N-Partner

如何設定
MS SQL 稽核事件記錄

V020

2024/07/26

版權聲明

商標

目錄

前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 MS SQL 事件記錄。

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

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

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

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

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

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

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

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

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

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

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

MS SQL Server 支援稽核記錄版本

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

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

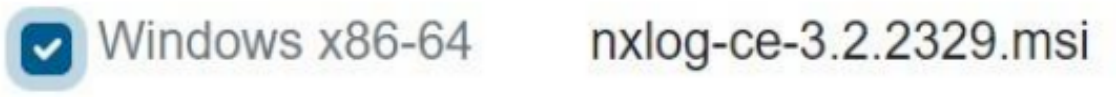
1 NXLog

1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition

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

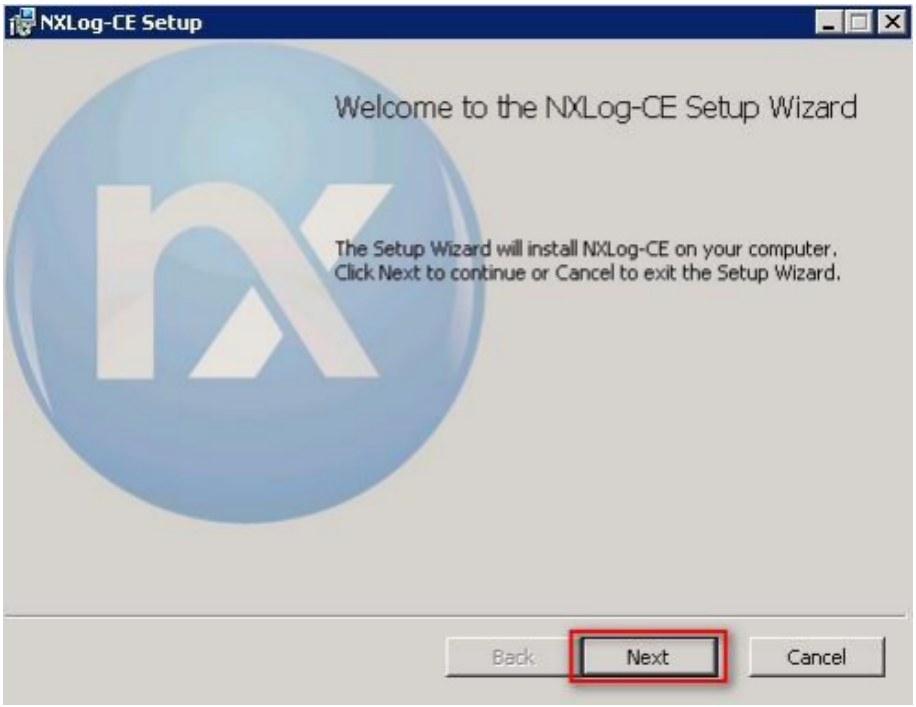
下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.2.2329.msi



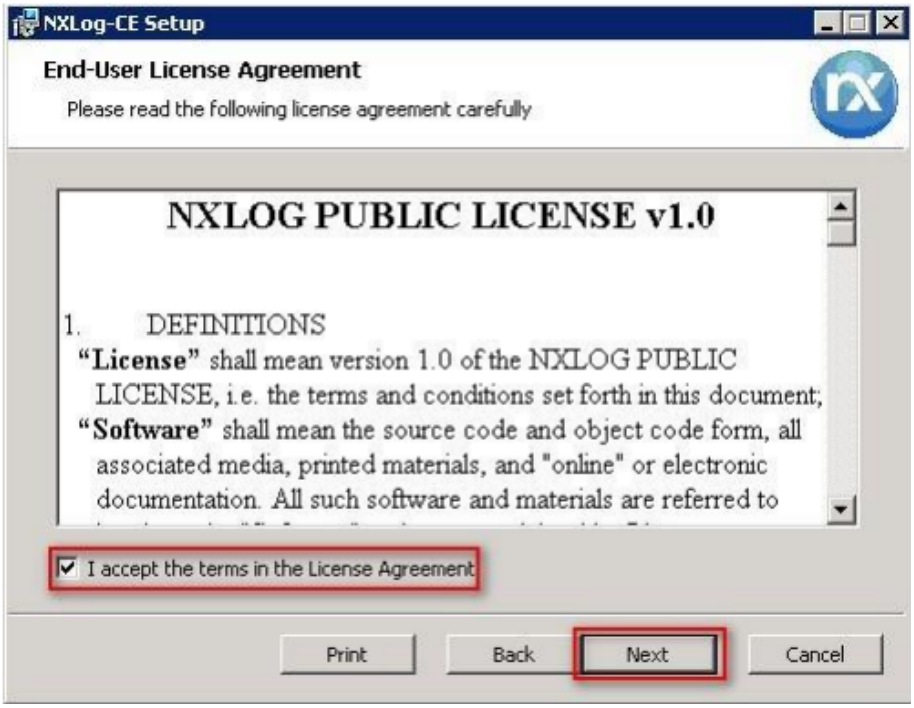
註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog

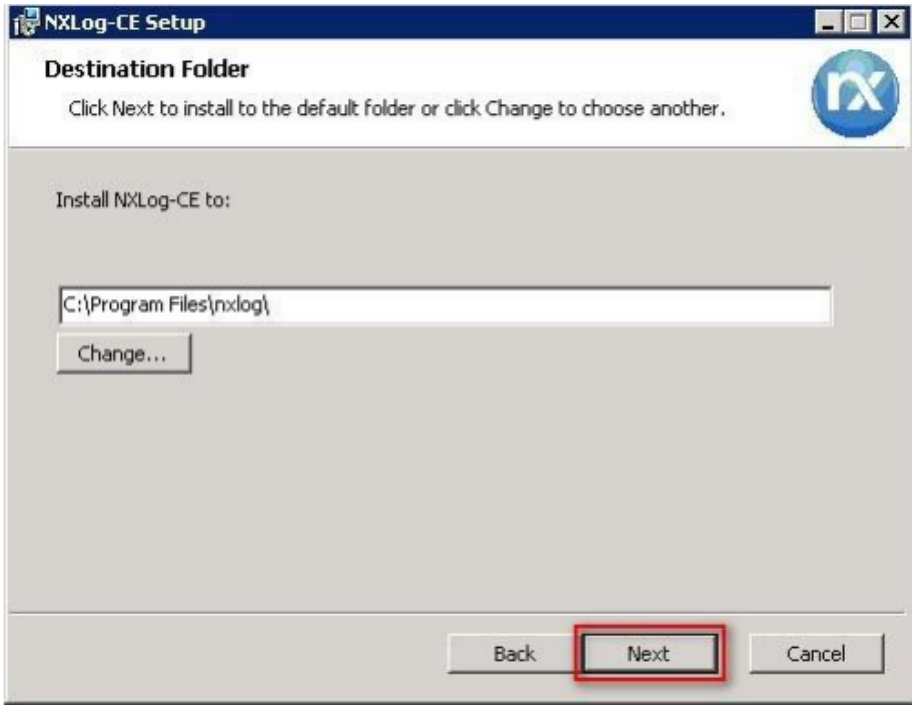
-> 點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



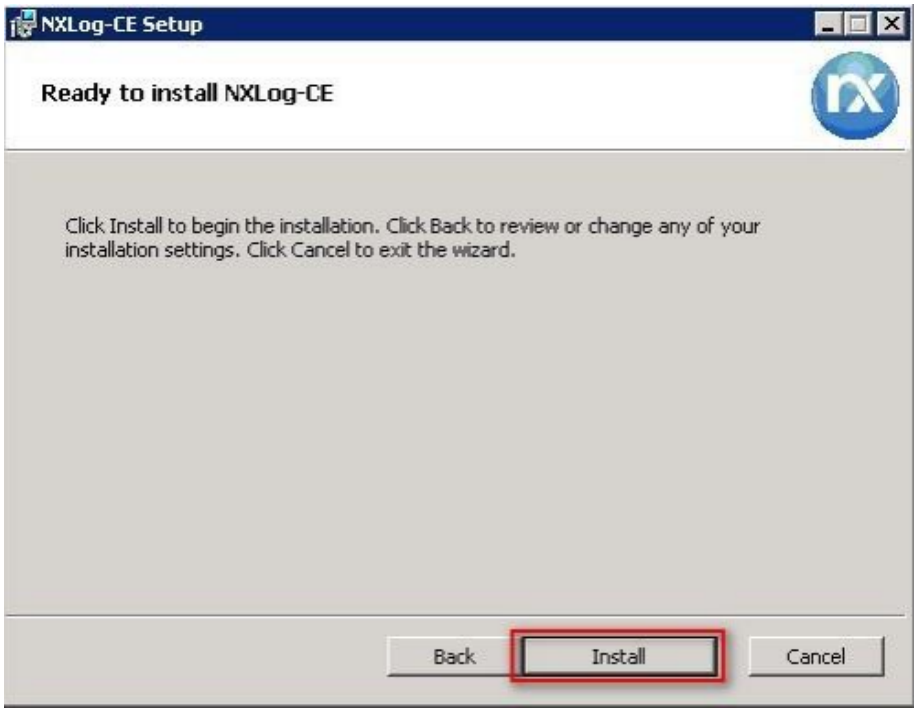
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



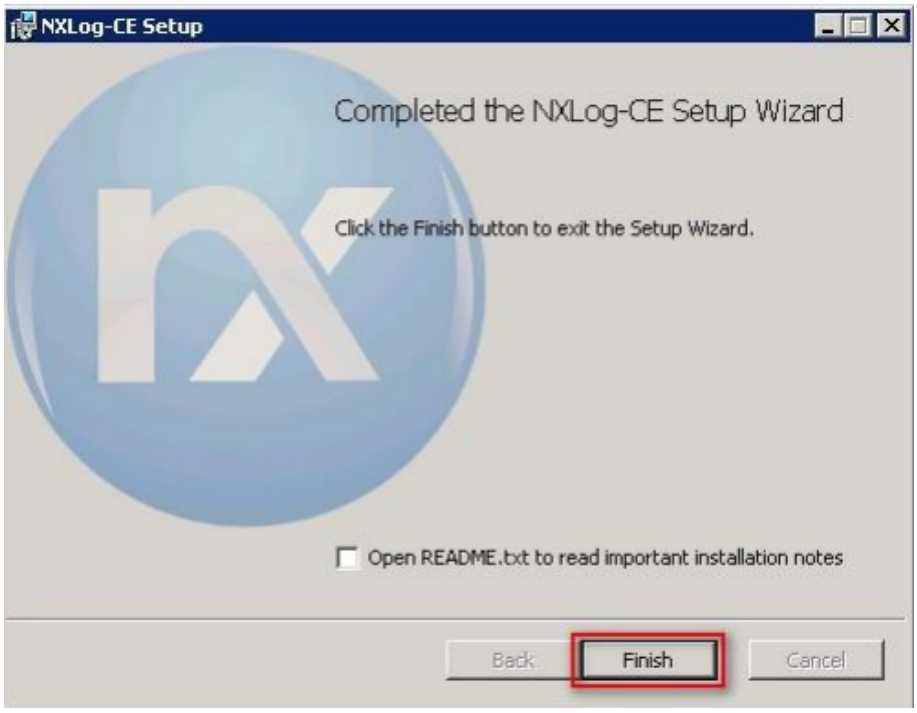
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].



-> 按 [Finish].



1.2 NXLog 設定檔下載

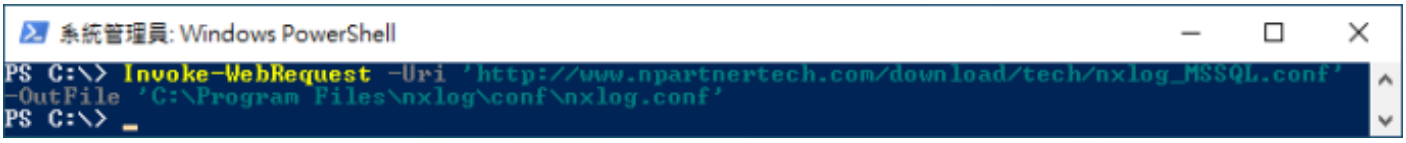
1.2.1 MS SQL 單機設定檔

(1) 開啟 [Windows PowerShell]

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

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

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



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

1.2.2 MS SQL Cluster 叢集設定檔

(1) 開啟 [Windows PowerShell]

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

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

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

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

1.3 NXLog 設定檔

1.3.1 MS SQL 單機設定檔

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

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

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

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

<Output out_sqllog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 18;
    Exec    $Message = "MSSQLSERVER" + ":  " + string($EventID) + ":  " + $Message;
    Exec    if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
                else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
                else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec    to_syslog_bsd();
</Output>

<Route sqllog>
    Path    in_sqllog => out_sqllog
</Route>

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

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

<Output out_eventlog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 17;
    Exec    $Message = string($SourceName) + ":  " + string($EventID) + ":  " + $Message;
    Exec    if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
                else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
                else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec    to_syslog_bsd();
</Output>

<Route eventlog>
    Path    in_eventlog => out_eventlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud  192.168.8.4
```

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

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

藍色文字部位請輸入 MS SQL 執行個體名稱

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

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

1.3.2 MS SQL Cluster 叢集設定檔

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

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

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

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

<Output out_sqllog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 18;
    Exec    $Message = "MSSQLSERVER" + ":  "  + string($EventID) + ":  "  + $Message;
    Exec    if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
                else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
                else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec    to_syslog_bsd();
</Output>

<Route sqllog>
    Path    in_sqllog => out_sqllog
</Route>

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

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

<Output out_eventlog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 17;
    Exec    $Message = string($SourceName) + ":  " + string($EventID) + ":  " + $Message;
    Exec    if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
                else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
                else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec    to_syslog_bsd();
</Output>

<Route eventlog>
    Path    in_eventlog => out_eventlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud  192.168.8.4
```

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

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

藍色文字部位請輸入 MS SQL 執行個體名稱

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

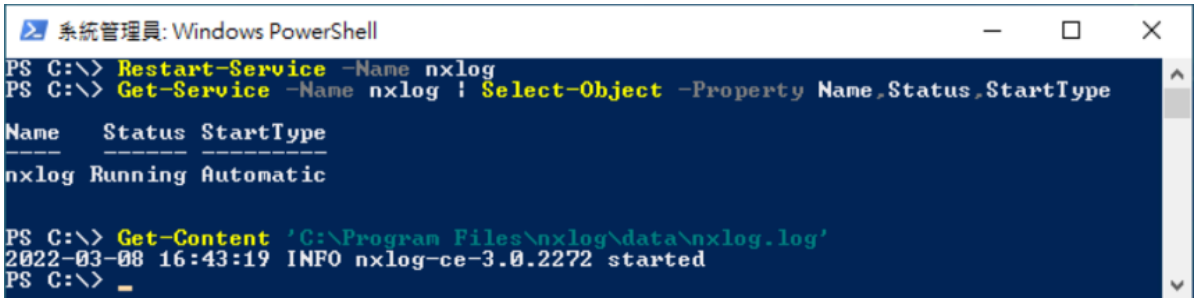
修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)”，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]

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

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

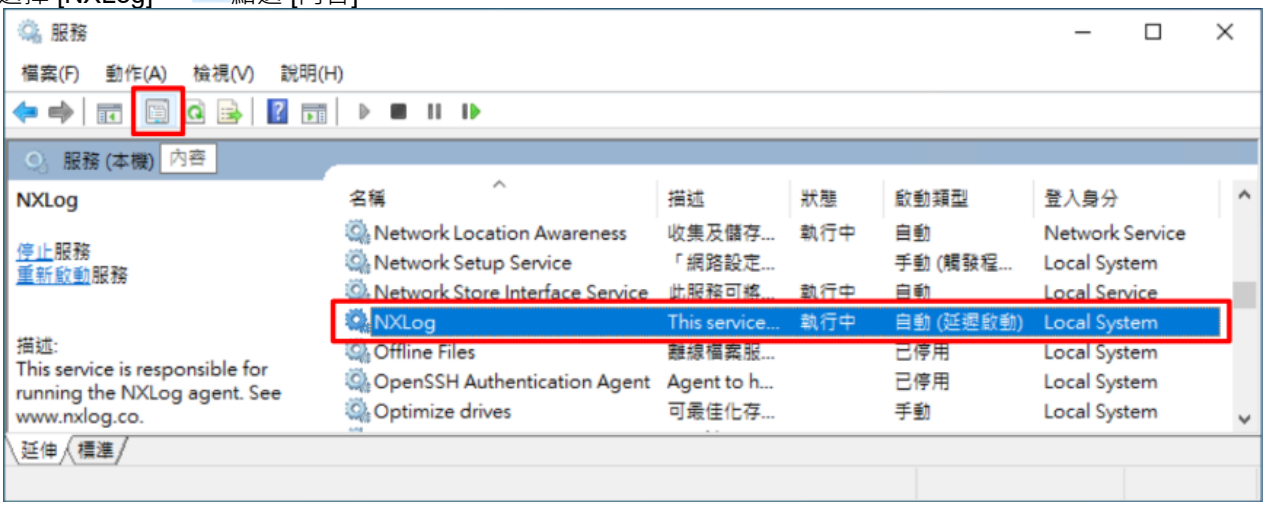


(3) 開啟 [服務] 功能

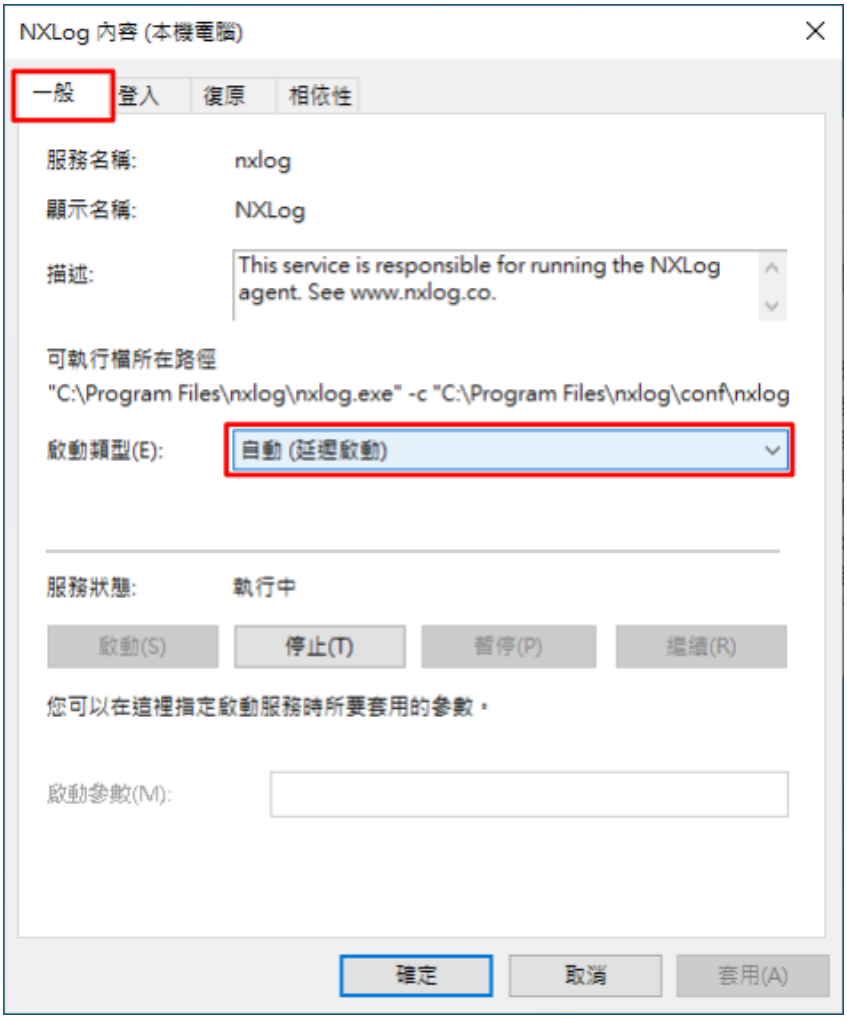
```
PS C:\> Services.msc
```

(4) 開啟 NXLog 服務內容

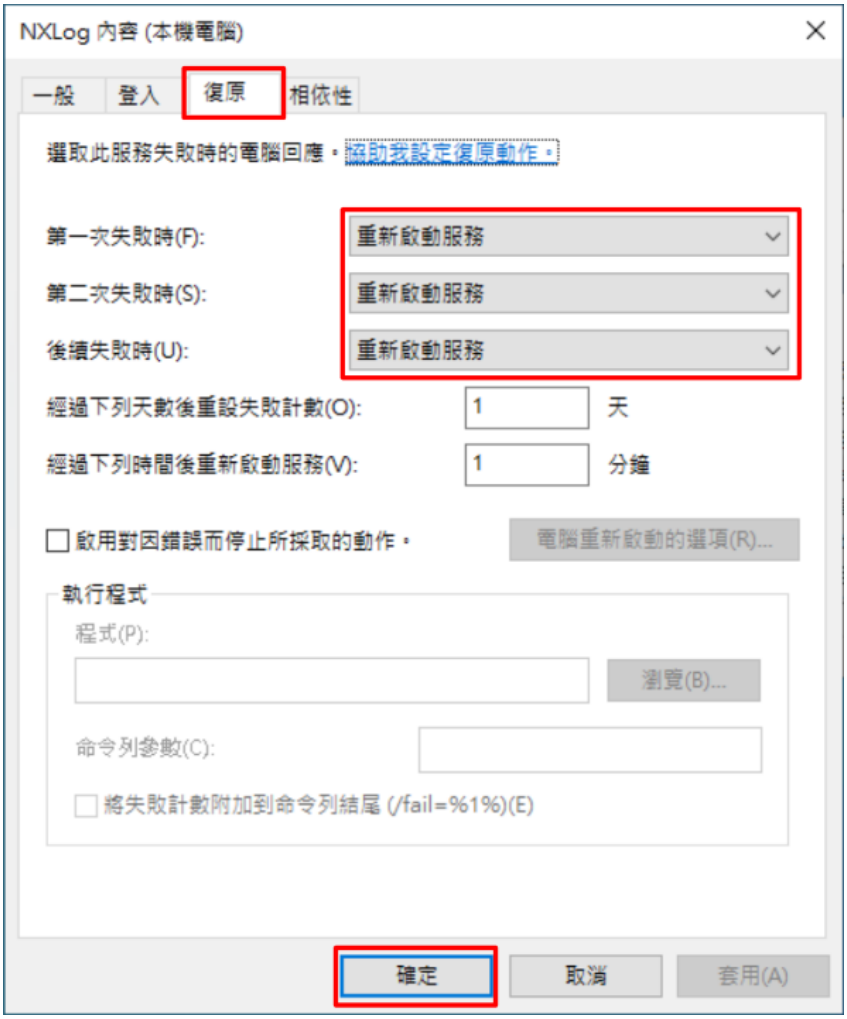
選擇 [NXLog] -> 點選 [內容]



(5) [一般] 頁面 -> 確認; 啟動類型: [自動 (延遲啟動)]



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



2 SQL2008

2.1 稽核登入

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

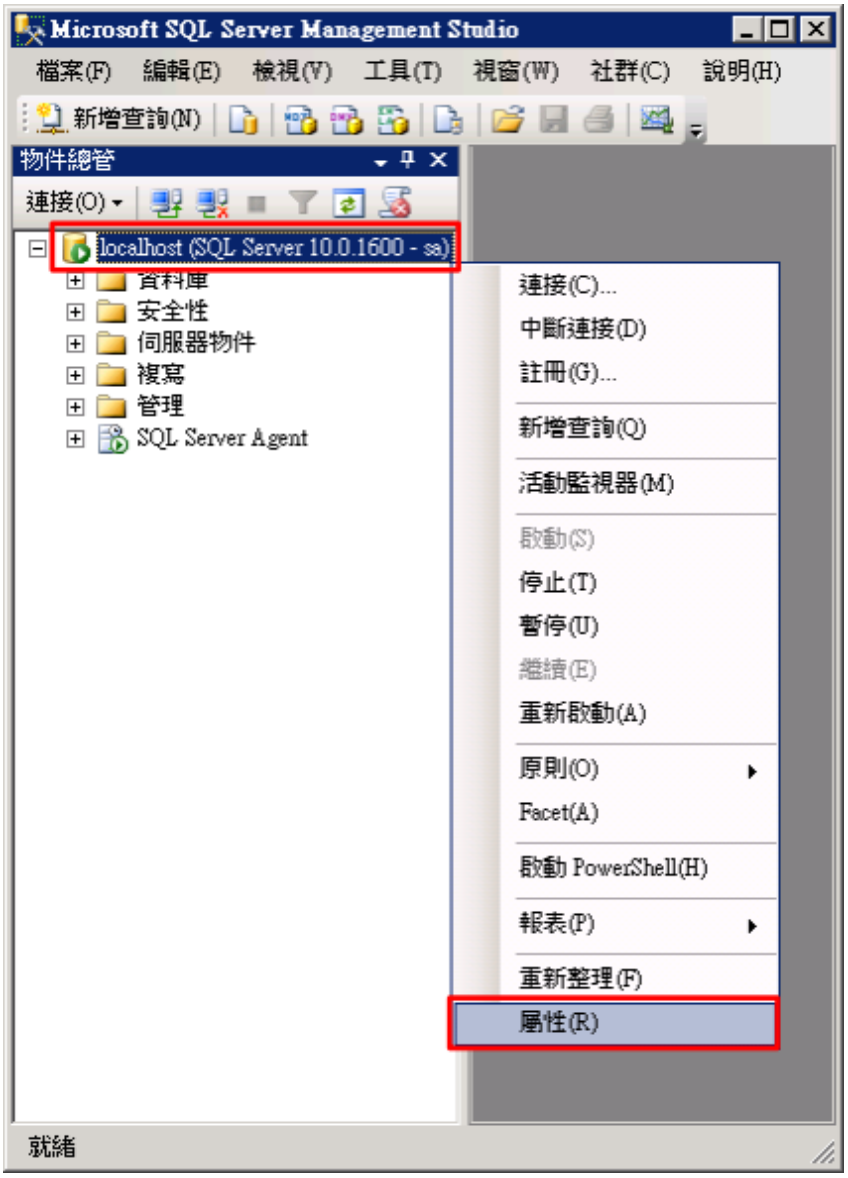
以下分別為圖形介面和指令介面設定方式。

2.1.1 使用圖形介面方式設定

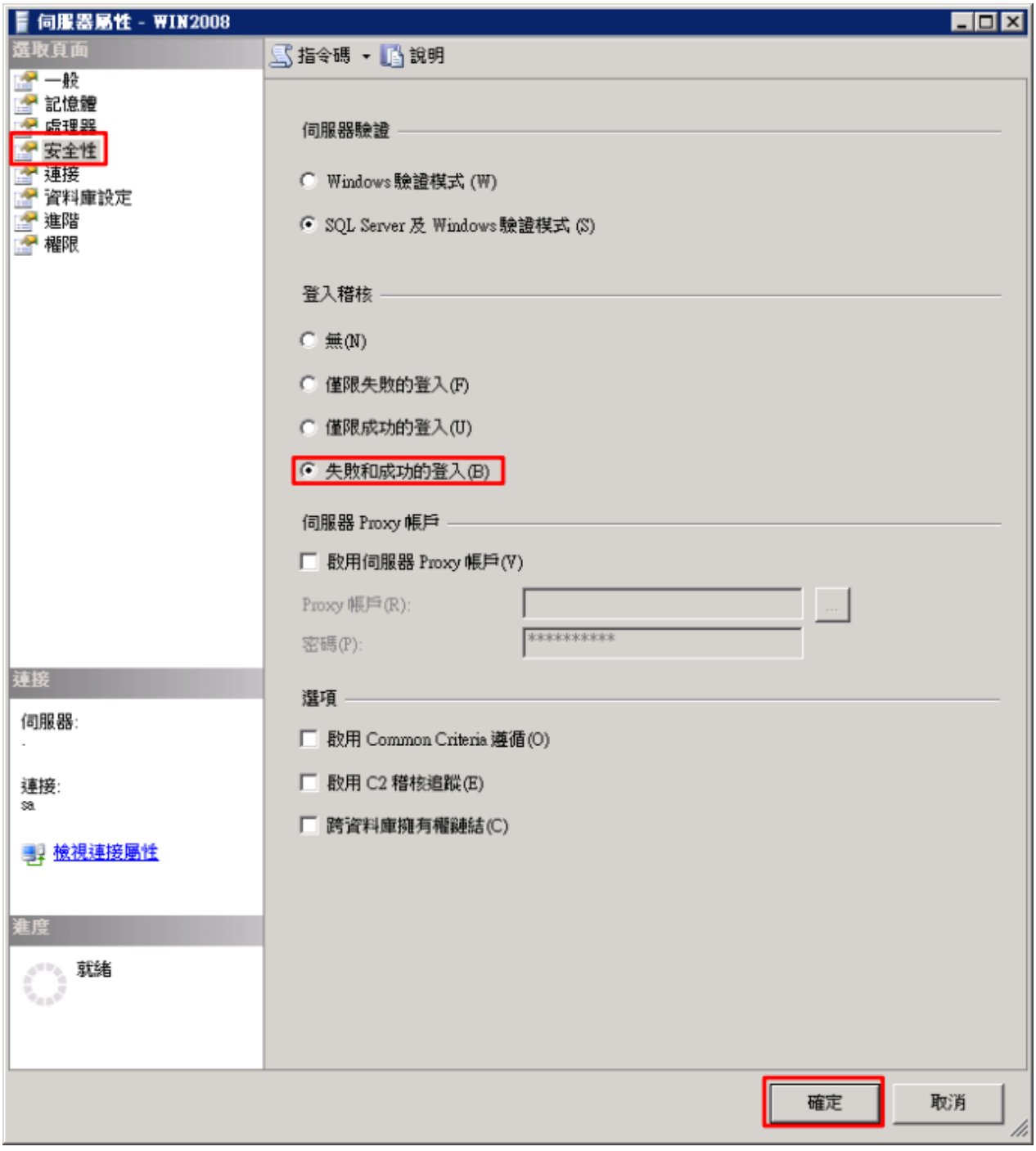
(1) 開啟 [SQL Server Management Studio]

(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

(3)　在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

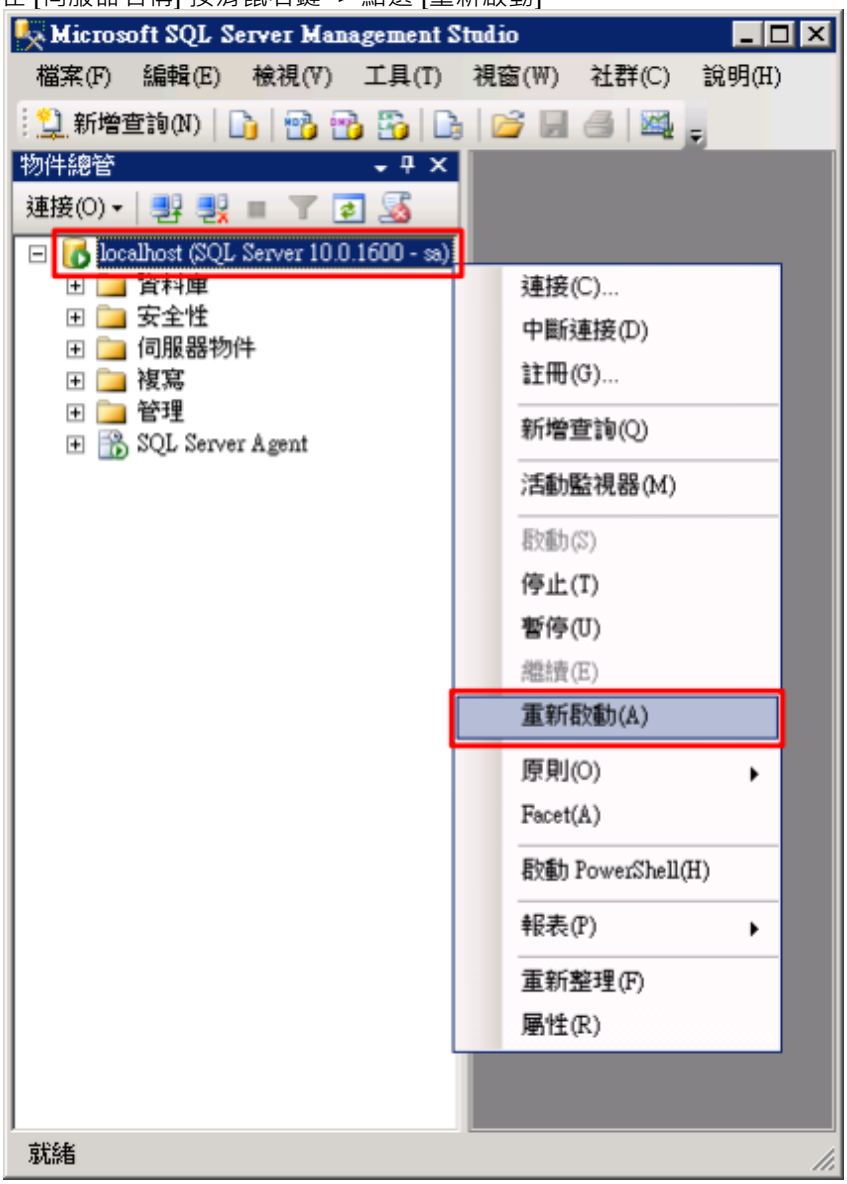


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

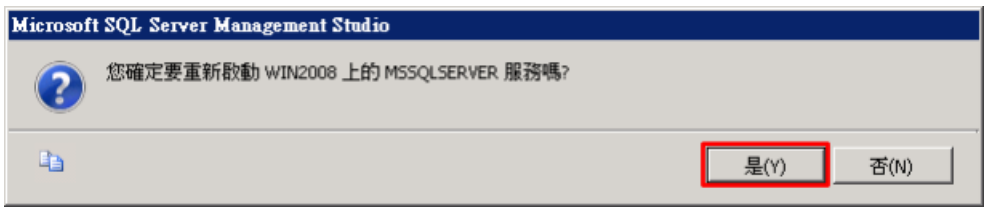


(5) 重新啟動 MS SQL SERVER 服務

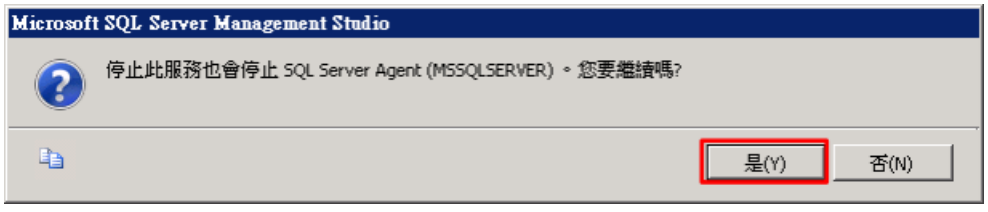
在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務



(7) 按 [是] 停止 SQL SERVER Agent 服務



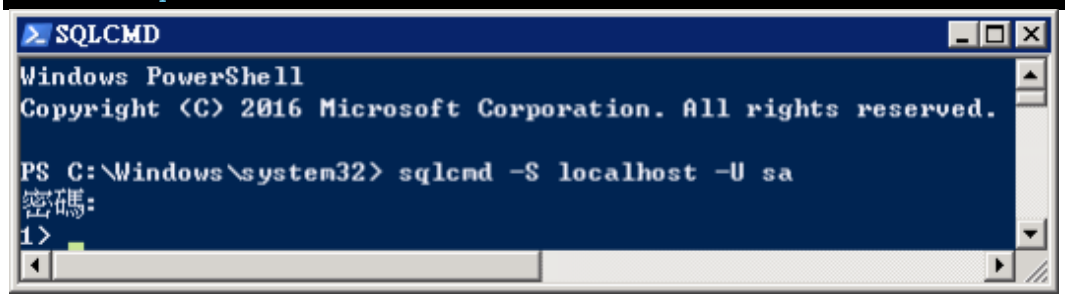
2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

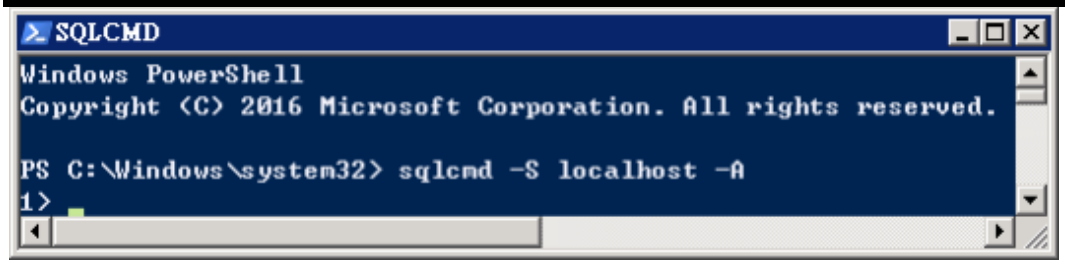
-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

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



(3) 切換資料庫

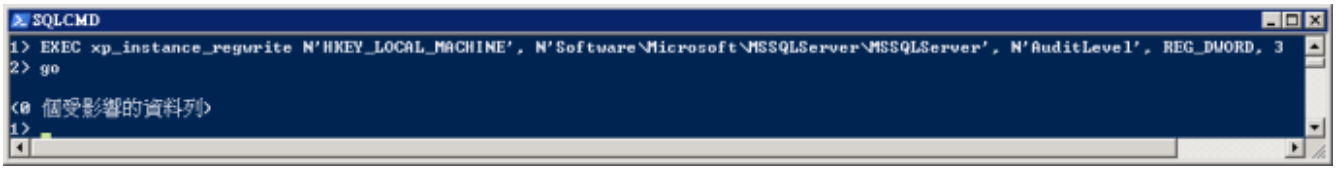
```
1 > use master
2 > go
```

(4) 使用 sp_configure 列出進階選項

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

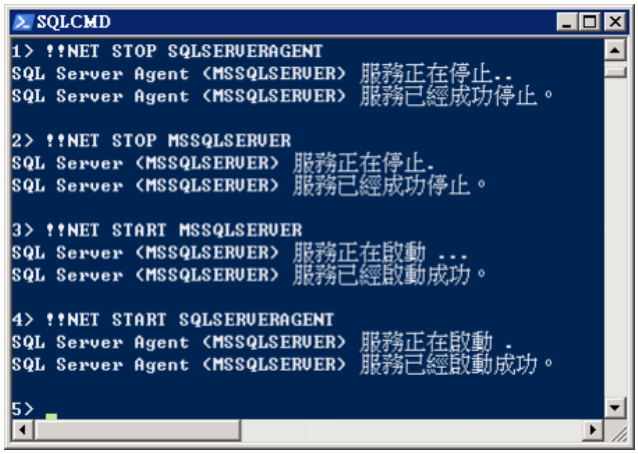
(5) 啟用失敗和成功的登入記錄

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



(6) 重新啟動 MS SQL SERVER 服務

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



2.2 設定稽核

2.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

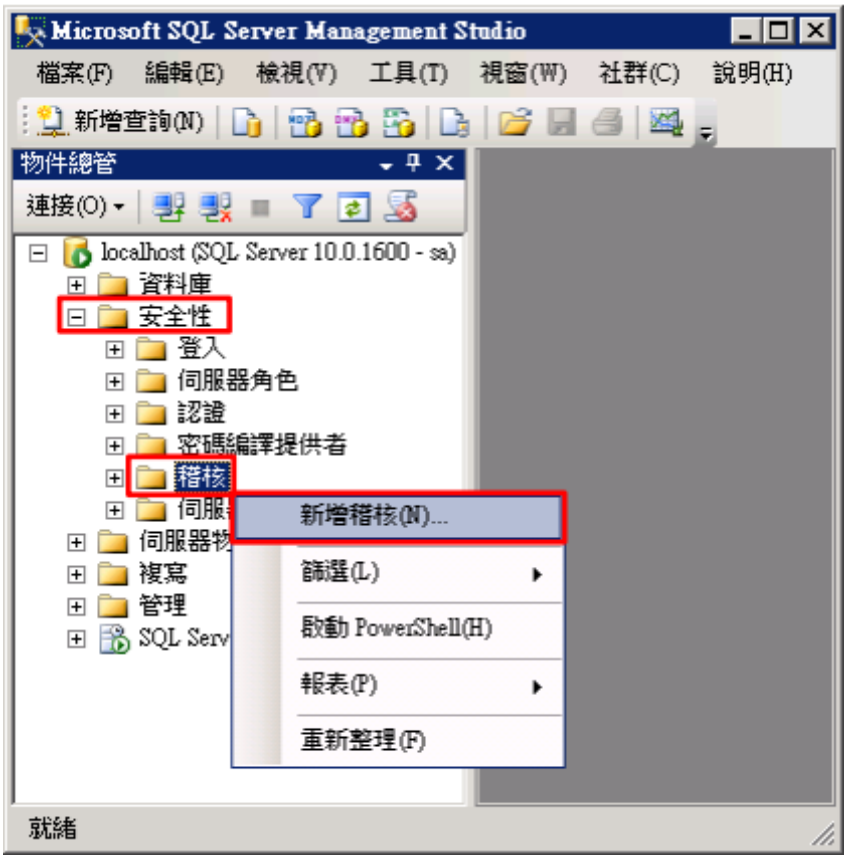
以下分別為圖形介面和指令介面設定方式。

2.2.1.1 使用圖形介面方式設定

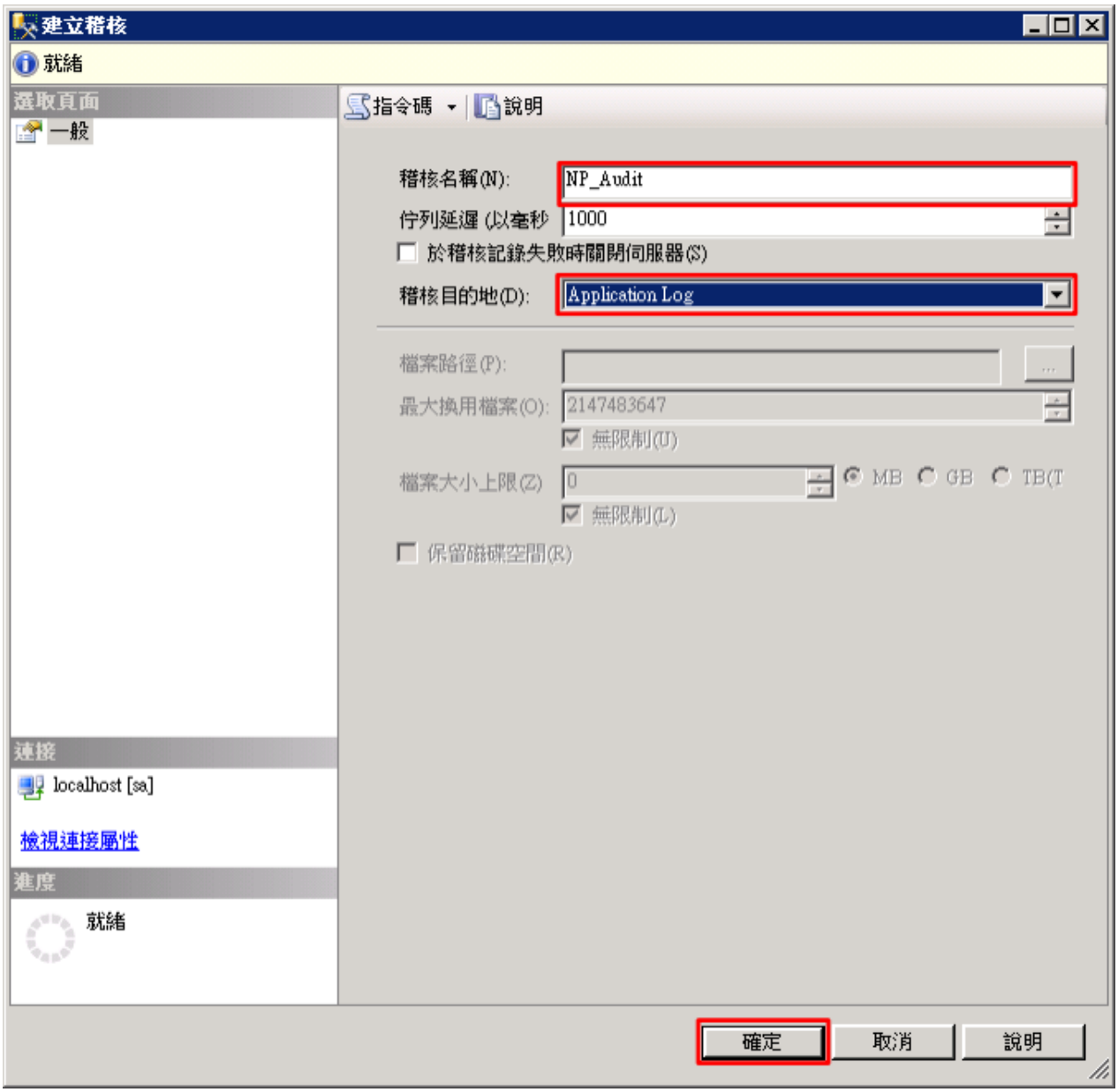
(1) 開啟 [SQL Server Management Studio]

(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

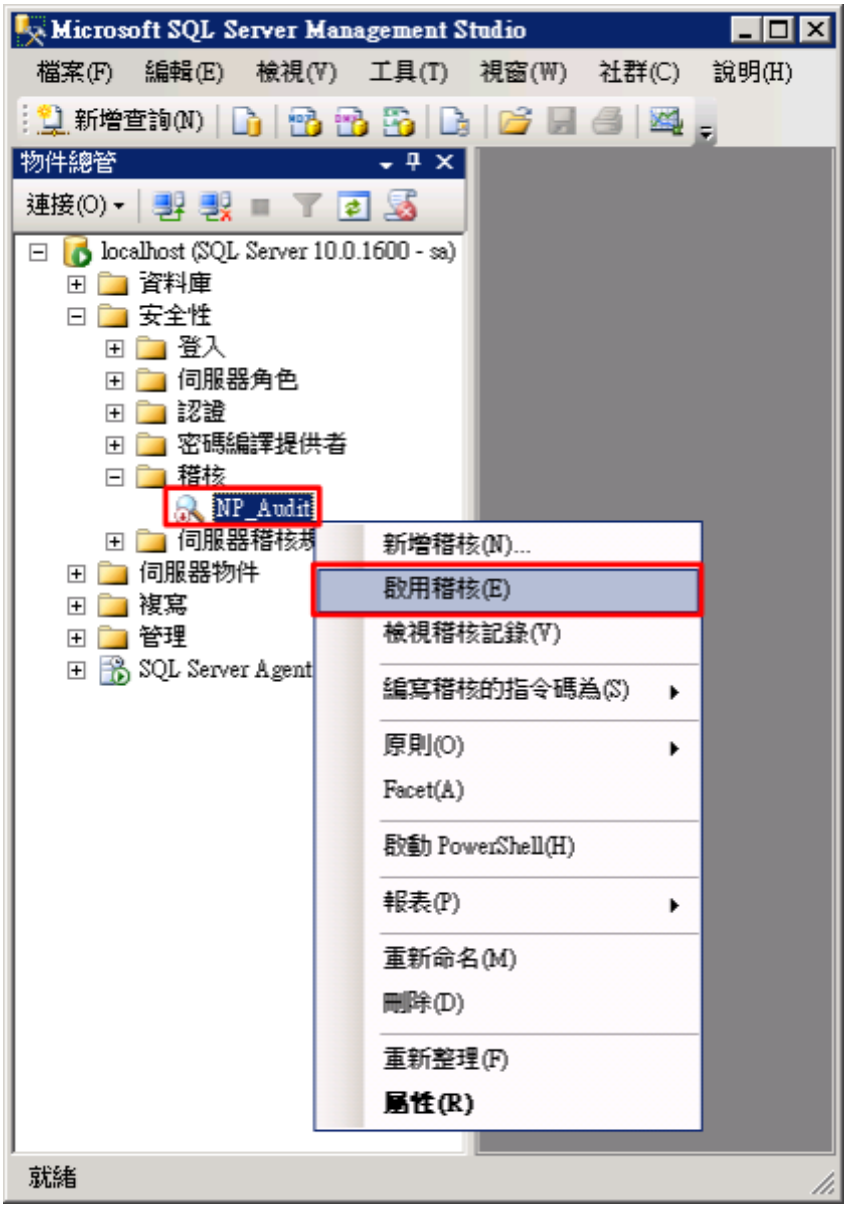
(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



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

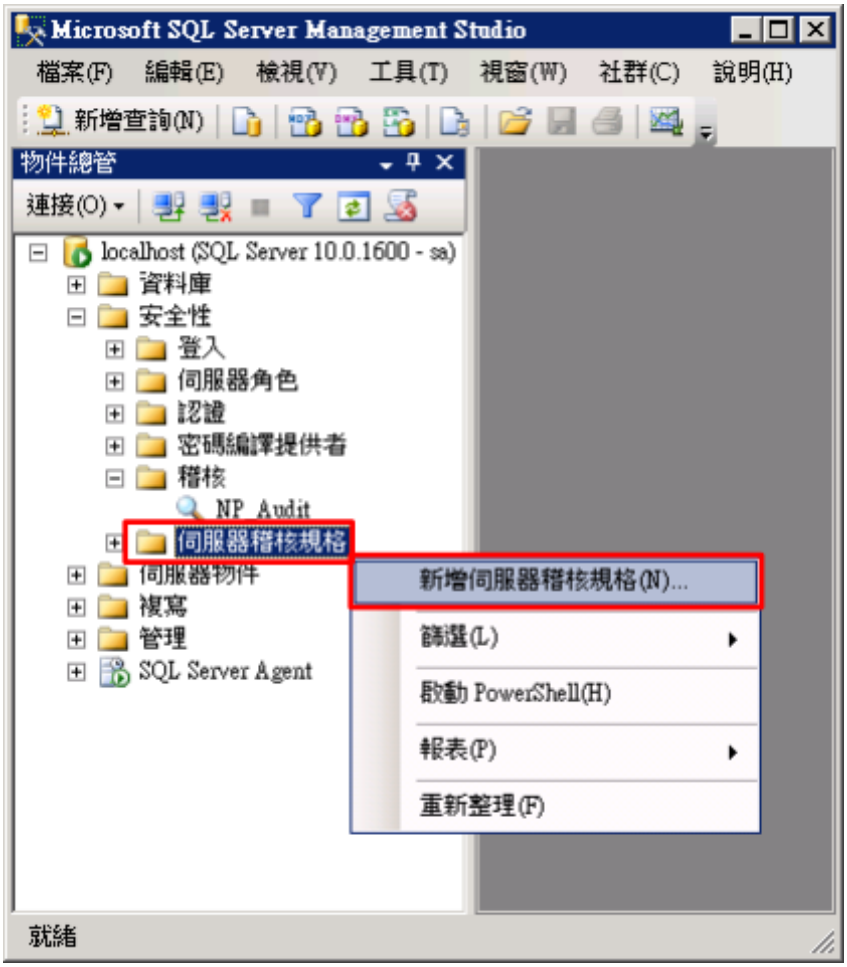


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]

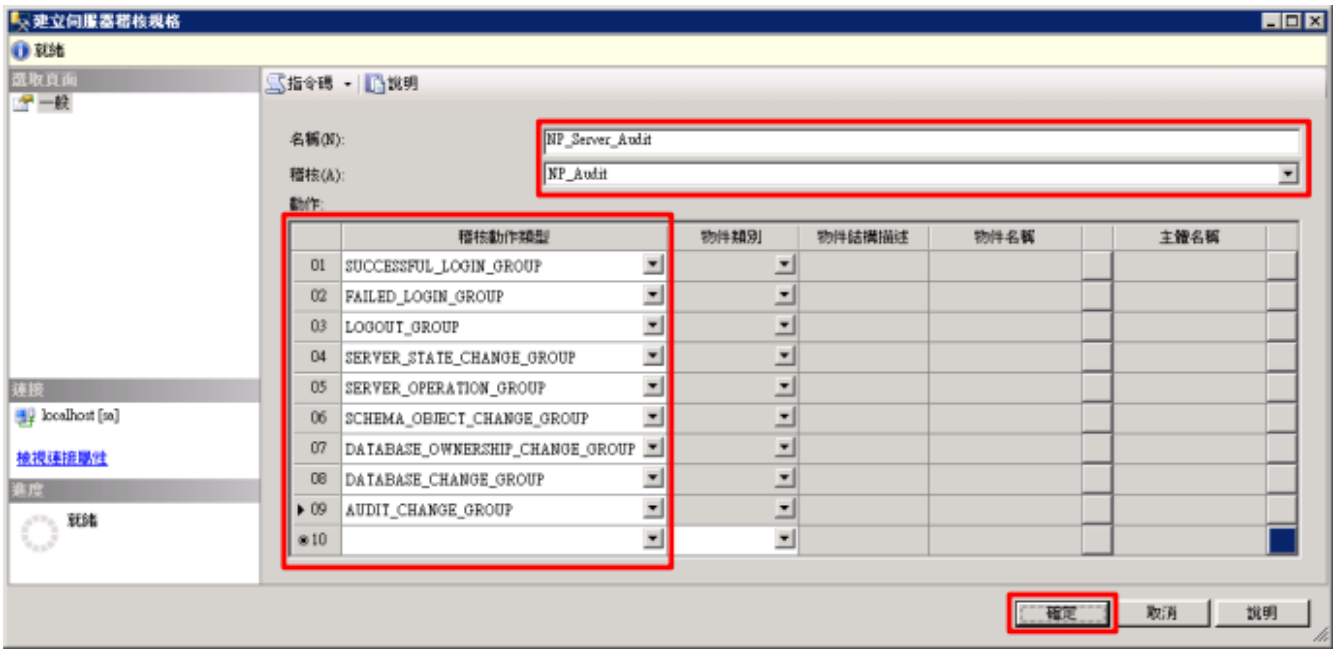


(6)　按 [關閉]

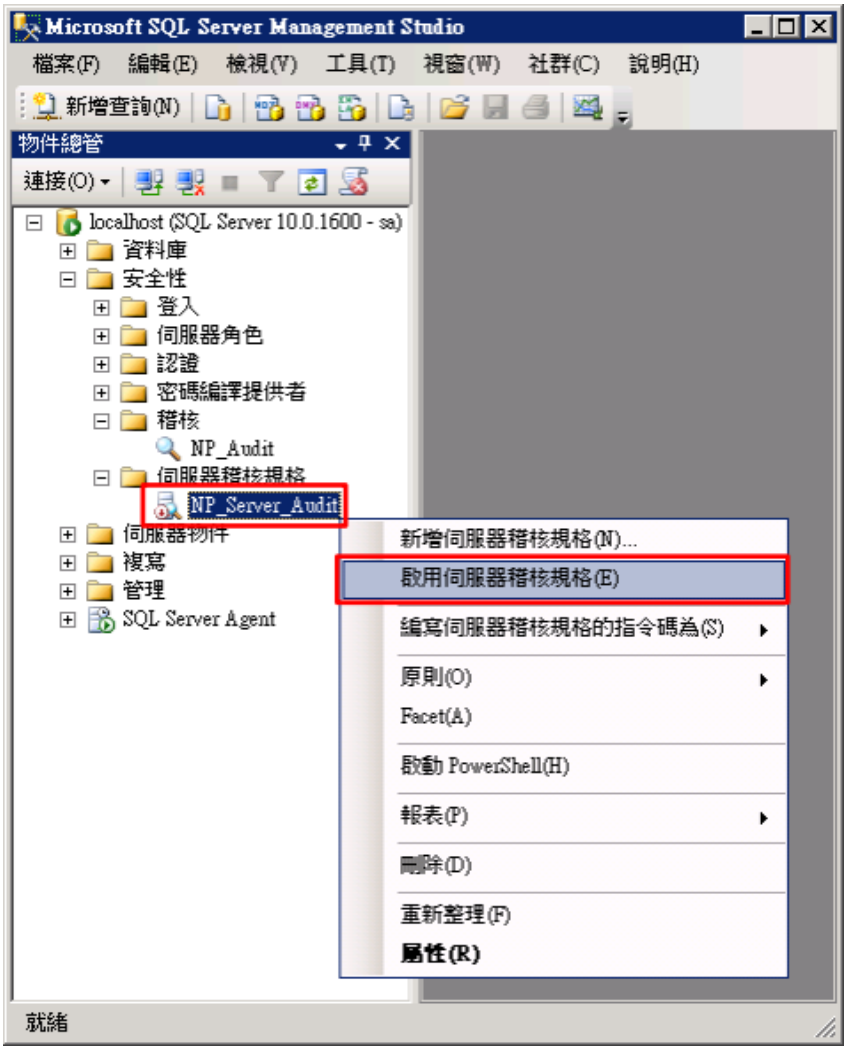
(7) 在 **[伺服器稽核規格]** 按滑鼠右鍵 **->** 點選 **[新增伺服器稽核規格...]**



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



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



(10)　按 [關閉]

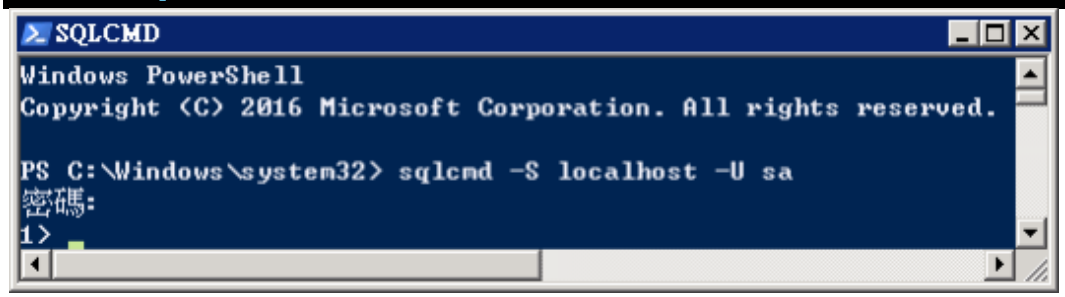
2.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

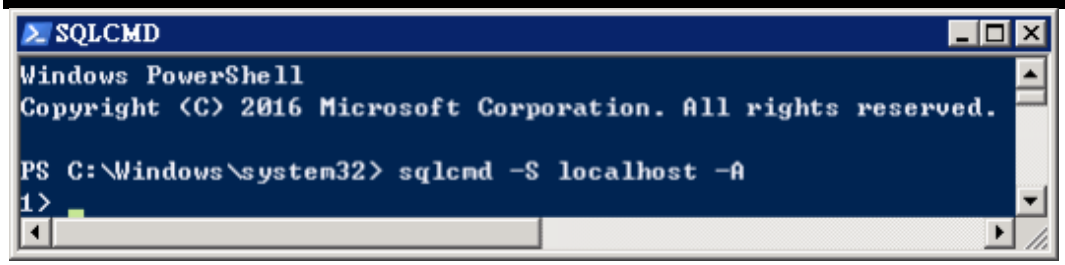
-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

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

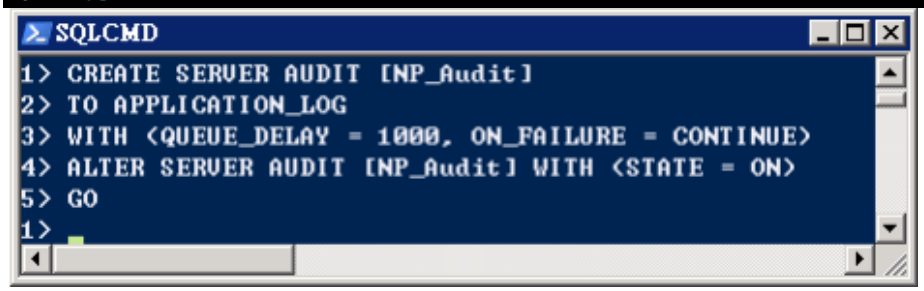


(3) 切換資料庫

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

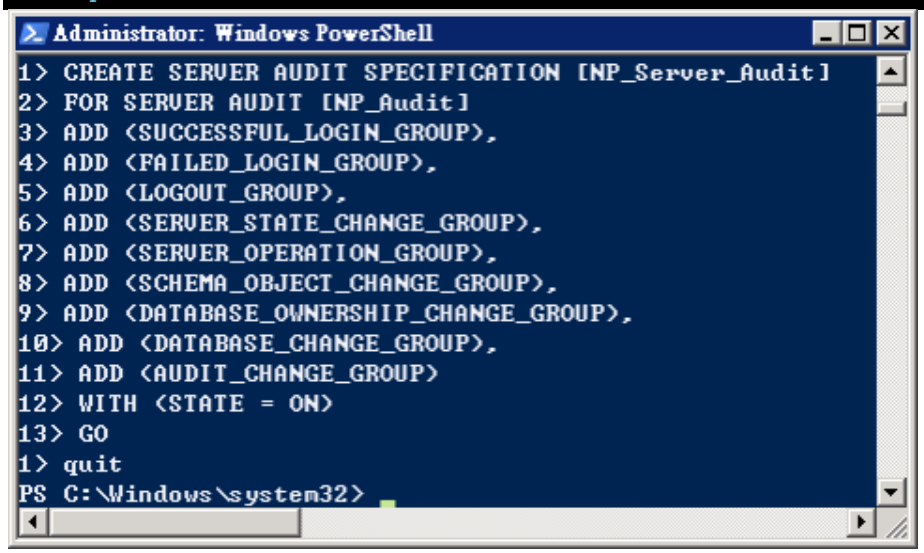
(4) 設定稽核 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄

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



(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
```



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。

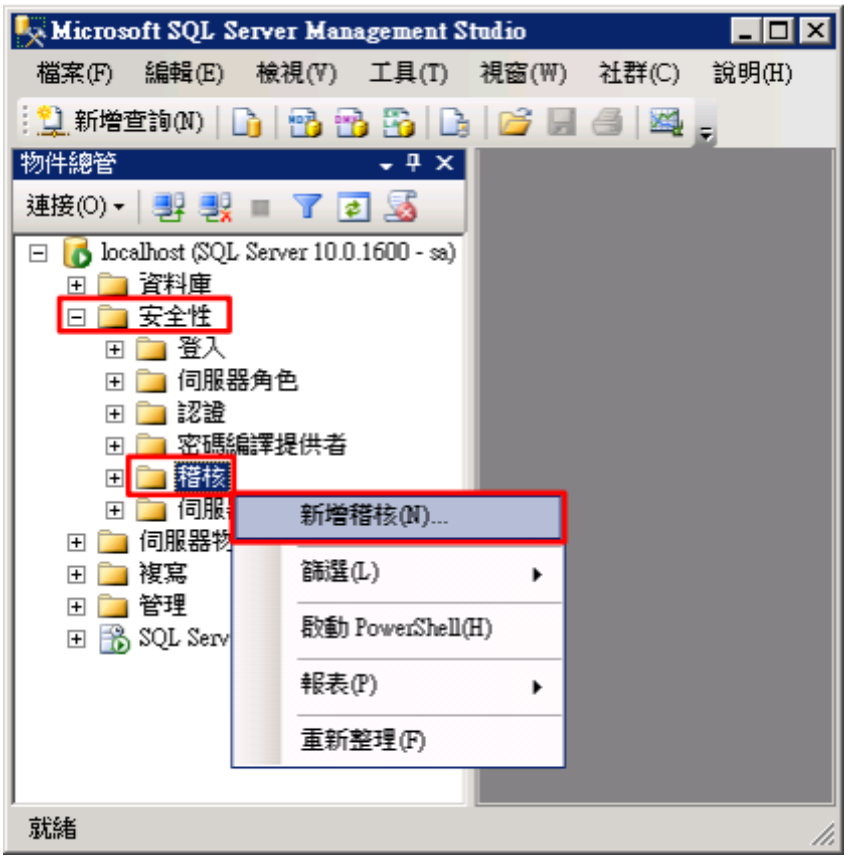
以下分別為圖形介面和指令介面設定方式。

2.2.2.1 使用圖形介面方式設定

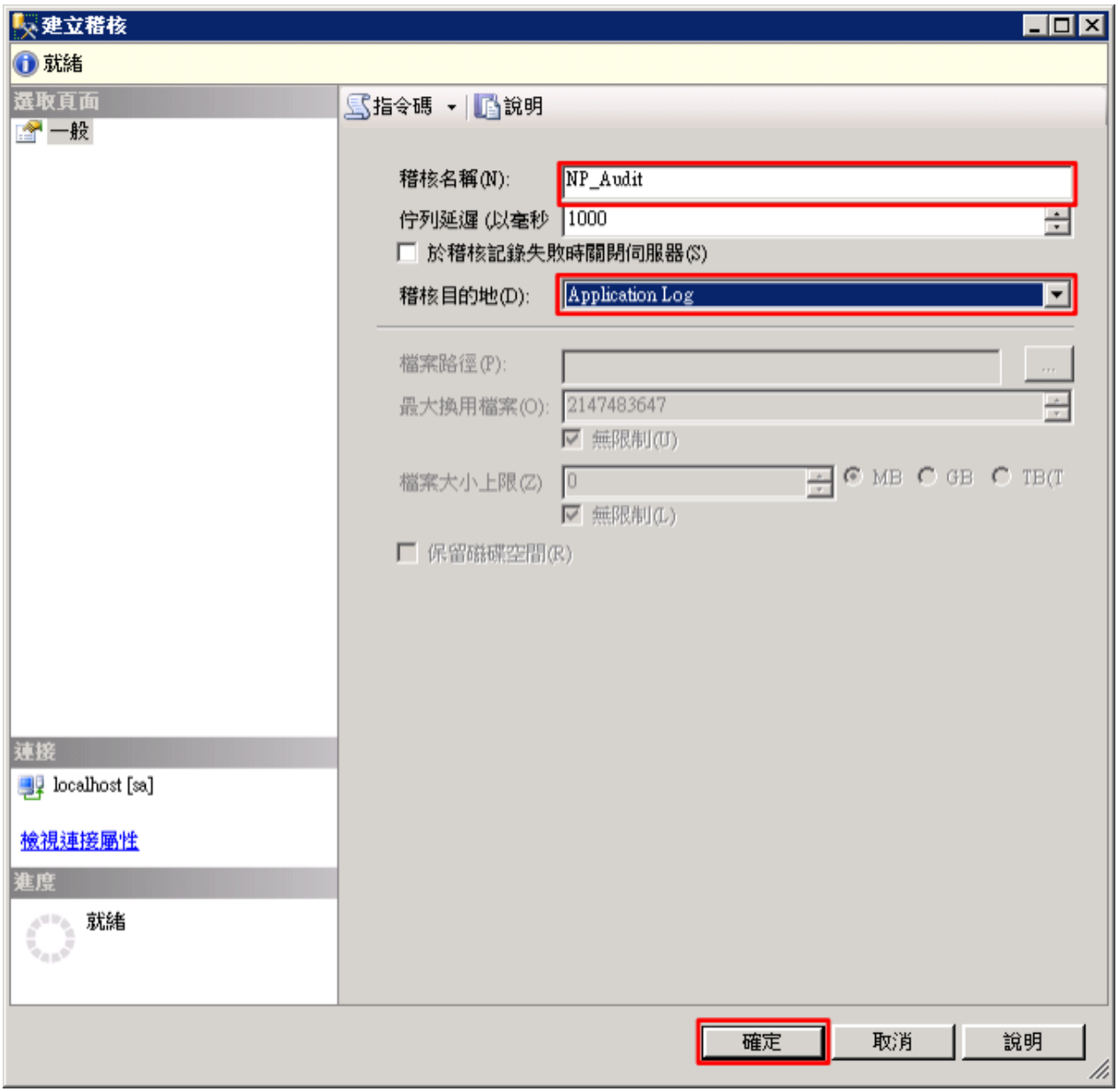
(1) 開啟 [SQL Server Management Studio]

(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

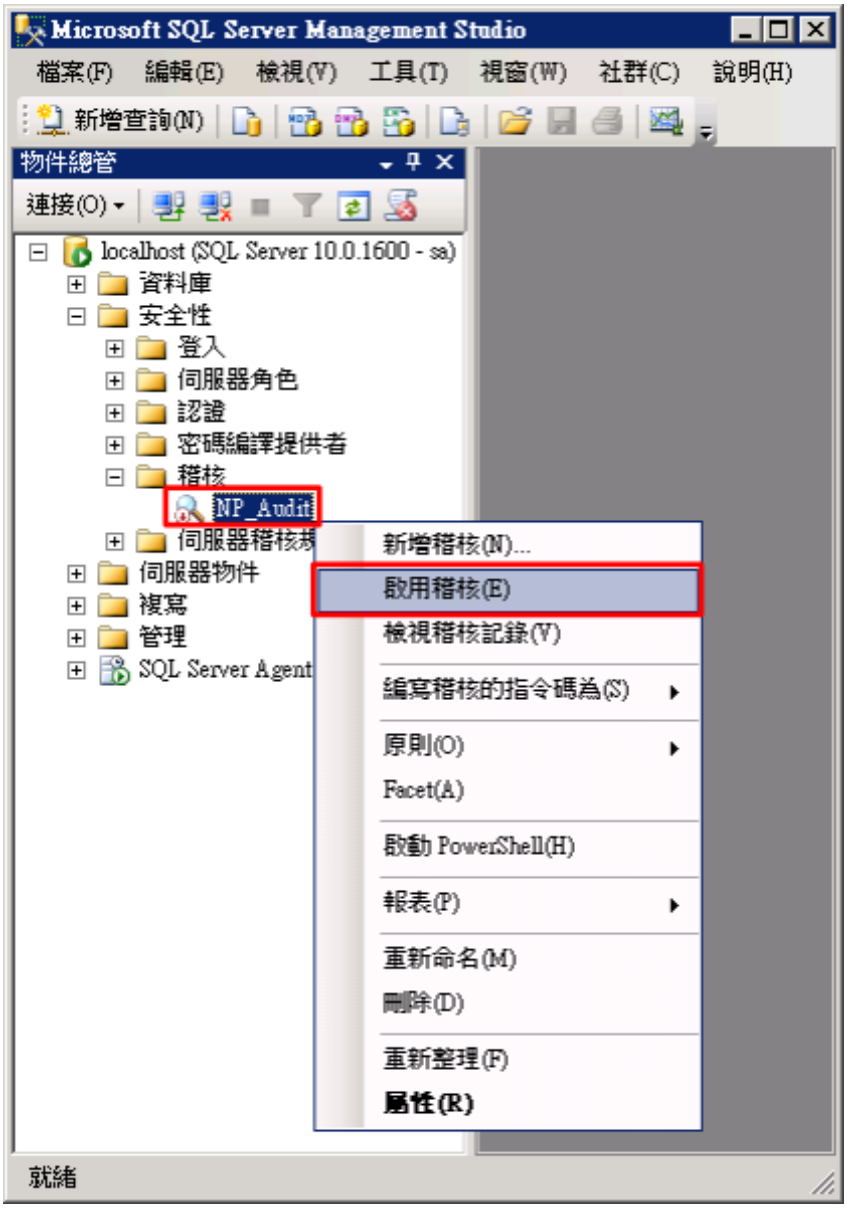
(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



(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]**

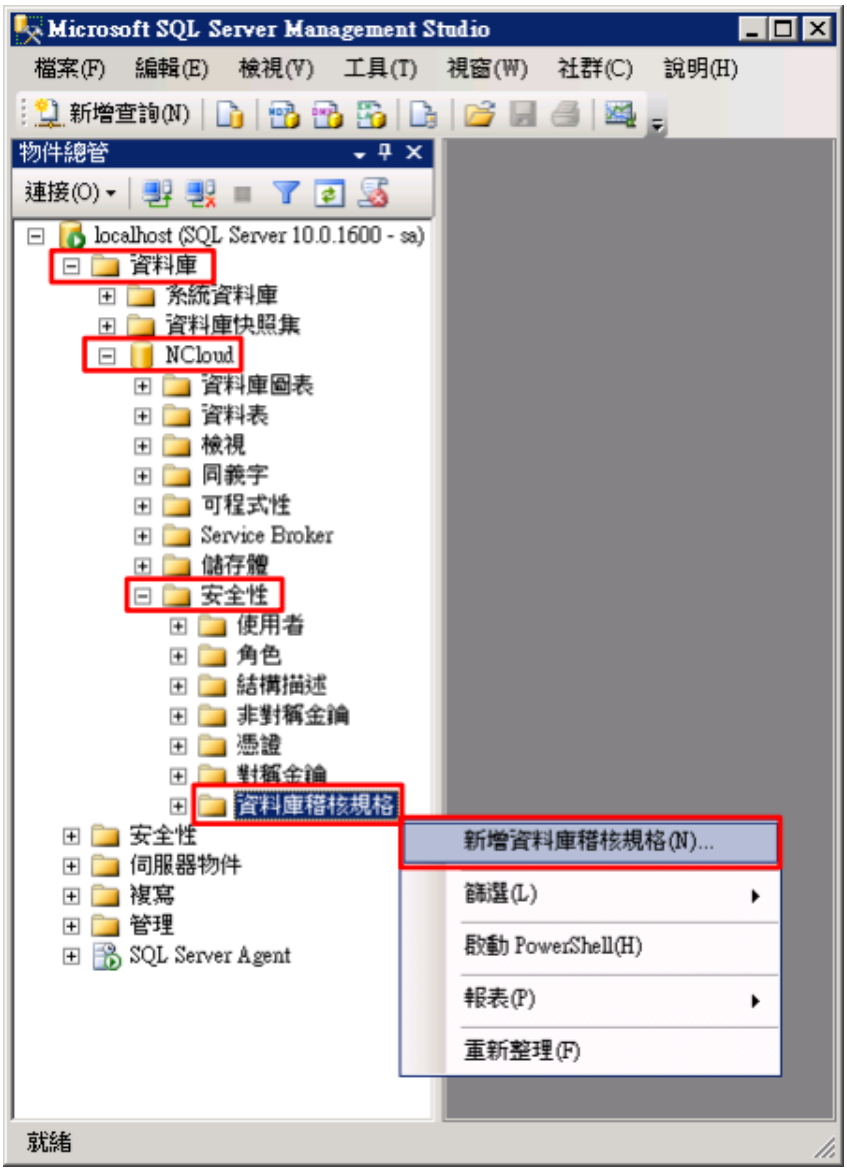


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]

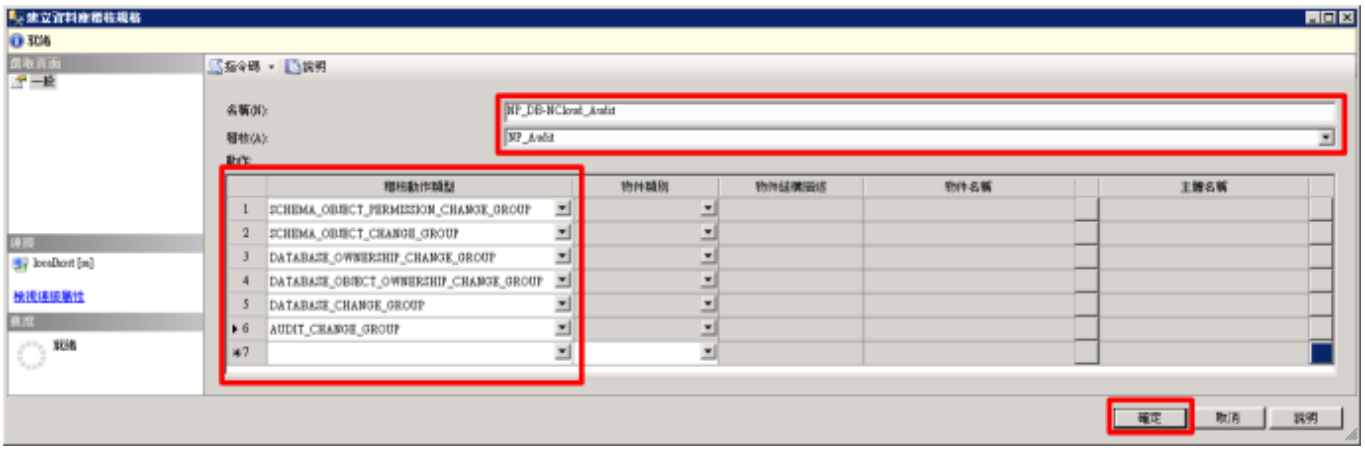


(6)　按 [關閉]

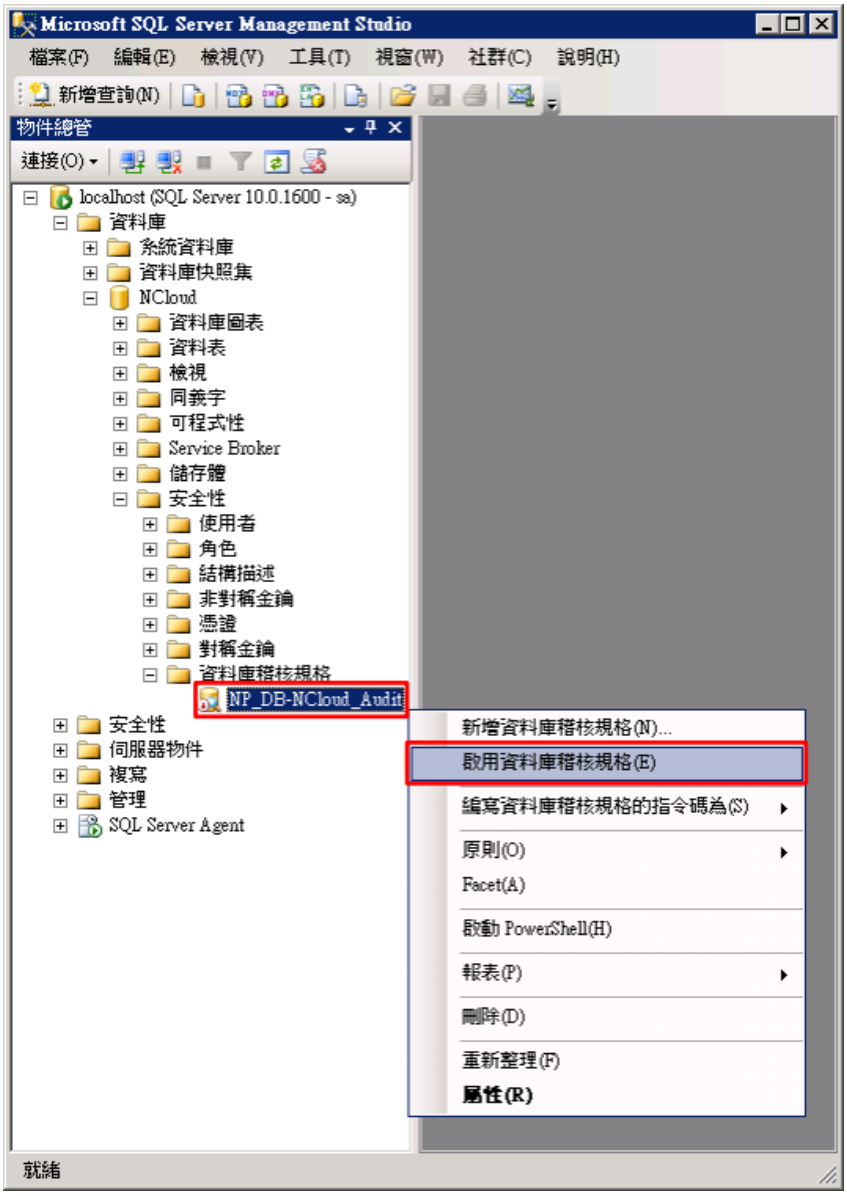
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



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



(9)　在資料庫稽核規格名稱: [NP_DB-NCloud_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10)　按 [關閉]

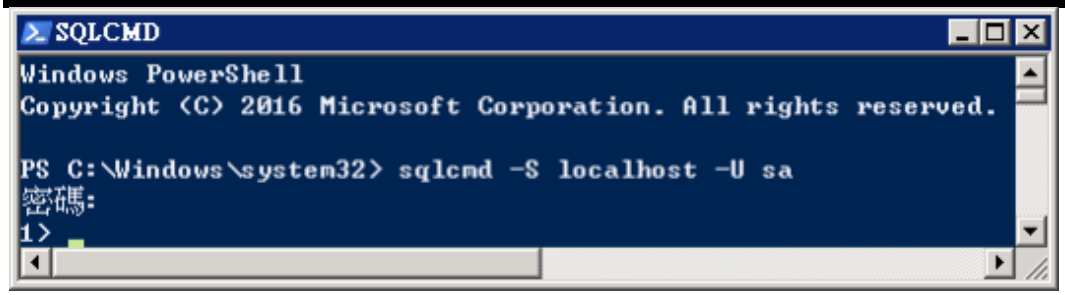
2.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

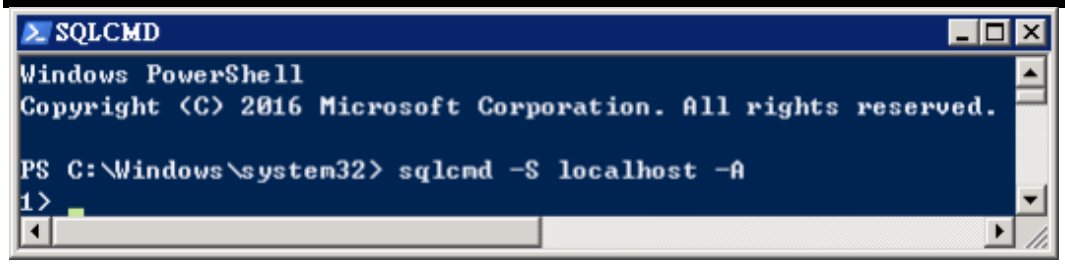
-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

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

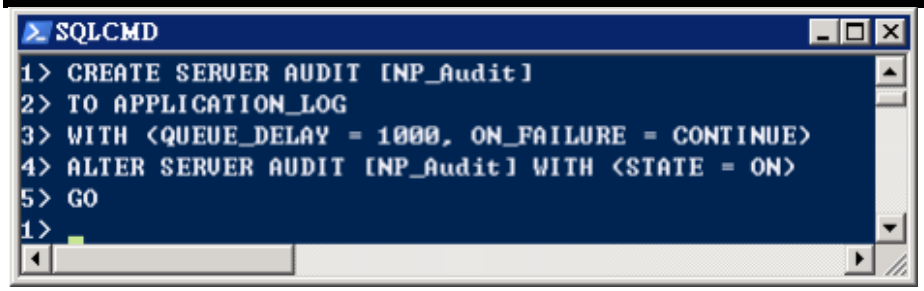


(3) 切換資料庫

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

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

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



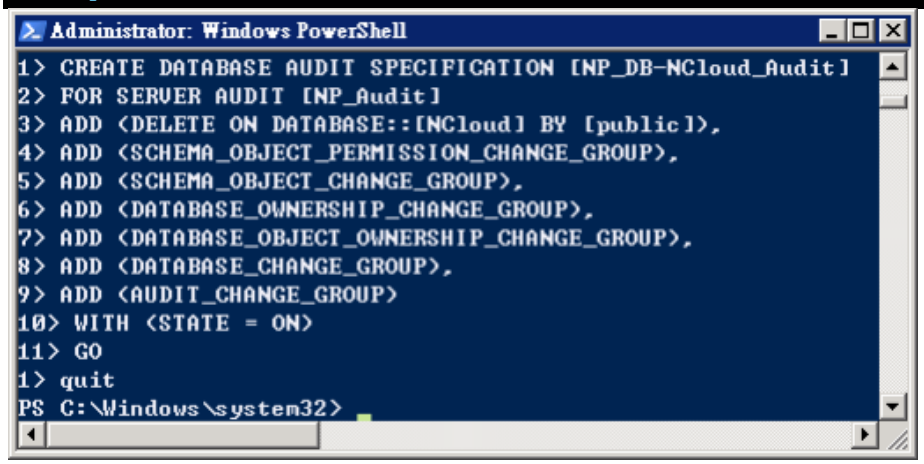
紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例： NCloud

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

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

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



紅色文字部位請輸入資料庫稽核規格名稱

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

紅色文字部位請輸入稽核資料庫名稱

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

2.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

2.3.1 網域

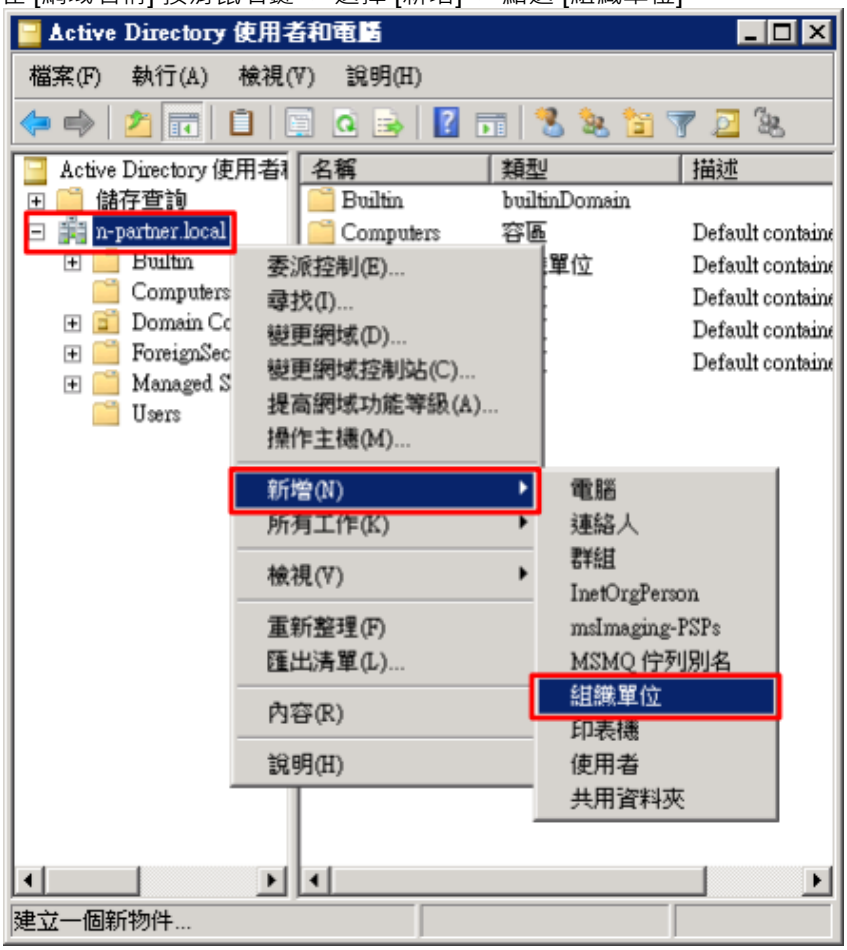
2.3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]

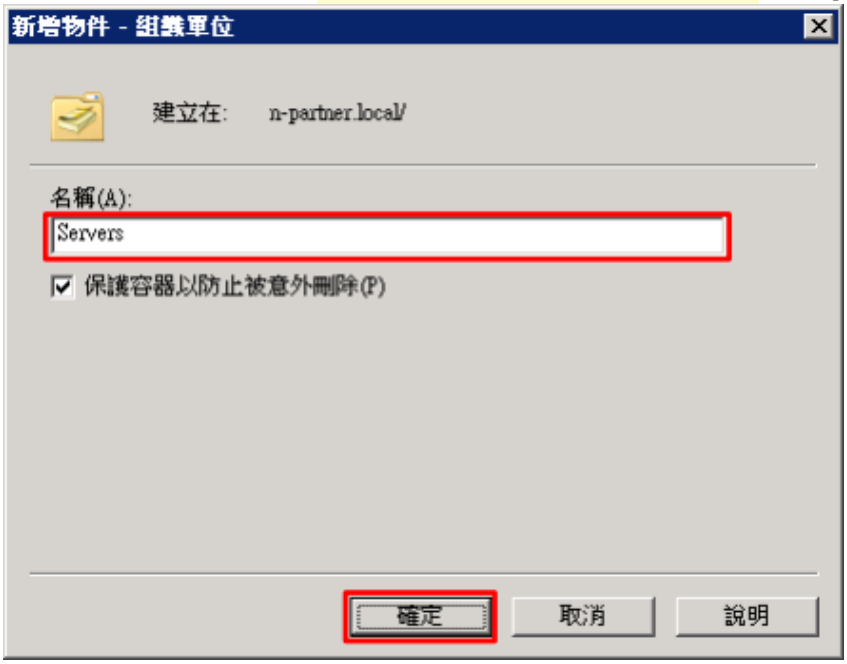
(2) 新增組織單位

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



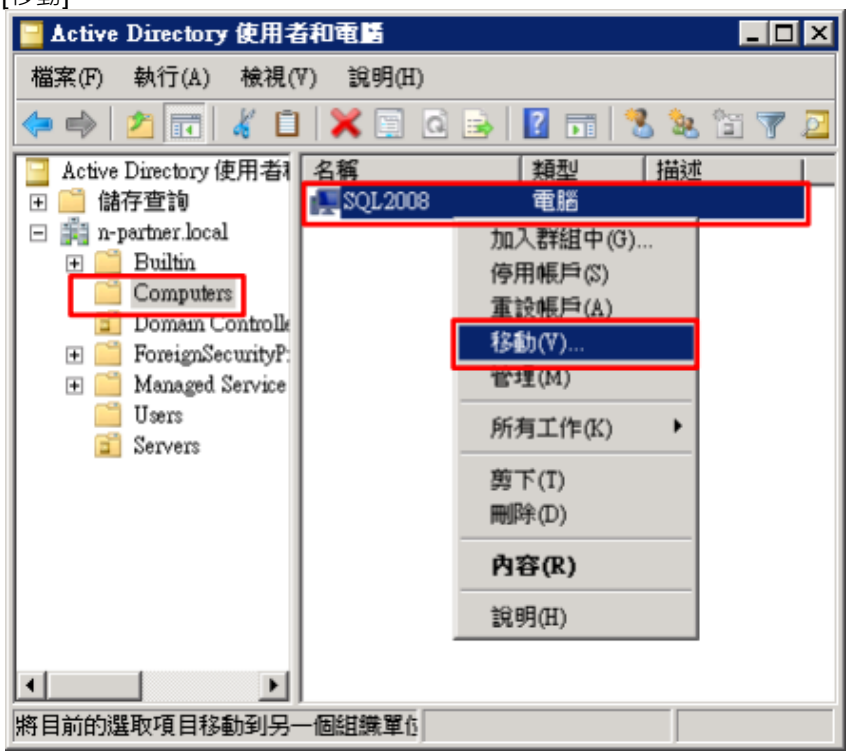
(3) 輸入組織單位名稱

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



(4) 移動伺服器至新的組織單位

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

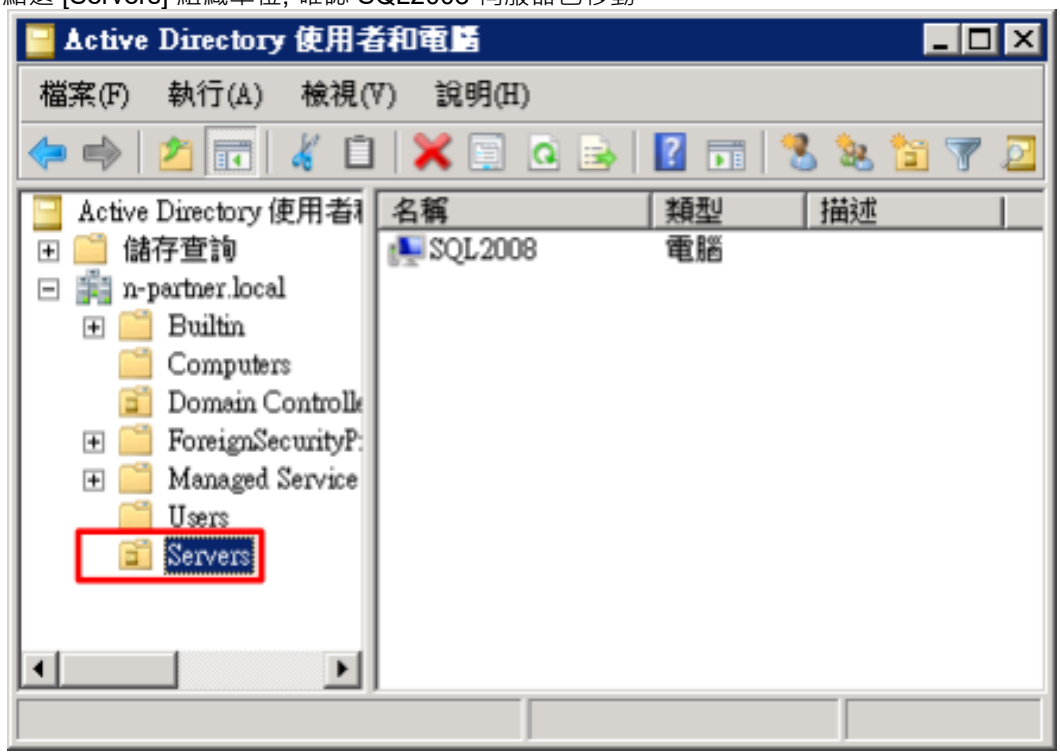


(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位, 確認 SQL2008 伺服器已移動。



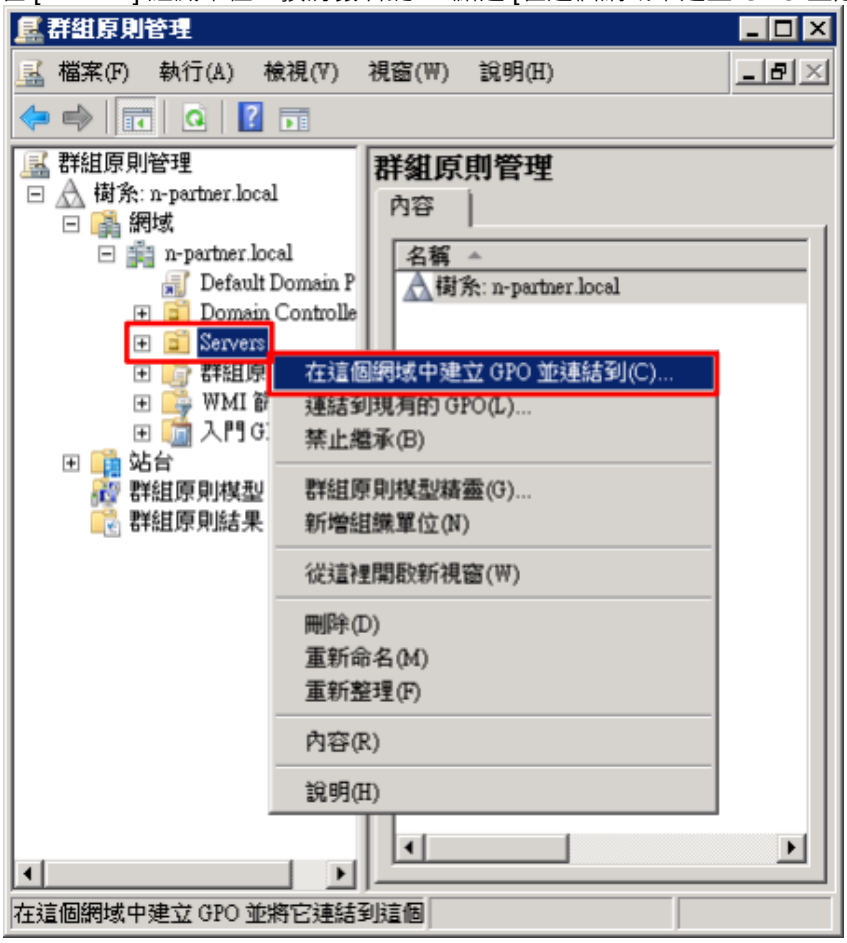
2.3.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]

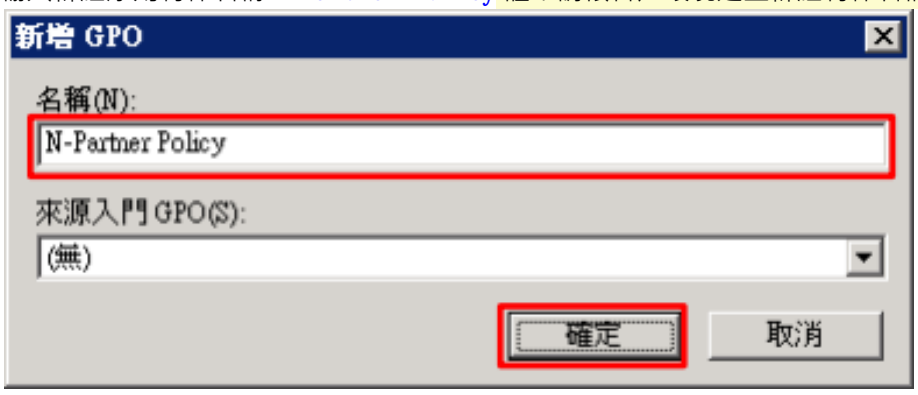
(2) 在 Servers 組織單位，新增群組原則物件

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



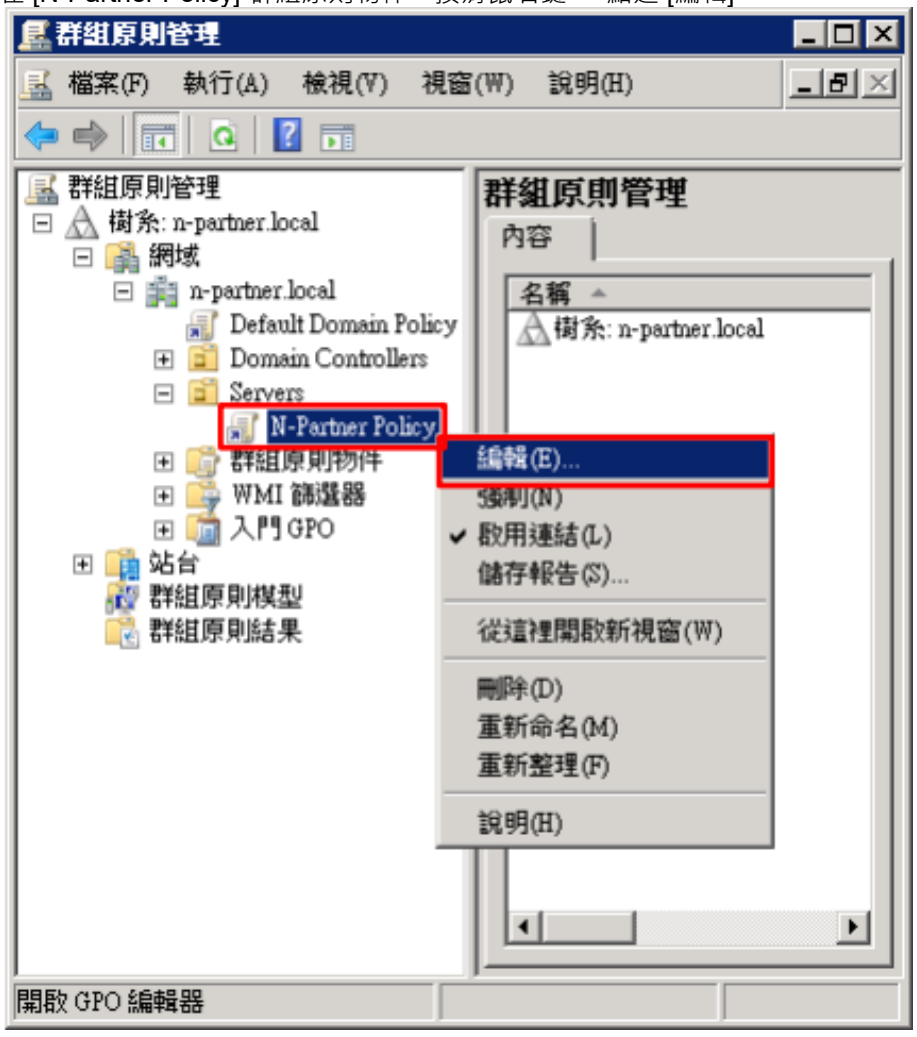
(3) 輸入群組原則物件名稱

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



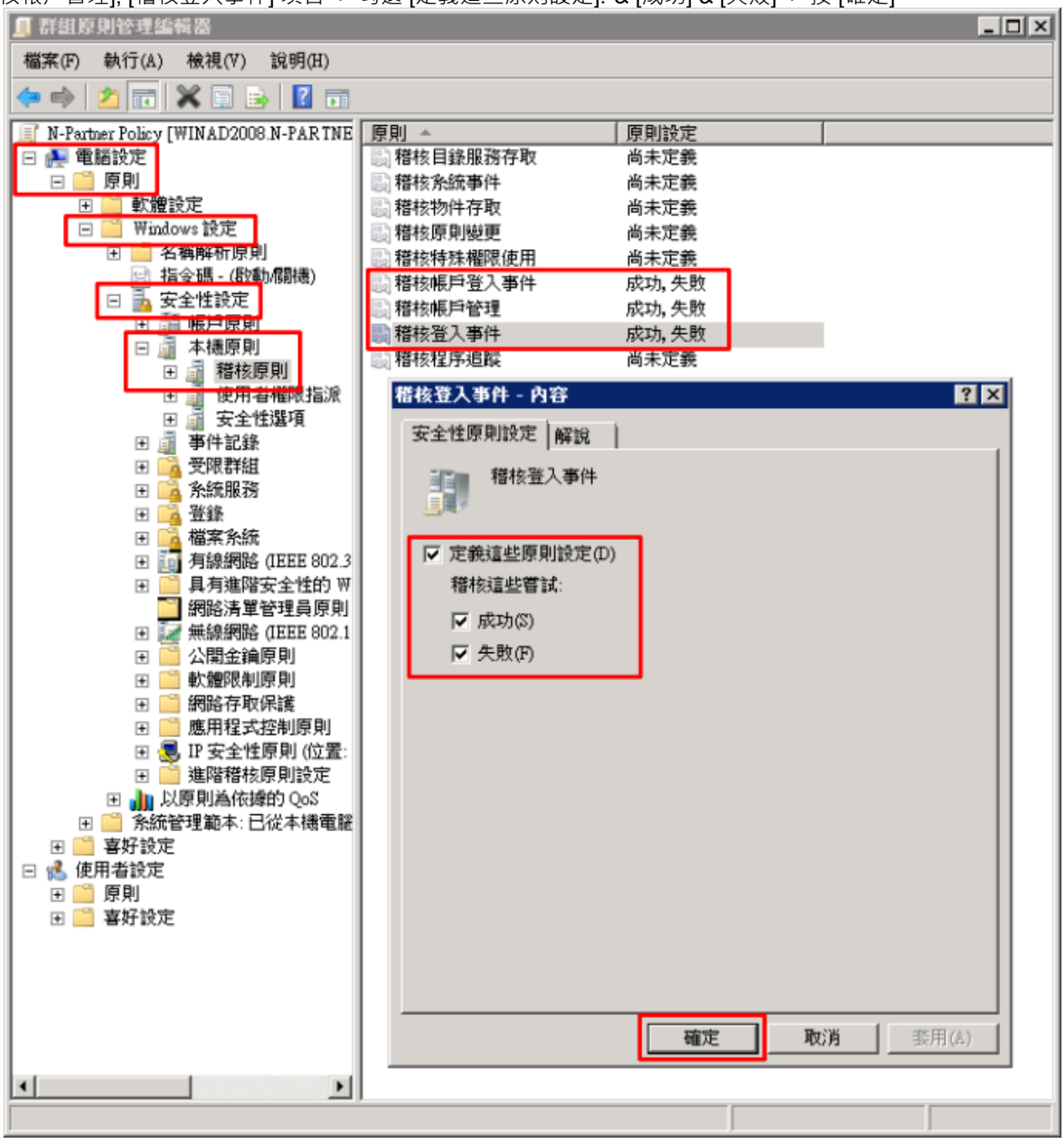
(4) 編輯群組原則物件

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



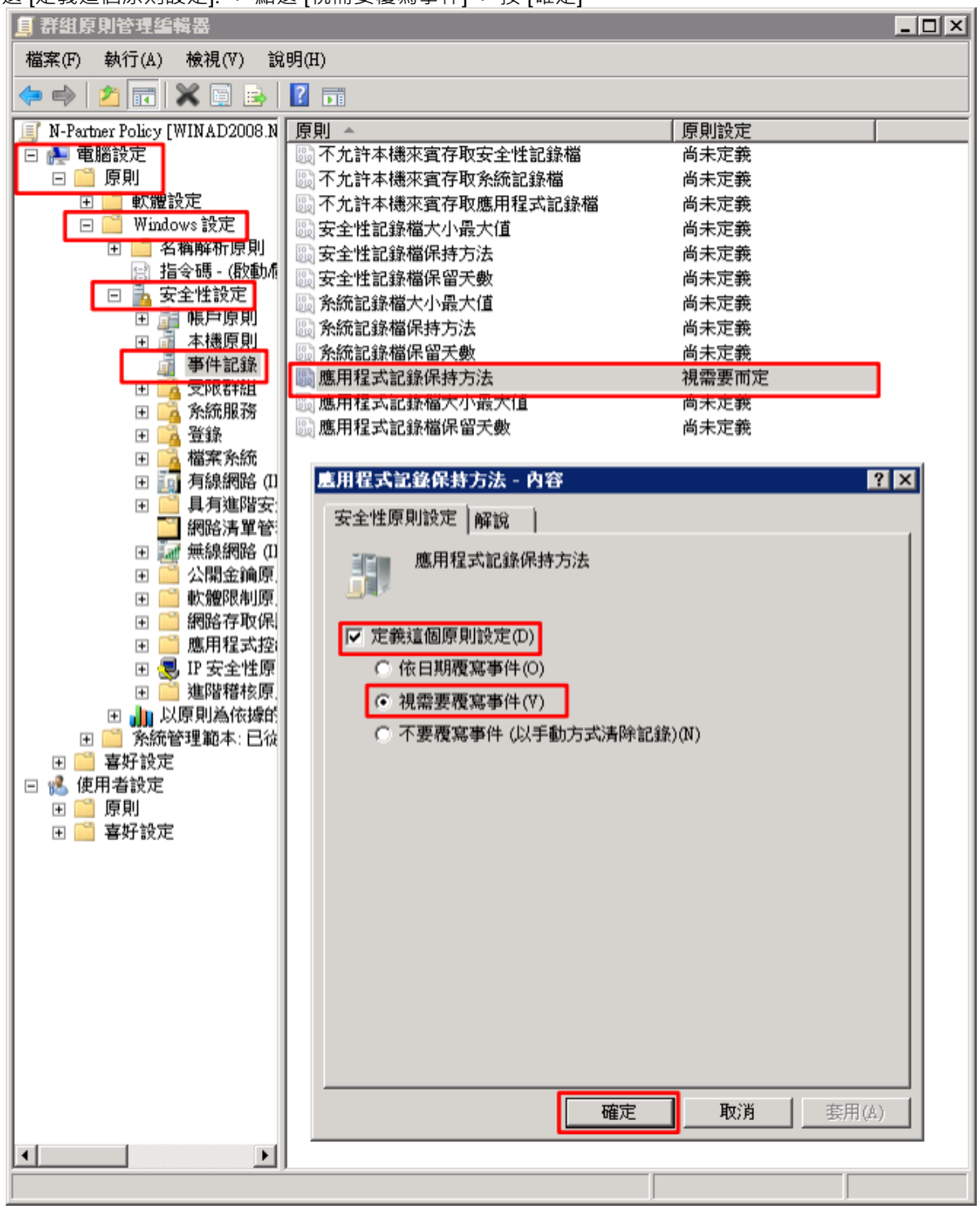
(5) 本機原則：稽核原則

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



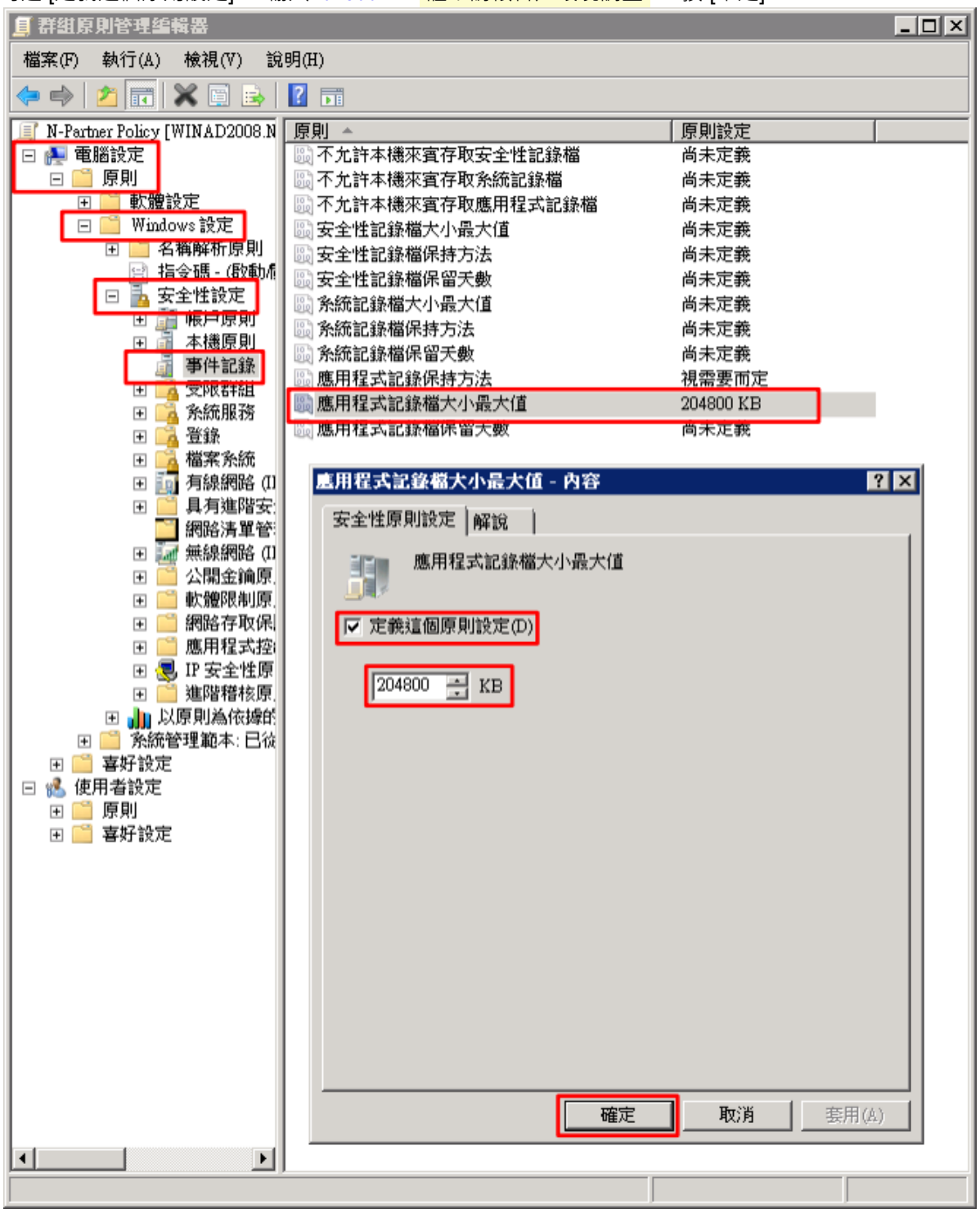
(6) 事件記錄：應用程式記錄保持方法

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



(7) 事件記錄：應用程式記錄檔大小最大值

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



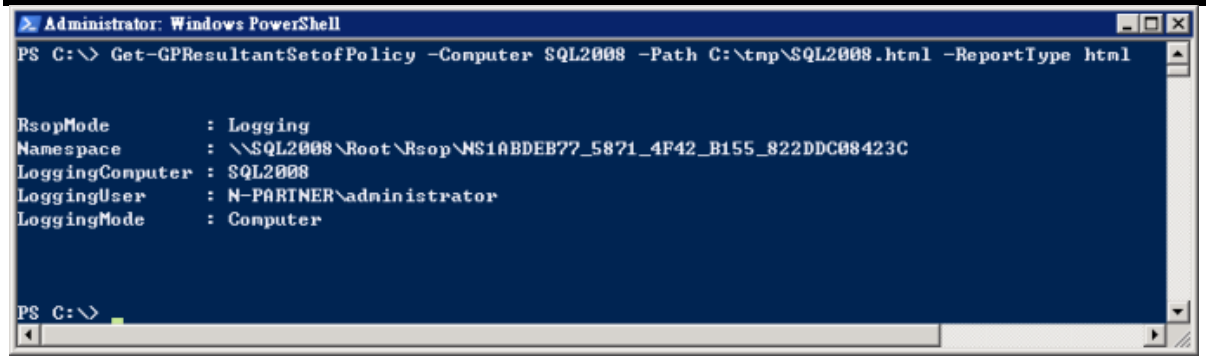
(8)　在 MS SQL Server 伺服器 -> 開啟 [Windows PowerShell]

(9)　更新群組原則

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

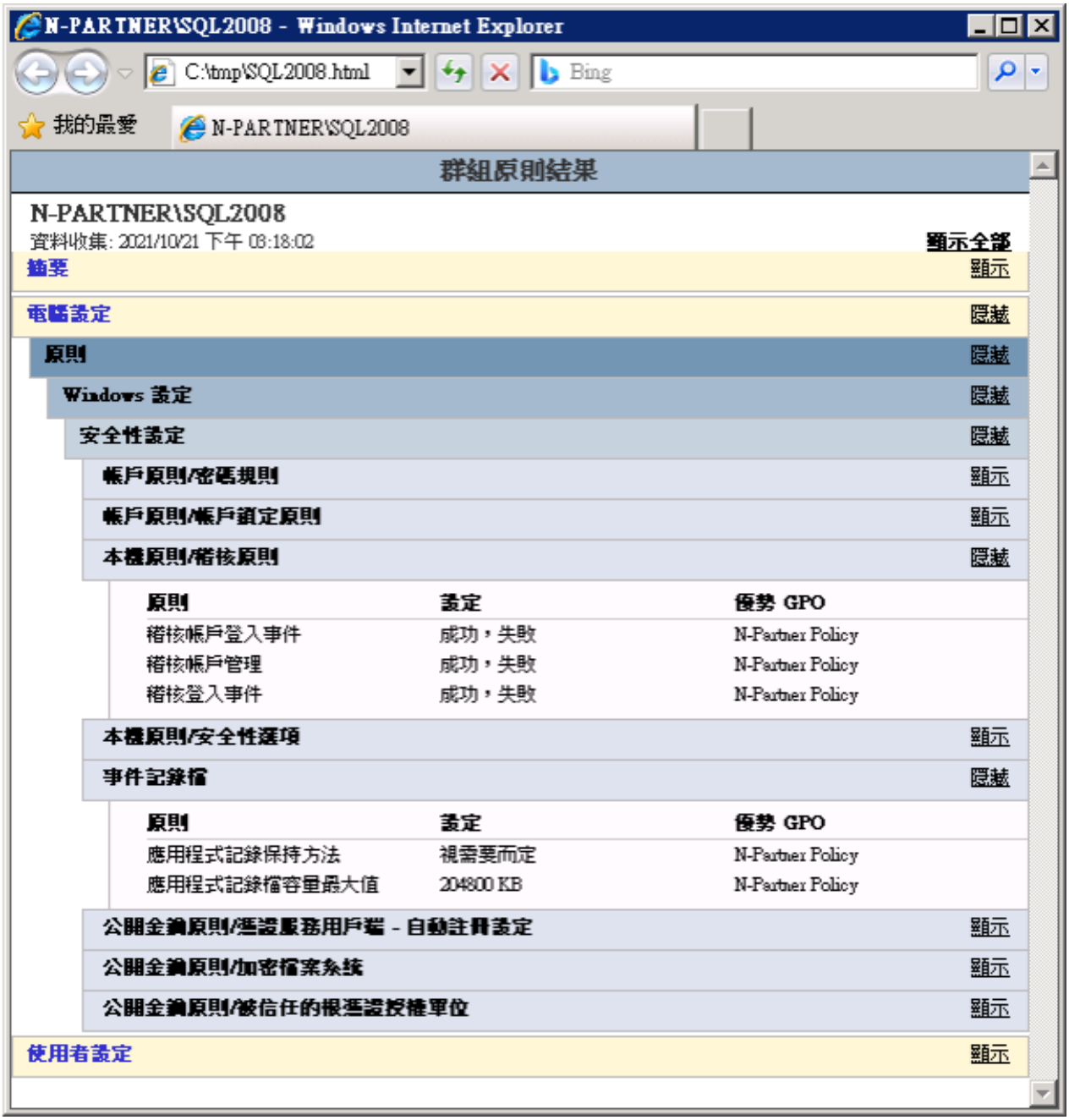
(10)　在 AD 網域伺服器 -> 產生 MS SQL Server 伺服器群組原則報表

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

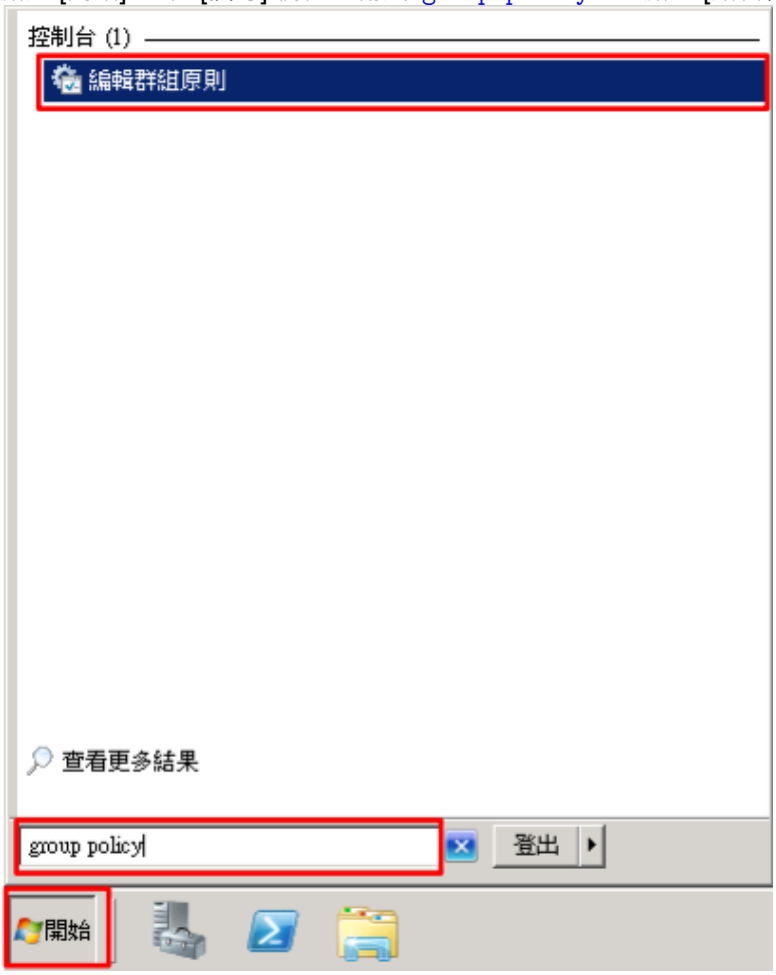


2.3.2 工作群組

2.3.2.1 稽核原則設定

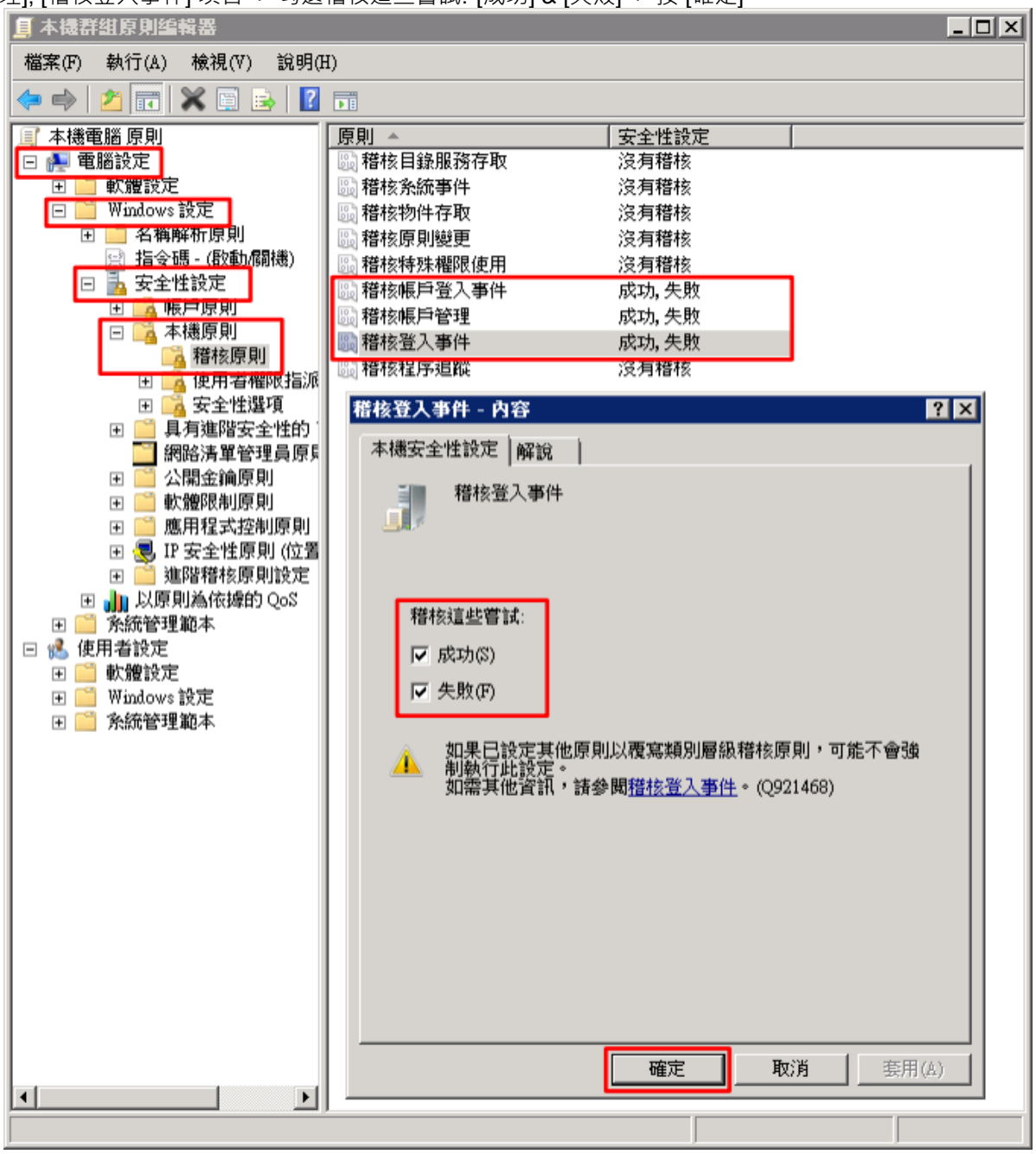
(1) 開啟 [本機群組原則編輯器]

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]



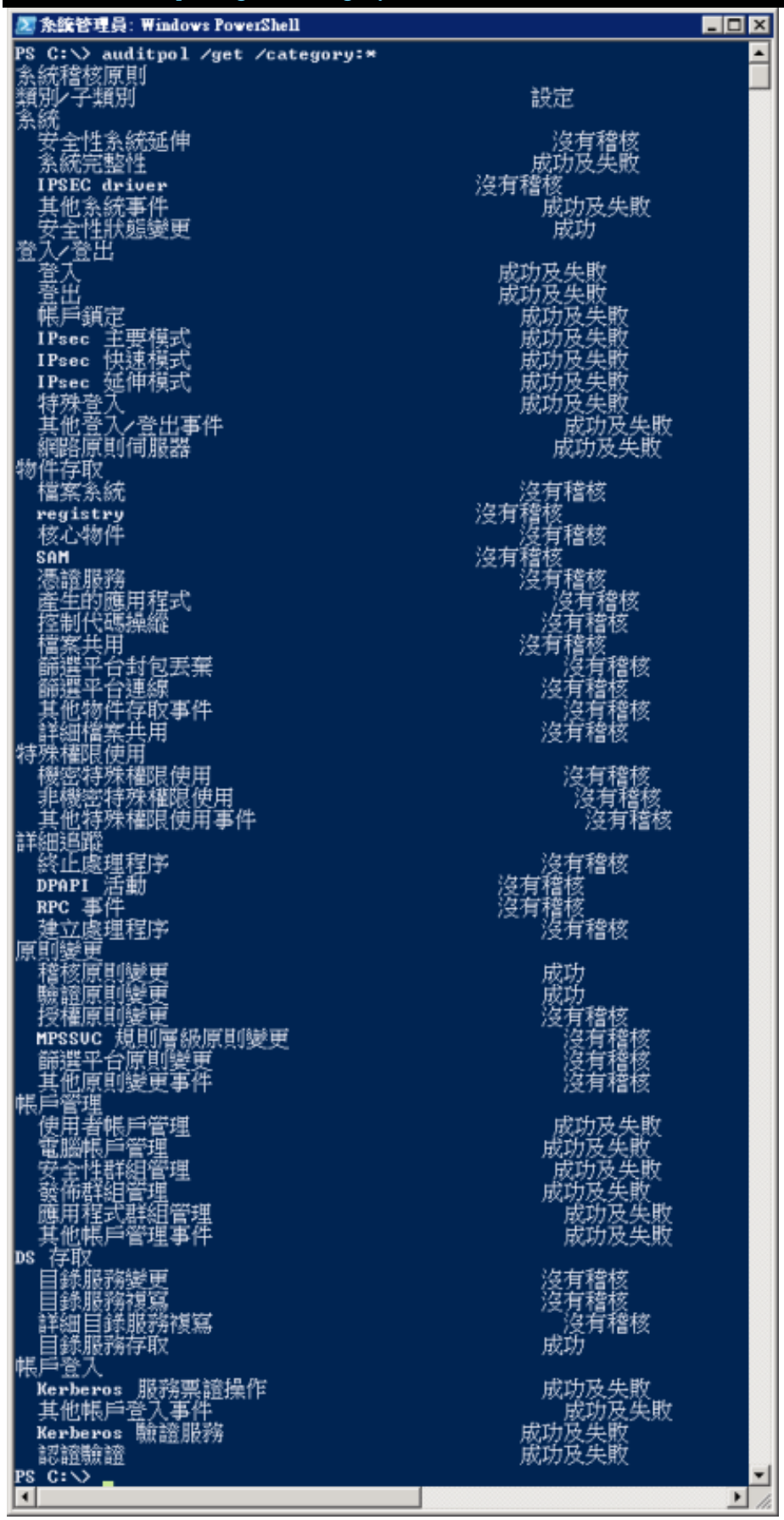
(3) 開啟 [Windows PowerShell]

(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:*
```

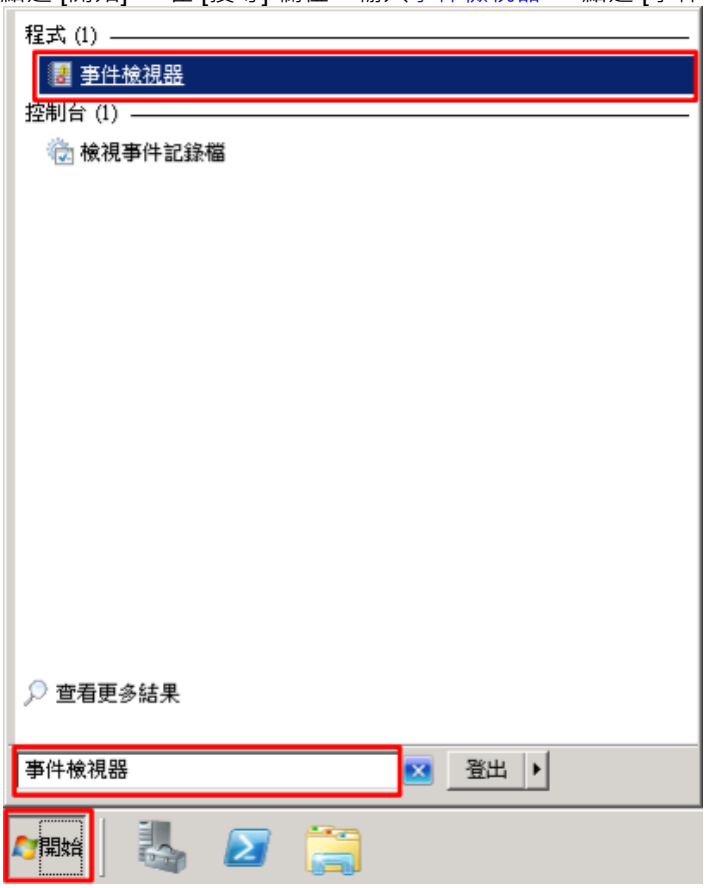


```
系統管理員: Windows PowerShell
PS C:\> auditpol /get /category:*
系統稽核原則
類別/子類別                                設定
系統
  安全性系統延伸                           沒有稽核
  系統完整性                               成功及失敗
  IPSEC driver                             沒有稽核
  其他系統事件                             成功及失敗
  安全性狀態變更                           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
  DPAPI 活動                               沒有稽核
  RPC 事件                                 沒有稽核
  建立處理程序                             沒有稽核
原則變更
  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
  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

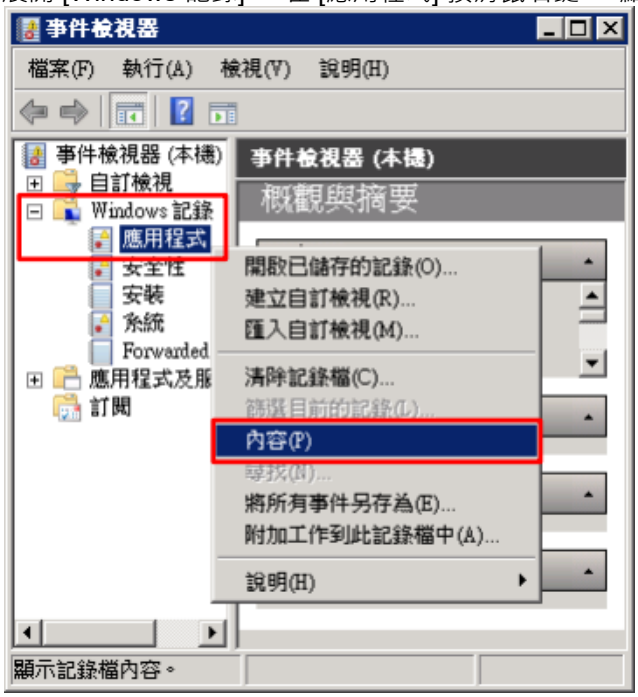
(1) 開啟 [事件檢視器]

點選 [開始] -> 在 [搜尋] 欄位，輸入事件檢視器 -> 點選 [事件檢視器]



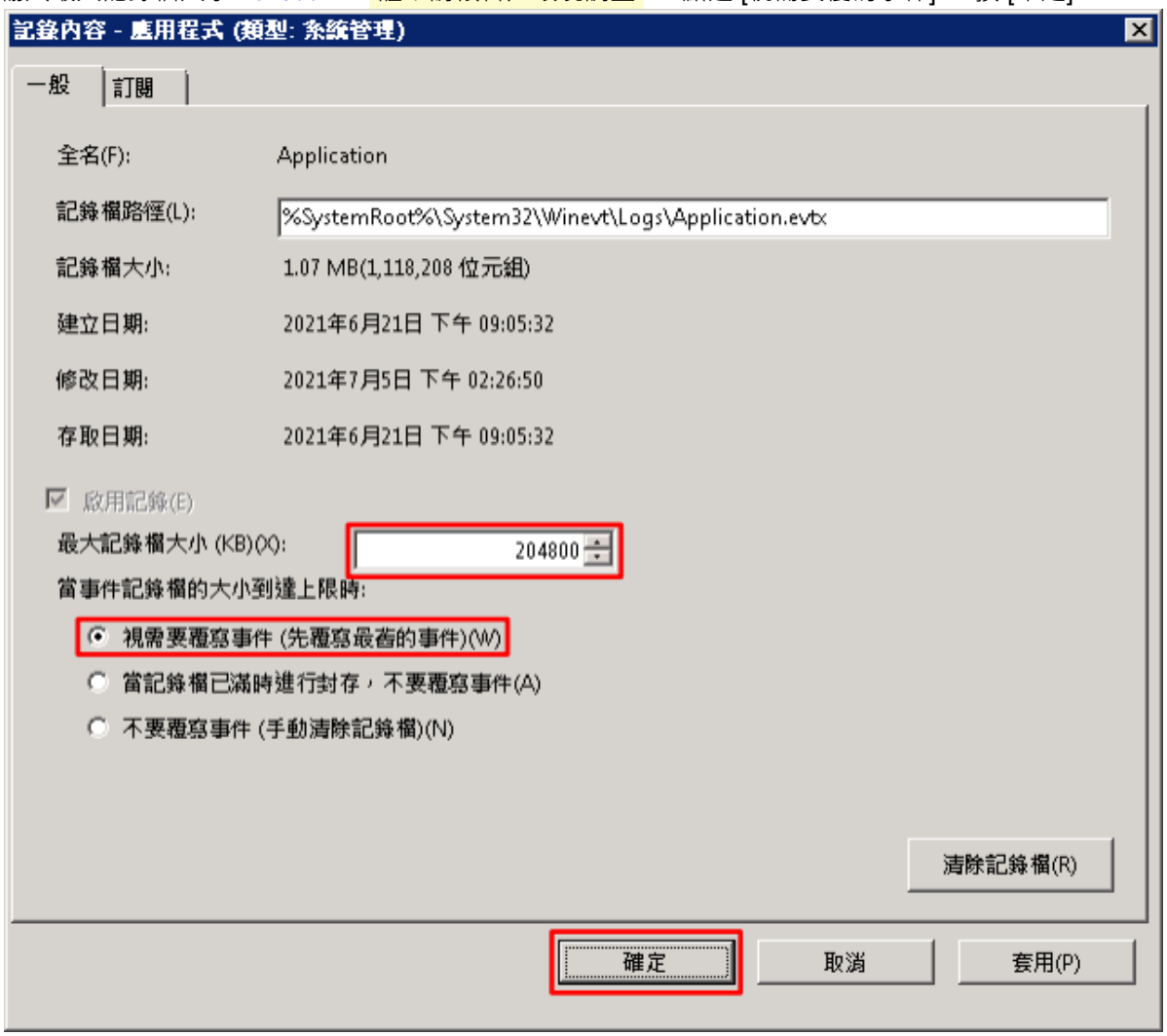
(2) 編輯應用程式記錄

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]



3 SQL2012

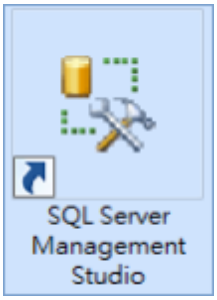
3.1 稽核登入

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

以下分別為圖形介面和指令介面設定方式。

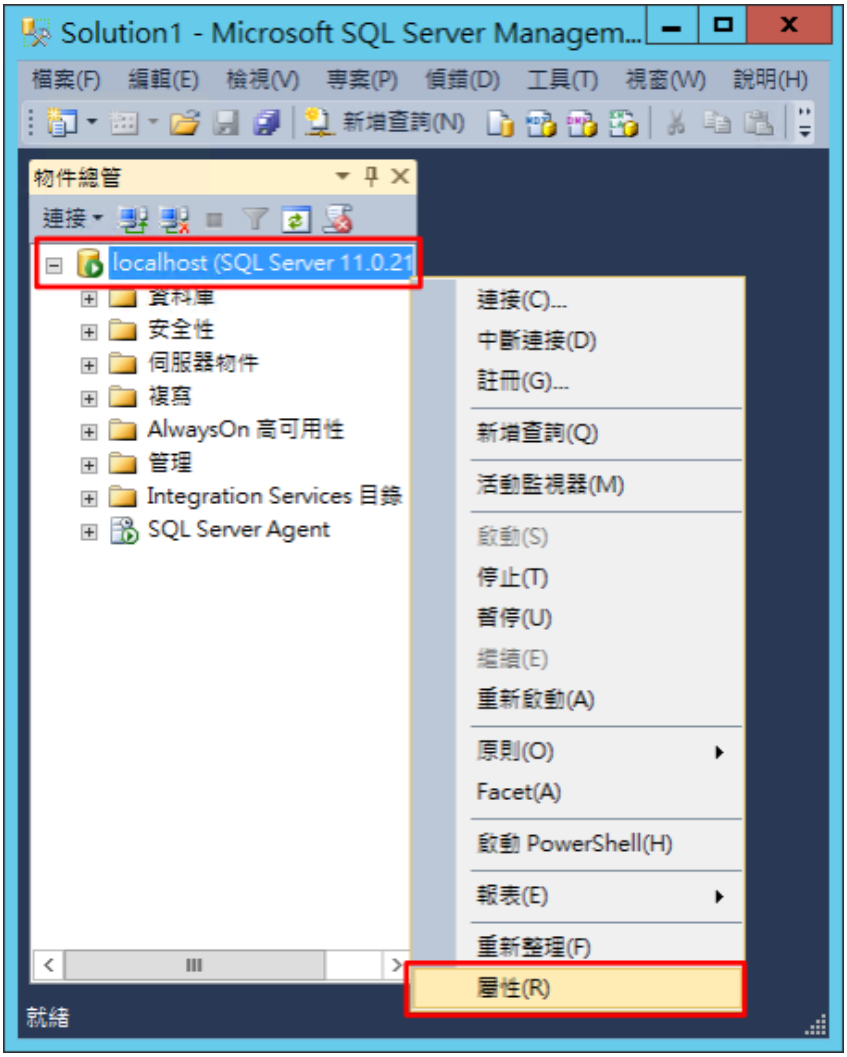
3.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]

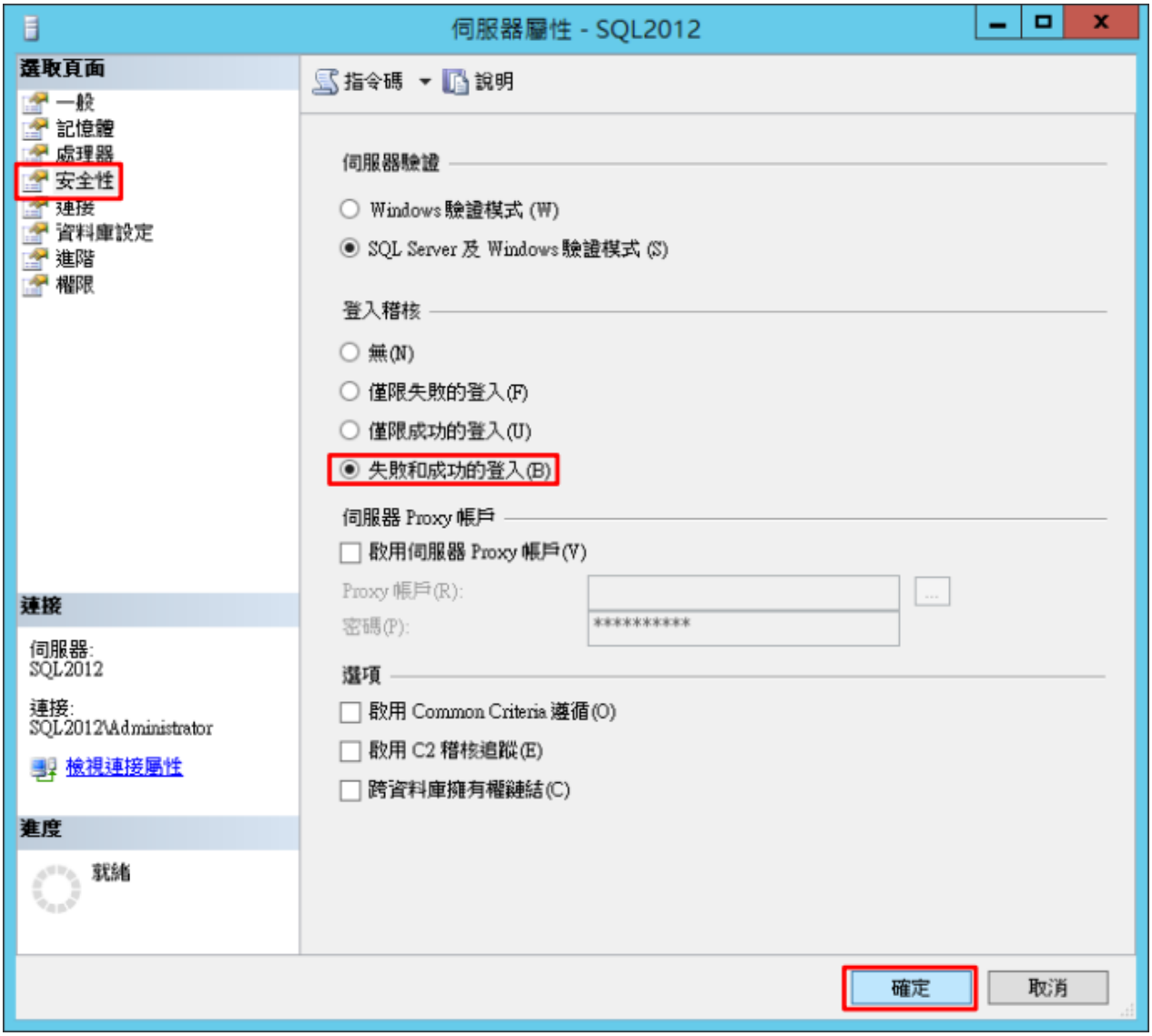


(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

(3)　在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

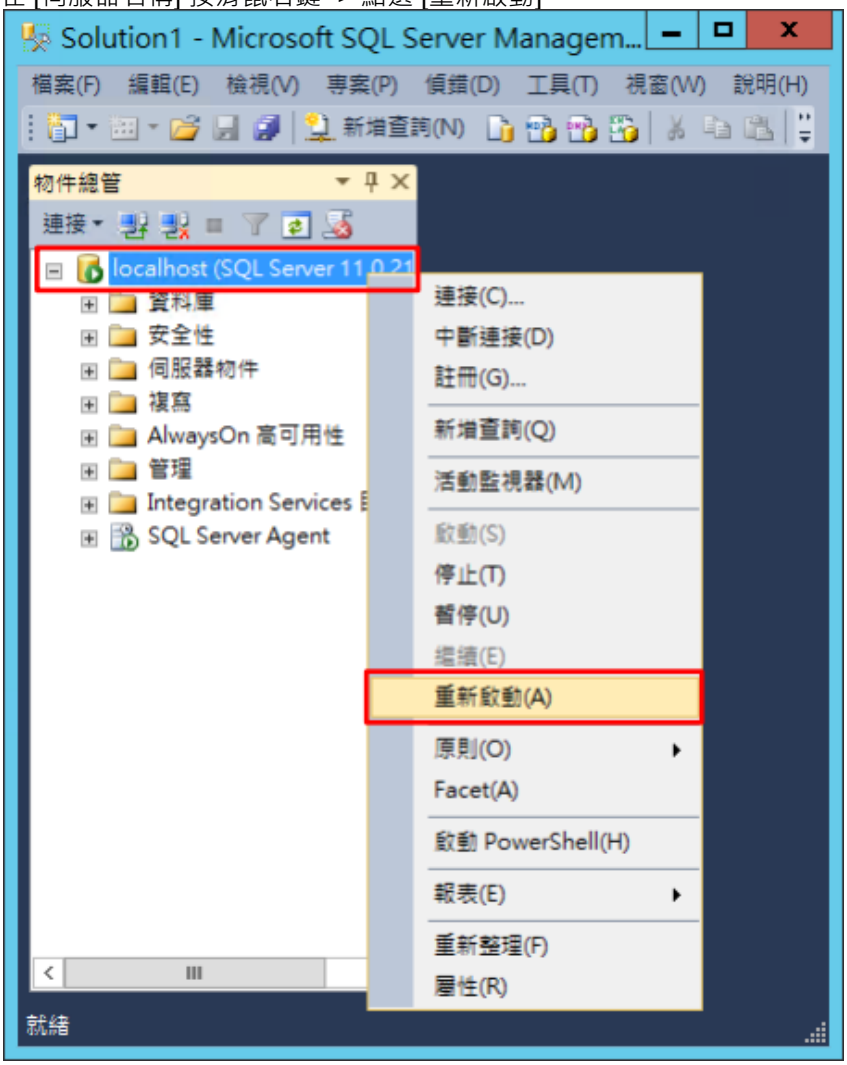


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]



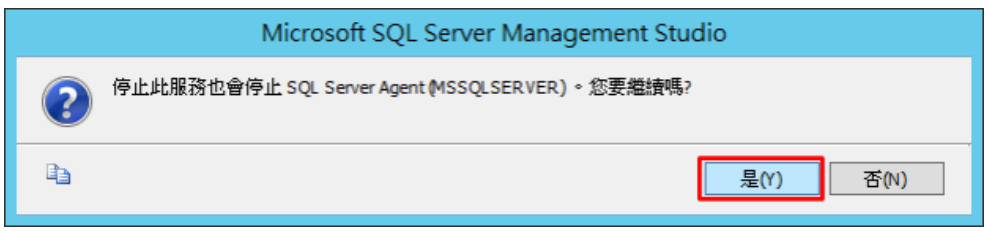
(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務

(7) 按 [是] 停止 SQL SERVER Agent 服務



3.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

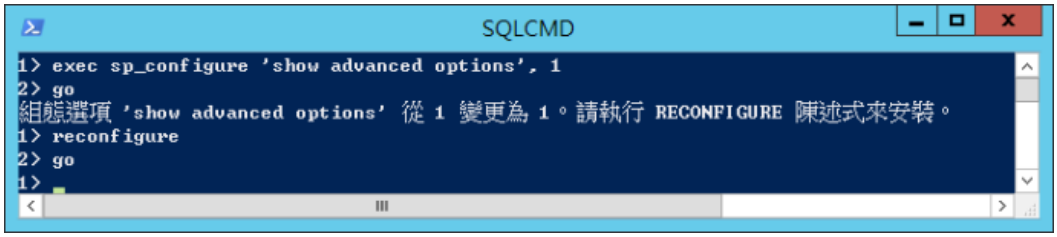
```
PS C:\> sqlcmd -S localhost -A
```

(3) 切換資料庫

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

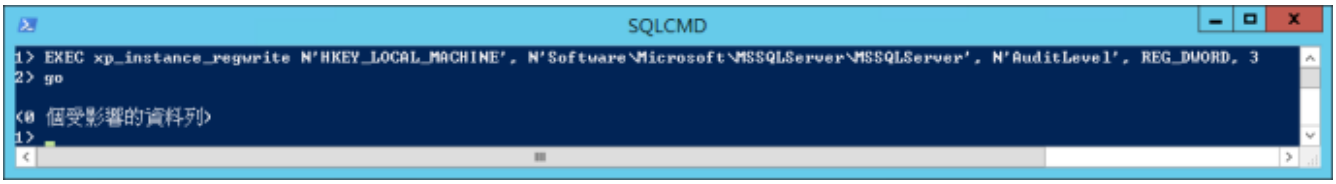
(4) 使用 sp_configure 列出進階選項

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



(5) 啟用失敗和成功的登入記錄

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



(6) 重新啟動 MS SQL SERVER 服務

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

3.2 設定稽核

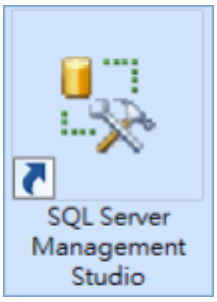
3.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

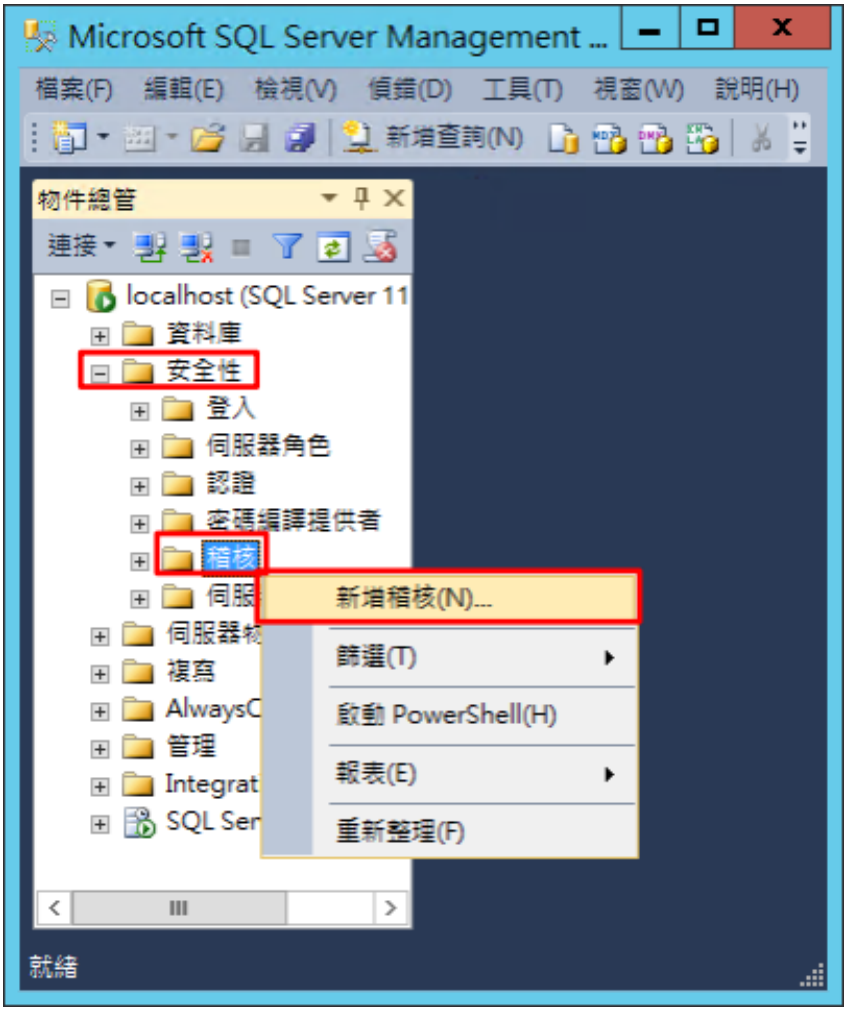
3.2.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]

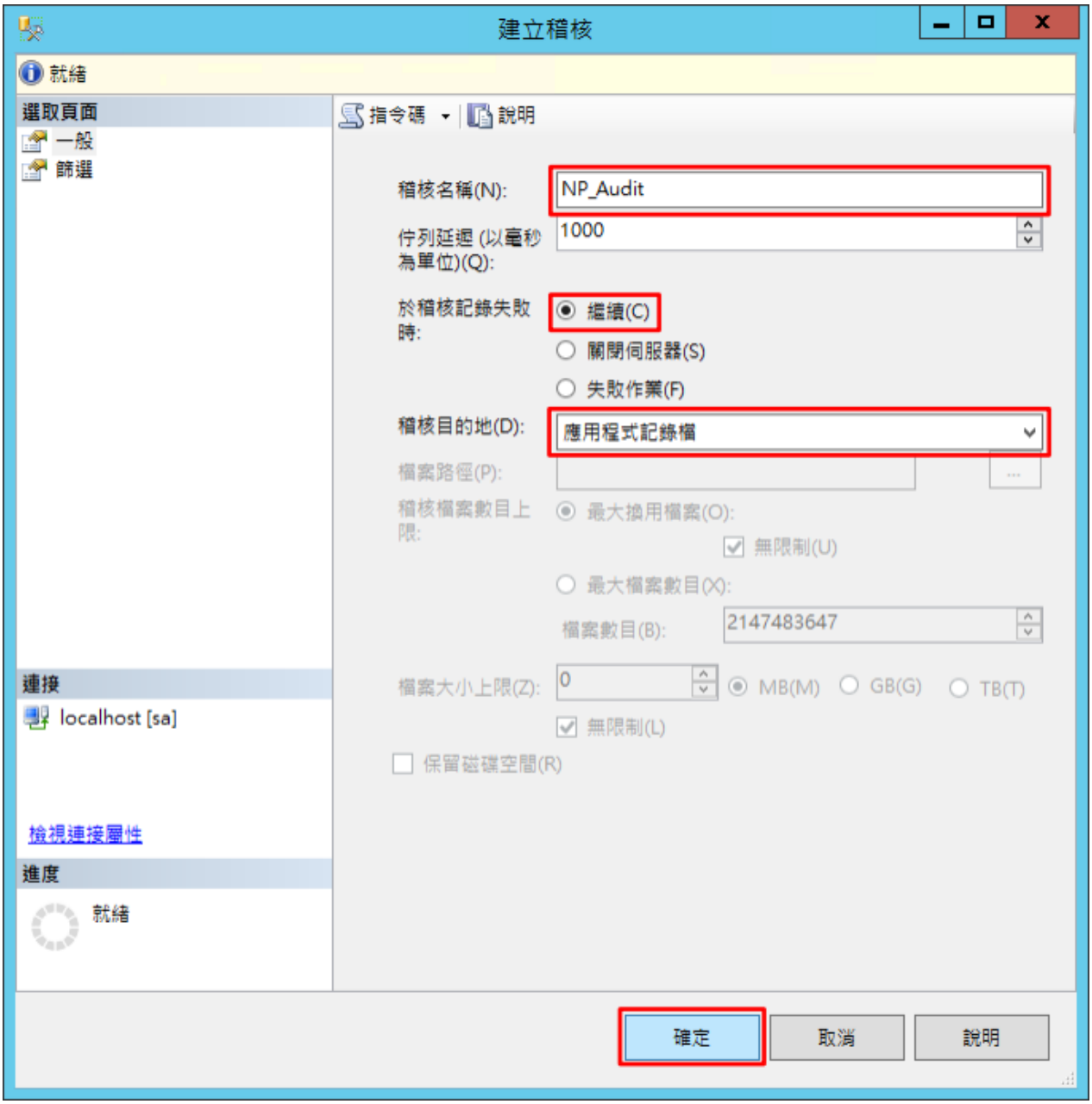


(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

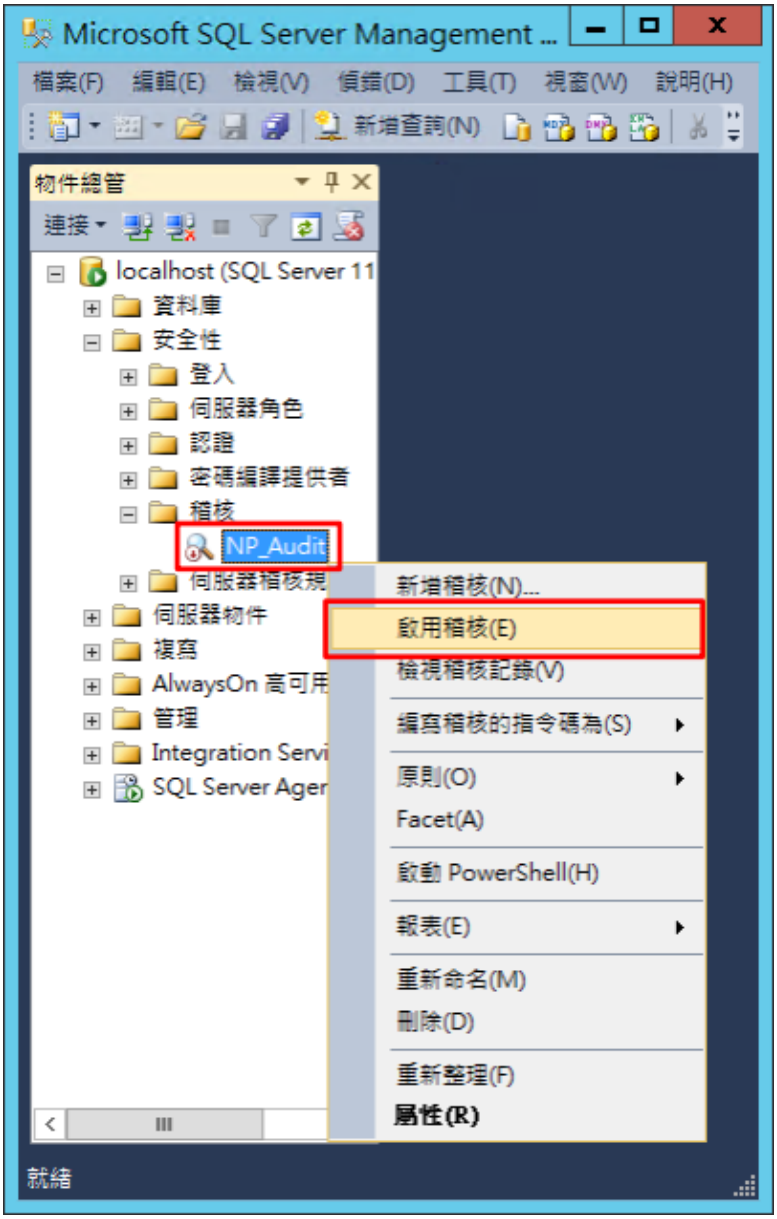
(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



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

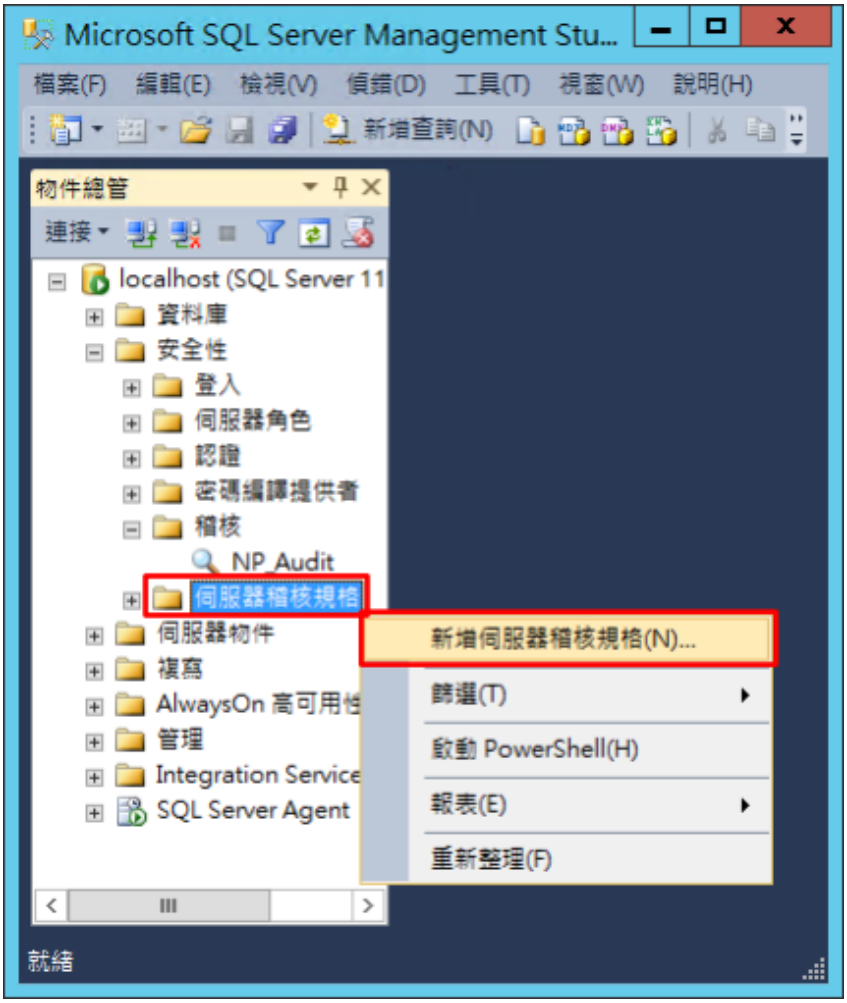


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



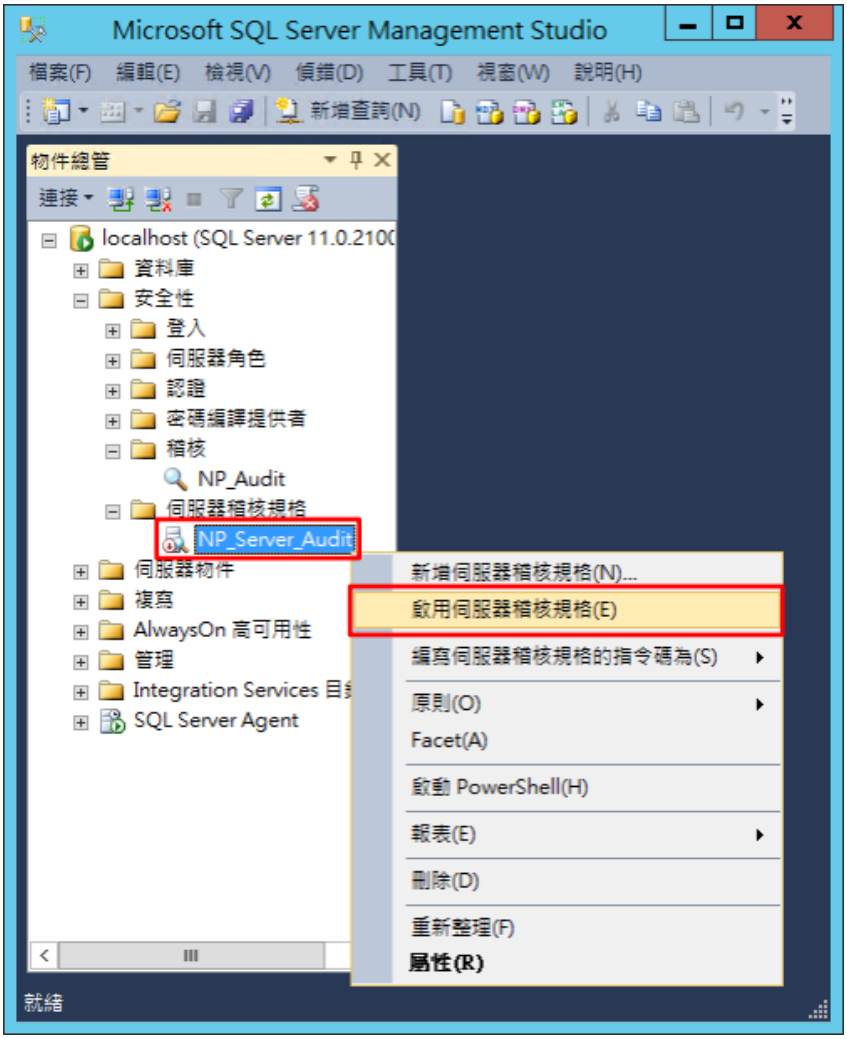
(6)　按 [關閉]

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



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

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



(10)　按 [關閉]

3.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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

Options:

-S [protocol:]server[instance_name][,port]

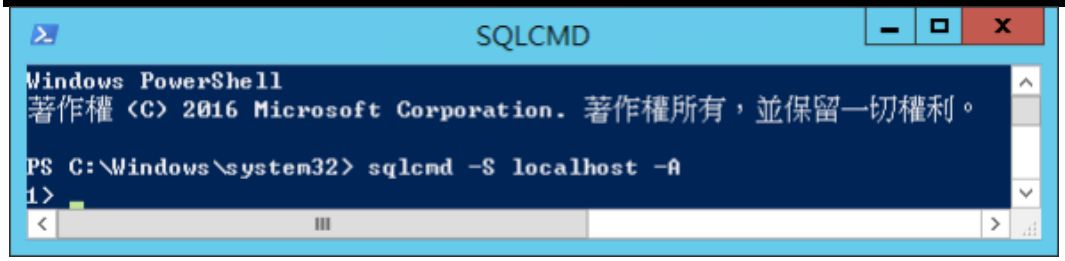
-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

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

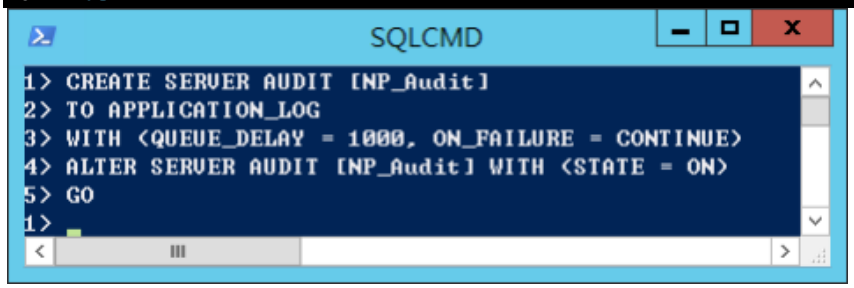


(3) 切換資料庫

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

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

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



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
```

