Applied Faculty

Database 3

التحكم بوصول المستخدم
Controlling User Access

التحكم بوصول المستخدم

Controlling User Access

في بيئة متعددة المستخدمين لا بد من الحفاظ على أمن وسرية الدخول إلى البيانات واستخدامها ، ومع الأمن الخاص بقاعدة بيانات خادم أوراكل يمكنك القيام بما يلي :

- التحكم بالوصول إلى قاعدة البيانات .
- إعطاء ميزة الوصول إلى غرض معين من أغراض قاعدة البيانات.
- التأكد من إعطاء وتسلم أو تلقي الامتيازات عن طريق قاموس بيانات أوراكل .
- إنشاء رديف أو مرادف لأغراض قاعدة البيانات.

أمن قاعدة البيانات يمكن أن يصنف ضمن فئتين:

- ✓ أمن النظام system security .
- ✓ أمن البيانات data security .

أمن النظام : يشمل عملية الوصول واستخدام قاعدة البيانات على مستوى النظام مثل اسم المستخدم و كلمة المرور ، سعة القرص المخصصة للمستخدمين ، عمليات النظام المسموح بها من قبل المستخدم .

أمن البيانات : يشمل عملية الوصول واستخدام أغراض البيانات والأحداث التي يمكن لمستخدمين أن يؤثروا بها على هذا الغرض .

الامتيازات (السماحيات)Privileges:

- أمن قاعدة البيانات : (أمن النظام – أمن البيانات).
- امتيازات (سماحيات) النظام : الحصول على إذن للوصول إلى قاعدة البيانات .
- امتيازات الأغراض : يتعامل مع محتويات أغراض قاعدة البيانات .
- المخطط : مجموعة من الأغراض مثل الجداول والمناظير والمسلسلات .

الامتيازات : تمثل الحق بتنفيذ عبارات SQL خاصة ، حيث يقوم مدير قاعدة البيانات والذي يملك مستوى عالي من قابلية منح الامتيازات بمنح السماحيات للمستخدمين للوصول إلى قاعدة البيانات، كما يمكن أن يعطى المستخدمون امتياز منح سماحيات إضافية لمستخدمين آخرين .

امتيازات النظام System Privileges:

- أكثر من ٨٠ امتياز متاح للمستخدمين والوظائف .
- The DBA has high-level system privileges :
  ⇒ Create new users إنشاء مستخدمين .
  ⇒ Remove tables حذف الجداول .

⇒ Back up tables إنشاء نسخة احتياطية للجداول .

System Privilege	Operations Authorized العمليات المرخص بها
CREATE USER	هذا الامتياز من وظائف مدير قواعد البيانات DBA
DROP USER	إسقاط (حذف) مستخدم ثاني
DROP ANY TABLE	حذف جدول من أي خطة
BACKUP ANY TABLE	إنشاء نسخة احتياطية لأي جدول في أي خطة باستخدام التصدير

إنشاء مستخدمين Creating Users:

يقوم مدير قاعدة البيانات DBA بإنشاء المستخدمين باستخدام عبارة CREATE USER ، ولا يملك المستخدم أي امتيازات في المرحلة الحالية يقوم عندها المدير بمنح عدد من الامتيازات للمستخدم ، تحدد هذه الامتيازات ما الذي يمكن للمستخدم القيام به على مستوى قاعدة البيانات :

الصيغة العامة:

CREATE USER user

IDENTIFIED BY passwords ;

مثال : إنشاء المستخدم scott و كلمة المرور له tiger :

SQL> **CREATE USER** scott

IDENTIFIED BY tiger ;

حيث:

user اسم المستخدم

password كلمة سر الدخول

امتيازات النظام للمستخدم User System Privileges:

يمكن لمدير قاعدة البيانات DBA منح المستخدم امتيازات نظام محددة عندما يتم إنشاؤه كما يلي :

الصيغة العامة :

CRANT privilege **[** , privilege ….]

