權限與角色

權限與角色

- 在以前，Oracle 的 DBA (資料庫管理者)必須將系統權限或物件權限一一授與每一個使用者，或者將系統權限或物件權限一一從每一個使用者中回收。如此在管理方面並不是很方便，因此 Oracle 就創造了「角色」(Role) 這資料庫物件來方便 DBA 在權限上的管理。

權限(Privilege)

- 系統權限(System Privilege)
- 物件權限(Object Privilege)

系統權限(System Privilege)

- 系統權限是指對於系統中執行特殊的資料庫操作的權利。系統權限可授權給使用者(User) 或角色(Role)。

物件權限(Object Privilege)

- 物件權限允許授與者對資料庫物件執行某種操作。

表二　物件權限

物件權限	表格	視觀表格	序列	程序、函數、套裝程式	快照
ALTER	✓		✓		
DELETE	✓	✓			
EXECUTE				✓	
INDEX	✓				
INSERT	✓	✓			
REFERENCES	✓				
SELECT	✓	✓	✓		✓
UPDATE	✓	✓			

角色(Role)

- 角色(role) 是一組已選擇的權限，它可授權給其他使用者或其他角色。
- ORACLE 系統利用角色來方便資料庫的權限管理。

使用角色管理資料庫的主要優點

- 減少權限管理
- 動態權限管理

減少權限管理

- 當對同一類型的使用者要授予相同的權限組時，只需將該權限組授權予某角色，然後再將角色授權給每個使用者。

動態權限管理

- 若某角色的使用者之權限需要改變，只需修改該角色的權限即可自動地修改該角色內每個使用者的權限，不必對角色中的每個使用者個別做修改。

建立與刪除角色的相關指令

1. 建立角色—CREATE ROLE
2. 更改角色—ALTER ROLE
3. 刪除角色—DROP ROLE
4. 暫時讓使用者所擁有的角色有效(Enable)或失效(Disable)—SET ROLE

建立角色—CREATE ROLE

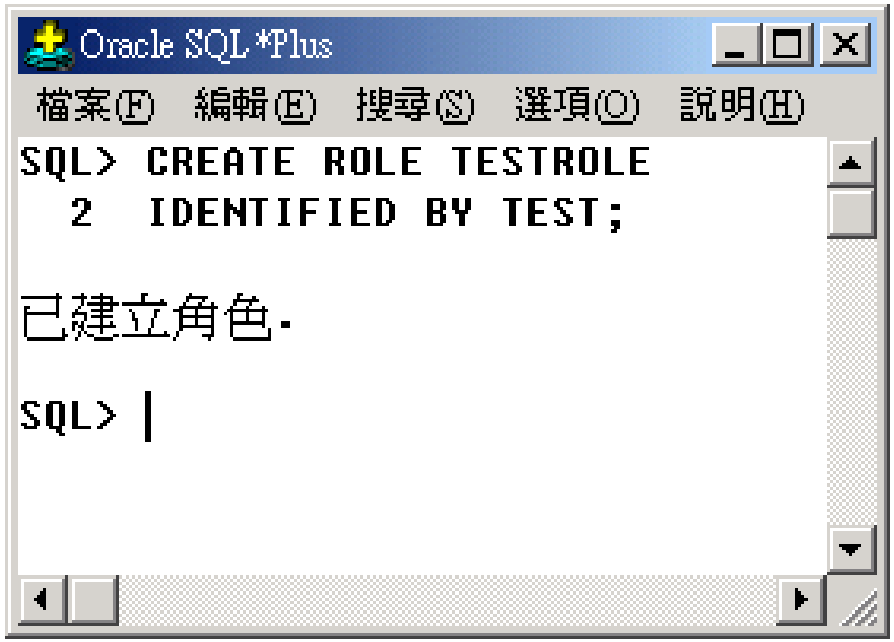
- 操作必須擁有 CREATE ROLE 系統權限，不然會出現權限不足的錯誤。語法如下：

```
CREATE ROLE <角色名>
    [IDENTIFIED BY <密碼>]
```

