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
1. NXLog	3
1.1 NXLog 架構	. 3
1.2 NXLog 安裝	. 4
1.3 NXLog 設定檔	. 5
1.4 NXLog 啟動服務	. 8
2. Windows	9
2.1 群組原則	. 9
2.1.1 網域	. 9
2.1.2 單機	17
2.2 稽核資料庫檔案夾	20
3. SQL 2008	24
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
4. SQL 2012	48
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
5. SQL 2014	72
- 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
6. SQL 2016	95
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1	03
6.3 稽核資料庫層級1	11
7. SQL 20191	20

7.1	稽核登入	120
7.1.	1 使用指令介面方式設定	120
7.1.	2 使用圖形介面方式設定	123
7.2	稽核伺服器層級	128
7.3	稽核資料庫層級	136
8. N	I-Reporter	145
8.1	MS SQL	145
8.2	Windows	147



pyright © All rights are reserved by N-Partner Technologies Co



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: <u>https://docs.microsoft.com/zh-tw/sql/database-engine/configure-windows/c2-</u> audit-mode-server-configuration-option?view=sql-server-ver15

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

設定登入稽核:<u>https://docs.microsoft.com/zh-tw/sql/ssms/configure-login-auditing-sql-server-</u>

management-studio?%20view=sql-server-2017&view=sql-server-ver15#SSMSProcedure

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

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

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





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

伊 NXLog-CE Setup	-		×
Ready to install NXLog-CE			
Click Install to begin the installation. Click Back to review or change ar installation settings. Click Cancel to exit the wizard.	ny of you	ır	
Back Install		Cance	el

(3) 下載並覆蓋 NXLog 設定檔

下載連結 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'

🔀 Administrator: Windows PowerShell	3 <u>.</u>		×
PS C:\Users\Administrator\Downloads> <mark>Copy-Item</mark> nxlog_SQLserver.conf 'C:\Program Files (x86)\nxlog\con PS C:\Users\Administrator\Downloads> _	f∖nxl	og.conf'	0





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
_ogFile %LOGFILE%
Vloduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
加載模組 xm_syslog
<extension syslog=""></extension>
Module xm_syslog
Windows File 事件記錄
<input in_eventlog=""/>
Module im_msvistalog
ReadFromLast TRUE
SavePos TRUE
Query <querylist> \</querylist>
<query id="0"> \</query>
<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 192.168.3.5

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

🔼 Adm	inistrator: Windo	ws PowerShell	_		×
PS C:\Us PS C:\Us	ers\Administ ers\Administ	rator\Downloads> <mark>Start-Service</mark> nxlog rator\Downloads> <mark>Get-Service</mark> nxlog			^
Status	Name	DisplayName			
Running	nxlog	nxlog			
PS C:\Us 2019-02- PS C:\Us	ers\Administ 12 17:09:34 ers\Administ	rator\Downloads> Get-Content 'C:\Program Files (x86)\nxlog\ INFO nxlog-ce-2.10.2150 started rator\Downloads> _	data∖nx	log.lo	g' ¥





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

Active Directory Users	and Computers					—		×			
File Action View H	lelp										
🗢 🔿 🖄 🖬 📋	🗐 🖸 🗟 🔽 🗊	1 🙁 🐮 🕯	17	2 %							
Active Directory Users Saved Queries Saved Queries Saved Queries Builtin Built	and Computers Na Delegate Control Find Change Domain Change Domain Con Raise domain functi Operations Masters.	me Builtin ntroller onal level	Type built	inDomain niner nizational niner nizational nizational	Description Default container for o Default container for o Default container for o Default container for o Default container for o	upgradeo domain o security i manageo upgradeo	d comp controll dentifie d service d user a	uter acco lers ers (SIDs) ; e account accounts			
	New		>	Comp	uter						
	All Tasks		>	Conta	ct						
	View			View >			Group				
	Refresh			InetOr	gPerson						
	Export List			msDS-	-ShadowPrincipalContai	iner					
	Properties			msima	aging-PSPs						
	Properties			Organ	izational Unit						
	Help			Printer	r						
				User							
<	> <			Shared	l Folder			>			
Create a new object											



輸入 Name(組織單位名稱): Servers -> 按下 OK(確定)

New Object - Organizational Unit						
Create in: npartner.local/						
Name:						
Servers						
✓ Protect container from accidental deletion						
OK Cancel Help						

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

Active Directory Users and Complexity		x i		
File Action View Help				
🗢 🔿 🖄 🖬 🖌 🖬	1 🗟 🔒 🛛	🗖 🕺 🐉 🛅 🦷	7 🖻	٤.
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers Signature Accourties Managed Service Accourties Servers Users Users	Name WIN2019	Type Computer Add to a group Disable Account Reset Account Move Manage All Tasks Cut Delete) >	ription
	<	Halp		3
Moves the current selection to anothe	er organizationa	пер		



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)...

📓 Group Policy Management			— (⊐ ×
📓 File Action View Window Help				_ & ×
🔶 🖄 🛅 📋 🗙 🗐 🖓 📷				
Image: Second Policy Management Image: Second Policy Management Image: Policy Management	Servers Linked Group Policy Objects	Group Policy Inheritance GPO	Delegation Enforced	Link Ena
Help				
	· · · · · · · · · · · · · · · · · · ·			>
Create a GPO in this domain and link it to this container				





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

New GPO	×
<u>N</u> ame:	
N-Partner Policy	
Source Starter GPO:	
(none)	~
	OK Cancel

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

🔜 Group Policy Management						—	o x
📓 File Action View Window Help							_ 8 ×
🗢 🔿 🙍 📰 📋 🗙 🗒 🝳 📝 📷							
Group Policy Management Group Policy Management Group Policy Management Group Policy Domain Policy Group Policy Object Group Policy Object Group Policy Object Group Policy Modeling Group Policy Results New W Delete Renam Refrest Help	ed nablect /indov	Serve	ers I Group Policy O Link Orde 1	bjects	Group Policy Inheritance GPO N-Partner Policy	Delegation Enforced No	Link Ena Yes
Open the GPO editor							



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



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





開啟 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。

			-	
70	[] file:///C:/tmp/SQL2019.1	htm 🎾 🔻 🖉 🥔 NPARTNER\W	IN2019 ×	66 57 88 9
		Group Policy Results		
NPART Data collec	NER\WIN2019 cted on: 2/13/2019 3:35:18 PM			show all
Summary				show
Computer	Details			hida
General				nice
Compone	nt Status			snow
Settings				show
Policies				<u>hide</u>
1 Olicicas				hide
windo	ws Settings			<u>hide</u>
Secu	inty Settings			<u>hide</u>
Ac	count Policies/Password Polic	Ϋ́		show
Ad	count Policies/Account Locko	ut Policy		show
Lo	cal Policies/Audit Policy			hide
	Policy	Setting	Winning GPO	
	Audit object access	Success, Failure	N-Partner Policy	
Lo	cal Policies/Security Options			show
Р	ublic Key Policies/Certificate S	ervices Client - Auto-Enrollment Set	lings	<u>chow</u>
Р	ublic Key Policies/Encrypting F	ile System		snow
A	Ivanced Audit Configuration			show
Group Po	licy Objects			show
WMI Filter	re			show
WIND FILLES	0			show
User Detai	s			





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

=		Ľ	\$ <u>\$</u>			Filters \checkmark
ធ	Best n	natch				
		Edit gr Control	oup policy panel			
ŝ						
	و کر	roup po	blicy			
	ρ		ê 📮			



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







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)					
Image: Share File Home Share View				- 0	× ^ (?)
Share Email Zip Send	dvanced sharing 🛊 Remove access Share with	Advanced security			
← → × ↑ 📙 « Program Files > Mic	rosoft SQL Server > MSSQL15.	MSSQLSERVER > MSSQL	~ ē	Search MSSQL	P
🏪 Local Disk (C:)	^ Name ^	Date modified	Туре	Size	
PerfLogs	Backup	4/17/2019 9:55 AM	File folder		
Program Files	Binn	4/17/2019 9:55 AM	File folder		
Common Files	DATA	4/17/2019 10:42 AM	File folder		
internet explorer	h Install	4/17/2019 9:54 AM	File folder		
Microsoft Analysis Services	JOBS	4/17/2019 9:55 AM	File folder		
Microsoft SQL Server	Log	4/17/2019 10:32 AM	File folder		
80	Sql_engine_core_	_inst_keyfile.dll 3/16/2019 2:49 PM	Application exten	s 104 K	В
90					
110					
150					
Client SDK					
MSSOL 15 MSSOL SERVER					
MSSOL					
Backup					
Binn					
DATA					
7 items 1 item selected	v			F	
riteriis riteriiserecteu					



