**Lab 2. Auditarea activitatilor in baza de date**

| Cuvinte cheie: | |
|---|---|
| • auditare<br>• database audit trail<br>• operating system audit trail | • trigger pentru audit<br>• politici de audit<br>• pachetul DBMS_FGA |

*Auditarea* activitatii pe baza de date are doua componente: *monitorizarea si înregistrarea* persistenta a unei mulțimi de activitati si evenimente, stabilita a-priori, din baza de date.

Obiectivul auditarii activitatilor pe baza de date cuprind: non-repudierea, investigarea activitatilor suspecte, detectarea problemelor generate de configurările curente privind autorizarea (accesul la resurse), complianta cu legislația in vigoare, controlul.

## I. Auditare standard

***Ce activitati auditam?***

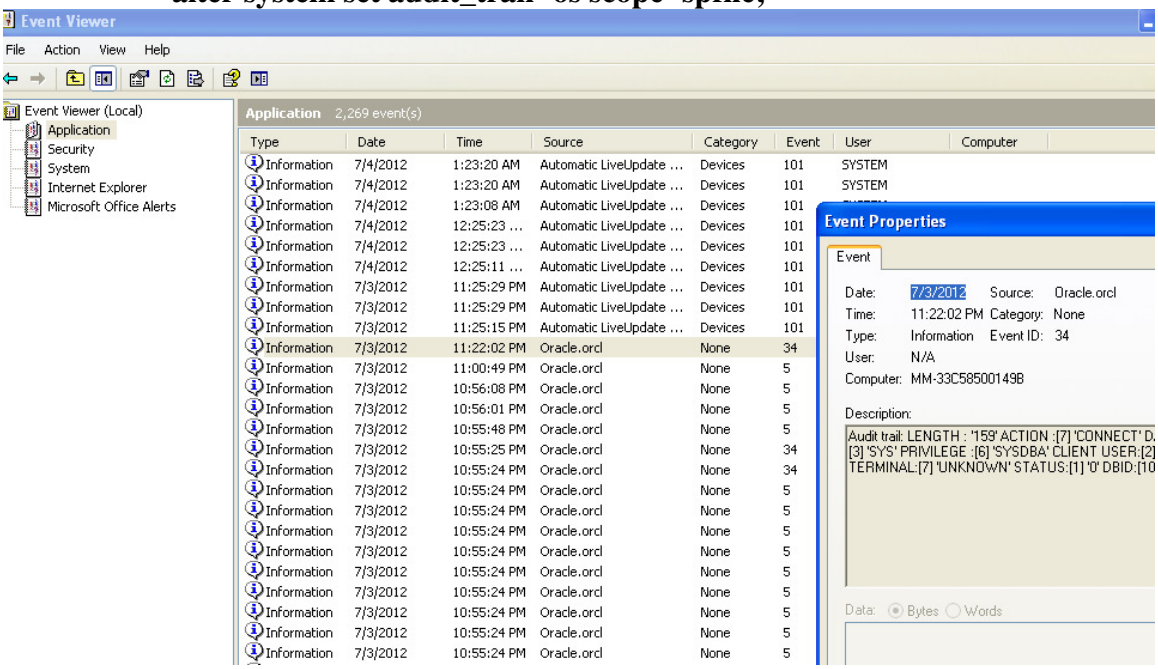
| | |
|---|---|
| pornirea si oprirea bazei de date, conectarea administratorului la baza de date | ***Sunt auditate implicit de catre Oracle; datele sunt stocate automat in OS*** |

