# Administrer la sécurité utilisateur



ORACLE

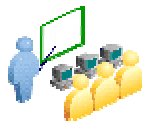
**Riadh ZAAFRANI**

2ème années SI - 2ème années SI

Mars 2010

## Objectifs du cours

- A la fin de ce cours, vous pourrez :
  - créer et gérer des comptes utilisateur de base de données
    - authentifier les utilisateurs
    - affecter des zones de stockage par défaut (tablespaces)
  - accorder et révoquer des privilèges
  - créer et gérer des rôles
  - créer et gérer des profils
    - implémenter des fonctionnalités standard de sécurité utilisant des mots de passe
    - contrôler l'utilisation des ressources par les utilisateurs



## Définitions

- Les termes suivants, qui ont trait à l'administration des utilisateurs de base de données, vous aideront à comprendre ce cours :
- Un **compte utilisateur de base de données** constitue un moyen d'organiser l'appartenance des objets de base de données et l'accès à ces objets.
- Un **mot de passe** est un mode d'authentification par la base de données Oracle.
- On nomme **privilège** le droit d'exécuter un type particulier d'instruction SQL ou d'accéder à l'objet d'un autre utilisateur.

## Définitions

- Un **rôle** est un groupe nommé de privilèges liés qui sont accordés à des utilisateurs ou à d'autres rôles.
- Les **profils** imposent un ensemble nommé de limites concernant l'utilisation de la base de données et les ressources des instances.
- Un **quota** est une allocation d'espace dans un tablespace donné. Il constitue l'un des moyens permettant de contrôler l'utilisation des ressources par les utilisateurs.

## Comptes utilisateur de base de données

- Pour accéder à la base de données, un utilisateur doit indiquer un **compte utilisateur** de base de données valide et **s'authentifier** via ce compte.
- Chaque utilisateur de base de données possède son propre compte. Cette méthode est recommandée par Oracle car elle permet d'éviter toute faille dans la sécurité et fournit des données significatives pour certaines activités d'audit.
- Chaque compte utilisateur comporte les éléments suivants :
- **Un nom utilisateur unique :** Les noms utilisateur ne peuvent pas dépasser 30 octets, ne doivent pas contenir de caractères spéciaux et doivent commencer par une lettre.

> Utilisateur
> Authentification
> Privilège
> Rôle
> Profil
> Mot de passe
> Quota



## Comptes utilisateur de base de données

- **Une méthode d'authentification :** La méthode la plus courante est l'authentification par mot de passe, mais Oracle Database 10*g* prend en charge plusieurs autres méthodes d'authentification, notamment l'authentification par biométrie, par certificat et par système tiers.
- **Un tablespace par défaut :** Il s'agit de l'emplacement dans lequel l'utilisateur crée des objets s'il n'a pas indiqué d'autre tablespace. Notez que le fait qu'un utilisateur dispose d'un tablespace par défaut n'implique pas qu'il bénéficie du *privilège* permettant de créer des objets dans ce tablespace, ni qu'il dispose d'un *quota* d'espace dans ce tablespace. En effet, les privilèges et les quotas sont accordés séparément.

## Comptes utilisateur de base de données

- **Un tablespace temporaire :** Il s'agit de l'emplacement dans lequel l'utilisateur peut créer des objets temporaires, tels que des tris et des tables temporaires.
- **Un profil utilisateur :** Il s'agit d'un ensemble de restrictions concernant les ressources et les mots de passe qui est affecté à l'utilisateur.
- **Un groupe de consommateurs de ressources :** Il est utilisé par le gestionnaire de ressources.
- **Un statut de verrouillage :** Les utilisateurs n'ont accès qu'aux comptes "déverrouillés".

## Comptes prédéfinis : SYS et SYSTEM

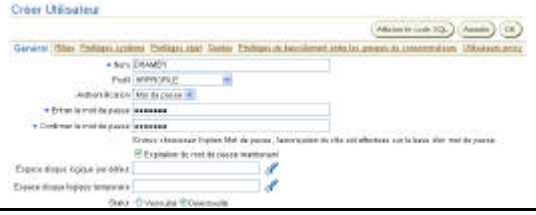
- Le rôle d'administrateur de base de données (**DBA**) est affecté par défaut aux comptes **SYS** et **SYSTEM**.
- Le compte **SYS** dispose, en outre, de tous les privilèges associés à **ADMIN OPTION**. Il est également le propriétaire du dictionnaire de données.
- Pour vous connecter au compte **SYS**, vous devez utiliser la clause **AS SYSDBA**. Tout utilisateur qui dispose du privilège **SYSDBA** peut se connecter au compte **SYS** à l'aide de la clause **AS SYSDBA**.
- De plus, seuls les utilisateurs bénéficiant du privilège **SYSDBA** ou **SYSOPER** sont autorisés à démarrer et arrêter l'instance de base de données. Le compte **SYSTEM** a par défaut le rôle DBA, mais pas le privilège **SYSDBA**.