IDENTIFIED BY 密碼： 指定授予該角色的使用者，在使用 SET ROLE 指令時必須檢驗密碼。

建立角色的例子

- 建立新的角色 TESTROLE 並加上密碼確認



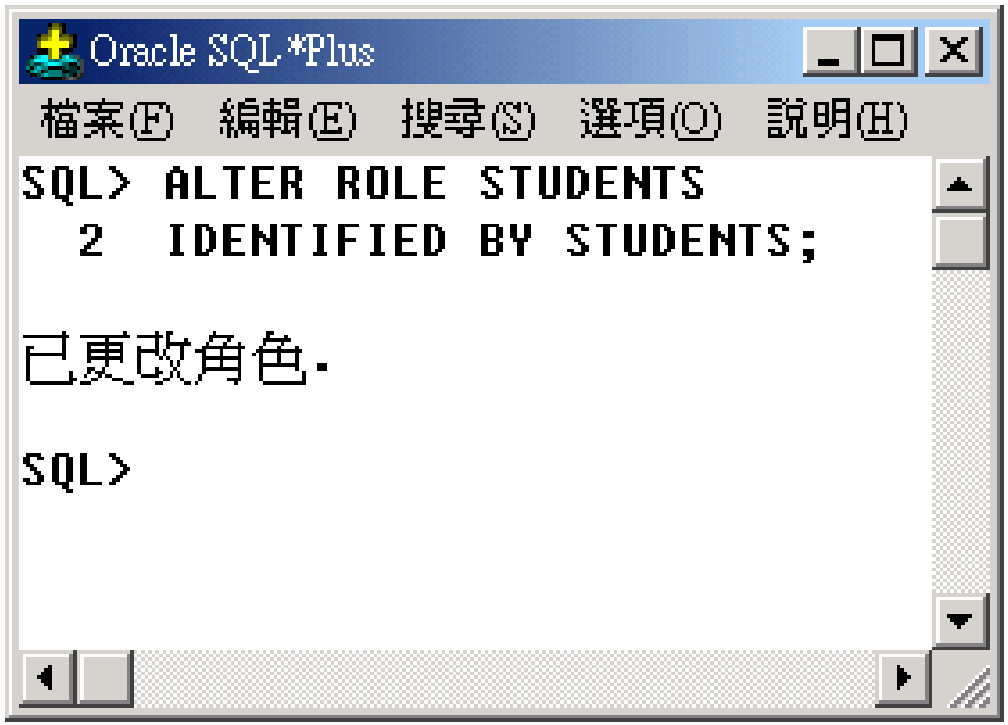
更改角色—ALTER ROLE

- 操作必須擁有 ALTER ROLE 系統權限，或在該角色上具有 ADMIN OPTION 的授權。語法如下：

ALTER ROLE <角色名> [IDENTIFIED BY <密碼>]

