11

Sécurité de la base de données Oracle

Objectifs

A la fin de ce chapitre, vous pourrez :

- **appliquer le principe du moindre privilège**
- **gérer les comptes utilisateur par défaut**
- **implémenter des fonctionnalités standard de sécurité des mots de passe**
- **auditer l'activité de la base 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**
- **Authentifier les utilisateurs**
- **Surveiller les activités suspectes**

Appliquer le principe du moindre privilège

- Protéger le dictionnaire de données
- Révoquer les privilèges non nécessaires de `PUBLIC`
- Limiter les répertoires accessibles par les utilisateurs
- 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 prenant soin d'affecter la valeur `FALSE` au paramètre d'initialisation suivant :

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

- 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`.
- La valeur par défaut de ce paramètre est `FALSE`. S'il s'avère qu'il a la valeur `TRUE`, vérifiez qu'il y a une bonne raison pour cela.

Révoquer les privilèges non nécessaires de PUBLIC

- Révoquez tous les privilèges et rôles non nécessaires du groupe d'utilisateurs PUBLIC du serveur de base de données.
- 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
  - UTL_TCP
  - UTL_HTTP
  - UTL_FILE
  - DBMS_OBFUSCATION_TOOLKIT

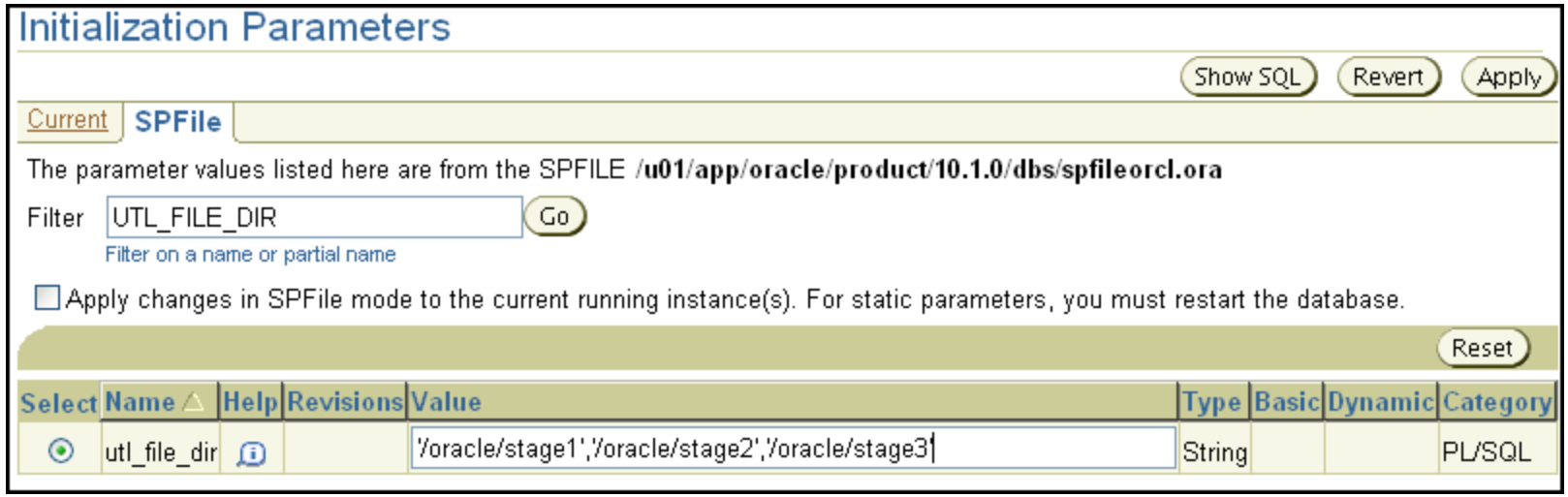
- Exemple :

```
SQL> REVOKE execute ON utl_file FROM PUBLIC;
```