## Comptes prédéfinis : SYS et SYSTEM

- Les comptes **SYS** et **SYSTEM** sont obligatoires dans la base de données. Par conséquent, vous ne pouvez pas les supprimer.
- Selon le principe du moindre privilège, ces comptes ne sont pas utilisés pour les opérations de routine. Les utilisateurs qui ont besoin de privilèges DBA disposent de comptes distincts auxquels sont affectés les privilèges requis.
- Ainsi, Jim peut avoir un compte ayant peu de privilèges, nommé **jim**, et un compte doté de privilèges élevés, appelé **jim_dba**. Cette méthode permet d'appliquer le principe du moindre privilège. Elle élimine tout besoin de recourir à un partage de compte et permet de réaliser des audits sur des actions individuelles.

## Créer un utilisateur

- Dans Enterprise Manager, vous pouvez gérer la liste des utilisateurs de base de données autorisés à accéder à la base actuelle, via la page Users. Dans cette page, vous pouvez créer, supprimer et modifier les paramètres d'un utilisateur.
- Pour créer un utilisateur de base de données, procédez de la manière suivante :
  1. Dans Enterprise Manager Database Control, sélectionnez **Administration > Schéma > Utilisateurs et privilèges > Utilisateurs**.
  2. Cliquez sur le bouton **Créer**. Fournissez les informations requises.




## Authentification des utilisateurs

- L'authentification consiste à vérifier l'identité d'une entité (utilisateur, périphérique ou autre) qui souhaite utiliser des données, des ressources ou des applications. La validation de cette identité établit une relation de confiance pour les interactions ultérieures. L'authentification permet également la responsabilisation, car il est possible de lier l'accès et les actions à des identités spécifiques. Après l'authentification, le processus d'autorisation peut autoriser ou restreindre l'accès et les actions associés à cette entité.
- Lorsque vous créez un utilisateur, vous devez décider de la technique d'authentification à utiliser, laquelle pourra être modifiée ultérieurement.






## Authentification des utilisateurs

- **Password :** Ce mode est appelé authentification par la base de données Oracle. Associez à chaque utilisateur créé un mot de passe qu'il devra saisir lors de chaque connexion. Lorsque vous définissez un mot de passe, vous pouvez le configurer afin qu'il expire immédiatement, ce qui oblige l'utilisateur à le changer lors de la première connexion. Dans ce cas, assurez-vous que les utilisateurs ont la possibilité de changer le mot de passe. Certaines applications n'offrent pas cette possibilité.
- Les mots de passe sont toujours cryptés de manière automatique et transparente lors des connexions réseau (client/serveur et serveur/serveur), à l'aide d'un algorithme DES (Data Encryption Standard), et ce avant d'être envoyés sur le réseau.

## Authentification des utilisateurs

- **External :** Ce mode est appelé authentification par le système d'exploitation. Les utilisateurs peuvent se connecter à la base de données Oracle sans fournir de nom utilisateur ou de mot de passe. Avec l'authentification externe, la base de données utilise le système d'exploitation sous-jacent ou le service d'authentification réseau pour limiter l'accès aux comptes de base de données. Aucun mot de passe de base de données n'est utilisé pour ce type de connexion.
- **Global :** Associée à l'option Oracle Advanced Security, l'authentification globale (qui est une authentification forte) permet l'identification des utilisateurs via la biométrie, les certificats x509, les systèmes tiers et Oracle Internet Directory.

## Authentification de l'administrateur

- Sécurité au niveau du système d'exploitation
  - Les administrateurs de base de données doivent disposer des privilèges de création et de suppression de fichiers au niveau du système d'exploitation.
  - Les utilisateurs de base de données ne bénéficient normalement pas des privilèges de création ou de suppression de fichiers de base de données au niveau du système d'exploitation.
- Sécurité au niveau de l'administrateur
  - Les connexions SYSBA et SYSOPER ne sont autorisées qu'après une vérification basée sur le fichier de mots de passe, ou les privilèges et permissions définis au niveau du système d'exploitation. .
    - L'authentification par fichier de mots de passe enregistre l'utilisateur DBA par son nom.
    - L'authentification par le système d'exploitation n'enregistre pas l'utilisateur.
    - L'authentification par le système d'exploitation est prioritaire sur l'authentification par fichier de mots de passe pour les privilèges SYSDBA et SYSOPER.

## Déverrouiller un compte utilisateur et redéfinir le mot de passe

- Vous pouvez déverrouiller plusieurs des comptes utilisateur définis par Oracle et redéfinir les mots de passe associés, en sélectionnant un utilisateur dans la page **Utilisateurs**, puis en cliquant sur **Déverouiller l'utilisateur**.




## Déverrouiller un compte utilisateur et redéfinir le mot de passe

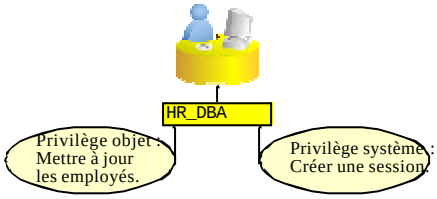
- Vous pouvez également effectuer les opérations suivantes dans la page **Modifier Utilisateur** :
  - 1. Entrez le nouveau mot de passe dans les champs **Entrer le mot de passe** et **Confirmer le mot de passe**.
  - 2. Cochez la case **Déverrouillé**.
  - 3. Cliquez sur **Appliquer** pour redéfinir le mot de passe et déverrouiller le compte utilisateur.