紅色文字部位請輸入伺服器稽核規格名稱

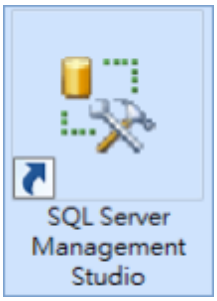
3.2.2 稽核資料庫層級

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。

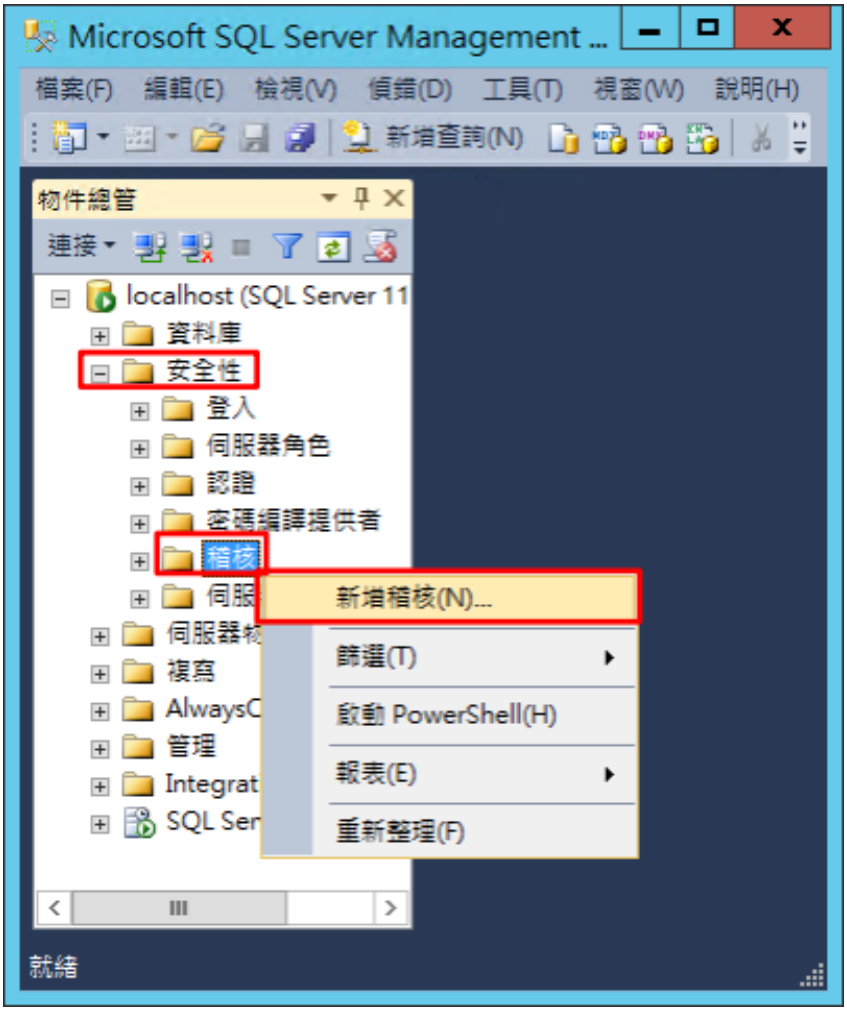
3.2.2.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]

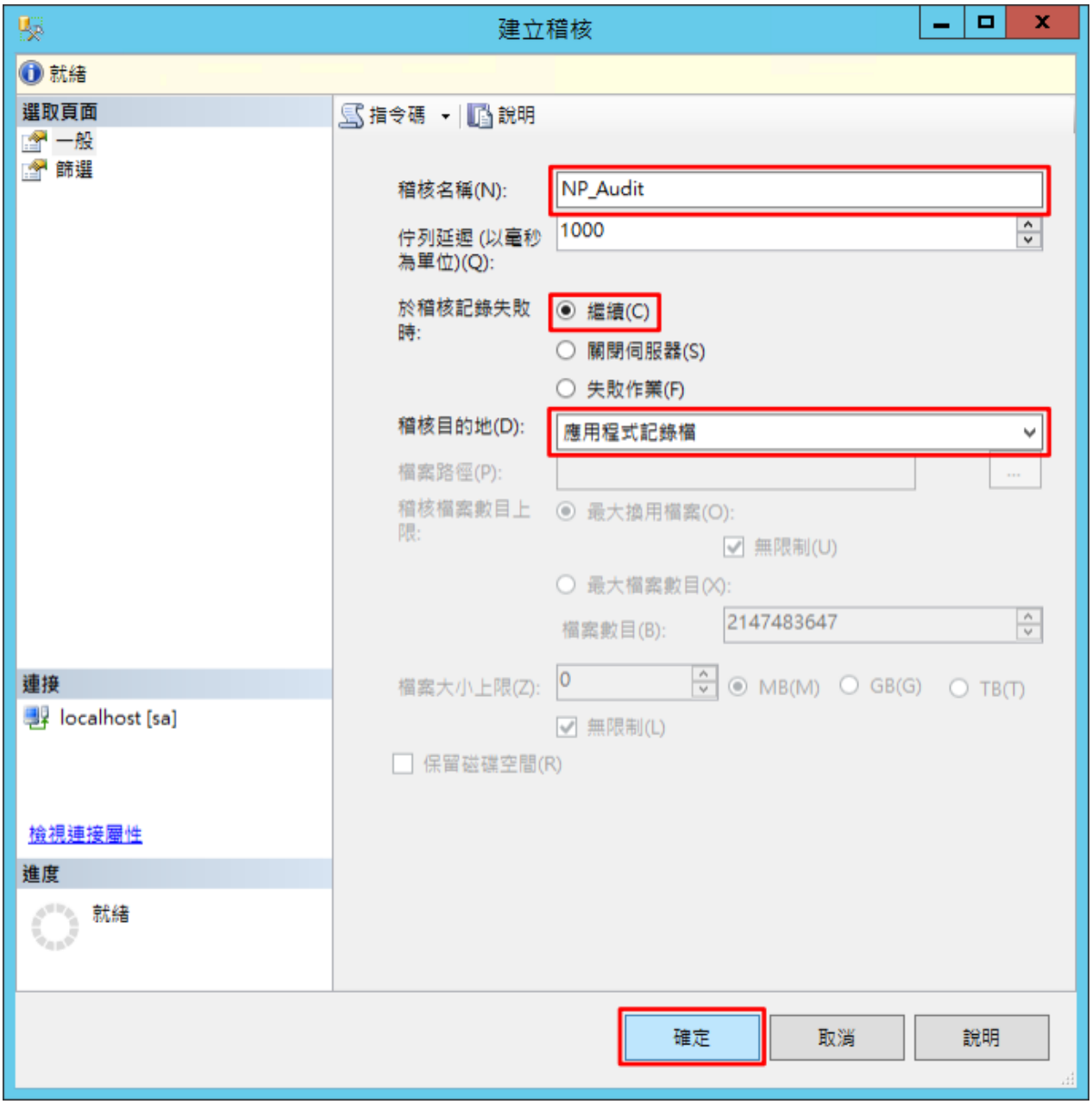


(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

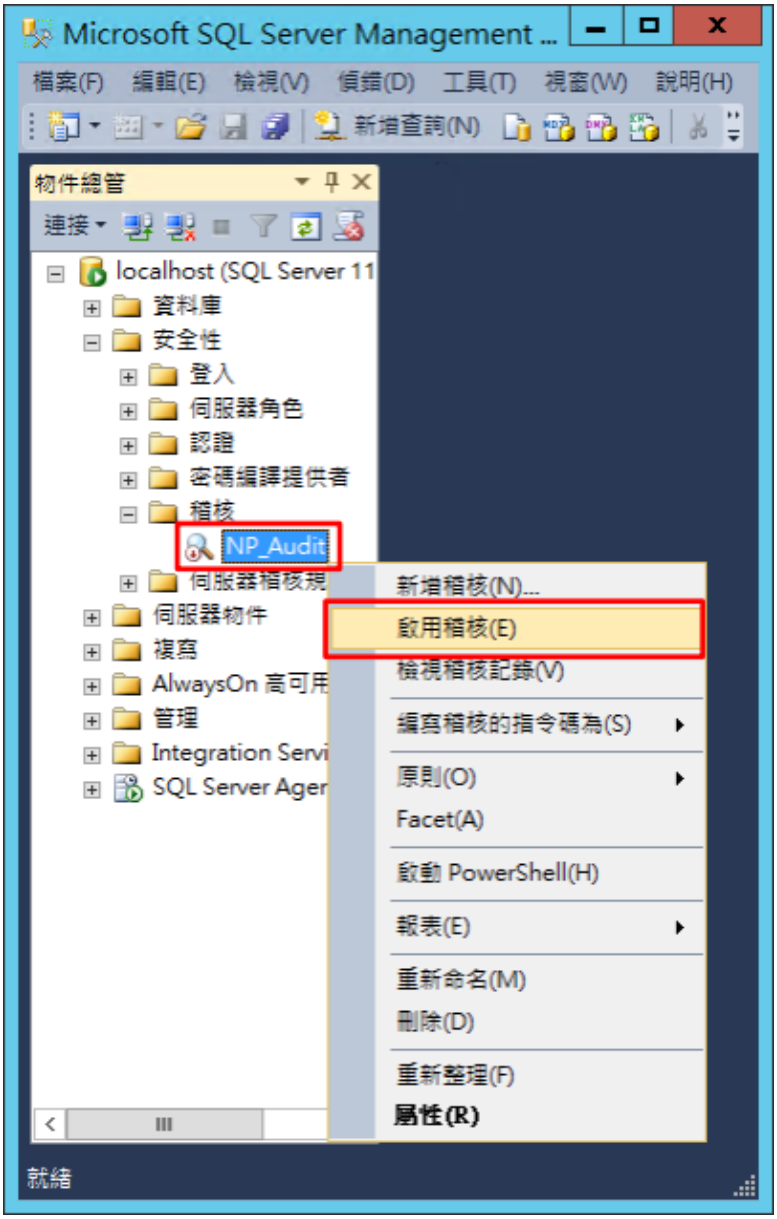
(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]



(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]

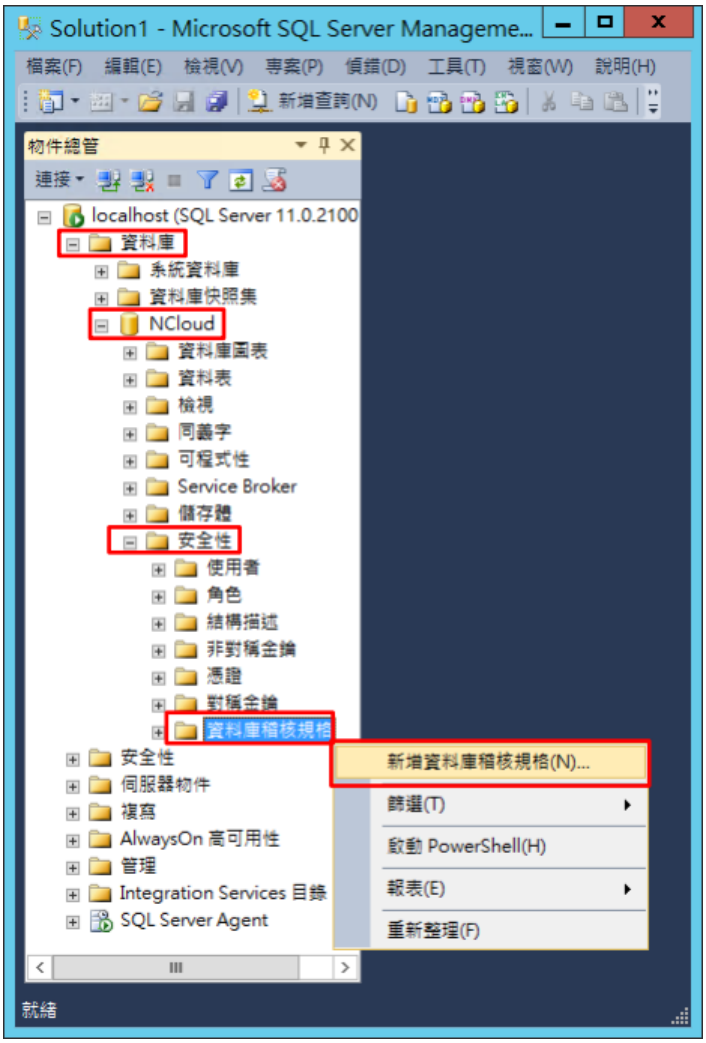


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



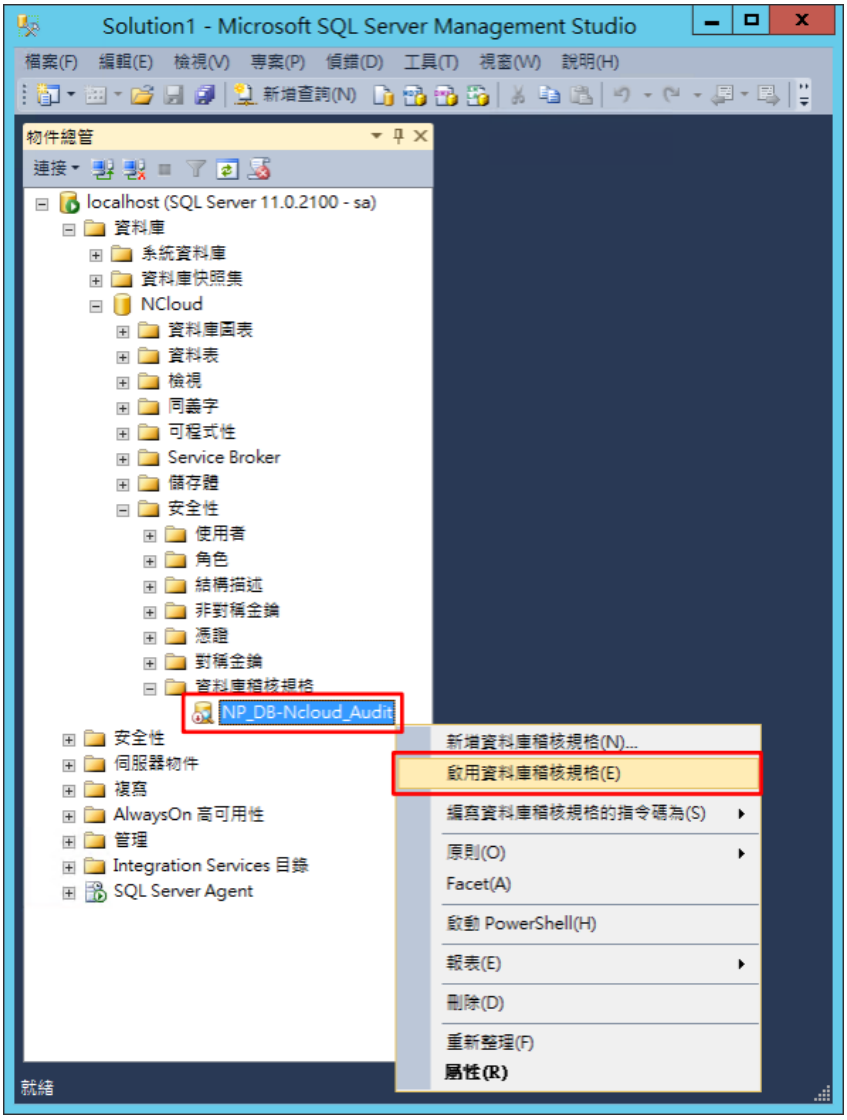
(6)　按 [關閉]

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

(9)　在資料庫稽核規格名稱: [NP_DB-NCloud_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10)　按 [關閉]

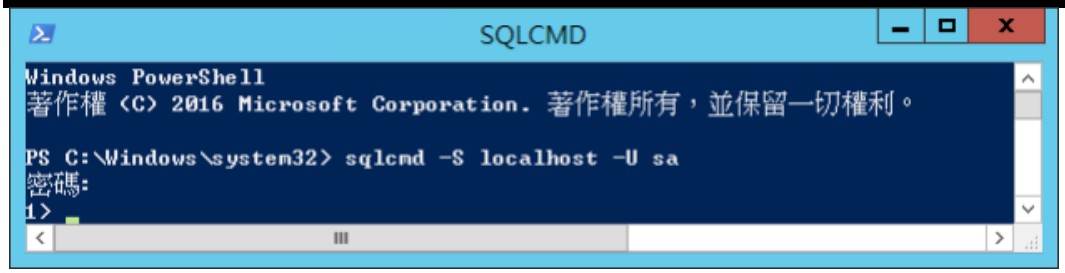
3.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

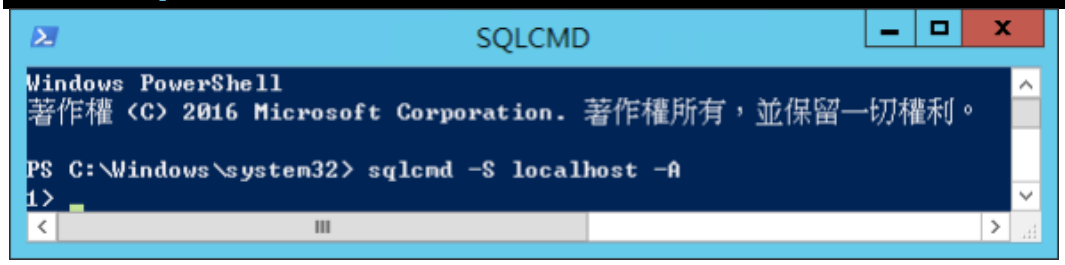
-U login_id

-P password

-A dedicated administrator connection

<2.2> 使用 Windows 帳號

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

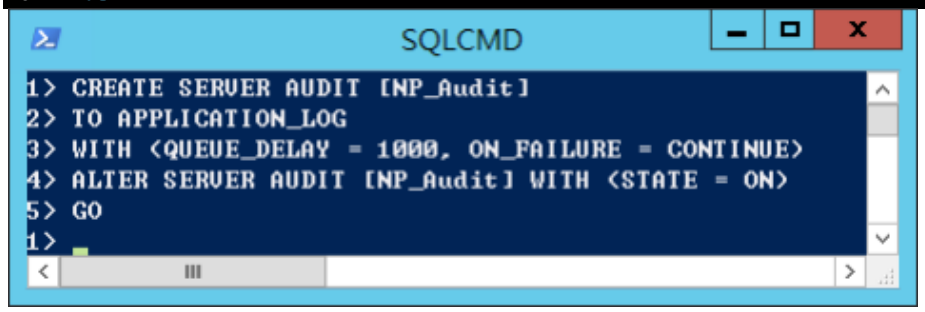


(3) 切換資料庫

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

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

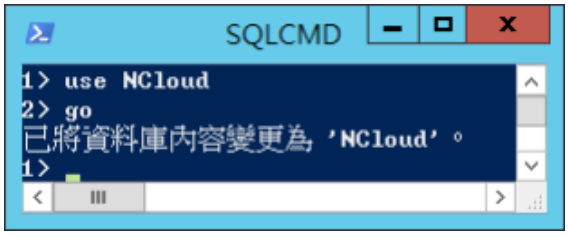
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例： NCloud

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



紅色文字部位請輸入稽核資料庫名稱

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

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

紅色文字部位請輸入資料庫稽核規格名稱

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

紅色文字部位請輸入稽核資料庫名稱

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

3.3 事件記錄檔設定

此為選項設定。

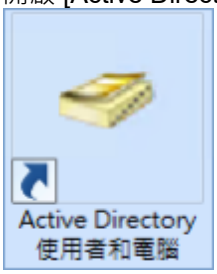
以下分別為網域和工作群組設定方式。

3.3.1 網域

3.3.1.1 組織單位設定

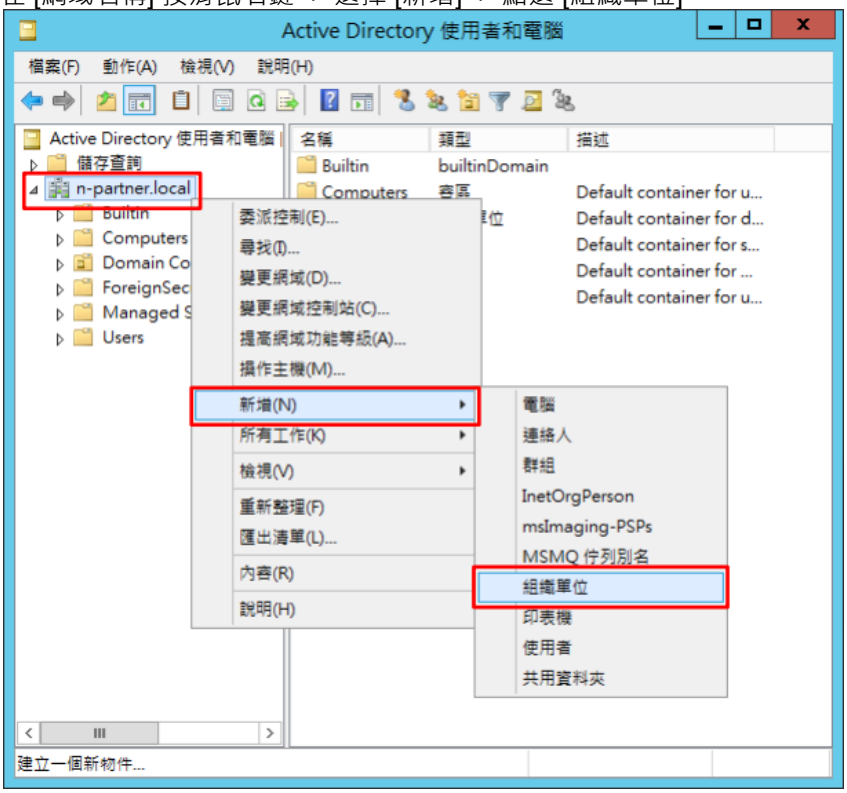
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



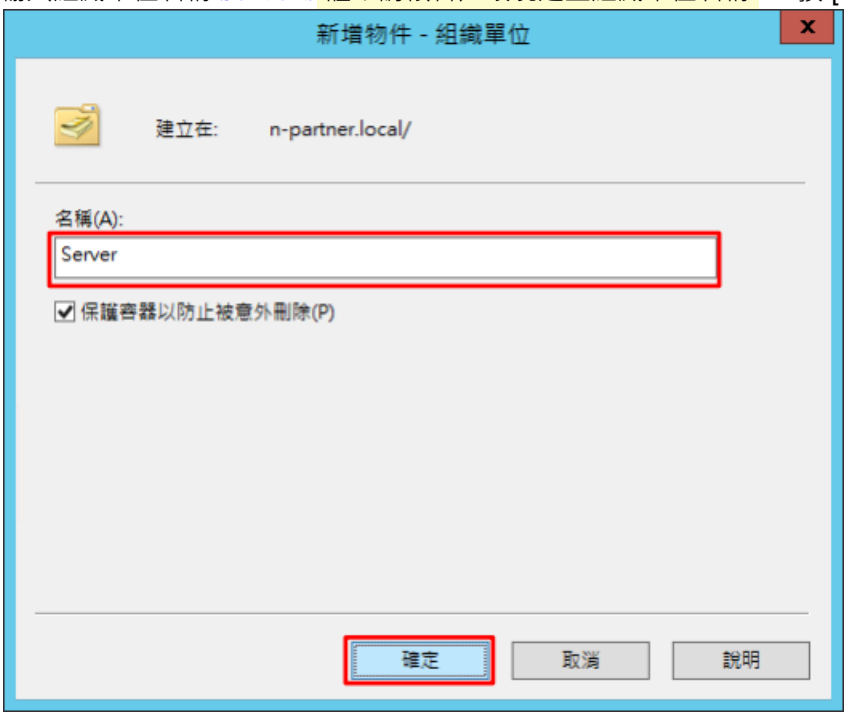
(2) 新增組織單位

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



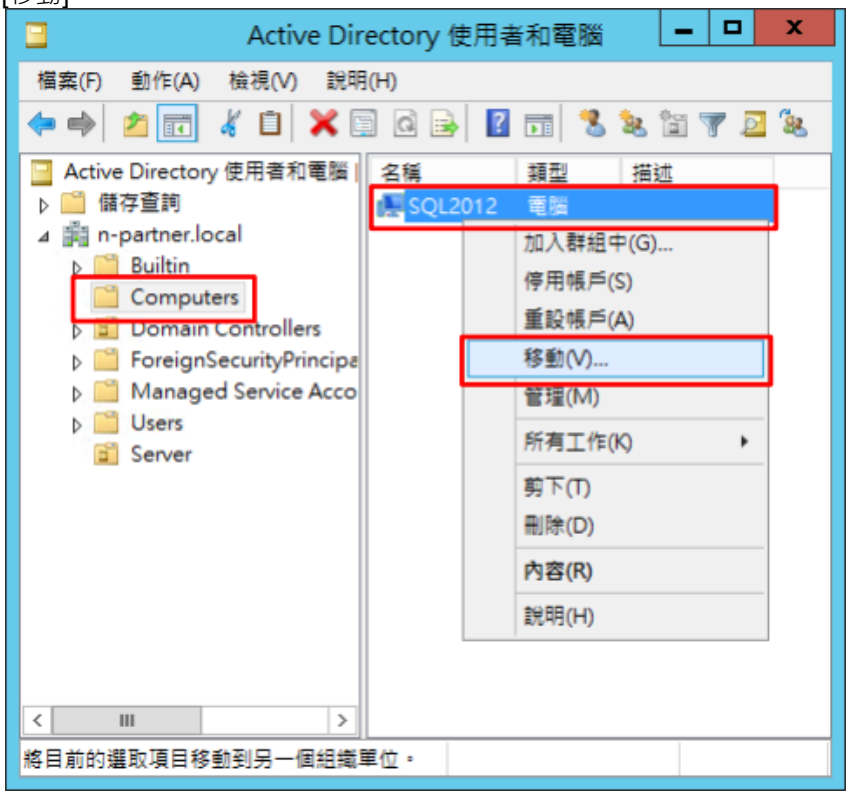
(3) 輸入組織單位名稱

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



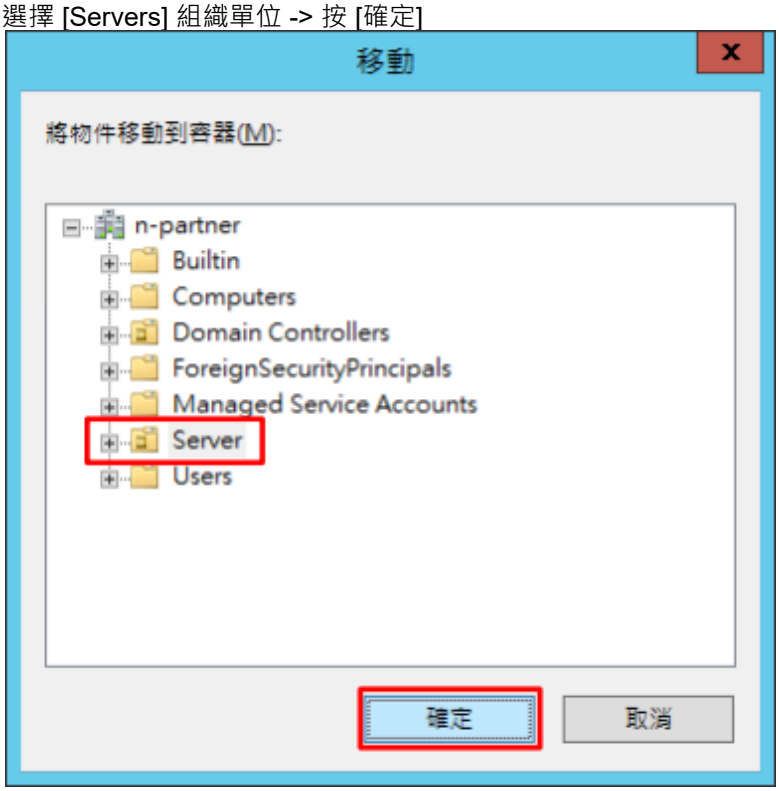
(4) 移動伺服器至新的組織單位

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



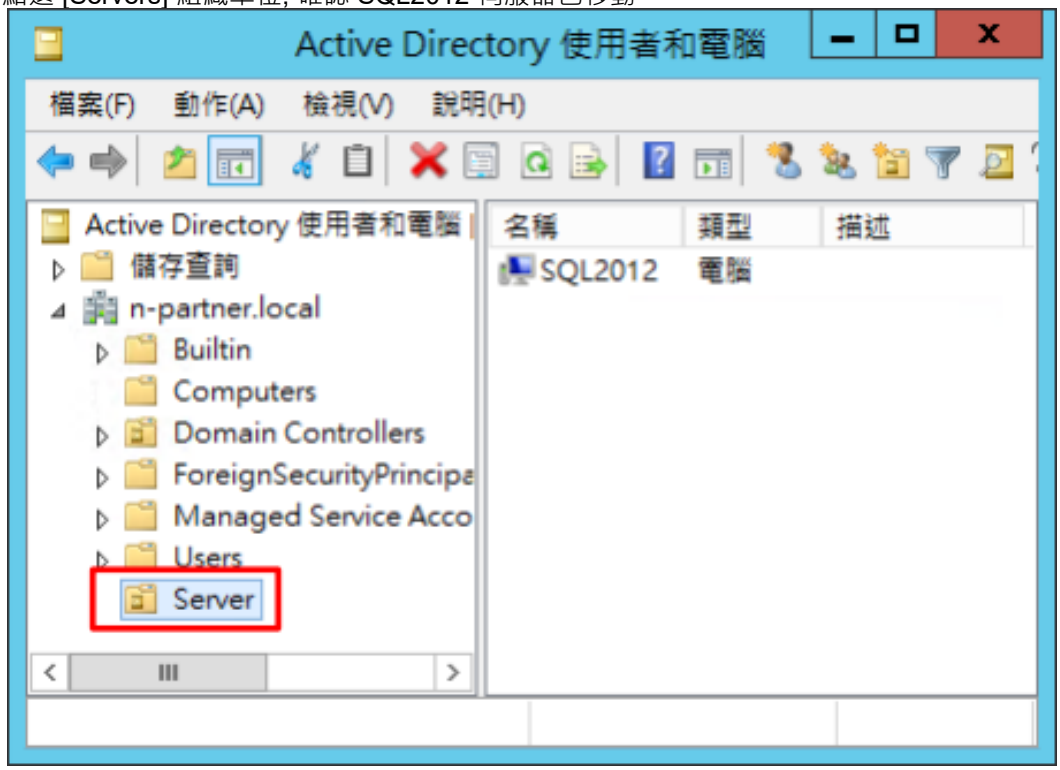
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

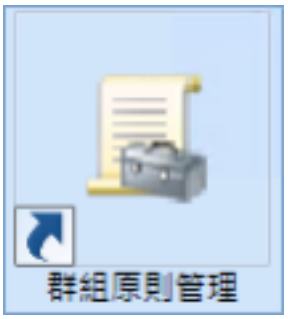
點選 [Servers] 組織單位, 確認 SQL2012 伺服器已移動。



3.3.1.2 群組原則設定

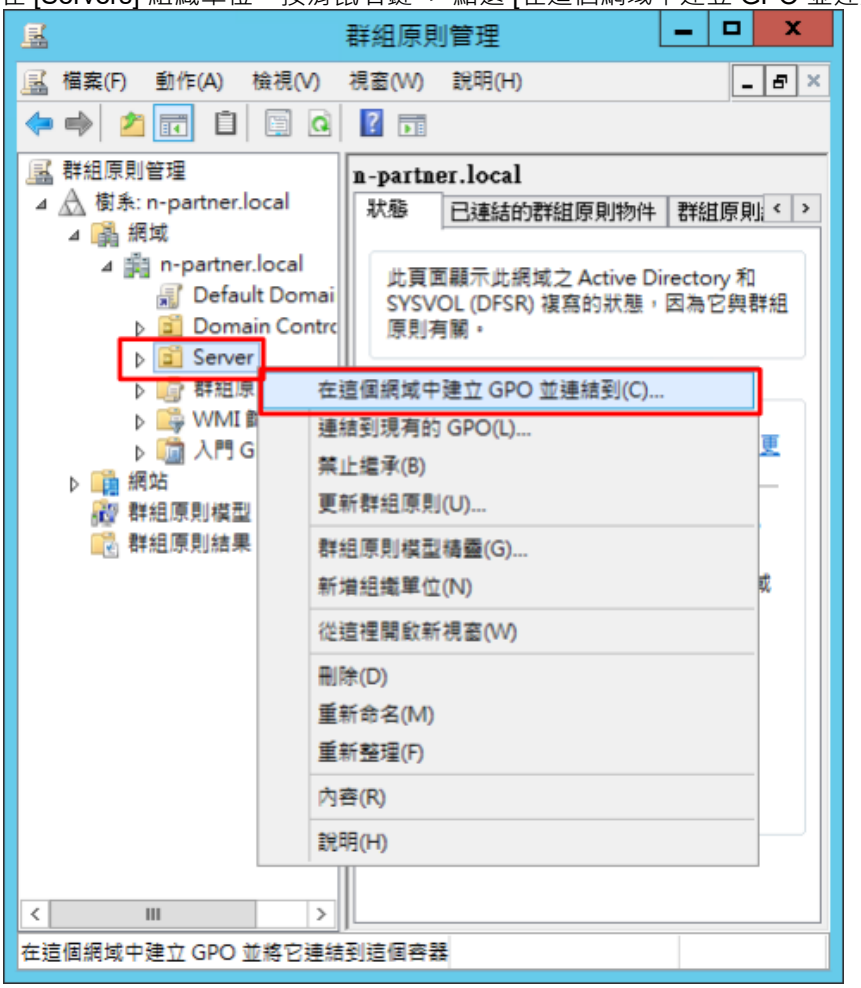
(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位，新增群組原則物件

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

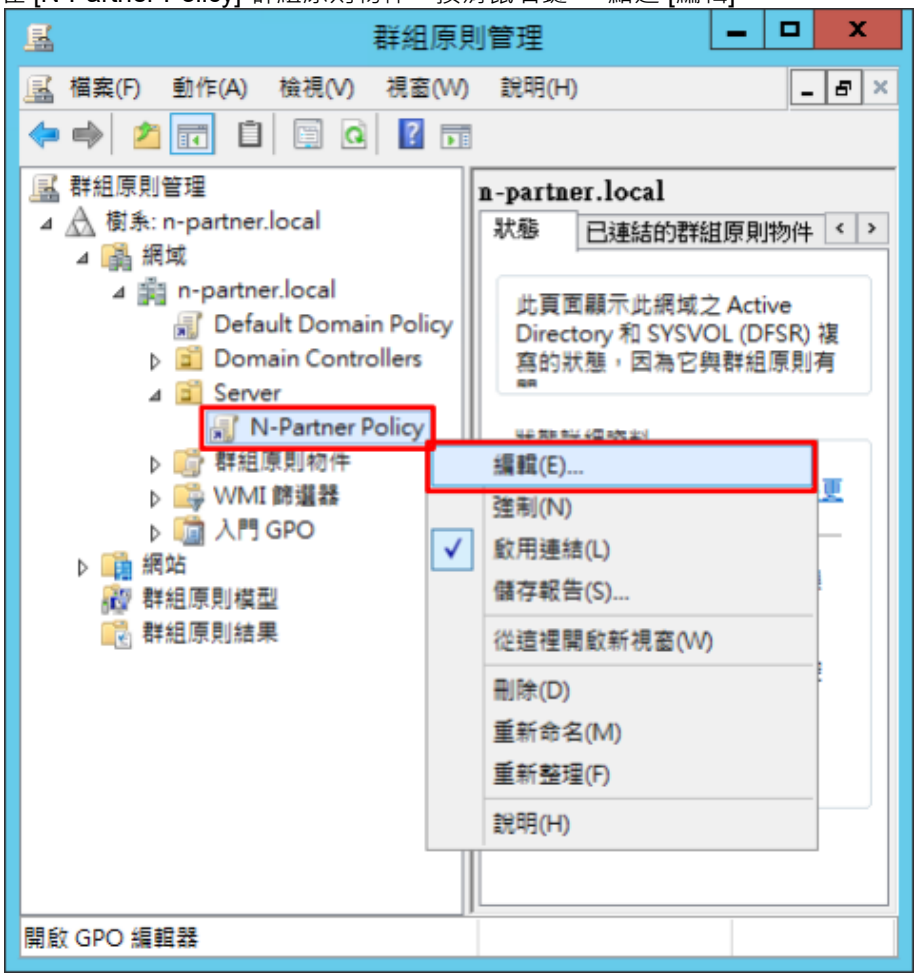


(3) 輸入群組原則物件名稱

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

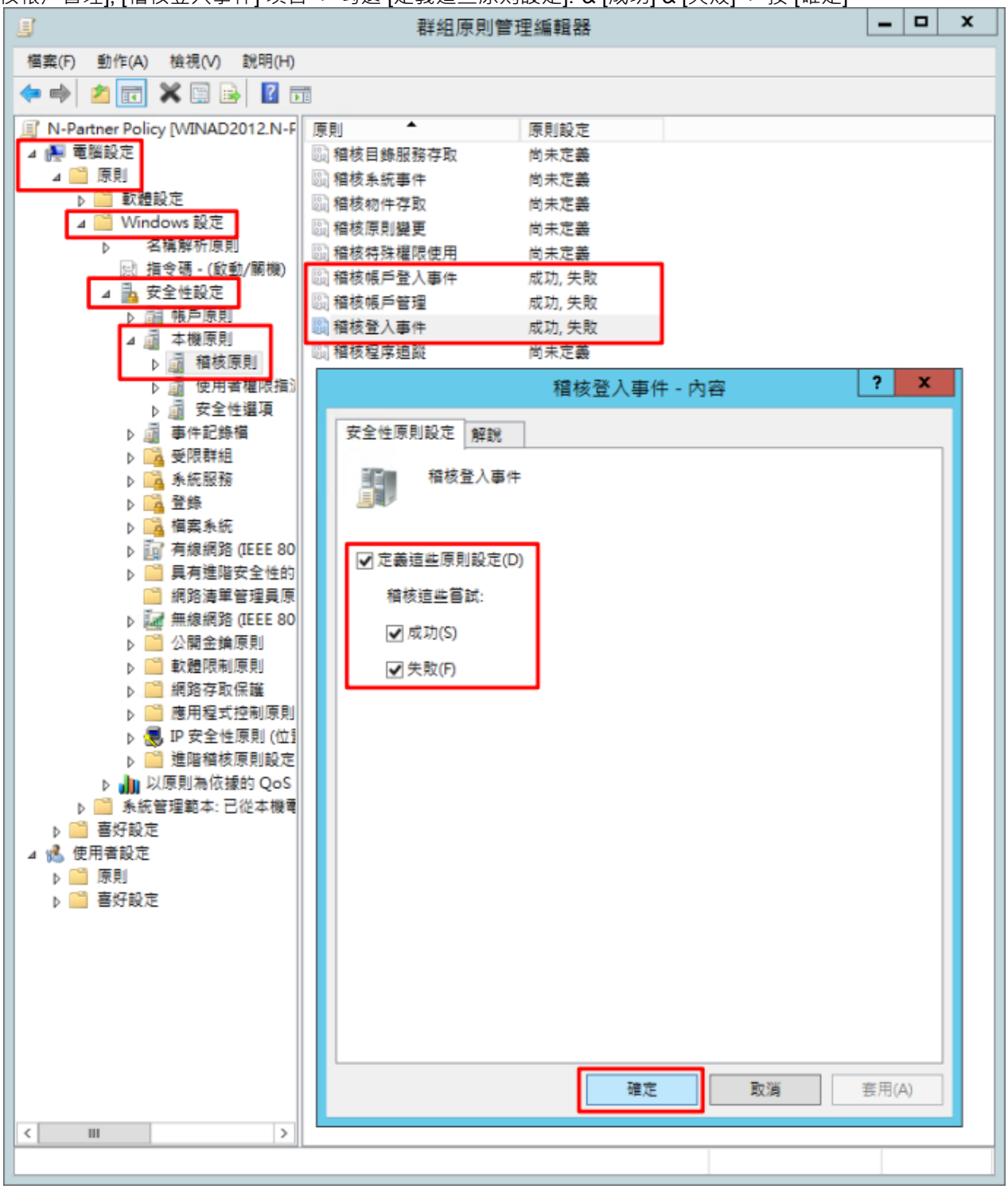
(4) 編輯群組原則物件

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



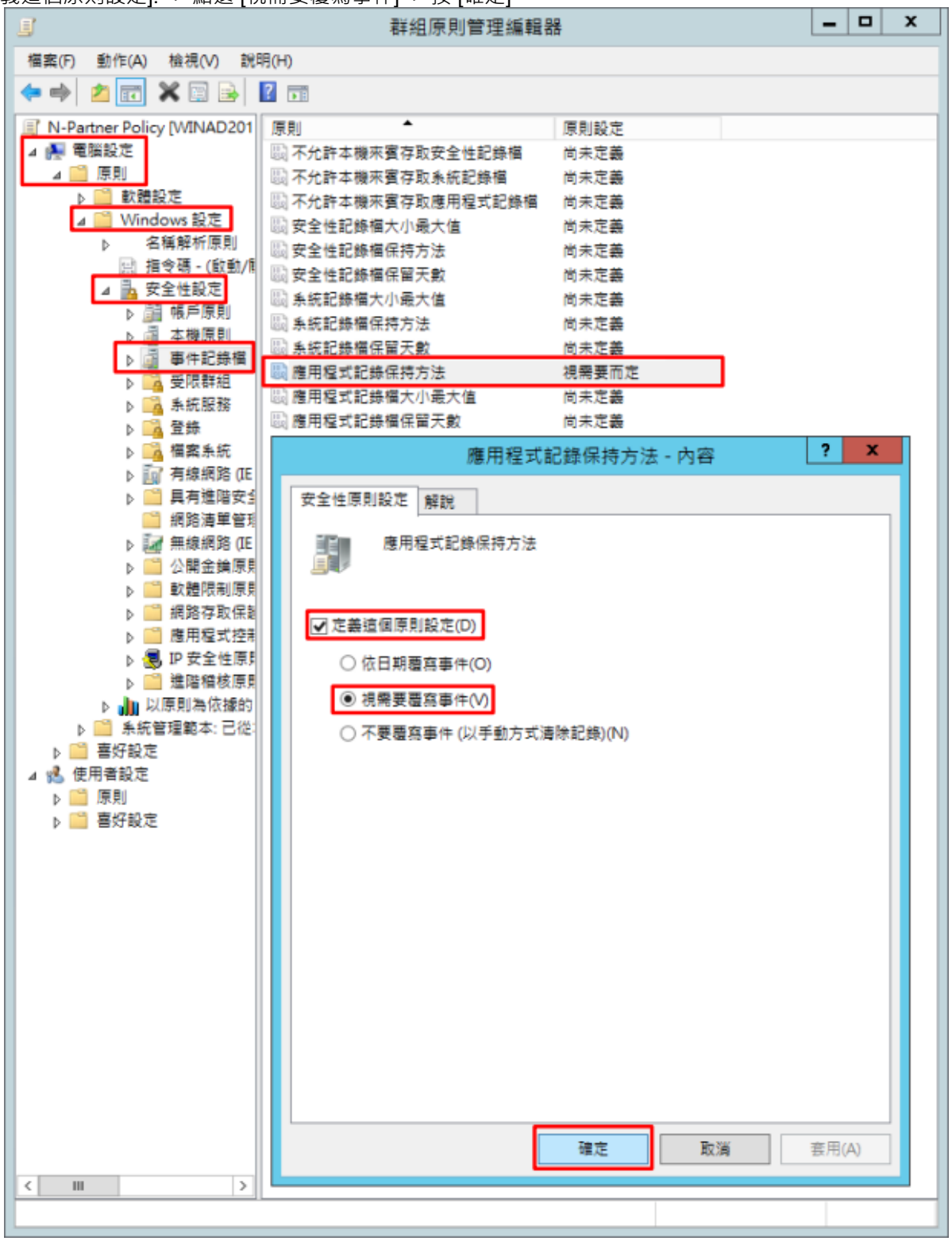
(5) 本機原則：稽核原則

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



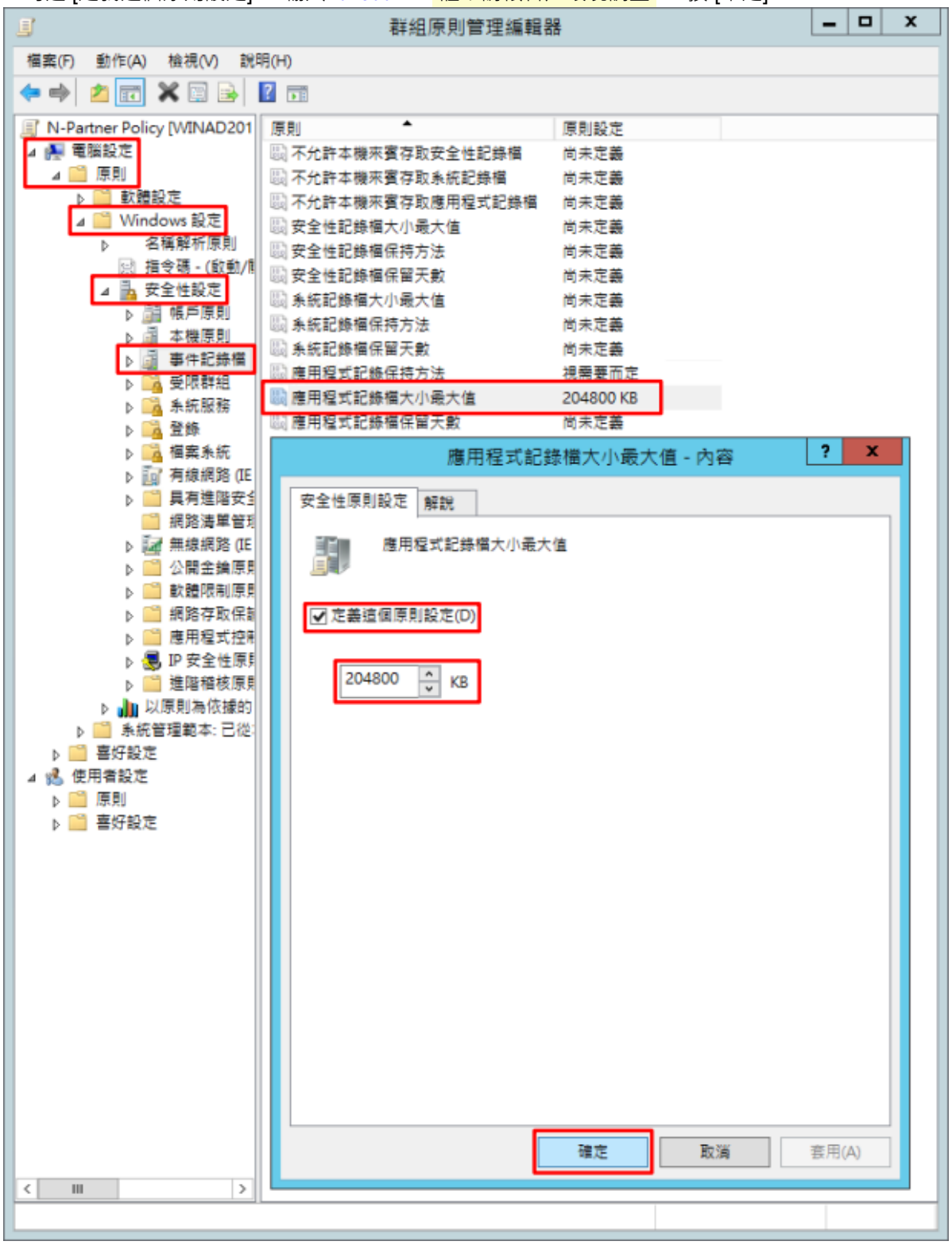
(6) 事件記錄：應用程式記錄保持方法

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



(7) 事件記錄：應用程式記錄檔大小最大值

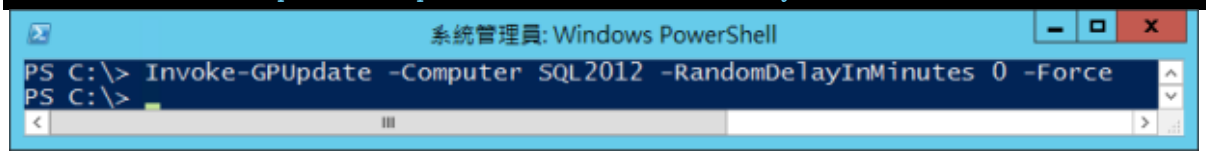
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入204800 KB 註：請依客戶環境調整 -> 按 [確定]



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

(9) 更新 MS SQL Server 群組原則

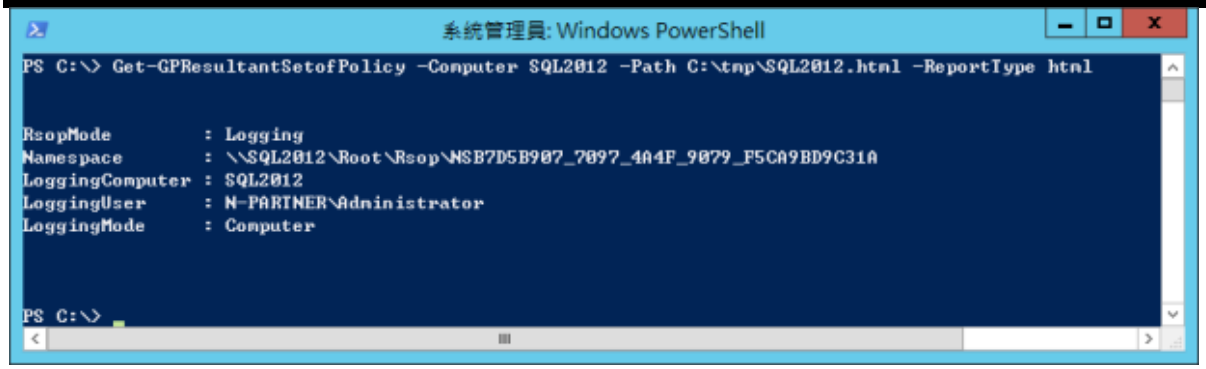
```
PS C:\> Invoke-GPUpdate -Computer SQL2012 -RandomDelayInMinutes 0 -Force
```



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.htnl -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

3.3.2 工作群組

3.3.2.1 稽核原則設定

(1) 開啟搜尋

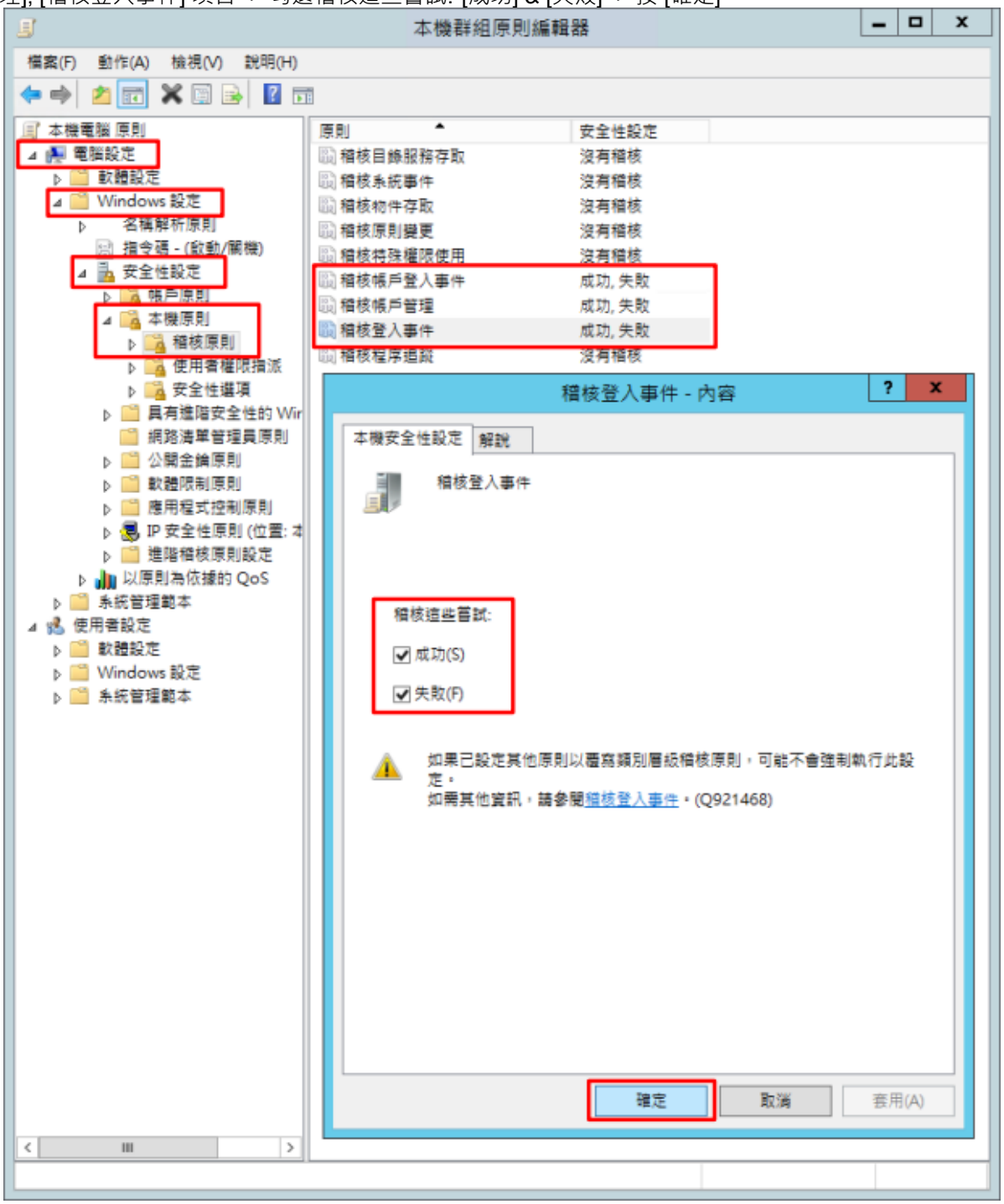
將滑鼠移到右下角點選 [搜尋]

(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

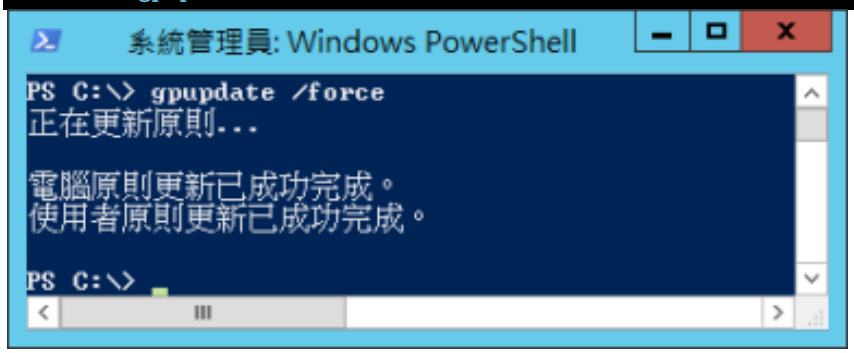
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(4) 開啟 [Windows PowerShell]

