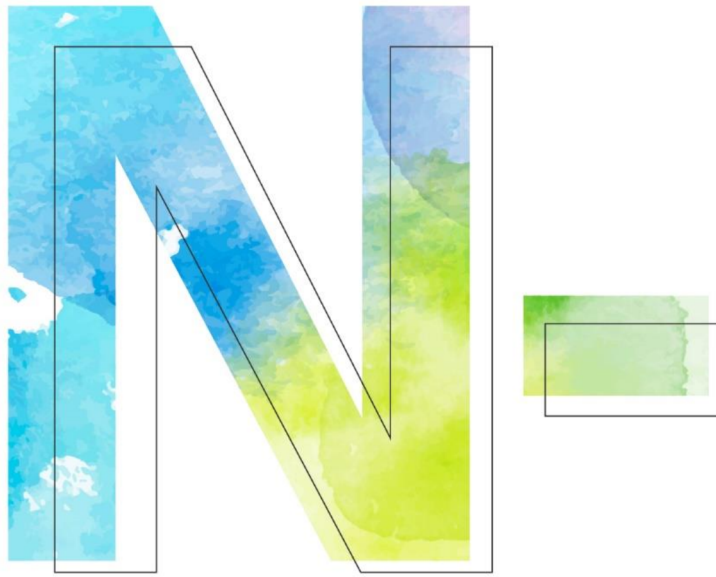




# Partner

## 如何設定 MS SQL 稽核事件記錄

V020

2024/07/26



## 版權聲明

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

## 商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

# 目錄

|                            |    |                             |     |
|----------------------------|----|-----------------------------|-----|
| 前言                         | 1  | 4.1.2 使用指令介面方式設定            | 96  |
| 1 NXLog                    | 2  | 4.2 設定稽核                    | 98  |
| 1.1 NXLog 安裝               | 2  | 4.2.1 稽核伺服器層級               | 98  |
| 1.2 NXLog 設定檔下載            | 5  | 4.2.2 稽核資料庫層級               | 106 |
| 1.2.1 MS SQL 單機設定檔         | 5  | 4.3 事件記錄檔設定                 | 115 |
| 1.2.2 MS SQL Cluster 叢集設定檔 | 6  | 4.3.1 網域                    | 115 |
| 1.3 NXLog 設定檔              | 7  | 4.3.2 工作群組                  | 125 |
| 1.3.1 MS SQL 單機設定檔         | 7  | 5 SQL2019                   | 131 |
| 1.3.2 MS SQL Cluster 叢集設定檔 | 9  | 5.1 稽核登入                    | 131 |
| 1.4 NXLog 啟動服務             | 11 | 5.1.1 使用圖形介面方式設定            | 131 |
| 2 SQL2008                  | 14 | 5.1.2 使用指令介面方式設定            | 135 |
| 2.1 稽核登入                   | 14 | 5.2 設定稽核                    | 137 |
| 2.1.1 使用圖形介面方式設定           | 14 | 5.2.1 稽核伺服器層級               | 137 |
| 2.1.2 使用指令介面方式設定           | 18 | 5.2.2 稽核資料庫層級               | 145 |
| 2.2 設定稽核                   | 20 | 5.3 事件記錄檔設定                 | 154 |
| 2.2.1 稽核伺服器層級              | 20 | 5.3.1 網域                    | 154 |
| 2.2.2 稽核資料庫層級              | 28 | 5.3.2 工作群組                  | 164 |
| 2.3 事件記錄檔設定                | 37 | 6 SQL2022                   | 170 |
| 2.3.1 網域                   | 37 | 6.1 稽核登入                    | 170 |
| 2.3.2 工作群組                 | 47 | 6.1.1 使用圖形介面方式設定            | 170 |
| 3 SQL2012                  | 53 | 6.1.2 使用指令介面方式設定            | 174 |
| 3.1 稽核登入                   | 53 | 6.2 設定稽核                    | 176 |
| 3.1.1 使用圖形介面方式設定           | 53 | 6.2.1 稽核伺服器層級               | 176 |
| 3.1.2 使用指令介面方式設定           | 57 | 6.2.2 稽核資料庫層級               | 184 |
| 3.2 設定稽核                   | 59 | 6.3 事件記錄檔設定                 | 193 |
| 3.2.1 稽核伺服器層級              | 59 | 6.3.1 網域                    | 193 |
| 3.2.2 稽核資料庫層級              | 67 | 6.3.2 工作群組                  | 203 |
| 3.3 事件記錄檔設定                | 76 | 7 N-Reporter                | 209 |
| 3.3.1 網域                   | 76 | 7.1 MS SQL Server Event Log | 211 |
| 3.3.2 工作群組                 | 86 | 7.2 Windows Event Log       | 214 |
| 4 SQL2016                  | 92 | 8 問題排除                      | 217 |
| 4.1 稽核登入                   | 92 | 8.1 Invoke-GPUUpdate 錯誤     | 217 |
| 4.1.1 使用圖形介面方式設定           | 92 |                             |     |

# 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 MS SQL 事件記錄。

NXLog 工具將 MS SQL 事件記錄轉成 syslog，再傳送到 N-Reporter 做正規化、稽核與分析。

此文件適用於 MS SQL 2008 / 2012 / 2016 / 2019 /2022 版本。

sqlcmd 公用程式：<https://docs.microsoft.com/zh-tw/sql/tools/sqlcmd-utility?view=sql-server-ver15>

通用條件已取代 C2 稽核：<https://learn.microsoft.com/zh-tw/sql/database-engine/configure-windows/c2-audit-mode-server-configuration-option?view=sql-server-ver15>

sys.dm\_exec\_sessions 表格：<https://docs.microsoft.com/zh-tw/sql/relational-databases/system-dynamic-management-views/sys-dm-exec-sessions-transact-sql?view=sql-server-ver15>

sys.trace 表格：<https://docs.microsoft.com/zh-tw/sql/relational-databases/system-catalog-views/sys-traces-transact-sql?view=sql-server-ver15>

啟用通用條件合規性伺服器設定：<https://docs.microsoft.com/zh-tw/sql/database-engine/configure-windows/common-criteria-compliance-enabled-server-configuration-option?view=sql-server-ver15>

設定登入稽核：<https://docs.microsoft.com/zh-tw/sql/ssms/configure-login-auditing-sql-server-management-studio?%20view=sql-server-2017&view=sql-server-ver15#SSMSProcedure>

伺服器稽核規格：<https://docs.microsoft.com/zh-tw/sql/relational-databases/security/auditing/create-a-server-audit-and-server-audit-specification?view=sql-server-ver15>

資料庫稽核規格：<https://docs.microsoft.com/zh-tw/sql/relational-databases/security/auditing/create-a-server-audit-and-database-audit-specification?view=sql-server-ver15>

稽核動作群組：<https://docs.microsoft.com/zh-tw/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15>

## MS SQL Server 支援稽核記錄版本

| 版本         | SQL Server 2008 | SQL Server 2012 and 2014 | SQL Server 2016, 2019 and 2022 |
|------------|-----------------|--------------------------|--------------------------------|
| Enterprise | 伺服器和資料庫層級       | 伺服器和資料庫層級                | 伺服器和資料庫層級                      |
| Developer  | 伺服器和資料庫層級       | 伺服器和資料庫層級                | 伺服器和資料庫層級                      |
| Standard   | 不支援             | 伺服器層級                    | 伺服器和資料庫層級                      |
| Web        | 不支援             | 伺服器層級                    | 伺服器和資料庫層級                      |
| Express    | 不支援             | 伺服器層級                    | 伺服器和資料庫層級                      |

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

# 1 NXLog

## 1.1 NXLog 安裝

### (1) 下載 NXLog CE(Community Edition)

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

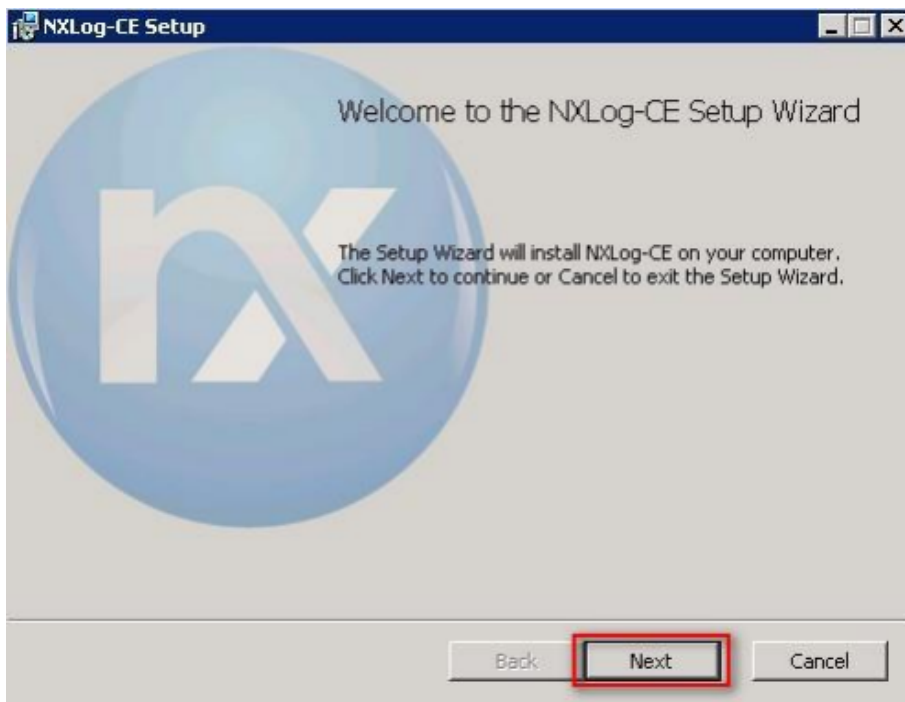
下載網址最新版 nxlog-ce-x.x.xxxx.msi · 範例: nxlog-ce-3.2.2329.msi



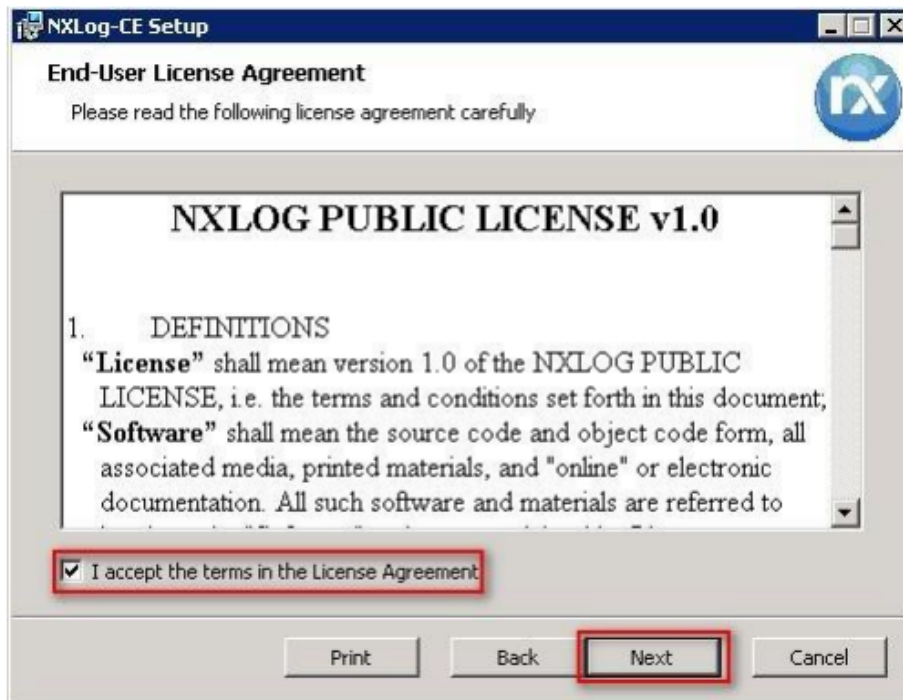
註：若需要下載 NXLog 32bit 版本，請與我們連繫。

### (2) 安裝 NXLog

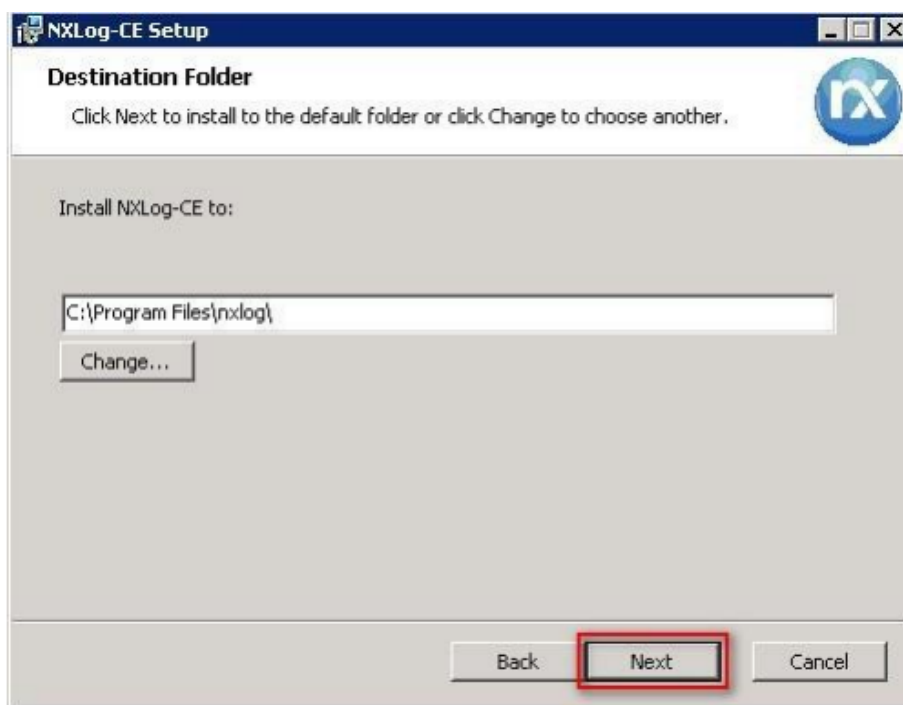
-> 點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



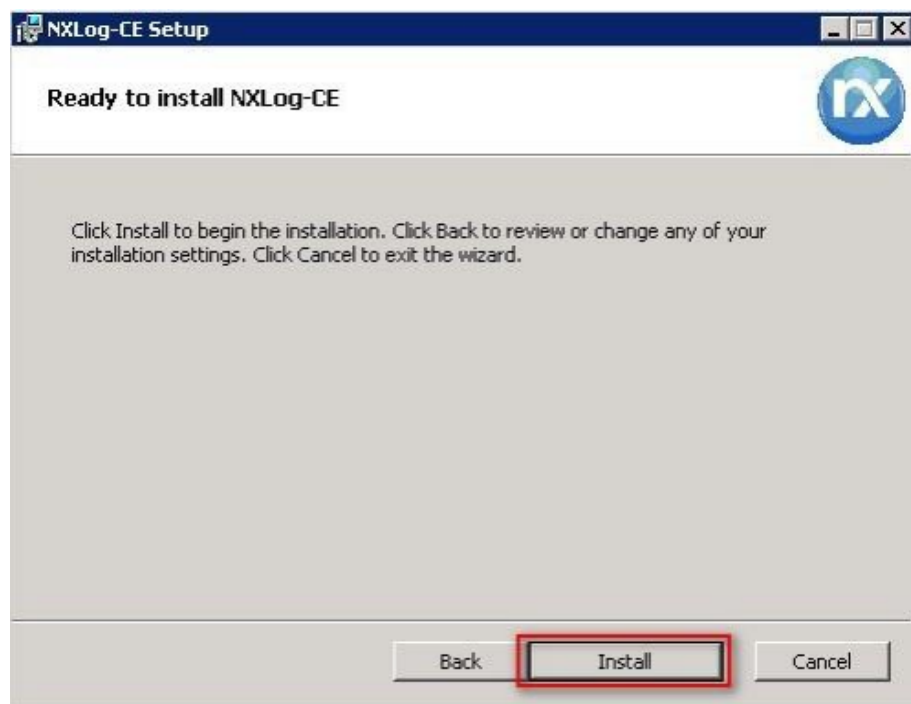
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



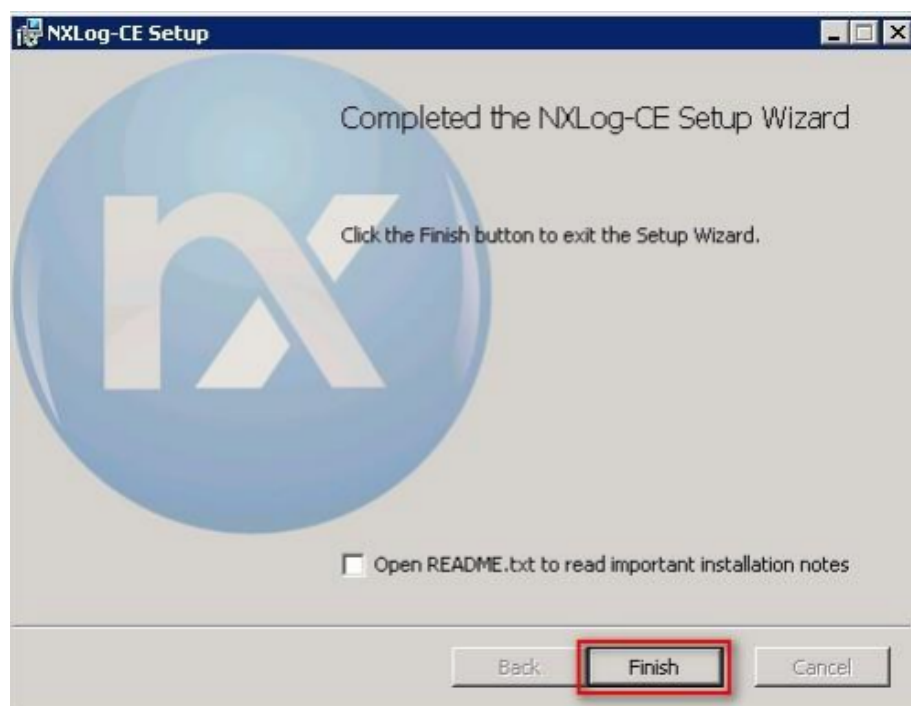
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].



-> 按 [Finish].



## 1.2 NXLog 設定檔下載

### 1.2.1 MS SQL 單機設定檔

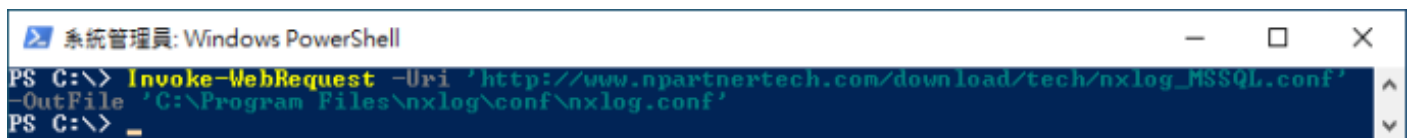
#### (1) 開啟 [Windows PowerShell]



#### (2) 下載 NXLog MS SQL 單機範本設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_MSSQL.conf](http://www.npartnertech.com/download/tech/nxlog_MSSQL.conf)

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



本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 位元，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

## 1.2.2 MS SQL Cluster 叢集設定檔

### (1) 開啟 [Windows PowerShell]



### (2) 下載 NXLog MS SQL Cluster 叢集範本設定檔 -> 覆蓋 Windows 系統 NXLog 設定檔

下載連結：[http://www.npartnertech.com/download/tech/nxlog\\_MSSQLcluster.conf](http://www.npartnertech.com/download/tech/nxlog_MSSQLcluster.conf)

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



本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 位元，紅色文字部位請改以下設定 'C:\Program Files (x86)  
\nxlog\conf\nxlog.conf'

## 1.3 NXLog 設定檔

### 1.3.1 MS SQL 單機設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

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

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

## For MS SQL instance Event Log use the following:
<Input in_sqllog>
    Module im_msvistalog
    ReadFromLast TRUE
    SavePos TRUE
    Query <QueryList> \
        <Query Id="0"> \
            <Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER']]]</Select> \
        </Query> \
    </QueryList>
</Input>

<Output out_sqllog>
    Module om_udp
    Host %NCloud%
    Port 514
    Exec $SyslogFacilityValue = 18;
    Exec $Message = "MSSQLSERVER" + ": " + string($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 sqllog>
    Path in_sqllog => out_sqllog
</Route>

## For Windows Event log use the following:
<Input in_eventlog>
    Module im_msvistalog
    ReadFromLast TRUE
    SavePos TRUE
    Query <QueryList> \
        <Query Id="0"> \
            <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626
or EventID=4627 or EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or
EventID=4672 or EventID=4675)]]</Select> \
            <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800
or EventID=4801 or EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or EventID=5058 or
EventID=5059 or EventID=4061)]]</Select> \
            <Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632
or EventID=5633 or EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or EventID=4772 or
EventID=4773 or EventID=4774)]]</Select> \
            <Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777
or EventID=4820 or EventID=4720 or EventID=4722 or EventID=4723 or EventID=4724 or EventID=4725 or
EventID=4726 or EventID=4727)]]</Select> \
            <Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733
or EventID=4734 or EventID=4735 or EventID=4738 or EventID=4739 or EventID=4740 or EventID=4749 or
EventID=4750 or EventID=4751)]]</Select> \
        </Query> \
    </QueryList>
```

```

        <Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764
or EventID=4765 or EventID=4766 or EventID=4767 or EventID=4780 or EventID=4781 or EventID=4782 or
EventID=4793 or EventID=4794)]]</Select> \
        <Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or
EventID=5376 or EventID=5377)]]</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 192.168.8.4
```

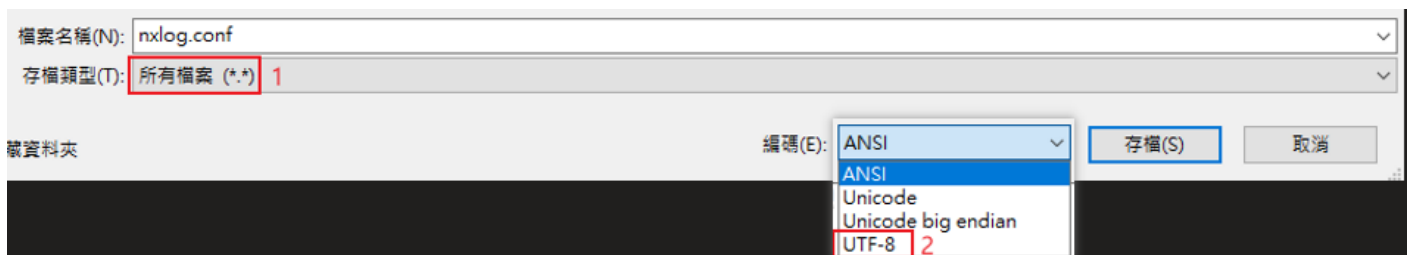
本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

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

藍色文字部位請輸入 MS SQL 執行個體名稱

```
<Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER'])]]</Select> \
```

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



### 1.3.2 MS SQL Cluster 叢集設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

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

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

## For MS SQL instance Event Log use the following:
<Input in_sqllog>
    Module im_msvistalog
    ReadFromLast TRUE
    SavePos TRUE
    Query <QueryList> \
        <Query Id="0"> \
            <Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER'])]]</Select> \
        </Query> \
    </QueryList>
</Input>

<Output out_sqllog>
    Module om_udp
    Host %NCloud%
    Port 514
    Exec $SyslogFacilityValue = 18;
    Exec $Message = "MSSQLSERVER" + ": " + string($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 sqllog>
    Path in_sqllog => out_sqllog
</Route>

## For Windows Event log use the following:
<Input in_eventlog>
    Module im_msvistalog
    ReadFromLast TRUE
    SavePos TRUE
    Query <QueryList> \
        <Query Id="0"> \
            <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626
or EventID=4627 or EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or
EventID=4672 or EventID=4675)]]</Select> \
            <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800
or EventID=4801 or EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or EventID=5058 or
EventID=5059 or EventID=4061)]]</Select> \
            <Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632
or EventID=5633 or EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or EventID=4772 or
EventID=4773 or EventID=4774)]]</Select> \
            <Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777
or EventID=4820 or EventID=4720 or EventID=4722 or EventID=4723 or EventID=4724 or EventID=4725 or
EventID=4726 or EventID=4727)]]</Select> \
            <Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733
or EventID=4734 or EventID=4735 or EventID=4738 or EventID=4739 or EventID=4740 or EventID=4749 or
EventID=4750 or EventID=4751)]]</Select> \
        </Query> \
    </QueryList>
```

```

        <Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764
or EventID=4765 or EventID=4766 or EventID=4767 or EventID=4780 or EventID=4781 or EventID=4782 or
EventID=4793 or EventID=4794)]]</Select> \
        <Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or
EventID=5376 or EventID=5377)]]</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering/ClusterSetDiagnostic">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering/Diagnostic">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering/DiagnosticVerbose">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering/Operational">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-CsvFs/Operational">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-Manager/Admin">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-Manager/Diagnostic">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-Manager/Tracing">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-NetFt/Operational">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-Clusport/Operational">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Management">*</Select> \
        <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Operational">*</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 192.168.8.4
```

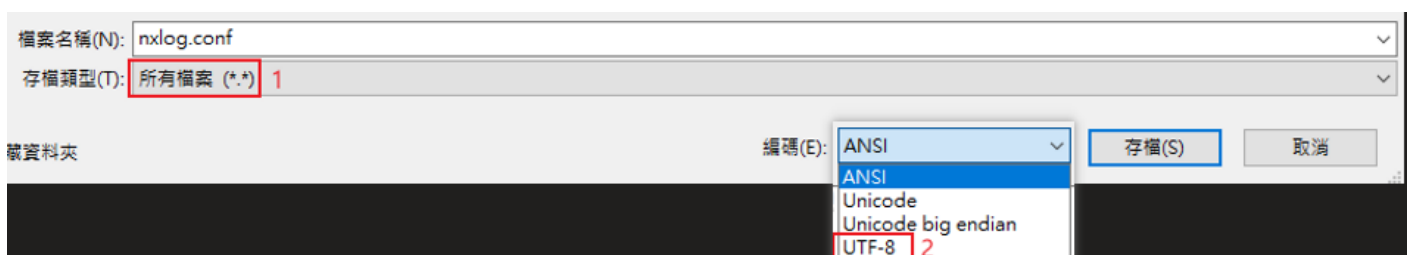
本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

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

藍色文字部位請輸入 MS SQL 執行個體名稱

```
<Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER'])]]</Select> \
```

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



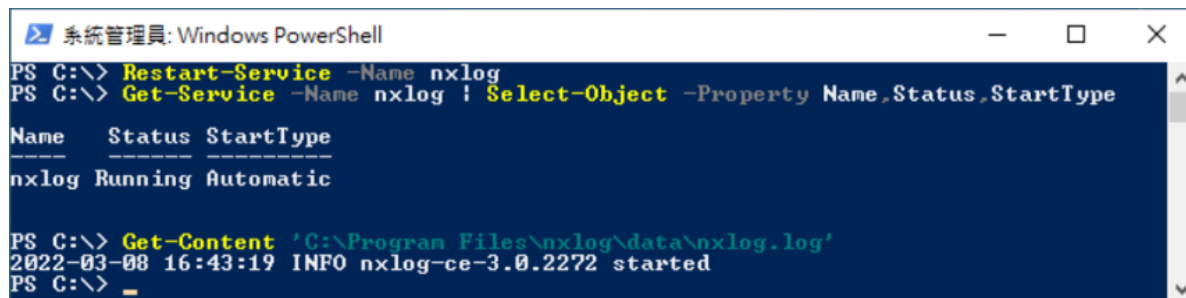
## 1.4 NXLog 啟動服務

### (1) 開啟 [Windows PowerShell]



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

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

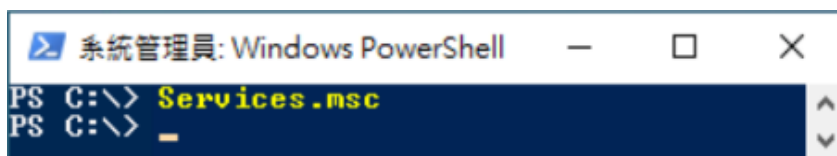
A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The window has a dark blue background with white text. The command prompt shows the following commands and output:  
PS C:\> Restart-Service -Name nxlog  
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType  

| Name  | Status  | StartType |
|-------|---------|-----------|
| nxlog | Running | Automatic |

  
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'  
2022-03-08 16:43:19 INFO nxlog-ce-3.0.2272 started  
PS C:\> \_

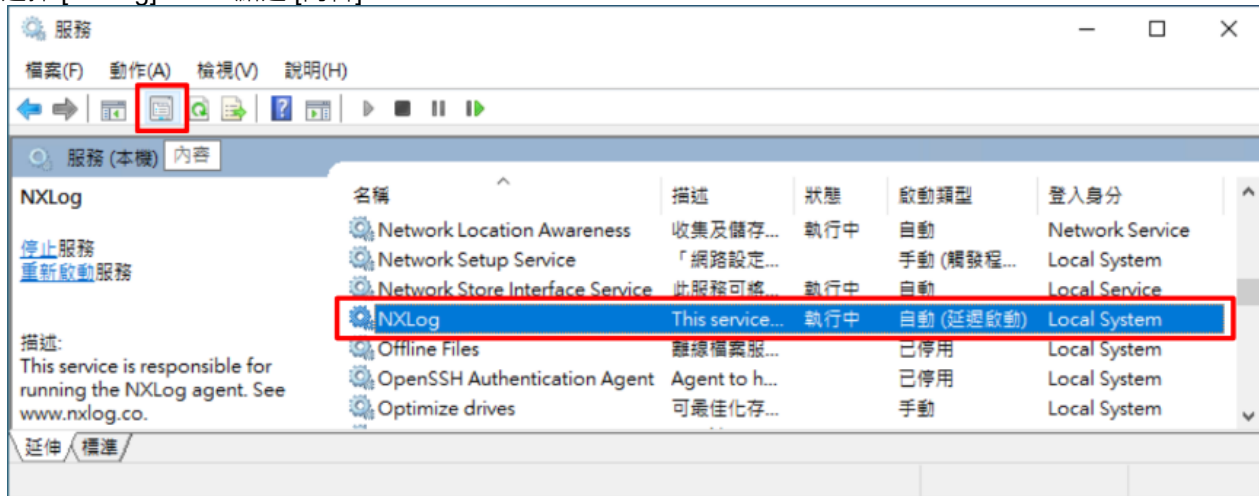
### (3) 開啟 [服務] 功能

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

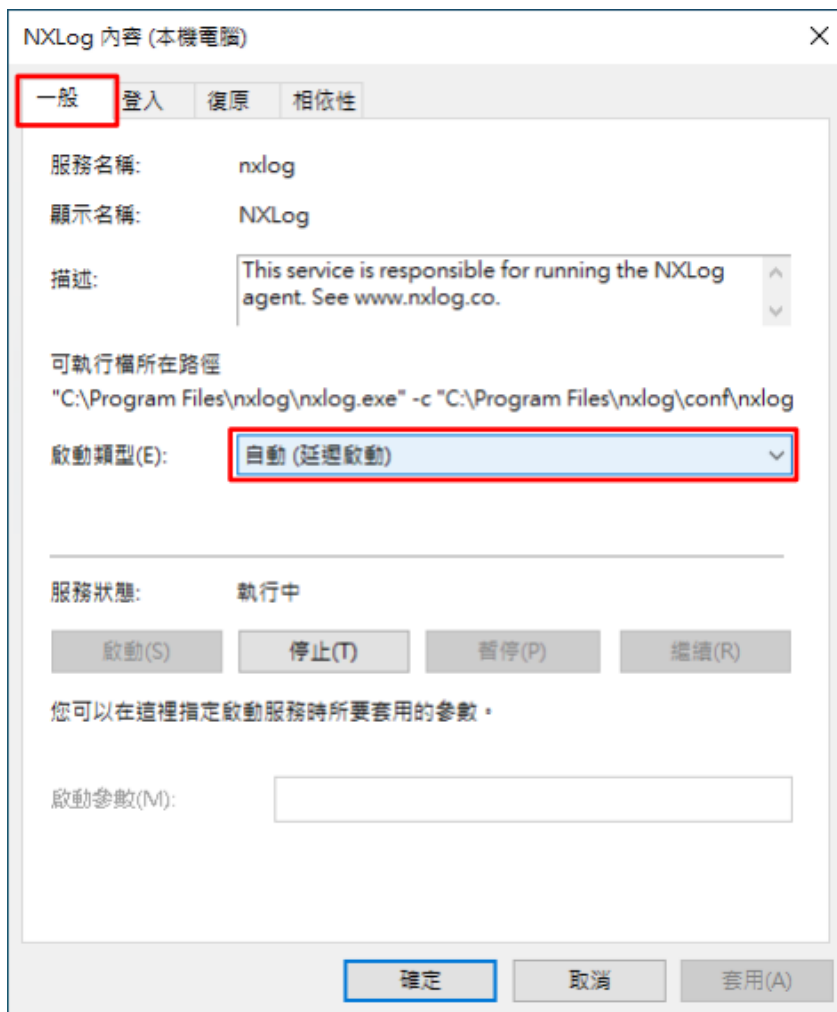


#### (4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選 [內容]



#### (5) [一般] 頁面 -> 確認; 啟動類型: [自動 (延遲啟動)]



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

NXLog 內容 (本機電腦) X

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務 v

第二次失敗時(S): 重新啟動服務 v

後續失敗時(U): 重新啟動服務 v

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

☐ 啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P):  瀏覽(B)...

命令列參數(C):

☐ 將失敗計數附加到命令列結尾 (/fail=%1%)(E)

**確定** 取消 套用(A)

## 2 SQL2008

### 2.1 稽核登入

啟用登入稽核，以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。

以下分別為圖形介面和指令介面設定方式。

#### 2.1.1 使用圖形介面方式設定

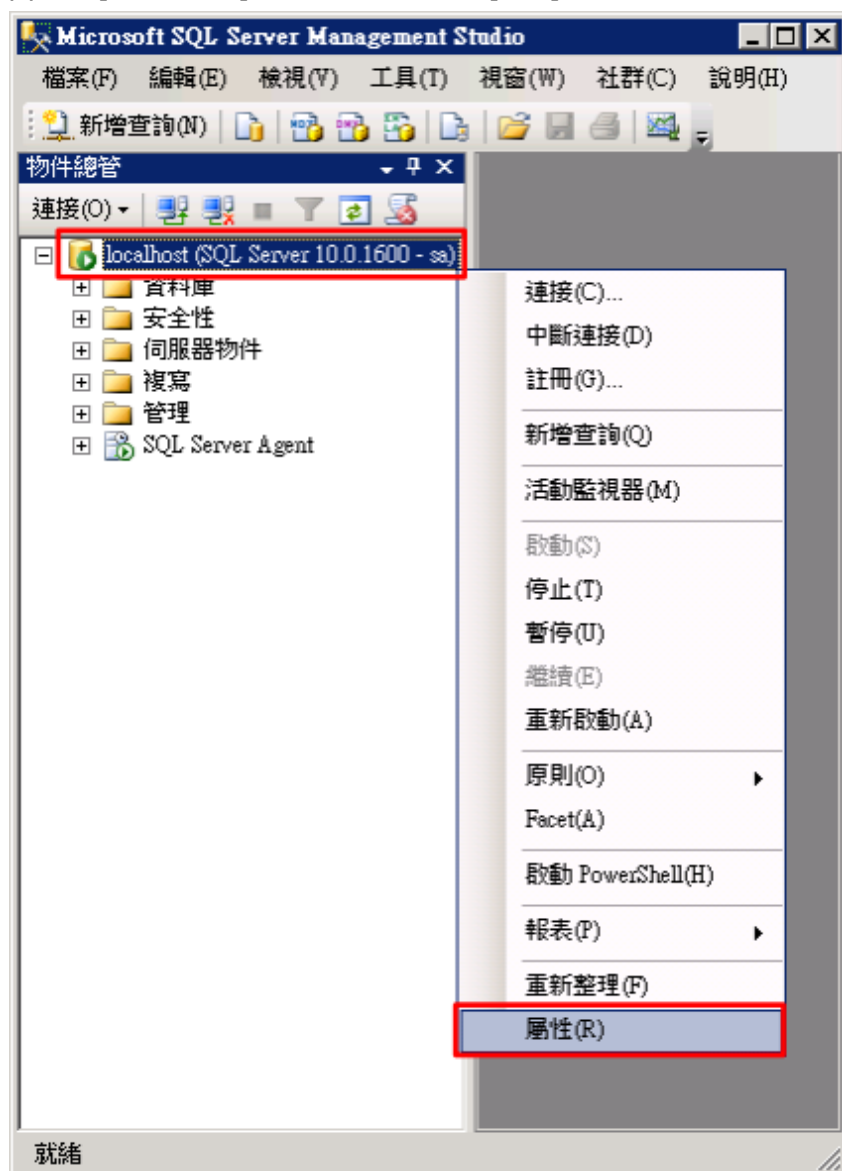
(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

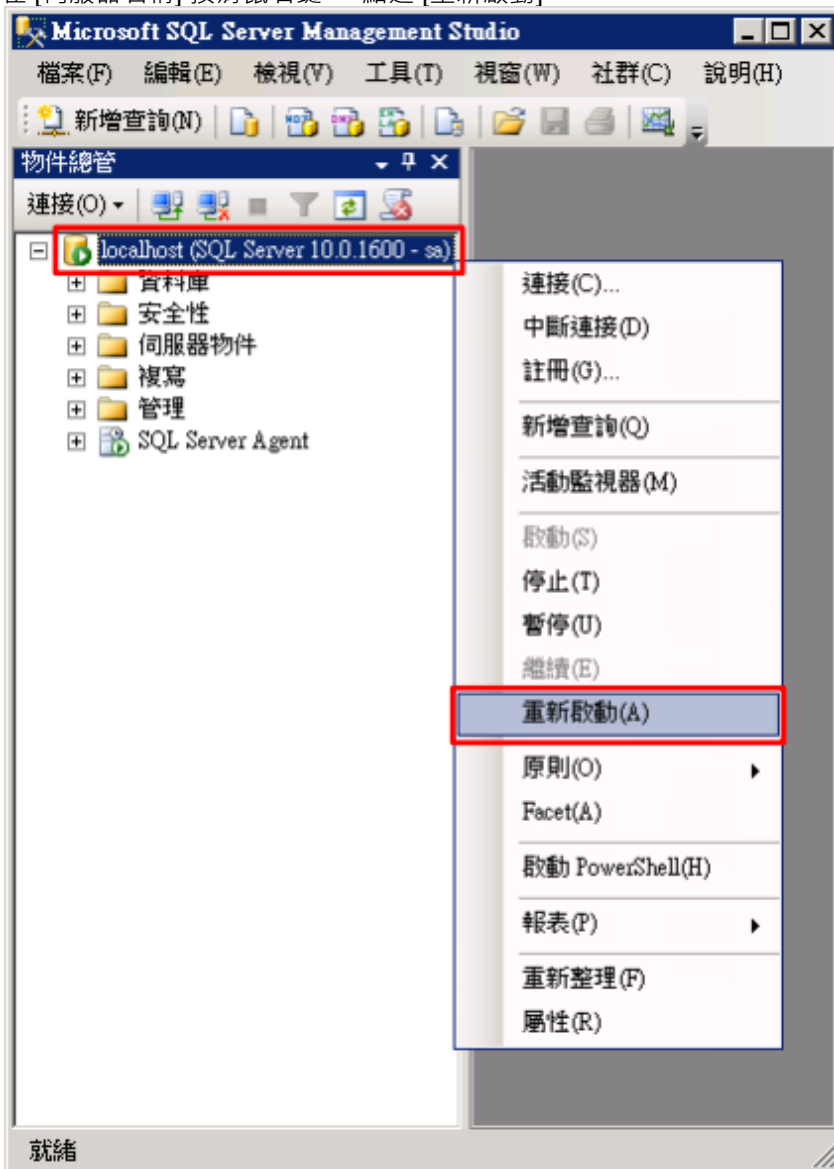


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

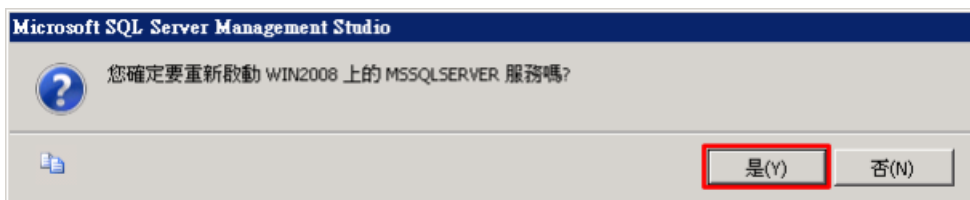


(5) 重新啟動 MS SQL SERVER 服務

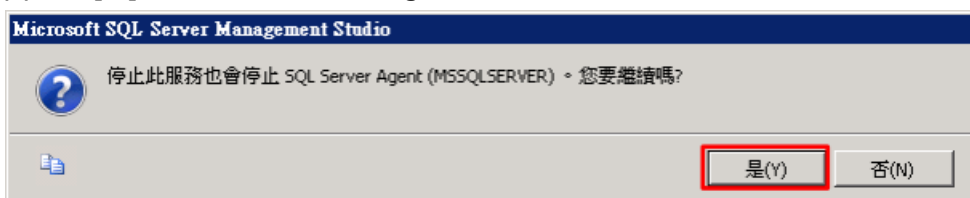
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務



(7) 按 [是] 停止 SQL SERVER Agent 服務



## 2.1.2 使用指令介面方式設定

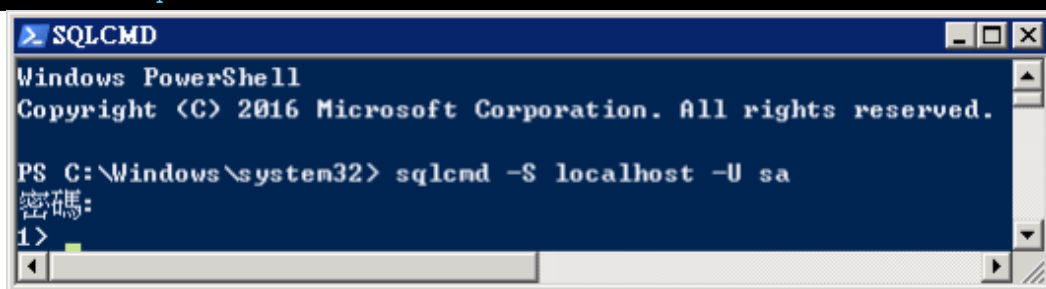
### (1) 開啟 [Windows Powershell]



### (2) 分別為 sa 或 Windows 帳號登入方式

#### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

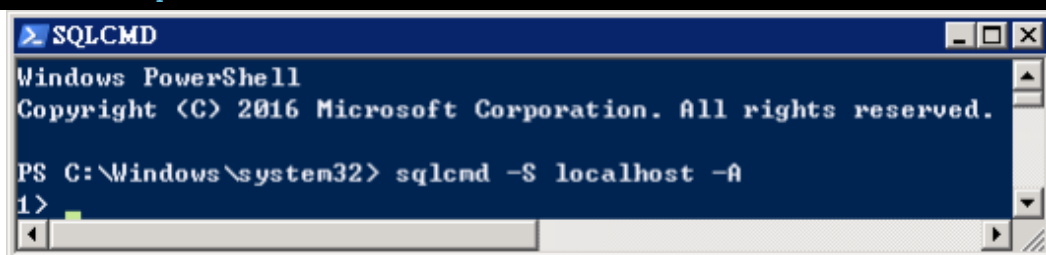


Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

#### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



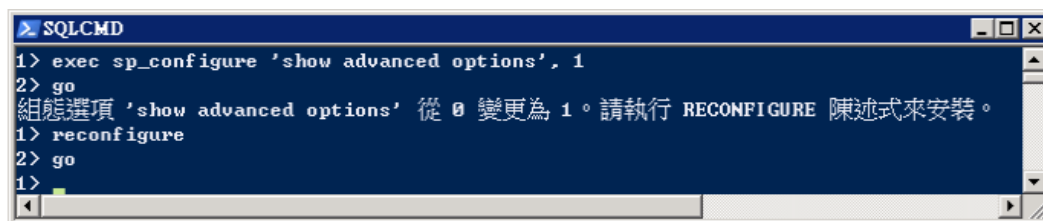
### (3) 切換資料庫

```
1 > use master
2 > go
```



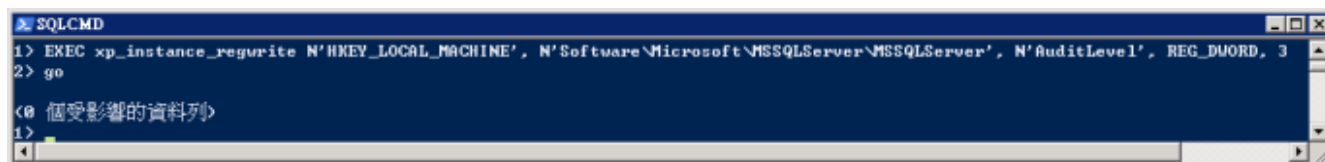
#### (4) 使用 sp\_configure 列出進階選項

```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



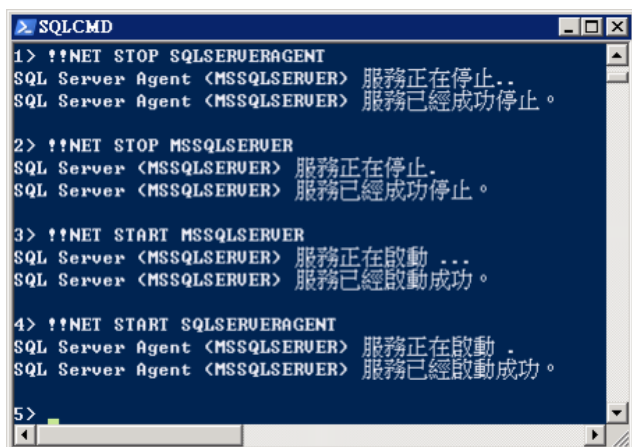
#### (5) 啟用失敗和成功的登入記錄

```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
```



#### (6) 重新啟動 MS SQL SERVER 服務

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



## 2.2 設定稽核

### 2.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

#### 2.2.1.1 使用圖形介面方式設定

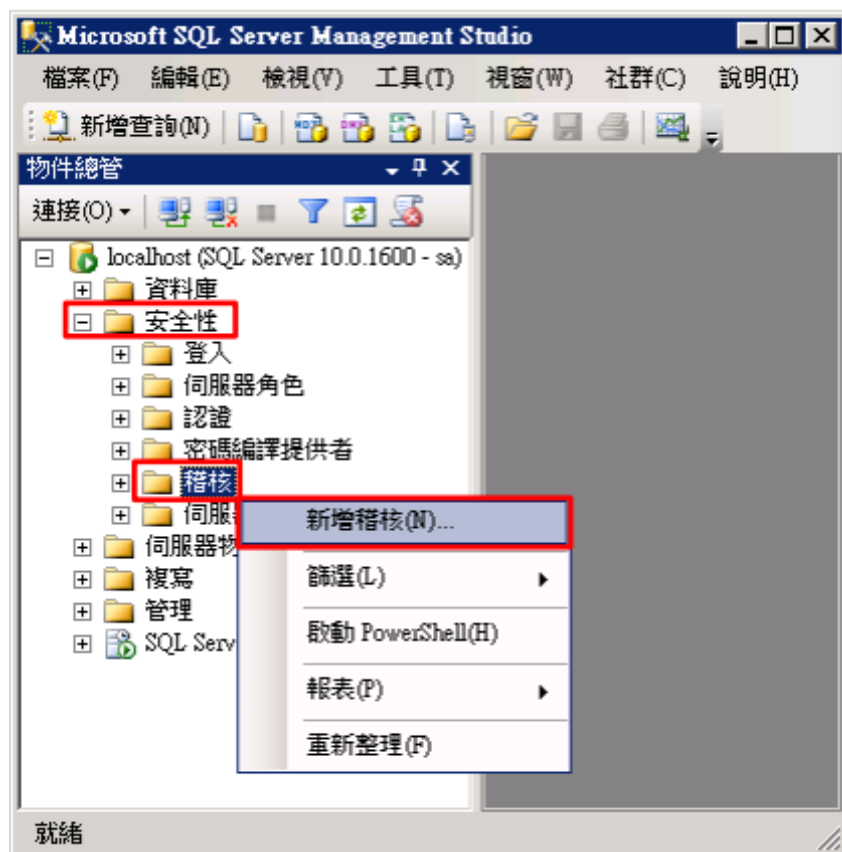
##### (1) 開啟 [SQL Server Management Studio]



##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 選擇稽核目的地: **[Application Log]** 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

**建立稽核**

就緒

選取頁面

一般

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒): 1000

☐ 於稽核記錄失敗時關閉伺服器(S)

稽核目的地(D): Application Log

檔案路徑(P):

最大換用檔案(O): 2147483647

☒ 無限制(U)

檔案大小上限(Z): 0 MB GB TB(T)

☒ 無限制(L)

☐ 保留磁碟空間(R)

連接

localhost [sa]

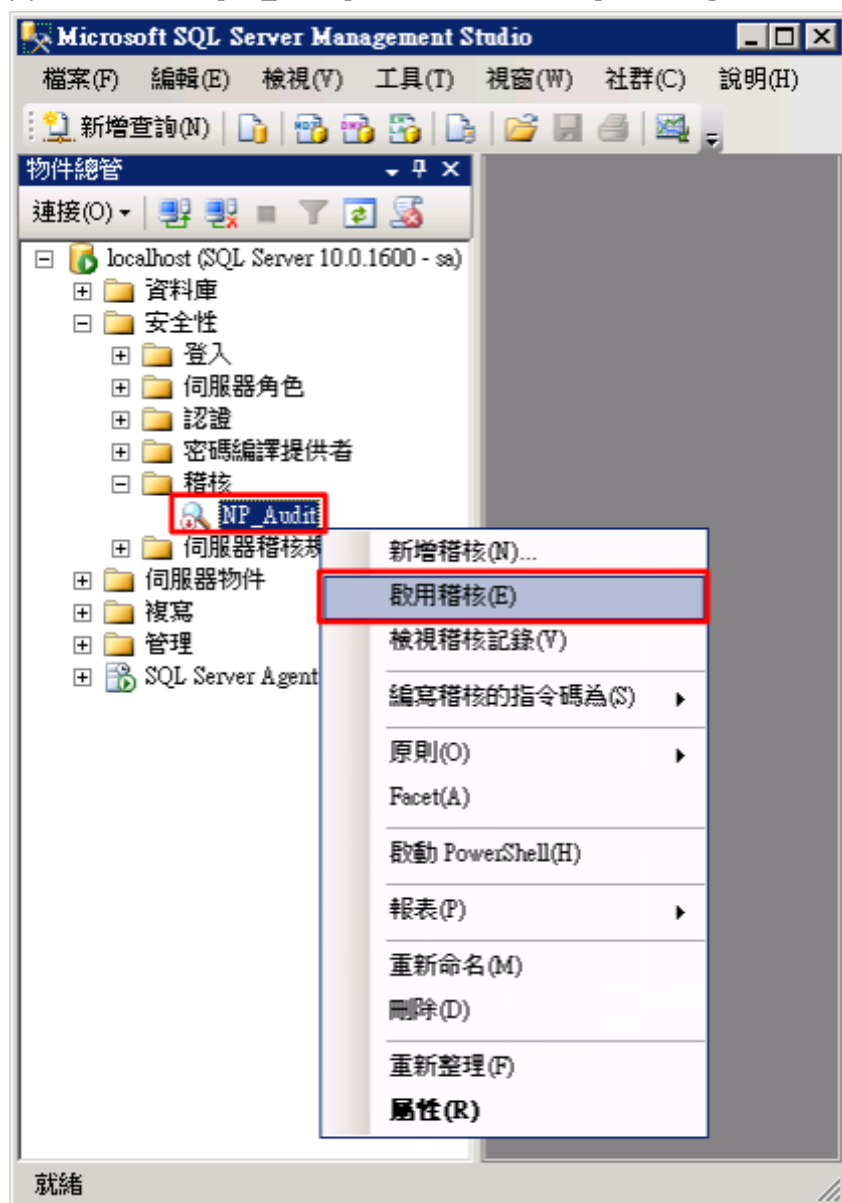
[檢視連接屬性](#)

進度

就緒

確定 取消 說明

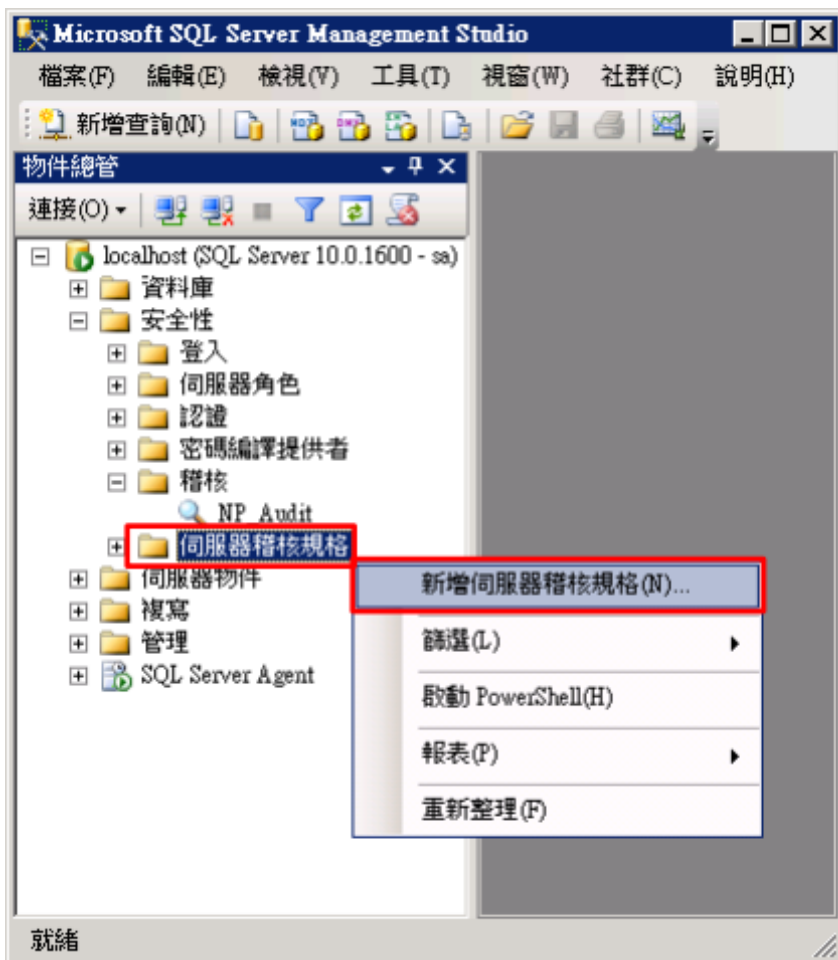
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



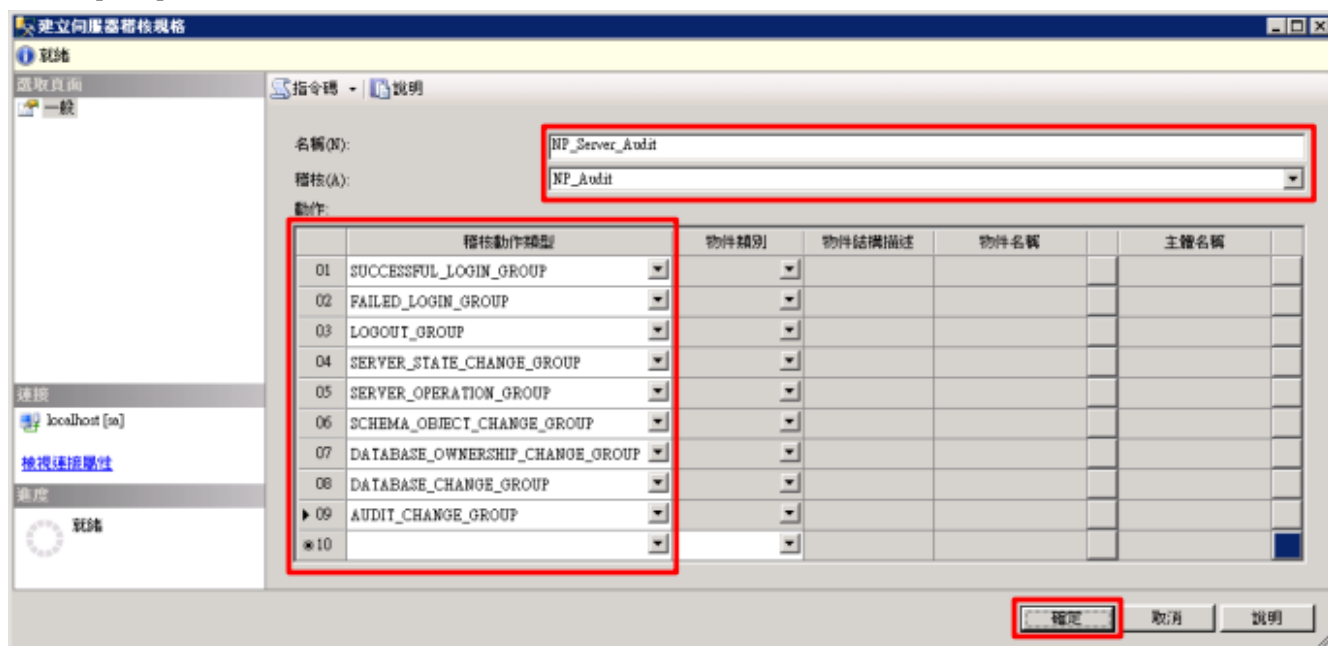
(6) 按 [關閉]



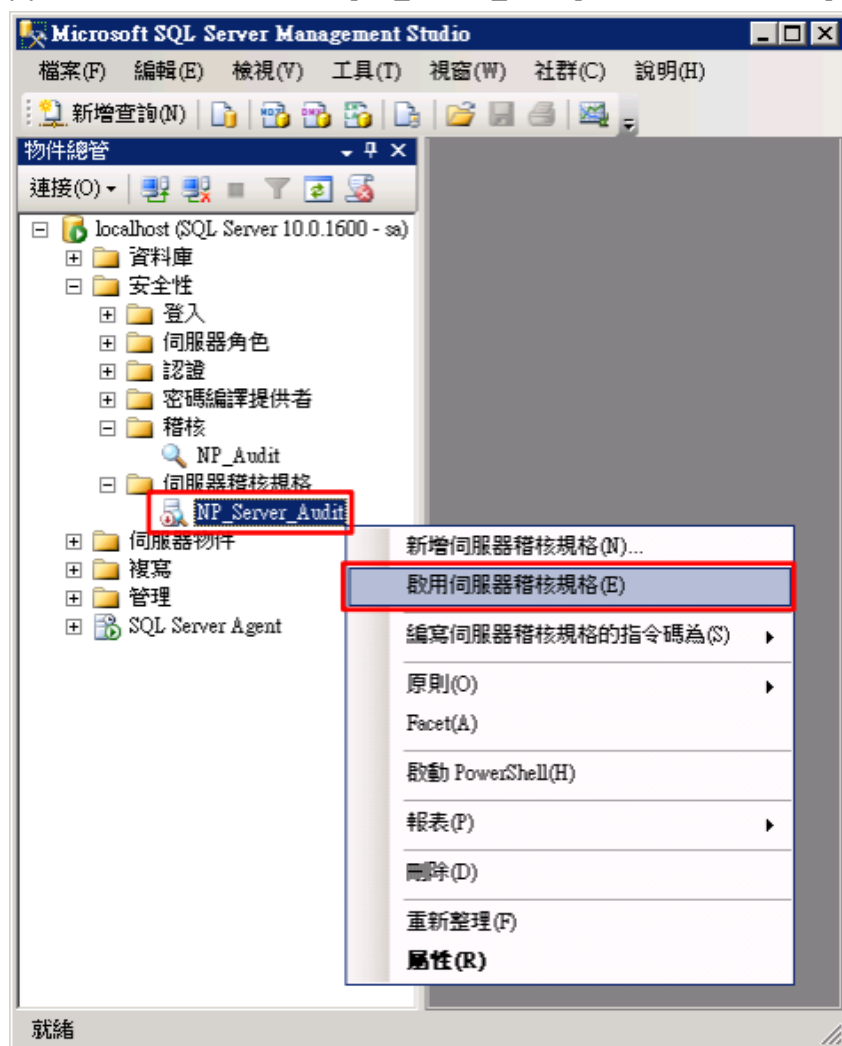
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



(8) 輸入稽核名稱: `NP_Server_Audit` -> 選擇稽核: `[NP_Audit]` 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在伺服器稽核規格名稱: [NP\_Server\_Audit] 按滑鼠右鍵 -> 點選 [啟用伺服器稽核規格]

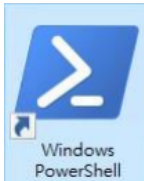


(10) 按 [關閉]



### 2.2.1.2 使用指令介面方式設定

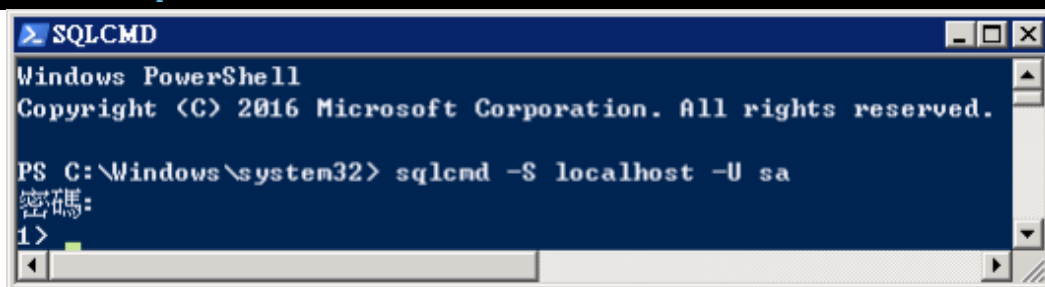
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

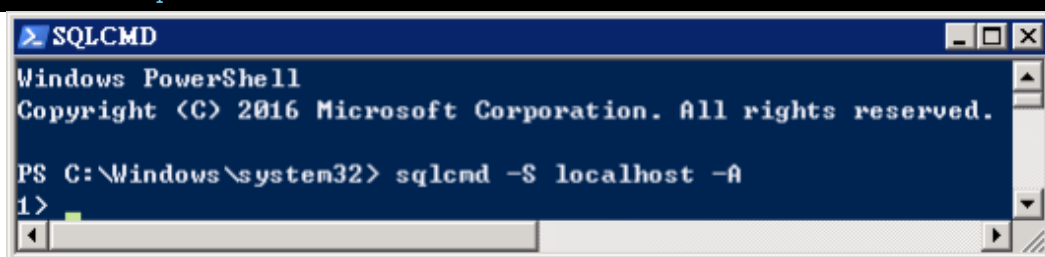


Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



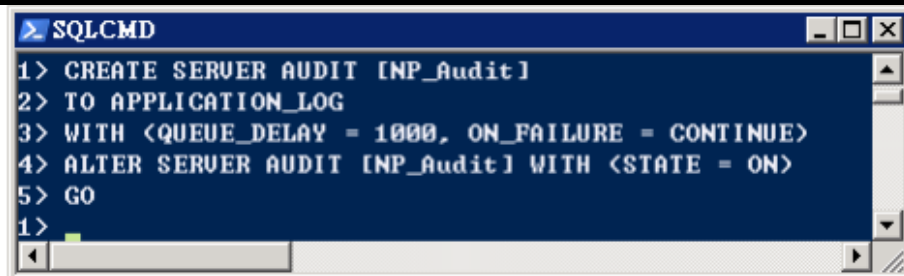
#### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

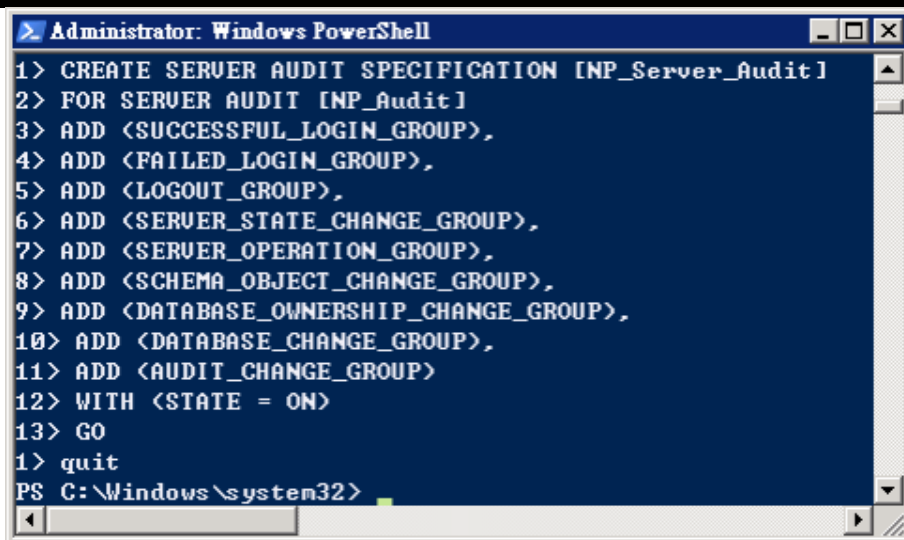
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



A screenshot of a SQLCMD command window. The title bar reads 'SQLCMD'. The command prompt shows the following commands being executed: 1> CREATE SERVER AUDIT [NP\_Audit], 2> TO APPLICATION\_LOG, 3> WITH <QUEUE\_DELAY = 1000, ON\_FAILURE = CONTINUE>, 4> ALTER SERVER AUDIT [NP\_Audit] WITH <STATE = ON>, 5> GO. The prompt is currently at 1>.

(5) 設定稽核伺服器・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP)
12 > WITH (STATE = ON)
13 > GO
1 > quit
```



A screenshot of an Administrator: Windows PowerShell window. The command prompt shows the following commands being executed: 1> CREATE SERVER AUDIT SPECIFICATION [NP\_Server\_Audit], 2> FOR SERVER AUDIT [NP\_Audit], 3> ADD <SUCCESSFUL\_LOGIN\_GROUP>, 4> ADD <FAILED\_LOGIN\_GROUP>, 5> ADD <LOGOUT\_GROUP>, 6> ADD <SERVER\_STATE\_CHANGE\_GROUP>, 7> ADD <SERVER\_OPERATION\_GROUP>, 8> ADD <SCHEMA\_OBJECT\_CHANGE\_GROUP>, 9> ADD <DATABASE\_OWNERSHIP\_CHANGE\_GROUP>, 10> ADD <DATABASE\_CHANGE\_GROUP>, 11> ADD <AUDIT\_CHANGE\_GROUP>, 12> WITH <STATE = ON>, 13> GO, 1> quit. The prompt is currently at PS C:\Windows\system32>.

