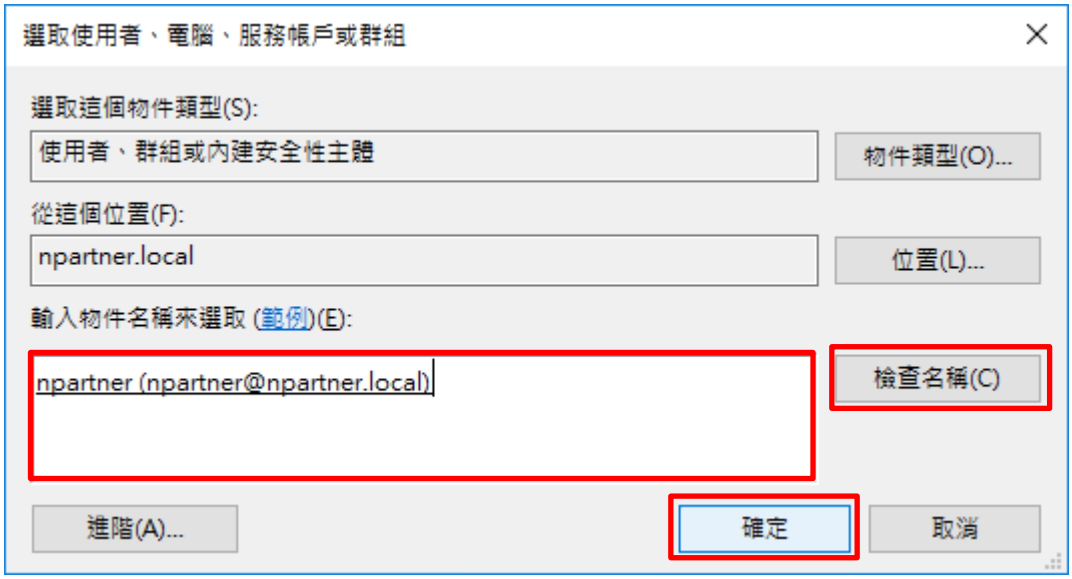
(5) 新增 DCOM 使用者權限

點選 [新增]



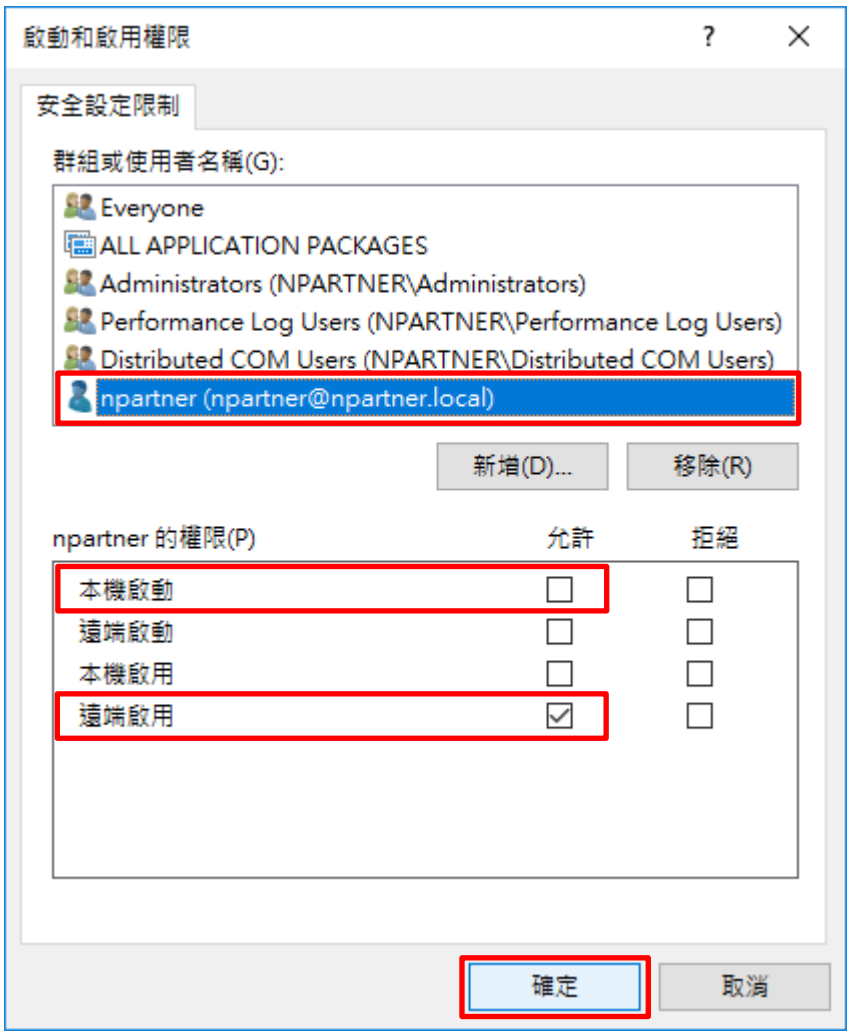
(6) 輸入使用者

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]

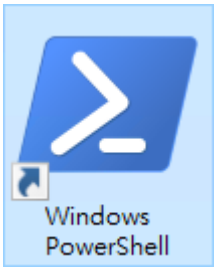


(8) 按 [確定]

6.3.3 設定 WMI 權限

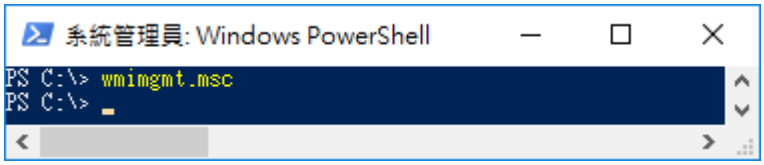
6.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]



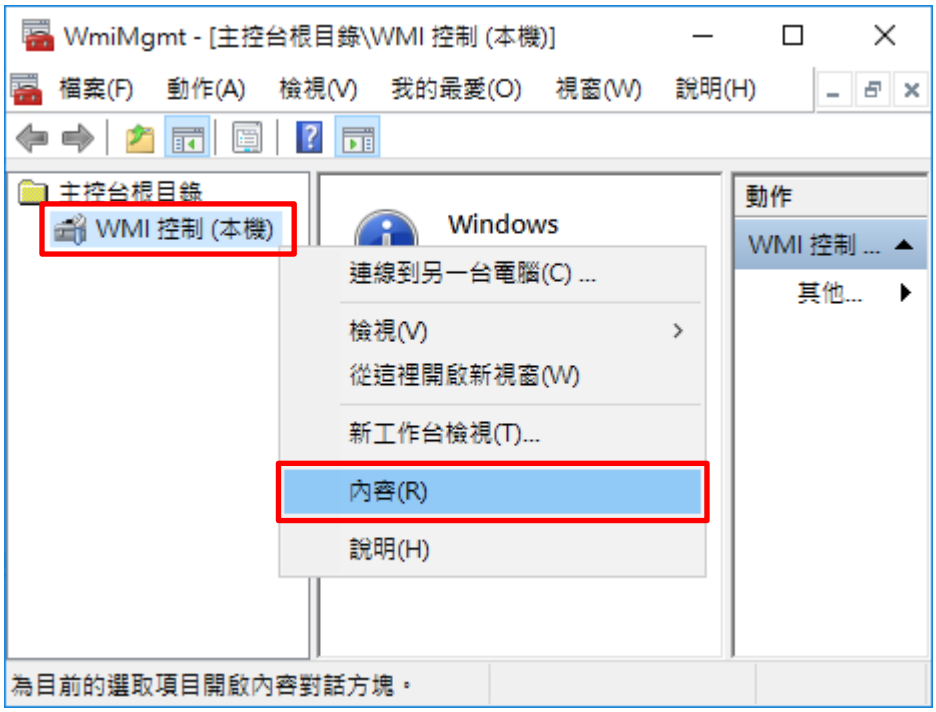
(2) 開啟元件服務

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



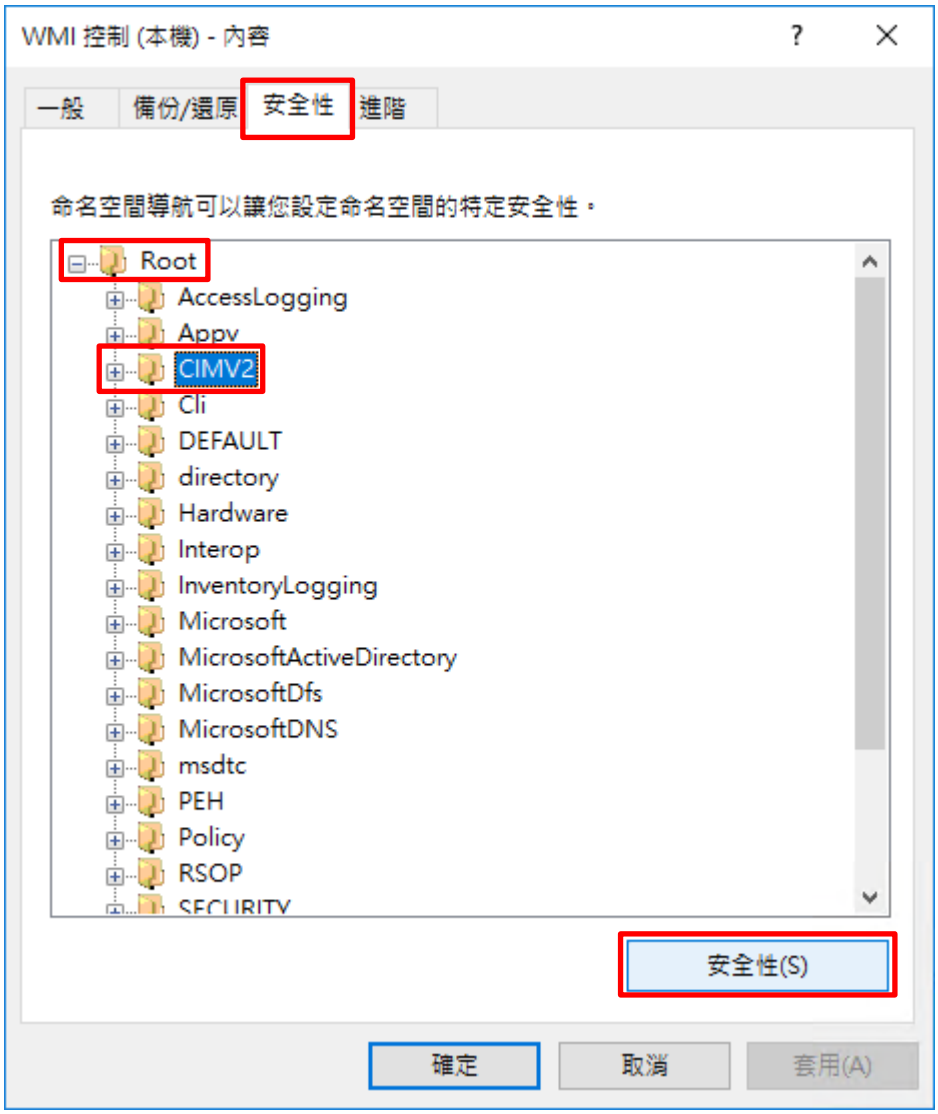
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



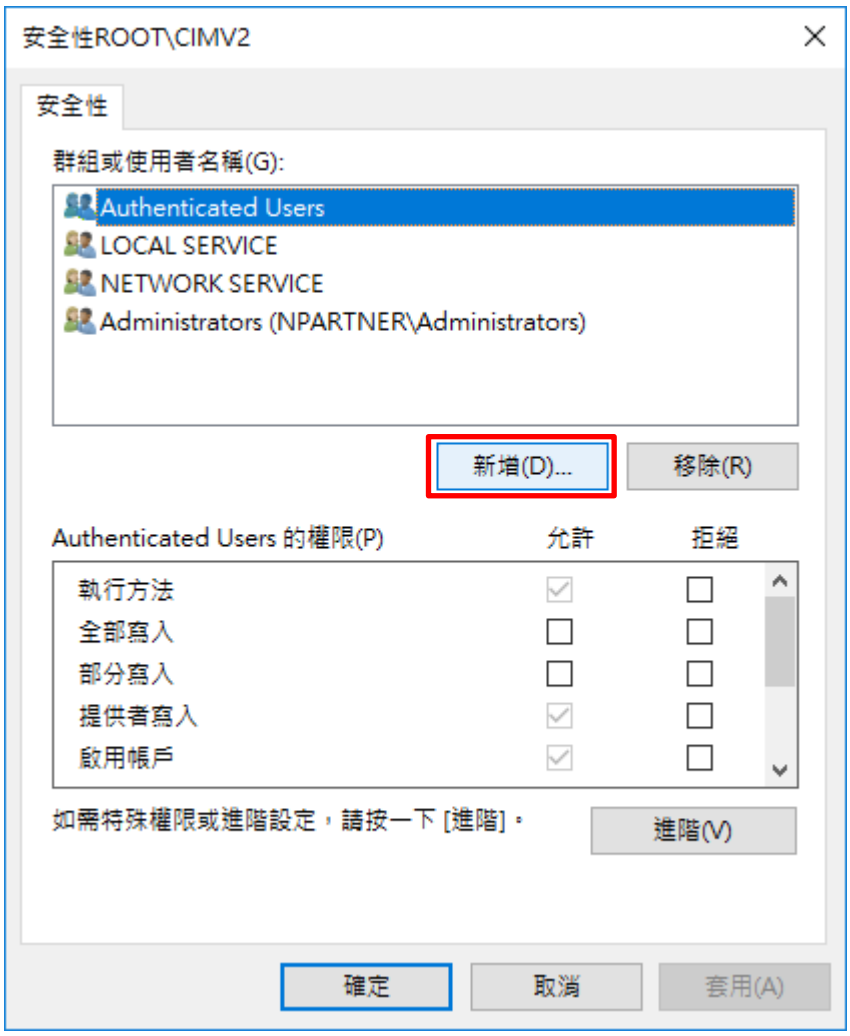
(4) 編輯 CIMV2 安全性

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



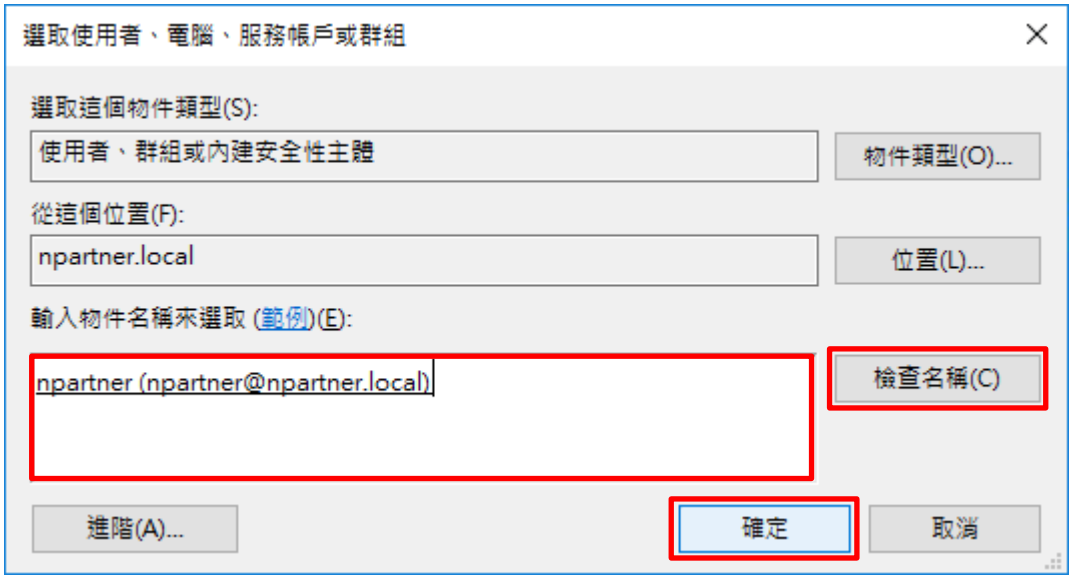
(5) 新增 WMI 使用者權限

按 [新增]



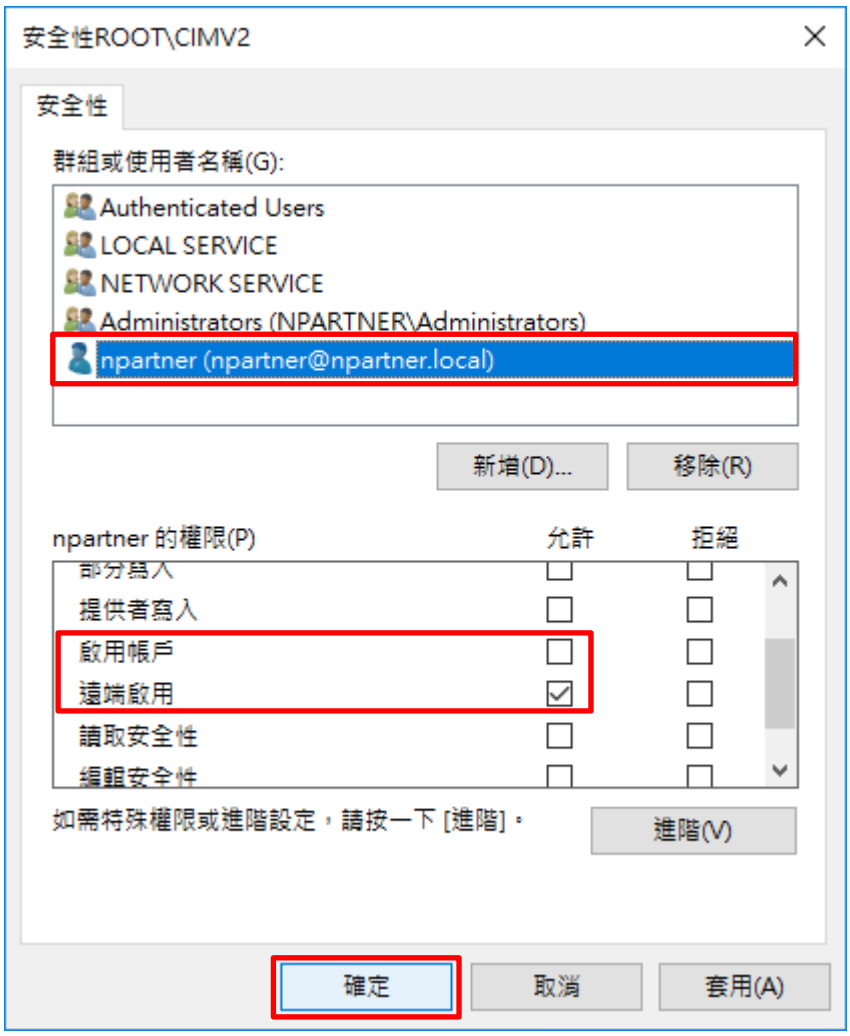
(6) 輸入使用者

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

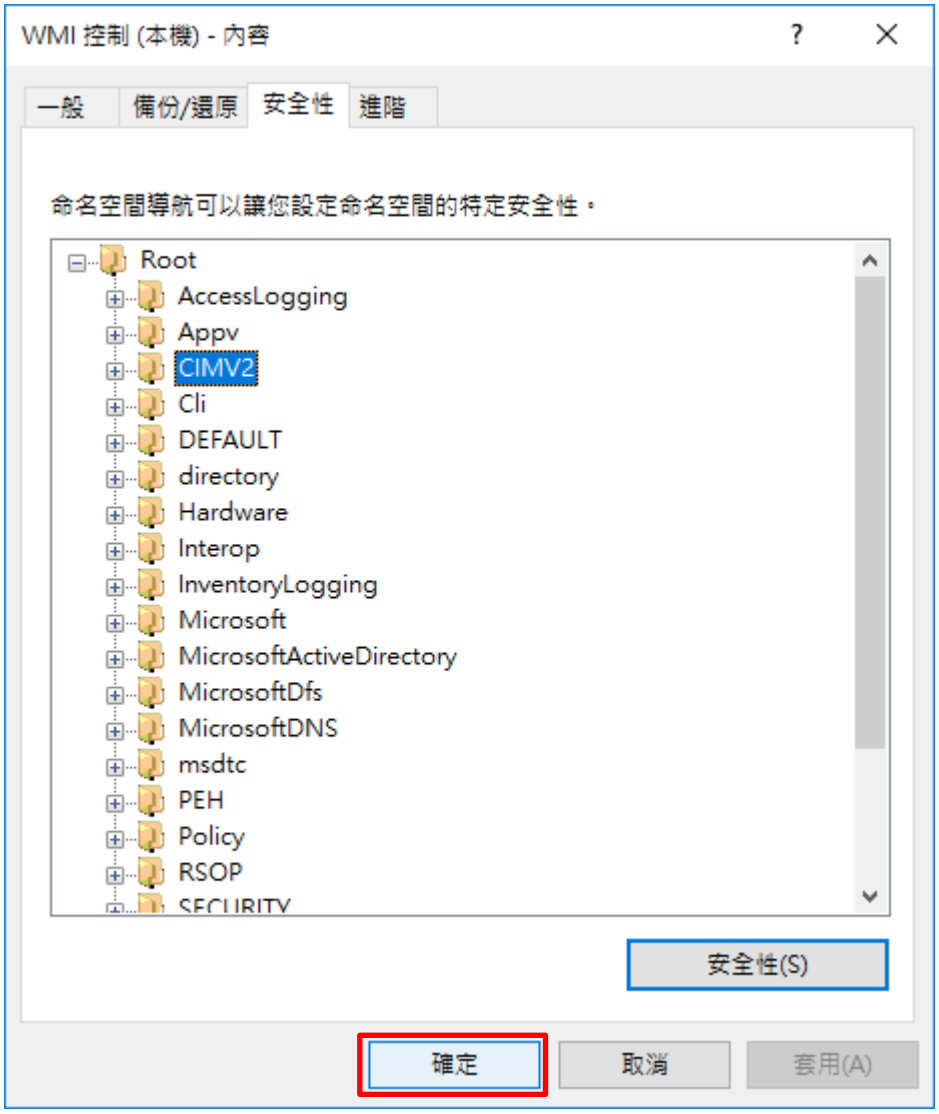


(7) 設定使用者權限

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]

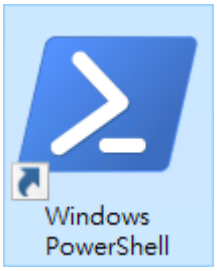


(8) 按 [確定]



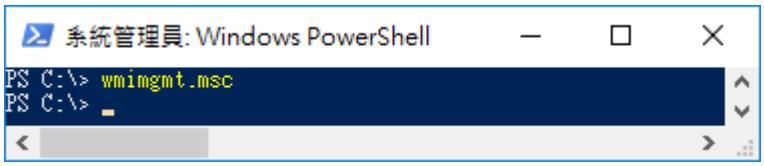
6.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]



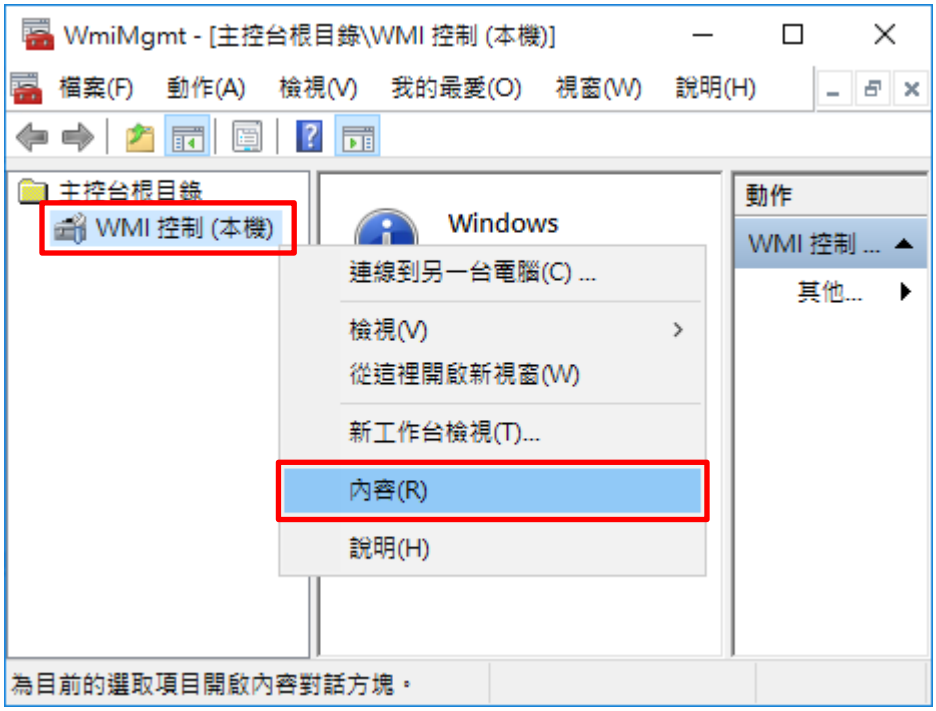
(2) 開啟元件服務

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



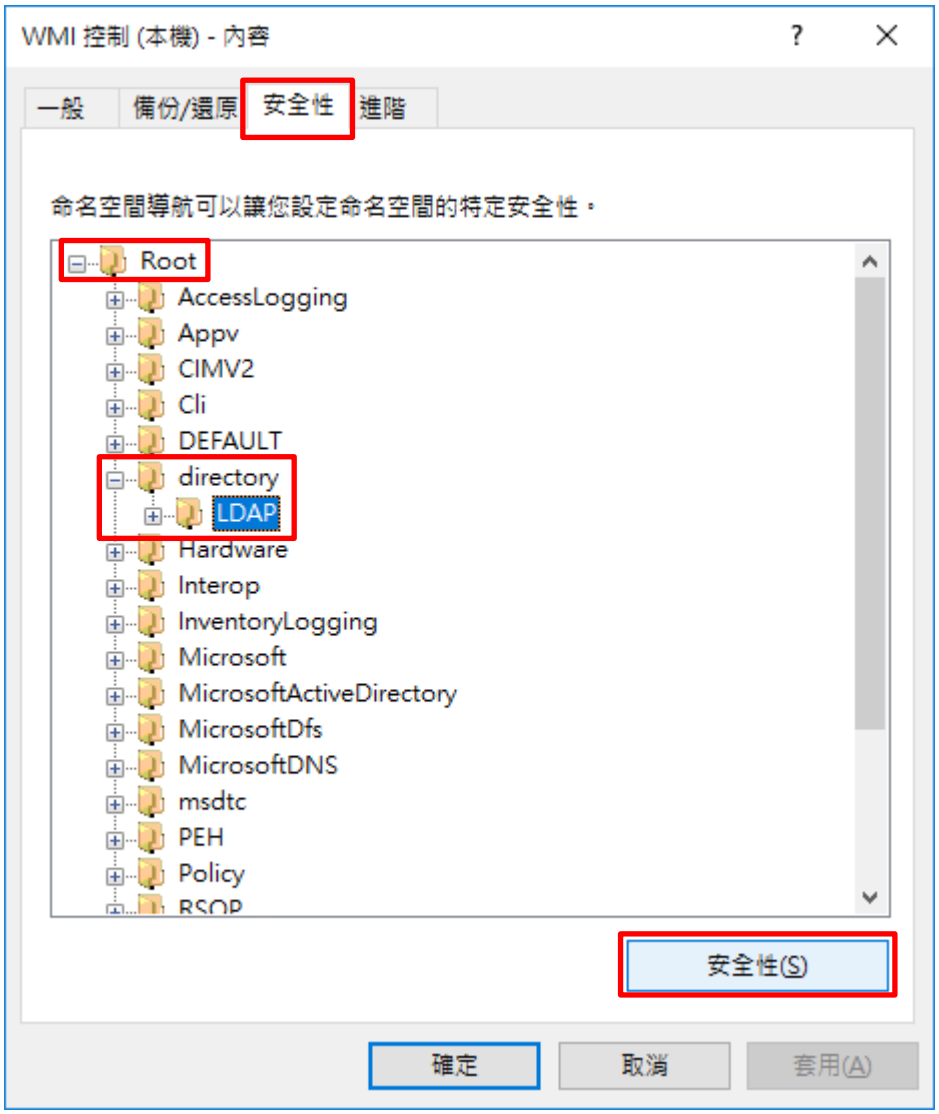
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



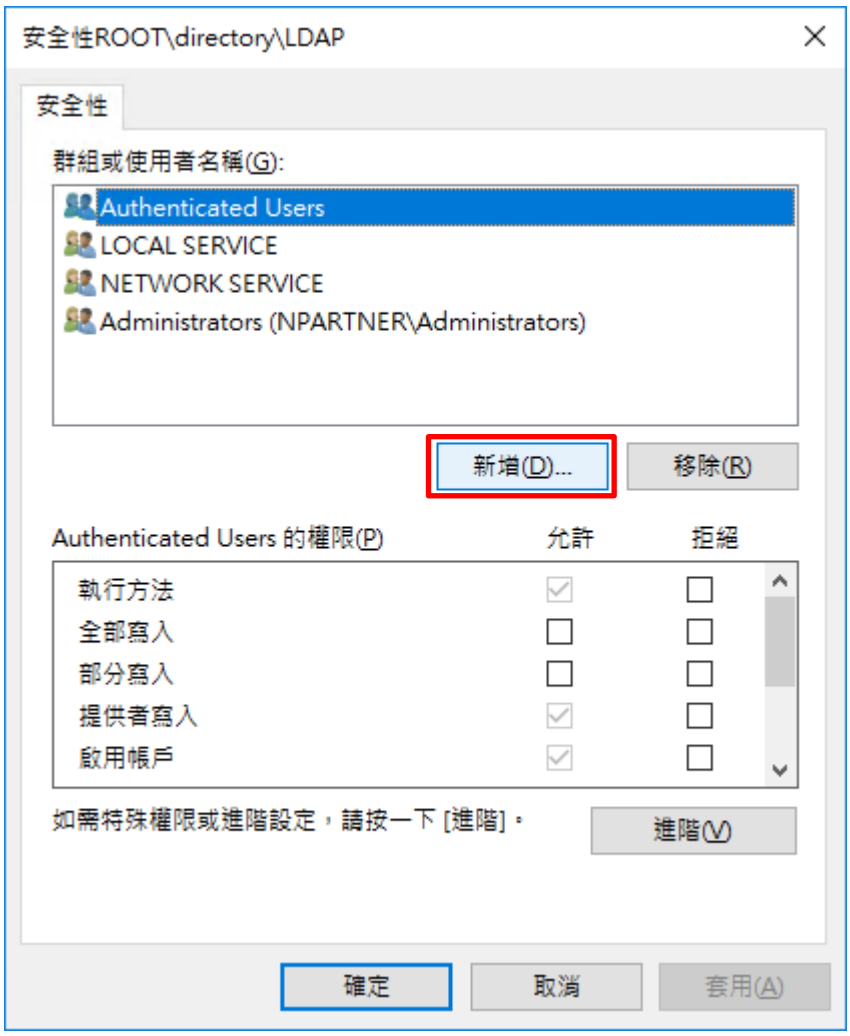
(4) 編輯 LDAP 安全性

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



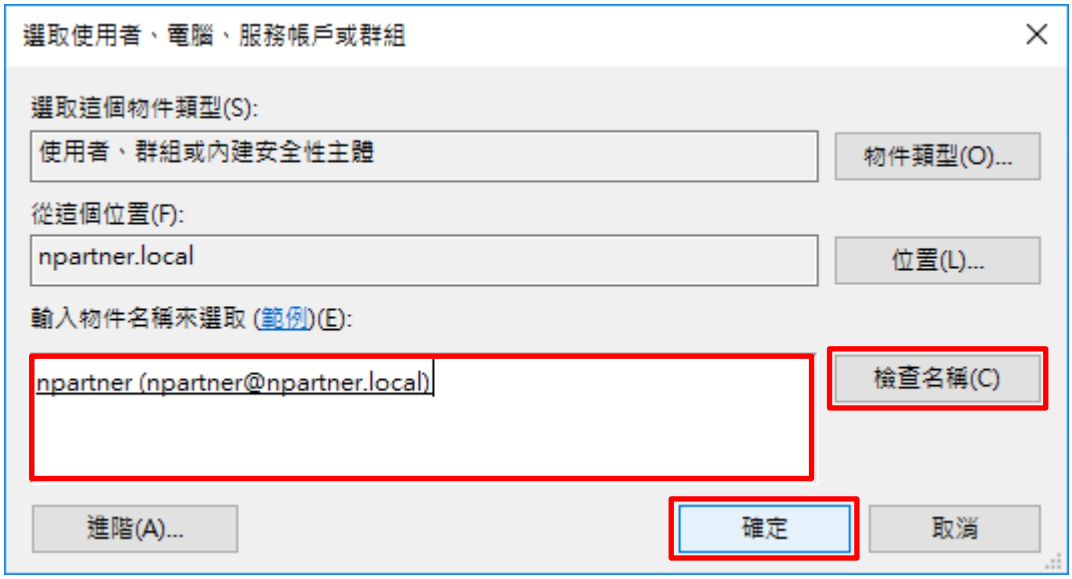
(5) 新增 WMI 使用者權限

按 [新增]



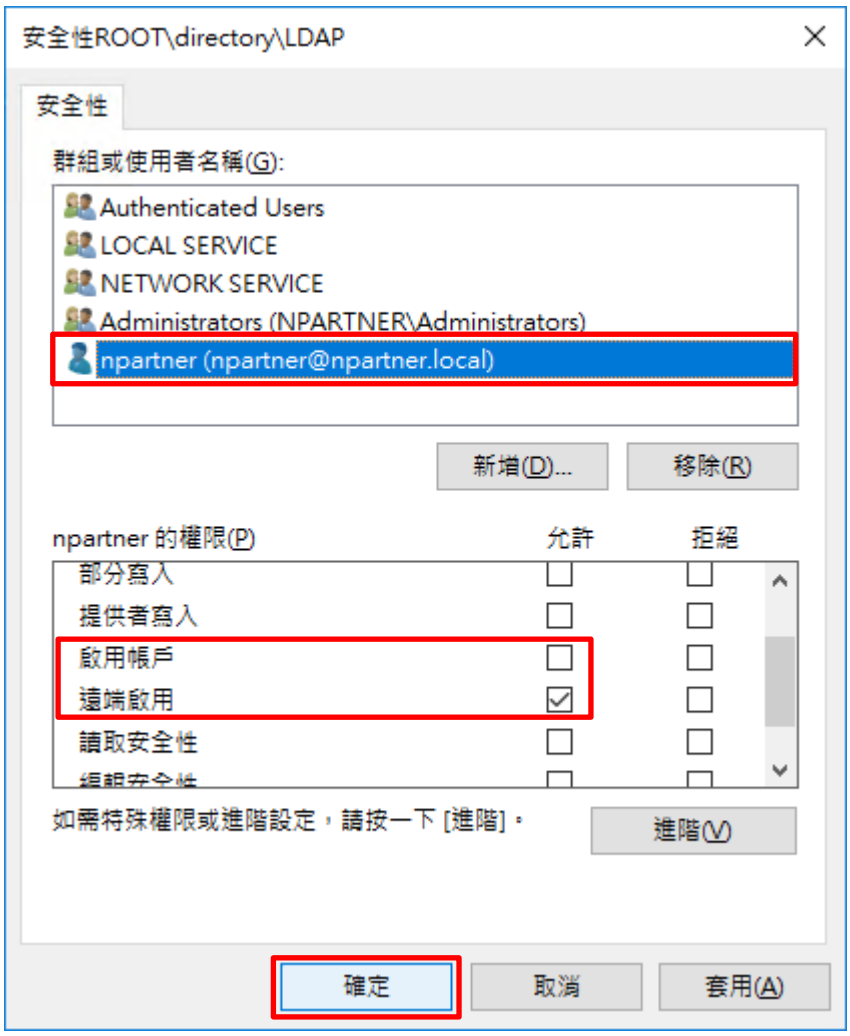
(6) 輸入使用者

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

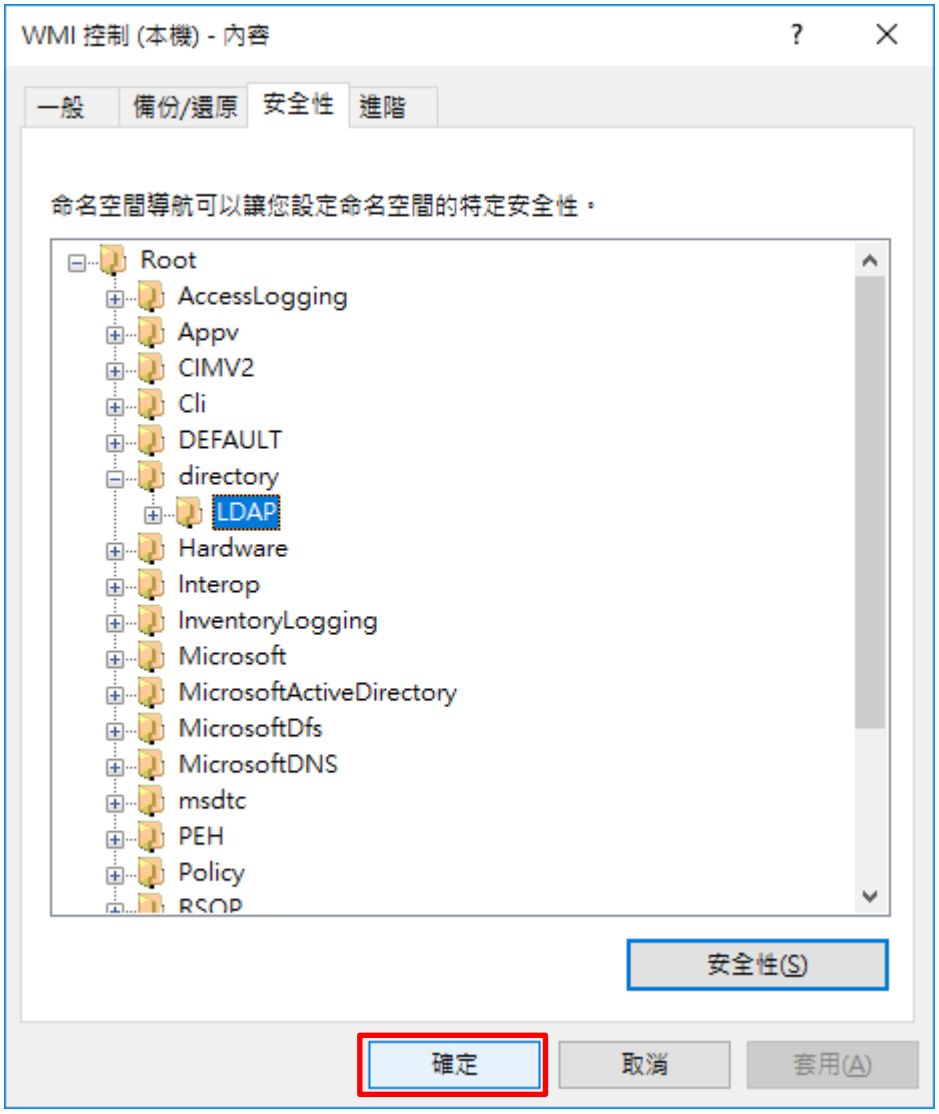


(7) 設定使用者權限

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]

