

Partner

如何設定

MS SQL 稽核事件記錄

V019

2022/06/16



版權聲明

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

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言	2	3.3.2.1 稽核原則設定.....	105
1. NXLog	3	3.3.2.2 事件檔案設定.....	109
1.1 NXLog 安裝.....	3	4. SQL 2016.....	112
1.2 NXLog 設定檔下載.....	4	4.1 稽核登入.....	112
1.2.1 MS SQL 單機設定檔.....	4	4.1.1 使用圖形介面方式設定	112
1.2.2 MS SQL Cluster 叢集設定檔	5	4.1.2 使用指令介面方式設定	117
1.3 NXLog 設定檔	6	4.2 設定稽核.....	119
1.3.1 MS SQL 單機設定檔.....	6	4.2.1 稽核伺服器層級.....	119
1.3.2 MS SQL Cluster 叢集設定檔	8	4.2.1.1 使用圖形介面方式設定	119
1.4 NXLog 啟動服務.....	10	4.2.1.2 使用指令介面方式設定	127
2. SQL 2008.....	13	4.2.2 稽核資料庫層級.....	130
2.1 稽核登入.....	13	4.2.2.1 使用圖形介面方式設定	130
2.1.1 使用圖形介面方式設定	13	4.2.2.2 使用指令介面方式設定	139
2.1.2 使用指令介面方式設定	18	4.3 事件記錄檔設定	142
2.2 設定稽核.....	21	4.3.1 網域.....	142
2.2.1 稽核伺服器層級	21	4.3.1.1 組織單位設定.....	142
2.2.1.1 使用圖形介面方式設定	21	4.3.1.2 群組原則設定.....	147
2.2.1.2 使用指令介面方式設定	29	4.3.2 工作群組.....	154
2.2.2 稽核資料庫層級.....	32	4.3.2.1 稽核原則設定.....	154
2.2.2.1 使用圖形介面方式設定	32	4.3.2.2 事件檔案設定.....	158
2.2.2.2 使用指令介面方式設定	41	5. SQL 2019.....	161
2.3 事件記錄檔設定	44	5.1 稽核登入.....	161
2.3.1 網域.....	44	5.1.1 使用圖形介面方式設定	161
2.3.1.1 組織單位設定.....	44	5.1.2 使用指令介面方式設定	166
2.3.1.2 群組原則設定.....	48	5.2 設定稽核.....	168
2.3.2 工作群組.....	55	5.2.1 稽核伺服器層級.....	168
2.3.2.1 稽核原則設定.....	55	5.2.1.1 使用圖形介面方式設定	168
2.3.2.2 事件檔案設定.....	59	5.2.1.2 使用指令介面方式設定	176
3. SQL 2012.....	62	5.2.2 稽核資料庫層級.....	179
3.1 稽核登入.....	62	5.2.2.1 使用圖形介面方式設定	179
3.1.1 使用圖形介面方式設定	62	5.2.2.2 使用指令介面方式設定	188
3.1.2 使用指令介面方式設定	67	5.3 事件記錄檔設定	191
3.2 設定稽核.....	70	5.3.1 網域.....	191
3.2.1 稽核伺服器層級.....	70	5.3.1.1 組織單位設定.....	191
3.2.1.1 使用圖形介面方式設定	70	5.3.1.2 群組原則設定.....	196
3.2.1.2 使用指令介面方式設定	78	5.3.2 工作群組.....	203
3.2.2 稽核資料庫層級.....	81	5.3.2.1 稽核原則設定.....	203
3.2.2.1 使用圖形介面方式設定	81	5.3.2.2 事件檔案設定.....	207
3.2.2.2 使用指令介面方式設定	90	6. N-Reporter	210
3.3 事件記錄檔設定	93	6.1 MS SQL Server Event Log.....	211
3.3.1 網域.....	93	6.2 Windows Event Log	212
3.3.1.1 組織單位設定.....	93		
3.3.1.2 群組原則設定.....	98		
3.3.2 工作群組.....	105		

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 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://docs.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 and 2019
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-3.0.2272.msi



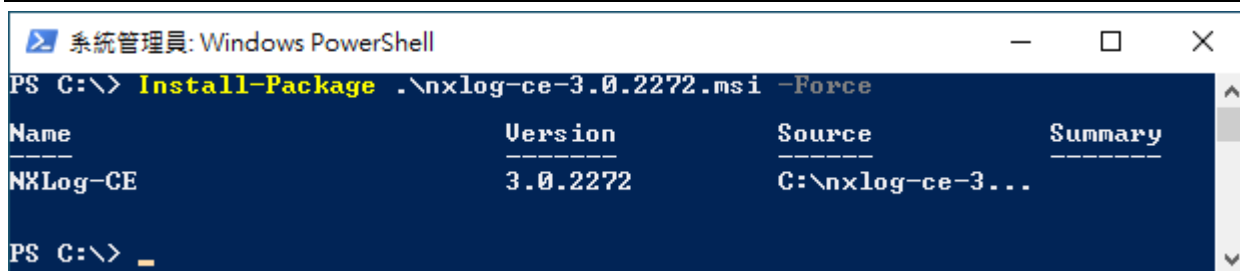
註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog · 開啟 [Windows PowerShell]



(3) 安裝 NXLog 軟體

```
PS C:\> Install-Package -Name .\nxlog-ce-3.0.2272.msi -Force
```



紅色文字部位請輸入 NXLog 軟體路徑和檔案

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

```
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 版本，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

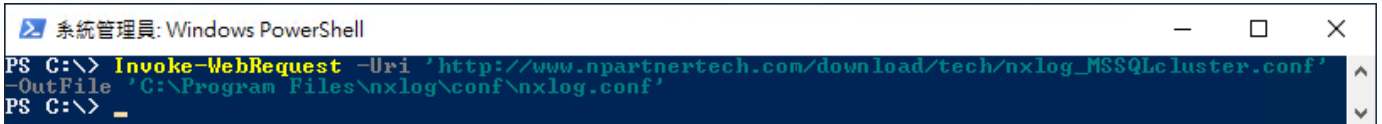
(1) 開啟 [Windows PowerShell]



(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

```
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 版本，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=5061)]]</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> \
<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
```

本文件範例是 NXLog 64bit 版本 · 若是 NXLog 32bit 版本請改為以下設定

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

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> \
```

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=5061)]]</Select> \
    </Query> \
  </QueryList>
</Input>
```

```

<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> \
<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
```

本文件範例是 NXLog 64bit 版本 · 若是 NXLog 32bit 版本請改為以下設定

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

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> \
```

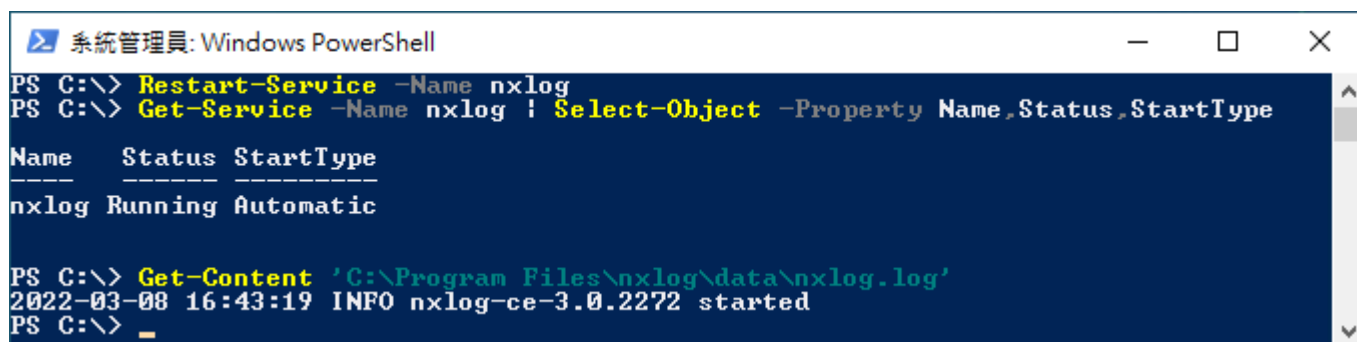
1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



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

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

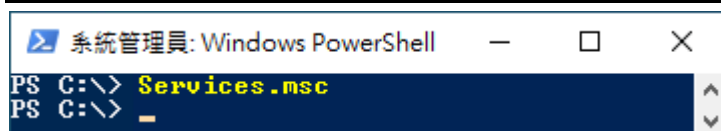
A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the following commands and output:

```
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

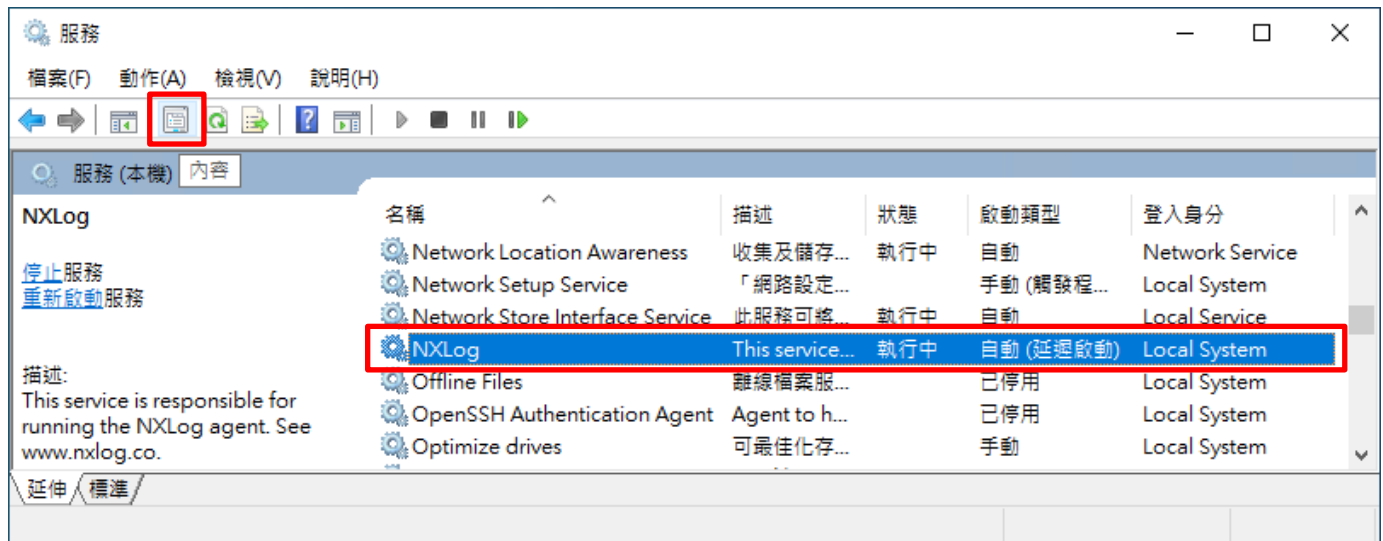
```
PS C:\> Services.msc
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the following commands and output:

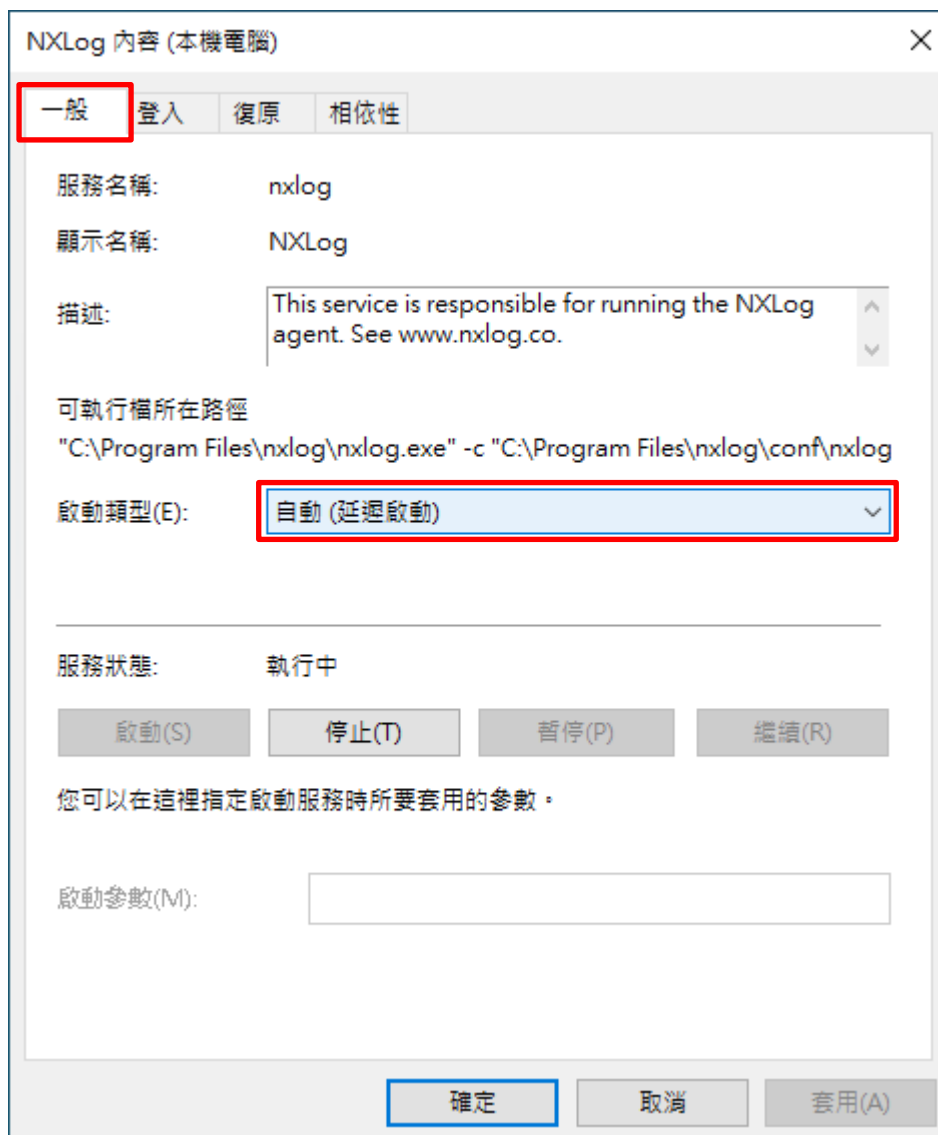
```
PS C:\> Services.msc
PS C:\> _
```

(4) 開啟 NXLog 服務內容

選擇 [NXLog] -> 點選  [內容]



(5) [一般] 頁面 -> 確認；啟動類型: [自動 (延遲啟動)]



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

NXLog 內容 (本機電腦)

一般 登入 **復原** 相依性

選取此服務失敗時的電腦回應。 [協助我設定復原動作。](#)

第一次失敗時(F): 重新啟動服務

第二次失敗時(S): 重新啟動服務

後續失敗時(U): 重新啟動服務

經過下列天數後重設失敗計數(O): 1 天

經過下列時間後重新啟動服務(V): 1 分鐘

啟用對因錯誤而停止所採取的動作。 電腦重新啟動的選項(R)...

執行程式

程式(P): 瀏覽(B)...

命令列參數(C):

將失敗計數附加到命令列結尾 (/fail=%1%)(E)

確定 取消 套用(A)

2. SQL 2008

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

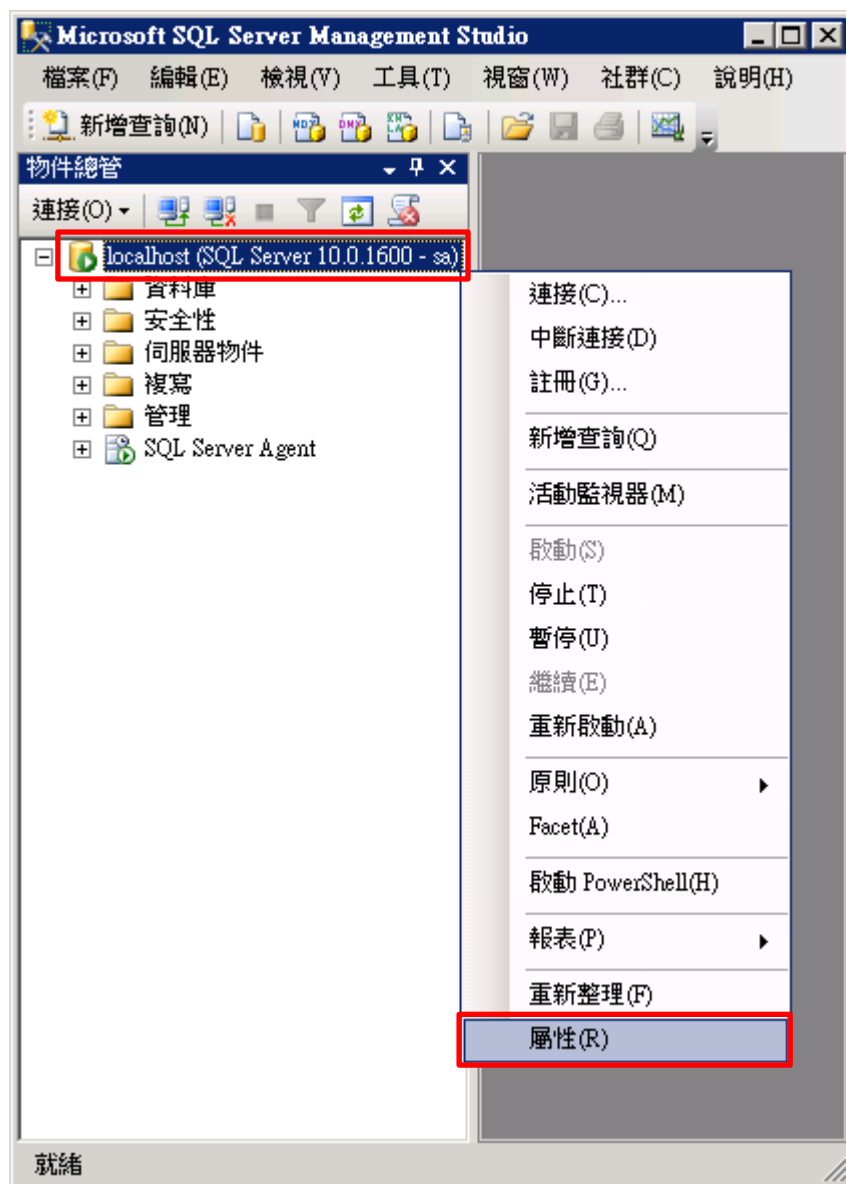
(1) 開啟 [SQL Server Management Studio]



(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]

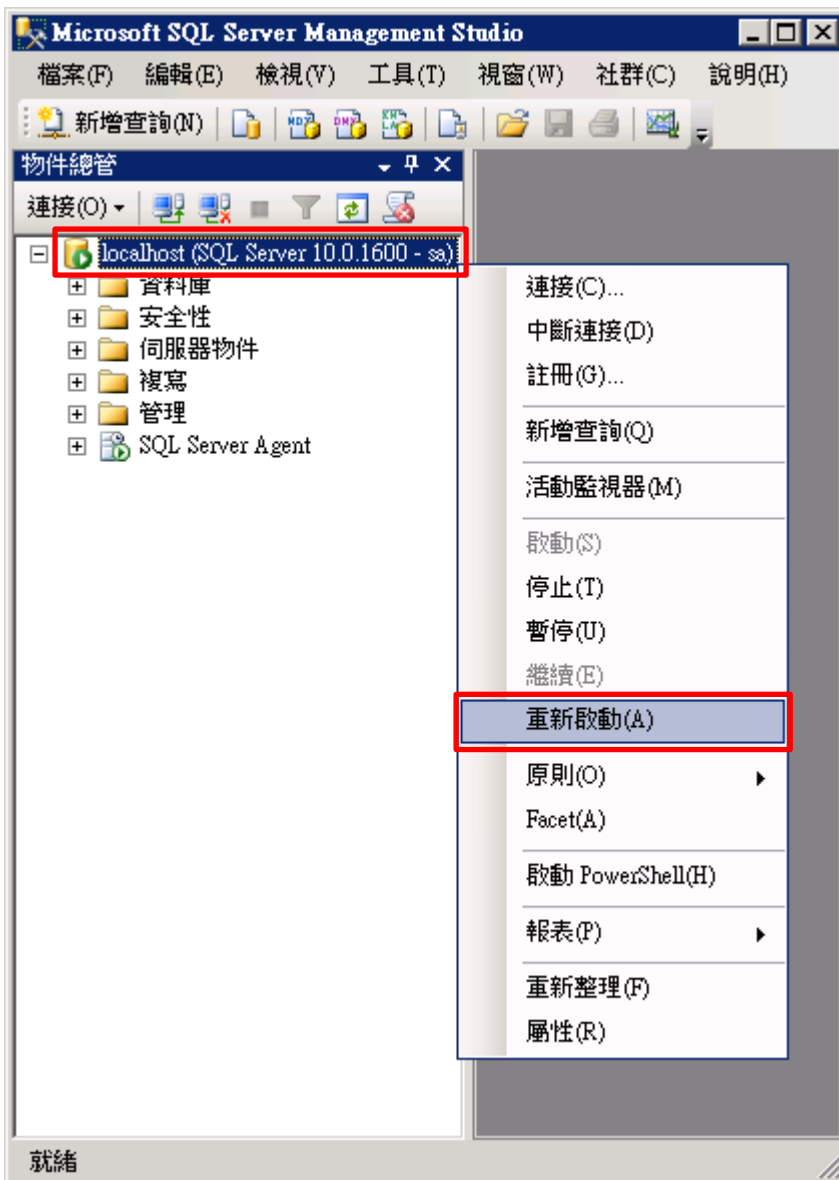


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

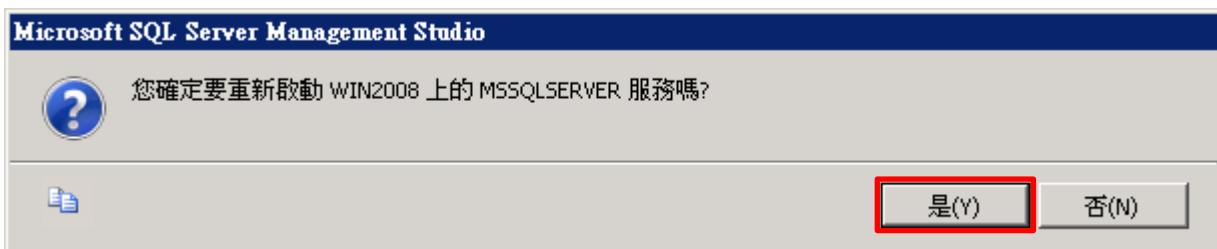


(5) 重新啟動 MS SQL SERVER 服務

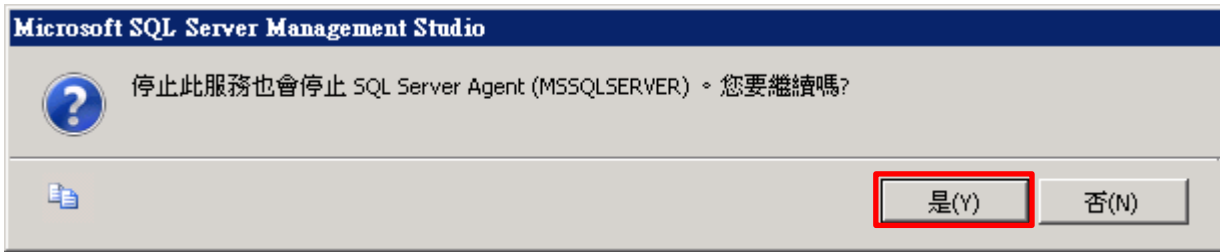
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(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
```

A screenshot of a Windows PowerShell window titled "SQLCMD". The window shows the command prompt with the text "Windows PowerShell Copyright (C) 2016 Microsoft Corporation. All rights reserved. PS C:\Windows\system32> sqlcmd -S localhost -U sa". Below the command, the text "密碼:" (Password:) is displayed, followed by a cursor and the number "1" entered as the password.

Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

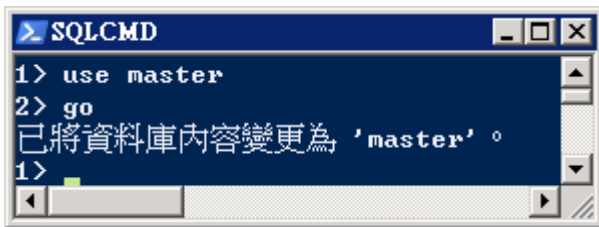
<2.2> 使用 Windows 帳號

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

A screenshot of a Windows PowerShell window titled "SQLCMD". The window shows the command prompt with the text "Windows PowerShell Copyright (C) 2016 Microsoft Corporation. All rights reserved. PS C:\Windows\system32> sqlcmd -S localhost -A". Below the command, the text "1>" is displayed, indicating a successful connection.

(3) 切換資料庫

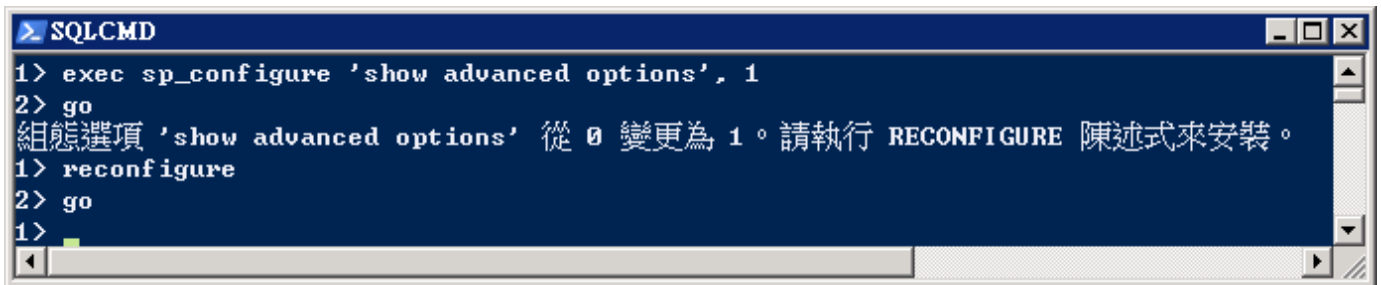
```
1 > use master
2 > go
```



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

(4) 使用 sp_configure 列出進階選項

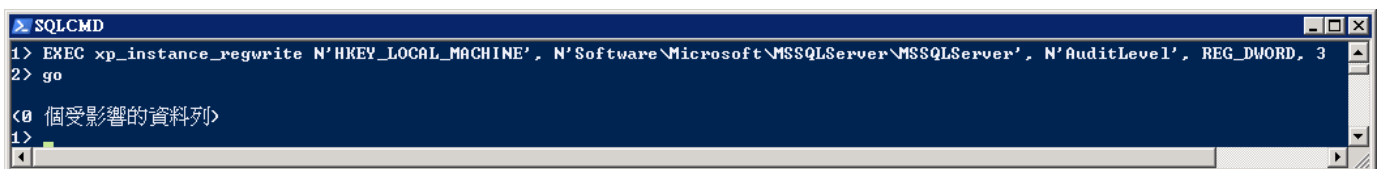
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
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

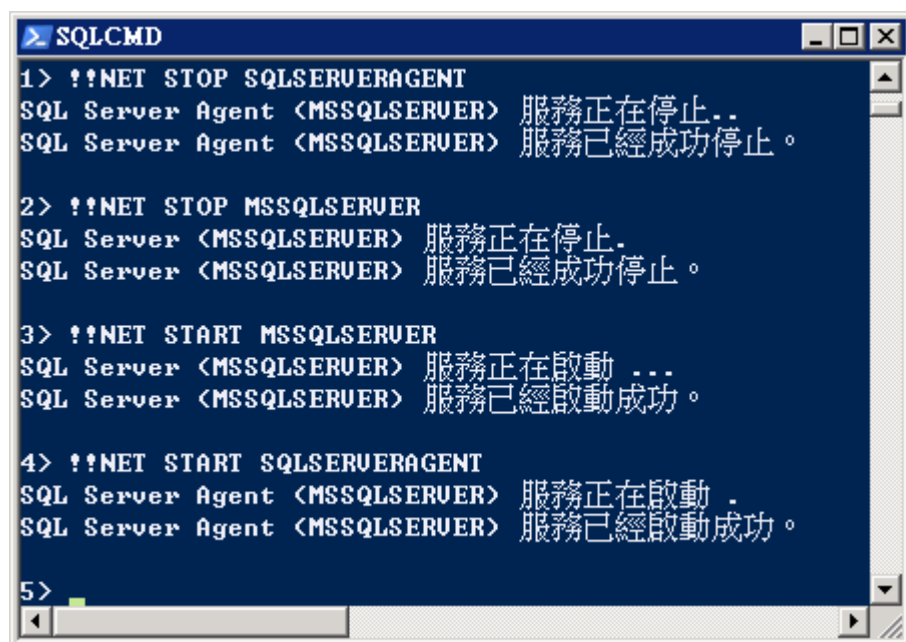
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
```



```
SQLCMD
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>
```

(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
```



```
> SQLCMD
1> !!NET STOP SQLSERVERAGENT
SQL Server Agent <MSSQLSERVER> 服務正在停止..
SQL Server Agent <MSSQLSERVER> 服務已經成功停止。

2> !!NET STOP MSSQLSERVER
SQL Server <MSSQLSERVER> 服務正在停止.
SQL Server <MSSQLSERVER> 服務已經成功停止。

3> !!NET START MSSQLSERVER
SQL Server <MSSQLSERVER> 服務正在啟動 ...
SQL Server <MSSQLSERVER> 服務已經啟動成功。

4> !!NET START SQLSERVERAGENT
SQL Server Agent <MSSQLSERVER> 服務正在啟動 .
SQL Server Agent <MSSQLSERVER> 服務已經啟動成功。

5>
```

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

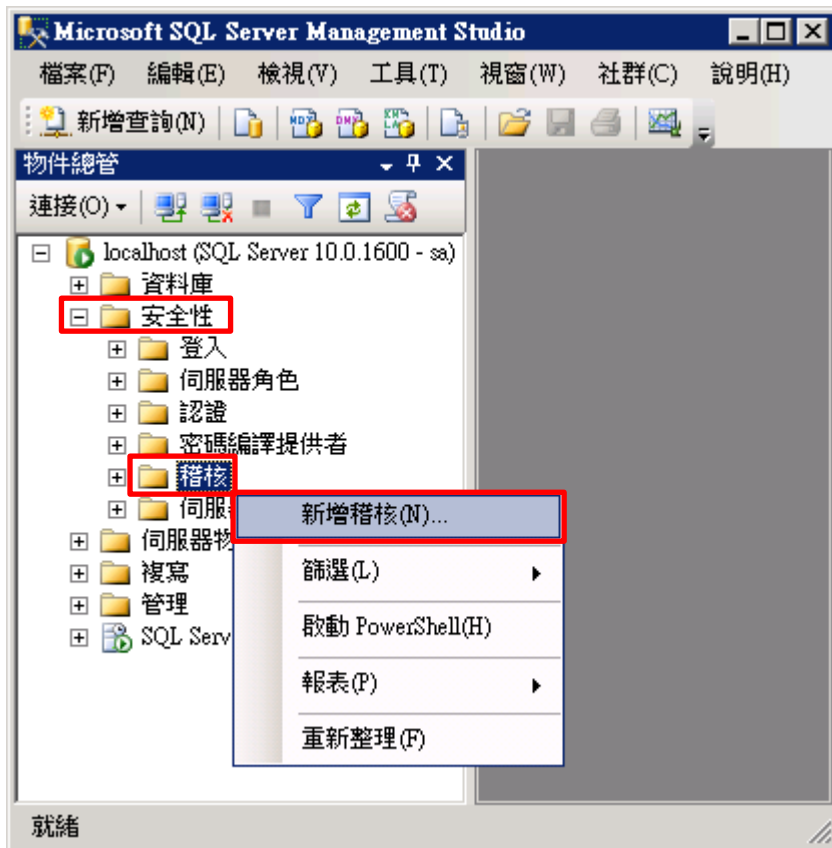
(1) 開啟 [SQL Server Management Studio]



(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]

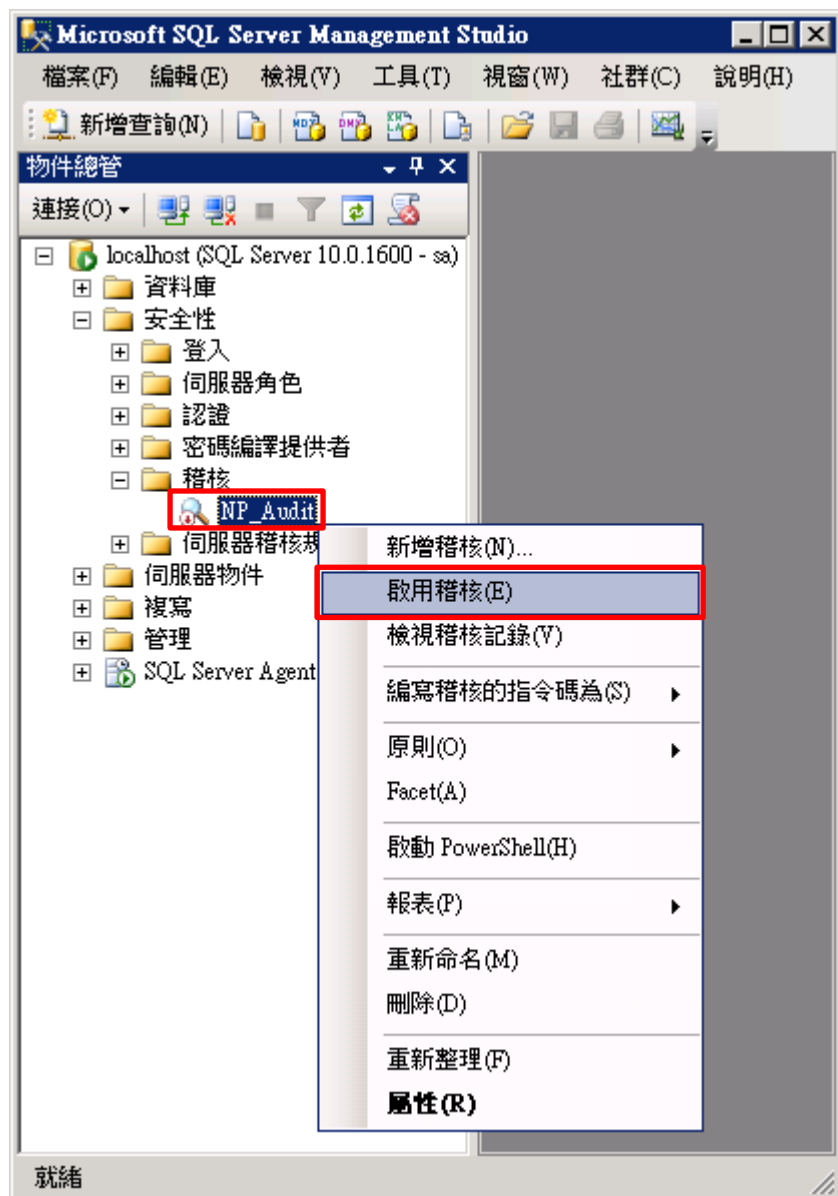
[檢視連接屬性](#)

進度

就緒

確定 取消 說明

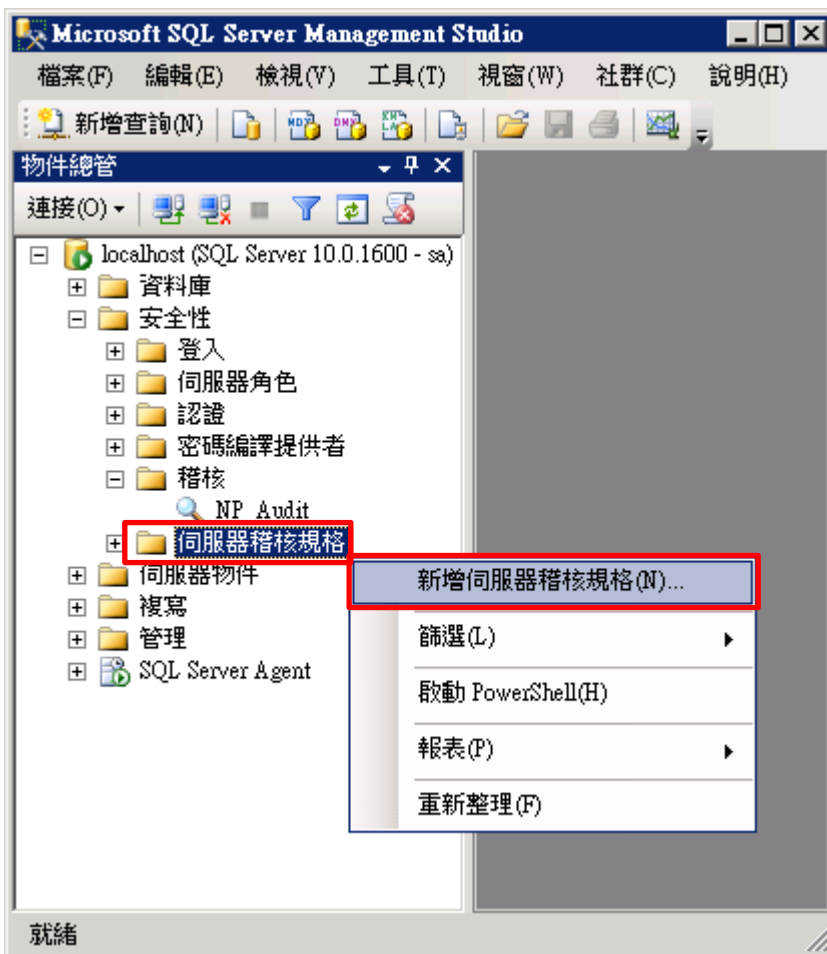
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



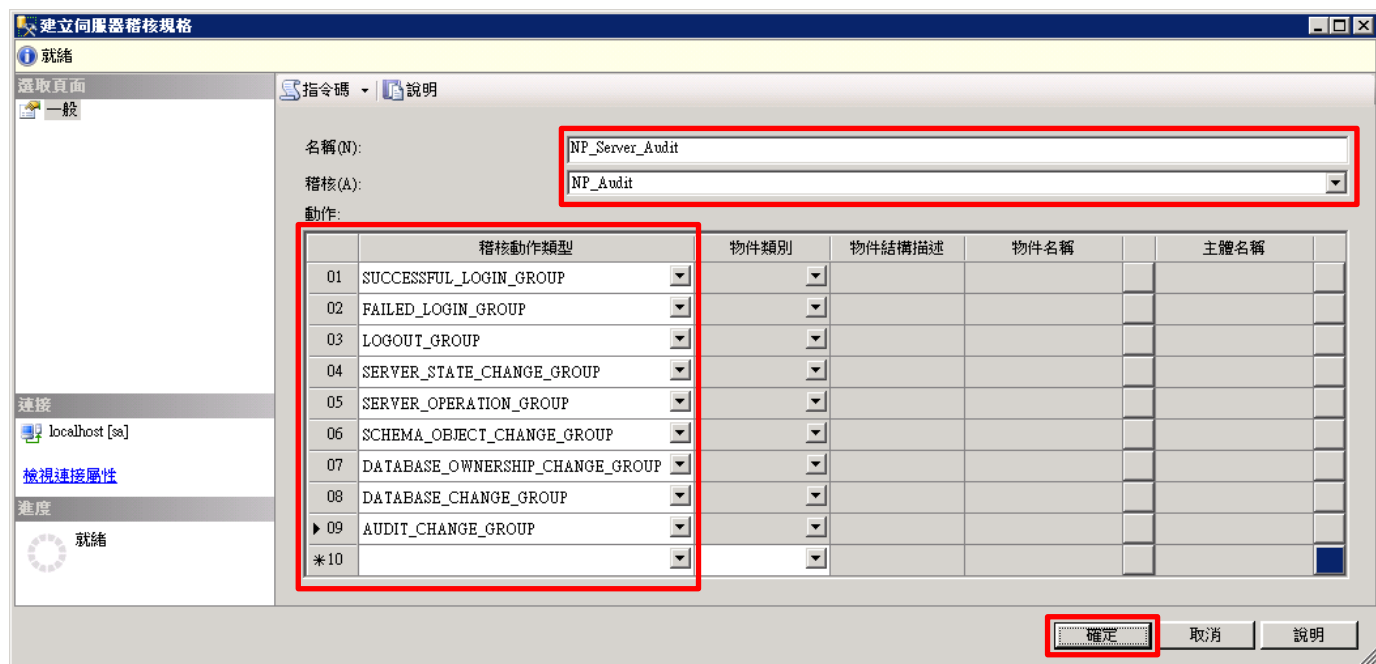
(6) 按 [關閉]



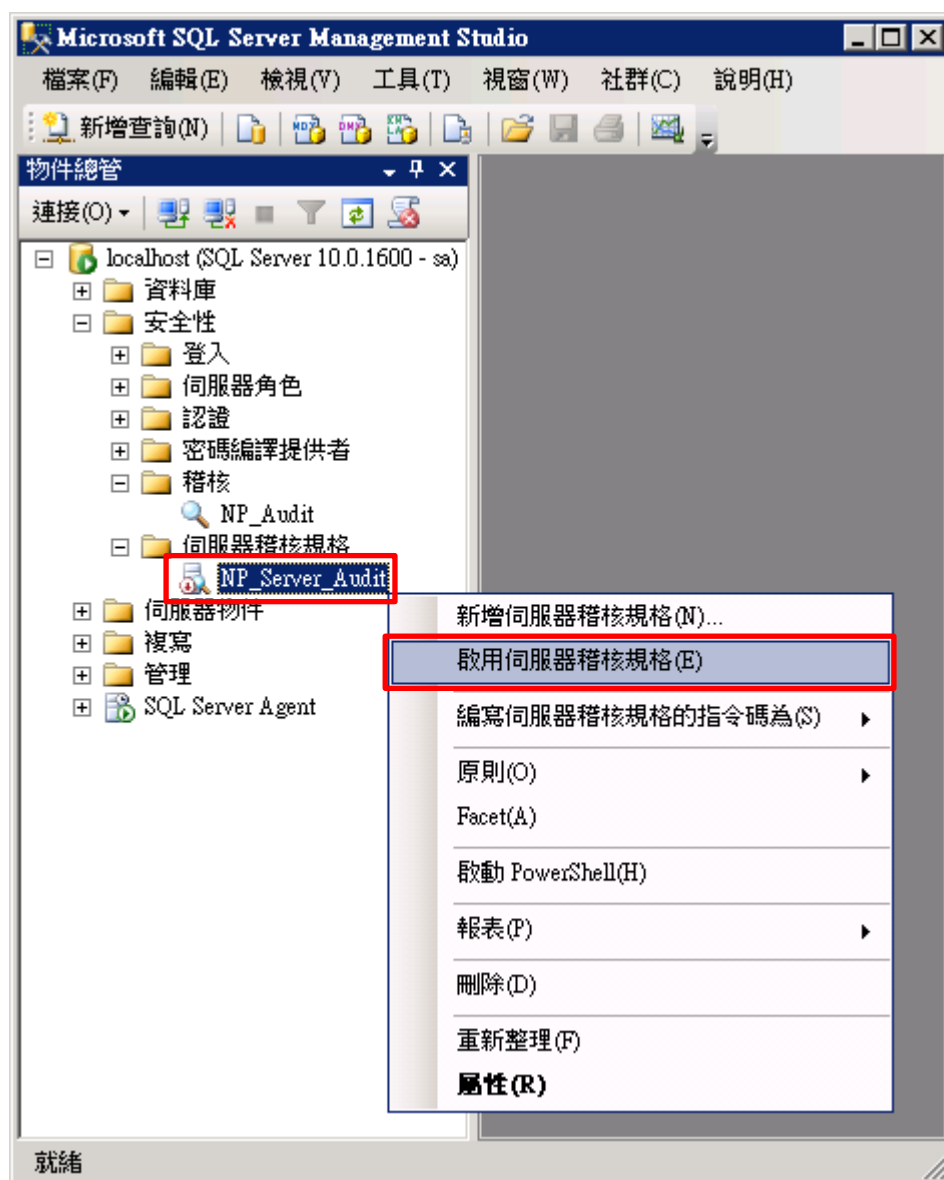
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



(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

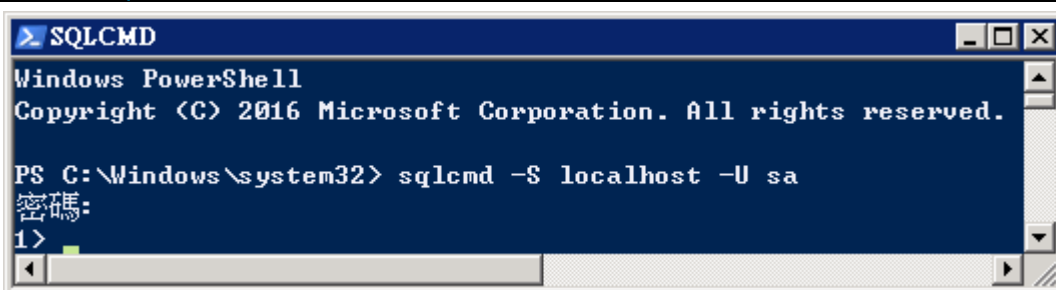
(1) 開啟 [Windows Powershell]



(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
```

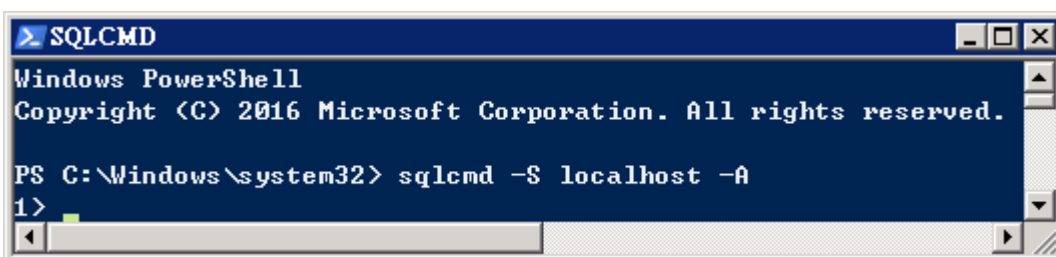


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

<2.2> 使用 Windows 帳號

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



(3) 切換資料庫

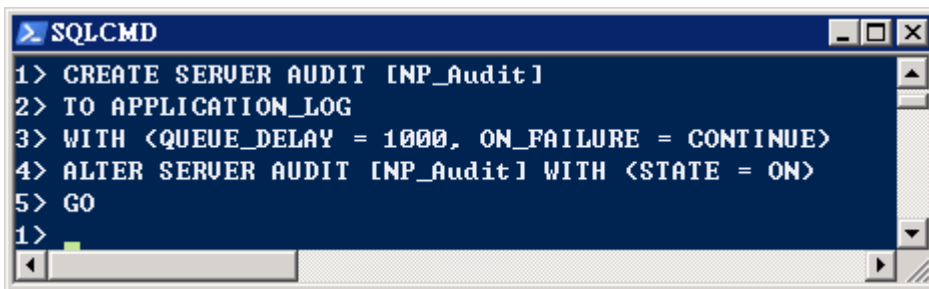
```
1 > use master  
2 > go
```



```
SQLCMD  
1> use master  
2> go  
已將資料庫內容變更為 '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
```

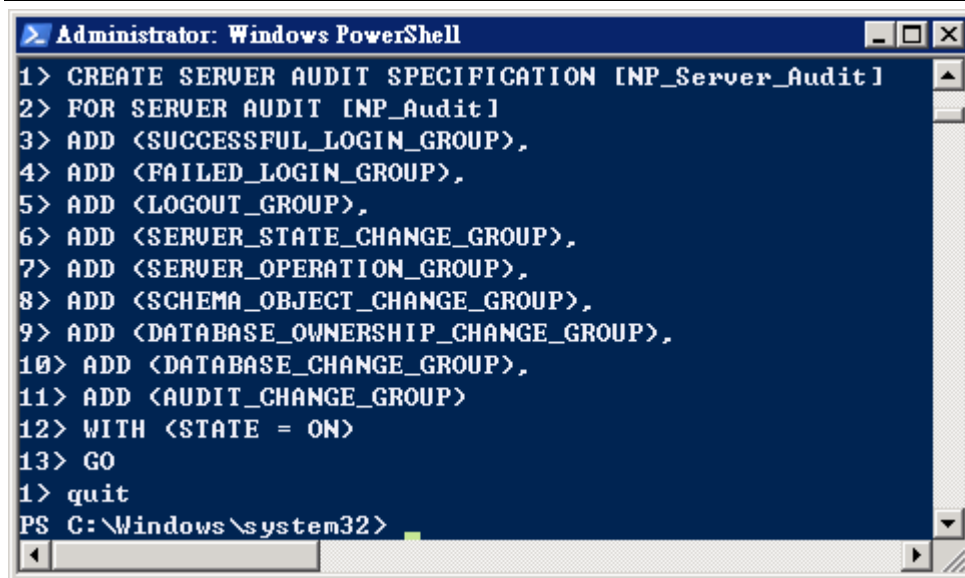


```
SQLCMD  
1> CREATE SERVER AUDIT [NP_Audit]  
2> TO APPLICATION_LOG  
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)  
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)  
5> GO  
1>
```

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 > WITH (STATE = ON)
13 > GO
1 > quit
```



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The terminal displays the following commands and their execution:

```
> Administrator: 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> WITH <STATE = ON>
13> 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

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

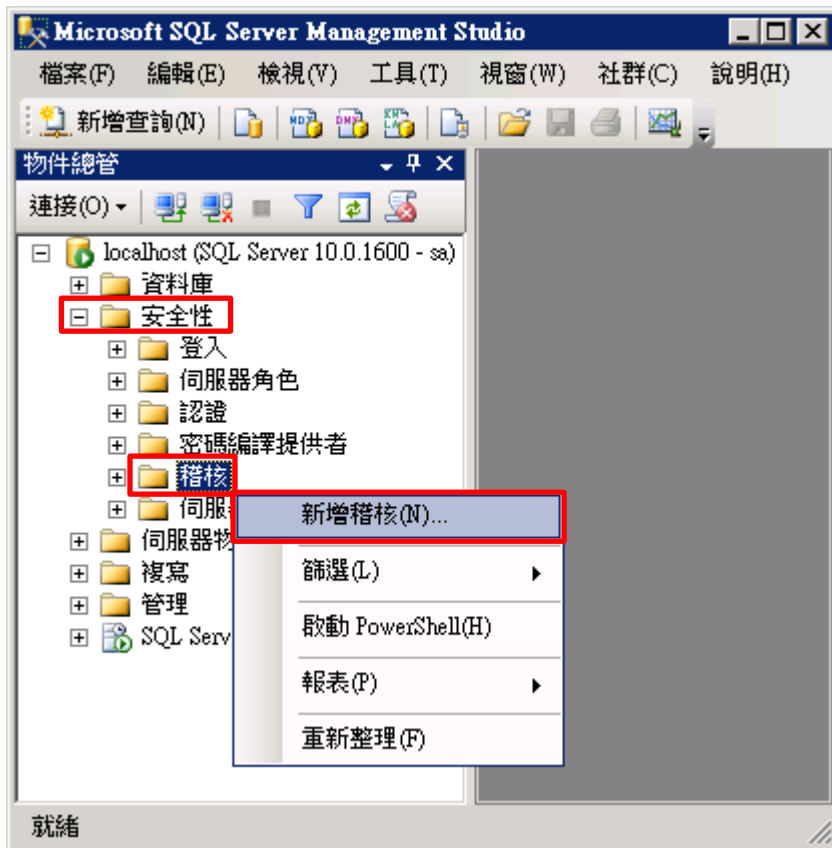
(1) 開啟 [SQL Server Management Studio]



