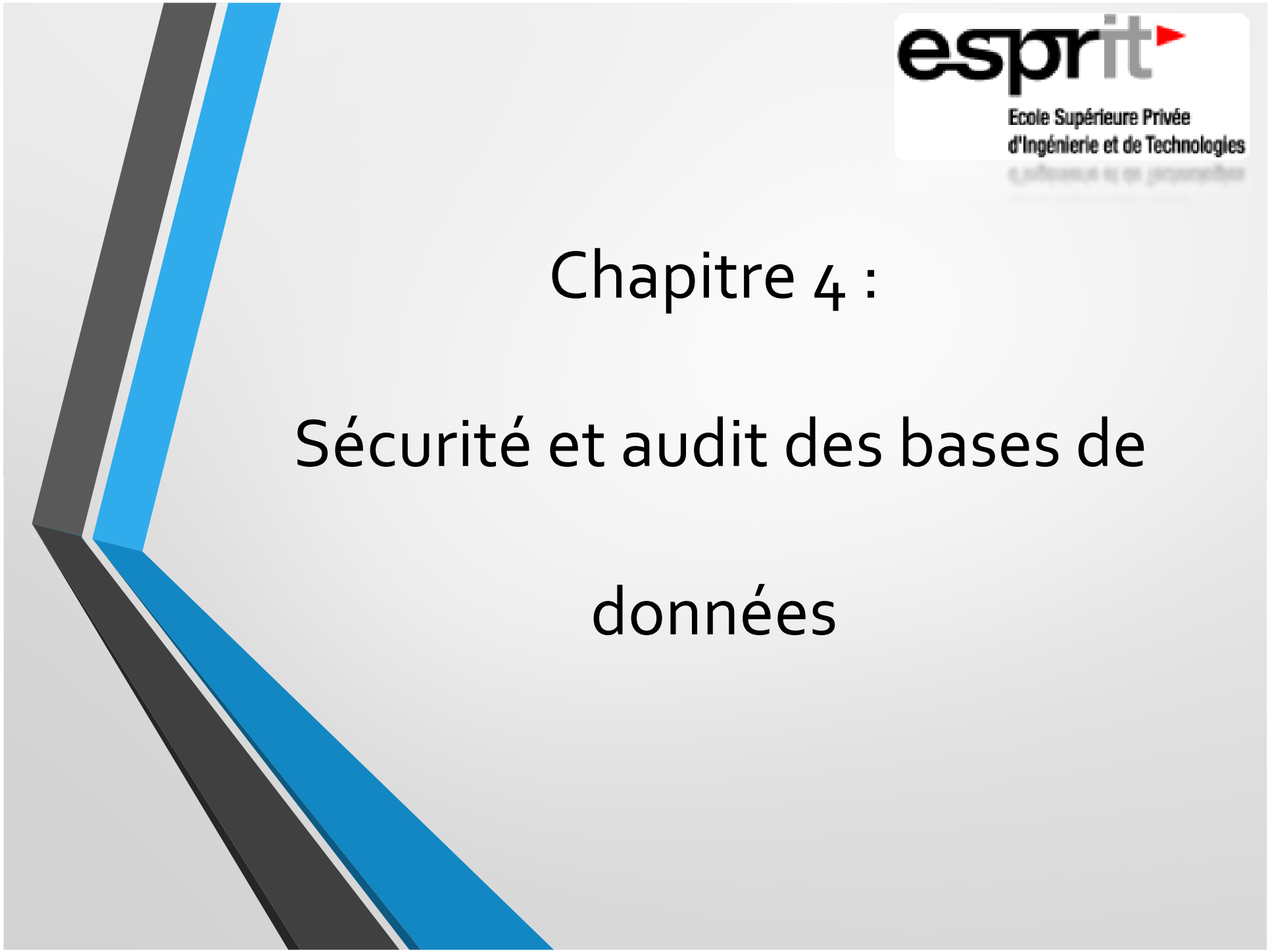

Chapitre 4 :

Sécurité et audit des bases de données

Sécurité de la base de données

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

Audit

- Une des possibilités de surveillance de l'activité de la base afin de
  - Contrôler l'accès à la base
  - Contrôler les tentatives d'accès aux objets
  - Vérifier les manipulations effectuées sur les objets
- Pour voir si une base est en mode audit :

```
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      NONE
```

Audit

- Pour activer l'audit, il faut modifier la valeur du paramètre de démarrage **AUDIT_TRAIL** dans le fichier d'initialisation ;

AUDIT_TRAIL = { none | os | db | db_extended | xml | xml_extended}.

