DATABASE ADMINISTRATION

Pertemuan ke-8

Database Security

source :
Database Administration
the complete guide to practices and procedures
chapter 14
by. Craig S. Mullins

pengantar

- Semua resource database dikontrol oleh DBMS
- Agar user dapat menggunakan seluruh fungsi DBMS kondisi di bawah harus ada
  - User diberikan hak untuk mengakses fungsi tersebut
  - Atau fungsi tersebut diberikan hak untuk diakses seluruh user
- Seluruh fungsi dalam sebuah organisasi harus ditentukan level autorized nya, contoh hanya programmer general-ledger dan batch jobs yang dapat mengakses dan modifikasi database general ledger
- Meski DBA memiliki tanggungjawab administrasi security db, beberapa organisasi mempunyai administrasi keamanan yang mengontrol seluruh keamanan IT
- Ketika sebuah administrator security grup ada, biasanya grup ini menggunakan third-party security software seperti IBM's RACF or Computer Associates ACF2 and Top Secret

Database Security Basics

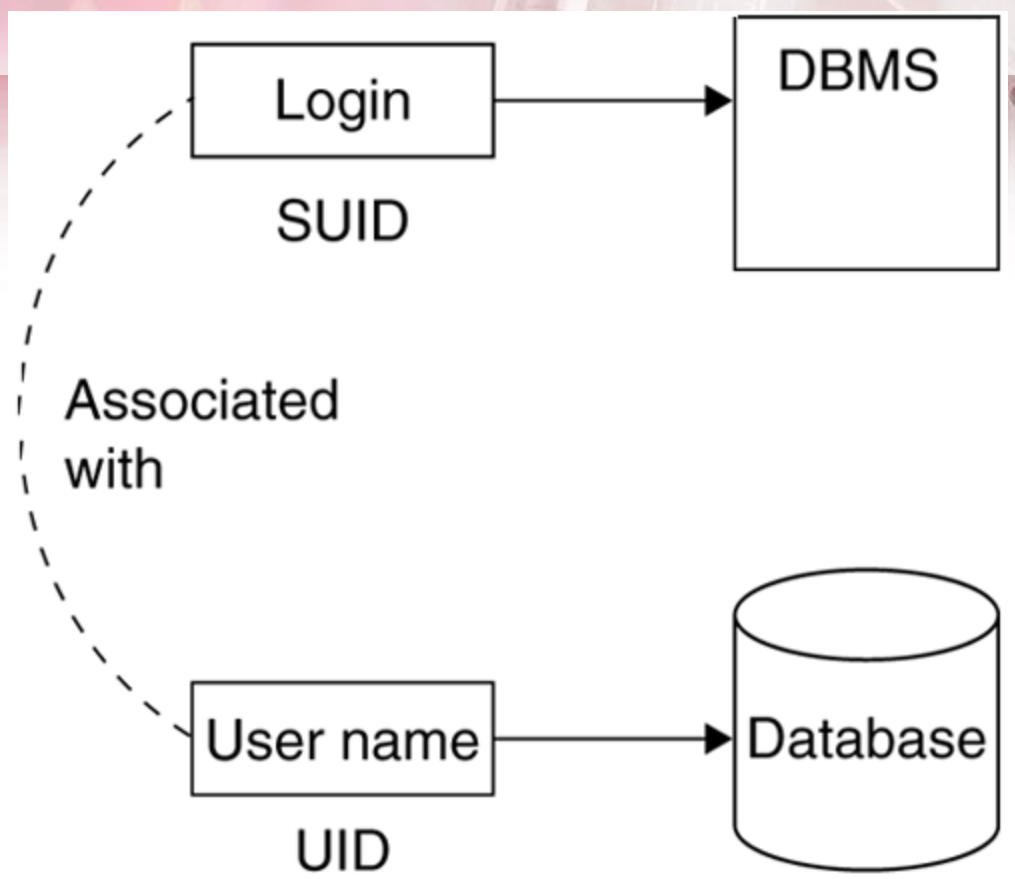
- Authentikasi yang kuat adalah batu pertama dari seluruh rencana implementasi sekuritas
- Ketika DBMS melakukan penambahan login, DBA perlu beberapa info terkait login yang dibuat, umumnya selain loginName atau ID, beberapa info dibawah perlu ditambahkan
  - **Password**— the key phrase, word, or character string associated with the new login that must be provided by the user before access to the database is permitted.
  - **Default database**— the name of the database to which the user will initially be connected during login.
  - **Default language**— the default language assigned to the login when using the DBMS if multiple languages are supported.
  - **Name**— the actual full name of the user associated with this login.
  - **Additional details**— additional details about the user for which the login has been created: e-mail, phone number, office location, business unit, and so on. This is useful for documentation purposes.

