Administration des bases de données
Chapitre 4 : Sécurité et audit des bases de données oracle

Ines BAKLOUTI

ines.baklouti@esprit.tn

Ecole Supérieure Privée d'Ingénierie et de Technologies

Plan

Introduction

- Un système sécurisé garantit la confidentialité des données qu'il contient. La sécurité englobe plusieurs aspects :
  - Authentifier les utilisateurs
    - Gestion des utilisateurs et des profils
  - Limiter l'accès aux données et aux services
    - doit passer par l'application du principe du moindre privilège
  - Surveiller les activités suspectes
    - Même autorisés, les utilisateurs authentifiés peuvent parfois compromettre le système
    - Audit de la base de données

Plan

Principe du moindre privilège

- Le principe du moindre privilège consiste à n'accorder à un utilisateur que les privilèges dont il a réellement besoin pour effectuer une tâche de manière efficace
  - Protéger le dictionnaire de données
  - Révoquer les privilèges non nécessaires du rôle PUBLIC
  - Limiter les utilisateurs dotés de privilèges d'administration
  - Limiter l'authentification à distance auprès de la base de données

Protéger le dictionnaire de données

- Protégez le dictionnaire de données en affectant la valeur FALSE au paramètre d'initialisation O7_DICTIONARY_ACCESSIBILITY
- Cette configuration empêche les utilisateurs dotés du privilège système ANY TABLE d'accéder aux tables de base du dictionnaire de données
- La valeur FALSE empêche également l'utilisateur SYS de se connecter sous un autre compte que SYSDBA

Révoquer les privilèges non nécessaires du rôle PUBLIC

- Etant donné que n'importe quel utilisateur de base de données peut se servir des privilèges accordés à PUBLIC, vous devez révoquer de PUBLIC les privilèges et rôles qui ne sont pas indispensables.
- De nombreux packages intégrés accordent le privilège EXECUTE à PUBLIC.
- Le privilège d'exécution sur les packages suivants doit toujours être révoqué de PUBLIC :
  - UTL_SMTP : permet l'envoi de messages électroniques arbitraires via l'utilisation de la base de données comme serveur de messagerie SMTP. L'octroi de ce package à PUBLIC peut permettre l'échange non autorisé de messages électroniques.
  - UTL_HTTP : permet au serveur de base de données de demander et d'extraire des données via HTTP. L'octroi de ce package à PUBLIC peut autoriser l'envoi de données à un site Web malveillant par l'intermédiaire de HTML.
  - UTL_FILE : si ce package est configuré de manière incorrecte, il permet l'accès au niveau texte à n'importe quel fichier du système d'exploitation. Même lorsqu'il est configuré correctement, ce package ne distingue pas les applications qui l'appellent ; autrement dit, une application disposant d'un accès à UTL_FILE peut écrire des données arbitraires dans le même emplacement qu'une autre application.

Exemple

```
REVOKE execute ON utl_file,utl_http,utl_smtp FROM PUBLIC ;
```

Limiter les utilisateurs dotés de privilèges d'administrateur

- Limiter les types de privilège suivants :
  - Octroi des privilèges système et objet
  - Connexions dotées des privilèges SYS : SYSDBA et SYSOPER
  - Privilèges de type DBA, tels que DROP ANY TABLE
- répertorier tous les utilisateurs avec le rôle DBA :

```
SQL> SELECT grantee FROM dba_role_privs
  2  WHERE granted_role = 'DBA';

GRANTEE
------------------------------
SYS
SYSTEM
```

- répertorier les utilisateurs auxquels le privilège SYSDBA ou SYSOPER a été accordé

```
SQL>  SELECT * FROM V$PWFILE_USERS;

USERNAME                       SYSDB SYSOP
------------------------------ ----- -----
SYS                            TRUE  TRUE
```

Désactiver l'authentification à distance par le système d'exploitation

- L'authentification à distance ne doit être utilisée que lorsque vous faites confiance à tous les clients pour authentifier de manière appropriée les utilisateurs.
- Processus d'authentification à distance :
  - L'utilisateur de base de données est authentifié en externe
  - Le système distant authentifie l'utilisateur
  - L'utilisateur se connecte à la base de données sans authentification complémentaire
- Pour désactiver l'authentification à distance, vérifier que la valeur FALSE (par défaut) est affectée au paramètre d'initialisation d'instance REMOTE_OS_AUTHENT

