

第六堂 與程式間的合作

聯成電腦

張明泰 mtchang.tw@gmail.com





常見的架構

- IIS+MySQL+PHP+PhpMyAdmin
- IIS+MsSQL+ASP+SQL ManagementStudio
- Apache+MySQL+PHP+phpmyadmin
- <http://www.appservnetwork.com> (懶人整合包)
- LAMP: Linux+Apache+Mysql+PHP



PHP與MySQL

- 確定自己的PHP及MySQL環境可以RUN。
- 講解複習預存程序。
- 工欲善其事必先利其器
<http://notepad-plus.sourceforge.net/uk/site.htm>



PHPMYADMIN

- 官方網站：
http://www.phpmyadmin.net/home_page/index.php
- 設定組態？ Config.default.php
- 操作...
- 教學文件：
<http://groups.google.com.tw/group/lccnetsql>
已有放置swf教學動畫檔



使用**PHP**讀取**MySQL**資料庫

```
<? # mysql_query.php檔案
# 設定mysql的連線ID
$conn = mysql_connect("localhost", "mtchang", "qw") or die("Could not connect");
# 設定再查詢mysql使用的字元編碼為UTF-8。很重要，沒設定出來會都是亂碼
mysql_query("SET NAMES 'utf8'");
# 選取資料庫
mysql_select_db("mtchang", $conn);
# 設定SQL敘述
$sql = "select * from students";
# 將SQL敘述傳給SQL server查詢，並節回傳結果放在變數$result
$result = mysql_query($sql);
# 計算此SQL表格有多少欄位
$numfields = mysql_num_fields($result);
# 迴圈，讀取$result裡面的內容，直到空為止
while ($row = mysql_fetch_row($result))
{
    # 迴圈，讀取列。依據欄位數顯示row值
    for($i = 0 ; $i < $numfields ; $i++)
    {
        echo $row[$i] . " ";
    }
    # html的斷行
    echo "<br />";
}
?>
```



練習：

- 請練習使用上頁範例程式，**改變SQL敘述及你的SQL server設定值**並輸出到網頁上。
- 請配合**SQL的limits**指令，限制輸出的row，並嘗試做到**分頁**的效果。



休息一下



改成表單**POST**傳值

(1)修改mysql_query.php最前面加入表單語法

```
<form enctype="multipart/form-data" action="mysql_inject.php"
method="post" name="mysql-test" target="_self">
<input name="query" type="text" value="" size="60" maxlength="300" />
<input type="submit" name="Submit" value="送出" />
</form>
```

(2)修改\$sql

將原本的 \$sql = "select * from students";

修改成爲 **\$sql=\$_POST['query'];**

接受來自於表單的值



一個**PHP**的例子**SQL- Injection**

- 我們修改一下剛剛表單輸入的程式，讓他成爲一個可以判斷學號是否正確的程式。

```
# 修改這行....設定SQL敘述
```

```
$sql='SELECT * FROM students WHERE 學號='.$_POST['query'].';';
```

```
# 在這行下面加入判斷式
```

```
$result = mysql_query($sql);
```

```
# 如果yes代表學號通過驗證，no代表不通過
```

```
if($result)
```

```
    echo "yes<br />";
```

```
else
```

```
    echo "no<br />";
```



SQL入侵練習與防範

- 上述範例如何讓他被SQL Injection ？
- 『資料隱碼』SQL Injection的源由與防範之道
- http://www.microsoft.com/taiwan/sql/SQL_Injection.htm
- SQL Injection (資料隱碼)– 駭客的 SQL填空遊戲
- http://www.microsoft.com/taiwan/sql/SQL_Injection_G1.htm



