



# N-Partner



如何設定 MS SQL Server 稽核事件記錄

V008

2019/04/25



## 版權聲明

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

## 商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

# 目錄

前言 .....	2	7.1 稽核登入.....	120
<b>1. NXLog.....</b>	<b>3</b>	7.1.1 使用指令介面方式設定.....	120
1.1 NXLog 架構 .....	3	7.1.2 使用圖形介面方式設定.....	123
1.2 NXLog 安裝 .....	4	7.2 稽核伺服器層級.....	128
1.3 NXLog 設定檔 .....	5	7.3 稽核資料庫層級.....	136
1.4 NXLog 啟動服務 .....	8	<b>8. N-Reporter.....</b>	<b>145</b>
<b>2. Windows.....</b>	<b>9</b>	8.1 MS SQL.....	145
2.1 群組原則.....	9	8.2 Windows.....	147
2.1.1 網域.....	9		
2.1.2 單機.....	17		
2.2 稽核資料庫檔案夾 .....	20		
<b>3. SQL 2008.....</b>	<b>24</b>		
3.1 稽核登入 .....	24		
3.1.1 使用指令介面方式設定.....	24		
3.1.2 使用圖形介面方式設定.....	27		
3.2 稽核伺服器層級 .....	32		
3.3 稽核資料庫層級 .....	40		
<b>4. SQL 2012.....</b>	<b>48</b>		
4.1 稽核登入 .....	48		
4.1.1 使用指令介面方式設定.....	48		
4.1.2 使用圖形介面方式設定.....	51		
4.2 稽核伺服器層級 .....	56		
4.3 稽核資料庫層級 .....	64		
<b>5. SQL 2014.....</b>	<b>72</b>		
5.1 稽核登入 .....	72		
5.1.1 使用指令介面方式設定.....	72		
5.1.2 使用圖形介面方式設定.....	75		
5.2 稽核伺服器層級 .....	80		
5.3 稽核資料庫層級 .....	87		
<b>6. SQL 2016.....</b>	<b>95</b>		
6.1 稽核登入 .....	95		
6.1.1 使用指令介面方式設定.....	95		
6.1.2 使用圖形介面方式設定.....	98		
6.2 稽核伺服器層級 .....	103		
6.3 稽核資料庫層級 .....	111		
<b>7. SQL 2019.....</b>	<b>120</b>		



## 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 Server 事件記錄。

NXLog 工具將 Windows 事件記錄轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。

此文件適用於 MS SQL Server 2008 / 2012 / 2014 / 2016 / 2019 版本。

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

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>

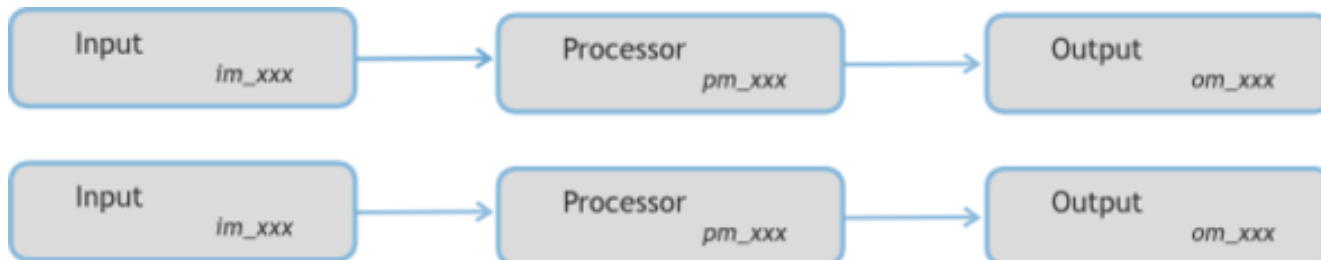
稽核動作群組：<https://docs.microsoft.com/zh-tw/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15>

# 1. NXLog

## 1.1 NXLog 架構

NXLog 的 plugin 架構允許任何類型的輸入讀取資料，解析和轉換訊息的格式，然後將其發送到任何類型的輸出。可以同時使用不同的輸入，處理和輸出模組來滿足事件記錄。

<https://nxlog.co/documentation/nxlog-user-guide#modules-im>

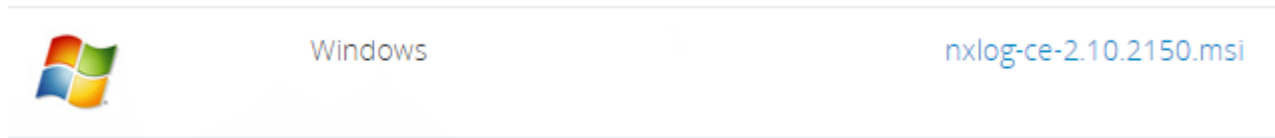


## 1.2 NXLog 安裝

### (1) 下載 NXLog

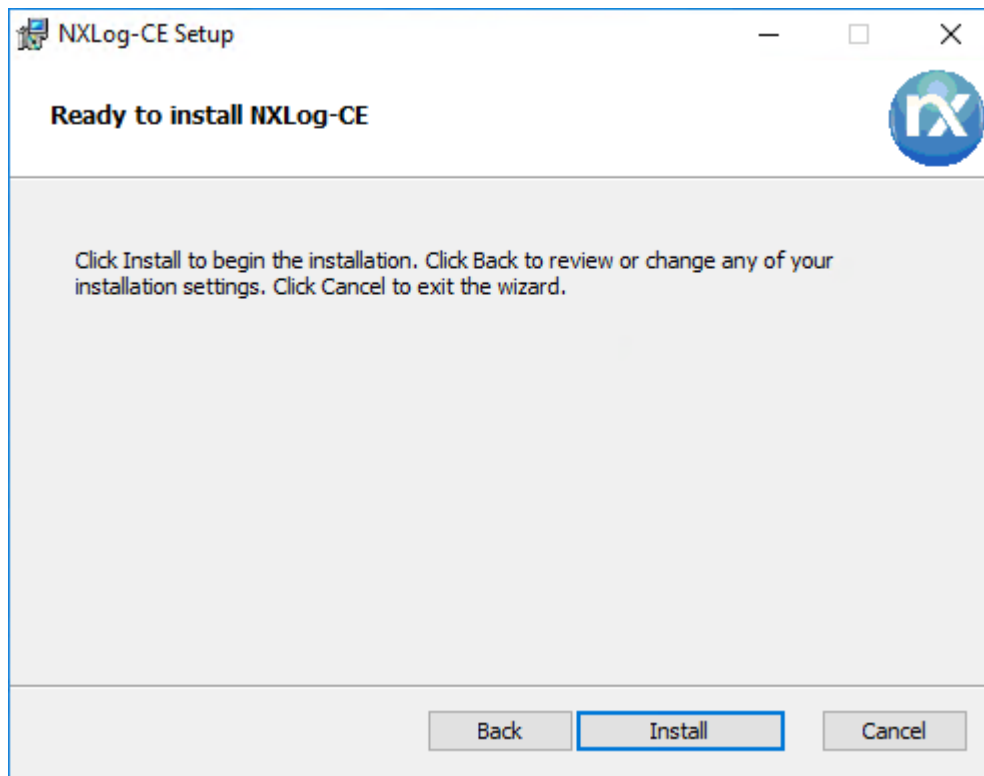
前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 **nxlog-ce-x.x.xxxx.msi** · 範例: **nxlog-ce-2.10.2150.msi**



### (2) 安裝 NXLog

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



### (3) 下載並覆蓋 NXLog 設定檔

下載連結 [http://www.npartnertech.com/download/tech/nxlog\\_SQLserver.conf](http://www.npartnertech.com/download/tech/nxlog_SQLserver.conf) ->

覆蓋 NXLog 設定檔 `Copy-Item nxlog_SQLserver.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'`



## 1.3 NXLog 設定檔

```
## 設定變數 ROOT 是 nxlog 安裝的資料夾

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

define NCloud    192.168.3.51

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

## 加載模組 xm_syslog

<Extension syslog>

  Module   xm_syslog

</Extension>

## Windows File 事件記錄

<Input in_eventlog>

  Module      im_msvistalog

  ReadFromLast TRUE

  SavePos     TRUE

  Query       <QueryList> \

              <Query Id="0"> \

                  <Select Path="Security">*[System[(EventID=4656)]]</Select> \

                  <Select Path="Security">*[System[(EventID=4658)]]</Select> \

                  <Select Path="Security">*[System[(EventID=4660)]]</Select> \
```



```
                <Select Path="Security">*[System[(EventID=4663)]]</Select> \
                <Select Path="Security">*[System[(EventID=4985)]]</Select> \
            </Query> \
        </QueryList>
        Exec $SyslogFacilityValue = 17;
    </Input>

## MS SQL Server 執行個體 (MSSQLSERVER) 事件記錄
<Input in_sqllog>
    Module        im_msvistalog
    ReadFromLast TRUE
    SavePos       TRUE
    Query         <QueryList> \
                    <Query Id="0"> \
                        <Select
Path="Application">*[System[Provider[@Name='MSSQLSERVER']]]</Select> \
                    </Query> \
                </QueryList>
    Exec $SyslogFacilityValue = 18;
</Input>

<Output out_eventlog>
    Module        om_udp
    Host          %NCloud%
    Port          514
    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, in_sqllog => out_eventlog
```

```
</Route>
```

紅色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud 192.168.3.51
```

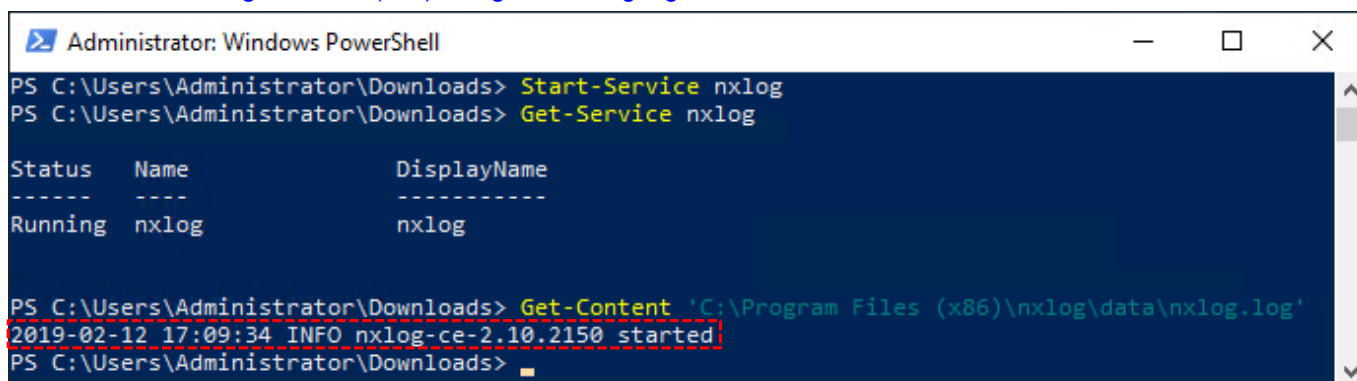
紅色文字部位請輸入 MS SQL Server 執行個體名稱

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

## 1.4 NXLog 啟動服務

開啟 PowerShell -> 輸入 `Start-Service nxlog` 啟動 nxlog 服務和 `Get-Service nxlog` 查看 nxlog 服務狀態 ->

`Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'` 確認沒有錯誤訊息



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads> Start-Service nxlog
PS C:\Users\Administrator\Downloads> Get-Service nxlog

Status      Name      DisplayName
-----
Running     nxlog     nxlog

PS C:\Users\Administrator\Downloads> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2019-02-12 17:09:34 INFO nxlog-ce-2.10.2150 started
PS C:\Users\Administrator\Downloads>
```

## 2. Windows

### 2.1 群組原則

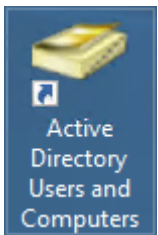
啟用稽核物件存取，指定 MS SQL Server 資料庫檔案夾存取控制清單(SACL)的事件。

以下分別為網域和單機設定方式。

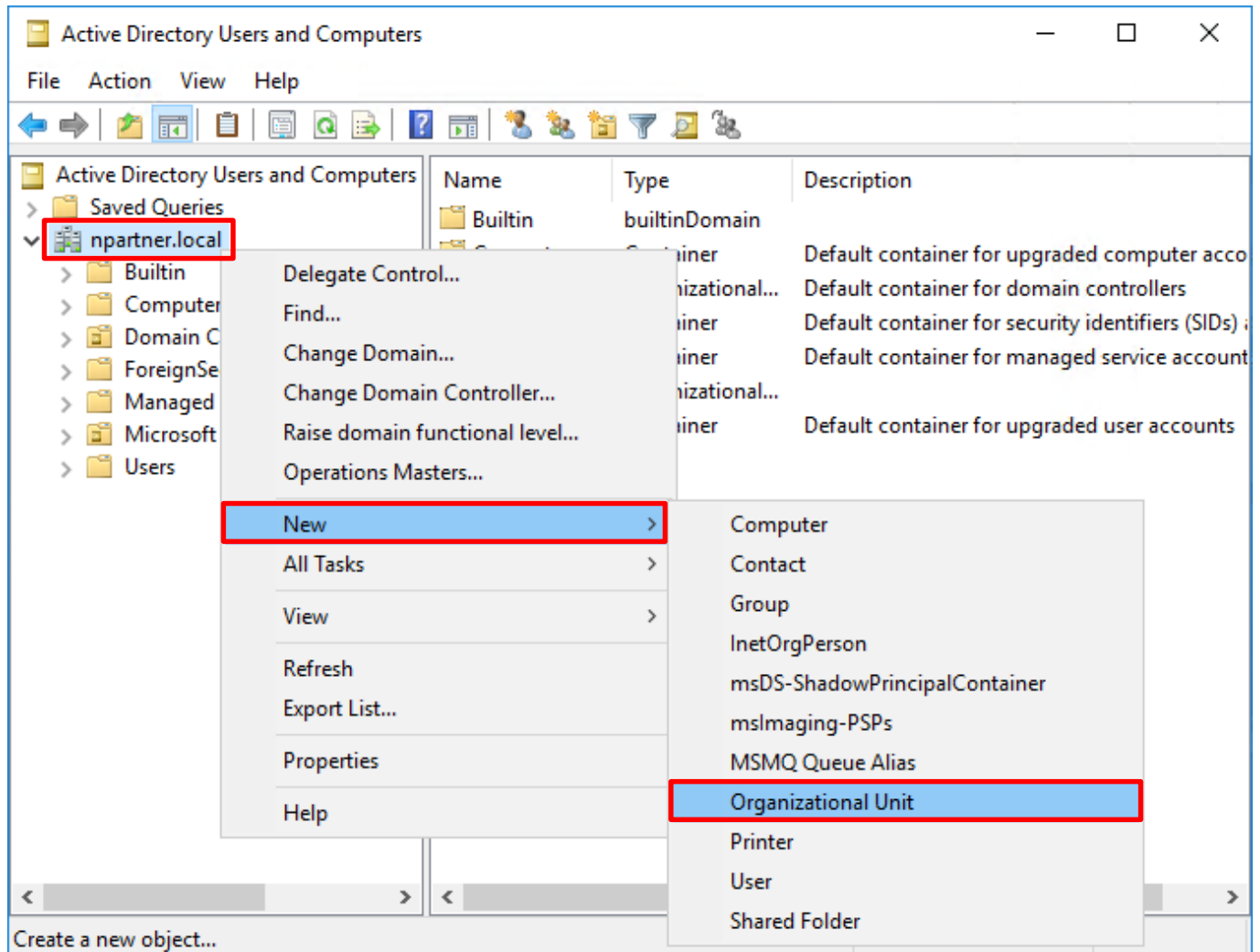
#### 2.1.1 網域

(1) 組織單位；建立新的組織單位，將 MS SQL 伺服器移到此組織單位，套用 N-Partner Policy 群組原則。

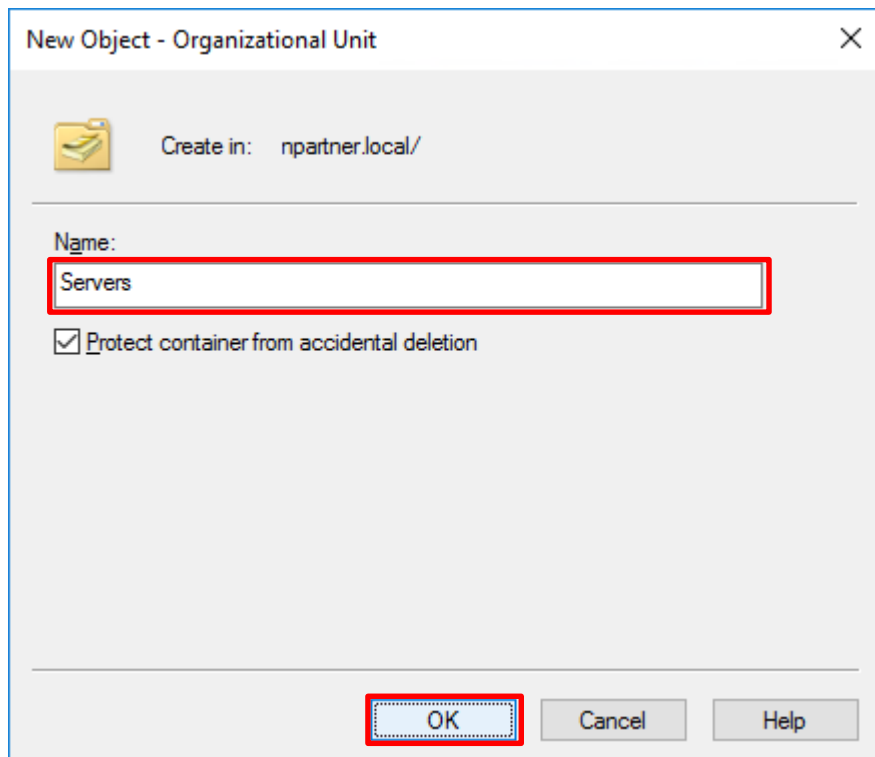
開啟 [Active Directory Users and Computers](#)



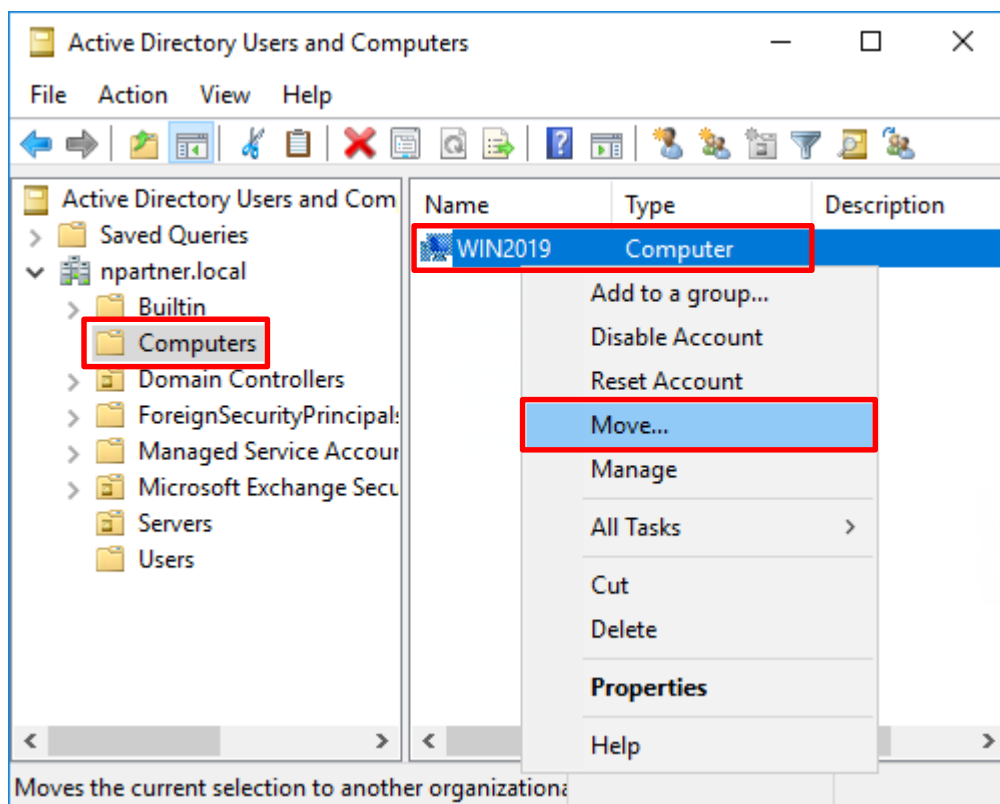
在 **Domain Name(網域名稱)** 按滑鼠右鍵 -> 選擇 **New(新增)** -> 點選 **Organizational Unit(組織單位)**



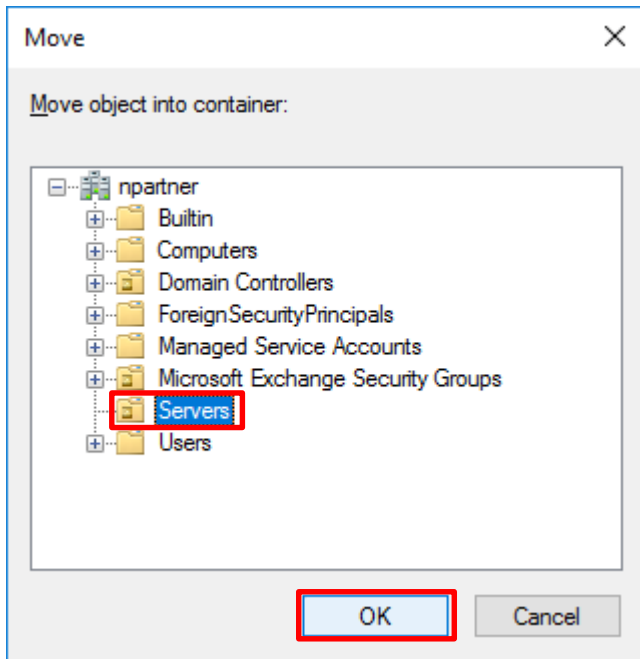
輸入 **Name(組織單位名稱): Servers** -> 按下 **OK(確定)**



選擇 **Computers** 組織單位 -> 在 **Server Name(MS SQL Server)** 上按滑鼠右鍵 -> 點選 **Move(移動)**



選擇 Servers 組織單位 -> 按下 OK(確定)

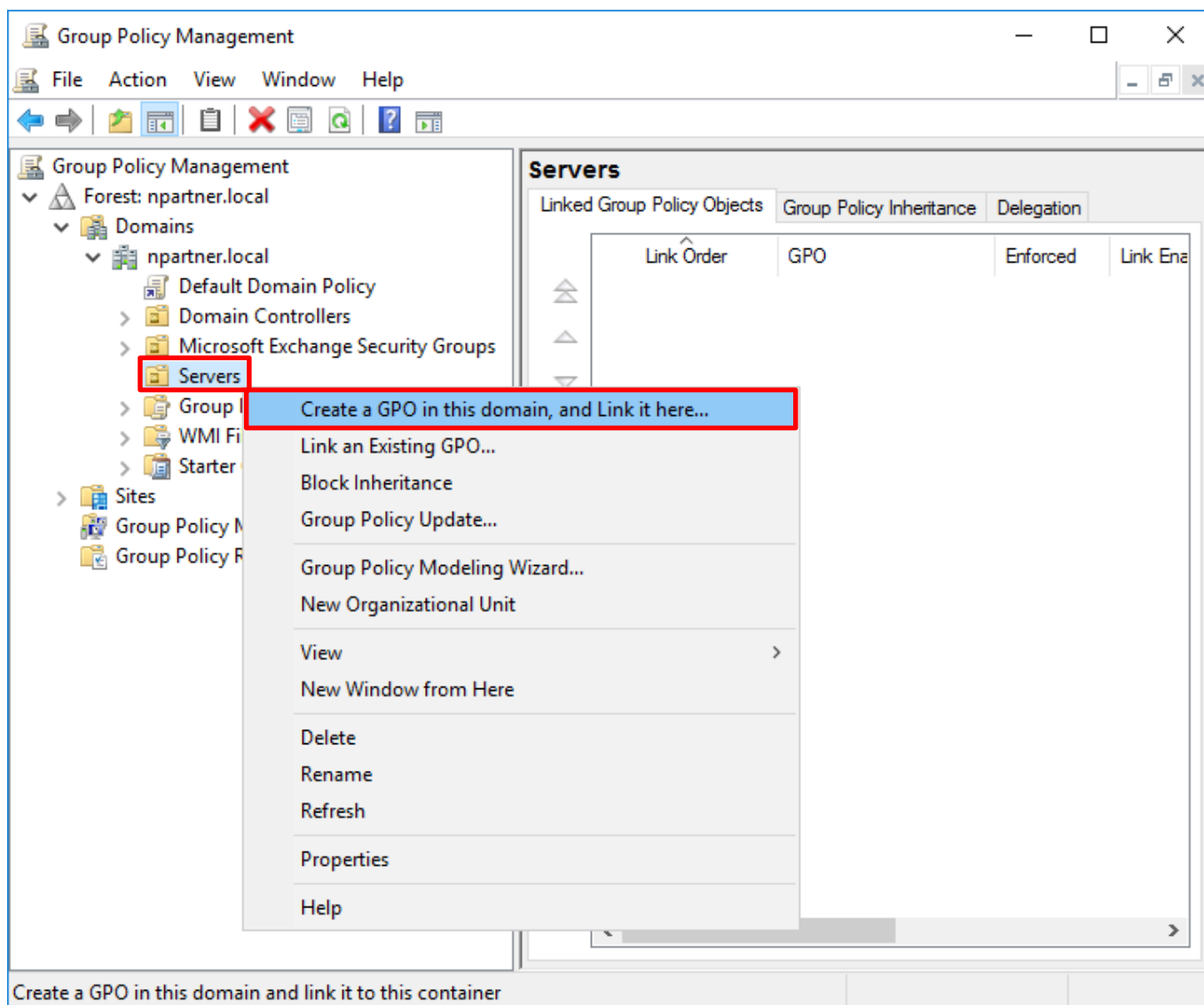


(2) 群組原則物件；在組織單位建立新的群組原則，啟用稽核物件存取成功和失敗，稽核 MS SQL 資料庫檔案夾。

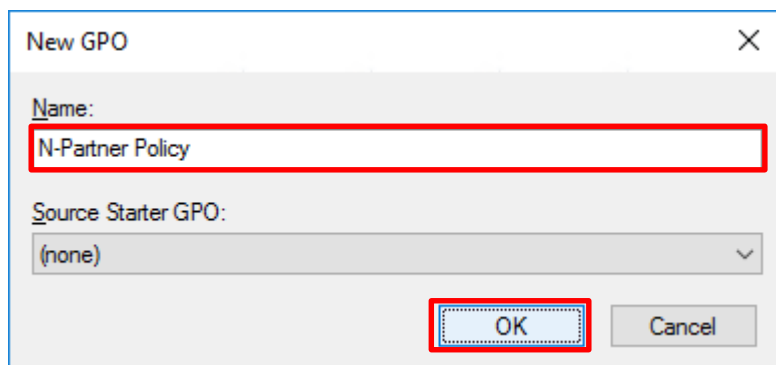
開啟 [Group Policy Management\(群組原則管理\)](#)



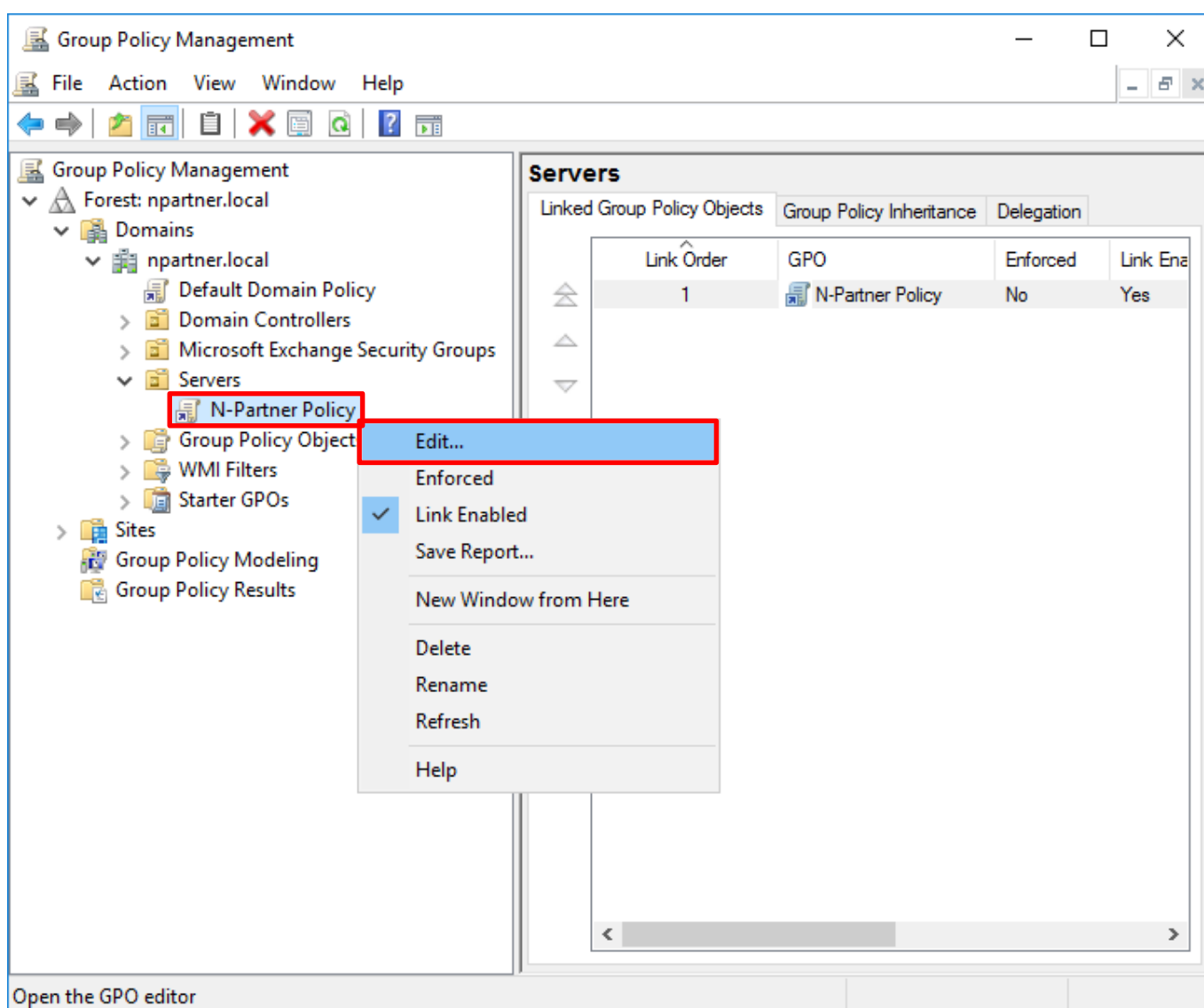
在 [Servers](#) 組織單位上按滑鼠右鍵 -> 點選 [Create a GPO in this domain, and Link it here\(在這個網域中建立 GPO 並連結到\)...](#)



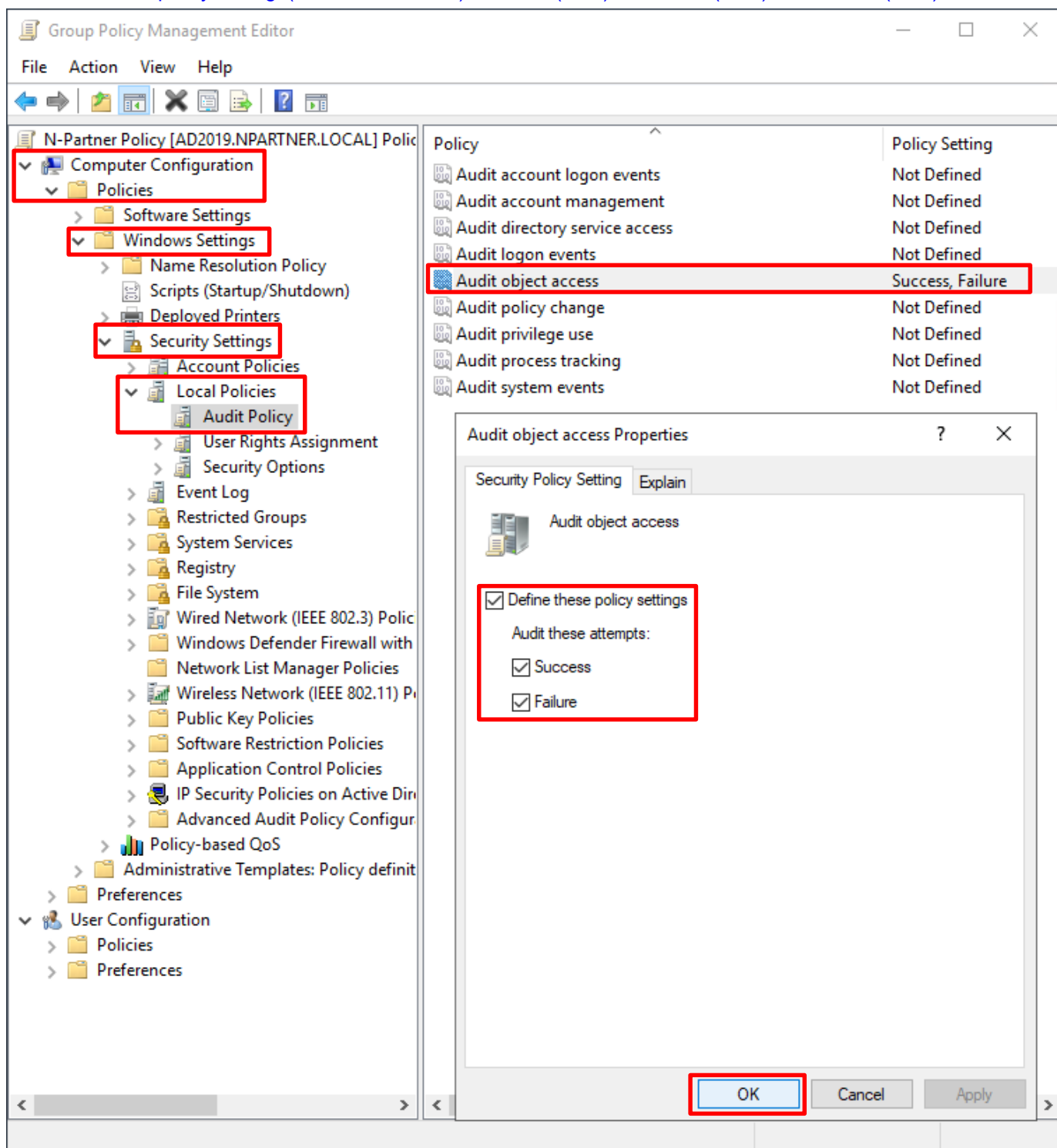
輸入 **Name(群組原則物件名稱): N-Partner Policy** -> 按下 **OK(確定)**



在 **N-Partner Policy** 群組原則物件上按滑鼠右鍵 -> 點選 **Edit(編輯)**



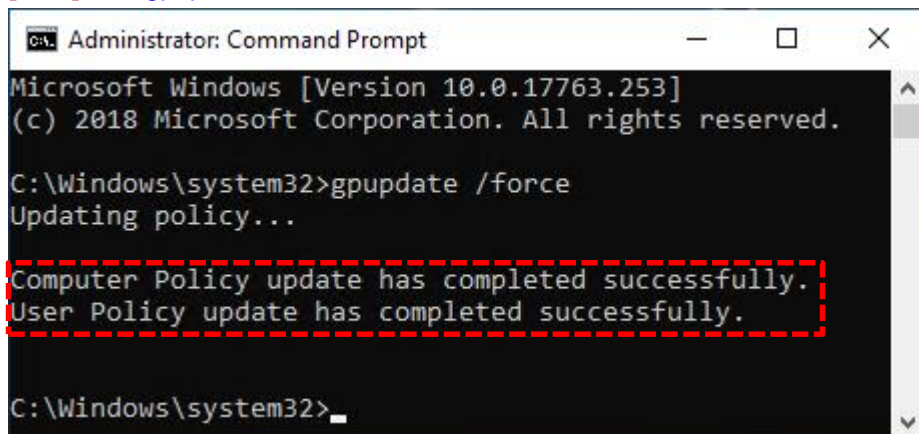
選擇 **Computer Configuration(電腦設定)** -> **Policies** -> **Windows Settings(Windows 設定)** -> **Security Settings(安全性設定)** -> **Local Policies(本機原則)** -> **Audit Policy(稽核原則)** -> 點選 **Audit object access(稽核物件存取)** 項目, 勾選 **Define these policy settings(定義這個原則設定): Success(成功)** 和 **Failure(失敗)** -> 按下 **OK(確定)**





在 MS SQL 伺服器更新群組原則

[SQL] C:\> gpupdate /force



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

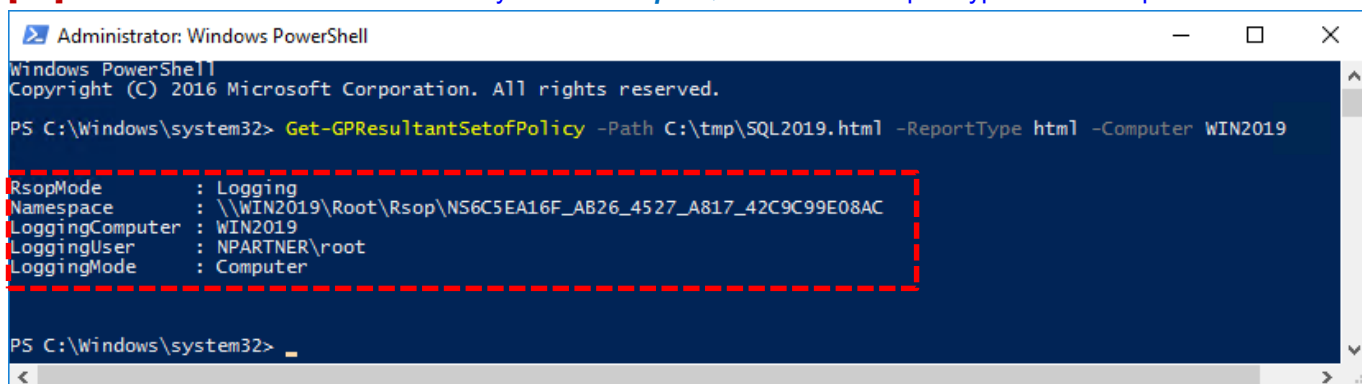
C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Windows\system32>
```

在 AD 網域伺服器，產生 MS SQL 伺服器群組原則報表

[AD] PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\SQL2019.html -ReportType html -Computer WIN2019



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-GPResultantSetofPolicy -Path C:\tmp\SQL2019.html -ReportType html -Computer WIN2019

RsopMode       : Logging
Namespace      : \\WIN2019\Root\Rsop\NS6C5E416F_AB26_4527_A817_42C9C99E08AC
LoggingComputer : WIN2019
LoggingUser    : NPARTNER\root
LoggingMode    : Computer

PS C:\Windows\system32>
```

開啟 [C:\tmp\SQL2019.html](file:///C:/tmp/SQL2019.html) 報表，確認 [Audit object access\(稽核物件存取\)](#) 套用 [N-Partner Policy](#) 群組原則。

**Group Policy Results**

**NPARTNER\WIN2019**  
Data collected on: 2/13/2019 3:35:18 PM [show all](#)

**Summary** [show](#)

**Computer Details** [hide](#)

**General** [show](#)

**Component Status** [show](#)

**Settings** [hide](#)

**Policies** [hide](#)

**Windows Settings** [hide](#)

**Security Settings** [hide](#)

Policy	Setting	Winning GPO
Audit object access	Success, Failure	N-Partner Policy

**Local Policies/Security Options** [show](#)

**Public Key Policies/Certificate Services Client - Auto-Enrollment Settings** [show](#)

**Public Key Policies/Encrypting File System** [show](#)

**Advanced Audit Configuration** [show](#)

**Group Policy Objects** [show](#)

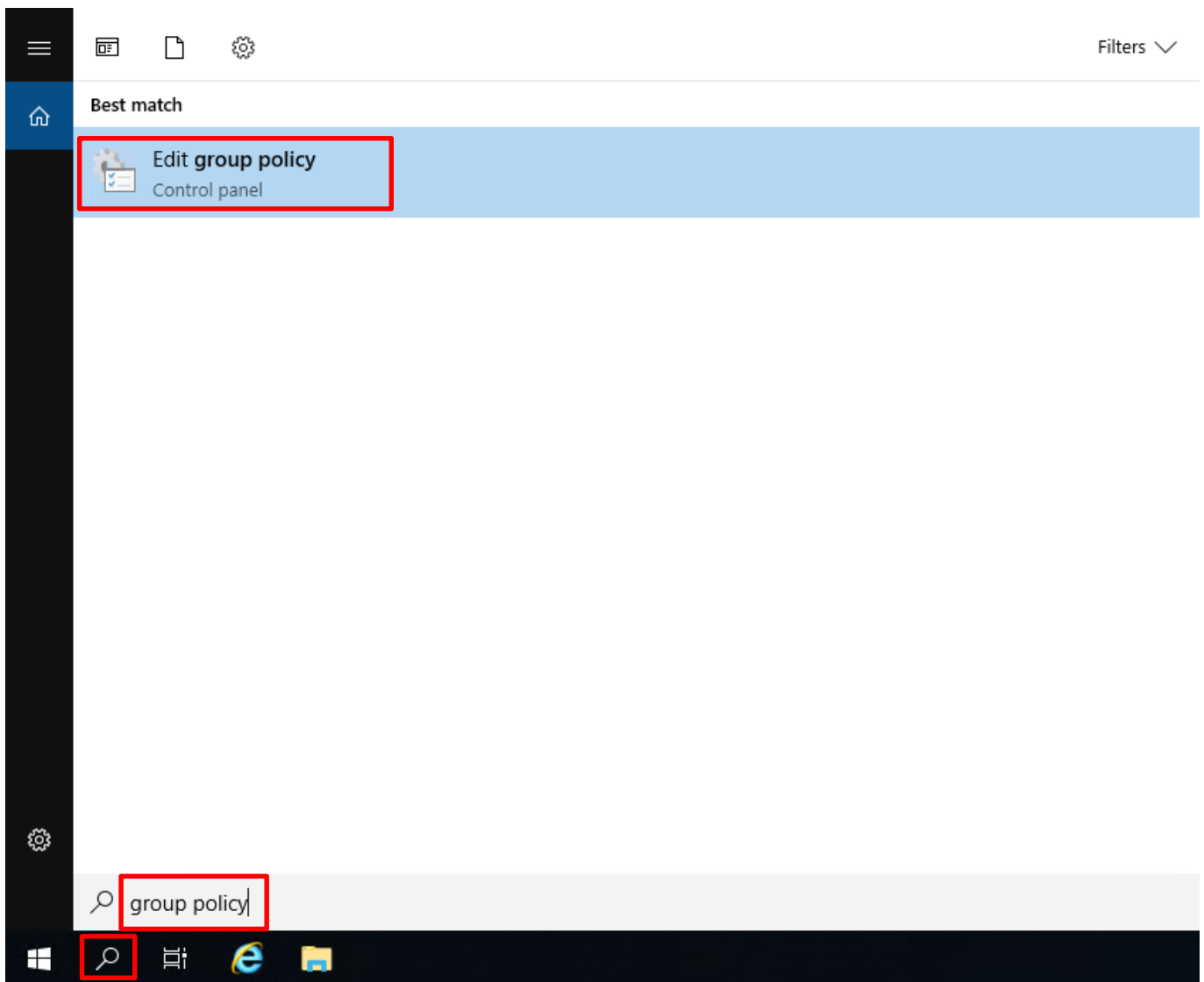
**WMI Filters** [show](#)

**User Details**

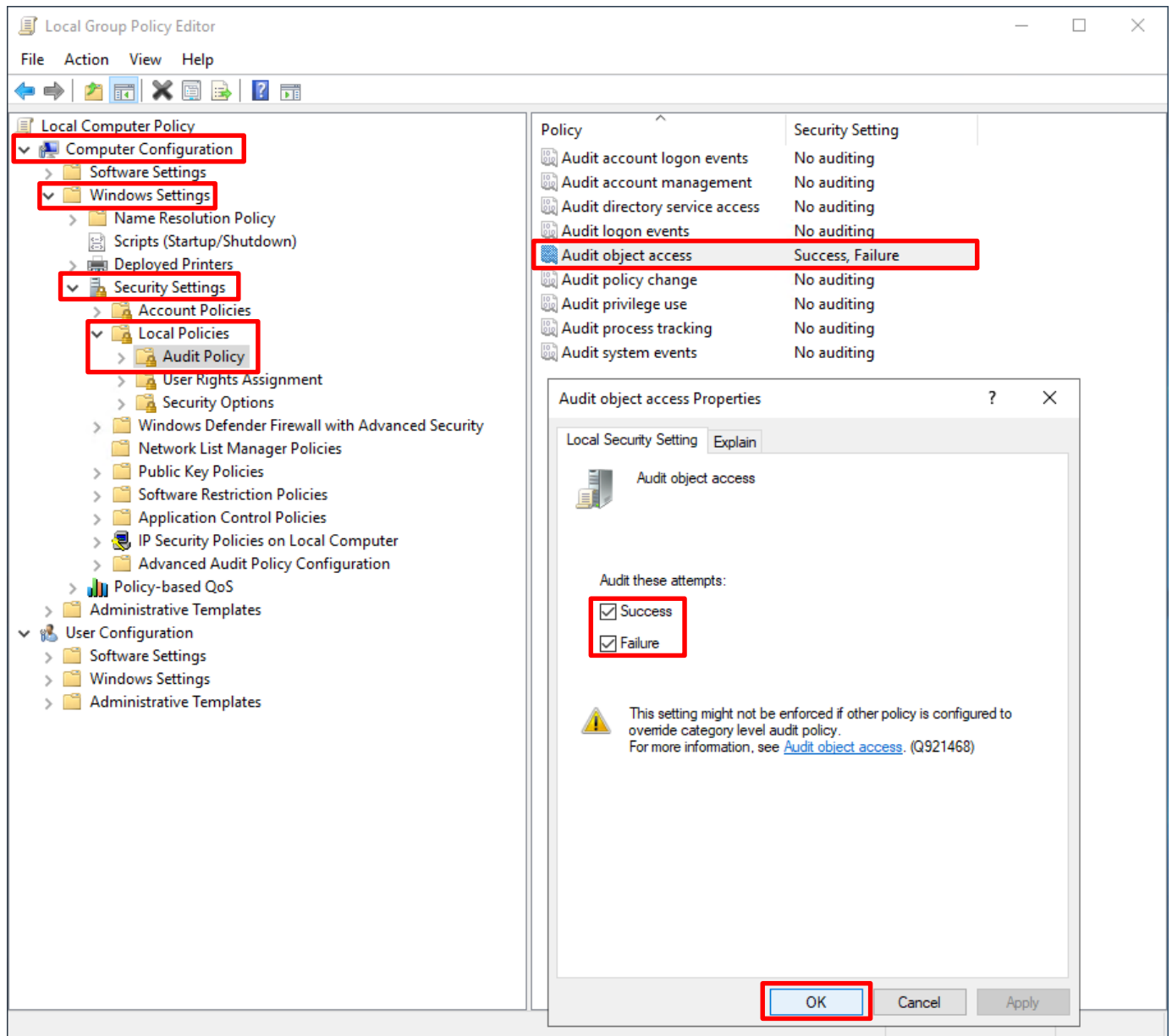
## 2.1.2 單機

編輯群組原則 · 啟用稽核物件存取成功和失敗。

點選 [Search](#) -> 輸入 [group policy](#) -> 點選 [Edit group policy](#)