Limiter les répertoires du système d'exploitation accessibles par l'utilisateur

Le paramètre de configuration `UTL_FILE_DIR` :

- **Désigne les répertoires disponibles pour les E/S de fichiers PL/SQL**
- **Permet aux utilisateurs de la base de lire ou d'écrire dans ces répertoires, sur le serveur de base de données**



Limiter les utilisateurs dotés de privilèges d'administration

- Limite 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`
  - Permissions lors de l'exécution
- Exemple : répertorier tous les utilisateurs avec le rôle `DBA` :

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

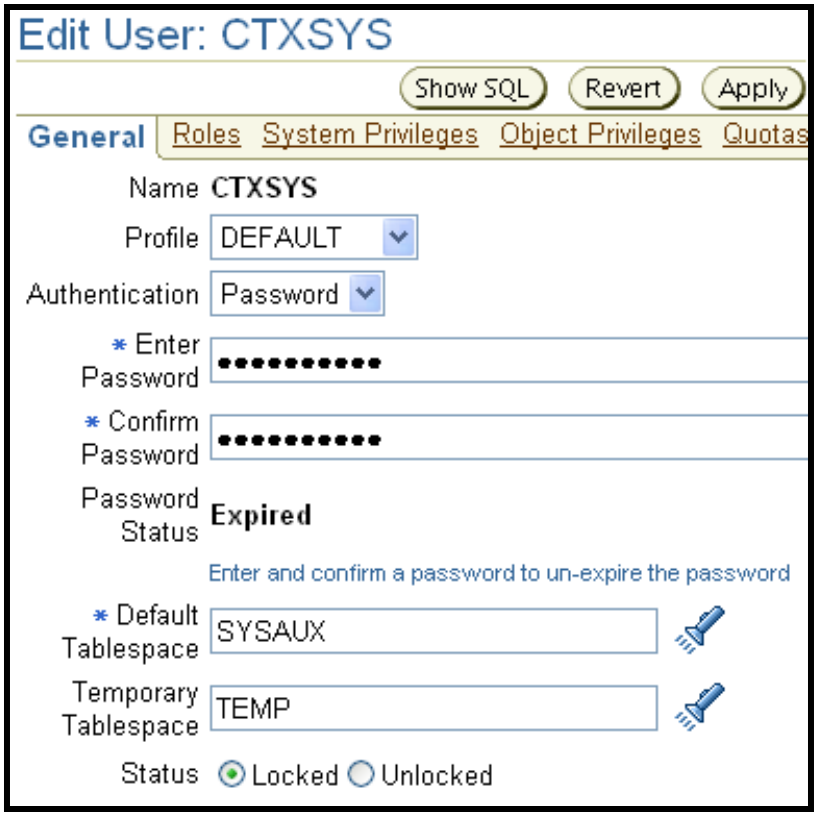
Désactiver l'authentification à distance par le système d'exploitation

- 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 la désactiver, vérifiez que la valeur par défaut est affectée au paramètre d'initialisation d'instance suivant :

```
REMOTE_OS_AUTHENT = FALSE
```

Gérer les comptes utilisateur par défaut

- **L'assistant DBCA provoque l'expiration et le verrouillage de tous les comptes, à l'exception des suivants :**
  - **SYS**
  - **SYSTEM**
  - **SYSMAN**
  - **DBSNMP**
- **Dans le cas d'une base de données créée manuellement, vous devez procéder au verrouillage et à l'expiration de tous les comptes non utilisés.**



Implémenter des fonctionnalités standard de sécurité des mots de passe

Verrouillage des comptes suite à la saisie d'un mot de passe erroné

Paramètre	Description
`FAILED_LOGIN_ATTEMPTS`	Nombre d'échecs de connexion avant le verrouillage du compte
`PASSWORD_LOCK_TIME`	Nombre de jours pendant lesquels le compte est verrouillé après le nombre déterminé d'échecs de connexion