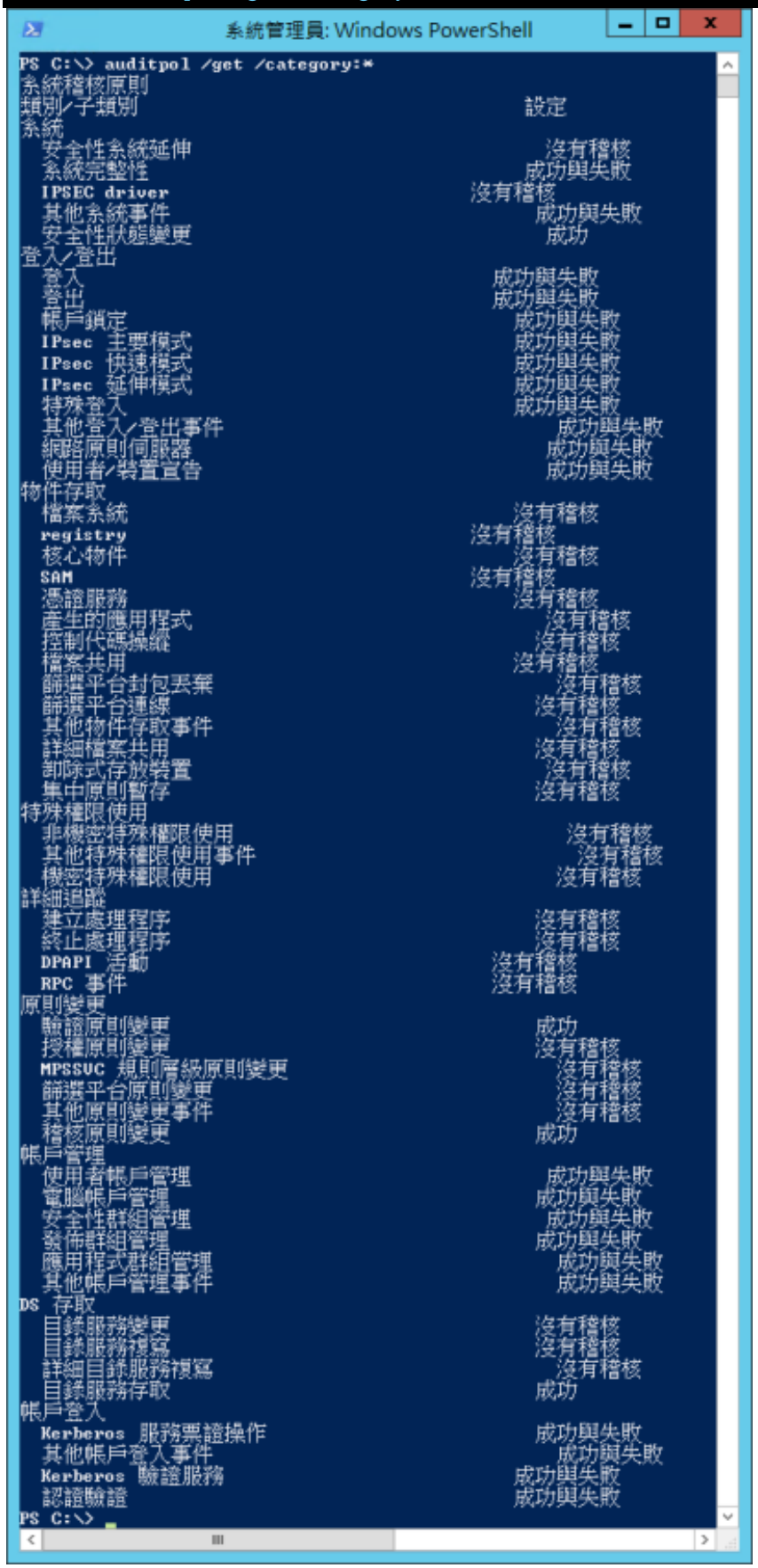
(5) 更新群組原則

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



(6) 查看群組原則套用情形

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



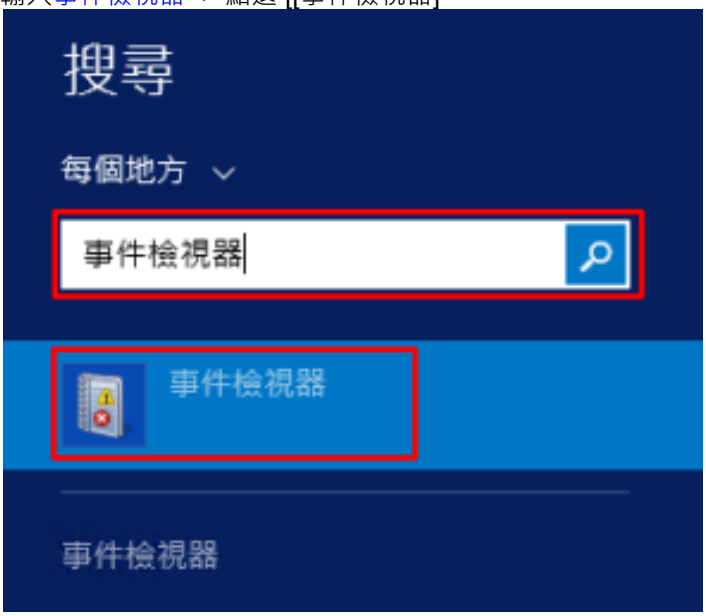
3.3.2.2 事件檔案設定

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]

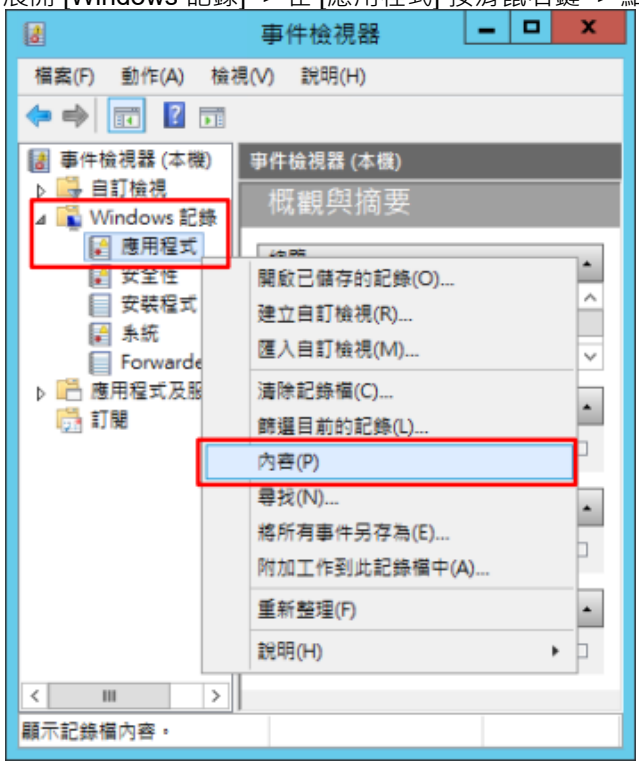
(2) 搜尋事件檢視器並執行

輸入事件檢視器 -> 點選 [[事件檢視器]



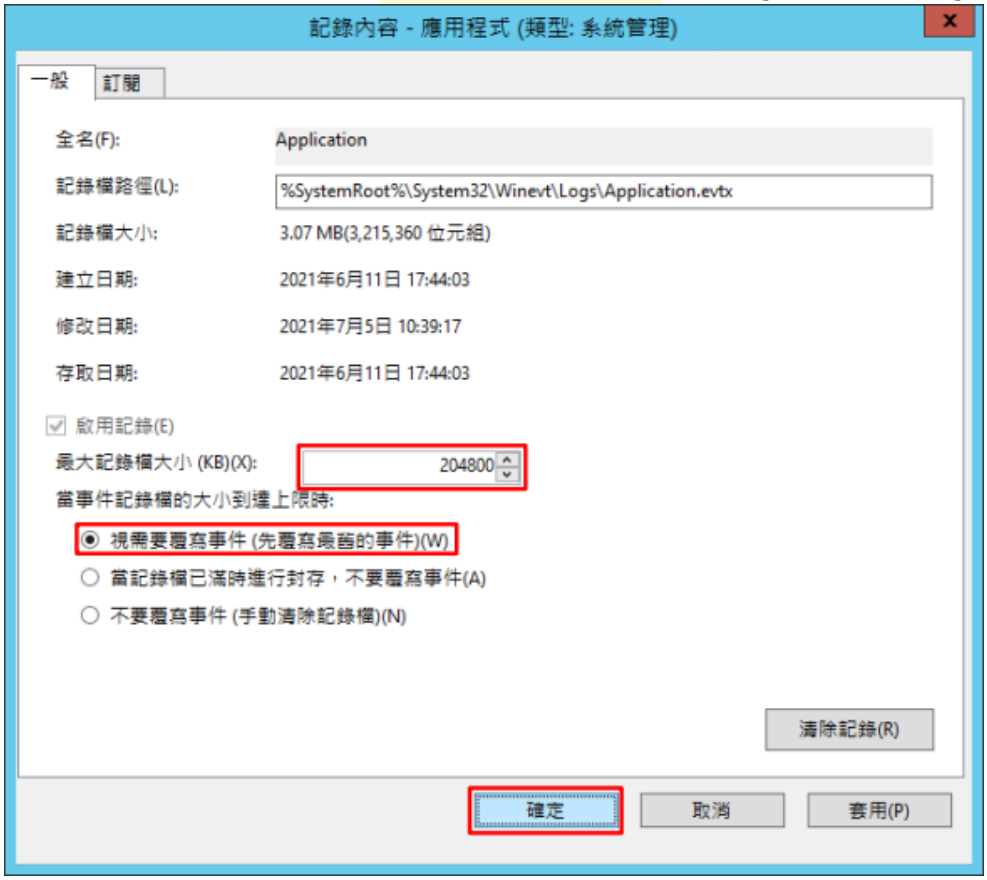
(3) 編輯安全性記錄

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



(4) 設定應用程式記錄檔

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



4 SQL2016

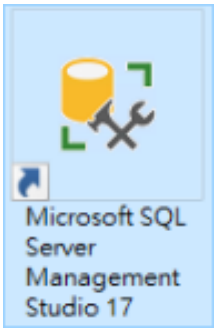
4.1 稽核登入

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

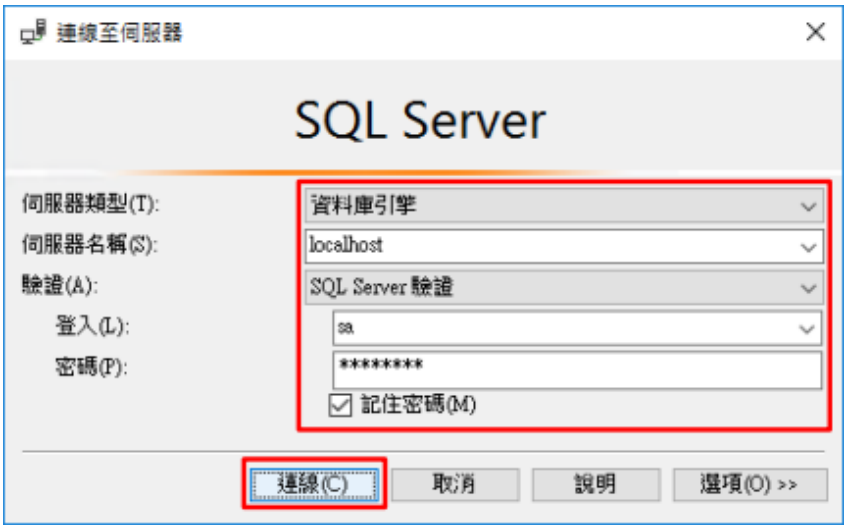
以下分別為圖形介面和指令介面設定方式。

4.1.1 使用圖形介面方式設定

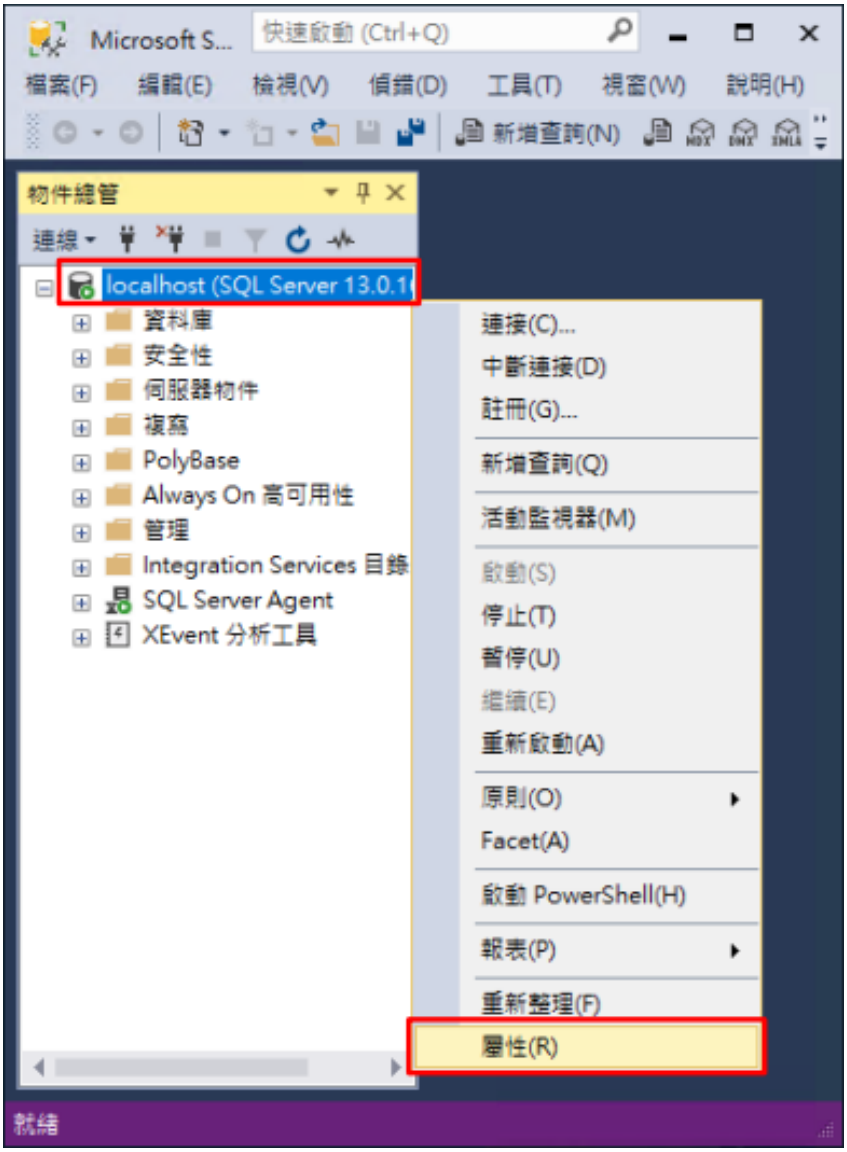
(1) 開啟 [Microsoft SQL Server Management Studio]



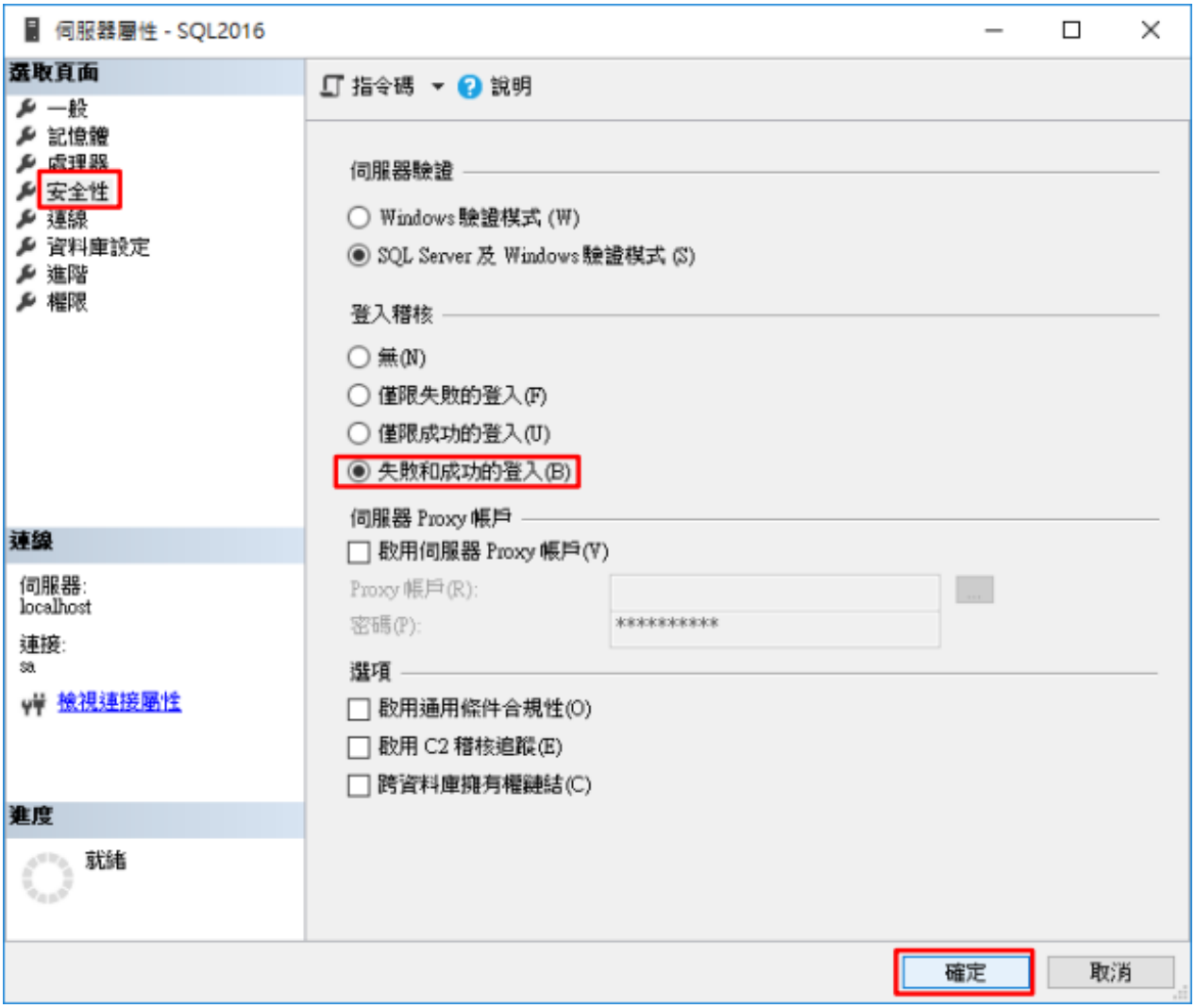
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

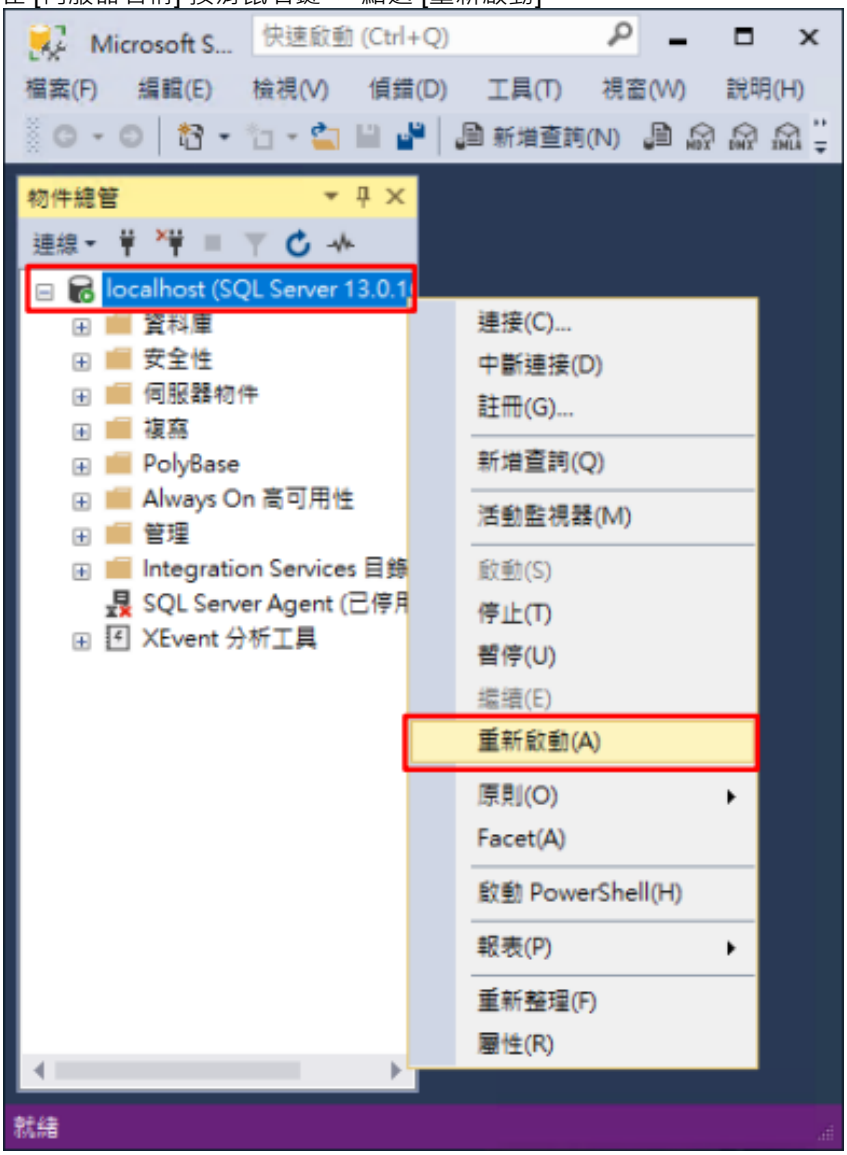


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]



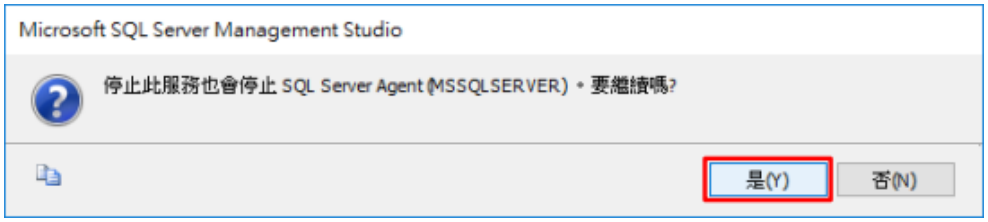
(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務

(7) 按 [是] 停止 SQL SERVER Agent 服務



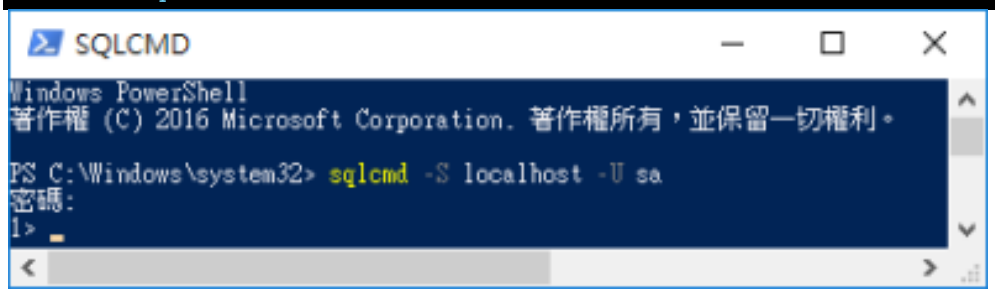
4.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

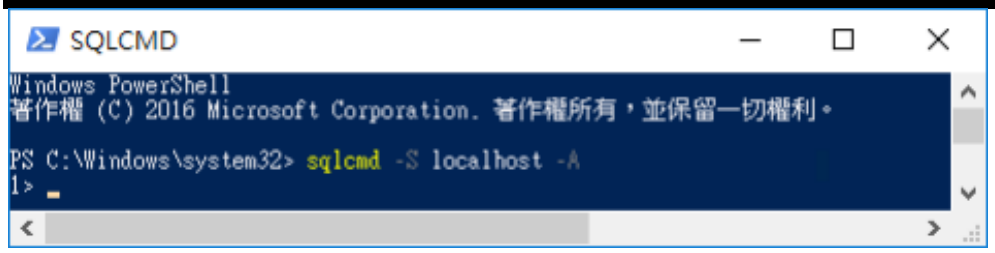
-U login_id

-P password

-A dedicated administrator connection

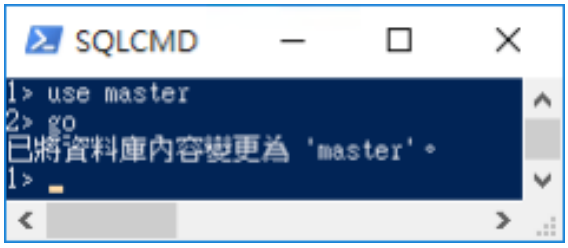
<2.2> 使用 Windows 帳號

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



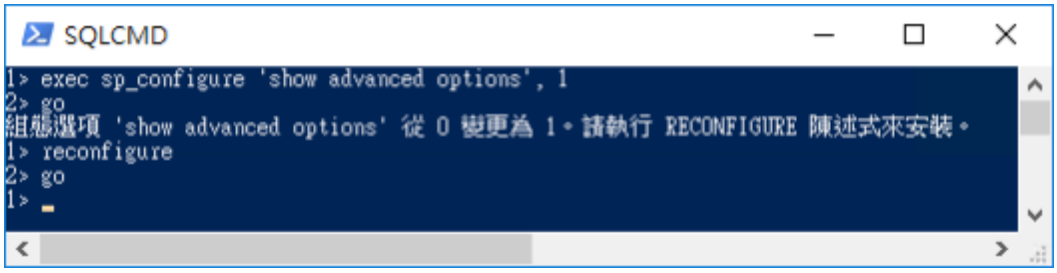
(3) 切換資料庫

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



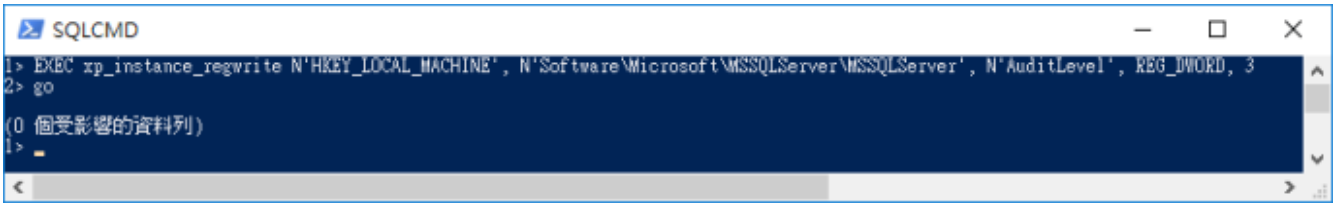
(4) 使用 sp_configure 列出進階選項

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



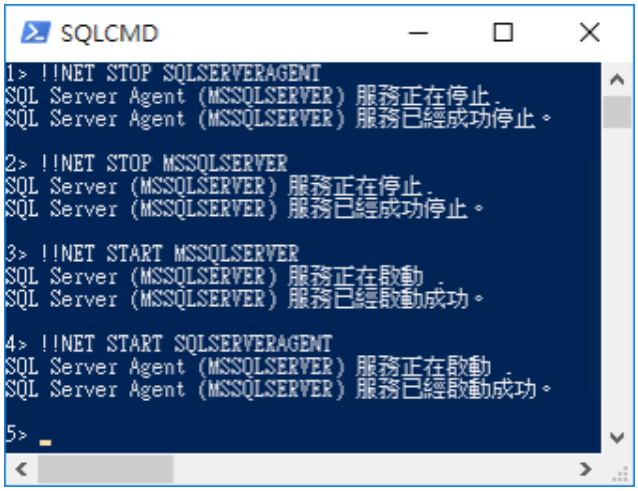
(5) 啟用失敗和成功的登入記錄

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



(6) 重新啟動 MS SQL SERVER 服務

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



4.2 設定稽核

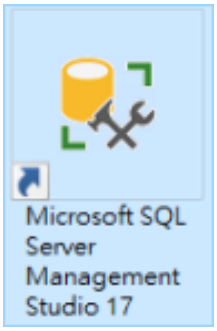
4.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

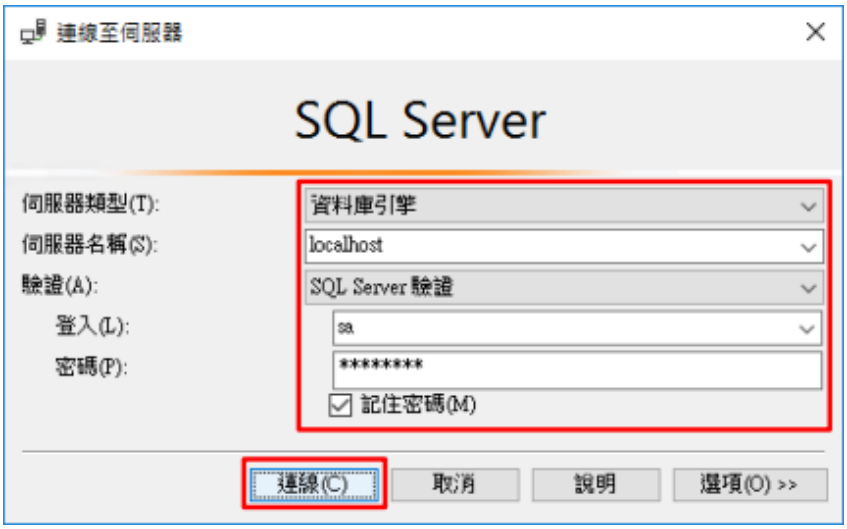
以下分別為圖形介面和指令介面設定方式。

4.2.1.1 使用圖形介面方式設定

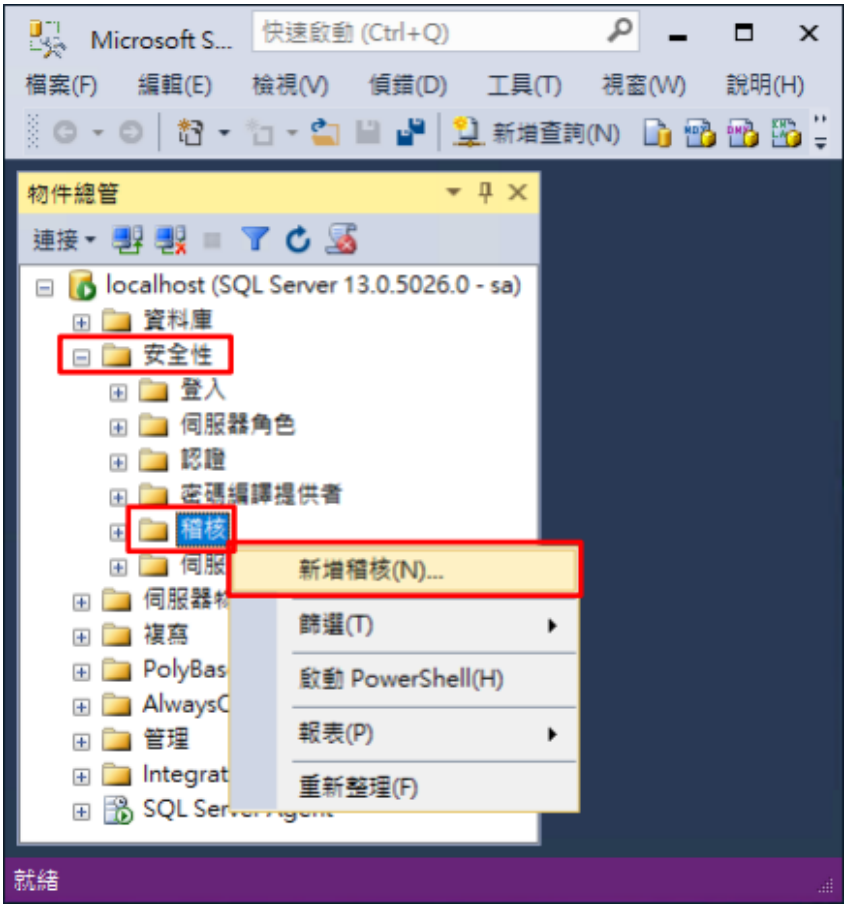
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

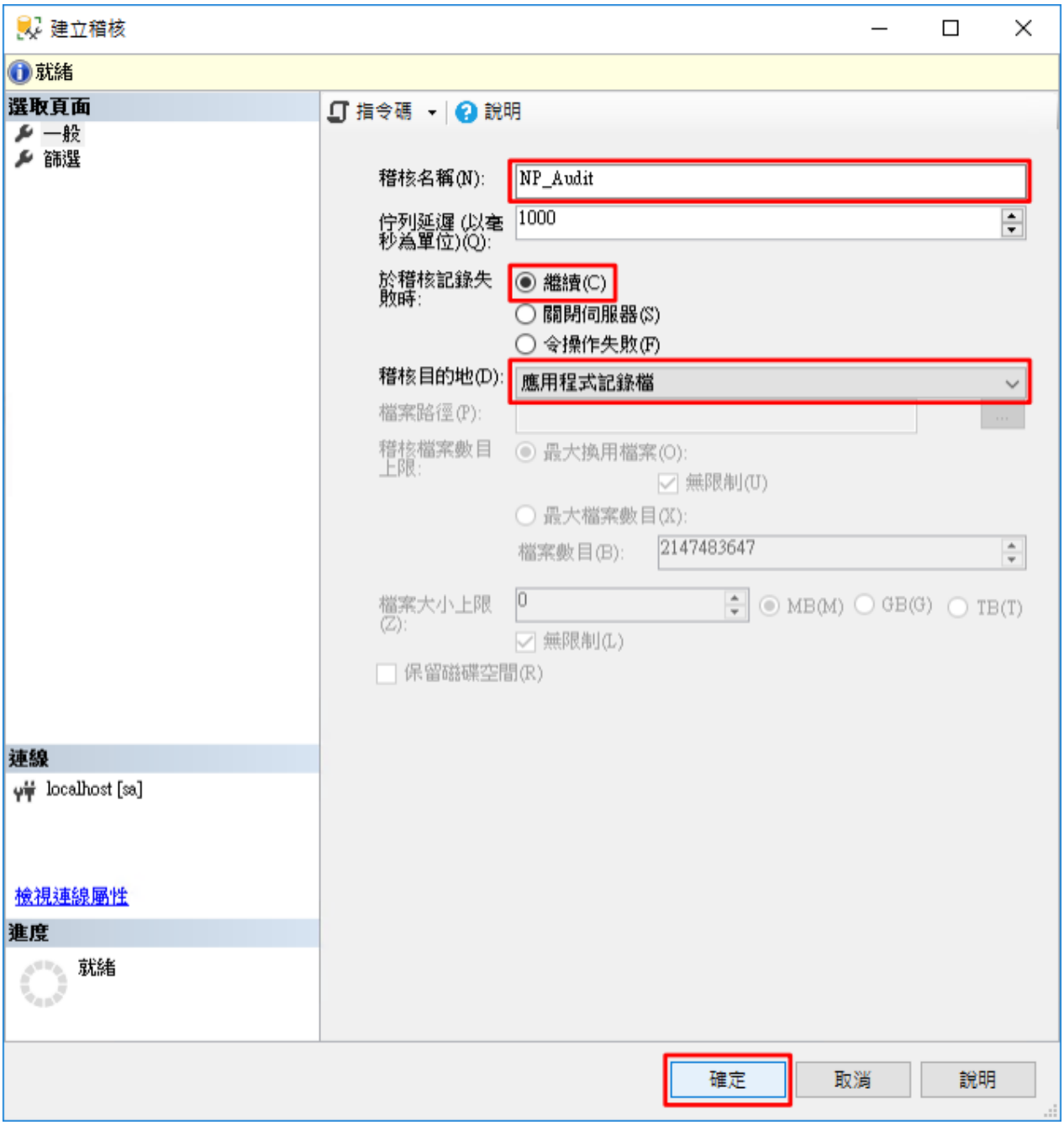


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

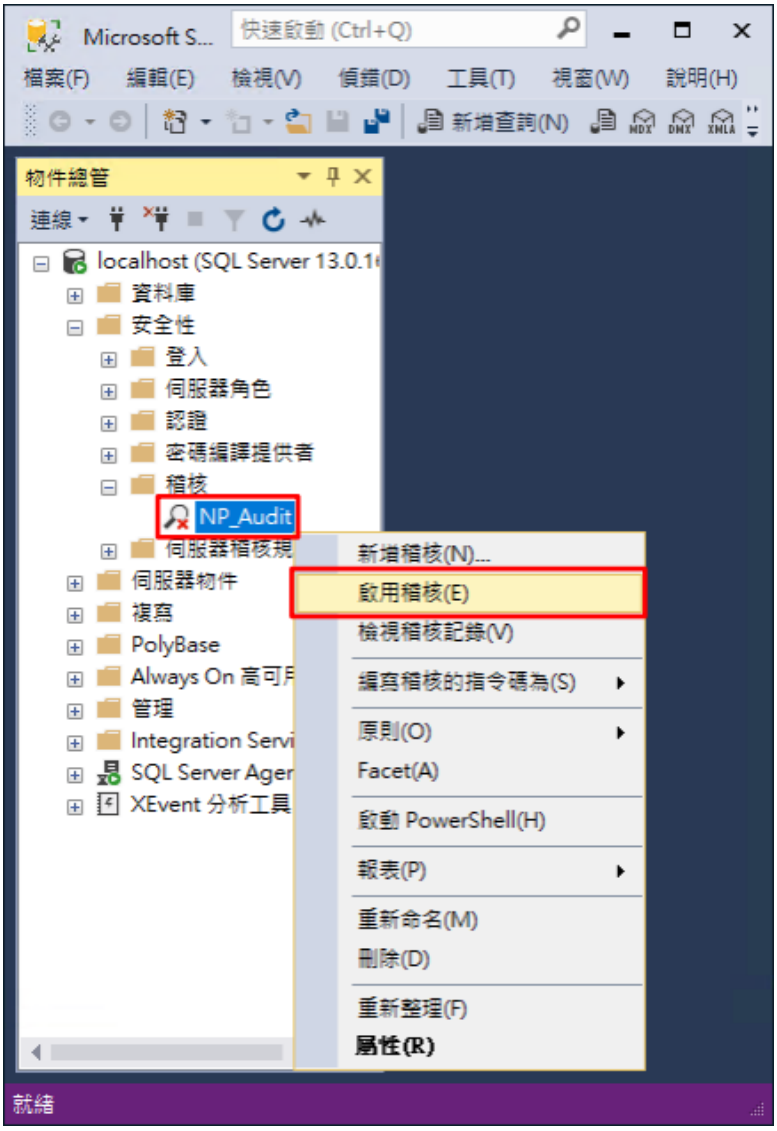


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

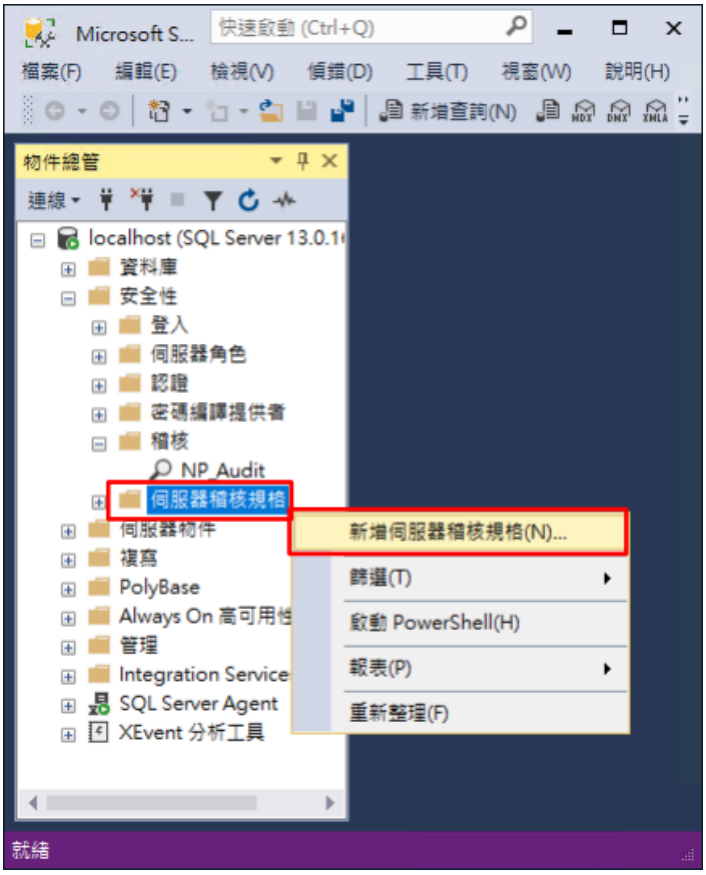


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]

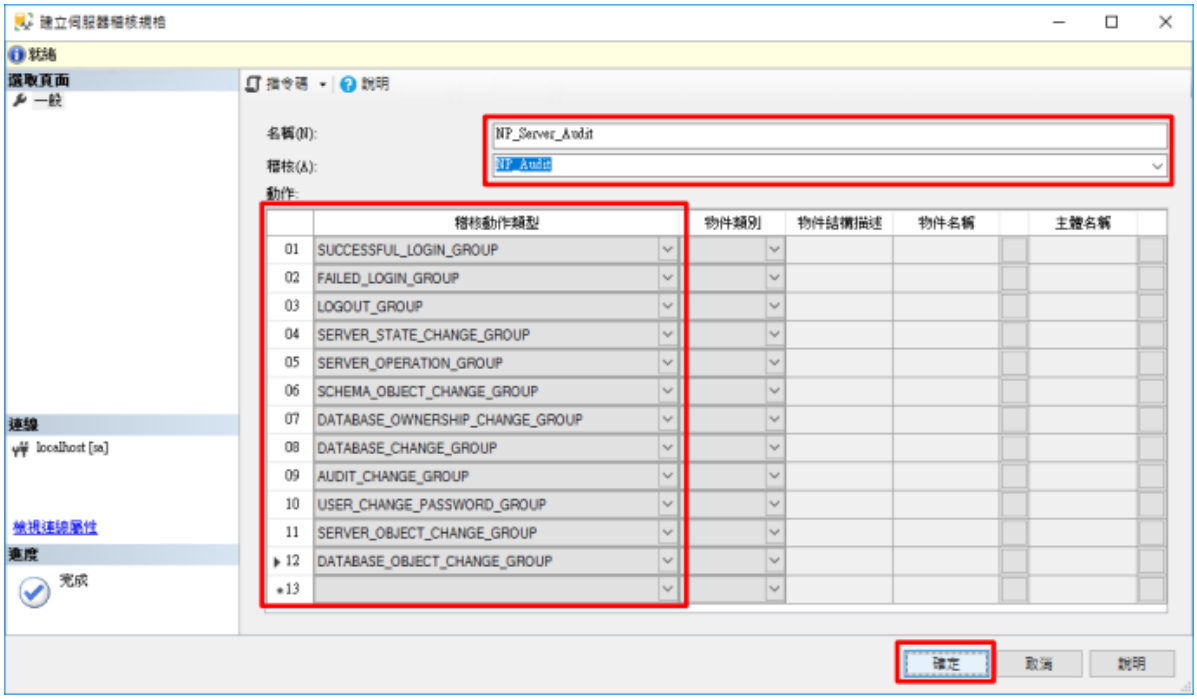


(6)　按 [關閉]

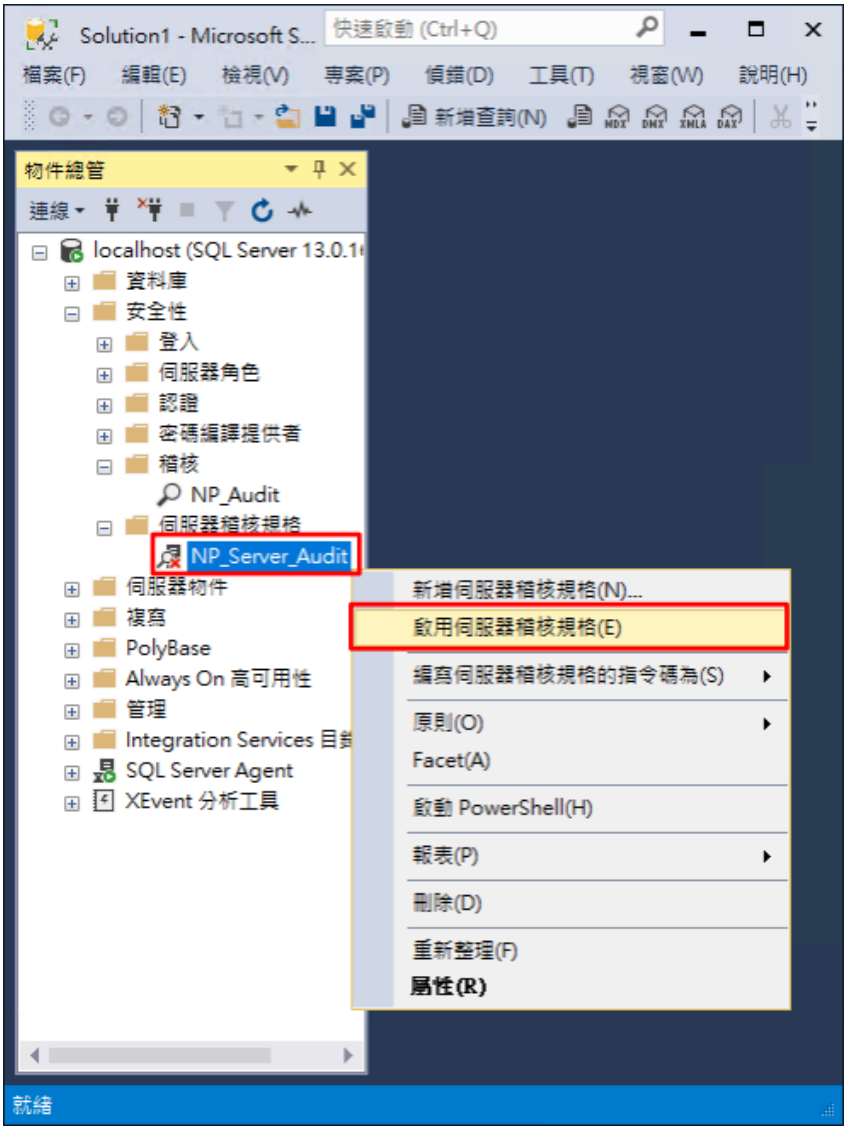
(7)　在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



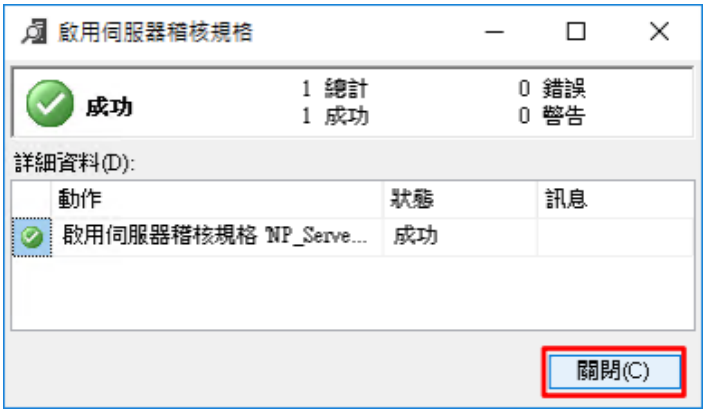
(8)　輸入名稱:　`NP_Server_Audit`　-> 選擇稽核: [NP_Audit] 和動作 詳細說明請參考前言的稽核動作群組連結 **-> 按 [確定]**



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



(10)　按 [關閉]



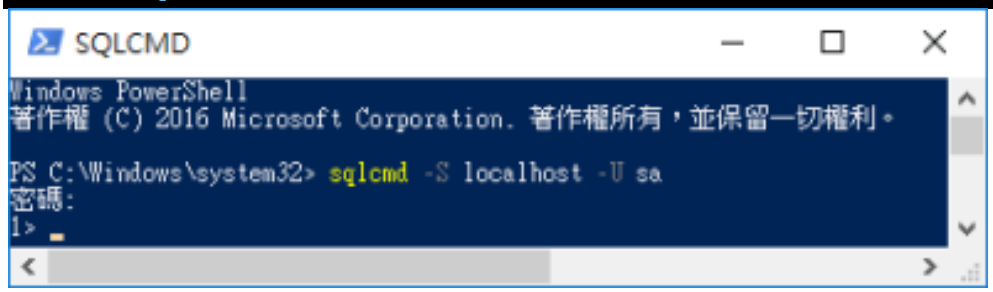
4.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

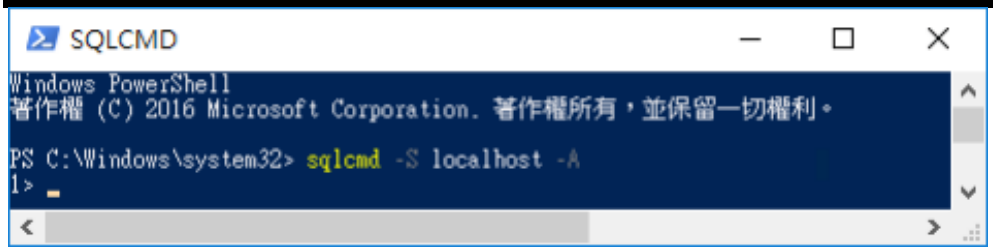
-U login_id

-P password

-A dedicated administrator connection

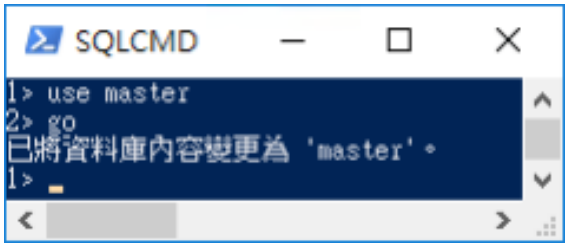
<2.2> 使用 Windows 帳號

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



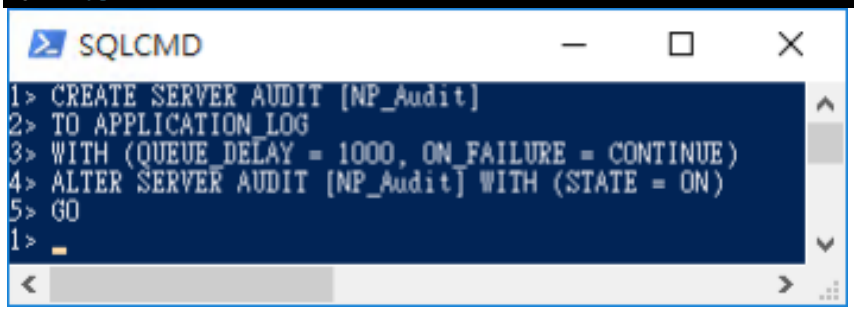
(3) 切換資料庫

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



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

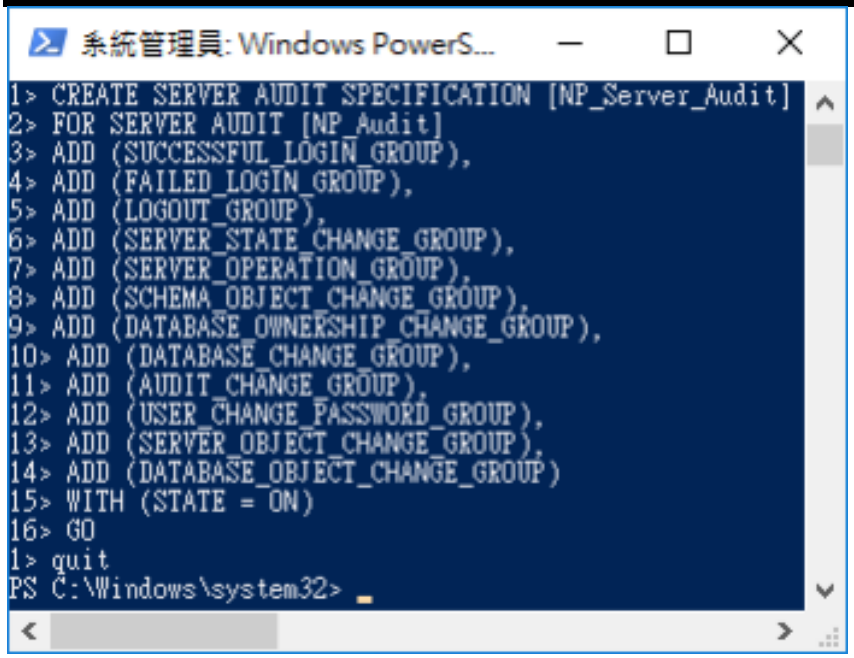
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



