Chapter

12

稽核、加密與自主資料庫

- 資料庫稽核
- 資料加密
- 自主資料庫

碁峰
www.gotop.com.tw

12-1 資料庫稽核

資料庫稽核（Database Audit）是一種資料庫安全機制，如同替資料庫安裝了一套監視系統，可以將資料庫各種存取行為都一一錄影記錄下來，當出問題時，就可以事後追蹤到底是誰作了這件事。

12-1-1 SQL Server Audit 的基礎

資料庫稽核是一個涉及多種監控觀點的資料庫安全性管理，可以記錄誰登入伺服器、誰登出伺服器、誰存取哪些資料庫物件等行為，將所有資料庫的存取行為都完整記錄下來。

一般來說，資料庫稽核工作很少是由資料庫管理師來親自執行，通常都是使用一套程式執行資料庫稽核，其主要目的是防止使用者偷竊資料庫的重要資料，因為我們可以透過稽核記錄來識別指定的使用者，記錄他執行哪些資料庫存取操作和檢查資料庫的變更，以便找出是誰存取了重要資料。

事實上，資料庫管理師只需開啟資料庫系統的稽核功能，就可以開始收集相關的資料庫存取操作，當發生資料外洩時，企業或組織可以透過稽核記錄，追查到是誰將資料洩漏出去。

SQL Server Audit

SQL Server 在 2008 版提供 SQL Server Audit 資料庫稽核功能，它是用來取代舊版 SQL Trace 的稽核功能，可以提供全方位的稽核能力，因為 SQL Trace 的功能不只有稽核，更提供效能追蹤，但是，SQL Server Audit 的唯一功能就是建立資料庫稽核。

基本上，SQL Server Audit 是架構在全新的事件引擎（Eventing Engine），稱為 Extended Events。Extended Events 是一個輕量級的事件引擎，所以不會影響資料庫引擎的執行效能，它可以允許我們定義需要捕抓動作的事件，當定義的事件觸發時，就可以將詳細資訊送至目標的作業系統檔案或事件記錄檔。

碁峰 www.gotop.com.tw

SQL Server 2012 企業版（評估版）支援完整功能的 SQL Server Audit，其他版本只提供基本稽核功能，和限制只能建立伺服器層級稽核規格。

SQL Server Audit 的三種物件

請注意！SQL Server Audit 是 SQL Server 提供資料庫稽核功能的名稱，Audit 是一個資料庫物件，SQL Server Audit 是使用三種物件來描述我們建立的資料庫稽核，其說明如下所示：

- 稽核（Audit）：定義整個稽核過程的稽核資料是送至哪裡儲存，其目的地可以是檔案、應用程式記錄檔或安全性記錄檔，稽核物件是一種執行個體層級的物件，每一個執行個體可以建立多個稽核物件。請注意！稽核物件本身並沒有任何稽核動作的資訊，它只是一個容器物件，可以用來儲存稽核規格定義的稽核動作。
- 伺服器層級稽核規格（Server Audit Specifications）：定義伺服器層級的稽核動作（Audit Actions），屬於指定的稽核物件，以便可以將稽核記錄送至定義的目的地，為了避免在稽核規格設定大量的稽核動作，SQL Server Audit 提供預先定義的稽核動作類型（Audit Groups）來定義稽核規格，每一個稽核動作類型包含相關的多種稽核動作。
- 資料庫層級稽核規格（Database Audit Specifications）：定義資料庫層級的稽核動作，它也是使用稽核動作類型來定義稽核規格。

SQL Server 建立資料庫稽核的基本步驟

基本上，在 SQL Server 建立資料庫稽核可以分成四個步驟，如下所示：

- Step 1：建立稽核物件和定義送至的目的地。
- Step 2：針對稽核物件建立稽核規格。
- Step 3：啟用稽核物件和稽核規格。
- Step 4：檢視稽核記錄。

12-1-2 建立稽核

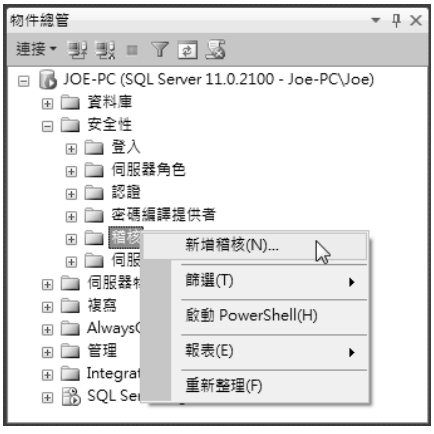
SQL Server 可以使用 Management Studio 或 T-SQL 指令來建立稽核物件。