## Privilèges

- La base de données Oracle vous permet de contrôler les opérations que les utilisateurs peuvent effectuer ou non au sein de la base. Il existedeux types de privilège utilisateur :
  - Système : permet aux utilisateurs d'effectuer des actions particulières dans la base de données
  - Objet : permet aux utilisateurs d'accéder à un objet spécifique et de le manipuler

Utilisateur
Authentification
> **Privilège**
**Rôle**
**Profil**
**Mot de passe**
**Quota**




## Privilèges

- **Privilèges système :** Chaque privilège système autorise un utilisateur à effectuer une certaine opération de base de données ou une certaine classe d'opérations. Par exemple, le privilège permettant de créer des tablespaces est un privilège système. Les privilèges système peuvent être accordés par l'administrateur ou par quelqu'un à qui la permission d'administrer le privilège a été accordée explicitement. Il existe plus d'une centaine de privilèges système différents. Un grand nombre d'entre eux contiennent la clause **ANY**.
- **Privilèges objet :** Les privilèges objet permettent à un utilisateur d'effectuer une action particulière sur un objet spécifique, tel qu'une table, une vue, une séquence, une procédure, une fonction ou un package. Sans permission spécifique, les utilisateurs ne peuvent accéder qu'à leurs propres objets. Les privilèges objet peuvent être octroyés par le propriétaire d'un objet, par l'administrateur, ou par un utilisateur auquel la permission d'accorder des privilèges sur l'objet a été attribuée explicitement.

## Privilèges système

- Pour accorder des privilèges système, cliquez sur l'onglet **Privilèges système** de la page **Modifier Utilisateur**. Sélectionnez les privilèges appropriés dans la liste des privilèges disponibles, puis déplacez-les vers la liste Privilèges système disponibles en cliquant sur le bouton Déplacer.



## Privilèges système

- Les privilèges contenant la clause **ANY** s'étendent au-delà des limites du schéma Par exemple, le privilège **CREATE TABLE** vous permet de créer une table, mais uniquement dans votre propre schéma. Le privilège **SELECT ANY TABLE** vous permet, quant à lui, d'effectuer une opération **SELECT** dans des tables appartenant à d'autres utilisateurs.
- Cochez la case **Option d'administration(Admin Option)** pour pouvoir administrer le privilège système considéré et l'accorder à d'autres utilisateurs.
- Tenez bien compte des exigences de sécurité avant d'octroyer des permissions système Certains privilèges système sont généralement accordés uniquement aux administrateurs :
- **RESTRICTED SESSION :** Ce privilège vous autorise à vous connecter même si la basede données a été ouverte en mode d'accès restreint.

## Privilèges système

- **SYSDBA et SYSOPER :** Ces privilèges vous autorisent à arrêter et à démarrer la base de données, ainsi qu'à effectuer des opérations de récupération et d'autres tâches d'administration. **SYSOPER** vous permet d'effectuer des tâches opérationnelles de base, mais ne vous autorise pas à voir les données utilisateur. Il inclut les privilèges système suivants :
  - ✓ `STARTUP` et `SHUTDOWN`
  - ✓ `CREATE SPFILE`
  - ✓ `ALTER DATABASE OPEN/MOUNT/BACKUP`
  - ✓ `ALTER DATABASE ARCHIVELOG`
  - ✓ `ALTER DATABASE RECOVER` (Récupération complète uniquement. Pour toute forme de récupération incomplète, telle que `UNTIL TIME|CHANGE|CANCEL|CONTROLFILE`, vous devez vous connecter en tant que `SYSDBA`.)
  - ✓ `RESTRICTED SESSION`
- Le privilège système **SYSDBA** autorise également les opérations de récupération incomplète et la suppression d'une base de données. En fait, il autorise un utilisateur à se connecter en tant qu'utilisateur **SYS**.

## Privilèges système

- **DROP ANY *object* :** Le privilège **DROP ANY** vous permet de supprimer des objets qui appartiennent à d'autres utilisateurs du schéma.
- **CREATE, MANAGE, DROP et ALTER TABLESPACE :** Ces privilèges permettent les opérations d'administration des tablespaces, notamment la création, la suppression et la modification des attributs.
- **CREATE ANY DIRECTORY :** La base de données Oracle autorise les développeurs à appeler du code externe (par exemple une bibliothèque C) à partir de code PL/SQL. Pour des raisons de sécurité, le répertoire du système d'exploitation dans lequel réside le code doit être lié à un objet de répertoire Oracle virtuel. Avec le privilège `CREATE ANY DIRECTORY`, vous pouvez potentiellement appeler des objets de code non sécurisés.