『資料隱碼』SQL Injection的源由與防範之道

- 利用特殊指令攻擊
- 駭客於任何要求輸入資料時打入特殊指令或程式碼，讓破壞性程式碼『隱藏』在標準的SQL程式中，達到其攻擊目的。
- 利用系統的錯誤訊息找出資料庫弱點
- 要對資料庫進行存取或修改，必需要對資料庫的結構有所瞭解，通常駭客很難瞭解資料庫結構，但未經掩飾的錯誤訊息反而容易造成問題。資料庫管理系統為能協助 程式開發與管理人員了解錯誤指令所造成的問題與根源，會在錯誤訊息上顯示完整的資訊，若電子商務系統未經防範而直接讓錯誤訊息顯示在網頁上，無異是給駭客 入侵留下線索。
- 為能有效的阻絕駭客利用『資料隱碼』方式入侵，微軟建議採取以下各項防範之道：
- 1. 加強程式上的安全檢查措施：在程式中加上輸入資料型態檢查、資料長度檢查與資料內容檢查，讓駭客無法利用隱藏於輸入資料的特殊指令或程式碼有機可乘。
- 2. 妥善使用權限管理：在程式中勿用較高權限來存取資料庫，比如說讓SQL程式使用資料庫管理員(System Administrator, SA)身份來存取資料庫。此外，若使用Windows 2000作業系統搭配SQL Server則建議使用Windows 2000認證機制。
- 3. 保持良好的程式開發習慣：撰寫資料庫存取或查詢程式時，利用兩個單引號『』來標註任何輸入的變數給SQL程式；利用單引號『』會讓駭客的隱碼易於得逞。
- 4. 將核心程式碼隱藏起來：勿讓網頁上程式直接存取或查詢資料庫，而是透過預存程式(Stored-procedure)來執行，而XML Web Service也是另一個提高安全性的好方法，保護核心程式邏輯與資料庫結構不至外洩，而Microsoft SQL Server 2000是目前唯一支援XML Web Service的資料庫管理系統。
- 5. 以標準的訊息回覆給客戶：電子商務網站對於任何回覆給客戶的訊息應有所規範，透過程式攔截下任何作業系統或資料庫管理系統所可能產生的錯誤訊息，改以統一且明確的訊息來指導客戶。
- 6. 刪除多餘的資料表(Table)：資料庫管理系統安裝後會有幾個既存的資料表，這些資料表是供程式開發、範例資料庫或暫存使用，如“pub”及“Northwind”等，請在電子商務網站上線後移除；因為這些公用的資料表架構是公開的，易為駭客所利用。



休息一下





變更欄位的結構

- 範例：**alter table test add writer varchar(30);**
- 說明：新增一個varchar(30)的欄位writer於test資料庫中
- 範例：**ALTER TABLE test ADD writer2 VARCHAR(30) DEFAULT 'ANK';**
- 說明：新增一個varchar(30)的欄位writer於test資料庫中並且設定其預設值為「ANK」



變更欄位的結構-2

- 範例：**ALTER TABLE `test` DROP `writer`**
- 說明：刪除write欄位



追加限制條件

- 範例：**ALTER TABLE `test` ADD PRIMARY KEY (學號);**
- 說明：在SQL中可以追加primary key, UNIQUE, check

結論：系統管理盡量用工具

127.0.0.1 / localhost / mtchang / test | phpMyAdmin 2.7.0-pl2 - Mozilla Firefox

檔案(F) 編輯(E) 檢視(V) 瀏覽(G) 書籤(B) 工具(T) 說明(H)

http://127.0.0.1/myweb/mysql_admin/index.php?lang=zh-tw-utf-8&server=1&collation_connecti





























































mtchang 常用文件網站 下載 最近焦點 快速搜尋 127.0.0.1 - /myweb/ Yahoo!奇摩 Google 電子化政府入口網

Google 吳佳諺 搜尋 PageRank ABC 檢查 選項 吳佳諺

127.0.0.1 - /myweb/sql/mt... Linux Company 127.0.0.1 / localhost / ... 博客來書籍館 SQL Injection (資料隱碼...)

localhost ▶ mtchang ▶ test "InnoDB free: 10240 kB"

