



如何設定 MS SQL 稽核事件記錄 V016



版權聲明

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

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標,均屬其合法註冊公司所有。



目錄

前言	
1. NXLog3	
1.1 NXLog 安裝3	
1.2 NXLog 設定檔下載4	
1.3 NXLog 設定檔5	
1.4 NXLog 啟動服務7	
2. SQL 20088	
2.1 稽核登入8	
2.1.1 使用圖形介面方式設定8	
2.1.2 使用指令介面方式設定13	
2.2 設定稽核16	
2.2.1 稽核伺服器層級16	
2.2.1.1 使用圖形介面方式設定16	
2.2.1.2 使用指令介面方式設定24	
2.2.2 稽核資料庫層級27	
2.2.2.1 使用圖形介面方式設定27	
2.2.2.2 使用指令介面方式設定	
2.3 事件記錄檔設定	
2.3.1 網域	
2.3.1.1 組織單位設定	
2.3.1.2 群組原則設定43	
2.3.2 工作群組50	
2.3.2.1 稽核原則設定50	
2.3.2.2 事件檔案設定54	
3. SQL 201257	
3.1 稽核登入57	
3.1.1 使用圖形介面方式設定	
3.1.2 使用指令介面方式設定62	
3.2 設定稽核65	
3.2.1 稽核伺服器層級65	
3.2.1.1 使用圖形介面方式設定65	
3.2.1.2 使用指令介面方式設定73	
3.2.2 稽核資料庫層級	
3.2.2.1 使用圖形介面方式設定	
3.2.2.2 使用指令介面方式設定85	
3.3 事件記錄檔設定	
3.3.1 網域	
3.3.1.1 組織單位設定88	
3.3.1.2 群組原則設定93	
3.3.2 工作群組100	
3.3.2.1 稽核原則設定100	
3.3.2.2 事件檔案設定104	
4. SQL 2016	
4.1 稽核登入107	

4.1.1 使用圖形介面方式設定1	07
4.1.2 使用指令介面方式設定1	12
4.2 設定稽核1	14
4.2.1 稽核伺服器層級1	14
4.2.1.1 使用圖形介面方式設定1	14
4.2.1.2 使用指令介面方式設定12	22
4.2.2 稽核資料庫層級1	25
4.2.2.1 使用圖形介面方式設定12	25
4.2.2.2 使用指令介面方式設定1	34
4.3 事件記錄檔設定1	37
4.3.1 網域1	37
4.3.1.1 組織單位設定1	37
4.3.1.2 群組原則設定14	42
4.3.2 工作群組14	49
4.3.2.1 稽核原則設定14	49
4.3.2.2 事件檔案設定1	53
5. SQL 20191	56
5.1 稽核登入1	56
5.1.1 使用圖形介面方式設定1	56
5.1.2 使用指令介面方式設定1	61
5.2 設定稽核1	63
5.2.1 稽核伺服器層級1	63
5.2.1.1 使用圖形介面方式設定1	63
5.2.1.2 使用指令介面方式設定1	71
5.2.2 稽核資料庫層級1	74
5.2.2.1 使用圖形介面方式設定1	74
5.2.2.2 使用指令介面方式設定1	83
5.3 事件記錄檔設定1	86
5.3.1 網域1	86
5.3.1.1 組織單位設定1	86
5.3.1.2 群組原則設定1	91
5.3.2 工作群組1	98
5.3.2.1 稽核原則設定1	98
5.3.2.2 事件檔案設定2	02
6. N-Reporter2	05
6.1 MS SQL Server Log2	.06
6.2 Windows Event Log2	07





本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 MS SQL 事件記錄。 NXLog 工具將 MS SQL 事件記錄轉成 syslog,再傳送到 N-Reporter 做正規化、稽核與分析。 此文件適用於 MS SQL 2008 / 2012 / 2016 / 2019 版本。

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

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

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

server-audit-and-server-audit-specification?view=sql-server-ver15

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> audit-action-groups-and-actions?view=sql-server-ver15

MS SQL Server 支援稽核記錄版本

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

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



1. NXLog

1.1 NXLog 安裝

(1) 下載 NXLog

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

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



(2) 開啟 [Windows PowerShell]



(3) 安裝 NXLog 軟體

PS C:\> Install-Package -Name .\nx	log-ce-2.10.2150.msi -F	orce		
ዾ 系統管理員: Windows PowerShel	I	_		×
PS C:\> Install-Package -N	ame .\nxlog-ce-2.1	0.2150.msi -Force		^
Name	Version	Source	Summary	
NXLog-CE	2.10.2150	C:\nxlog-ce-2		
PS C:>> _				~
紅色文字部位請輸入 NXLog 軟體路	各徑和檔案			



1.2 NXLog 設定檔下載

(1) 開啟 [Windows PowerShell]



(2) 下載 MS SQL 的 NXLog 範本設定檔並覆蓋 NXLog 設定檔

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

PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_MSSQL.conf' -OutFile 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

▶ 条統管理員: Windows PowerShell - □ × PS C:\Users\Administrator> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_MSSQL.conf' -OutFile 'C:\Program Files (x86)\nxlog\conf\nxlog.conf' PS C:\Users\Administrator> _



1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define ROOT
                 C:\Program Files (x86)\nxlog
define NCloud
                 192.168.8.184
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR
                  %ROOT%\data
define LOGFILE
                 %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile
          %ROOT%\data\nxlog.pid
SpoolDir
          %ROOT%\data
## Load the modules needed by the outputs
<Extension syslog>
  Module
            xm_syslog
</Extension>
## For MS SQL instance Event Log use the following:
<Input in_sqllog>
 Module
                im_msvistalog
  ReadFromLast TRUE
  SavePos
                TRUE
 Query
                <QueryList> \
    <Query Id="0"> \
      <Select Path="Application">*[System[Provider[@Name='MSSQLSERVER']]]</Select>\
    </Query> \
  </QueryList>
</Input>
<Output out_sqllog>
  Module om_udp
         %NCloud%
 Host
  Port
         514
  Exec $SyslogFacilityValue = 18;
  Exec $Message = "MSSQLSERVER" + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
       else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
       else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>
<Route sqllog>
  Path
         in_sqllog => out_sqllog
</Route>
```



```
## For Windows Event log use the following:
<Input in_eventlog>
 Module
                im_msvistalog
 ReadFromLast TRUE
 SavePos
                TRUE
 Query <QueryList> \
            <Query Id="0"> \
                <Select Path="Security">*[System[(EventID=4624 or EventID=4769)]]</Select> \
                <Select Path="Security">*[System[(EventID=4634)]]</Select> \
                <Select Path="Security">*[System[(EventID=4625 or EventID=4768 or EventID=4771)]]</Select>
                    <Select Path="Security">*[System[(EventID=4648 or EventID=4647)]]</Select> \
                </Query> \
            </QueryList>
</Input>
<Output out_eventlog>
 Module om_udp
 Host
          %NCloud%
 Port
         514
          $SyslogFacilityValue = 17;
 Exec
 Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
 Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
       else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
       else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
 Exec
          to syslog bsd();
</Output>
<Route eventlog>
 Path in_eventlog => out_eventlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address 和 MS SQL 執行個體名稱



1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



(2) 啟動 NXLog 服務,檢查 NXLog 服務狀態和確認 NXLog 記錄沒有錯誤訊息

PS C:\> Start-Service -Name nxlog PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType PS C:\> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'

≥ 系統管理員: Windows PowerShell	_		\times
PS C:\Windows\system32> <mark>Start-Service</mark> -Name nxlog PS C:\Windows\system32> <mark>Get-Service</mark> -Name nxlog ¦ <mark>Select-Object</mark> -Property Name,Status	,Star	tType	^
Name Status StartType			
nxlog Running Automatic			
PS C:\Windows\system32> <mark>Get-Content</mark> 'C:\Program Files (x86)\nxlog\data\nxlog.log' 2020-11-18 10:52:59 INFO nxlog-ce-2.10.2150 started PS C:\Windows\system32> _			v

2. SQL 2008

2.1 稽核登入

啟用登入稽核,以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。 以下分別為圖形介面和指令介面設定方式。

2.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

■ 建接到伺服器 Microsoft* SQLS	■ erver [•] 2008
伺服器類型(T):	Database Engine
伺服器名稱(S):	localhost
驗證(A):	SQL Server 驗證
登入(L):	5a 💌
密碼(P):	******
	✓ 記住密碼(M)
連接(C)	



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

💺 Microsoft SQL Server Management S	tudio 💶 🗵 🗙
檔案(F) 編 <mark>輯</mark> (E) 檢視(V) 工具(T)	視窗(₩) 社群(C) 說明(H)
🔡 新增查詢(N) 🕞 🐴 🐴 🌇 🕞	🚰 🗐 🎒 🜉 💂
物件總管	
連接(0) 🕶 🛃 📑 🝸 🛃 📓	
🖃 🐻 localhost (SQL Server 10.0.1600 - sa)	Net let un
 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	建接(C)
🗉 🧰 伺服器物件	甲斷建接(D)
1 🔃 複寫	証冊(G)
	新增查詢(Q)
	活動監視器(M)
	取動(S)
	停止(T)
	暫停(U)
	繼續(E)
	重新啟動(A)
	原則(0) ▶
	Facet(A)
	啟動 PowerShell(H)
	報表(P) ▶
	重新整理(F)
	屬性(R)
<u> </u>	
就緒	1.



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

[伺服器屬性 - ₩IN2008	-	
選取頁面	🖳 指令碼 👻 📑 說明	
 ☆ 一般 記憶體 ☆ 處理器 愛 安全性 ☆ 連接 ☆ 資料庫設定 ☆ 準限 	伺服器驗證 ○ Windows驗證模式 (W) ● SQL Server 及 Windows驗證模式 (S)	
	金人稽核 ○ 無(N) ○ 僅限失敗的登入(F)	
	 ● 僅限成功的登入(U) ● 失敗和成功的登入(B) (回照照 D = 155) 	
	「可服器 Proxy 帳戶 「 取用伺服器 Proxy 帳戶(♡) Proxy 帳戶(ℝ):	
連接	密碼(P): ************************************	
伺服器: ·	► 取用 Common Criteria 遵循(O)	
· 連接: ∞ ■ ● 檢視連接屬性	 ▶ 取用 C2 稽核追蹤(E) ▶ 跨資料庫擁有權鏈結(C) 	
進度		
就緒		
	確定取消	



(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]

🍢 Microsoft SQL Server Management S	tudio 💶 🗵 🗙
檔案(F) 編輯(E) 檢視(V) 工具(T)	視窗(W) 社群(C) 說明(H)
🎦 新増査詢(N) 🕞 🐴 🐴 🌇 🕞	
物件總管	
連接(0) - 影影 = 7 🖉 🔊	
🖃 🚺 localhost (SQL Server 10.0.1600 - 38)	清焼(の)
🗉 🧰 伺服器物件	中國建接(D)
■ ■ 複寫	註冊(牙)
⊡ 📮 🖬 🖓 ⊞ 📆 SQL Server Agent	新增查詢(Q)
	活動監視器(M)
	停止(T)
	暫停(U)
	繼續(E)
	重新啟動(A)
	原則(O) 🕨
	Facet(A)
	取動 PowerShell(H)
	報表(P) →
	重新整理(F)
	屬性(R)
就緒	1.

(6) 按 [是] 重新啟動 MS SQL SERVER 服務

Microsoft SQL Server Management Studio				
您確定要重新啟動 WIN2008 上的 MSSQLSERVER 服務嗎?				
4		是(Y)	否(N)	



(7) 按 [是] 停止 SQL SERVER Agent 服務

Microsoft SQL Server Management Studio					
?	停止此服務也會停止 SQL Server Agent (MSSQLSERVER)。 您要繼續嗎?				
Ē.		是(Y)	否(N)		



2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號

C:\> sqlcmd -S localhost -A





(3) 切換資料庫



(4) 使用 sp_configure 列出進階選項

1 > exec sp_configure 'show advanced options', 1	
2 > go	
1 > reconfigure	
2 > go	
∑ SQLCMD	
1> exec sp_configure 'show advanced options', 1	
2> go 組態選項 'show advanced options' 從 0 變更為 1。請執行 RECONFIGURE [1> reconfigure	東述式來安裝。
2> go	

(5) 啟用失敗和成功的登入記錄

1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer',					
N'AuditLevel', REG_DWORD, 3					
2 > go					
∑ SÓTCMD	×				
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3 2> go					
 (8) 個受影響的資料列> 1> 	-				



(6) 重新啟動 MS SQL SERVER 服務

2 > !!NET STOP MSSQLSERVER	
3 > !!NET START MSSQLSERVER	
4 > !!NET START SQLSERVERAGENT	
	_
Normal Solution Solution States and Solution S	×
1> !!NET STOP SQLSERVERAGENT	
SQL Server Agent (MSSQLSERVER) 服務正在停止	
SQL Server Agent (MSSQLSERVER) 服務已經成功停止。	
2> !!NET STOP MSSQLSERVER	
SQL Server(MSSQLSERVER)服務正在停止.	
SQL Server(MSSQLSERVER)服務已經成功停止。	
3> !!NET START MSSQLSERVER	
SQL Server (MSSQLSERVER) 服務正在啟動	
SQL Server(MSSQLSERVER)服務已經啟動成功。	
4> !!NET START SQLSERVERAGENT	
SQL Server Agent (MSSQLSERVER) 服務正在啟動 .	
SQL Server Agent (MSSQLSERVER) 服務已經啟動成功。	
5>	•
	//.



2.2 設定稽核

2.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業,例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

2.2.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

■見建接到伺服器 Microsoft* SQLS	■ erver [•] 2008
伺服器類型(T):	Database Engine
伺服器名稱(\$):	localhost 💌
驗證(A):	SQL Server 驗證
登入(L):	3a 💌
密碼(P):	*****
	☑ 記住密碼(M)



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

🍢 Microsoft SQI	L Server Mai	agement S	tudio		_ 🗆 🗡		
檔案(F) 編輯(E) 檢視(V)	工具(T)	視窗(₩)	社群(C)	說明(H)		
门 <u>)</u> 新增查詢(N)	🗅 📸 🗄	b 🌇 🕞	💕 🖵	6	Ŧ		
物件總管 ● ● × 連接(0) ● 課 課 ● ● ⑤ 回 ⑥ localhost (SQL Server 10.0.1600 - sa) 回 ⑧ 資料庫 ● ● 登入 ● ● 個服器角色 ● ● 認證							
 E □ 容 E □ 容 	碼編譯提供者 <mark>该</mark>						
● ● 伺服器	服; 新增	稽核(N)					
∃ 10,0000	篩選	(L)	•				
	erv 取動	PowerShell(H)				
	報表	(P)	•				
	重新	整理(F)					
<u> </u>							
就緒					11.		

(4) 輸入稽核名稱: NP_Audit -> 選擇稽核目的地: [Application Log] 將 MS SQL 稽核記錄儲存於 Windows 事件檢

<mark>視器的應用程式記錄</mark> -> 按 [確定]

吴 建立稽核		_ 🗆 🗡
🕕 就緒		
選取頁面	指令碼 →	
☆ 一般		
	稽核名稱(N): NP_Audit	
	作列延遲 (以毫秒 1000	÷
	□ 於稽核記錄失敗時關閉伺服器(S)	
	稽核目的地(D): Application Log	┍
	檔案路徑(P):	
	最大換用檔案(O): 2147483647	÷
	✓ 無限制(U)	
	檔案大小上限(Z) 0 → 6 MB 0 GB 0 7	TB(T
清读		
2012 2012		
<u> 檢視連接屬性</u>		
進度		
就緒		
	確定 取消 說	明



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

🍢 Microsoft SQL Server Ma	nagement Studio			
檔案(F) 編輯(E) 檢視(V)	工具(T) 視窗(W)	社群(C) 說明(H)		
[🔔 新增查詢(N) 🛛 🛅 👘	🔥 🌇 🕞 🚰 🔙	a 🗠 🗸		
物件總管	• 4 ×			
連接(0) ▼ 📑 📑 👅 🗌	2 🔏 🔤			
🖃 🚺 localhost (SQL Server 10.	0.1600 - 38)			
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□				
● 🛨 🧰 伺服器角色				
┃	i la			
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □				
∃ □ 同服器物件 -	新增格核(3)			
🗉 🧰 複寫	权用稽核(E)			
田 🛄 管理	里			
H D SQL Server Agent	編寫稽核的指令碼為	à(S) ▶		
	原則(O)	•		
	Facet(A)			
	啟動 PowerShell(H)			
	報表(P)	•		
	重新命名(M)			
	刪除(D)			
	重新整理(F)			
	屬性(R)			
就緒		11.		