## Privilèges système

- Le privilège `CREATE ANY DIRECTORY` permet à un utilisateur de créer un objet répertoire (Directory) avec un accès en lecture et en écriture pour tous les répertoires auxquels le propriétaire du logiciel Oracle a accès. Cela signifie que l'utilisateur peut accéder aux procédures externes figurant dans ces répertoires. Il peut tenter d'effectuer des opérations de lecture et d'écriture directement dans un fichier de base de données (fichier de données, fichier de journalisation (redo log) et journal d'audit, par exemple). Assurez-vous que votre organisation dispose d'une stratégie de sécurité qui évite toute mauvaise utilisation de privilèges puissants tels que celui-ci.
- **GRANT ANY OBJECT PRIVILEGE :** Ce privilège vous autorise à accorder des permissions sur des objets qui ne vous appartiennent pas.
- **ALTER DATABASE et ALTER SYSTEM :** Très puissants, ces privilèges vous autorisent à modifier la base de données et l'instance Oracle. Vous pouvez, par exemple, renommer un fichier de données ou vider le cache de tampons (buffer cache).

## Privilèges objet

- Pour accorder des privilèges objet, cliquez sur l'onglet **Privilèges objet** de la page **Modifier Utilisateur**. Sélectionnez le type d'objet pour lequel vous voulez octroyer des privilèges, puis cliquez sur le bouton **Ajouter**.



## Privilèges objet

- Indiquez les objets concernés sous la forme <*nom_utilisateur.nom_objet*> ou sélectionnez-les dans la liste.
- Sélectionnez ensuite les privilèges appropriés dans la liste **Privilèges disponibles**, puis cliquez sur le bouton **Déplacer**. Une fois les privilèges sélectionnés, cliquez sur OK.
- Dans la page **Modifier Utilisateur**, cochez la case **Option d'autorisation** (Grant) si l'utilisateur est autorisé à octroyer le même accès aux autres utilisateurs.

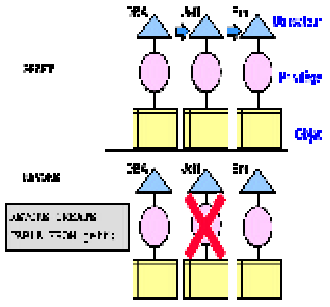



## Révoquer des privilèges système accordés avec ADMIN OPTION

- Les privilèges système qui ont été octroyés directement à l'aide de la commande **GRANT** peuvent être révoqués via l'instruction SQL **REVOKE**.
- Les utilisateurs disposant de l'option **ADMIN OPTION** pour un privilège système peuvent révoquer ce privilège pour tout autre utilisateur de la base de données. La révocation peut être effectuée par un utilisateur différent de celui qui a initialement octroyé le privilège.
- Aucune répercussion en cascade ne se produit lorsqu'un privilège système est révoqué, que celui-ci ait été ou non accordé avec l'option **ADMIN OPTION**.
- A titre d'exemple, considérons le scénario ci-après.

## Révoquer des privilèges système accordés avec ADMIN OPTION

- **Scénario**
- 1. L'administrateur de base de données (DBA) octroie à Jeff le privilège système **CREATE TABLE**, avec l'option **ADMIN OPTION**.
- 2. Jeff crée une table.
- 3. Jeff accorde le privilège système **CREATE TABLE** à Emi.
- 4. Emi crée une table.
- 5. Le DBA révoque le privilège système **CREATE TABLE** pour Jeff.
- **Résultat**
- La table de Jeff existe toujours mais aucune autre table ne peut être créée.
- La table d'Emi existe toujours et Emi conserve le privilège système **CREATE TABLE**.

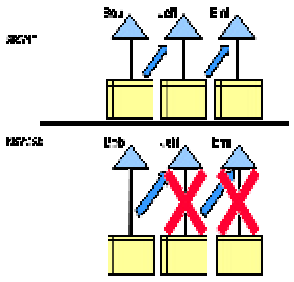



## Révoquer des privilèges système accordés avec GRANT OPTION

- Des effets en cascade peuvent être observés lors de la révocation d'un privilège système lié à une opération LMD (Langage de manipulation de données).
- Par exemple, si le privilège **SELECT ANY TABLE** est octroyé à un utilisateur et que ce dernier a créé des procédures qui utilisent la table concernée, toutes les procédures contenues dans le schéma de l'utilisateur doivent être recompilées pour pouvoir être utilisées à nouveau.
- La révocation de privilèges objet accordés avec l'option **WITH GRANT OPTION** produit également des effets en cascade.

## Révoquer des privilèges système accordés avec GRANT OPTION

- A titre d'exemple, considérons le scénario ci-après.
- **Scénario**
- 1. Jeff se voit octroyer le privilège objet **SELECT** sur la table **EMPLOYEES**, avec l'option **GRANT OPTION**.
- 2. Jeff accorde à Emi le privilège **SELECT** sur la table **EMPLOYEES**.
- 3. Ultérieurement, le privilège **SELECT** de Jeff est révoqué. Cette révocation est répercutée sur Emi.