Plan

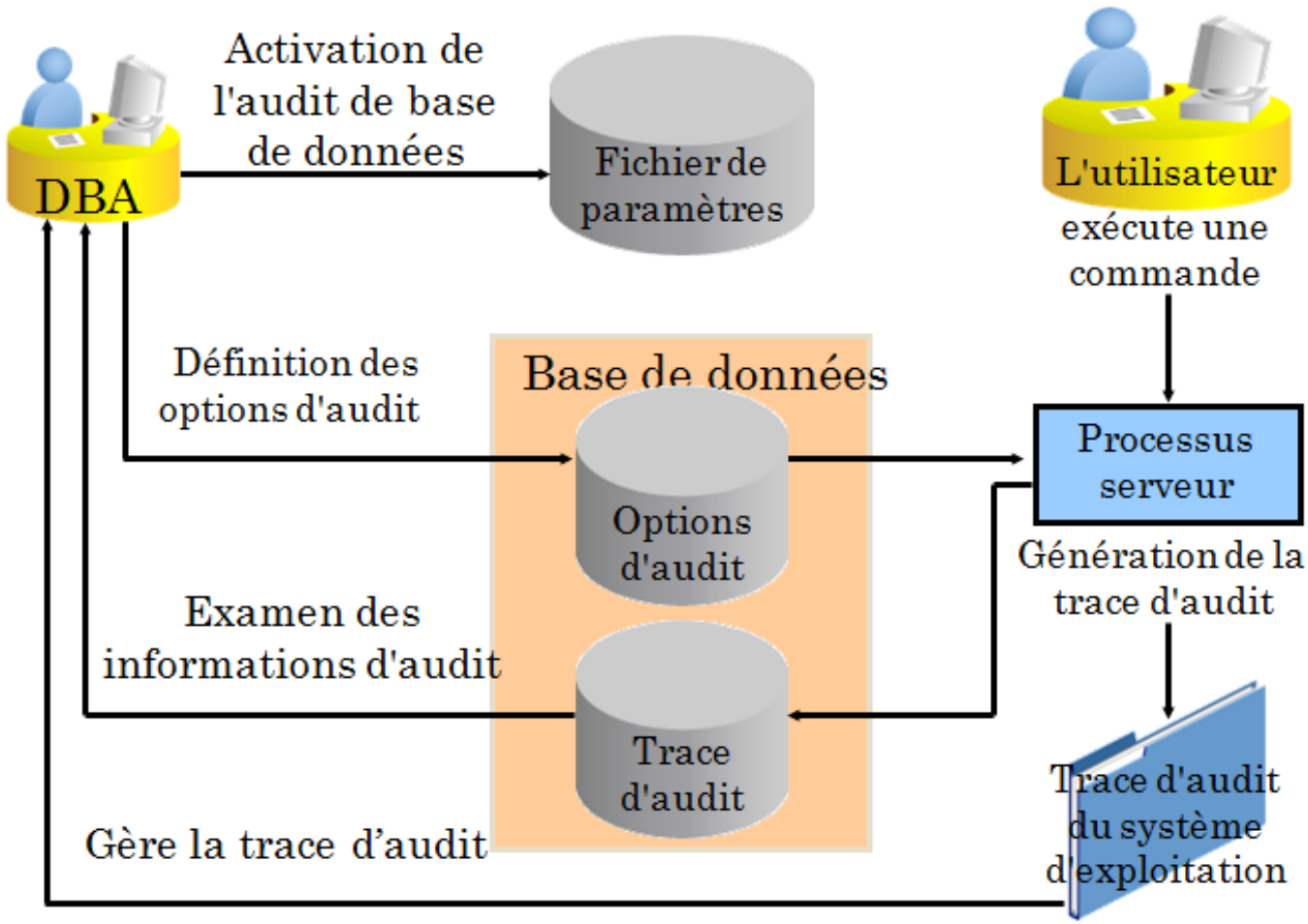
Audit de la base de données

- La surveillance ou l'audit doit faire partie intégrante des procédures de sécurité.
- Les outils d'audit intégrés d'Oracle sont les suivants :
  - Oracle standard auditing appelé audit de la BD
  - Auditing par Trigger appelé aussi audit basé sur les valeurs ou sur les données
  - Fine Grained Auditing n'est pas disponible sur toutes les versions (à partir de 8i) (audit détaillé)