Expiration et durée de vie des mots de passe

Paramètre	Description
PASSWORD_LIFE_TIME	Durée de vie du mot de passe, en jours, avant expiration
PASSWORD_GRACE_TIME	Période de grâce, en jours, permettant le changement de mot de passe après la première connexion réussie suite à l'expiration du mot de passe

Historique des mots de passe

Paramètre	Description
PASSWORD_REUSE_TIME	Nombre de jours pendant lesquels le mot de passe ne peut pas être réutilisé
PASSWORD_REUSE_MAX	Nombre de changements de mot de passe requis avant réutilisation du mot de passe actuel

Vérification des mots de passe

Paramètre	Description
`PASSWORD_VERIFY_FUNCTION`	Fonction PL/SQL qui effectue une vérification de complexité avant l'affectation d'un mot de passe

Les fonctions de vérification des mots de passe doivent :

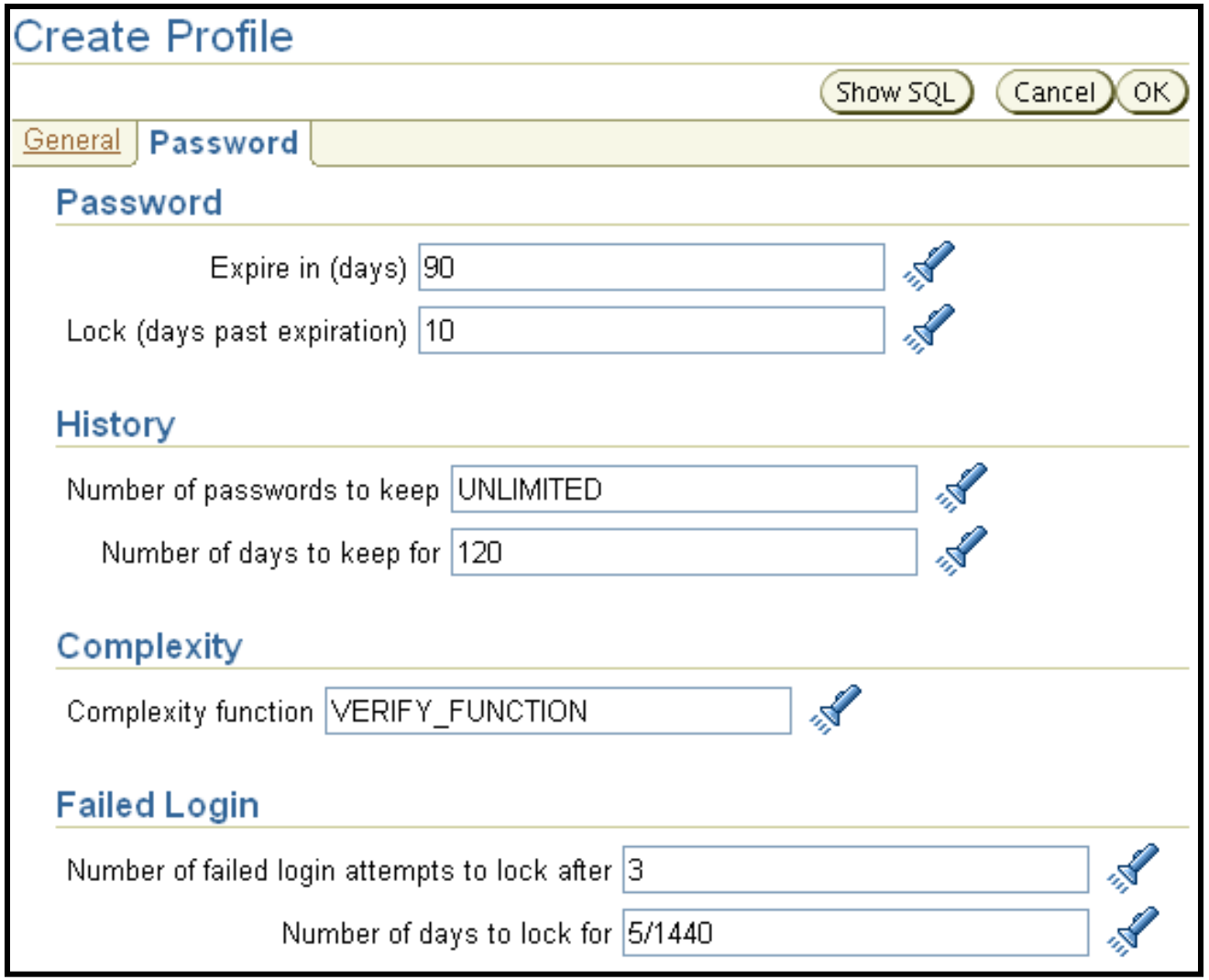
- **Appartenir à l'utilisateur `SYS`**
- **Renvoyer une valeur booléenne (true ou false)**