(6) 按 [關閉]

🔍 啟用稽核					
🐼 威功	1 總計 1 成功		0 0	錯誤 警告	
詳細資料(D):					
動作		狀態		訊息	
⊘ 取用稽核 NP_Audit'		成功			
				關思	₽(C)

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





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

[確定]

吴 建立伺服器楷核規格						-	
 ① 就緒 選取頁面 	『指令碼						
	2010 4 10						
	名稱(N)	NP_Server_Audit					
	稽核(A)	: NP_Audit					.
	動作:						
		稽核動作類型	物件類別	物件結構描述	物件名稱	主體名稱	
	01	SUCCESSFUL_LOGIN_GROUP	<u> </u>				
	02	FAILED_LOGIN_GROUP	<u> </u>			_	
	03	LOGOUT_GROUP	<u> </u>				
	04	SERVER_STATE_CHANGE_GROUP	<u> </u>				
連接	05	SERVER_OPERATION_GROUP	_				
📑 localhost [sa]	06	SCHEMA_OBJECT_CHANGE_GROUP	_				
 	07	DATABASE_OWNERSHIP_CHANGE_GROUP	_				
進度	08	DATABASE_CHANGE_GROUP	_				
就緒	▶ 09	AUDIT_CHANGE_GROUP	_				
No. A	*10	·	•				
			-				
					確定	取消 說明	



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





(10) 按 [關閉]

、 段用伺服器稽核規	格			_ 🗆 X
🐼 威功	1 總計 1 成功		0 錯誤 0 警告	
詳細資料(D):				
動作		狀態	訊息	
📀 啟用伺服器稽核規	札格 NP_Serv	成功		
			ß	朝閉(C)



2.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號





(3) 切換資料庫



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

1 > CREATE SERVER AUDIT [NP_Audit] 2 > TO APPLICATION_LOG 3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE) 4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON) 5 > <mark>GO</mark> 🚬 SQLCMD _ 🗆 🗵 1> CREATE SERVER AUDIT [NP_Audit] 2> TO APPLICATION_LOG 3> WITH <QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE> 4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON) 5> GO 1> ┛ ▶ 紅色文字部位請輸入稽核名稱



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

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

	- 비 스
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]	
2> FOR SERVER AUDIT [NP_Audit]	
3> ADD <successful_login_group>,</successful_login_group>	
4> ADD (FAILED_LOGIN_GROUP),	
5> ADD (LOGOUT_GROUP),	
6> ADD <server_state_change_group>,</server_state_change_group>	
<pre>7> ADD (SERVER_OPERATION_GROUP),</pre>	
8> ADD <schema_object_change_group>,</schema_object_change_group>	
9> ADD <database_ownership_change_group>,</database_ownership_change_group>	
10> ADD <database_change_group>,</database_change_group>	
11> ADD (AUDIT_CHANGE_GROUP)	
12> WITH (STATE = ON)	
13> GO	
1> quit	
PS C:\Windows\system32>	•

紅色文字部位請輸入伺服器稽核規格名稱



2.2.2 稽核資料庫層級

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

以下分別為圖形介面和指令介面設定方式。

2.2.2.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

■「連接到伺服器 Microsoft* SQLS	× erver °2008
伺服器類型(T):	Database Engine
伺服器名稱(\$):	localhost
驗證(A):	SQL Server 驗證
登入(L):	38.
密碼(P):	*****
	▶ 記住密碼(M)
	取消 說明 選項(O) >>





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



(4) 輸入稽核名稱: NP_Audit -> 選擇稽核目的地: [Application Log] 將 MS SQL 稽核記錄儲存於 Windows 事件檢

<mark>視器的應用程式記錄</mark> -> 按 [確定]

吴 建立稽核		. 🗆 🗙
① 就緒		
選取頁面		
11 一般		
	稽核名稱(N): NP_Audit	
	住列延遲 (以毫秒 1000	÷
	□ 於稽核記錄失敗時關閉伺服器(S)	
	稽核目的地(D): Application Log	
	檔案路徑(P):	
	最大換用檔案(O): 2147483647	A.
	✓ 無限制(U)	_
	檔案大小上限(Z) 0 → ● MB ● GB ● TI	B(T
 遠接		
Proceedings (sa)		
<u>檢視連接屬性</u>		
進度		
就緒		
	確定 取消 說明	



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

🍢 Microsoft SQL Server Management Studio 📃 🖂 🗙						
檔案(F) 編輯(E) 檢視(V)	工具(T) 視窗(₩) 社群(C)	說明(H)				
🔔 新增查詢(N) 🛛 🛅 👘	🔥 🜇 🕞 💕 🗔 🍊 💐	-				
 幅菜(F) 編輯(E) 微視(V) ① 新增查詢(N) □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● <li< th=""><th>上具(1) 祝醬(W) 社苷(C) 予 予 ● ● ● ● ● ● ●</th><th>2ℝ99(H)</th></li<>	上具(1) 祝醬(W) 社苷(C) 予 予 ● ● ● ● ● ● ●	2 ℝ 99(H)				
	屬性(R)					
就緒		11.				



(6) 按 [關閉]

🔍 啟用稽核					_ 🗆 X
🐼 威功	1 總計 1 成功		0) 錯誤) 警告	
詳細資料(D):					
動作		狀態		訊息	
⊘ 取用稽核 NP_Audit'		成功			
I					
				6	閘閉(C)



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

料庫稽核規格...]





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

按 [確定]

建立資料庫稽核規格								
🕕 就緒								
選取頁面	「「「「」」「「」」「「」」」。							
La** — 較	名稱(N) 稽核(A) 動作:	NF_DB-NC	ICloud_A:	udit			×	
		帮 核動作類型		物件類別	物件結構描述	物件名稱	主體名稱	
	1	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	-	_				
 禈搊	2	SCHEMA_OBJECT_CHANGE_GROUP		<u> </u>				
🚚 localhost [sa]	3	DATABASE_OWNERSHIP_CHANGE_GROUP	_	<u> </u>				
10-11-11-11-11-11-11-11-11-11-11-11-11-1	4	DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	_	<u> </u>				
<u>惯代建佞唐住</u>	5	DATABASE_CHANGE_GROUP	-	<u> </u>				
建度	▶6	AUDIT_CHANGE_GROUP	-	<u> </u>				
玩箱	*7		-	_				
-							確定 取消 說明	



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




(10) 按 [關閉]

[啟用資料庫稽核規	格				_ 🗆 🗙
🐼 成功	1 總計 1 成功		0 0	錯誤 警告	
詳細資料(D):					
動作		狀態		訊息	
② 取用資料庫稽核規	礼格 NP_DB	成功			
,					朝開(C)



2.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號

C:\> sqlcmd -S localhost -A





(3) 切換資料庫



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

1 > CREATE SERVER AUDIT [NP_Audit]

- 2 > TO APPLICATION_LOG
- 3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
- 4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)





紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫,範例:NCloud



紅色文字部位請輸入稽核資料庫名稱



(6) 設定稽核 NCloud(範例) 資料庫 · ADD 動作 <mark>詳細說明請參考**前言**的稽核動作群組連結</mark>

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

🚬 Administrator: Windows PowerShell



紅色文字部位請輸入資料庫稽核規格名稱

1 > CREATE DATABASE AUDIT SPECIFICATION [NP DB-NCloud Audit]

紅色文字部位請輸入稽核資料庫名稱

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



2.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

2.3.1 網域

2.3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





(2) 新增組織單位

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

📔 Active Directory	使用者和電腦		
檔案(F) 執行(A)	檢視(V) 說明(H)		
🗢 🔿 🚈 📘	🗎 🚍 🧕 🗐 🖺	iii 🐮 🗽 🖆	1 🔻 🗾 🐍
Active Directory 使 ■	 用者和 名稱 Builtin Computers 委派控制(E) 尋找(I) 變更網域(D) 變更網域控制站(C) 提高網域功能等級(A). 操作主機(M) 	▲類型 builtinDomain 容區 單位	描述 Default contains Default contains Default contains Default contains Default contains
	新增(N) 所有工作(K) 檢視(V) 重新整理(F) 匯出清單(L) 內容(R) 說明(H)	 ▶ 電腦 ▶ 連絡人 群組 InetOrgl msImag MSMQ 組織單 印表機 使用者 共用資 	Person ing-PSPs 佇列別名 位 料夾
▲ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			



(3) 輸入組織單位名稱

新增物件 - 組裁單位	×
建立在: n-partner.local/	
名稱(A):	
Servers	
✔ 保護容器以防止被意外刪除(P)	
<u>工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工工</u>	月

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

(4) 移動伺服器至新的組織單位

選擇 [Computers] 組織單位 -> 在 [SQL2008] 伺服器 · 按滑鼠右鍵 · <mark>註:請依客戶環境選擇 MS SQL Server 主機</mark>

-> 點選 [移動]

📔 Active Directory 使用者	和電腦		
檔案(F) 執行(A) 檢視(♡) 說明(H)		
🗢 🔿 🖄 📅 🖌 📋	i 🗙 🗐 🙆	🗟 🛛 🖬 🗏	と 🛅 🍸 🗾
Active Directory 使用者 ★ ○ 儲存查詢 □ 詳 n-partner.local ★ ○ Builtin ○ Computers □ Domain Controlls ★ ○ ForeignSecurityP: ★ ○ Managed Service ○ Users ○ Servers	名稱	類型 電腦 加入群組中(G) 停用帳戶(S) 重設帳戶(A) 移動(V) 管理(M) 所有工作(K) 鄭下(T) 刪除(D) 內容(R) 説明(H)	
將目前的選取項目移動到另-	個組織單位		



(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	×
將物件移動到容器(M):	
In-partner Image Service Accounts Servers Users	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 SQL2008 伺服器已移動。

📴 Active Directory 使用者	街和電腦		
檔案(F) 執行(A) 檢視(7) 說明(H)		
🗢 🔿 🖄 🖬 🐇 📋	🗙 🗐 🙆 🗟) 🛛 🖬 🗏	🚴 🛅 🍸 🗾
 Active Directory 使用者 ● 儲存查詢 ● 請 n-partner.local ● 简 Builtin ○ Computers ○ Domain Controlls ● ⑦ ForeignSecurityP: ● ③ Managed Service ○ Users ○ Servers 	名稱 NGL2008	<u>類型</u> 電腦	描述



2.3.1.2 群組原則設定

- (1) 開啟群組原則管理
- 開啟 [群組原則管理]



(2) 在 Servers 組織單位,新增群組原則物件

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





(3) 輸入群組原則物件名稱

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

新増 GPO		×
_名稱(N):		
N-Partner Policy		
來源入門 GPO(\$):		
(無)		•
	確定	取消

(4) 編輯群組原則物件

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





(5) 本機原則:稽核原則

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





(6) 事件記錄:應用程式記錄保持方法

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





(7) 事件記錄:應用程式記錄檔大小最大值

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





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



(9) 更新群組原則



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

Administrator: Windows PowerShell PS C:\> Get-GPResultantSetofPolicy -Computer SQL2008 -Path C:\tmp\SQL2008.html -ReportType html					
RsopMode Namespace LoggingComputer LoggingUser LoggingMode	: Logging : \\\$QL2008\Root\Rsop\N\$1ABDEB77_5871_4F42_B155_822DDC08423C : \$QL2008 : N-PARTNER\administrator : Computer				
PS C: \>		<u> </u>			

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



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

N-PARTNE	R\SQL2008 - Windows I	nternet Explorer		_ 🗆	1
	C:\tmp\SQL2008.html	🔹 😽 🗙 🚺 Bing		P	
我的最愛	🔎 N-PAR TNERSOL 200	8			
•					
		行物组织 別約日米			_
N-PARTNE 密料1版集: 2021	R\SQL2008 /10/21 下午 03:18:02			新示全部	
₫要	1011 00.10.00			副示服	
電腦設定				隠藏	1
原則				隠滅	
Windows	新定				
安全性的				四城	
A THE	581 <i>7</i> 42264881			85.99	
帳戶具	限则/账户租正原则			離不	
本權調	〔則/楷核原則			隠藏	
j	東則	設定	優勢 GPO		
ŧ	蒈核帳戶登入事件	成功,失敗	N-Partner Policy		
ŧ	蒈核帳戶管理	成功,失敗	N-Partner Policy		
ŧ	蒈核登入事件	成功,失敗	N-Partner Policy		
本機調	則/安全性運 項			翻示	
事件言	2 録 宿			隠藏	
j	朝	表定	優勢 GPO		
ß	#用程式記錄保持方法	視需要而定	N-Partner Policy		
ß	患用程式記錄檔容量最 大值	204800 KB	N-Partner Policy		
公開会	注論原則/進證服務用戶端。	自動註冊設定		顯示	
公開会	注鎖原則/加密檔案系統			顯示	
公開会	注鎖原則/被信任的根運證授	そ、「推理位」		顯示	
「田者書定				顯示	
CALCE BEAC					



2.3.2 工作群組

2.3.2.1 稽核原則設定

(1) 開啟 [本機群組原則編輯器]

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

控制台((1)				
輸編	輯群組原則				
🔎 查看	更多結果				
group po	licy			登出▶	
尽 開始		\geq			



(2) 本機原則:稽核原則

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





(3) 開啟 [Windows PowerShell]



(4) 更新群組原則





(5) 查看群組原則套用情形

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

🜌 条统管理員:Windows PowerShell		
PS C:>> auditpol /get /category:*		
条統稽核原則 難見して難則	≥r,,, ,,,,	
) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	· · · · · · · · · · · · · · · · · · ·	
安全性系統延伸	沒有稽核	
系統完整性	成历及英殿	
IPSEC driver	沒有稽核	
	成功及失敗	
女主性状態愛史 ネルーター	成切	
요//요山 참궀	成功及失敗	
	成功及失敗	
	成功及失敗	
IPsec 主要模式	成功及失敗	
IPsec 快速模式	成功及失敗	
IPsec 她伸快式。 特殊感动	成切皮矢敗	
付/本品人	成功及天敗 成功及失敗	
網路原則伺服器	成功及失敗	
物件存取	100100000000	
檔案系統	沒有稽核	
registry	沒有稽核	
	》	
	~ · · · · · · · · · · · · · · · · · · ·	
產年的應用程式	沒有稽核	
控制代碼操縱	沒有稽核	
檔案共用	沒有稽核	
- 篩選平台封包丟棄	<u>、沒有稽核</u>	
前選半台建線 	》	
特殊權限使用	7文7月71首193	
機密特殊權限使用	沒有稽核	
非機密特殊權限使用	沒有稽核	
其他特殊權限使用事件	沒有稽核	
評細追蹤	没方我按	
NPAPI 活動	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
RPC 事件	沒有稽核	
建立處理程序	沒有稽核	
原則變更		
稽核原則變更	感辺	
	火	
了这个人的变更 MPSSUC 相盯国幼宵盯能着再	》 · · · · · · · · · · · · · · · · · · ·	
新選平台原則變更 新聞 新	沒有稽核	
其他原則變更事件	沒有稽核	
帳戶管理		
使用者帳戶管理	成功及失敗	
電腦帳戶官埋 一菜本紙料組幣堆	成切皮失敗。	
- 久王][[4][[][4] 	成初及天殿 成功及失敗	
應用程式群組管理	成功及失敗	
其他帳戶管理事件	成功及失敗	
DS 存取) <u>E</u>	
日球服務愛史	没有稽核	
日邦版狩贤易	》	
日錄服務存取		
帳戶登入	7773773	
Kerberos 服務票證操作	成功及失敗	
其他帳戶登入事件	成功及失敗	
Kerberos 驗證服務	成功及失敗	
認識問題	成切及失敗	



2.3.2.2 事件檔案設定

(1) 開啟 [事件檢視器]

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

程式 (1)
■ <u>事件檢視器</u>
控制台 (1)
🤠 檢視事件記錄檔
0 +
>>2 宣看更多結果
来供给祖婴 家中 、



(2) 編輯應用程式記錄

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





(3) 設定應用程式記錄檔

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

記錄內容 - 鷹用程式	(類型: 糸統管理) 🛛 🗙
一般 訂閱	
全名(F):	Application
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Application.evtx
記錄檔大小:	1.07 MB(1,118,208 位元組)
建立日期:	2021年6月21日下午 09:05:32
修改日期:	2021年7月5日 下午 02:26:50
存取日期:	2021年6月21日下午 09:05:32
 ▶ 啟用記錄(E) 最大記錄欄大小(K) 當事件記錄欄的大: ● 視需要覆寫: ● 宿記錄欄已: ● 不要覆寫事: 	B)(X): 204800
	確定 取消 套用(P)



3. SQL 2012

3.1 稽核登入

啟用登入稽核,以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。 以下分別為圖形介面和指令介面設定方式。

3.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

e ^p	連接到伺服器				
SQL Server 2012					
伺服器類型(T):	Database Engine 🗸				
伺服器名稱(\$):	localhost				
驗證(A):	SQL Server 驗證 🗸				
登入(L):	Sa. 🗸				
密碼(P):	****				
✓ 記住密碼(M)					