| | Pentru toți utilizatorii | Pentru utilizatorul Tom |
|---|---|---|
| **Comenzi SQL** | | |
| ***- LDD :*** *toate comenzile CREATE TABLE si DROP TABLE* | ***AUDIT TABLE*** | ***AUDIT TABLE BY Tom*** |
| ***- LMD :*** *toate comenzile INSERT, UPDATE, respectiv DELETE* | ***AUDIT INSERT TABLE***<br>***AUDIT DELETE TABLE***<br>***AUDIT UPDATE TABLE*** | ***AUDIT INSERT TABLE BY Tom***<br>***s.a.m.d.*** |
| ***- SELECT:*** *toate interogările pe toate tabelele si toate vizualizările* | ***AUDIT SELECT TABLE*** | ***AUDIT SELECT TABLE BY Tom*** |
| **Comenzi SQL pe un obiect specificat (schema.obiect) al bazei de date** | | |
| **- doar când comanda esueaza** | ***AUDIT SELECT, INSERT, UPDATE, DELETE ON Tom.employees BY ACCESS WHENEVER NOT SUCCESSFUL;*** | ***AUDIT SELECT, INSERT, UPDATE, DELETE ON Tom.employees BY Tom WHENEVER NOT SUCCESSFUL;*** |
| **- oricând** | ***AUDIT SELECT, INSERT, UPDATE, DELETE ON Tom.employees;*** | ***AUDIT SELECT, INSERT, UPDATE, DELETE ON Tom.employees BY Tom;*** |
| **Activitatea in rețea** | ***AUDIT NETWORK*** | **-** |
| **Exercitare privilegii**[1] **-** *de fiecare data când este utilizat un privilegiu pentru efectuarea unei acțiuni pe baza de date* | ***Ex:***<br>***AUDIT CREATE ANY VIEW (in orice schema)***<br>***AUDIT CREATE VIEW (in schema proprie)*** | ***AUDIT CREATE ANY VIEW BY Tom***<br>***s.a.m.d.*** |
| **Sesiune de lucru pe baza de date** | ***AUDIT SESSION*** | ***AUDIT SESSION BY Tom*** |

[1] (pentru detalii vedeti cursul si laboratorul 4 ce va urma)

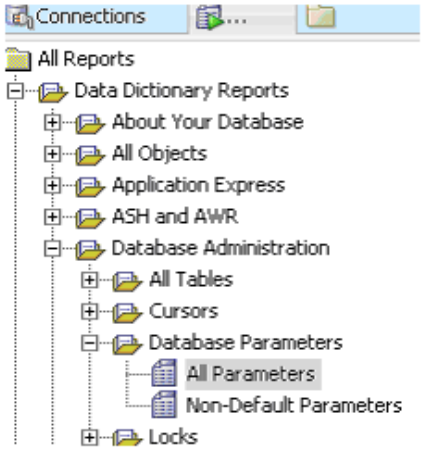
***Unde înregistram informațiile monitorizate?***

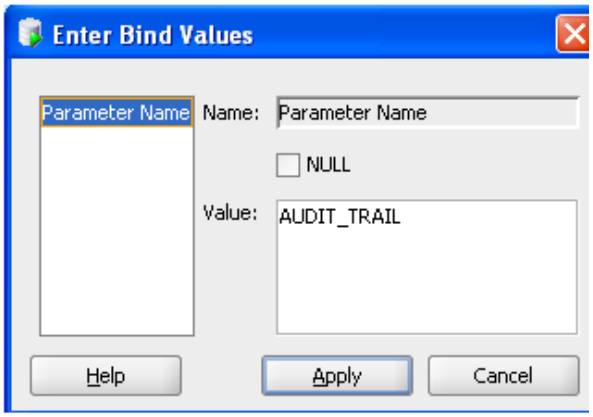
- in baza de date –database audit trail :
  → **audit_trail =DB** ( tabela SYS.AUD$ , view DBA_AUDIT_TRAIL, view DBA_COMMON_AUDIT_TRAIL)
  **alter system set audit_trail=db scope=spfile;**
  → **audit_trail =DB,EXTENDED** (aceleasi tabela, view-uri, dar se stocheaza si textul comenzilor in campul SQLTEXT de tip CLOB)
- extern bazei de date - operating system audit trail. Variante :
  → **audit_trail = OS** (sub Windows, Control Panel – Administrative Tools – Event Viewer - zona „Application" din Windows Event Viewer)
  **alter system set audit_trail=os scope=spfile;**