Fonction de vérification des mots de passe fournie : VERIFY_FUNCTION

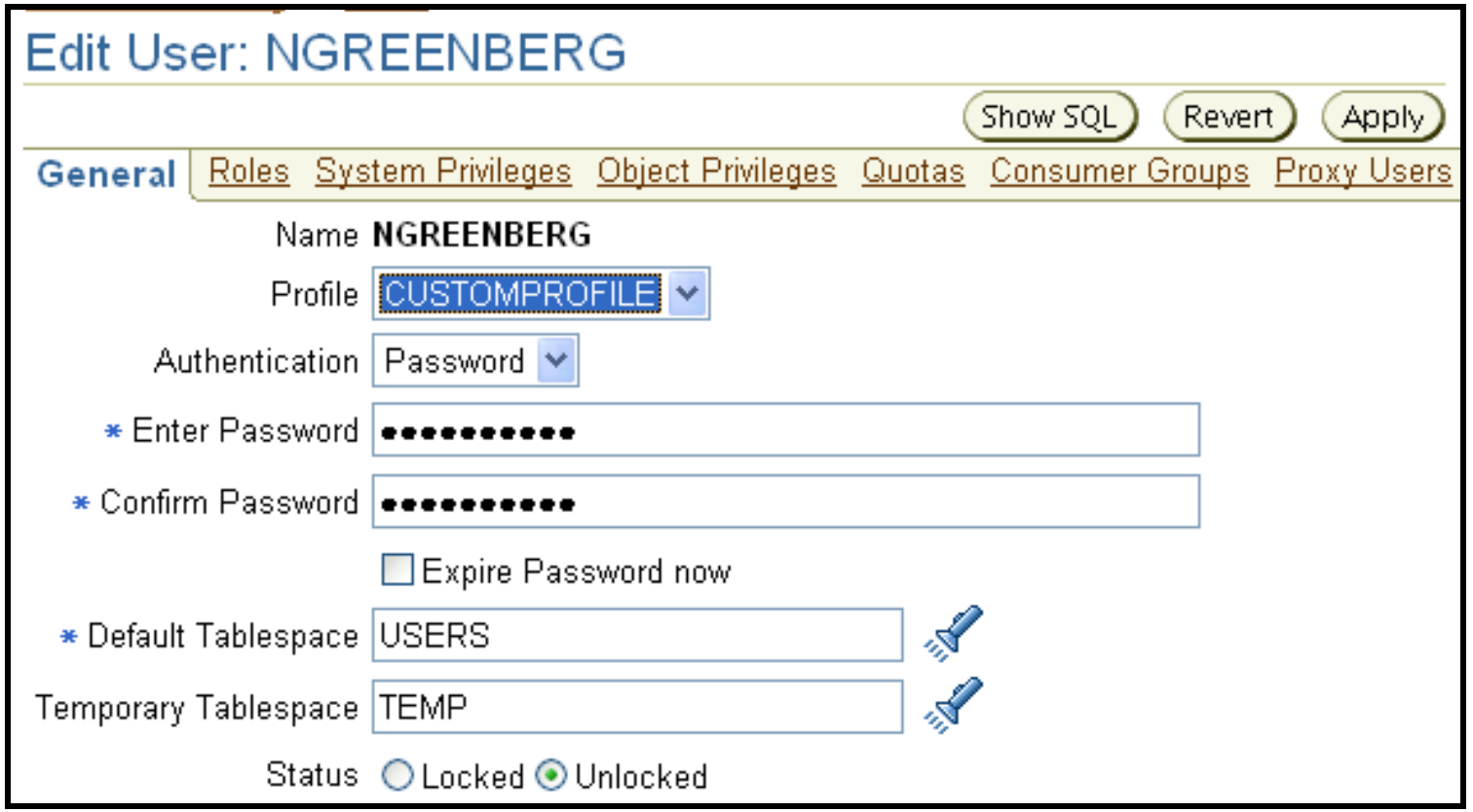
La fonction de vérification des mots de passe fournie applique les restrictions suivantes :