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

🍢 Solution1 - Microsoft SQL S	Server Managem 🗕 🗖 🗙
檔案(F) 編輯(E) 檢視(V) 專案(P)	傾錯(D) 工具(T) 視窗(W) 說明(H)
🤅 🛅 🕶 🗁 📂 🔚 🎒 🔔 新増査	前(N) 🗋 📸 📸 🌇 👗 🛍 📖 🗒
物件總管 ▼ 早 ×	
連接 📲 🛃 🔳 🍸 👩 📓	
🗉 🐻 localhost (SQL Server 11.0.21	
	連接(C)
I I I I I I I I I I I I I I I I I I I	中斷連接(D)
III III III III III IIII IIII	註冊(G)
	新増查詢(Q)
■ □ 管理	
	litter (G) 信止(T)
	哲停(U)
	維續(E)
	重新啟動(A)
	Facet(A)
	IIII(H) ─────
	報表(E) ▶
	重新整理(F)
	屬性(R)
就緒	



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

3	伺服器屬性 - SQL2012 - C ×
選取頁面	🔄 指令碼 👻 🚺 說明
 一般 記憶體 虚理器 愛生性 愛生性 運行 資料庫設定 資準階 運行 確限 	 伺服器驗證 ○ Windows 驗證模式 (W) ⑥ SQL Server 及 Windows 驗證模式 (S) 登入稽核 ○ 無(N) ○ 僅限失敗的登入(F) ○ 僅限成功的登入(U) ④ 失敗和成功的登入(B) 伺服器 Proxy 帳戶 □ 取用伺服器 Proxy 帳戶(V)
連接	Proxy 帳戶(R):
伺服器: SQL2012 連接: SQL2012\Administrator 型 <u>檢視連接屬性</u> 進度	器碼(): 選項 □ 歇用 Common Criteria 遵循(0) □ 歇用 C2 稽核追蹤(E) □ 跨資料庫擁有權鏈結(C)
就緒	
	確定 取消



(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]

🗏 Solution1 - Microsoft SQL Server Managem 🗕 🗖 🗙					
檔案(F) 編輯(E) 檢視(V) 専案(P) 偵錯(D) 工具(T) 視窗(W) 說明(H)					
: 🗊 * 🖽 * 🎽 📓 🗿 📜 新坊	: 🛅 🕶 📨 💕 🔚 🥔 🔔 新増査詞(N) 📑 🐴 🐴 👗 斗 🖳 🍹				
物件總管 ▼ 🖓	Р ×				
連接 📲 🛃 🔳 🍸 🛃 📓					
🖃 🐻 localhost (SQL Server 11	<u>n 21</u>				
■	· 建接(C)				
■ 🔤 安全性	中斷連接(D)				
■ ■ 四成額初下					
⊪ 🧰 AlwaysOn 高可用性	新增查詢(Q)				
🗉 🚞 管理					
	(武型)(S) (度止(四)				
	17年(1)				
	自行(U) () () ()				
l (が座 詞(し) 手 かて ジトズトノムン				
	里新戲團(A)				
	原則(O) ▶				
	Facet(A)				
	愈動 PowerShell(H)				
	報表(E) ▶				
	重新整理(F)				
< 111	/////////////////////////////////////				
就緒					

(6) 按 [是] 重新啟動 MS SQL SERVER 服務





(7) 按 [是] 停止 SQL SERVER Agent 服務





3.1.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號

PS C:\> sqlcmd -S localhost -L	sa		
Σ	SQLCMD	Ŀ	- 🗆 X
Windows PowerShell 著作權 (C) 2016 Micros	soft Corporation. 著作權所	所有,並保留一切權利	•
PS C:\Windows\system3% 密碼: 1> _	2> sqlcmd —S localhost —U	sa	
<	Ш		>
Options:			
-S [protocol:]server[instan	ce_name][,port]		
-U login_id			
-P password			
-A dedicated administratro	r connection		

<2.2> 使用 Windows 帳號





(3) 切換資料庫



(4) 使用 sp_configure 列出進階選項

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

(5) 啟用失敗和成功的登入記錄



(6) 重新啟動 MS SQL SERVER 服務

1 > !!NET STOP SQLSERVERAGENT		
2 > !!NET STOP MSSQLSERVER		
3 > !!NET START MSSQLSERVER		
4 > !!NET START SQLSERVERAGENT		-
SQLCMD -	x	
1> !!NET STOP SQLSERVERAGENT SQL Server Agent (MSSQLSERVER) 服務正在停止.	^	
SQL Server Agent (MSSQLSERVER) 服務已經成功停止。		
2> **NET STOP MSSQLSERUER		
SQL Server(MSSQLSERVER)服務正任停止。 SQL Server(MSSQLSERVER)服務已經成功停止。		
3> !!NET START MSSQLSERVER		
SQL Server(MSSQLSERUER)服務止在取動. SQL Server(MSSQLSERUER)服務已經啟動成功。		
4> !!NET START SQLSERVERAGENT		
SQL Server Agent (MSSQLSERVER) 服務正在啟動 . SQL Server Agent (MSSQLSERVER) 服務已經啟動成功。		
	>	



3.2 設定稽核

3.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業,例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

3.2.1.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

e ^{ji}	連接到伺服器 ×				
SQL Server 2012					
伺服器類型(T):	Database Engine 🗸				
伺服器名稱(\$):	localhost 🗸				
驗證(A):	SQL Server 驗證 🗸 🗸				
登入(L):	3a 🗸 🗸				
密碼(P):	*****				
☑ 記住密碼(M)					
	取消 說明 選項(O) >>				



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

🍢 Microsoft SQL Se	rver Management 🗕 🗖 🗙
檔案(F) 編輯(E) 檢視(N	/) 偵錯(D) 工具(T) 視窗(W) 説明(H)
i 🛅 • 🕮 - 🎽 📓 🥔	🛄 新増査詢(N) 🔓 🐴 🐴 🕌
物件總管	<mark>▼ </mark>
連接 📲 🛃 🔳 🍸	e 🔏
🖃 🐻 localhost (SQL Se	erver 11
田 □ 資料庫 □ □ ☆ 安全性 □	
🗉 🧰 伺服器角色	e la
	3/# #
🗉 🧰 伺服	新増稽核(N)
	篩選(T) ▶
± ⊆ ≰⊜ ⊕ ⊇ AlwaysC	
⊡ Integrat	₩xt(E)
H 🗊 SAF Sel	重新整理(F)
<	>
±+/≠	
4/4/#8	



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

1 5	建立	稽核
🛈 就緒		
選取頁面	🔄 指令碼 👻 📭 說明	
≝〕師瑳	稽核名稱(N):	NP_Audit
	佇列延遲 (以毫秒 為單位)(Q):	1000
	於稽核記錄失敗 時:	 ● 繼續(C)
		○ 開閉伺服器(S)
		○ 失敗作業(F)
	栺核日的地(D):	應用程式記錄檔
	檔案路徑(P):	
	稽核檔案數目上 限:	 ● 最大換用檔案(O): ✓ 無限制(U)
		○ 最大檔案數目(X):
		檔案數目(B): 2147483647 文
連接	檔案大小上限(Z):	0
🛃 localhost [sa]		✓ 無限制(L)
	□ 保留磁碟空間(F)	R)
<u>檢視連接屬性</u>		
進度		
就緒		
		確定 取消 説明



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

🇏 Microsoft SQL Serve	er M	anagement 💻 🗖 💙	2
檔案(F) 編輯(E) 檢視(V)	偵錯	t(D) 工具(T) 視窗(W) 說明(H	ł)
i 🛅 = 🕮 - 📂 🗐 🥥 🚺	〕新	增查詢(N) 🔓 🐴 🐴 💑 👗	Ŧ
物件總管 ● 連接 ● 認 型 ● 連接 ● 認 型 ● ● ⑦ localhost (SQL Server) ● ● ② ● ● ② ● ● ② ● ● ○ ● ● ○ ● ● ○ ● ● ○ ● ● ○ ● ● ○ ● ● ○ ● ● ○ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●<	〕新	增查詢(N) ♪ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
		里新登理(F) 屬性(R)	
就緒			



٩	啟用稽	核	– – X
🐼 威功	1 總計 1 成功	0	錯誤 警告
詳細資料(D):			
動作	Я	伏態	訊息
⊘ 取用稽核 'NP_Audit'	ş	成功	
			關閉(C)

(6) 按 [關閉]

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





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

確定]								
ķ	Create Server Audit Specification							
🕕 就緒								
選取頁面	🔄 指令硬	『 ▼ 🖺 說明						
	名稱(I 稽核(J 動作:	N): A): NP_Audit					v	
		稽核動作類型		物件類別	物件結構描述	物件名稱	主體名稱	
	01	SUCCESSFUL_LOGIN_GROUP	~	~				
	02	FAILED_LOGIN_GROUP	~	~				
	03	LOGOUT_GROUP	~	~				
* i.e.	04	SERVER_STATE_CHANGE_GROUP	~	~				
建 膜 ■ localhost [sa] <u>检視連接層性</u>	05	SERVER_OPERATION_GROUP	~	~				
	06	SCHEMA_OBJECT_CHANGE_GROUP	~	~				
	07	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~				
	08	DATABASE_CHANGE_GROUP	~	~				
	09	AUDIT_CHANGE_GROUP	~	~				
進度	▶ 10	USER_CHANGE_PASSWORD_GROUP	~	~				
就緒	*11		~	×				
				-		確定	取消 說明	


5 Microsoft SQL Server Ma	inagement Studio 🛛 🗕 🗖 🗙					
檔案(F) 編輯(E) 檢視(V) 偵錯(D) 工具(T) 視窗(W) 說明(H)						
: 🛅 🕶 📨 📂 🔙 🥥 🔔 新増査詞(N) 📑 🐴 🐴 🌇 🖄 🖉 🗧 🗒						
物件總管 ▼ 平 × 連接 ▼ 認認 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●						
NP_Audit 同 同 同 同服器稽核規格 □ □ 同服器稽核規格 □ □ □ □ 同服器稿核規格 □ □ □ □ 同服器物件 □ □ □ □ □ □ □	新增伺服器稽核規格(N)					
	取用伺服器档核规格(E)					
⊪ 🚞 管理 ⊮ 🚞 Integration Services 目≸ ⊮ 📆 SQL Server Agent	編寫伺服器稽核規格的指令碼為(S) → 原則(O) → Facet(A) 愈動 PowerShell(H) 報表(E) →					
	刪除(D) 重新整理(F)					
就緒	·····································					

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



(10) 按 [關閉]

ē.	啟用伺服器稽核	ええんと□	
🐼 威功	1 總計 1 成功	0 錯讀 0 警告	<u>果</u> 告
詳細資料(D):			
動作	狀態	訊息	Į
⊘ 啟用伺服器稽核規	見格 NP_Ser 成功	h	
			關閉(C)



3.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號





(3) 切換資料庫



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



紅色文字部位請輸入稽核名稱



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

- 1 > CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
- 2 > FOR SERVER AUDIT [NP_Audit]
- 3 > ADD (SUCCESSFUL_LOGIN_GROUP),
- 4 > ADD (FAILED_LOGIN_GROUP),
- 5 > ADD (LOGOUT_GROUP),
- 6 > ADD (SERVER_STATE_CHANGE_GROUP),
- 7 > ADD (SERVER_OPERATION_GROUP),
- 8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
- 9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
- 10 > ADD (DATABASE_CHANGE_GROUP),
- 11 > ADD (AUDIT_CHANGE_GROUP),
- 12 > ADD (USER_CHANGE_PASSWORD_GROUP)
- 13 > WITH (STATE = ON)
- 14 > <mark>G</mark>O

1 > quit

≥ 系統管理員: Windows PowerShell ×
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit] 💦 🔼
2> FOR SERVER AUDIT [NP_Audit]
<pre>3> ADD (SUCCESSFUL_LOGIN_GROUP),</pre>
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD <server_state_change_group>,</server_state_change_group>
<pre>7> ADD (SERVER_OPERATION_GROUP),</pre>
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
<pre>9> ADD 〈DATABASE_OWNERSHIP_CHANGE_GROUP〉,</pre>
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP)
13> WITH (STATE = ON)
14> GO
1> quit
PS C:\Windows\system32>

紅色文字部位請輸入伺服器稽核規格名稱



3.2.2 稽核資料庫層級

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

以下分別為圖形介面和指令介面設定方式。

3.2.2.1 使用圖形介面方式設定

(1) 開啟 [SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連接]

建接到伺服器 ×					
SQL Server 2012					
伺服器類型(T):	Database Engine 🗸				
伺服器名稱(S):	localhost 🗸				
驗證(A):	SQL Server 驗證 🗸 🗸				
登入(L):	Sa. 🗸				
密碼(P):	****				
✓ 記住密碼(M)					
連接(C) 取消 說明 選項(O) >>					



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

🍢 Microsoft SQL Se	rver Management 😑 🗖 🗙
檔案(F) 編輯(E) 檢視(N	/) 偵錯(D) 工具(T) 視窗(W) 說明(H)
i 🗊 • 🕮 • 🎽 📓 🥔	🛄 新増査詢(N) 🔓 🐴 🐴 🕌
物件總管	<mark>▼ </mark>
連接 📲 🛃 🔳 🍸	e 🔏
🖃 🐻 localhost (SQL S	erver 11
田 □ 資料庫 □ □ □ 毋全性 □	
□ □ □ □ 至入	
🗉 🚞 伺服器角色	e la
■ 📄 認證	3/#-₽
	新増稽核(N)
□ □ □ □ □ □ □	
± ⊆ ॡक़	
. ■ 管理	
⊡ Integrat □ □	±0.4%(C) ►
H D SQL Ser	重新整理(F)
<	>
計 体	
4/6/201	



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

5	建立	稽核
🕕 就緒		
選取頁面	🔄 指令碼 👻 📭 說明	
	稽核名稱(N):	NP_Audit
	佇列延遲 (以毫秒 為單位)(Q):	1000
	於稽核記錄失敗 時:	 ● 繼續(C) ○ 開閉 (2) 円間(2)
		○ 開閉伺服器(S)
	統技日は小い。	
	伯攸日的地(D):	應用程式記錄檔 イ
	檔案路徑(P):	
	稽核檔案數目上 限:	 ● 最大換用檔案(O): ✓ 無限制(U)
		○ 最大檔案數目(X):
		檔案數目(B): 2147483647
連接	檔案大小上限(Z):	0
🛃 localhost [sa]		☑ 無限制(L)
	□ 保留磁碟空間(F	र)
進度		
以 就結		
		建定 取消 說明



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

🇏 Microsoft SQL Server Management 💻 🗖 🗙						
檔案(F) 編輯(E) 檢視(V)	偵錯	(D) 工具(T) 視窗(W) 說明(H	H)			
i 🛅 • 🚈 • 🎬 📓 🧋 🛔	〕新	增查詢(N) 📑 🐴 🐴 🍒	Ŧ			
物件總管 🔹	q×					
連接 📲 🛃 🔳 🍸 🧟	2					
😑 🐻 localhost (SQL Serve	er 11					
■ 🛄 句服器角色						
⊡ 🖻 密碼編譯提供	者					
NP_Audit		م مر خل مع بدر حم				
图 🦲 伺服器物件		新增梢核(N)				
		啟用稽核(E)				
		檢視稽核記錄(V)				
		編寫稽核的指令碼為(S) ▶				
		原則(O) ▶				
		Facet(A)				
		愈動 PowerShell(H)				
		報表(E) ▶				
		重新命名(M)				
		刪除(D)				
< 111		屬性(R)				
就緒						



(6) 按 [關閉]

٩,	啟用和	曽核		- 🗆 X
🐼 威功	1 總計 1 成功		0 0	錯誤 警告
詳細資料(D):				
動作		狀態		訊息
🥝 啟用稽核 'NP_Audit'		成功		
				關閉(C)



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

料庫稽核規格...]