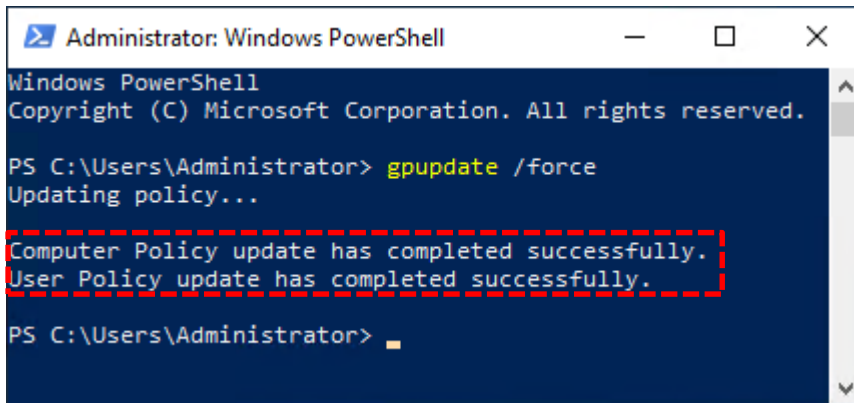


選擇 **Computer Configuration(電腦設定)** -> **Windows Settings(Windows 設定)** -> **Security Settings(安全性設定)** -> **Local Policies(本機原則)** -> **Audit Policy(稽核原則)** -> 點選 **Audit object access(稽核物件存取)** 項目 -> 勾選 **Audit these attempts: Success(成功) & Failure(失敗)** -> 按下 **OK(確定)**



## MS SQL 伺服器更新群組原則

C:\> gpupdate /force



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

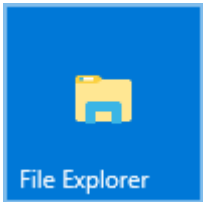
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

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

## 2.2 稽核資料庫檔案夾

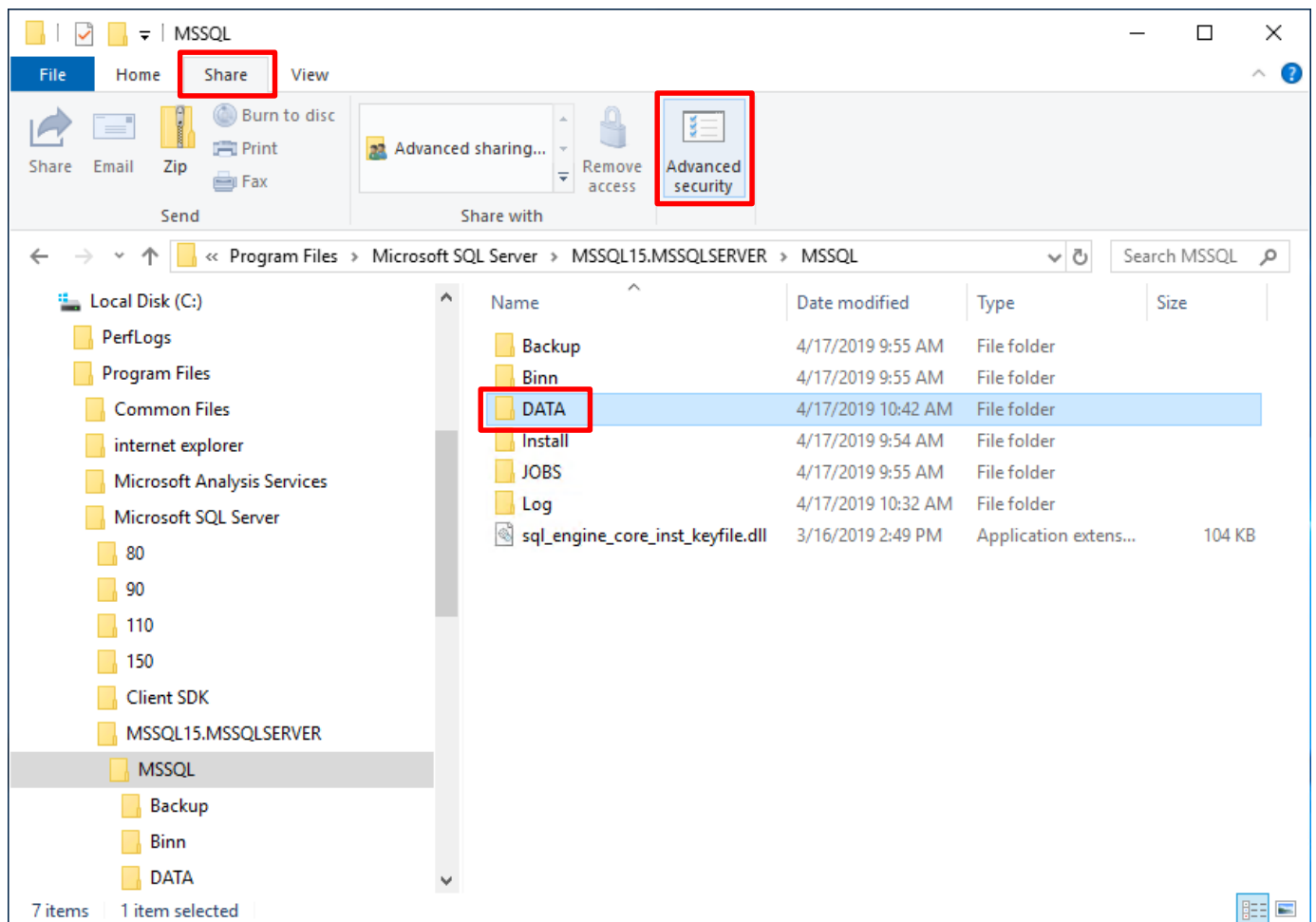
稽核 MS SQL Server 資料庫檔案夾記錄檔案動作。

開啟 File Explorer(檔案總管)

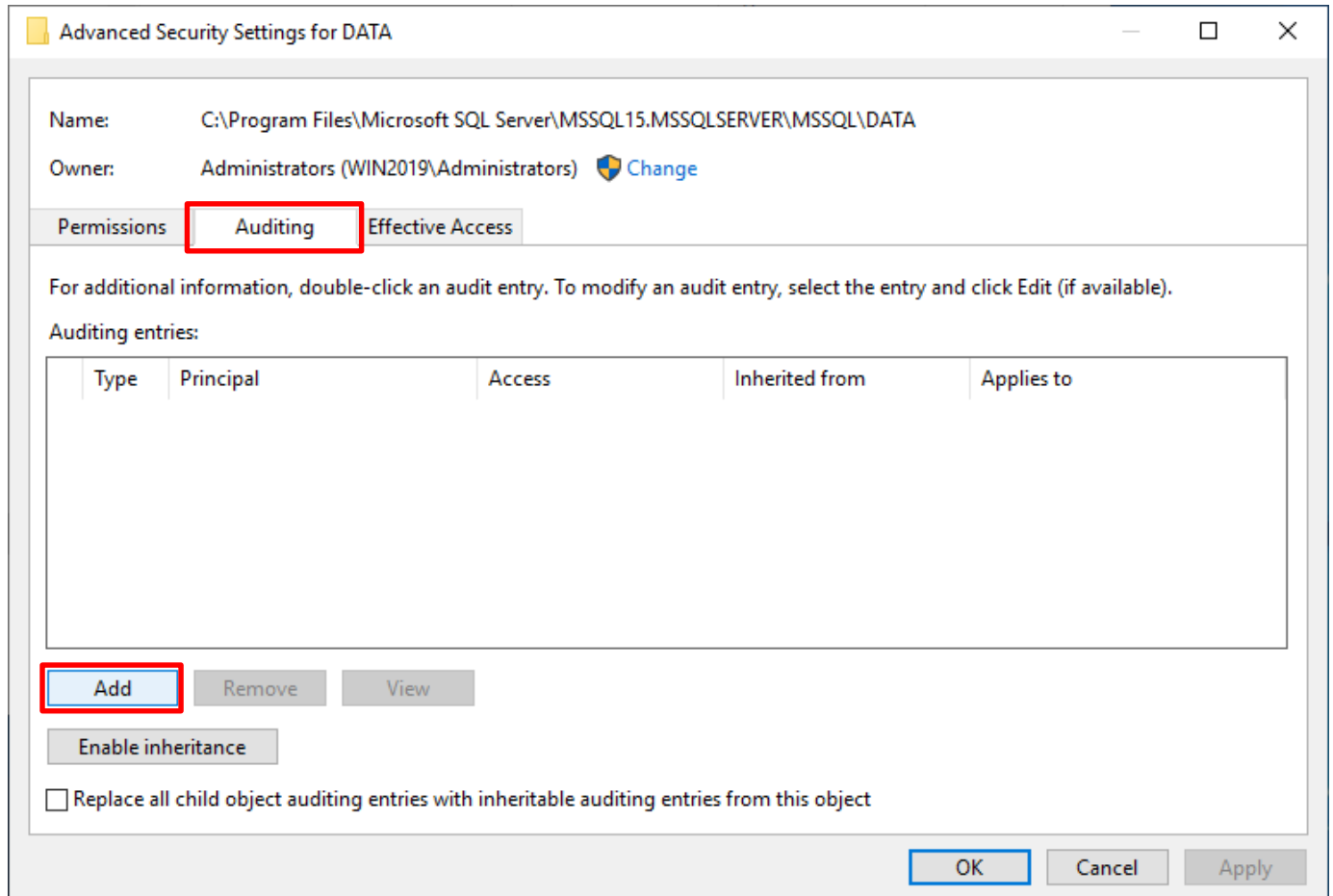


選擇 MS SQL 資料庫資料夾 (範例: C:\Program Files\Microsoft SQL

Server\MSSQL15.MSSQLSERVER\MSSQL\DATA) -> 點選 Share(共用) 頁面 -> 按下 Advanced security(進階安全性)



點選 Auditing(稽核) 頁面 -> 按下 Add(新增)

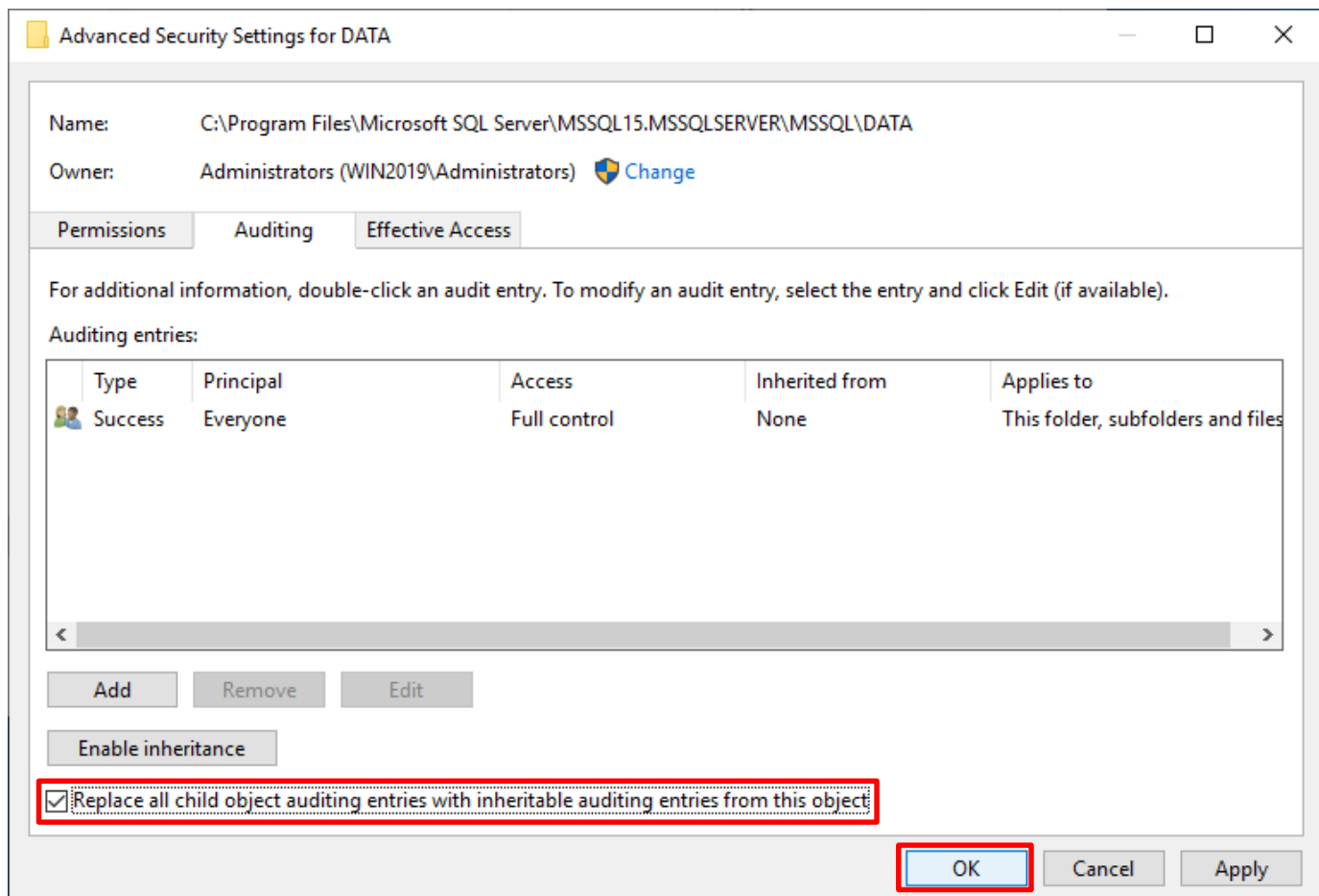


選擇 **Principal(主體): Everyone** -> **Type(類型): All(全部)** -> **Applies to(套用到): This folder, subfolders and files(這個資料夾、子資料夾及檔案)** -> 勾選 **Basic permissions(基本權限): Full control(完全控制), Modify(修改), Read & execute(讀取和執行), List folder contents(列出資料夾內容), Read(讀取), Write(寫入)** -> 按下 **OK(確定)**

The screenshot shows the 'Auditing Entry for DATA' dialog box. The 'Principal' is set to 'Everyone' with a 'Select a principal' link. The 'Type' is set to 'All' and 'Applies to' is set to 'This folder, subfolders and files'. Under 'Basic permissions', the following are checked: Full control, Modify, Read & execute, List folder contents, Read, and Write. 'Special permissions' is unchecked. There is a 'Show advanced permissions' link and a 'Clear all' button. At the bottom, the 'OK' button is highlighted with a red box, and the 'Cancel' button is also visible.



勾選 **Replace all child object auditing entries with inheritable auditing entries from this object**(以此物件中的可繼承稽核項目取代所有子物件稽核項目) -> 按下 **OK**(確定)



## 3. SQL 2008

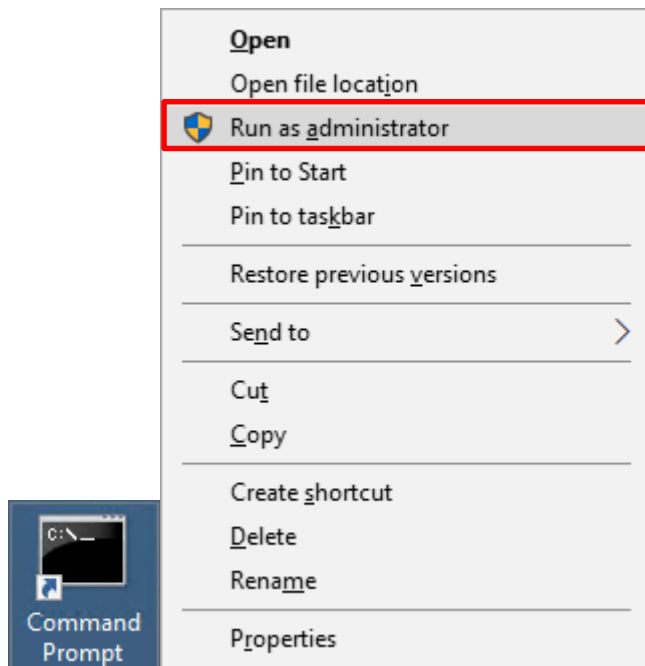
### 3.1 稽核登入

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，才會生效。

以下分別為指令介面和圖形介面設定方式。

#### 3.1.1 使用指令介面方式設定

在 **Command Prompt(命令提示字元)** 上按滑鼠右鍵 -> 點選 **Run as administrator(以系統管理員身分執行)**



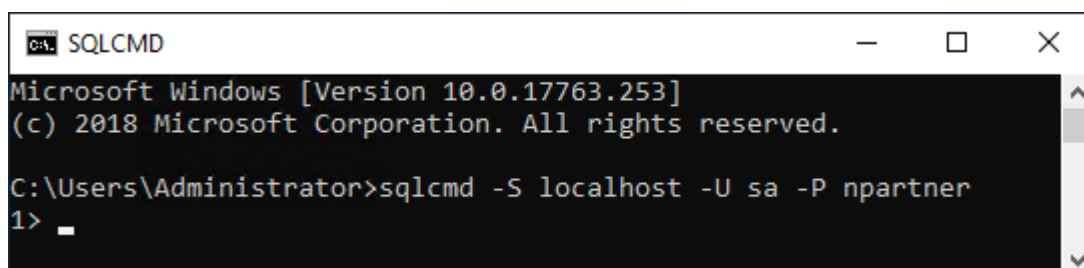
輸入 `sqlcmd -S localhost -U sa -P npartner`

#### Options:

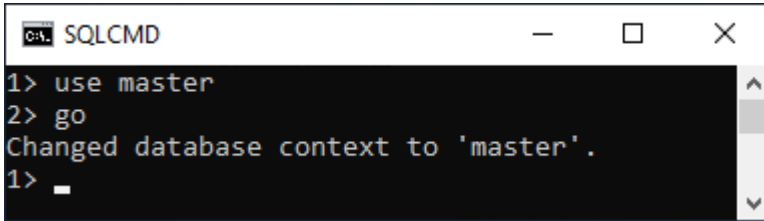
**-S** [protocol:]server[instance\_name][,port]

**-U** login\_id

**-P** password



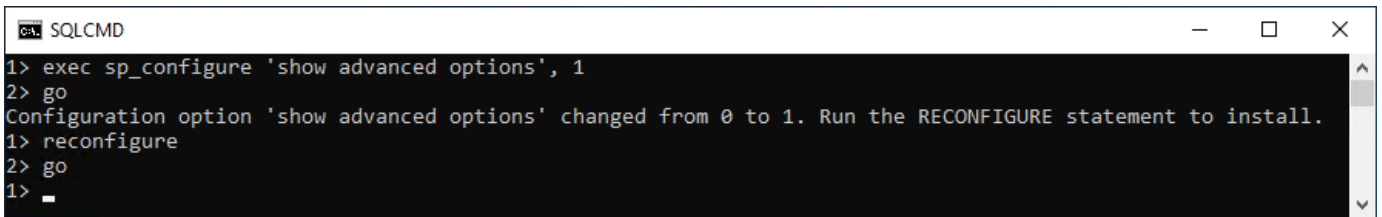
輸入 `use master -> go`



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

使用 `sp_configure` 列出進階選項

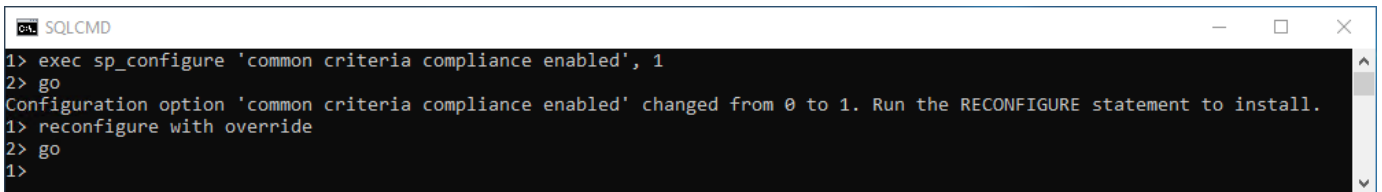
輸入 `exec sp_configure 'show advanced options', 1 -> go -> reconfigure -> go`



```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

啟用通用條件合規性

輸入 `exec sp_configure 'common criteria compliance enabled', 1 -> go -> reconfigure with override -> go`

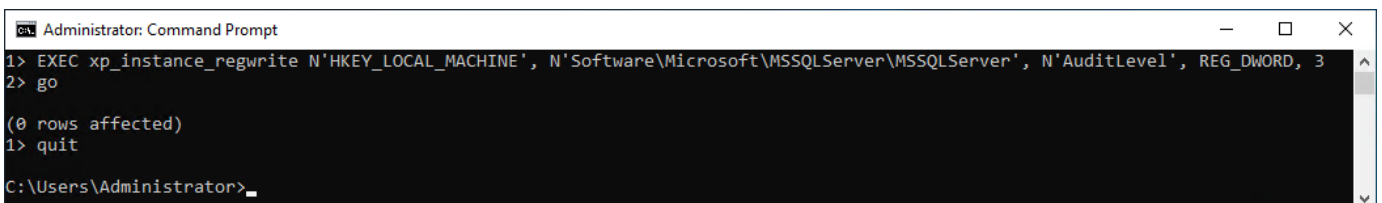


```
SQLCMD
1> exec sp_configure 'common criteria compliance enabled', 1
2> go
Configuration option 'common criteria compliance enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure with override
2> go
1> _
```

啟用失敗和成功的登入記錄

輸入 `EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',`

`N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 -> go -> quit`



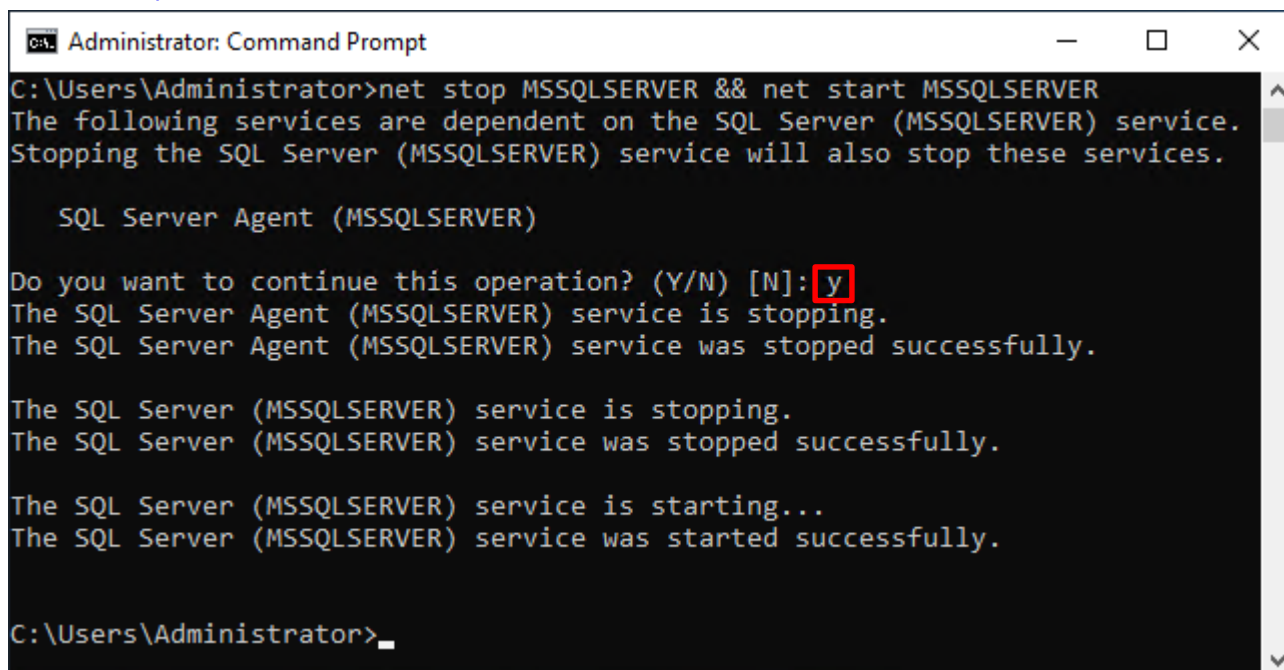
```
Administrator: Command Prompt
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit

C:\Users\Administrator>_
```

重新啟動 MSSQLSERVER 服務

輸入 `net stop MSSQLSERVER && net start MSSQLSERVER`



```
Administrator: Command Prompt
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSERVER
The following services are dependent on the SQL Server (MSSQLSERVER) service.
Stopping the SQL Server (MSSQLSERVER) service will also stop these services.

    SQL Server Agent (MSSQLSERVER)

Do you want to continue this operation? (Y/N) [N]: y
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

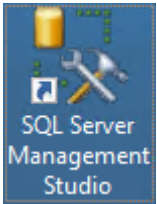
The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is starting...
The SQL Server (MSSQLSERVER) service was started successfully.