碁峰 www.gotop.com.tw

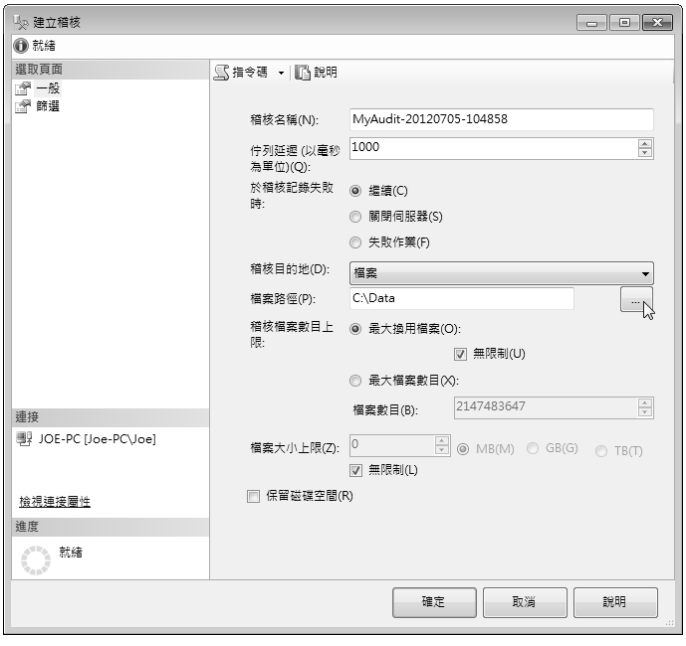
使用 Management Studio 建立稽核

Management Studio 提供圖形介面建立稽核物件。例如：建立目的地是檔案的稽核物件，其步驟如下所示：

step 1 請啟動 Management Studio 且建立連接後，在「物件總管」視窗展開伺服器下的【安全性】項目，如右圖所示：



step 2 在【稽核】上，執行【右】鍵快顯功能表的【新增稽核】指令，可以看到「建立稽核」對話方塊。



碁峰 www.gotop.com.tw

上述對話方塊的主要欄位說明，如下所示：

- 稽核名稱：預設的稽核名稱格式是 Audit 加上日期/時間。
- 佇列延遲：稽核記錄寫入目的地的延遲時間，單位是毫秒，0 就是馬上寫入。
- 於稽核記錄失敗時：如果無法成功寫入稽核記錄時的處理方式，預設值【繼續】是 SQL Server 不會保留稽核記錄，作業繼續進行；【關閉伺服器】是強制關閉伺服器，此時的登入需要擁有 SHUTDOWN 權限；【失敗作業】是當稽核記錄失敗時，執行的交易也會失敗，沒有稽核的交易則繼續執行。
- 稽核目的地：指定稽核資料送至的目的地，可以是檔案、安全性記錄檔和應用程式記錄檔。

step 3 將名稱改為【MyAudit-yyyyMMdd-hhmmss】格式後，在【稽核目的地】欄位選【檔案】，按【檔案路徑】欄位後的按鈕，選擇檔案儲存的路徑，以此例是「C:\Data」，按【確定】鈕建立稽核物件。

在 Management Studio 的「物件總管」視窗可以看到新建立的稽核物件，如下圖所示：

使用 T-SQL 指令建立稽核

T-SQL 提供 CREATE SERVER AUDIT 指令來建立稽核，其基本語法如下：

```
CREATE SERVER AUDIT audit_name
TO { [ FILE file_options ] | APPLICATION_LOG | SECURITY_LOG }
[ WITH audit_options ]
```


碁峰 www.gotop.com.tw

上述語法可以建立名為 audit_name 的稽核，TO 子句指定稽核目的地是檔案 FILE、應用程式記錄檔 APPLICATION_LOG 或安全性記錄檔 SECURITY_LOG。

file_options 是使用「( )」符號括起，以「,」號分隔的 FILEPATH、MAXSIZE、MAX_ROLLOVER_FILES、RESERVE_DISK_SPACE 和 MAX_FILES 屬性，依序可以指定稽核記錄檔的路徑、檔案尺寸的最大值、保留在檔案系統中的檔案數目上限、是否在磁碟上預先配置 MAXSIZE 值的檔案（ON 是配置；OFF 是不配置）和最大的稽核檔案數。

audit_options 使用「( )」符號括起，以「,」號分隔的 QUEUE_DELAY 和 ON_FAILURE 等稽核屬性，即前述的佇列延遲和於稽核記錄失敗時欄位，ON_FAILURE 屬性值可以是 CONTINUE、SHUTDOWN 和 FAIL_OPERATION。

SQL 指令碼檔：Ch12-1-2-01.sql

請建立名為 MyServerAudit 的稽核物件，其目的地是「C:\Data\Audit\」路徑，ON_FAILURE 稽核屬性值為 CONTINUE，如下所示：

```
CREATE SERVER AUDIT MyServerAudit
TO FILE
(  FILEPATH = 'C:\Data\Audit\',
   MAXSIZE = 5MB,
   MAX_ROLLOVER_FILES = 100
)
WITH ( QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE )
```

12-1-3 建立伺服器層級稽核規格

在建立稽核物件後，我們就可以在此稽核物件新增稽核規格，首先是伺服器層級稽核規格。SQL Server 可以使用 Management Studio 或 T-SQL 指令來建立伺服器層級稽核規格。

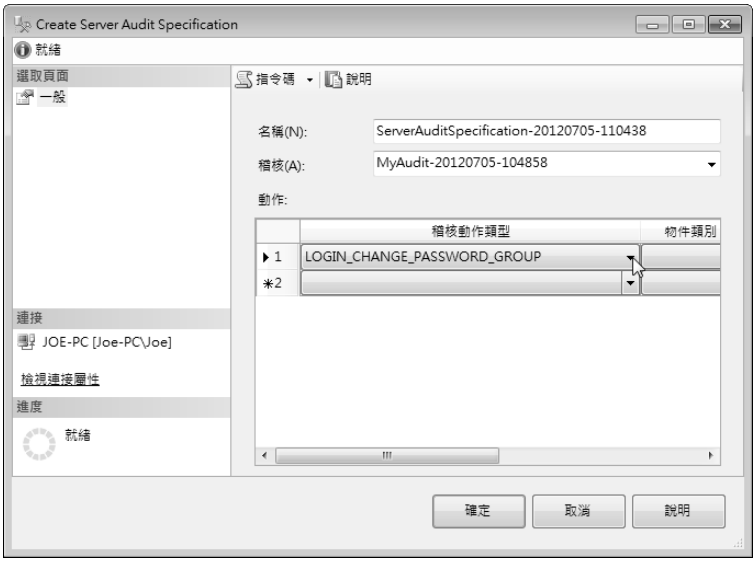
碁峰 www.gotop.com.tw

使用 Management Studio 建立伺服器層級稽核規格

Management Studio 提供圖形介面建立稽核規格物件。例如：建立稽核動作類型為 LOGIN_CHANGE_PASSWORD_GROUP 的稽核規格物件，可以稽核更改登入密碼的事件，其步驟如下所示：

step 1 請啟動 Management Studio 且建立連接後，在「物件總管」視窗展開伺服器下的【安全性】項目，如右圖所示：

step 2 在【伺服器稽核規格】上，執行【右】鍵快顯功能表的【新增伺服器稽核規格】指令，可以看到「Create Server Audit Specification」對話方塊。



碁峰 www.gotop.com.tw

step 3 在【名稱】欄輸入伺服器稽核規格名稱，以此例是使用預設名稱，【稽核】欄選擇第 12-1-2 節建立的稽核物件【MyAudit-yyyyMMdd-hhmmss】後，就可以在下方選擇稽核動作，請選稽核動作類型【LOGIN_CHANGE_PASSWORD_GROUP】，如果需要，可以同時選擇多個，按【確定】鈕建立伺服器層級稽核規格。