更改角色的例子

- 更改角色 STUDENTS 的密碼。



刪除角色—DROP ROLE

操作必須擁有 DROP ROLE 系統權限或在該角色上具有 ADMIN OPTION 的授權，語法如下：

DROP ROLE <角色名>

刪除角色的例子

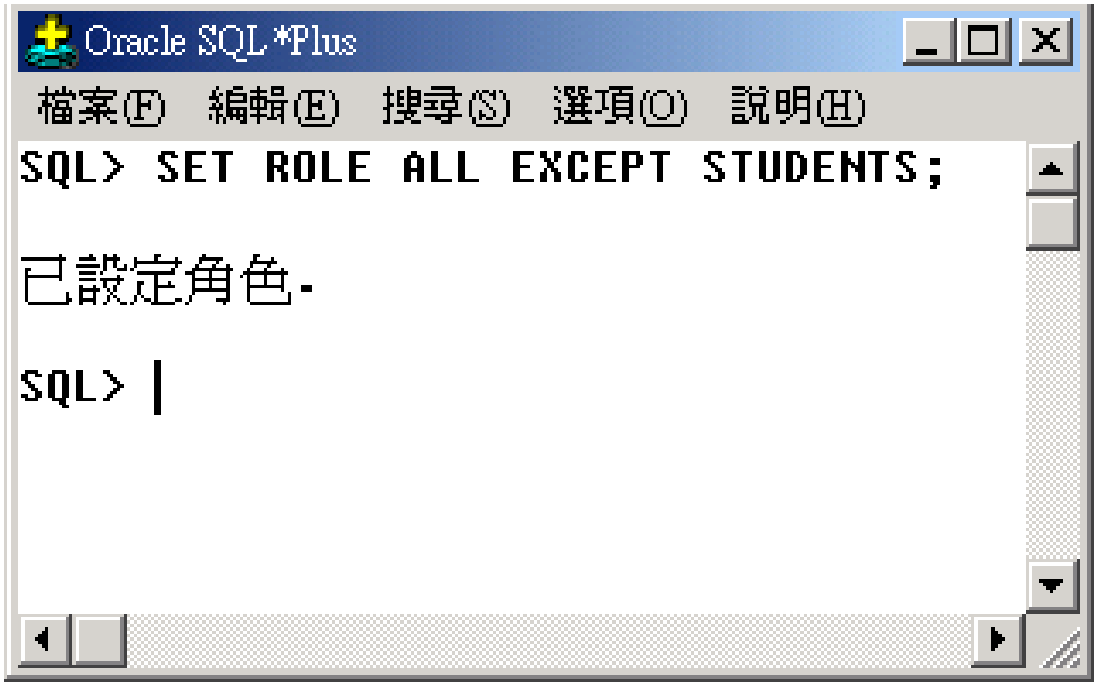
- 刪除角色 TESTROLE。

暫時讓使用者所擁有的角色有效(Enable) 或失效(Disable)—SET ROLE

- 有時候使用者在連線會談期間(**Session**)，希望將自己所擁有的某些角色暫時使之失效(**Disable**) 或有效(**Enable**)，以便使自己以某些特定的角色身份執行某些工作，語法如下：

```
SET ROLE {<角色名>｜ALL
          [EXCEPT <角色名>]｜NONE}
          [IDENTIFIED BY <密碼>]
```

- 恢復除了 STUDENTS 角色以外之使用者所有的角色。



授予系統權限或角色的指令

1. 系統權限或角色之授予 — GRANT
2. 回收系統權限或角色 — REVOKE

系統權限或角色之授予 — GRANT

- 其語法爲：

```
GRANT {<系統權限>| <角色>}[,
        {<系統權限>| <角色>}...]
TO {<使用者> | <角色>
[, {<使用者> | <角色>...}] | PUBLIC}
[ WITH ADMIN OPTION]
```