→ **audit_trail = XML , AUDIT_FILE_DEST = calea la fişier** (implicit este $ORACLE_BASE/admin/$ORACLE_SID/adump. A NU SE MODIFICA!)
**alter system set audit_trail=xml scope=spfile;**

Pentru a afla configurația curenta privind locul stocarii datelor monitorizate (cu lowercase!):
**select value from v$parameter where name='audit_trail';**
sau, din SQLPlus:
**show PARAMETER audit_trail**
sau, din SQLDeveloper:
meniul View-> Reports
→ All Reports- Data Dictionary Reports – Database Administration – Database Parameters – All Parameters
→ se selectează conexiunea de utilizat, iar in fereastra de dialog se înscrie valoarea AUDIT_TRAIL , apoi se apasă butonul „Apply"




***Pornirea auditului pentru activitatea X(vezi tabel prima pagina):*** ***AUDIT X***
***Oprirea auditului pentru activitatea X:*** ***NOAUDIT X***
***Oprirea in masa a auditului pentru toate comenzile SQL nelegate la un obiect specific :*** ***NOAUDIT ALL***
***Oprirea in masa a auditului pentru exercitarea privilegiilor:*** ***NOAUDIT ALL PRIVILEDGES***
***Oprirea in masa a auditului pentru toate comenzile SQL legate la obiecte specifice :*** ***NOAUDIT ALL ON DEFAULT***

***Ştergerea informaţiilor de monitorizare, după ce le arhivam:***

In funcție de numărul activitatilor auditate, de frecventa lor zilnica, volumul datelor de monitorizare poate deveni foarte mare si ocupa astfel spațiu util pe disc. De aceea se recomanda arhivarea periodica a datelor monitorizate si ştergerea lor din sistemul de producție.

Daca se realizează înregistrarea datelor in baza de date (database audit trail), atunci se pot utiliza comenzi de ştergere (reținem, după arhivarea datelor in prealabil!) :

**DELETE FROM SYS.AUD$;**

Se poate opta pentru ştergerea informațiilor monitorizate pentru un anumit obiect al bazei de date, de exemplu pentru tabela employees:

**DELETE FROM SYS.AUD$ WHERE OBJ$NAME='EMPLOYEES';**

## II. Triggeri pentru auditare

Ne reamintim de la cursul de SGBD [2] ca „*un declanşator(trigger) este un bloc PL/SQL sau apelul CALL al unei proceduri PL/SQL care se executa automat ori de cate ori are loc un anumit eveniment declanşator*”.

Triggerii sunt de doua tipuri: la nivelul bazei de date (operații pe baza de date) si la nivel de aplicație(ex: apăsarea unui buton pe un formular in Oracle Forms). Obiectul de interes pentru noi in acest material este categoria triggerilor la nivelul bazei de date.

[2] Pentru recapitulare, recomandare bibliografica: POPESCU I., ALECU A., VELCESCU L., FLOREA G., Programare avansata in Oracle9i,Editura Tehnica, Bucuresti, 2004

**Triggerii la nivelul bazei de date (database triggers)** se clasifica la rândul lor in 3 categorii:

- triggeri LMD – declansati de comenzi LMD pe o tabela. Pot fi executați o singura data la nivelul unei comenzi indiferent de numărul de înregistrări afectate (triggeri la nivel de instrucțiune) sau pot fi executați FOR EVERY ROW (triggeri la nivel de inregistrare). Le corespund tipurile de triggeri BEFORE STATEMENT, AFTER STATEMENT, BEFORE EACH ROW, AFTER EACH ROW;
- triggeri INSTEAD OF - declansati de comenzi LMD pe o vizualizare;
- triggeri SYSTEM – declansati de evenimente precum pornire/oprire baza de date, comenzi LDD, conectare/deconectare utilizator. Le corespund tipurile de triggeri AFTER EVENT, BEFORE EVENT.