C:\Users\Administrator>
```

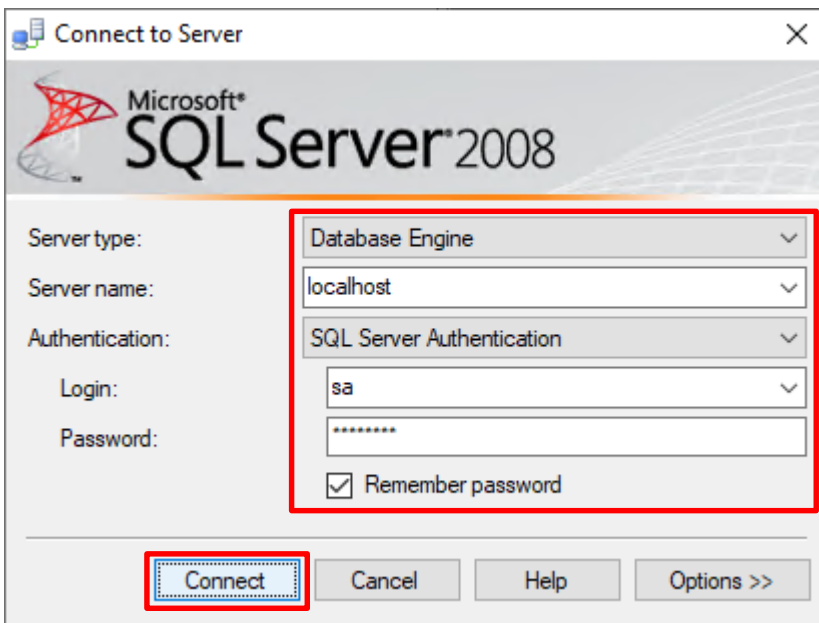
### 3.1.2 使用圖形介面方式設定

開啟 [Microsoft SQL Server Management Studio](#)

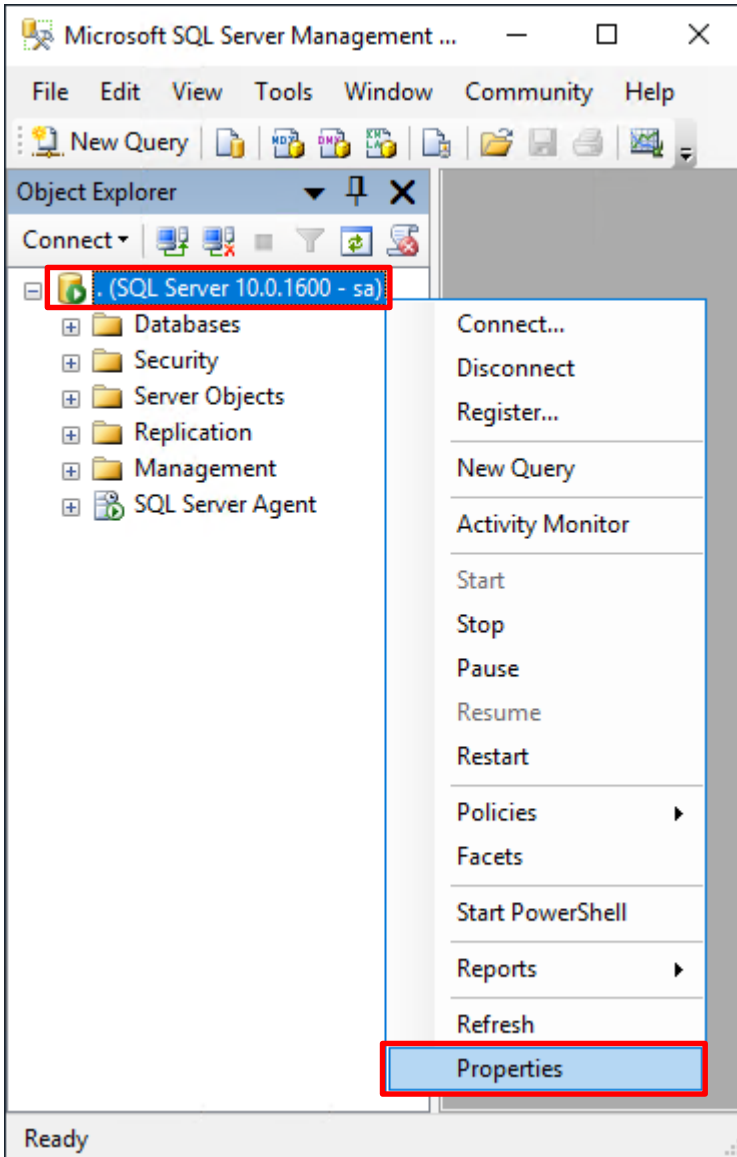


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

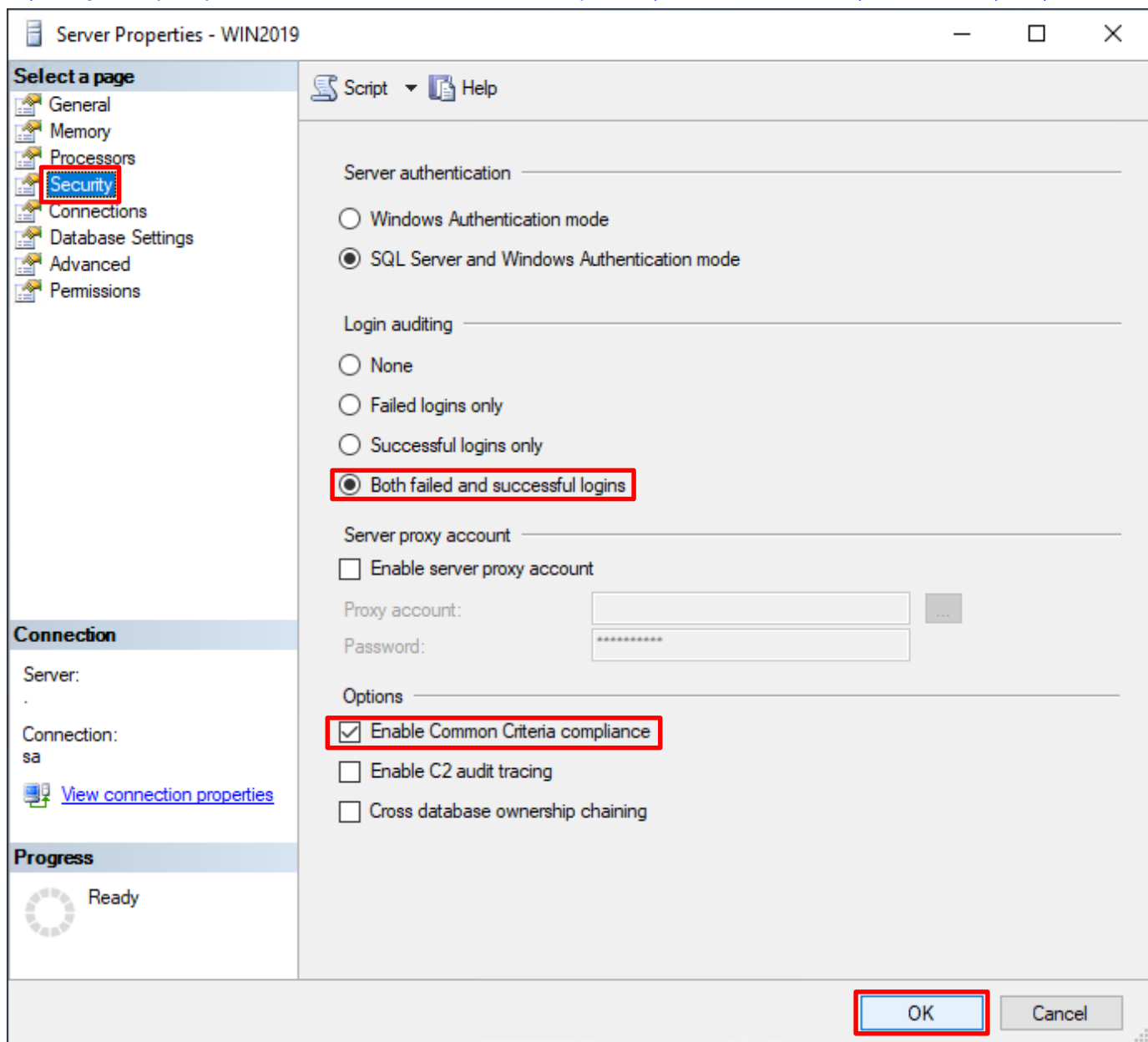
**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



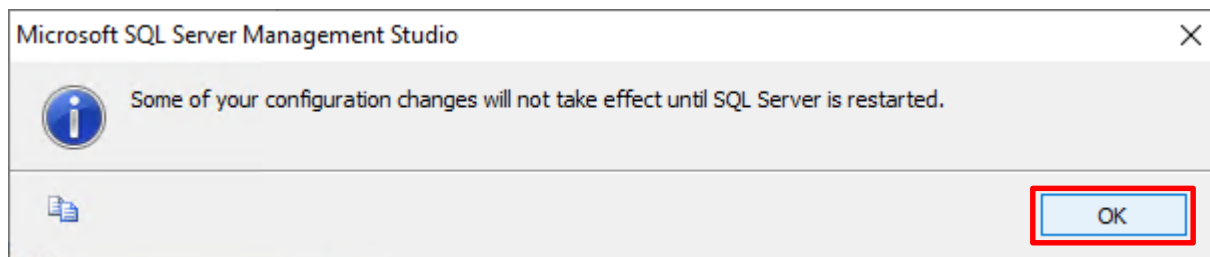
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Properties(屬性)**



選擇 **Security(安全性)** 頁面 -> **Login auditing(登入稽核)**: 點選 **Both failed and successful logins(失敗和成功的登入)** -> **Options(選項)**: 勾選 **Enable Common Criteria compliance(啟用通用條件合規性)** -> 按下 **OK(確定)**

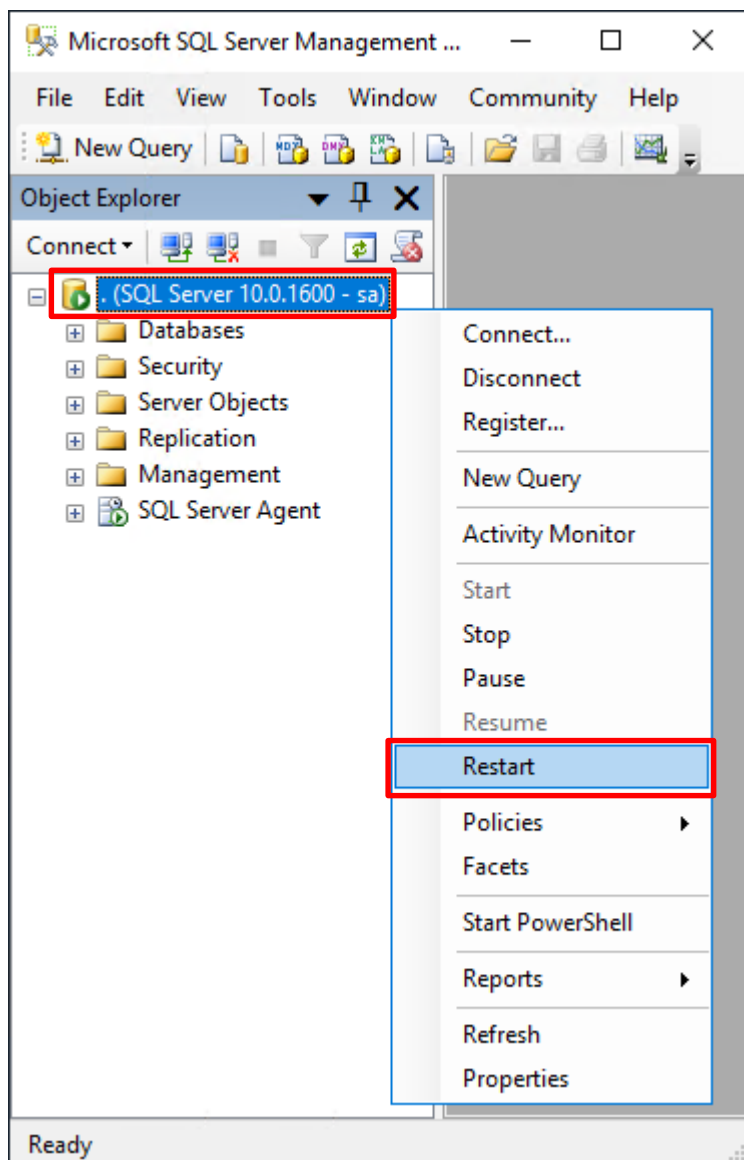


按下 **OK(確定)**

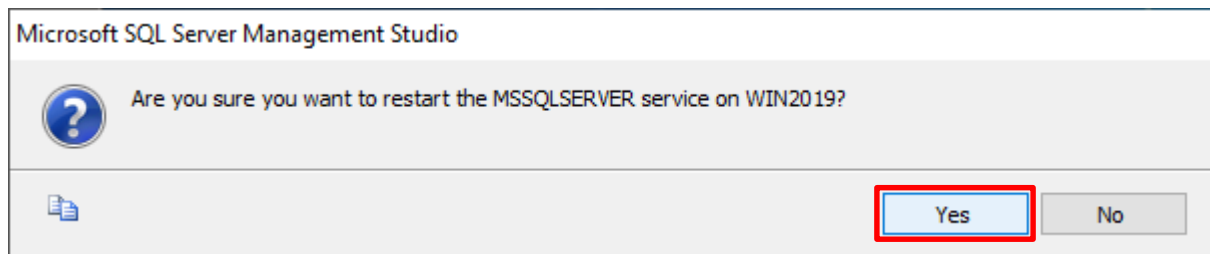


重新啟動 MSSQLSERVER 服務

在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Restart(重新啟動)**

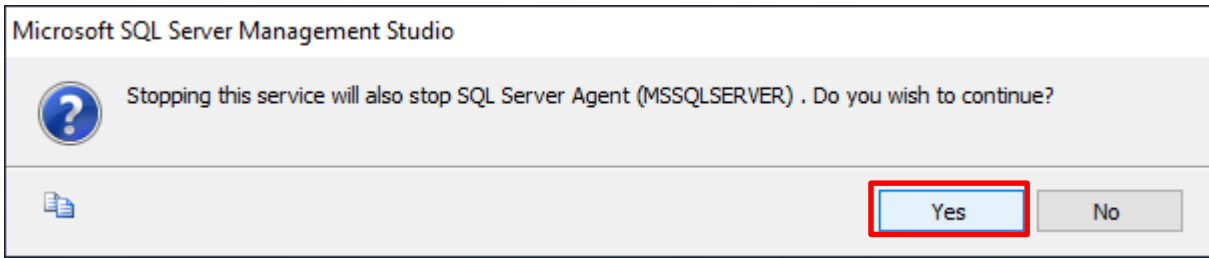


按下 **Yes(是)** 重新啟動 MSSQLSERVER 服務





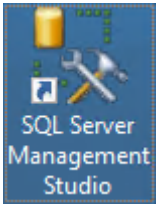
按下 **Yes(是)** 停止 SQLSERVER Agent



## 3.2 稽核伺服器層級

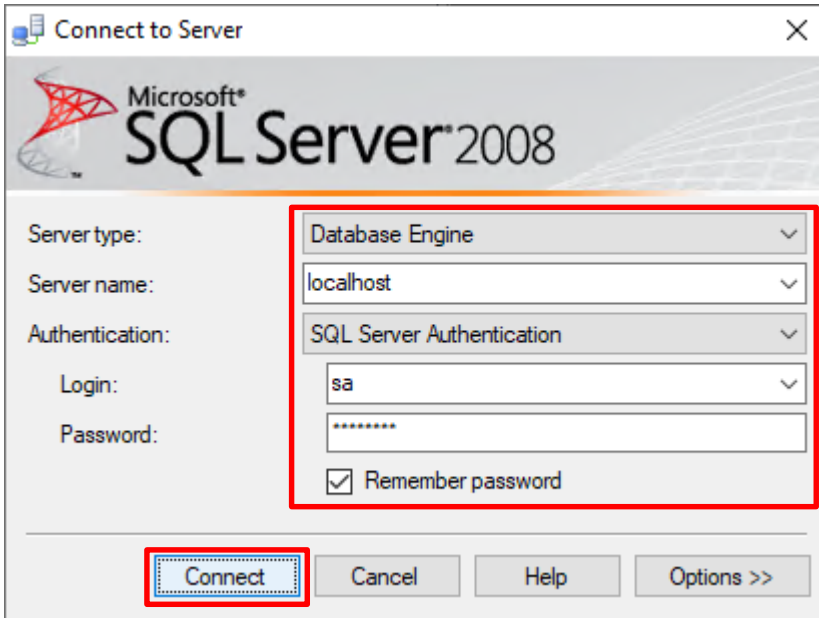
啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

開啟 [Microsoft SQL Server Management Studio](#)

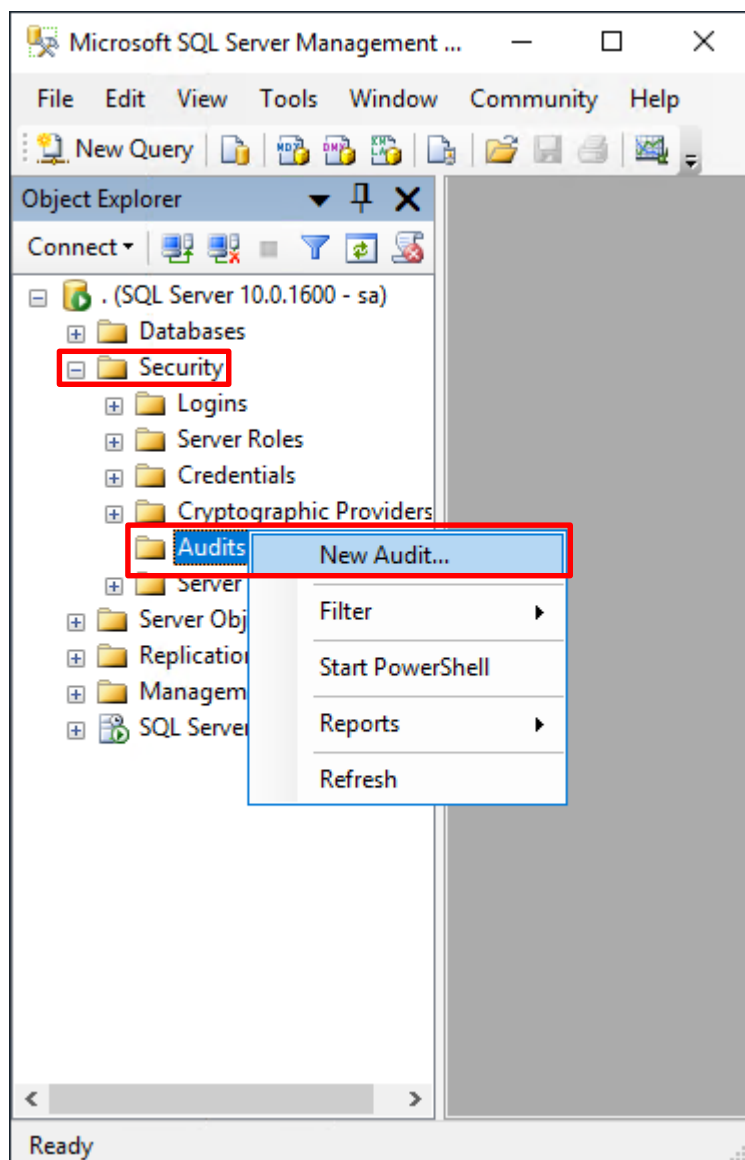


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



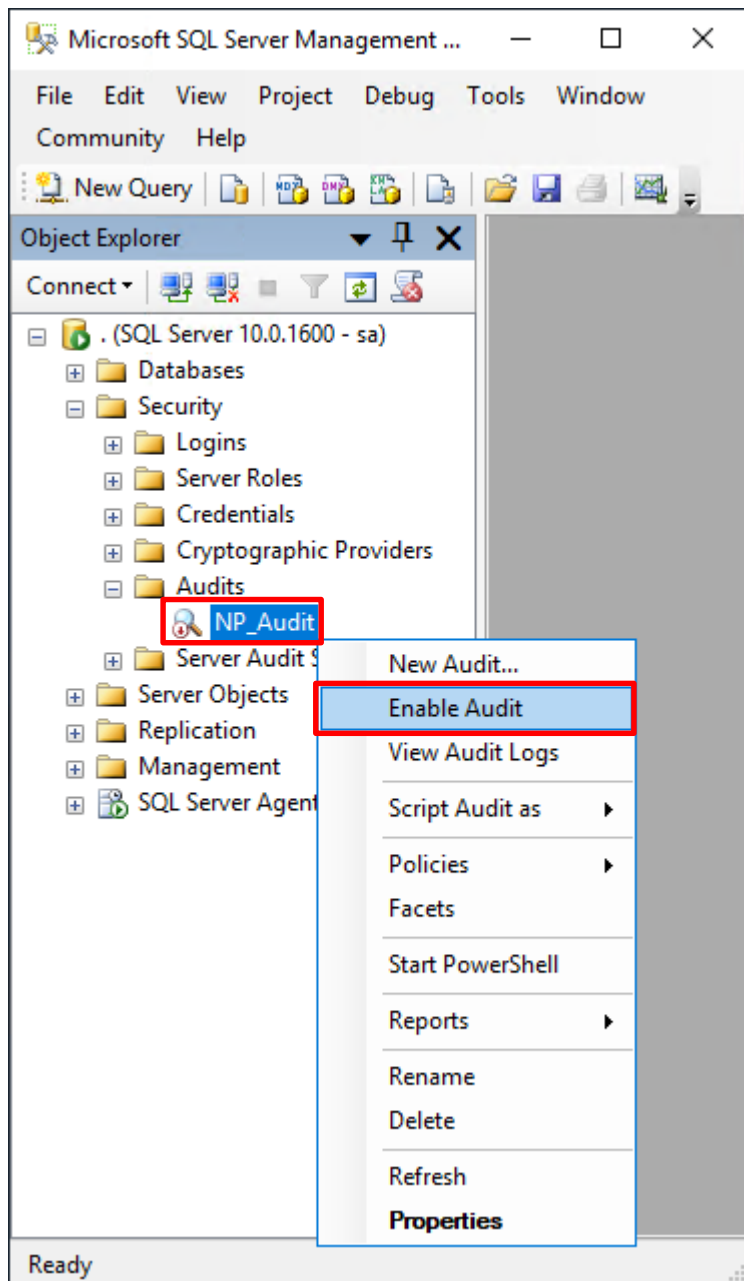
輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(應用程式記錄檔) 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄裡 -> 按下 **OK**(確定)

The screenshot shows the 'Create Audit' dialog box with the following configuration:

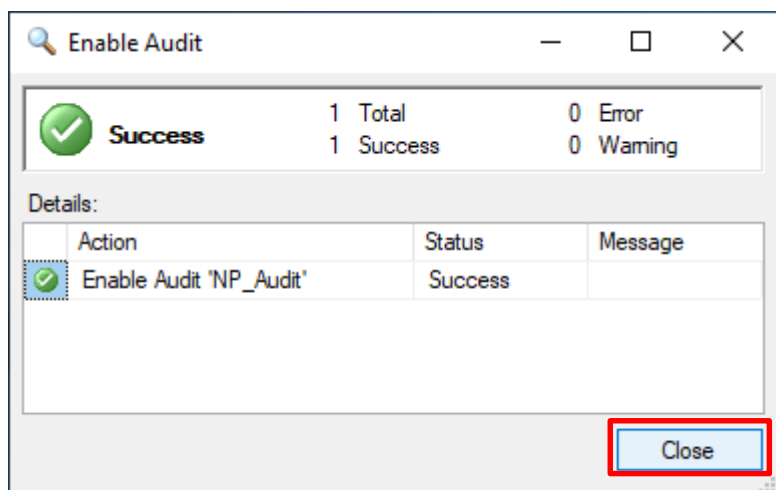
- Audit name:** NP\_Audit
- Queue delay:** 1000
- Shut down server on audit log failure
- Audit:** Application Log
- File path:** (empty)
- Maximum:** 2147483647
- Unlimited
- Maximum file:** 0
- MB  GB  TB
- Unlimited
- Reserve disk space

The 'OK' button at the bottom right is highlighted with a red box.

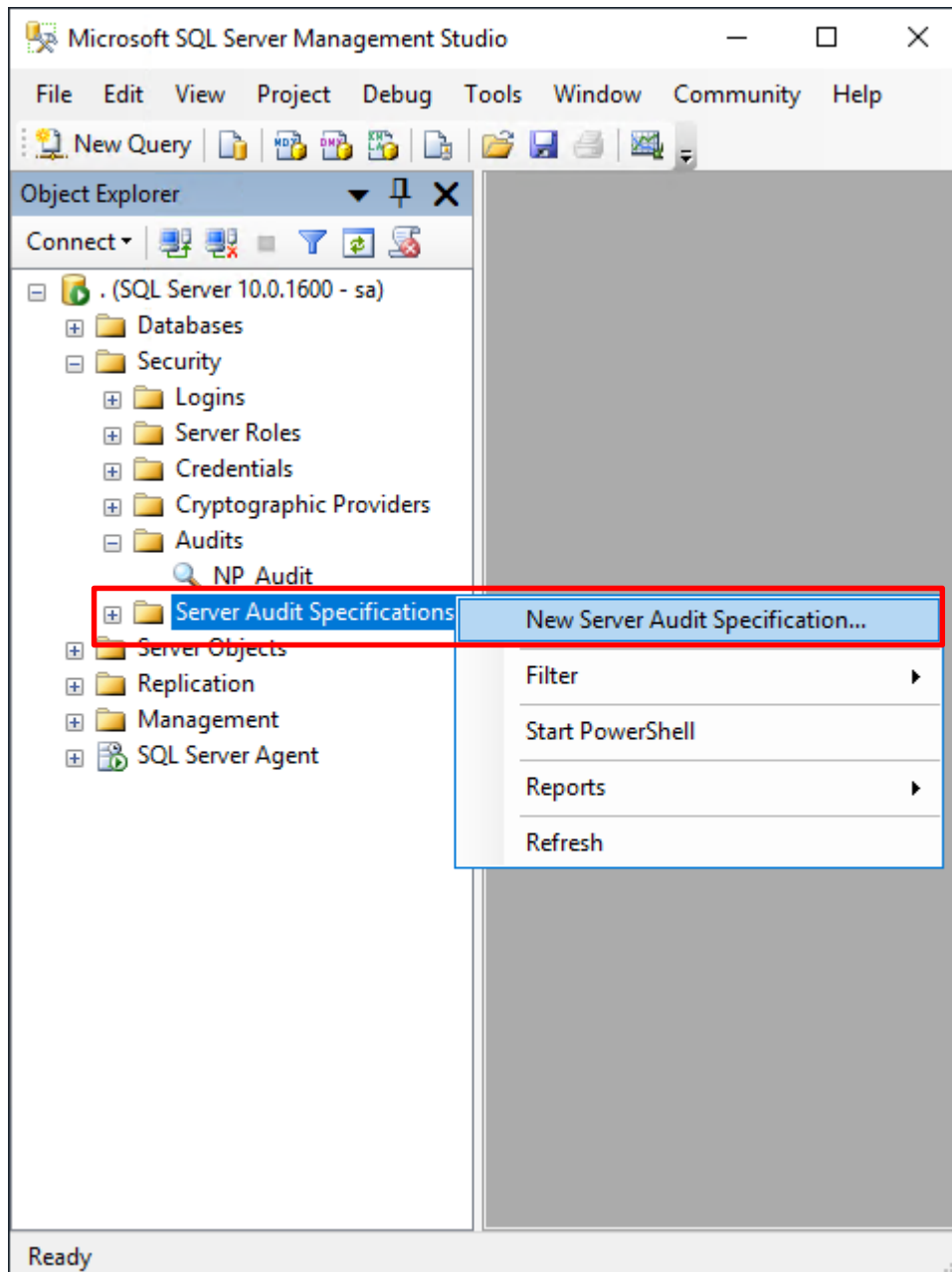
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



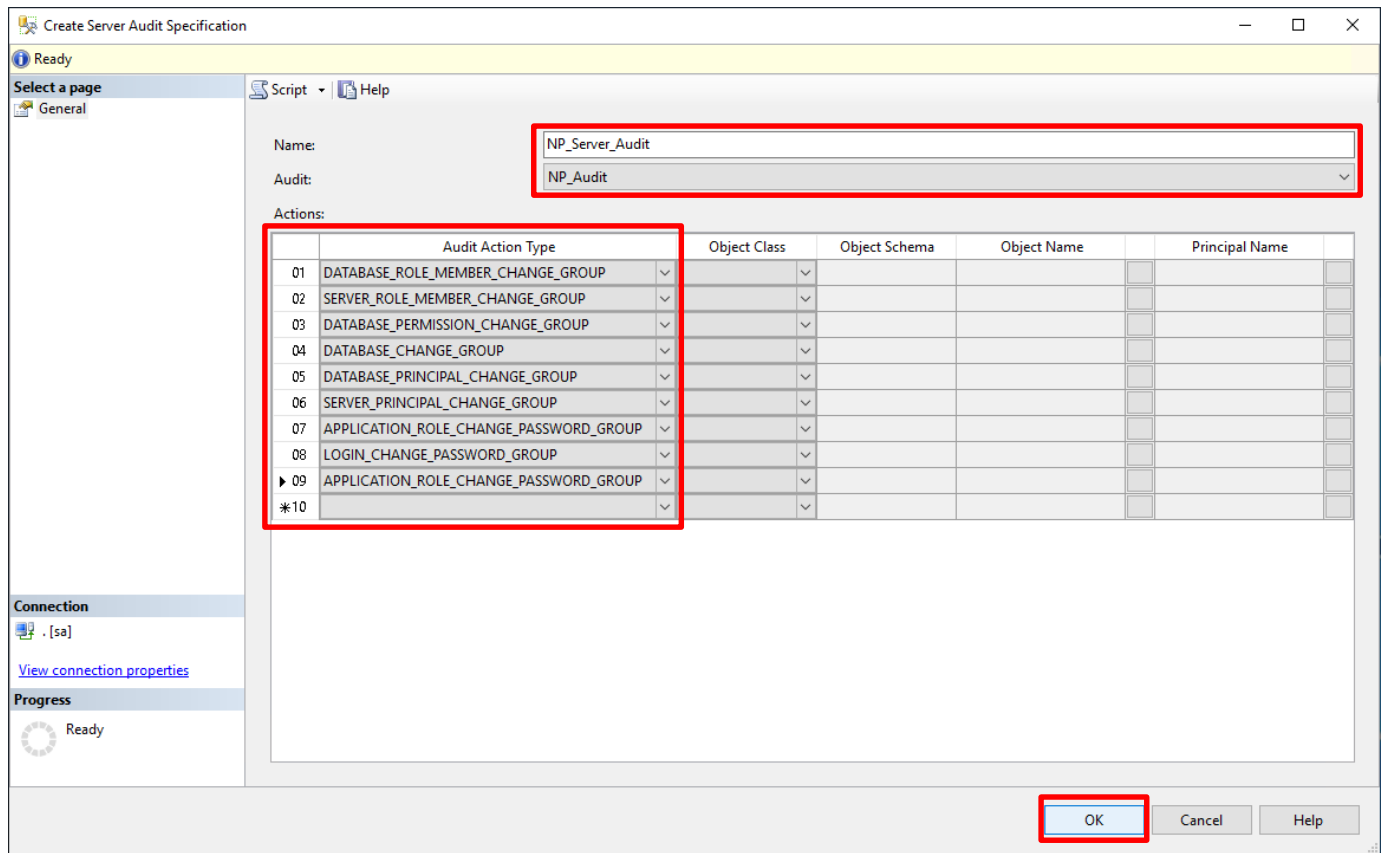
按下 **Close(關閉)**



在 **Server Audit Specifications**(伺服器稽核規格) 按滑鼠右鍵 -> 點選 **New Server Audit Specification**(新增伺服器稽核規格)...

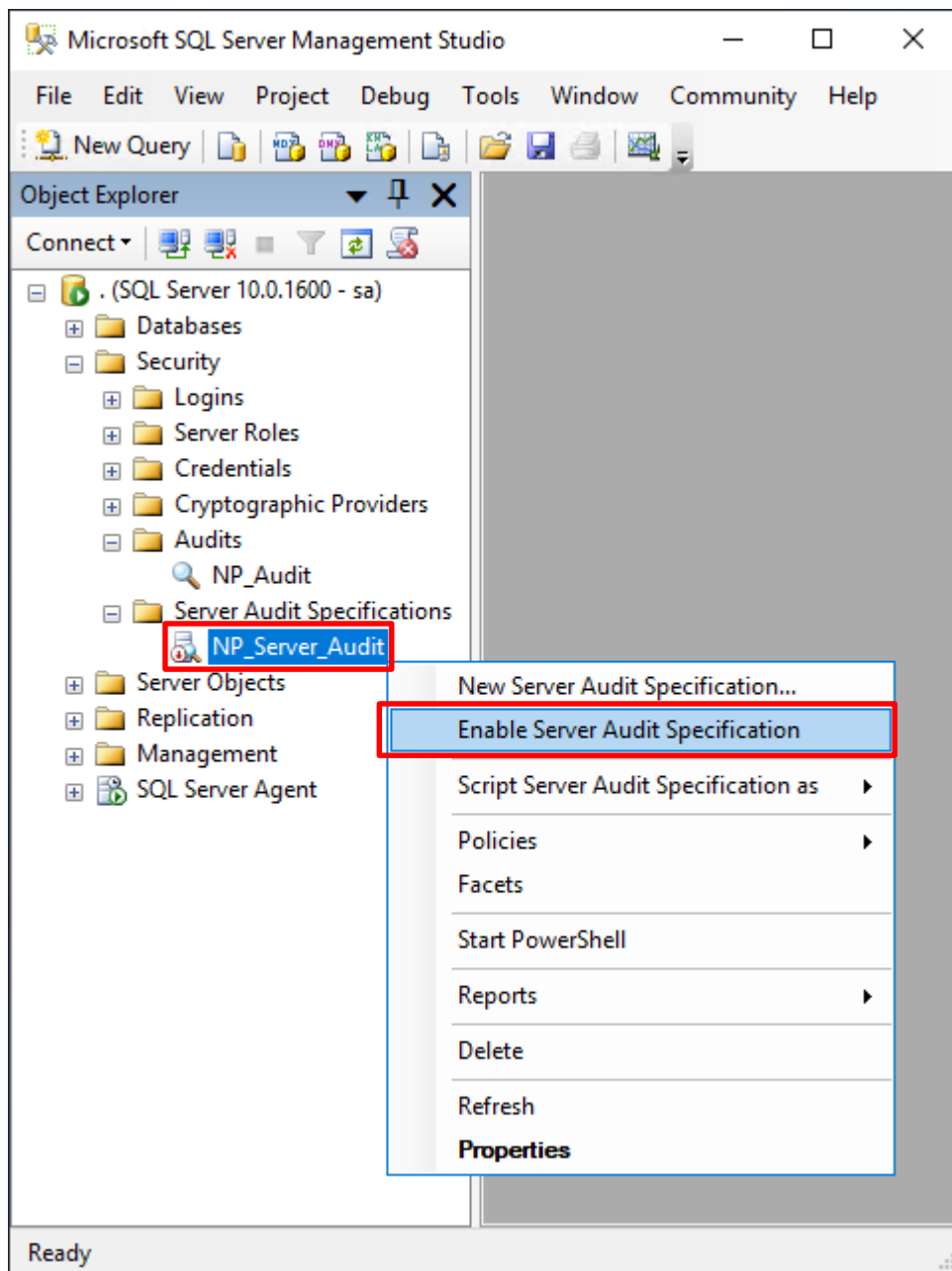


輸入 **Name(伺服器稽核規格名稱): NP\_Server\_Audit** -> 選擇 **Audit(稽核): NP\_Audit** 和 **Actions(動作): 範例簡易條列** · 詳細說明請參考前言的[稽核動作群組連結](#) -> 按下 **OK(確定)**



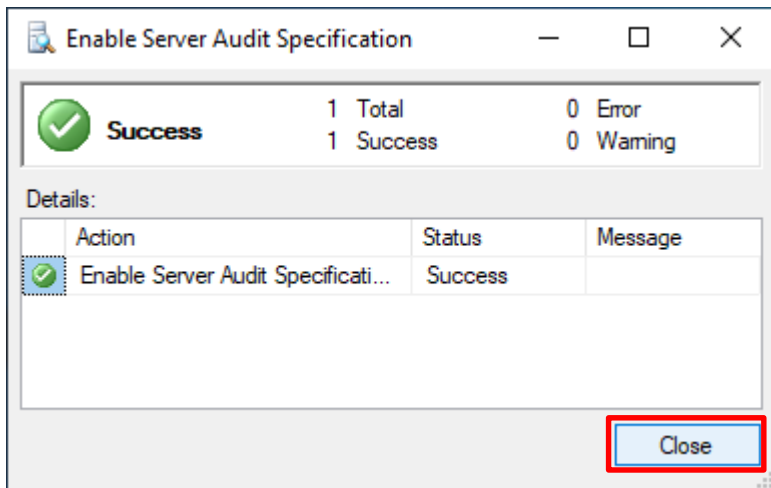
在 **Server Audit Specifications name**(伺服器稽核規格名稱): **NP\_Server\_Audit** 按滑鼠右鍵 -> 點選 **Enable**

**Server Audit Specification**(啟用伺服器稽核規格)





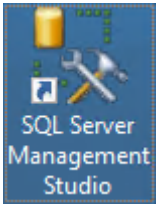
按下 **Close(關閉)**



### 3.3 稽核資料庫層級

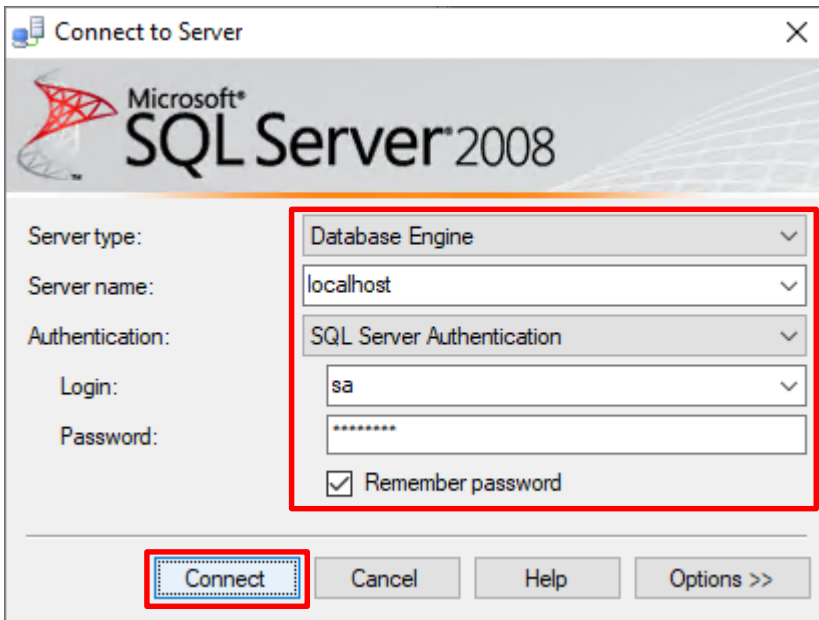
啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

開啟 [Microsoft SQL Server Management Studio](#)

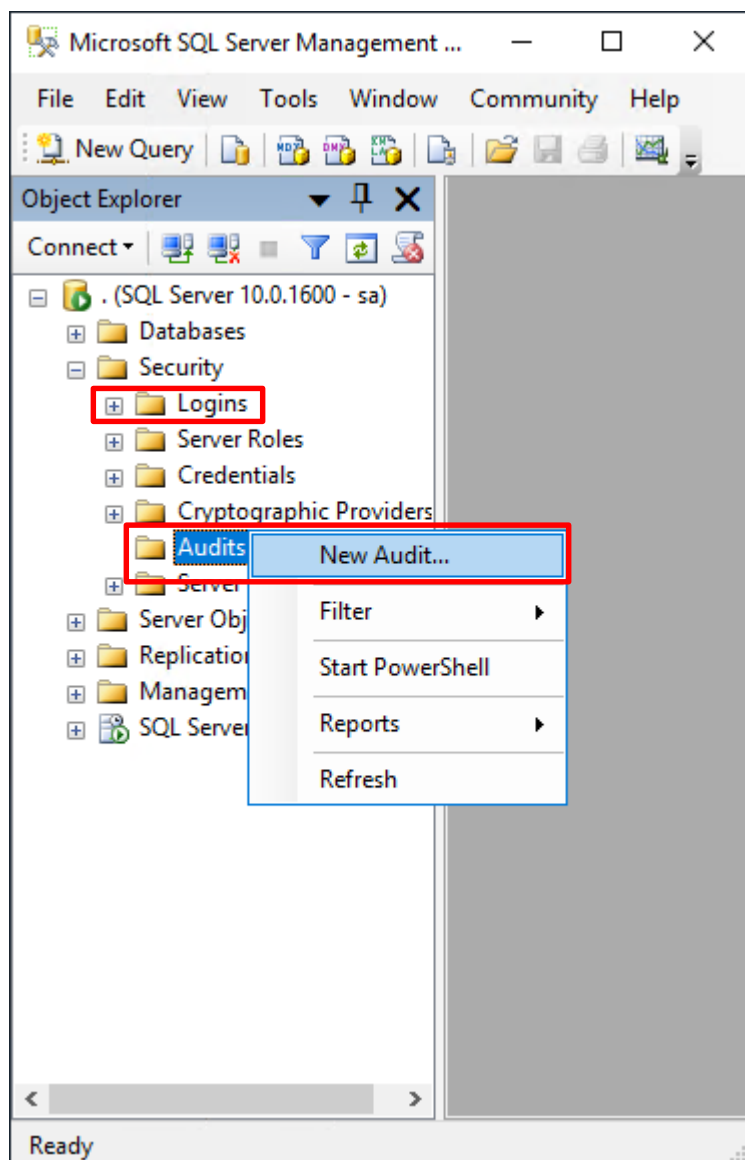


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



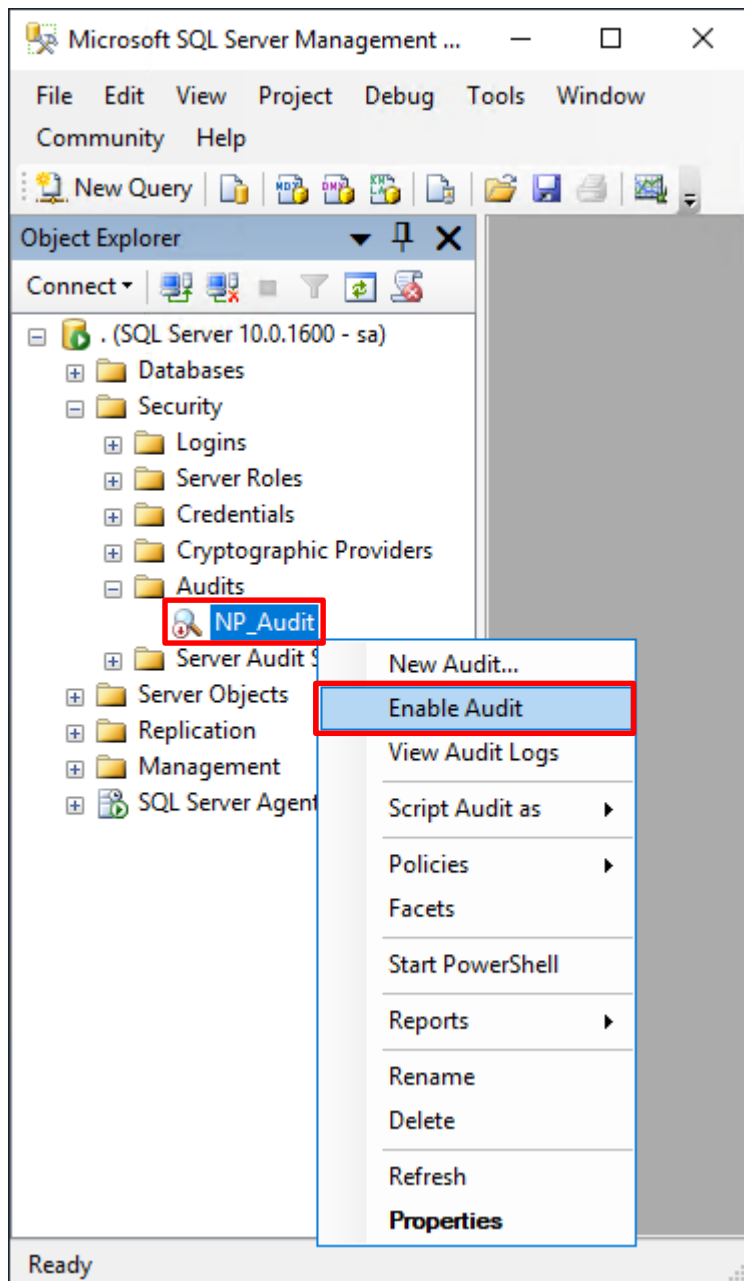
輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(應用程式記錄檔) 將 MS SQL 稽核記錄儲存於 Windows 事件檢視器的應用程式記錄裡 -> 按下 **OK**(確定)

The screenshot shows the 'Create Audit' dialog box with the following configuration:

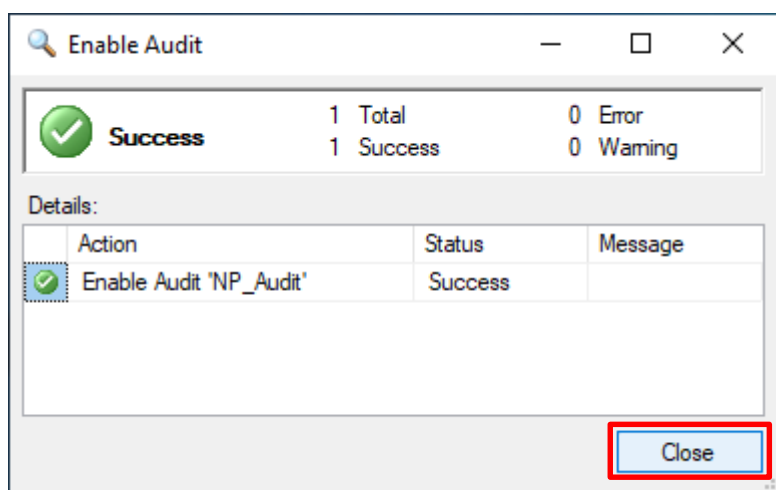
- Audit name:** NP\_Audit
- Queue delay:** 1000
- Shut down server on audit log failure
- Audit:** Application Log
- File path:** (empty)
- Maximum:** 2147483647
- Unlimited
- Maximum file:** 0
- MB  GB  TB
- Unlimited
- Reserve disk space

The 'OK' button at the bottom right is highlighted with a red box.

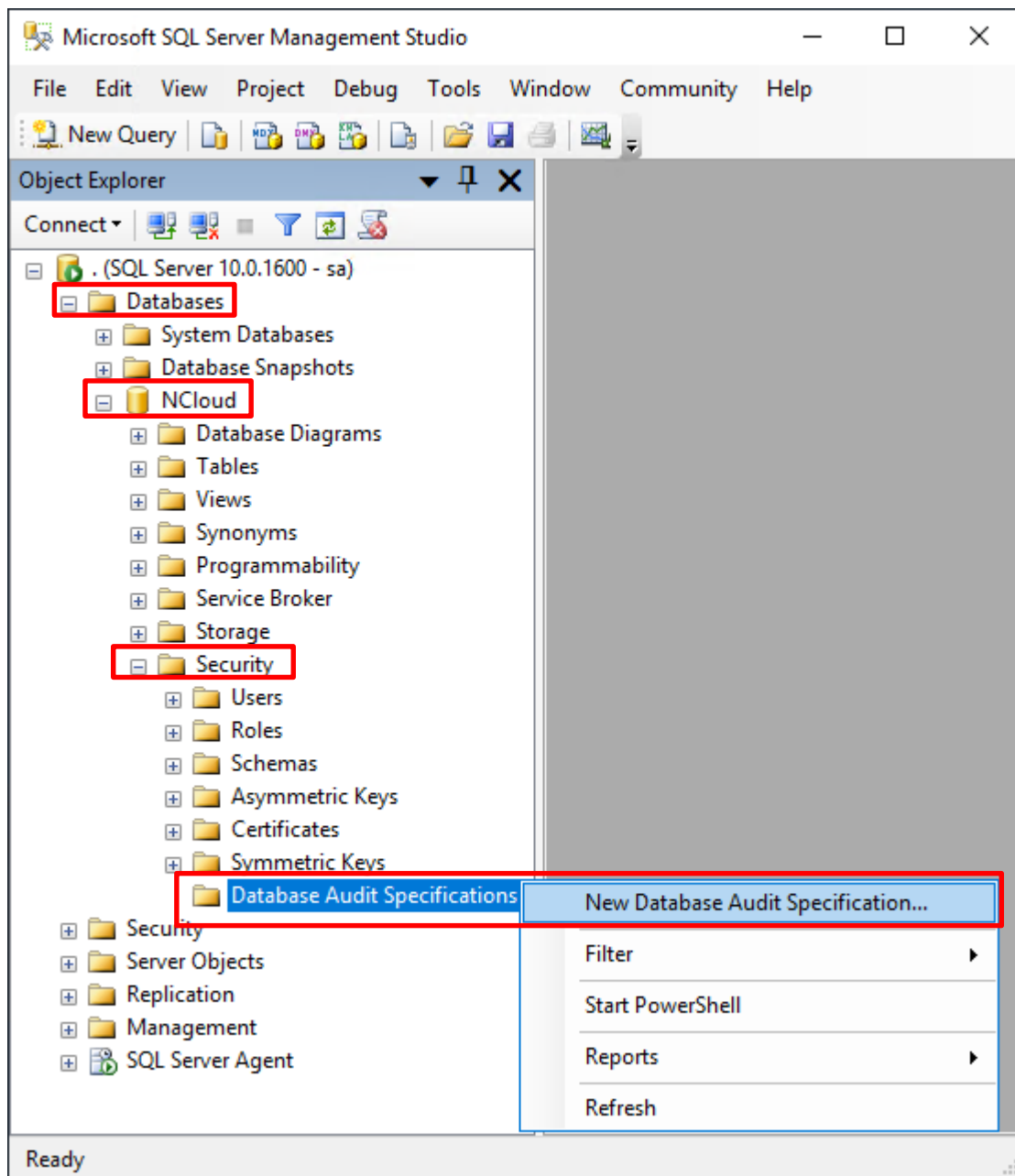
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



按下 **Close(關閉)**



選擇 **Databases(資料庫)** -> **DB(NCloud)** -> **Security(安全性)** -> 在 **Database Audit Specifications(資料庫稽核規格)**  
上按滑鼠右鍵 -> 點選 **New Database Audit Specification(新增資料庫稽核規格)**...



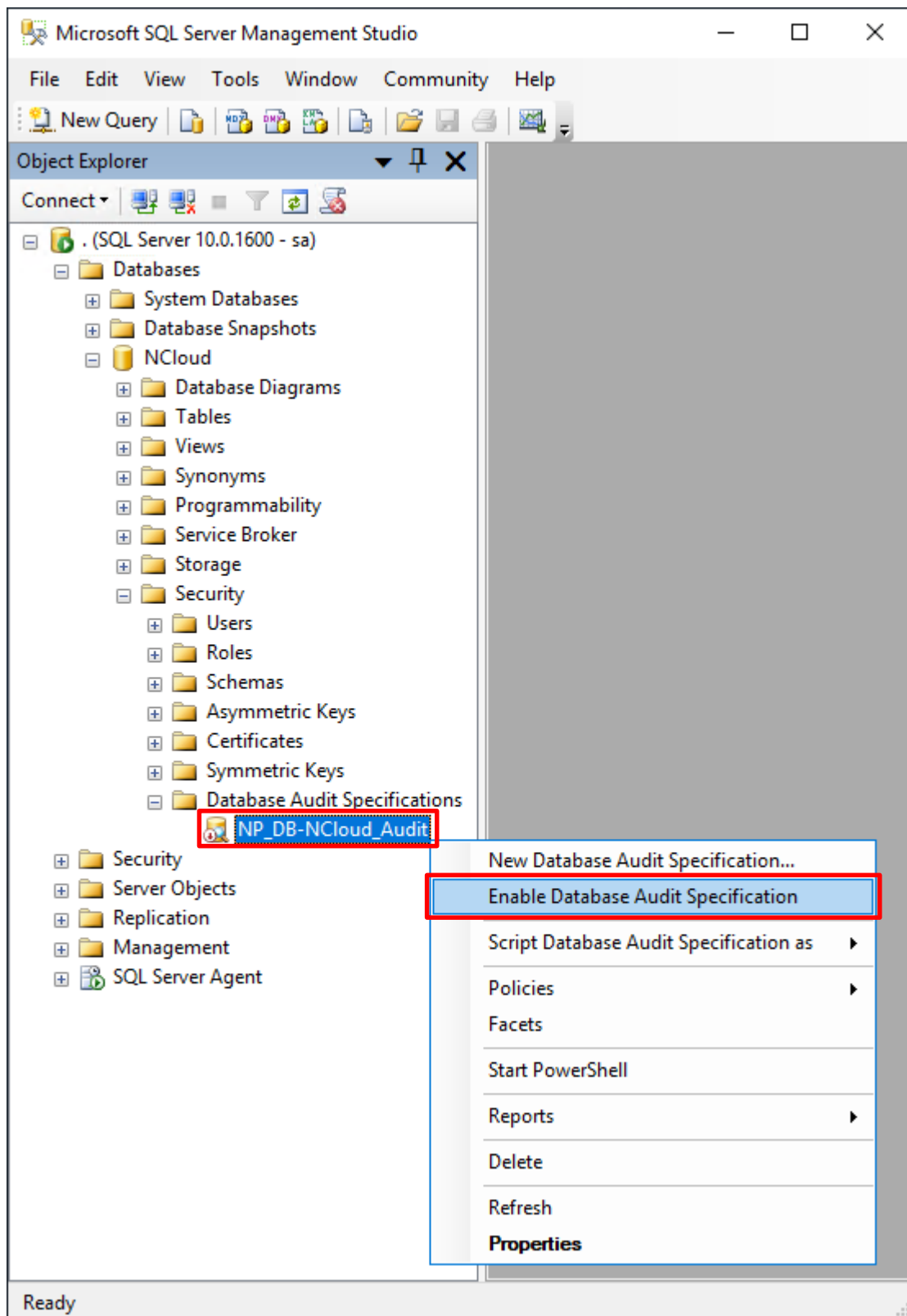
輸入 **Name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 選擇 **Audit**(稽核名稱): **NP\_Audit** 和 **Actions**(動作):  
範例簡易條列 · 詳細說明請參考前文的[稽核動作群組連結](#) -> 按下 **OK**(確定)

The screenshot shows the 'Create Database Audit Specification' dialog box. The 'Name' field contains 'NP\_DB-NCloud\_Audit' and the 'Audit' dropdown is set to 'NP\_Audit'. The 'Actions' table is as follows:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
2	BACKUP_RESTORE_GROUP				
3	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
4	SCHEMA_OBJECT_CHANGE_GROUP				
▶▶5					

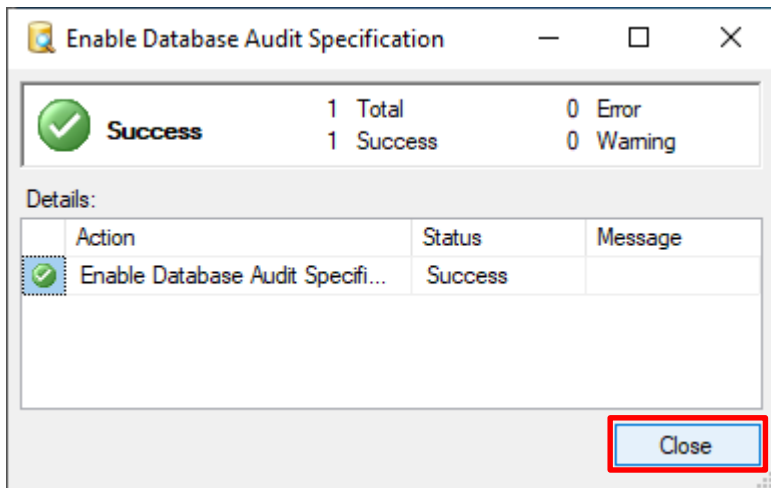
The 'OK' button is highlighted with a red box.

在 **Database Audit Specifications name**(資料庫稽核規格名稱): *NP\_DB-NCloud\_Audit* -> 點選 **Enable Database Audit Specification**(啟用資料庫稽核規格)





按下 **Close(關閉)**



## 4. SQL 2012

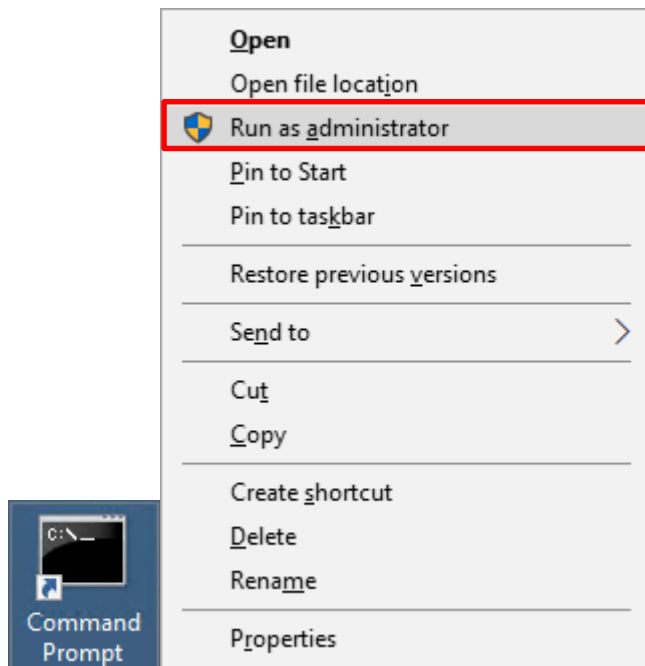
### 4.1 稽核登入

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，才會生效。

以下分別為指令介面和圖形介面設定方式。

#### 4.1.1 使用指令介面方式設定

在 **Command Prompt(命令提示字元)** 上按滑鼠右鍵 -> 點選 **Run as administrator(以系統管理員身分執行)**



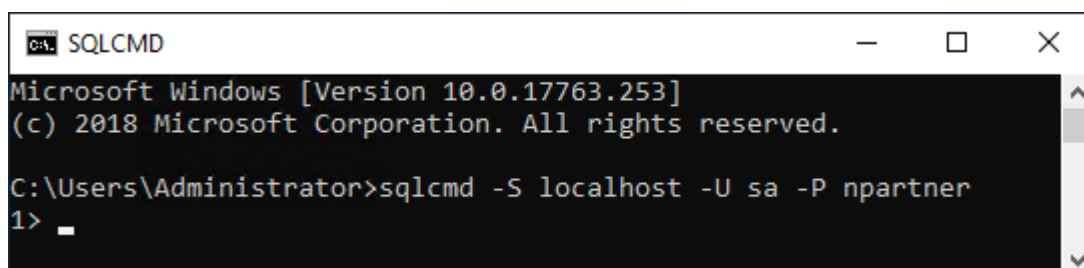
輸入 `sqlcmd -S localhost -U sa -P npartner`

#### Options:

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

**-U** login\_id

**-P** password



輸入 `use master -> go`

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

使用 `sp_configure` 列出進階選項

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

```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

啟用通用條件合規性

輸入 `exec sp_configure 'common criteria compliance enabled', 1 -> go -> reconfigure with override -> go`

```
SQLCMD
1> exec sp_configure 'common criteria compliance enabled', 1
2> go
Configuration option 'common criteria compliance enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure with override
2> go
1> _
```

啟用失敗和成功的登入記錄

輸入 `EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',`

`N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 -> go -> quit`

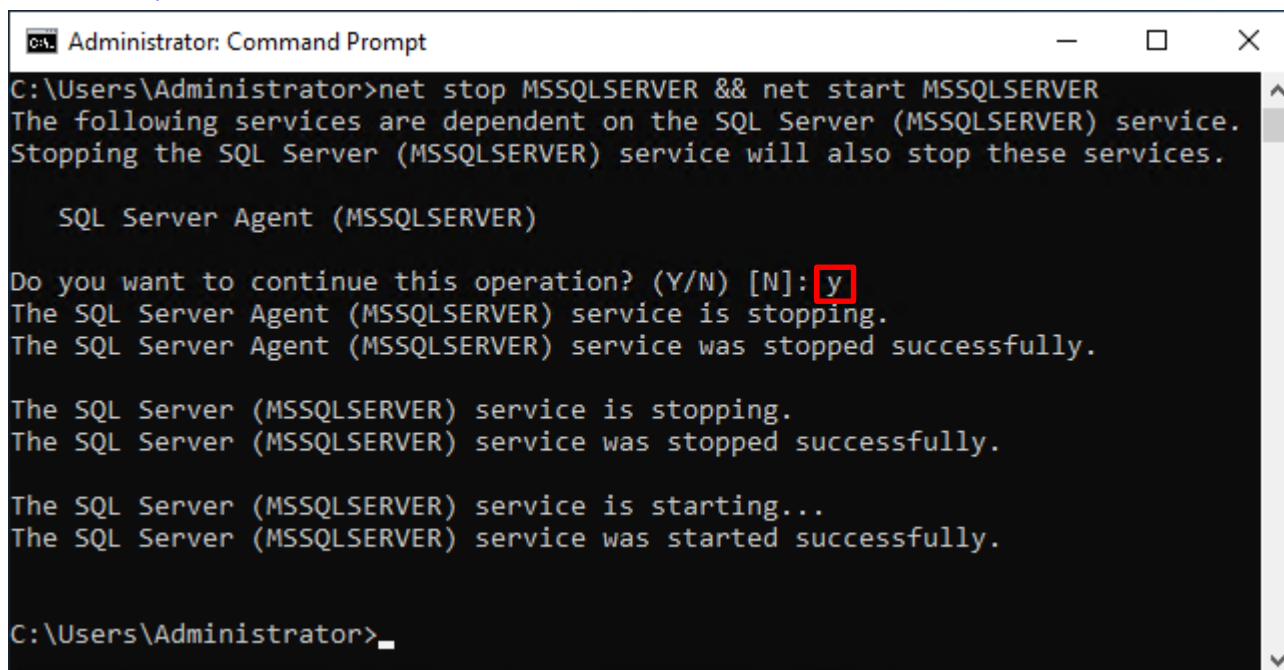
```
Administrator: Command Prompt
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit

C:\Users\Administrator>_
```

重新啟動 MSSQLSERVER 服務

輸入 `net stop MSSQLSERVER && net start MSSQLSERVER`



```
Administrator: Command Prompt
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSERVER
The following services are dependent on the SQL Server (MSSQLSERVER) service.
Stopping the SQL Server (MSSQLSERVER) service will also stop these services.

    SQL Server Agent (MSSQLSERVER)

Do you want to continue this operation? (Y/N) [N]: y
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is starting...
The SQL Server (MSSQLSERVER) service was started successfully.

C:\Users\Administrator>
```

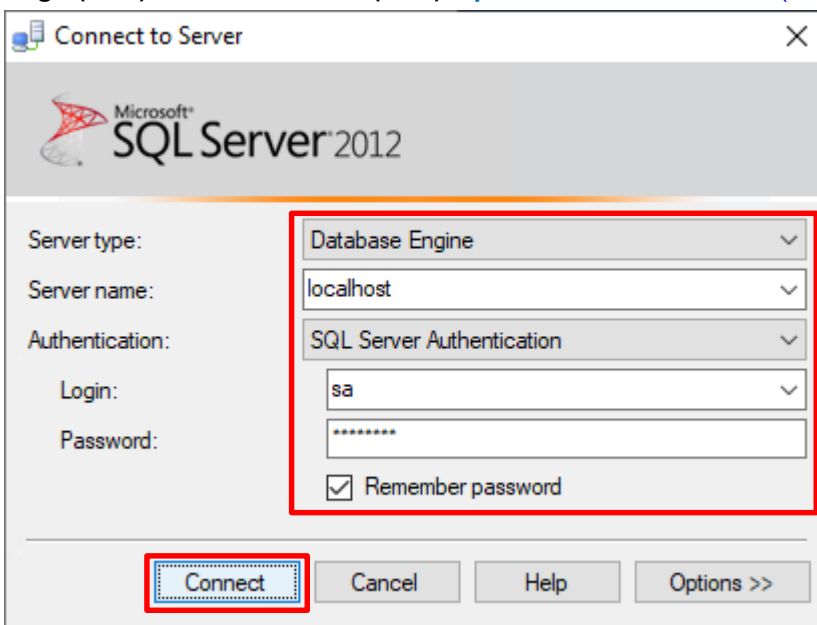
## 4.1.2 使用圖形介面方式設定

開啟 [Microsoft SQL Server Management Studio](#)

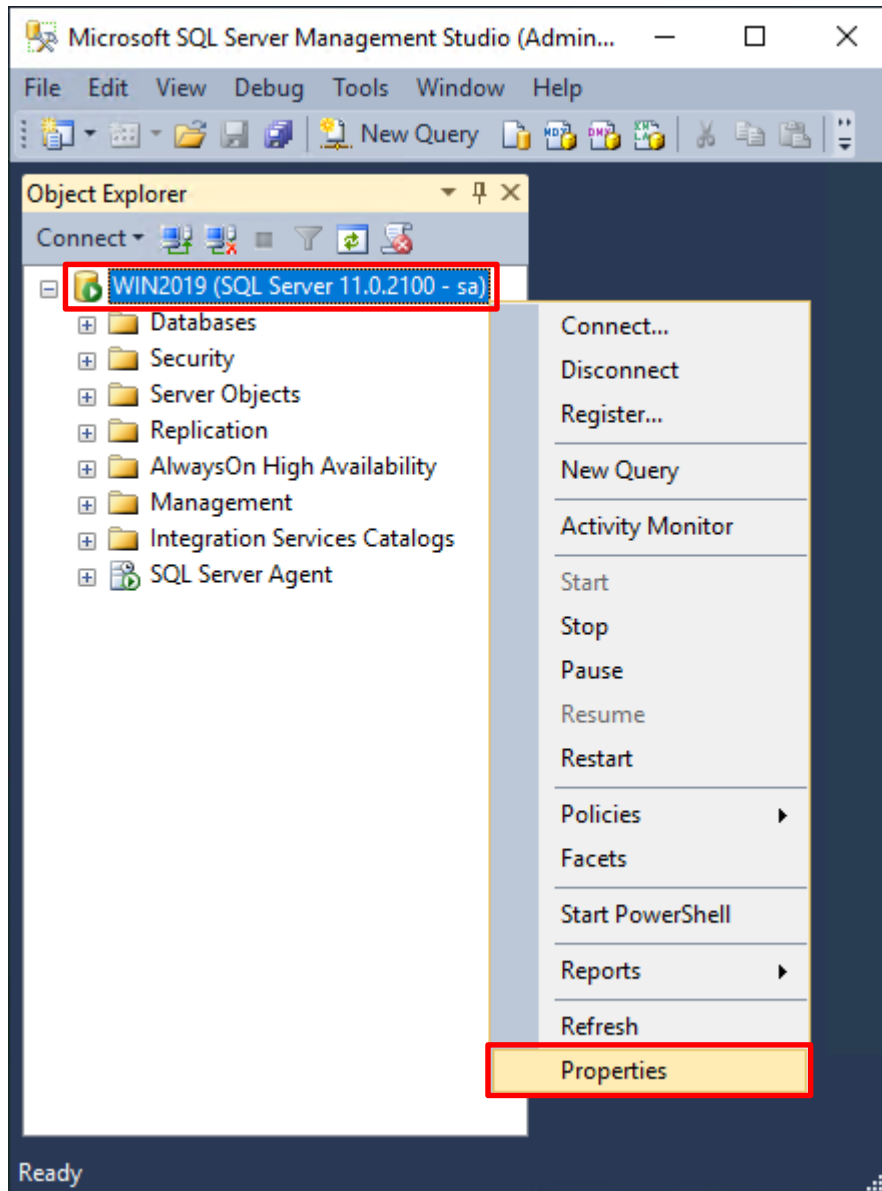


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

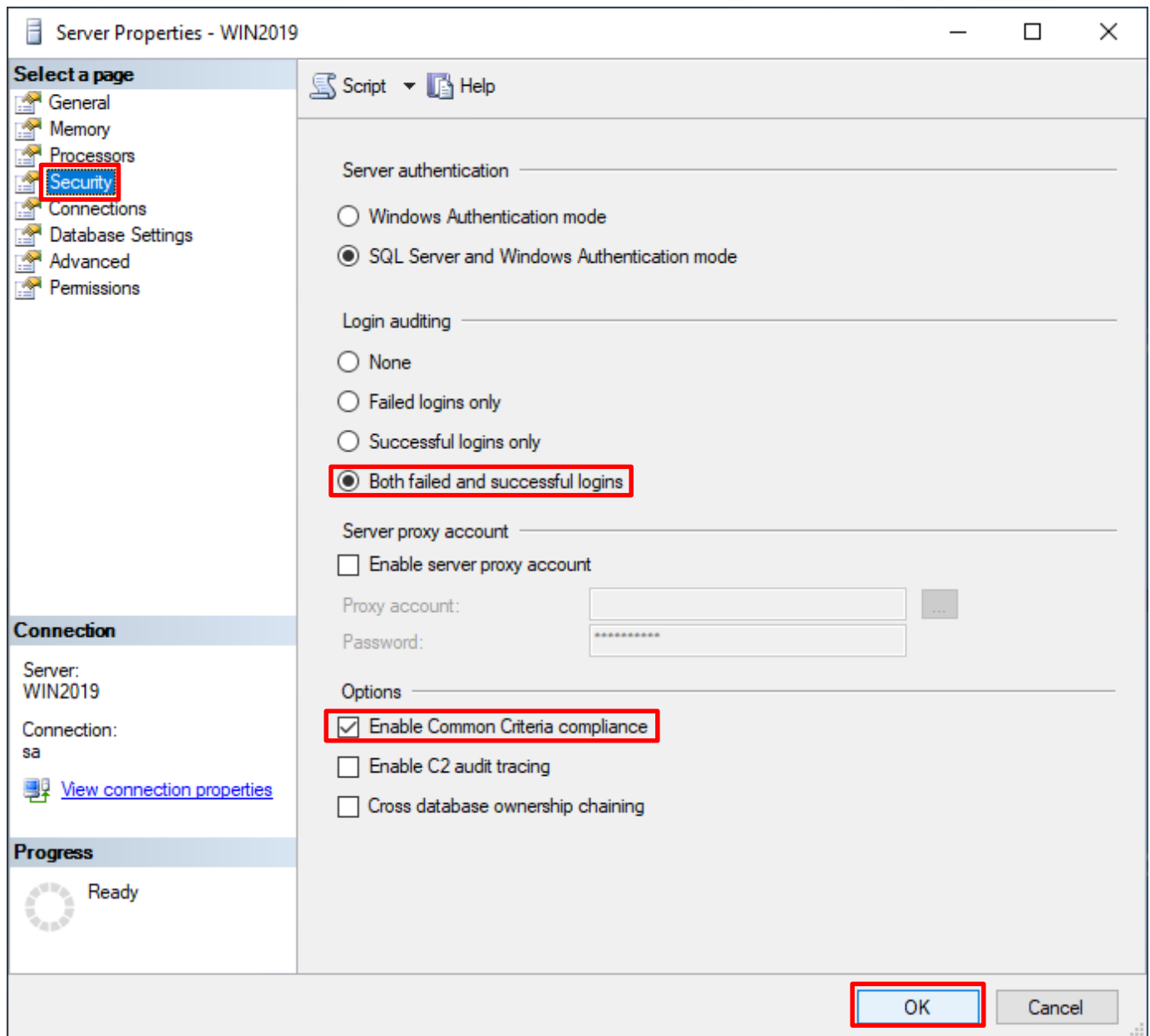
**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