點選 Auditing(稽核) 頁面 -> 按下 Add(新增)

Advanced Se	curity Settings for [ATA		-		>
Name:	C:\Program Files	s\Microsoft SQL Server\M	ISSQL15.MSSQLSERVER\MSSQL\DATA			
Owner:	Administrators (WIN2019\Administrators)	🗣 Change			
Permissions	Auditing	Effective Access				
For additional Auditing entrie	information, doub	le-click an audit entry. To	modify an audit entry, select the entry	y and click Edit (if availal	ble).	
-						
Туре	Principal	Access	Inherited from	Applies to		
Туре	Principal	Access	Inherited from	Applies to		
Туре	Principal	Access	Inherited from	Applies to		
Туре	Principal	Access	Inherited from	Applies to		
Туре	Principal	Access	Inherited from	Applies to		
Туре	Principal	Access	Inherited from	Applies to		
Type	Principal	Access	Inherited from	Applies to		
Type Add Enable inhe	Principal Remove	Access	Inherited from	Applies to		
Add Enable inhe	Principal Remove eritance child object auditin	Access View	auditing entries from this object	Applies to		



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)

Auditing E	ntry for DATA							_	0		Х
Principal: Type: Applies to:	Everyone Select a prince All This folder, subfolders ar	ipal Id files	~								
Basic permi	ssions: Full control Modify Read & execute List folder contents Read Write Special permissions ly these auditing settings t	o objects and/or contai	iners withi	in this conta	ainer		SI	how advan	ced per	rmissio ear all	ons
		-									
							[ОК		Canc	el



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)

Advanced Se	curity Settings for DATA			-	- 🗆	×
Name: Owner:	C:\Program Files\Mid	crosoft SQL Server\MSSQL15.MS 2019\Administrators) 🛭 😯 Chan	SSQLSERVER\MSSQL\DATA			
Permissions	Auditing Eff	fective Access				
For additional Auditing entri	information, double-cli es:	ick an audit entry. To modify an	audit entry, select the entry ar	nd click Edit (if availa	ble).	
Туре	Principal	Access	Inherited from	Applies to		
Success	Everyone	Full control	None	This folder, su	bfolders an	d files
۲						>
Add	Remove	Edit				
Enable inh	eritance					
✓ Replace all	child object auditing en	tries with inheritable auditing er	ntries from this object			
				OK Cance	A	pply





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



使用 sp_configure 列出進階選項

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



啟用通用條件合規性

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



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





重新啟動 MSSQLSERVER 服務

輸入 net stop MSSQLSERVER && net start MSSQLSERVER

Administrator: Command Prompt	_		\times
C:\Users\Administrator>net stop MSSQLSERVER && net star The following services are dependent on the SQL Server Stopping the SQL Server (MSSQLSERVER) service will also	t MSSQLSERVER (MSSQLSERVER) stop these s	service	^ 2.
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 succes	sfully.		
The SQL Server (MSSQLSERVER) service is starting The SQL Server (MSSQLSERVER) service was started succes	sfully.		
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)

J Connect to Server	×
SQL S	Server 2008
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	•••••
	Remember password
Connect	Cancel Help Options >>





5 Microsoft SQL Server Manageme	ent — 🗆 🗙
File Edit View Tools Windo	ow Community Help
🔛 New Query 📑 📸 📸	🕞 💕 🖬 🚳 🔤 🖕
Object Explorer 🛛 👻 🕂 🗙	(
Connect 🕶 📑 📑 🛒 🔳 🐺 🛃	5
😑 💦 . (SQL Server 10.0.1600 - sa)	
🕀 🚞 Databases	Connect
Security	Disconnect
	Register
🕀 🧰 Management	New Query
🗄 📸 SQL Server Agent	Activity Monitor
	Start
	Stop
	Pause
	Resume
	Restart
	Policies
	Facets
	Start PowerShell
	Reports +
	Refresh
	Properties
Ready	.:



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	用通用條件領	合規性) ->	按下	OK(確定)	
--	--------------------	----	--------	--------	----------	--------------	--------	--------------------	----	----------------	--

Server Properties - WIN2019)	_		×
Select a page General	🖾 Script 🔻 📑 Help			
Memory Processors Security Connections Database Settings Advanced Permissions	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proxy account Enable server proxy account			
Connection	Password:			
Server: Connection: sa View connection properties Progress Ready	Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining			
		ОК	Canc	el .

按下 OK(確定)

Microsoft	SQL Server Management Studio	×
1	Some of your configuration changes will not take effect until SQL Server is restarted.	
₽ <u></u>		ОК

Copyright © All rights are reserved by N-Partner Technologies Co

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

Microsoft SQL Server Management Studio						
?	Are you sure you want to restart the MSSQLSERVER service on WIN2019?					
E)		Yes	No			





按下 Yes(是) 停止 SQLSERVER Agent







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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

J Connect to Server		\times							
SQL Server 2008									
Server type:	Database Engine	~							
Server name:	localhost	~							
Authentication:	SQL Server Authentication	~							
Login:	sa	~							
Password:	******								
	Remember password								
Connec	t Cancel Help Opti	ons >>							

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

😓 Create Audit						×
🕕 Ready						
Select a page	🔄 Script 🕞 📑 Hel	p				
🚰 General						
	Audit name:	NP_Audit				
	Queue delay	1000				-
Shut down server on audit log failure						
	Audit	Application Log				~
	File path:					
	Maximum	2147483647				
		✓ Unlimited				
	Maximum file	0	• MB	⊖ GB	🔿 тв	
		✓ Unlimited				
	Reserve dis	cspace				
Connection						
📑 . [sa]						
View connection properties						
Progress						
Oone Done						
		ОК	Cance	el	Help	

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)






按下 Close(關閉)

<u>م</u>

🔍 Enable Audit				-		×
Success	1	Total Succe	ess	0 0	Error Warning	
Action Enable Audit 'NP_Audit'			Status Success		Message	
					Clos	e

Copyright © All rights are reserved by N-Partner Technologies Co

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







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)

😓 Create Server Audit Specification									- [I X	
🕕 Ready											
Select a page	Script	🕶 📑 Help									
🚰 General	General										
	Name:		NP_Server_Audit								
	Audit:		NP_Audit								
	Action	5:									
		Audit Action Ty	pe		Object Class	Object Schema	Object Name		Principal Name		
	01	DATABASE_ROLE_MEMBER_CHAN	GE_GROUP	\sim	~						
	02	SERVER_ROLE_MEMBER_CHANGE_	GROUP	\sim	~						
	03	DATABASE_PERMISSION_CHANGE	_GROUP	\sim	~						
	04	DATABASE_CHANGE_GROUP		\sim	~						
	05	DATABASE_PRINCIPAL_CHANGE_G	ROUP	\sim	~						
	06	SERVER_PRINCIPAL_CHANGE_GRO	UP	\sim	~						
	07	APPLICATION_ROLE_CHANGE_PAS	SSWORD_GROUP	\sim	~						
	08	LOGIN_CHANGE_PASSWORD_GRO	UP	\sim	~						
	▶ 09	APPLICATION_ROLE_CHANGE_PAS	SSWORD_GROUP	\sim	~						
	*10			\sim	~						
Connection											
-51 . [20]											
View connection properties											
Progress											
Ready											

								_			
							ок		Cancel H	elp	



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)

¢¢

Microsoft SQL Server Management	Studio	—		Х
File Edit View Project Debug	Tools Window	Community	Help	
🕄 New Query 👔 📸 📸 🕻	s 🗃 🖬 🕘 🌉	=		
Object Explorer 🛛 👻 🕂	K			
Connect - 📑 📑 🖉 🔳 🝸 🛃				
🖃 🐻 . (SQL Server 10.0.1600 - sa)				
🕀 🧰 Databases				
🖃 🚞 Security				
🕀 🧰 Logins				
🕀 🧰 Server Roles				
🕀 🧰 Credentials				
🕀 🚞 Cryptographic Providers				
🖃 🚞 Audits				
🔍 NP_Audit				
Server Audit Specification	s			
🗟 NP_Server_Audit				
🕀 🚞 Server Objects	New Server Audit S	pecification		
🕀 🚞 Replication	Enable Server Audit	Specification		
🕀 🚞 Management		1		
🗄 📸 SQL Server Agent	Script Server Audit S	Specification a	s 🕨	
	Policies		- - - -	
	Facets			
	Start PowerShell			
	Reports		•	
	Delete			
	Refresh			
	Properties			
Ready				