Interogarea tabelei **SYS.TRIGGER$** sau a vizualizarii **ALL_TRIGGERS** oferă informații despre toți triggerii de la nivelul bazei de date.

**SELECT DISTINCT TRIGGER_TYPE FROM ALL_TRIGGERS;**

```
TRIGGER_TYPE
----------------
BEFORE STATEMENT
BEFORE EACH ROW
AFTER EACH ROW
BEFORE EVENT
AFTER STATEMENT
AFTER EVENT
INSTEAD OF

7 rows selected.
```

View-ul **DBA_TRIGGERS** oferă informații despre triggerii creați de produsele Oracle automat la instalare. Imediat după crearea unei baze de date regăsim 617 triggeri DBA. Sa aflam informații despre triggerii SYSTEM (de tip **'BEFORE EVENT' si 'AFTER EVENT'**) creați automat la instalare:

**SELECT SUBSTR(OWNER,1,20) OWNER ,SUBSTR(TRIGGER_NAME,1,30) TRIGGER_NAME,SUBSTR(TRIGGERING_EVENT,1,30) TRIGGERING_EVENT, TRIGGER_TYPE**
**FROM DBA_TRIGGERS**
**WHERE TRIGGER_TYPE='BEFORE EVENT' OR TRIGGER_TYPE='AFTER EVENT'**
**ORDER BY TRIGGER-TYPE DESC;**

```
OWNER                TRIGGER_NAME                   TRIGGERING_EVENT                 TRIGGER_TYPE
-------------------- ------------------------------ -------------------------------- ----------------
SYS                  XDB_PI_TRIG                    DROP OR TRUNCATE                 BEFORE EVENT
SYS                  CDC_ALTER_CTABLE_BEFORE        ALTER                            BEFORE EVENT
MDSYS                SDO_ST_SYN_CREATE              CREATE                           BEFORE EVENT
MDSYS                SDO_TOPO_DROP_FTBL             DROP                             BEFORE EVENT
EXFSYS               EXPFIL_RESTRICT_TYPEEVOLVE     CREATE OR ALTER                  BEFORE EVENT
EXFSYS               EXPFIL_DROPOBJ_MAINT           DROP                             BEFORE EVENT
SYS                  CDC_DROP_CTABLE_BEFORE         DROP                             BEFORE EVENT
MDSYS                SDO_GEOR_BDDL_TRIGGER          DDL                              BEFORE EVENT
SYS                  CDC_CREATE_CTABLE_BEFORE       CREATE                           BEFORE EVENT
EXFSYS               RLMGR_TRUNCATE_MAINT           TRUNCATE                         BEFORE EVENT
WMSYS                NO_UM_DDL                      CREATE OR ALTER OR DROP OR REN   BEFORE EVENT

OWNER                TRIGGER_NAME                   TRIGGERING_EVENT                 TRIGGER_TYPE
-------------------- ------------------------------ -------------------------------- ----------------
SYS                  OLAPISHUTDOWNTRIGGER           SHUTDOWN                         BEFORE EVENT
MDSYS                SDO_NETWORK_DROP_USER          DROP                             AFTER EVENT
MDSYS                SDO_GEOR_ADDL_TRIGGER          DDL                              AFTER EVENT
MDSYS                SDO_DROP_USER                  DROP                             AFTER EVENT
SYS                  OLAPISTARTUPTRIGGER            STARTUP                          AFTER EVENT
MDSYS                SDO_GEOR_ERR_TRIGGER           ERROR                            AFTER EVENT
EXFSYS               EXPFIL_DROPUSR_MAINT           DROP                             AFTER EVENT
EXFSYS               EXPFIL_ALTEREXPTAB_MAINT       ALTER OR RENAME                  AFTER EVENT
SYS                  CDC_CREATE_CTABLE_AFTER        CREATE                           AFTER EVENT
WMSYS                NO_UM_DROP_A                   DROP                             AFTER EVENT
SYS                  AW_REN_TRG                     RENAME                           AFTER EVENT

OWNER                TRIGGER_NAME                   TRIGGERING_EVENT                 TRIGGER_TYPE
-------------------- ------------------------------ -------------------------------- ----------------
SYSMAN               MGMT_STARTUP                   STARTUP                          AFTER EVENT
SYS                  AW_DROP_TRG                    DROP                             AFTER EVENT
SYS                  AW_TRUNC_TRG                   TRUNCATE                         AFTER EVENT

25 rows selected.
```