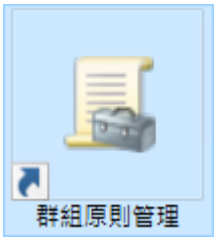


(8) 按 [確定]



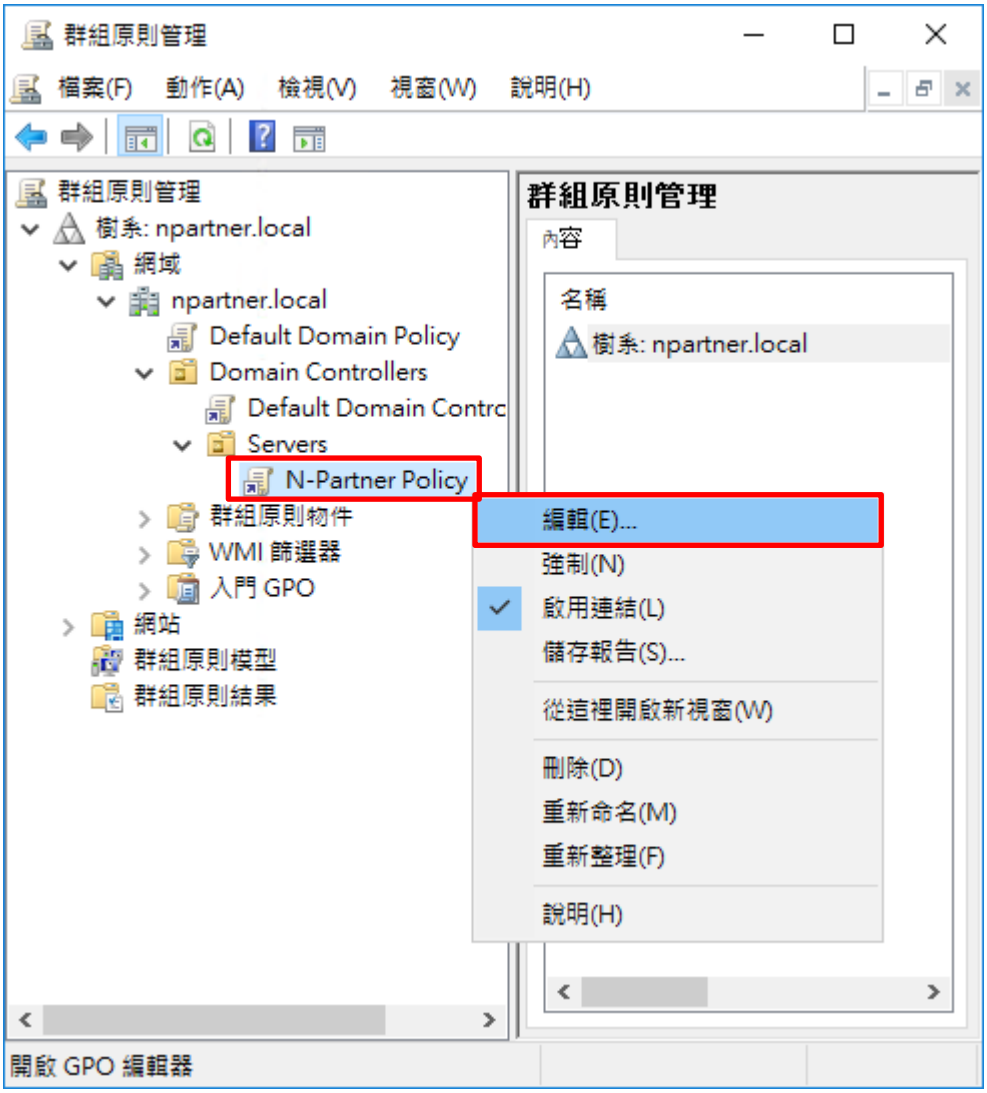
6.3.4 設定 Event log 讀取權限

(1) 開啟 [群組原則管理]



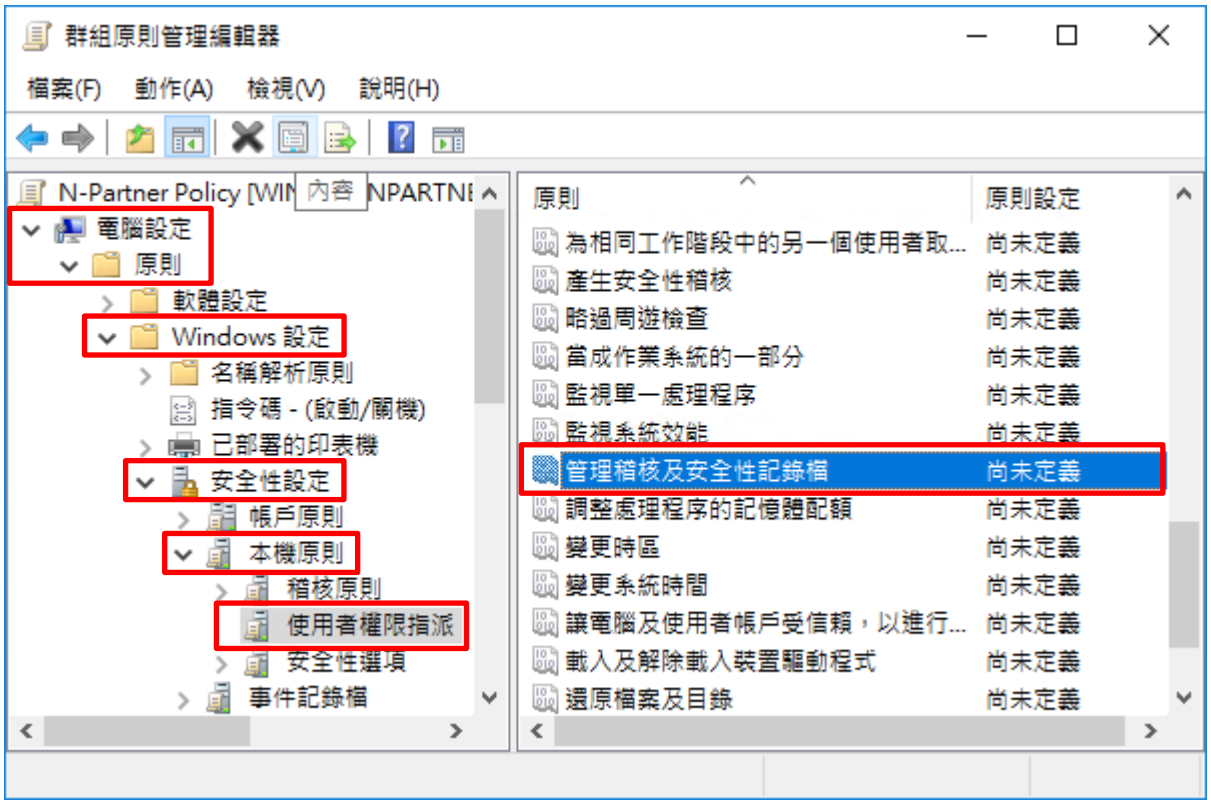
(2) 編輯群組原則物件

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

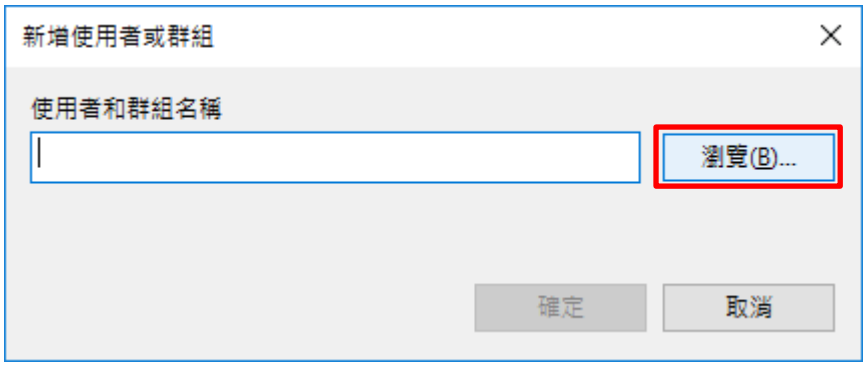


(4) 新增管理稽核使用者

勾選 [定義這些原則設定] -> 按 [新增使用者或群組...]

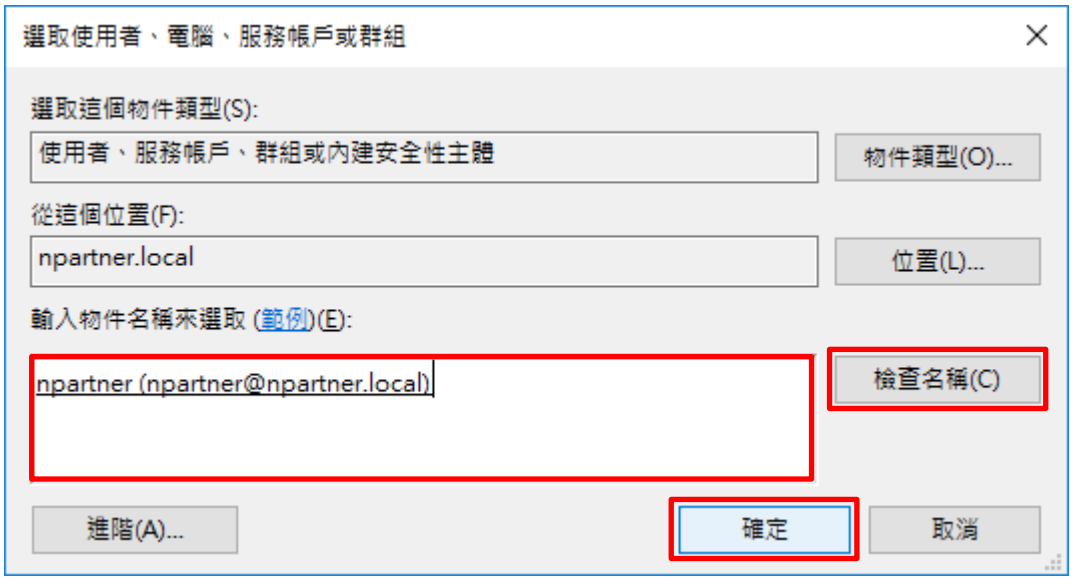
(5) 搜尋使用者

按 [瀏覽]



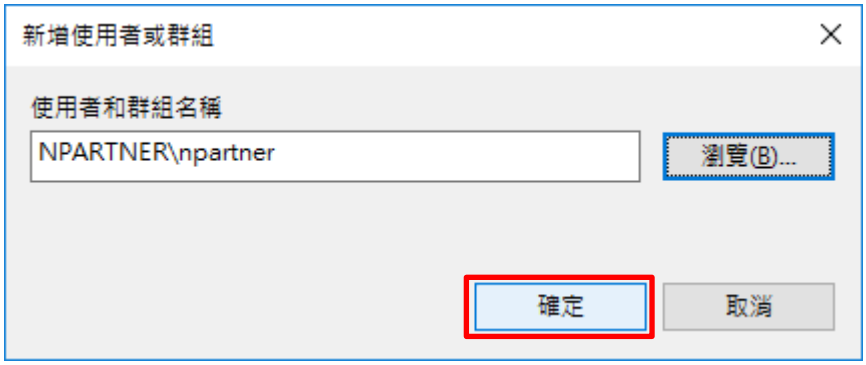
(6) 輸入使用者

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



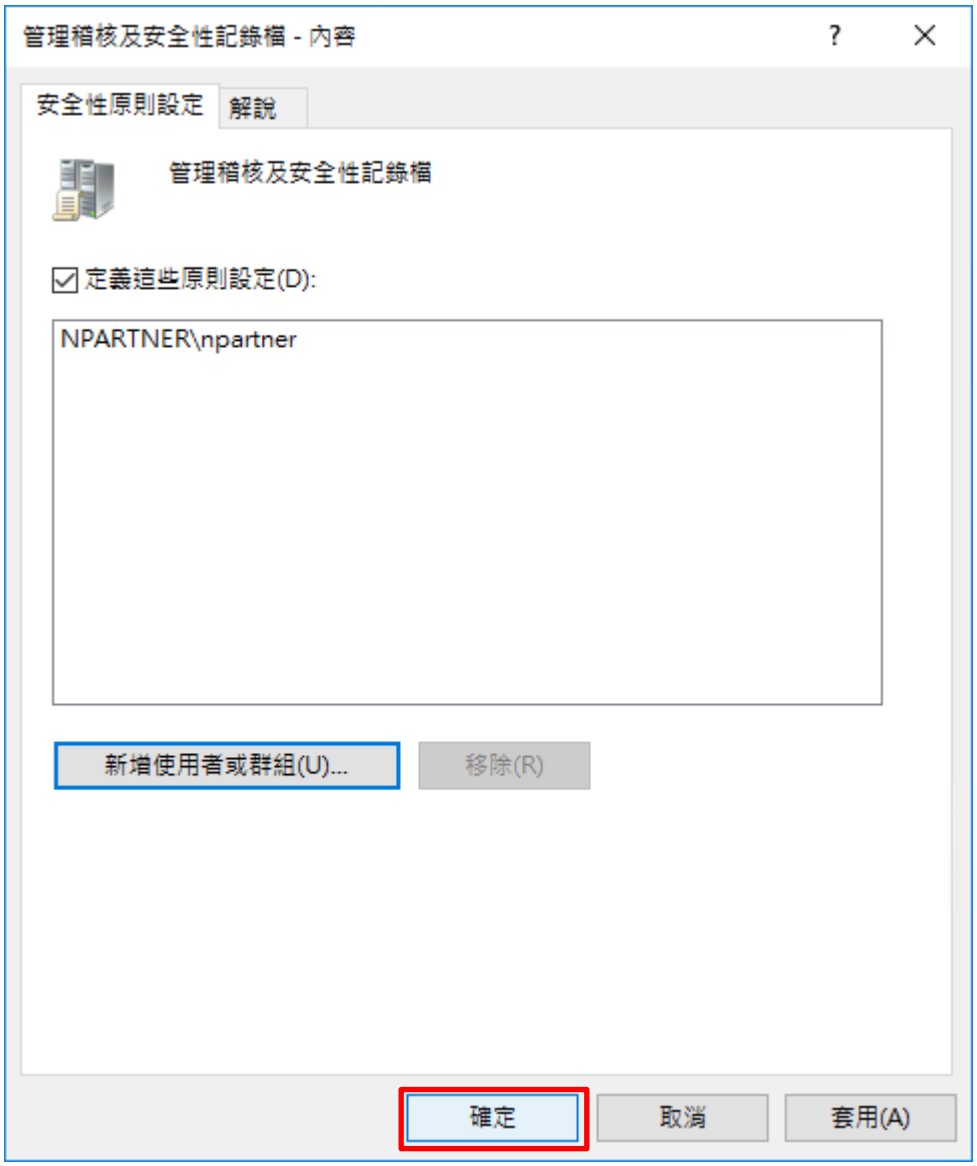
(7) 確定使用者

按 [確定]



(8) 確定設定記錄檔

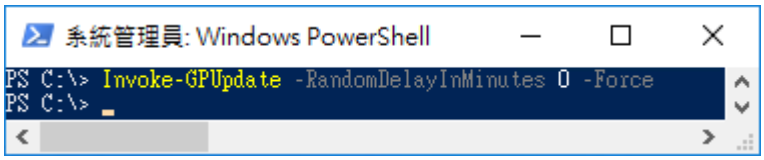
按 [確定]



(9) 開啟 [Windows PowerShell]

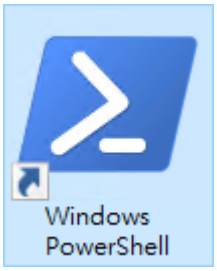
(10) 更新群組原則

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



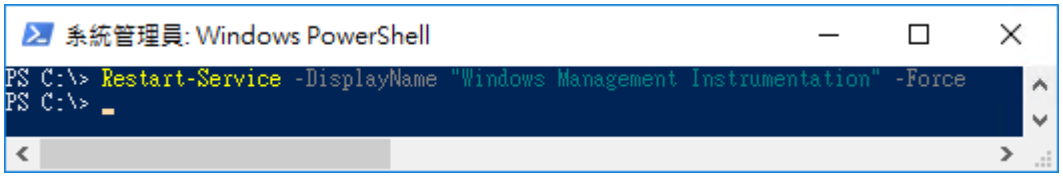
6.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]



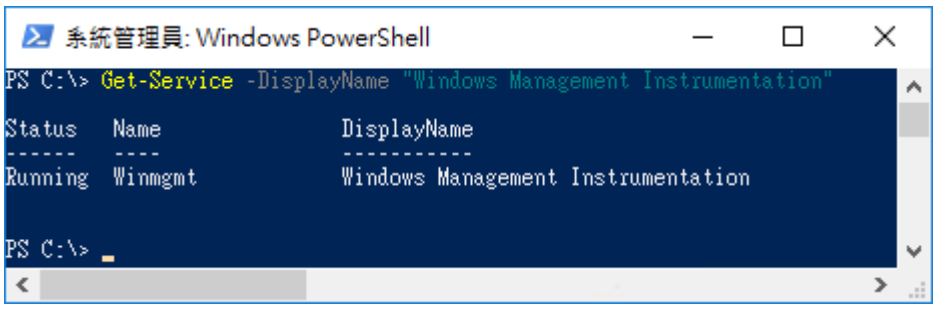
(2) 重啟 WMI 服務

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



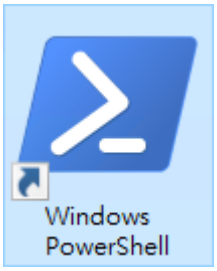
(3) 查看 WMI 服務

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



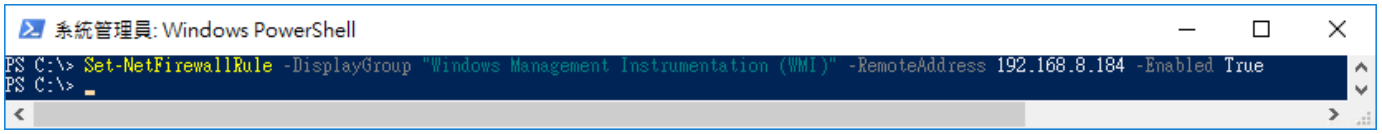
6.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]