按下 Close(關閉)

🗟 Enable Server Audit Specification			-		×
Success Details:	1 Total 1 Succe	0	Error Warning		
Action	Specificati	Status		Message	
	peonodi	0000000			
				Clos	e





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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

		////COU(Æ)
J Connect to Server		×
SQL	Server ⁻ 2008	
Server type:	Database Engine	~
Server name:	localhost	~
Authentication:	SQL Server Authentication	~
Login:	sa	~
Password:		
	Remember password	
Connec	t Cancel Help Opti	ons >>

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

🐙 Create Audit				_		×
🕕 Ready						
Select a page General	🔄 Script 🕞 📑 Hel	р				
	Audit name:	NP_Audit				
	Queue delay	1000				* *
	Shut down	server on audit log failure				
	Audit	Application Log				~
	File path:					
	Maximum	2147483647				*
		🗹 Unlimited				
	Maximum file	0	• MB	⊖ GB	🔿 тв	
		🗹 Unlimited				
	Reserve dis	k space				
6						
Isa]						
View connection properties						
Progress						
Oone Done						
		ОК	Cance	el	Help	

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)







按下 Close(關閉)

<u>م</u>

🔍 Enable Audit				-		×
Success	1 1	Total Succe	ess	0 0	Error Warning	
Details:						
Action			Status		Message	
📀 Enable Audit 'NP_Audit'			Success			
					Clos	e

Copyright © All rights are reserved by N-Partner Technologies Co

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

·				
💺 Microsoft SQL Server Management Studio		_		×
File Edit View Project Debug Tools Wind	ow Community	Help		
🗄 🔔 New Query 🛅 📸 📸 🖏 📑 😂 🔙 🍏	🕰 ₊			
Object Explorer 🛛 🗸 🗸				
Connect 🕶 📑 📑 🖉 🖉 📓				
□ 10.0.1600 - sa) □ 10.0.1600 - sa) □ 10.0.1600 - sa)				
🕀 🚞 System Databases				
🕀 🧰 Database Snapshots				
🖃 📔 NCloud				
🕀 🚞 Database Diagrams				
🕀 🧰 Tables				
🕀 🧰 Views				
🕀 🚞 Synonyms				
🕀 🚞 Programmability				
🕀 🚞 Service Broker				
🕀 🧰 Storage				
🖃 🚞 Security				
⊕ 📴 Users				
🕀 🚞 Schemas				
🕀 🚞 Asymmetric Keys				
🕀 🚞 Certificates				
🕢 🧰 Symmetric Keys				
🚞 Database Audit Specifications	New Database A	udit Specific	ation	
🕀 🤖 Seculity				_
🕀 🧰 Server Objects	Filter			•
🕀 🧰 Replication	Start PowerShell			
🕀 🧰 Management				
🗄 📸 SQL Server Agent	Reports			•
	Refresh			
Ready				
*				

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

Ō





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)

🖳 Create Database Audit Specifi	ication							-		×
🕕 Ready										
Select a page	Script	🕶 [🔂 Help								
🚰 General										
	Name	:	NP_DB-NC	Cloud_Audit						
	Audit		NP_Audit							~
	Actio	ns:								
		Audit Action Type		Object Class	Object Schema	Object Name	Principal Nar	ne		
	1	APPLICATION_ROLE_CHANGE_PASSWORD_GR	OUP 🗸	~						
Connection	2	BACKUP_RESTORE_GROUP	~	~						
, [sa]	3	DATABASE_ROLE_MEMBER_CHANGE_GROUP	~	~						
	4	SCHEMA_OBJECT_CHANGE_GROUP	~	~						
View connection properties	▶#5		~	~						
Progress										
Ready										
							OK Canc	el	Help	



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)

💺 Microsoft SQL Server Management Studio	– 🗆 X
File Edit View Tools Window Com	munity Help
😫 New Query 📑 📑 📸 🌇 📄	J 🕘 🏧 🛓
Object Explorer 🛛 👻 📮	×
Connect - 📑 🛃 🔳 🝸 🛃 🍒	
🖃 🐻 . (SQL Server 10.0.1600 - sa)	
🖃 🚞 Databases	
🕀 🚞 System Databases	
🕀 🚞 Database Snapshots	
🖃 🔰 NCloud	
🕀 🧰 Database Diagrams	
Views	
🗄 🦲 Synonyms	
Programmability Septice Broker	
Geeding Geeding Geeding Geeding Geeding	
🐨 🧰 Schemas	
🗉 🚞 Asymmetric Keys	
🕀 🧰 Certificates	
🕀 🧰 Symmetric Keys	
🖃 🚞 Database Audit Specificati	ions
📆 NP_DB-NCloud_Audit	
	New Database Audit Specification
Server Objects Deplication	Enable Database Audit Specification
	Script Database Audit Specification as
🗄 📸 SQL Server Agent	Policies
	Facets
	Start PowerShell
	Reports +
	Delete
	Refresh
	Properties
Ready	





按下 Close(關閉)

🔯 Enable Database Audit Specification			-		×
Success	1 Total 1 Succe	0 0	Error Warning		
Details: Action		Status		Message	
Enable Database Auc	lit Specifi	Success		_	
				Clos	е
				<u> </u>	





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



使用 sp_configure 列出進階選項

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



啟用通用條件合規性

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



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





重新啟動 MSSQLSERVER 服務

輸入 net stop MSSQLSERVER && net start MSSQLSERVER

Administrator: Command Prompt	—		\times
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLS The following services are dependent on the SQL Server (MSSQLSE Stopping the SQL Server (MSSQLSERVER) service will also stop th	ERVER RVER) ese se	service rvices.	^ -
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 successf	ully.		
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)

~
~
~
~
Options >>



Microsoft SQL Server Management Stud	io (Admin — 🗆 🗙	
File Edit View Debug Tools Window <td <<="" td=""><td>w Help</td></td>	<td>w Help</td>	w Help
Object Explorer Image: Connect Imag	X Connect Disconnect Register New Query Activity Monitor Start Stop Pause Resume Restart Policies Facets Start PowerShell Reports Refresh Properties	
Ready		

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

Server Properties - WIN2019)			×
Select a page General Memory Processors Security Connections Database Settings Advanced Permissions	Script			
Connection Server: WIN2019 Connection: sa View connection properties Progress Ready	Proxy account: Password: Options □ Enable Common Criteria compliance □ Enable C2 audit tracing □ Cross database ownership chaining			
		ОК	Cance	

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)

<u>م</u>

Microsoft	SQL Server Management Studio	×
1	Some of your configuration changes will not take effect until SQL Server is restarted.	
₿ a		ОК

Copyright © All rights are reserved by N-Partner Technologies Co

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)
Server Management Stud	dio (Ad	dmin — 🗆	×
File Edit View Debug Tools Windo	w H	lelp	
🗄 🚰 🕶 👻 📁 📁 🍠 🗎 🤔 New Query	D	🔁 🔁 🍒 🕹 🔁 🔁	÷ Ŧ
Object Explorer 👻 🖣	I X		
Connect 🕶 🛃 🔳 🍸 😰 🎿			
WIN2019 (SQL Server 11.0.2100 - sa)			
Databases		Connect	
Security Server Objects		Disconnect	
		Register	
🗉 🚞 AlwaysOn High Availability		New Query	
Management Integration Services Catalogs		Activity Monitor	
🕀 📸 SQL Server Agent		Start	
		Stop	
		Pause	
		Resume	
		Restart	
		Policies 🕨	
		Facets	
		Start PowerShell	
		Reports +	
		Refresh	
		Properties	
Ready			.:

按下 Yes(是) 重新啟動 MSSQLSERVER 服務

Microsoft	SQL Server Management Studio		
?	Are you sure you want to restart the MSSQLSERVER service on WIN2019?		
E)		Yes	No





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

SQL Ser	ver "2012
Server type:	Database Engine \sim
Server name:	localhost ~
Authentication:	SQL Server Authentication $\qquad \lor$
Login:	sa 🗸 🗸
Password:	•••••
	Remember password
Connect	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

y Create Audit		– 🗆 X
🕕 Ready		
Select a page General	🕵 Script 🕞 📑 Help	
🚰 Filter	Audit name:	NP_Audit
	Queue delay (in milliseconds):	1000
	On Audit Log Failure:	 Continue Shut down server
	Audit	Fail operation
	destination:	Application Log V
	File path:	
	Audit File Maximum Limit:	 Maximum rollover files: Unlimited
		O Maximum files:
		Number of files: 214/48304/
	Maximum file	0
Connection	SIZE.	Unlimited
■ WIN2019 [sa]	Reserve disk sp	bace
View connection properties		
Progress		
Ready		
		OK Cancel Help

