

11

Keamanan Database Oracle

By: Ahmad Syauqi Ahsan

ORACLE®

Tujuan

Setelah menyelesaikan bab ini, Anda seharusnya dapat melakukan hal-hal berikut:

- Menerapkan keutamaan tentang hak akses
- Mengatur user yang ada
- Menerapkan fungsi keamanan standard password
- Mengaudit aktivitas database

KEAMANAN DATABASE

Sistem yang aman memastikan kerahasiaan data yang terdapat didalamnya.

Beberapa aspek keamanan yaitu:

- Membatasi akses ke data dan service
- Melakukan autentifikasi pada User
- Memonitor aktifitas-aktifitas yang mencurigakan

Menerapkan Prinsip Hak Minimum

- Melindungi data dictionary
- Mengambil hak akses yang tidak diperlukan dari PUBLIC
- Membatasi directory-directory pada sistem operasi yang dapat diakses oleh user
- Membatasi jumlah user dengan hak akses administrator
- Membatasi autentikasi user pada database secara remote

Melindungi Data Dictionary

- Melindungi data dictionary dengan memastikan parameter inisialisasi berikut di set FALSE
`O7_DICTIONARY_ACCESSIBILITY = FALSE;`
- Konfigurasi ini mencegah user dengan ANY TABLE system privilege mengakses tabel dasar dari data dictionary
- Nilai FALSE konfigurasi juga mencegah user SYS dari logging selain SYSDBA
- Nilai default dari parameter ini adalah FALSE. Jika nilai parameter ini di set TRUE, maka harus ada alasan yang benar-benar sesuai

Menolak Hak Akses dari Luar yang Tidak Diperlukan

- Menolak semua hak akses yang tidak perlu dan role – role dari database server dengan group PUBLIC
- Banyak paket yang terintegrasi di grant EXECUTE ke hak akses PUBLIC
- Mengeksekusi paket-paket berikut yang harus di tolak dari PUBLIC antara lain :
 - UTL_SMTP
 - UTL_TCP
 - UTL_HTTP

MENOLAK HAK AKSES DARI LUAR YANG TIDAK PERLU

- UTL_FILE
- DBMS_OBFUSCATION_TOOLKIT
- Banyak paket yang terintegrasi di grant EXECUTE ke hak akses PUBLIC
 - Contoh:
 - SQL> REVOKE execute ON utl_file FROM PUBLIC;

Membatasi User dengan Role DBA

Menolak model hak akses seperti berikut ini :

- Memberikan hak akses system dan object secara penuh
- Koneksi hak akses SYS, SYSDBA dan SYSOPER
- Hak akses model DBA antara lain MENGHAPUS SEMUA TABLE
- Hak akses Run-Time

```
SQL> SELECT grantee FROM dba_role_privs
      2 WHERE granted_role = 'DBA';
GRANTEE
-----
SYS
SYSTEM
```


Mematikan Semua Fungsi Autentifikasi Secara Remote

- Autentifikasi secara remote harus hanya digunakan ketika Anda memberikan kepercayaan kepada client dengan autentifikasi sewajarnya
- Proses autentifikasi remote :
 - user mengakses database dari luar
 - remote autentifikasi dilakukan oleh user
 - user masuk ke database
- Untuk mematikan, yakinkan bahwa instance diinisialisasi parameter dengan setting default :

```
REMOTE_OS_AUTHENT = FALSE
```