Audit de la base de données

Type d'audit	Événements audités	Contenu de la trace d'audit
Audit standard de base de données	Utilisation des privilèges, notamment l'accès aux objets	Ensemble fixe de données
Audit basé sur les données	Données modifiées par les instructions LMD	Défini par l'administrateur
Audit détaillé (FGA)	Instructions SQL (INSERT, UPDATE, DELETE et SELECT) en fonction du contenu	Ensemble fixe de données, incluant l'instruction SQL

Audit standard de base de données



Audit standard de base de données

- Activé via le paramètre AUDIT_TRAIL
  - NONE : désactive la collecte des enregistrements d'audit
  - OS : active l'audit, enregistrements stockés dans la trace d'audit du système d'exploitation
    - L'emplacement du fichier est défini par le paramètre AUDIT_FILE_DEST
  - DB : active l'audit, enregistrements stockés dans la table système de base de données SYS.aud$
  - DB, EXTENDED : active l'audit, enregistrements stockés dans la table système de base de données SYS.aud$. En plus les colonnes SQLBIND et SQLTEXT de la table SYS.AUD$ renseignées
  - XML : active l'audit, enregistrements stockés dans des fichiers au format XML dans la trace d'audit du système d'exploitation
  - XML, EXTENDED : active l'audit, les colonnes SQLBIND et SQLTEXT de la table SYS.AUD$ renseignées. les enregistrements stockés dans des fichiers au format XML dans la trace d'audit du système d'exploitation

Audit standard de base de données

Paramètre AUDIT_TRAIL

- Afficher la valeur du paramètre audit_trail :

```
SQL> show parameter audit

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      C:\ORACLEXE\APP\ORACLE\ADMIN\X
                                                 E\ADUMP
audit_sys_operations                 boolean     FALSE
audit_trail                          string      DB
```

- Pour changer la valeur du paramètre audit_trail :
  - Si on a un pfile, alors il suffit d'éditer le contenu du fichier
  - Si on a un spfile, alors il faut exécuter la commande suivante :
    - alter system set audit_trail=DB scope=spfile ;

Audit standard de base de données

Audit OS vis DB

- L'audit via l'OS est préféré lorsqu'on veut auditer plusieurs BDs et d'écrire les audits dans une même destination, afin de visualiser le résultat de tous les audits dans un seul rapport
  =>Limites : Pas tous les OS qui offrent cette possibilité (Unix)
- L'audit via la BD permet de visualiser les résultats par des requêtes simples contre les vues du dictionnaire relatives à l'audit
  =>Limites :
  - Table SYS.aud$ (tablespace System) doit être archivée et purgée périodiquement puisque les informations auditées peuvent être volumineuses
  - Nécessité d'une protection pour la SYS.aud$ sinon un user malicieux peut effacer de cette table les actions non autorisées qu'il a effectué dans la BD
    =>Solution :
    - auditer toutes les actions qui s'effectuent sur la table SYS.AUD$ par la commande suivante : audit all on SYS.AUD$ by access

Audit standard de base de données

Niveaux d'audit

- Oracle permet un auditing standard sur 4 niveaux :
  - Auditing de commandes (LDD)
  - Audit de privilèges (systèmes)
  - Audit d'objets de schéma (privilèges objets)
  - Audit de connexion à la BD

Audit de privilèges ou de commandes

```
AUDIT {commande | privilège_système}
      [ , {commande | privilège_système} ] ...
      [BY user [ , user ] ... ]
      [BY {SESSION | ACCESS} ]
      [WHENEVER [NOT] SUCCESSFUL]
```

Audit d'objets

```
AUDIT commande [ , commande ] ...
      ON { [ schema. ] objet | DEFAULT }
      [BY {SESSION | ACCESS} ]
      [WHENEVER [NOT] SUCCESSFUL]
```