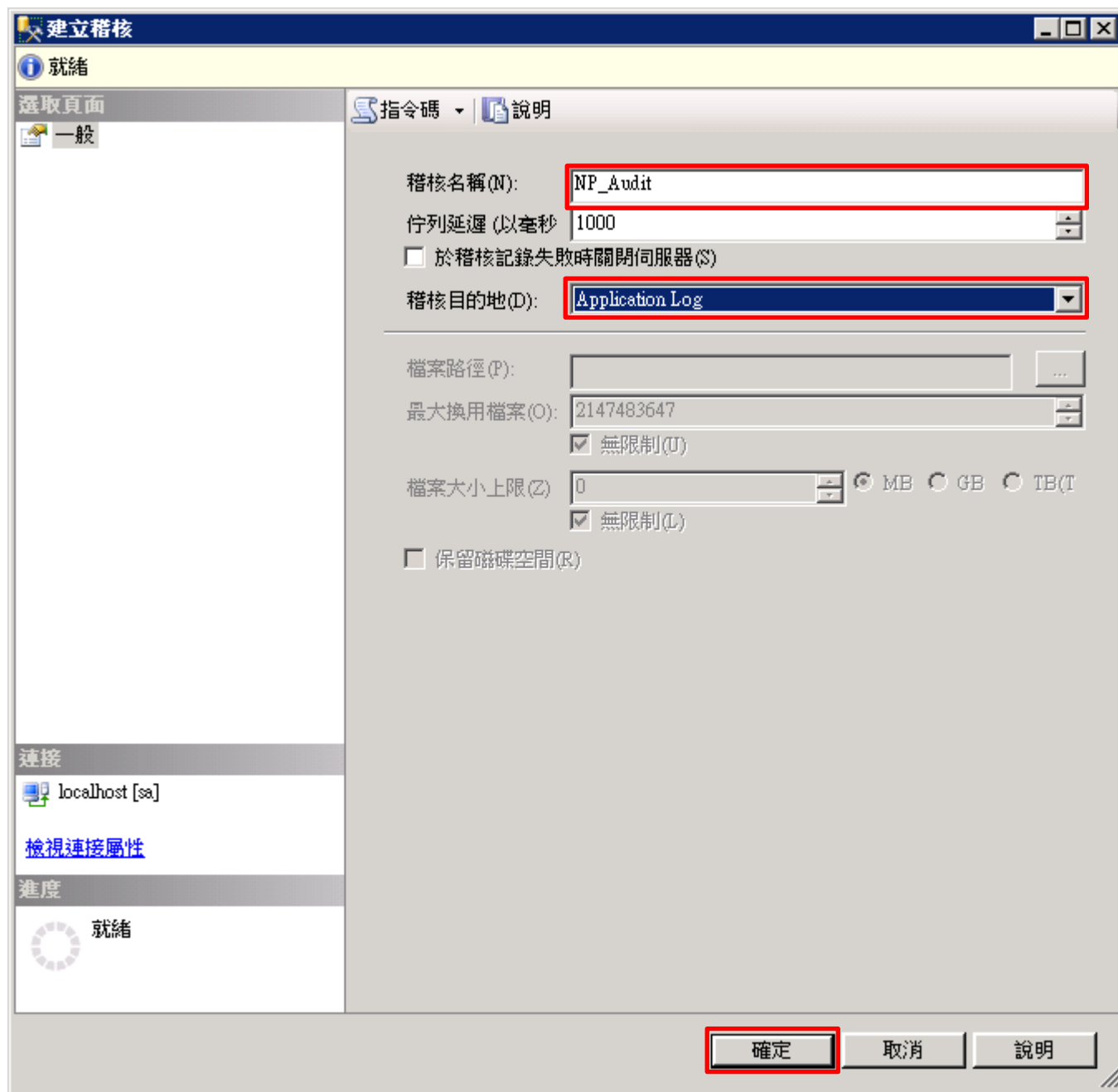
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



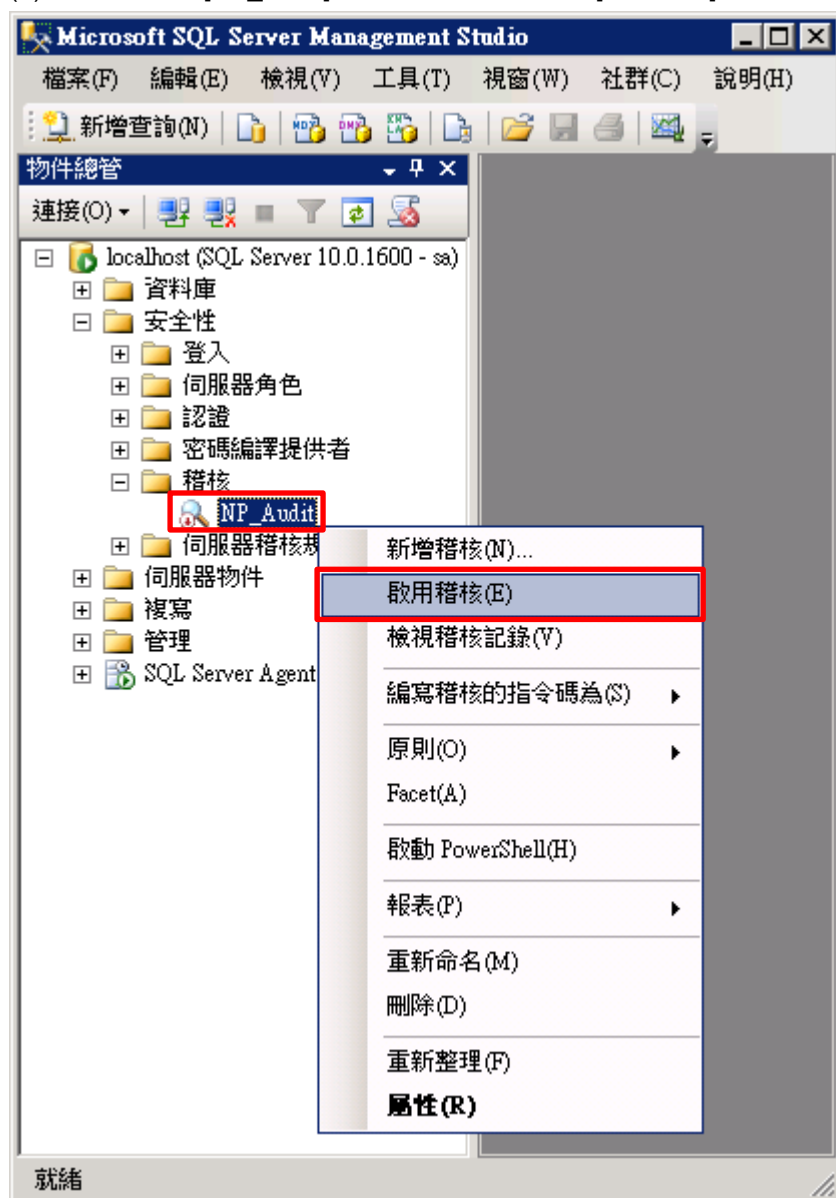
(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



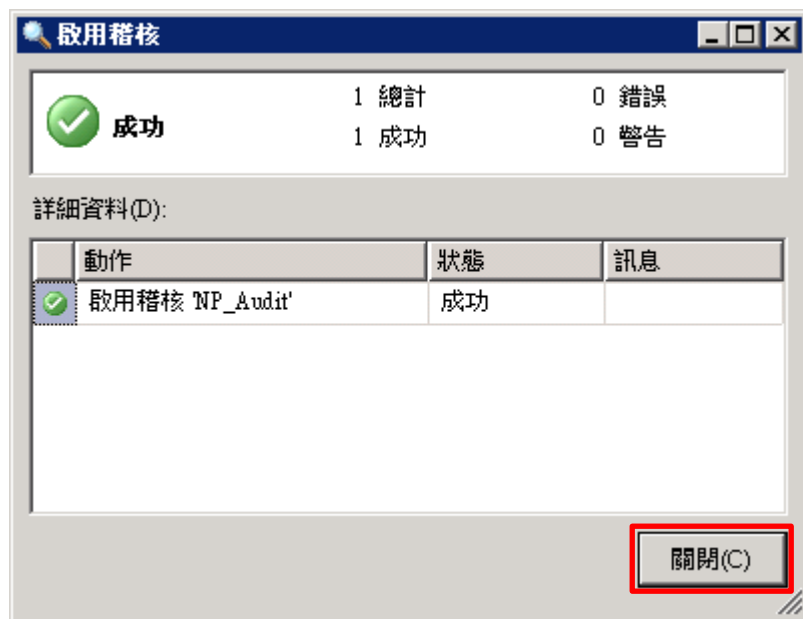
(4) 輸入稽核名稱: NP_Audit -> 選擇稽核目的地: [Application Log] 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]



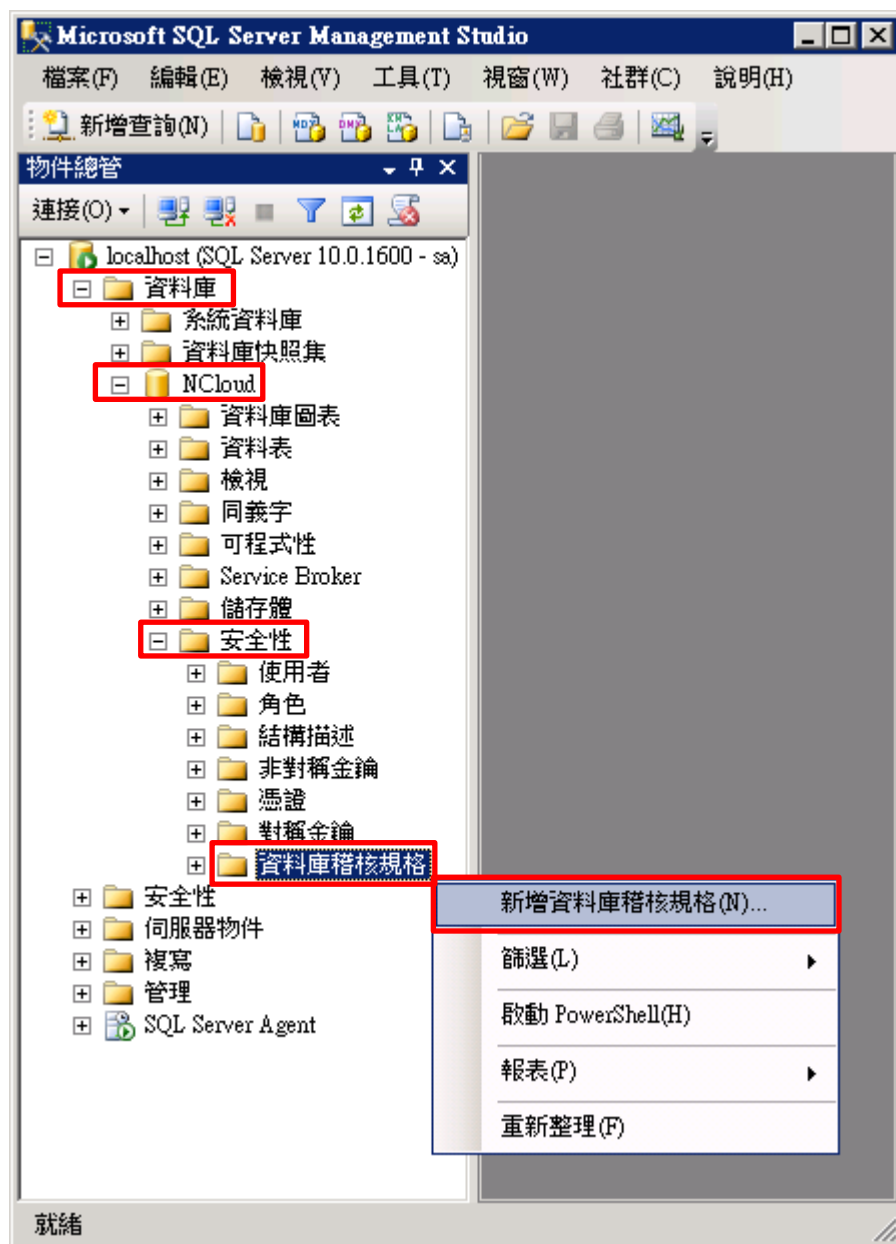
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



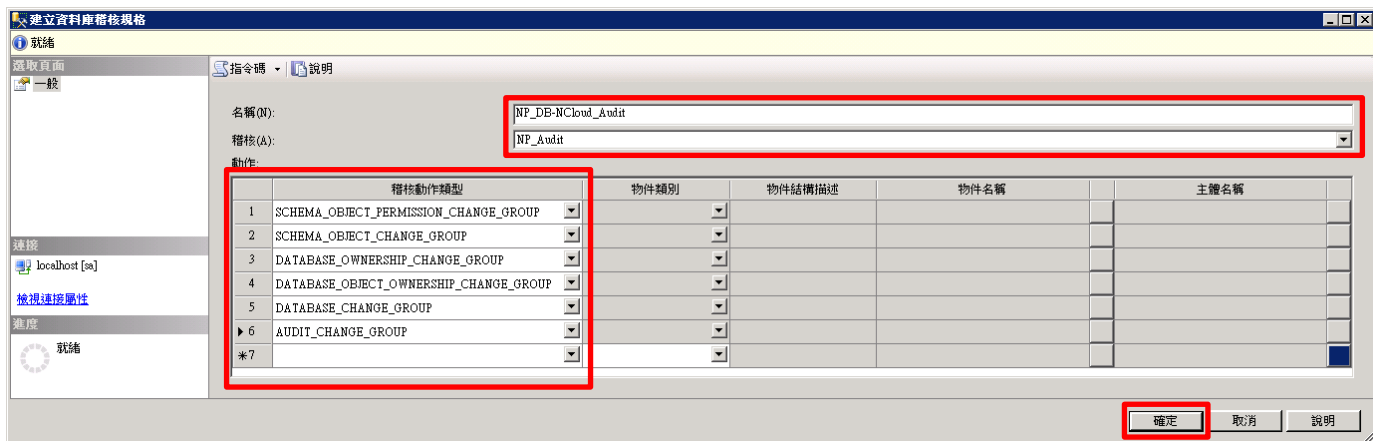
(6) 按 [關閉]



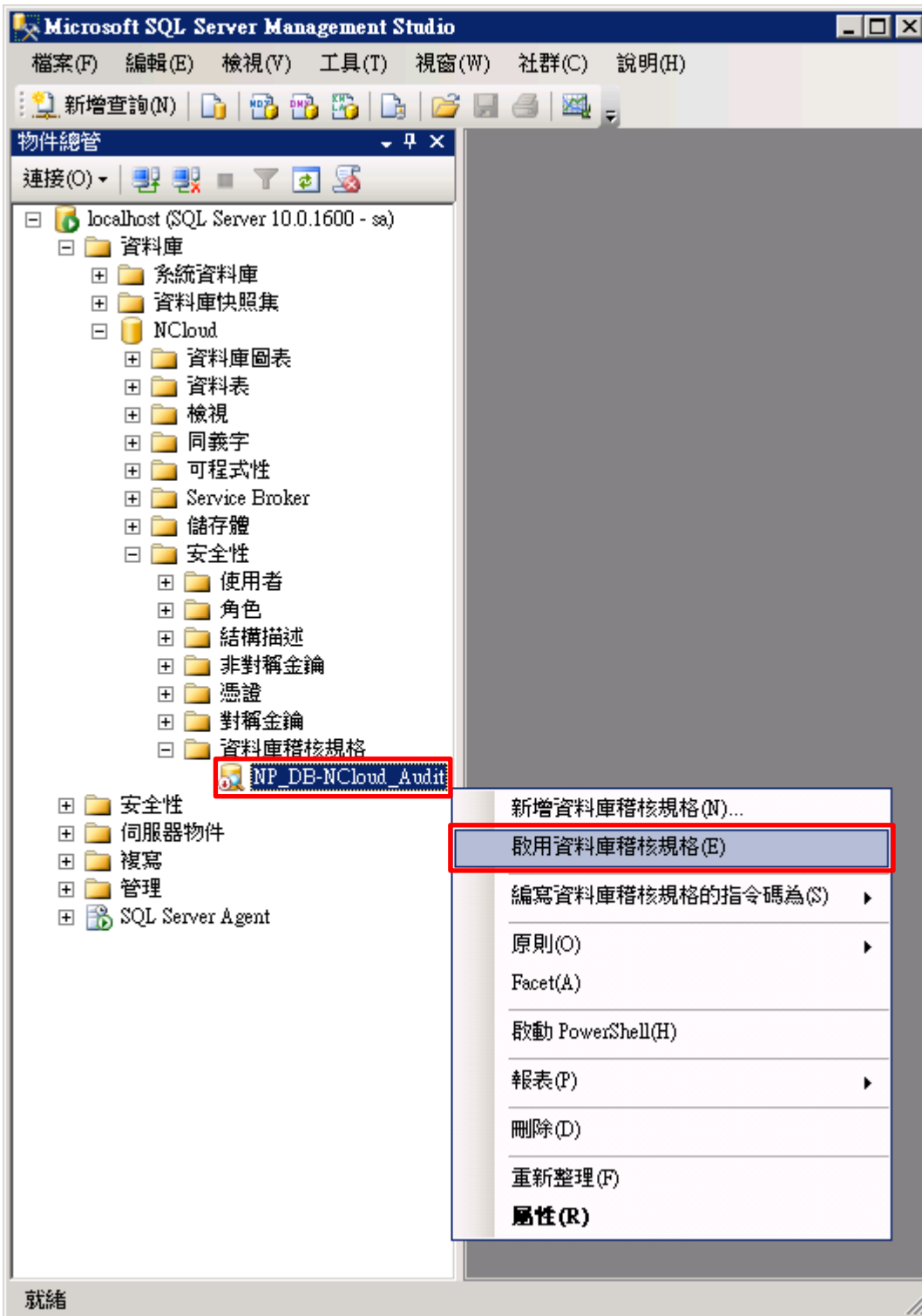
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



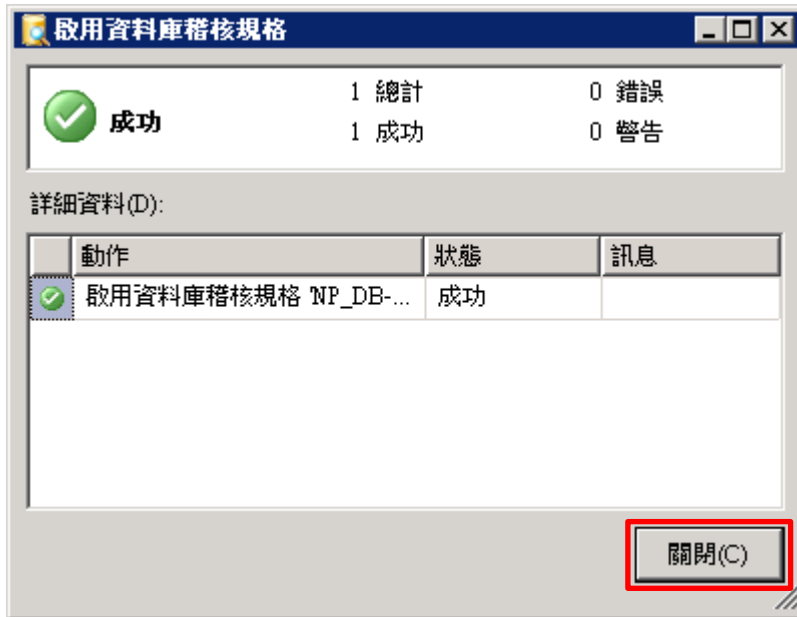
(8) 輸入名稱: NP_DB-NCloud_Audit -> 選擇稽核: [NP_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]



(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

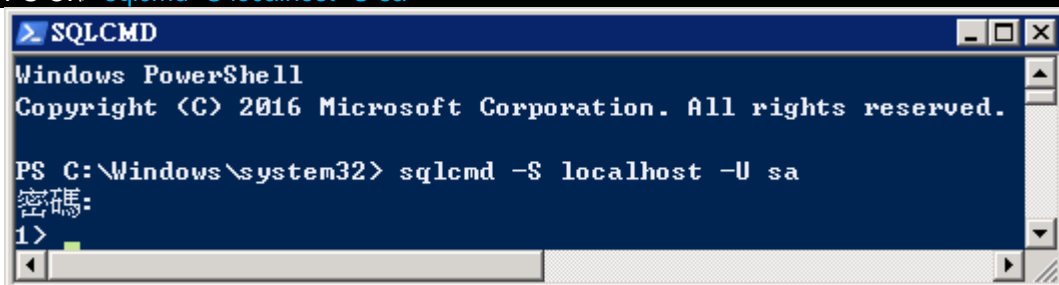
(1) 開啟 [Windows Powershell]



(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
```

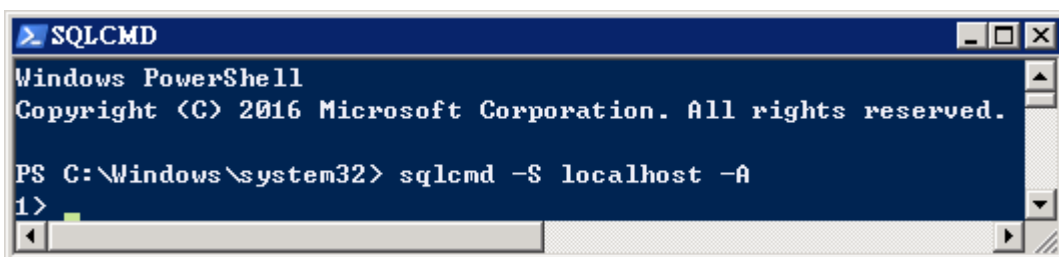


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

<2.2> 使用 Windows 帳號

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



(3) 切換資料庫

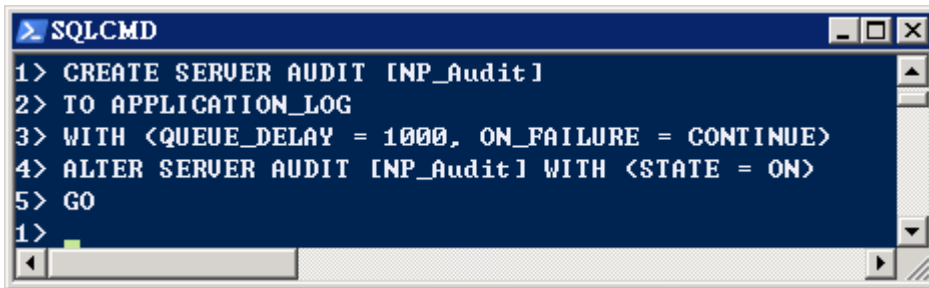
```
1 > use master  
2 > go
```



```
SQLCMD  
1> use master  
2> go  
已將資料庫內容變更為 '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
```



```
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
```

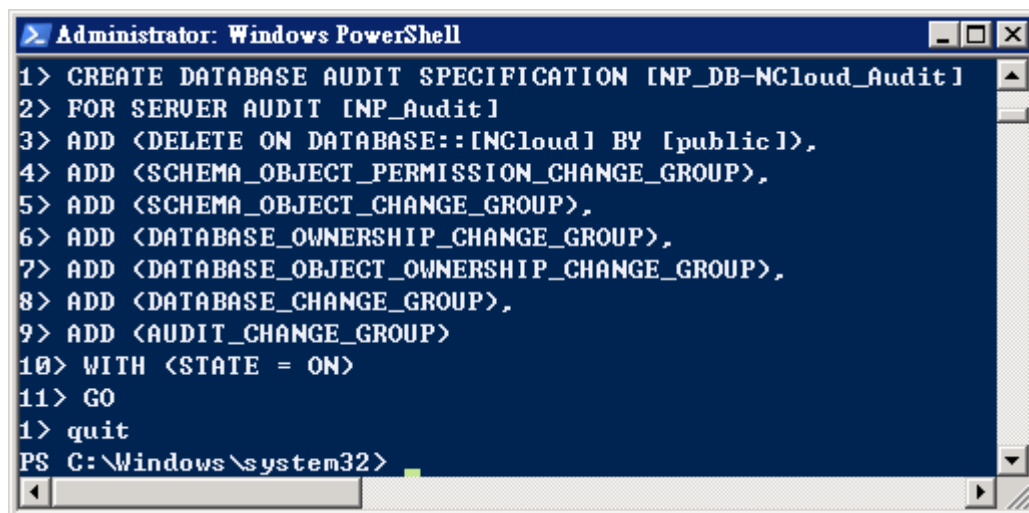


```
SQLCMD  
1> use NCloud  
2> go  
已將資料庫內容變更為 'NCloud' 。  
1>
```

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_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
```



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The terminal displays the following SQL commands and their execution:

```
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
PS C:\Windows\system32>
```

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

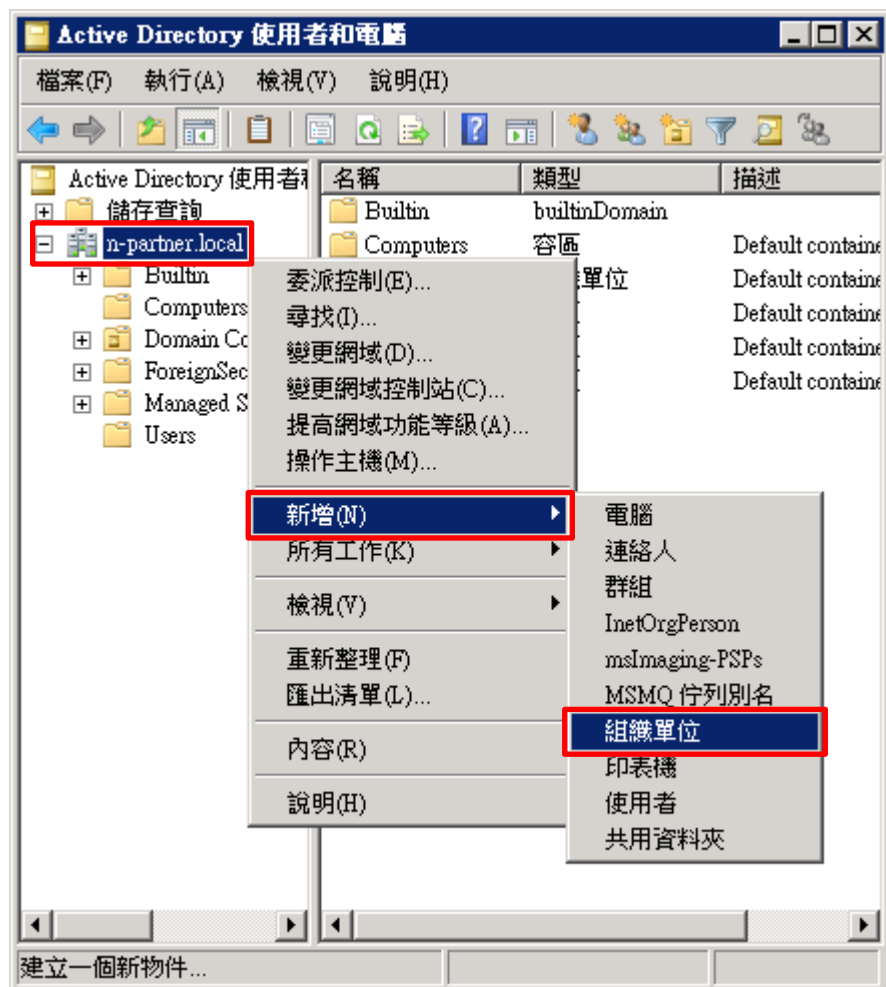
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



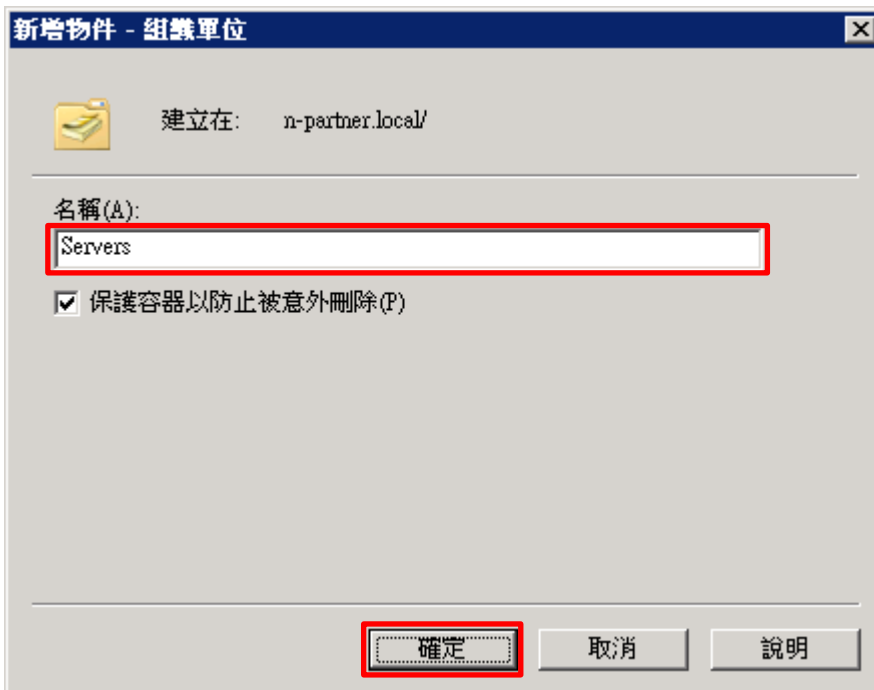
(2) 新增組織單位

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



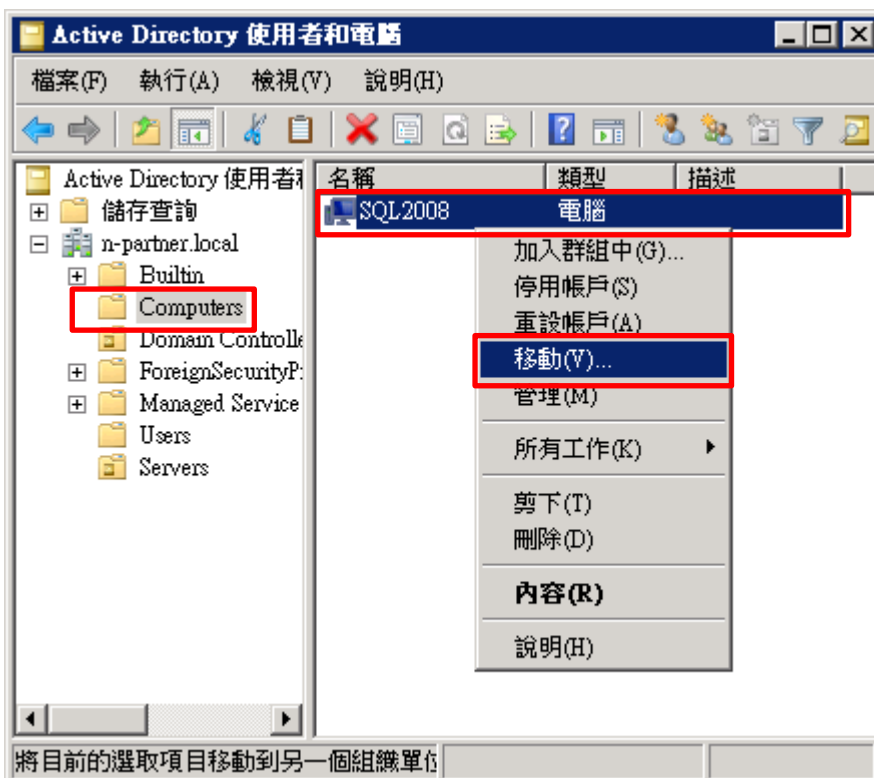
(3) 輸入組織單位名稱

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]



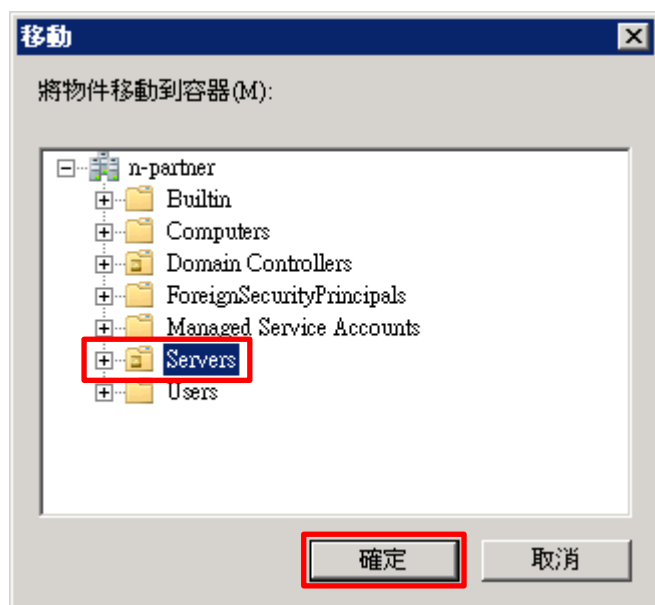
(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL2008] 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]



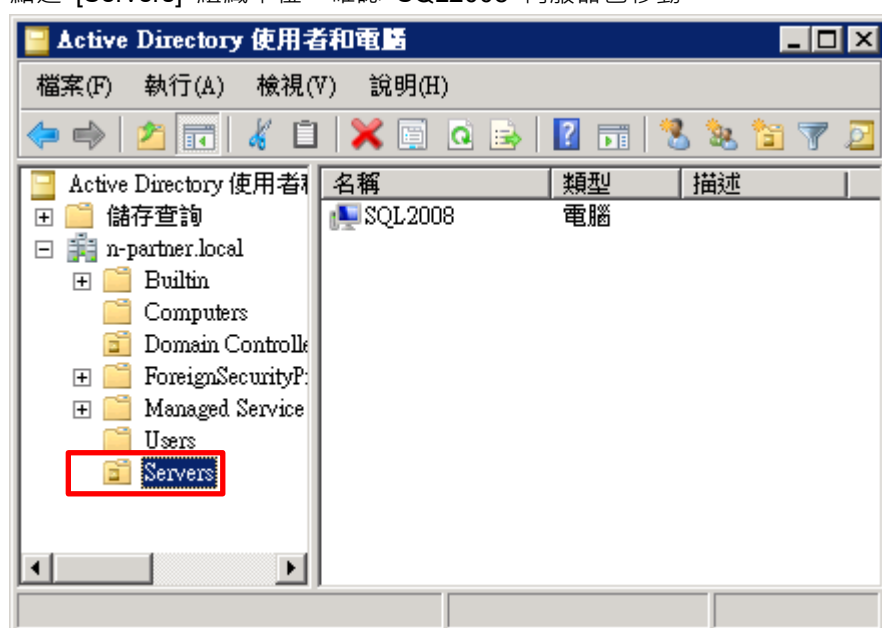
(5) 選擇組織單位

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

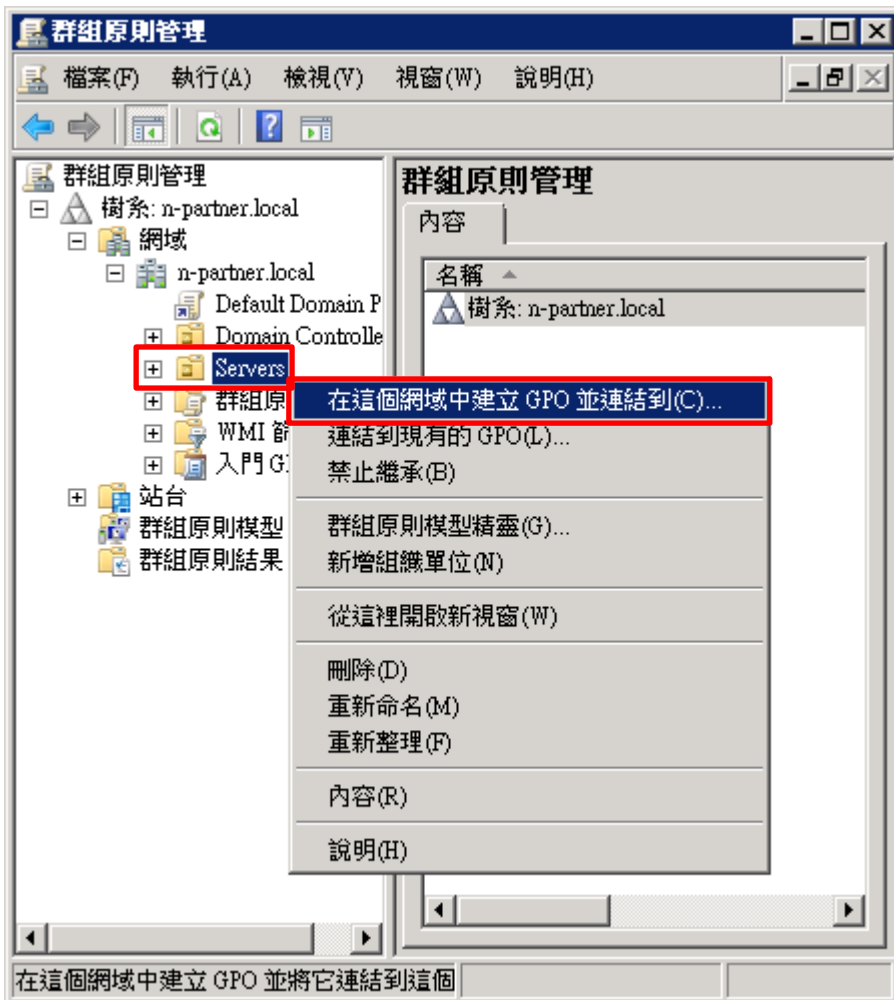
(1) 開啟群組原則管理

開啟 [群組原則管理]



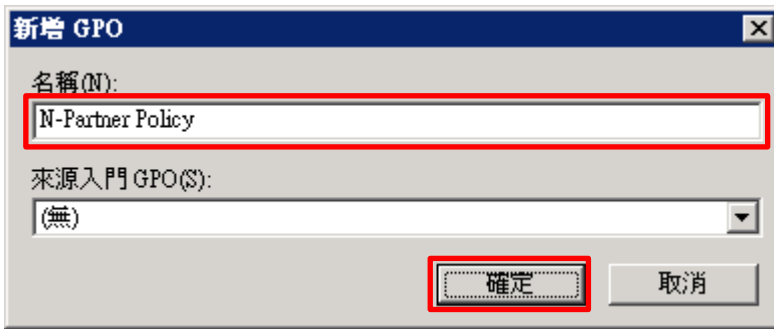
(2) 在 Servers 組織單位，新增群組原則物件

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...]



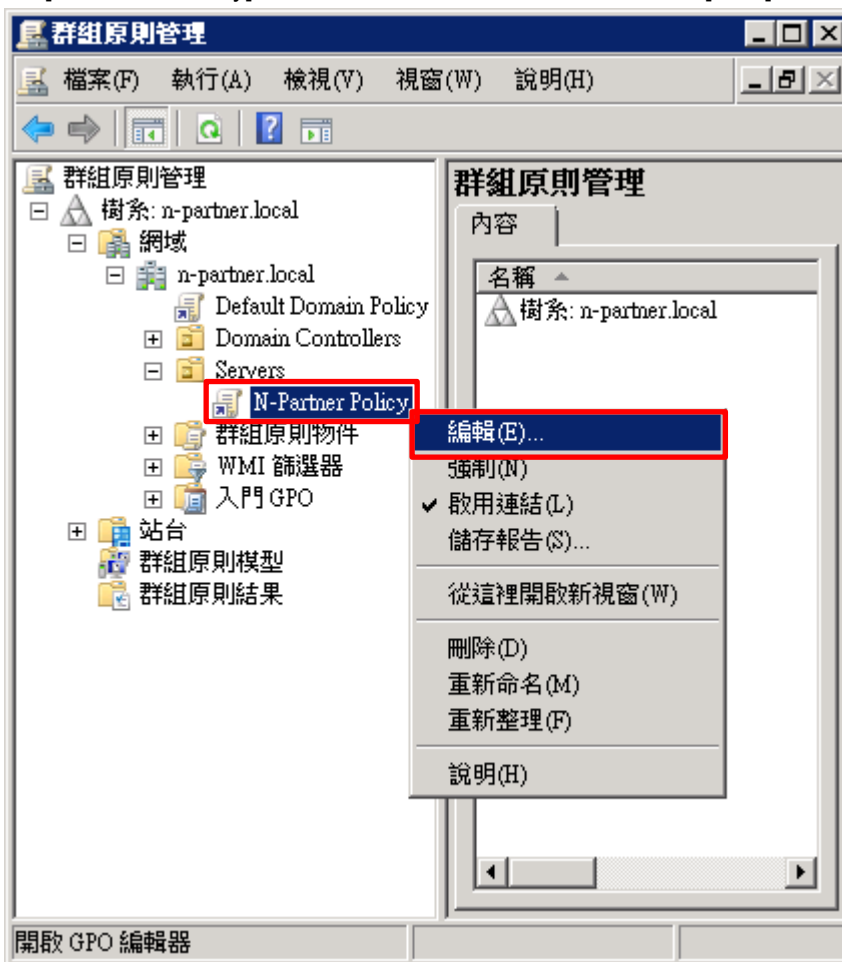
(3) 輸入群組原則物件名稱

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]



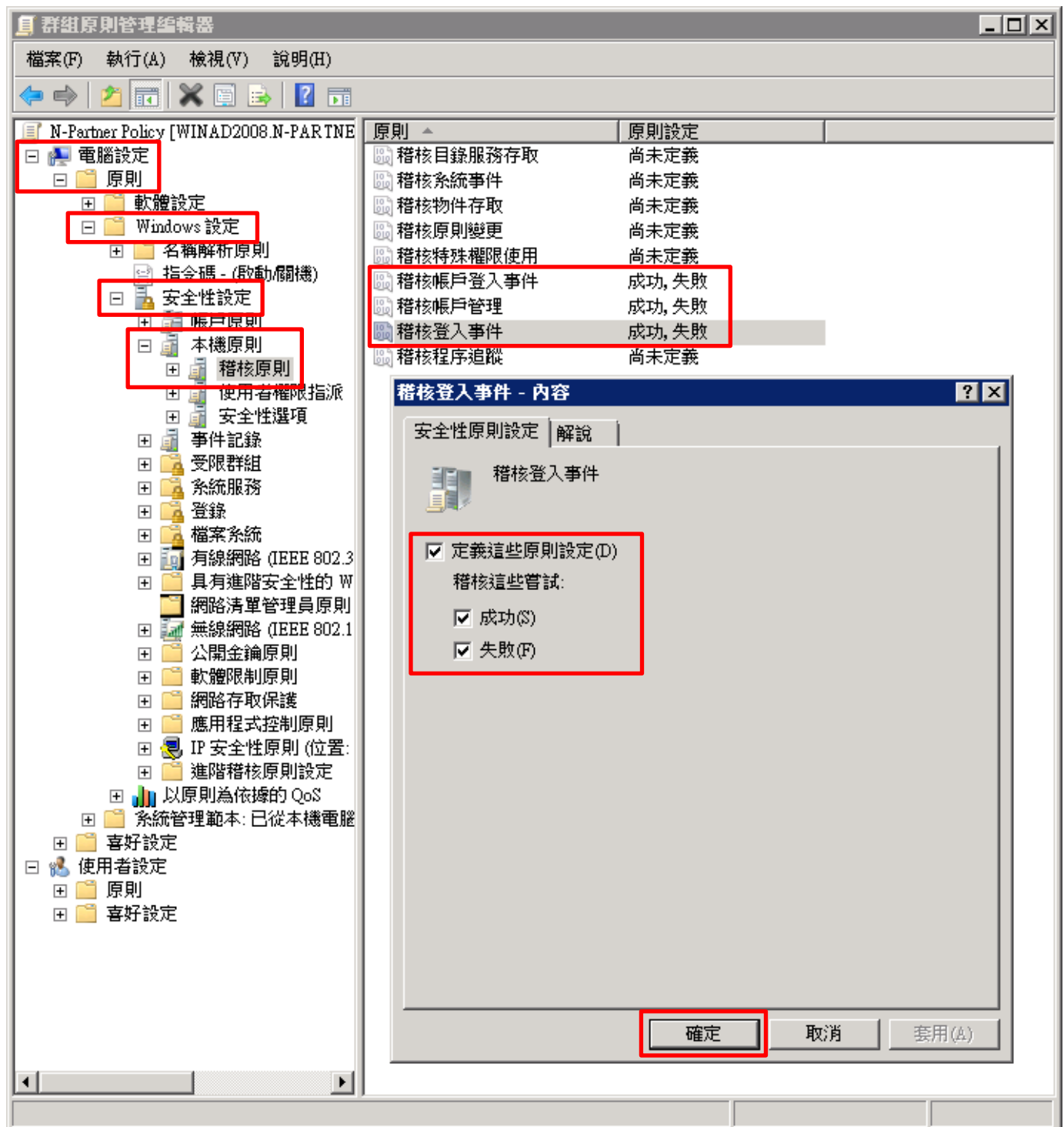
(4) 編輯群組原則物件

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



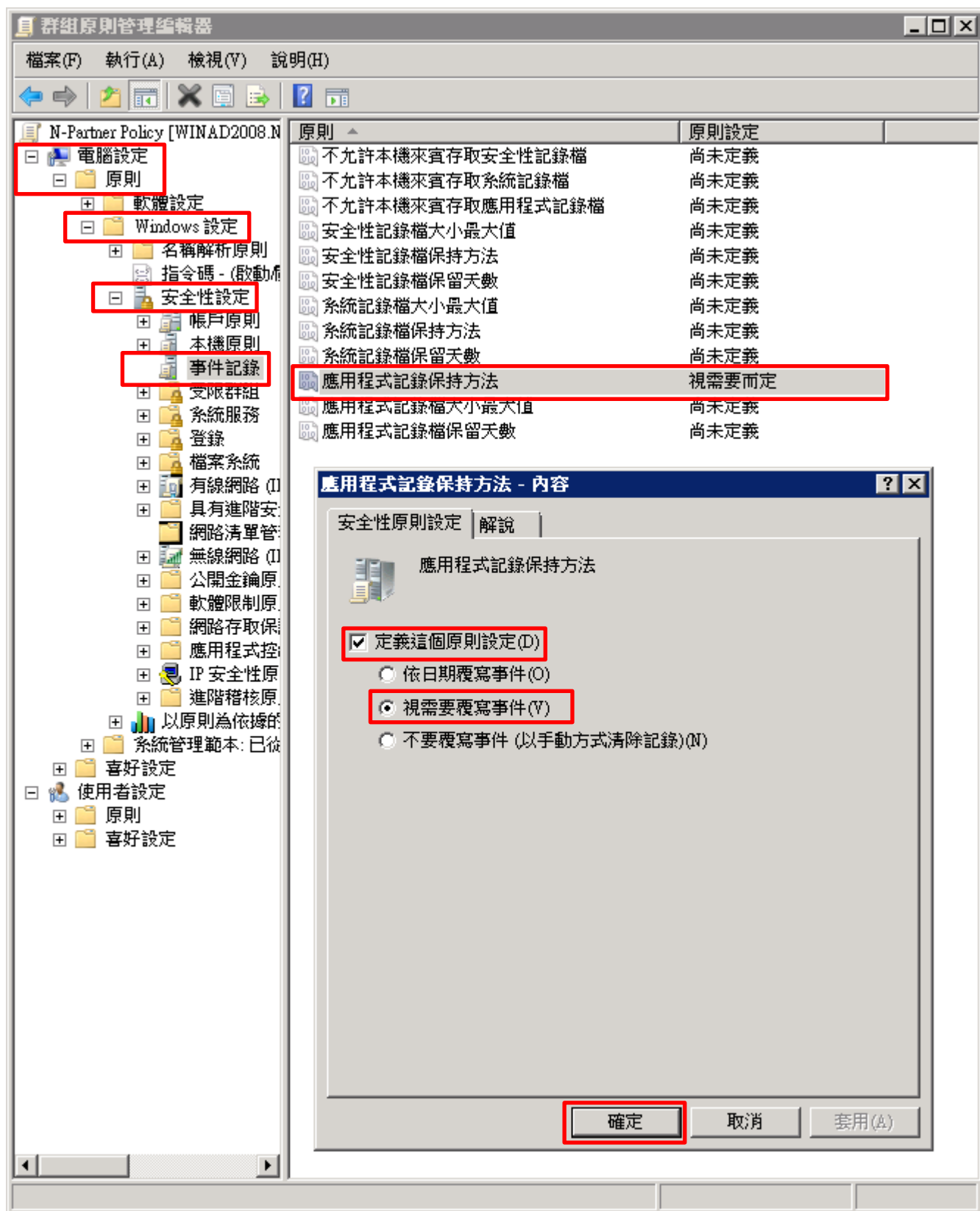
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [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]



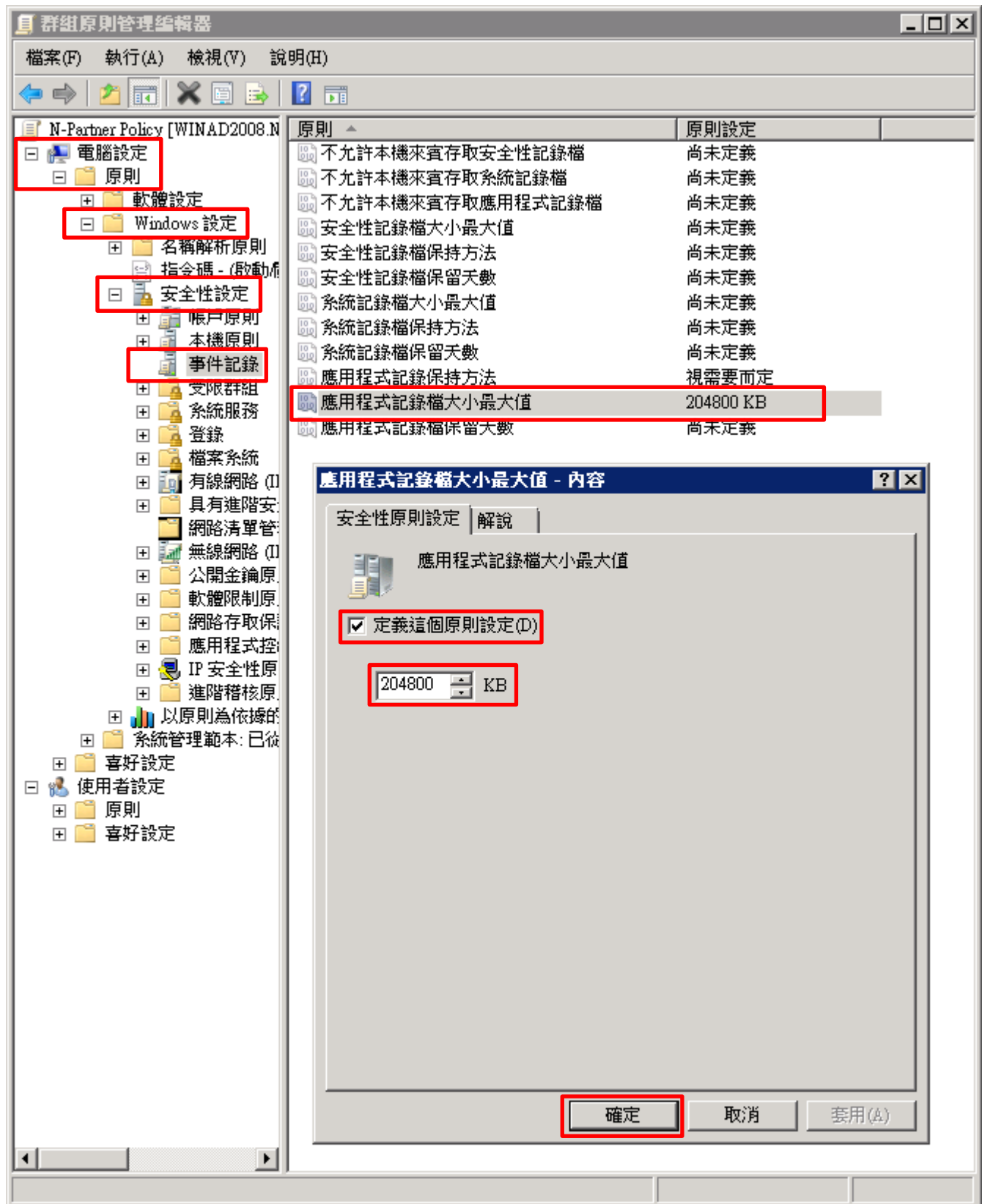
(6) 事件記錄：應用程式記錄保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄] -> 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

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

(10) 在 AD 網域伺服器 -> 產生 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

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command "PS C:\> Get-GPResultantSetofPolicy -Computer SQL2008 -Path C:\tmp\SQL2008.html -ReportType html" being entered. The output is a list of properties: "RsopMode : Logging", "Namespace : \\SQL2008\Root\Rsop\NS1ABDEB77_5871_4F42_B155_822DDC08423C", "LoggingComputer : SQL2008", "LoggingUser : N-PARTNER\administrator", and "LoggingMode : Computer". The prompt "PS C:\> " is visible at the bottom of the terminal.