(2) 設定防火牆，只允許 N-Reporter IP query WMI

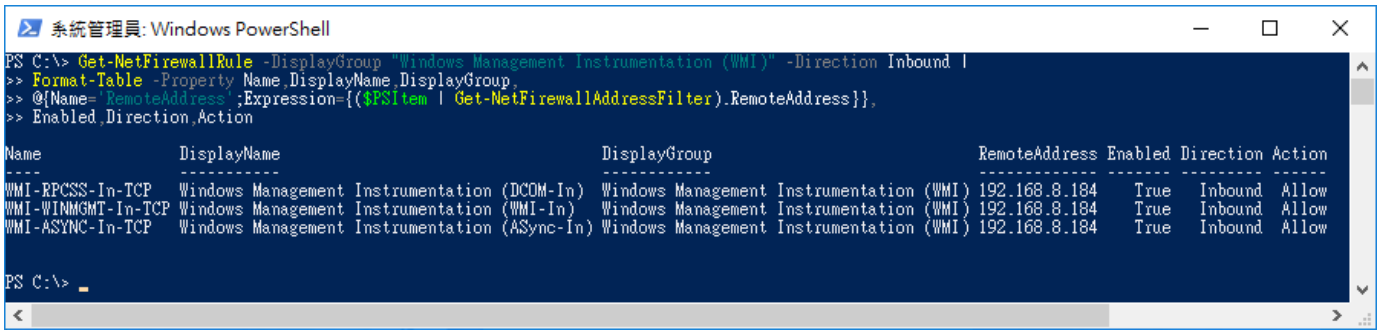
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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
```



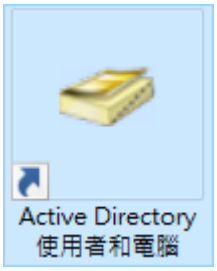
7. Windows 2019

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

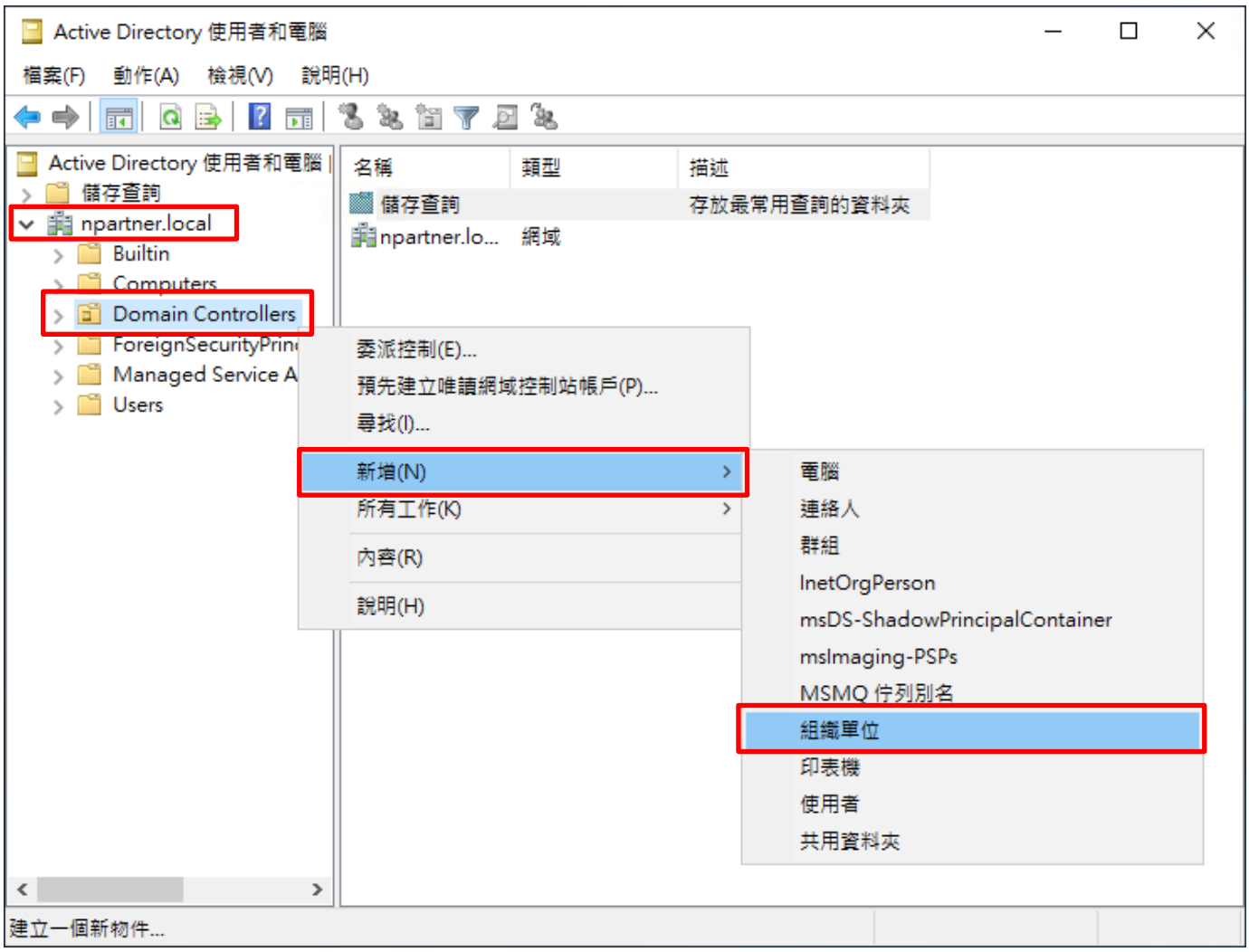
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



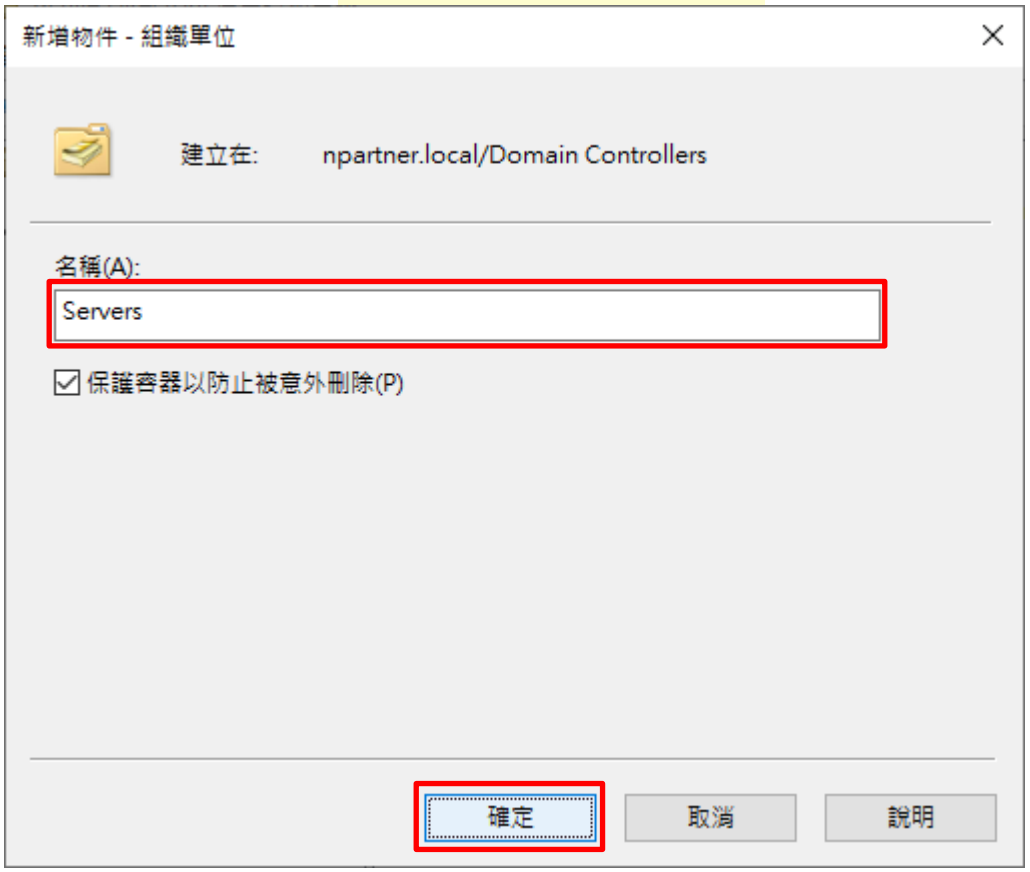
(2) 新增組織單位

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]



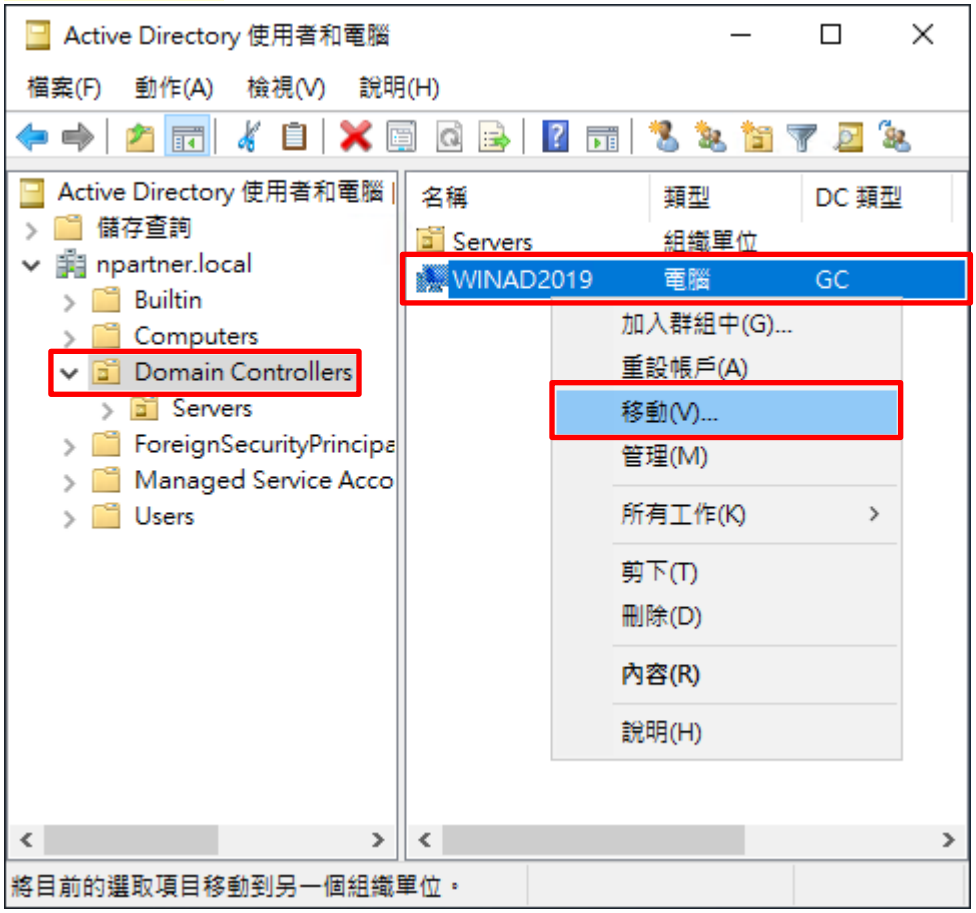
(3) 輸入組織單位名稱

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]



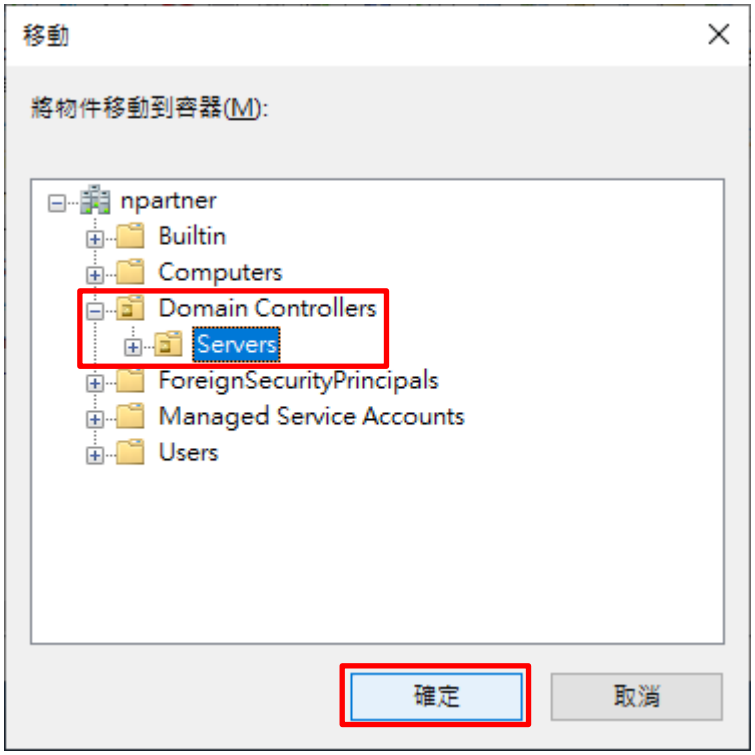
(4) 移動伺服器至新的組織單位

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]



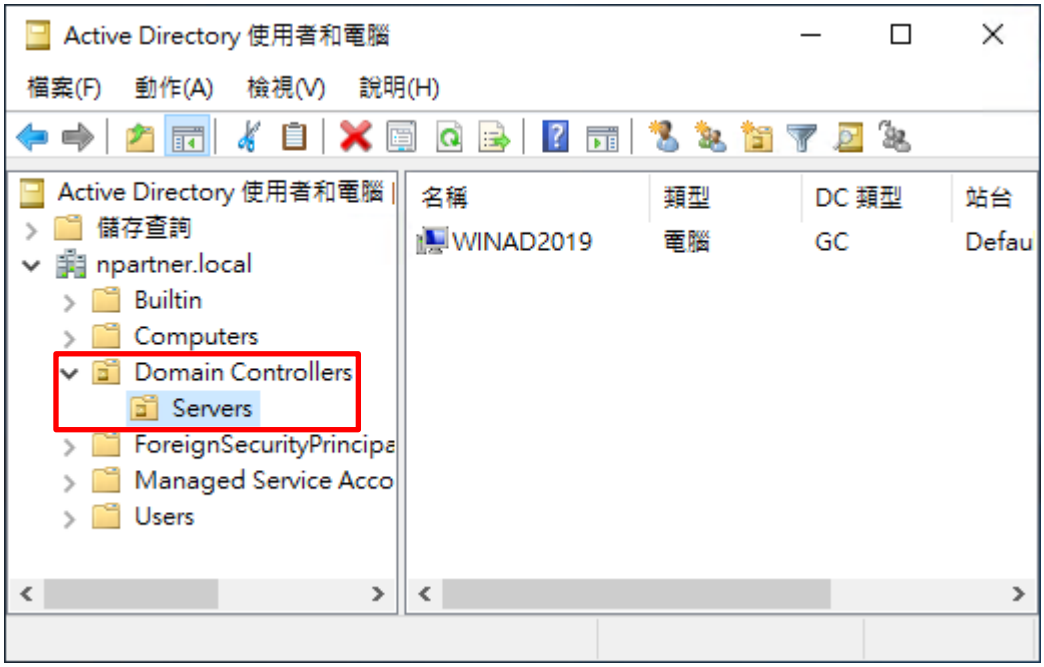
(5) 選擇組織單位

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

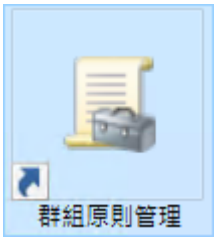
點選 [Domain Controllers] 的 [Servers] 組織單位，確認 [WinAD2019] 網域伺服器已移動。



7.2 群組原則設定

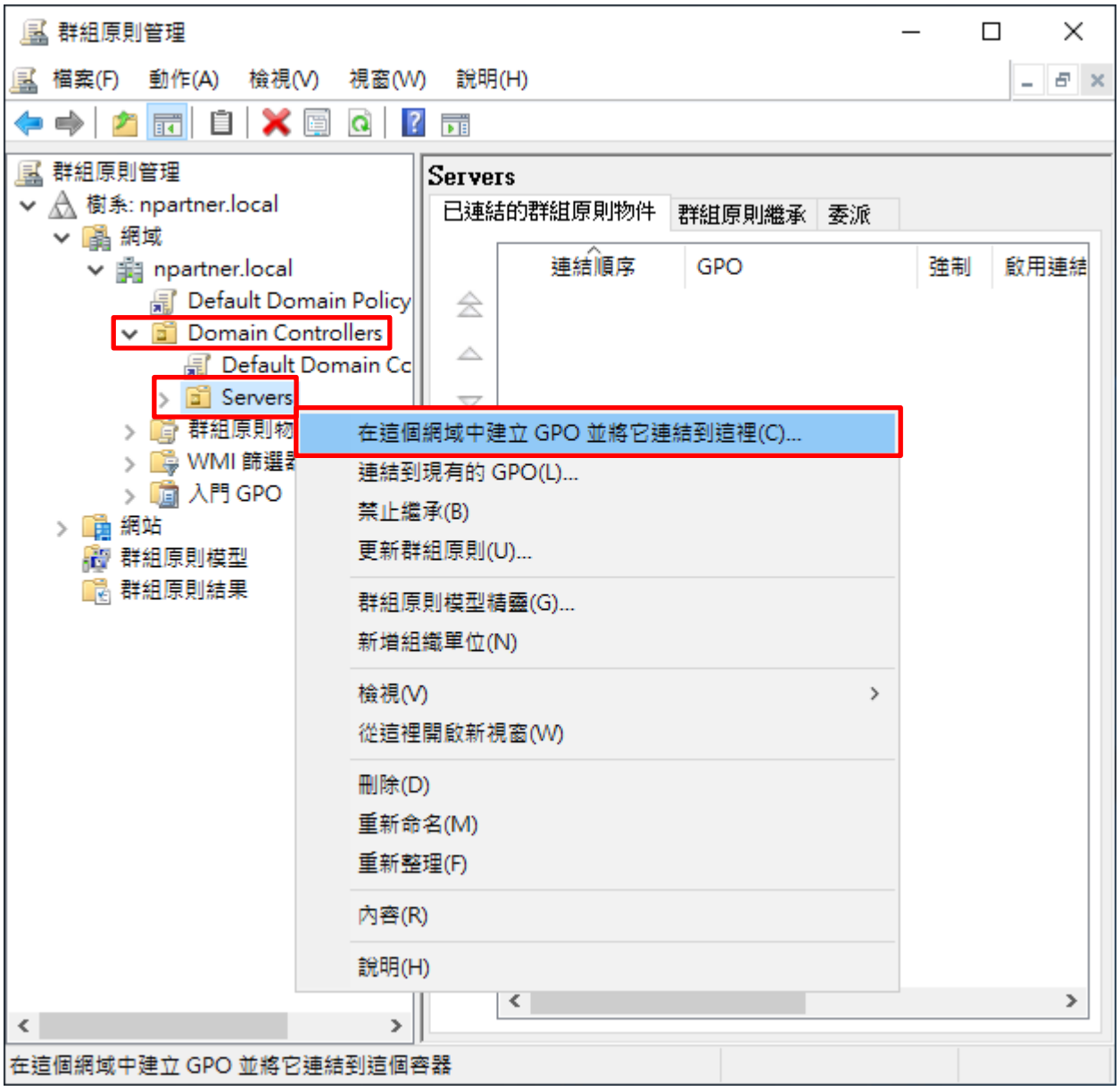
(1) 開啟群組原則管理

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...]

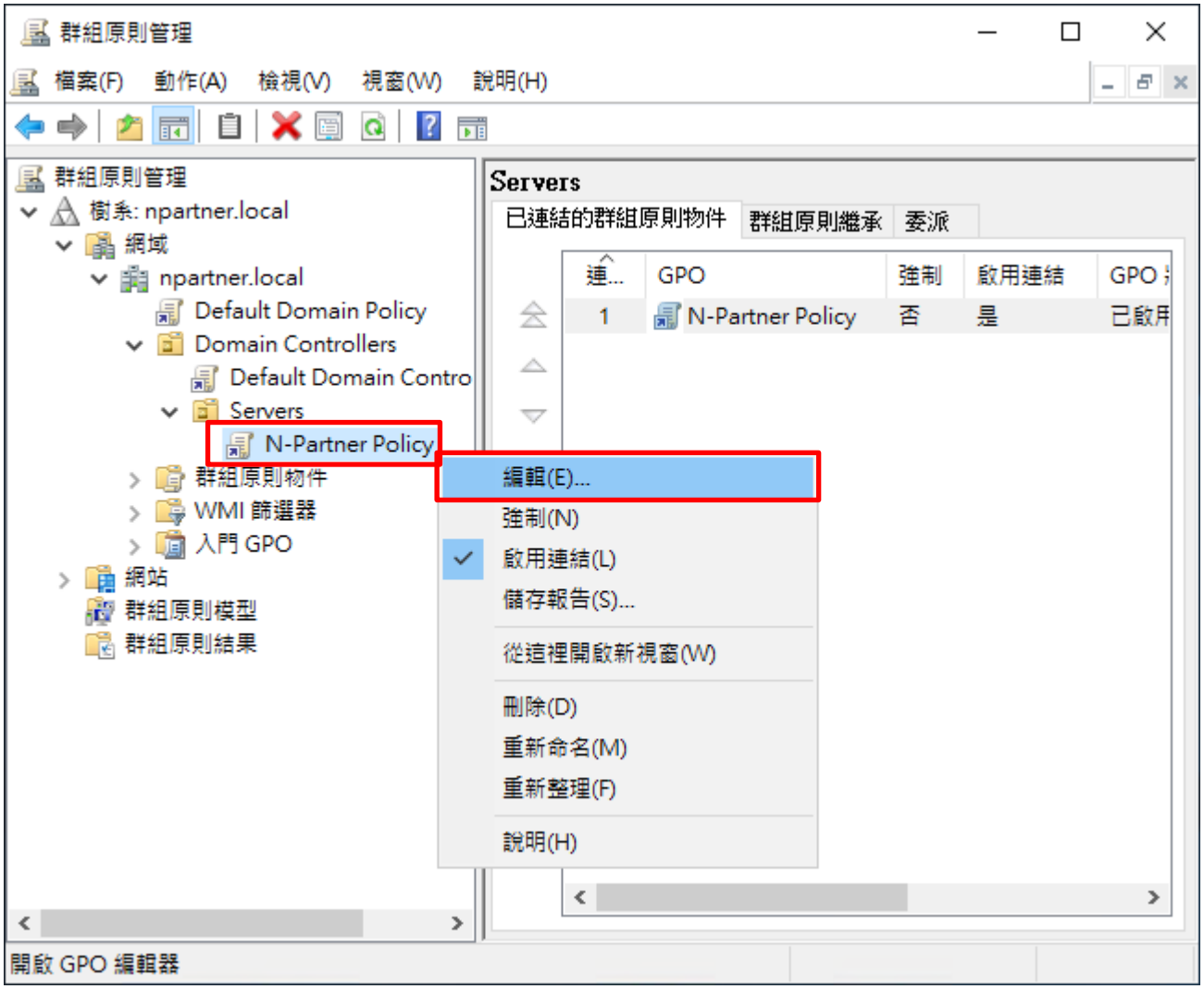


(3) 輸入群組原則物件名稱

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]

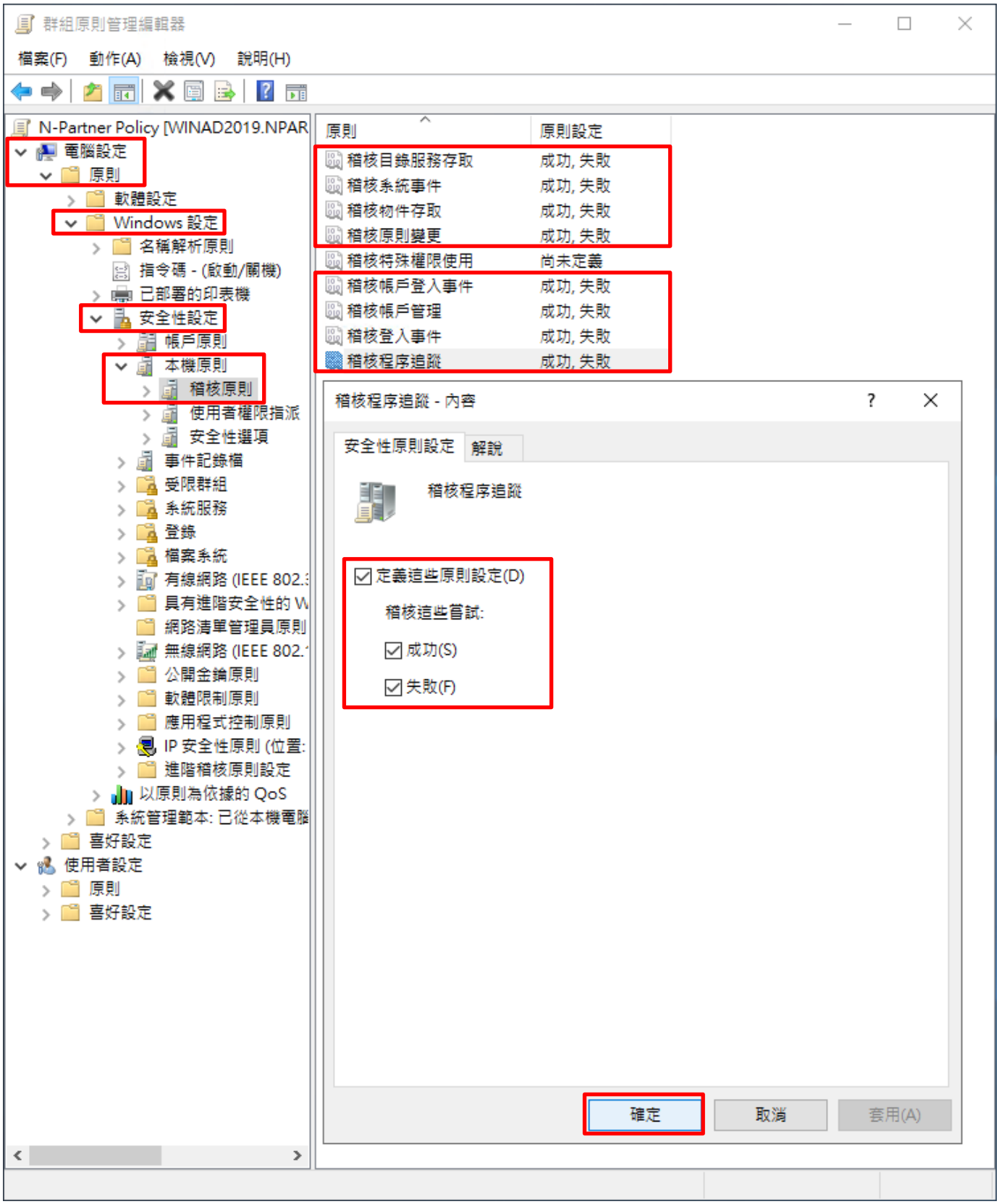
(4) 編輯群組原則物件

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



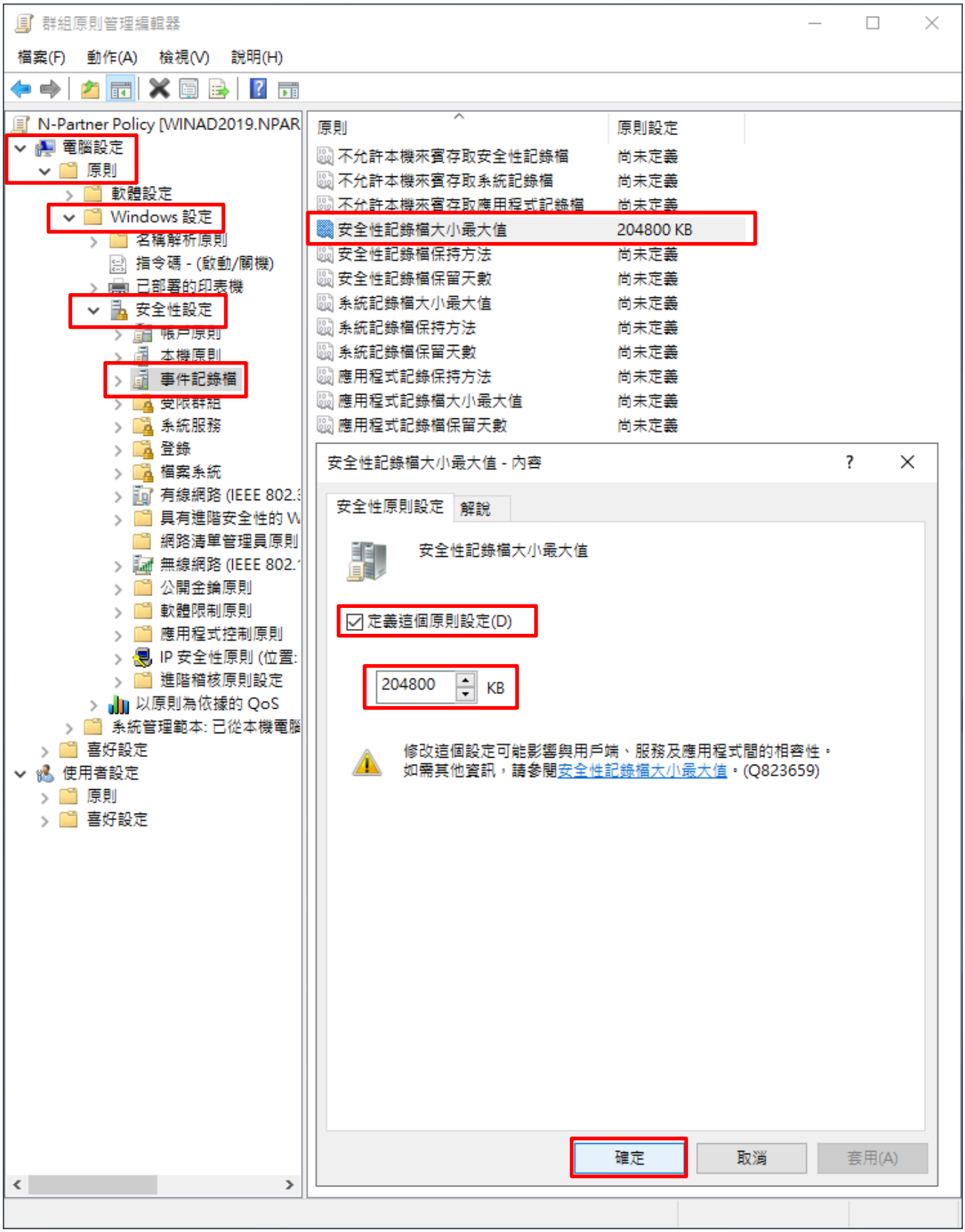
(5) 本機原則：稽核原則

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]



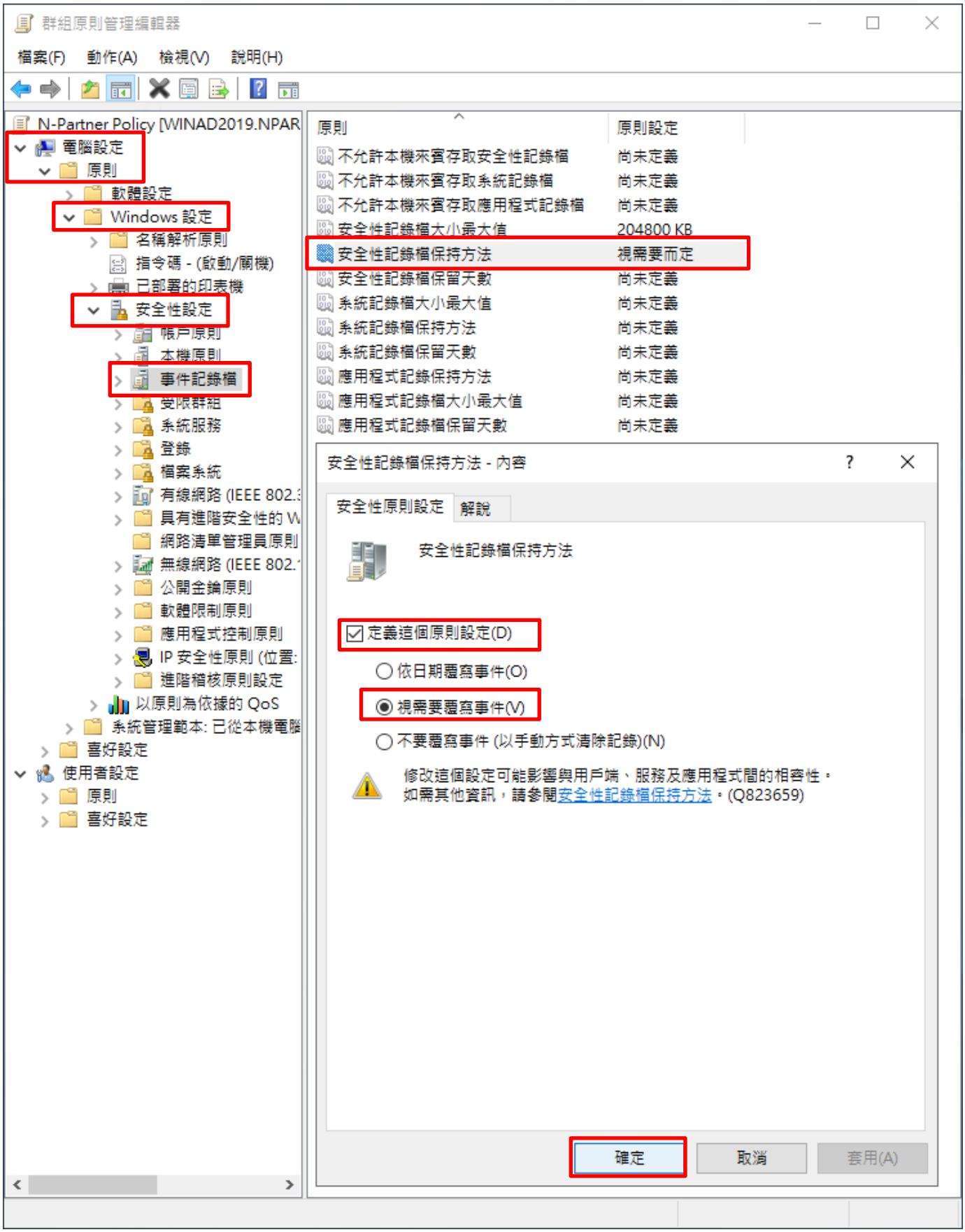
(6) 事件記錄檔：安全性記錄檔大小最大值

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



(7) 事件記錄檔：安全性記錄檔保持方法

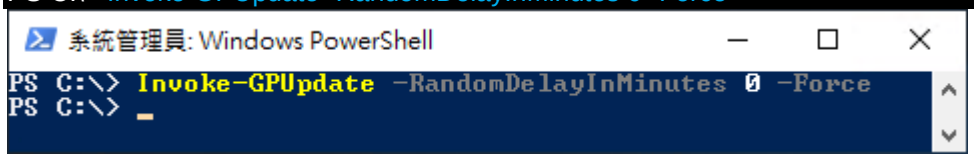
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [安全性記錄檔保持方法] 項目 -> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(8) 開啟 [Windows PowerShell]

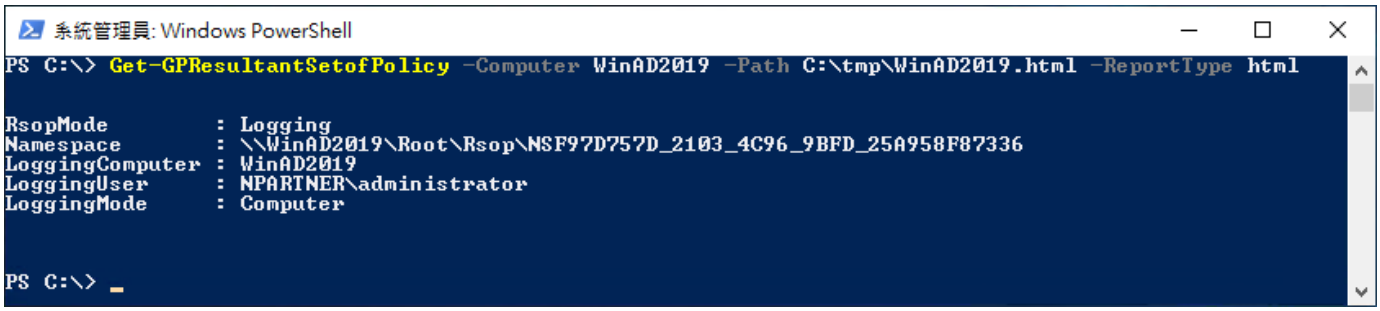
(9) 更新群組原則

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

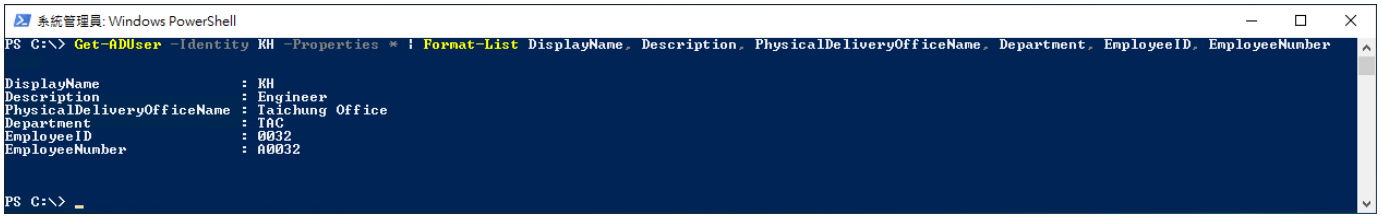
(11) 開啟報表，確認 Windows AD 2019 伺服器，套用 N-Partner Policy 群組原則

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
```



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 

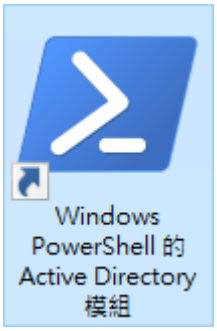
等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500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

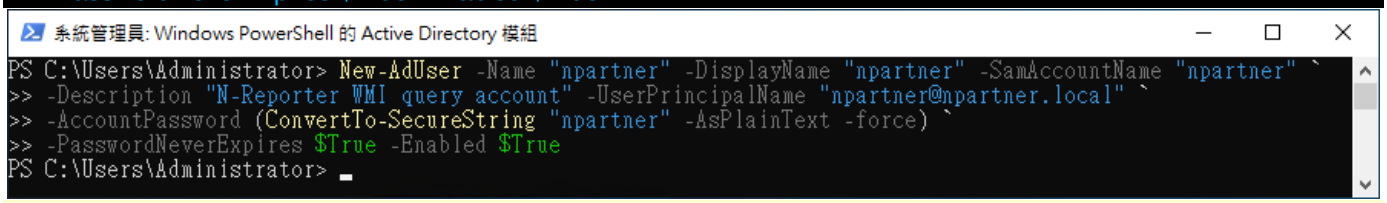
7.3.1 新增非管理帳號

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



(2) 新增帳號

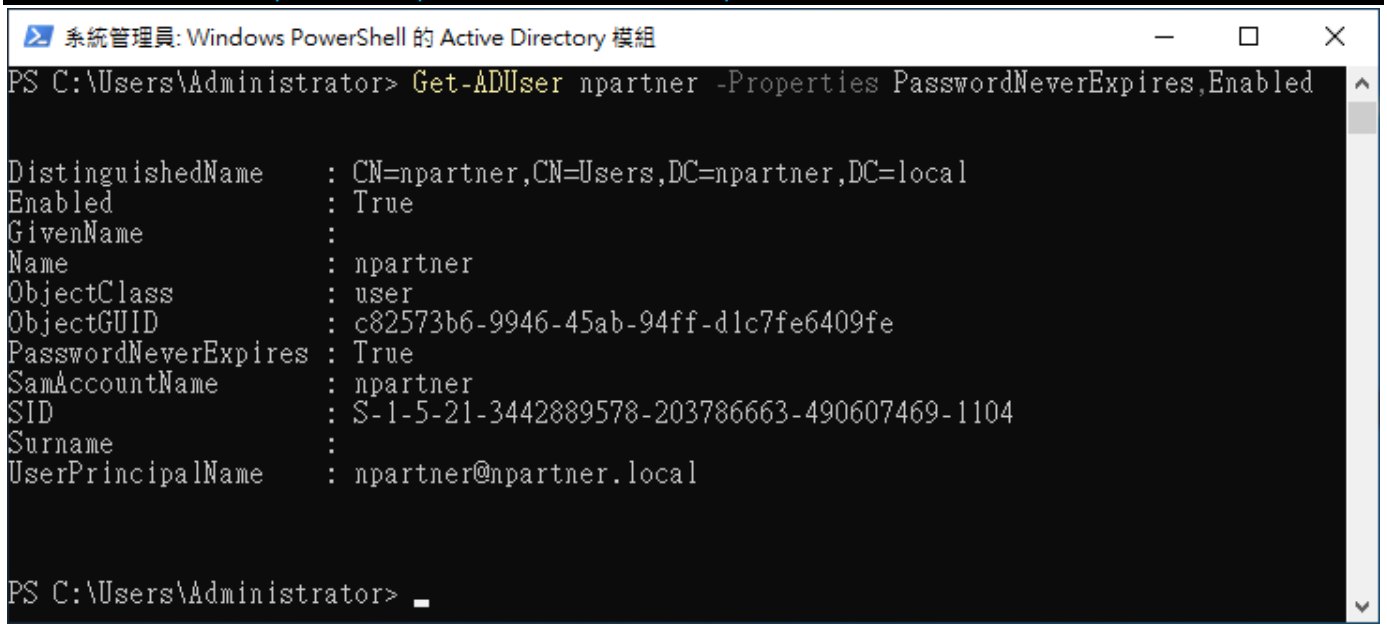
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



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
```

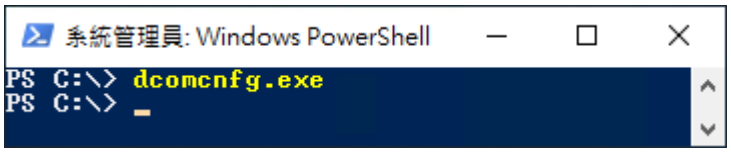


7.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

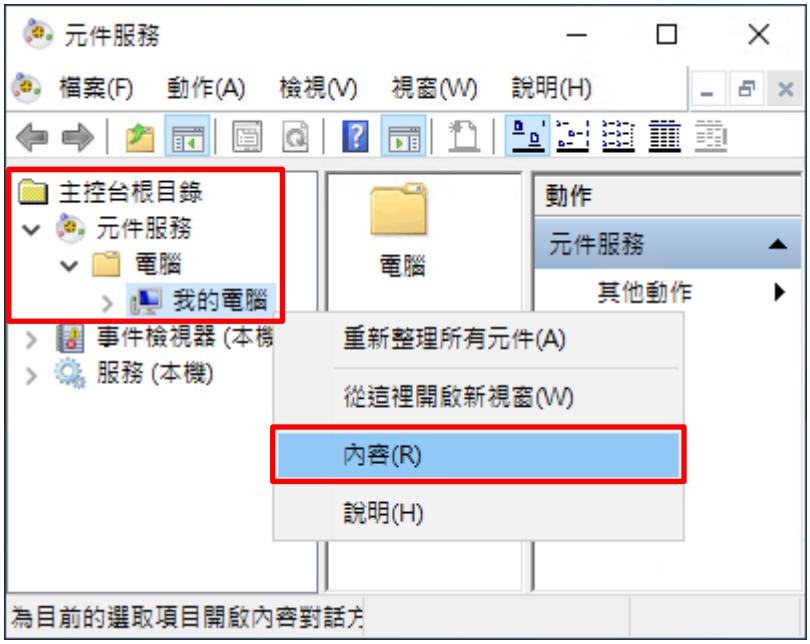
(2) 開啟元件服務

```
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]

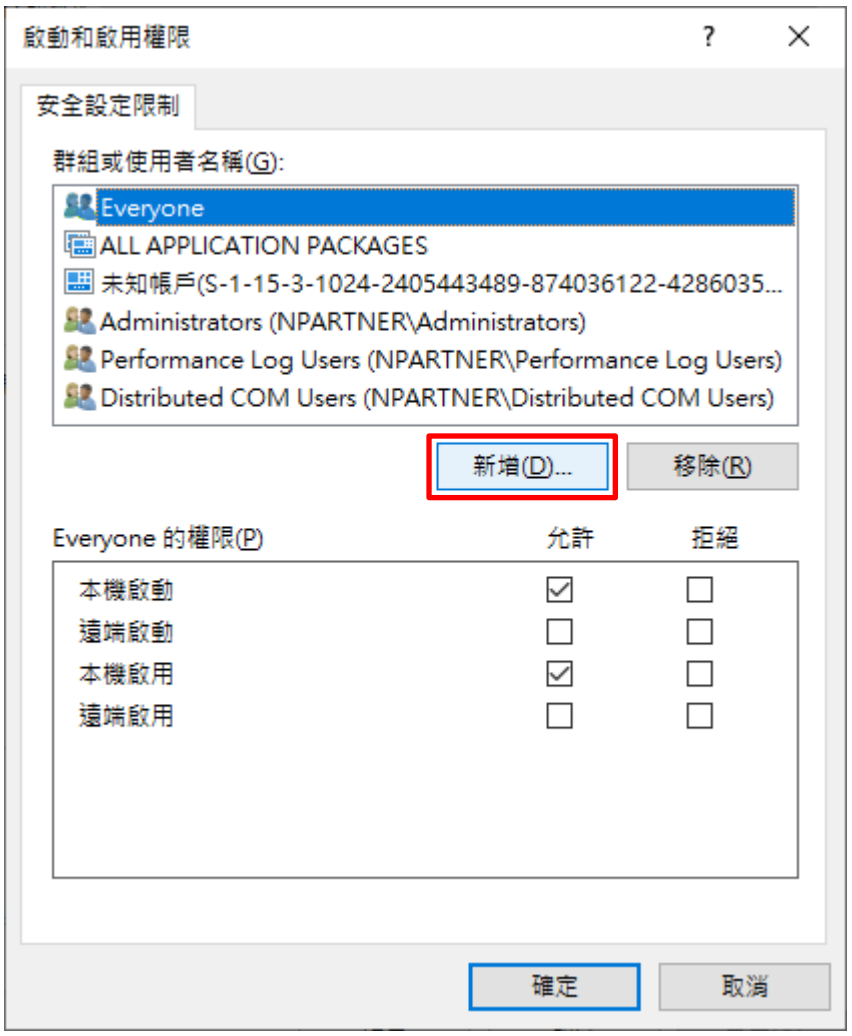


(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]

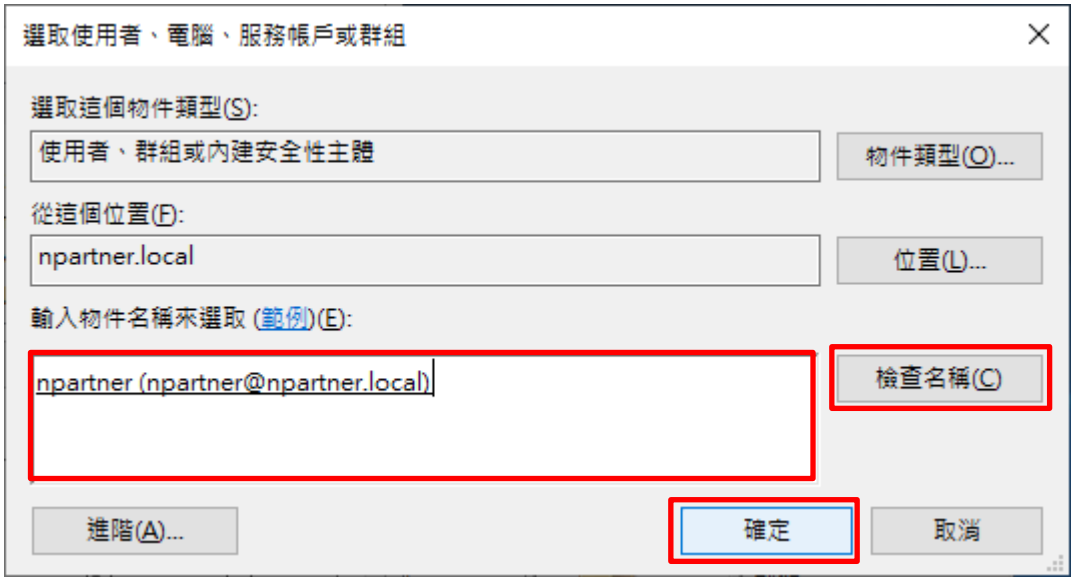
(5) 新增 DCOM 使用者權限

點選 [新增]



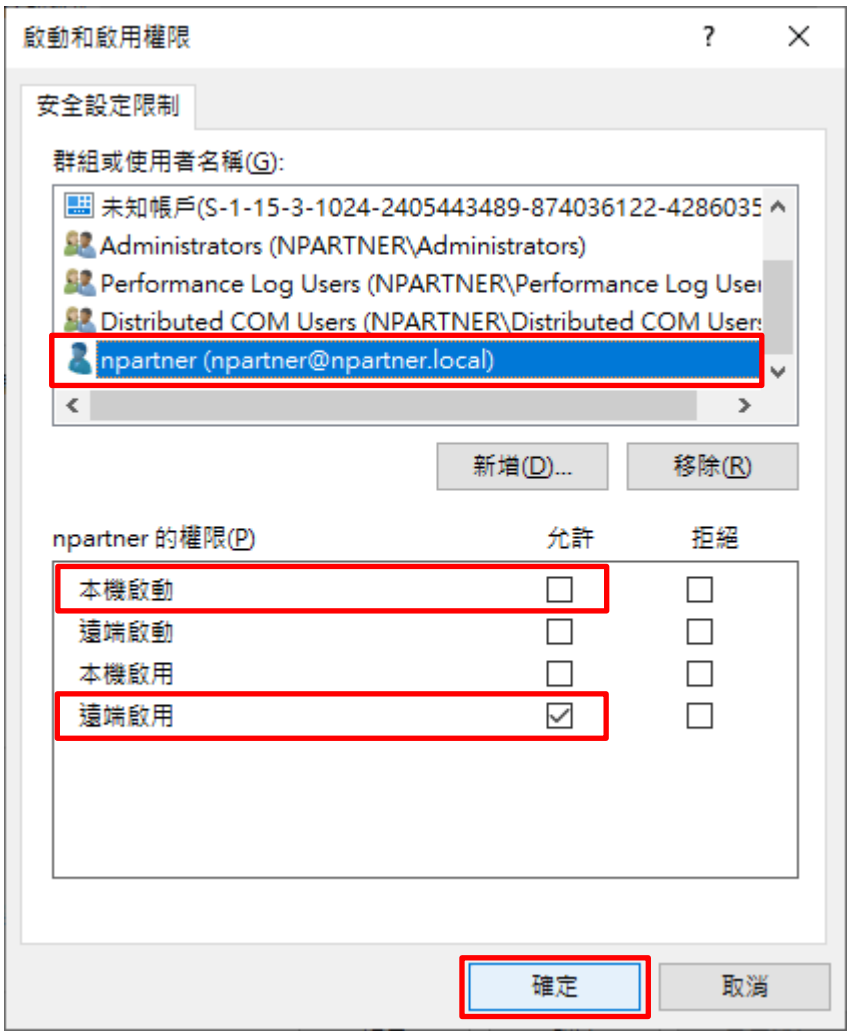
(6) 輸入使用者

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

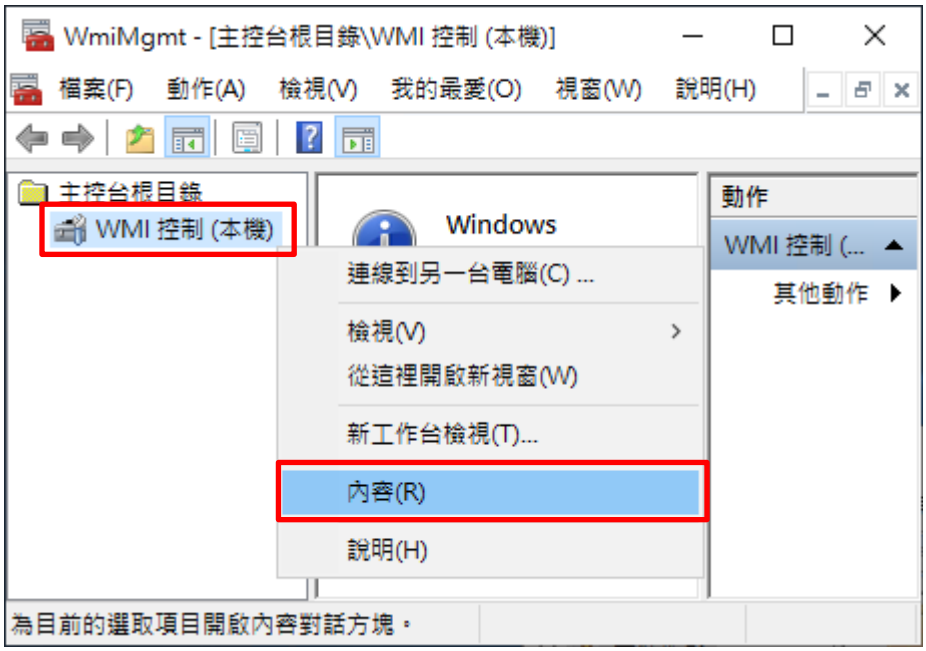
(1) 開啟 [Windows PowerShell]