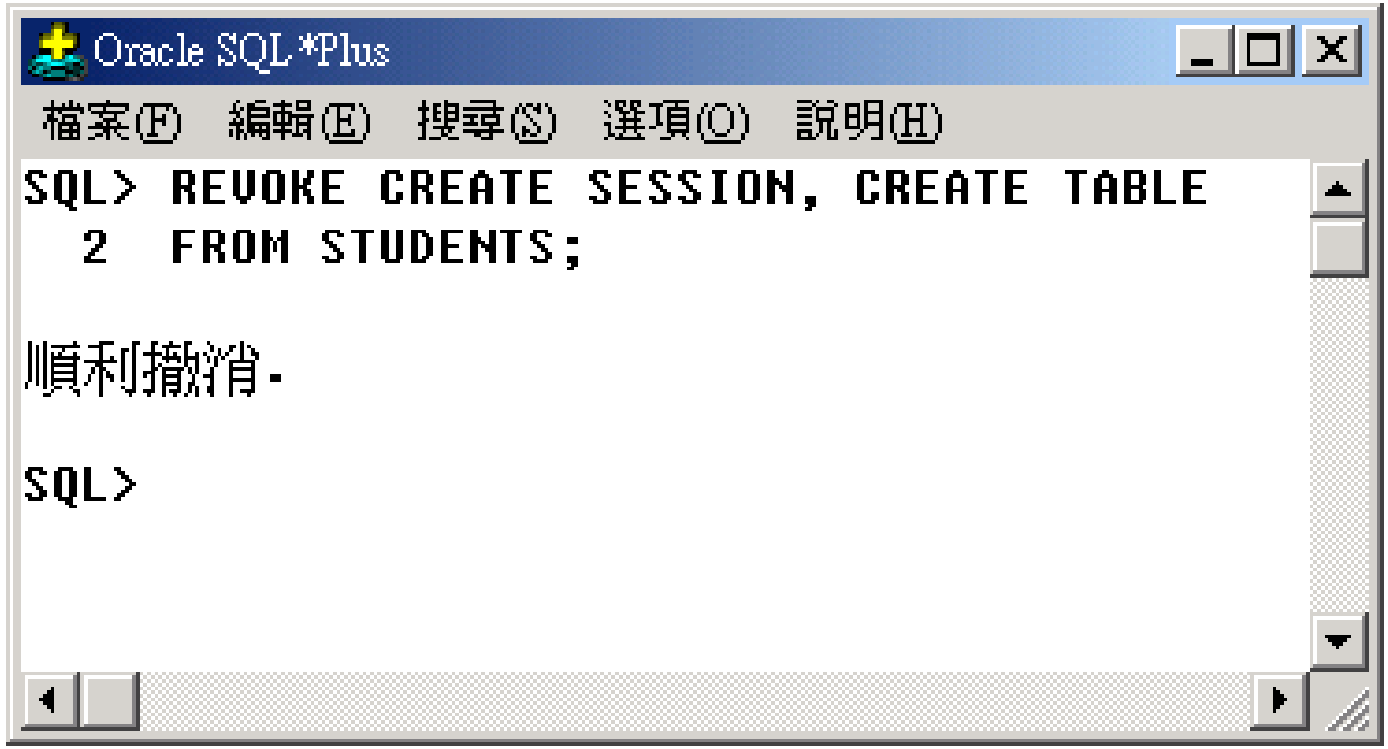
授權的例子


Oracle SQL*Plus
檔案(F) 編輯(E) 搜尋(S) 選項(O) 說明(H)
SQL> GRANT CREATE SESSION, CREATE TABLE TO STUDENTS;
順利授權.
SQL>

回收系統權限或角色 — REVOKE

```
REVOKE {<系統權限> | <角色>}
    [, {<系統權限> | <角色>}…]
 FROM {<使用者> | <角色>
    [, {<使用者> | <角色>…}] | PUBLIC}
```

回收權限的例子


Oracle SQL*Plus
檔案(F) 編輯(E) 搜尋(S) 選項(O) 說明(H)
SQL> REVOKE CREATE SESSION, CREATE TABLE
2 FROM STUDENTS;
順利撤消.
SQL>