紅色文字部位請輸入 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 08:18:02

摘要 顯示全部

電腦設定 隱藏

原則 隱藏

Windows 設定 隱藏

安全性設定 隱藏

帳戶原則/密碼規則 顯示

帳戶原則/帳戶鎖定原則 顯示

本機原則/稽核原則 隱藏

原則	設定	優勢 GPO
稽核帳戶登入事件	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

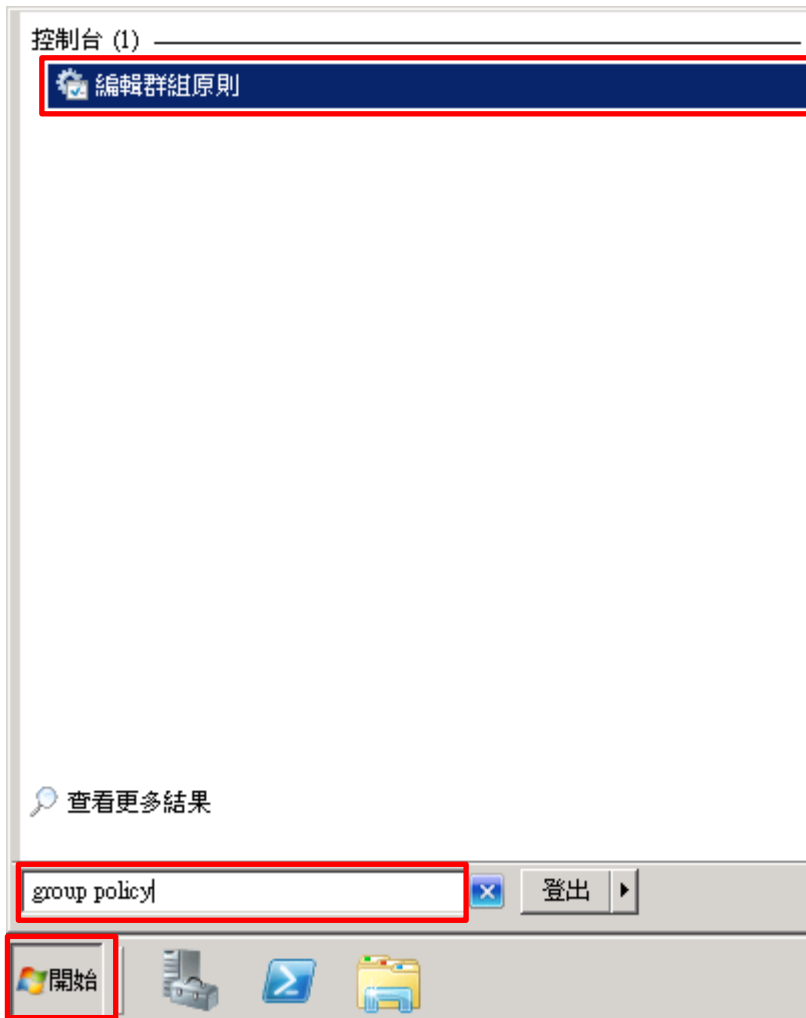
使用者設定 顯示

2.3.2 工作群組

2.3.2.1 稽核原則設定

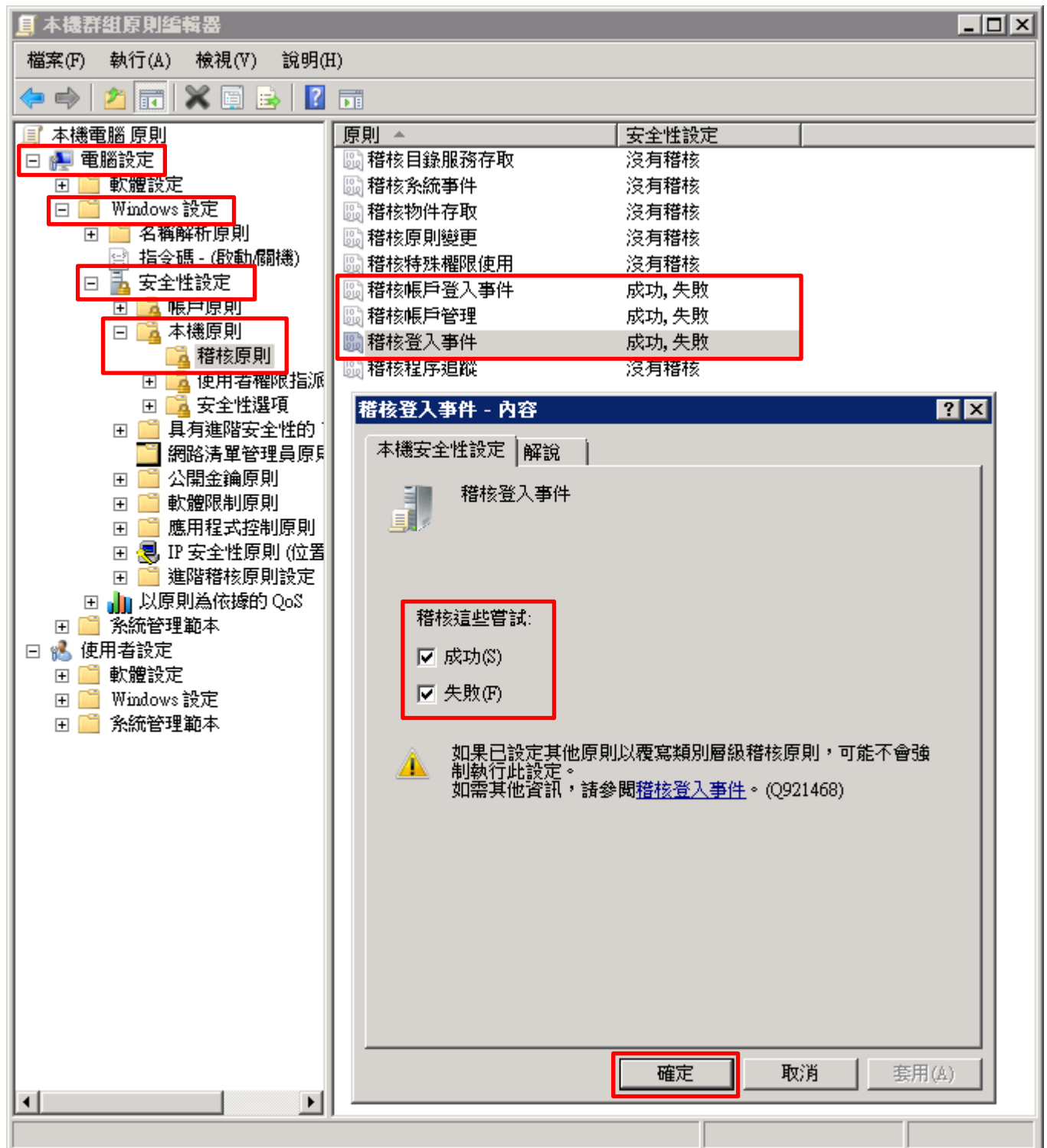
(1) 開啟 [本機群組原則編輯器]

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

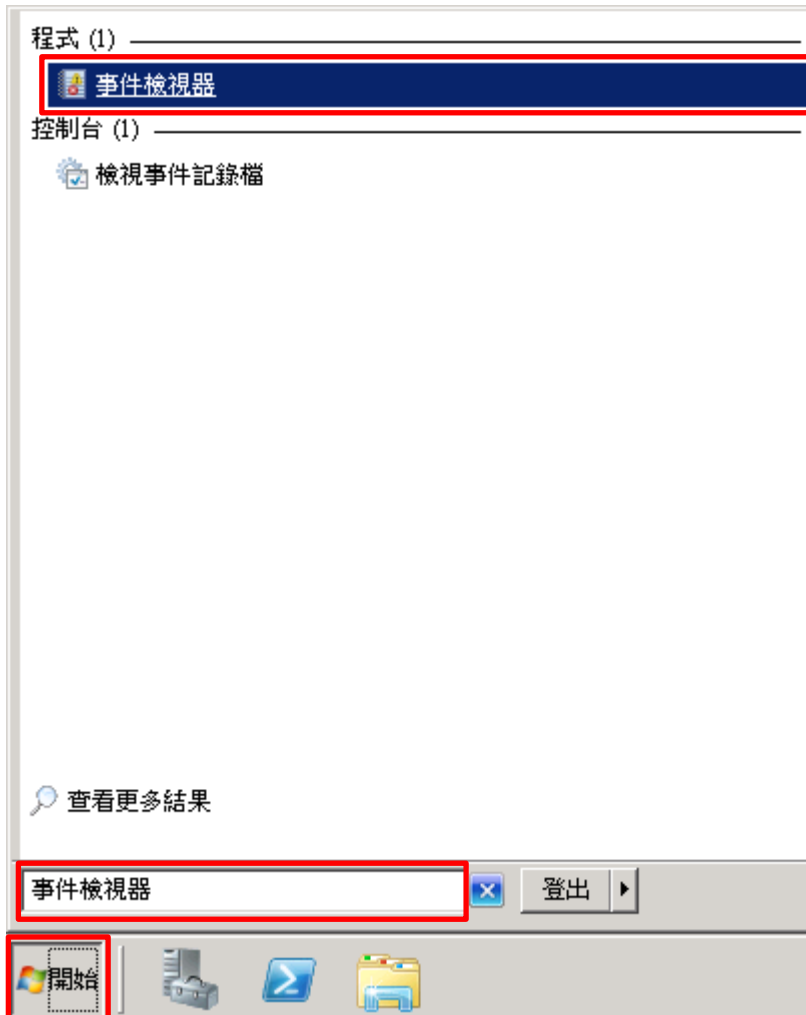
PS C:\> auditpol /get /category:*

```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
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
登入                成功及失敗
登出                成功及失敗
帳戶鎖定            成功及失敗
IPsec 主要模式      成功及失敗
IPsec 快速模式      成功及失敗
IPsec 延伸模式      成功及失敗
特殊登入            成功及失敗
其他登入/登出事件  成功及失敗
網路原則伺服器      成功及失敗
物件存取
檔案系統            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
機密特殊權限使用    沒有稽核
非機密特殊權限使用  沒有稽核
其他特殊權限使用事件 沒有稽核
詳細追蹤
終止處理程序        沒有稽核
DPIAPI 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
稽核原則變更        成功
驗證原則變更        成功
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
使用者帳戶管理      成功及失敗
電腦帳戶管理        成功及失敗
安全性群組管理      成功及失敗
發佈群組管理        成功及失敗
應用程式群組管理    成功及失敗
其他帳戶管理事件    成功及失敗
DS 存取
目錄服務變更        沒有稽核
目錄服務複寫        沒有稽核
詳細目錄服務複寫    沒有稽核
目錄服務存取        成功
帳戶登入
Kerberos 服務票證操作 成功及失敗
其他帳戶登入事件    成功及失敗
Kerberos 驗證服務    成功及失敗
認證驗證            成功及失敗
PS C:\>
```

2.3.2.2 事件檔案設定

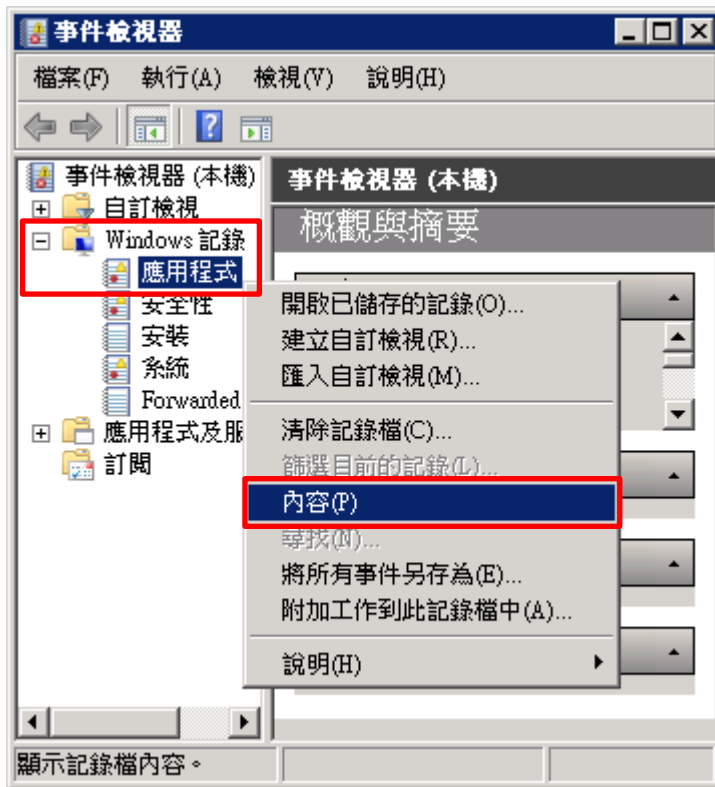
(1) 開啟 [事件檢視器]

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)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄檔(R)

確定 取消 套用(P)

3. SQL 2012

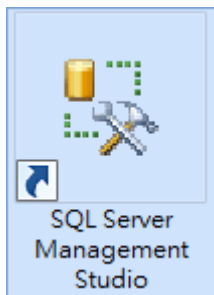
3.1 稽核登入

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

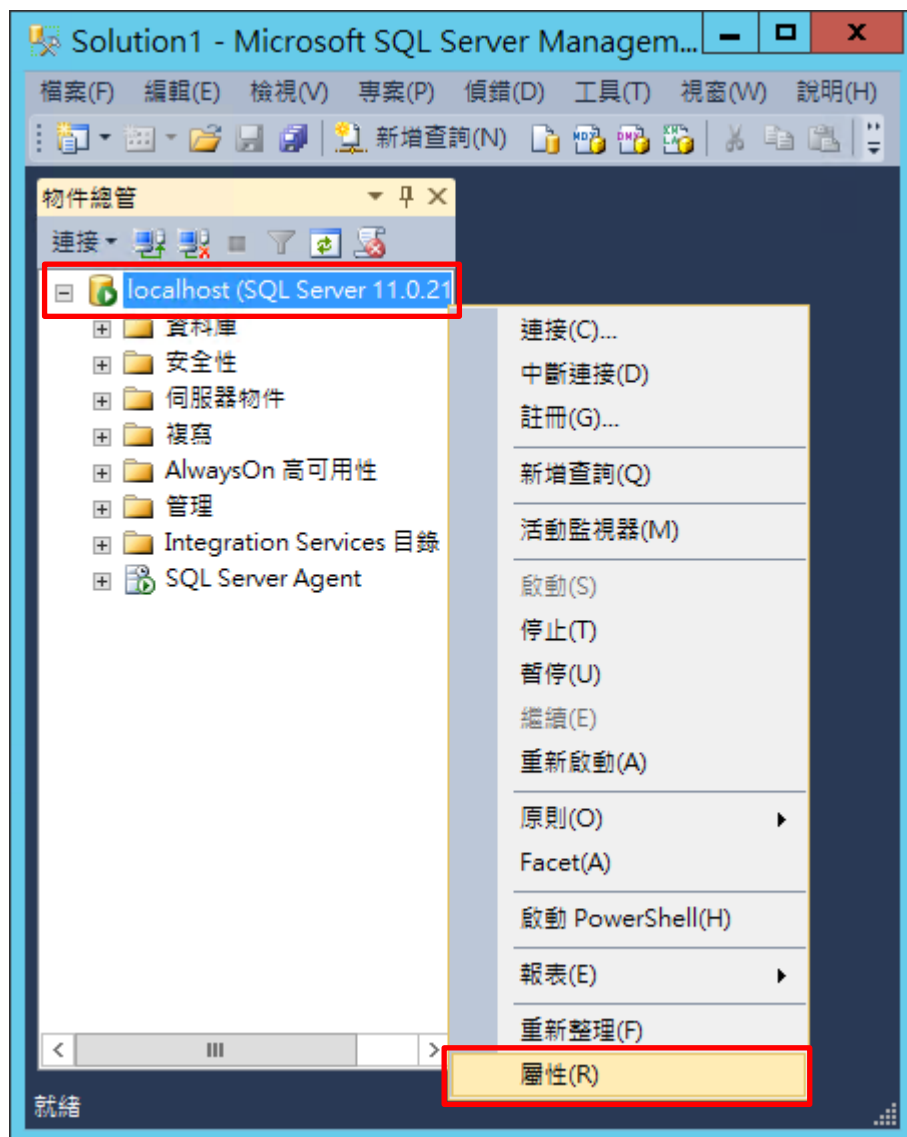
(1) 開啟 [SQL Server Management Studio]



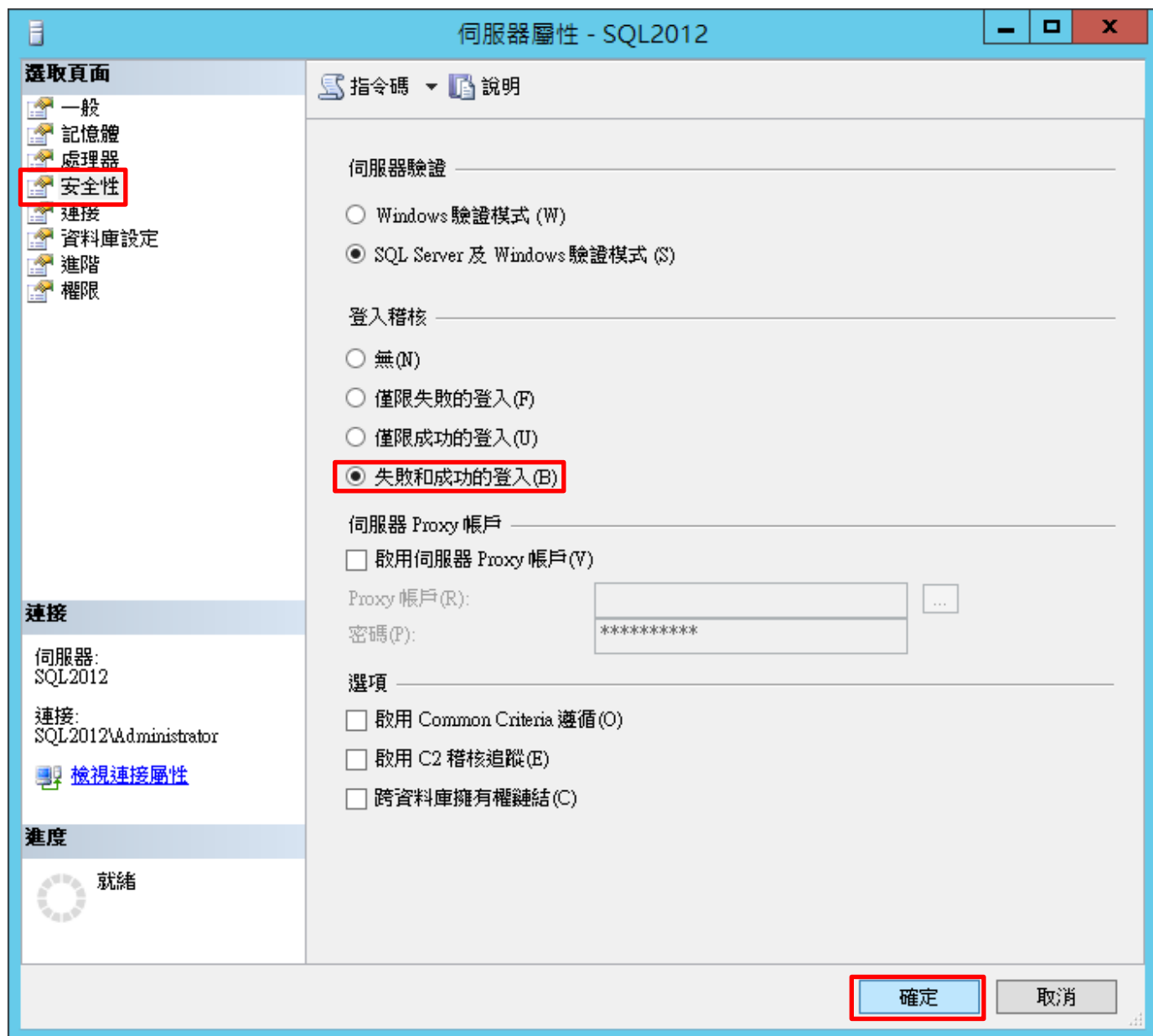
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

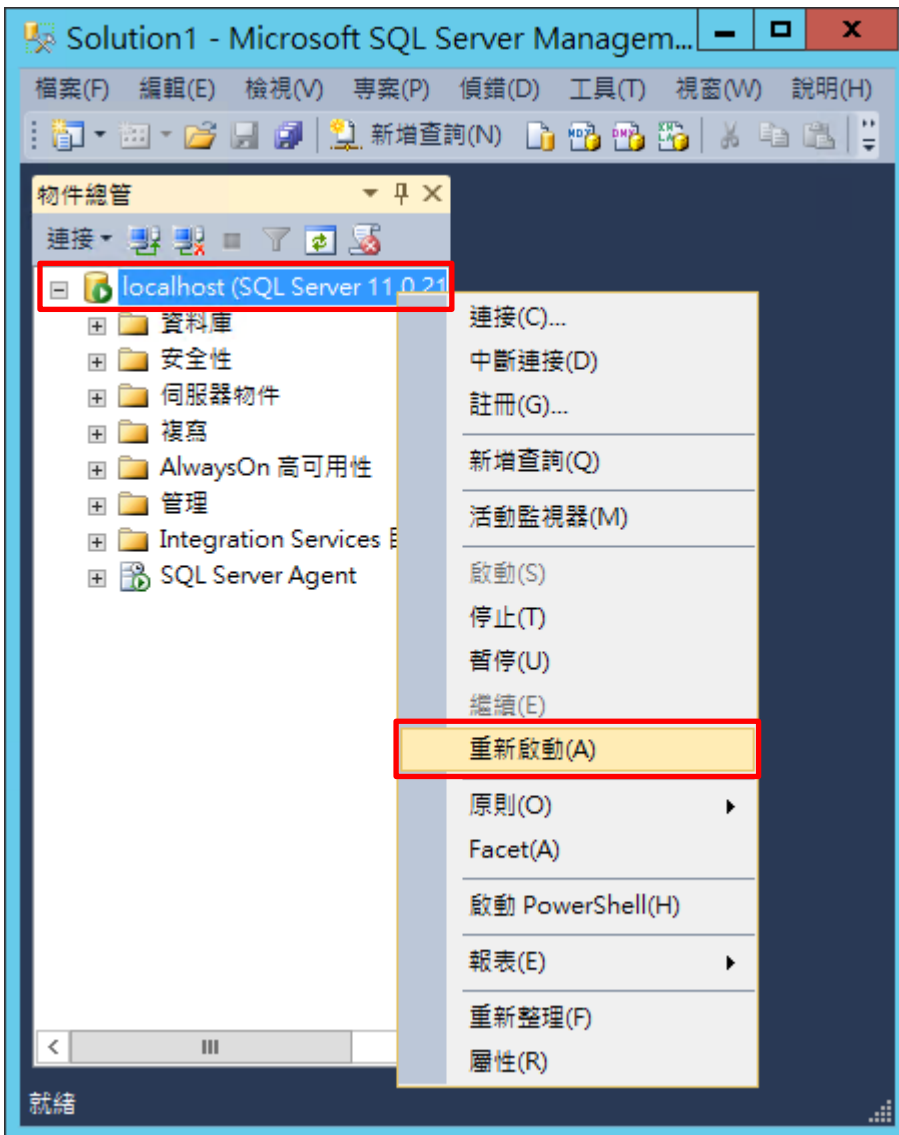


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

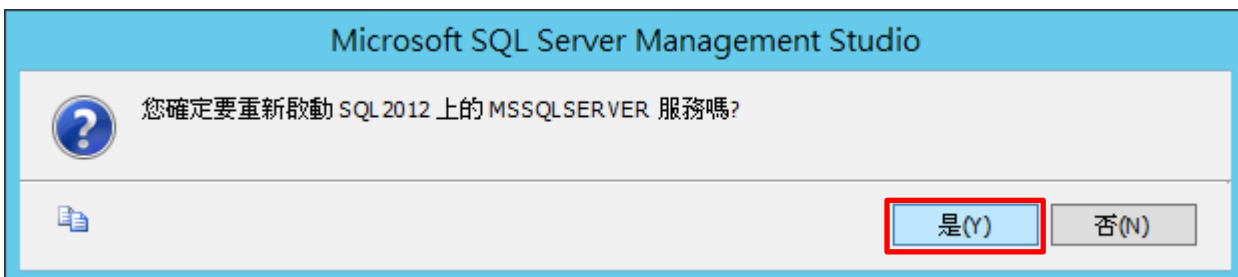


(5) 重新啟動 MS SQL SERVER 服務

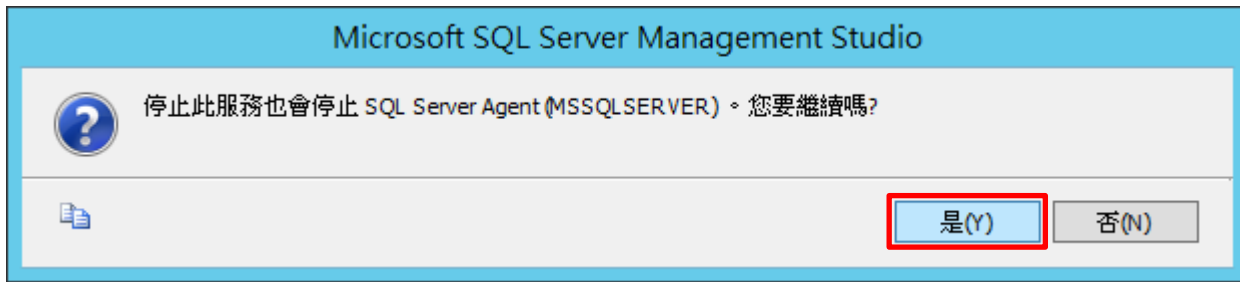
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(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

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



(3) 切換資料庫

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

```
SQLCMD
1> use master
2> go
已將資料庫內容變更為 '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
```

```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
組態選項 'show advanced options' 從 1 變更為 1。請執行 RECONFIGURE 陳述式來安裝。
1> reconfigure
2> go
1>
```

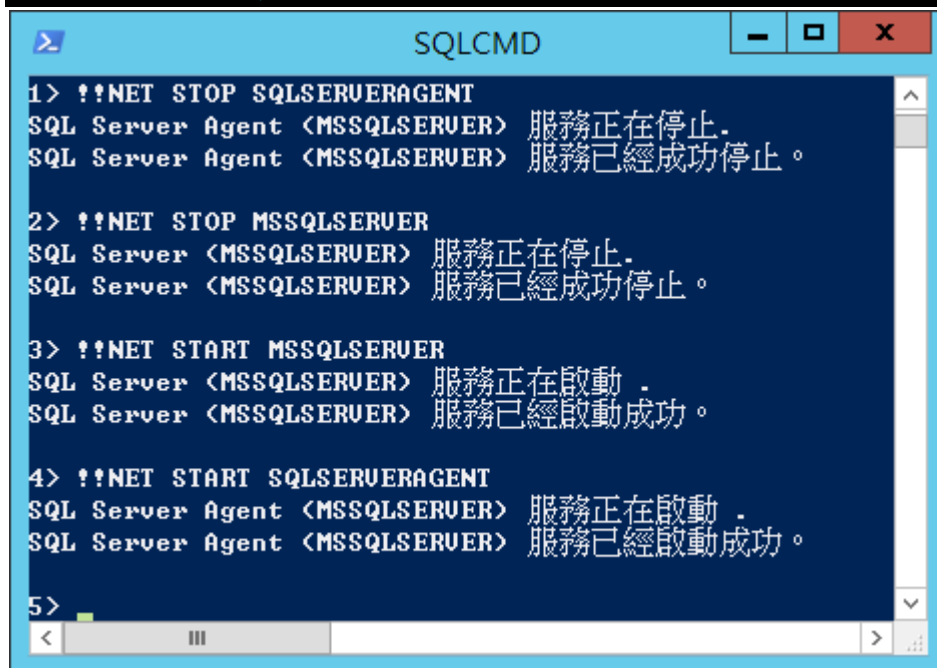
(5) 啟用失敗和成功的登入記錄

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

```
SQLCMD
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>
```

(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
```



```
SQLCMD
1 > !!NET STOP SQLSERVERAGENT
SQL Server Agent (MSSQLSERVER) 服務正在停止。
SQL Server Agent (MSSQLSERVER) 服務已經成功停止。

2 > !!NET STOP MSSQLSERVER
SQL Server (MSSQLSERVER) 服務正在停止。
SQL Server (MSSQLSERVER) 服務已經成功停止。

3 > !!NET START MSSQLSERVER
SQL Server (MSSQLSERVER) 服務正在啟動。
SQL Server (MSSQLSERVER) 服務已經啟動成功。

4 > !!NET START SQLSERVERAGENT
SQL Server Agent (MSSQLSERVER) 服務正在啟動。
SQL Server Agent (MSSQLSERVER) 服務已經啟動成功。

5 >
```

3.2 設定稽核

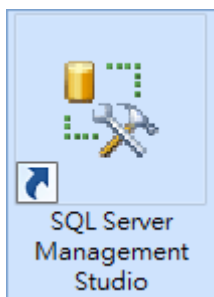
3.2.1 稽核伺服器層級

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

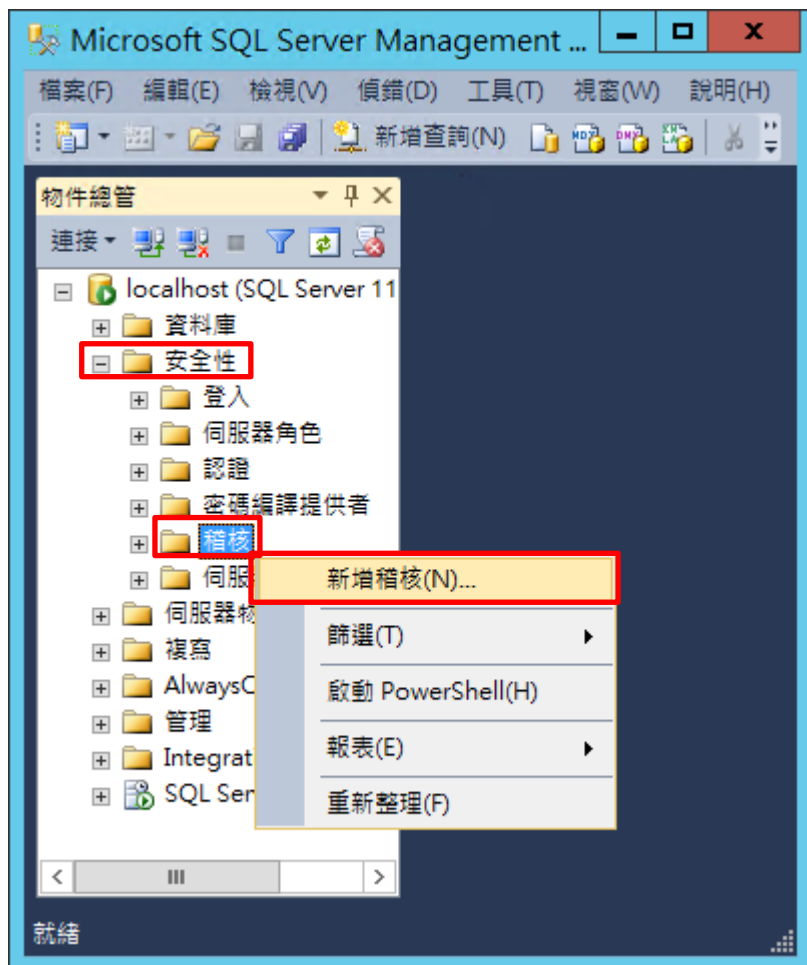
(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

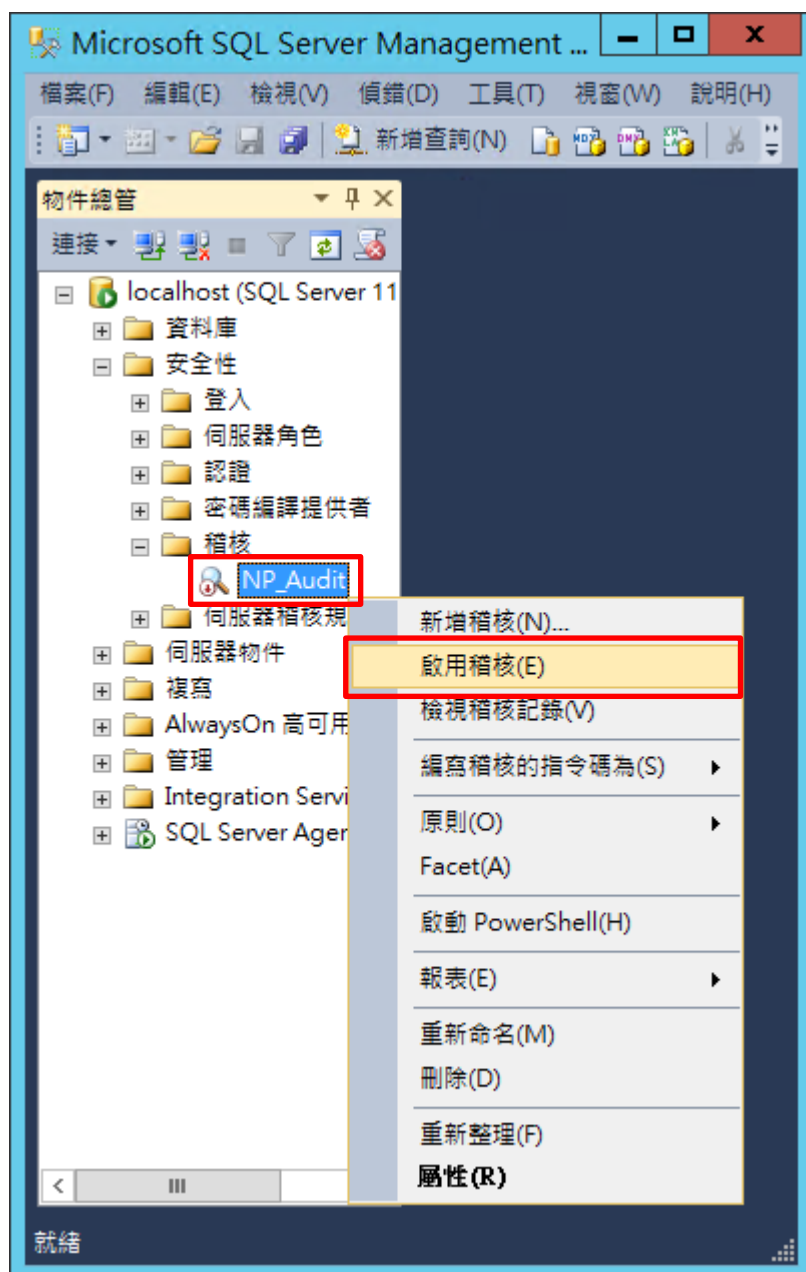


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



(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]

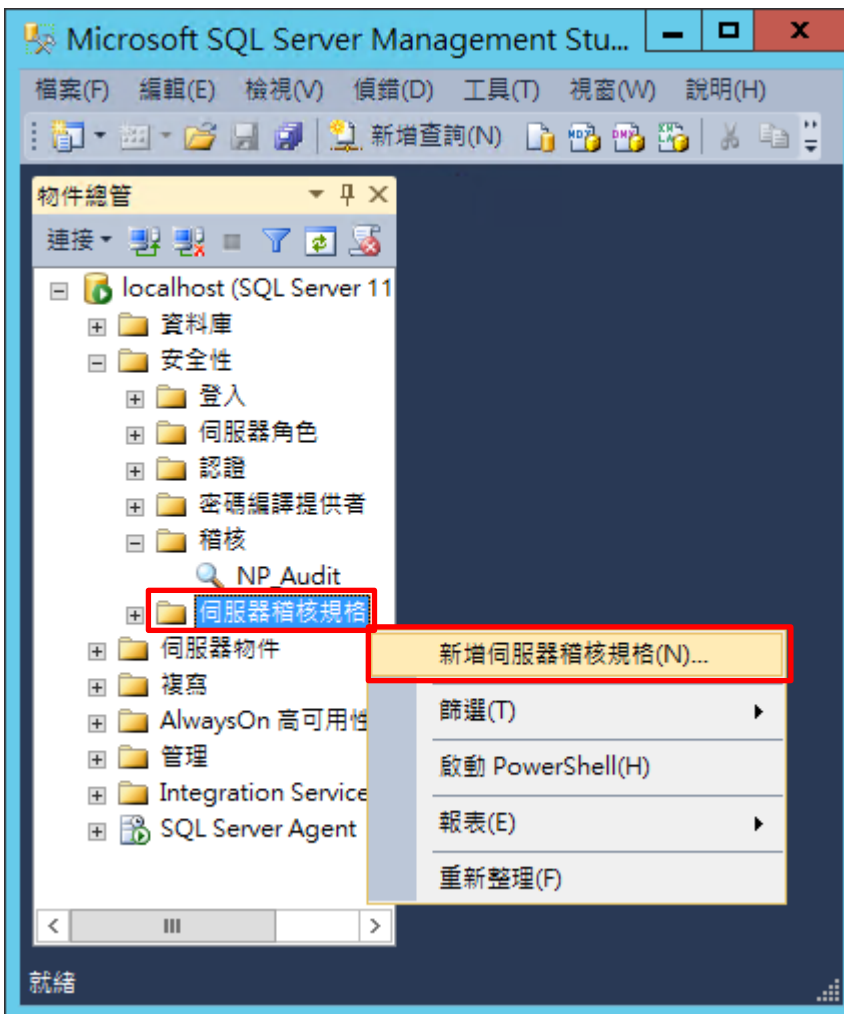
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



(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...]



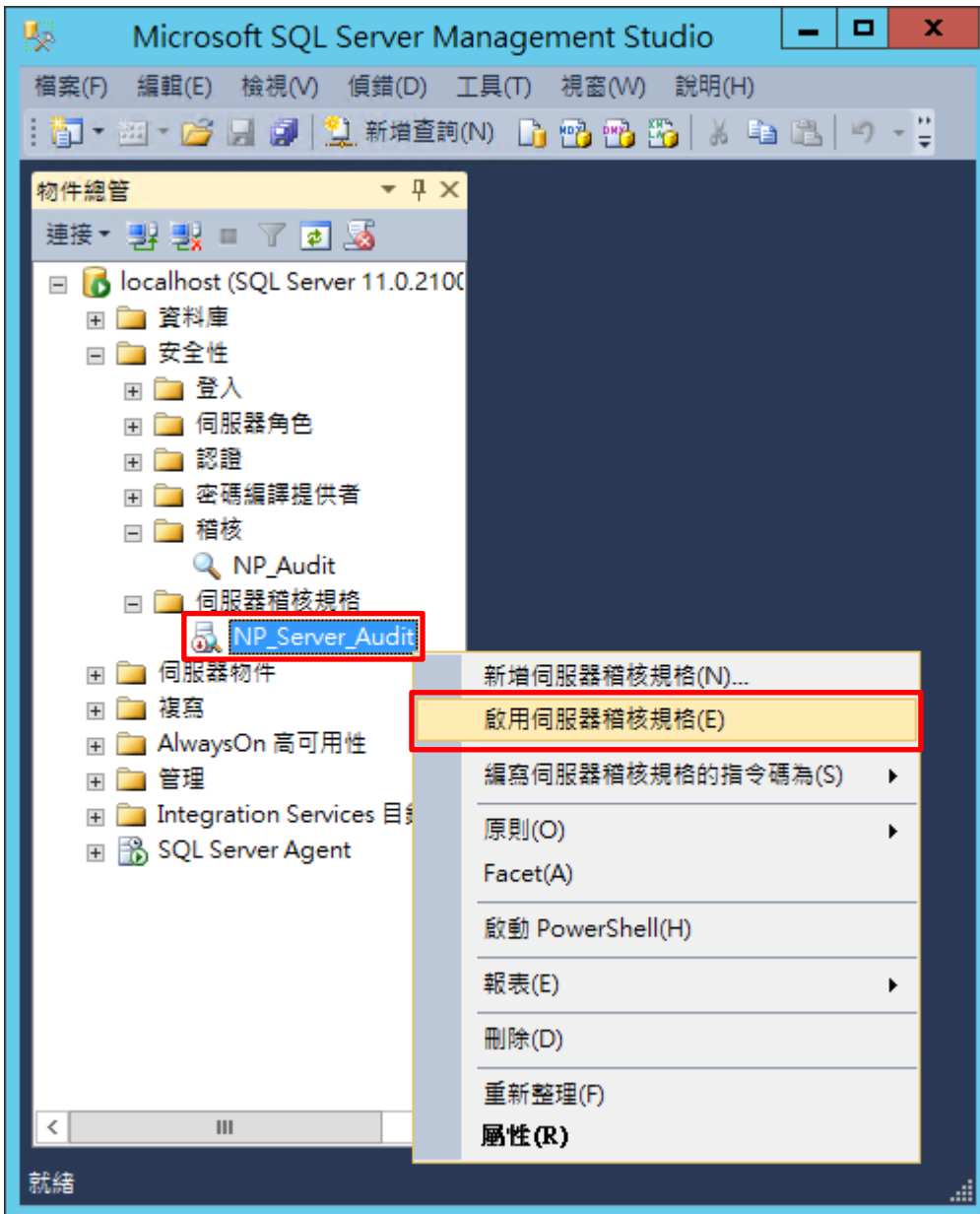
(8) 輸入名稱: NP_Server_Audit -> 選擇稽核: [NP_Audit] 和動作 [詳細說明請參考前言的稽核動作群組連結](#) -> 按 [確定]

The screenshot shows the 'Create Server Audit Specification' dialog box. The 'Name (N):' field contains 'NP_Server_Audit'. The 'Audit (A):' dropdown menu is set to 'NP_Audit'. The 'Actions' section contains a table with the following data:

	稽核動作類型	物件類別	物件結構描述	物件名稱	主體名稱
01	SUCCESSFUL_LOGIN_GROUP	▼			<input type="checkbox"/>
02	FAILED_LOGIN_GROUP	▼			<input type="checkbox"/>
03	LOGOUT_GROUP	▼			<input type="checkbox"/>
04	SERVER_STATE_CHANGE_GROUP	▼			<input type="checkbox"/>
05	SERVER_OPERATION_GROUP	▼			<input type="checkbox"/>
06	SCHEMA_OBJECT_CHANGE_GROUP	▼			<input type="checkbox"/>
07	DATABASE_OWNERSHIP_CHANGE_GROUP	▼			<input type="checkbox"/>
08	DATABASE_CHANGE_GROUP	▼			<input type="checkbox"/>
09	AUDIT_CHANGE_GROUP	▼			<input type="checkbox"/>
▶ 10	USER_CHANGE_PASSWORD_GROUP	▼			<input type="checkbox"/>
*11		▼			<input type="checkbox"/>

The 'OK' button is highlighted with a red box.

(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]

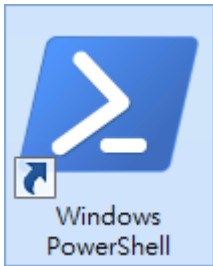


(10) 按 [關閉]



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

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



(3) 切換資料庫

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

```
SQLCMD  
1> use master  
2> go  
已將資料庫內容變更為 '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
```

```
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 > WITH (STATE = ON)
14 > GO
1 > quit
```



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The terminal displays the following commands and their execution:

```
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 > WITH (STATE = ON)
14 > 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

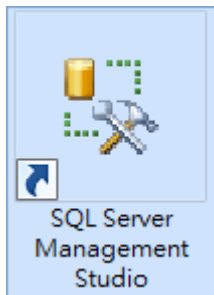
3.2.2 稽核資料庫層級

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

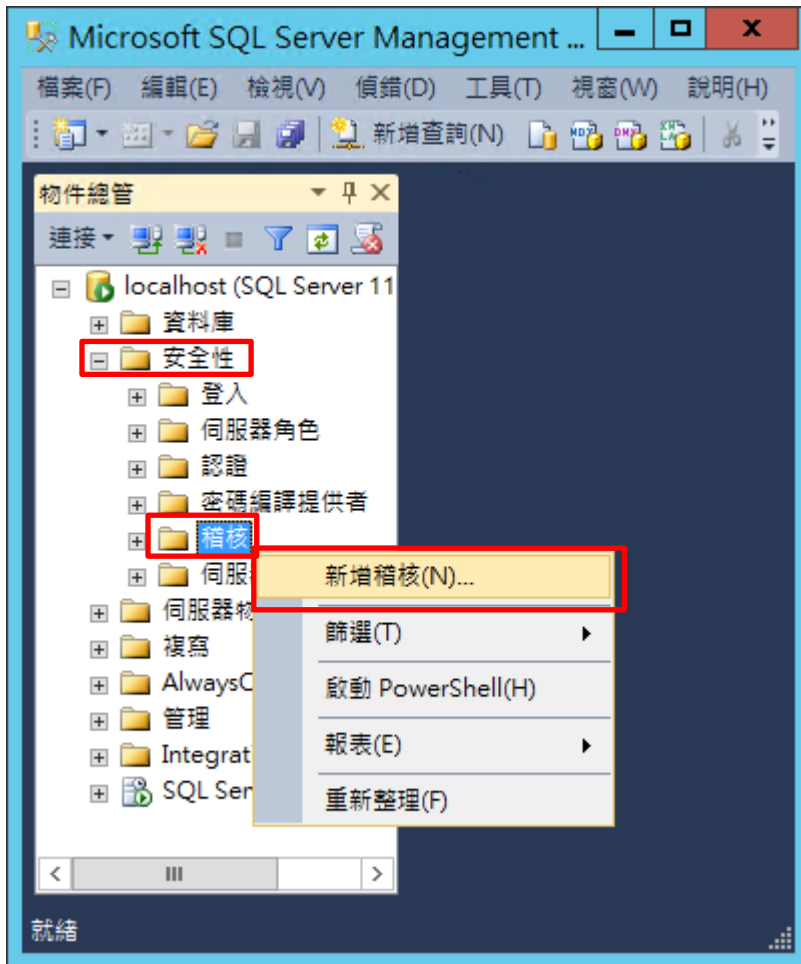
(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

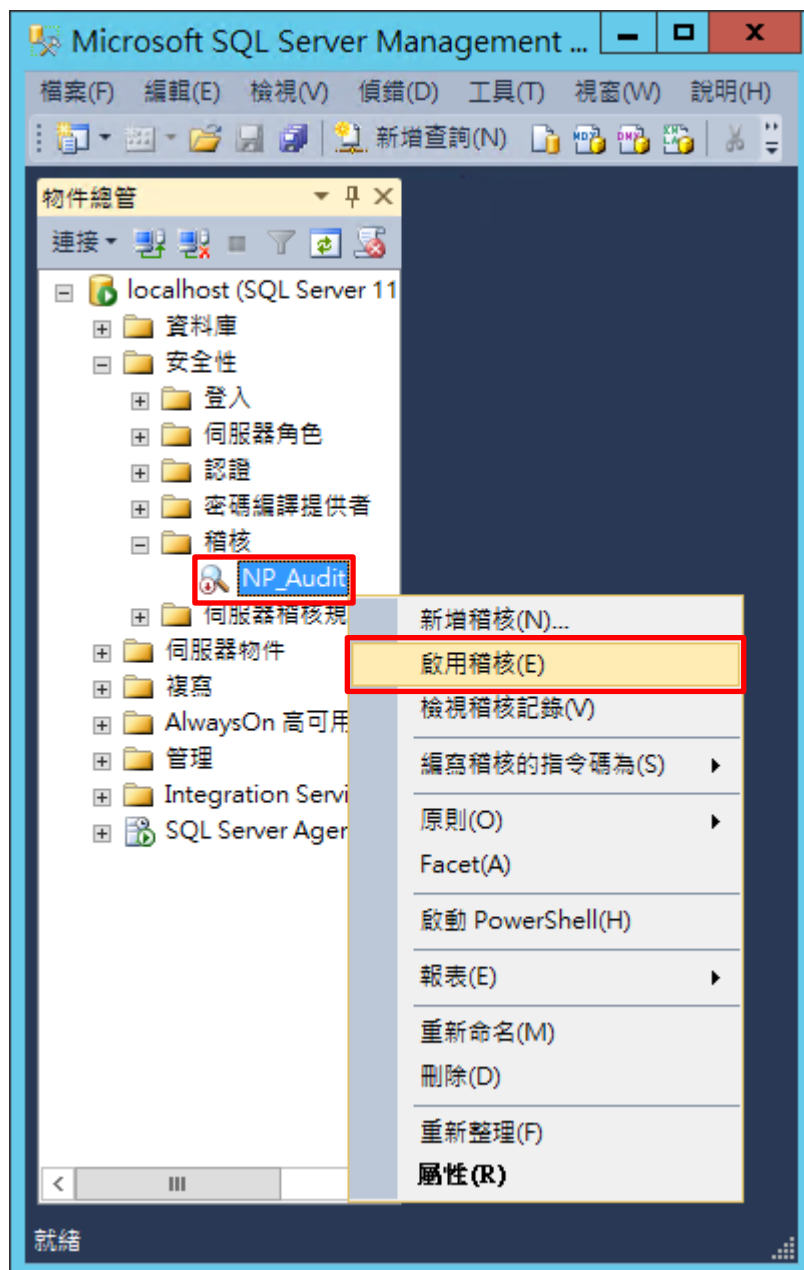


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



(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]