結構 SQL 搜索 依範例查詢 (QBE) 輸出 Import 管理 權限 刪除

	資料表	執行	記錄	型態	校對	大小	多餘
<input type="checkbox"/>	conduct	    	479	InnoDB	utf8_general_ci	48.0 KB	-
<input type="checkbox"/>	customer	    	60	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	dept	    	17	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	employee	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	exp	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	leave	    	83	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	overtime	    	110	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	person	    	97	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	product	    	20	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	quota	    	16	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	quotat1	    	16	InnoDB	utf8_general_ci	16.0 KB	-
<input type="checkbox"/>	records	    	300	InnoDB	utf8_general_ci	48.0 KB	-

phpMyAdmin

資料庫

mtchang (19)

- conduct
- customer
- dept
- employee
- exp
- leave
- overtime
- person
- product
- quota
- quotat1
- records
- sales
- sales1
- sales2
- students
- test



SQL 進階操作

- 備份及還原
- 權限及安全性



資料備份及還原

- 備份觀念

- 備份方式

- 完整備份→將資料庫資料完整備份。
 - 差異式備份→從上次資料庫完整備份算起，到目前的資料異動的部份，備份下來。
 - 交易記錄檔備份→從上次交易記錄檔備份之後，到目前為止的資料，備份下來。
 - 檔案與檔案群組→用於大型資料庫或分散式資料庫。



資料備份及還原

- 備份策略

- 考慮資料的重要性
 - 資料的變動率是不是很高
 - 資料庫內的表格，哪些是常動作的，哪些是不動作的。
 - 資料庫大小，以及其成長速度。
- 考慮人員因素
 - 執行備份的人員
 - 備份資料的管理人員
 - 監視備份進行人員
- 考慮時間點因為
 - 復原等待的時間
 - 備份時間的選擇
 - 備份週期



資料備份及還原

- 開始備份與還原

- 使用 Management Studio 進行備份

- 在欲執行備份的資料庫上，按右鍵。
 - 選擇“工作”→“備份”。
 - 在“來源”的框格中
 - 確認資料庫是否為你所選的
 - 所需要的備份方式
 - 按下目的地框格中，“加入”的按鍵
 - 在按下來的視窗中，請確認路徑以及檔案名稱。
 - 如果有其他的備份裝置，可以在此勾選。
 - 回到前一步驟的視窗後，按下“確定”即可。



資料備份及還原

- 使用 Management Studio 進行還原
 - 在資料庫的資料匣上，按滑鼠右鍵。
 - 選擇“還原資料庫”
 - 在“還原的來源”窗框中，選擇“來源裝置”。
 - 在來源裝置項目中，按下“…”按鈕。
 - 按下“加入”按鈕，並按下“確定”。
 - 回到上一步驟的視窗中，在“選取要還原的備份組”視窗中，勾選欲還原的備份資料。
 - 在“目的地資料庫”中，輸入資料庫名稱。
 - 最後，按下“確定”即可。



資料備份及還原

- 使用SQL語言來備份、還原

- 首先建立備份裝置

- 有兩個預存程序可以建立及移除

Use eBook

Exec sp_addumpdevice

'disk', 'ebookBackup1', 'C:\ebookBackup1.bak'

使用sp_addumpdevice來建立備份裝置，共有四個引數。

第一個引數，裝置型態→disk, tape, pipe

第二個引數，裝置名稱

第三個引數，實體檔案名稱

第四個引數，磁帶機狀態→noskip, skip

use eBook

exec sp_dropdevice 'ebookBackup0104'; delfile'

2007/12/16

聯成電腦SQL描述語言課程 張明泰



資料備份及還原

- 查看裝置

- RESTORE FILELISTONLY → 列出指定備份裝置或基本資料

RESTORE FILELISTONLY

FROM DISK='C:\ebookBackup1.bak'

Go

RESTORE FILELISTONLY

FROM ebookBackup1

- 標準語法

RESTORE FILELISTONLY

FROM <備份檔案或是裝置名稱>

[with

[FILE = 備份組編號]

[[,] PASSWORD = {備份組的密碼}]