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
```



紅色文字部位請輸入伺服器稽核規格名稱

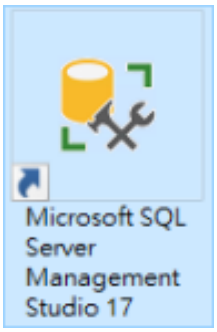
4.2.2 稽核資料庫層級

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

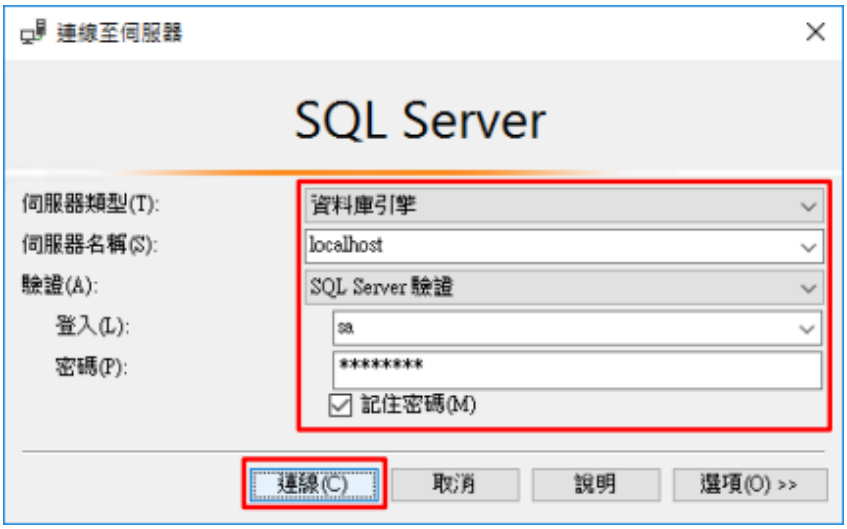
以下分別為圖形介面和指令介面設定方式。

4.2.2.1 使用圖形介面方式設定

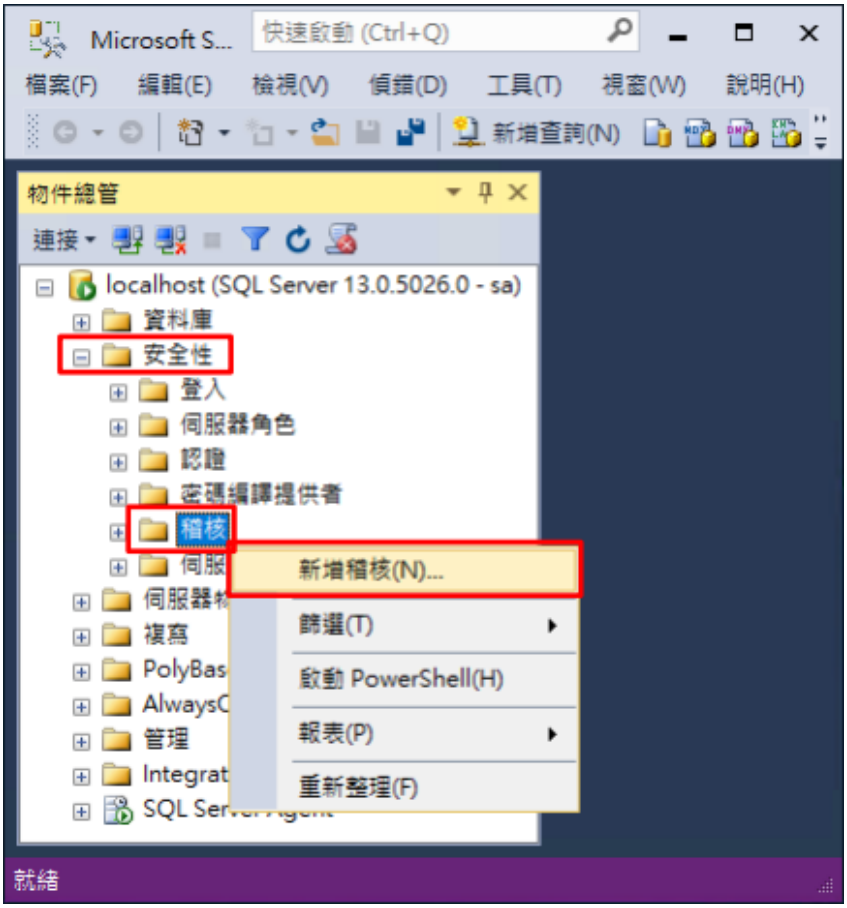
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

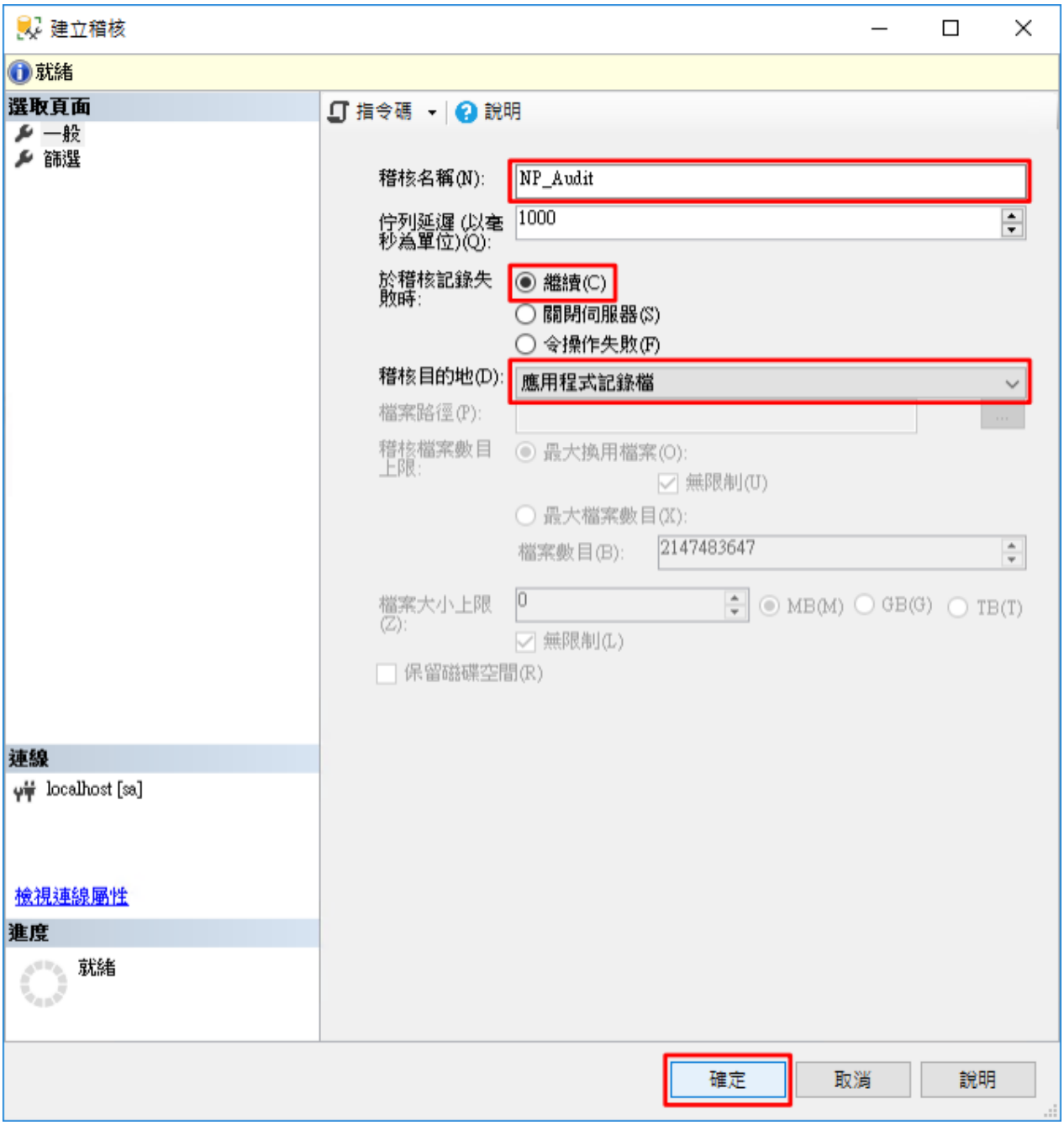


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

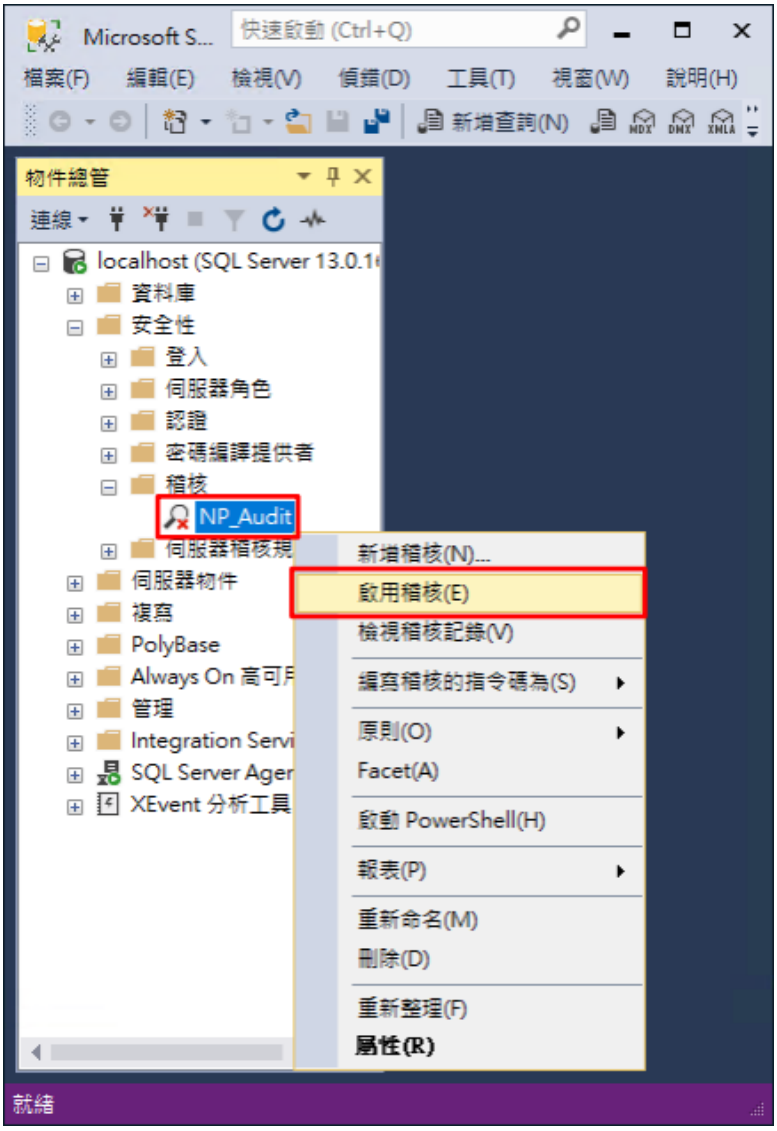


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]



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

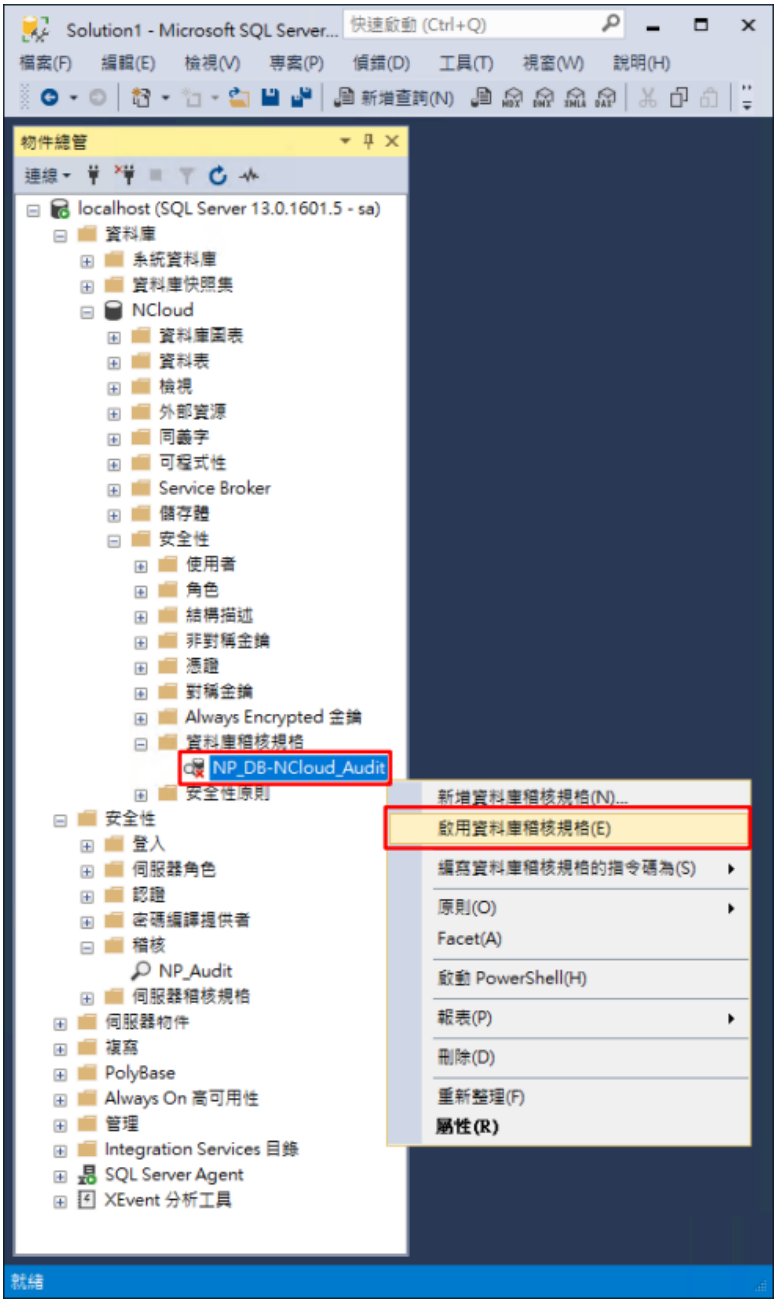


(6)　按 [關閉]

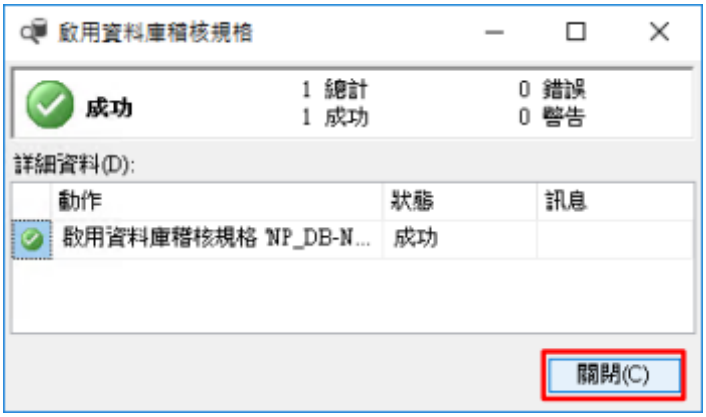
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]

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

(9)　在資料庫稽核規格名稱: [NP_DB-NCloud_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10)　按 [關閉]



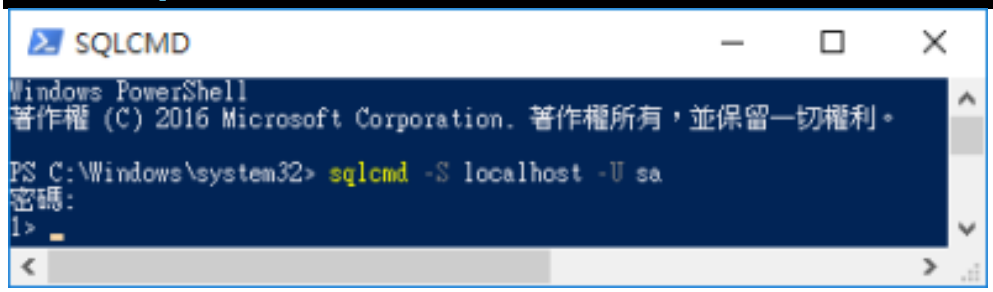
4.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

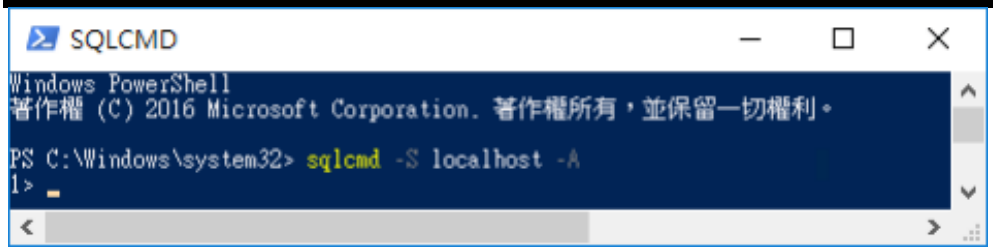
-U login_id

-P password

-A dedicated administrator connection

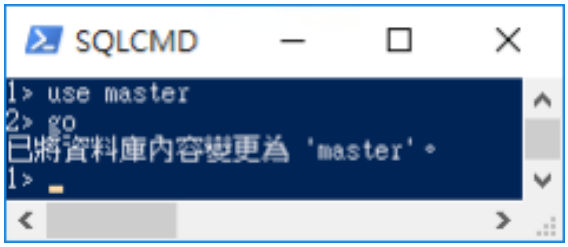
<2.2> 使用 Windows 帳號

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



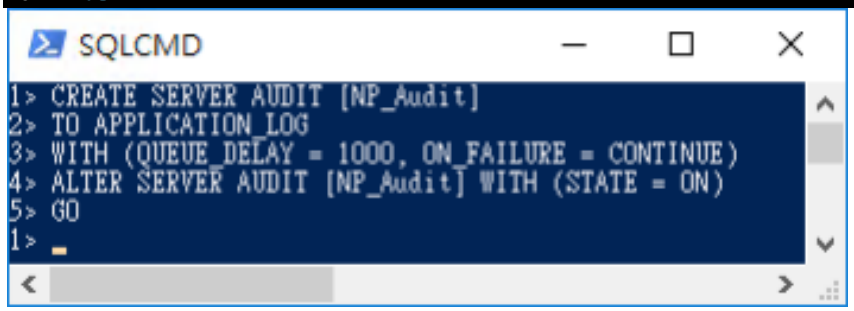
(3) 切換資料庫

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



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

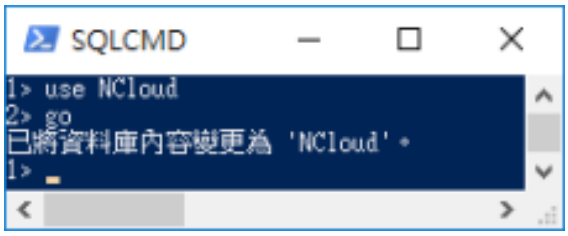
```
1 >  CREATE SERVER AUDIT [NP_Audit]
2 >  TO APPLICATION_LOG
3 >  WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 >  ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 >  GO
```



紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例： NCloud

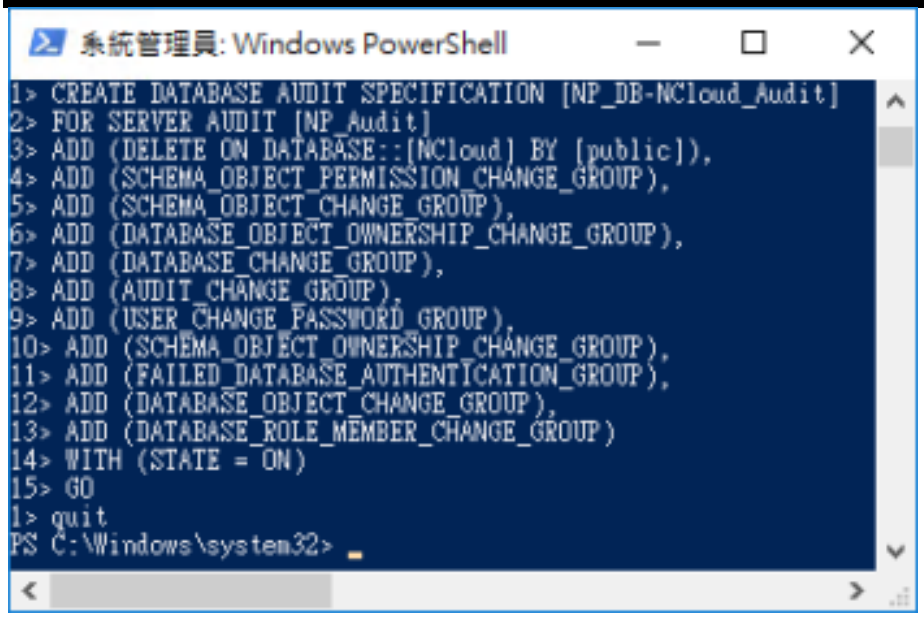
```
1 >  use NCloud
2 >  go
```



紅色文字部位請輸入稽核資料庫名稱

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

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



紅色文字部位請輸入資料庫稽核規格名稱

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

紅色文字部位請輸入稽核資料庫名稱

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

4.3 事件記錄檔設定

此為選項設定。

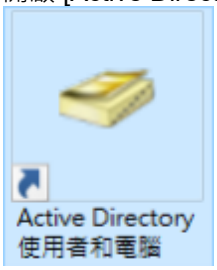
以下分別為網域和工作群組設定方式。

4.3.1 網域

4.3.1.1 組織單位設定

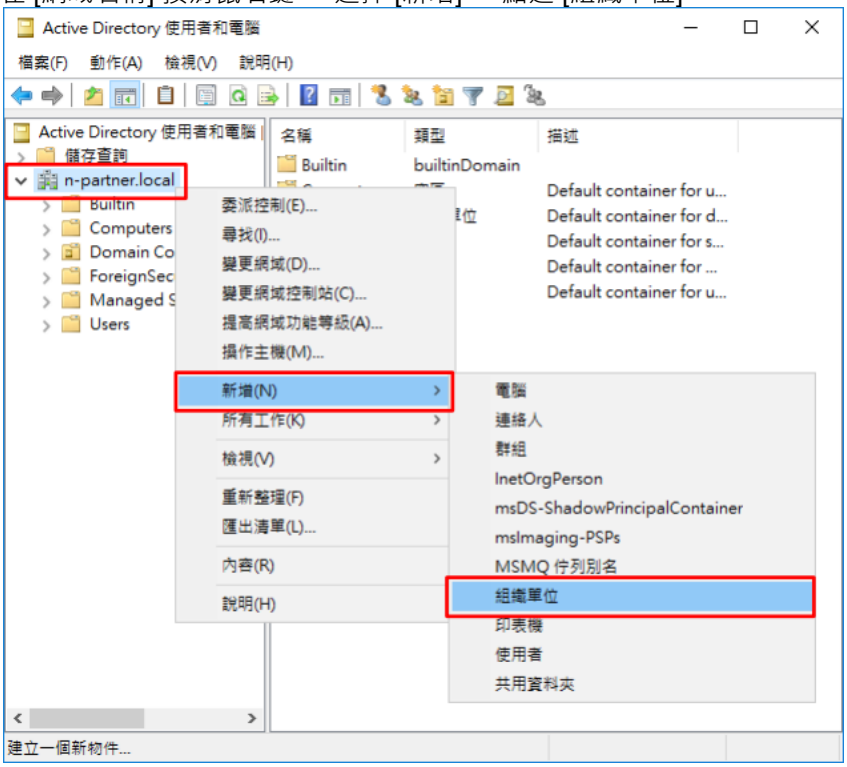
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



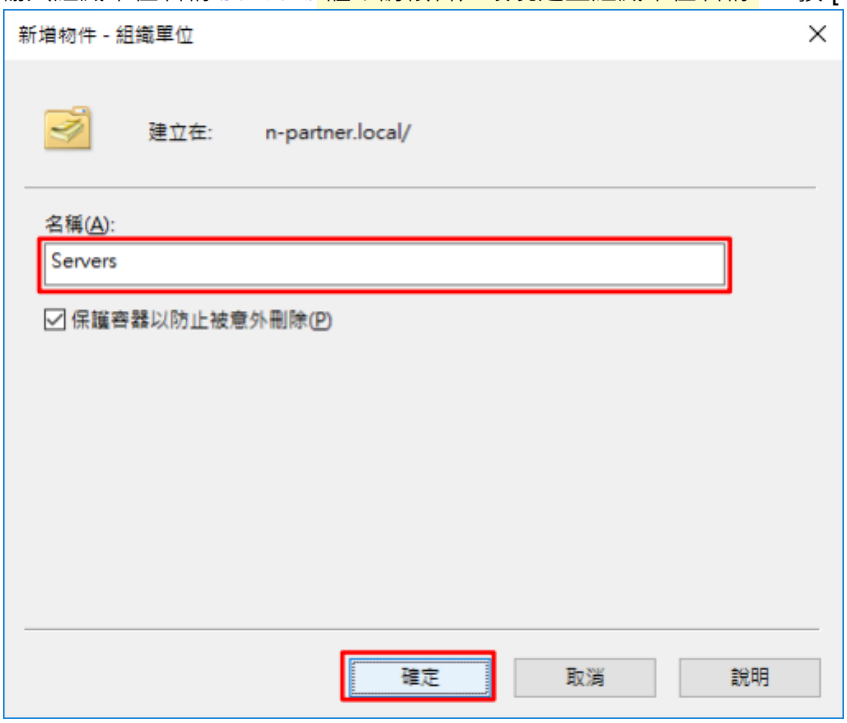
(2) 新增組織單位

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



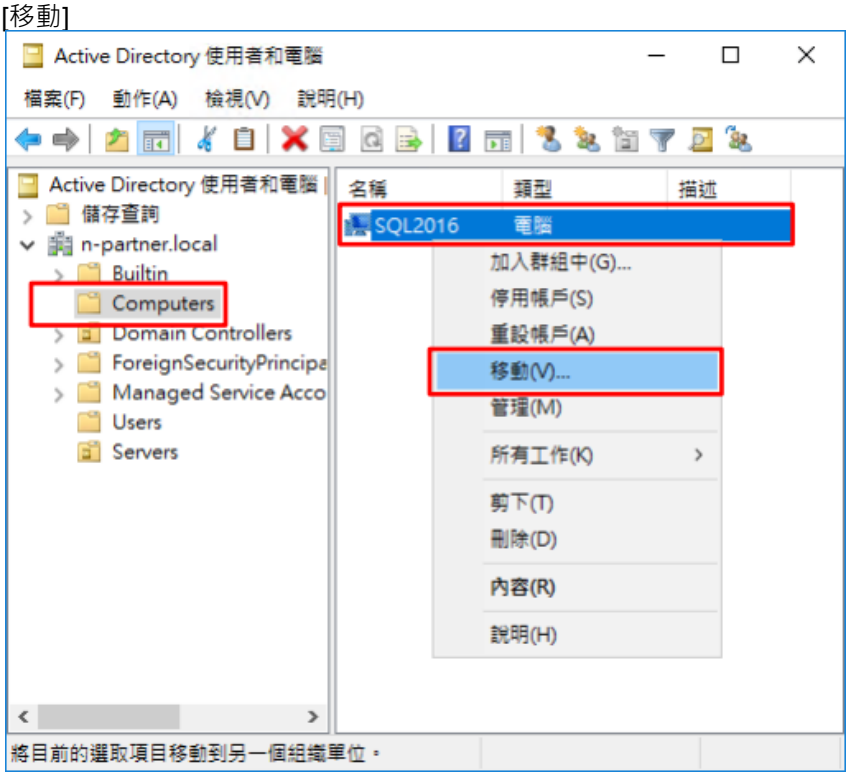
(3) 輸入組織單位名稱

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



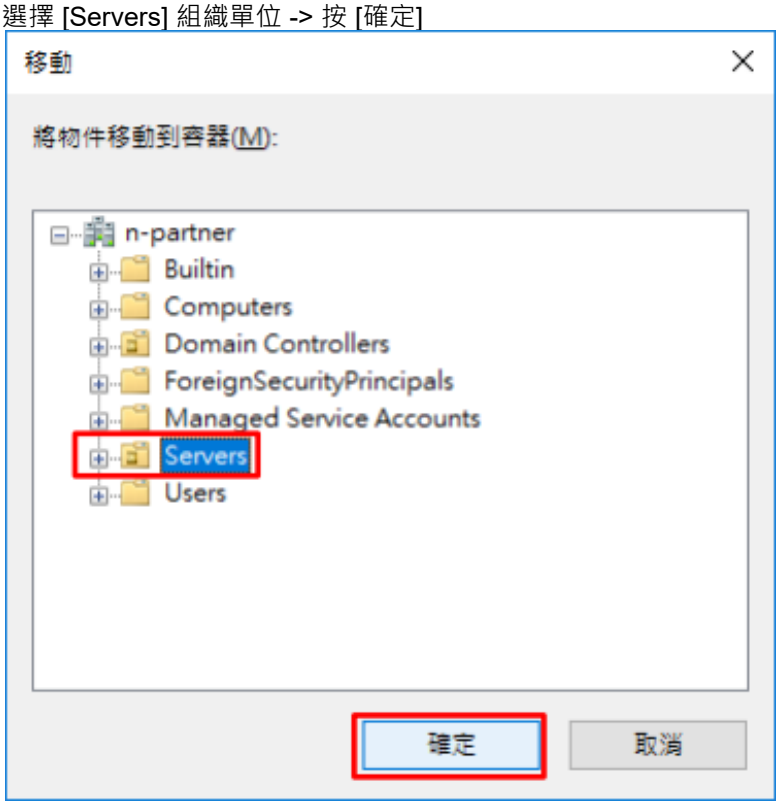
(4) 移動伺服器至新的組織單位

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



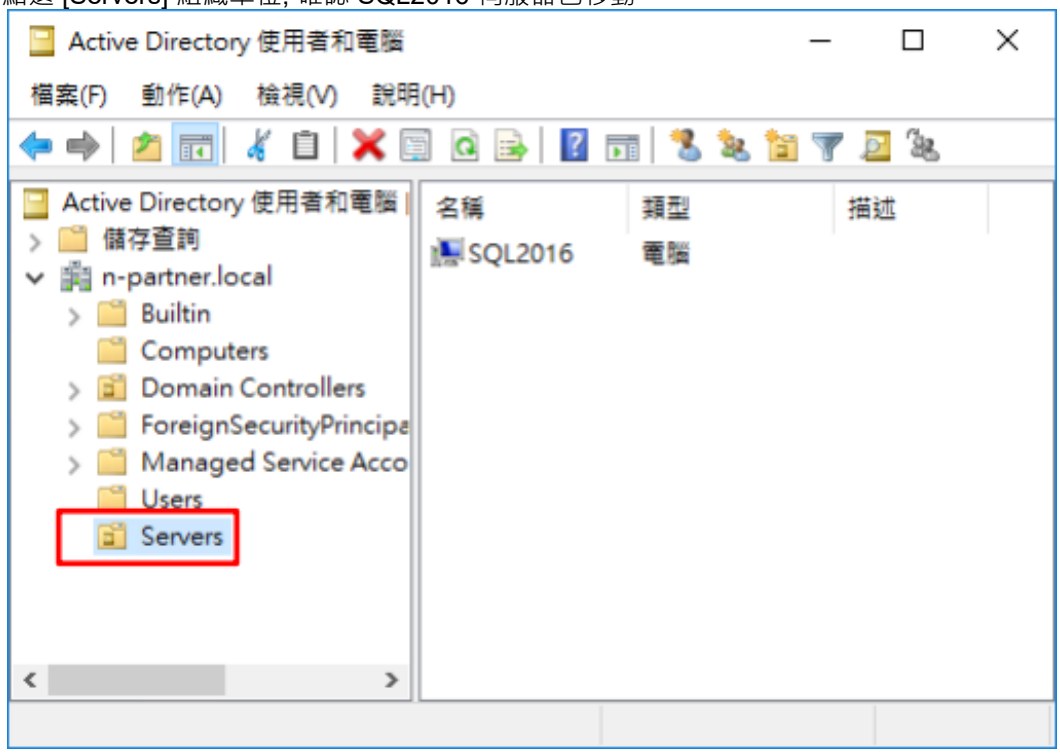
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

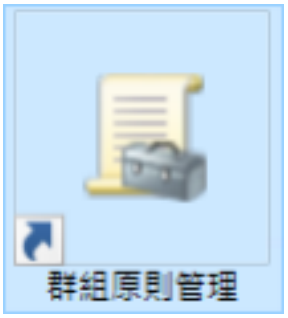
點選 [Servers] 組織單位, 確認 SQL2016 伺服器已移動。



4.3.1.2 群組原則設定

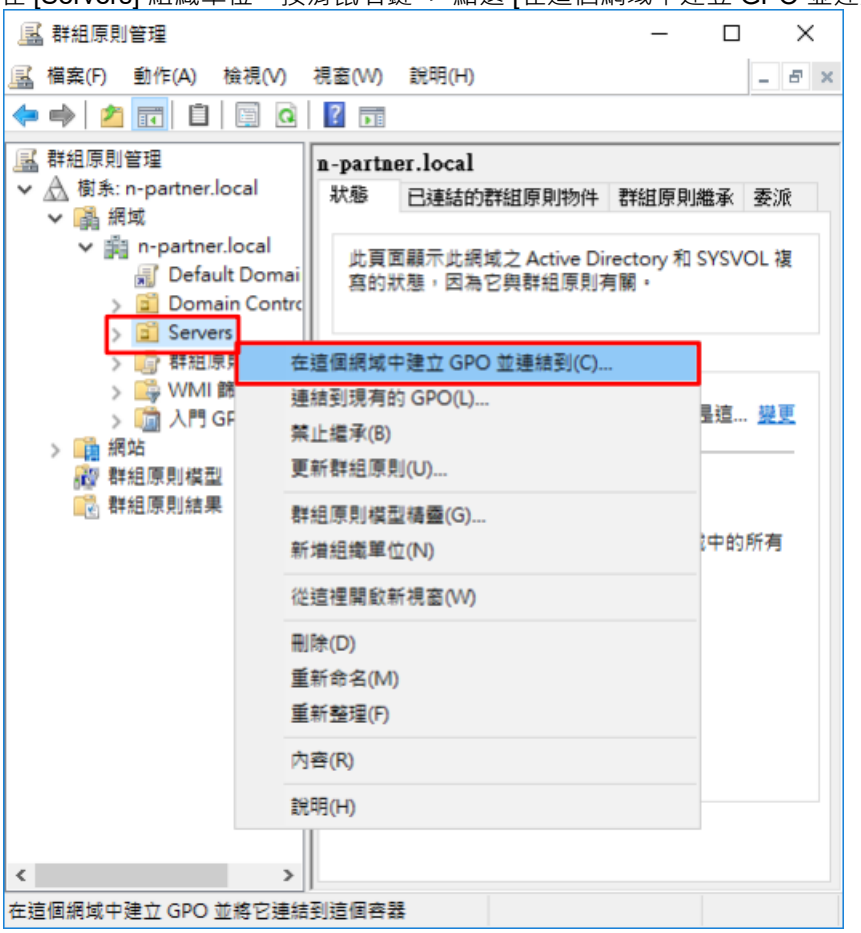
(1) 開啟群組原則管理

開啟 [群組原則管理]



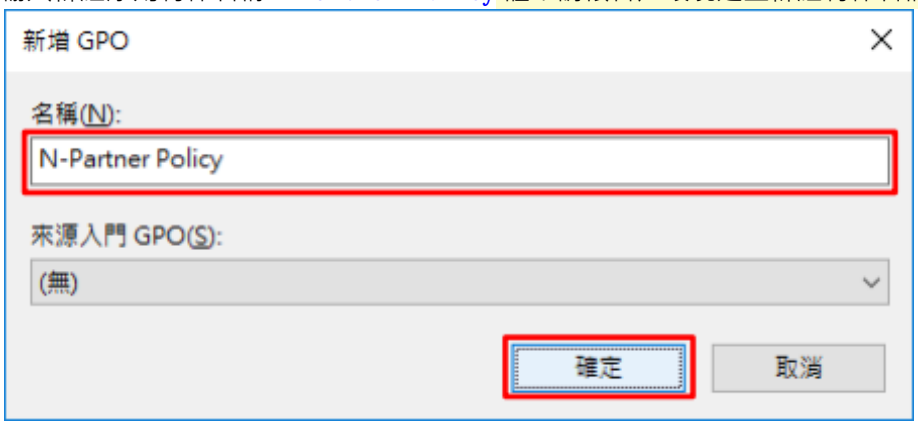
(2) 在 Servers 組織單位，新增群組原則物件

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



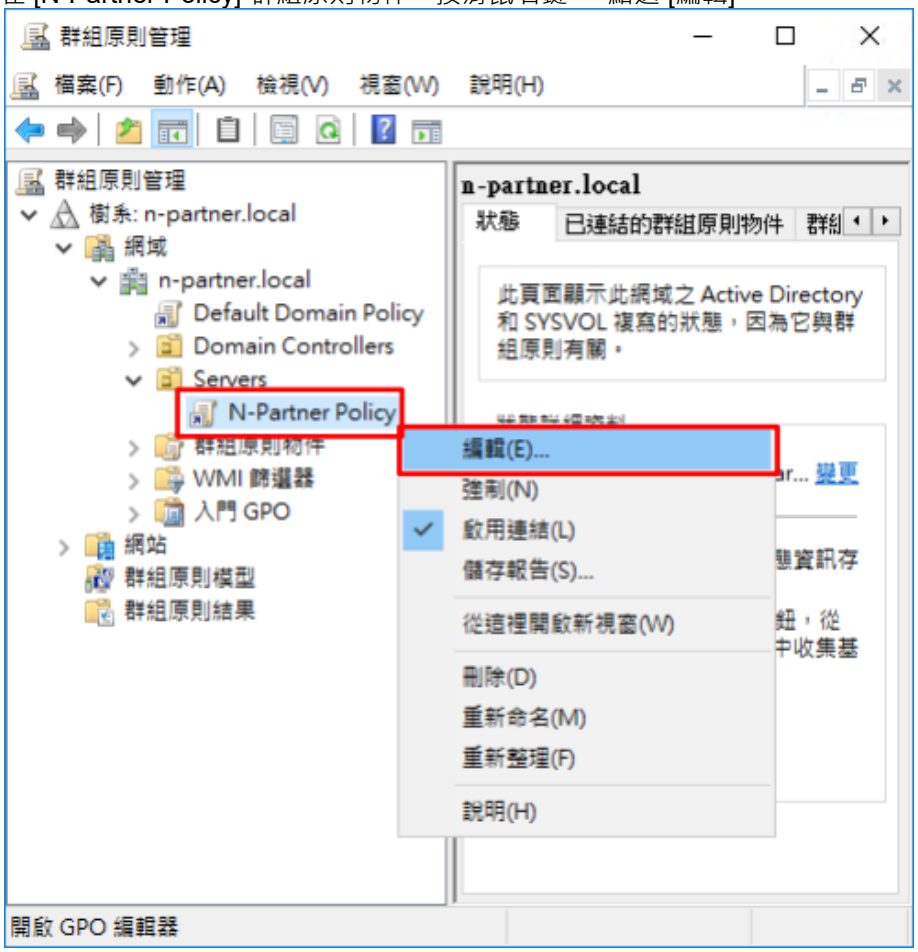
(3) 輸入群組原則物件名稱

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



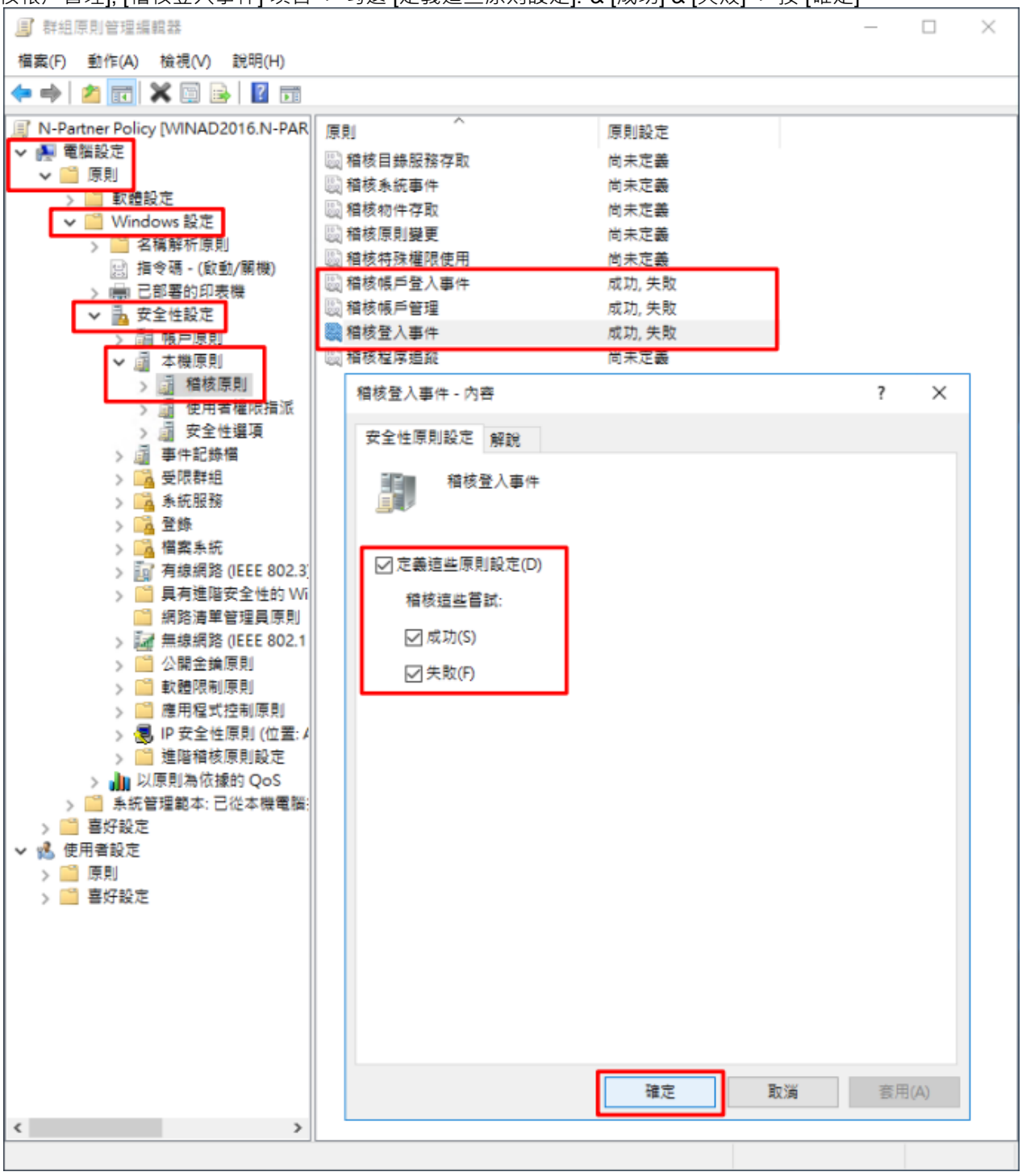
(4) 編輯群組原則物件

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



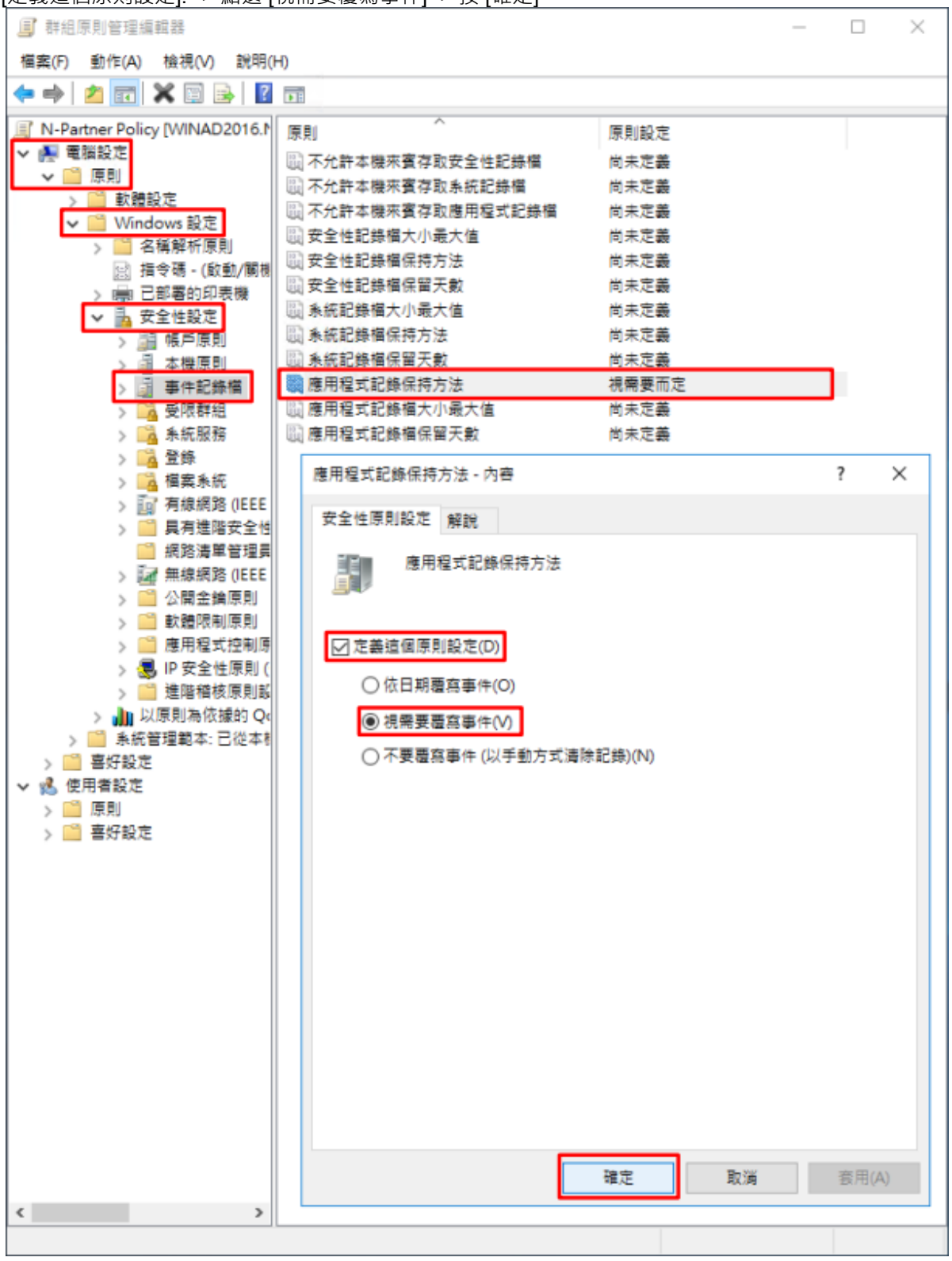
(5) 本機原則：稽核原則

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



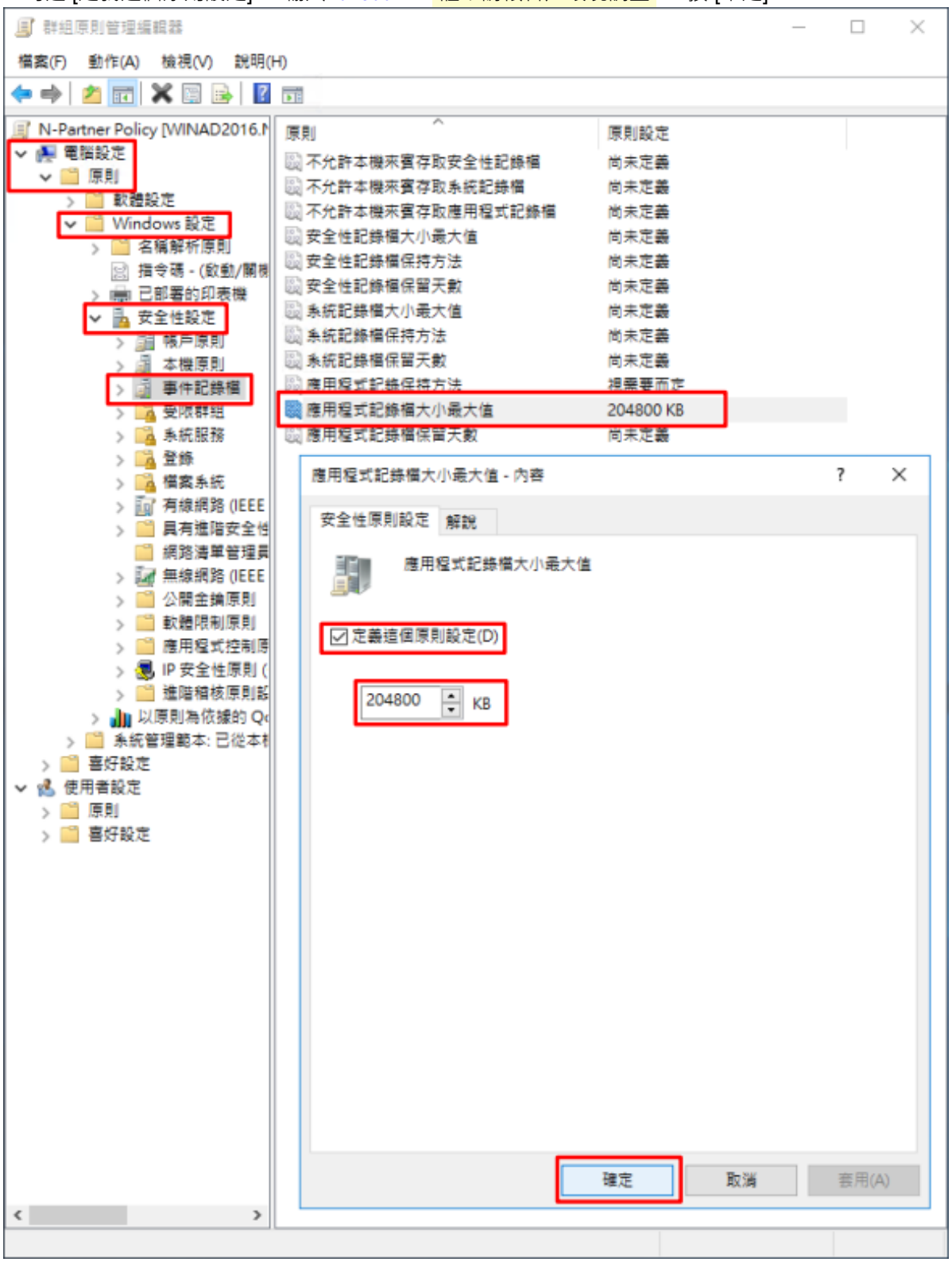
(6) 事件記錄：應用程式記錄保持方法

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



(7) 事件記錄：應用程式記錄檔大小最大值

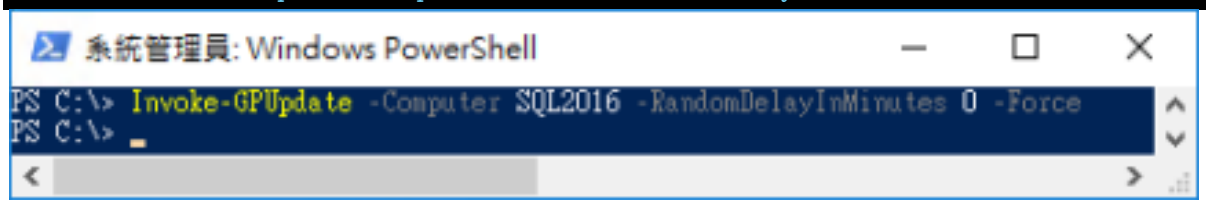
展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄檔大小最大值] 項目 -> 勾選 [定義這個原則設定] -> 輸入204800 KB 註：請依客戶環境調整 -> 按 [確定]



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

(9) 更新 MS SQL Server 群組原則

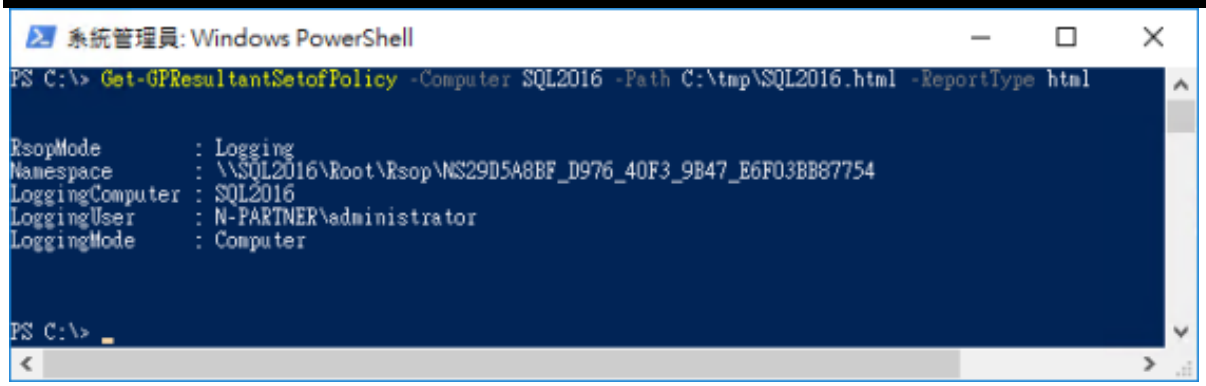
```
PS C:\> Invoke-GPUpdate -Computer SQL2016 -RandomDelayInMinutes 0 -Force
```



紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表

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

4.3.2 工作群組

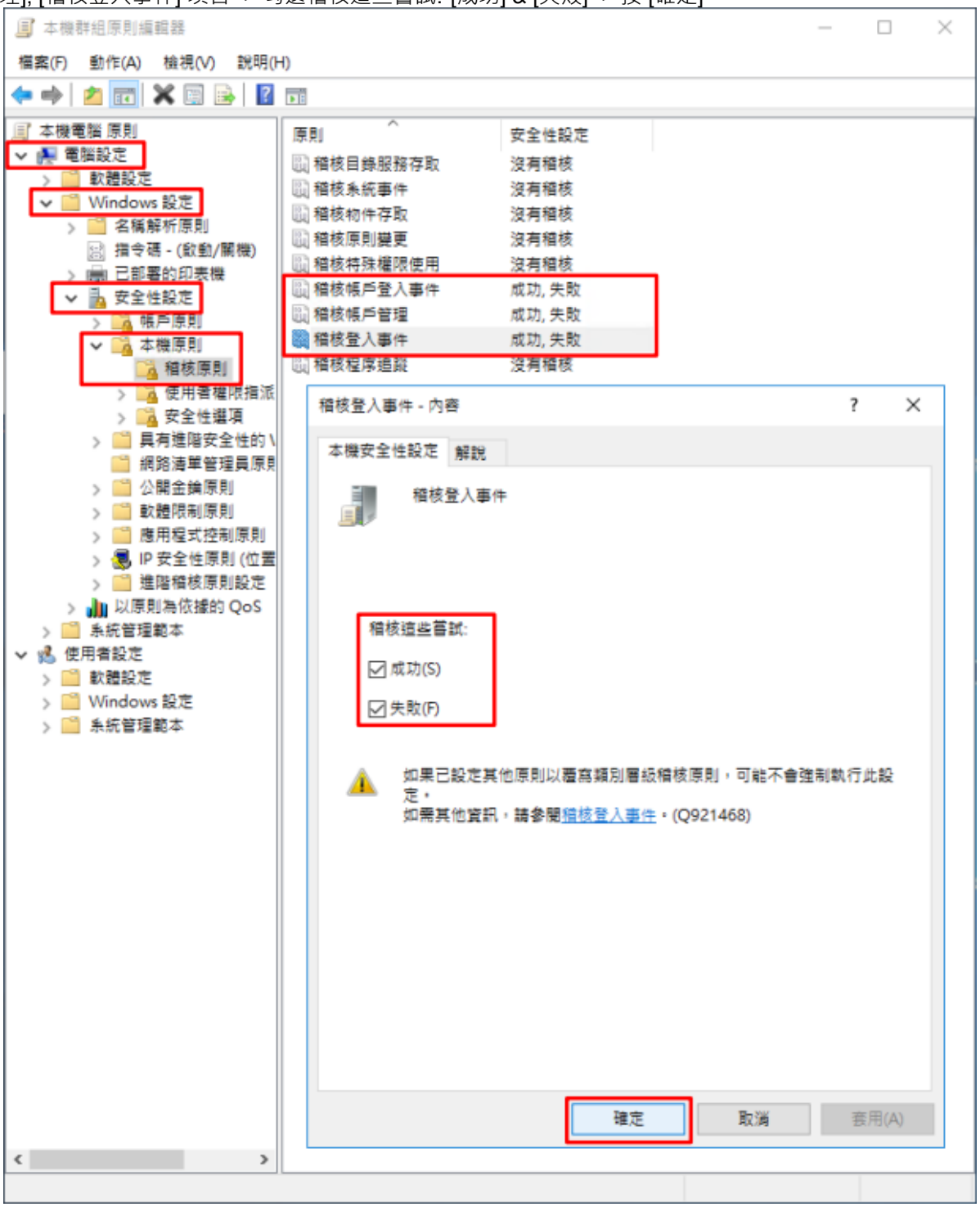
4.3.2.1 稽核原則設定

(1) 開啟 [本機群組原則編輯器]

點選 [搜尋] -> 輸入群組原則 -> 點選 [編輯群組原則]

(2) 本機原則：稽核原則

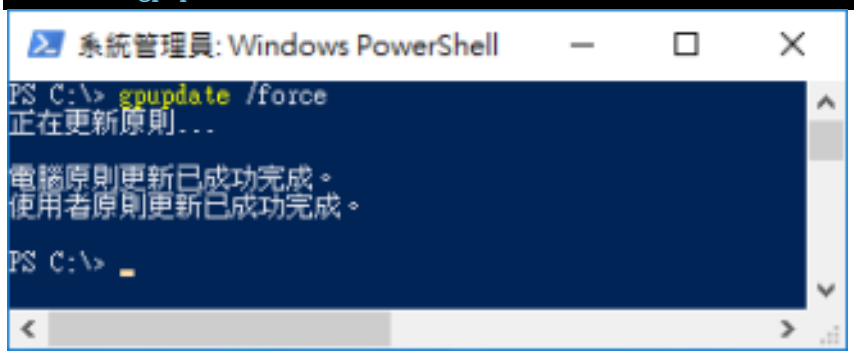
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

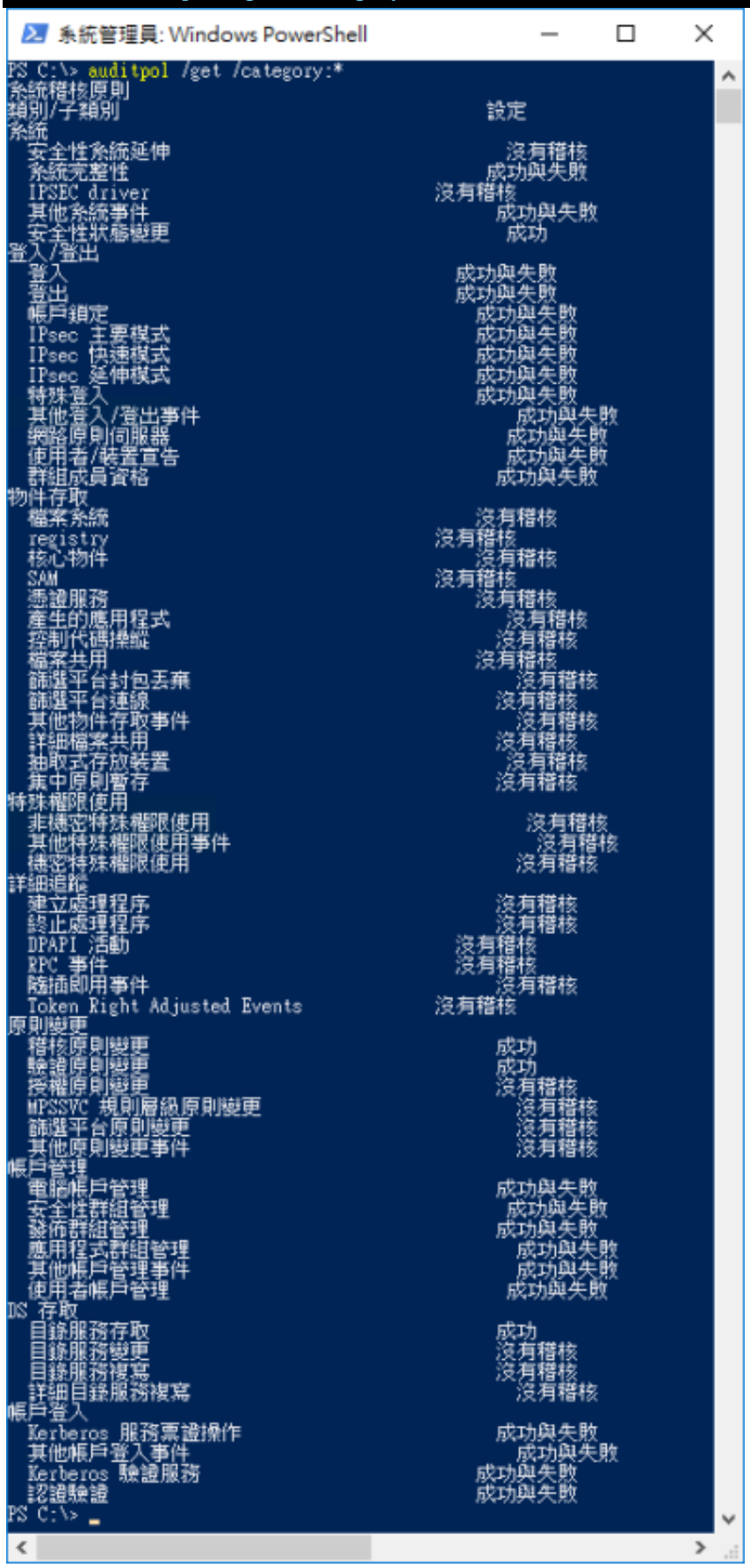
(4) 更新群組原則

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



(5) 查看群組原則套用情形

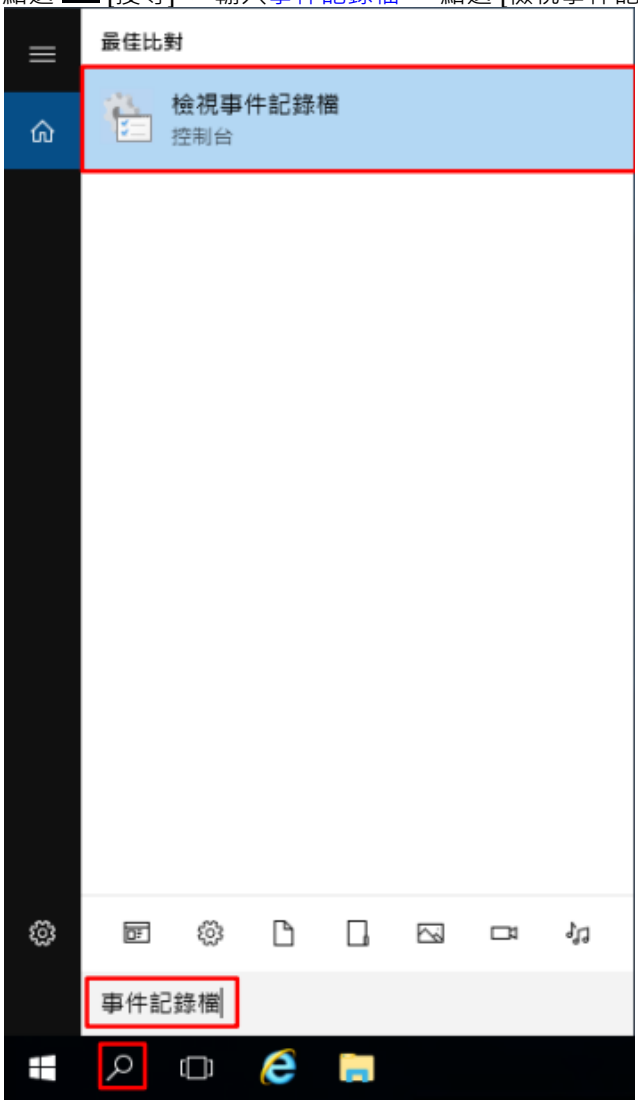
```
PS C:\> auditpol /get /category:*
```



4.3.2.2 事件檔案設定

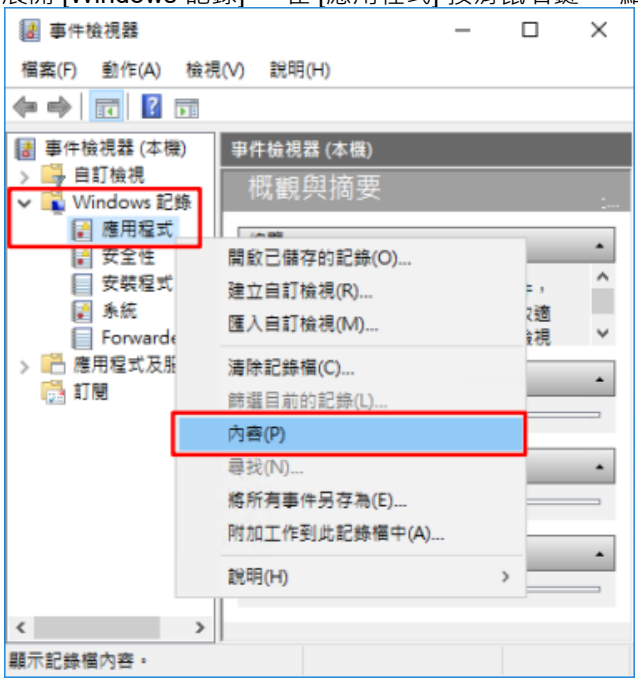
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入事件記錄檔 -> 點選 [檢視事件記錄檔]



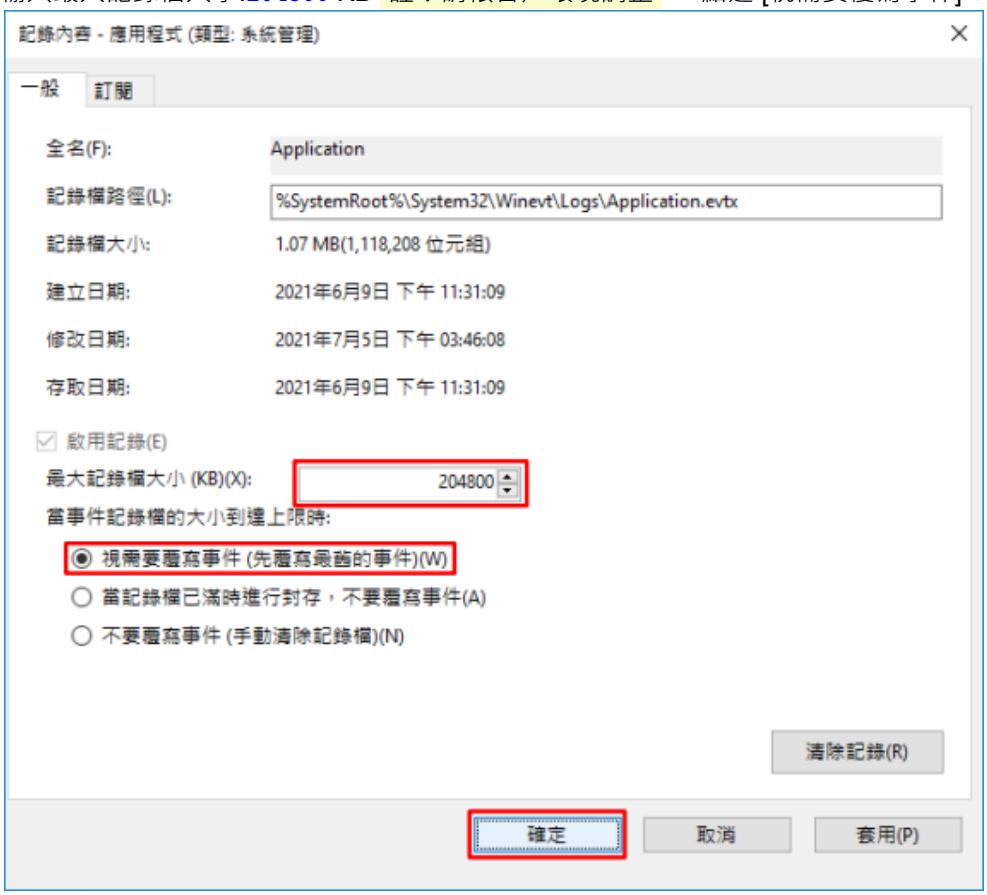
(2) 編輯安全性記錄

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



(3) 設定應用程式記錄檔

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



5 SQL2019

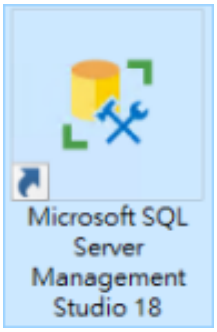
5.1 稽核登入

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

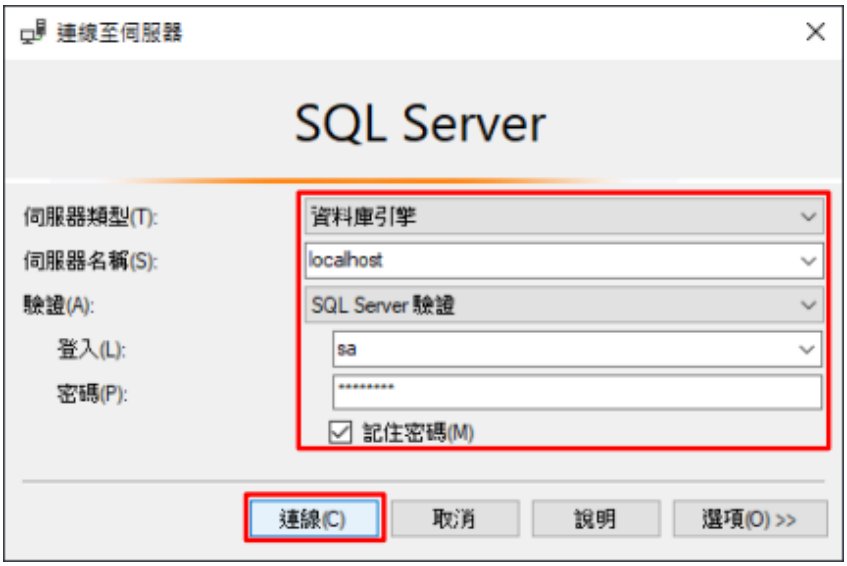
以下分別為圖形介面和指令介面設定方式。

5.1.1 使用圖形介面方式設定

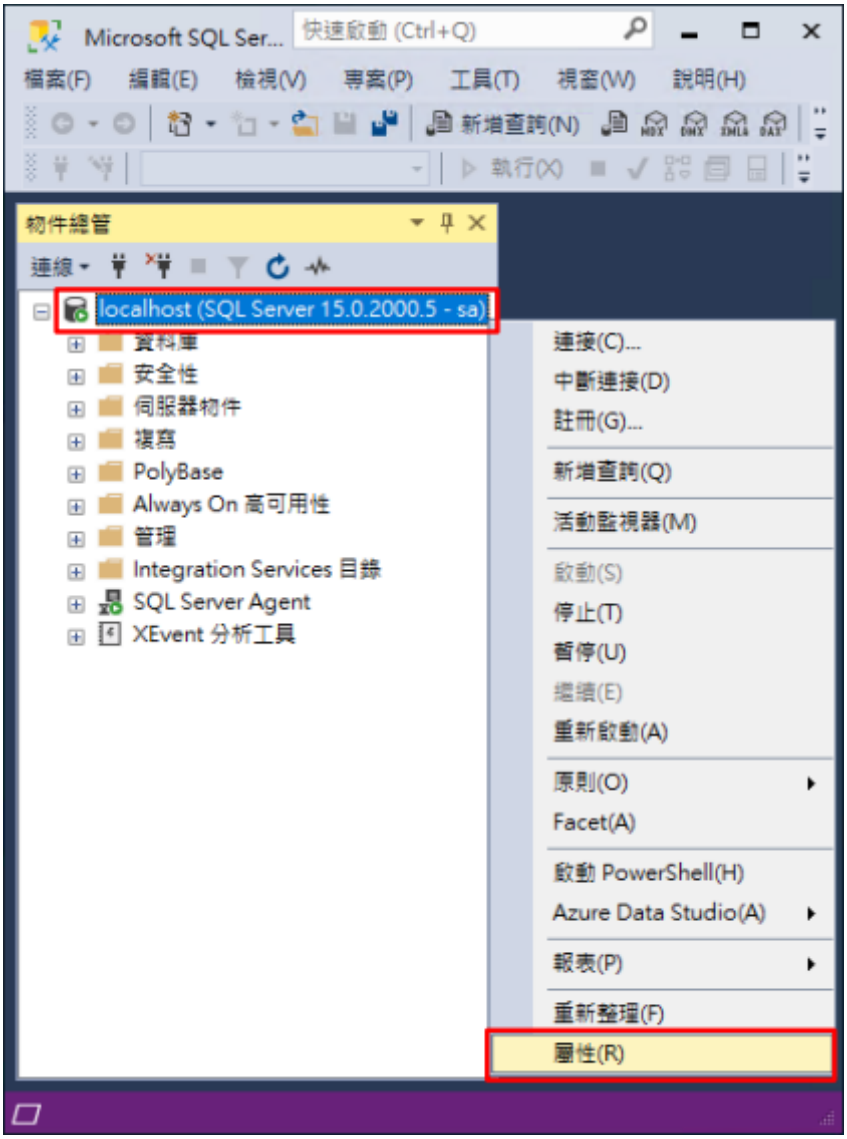
(1) 開啟 [Microsoft SQL Server Management Studio]



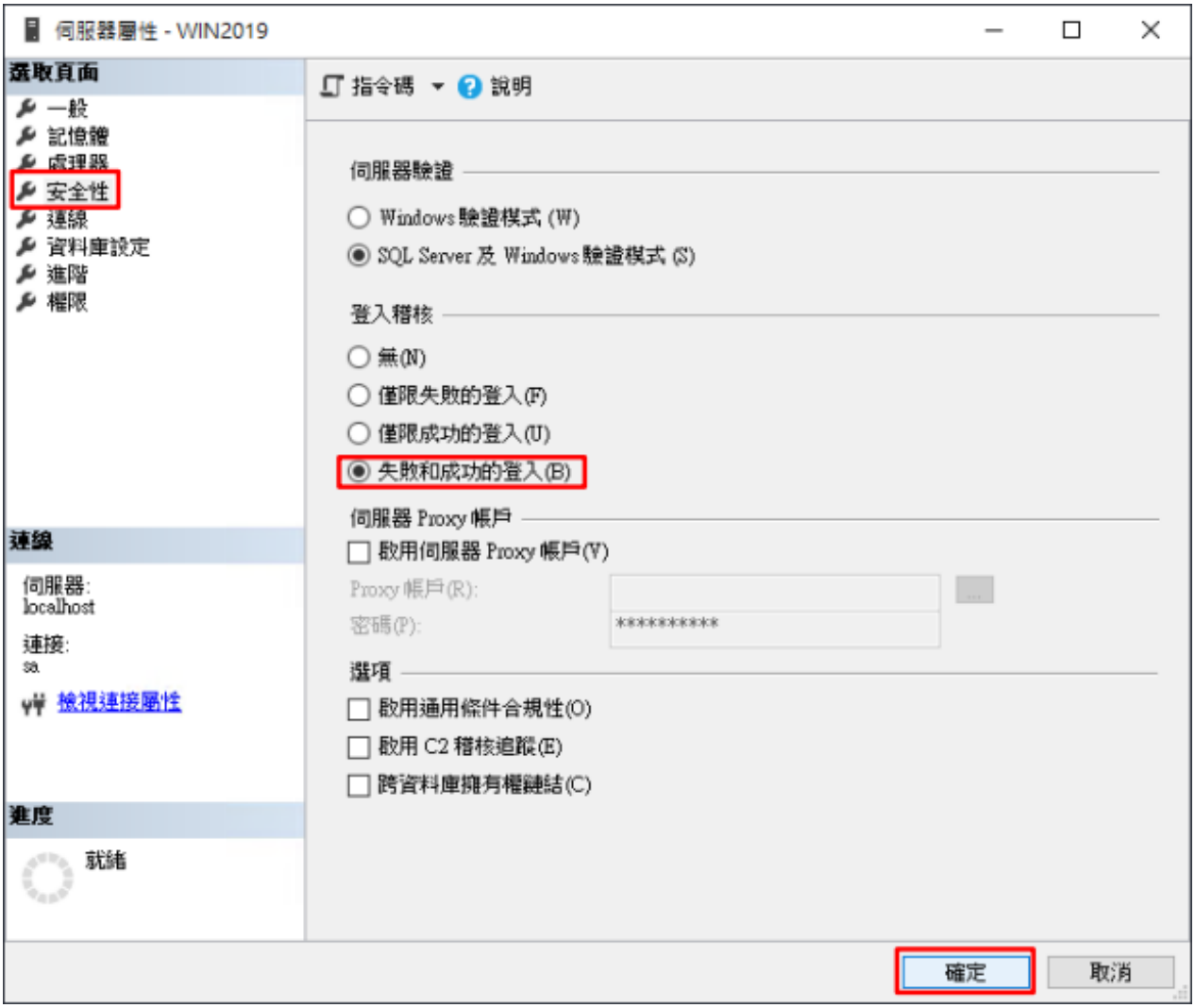
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

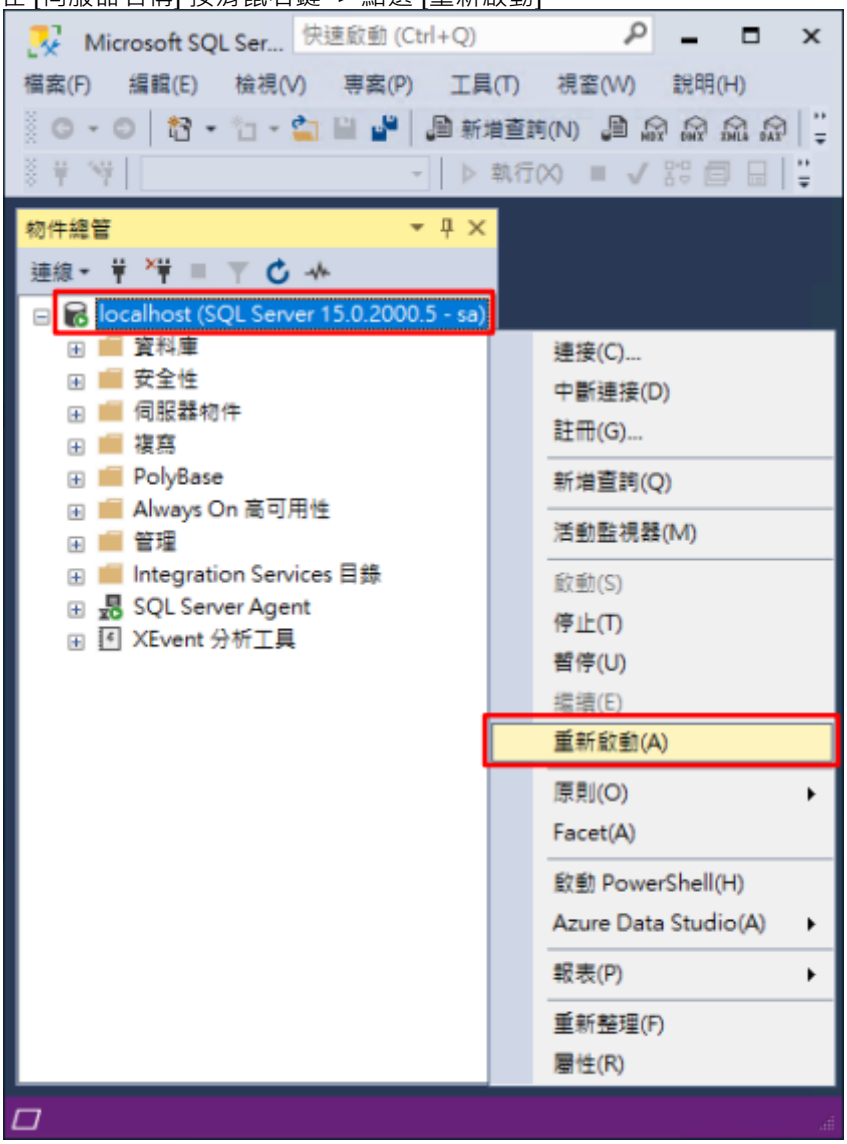


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

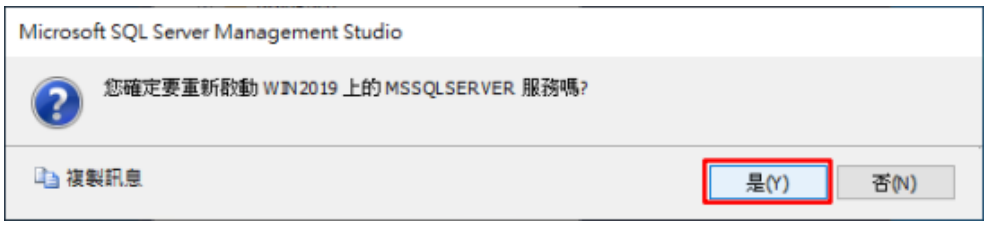


(5) 重新啟動 MS SQL SERVER 服務

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

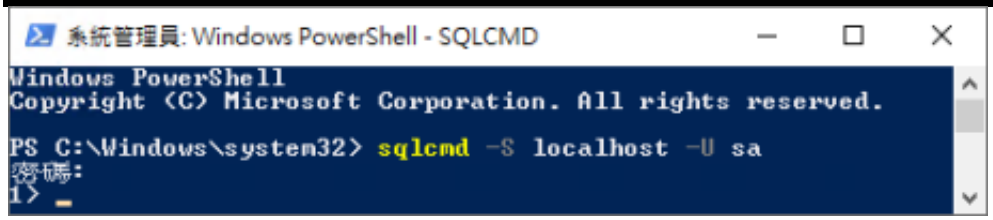
5.1.2 使用指令介面方式設定

(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]

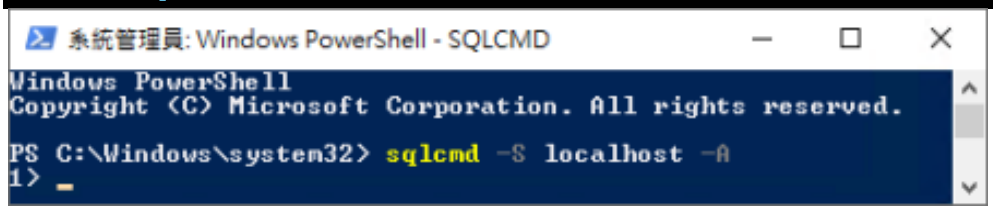
-U login_id

-P password

-A dedicated administrator connection

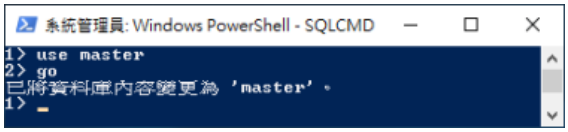
<2.2> 使用 Windows 帳號

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



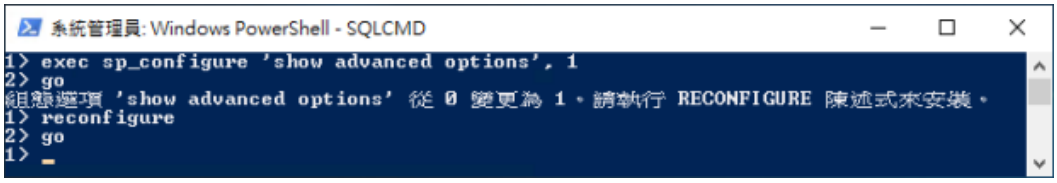
(3) 切換資料庫

```
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
```

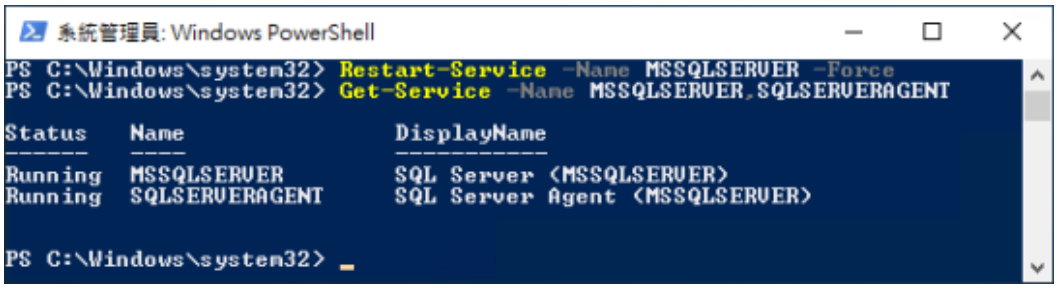


(5) 啟用失敗和成功的登入記錄

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

(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
```



5.2 設定稽核

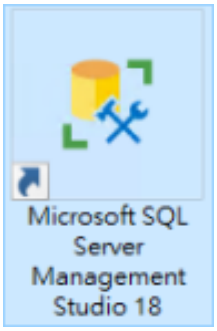
5.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

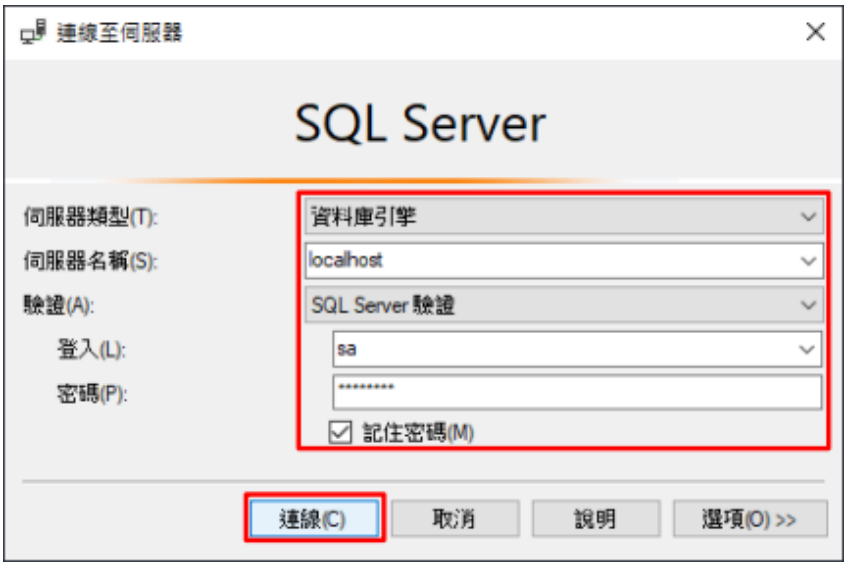
以下分別為圖形介面和指令介面設定方式。

5.2.1.1 使用圖形介面方式設定

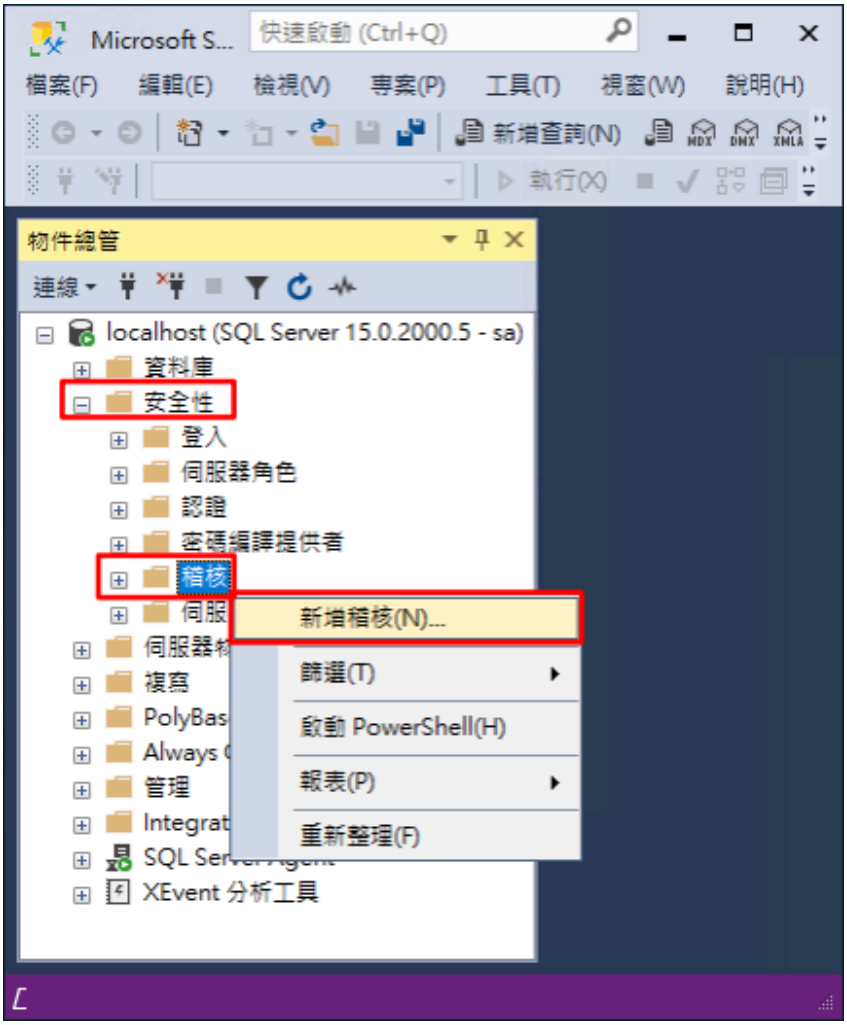
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

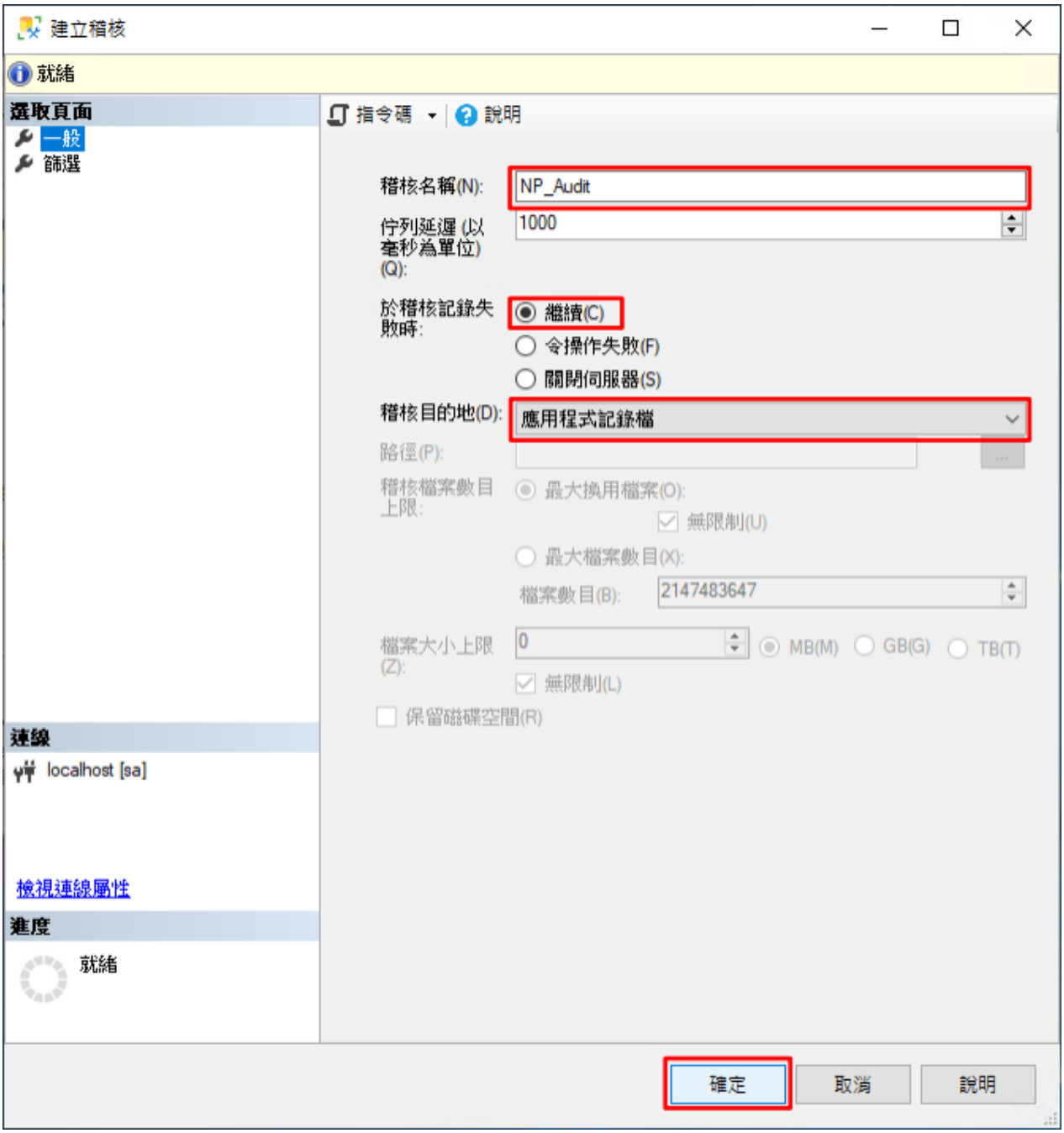


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

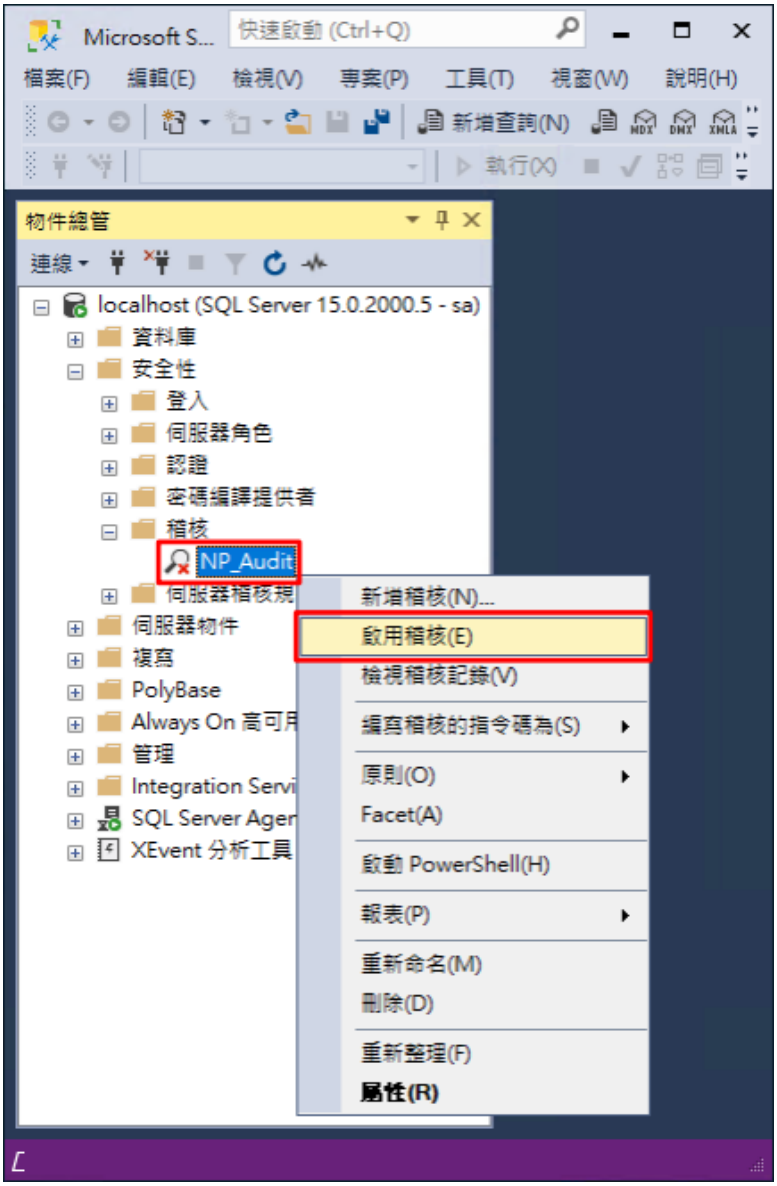


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

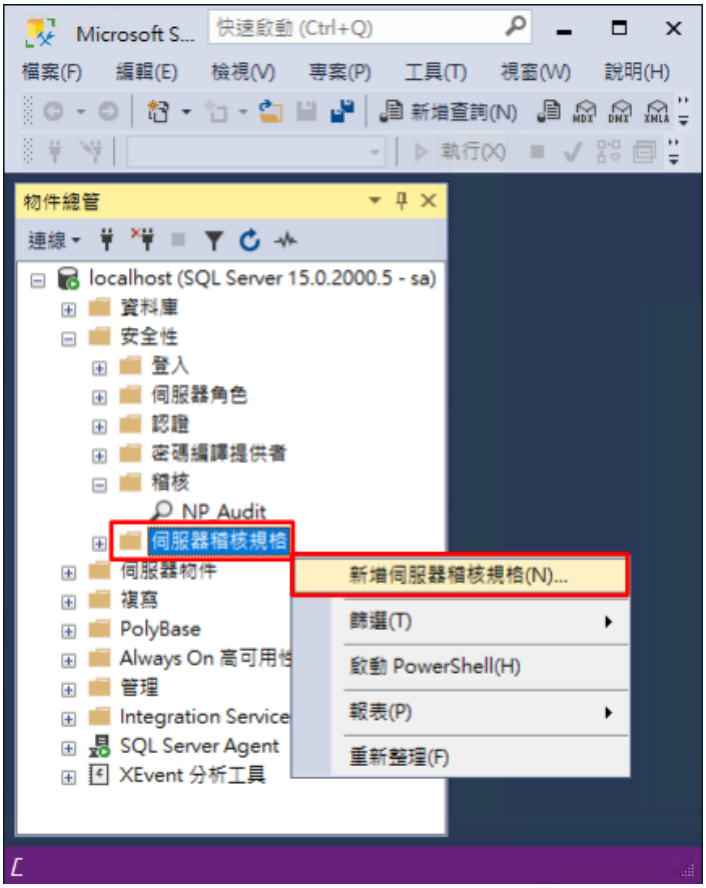


(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]