Solution1 - Microsoft SQL S 檔案(F) 編輯(F) 檢視(V) 専案(P)	Server Manageme ×
: 🛅 • 四 • 💕 📓 🥥 🔔 新增查	
 ○ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
 □ □	
	新增資料庫稽核規格(N)
 ① 回版 茲 物件 ① 直 複寫 	篩選(T) ▶
田	
Image: The service of a se	
	重新整理(F)
就緒	



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

按 [催足]	
--------	--

5	建立資料庫稽核規格					x נ			
🛈 就緒									
選取頁面	<u> </u> 指令碼	▼ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
·▲ 一股									
	名稱(N	I): NP_DB-Ncloud_Audit							
	稽核(A): NP_Audit							~
	動作:								-
		稽核動作類型		物件類別	物件結構描述	物件名稱		主體名稱	
	01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	~	~					
	02	SCHEMA_OBJECT_CHANGE_GROUP	~	~					
	03	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~					
連接	04	DATABASE_CHANGE_GROUP	~	~					
đ¥ localhost [sa]	05	AUDIT_CHANGE_GROUP	~	~					
	06	USER_CHANGE_PASSWORD_GROUP	~	~					
	07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	~	~					
<u> </u>	08	FAILED_DATABASE_AUTHENTICATION_GROUP	~	~					
進度	09	DATABASE_OBJECT_CHANGE_GROUP	~	~					
🔗 完成	▶*10		~	Ý					
-									
						確定	取消	說明	月





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



(10) 按 [關閉]

۵	啟用資料庫稽核規	1格 ×
🐼 成功	1 總計 1 成功	0 錯誤 0 警告
詳細資料(D):		
動作	狀態	訊息
② 取用資料庫稽核	梘格 NP_DB 成功	
		關閉(C)



3.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

(2.1) 使用 sa 帳號

PS C:\> sqlcmd	-S localhost -U sa -P npartne	r		
Σ		SQLCMD	_ □	x
Windows Pow 著作權(C)	erShell 2016 Microsoft Corpor	ation. 著作權所有,	並保留一切權利。	Â
PS C:∖Windo 密碼: 1〉	ws∖system32> sqlcmd -:	S localhost -U sa		~
<	Ш			>
Options:				
-S [protocol	:]server[instance_name][,port	:]		
-U login_id				
-P passwore	d			
-A dedicate	d administratror connection			

(2.2) 使用 Windows 帳號





(3) 切換資料庫



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

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



(5) 切換到稽核資料庫,範例:NCloud



紅色文字部位請輸入稽核資料庫名稱



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

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

1 > quit

λ	系統管理員: Windows PowerShell 📃 🗖	x	
1> 2> 3> 4> 5> 7> 8> 10 11 12 13 14 12	CREATE DATABASE AUDIT SPECIFICATION [NP_DB-Ncloud_Audit] FOR SERVER AUDIT [NP_Audit] ADD (DELETE ON DATABASE::[NCloud] BY [public]), ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP), ADD (SCHEMA_OBJECT_CHANGE_GROUP), ADD (DATABASE_OWNERSHIP_CHANGE_GROUP), ADD (DATABASE_CHANGE_GROUP), ADD (AUDIT_CHANGE_GROUP), ADD (USER_CHANGE_GROUP), ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP), > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP), > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP), > ADD (DATABASE_OBJECT_CHANGE_GROUP) > MITH (STATE = ON) > GO quit		^
PS <	C:\Windows\system32>	>	≻

紅色文字部位請輸入資料庫稽核規格名稱

1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]

紅色文字部位請輸入稽核資料庫名稱

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



3.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

3.3.1 網域

3.3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





(2) 新增組織單位

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

	Active Director	y 使用者和電腦	ă 🗕 🗖	x I
檔案(F) 動作(A) 檢視(V)) 說明(H)			
🗢 🏟 🖄 📰 📋	0 🗟 🔀	🐮 🛅 🗶 💈	ile.	
 Active Directory 使用者 儲存查詢 ■ 開 n-partner.local ■ Builtin ■ Computers ■ Domain Co ■ ForeignSec ■ Managed S ■ Users 	和電腦 名稱 Builtin Computers 委派控制(E) 尋找(I) 變更網域(D) 變更網域控制站(C) 提高網域功能等級(A) 操作主機(M)	類型 builtinDomain 容區	描述 Default container for u. Default container for d. Default container for s Default container for Default container for u.	- -
	新瑁(N) 彩石工作(10			
	所有工作(N) 檢視(V)	· 建相 ▶ 群組	^	
	重新整理(F) 匯出清單(L)	InetC msIm	DrgPerson naging-PSPs	
	內容(R)	MSN 20 det	AQ 佇列別名	
	說明(H)	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	¥₩	
使用者 共用資料夾				
建立一個新物件				



(3) 輸入組織單位名稱

新增物件 - 組織單位
建立在: n-partner.local/
名稱(A):
Server
✔ 保護容器以防止被意外刪除(P)
確定 取消 說明

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



(4) 移動伺服器至新的組織單位

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

-> 點選 [移動]





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	x
將物件移動到容器(<u>M</u>):	
In-partner Builtin Gomputers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Server Server Users	
確定 取消	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 SQL2012 伺服器已移動。





3.3.1.2 群組原則設定

(1) 開啟群組原則管理

開啟 [群組原則管理]



(2) 在 Servers 組織單位,新增群組原則物件

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





(3) 輸入群組原則物件名稱

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

	新增 GPO	x
名稱(<u>N</u>): N-Partner Policy		
來源入門 GPO(<u>S</u>): (無)		~
	確定取	消

(4) 編輯群組原則物件

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

■ 群組	
🔜 檔案(F) 動作(A) 檢視(V) 視窗	(W) 説明(H) - ×
🗢 🔿 📶 🗊 🖬 🖉	▶ <u>:</u>
 ▲ 計組原則管理 ▲ 掛 樹系: n-partner.local ▲ 調 n-partner.local ▲ 回 Default Domain Pol ▷ 回 Domain Controllers ▲ 回 Server ● ○ Partner Policy ▷ ○ 群組原則物件 ▷ ○ 和組原則物件 ▷ ○ 入門 GPO ▷ ○ 群組原則模型 ○ 詳組原則結果 	n-partner.local 状態 已連結的群組原則物件 < > 此頁面顯示此網域之 Active Directory和 SYSVOL (DFSR) 複 寫的狀態,因為它與群組原則有 理報##4/400x8/ 編輯(E) 強制(N) 酸用連結(L) 儲存報告(S) 從這裡開啟新視窗(W) 刪除(D) 重新 命名(M) 重新整理(F) 說明(H)
開啟 GPO 編輯器	



(5) 本機原則:稽核原則

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





(6) 事件記錄檔:應用程式記錄保持方法

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



(7) 事件記錄檔:應用程式記錄檔大小最大值

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



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

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



(9) 更新 MS SQL Server 群組原則

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

$\mathbf{\Sigma}$	系統管理員: Windows PowerShell 📃 🗖	x
PS PS	C:\> Invoke-GPUpdate -Computer SQL2012 -RandomDelayInMinutes 0 -Force C:\>	^ ~
<	III	>

紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表



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



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

\sim					_ D ×	C
()	E:\tmp\SQL2012.html	D-0	N-PARTNER\SQL2012	×	🕀 🖈 🗄	Ċ;
		群組	原則結果			
N-PA	ARTNER\SQL2012					· _
資料收	(集: 22/10/2021 10:13:34				顯示全部	
摘要					顯示	
電腦詳	細資料				<u> </u>	
一般					顯示	
元件别	犬態				顯示	
設定					医藏	
原則					<u> </u>	
Wi	indows 設定				<u> </u>	
3	安全性設定				<u> </u>	
	帳戶原則/密碼規則				顯示	
	帳戶原則/帳戶鎖定原則				顯示	
	本機原則/緒核原則				<u> </u> 匿藏	
	原則	設定	ę	憂勢 GPO		
	稽核帳戶登入事件	成功,约	失敗 ▶	N-Partner Poli	зy	
	稽核帳戶管理	成功,约	失敗 ▶	N-Partner Poli	y .	
	稽核登入事件	成功,约	失敗 ▶	N-Partner Poli	х У	
	本機原則/安全性選項				顯示	
	事件記錄檔				<u> </u>	
	原則	設定	6	憂勢 GPO		
	應用程式記錄保持方法	視需要で	而定 ト	N-Partner Poli	y .	
	應用程式記錄檔容量最大值	204800	KB N	N-Partner Poli	су У	
	公開金鑰原則/憑證服務用戶端 - 自	動註冊設定			顯示	
	公開金鑰原則/加密檔案系統				顯示	
群組厚	〔則物件				顯示	
WMI	篩選器				顯示	
使用者	詳細資料				顯示	\sim



3.3.2 工作群組

3.3.2.1 稽核原則設定

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



(2) 搜尋群組原則物件編輯器並執行

輸入群組原則 -> 點選 [編輯群組原則]





(3) 本機原則:稽核原則

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





(4) 開啟 [Windows PowerShell]



(5) 更新群組原則





(6) 查看群組原則套用情形

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

▶ 系統管理員: Windo	ows PowerShell		x
PS C:\> auditpol /get /category:* 么然我这百时			^
類別/子類別	設定		
系統 安全性系統延伸	沒有稽	核	
系統完整性	成分與失	敗	
IPSEC driver 其他系統事件	としていた。 一次月稽核 成功與4	夫敗	
安全性狀態變更	「成功」		
夏人/夏山 登入	成功與失敗		
登出 「「「」」 「「」」	成功與失敗	¥ r	
IPsec 主要模式	成功與天見	ix 牧	
IPsec 快速模式 IPsec 並伸模式	成功與失敗	牧	
特殊登入	成功與失見	<u>ф</u>	
其他登入/登出事件 編略原則伺服嬰	成功吗 成功師	與失敗 生敗	
"使用者/裝置宣告	成功與	英殿	
物件存取 禮室系統	沒有稽核		
	沒有稽核		
核心物的件 SAM	没月稽核 沒有稽核		
憑證服務 臺遊服務出現————————————————————————————————————	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	÷+**	
)没月稽 	该	
檔案共用	沒有稽核	-~	
	(2月4) 没有稽相	省12 亥	
其他物件存取事件	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	稽核 资	
却除式存放裝置	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	× 核	
集中原則暫存 转離機能	沒有稽相	亥	
非機密特殊權限使用	沒有	稽核	
Ⅰ 其他特殊權限使用事件 綴宓转務權限使用	沒有 沒有新	肎稽核 渗核	
詳細追蹤	/文月1		
■ 建立處理程序 終止處理程序	沒有稽析 沒有稽析	炙 弦	
DPAPI活動	沒沒	^	
RPC 事件 原則變更	没月稽核		
驗證原則變更	成功	÷ };	
」授權原則變更 MPSSUC 規則層級原則變更	沒有檔1 沒有積	沒 詟核	
	沒有	灌核 器技	
	」 成功	音192	
帳戶管理	成计照	生 胎	
電腦帳戶管理	成功與	夫敗	
- 安全性群組管理 - 發佈理組營理	成功與 成功與	!失敗 ≨敗	
應用程式群組管理	成功	真矢取	
	成功	興失敗	
目錄服務變更	沒有稽相	亥 杂	
日邨服務援舄 詳細目錄服務複寫	一 没有稽怀。 沒有新	_交 稽核	
目錄服務存取	成功		
Kerberos 服務票證操作		夫敗	
其他帳戶登入事件 Keybeyos 輪發肥發	成功調	與失敗 世	
認證驗證	成功與大則	b b	
			>
	1		- 33



3.3.2.2 事件檔案設定

(1) 開啟搜尋

將滑鼠移到右下角點選 [搜尋]



(2) 搜尋事件檢視器並執行

輸入事件檢視器 -> 點選 [事件檢視器]





(3) 編輯安全性記錄

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





(4) 設定應用程式記錄檔

輸入最大記錄檔大小: 204800 KE	3 <mark>註:請依客戶環境調整</mark> _	-> 點選	[視需要覆寫事件]	-> 按	[確定]
----------------------	-----------------------------	-------	-----------	------	------

	記錄內容 - 應用程式 (類型: 系統管理)	
一般訂閱		
全名(F):	Application	
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Application.evtx	
記錄檔大小:	3.07 MB(3,215,360 位元組)	
建立日期:	2021年6月11日 17:44:03	
修改日期:	2021年7月5日 10:39:17	
存取日期:	2021年6月11日 17:44:03	
存取日期: 201年6月11日 17:44:03 ✓ 飲用記錄(C) ★ 一日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		
確定 取消 套用(P)		


4. SQL 2016

4.1 稽核登入

啟用登入稽核,以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。 以下分別為圖形介面和指令介面設定方式。

4.1.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

🚽 連線至伺服器		×
	SQL Server	
伺服器類型(T):	資料庫引擎	~
伺服器名稱(\$):	localhost	~
驗證(A):	SQL Server 驗證	~
登入(L):	sa	~
密碼(P):	****	
	☑ 記住密碼(M)	
	連線(C) 取消 說明	選項(O) >>



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

😥 Microsoft S 快速啟動 (Ctrl-	PQ)		P	-		x
檔案(F) 編輯(E) 檢視(V) 偵錯	(D)	工具(T)	視識	5(W)	說明	∃(H)
G - O 🏠 - 🖆 - 🚔 🗎	•	🗎 新増査詢](N)			XHLA =
物件總管 ▼ ₽ × 連線 ▼ 単 × ■ ▼ C 小						
 ■ Calhost (SQL Server 13.0.1) ● 資料庫 ● 安全性 ● 伺服器物件 ● 複寫 ● PolyBase ● Always On 高可用性 ● 管理 ● Integration Services 目錄 ● SQL Server Agent ● YEvent 分析工具 		· · · · · · · · · · · · · ·	D) Q) 器(M) 器(M) erShe	+II(H)		
計在	J					
初心神台						



(4) 選擇 [安全性] 頁面 -> 點選登入稽核: [失敗和成功的登入] -> 勾選選項: [啟用通用條件合規性] -> 按 [確定]

🚪 伺服器屬性 - SQL2016		_		\times
選 取頁面	🖵 指令碼 🔻 😮 說明			
 一板 記憶體 「広理器 安全性 連線 資料庫設定 進階 離限 	 伺服器驗證 ○ Windows 驗證模式 (W) ● SQL Server 及 Windows 驗證模式 (S) 登入稽核 ○ 無(N) ○ 僅限失敗的登入(F) ○ 僅限成功的登入(D) ● 失敗和成功的登入(B) ④ 個服器 Proce 幅戶 			
連線	□加器 HOXY 帳戶(V)			
伺服器: localhost 連接: sa ₩ 檢視連接屬性 進度	Proxy 帳戶(R): 密碼(P): 濫項 □ 啟用通用條件合規性(O) □ 啟用 C2 稽核追蹤(E) □ 跨資料庫擁有權鏈結(C)			
		確定	Ę	刘肖



(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]

😡 Microsoft S 快速啟動 (Ctrl	+Q)		٩	-		x
檔案(F) 編輯(E) 檢視(V) 偵銷	ŧ(D)	工具(T)	視窗	(W)	說明	∃(H)
G • O 📅 • 🛅 • 🚰 💾 🖁	• •	圖 新増査詢	i(N)		DHX	XHLA =
物件總管 マリン 連線マ 草 ×草 ■ マ C 小 □ 記 localhost (SQL Server 13.0.1)]					
■ 資料庫 □ ■ 安全性		連接(C)				
田 単 女王性 田 ■ 伺服器物件		中斷連接(D)			
		註册(G)			_	
⊕ 🛑 PolyBase		新増査詢((Q)			
I Always On 局可用性		活動監視器	≸(M)			
		啟動(S)				
SQL Server Agent (已停用)		停止(T)				
⊞ XEvent 分析工具		暂停(U)				
		繼續(E)				
		重新啟動(/	4)			
		原則(O)			×	
		Facet(A)				
		啟動 Powe	erShell	(H)		
		報表(P)			۲	
		重新整理(F)			
		屬性(R)				
就緒						.4

(6) 按 [是] 重新啟動 MS SQL SERVER 服務

Microso	Microsoft SQL Server Management Studio							
?	您確定要重新啟動 SQL 2016 上的 MSSQL SER VER 服務嗎?							
		是(Y)	否 <mark>(</mark> N)					



(7) 按 [是] 停止 SQL SERVER Agent 服務

Microso	ft SQL Server Management Studio		
?	停止此服務也會停止 SQL Server Agent (MSSQLSER VER)。要繼續嗎?		
Ē		是(Y)	否(N)



4.1.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

(2.1) 使用 sa 帳號



(2.2) 使用 Windows 帳號



(3) 切換資料庫



(4) 使用 sp_configure 列出進階選項

1 > exec sp_configure 'show advanced options2 > go	s', 1			
1 > reconfigure				
2 > g0				
SQLCMD		_		×
1> exec sp_configure 'show advanced options',	1			^
41 wood and anced options' 從 O 變更為 1	1。諸執行 RECONFIGURE	陳述式	來安裝。	
1> reconfigure 2> go				
1> _				×
<				> .a