[[,] MEDIAPASSWORD = {媒體集的密碼}]

[[,] { NOUNLOAD | UNLOAD }] - 使用於磁帶機，表示是否自動捲回及載

出



資料備份及還原

- 查看表頭資訊

- RESTORE HEADERONLY

- RESTORE HEADERONLY

- FROM DISK='C:\ ebookBackup1.bak '

- Go

- RESTORE HEADERONLY

- FROM ebookBackup1

- 相關欄位說明

- Backuptype→1:資料庫 2:交易記錄 4:檔案 5:資料庫差異備份 6:檔案差異備份 7:部份備份 8:部份差異備份



資料備份及還原

- 傳回有關媒體集的資訊

- RESTORE LABELONLY

- RESTORE LABELONLY

- FROM DISK='C:\ebookBackup1.bak '

- Go

- RESTORE LABELONLY

- FROM ebookBackup1

- 每一個媒體集，可以包含多個備份組，每一個備份組，又可以使用多個媒體。



資料備份及還原

- 驗證備份集是否完整，所有媒體是否可讀取。

- RESTORE VERIFYONLY

- RESTORE VERIFYONLY

- FROM DISK='C:\ ebookBackup1.bak '

- Go

- RESTORE VERIFYONLY

- FROM ebookBackup1

資料備份及還原

- 備份的T-SQL標準語法 → backup

```
BACKUP DATABASE {資料庫名稱}
TO <備份裝置名稱>
[ WITH
  [ BLOCKSIZE = { 區塊大小 } ]
  [ [, ] DESCRIPTION = { '文字說明' } ]
  [ [, ] DIFFERENTIAL ]
  [ [, ] EXPIREDATE = { 到期日 } | RETAINDAYS = { 到期天數 } ]
  [ [, ] PASSWORD = { 密碼 } ]
  [ [, ] FORMAT | NOFORMAT ]
  [ [, ] { INIT | NOINIT } ]
  [ [, ] MEDIADESCRIPTION = { '媒體集的文字說明' } ]
  [ [, ] MEDIANAME = { 媒體集名稱 } ]
  [ [, ] MEDIAPASSWORD = { 媒體集密碼 } ]
  [ [, ] NAME = { 備份組名稱 } ]
  [ [, ] { NOSKIP | SKIP } ]
  [ [, ] { NOREWIND | REWIND } ]
  [ [, ] { NOUNLOAD | UNLOAD } ]
  [ [, ] RESTART ]
  [ [ 1 STATS ] ] =更新顯示訊息的級距 ] ]
```



資料備份及還原

- 備份實例

- 完整備份

Backup Database eBook

To Disk='C:\eBook.bak'

With Password='1234',Stats=10,INIT

使用完整備份，並加上密碼，每完成10%，要顯示訊息，最後的INIT表示，如有相同檔案，則加以覆蓋。

- 差異備份

Backup Database eBook To Disk='C:\eBook.bak'

With Differential

- 交易記錄備份

Backup Log eBook To Disk='C:\eBookLog.bak'

With No_Log

2007/12/16

資料備份及還原

- 還原方法

- 還原指令→RESTORE 完整語法

```
RESTORE DATABASE {資料庫名稱}
[ FROM <備份裝置名稱> [,....n] ]
[ WITH
  [ RESTRICTED_USER ]
  [[,] FILE = { 備份組編號 } ]
  [[,] PASSWORD = { 密碼 } ]
  [[,] MEDIANAME = { 媒體集名稱 } ]
  [[,] MEDIAPASSWORD = { 媒體集密碼 } ]
  [[,] MOVE '邏輯名稱' TO '實體名稱' ][,....n]
  [[,] KEEP_REPLICATION ]
  [[,] { NORECOVERY | RECOVERY | STANDY = {復原檔案名稱} } ]
  [[,] { NOREWIND | REWIND } ]
  [[,] { NOUNLOAD | UNLOAD } ]
  [[,] REPLACE ]
  [[,] RESTART ]
```