紅色文字部位請輸入伺服器稽核規格名稱

## 2.2.2 稽核資料庫層級

啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

以下分別為圖形介面和指令介面設定方式。

### 2.2.2.1 使用圖形介面方式設定

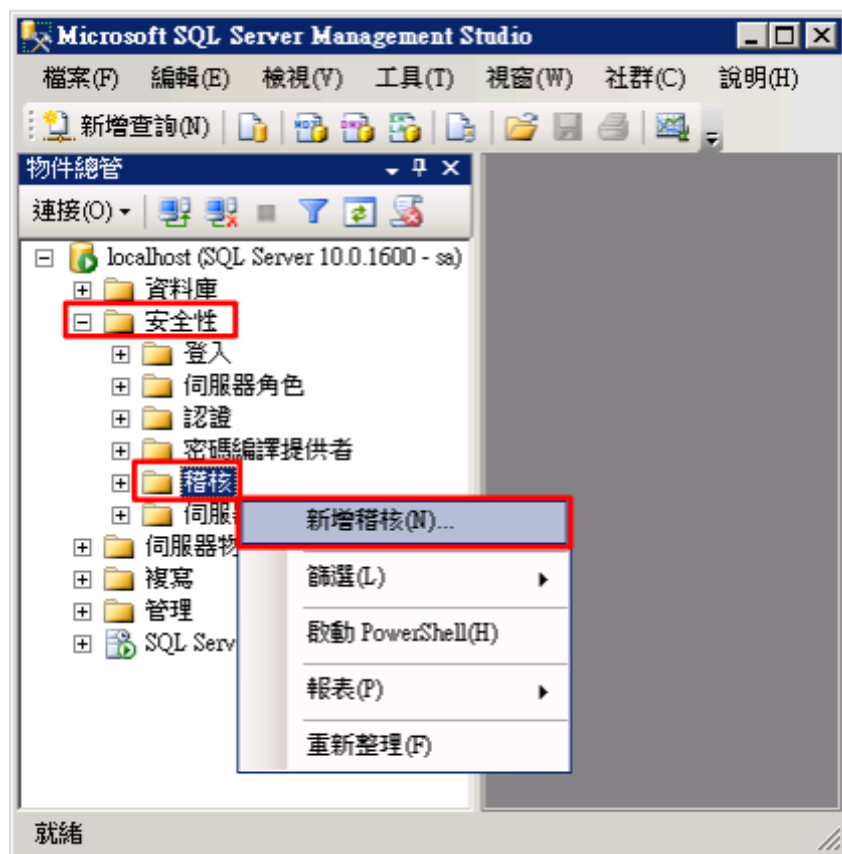
#### (1) 開啟 [SQL Server Management Studio]



#### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 選擇稽核目的地: **[Application Log]** 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

**建立稽核**

就緒

選取頁面

一般

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒): 1000

☐ 於稽核記錄失敗時關閉伺服器(S)

稽核目的地(D): Application Log

檔案路徑(P):

最大換用檔案(O): 2147483647

☒ 無限制(U)

檔案大小上限(Z): 0 MB GB TB(T)

☒ 無限制(L)

☐ 保留磁碟空間(R)

連接

localhost [sa]

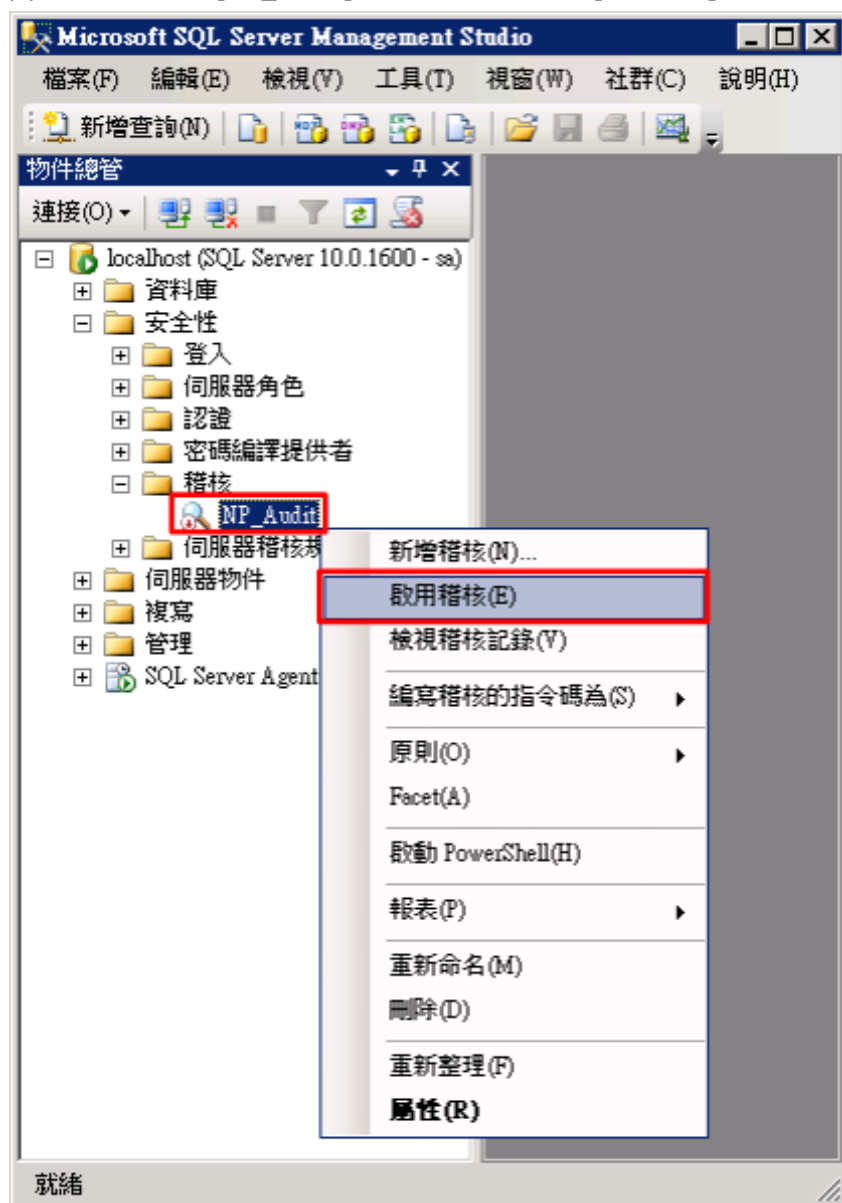
[檢視連接屬性](#)

進度

就緒

確定 取消 說明

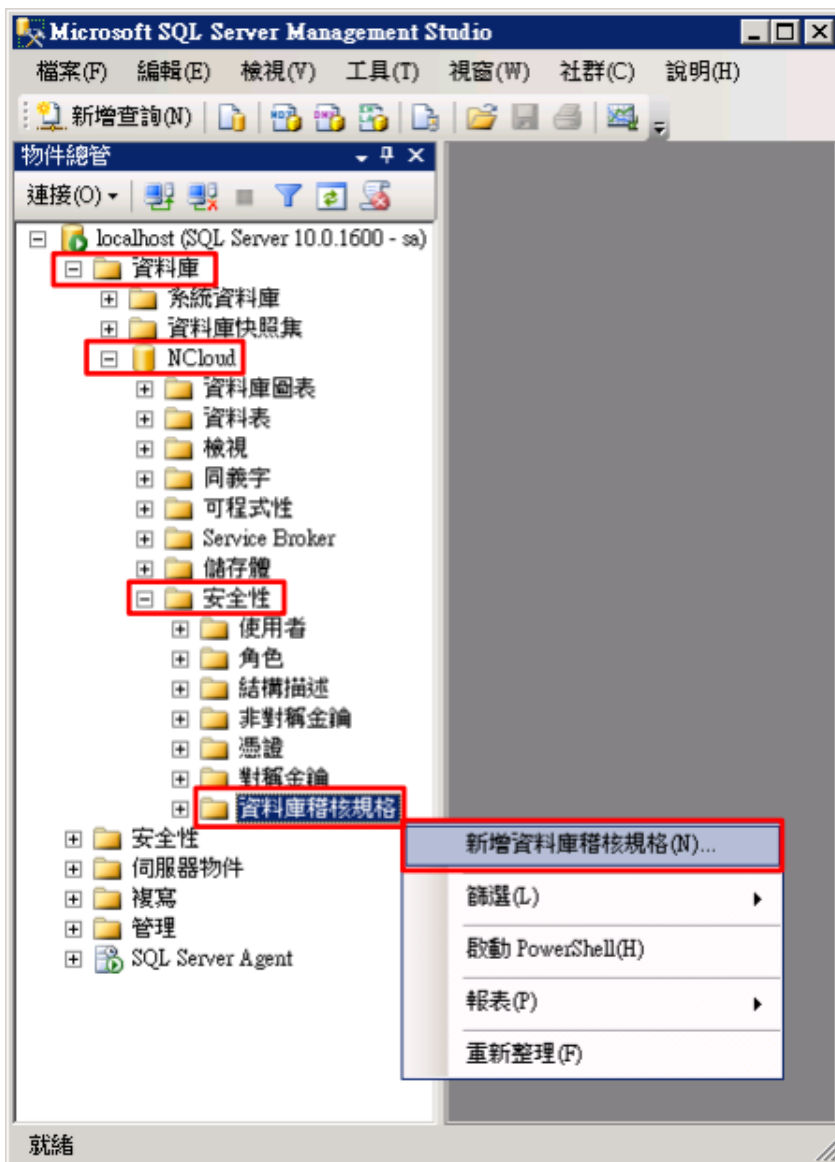
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



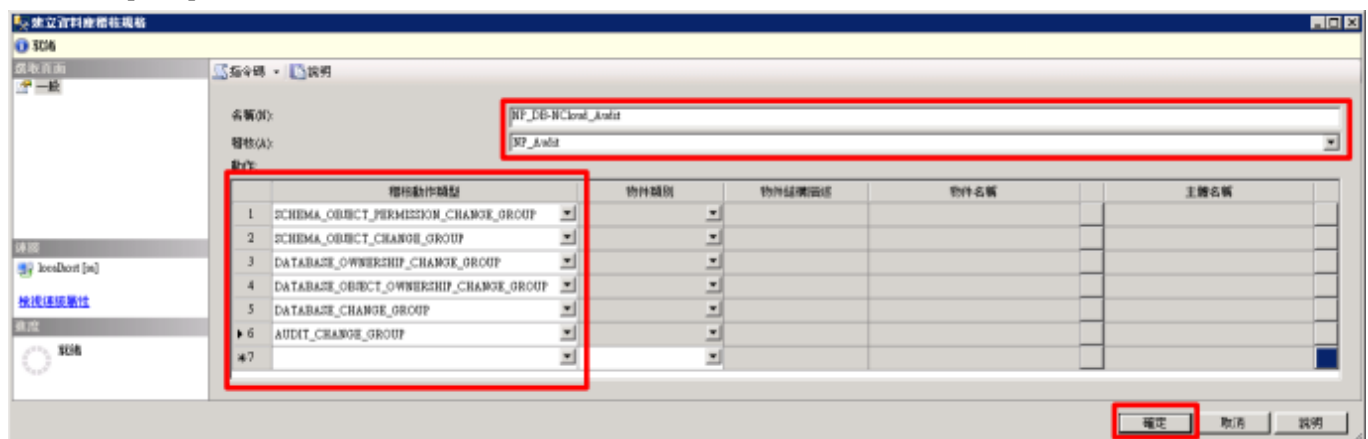
(6) 按 [關閉]



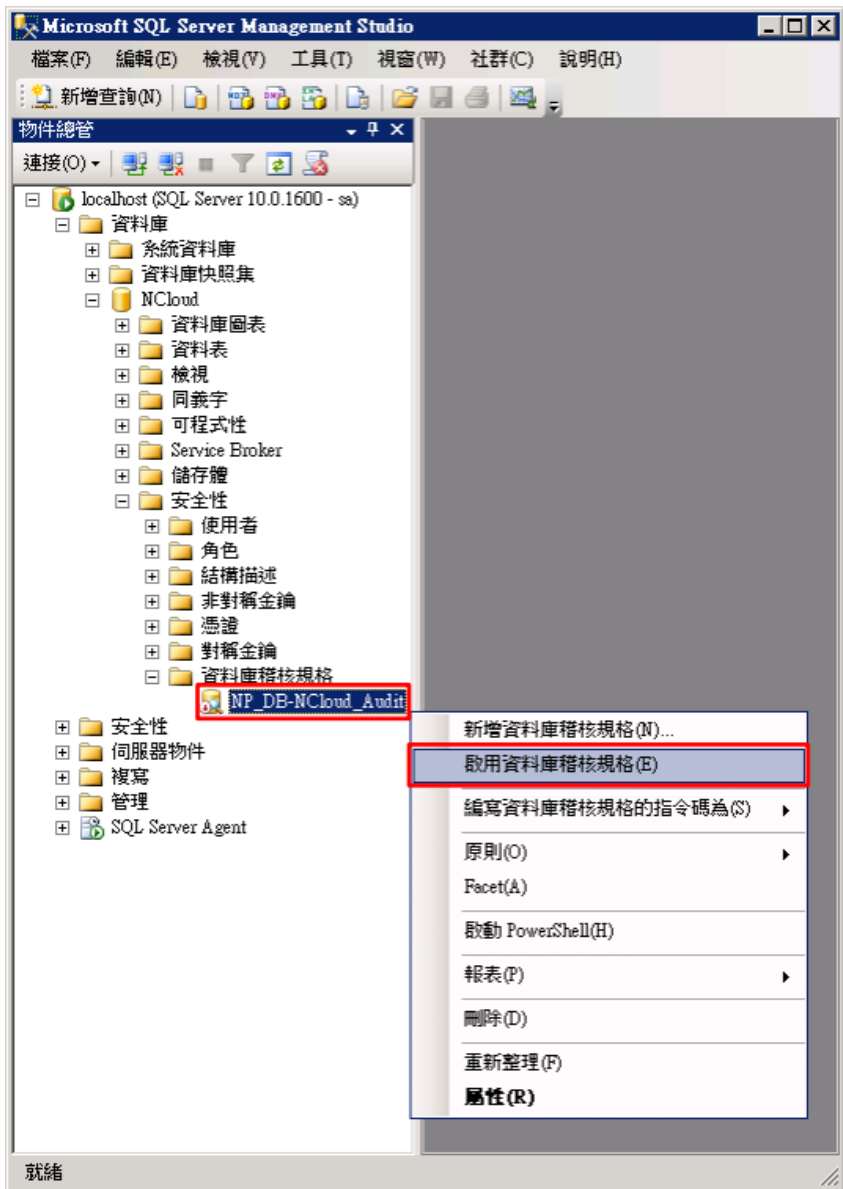
- (7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



- (8) 輸入稽核名稱: NP\_DB-NCloud\_Audit -> 選擇稽核: [NP\_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在資料庫稽核規格名稱: [NP\_DB-NCloud\_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10) 按 [關閉]



### 2.2.2.2 使用指令介面方式設定

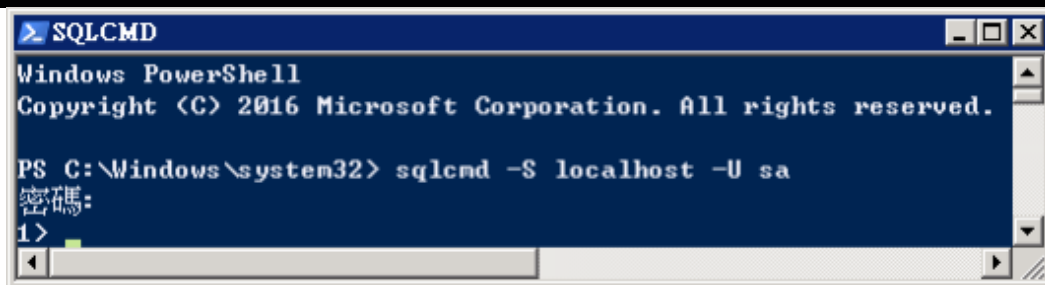
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

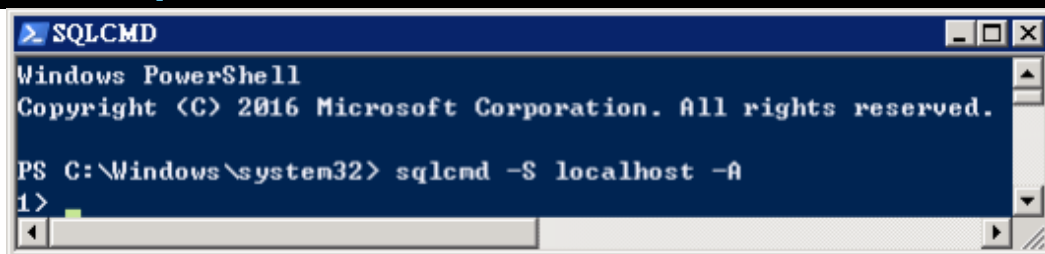


Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



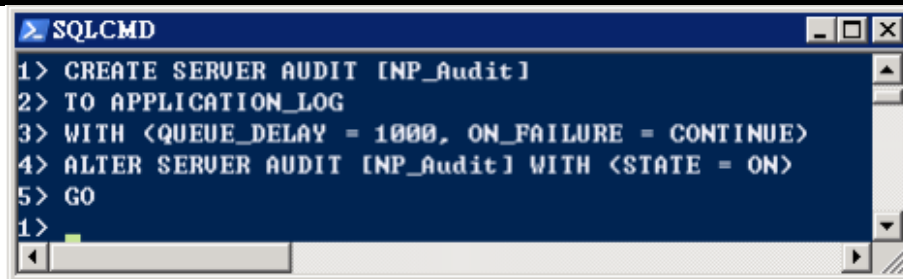
### (3) 切換資料庫

```
1 > use master
2 > go
```



### (4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



紅色文字部位請輸入稽核名稱

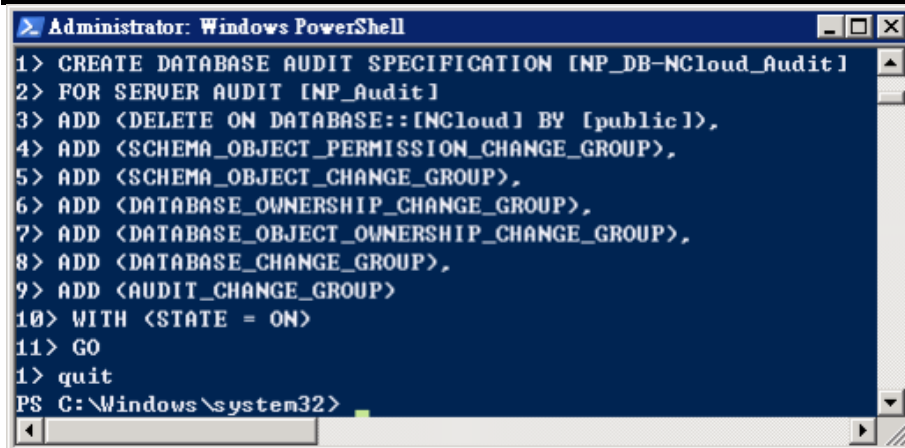
### (5) 切換到稽核資料庫，範例：NCloud

```
1 > use NCloud
2 > go
```



(6) 設定稽核 NCloud(範例) 資料庫・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8 > ADD (DATABASE_CHANGE_GROUP),
9 > ADD (AUDIT_CHANGE_GROUP)
10 > WITH (STATE = ON)
11 > GO
1 > quit
```



紅色文字部位請輸入資料庫稽核規格名稱

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

紅色文字部位請輸入稽核資料庫名稱

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

## 2.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

### 2.3.1 網域

#### 2.3.1.1 組織單位設定

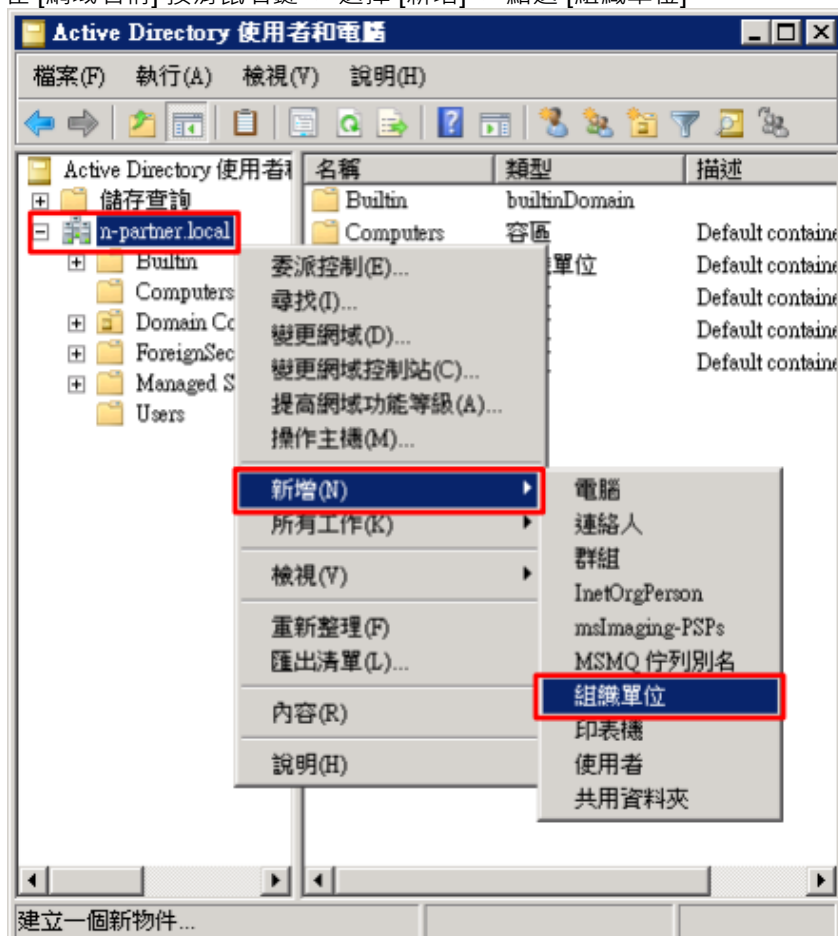
##### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



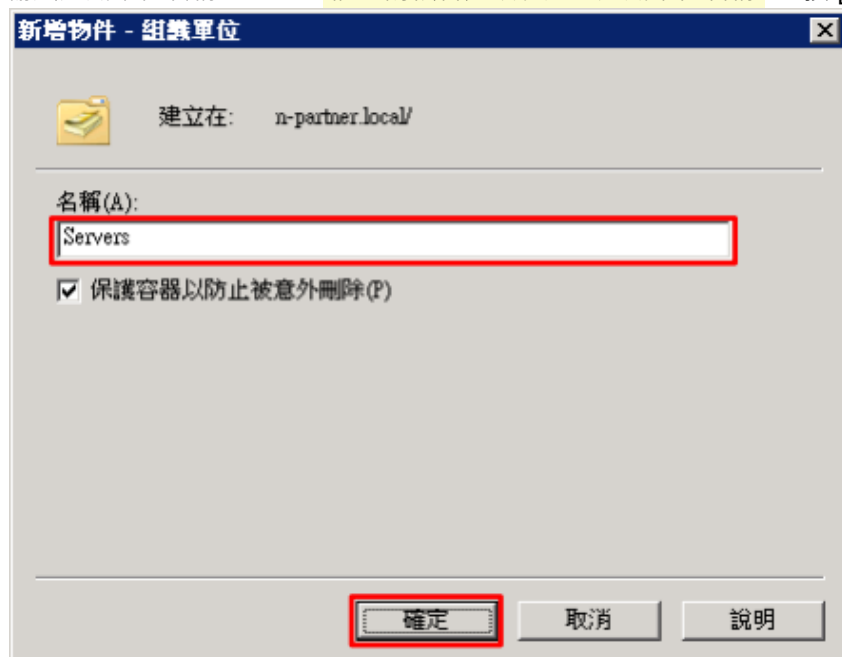
##### (2) 新增組織單位

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



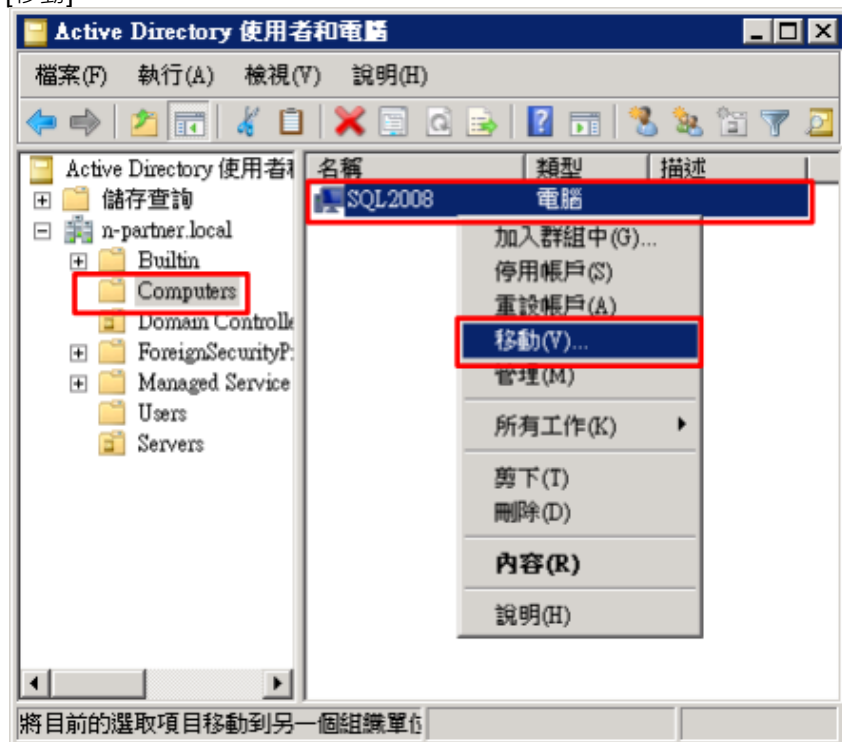
### (3) 輸入組織單位名稱

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



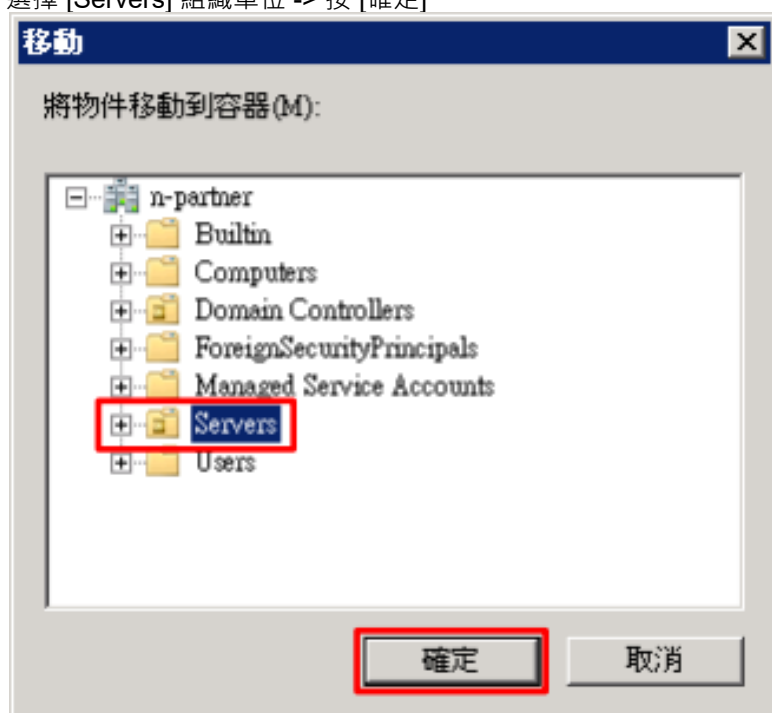
### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL 2008] 伺服器, 按滑鼠右鍵, 註：請依客戶環境選擇 MS SQL Server 主機 -> 點選 [移動]



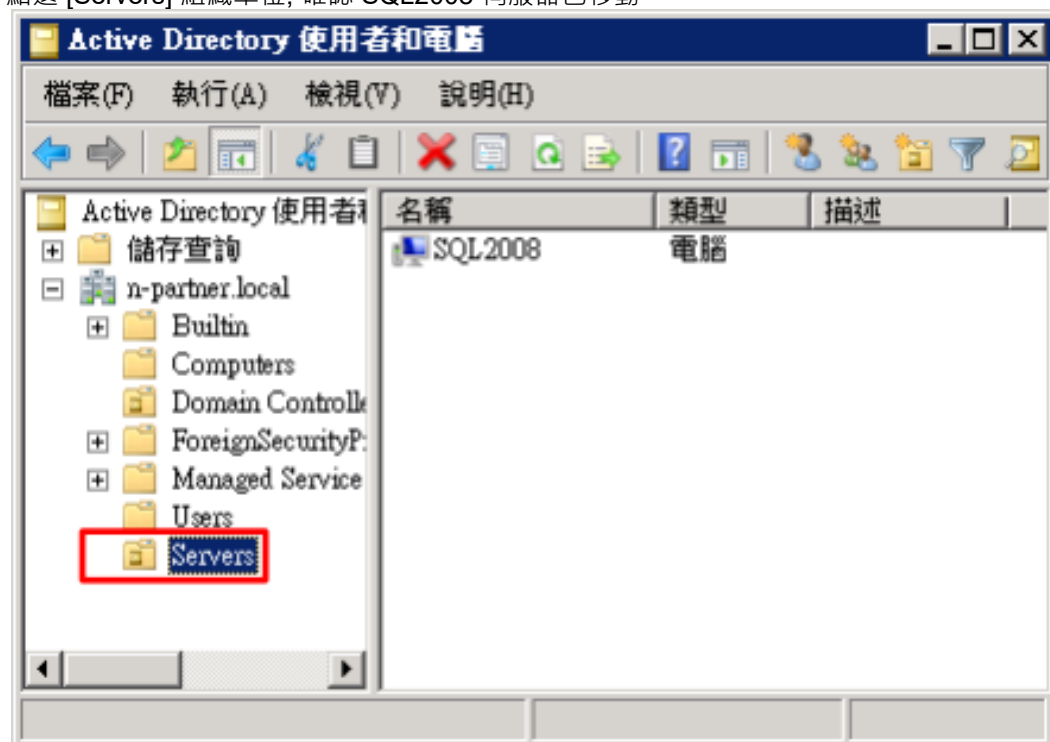
### (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



### (6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位, 確認 SQL2008 伺服器已移動。



### 2.3.1.2 群組原則設定

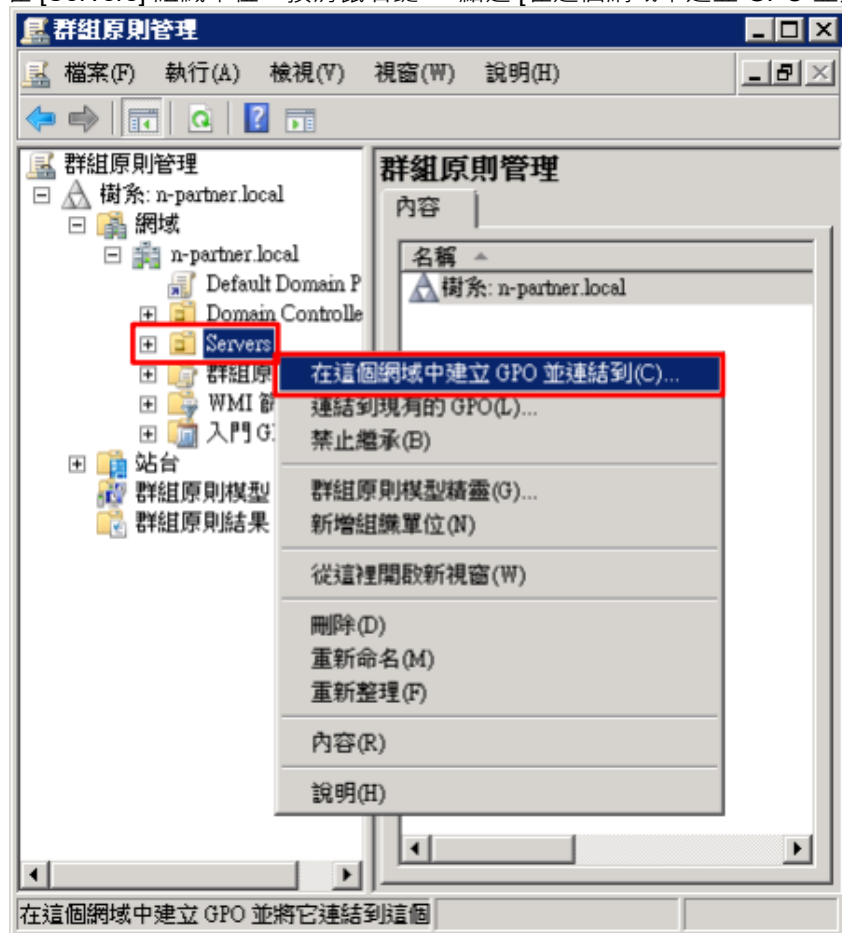
#### (1) 開啟群組原則管理

開啟 [群組原則管理]



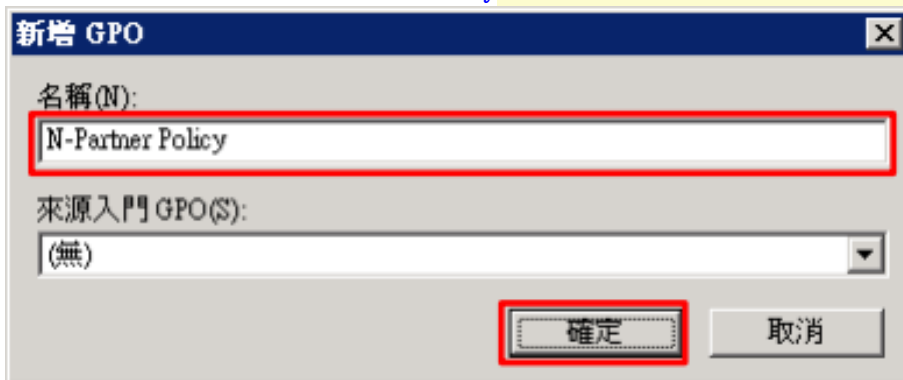
#### (2) 在 Servers 組織單位，新增群組原則物件

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



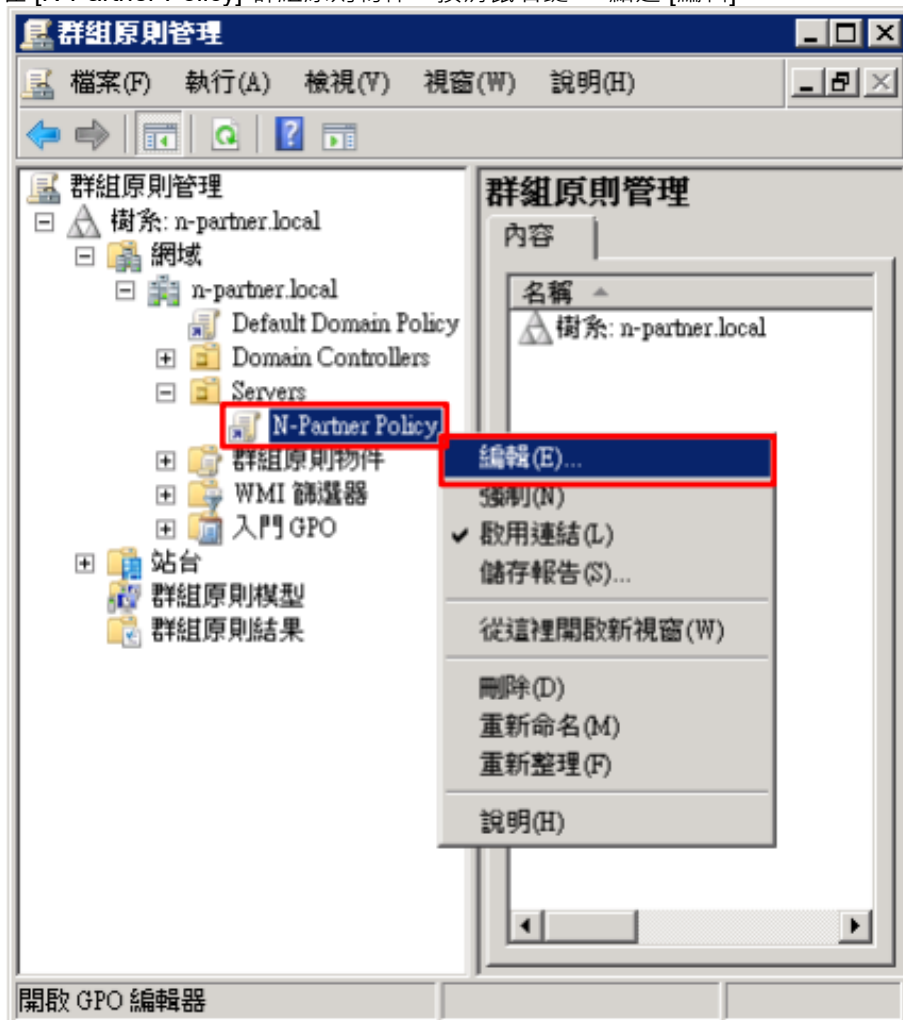
### (3) 輸入群組原則物件名稱

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



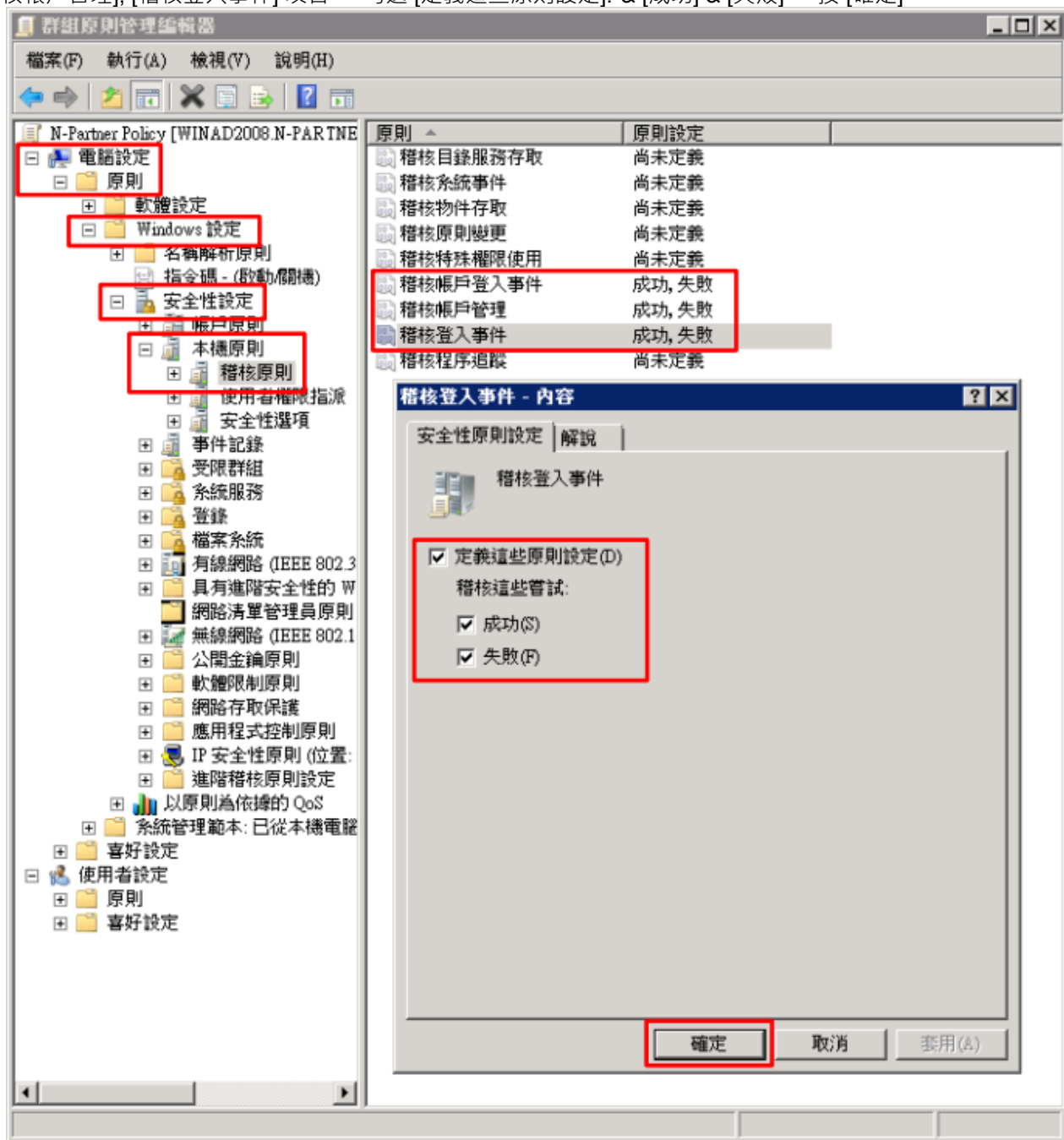
### (4) 編輯群組原則物件

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



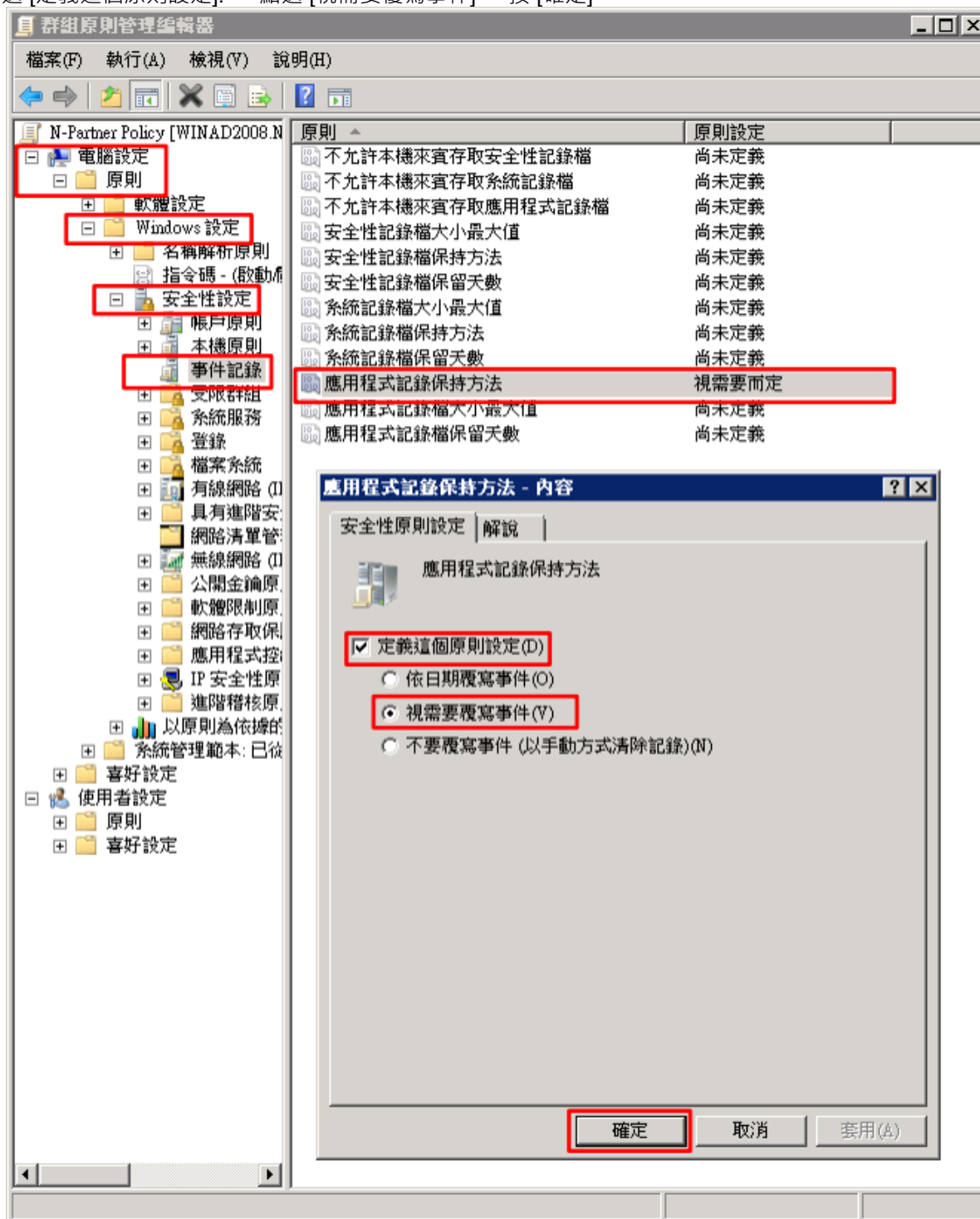
##### (5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



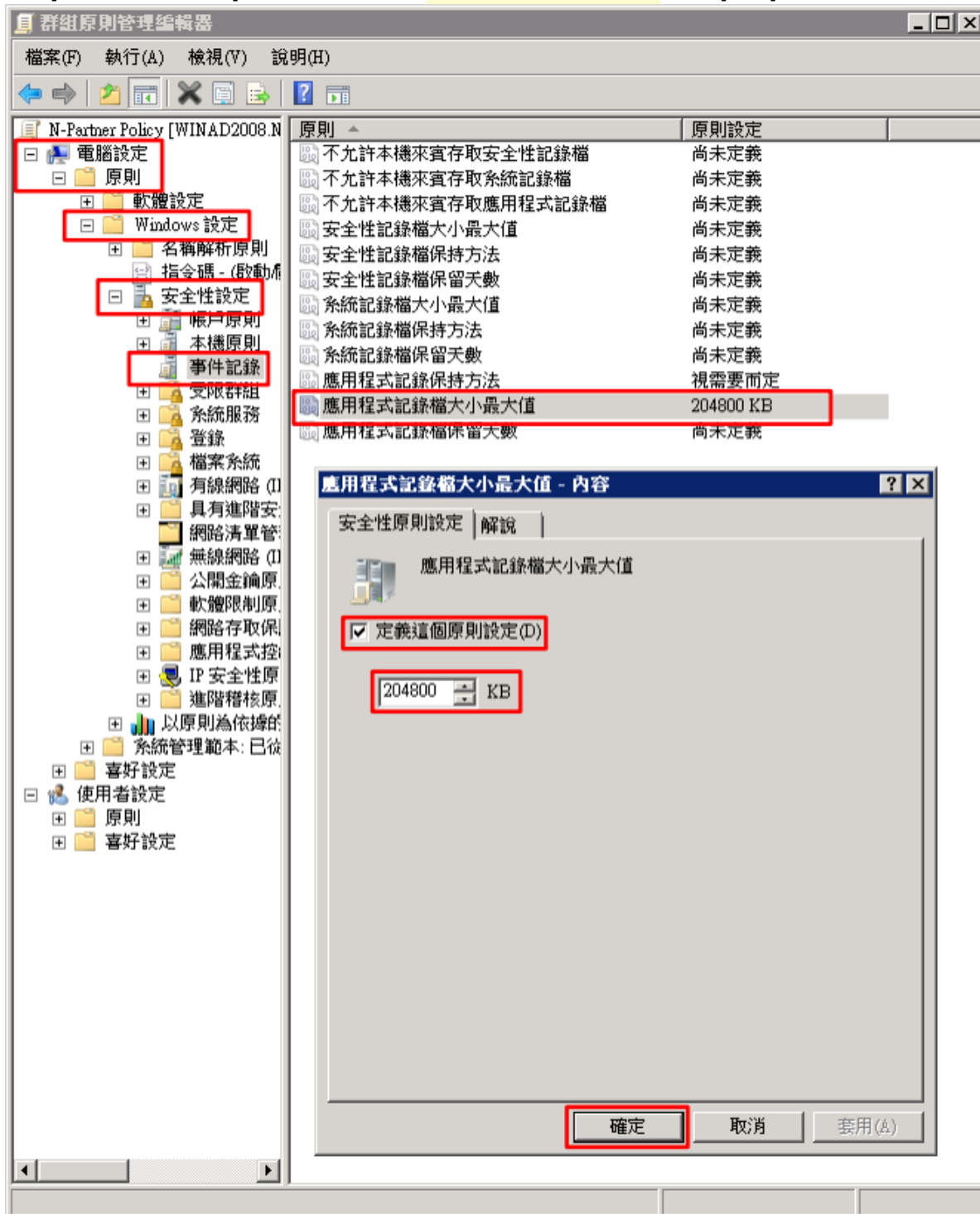
## (6) 事件記錄：應用程式記錄保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄保持方法] 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：應用程式記錄檔大小最大值

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

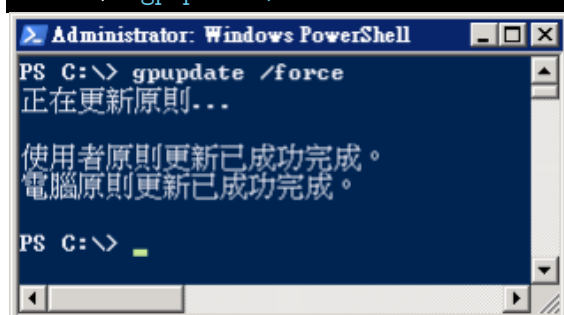


(8) 在 MS SQL Server 伺服器 -> 開啟 [Windows PowerShell]



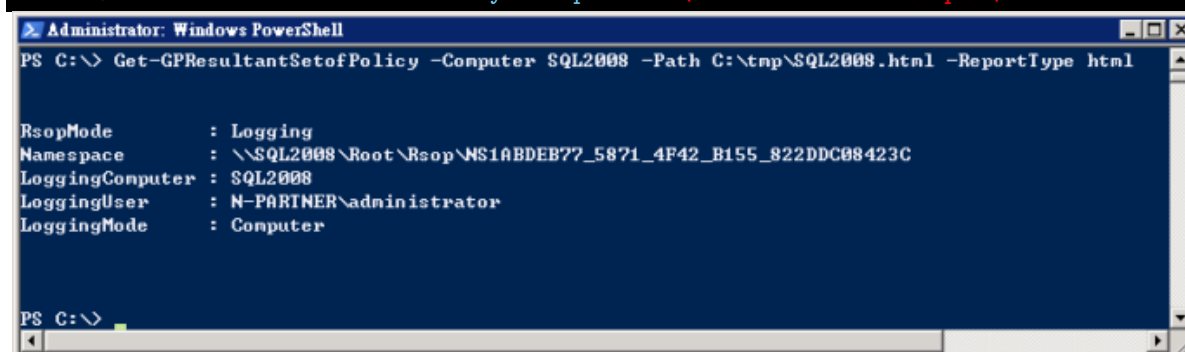
(9) 更新群組原則

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



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

```
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2008 -Path C:\tmp\SQL2008.html -ReportType.html
```



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

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

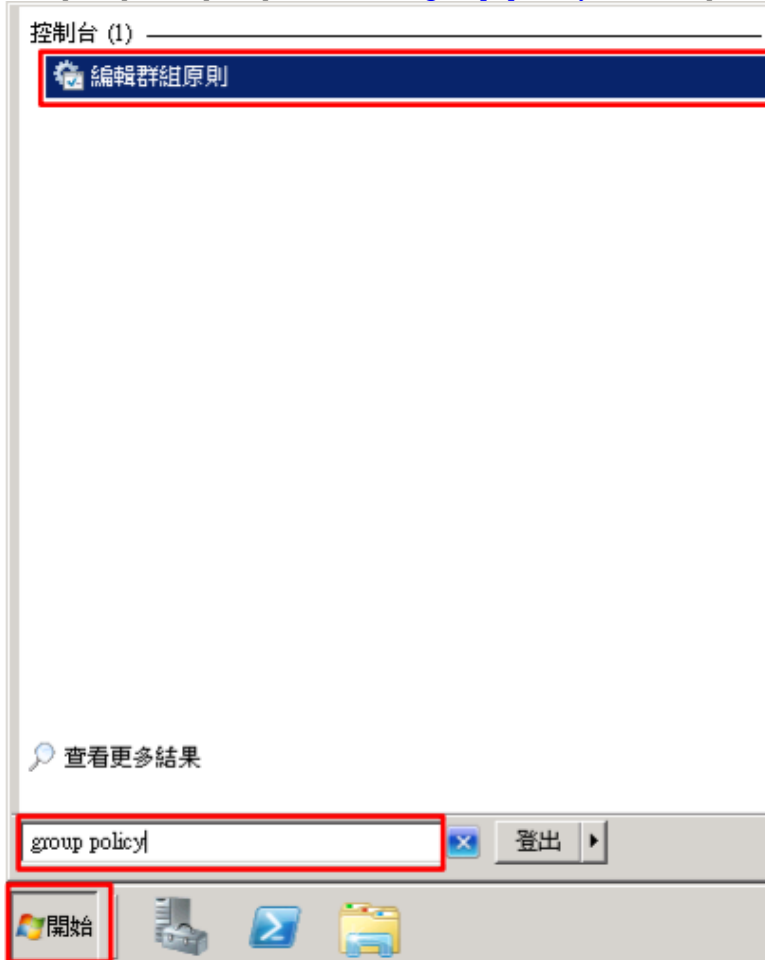
| 群組原則結果                       |           |                  |
|------------------------------|-----------|------------------|
| N-PARTNER\SQL2008            |           |                  |
| 資料收集: 2021/10/21 下午 03:18:02 |           | 顯示全部             |
| 摘要                           |           | 顯示               |
| 電腦設定                         |           | 隱藏               |
| 原則                           |           | 隱藏               |
| Windows 設定                   |           | 隱藏               |
| 安全性設定                        |           | 隱藏               |
| 帳戶原則/密碼規則                    |           | 顯示               |
| 帳戶原則/帳戶鎖定原則                  |           | 顯示               |
| 本機原則/稽核原則                    |           | 隱藏               |
| 原則                           | 設定        | 優勢 GPO           |
| 稽核帳戶登入事件                     | 成功, 失敗    | N-Partner Policy |
| 稽核帳戶管理                       | 成功, 失敗    | N-Partner Policy |
| 稽核登入事件                       | 成功, 失敗    | N-Partner Policy |
| 本機原則/安全性選項                   |           | 顯示               |
| 事件記錄檔                        |           | 隱藏               |
| 原則                           | 設定        | 優勢 GPO           |
| 應用程式記錄保持方法                   | 視需要而定     | N-Partner Policy |
| 應用程式記錄檔容量最大值                 | 204800 KB | N-Partner Policy |
| 公開金鑰原則/憑證服務用戶端 - 自動註冊設定      |           | 顯示               |
| 公開金鑰原則/加密檔案系統                |           | 顯示               |
| 公開金鑰原則/被信任的根憑證授權單位           |           | 顯示               |
| 使用者設定                        |           | 顯示               |

## 2.3.2 工作群組

### 2.3.2.1 稽核原則設定

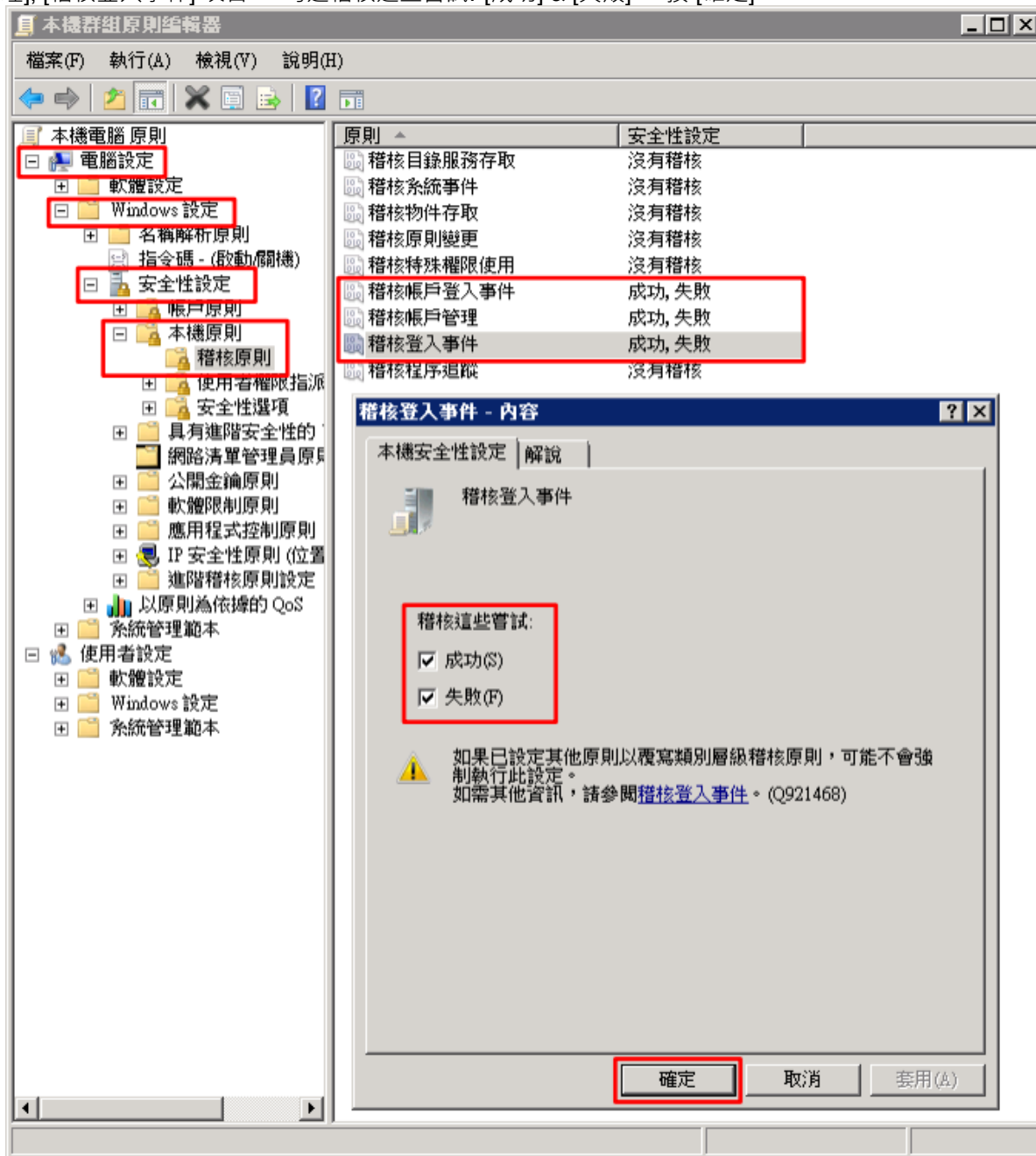
#### (1) 開啟 [本機群組原則編輯器]

點選 [開始] -> 在 [搜尋] 欄位，輸入 `group policy` -> 點選 [編輯群組原則]



## (2) 本機原則：稽核原則

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



(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

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



(5) 查看群組原則套用情形

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