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)





Kicrosoft SQL Server Manage	ment Studio (Admin — 🗆 🗙
File Edit View Debug Tool	s Window Help
i 🛅 🕈 🔤 🕈 💕 📓 🎒 🔔 N	ew Query 📑 📸 📸 🕉 🕹 🛍 🛍 🗒
Object Explorer	▼ ₽ ×
 WIN2019 (SQL Server 11.0 	2100 - sa)
 	viders
🕀 🧰 Server Audit S	New Audit
⊕	Enable Audit
⊕ 🧰 AlwaysOn High A ⊕ 🚞 Management	Script Audit as
	Policies
	Facets
	Start PowerShell
	Reports
	Rename
	Delete
	Refresh
Ready	Properties
Keauy	

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

Create Server Audit Specifica	tion						_	
Ready								
ect a page	Script	🕶 🕼 Help						
General								
	Name:	NP_Server_Audit						
	Audite	NP Audit						
	Addit							
	Action	5:						
		Audit Action Type		Object Class	Object	Object Name	Princi	pal
	01	DATABASE_ROLE_MEMBER_CHANGE_GROUP	\sim	~				
	02	SERVER_ROLE_MEMBER_CHANGE_GROUP	\sim	~				
	03	DATABASE_LOGOUT_GROUP	\sim	~				
	04	DATABASE_PERMISSION_CHANGE_GROUP	\sim	~				
	05	DATABASE_CHANGE_GROUP	\sim	~				
nection	06	DATABASE_PRINCIPAL_CHANGE_GROUP	\sim	~				
WIN2019 [sa]	07	SERVER_PRINCIPAL_CHANGE_GROUP	\sim	~				
	08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	\sim	~				
	09	LOGIN_CHANGE_PASSWORD_GROUP	\sim	~				
w connection properties	10	DATABASE_OWNERSHIP_CHANGE_GROUP	\sim	~				
	▶ 11	USER_CHANGE_PASSWORD_GROUP	\sim	~				
jress	• 12		\sim	~				
Ready								
10.0								
						OK Can	cel	Help

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)

φ**.**

💺 Microsoft SQL Server Management S	Studio (Administrator) — 🗆 🗙
File Edit View Debug Tools Win	ndow Help
🗄 🛅 🕶 🗃 🛩 🎯 🔙 🎒 😫 New Qu	ery 🗋 📸 📸 👗 👗 🛍 🛍 🔊 - 🚆
Object Explorer	<mark>▼ </mark>
Connect 🕶 📑 📑 🔳 🖉 🛃	
 WIN2019 (SQL Server 11.0.2100 - Databases Security Logins Server Roles Credentials Cryptographic Providers Audits 	sa)
🔍 NP_Audit 🖃 🛅 Server Audit Specification	ns
🗟 NP_Server_Audit	
🕀 🧰 Server Objects	New Server Audit Specification
Constant Constant	Enable Server Audit Specification
	Script Server Audit Specification as
	Policies Facets
	Start PowerShell
	Reports
	Delete
	Refresh
Ready	Properties





按下 Close(關閉)

🗟 Enable Server Audit Specification			-		×
Success Details:	1 Total Success 1 Success				
Action		Status		Message	
Enable Server Audit \$	Specificati	Success			
				Clos	e





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(±/(). Sa An I		Juneor(Æ]
Connect to Server		×
SQL Ser	'Ver ''2012	
Server type:	Database Engine	~
Server name:	localhost	~
Authentication:	SQL Server Authentication	~
Login:	sa	~
Password:	•••••	
	Remember password	
Connec	t Cancel Help Opt	ions >>

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

y Create Audit		– 🗆 X
🕕 Ready		
Select a page General	🔄 Script 🕞 📑 Help	
🚰 Filter	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:
	Maximum file	
Connection	3120	✓ Unlimited
■ WIN2019 [sa]	Reserve disk sp	ace
View connection properties		
Progress		
Ready		i
		OK Cancel Help

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)





Kicrosoft SQL Server Manage	ement Studio (Admin — 🗆 🗙
File Edit View Debug Tools	ls Window Help
🗄 🖥 🕈 🔤 🕈 💕 📓 🎒 🔔 Ne	lew Query 📑 📸 📸 🍒 🕹 🛍 🚆
Object Explorer	▼
 WIN2019 (SQL Server 11.0 	0.2100 - sa) oviders
🕀 🧰 Server Audit S	New Audit
Server Objects Replication AlwaysOn High A AlwaysOn High A Integration Servic SQL Server Agent	Enable AuditView Audit LogsScript Audit asPoliciesFacetsFacetsStart PowerShellReportsRenameDeleteRefresh
Ready	Properties

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)...

Ŷ

Microsoft SQL Server Management Studio (Administrator) - 🗆 🗙
File Edit View Debug Tools Window Help
🗄 🏹 🕶 🖅 📁 📁 💭 🎒 🔔 New Query 📑 📸 📸 🍒 🔺 🛍 📇 🔊 – (** – 💭 – 🔍 🖉
Object Explorer T A X
$Connect \star \exists z \equiv \forall z \equiv \forall z$
□
Databases
🕀 🛅 System Databases
🕀 🛅 Database Snapshots
🕀 🧰 Database Diagrams
🕀 🧾 Tables
Programmability
🕀 🚞 Storage
😑 🚞 Security
⊕ ¹
Roles
🕀 🧾 Schemas
Asymmetric Reys
Symmetric Keys
Database Audit Specifications New Database Audit Specification
Replication Start PowerShell
H
Integration Services Catalogs Refresh
⊞ SQL Server Agent
Ready





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)

Create Database Audit Specific	ation							-	- 🗆	×
🕕 Ready										
Select a page	2	Script	🕶 📑 Help							
🚰 General										
	Name: Audit:		NP_DB-NCloud_Audit	NP_DB-NCloud_Audit						
			NP_Audit					``		
		Action	is:							
			Audit Action Type		Object Class	Object Schema	Object Name	Princi	pal Name	
		1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	\sim	~					
Connection		2	BACKUP_RESTORE_GROUP	\sim	~					
📑 WIN2019 [sa]		3	DATABASE_ROLE_MEMBER_CHANGE_GROUP	\sim	~					
	4	FAILED_DATABASE_AUTHENTICATION_GROUP	\sim	~						
	5	SCHEMA_OBJECT_CHANGE_GROUP	\sim	~						
View connection properties		6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	\sim	~					
Progress		>*7		\sim	~					
Ready										
							ОК	Cancel	Help	



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) Microsoft SQL Server Management Studio (Administrator) \times File Edit View Debug Tools Window Help 🗄 📅 🕶 🖅 📁 💭 💭 🎒 🔔 New Query 👘 📸 📸 🦓 🏭 🌡 🖬 🛍 🖉 🗸 🖓 🖉 🖉 🖉 🖉 **-** ₽ × Object Explorer Connect 🕶 🛃 🛃 🔳 🍸 🛃 🍒 WIN2019 (SQL Server 11.0.2100 - sa) 🖃 🚞 Databases 🗄 🚞 System Databases 🗄 🚞 Database Snapshots 🖃 间 NCloud 🗄 🚞 Database Diagrams 🕀 🚞 Tables 🕀 🚞 Views 🗄 🚞 Synonyms 🗄 🚞 Programmability 🗄 🚞 Service Broker 🗄 🚞 Storage E Security 🕀 🚞 Users 🗄 🚞 Roles 🗄 🚞 Schemas 🗄 🚞 Asymmetric Keys 🗄 🚞 Certificates 🗄 🚞 Symmetric Keys 🖃 🚞 Database Audit Specifications NP_DB-NCloud_Audit 🗄 🚞 Security New Database Audit Specification... 🗄 🚞 Server Objects Enable Database Audit Specification E Image: Explication
 E Image: Explication
 E Image: Explicit Action
 E Image: Explit Script Database Audit Specification as Þ 🗄 🚞 AlwaysOn High Availability 🕀 🚞 Management Policies ۲ Integration Services Catalogs Facets 🗄 📆 SQL Server Agent Start PowerShell Reports ۲ Delete Refresh Properties Ready




按下 Close(關閉)

Enable Database Aud	lit Specificat	ion	-		×
Success	1 Total 1 Success		0 0	Error Warning	
Action Chable Database Aud	lit Specifi	Status Success		Message	_
				Clos	е





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



使用 sp_configure 列出進階選項

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



啟用通用條件合規性

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



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





重新啟動 MSSQLSERVER 服務

輸入 net stop MSSQLSERVER && net start MSSQLSERVER

Administrator: Command Prompt	_		\times
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSE The following services are dependent on the SQL Server (MSSQLSER Stopping the SQL Server (MSSQLSERVER) service will also stop the	RVER (VER) se se	service rvices	• •
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 successfu	lly.		
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)

Dented to Server	Connect to Server X					
Microsoft S	QL Server 2014					
Server type:	Database Engine 🗸 🗸					
Server name:	localhost ~					
Authentication:	SQL Server Authentication \sim					
Login:	sa 🗸					
Password:						
Remember password						
Connec	t Cancel Help Options >>					





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

|--|

Server Properties - WIN2019)	_		×
Select a page	🔄 Script 🔻 📑 Help			
Memory Processors Security Connections Database Settings Advanced Permissions	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proxy account Enable server proxy account			
Connection	Password:			
Server: WIN2019 Connection: sa View connection properties Progress Ready	Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining			
		ОК	Canc	el .