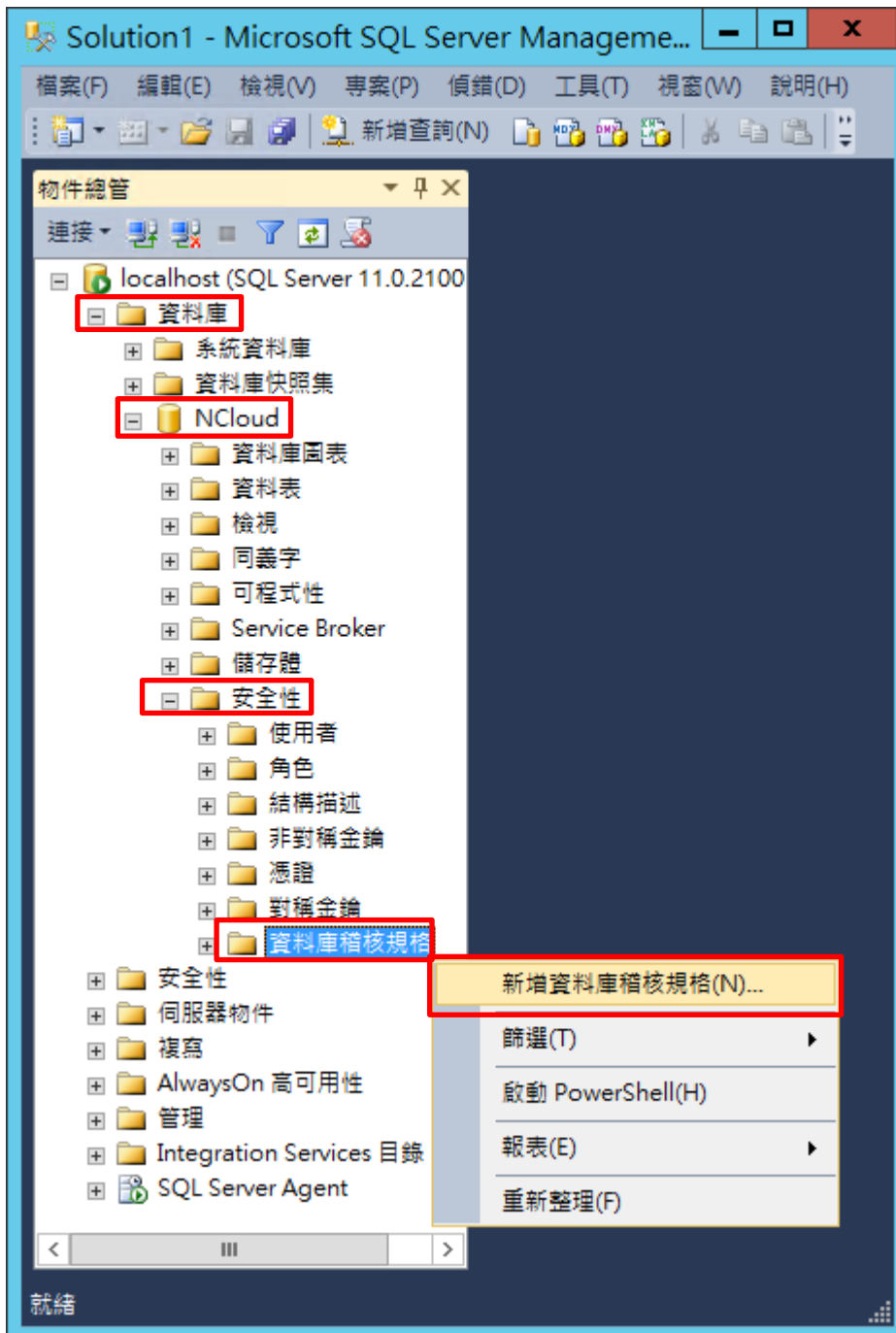
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



(6) 按 [關閉]



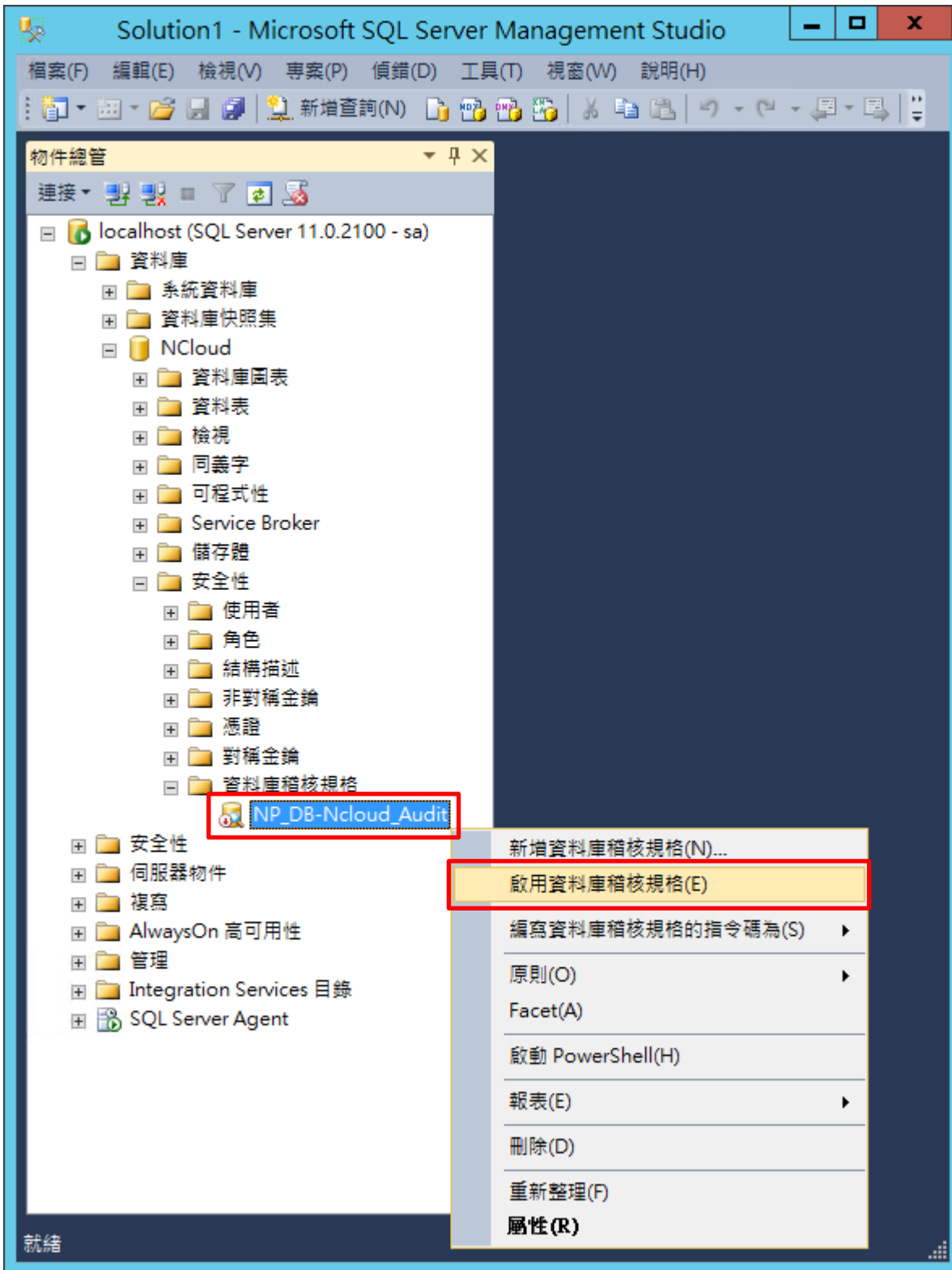
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



(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 -P npartner
```

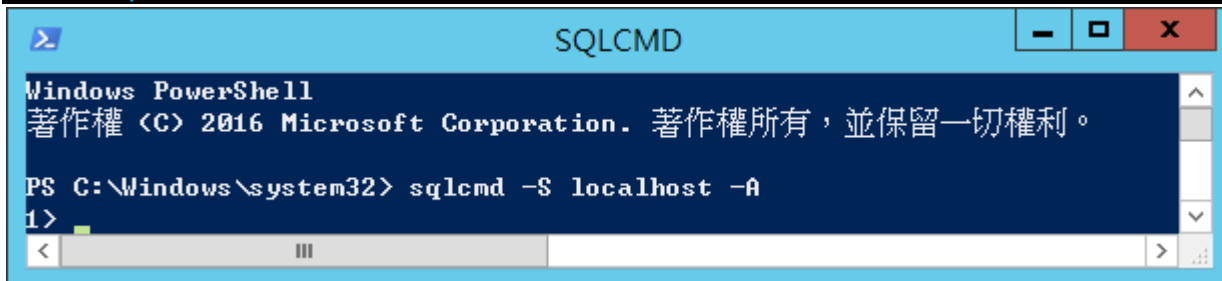


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

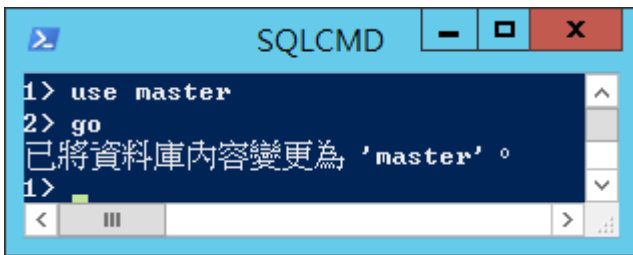
(2.2) 使用 Windows 帳號

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



(3) 切換資料庫

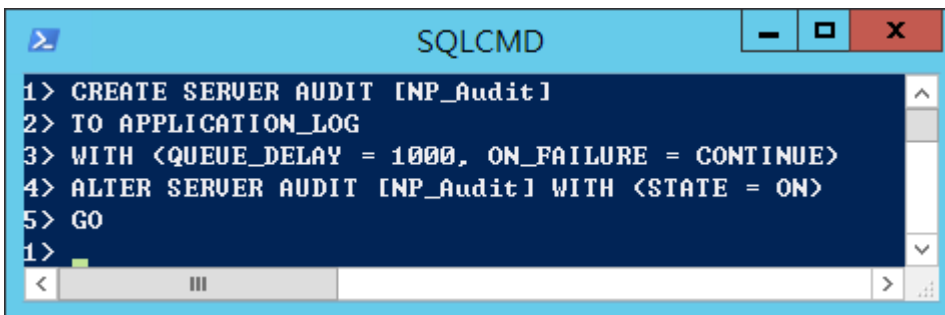
```
1 > use master
2 > go
```



```
SQLCMD
1> use master
2> go
已將資料庫內容變更為 '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

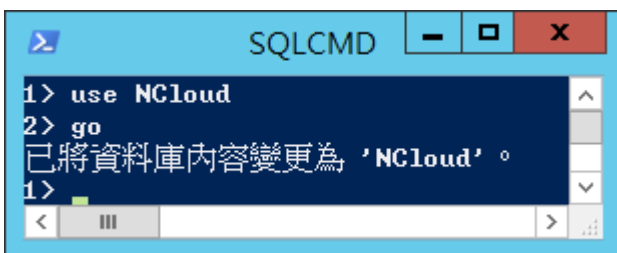
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
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>
```

(5) 切換到稽核資料庫 · 範例：NCloud

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




```
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_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 > WITH (STATE = ON)
14 > GO
1 > quit
```



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerShell". The command prompt displays the following SQL Server commands:

```
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_OWNERSHIP_CHANGE_GROUP>,
11 > ADD <FAILED_DATABASE_AUTHENTICATION_GROUP>,
12 > ADD <DATABASE_OBJECT_CHANGE_GROUP>
13 > WITH <STATE = ON>
14 > GO
1 > quit
PS C:\Windows\system32>
```

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。

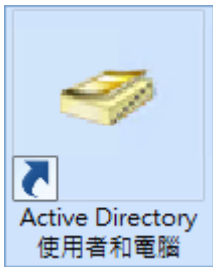
以下分別為網域和工作群組設定方式。

3.3.1 網域

3.3.1.1 組織單位設定

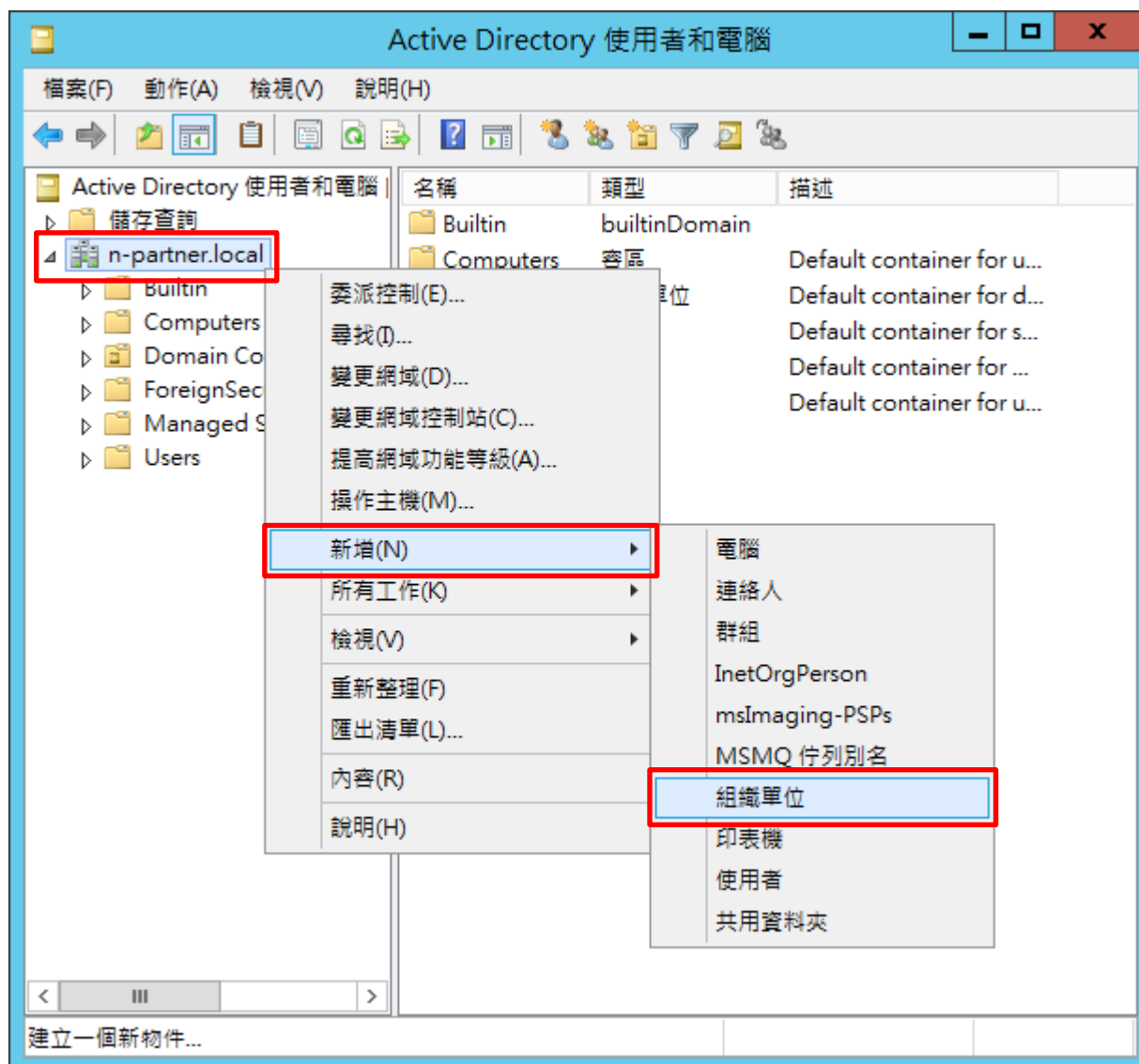
(1) 開啟 AD 使用者和電腦

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]



新增物件 - 組織單位

建立於: n-partner.local/

名稱(A):
Server

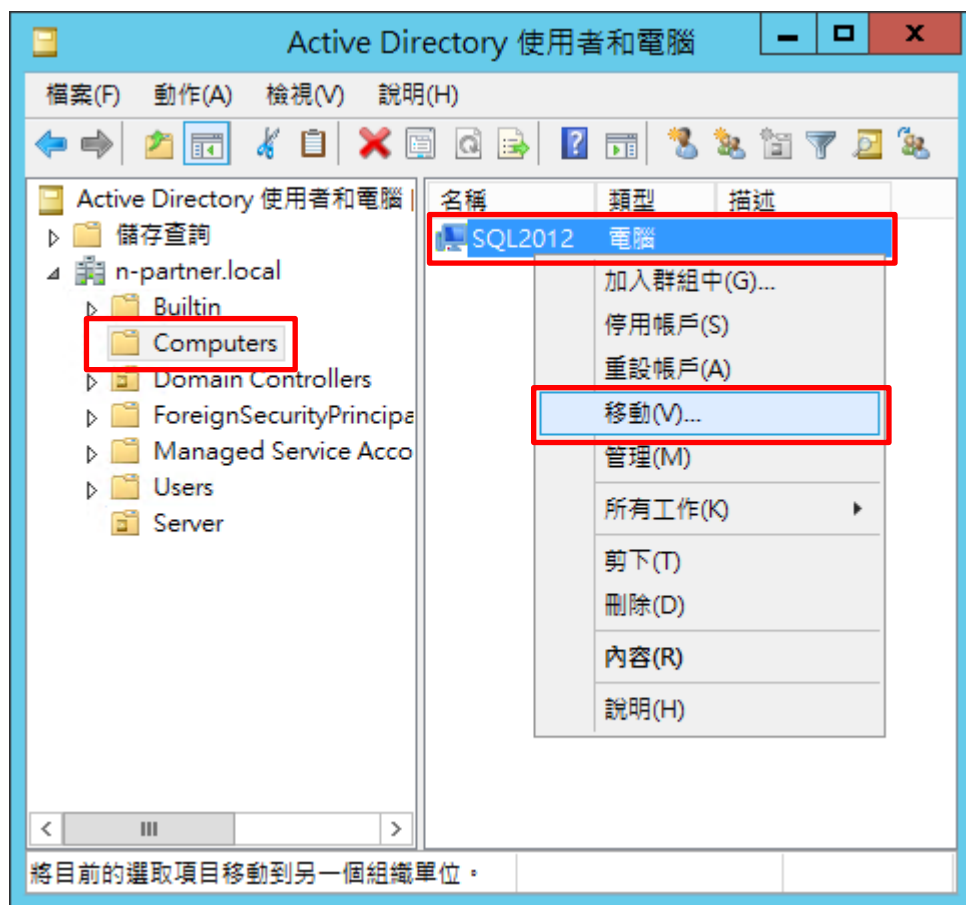
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

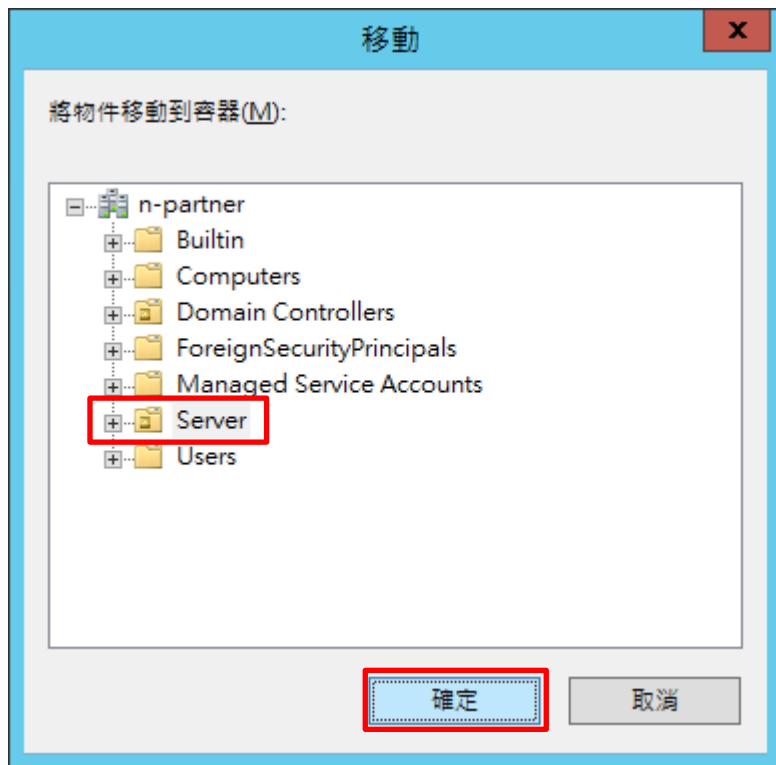
選擇 [Computers] 組織單位 -> 在 [SQL2012] 伺服器，按滑鼠右鍵 註：請依客戶環境選擇 MS SQL Server 主機

-> 點選 [移動]



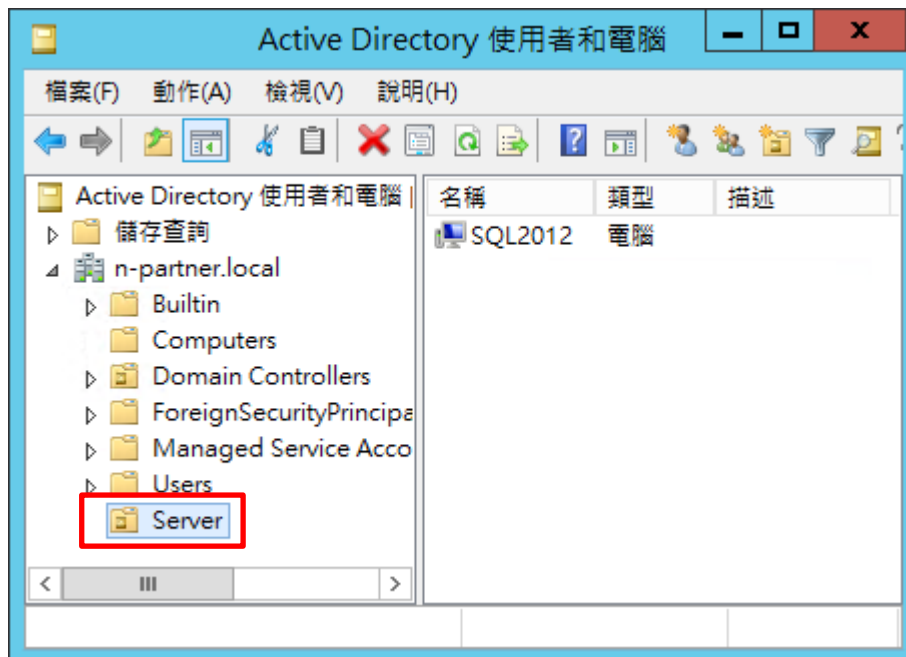
(5) 選擇組織單位

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

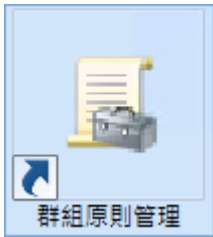
點選 [Servers] 組織單位，確認 SQL2012 伺服器已移動。



3.3.1.2 群組原則設定

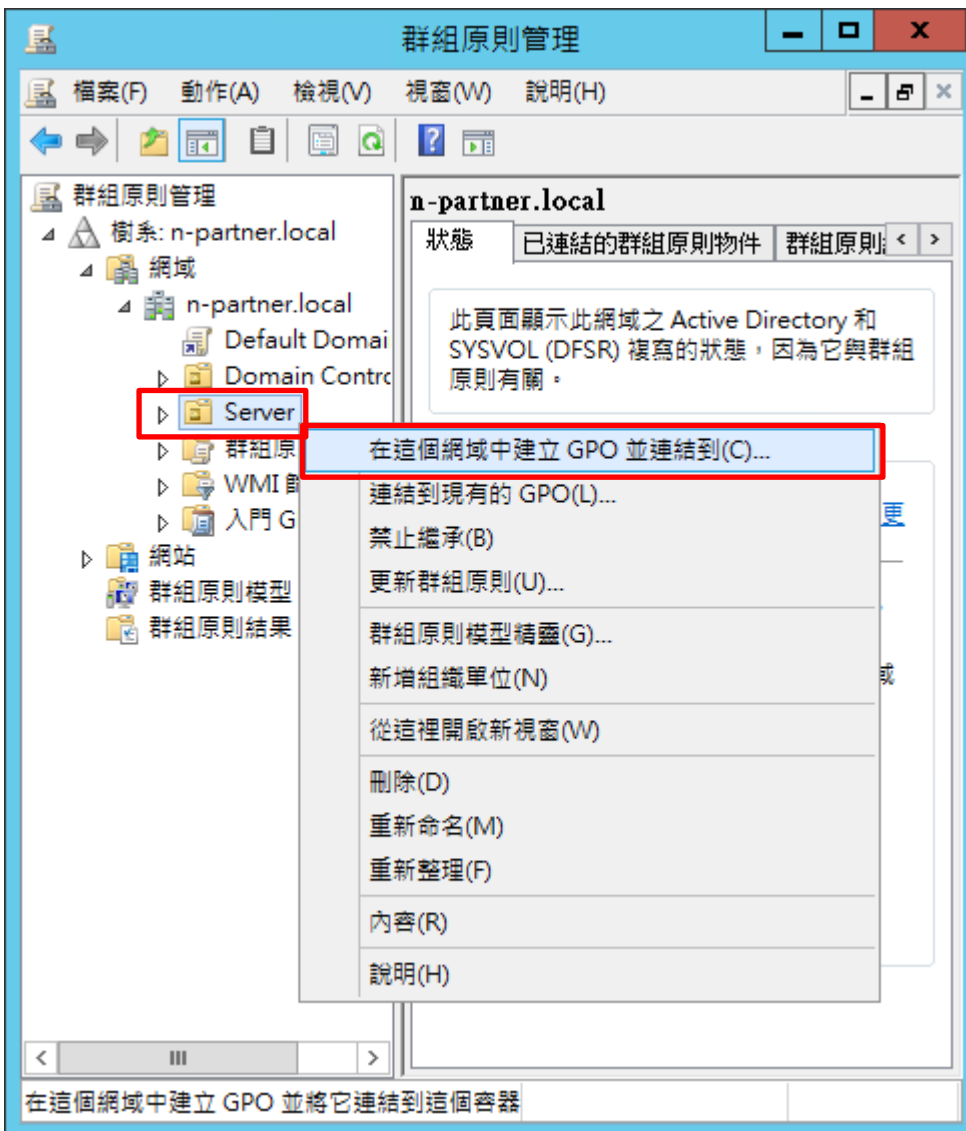
(1) 開啟群組原則管理

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...]



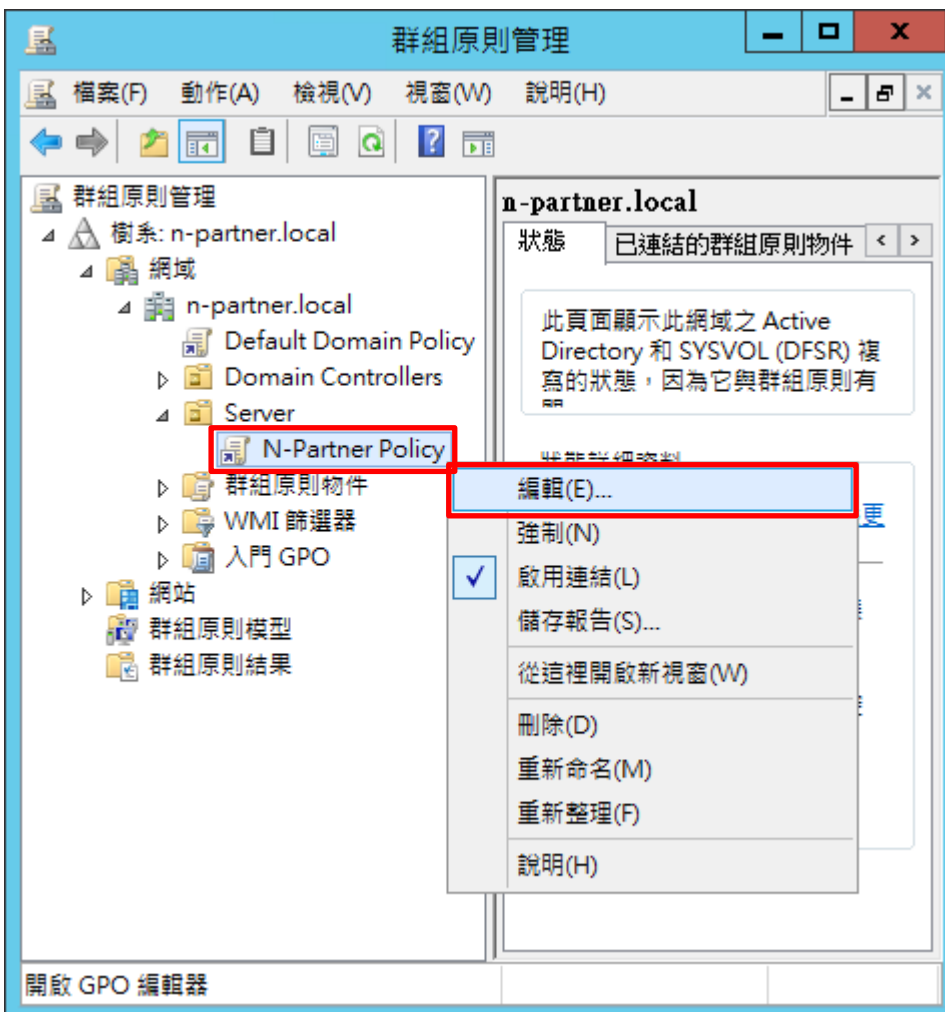
(3) 輸入群組原則物件名稱

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]



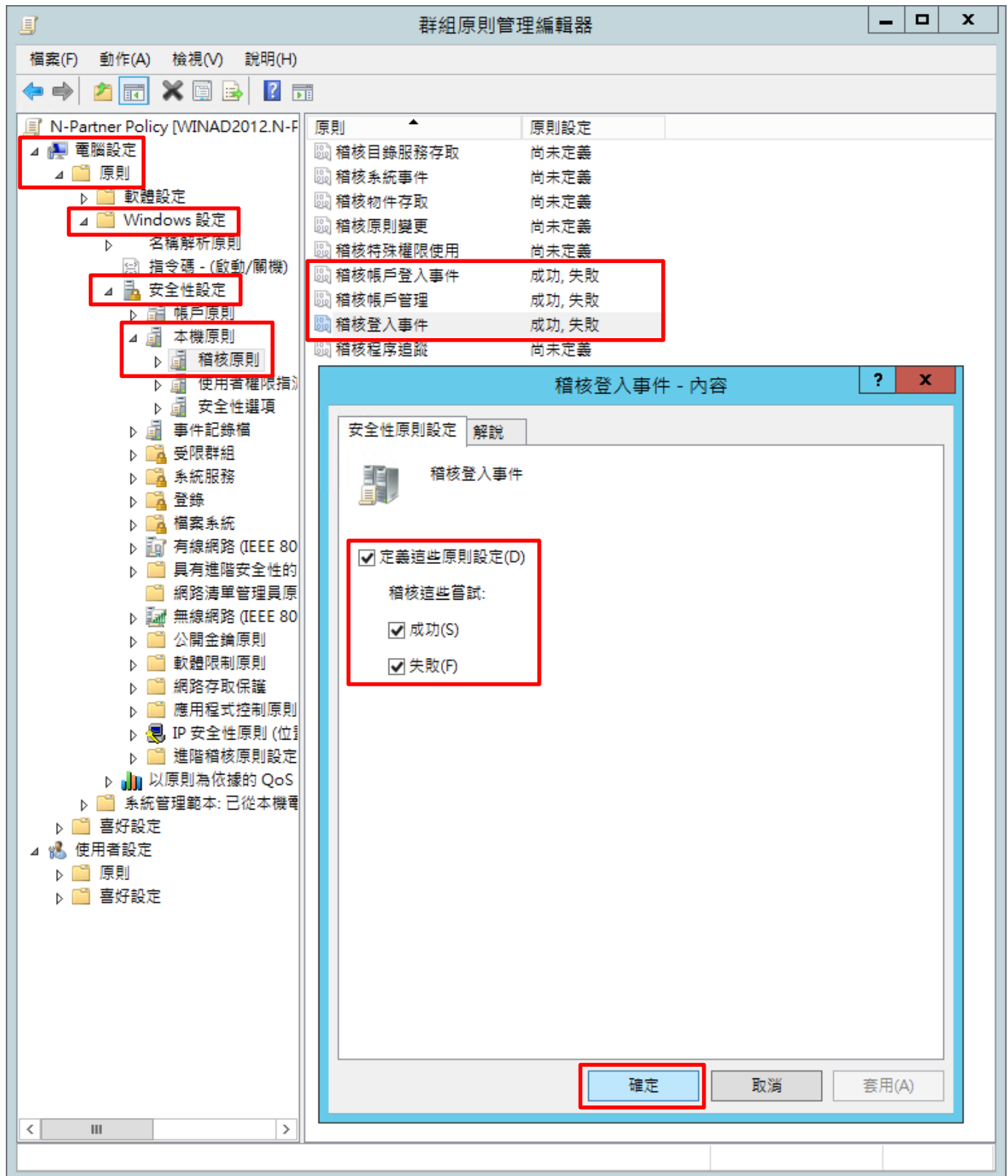
(4) 編輯群組原則物件

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



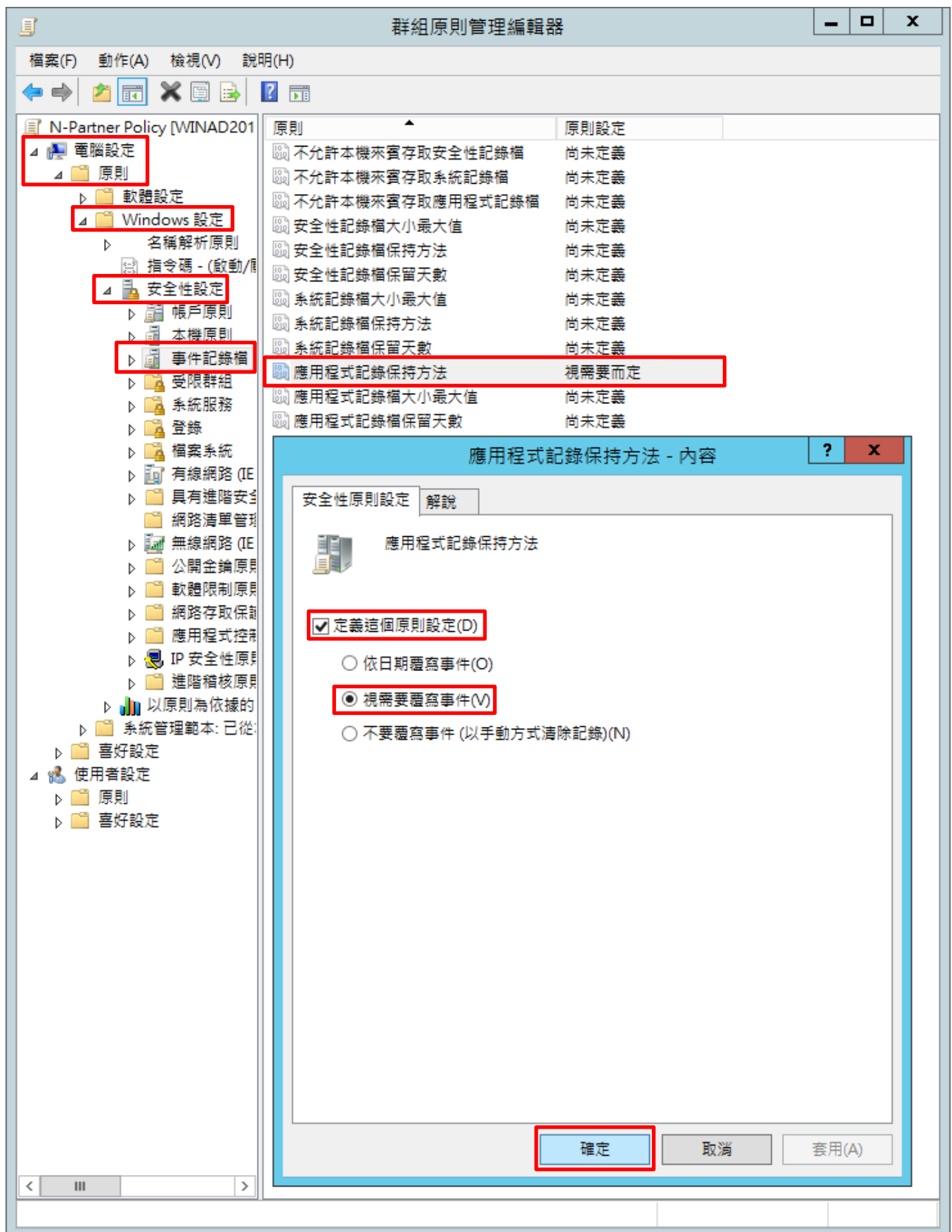
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [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]



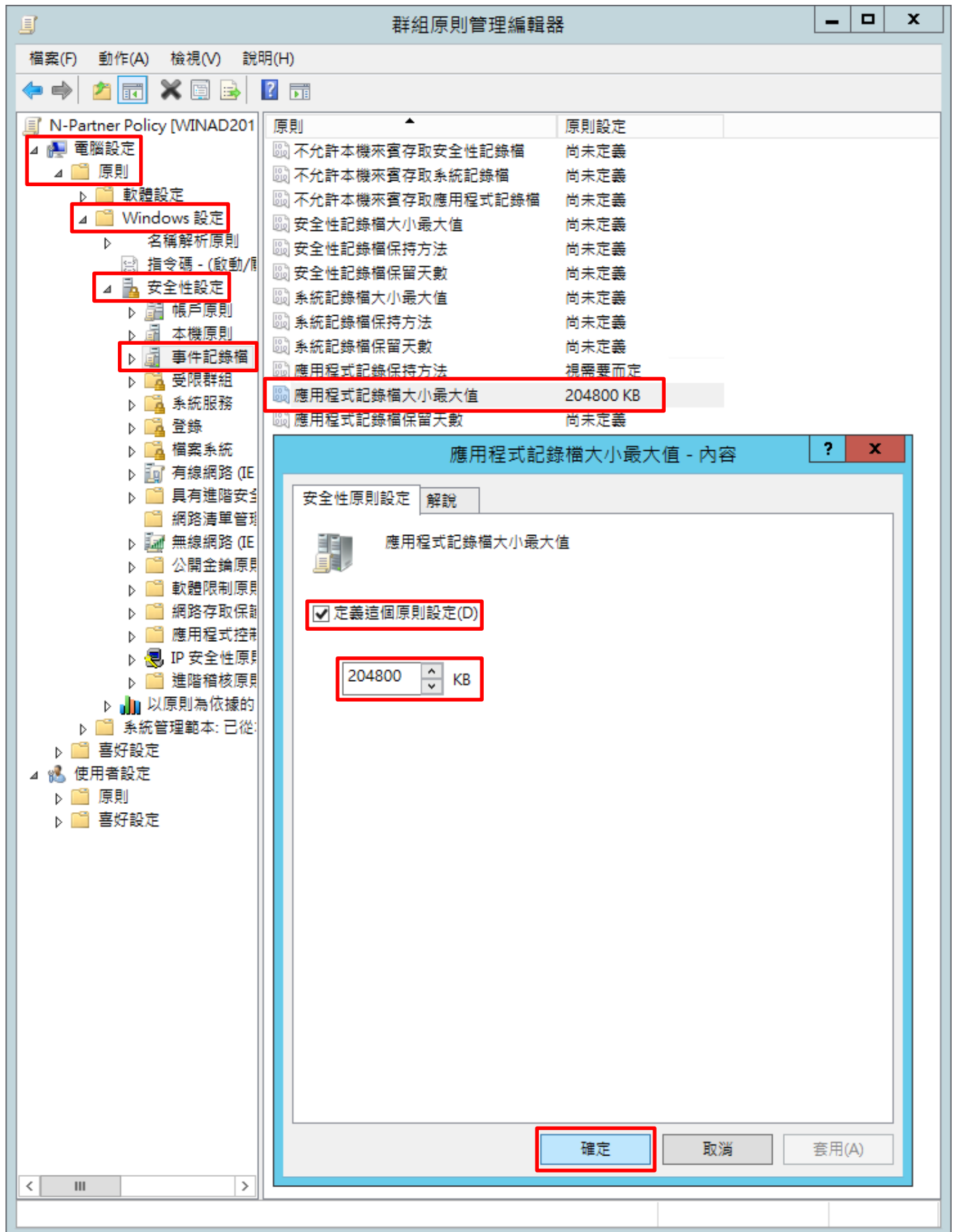
(6) 事件記錄檔：應用程式記錄保持方法

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) 事件記錄檔：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]
-> 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]

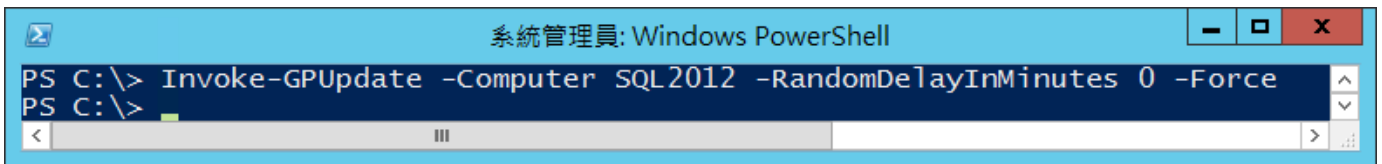


(8) 在 AD 網域伺服器 -> 開啟 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

```
PS C:\> Invoke-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

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

The screenshot shows a web browser window with the address bar displaying 'C:\tmp\SQL2012.html' and the page title '群組原則結果'. The main content area shows a tree view of policy settings for the computer 'N-PARTNER\SQL2012'. The data is as follows:

Category	Item	Status	Priority
群組原則結果			
N-PARTNER\SQL2012			
資料收集: 22/10/2021 10:13:34			
摘要		顯示全部	
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]



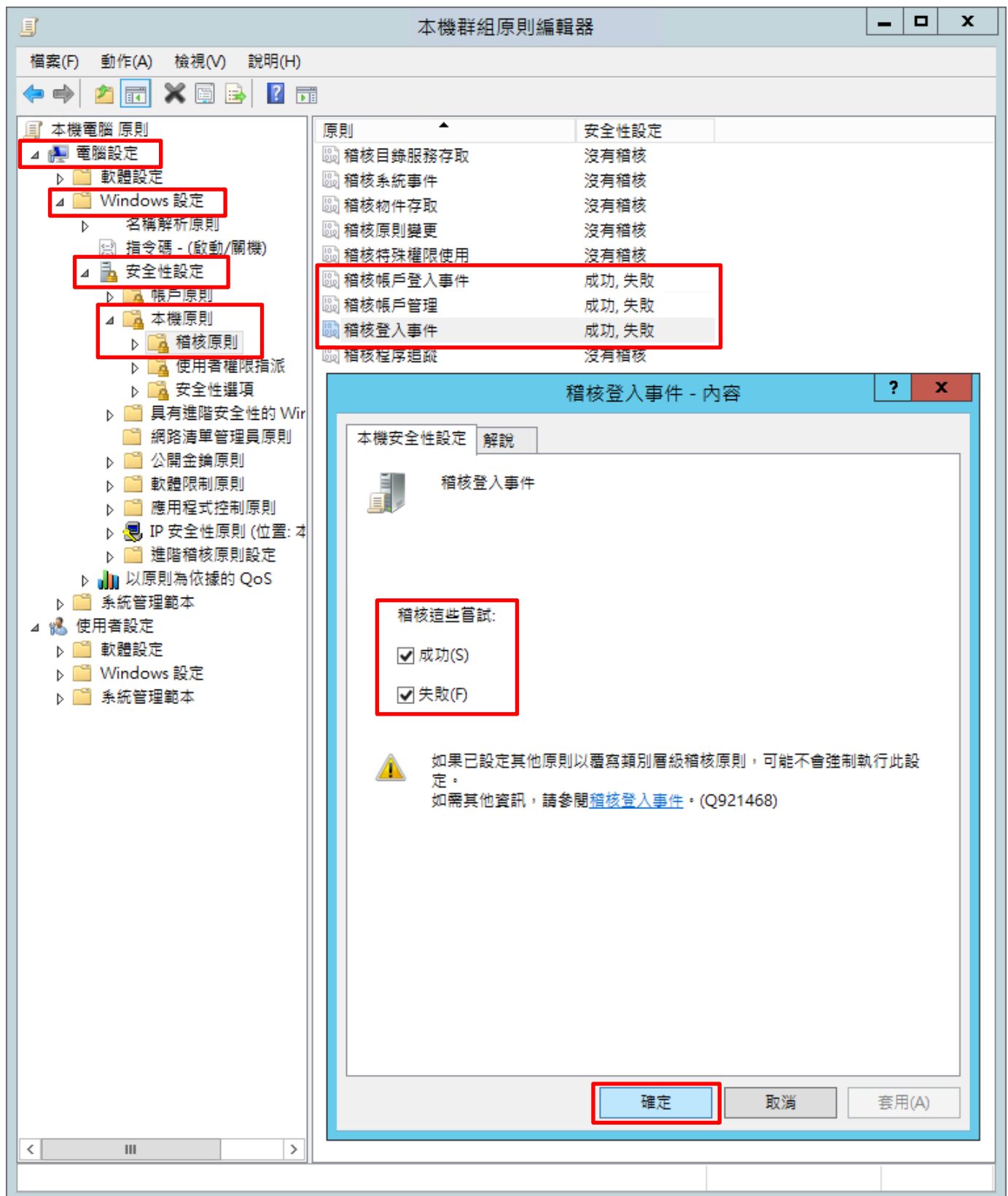
(2) 搜尋群組原則物件編輯器並執行

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]

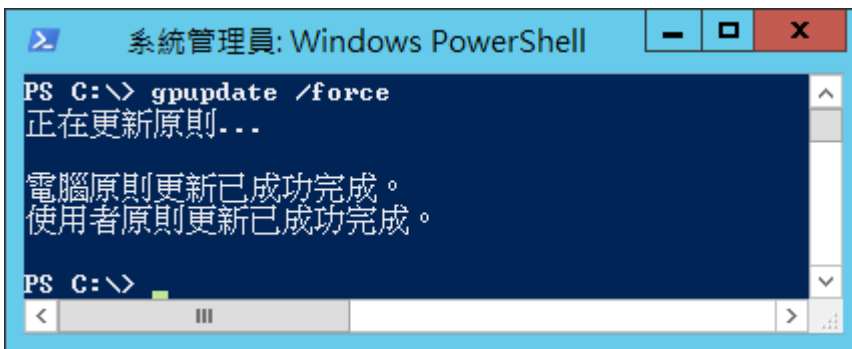


(4) 開啟 [Windows PowerShell]



(5) 更新群組原則

PS C:\> gpupdate /force



(6) 查看群組原則套用情形

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

```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
系統稽核原則
類別/子類別          設定
系統
安全性系統延伸      沒有稽核
系統完整性          成功與失敗
IPSEC driver        沒有稽核
其他系統事件        成功與失敗
安全性狀態變更      成功
登入/登出
登入                成功與失敗
登出                成功與失敗
帳戶鎖定            成功與失敗
IPsec 主要模式      成功與失敗
IPsec 快速模式      成功與失敗
IPsec 延伸模式      成功與失敗
特殊登入            成功與失敗
其他登入/登出事件  成功與失敗
網路原則伺服器      成功與失敗
使用者/裝置宣告     成功與失敗
物件存取
檔案系統            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
卸除式存放裝置      沒有稽核
集中原則暫存        沒有稽核
特殊權限使用
非機密特殊權限使用  沒有稽核
其他特殊權限使用事件 沒有稽核
機密特殊權限使用    沒有稽核
詳細追蹤
建立處理程序        沒有稽核
終止處理程序        沒有稽核
DPIAPI 活動          沒有稽核
RPC 事件             沒有稽核
原則變更
驗證原則變更        成功
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
稽核原則變更        成功
帳戶管理
使用者帳戶管理      成功與失敗
電腦帳戶管理        成功與失敗
安全性群組管理      成功與失敗
發佈群組管理        成功與失敗
應用程式群組管理    成功與失敗
其他帳戶管理事件    成功與失敗
DS 存取
目錄服務變更        沒有稽核
目錄服務複寫        沒有稽核
詳細目錄服務複寫    沒有稽核
目錄服務存取        成功
帳戶登入
Kerberos 服務票證操作 成功與失敗
其他帳戶登入事件    成功與失敗
Kerberos 驗證服務    成功與失敗
認證驗證            成功與失敗
PS C:\>
```

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]



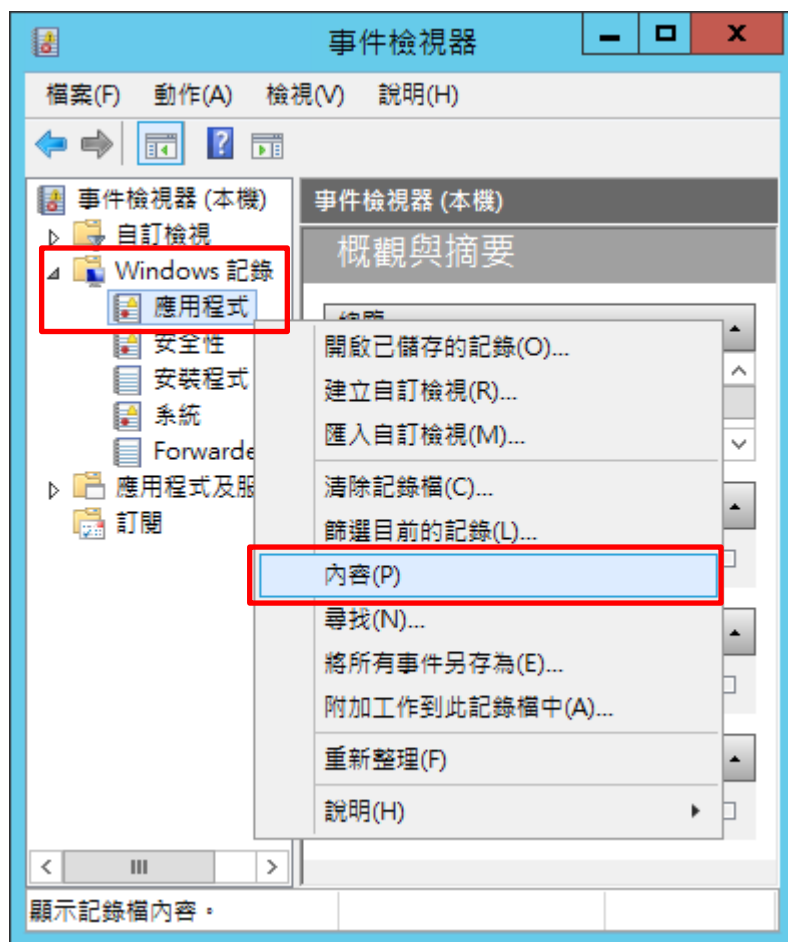
(2) 搜尋事件檢視器並執行

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]

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: 3.07 MB(3,215,360 位元組)

建立日期: 2021年6月11日 17:44:03

修改日期: 2021年7月5日 10:39:17

存取日期: 2021年6月11日 17:44:03

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

確定 取消 套用(P)

