

Oracle Academic Initiative

Oracle9i Introduction to SQL



Oleh:

Tessy Badriyah, SKom.MT

**Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Surabaya**

BAB 14 : Pengontrolan Akses User

14.1. Sasaran

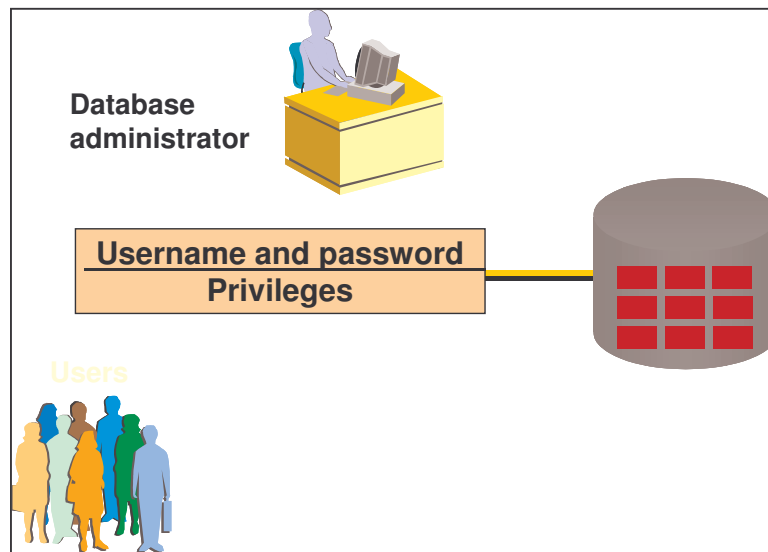
- Membuat User dan Privilege
- Pengaturan Role
- Penggunaan statement GRANT dan REVOKE untuk mengatur object privileges

14.2. Pengontrolan Akses User

Pada lingkungan dengan banyak user, perlu dipelihara keamanan data (security) untuk mengakses dan menggunakan database.

Dengan security dari Oracle Server maka kita bisa :

- Mengontrol akses database
- Memberikan akses terhadap object spesifik yang ada dalam database
- Mengkonfirmasi pemberian privilege (hak akses) dalam data dictionary
- Membuat synonym untuk object database



Database security dapat dikelompokkan menjadi 2 (dua) hal :

- System security
- Data security

System security meliputi akses dan penggunaan database pada level system, semisal username dan password, ruang disk yang dialokasikan ke user, dan operasi system yang diperbolehkan pada user. Database security meliputi akses dan penggunaan database object dan perlakuan yang bisa diberikan oleh user terhadap object dari database.

14.3. Privileges

- Privilege adalah hak atas sesuatu.
- System privilege adalah hak akses terhadap database
- Object privilege adalah hak untuk memanipulasi isi dari database object
- Schema (skema) adalah kumpulan object, semisal table, view dan sequence.

14.4. System Privileges

Ada lebih dari 100 privilege yang tersedia. DBA memiliki level privilege tertinggi yang bisa melakukan :

- Pembuatan user baru : CREATE USER

- Menghapus user : DROP USER
- Menghapus table : DROP ANY TABLE
- Membackup table : BACKUP ANY TABLE

14.5. Pembuatan User

Untuk membuat user baru digunakan perintah CREATE USER.

Sintak penulisan :

```
CREATE USER user
IDENTIFIED BY password;
```

Contoh penggunaan :

```
CREATE USER scott
IDENTIFIED BY tiger;
User created.
```

14.6. User System Privileges

Sekali user dibuat, maka DBA dapat memberikan system privilege yang spesifik terhadap user tersebut, yaitu :

- CREATE SESSION : untuk berhubungan dengan database
- CREATE TABLE : untuk membuat table dalam skema user
- CREATE SEQUENCE : untuk membuat sequence
- CREATE VIEW : untuk membuat view
- CREATE PROCEDURE : untuk membuat procedure

```
GRANT privilege [, privilege...]
TO user [, user/ role, PUBLIC...];
```

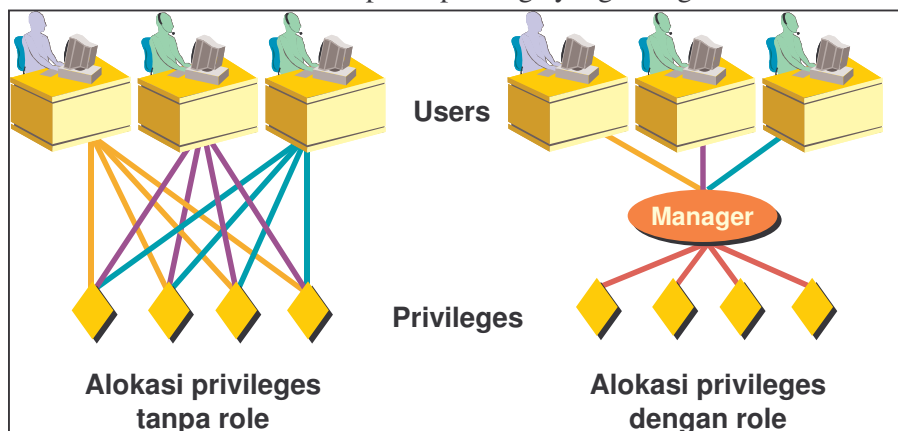
14.7. Granting System Privileges

DBA dapat memberi atau grant privilege system terhadap suatu user tertentu.

```
GRANT create session, create table,
create sequence, create view
TO scott;
Grant succeeded.
```

14.8. Apa itu Role ?

Role adalah nama dari sekumpulan privilege yang saling berelasi dan diberikan pada user.