在 Management Studio 的「物件總管」視窗可以看到新建立的伺服器層級稽核規格物件，如右圖所示：

使用 T-SQL 指令建立伺服器層級稽核規格

T-SQL 提供 CREATE SERVER AUDIT SPECIFICATION 指令來建立伺服器層級稽核規格，其基本語法如下所示：

```
CREATE SERVER AUDIT SPECIFICATION audit_spec_name
FOR SERVER AUDIT audit_name
ADD ( audit_action_group_name ) [, ...n]
[ WITH ( STATE = ON | OFF ) ]
```

上述語法可以建立名為 audit_spec_name 的伺服器層級稽核規格，FOR SERVER AUDIT 子句指定所屬的稽核物件。ADD 子句可以新增稽核動作類型，如果不只一個請重複使用 ADD 子句來新增，並且使用「,」號分隔。

WITH 子句可有可無，STATE 屬性值 ON 表示啟用；OFF 是停用伺服器層級稽核規格。

碁峰 www.gotop.com.tw

SQL 指令碼檔：Ch12-1-3-01.sql

請建立名為 MyServerAuditSpec 的伺服器層級稽核規格，屬於 MyServerAudit 稽核，並且新增稽核動作類型 FAILED_LOGIN_GROUP 來稽核登入失敗，如下：

```
CREATE SERVER AUDIT SPECIFICATION MyServerAuditSpec
FOR SERVER AUDIT MyServerAudit
ADD (FAILED_LOGIN_GROUP)
```

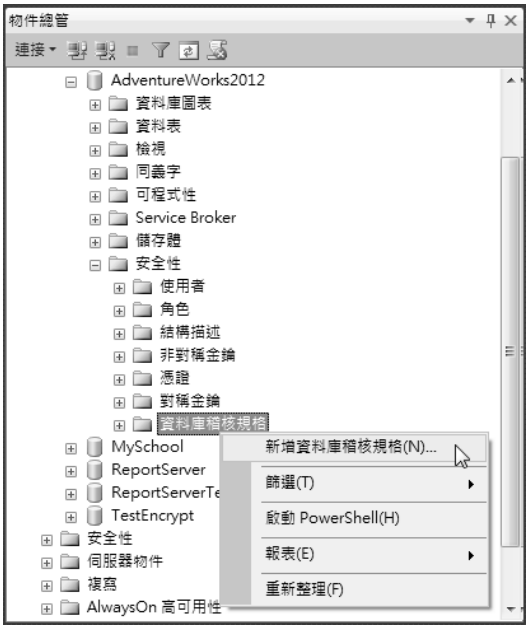
12-1-4 建立資料庫層級稽核規格

我們可以使用 Management Studio 或 T-SQL 指令來建立資料庫層級稽核規格。

使用 Management Studio 建立資料庫層級稽核規格

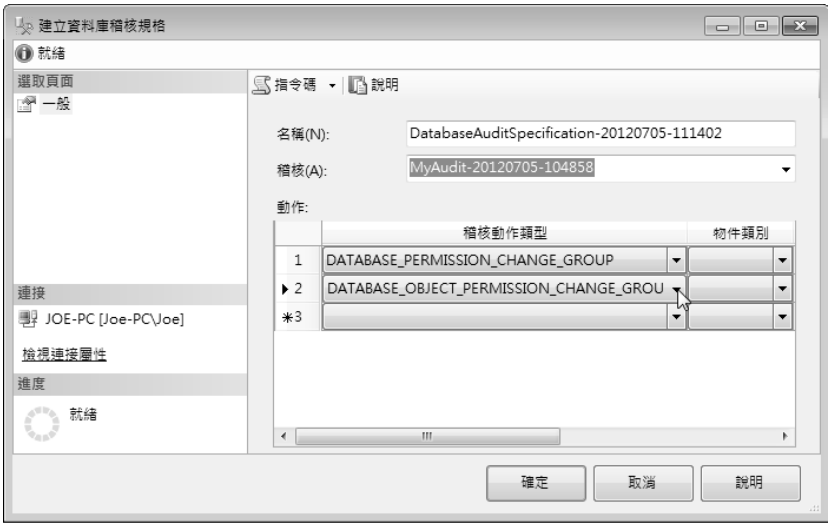
Management Studio 提供圖形介面建立資料庫層級稽核規格物件。例如：替 AdventureWorks2012 資料庫建立資料庫層級稽核規格，稽核動作類型為 DATABASE_PERMISSION_CHANGE_GROUP 和 DATABASE_OBJECT_PERMISSION_CHANGE_GROUP 來稽核資料庫物件的權限變更，其步驟如下所示：

step 1 請啟動 Management Studio 且建立連接後，在「物件總管」視窗展開 AdventureWorks2012 資料庫下的【安全性】項目。



碁峰 www.gotop.com.tw

step 2 在【資料庫稽核規格】上，執行【右】鍵快顯功能表的【新增資料庫稽核規格】指令，可以看到「建立資料庫稽核規格」對話方塊。



step 3 在【名稱】欄輸入資料庫稽核規格名稱，此例是使用預設名稱，【稽核】欄選擇第 12-1-2 節建立的稽核物件【MyAudit-yyyyMMdd-hhmmss】，就可以在下方選擇稽核動作，請選稽核動作類型【DATABASE_PERMISSION_CHANGE_GROUP】和【DATABASE_OBJECT_PERMISSION_CHANGE_GROUP】，按【確定】鈕建立資料庫層級稽核規格。

使用 T-SQL 指令建立資料庫層級稽核規格

T-SQL 提供 CREATE DATABASE AUDIT SPECIFICATION 指令來建立資料庫層級稽核規格，其基本語法如下所示：

```
CREATE DATABASE AUDIT SPECIFICATION audit_spec_name
FOR SERVER AUDIT audit_name
ADD ( audit_action_group_name | audit_action_specification ) [, ...n]
[ WITH ( STATE = ON | OFF ) ]
```


碁峰 www.gotop.com.tw

上述語法可以建立名為 audit_spec_name 的資料庫層級稽核規格，FOR SERVER AUDIT 子句指定所屬的稽核物件。ADD 子句可以新增稽核動作類型，如果不只一個請重複使用 ADD 子句來新增，並且使用「,」號分隔。WITH 子句可有可無，STATE 屬性值 ON 表示啟用；OFF 是停用資料庫層級稽核規格。