- Password harus rutin diganti untuk mempersulit hacker untuk menjebol sekuritas
- DBA dapat melakukan otomatisasi prosedur (misal mengirim emal notifikasi password) untuk mengingatkan user rutin mengganti password tiap bulan
- Ada beberapa DBMS yang memiliki fungsi otomatis (default) mengirimkan notiftikasi rutin terkait pergantian password
- Jika seorang user DBMS sudah keluar dari perusahaan atau tidak memiliki hak mengakses DBMS, maka DBA harus segera menghapus login dari sistem secepatnya
- User yang dapat membuat database objek harus dibatasi pada DBA saja

Password Guidance

- **Avoid passwords that are too short**. Each password should be at least six characters long, more if possible.
- **Each password should consist of at least a combination of alphabetic characters and numeric characters**. Using other allowable symbols makes the password harder to guess.
- **Avoid creating a password that is a complete word** (in either the native language of the user or any foreign language).
- **Do not embed personal statistics in the password**. Street addresses, social security numbers, phone numbers, and the like are easily guessed and do not belong in passwords.
- **Consider concatenating two unrelated words with a symbol or number between them**. For example, "toe3star" is a viable password.
- **Use mnemonic devices to help you remember passwords**

Figure 14-1. DBMS and database logins



Granting and Revoking Authority

- DBA melakukan kontrol DB sekuriti dan authorisasi dengan Data Control Language atau DCL, salah satu dari subtipe SQL (selain DDL dan DML)
- DCL statemen memiliki dua dasar : GRANT dan REVOKE.
- Hindari penggunaan Grand dan Revoke statement dalam program aplikasi, hanya gunakan lewat DBMS manager

Beberapa tipe privilige yang didukung modern DBMS antara lain

- Table: untuk melakukan kontrol siapa yang bisa mengases dan modifikasi table
- Database object: untuk melakukan kontrol siapa yang dapat membuat database baru atau menghapus objek database
- System: untuk mengkontrol siapa saja yang dapat melakukan beberapa aktifitas level sistem
- Program: untuk melakukan kontrol siapa yang bisa menambah, modifikasi dan menggunakan database program
- Stored procedure: untuk melakukan kontrol siapa saja yang dapat melakukan eksekusi pada fungsi tertentu ada store prosedur tertentu

- **Table privilage**
  - For example, to enable user7 to delete rows from the Titles table, the following statement can be issued:

    GRANT DELETE on Titles to user7;
- **Database object**
  - For example, to enable user5 and user9 to create tables and indexes, the following statement can be issued:

    GRANT CREATE table,
    CREATE index
    TO user5,
    user9;

Revoking Privileges

- Revoke statement digunakan untuk menghapus privilege dari yang sebelumnya sudah diset. Sintak dari Revok kebalikan dari GRANT sintak
- Umumnya semua privilege akan dihapus ketika objek database dihapus
- Contoh untuk revoke the ability to update the au_id column of the titles table from user7

  REVOKE UPDATE on titles (au_id) from user7;

Authorization Roles and Groups

- Untuk lebih memudahkan dalam grant privilege pada user individu, DBMS menyediakan kemampuan untuk menambahkan
  - Specific privileges to a role, which is then granted to others
  - Specific built-in groups of privileges to users