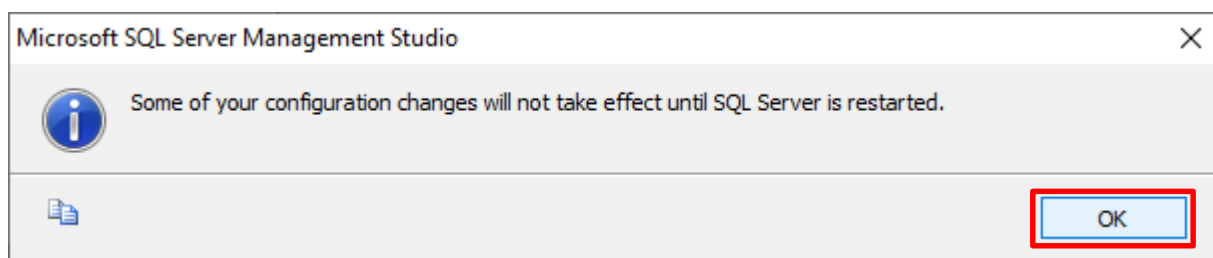
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Properties(屬性)**



選擇 **Security(安全性)** 頁面 -> **Login auditing(登入稽核)**: 點選 **Both failed and successful logins(失敗和成功的登入)** -> **Options**: 勾選 **Enable Common Criteria compliance(啟用通用條件合規性)** -> 按下 **OK(確定)**

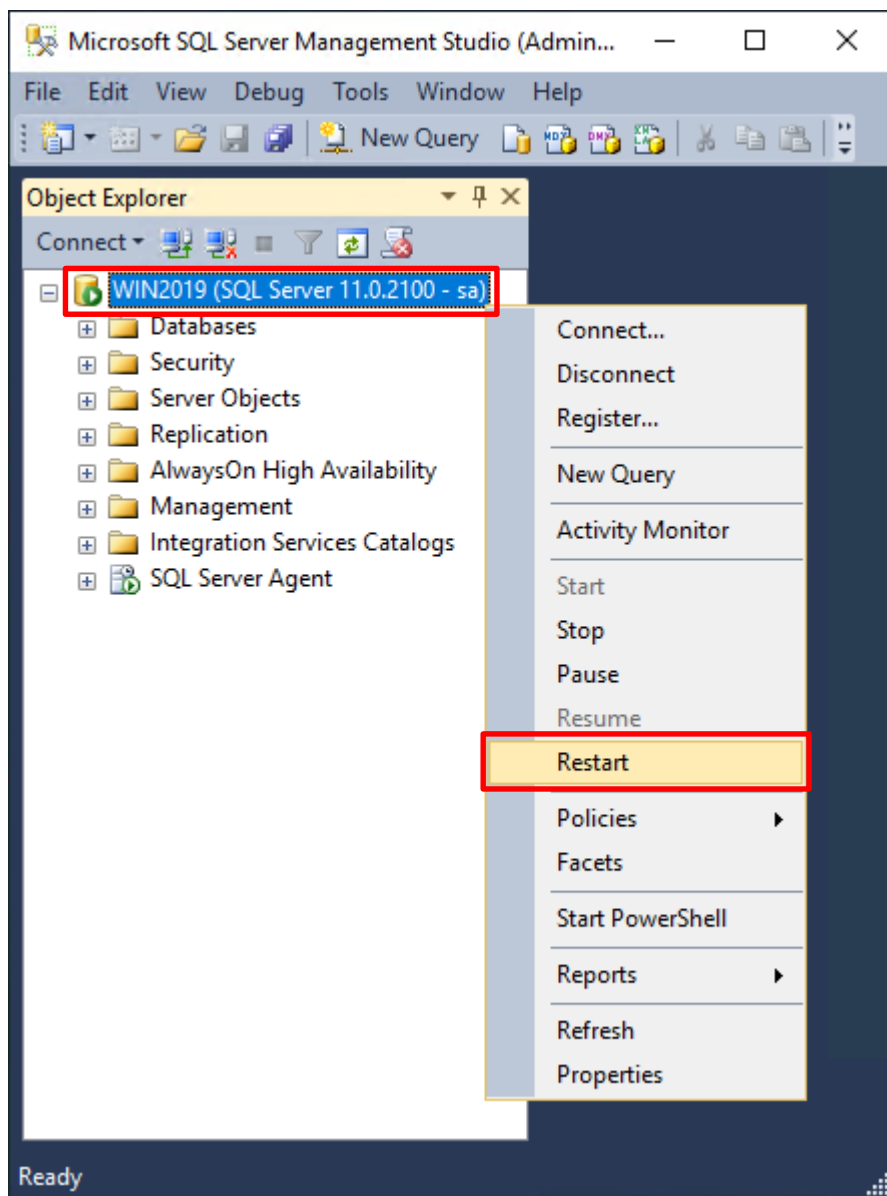


按下 **OK(確定)**

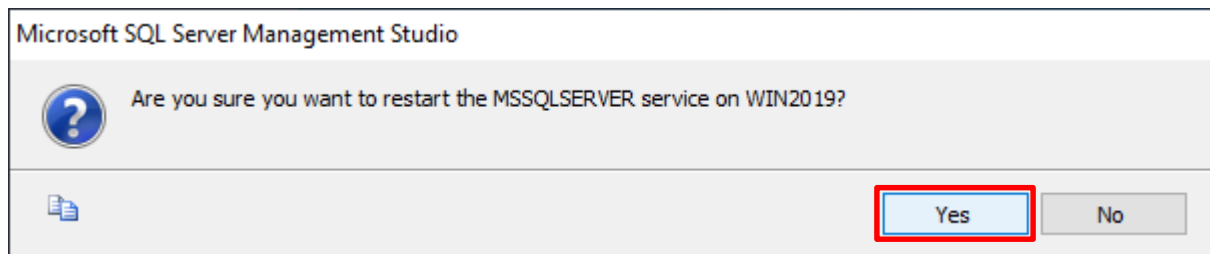


重新啟動 MSSQLSERVER 服務

在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Restart(重新啟動)**

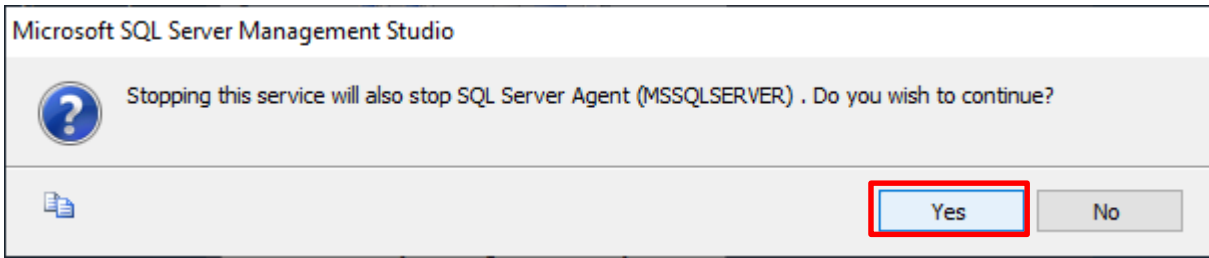


按下 **Yes(是)** 重新啟動 MSSQLSERVER 服務





按下 **Yes(是)** 停止 SQLSERVER Agent



## 4.2 稽核伺服器層級

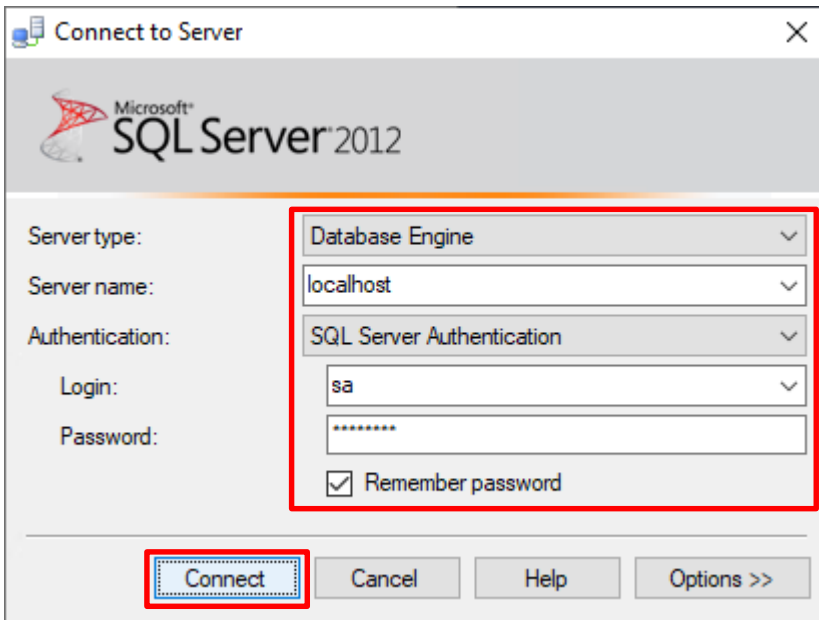
啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

開啟 [Microsoft SQL Server Management Studio](#)

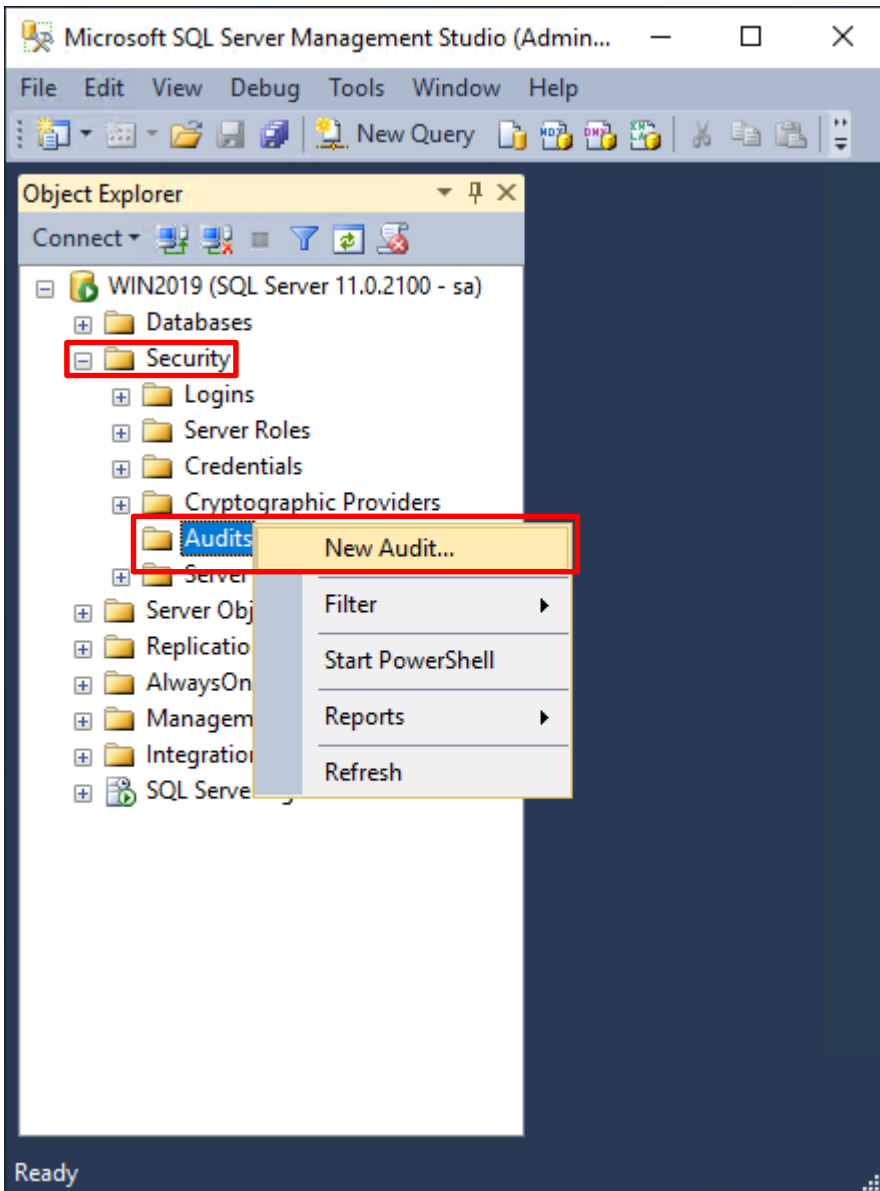


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page: General, Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:  Continue  
 Shut down server  
 Fail operation

Audit destination: Application Log

File path: [Empty]

Audit File Maximum Limit:  Maximum rollover files:  Unlimited  
 Maximum files: Number of files: 2147483647

Maximum file size: 0  MB  GB  TB  
 Unlimited

Reserve disk space

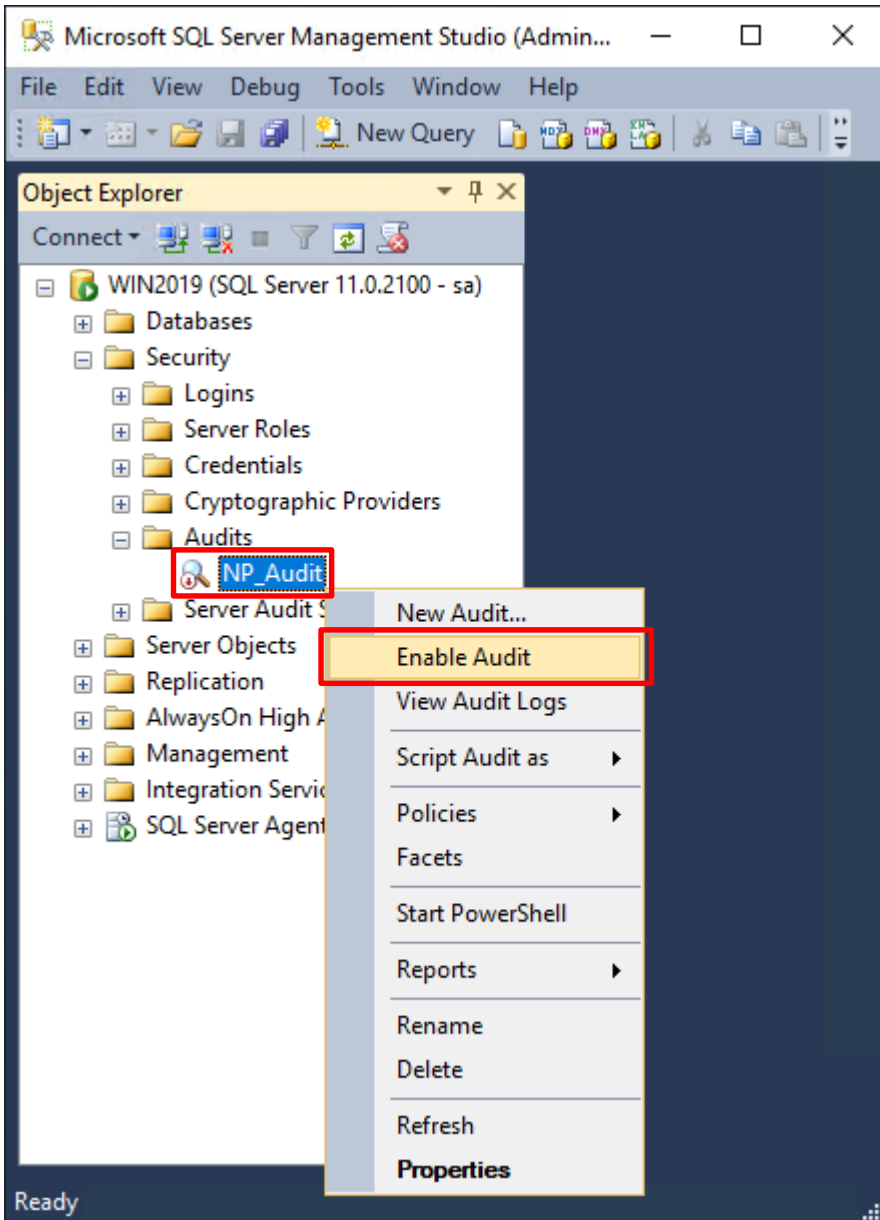
Connection: WIN2019 [sa]

[View connection properties](#)

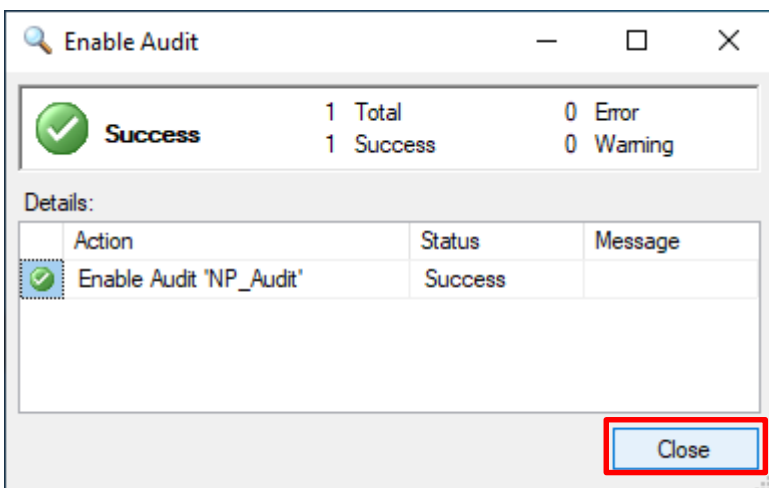
Progress: Ready

OK Cancel Help

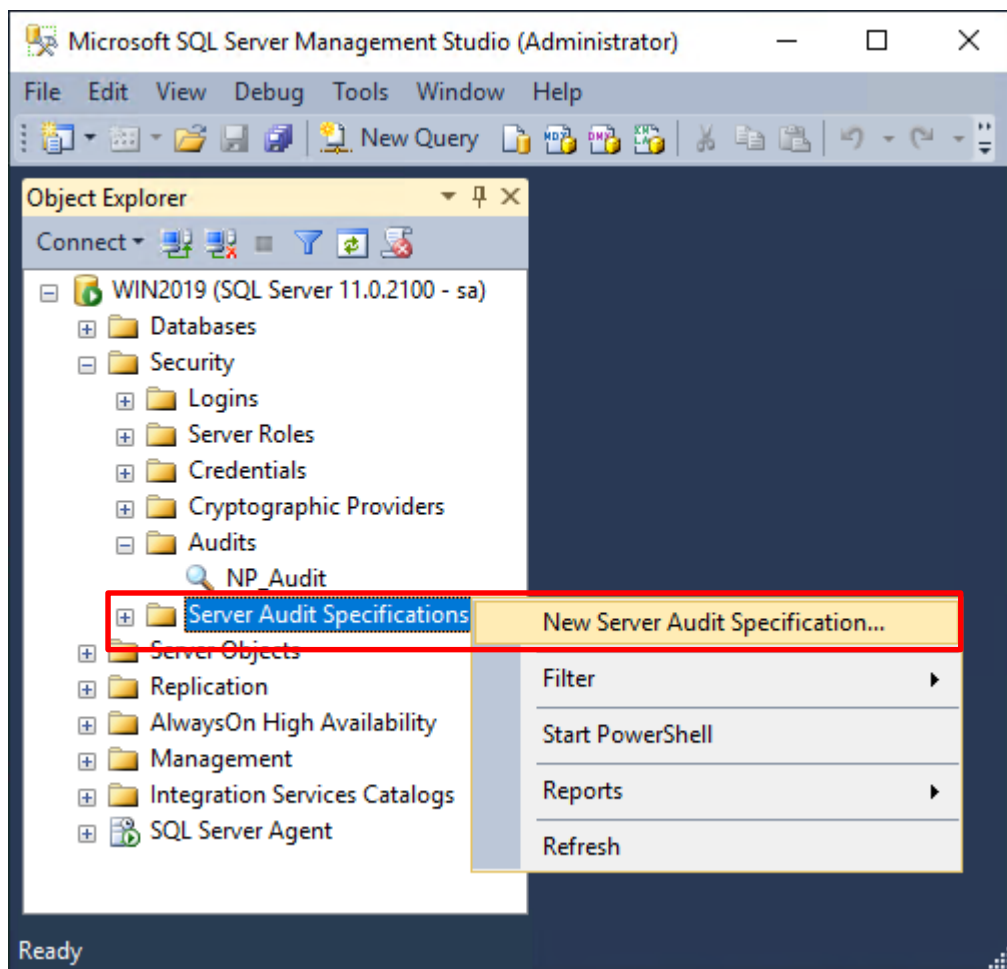
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



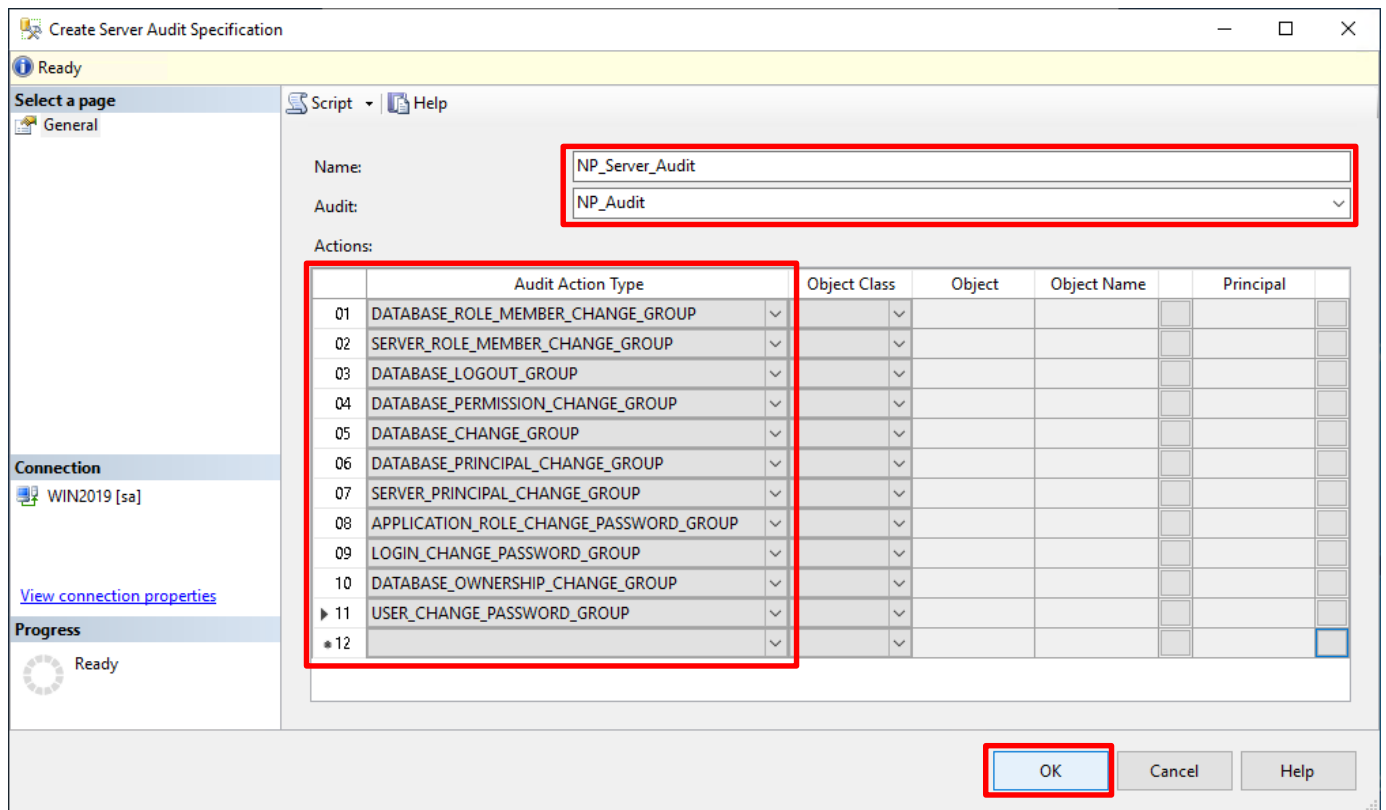
按下 **Close(關閉)**



在 [Server Audit Specifications](#)(伺服器稽核規格) 按滑鼠右鍵 -> 點選 [New Server Audit Specification](#)(新增伺服器稽核規格)...

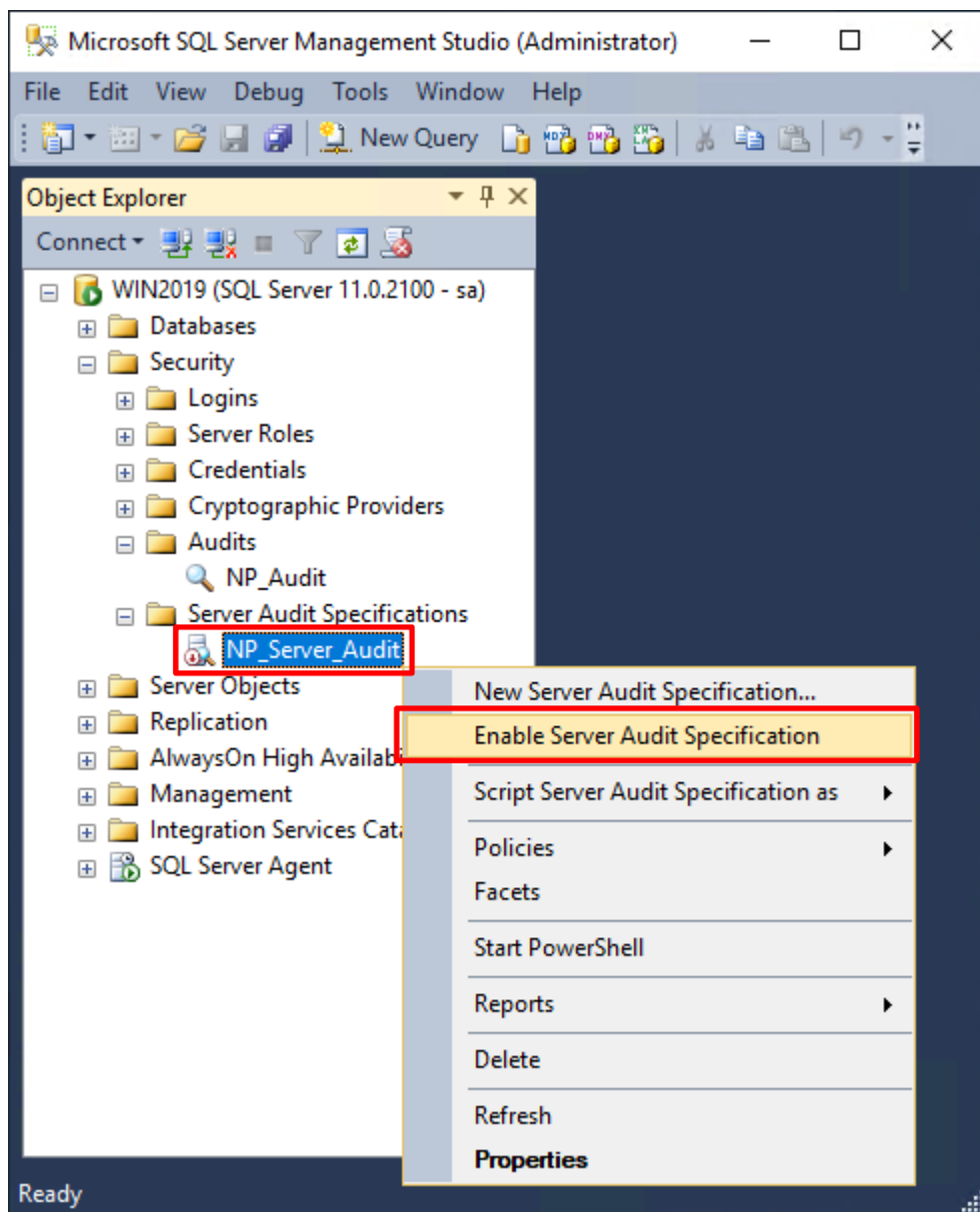


輸入 **Name(伺服器稽核規格名稱): NP\_Server\_Audit** -> 選擇 **Audit(稽核): NP\_Audit** 和 **Actions(動作): 範例簡易條列** · 詳細說明請參考前言的[稽核動作群組連結](#) -> 按下 **OK(確定)**



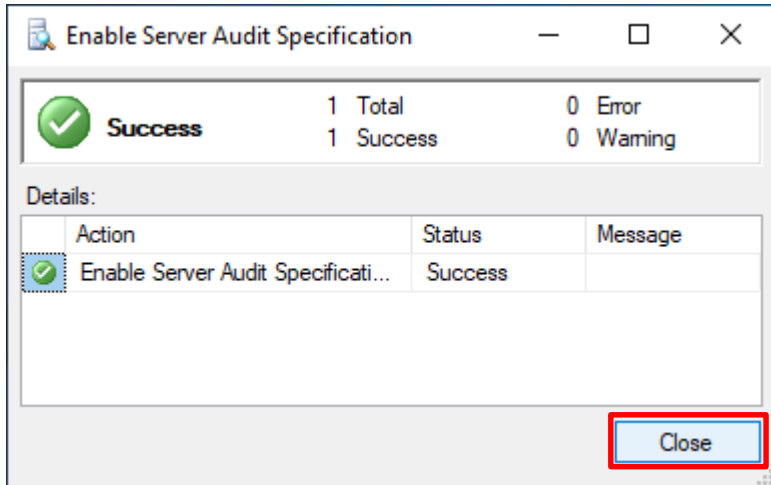
在 **Server Audit Specifications name**(伺服器稽核規格名稱): **NP\_Server\_Audit** 按滑鼠右鍵 -> 點選 **Enable**

**Server Audit Specification**(啟用伺服器稽核規格)





按下 **Close(關閉)**



## 4.3 稽核資料庫層級

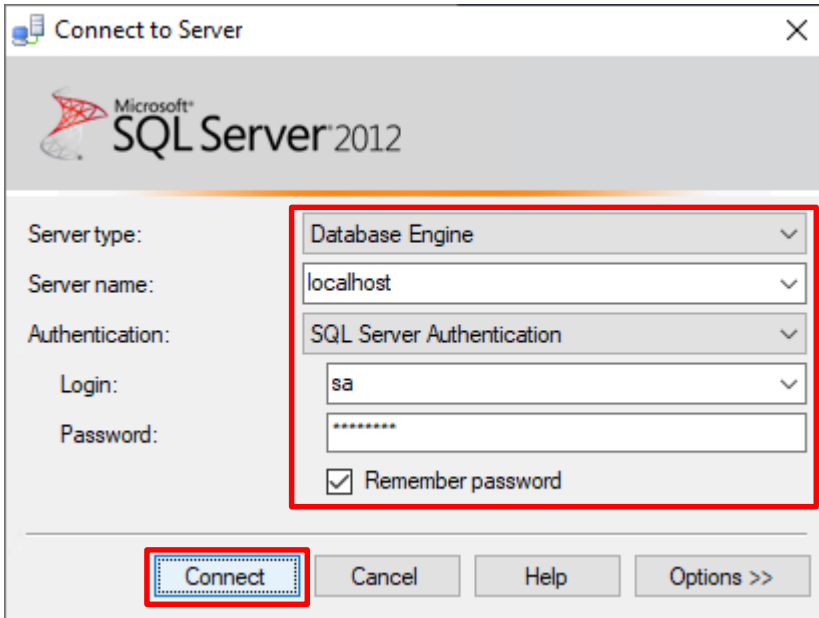
啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

開啟 [Microsoft SQL Server Management Studio](#)

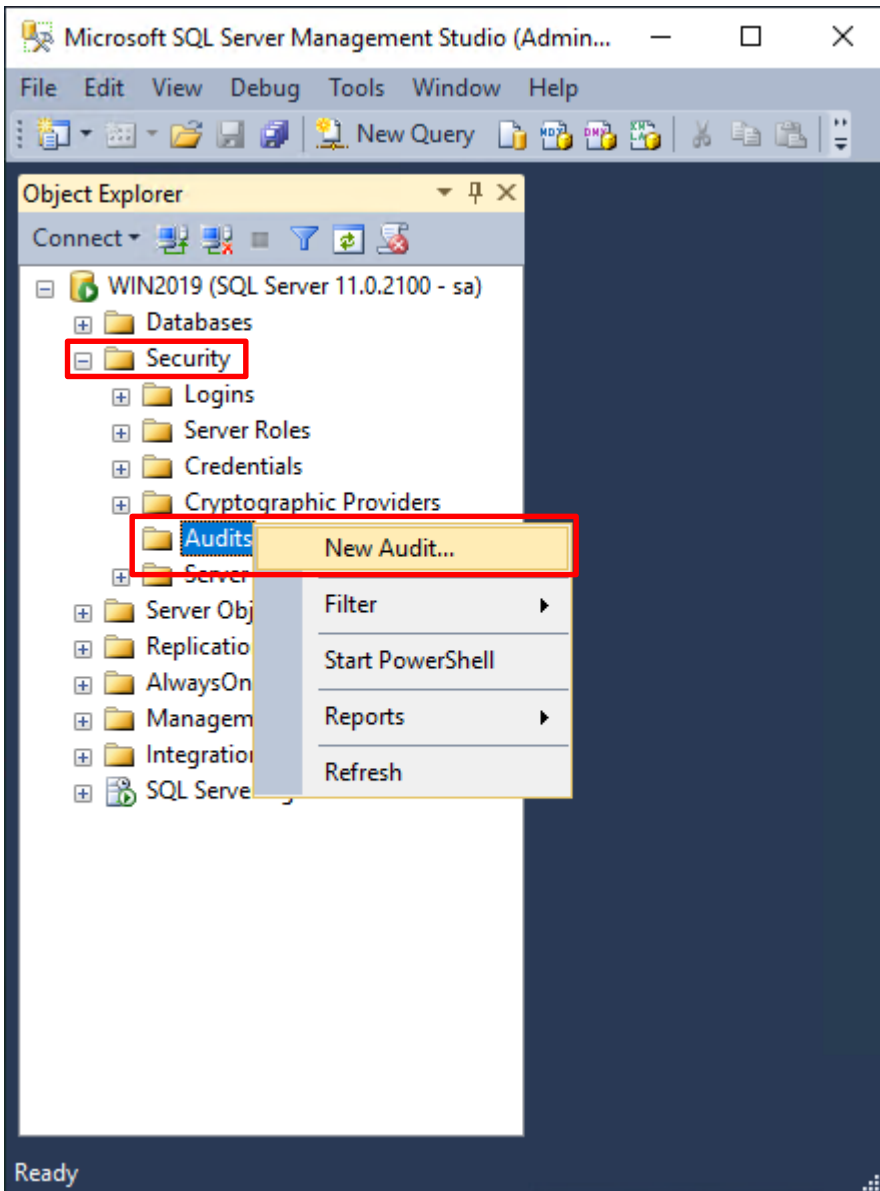


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page: General, Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:  Continue  
 Shut down server  
 Fail operation

Audit destination: Application Log

File path: [Empty]

Audit File Maximum Limit:  Maximum rollover files:  Unlimited  
 Maximum files: Number of files: 2147483647

Maximum file size: 0  MB  GB  TB  
 Unlimited

Reserve disk space

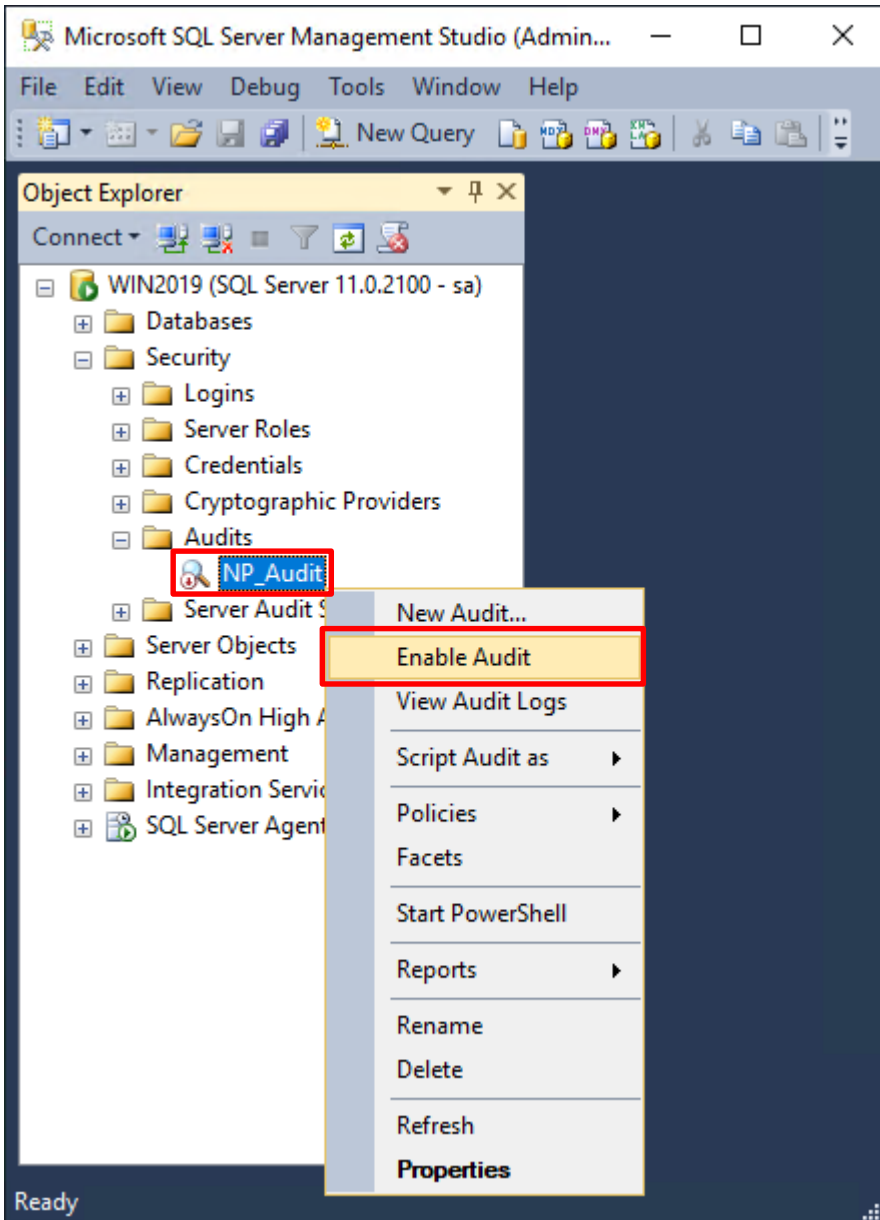
Connection: WIN2019 [sa]

[View connection properties](#)

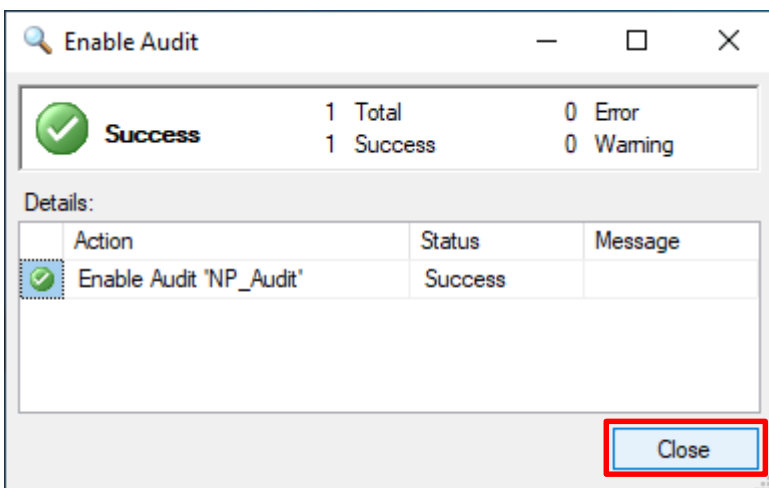
Progress: Ready

OK Cancel Help

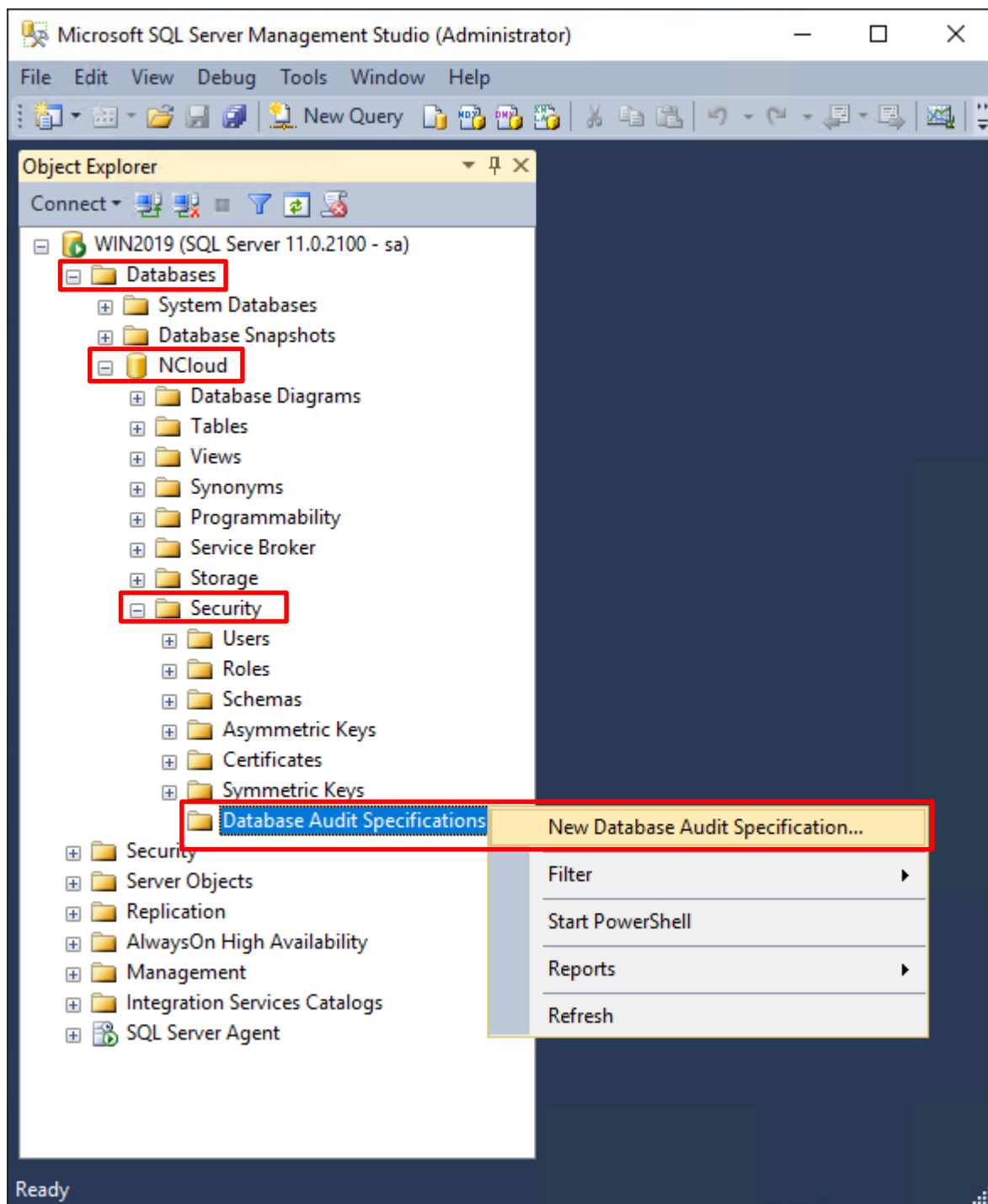
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



按下 **Close(關閉)**



選擇 **Databases(資料庫)**, **DB(NCloud)**, **Security(安全性)** -> 在 **Database Audit Specifications(資料庫稽核規格)** 上  
按滑鼠右鍵 -> 點選 **New Database Audit Specification(新增資料庫稽核規格)...**



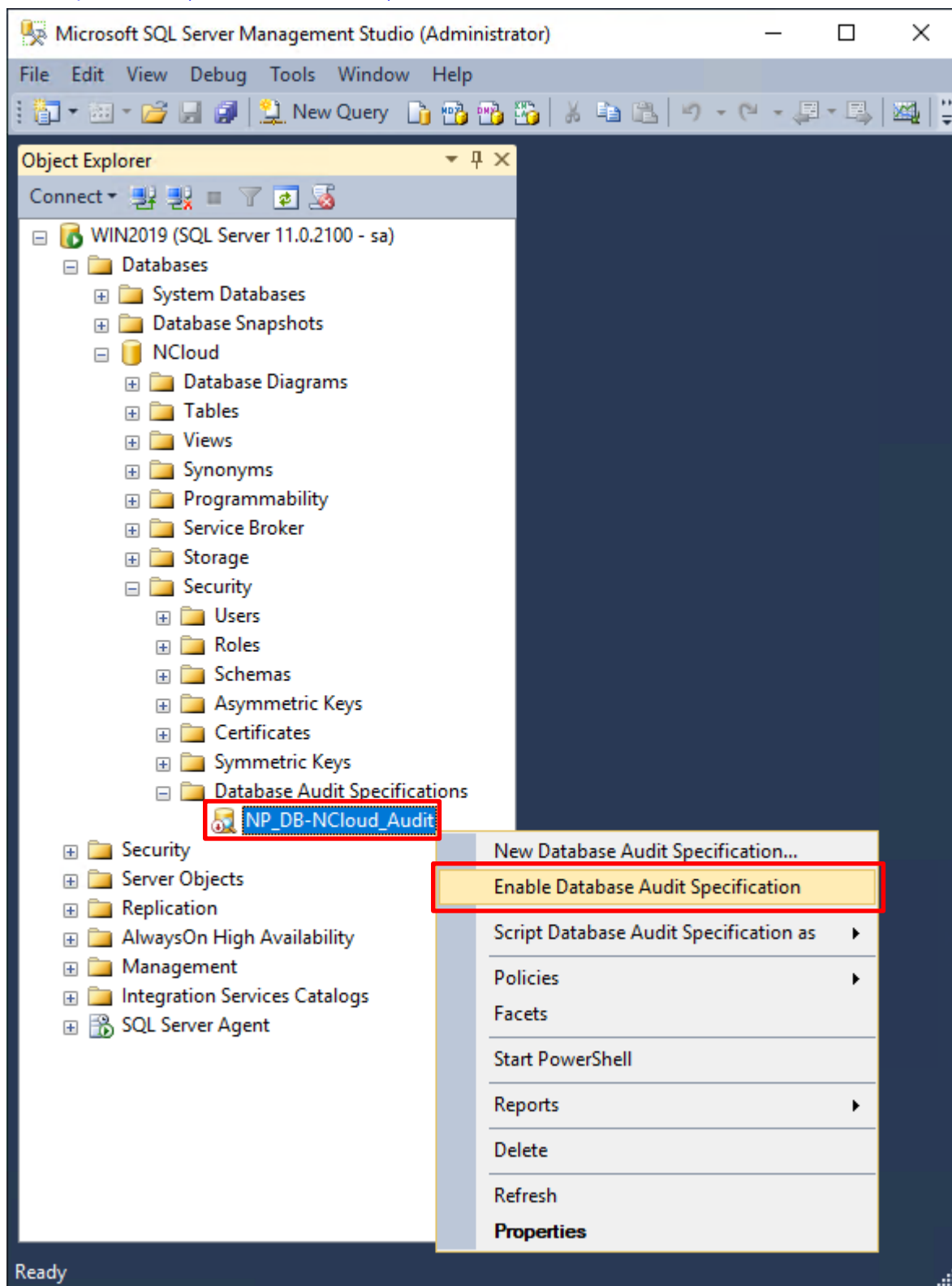
輸入 **Name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 選擇 **Audit**(稽核名稱): **NP\_Audit** 和 **Actions**(動作):  
範例簡易條列 · 詳細說明請參考前言的[稽核動作群組連結](#) -> 按下 **OK**(確定)

The screenshot shows the 'Create Database Audit Specification' dialog box. The 'Name' field is 'NP\_DB-NCloud\_Audit' and the 'Audit' dropdown is 'NP\_Audit'. The 'Actions' table is as follows:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
2	BACKUP_RESTORE_GROUP				
3	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
4	FAILED_DATABASE_AUTHENTICATION_GROUP				
5	SCHEMA_OBJECT_CHANGE_GROUP				
6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP				
7					

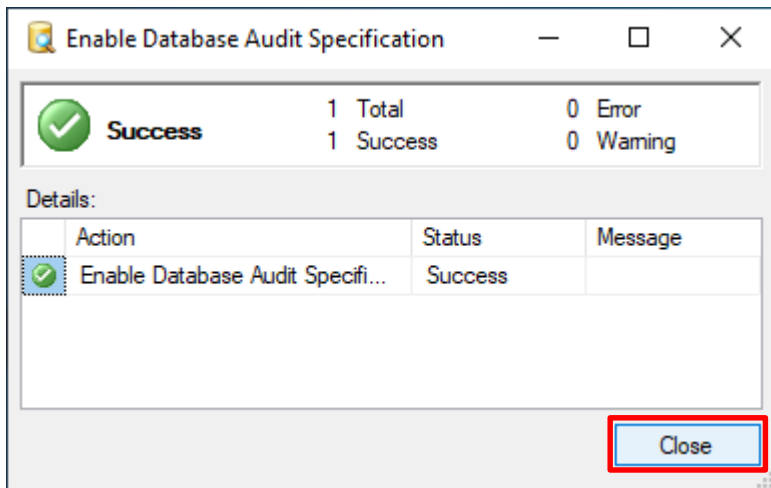
The 'OK' button is highlighted with a red box.