- BY SESSION : indique à Oracle de n'insérer par session qu'un enregistrement par objet de BD, quel que soit le nombre de commandes SQL de même type
- BY ACCESS : indique à Oracle d'insérer un enregistrement dans la trace chaque fois qu'une action est soumise
  - Pour les commandes DDL, Oracle fait toujours les audits par accès
- WHENEVER : spécifie que les audits ne doivent être exécutés que lorsque l'exécution de commandes SQL est terminée, réussie ou non

Audit standard de base de données

Niveaux d'audit

Exemples

1. Audit de commandes
   - non ciblé : AUDIT table ; (audite toute instruction LDD qui affecte une table)
   - ciblé : AUDIT TABLE BY hr WHENEVER NOT SUCCESSFUL ;
2. Audit de privilèges systèmes
   - non ciblé : AUDIT select any table, create any trigger ;
   - ciblé : AUDIT select any table BY hr BY SESSION ;
3. Audit de privilèges objets
   - non ciblé : AUDIT ALL on hr.employees ;
   - ciblé : AUDIT UPDATE, DELETE on hr.employees BY ACCESS ;
4. Audit de session
   - AUDIT session whenever not successful ;

Audit standard de base de données

Arrêt et Annulation de l'audit

Disabling Statement and Privilege Auditing

The following statements turn off the corresponding audit options:

```
NOAUDIT session;
NOAUDIT session BY scott, lori;
NOAUDIT DELETE ANY TABLE;
NOAUDIT SELECT TABLE, INSERT TABLE, DELETE TABLE,
     EXECUTE PROCEDURE;
```

The following statements turn off all statement (system) and privilege audit options:

```
NOAUDIT ALL;
NOAUDIT ALL PRIVILEGES;
```

To disable statement or privilege auditing options, you must have the AUDIT SYSTEM system privilege.

Disabling Object Auditing

The following statements turn off the corresponding auditing options:

```
NOAUDIT DELETE
    ON emp;
NOAUDIT SELECT, INSERT, DELETE
    ON jward.dept;
```

Furthermore, to turn off all object audit options on the EMP table, enter the following statement:

```
NOAUDIT ALL
    ON emp;
```