(2) 開啟元件服務

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

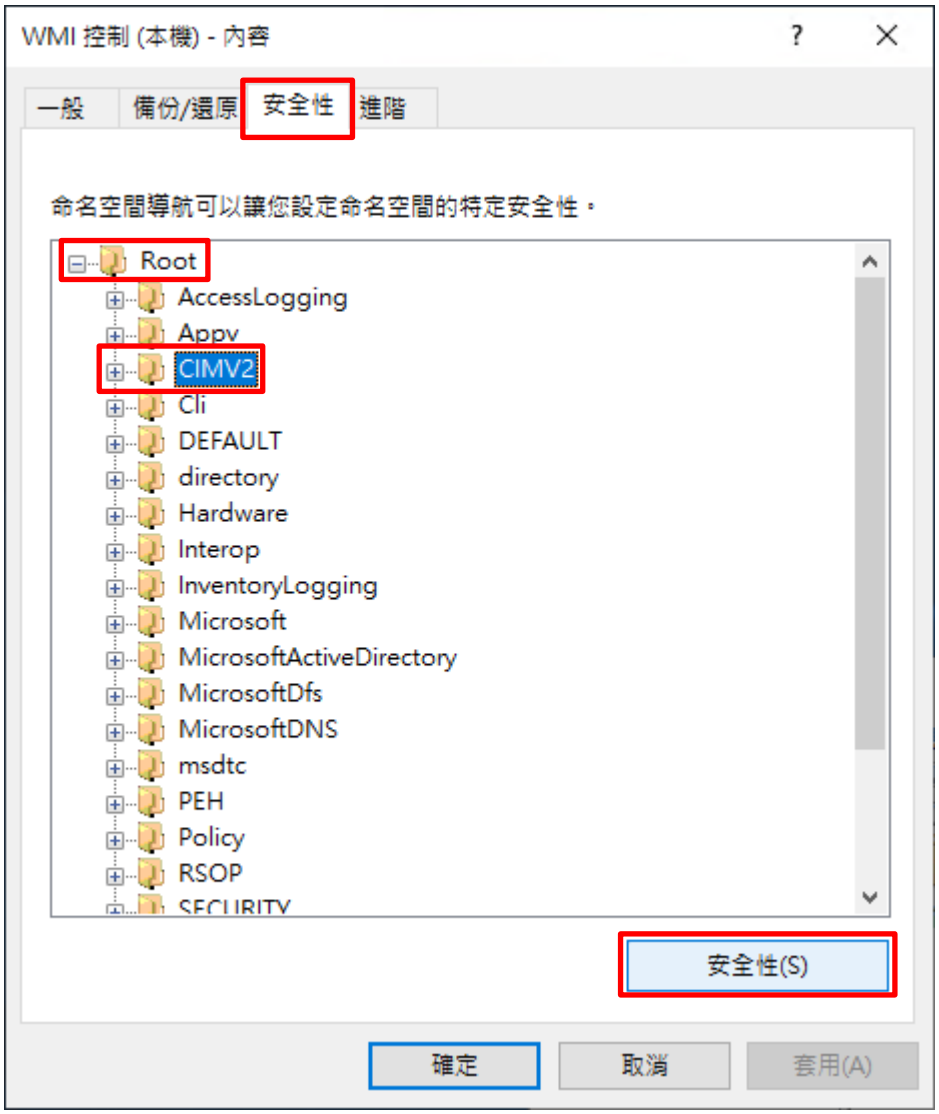
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



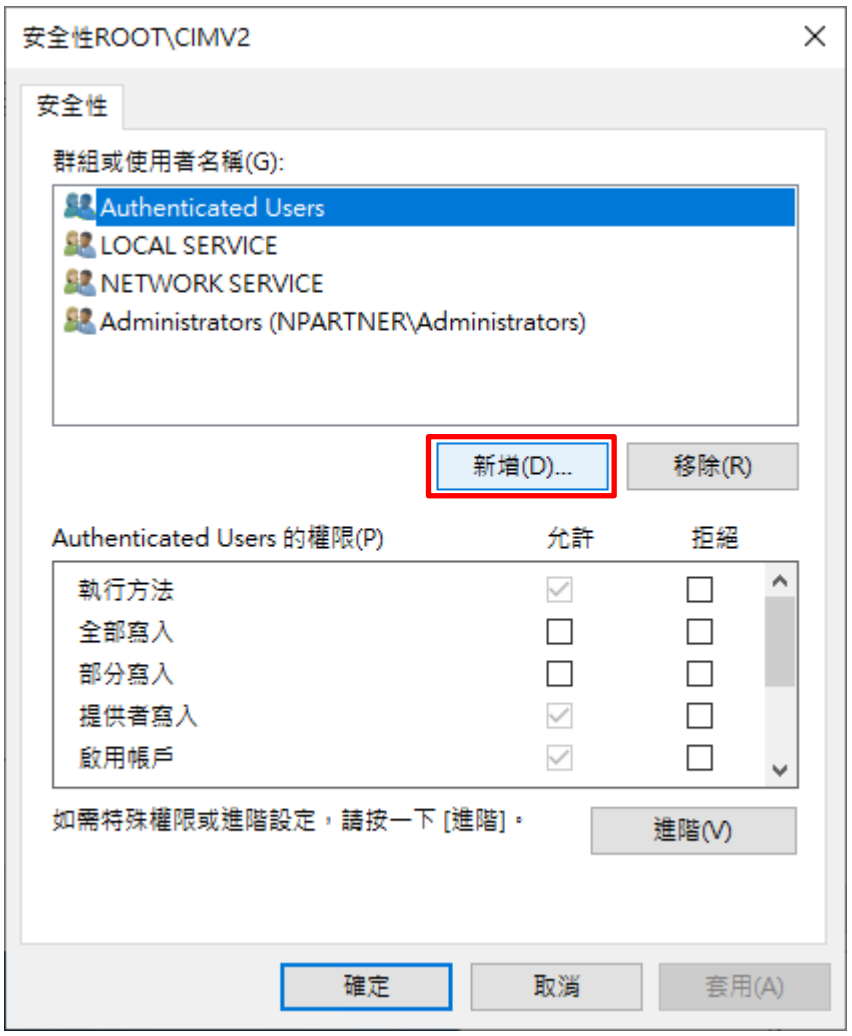
(4) 編輯 CIMV2 安全性

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]

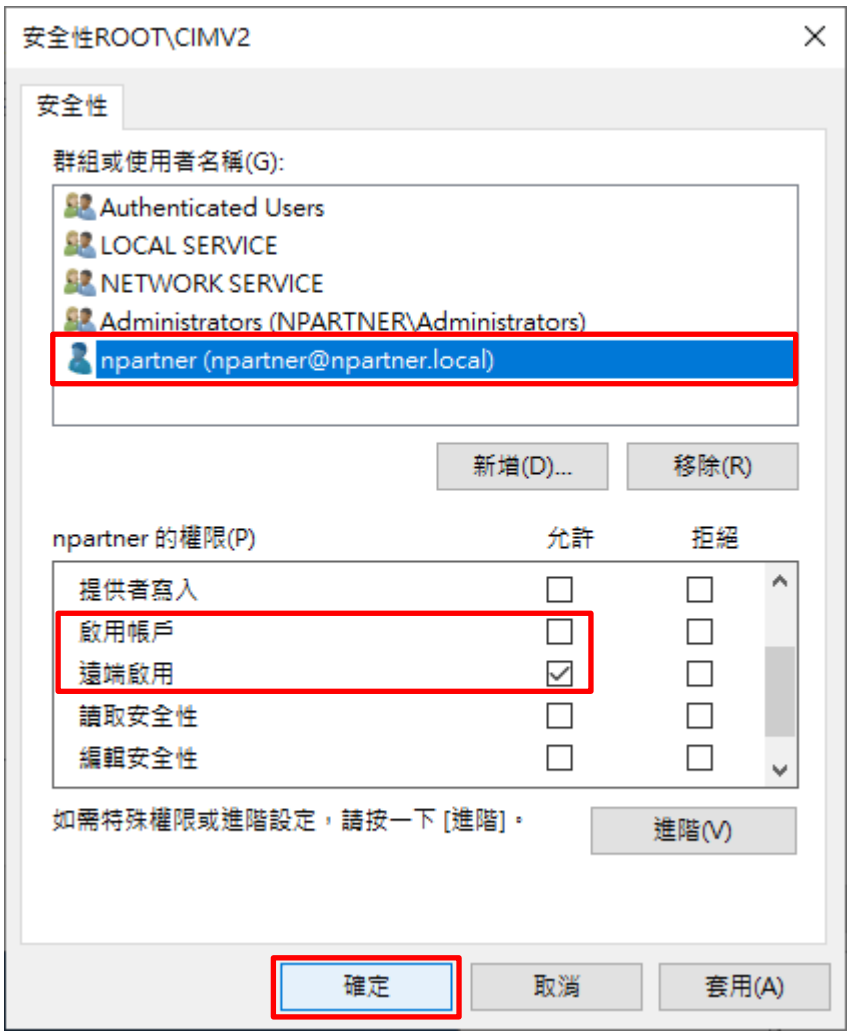


(6) 輸入使用者

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

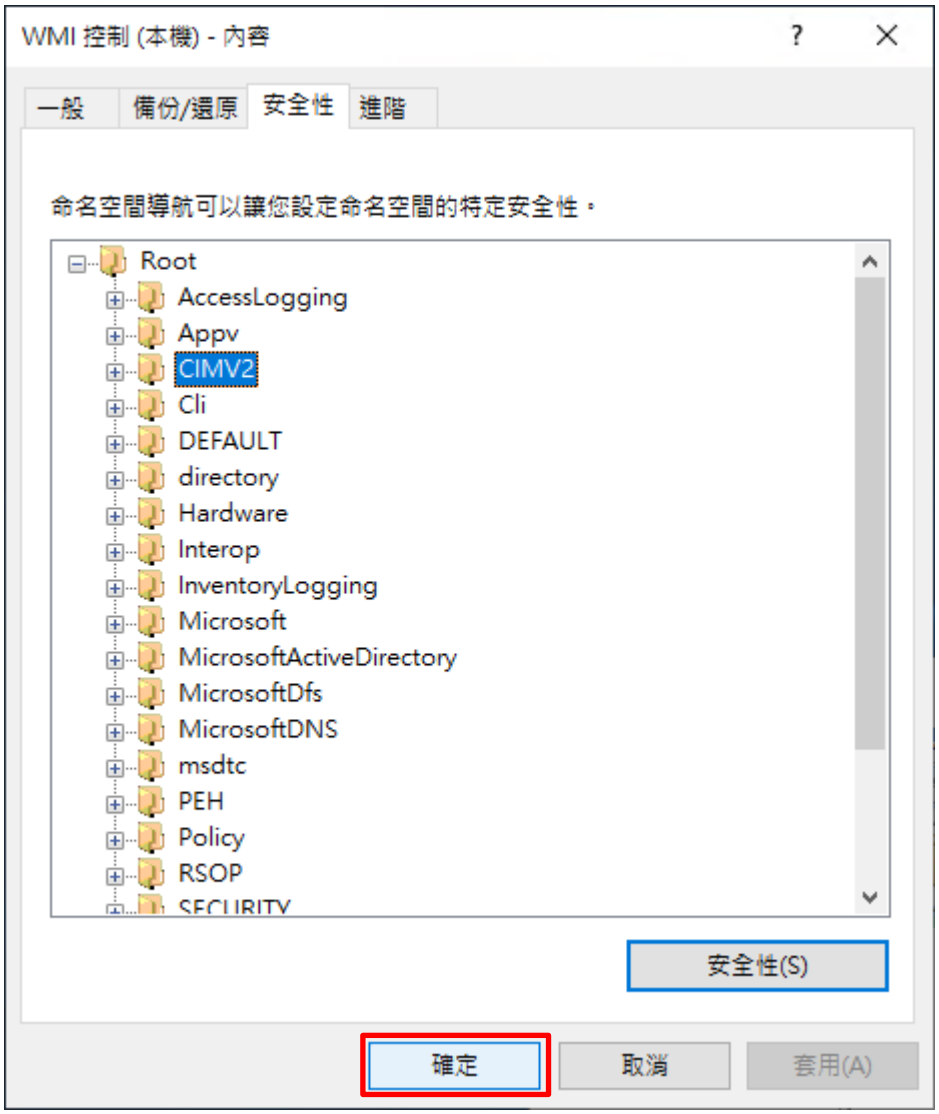
(7) 設定使用者權限

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]

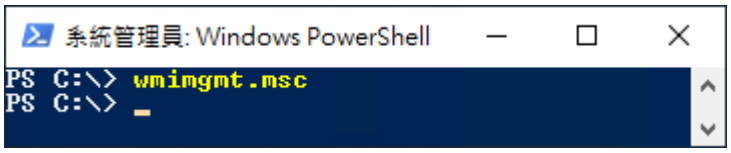


7.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

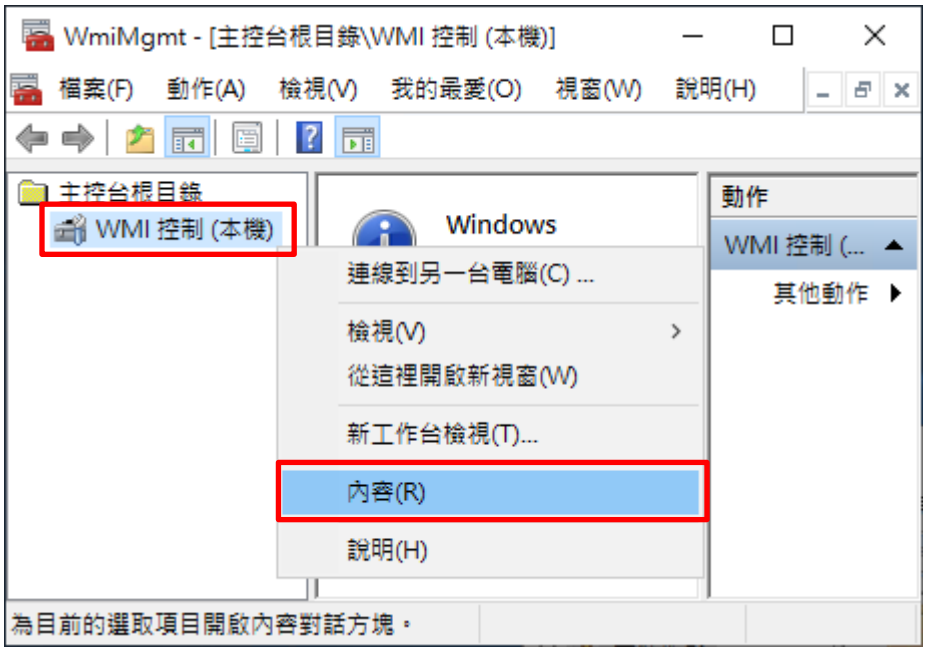
(2) 開啟元件服務

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



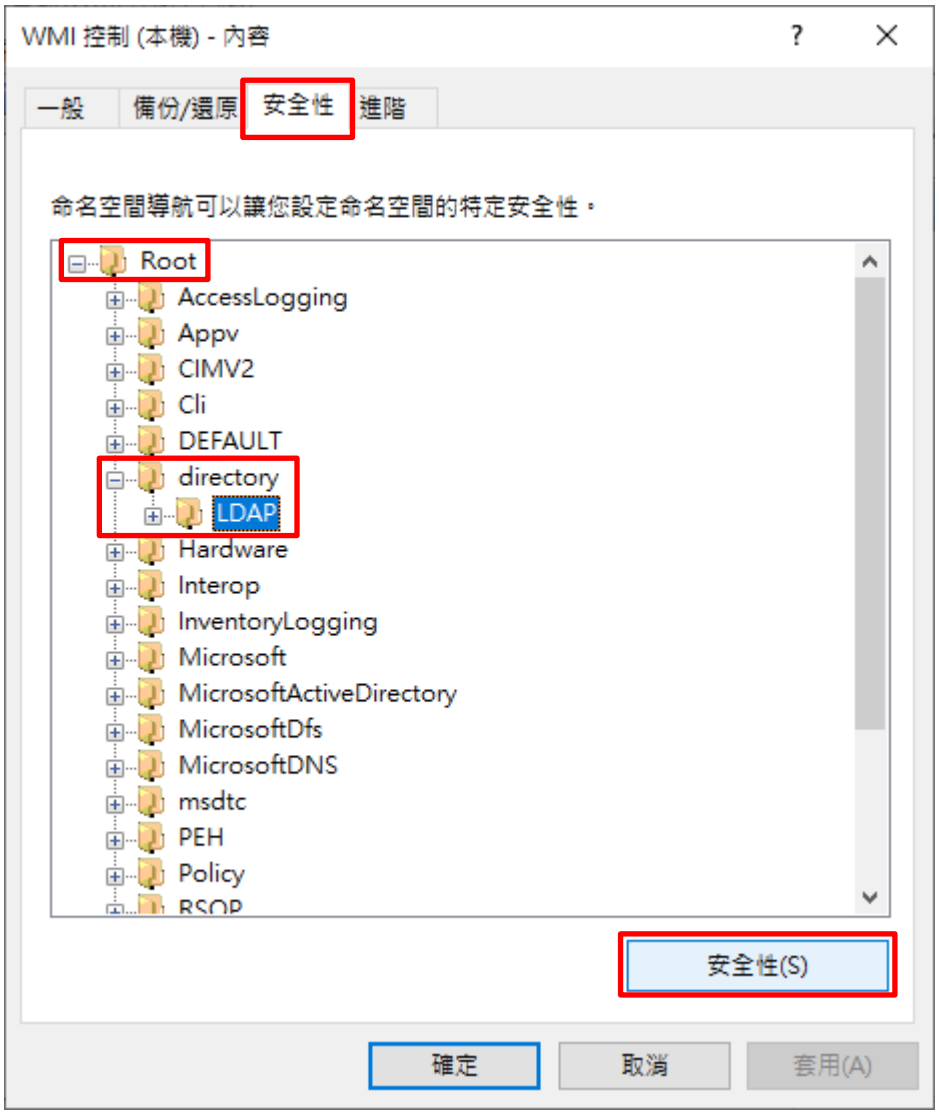
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



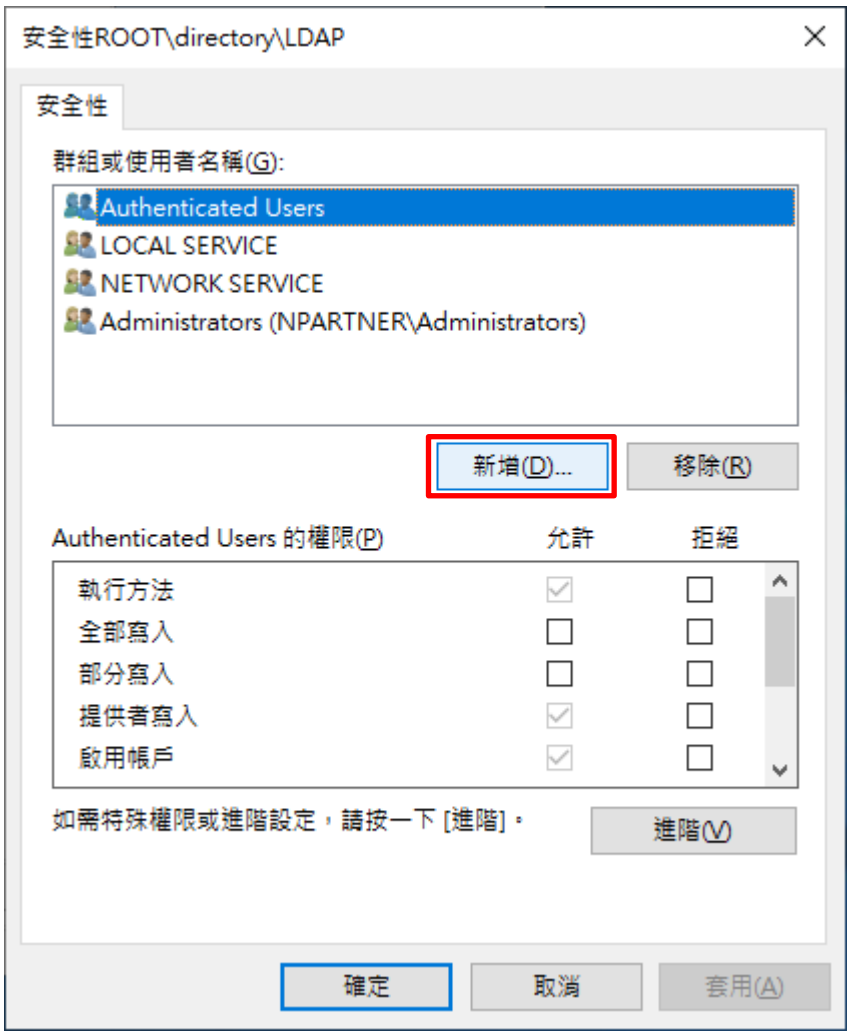
(4) 編輯 LDAP 安全性

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]

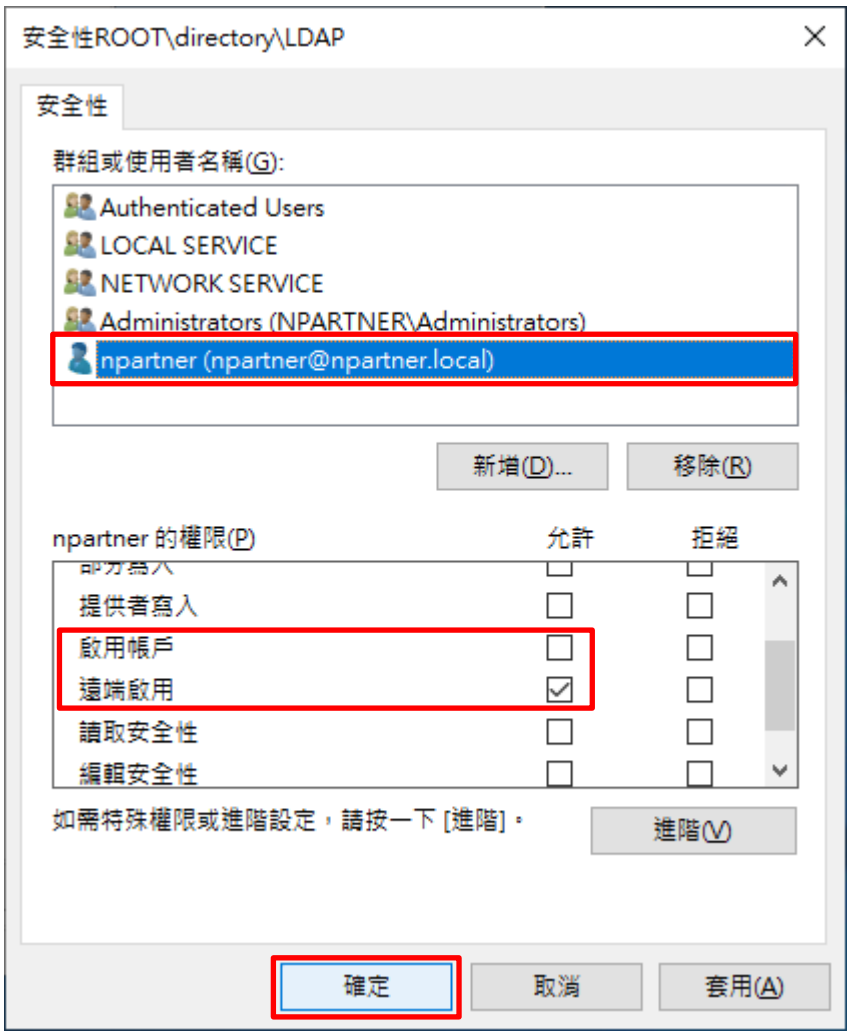


(6) 輸入使用者

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

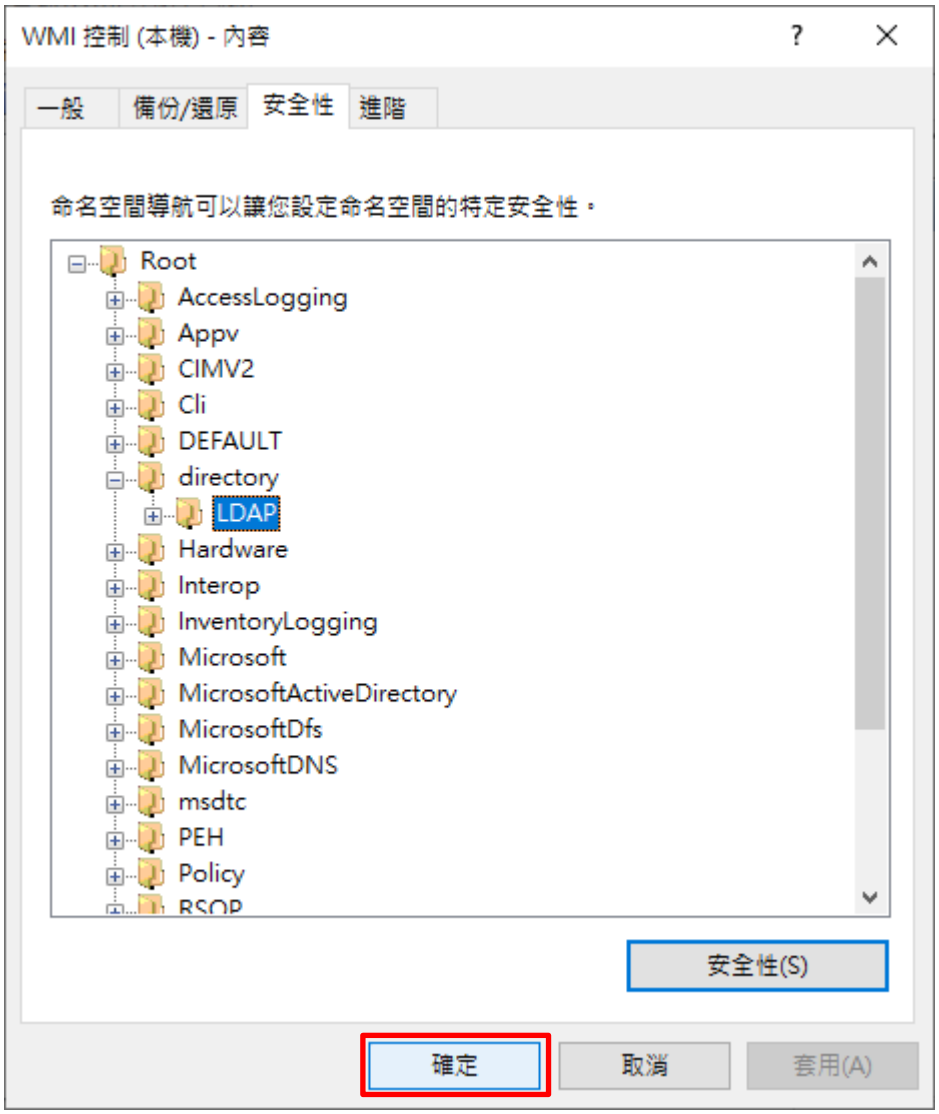
(7) 設定使用者權限

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

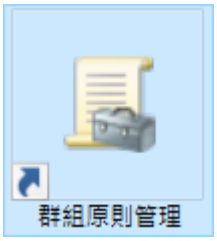
按 [確定]



7.3.4 設定 Event log 讀取權限

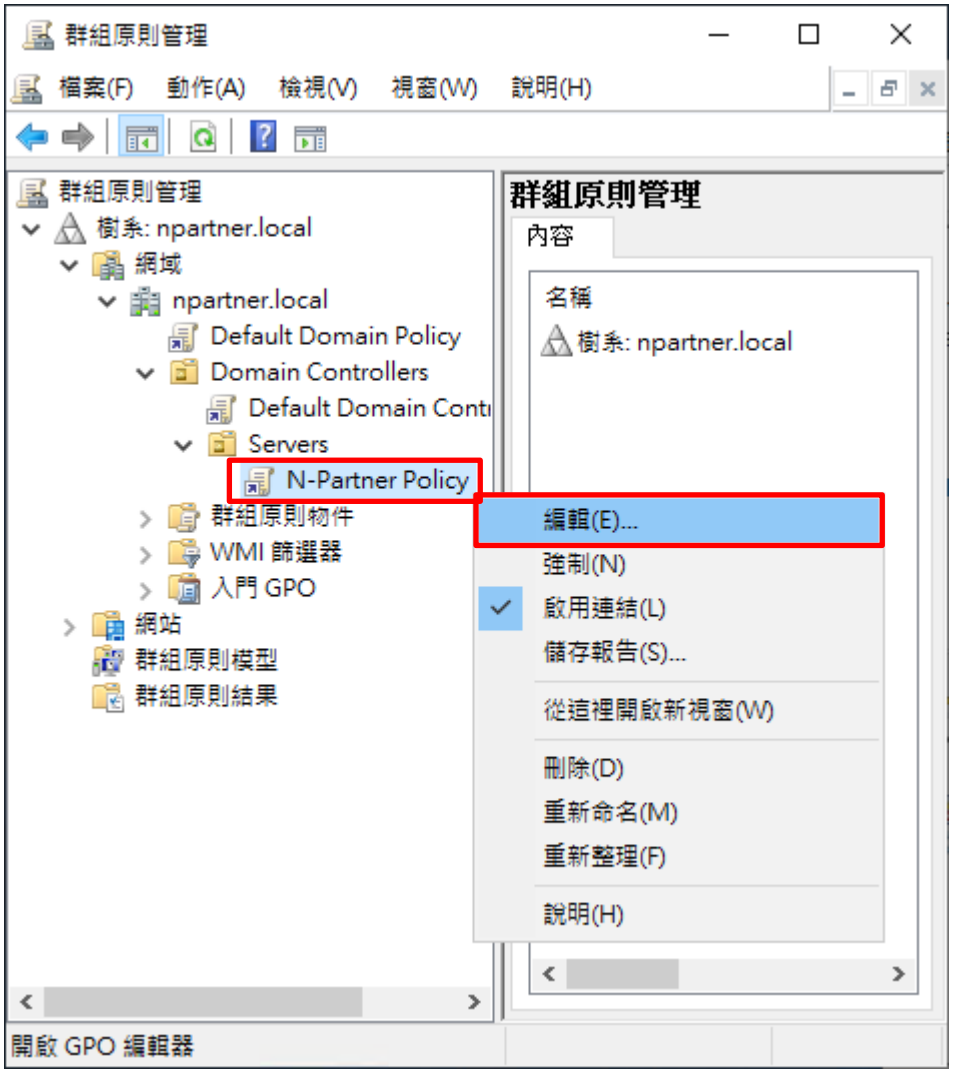
(1) 開啟群組原則管理

開啟 [群組原則管理]



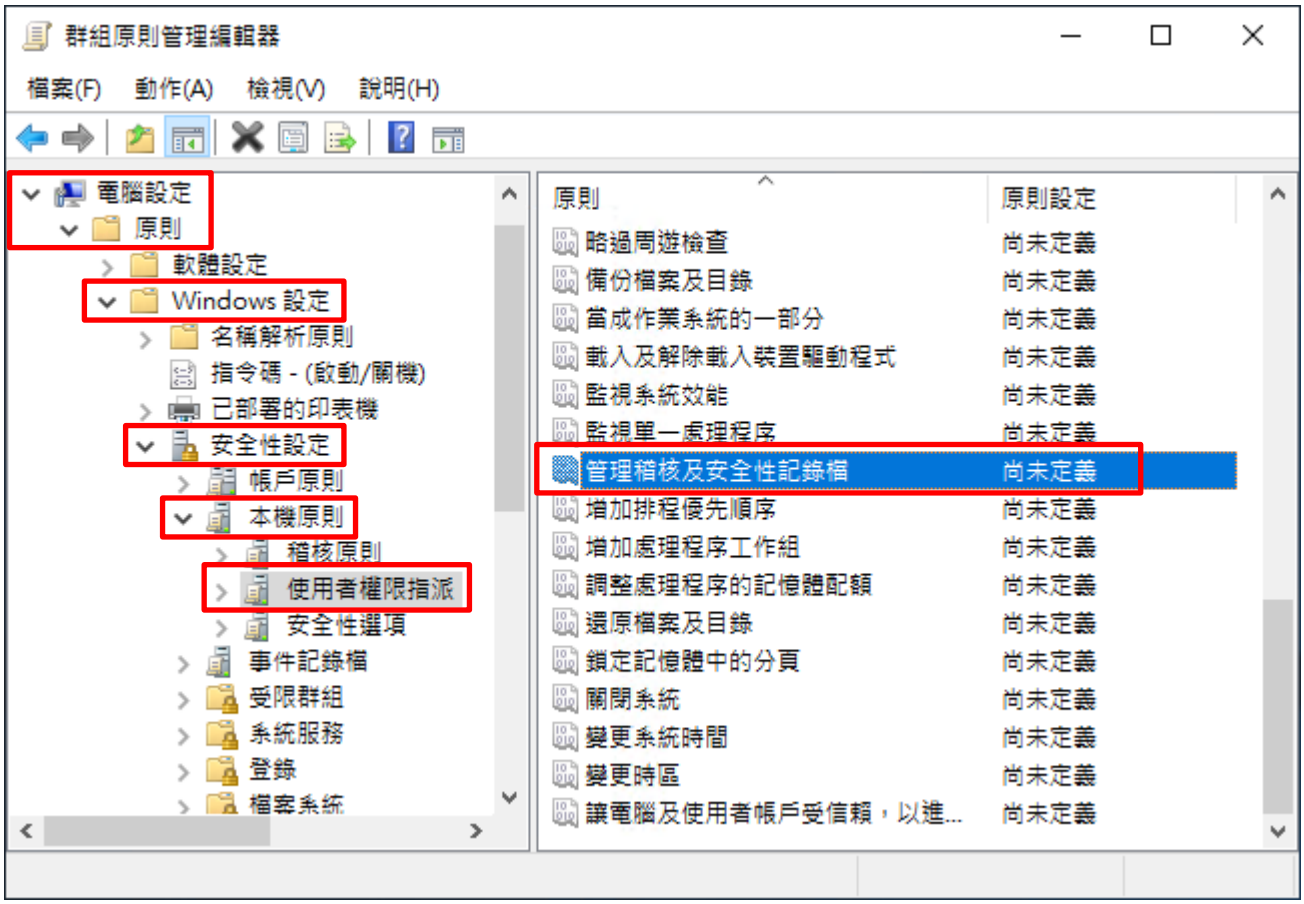
(2) 編輯群組原則物件

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

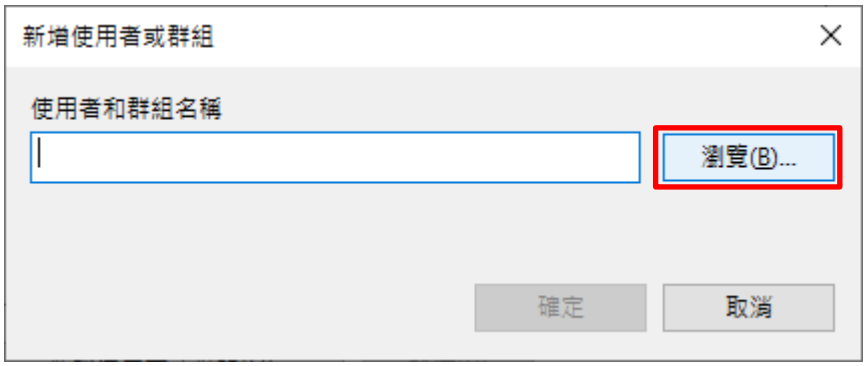


(4) 新增管理稽核使用者

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

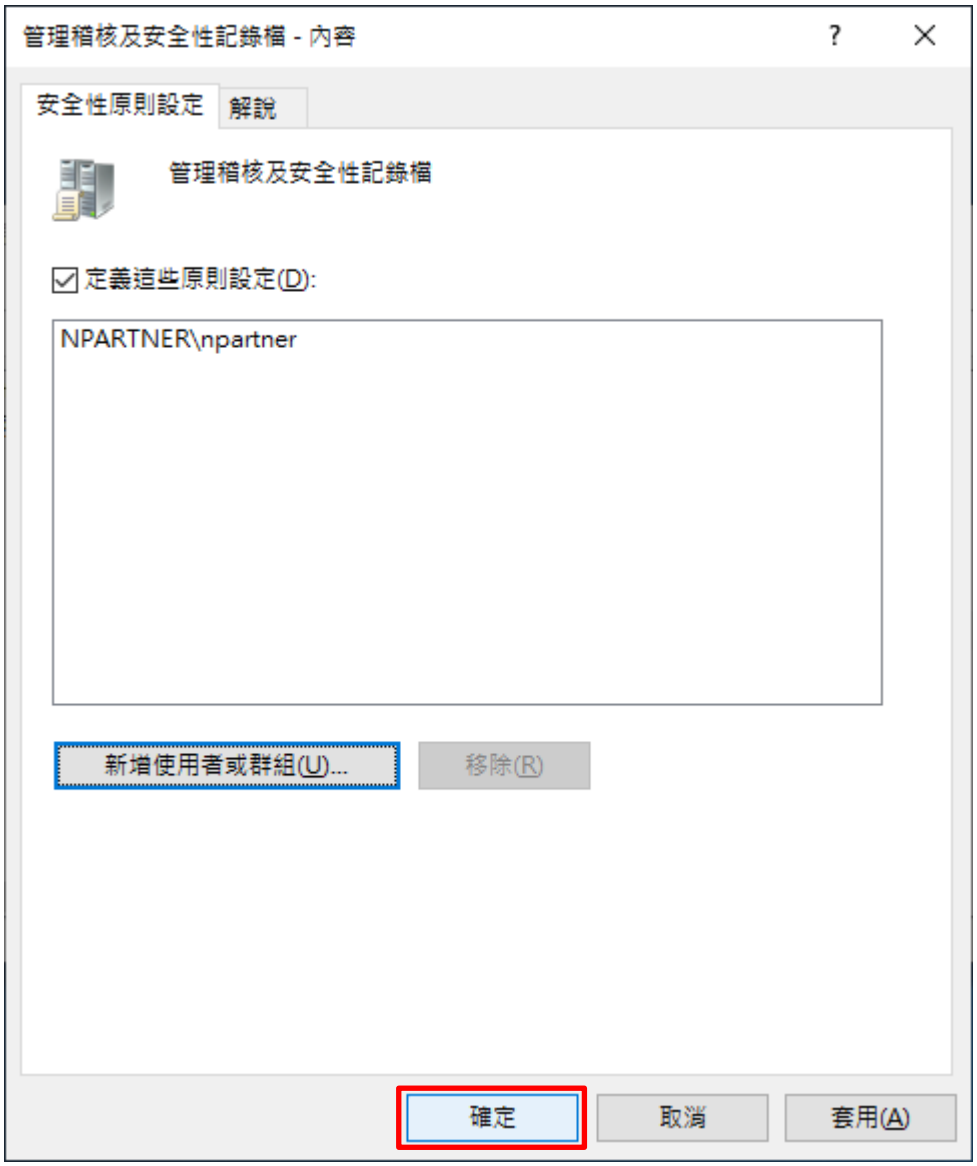
輸入使用者帳號: npartner -> 點選 [檢查名稱] -> 按 [確定]