不同於伺服器層級稽核規格，除了使用稽核動作類型外，我們也可以使用 audit_action_specification，直接指定主體針對安全性實體進行之動作，可以將這些動作記錄在稽核中，其語法如下所示：

```
action [ ,...n ] ON [ class :: ] securable BY principal [ ,...n ]
```

上述語法的 action 是執行的動作，例如：SELECT 指令，如果有多個請使用「,」號分隔，ON 子句是作用在安全性實體的類別名稱 class，例如：資料庫物件 OBJECT，在「::」之後是安全性實體名稱的 securable，BY 子句是套用稽核動作的 SQL Server 主體名稱。

SQL 指令碼檔：Ch12-1-4-01.sql

請建立名為 MyDatabaseAuditSpec 的資料庫層級稽核規格，屬於 MyServerAudit 稽核，並且新增稽核動作查詢 HumanResources.Employee 資料表，如下所示：

```
USE AdventureWorks2012
GO
CREATE DATABASE AUDIT SPECIFICATION MyDatabaseAuditSpec
FOR SERVER AUDIT MyServerAudit
ADD (SELECT
     ON OBJECT::[HumanResources].[Employee]
     BY [public])
```

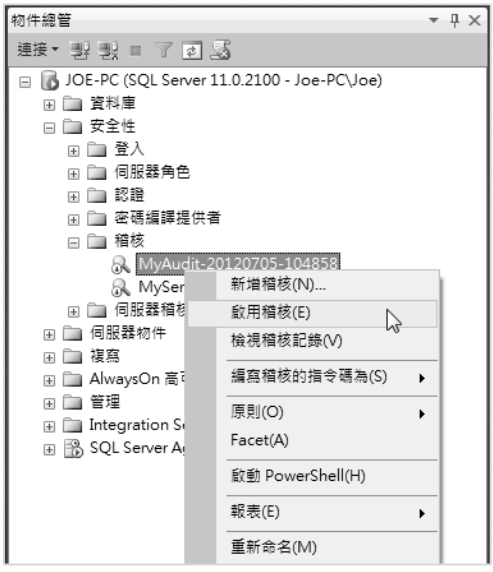
12-1-5 稽核管理

在使用 Management Studio 建立的稽核和稽核規格後，預設是停用狀態，T-SQL 指令可以加上 WITH (STATE = ON)子句來啟用。我們可以使用 Management Studio 或 T-SQL 指令來啟用或停用稽核物件和稽核規格，並且檢視稽核記錄。

碁峰 www.gotop.com.tw

啓用與停用稽核物件

在 Management Studio 啟用與停用稽核物件，請建立連接後，在「物件總管」視窗展開伺服器下【安全性】項目下的【稽核】，如右圖所示：



右述圖例可以看到我們之前建立的 2 個稽核物件，在物件上，執行【右】鍵快顯功能表的【啟用稽核】指令，可以看到「啟用稽核」對話方塊正在啟用稽核，請稍等一下，如下圖所示：

上述訊息顯示已經成功啟用稽核後，按【關閉】鈕完成稽核的啟用。對於已經啟用的稽核，請執行【右】鍵快顯功能表的【停用稽核】指令來停用稽核。

T-SQL 指令是使用 ALTER SERVER AUDIT 指令加上 WITH 子句來更改稽核狀態，WITH (STATE = ON)是啟用；WITH (STATE = OFF)是停用。

SQL 指令碼檔：Ch12-1-5-01.sql

請使用 ALTER SERVER AUDIT 指令來啟用 MyServerAudit 稽核，如下所示：

```
ALTER SERVER AUDIT MyServerAudit
WITH ( STATE = ON )
```


碁峰 www.gotop.com.tw

啓用與停用稽核規格

在 Management Studio 啟用與停用稽核規格，伺服器層級稽核規格是在「物件總管」視窗展開伺服器下【安全性】項目下的【伺服器稽核規格】，然後在指定伺服器層級稽核規格上，執行【右】鍵快顯功能表的【啟用伺服器稽核規格】指令來啟用伺服器層級稽核規格。

資料庫層級稽核規格是在「物件總管」視窗展開資料庫下【安全性】項目下的【資料庫稽核規格】，然後在指定資料庫層級稽核規格上，執行【右】鍵快顯功能表的【啟用資料庫稽核規格】指令來啟用資料庫層級稽核規格。

當啟用稽核規格後，就可以在稽核規格上，執行右鍵快顯功能表的【停用伺服器稽核規格】或【停用資料庫稽核規格】指令來停用稽核規格。

T-SQL 指令是使用 ALTER SERVER AUDIT SPECIFICATION 或 ALTER DATABASE AUDIT SPECIFICATION 指令加上 WITH 子句來更改稽核規格狀態，WITH (STATE = ON)是啟用；WITH (STATE = OFF)是停用。

SQL 指令碼檔：Ch12-1-5-02.sql

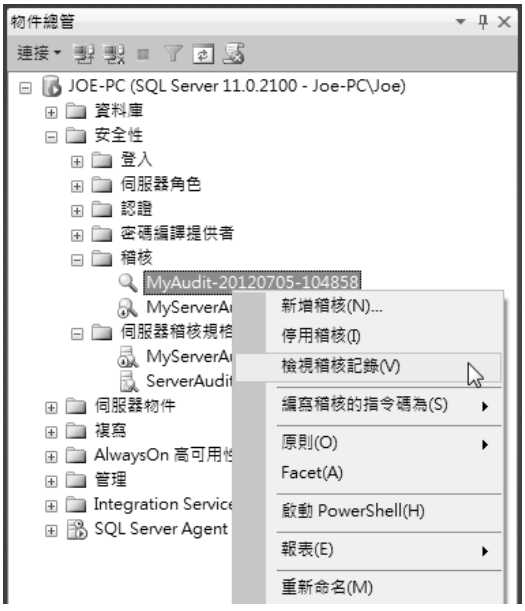
請啟用 AdventureWorks2012 資料庫的 MyDatabaseAuditSpec 稽核規格，如下：

```
USE AdventureWorks2012
GO
ALTER DATABASE AUDIT SPECIFICATION MyDatabaseAuditSpec
WITH ( STATE = ON )
```