4. SQL 2016

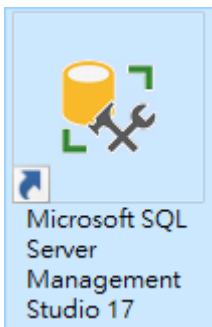
4.1 稽核登入

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。

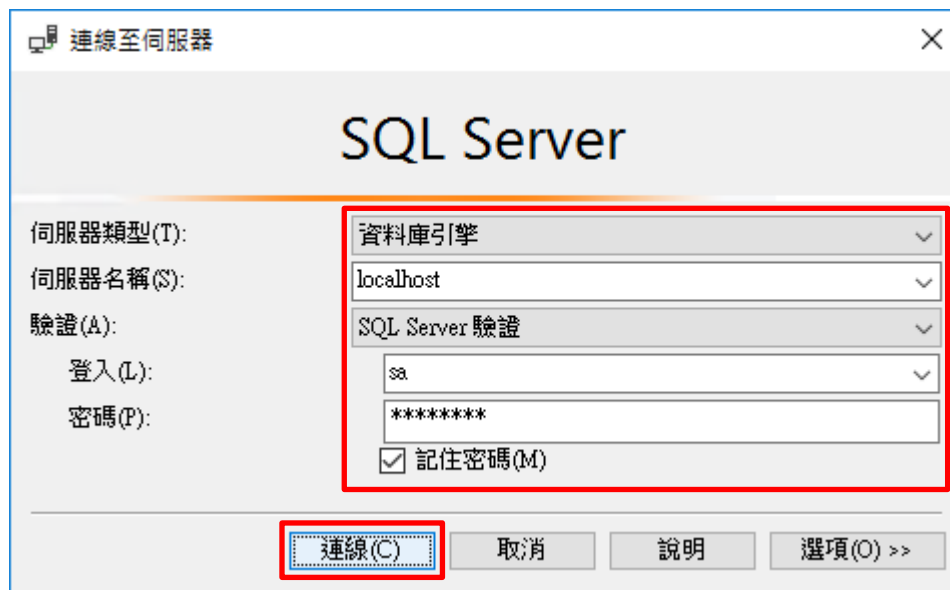
以下分別為圖形介面和指令介面設定方式。

4.1.1 使用圖形介面方式設定

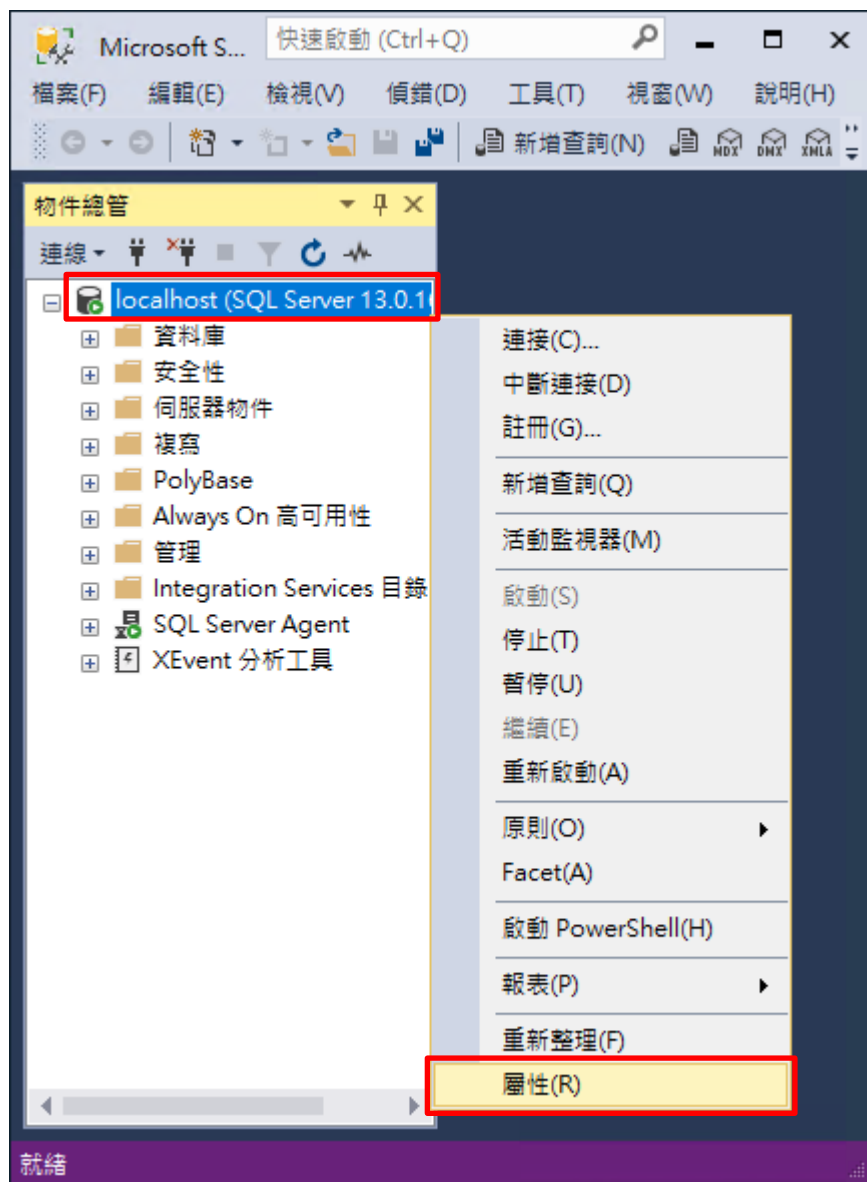
(1) 開啟 [Microsoft SQL Server Management Studio]



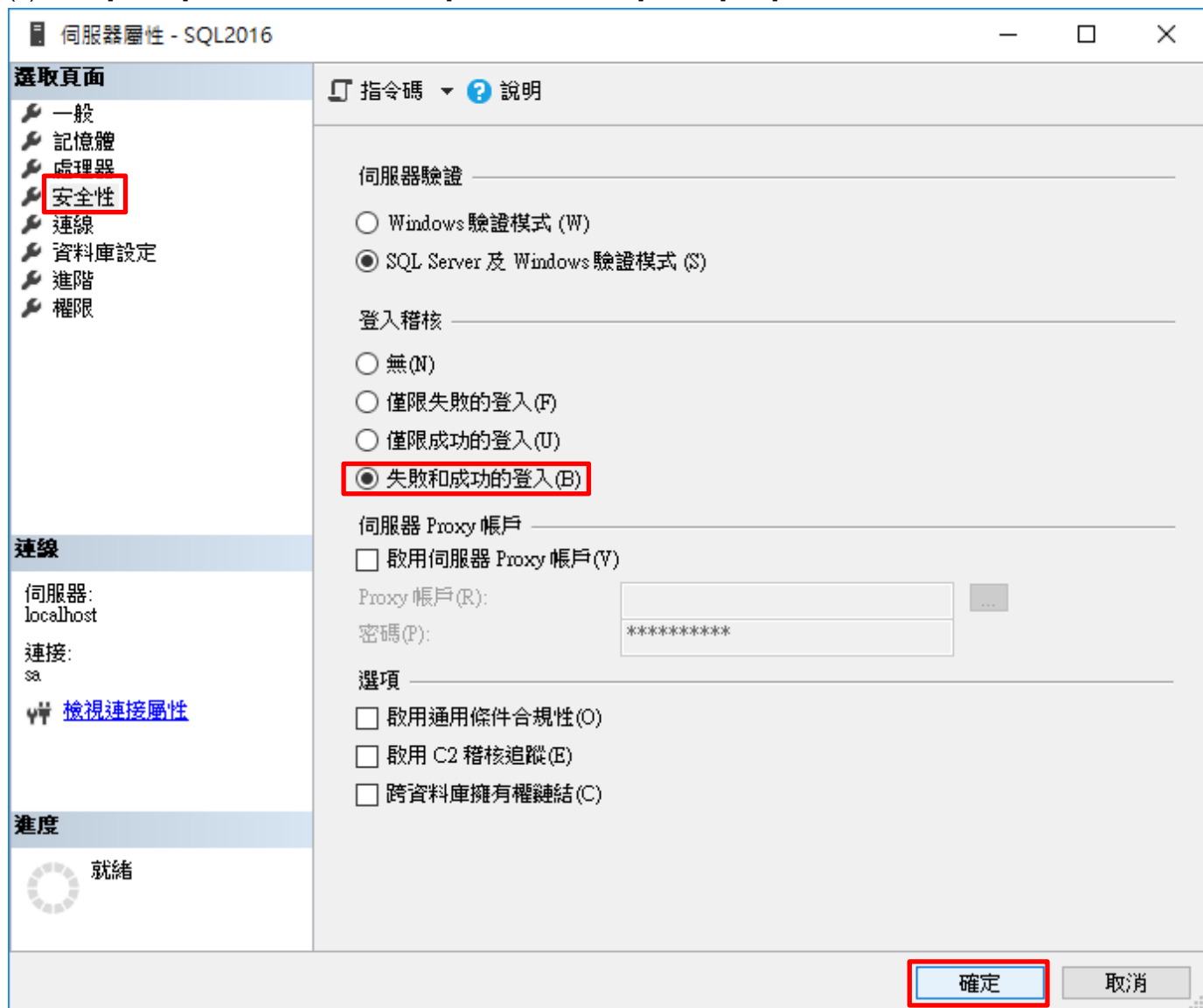
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

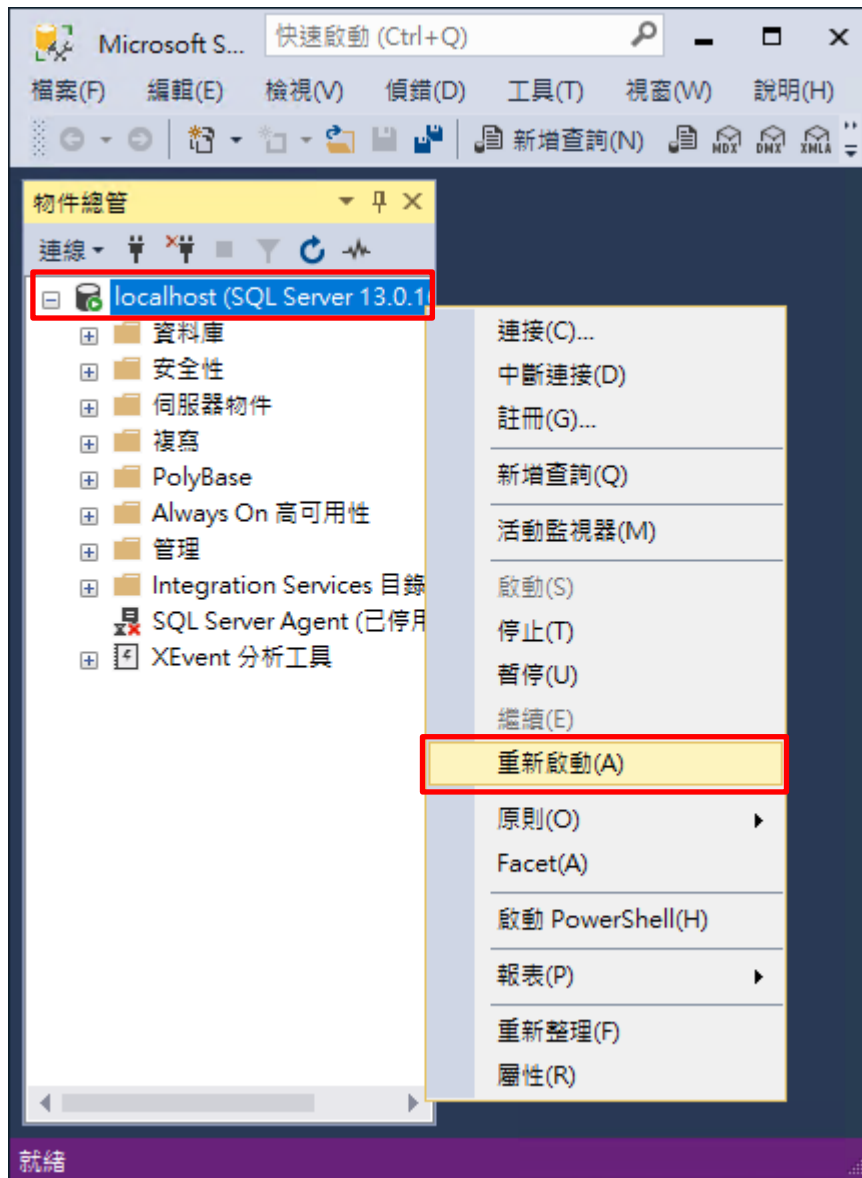


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

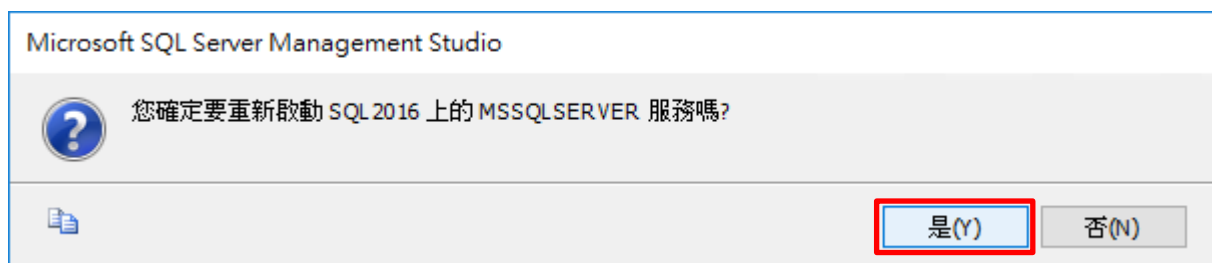


(5) 重新啟動 MS SQL SERVER 服務

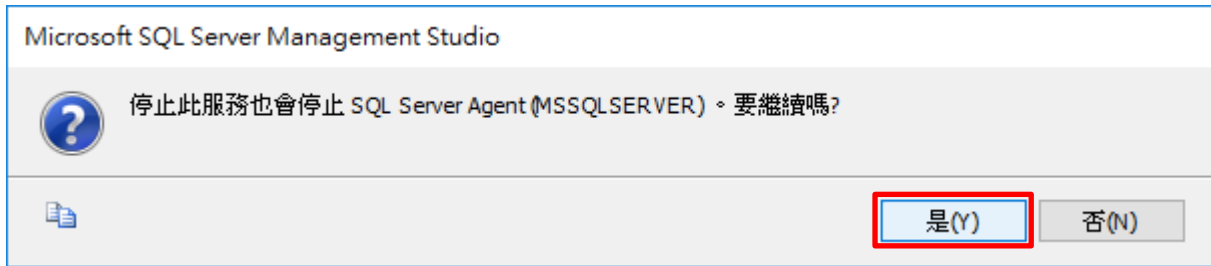
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務



(7) 按 [是] 停止 SQL SERVER Agent 服務



4.1.2 使用指令介面方式設定

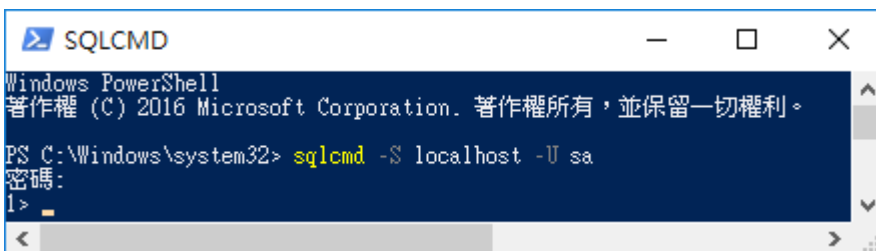
(1) 開啟 [Windows PowerShell]



(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
```

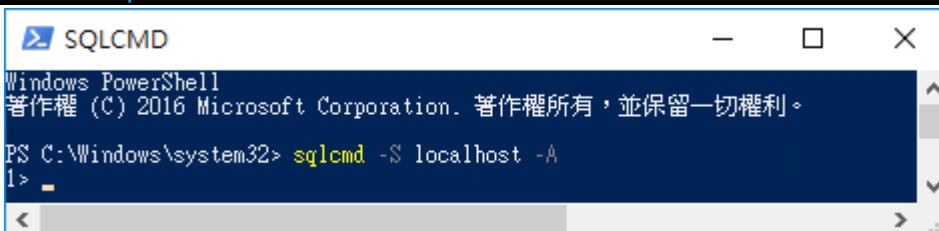


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

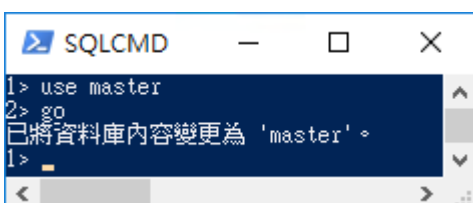
(2.2) 使用 Windows 帳號

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



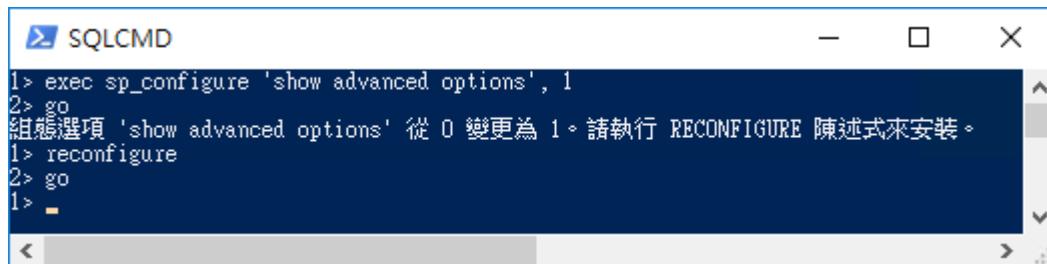
(3) 切換資料庫

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



(4) 使用 sp_configure 列出進階選項

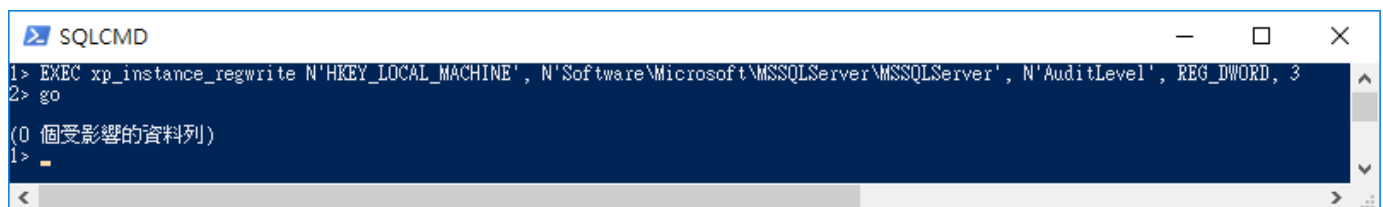
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
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

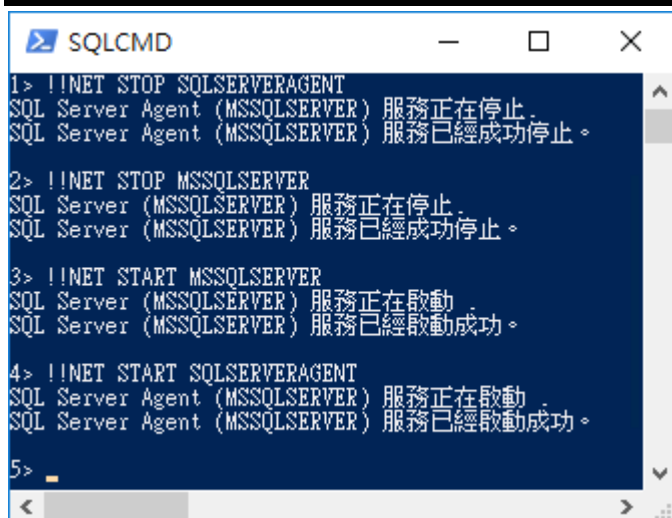
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
```



```
SQLCMD
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>
```

(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
```



```
SQLCMD
1> !!NET STOP SQLSERVERAGENT
SQL Server Agent (MSSQLSERVER) 服務正在停止。
SQL Server Agent (MSSQLSERVER) 服務已經成功停止。
2> !!NET STOP MSSQLSERVER
SQL Server (MSSQLSERVER) 服務正在停止。
SQL Server (MSSQLSERVER) 服務已經成功停止。
3> !!NET START MSSQLSERVER
SQL Server (MSSQLSERVER) 服務正在啟動。
SQL Server (MSSQLSERVER) 服務已經啟動成功。
4> !!NET START SQLSERVERAGENT
SQL Server Agent (MSSQLSERVER) 服務正在啟動。
SQL Server Agent (MSSQLSERVER) 服務已經啟動成功。
5>
```


4.2 設定稽核

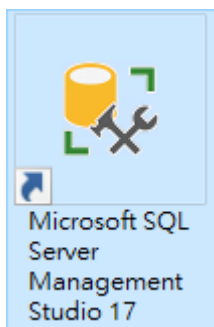
4.2.1 稽核伺服器層級

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。

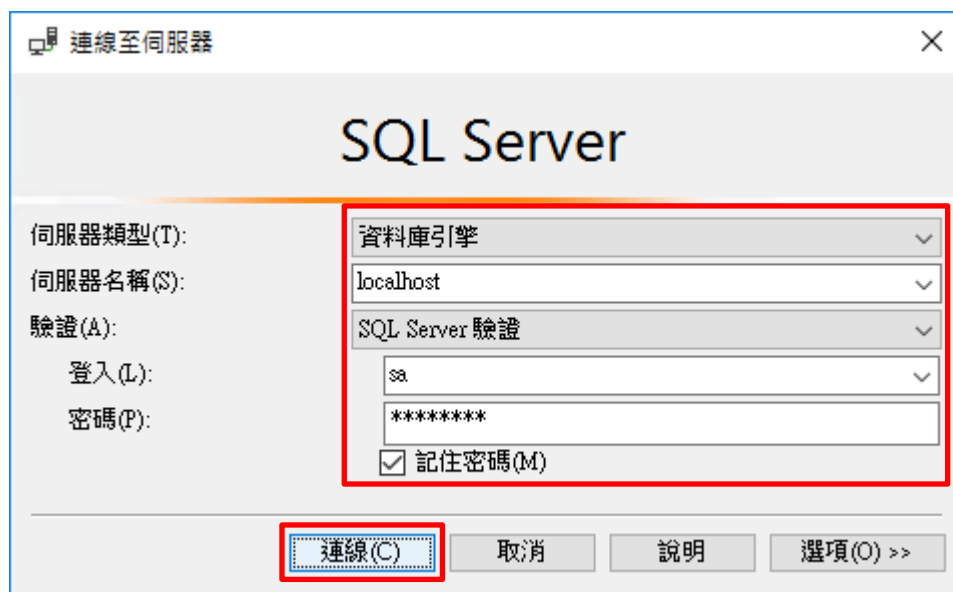
以下分別為圖形介面和指令介面設定方式。

4.2.1.1 使用圖形介面方式設定

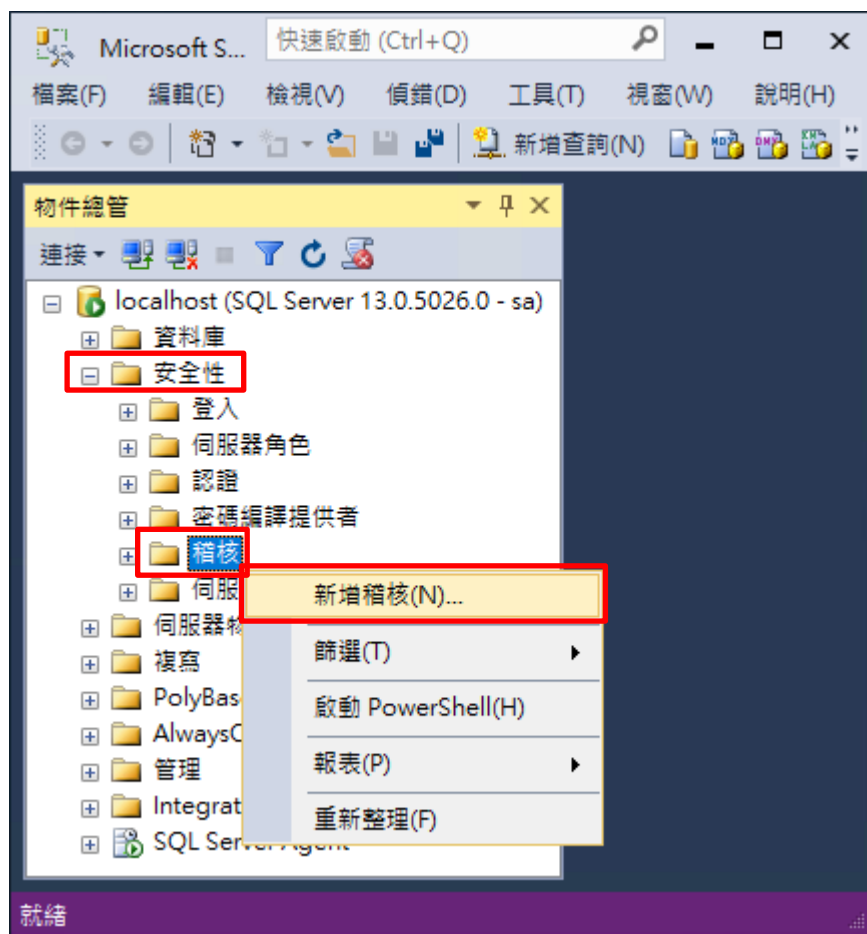
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(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]

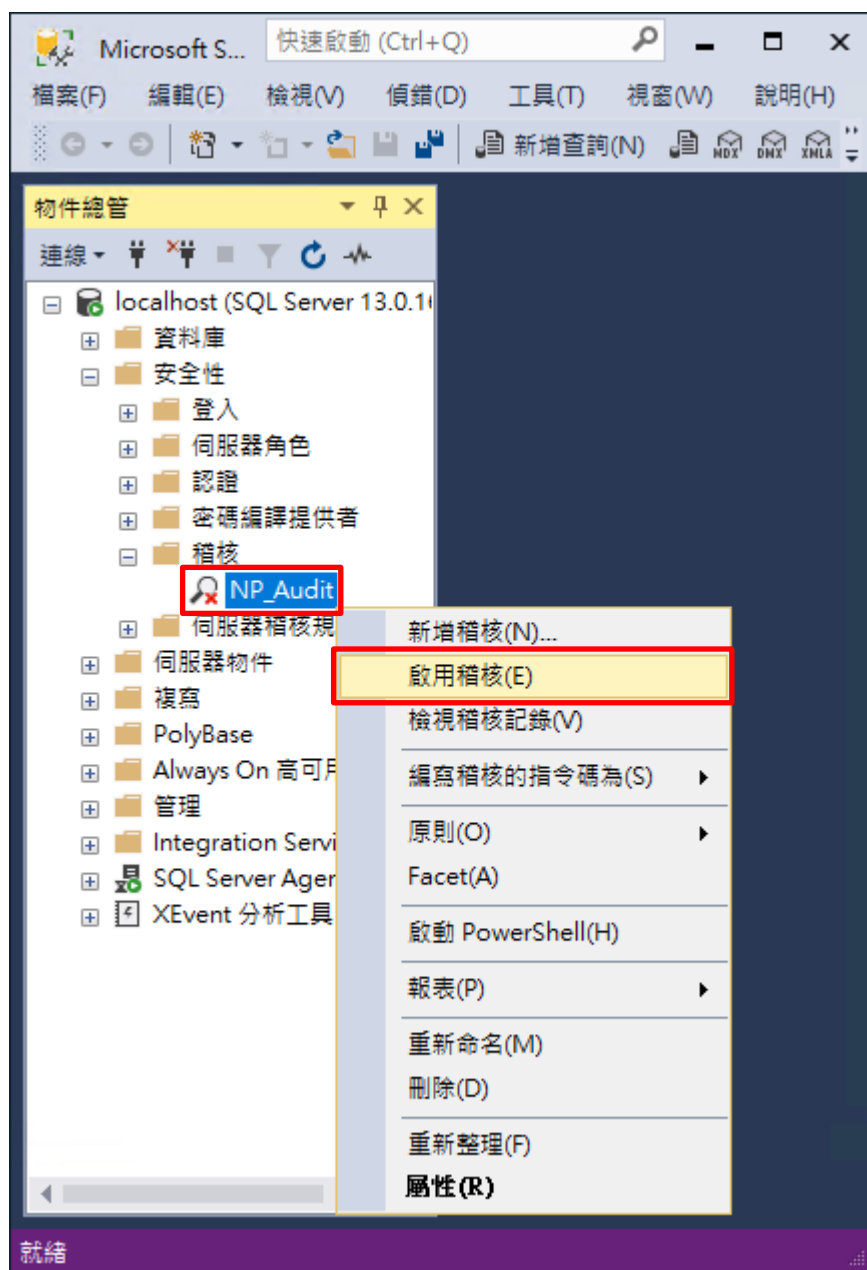
檢視連線屬性

進度

就緒

確定 取消 說明

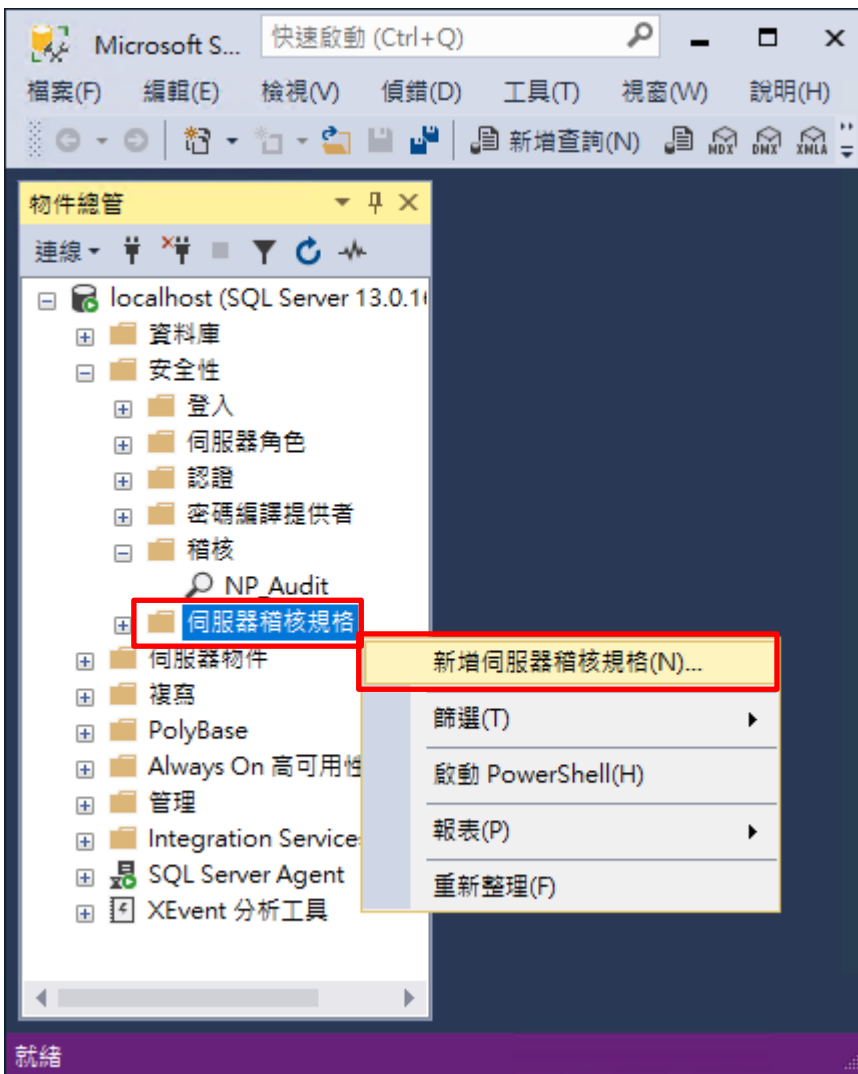
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



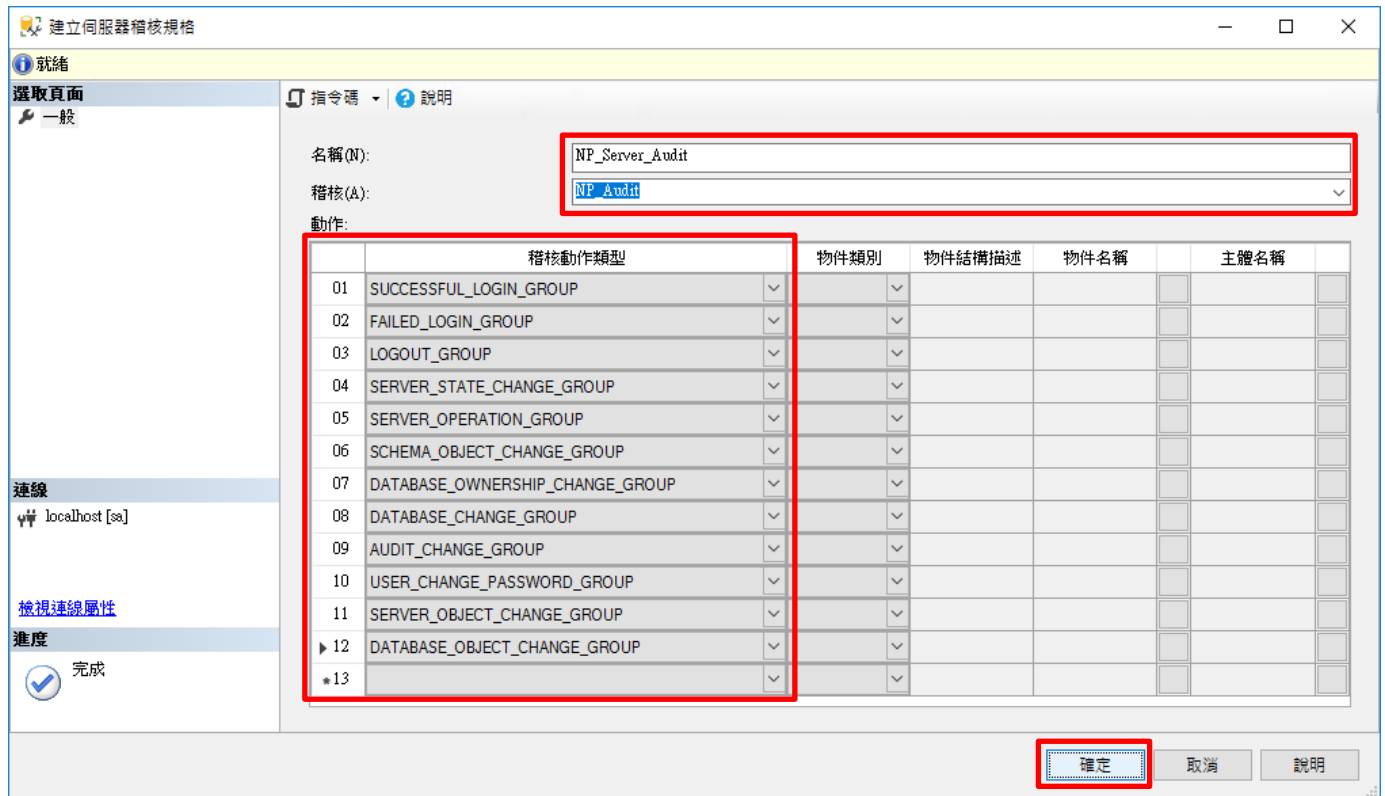
(6) 按 [關閉]



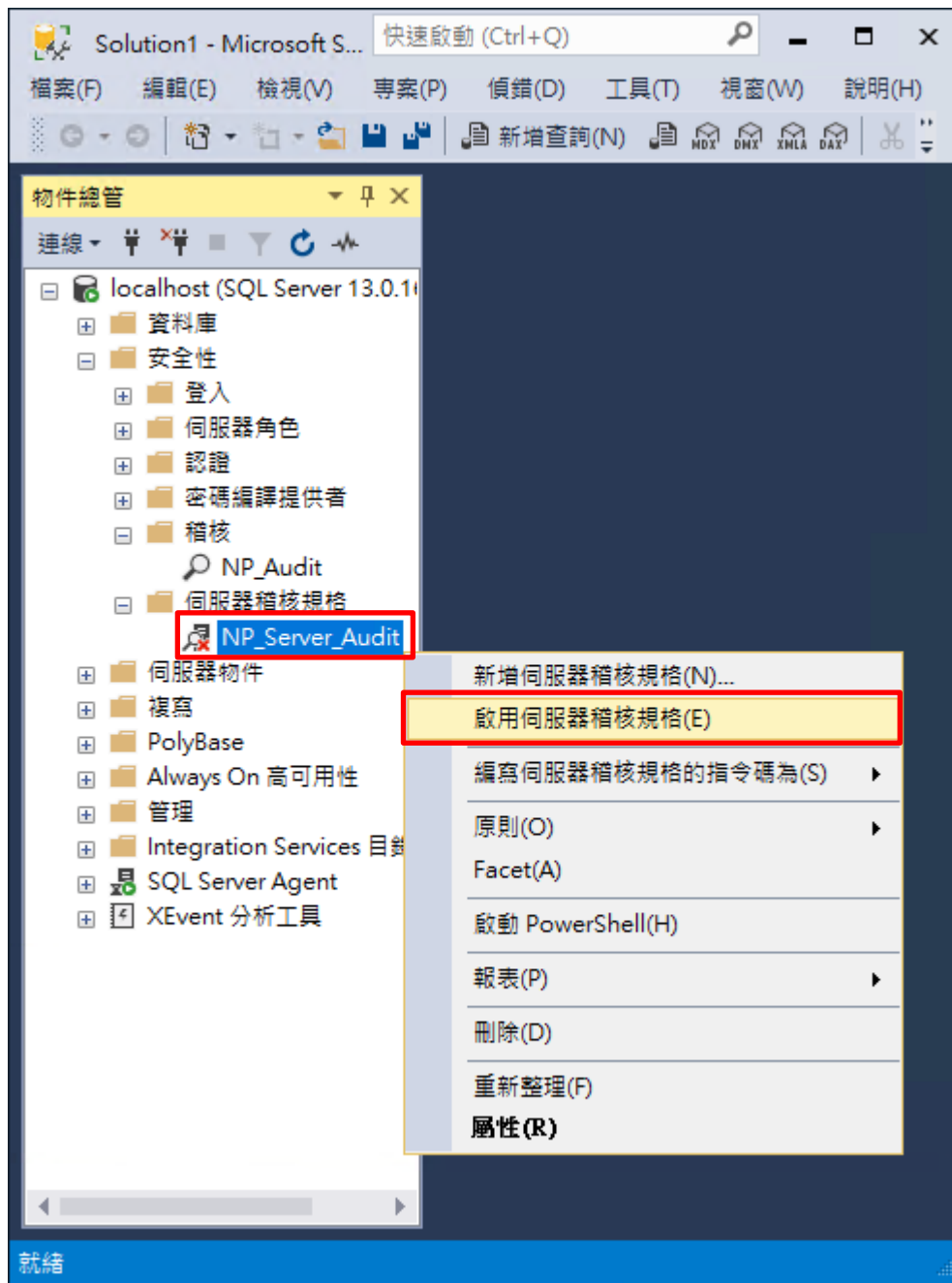
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



(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]

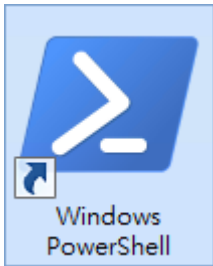


(10) 按 [關閉]



4.2.1.2 使用指令介面方式設定

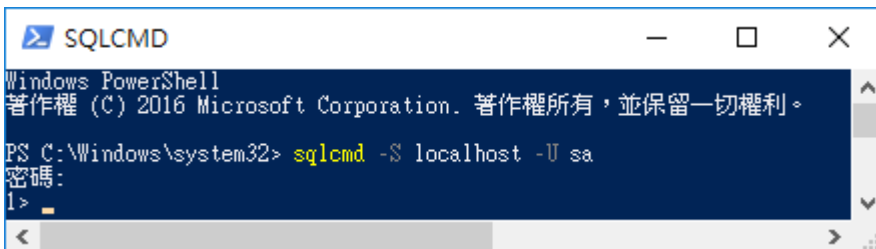
(1) 開啟 [Windows Powershell]



(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
```

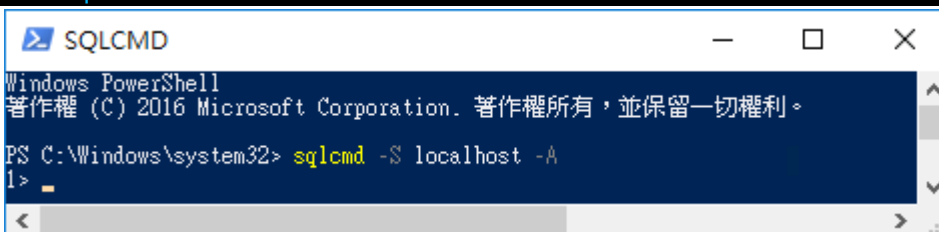


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

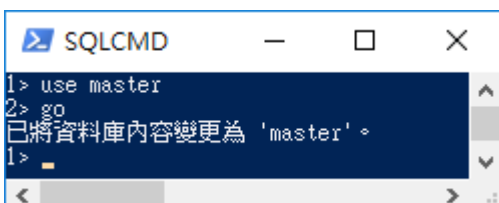
<2.2> 使用 Windows 帳號

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



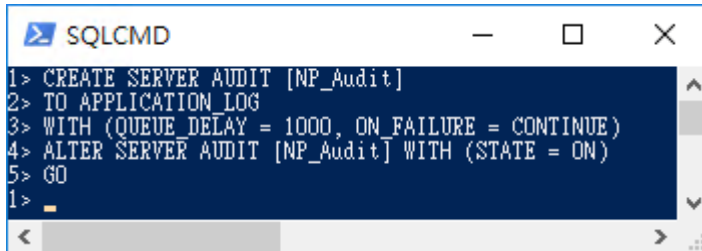
(3) 切換資料庫

```
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
```



```
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
```



The screenshot shows a Windows PowerShell window titled "系統管理員: Windows PowerS...". The console displays the following commands and their execution:

```
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

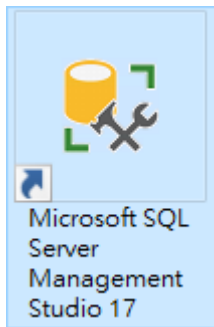
4.2.2 稽核資料庫層級

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。

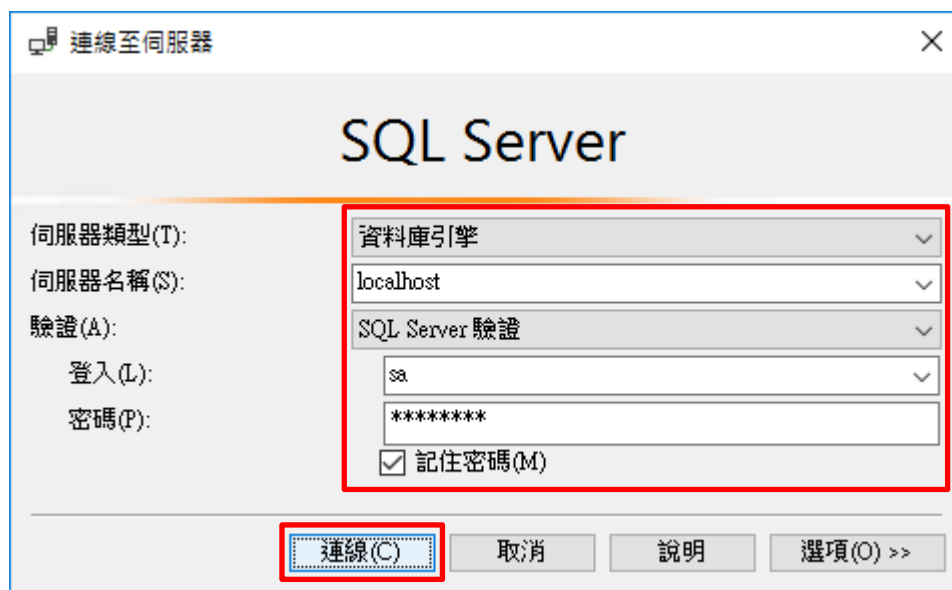
以下分別為圖形介面和指令介面設定方式。

4.2.2.1 使用圖形介面方式設定

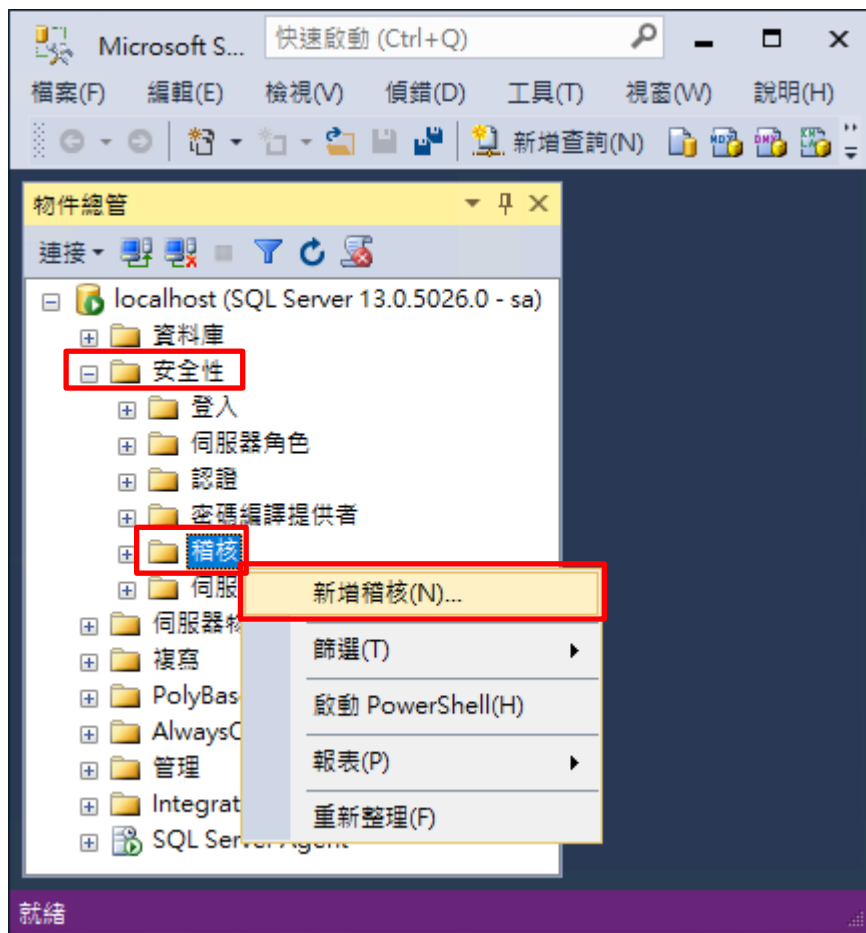
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(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

Ready

Select a page

一般

篩選

Script | Help

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)

Connection

localhost [sa]

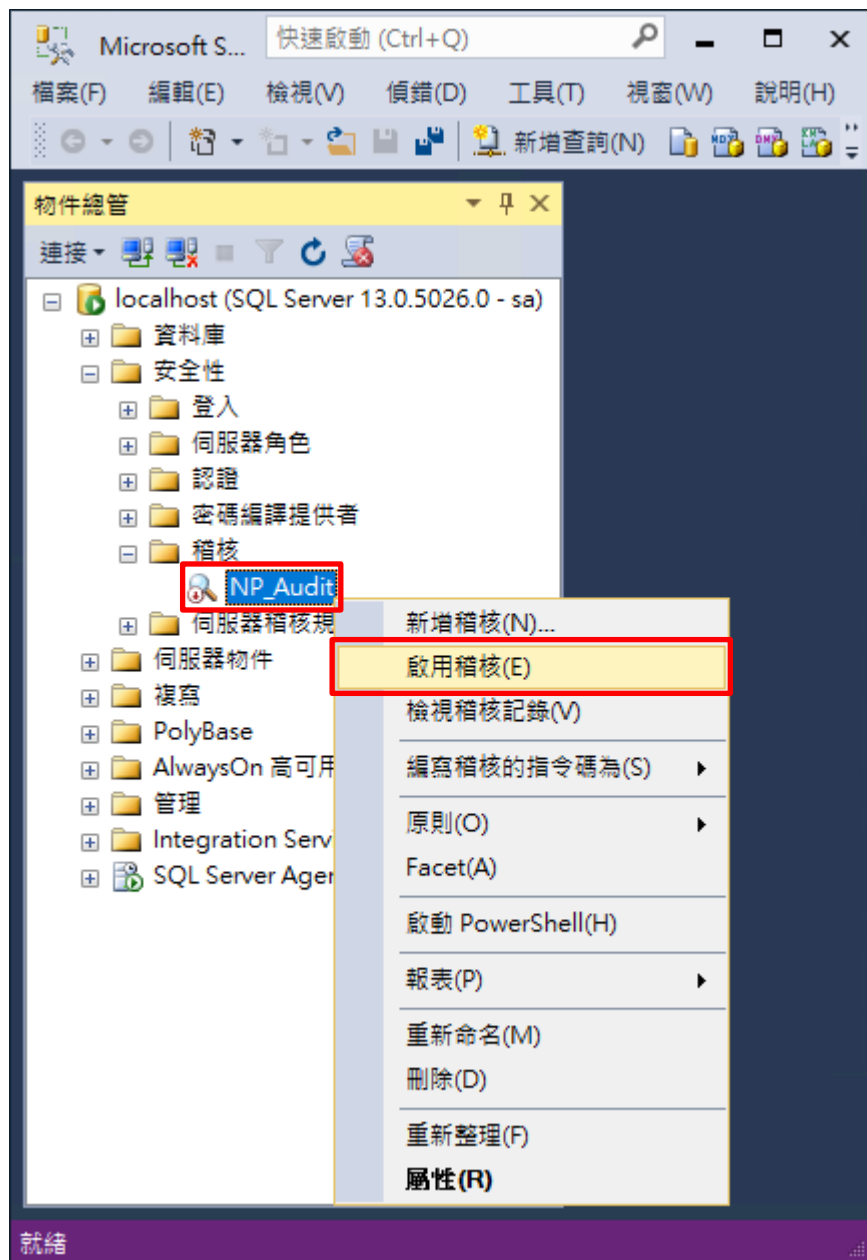
[檢視連接屬性](#)

Progress

Ready

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]



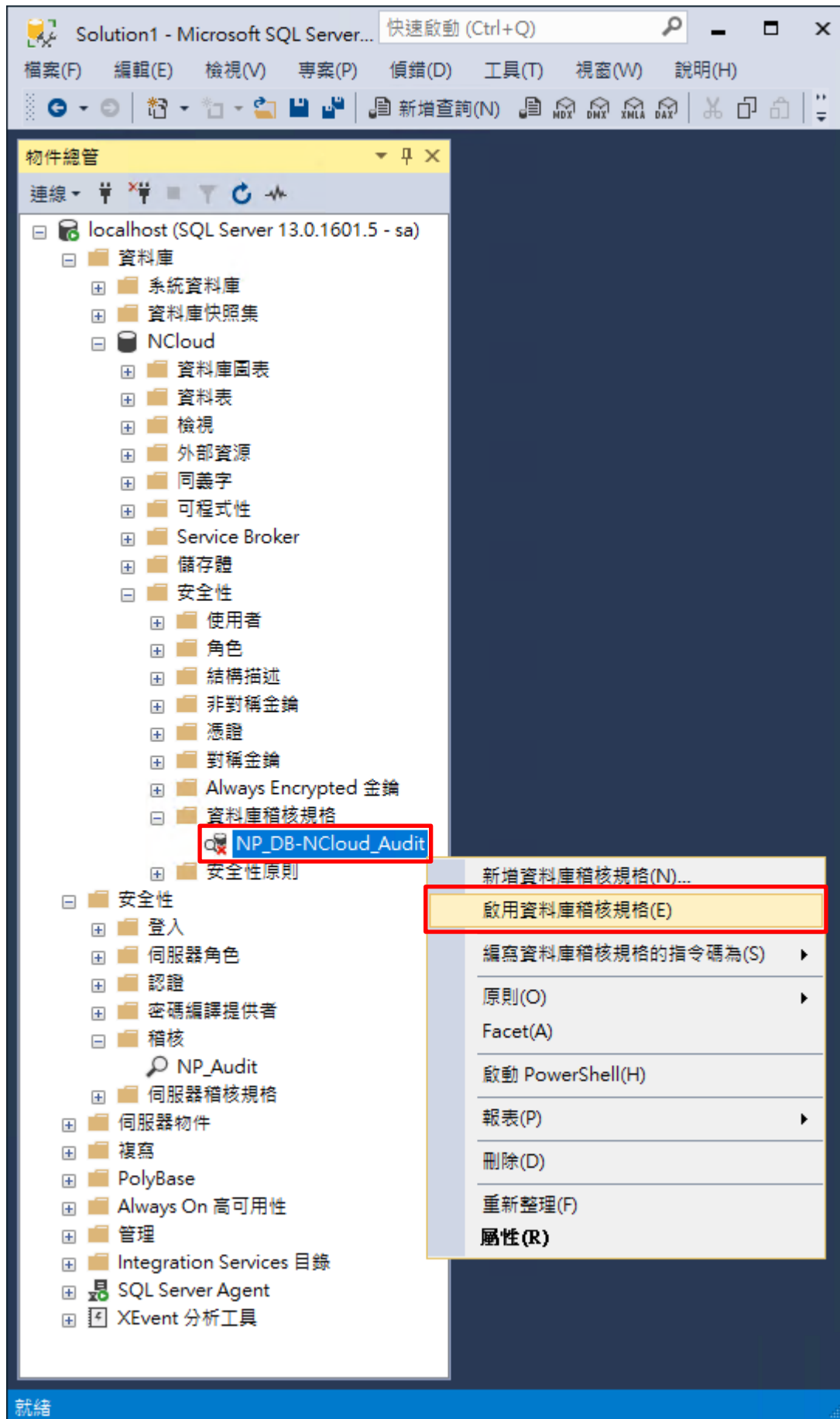
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



(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

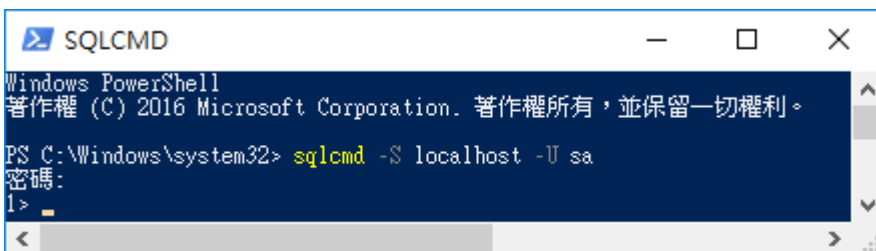
(1) 開啟 [Windows PowerShell]



(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
```