- **AUDIT_TRAIL=none**, L'audit de la base de données Oracle est désactivé.
- **AUDIT_TRAIL = db**, les résultats seront stockés au niveau de la table d'audit
- **AUDIT_TRAIL = os**, les résultats seront stockés dans un fichier externe indiqué par le paramètre **AUDIT_FILE_DEST**
- **AUDIT_TRAIL=db_extended**. Activation de l'audit, redirection de tous les enregistrements de traces dans la table de trace avec en supplément la colonne SQL_TEXT de la table DBA_AUDIT_TRAIL renseignées.

Audit

On déclenche l'audit dans Oracle avec la commande sql **AUDIT**

Syntaxe :

AUDIT audit_option [**ON** schema.object_name] [**BY** username] [**BY** { SESSION | ACCESS }] [**WHENEVER** { SUCCESSFUL | NOT SUCCESSFUL }]

Niveaux d’audit

- On a quatre niveaux d’audit :
  - Niveau connexion (surveiller les connexions et les déconnexions)
  - Niveau ordre SQL (Par type d’ordre SQL)
  - Niveau privilège (privilège système)
  - Niveau Objet (Ordre SQL sur un objet : Ex. SELECT sur une table)
- On peut aussi surveiller les succès et les échecs et avoir une entrée d’audit par commande utilisateur ou pour la session

Déclenchement de l'audit

- Auditer les tentatives de connexions échoués

  AUDIT CONNECT WHENEVER NOT SUCCESSFUL

- Auditer tous les ordres SQL (LDD) et les connexions d'un utilisateur

  AUDIT all By user1 BY access;

- Auditer toutes les modifications de données effectuées par un utilisateur :

  AUDIT delete table, insert table, update table by user1 by access

- Auditer toutes les exécutions de procédures par un utilisateur :

  AUDIT execute procedure by user1 by access

- Auditer toutes les select et insert apportées à la table EMPLOYEES du schéma HR :

  AUDIT Select, insert on HR.Employees By access

Vues Audit (Dictionnaire)

STMT_AUDIT_OPTION_MAP	code des types d'options (INSERT ANY TABLE, ALTER ANY USER, DELETE ANY TABLE, EXECUTE ANY PROCEDURE …)
DBA_OBJ_AUDIT_OPTS	options d'audit sur tous les objets
DBA_STMT_AUDIT_OPTS	Options d'audit des instructions
DBA_PRIV_AUDIT_OPTS	options d'audit des privilèges
DBA_AUDIT_TRAIL	toutes les entrés d'audit
DBA_AUDIT_OBJECT	toutes les entrés d'audit objets
DBA_AUDIT_SESSION	les entrées d'audit concernant les connexions et déconnexions
DBA_AUDIT_STATEMENT	les entrés d'audit concernant GRANT, REVOKE, AUDIT, NOAUDIT et ALTER SYSTEM

Vérification des options d'audit

- Pour vérifier les options d'audit, il suffit de consulter les vues adéquates.

  les valeurs des colonnes des tuples sont :

  - '-' : pas d'audit

  - 'S' : par session

  - 'A' : par accès

  - A gauche de / : succès

  - A droite du / : échoue

```
SQL> audit delete,update on hr.employees whenever successful;
Audit rÚussi.
SQL> select object_name,sel,ins,upd,del from dba_obj_audit_opts ;
OBJECT_NAME                    SEL       INS       UPD       DEL
------------------------------ --------- --------- --------- ---------
EMPLOYEES                      -/-       -/-       S/-       S/-
SQL>
```

Vérification des options d'audit

- DBA_STMT_AUDIT_OPTS

```
SQL> AUDIT select table,delete table by hr by access whenever successful ;

Audit rúussi.

SQL> AUDIT execute procedure by hr by session ;

Audit rúussi.

SQL> select substr(user_name,1,3), audit_option ,success,failure from DBA_STMT_A
UDIT_OPTS where user_name='HR';

SUBSTR(USER_ AUDIT_OPTION                              SUCCESS    FAILURE
------------ ----------------------------------------- ---------- ----------
HR           SELECT TABLE                              BY ACCESS  NOT SET
HR           DELETE TABLE                              BY ACCESS  NOT SET
HR           EXECUTE PROCEDURE                         BY SESSION BY SESSION

SQL>
```