(5) 啟用失敗和成功的登入記錄

(6) 重新啟動 MS SQL SERVER 服務

(0) =		נעניאנו		
1 > !!!	NET STOP SQLSERVERAG	GENT		
2 > !!	> !!NET STOP MSSQLSERVER			
3 > !!	NET START MSSQLSERVE	R		
4 > !!	NET START SQLSERVERA	GENT		
Σ	SQLCMD	- 0	Х	
1> !!! SQL So SQL So	NET STOP SQLSERVERAGENT erver Agent (MSSQLSERVER) 用 erver Agent (MSSQLSERVER) 用	務正在停止 <u>.</u> 務已經成功停」	^	
2> !!! SQL Sa SQL Sa	NET STOP MSSQLSERVER erver (MSSQLSERVER) 服務正在 erver (MSSQLSERVER) 服務已經	停止. 旅功停止。		
3> !! SQL SG SQL SG	NET START MSSQLSERVER erver (MSSQLSERVER) 服務正在 erver (MSSQLSERVER) 服務已經	- 啟動 - 殷動成功。		
4> !! SQL So SQL So	NET START SQLSERVERAGENT erver Agent (MSSQLSERVER) A erver Agent (MSSQLSERVER) A	3務正在啟動 3務已經啟動成1	叻。	
5> 🛓			~	
<			>	



4.2 設定稽核

4.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業,例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

4.2.1.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

🚽 連線至伺服器	×
	SQL Server
伺服器類型(T):	資料庫引擎
伺服器名稱(\$):	localhost 🗸
驗證(A):	SQL Server 驗證 🛛 🗸
登入(L):	sa 🗸 🗸
密碼(P):	****
	☑ 記住密碼(M)
	連線(C) 取消 說明 選項(O) >>



Microsoft S	快速啟動 (Ctrl+Q)	₽ = ¤ ×
檔案(F) 編輯(E)	檢視(V) 偵錯(D) 工具(T)	視窗(W) 說明(H)
G - O 🏠 -	🔄 - 놀 🔛 💕 🔔 新増査調	I(N) 🗋 📸 📸 🚆
物件總管	- ₽ ×	
連接 ▼ 副 副 = 5	T C 📓	
🖃 🐻 localhost (SQ	L Server 13.0.5026.0 - sa)	
□ □ 安全性		
🗉 🧰 登入		
🗉 🗀 伺服器	角色	
🗉 🚞 認證		
🛛 🗀 密碼編	譯提供者	
		1
🕀 🧰 伺服	新増稽核(N)	
● 📄 伺服器物	66週(円)	
⊕ PolyBas	啟動 PowerShell(H)	
🕀 🛄 AlwaysC		
	+K-1x(F)	
Integrat	重新整理(F)	
H D SQL Ser-	- Agent	
計续		
dyLane		

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



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

<mark>核記錄儲存於 Windows 事件檢視器的應用程式記錄</mark> -> 按 [確定]

晃 建立稽核		_		×
🕕 就緒				
選取頁面	🕤 指令碼 👻 😮 説	明		
▶ 一般 ▶ 篩躍				
B-PASE	稽核名稱(N):	NP_Audit		
	佇列延遲 (以毫 秒為單位)(Q):	1000		•
	於稽核記錄失 敗時:	 ● 繼續(C) ○ 周期(司昭昭(3)) 		
		 ○ 含操作失敗(F) 		
	稽核目的地(D):	應用程式記錄檔		\sim
	檔案路徑(P):			
	稽核檔案數目 上限:	● 最大換用檔案(0):		
		 ● 最大檔案數目(X): 		
		檔案數目(B): 2147483647		A V
	檔案大小上限	0 (MB(M)) GB(ЭОТ	B(T)
	(Z):	✓ 無限制(L)		- (-)
	- 保留磁碟空間	引(R)		
連線				
y ₩ localhost [sa]				
檢視連線屬性				
進度				
就緒				
		確定 取消	說明	月 .:



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

Wicrosoft S 快速館 檔案(F) 編輯(E) 檢視(V G - 〇 約 - 1 - 9	攻動 (Ctrl+Q) 偵錯(D	2))) 工具(T) 🗐 新増査論	♪ 視窗(∮(N) 』	₩) È 🕅	□ 說明	× (H)
 物件總管 連線 - 草 ×草 ■ ○ ◎ localhost (SQL Server) ● 資料庫 ● 安全性 ● 登入 ● 伺服器角色 ● 配数證 ● 電磁 ● 個服器稿様規 ● 伺服器物件 ● 複寫 ● PolyBase ● Always On 高可用 ● 管理 ● Integration Servi ● SQL Server Ager ● XEvent 分析工具 	 · · · × er 13.0.1(稽核(N) 稽核(E) 稽核記錄(V) 稽核的指令碼 (O) et(A) PowerShell(I (P) 命名(M) (D) 整理(F) (R)	為(S) H)	•		
就緒						



(6) 按 [關閉]

₽ 啟用稽核				—		×
🐼 威功	1 1	總計 成功		0 0	錯誤 警告	
詳細資料(D):						
動作			狀態		訊息	
🥝 啟用稽核 NP_Audit'			成功			
					關閉((C)

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





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

[確定]

〕就緒								
異取頁面	_ 指令碼	✔ 😧 說明						
▶ —殷	名稱(N) 稽核(A)): NP_Server_Audit NP_Audit						
	動作:	稽核動作類型		物件類別	物件結構描述	物件名稱	主體名稱	
	01	SUCCESSFUL_LOGIN_GROUP	~	~				
	02	FAILED_LOGIN_GROUP	~	~				
	03	LOGOUT_GROUP	~	~				
	04	SERVER_STATE_CHANGE_GROUP	~	~				
	05	SERVER_OPERATION_GROUP	~	~				
	06	SCHEMA_OBJECT_CHANGE_GROUP	~	~				
瀑	07	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~				
localhost [sa]	08	DATABASE_CHANGE_GROUP	~	~				
	09	AUDIT_CHANGE_GROUP	~	~				
	10	USER_CHANGE_PASSWORD_GROUP	~	~				
<u>視連線屬性</u>	11	SERVER_OBJECT_CHANGE_GROUP	~	~				
 王 小	▶ 12	DATABASE_OBJECT_CHANGE_GROUP	~	~				
✓ 元成	*13		~	~				
<u> </u>								



😥 Solution1 - Microsoft S 快速啟	(動 (Ctrl+Q) 🛛 🔎 🗕 🗖 🗙
檔案(F) 編輯(E) 檢視(V) 專案(P)	偵錯(D) 工具(T) 視窗(W) 說明(H)
80.01*******	
	입의 채가비르 HO(LA) 입의 MDX, DMX, XMLM DAX, GP 두
物件總管 ▼ ₽ ×	
連線 → 草 ×草 ≡ ▼ С	
□ 局 localhost (SQL Server 13.0.1)	
□ □ ~ ~	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	
₽ NP_Audit	
🖂 🛑 伺服器稽核規格	
🕂 NP_Server_Audit	
🗉 🛑 伺服器物件	新增伺服器稽核規格(N)
	啟用伺服器稽核規格(E)
	原則(O) ►
🗄 💀 SQL Server Agent	Facet(A)
. I XEvent 分析工具	啟動 PowerShell(H)
	報表(P) ▶
	屬性(R)
÷#//#	
4/L#B	

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



(10) 按 [關閉]

🧖 啟用伺服器稽核規格			—		×
🕢 成功	1 總計 1 成功		0 0	錯誤 警告	
詳細資料(D):					
動作		狀態		訊息	
🥝 啟用伺服器稽核規格 N	IP_Serve	成功			
				國民	月 (C)



4.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows Powershell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號



(3) 切換資料庫



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

1 > CREATE SERVER AUDIT [NP_Audit]

- 2 > TO APPLICATION_LOG
- 3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
- 4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)

5 > <mark>GO</mark>



紅色文字部位請輸入稽核名稱



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

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



紅色文字部位請輸入伺服器稽核規格名稱



4.2.2 稽核資料庫層級

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

以下分別為圖形介面和指令介面設定方式。

4.2.2.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

및╸連線至伺服器	×
	SQL Server
伺服器類型(T):	資料庫引擎
伺服器名稱(\$):	localhost 🗸
驗證(A):	SQL Server 驗證 🛛 🗸 🗸
登入(L):	Sa ~
密碼(P):	****
	☑ 記住密碼(M)
ž	〔線(C)





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



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

核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

🍢 建立稽核			_		\times
🕕 Ready					
Select a page	Script → I Hel 稽核名稱(N): 佇列延遅(以 毫秒為單位) (Q): 於稽核記錄失 問時.	p NP_Audit 1000 ● 繼續(C)			÷
	照時: 稽核目的地(D): 檔案路徑(P): 稽核檔案數目 上限: 檔案大小上限	 □ 關閉伺服器(S) ○ 令操作失敗(F) 應用程式記錄檔 □ 最大換用檔案(O): □ 最大檔案數目(X): 檔案數目(B): 2147483647 □ MB 	(M) (MB)	а) _О т	► B(T)
		☑ 無限制(L) 罰(R)			
Connection					
Iocalhost [sa]					
<u>慨倪理接團性</u>					
Progress Ready					
		確定	取消	說明	A



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

Microsoft S 快速啟動(Ctrl+Q)	
福案(F) 編輯(E) 檢視(V)	偵錯(D) 工具(T) 視窗(W)	說明(H)
🍈 G + O 🛛 🎦 + 🛅 + 當 🖥	🛯 📲 📜 新増査詢(N) 🛯 🏠 📸	📸 😳 🍟
物件總管	• ₽ ×	
連接 🕈 🛃 📕 🝸 🖒 🍒		
😑 🐻 localhost (SQL Server 13	.0.5026.0 - sa)	
🕀 📄 資料庫		
🖂 🚞 安全性		
🗉 🚞 伺服器角色		
■ 📄 密碼編譯提供者		
💦 NP_Audit		
	新增稽核(N)	
	啟用稽核(E)	
	檢視稽核記錄(V)	
业 Mail AlwaysOn 同可开	編爲相核的指マ犒氛(S) ▶	
世 Integration Servi	原則(O) ▶	
	Facet(A)	
🗄 🔟 SQL Server Ager		
	啟動 PowerShell(H)	
	報表(P) ▶	
	重新命名(M)	
	刪除(D)	
	重新整理(F)	
	屬性(R)	
就緒		



(6) 按 [關閉]

🔍 啟用稽核				_		×
🐼 威功	1	總計 成功		0 0	錯誤 警告	
詳細資料 <mark>(</mark> D):						
動作			狀態		訊息	
🥝 啟用稽核 'NP_Audit'			成功			
					6 9	閉(C)



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

料庫稽核規格...]





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

按 [確定]

딣 建立資料庫稽核規格							-	
<u>()</u> 就緒								
選取頁面 ダ 一般	 「」指令碼 名稱(N) 稽核(A) 動作: 	▼ ② 説明): NP_DB-NCloud_Audit): NP_Audit		÷				~
		稽核動作類型		物件類別	物件結構描述	物件名稱	主體名種	я I
	01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	~	~				
	02	SCHEMA_OBJECT_CHANGE_GROUP	~	~				
	03	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~				
	04	DATABASE_CHANGE_GROUP	~	~				
連線	05	AUDIT_CHANGE_GROUP	\sim	~				
q₩ localhost [sa]	06	USER_CHANGE_PASSWORD_GROUP		~				
	07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	IECT_OWNERSHIP_CHANGE_GROUP					
	08	FAILED_DATABASE_AUTHENTICATION_GROUP	~	~				
檢視連線屬性	09	DATABASE_OBJECT_CHANGE_GROUP	~	~				
進度	10	DATABASE_ROLE_MEMBER_CHANGE_GROUP	\sim	~				
就緒	▶ *1 1		~	~				
						確定	取消	說明



😡 Solution1 - Microsoft SQL Server 快速啟動	(Ctrl+Q)
檔案(F) 編輯(E) 檢視(V) 專案(P) 偵錯(D)	工具(T) 視窗(W) 說明(H)
🦉 🗸 💿 🛛 📸 🖌 🛅 🖌 🍟 🔛 新増査	前(N) 🛢 📾 📾 📾 🐼 🕹 🗗 台 🗒 🚆
物件總管 ▼ 및 ×	
連線 - 単 ×単 = ▼	
🖃 🔀 localhost (SQL Server 13.0.1601.5 - sa)	
□ ■ 資料庫	
🗉 💼 系統資料庫	
④ ■ 資料庫快照集	
□	
🗉 🔲 外部資源	
😠 💼 同義字	
④ 🛑 可程式性	
④ ■ 簡仔證	
🗉 💼 結構描述	
🗉 🛑 非對稱金鑰	
I ■ 對佛玉靖	
Always Encrypted 亚旗	
Regional Audit	
😠 💼 安全性原則	新増資料庫稽核規格(N)
	啟用資料庫稽核規格(E)
	组窗姿料庙蕴按坦热的铝金珊瑚(C) 、
	編為具科/単恒仪成10的指マ%的荷(5) ▶
□ □ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎ ◎	原則(O) ▶
□ □ □ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Facet(A)
₽ NP_Audit	啟動 PowerShell(H)
→ 同服器稽核規格	
	¥Q-to(P) ►
图 I PolyBase	刪除(D)
····································	重新整理(F)
	屬性(R)
⊛ 🛑 Integration Services 目錄	
新 续	

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

(10) 按 [關閉]

Q ● 啟用資料庫稽核規格			—		\times
🕢 成功	1 總計 1 成功		0 0	錯誤 警告	
詳細資料(D):					
動作		狀態		訊息	
🥝 啟用資料庫稽核規格	NP_DB-N	成功			
				88 8	閉(C)



4.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號





(3) 切換資料庫

0) 切入其相样	
> use master	
2 > go	
🔁 SQLCMD — 🗆	×
> use master ?> go 已將資料庫內容變更為 'master'· .> _	•
<	>

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

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

		0)
5	>	(-	
-		-	-

Z		—		×	
CREATE SERVER AUD	T [NP_Audit]				^
TU APPLICATION_LU	י – 1000 - 00 קטננוו	Ф Р – СОМТ	INTE Y		
ALTER SERVER AUDI	[NP Audit] WITH	I (STATE =	ON)		
GO					
_					×
				>	
	≥ 選取 SQLCMD CREATE SERVER AUDI TO APPLICATION LOG WITH (QUEUE_DELAY ALTER SERVER AUDIT GO	≥ 選取 SQLCMD CREATE SERVER AUDIT [NP_Audit] TO APPLICATION LOG WITH (QUEUE_DELAY = 1000, ON_FAILU ALTER SERVER AUDIT [NP_Audit] WITH GO	■ 選取 SQLCMD — CREATE SERVER AUDIT [NP_Audit] TO APPLICATION LOG WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONT ALTER SERVER AUDIT [NP_Audit] WITH (STATE = GO	■ 建取 SQLCMD □ CREATE SERVER AUDIT [NP_Audit] TO APPLICATION LOG WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE) ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON) GO	Z 選取 SQLCMD □ × CREATE SERVER AUDIT [NP_Audit] TO APPLICATION_LOG WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE) ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON) GO

紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫,範例:NCloud



紅色文字部位請輸入稽核資料庫名稱



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

1 > CREATE DATABASE AUDIT	SPECIFICATION [NP_DB-NCloud_A	Audit]	
2 > FOR SERVER AUDIT [NP_A	udit]		
3 > ADD (DELETE ON DATABAS	SE::[<mark>NCloud]</mark> BY [public]),		
4 > ADD (SCHEMA_OBJECT_PI	ERMISSION_CHANGE_GROUP),		
5 > ADD (SCHEMA_OBJECT_C	HANGE_GROUP),		
6 > ADD (DATABASE_OBJECT_	OWNERSHIP_CHANGE_GROUP),		
7 > ADD (DATABASE_CHANGE	_GROUP),		
8 > ADD (AUDIT_CHANGE_GRO	DUP),		
9 > ADD (USER_CHANGE_PAS	SWORD_GROUP),		
10 > ADD (SCHEMA_OBJECT_O	DWNERSHIP_CHANGE_GROUP),		
11 >ADD (FAILED_DATABASE_	AUTHENTICATION_GROUP),		
12 > ADD (DATABASE_OBJECT	_CHANGE_GROUP),		
13 > ADD (DATABASE_ROLE_N	IEMBER_CHANGE_GROUP)		
14 > WITH (STATE = ON)			
15 > GO			
A mult			



紅色文字部位請輸入資料庫稽核規格名稱

1 > CREATE DATABASE AUDIT SPECIFICATION [NP DB-NCloud Audit

紅色文字部位請輸入稽核資料庫名稱

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



4.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

4.3.1 網域

4.3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





(2) 新增組織單位

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

🧧 Active Directory 使用者	和電腦				_		×
檔案(F) 動作(A) 檢視(V) 說明(H)						
🗢 🔿 🖄 📊 📋 📺] 🖬 📑 🚘 🔊 [8 🛅	7 🔎	- ⁶ 8			
 Active Directory 使用者: 留存查詢 留 内 百 前 Builtin Computers Domain Co	和電腦 名稱 Builtin 委派控制(E) 尋找(I) 變更網域(D) 變更網域控制站(C) 提高網域功能等級(A) 操作主機(M)	類型 builti	nDoma ፤位	描述 Default conta Default conta Default conta Default conta Default conta	ainer for u ainer for d ainer for s ainer for ainer for u		
	新増(N)	>	電	1886 1886			
	所有工作(K)	>	通	植給人			
	檢視(V)	>	帮	ŧ組			
	重新整理(F) 匯出清單(L)		in m	ietOrgPerson isDS-ShadowPrinc isImaging-PSPs	ipalContain	er	
	內容(R)		N	ISMQ 佇列別名			
	說明(H)	[維	1織單位			
		_	Ę	〕表機			
			使	使用者			
			共	共用資料 夾			
<	>						
建立一個新物件							