- **La longueur minimale est de quatre caractères.**
- **Le mot de passe ne peut pas être identique au nom utilisateur.**
- **Le mot de passe doit comporter au moins un caractère alphabétique, un chiffre et un caractère spécial.**
- **La différence entre le mot de passe et le précédent doit être d'au moins trois lettres.**

Créer un profil de mot de passe



Affecter des utilisateurs à un profil de mot de passe



Surveiller les activités suspectes

La surveillance ou l'audit doit faire partie intégrante des procédures de sécurité.

Les outils d'audit intégrés d'Oracle sont les suivants :

- **Audit de base de données**
- **Audit basé sur les données**
- **Audit détaillé (FGA)**

Comparaison entre les outils d'audit

Type d'audit	Evénements audités	Contenu de la trace d'audit
Audit de base de données standard	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 de base de données standard

Activé via le paramètre `AUDIT_TRAIL`

- `NONE` : désactive la collecte des enregistrements d'audit
- `DB` : active l'audit, enregistrements stockés dans la base de données
- `OS` : active l'audit, enregistrements stockés dans la trace d'audit du système d'exploitation

Evénements audités :

- Evénements de connexion
- Utilisation des privilèges système
- Utilisation des privilèges objet
- Utilisation d'instructions SQL

Définir les options d'audit

- Audit des instructions SQL

```
AUDIT table;
```

- Audit des privilèges système (non ciblé et ciblé)

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

- Audit des privilèges objet (non ciblé et ciblé)