在 **Database Audit Specifications name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 點選 **Enable Database Audit Specification**(啟用資料庫稽核規格)





按下 **Close(關閉)**



## 5. SQL 2014

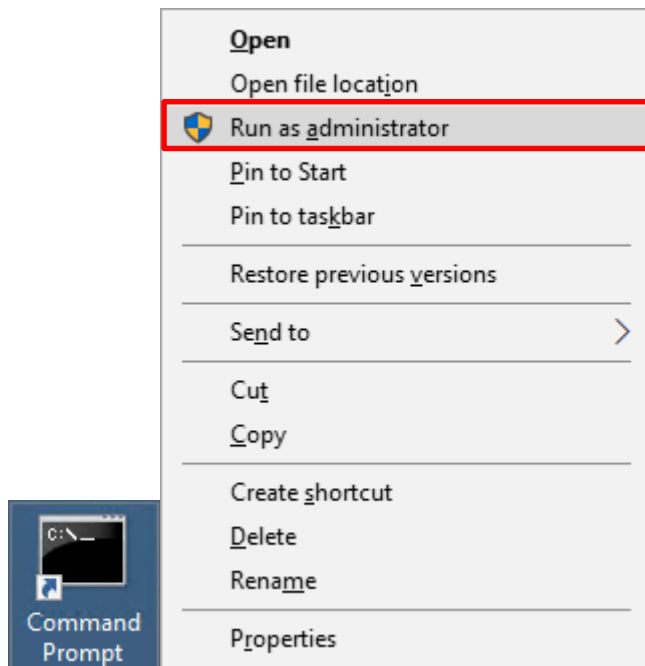
### 5.1 稽核登入

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，才會生效。

以下分別為指令介面和圖形介面設定方式。

#### 5.1.1 使用指令介面方式設定

在 **Command Prompt(命令提示字元)** 上按滑鼠右鍵 -> 點選 **Run as administrator(以系統管理員身分執行)**



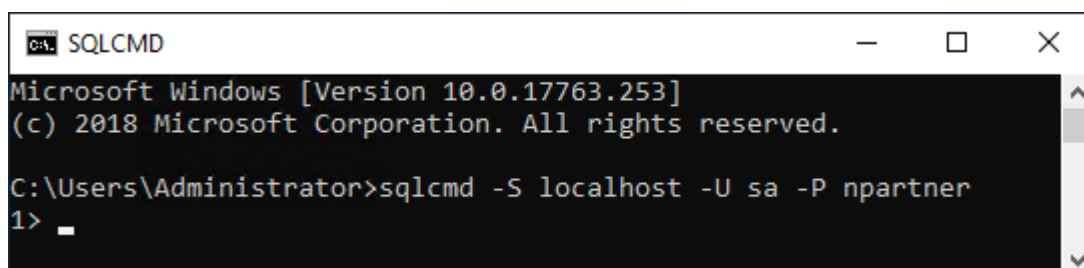
輸入 `sqlcmd -S localhost -U sa -P npartner`

#### Options:

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

**-U** login\_id

**-P** password



輸入 `use master -> go`

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

使用 `sp_configure` 列出進階選項

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

```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

啟用通用條件合規性

輸入 `exec sp_configure 'common criteria compliance enabled', 1 -> go -> reconfigure with override -> go`

```
SQLCMD
1> exec sp_configure 'common criteria compliance enabled', 1
2> go
Configuration option 'common criteria compliance enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure with override
2> go
1> _
```

啟用失敗和成功的登入記錄

輸入 `EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',`

`N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 -> go -> quit`

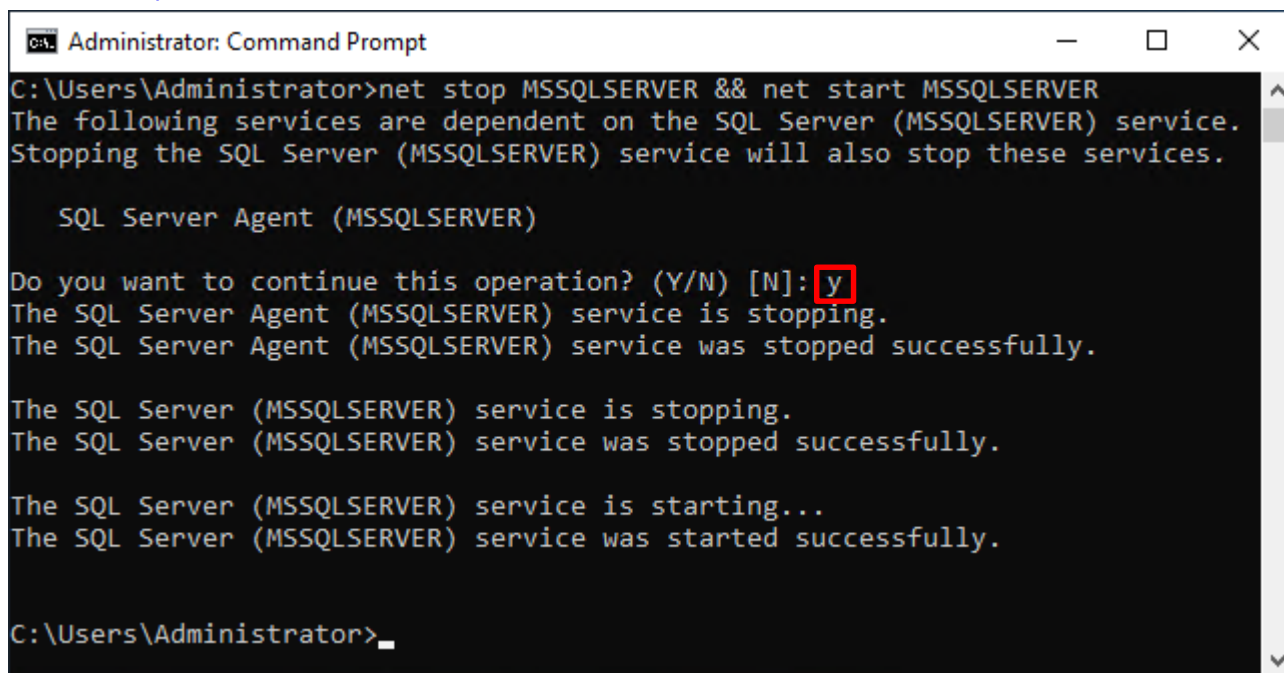
```
Administrator: Command Prompt
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit

C:\Users\Administrator>_
```

重新啟動 MSSQLSERVER 服務

輸入 `net stop MSSQLSERVER && net start MSSQLSERVER`



```
Administrator: Command Prompt
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSERVER
The following services are dependent on the SQL Server (MSSQLSERVER) service.
Stopping the SQL Server (MSSQLSERVER) service will also stop these services.

    SQL Server Agent (MSSQLSERVER)

Do you want to continue this operation? (Y/N) [N]: y
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is starting...
The SQL Server (MSSQLSERVER) service was started successfully.

C:\Users\Administrator>
```

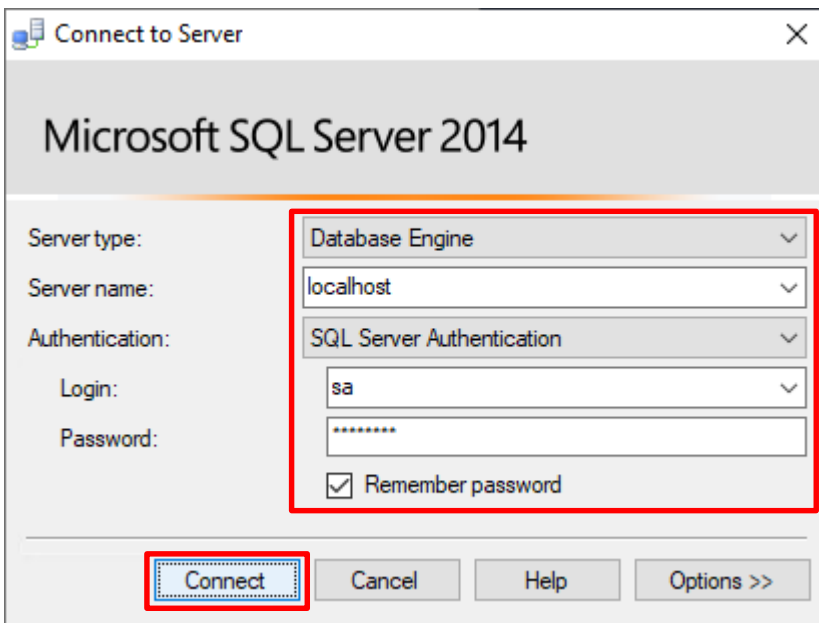
## 5.1.2 使用圖形介面方式設定

開啟 [Microsoft SQL Server Management Studio](#)

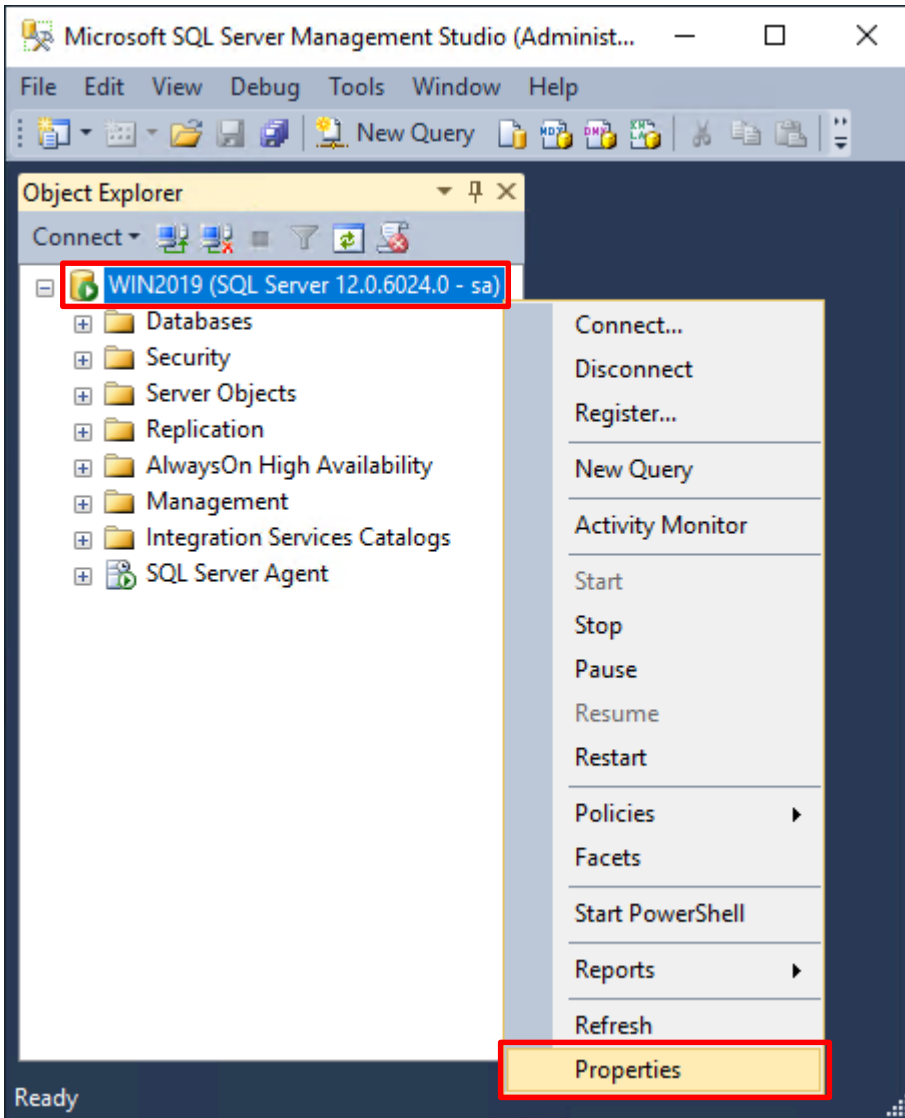


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

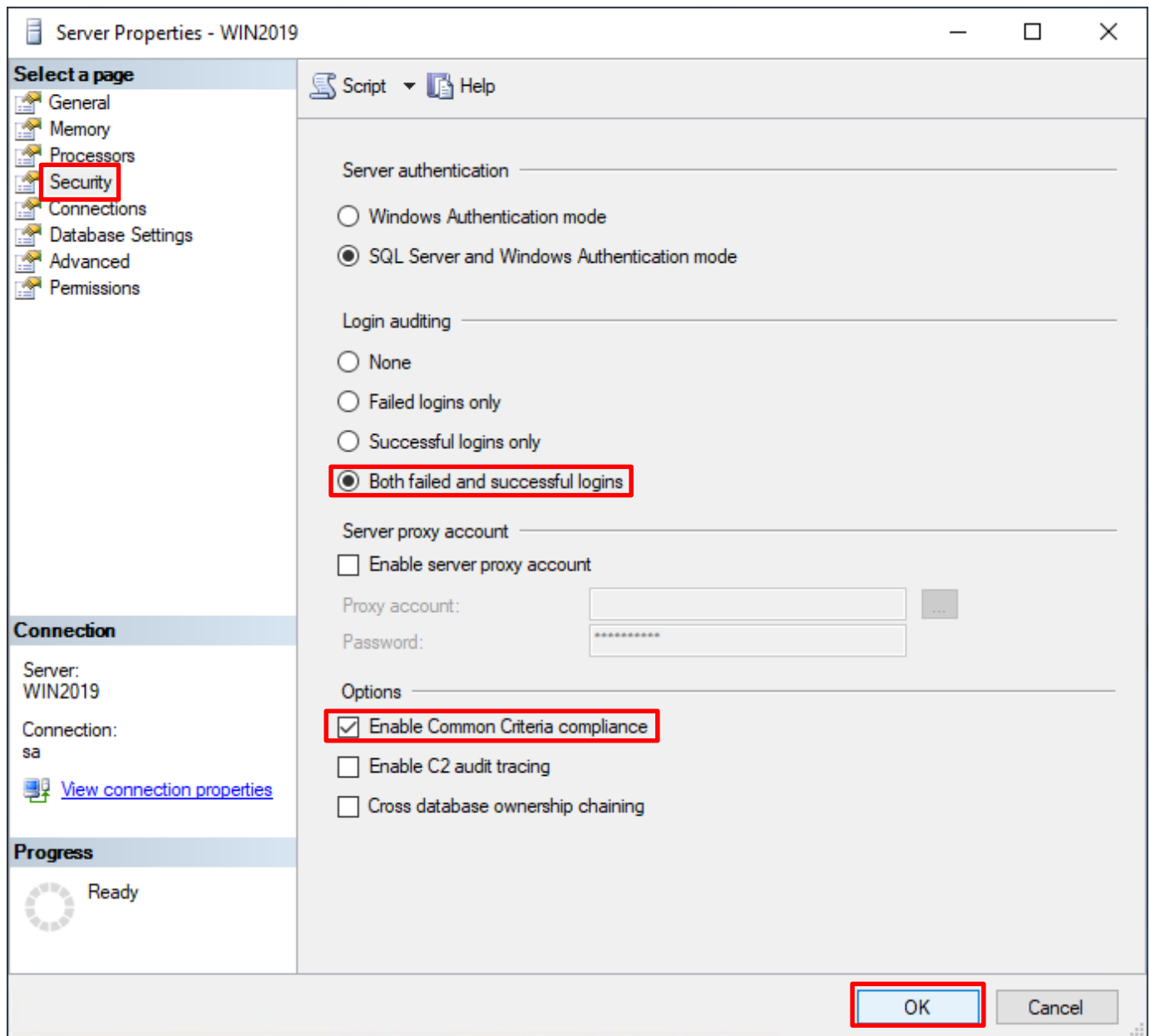
**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



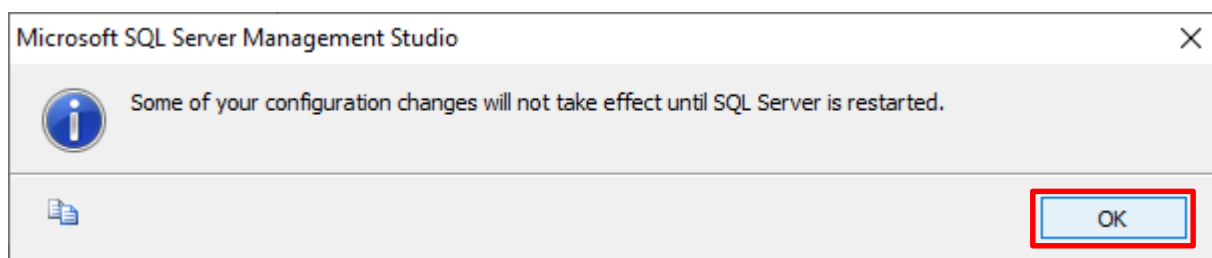
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Properties(屬性)**



選擇 **Security(安全性)** 頁面 -> **Login auditing(登入稽核)**: 點選 **Both failed and successful logins(失敗和成功的登入)** -> **Options(選項)**: 勾選 **Enable Common Criteria compliance(啟用通用條件合規性)** -> 按下 **OK(確定)**

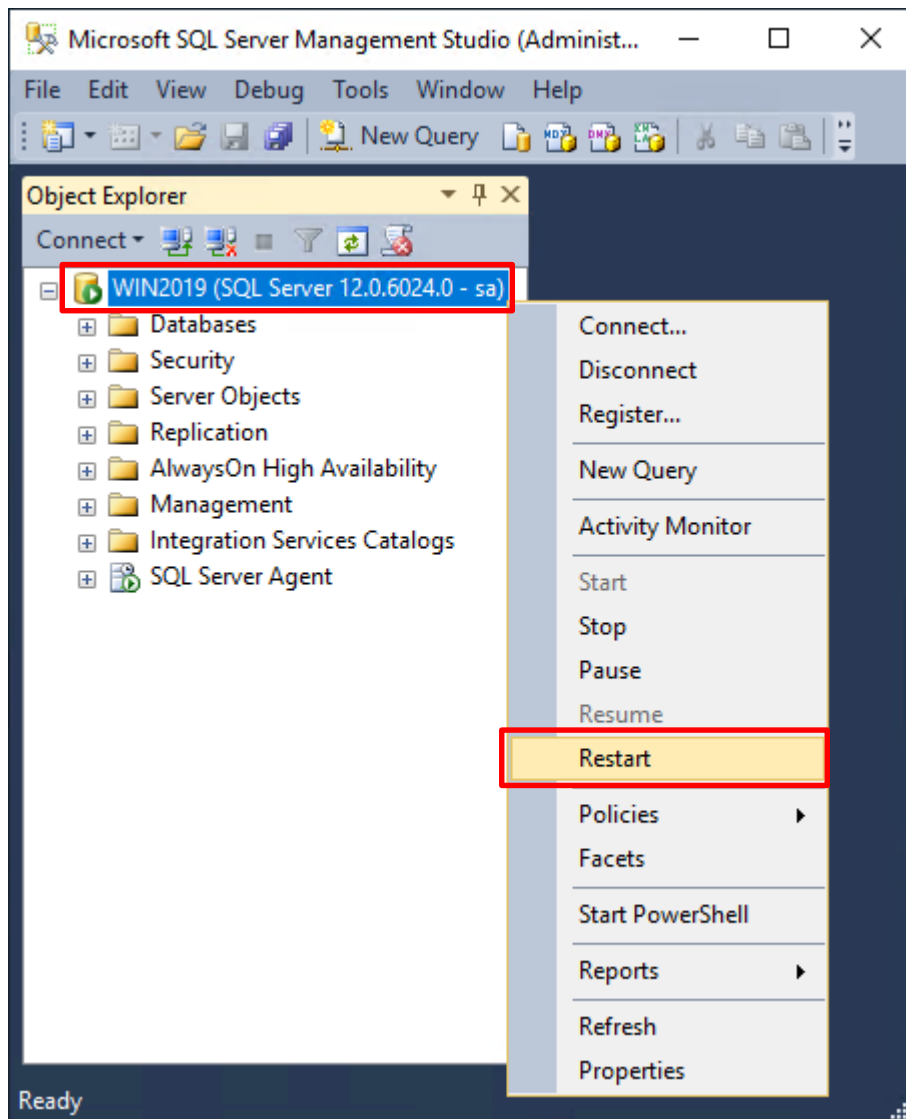


按下 **OK(確定)**

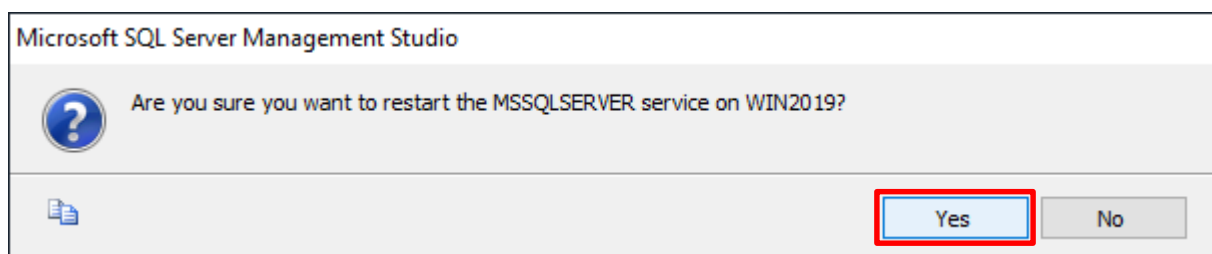


重新啟動 MSSQLSERVER 服務

在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Restart(重新啟動)**

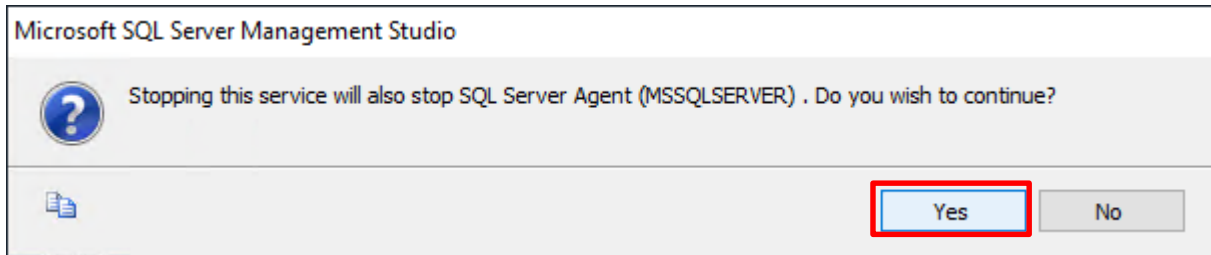


按下 **Yes(是)** 重新啟動 MSSQLSERVER 服務





按下 **Yes(是)** 停止 SQLSERVER Agent



## 5.2 稽核伺服器層級

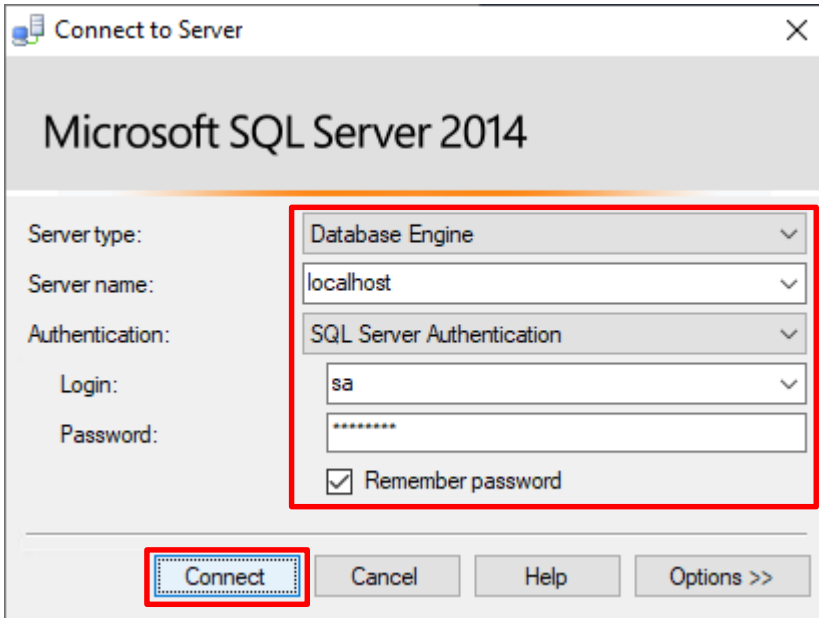
啟用稽核伺服器層級包含伺服器作業，例如管理變更及登入和登出作業。

開啟 [Microsoft SQL Server Management Studio](#)

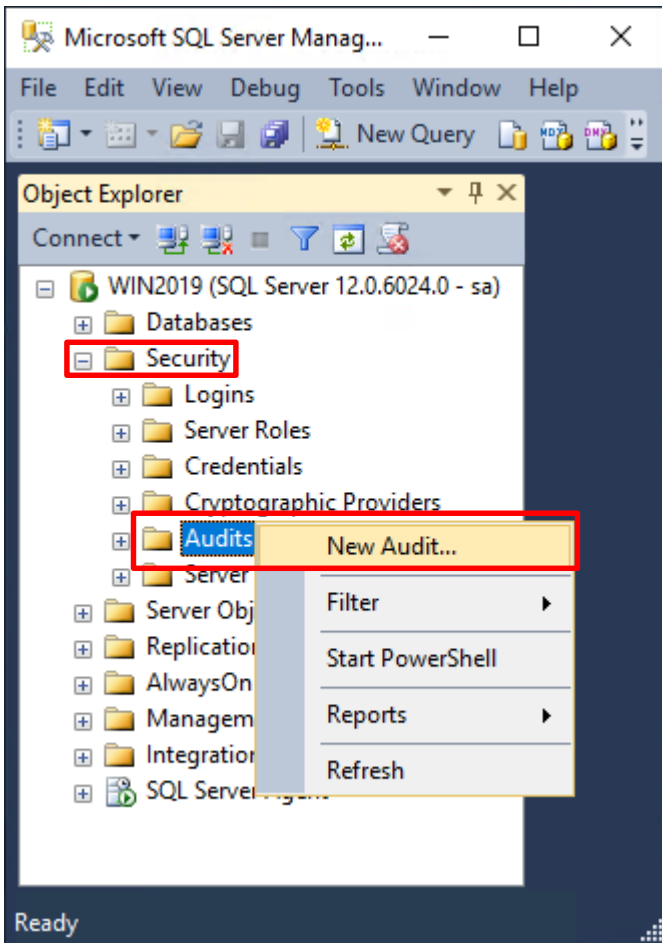


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** & **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- Continue
- Shut down server
- Fail operation

Audit destination: Application Log

File path: [Empty]

Audit File Maximum Limit:

- Maximum rollover files:
  - Unlimited
- Maximum files:
  - Number of files: 2147483647

Maximum file size: 0 MB GB TB

- Unlimited

Reserve disk space

Connection

- WIN2019 [sa]

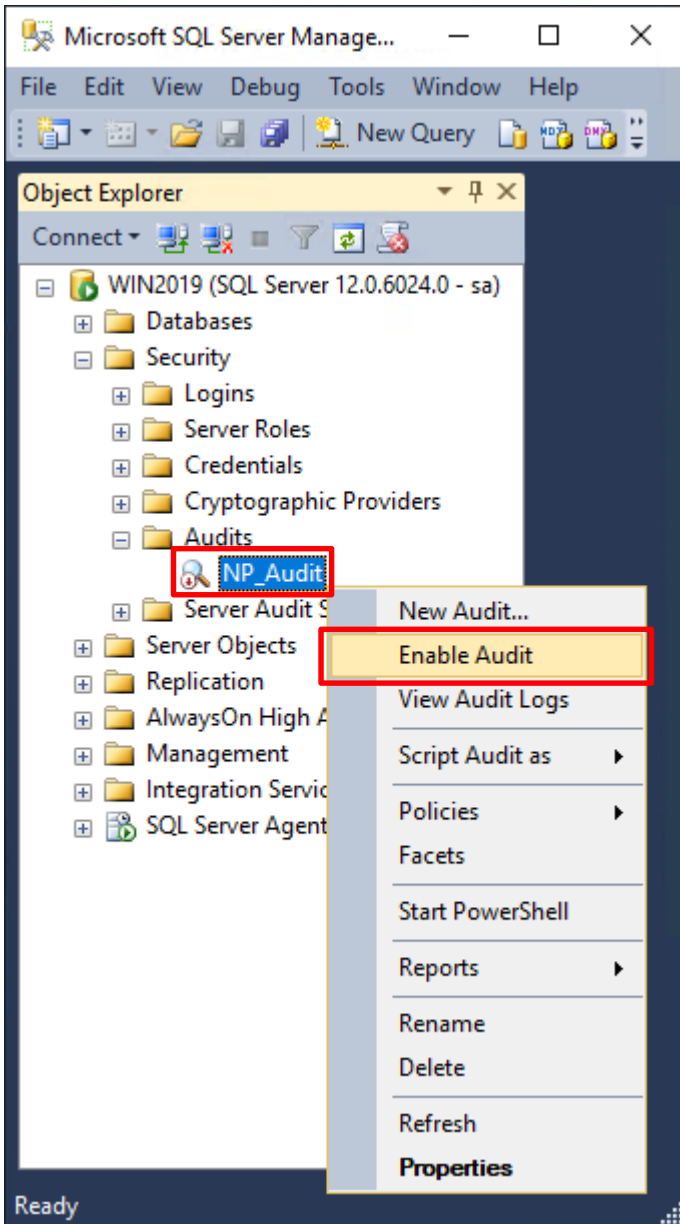
[View connection properties](#)

Progress

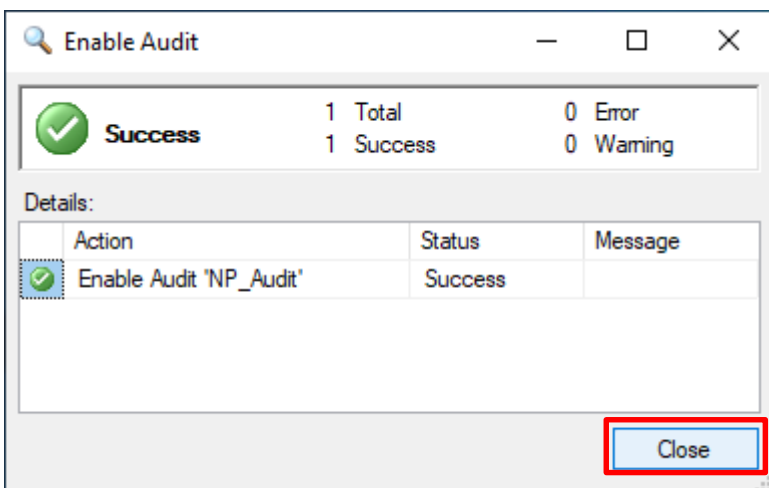
Ready

OK Cancel Help

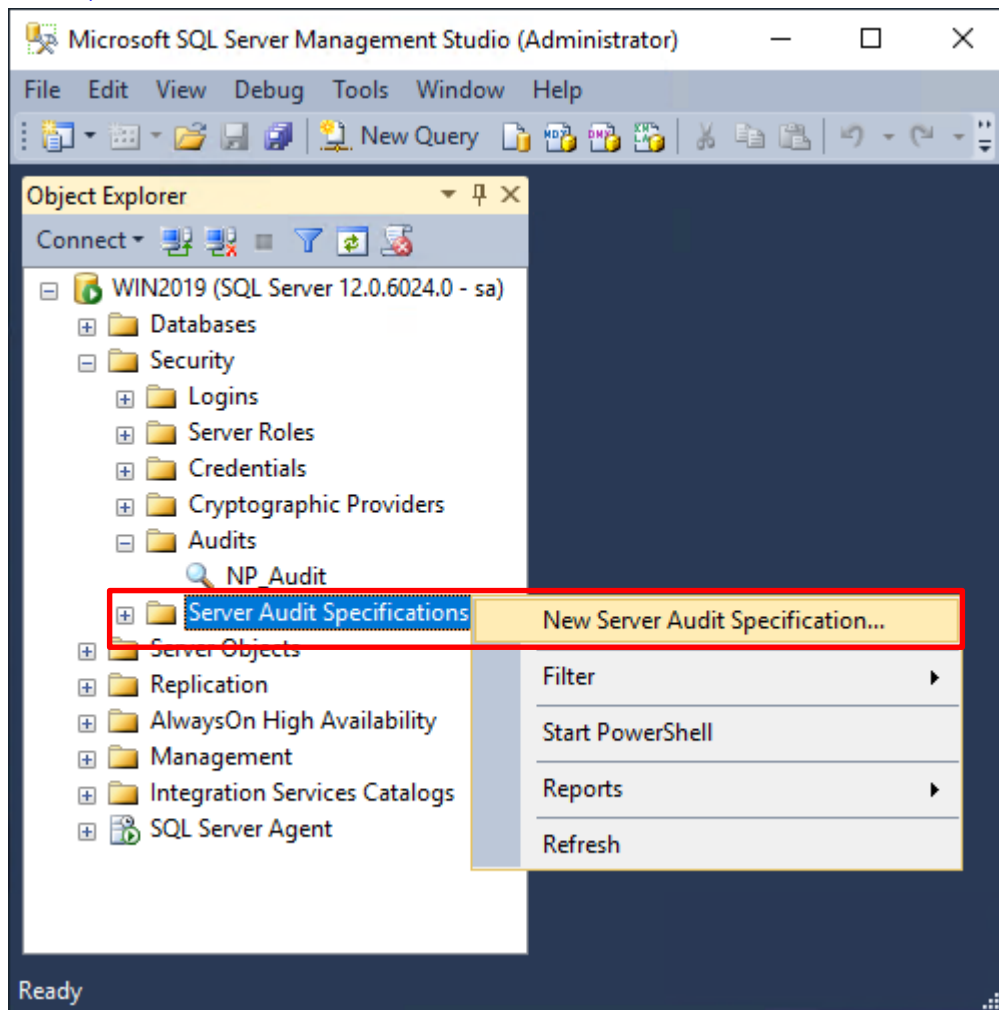
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



按下 **Close(關閉)**



在 **Server Audit Specifications**(伺服器稽核規格) 按滑鼠右鍵 -> 點選 **New Server Audit Specification**(新增伺服器稽核規格)...



輸入 **Name(伺服器稽核規格名稱): NP\_Server\_Audit** -> 選擇 **Audit(稽核): NP\_Audit** 和 **Actions(動作): 範例簡易條列** · 詳細說明請參考前言的稽核動作群組連結 -> 按下 **OK(確定)**

Ready

Select a page

General

Script Help

Name: NP\_Server\_Audit

Audit: NP\_Audit

Actions:

	Audit Action Type	Object Class	Object	Object Name	Principal
01	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
02	SERVER_ROLE_MEMBER_CHANGE_GROUP				
03	DATABASE_LOGOUT_GROUP				
04	DATABASE_PERMISSION_CHANGE_GROUP				
05	DATABASE_CHANGE_GROUP				
06	DATABASE_PRINCIPAL_CHANGE_GROUP				
07	SERVER_PRINCIPAL_CHANGE_GROUP				
08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
09	LOGIN_CHANGE_PASSWORD_GROUP				
10	DATABASE_OWNERSHIP_CHANGE_GROUP				
▶ 11	USER_CHANGE_PASSWORD_GROUP				
* 12					

Connection

WIN2019 [sa]

[View connection properties](#)

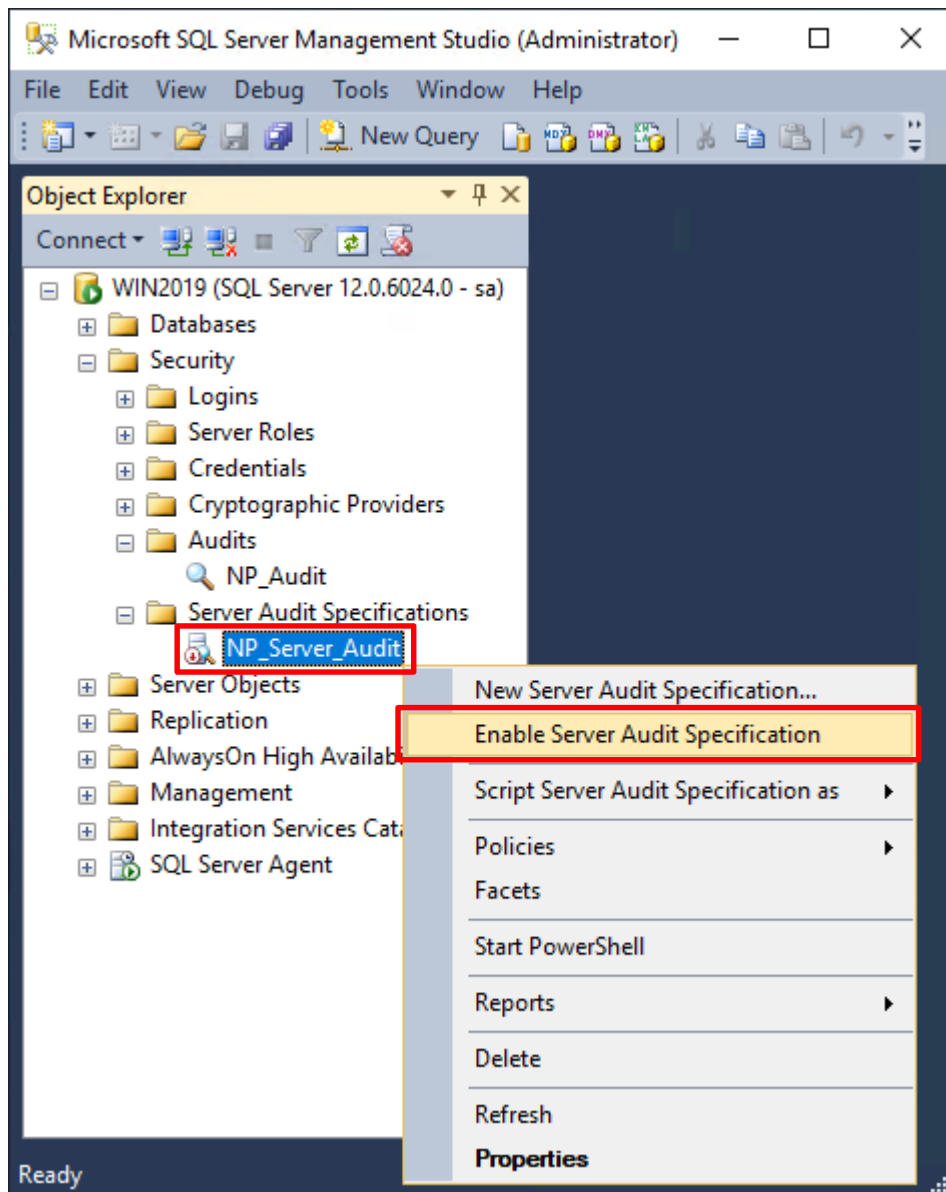
Progress

Ready

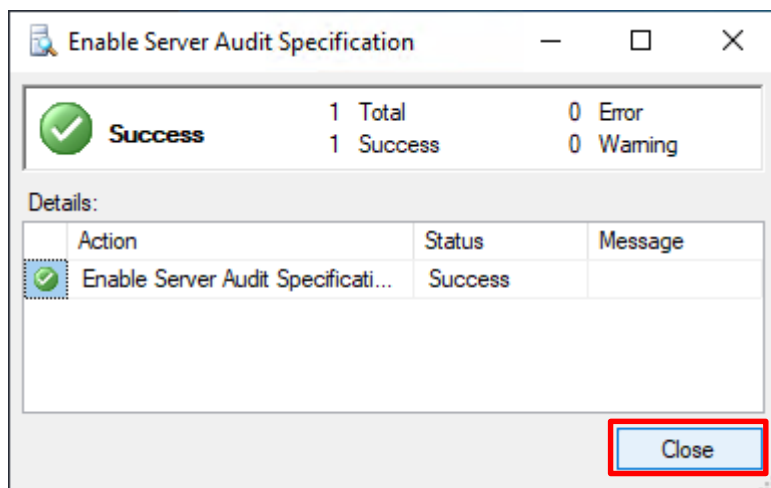
OK Cancel Help

在 **Server Audit Specifications name**(伺服器稽核規格名稱): **NP\_Server\_Audit** 按滑鼠右鍵 -> 點選 **Enable**

**Server Audit Specification**(啟用伺服器稽核規格)



按下 **Close**(關閉)





## 5.3 稽核資料庫層級

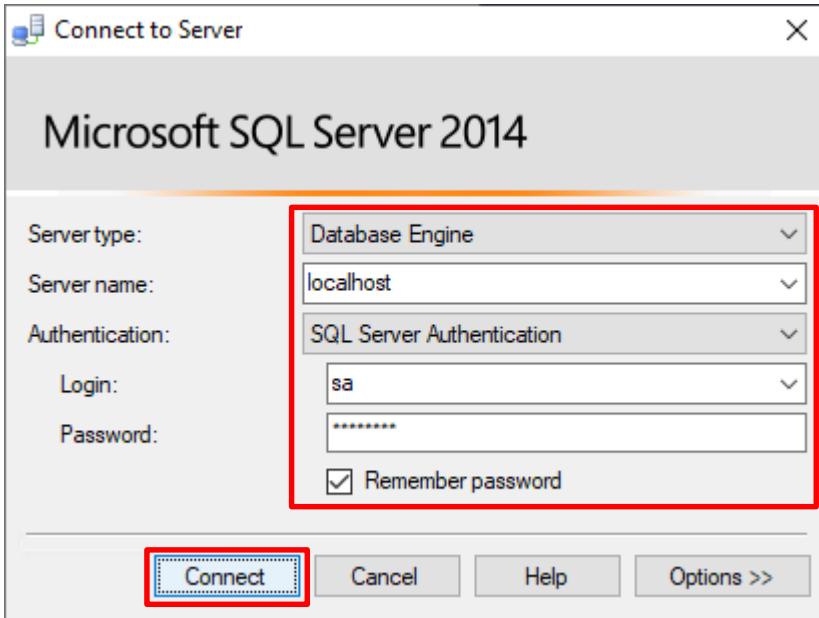
啟用稽核資料庫層級包括資料操作語言 (DML) 及資料定義語言 (DDL) 作業。

開啟 [Microsoft SQL Server Management Studio](#)

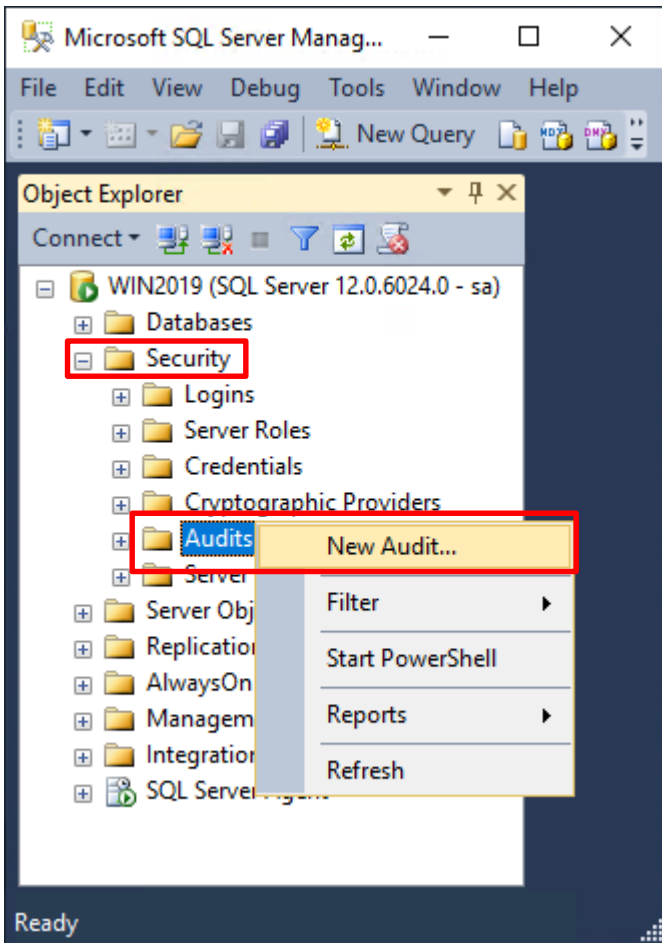


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**



選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:  Continue

Shut down server

Fail operation

Audit destination: Application Log

File path: [Empty]

Audit File Maximum Limit:

- Maximum rollover files:  Unlimited
- Maximum files: Number of files: 2147483647

Maximum file size: 0  MB  GB  TB

Unlimited

Reserve disk space

Connection

- WIN2019 [sa]

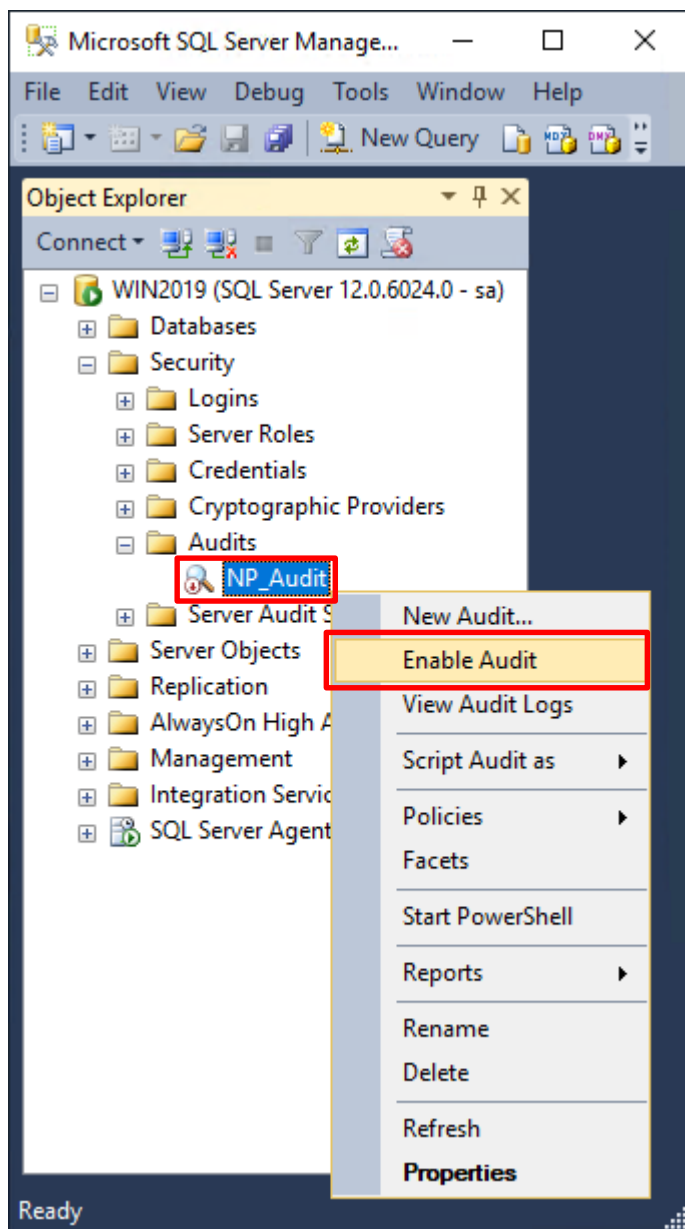
[View connection properties](#)

Progress

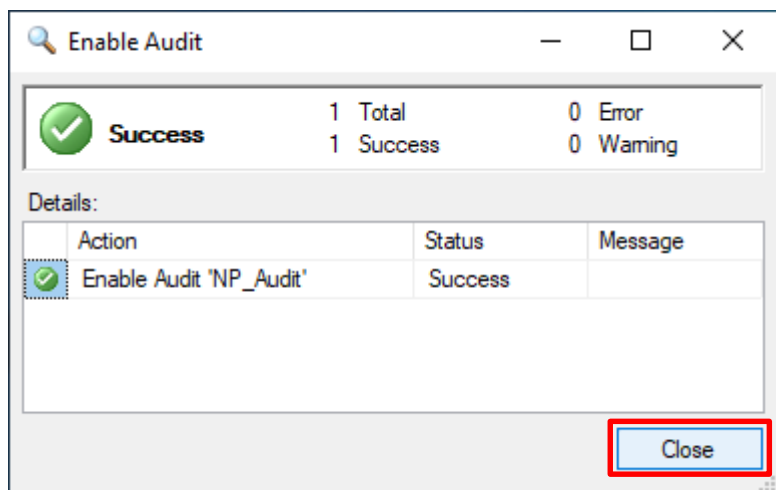
Ready

OK Cancel Help

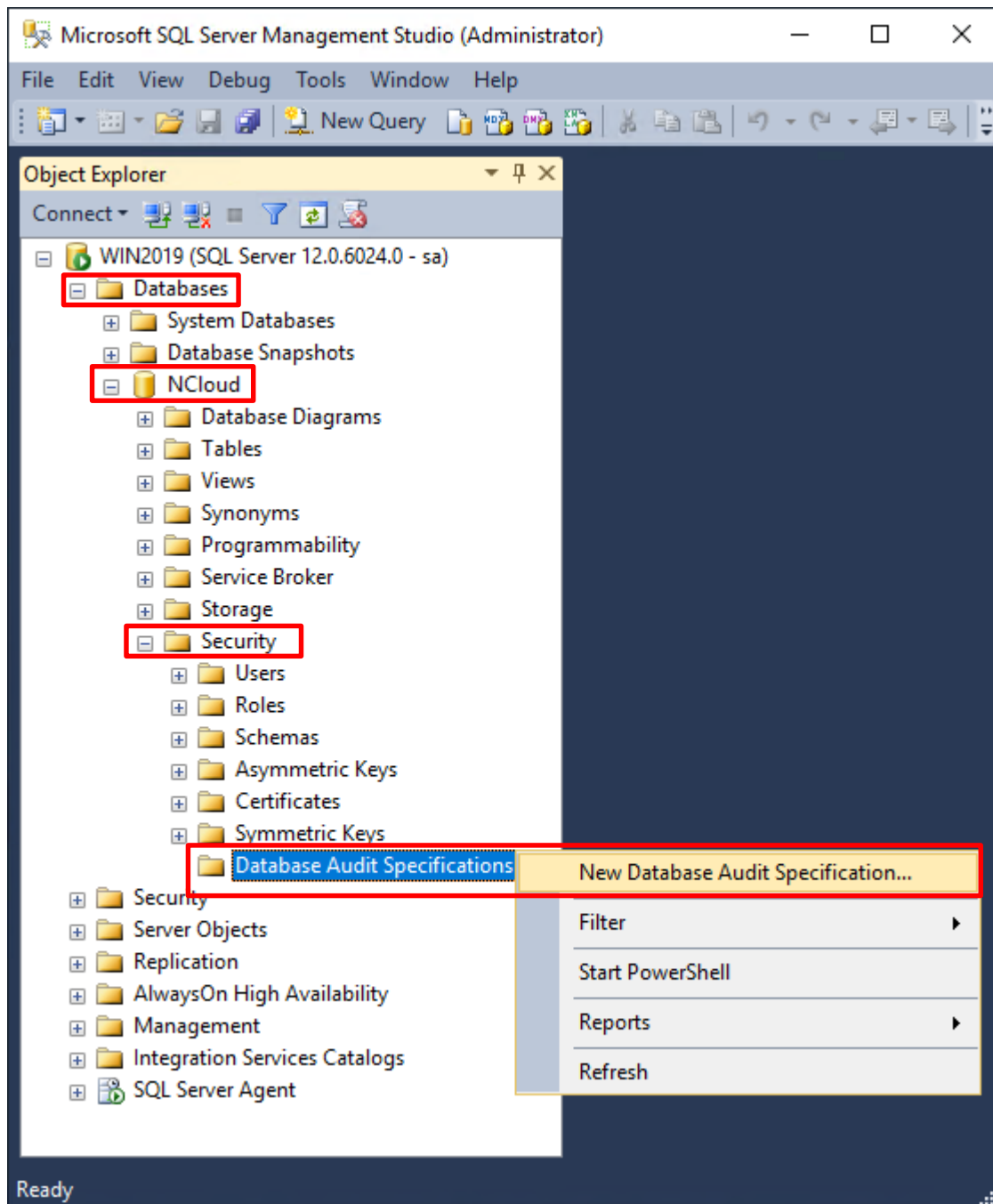
在 **Audits name(稽核名稱): NP\_Audit** 上按滑鼠右鍵 -> 點選 **Enable Audit(啟用稽核)**



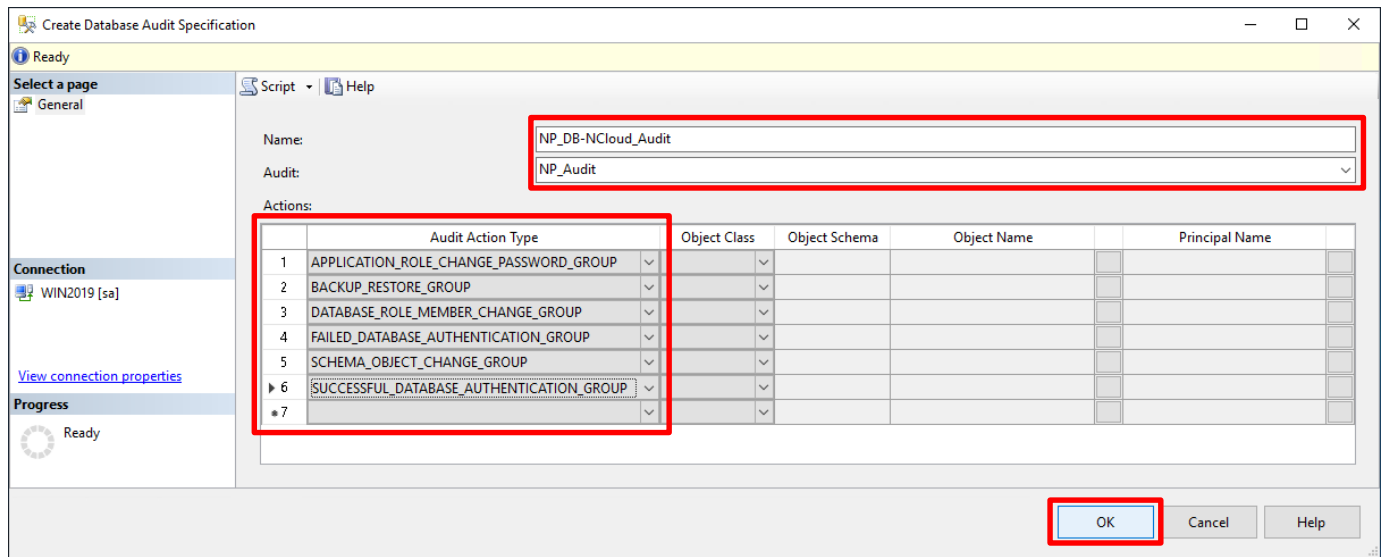
按下 **Close(關閉)**



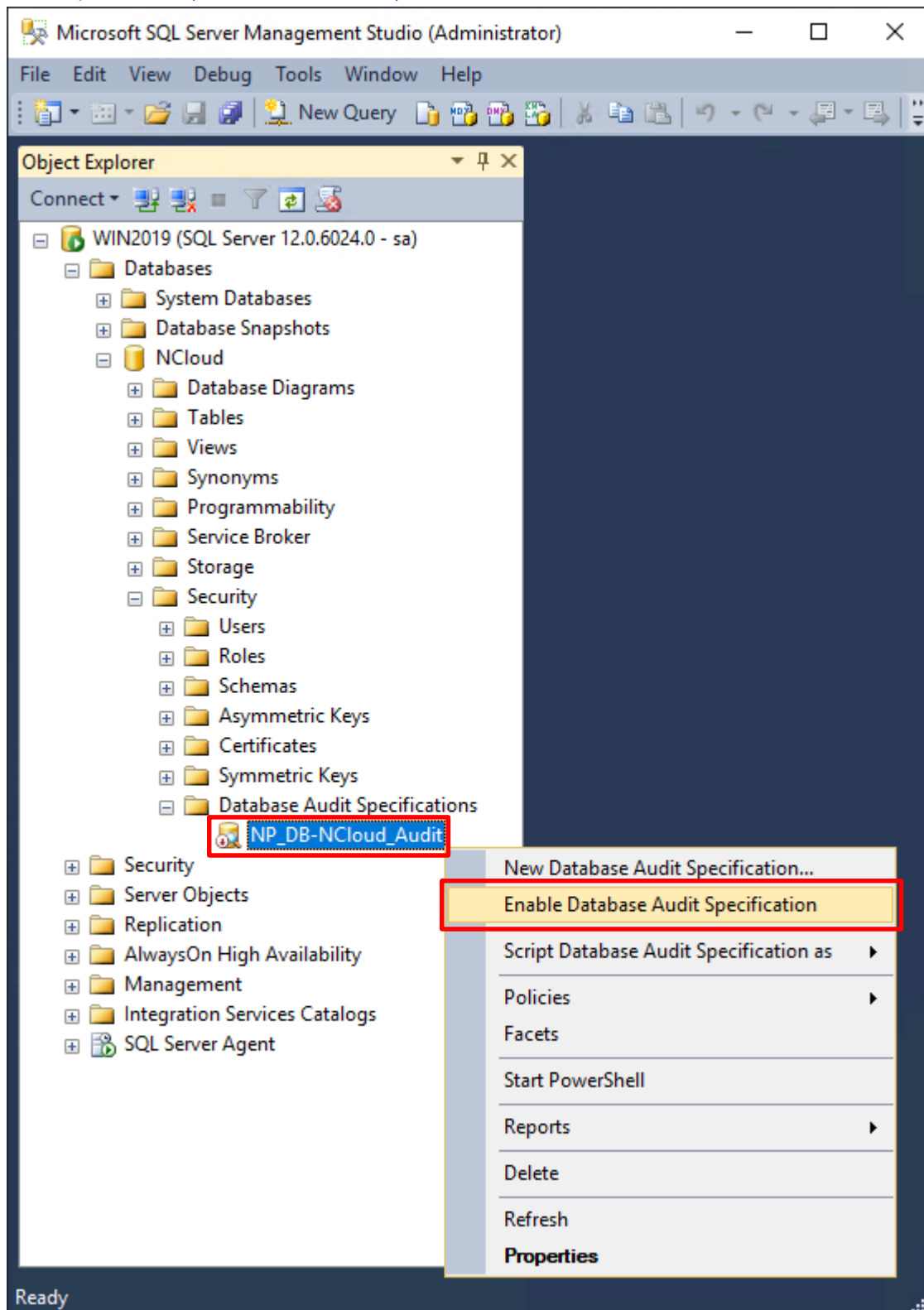
選擇 **Databases(資料庫)** -> **DB(NCloud)** -> **Security(安全性)** -> 在 **Database Audit Specifications(資料庫稽核規格)**  
上按滑鼠右鍵 -> 點選 **New Database Audit Specification(新增資料庫稽核規格)...**



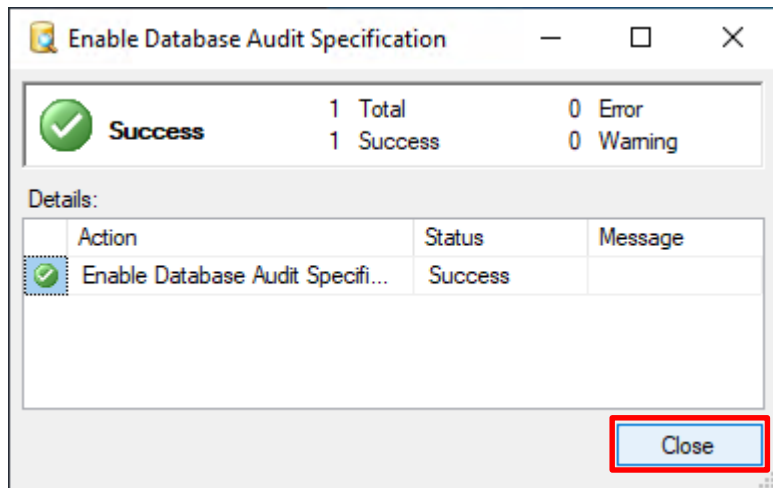
輸入 **Name**(資料庫稽核規格名稱): *NP\_DB-NCloud\_Audit* -> 選擇 **Audit**(稽核名稱): *NP\_Audit* 和 **Actions**(動作):  
範例簡易條列 · 詳細說明請參考前文的[稽核動作群組連結](#) -> 按下 **OK**(確定)



在 **Database Audit Specifications name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 點選 **Enable Database Audit Specification**(啟用資料庫稽核規格)



按下 **Close(關閉)**





## 6. SQL 2016

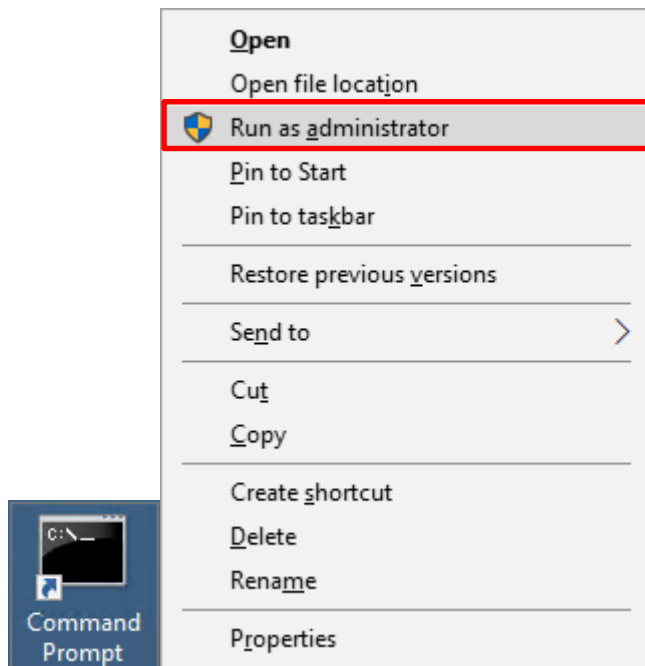
### 6.1 稽核登入

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，才會生效。

以下分別為指令介面和圖形介面設定方式。

#### 6.1.1 使用指令介面方式設定

在 **Command Prompt(命令提示字元)** 上按滑鼠右鍵 -> 點選 **Run as administrator(以系統管理員身分執行)**



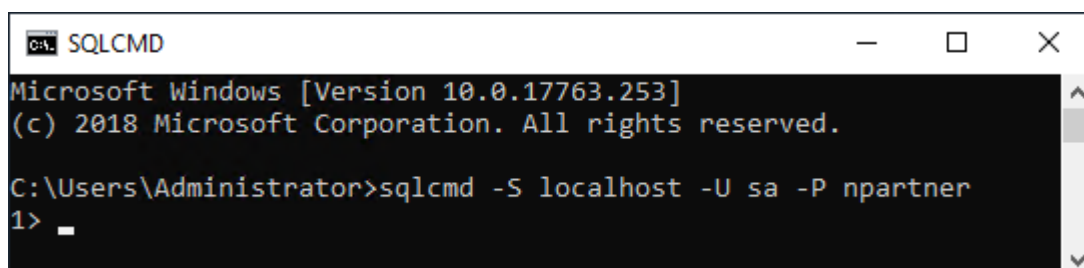
輸入 `sqlcmd -S localhost -U sa -P npartner`

#### Options:

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

**-U** login\_id

**-P** password