TO user [, user …] ;

مطور التطبيق يملك امتيازات النظام التالية:

- An application developer may have the following system privileges :
  ⇒ CREATE SESSION إنشاء جلسة
  ⇒ CREATE TABLE إنشاء جدول
  ⇒ CREATE SEQUENCE إنشاء مسلسل ضمن خطة المستخدم
  ⇒ CREATE VIEW إنشاء منظور ضمن خطة المستخدم
  ⇒ CREATE PROCEDURE إنشاء تابع أو إجراء مخزن أو حزمة ضمن خطة المستخدم

إنشاء ومنح امتيازات لوظيفة Creating and Granting Privileges to a Role

وظيفة أوراكل (Oracle Role) : هي مجموعة من الامتيازات أو نوع من أنواع الولوج إلى المعلومات التي يحتاجها المستخدم والتي تتعلق بالمسؤوليات والوظائف المتاحة له، وتحوي وظيفة مدير قاعدة المعطيات كل سماحيات وامتيازات النظام بما فيها إعطاء الامتيازات للآخرين .

كما يمكن إعطاء مجموعة امتيازات لوظيفة ثم منح هذه الوظيفة لمستخدم أو أكثر وبالتالي أي مستثمر يمكنه مباشرة إعطاء سماحيات أو امتيازات لمستثمر آخر.

ما هي الوظيفة؟ What is a Role:

- الوظيفة هي عبارة عن اسم لمجموعة امتيازات يمكن أن تمنح لمستخدم ، تجعل هذه الطريقة عملية منح وسحب الامتيازات أسهل في التنفيذ والإبقاء .
- يمكن أن يمتلك المستخدم الوصول إلى وظائف متعددة ، كما يمكن تخصيص نفس الوظيفة لعدد من المستخدمين ، ثم إنشاء الوظائف نموذجياً من أجل تطبيق قاعدة البيانات .

الصيغة العامة :

CREATE ROLE role ;

حيث:

role اسم الوظيفة المنشأة

مثال : إنشاء الوظيفة manager **:**

```
SQL> CREATE  ROLE   manager   ;
```

مثال : منح السماحيات للوظيفة manager **:**

```
SQL> GRANT  create table , create view
      TO        manager   ;
```

مثال : منح الوظيفة manager للمستخدمين BLAKE و CLARK**:**

```
SQL> GRANT  manager  to  BLAKE , CLEARK ;
```

تغيير كلمة السر Changing Your Password:

يمكننا تغيير كلمة المرور باستخدام عبارة ALTER USER

الصيغة العامة :

```
ALTER USER  user   IDENTIFIED  BY   passwords  ;
```

حيث:

user اسم المستخدم

password كلمة السر الجديدة

مثال : تغيير كلمة السر للمستخدم scott **:**

```
SQL> ALTER  USER  scott
      IDENTIFIED  BY  lion  ;
```

منح سماحيات النظام Granting System Privileges:

يمكن لمدير قاعدة المعطيات أن يقوم بمنح امتيازات محددة للمستخدم .

مثال : منح بعض امتيازات النظام للمستخدم scott **:**

```
SQL> GRANT   create table , create sequence , create view
      TO    scott   ;
```

امتيازات الأغراضObject Privileges:

- تتنوع امتيازات الغرض من غرض إلى آخر .
- المالك أو صاحب الغرض يملك جميع الامتيازات على الغرض التابع له .
- يستطيع المالك إعطاء سماحية معينة على غرض تابع له.

الصيغة العامة:

Grant *object_priv* **[(***columns***)]**

ON *object*

TO **{** *user*|*role*|PUBLIC **}**

[WITH GRANT OPTION] ;

حيث:

object_priv امتياز الغرض الممنوح

ALL تحدد كافة امتيازات الغرض

object **ON** اسم الغرض الممنوح وظيفة ما

TO يحدد المستخدم الذي منح إليه الامتياز

PUBLIC منح سماحيات الغرض لكافة المستخدمين

[WITH GRANT OPTION] يسمح هذا الخيار للشخص الممنوح بمنح امتيازات الغرض لمستخدمين أو وظائف آخرين .