## Avantages des rôles

- **Gestion simplifiée des privilèges :** Utilisez des rôles pour simplifier la gestion des privilèges. Plutôt que d'accorder le même ensemble de privilèges à plusieurs utilisateurs, vous pouvez accorder ces privilèges à un rôle, puis octroyer ce rôle à chaque utilisateur.




- **Gestion dynamique des privilèges :** Si les privilèges associés à un rôle sont modifiés, tous les utilisateurs auxquels ce rôle est accordé bénéficient automatiquement et immédiatement des privilèges modifiés.
- **Disponibilité sélective des privilèges :** Les rôles peuvent être activés et désactivés afin d'activer ou de désactiver temporairement les privilèges correspondants. L'activation d'un rôle peut également être utilisée pour vérifier que le rôle a été accordé à un utilisateur.

## Affecter des privilèges à des rôles et des rôles à des utilisateurs

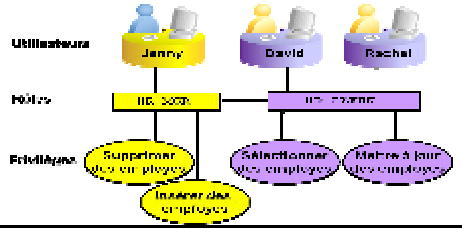
- Dans la plupart des systèmes, il est trop fastidieux d'accorder à chaque utilisateur les privilèges nécessaires et le risque d'erreur est trop important. Le logiciel Oracle permet la gestion facile et contrôlée des privilèges par l'intermédiaire de rôles.
- Les rôles sont des **groupes nommés de privilèges liés** qui sont accordés aux utilisateurs ou à d'autres rôles. Ils sont conçus pour faciliter l'administration des privilèges dans la base de données, et donc améliorer la sécurité.

## Affecter des privilèges à des rôles et des rôles à des utilisateurs

- **Caractéristiques des rôles**
  - Les privilèges sont accordés aux rôles (et révoqués) comme si le rôle était un utilisateur.
  - Les rôles peuvent être accordés aux utilisateurs ou à d'autres rôles (et révoqués) comme s'il s'agissait de privilèges système.
  - Un rôle peut être constitué de privilèges système et objet.
  - Un rôle peut être activé ou désactivé pour chaque utilisateur auquel il est accordé.
  - L'activation d'un rôle peut nécessiter un mot de passe.
  - Les rôles n'appartiennent à personne et ne résident dans aucun schéma.

## Affecter des privilèges à des rôles et des rôles à des utilisateurs

- Dans l'exemple, les privilèges **SELECT** et **UPDATE** sont accordés au rôle **HR_CLERK** sur la table **employees**. Les privilèges **DELETE** et **INSERT** sur la table **employees**, *ainsi que* le rôle **HR_CLERK**, sont accordés au rôle **HR_MGR**. Le rôle **HR_MGR** est accordé au manager, lequel peut à présent effectuer des sélections, des suppressions, des insertions et des mises à jour dans la table **employees**.




## Rôles prédéfinis

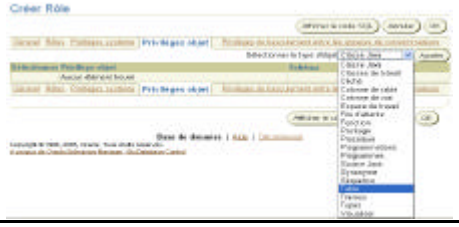
- Il existe plusieurs rôles qui sont définis automatiquement pour les bases de données Oracle lorsque vous exécutez les scripts de création de la base.
- Le rôle **CONNECT** est accordé automatiquement à tout utilisateur créé avec Enterprise Manager. Dans les versions antérieures (avant Oracle Database 10*g* Release 2), le rôle **CONNECT** incluait davantage de privilèges, tels que **CREATE TABLE** et **CREATE DATABASE LINK**. Ces privilèges ont été supprimés pour des raisons de sécurité.
- D'autres rôles permettant l'administration de fonctions spéciales sont créés lors de l'installation des fonctions correspondantes.
- Par exemple, le rôle **XDBADMIN** dispose des privilèges requis pour administrer XML Database si cette fonctionnalité est installée.

## Rôles prédéfinis

| | |
|---|---|
| **CONNECT** | **CREATE SESSION** |
| **RESOURCE** | **CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE** |
| **SCHEDULER_ ADMIN** | **CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER** |
| **DBA** | **La plupart des privilèges système et plusieurs autres rôles. Ce rôle ne doit pas être accordé aux utilisateurs qui ne sont pas administrateurs.** |
| **SELECT_ CATALOG_ ROLE** | **Aucun privilège système, mais le rôle HS_ADMIN_ROLE et plus de 1 700 privilèges objet sur le dictionnaire de données.** |

## Créer un rôle

- Un **rôle** est un groupe nommé de privilèges liés qui sont accordés à des utilisateurs ou à d'autres rôles. Un administrateur de base de données (DBA) gère les privilèges via des rôles. Pour créer un rôle, procédez de la manière suivante :
  - 1. Dans Enterprise Manager Database Control, sélectionnez Administration > Schéma > Utilisateurs et privilèges > Rôles.
  - 2. Cliquez sur le bouton Créer.