(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:\> Invoke-GPUpdate -RandomDelayInMinutes 0 -Force
```

7.3.5 重啟 WMI 服務

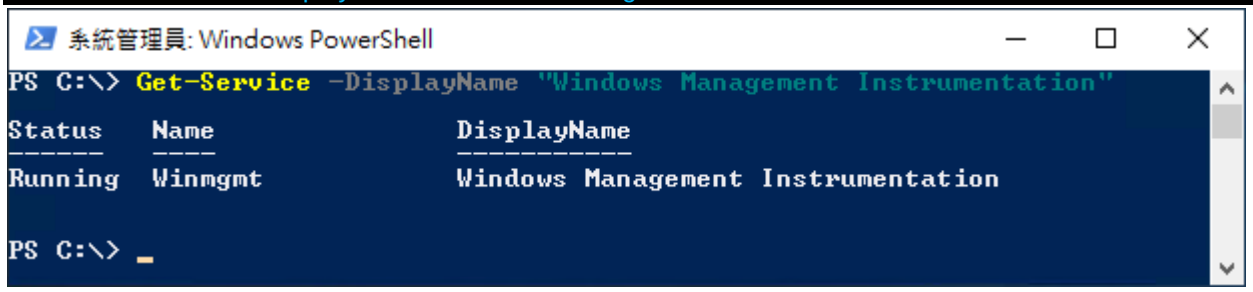
(1) 開啟 [Windows PowerShell]

(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]

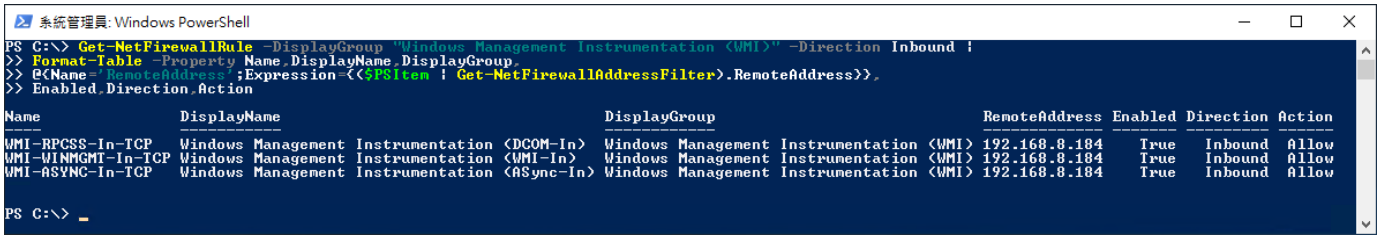
(2) 設定防火牆，只允許 N-Reporter IP query WMI

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

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
```



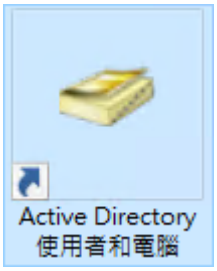
8. Windows 2022

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

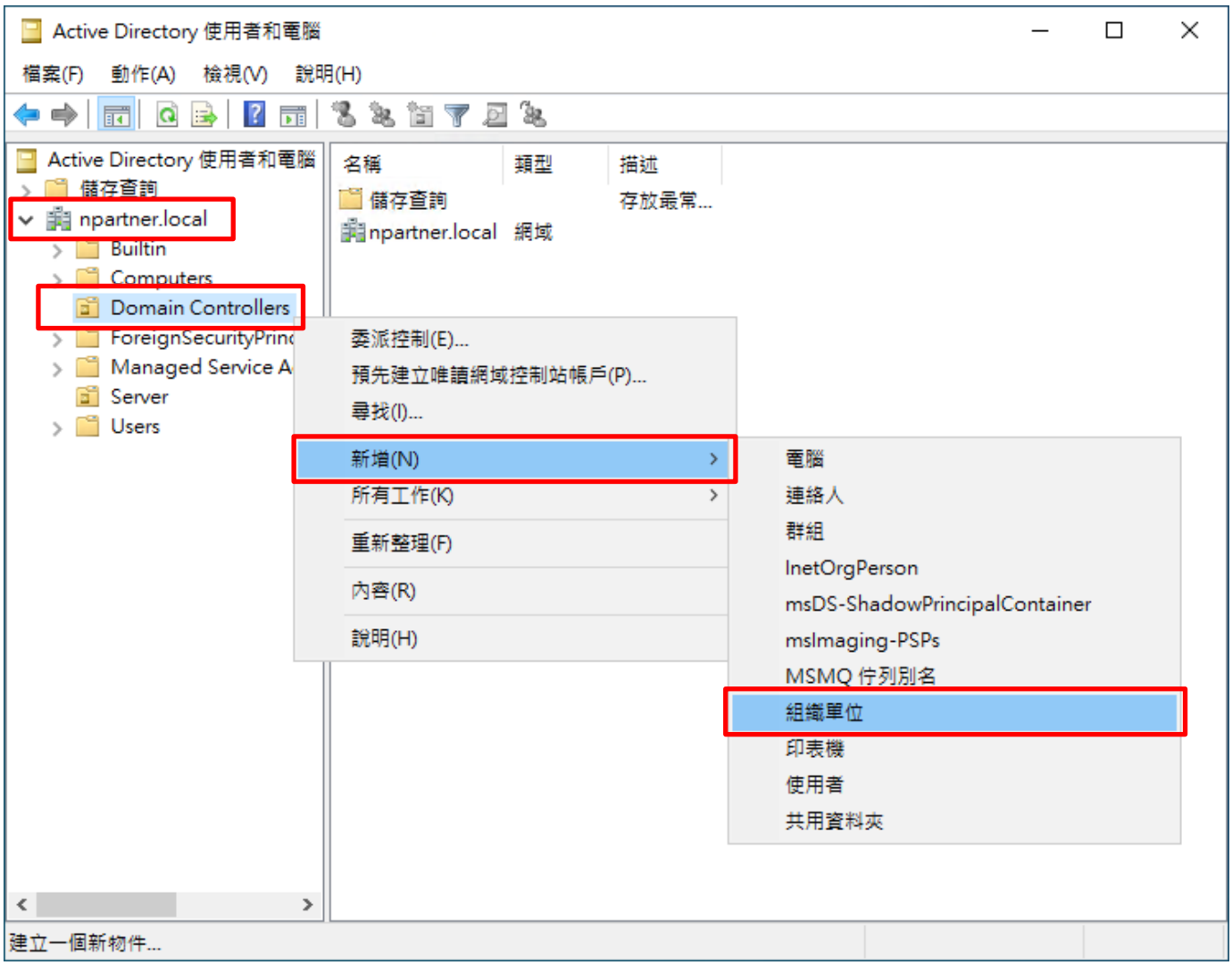
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



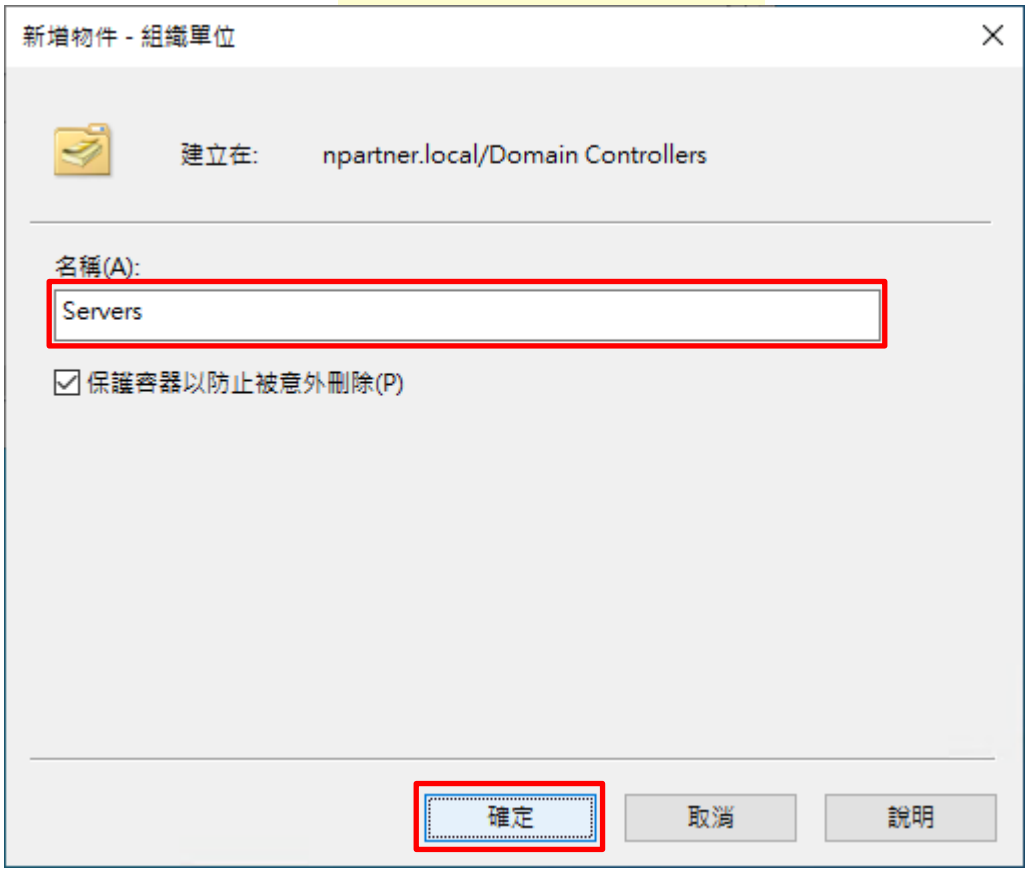
(2) 新增組織單位

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]



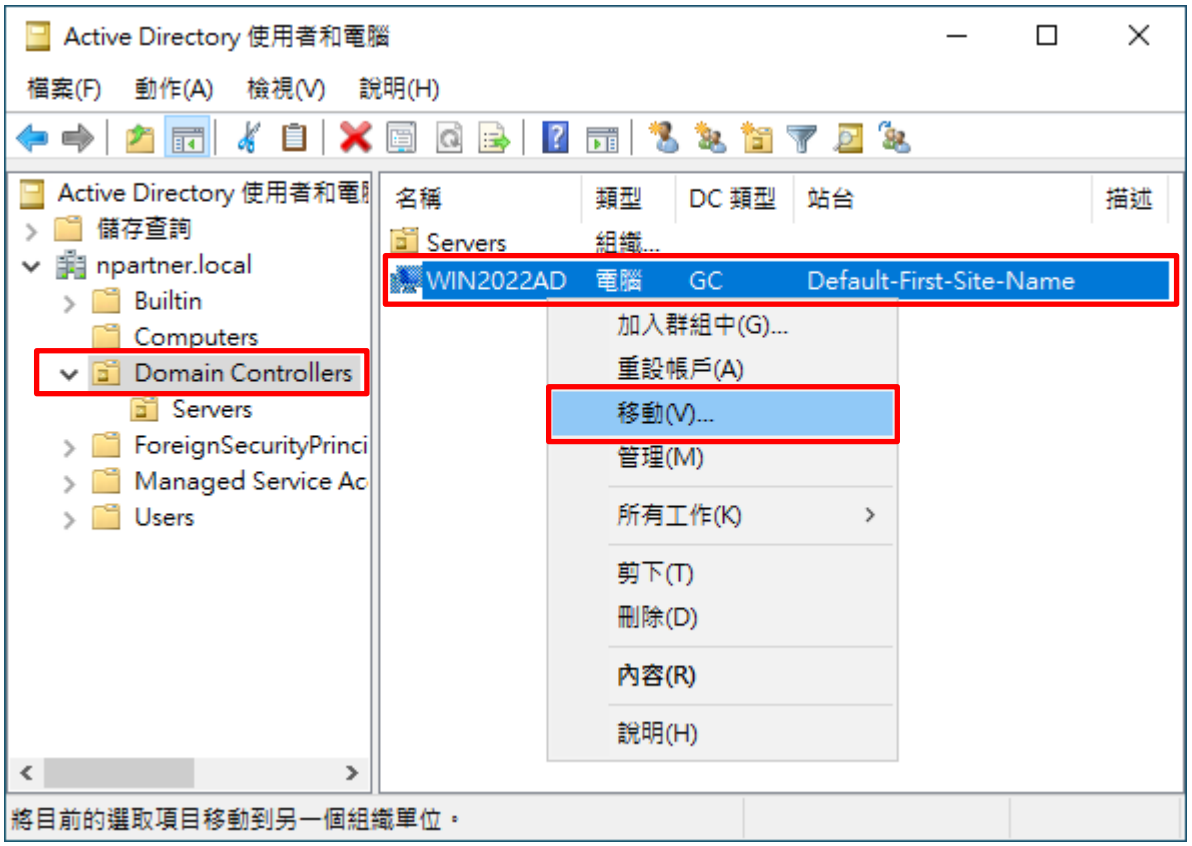
(3) 輸入組織單位名稱

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]



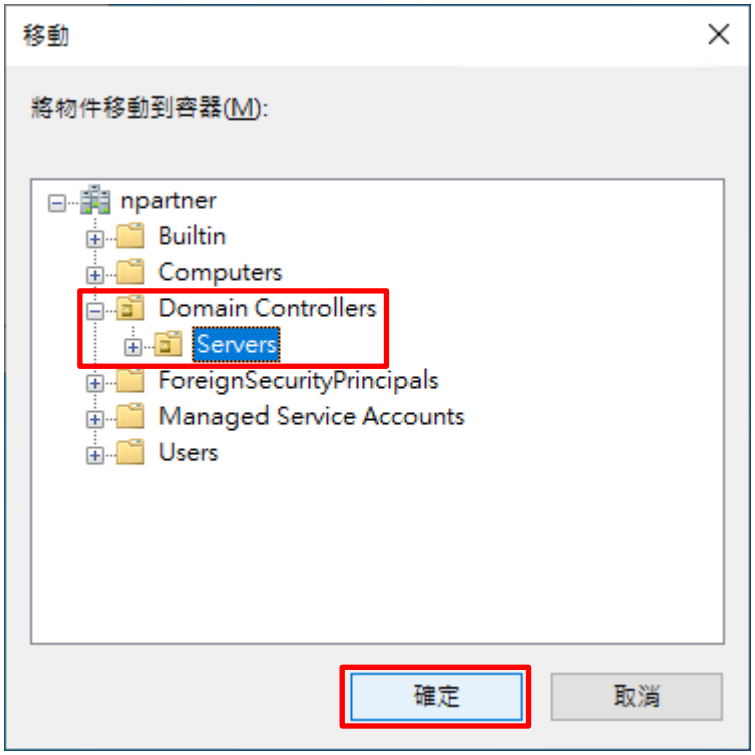
(4) 移動伺服器至新的組織單位

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]



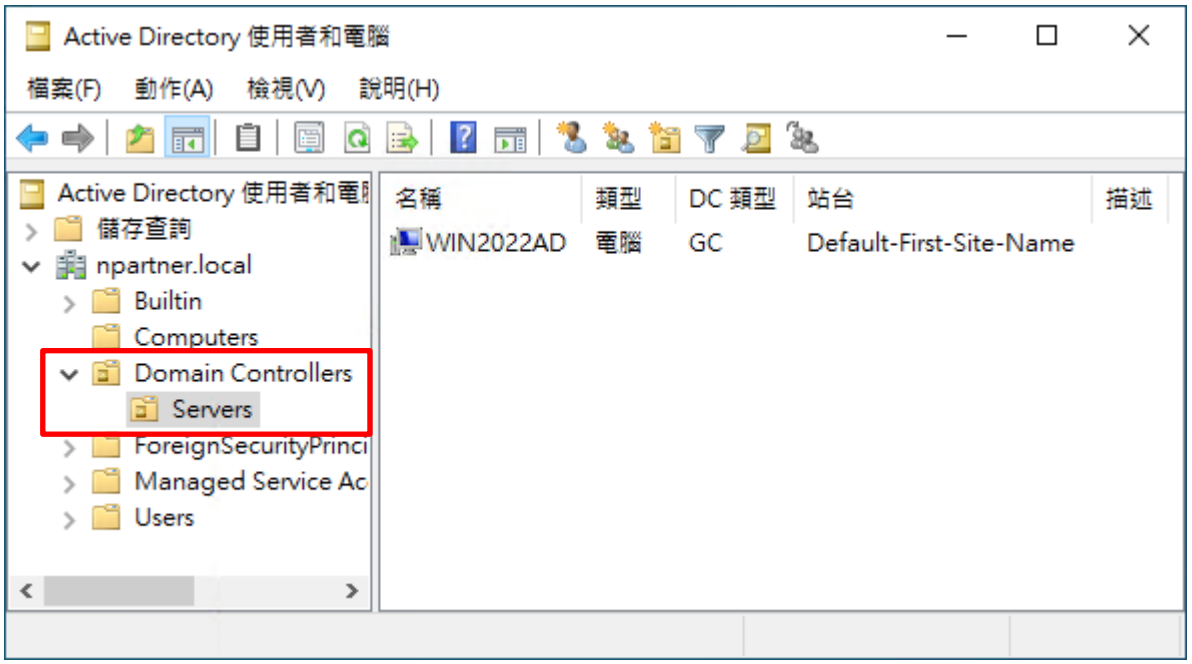
(5) 選擇組織單位

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

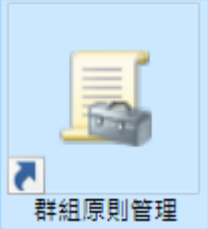
點選 [Domain Controllers] 的 [Servers] 組織單位，確認 [Win2022AD] 網域伺服器已移動。



8.2 群組原則設定

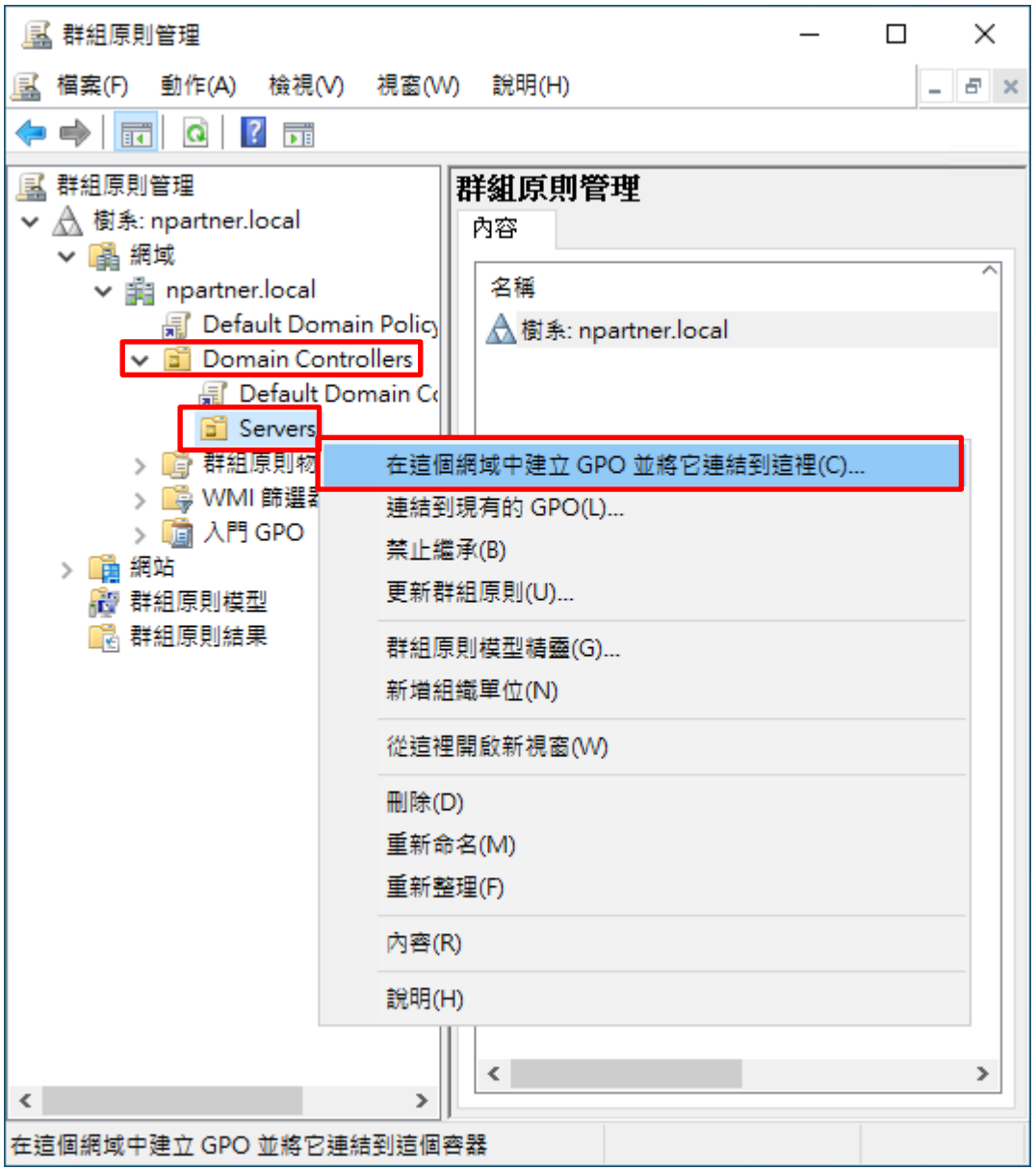
(1) 開啟群組原則管理

開啟 [群組原則管理]



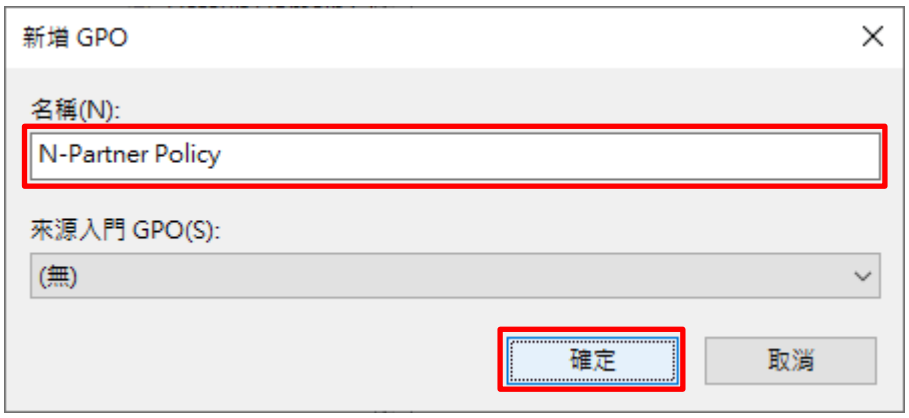
(2) 在 Servers 組織單位，新增群組原則物件

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...]



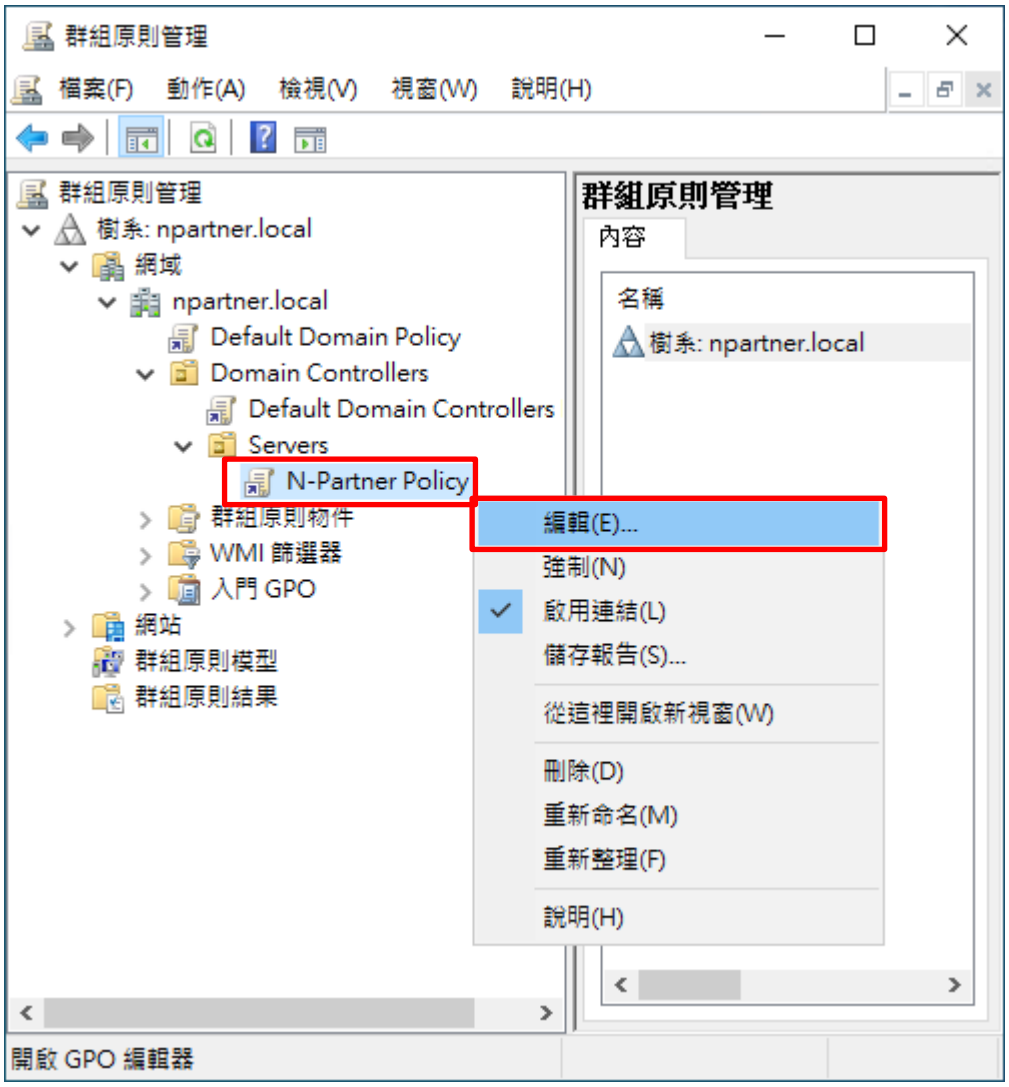
(3) 輸入群組原則物件名稱

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]



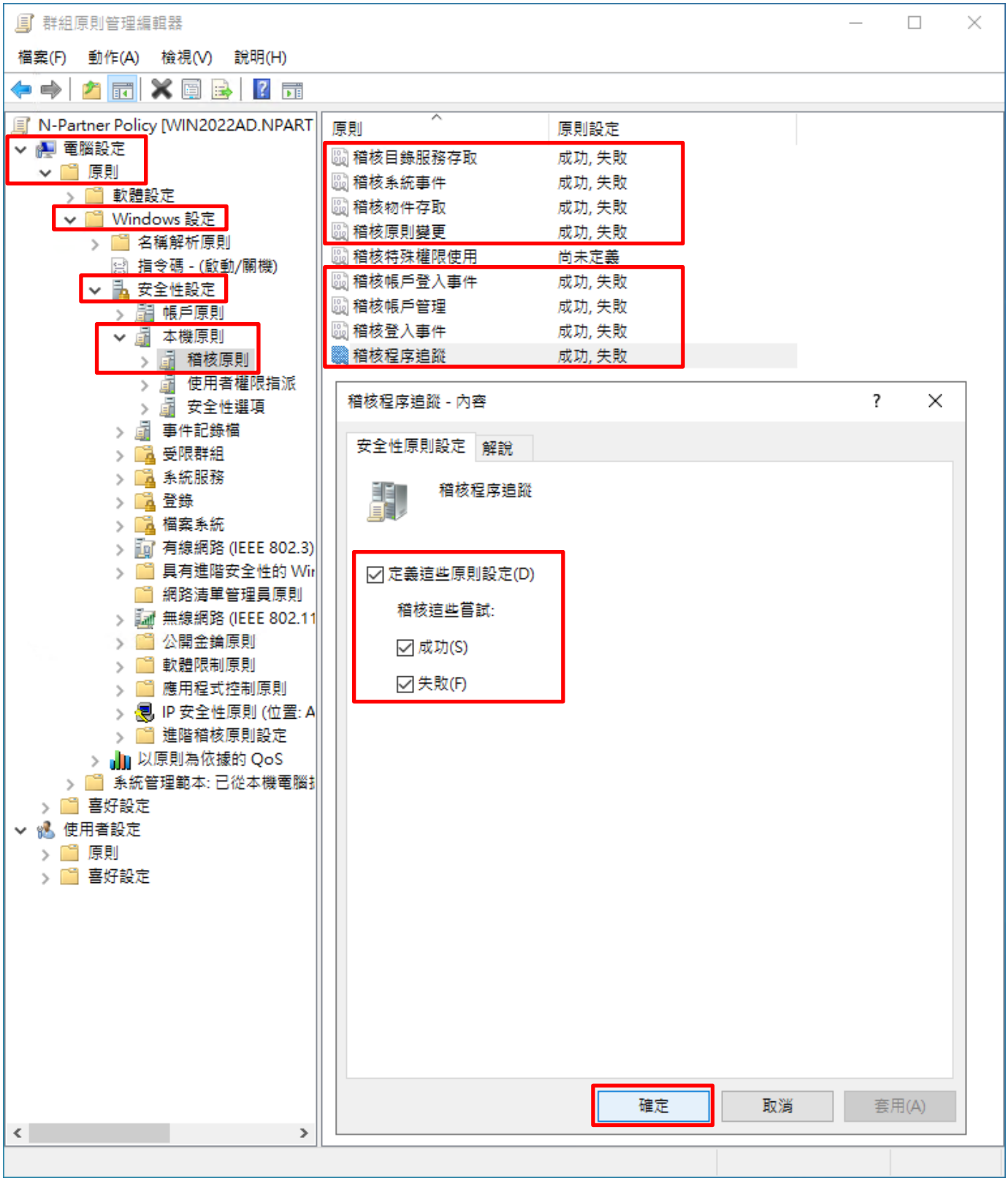
(4) 編輯群組原則物件

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



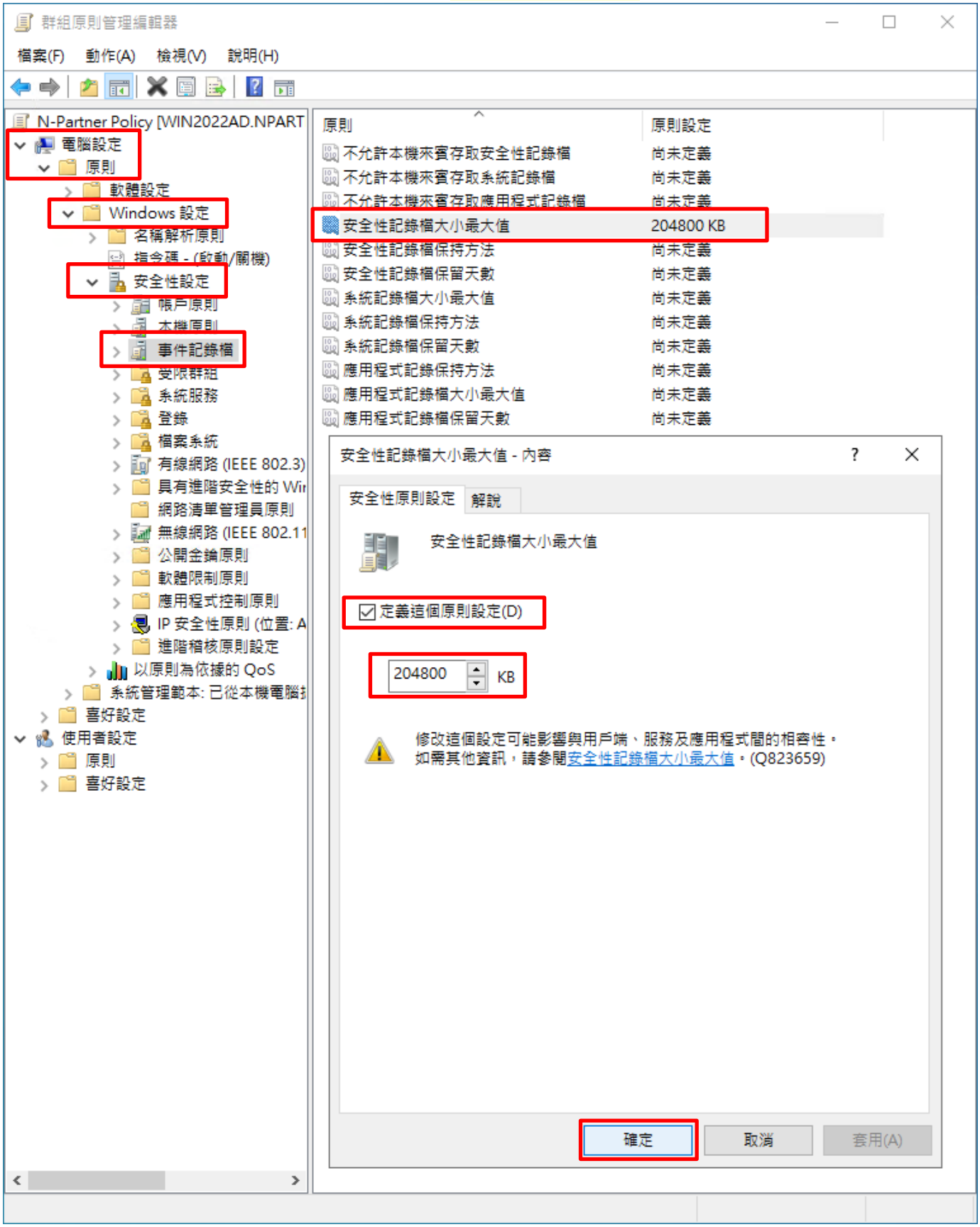
(5) 本機原則：稽核原則

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]



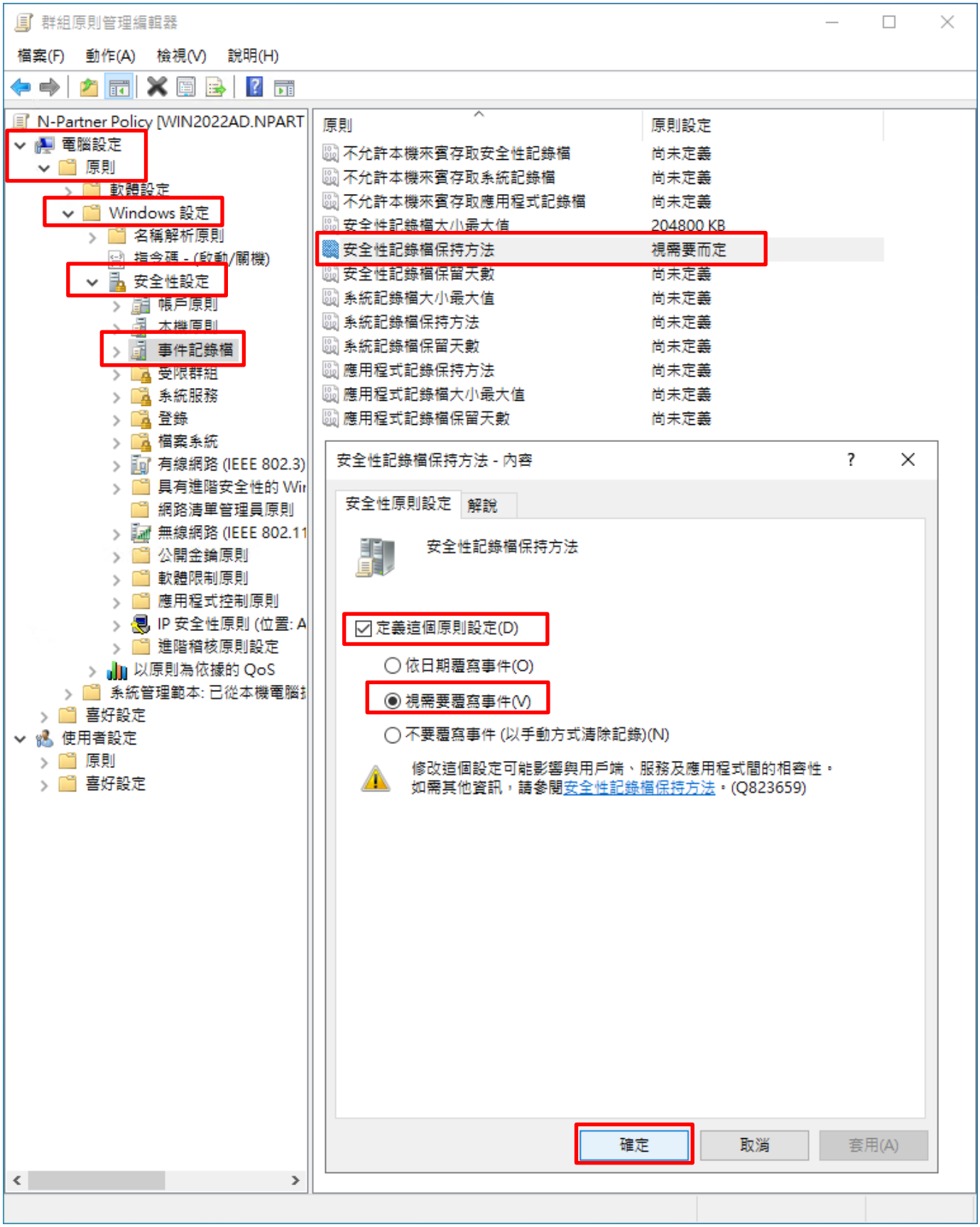
(6) 事件記錄檔：安全性記錄檔大小最大值

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]