檢視稽核記錄

當啟用稽核物件和稽核規格後，如果發生稽核規格中定義的稽核動作，SQL Server 就會將稽核記錄寫入稽核物件定義的目的地，例如：第 12-1-2 節建立的稽核物件【MyAudit-yyyyMMdd-hhmmss】可以稽核登入的密碼變更，請先更改 sa 登入密碼後，我們就可以檢視稽核記錄。請在「物件總管」視窗展開伺服器下【安全性】項目下的【稽核】，如下所示：

碁峰 www.gotop.com.tw



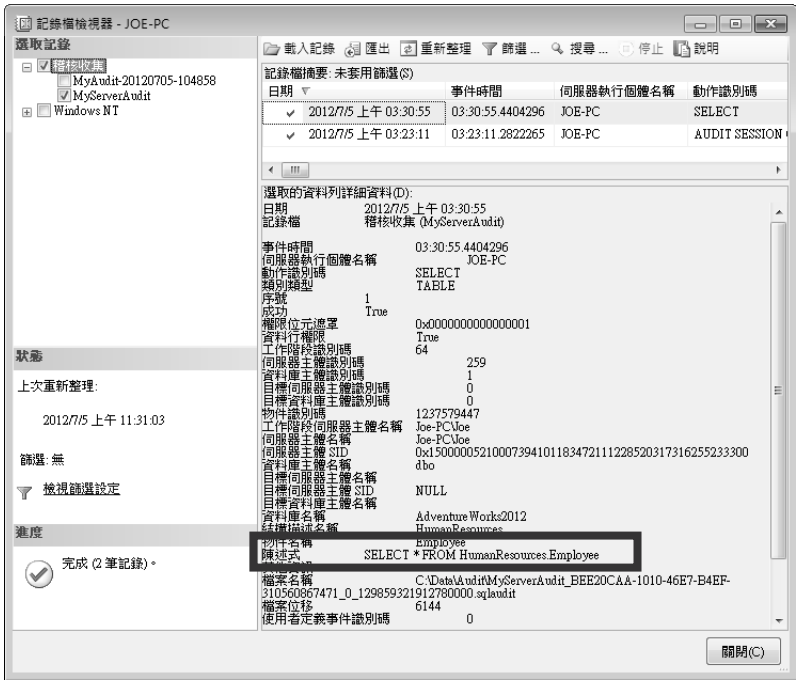
請在【稽核】物件上，執行【右】鍵快顯功能表的【檢視稽核記錄】指令，可以開啟記錄檔檢視器來顯示稽核記錄，如下圖所示：

碁峰 www.gotop.com.tw

上述稽核記錄顯示我們更改 sa 登入的密碼。因為 MyServerAudit 稽核啟用資料庫稽核規格，可以稽核使用者查詢 HumanResources.Employee 資料表（SQL 指令碼檔：Ch12-1-5-03.sql），如下所示：

```
USE AdventureWorks2012
GO
SELECT * FROM HumanResources.Employee
```

在執行上述 SQL 指令後，我們就可以檢視 MyServerAudit 稽核的稽核記錄，顯示查詢 HumanResources.Employee 資料表的記錄，如下圖所示：



碁峰 www.gotop.com.tw

12-2 資料加密

資料加密（Encryption）是將資料庫的資料使用數學運算的演算法加密（Encrypt）成無法一眼就識別的一堆亂碼來保護資料安全。而且只有授權使用者才能解密（Decrypt）成原來資料，看到真正的資料內容。

SQL Server 支援對稱金鑰、非對稱金鑰和憑證，並且提供完整的加密階層來加密資料，可以進一步保障資料庫儲存資料的安全性。

12-2-1 資料加密的基礎

資料庫管理系統的資料庫如果是儲存在不安全的儲存媒體，例如：備份資料，或需要在不安全網路上傳遞資料，資料庫就需使用密碼系統（Cryptographic System）來執行資料加密處理，以保障資料庫的安全。

對稱加密（Symmetric Encryption）

對稱加密技術使用同一把金鑰（Key）來進行資料加密和解密，當使用金鑰將資料加密後，需要使用同一把金鑰來進行解密，才能知道資料內容。

非對稱加密（Asymmetric Encryption）

非對稱加密是使用一對金鑰（Key）來加密和解密資料。公開金鑰密碼系統（Public Key Cryptograpy）使用公開金鑰（Public Key）和私人金鑰（Private Key）進行資料加密處理，每一個金鑰可以解密由另一個金鑰加密的資料。

憑證（Certificates）

憑證是一張電子版的身份証，其基本內容有：一把公開金鑰、姓名、電子郵件地址，憑證的目的是在證明這把公開金鑰確實是此姓名的使用者所擁有。

憑證是由憑證授權單位（Certificate Authority；CA）所簽署，所以憑證內容除公開金鑰、姓名和電子郵件地址外，最重要的是發行者的資訊和其數位簽章。

碁峰 www.gotop.com.tw

數位簽章（Digital Signatures）如同手寫簽名，其目的是為了證明確實是某位使用者送出的訊息。換句話說，發行者的數位簽章就是證明此憑證確實是由此單位所簽發。

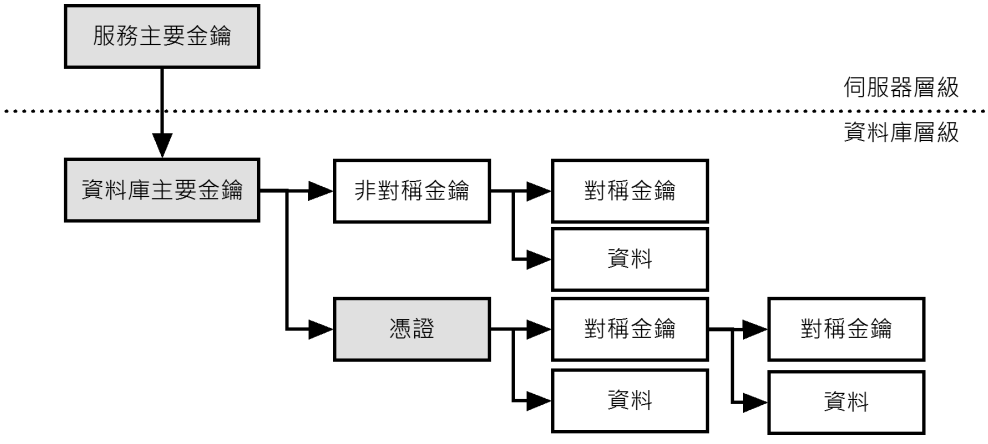
12-2-2 SQL Server 的資料加密

SQL Server 可以針對連接、資料和預存程序使用資料加密來保護資料庫儲存的資料。

加密階層（Encryption Hierarchy）

在 SQL Server 的加密階層（Encryption Hierarchy）中，每一個執行個體在安裝時就自動由 Windows 作業系統的 DPAPI（Data Protection API）建立服務主要金鑰（Service Master Key），其主要目的是用來保護系統資訊。