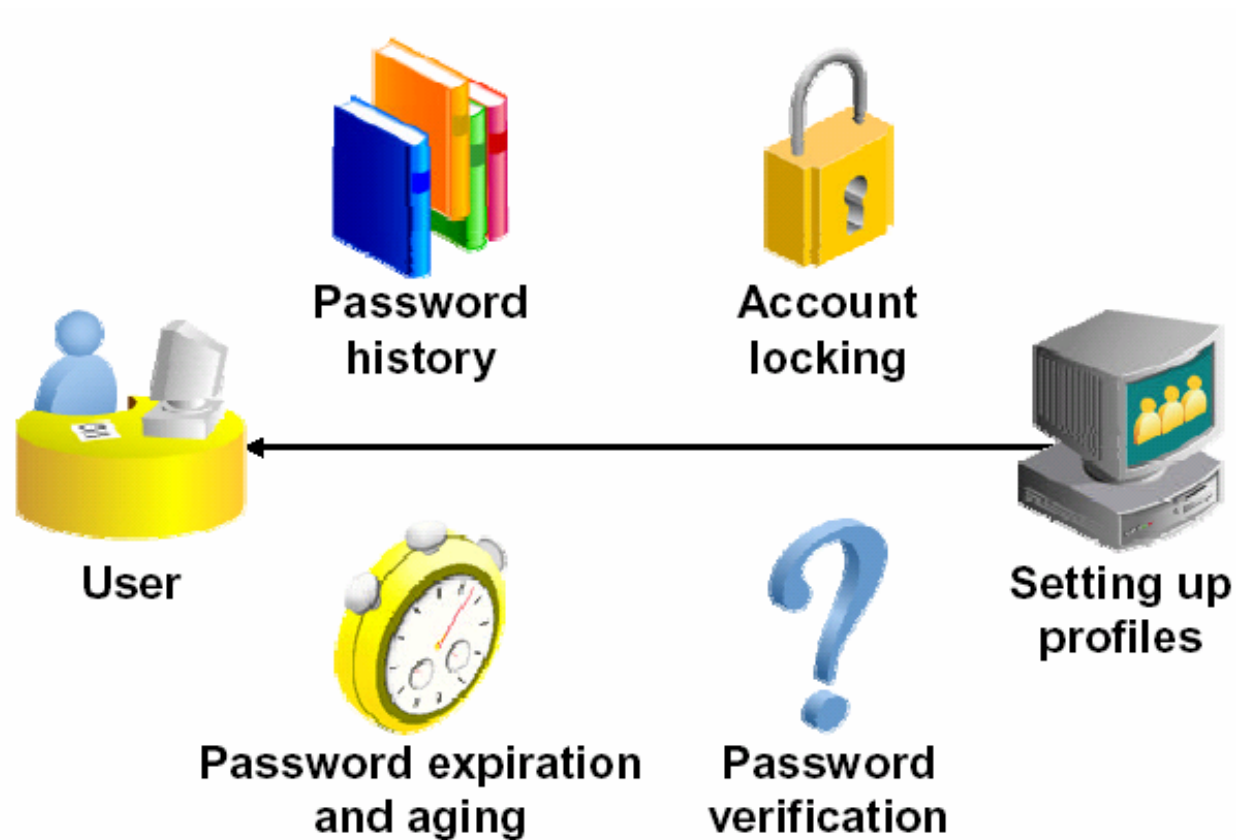
Mengelola User Account Standart

- DBCA membatasi dan mengunci semua account, kecuali :
 - SYS, SYSTEM, SYSMAN, DBSNMP
- Untuk membuat database secara manual, kunci dan batasi account yang tidak digunakan

The screenshot shows the 'Edit User: CTXSYS' dialog box with the following details:

- Title:** Edit User: CTXSYS
- Buttons:** Show SQL, Revert, Apply
- Tabs:** General (selected), Roles, System Privileges, Object Privileges, Quotas
- Name:** CTXSYS
- Profile:** DEFAULT
- Authentication:** Password
- * Enter Password:** [Masked]
- * Confirm Password:** [Masked]
- Password Status:** Expired
Enter and confirm a password to un-expire the password
- * Default Tablespace:** SYSAUX
- Temporary Tablespace:** TEMP
- Status:** ☒ Locked ☐ Unlocked

Implementasi Fitur-fitur Keamanan Password Standart



Mengunci Password Account

PARAMETER

FAILED_LOGIN_ATTEMPTS

PASSWORD_LOCK_TIME

KETERANGAN

Jumlah dari login yang salah sebelum account dikunci

Jumlah hari dari account yang dikunci sesudah jumlah dari user yang salah login

Password Expiration and Aging

PARAMETER	KETERANGAN
PASSWORD_LIFE_TIME	Lifetime dari password sesudah password expires
PASSWORD_GRACE_TIME	Waktu dalam hari untuk merubah password sesudah sukses login pertama sesudah password expires