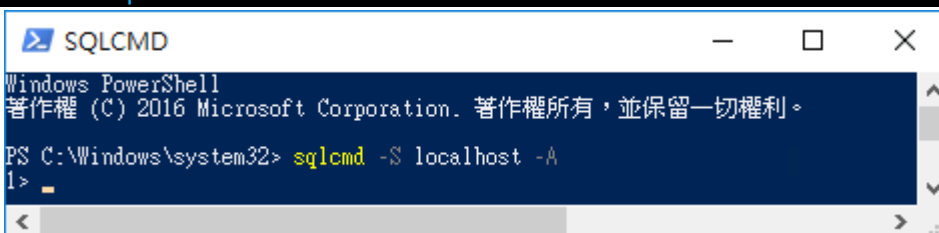


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

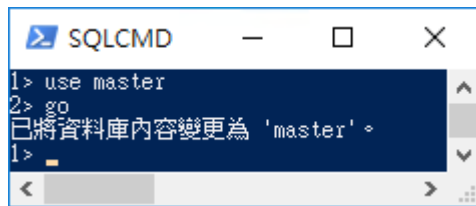
<2.2> 使用 Windows 帳號

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



(3) 切換資料庫

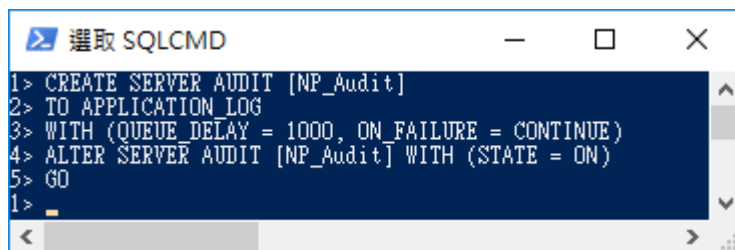
```
1 > use master  
2 > go
```



```
SQLCMD  
1> use master  
2> go  
已將資料庫內容變更為 '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
```

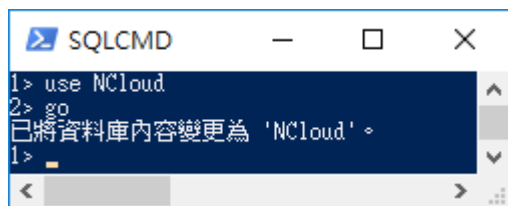


```
選取 SQLCMD  
1> CREATE SERVER AUDIT [NP_Audit]  
2> TO APPLICATION_LOG  
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)  
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)  
5> GO  
1>
```

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
```



```
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 terminal displays the same SQL commands as the previous block, with the prompt "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 (SELECT ON DATABASE::[NCloud] BY [public])
```

4.3 事件記錄檔設定

此為選項設定。

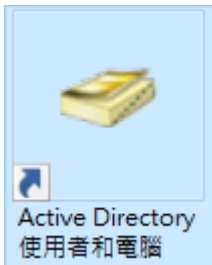
以下分別為網域和工作群組設定方式。

4.3.1 網域

4.3.1.1 組織單位設定

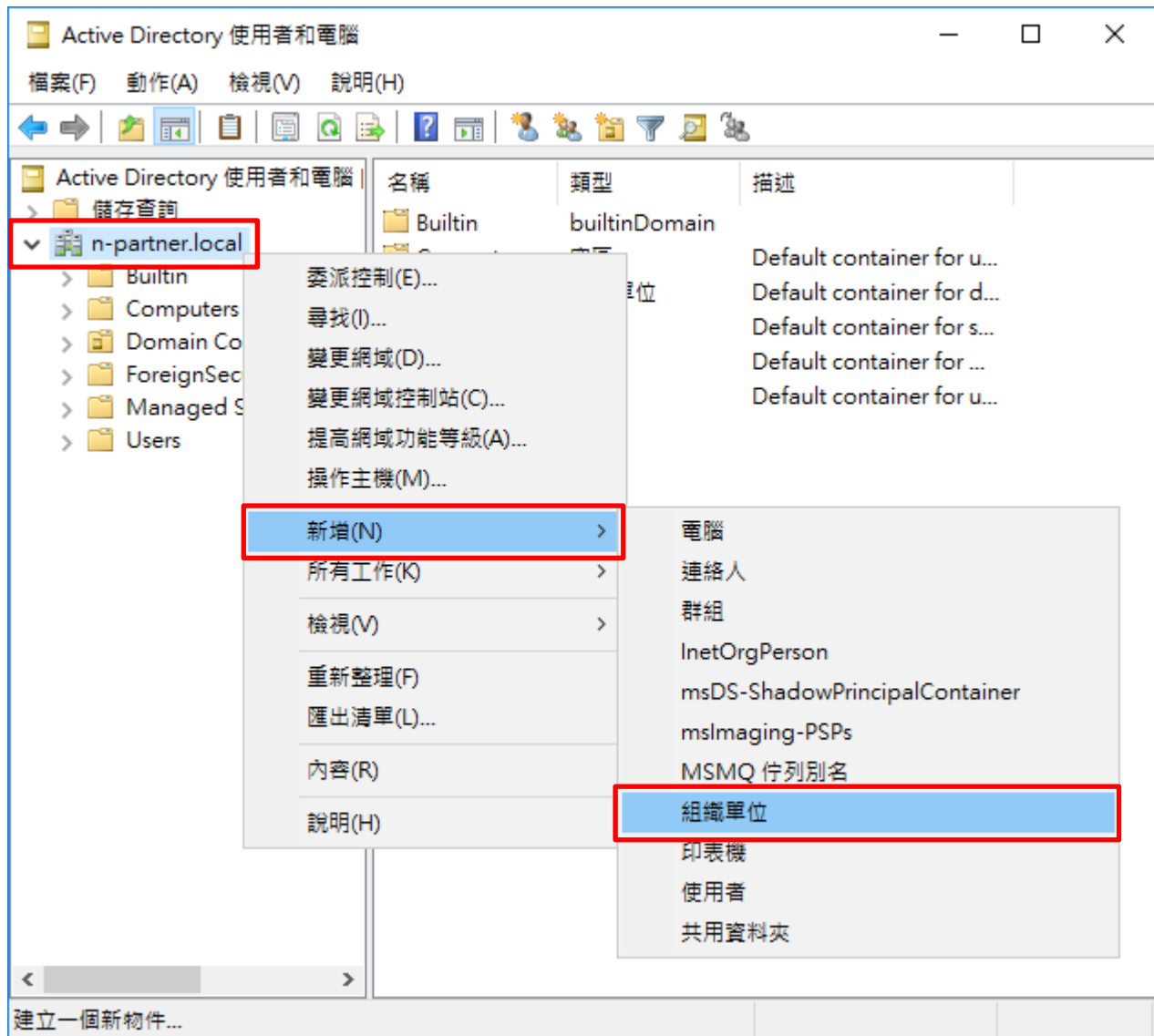
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



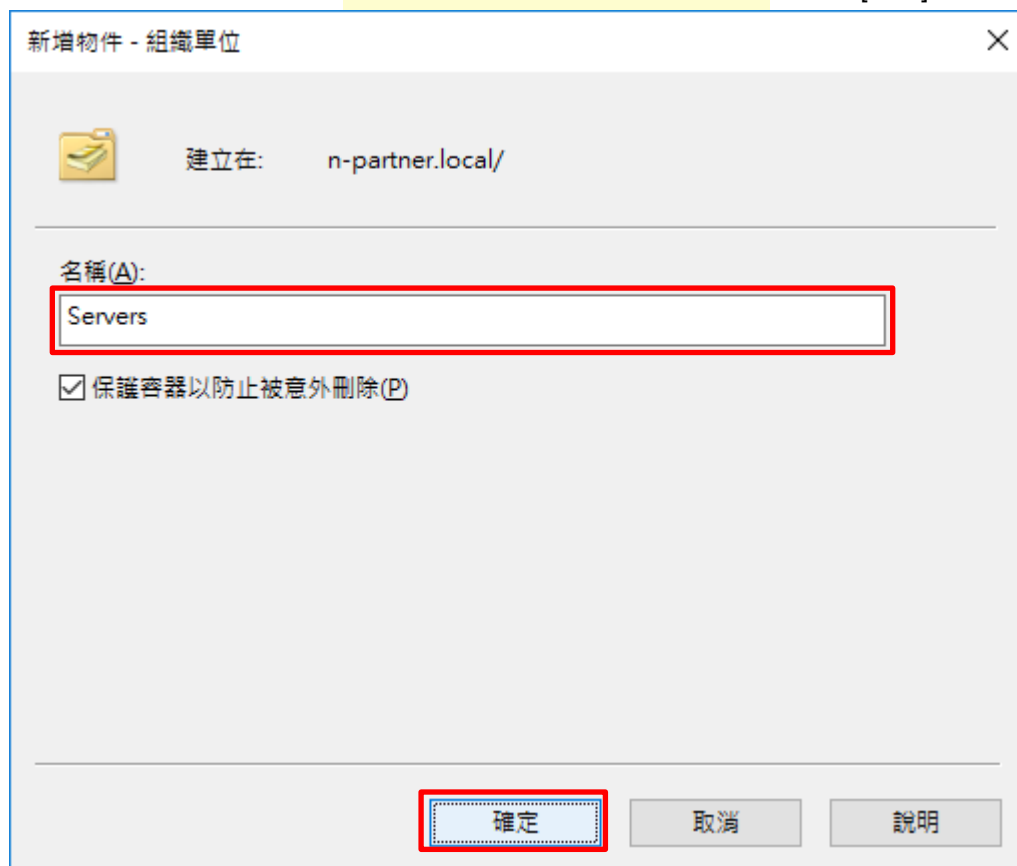
(2) 新增組織單位

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]



新增物件 - 組織單位

建立在: n-partner.local/

名稱(A):
Servers

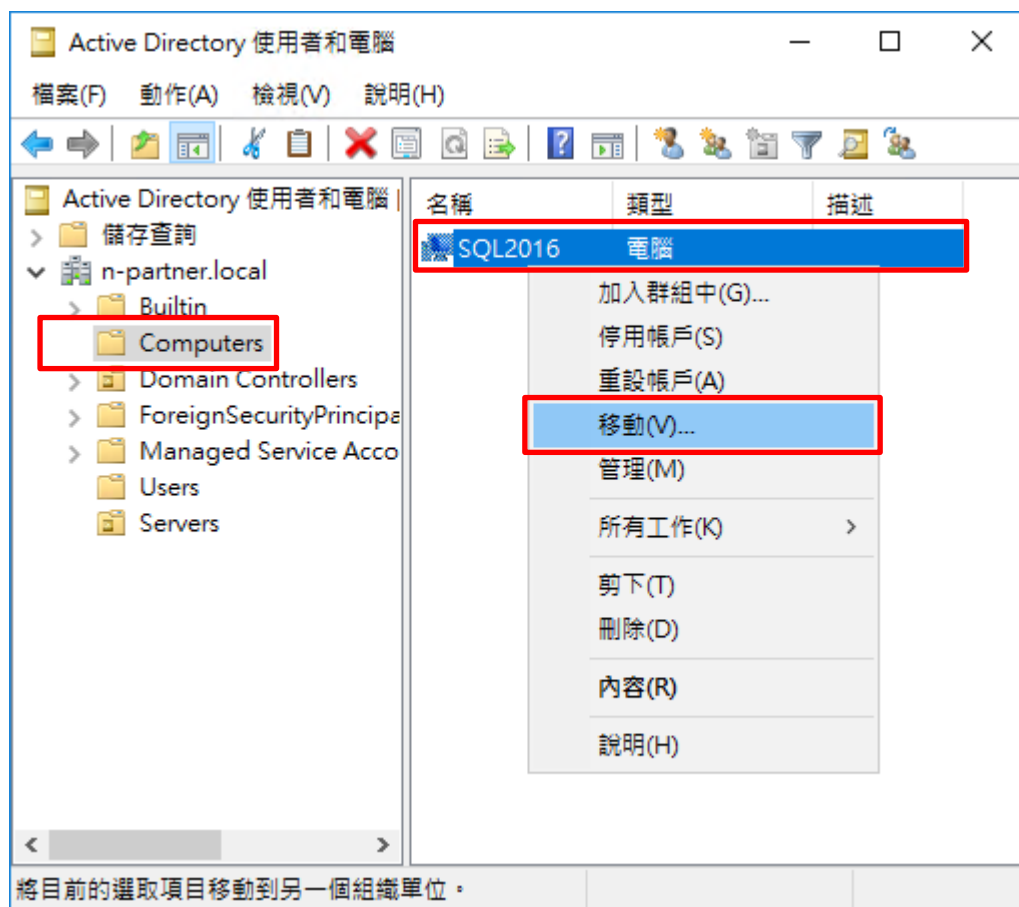
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

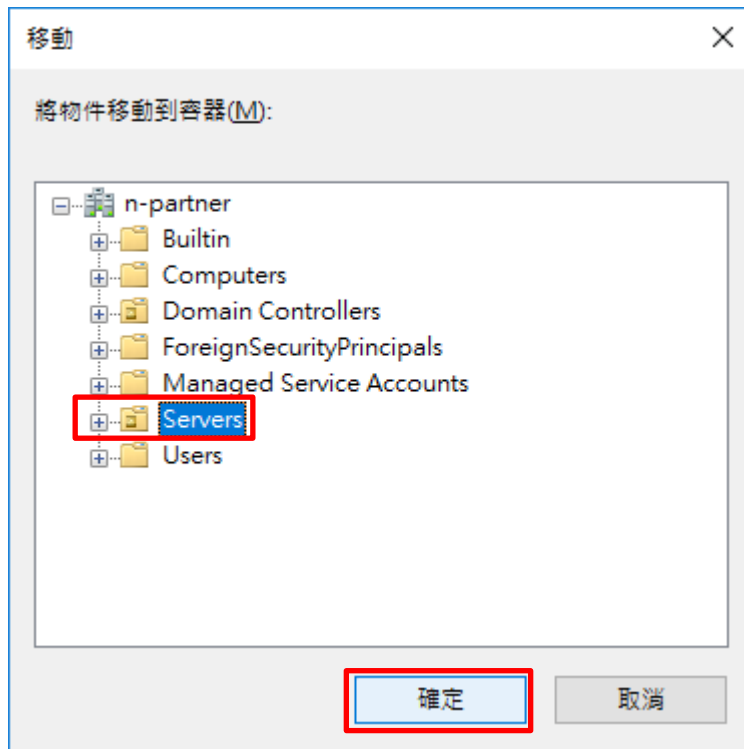
選擇 [Computers] 組織單位 -> 在 [SQL2016] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 MS SQL Server 主機

-> 點選 [移動]



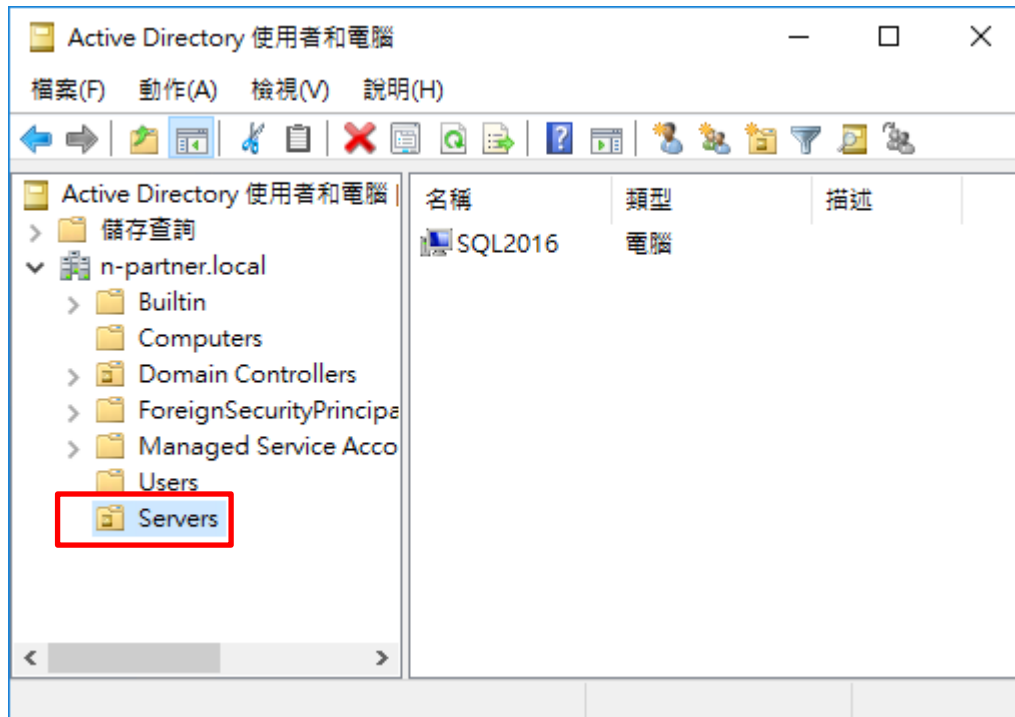
(5) 選擇組織單位

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

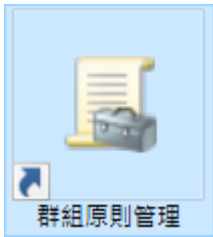
點選 [Servers] 組織單位，確認 SQL2016 伺服器已移動。



4.3.1.2 群組原則設定

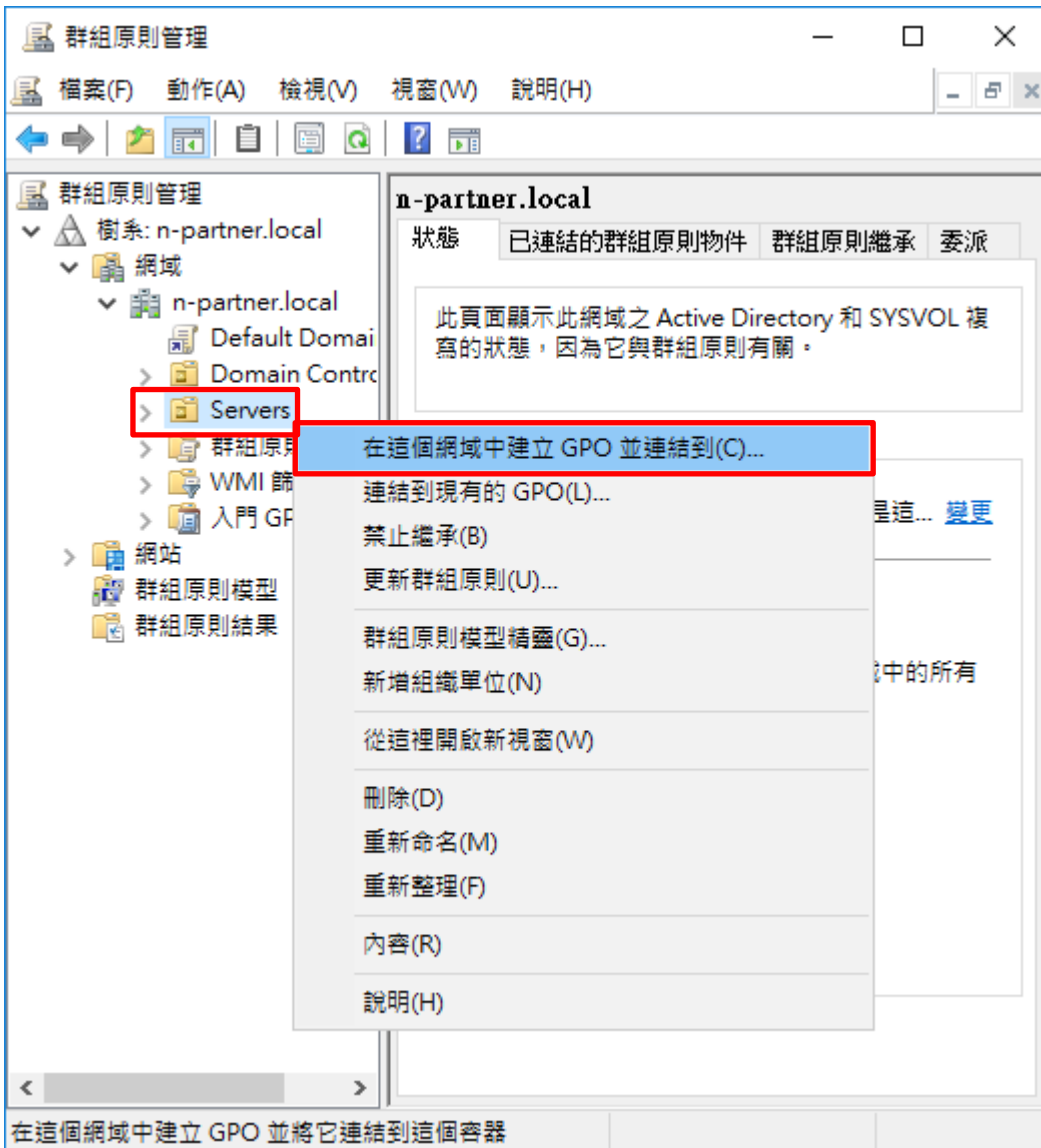
(1) 開啟群組原則管理

開啟 [群組原則管理]



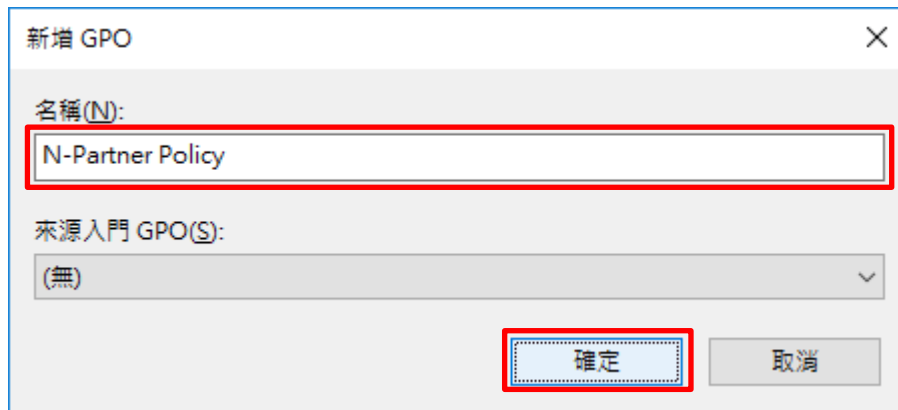
(2) 在 Servers 組織單位，新增群組原則物件

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



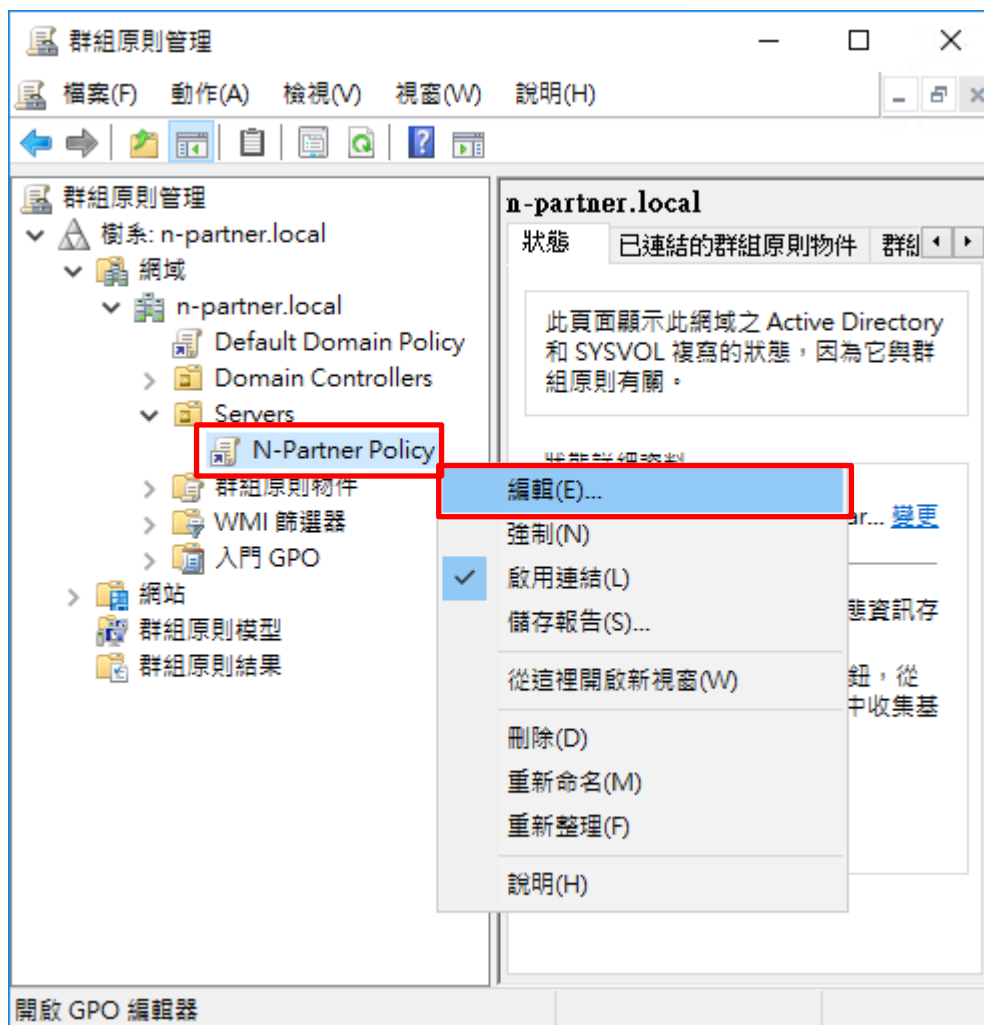
(3) 輸入群組原則物件名稱

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



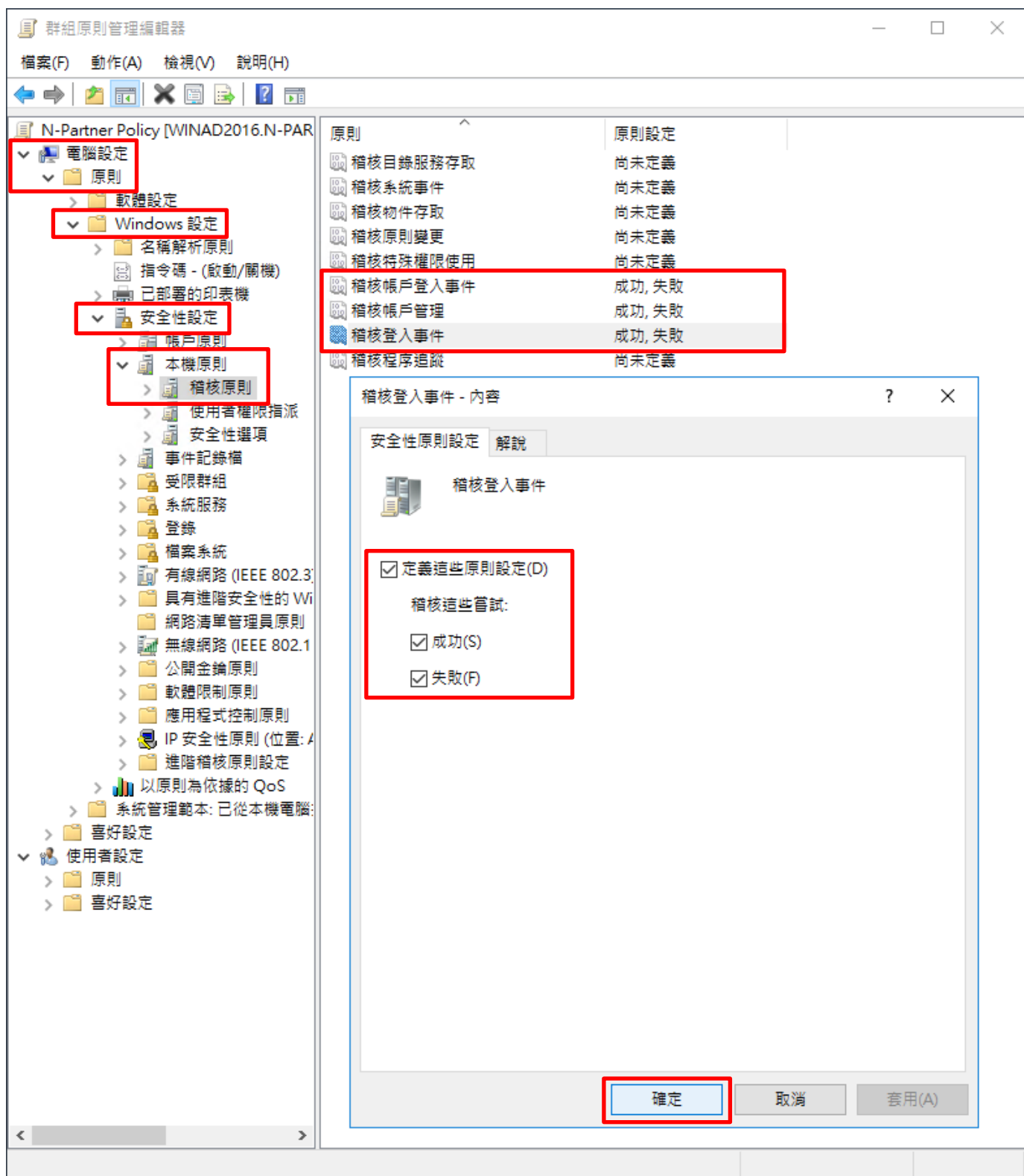
(4) 編輯群組原則物件

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



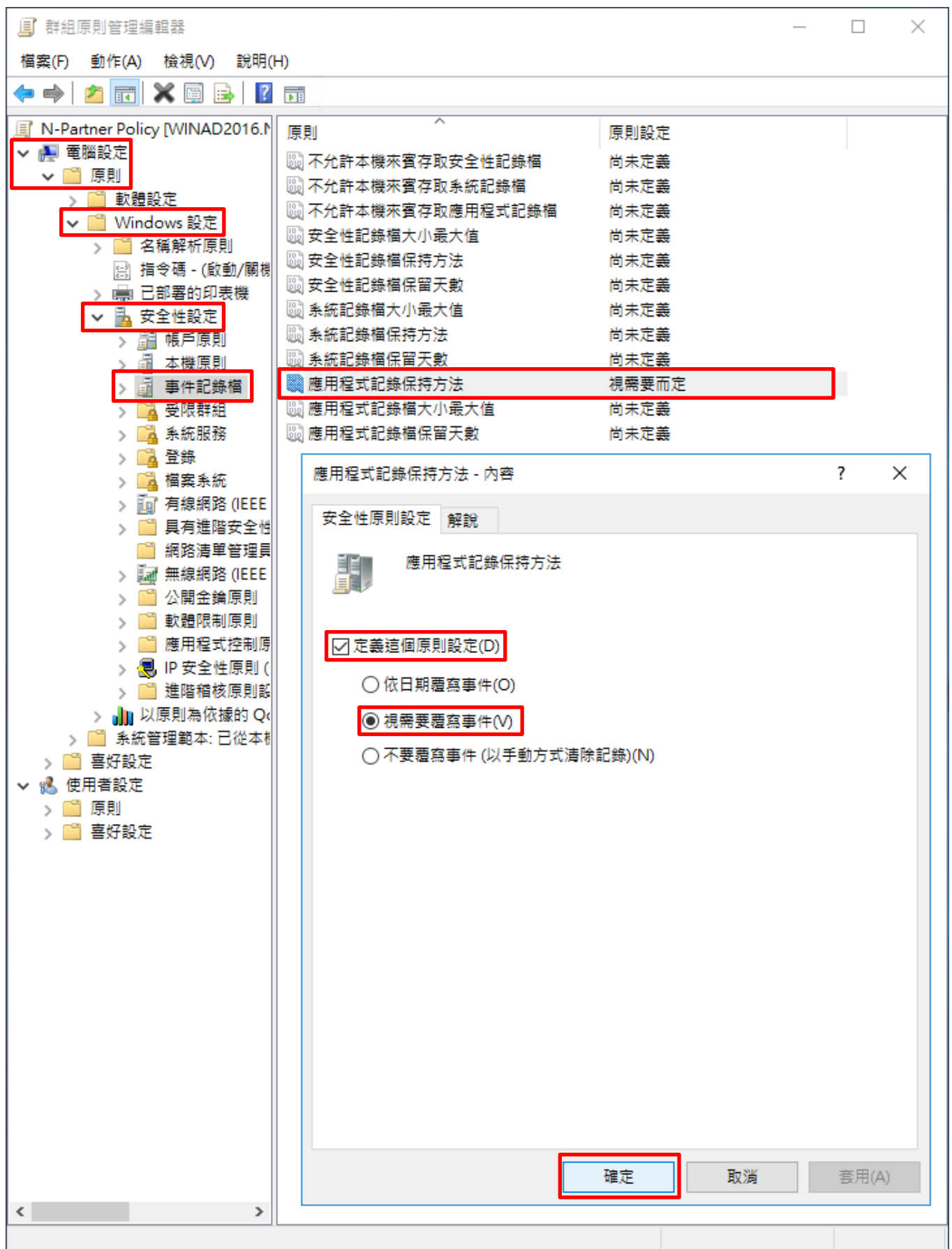
(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [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) 事件記錄檔：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) 事件記錄檔：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] -> 勾選 [定義這個原則設定] -> 輸入 204800 KB 註：請依客戶環境調整 -> 按 [確定]

The screenshot shows the Group Policy Editor window titled '群組原則管理編輯器'. The left-hand navigation pane is expanded to show the path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The '應用程式記錄檔大小最大值' (Application Log Size Maximum) policy is selected and highlighted in red. The right-hand pane shows a list of policies with their current settings. The selected policy is set to '204800 KB'. A dialog box titled '應用程式記錄檔大小最大值 - 內容' (Application Log Size Maximum - Content) is open, showing the '安全性原則設定' (Security Policy Settings) tab. In this dialog, the checkbox '定義這個原則設定(D)' (Define this policy setting) is checked, and the value '204800 KB' is entered in the text box. The '確定' (OK) button is highlighted in red at the bottom of the dialog.

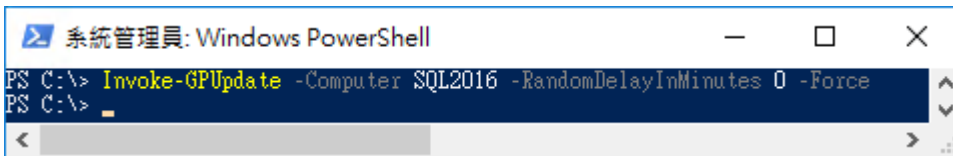
原則	原則設定
不允許本機來賓存取安全性記錄檔	尚未定義
不允許本機來賓存取系統記錄檔	尚未定義
不允許本機來賓存取應用程式記錄檔	尚未定義
安全性記錄檔大小最大值	尚未定義
安全性記錄檔保持方法	尚未定義
安全性記錄檔保留天數	尚未定義
系統記錄檔大小最大值	尚未定義
系統記錄檔保持方法	尚未定義
系統記錄檔保留天數	尚未定義
應用程式記錄保持方法	視需要而定
應用程式記錄檔大小最大值	204800 KB
應用程式記錄檔保留天數	尚未定義

(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-GPUdate -Computer SQL2016 -RandomDelayInMinutes 0 -Force
```

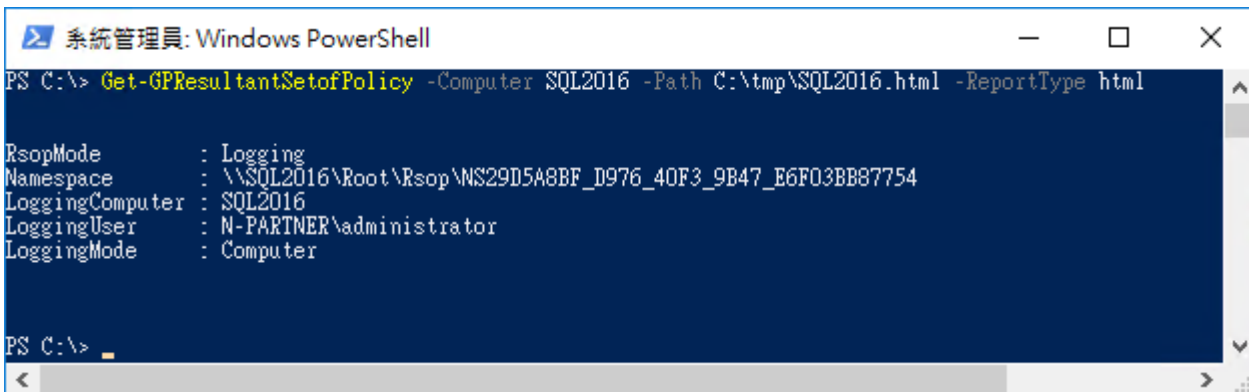
A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Invoke-GPUdate -Computer SQL2016 -RandomDelayInMinutes 0 -Force` being entered and executed. The output is a single underscore character `_`.

```
系統管理員: Windows PowerShell
PS C:\> Invoke-GPUdate -Computer SQL2016 -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 SQL2016 -Path C:\tmp\SQL2016.html -ReportType html
```

A screenshot of a Windows PowerShell terminal window titled "系統管理員: Windows PowerShell". The terminal shows the command `Get-GPResultantSetofPolicy -Computer SQL2016 -Path C:\tmp\SQL2016.html -ReportType html` being entered and executed. The output displays several properties: `RsopMode : Logging`, `Namespace : \\SQL2016\Root\Rsop\NS29D5A8BF_D976_40F3_9B47_E6F03BB87754`, `LoggingComputer : SQL2016`, `LoggingUser : N-PARTNER\administrator`, and `LoggingMode : Computer`.

```
系統管理員: Windows PowerShell
PS C:\> Get-GPResultantSetofPolicy -Computer SQL2016 -Path C:\tmp\SQL2016.html -ReportType html

RsopMode       : Logging
Namespace      : \\SQL2016\Root\Rsop\NS29D5A8BF_D976_40F3_9B47_E6F03BB87754
LoggingComputer : SQL2016
LoggingUser    : N-PARTNER\administrator
LoggingMode    : Computer

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

Browser address bar: C:\tmp\SQL2016.html N-PARTNER\SQL2016

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	
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	
系統管理範本	顯示	
群組原則物件	顯示	
WMI 篩選器	顯示	
使用者詳細資料	顯示	

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]

The screenshot shows the 'Local Group Policy Editor' window. The left pane shows the navigation tree with 'Computer Configuration' > 'Windows Settings' > 'Security Settings' > 'Local Policies' > 'Audit Policies' expanded. The right pane shows a list of audit policies. The 'Audit Logon Events' policy is selected and highlighted. A dialog box titled 'Audit Logon Events - Content' is open, showing the configuration for auditing logon events. The 'Audit these attempts' section has 'Success (S)' and 'Failure (F)' checked. A warning icon and text at the bottom of the dialog state: 'If other policies are set to override this audit policy, this policy may not be enforced. For more information, see Audit Logon Events (Q921468)'. The 'OK' button is highlighted.

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

稽核登入事件 - 內容

本機安全性設定 解說

稽核登入事件

稽核這些嘗試:

- 成功(S)
- 失敗(F)

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

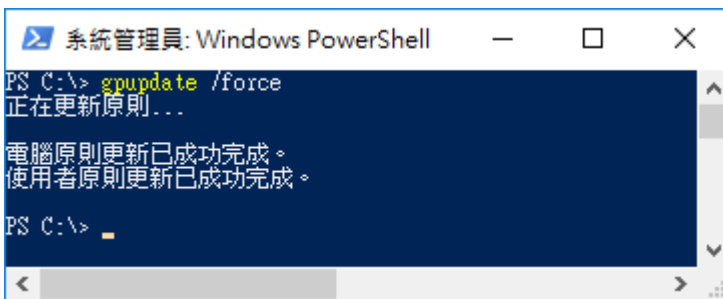
確定 取消 套用(A)

(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The terminal content shows the command "PS C:\> gpupdate /force" being entered. The output is "正在更新原則..." followed by two lines of status messages: "電腦原則更新已成功完成。" and "使用者原則更新已成功完成。". The prompt "PS C:\> " is visible at the bottom of the terminal.