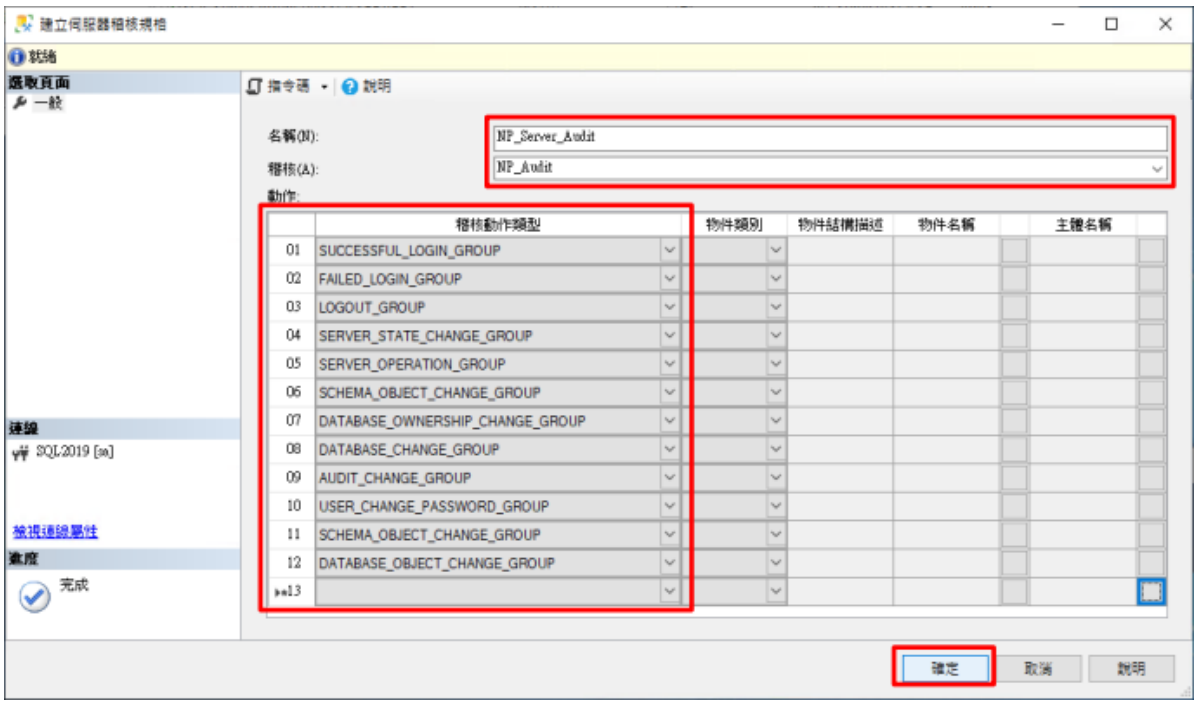


(6)　按 [關閉]

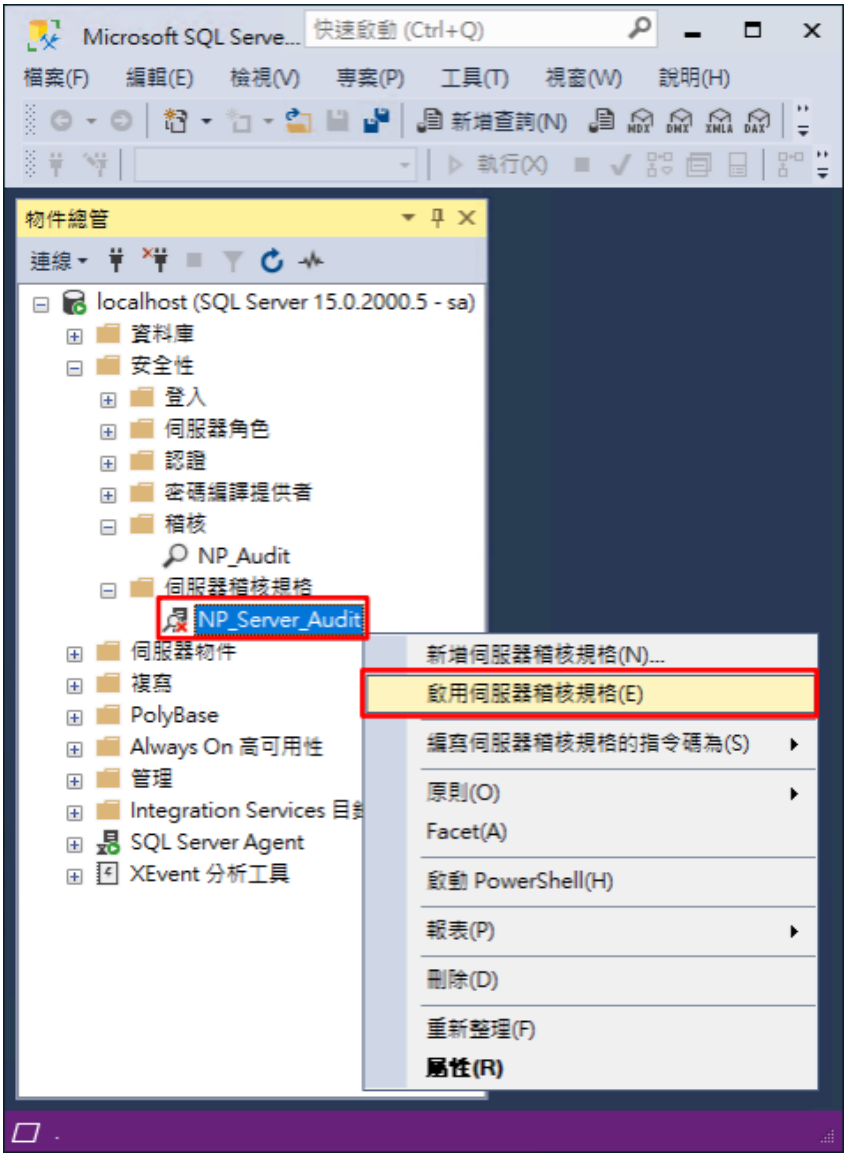
(7)　在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



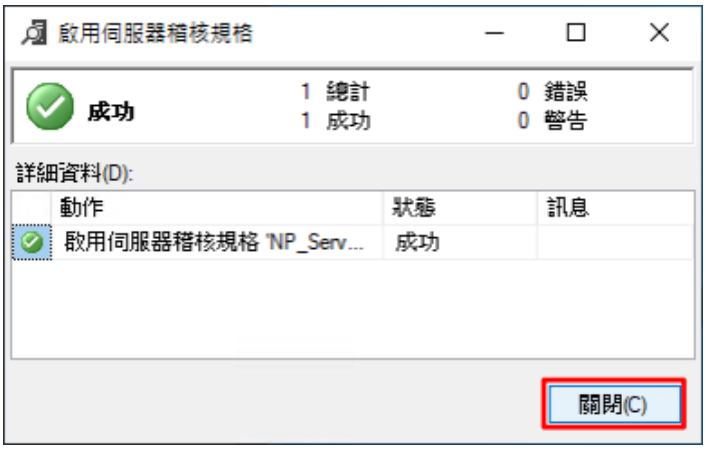
(8)　輸入名稱:　`NP_Server_Audit`　-> 選擇稽核: [NP_Audit] 和動作 詳細說明請參考前言的稽核動作群組連結 **-> 按 [確定]**



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



(10)　按 [關閉]



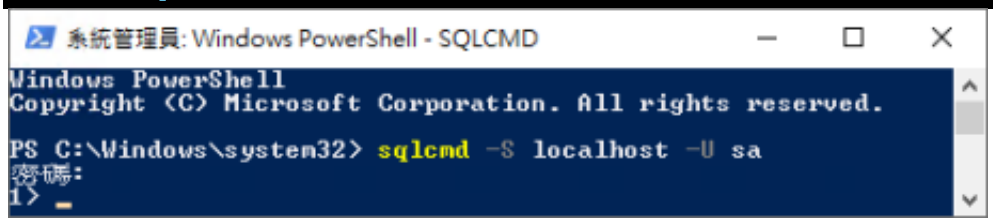
5.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

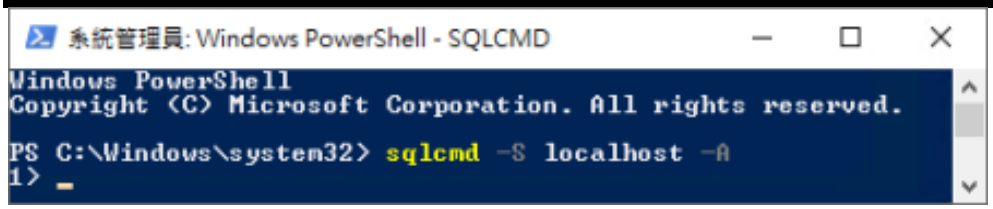
-U login_id

-P password

-A dedicated administrator connection

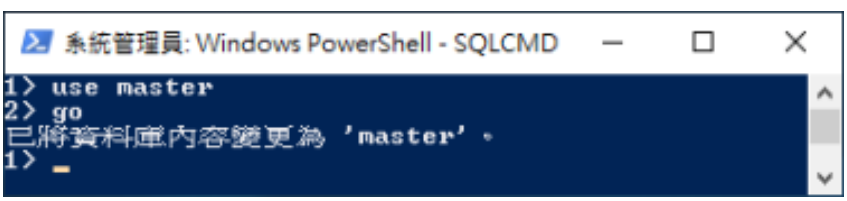
<2.2> 使用 Windows 帳號

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



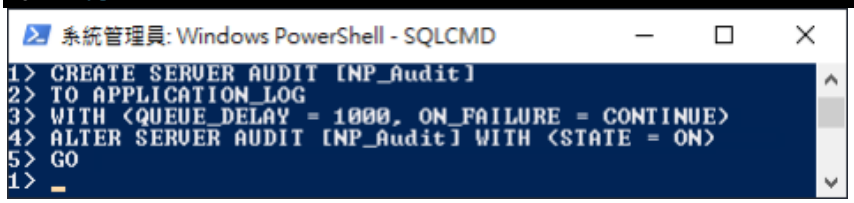
(3) 切換資料庫

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



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

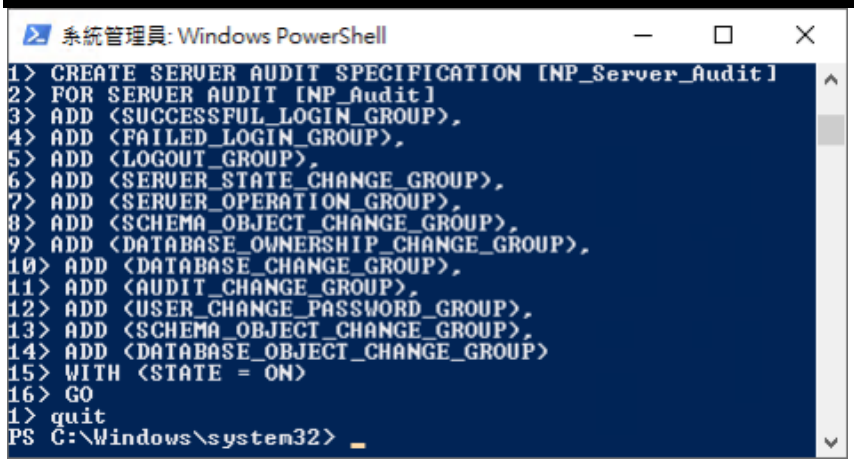
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



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
```



紅色文字部位請輸入伺服器稽核規格名稱

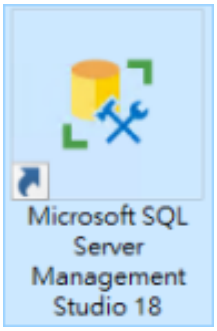
5.2.2 稽核資料庫層級

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

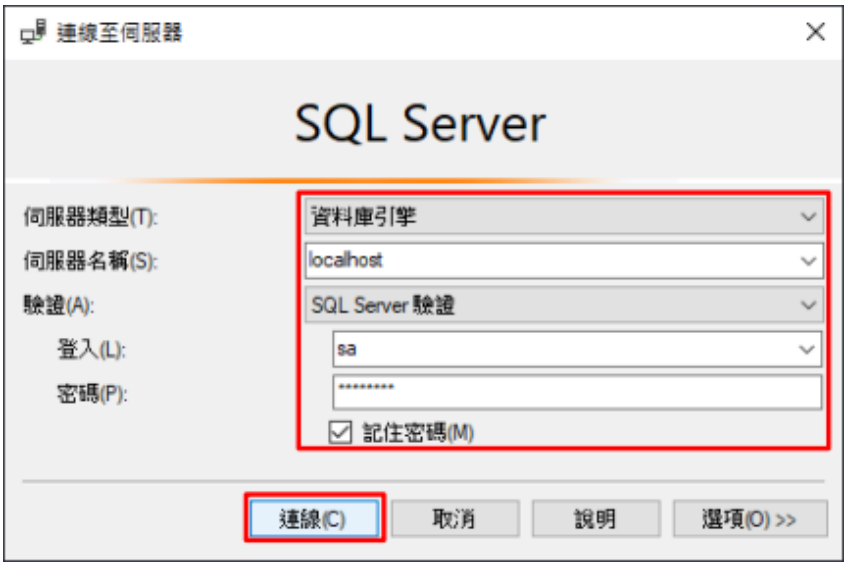
以下分別為圖形介面和指令介面設定方式。

5.2.2.1 使用圖形介面方式設定

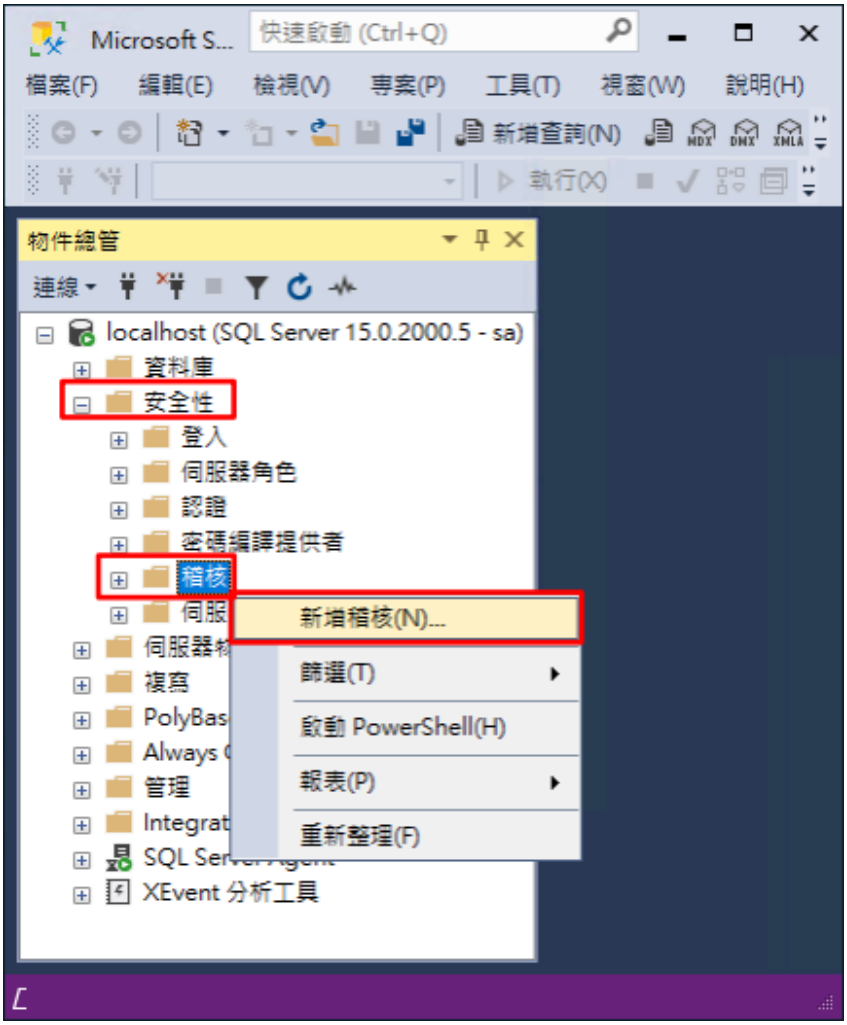
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

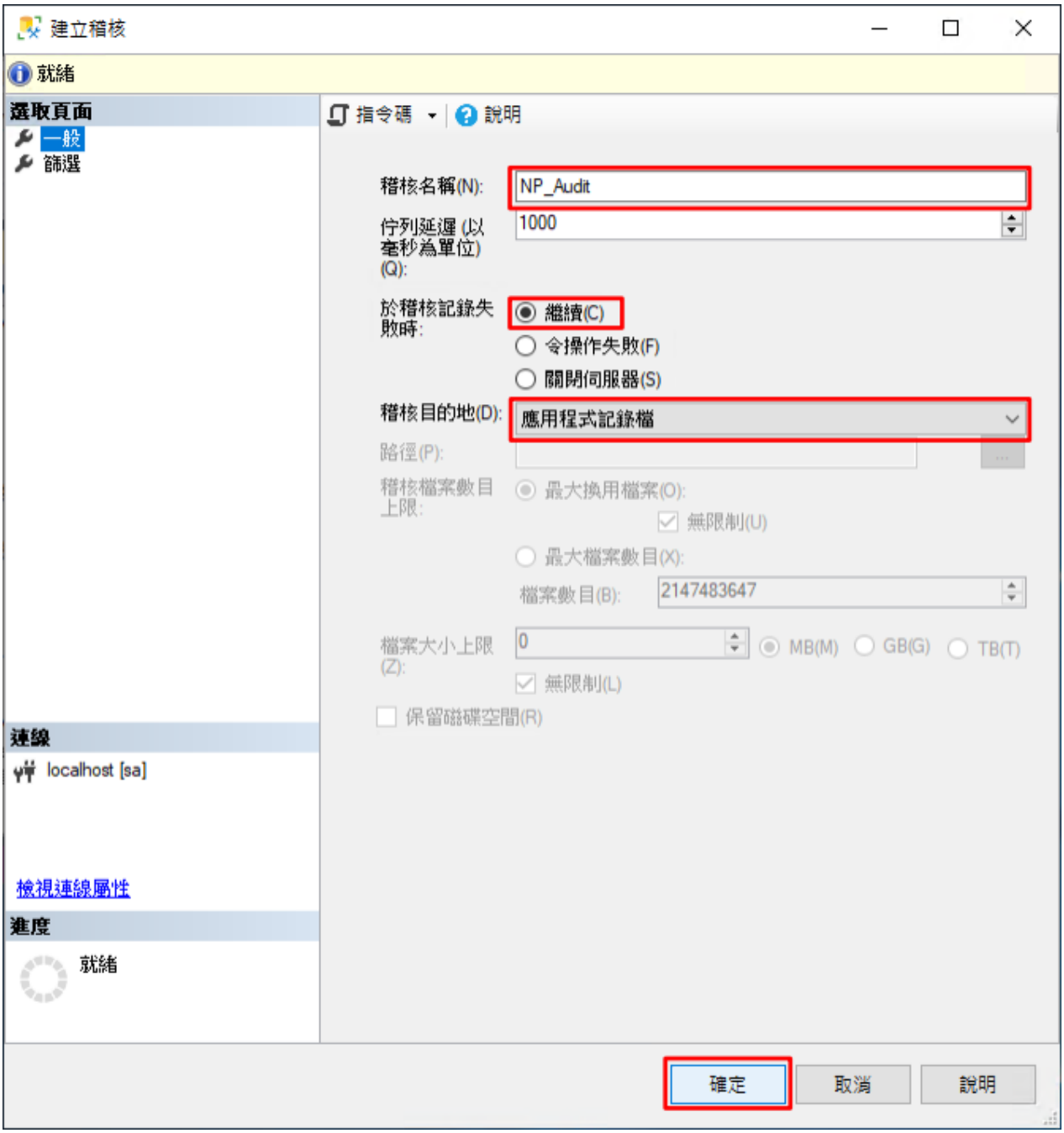


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

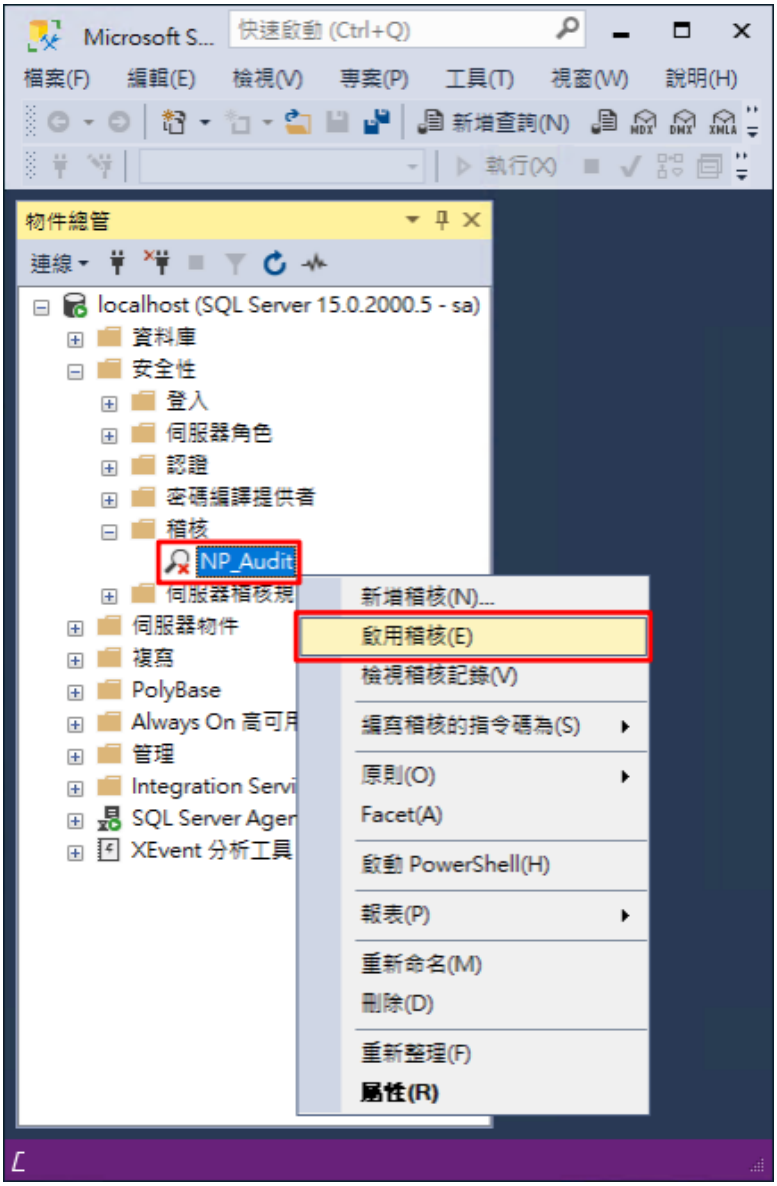


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]



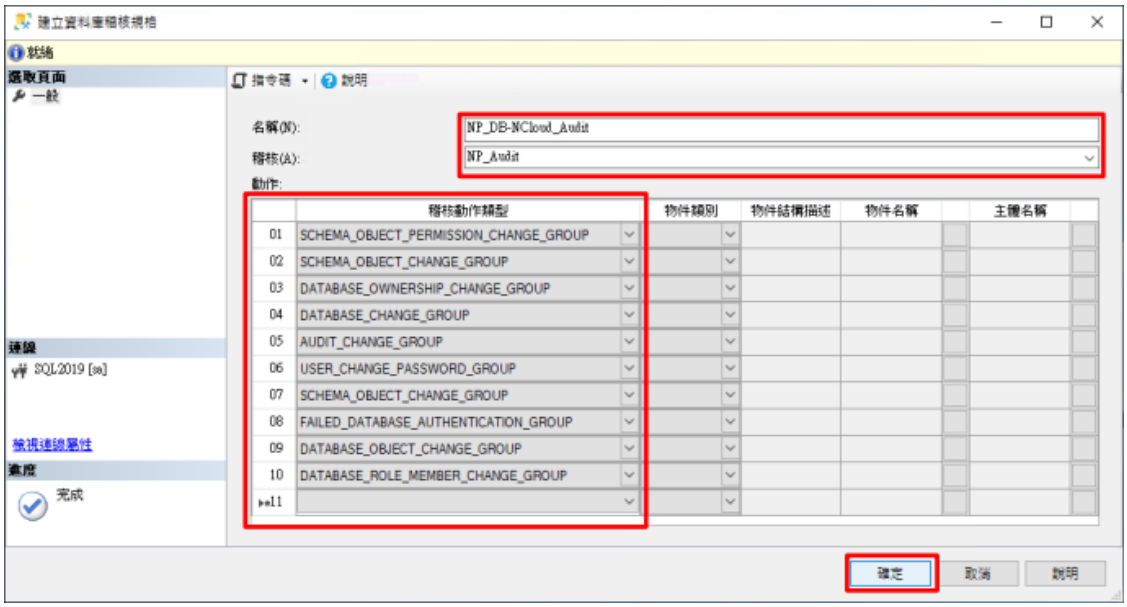
(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



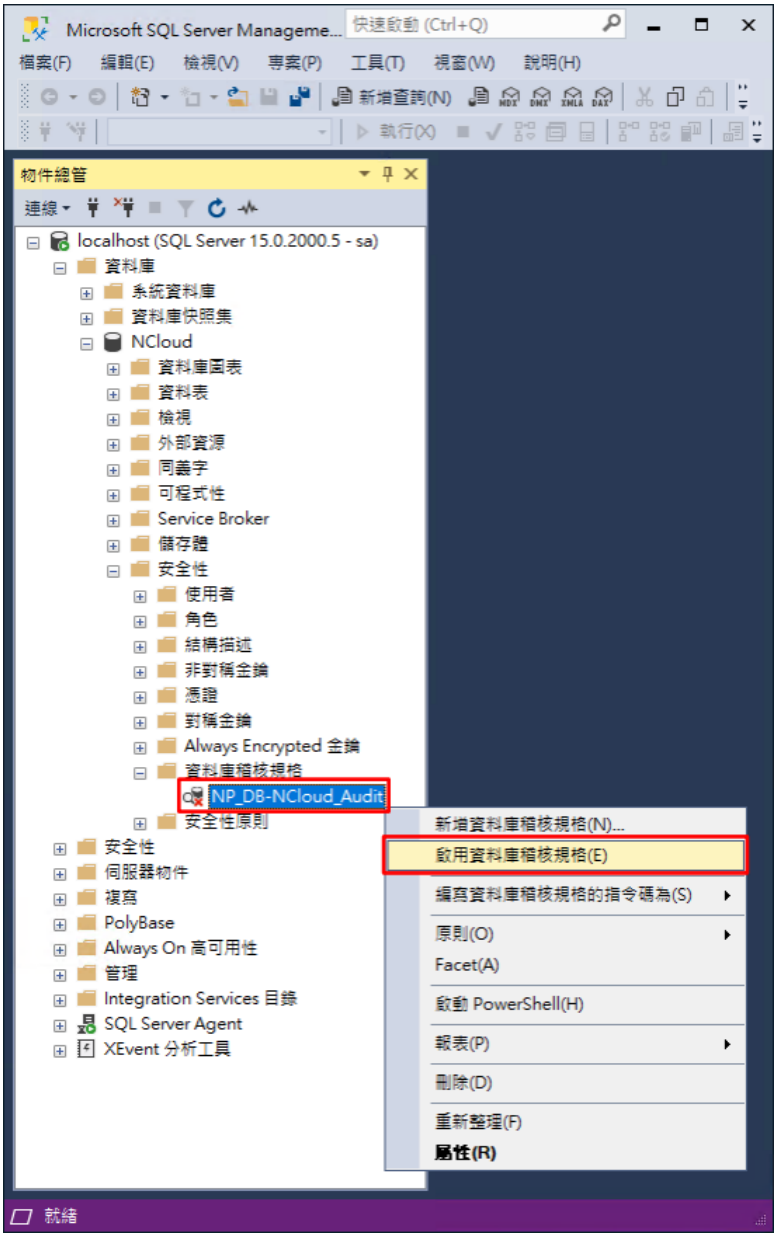
(6)　按 [關閉]

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

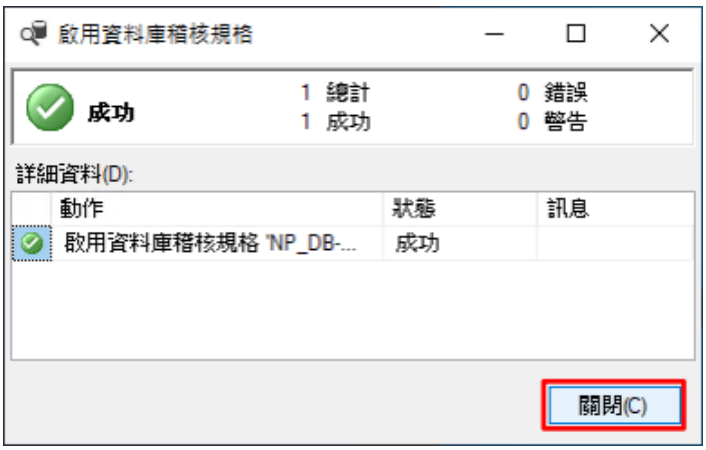
(8) **輸入稽核名稱:** `NP_DB-NCloud_Audit` **-> 選擇稽核: [NP_Audit] 和動作** 詳細說明請參考前言的稽核動作群組連結 **-> 按 [確定]**



(9)　在資料庫稽核規格名稱: [NP_DB-NCloud_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10)　按 [關閉]



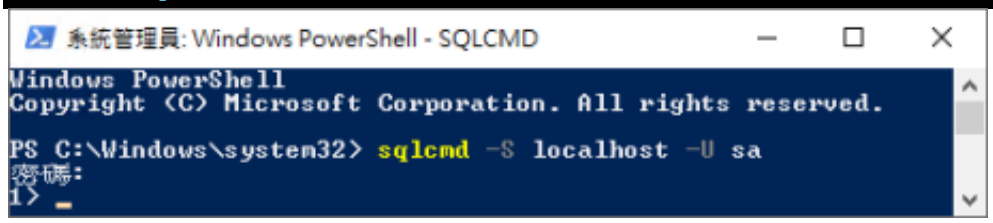
5.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

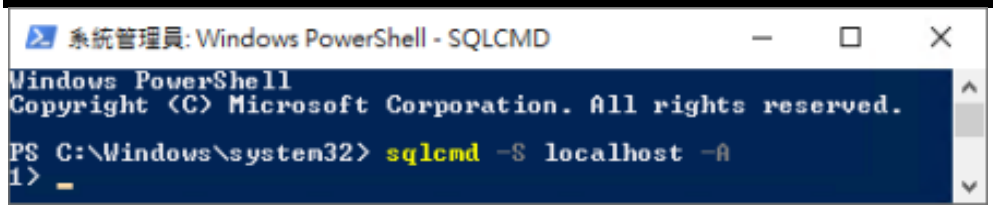
-U login_id

-P password

-A dedicated administrator connection

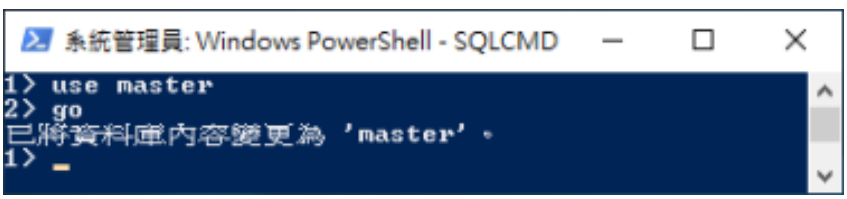
<2.2> 使用 Windows 帳號

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



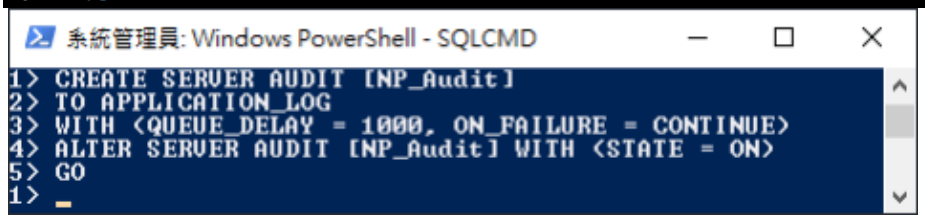
(3) 切換資料庫

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



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

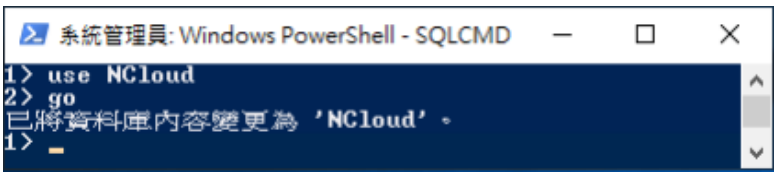
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例： NCloud

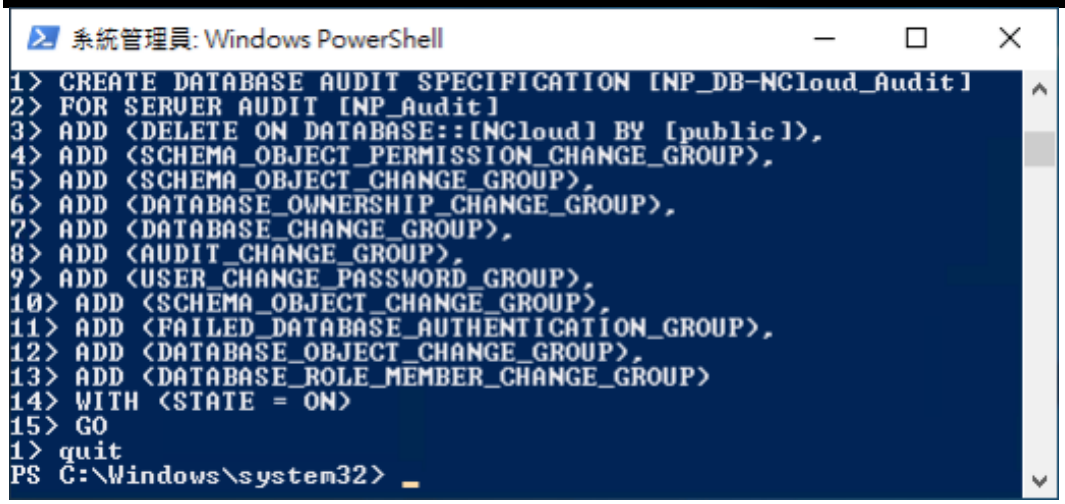
```
1 > use NCloud
2 > go
```



紅色文字部位請輸入稽核資料庫名稱

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

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



紅色文字部位請輸入資料庫稽核規格名稱

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

紅色文字部位請輸入稽核資料庫名稱

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

5.3 事件記錄檔設定

此為選項設定。

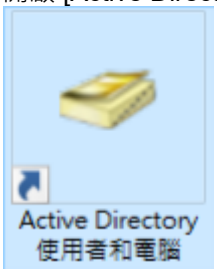
以下分別為網域和工作群組設定方式。

5.3.1 網域

5.3.1.1 組織單位設定

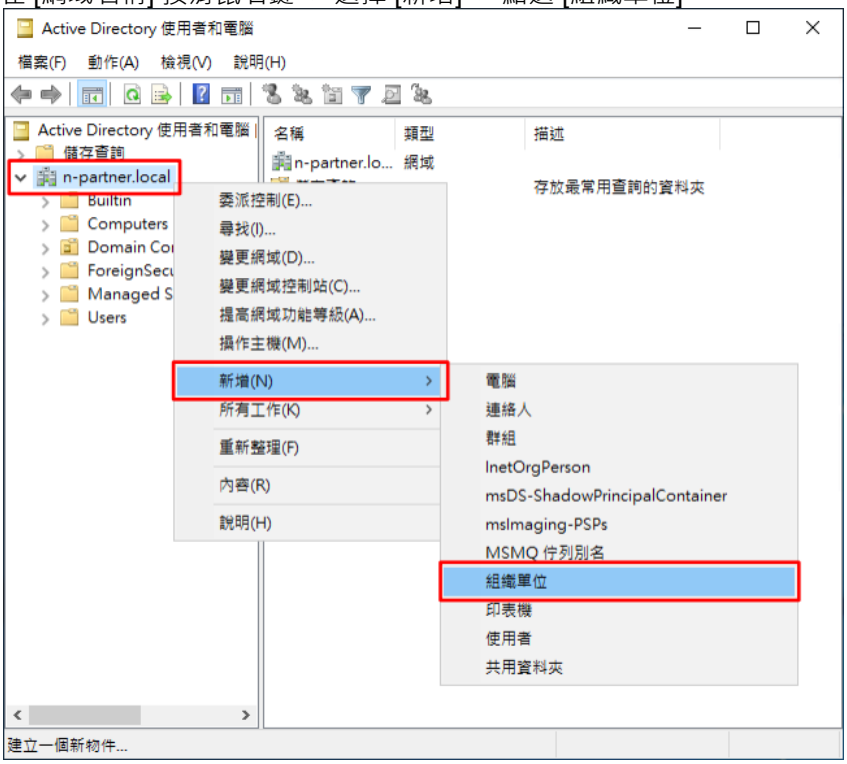
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



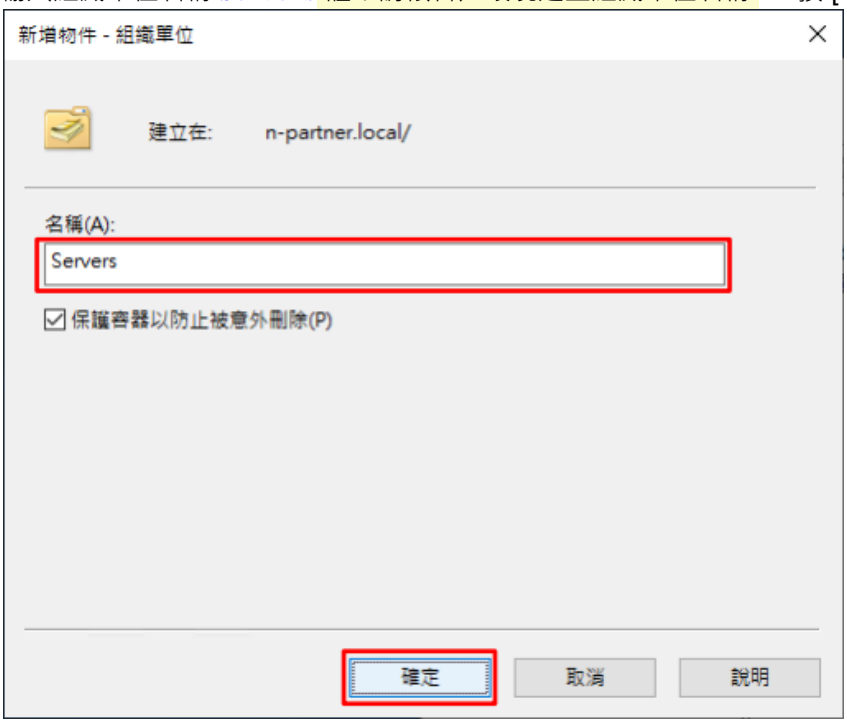
(2) 新增組織單位

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



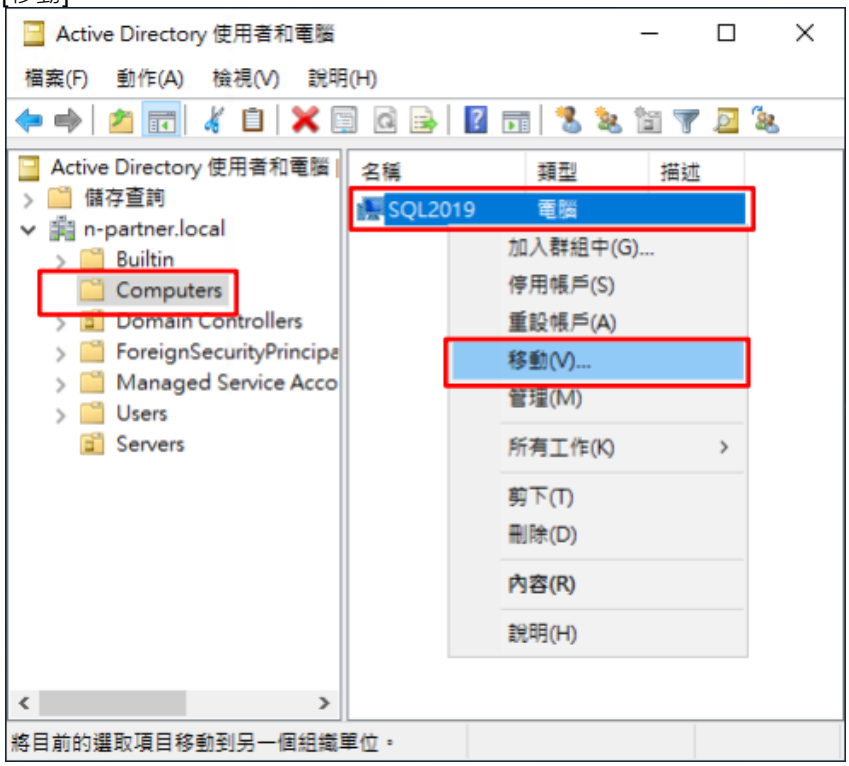
(3) 輸入組織單位名稱

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



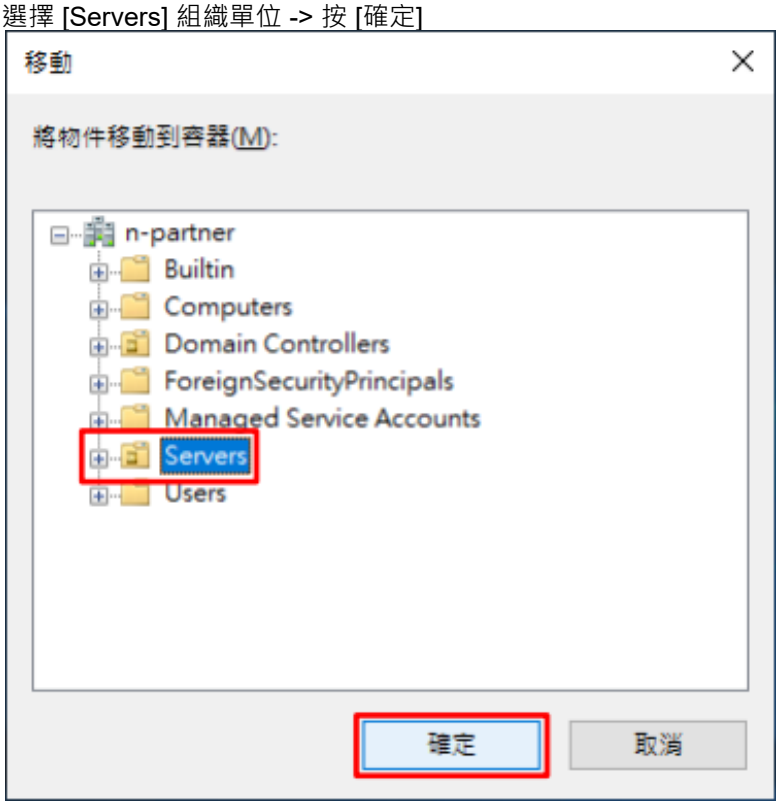
(4) 移動伺服器至新的組織單位

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



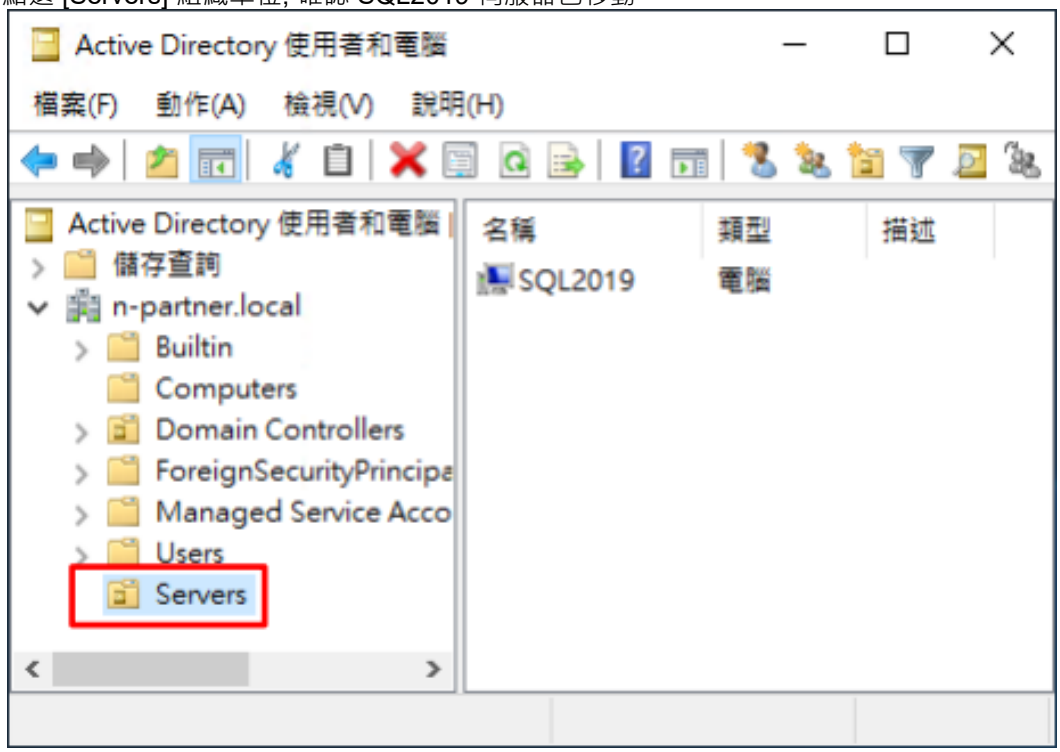
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

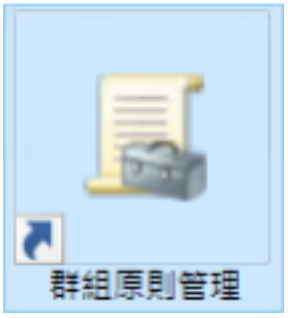
點選 [Servers] 組織單位, 確認 SQL2019 伺服器已移動。



5.3.1.2 群組原則設定

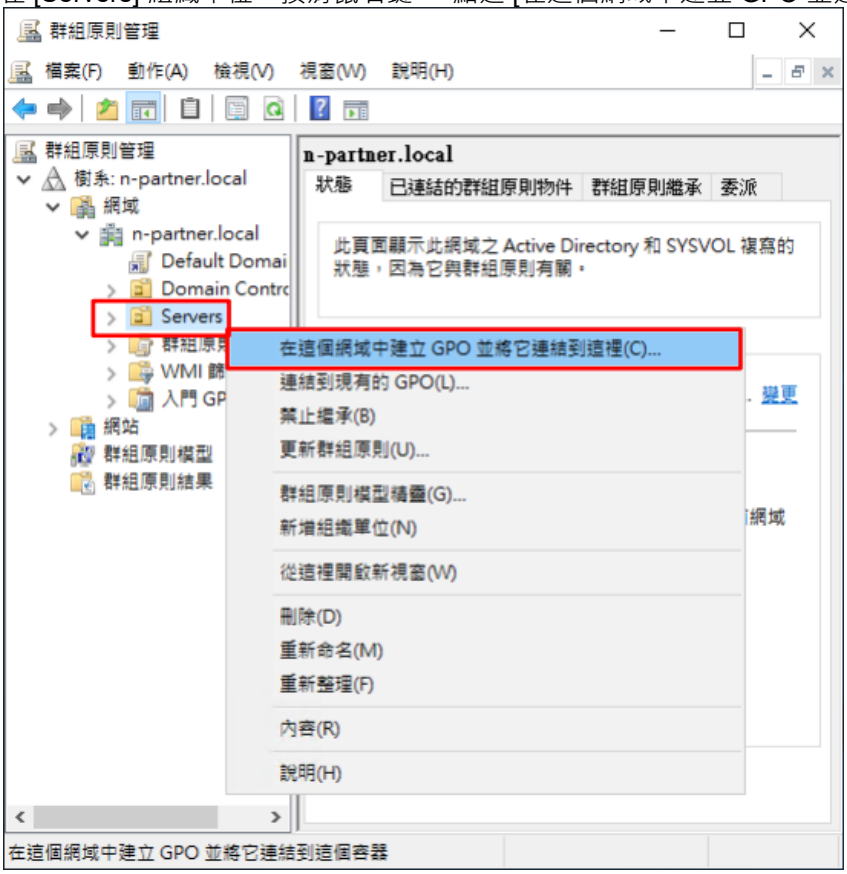
(1) 開啟群組原則管理

開啟 [群組原則管理]



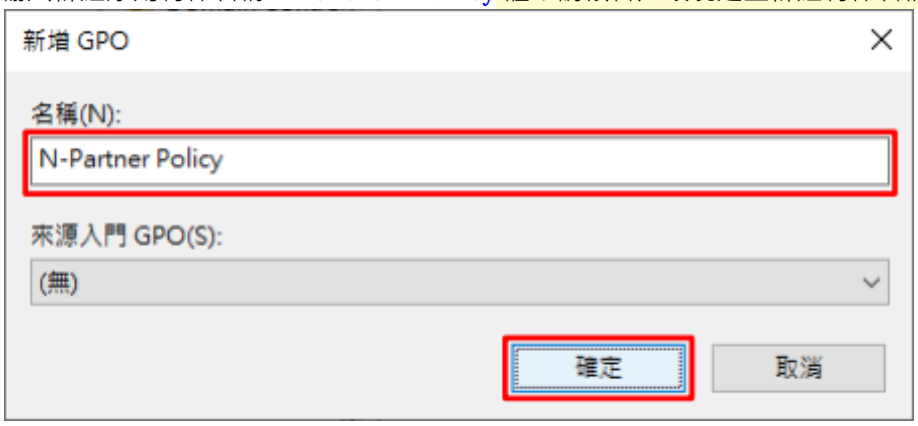
(2) 在 Servers 組織單位，新增群組原則物件

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



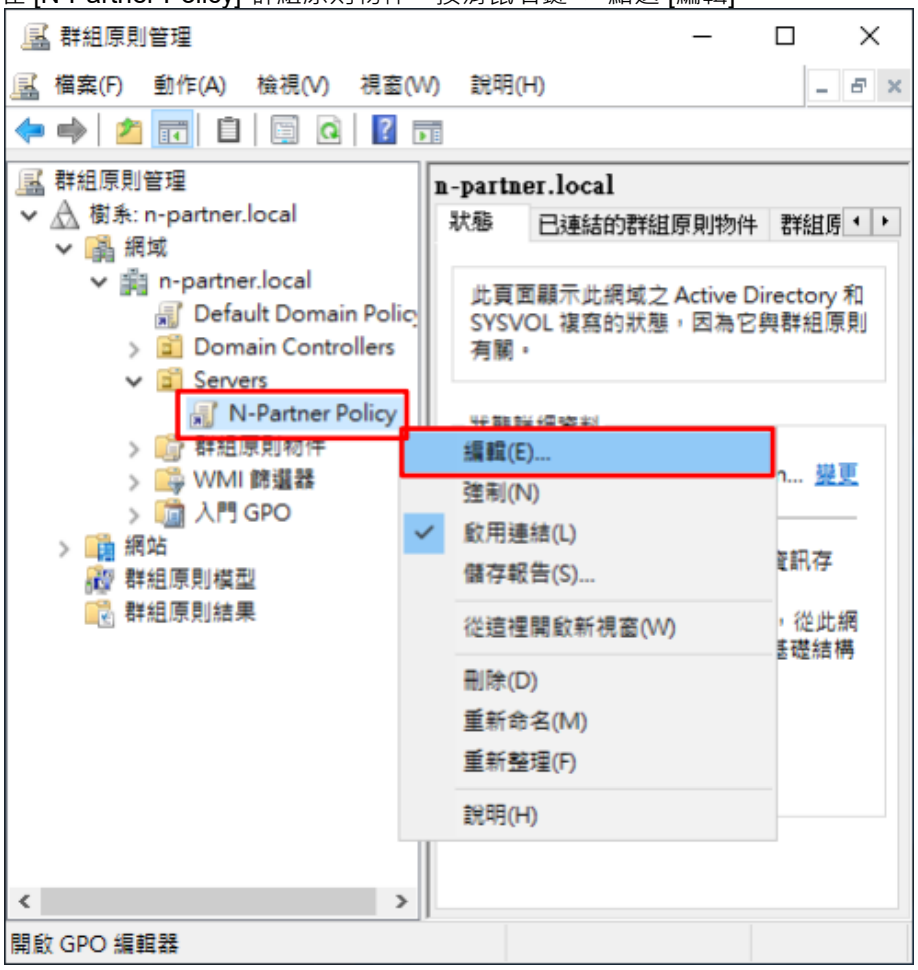
(3) 輸入群組原則物件名稱

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



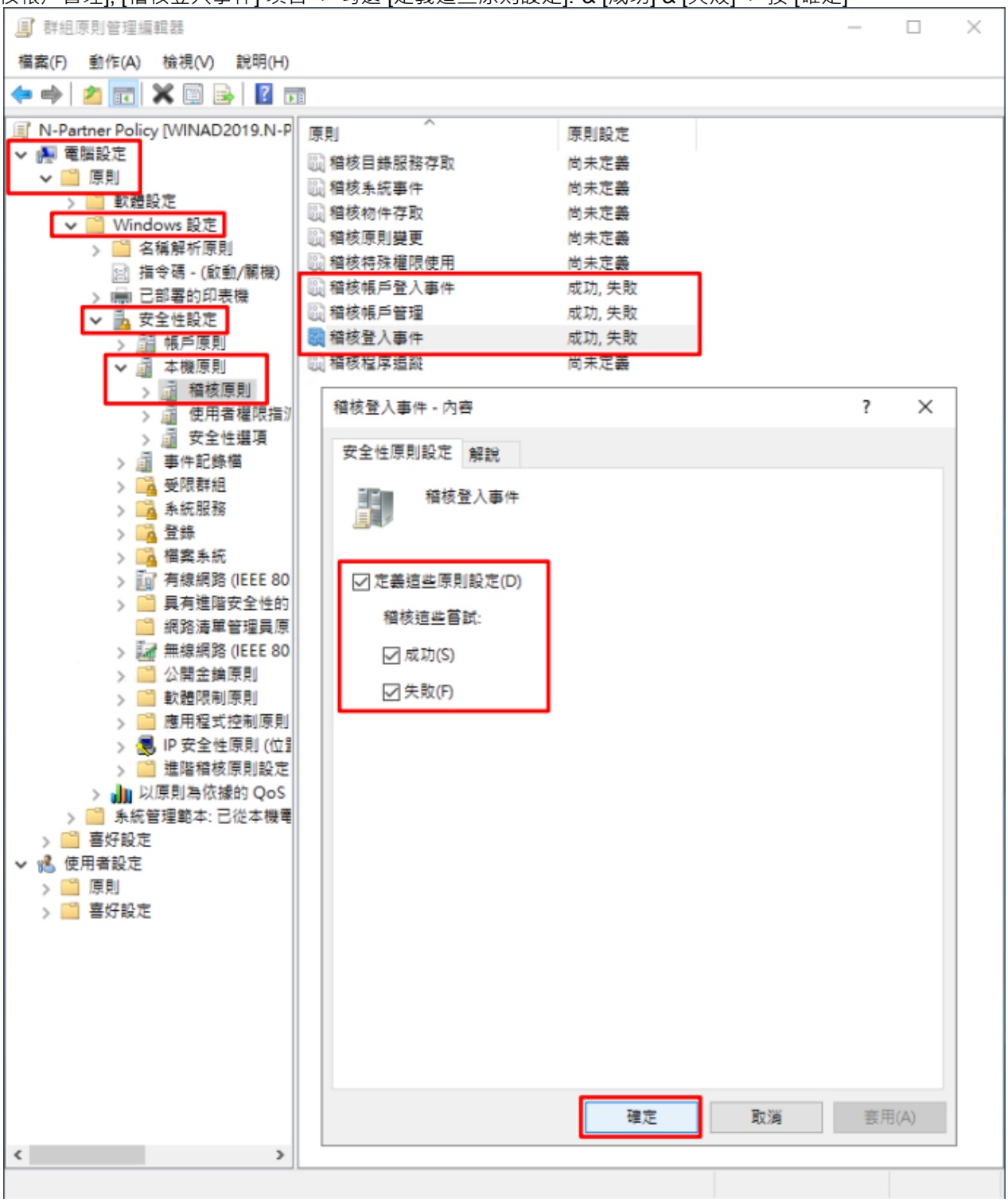
(4) 編輯群組原則物件

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



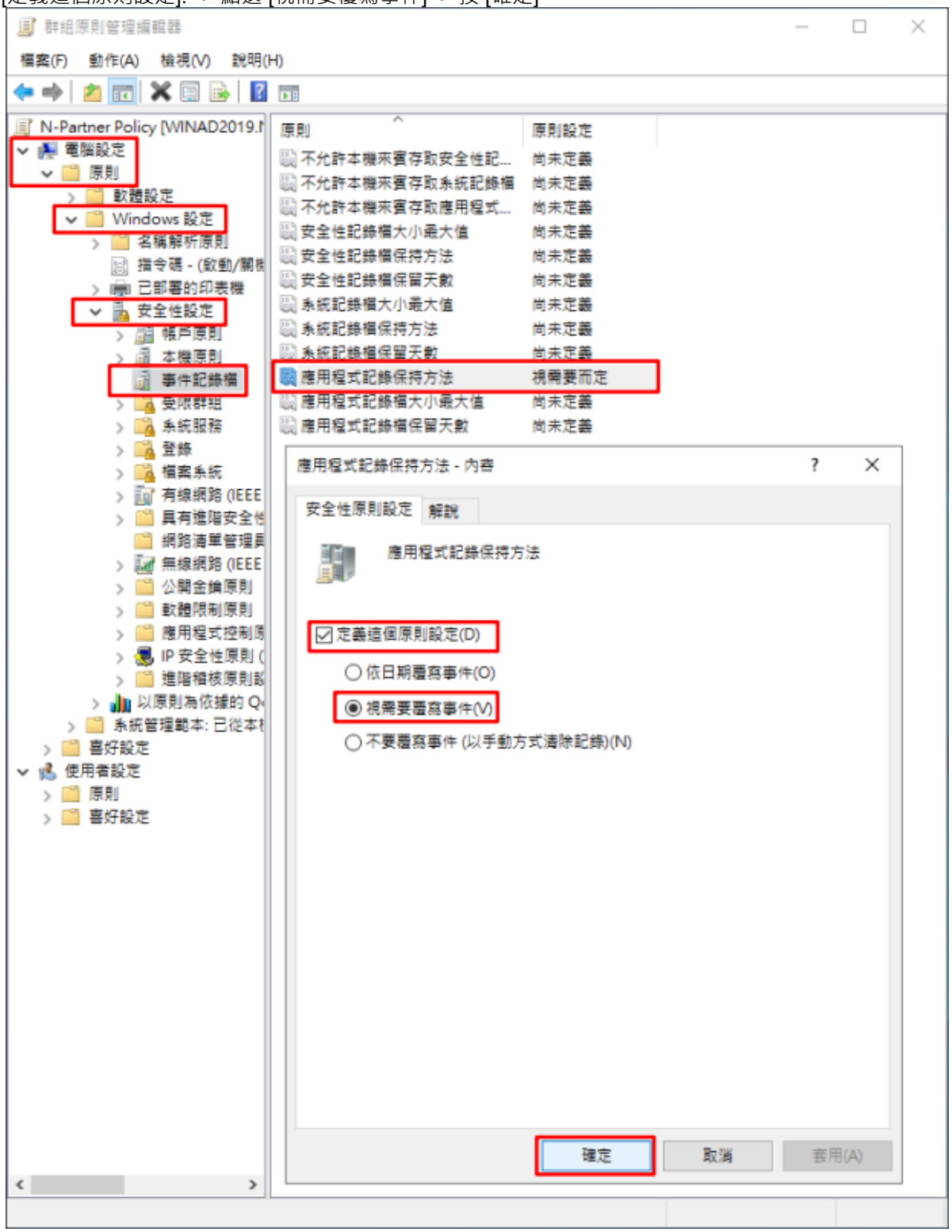
(5) 本機原則：稽核原則

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



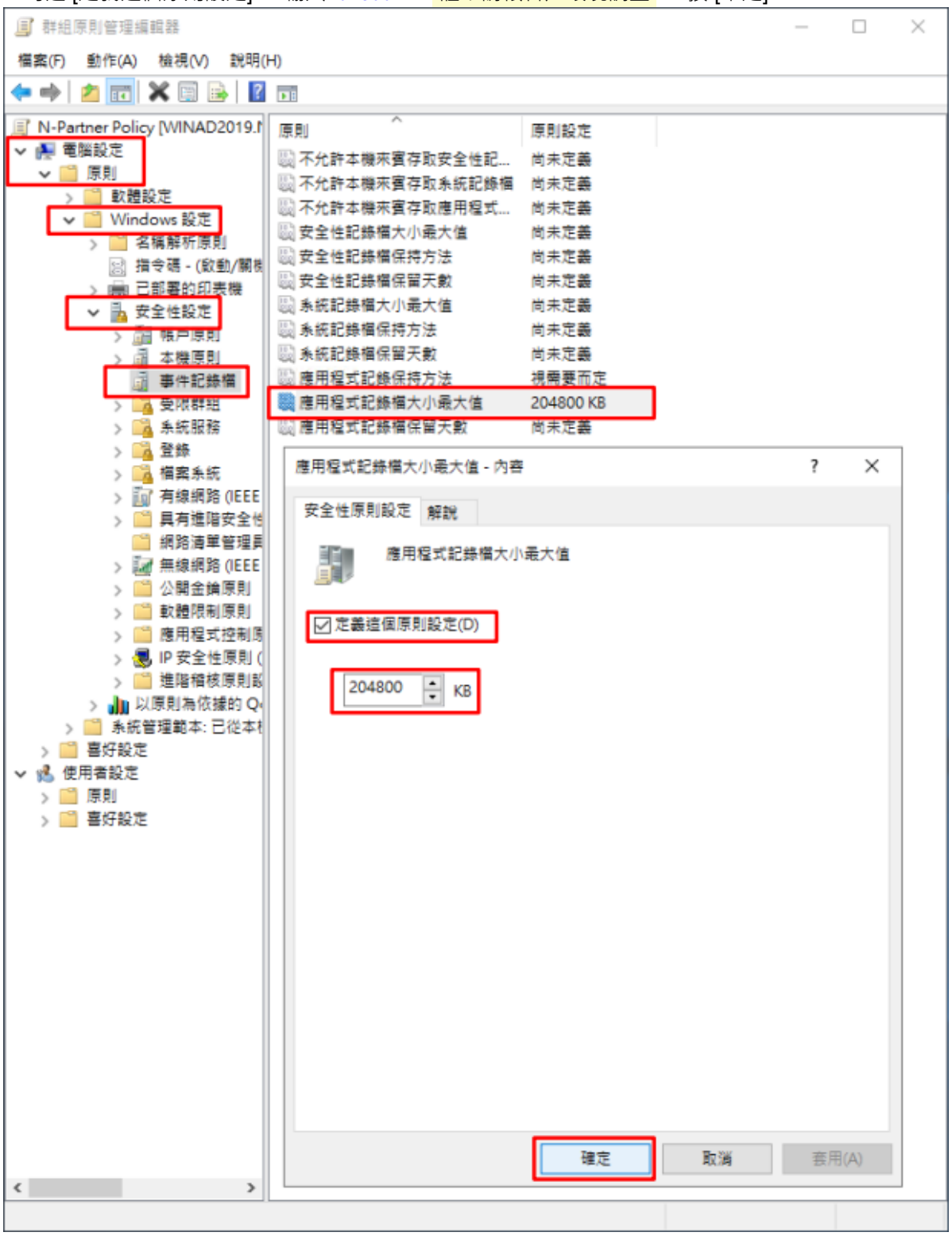
(6) 事件記錄：應用程式記錄保持方法

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



(7)　事件記錄：應用程式記錄檔大小最大值

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



(8) 開啟 [Windows PowerShell]

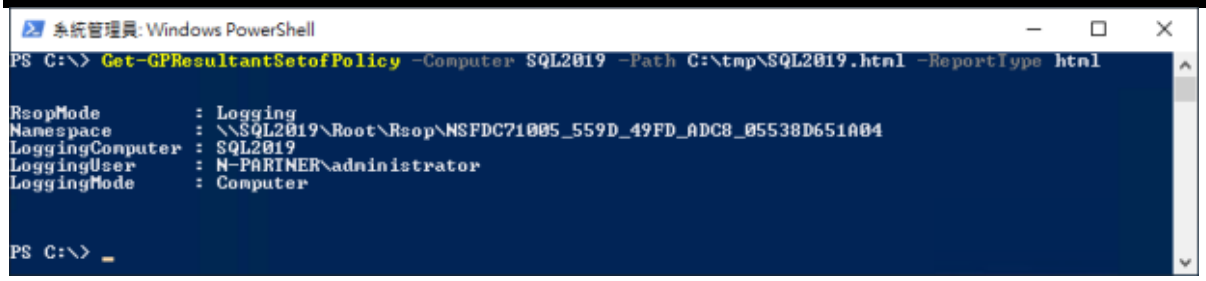
(9) 更新 MS SQL Server 群組原則

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

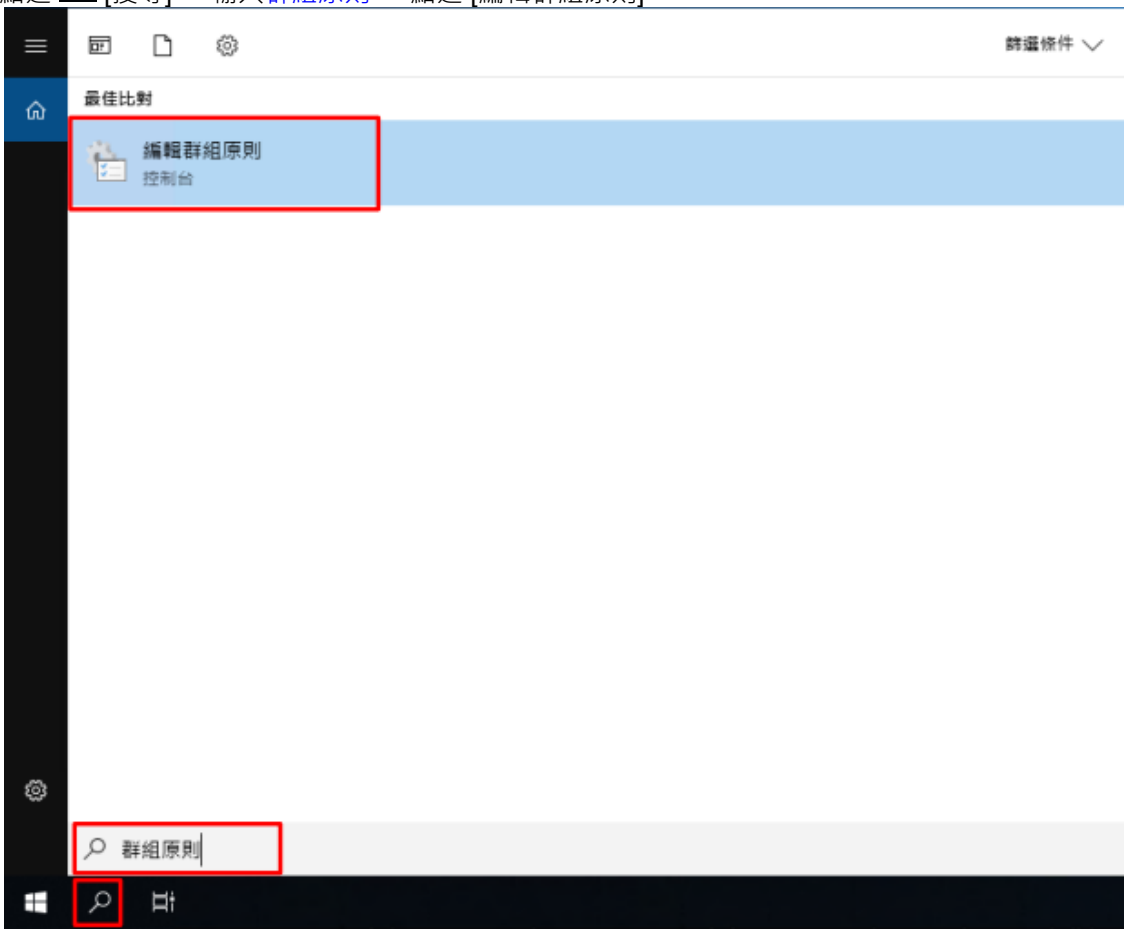
(11) 開啟報表 -> 確認 MS SQL Server 伺服器 -> 套用 N-Partner Policy 群組原則

5.3.2 工作群組

5.3.2.1 稽核原則設定

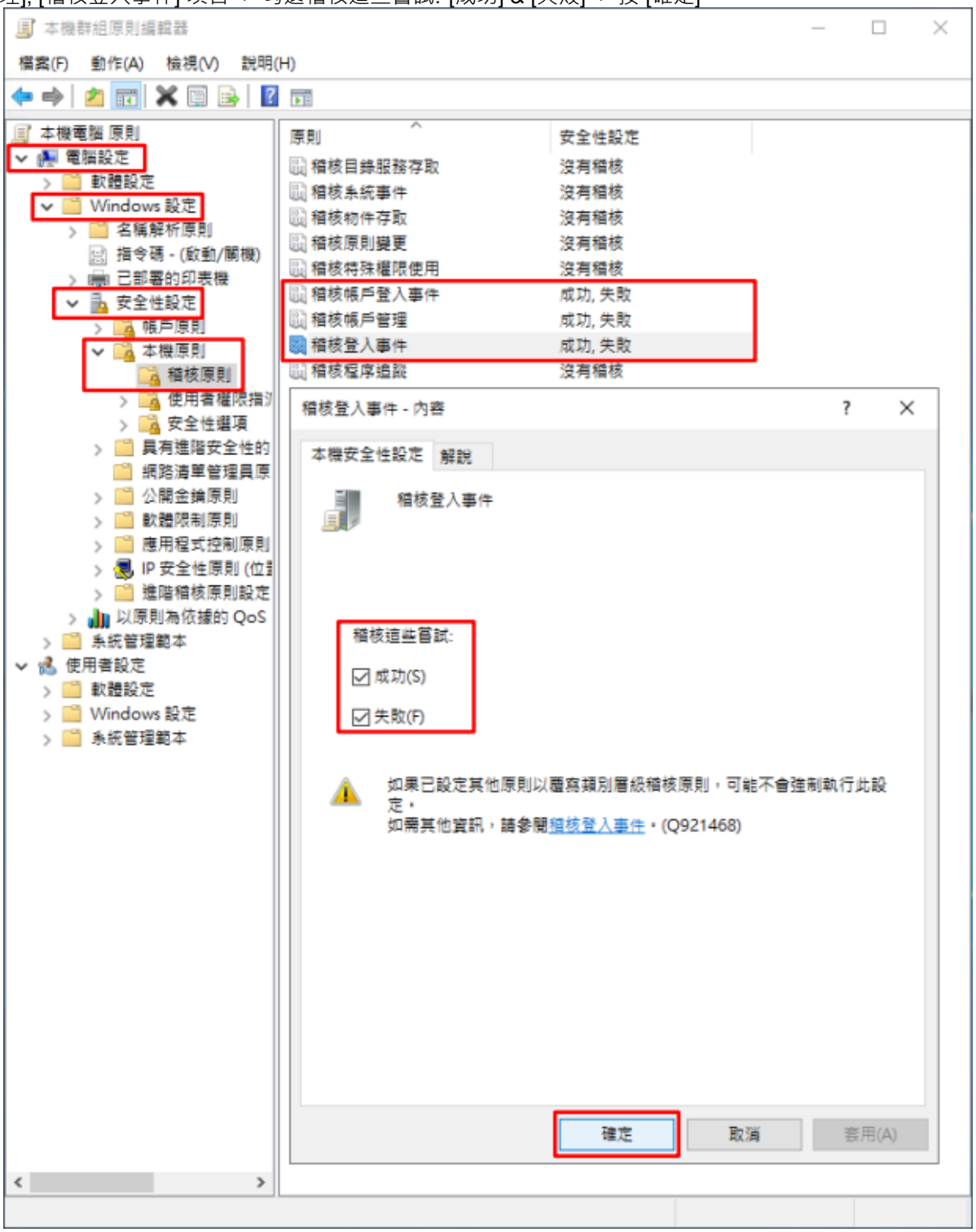
(1) 開啟 [本機群組原則編輯器]

點選 [搜尋] -> 輸入群組原則 -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

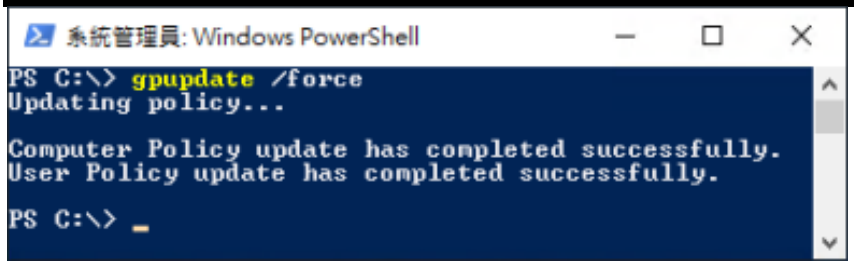
展開 [電腦設定] -> [Windows 設定] -> [安全性設定] -> [本機原則] -> [稽核原則] -> 點選 [稽核帳戶登入事件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選稽核這些嘗試: [成功] & [失敗] -> 按 [確定]



(3) 開啟 [Windows PowerShell]

(4) 更新群組原則

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



(5) 查看群組原則套用情形

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

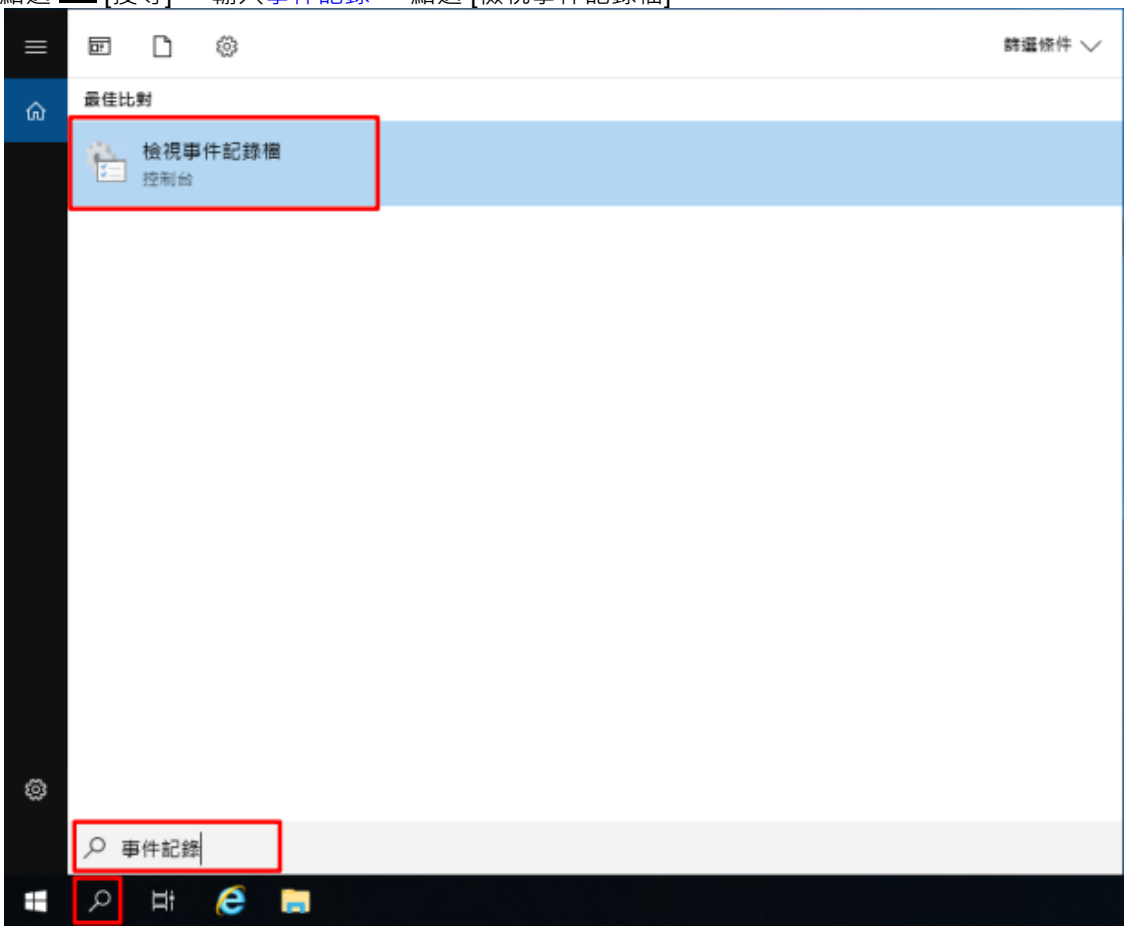
系統管理員: Windows PowerShell