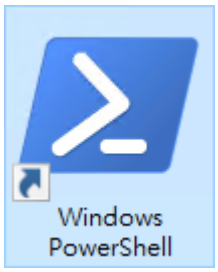


(7) 事件記錄檔：安全性記錄檔保持方法

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]

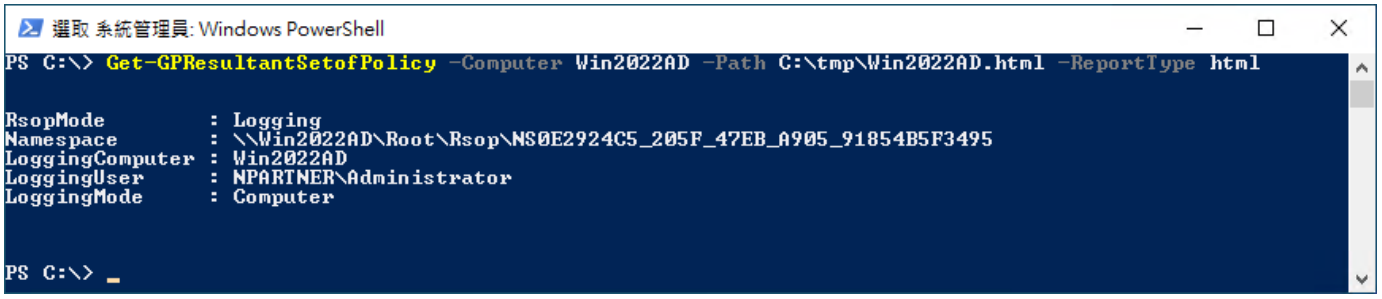


(9) 更新群組原則

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

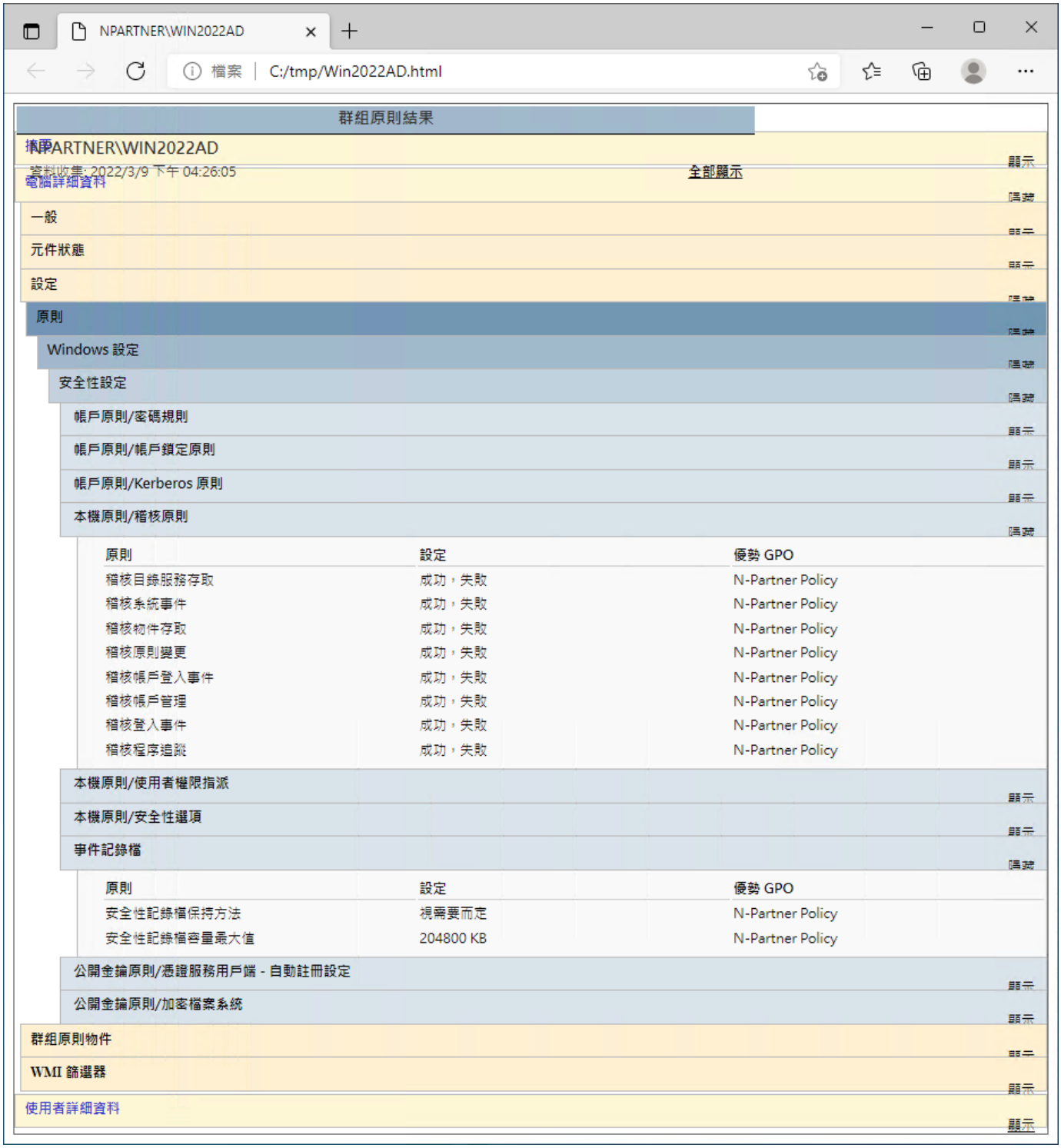
(10) 產生 Windows AD 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2022AD -Path C:\tmp\Win2022AD.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 2022 伺服器，套用 N-Partner Policy 群組原則

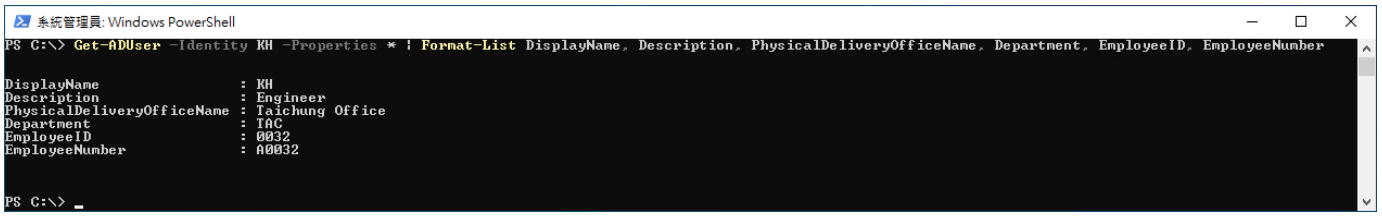


8.3 設定 WMI

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
```



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 

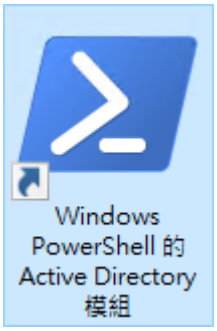
等級	事件	次數	事件型態	來源使用者名稱	目的使用者名稱	Policy ID	Audit User	分類
Notice	<13>Mar 9 21:56:47 WIN-OS55N6KF7BJ.npartner.local Microsoft-Windows-Security-Auditing[616]: Microsoft-Windows-Security-Auditing: 4724: An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-3283165886-1174691238-2893489689-500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

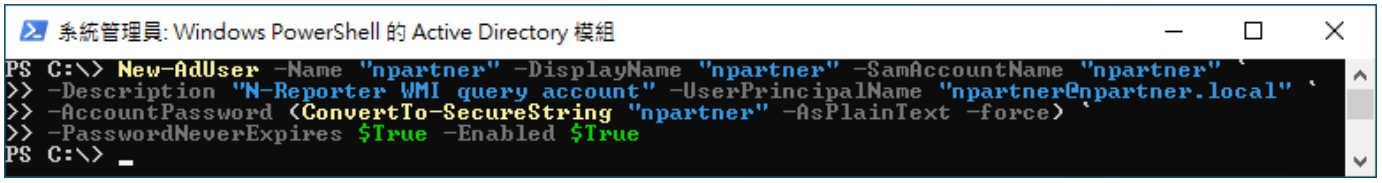
8.3.1 新增非管理帳號

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



(2) 新增帳號

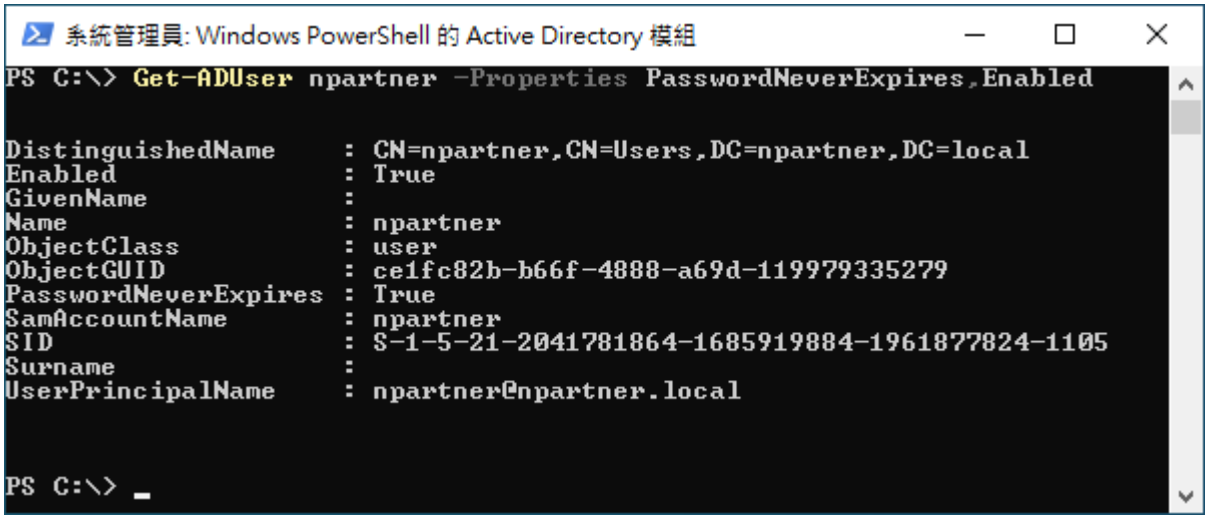
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



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
```

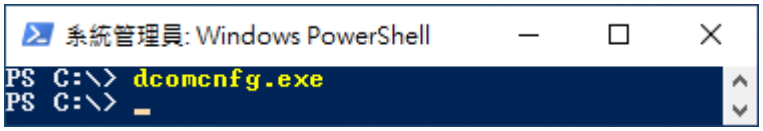


8.3.2 設定 DCOM 權限

(1) 開啟 [Windows PowerShell]