按下 OK(確定)

@

Microsoft	SQL Server Management Studio	×
1	Some of your configuration changes will not take effect until SQL Server is restarted.	
₿ a		ОК

Copyright © All rights are reserved by N-Partner Technologies Co

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

Microsoft	SQL Server Management Studio				
?	Are you sure you want to restart the MSSQLSERVER service on WIN2019?				
E <u>a</u>		Yes	No		





按下 Yes(是) 停止 SQLSERVER Agent







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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

Login(宜入): sa & Pas	sword(密碼): <i>npartner</i> -> 按下 C	onnect(建按				
Connect to Server		×				
Microsoft SQ	L Server 2014					
Server type:	Database Engine	~				
Server name:	localhost	~				
Authentication:	SQL Server Authentication	~				
Login:	sa	~				
Password:	•••••					
Remember password						
Connect	Cancel Help C	Options >>				

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

😓 Create Audit		- 🗆 X
🕕 Ready		
Select a page	🔄 Script 🕞 📑 Help	
Filter	Audit name: Queue delay (in milliseconds):	NP_Audit 1000
	On Audit Log Failure:	Continue Shut down server Fail operation
	Audit destination:	Application Log
	File path:	
	Maximum Limit:	Maximum rollover files: Unlimited Maximum files:
		Number of files: 2147483647
	Maximum file size:	
Connection		✓ Unlimited
📴 WIN2019 [sa]	Reserve disk sp	ace
View connection properties		
Progress		
Ready		
		OK Cancel Help

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)





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)					
Microsoft SQL Server Management Stu	dio (/	Administrator)	_		×
File Edit View Debug Tools Windo	ow	Help			
🗄 🛅 🕶 🖅 📂 💭 🎒 😫 New Query		📸 📸 👘	xee	り - (2 문
Object Explorer 🗸 🗸	ł×				
Connect 🕶 📑 🛃 🔲 🍸 🛃					
😑 🐻 WIN2019 (SQL Server 12.0.6024.0 - :	sa)				
🕀 🚞 Databases					
🖃 🚞 Security					
E D Logins					
Generation					
E Credentials					
Cryptographic Providers					
Contraction Contraction Contraction		New Server Au	dit Specificat	tion	
Server Objects					-
🕀 🚞 Replication		Filter			
AlwaysOn High Availability AlwaysOn High Availability		Start PowerShe	ell		
	Reports			•	
🕀 📸 SQL Server Agent		Refresh			
Ready					





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)

📡 Create Server Audit Specification — 🗆 🗙									
🕕 Ready									
Select a page	Script	🕶 🔀 Help							
	Name:	NP_Server_Audit							
	Audit:	NP_Audit							~
		Audit Action Type		Object Class	Object	Object Name	P	rincipal	
	01	DATABASE_ROLE_MEMBER_CHANGE_GROUP	~	~					
	02	SERVER_ROLE_MEMBER_CHANGE_GROUP	~	~					
	03	DATABASE_LOGOUT_GROUP	~	~					
	04	DATABASE_PERMISSION_CHANGE_GROUP		~			_		
Connection	05	DATABASE_CHANGE_GROUP	~	~					
WIN2010 [cal	06	DATABASE_PRINCIPAL_CHANGE_GROUP	~	~			_		
	07	SERVER_PRINCIPAL_CHANGE_GROUP	~	~					
	08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	~	~			_		
	09		~	~			_		
View connection properties	10		~	~			_		
Progress	• • •	USER_CHANGE_PASSWORD_GROUP	~	~			_		
Ready	* 12		×	×					
	1					OK Car	ncel	Help	





Server Audit Specification(啟用伺服器稽核規格)

Ō

Microsoft SQL Server Management Studio (Administrator) — 🛛 🗙						
File Edit View Debug Tools V	Vindow Help					
🗄 🛅 🕶 📨 🎽 📓 🎒 🔔 New C	Query 📑 📸 🌇 🕹 💺 🖿 📲 👘					
Object Explorer Connect ▼ Image:	▼ ₽ × 4.0 - sa)					
 □ Audits Q NP_Audit □ Server Audit Specificat □ NP_Server_Audit □ Server Objects 	ions New Server Audit Specification					
Replication	Enable Server Audit Specification					
 	Script Server Audit Specification as Policies Facets Start PowerShell					
	Reports					
	Delete					
	Refrech					
Ready	Properties					

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)

J Connect to Server	×						
Microsoft SQL Server 2014							
Server type:	Database Engine 🗸 🗸						
Server name:	localhost ~						
Authentication:	SQL Server Authentication \checkmark						
Login:	sa 🗸 🗸						
Password:							
	Remember password						
Connect 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		– 🗆 X
🕕 Ready		
Select a page General	🔄 Script 🕞 📑 Help	
🚰 Filter	Audit name: Queue delay (in milliseconds):	NP_Audit
	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 file	 Maximum files: Number of files: 2147483647 ▼ ● MB ○ GB ○ TB
Connection	ar 1 die Sect	✓ Unlimited
聾 WIN2019 [sa]	Reserve disk sp	ace
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)...

S Microsoft SQL Server Management Studio (Administr	ator)	– 🗆 ×
File Edit View Debug Tools Window Help		
🗄 🔚 🕶 📨 📂 🔙 🥔 🔔 New Query 📑 📸 📸	13 単品 の	- (*) - 🔍 - 🔍 -
WIN2019 (SQL Server 12.0.6024.0 - sa)		
Databases		
Database Snapshots		
□ □ NCloud		
🕀 🚞 Database Diagrams		
🕀 🧰 Tables		
🕀 🧰 Views		
🕀 🧰 Synonyms		
🕀 🧰 Programmability		
Service Broker		
scorage Security		
🕀 🧫 Roles		
🗄 🚞 Schemas		
🕀 🧰 Asymmetric Keys		
🕀 🚞 Certificates		
🕀 🧰 Symmetric Keys		
Database Audit Specifications	New Database Audit S	pecification
Security Security Security	Filter	•
🗄 🧰 AlwaysOn High Availability	Start PowerShell	
🗄 🧰 Management	Reports	•
🕀 🧰 Integration Services Catalogs	Refresh	
🗄 📸 SQL Server Agent		
Parata.		
Ready		



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):

🧏 Create Database Audit Specificat	ion								-		×
🕕 Ready											
Select a page	Script	Script 👻 🚺 Help									
🚰 General											_
	Nam	e	NP_DB-NCloud_	Audi	t						
	Audi	:	NP_Audit								~
	Actio	ns:			_						
		Audit Action Typ	e		Object Class	Object Schema	Object Name		Principal Name		
Connection	1	APPLICATION_ROLE_CHANGE_PASS	WORD_GROUP	\sim	~						
📲 WIN2019 [sa]	2	BACKUP_RESTORE_GROUP		\sim	~						
	3	DATABASE_ROLE_MEMBER_CHANGE	_GROUP	\sim	~						
View connection properties	4	FAILED_DATABASE_AUTHENTICATIO	N_GROUP	~	~						
	5	SCHEMA_OBJECT_CHANGE_GROUP		~	~						
Progress	▶ 6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP] ~		~							
Ready	•7			\sim	~						
Ready											
								ОК	Cancel	Help	

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 Database Audit Specifications name(資料庫稽核規格名稱): NP_DB-NCloud_Audit -> 點選 Enable Database