服務主要金鑰是用來加密每一個資料庫的資料庫主要金鑰（Database Master Key），如下圖所示：



上述圖例上方是伺服器層級；下方是資料庫層級的加密階層，對於每一個資料庫，資料庫主要金鑰可以加密建立下一層憑證或非對稱金鑰，然後，我們就可以使用憑證或非對稱金鑰來加密資料表的欄位資料，即第 12-2-3 節的欄位層級資料加密（Column-level Encryption）。

碁峰 www.gotop.com.tw

或者是在擴充下一層的加密階層，透過憑證或非對稱金鑰來加密下一層的對稱金鑰或資料。

透明資料加密

對於資料庫安全性來說，最常遺漏的部分是資料檔、記錄檔或備份檔案，如果沒有加密，有心人只需取得資料檔、交易記錄檔或備份檔，就可以取得資料庫的機密資料。

「透明資料加密」（Transparent Data Encryption，TDE）是 SQL Server 2008 之後版本新增的功能，可以執行資料和記錄檔的即時 I/O 加密和解密。TDE 可以讓我們不用修改應用程式，就可以加密保護資料庫。

TDE 在資料庫層級是使用資料庫加密金鑰（Database Encryption Key，DEK）對資料檔和交易紀錄檔進行寫入加密和讀取解密，DEK 是一個對稱金鑰，它是使用儲存於 master 系統資料庫的憑證或 EKM 模組保護的非對稱金鑰所加密建立的對稱金鑰。

Extensible Key Management，EKM

Extensible Key Management（EKM）是 SQL Server 2008 版新增的功能，允許讓外部資源，例如：Hardware Security Module（HSM）或其他廠商的加密提供者來幫助我們管理資料庫使用的眾多金鑰。

當企業或組織大量使用金鑰來保護資料時，眾多金鑰的管理便成為一項大工程，EKM 允許更大彈性和選擇來使用外部的加密提供者，可以幫助我們建立跨企業的金鑰管理。

例如：智慧卡公司提供集中管理的智慧卡系統儲存每一張智慧卡的金鑰，並且提供可以安裝在 SQL Server 伺服器的函數庫來存取每一張智慧卡的金鑰，在 SQL Server 伺服器可以註冊函數庫為提供者，即 EKM 提供者，此時，SQL Server 就可以透過外部資源來取得金鑰進行資料加密和解密。

因為 EKM 的使用已經超過本書範圍，筆者只準備簡單說明 EKM，其進一步說明請參閱 SQL Server 線上叢書，或相關書籍。

碁峰 www.gotop.com.tw

12-2-3 欄位層級資料加密

欄位層級資料加密（Column-level Encryption，也稱為 Cell-level Encryption）是在 SQL Server 2005 版就支援的資料加密，可以讓我們加密資料表的指定欄位資料，例如：信用卡卡號的欄位等。

欄位層級的資料加密是使用 SQL Server 的加密階層和相關內建函數來實作，相關函數的說明，如下表所示：

函數	說明
EncryptByCert()、DecryptByCert()	使用憑證公開金鑰產生的私人金鑰進行加密和解密
EncryptByAsymKey()、DecryptByAsymKey()	使用非對稱金鑰進行加密和解密
EncryptByKey()、DecryptByKey()	使用對稱金鑰進行加密和解密

例如：當在資料庫層級使用憑證加密下一層對稱金鑰後，我們就可以使用對稱金鑰進行欄位資料的加密和解密。首先請執行第 10 章的 TestEncrypt.sql 指令碼檔建立測試資料庫 TestEncrypt，擁有信用卡資料的 CreditCards 資料表，此為沒有加密欄位的資料表。

現在，我們準備建立一個準備加密 number 欄位的 CreditCards01 資料表，其 SQL 指令（SQL 指令碼檔：Ch12-2-3-01.sql）如下所示：

```
USE TestEncrypt
GO
CREATE TABLE CreditCards01 (
   cid  INT  PRIMARY KEY,
   number VARBINARY(200)
)
GO
```

上述資料表欄位 cid 是主鍵，number 儲存信用卡卡號資料，這也是我們需要加密的欄位資料。

碁峰 www.gotop.com.tw

步驟一：建立資料庫主要金鑰、憑證和對稱金鑰

T-SQL 是使用 CREATE MASTER KEY ENCRYPTION 指令建立資料庫主要金鑰（Database Master Key），在建立後就可以使用 CREATE CERTIFICATE 和 CREATE SYMMETRIC KEY 指令分別建立憑證和使用憑證來建立對稱金鑰，其 SQL 指令（SQL 指令碼檔：Ch12-2-3-02.sql）如下所示：

```
USE TestEncrypt
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'MyMasterKeyPassword!'
GO
```

上述 SQL 指令使用 BY PASSWORD 指定密碼來建立資料庫主要金鑰後，新增名為 cert_MyKey 的憑證，如下所示：

```
CREATE CERTIFICATE cert MyKey
  WITH SUBJECT = 'Table Data Protection'
GO
```

上述 WITH SUBJECT 是主旨說明。然後就可以使用憑證來加密建立對稱金鑰 MyKey，如下所示：

```
CREATE SYMMETRIC KEY MyKey
  WITH ALGORITHM = AES_128
  ENCRYPTION BY CERTIFICATE cert_MyKey
GO
```