```

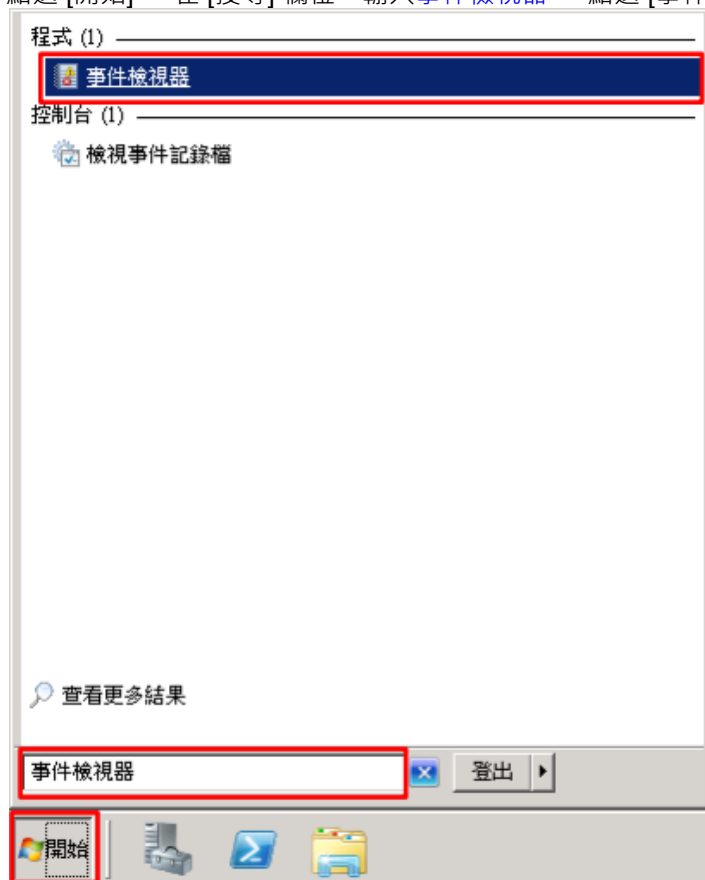
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
系統稽核原則
類別/子類別
系統
系統
設定
安全性系統延伸
沒有稽核
系統完整性
成功及失敗
IPSEC driver
沒有稽核
其他系統事件
成功及失敗
安全性狀態變更
成功
登入/登出
成功及失敗
登入
成功及失敗
登出
成功及失敗
帳戶鎖定
成功及失敗
IPsec 主要模式
成功及失敗
IPsec 快速模式
成功及失敗
IPsec 延伸模式
成功及失敗
特殊登入
成功及失敗
其他登入/登出事件
成功及失敗
網路原則伺服器
成功及失敗
物件存取
沒有稽核
檔案系統
沒有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

```

### 2.3.2.2 事件檔案設定

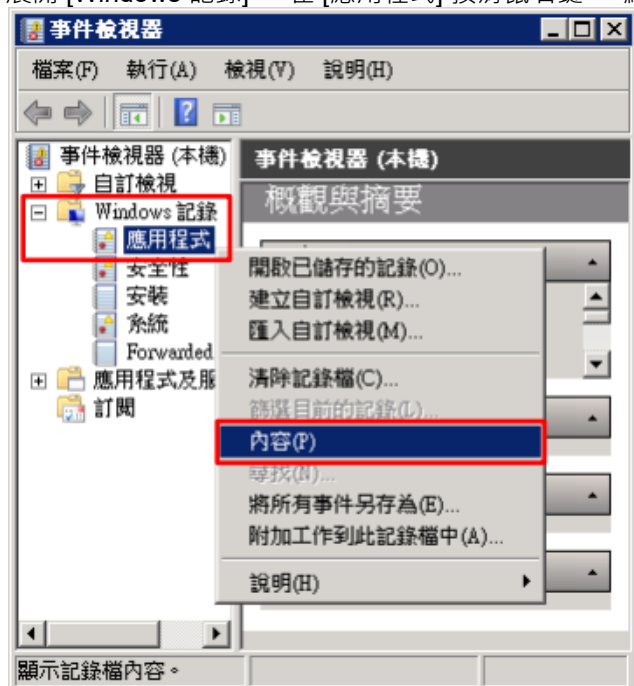
#### (1) 開啟 [事件檢視器]

點選 [開始] -> 在 [搜尋] 欄位，輸入 [事件檢視器](#) -> 點選 [事件檢視器]



#### (2) 編輯應用程式記錄

展開 [Windows 記錄] -> 在 [應用程式] 按滑鼠右鍵 -> 點選 [內容]



### (3) 設定應用程式記錄檔

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

記錄內容 - 應用程式 (類型: 系統管理)

一般 | 訂閱

全名(F): Application

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

記錄檔大小: 1.07 MB(1,118,208 位元組)

建立日期: 2021年6月21日 下午 09:05:32

修改日期: 2021年7月5日 下午 02:26:50

存取日期: 2021年6月21日 下午 09:05:32

☒ 啟用記錄(E)

最大記錄檔大小 (KB)(Q): 204800

當事件記錄檔的大小到達上限時:

☒ 視需要覆寫事件 (先覆寫最舊的事件)(W)

☐ 當記錄檔已滿時進行封存，不要覆寫事件(A)

☐ 不要覆寫事件 (手動清除記錄檔)(N)

清除記錄檔(R)

確定 取消 套用(P)

## 3 SQL2012

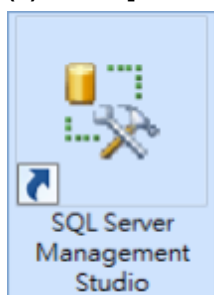
### 3.1 稽核登入

啟用登入稽核，以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。

以下分別為圖形介面和指令介面設定方式。

#### 3.1.1 使用圖形介面方式設定

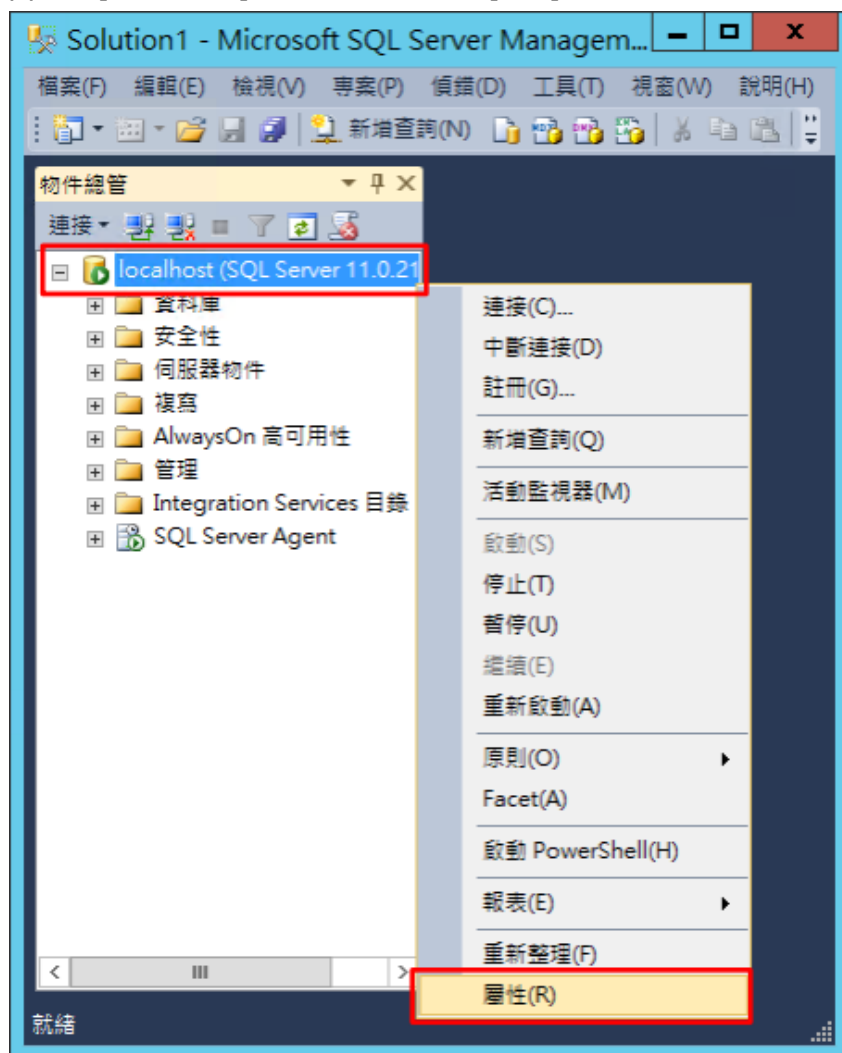
##### (1) 開啟 [SQL Server Management Studio]



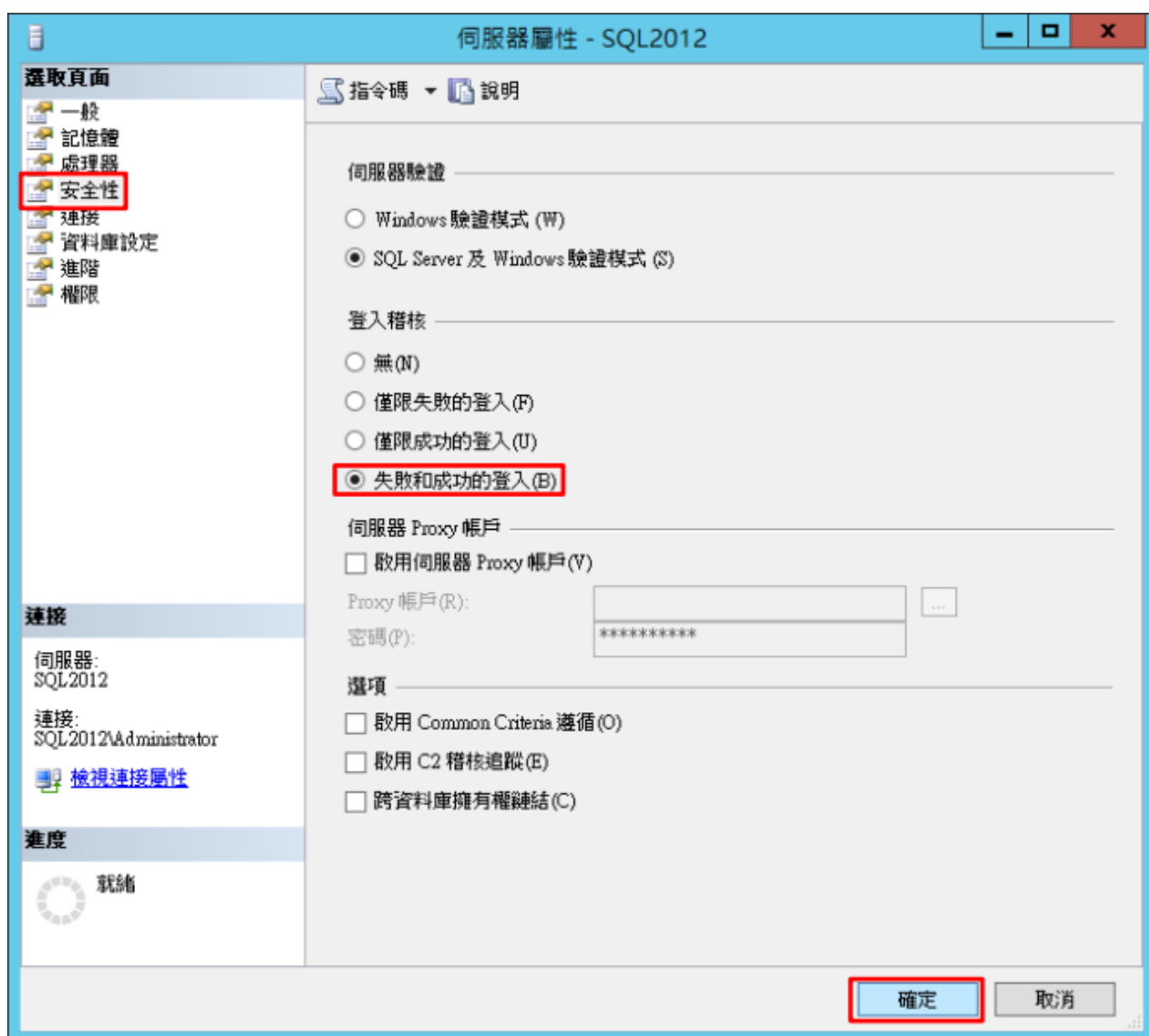
##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

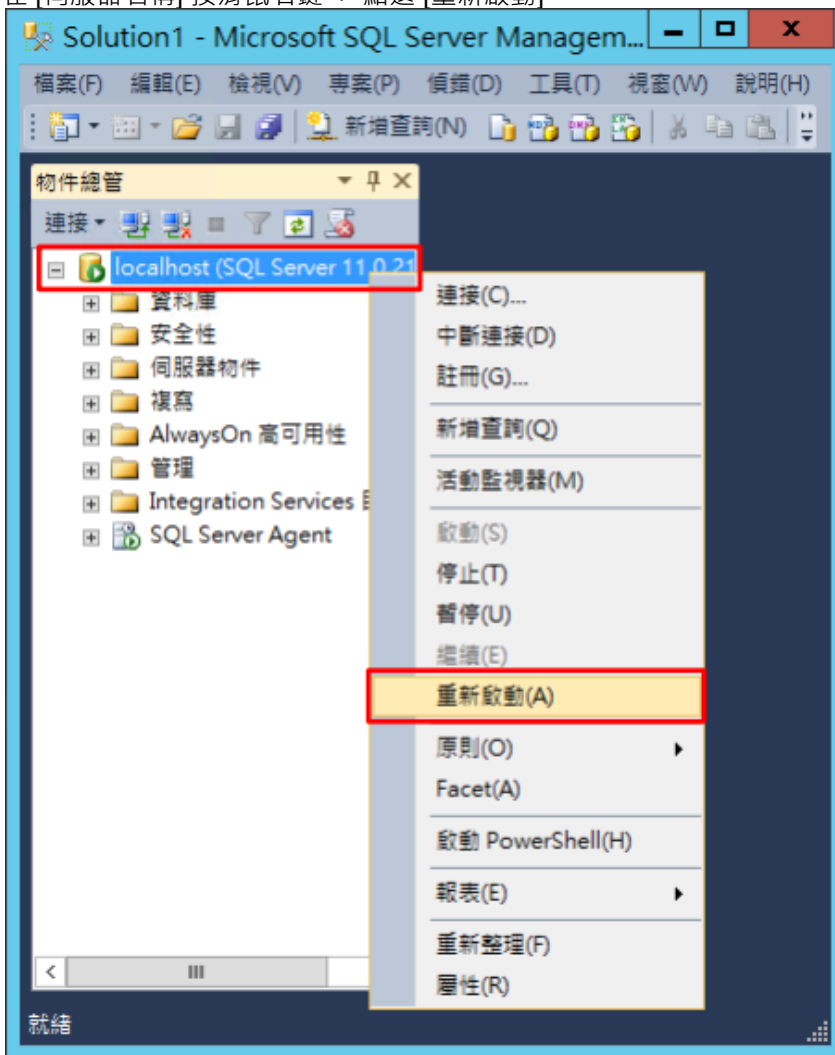


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

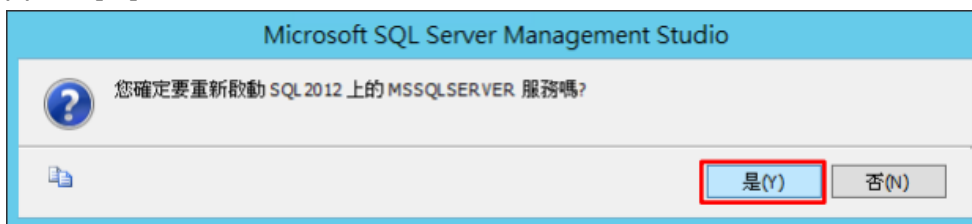


(5) 重新啟動 MS SQL SERVER 服務

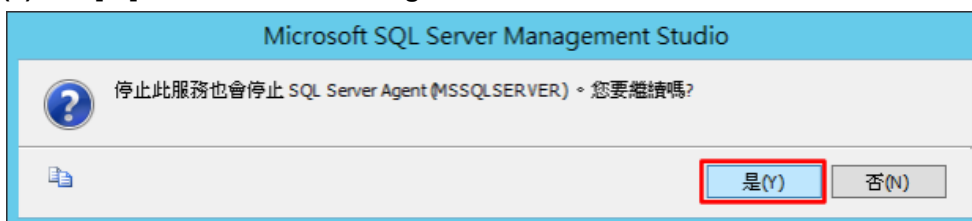
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務



(7) 按 [是] 停止 SQL SERVER Agent 服務



### 3.1.2 使用指令介面方式設定

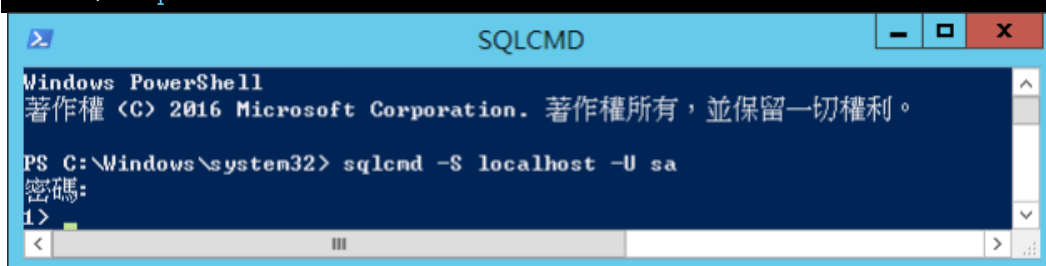
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

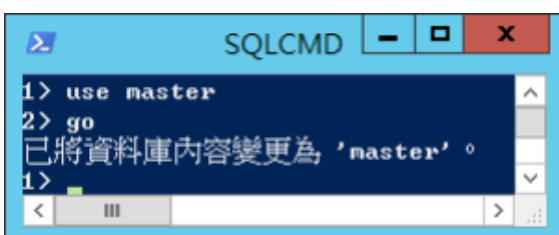
##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



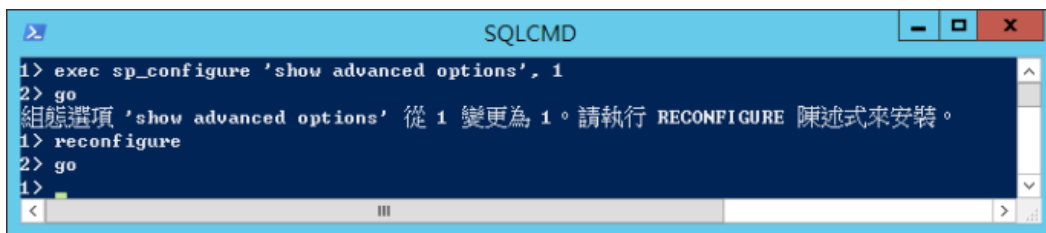
#### (3) 切換資料庫

```
1 > use master
2 > go
```



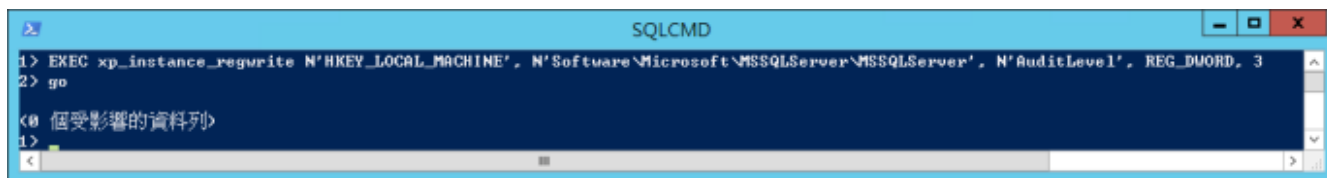
#### (4) 使用 sp\_configure 列出進階選項

```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



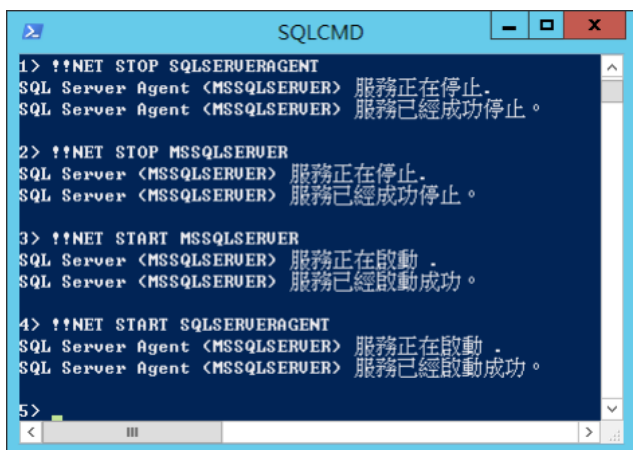
#### (5) 啟用失敗和成功的登入記錄

```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2 > go
```



#### (6) 重新啟動 MS SQL SERVER 服務

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



## 3.2 設定稽核

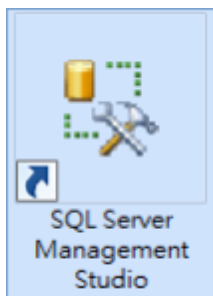
### 3.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

#### 3.2.1.1 使用圖形介面方式設定

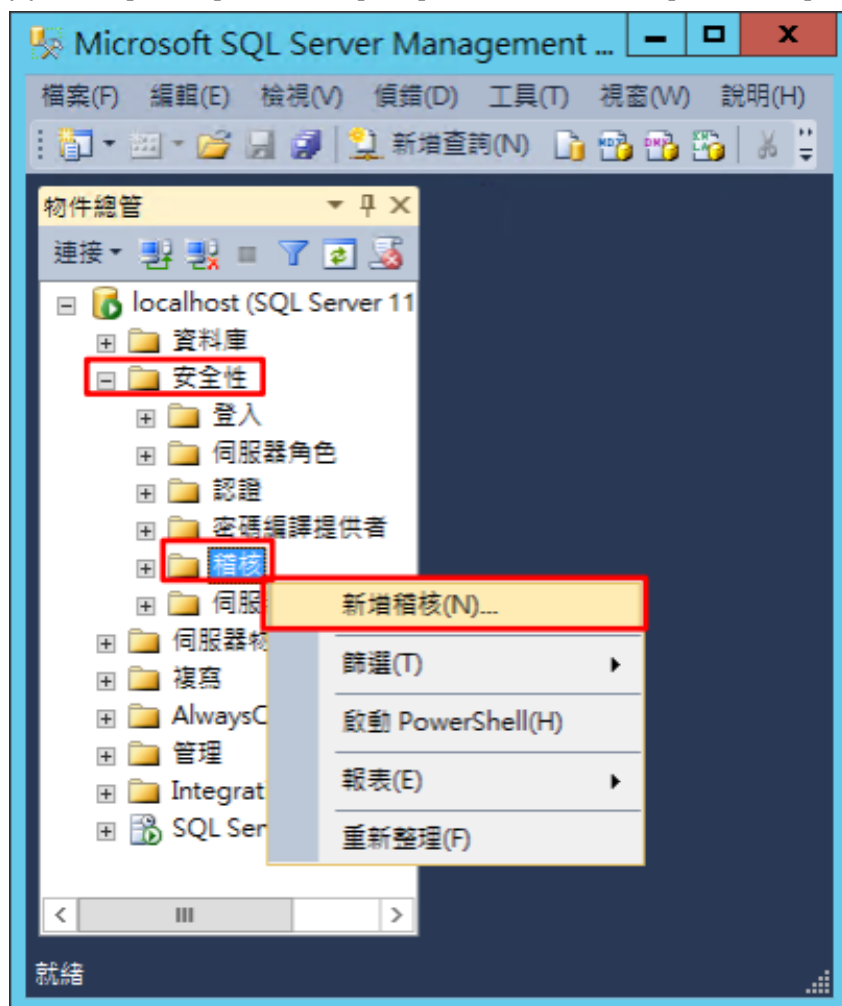
##### (1) 開啟 [SQL Server Management Studio]



##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

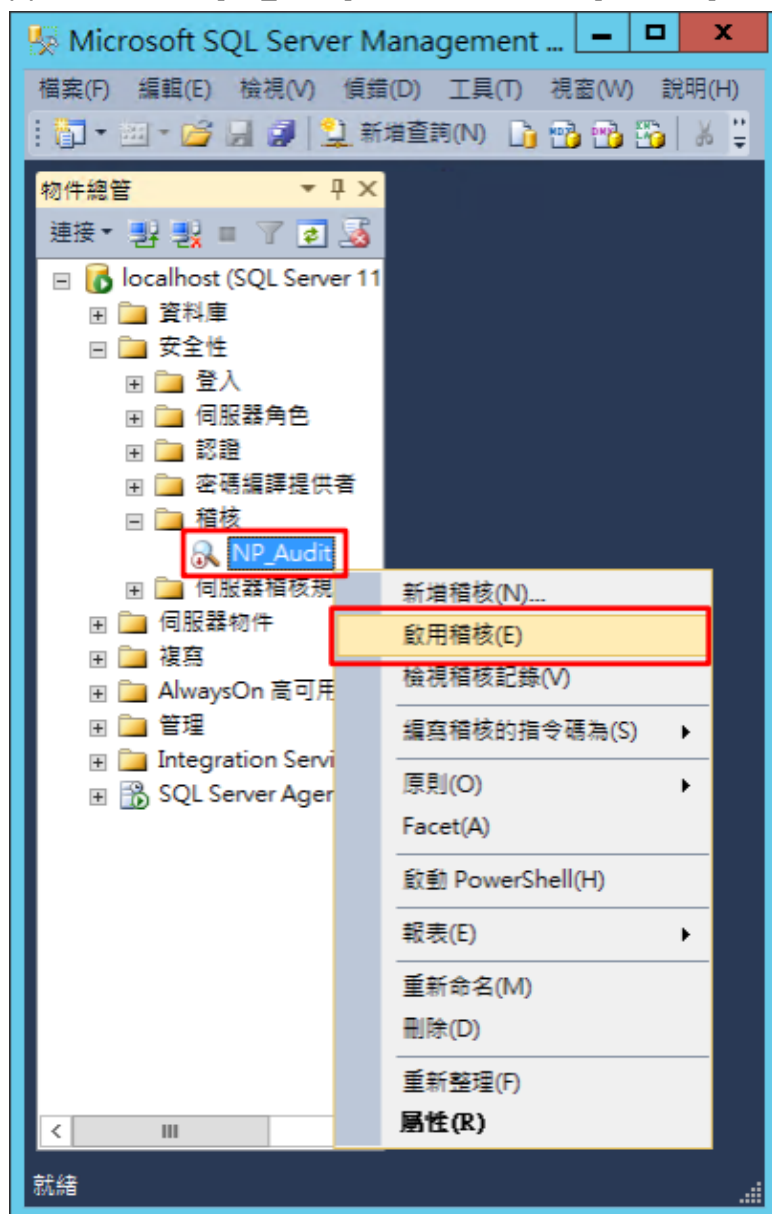


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

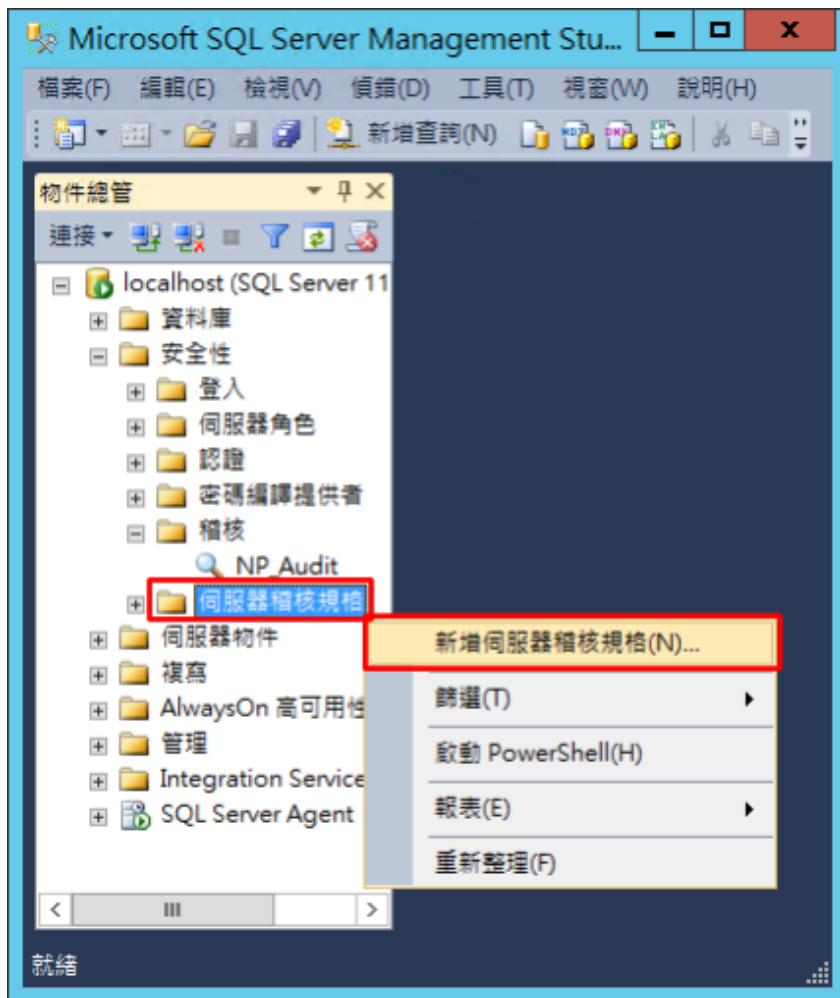
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



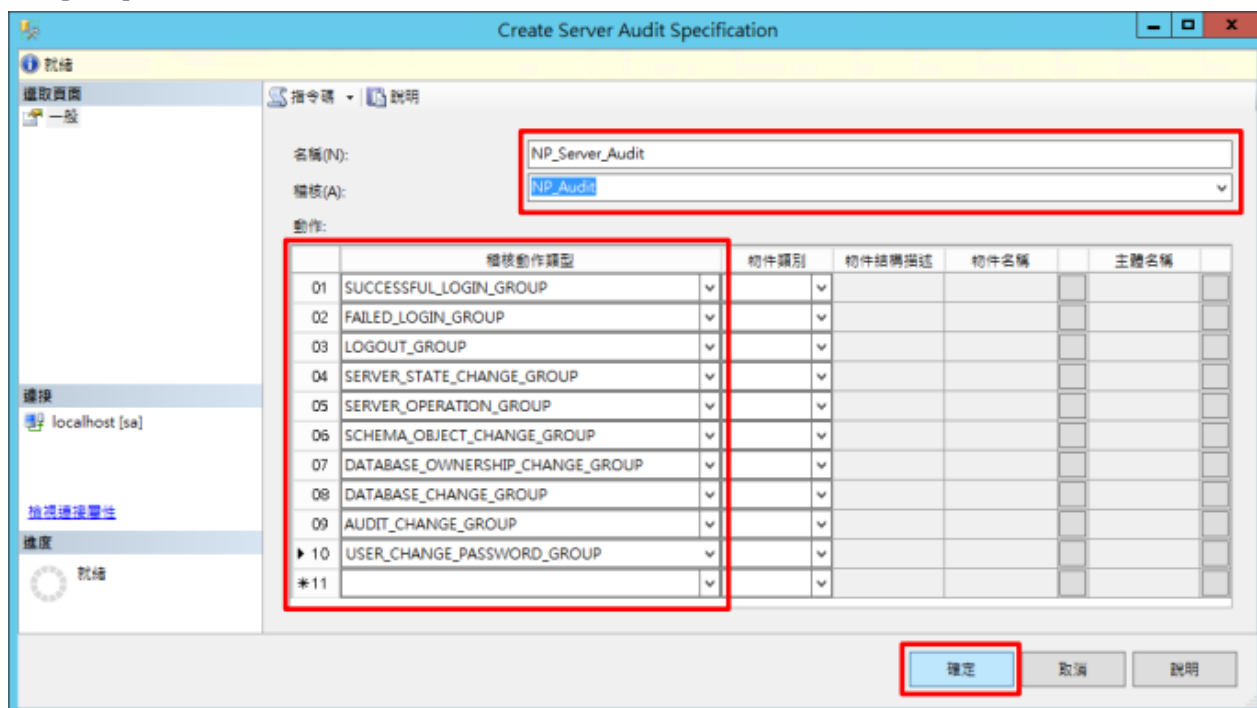
(6) 按 [關閉]



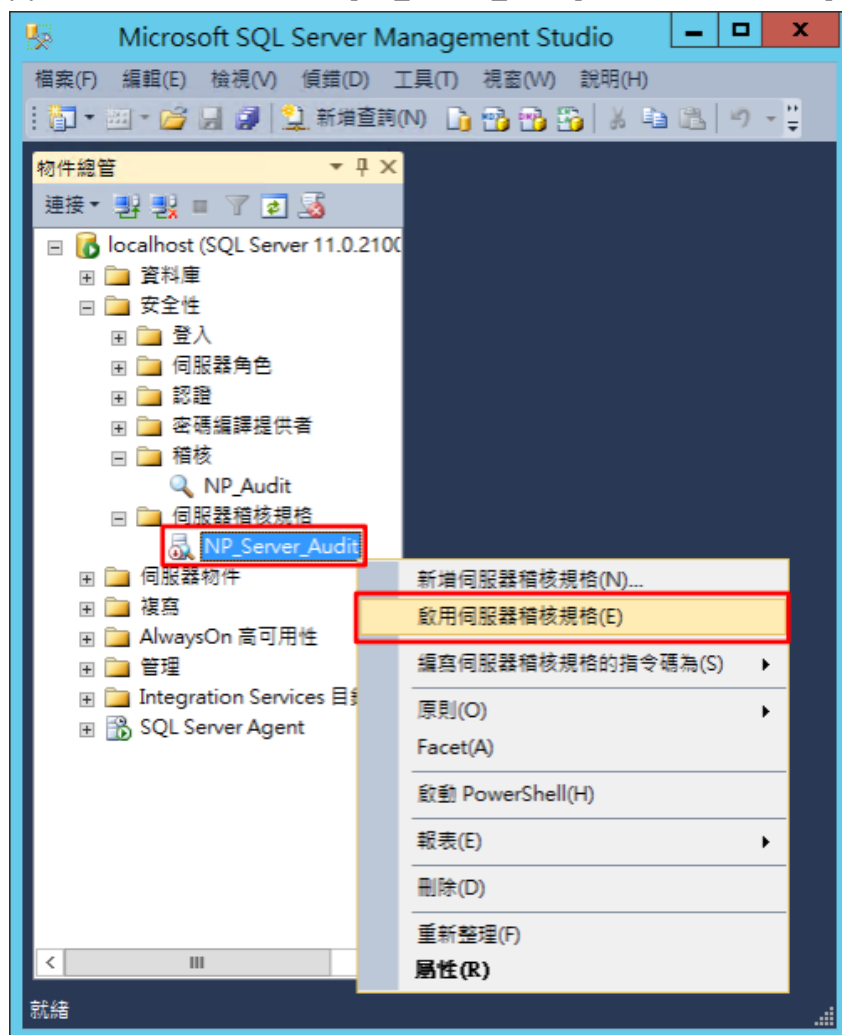
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



(8) 輸入名稱: `NP_Server_Audit` -> 選擇稽核: `[NP_Audit]` 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在伺服器稽核規格名稱: [NP\_Server\_Audit] 按滑鼠右鍵 -> 點選 [啟用伺服器稽核規格]



(10) 按 [關閉]



### 3.2.1.2 使用指令介面方式設定

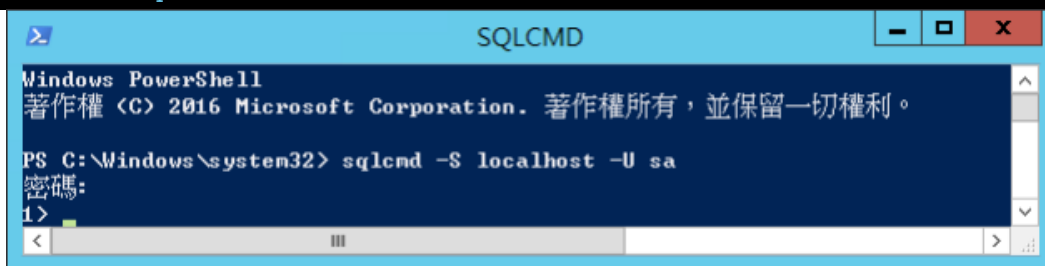
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

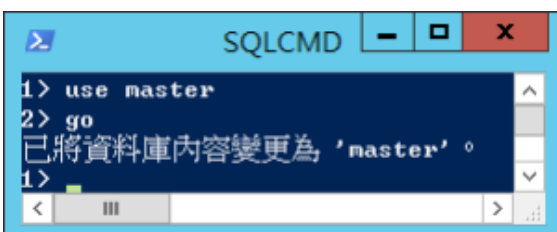
##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



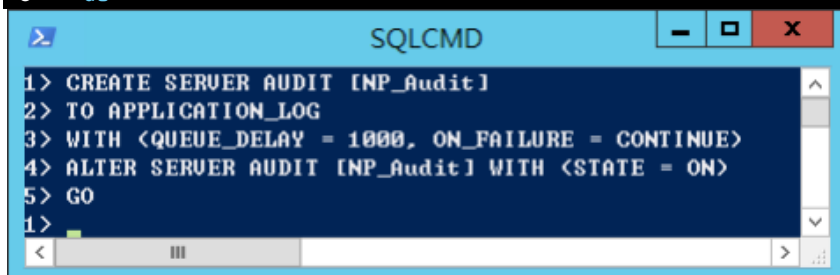
#### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



The screenshot shows a window titled "SQLCMD" with a dark blue background. It contains the same SQL commands as the previous block, with the prompt "1>" at the bottom. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

紅色文字部位請輸入稽核名稱

(5) 設定稽核伺服器・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP)
12 > WITH (STATE = ON)
13 > GO
1 > quit
```



The screenshot shows a window titled "系統管理員: Windows PowerShell" with a dark blue background. It contains the same SQL commands as the previous block, with the prompt "1>" at the bottom. The window has standard Windows window controls in the top right corner. At the bottom, the prompt "PS C:\Windows\system32>" is visible.

紅色文字部位請輸入伺服器稽核規格名稱

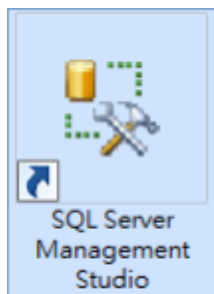
### 3.2.2 稽核資料庫層級

啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

以下分別為圖形介面和指令介面設定方式。

#### 3.2.2.1 使用圖形介面方式設定

##### (1) 開啟 [SQL Server Management Studio]



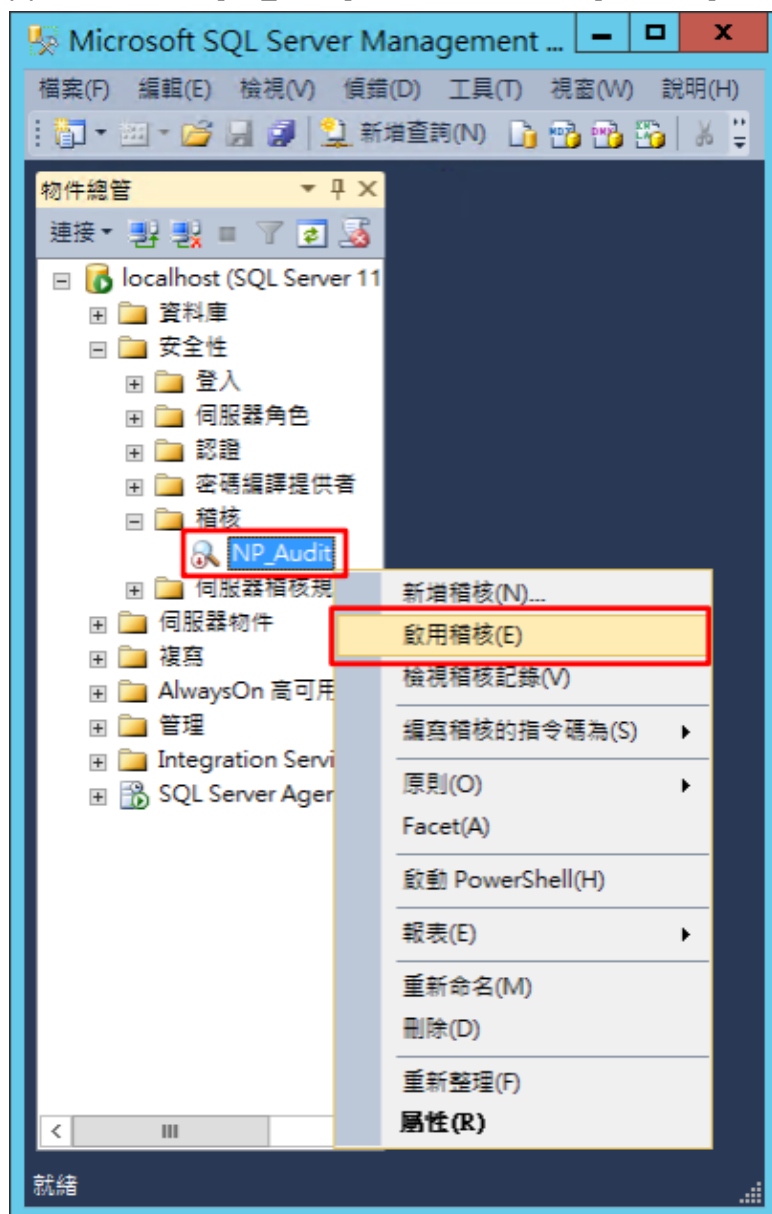
##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



The screenshot shows the Microsoft SQL Server Enterprise Manager interface. The '物件總管' (Object Explorer) pane on the left displays the server hierarchy for 'localhost (SQL Server 11)'. The '安全性' (Security) folder is expanded and highlighted with a red box. A right-click context menu is open over the '安全性' folder, with the '新增稽核(N)...' (New Audit...) option highlighted by a red box. The menu also includes options like '篩選(T)' (Filter), '啟動 PowerShell(H)' (Start PowerShell), '報表(E)' (Reports), and '重新整理(F)' (Refresh).

- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

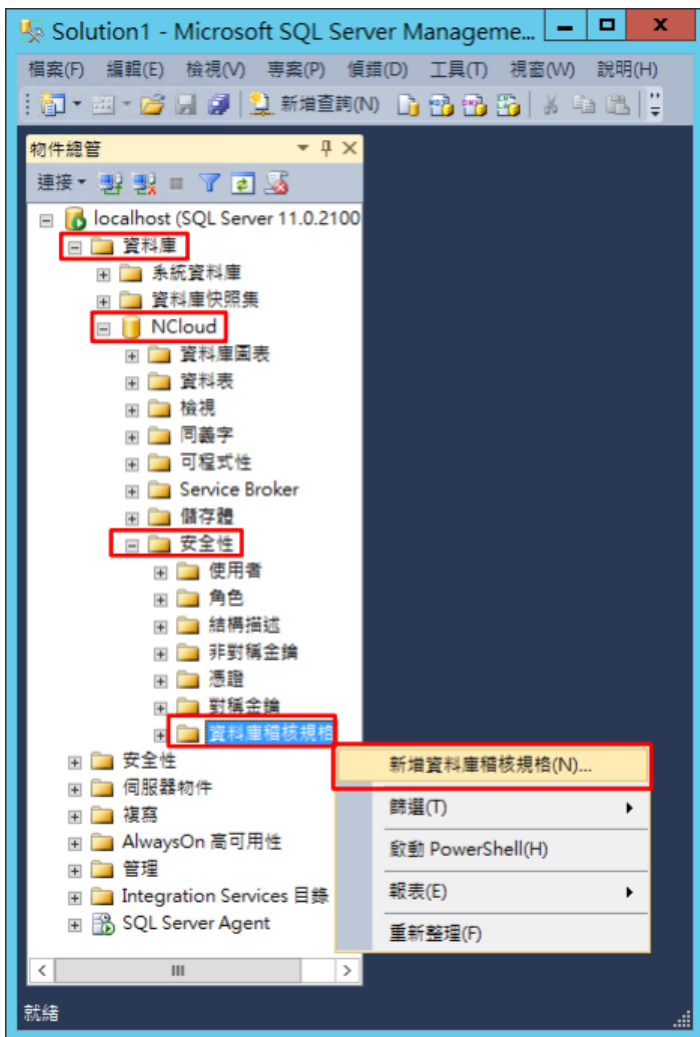
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



(6) 按 [關閉]



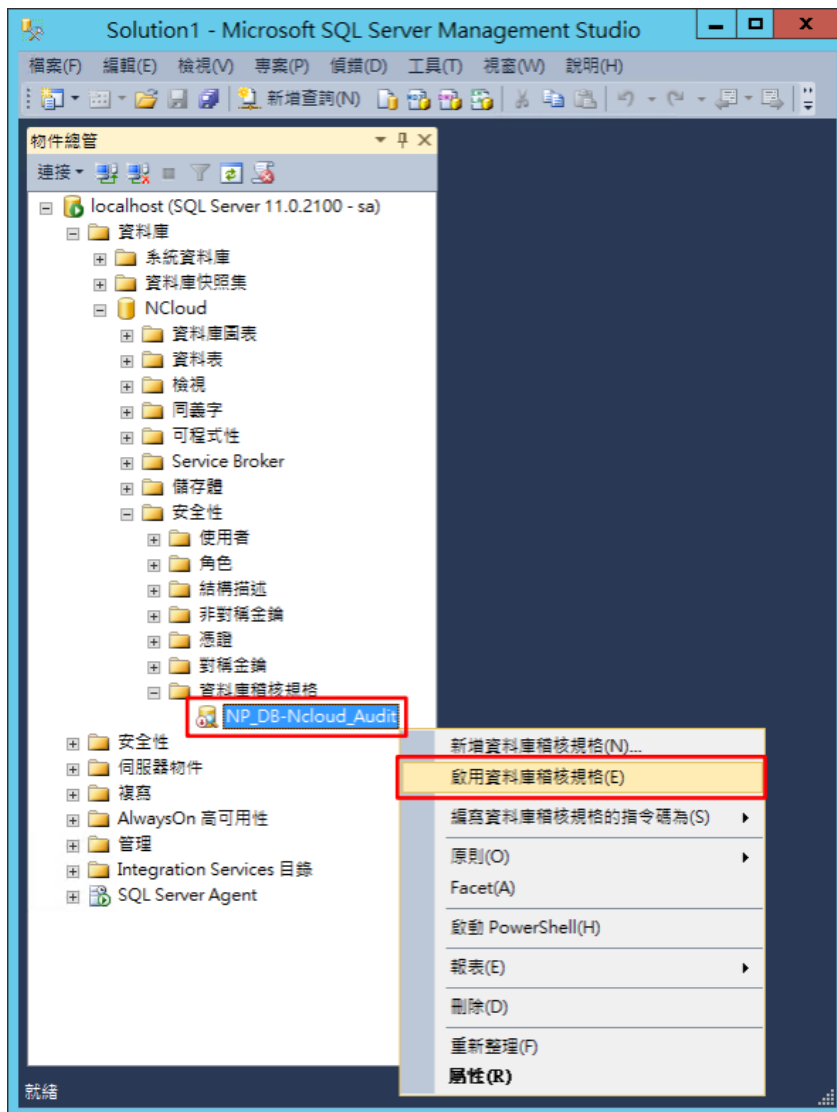
- (7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



- (8) 輸入稽核名稱: `NP_DB-Ncloud_Audit` -> 選擇稽核: [NP\_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在資料庫稽核規格名稱: [NP\_DB-Ncloud\_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10) 按 [關閉]



### 3.2.2.2 使用指令介面方式設定

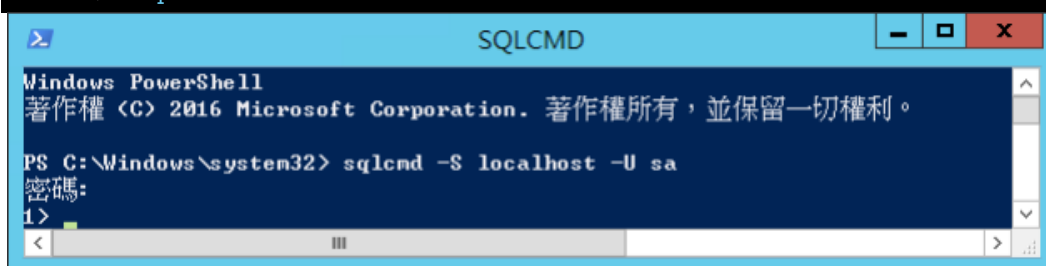
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

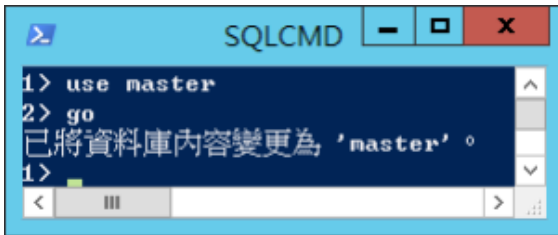
##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



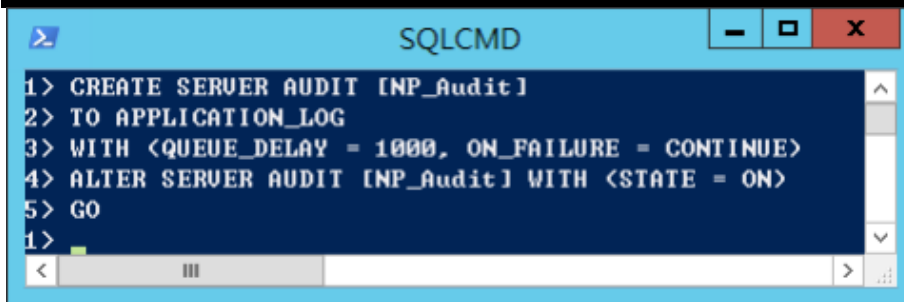
### (3) 切換資料庫

```
1 > use master
2 > go
```



### (4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

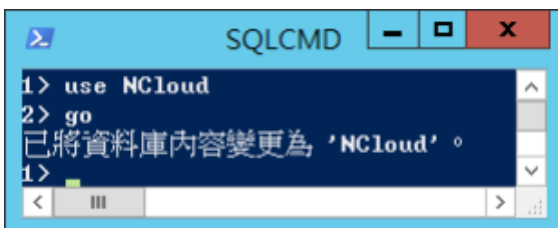
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



紅色文字部位請輸入稽核名稱

### (5) 切換到稽核資料庫，範例：NCloud

```
1 > use NCloud
2 > go
```



紅色文字部位請輸入稽核資料庫名稱

(6) 設定稽核 NCloud(範例) 資料庫・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8 > ADD (DATABASE_CHANGE_GROUP),
9 > ADD (AUDIT_CHANGE_GROUP)
10 > WITH (STATE = ON)
11 > GO
1 > quit
```



紅色文字部位請輸入資料庫稽核規格名稱

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

紅色文字部位請輸入稽核資料庫名稱

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

## 3.3 事件記錄檔設定

此為選項設定。

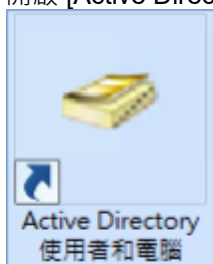
以下分別為網域和工作群組設定方式。

### 3.3.1 網域

#### 3.3.1.1 組織單位設定

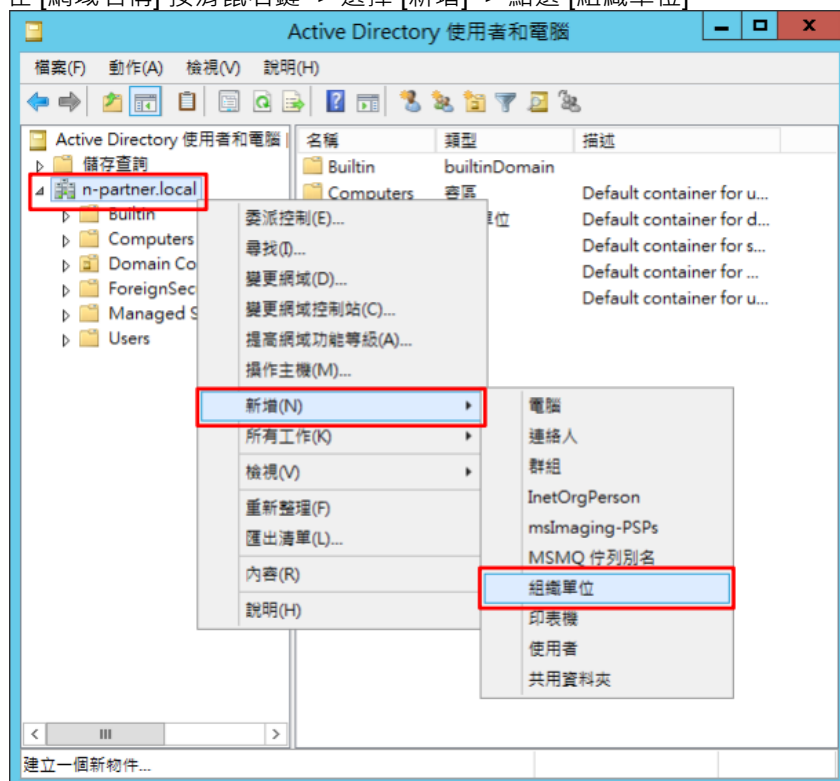
##### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



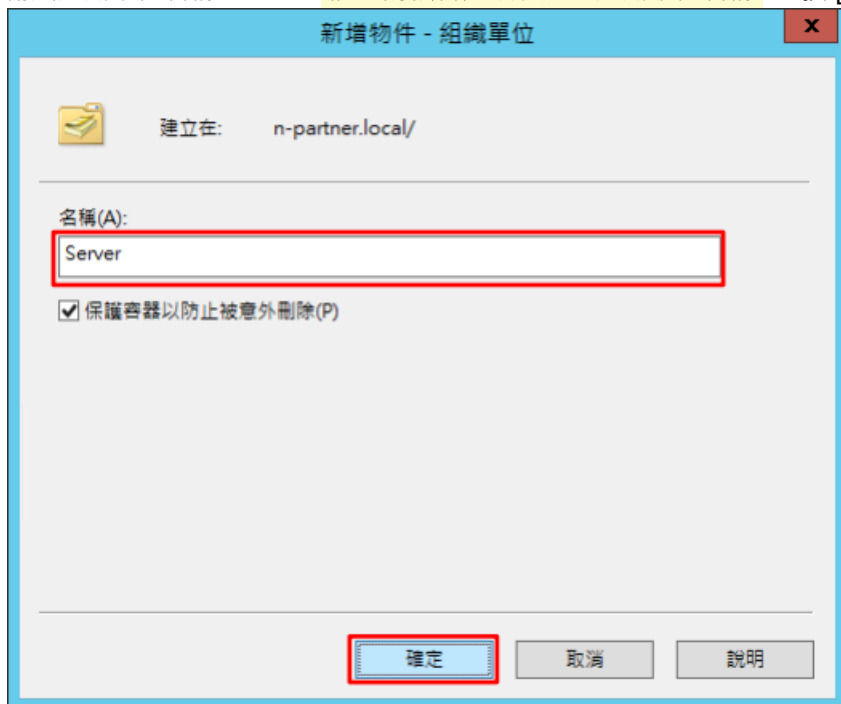
##### (2) 新增組織單位

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



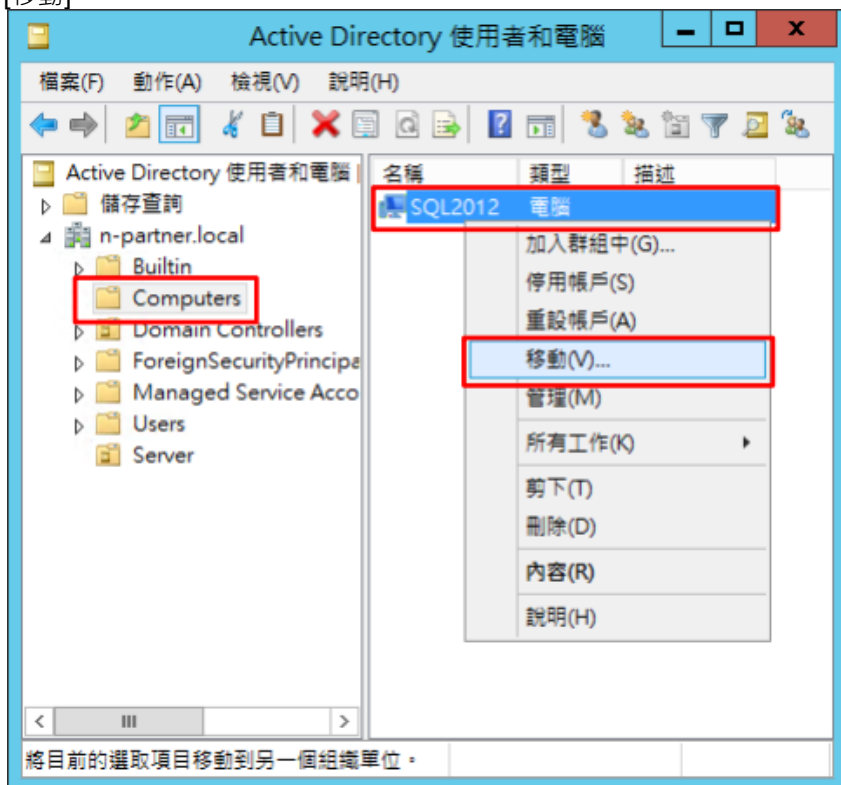
### (3) 輸入組織單位名稱

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



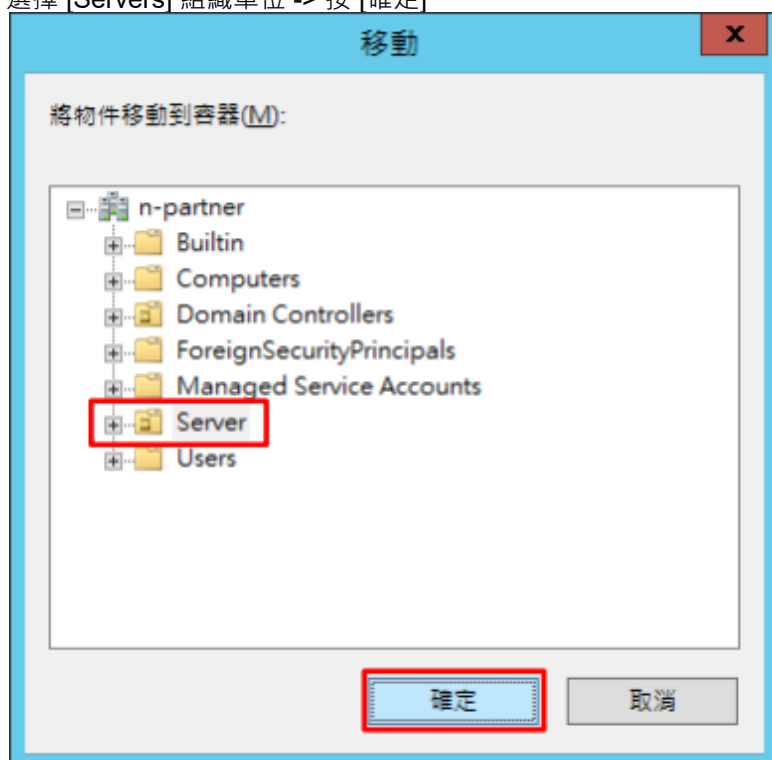
### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL 2012] 伺服器, 按滑鼠右鍵, 註：請依客戶環境選擇 MS SQL Server 主機 -> 點選 [移動]



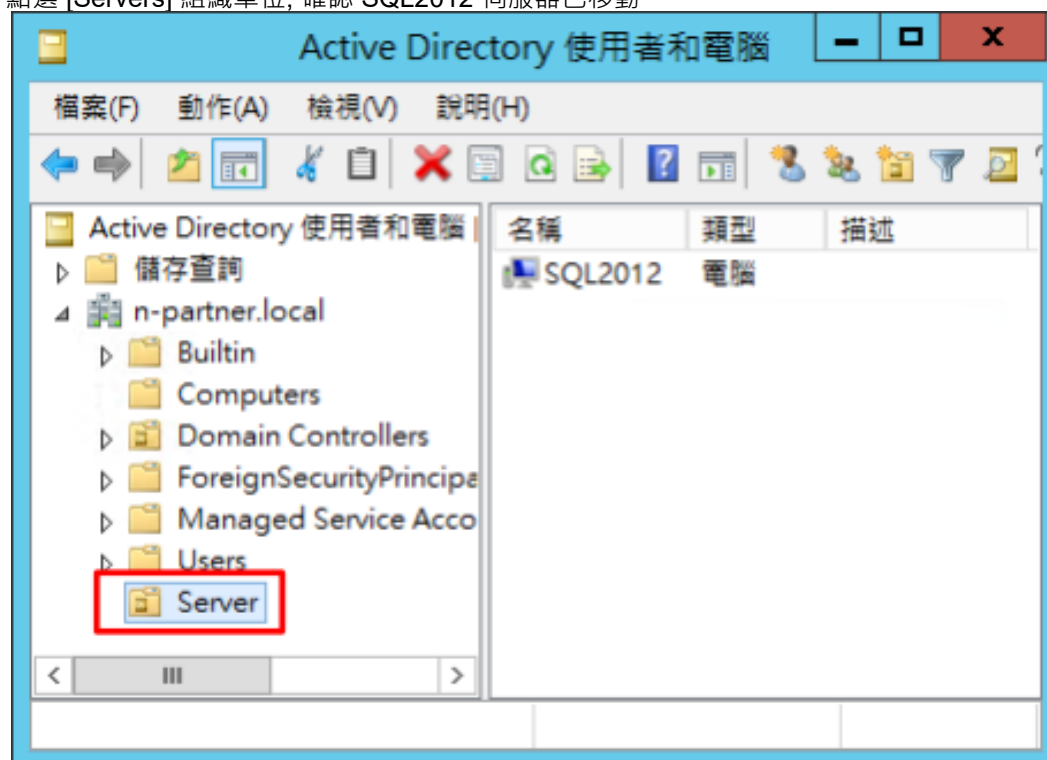
### (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



### (6) 確認伺服器已移動至新的組織單位

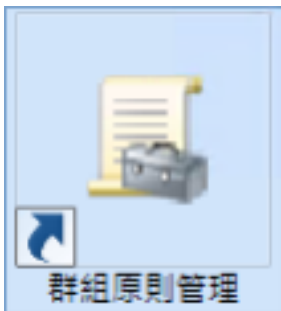
點選 [Servers] 組織單位, 確認 SQL2012 伺服器已移動。



### 3.3.1.2 群組原則設定

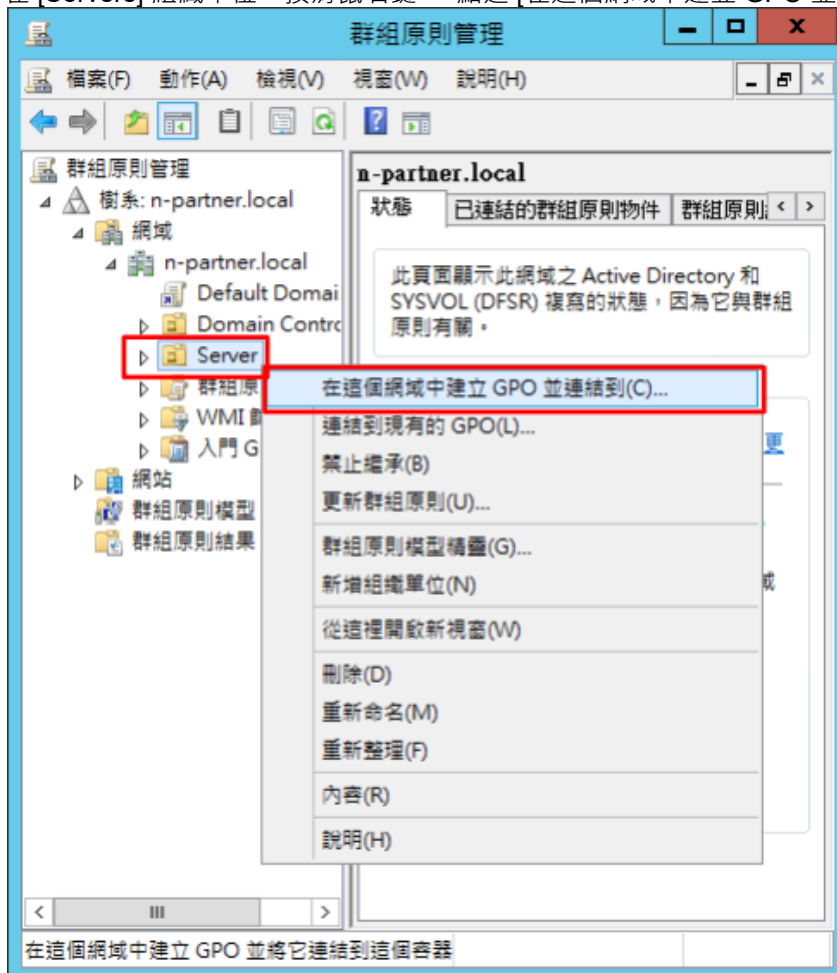
#### (1) 開啟群組原則管理

開啟 [群組原則管理]



#### (2) 在 Servers 組織單位，新增群組原則物件

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



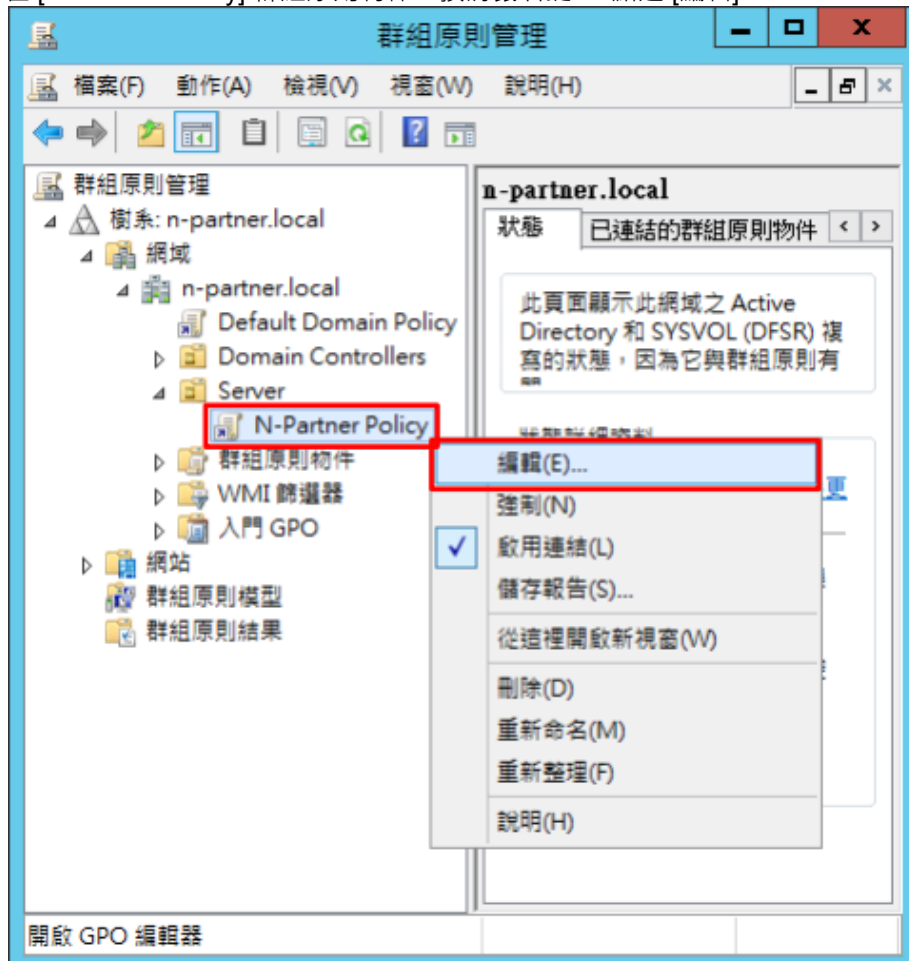
### (3) 輸入群組原則物件名稱

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



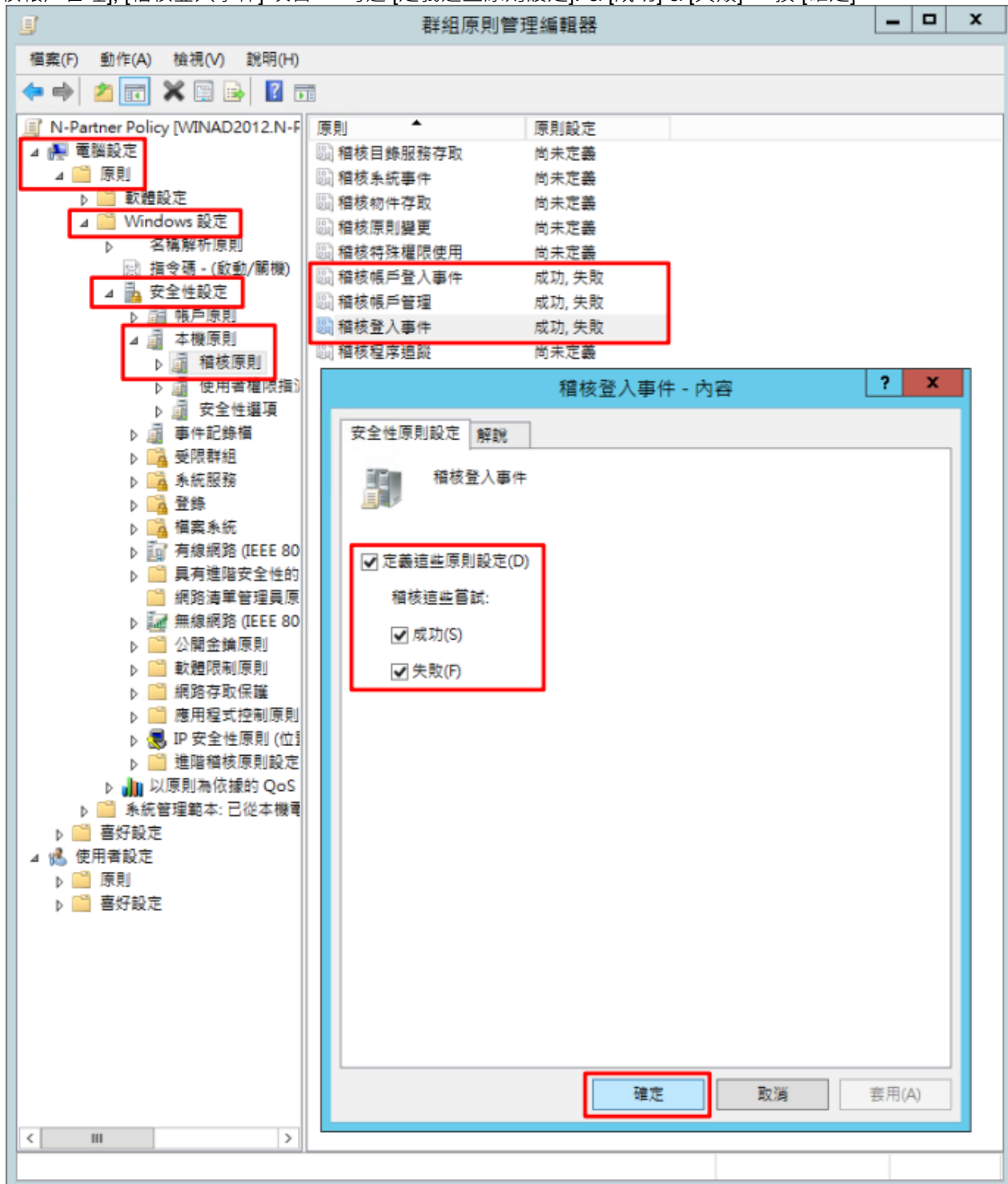
### (4) 編輯群組原則物件

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



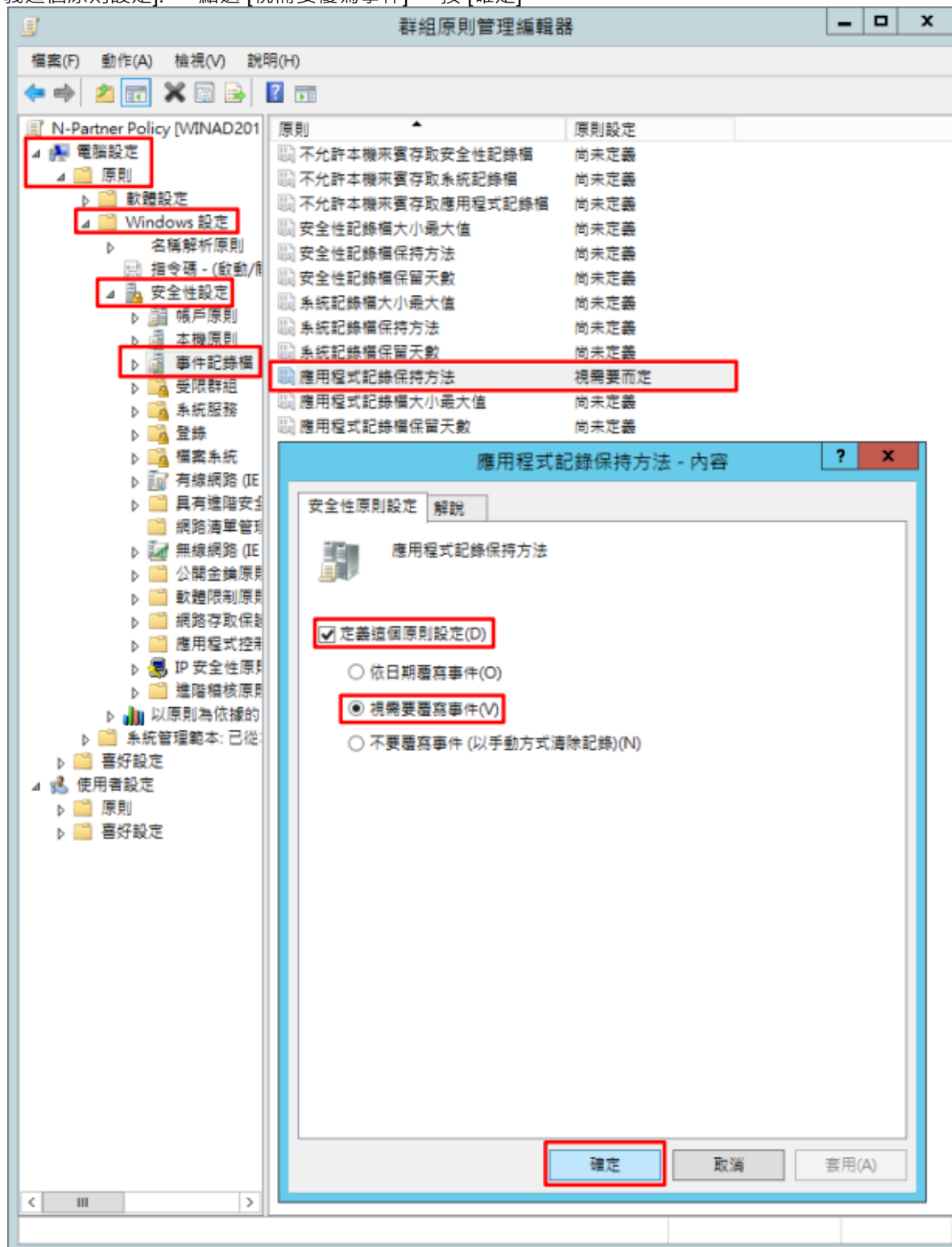
##### (5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



