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

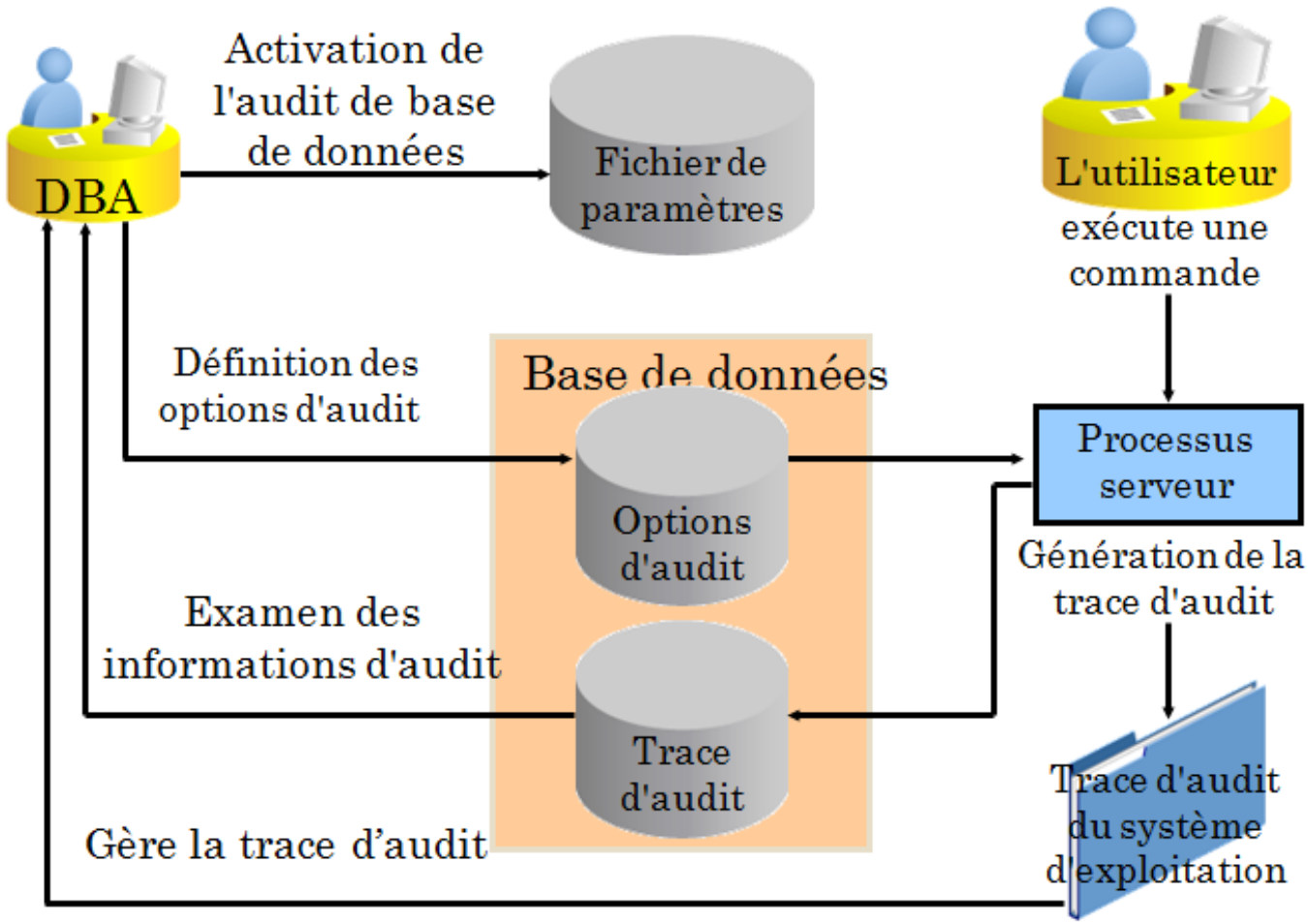
Audit de la base de données

- 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