(3) 輸入組織單位名稱

新増物件 - 組織單位	×
建立在: n-partner.local/	
名稱(<u>A</u>):	
Servers	
☑ 保護容器以防止被意外刪除(P)	
確定 取消 說明	

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



(4) 移動伺服器至新的組織單位

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

-> 點選 [移動]





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	Х
將物件移動到容器(<u>M</u>):	
 n-partner Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Servers Users 	
確定 取消	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 SQL2016 伺服器已移動。

📔 Active Directory 使用者和電腦	_	
檔案(F) 動作(A) 檢視(V) 說明(H)		
🗢 🔿 📶 🦌 📋 🗙 🖼 🧟 🕞 🛛 🖬 🗏 📚 🛅	7 🖻	۲. Be
 Active Directory 使用者和電腦 ○ 儲存查詢 ◇ 圖 協存查詢 ◇ 圖 Builtin ③ Computers > 圖 Domain Controllers > 圖 ForeignSecurityPrincipa > 圖 Managed Service Acco ③ Servers 	描述	



4.3.1.2 群組原則設定

(1) 開啟群組原則管理





(2) 在 Servers 組織單位,新增群組原則物件

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




(3) 輸入群組原則物件名稱

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

新增 GPO	×
名稱(№):	
N-Partner Policy	
來源入門 GPO(<u>S</u>):	
(無)	~
	確定 取消

(4) 編輯群組原則物件

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

🔜 群組原則管理	– 🗆 X
🔜 檔案(F) 動作(A) 檢視(V) 視窗(W)	說明(H) _ & ×
🗢 🔿 🙋 📰 📋 📓 🐼 🛐	
	n-partner.local
 ✓ △ 個示: n-partner.iocai ✓ 圖 網域 	狀態 已連結的群組原則物件 群組 ◆ ▶
 in-partner.local Default Domain Policy Domain Controllers Servers 	此頁面顯示此網域之 Active Directory 和 SYSVOL 複寫的狀態,因為它與群 組原則有關。
🛒 N-Partner Policy	44.55.54.40.55.20
> 前田原則物件	編輯(E)
> Ling WMI 師選茲 > Chi 入門 GPO	弹制(N)
> 确站	啟用連結(L) 非密印方
おお おお 日本	儲存報告(S) 医真肌特
■武群組尽則結果	從這裡開啟新視窗(W) 鈕,從 由收集基
	刪除(D)
	重新命名(M)
	重新整理(F)
	說明(H)
開啟 GPO 編輯器	,



(5) 本機原則:稽核原則

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

件], [稽核帳戶管理], [稽核登入事件] 項目 -> 勾選 [定義這些原則設定]: & [成功] & [失敗] -> 按 [確定]





(6) 事件記錄檔:應用程式記錄保持方法

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





(7) 事件記錄檔:應用程式記錄檔大小最大值

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

> 勾選 [定義這個原則設定] -> 輸入 204800 KB <mark>註:請依客戶環境調整</mark> -> 按 [確定]





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



(9) 更新 MS SQL Server 群組原則

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



紅色文字部位請輸入 MS SQL Server 伺服器名稱

(10) 產生 MS SQL Server 伺服器群組原則報表



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



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

中口 中口 ●				– 🗆 X
群組原則結果 N-PARINER/SQL2016 室は刻集:2021/10/22 TF 01:56:47 全部要素 確果 単元 確果 単元 管調算確意料	😓 🔿 🗿 C:\tmp\SQL2016.html	P → C 🥔 N-PARTNER\SQL2016	×	슈 ☆ 쁖 🙂
N-PARINER/SQL2016 全部単元 資素		群組原則結果		
	N-PARTNER\SQL2016			
	資料收集: 2021/10/22 下午 01:56:47			全部顯示
電話 第第 一会 第第 元件状態 第示 第2 第示 第2 第章 第2 第章 文官臣定 第章 東川 第章 第章 東川 第章 第章 東川 「「「」」」」」」 第章 東川 「「」」」」」」」 第章 東川 「」」」」」」 第章 東川 「「」」」」」」 第章 東川 「「」」」」」」 第章 東川 「」」」」」」」 第章 東川 「」」」」」」」 「」」」」 東川 「」」」」」」」」 「」」」」」 東川 「」」」」」」 「」」」」 東川 「」」」」」」 「」」」」 東川 「」」」」」 「」」」 東川 「」」」」」 「」」」 東川 「」」」 「」」」 「「」」」」 「」」」 「」」」 「「」」」」 「」」」 「」」」 「「」」」」 「」」」 「」」」 「「」」」」」」 「」」」」 「」」」	摘要			顯示
→化 協業 ス井秋玉 御示 第201 福示 第21 「「「「「「」」」」」」」」」」」」」」」」」」 第21 「「」」」」」」 第21 「「」」」」」 第21 「「」」」」 第21 「「」」」」」 第21 「「」」」」 第21 「」」」」 第22 「」」」」 <t< td=""><td>電腦詳細資料</td><td></td><td></td><td></td></t<>	電腦詳細資料			
大井松志 編示 第2 編示 第2 第第 第2 第第 第2 第第 第2 第第 第2 第第 第2 第第 第月 第二 第二 第二 第二 </td <td>一般</td> <td></td> <td></td> <td></td>	一般			
設定 展示 DEL 厚蔵 Vindows 設定 厚蔵 文主性設定 厚蔵 使戶原則/或視規則 厚蔵 健戶原則/或視規則 一 健戶原則/或視規則 一 健戶原則/或視規則 一 健児間に 一 愛則 設定 優勢 GPO 増核集単合業 成功 ·失敗 N-Partner Policy 増核集単合業 成功 ·失敗 N-Partner Policy 増核集単の学生は選厚 成功 ·失敗 N-Partner Policy 単作記録信 成支 優勢 GPO 増和度非記録値音量 成功 ·失敗 N-Partner Policy 本機原則/安全性選厚 販売 - 原利 設定 優勢 GPO 増和量量に記録値音量 20480 KB N-Partner Policy 公開金値原則/流確認務用戶幅・自動註冊設定 - - 公開金鐘原則/加雪幅意素統 - - K#S管理整本 - - K#S管理整本 - - K#S管理整本 - - K#S管理整本 - - K - - K	元件狀態			顧示
展載 陽載 Windows 設定 陽載 女主性設定 陽載 健戶原則/虛唱規則 陽載 健戶原則/虛唱規則 周示 健戶原則/虛唱規則 周示 「原則 設定 優勢 GPO 智枝帳戶管理 成功 ·失敗 N-Partner Policy 智枝帳戶管理 成功 ·失敗 N-Partner Policy 「春根原則/安全性選項 成功 ·失敗 N-Partner Policy 「春秋原原則/安全性選項 一個 一個 「日程式記錄磁時方法 現需要而定 N-Partner Policy 「原則 設定 優勢 GPO 「日程式記錄磁時方法 現需要而定 N-Partner Policy 「原用程式記錄磁時月/強 1 日 「個和電式記錄碼時方法 現需要而定 N-Partner Policy 「成用程式記錄碼時月/論: 1 日 「公園金鐘原則/透證服務用戶端:				顧示
Windows 設定 隔壊 女主性設え 隔壊 転戸原則/客環規則 福菜 帳戸原則/客環規則 銀菜 「「日原則/客環規則] 日菜 「「日原則/電視原則/<				医藏
Windows 設定 隔端 安全性設定 6歳 帳戶原則/碳環規則 編示 帳戶原則/碳環規則 編示 年幾原則/磁長原則 編示 春期 設定 優勢 GPO 福枝県戶雪狸 成功 · 失敗 N-Partner Policy 福枝泉戶雪狸 成功 · 失敗 N-Partner Policy 福枝泉山牛牛 成功 · 失敗 N-Partner Policy 福枝泉山牛牛 成功 · 失敗 N-Partner Policy 福枝泉山牛牛 成功 · 失敗 N-Partner Policy 七枝泉山牛 成功 · 失敗 N-Partner Policy 七枝泉山牛 成功 · 失敗 N-Partner Policy 草用泉山/安全性螺頂 編示 編示 原則 設定 優勢 GPO 唐和信式記錄保持方法 福葉要而定 N-Partner Policy 原用電式記錄保持方法 視葉更而定 N-Partner Policy 次間金鐘原則/添證服務用戶端 - 自動註冊設定 編示 編示 素統管理範本 編示 編示 MI 餘送器 近 編示	JACK3			隱藏
安全性設定 隔端 幅戸原則/喀瑪規則 編元 幅戸原則/喀西銀回 編元 福原町 第元 「原町 設定 優勢 GPO 宿枝瓜戸宮山/南京山 成功、失取 N-Partner Policy 宿枝瓜戸管理 成功、失取 N-Partner Policy 宿枝瓜戸管理 成功、失取 N-Partner Policy 宿枝瓜戸管理 成功、失取 N-Partner Policy 「春秋原則/安全性選項 N-Partner Policy 編元 「春秋原則/安全性選項 「日本 「日本 「春秋原則/安全性選項 「日本 「日本 「日本 「日本 日本 「日本 「日本 日本 「日本	Windows 設定			馮藏
・ ・	安全性設定			に蔵
	帳戶原則/密碼規則			87
本機原則/緒核原則 設定 優勢 GPO 層則 設定 優勢 GPO 榕核师音型 成功 · 失取 N-Partner Policy 榕核戶音理 成功 · 失取 N-Partner Policy 榕核型 (成功 · 失取 N-Partner Policy 榕核型 (成功 · 失取 N-Partner Policy 糖核型 (成功 · 失取 N-Partner Policy 摩件記錄幅 成功 · 失取 N-Partner Policy 摩用 設定 優勢 GPO 原則 設定 優勢 GPO 原用程式記錄幅容量最大值 204800 K8 N-Partner Policy 位間金鐘原則//恣證服務用戶燭 - 自動註冊設定 顧示 顧示 A號答理整本 顧示 翻示 YMI 餘諾器 近 「	帳戶原則/帳戶鎖定原則			#875
原則 設定 優勢 GPO 箱枝帳戶登入事件 成功,失敗 N-Partner Policy 稽枝帳戶營理 成功,失敗 N-Partner Policy 稽枝億戶營及事件 成功,失敗 N-Partner Policy 宿枝園入事件 成功,失敗 N-Partner Policy 宿枝園入事件 成功,失敗 N-Partner Policy 華作記録宿 成功,失敗 N-Partner Policy 厚則 設定 優勢 GPO 應用程式記錄保持方法 根需要而定 N-Partner Policy 成間金鏞原則/次證服務用戶端 - 自動註冊設定 編示 公園金鏞原則/次證服務用戶端 - 自動註冊設定 編示 系統管理範本 編示 都原則/加密宿窓系统 野相民 近 「細示 1000 KB	本機原則/緒核原則			顯示
権核城戶登入事件 成功,失敗 N-Partner Policy 稽核城戶管理 成功,失敗 N-Partner Policy 稽核登入事件 成功,失敗 N-Partner Policy 權援原則/安全性選項 水子敷 N-Partner Policy 事件記錄檔 医見 優勢 GPO 應用程式記錄保持方法 視需要而定 N-Partner Policy 確認金鏞原則/憑證服務用戶端 - 自動註冊設定 正 顧示 公開金鏞原則/加寧檔案系統 顧示 詳細見明/加寧檔案系統 服示 詳細見明/加寧檔案系統 服示 詳細見明 加寧福泰 「日動註冊設定 正 詳細見明 「日動註冊設定 「日動註冊設定 正 詳細見明 「日助註冊設定 「日助註冊設定 「日助註冊設定 「日助註冊設定 「日勤註冊設定 「日勤註冊設定 「日勤註冊設定 「日勤註冊設定 「日勤註冊設定 「日勤記	原則	設定	優勢 GPO	靖臧
楷核條戶管理 棺核登入事件 成功,失敗 N-Partner Policy 本帳原則/安全性選項 事件記錄檔	稽核帳戶登入事件	成功,失敗	N-Partner Policy	
棺核登入事件 成功,失敗 N-Partner Policy 本機原則/安全性選項 羅示 事件記録檔 事件記録檔 原則 設定 原則 設定 原用程式記錄保持方法 視需要而定 N-Partner Policy 度用程式記錄檔會量最大值 204800 KB 公園金鏞原則/憑證服務用戶端 - 自動註冊設定 素統管理範本 群組原則物件 WMI 餘選器	稽核帳戶管理	成功,失敗	N-Partner Policy	
本機原則/安全性選項 預示 事件記錄檔 面示 原則 設定 優勢 GPO 應用程式記錄保持方法 視需要而定 N-Partner Policy 應用程式記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 工 羅示 系統管理範本 正 羅示 WILIKER	稽核登入事件	成功,失敗	N-Partner Policy	
事件記錄檔 廣則 設定 優势 GPO 應用程式記錄保持方法 視需要而定 N-Partner Policy 應用程式記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顕示 承統管理範本 顕示 翻示 評判 Year 評判 Year The policy WIL 誘送器 Year The policy	本機原則/安全性選項			麻子
原則 設定 優勢 GPO 應用程式記錄保持方法 視案要而定 N-Partner Policy 應用程式記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顕示 五丁 五丁 条統管理範本 五丁 新原則/協議器器 第二	事件記錄檔			
應用程式記錄保持方法 視需要而定 N-Partner Policy 應用程式記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顕示 公開金鏞原則/加密檔案系統 顕示 系統管理範本 顕示 ¥紅原則物件 顕示 WMI 餘蹉器 顕示	原則	設定	優勢 GPO	四方 相比
應用程式記錄檔容量最大值 204800 KB N-Partner Policy 公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顧示 公開金鏞原則/加密檔案系統 顧示 系統管理範本 顧示 詳組原則/物件 福示 WMI 餘凝器 顧示	應用程式記錄保持方法	視需要而定	N-Partner Policy	
公開金鏞原則/憑證服務用戶端 - 自動註冊設定 顧示 公開金鏞原則/加密檔案系統 顧示 系統管理範本 顧示 詳組原則物件 顧示 WMI 餘選器 顧示	應用程式記錄檔容量最大值	204800 KB	N-Partner Policy	
A開金鑰原則/加密檔案系統 顧示 系統管理範本 顧示 詳組原則物件 顧示 WMI 餘蹉器 顧示	公開金鑰原則/憑證服務用戶端 - 自動語	t冊設定		
<u>顧示</u> 系統管理範本 新統管理範本 群紙原則物件 WMI 餘蹉器 顧示	公開金鑰原則/加密檔案系統			鎺木
	系统管理箭本			<u>顧示</u>
WMI 餘麗器 顧示	彩印度印刷物件			顧示
				顧示
	WMI 碗建甜			顧示
使用者詳細資料	使用者詳細資料			顯示

4.3.2 工作群組

4.3.2.1 稽核原則設定

- (1) 開啟 [本機群組原則編輯器]
- 點選 🔎 [搜尋] -> 輸入群組原則 -> 點選 [編輯群組原則]

	最佳比	對				
ŵ		編輯群 控制台	組原則			
ŝ		ŝ	ß		□	1
	群組原	則				
	ρ	[[]]	e			



(2) 本機原則:稽核原則

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





(3) 開啟 [Windows PowerShell]