Microsoft SQL Server Management Studio (Administrator) × File Edit View Debug Tools Window Help i 🛅 • 🔠 - 📂 🔚 🍠 🔔 New Query 📑 🐴 🐴 🌇 👗 🕨 🛍 🖄 🖉 - 🔍 - 🚚 - 🖳 🍟 - 4 × **Object Explorer** Connect 🕶 🛃 📑 👕 🏹 🛃 WIN2019 (SQL Server 12.0.6024.0 - sa) 😑 🚞 Databases 🗄 🚞 System Databases 🗄 🚞 Database Snapshots 🖃 📔 NCloud 🗄 🚞 Database Diagrams 🕀 🚞 Tables 🗉 🚞 Views 🗄 🚞 Synonyms 🗄 🚞 Programmability 🗄 🚞 Service Broker 🕀 🚞 Storage E Security 🗄 🚞 Users 🕀 🚞 Roles 🗄 🚞 Schemas 🗄 🚞 Asymmetric Keys 🗄 🚞 Certificates 🗄 🚞 Symmetric Keys 🖃 🚞 Database Audit Specifications and the second s New Database Audit Specification... 🕀 🚞 Server Objects Enable Database Audit Specification E Image: Explication
 E Image: Explication
 E Image: Explicit Action
 E Image: Explit Script Database Audit Specification as 🗄 🚞 AlwaysOn High Availability ۲ 🗄 🚞 Management Policies ۲ Integration Services Catalogs Facets 🗄 📸 SQL Server Agent Start PowerShell Reports ۲ Delete Refresh Properties Ready

Audit Specification(啟用資料庫稽核規格)

Copyright © All rights are reserved by N-Partner Technologies Co



按下 Close(關閉)

🛃 Enable Database Audit Specification			-		×
Success Details:	1 Total 1 Succe	0	Error Warning		
Action Action Enable Database Au	dit Specifi	Status Success		Message	
				Clos	e .





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



Copyright © All rights are reserved by N-Partner Technologies Co

輸入 use master -> go



使用 sp_configure 列出進階選項

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



啟用通用條件合規性

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



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





重新啟動 MSSQLSERVER 服務

輸入 net stop MSSQLSERVER && net start MSSQLSERVER

Administrator: Command Prompt	_		\times
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLSE The following services are dependent on the SQL Server (MSSQLSE Stopping the SQL Server (MSSQLSERVER) service will also stop the	ERVER RVER) ese se	services	e.
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 successfu	ully.		
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)

다. Connect to Server	×
	SQL Server
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	
	Remember password
	Connect Cancel Help Options >>





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

<u>م</u>



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

				V
Server Properties - WIN2019		_		X
Select a page General Memory Processors Security Connections Database Settings Advanced Permissions	 ✓ Script ▼ ♥ Help Server authentication ○ Windows Authentication mode ● SQL Server and Windows Authentication mode Login auditing ○ None ○ Failed logins only ○ Successful logins only ● Successful logins only ● Both failed and successful logins 			
Connection Server: WIN2019 Connection: sa If we connection properties Progress Ready	Enable server proxy account Proxy account: Password: Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining			
The Bar		ок	Can	cel

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)

Microsof	it SQL Server Management Studio	×
1	Some of your configuration changes will not take effect until SQL Server is restarted.	
B		ОК



重新啟動 MSSQLSERVER 服務

۹Ŵ



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



Copyright © All rights are reserved by N-Partner Technologies Co



按下 Yes(是) 停止 SQLSERVER Agent

Microso	ft SQL Server Management Studio
?	Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?
E)	Yes No





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)

모 ^를 Connect to Server	×
	SQL Server
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	
	Remember password
	Connect 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)...



Ō



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

灵 Create Audit	— 🗆 🗙	
Ready		
Select a page	🗊 Script 👻 😧 Help	
Filter	Audit name: NP_Audit Queue delay (in milliseconds): 1000 On Audit Log Continue Failure: Shut down server Fail operation Audit destination: Application Log File path: Maximum Limit: Maximum rollover files: Unlimited Maximum files: Number of files: 2147483647 Maximum file size: Unlimited Maximum file Unlimited 	
Connection v∰ WIN2019 [sa]		
View connection properties		
Progress		
Ready		
	OK Cancel Help]

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)



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)

🔎 Enable Audit				—			Х
Success	1 1	Total Succe	ss		0 0	Error Warning	
Details:							
Action			Status			Message	
Enable Audit 'NP_Audit'			Success				
						Close	;

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

			= ~L)	/					
🗜 Create Server Audit Specification — 🗆 🗙					×				
🕕 Ready									
Select a page	💭 Script	🕶 😮 Help							
🔑 General									
	Name:	NP_Server_Audit							
	Audit:	NP_Audit							~
	Actions:	:							
		Audit Action Type		Object Class	Object Schema	Object Name	Pri	incipal Name	
	01	DATABASE_ROLE_MEMBER_CHANGE_GROUP	\sim	~					
	02	SERVER_ROLE_MEMBER_CHANGE_GROUP	\sim	~					
	03	DATABASE_LOGOUT_GROUP	~	~					
	04	DATABASE_PERMISSION_CHANGE_GROUP	\sim	~					
-	05	DATABASE_CHANGE_GROUP	~	~					
Connection	06	DATABASE_PRINCIPAL_CHANGE_GROUP	\sim	~					
₩ WIN2019 [sa]	07	SERVER_PRINCIPAL_CHANGE_GROUP	\sim	~					
	08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	\sim	~					
	09	LOGIN_CHANGE_PASSWORD_GROUP	\sim	~					
View connection properties	10	DATABASE_OWNERSHIP_CHANGE_GROUP	\sim	~					
Progress	▶ 11	USER_CHANGE_PASSWORD_GROUP	\sim	~					
Ready	•12		~	~					
New Y									
						OK	Canad		In
						UK	Cance	I He	p .

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)

A

Microsoft SQL Server M Quick	Launch (Ctrl+Q)
File Edit View Debug Tools	Window Help
0 - 0 📅 - 🏪 - 💾 💾	B New Ouerv B A A A A A *
Object Explorer 🔹	т ×
Connect 🕶 🌹 🌹 🗏 🝸 🖒 🚸	
🖃 🐻 WIN2019 (SQL Server 13.0.5026.0	0 - sa)
🕀 📕 Databases	
🖃 📕 Security	
🕀 💼 Logins	
🕀 💼 Server Roles	
Credentials	
Cryptographic Providers	
Audits	
🖓 NP_Audit	nr.
Server Addit Specificatio	
Server Objects	New Server Audit Specification
E Replication	Enable Server Audit Specification
🕀 💼 PolyBase	Enable Server Addit Specification
🗉 📕 Always On High Availab	Script Server Audit Specification as
🕀 💼 Management	Policies
🕀 💼 Integration Services Cat	Fondes
🗄 🛃 SQL Server Agent	racets
🕀 🔄 XEvent Profiler	Start PowerShell
	Reports +
	Delete
	Refresh
	Properties
Ready	





按下 Close(關閉)

🔊 Enable Server Audit Specification					×
Success	1 Total 1 Success			Error Warning	
Details:					
Action		Status		Message	
Enable Server Audit Sp	ecification	Success			
				Close	;





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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

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

모 ^를 Connect to Server	×			
	SQL Server			
Server type:	Database Engine 🗸 🗸			
Server name:	localhost ~			
Authentication:	SQL Server Authentication \sim			
Login:	sa 🗸 🗸			
Password:				
	Remember password			
	Connect 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

规 Create Audit		– 🗆 X
n Ready		
Select a page	G Script - 2 Halp	
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: ● Maximum rollover files: Audit File Maximum Limit: ● Maximum files: Number of files: 2147483647 Maximum file size: ● Unlimited	
Connection	Reserve disk space	
ү₩ WIN2019 [sa]		
View connection properties		
Progress		
Ready		
	ОК	Cancel Help

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)



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)

₽ Enable Audit				-			×
Success	1 1	Total Succe	55		0 0	Error Warning	
Details:							
Action			Status			Message	
🥝 Enable Audit 'NP_Audit'			Success				
						Close	;



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)