Password History

PARAMETER	KETERANGAN
PASSWORD_REUSE_TIME	Lifetime dari password sesudah password expires
PASSWORD_REUSE_MAX	Jumlah password memerlukan perubahan sebelum password yang sekarang dapat digunakan kembali

Memberikan Fungsi Verifikasi Password: **VERIFY_FUNCTION**

Untuk memberikan fungsi password verifikasi lakukan kebutuhan password antara lain :

- panjang minimum adalah 4 karakter
- password tidak boleh sama dengan username
- password harus memiliki sedikitnya satu huruf, satu angka, dan satu huruf khusus
- password harus berbeda dari password sebelumnya sedikitnya 3 huruf


Membuat Profile untuk Password


Create Profile

Show SQL Cancel OK


General **Password**


Password

Expire in (days) 90 


Lock (days past expiration) 10 

History


Number of passwords to keep UNLIMITED 


Number of days to keep for 120 

Complexity

Complexity function VERIFY_FUNCTION 

Failed Login

Number of failed login attempts to lock after 3 

Number of days to lock for 5/1440 

Memasukkan User ke dalam Profile untuk Password

Edit User: NGREENBERG

Show SQL Revert Apply

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

Name **NGREENBERG**

Profile **CUSTOMPROFILE** ▼


Authentication Password ▼

* Enter Password

* Confirm Password

☐ Expire Password now

* Default Tablespace 

Temporary Tablespace 

Status ☐ Locked ☒ Unlocked

Mengawasi Aktivitas yang Mencurigakan

Mengawasi atau mengaudit harus menyatu dengan prosedur keamanan.

Tool-tool yang diaudit dalam database Oracle antara lain:

- Database Auditing
- Value Base Auditing
- Fine-Granted Auditing (FGA)

Perbandingan Tool-tool untuk Auditing

MODEL AUDIT

Standart Database

Value Base

Fine-Grained

OBYEK YANG DIAUDIT

Hak akses terhadap object

Merubah data melalui DML

Perintah SQL

**(insert,update,delete dan
select) berdasarkan isi**

Standart Database Auditing

Diaktifkan melalui parameter AUDIT_TRAIL

- NONE : mematikan kumpulan history dari audit
- DB : mengaktifkan audit dari data yang ada di database
- OS : mengaktifkan audit dari OS

Yang dapat di audit yaitu :

- Event Login
- Hak Akses System
- Hak Akses Object

Option Audit

- **SQL statement auditing**

```
AUDIT table;
```

- **System privilege auditing (nonfocused and focused)**

```
AUDIT select any table, create any trigger;  
AUDIT select any table BY hr BY SESSION;
```