Roles

- Sekali didefinisikan, sebuah Roles dapat digunakan untuk grant satu atau lebih privilege user
- Role adalah koleksi dari privilege yang esensial, DBA dapat membuat role dan menetapkan privilege tertentu pada Role tsb

```
CREATE role MANAGER;
COMMIT;
GRANT select, insert, update, delete on employee to MANAGER;
GRANT select, insert, update, delete on job_title to MANAGER;
GRANT execute on payroll to MANAGER;
COMMIT;
GRANT MANAGER to user1
COMMIT;
```

Groups

- Group-level authority mirip dengan roles. Setiap DBMS memiliki built-in group yang tidak dapat diganti. Setiap DBMS memiliki beberapa grup level dengan nama berbeda dan dengan cara berbeda, meski secara umum sama :

- **System administrator**. Biasa disebut SA atau SYSADM : user paling powerfull di DBMS. User dengan level SA dapat mengeksekusi ***semua perintah DBMS pada seluruh DB***

- **Database administrator**.biasa disebut DBADM atau DBA, dba memiliki ***seluruh privilige perintah pada database tertentu*** Sometimes abbreviated as DBADM or DBA, the database, kemampuan untuk mengakses data pada table, termasuk drop objek pada database

- **Database maintenance**.biasa disebut DBMAINT memiliki privilage untuk maintening DB objek (misal untuk run utility) seperti DBA biasanya hanya memiliki hak pada DB tertentu
- **Security administrator**. Memiliki hak untuk granting dan revoke sekuritas beberapa DB. Nama lain untuk administrator sekuriti adalah SSO
- **Operations control**. Biasa disebut OPER atauSYSOPR, the operations control role memiliki otorasi untuk melakukan task operasi database seperti backup dan recovery atau terminating task

Other Database Security Mechanisms

Modern relational DBMS support beberap kemampuan dan kualitas tambahan untuk sekurtias data. Meski bukan fungsi utama, seperti contoh views dan stored procedures dapat digunakan, meski sekuriti bukan fungsi utama mereka

- **Using Views for Security :** ada dua tipe
- **Vertical restriction** using views is an alternative to specifying columns when granting table privileges. It also can be easier to implement and administer.
- **horizontal restriction** Views can also be used to provide row-level security based on the content of data. implemented by coding the appropriate WHERE clauses into the view.