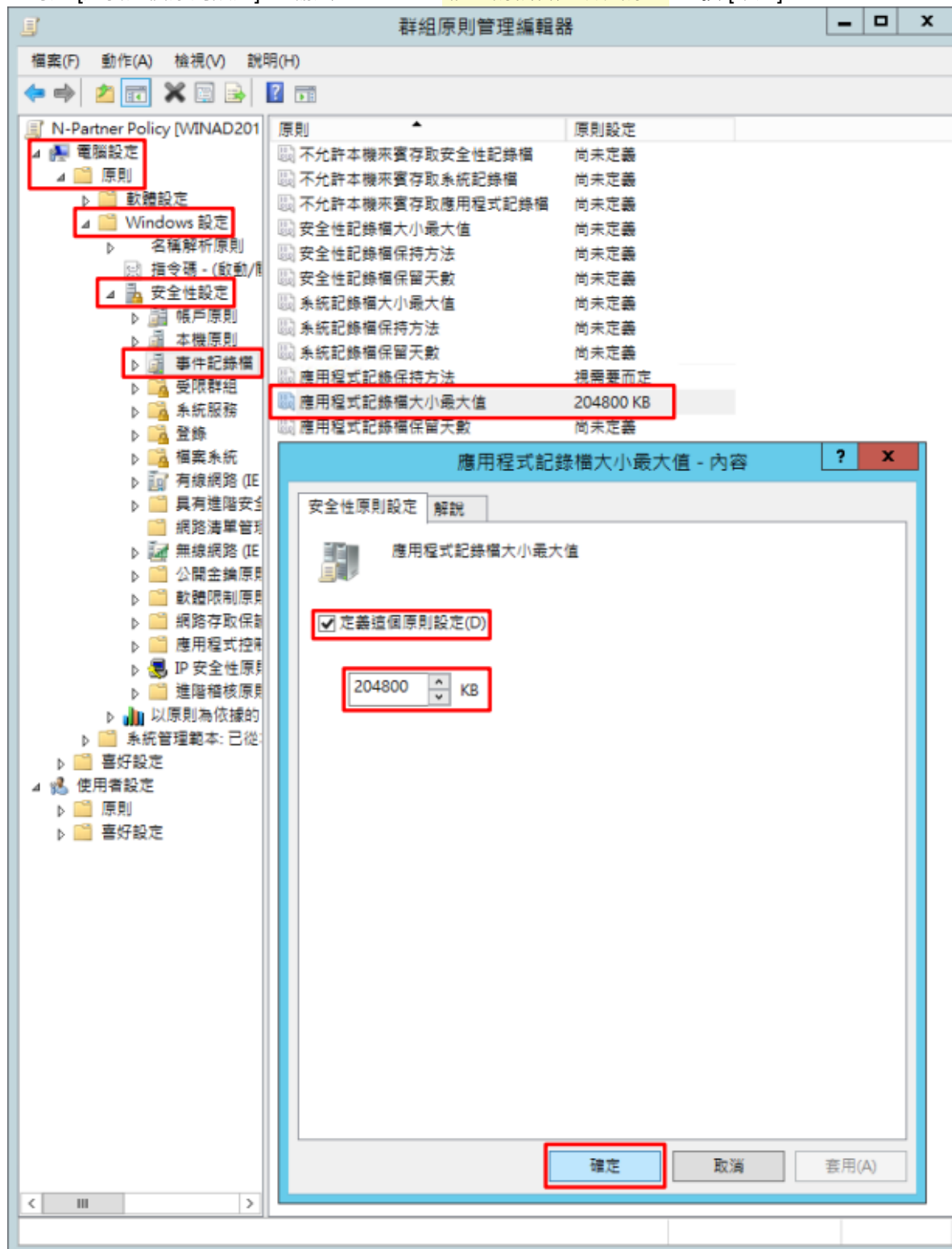
## (6) 事件記錄：應用程式記錄保持方法

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



### (7) 事件記錄：應用程式記錄檔大小最大值

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

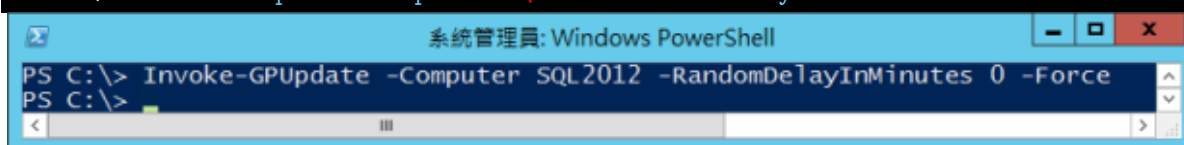


(8) 在 MS SQL Server 伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

```
PS C:\> Invoke-GPUdate -Computer SQL2012 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2012 -Path C:\tmp\SQL2012.html -ReportType.html
```



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

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

← →

C:\tmp\SQL2012.html

N-PARTNER\SQL2012

群組原則結果

N-PARTNER\SQL2012

資料收集: 22/10/2021 10:13:34

顯示全部

摘要

顯示

電腦詳細資料

隱藏

一般

顯示

元件狀態

顯示

設定

隱藏

原則

隱藏

Windows 設定

隱藏

安全性設定

隱藏

帳戶原則/密碼規則

顯示

帳戶原則/帳戶鎖定原則

顯示

本機原則/稽核原則

隱藏

| 原則       | 設定     | 優勢 GPO           |
|----------|--------|------------------|
| 稽核帳戶登入事件 | 成功, 失敗 | N-Partner Policy |
| 稽核帳戶管理   | 成功, 失敗 | N-Partner Policy |
| 稽核登入事件   | 成功, 失敗 | N-Partner Policy |

本機原則/安全性選項

顯示

事件記錄檔

隱藏

| 原則           | 設定        | 優勢 GPO           |
|--------------|-----------|------------------|
| 應用程式記錄保持方法   | 視需要而定     | N-Partner Policy |
| 應用程式記錄檔容量最大值 | 204800 KB | N-Partner Policy |

公開金鑰原則/憑證服務用戶端 - 自動註冊設定

顯示

公開金鑰原則/加密檔案系統

顯示

群組原則物件

顯示

WMI 篩選器

顯示

使用者詳細資料

顯示

### 3.3.2 工作群組

#### 3.3.2.1 稽核原則設定

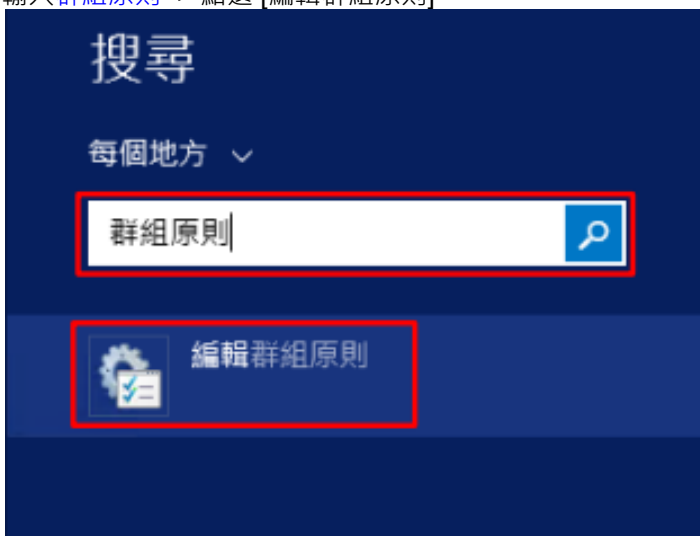
##### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



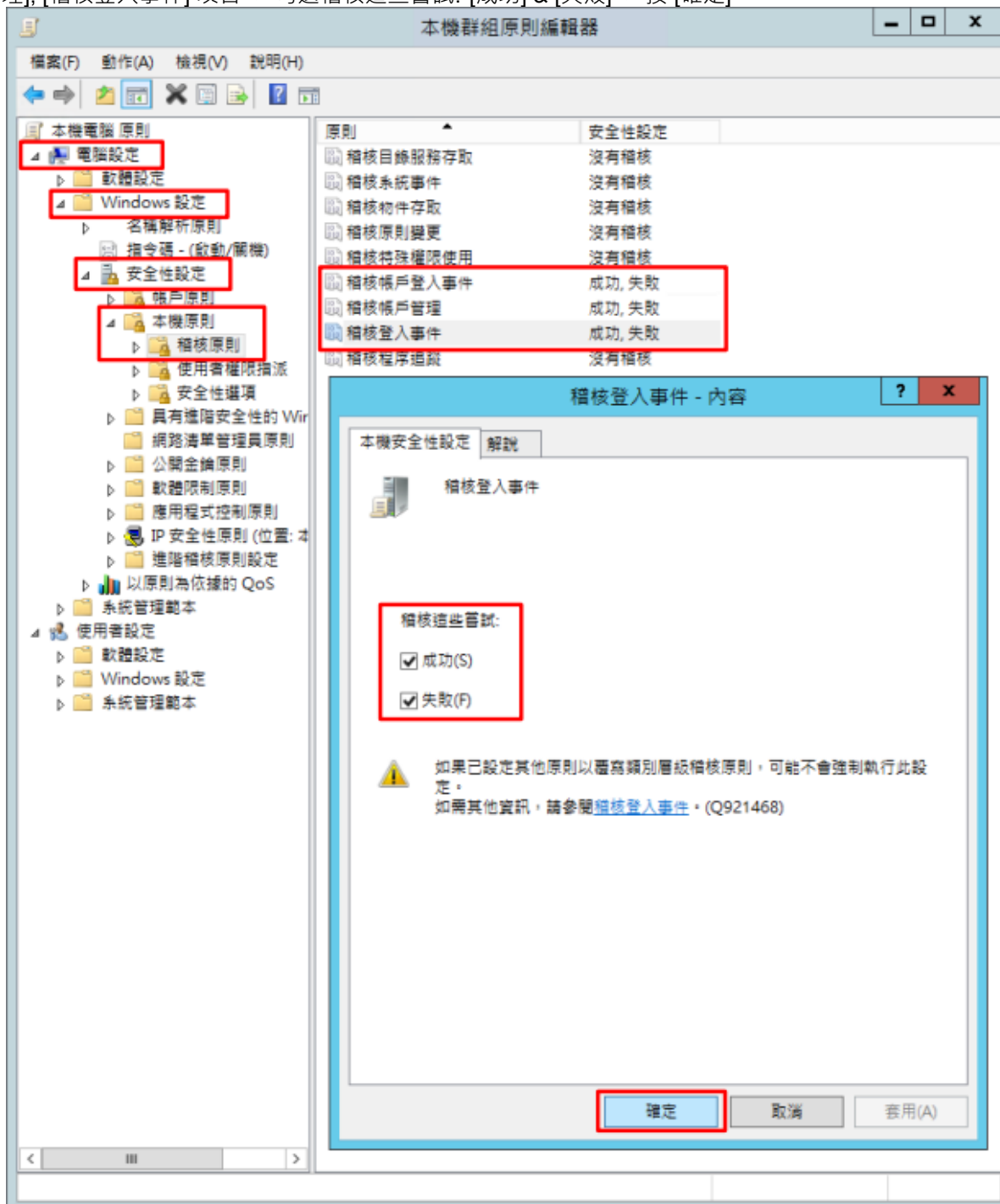
##### (2) 搜尋群組原則物件編輯器並執行

輸入 [群組原則](#) -> 點選 [編輯群組原則]



### (3) 本機原則：稽核原則

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

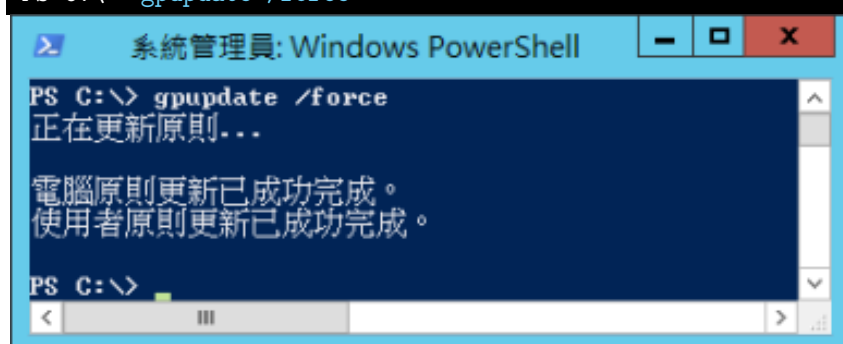


(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

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



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

系統管理員: Windows PowerShell

```

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

```

### 3.3.2.2 事件檔案設定

#### (1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



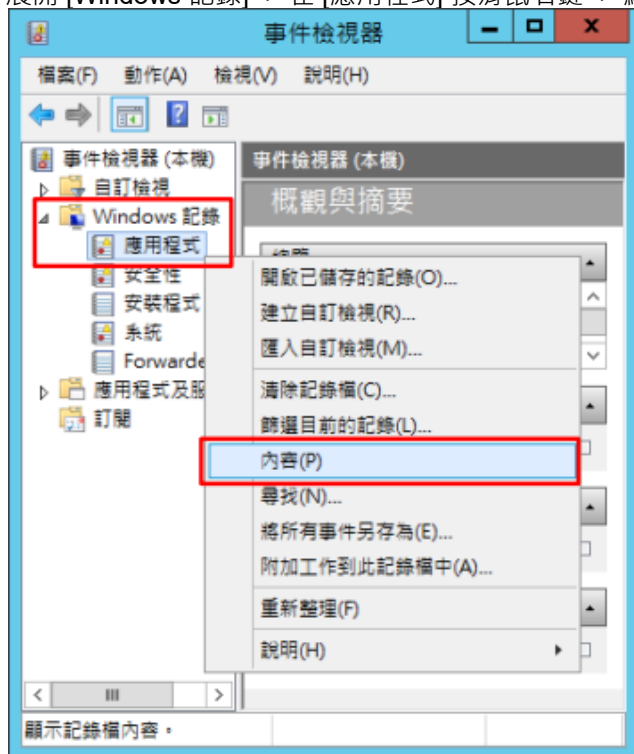
#### (2) 搜尋事件檢視器並執行

輸入 [事件檢視器](#) -> 點選 [[事件檢視器]]



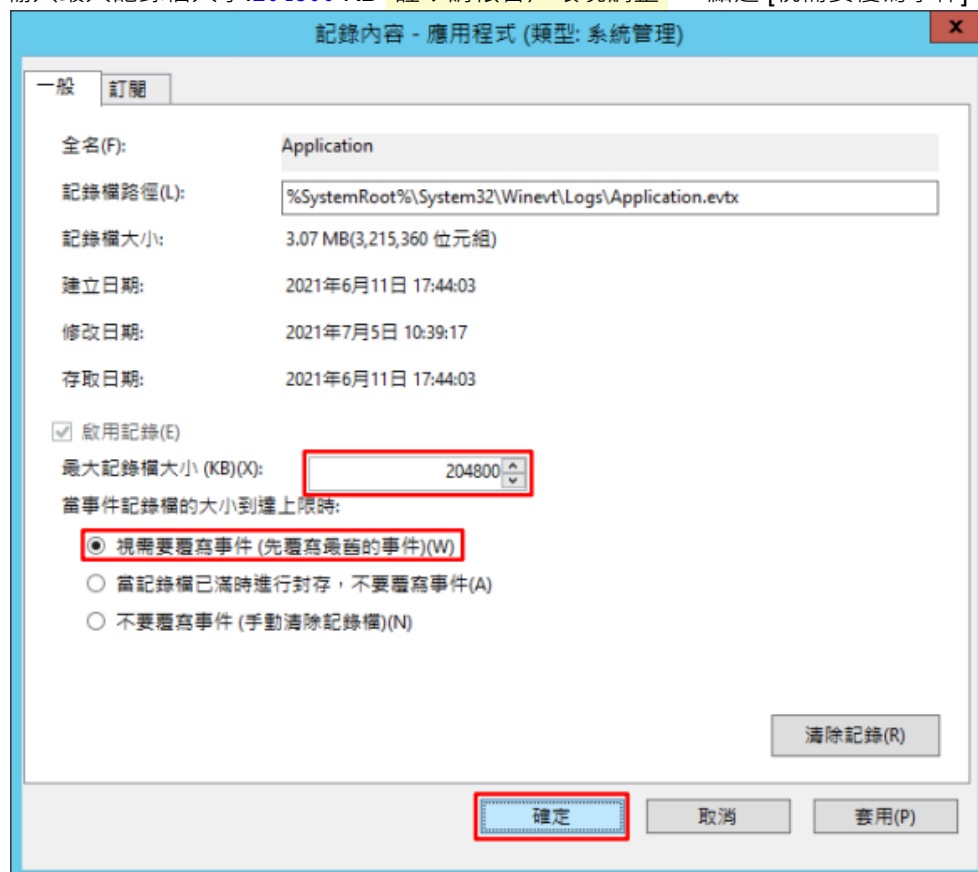
### (3) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [應用程式] 按滑鼠右鍵 -> 點選 [內容]



### (4) 設定應用程式記錄檔

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



## 4 SQL2016

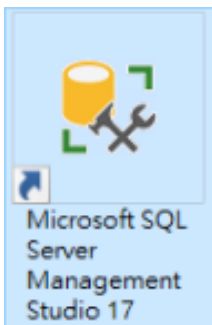
### 4.1 稽核登入

啟用登入稽核，以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。

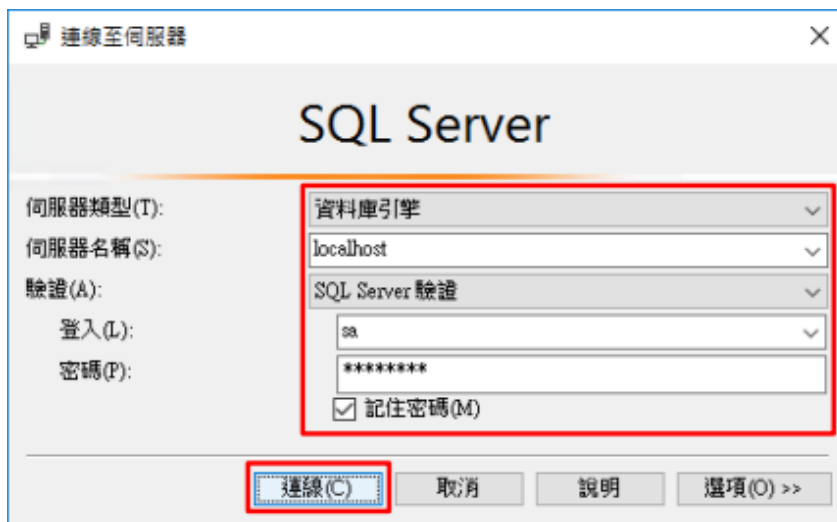
以下分別為圖形介面和指令介面設定方式。

#### 4.1.1 使用圖形介面方式設定

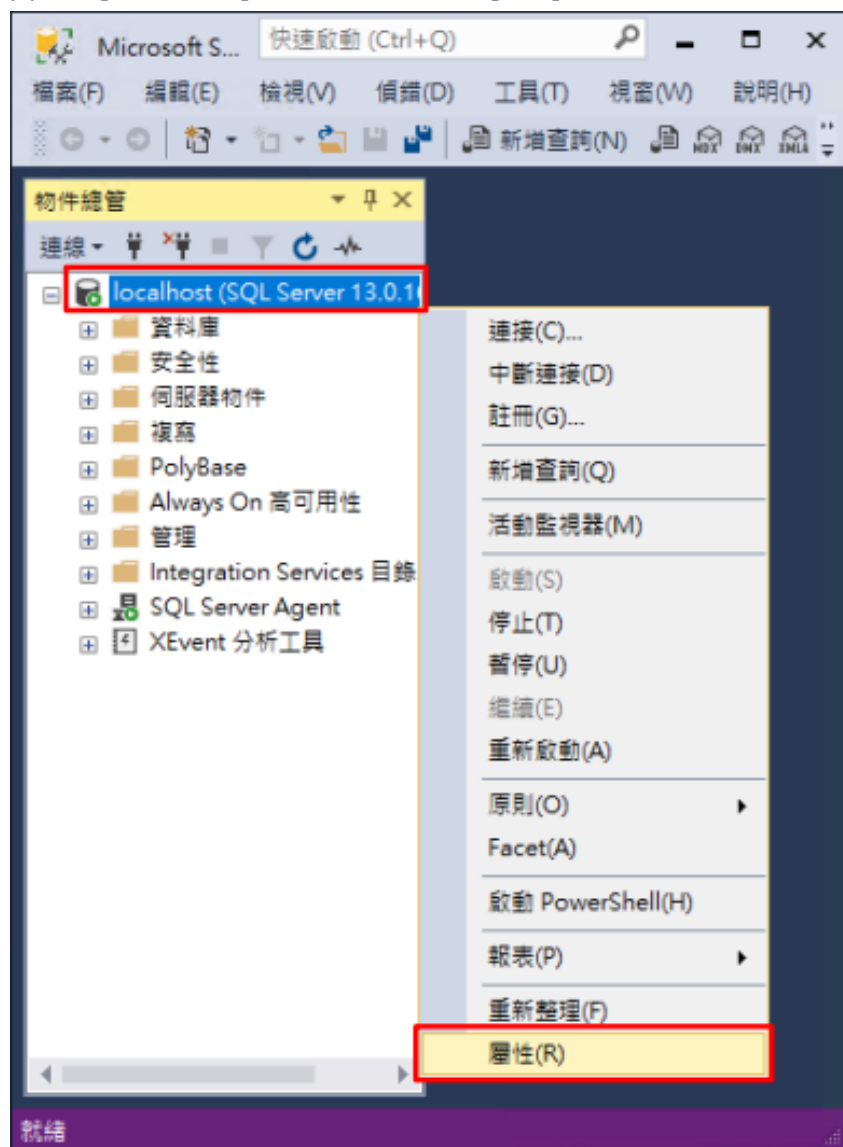
##### (1) 開啟 [Microsoft SQL Server Management Studio]



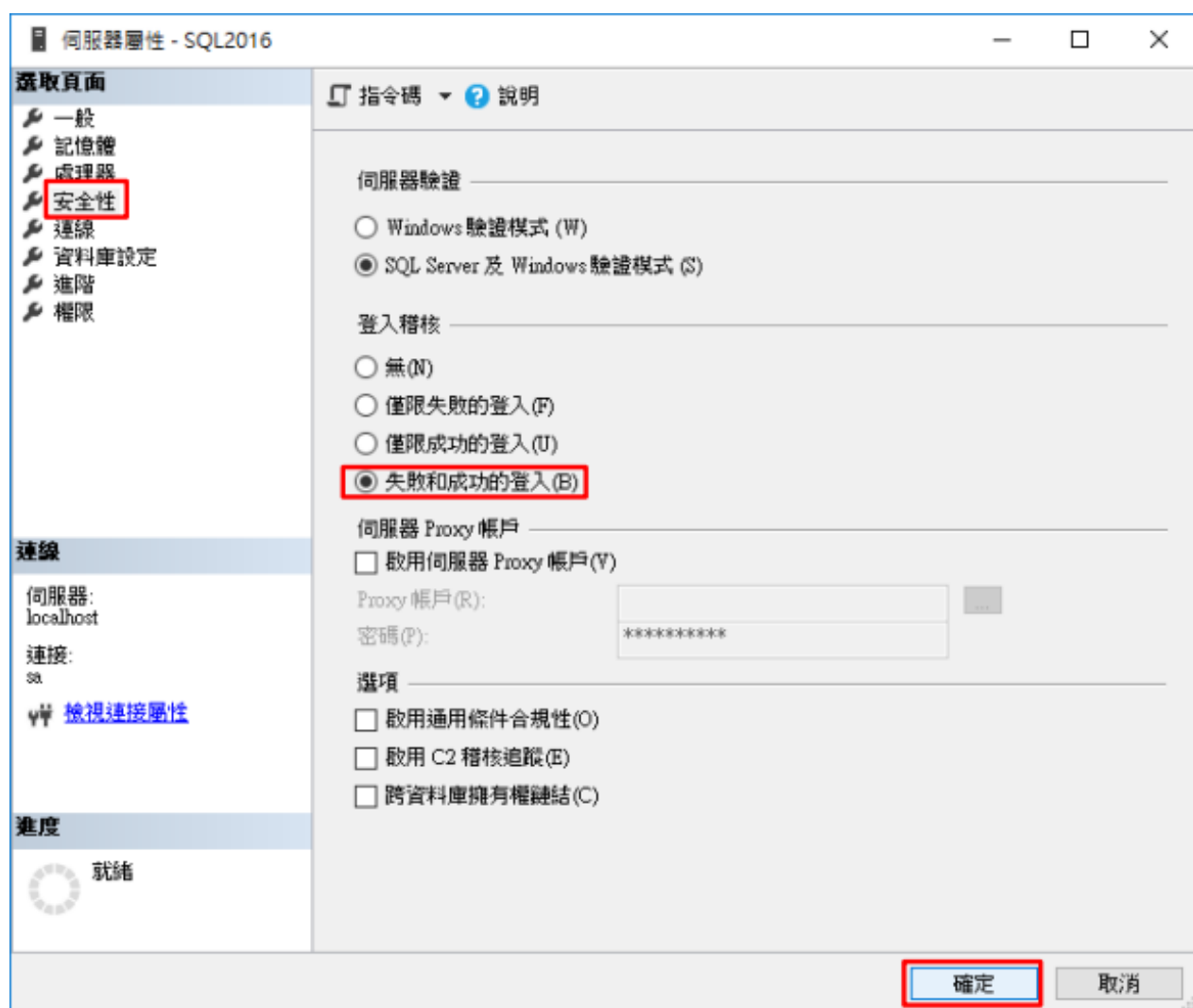
##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

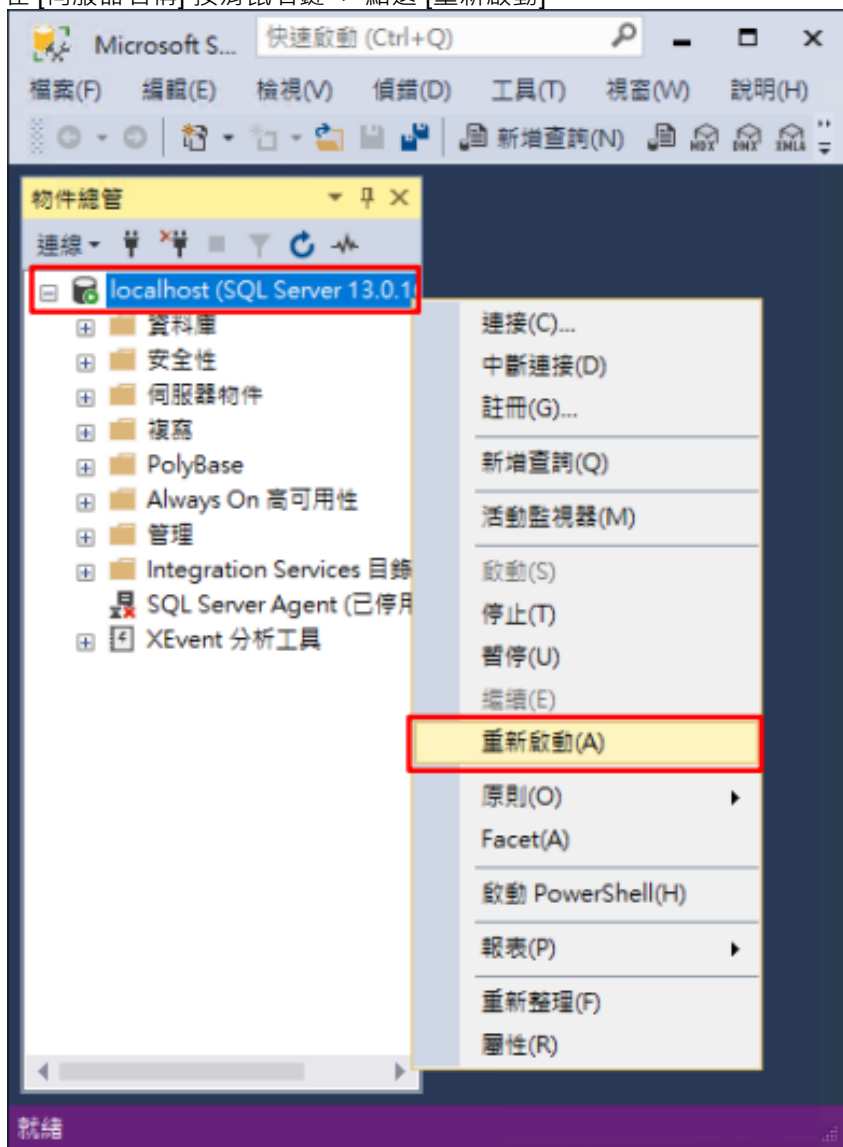


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

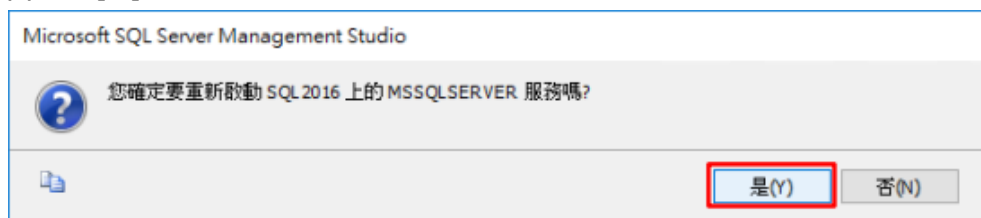


### (5) 重新啟動 MS SQL SERVER 服務

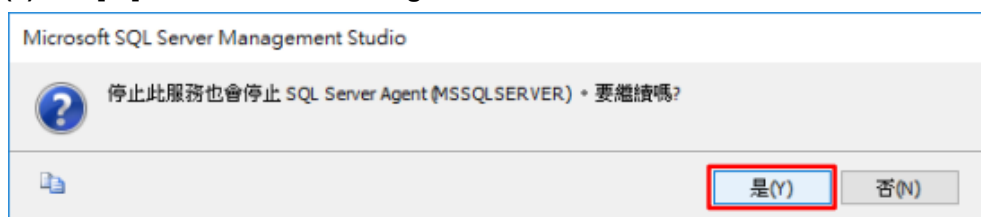
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



### (6) 按 [是] 重新啟動 MS SQL SERVER 服務



### (7) 按 [是] 停止 SQL SERVER Agent 服務



## 4.1.2 使用指令介面方式設定

### (1) 開啟 [Windows Powershell]



### (2) 分別為 sa 或 Windows 帳號登入方式

#### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

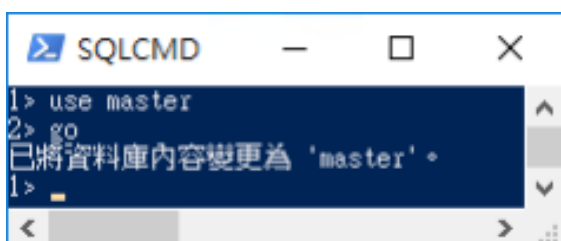
#### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



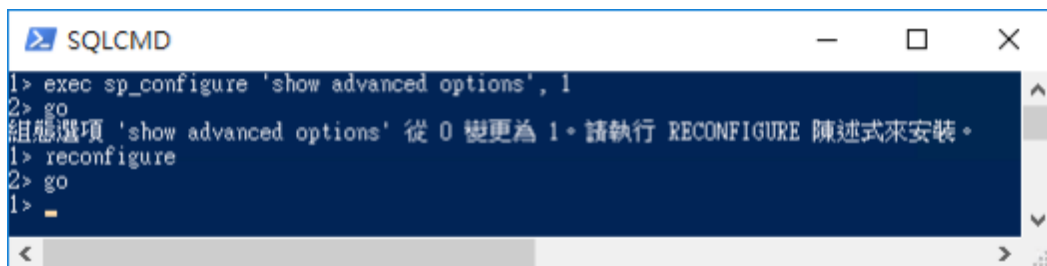
### (3) 切換資料庫

```
1 > use master
2 > go
```



#### (4) 使用 sp\_configure 列出進階選項

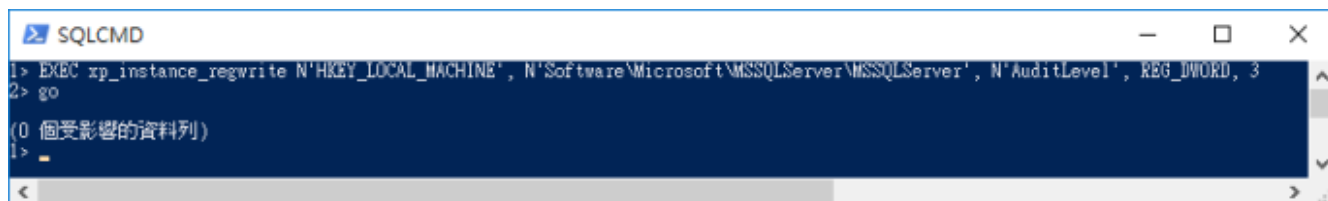
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



A screenshot of a SQLCMD window. The title bar says 'SQLCMD'. The command prompt shows the following sequence: '1> exec sp\_configure 'show advanced options', 1', '2> go', and then a message in Chinese: '組態選項 'show advanced options' 從 0 變更為 1。請執行 RECONFIGURE 陳述式來安裝。' (Configuration option 'show advanced options' changed from 0 to 1. Please execute the RECONFIGURE statement to install.). This is followed by '1> reconfigure', '2> go', and '1>'.

#### (5) 啟用失敗和成功的登入記錄

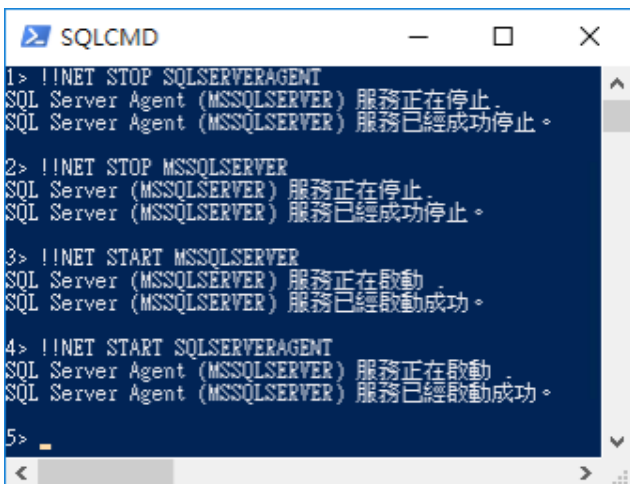
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
```



A screenshot of a SQLCMD window. The title bar says 'SQLCMD'. The command prompt shows: '1> EXEC xp\_instance\_regwrite N'HKEY\_LOCAL\_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG\_DWORD, 3', '2> go', and then '(0 個受影響的資料列)' (0 rows affected). It ends with '1>'.

#### (6) 重新啟動 MS SQL SERVER 服務

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



A screenshot of a SQLCMD window. The title bar says 'SQLCMD'. The command prompt shows the following sequence: '1> !!NET STOP SQLSERVERAGENT' followed by 'SQL Server Agent (MSSQLSERVER) 服務正在停止。' and 'SQL Server Agent (MSSQLSERVER) 服務已經成功停止。'; '2> !!NET STOP MSSQLSERVER' followed by 'SQL Server (MSSQLSERVER) 服務正在停止。' and 'SQL Server (MSSQLSERVER) 服務已經成功停止。'; '3> !!NET START MSSQLSERVER' followed by 'SQL Server (MSSQLSERVER) 服務正在啟動。' and 'SQL Server (MSSQLSERVER) 服務已經啟動成功。'; '4> !!NET START SQLSERVERAGENT' followed by 'SQL Server Agent (MSSQLSERVER) 服務正在啟動。' and 'SQL Server Agent (MSSQLSERVER) 服務已經啟動成功。'; and finally '5>'.

## 4.2 設定稽核

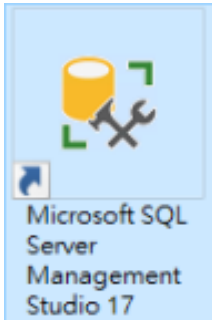
### 4.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

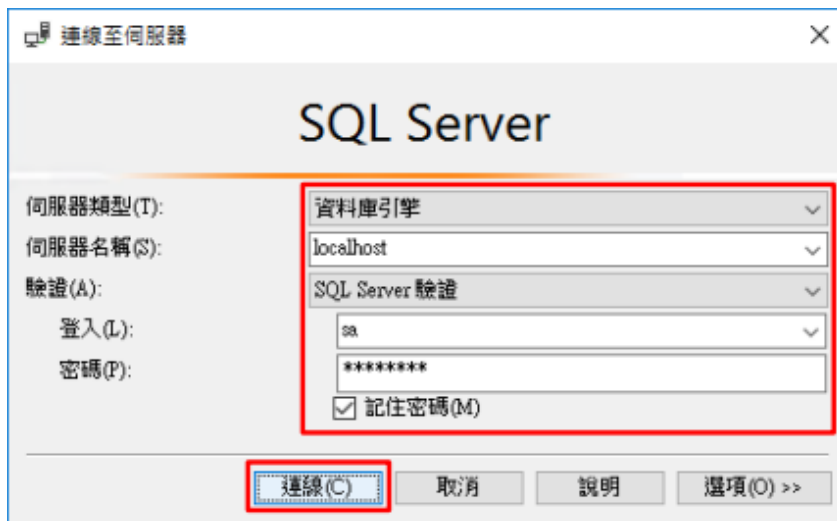
以下分別為圖形介面和指令介面設定方式。

#### 4.2.1.1 使用圖形介面方式設定

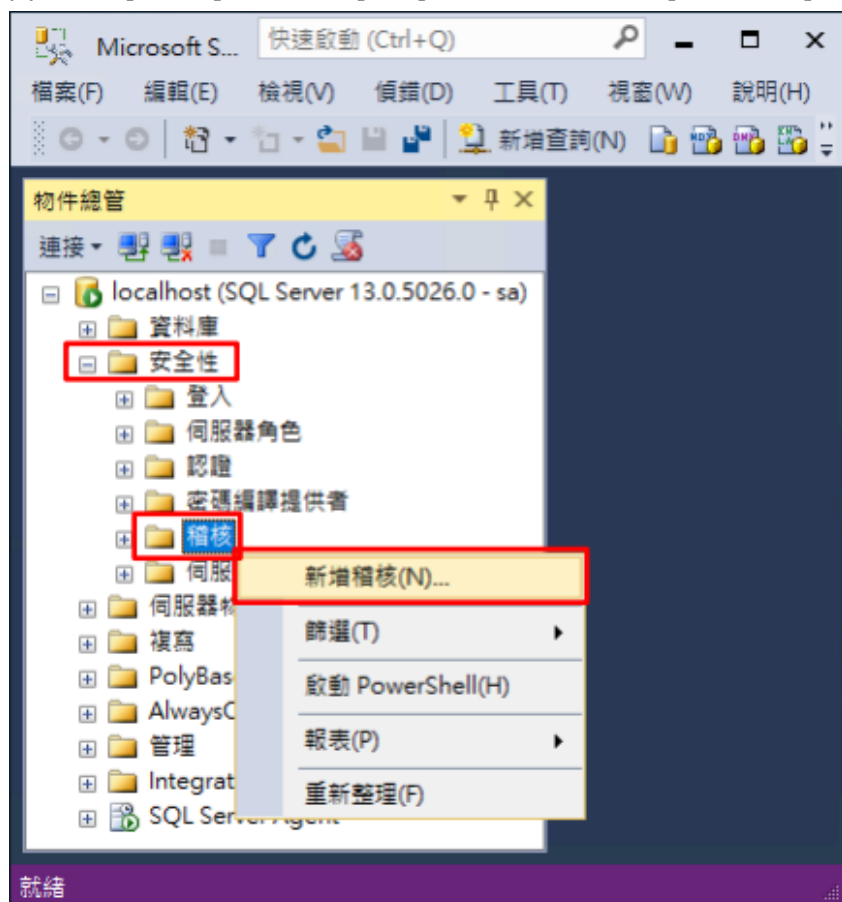
##### (1) 開啟 [Microsoft SQL Server Management Studio]



##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

建立稽核

就緒

選取頁面

- 一般
- 篩選

連線

localhost [sa]

檢視連線屬性

進度

就緒

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒為單位)(Q): 1000

於稽核記錄失敗時:

- ☒ 繼續(C)
- ☐ 關閉伺服器(S)
- ☐ 令操作失敗(F)

稽核目的地(D): 應用程式記錄檔

檔案路徑(P):

稽核檔案數目上限:

- ☒ 最大換用檔案(O):  
☒ 無限制(U)
- ☐ 最大檔案數目(X):  
檔案數目(B): 2147483647

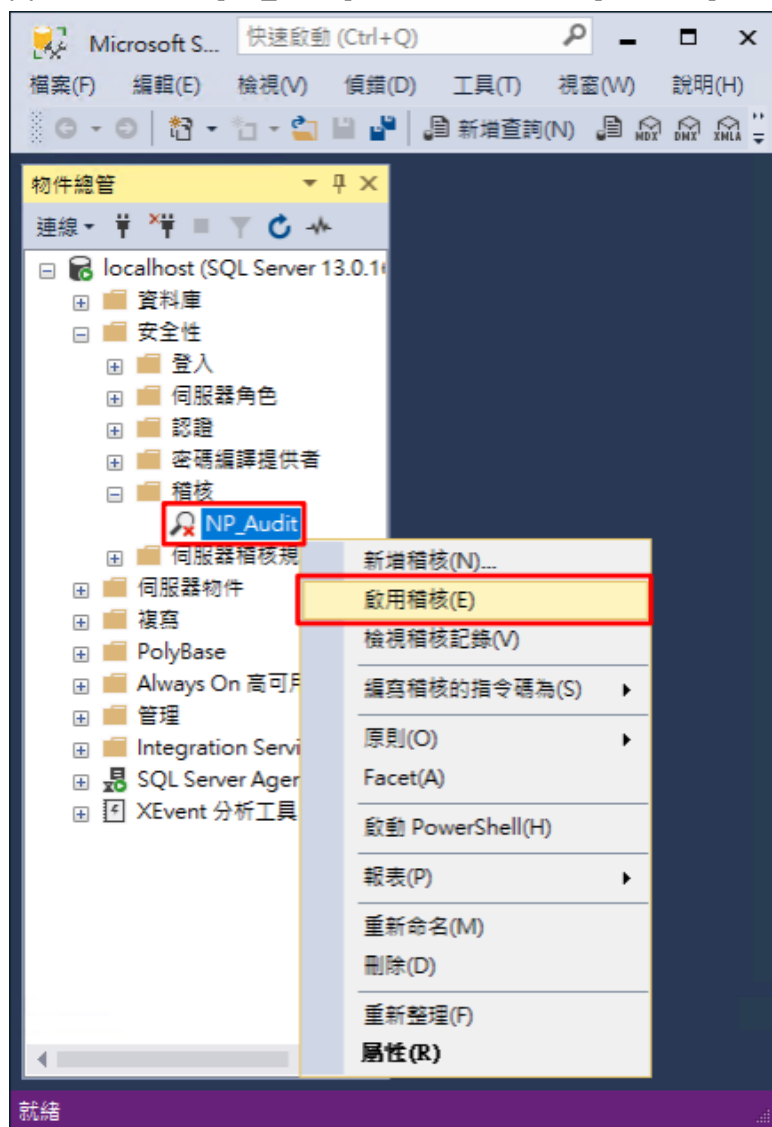
檔案大小上限(Z): 0

- ☒ MB(M) ☐ GB(G) ☐ TB(T)
- ☒ 無限制(L)

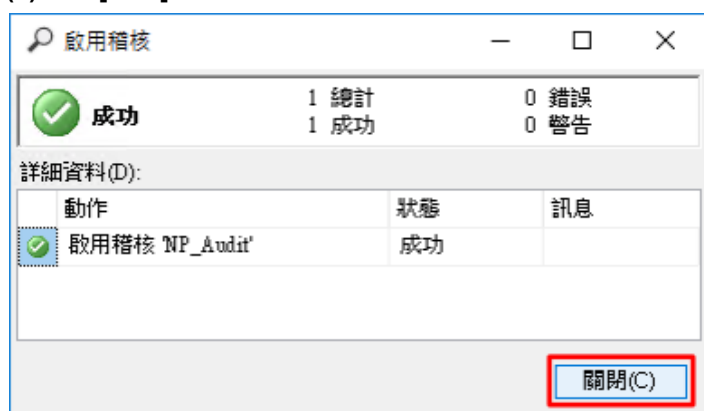
☐ 保留磁碟空間(R)

確定 取消 說明

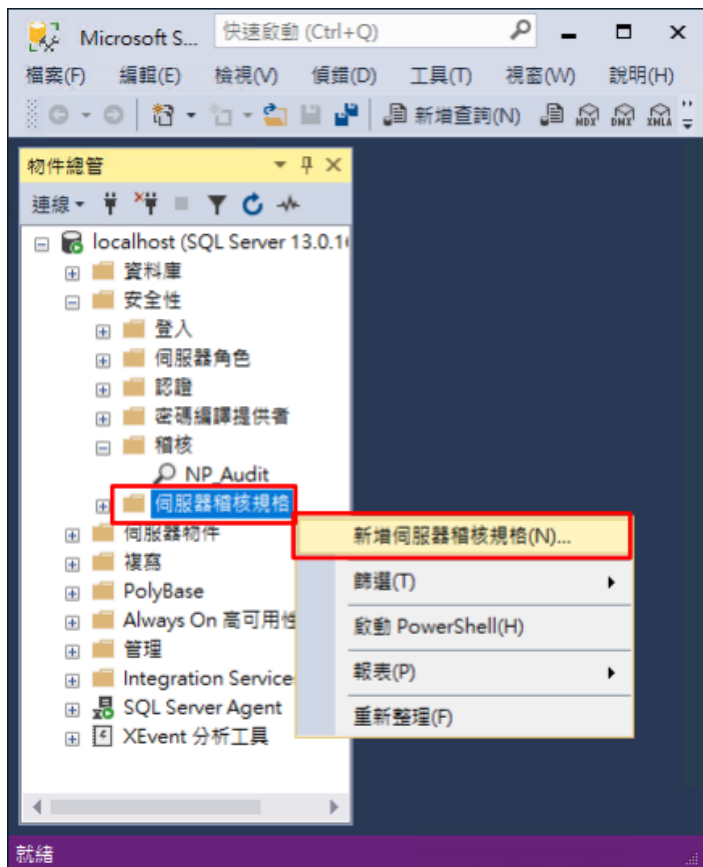
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



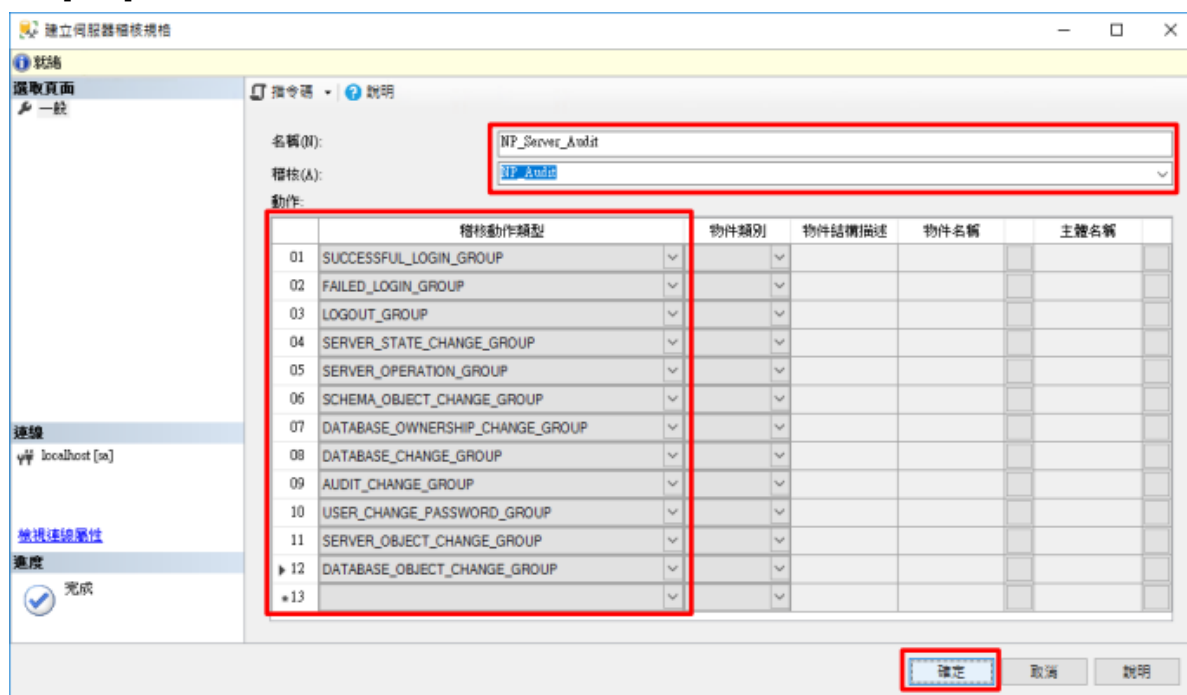
(6) 按 [關閉]



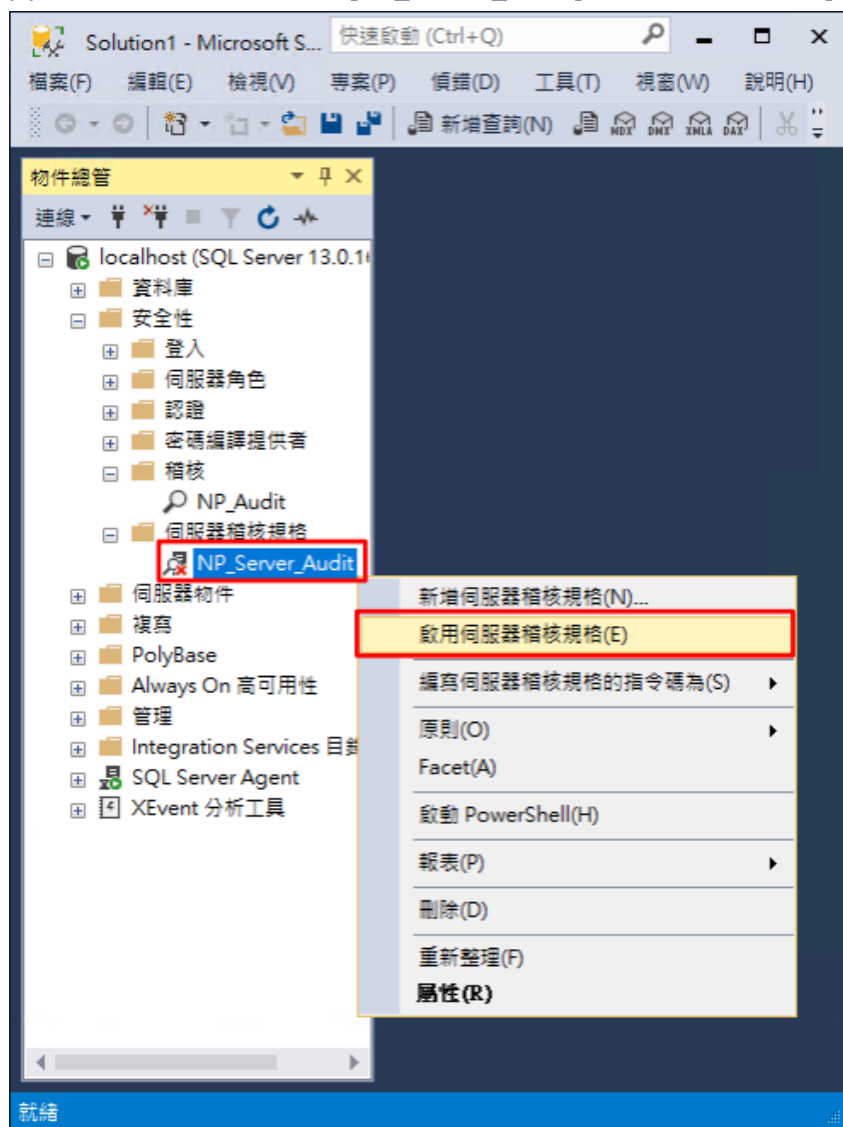
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



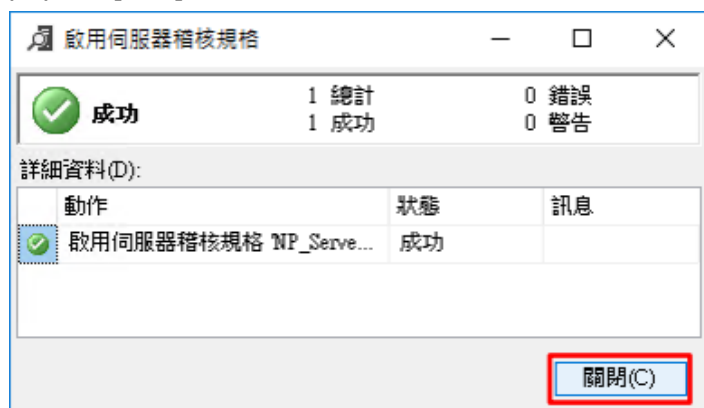
(8) 輸入名稱: `NP_Server_Audit` -> 選擇稽核: `[NP_Audit]` 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在伺服器稽核規格名稱: [NP\_Server\_Audit] 按滑鼠右鍵 -> 點選 [啟用伺服器稽核規格]

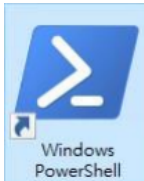


(10) 按 [關閉]



#### 4.2.1.2 使用指令介面方式設定

##### (1) 開啟 [Windows Powershell]



##### (2) 分別為 sa 或 Windows 帳號登入方式

###### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

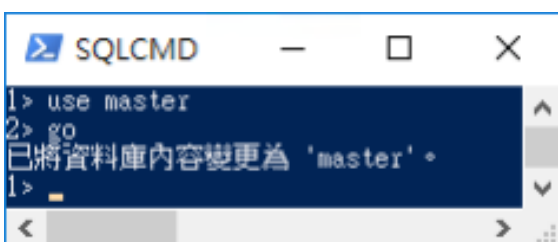
###### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



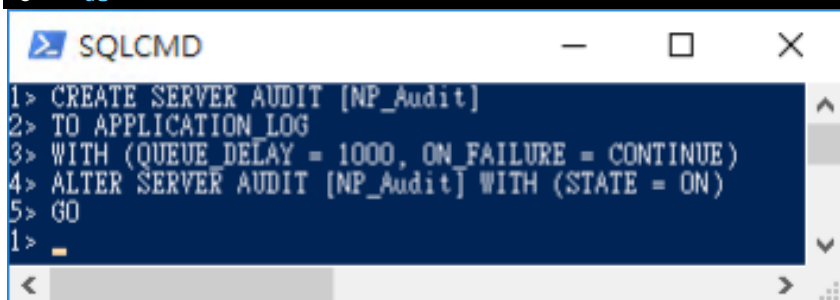
##### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



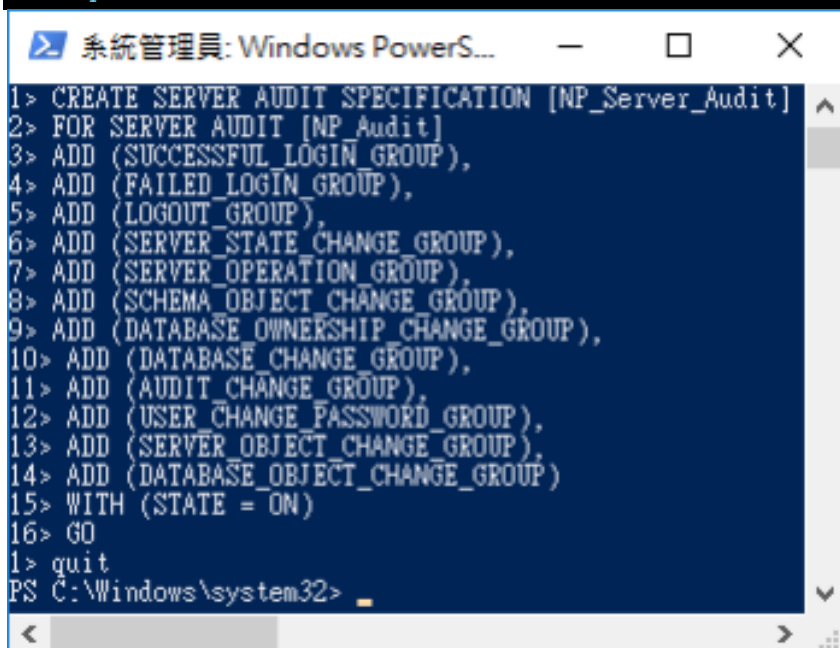
The screenshot shows a SQLCMD window with the following commands entered:

```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

紅色文字部位請輸入稽核名稱

(5) 設定稽核伺服器 · ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP)
12 > WITH (STATE = ON)
13 > GO
1 > quit
```



The screenshot shows a Windows PowerShell window titled '系統管理員: Windows PowerS...' with the following commands entered:

```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP),
13> ADD (SERVER_OBJECT_CHANGE_GROUP),
14> ADD (DATABASE_OBJECT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\Windows\system32> _
```

紅色文字部位請輸入伺服器稽核規格名稱

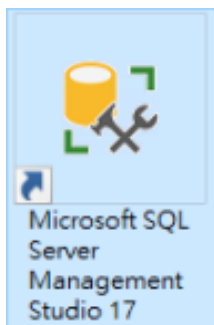
## 4.2.2 稽核資料庫層級

啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

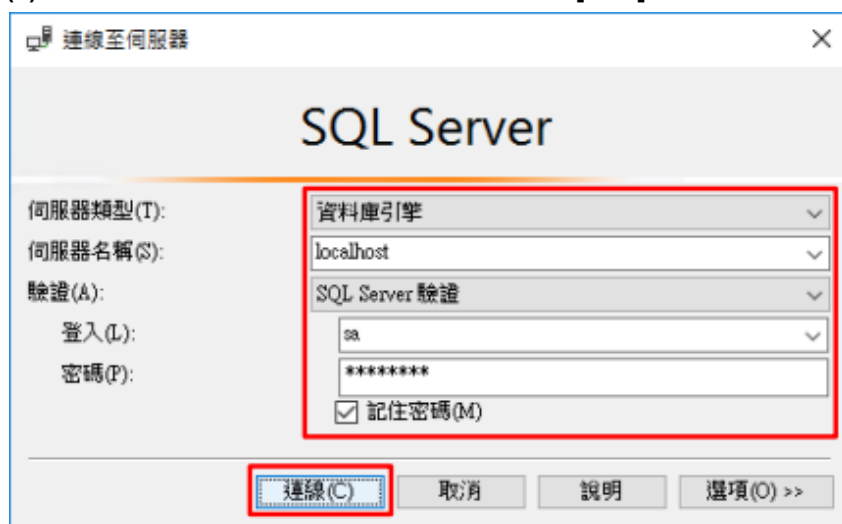
以下分別為圖形介面和指令介面設定方式。

### 4.2.2.1 使用圖形介面方式設定

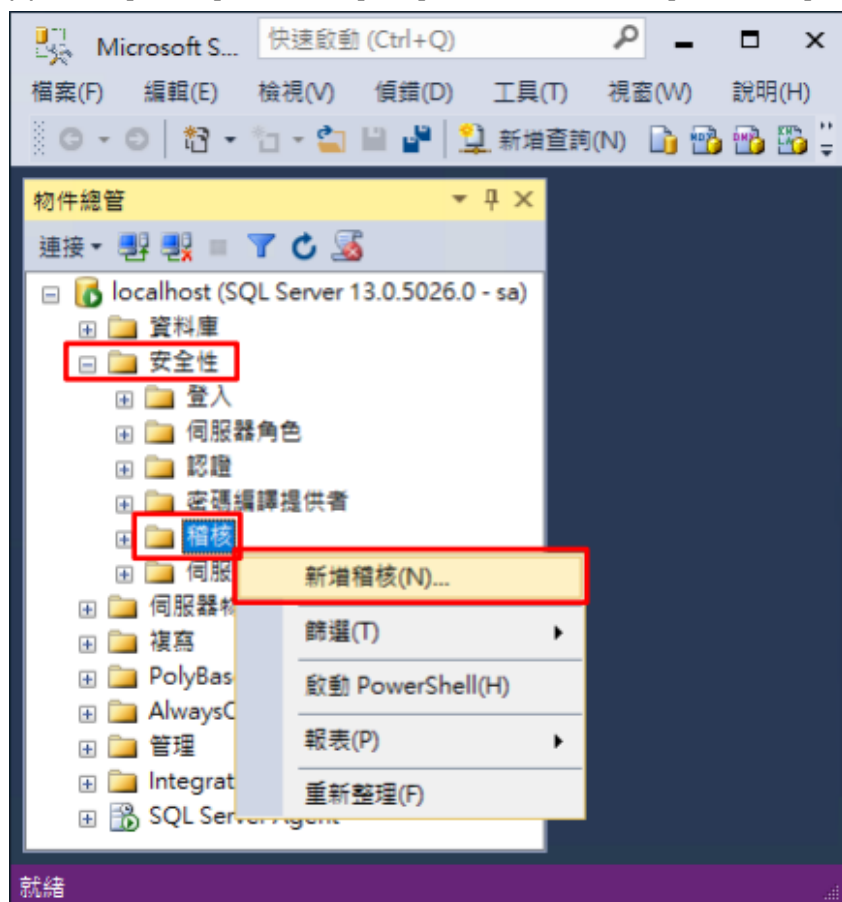
#### (1) 開啟 [Microsoft SQL Server Management Studio]



#### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

建立稽核

就緒

選取頁面

- 一般
- 篩選

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒為單位)(Q): 1000

於稽核記錄失敗時:

- ☒ 繼續(C)
- ☐ 關閉伺服器(S)
- ☐ 令操作失敗(F)

稽核目的地(D): 應用程式記錄檔

檔案路徑(P):

稽核檔案數目上限:

- ☒ 最大換用檔案(O):
  - ☒ 無限制(U)
- ☐ 最大檔案數目(X):
  - 檔案數目(B): 2147483647

檔案大小上限(Z): 0

- ☒ MB(M)
- ☐ GB(G)
- ☐ TB(T)

- ☒ 無限制(L)

☐ 保留磁碟空間(R)

連線

localhost [sa]

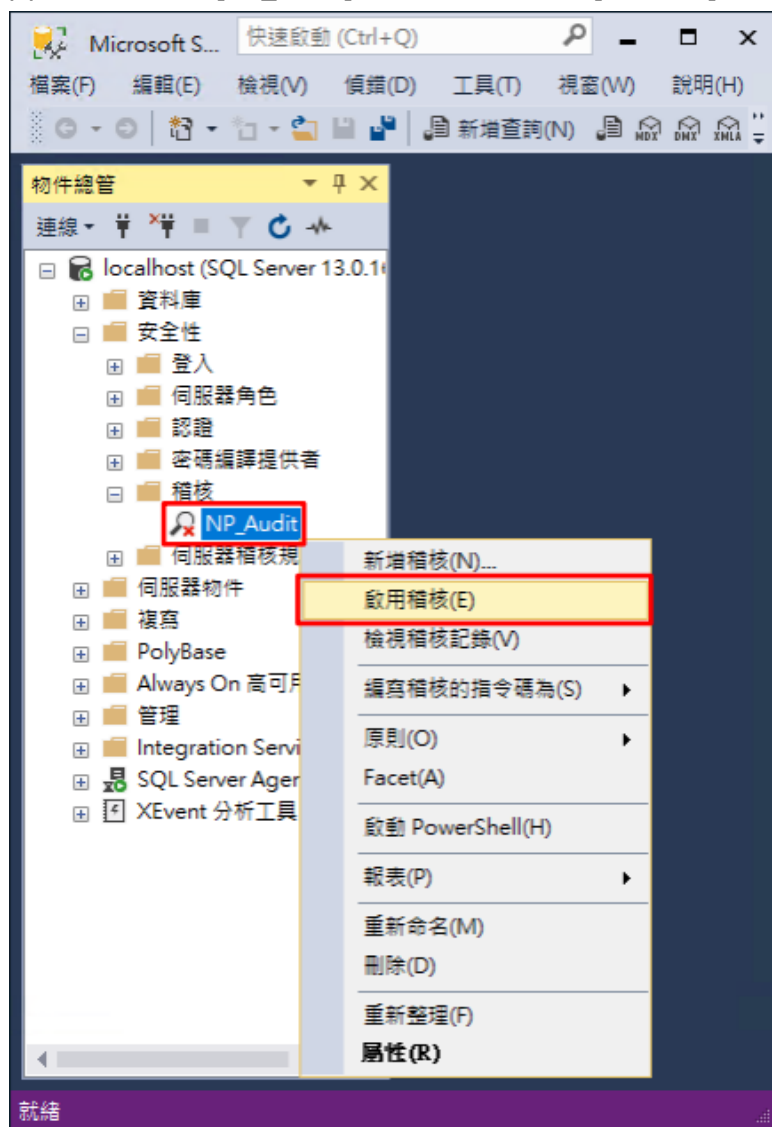
[檢視連線屬性](#)

進度

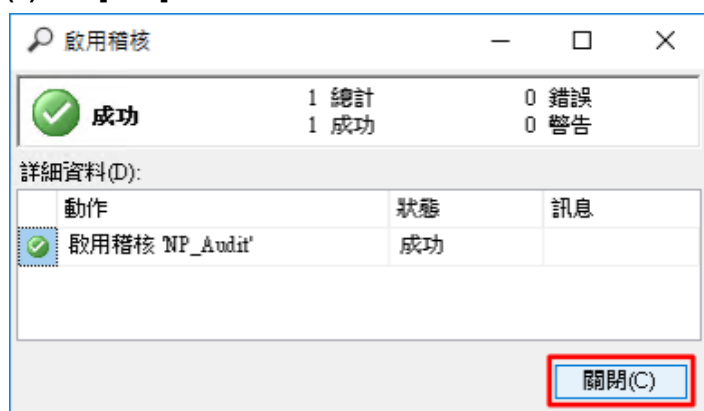
就緒

確定 取消 說明

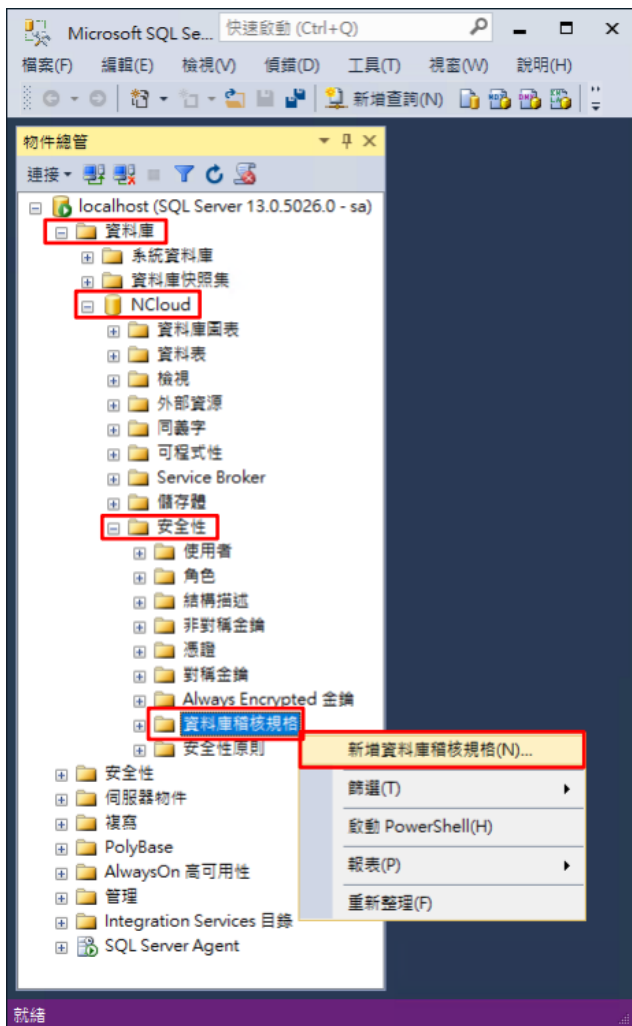
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



(6) 按 [關閉]



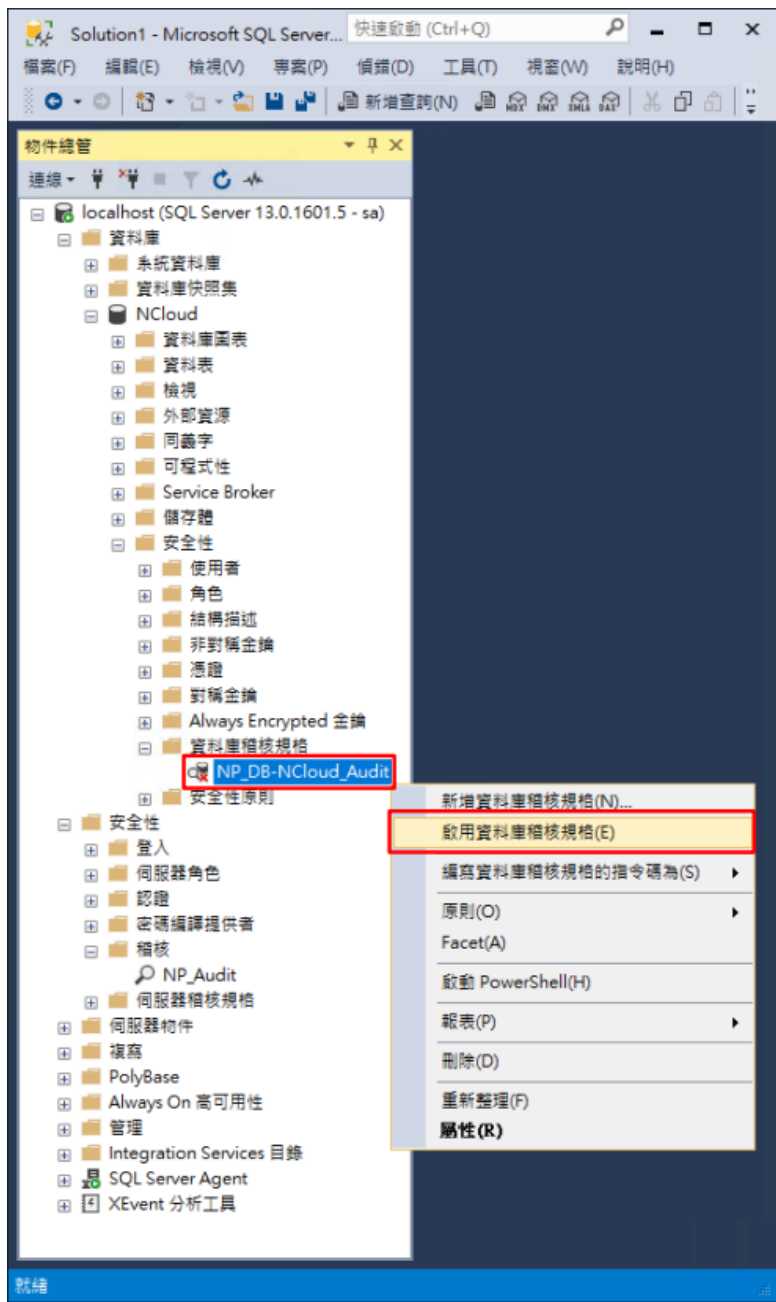
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



(8) 輸入稽核名稱: NP\_DB-NCloud\_Audit -> 選擇稽核: [NP\_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在資料庫稽核規格名稱: [NP\_DB-NCloud\_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10) 按 [關閉]



#### 4.2.2.2 使用指令介面方式設定

##### (1) 開啟 [Windows Powershell]



##### (2) 分別為 sa 或 Windows 帳號登入方式

###### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

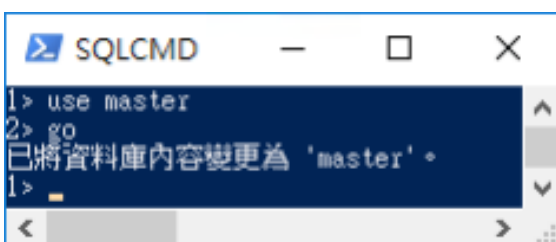
###### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



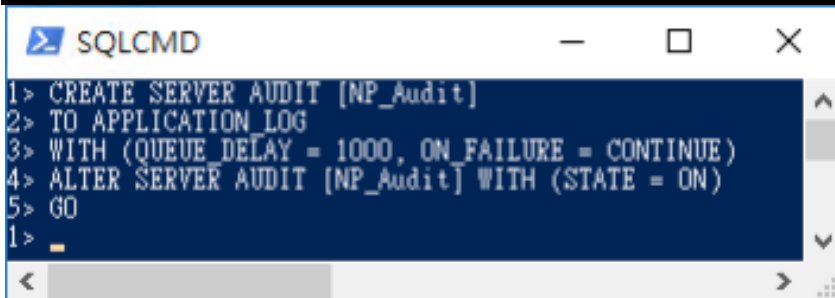
##### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

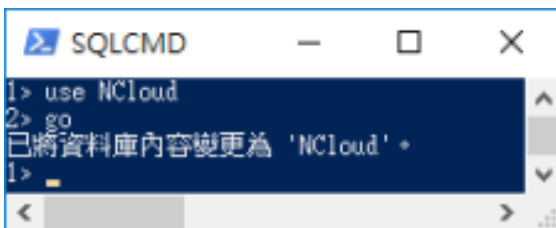
```
1 > CREATE SERVER AUDIT [NP_Audit]  
2 > TO APPLICATION_LOG  
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)  
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)  
5 > GO
```



紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫 · 範例：NCloud

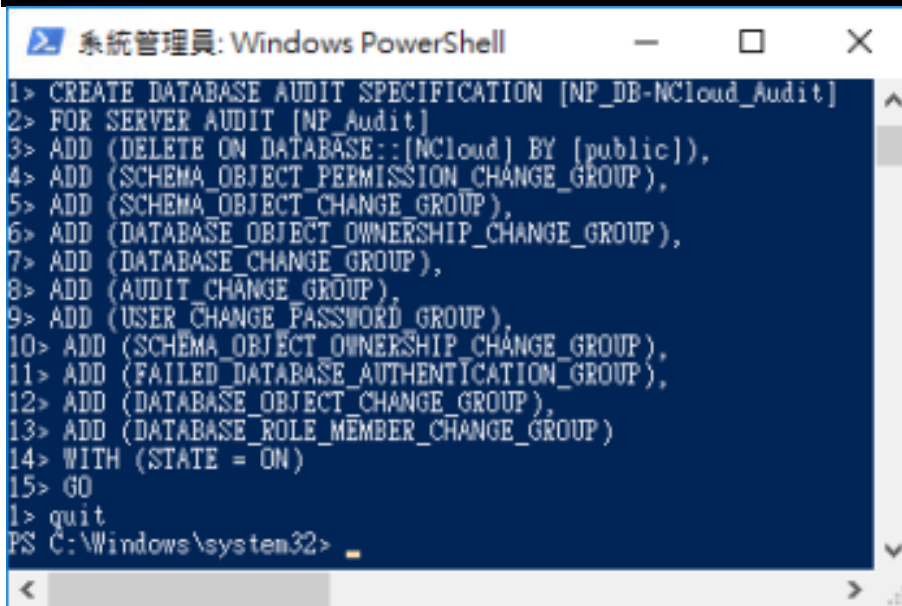
```
1 > use NCloud  
2 > go
```



紅色文字部位請輸入稽核資料庫名稱

(6) 設定稽核 NCloud(範例) 資料庫・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```



紅色文字部位請輸入資料庫稽核規格名稱

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

紅色文字部位請輸入稽核資料庫名稱

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

## 4.3 事件記錄檔設定

此為選項設定。

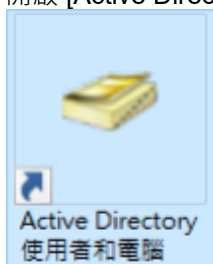
以下分別為網域和工作群組設定方式。

### 4.3.1 網域

#### 4.3.1.1 組織單位設定

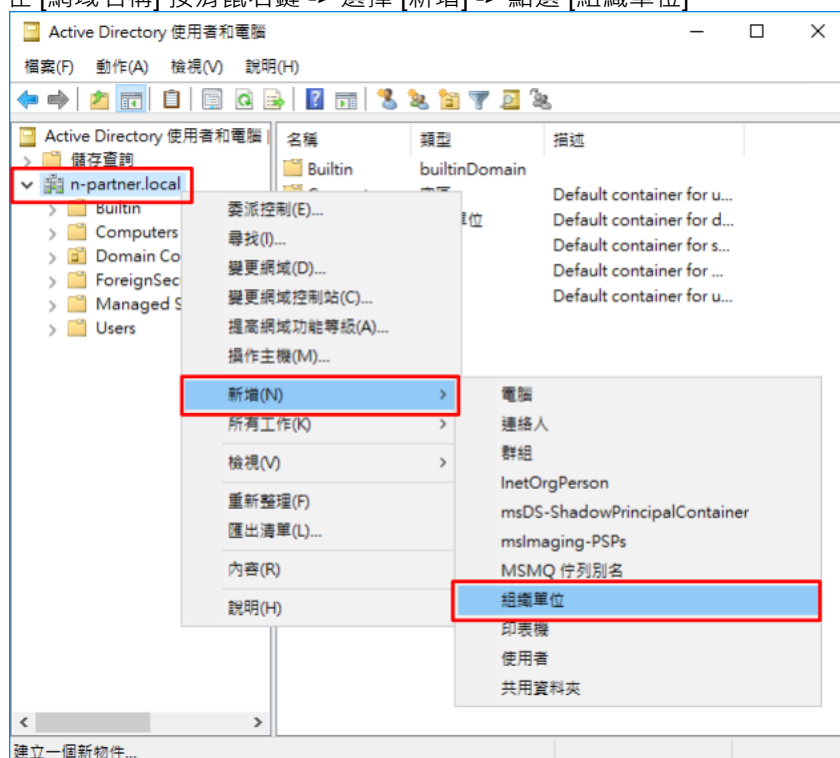
##### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



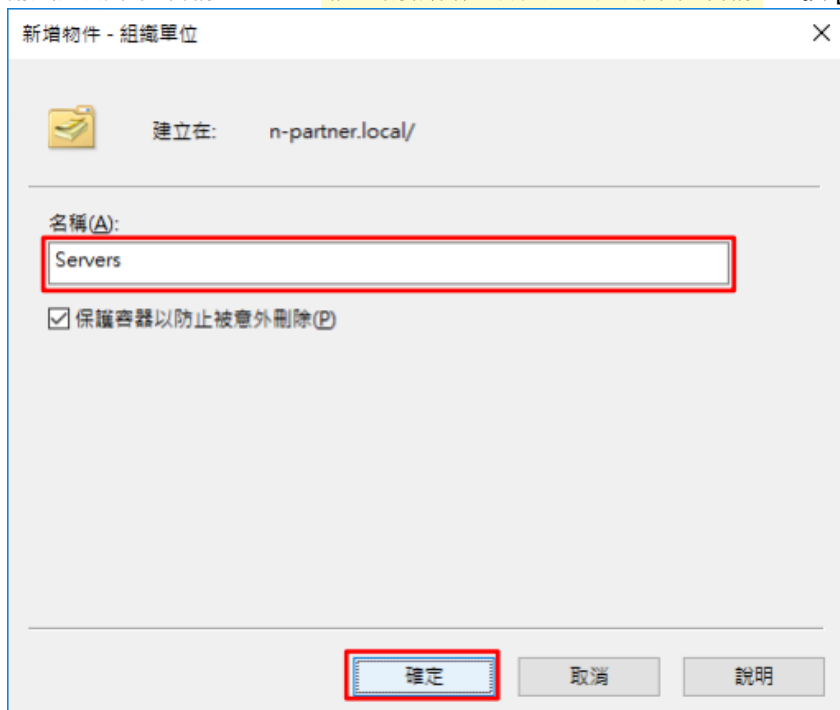
##### (2) 新增組織單位

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



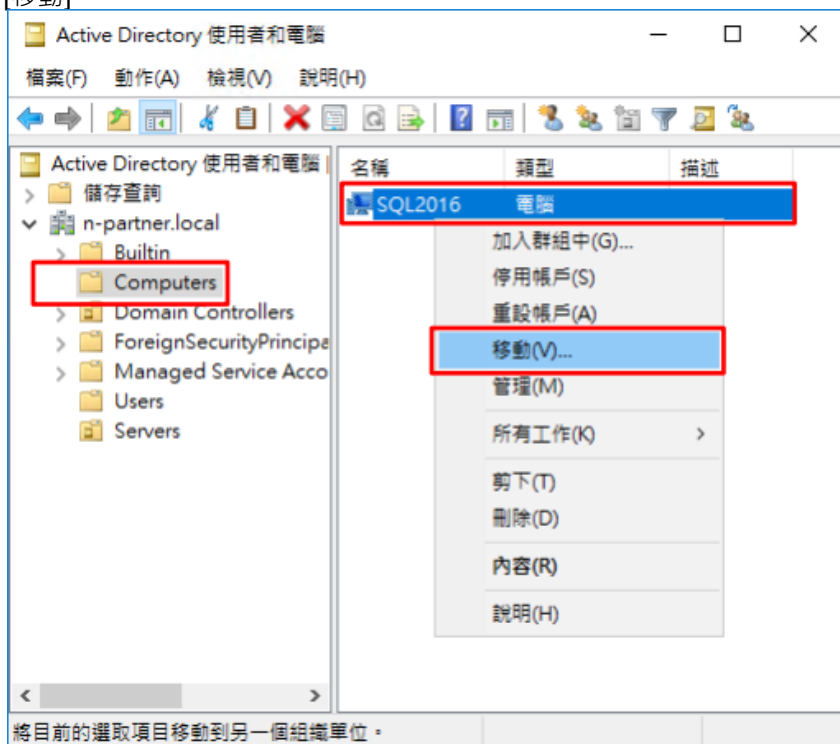
### (3) 輸入組織單位名稱

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



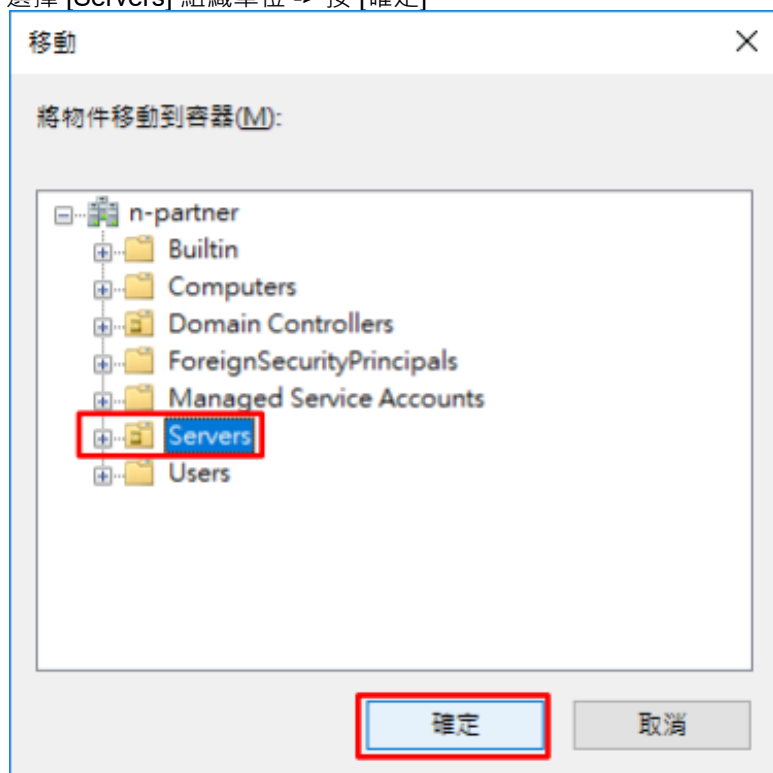
### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL 2016] 伺服器, 按滑鼠右鍵, 註：請依客戶環境選擇 MS SQL Server 主機 -> 點選 [移動]



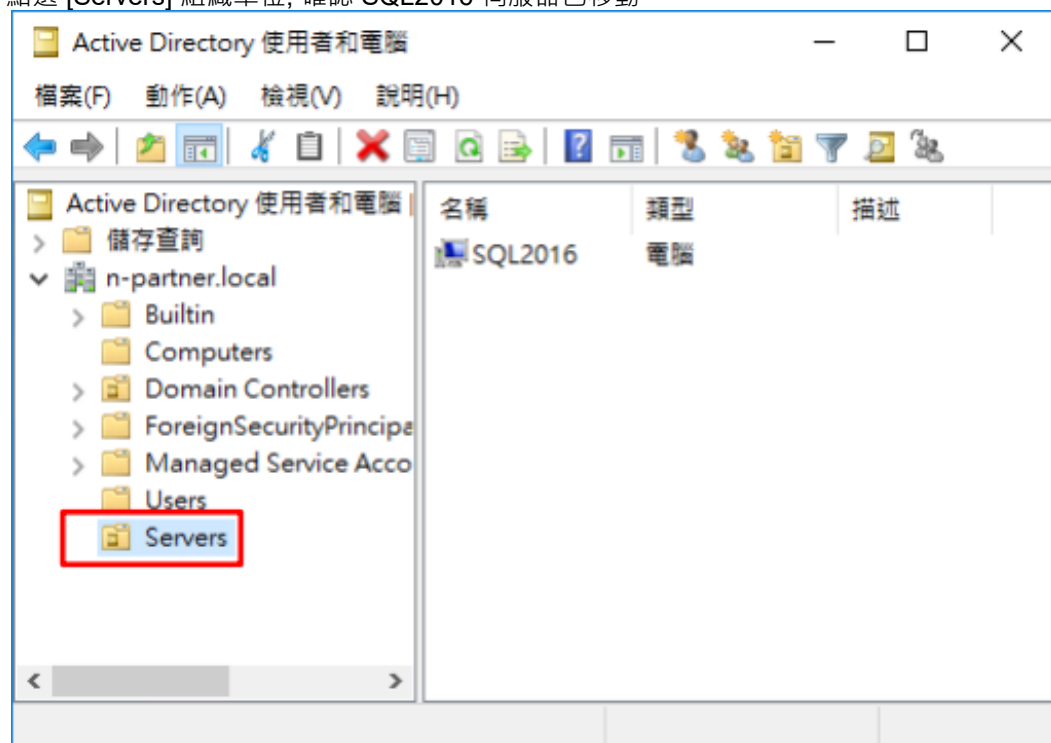
## (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



## (6) 確認伺服器已移動至新的組織單位

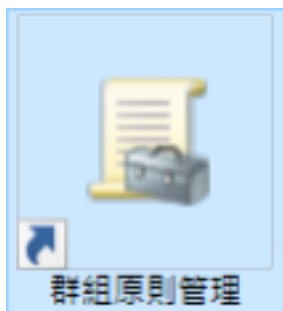
點選 [Servers] 組織單位, 確認 SQL2016 伺服器已移動。



#### 4.3.1.2 群組原則設定

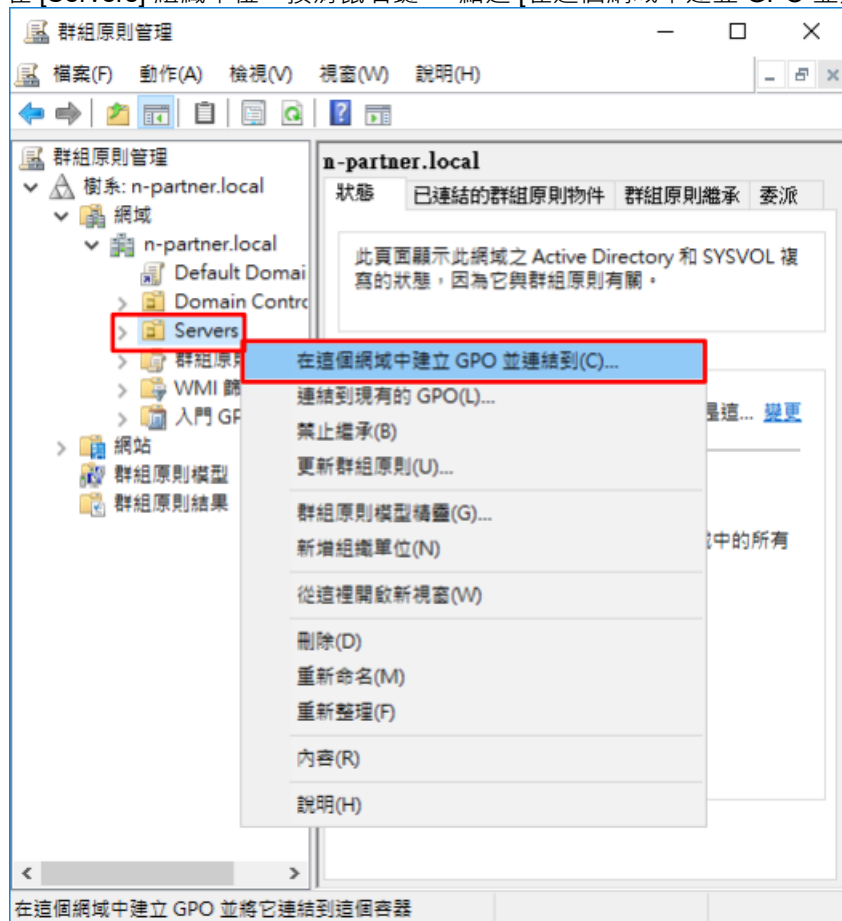
##### (1) 開啟群組原則管理

開啟 [群組原則管理]



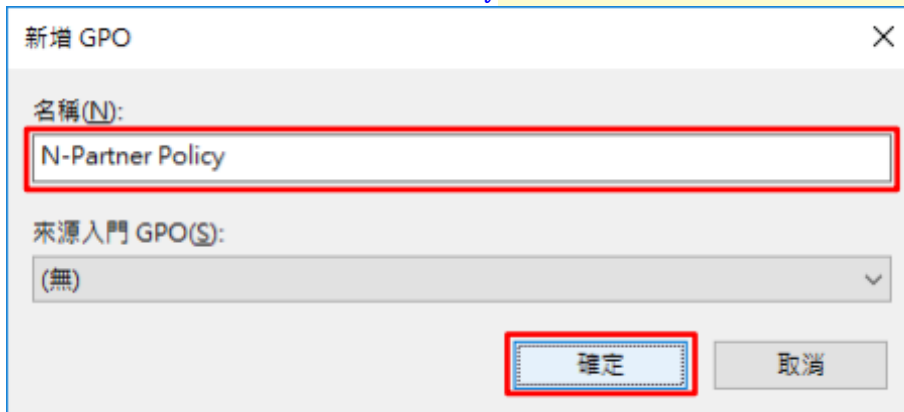
##### (2) 在 Servers 組織單位，新增群組原則物件

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



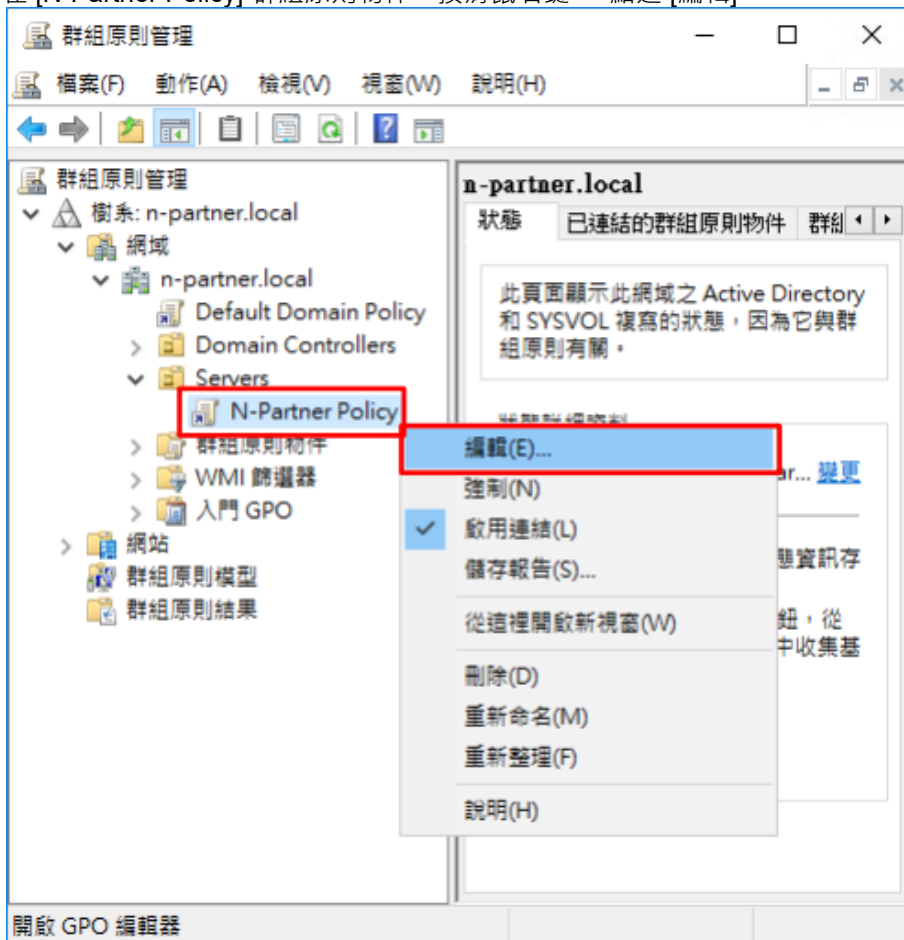
### (3) 輸入群組原則物件名稱

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



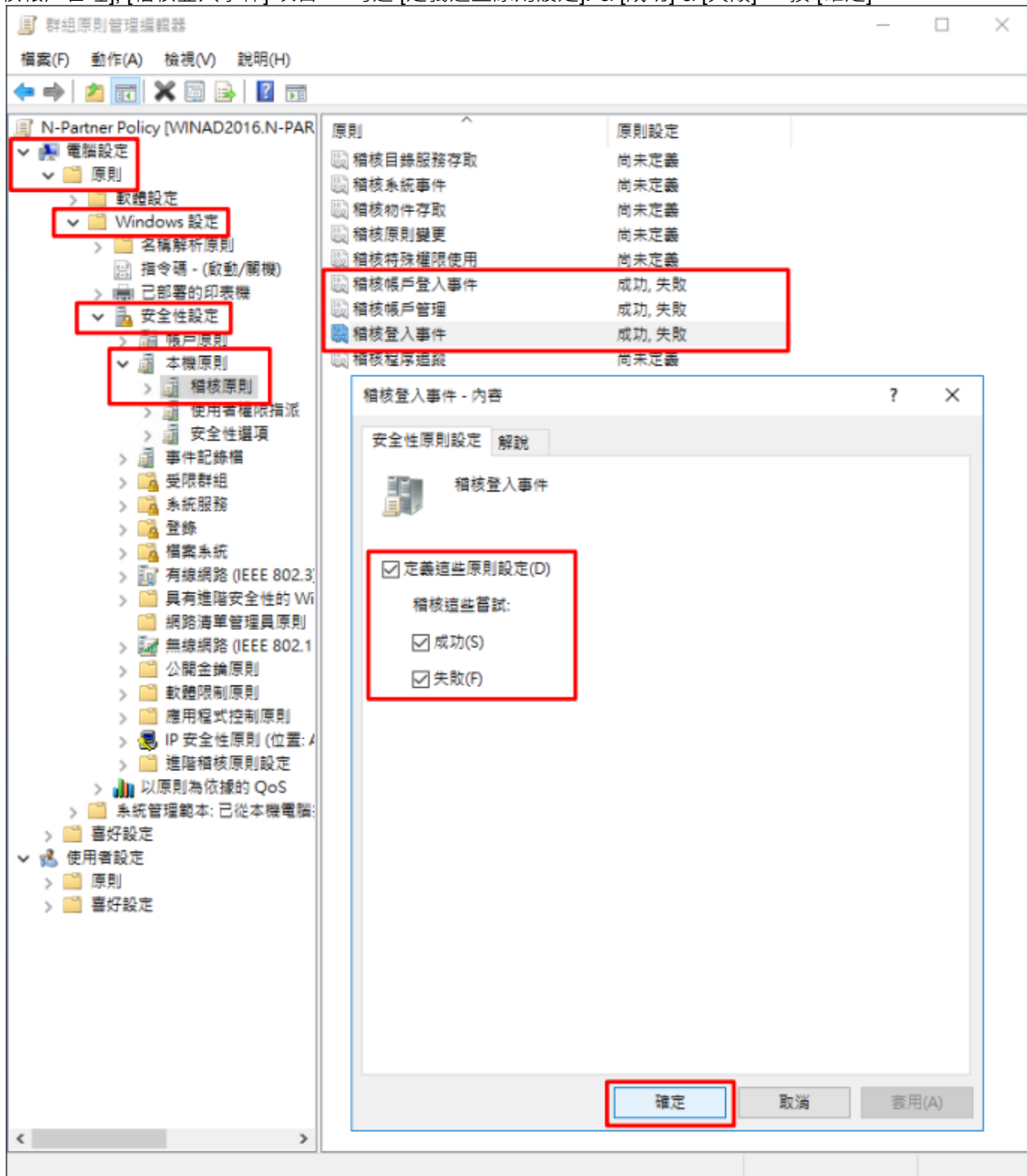
### (4) 編輯群組原則物件

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



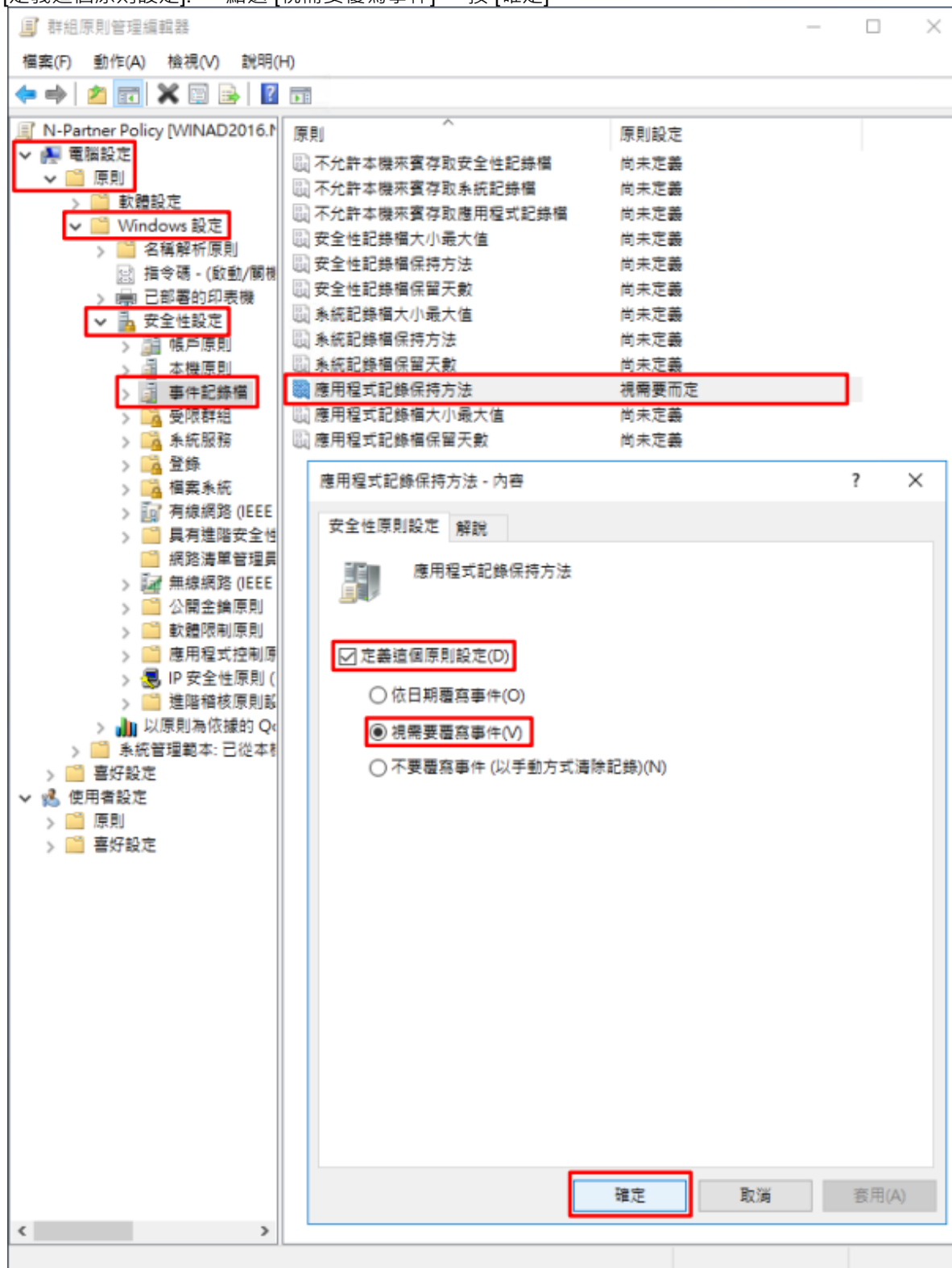
##### (5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



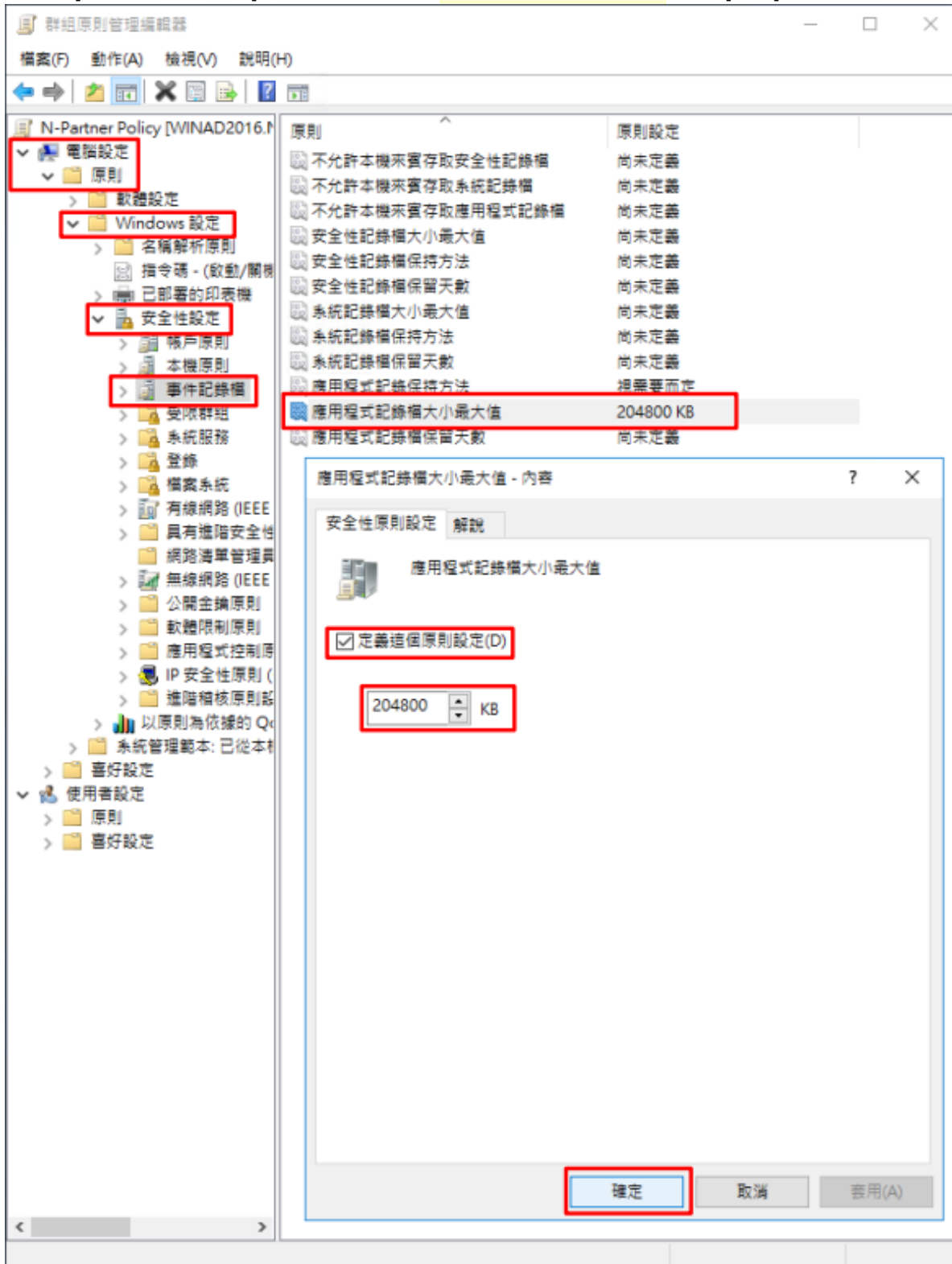
## (6) 事件記錄：應用程式記錄保持方法

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



### (7) 事件記錄：應用程式記錄檔大小最大值

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

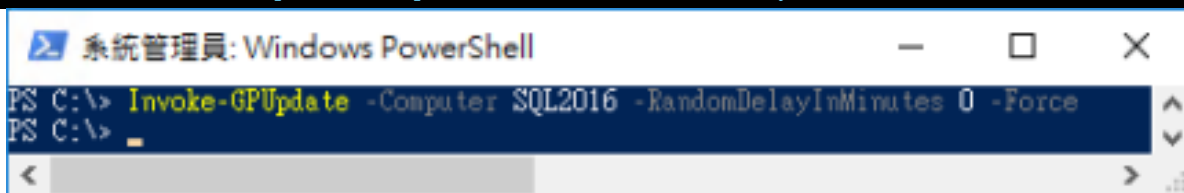


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

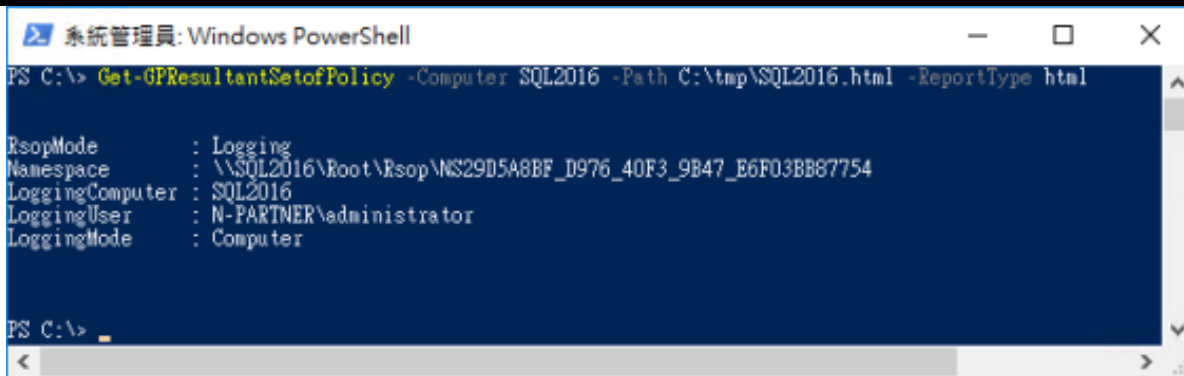
```
PS C:\> Invoke-GPUUpdate -Computer SQL2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2016 -Path C:\tmp\SQL2016.html -ReportType.html
```



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

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

|                              |           |                  |
|------------------------------|-----------|------------------|
| 群組原則結果                       |           |                  |
| N-PARTNER\SQL2016            |           |                  |
| 資料收集: 2021/10/22 下午 01:56:47 |           | 全部顯示             |
| 摘要                           |           | 顯示               |
| 電腦詳細資料                       |           | 隱藏               |
| 一般                           |           | 顯示               |
| 元件狀態                         |           | 顯示               |
| 識定                           |           | 隱藏               |
| 原則                           |           | 隱藏               |
| Windows 設定                   |           | 隱藏               |
| 安全性設定                        |           | 隱藏               |
| 帳戶原則/密碼規則                    |           | 顯示               |
| 帳戶原則/帳戶鎖定原則                  |           | 顯示               |
| 本機原則/稽核原則                    |           | 隱藏               |
| 原則                           | 設定        | 優勢 GPO           |
| 稽核帳戶登入事件                     | 成功, 失敗    | N-Partner Policy |
| 稽核帳戶管理                       | 成功, 失敗    | N-Partner Policy |
| 稽核登入事件                       | 成功, 失敗    | N-Partner Policy |
| 本機原則/安全性選項                   |           | 顯示               |
| 事件記錄檔                        |           | 隱藏               |
| 原則                           | 設定        | 優勢 GPO           |
| 應用程式記錄保持方法                   | 視需要而定     | N-Partner Policy |
| 應用程式記錄檔容量最大值                 | 204800 KB | N-Partner Policy |
| 公開金鑰原則/添設服務用戶端 - 自動註冊設定      |           | 顯示               |
| 公開金鑰原則/加密檔案系統                |           | 顯示               |
| 系統管理範本                       |           | 顯示               |
| 群組原則物件                       |           | 顯示               |
| WMI 監視器                      |           | 顯示               |
| 使用者詳細資料                      |           | 顯示               |

## 4.3.2 工作群組

### 4.3.2.1 稽核原則設定

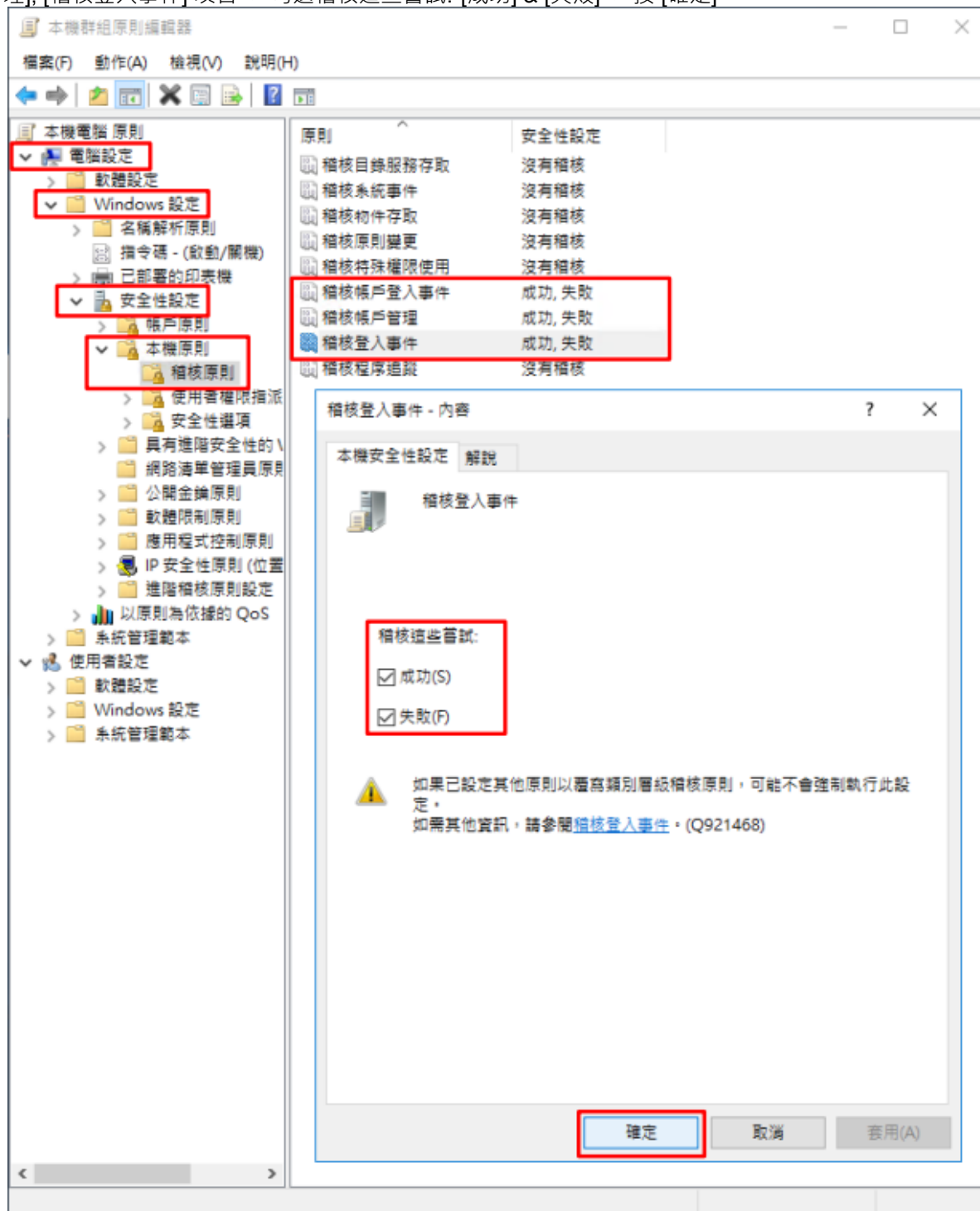
#### (1) 開啟 [本機群組原則編輯器]

點選  [搜尋] -> 輸入 [群組原則](#) -> 點選 [編輯群組原則]



## (2) 本機原則：稽核原則

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

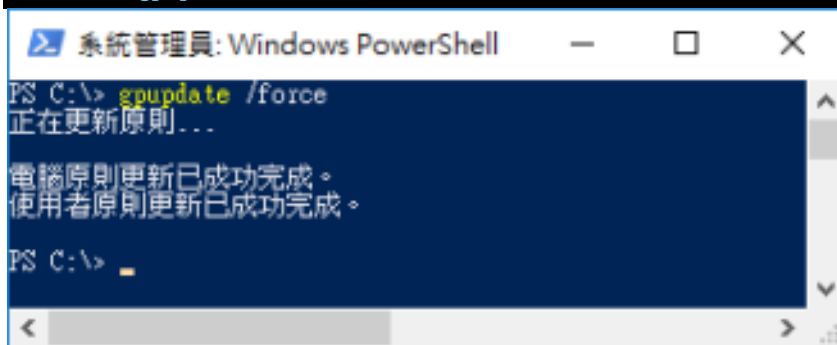


### (3) 開啟 [Windows PowerShell]



### (4) 更新群組原則

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



## (5) 查看群組原則套用情形

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

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

#### 4.3.2.2 事件檔案設定

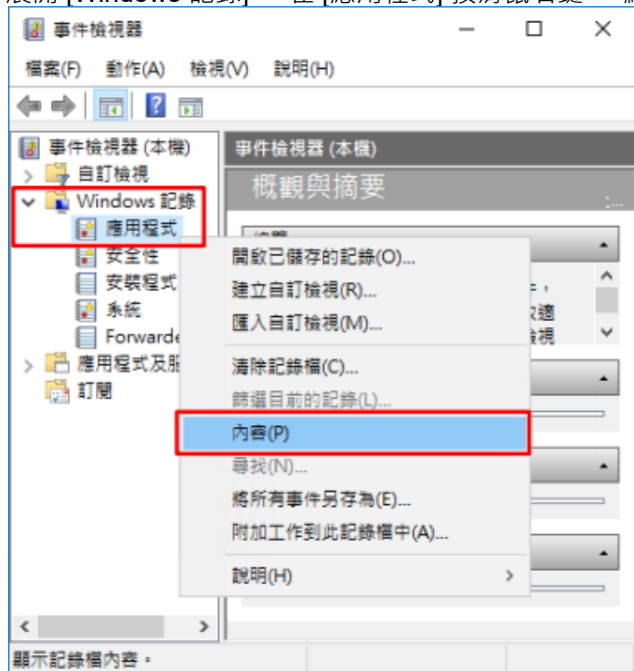
##### (1) 開啟 [檢視事件記錄檔]

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



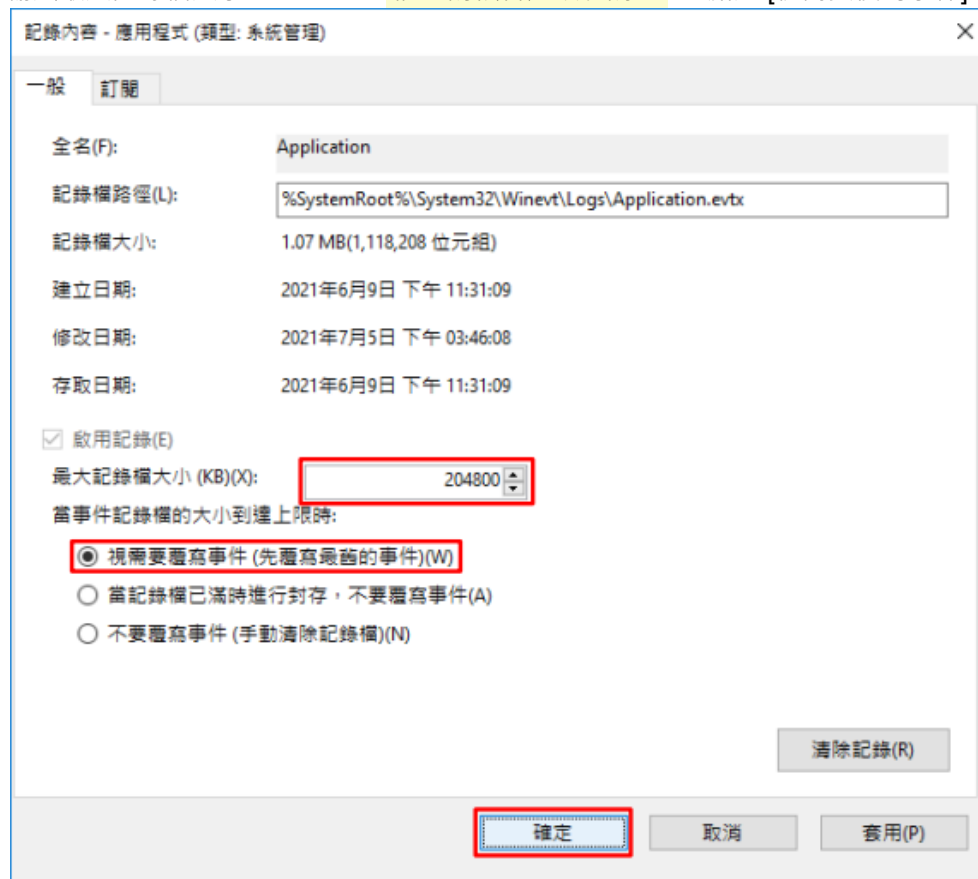
## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [應用程式] 按滑鼠右鍵 -> 點選 [內容]



## (3) 設定應用程式記錄檔

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



## 5 SQL2019

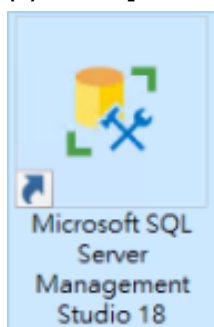
### 5.1 稽核登入

啟用登入稽核，以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。

以下分別為圖形介面和指令介面設定方式。

#### 5.1.1 使用圖形介面方式設定

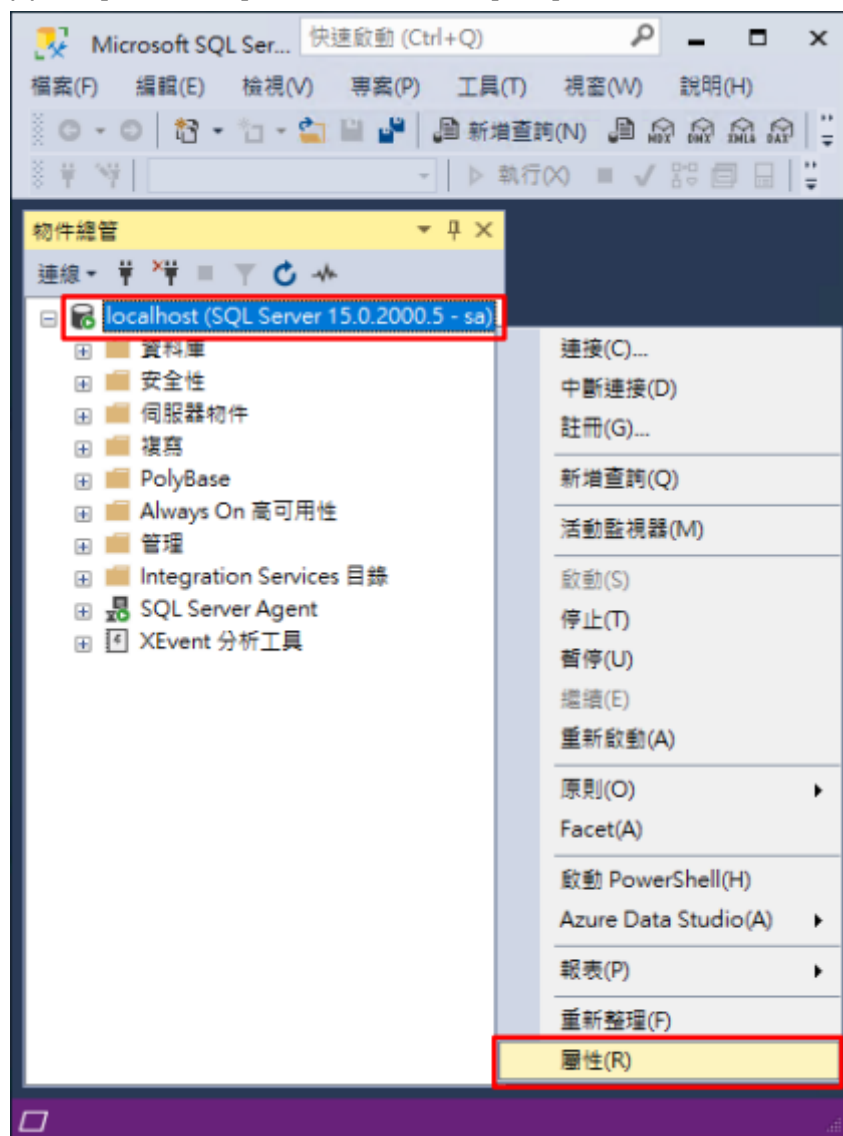
##### (1) 開啟 [Microsoft SQL Server Management Studio]



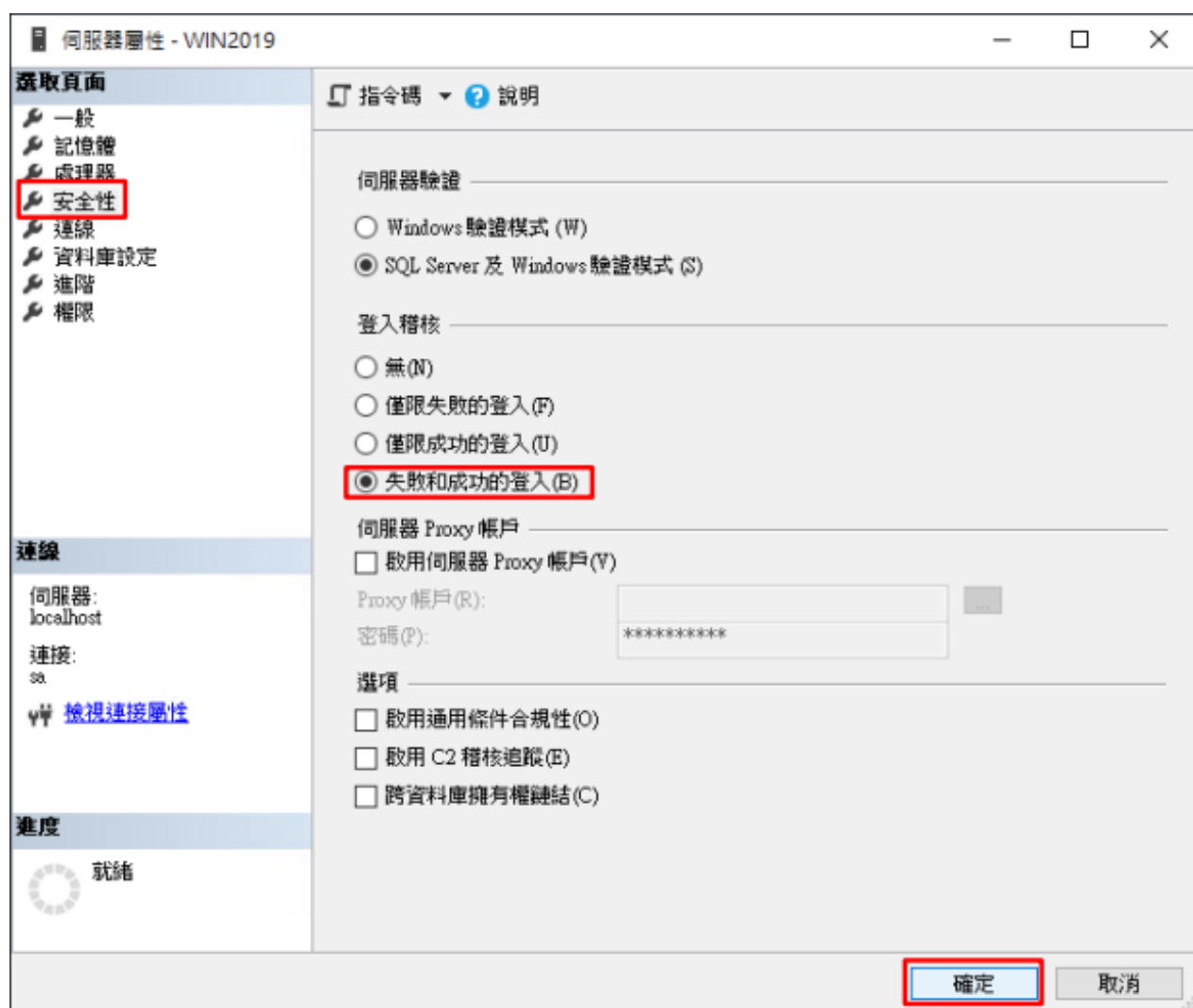
##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

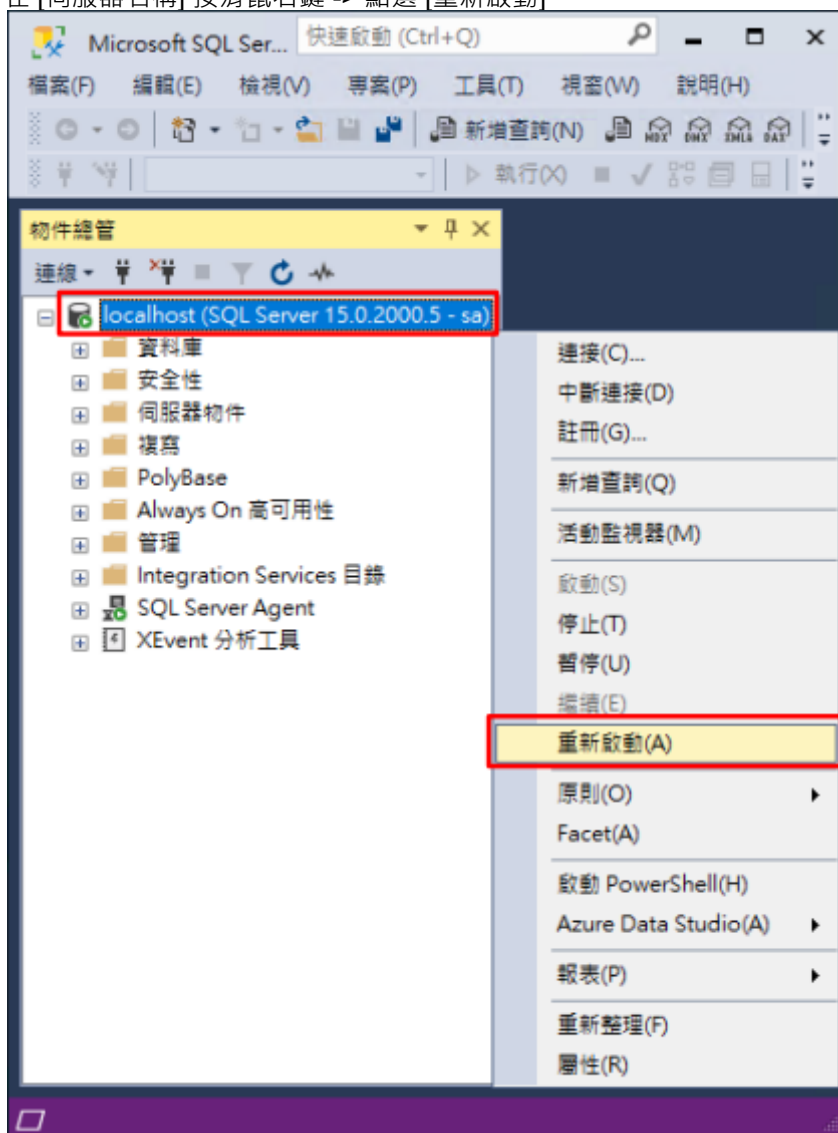


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]



(5) 重新啟動 MS SQL SERVER 服務

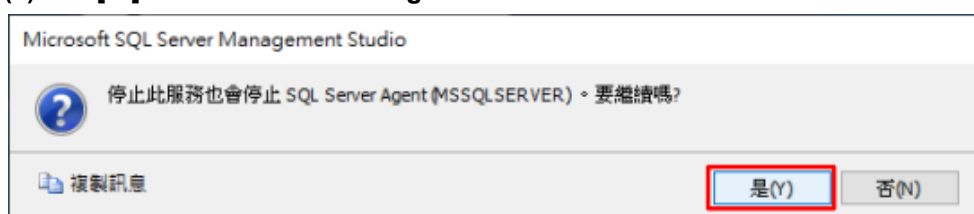
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務

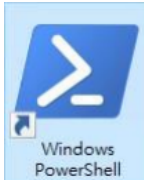


(7) 按 [是] 停止 SQL SERVER Agent 服務



## 5.1.2 使用指令介面方式設定

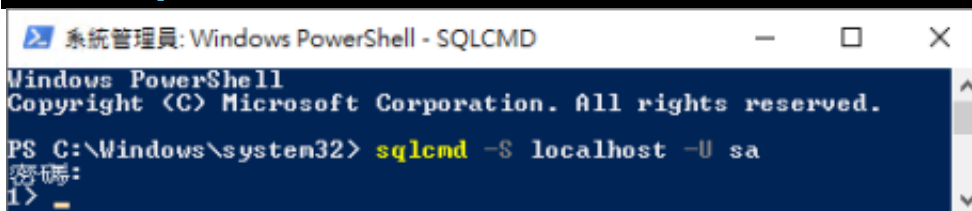
### (1) 開啟 [Windows Powershell]



### (2) 分別為 sa 或 Windows 帳號登入方式

#### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```



Options:

-S [protocol:]server[instance\_name][,port]

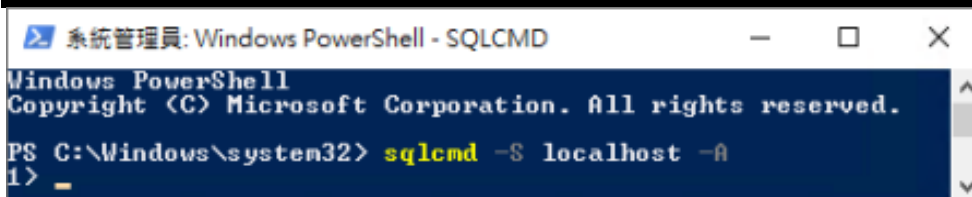
-U login\_id

-P password

-A dedicated administrator connection

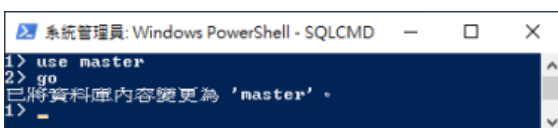
#### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



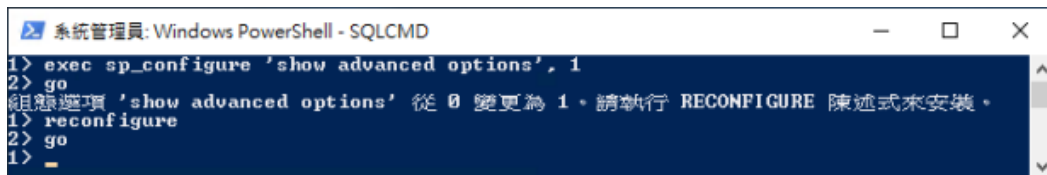
### (3) 切換資料庫

```
1 > use master
2 > go
```



#### (4) 使用 sp\_configure 列出進階選項

```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
系統管理員: Windows PowerShell - SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
組態選項 'show advanced options' 從 0 變更為 1。請執行 RECONFIGURE 陳述式來安裝。
1> reconfigure
2> go
1>
```

#### (5) 啟用失敗和成功的登入記錄

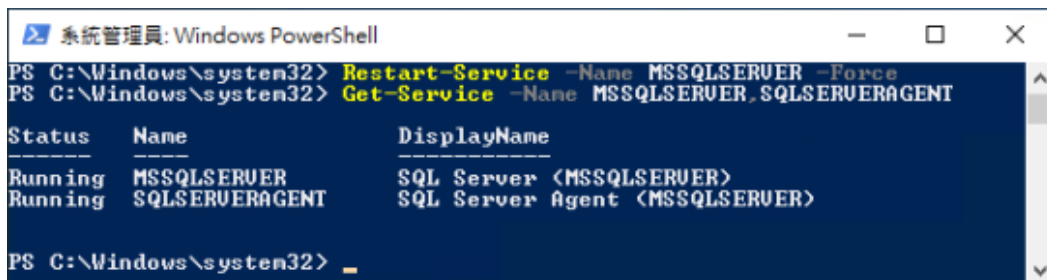
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
1 > quit
```



```
系統管理員: Windows PowerShell
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go
<0 個受影響的資料列>
1> quit
PS C:\Users\Administrator>
```

#### (6) 重新啟動 MS SQL SERVER 服務和確認 MS SQL SERVER 服務狀態

```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT
```



```
系統管理員: Windows PowerShell
PS C:\Windows\system32> Restart-Service -Name MSSQLSERVER -Force
PS C:\Windows\system32> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT

Status      Name                DisplayName
-----
Running     MSSQLSERVER         SQL Server (MSSQLSERVER)
Running     SQLSERVERAGENT       SQL Server Agent (MSSQLSERVER)

PS C:\Windows\system32>
```