Tot la instalare, in mod automat sunt creați triggeri LMD pe schema utilizatorului HR:

```
SELECT SUBSTR(TABLE_NAME,1,20) TABLE_NAME,
SUBSTR(TRIGGER_TYPE,1,30) TRIGGER_TYPE,TRIGGER_BODY
FROM DBA_TRIGGERS
WHERE  OWNER='HR';
```

```
TABLE_NAME           TRIGGER_TYPE     TRIGGER_BODY
-------------------- ---------------- --------------------------------------------------------------------
EMPLOYEES            BEFORE STATEMENT BEGIN
                                        secure_dml;
                                      END secure_employees;

EMPLOYEES            AFTER EACH ROW   BEGIN
                                        add_job_history(:old.employee_id, :old.hire_date, sysdate,
```

**Pentru auditare, putem crea triggeri personalizați care sa înregistreze anumite informații de interes. In general, vom crea o tabela speciala pentru stocarea informațiilor monitorizate.**
Triggerii construiți de noi se regăsesc la interogarea tabelului TRIGGER$ si a view-urilor ALL_TRIGGERS, USER_TRIGGERS.

**Câteva recapitulări utile referitoare la procesarea triggerilor, utile in auditare:**

**1) Trebuie sa avem grija ca triggerii pe care ii construim sa nu influențeze activitatea normala din baza de date. Scopul auditului este sa monitorizeze pasiv si sa înregistreze activitatea pentru analiza ulterioara.** Prin urmare NU vom defini triggeri INSTEAD OF care sa deturneze rezultatele din tabelele vizate către tabela de audit!

**2) Triggerii LMD la nivel de instrucțiune si la nivel de înregistrare pot coexista.**
**Vor fi apelați:**

- Trigger BEFORE instrucțiune
- Pentru fiecare înregistrate afectata
  - Trigger BEFORE înregistrare
  - Operație LMD propriu-zisa
  - Trigger AFTER înregistrare
- Trigger AFTER instrucțiune

**Din perspectiva auditului, trebuie decisa cu atenție granularitatea monitorizării, pentru ca scopul nu este sa clonam tabelele de baza, ci sa înregistram activitatea pe ele.**

**3) Triggerii definiți de utilizatori vor fi executați doar daca din punct de vedere al lui Oracle instrucțiunea este corecta si poate avea loc. Pentru o instrucțiune LMD greşit construita sau care încalcă unele constrangeri, de exemplu, nu se va ajunge pana la triggerul definit de utilizator, ci eroarea va fi returnata inainte.**

**In concluzie, pentru audit sunt adecvați in special triggerii LMD la nivel de instrucțiune.**

## III. Politici de auditare

Cea de-a treia modalitate de audit se refera la *Fine Grain Audit* prin politici de auditare. Anatomia unei politici de auditare este următoarea:

- specificarea obiectului (schema, nume obiect, coloane ) supus monitorizării;
- specificarea acțiunilor monitorizate asupra obiectului (SELECT, INSERT,UPDATE, DELETE); implicit este SELECT;
- specificarea condițiilor sub care se înregistrează informațiile monitorizate, este corespondentul clauzei WHEN din triggeri si este opțional;
- un *event handler* care sa trateze suplimentar evenimentul, acesta este opțional.