```
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
  MPSSVC 規則層級原則變更                       No Auditing
  篩選平台原則變更                            No Auditing
  其他原則變更事件                            No Auditing
帳戶管理
  電腦帳戶管理                              Success and Failure
  安全性群組管理                             Success and Failure
  發佈群組管理                              Success and Failure
  應用程式群組管理                            Success and Failure
  其他帳戶管理事件                            Success and Failure
  使用者帳戶管理                             Success and Failure
DS 存取
  目錄服務存取                              Success
  目錄服務變更                              No Auditing
  目錄服務複寫                              No Auditing
  詳細目錄服務複寫                            No Auditing
帳戶登入
  Kerberos 服務票證操作                       Success and Failure
  其他帳戶登入事件                            Success and Failure
  Kerberos 驗證服務                       Success and Failure
  認證驗證                                Success and Failure
PS C:\> _
```

5.3.2.2 事件檔案設定

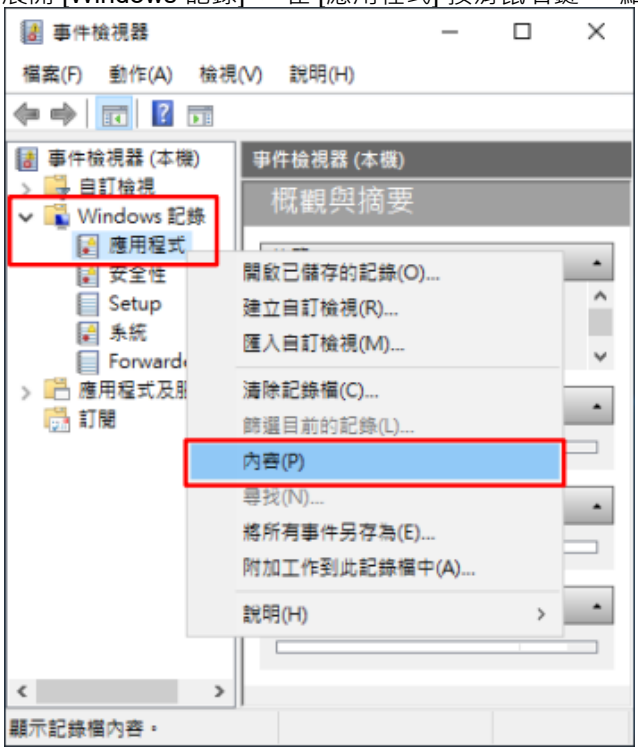
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入事件記錄 -> 點選 [檢視事件記錄檔]



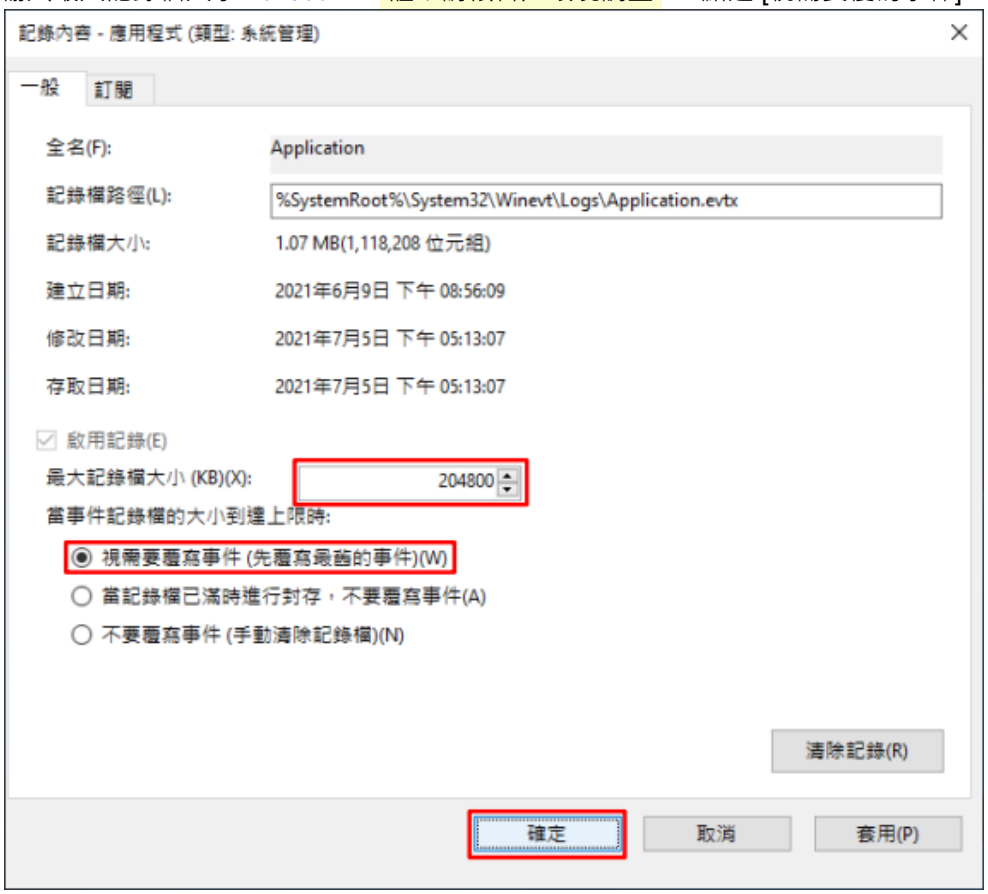
(2) 編輯安全性記錄

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



(3) 設定應用程式記錄檔

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



6 SQL2022

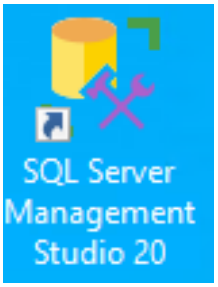
6.1 稽核登入

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

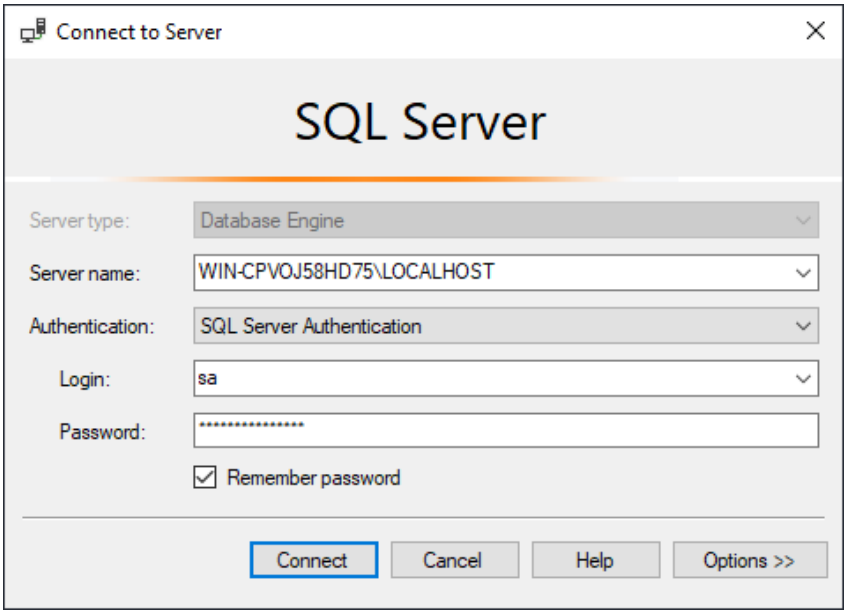
以下分別為圖形介面和指令介面設定方式。

6.1.1 使用圖形介面方式設定

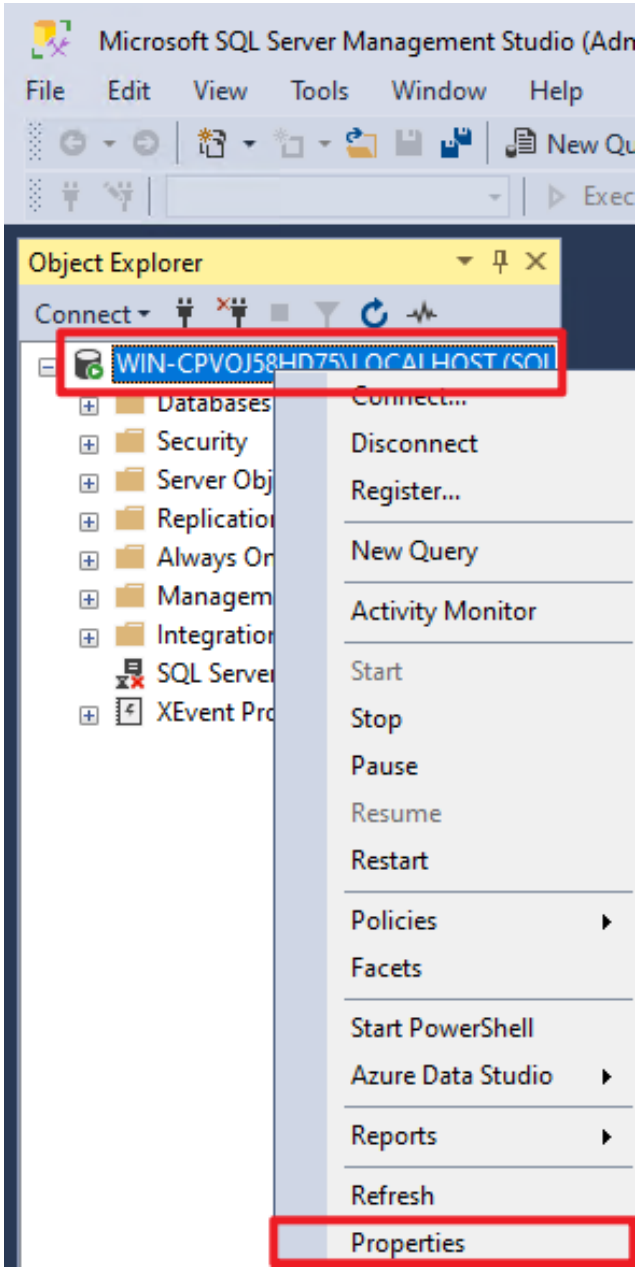
(1) 開啟 [Microsoft SQL Server Management Studio]



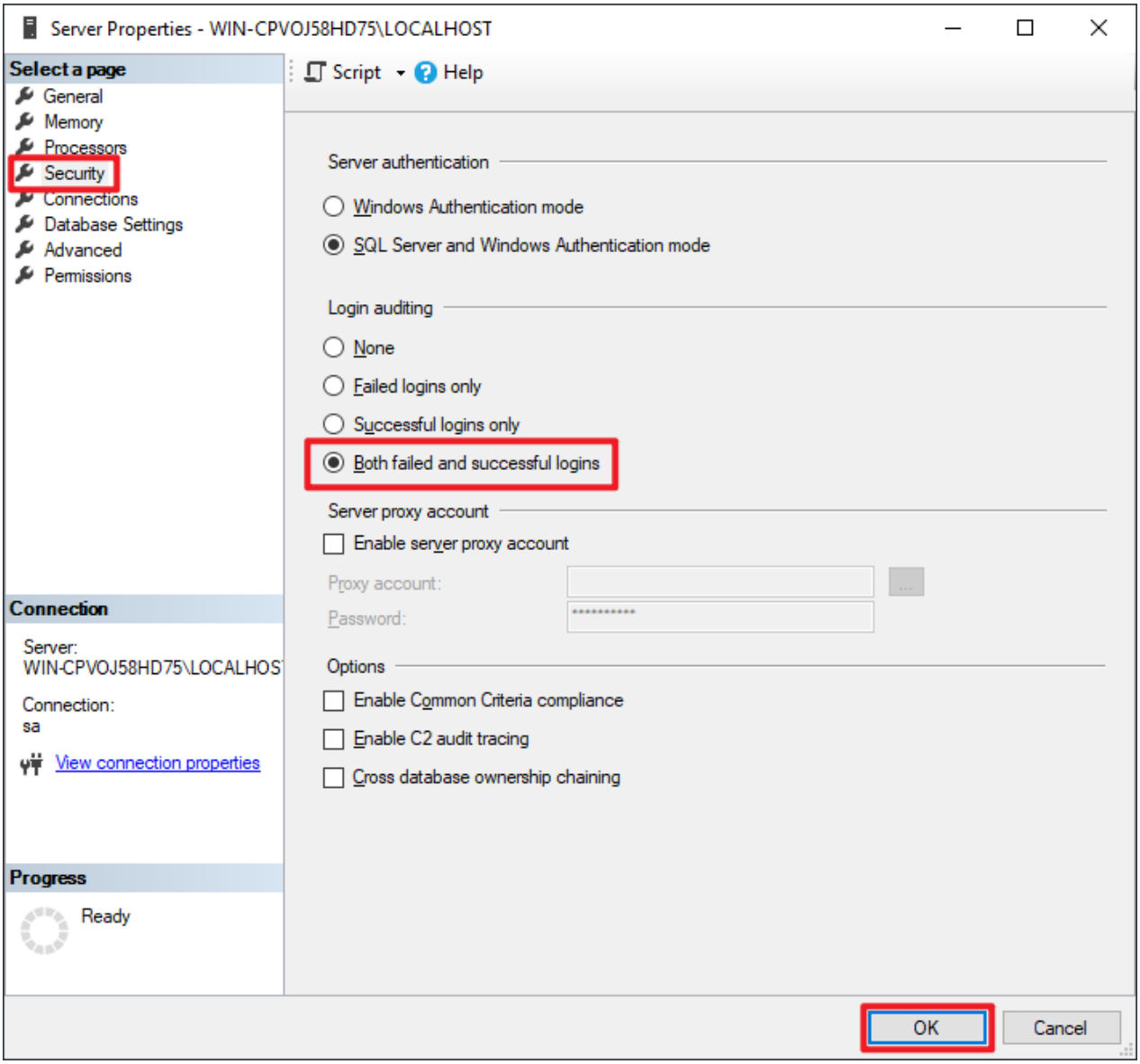
(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

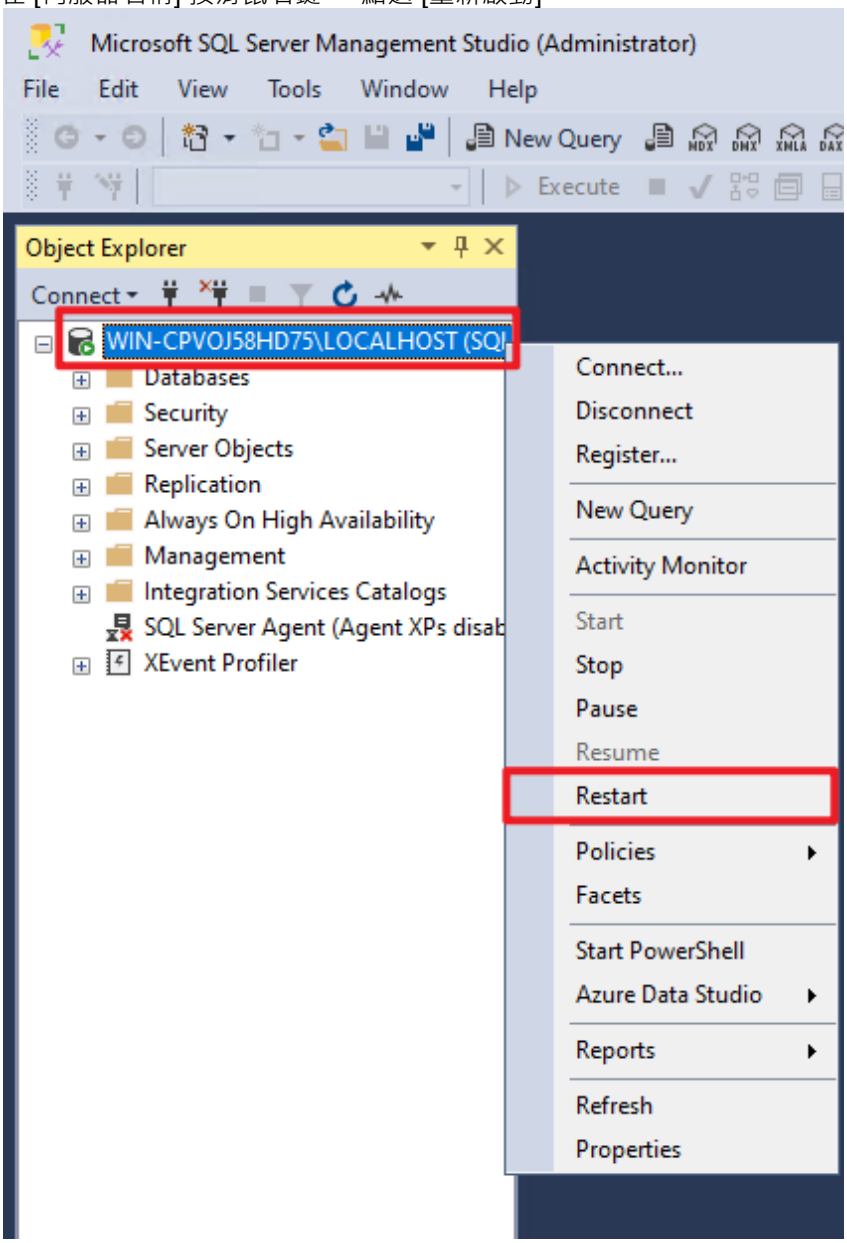


(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 按 [確定]

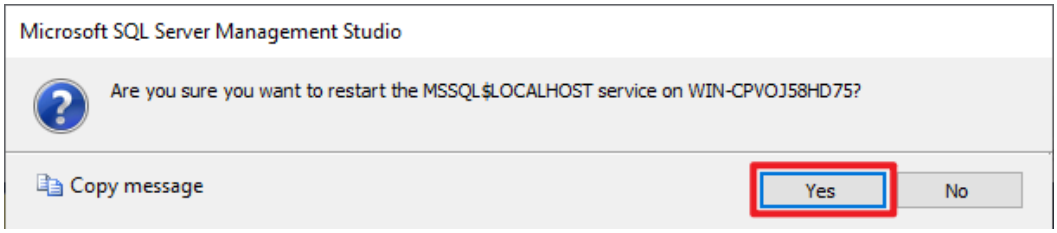


(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MS SQL SERVER 服務



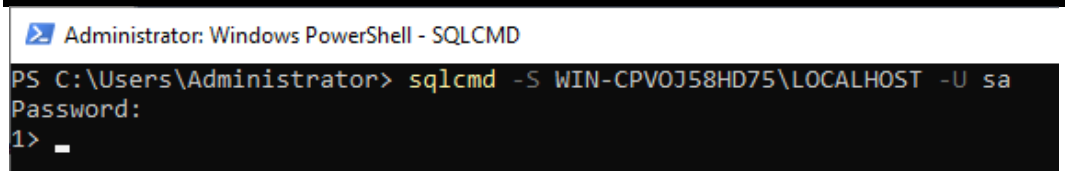
6.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

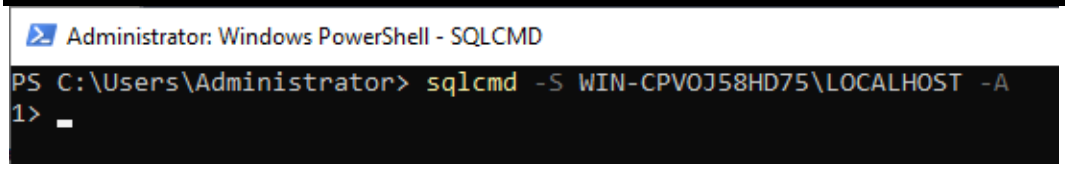
-U login_id

-P password

-A dedicated administrator connection

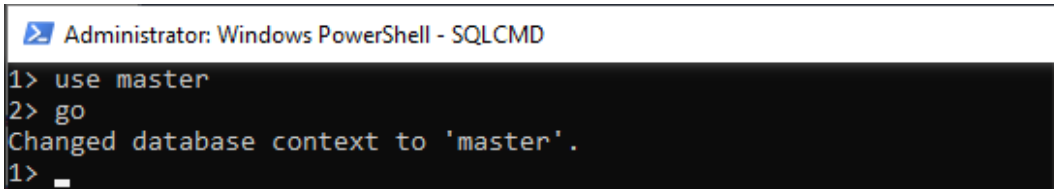
<2.2> 使用 Windows 帳號

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



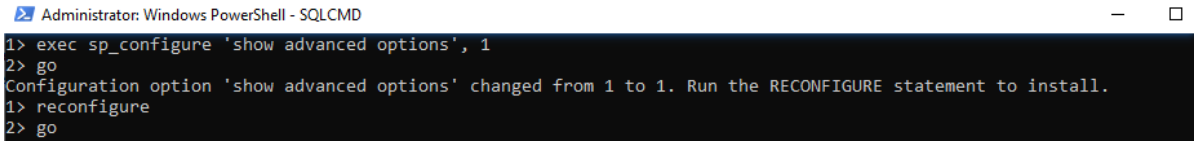
(3) 切換資料庫

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



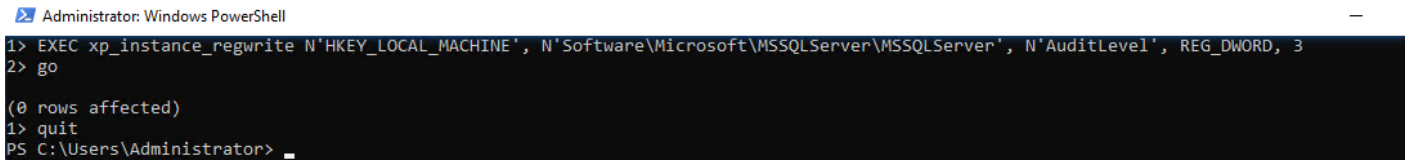
(4) 使用 sp_configure 列出進階選項

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



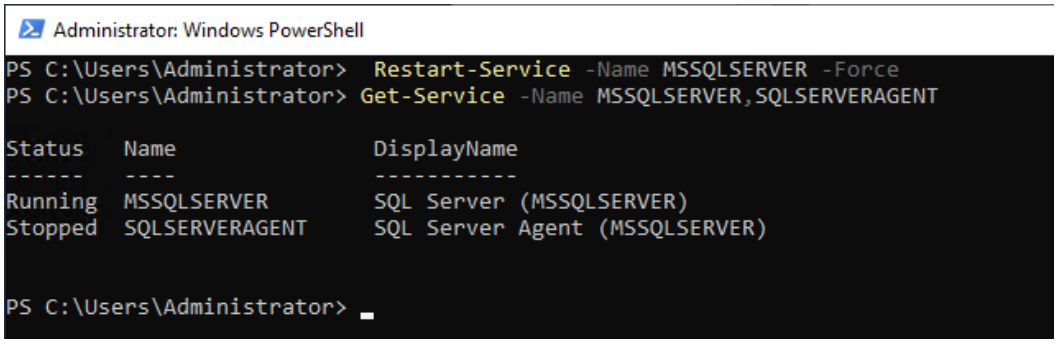
(5) 啟用失敗和成功的登入記錄

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



(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
```



6.2 設定稽核

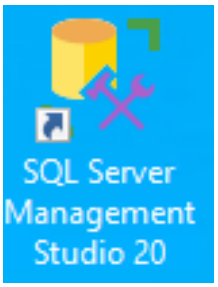
6.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

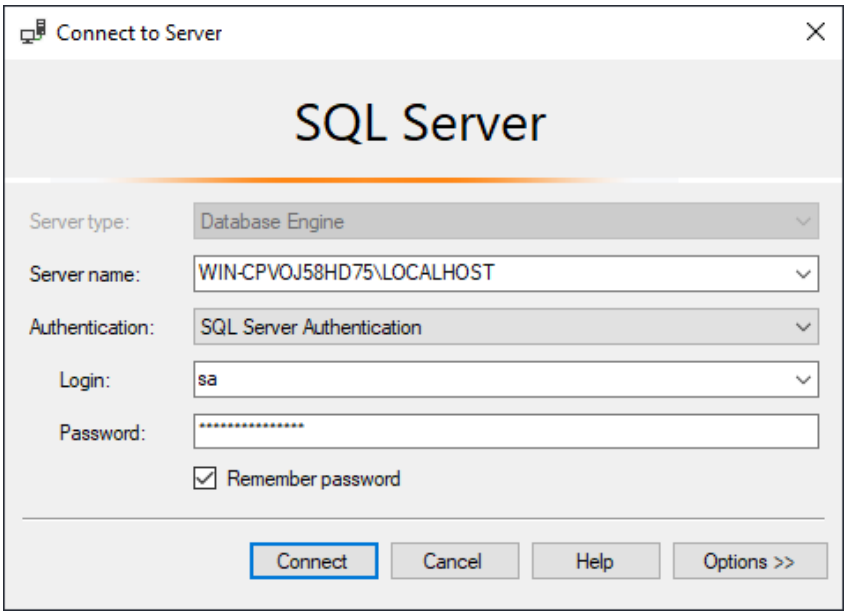
以下分別為圖形介面和指令介面設定方式。

6.2.1.1 使用圖形介面方式設定

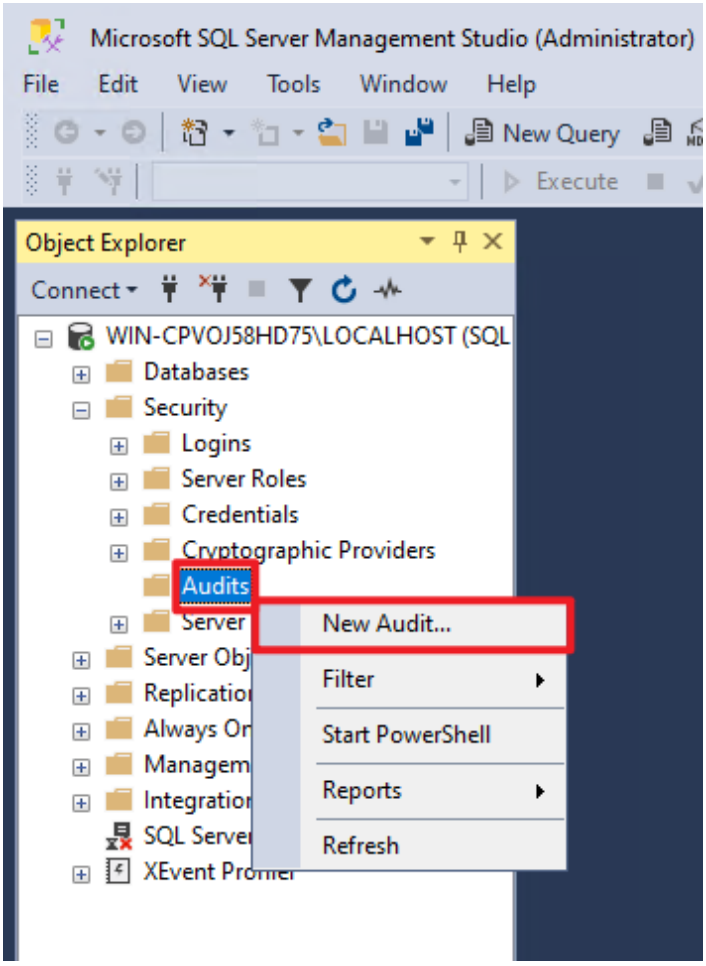
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

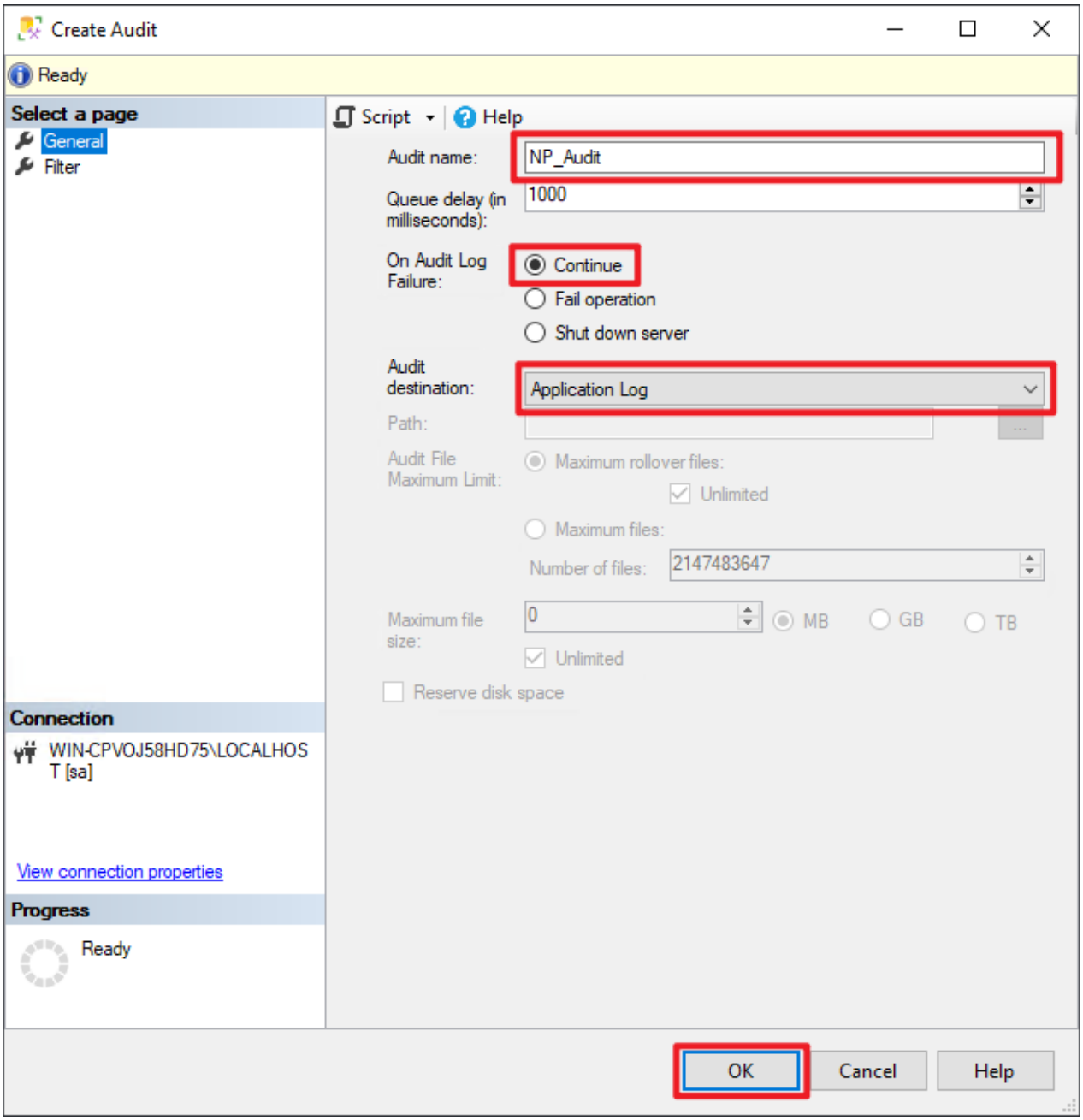


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

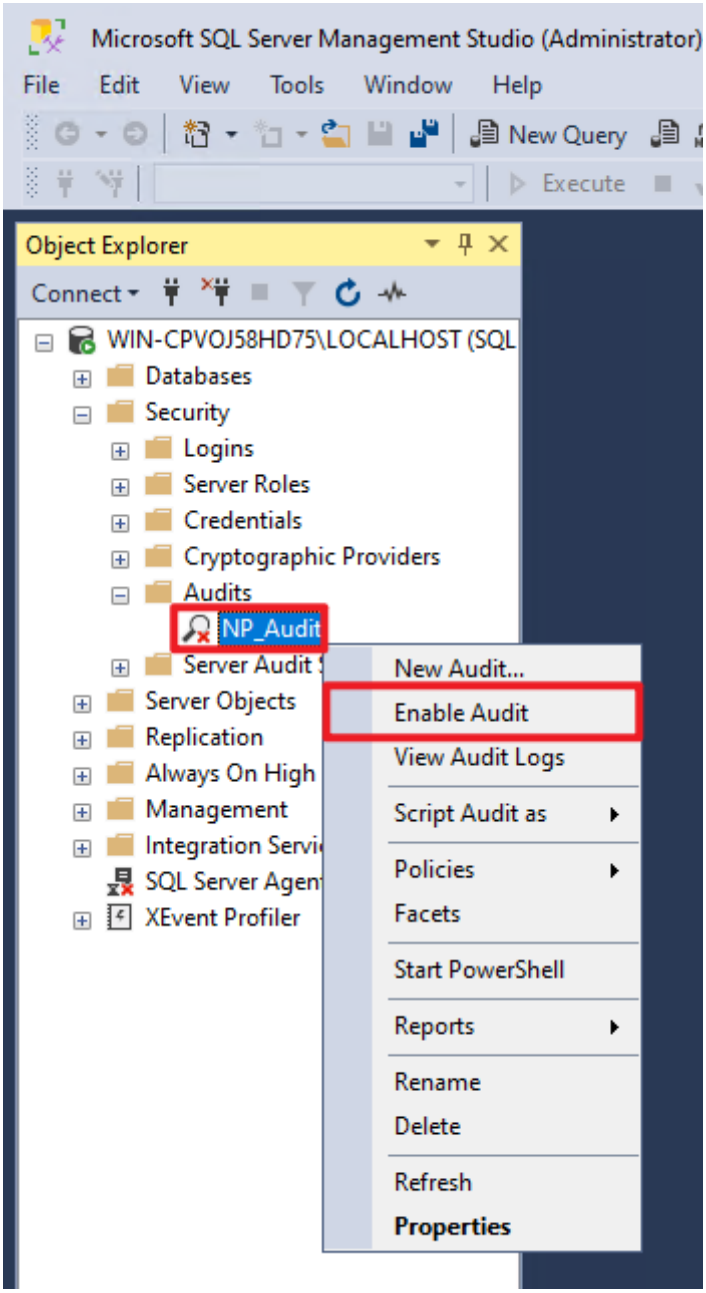


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

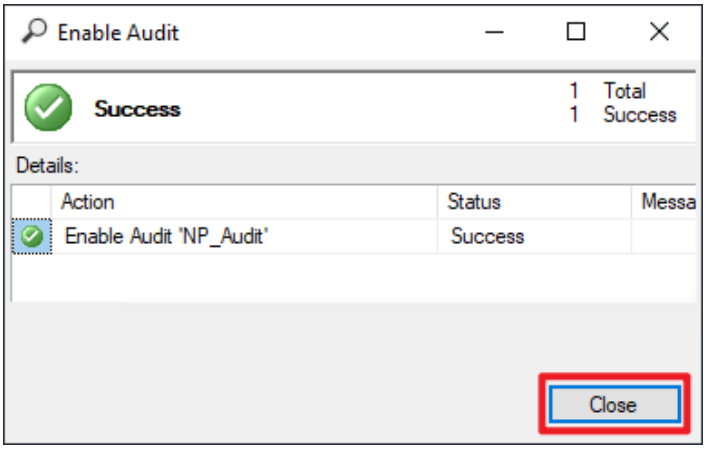
將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]



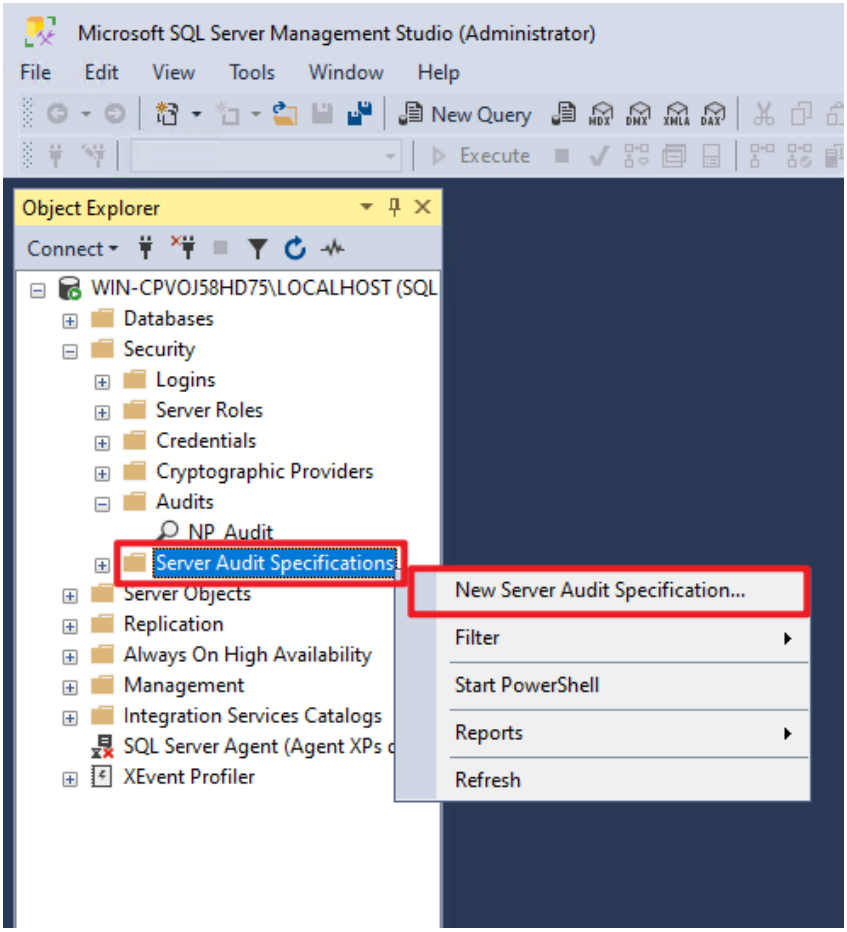
(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



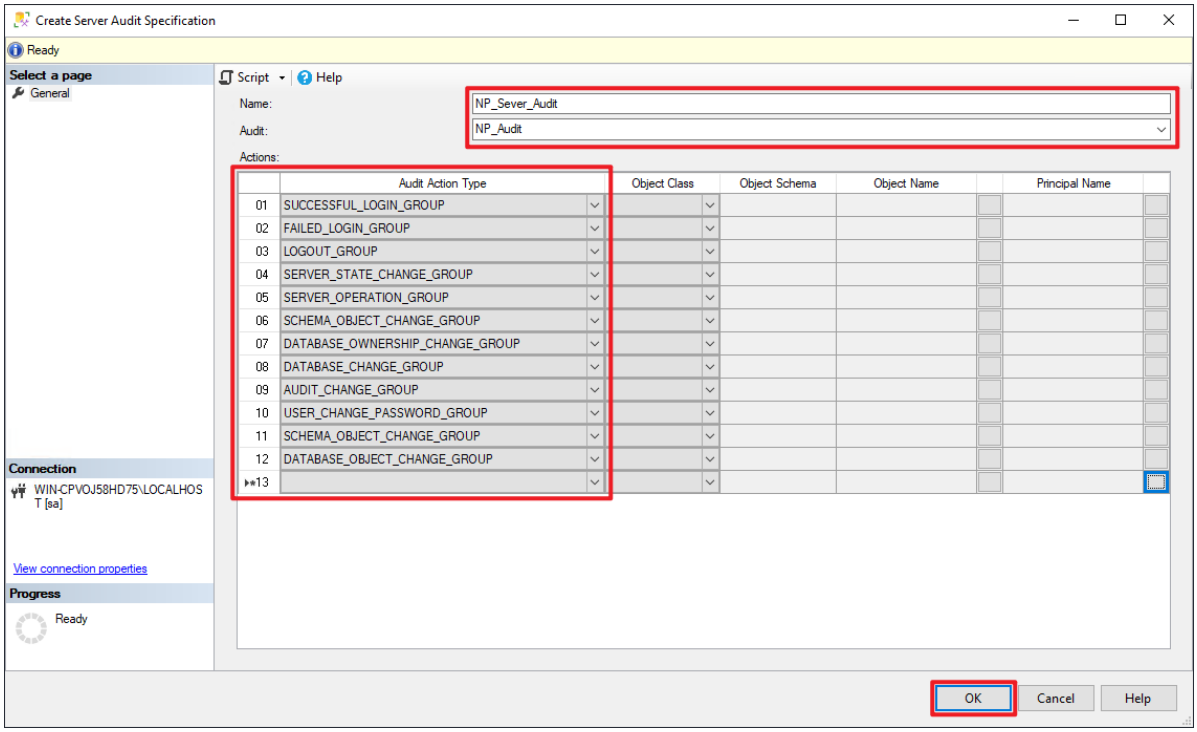
(6)　按 [關閉]



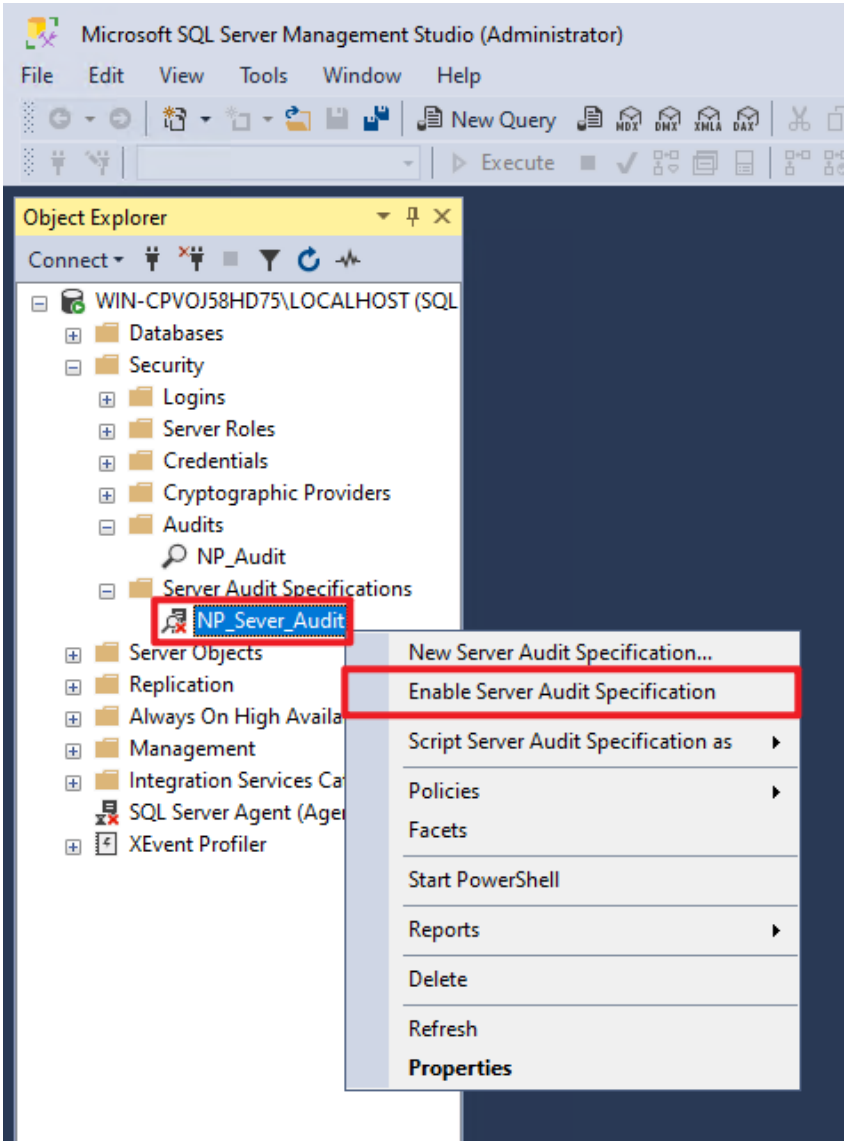
(7) 在 [伺服器稽核規格] 按滑鼠右鍵 -> 點選 [新增伺服器稽核規格...]



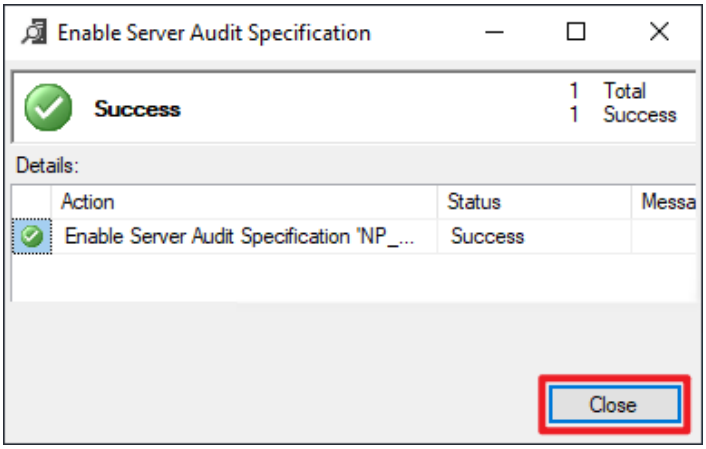
(8) 輸入名稱: `NP_Server_Audit` -> 選擇稽核: [NP_Audit] 和動作 詳細說明請參考前言的稽核動作群組連結 -> 按 [確定]



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



(10)　按 [關閉]



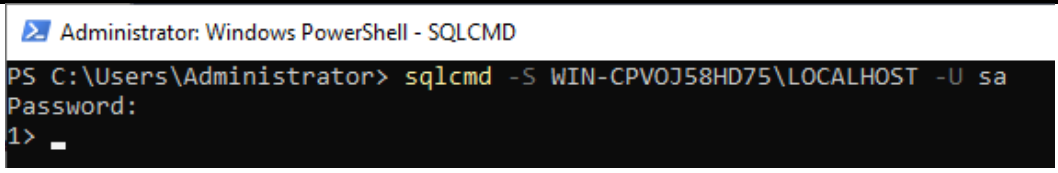
6.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

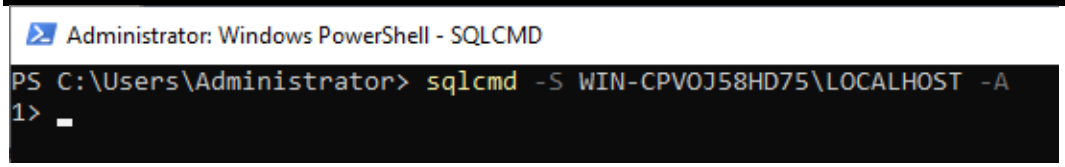
-U login_id

-P password

-A dedicated administrator connection

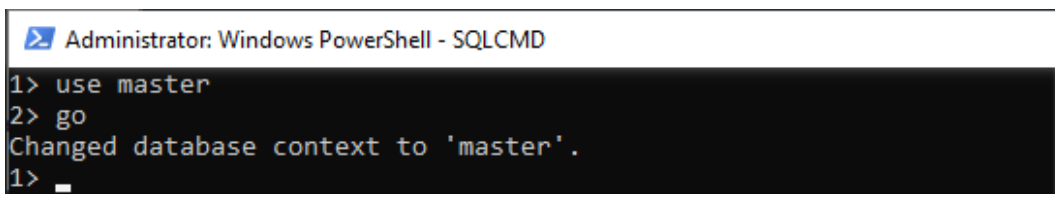
<2.2> 使用 Windows 帳號

```
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
```

Administrator: Windows PowerShell - SQLCMD

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

紅色文字部位請輸入稽核名稱

(5) 設定稽核伺服器，ADD 動作 詳細說明請參考前言的稽核動作群組連結

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

Administrator: Windows PowerShell - SQLCMD

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

紅色文字部位請輸入伺服器稽核規格名稱

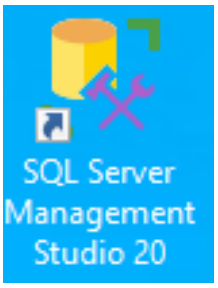
6.2.2 稽核資料庫層級

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

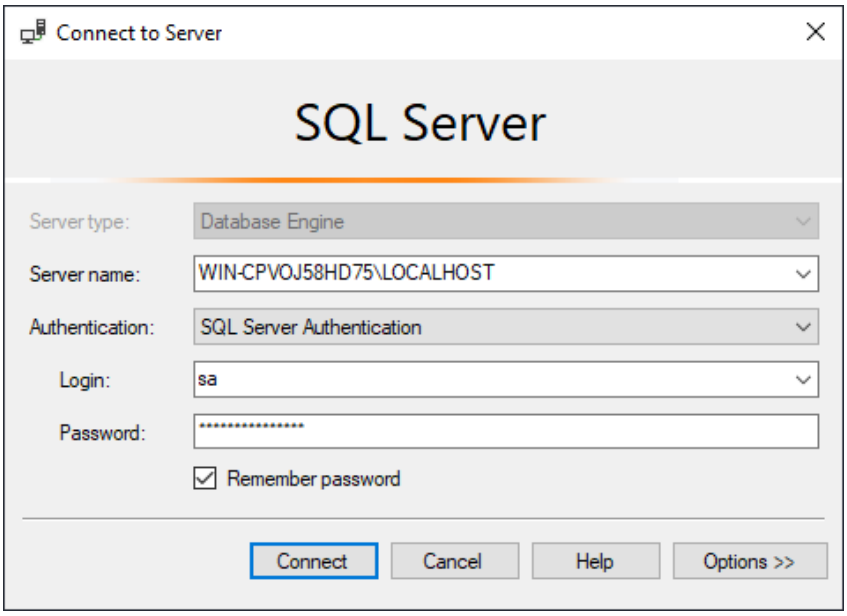
以下分別為圖形介面和指令介面設定方式。

6.2.2.1 使用圖形介面方式設定

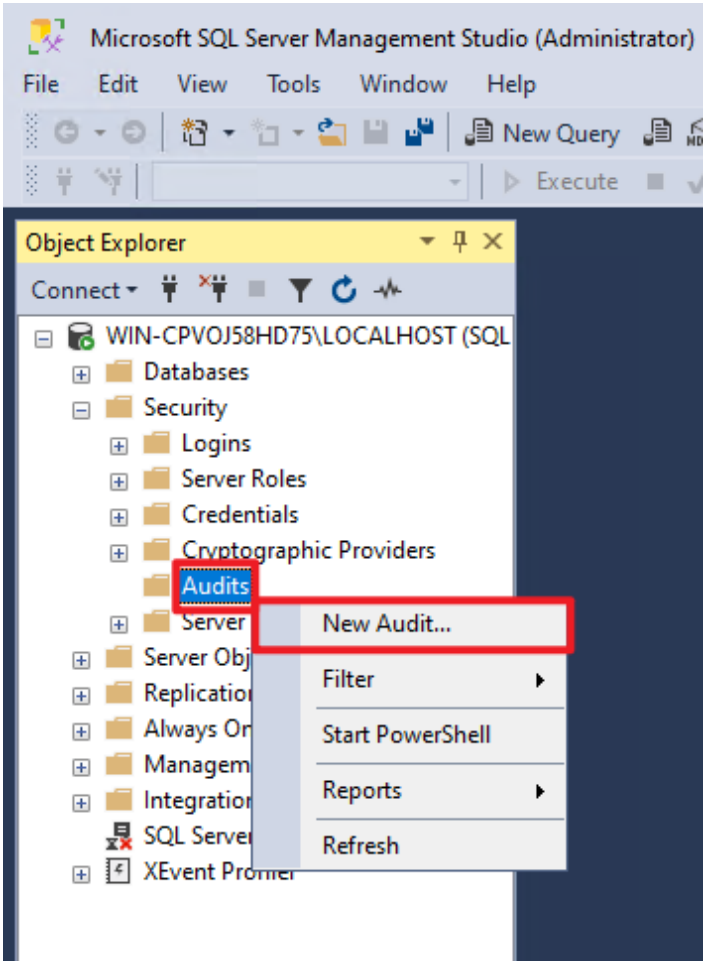
(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

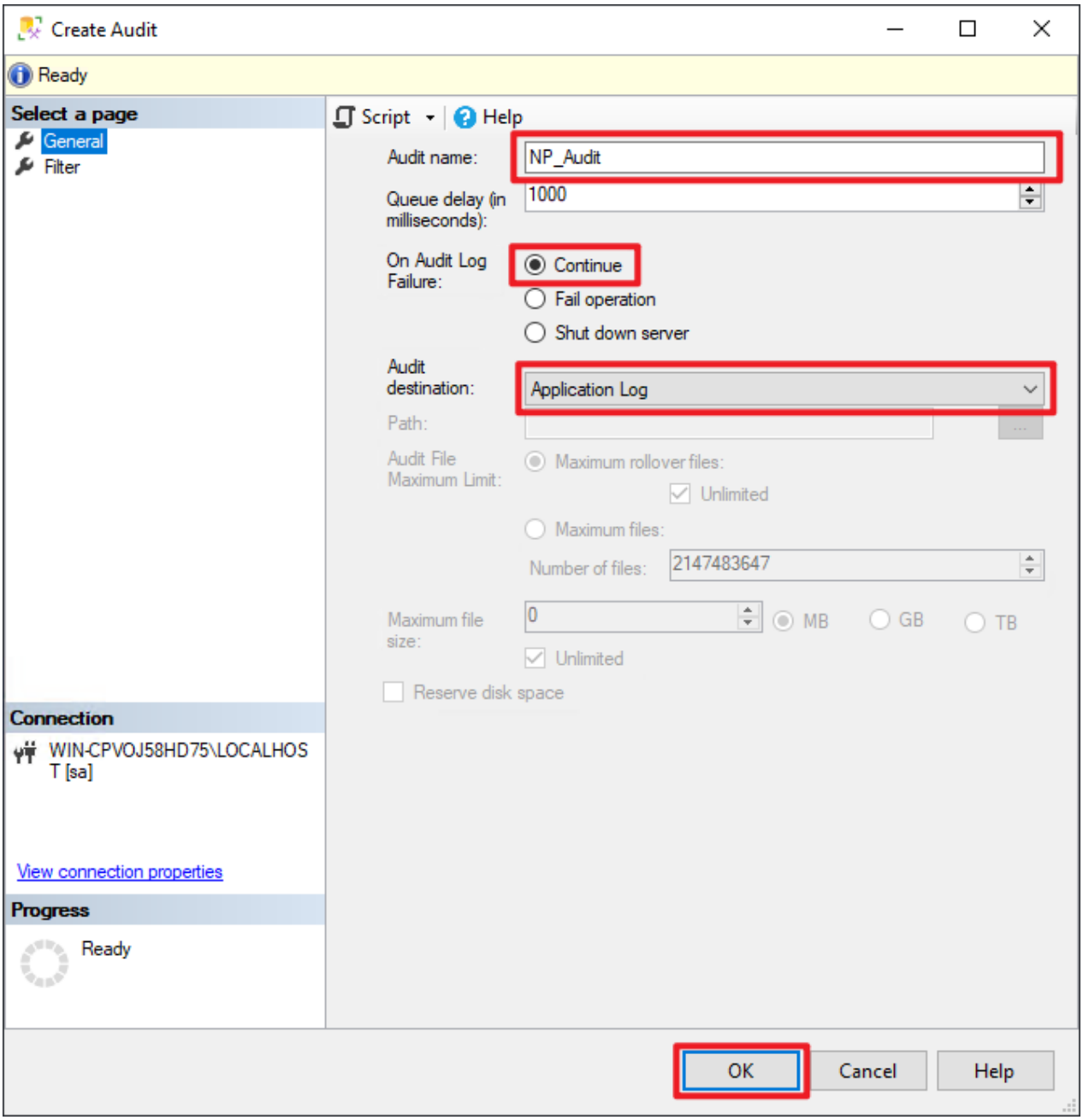


(3) 展開 [安全性] 項目 -> 在 [稽核] 按滑鼠右鍵 -> 點選 [新增稽核...]

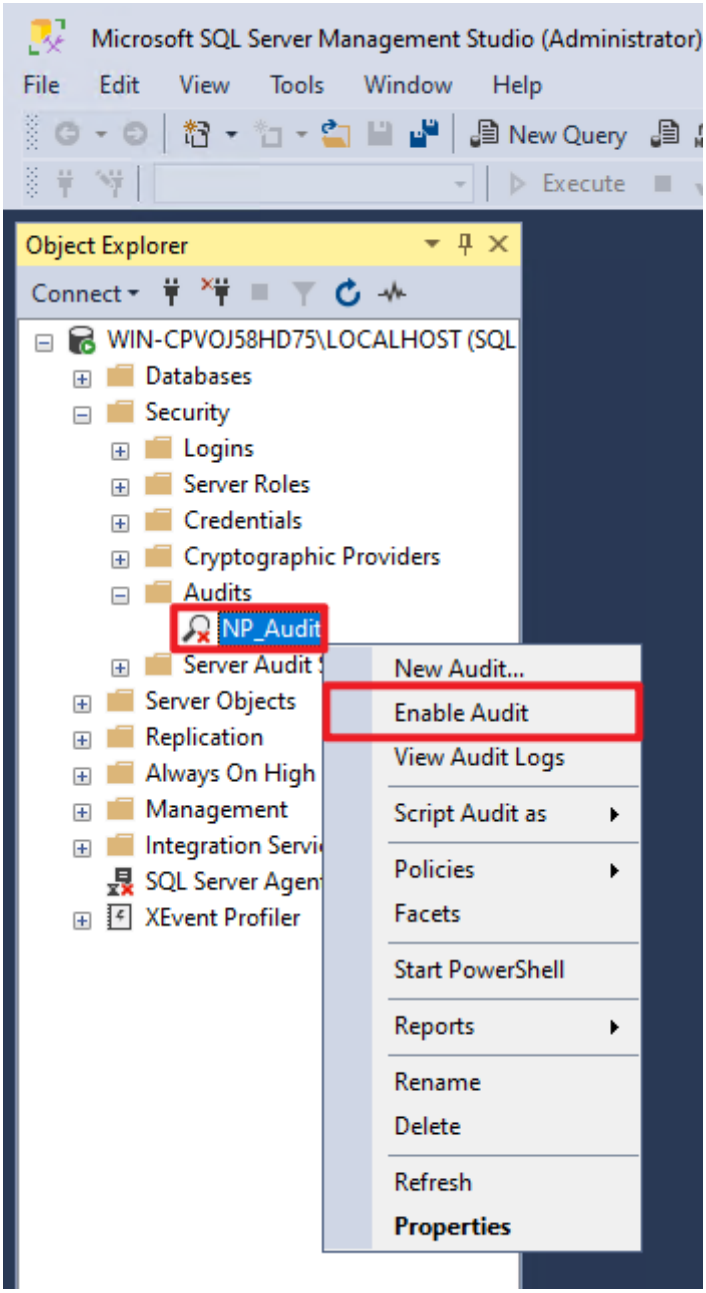


(4) 輸入稽核名稱: NP_Audit -> 點選於稽核記錄失敗時: [繼續] -> 選擇稽核目的地: [應用程式記錄檔]

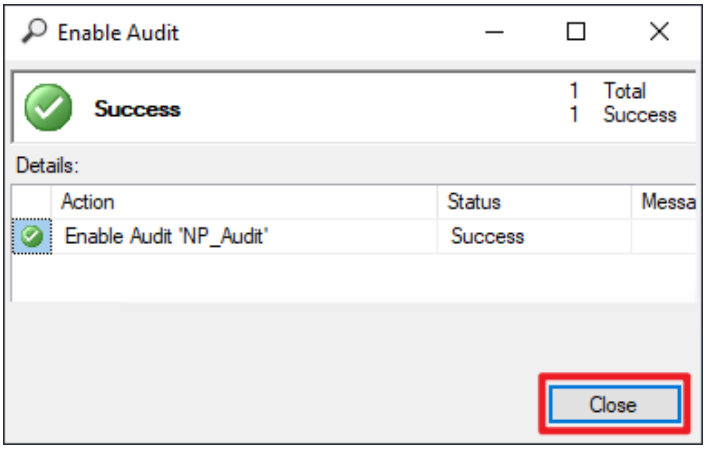
將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]



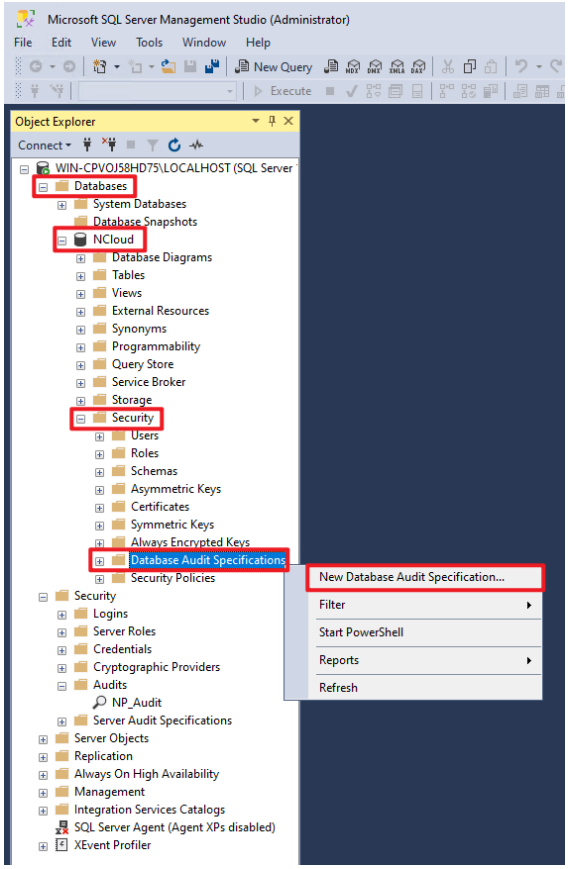
(5)　在稽核名稱: [NP_Audit] 按滑鼠右鍵 -> 點選 [啟用稽核]



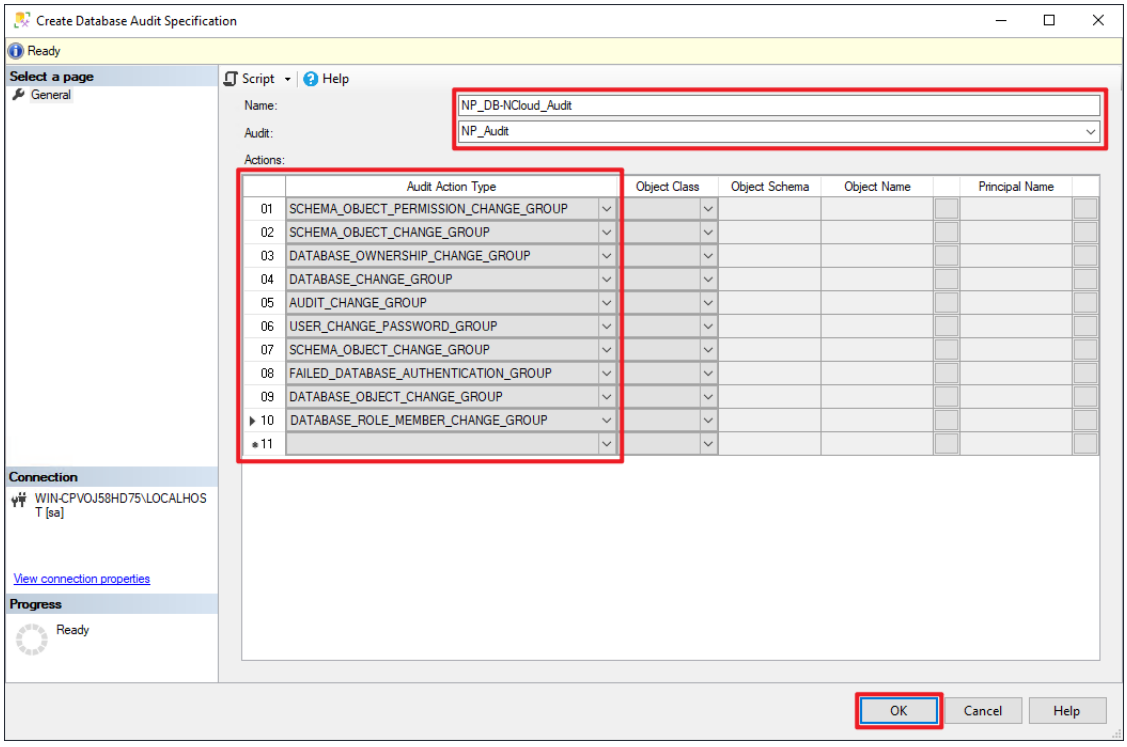
(6)　按 [關閉]



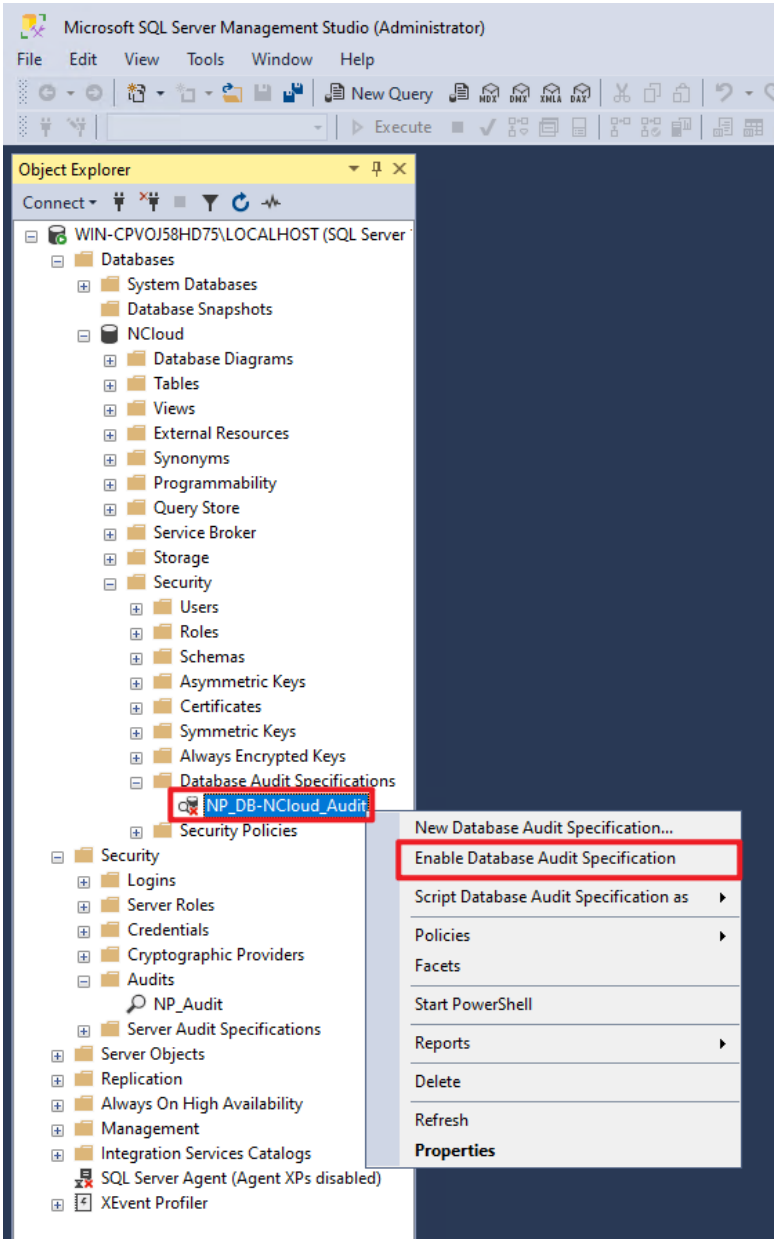
(7) 選擇 [資料庫] 項目 -> 資料庫範例: [NCloud] -> [安全性] -> 在 [資料庫稽核規格] 按滑鼠右鍵 -> 點選 [新增資料庫稽核規格...]