```
系統管理員: Windows PowerShell
PS C:\> gpupdate /force
正在更新原則...
電腦原則更新已成功完成。
使用者原則更新已成功完成。
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:*
系統稽核原則
類別/子類別          設定
系統
安全性系統延伸      沒有稽核
系統完整性          成功與失敗
IPSEC driver        沒有稽核
其他系統事件        成功與失敗
安全性狀態變更      成功
登入/登出
登入                成功與失敗
登出                成功與失敗
帳戶鎖定            成功與失敗
IPsec 主要模式      成功與失敗
IPsec 快速模式      成功與失敗
IPsec 延伸模式      成功與失敗
特殊登入            成功與失敗
其他登入/登出事件  成功與失敗
網路原則伺服器      成功與失敗
使用者/裝置宣告     成功與失敗
群組成員資格        成功與失敗
物件存取
檔案系統            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
抽取式存放裝置      沒有稽核
集中原則暫存        沒有稽核
特殊權限使用
非機密特殊權限使用  沒有稽核
其他特殊權限使用事件  沒有稽核
機密特殊權限使用    沒有稽核
詳細追蹤
建立處理程序        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
隨插即用事件        沒有稽核
Token Right Adjusted Events 沒有稽核
原則變更
稽核原則變更        成功
驗證原則變更        成功
授權原則變更        沒有稽核
MPSSVC 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
電腦帳戶管理        成功與失敗
安全性群組管理      成功與失敗
發佈群組管理        成功與失敗
應用程式群組管理    成功與失敗
其他帳戶管理事件    成功與失敗
使用者帳戶管理      成功與失敗
DS 存取
目錄服務存取        成功
目錄服務變更        沒有稽核
目錄服務複寫        沒有稽核
詳細目錄服務複寫    沒有稽核
帳戶登入
Kerberos 服務票證操作 成功與失敗
其他帳戶登入事件    成功與失敗
Kerberos 驗證服務    成功與失敗
認證驗證            成功與失敗
PS C:\>
```

4.3.2.2 事件檔案設定

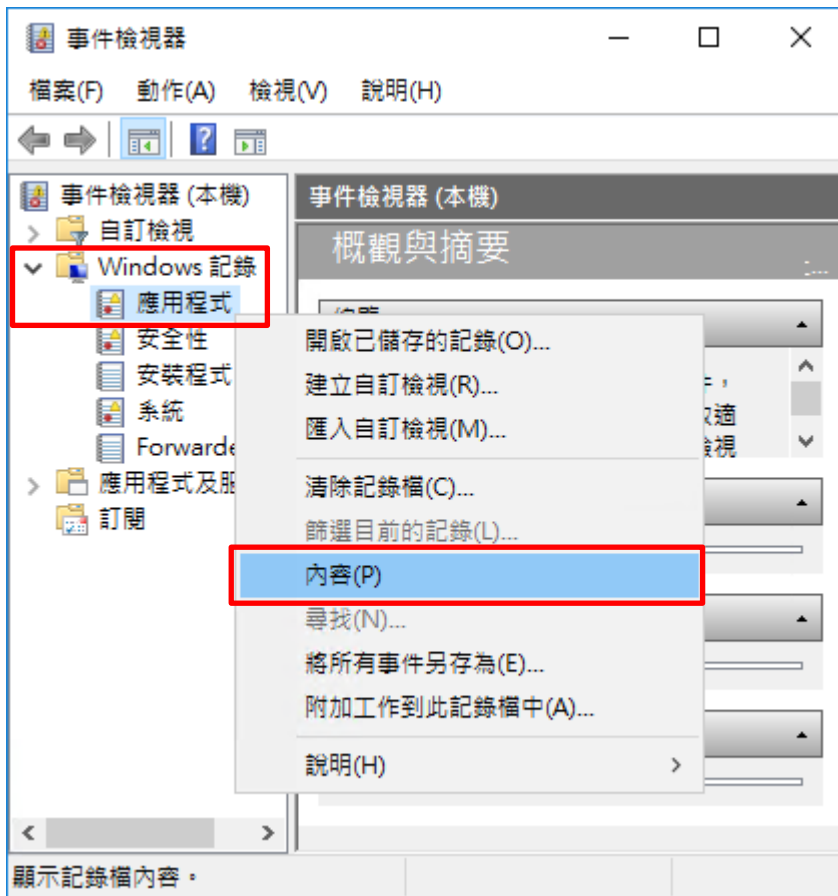
(1) 開啟 [檢視事件記錄檔]

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]



(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]

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9日 下午 11:31:09

修改日期: 2021年7月5日 下午 03:46:08

存取日期: 2021年6月9日 下午 11:31:09

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

清除記錄(R)

確定 取消 套用(P)

5. SQL 2019

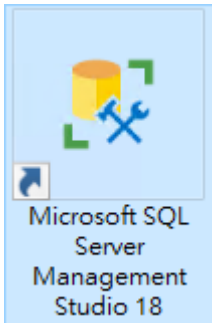
5.1 稽核登入

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

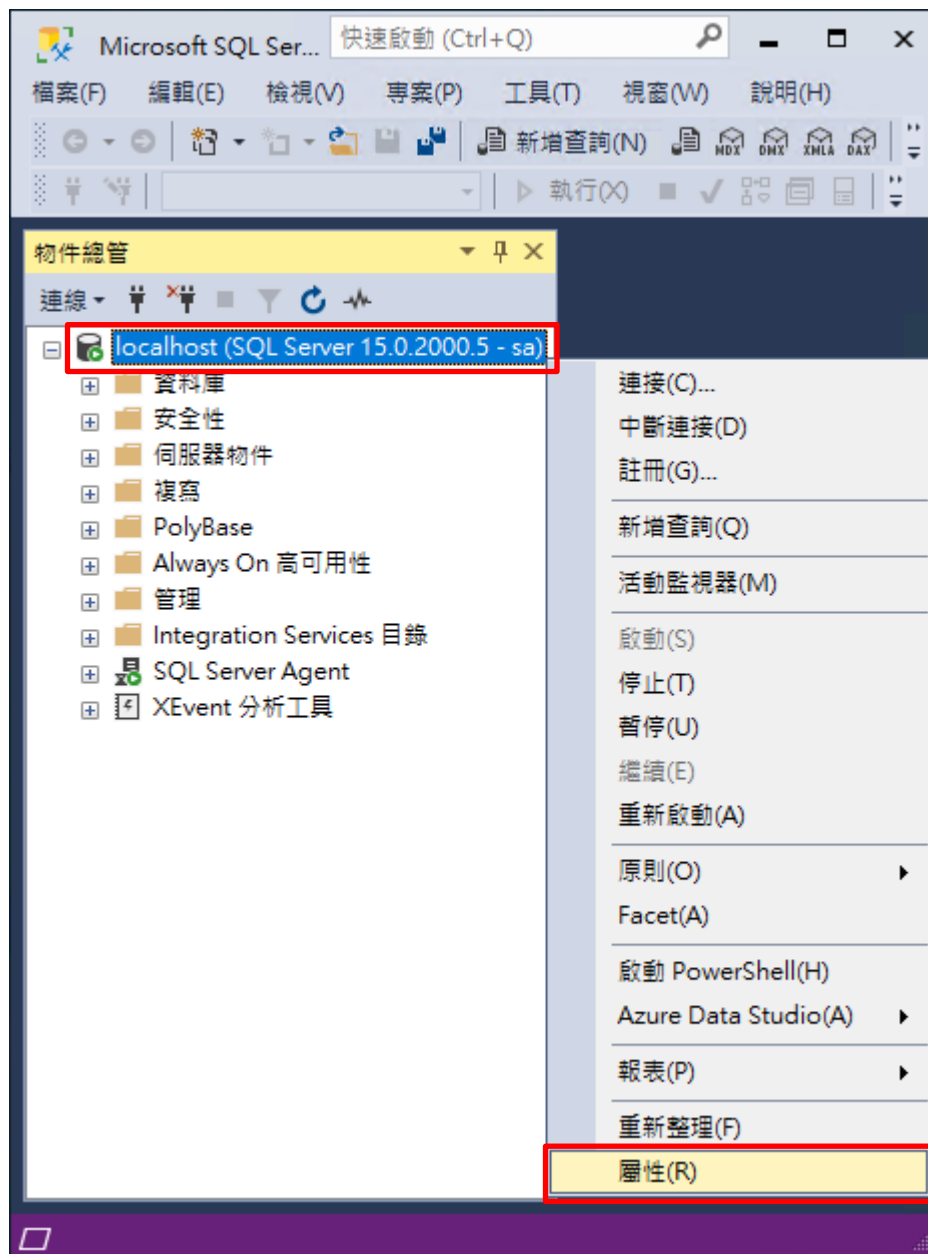
(1) 開啟 [Microsoft SQL Server Management Studio]



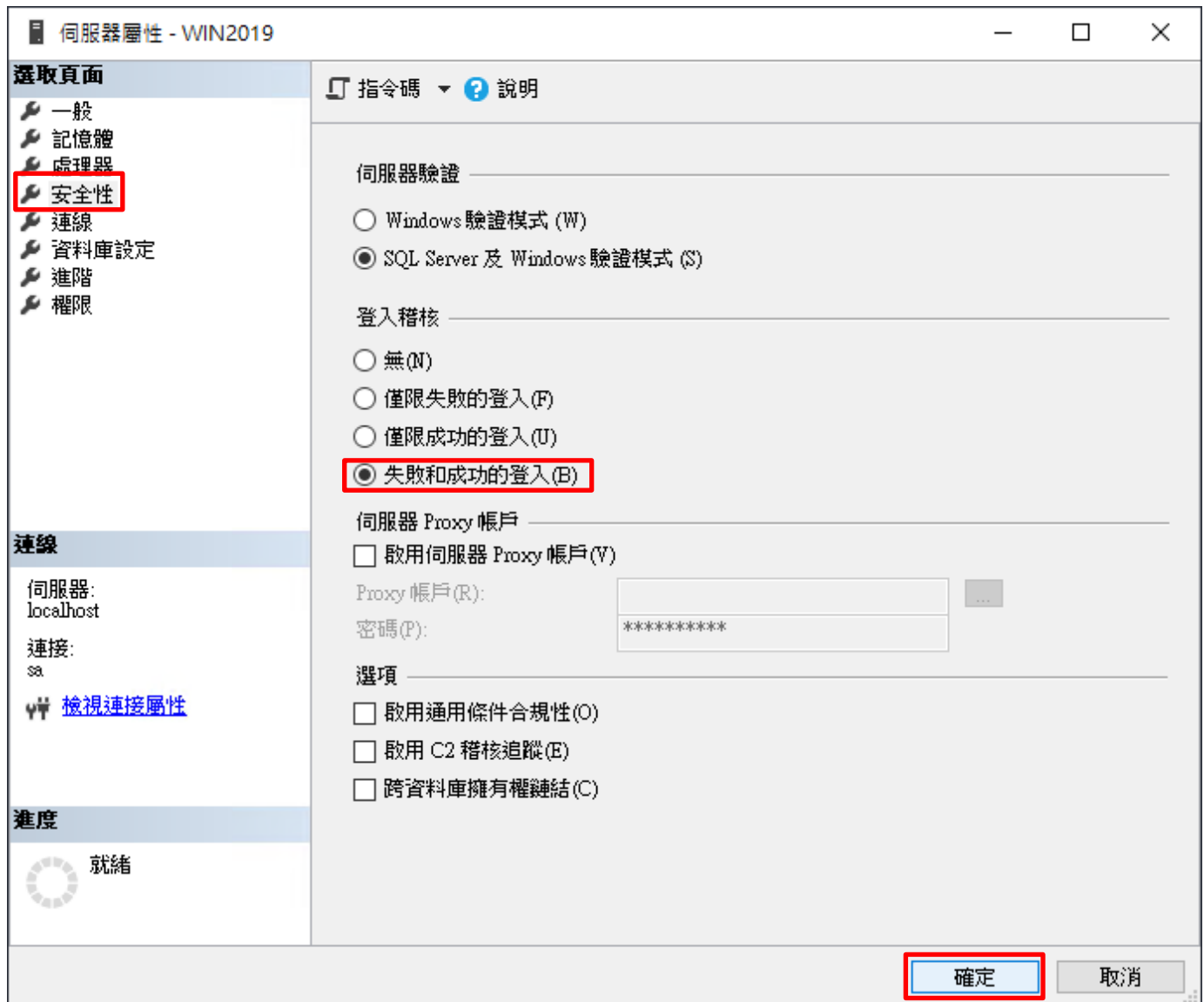
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

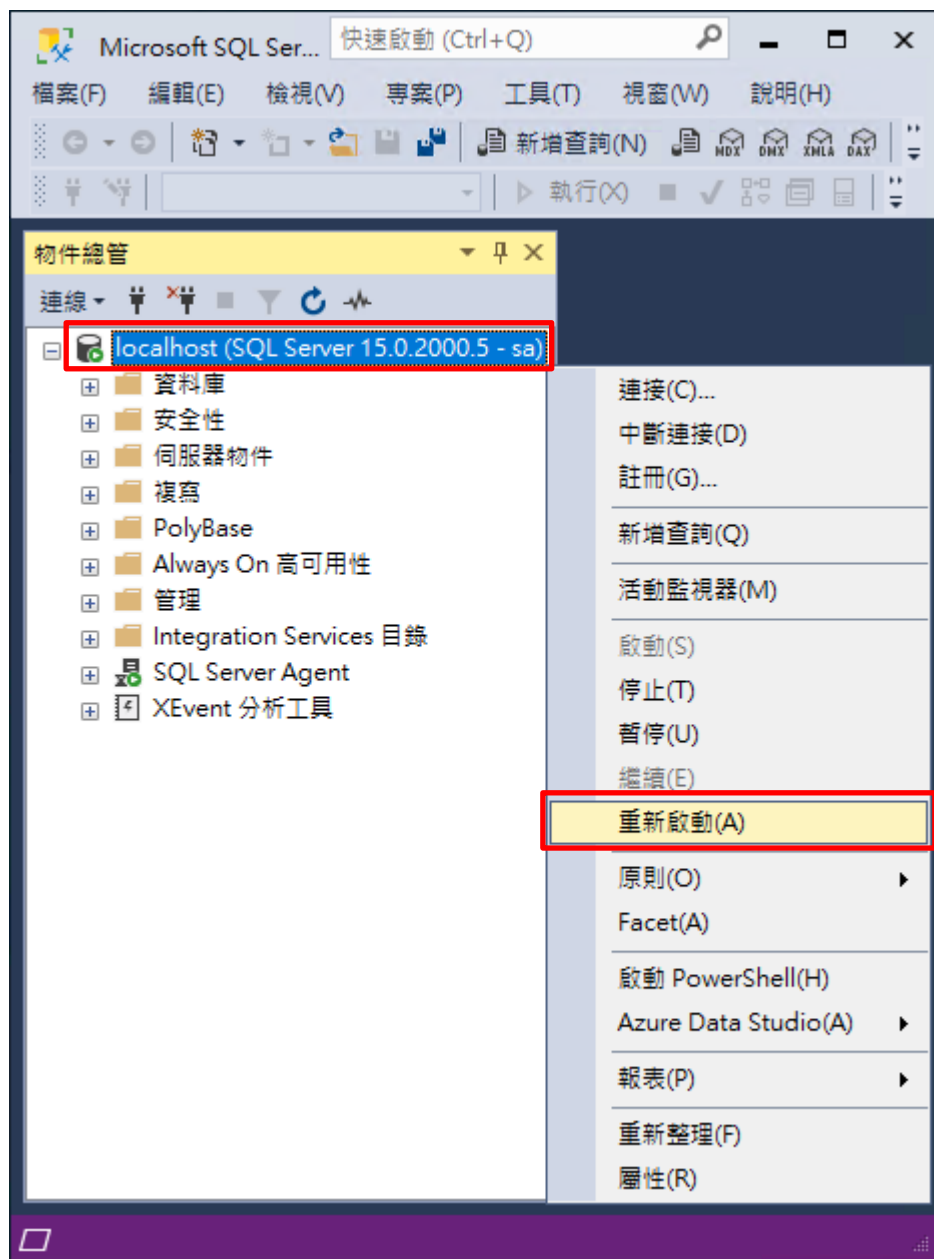


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

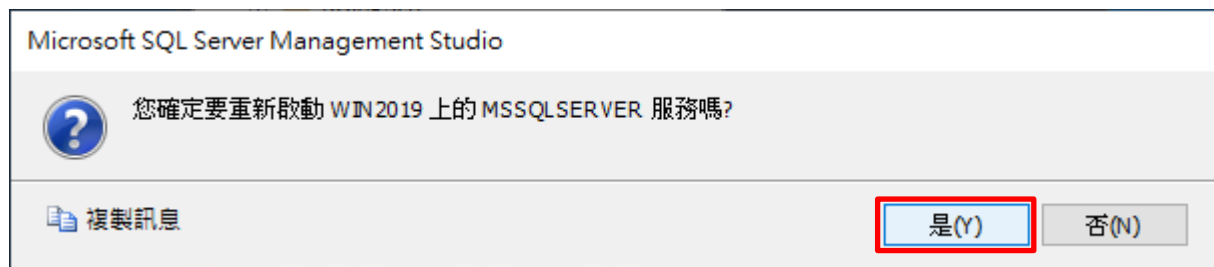


(5) 重新啟動 MS SQL SERVER 服務

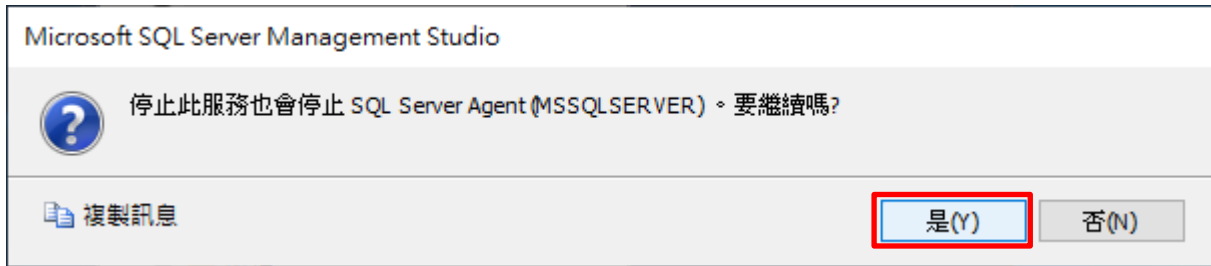
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MSSQLSERVER 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

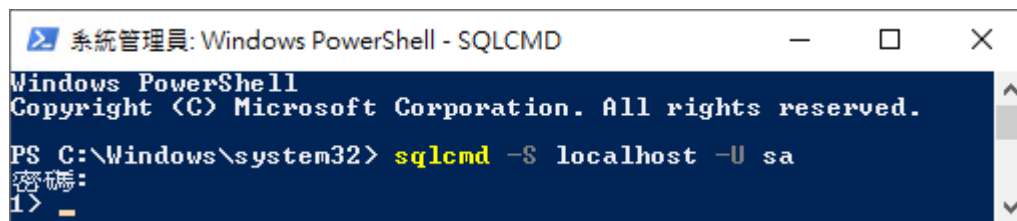
(1) 開啟 [Windows PowerShell]



(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
```

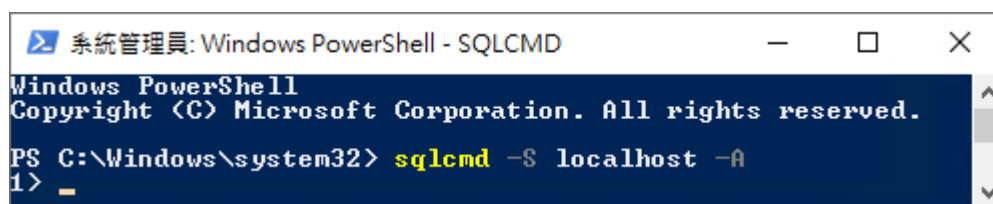


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

<2.2> 使用 Windows 帳號

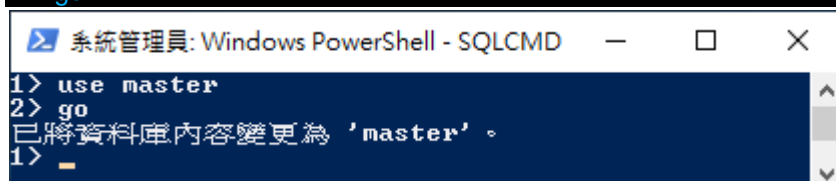
```
PS C:\> sqlcmd -S localhost -A
```



(3) 切換資料庫

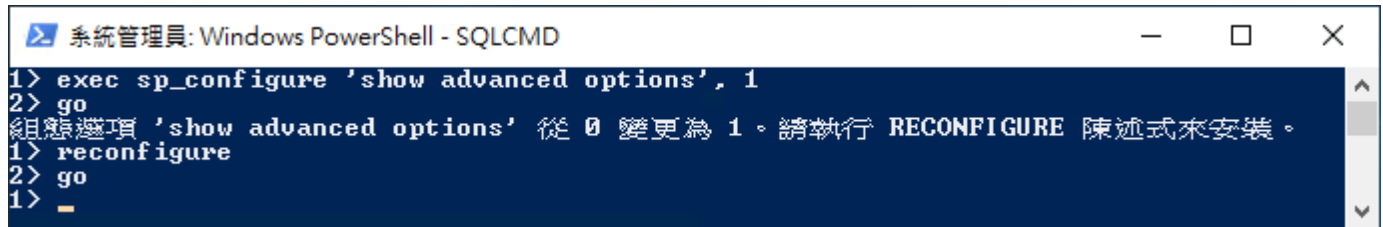
```
1 > use master
```

```
2 > go
```



(4) 使用 sp_configure 列出進階選項

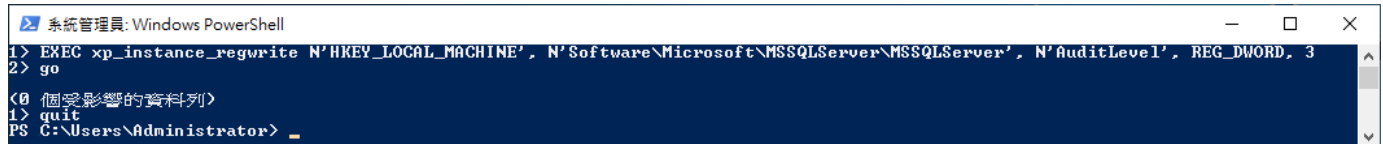
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
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

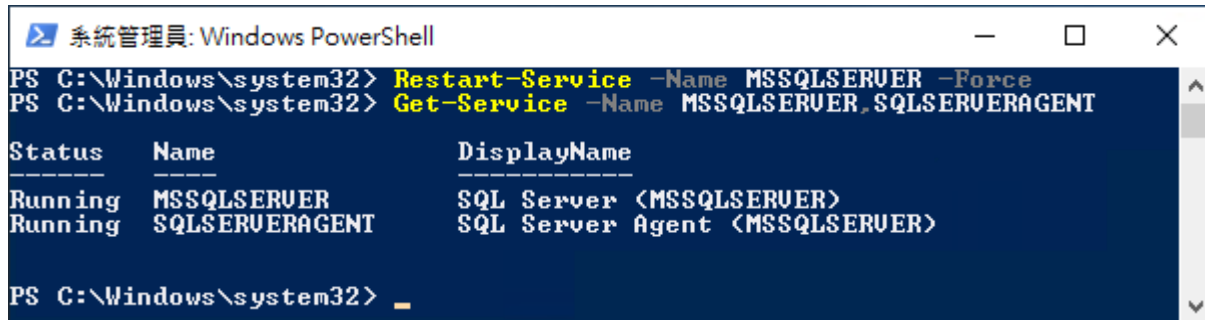
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',
N'AuditLevel', REG_DWORD, 3
2 > go
1 > quit
```



```
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

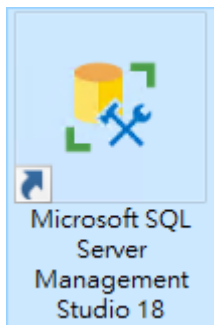
5.2.1 稽核伺服器層級

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

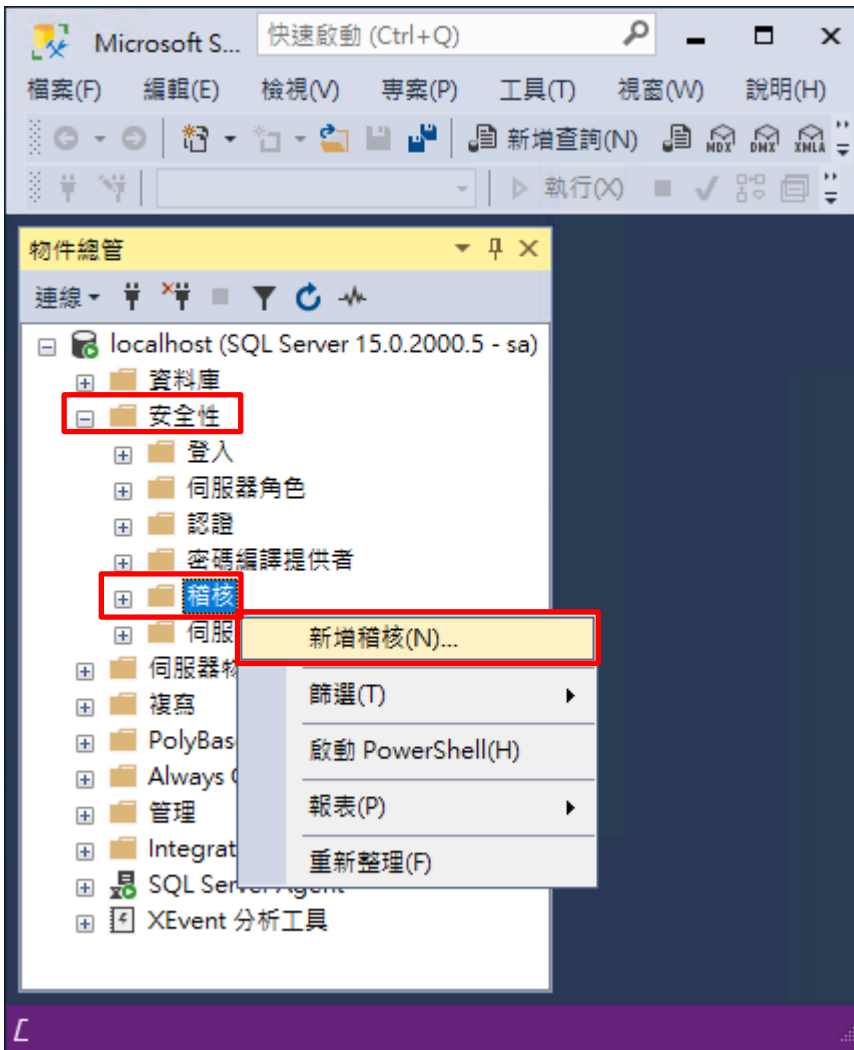
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

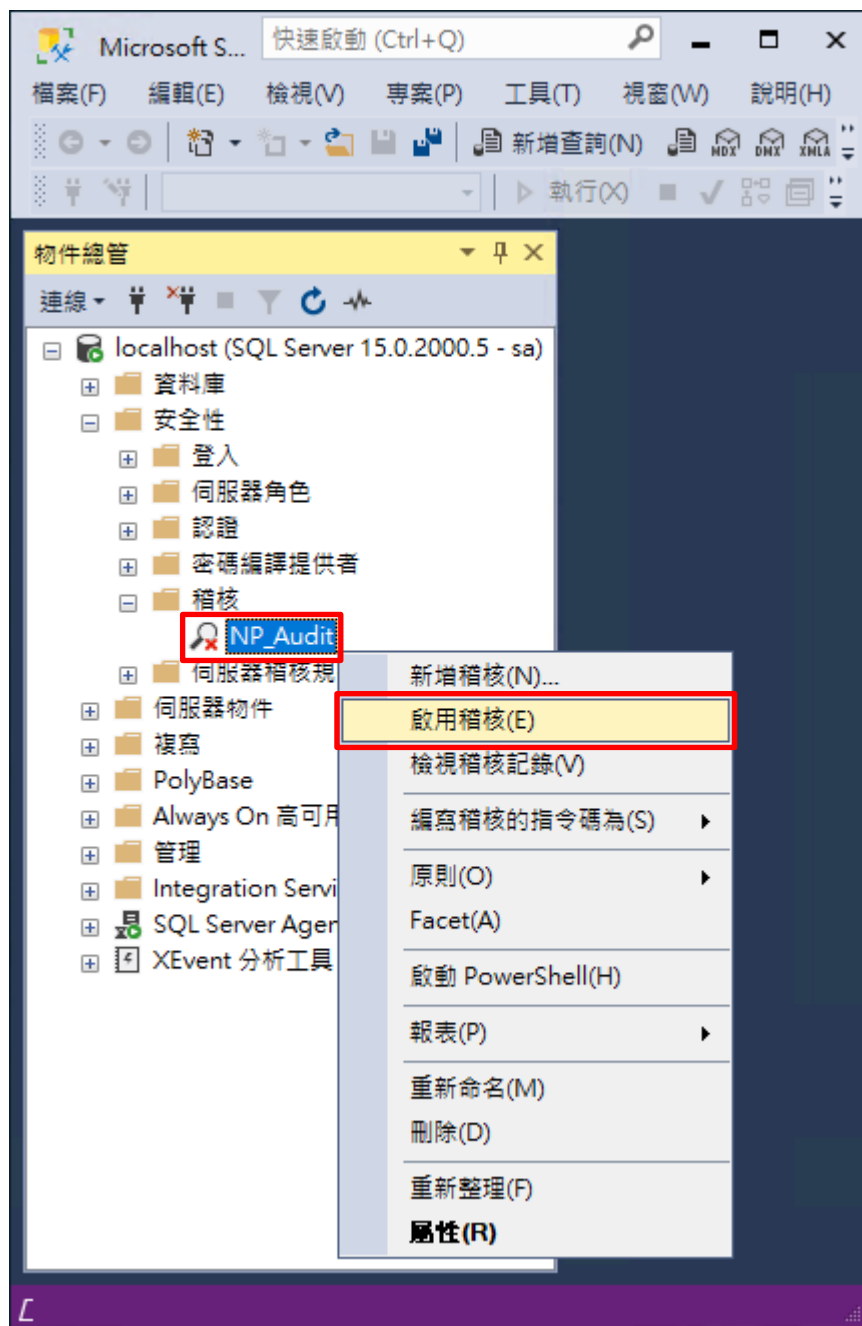


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

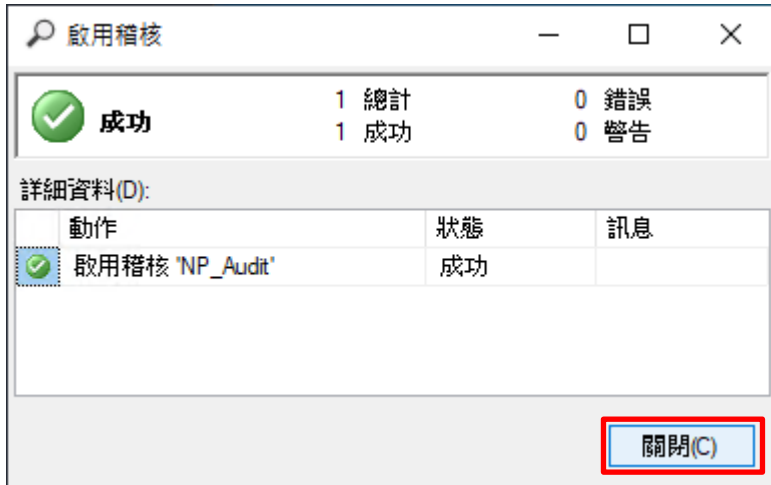


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔] 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

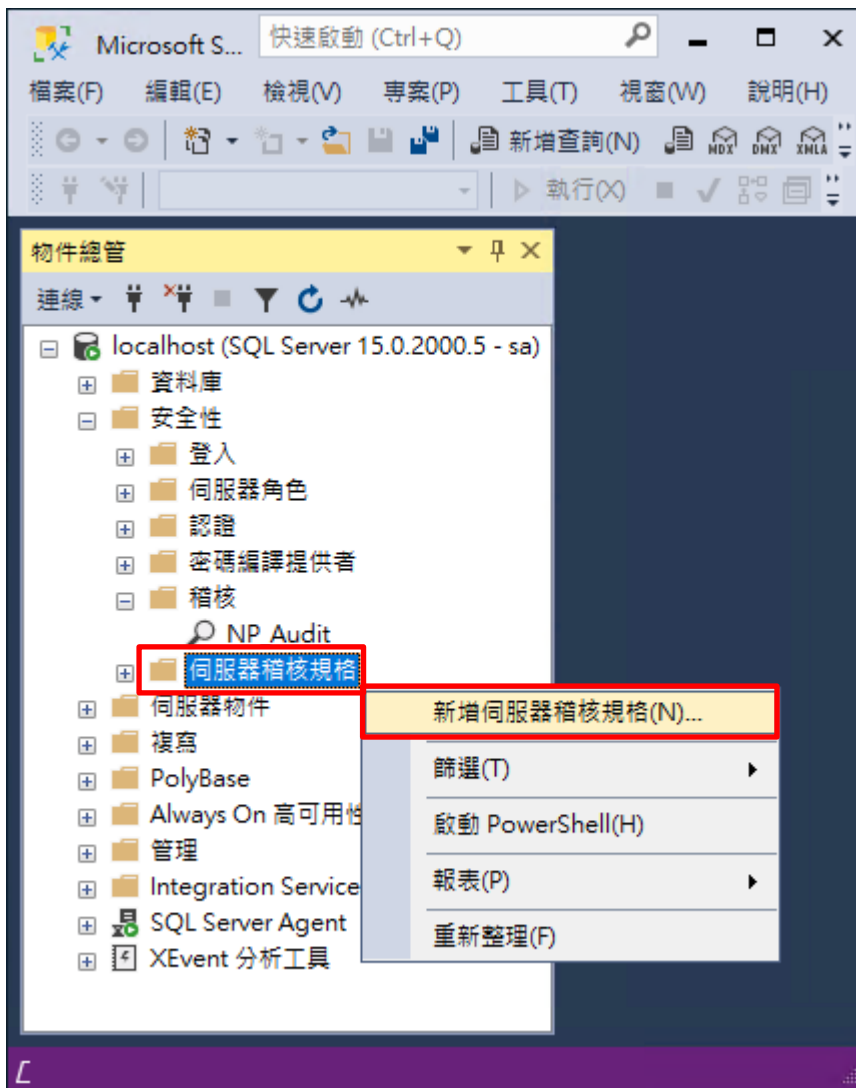
(5) 在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



(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]

建立伺服器稽核規格

就緒

選取頁面

一般

指令碼 說明

名稱(N): NP_Server_Audit

稽核(A): NP_Audit

動作:

	稽核動作類型	物件類別	物件結構描述	物件名稱	主體名稱
01	SUCCESSFUL_LOGIN_GROUP				
02	FAILED_LOGIN_GROUP				
03	LOGOUT_GROUP				
04	SERVER_STATE_CHANGE_GROUP				
05	SERVER_OPERATION_GROUP				
06	SCHEMA_OBJECT_CHANGE_GROUP				
07	DATABASE_OWNERSHIP_CHANGE_GROUP				
08	DATABASE_CHANGE_GROUP				
09	AUDIT_CHANGE_GROUP				
10	USER_CHANGE_PASSWORD_GROUP				
11	SCHEMA_OBJECT_CHANGE_GROUP				
12	DATABASE_OBJECT_CHANGE_GROUP				
▶▶13					

連線

SQL2019 [sa]

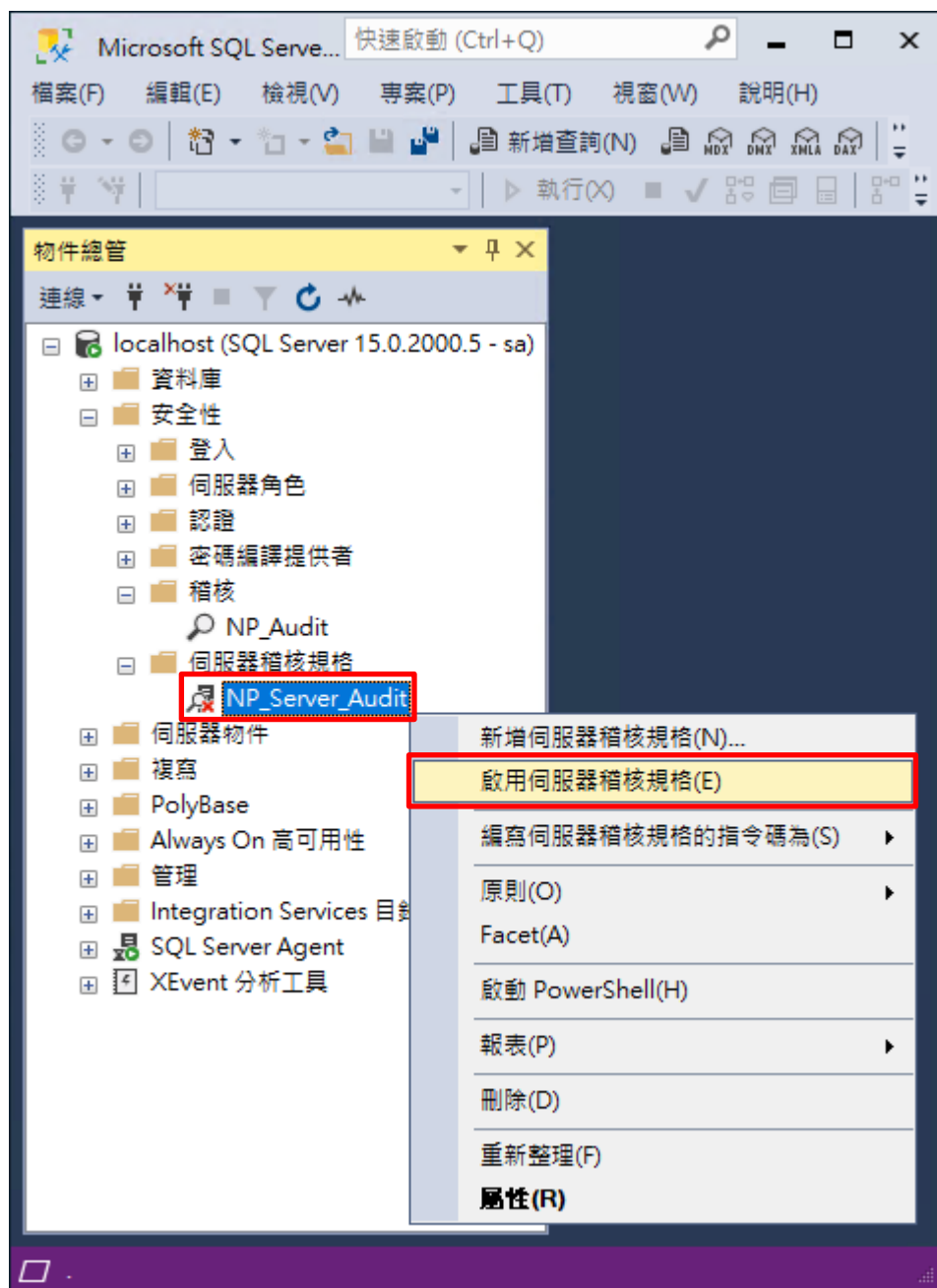
檢視連線屬性

進度

完成

確定 取消 說明

(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

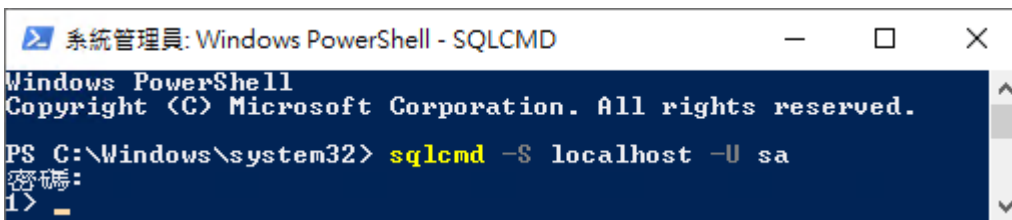
(1) 開啟 [Windows PowerShell]



(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
```

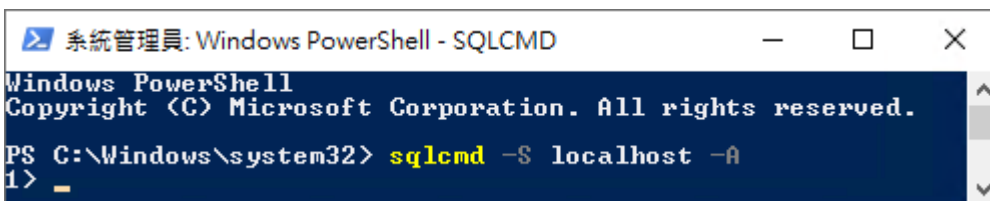


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

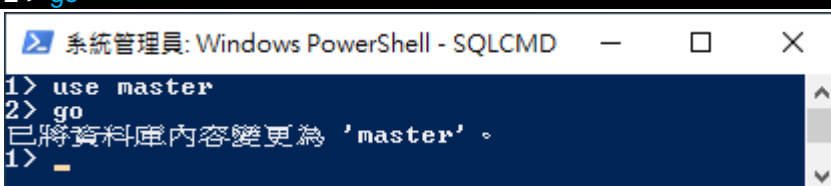
<2.2> 使用 Windows 帳號

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



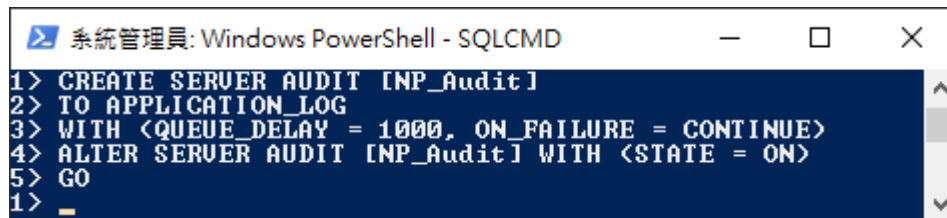
(3) 切換資料庫

```
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
```

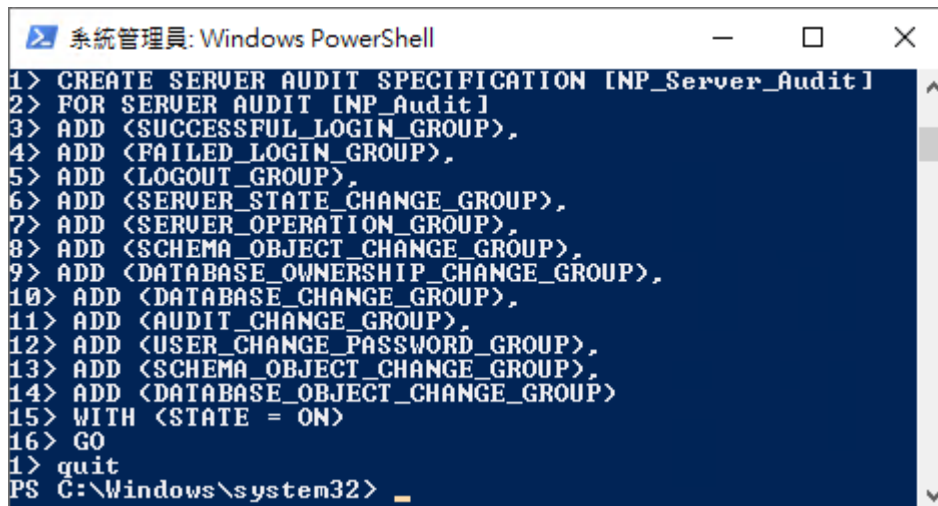


```
系統管理員: Windows PowerShell - SQLCMD
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

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

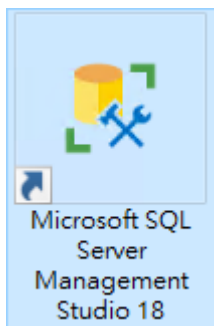
5.2.2 稽核資料庫層級

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

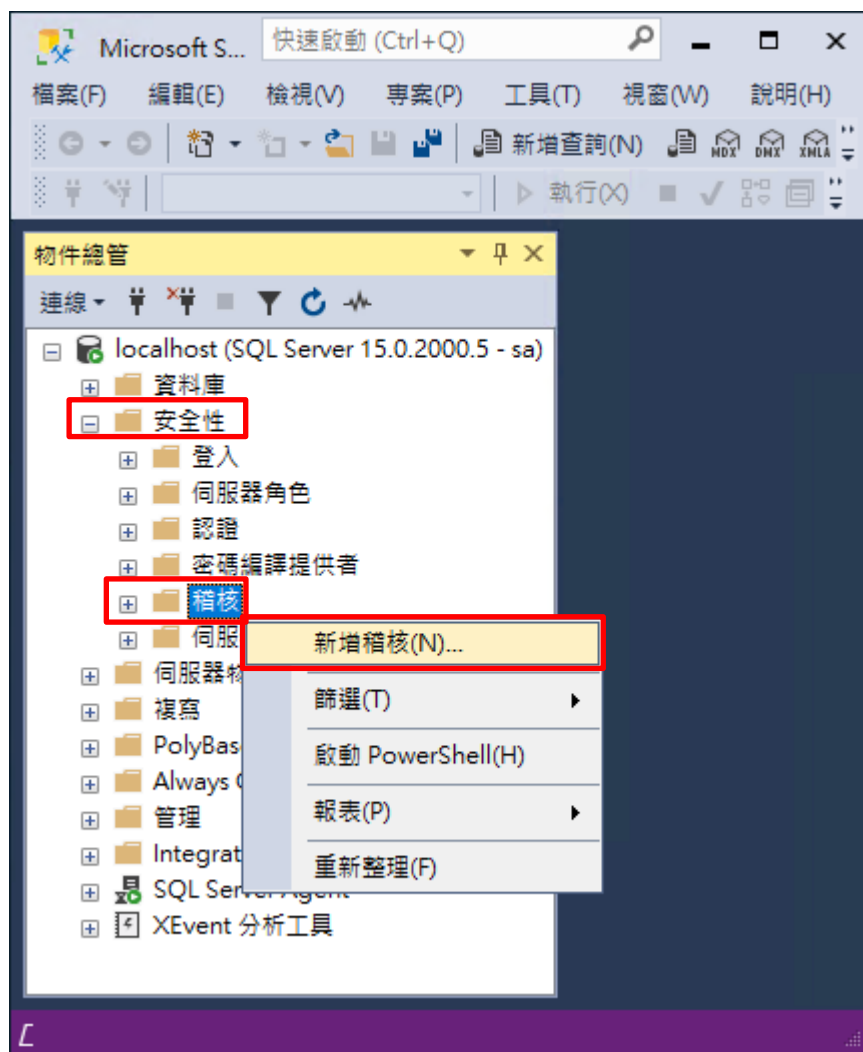
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]



(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): 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]

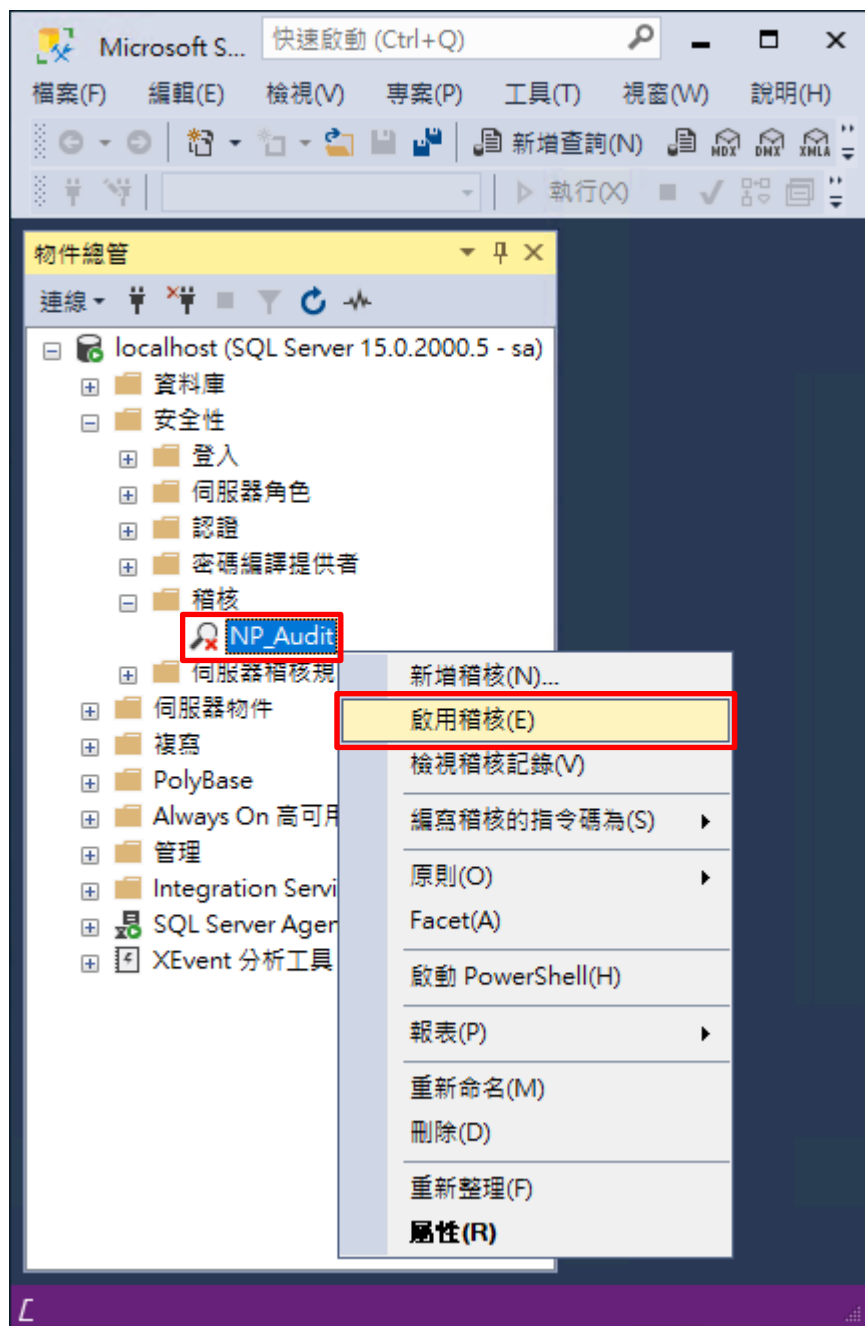
[檢視連線屬性](#)

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) 輸入資料庫稽核規格名稱: NP_DB-NCloud_Audit -> 選擇稽核名稱: [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]

建立資料庫稽核規格

就緒

選取頁面
一般

指令碼 說明

名稱(N): NP_DB-NCloud_Audit

稽核(A): NP_Audit

動作:

	稽核動作類型	物件類別	物件結構描述	物件名稱	主體名稱
01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP				
02	SCHEMA_OBJECT_CHANGE_GROUP				
03	DATABASE_OWNERSHIP_CHANGE_GROUP				
04	DATABASE_CHANGE_GROUP				
05	AUDIT_CHANGE_GROUP				
06	USER_CHANGE_PASSWORD_GROUP				
07	SCHEMA_OBJECT_CHANGE_GROUP				
08	FAILED_DATABASE_AUTHENTICATION_GROUP				
09	DATABASE_OBJECT_CHANGE_GROUP				
10	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
▶▶11					

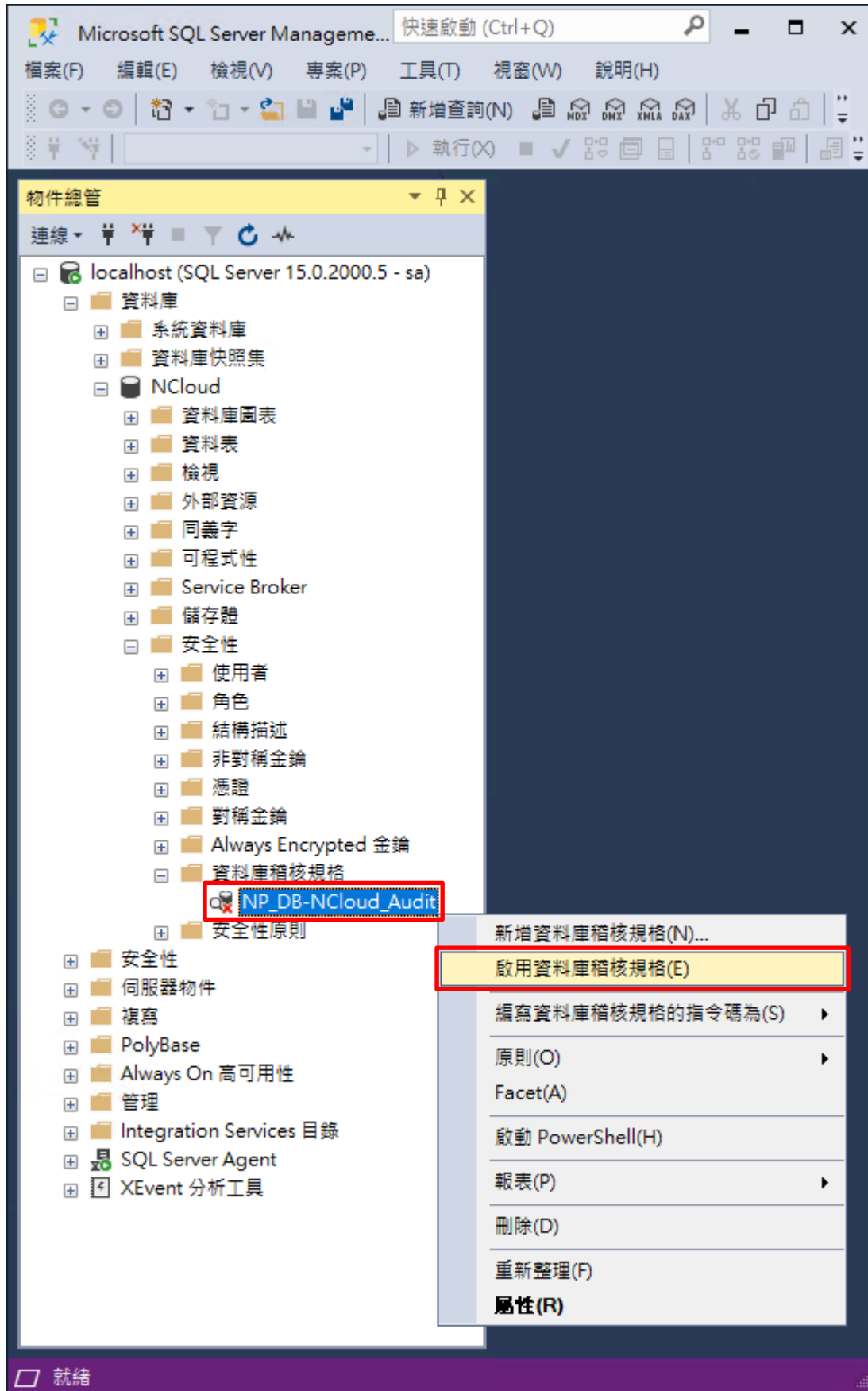
連線
SQL2019 [∞]

檢視連線屬性

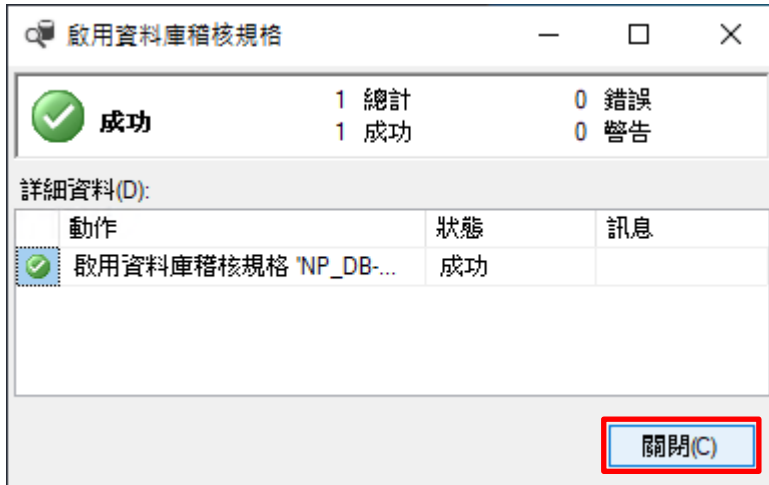
進度
完成

確定 取消 說明

(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

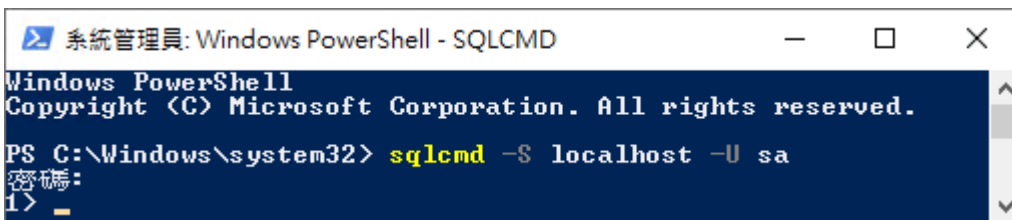
(1) 開啟 [Windows PowerShell]



(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
```

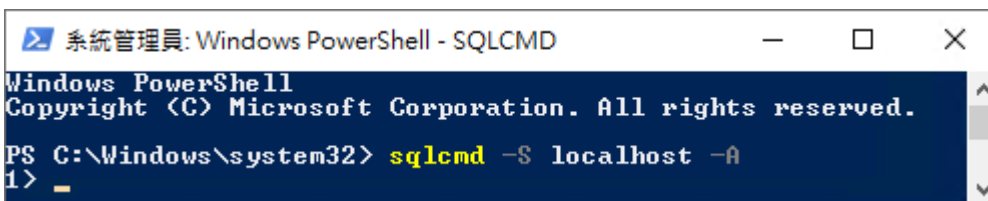


Options:

- S [protocol:]server[instance_name][,port]
- U login_id
- P password
- A dedicated administrator connection

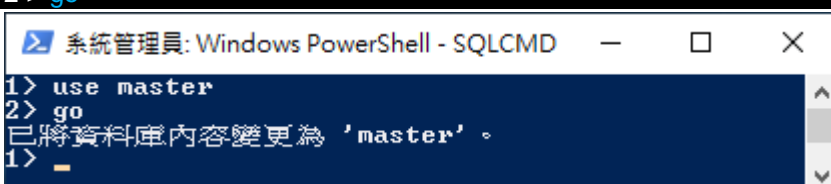
<2.2> 使用 Windows 帳號

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



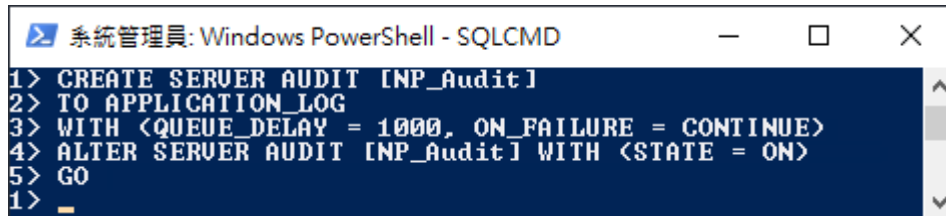
(3) 切換資料庫

```
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
```

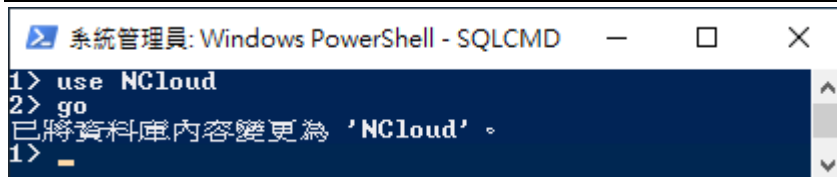


```
系統管理員: Windows PowerShell - SQLCMD
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