2007/12/16

聯成電腦SQL描述語言課程-張明泰

29



資料備份及還原

- 實例：還原整個資料庫

```
RESTORE DATABASE eBook  
FROM DISK = 'c:\eBook.bak'  
WITH Password='1234',  
MOVE 'eBook' TO 'C:\Program Files\  
Microsoft SQL  
Server\MSSQL.1\MSSQL\Data\eBook_Data.mdf',  
MOVE 'eBook_Log' TO 'C:\Program Files\  
Microsoft SQL Server\MSSQL.1\MSSQL\Data\eBook_Log.ldf'
```

資料備份及還原

```
RESTORE DATABASE {資料庫名稱}
[ FROM <備份裝置名稱> [,....n]]
[ WITH
  [ RESTRICTED_USER ]
  [[,] FILE = { 備份組編號 } ]
  [[,] PASSWORD = { 密碼 } ]
  [[,] MEDIANAME = { 媒體集名稱 } ]
  [[,] MEDIAPASSWORD = { 媒體集密碼 } ]
  [[,] MOVE '邏輯名稱' TO '實體名稱' ][,....n]
  [[,] KEEP_REPLICATION ]
  [[,] { NORECOVERY | RECOVERY | STANDY = {復原檔案名稱} } ]
  [[,] { NOREWIND | REWIND } ]
  [[,] { NOUNLOAD | UNLOAD } ]
  [[,] REPLACE ]
  [[,] RESTART ]
  [[,] STATS [[ =更新顯示訊息的級距 ] ]
  [[,] STOPAT = { 時間點 } | [[,] STOPATMARK = '標記名稱' [AFTER 時間點 ]
    | [[,] STOPBEFOREMARK = '標記名稱' [AFTER 時間點 ] ] ]
```



權限及安全性

- MS-SQL Server安全機制是由驗證模式開始，再以登入帳戶、使用者、角色及權限四個元素所組成。
- 驗證模式
 - Windows 驗證模式→SQL Server呼叫Windows系統，詢問使用者的有關資訊，以便驗證帳戶名稱與密碼。
 - SQL Server 及 Windows 驗證模式(混合模式)→使用者從非信任連線進行連線時，SQL Server本身會執行驗證。



權限及安全性

- 更改驗證模式

- 在已連結的伺服器，按滑鼠右鍵，選擇“屬性”
- 選擇“安全性”
- 伺服器驗證→更改驗證模式
- 登入稽核→記錄檔要記錄的項目
- 伺服器Proxy帳戶→表示使用者可以使用Proxy伺服器連線到SQL Server。
- 選項
 - C2→美國安全標準，會建立追蹤檔，但檔案會很大。
 - 跨資料庫擁有權鏈結→可以以同一個帳戶登入兩個以上的資料庫，並且有相同權限



權限及安全性

– 登入帳戶及角色

- 登入帳戶 → 連結SQL Server使用
- 角色 → 使用資料庫的使用者帳戶
- 登入帳戶會對應到SQL Server內部的使用者帳戶，
以方便可以操作資料庫。

– Sa

- SQL Server內建的管理員帳戶，而且不得變更。
- 需要在安裝過程中指派密碼。
- 如果使用Windows驗證，也必須在安裝之後，立即
指派密碼。



權限及安全性

- 帳號管理

- 使用 Management Studio 建立新帳號

- 在安全性資料匣，按滑鼠右鍵，選擇“新增登入…”
 - 在對話視窗中，輸入登入名稱
 - 選擇使用 SQL Server 驗證
 - 選擇密碼管理選項
 - 選擇可登入的資料庫
 - 設定語言
 - 按下確定，即可完成