上述 WITH ALGORITHM 指定演算法，可以是 DES、TRIPLE_DES、RC2、RC4、RC4_128、DESX、AES_128、AES_192 和 AES_256，ENCRYPTION BY CERTIFICATE 子句是使用的加密憑證，即我們之前建立的憑證。

步驟二：加密欄位資料

在建立對稱金鑰後，就可以使用 OPEN SYMMETRIC KEY 指令開啟對稱金鑰來加密欄位資料。T-SQL 指令是呼叫 Key_GUID()函數取得對稱金鑰的 GUID 碼後，使用 EncryptByKey()函數加密欄位資料，其 SQL 指令（SQL 指令碼檔：Ch12-2-3-03.sql）如下所示：

碁峰 www.gotop.com.tw

```
OPEN SYMMETRIC KEY MyKey
  DECRYPTION BY CERTIFICATE cert_MyKey
GO
INSERT INTO CreditCards01 VALUES
(1,EncryptByKey(Key_GUID('MyKey'), N'5555-1234-1234-1234'))
GO
INSERT INTO CreditCards01 VALUES
(2,EncryptByKey(Key_GUID('MyKey'), N'6666-5678-5678-5678'))
GO
CLOSE SYMMETRIC KEY MyKey
GO
```

上述 SQL 指令使用 INSERT 指令插入 2 筆加密的信用卡卡號資料後，使用 CLOSE SYMMETRIC KEY 指令關閉對稱金鑰。

步驟三：查詢加密的欄位資料

查詢加密資料是在開啟對稱金鑰後，使用 DecryptByKey()函數解密欄位資料，其 SQL 指令（SQL 指令碼檔：Ch12-2-3-04.sql）如下所示：

```
SELECT cid, number,
cast(DecryptByKey(number) AS NVARCHAR(100))
AS Card_Number
FROM CreditCards01
```

上述 SQL 指令 SELECT 在呼叫 DecryptByKey()函數解密資料後，使用 cast()函數執行類型轉換，可以看到查詢結果加密和解密的欄位資料，number 是加密資料；Card_Number 是解密後的資料，如下圖所示：

結果 訊息

	cid	number	Card_Number
1	1	0x00780D4A65A90A45ACF3A8BF5691398B01000000884439C...	5555-1234-1234-1234
2	2	0x00780D4A65A90A45ACF3A8BF5691398B010000009FA706...	6666-5678-5678-5678

碁峰 www.gotop.com.tw

12-2-4 實作透明資料加密

欄位層級資料加密只是針對資料表的指定欄位進行資料加密，我們可以使用透明資料加密 TDE 替整個資料庫進行資料加密，其建立的基本步驟，如下所示：

step 1 建立 master 資料庫的主要金鑰。

step 2 使用主要金鑰建立憑證。

step 3 使用憑證建立資料庫加密金鑰（Database Encryption Key）。

step 4 在資料庫使用加密。

當資料庫使用 TDE 後，加密資料包含資料庫的 mdf、ndf 資料檔、ldf 的交易記錄檔、備份檔和 tempdb 系統資料庫，如果伺服器上有任何資料庫使用 TDE，tempdb 資料庫也會自動使用 TDE 加密。

建立測試 TDE 的資料庫

在本節筆者準備建立 2 個測試資料庫 TestTDE 和 TestTDE01，分別擁有 CreditCards 資料庫儲存信用卡卡號資料（SQL 指令碼檔：Ch12-2-4-01.sql），如下所示：

```
CREATE DATABASE TestTDE
GO
USE TestTDE
GO
CREATE TABLE CreditCards (
   cid  INT  PRIMARY KEY,
   number VARCHAR(200)
)
GO
CREATE DATABASE TestTDE01
GO
USE TestTDE01
GO
CREATE TABLE CreditCards (
   cid  INT  PRIMARY KEY,
```


碁峰 www.gotop.com.tw

```
    number VARCHAR(200)
)
GO
```

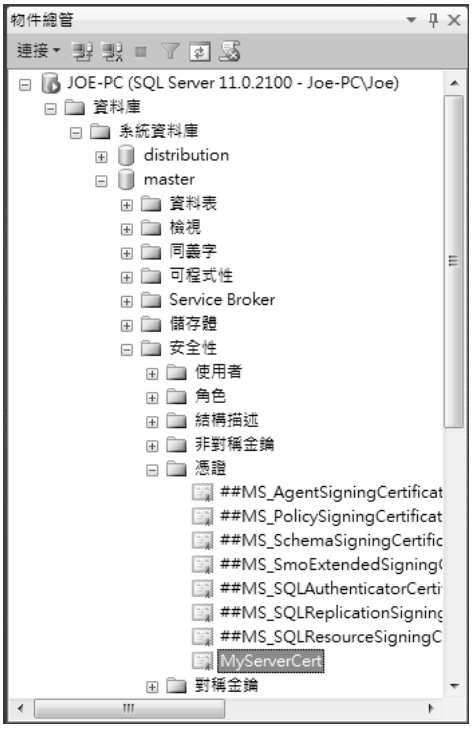
建立 master 系統資料庫的主要金鑰和憑證

然後，我們可以使用 CREATE MASTER KEY ENCRYPTION 指令建立 master 系統資料庫的主要金鑰（SQL 指令碼檔：Ch12-2-4-02.sql），如下所示：

```
USE master
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = 'MyMasterKeyPassword!'
GO
CREATE CERTIFICATE MyServerCert
  WITH SUBJECT = 'My DEK Certificate for TDE'
GO
```

上述指令建立資料庫主要金鑰後，使用 CREATE CERTIFICATE 指令建立加密 DEK 的憑證 MyServerCert，WITH SUBJECT 是主旨說明。

在 Management Studio 的「物件總管」視窗，展開【資料庫】下的【系統資料庫】，可以在【master】系統資料庫下【安全性】下的【憑證】項目，看到我們新增的憑證 MyServerCert，如右圖所示：



碁峰 www.gotop.com.tw

對於資料庫的憑證，我們可以在上述圖例的項目上，執行【右】鍵快顯功能表的【刪除】指令，或使用 DROP CERTIFICATE 指令來刪除（SQL 指令碼檔：Ch12-2-4-03.sql），如下所示：

```
DROP CERTIFICATE MyServerCert
```