(4) 更新群組原則





(5) 查看群組原則套用情形

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

🔀 系統管理員: Windows PowerShell	— C	x c
PS C:\> <mark>auditpol</mark> /get /category:* 多統藉核原則		^
類別/子類別	設定	
水湖 安全性系統延伸 多全性系統延伸	没有稽核	
系統元程任 IPSEC driver	成切與失敗 沒有稽核	
其他系統事件 安全性狀態變更	成功與失敗 成功	
登入7登出 祭入	成功與生物	
	成功與失敗	
NRF頭足 IPsec 主要模式	成功與失敗	
IPsec 快速棋式 IPsec 延伸棋式	成功與失敗 成功與失敗	
│ 特殊登入 │ 其他習入/浴出事件	成功與失敗 成功與失敗	
- 網路原則伺服器 - 使用者/結果宣告	成功與关敗。	
医血石管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管管	成功與失敗	
物件存取 描案系統	<u>沒</u> 有稽核	
registry 核心物件	没月楷核 沒有稽核	
SAM 馮諍服務	沒有稽核 沒有稽核	
產生的應用程式	沒有稽核	
	沒有稽核	
- 師選平台到包去無 - 篩選平台連銀	沒有稽核 沒有稽核	
│ 其他物件存取事件 │ 詳細檔案共用	沒有稽核 沒有稽核	
□ 抽取式存放裝置 重中原則暫存	沒有稽核 沒有稽核	
特殊權限使用。	治有楚族	
了。 其他特殊權限使用 機物转動機使用	沒有稽核	
「海空行沐福附足用」 詳細追蹤 油注電調報	次方植物	
—————————————————————————————————————	沒有稽核 。 <u>沒</u> 有稽核	
DPAPI 活動 RPC事件	没月楷核 沒有權核	
隨插即用事件 Token Right Adjusted Events	沒有稽核 沒有稽核	
原則變更 ´ ´ ´ 「 藉核原則變更	成功	
· 驗證原則變更 透證原則變更	成功	
WPSSW在人名思维克 维护SSW在人名思维克	沒有稽核	
一師選半百原則變更 其他原則變更事件	沒月稽核 沒有稽核	
帳戶管理 - 電腦帳戶管理 _	成功與失敗	
安全性群組管理 發佈群組管理	成功與失敗 成功與失敗	
應用程式群組管理 其他帳戶管理事件	成功與失敗 成功與失敗	
※他派にはなり 使用者帳戶管理 1999 友服	成功與失敗	
	成功	
日報服務程度	沒 月 稽核 沒有稽核	
	没有稽核	
Kerberos 服務票證操作 其他帳戶登入事件	成功與失敗 成功與失敗	
Kerberos 驗證服務 認證驗證	成功與失敗 成功與失敗	
PS C:/>		×
<		>



4.3.2.2 事件檔案設定

(1) 開啟 [檢視事件記錄檔]

點選 🔎 [搜尋] -> 輸入事件記錄檔 -> 點選 [檢視事件記錄檔]

	最佳比	對				
ŵ		檢視事 控制台	件記錄	闣		
Ö		ŝ	ß			13
	事件言	己錄檔				
	ρ	[]]	e			



(2) 編輯安全性記錄

🛃 事件檢視器		_		×
檔案(F) 動作(A)	檢視(V) 說明(H)			
🔶 🏟 🕅 🚺 👔				
 書件檢視器 (本機) 局 自訂檢視 ♥ Windows 記録 ● 確田現式 	^{事件檢視器 (本機)} 概觀與摘要			
 ■ 100 m 42 × 100 ×	開啟已儲存的記錄(O) 建立自訂檢視(R) 匯入自訂檢視(M) 清除記錄檔(C)		 2適 資視	•
	前進日前的記錄(□) 內容(P)			
	尋找(N) 將所有事件另存為(E) 附加工作到此記錄檔中(A) 說明(H)		>	
< 顯示記錄檔內容。	>			

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



(4) 設定應用程式記錄檔

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

記錄內容 - 應用程式 (類型: 系統	充管理)	×
一般訂閱		
全名(F):	Application	
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Application.evtx	1
記錄檔大小:	1.07 MB(1,118,208 位元組)	-
建立日期:	2021年6月9日下午 11:31:09	
修改日期:	2021年7月5日 下午 03:46:08	
存取日期:	2021年6月9日 下午 11:31:09	
 ✓ 啟用記錄(E) 最大記錄檔大小 (KB)(X): 當事件記錄檔的大小到達 ● 視需要覆寫事件 (分 ○ 當記錄檔已滿時進 ○ 不要覆寫事件 (手重 	204800 上限時: 2週寫最酱的事件)(W) 行封存,不要覆寫事件(A) 訪清除記錄檔)(N) 清除記錄(R)	
	確定 取消 套用(P)	



5. SQL 2019

5.1 稽核登入

啟用登入稽核,以監視 SQL Server Database Engine 登入活動。設定後必須重新啟動 MS SQL Server 服務。 以下分別為圖形介面和指令介面設定方式。

5.1.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

🚽 連線至伺服器		×
	SQL Server	
伺服器類型(T):	資料庫引擎	\sim
伺服器名稱 <mark>(</mark> S):	localhost	7
驗證(A):	SQL Server 驗證	\sim
登入(L):	sa	7
密碼(P):		
	連線(C) 取消 說明 選項(O) >>	



(3) 在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [屬性]

🧏 Microsoft SQL Ser 快速啟動 (Ctrl+Q)	× 🗆 _ ۹
檔案(F) 編輯(E) 檢視(V) 專案(P) 工具(T) 視窗(W) 說明(H)
🛛 🖸 - 🗿 🖓 - 🛅 - 🎦 🔛 💕 📳 新増	查詢(N) 🗐 🕅 🕅 🕅 🕅 🚆
· 부 · 달 🗸 - 🗸 - 🕹	城行(X) 🔳 🗸 📅 🗐 🔒 🚆
物件總管 ▼ ♀×	
連線▼ 単 *単 ■ ▼ 🖒	
🖃 🐻 localhost (SQL Server 15.0.2000.5 - sa)	
	連接(C)
	中斷連接(D)
🛃 🔲 伺服器物件	註冊(G)
⊞ 💻 復命 雨 📕 PolyBase	
→ I Always On 高可用性	
	活動監視器(M)
🗄 📕 Integration Services 目錄	啟動(S)
🗄 🛃 SQL Server Agent	停止(T)
	暫停(U)
	繼續(E)
	重新啟動(A)
	原則(O) ▶
	Facet(A)
	 啟動 PowerShell(H)
	Azure Data Studio(A)
	+0x+0x(F)
	重新整理(F)
	屬性(R)
_	



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

■ 伺服器屬性 - WIN2019		_		\times
選取頁面	🖵 指令碼 🔻 😮 說明			
 一般 記憶體 点理器 安全性 逆線 資料庫設定 進階 離限 	 伺服器驗證 ○ Windows 驗證模式 (W) ● SQL Server 及 Windows 驗證模式 (S) 登入稽核 ○ 無(N) ○ 僅限失敗的登入(F) ○ 僅限成功的登入(D) ● 失敗和成功的登入(B) (伺服器 Prove 無戶 			
連線	□ 取用伺服器 Proxy 帳戶(V)			
伺服器: localhost 連接: sa yず <u>檢視連接屬性</u>	Proxy 帳戶(R): 密碼(P): 選項 □ 歇用通用條件合規性(O) □ 歇用 C2 稽核追蹤(E)			
	— 跨資料庫擁有權鏈結(C)			
進度				
就緒				
		確定	取	消



(5) 重新啟動 MS SQL SERVER 服務

在 [伺服器名稱] 按滑鼠右鍵 -> 點選 [重新啟動]



(6) 按 [是] 重新啟動 MSSQLSERVER 服務

Microso	Microsoft SQL Server Management Studio				
?	您確定要重新啟動 ₩I№ 2019 上的 MSSQLSER VER 服務嗎?				
∎ <mark>⊇</mark> 複集	製訊息	是(Y) 否(N)			



(7) 按 [是] 停止 SQL SERVER Agent 服務

Microso	ft SQL Server Management Studio		
?	停止此服務也會停止 SQL Server Agent (MSSQLSER VER)。要繼續嗎?		
₽ <u></u> 」複	製訊息	是(Y)	否(N)



5.1.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式



<2.2> 使用 Windows 帳號



(3) 切換資料庫





(4) 使用 sp_configure 列出進階選項

1 > exec sp_configure 'show advanced options', 1			
2 > go			
1 > reconfigure			
2 > go			
≥ 系統管理員: Windows PowerShell - SQLCMD	_		×
1> exec sp_configure 'show advanced options', 1			^
27 go 組態邏項_'show advanced options' 從 0 變更為 1。請執行 RECONFIGURE	陳述式來	を安装。	
1> reconfigure 2> go			
1> _			~

(5) 啟用失敗和成功的登入記錄

1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\I	MSSQ	LServ	'er',
N'AuditLevel', REG_DWORD, 3			
2 > go			
1 > quit			
▶ 系統管理員: Windows PowerShell	_		×
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', 2> go	REG_DWO	ORD, 3	^
(0 個受影響的資料列)			
PS C:\Users\Administrator> _			v

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

PS C:\> Restart-Service -Name MSSQLSERVER -Force						
PS C:\> Ge	et-Service -Name MSSC	LSERVER,SQLSERVERAGENT				
🚬 系統管	理員: Windows PowerShe	- II		×		
PS C:∖Wi PS C:∖Wi	ndows\system32> <mark>R</mark> ndows\system32> <mark>G</mark>	start-Service -Name MSSQLSERVER -Force t-Service -Name MSSQLSERVER,SQLSERVER	GENT	^		
Status 	Name	DisplayName 				
Running Running	MSSQLSERUER SQLSERVERAGENT	SQL Server (MSSQLSERVER) SQL Server Agent (MSSQLSERVER)				
PS C:∖Wi	ndows\system32> _			.		



5.2 設定稽核

5.2.1 稽核伺服器層級

啟用稽核伺服器層級包含伺服器作業,例如管理變更及登入和登出作業。

以下分別為圖形介面和指令介面設定方式。

5.2.1.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

🚽 連線至伺服器		×
	SQL Server	
伺服器類型(T):	資料庫引擎	~
伺服器名稱(S):	localhost	~
驗證(A):	SQL Server 驗證	~
登入(L):	sa	~
密碼(P):		
	☑ 記住密碼(M)	
	連線(C) 取消 說明	選項(O) >>



🛃 Microsoft S	快速啟動 (Ctrl+Q)	₽ = □ ×
檔案(F) 編輯(E)	檢視(V) 專案(P) 工具(T)	視窗(W) 說明(H)
0.0 13.	* 🍾 🖕 🔛 📕 📑 新増査部	NN
× T Y	· P #411	
物件總管	▼ ∓ ×	
連線 ▼ 岸 🎽 🔳	▼ C -*	
😑 🔀 localhost (S	QL Server 15.0.2000.5 - sa)	
🗉 💼 資料庫		
🖂 🗐 安全性		
🗉 🗐 登入		
🕀 💻 伺服	器角色	
🛛 🖃 認證		
🛛 🗐 密碼	編譯提供者	
🕀 💼 稽核		
🕀 💼 伺服	新増稽核(N)	
🗉 💼 伺服器物		
🗉 📕 複寫	即進(1)	
🕀 🛄 PolyBas	啟動 PowerShell(H)	
Always		
I ■ 管理		
	重新整理(F)	
⊕ <u>e</u> r ∧event	77771工具	
L		

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



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

核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

💦 建立稽核			_		×
🕕 就緒					
<mark>選取頁面</mark> ✓ <u>般</u> ✓ 新選	 損令碼 ▼ ? 説 群核名稱(N):	 INP_Audit 1000 ● 維續(C) ● 令操作失敗(F) ● 關閉伺服器(S) 應用程式記錄檔 ● 最大換用檔案(O): ● 最大檔案數目(X): 檔案數目(B): 2147483647 			
	檔案大小上限 (乙): □ 保留磁碟空間	0 ◆ M ● M ⑤ 無限制(L) ⑤(R)	ИВ(М) 🔾 GB(С	й) () Т	`B(T)
建設					
被視連線屬性 進度 就緒					
		· · · · · · · · · · · · · · · · · · ·			
		確定	取消	說印	A



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

🔀 Microsoft S 快速啟動) (Ctrl+Q)
檔案(F) 編輯(E) 檢視(V)	專案(P) 工具(T) 視窗(W) 說明(H)
G - O 📅 - 🛅 - 當	🔛 📲 🏮 新増査詢(N) 🟮 🔬 🔬 🏛
	- ▶ 執行(X) ■ ✓ 閉 回 💾
4- 14- 1/2 M	
初行総官	• • • ×
連線▼ 〒 ^〒 ■ Y ℃ →	►
🖃 🐻 localhost (SQL Server	15.0.2000.5 - sa)
🛛 🔲 並べ	
. 🗐 認證	
🗈 🛑 密碼編譯提供者	
	±122 ≤= 1÷ (a.).
	新瑁植核(N)
	啟用稽核(E)
🕀 🛑 PolyBase	檢視稽核記錄(V)
🗉 📕 Always On 高可月	編寫稽核的指令碼為(S) ▶
🗄 💼 管理	
Integration Servi	Epoct(A)
E E ALVent ////⊥₽	啟動 PowerShell(H)
	報表(P) ▶
	重新命名(M)
	刪除(D)
	局性 (R)
L	



(6) 按 [關閉]

₽ 啟用稽核				_		×
🐼 威功	1 1	總計 成功		0 0	錯誤 警告	
詳細資料(D):						
動作			狀態		訊息	
			成功			
					69	閉(C)

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



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

建立伺服器稽核規格							- 0]
就緒								
x頁面	♫ 指令碼	- 😮 說明						
一般								
	名稱(N)): NP_Serve	r_Audit					
	稽核(A)): NP_Audi	:					
	動作:							
		稽核動作類型		物件類別	物件結構描述	物件名稱	主體名稱	
	01	SUCCESSFUL_LOGIN_GROUP	~	~				
	02	FAILED_LOGIN_GROUP	~	~				
	03	LOGOUT_GROUP	~	~				
	04	SERVER_STATE_CHANGE_GROUP	~	~				
	05	SERVER_OPERATION_GROUP	~	~				
	06	SCHEMA_OBJECT_CHANGE_GROUP	~	~				
ġ.	07	DATABASE_OWNERSHIP_CHANGE_G	ROUP 🗸	~				
SQL2019 [sa]	08	DATABASE_CHANGE_GROUP	~	~				
	09	AUDIT_CHANGE_GROUP	~	~				
	10	USER_CHANGE_PASSWORD_GROUP	~	~				
視連線屬性	11	SCHEMA_OBJECT_CHANGE_GROUP	~	~				
£	12	DATABASE_OBJECT_CHANGE_GROU	• v	~				
入 完成	▶ *13		~	~				



- 🔀 Microsoft SQL Serve 快速啟	動 (Ctrl+Q)
檔案(F) 編輯(E) 檢視(V) 專案	(P) 工具(T) 視窗(W) 說明(H)
80-0 😚 - 5 🖕 🗎 🖥	
8 T Y	
物件總管	▼ ₽ ×
連線 - 単 ×単 = ▼	
Relocalbost (SQL Server 15.0.2)	000 5 - sa)
🗉 💼 伺服器角色	
🗉 🛑 密碼編譯提供者	
	新世白肥器遊校坦応(N)
⊕ 💼 PolyBase	取用何服薪档核规倍(E)
■ I Always On 高可用性	編寫伺服器稽核規格的指令碼為(S) ▶
	 原則(O)
🗉 📒 Integration Services 目覚	Eacet(A)
E SQL Server Agent	
⊞ <u>1</u> XEvent 分析工具	愈動 PowerShell(H)
	報表(P) ▶
	刪除(D)
	重新整理(F)
	屬性(R)

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



(10) 按 [關閉]

🧖 啟用伺服器稽核規格			_		×
🕢 成功	1 總計 1 成功		0 0	錯誤 警告	
詳細資料(D):					
動作		狀態		訊息	
🥝 啟用伺服器稽核規格	'NP_Serv	成功			
				ߨ	閉(C)



5.2.1.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號



(3) 切換資料庫





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

×

۸

¥

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

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

紅色文字部位請輸入稽核名稱



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

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



紅色文字部位請輸入伺服器稽核規格名稱

5.2.2 稽核資料庫層級

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

以下分別為圖形介面和指令介面設定方式。

5.2.2.1 使用圖形介面方式設定

(1) 開啟 [Microsoft SQL Server Management Studio]



(2) 輸入伺服器名稱 -> 選擇登入驗證方式 -> 按 [連線]

🚽 連線至伺服器	×
	SQL Server
伺服器類型(T):	資料庫引擎 ~
伺服器名稱(S):	localhost ~
驗證(A):	SQL Server 驗證 ~
登入(L):	sa 🗸 🗸
密碼(P):	******
	☑ 記住密碼(M)
	連線(C) 取消 說明 選項(O) >>



(-) , , , , , , , , , , , , , , , , , , ,		
🔀 Microsoft S	快速啟動 (Ctrl+Q)	₽ = ¤ ×
檔案(F) 編輯(E)	檢視(V) 專案(P) 工具(T)	視窗(W) 說明(H)
0-0 M-	**** - *** 🕒 遇 新婚査部	
	▼ ▶ 報(1)	
物件總管	▼ ₽ ×	
連線 ▼ 🕴 🎽 🔳	▼ Ċ -*	
🖃 🔂 localhost (S	QL Server 15.0.2000.5 - sa)	
🗉 📄 資料庫		
□ 🗐 安全性		
🗉 🗐 登入		
🗄 🗐 🖬	器角色	
🗉 📃 認證		
😠 💼 密碼	编譯提供者	
🕀 💼 稽核		
🗉 💼 伺服	新増稽核(N)	
🕀 🛑 伺服器核		
🕀 🛑 複寫	師選(!) ▶	
🕀 🛑 PolyBas	啟動 PowerShell(H)	
🕀 📕 Always 🕯	把主(D)	
	≠K衣(P) ►	
	重新整理(F)	
	1.+C.7.8	
Γ		