💀 Create Database Audit Specification — 🗆 🗙									
🕕 Ready									
Select a page	C Script	Help INP. DB NClaud, Auda							_
	Audit: Actions	NP_Audit							~
		Audit Action Type		Object Class	Object Schema	Object Name	Principa	al Name	
Connection	1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	\sim	~		[
WIN2019 [sa]	2	BACKUP_RESTORE_GROUP	\sim	~					
YT WIN2013 [30]	3	DATABASE_ROLE_MEMBER_CHANGE_GROUP	\sim	~					
	4	FAILED_DATABASE_AUTHENTICATION_GROUP	\sim	~					
	5	SCHEMA_OBJECT_CHANGE_GROUP	\sim	~					
View connection properties	▶ 6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	\sim	~					
Progress	•7		\sim	~				ſ	
Ready						. ja			
						ОК	Cancel	Help	,



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)

Solution1 - Microsoft SQL Server Mana	Quick Launch (Ctrl+Q)
File Edit View Project Debug Too	ols Window Help
🖸 - O 🏠 - 🖕 - 🐂 💾 🖨 Ne	ew Query 🛢 📾 📾 📾 🔝 🛣 🖓 🕹 🗇 🔒 🤊 - 🚆
Object Explorer	пх
	-
Databases	
💮 💮 🗐 System Databases	
🕀 💼 Database Snapshots	
E NCloud	
Database Diagrams	
🗄 💼 External Resources	
🕀 📕 Synonyms	
🕀 💻 Programmability	
🕀 💼 Service Broker	
E Security	
E Users	
🕀 💼 Roles	
🕀 💼 Schemas	
🕀 📕 Asymmetric Keys	
E Certificates	
Symmetric Keys Always Encrypted Keys	
Database Audit Specificati	ions
c <mark>≩</mark> NP_DB-NCloud_Audit	
Security Policies	New Database Audit Specification
Security Security	Enable Database Audit Specification
Beplication	Script Database Audit Specification as
PolyBase	Policies
🗉 🛑 Always On High Availability	Exects
🕀 📕 Management	
Integration Services Catalogs E SOL Server Agent	Start PowerShell
	Reports •
	Delete
	Refresh
	Properties
Ready	i i i i i i i i i i i i i i i i i i i





按下 Close(關閉)

🔎 Enable Database Audit Specification					×
Success	1 Total 1 Succe	0 0	Error Warning		
Details:					
Action		Status		Message	
🥝 Enable Database Audi	t Specificat	Success			
				Close	;





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



使用 sp_configure 列出進階選項

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



啟用通用條件合規性

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



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





重新啟動 MSSQLSERVER 服務

輸入 net stop MSSQLSERVER && net start MSSQLSERVER

Administrator: Command Prompt	_		\times
C:\Users\Administrator>net stop MSSQLSERVER && net start MSSQLS The following services are dependent on the SQL Server (MSSQLSE Stopping the SQL Server (MSSQLSERVER) service will also stop th	ERVER RVER) ese se	service rvices.	^ -
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 successf	ully.		
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)

다. Connect to Server	×
	SQL Server
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	
	Remember password
	Connect Cancel Help Options >>





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

Server Properties - WIN2019		_		\times
Select a page General Memory Processors Security Connections Database Settings Advanced Pemissions	 Script ▼ ? Help Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Successful logins only Server proxy account 			
Connection Server: WIN2019 Connection: sa Y View connection properties Progress Ready	 Enable server proxy account Proxy account: Password: Options Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining 			
		ОК	Cano	cel

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)

<u>م</u>

Microso	ft SQL Server Management Studio	×
1	Some of your configuration changes will not take effect until SQL Server is restarted.	
Co	py message	ОК

Copyright © All rights are reserved by N-Partner Technologies Co

重新啟動 MSSQLSERVER 服務



按下 Yes(是) 重新啟動 MSSQLSERVER 服務

Microsoft SQL Server Management Studio							
Are you sure you want to restart the MSSQLSERVER service on WIN2019?							
Copy message	Yes	No					





按下 Yes(是) 停止 SQLSERVER Agent

Microso	ft SQL Server Management Studio		
?	Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do yo	ou wish to continue?	
🖹 Co	py message	Yes No	





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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

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

다. Connect to Server	×
	SQL Server
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	
	Remember password
	Connect 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)...



<u>م</u>

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

🛃 Create Audit	_	
🕕 Ready		
Select a page General Filter	Script Help Audit name: NP_Audit Queue delay (in milliseconds): 1000 On Audit Log Ocontinue Failure: Fail operation Shut down server Audit destination: Audit destination: Application Log Path: Audit File Audit File Maximum rollover files: Maximum Limit: Unlimited	
Connection	Number of files: 2147483647 Maximum file 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	O TB
WIN2019 [sa] View connection properties Progress Ready		
	OK Cancel	Help

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)





_		
🔀 🗸 Quick Launch	(Ctrl+Q) - C	ĸ
File Edit View Project	ect Tools Window Help	•
	b Execute	
Object Explorer	¥ ¥ ×	
Connect • • • • •	C -**	
😑 🐻 WIN2019 (SQL Server	r 15.0.1400.75 - sa)	
🕀 📕 Databases		
🖃 📕 Security		
E Logins		
Server Roles		
🕀 📕 Credentials	in Dura di dana	
🗄 📕 Cryptographic	ic Providers	
	ם ביו	
E Server Audit S	S New Audit	
🕀 📕 Server Objects	Enable Audit	
🕀 📕 Replication		
🕀 🛑 PolyBase	View Audit Logs	
🕀 🛑 Always On High /	Script Audit as	
Management	Policies	
🗄 📕 SQL Server Agent	t Facets	
🕀 🗹 XEvent Profiler	Start PowerShell	
	Reports +	
	Rename	
	Delete	
	Refresh	
	Properties	





按下 Close(關閉)

🔎 Enable Audit				-			\times
Success	1 1	Total Succe	ss	())	Error Warning	
Details:							
Action			Status			Message	
🥝 Enable Audit 'NP_Audit'			Success				
						Close	

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







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)

💀 Create Server Audit Specificati	on							- 0	×
🕕 Ready									
Select a page	🚺 Script	🛛 😮 Help							
🖉 General									
	Name:	NP_Server_Audit							
	Audit:	NP_Audit							~
	Actions:								
		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	\sim	~					
Connection	06	DATABASE_PRINCIPAL_CHANGE_GROUP	\sim	~					
ψ₩ WIN2019 [sa]	07	SERVER_PRINCIPAL_CHANGE_GROUP	\sim	~					
	08	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	~	~					
	09	LOGIN_CHANGE_PASSWORD_GROUP	~	~					
Vérie a serie d'an annualise	10	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~					
view connection properties	▶ 11	USER_CHANGE_PASSWORD_GROUP		~					
Progress	•12		\sim	~					
Ready									
						ОК	Can	icel Hel	p

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)

Nicrosoft SQL Ser 🗸 🛛	Quick	Launch (Ctrl+Q)
File Edit View Project To	ools	Window Help
G - O 📅 - 🛅 - 🖆 🗎	-	🕒 New Query 🗿 🔊 🖓 🖓 🖓 🐇 🚆
8 ¥ №		- ▷ Execute 🔳 🗸 🖧 🗐 📄 👫 🚆
Object Explorer	•	Ț ×
Connect + + + = + ℃ +	Ľ.	
🖃 🐻 WIN2019 (SQL Server 15.0.14	100.75	- sa)
🕀 🛑 Databases		
E Security		
Eogins Server Roles		
🕀 📻 Credentials		
🕀 💼 Cryptographic Provid	ders	
DNP_Audit	ation	
P Server Addit Specific	ation	
🕀 💼 Server Objects		New Server Audit Specification
Replication		Enable Server Audit Specification
🕀 💼 PolyBase		Script Server Audit Specification as
Always On High Availab Management		
Integration Services Cata		Policies •
🗉 🛃 SQL Server Agent		Facets
🕀 💽 XEvent Profiler		Start PowerShell
		Reports
		Delete
		Refresh
□ Re		Properties



按下 Close(關閉)

🔊 Enable Server Audit Sp	pecification		-		×
Success	1 Total 1 Succe	ss	0 0	Error Warning	
Details:					
Action		Status		Message	
Enable Server Audit Sp	ecification	Success			
				Close	;





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): Iocalhost -> 選擇 Authentication(驗證): SQL Server Authentication -> 輸入

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

다. Connect to Server	×
	SQL Server
Server type:	Database Engine 🗸 🗸
Server name:	localhost ~
Authentication:	SQL Server Authentication \sim
Login:	sa 🗸 🗸
Password:	
	Remember password
	Connect 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)...