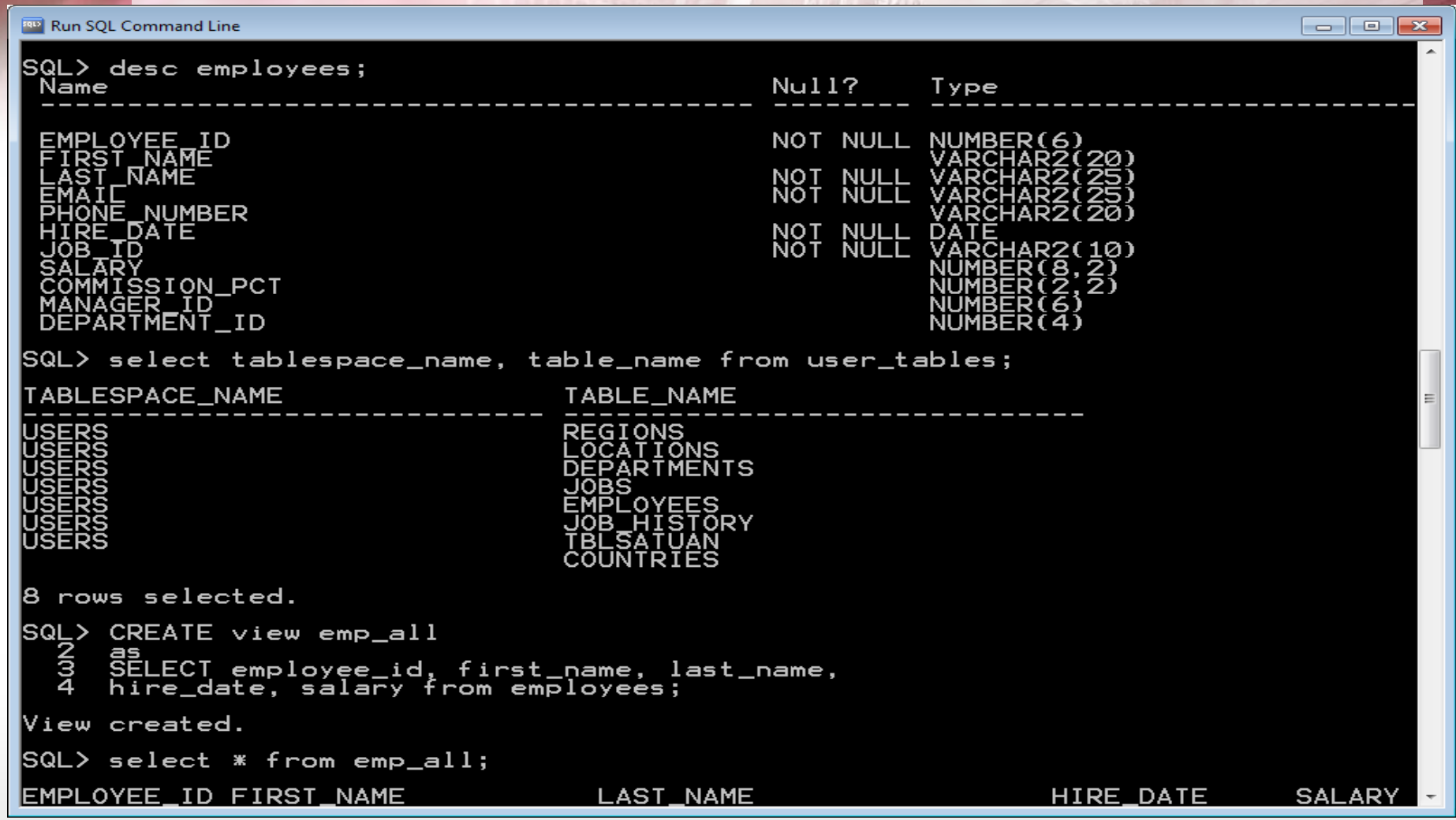
- Contoh horisontal restriction

```
CREATE view emp_all
AS
SELECT first_name, last_name, middle_initial,
street_address, state, zip_code
FROM employee;
```

- Contoh vertikal restriction

```
CREATE view emp_dept20
AS
SELECT first_name, last_name, middle_initial,
street_address, state, zip_code
FROM employee
WHERE deptno = 20;
```

Hasil create view



Auditing

- Auditing adalah fasilitas DBMS yang memungkinkan DBA untuk track penggunaan resource DB dan privilige. Ketika auditing di aktifkan, DBMS akan menghasilkan audit trail dari setiap operasi DB
- Auditing juga dapat digunakan sebagai data recovery.
- Setiap DBMS memiliki perbedaan kemampuan auditing, secara umum fasilitas auditing tersebut antara lain :

- Login and logoff attempts (both successful and unsuccessful)
- Database server restarts
- Commands issued by users with system administrator privileges
- Attempted integrity violations (where changed or inserted data does not match a referential, unique, or check constraint)
- SELECT, INSERT, UPDATE, and DELETE operations
- Stored procedure executions
- Unsuccessful attempts to access a database or a table (authorization failures)
- Changes to system catalog tables
- Row-level operations

External Security

- Fokus pada data set dan file yang digunakan oleh DBMS
- Enkripsi data adalah teknik encode data menjadi data acak, membuat data tidak dapat dibaca tanpa encripsi key

- **Job Scheduling and Security**

  schedulling biasanya menggunakan third party job scheduller seperti : CA-7, Control-M, or AutoSys
- **Non-DBMS DBA Security**
- Contoh root pada security di linux

Summary

- Database sekuriti adalah komponen penting dalam tugas DBA
- Tanpa rencana sekuritu yang komperhensif, integritas database organisasi akan dipertanyakan
- Setiap DBA harus mempelajari mekanisme sekuritas agar dipastikan hanya user yang mebutuhkan saja yang dapat mengakses fungsi pada database tertentu

Terima kasih