- **Object privilege auditing (nonfocused and focused)**

```
AUDIT ALL on hr.employees;  
AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

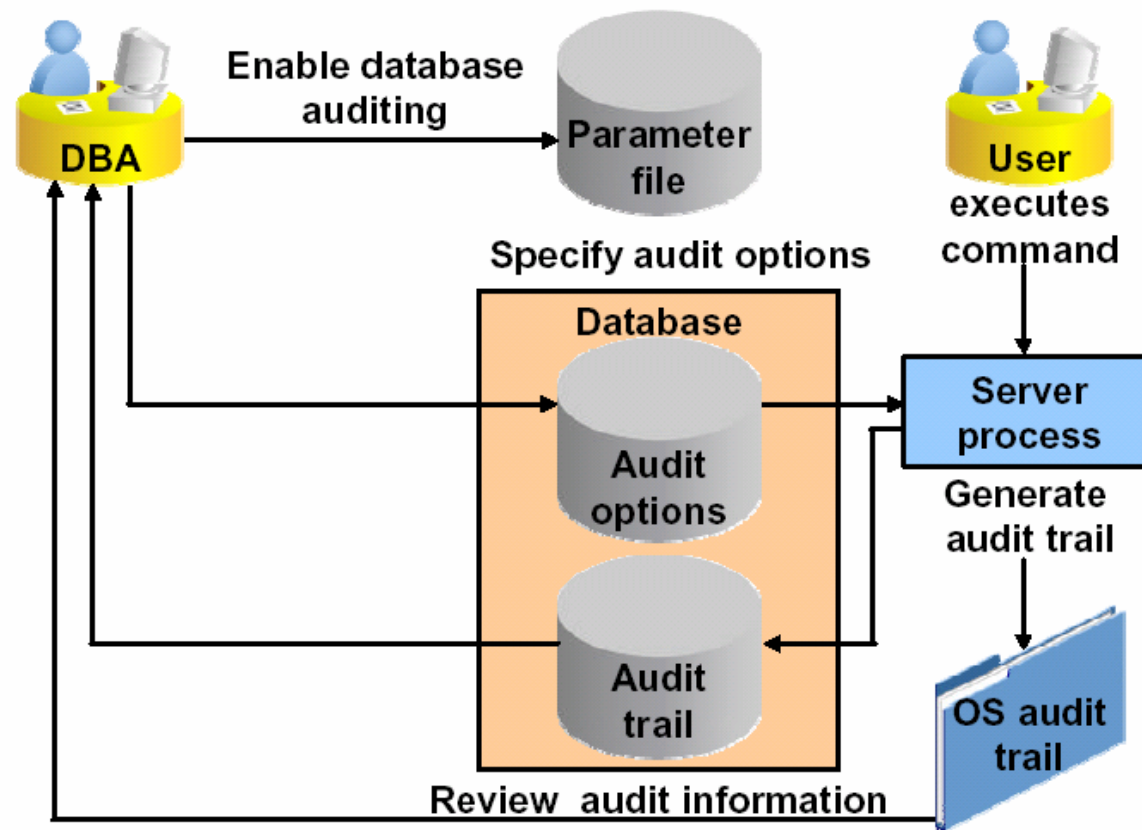
- **Session auditing**