۹Ŵ

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

🛃 Create Audit	_	
🕕 Ready		
Select a page General Filter	Script Kelp Audit name: NP_Audit Queue delay (in milliseconds): On Audit Log Failure: On Audit Log Failure: Fail operation Fail operation Shut down server Audit destination: Audit destination: Path: Audit File Maximum Limit: On Maximum rollover files: Unlimited On Maximum files: On Maximum files: On Audit On Aud	×
Connection	Number of files: 2147483647 Maximum file size: Unlimited Reserve disk space	▲
v₩ WIN2019 [sa]		
View connection properties		
Progress Ready		
	OK Cancel	Help

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)

Å





V Quick Launch (Ctrl+Q) File Edit View Project Tools Window Help Object Explorer VIN2019 (SQL Server 15.0.1400.75 - sa) Object Explorer VIN2019 (SQL Server 15.0.1400.75 - sa) Databases Security Databases Security Corpetentials Cryptographic Providers Audits VIN2019 (SQL Server 15.0.1400.75 - sa) Server Roles Security Server Audit S NP_Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent Facets XEvent Profiler XEvent Profiler Kename Delete									
File Edit View Project Tools Window Help Image: Consect -	🔀 💎 Quick Launch	(Ctrl+C	2)	-	. 🗖	×			
Object Explorer Object Explore	File Edit View Proje	ct To	ools	Wind	dow Hel	lр			
Object Explorer Connect - # *# = C • * Object Explorer Connect - # *# = C • * Object Explorer Connect - # *# = C • * Object Explorer Connect - # *# = C • * Object Explorer Connect - # *# = C • * Object Explorer Connect - # *# = C • * Object Explorer Object Explorer Connect - # *# = C • * Object Explorer Object Explo	G - O 13 - 1 - 1	1	- P	A 🕄	ew Query	**			
Object Explorer Image: Addite Image: Connect Image: Addite Image: Addite				- 	Execute				
Object Explorer Connect WIN2019 (SQL Server 15.0.1400.75 - sa) Databases Databases Security Enable Server Roles Enable Audit Enable Audit Enable Audit Enable Audit Enable Audit Enable Audit Logs		_				Ŧ			
Connect V V VI	Object Explorer		тņ	×					
 WIN2019 (SQL Server 15.0.1400.75 - sa) Databases Security Cogins Server Roles Credentials Cryptographic Providers Audits Providers Server Audit 5 New Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent XEvent Profiler XEvent Profiler 	Connect 🕶 🌹 🎽 👅 🝸	C -*	-						
 Databases Security Cogins Server Roles Credentials Cryptographic Providers Audits Replication Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🖃 🐻 WIN2019 (SQL Server	15.0.14	400.75 -	· sa)					
 Security Logins Server Roles Credentials Cryptographic Providers Audits Server Audit S New Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🕀 📕 Databases								
 Logins Server Roles Cryptographic Providers Audits NP_Audit Server Audit S New Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent Start PowerShell Reports Rename Delete 	🖃 🛑 Security								
 Server Roles Credentials Cryptographic Providers Audits NP_Audit Server Audit 5 New Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🕀 🛑 Logins								
 Credentials Cryptographic Providers Audits Server Audit S Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🕀 📕 Server Roles								
 Audits Audits NP_Audit Server Audit \$ New Audit Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🕂 📕 Credentials	- Drowie	dore						
 NP_Audit Server Audit S Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	E Cryptographi	Cryptographic Providers							
 Server Audit S Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	Rudit								
 Server Objects Replication PolyBase Always On High Management Integration Servic SQL Server Agent SQL Server Agent XEvent Profiler 	🕀 📕 Server Audit S		New A	udit					
 Replication PolyBase Always On High Management Integration Servic SQL Server Agent ✓ XEvent Profiler View Audit Logs Script Audit as Policies Facets Start PowerShell Reports Rename Delete 	🕀 📕 Server Objects		Enable	Audi	t				
 PolyBase Always On High , Management Integration Servic SQL Server Agent ✓ XEvent Profiler Start PowerShell Reports ▶ Rename Delete 	🕀 🛑 Replication			udit I	0.05				
 Always On High / Management Management Integration Servic SQL Server Agent ✓ XEvent Profiler Start PowerShell Reports → Rename Delete 	🕀 🛑 PolyBase	-	VIEW A	uuitt	logs				
 Management Integration Servic SQL Server Agent YEvent Profiler Policies Facets Start PowerShell Reports Rename Delete 	🕀 💼 Always On High		Script A	Audit	as 🕨				
	🕀 📕 Management	1	Policies	s	+				
Image: Approximation Start PowerShell Reports Rename Delete Delete	B SOL Server Agent		Facets						
Start PowerShell Reports Rename Delete		-							
Reports Rename Delete			Start Po	owerS	Shell				
Rename Delete			Reports	s	•				
Delete		1	Renam	e					
			Delete						
Refresh		1	Refresh	n					
Properties			Proper	ties					





按下 Close(關閉)

₽ Enable Audit				-			×
Success	1 1	Total Succe	ss		0 0	Error Warning	
Details:							
Action			Status			Message	
Enable Audit 'NP_Audit'			Success				
						Close	





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

AÔ





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):

💀 Create Database Audit Spec	tification						-	
🕕 Ready								
Select a page	🚺 Script	🕶 😮 Help						
🖉 General								
	Name:	NP_DB-NCloud_Audit			Deject Class Object Schema Object Name Principal Name			
	Audit:	NP_Audit						
	Actions	:						
		Audit Action Type		Object Class	Object Schema	Object Name	Princip	al Name
Connection	1	APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	\sim	~				
🛱 WIN2019 [sa]	2	BACKUP_RESTORE_GROUP	~	~				
	3	DATABASE_ROLE_MEMBER_CHANGE_GROUP	~	~				
	4	FAILED_DATABASE_AUTHENTICATION_GROUP	~	~				
View connection properties	5	SCHEMA_OBJECT_CHANGE_GROUP	\sim	~				
rogress	▶ 6	SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	\sim	~				
Beady	•7		\sim	~				
\bigcirc								
						OK	Cancel	Help

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)




Audit Specification(啟用資料庫稽核規格)

🧏 Microsoft SQL Server Managemen 🗸	Quick Launch (Ctrl+Q)
File Edit View Project Tools Wind	low Help
8 G + G 💏 + 🌴 - 🖆 💾 🔎 🔊 Ne	w Ouev A A A A A A A A - "
Object Explorer 🔹	<mark>₽×</mark>
Connect → 🛱 🎽 🗏 🝸 🖒 -ሎ	
WIN2019 (SQL Server 15.0.1400.75 - sa)	
🖃 🗰 Databases	
System Databases	
Database Snapshots	
Views	
🕀 🔲 Synonyms	
🕀 💼 Programmability	
🕀 📕 Service Broker	
🕀 🛑 Storage	
🖃 📕 Security	
🕂 💼 Users	
H Koles	
Asymmetric Keys	
Certificates	
Symmetric Keys	
🗄 📕 Always Encrypted Keys	
🖃 🛑 Database Audit Specificati	ons
c NP_DB-NCloud_Audit	
🕀 📕 Security Policies	New Database Audit Specification
Server Objects	Enable Database Audit Specification
	Script Database Audit Specification as
⊕ 📕 PolyBase	Policies
Always On High Availability Management	Facets
Integration Services Catalogs	Start DowerShell
🛨 📧 XEvent Profiler	Reports
	Delete
	Refresh
	Properties
🗇 Ready	

Copyright © All rights are reserved by N-Partner Technologies Co



按下 Close(關閉)

ᡇ Enable Database Audit	Specificatio	on	-		×
Success	1 Total 1 Succe	ess	0 0	Error Warning	
Details:					
Action		Status		Message	
🥝 Enable Database Audit :	Specificat	Success			
				Close	;





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	ד ר
SQL-192.168.2.217	
IP	
192.168.2.217	
設備種類	- 1
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 ■	7
icon-host 🗸	
Login Account	1
Login Password	1
Action 設備	
│	
智無貞科告言 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
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

曾設備	
b 備基本設定	
花 樽	
Windows-192.168.2.217	
,	
192.168.2.217	
と備種類	
Syslog Flow SNMP	
YSIOg 作II网起走	
資料格式	
Windows	~
Facility	
(17) local use 1 (local1)	~
編碼方式	
UTF-8	~
使備進階設定	
設備 Icon	
Icon-nost	·
Login Account	
Login Password	
₩ ₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	
新每次判止政	
暫無資料告警 ── 啟用 Syslog/Flow 暫無資料告警	



連絡資訊

TEL: +886-4-23752865 FAX: +886-4-23757458 技術問題請洽: Email: support@npartnertech.com Skype: support@npartnertech.com 業務相關請洽: Email: sales@npartnertech.com