```
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sqlcmd -S localhost -U sa -P npartner
1> _
```

輸入 `use master -> go`

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

使用 `sp_configure` 列出進階選項

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

```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

啟用通用條件合規性

輸入 `exec sp_configure 'common criteria compliance enabled', 1 -> go -> reconfigure with override -> go`

```
SQLCMD
1> exec sp_configure 'common criteria compliance enabled', 1
2> go
Configuration option 'common criteria compliance enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure with override
2> go
1> _
```

啟用失敗和成功的登入記錄

輸入 `EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',`

`N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 -> go -> quit`

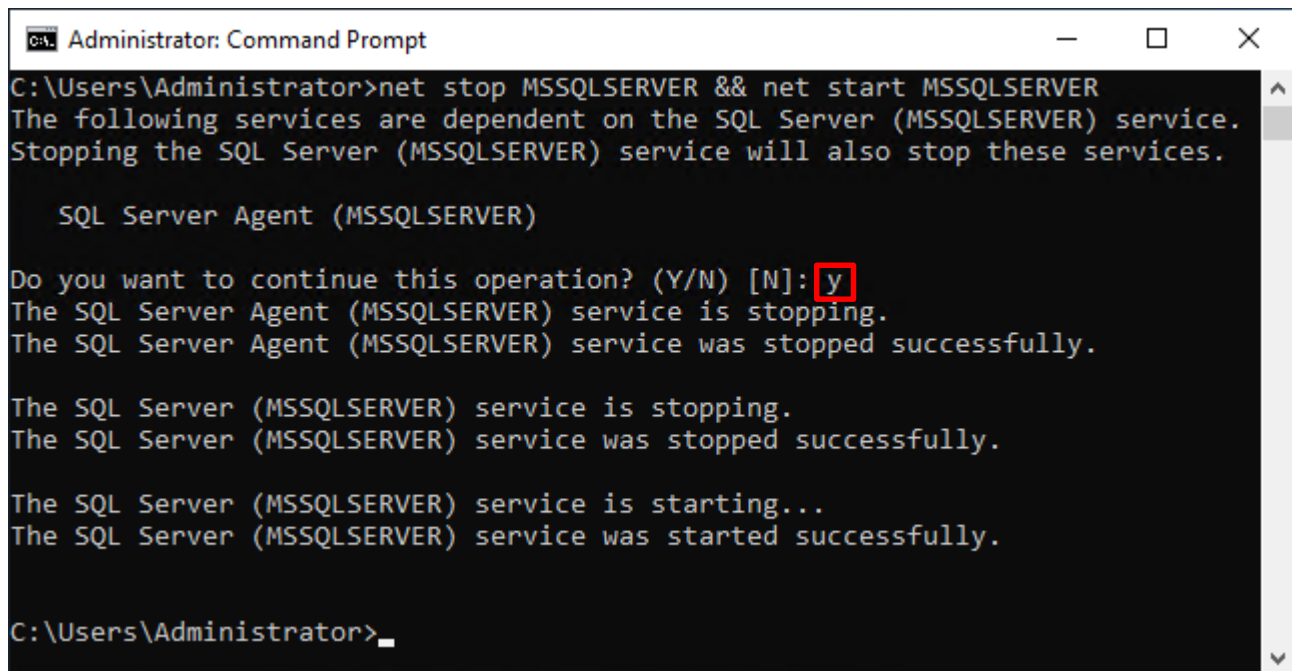
```
Administrator: Command Prompt
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit

C:\Users\Administrator>_
```

重新啟動 MSSQLSERVER 服務

輸入 `net stop MSSQLSERVER && net start MSSQLSERVER`



```
Administrator: Command Prompt
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSERVER
The following services are dependent on the SQL Server (MSSQLSERVER) service.
Stopping the SQL Server (MSSQLSERVER) service will also stop these services.

    SQL Server Agent (MSSQLSERVER)

Do you want to continue this operation? (Y/N) [N]: y
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is starting...
The SQL Server (MSSQLSERVER) service was started successfully.

C:\Users\Administrator>
```

## 6.1.2 使用圖形介面方式設定

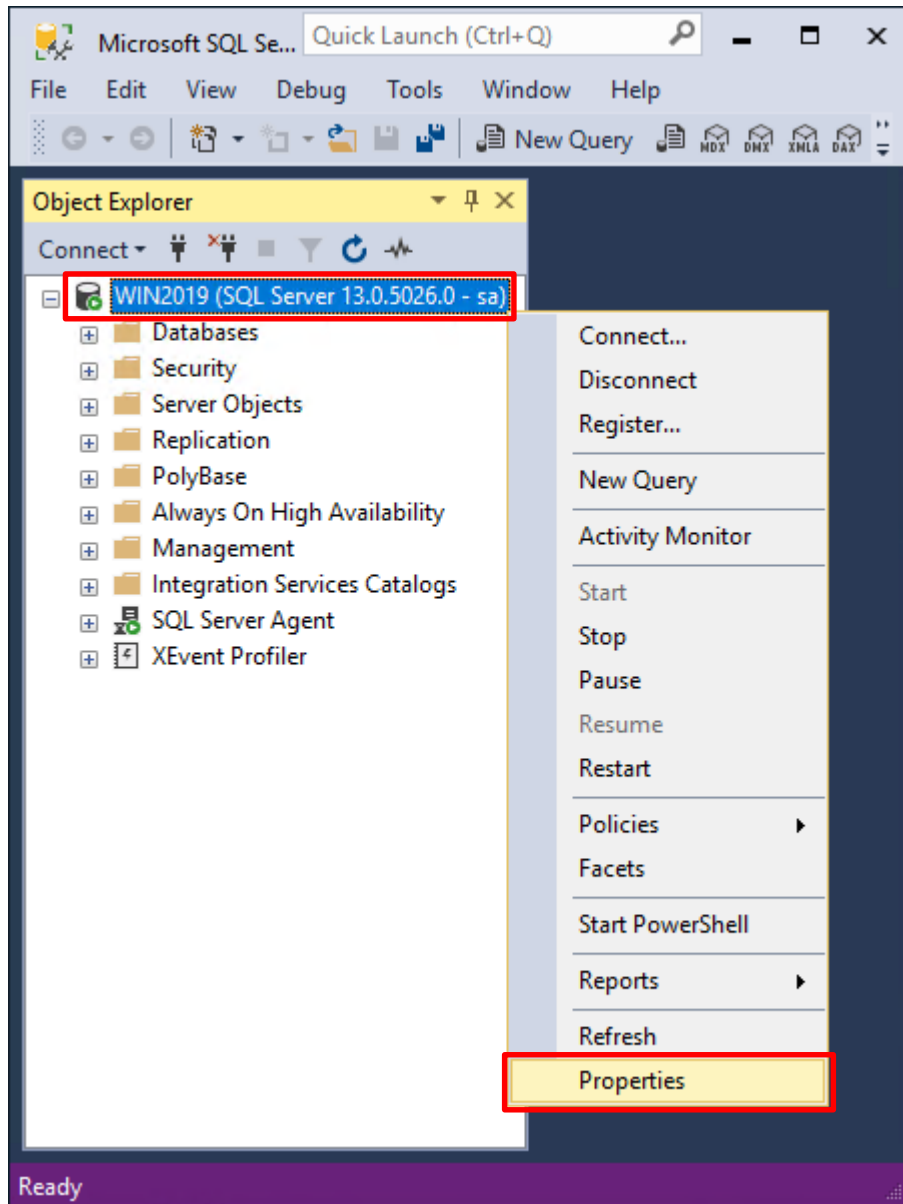
開啟 [Microsoft SQL Server Management Studio](#)



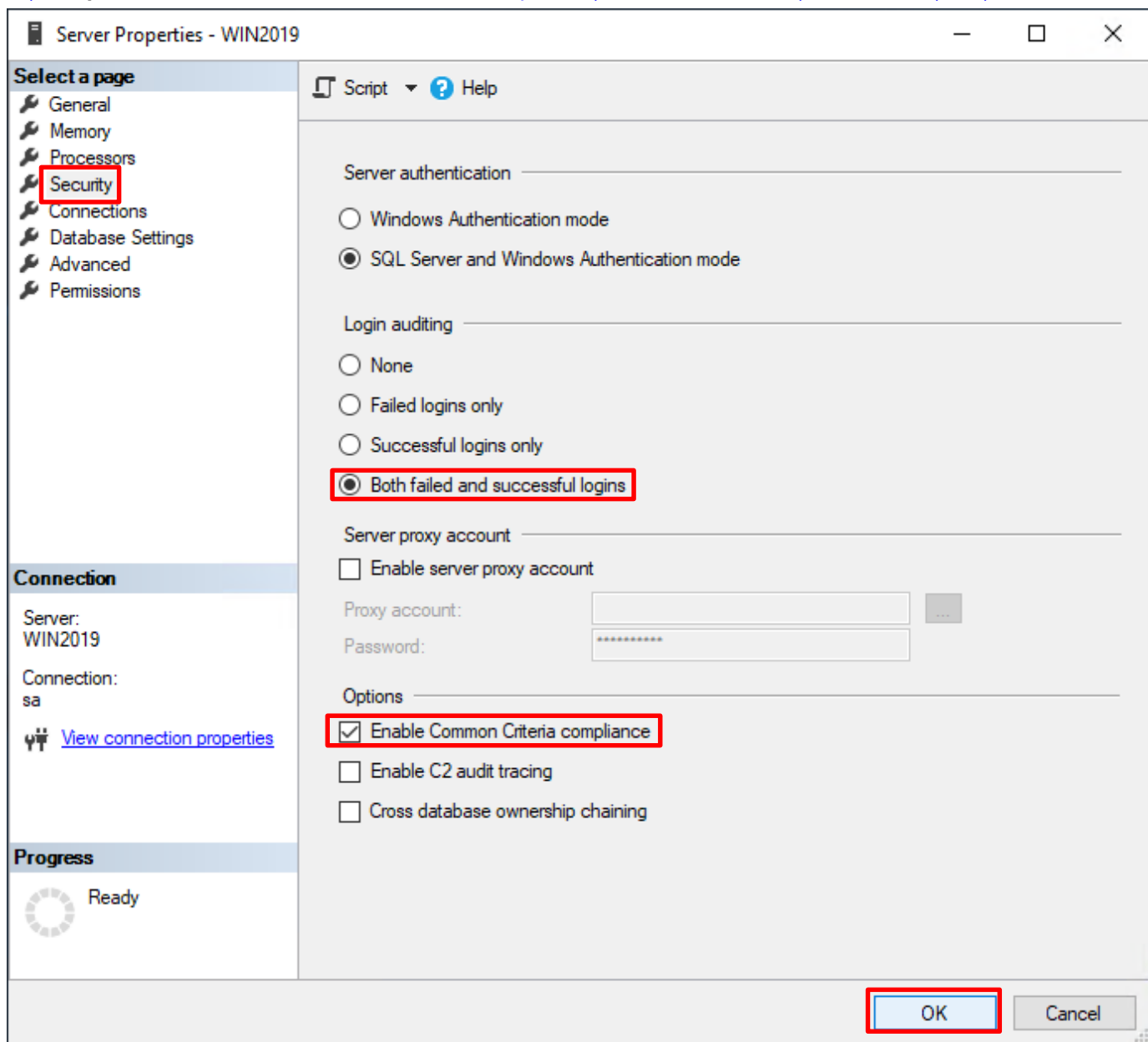
輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入 **Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

The screenshot shows the "Connect to Server" dialog box in SQL Server Management Studio. The title bar reads "Connect to Server" with a close button (X) on the right. The main heading is "SQL Server". The dialog contains several fields: "Server type:" with a dropdown menu set to "Database Engine"; "Server name:" with a dropdown menu set to "localhost"; "Authentication:" with a dropdown menu set to "SQL Server Authentication"; "Login:" with a dropdown menu set to "sa"; and "Password:" with a text box containing seven asterisks. Below the password field is a checked checkbox labeled "Remember password". At the bottom, there are four buttons: "Connect", "Cancel", "Help", and "Options >>". The "Connect" button is highlighted with a red dashed border, and the entire input area is enclosed in a solid red border.

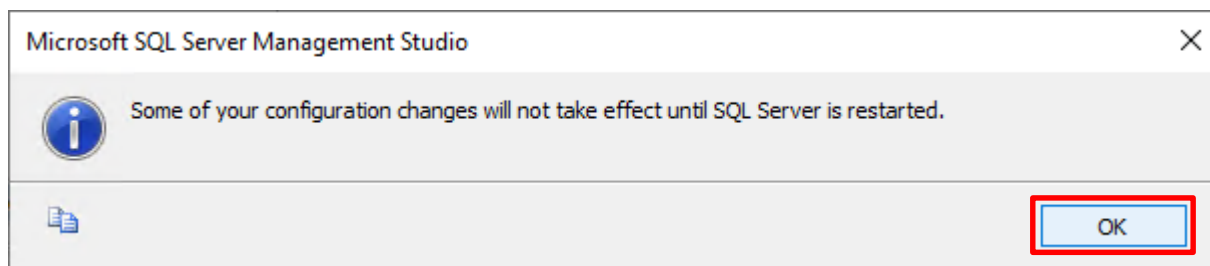
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Properties(屬性)**



選擇 **Security(安全性)** 頁面 -> **Login auditing(登入稽核)**: 點選 **Both failed and successful logins(失敗和成功的登入)** -> **Options**: 勾選 **Enable Common Criteria compliance(啟用通用條件合規性)** -> 按下 **OK(確定)**

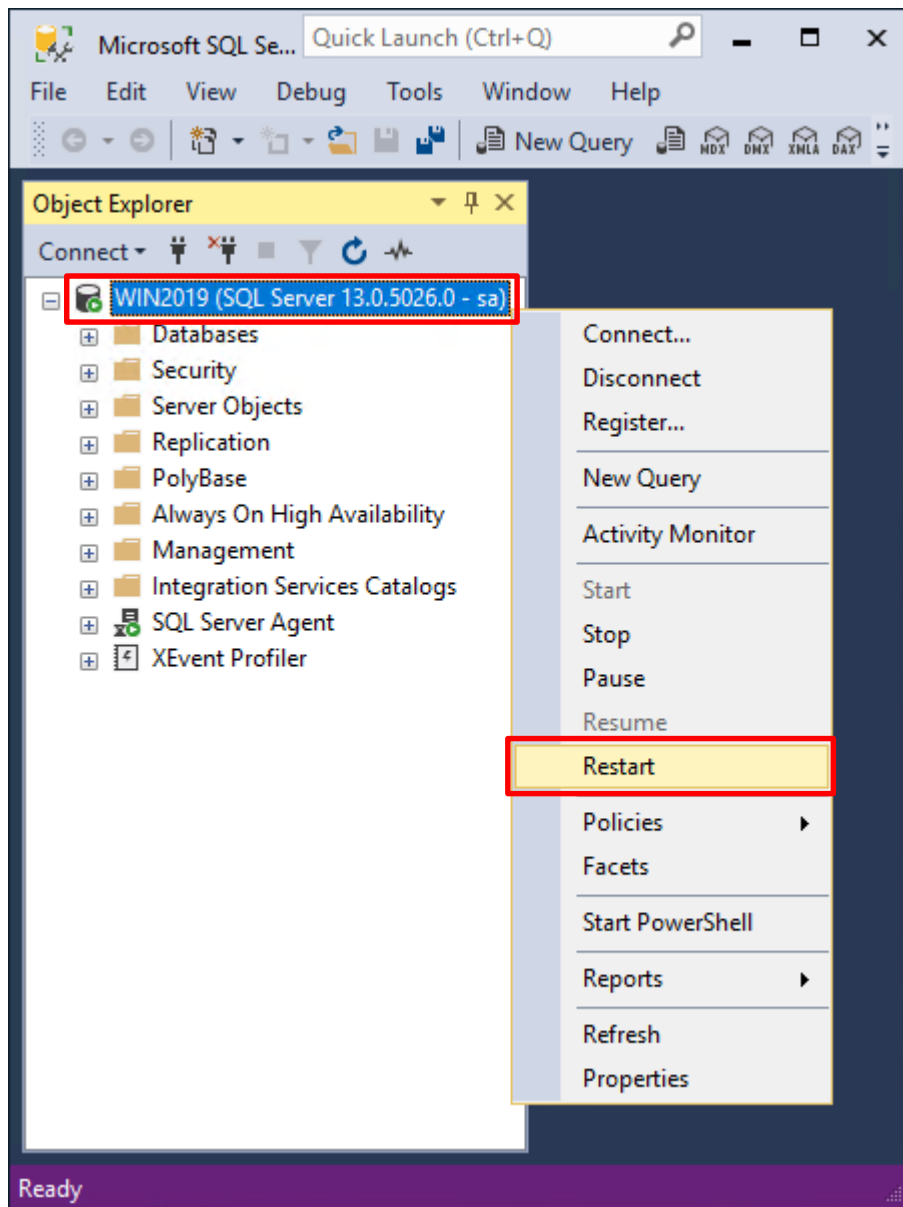


按下 **OK(確定)**

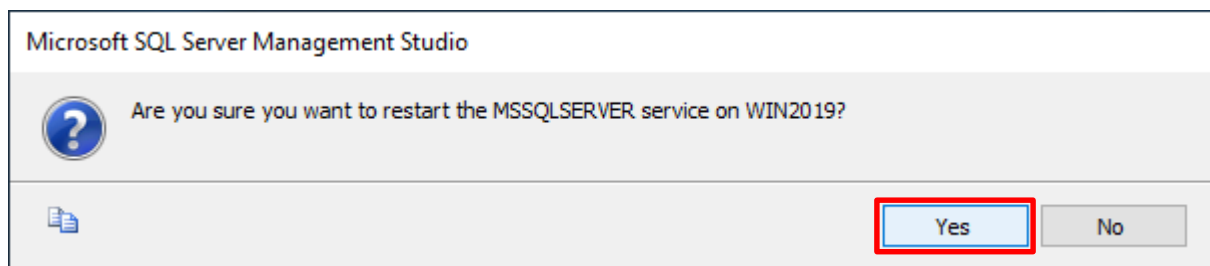


重新啟動 MSSQLSERVER 服務

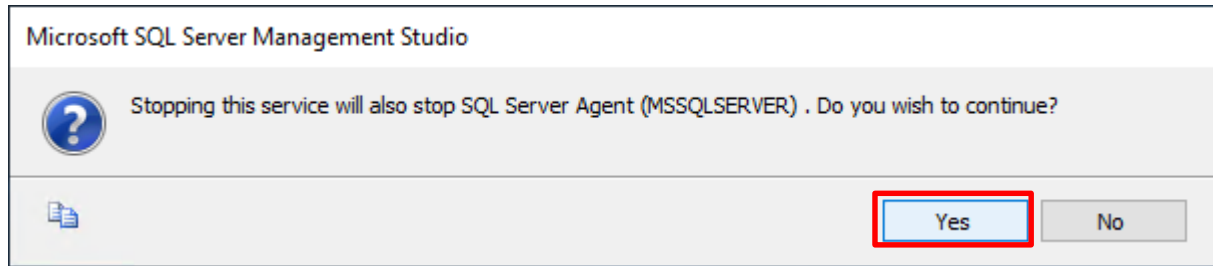
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Restart(重新啟動)**



按下 **Yes(是)** 重新啟動 MSSQLSERVER 服務



按下 **Yes(是)** 停止 SQLSERVER Agent





## 6.2 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。

開啟 [Microsoft SQL Server Management Studio](#)

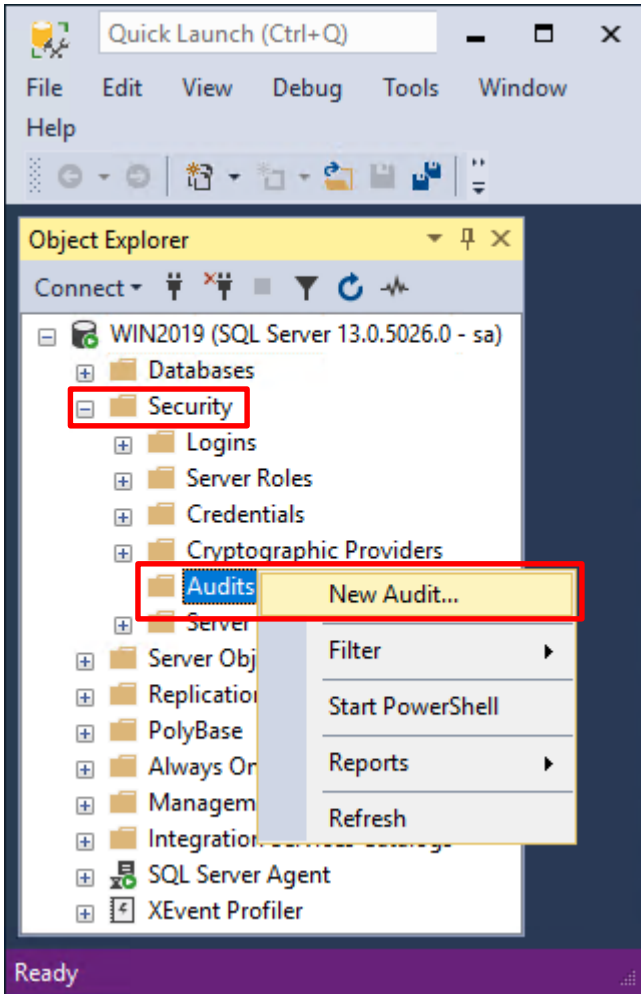


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入 **Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

The screenshot shows the 'Connect to Server' dialog box. The title bar reads 'Connect to Server' with a close button. The main heading is 'SQL Server'. The dialog contains the following fields and controls:

- Server type: Database Engine (dropdown menu)
- Server name: localhost (dropdown menu)
- Authentication: SQL Server Authentication (dropdown menu)
- Login: sa (dropdown menu)
- Password: [masked with asterisks]
- Remember password
- Buttons: Connect (highlighted with a red dashed box), Cancel, Help, Options >>

選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- Continue
- Shut down server
- Fail operation

Audit destination: Application Log

File path:

Audit File Maximum Limit:

- Maximum rollover files:
  - Unlimited
- Maximum files:
  - Number of files: 2147483647

Maximum file size: 0

- Unlimited
- MB
- GB
- TB

Reserve disk space

Connection

WIN2019 [sa]

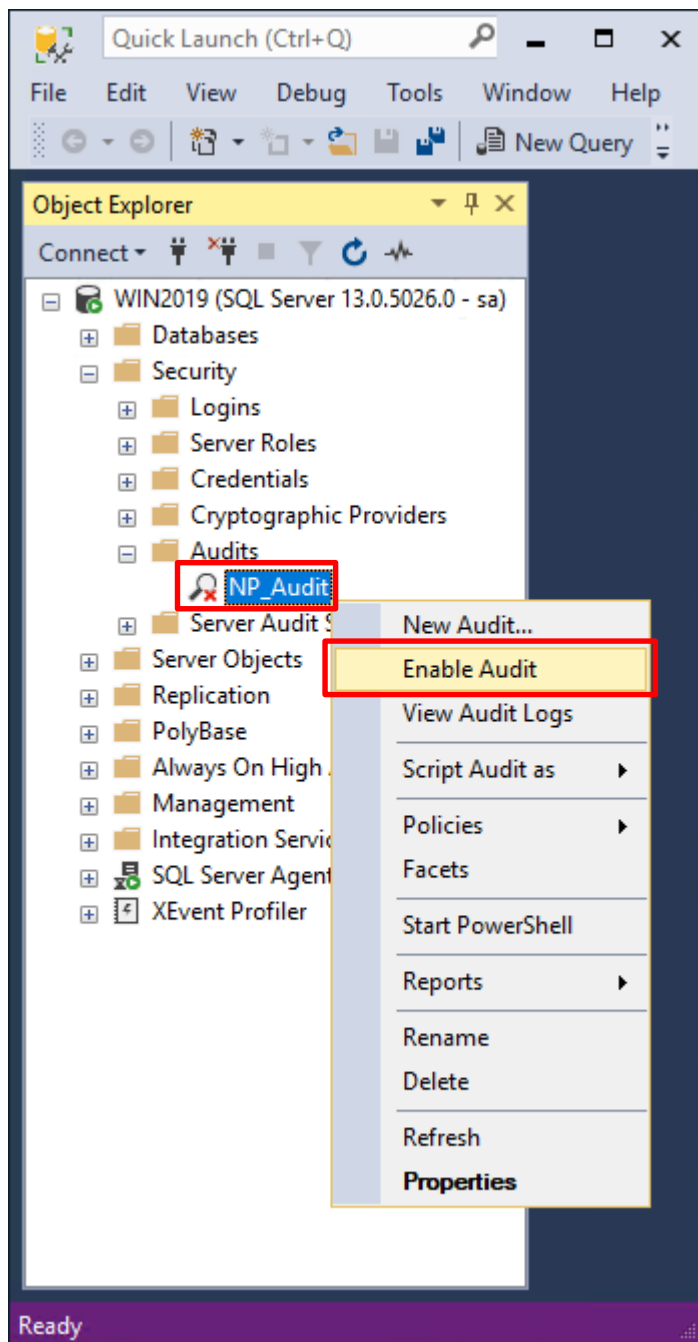
[View connection properties](#)