```
AUDIT session whenever not successful;
```

Melihat Option Audit

DATA DICTIONARY	KETERANGAN
ALL_DEF_AUDIT_OPTS	Default pilihan audit
DBA_STMT_AUDIT_OPTS	Statement audit
DBA_PRIV_AUDIT_OPTS	Hak akses audit
DBA_STMT_AUDIT_OPTS	Schema object audit

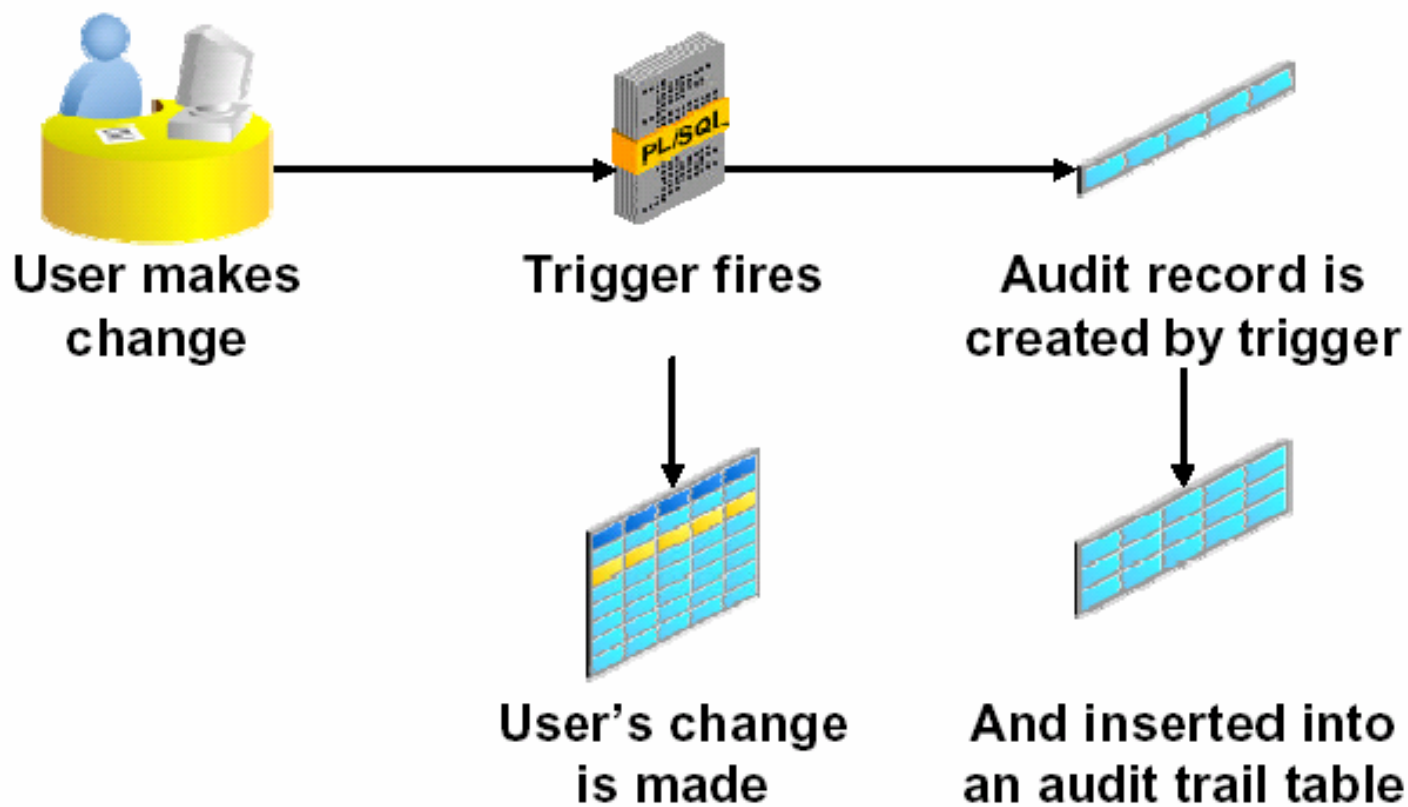
Standart Database Audit



Melihat Hasil Audit

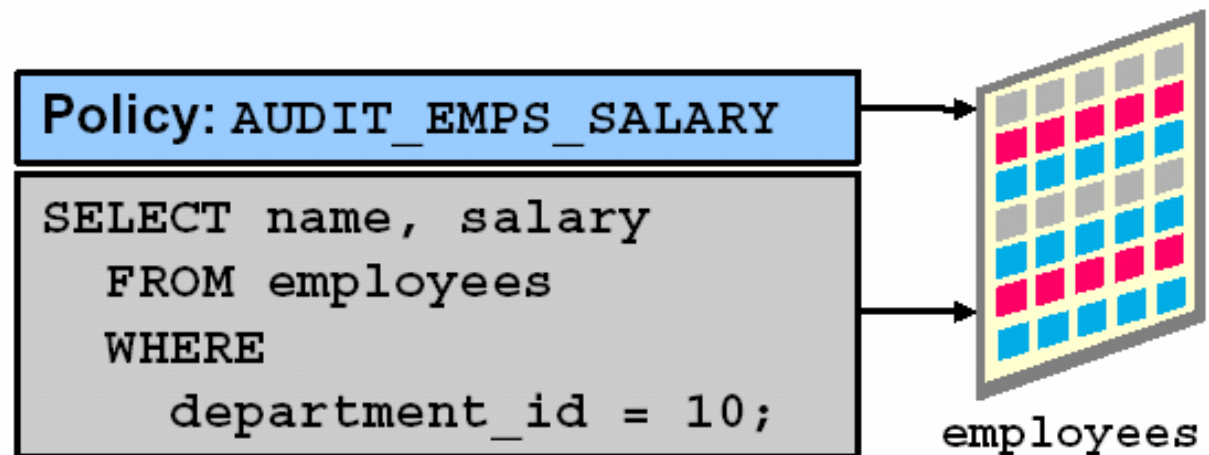
AUDIT	KETERANGAN
DBA_AUDIT_TRAIL	Semua audit yang dimasukkan
DBA_AUDIT_EXISTS	Daftar audit yang ada dan tidak ada
DBA_AUDIT_OBJECT	Daftar schema object
DBA_AUDIT_SESSION	Semua audit yang terhubung dan tidak terhubung
DBA_AUDIT_SESSION	Daftar semua audit