物件權限的指令

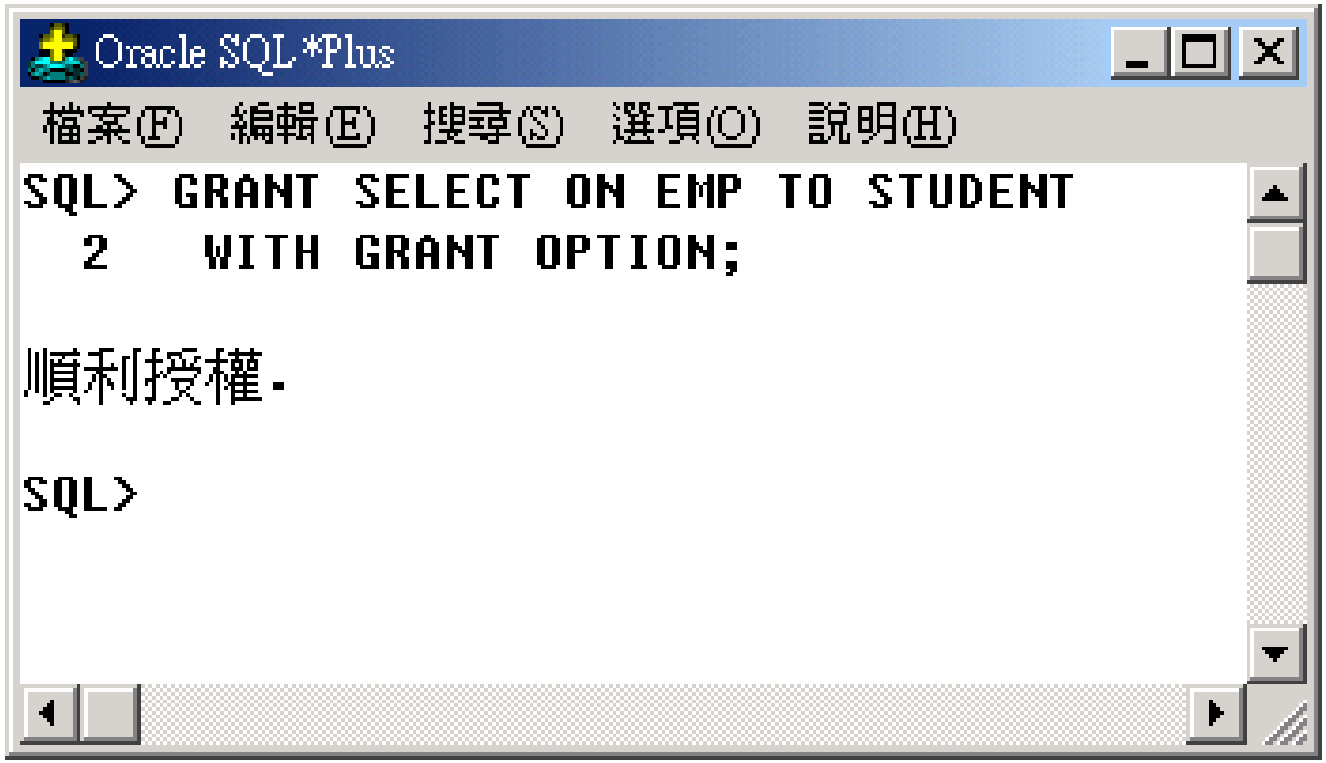
1. 授予物件權限指令－GRANT
2. 回收物件權限指令－REVOKE

授予物件權限指令－GRANT

- 操作者本身必須擁有該物件的權限並具備有 GRANT OPTION 權限。其語法為：

```
GRANT {<物件權限> [(<欄位列>[,<欄位列>]...)]
[,<物件權限> [(<欄位列>[,<欄位列>]...)]...] | ALL}
  ON <物件名>
  TO {<使用者> | <角色>
  [, {<使用者> | <角色>...}] | PUBLIC}
  [WITH GRANT OPTION]
```