Progress

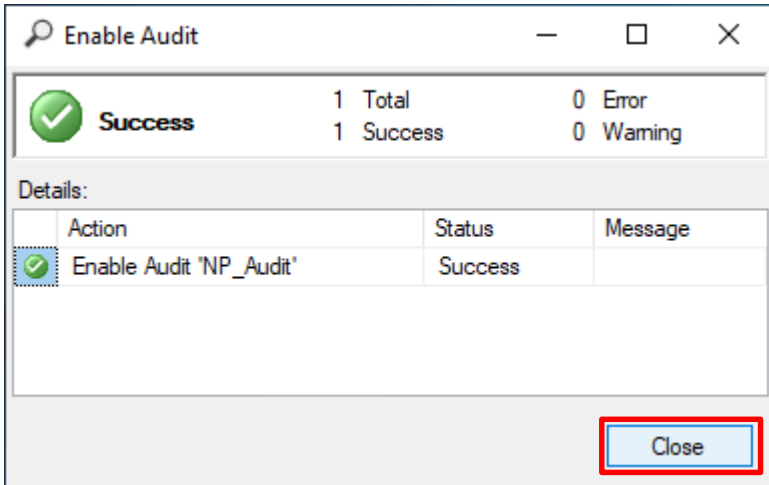
Ready

OK Cancel Help

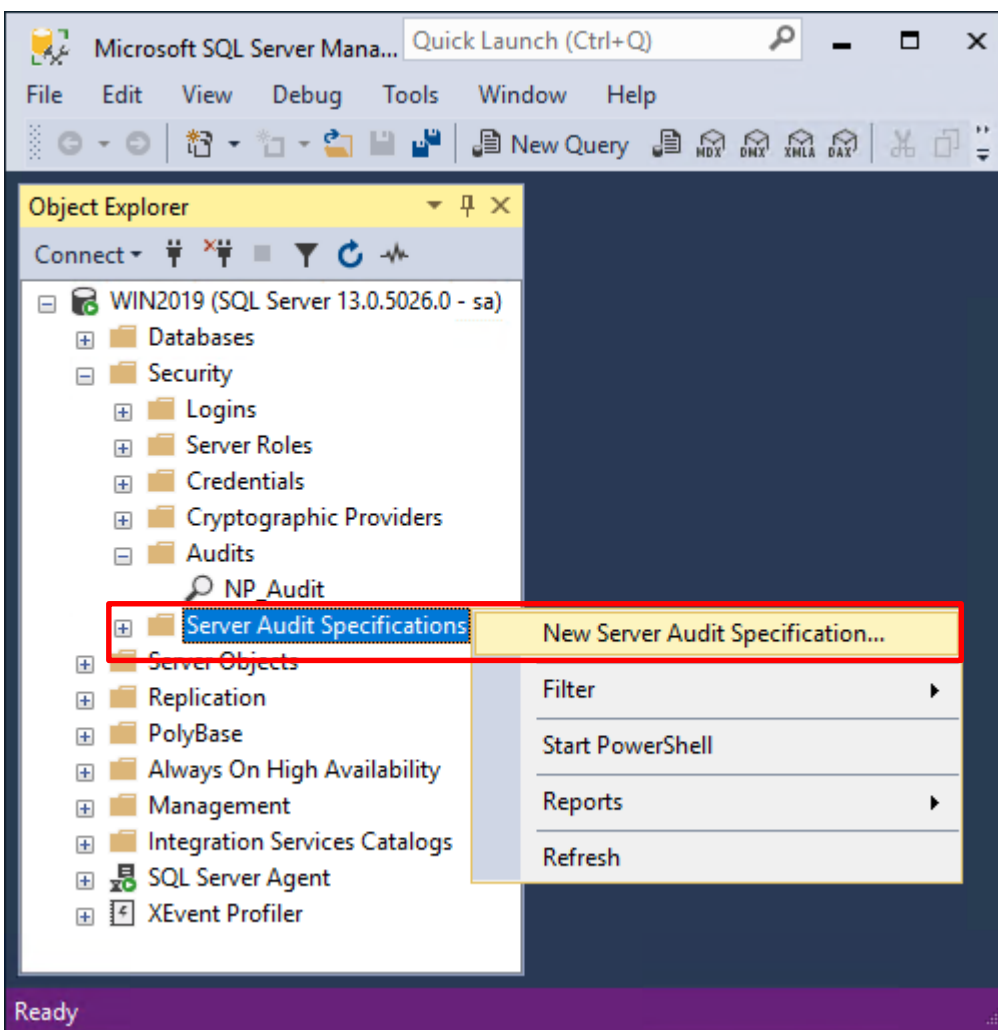
在 Audits name(稽核名稱): NP\_Audit 上按滑鼠右鍵 -> 點選 Enable Audit(啟用稽核)



按下 **Close(關閉)**



在 **Server Audit Specifications(伺服器稽核規格)** 按滑鼠右鍵 -> 點選 **New Server Audit Specification(新增伺服器稽核規格)...**



輸入 **Name(伺服器稽核規格名稱): NP\_Server\_Audit** -> 選擇 **Audit(稽核): NP\_Audit** 和 **Actions(動作): 範例簡易條列** · 詳細說明請參考前言的[稽核動作群組連結](#) -> 按下 **OK(確定)**

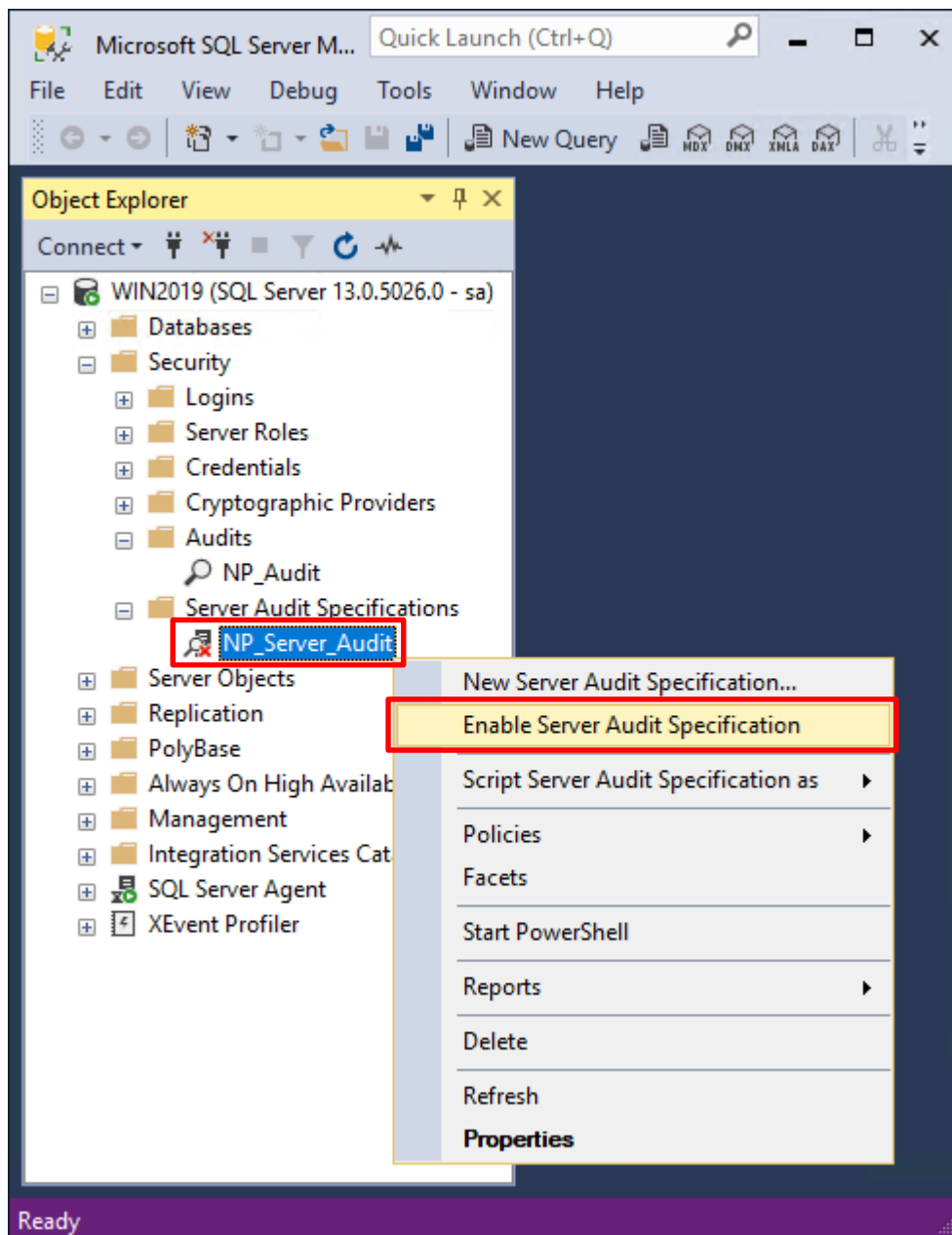
The screenshot shows the 'Create Server Audit Specification' dialog box. The 'Name' field contains 'NP\_Server\_Audit' and the 'Audit' dropdown is set to 'NP\_Audit'. The 'Actions' section contains a table with the following data:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
01	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
02	SERVER_ROLE_MEMBER_CHANGE_GROUP				
03	DATABASE_LOGOUT_GROUP				
04	DATABASE_PERMISSION_CHANGE_GROUP				
05	DATABASE_CHANGE_GROUP				
06	DATABASE_PRINCIPAL_CHANGE_GROUP				
07	SERVER_PRINCIPAL_CHANGE_GROUP				
08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
09	LOGIN_CHANGE_PASSWORD_GROUP				
10	DATABASE_OWNERSHIP_CHANGE_GROUP				
11	USER_CHANGE_PASSWORD_GROUP				
*12					

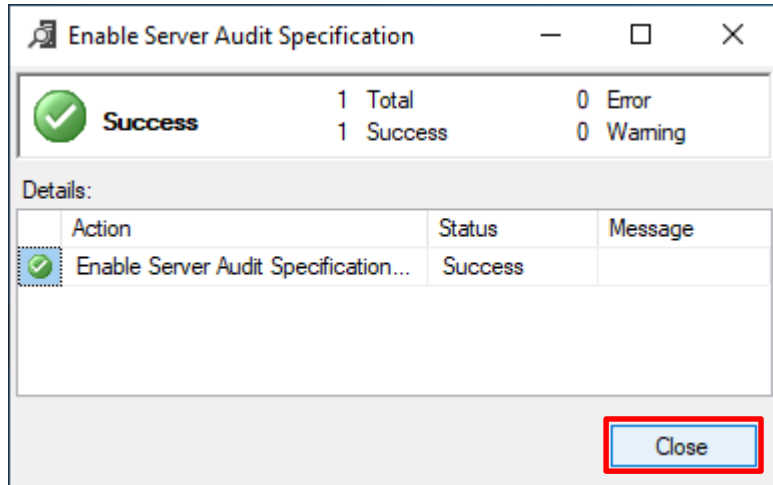
The 'OK' button is highlighted with a red box.

在 **Server Audit Specifications name**(伺服器稽核規格名稱): **NP\_Server\_Audit** 按滑鼠右鍵 -> 點選 **Enable**

**Server Audit Specification**(啟用伺服器稽核規格)



按下 [Close\(關閉\)](#)





## 6.3 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。

開啟 [Microsoft SQL Server Management Studio](#)

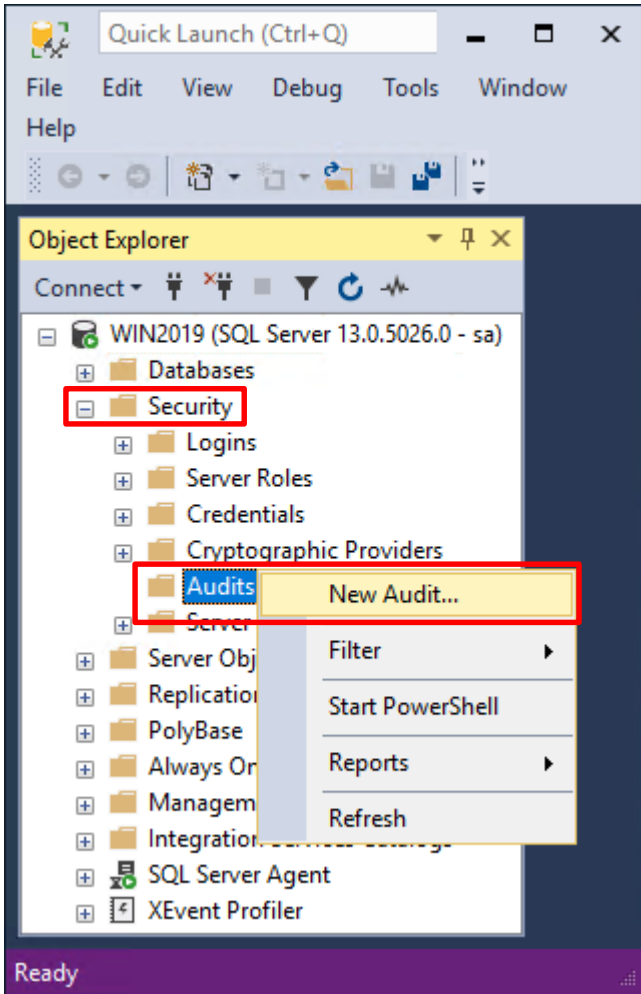


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

A screenshot of the "Connect to Server" dialog box in Microsoft SQL Server Management Studio. The dialog has a title bar with a close button (X) and the text "Connect to Server". The main area is titled "SQL Server". Below the title, there are several fields: "Server type:" with a dropdown menu showing "Database Engine"; "Server name:" with a dropdown menu showing "localhost"; "Authentication:" with a dropdown menu showing "SQL Server Authentication"; "Login:" with a dropdown menu showing "sa"; and "Password:" with a text box containing "\*\*\*\*\*". There is also a checkbox labeled "Remember password" which is checked. At the bottom of the dialog, there are four buttons: "Connect", "Cancel", "Help", and "Options >>". The "Connect" button is highlighted with a red dashed border.

選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page  
General  
Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:  
 Continue  
 Shut down server  
 Fail operation

Audit destination: Application Log

File path: [ ]

Audit File Maximum Limit:  
 Maximum rollover files:  Unlimited  
 Maximum files: Number of files: 2147483647

Maximum file size: 0 MB GB TB  
 Unlimited

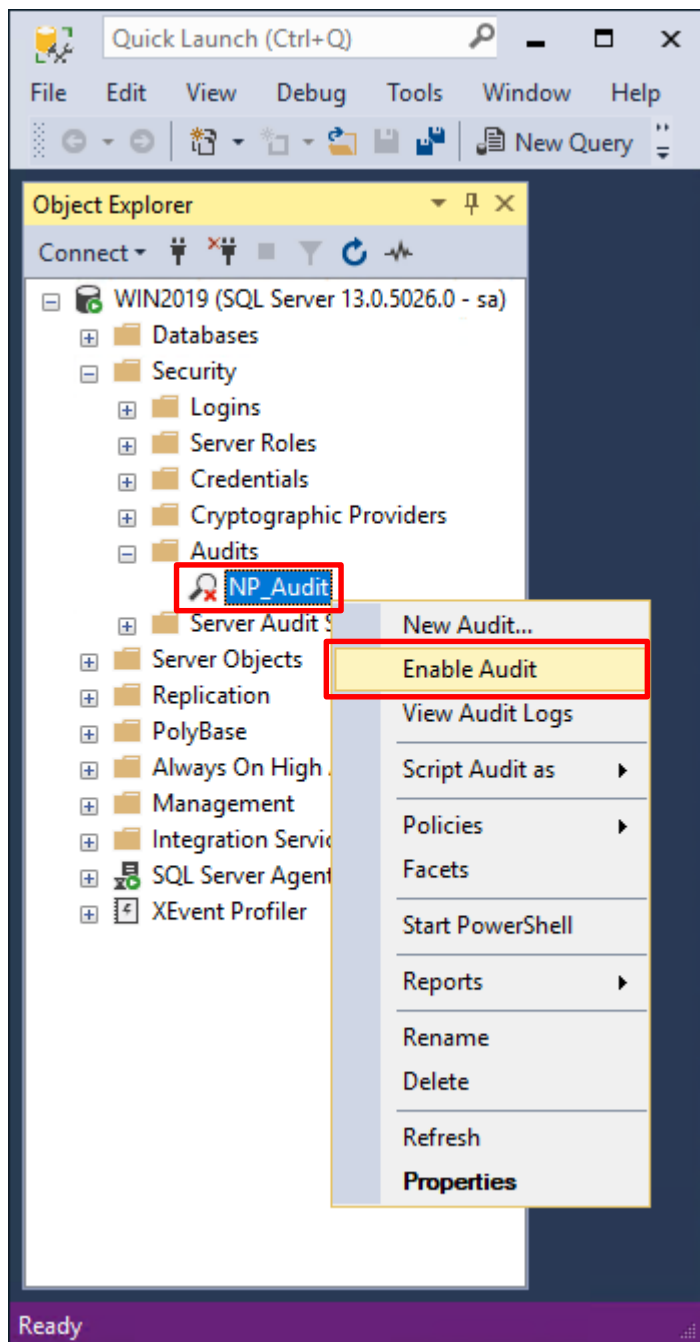
Reserve disk space

Connection  
WIN2019 [sa]  
[View connection properties](#)

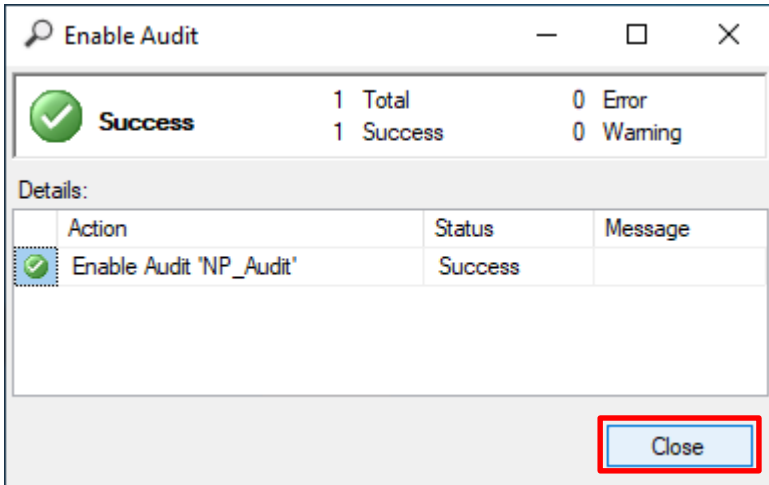
Progress  
Ready

OK Cancel Help

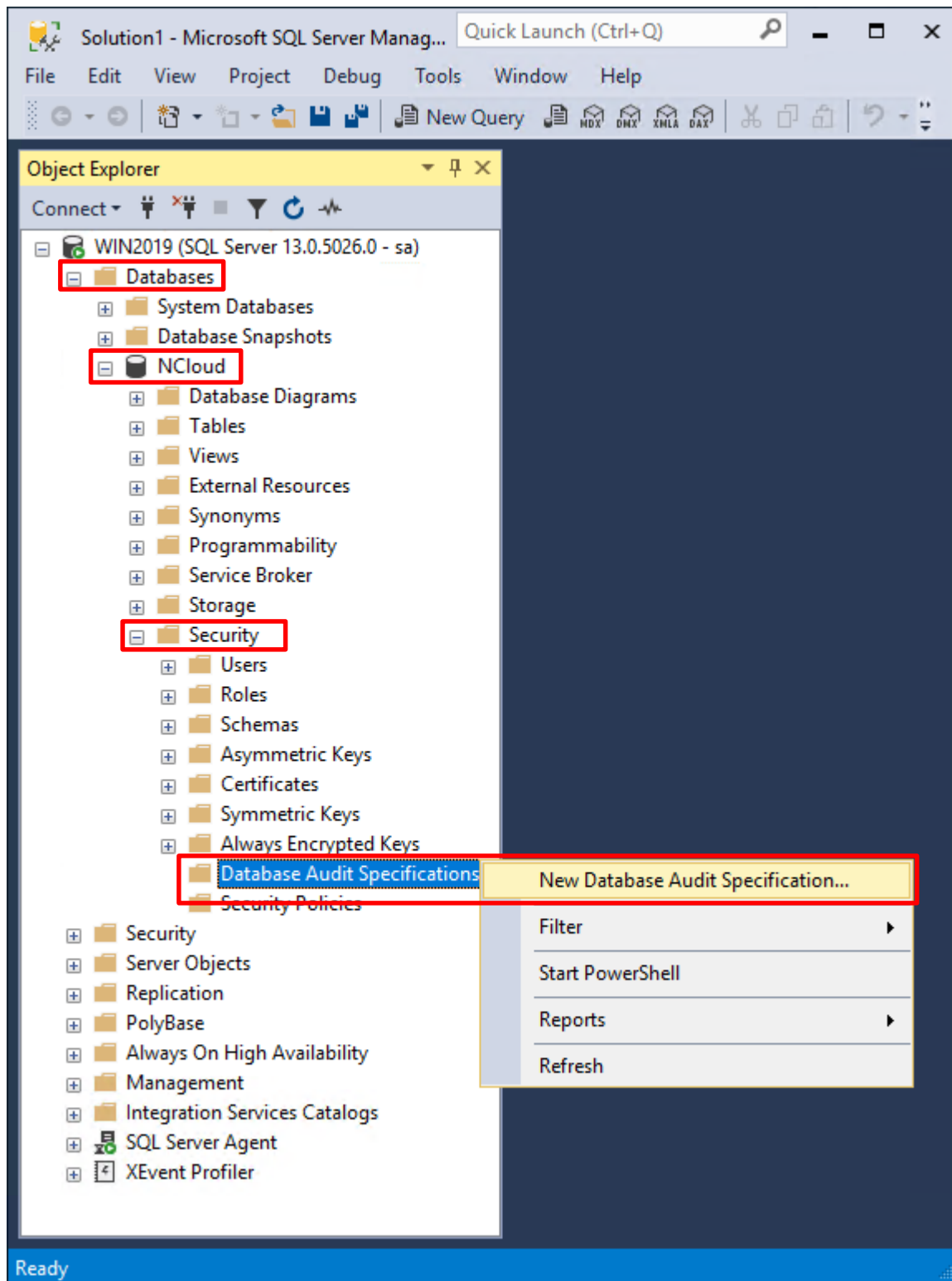
在 Audits name(稽核名稱): NP\_Audit 上按滑鼠右鍵 -> 點選 Enable Audit(啟用稽核)



按下 [Close\(關閉\)](#)



選擇 **Databases(資料庫)** -> **DB(NCloud)** -> **Security(安全性)** -> 在 **Database Audit Specifications(資料庫稽核規格)**  
上按滑鼠右鍵 -> 點選 **New Database Audit Specification(新增資料庫稽核規格)**...



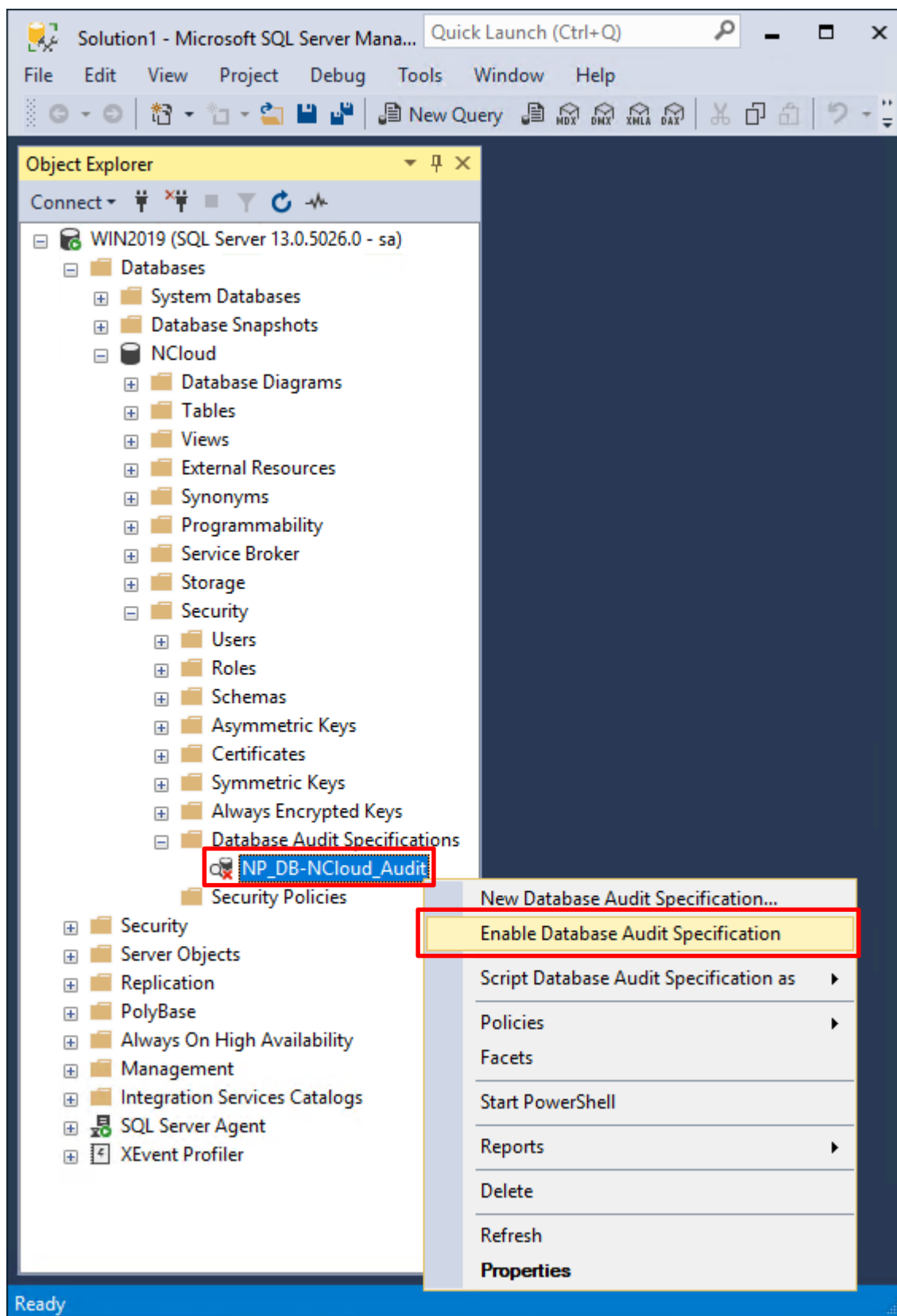
輸入 **Name**(資料庫稽核規格名稱): *NP\_DB-NCloud\_Audit* -> 選擇 **Audit**(稽核名稱): *NP\_Audit* 和 **Actions**(動作):  
範例簡易條列 · 詳細說明請參考前文的稽核動作群組連結 -> 按下 **OK**(確定)

The screenshot shows the 'Create Database Audit Specification' dialog box. The 'Name' field is set to 'NP\_DB-NCloud\_Audit' and the 'Audit' dropdown is set to 'NP\_Audit'. The 'Actions' table is highlighted with a red box and contains the following data:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
2	BACKUP_RESTORE_GROUP				
3	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
4	FAILED_DATABASE_AUTHENTICATION_GROUP				
5	SCHEMA_OBJECT_CHANGE_GROUP				
▶ 6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP				
* 7					

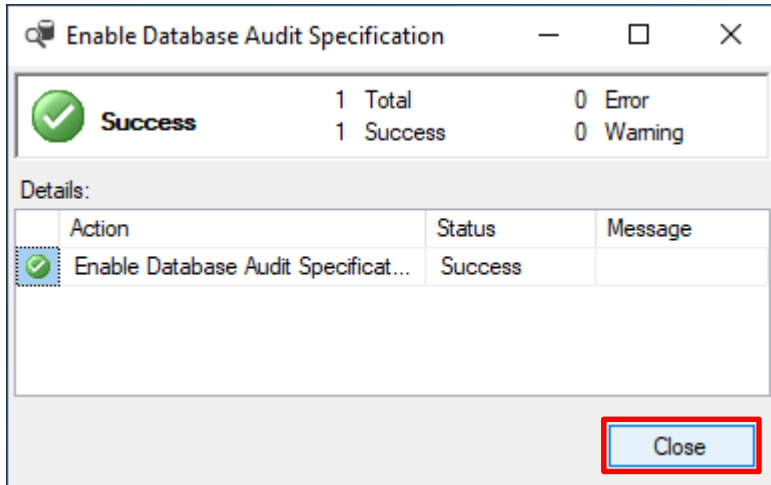
The 'OK' button is highlighted with a red box.

在 **Database Audit Specifications name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 點選 **Enable Database Audit Specification**(啟用資料庫稽核規格)





按下 **Close(關閉)**



## 7. SQL 2019

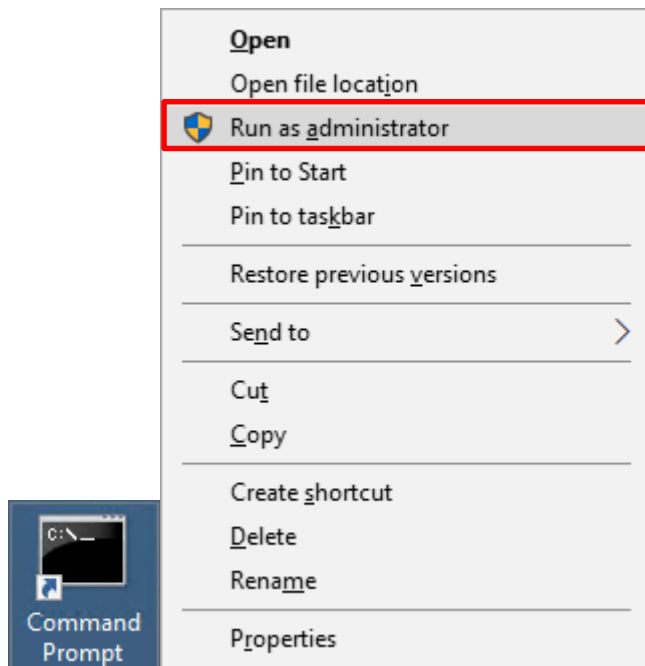
### 7.1 稽核登入

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，才會生效。

以下分別為指令介面和圖形介面設定方式。

#### 7.1.1 使用指令介面方式設定

在 **Command Prompt(命令提示字元)** 上按滑鼠右鍵 -> 點選 **Run as administrator(以系統管理員身分執行)**



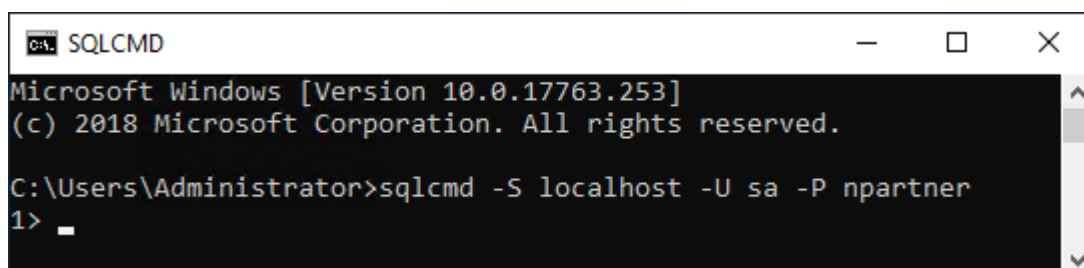
輸入 `sqlcmd -S localhost -U sa -P npartner`

#### Options:

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

**-U** login\_id

**-P** password



輸入 `use master -> go`

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

使用 `sp_configure` 列出進階選項

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

```
SQLCMD
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

啟用通用條件合規性

輸入 `exec sp_configure 'common criteria compliance enabled', 1 -> go -> reconfigure with override -> go`

```
SQLCMD
1> exec sp_configure 'common criteria compliance enabled', 1
2> go
Configuration option 'common criteria compliance enabled' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure with override
2> go
1> _
```

啟用失敗和成功的登入記錄

輸入 `EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',`

`N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 -> go -> quit`

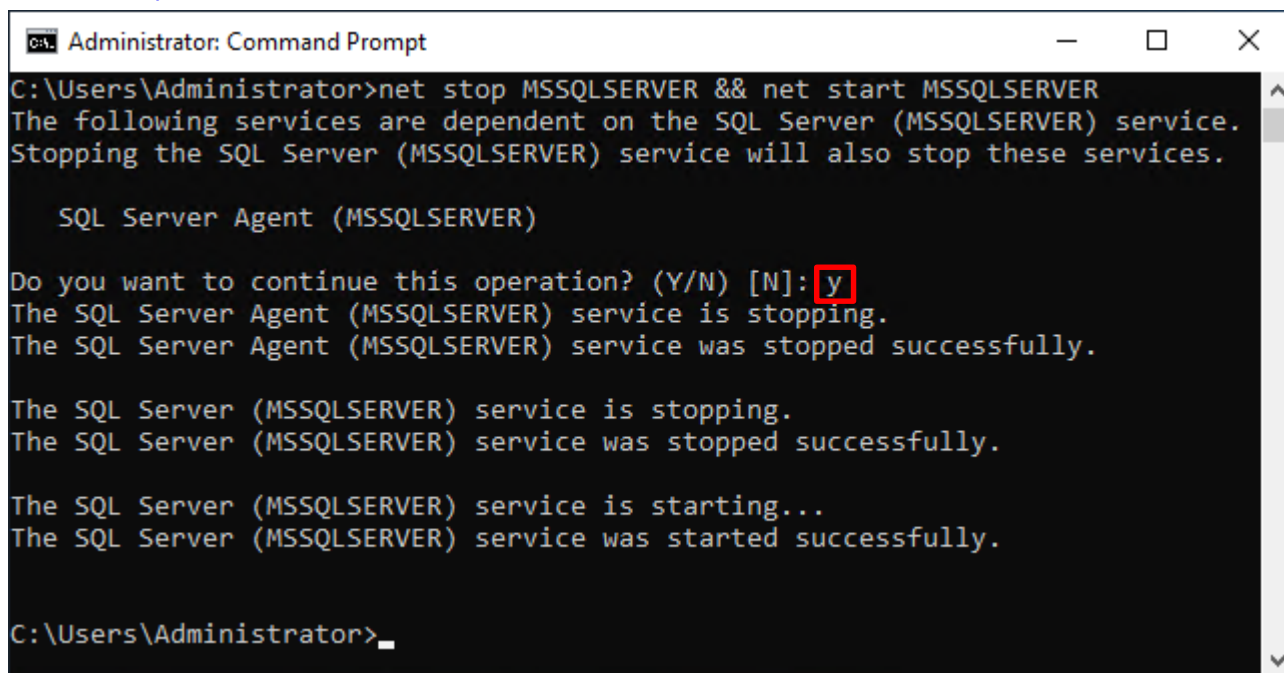
```
Administrator: Command Prompt
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1> quit

C:\Users\Administrator>_
```

重新啟動 MSSQLSERVER 服務

輸入 `net stop MSSQLSERVER && net start MSSQLSERVER`



```
Administrator: Command Prompt
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSERVER
The following services are dependent on the SQL Server (MSSQLSERVER) service.
Stopping the SQL Server (MSSQLSERVER) service will also stop these services.

    SQL Server Agent (MSSQLSERVER)

Do you want to continue this operation? (Y/N) [N]: y
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

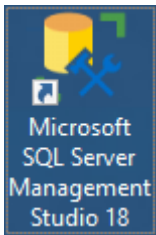
The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

The SQL Server (MSSQLSERVER) service is starting...
The SQL Server (MSSQLSERVER) service was started successfully.