權限及安全性

- 使用SQL語法，新增登入的使用者

USE master

CREATE LOGIN David

WITH PASSWORD='1234',

DEFAULT_DATABASE=eBook,

DEFAULT_LANGUAGE=[繁體中文],

CHECK_EXPIRATION=ON,

CHECK_POLICY=ON

GO



權限及安全性

- 登入帳戶的設定
 - 使用Management Studio來對應其可進行的工作
 - 在登入帳戶名稱上，按右鍵，選擇”屬性”
 - 在視窗左方，選擇”伺服器角色”
 - 勾選其所扮演的角色為何
 - 選擇”使用者對應”
 - 勾選其可操作的資料庫
 - 選擇”安全性實體”
 - 按”加入”，加入目前的實體
 - 勾選授權的實際權限。
 - 選擇狀態，記得設定可連結及可登入。



權限及安全性

- 伺服器角色定義

- 共八個，管理人員無法自行新增角色。

- bulkadmin→ 可使用BULK INSERT，執行大量記錄
 - dbcreator→可建立、改變、卸除及還原任何資料庫
 - diskadmin→可管理資料庫在磁碟機上的檔案
 - processadmin→可結束SQL Server執行的處理序
 - securityadmin→可管理登入及屬性
 - serveradmin→可設定伺服器組態及關閉伺服器
 - setupadmin→可新增及連結伺服器，亦可執行部份系統預存程序
 - sysadmin2007/12/16 聯成電腦SQL描述語言課程 張明春→可執行伺服器中的所有動作。



權限及安全性

- 可用T-SQL的系統預存程序，查看每一登入帳戶的設定

EXEC sp_helplogins

- 可用T-SQL的系統預存程序，查看伺服器角色詳細內容

EXEC sp_srvrolepermission

- 可使用Management Studio新增角色的成員
 - 選擇"安全性"→"伺服器角色"→任選一個角色，按右鍵，選"屬性"。
 - 按"新增"→再按下"瀏覽"，即可新增一個成員。
 - 按"移除"→亦可移除不要的帳號。



權限及安全性

- 使用T-SQL來處理伺服器角色及登入帳號
 - sp_addsrvrolemember→加入帳號至伺服器角色
EXEC sp_addsrvrolemember
'server\David','sysadmin'
 - sp_dropsrvrolemember→自伺服器角色移除帳號
EXEC sp_dropsrvrolemember 'David','sysadmin'
 - sp_helpsrvrolemember→查看每一伺服器角色的成員
EXEC sp_helpsrvrolemember



權限及安全性

- 使用者管理

- **dbo**→資料庫擁有者，具有隱含權限的使用者，可在資料庫中執行所有的動作。所有sysadmin的成員，所建立的任何物件，都屬於dbo。
- **guest**→資料庫建立後，自動會產生。其目的是提供未經授權或明確定義的使用者，具有一定程度的權限。其帳號不可以刪除，但可更改其權限。



權限及安全性

- 利用 Management Studio 來建立使用者
 - 開啟 ebook 資料庫
 - 選擇"安全性"→"使用者"→按右鍵→"新增使用者"
 - 輸入使用者名稱
 - 選擇登入名稱(登入帳號)
 - 按下確定
- 使用 SQL 語言，授與登入帳戶使用資料庫權利

```
CREATE LOGIN David WITH PASSWORD = '123456'
```

```
USE eBook
```

```
CREATE USER DavidUser FOR LOGIN David
```

```
WITH DEFAULT_SCHEMA = dbo
```

2007/12/16

聯成電腦SQL描述語言課程-張明泰

ps:可用 DROP USER 及 ALTER USER



權限及安全性

- 利用預存程序來查詢使用者資訊

USE ebook

EXEC sp_helpuser

- 資料庫角色定義

- 資料庫角色為擁有實際存取權限的群組。
- 每一個使用者可隸屬多個角色，而擁有該角色的權限。
- 內建的資料庫角色共有九種。
 - db_accessadmin→可新增或移除 Windows 登入、Windows群組及SQL Server登入的存取權。
 - db_backupoperator→可備份資料庫
 - db_datareader→可讀取所有使用者資料表中的資料
 - db_datawriter→可新增、刪除、修改資料表中的資料