- DBA_PRIV_AUDIT_OPTS

```
SQL> AUDIT create session,create table by hr by access whenever successful ;

Audit rúussi.

SQL> select substr(user_name,1,3),privilege ,success,failure from DBA_priv_AUDIT
_OPTS where user_name='HR';

SUBSTR(USER_ PRIVILEGE                                SUCCESS    FAILURE
------------ ---------------------------------------- ---------- ----------
HR           CREATE SESSION                           BY ACCESS  NOT SET
HR           CREATE TABLE                             BY ACCESS  NOT SET

SQL>
```

Audit détaillé (DBMS_FGA)

- On peut utiliser le package prédéfini DBMS_FGA pour permettre à l'utilisateur d'auditer des actions en se basant sur des prédicats.
- Il est indépendant du paramètre AUDIT_TRAIL
- Les résultats sont stockés dans la table FGA_LOG$
- On peut vérifier que le package est installé à travers la vue dba_objects
- Si le package n'est pas installé on peut exécuter le script ***dbms_fga.sql***

DBMS_FGA (Procédures et fonctions)

- Le package dbms_fga dispose de quatre procédures et fonctions qui sont :
  - Add_Policy : création d'une politique d'audit
  - Drop_Policy : suppression d'une politique d'audit
  - Enable_Policy : activation d'une politique d'audit
  - Disable_Policy : désactivation d'une politique d'audit
- On pourra ainsi créer une politique d'audit sur une colonne d'une table par exemple et en précisant une clause where

DBMS_FGA (Création d'une stratégie d'audit)

- Se fait à travers DBMS_FGA.**ADD_POLICY**

```
PROCEDURE add_policy(
    object_schema   IN VARCHAR2 := NULL,
    object_name     IN VARCHAR2,
    policy_name     IN VARCHAR2,
    audit_condition IN VARCHAR2 := NULL,
    audit_column    IN VARCHAR2 := NULL,
    enable          IN BOOLEAN  := TRUE,
    statement_type  IN  VARCHHAR2 ,) ;
```

DBMS_FGA.ADD_POLICY

- **object_schema :** le schéma de l'objet à auditer
- **object_name** : nom de l'objet (table,vue,synonyme,..)) à auditer
- **policy_name :**nom de la stratégie d'audit
- **audit_condition :** La condition d'audit Le type d'instruction
- **audit_column :** La colonne d'audit
- **enable :** Le statut : activation (TRUE) ou désactivation (FALSE) de la stratégie d'audit
- **statement_type :** type d'instructions SQL devant être audité : select,update,delete,insert

DBMS_FGA.ADD_POLICY (Exemple)

```
exec  dbms_fga.add_policy(object_schema=>‘HR',
                          object_name=> ‘EMPLOYEES',
                          policy_name=> ‘HR_EMPLOYEES',
                          audit_condition=> ‘department_id=10’,
                          audit_column=> ‘salary,first_name',
                          enable => TRUE,
                          statement_types => 'INSERT, UPDATE’);
```

DBMS_FGA (Suite)

- **dbms_fga.drop_policy**(

  object_schema IN VARCHAR2 := NULL,

  object_name IN VARCHAR2,

  policy_name IN VARCHAR2);

Exemple : exec dbms_fga.drop_policy(‘TD8', 'Article', ' TD8_Article_Audit');

- **dbms_fga.enable_policy**(

  object_schema IN VARCHAR2 := NULL,

  object_name IN VARCHAR2,

  policy_name IN VARCHAR2

  enable IN BOOLEAN := TRUE);

Exemple: exec dbms_fga.enable_policy(TD8', ‘Article', ‘TD8_Article_Audit ', TRUE);

DBMS_FGA (Vues dictionnaire)

- **DBA_FGA_AUDIT_TRAIL :** Toutes les stratégies d'audit détaillé auxquels l'utilisateur peut accéder
- **DBA_AUDIT_POLICIES :** Toutes les stratégies d'audit détaillé