## Rôles sécurisés

- Les rôles sont généralement activés par défaut, ce qui signifie que si un rôle est accordé à un utilisateur, cet utilisateur peut exercer les privilèges accordés à ce rôle. Vous pouvez effectuer les opérations suivantes :
  - Rendre un rôle **inactif** par défaut. Lorsque le rôle est affecté à un utilisateur, désélectionnez la case **Valeur par défaut(DEFAULT)**. L'utilisateur doit à présent activer explicitement le rôle pour pouvoir exercer les privilèges correspondants.
  - Configurer un rôle afin qu'il nécessite une **authentification**. L'authentification par défaut d'un rôle est **Aucune(None)**, mais il est possible de configurer le rôle afin qu'il ne puisse être activé qu'après authentification.




## Rôles sécurisés

- Créer des rôles applicatifs sécurisés qui ne peuvent être activés que via l'exécution d'une procédure PL/SQL.
- La procédure PL/SQL peut vérifier des éléments tels que l'adresse réseau de l'utilisateur, le programme exécuté par l'utilisateur, l'heure ou tout autre élément nécessaire pour sécuriser correctement un groupe de permissions.

```
CREATE ROLE secure_application_role
IDENTIFIED USING  <security_procedure_name>;
```

## Affecter des rôles aux utilisateurs

- Un **rôle** est un ensemble de privilèges pouvant être accordés à des utilisateurs ou à d'autres rôles. Vous pouvez utiliser les rôles pour administrer les privilèges de base de données. Vous pouvez ajouter des privilèges à un rôle, puis accorder le rôle à un utilisateur. L'utilisateur peut alors activer le rôle et exercer les privilèges octroyés par ce rôle. Un rôle a tous les privilèges qui lui ont été accordés, ainsi que tous les privilèges des autres rôles qui lui sont affectés.
- Par défaut, Enterprise Manager accorde automatiquement le rôle **CONNECT** aux nouveaux utilisateurs. Ces derniers peuvent ainsi se connecter à la base de données et créer des objets dans leur propre schéma.

## Affecter des rôles aux utilisateurs

- Pour affecter un rôle à un utilisateur, procédez de la manière suivante :
  1. Dans Enterprise Manager Database Control, sélectionnez **Administration** > **Schéma** > **Utilisateurs et privilèges** > **Utilisateurs**.
  2. Sélectionnez l'utilisateur, puis cliquez sur le bouton Modifier.
  3. Cliquez sur l'onglet Rôles, puis sur le bouton **Modifier la liste**.
  4. Sous **Rôles disponibles**, sélectionnez le rôle souhaité et déplacez-le sous **Rôles sélectionnés**.
  5. Une fois que vous avez affecté tous les rôles appropriés, cliquez sur le bouton **OK**.



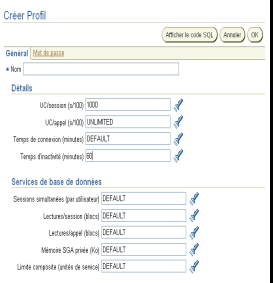

## Profils et utilisateurs

- Les **profils** imposent un ensemble nommé de **limites** concernant l'utilisation de la base de données et les ressources des instances.
- Les profils gèrent également le **statut des comptes** et imposent des restrictions sur les mots de passe des utilisateurs (longueur, délai d'expiration, etc.).
- Chaque utilisateur se voit affecter un profil et ne peut appartenir qu'à un seul profil à la fois. Si des utilisateurs sont connectés lorsque vous modifiez leur profil, le changement ne prend effet que lors de leur prochaine connexion.




## Profils et utilisateurs

- Le profil par défaut sert de base pour tous les autres profils. Comme l'illustre cette diapositive, les limitations associées à un profil peuvent être définies implicitement (**CPU/Session**), être illimitées (**CPU/appel**) ou faire référence à un paramètre du profil par défaut (**Temps de connection**).
- Les profils ne peuvent imposer des limitations de ressources aux utilisateurs que si la valeur **TRUE** est affectée au paramètre d'initialisation **RESOURCE_LIMIT**. Avec la valeur par défaut (**FALSE**) de **RESOURCE_LIMIT**, les limitations des profils sont ignorées.



## Profils et utilisateurs

- Les profils permettent à l'administrateur de contrôler les ressources système suivantes :
- **CPU :** Les ressources CPU peuvent être limitées par session ou par appel. Avec une limite **CPU/Session** de 1 000, une session qui utilise ce profil et qui consomme plus de 10 secondes de temps CPU (les limites de temps CPU étant exprimées en centièmes de seconde) reçoit une erreur et est déconnectée :
  - ORA-02392: exceeded session limit on CPU usage, you are being logged off
- Une limitation par appel a le même effet, mais au lieu de limiter la session globale de l'utilisateur, elle empêche chaque commande de consommer trop de temps CPU. Si une limite **CPU/Call** est définie et que l'utilisateur la dépasse, la commande s'arrête et l'utilisateur reçoit un message d'erreur semblable à ce qui suit :
  - ORA-02393: exceeded call limit on CPU usage