## 5.2 設定稽核

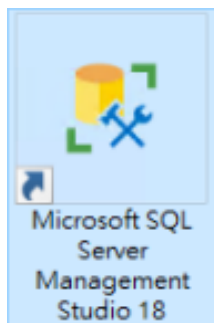
### 5.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

#### 5.2.1.1 使用圖形介面方式設定

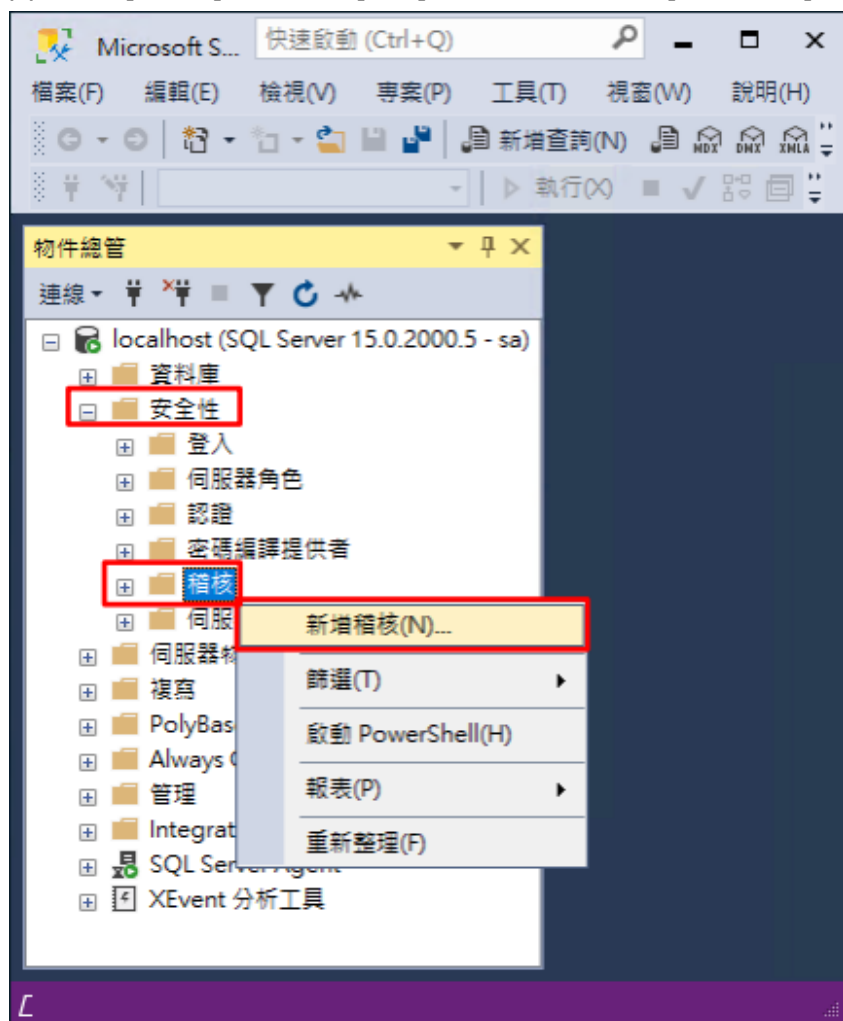
##### (1) 開啟 [Microsoft SQL Server Management Studio]



##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

建立稽核

就緒

選取頁面

一般  
篩選

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒為單位) (Q): 1000

於稽核記錄失敗時:

☒ 繼續(C)  
☐ 令操作失敗(F)  
☐ 關閉伺服器(S)

稽核目的地(D): 應用程式記錄檔

路徑(P):

稽核檔案數目上限:

☒ 最大換用檔案(O):  
☐ 最大檔案數目(X):

檔案數目(B): 2147483647

檔案大小上限 (Z): 0

☒ MB(M) ☐ GB(G) ☐ TB(T)

☒ 無限制(U)  
☒ 無限制(L)

☐ 保留磁碟空間(R)

連線

localhost [sa]

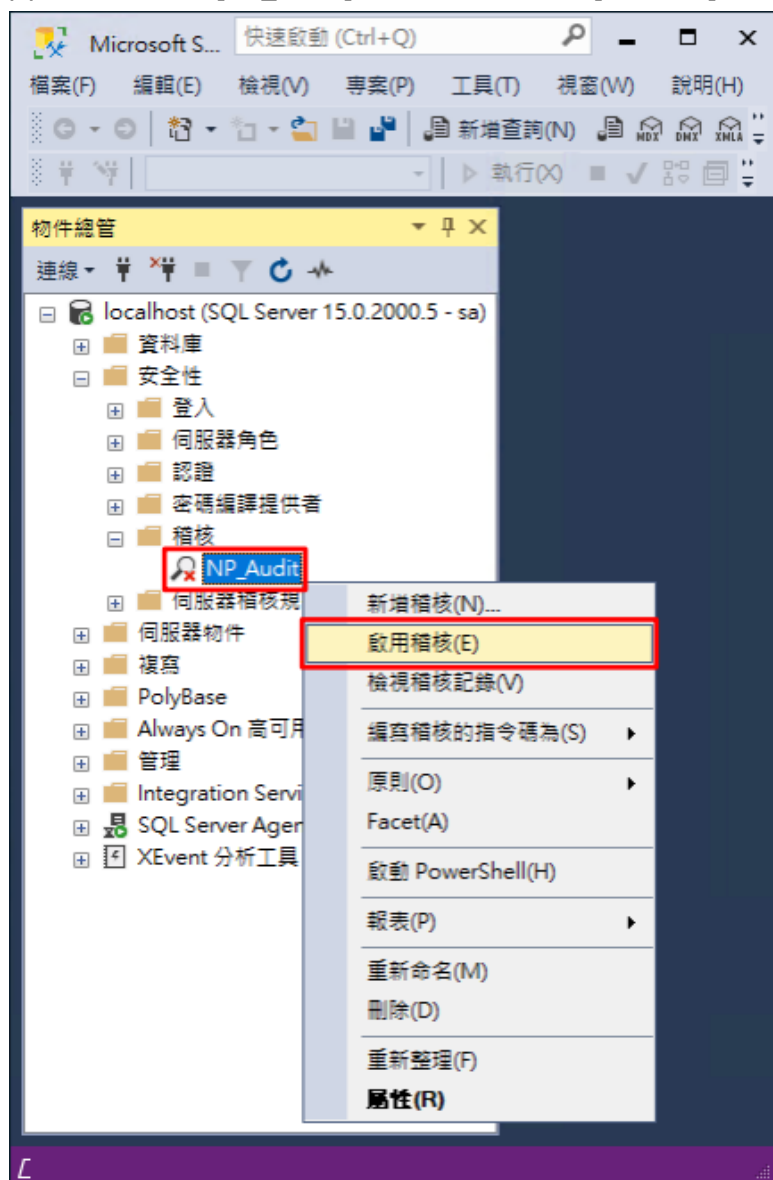
檢視連線屬性

進度

就緒

確定 取消 說明

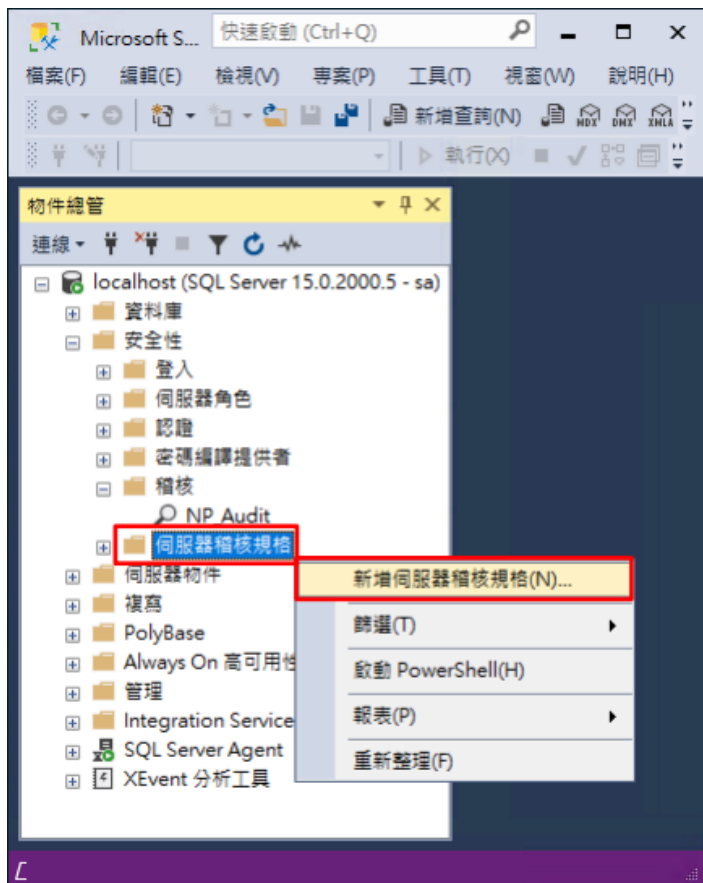
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



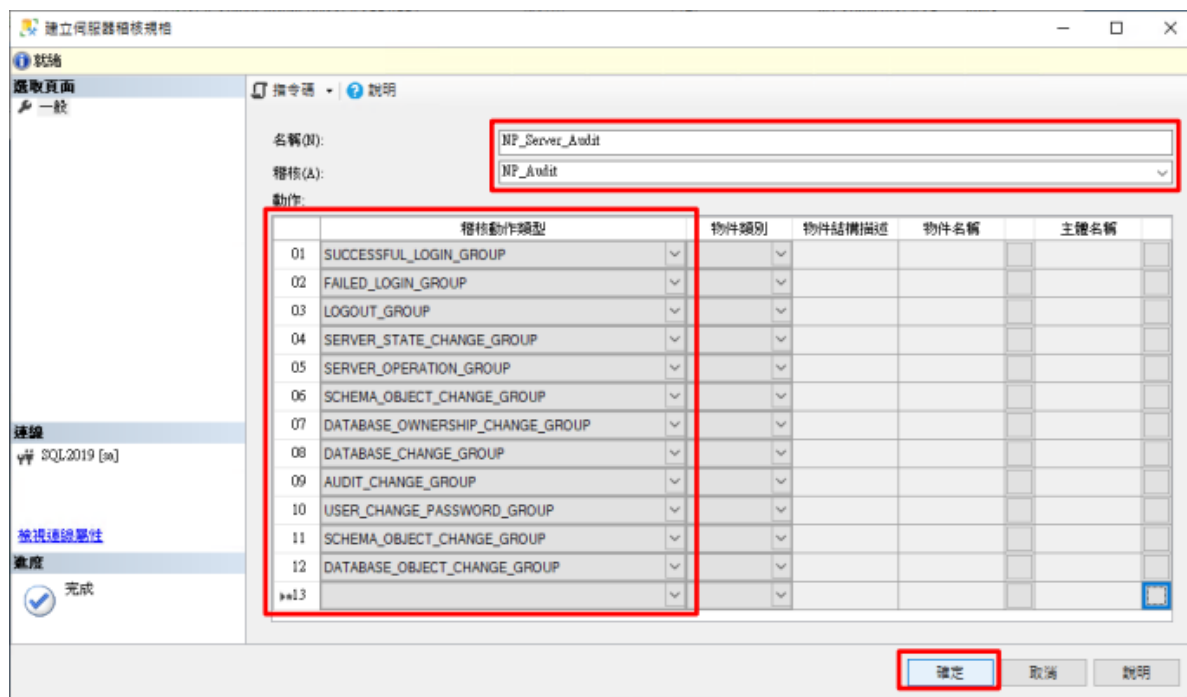
(6) 按 [關閉]



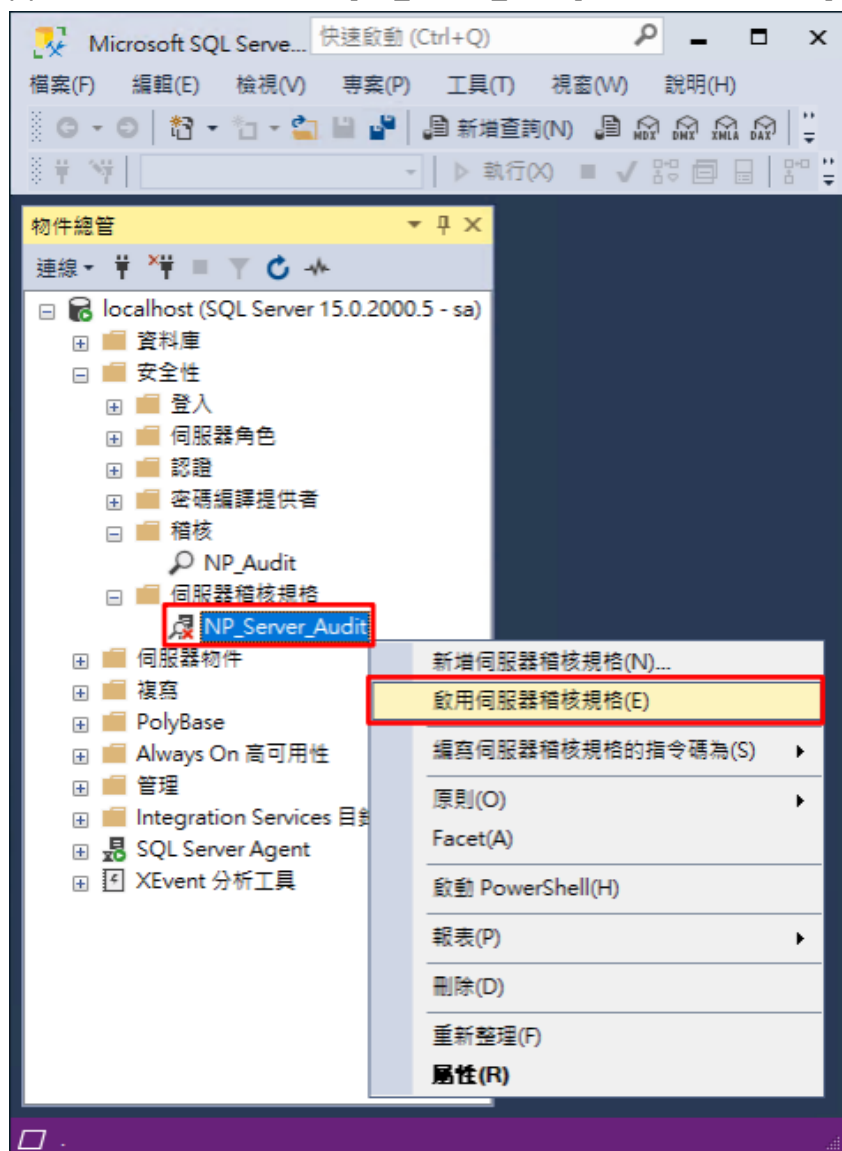
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



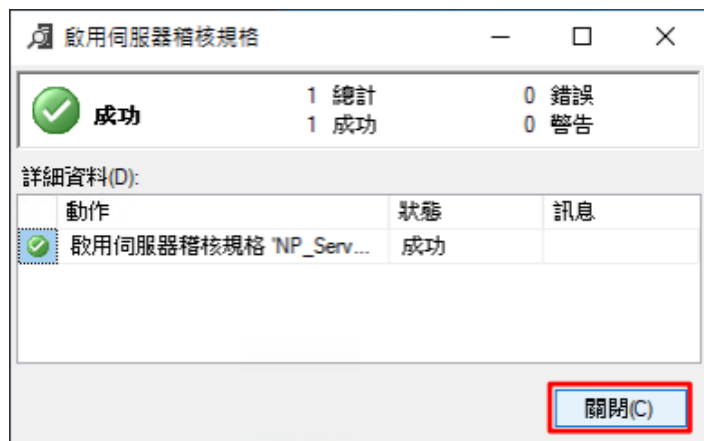
(8) 輸入名稱: `NP_Server_Audit` -> 選擇稽核: `[NP_Audit]` 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在伺服器稽核規格名稱: [NP\_Server\_Audit] 按滑鼠右鍵 -> 點選 [啟用伺服器稽核規格]



(10) 按 [關閉]



### 5.2.1.2 使用指令介面方式設定

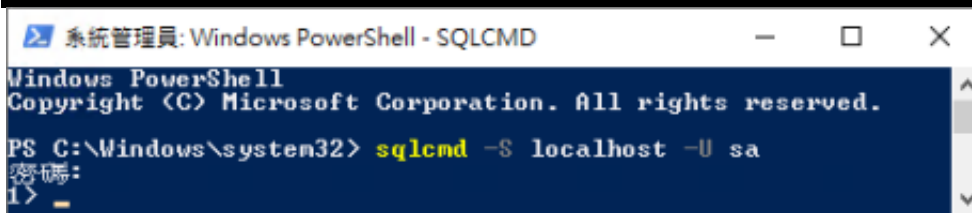
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

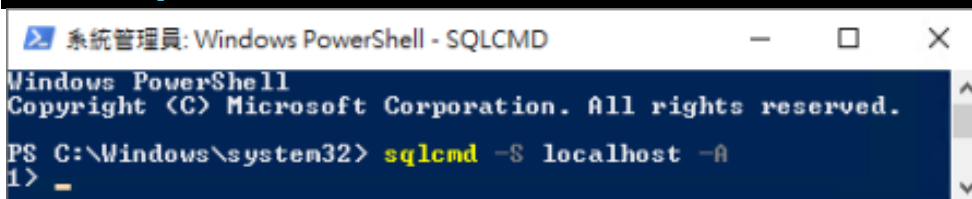


Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

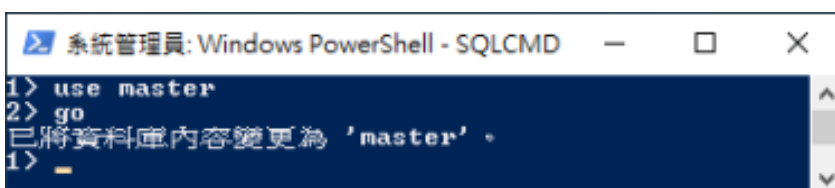
##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



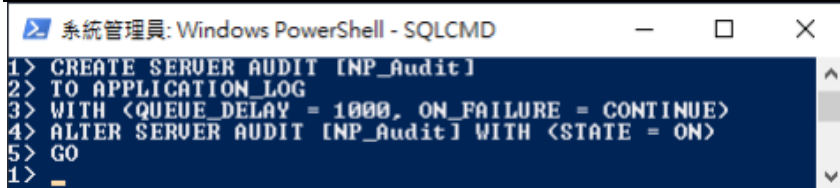
#### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

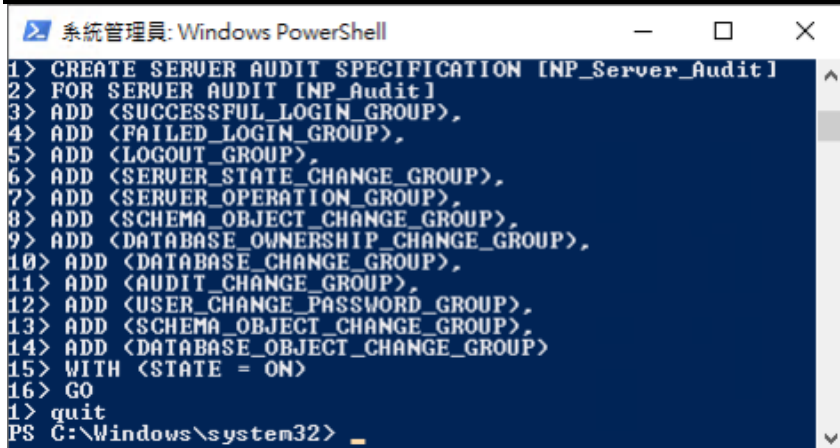


```
系統管理員: Windows PowerShell - SQLCMD
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1>
```

紅色文字部位請輸入稽核名稱

(5) 設定稽核伺服器，ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP),
12 > ADD (USER_CHANGE_PASSWORD_GROUP),
13 > ADD (SERVER_OBJECT_CHANGE_GROUP),
14 > ADD (DATABASE_OBJECT_CHANGE_GROUP)
15 > WITH (STATE = ON)
16 > GO
1 > quit
```



```
系統管理員: Windows PowerShell
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP),
13> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
14> ADD (DATABASE_OBJECT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\Windows\system32>
```

紅色文字部位請輸入伺服器稽核規格名稱

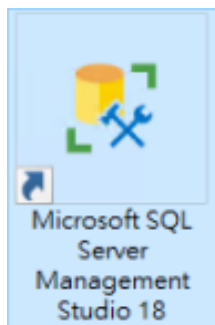
## 5.2.2 稽核資料庫層級

啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

以下分別為圖形介面和指令介面設定方式。

### 5.2.2.1 使用圖形介面方式設定

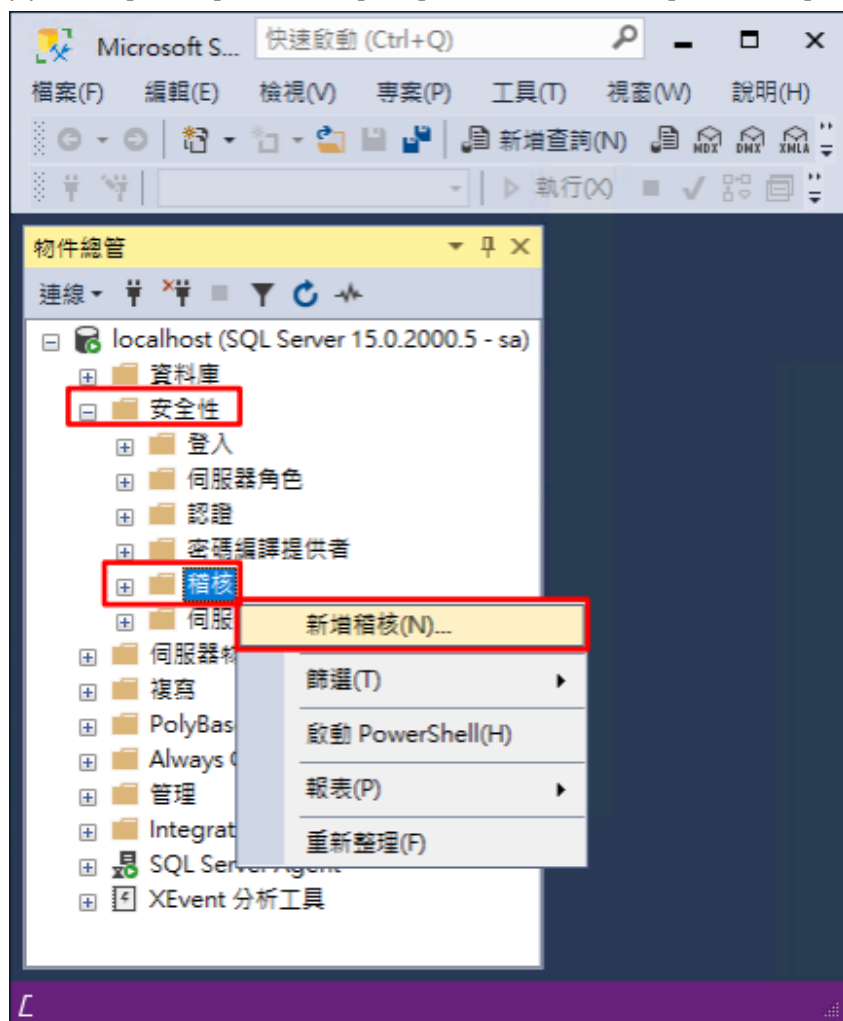
#### (1) 開啟 [Microsoft SQL Server Management Studio]



#### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: **[繼續]** -> 選擇稽核目的地: **[應用程式記錄檔]**  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 **[確定]**

建立稽核

就緒

選取頁面

一般  
篩選

指令碼 | 說明

稽核名稱(N): NP\_Audit

佇列延遲 (以毫秒為單位) (Q): 1000

於稽核記錄失敗時:

☒ 繼續(C)  
☐ 令操作失敗(F)  
☐ 關閉伺服器(S)

稽核目的地(D): 應用程式記錄檔

路徑(P):

稽核檔案數目上限:

☒ 最大換用檔案(O):  
☐ 最大檔案數目(X):

檔案數目(B): 2147483647

檔案大小上限 (Z): 0

☒ MB(M) ☐ GB(G) ☐ TB(T)

☒ 無限制(L)

☐ 保留磁碟空間(R)

連線

localhost [sa]

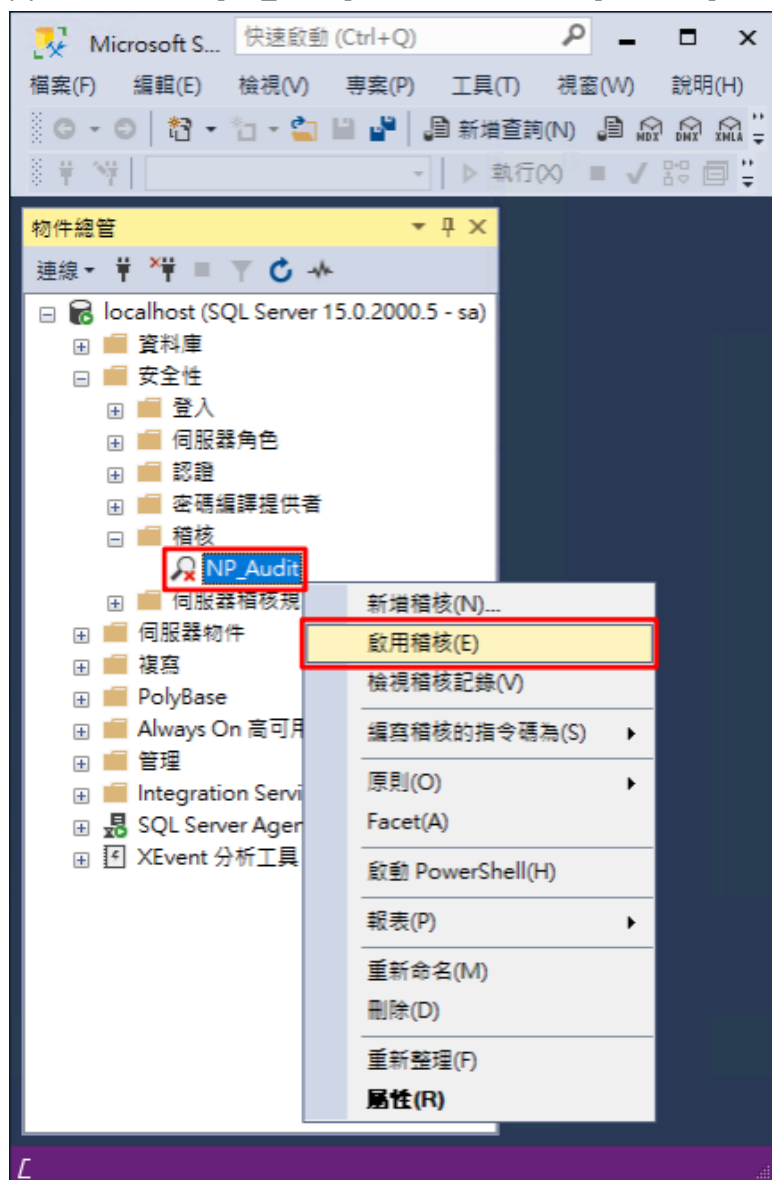
檢視連線屬性

進度

就緒

確定 取消 說明

(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



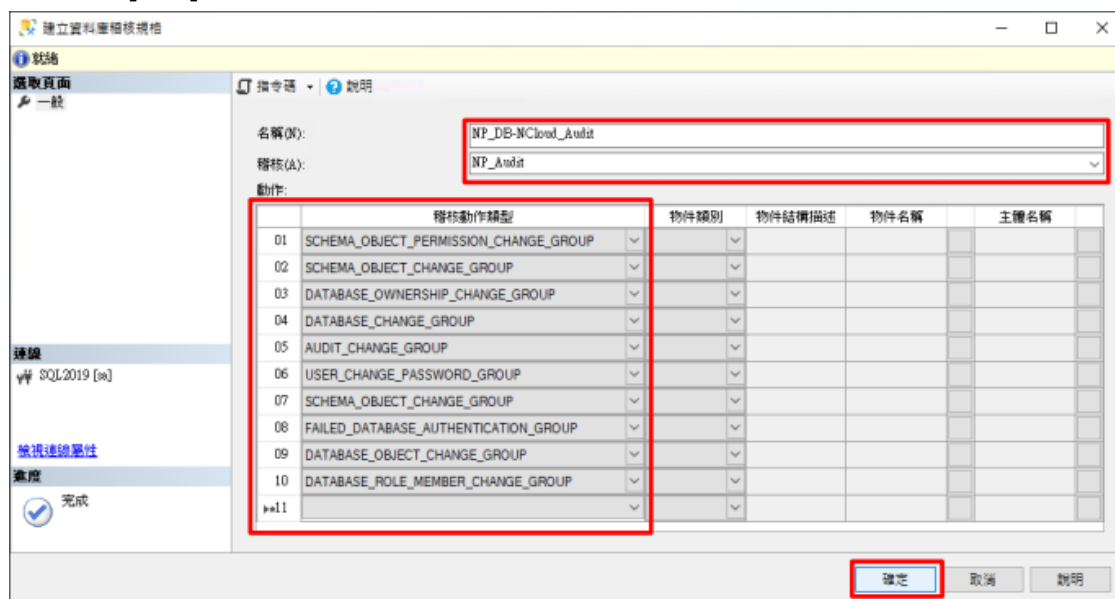
(6) 按 [關閉]



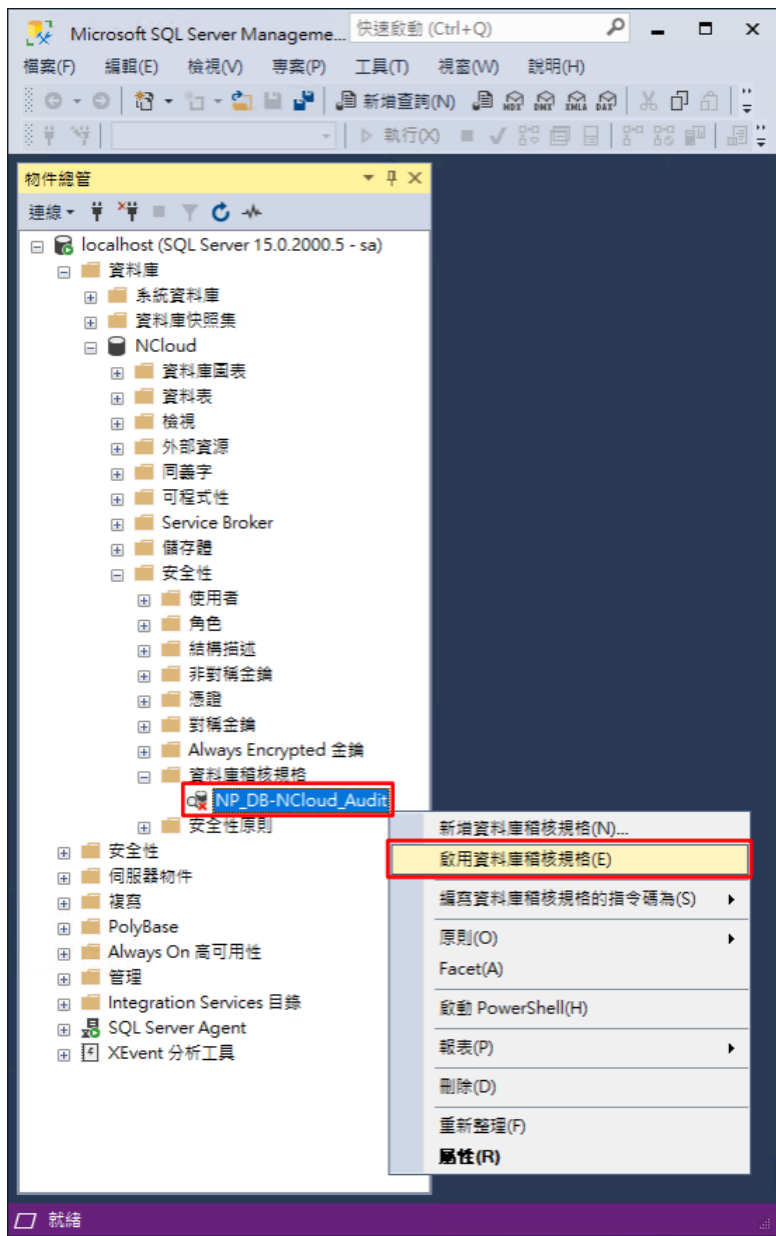
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



(8) 輸入稽核名稱: NP\_DB-NCloud\_Audit -> 選擇稽核: [NP\_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在資料庫稽核規格名稱: [NP\_DB-NCloud\_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10) 按 [關閉]



### 5.2.2.2 使用指令介面方式設定

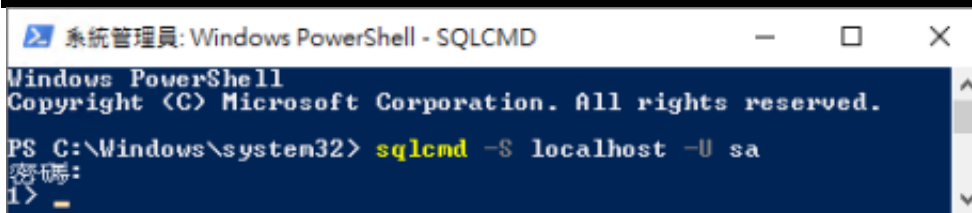
#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

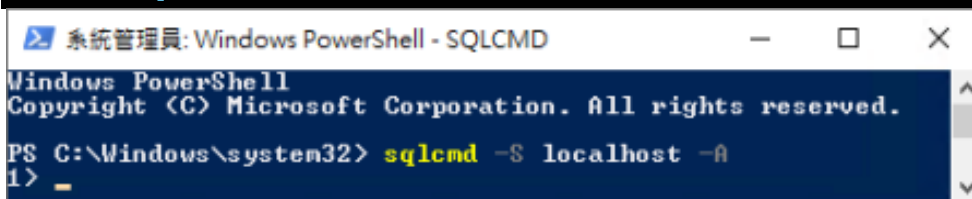


Options:

- S [protocol:]server[instance\_name][,port]
- U login\_id
- P password
- A dedicated administrator connection

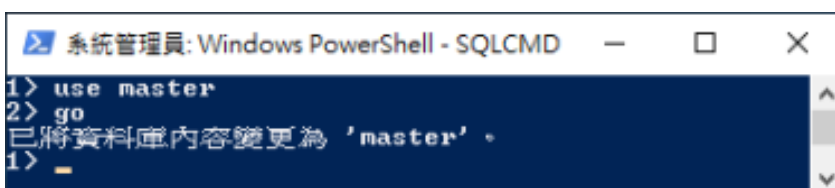
##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```



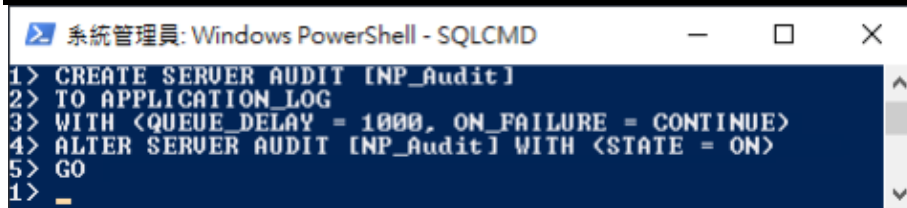
#### (3) 切換資料庫

```
1 > use master
2 > go
```



(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [NP_Audit]  
2 > TO APPLICATION_LOG  
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)  
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)  
5 > GO
```



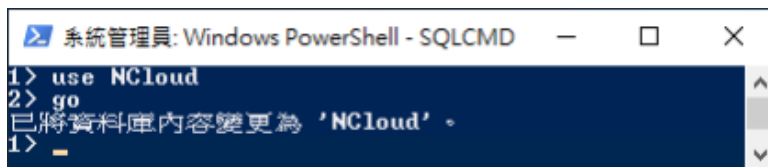
系統管理員: Windows PowerShell - SQLCMD

```
1> CREATE SERVER AUDIT [NP_Audit]  
2> TO APPLICATION_LOG  
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)  
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)  
5> GO  
1> _
```

紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例：NCloud

```
1 > use NCloud  
2 > go
```



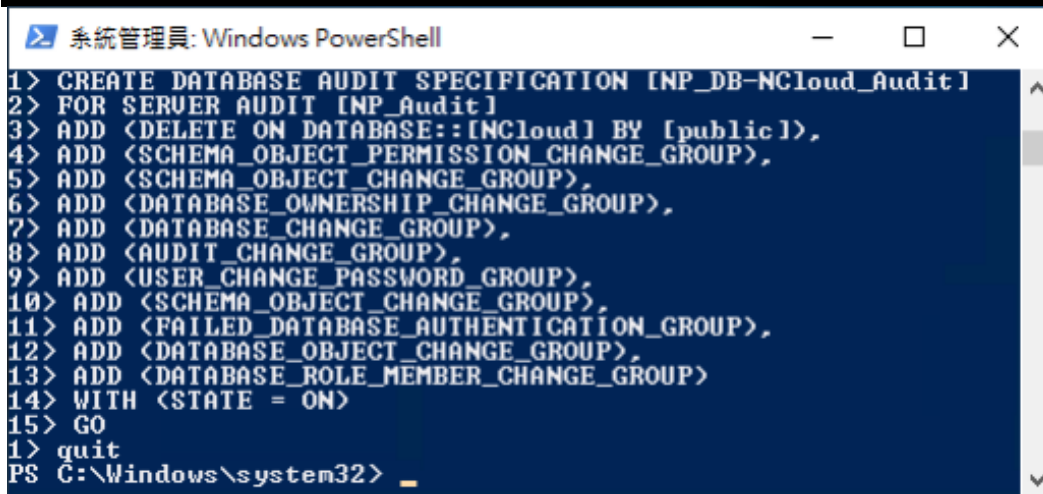
系統管理員: Windows PowerShell - SQLCMD

```
1> use NCloud  
2> go  
已將資料庫內容變更為 'NCloud'。  
1> _
```

紅色文字部位請輸入稽核資料庫名稱

(6) 設定稽核 NCloud(範例) 資料庫・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command prompt displays the same SQL commands as the previous block, with the output "PS C:\Windows\system32> \_" at the bottom.

紅色文字部位請輸入資料庫稽核規格名稱

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

紅色文字部位請輸入稽核資料庫名稱

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

## 5.3 事件記錄檔設定

此為選項設定。

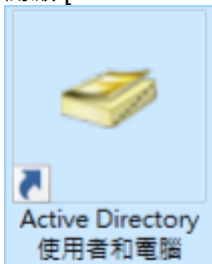
以下分別為網域和工作群組設定方式。

### 5.3.1 網域

#### 5.3.1.1 組織單位設定

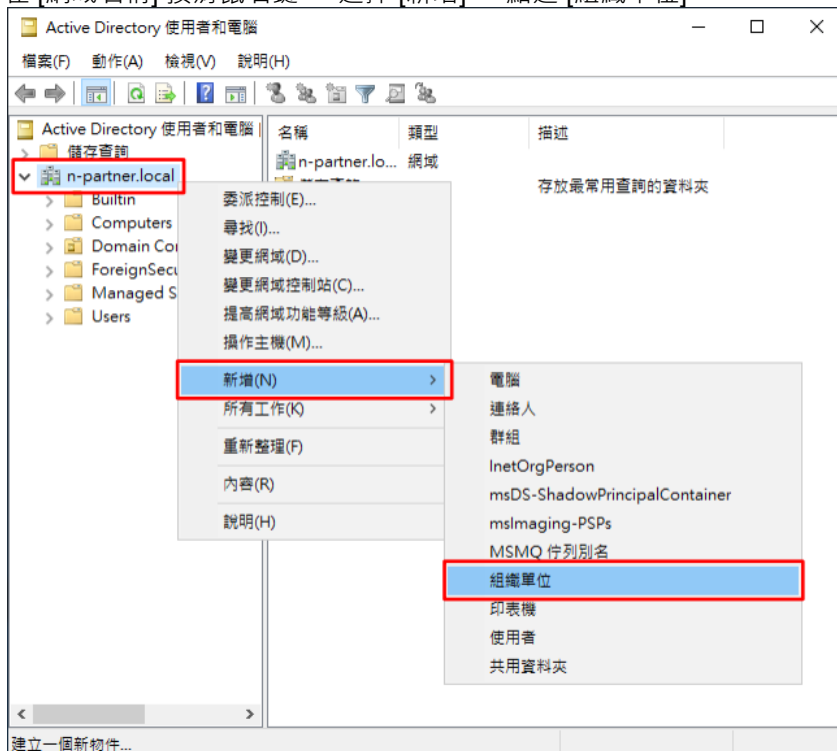
##### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



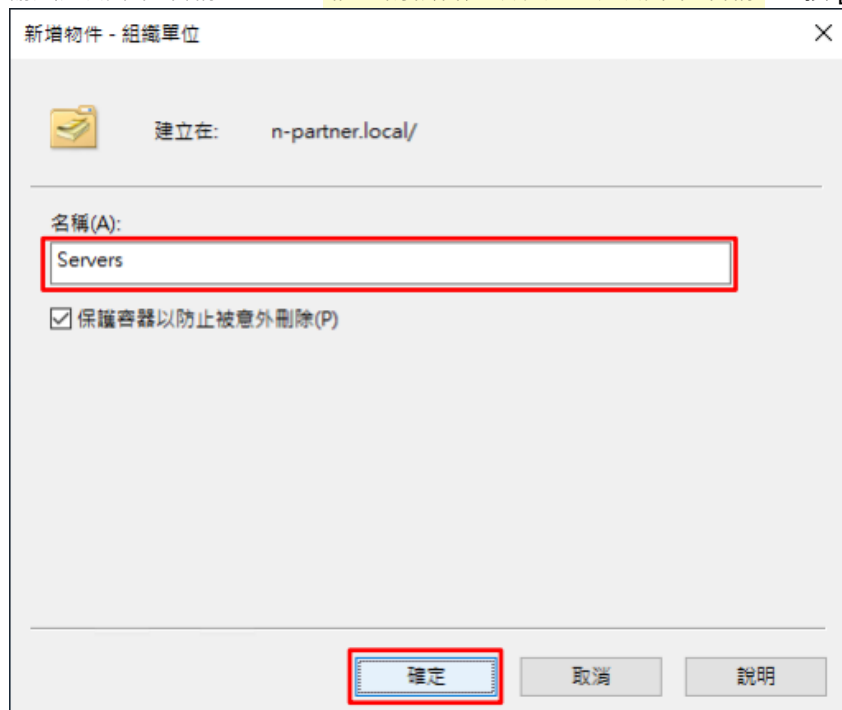
##### (2) 新增組織單位

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



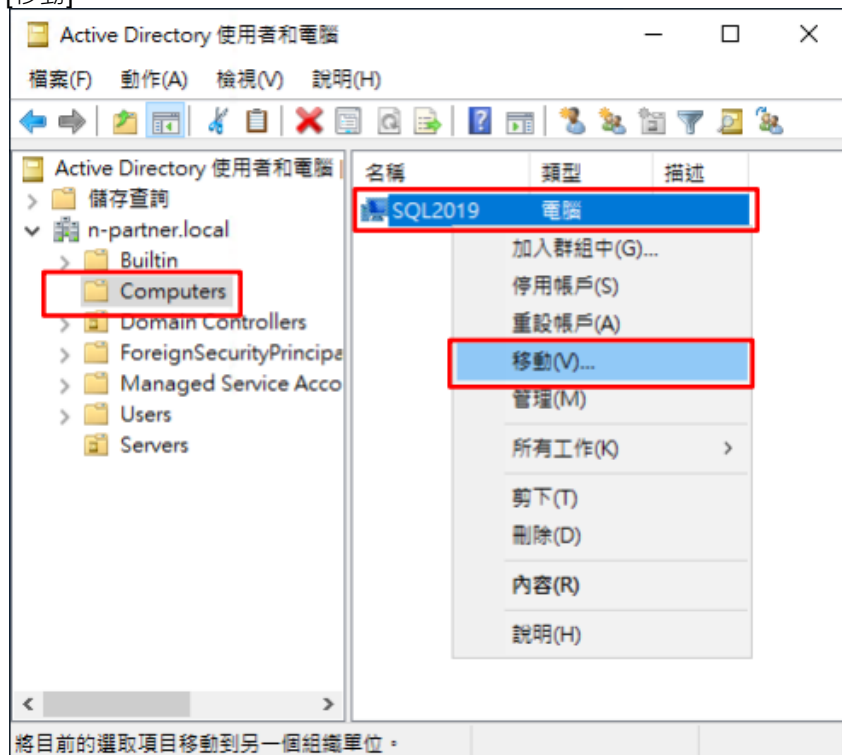
### (3) 輸入組織單位名稱

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



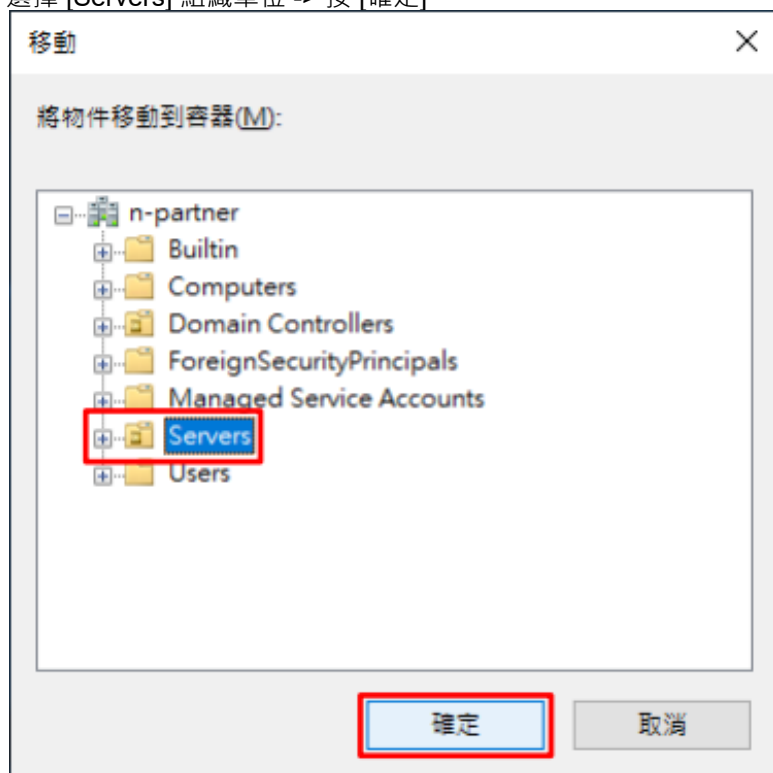
### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL 2019] 伺服器, 按滑鼠右鍵, 註：請依客戶環境選擇 MS SQL Server 主機 -> 點選 [移動]



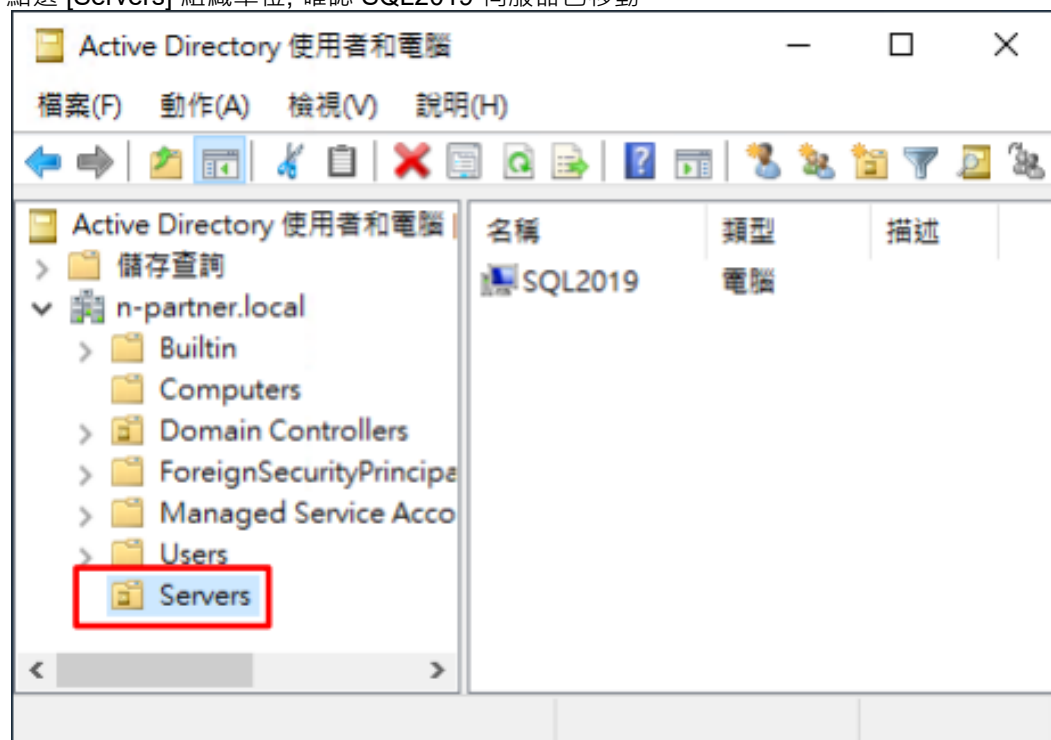
## (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



## (6) 確認伺服器已移動至新的組織單位

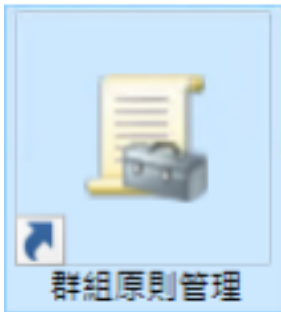
點選 [Servers] 組織單位, 確認 SQL2019 伺服器已移動。



### 5.3.1.2 群組原則設定

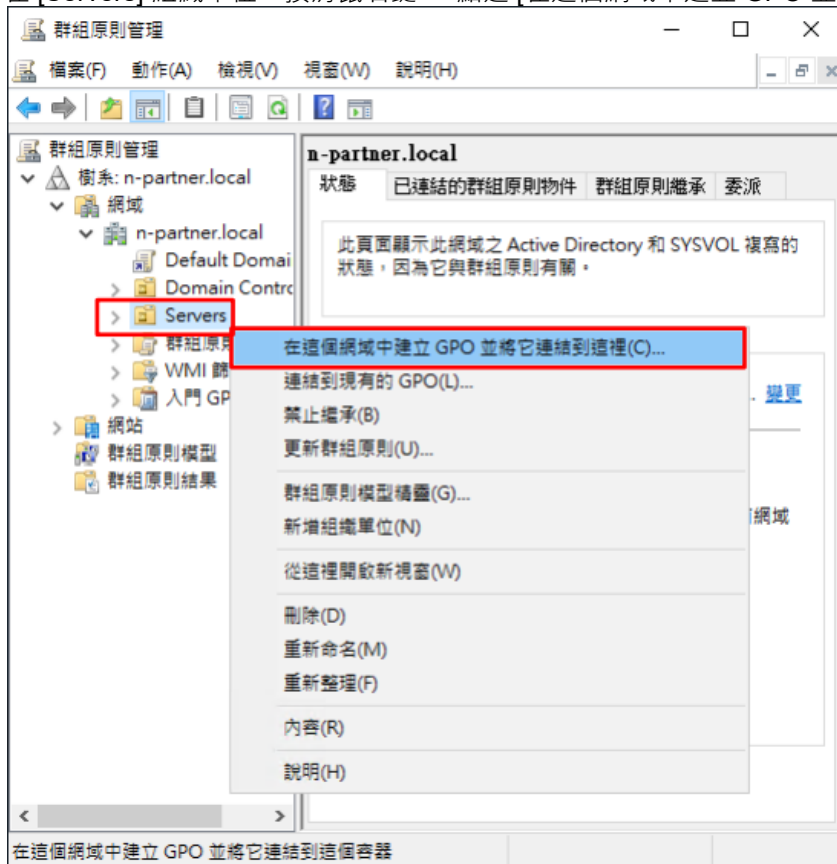
#### (1) 開啟群組原則管理

開啟 [群組原則管理]



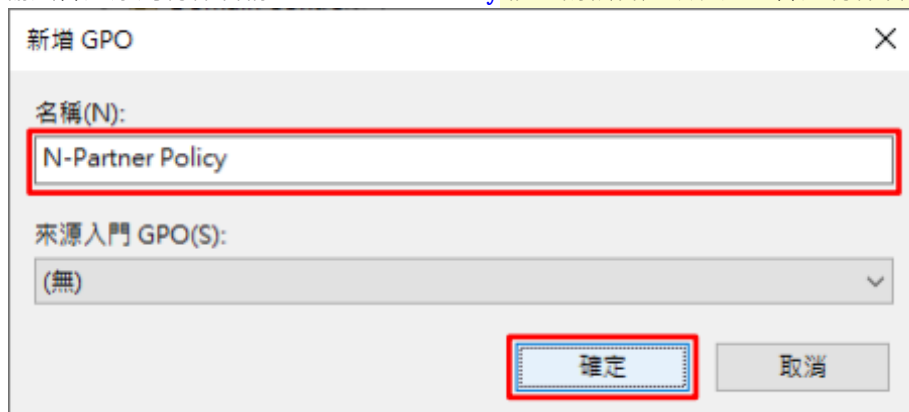
#### (2) 在 Servers 組織單位，新增群組原則物件

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



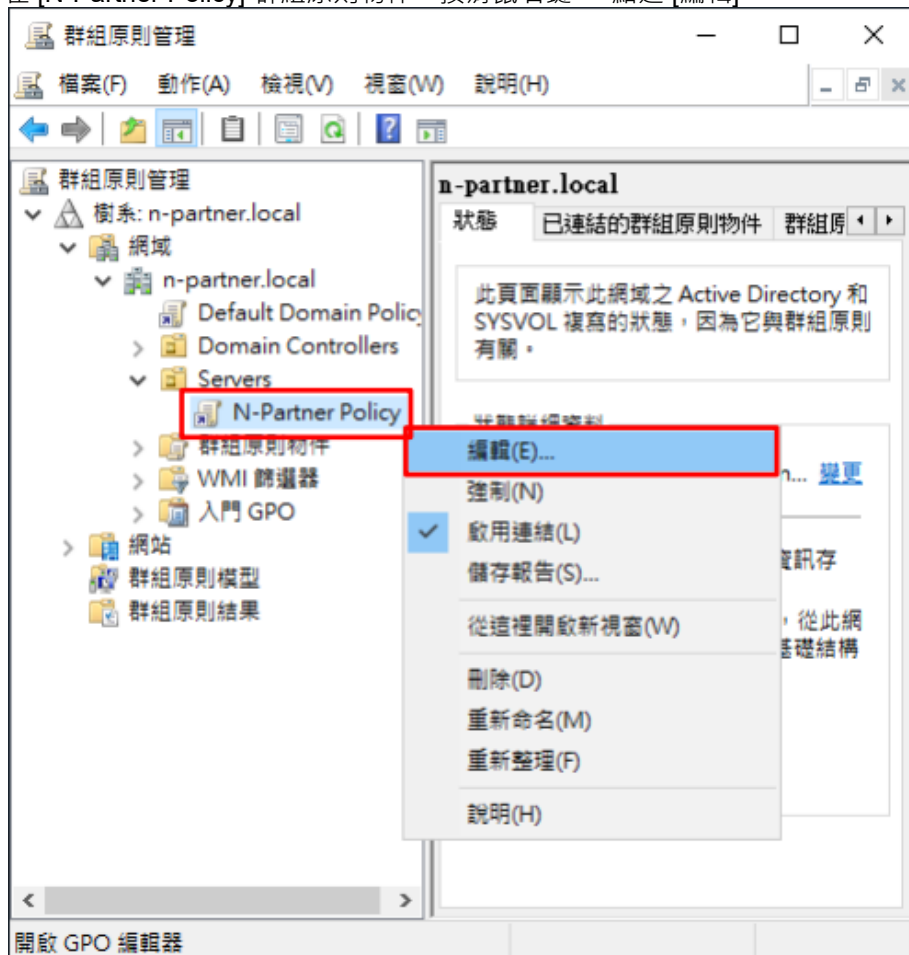
### (3) 輸入群組原則物件名稱

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



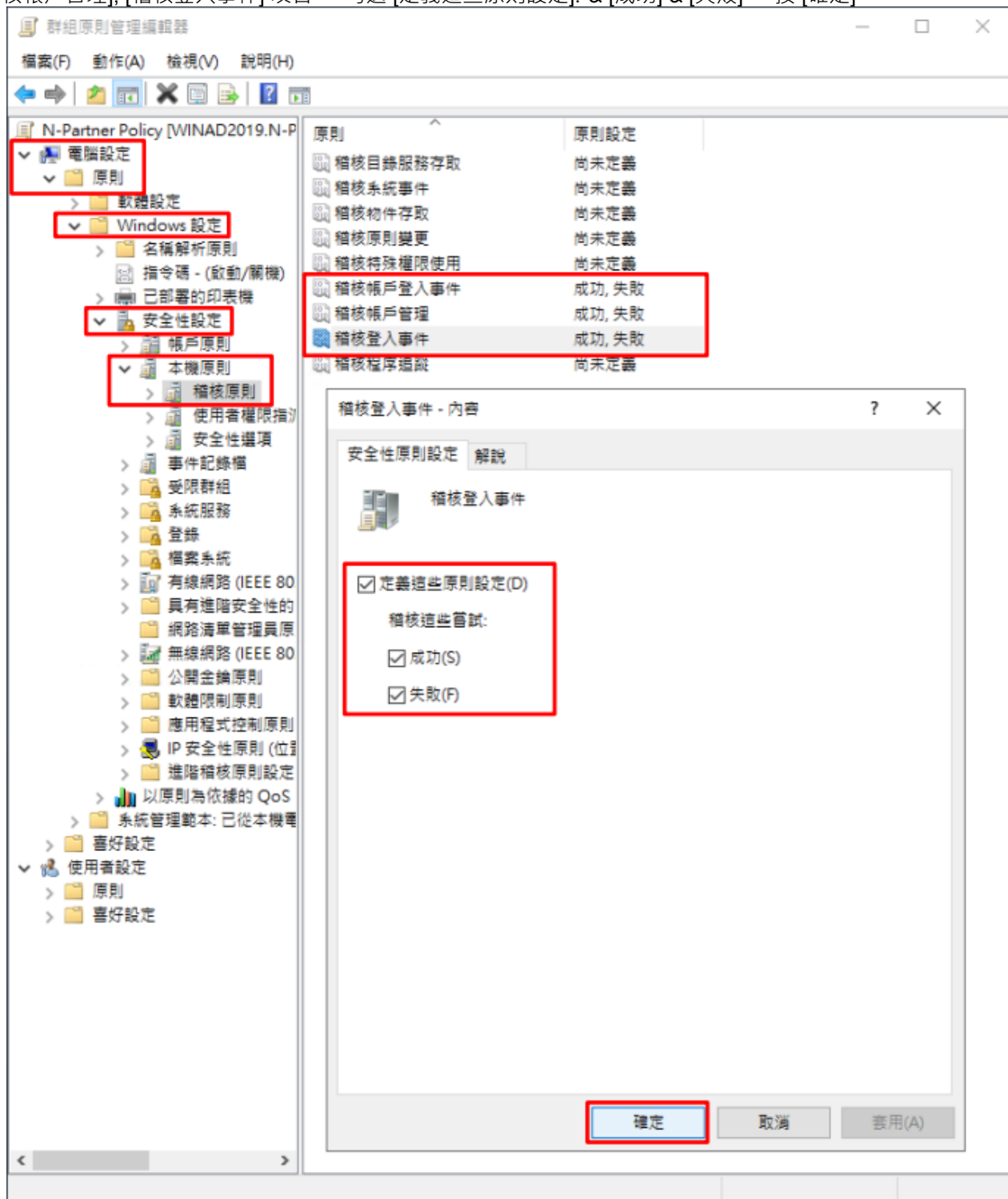
### (4) 編輯群組原則物件

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



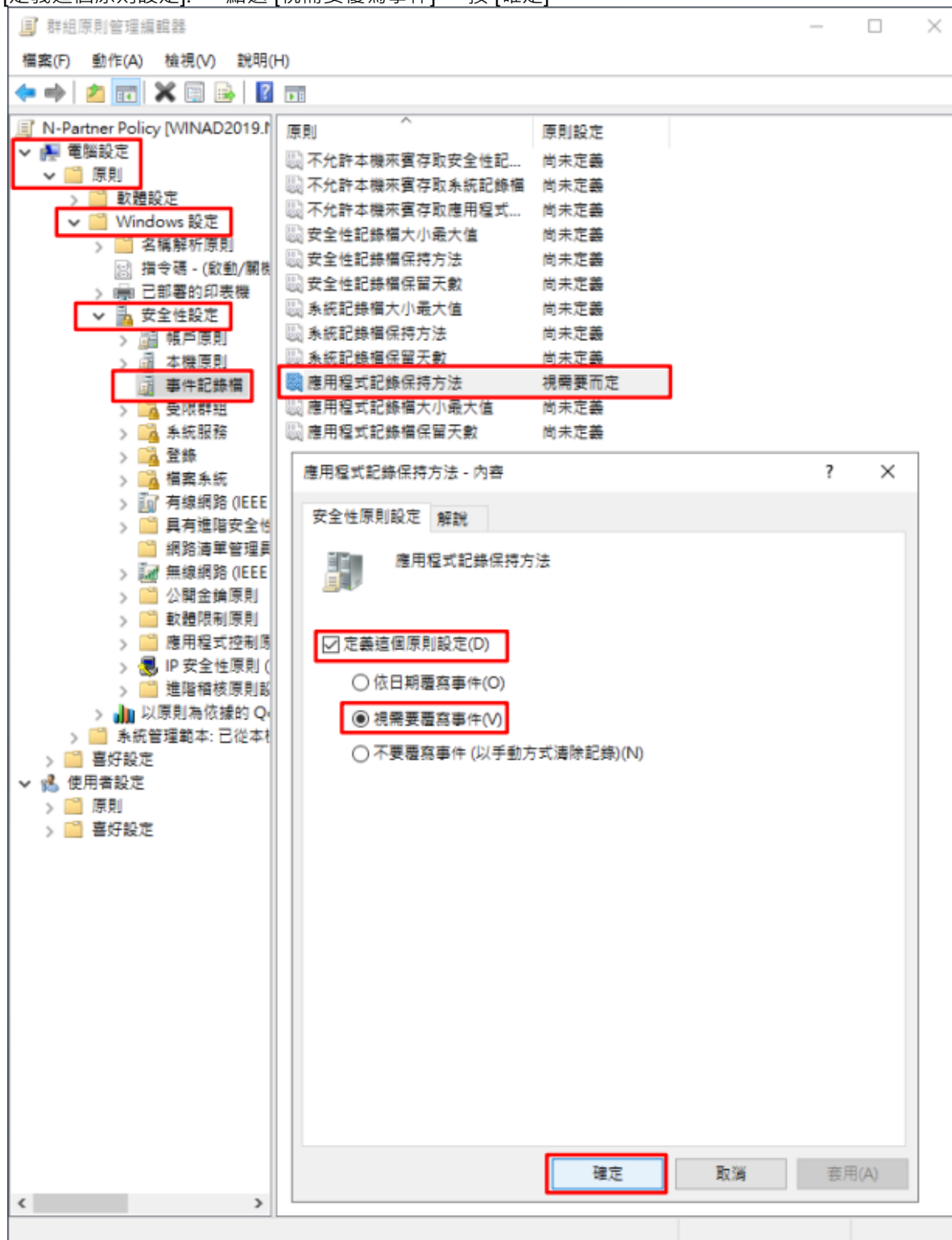
## (5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



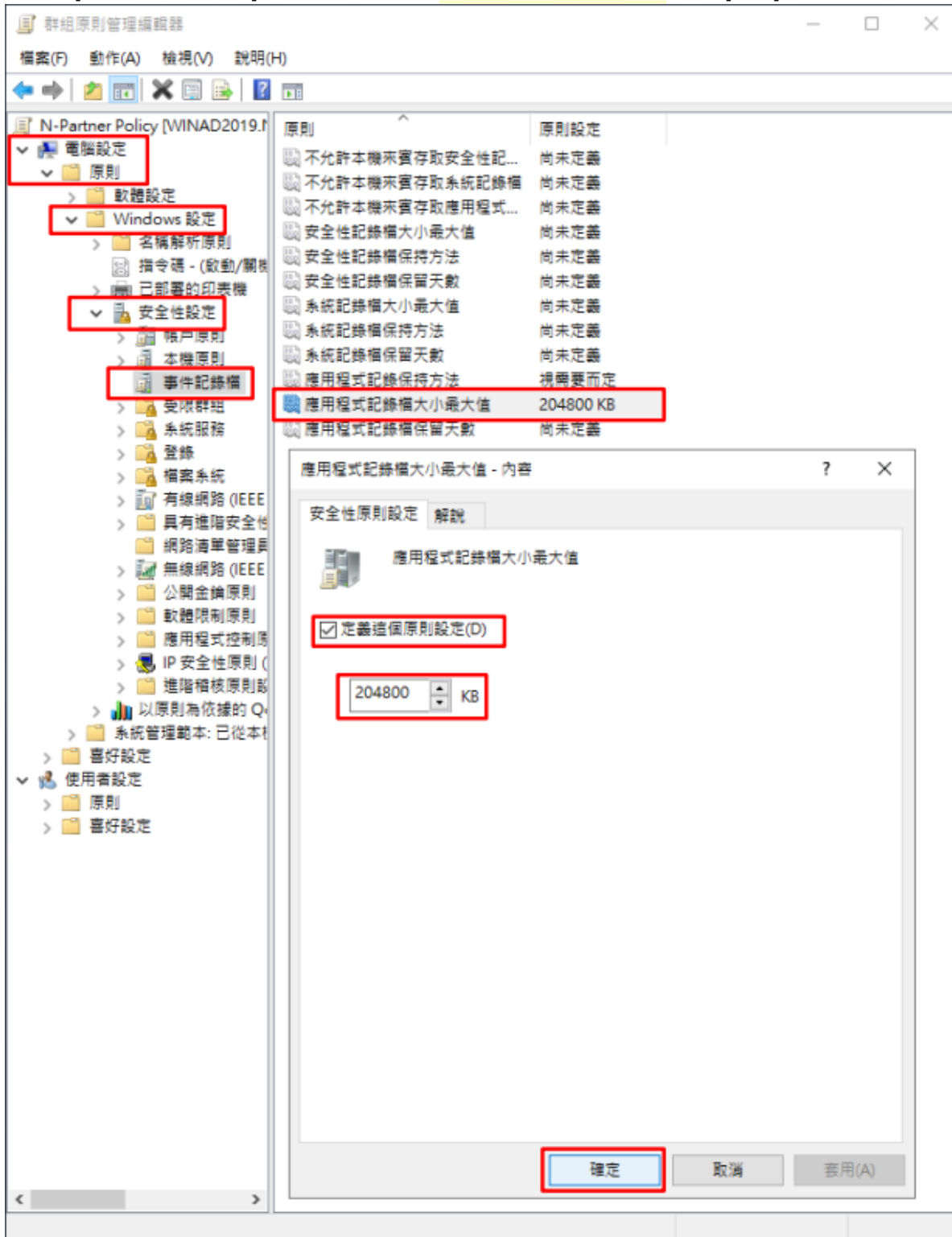
## (6) 事件記錄：應用程式記錄保持方法

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



## (7) 事件記錄：應用程式記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄檔大小最大值] 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 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