Role dibuat untuk mempermudah proses pemberian dan pelepasan privilege. Hal pertama yang dikerjakan sehubungan dengan role adalah : pertama role dibuat dengan perintah CREATE ROLE *nama_role*. Kemudian DBA dapat menandai privilege apa saja yang diberikan kepada role. Setelah itu baru ditentukan user mana saja yang boleh memiliki role tersebut.

14.9. Pembuatan dan Granting Privileges sebuah Role

Membuat role :

```
CREATE ROLE manager;
Role created.
```

Grant privilege ke role :

```
GRANT create table, create view
TO manager;
Grant succeeded.
```

Grant role ke user :

```
GRANT manager TO DEHAAN, KOCHHAR;
Grant succeeded.
```

14.10. Merubah Password

Setiap user dapat merubah sendiri passwordnya dengan perintah ALTER USER.

```
ALTER USER scott
IDENTIFIED BY lion;
User altered.
```

14.11. Object Privileges

Object privilege adalah privilege yang sesuai untuk membentuk perlakuan terhadap object database. Tabel berikut menjelaskan ada tidaknya object privilege terhadap suatu object dalam database.

Object privilege	Table	View	Sequence	Procedure
ALTER	ada		Ada	
DELETE	ada	Ada		
EXECUTE				Ada
INDEX	Ada			
INSERT	ada	Ada		
REFERENCES	Ada			
SELECT	ada	ada	Ada	
UPDATE	ada	Ada		

Perintah untuk memberikan object privilege :

```
GRANT      object_priv [(columns)]
ON         object
TO         [user/role|PUBLIC]
[WITH GRANT OPTION];
```

14.12. Granting Object Privileges

Grant query privileges pada table EMPLOYEES :

```
GRANT select
ON employees
TO sue, rich;
Grant succeeded.
```

Grant privileges untuk mengubah kolom yang spesifik terhadap user dan role :

```
GRANT update (department_name, location_id)
ON departments
TO scott, manager;
Grant succeeded.
```

14.13. Penggunaan Keyword WITH GRANT OPTION dan PUBLIC

Dengan penambahan WITH GRANT OPTION pada saat memberikan suatu object privilege, maka akan membuat user yang diberi object privilege dapat memberikan hak yang diberikan atasnya itu kepada user yang lain.

Contoh penggunaan WITH GRANT OPTION :

```
GRANT select, insert
ON departments
TO scott
WITH GRANT OPTION;
Grant succeeded.
```

Jika pada saat pemberian suatu object privilege diberikan keyword PUBLIC, maka akan menyebabkan object privilege yang didefinisikan diberikan ke semua user yang ada dalam system.

Perintah berikut mengizinkan semua user pada system untuk melakukan query data dari table DEPARTMENTS yang menjadi kepunyaan Alice.

```
GRANT select
ON alice.departments
TO PUBLIC;
Grant succeeded.
```

14.14. Memeriksa Keberadaan Privilege

Untuk memeriksa keberadaan dari privilege, dapat dilihat pada data dictionary berikut :

Data dictionary	Keterangan
ROLE_SYS_PRIVS	System privilege yang diberikan pada role
ROLE_TAB_PRIVS	Table privilege yang diberikan pada role
USER_ROLE_PRIVS	Role yang bisa diakses oleh user
USER_TAB_PRIVS_MADE	Object privilege yang diberikan pada objectnya user
USER_TAB_PRIVS_RECD	Object privilege yang diberikan pada user
USER_COL_PRIVS_MADE	Object privilege atas kolom yang dimiliki user
USER_COL_PRIVS_RECD	Object priv. Yang diberikan pada user pada kolom yg spesifik.

14.15. Menghapus Object Privileges

Untuk menghapus privilege, digunakan perintah REVOKE. Dengan perintah REVOKE, privilege yang diberikan ke user yang lain melalui WITH GRANT OPTION juga akan dihapus.

Sintak umum dari REVOKE :

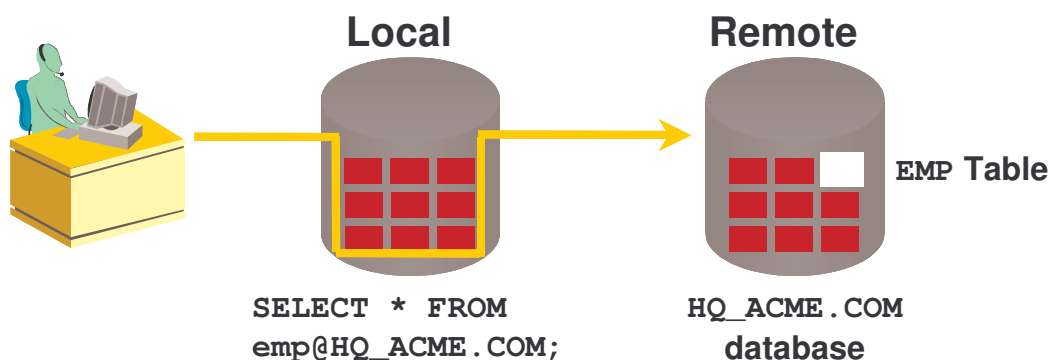
```
REVOKE      {privilege }, privilege ...]|ALL}
ON          object
FROM {user[, user ...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

Misal sebagai user, Alice menghapus privilege SELECT dan INSERT yang diberikan untuk user Scott pada table DEPARTMENTS.

```
REVOKE select, insert
ON departments
FROM scott;
Revoke succeeded.
```

14.16. Database Link

Koneksi database link memungkinkan local user untuk mengakses data pada remote database.



Untuk membuat database link :

```
CREATE PUBLIC DATABASE LINK hq.acme.com
USING 'sales';
Database link created.
```

Menulis SQL Statement yang menggunakan database link :

```
SELECT *
FROM emp@HQ.ACME.COM;
```