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
```

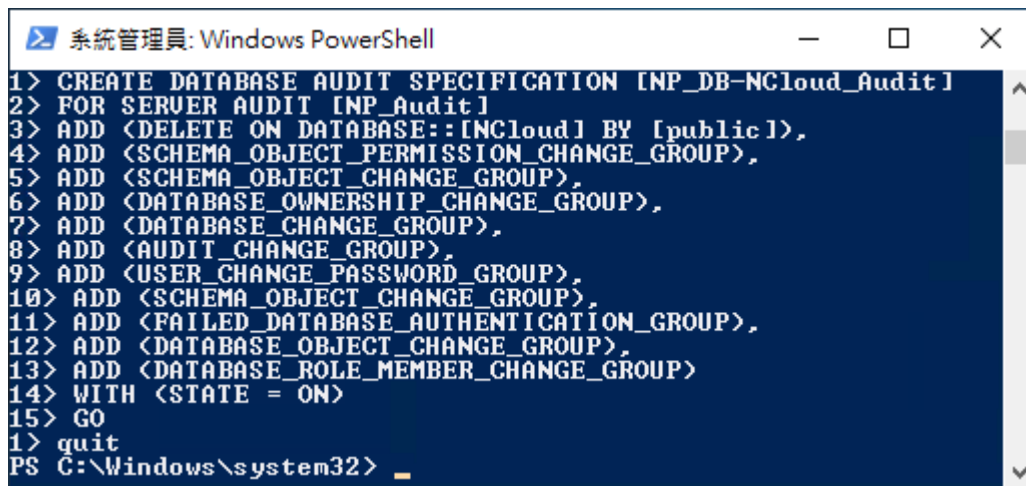


```
系統管理員: Windows PowerShell - SQLCMD
1> use NCloud
2> go
已將資料庫內容變更為 'NCloud'。
1> _
```

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::
```



```
系統管理員: Windows PowerShell
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::
```

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 (SELECT ON DATABASE::
```


5.3 事件記錄檔設定

此為選項設定。

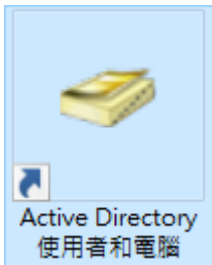
以下分別為網域和工作群組設定方式。

5.3.1 網域

5.3.1.1 組織單位設定

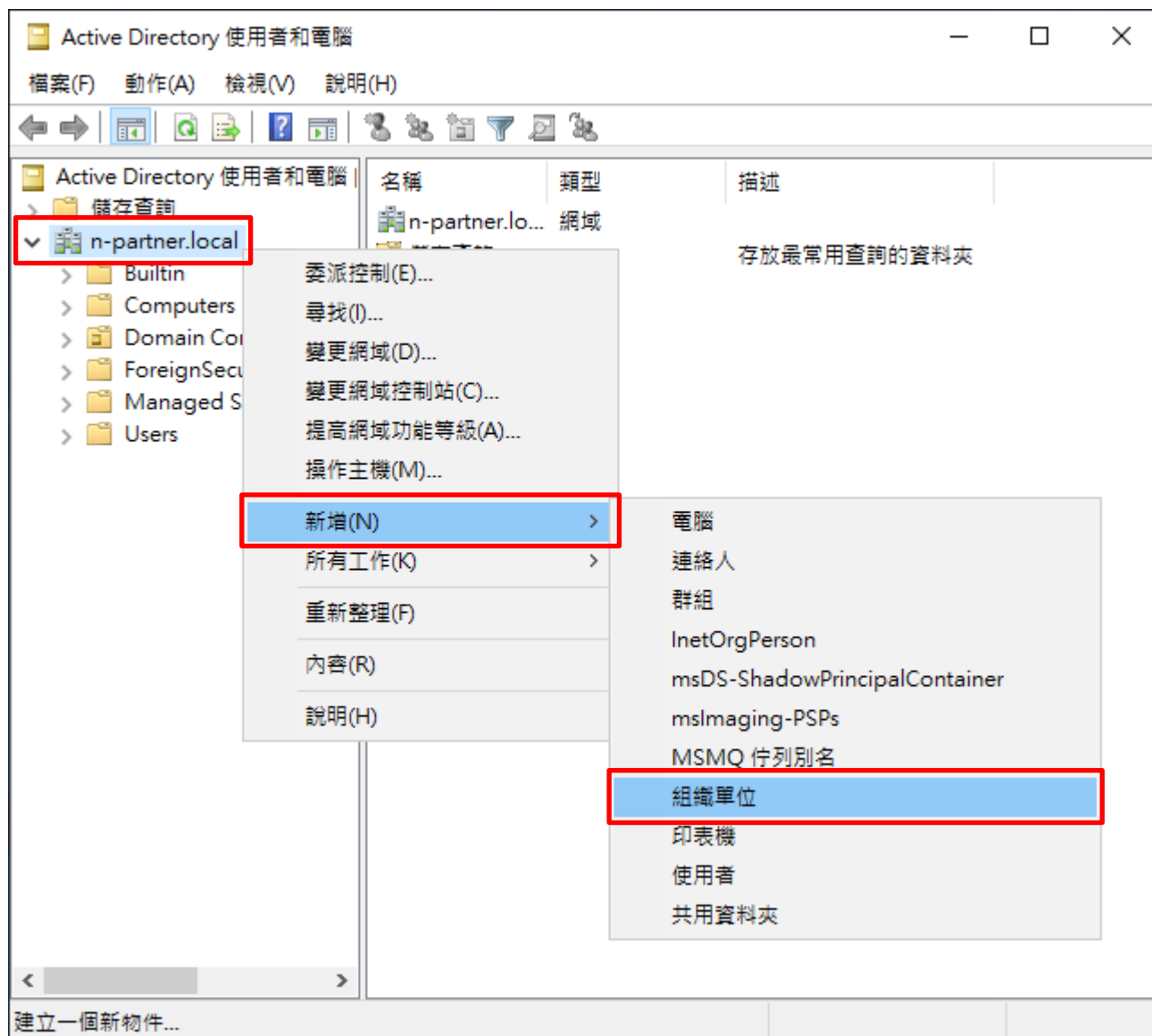
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



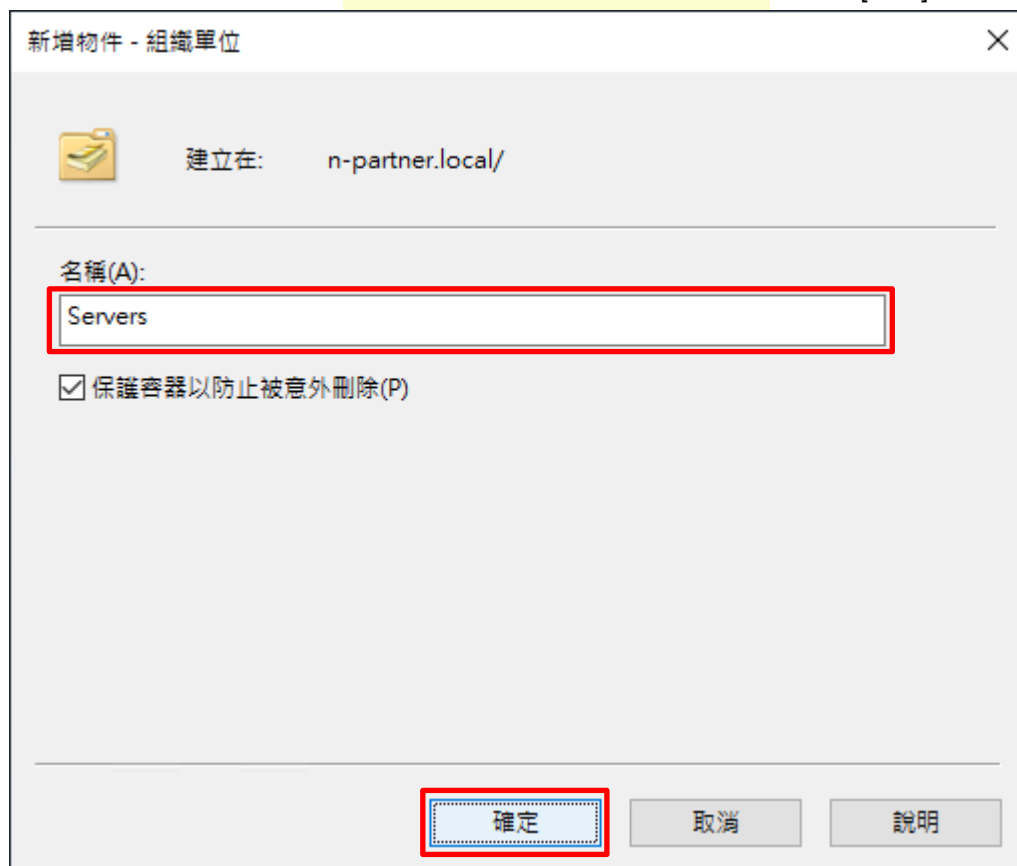
(2) 新增組織單位

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]



新增物件 - 組織單位

建立在: n-partner.local/

名稱(A):
Servers

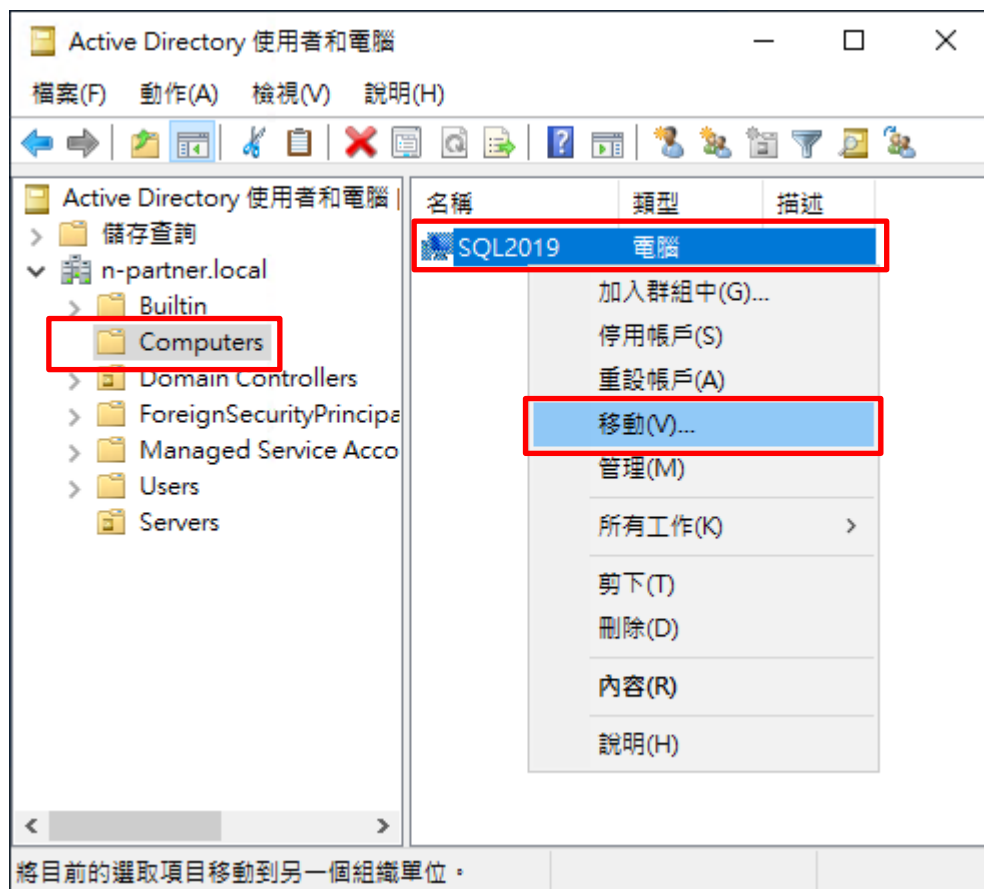
保護容器以防止被意外刪除(P)

確定 取消 說明

(4) 移動伺服器至新的組織單位

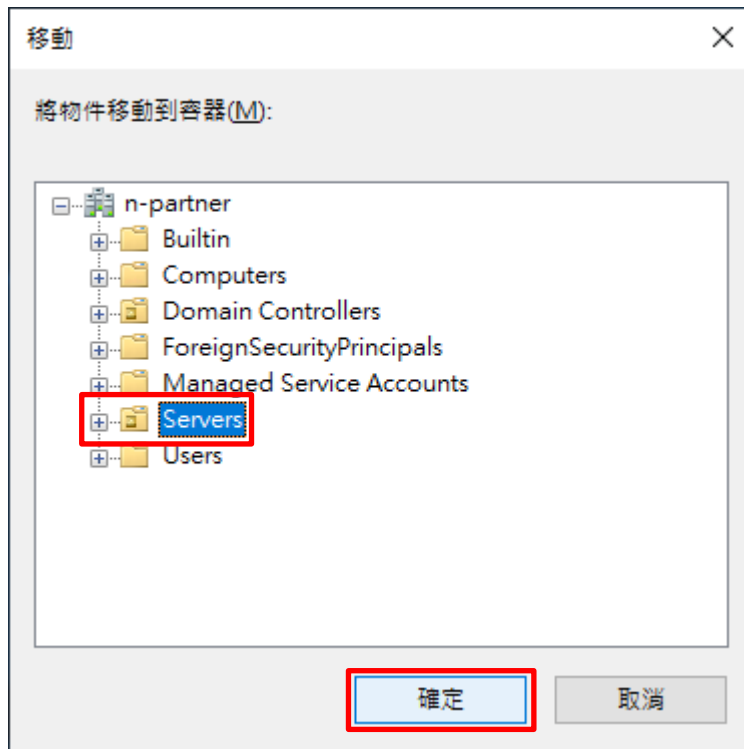
選擇 [Computers] 組織單位 -> 在 [SQL2019] 伺服器，按滑鼠右鍵，註：請依客戶環境選擇 MS SQL Server 主機

-> 點選 [移動]



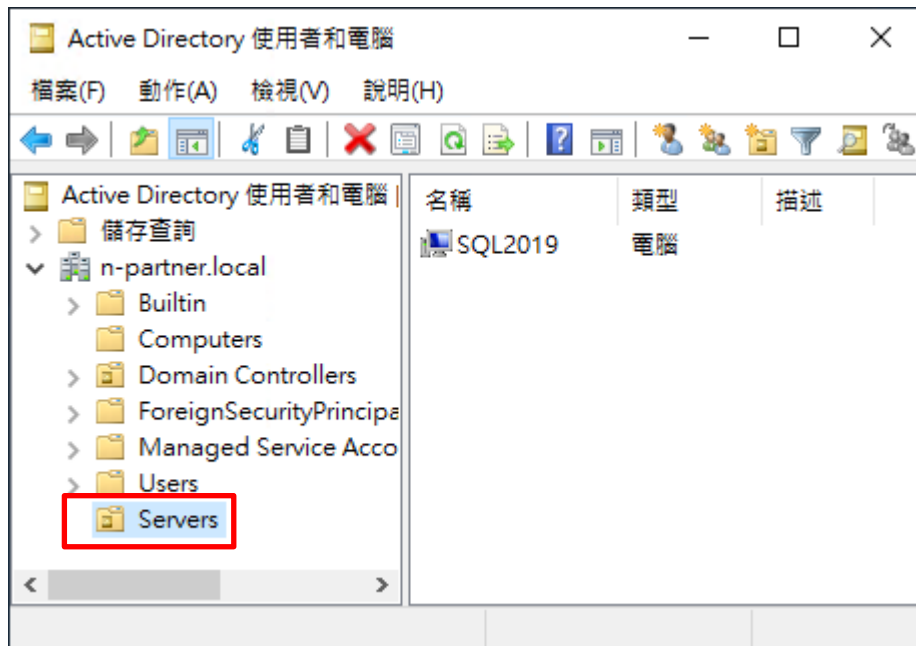
(5) 選擇組織單位

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

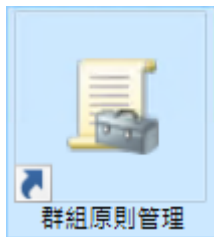
點選 [Servers] 組織單位，確認 SQL2019 伺服器已移動。



5.3.1.2 群組原則設定

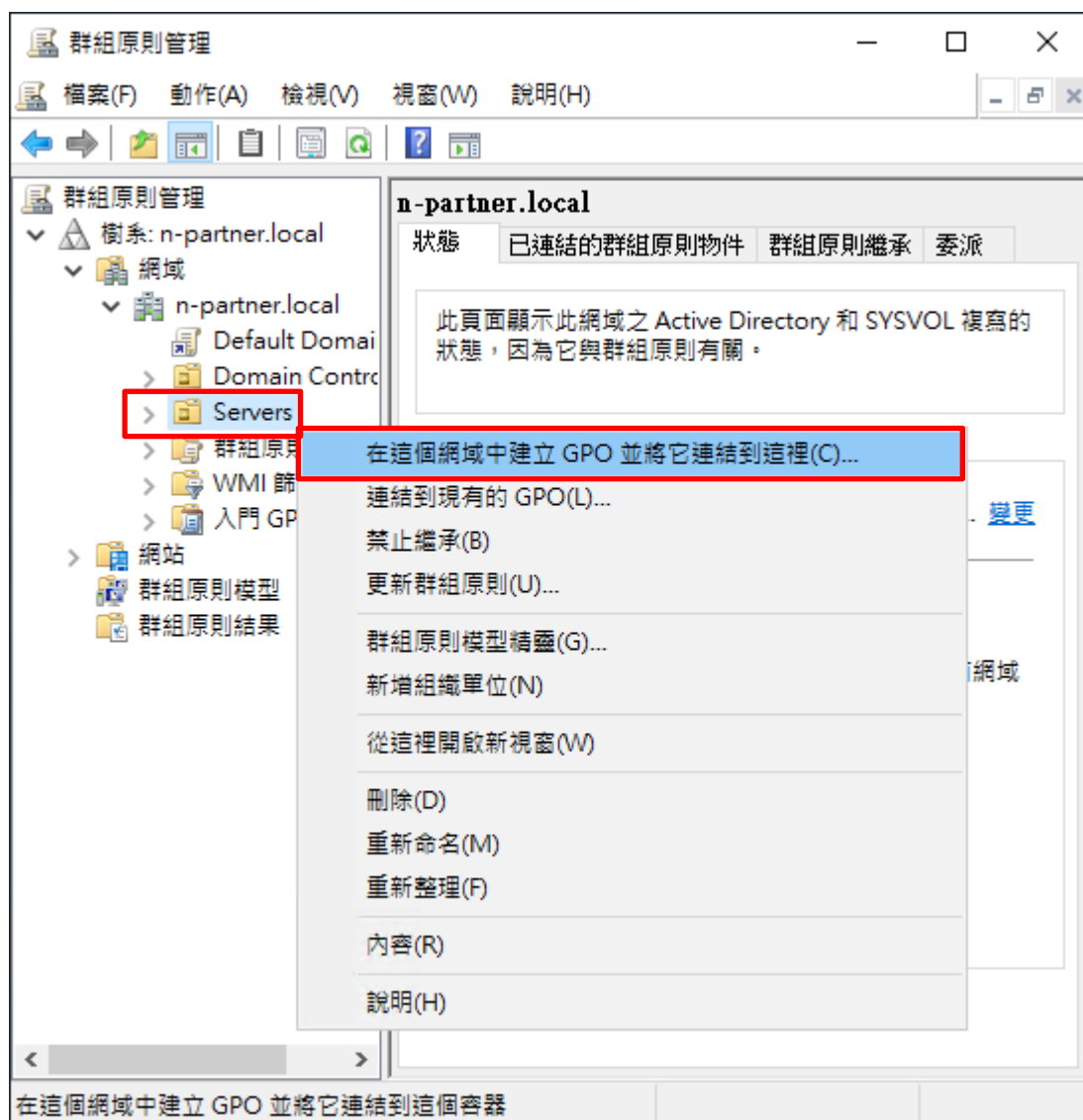
(1) 開啟群組原則管理

開啟 [群組原則管理]



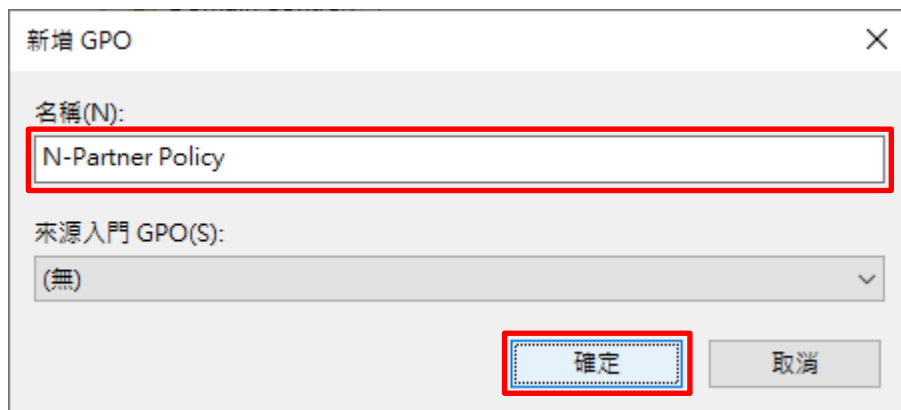
(2) 在 Servers 組織單位，新增群組原則物件

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



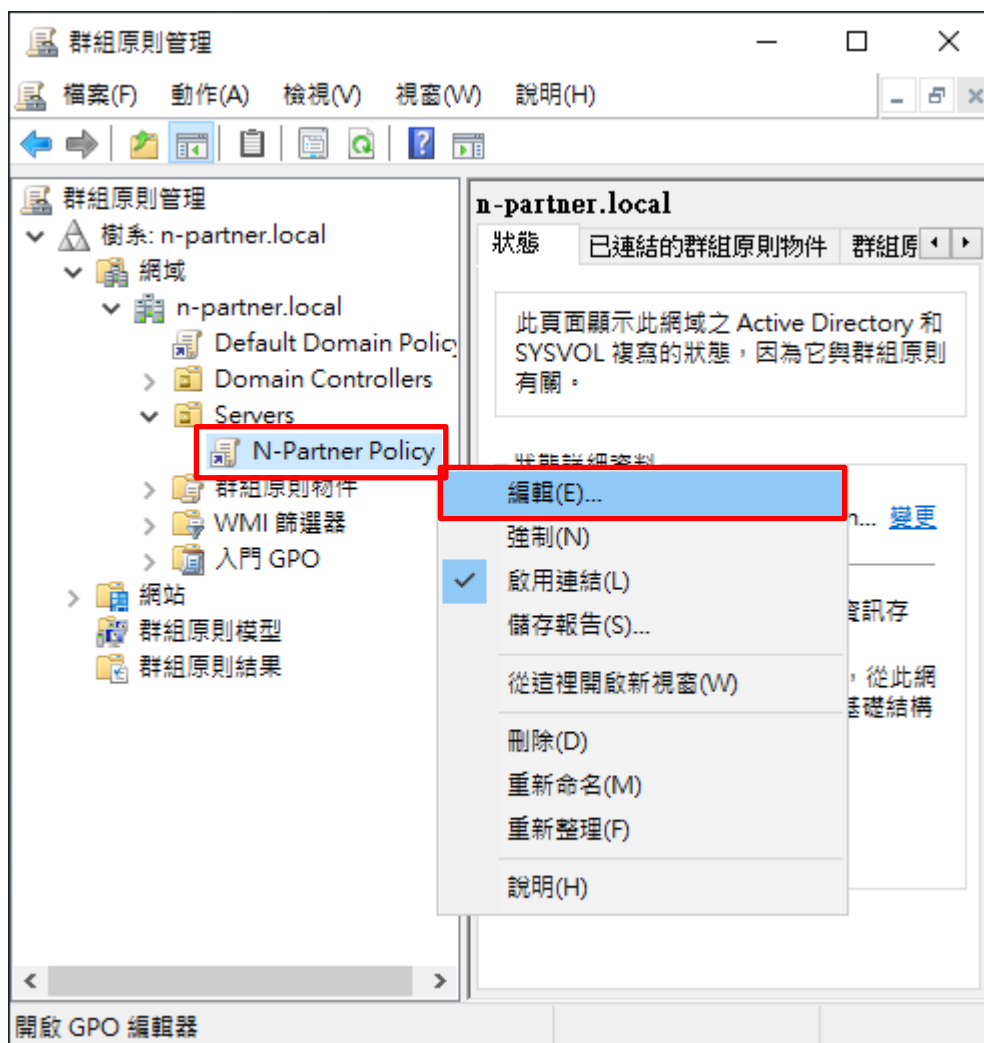
(3) 輸入群組原則物件名稱

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



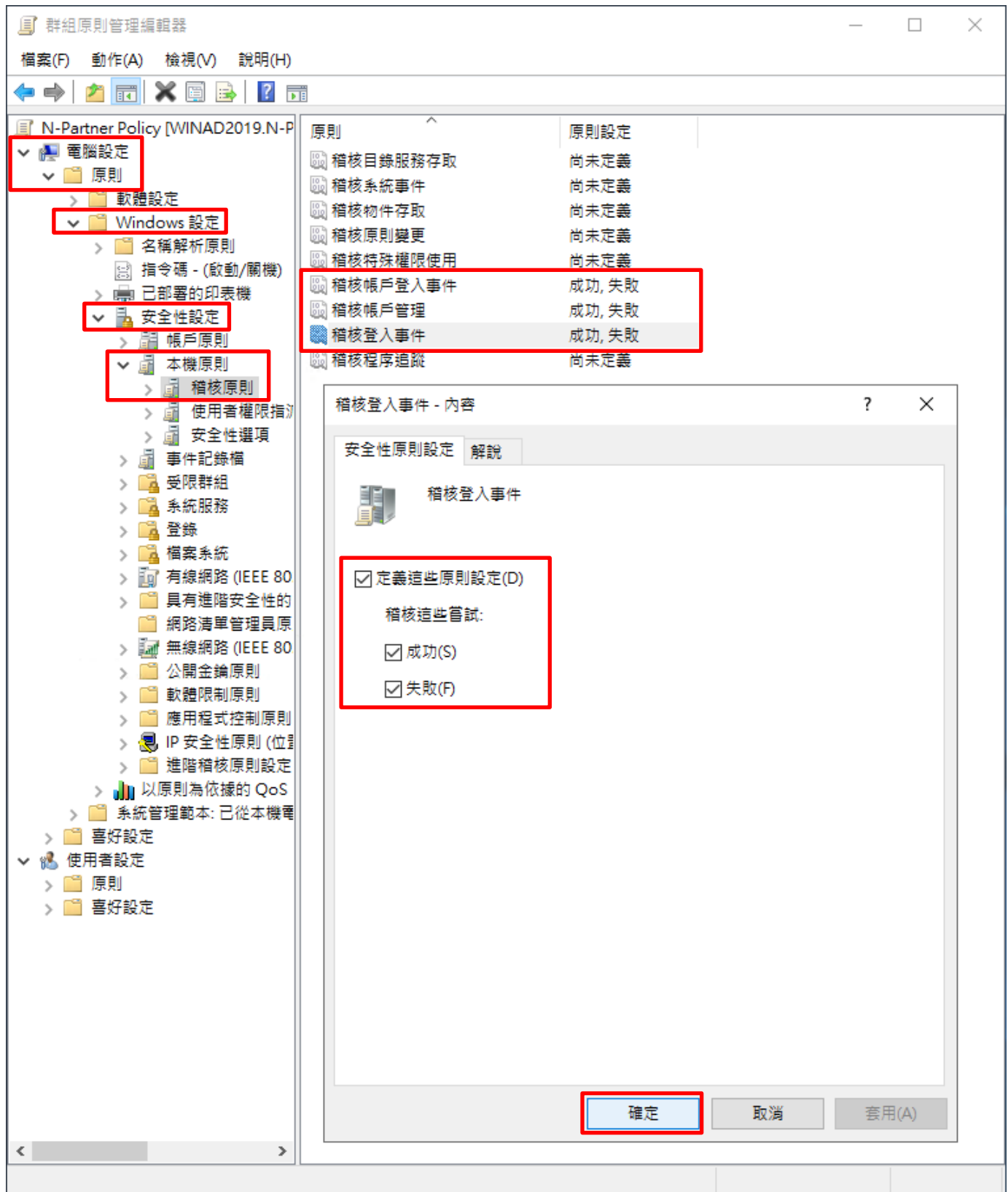
(4) 編輯群組原則物件

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



(5) 本機原則：稽核原則

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [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) 事件記錄檔：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]

The screenshot shows the Group Policy Editor window titled '群組原則管理編輯器'. The left-hand navigation pane is expanded to show the path: 電腦設定 > 原則 > Windows 設定 > 安全性設定 > 事件記錄檔. The '事件記錄檔' folder is selected, and the '應用程式記錄保持方法' policy is highlighted in the main list. The policy's current setting is '視需要而定'. A secondary dialog box titled '應用程式記錄保持方法 - 內容' is open, showing the configuration options for this policy. The '定義這個原則設定(D)' checkbox is checked. The '視需要覆寫事件(M)' radio button is selected. The '確定' button is highlighted at the bottom of the dialog.

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

應用程式記錄保持方法 - 內容

安全性原則設定 解說

應用程式記錄保持方法

定義這個原則設定(D)

依日期覆寫事件(O)

視需要覆寫事件(M)

不要覆寫事件 (以手動方式清除記錄)(N)

確定 取消 套用(A)

(7) 事件記錄檔：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]

The screenshot shows the Group Policy Editor window titled "群組原則管理編輯器". The left-hand navigation pane is expanded to show the following path: 電腦設定 (Computer Configuration) > 原則 (Policies) > Windows 設定 (Windows Settings) > 安全性設定 (Security Settings) > 事件記錄檔 (Event Log). The right-hand pane displays a list of policies. The policy "應用程式記錄檔大小最大值" (Application Log Size Limit) is selected and highlighted with a red box. Its value is set to "204800 KB".

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

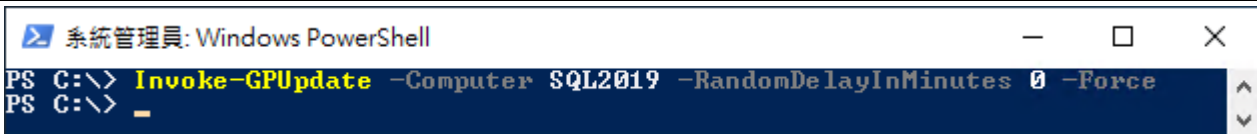
An inset dialog box titled "應用程式記錄檔大小最大值 - 內容" (Application Log Size Limit - Content) is open. It shows the "安全性原則設定" (Security Policy Settings) tab. The "定義這個原則設定(D)" (Define this policy setting) checkbox is checked. Below it, the value "204800" is entered in a text box, followed by "KB". The "確定" (OK) button is highlighted with a red box.

(8) 開啟 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

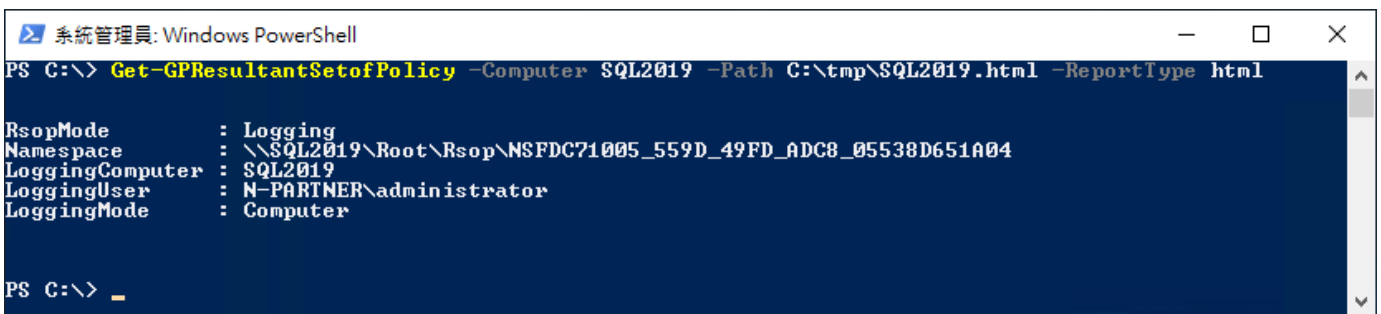
```
PS C:\> Invoke-GPUdate -Computer SQL2019 -RandomDelayInMinutes 0 -Force
```



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

Browser: C:\tmp\SQL2019.html | 搜尋... | N-PARTNER\SQL2019

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

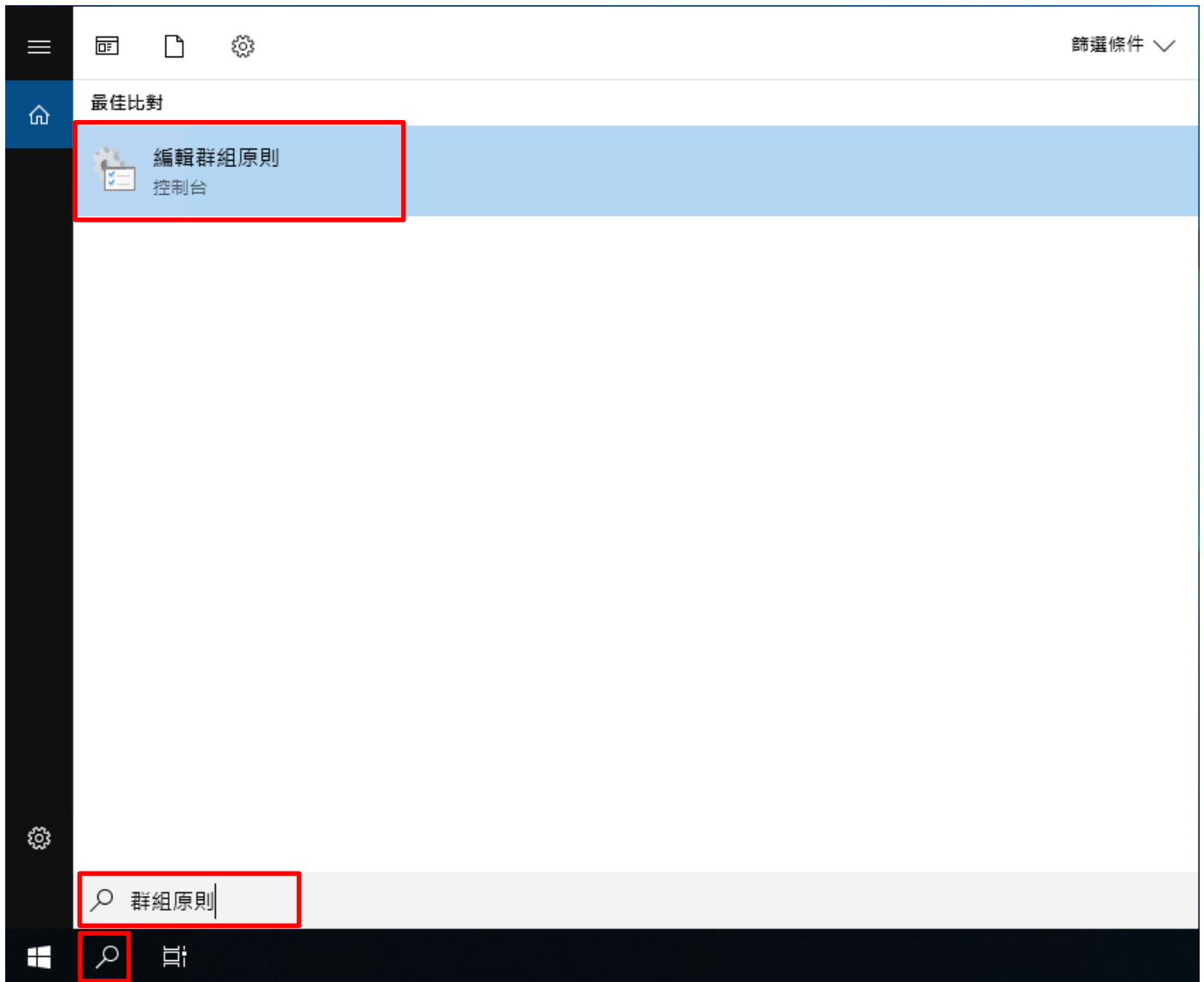
摘要	顯示												
電腦詳細資料	隱藏												
一般	顯示												
元件狀態	顯示												
設定	隱藏												
原則	隱藏												
Windows 設定	隱藏												
安全性設定	隱藏												
帳戶原則/密碼規則	顯示												
帳戶原則/帳戶鎖定原則	顯示												
本機原則/稽核原則	隱藏												
	<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>稽核帳戶登入事件</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> <tr> <td>稽核帳戶管理</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> <tr> <td>稽核登入事件</td> <td>成功, 失敗</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	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
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												
	<table border="1"> <thead> <tr> <th>原則</th> <th>設定</th> <th>優勢 GPO</th> </tr> </thead> <tbody> <tr> <td>應用程式記錄保持方法</td> <td>視需要而定</td> <td>N-Partner Policy</td> </tr> <tr> <td>應用程式記錄檔容量最大值</td> <td>204800 KB</td> <td>N-Partner Policy</td> </tr> </tbody> </table>	原則	設定	優勢 GPO	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			
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]

The screenshot shows the Windows Security Policy Editor window titled "本機群組原則編輯器". The left-hand navigation pane shows a tree view where "電腦設定" (Computer Settings) is expanded, followed by "Windows 設定" (Windows Settings), "安全性設定" (Security Settings), "本機原則" (Local Policies), and "稽核原則" (Audit Policies). The main pane displays a list of audit policies with their corresponding "安全性設定" (Security Settings). The "稽核登入事件" (Audit Logon Events) policy is selected and highlighted with a red box. Below the list, a dialog box titled "稽核登入事件 - 內容" (Audit Logon Events - Content) is open, showing the "稽核這些嘗試" (Audit these attempts) section with checkboxes for "成功(S)" (Success) and "失敗(F)" (Failure), both of which are checked. A warning icon and message are visible at the bottom of the dialog, stating: "如果已設定其他原則以覆寫類別層級稽核原則，可能不會強制執行此設定。如需其他資訊，請參閱稽核登入事件。(Q921468)". The "確定" (OK) button is highlighted with a red box.

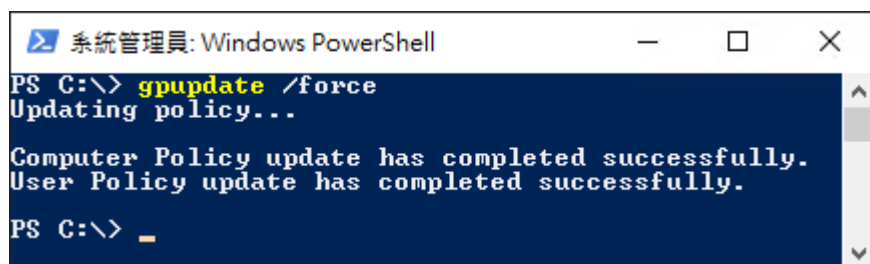
原則	安全性設定
稽核目錄服務存取	沒有稽核
稽核系統事件	沒有稽核
稽核物件存取	沒有稽核
稽核原則變更	沒有稽核
稽核特殊權限使用	沒有稽核
稽核帳戶登入事件	成功, 失敗
稽核帳戶管理	成功, 失敗
稽核登入事件	成功, 失敗
稽核程序追蹤	沒有稽核

(3) 開啟 [Windows PowerShell]



(4) 更新群組原則

PS C:\> gpupdate /force

A screenshot of a Windows PowerShell terminal window. The title bar reads "系統管理員: Windows PowerShell". The terminal content shows the command "gpupdate /force" being executed, followed by "Updating policy...", "Computer Policy update has completed successfully.", and "User Policy update has completed successfully.". The prompt "PS C:\> _" is visible at the bottom.

```
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

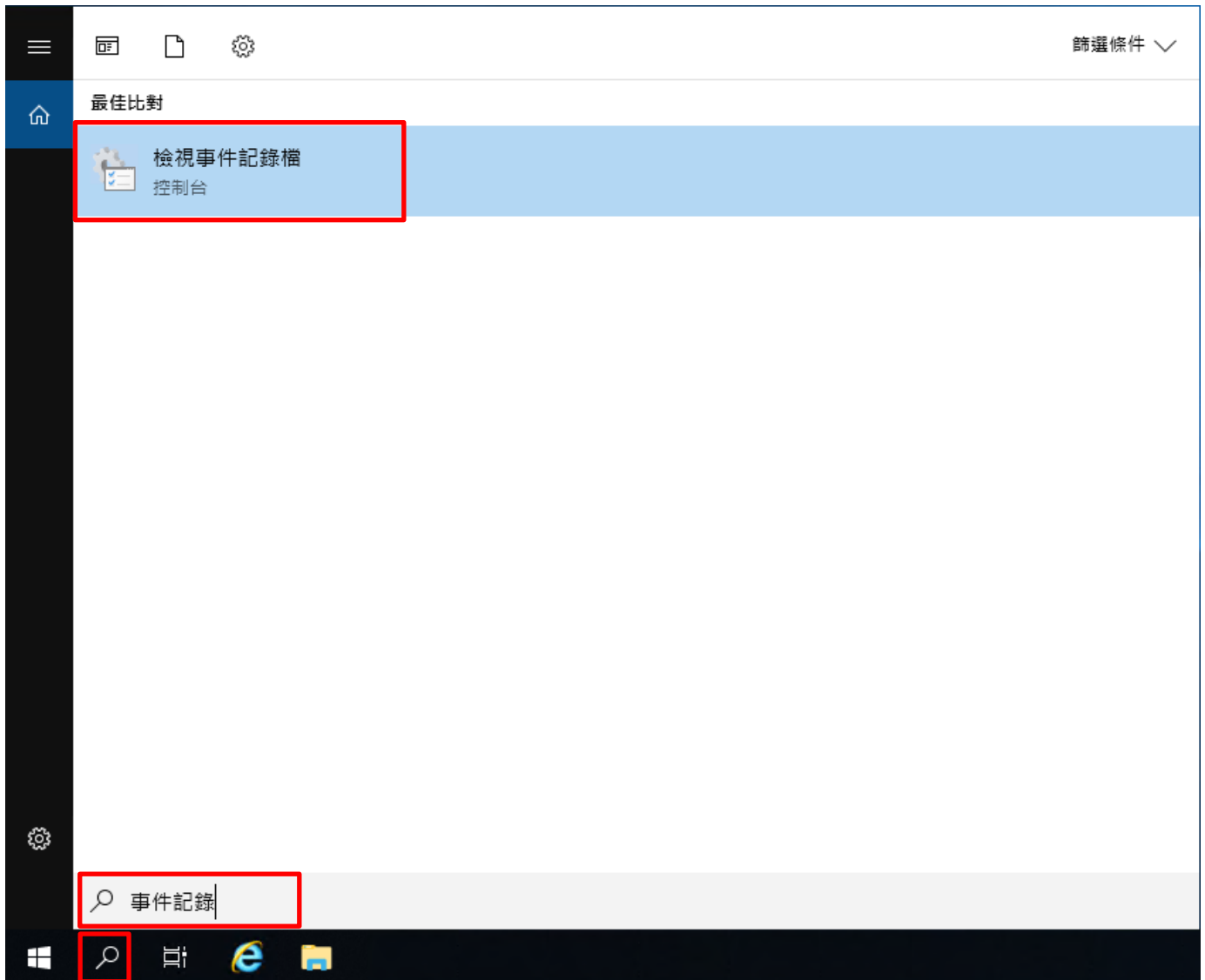
PS C:\> auditpol /get /category:*

```
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

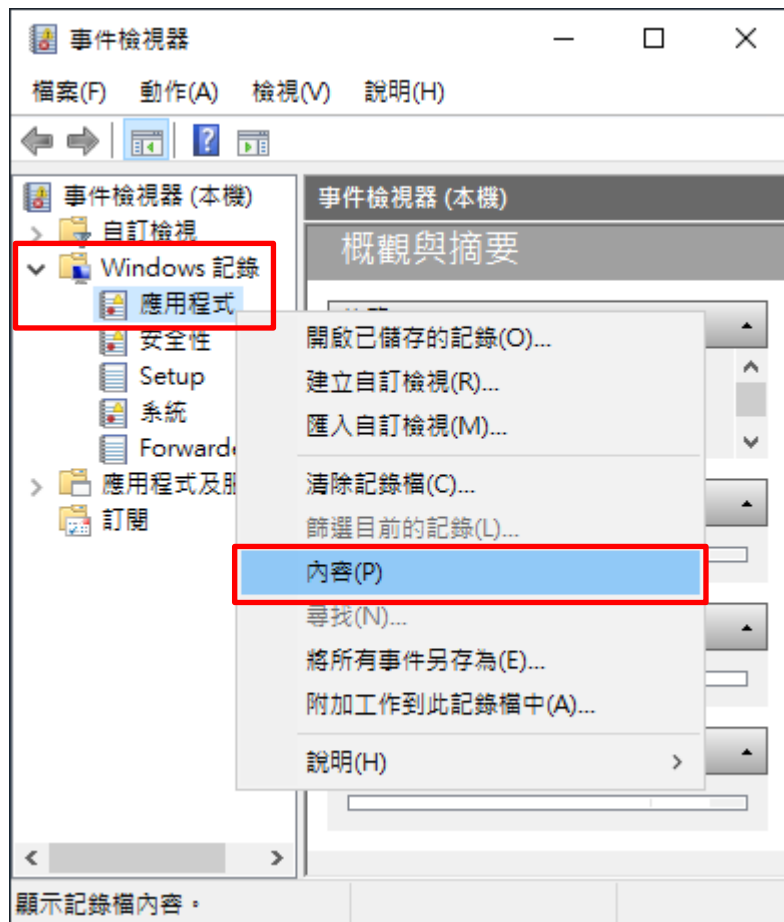
(1) 開啟 [檢視事件記錄檔]

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]



(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]

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9日 下午 08:56:09

修改日期: 2021年7月5日 下午 05:13:07

存取日期: 2021年7月5日 下午 05:13:07

啟用記錄(E)

最大記錄檔大小 (KB)(X): 204800

當事件記錄檔的大小到達上限時:

視需要覆寫事件 (先覆寫最舊的事件)(W)

當記錄檔已滿時進行封存，不要覆寫事件(A)

不要覆寫事件 (手動清除記錄檔)(N)

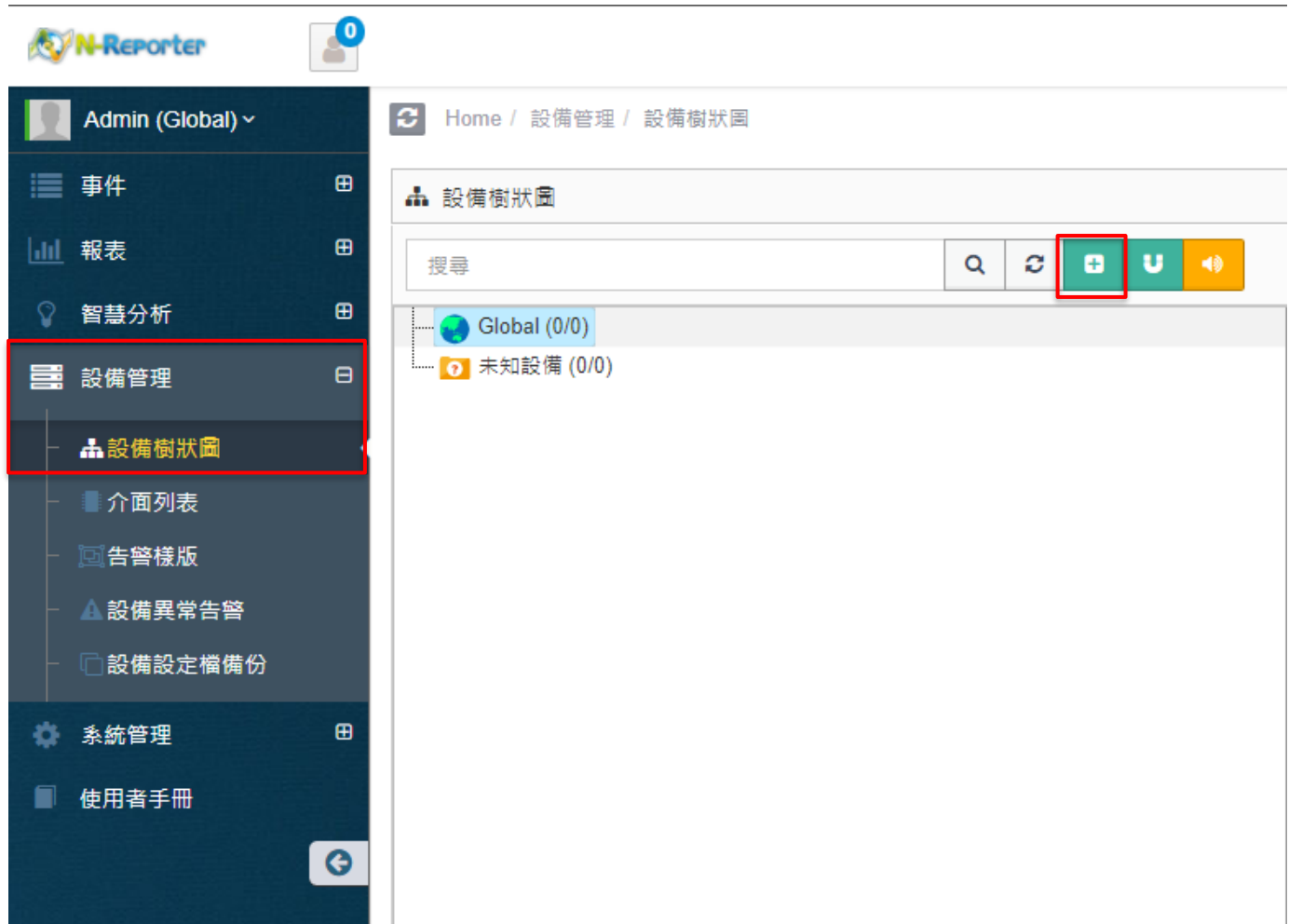
清除記錄(R)

確定 取消 套用(P)

6. N-Reporter

(1) 新增 MS SQL 設備

[設備管理] -> [設備樹狀圖] -> 點選  [新增]



The screenshot displays the N-Reporter web application interface. On the left is a dark sidebar menu with the following items: Admin (Global) v, 事件, 報表, 智慧分析, 設備管理 (highlighted with a red box), 設備樹狀圖 (highlighted with a red box), 介面列表, 告警樣版, 設備異常告警, 設備設定檔備份, 系統管理, and 使用者手冊. The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖' and a search bar with a search icon, a refresh icon, a green 'add' icon (highlighted with a red box), a 'U' icon, and a speaker icon. Below the search bar, there is a tree view with 'Global (0/0)' and '未知設備 (0/0)'.

6.1 MS SQL Server Event Log

(2) 設定 MS SQL Event log 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [MS SQL] 和 Facility: [(18) local use 2 (local2)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

設備基本設定

名稱
MSSQL-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
MS SQL

使用自定義資料格式

Facility
(18) local use 2 (local2)

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

設備進階設定

ICMP 告警樣版
N/A

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊

6.2 Windows Event Log

(2) 設定 Windows Event log 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] 和 Facility: [(17) local use 1 (local1)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

新增設備

設備基本設定

名稱
Windows-192.168.8.183

IP
192.168.8.183

設備種類
 Syslog Flow SNMP PM

Syslog 相關設定

資料格式
Windows

使用自定義資料格式

Facility
(17) local use 1 (local1)

編碼方式
UTF-8

日誌保留 Raw Data Raw Data

設備進階設定

ICMP 告警樣版
----- N/A -----

設備 Icon
icon-host

Login Account

Login Password

Enable Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog 暫無資料告警

告警通報設定
預設

資料保留天數

經緯度
緯度 經度

確定 取消

若勾選 [日誌保留 Raw Data] ·

[事件查詢] 顯示 Raw Data 資訊



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