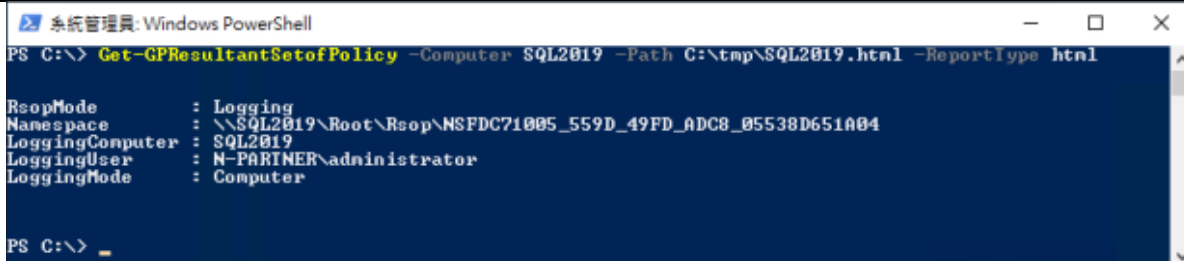
```
PS C:\> Invoke-GPUUpdate -Computer SQL2019 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2019 -Path C:\tmp\SQL2019.html -ReportType.html
```



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

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

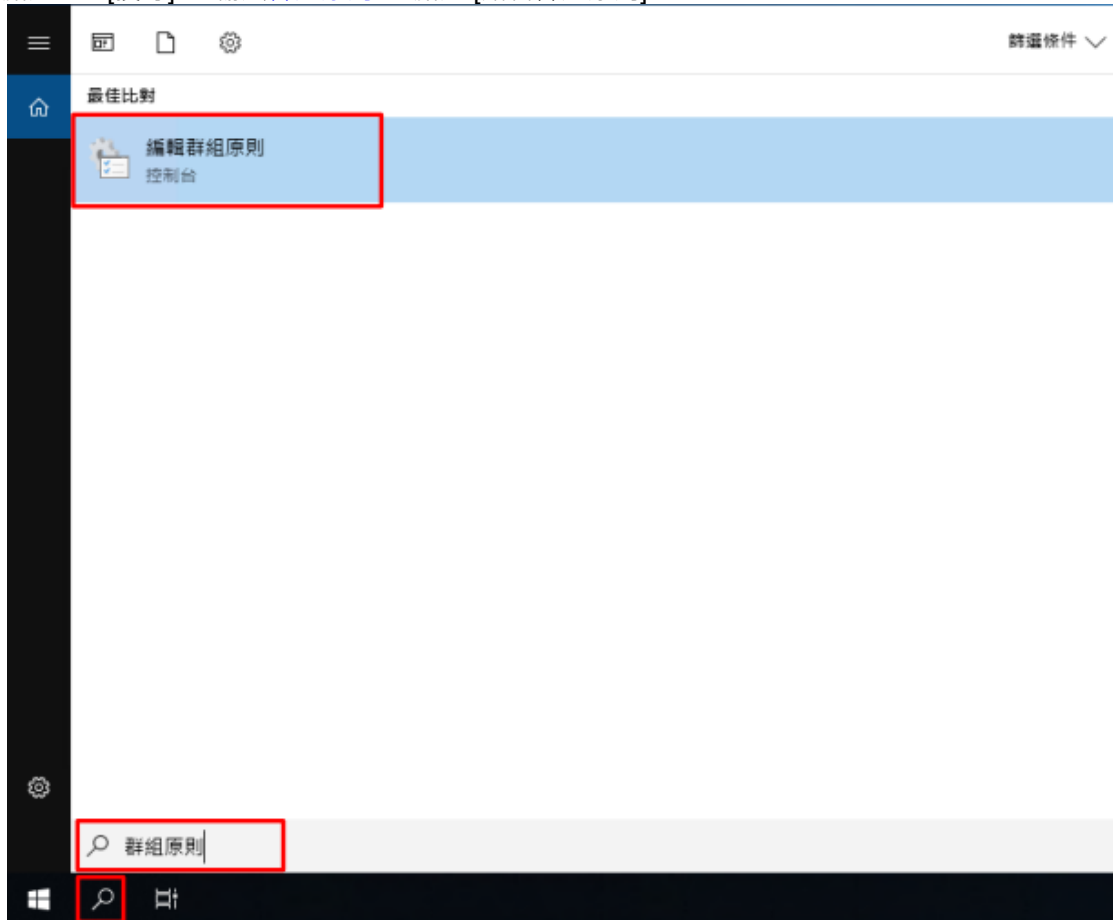
|                              |           |                  |      |
|------------------------------|-----------|------------------|------|
| 群組原則結果                       |           |                  |      |
| N-PARTNER\SQL2019            |           |                  |      |
| 資料收集: 2021/10/22 下午 04:02:35 |           |                  | 全部顯示 |
| 摘要                           |           |                  | 顯示   |
| 電腦詳細資料                       |           |                  | 隱藏   |
| 一般                           |           |                  | 顯示   |
| 元件狀態                         |           |                  | 顯示   |
| 設定                           |           |                  | 隱藏   |
| 原則                           |           |                  | 隱藏   |
| Windows 設定                   |           |                  | 隱藏   |
| 安全性設定                        |           |                  | 隱藏   |
| 帳戶原則/密碼規則                    |           |                  | 顯示   |
| 帳戶原則/帳戶鎖定原則                  |           |                  | 顯示   |
| 本機原則/稽核原則                    |           |                  | 隱藏   |
| 原則                           | 設定        | 優勢 GPO           |      |
| 稽核帳戶登入事件                     | 成功, 失敗    | N-Partner Policy |      |
| 稽核帳戶管理                       | 成功, 失敗    | N-Partner Policy |      |
| 稽核登入事件                       | 成功, 失敗    | N-Partner Policy |      |
| 本機原則/安全性選項                   |           |                  | 顯示   |
| 事件記錄檔                        |           |                  | 隱藏   |
| 原則                           | 設定        | 優勢 GPO           |      |
| 應用程式記錄保持方法                   | 視需要而定     | N-Partner Policy |      |
| 應用程式記錄檔容量最大值                 | 204800 KB | N-Partner Policy |      |
| 公開金鑰原則/憑證服務用戶端 - 自動註冊設定      |           |                  | 顯示   |
| 公開金鑰原則/加密檔案系統                |           |                  | 顯示   |
| 群組原則物件                       |           |                  | 顯示   |
| WMI 篩選器                      |           |                  | 顯示   |
| 使用者詳細資料                      |           |                  | 顯示   |

## 5.3.2 工作群組

### 5.3.2.1 稽核原則設定

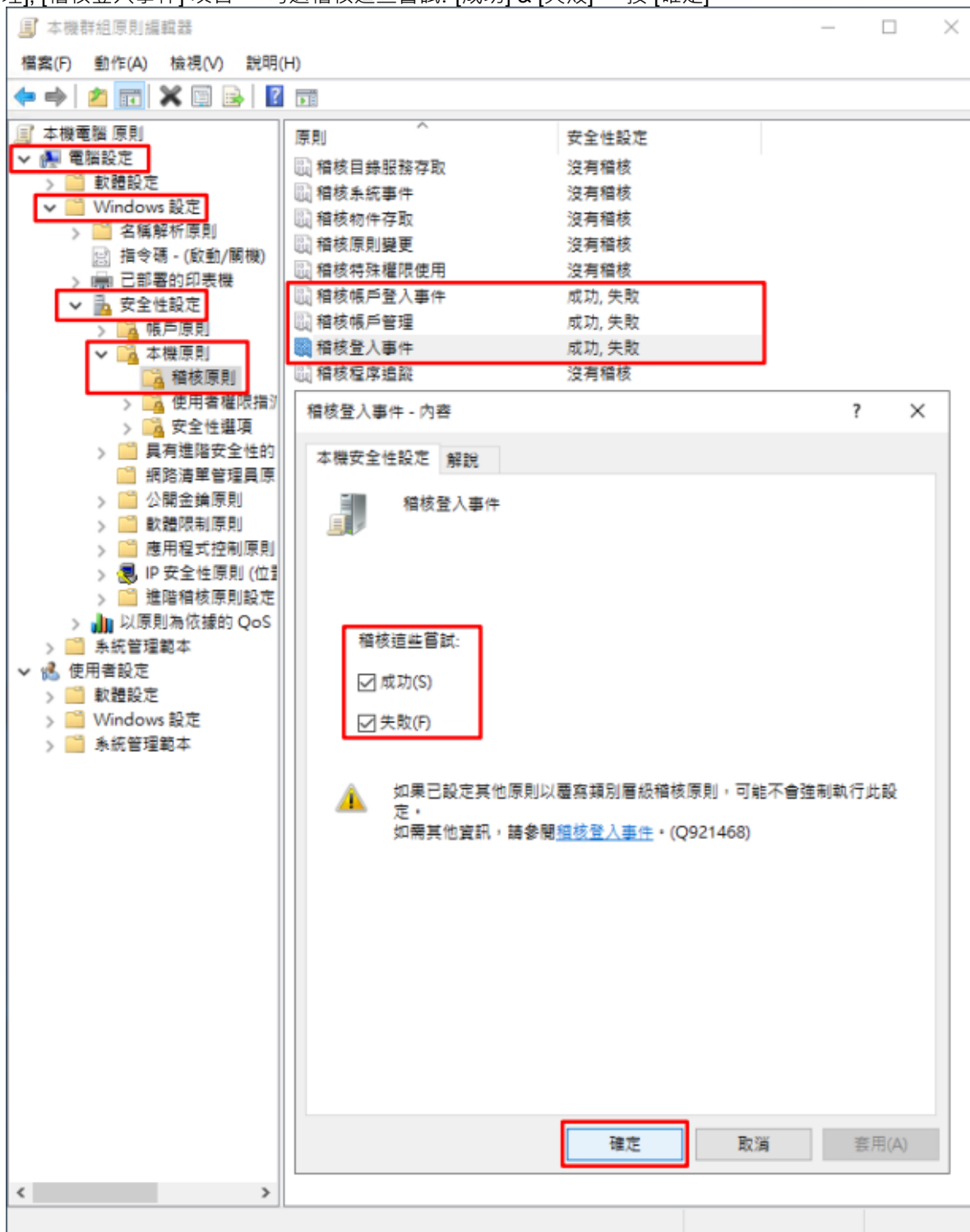
#### (1) 開啟 [本機群組原則編輯器]

點選  [搜尋] -> 輸入 [群組原則](#) -> 點選 [編輯群組原則]



## (2) 本機原則：稽核原則

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

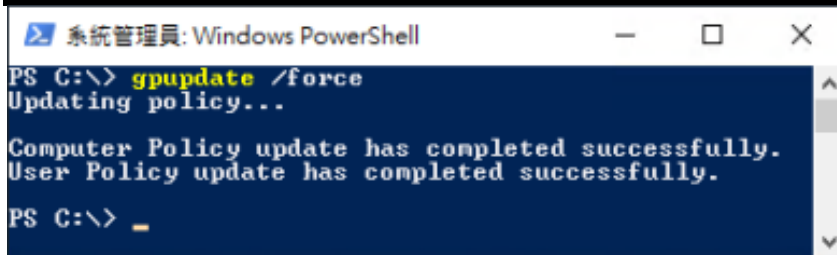


### (3) 開啟 [Windows PowerShell]



### (4) 更新群組原則

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

A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The window has a dark blue background and white text. The command "PS C:\> gpupdate /force" has been entered, and the output shows "Updating policy...", "Computer Policy update has completed successfully.", and "User Policy update has completed successfully." followed by a prompt "PS C:\> \_".

```
系統管理員: Windows PowerShell
PS C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\> _
```

(5) 查看群組原則套用情形

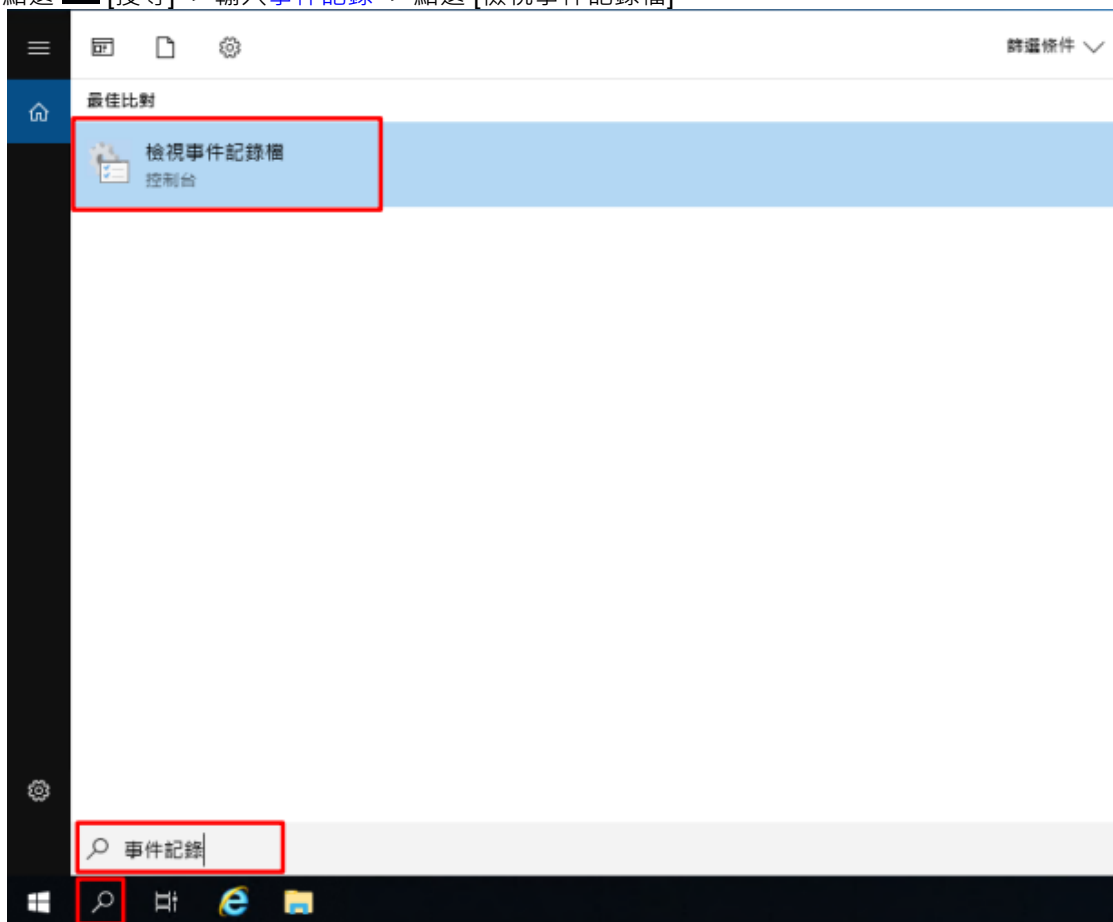
```
PS C:\> auditpol /get /category:*
```

```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
系統
  安全性系統延伸          No Auditing
  系統完整性              Success and Failure
  IPSEC driver            No Auditing
  其他系統事件            Success and Failure
  安全性狀態變更          Success
登入/登出
  登入                    Success and Failure
  登出                    Success and Failure
  帳戶鎖定                Success and Failure
  IPsec 主要模式          Success and Failure
  IPsec 快速模式          Success and Failure
  IPsec 延伸模式          Success and Failure
  特殊登入                Success and Failure
  其他登入/登出事件      Success and Failure
  網路原則伺服器          Success and Failure
  使用者/裝置宣告        Success and Failure
  群組成員資格            Success and Failure
物件存取
  檔案系統                No Auditing
  registry                No Auditing
  核心物件                No Auditing
  SAM                     No Auditing
  憑證服務                No Auditing
  產生的應用程式          No Auditing
  控制代碼操縱            No Auditing
  檔案共用                No Auditing
  篩選平台封包丟棄        No Auditing
  篩選平台連線            No Auditing
  其他物件存取事件        No Auditing
  詳細檔案共用            No Auditing
  抽取式存放裝置          No Auditing
  集中原則暫存            No Auditing
特殊權限使用
  非機密特殊權限使用      No Auditing
  其他特殊權限使用事件    No Auditing
  機密特殊權限使用        No Auditing
詳細追蹤
  建立處理程序            No Auditing
  終止處理程序            No Auditing
  DPAPI 活動              No Auditing
  RPC 事件                No Auditing
  隨插即用事件            No Auditing
  權杖權限調整事件        No Auditing
原則變更
  稽核原則變更            Success
  驗證原則變更            Success
  授權原則變更            No Auditing
  MPSSUC 規則層級原則變更 No Auditing
  篩選平台原則變更        No Auditing
  其他原則變更事件        No Auditing
帳戶管理
  電腦帳戶管理            Success and Failure
  安全性群組管理          Success and Failure
  發佈群組管理            Success and Failure
  應用程式群組管理        Success and Failure
  其他帳戶管理事件        Success and Failure
  使用者帳戶管理          Success and Failure
DS 存取
  目錄服務存取            Success
  目錄服務變更            No Auditing
  目錄服務複寫            No Auditing
  詳細目錄服務複寫        No Auditing
帳戶登入
  Kerberos 服務票證操作    Success and Failure
  其他帳戶登入事件        Success and Failure
  Kerberos 驗證服務        Success and Failure
  認證驗證                Success and Failure
PS C:\>
```

### 5.3.2.2 事件檔案設定

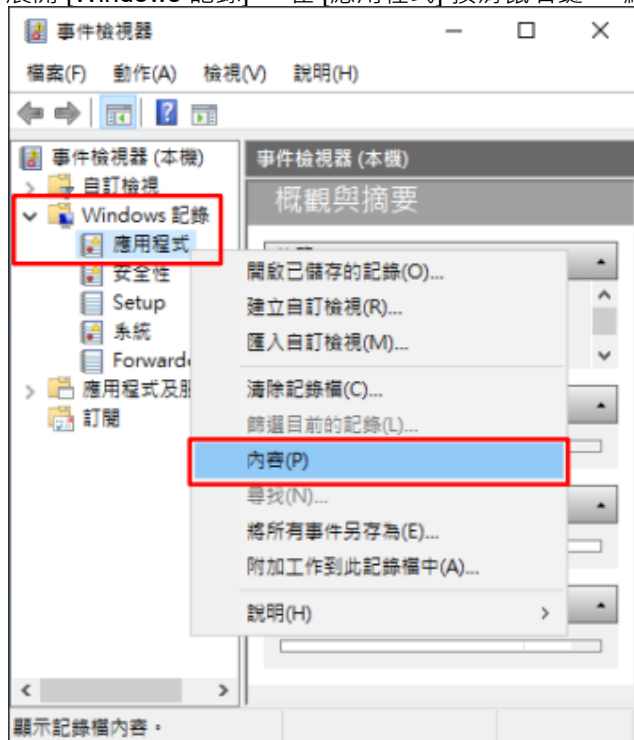
#### (1) 開啟 [檢視事件記錄檔]

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



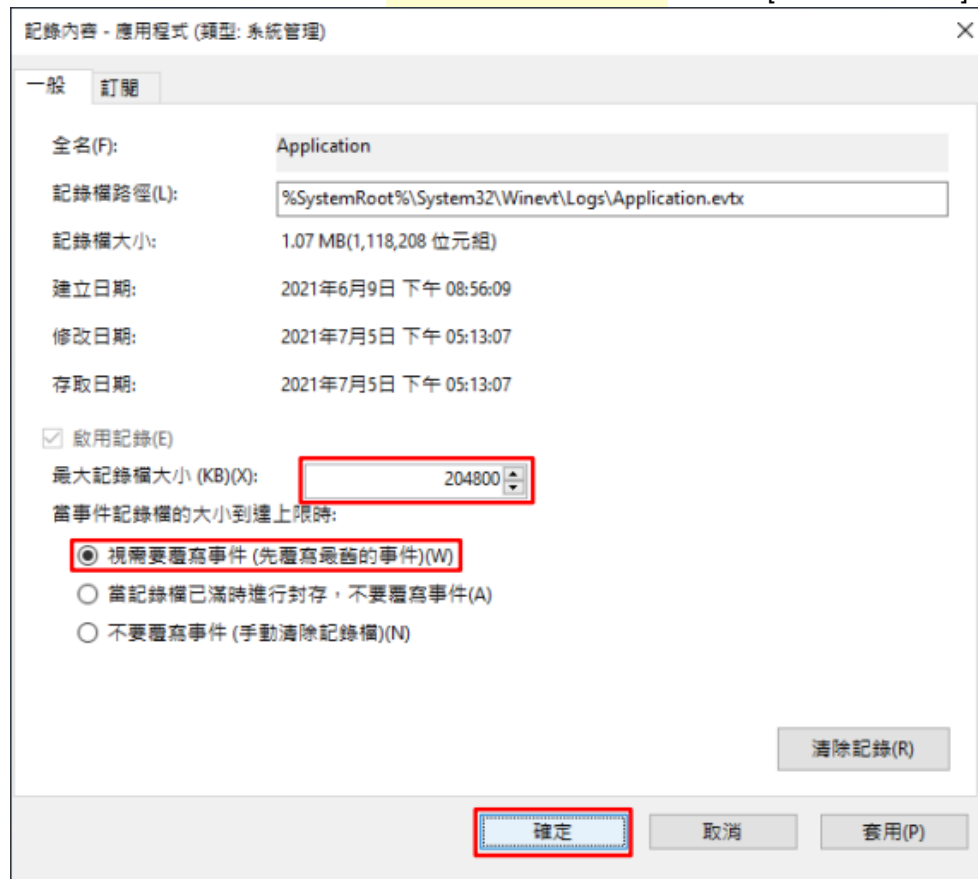
## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [應用程式] 按滑鼠右鍵 -> 點選 [內容]



## (3) 設定應用程式記錄檔

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



## 6 SQL2022

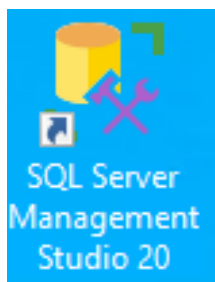
### 6.1 稽核登入

啟用登入稽核，以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。

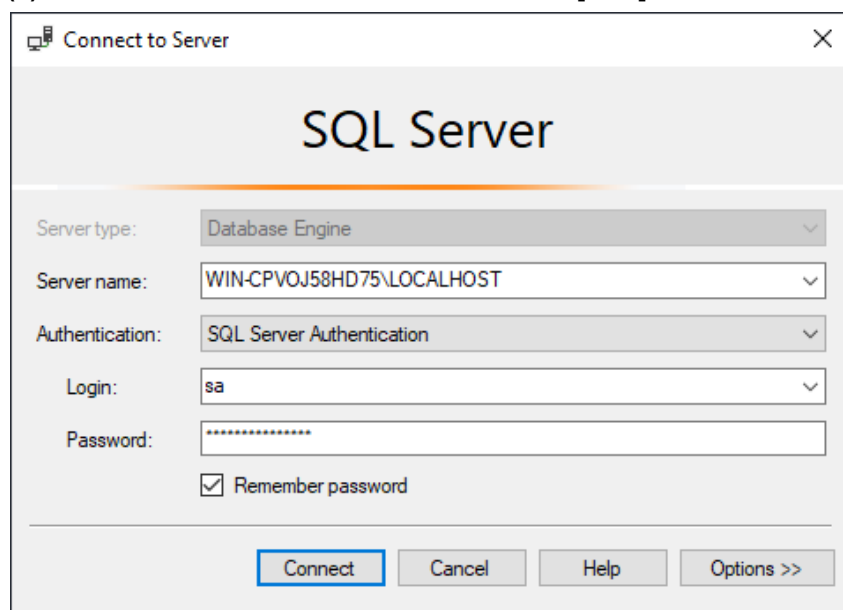
以下分別為圖形介面和指令介面設定方式。

#### 6.1.1 使用圖形介面方式設定

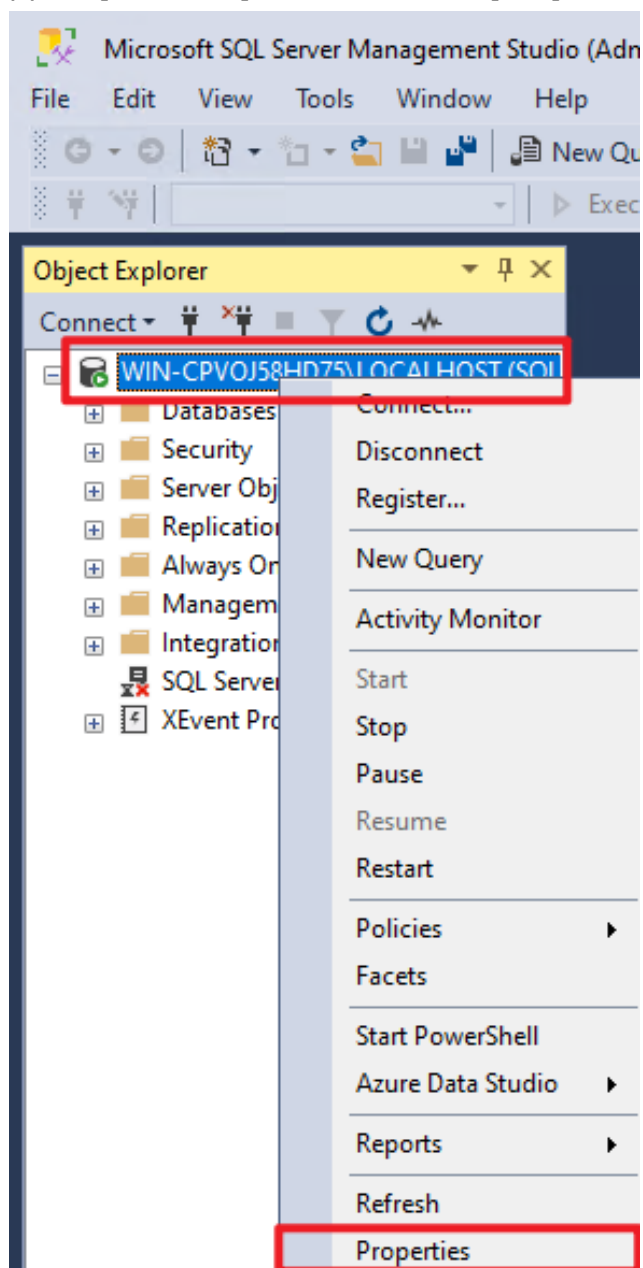
##### (1) 開啟 [Microsoft SQL Server Management Studio]



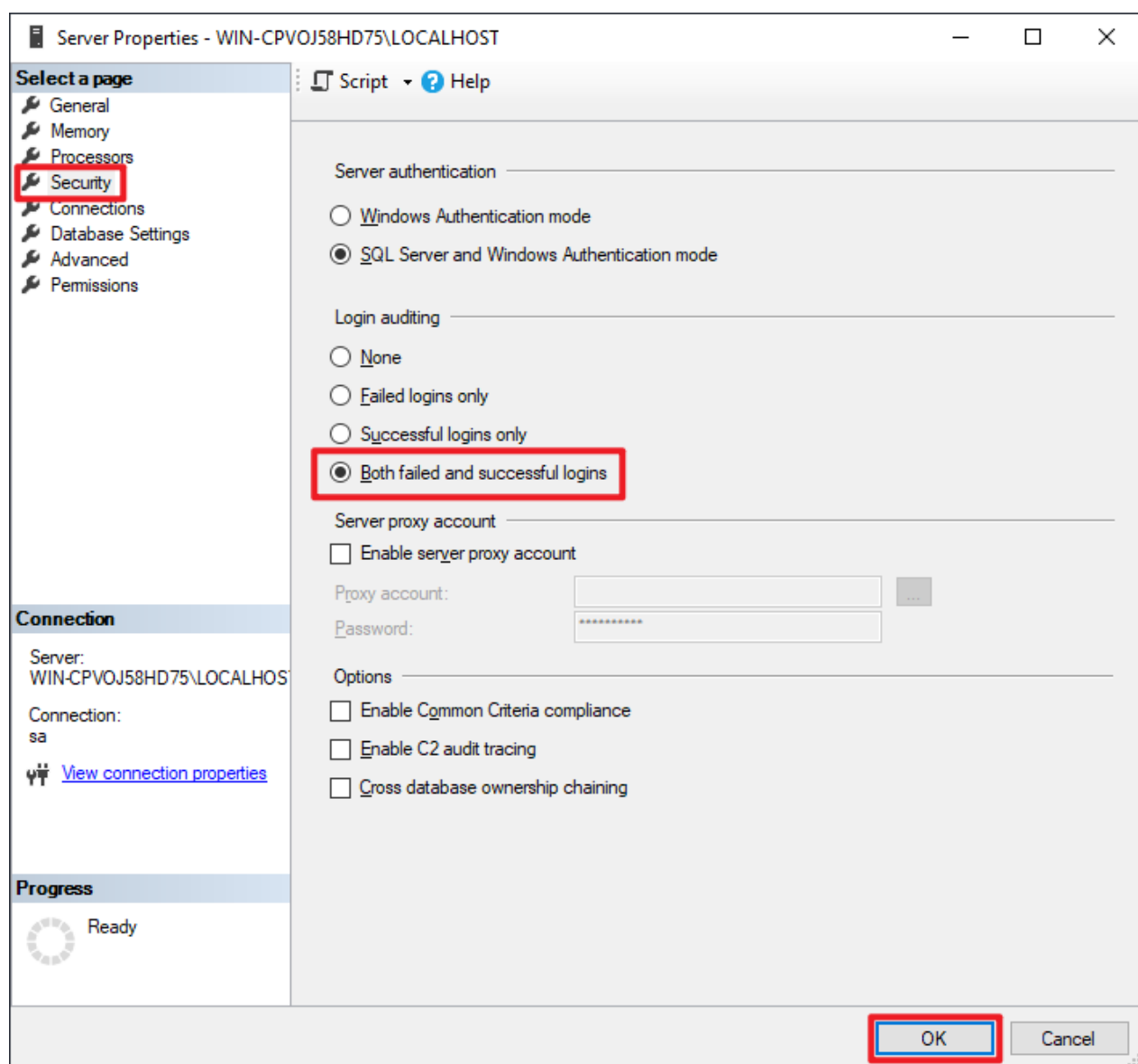
##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

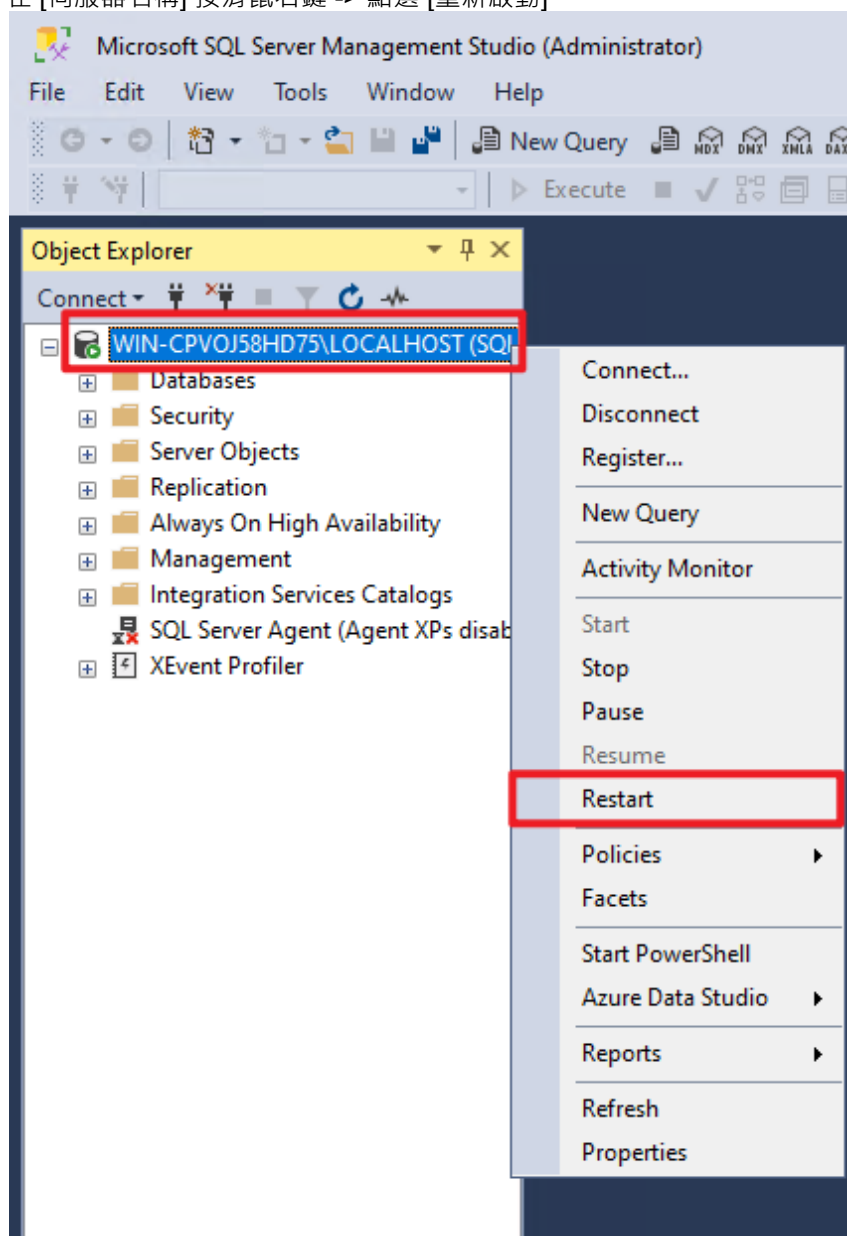


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

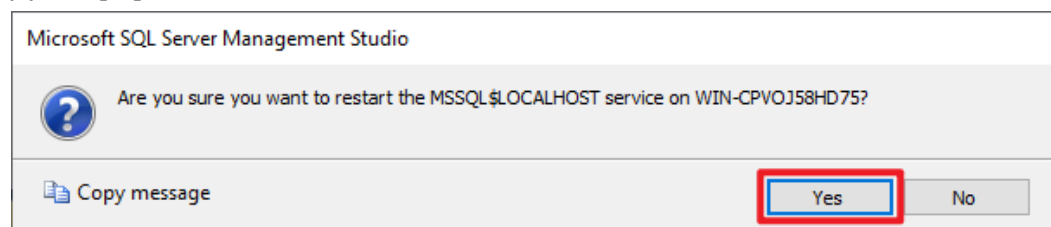


##### (5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



##### (6) 按 [是] 重新啟動 MS SQL SERVER 服務



## 6.1.2 使用指令介面方式設定

### (1) 開啟 [Windows Powershell]



### (2) 分別為 sa 或 Windows 帳號登入方式

#### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPV0J58HD75\LOCALHOST -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance\_name][,port]

-U login\_id

-P password

-A dedicated administrator connection

#### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPV0J58HD75\LOCALHOST -A
1> _
```

### (3) 切換資料庫

```
1 > use master
2 > go
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
1> use master
2> go
Changed database context to 'master'.
1> _
```

#### (4) 使用 sp\_configure 列出進階選項

```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```

Administrator: Windows PowerShell - SQLCMD

```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
```

#### (5) 啟用失敗和成功的登入記錄

```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
1 > quit
```

Administrator: Windows PowerShell

```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit
PS C:\Users\Administrator> _
```

#### (6) 重新啟動 MS SQL SERVER 服務和確認 MS SQL SERVER 服務狀態

```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT
```

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Restart-Service -Name MSSQLSERVER -Force
PS C:\Users\Administrator> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT

Status      Name                DisplayName
-----
Running     MSSQLSERVER         SQL Server (MSSQLSERVER)
Stopped     SQLSERVERAGENT      SQL Server Agent (MSSQLSERVER)

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

## 6.2 設定稽核

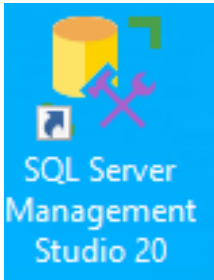
### 6.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

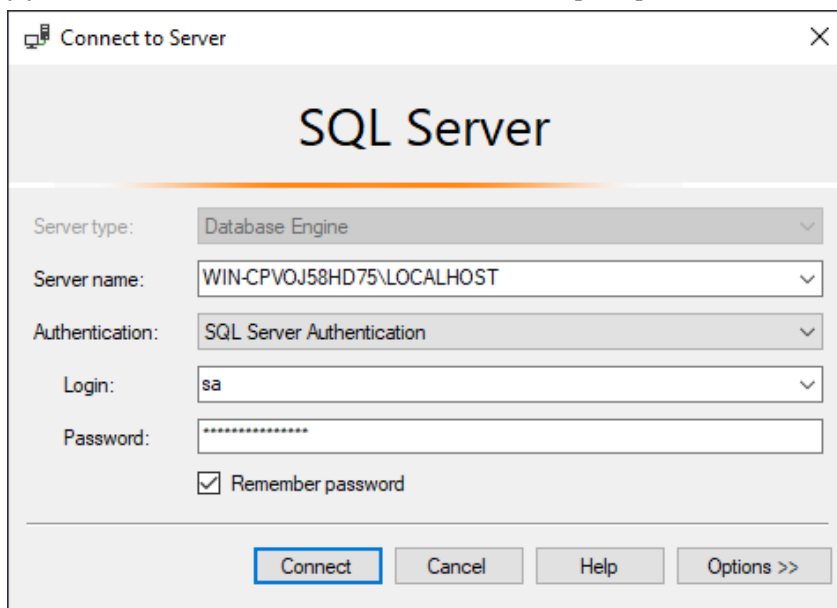
以下分別為圖形介面和指令介面設定方式。

#### 6.2.1.1 使用圖形介面方式設定

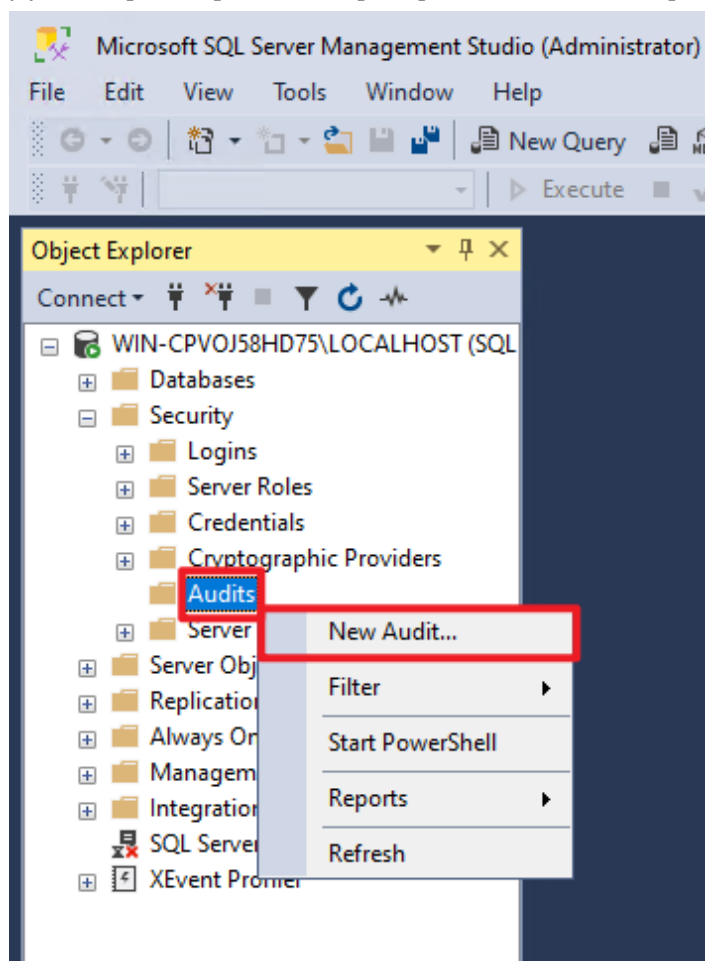
##### (1) 開啟 [Microsoft SQL Server Management Studio]



##### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 [確定]

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- ☒ Continue
- ☐ Fail operation
- ☐ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:

- ☒ Maximum rollover files: ☒ Unlimited
- ☐ Maximum files: 2147483647

Maximum file size: 0 MB ☒ Unlimited

☐ Reserve disk space

Connection

WIN-CPVOJ58HD75\LOCALHOST [sa]

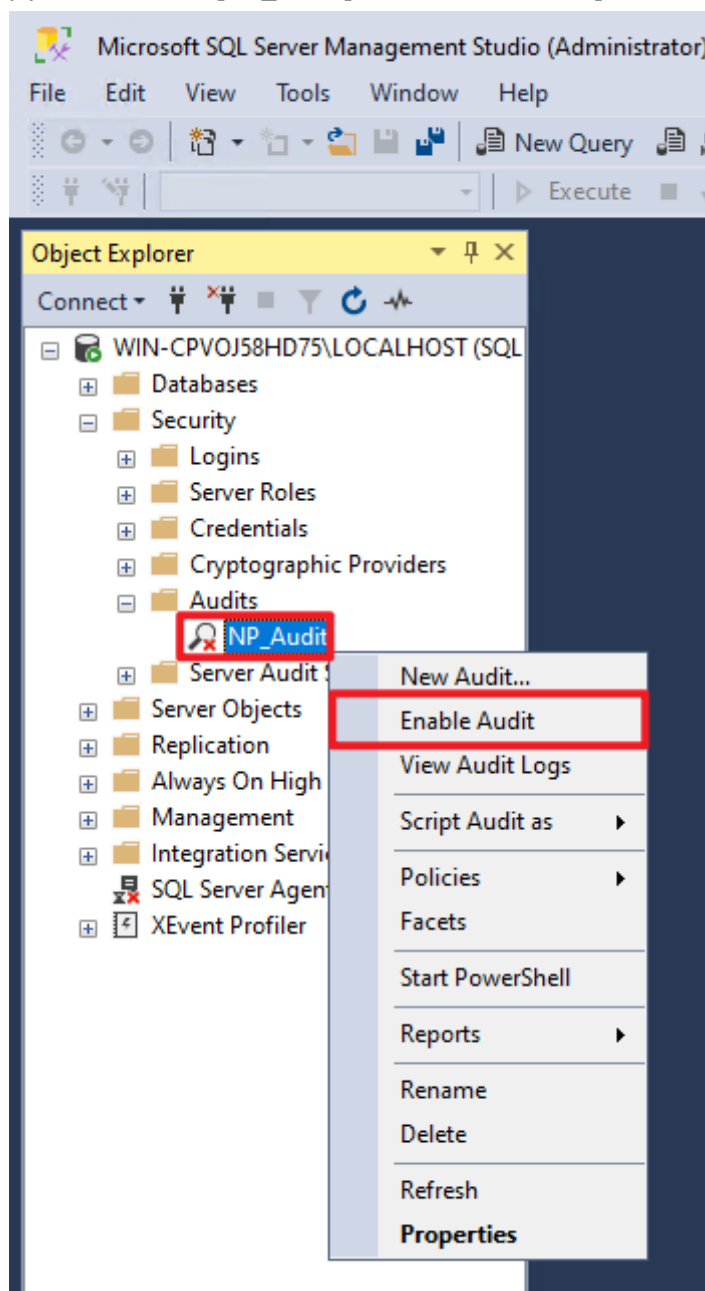
[View connection properties](#)

Progress

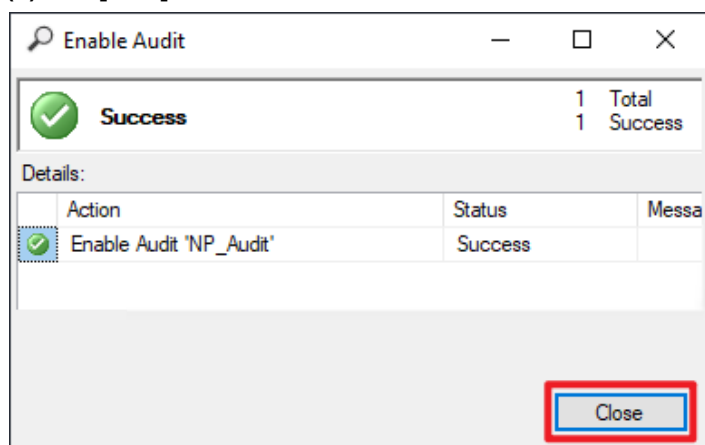
Ready

OK Cancel Help

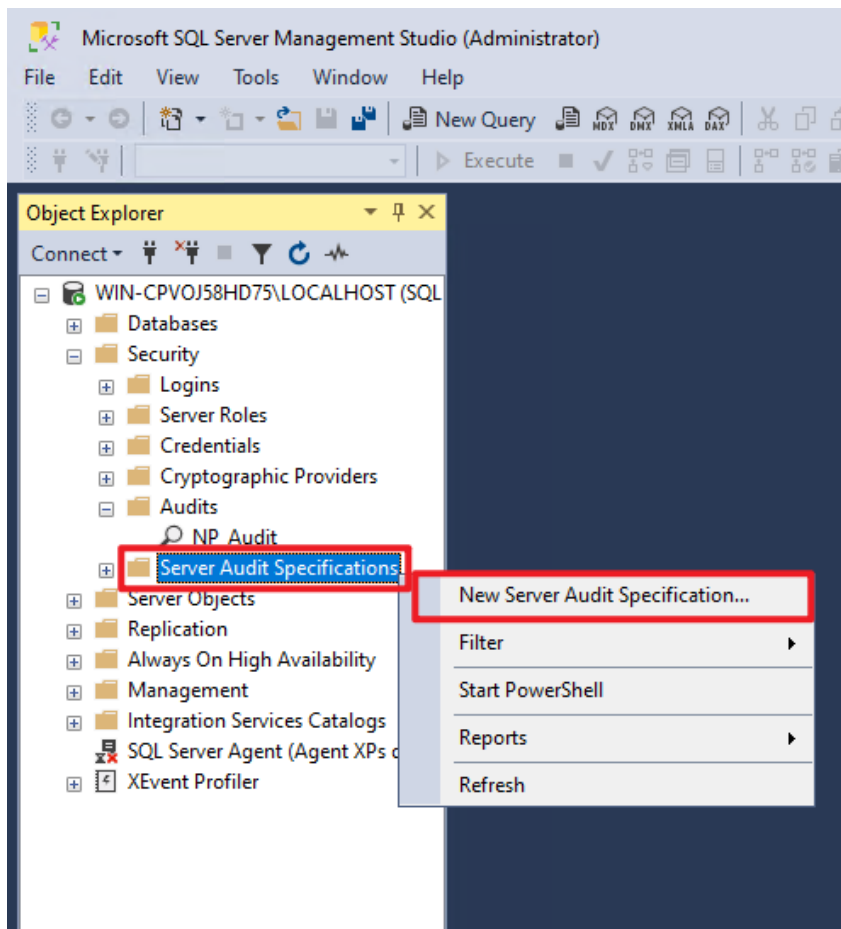
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



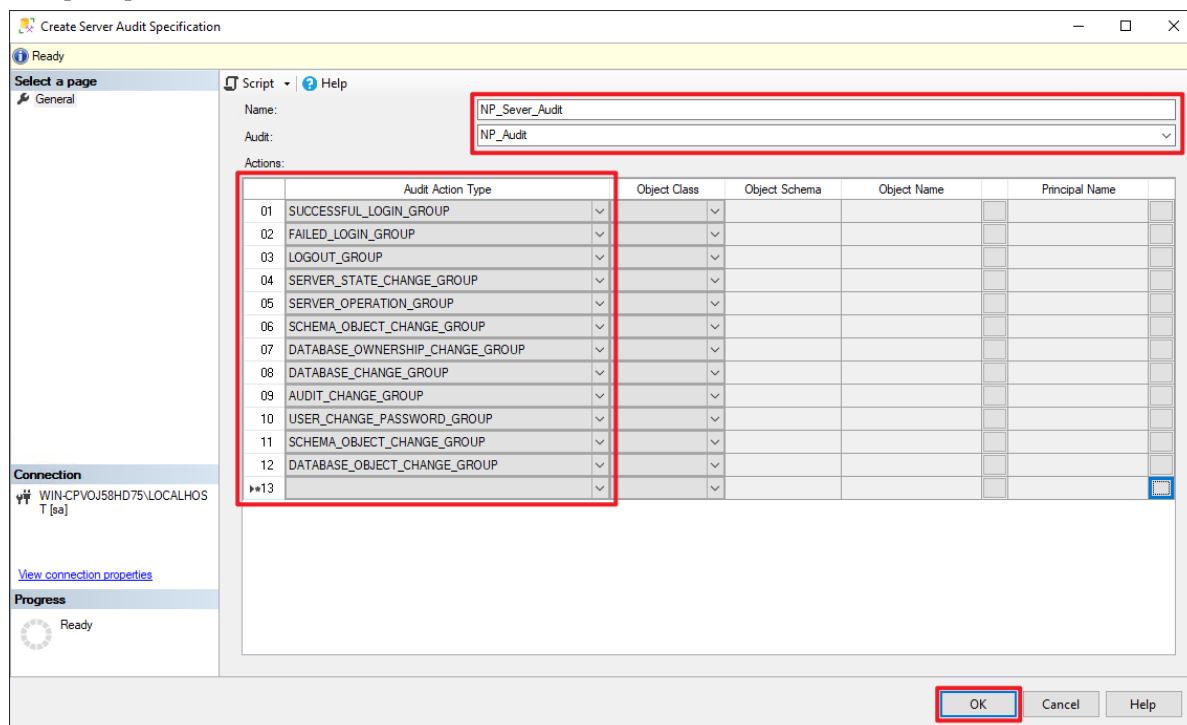
(6) 按 [關閉]



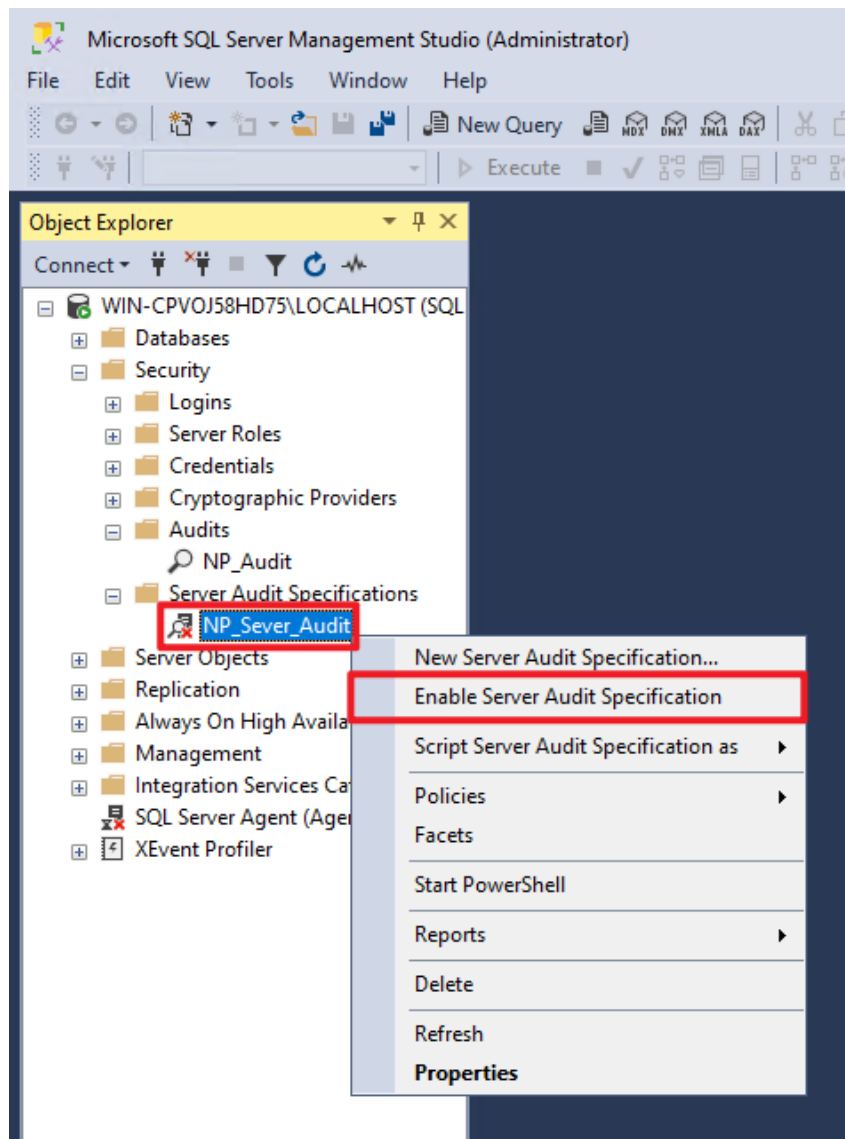
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



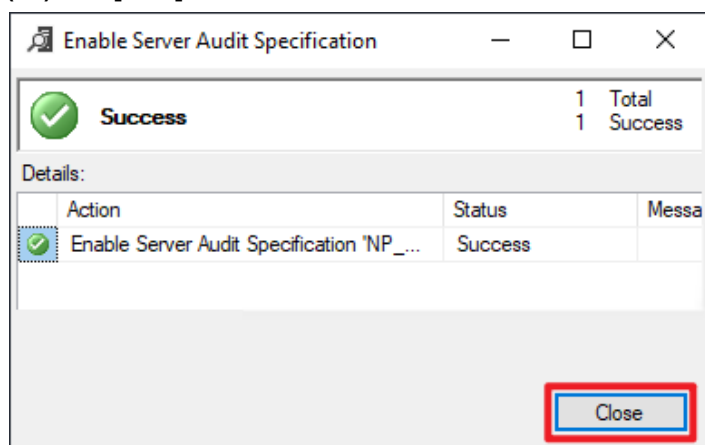
(8) 輸入名稱: **NP\_Server\_Audit** -> 選擇稽核: **[NP\_Audit]** 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(9) 在伺服器稽核規格名稱: [NP\_Server\_Audit] 按滑鼠右鍵 -> 點選 [啟用伺服器稽核規格]

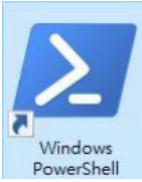


(10) 按 [關閉]



### 6.2.1.2 使用指令介面方式設定

#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPVOJ58HD75\LOCALHOST -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance\_name][,port]

-U login\_id

-P password

-A dedicated administrator connection

##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPVOJ58HD75\LOCALHOST -A
1> _
```

#### (3) 切換資料庫

```
1 > use master
2 > go
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

Administrator: Windows PowerShell - SQLCMD

```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1>
```

紅色文字部位請輸入稽核名稱

(5) 設定稽核伺服器，ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP),
12 > ADD (USER_CHANGE_PASSWORD_GROUP),
13 > ADD (SERVER_OBJECT_CHANGE_GROUP),
14 > ADD (DATABASE_OBJECT_CHANGE_GROUP)
15 > WITH (STATE = ON)
16 > GO
1 > quit
```

Administrator: Windows PowerShell - SQLCMD

```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP),
13> ADD (SERVER_OBJECT_CHANGE_GROUP),
14> ADD (DATABASE_OBJECT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\Users\Administrator>
```

紅色文字部位請輸入伺服器稽核規格名稱

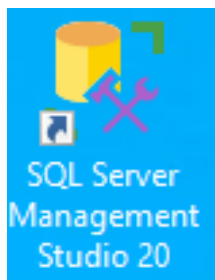
## 6.2.2 稽核資料庫層級

啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

以下分別為圖形介面和指令介面設定方式。

### 6.2.2.1 使用圖形介面方式設定

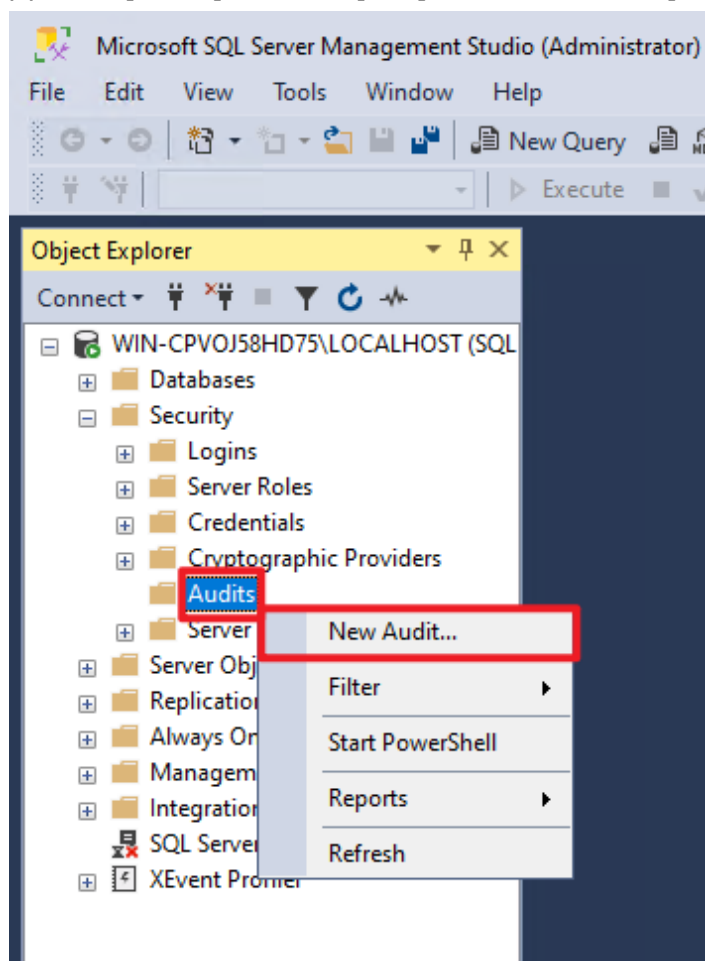
#### (1) 開啟 [Microsoft SQL Server Management Studio]



#### (2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

The image shows the "Connect to Server" dialog box in Microsoft SQL Server. The title bar says "Connect to Server" with a close button. The main heading is "SQL Server". Below this, there are several fields: "Server type:" with a dropdown menu showing "Database Engine"; "Server name:" with a dropdown menu showing "WIN-CPVOJ58HD75\LOCALHOST"; "Authentication:" with a dropdown menu showing "SQL Server Authentication"; "Login:" with a dropdown menu showing "sa"; and "Password:" with a text box containing eight asterisks. There is a checkbox labeled "Remember password" which is checked. At the bottom, there are four buttons: "Connect" (highlighted with a blue border), "Cancel", "Help", and "Options >>".

(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



- (4) 輸入稽核名稱: **NP\_Audit** -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]  
將 **MS SQL** 稽核記錄儲存於 **Windows** 事件檢視器的應用程式記錄 -> 按 [確定]

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- ☒ Continue
- ☐ Fail operation
- ☐ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:

- ☒ Maximum rollover files: ☒ Unlimited
- ☐ Maximum files: 2147483647

Maximum file size: 0 MB ☒ Unlimited

☐ Reserve disk space

Connection

WIN-CPVOJ58HD75\LOCALHOST [sa]

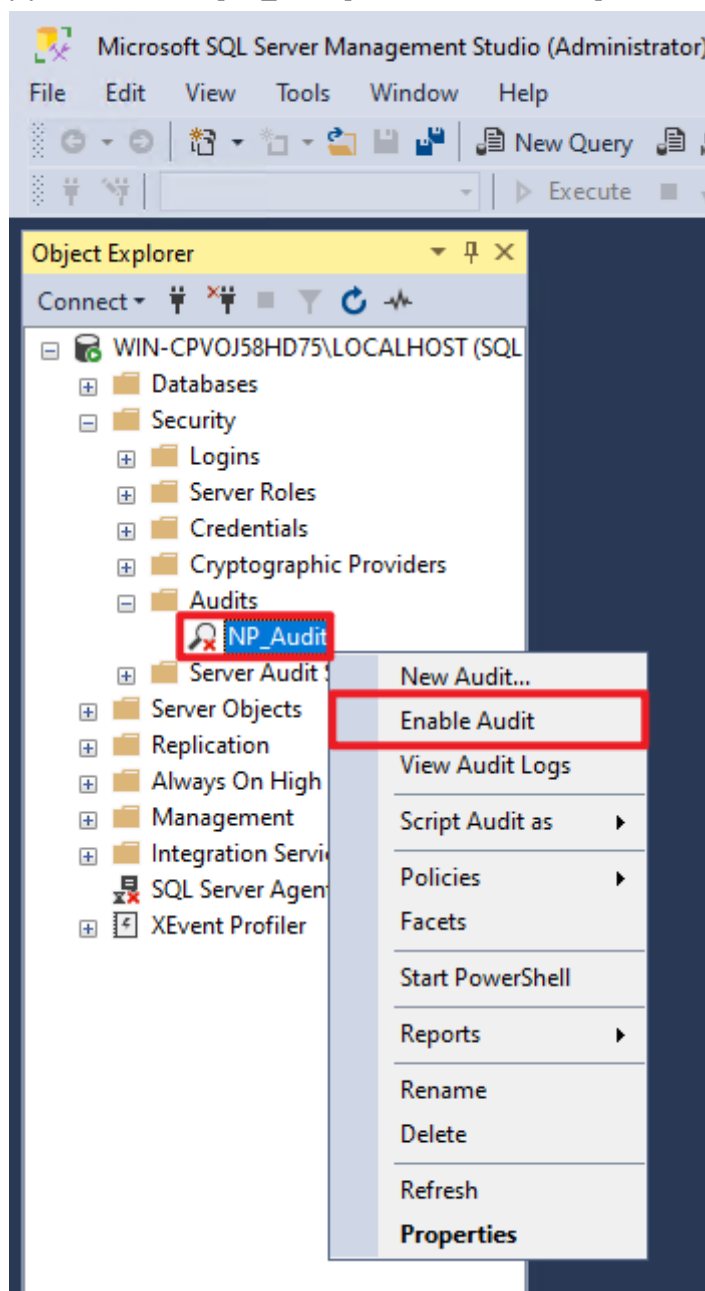
[View connection properties](#)

Progress

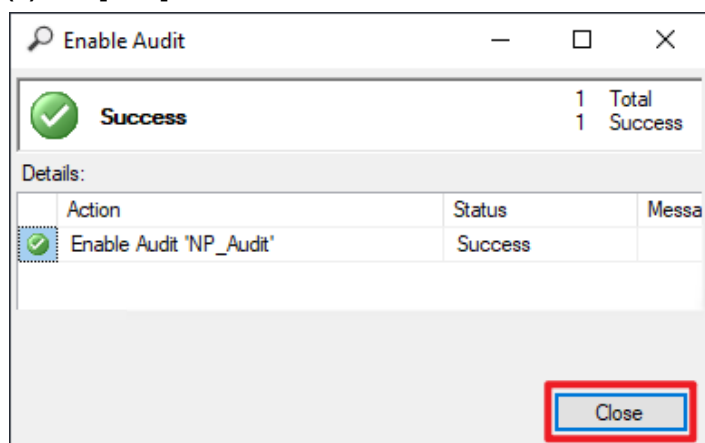
Ready

OK Cancel Help

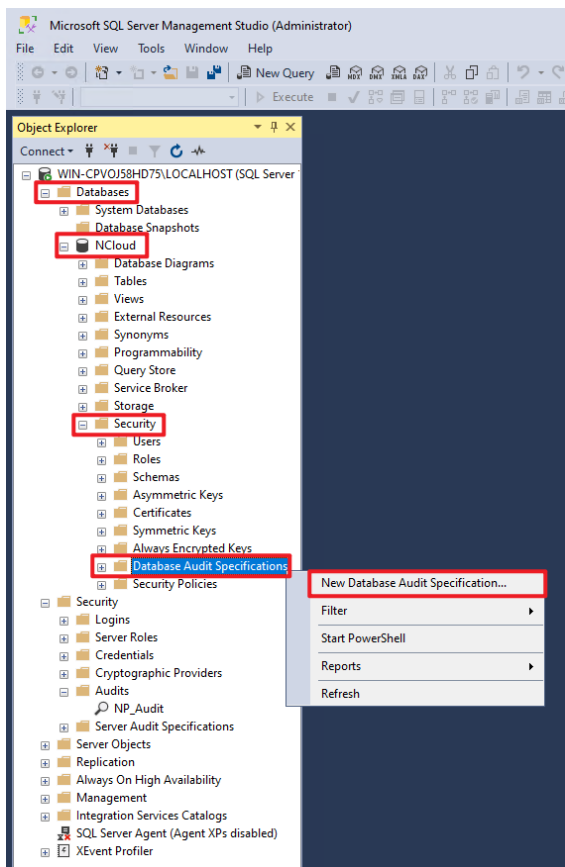
(5) 在稽核名稱: [NP\_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



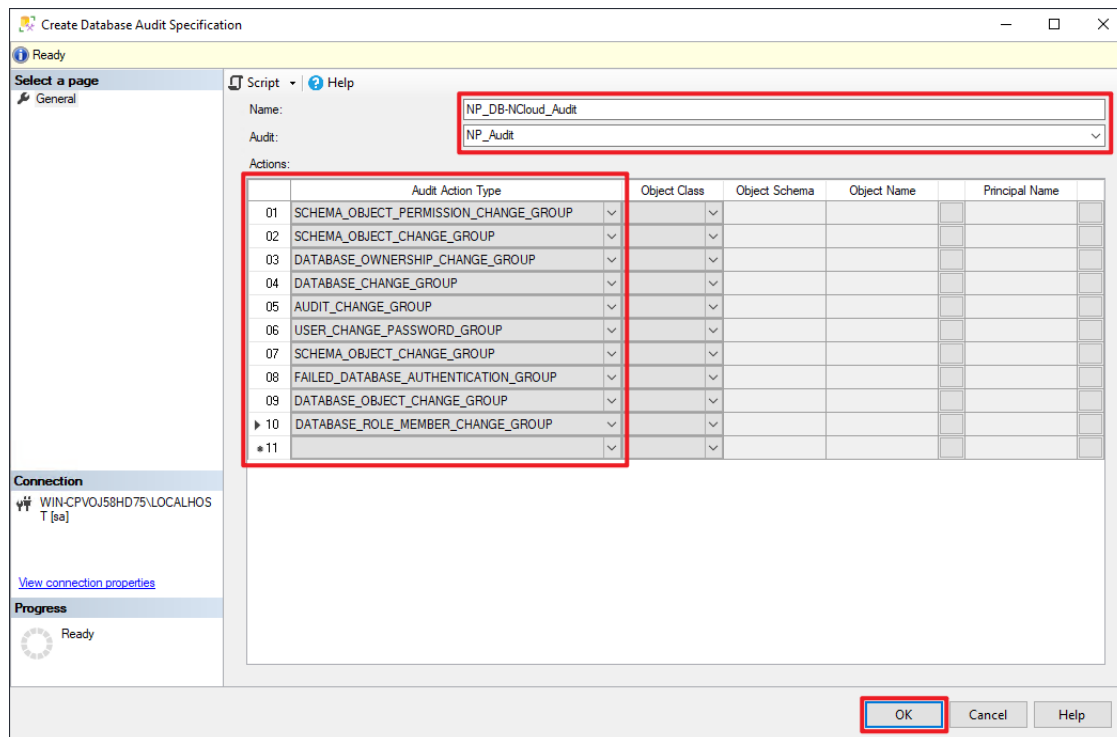
(6) 按 [關閉]



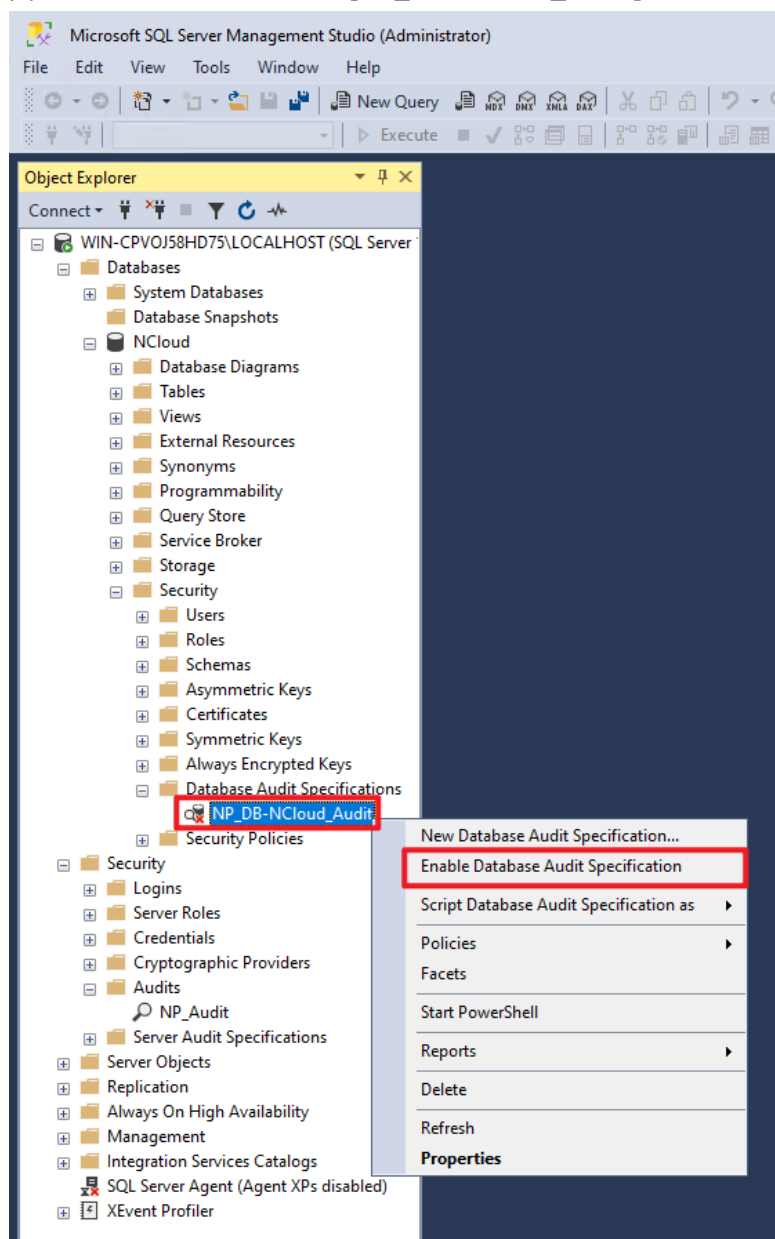
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



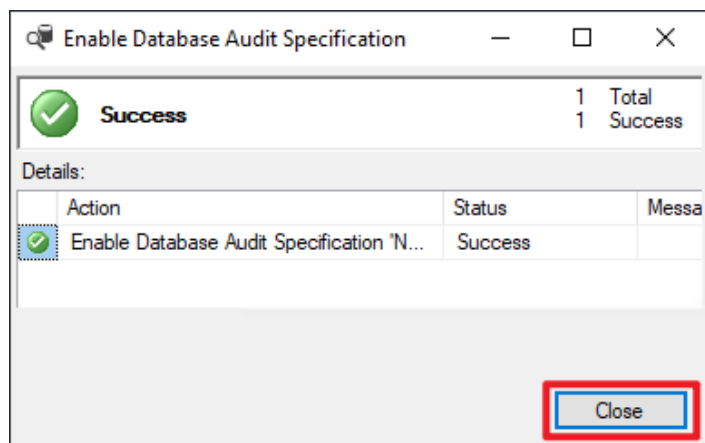
(8) 輸入稽核名稱: NP\_DB-NCloud\_Audit -> 選擇稽核: [NP\_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#)  
-> 按 [確定]



(9) 在資料庫稽核規格名稱: [NP\_DB-NCloud\_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]

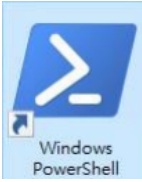


(10) 按 [關閉]



### 6.2.2.2 使用指令介面方式設定

#### (1) 開啟 [Windows Powershell]



#### (2) 分別為 sa 或 Windows 帳號登入方式

##### <2.1> 使用 sa 帳號