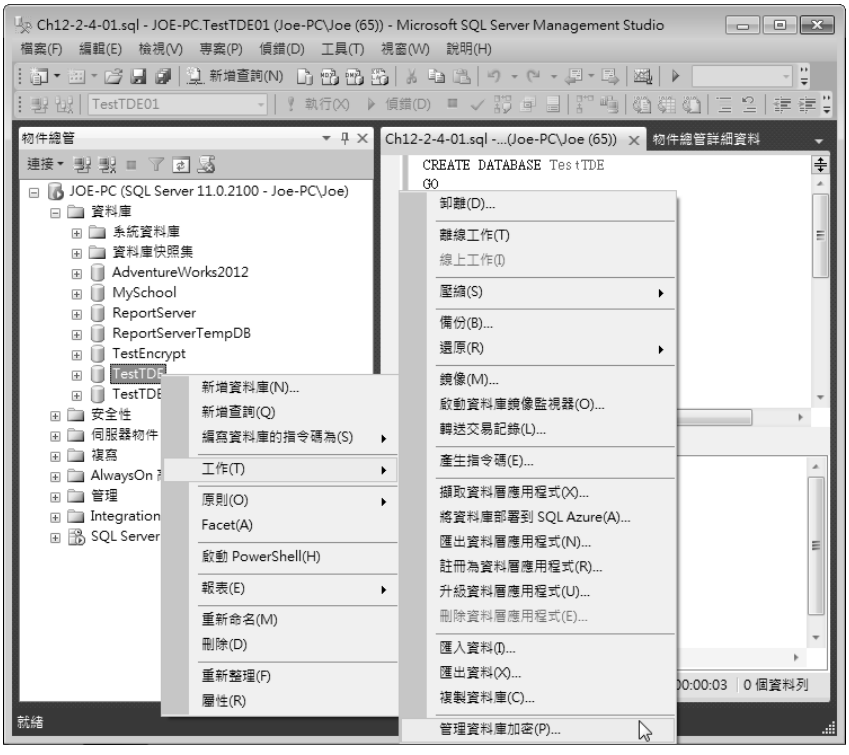
上述指令可以刪除憑證 MyServerCert。刪除資料庫的主要金鑰是使用 DROP MASTER KEY 指令，如下所示：

```
DROP MASTER KEY
```

使用 Management Studio 建立透明資料加密的資料庫

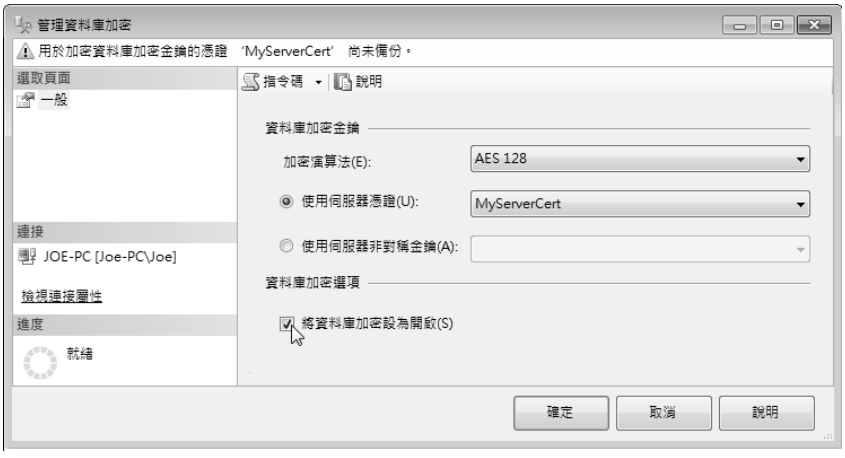
在 master 系統資料庫建立主要金鑰和憑證後，我們就可以使用 Management Studio 建立 TestTDE 資料庫的透明資料加密，其步驟如下所示：

step 1 請啟動 Management Studio 且建立連接後，在「物件總管」視窗展開【資料庫】項目，如下圖所示：



碁峰 www.gotop.com.tw

step 2 在【TestTDE】資料庫上，執行【右】鍵快顯功能表的「工作>管理資料庫加密」指令，可以看到「管理資料庫加密」對話方塊。



step 3 選【使用伺服器憑證】和選之前建立的【MyServerCert】來建立資料庫加密金鑰，勾選【將資料庫加密設為開啟】，按【確定】鈕建立透明資料加密的資料庫。

使用 T-SQL 指令建立透明資料加密的資料庫

除了使用 Management Studio 工具，我們也可以使用 T-SQL 指令建立 TestTDE01 資料庫的透明資料加密，首先建立資料庫加密金鑰（SQL 指令碼檔：Ch12-2-4-04.sql），如下所示：

```
USE TestTDE01
GO
CREATE DATABASE ENCRYPTION KEY
  WITH ALGORITHM = AES_128
  ENCRYPTION BY SERVER CERTIFICATE MyServerCert
```

上述 CREATE DATABASE ENCRYPTION KEY 指令可以建立資料庫加密金鑰，演算法是 AES_128，使用伺服器憑證 MyServerCert 來加密金鑰。然後就可以更改資料庫啟用透明資料加密，如下所示：

```
ALTER DATABASE TestTDE01
SET ENCRYPTION ON
```


碁峰 www.gotop.com.tw

學 習 評 量

1. 請簡單說明什麼是資料庫稽核？
2. 請問 SQL Server Audit 是使用哪三種物件來描述我們建立的資料庫稽核？
3. 請問 SQL Server 建立資料庫稽核的基本步驟為何？
4. 請問何謂對稱加密？非對稱加密？憑證？數位簽章？並且使用圖例說明 SQL Server 的加密階層（Encryption Hierarchy）。
5. 請簡單說明什麼是欄位層級資料加密？何謂透明資料加密 TDE？
6. 請問什麼是自主資料庫？自主資料庫可以分為哪兩種？自主資料庫的使用者有哪兩種？
7. 請以 AdventureWorks2012 範例資料庫為例，使用 T-SQL 指令啟用透明資料加密 TDE。
8. 請使用 Management Studio 建立名為 MyContainedDB 的自主資料庫，並且新增名為 test 擁有密碼 1234 的使用者來連接自主資料庫。

碁峰 www.gotop.com.tw