O politica de auditare poate fi activa (status ENABLED) sau inactiva (status DISABLED). Nu pot fi definite mai mult de 256 de politici de auditare la nivelul unui obiect al BD. Lista politicilor de auditare active se obține prin interogarea vizualizării ALL_AUDIT_POLICIES astfel:

```
SELECT POLICY_TEXT,ENABLED
FROM ALL_AUDIT_POLICIES
WHERE OBJECT_NAME='DEPARTMENTS';
```

Pentru gestionarea politicilor de auditare avem la dispoziție pachetul DBMS_FGA (este necesar sa acordați privilegiu[3] pentru utilizatorii ce vor scrie cod PL/SQL care sa folosească acest pachet: *grant execute on dbms_fga to nume_utilizator;*).

**Sintaxa:**

```
DBMS_FGA.ADD_POLICY (
        object_schema=>'nume schema',
        object_name=>'obiect auditat',
        policy_name=>'nume unic de politica',
        audit_column=>'col1,col2,.. din obiectul auditat',
        enable=>false,
        statement_types=>'select,insert,update,delete'
        handler_schema=>'schema ce contine handler'
        handler_module=>'nume handler');
```

Se impune ca modulul handler sa fie o procedura PL/SQL cu urmatoarea signatura:

```
CREATE OR REPLACE PROCEDURE <fname> ( object_schema VARCHAR2,
object_name VARCHAR2, policy_name VARCHAR2 )  AS ..
```

Rezultatele auditului pot fi obținute din tabela SYS.FGA_LOG$ si din view **dba_fga_audit_trail**
Pentru activare sau dezactivarea unei politici de auditare:

```
DBMS_FGA.ENABLE_POLICY /  DBMS_FGA.DISABLE_POLICY (
    object_schema=>'nume schema de care apartine obiectul',
    object_name=>'obiect auditat',
    policy_name=>'nume unic de politica');
```

*Obs: acțiunile administratorului (as SYSDBA) nu sunt auditate (modificare in ini.ora)!*

[3] mai multe detalii vor urma in laboratorul 4 dedicat rolurilor si privilegiilor

**Exerciţii:**

**1. Configuraţi baza de date pentru audit standard cu stocarea datelor monitorizate in cadrul bazei de date.**
**Se vor monitoriza toate activitatile de interogare efectuate in baza de date, cu stocarea textului cererilor efectuate de utilizatori.**

**Sa se afişeze un raport al acestor activitati pentru tabelele date anterior.**
**Opriţi auditul configurat.**

**2. Configuraţi baza de date pentru audit stadard cu stocarea datelor monitorizate in cadrul unui fisier XML in calea standard.**
**Se vor monitoriza toate comenzile LMD pe tabela HR.employees care esueaza.**

**Sa se consulte fisierele XML rezultate.**
**Opriţi auditul configurat.**

**3. Cu scopul auditarii, creaţi trigger(i) care sa înregistreze intr-o tabela de audit (TAB_AUDIT_EMP) informaţii despre operaţiile LMD de stergere pe tabela** GRUPASEC2012.EMPLOYEES si numarul de inregistrari afectate

**4. Cu scopul auditarii, creaţi un trigger care sa înregistreze intr-o tabela de audit (TAB_AUDIT_EMP) informaţii despre operaţiile LMD care stabilesc salarii peste plafonul de 20000.**

**5. Creaţi o politica de auditare astfel încât sa fie înregistrate instrucţiunile LMD de modificare a şefilor departamentelor (MANAGER_ID) pe tabela** GRUPASEC2012.DEPARTMENTS

**Bibliografie:**
http://docs.oracle.com/cd/B10501_01/server.920/a96521/audit.htm
http://docs.oracle.com/cd/E11882_01/network.112/e16543/auditing.htm
http://www.datadisk.co.uk/html_docs/oracle/auditing.htm