```
PS C:\> sqlcmd -S localhost -U sa
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPVOJ58HD75\LOCALHOST -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance\_name][,port]

-U login\_id

-P password

-A dedicated administrator connection

##### <2.2> 使用 Windows 帳號

```
PS C:\> sqlcmd -S localhost -A
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
PS C:\Users\Administrator> sqlcmd -S WIN-CPVOJ58HD75\LOCALHOST -A
1> _
```

#### (3) 切換資料庫

```
1 > use master
2 > go
```

```
Administrator: Windows PowerShell - SQLCMD
```

```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

Administrator: Windows PowerShell - SQLCMD

```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例：NCloud

```
1 > use NCloud
2 > go
```

Administrator: Windows PowerShell - SQLCMD

```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1> _
```

紅色文字部位請輸入稽核資料庫名稱

(6) 設定稽核 NCloud(範例) 資料庫・ADD 動作 詳細說明請參考前言的稽核動作群組連結

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```

```
Administrator: Windows PowerShell

1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_CHANGE_GROUP),
8> ADD (AUDIT_CHANGE_GROUP),
9> ADD (USER_CHANGE_PASSWORD_GROUP),
10> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
11> ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12> ADD (DATABASE_OBJECT_CHANGE_GROUP),
13> ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14> WITH (STATE = ON)
15> GO
1> quit
PS C:\Users\Administrator> _
```

紅色文字部位請輸入資料庫稽核規格名稱

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

紅色文字部位請輸入稽核資料庫名稱

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

## 6.3 事件記錄檔設定

此為選項設定。

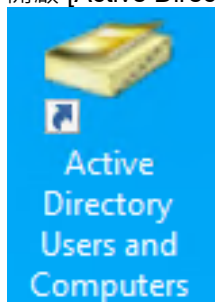
以下分別為網域和工作群組設定方式。

### 6.3.1 網域

#### 6.3.1.1 組織單位設定

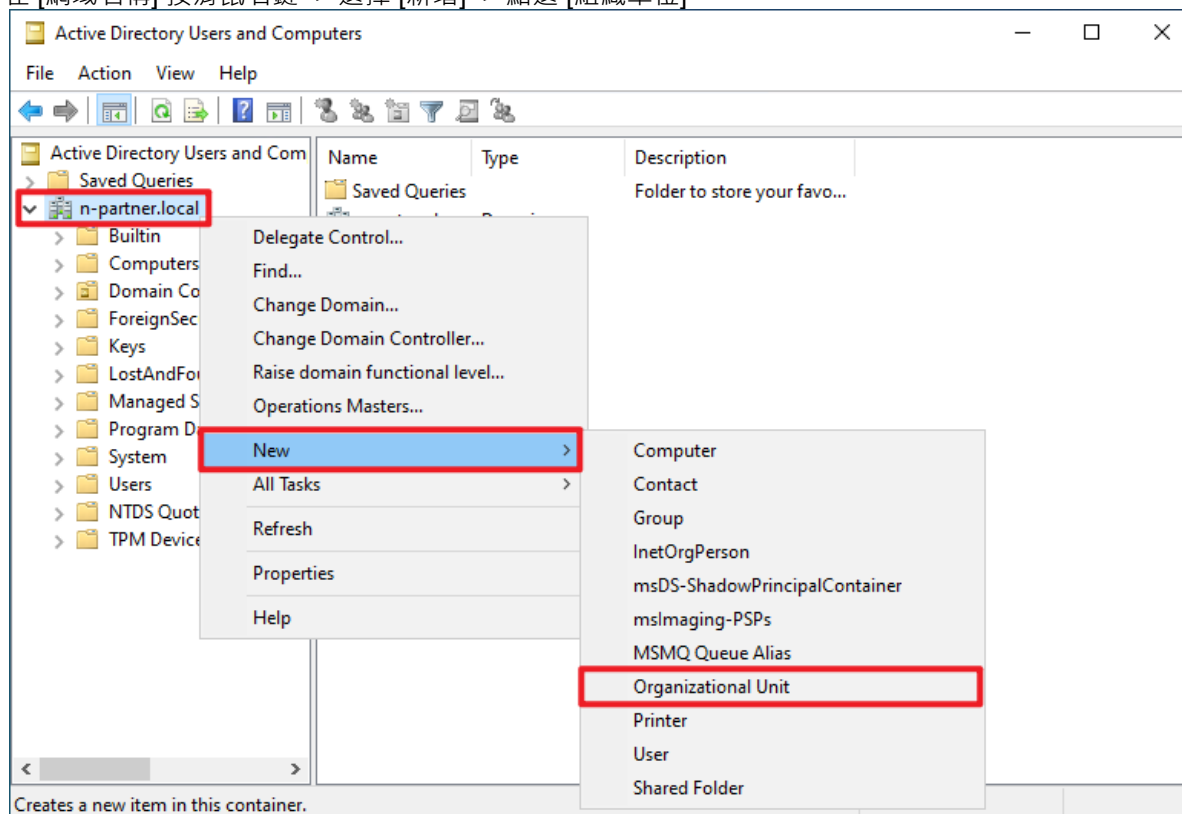
##### (1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



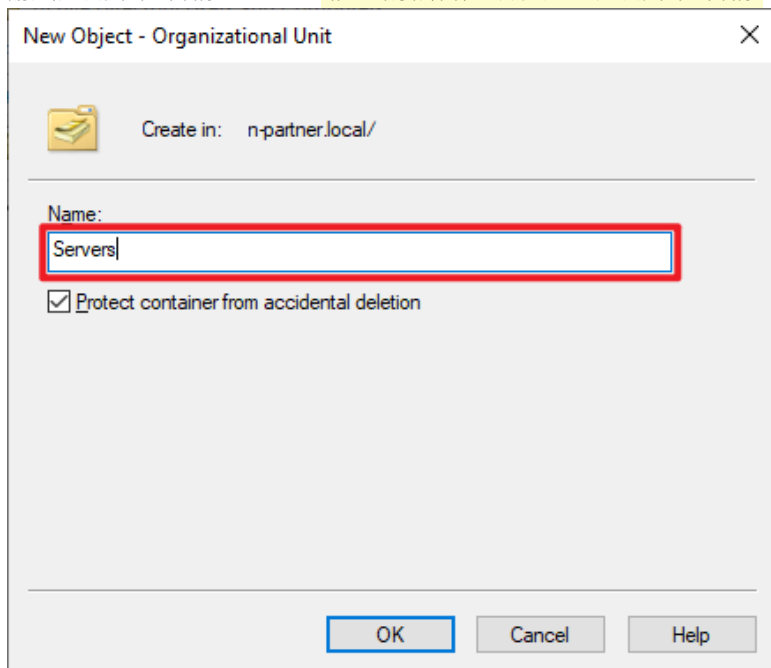
##### (2) 新增組織單位

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



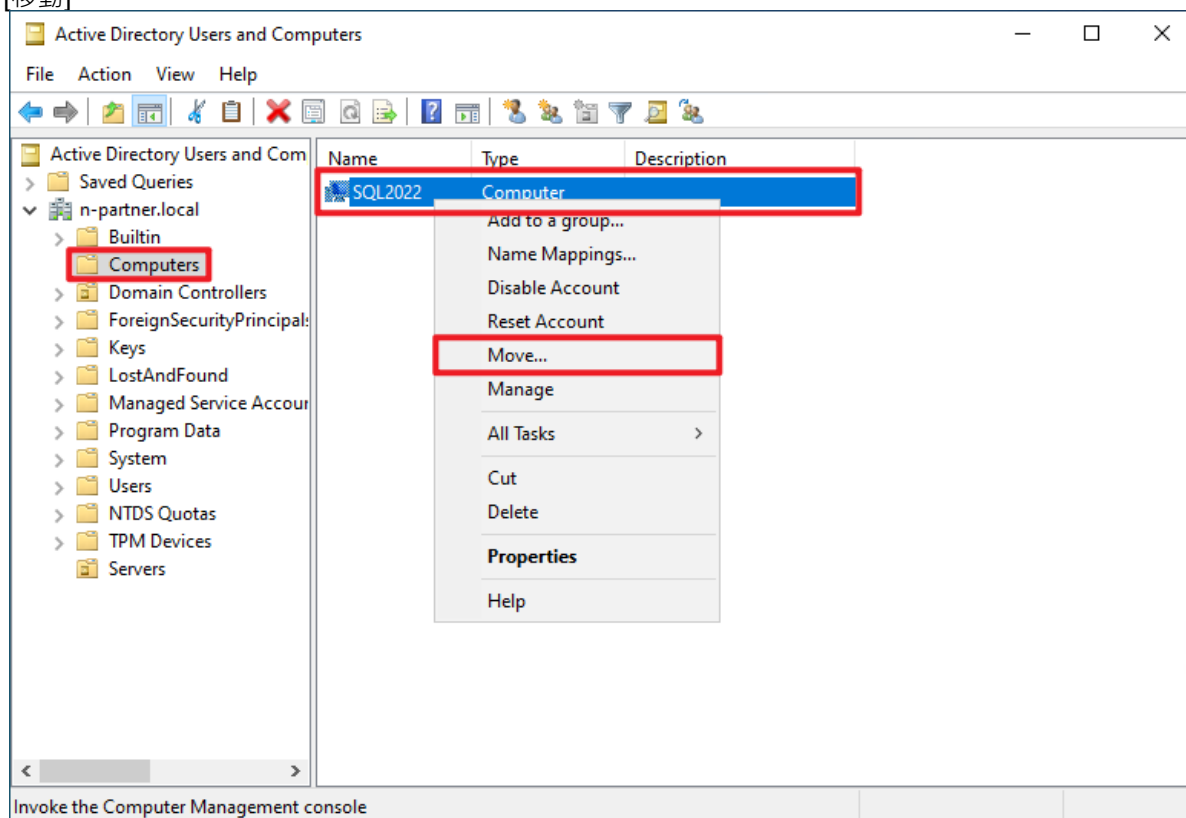
### (3) 輸入組織單位名稱

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



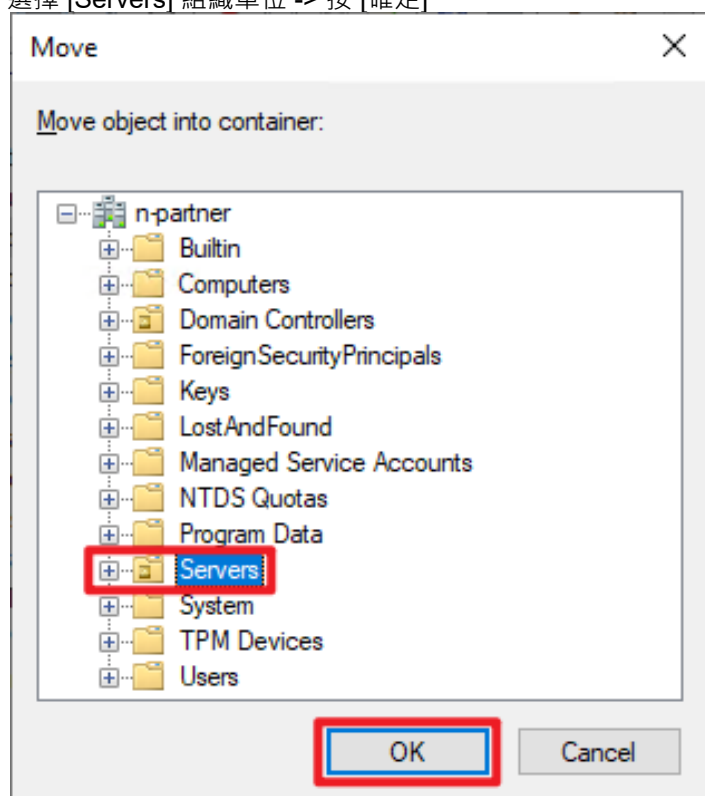
### (4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL 2022] 伺服器, 按滑鼠右鍵, 註：請依客戶環境選擇 MS SQL Server 主機 -> 點選 [移動]



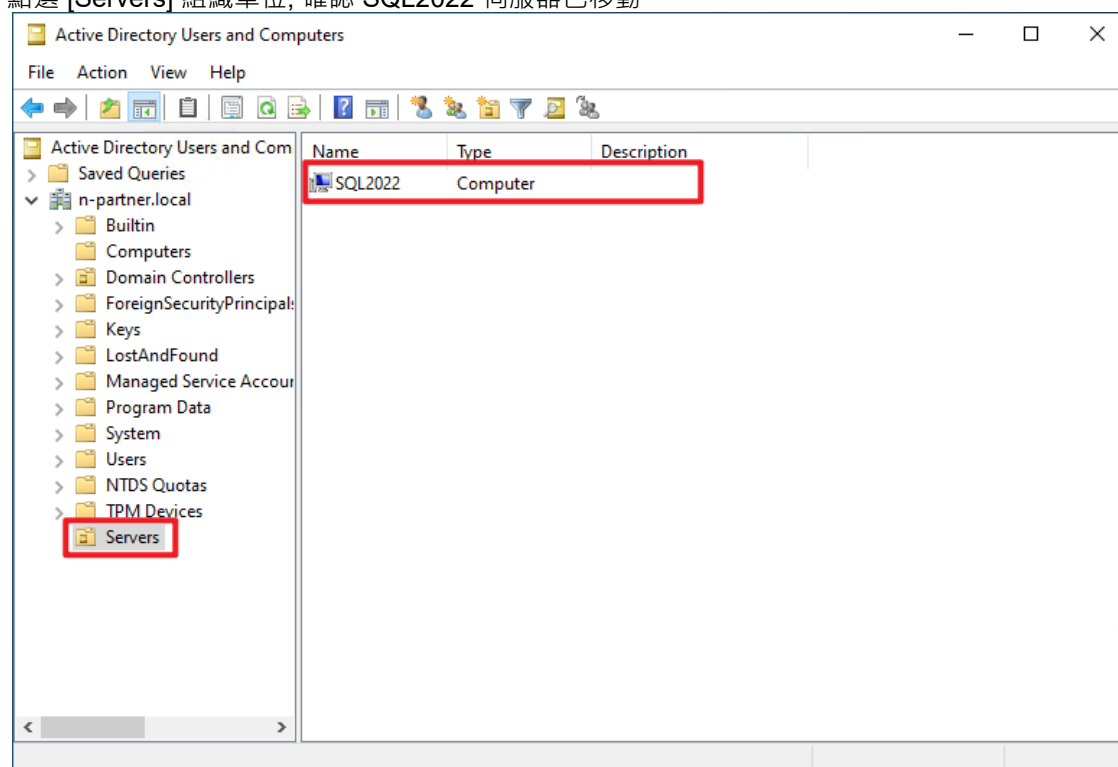
## (5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



## (6) 確認伺服器已移動至新的組織單位

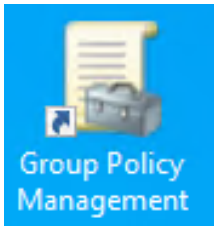
點選 [Servers] 組織單位, 確認 SQL2022 伺服器已移動。



### 6.3.1.2 群組原則設定

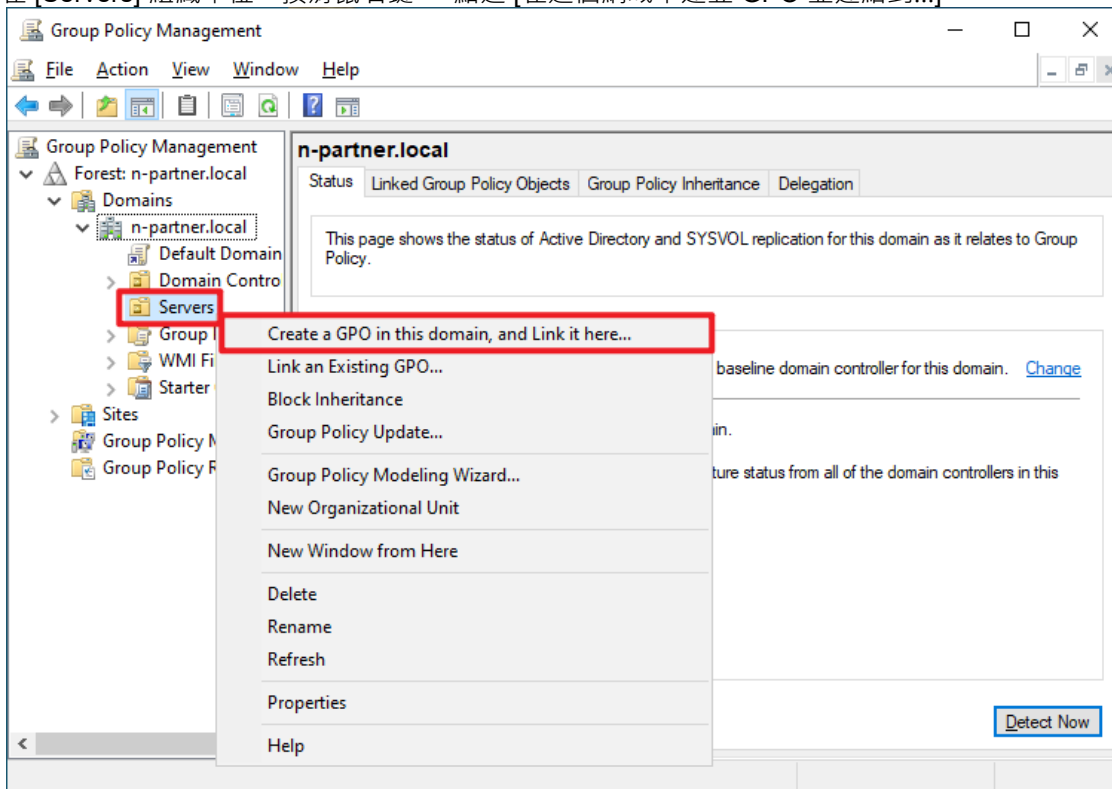
#### (1) 開啟群組原則管理

開啟 [群組原則管理]



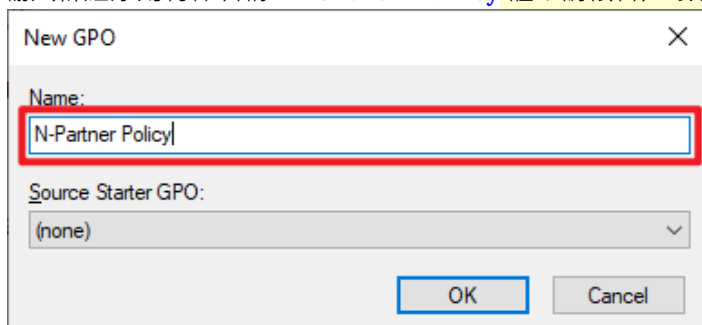
#### (2) 在 Servers 組織單位，新增群組原則物件

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



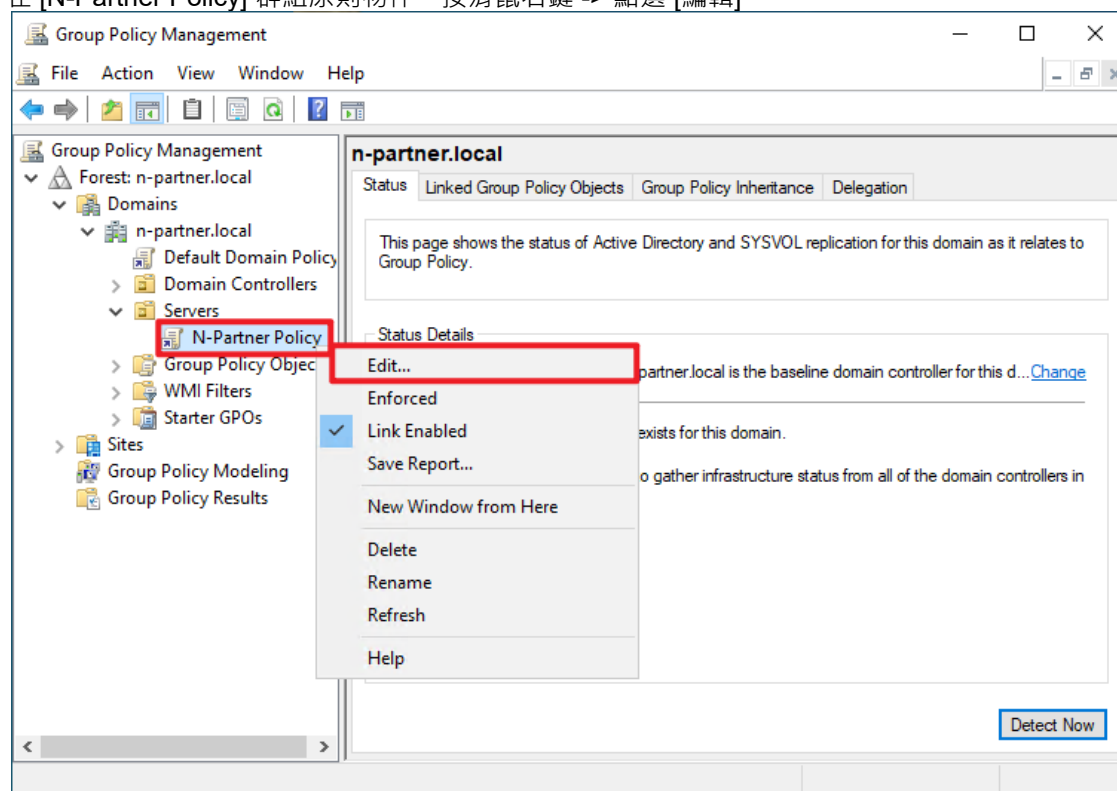
#### (3) 輸入群組原則物件名稱

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



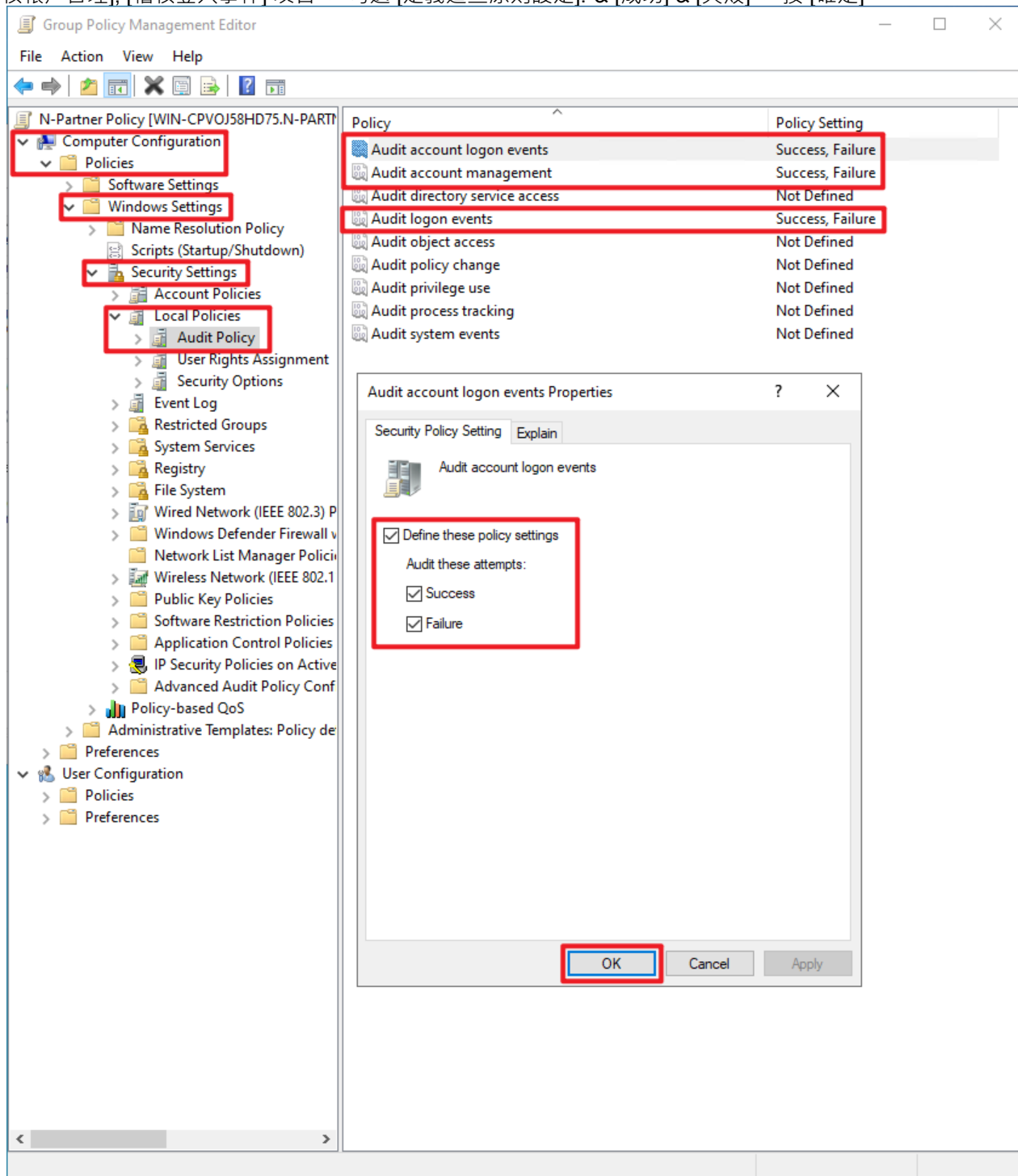
#### (4) 編輯群組原則物件

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



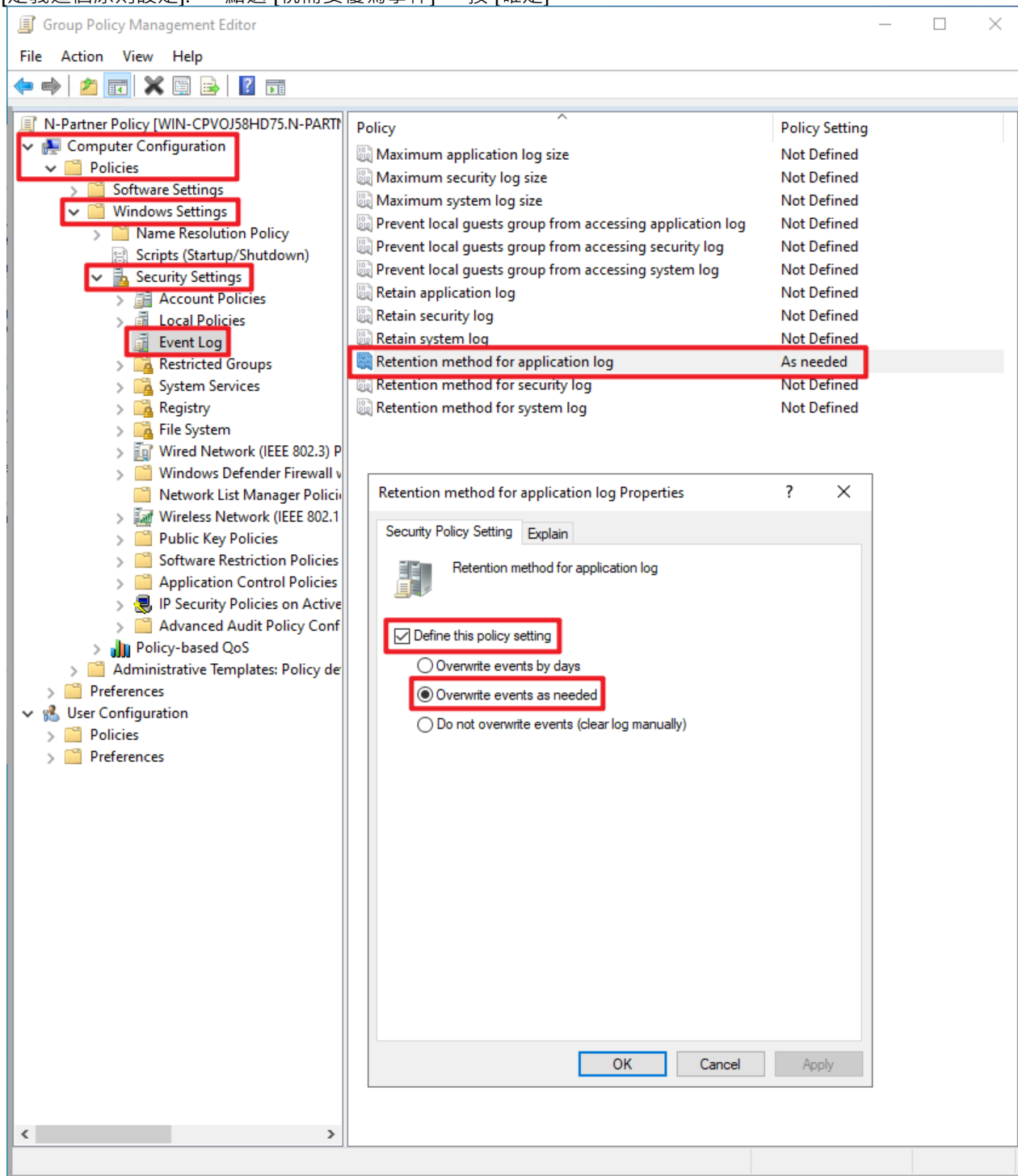
## (5) 本機原則：稽核原則

選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]



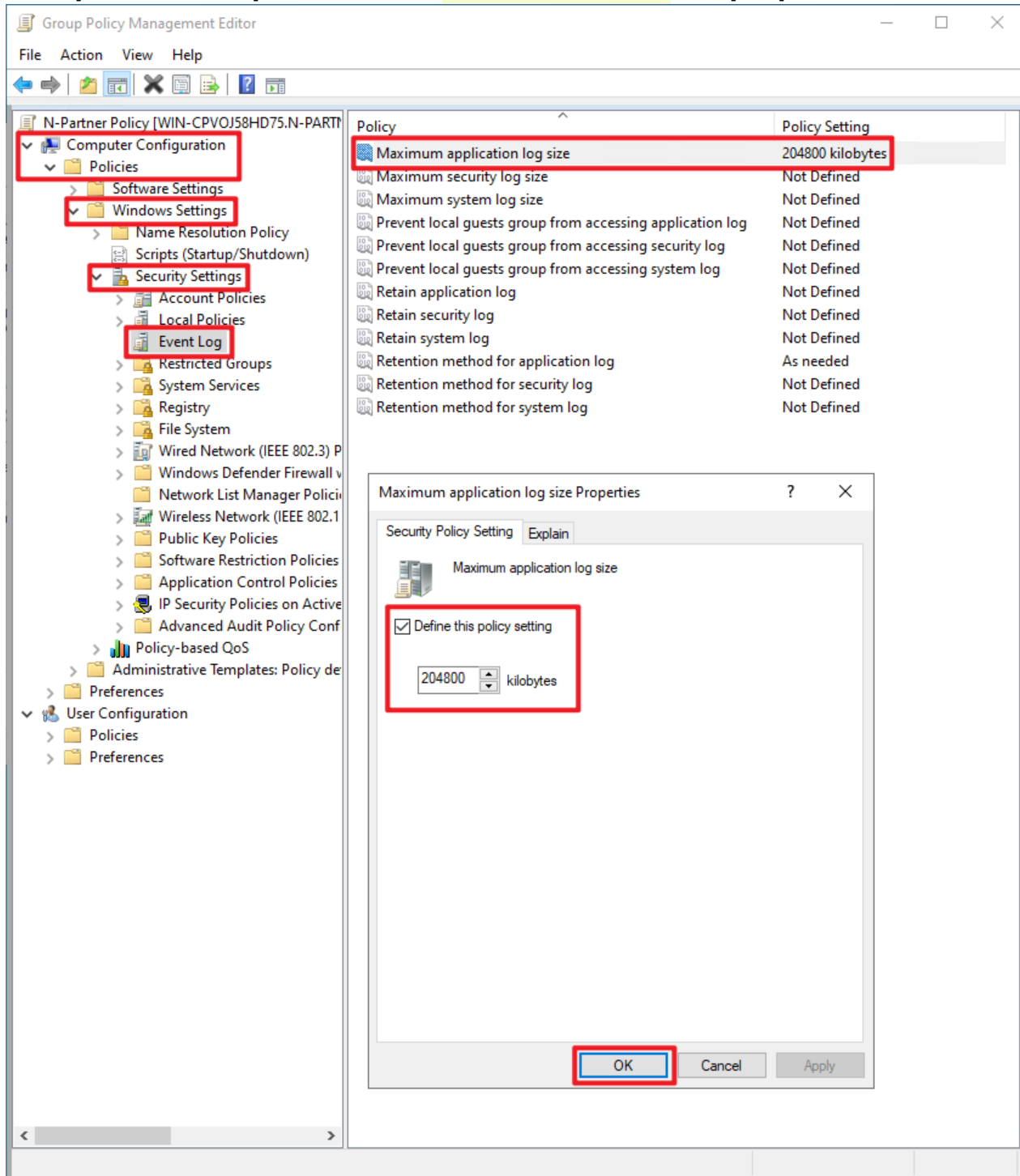
## (6) 事件記錄：應用程式記錄保持方法

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



## (7) 事件記錄：應用程式記錄檔大小最大值

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄檔大小最大值] 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 [Windows PowerShell]



## (9) 更新 MS SQL Server 群組原則

```
PS C:\> Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
```

Administrator: Windows PowerShell

```
PS C:\> Invoke-GPUUpdate -Computer $_.name -RandomDelayInMinutes 0 -Force
```

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

紅色文字部位請輸入 MS SQL Server 伺服器名稱

## (10) 產生 MS SQL Server 伺服器群組原則報表

```
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2022 -Path C:\tmp\SQL2022.html -ReportType.html
```

Administrator: Windows PowerShell

```
PS C:\> Get-GPResultantSetofPolicy -Computer $_.name -Path C:\tmp\SQL2022.html -ReportType html
```

```
RsopMode       : Logging
Namespace      : \\WIN-CPVOJ58HD75\Root\Rsop\NS296D4EEF_936C_483A_A5E7_E4CE37420FE6
LoggingComputer : WIN-CPVOJ58HD75
LoggingUser     : N-PARTNER\Administrator
LoggingMode     : UserAndComputer
```

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

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

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

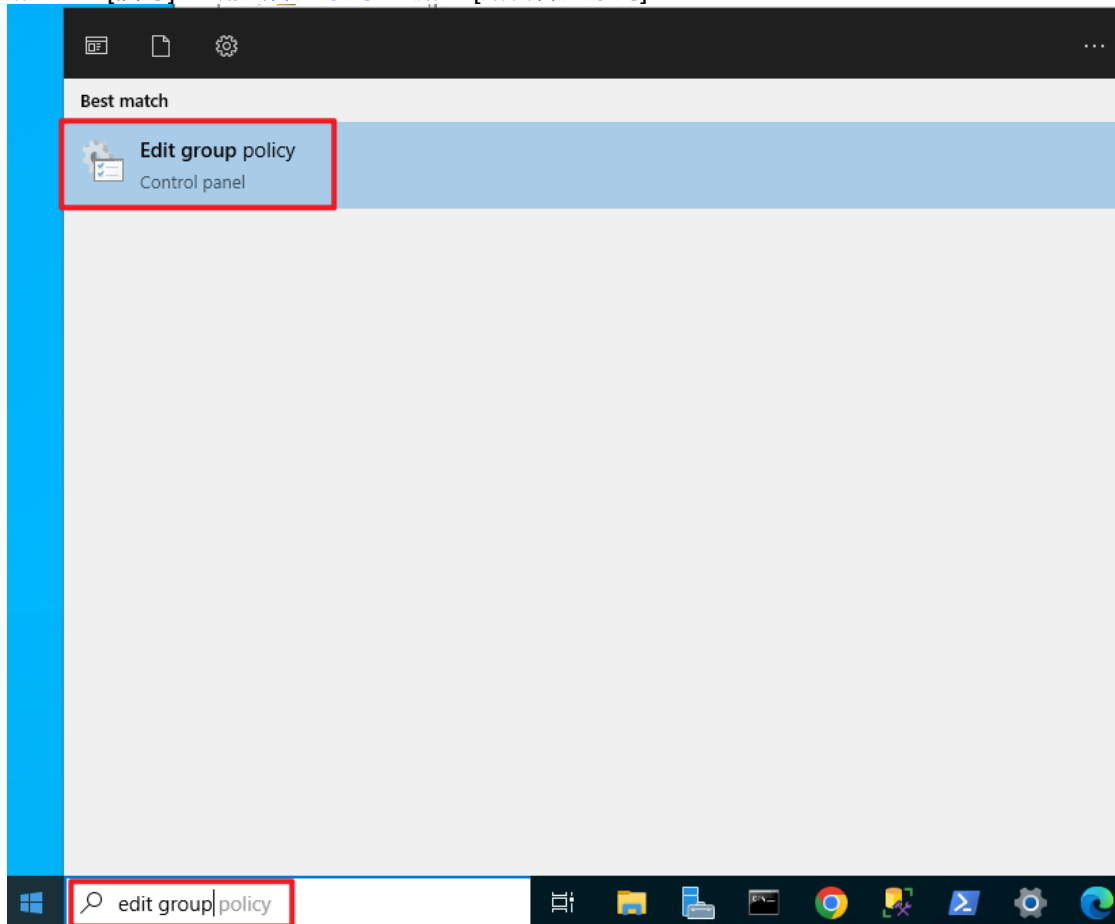
| Group Policy Results                                                       |                  |                  |                          |
|----------------------------------------------------------------------------|------------------|------------------|--------------------------|
| N-PARTNER\Administrator on N-PARTNER\WIN-CPVOJ58HD75                       |                  |                  |                          |
| Data collected on: 7/19/2024 04:35:59 PM                                   |                  |                  | <a href="#">show all</a> |
| <a href="#">Computer Details</a>                                           |                  |                  | <a href="#">hide</a>     |
| General                                                                    |                  |                  | <a href="#">show</a>     |
| Component Status                                                           |                  |                  | <a href="#">show</a>     |
| Settings                                                                   |                  |                  | <a href="#">hide</a>     |
| Policies                                                                   |                  |                  | <a href="#">hide</a>     |
| Windows Settings                                                           |                  |                  | <a href="#">hide</a>     |
| Security Settings                                                          |                  |                  | <a href="#">hide</a>     |
| Account Policies/Password Policy                                           |                  |                  | <a href="#">show</a>     |
| Account Policies/Account Lockout Policy                                    |                  |                  | <a href="#">show</a>     |
| Account Policies/Kerberos Policy                                           |                  |                  | <a href="#">show</a>     |
| Local Policies/Audit Policy                                                |                  |                  | <a href="#">hide</a>     |
| Policy                                                                     | Setting          | Winning GPO      |                          |
| Audit account logon events                                                 | Success, Failure | N-Partner Policy |                          |
| Audit account management                                                   | Success, Failure | N-Partner Policy |                          |
| Audit logon events                                                         | Success, Failure | N-Partner Policy |                          |
| Local Policies/Security Options                                            |                  |                  | <a href="#">show</a>     |
| Event Log                                                                  |                  |                  | <a href="#">hide</a>     |
| Policy                                                                     | Setting          | Winning GPO      |                          |
| Maximum application log size                                               | 204800 kilobytes | N-Partner Policy |                          |
| Retention method for application log                                       | As needed        | N-Partner Policy |                          |
| Public Key Policies/Certificate Services Client - Auto-Enrollment Settings |                  |                  | <a href="#">show</a>     |
| Public Key Policies/Encrypting File System                                 |                  |                  | <a href="#">show</a>     |
| Windows Firewall with Advanced Security                                    |                  |                  | <a href="#">show</a>     |
| Group Policy Objects                                                       |                  |                  | <a href="#">hide</a>     |
| Applied GPOs                                                               |                  |                  | <a href="#">show</a>     |
| Denied GPOs                                                                |                  |                  | <a href="#">show</a>     |
| WMI Filters                                                                |                  |                  | <a href="#">show</a>     |
| <a href="#">User Details</a>                                               |                  |                  | <a href="#">show</a>     |

## 6.3.2 工作群組

### 6.3.2.1 稽核原則設定

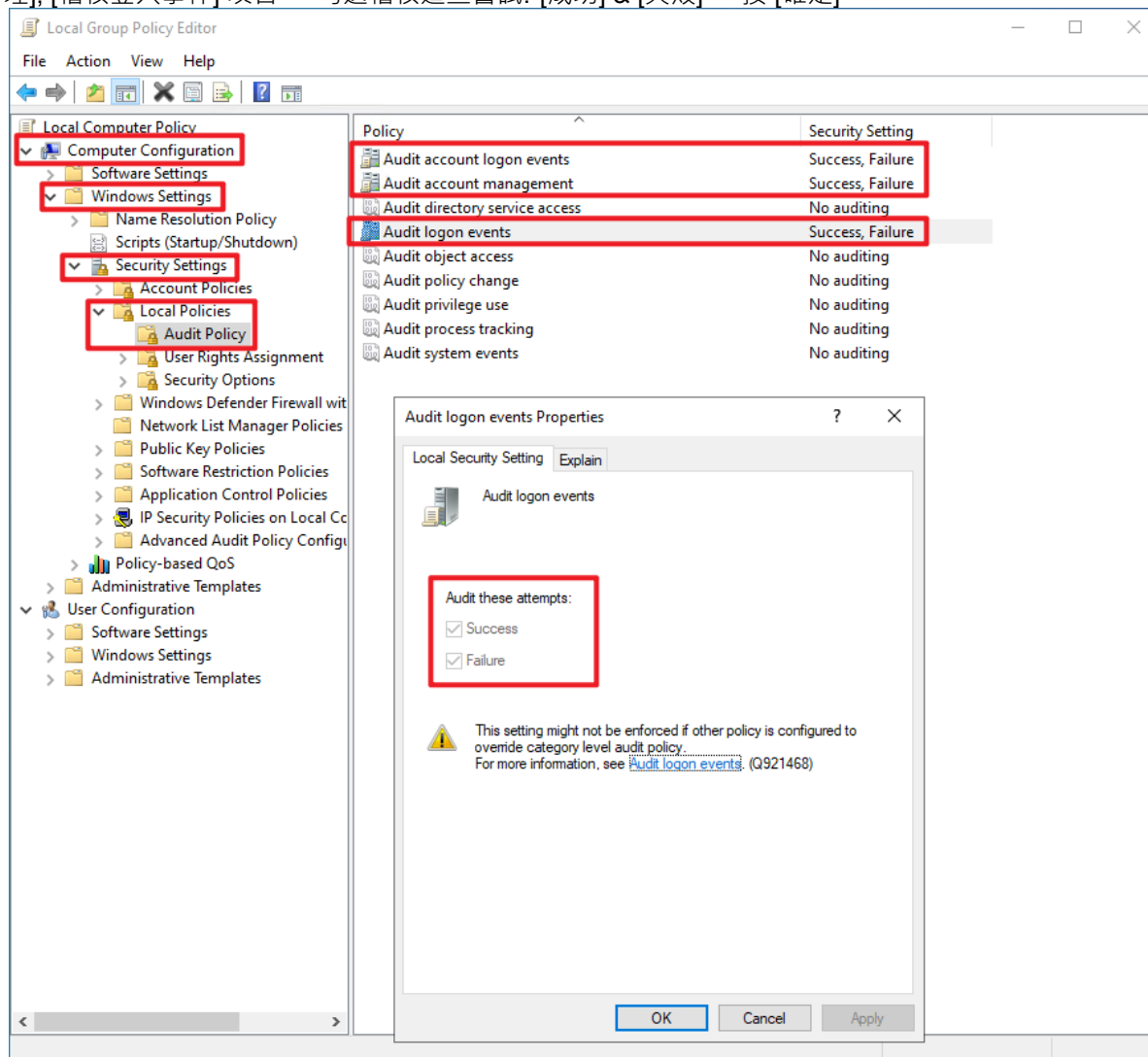
#### (1) 開啟 [本機群組原則編輯器]

點選  [搜尋] -> 輸入 [群組原則](#) -> 點選 [編輯群組原則]



## (2) 本機原則：稽核原則

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



### (3) 開啟 [Windows PowerShell]



### (4) 更新群組原則

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

```
> Administrator: Windows PowerShell
```

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

```
Computer policy update has completed successfully.  
User policy update has completed successfully.
```

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

## (5) 查看群组原则套用情形

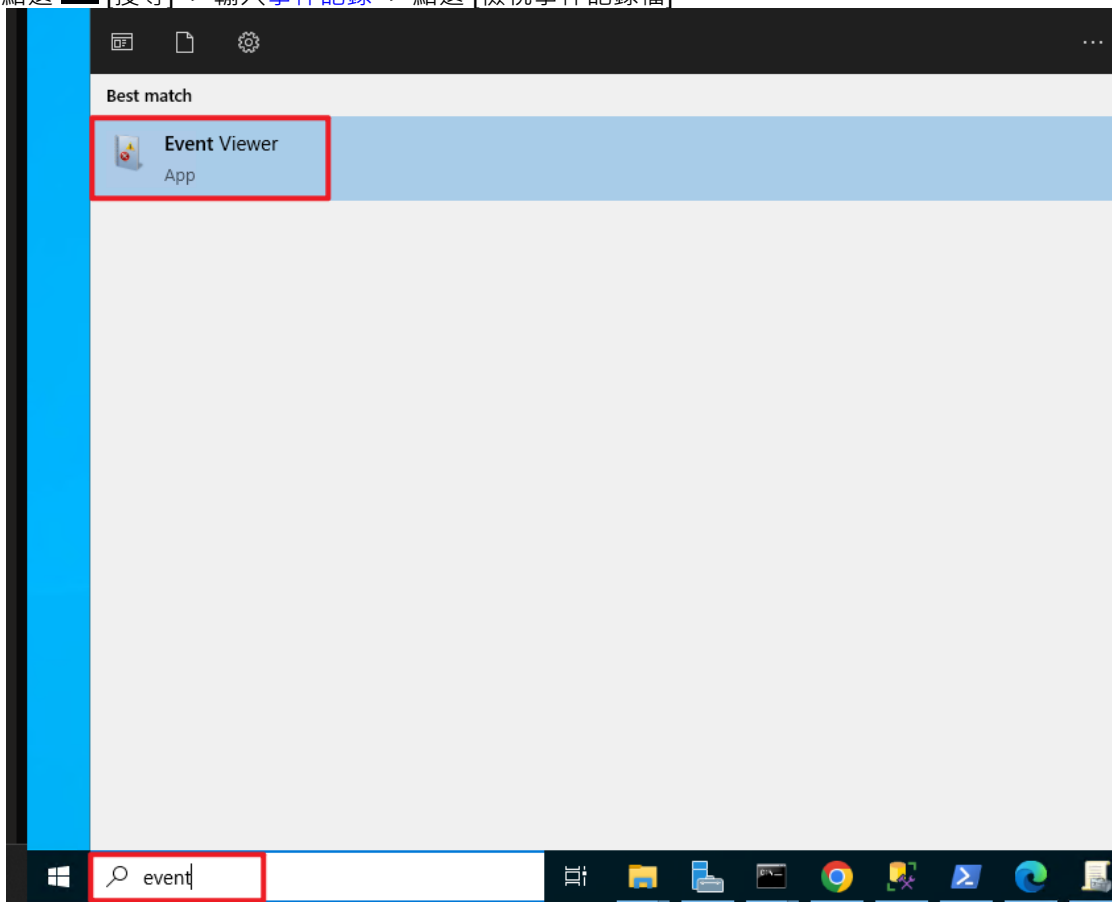
```
PS C:\> auditpol /get /category:*
```

```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension No Auditing
  System Integrity        Success and Failure
  IPsec Driver             No Auditing
  Other System Events      Success and Failure
  Security State Change    Success
Logon/Logoff
  Logon                   Success and Failure
  Logoff                  Success and Failure
  Account Lockout          Success and Failure
  IPsec Main Mode          Success and Failure
  IPsec Quick Mode         Success and Failure
  IPsec Extended Mode      Success and Failure
  Special Logon            Success and Failure
  Other Logon/Logoff Events Success and Failure
  Network Policy Server    Success and Failure
  User / Device Claims     Success and Failure
  Group Membership         Success and Failure
Object Access
  File System              No Auditing
  Registry                 No Auditing
  Kernel Object            No Auditing
  SAM                     No Auditing
  Certification Services   No Auditing
  Application Generated     No Auditing
  Handle Manipulation       No Auditing
  File Share               No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events No Auditing
  Detailed File Share       No Auditing
  Removable Storage        No Auditing
  Central Policy Staging    No Auditing
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events  No Auditing
  Sensitive Privilege Use     No Auditing
Detailed Tracking
  Process Creation          No Auditing
  Process Termination       No Auditing
  DPAPI Activity            No Auditing
  RPC Events                No Auditing
  Plug and Play Events      No Auditing
  Token Right Adjusted Events No Auditing
Policy Change
  Audit Policy Change        Success
  Authentication Policy Change Success
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events  No Auditing
Account Management
  Computer Account Management Success and Failure
  Security Group Management  Success and Failure
  Distribution Group Management Success and Failure
  Application Group Management Success and Failure
  Other Account Management Events Success and Failure
  User Account Management    Success and Failure
DS Access
  Directory Service Access    Success
  Directory Service Changes   No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events  Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation        Success and Failure
PS C:\>
```

### 6.3.2.2 事件檔案設定

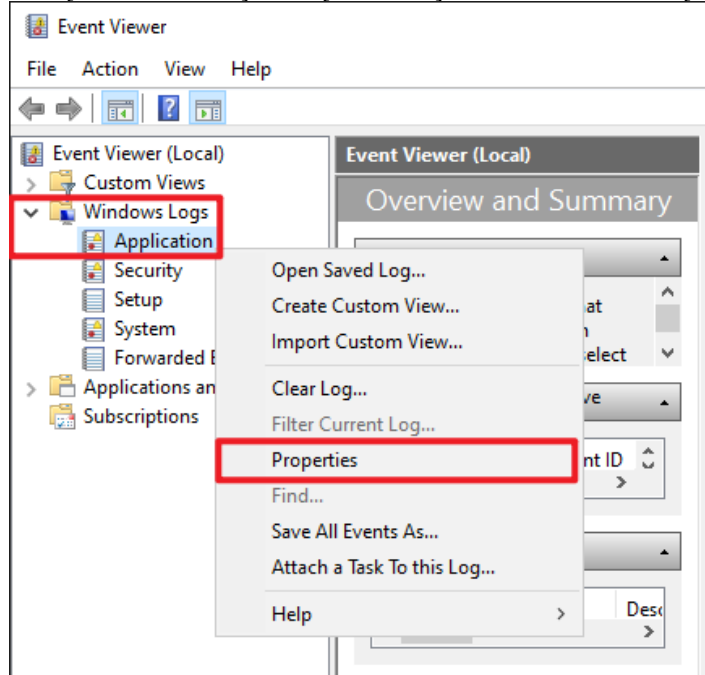
#### (1) 開啟 [檢視事件記錄檔]

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



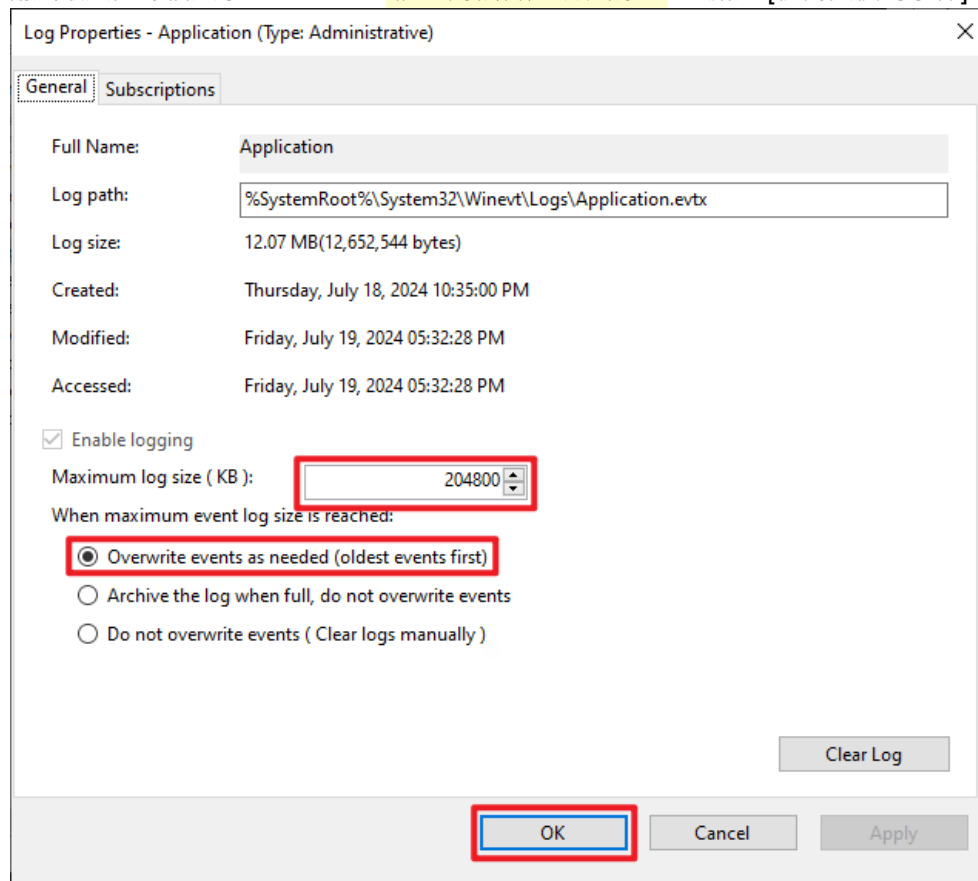
## (2) 編輯安全性記錄

展開 [Windows 記錄] -> 在 [應用程式] 按滑鼠右鍵 -> 點選 [內容]



## (3) 設定應用程式記錄檔

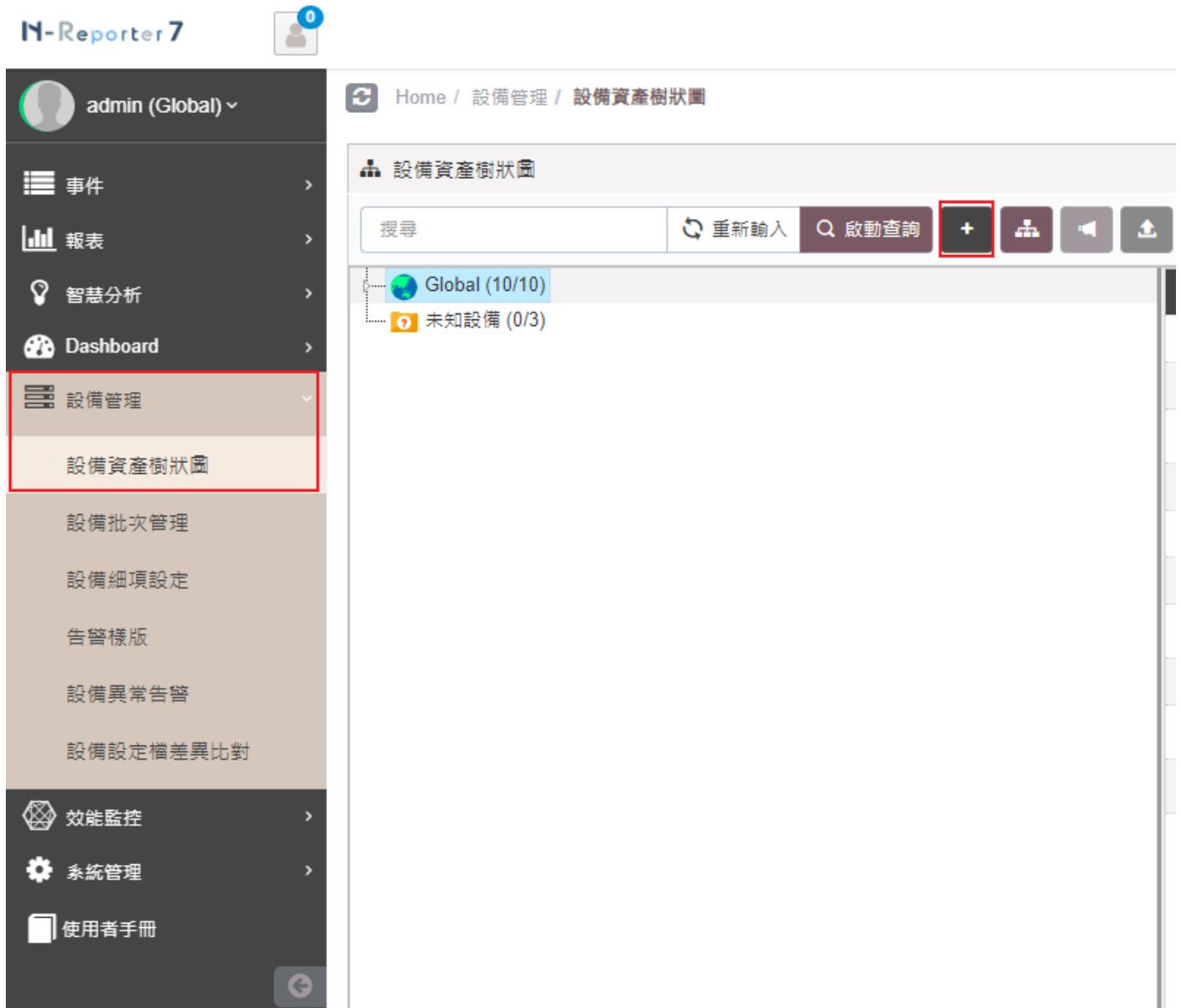
輸入最大記錄檔大小: 204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]



## 7 N-Reporter

### (1) 新增 MS SQL 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



## (2) 選擇設備種類

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



## 7.1 MS SQL Server Event Log

### (1) 設備基本設定

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

新增設備 - 設備基本設定

設備基本設定

設備名稱 \*

MSSQL-192.168.8.196

IP \*

192.168.8.196

所屬領域 \*

Global

Syslog 資料格式 ⓘ

MS SQL

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

未啟用

Web 監控 ⓘ

☐ 啟用網頁監控功能

上一步

下一步

取消

## (2) Syslog 相關設定

Facility 選擇 [(18) local use 2 (local2)]-> 點選 [下一步]

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

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ

(18) local use 2 (local2)

編碼方式

UTF-8

Syslog 正規化資料保留天數上限 ⓘ

Raw Data 保留與轉發

☒ Raw Data 保留

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

☐ 轉發方式將使用來源設備的 IP

上一步 下一步 取消

### (3) 其他

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

新增設備 - 其它

其它

設備 Icon

Host

接收狀態

☒ 啟用 ☐ 停用

經緯度

緯度  經度

上一步 下一步 取消

是否啟用預設報表，將套用至相同廠牌型號設備-> 點擊 [否]

是否啟用預設報表，將套用至相同廠牌型號設備？

是 否

## 7.2 Windows Event Log

### (1) 設備基本設定

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

新增設備 - 設備基本設定

設備基本設定

設備名稱 \*

Windows-192.168.8.196

IP \*

192.168.8.196

所屬領域 \*

Global

Syslog 資料格式 ⓘ

Windows

自定義資料格式 ⓘ +

未啟用

SNMP Model ⓘ

Host Mib

Web 監控 ⓘ

☐ 啟用網頁監控功能

上一步

下一步

取消

## (2) Syslog 相關設定

Facility 選擇 [(17) local use 1 (local1)]-> 點選 [下一步]

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

新增設備 - Syslog 相關設定

Syslog 相關設定

Facility ⓘ

(17) local use 1 (local1)

編碼方式

UTF-8

Syslog 正規化資料保留天數上限 ⓘ

Raw Data 保留與轉發

☒ Raw Data 保留

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

☐ 轉發方式將使用來源設備的 IP

上一步 下一步 取消

### (3) 其他

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

新增設備 - 其它

其它

設備 Icon

Host

接收狀態

☒ 啟用 ☐ 停用

經緯度

緯度  經度

上一步 下一步 取消

是否啟用預設報表，將套用至相同廠牌型號設備-> 點擊 [否]

是否啟用預設報表，將套用至相同廠牌型號設備？

是 否

## 8 問題排除

### 8.1 Invoke-GPUUpdate 錯誤

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

```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
Invoke-GPUUpdate : Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled
Tasks Management Firewall rules are disabled.
Parameter name: computer
At line:1 char:1
+ Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
+ ~~~~~
+ CategoryInfo          : OperationTimeout: (:) [Invoke-GPUUpdate], ArgumentException
+ FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUUpdateCommand

PS C:\>
```

(2) 在 Windows Server 開啟 [Windows PowerShell]



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

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

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

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

PS C:\>
```

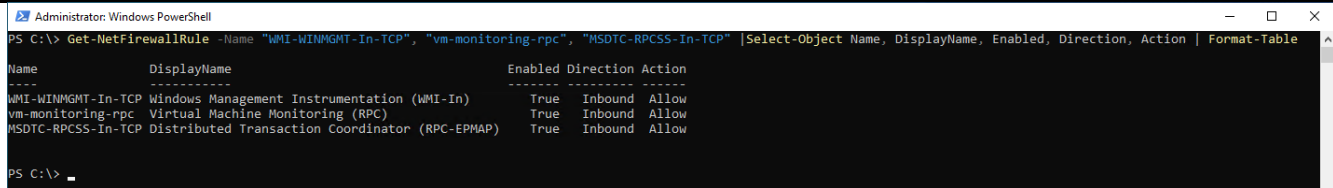
(4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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

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

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

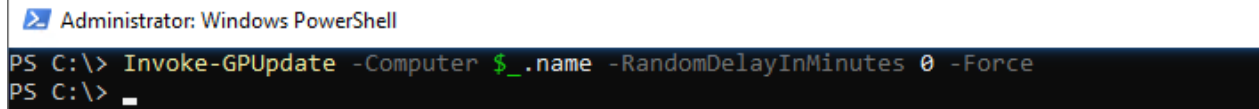
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |  
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



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

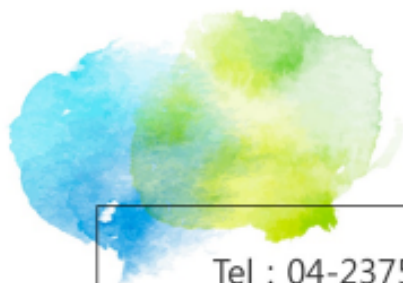
(6) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

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



```
Administrator: Windows PowerShell  
PS C:\> Invoke-GPUUpdate -Computer $_.name -RandomDelayInMinutes 0 -Force  
PS C:\>
```

紅色文字部位請輸入 Windows Server 伺服器名稱



Tel : 04-23752865    Fax : 04-23757458

業務詢問 : [sales@npartner.com](mailto:sales@npartner.com)

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