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

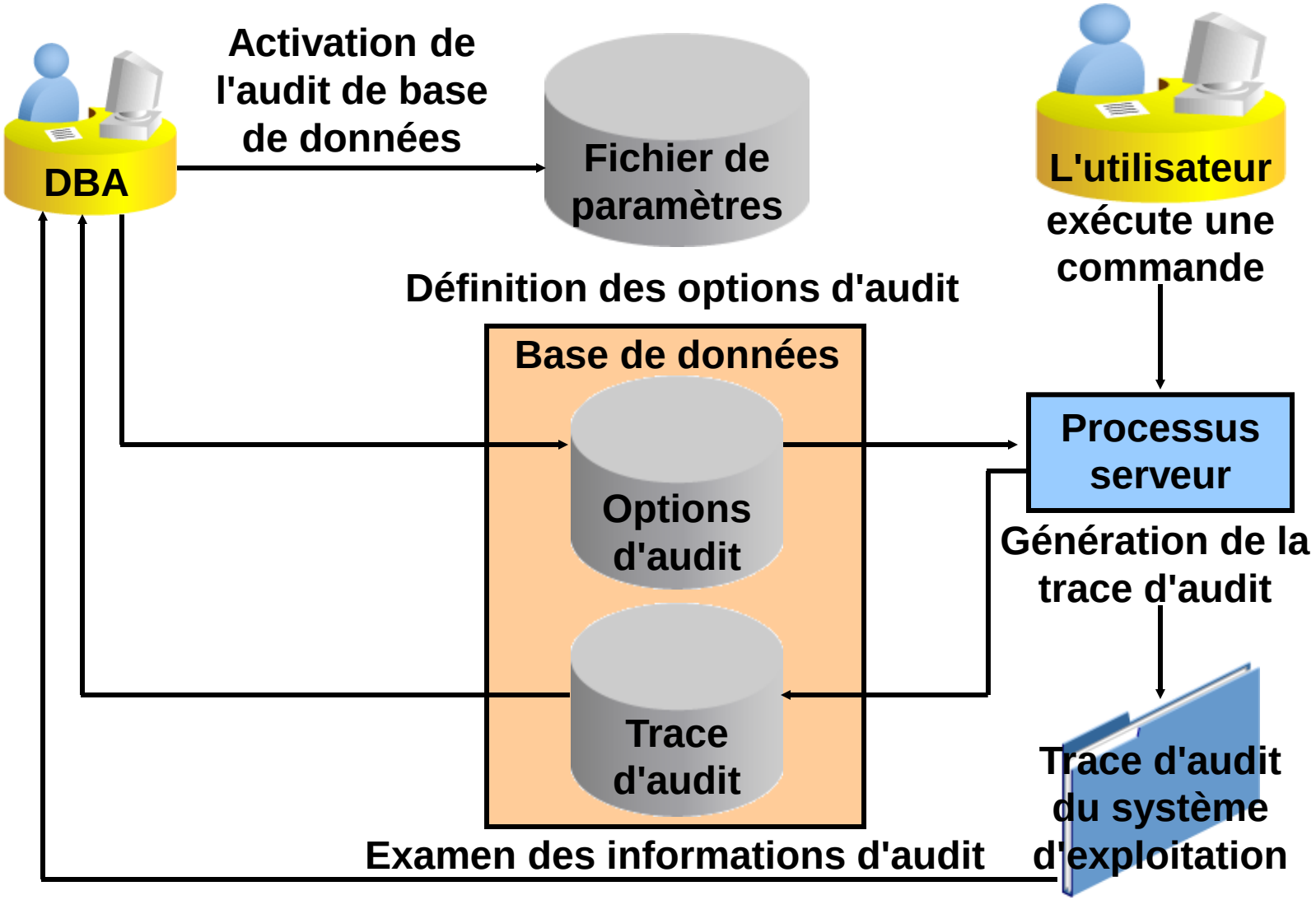
- Audit de session

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

Afficher les options d'audit

Vue du dictionnaire de données	Description
ALL_DEF_AUDIT_OPTS	Options d'audit par défaut
DBA_STMT_AUDIT_OPTS	Options d'audit des instructions
DBA_PRIV_AUDIT_OPTS	Options d'audit des privilèges
DBA_OBJ_AUDIT_OPTS	Options d'audit des objets de schéma