Object Privileges - امتيازات الأغراض				
Object privilege	**Table**	**View**	**Sequence**	**Procedure**
ALTER	☒		☒	
DELETE	☒	☒		
EXECUTE				☒

INDEX	☒			
INSERT	☒	☒		
REFERENCES	☒			
SELECT	☒	☒	☒	
UPDATE	☒	☒		

مثال١ : منح امتيازات الاستفسار على الجدول EMP للمستخدمين sue و rich **:**

SQL> **GRANT select**

ON emp

TO sue , rich **;**

مثال٢ : منح الامتيازات لتحديث أعمدة معينة للمستخدم والوظيفة**:**

SQL> **GRANT update (dname , loc)**

ON dept

TO scott , manger **;**

حتى تقوم بمنح امتيازات على غرض ما يجب أن يكون هذا الغرض من ضمن الخطة Schema الخاصة بك أو أن تكون قد منحت الخيار WITH GRANT OPTION والذي يمنحك الحق بتمرير أو منح امتيازات الغرض لمستخدمين آخرين أو لوظائف أخرى .

مثال٣ : منح المستخدم الحق بتمرير الامتيازات باستخدام الخيار WITH GRANT OPTION **:**

SQL> **GRANT select , insert**

ON dept

TO scott

WITH GRANT OPTION **;**

مثال4 : السماح لكافة المستخدمين ضمن النظام بالاستفسار عن الجدول DEPT الخاص بالمستخدم Alice باستخدام الكلمة المفتاحية PUBLIC والتي تجعل مالك الجدول من منح حق الوصول للجدول لكافة المستخدمين **:**

```
SQL> GRANT    select
     ON       alice.dept
     TO       PUBLIC ;
```

بعض الجداول الخاصة بقاموس البيانات	
Data Dictionary Table	**Description- الوصف**
ROLE_SYS_PRIVS	يحوي امتيازات النظام الممنوحة للوظائف System privileges granted to roles -
ROLE_TAB_PRIVS	Table privileges granted to roles – يحوي امتيازات الجدول الممنوحة للوظائف
USER_ROLE_PRIVS	يحوي الوظائف التي يمكن الوصول إليها من قبل المستخدم Roles accessible by the user -
USER_TAB_PRIVS_MADE	يحوي سماحيات الغرض الممنوحة على أغراض المستخدم Object privileges granted on the user's objects
USER_ TAB _PRIVS_RECD	يحوي امتيازات الغرض الممنوحة للمستخدم Object privileges granted to the user-
USER_COL_PRIVS_MADE	يحوي سماحيات الغرض الممنوحة على أعمدة من غرض المستخدم Object privileges granted on the columns of the user's objects
USER_COL_PRIVS_RECD	يحوي سماحيات الغرض الممنوحة للمستخدم على أعمدة محددة Object privileges granted to the user on specific columns

سحب (إلغاء) امتيازات الغرض Revoking Object Privileges:

- نستخدم التعليمة REVOKE لسحب الامتيازات الممنوحة لمستخدمين آخرين .كما أن الامتيازات الممنوحة باستخدام الخيار WITH GRANT OPTION يتم سحبها أيضاً بنفس التعليمة .

الصيغة العامة

REVOKE { privilege [, privilege …]|ALL }

ON object

FROM { user [, user …]|role|PUBLIC }

[CASCADE CONSTRAINTS] ;

حيث: CASCADE CONSTRAINTS:هذا الخيار مطلوب لحذف أي قيود مرجعية منشأة للغرض بواسطة امتياز المراجع .

مثال : سحب الامتيازين Select و Insert على الجدول DEPT والممنوحين للمستخدم SCOTT :

```
SQL> REVOKE   select , insert
     ON       dept
     FROM     scott  ;
```

- إذا منح المستخدم امتياز ما مع الخيار WITH GRANT OPTION يستطيع عندها أن يمنح هذا الامتياز أيضاً، وعندها يمكن حدوث سلسلة طويلة من عملية منح الامتيازات لكن لا يسمح بعملية المنح بشكل دائري، وعند سحب المالك الامتياز الذي منحه لمستخدم تقوم تعليمة سحب الامتياز REVOKE بسحب كافة الامتيازات الممنوحة بناء على هذا الامتياز.

مثال : إذا قام مستخدم ما A بمنح امتياز الاستفسار SELECT إلى مستخدم ثاني B مع خيار المنح WITH GRANT OPTION يستطيع المستخدم B عندها أن يمنح هذا الامتياز مع خيار المنح WITH GRANT OPTION إلى مستخدم ثالث C وهكذا، وفي حالة قرر المستخدم A سحب هذا الامتياز من المستخدم B عندها يتم سحب الامتياز الممنوح إلى كل من المستخدمين B وC .