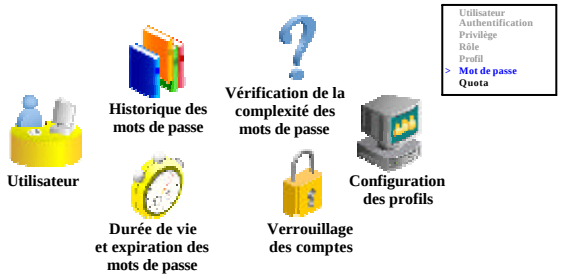
## Profils et utilisateurs

- **Network/Memory :** Chaque session de base de données consomme des ressources mémoire du système et (si la session est ouverte par un utilisateur qui ne se trouve pas en local sur le serveur) des ressources réseau. Vous pouvez définir les éléments suivants :
  - **Connect Time :** Indique le nombre de minutes pendant lesquelles un utilisateur peut rester connecté avant d'être automatiquement déconnecté
  - **Idle Time :** Définit le nombre de minutes pendant lesquelles la session d'un utilisateur peut rester inactive avant d'être automatiquement déconnectée. Le temps d'inactivité est calculé pour le processus serveur uniquement. Il ne tient pas compte de l'activité des applications. La limite `IDLE_TIME` n'est pas affectée par les interrogations longues et les autres opérations.
  - **Concurrent Sessions :** Indique le nombre de sessions simultanées pouvant être créées à l'aide d'un compte utilisateur de base de données.

## Profils et utilisateurs

- **Private SGA :** Limite la quantité d'espace consommé dans la mémoire SGA (System Global Area) pour le tri, la fusion de bitmaps, etc. Cette restriction ne prend effet que si la session utilise un serveur partagé.
- **Disk I/O :** Cette option limite la quantité de données qu'un utilisateur peut lire, par session ou par appel. Les options Reads/Session et Reads/Call limitent le nombre total de lectures réalisées à partir de la mémoire et du disque. Elles permettent de s'assurer, par exemple, qu'aucune instruction consommant beaucoup d'E/S n'utilise trop intensément la mémoire et les disques.
- Les profils autorisent également une limite composite. Les limites composites sont basées sur une combinaison pondérée des limites CPU/Session, Reads/Session, Connect Time et Private SGA.
- Pour créer un profil, sélectionnez Administration > Schéma > Utilisateurs et privilèges > Profils, puis cliquez sur le bouton Créer.

## Implémenter des fonctionnalités de sécurité utilisant des mots de passe




## Implémenter des fonctionnalités de sécurité utilisant des mots de passe

- La gestion des mots de passe Oracle est implémentée par l'intermédiaire de profils utilisateur. Les profils peuvent fournir de nombreuses fonctionnalités de sécurité standard, telles que :
- **Verrouillage des comptes :** Permet le verrouillage automatique des comptes pour une durée définie lorsque les utilisateurs ne parviennent pas à se connecter au système après un nombre déterminé de tentatives.
  - Le paramètre **`FAILED_LOGIN_ATTEMPTS`** indique le nombre d'échecs de connexion autorisés avant le verrouillage du compte.
  - Le paramètre **`PASSWORD_LOCK_TIME`** définit le nombre de jours pendant lesquels le compte est verrouillé une fois le nombre d'échecs de connexion atteint.

## Implémenter des fonctionnalités de sécurité utilisant des mots de passe

- **Durée de vie des mots de passe et expiration :** Permet de définir la durée de vie des mots de passe utilisateur. Au terme de cette durée, ils expirent et doivent être modifiés.
  - Le paramètre **`PASSWORD_LIFE_TIME`** détermine la durée de vie du mot de passe (en nombre de jours). Au terme de cette durée, le mot de passe expire.
  - Le paramètre **`PASSWORD_GRACE_TIME`** définit la période de grâce (en nombre de jours) permettant de changer le mot de passe après la première connexion réussie suite à l'expiration du mot de passe.
- **Remarque :** N'utilisez pas de profils qui entraînent l'expiration des mots de passe **`SYS`**, **`SYSMAN`** et **`DBSNMP`** et le verrouillage des comptes.

## Implémenter des fonctionnalités de sécurité utilisant des mots de passe

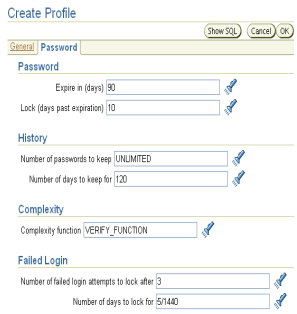
- **Historique des mots de passe :** Vérifie le nouveau mot de passe afin de garantir qu'il n'est pas réutilisé pendant une durée déterminée ou avant un certain nombre de changements de mot de passe. Ces vérifications peuvent être implémentées via l'un des paramètres suivants :
  - **PASSWORD_REUSE_TIME :** Indique qu'un utilisateur ne peut pas réutiliser un mot de passe pendant un nombre déterminé de jours.
  - **PASSWORD_REUSE_MAX :** Indique le nombre de changements de mot de passe requis avant réutilisation du mot de passe actuel.
- Ces deux paramètres s'excluent mutuellement, ce qui veut dire que lorsqu'une valeur différente de UNLIMITED (ou DEFAULT si la valeur UNLIMITED est affectée au profil DEFAULT) est affectée à l'un des paramètres, la valeur UNLIMITED doit être affectée à l'autre paramètre.