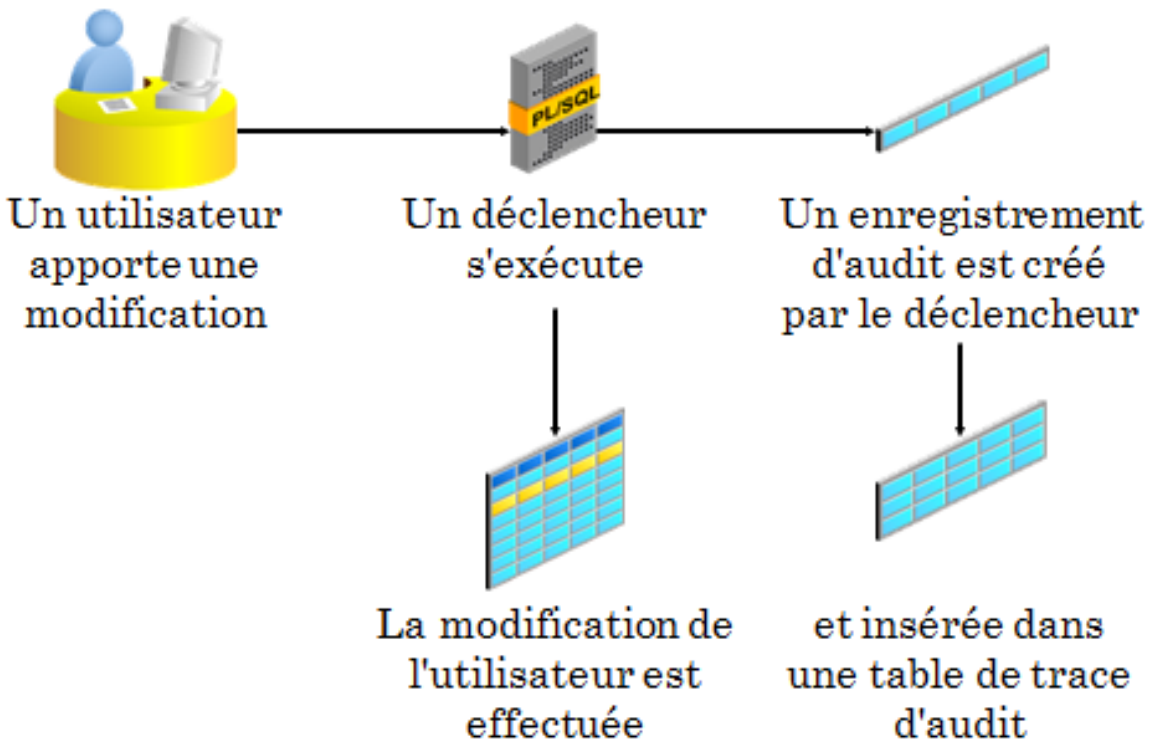
Audit standard de base de données

Vues d'audit

Vue de la trace d'audit	Description
DBA_AUDIT_TRAIL	Toutes les entrées de la trace d'audit
DBA_AUDIT_OBJECT	Enregistrements concernant les objets de schémas
DBA_AUDIT_SESSION	Toutes les entrées de connexion et de déconnexion
DBA_AUDIT_STATEMENT	Enregistrements d'audit des instructions

Audit basé sur les données

- L'audit standard permet d'identifier les commandes exécutées sur une table, mais ne peut pas fournir des informations sur les modifications faite. Pour garder trace sur ces modification, on peut avoir recours à l'audit basé sur les données avec des triggers.



Audit basé sur les données

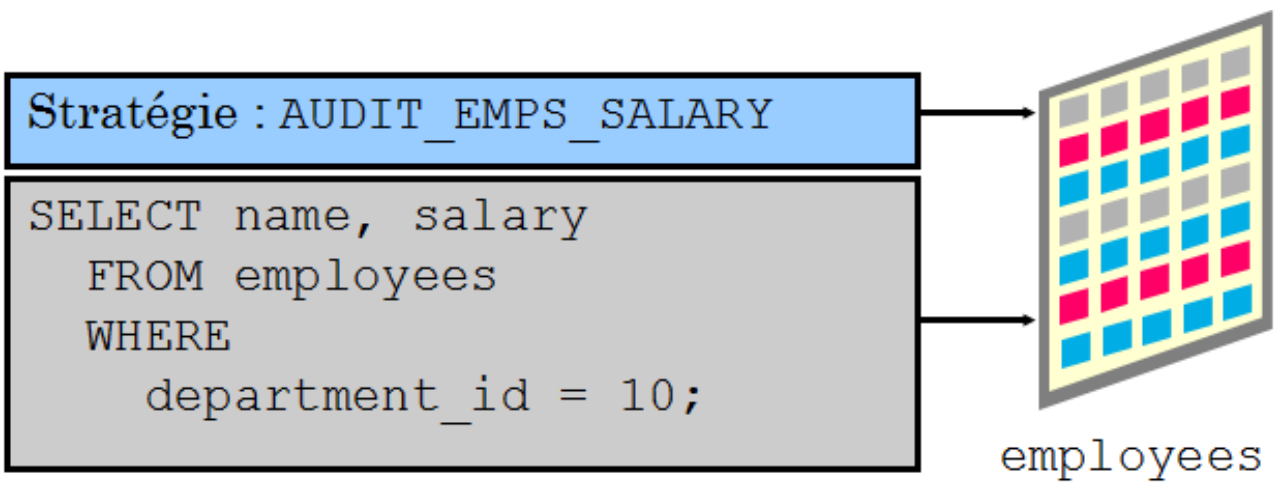
- Deux types de triggers :
  - DML trigger : permet d'enregistrer les valeurs de toutes les modifications apportées à la BD
    Tâche impossible, si vous utilisez l'audit intégré d'Oracle
  - System trigger : auditing de toute action de création, de suppression ou de connexion à la base
    Inutile puisqu'on pourra auditer ces informations en utilisant l'audit intégré d'Oracle

Syntaxe

```
CREATE [OR REPLACE] TRIGGER nom_trigger
{BEFORE|AFTER|INSTEAD OF}
{INSERT|UPDATE [ OF nom_colonne [, nom_colonneN]] |DELETE}
OR {INSERT|UPDATE [OF nom_colonne [, nom_colonneN ]] |DELETE}
REFERENCING {[OLD [AS] ancien] | [NEW [AS] nouveau]}
ON nom_table
[FOR EACH ROW]
[WHEN] (condition)
DECLARE
/* déclaration */
BEGIN
/* traitement */
[EXCEPTION]
END;
```