C:\Users\Administrator>
```

## 7.1.2 使用圖形介面方式設定

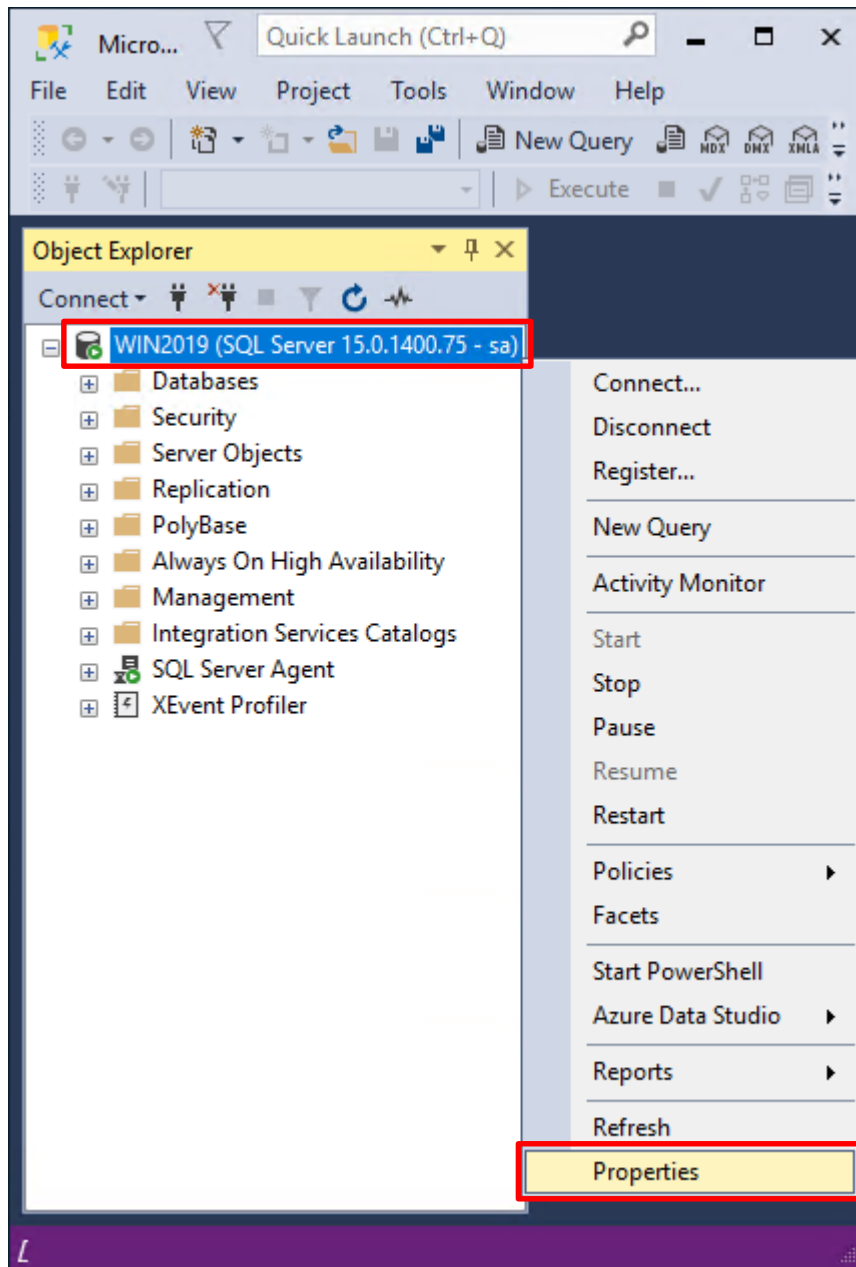
開啟 Microsoft SQL Server Management Studio



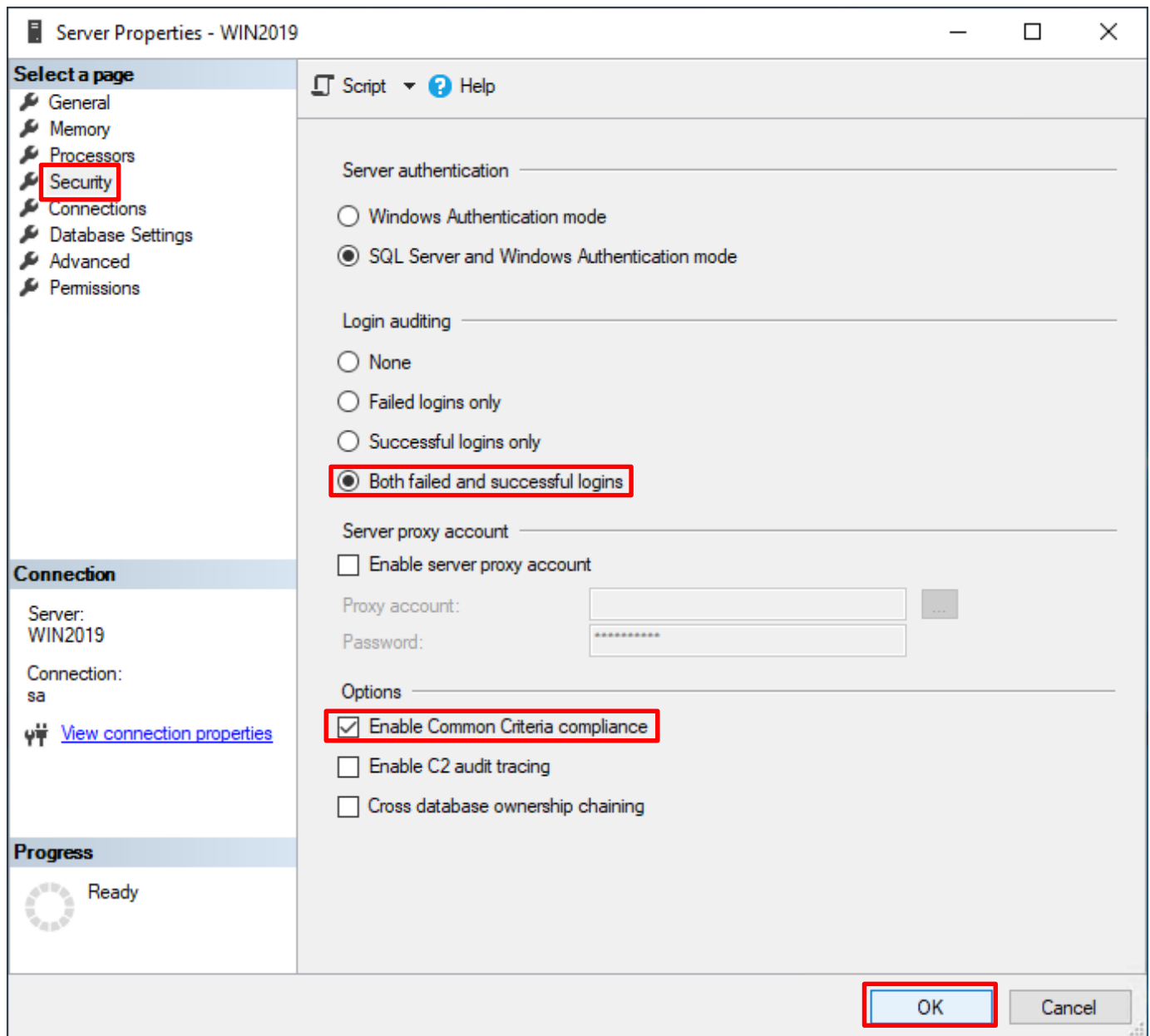
輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入 **Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

The screenshot shows the "Connect to Server" dialog box in SQL Server Management Studio. The title bar reads "Connect to Server" with a close button. The main heading is "SQL Server". The dialog contains several fields: "Server type:" with a dropdown menu set to "Database Engine"; "Server name:" with a dropdown menu set to "localhost"; "Authentication:" with a dropdown menu set to "SQL Server Authentication"; "Login:" with a dropdown menu set to "sa"; and "Password:" with a text box containing "\*\*\*\*\*". There is a checkbox labeled "Remember password" which is checked. At the bottom, there are four buttons: "Connect", "Cancel", "Help", and "Options >>". The "Connect" button is highlighted with a red dashed border.

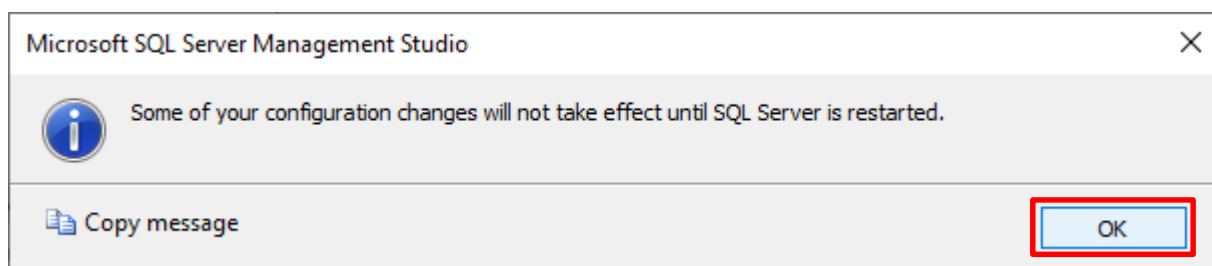
在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Properties(屬性)**



選擇 **Security(安全性)** 頁面 -> **Login auditing(登入稽核)**: 點選 **Both failed and successful logins(失敗和成功的登入)** -> **Options**: 勾選 **Enable Common Criteria compliance(啟用通用條件合規性)** -> 按下 **OK(確定)**

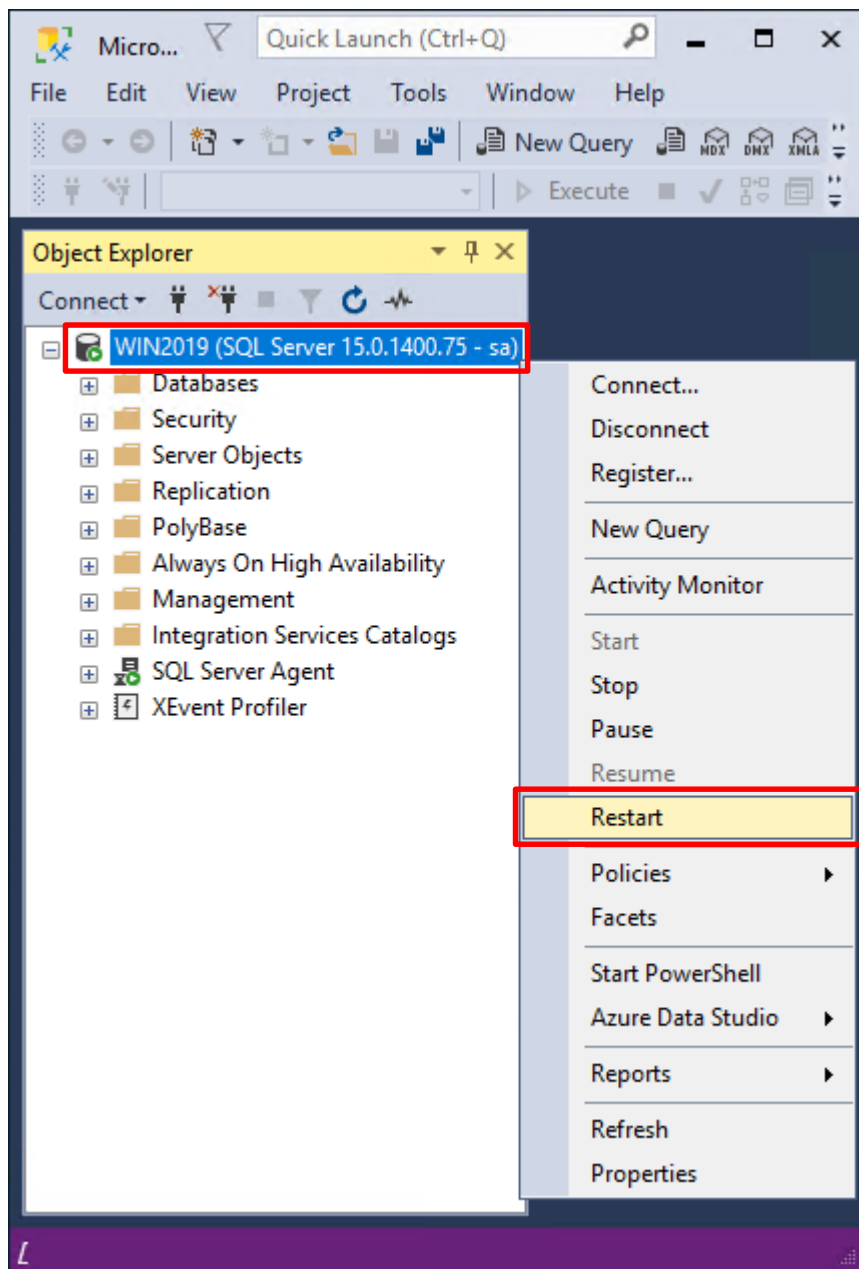


按下 **OK(確定)**

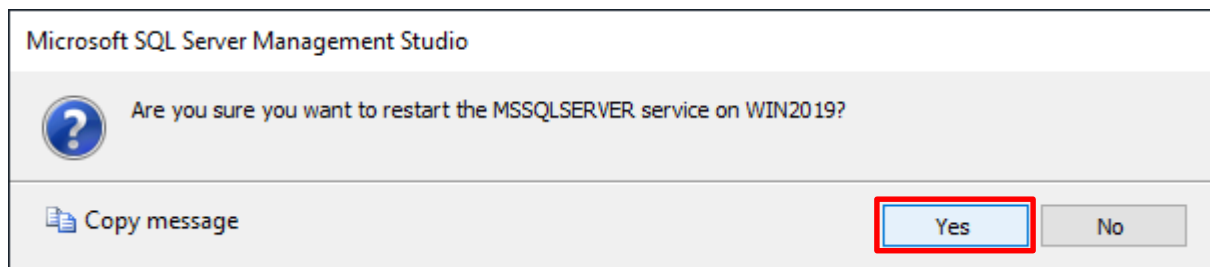


重新啟動 MSSQLSERVER 服務

在 **Server name(伺服器名稱)** 上按滑鼠右鍵 -> 點選 **Restart(重新啟動)**

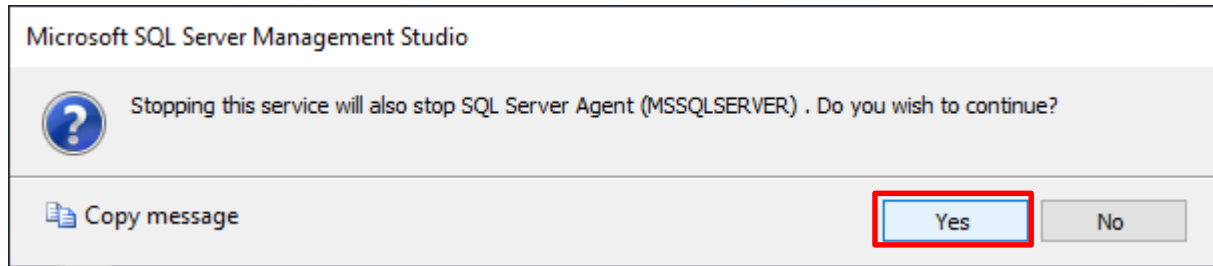


按下 **Yes(是)** 重新啟動 MSSQLSERVER 服務





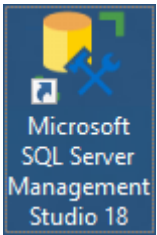
按下 **Yes(是)** 停止 SQLSERVER Agent



## 7.2 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。

開啟 [Microsoft SQL Server Management Studio](#)

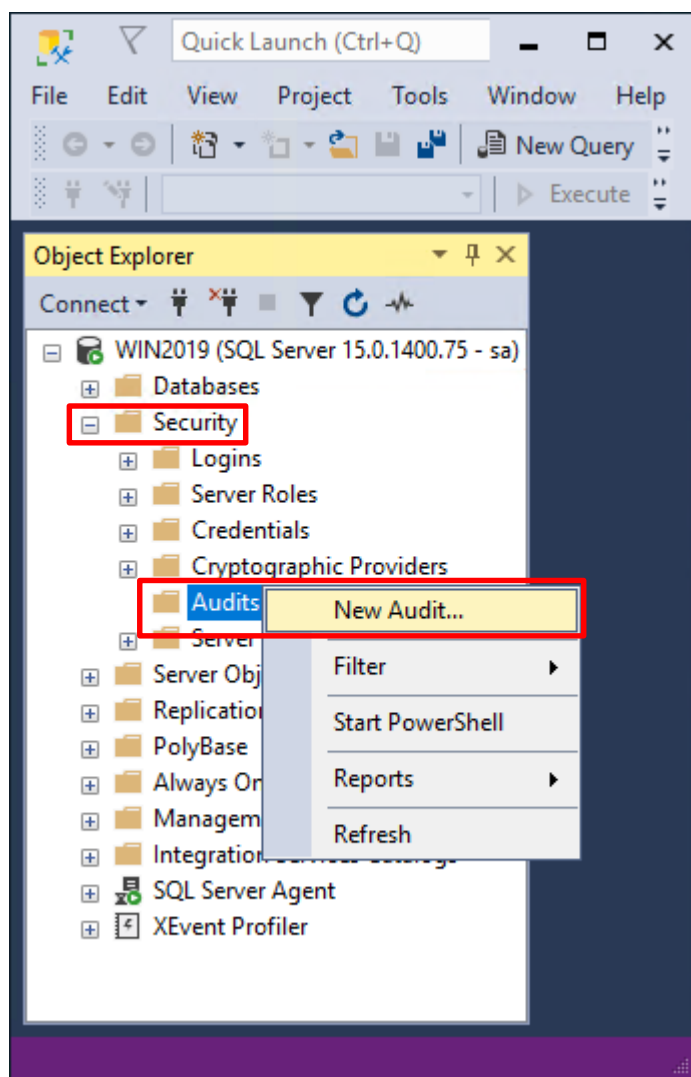


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

A screenshot of the 'Connect to Server' dialog box in SQL Server Management Studio. The dialog has a title bar 'Connect to Server' and a close button. The main title is 'SQL Server'. Below the title, there are several fields: 'Server type:' with a dropdown menu showing 'Database Engine'; 'Server name:' with a dropdown menu showing 'localhost'; 'Authentication:' with a dropdown menu showing 'SQL Server Authentication'; 'Login:' with a dropdown menu showing 'sa'; and 'Password:' with a text box containing '\*\*\*\*\*'. There is a checkbox labeled 'Remember password' which is checked. At the bottom, there are four buttons: 'Connect', 'Cancel', 'Help', and 'Options >>'. The 'Connect' button is highlighted with a red dashed border.

選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name(稽核名稱): NP\_Audit** -> 選擇 **Audit(稽核目的地): Application Log(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裡 -> 按下 **OK(確定)**

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:

- Continue
- Fail operation
- Shut down server

Audit destination: Application Log

Path: [ ]

Audit File Maximum Limit:

- Maximum rollover files:  Unlimited
- Maximum files: Number of files: 2147483647

Maximum file size: 0 MB GB TB

- Unlimited

Reserve disk space

Connection

WIN2019 [sa]

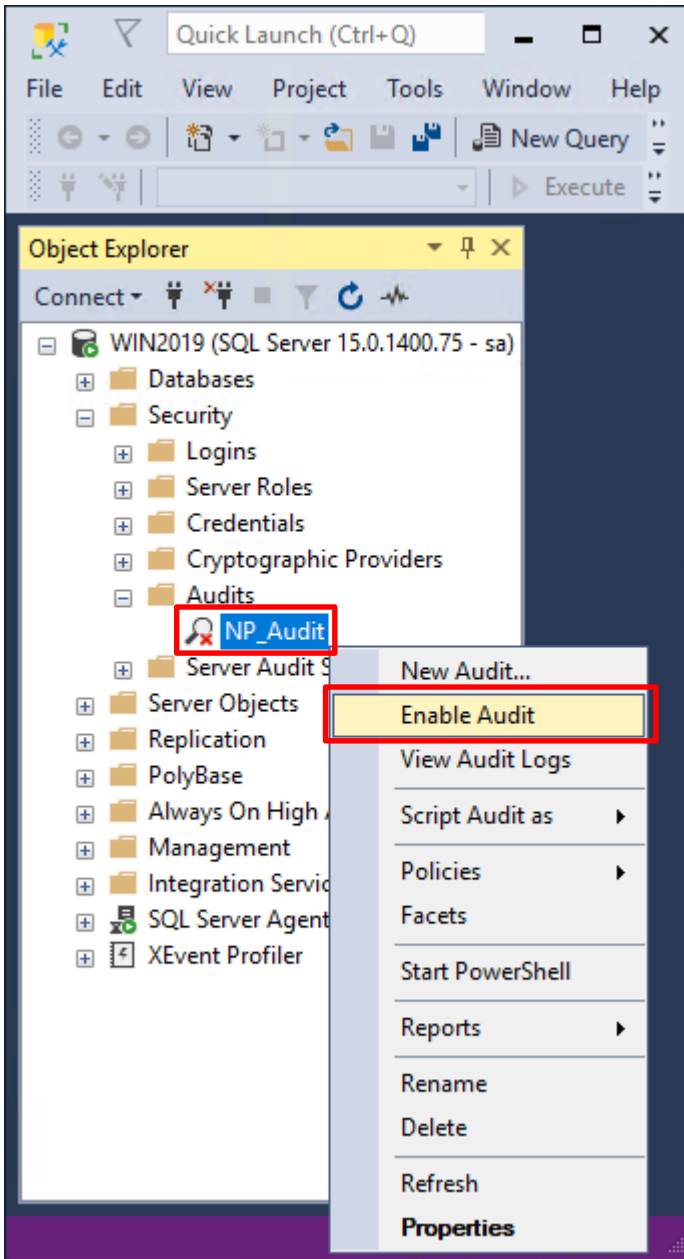
[View connection properties](#)

Progress

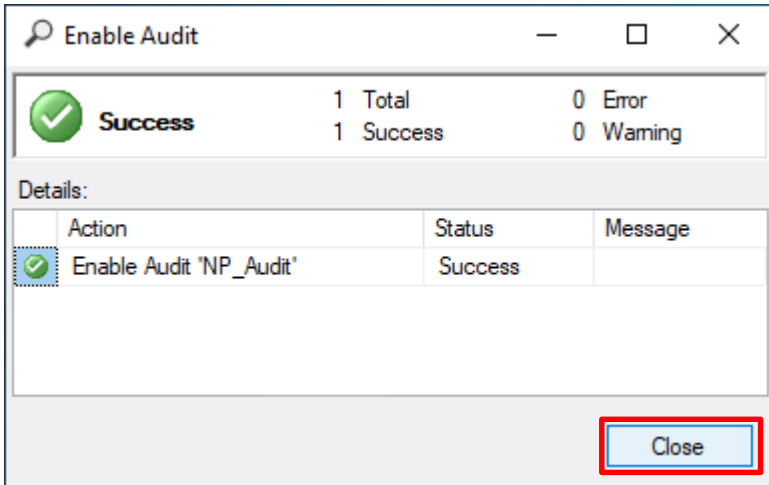
Ready

OK Cancel Help

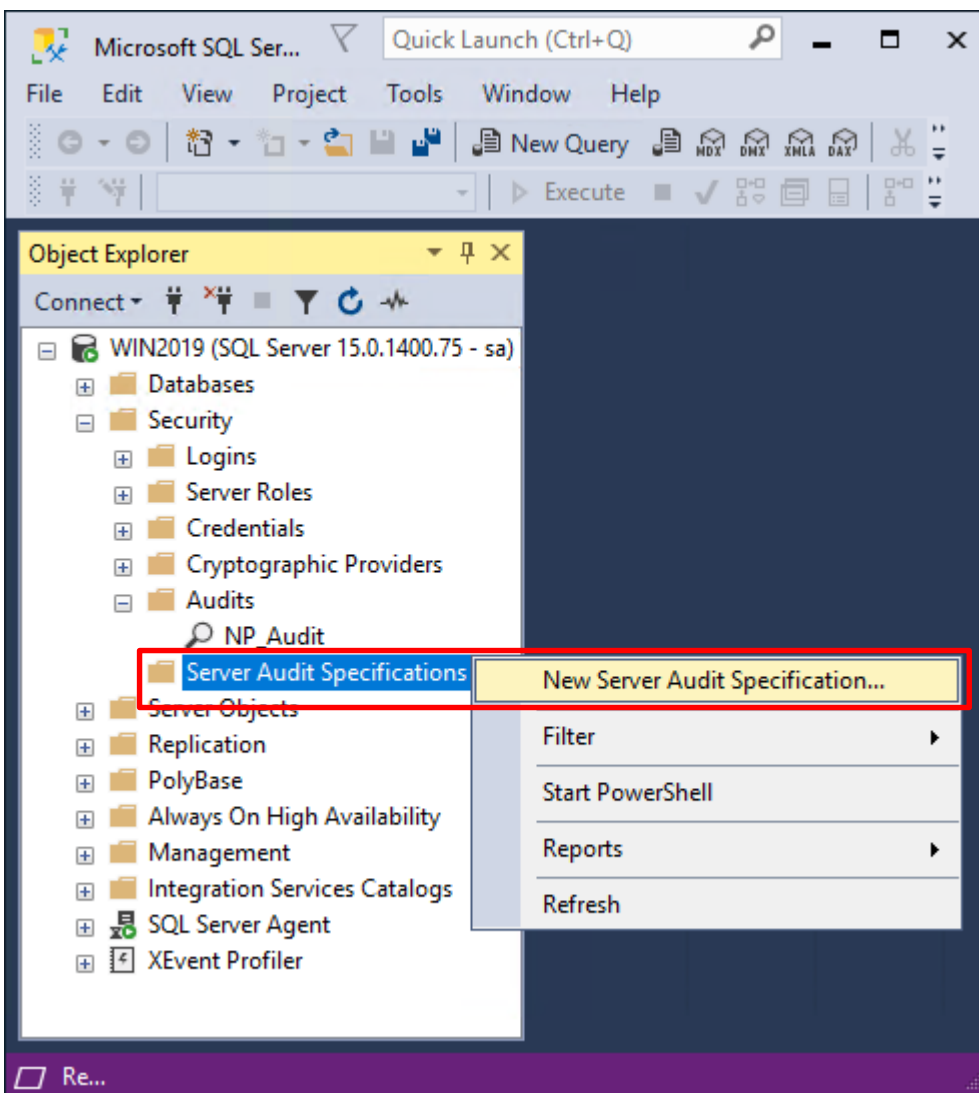
在 Audits name(稽核名稱): NP\_Audit 上按滑鼠右鍵 -> 點選 Enable Audit(啟用稽核)



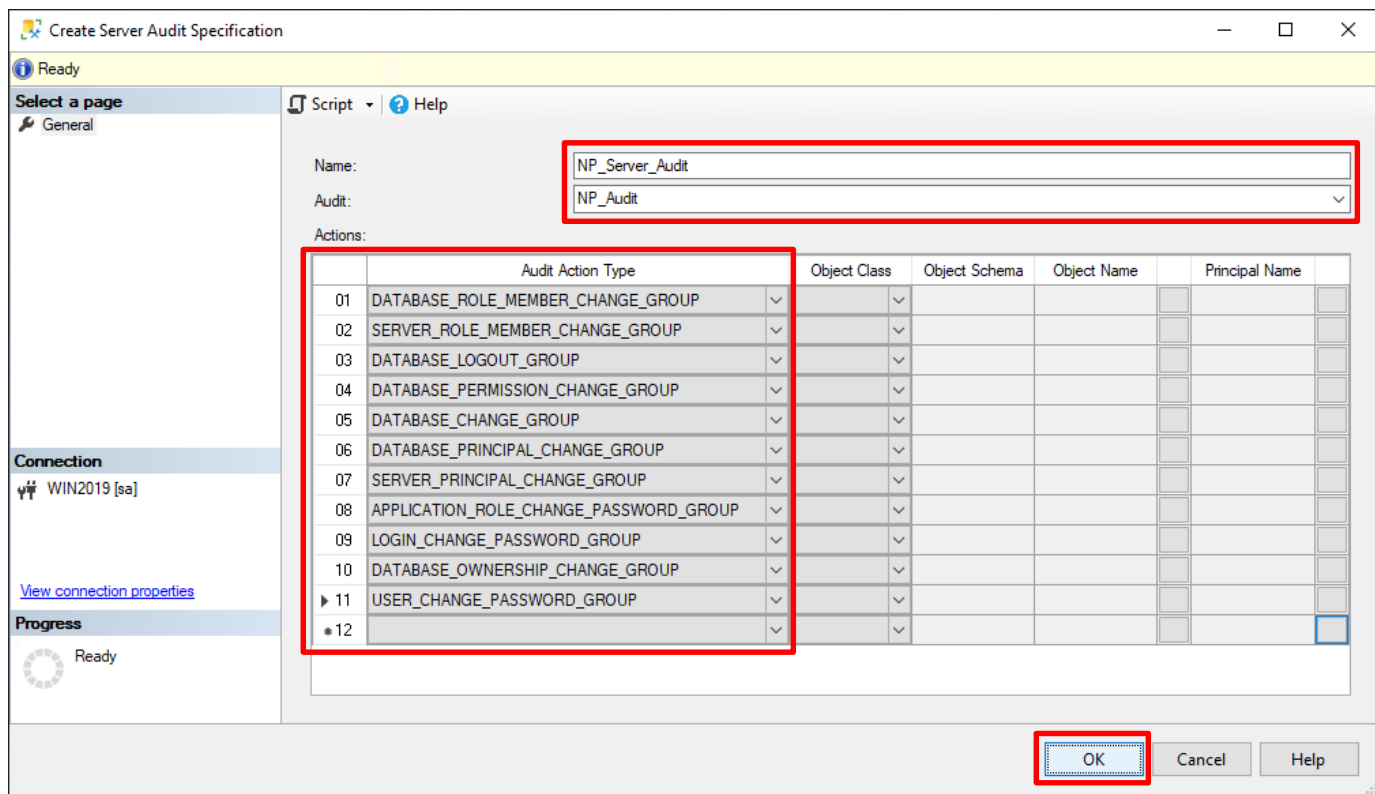
按下 **Close(關閉)**



在 **Server Audit Specifications(伺服器稽核規格)** 按滑鼠右鍵 -> 點選 **New Server Audit Specification(新增伺服器稽核規格)...**

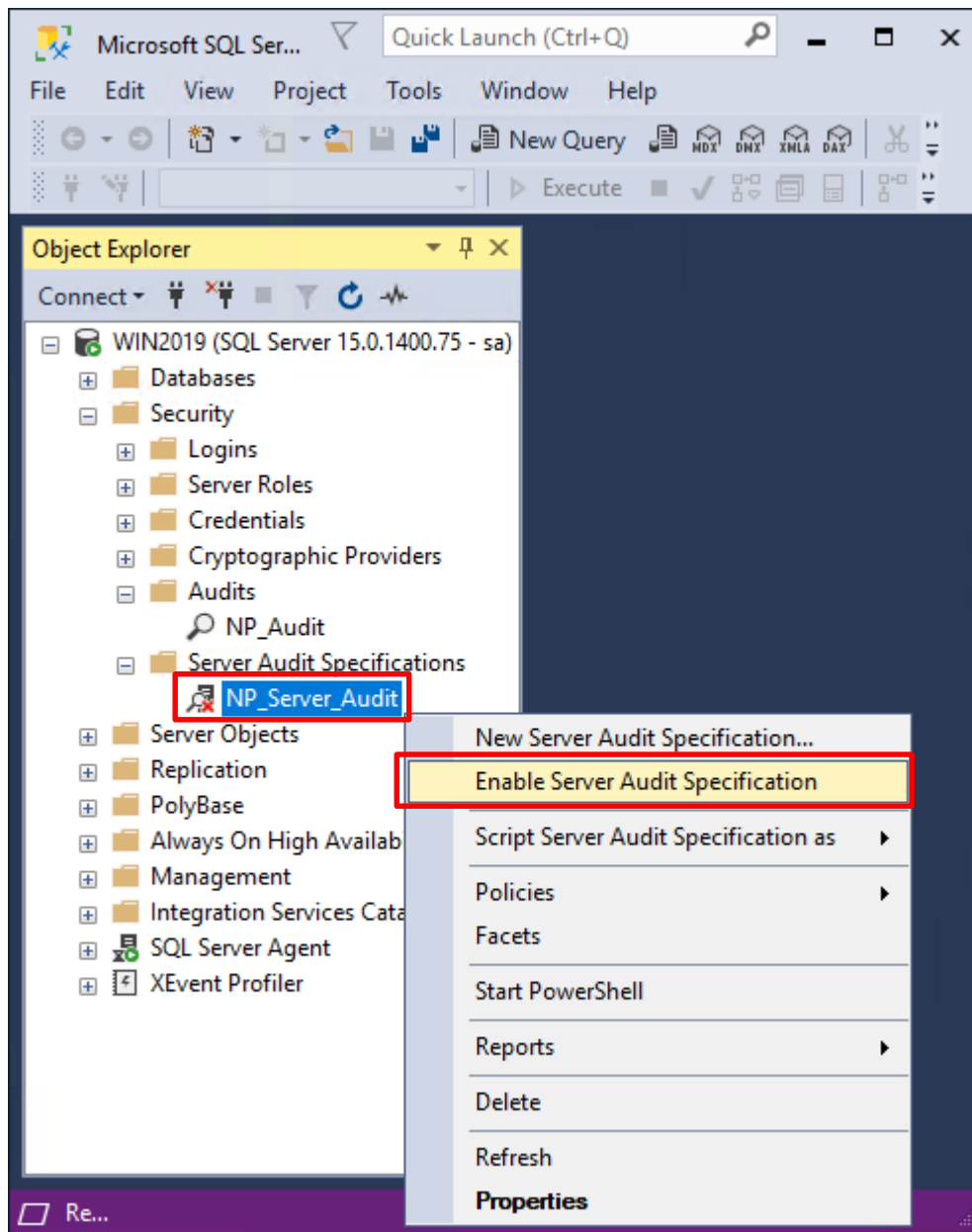


輸入 **Name(伺服器稽核規格名稱): NP\_Server\_Audit** -> 選擇 **Audit(稽核): NP\_Audit** 和 **Actions(動作): 範例簡易條列** · 詳細說明請參考前言的[稽核動作群組連結](#) -> 按下 **OK(確定)**



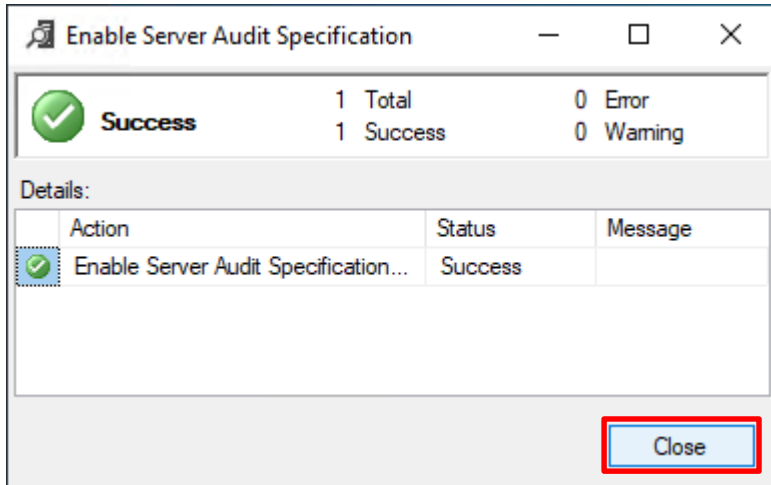
在 **Server Audit Specifications name**(伺服器稽核規格名稱): **NP\_Server\_Audit** 按滑鼠右鍵 -> 點選 **Enable**

Server Audit Specification(啟用伺服器稽核規格)





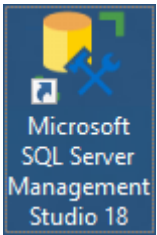
按下 **Close(關閉)**



## 7.3 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。

開啟 [Microsoft SQL Server Management Studio](#)

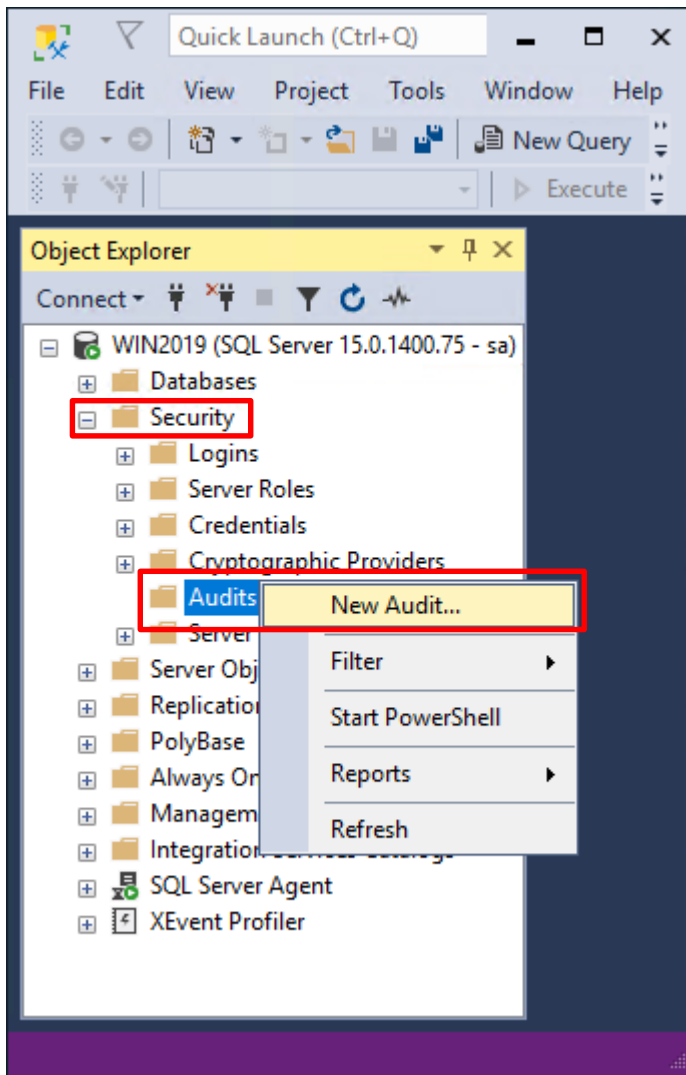


輸入 **Server name(伺服器名稱): localhost** -> 選擇 **Authentication(驗證): SQL Server Authentication** -> 輸入

**Login(登入): sa** 和 **Password(密碼): npartner** -> 按下 **Connect(連接)**

A screenshot of the "Connect to Server" dialog box in SQL Server Management Studio. The dialog has a title bar "Connect to Server" and a close button. The main heading is "SQL Server". Below this, there are several fields: "Server type:" with a dropdown menu showing "Database Engine"; "Server name:" with a dropdown menu showing "localhost"; "Authentication:" with a dropdown menu showing "SQL Server Authentication"; "Login:" with a dropdown menu showing "sa"; and "Password:" with a text box containing "\*\*\*\*\*". There is a checkbox labeled "Remember password" which is checked. At the bottom, there are four buttons: "Connect", "Cancel", "Help", and "Options >>". The "Connect" button is highlighted with a red dashed border.

選擇 Security(安全性) -> 在 Audits(稽核) 上按滑鼠右鍵 -> 點選 New Audit(新增稽核)...



輸入 **Audit name**(稽核名稱): NP\_Audit -> 選擇 **Audit**(稽核目的地): Application Log(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裡 -> 按下 **OK**(確定)

**Create Audit**

Ready

Select a page

- General
- Filter

Script | Help

Audit name: NP\_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:  Continue  
 Fail operation  
 Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:  Maximum rollover files:  Unlimited  
 Maximum files: Number of files: 2147483647

Maximum file size: 0  MB  GB  TB  
 Unlimited

Reserve disk space

Connection

WIN2019 [sa]

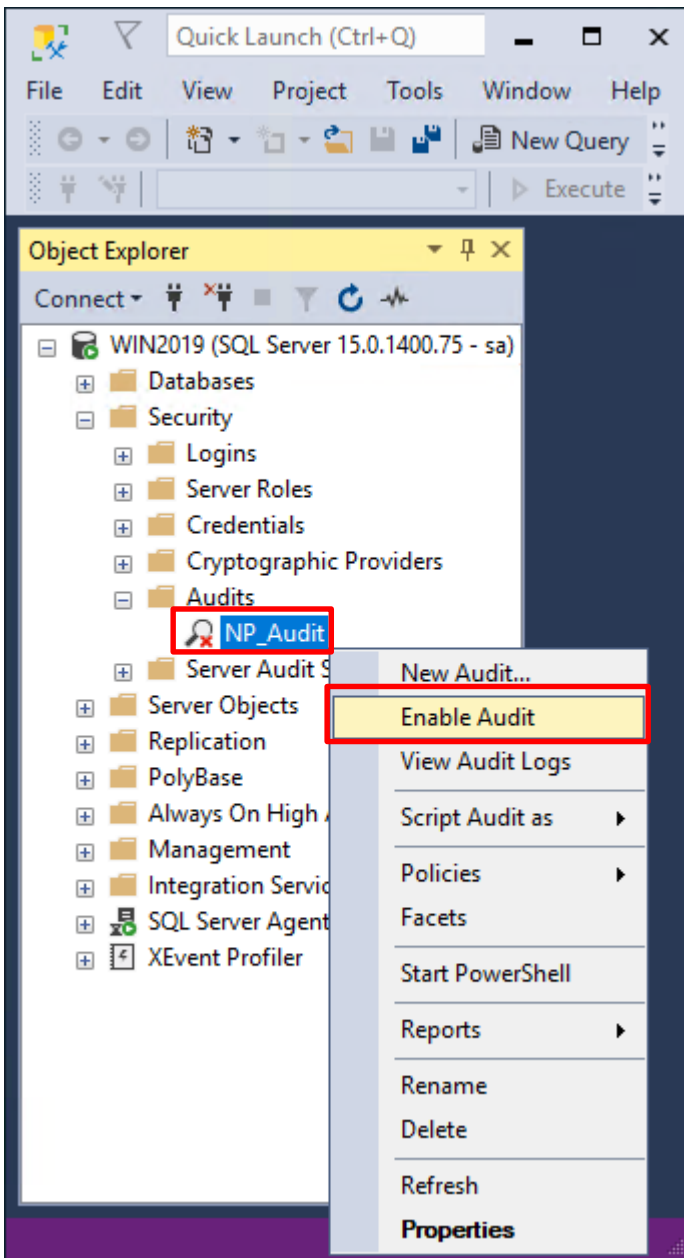
[View connection properties](#)

Progress

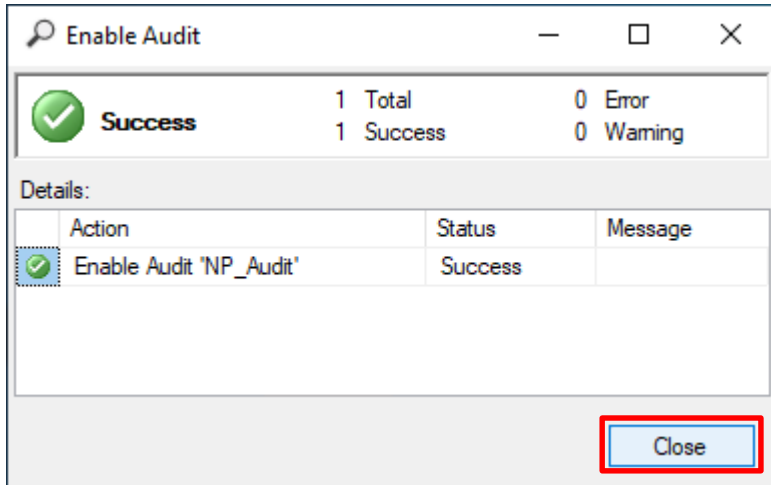
Ready

OK Cancel Help

在 Audits name(稽核名稱): NP\_Audit 上按滑鼠右鍵 -> 點選 Enable Audit(啟用稽核)

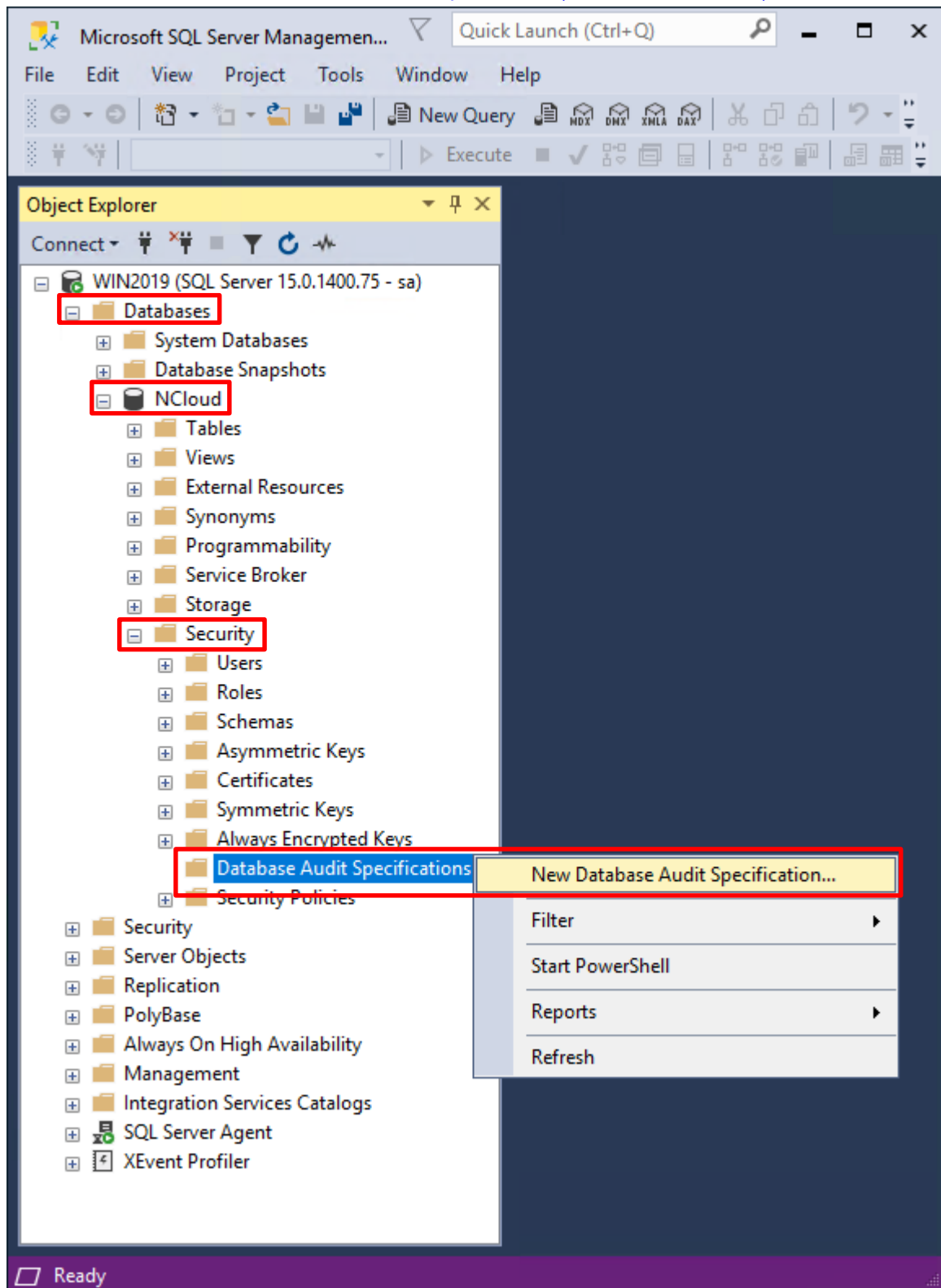


按下 [Close\(關閉\)](#)



選擇 **Databases(資料庫)** -> **DB(NCloud)** -> **Security(安全性)** -> 在 **Database Audit Specifications(資料庫稽核規格)**

上按滑鼠右鍵 -> 點選 **New Database Audit Specification(新增資料庫稽核規格)...**



輸入 **Name**(資料庫稽核規格名稱): *NP\_DB-NCloud\_Audit* -> 選擇 **Audit**(稽核名稱): *NP\_Audit* 和 **Actions**(動作):  
範例簡易條列 · 詳細說明請參考前文的[稽核動作群組連結](#) -> 按下 **OK**(確定)

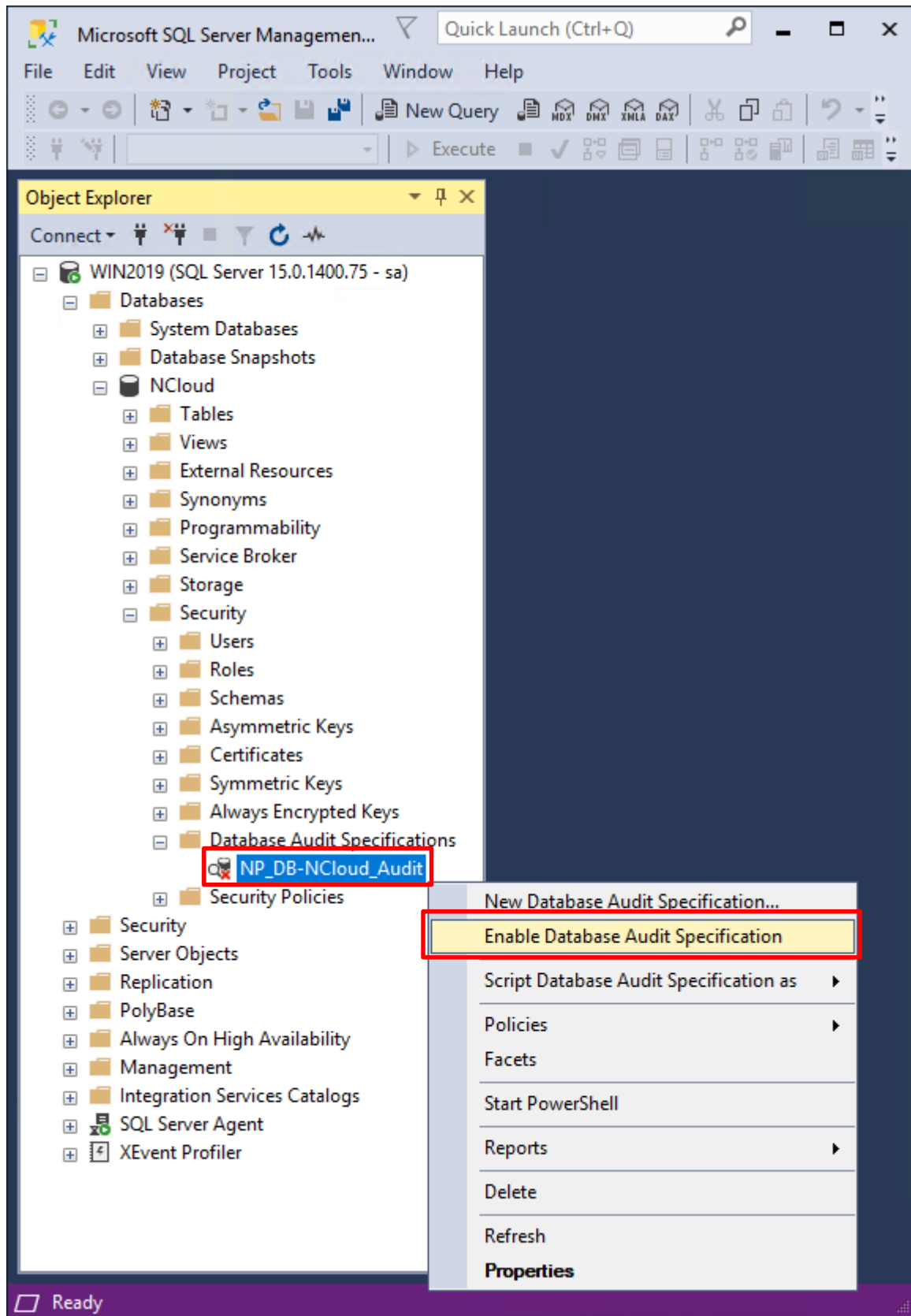
The screenshot shows the 'Create Database Audit Specification' dialog box. The 'Name' field is 'NP\_DB-NCloud\_Audit' and the 'Audit' dropdown is 'NP\_Audit'. The 'Actions' table is as follows:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP				
2	BACKUP_RESTORE_GROUP				
3	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
4	FAILED_DATABASE_AUTHENTICATION_GROUP				
5	SCHEMA_OBJECT_CHANGE_GROUP				
6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP				
*7					

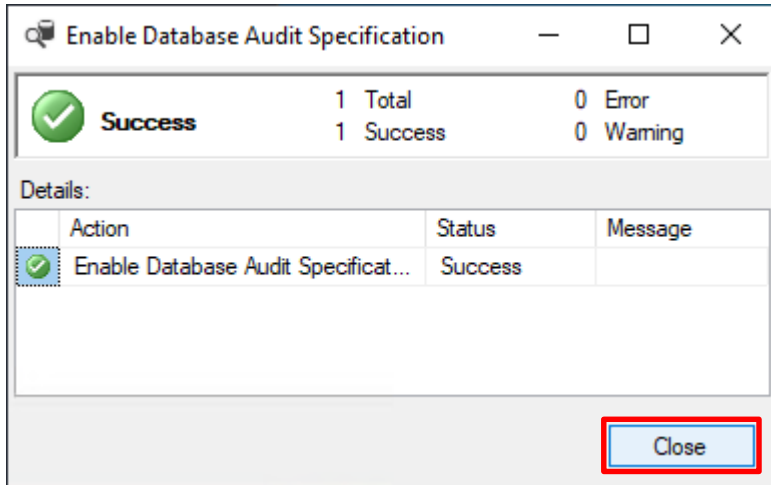
The 'OK' button is highlighted with a red box.



在 **Database Audit Specifications name**(資料庫稽核規格名稱): **NP\_DB-NCloud\_Audit** -> 點選 **Enable Database Audit Specification**(啟用資料庫稽核規格)



按下 [Close\(關閉\)](#)

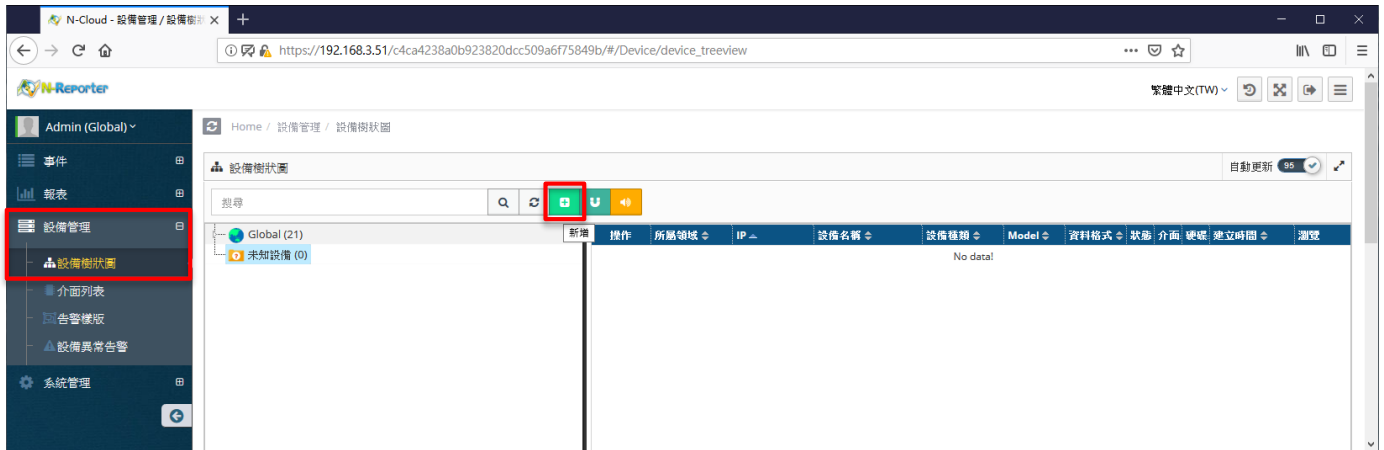


## 8. N-Reporter

### 8.1 MS SQL

(1) 新增 MS SQL Server 設備

選擇 **設備管理** -> **設備樹狀圖** -> 按下 **新增**



(2) 設定 MS SQL Server 設備的資料格式和 Facility

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

**新增設備**

設備基本設定

名稱  
SQL-192.168.2.217

IP  
192.168.2.217

設備種類  
 Syslog  Flow  SNMP

Syslog 相關設定

資料格式  
MS SQL

Facility  
(18) local use 2 (local2)

編碼方式  
UTF-8

設備進階設定

設備 Icon  
icon-host

Login Account

Login Password

Action 設備  
 是否為 Action 設備

接收狀態  
 啟用  停用

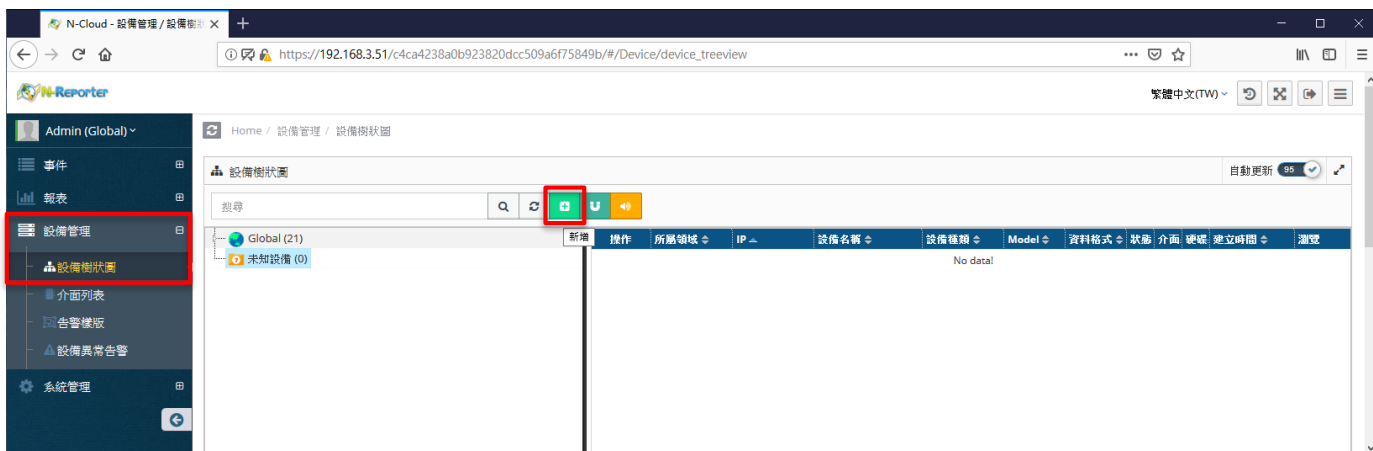
暫無資料告警  
 啟用 Syslog/Flow 暫無資料告警

確定 取消

## 8.2 Windows

### (1) 新增 Windows Server 設備

選擇 設備管理 -> 設備樹狀圖 -> 按下 新增



(2) 設定 Windows Server 設備的資料格式和 Facility

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

新增設備

設備基本設定

名稱  
Windows-192.168.2.217

IP  
192.168.2.217

設備種類  
 Syslog  Flow  SNMP

Syslog 相關設定

資料格式  
Windows

Facility  
(17) local use 1 (local1)

編碼方式  
UTF-8

設備進階設定

設備 Icon  
icon-host

Login Account

Login Password

Action 設備  
 是否為 Action 設備

接收狀態  
 啟用  停用

暫無資料告警  
 啟用 Syslog/Flow 暫無資料告警

確定 取消



## 連絡資訊

TEL: +886-4-23752865

FAX: +886-4-23757458

技術問題請洽：

Email: [support@npartnertech.com](mailto:support@npartnertech.com)

Skype: [support@npartnertech.com](https://www.skype.com/partner)

業務相關請洽：

Email: [sales@npartnertech.com](mailto:sales@npartnertech.com)