授予物件權限的例子

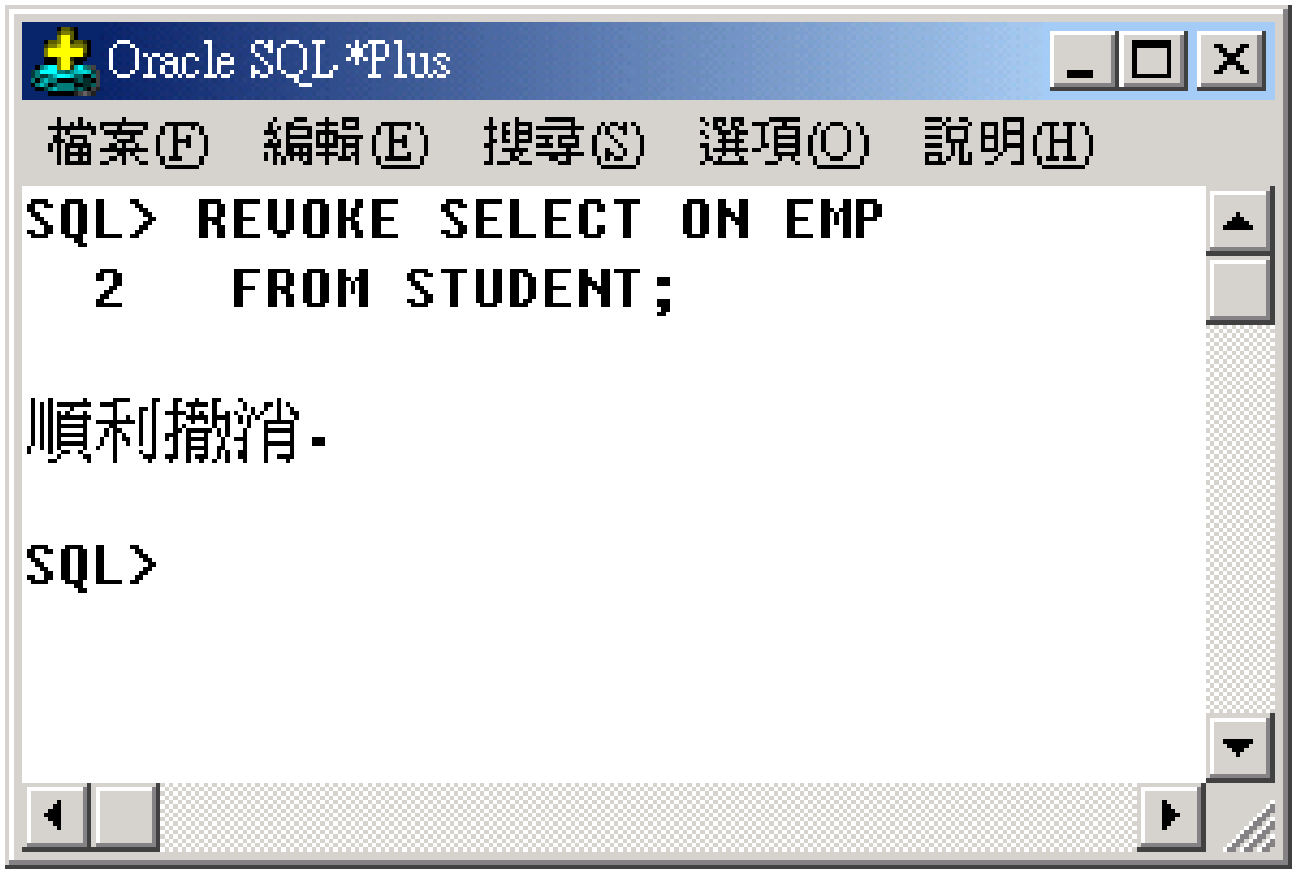

Oracle SQL*Plus
檔案(F) 編輯(E) 搜尋(S) 選項(O) 說明(H)
SQL> GRANT SELECT ON EMP TO STUDENT
2 WITH GRANT OPTION;
順利授權.
SQL>

回收物件權限指令－REVOKE

- 操作者必須曾將該物件權限授予某使用者或角色。其語法如下：

```
REVOKE {<物件權限> [, <物件權限>...] | ALL}
ON <物件名>
FROM {<使用者> | <角色>
  [, {<使用者> | <角色>...}] | PUBLIC}
[CASCADE  CONSTRAINT]
```

回收物件權限的例子


Oracle SQL*Plus
檔案(F) 編輯(E) 搜尋(S) 選項(O) 說明(H)
SQL> REVOKE SELECT ON EMP
2 FROM STUDENT;
順利撤消.
SQL>