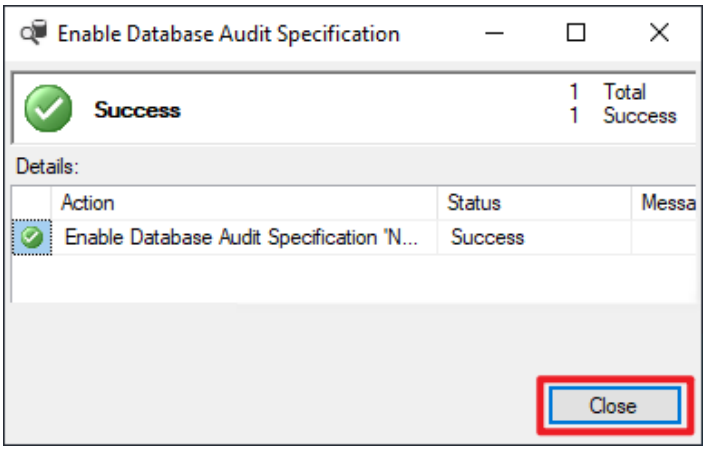
(8) 輸入稽核名稱: `NP_DB-NCloud_Audit` -> 選擇稽核: [NP_Audit] 和動作 詳細說明請參考前言的稽核動作群組連結 **-> 按 [確定]**



(9)　在資料庫稽核規格名稱: [NP_DB-NCloud_Audit] 按滑鼠右鍵 -> 點選 [啟用資料庫稽核規格]



(10)　按 [關閉]



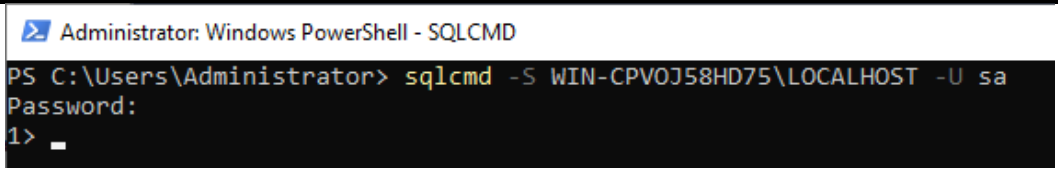
6.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]

(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

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



Options:

-S [protocol:]server[instance_name][,port]

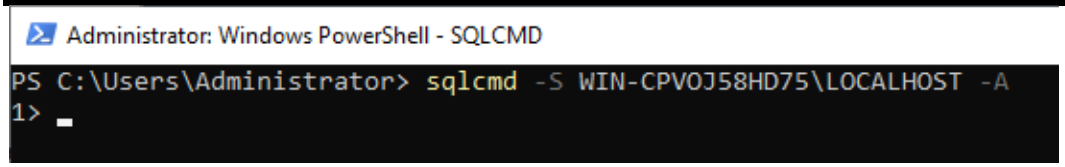
-U login_id

-P password

-A dedicated administrator connection

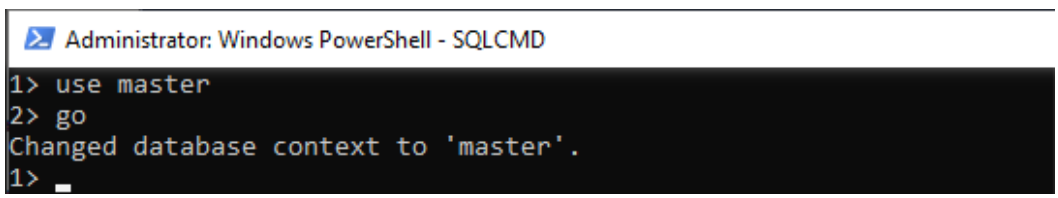
<2.2> 使用 Windows 帳號

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



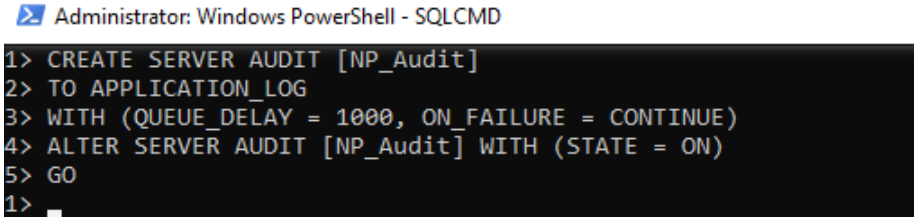
(3) 切換資料庫

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



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

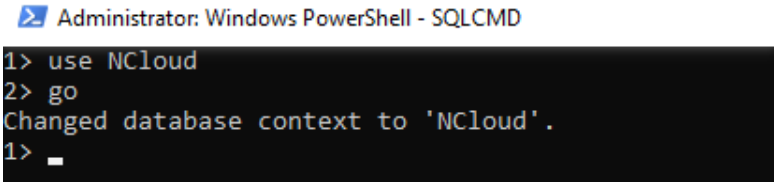
```
1 > CREATE SERVER AUDIT [NP_Audit]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫，範例： NCloud

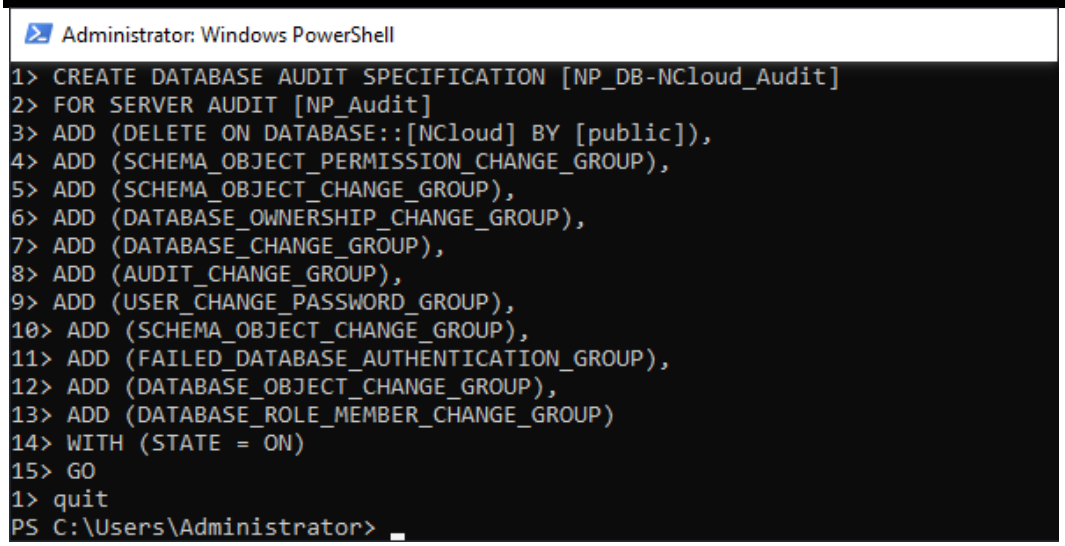
```
1 > use NCloud
2 > go
```



紅色文字部位請輸入稽核資料庫名稱

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

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



紅色文字部位請輸入資料庫稽核規格名稱

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

紅色文字部位請輸入稽核資料庫名稱

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

6.3 事件記錄檔設定

此為選項設定。

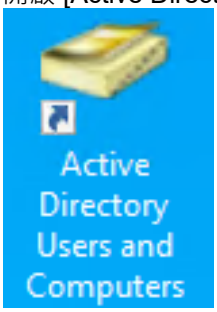
以下分別為網域和工作群組設定方式。

6.3.1 網域

6.3.1.1 組織單位設定

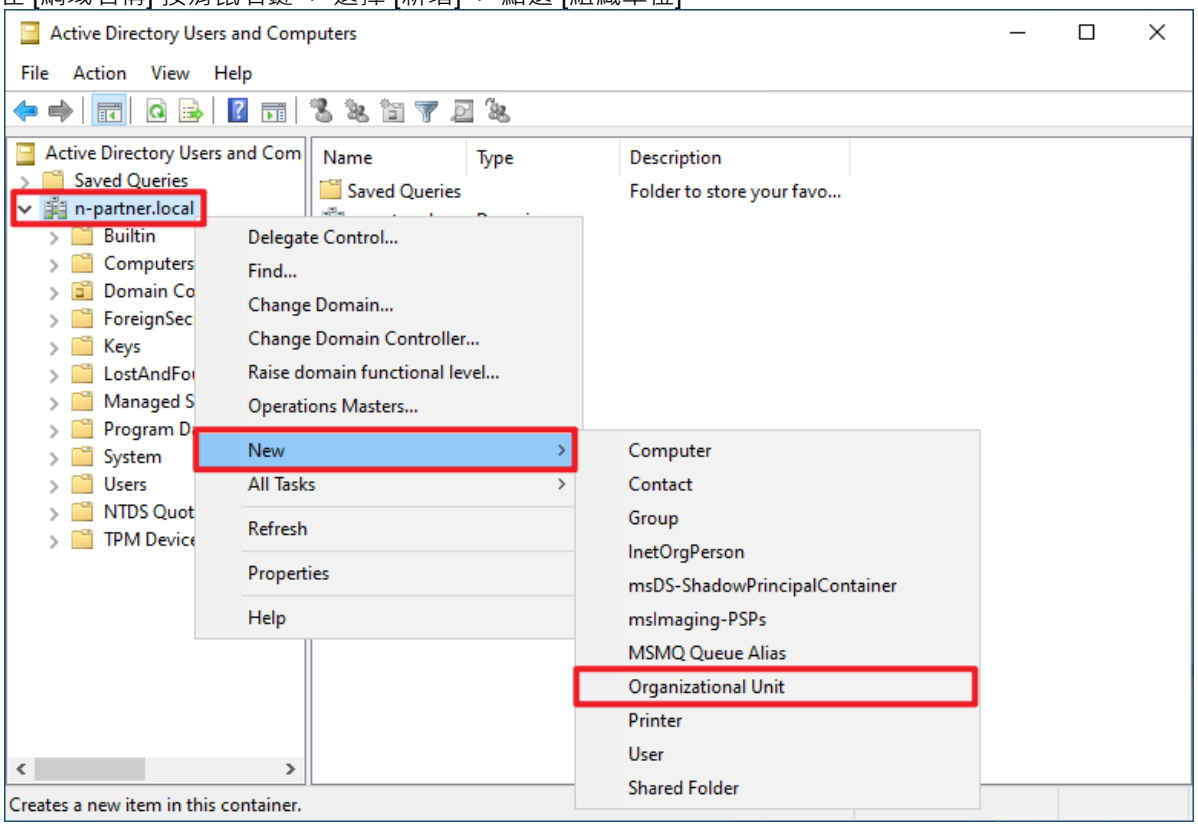
(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]



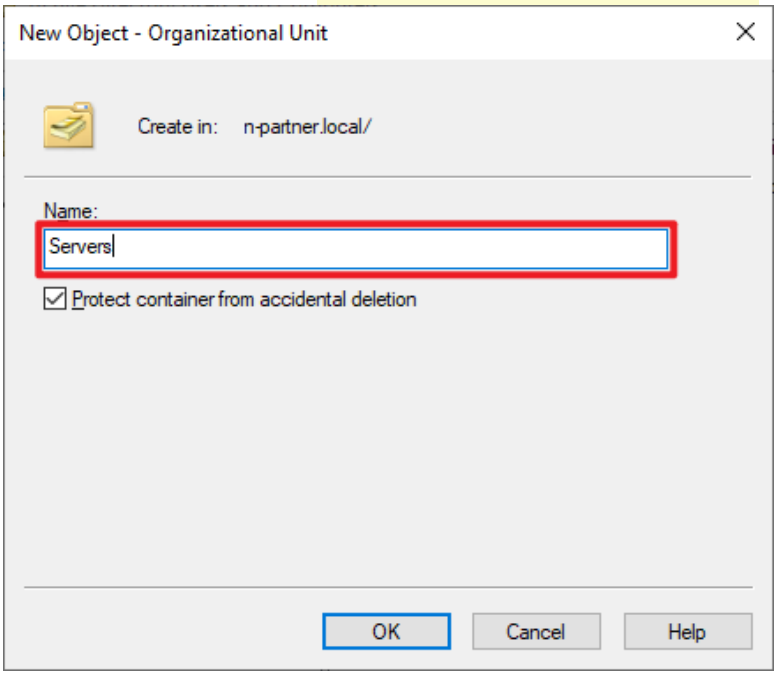
(2) 新增組織單位

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



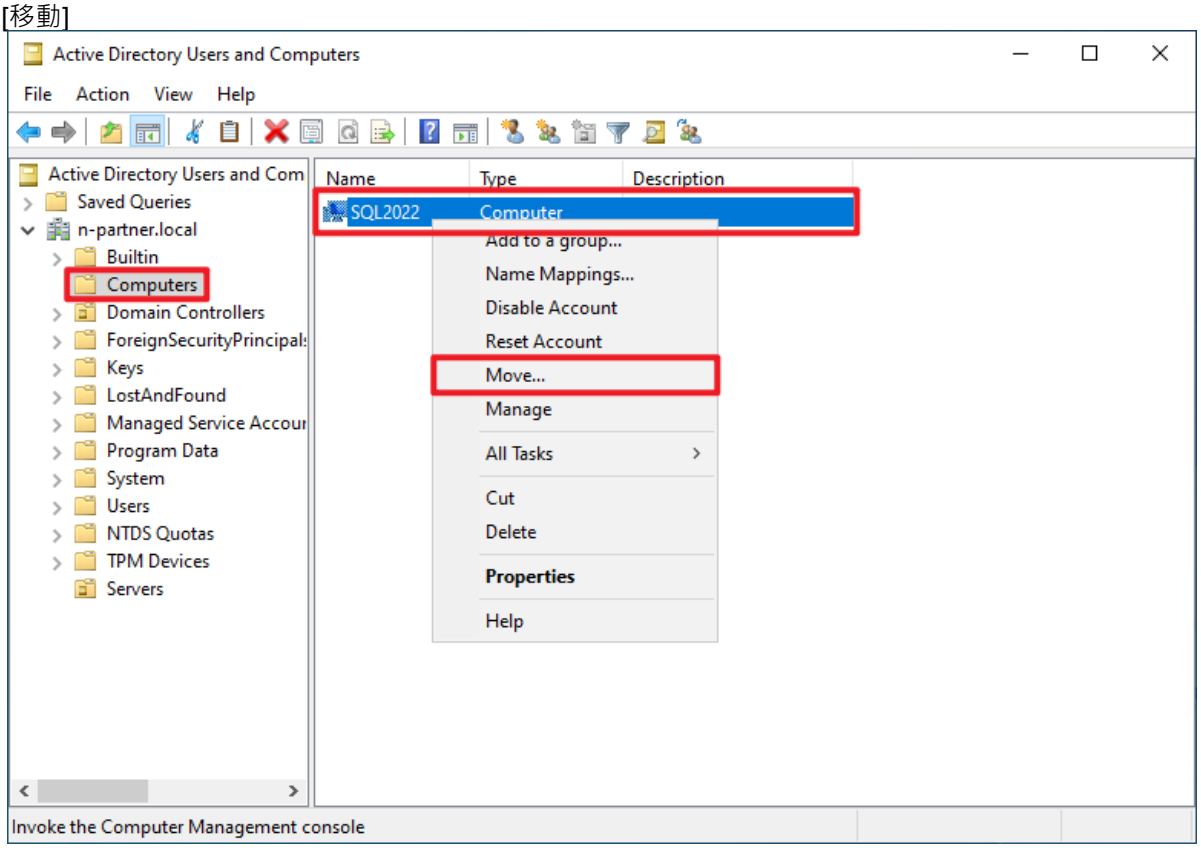
(3) 輸入組織單位名稱

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



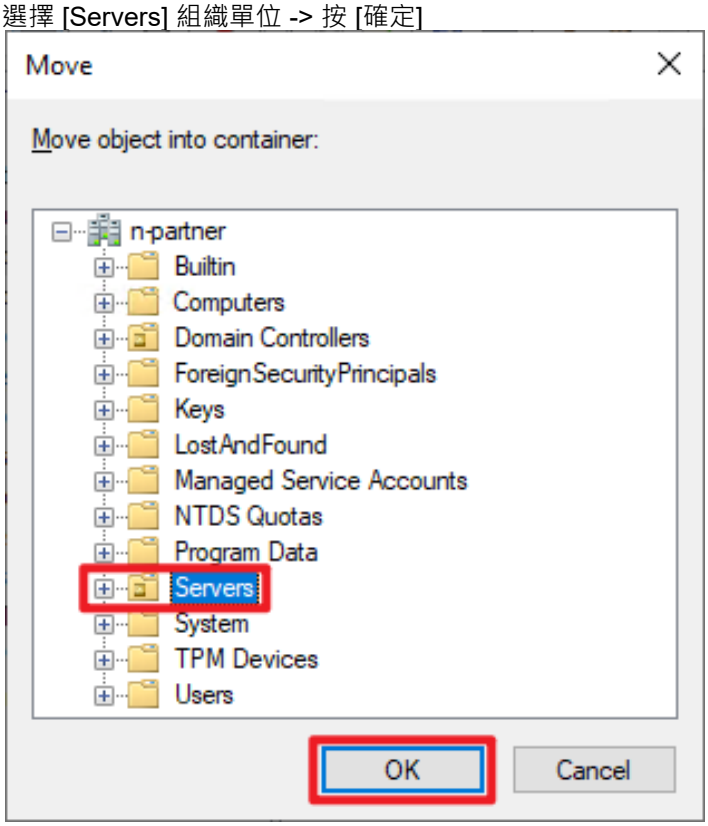
(4) 移動伺服器至新的組織單位

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



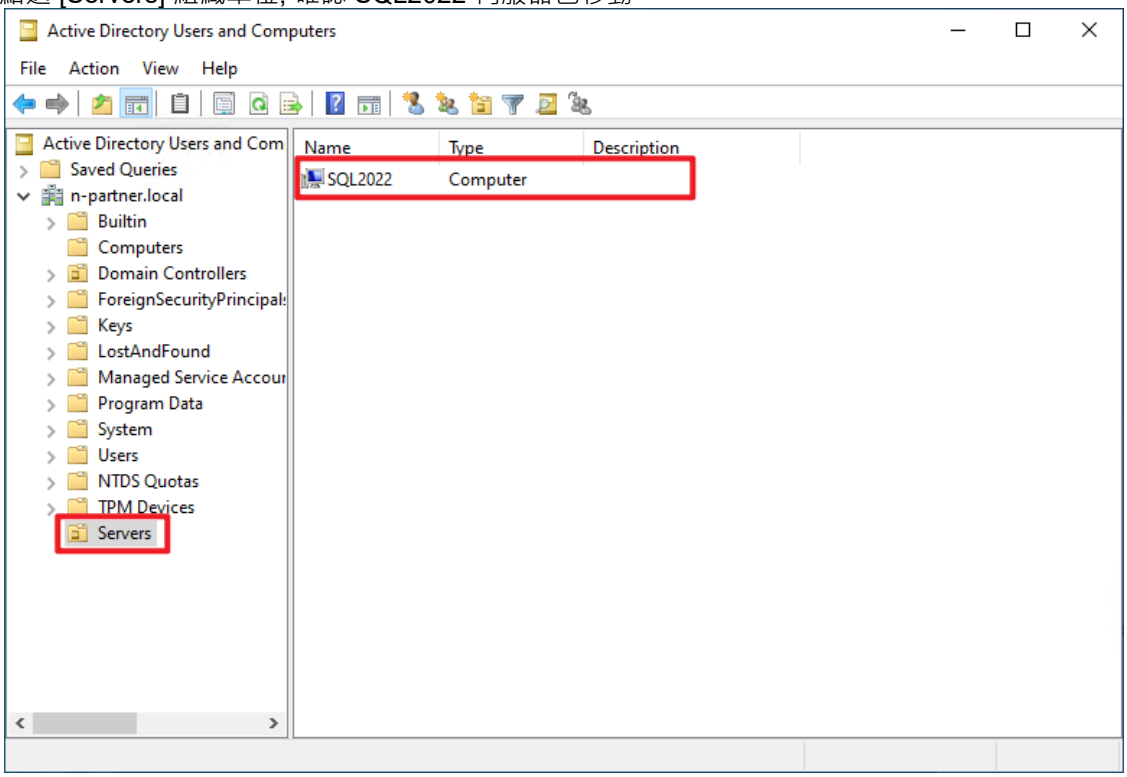
(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]



(6) 確認伺服器已移動至新的組織單位

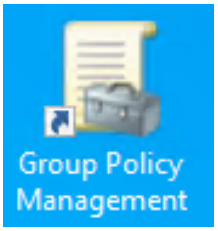
點選 [Servers] 組織單位, 確認 SQL2022 伺服器已移動。



6.3.1.2 群組原則設定

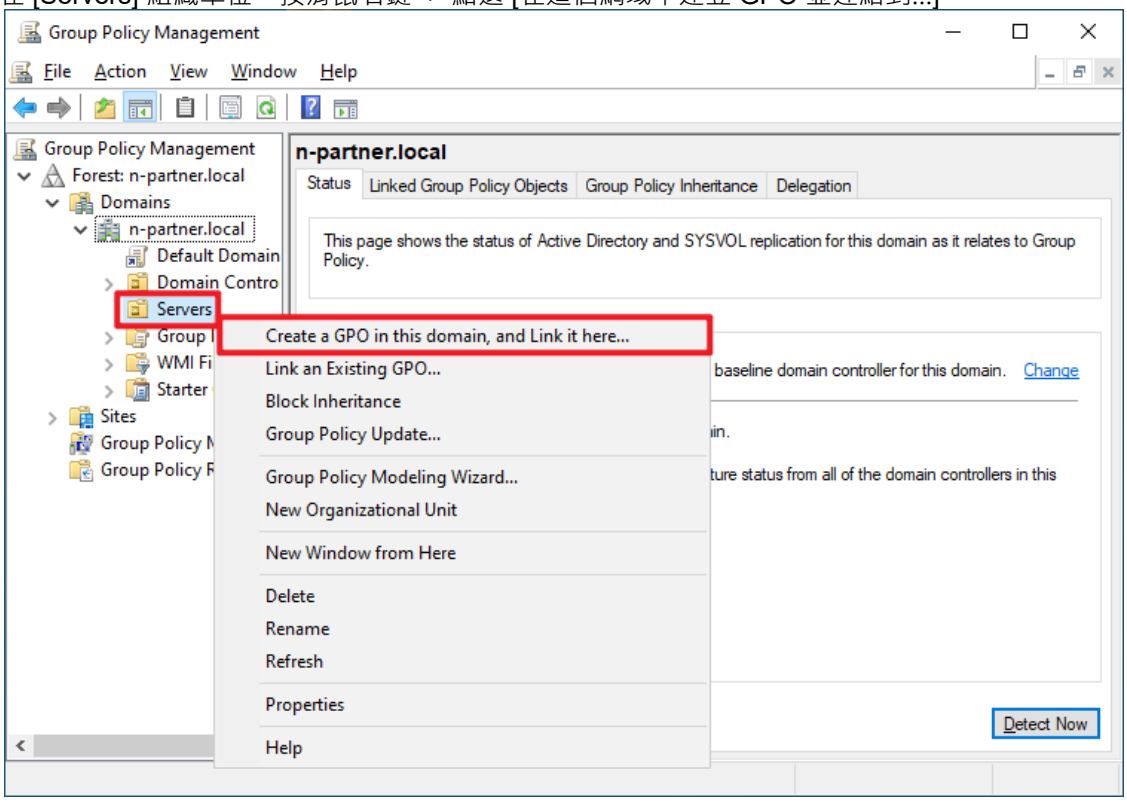
(1) 開啟群組原則管理

開啟 [群組原則管理]



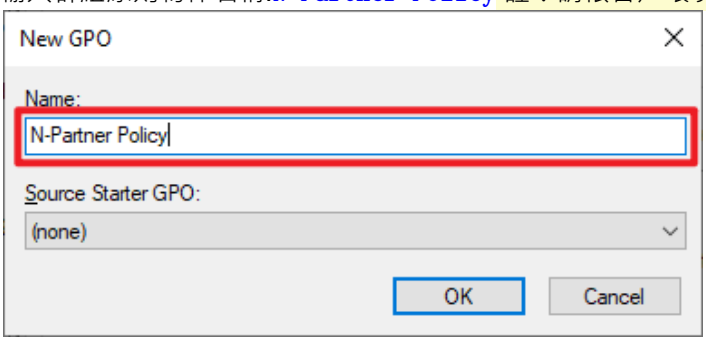
(2) 在 Servers 組織單位，新增群組原則物件

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



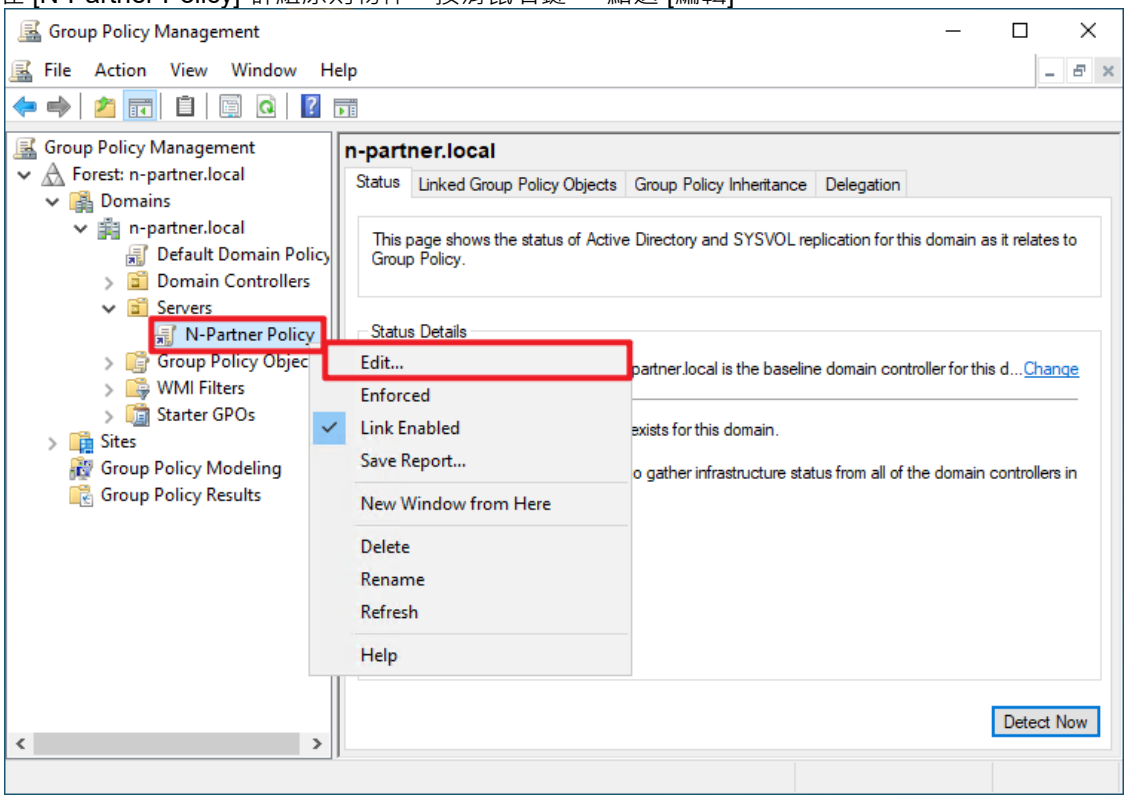
(3) 輸入群組原則物件名稱

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



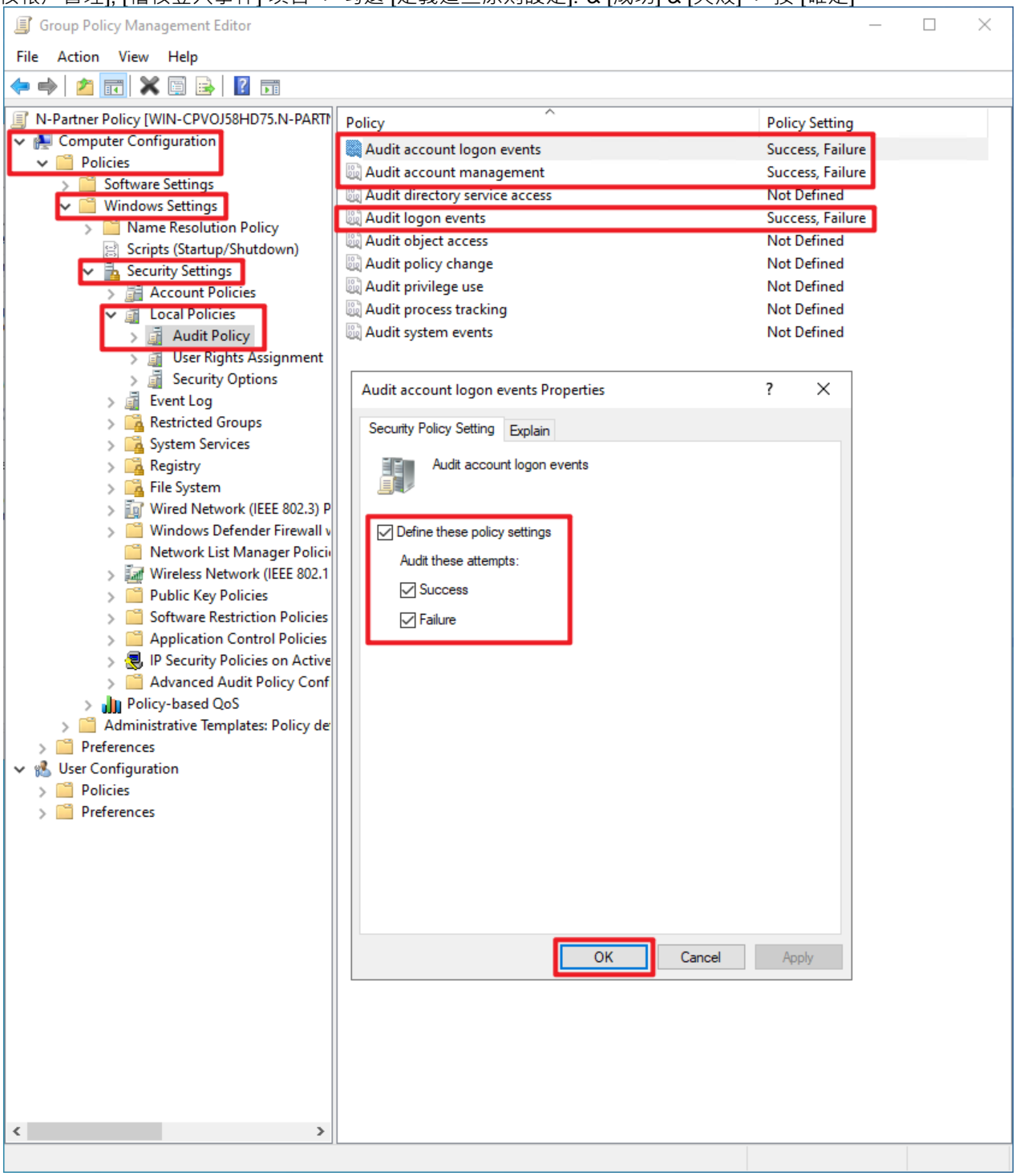
(4) 編輯群組原則物件

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



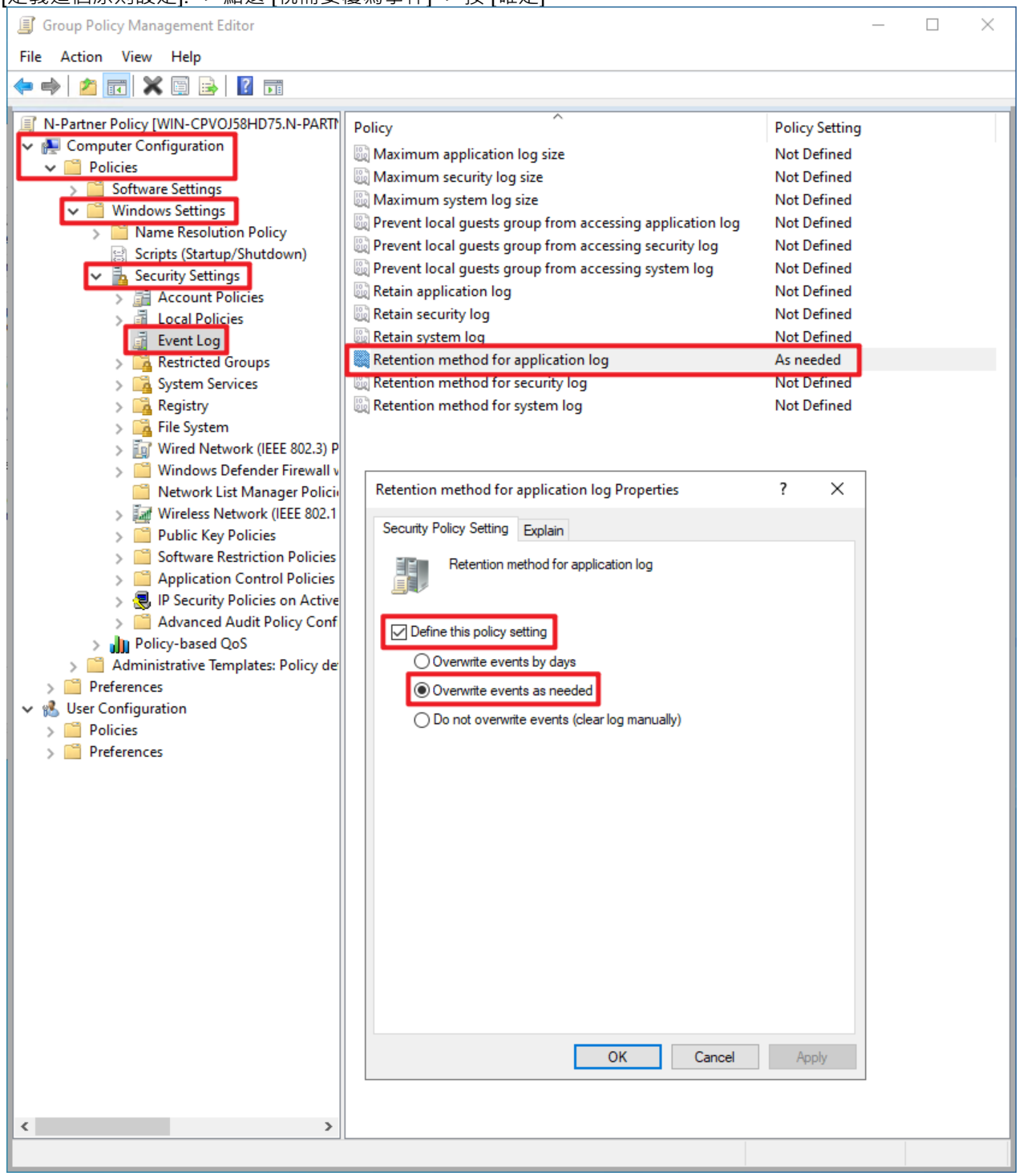
(5) 本機原則：稽核原則

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



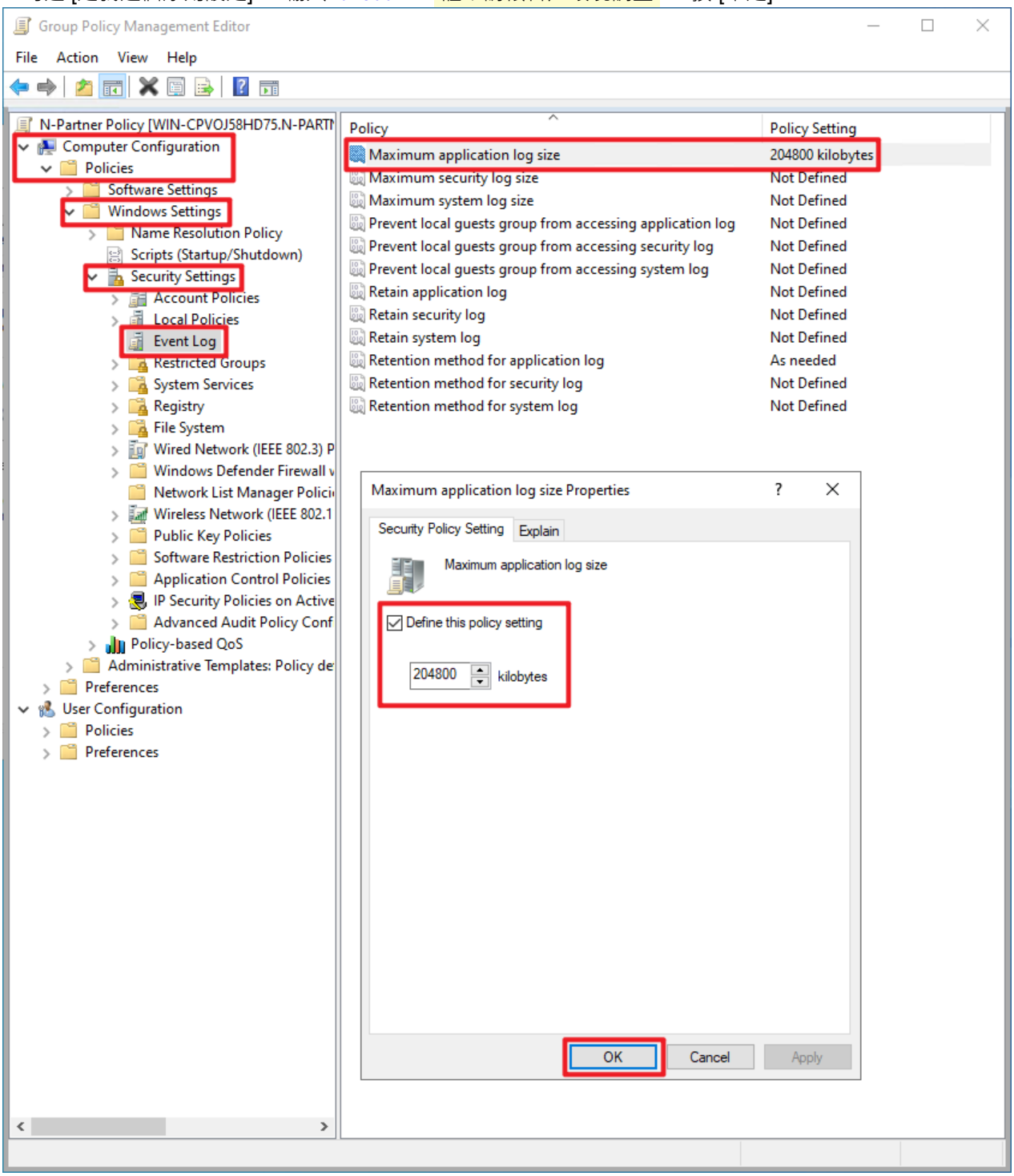
(6) 事件記錄：應用程式記錄保持方法

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



(7) 事件記錄：應用程式記錄檔大小最大值

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



(8) 開啟 [Windows PowerShell]

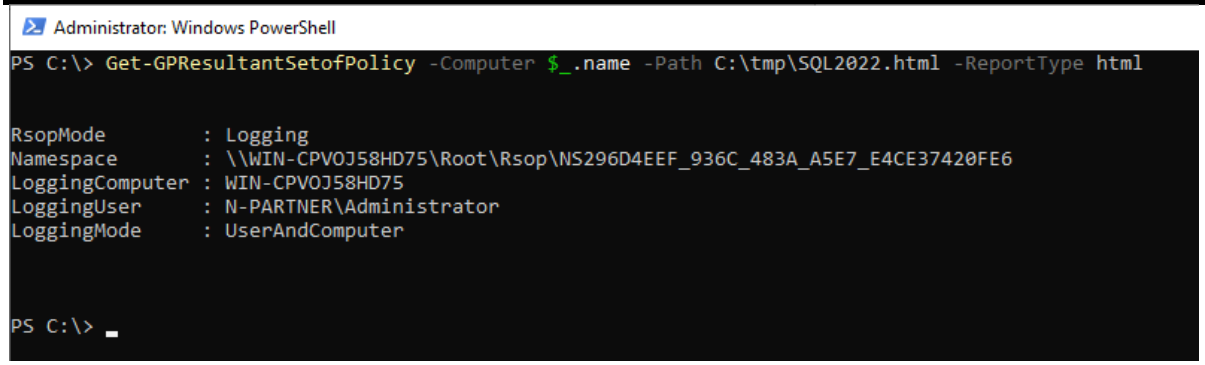
(9) 更新 MS SQL Server 群組原則

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

紅色文字部位請輸入 MS SQL Server 伺服器名稱

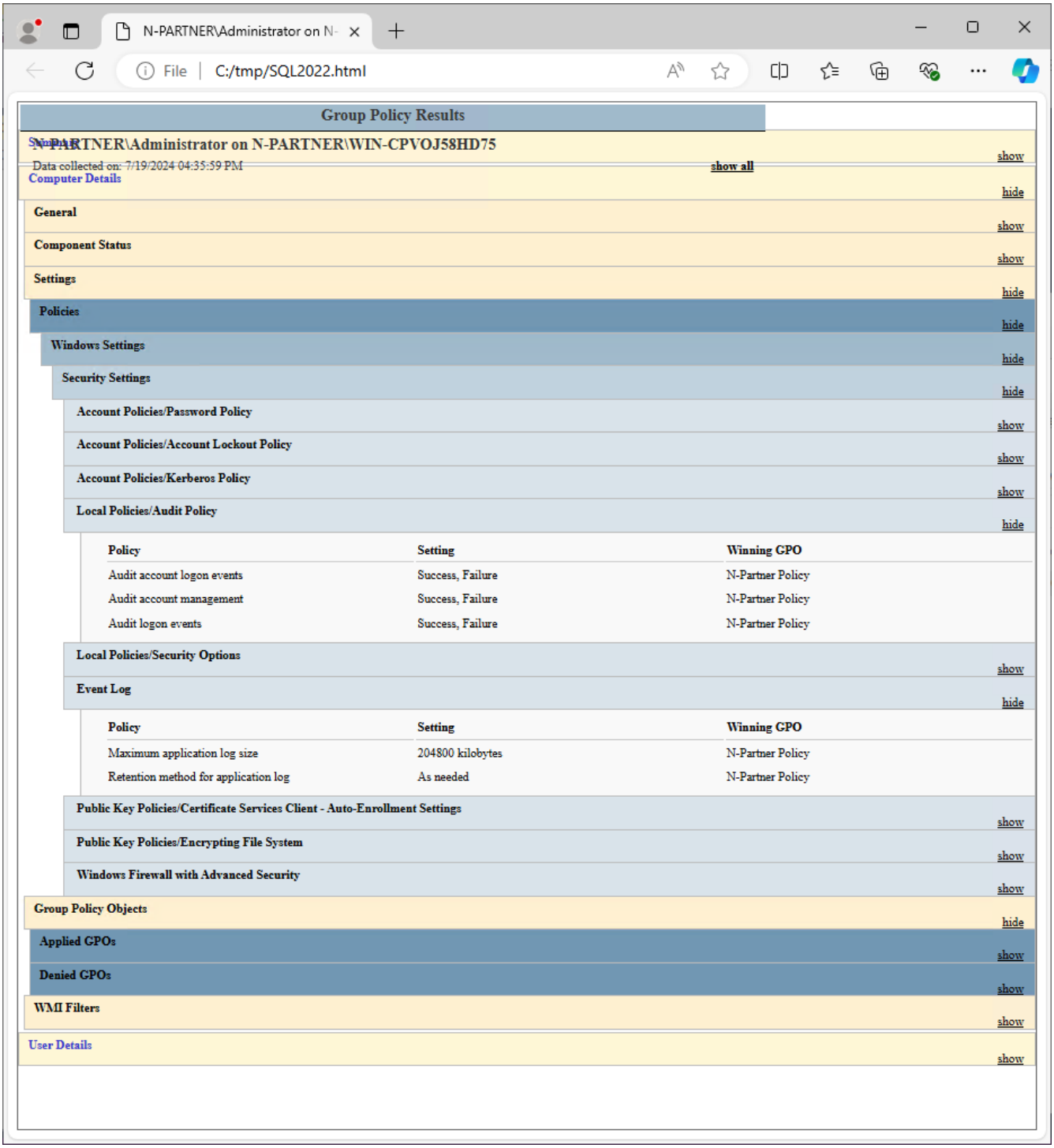
(10) 產生 MS SQL Server 伺服器群組原則報表

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

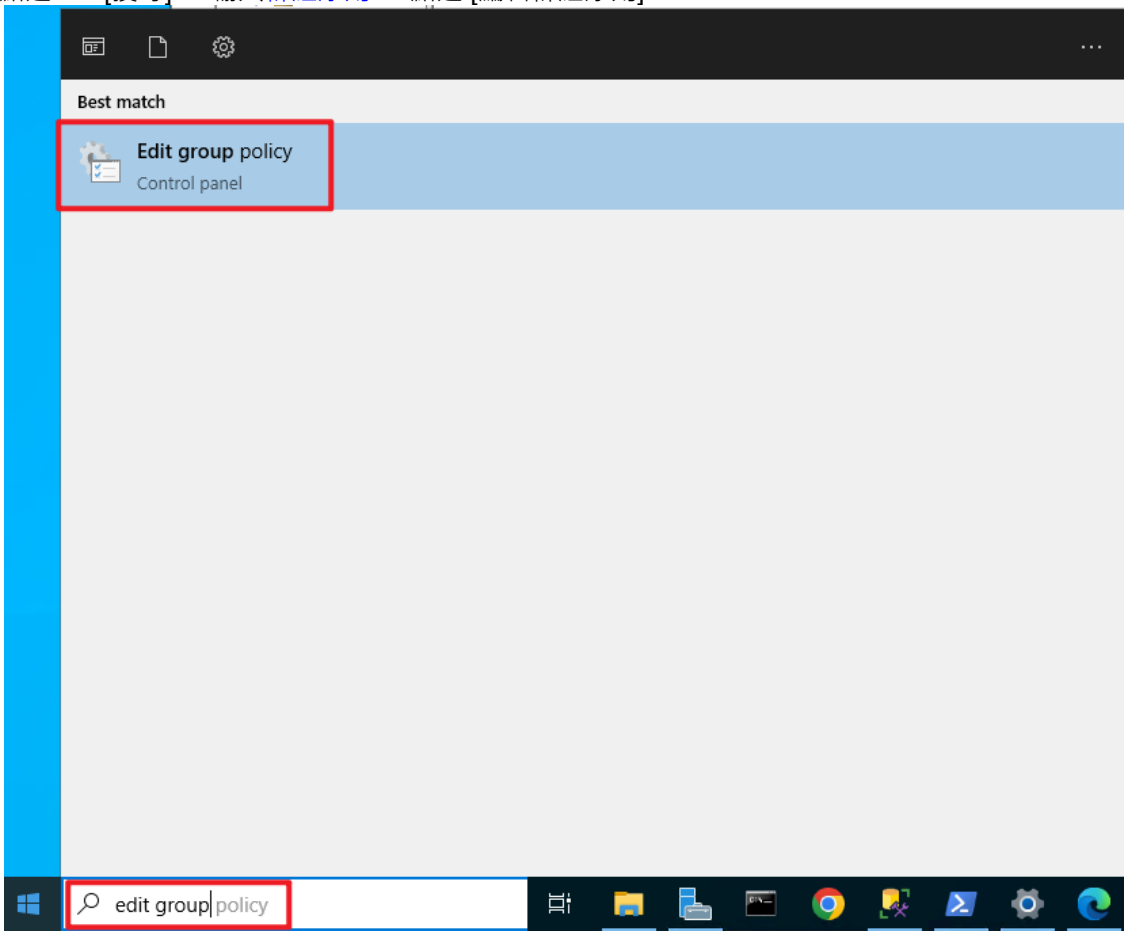


6.3.2 工作群組

6.3.2.1 稽核原則設定

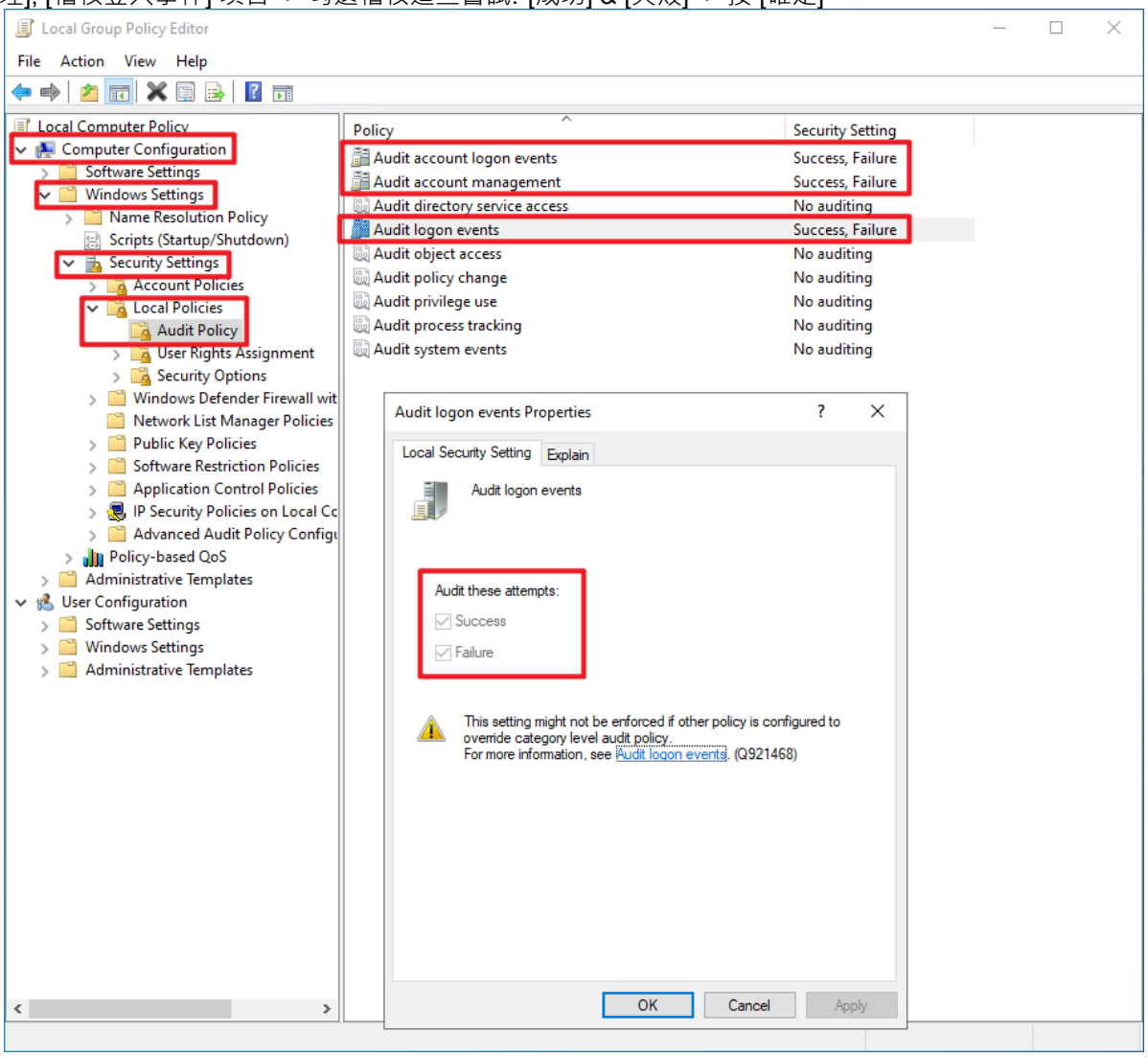
(1) 開啟 [本機群組原則編輯器]

點選 [搜尋] -> 輸入群組原則 -> 點選 [編輯群組原則]



(2) 本機原則：稽核原則

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



(3) 開啟 [Windows PowerShell]

(4) 更新群組原則

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

Administrator: Windows PowerShell

```
PS C:\> gpupdate /force

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

PS C:\>
```

(5) 查看群組原則套用情形

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

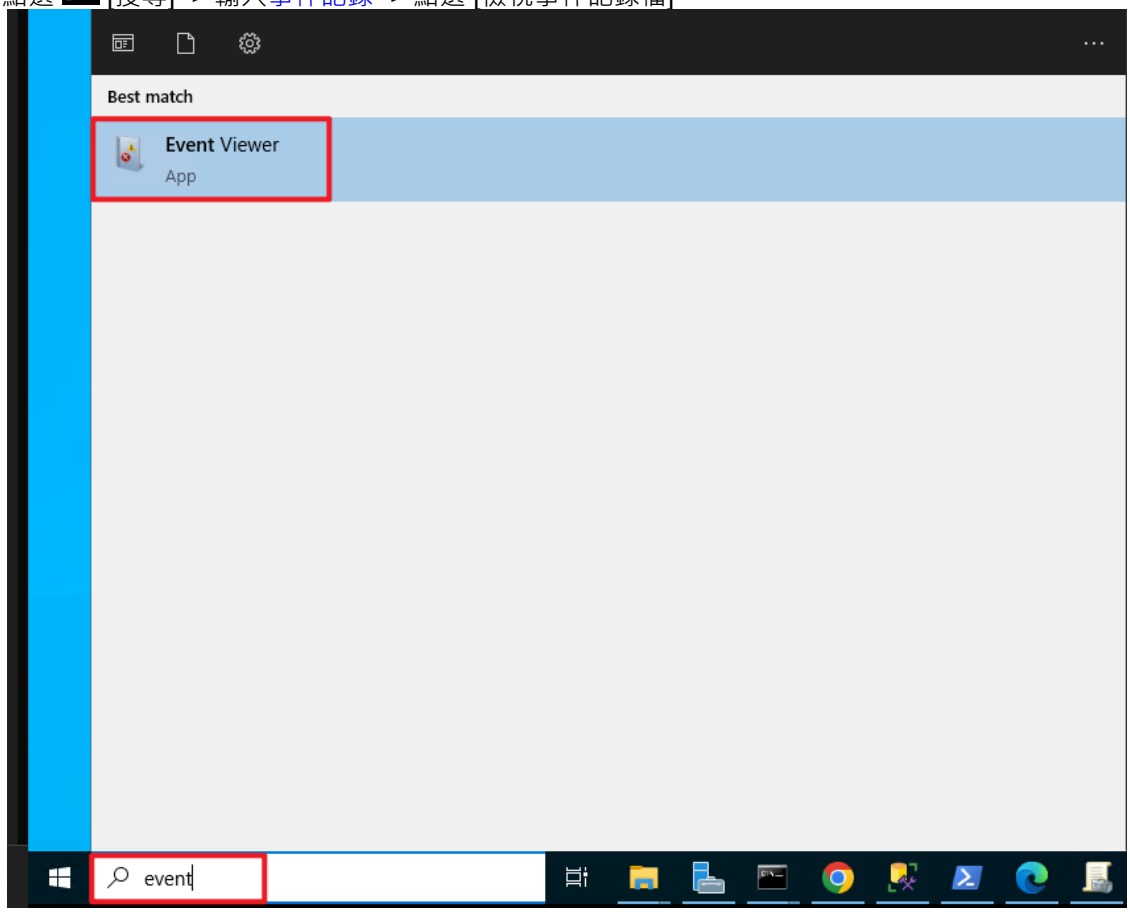
Administrator: Windows PowerShell

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

6.3.2.2 事件檔案設定

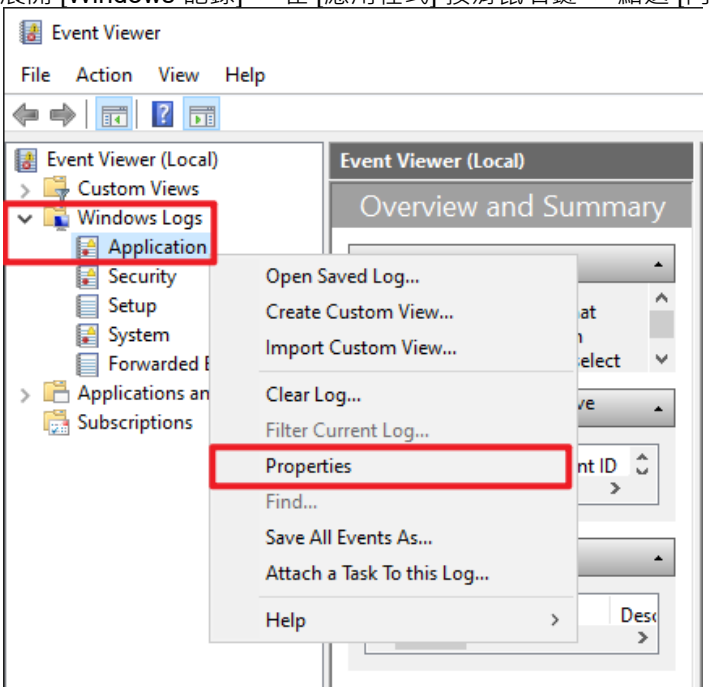
(1) 開啟 [檢視事件記錄檔]

點選 [搜尋] -> 輸入事件記錄 -> 點選 [檢視事件記錄檔]



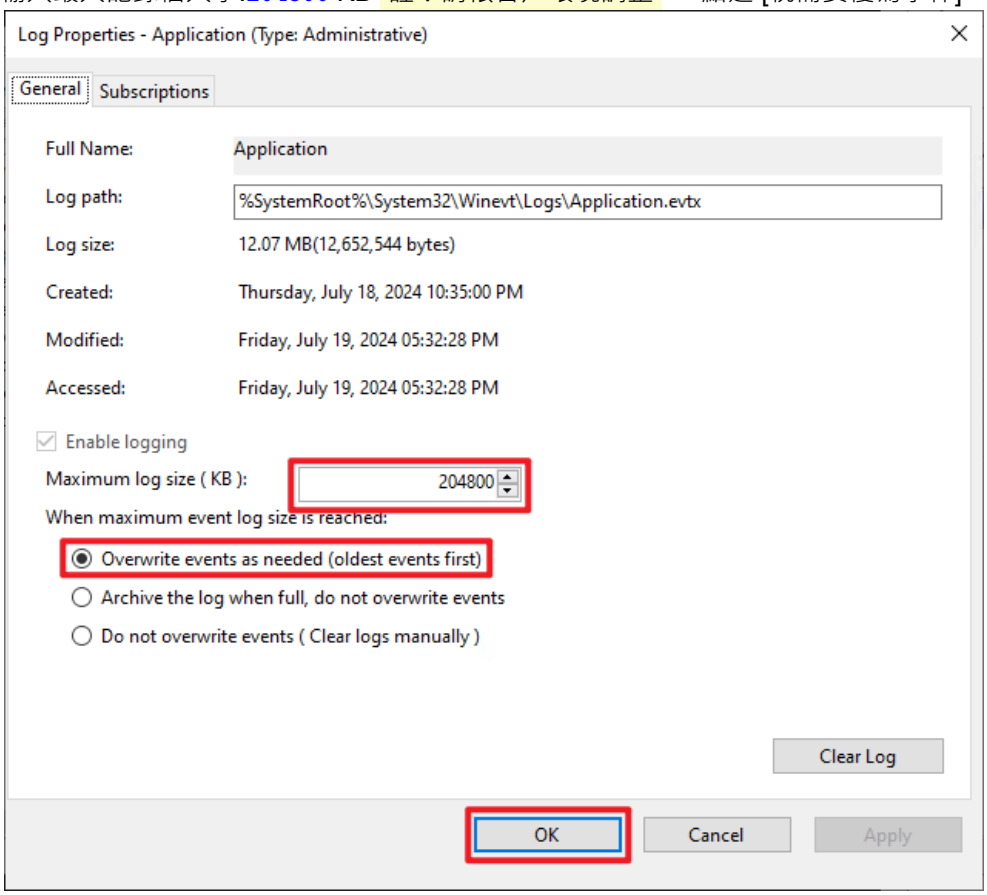
(2) 編輯安全性記錄

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



(3) 設定應用程式記錄檔

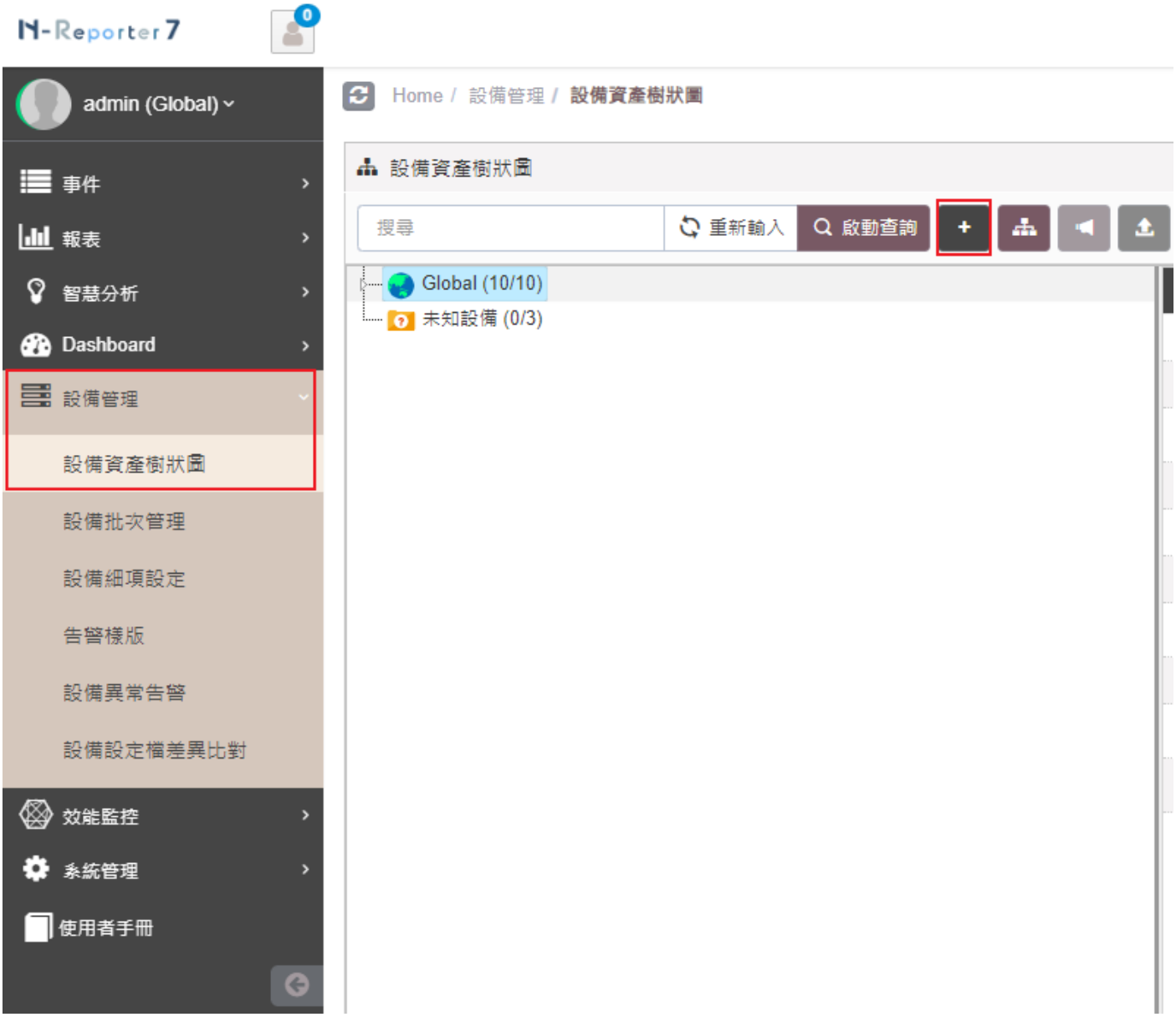
輸入最大記錄檔大小:204800 KB 註：請依客戶環境調整 -> 點選 [視需要覆寫事件] -> 按 [確定]



7 N-Reporter

(1) 新增 MS SQL 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

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

7.1 MS SQL Server Event Log

(1) 設備基本設定

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

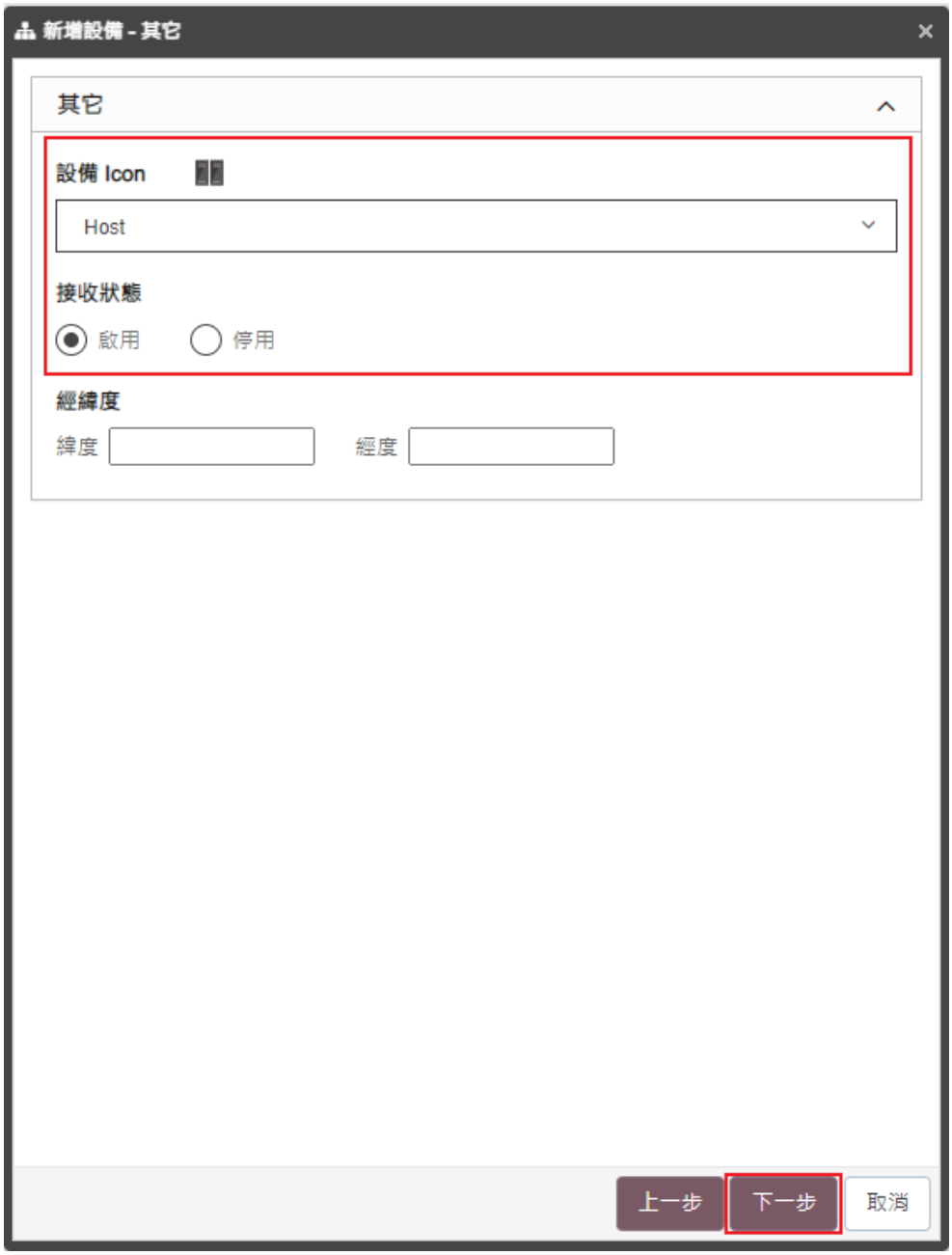
(2) Syslog 相關設定

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

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

(3) 其他

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



是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]

7.2 Windows Event Log

(1) 設備基本設定

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

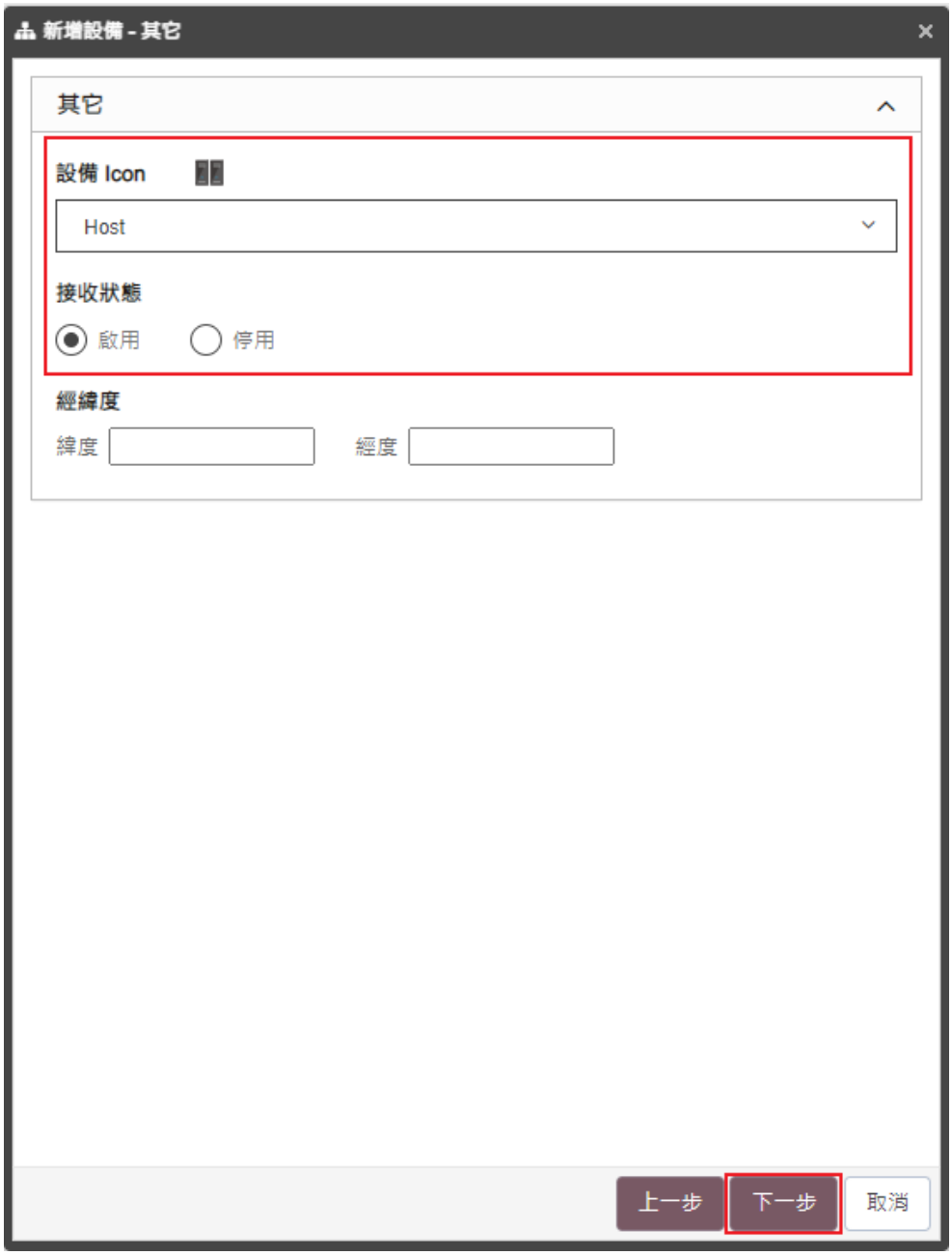
(2) Syslog 相關設定

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

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

(3) 其他

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

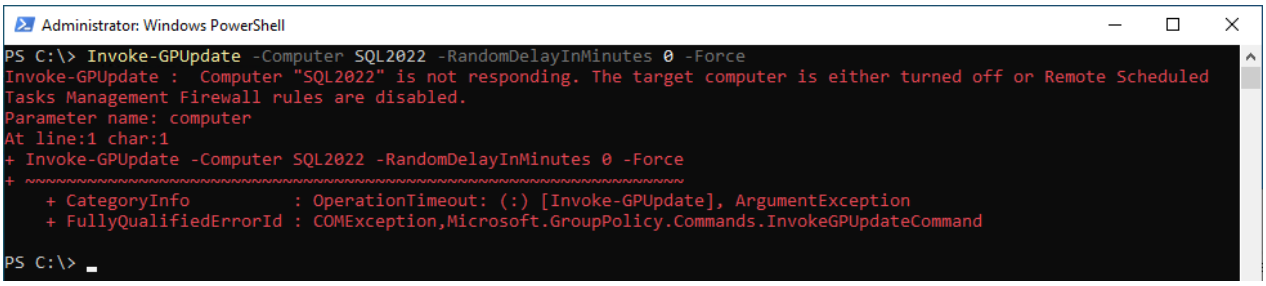


是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]

8 問題排除

8.1 Invoke-GPUpdate 錯誤

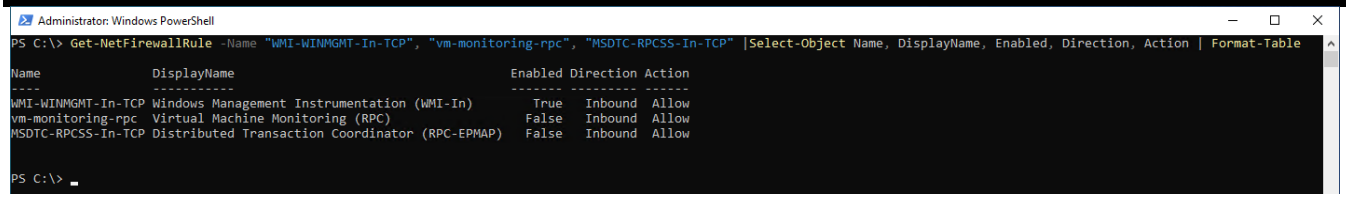
(1) 在 AD 網域伺服器 -> 執行 Invoke-GPUpdate 更新 Windows Server 群組原則出現錯誤訊息



(2) 在 Windows Server 開啟 [Windows PowerShell]

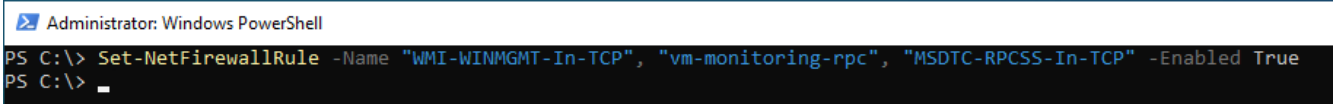
(3) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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



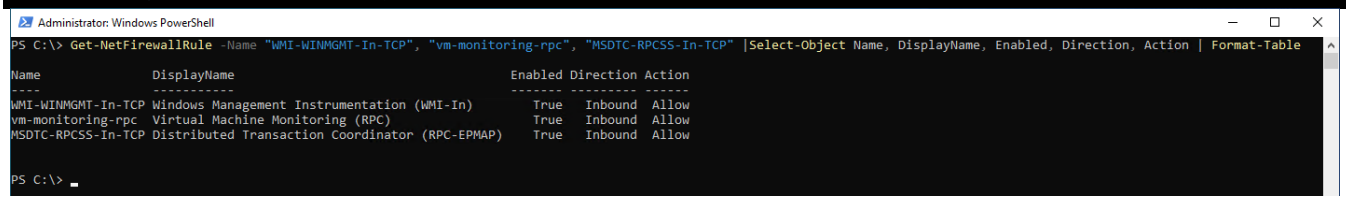
(4) 啟用 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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



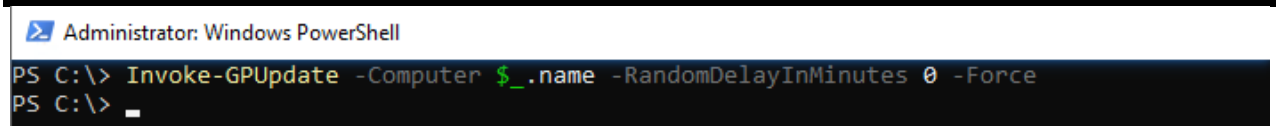
(5) 查看 Windows Firewall 的 WMI-WINMGMT-In-TCP、vm-monitoring-rpc、MSDTC-RPCSS-In-TCP 規則

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

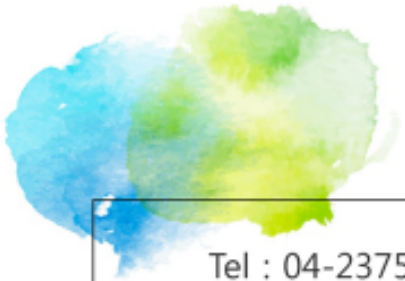


(6) 在 AD 網域伺服器 -> 更新 Windows Server 群組原則

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



紅色文字部位請輸入 Windows Server 伺服器名稱



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