Audit détaillé

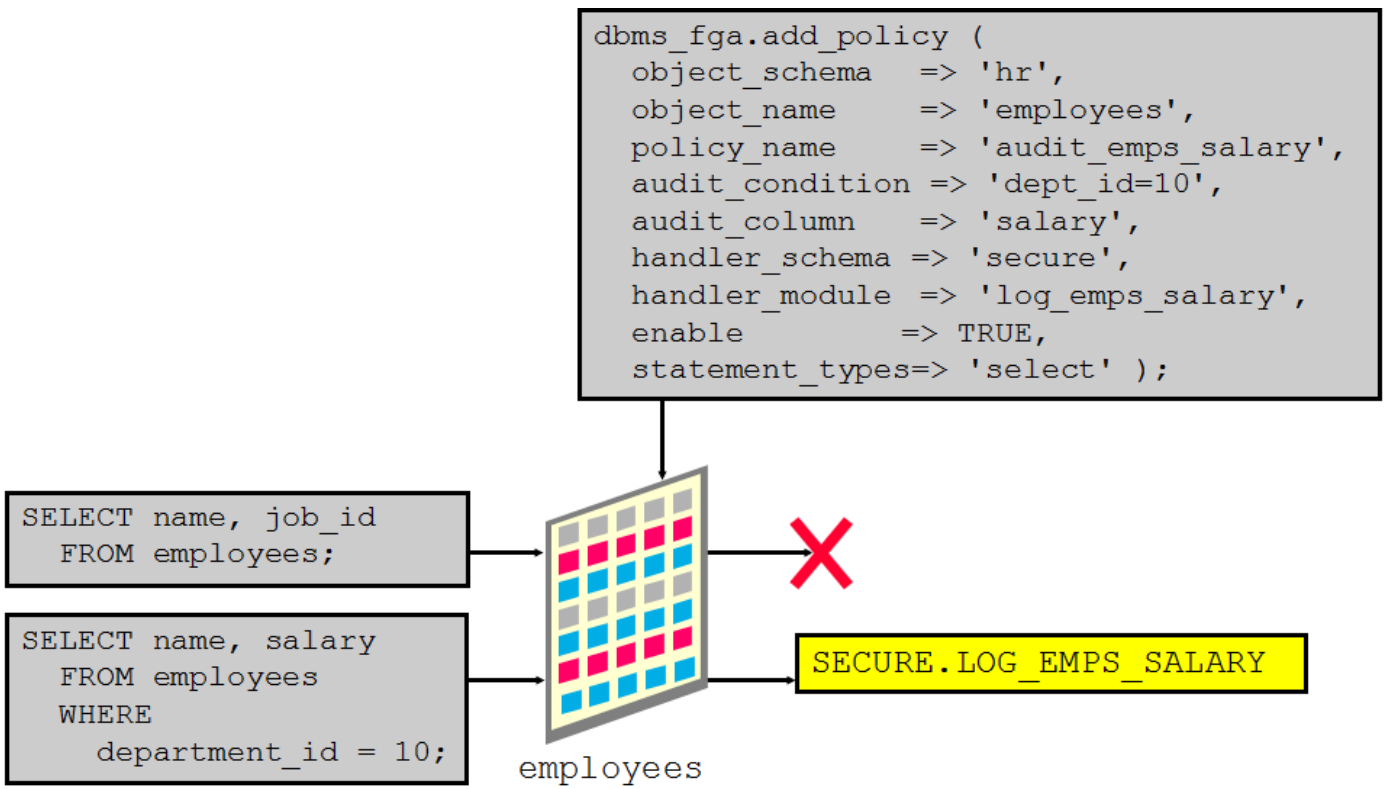
- L'audit détaillé "Fine Grained Auditing" (FGA) permet de définir des conditions fines pour l'auditing
  - Surveille l'accès aux données en fonction du contenu
  - Audite les opérations SELECT ou INSERT,UPDATE,DELETE
  - Peut être lié à une table ou à une vue
  - Peut exécuter une procédure PL/SQL
  - Est administré via le package DBMS_FGA