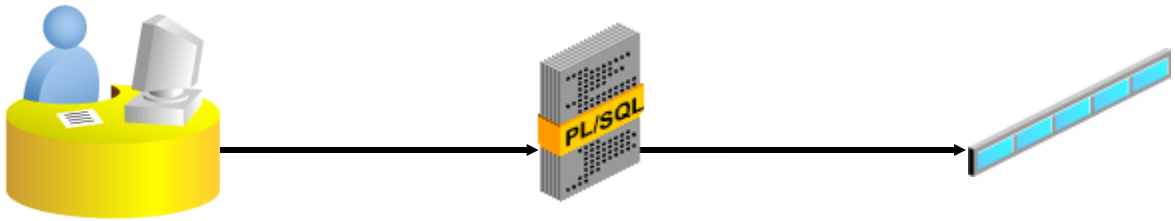
Audit de base de données standard



Afficher les résultats de l'audit

Vue de la trace d'audit	Description
DBA_AUDIT_TRAIL	Toutes les entrées de la trace d'audit
DBA_AUDIT_EXISTS	Enregistrements concernant AUDIT EXISTS/NOT EXISTS
DBA_AUDIT_OBJECT	Enregistrements concernant les objets de schéma
DBA_AUDIT_SESSION	Toutes les entrées de connexion et de déconnexion
DBA_AUDIT_STATEMENT	Enregistrements d'audit des instructions

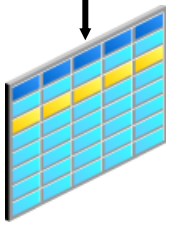
Audit basé sur les données



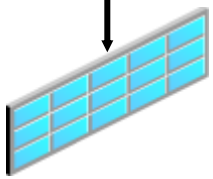
Un utilisateur apporte une modification

Un déclencheur s'exécute

Un enregistrement d'audit est créé par le déclencheur



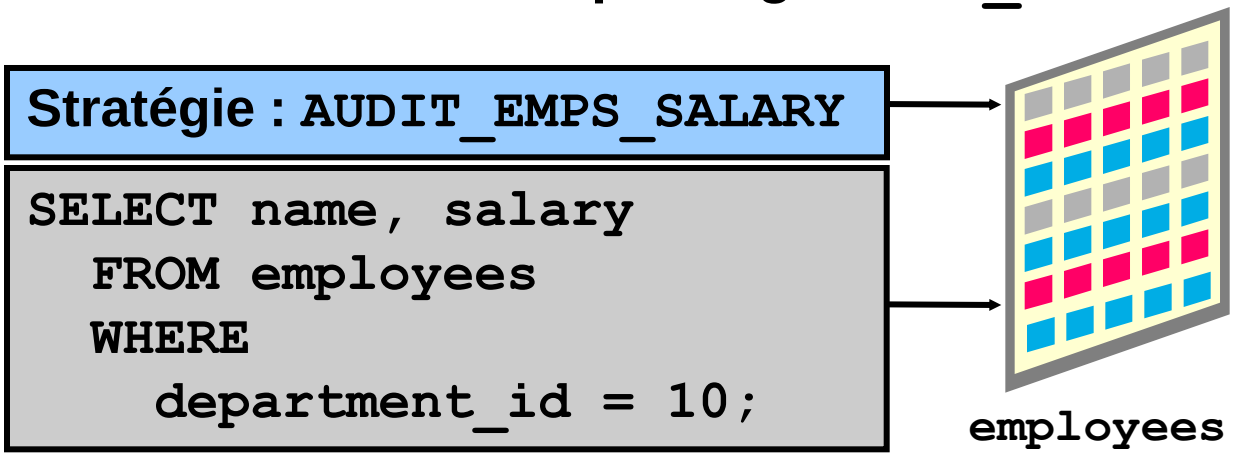
La modification de l'utilisateur est effectuée



et insérée dans une table de trace d'audit

Audit détaillé (FGA)

- 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
- Est administré via le package `DBMS_FGA`