2007/12/16

聯成電腦SQL描述語言課程-張明泰



權限及安全性

- db_ddladmin→可執行任何DDL的命令
- db_denydatareader→不可資料庫中的任何資料
- db_denydatawriter→不可新增、修改、刪除任何資料
- db_owner→可在資料庫中執行所有的組態、維護、卸除資料庫的動作。
- db_securityadmin→可修改角色員資格及管理權限
- public→每個資料庫都一定會有的角色
 - » 擁有資料庫中使用者的所有預設權限
 - » 無法將使用者、群組、角色指派給它
 - » 系統及資料庫都有它存在
 - » 無法移除
 - » 管理人員可更改其權限



權限及安全性

- 使用Management Studio新增角色
 - 選擇ebook資料庫
 - 選擇”安全性”→”角色”→”資料庫角色”→按右鍵→”新增資料庫角色”
 - 輸入角色名稱(David_role)
 - 指定擁有者→dbo
 - 按下”加入”，選擇DavidUser
 - 按下確定

- 使用SQL語言，授予使用者資料庫的角色

use eBook

CREATE ROLE David_role AUTHORIZATION dbo

exec sp_addrolemember 'David_role','DavidUser'

PS:如要刪除角色，須先刪除成員後，才可刪角色。



權限及安全性

- 可利用系統預存程序來查詢
USE ebook
exec sp_helprolemember
exec sp_helprole
- 設定權限
 - 不論使用者或是角色，都是權限設定對象。
 - 使用者所取得的實際權限，原則上是“聯集”，除非有禁止的狀況。
 - 在作用的對象上，可分成伺服器及資料庫。



權限及安全性

– 使用 Management Studio 來設定權限

- 設定伺服器權限

- 在伺服器的圖案上，按右鍵，選擇屬性
- 在左方的視窗中，選擇“權限”
- 在“登入或角色”中，選擇欲設定的對象(David)
- 在“明確權限”中，勾選權限設定

授與者→目前登入SQL Server的伺服器帳號

權限→目前登入的帳號可設定的權限

授與→表示給予授權

可授與→表示給予的權限，亦可轉授與其他帳號

拒絕→禁止權限

- 按下確定即可



權限及安全性

- 設定資料庫權限
 - 選擇ebook資料庫
 - 按右鍵→"屬性"
 - 在左方視窗中，選擇"權限"
 - 在右方的視窗中，在"使用者或角色"中，選擇"DavidUser"
 - 在右下的視窗中，勾選想到授與的權限
 - 按下"確定"即可
- 設定物件(資料表)權限
 - 選擇ebook資料庫→選擇"資料表"
 - 選擇"dbo.Products"資料表→按右鍵→選擇"屬性"
 - 在左方的視窗中，選擇"權限"
 - 在右方的視窗中，在"使用者或角色"的視窗中，新增"DavidUser"
 - 在下方的視窗中，勾選合適的權限，再按下"確定"即可



權限及安全性

– 利用T-SQL來設定權限

- GRANT(授與)

GRANT [ALL or 權限名稱] ON [物件] TO [使用者或角色]
WITH [選項]

範例：

Use ebook

GRANT SELECT ON OBJECT::dbo.members TO
DavidUser

GRANT REFERENCES (MemberID) ON
OBJECT::dbo.orders

TO DavidUser WITH GRANT OPTION

ps : WITH GRANT OPTION → 可授與

2007/12/16

聯成電腦SQL描述語言課程-張明泰

- DENY(拒絕)



權限及安全性

- REVOKE(撤銷)

REVOKE [ALL or 權限名稱] ON [物件] TO [使用者或角色]
[CASCADE]

PS: [CASCADE]→表示取消可授與的權限

- 查看可用權限

Select * From sys.fn_builtin_permissions(DEFAULT)

- 查看權限內容

USE ebook

exec sp_helprotect



感謝各位

<http://groups.google.com.tw/group/lccnetsql>

<msn/email:mtchang.tw@gmail.com>



參考

- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010313014>
- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010317524>
- <http://www.books.com.tw/exep/prod/booksfile.php?item=0010284070>