Value Based Auditing



Fine-Grained Auditing (FGA)

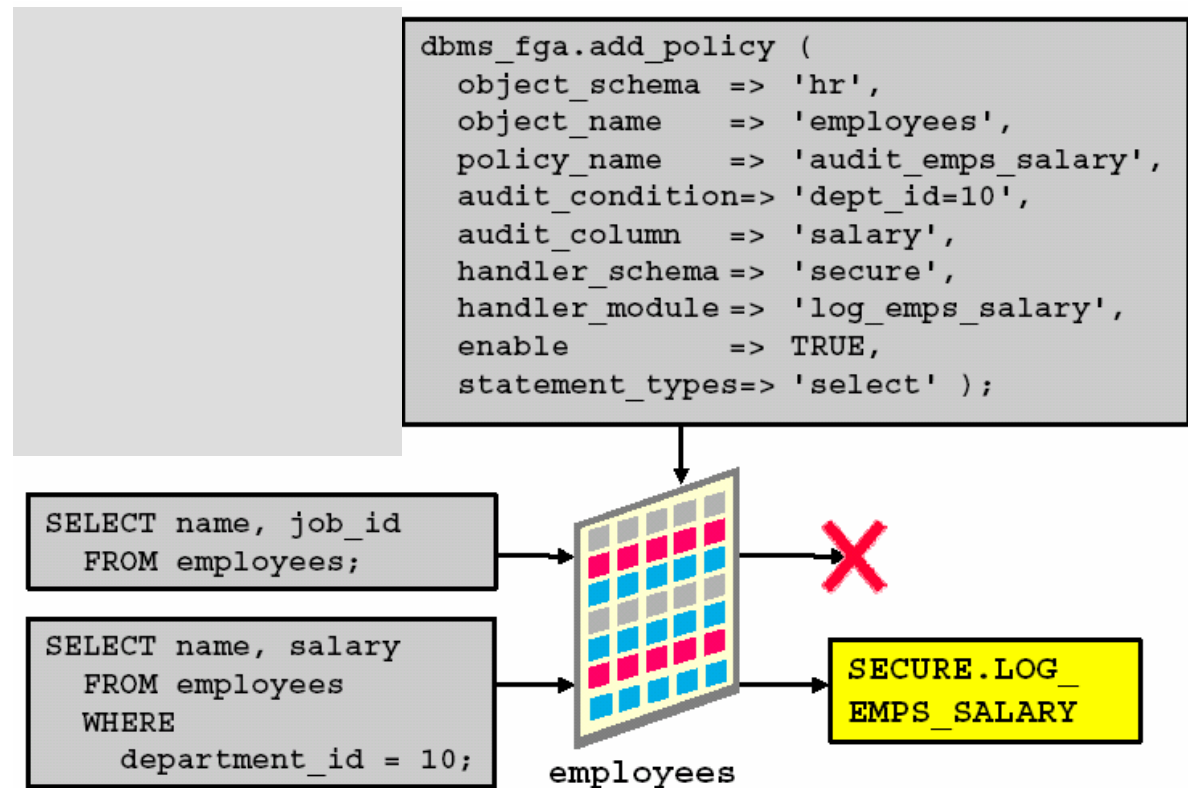
- Mengawasi data yang diakses berdasarkan isi
- Audit SELECT atau INSERT, UPDATE, DELETE
- Dapat dihubungkan ke tabel atau view
- Prosedur yang membahayakan
- Menghubungkan dengan paket DBMS_FGA



Aturan FGA

Definisi :

- Audit kriteria
- Audit Action
- Dibuat dengan DBMS_FGA
- ADD_POLICY



Paket DBMS

SUB PROGRAM	KETERANGAN
ADD_POLICY	Membuat aturan audit menggunakan keterangan sebagai kondisi audit
DROP_POLICY	Menghapus audit
ENABLE_POLICY	Mengaktifkan policy
DISABLE_POLICY	Mematikan policy

Mengaktifkan dan Mematikan FGA Policy

Mengaktifkan Audit