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



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

核記錄儲存於 Windows 事件檢視器的應用程式記錄 -> 按 [確定]

💦 建立稽核			_	
🕕 就緒				
● ⁹⁴¹³⁸ 選取頁面 御選	① 指令碼 ▼	 Ⅰ NP_Audit 1000 ● 繼續(C) ● 令操作失敗(F) ● 闡閉伺服器(S) 應用程式記錄檔 		
	路徑(P): 稽核檔案數目 上限: 檔案大小上限 (Z): 保留磁碟空間	 最大換用檔案(O): 無限制(U) 最大檔案數目(X): 檔案數目(B): 2147483647 ① ② ④ ④ ④ ③ (B):) MB(M) () GB(G)	 •
連線 y荦 localhost [sa]				
<u>檢視連線屬性</u>				
理 度 就緒				
		確定	取消	說明



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

Wicrosoft S 快速節 構築(F) 編輯(E) 檢視(V, G・G) 約・泊・C ・ ・ ・ ・ ・ ・ ・ ・	 (b) (Ctrl+Q) (c) 專案(P) 工具(T) 視窗(W) 説明(H) (c) 副 (A) (A) (A) (A) (A) (A) (A) (A) (A) (A)
物件總管 連線 ▼ ♥ ×♥ ■ ▼ ♥ ■ 資料庫 ■ 資料庫 ■ 安全性 ■ 愛入 ● ● 日服器角色 ● ● 日服器 ● ● 日服 ● ● 日服 ● ● 日服 ● ● 日 ● ● 日 ● ● ● 日 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	 ↓ ↓ Image: A + 15.0.2000.5 - sa) a 新增稽核(N) 取用稽核(E) 検視稽核記錄(V) 編高稽核的指令碼為(S) ↓ 原則(O) ↓ Facet(A) 原則(O) ↓ Facet(A) 取動 PowerShell(H) 報表(P) ↓ 重新命名(M) 刪除(D) 重新整理(F) 屬性(R)
Ĺ	4



(6) 按 [關閉]

₽ 啟用稽核				_		×
🐼 威功	1	總計 成功		0 0	錯誤 警告	
詳細資料(D):						
動作			狀態		訊息	
🥝 啟用稽核 'NP_Audit'			成功			
					ߨ	閉(C)


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

料庫稽核規格...]





(8) 輸入資料庫稽核規格名稱: NP_DB-NCloud_Audit -> 選擇稽核名稱: [NP_Audit] 和動作 詳細說明請參考前言的稽

<u>核動作群組連結</u> -> 按 [確定]

💦 建立資料庫稽核規格								- 0	×
 就緒 									
選取頁面 チ 一般	♫ 指令碼	▼ (2) 說明							
	名稱(N): NP_DB-NCloud_Audit								
	稽核(A)): NP_Audit							~
		稽核動作類型		物件類別	物件結構描述	物件名稱		主體名稱	
	01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	~	~					
	02	SCHEMA_OBJECT_CHANGE_GROUP	~	~					
	03	DATABASE_OWNERSHIP_CHANGE_GROUP	~	~					
	04 DATABASE_CHANGE_GROUP		~	~					
連線	05	AUDIT_CHANGE_GROUP	~	~					
q ₩ SQL2019 [∞]	06	USER_CHANGE_PASSWORD_GROUP	~	~					
	07	SCHEMA_OBJECT_CHANGE_GROUP	~	~					
	08	FAILED_DATABASE_AUTHENTICATION_GROUP	~	~					
<u> 檢視連線 </u>	09	DATABASE_OBJECT_CHANGE_GROUP	~	~					
建度 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	10	DATABASE_ROLE_MEMBER_CHANGE_GROUP	~	~					
	▶ *1 1		~	~					
						確定	取消	ŧ	胡





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



(10) 按 [關閉]

Q ▶ 啟用資料庫稽核規格			_		×		
🐼 成功	1 總計 1 成功		0 0	錯誤 警告			
詳細資料(D):							
動作		狀態		訊息			
② 啟用資料庫稽核規格	NP_DB	成功					
				60	閉(C)		



5.2.2.2 使用指令介面方式設定

(1) 開啟 [Windows PowerShell]



(2) 分別為 sa 或 Windows 帳號登入方式

<2.1> 使用 sa 帳號



<2.2> 使用 Windows 帳號



(3) 切換資料庫





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

1 > CREATE SERVER AUDIT [NP_Audit] 2 > TO APPLICATION_LOG 3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE) 4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON) 5 > GO 反 条统管理号: Windows PowerShell - SOLCMD — □ ×

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

紅色文字部位請輸入稽核名稱

(5) 切換到稽核資料庫,範例:NCloud

1 > use <mark>NCloud</mark> 2 > go		
≥ 系統管理員: Windows PowerShell - SQLCMD	_	×
1〉use NCloud 2〉go 已將資料庫內容變更為'NCloud'。 1〉_		^ ~
紅色文字部位請輸入稽核資料庫名稱		

۸

¥



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

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

1 > quit



紅色文字部位請輸入資料庫稽核規格名稱

1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]

紅色文字部位請輸入稽核資料庫名稱

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



5.3 事件記錄檔設定

此為選項設定。

以下分別為網域和工作群組設定方式。

5.3.1 網域

5.3.1.1 組織單位設定

(1) 開啟 AD 使用者和電腦

開啟 [Active Directory 使用者和電腦]





(2) 新增組織單位

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

🞴 Active Directory 使用者	首和電腦	– 🗆 X					
檔案(F) 動作(A) 檢視(\	檔案(F) 動作(A) 檢視(V) 說明(H)						
← → □□ 2 □□ 2 ≥ 1 □ 2 ≥ 1 □ 2 ≥ 2							
 Active Directory 使用者 G 儲存查詢 G 儲存查詢 G Builtin G Domain Cor G ForeignSect Managed S G Users 	 和電腦 名稱 類型 第 n-partner.lo 網域 委派控制(E) 尋找(I) 變更網域(D) 變更網域控制站(C) 提高網域功能等級(A) 	描述 存放最常用查詢的資料夾					
	操作主機(M)						
	新増(N) >	電腦					
	所有工作(K) >	連絡人					
	重新整理(F)	群組					
	市恋(D)	InetOrgPerson					
	NH(N)	msDS-ShadowPrincipalContainer					
	說明(H)	msImaging-PSPs					
		MSMQ 佇列別名					
		組織單位					
		印表機					
		使用者					
		共用資料夾					
<	>						
建立一個新物件							



(3) 輸入組織單位名稱

新増物件 - 組織單位	\times
建立在: n-partner.local/	
名稱(A):	
Servers	
☑ 保護容器以防止被意外刪除(P)	
確定 取消 說明	

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



(4) 移動伺服器至新的組織單位

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

-> 點選 [移動]





(5) 選擇組織單位

選擇 [Servers] 組織單位 -> 按 [確定]

移動	\times
將物件移動到容器(<u>M</u>):	
 n-partner Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Servers Users 	
確定 取消	

(6) 確認伺服器已移動至新的組織單位

點選 [Servers] 組織單位,確認 SQL2019 伺服器已移動。





5.3.1.2 群組原則設定

- (1) 開啟群組原則管理
- 開啟 [群組原則管理]



(2) 在 Servers 組織單位,新增群組原則物件

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





(3) 輸入群組原則物件名稱

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

新増 GPO	×	
名稱(N):		
N-Partner Policy		
來源入門 GPO(S):		
(無)	~	
	確定取消	

(4) 編輯群組原則物件

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

🔜 群組原則管理	_								
🔜 檔案(F) 動作(A) 檢視(V) 視窗(V	/) 說明(H)	_ & ×							
🗢 🔿 📶 📋 🖾 🧟 🛛									
■ 群組原則管理	n-partner.local								
✓ ▲ 樹系: n-partner.local	狀態 已連結的群組原則物(牛 群組原 ◀ ▶							
 ● 調理場 ● 二 n-partner.local ② Default Domain Polic > ② Domain Controllers > ③ Servers 	此頁面顯示此網域之 Active SYSVOL 複寫的狀態,因為 有關。	Directory 和 2與群組原則							
N-Partner Policy									
	編輯(E)	1 <u>婆更</u>							
> 💼 入門 GPO	空司(N)								
> 📫 網站	▲ 成用理描(L)	資訊存							
122 群組原則模型	1館1子和百(5)	_							
	從這裡開啟新視窗(W)	,從此網 ま礎結構							
	刪除(D)	2 32 74 11 7							
	重新命名(M)								
	重新整理(F)								
	說明(H)								
< >>									
開啟 GPO 編輯器									



(5) 本機原則:稽核原則

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





(6) 事件記錄檔:應用程式記錄保持方法

展開 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [事件記錄檔] -> 點選 [應用程式記錄保持方法] 項目

-> 勾選 [定義這個原則設定]: -> 點選 [視需要覆寫事件] -> 按 [確定]



(7) 事件記錄檔:應用程式記錄檔大小最大值

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

項目 -> 勾選 [定義這個原則設定]: -> 輸入 204800 KB 註:請依客戶環境調整 -> 按 [確定]





(8) 開啟 [Windows PowerShell]



(9) 更新 MS SQL Server 群組原則

PS C:> Invoke-GPUpdate -Computer SQL2019 -RandomDelayInMinutes 0 -Force			
≥ 条統管理員: Windows PowerShell	_		×
PS C:\> Invoke-GPUpdate -Computer SQL2019 -RandomDelayInMinutes PS C:\> _	Ø	-Force	0
紅色文字部位請輸入 MS SQL Server 伺服器名稱			

(10) 產生 MS SQL Server 伺服器群組原則報表

PS C:\> Get-GPR	esultantSetofPolicy -Computer SQL2019 -Path C:\tmp\SQL2019.html -Re	portType html	
🗾 系統管理員: Wind	ows PowerShell	– [- X
PS C:\> Get-GPRe	sultantSetofPolicy -Computer SQL2019 -Path C:\tmp\SQL2019.html -R	eportType htm]	^
RsopMode Namespace LoggingComputer LoggingUser LoggingMode	: Logging : \\SQL2019\Root\Rsop\NSFDC71005_559D_49FD_ADC8_05538D651A04 : SQL2019 : N-PARTNER\administrator : Computer		
PS C:\> _			v

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



		-	X
(=) (=) (=) C:\tmp\SQL2019.html	▼ ♂ 搜尋.	,0 ,	슈 ☆ 🙂
Ø N-PARTNER\SQL2019 × □ [*]			
	群組原則結果		
N-PARTNER\SQL2019			
資料收集: 2021/10/22 下午 04:02:35			全部顯示
摘要			ᄪᆕ
電腦詳細資料			<u>HR/IN</u>
元件狀態			
			隱藏
MCC1			隱藏
Windows 設定			冯 藏
安全性設定			四藏
帳戶原則/密碼規則			##
帳戶原則/帳戶鎖定原則			#8/1
本機原則/着核原則			顯示
E Pul	-10 - 1 1	(F# opo	[]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]
		世界 GPO	
相核限户意入事件	成功,失敗	N-Partner Policy	
作权限户管理 经按照) 由件	成功,大规	N-Partner Policy	
	MM 70 , XM	N-Partner Policy	
半碳原剂/女主II进程			顯示
爭件記錄福			傿藏
原則	設定	優勢 GPO	
應用程式記錄保持方法	視需要而定	N-Partner Policy	
應用程式記錄檔容量最大值	204800 KB	N-Partner Policy	
公開金鑰原則/憑證服務用戶端 - 自動註冊設定			82-
公開金鑰原則/加密檔案系統			
群組原則物件			翻示
WMI 能結果器			顧示
			顧示
使用者詳細資料			顧示
L			

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



5.3.2 工作群組

5.3.2.1 稽核原則設定

(1) 開啟本機群組原則編輯器

點選 🔎 [搜尋] -> 輸入群組原則 -> 點選 [編輯群組原則]

≡		篩選條件 🏏
ŵ	最佳比對	
	編輯群組原則 控制台	
ŝ		
	▶ 群組原則	
	ト P 目	



(2) 本機原則:稽核原則

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

戶管理], [稽核登入事件] 項目 -> 勾選 稽核這些嘗試: [成功] & [失敗] -> 按 [確定]





(3) 開啟 [Windows PowerShell]



(4) 更新群組原則





(5) 查看群組原則套用情形

PS C: \> auditpol /get /category:* ➢ 系統管理員: Windows PowerShell PS C:\> <mark>auditpol</mark> /get /category:* System audit policy Category/Subcategory Setting 系統 安 航 安全性象統延伸 象統完整性 IPSEC driver 其他象統事件 安全性狀態變更 人登出 No Auditing Success and Failure No Auditing Success and Failure Success 入之。 登入 登出 限戶鑽定 IPsec 主要模式 IPsec 快速模式 IPsec 延伸模式 登 Success and Failure IPsec 延伸模式 特殊登入 其他登入/登出事件 網路原則伺服器 使用者/装置宣告 詳組成員資格 物件存取 檔案系統 registry 核心物件 SAM 屬證照務 Success and Failure Success and Failure Success and Failure No Auditing Success Success No Auditing No Auditing No Auditing No Auditing Success and Failure Success No Auditing No Auditing No Auditing Success and Failure Success and Failure Success and Failure Success and Failure



×

~

5.3.2.2 事件檔案設定

(1) 開啟 [檢視事件記錄檔]

點選 🔎 [搜尋]-> 輸入事件記錄 -> 點選 [檢視事件記錄檔]

		ß	ŝ				篩選條件 ∨
ŵ	最佳比	對					
		檢視事 控制台	件記錄檔				
ŝ							
	₽∎	件記錄					
	ρ	Ξi	ê				



(2) 編輯安全性記錄

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





(4) 設定應用程式記錄檔

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

記錄內容 - 應用程式 (類型: 系統管理)							
一般訂閱							
全名(F):	Application						
記錄檔路徑(L):	%SystemRoot%\System32\Winevt\Logs\Application.evtx						
記錄檔大小:	1.07 MB(1,118,208 位元組)	_					
建立日期:	2021年6月9日 下午 08:56:09						
修改日期:	2021年7月5日 下午 05:13:07						
存取日期:	2021年7月5日 下午 05:13:07						
 ✓ 啟用記錄(E) 最大記錄檔大小 (KB)(X): 204800 當事件記錄檔的大小到達上限時: ④ 視需要覆寫事件 (先覆寫最舊的事件)(W) ○ 當記錄檔已滿時進行封存,不要覆寫事件(A) ○ 不要覆寫事件 (手動清除記錄檔)(N) 							
	清除記錄(R) 確定 取消 套用(P)]					



6. N-Reporter			
(1) 新增 MS SQL 設備			
[設備管理] -> [設備樹狀圖]-> 點選		
N-Reporter	_		
Admin (Global) ~		❸ Home / 設備管理 / 設備樹狀圖	
■ 事件	æ	▲ 設備樹狀圖	
▲	œ	搜尋	Q 2 🗉 U 📣
♀ 智慧分析	æ	🛃 Global (0/0)	
■ 設備管理	Θ	〒 未知設備 (0/0)	
──────────────────────────────────────			
- ■ 介面列表			
- 回告警様版			
- ▲設備異常告警			
- □設備設定檔備份			
● 系統管理	æ		
使用者手冊			
	G		



6.1 MS SQL Server Log

(2) 設定 MS SQL Event log 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [MS SQL] 和 Facility: [(18) local use 2 (local2)] -> 選擇

設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按 [確定]

瞐 新増設備		×
設備基本設定		•
名稱		ור
M55QL-192.168.8.183		
IP		
192.168.8.183		
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	~	
本設備於分時監控報表啟動Syslog轉發時,採用 Raw Data		
設備進階設定		
ICMP 告警樣版		
N/A	~	
設備 Icon		
icon-host	~	
Login Account		
Login Password		
Enable Password		
接收狀態 ● 啟用		
暫無資料告警		
■ 愈用 Syslog 暫無資料告警		
		•
	確定	取消



6.2 Windows Event Log

(2) 設定 Windows Event log 設備的資料格式

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

所増設備	
設備基本設定	
名稱	ור
Windows-192.168.8.183	
	-
192.108.8.183	
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	1
UTF-8 🗸	
設備進階設定	
ICMP 告警樣版	
N/A	
設備 Icon	
icon-host 🗸	
Login Account	1
Login Password	
Enable Password	
接收狀態 ③ 啟用	
暫無資料告警	
▶ 啟用 Syslog 暫無資料告督	
確定	取消