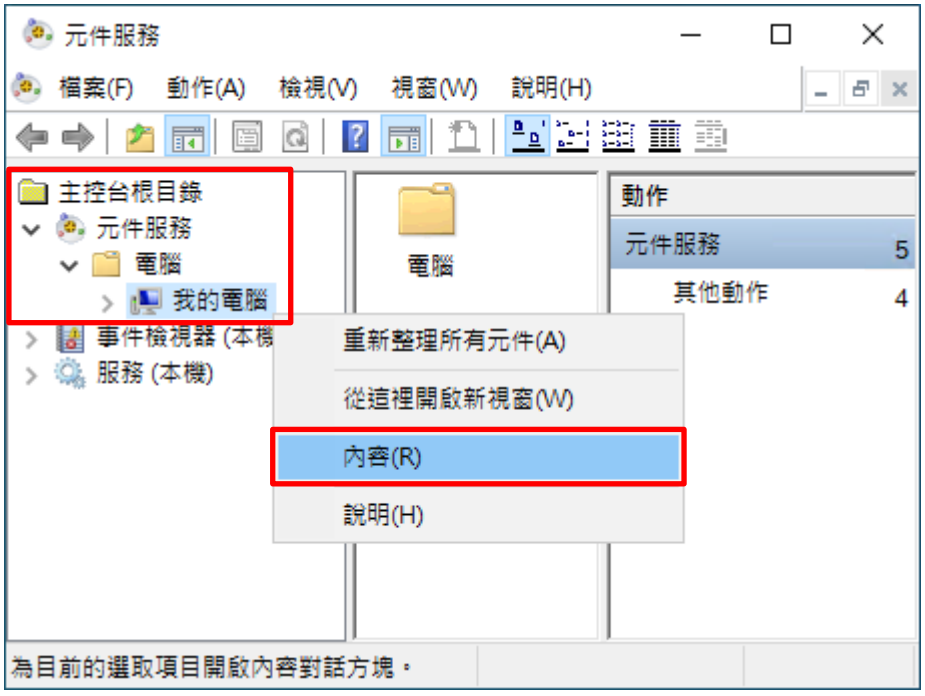
(2) 開啟元件服務

```
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]

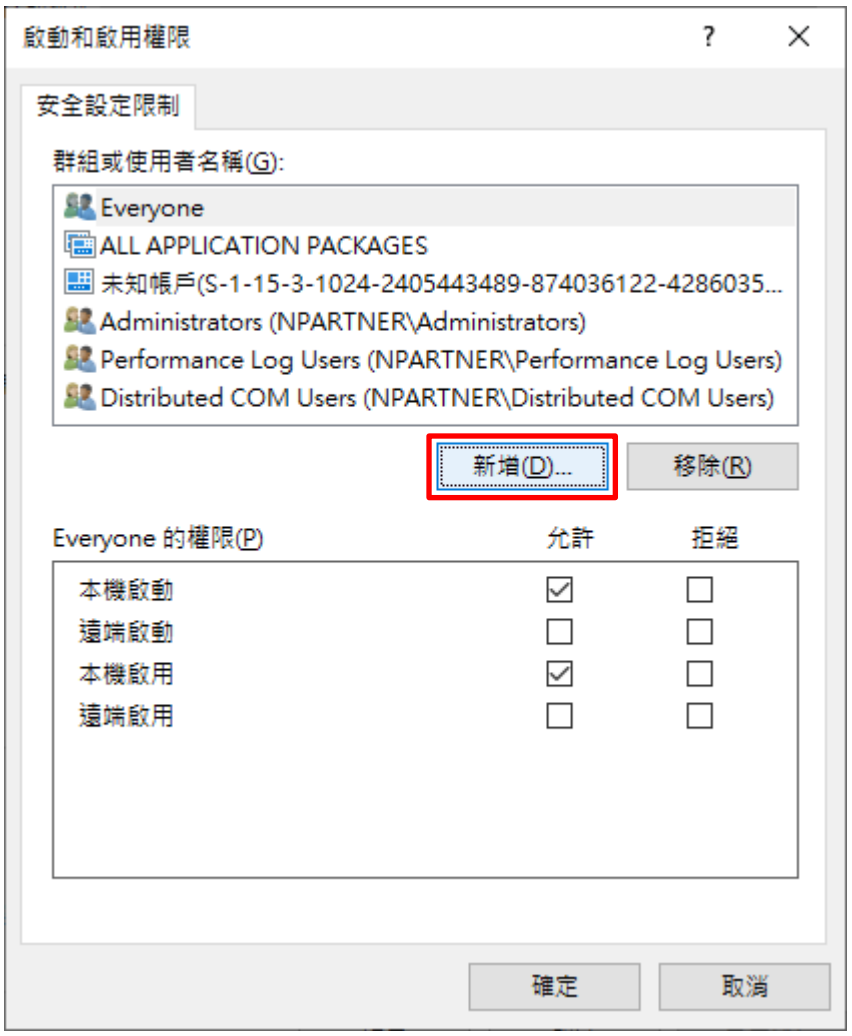


(4) 啟用權限

點選 [COM 安全性] 頁面 -> 啟動和啟用權限，按 [編輯限制]

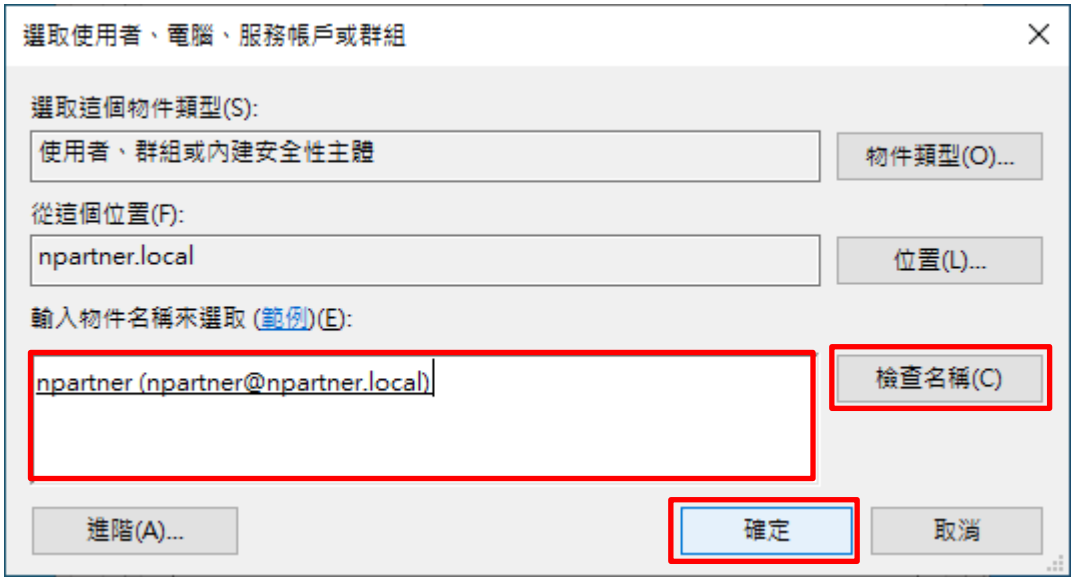
(5) 新增 DCOM 使用者權限

按 [新增]



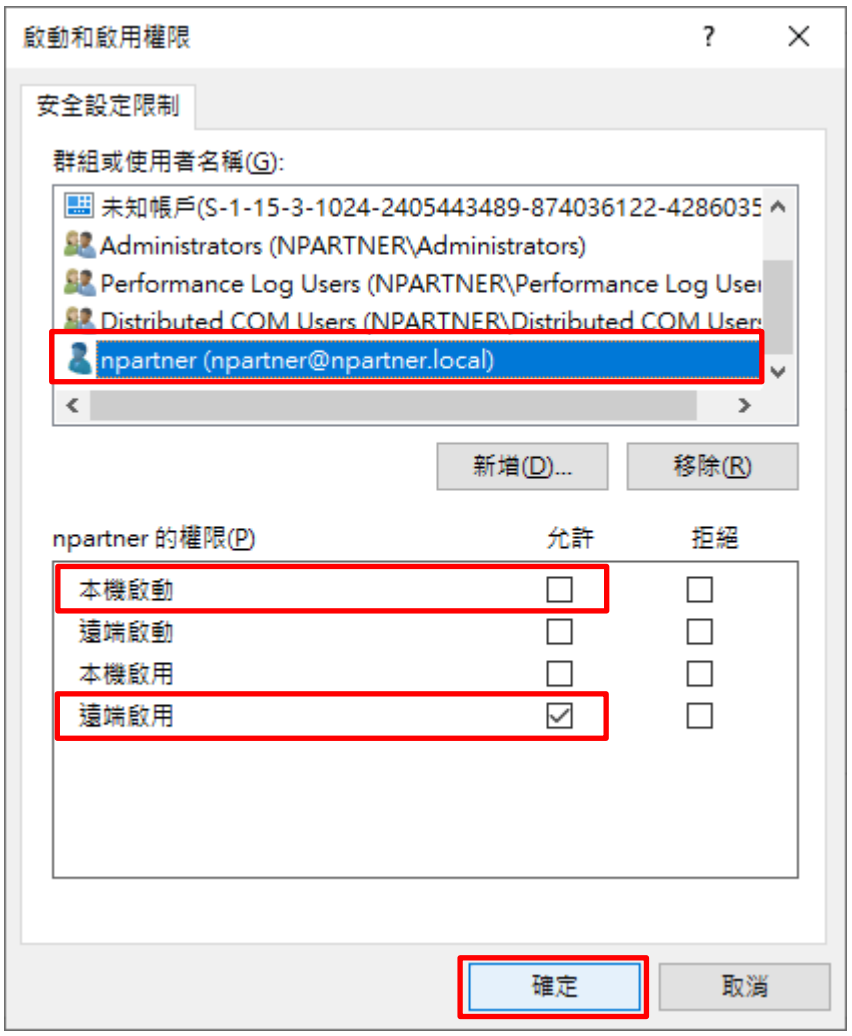
(6) 輸入使用者

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]

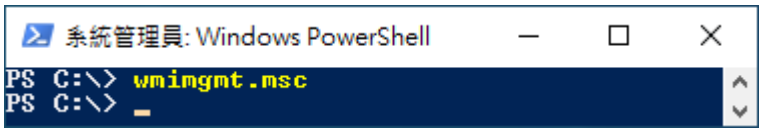
8.3.3 設定 WMI 權限

8.3.3.1 設定事件日誌權限

(1) 開啟 [Windows PowerShell]

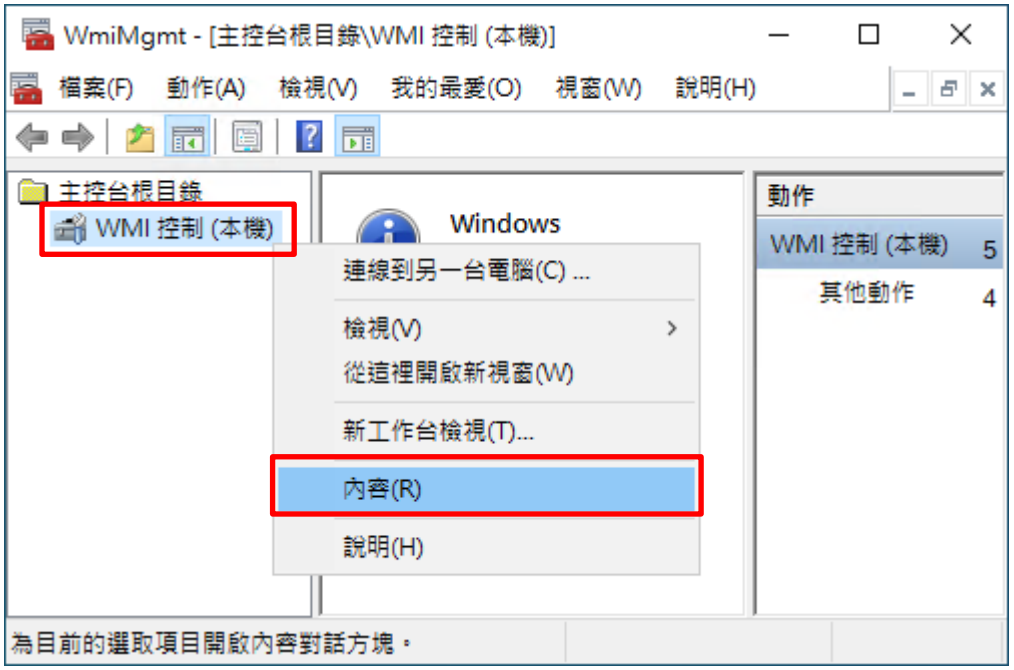
(2) 開啟元件服務

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



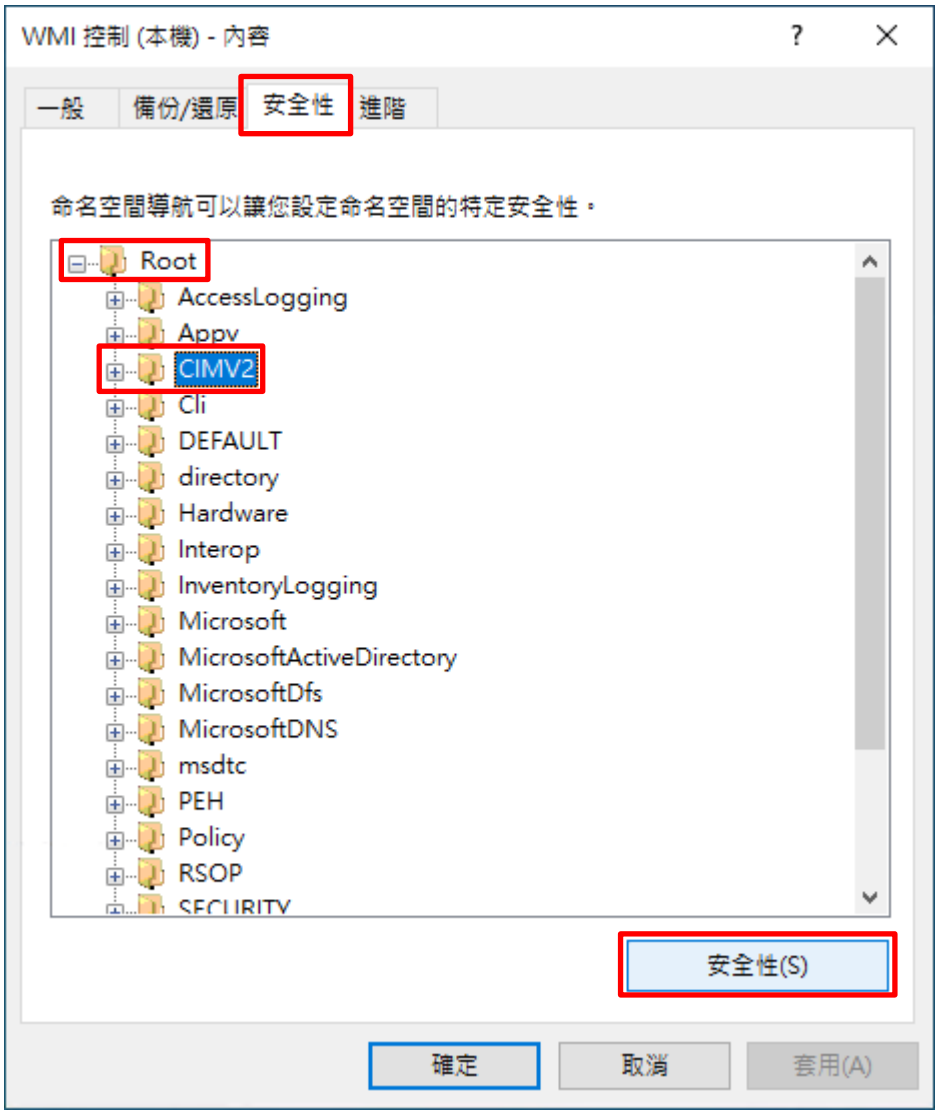
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



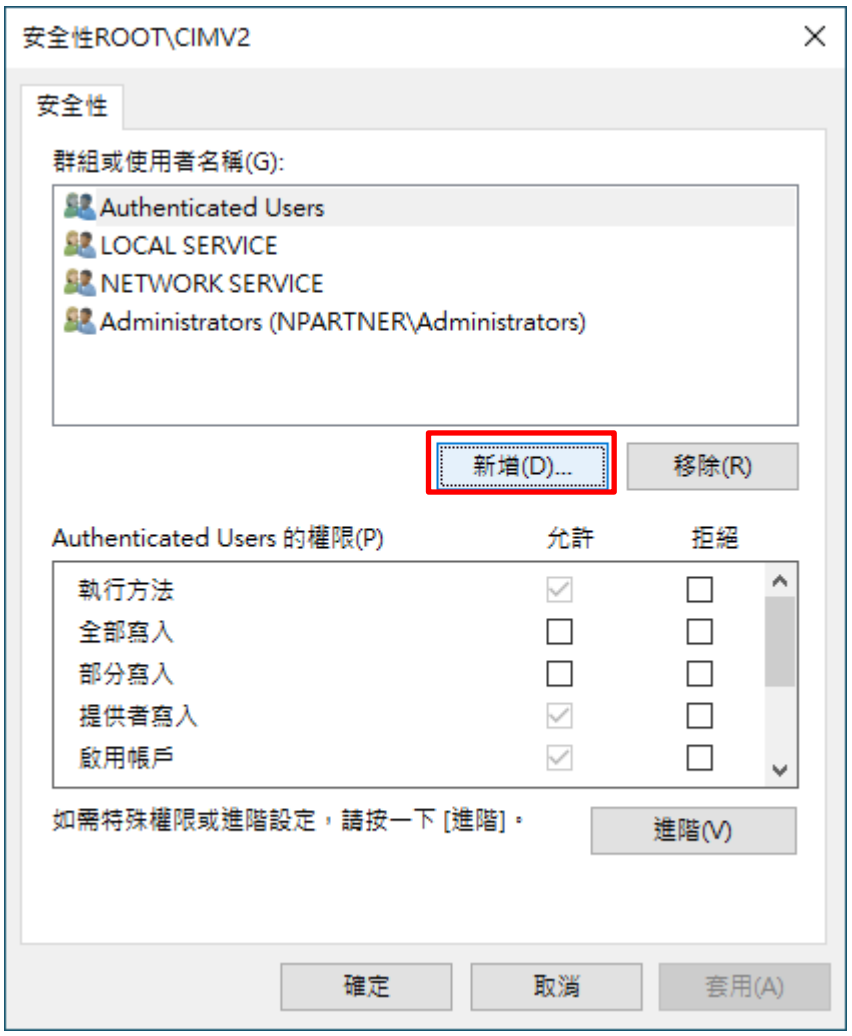
(4) 編輯 CIMV2 安全性

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



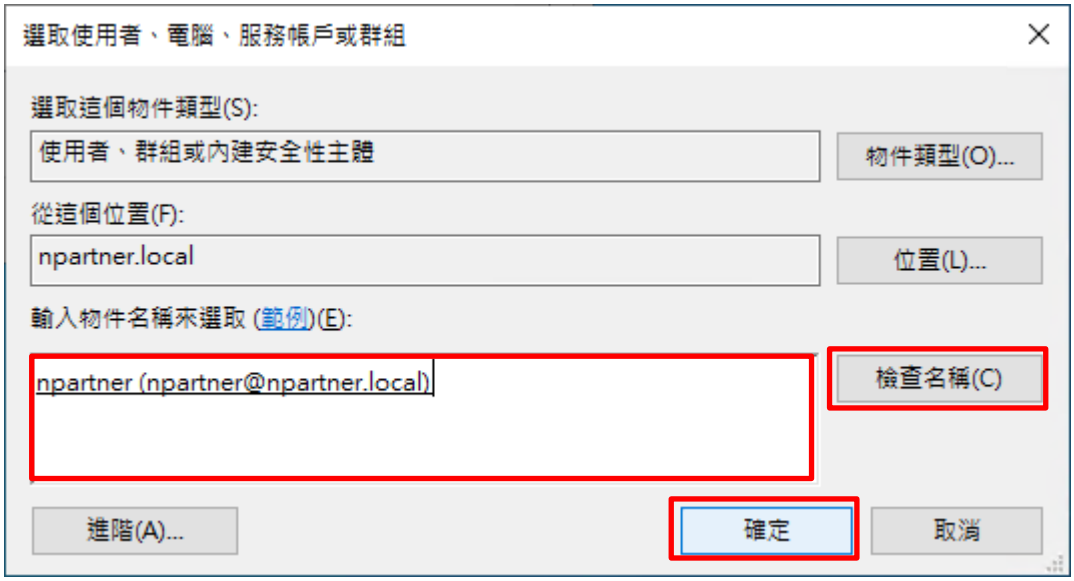
(5) 新增 WMI 使用者權限

按 [新增]



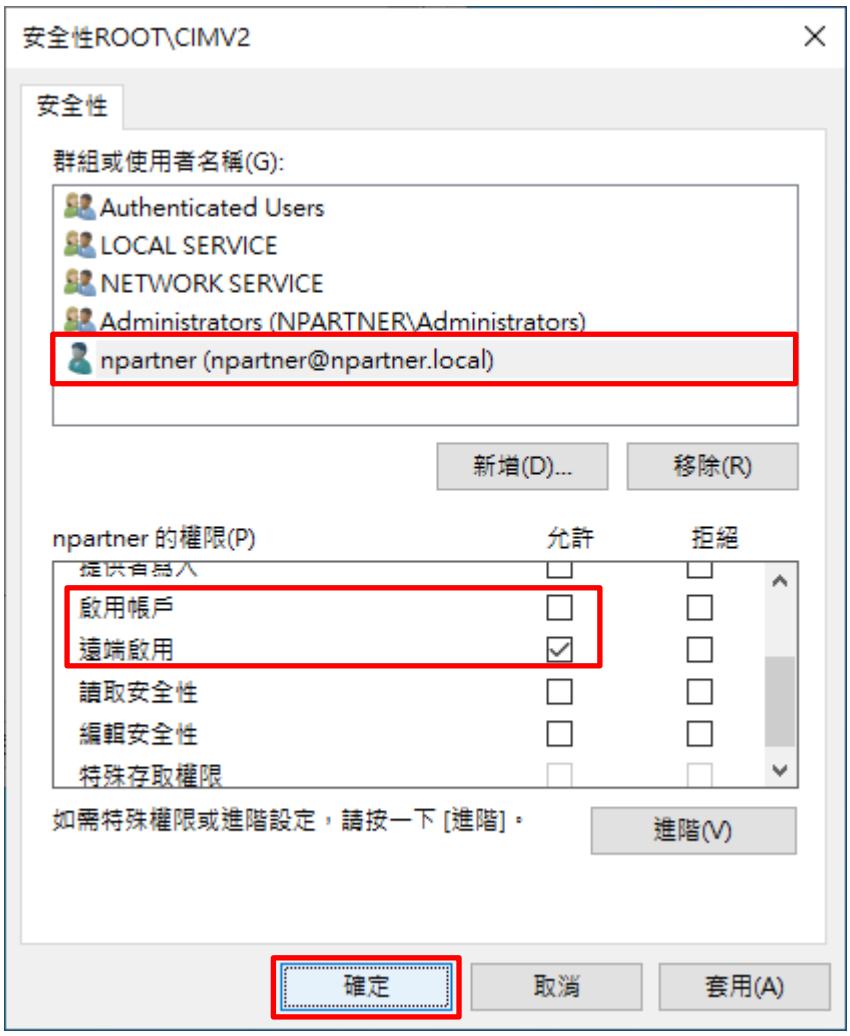
(6) 輸入使用者

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



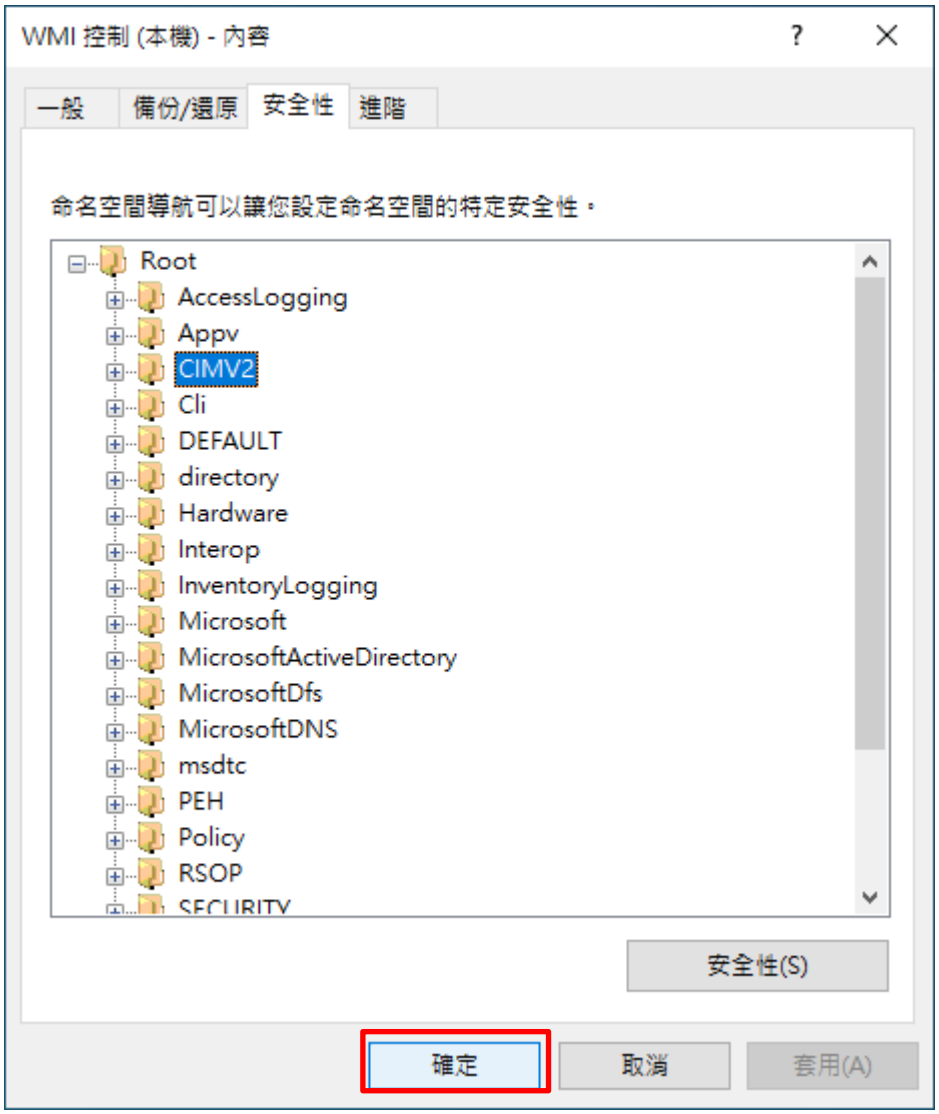
(7) 設定使用者權限

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]

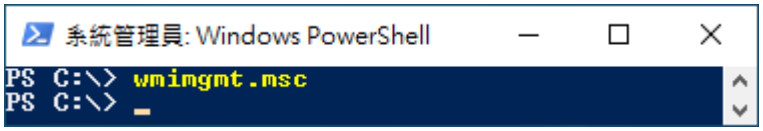


8.3.3.2 設定讀取使用者資料權限

(1) 開啟 [Windows PowerShell]

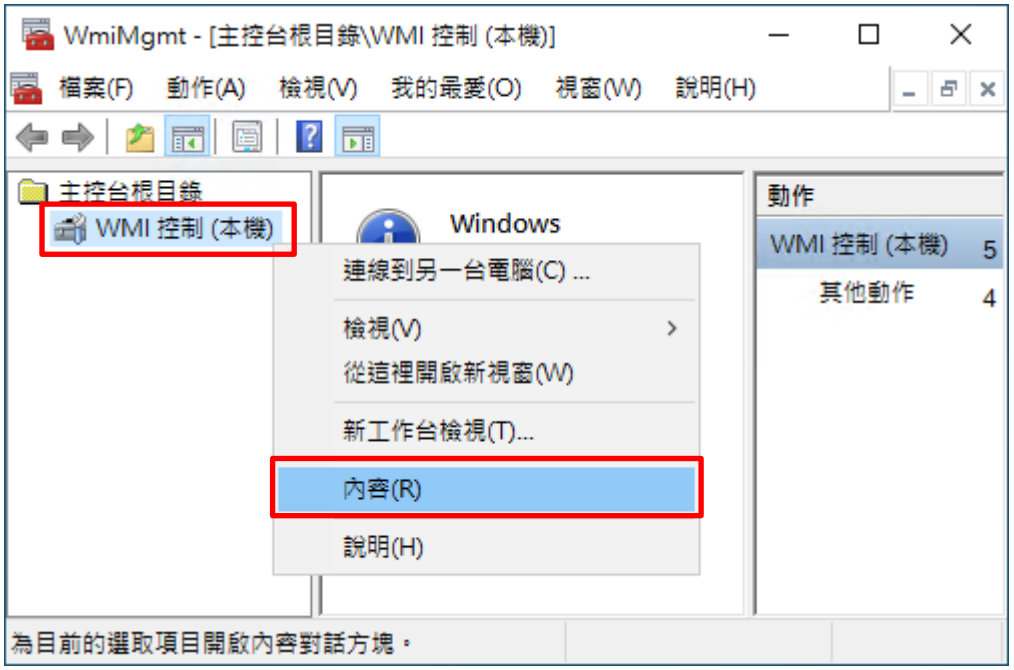
(2) 開啟元件服務

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



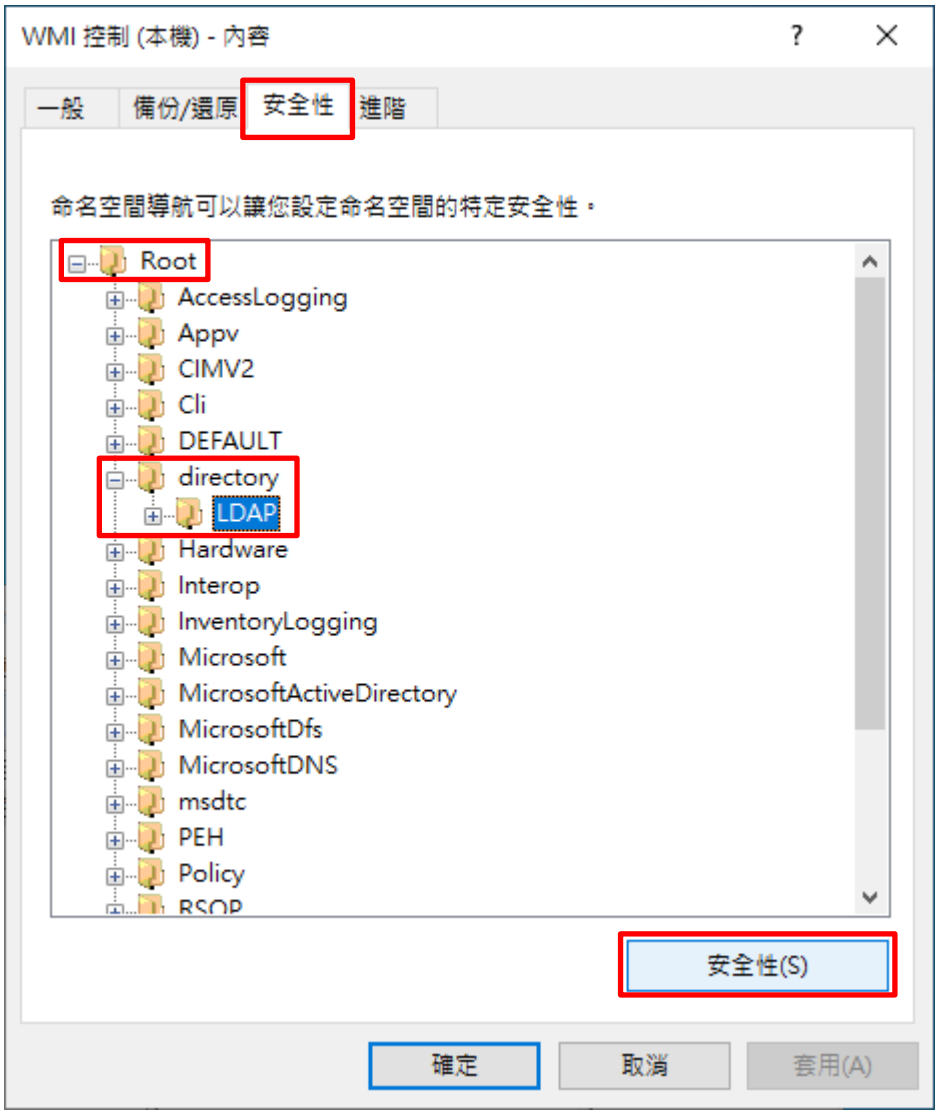
(3) 編輯 WMI 控制

在 [WMI 控制 (本機)] 按滑鼠右鍵 -> 點選 [內容]



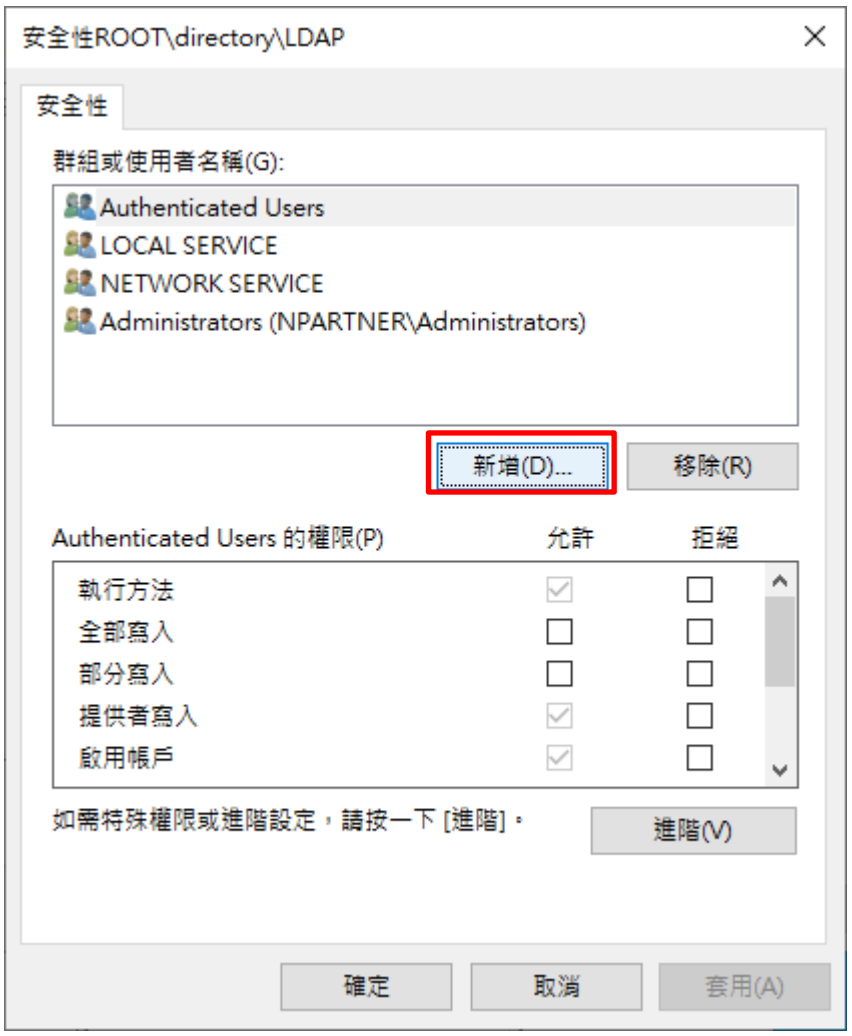
(4) 編輯 LDAP 安全性

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]

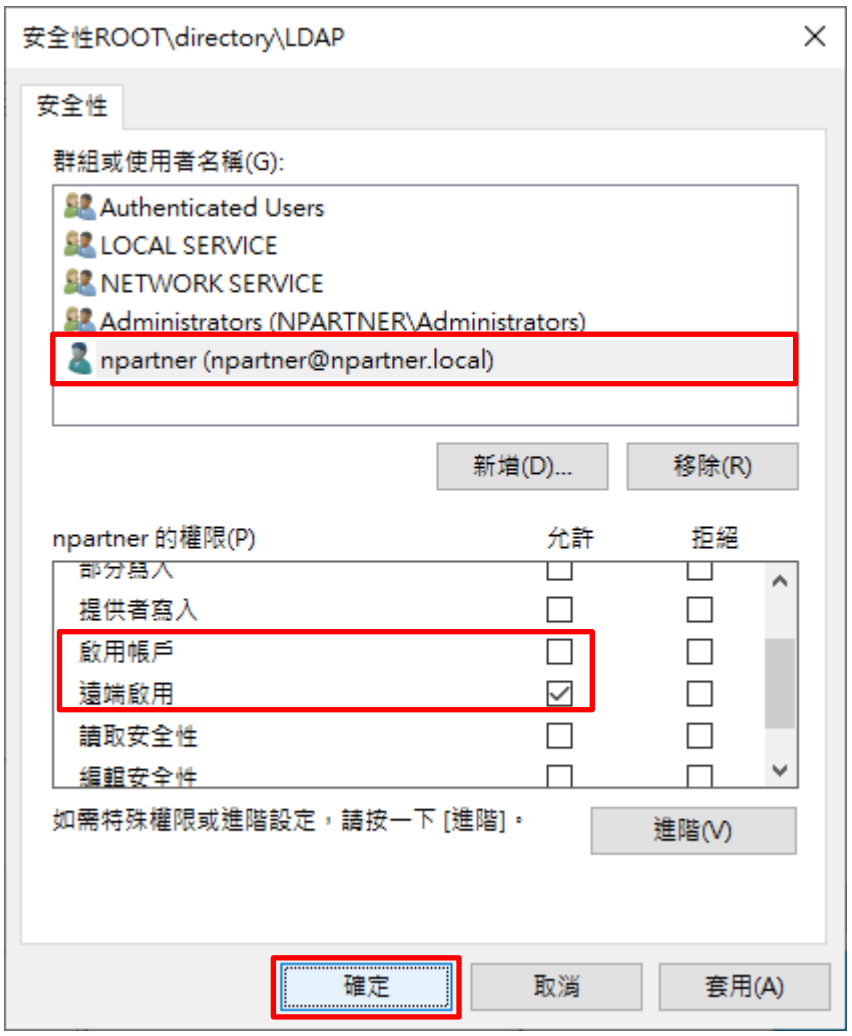


(6) 輸入使用者

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

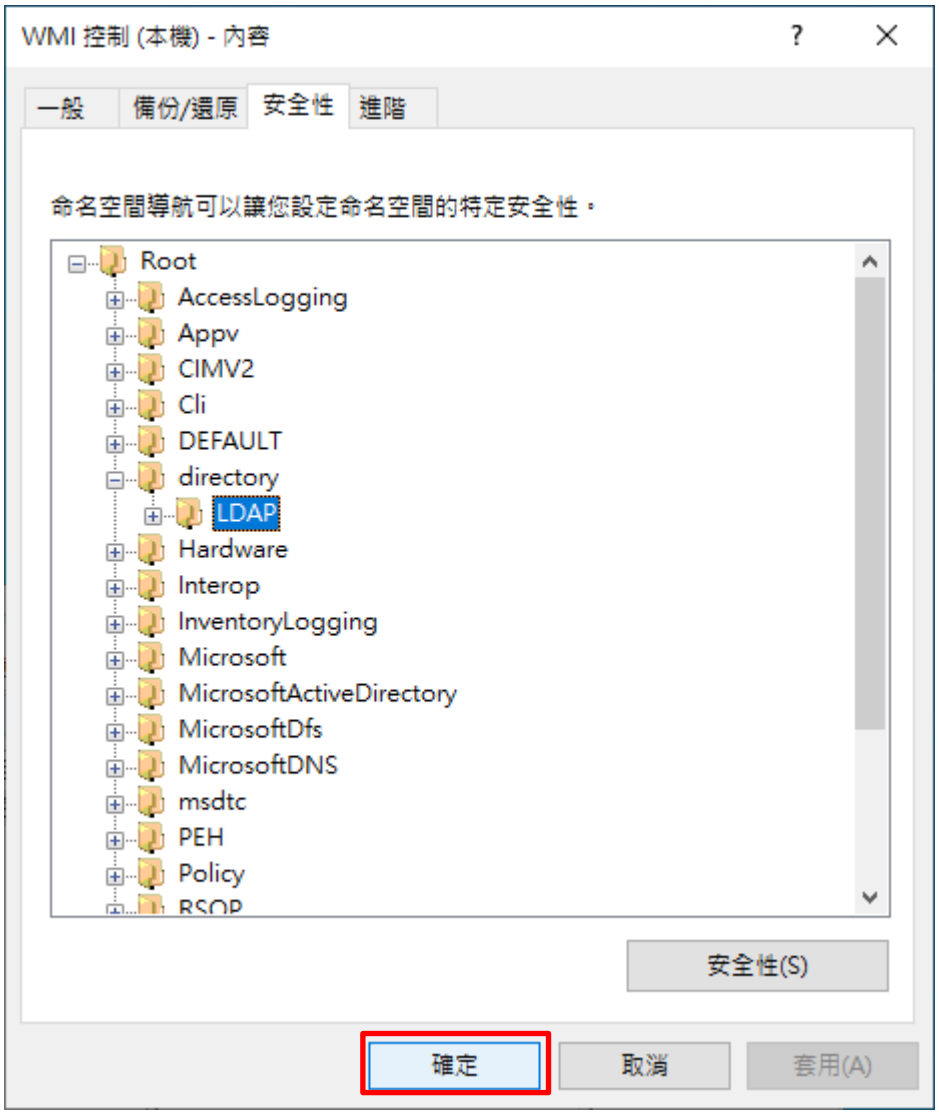
(7) 設定使用者權限

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

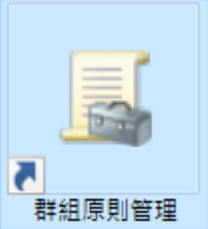
按 [確定]



8.3.4 設定 Event log 讀取權限

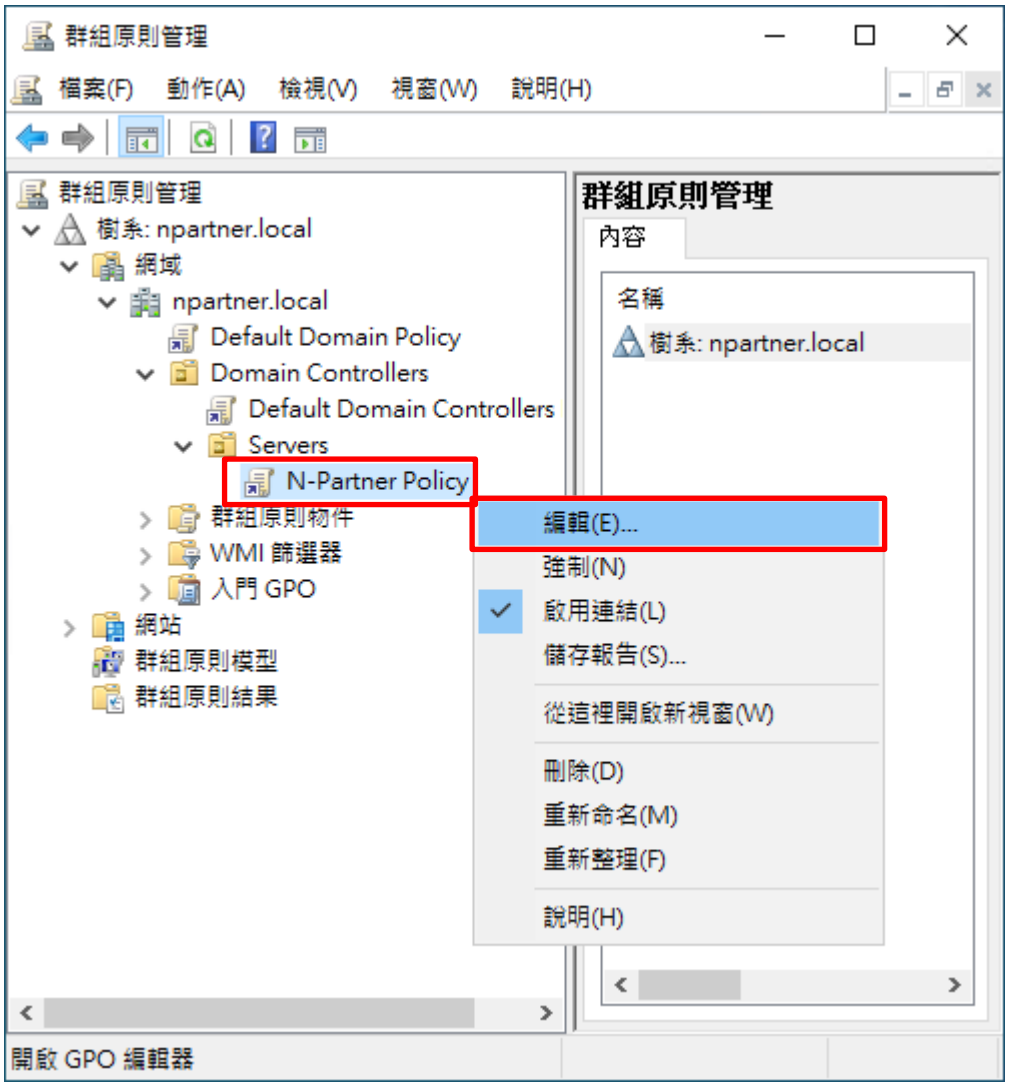
(1) 開啟群組原則管理

開啟 [群組原則管理]



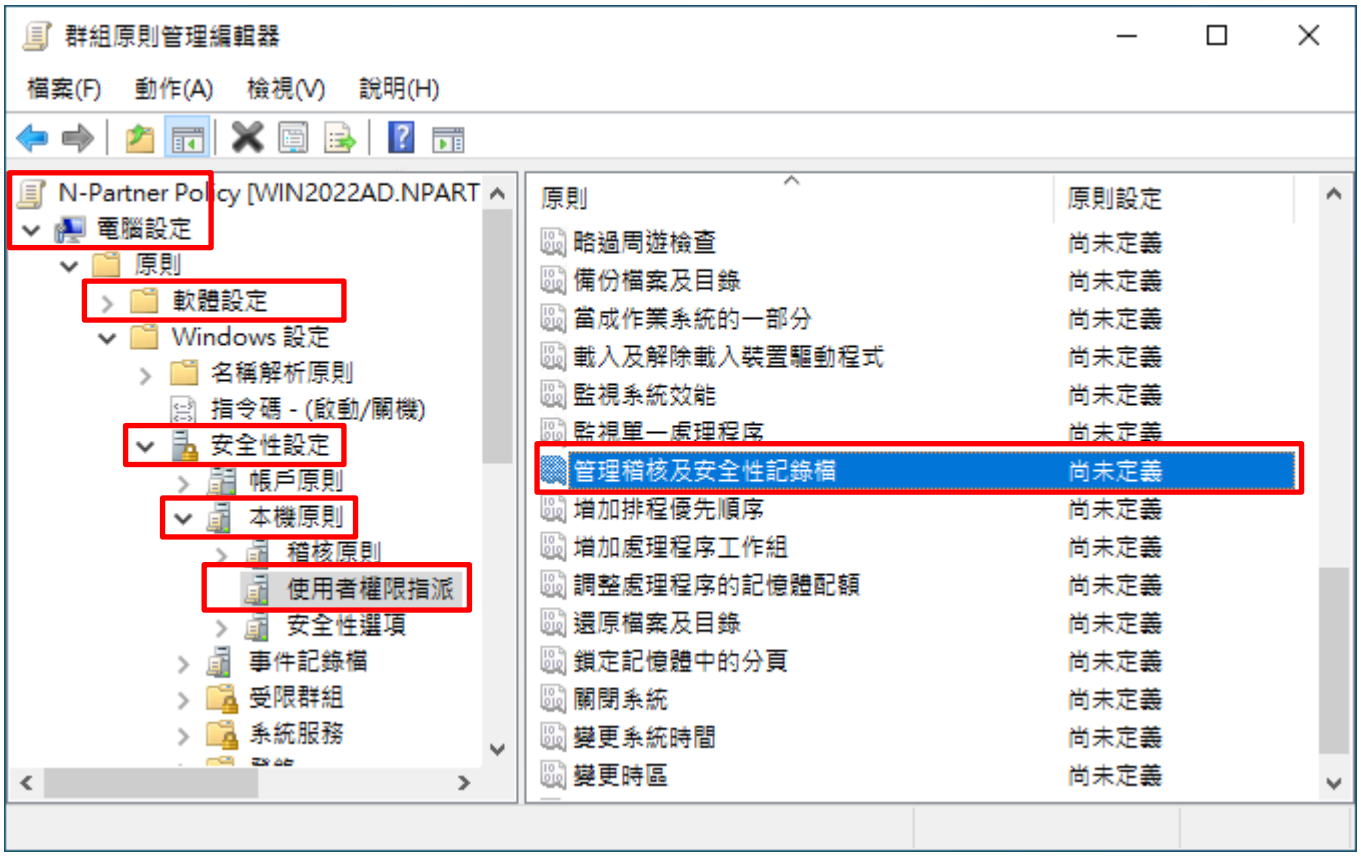
(2) 編輯群組原則物件

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

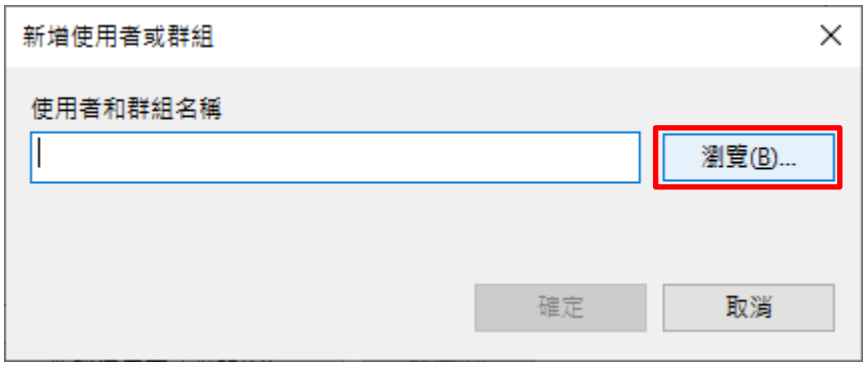


(4) 新增管理稽核使用者

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]

(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

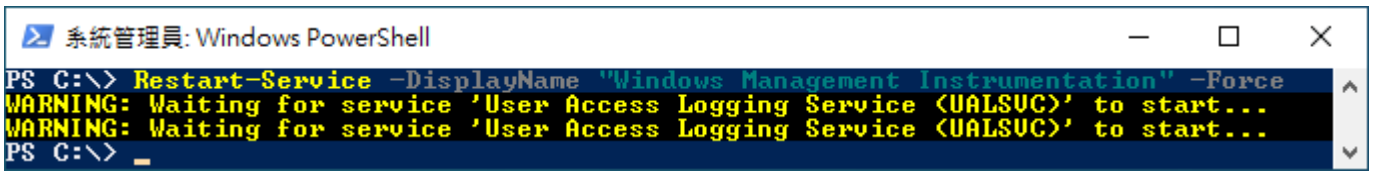
```
PS C:\> Invoke-GPUpdate -RandomDelayInMinutes 0 -Force
```

8.3.5 重啟 WMI 服務

(1) 開啟 [Windows PowerShell]

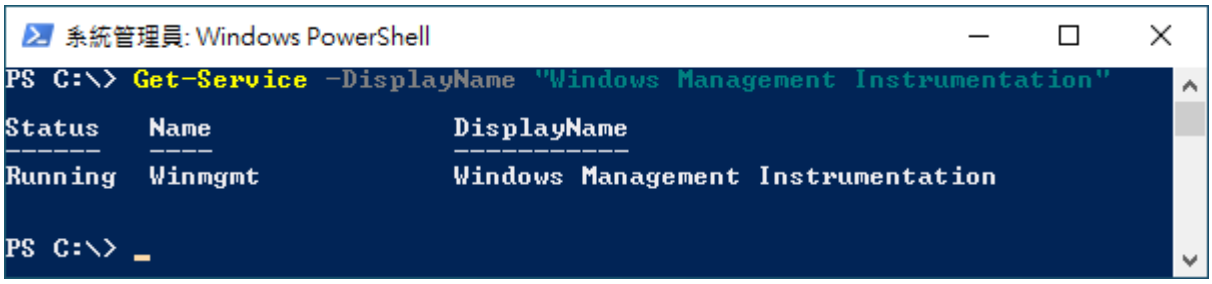
(2) 重啟 WMI 服務

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



(3) 查看 WMI 服務

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

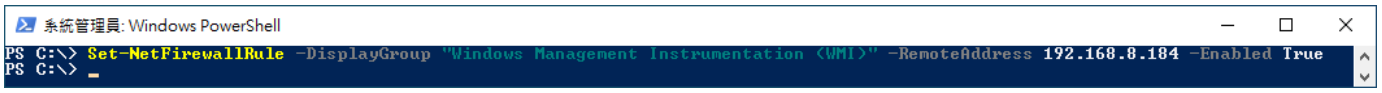


8.3.6 設定防火牆

(1) 開啟 [Windows PowerShell]

(2) 設定防火牆，只允許 N-Reporter IP query WMI

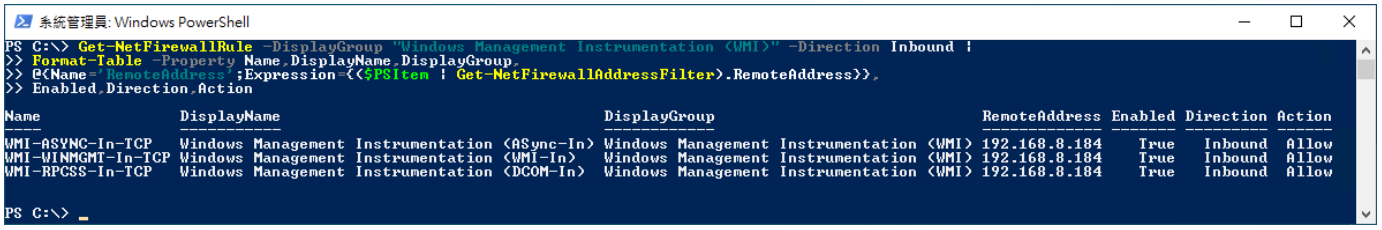
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.184 -Enabled True
```