```
dbms_fga.enable_policy (  
  object_schema => 'hr',  
  object_name   => 'employees',  
  policy_name   => 'audit_emps_salary' );
```

Mematikan Audit

```
dbms_fga.disable_policy (  
  object_schema => 'hr',  
  object_name   => 'employees',  
  policy_name   => 'audit_emps_salary' );
```

Menghapus FGA Policy

```
SQL> EXEC dbms_fga.drop_policy ( -  
> object_schema => 'hr', -  
> object_name    => 'employees', -  
> policy_name    => 'audit_emps_salary');
```

```
PL/SQL procedure successfully completed.
```

```
SQL>
```

Memicu Audit Events

Statement untuk yang menyebabkan audit

```
SELECT count (*)  
  FROM hr.employees  
 WHERE department_id = 10  
        AND salary > v_salary;
```

```
SELECT salary  
  FROM hr.employees;
```

Statement yang tidak menyebabkan audit

```
SELECT last_name  
  FROM hr.employees  
 WHERE department_id = 10;
```

Dictionary View

NAMA VIEW	KETERANGAN
DBA_FGA_AUDIT_TRAIL	Semua aturan FGA yang dapat diakses oleh user saat ini
ALL_AUDIT_POLICY	Menghapus audit
DBA_AUDIT_POLICY	Semua aturan FGA di dalam database
USER_AUDIT_POLICY	Semua aturan FGA untuk object pada schema user

DBA_FGA_AUDIT_TRAIL

```
SQL> SELECT to_char(timestamp, 'YYMMDDHH24MI')
2          AS timestamp,
3          db_user,
4          policy_name,
5          sql_bind,
6          sql_text
7  FROM dba_fga_audit_trail;
```

TIMESTAMP	DB_USER	POLICY_NAME	SQL_BIND

SQL_TEXT			

0201221740	SYSTEM	AUDIT_EMPS_SALARY	#1(4):1000
SELECT count(*)			
FROM hr.employees			
WHERE department_id = 10			
AND salary > :b1			

Sekilas Tentang FGA

- Untuk meng-audit semua statement, gunakan kondisi null
- Jika Anda ingin menambahkan sebuah aturan yang sudah ada, error ORA-28101 akan muncul
- Tabel atau View audit harus sudah ada ketika anda membuat aturan
- Jika sintak kondisi audit tidak benar, error ORA 28112 akan muncul ketika objek audit di akses
- Jika kolom audit tidak ada di dalam tabel, tidak ada kolom yang akan diaudit
- Jika penanganan error tidak ada, tidak ada error yang dikembalikan dan audit record tetap dibuat

Mengaudit User SYSDBA dan SYSOPER

User dengan hak akses **SYSDBA** dan **SYSOPER** dapat mengakses database yang tertutup

- Audit trail harus disimpan di dalam database
- Koneksi dengan SYSDBA dan SYSOPER selalu diaudit
- Mengaktifkan audit tambahan dari SYSDBA dan SYSOPER dengan AUDIT_SYS_OPERATION
- Mengontrol audit trail dengan AUDIT_TRAIL_DEST. Defaultnya adalah:
 - \$ORACLE_HOME/rdbms/audit (UNIX/Linux)
 - Windows Event Log (Windows)

Mengupdate Keamanan

- Alamat web site keamanan database pada web site Oracle Technology Network :
 - <http://otn.oracle.com/deploy/security/alerts.htm>
- Oracle database administrator dan developer dapat juga menjadi anggota dalam forum keamanan dengan mengirim email dengan mengeklik link
 - “Subscribe to Security Alerts Here”

Ringkasan

Pada bab ini, Anda seharusnya telah mempelajari bagaimana cara untuk:

- Menerapkan prinsip-prinsip hak akses
- Manajemen user account default
- Menerapkan standard keamanan standard
- Mengaudit aktivitas database

Latihan 1

Tugas :

- Mencegah penggunaan password yang sederhana
- Kemampuan account untuk mengunci dalam waktu 10 menit ketika terjadi kesalahan login
- Membebaskan aplikasi login server dari perubahan password
- Kegagalan audit untuk koneksi ke database

Latihan 2

Tugas :

- Audit SELECT pada kolom SALARY pada tabel EMPLOYEES
- Audit perubahan pada kolom SALARY dari tabel EMPLOYEES:
 - Nilai lama
 - Nilai baru
 - User yang membuat perubahan
 - Lokasi mana yang telah diubah dari yang dibuat