Audit détaillé

Stratégie d'audit

- Une stratégie d'audit détaillé :
  - Est constituée de 2 parties
    - Les critères d'audit : définit la condition qui doit être vérifiée pour que l'instruction soit auditée
    - L'action d'audit : le nom d'une procédure qui sera exécutée lorsque la condition est vérifiée
  - Est créée via la procédure ADD_POLICY du package DBMS_FGA



Audit détaillé

Package DBMS_FGA

- Le package DBMS_FGA permet de gérer les stratégies d'audit détaillé
- Pour pouvoir l'utiliser il faut accorder le privilège d'exécution pour ce package
- DBMS_FGA inclut les sous-programmes suivants :

Sous-programme	Description
ADD_POLICY	Crée une stratégie d'audit à l'aide du prédicat fourni en tant que condition d'audit
DROP_POLICY	Supprime une stratégie d'audit
ENABLE_POLICY	Active une stratégie d'audit
DISABLE_POLICY	Désactive une stratégie d'audit

Audit détaillé

Activer / Désactiver et supprimer une stratégie d'audit

Activer une stratégie

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

Désactiver une stratégie

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

Supprimer une stratégie

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

Audit détaillé

Vues d'audit

Vue de la trace d'audit	Description
DBA_FGA_AUDIT_TRAIL	Tous les événements d'audit détaillé
ALL_AUDIT_POLICIES	Toutes les stratégies d'audit détaillé pour les objets auxquels l'utilisateur actuel peut accéder
DBA_AUDIT_POLICIES	Toutes les stratégies d'audit détaillé dans la base de données
USER_AUDIT_POLICIES	Toutes les stratégies d'audit détaillé pour les objets du schéma de l'utilisateur actuel

Audit détaillé

Exemple

- Auditer les requêtes recherchant le salaire des employés du département 20

```
CREATE OR REPLACE PROCEDURE ins_audit_message(
  p_schema VARCHAR2, p_table VARCHAR2, p_policy VARCHAR2) IS
BEGIN
  INSERT INTO audit_messages VALUES(
    SYSDATE, p_schema||'.'||p_table||'.'||p_policy);
END;
/
BEGIN
 DBMS_FGA.ADD_POLICY(
    object_schema=> 'SCOTT',
    object_name  => 'EMP',
    policy_name  => 'DEPTNO20_SAL',
    audit_condition       => 'DEPTNO = 20',
    audit_column          => 'SAL',
    handler_schema        => 'SYSTEM',
    handler_module        => 'INS_AUDIT_MESSAGE',
    enable                => true);
END;
```

Audit détaillé

Exemple

- DBA_FGA_AUDIT_TRAIL

```
SQL> SELECT
session_id,timestamp,db_user,os_user,object_schema,object_name,
  2         policy_name,scn,sql_text
  3  FROM   dba_fga_audit_trail
  4  WHERE  policy_name = 'DEPTNO20_SAL'
  5  ORDER BY scn DESC
  6  /

SESSION_ID TIMESTAMP DB_USER  OS_USER   OBJECT_SCH OBJECT_NAM POLICY_NAME
---------- --------- -------- --------- ---------- ---------- -----------
       SCN SQL_TEXT
---------- --------------------------------------------------------------
       186 13-AUG-01 SCOTT    reb       SCOTT      EMP        DEPTNO20_SAL
    358210 SELECT 6,DEPTNO,ENAME,SAL FROM EMP WHERE DEPTNO = 20

       186 13-AUG-01 SCOTT    reb       SCOTT      EMP        DEPTNO20_SAL
    358189 SELECT 1,DEPTNO,ENAME,SAL FROM EMP
```

Règles d'audit détaillé

- Pour auditer toutes les instructions, utilisez une condition NULL
- Si vous tentez d'ajouter une stratégie qui existe déjà, une erreur est générée
- La table ou la vue auditée doit déjà exister lorsque vous créez la stratégie
- Si la syntaxe de la condition d'audit n'est pas valide, une erreur est générée lors de l'accès à l'objet audité
- Si la colonne d'audit n'existe pas dans la table, aucune ligne n'est auditée