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

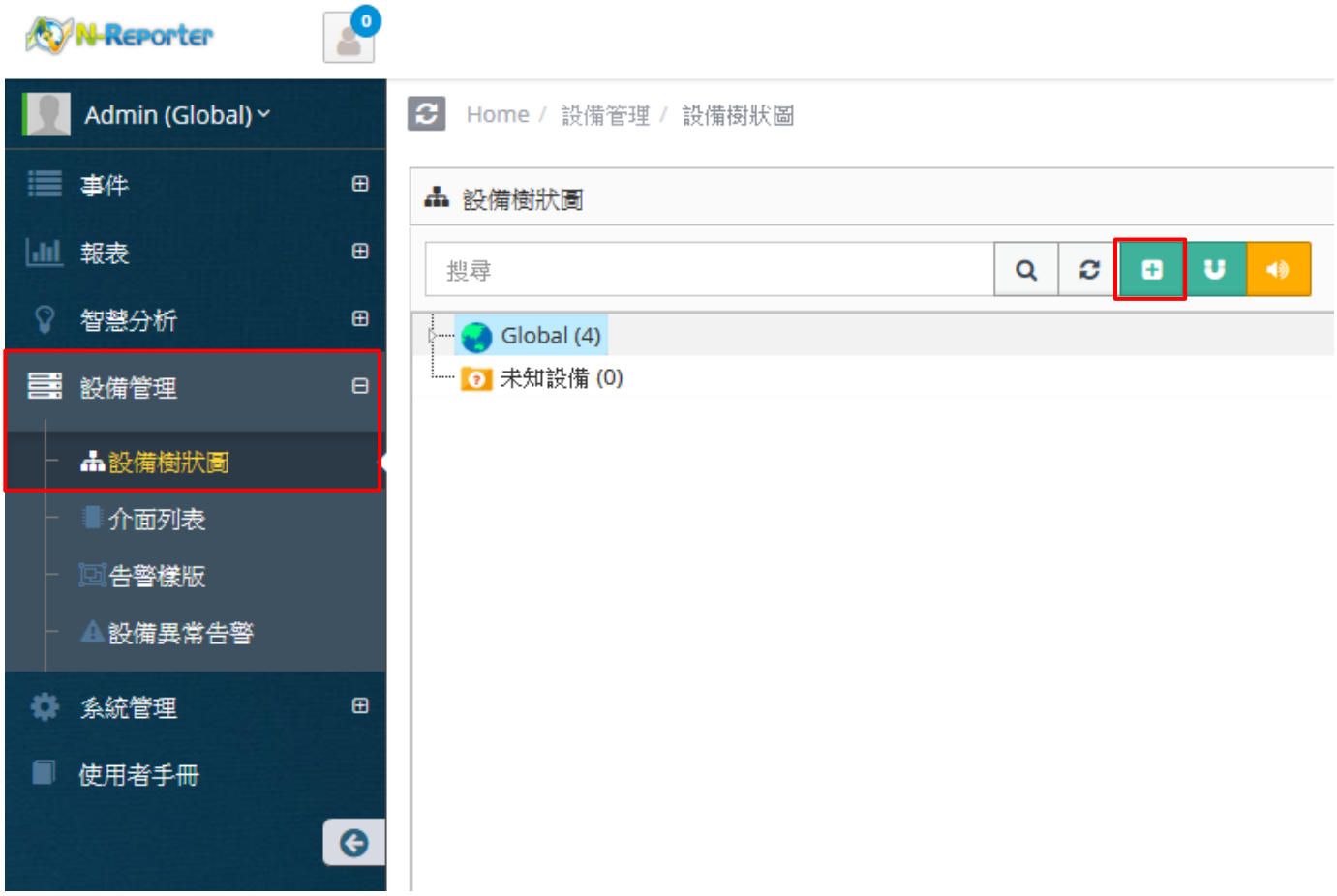
```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



9. N-Reporter

(1) 新增 Windows AD 設備

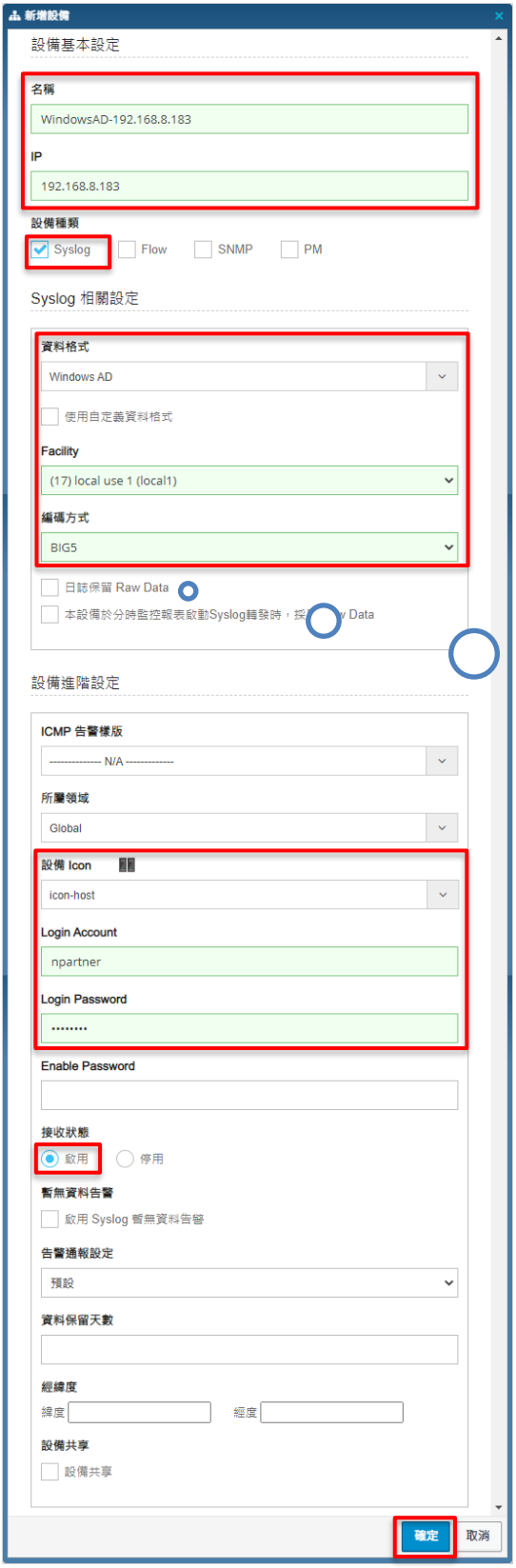
[設備管理] -> [設備樹狀圖] -> 點選 [新增]



9.1 Windows 2003 或之前版本作業系統

(2) 設定 Windows AD 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows AD] 和 Facility: [(17) local user 1 (local1)] 和 編碼方式: [BIG5] -> 選擇設備 Icon: [icon-host] -> 輸入 Windows AD 的 WMI Login Account 和 Login Password 若沒設定 WMI 可以不用輸入帳密 -> 點選接收狀態: [啟用] -> 按 [確定]



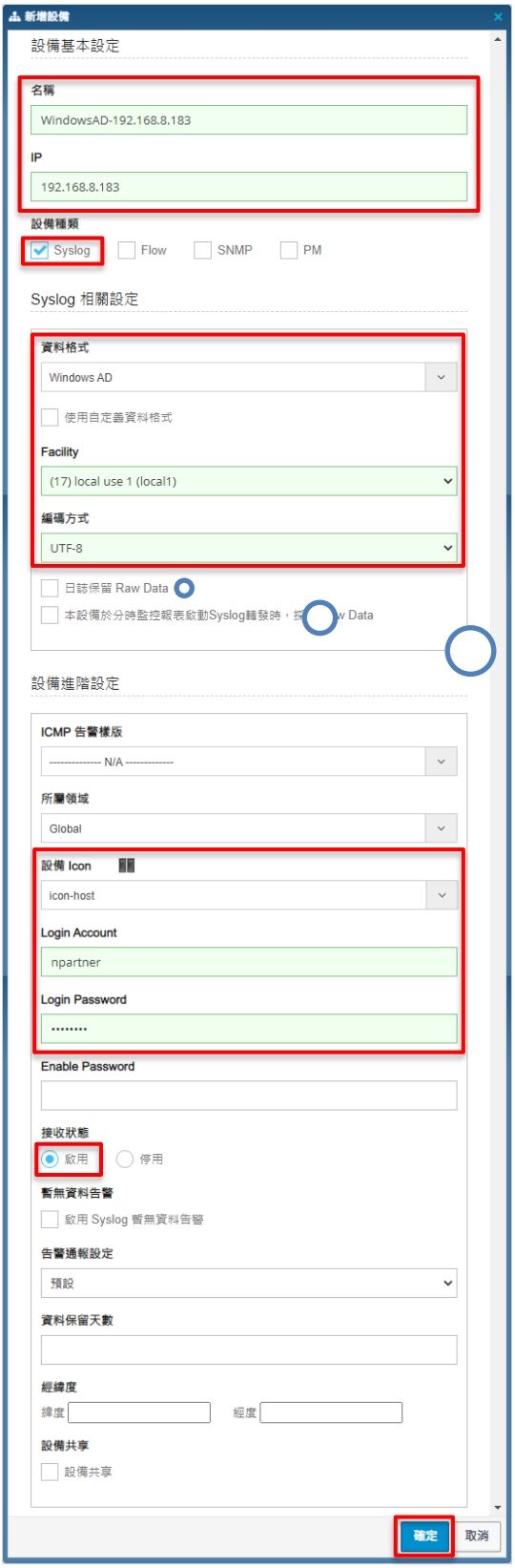
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

9.2 Windows 2008 或之後版本作業系統

(2) 設定 Windows AD 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows AD] 和 Facility: [(17) local user 1 (local1)] 和 編碼方式: [UTF-8] -> 選擇設備 Icon: [icon-host] -> 輸入 Windows AD 的 WMI Login Account 和 Login Password 若沒設定 WMI 可以不用輸入帳密 -> 點選接收狀態: [啟用] -> 按 [確定]



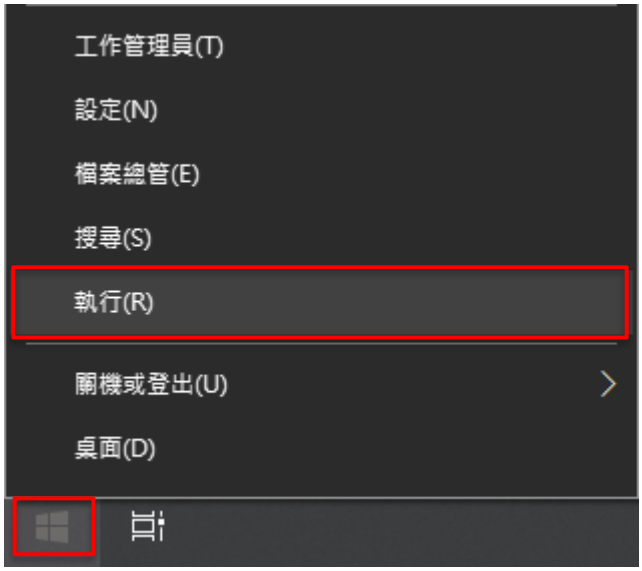
若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

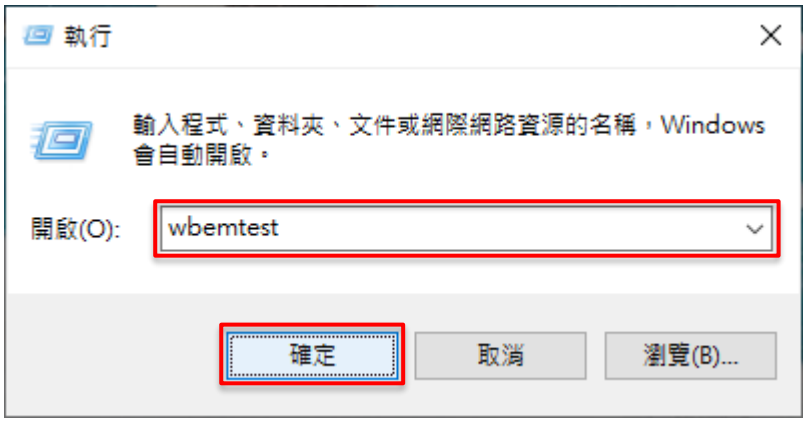
10. 問題排除

10.1 WMI Query Language 檢查

(1) 按  -> 點選 [執行]

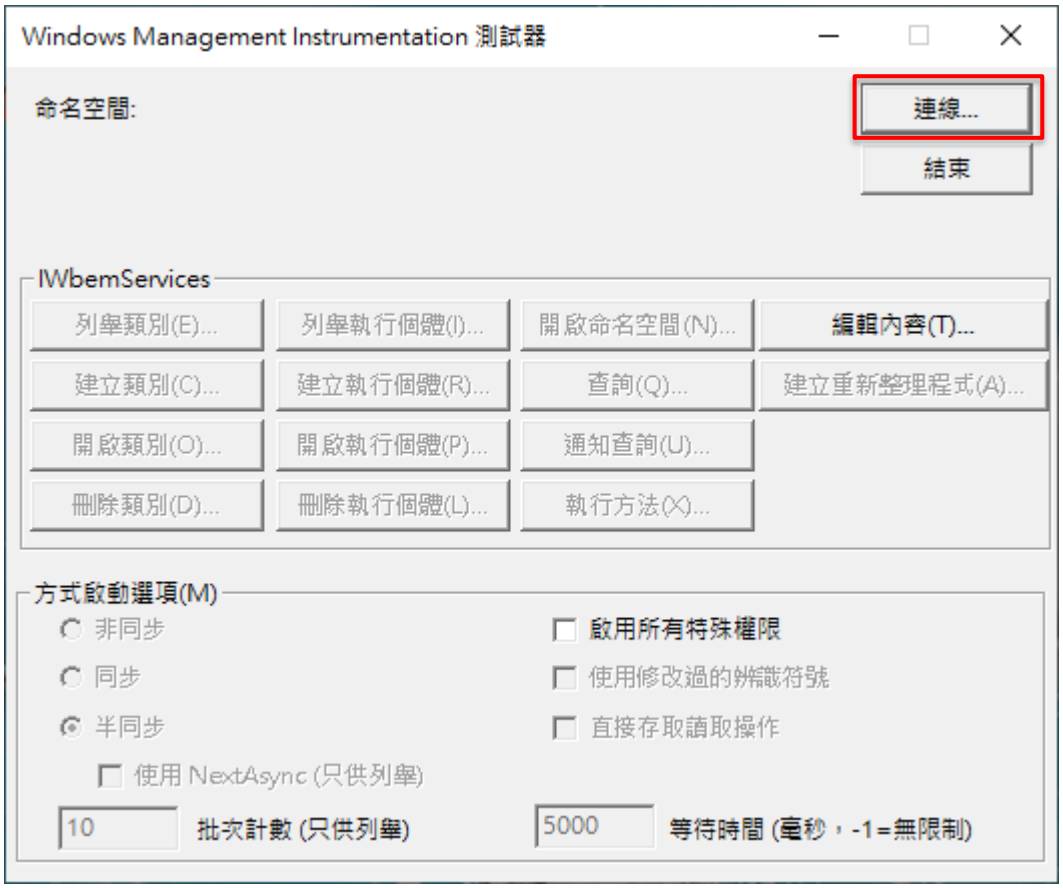


(2) 輸入 wbemtest -> 按 [確定]

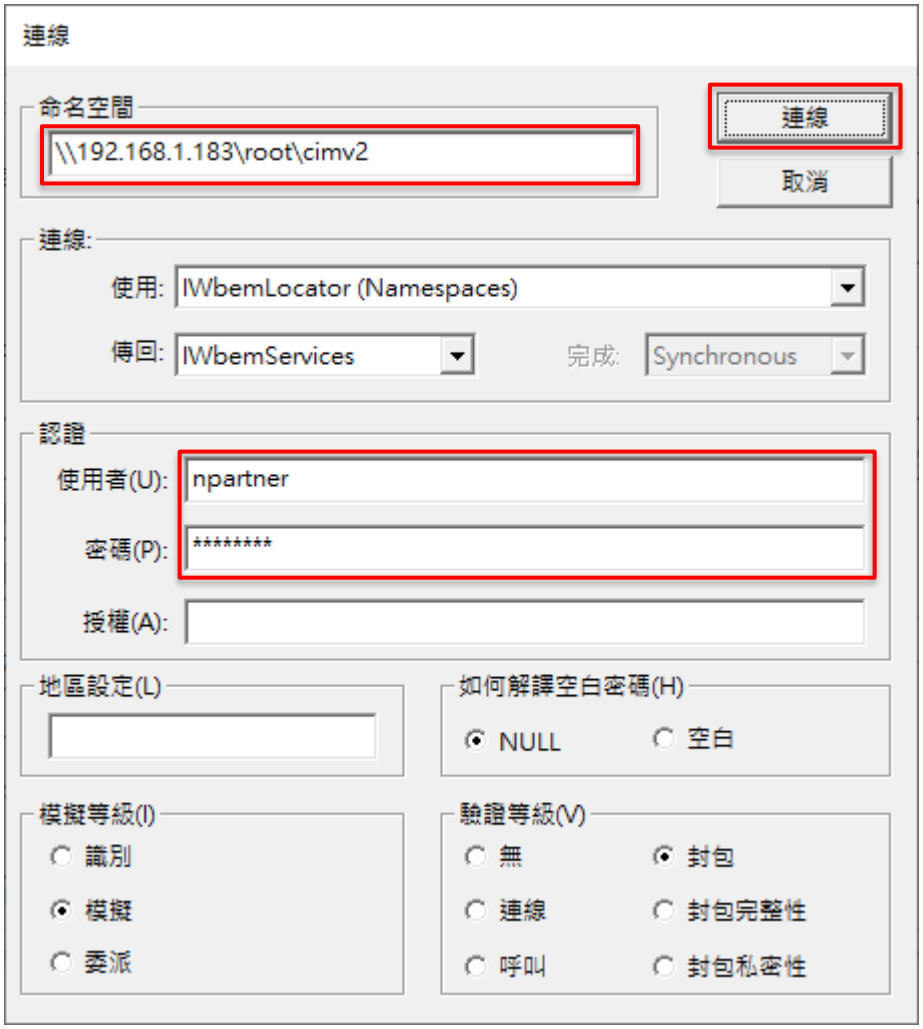


10.1.1 查詢事件日誌

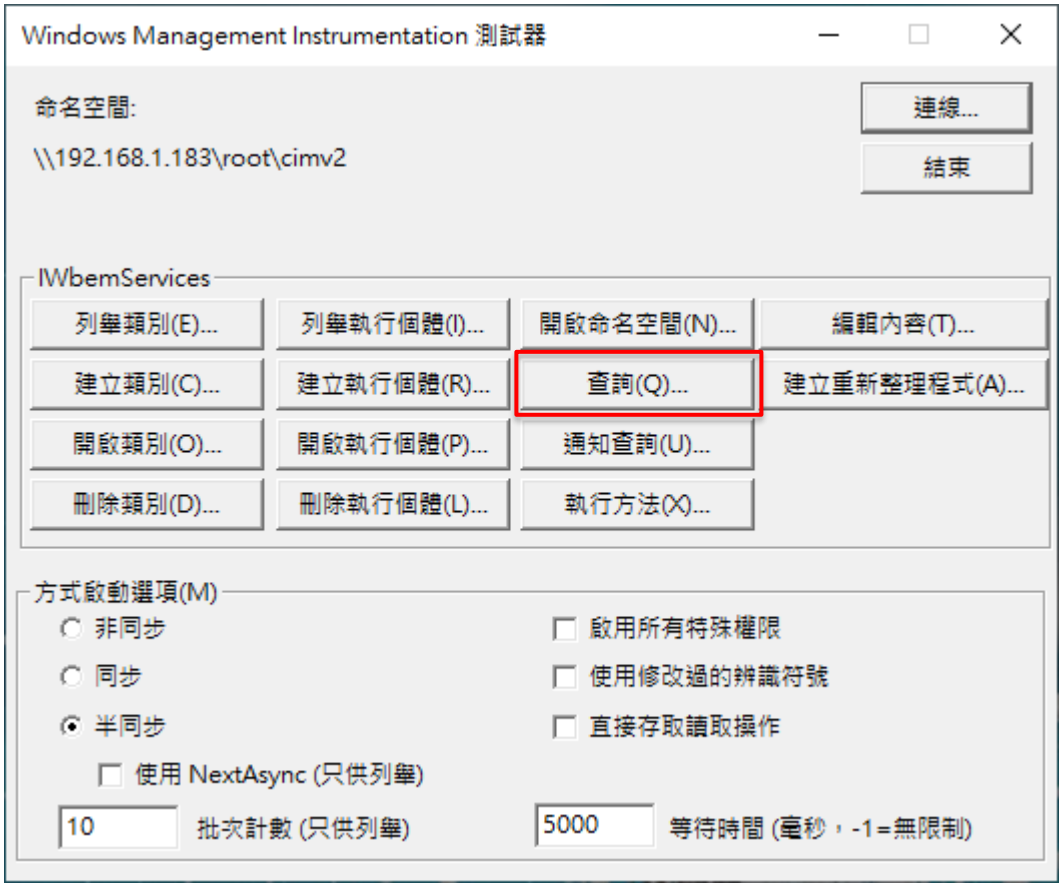
(1) 按 [連線]



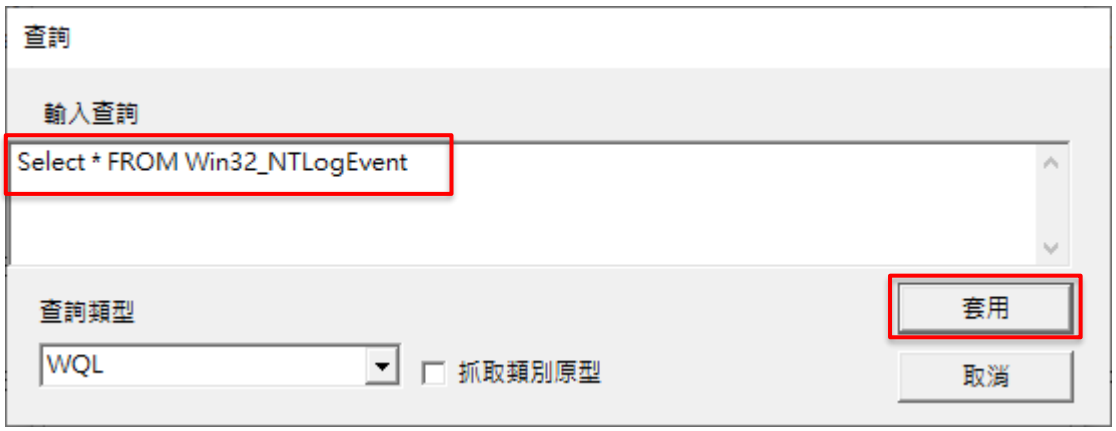
(2) 輸入命名空間 \\<*Windows AD IP*>\root\cimv2 -> 使用者帳號和密碼 -> 按 [連線]



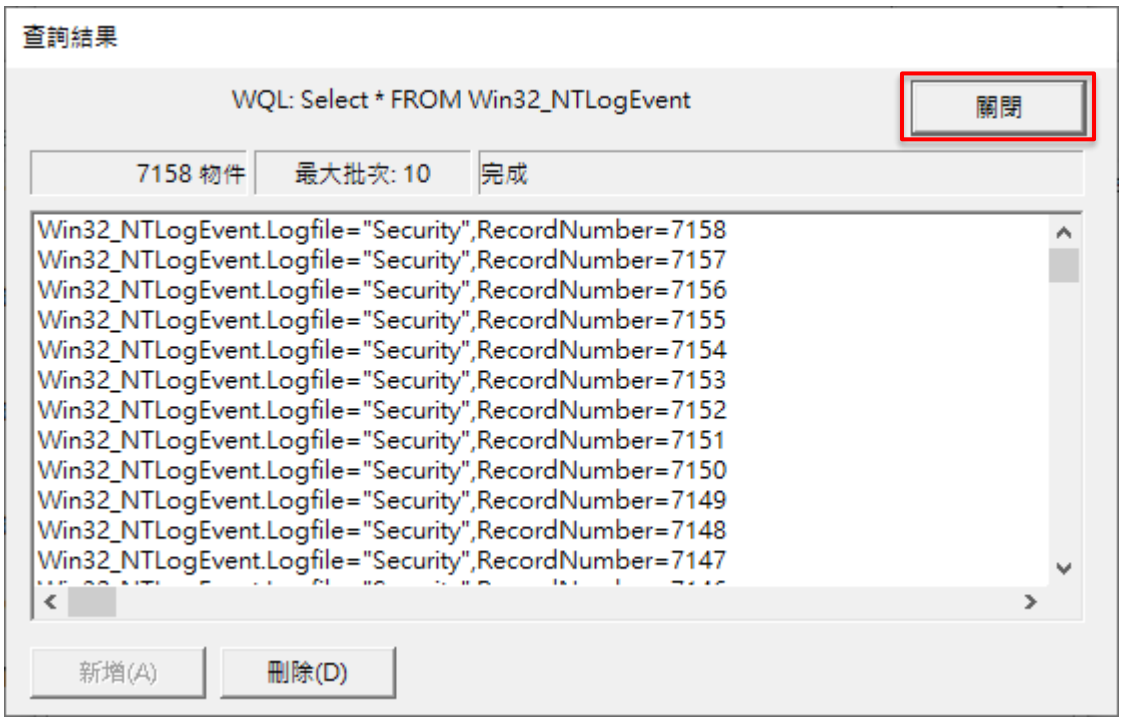
(3) 按 [查詢]



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

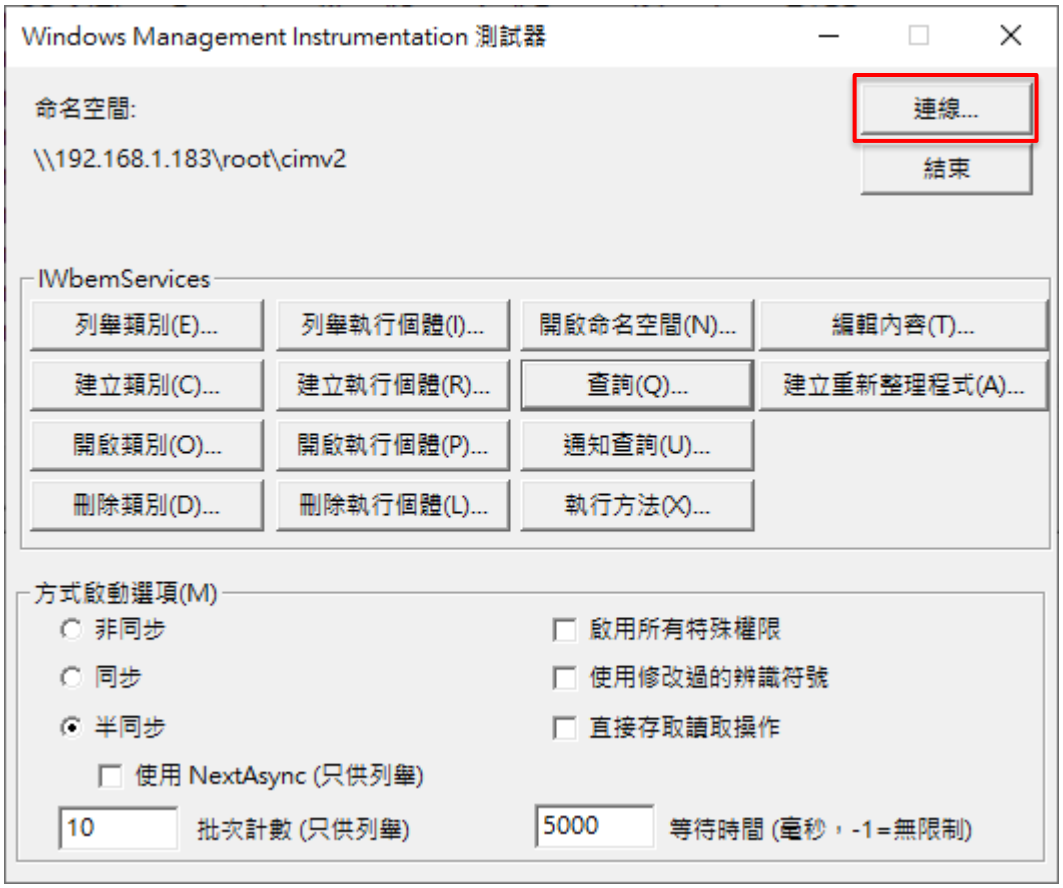


(5) 顯示查詢到資料 -> 按 [關閉]

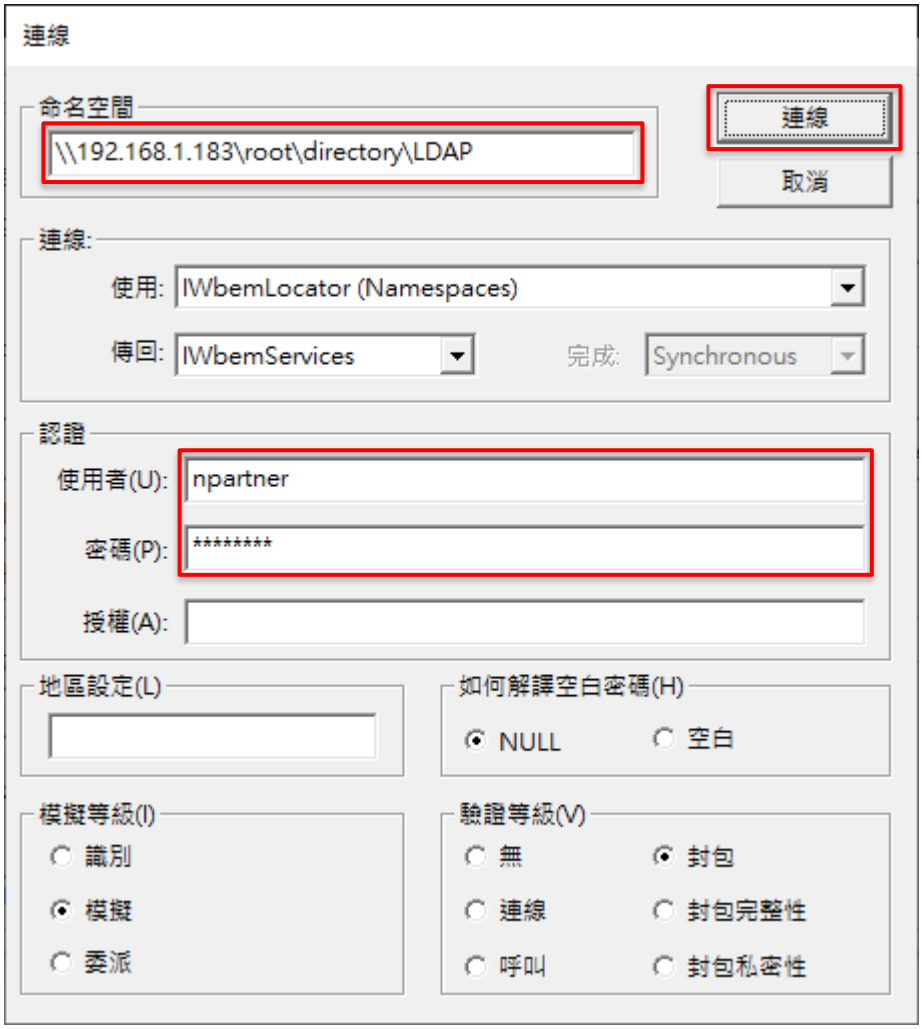


10.1.2 查詢使用者資料

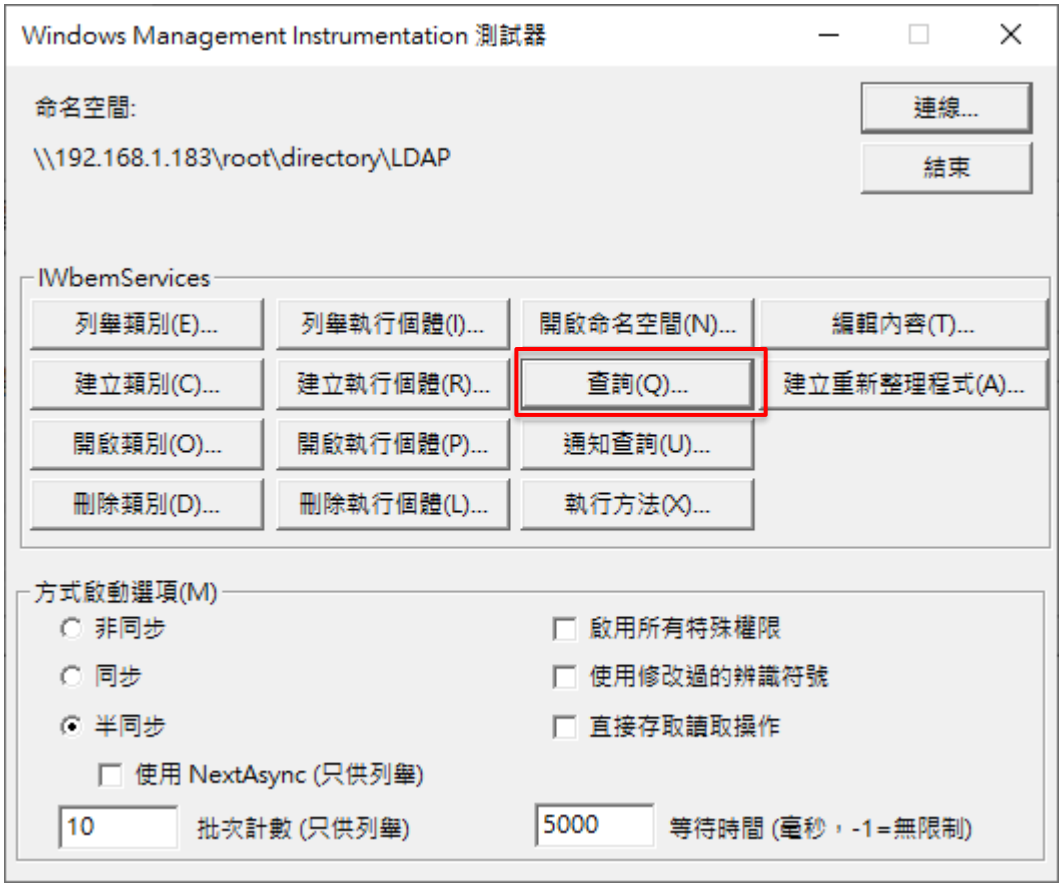
(1) 按 [連線]



(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]

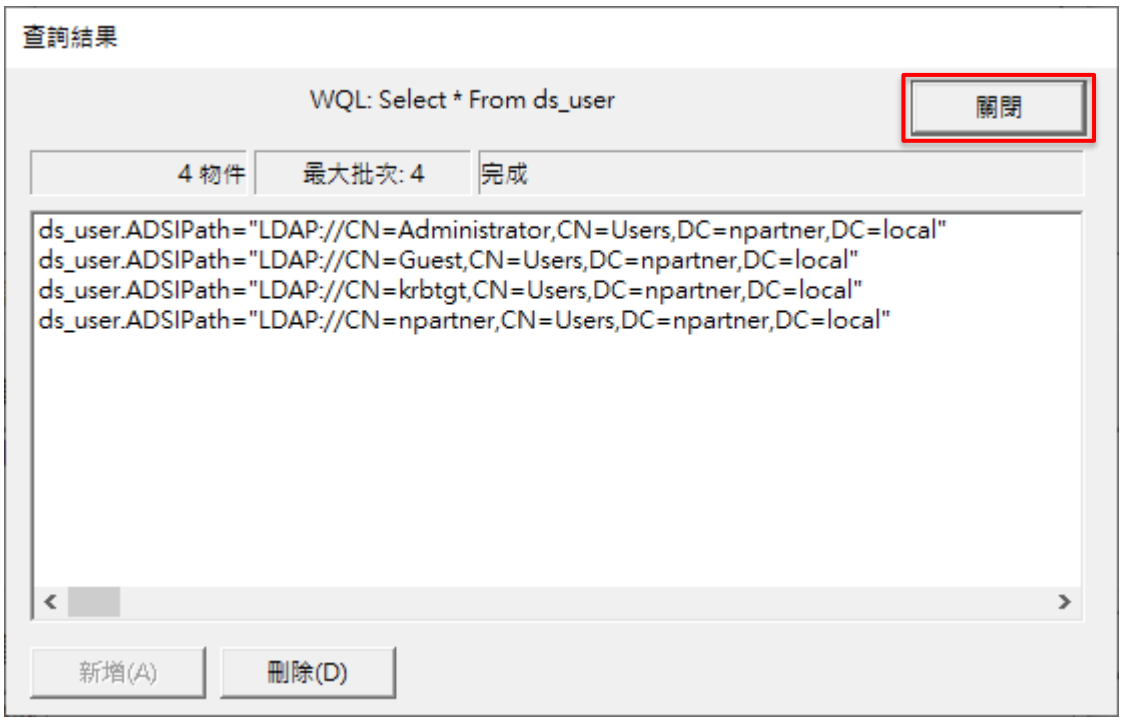


(3) 按 [查詢]

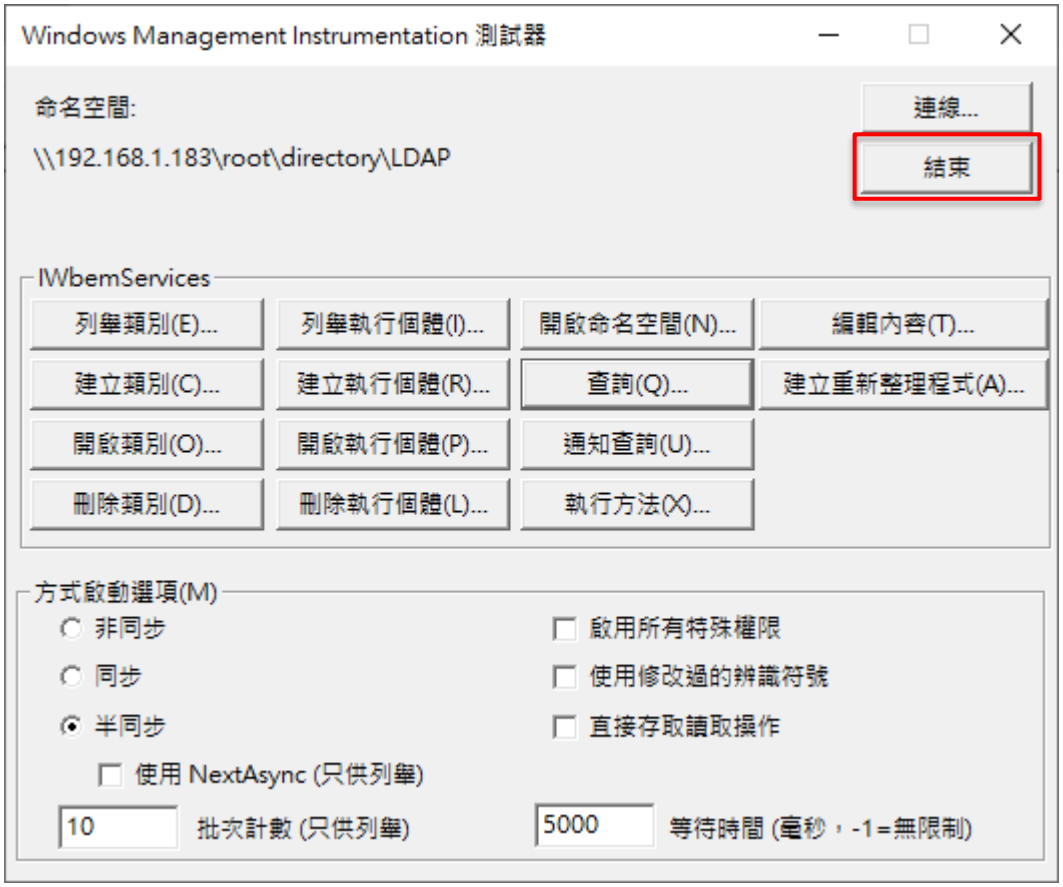


(4) 輸入查詢 Select * FROM ds_user -> 按 [套用]

(5) 顯示查詢到資料 -> 按 [關閉]

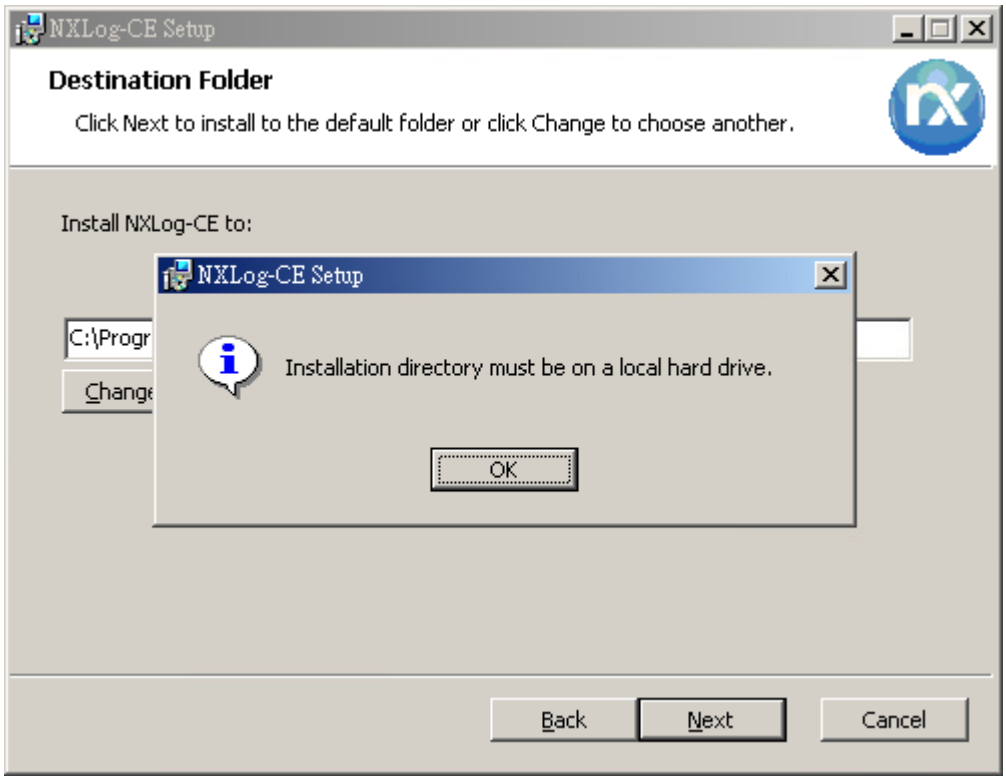


(6) 使用者帳號密碼可以查詢到資料；按 [結束] 關閉 WMI 測試器



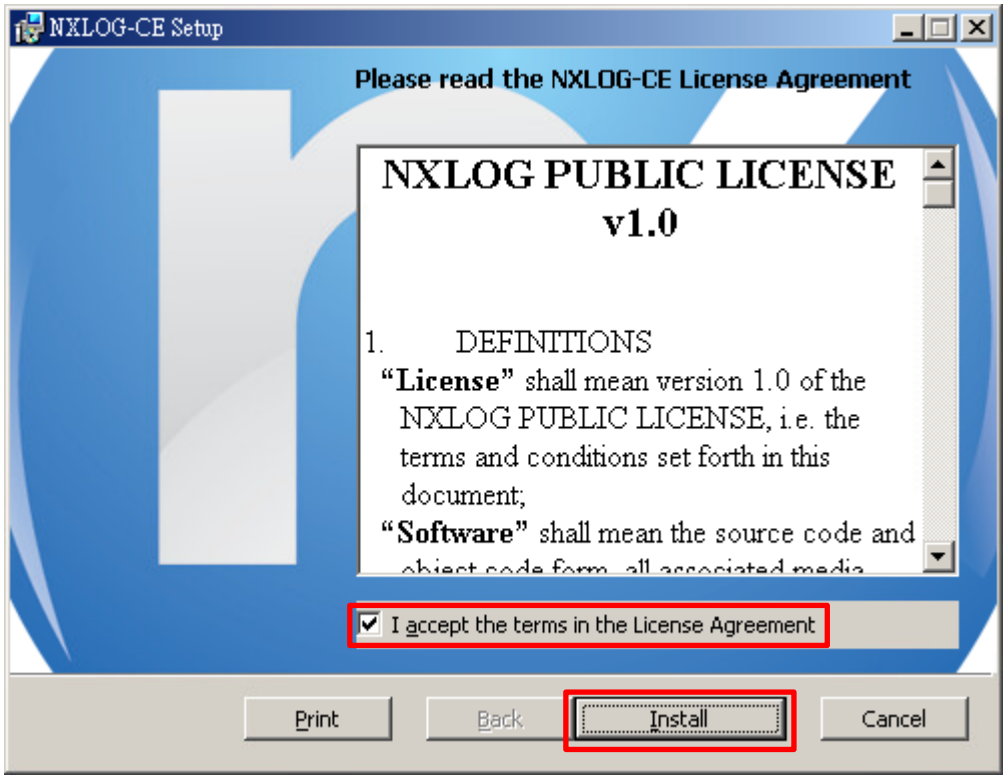
10.2 NXLog 安裝問題

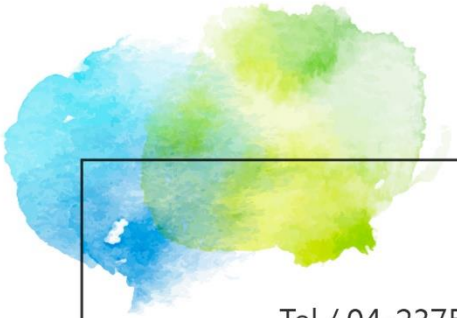
(1) 安裝 NXLog(2.10.2150) 顯示 Installation directory must be on a local hard drive.



(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