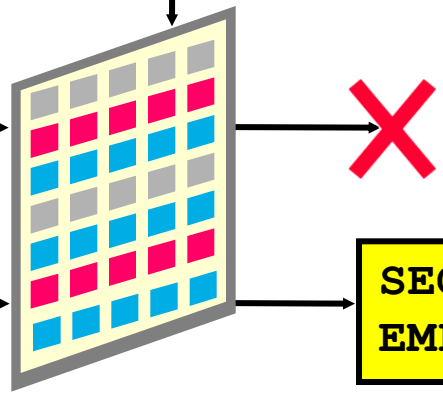
Stratégie d'audit détaillé

- Définit :
  - Les critères d'audit
  - L'action d'audit
- Est créée via `DBMS_FGA.ADD_POLICY`

```
dbms_fga.add_policy (
  object_schema  =>    'hr',
  object_name          =>    'employees',
  policy_name          =>
'audit_emps_salary',
  audit_condition=>    'dept_id=10',
  audit_column   =>    'salary',
  handler_schema =>    'secure',
  handler_module =>    'log_emps_salary',
  enable               =>    TRUE,
  statement_types=>    'select' );
```

```
SELECT name, job_id
  FROM employees;
```

```
SELECT name, salary
  FROM employees
  WHERE
    department_id = 10;
```



employees

SECURE.LOG_EMPS_SALARY

Package DBMS_FGA

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

Activer et désactiver une stratégie d'audit détaillé

- **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 d'audit détaillé

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

PL/SQL procedure successfully completed.

SQL>
```

Déclencher des événements d'audit

- Les instructions SQL suivantes provoquent un audit :

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

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

- Les instructions SQL suivantes *ne* provoquent *pas* d'audit :

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

Vues du dictionnaire de données

Nom de la vue	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

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
```

Règles relatives à l'audit détaillé

- Pour auditer toutes les instructions, utilisez une condition `null`.
- Si vous tentez d'ajouter une stratégie qui existe déjà, l'erreur ORA-28101 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 ORA-28112 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.
- Si le gestionnaire d'événements n'existe pas, aucune erreur n'est renvoyée et les enregistrements d'audit sont quand même créés.

Auditer les utilisateurs SYSDBA et SYSOPER

Les utilisateurs dotés des privilèges SYSDBA ou SYSOPER peuvent se connecter alors que la base de données est fermée.

- **La trace d'audit doit être stockée à l'extérieur de la base de données.**
- **La connexion en tant que SYSDBA ou SYSOPER est toujours auditée.**
- **Activez l'audit complémentaire des actions SYSDBA ou SYSOPER avec audit_sys_operations.**
- **Contrôlez l'emplacement de la trace d'audit avec audit_file_dest. L'emplacement par défaut est le suivant :**
  - **$ORACLE_HOME/rdbms/audit (UNIX/Linux)**
  - **Journal des événements (Windows)**

Mises à jour de sécurité

- Oracle publie les alertes de sécurité sur le site Web Oracle Technology Network, à l'adresse suivante :

  http://otn.oracle.com/deploy/security/alerts.htm

- Les administrateurs de base de données et les développeurs Oracle peuvent également s'abonner afin d'être informés par e-mail des alertes de sécurité, en cliquant sur le lien "Subscribe to Security Alerts Here".

Synthèse

Ce chapitre vous a permis d'apprendre à :

- **appliquer le principe du moindre privilège**
- **gérer les comptes utilisateur par défaut**
- **implémenter des fonctionnalités standard de sécurité des mots de passe**
- **auditer l'activité de la base de données**

Présentation de l'exercice 11-1 : Sécurité de la base de données (partie 1)

Tâches à accomplir :

- **Empêcher l'utilisation de mots de passe simples**
- **Forcer le verrouillage des comptes pendant 10 minutes après quatre échecs de connexion**
- **Exempter le serveur d'applications des changements forcés de mots de passe**
- **Auditer les tentatives réussies de connexion à la base de données**

Présentation de l'exercice 11-2 : Sécurité de la base de données (partie 2)

Tâches à accomplir :

- **Auditer les opérations SELECT sur la colonne `SALARY` de la table `EMPLOYEES`**
- **Auditer les modifications apportées à la colonne `SALARY` de la table `EMPLOYEES` et capturer :**
  - **L'ancienne valeur**
  - **La nouvelle valeur**
  - **L'utilisateur ayant apporté la modification**
  - **L'ordinateur à partir duquel la modification a été apportée**