## Implémenter des fonctionnalités de sécurité utilisant des mots de passe

- **Vérification de la complexité des mots de passe :** Effectue une vérification de complexité du mot de passe afin de garantir qu'il respecte certaines règles. La vérification doit permettre de garantir que le mot de passe est suffisamment complexe pour offrir une protection contre les intrus qui tenteraient de pénétrer dans le système en devinant le mot de passe.
  - Le paramètre **PASSWORD_VERIFY_FUNCTION** nomme une 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** et renvoyer une valeur booléenne (**TRUE** ou **FALSE**).

## Créer un profil de mot de passe

- Pour créer un profil de mot de passe, sélectionnez Administration > Schéma > Utilisateurs et privilèges > Profils, puis cliquez sur le bouton Créer. Vous pouvez choisir les valeurs courantes de chaque paramètre dans une liste de valeurs (cliquez sur l'icône représentant une torche), ou entrer une valeur personnalisée.
- Toutes les périodes sont exprimées en jours, mais elles peuvent également être indiquées sous forme de fractions. Une journée compte 1440 minutes. Par conséquent, 5/1440 représente cinq minutes.




## Créer un profil de mot de passe

- Enterprise Manager peut également être utilisé pour modifier des profils de mot de passe existants.
- **Supprimer un profil de mot de passe**
- Dans Enterprise Manager, vous ne pouvez pas supprimer un profil dont se servent des utilisateurs. Toutefois, si vous supprimez un profil à l'aide de l'option **CASCADE** (par exemple, dans SQL*Plus), tous les utilisateurs dotés de ce profil se voient affecter automatiquement le profil **DEFAULT**.

## Fonction de vérification des mots de passe fournie : VERIFY_FUNCTION

- Le serveur Oracle fournit une fonction de vérification de la complexité des mots de passe, nommée **VERIFY_FUNCTION**. Cette fonction est créée à l'aide du script `<oracle_home>/rdbms/admin/utlpwdmg.sql`. Elle doit être créée dans le schéma **SYS**. Elle peut servir de modèle pour la définition d'une fonction de vérification personnalisée.
- Cette fonction applique les restrictions suivantes :
  - La longueur minimale est de quatre caractères.
  - Le mot de passe doit être différent du nom utilisateur.
  - Le mot de passe doit comporter au moins un caractère alphabétique, un chiffre et un caractère spécial.
  - Le mot de passe doit comporter au moins trois lettres différentes du précédent mot de passe.



## Fonction de vérification des mots de passe fournie : VERIFY_FUNCTION

- En plus de créer la fonction **VERIFY_FUNCTION**, le script **utlpwdmg** change le profil **DEFAULT** via la commande **ALTER PROFILE** suivante :

```
– ALTER PROFILE default LIMIT
  PASSWORD_LIFE_TIME 60
  PASSWORD_GRACE_TIME 10
  PASSWORD_REUSE_TIME 1800
  PASSWORD_REUSE_MAX UNLIMITED
  FAILED_LOGIN_ATTEMPTS 3
  PASSWORD_LOCK_TIME 1/1440
  PASSWORD_VERIFY_FUNCTION verify_function;
```

- Rappelez-vous que lorsque les utilisateurs sont créés, le profil **DEFAULT** leur est affecté, sauf si un autre profil est indiqué.

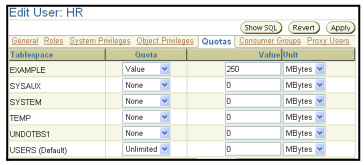
## Affecter des quotas aux utilisateurs

- Un quota est une allocation d'espace dans un tablespace donné. Par défaut, un utilisateur ne dispose d'aucun quota sur aucun des tablespaces. Trois options vous permettent d'affecter un quota utilisateur sur un tablespace.
  - **Unlimited :** Cette option permet à l'utilisateur d'employer tout l'espace disponible dans le tablespace.
  - **Value :** Il s'agit de l'espace pouvant être employé par l'utilisateur, exprimé en kilo-octets ou en mégaoctets. Cette valeur ne garantit cependant pas que l'espace est réservé pour l'utilisateur. Elle peut être supérieure ou inférieure à l'espace actuellement disponible dans le tablespace.
  - **Privilège système `UNLIMITED TABLESPACE` :** Ce privilège système remplace chaque quota de tablespace et accorde à l'utilisateur un quota illimité sur tous les tablespaces, y compris `SYSTEM` et `SYSAUX`. Il doit être accordé avec précaution.
- Remarque : Lorsque vous octroyez le rôle **RESOURCE**, vous devez également accorder le privilège **UNLIMITED TABLESPACE**.

Utilisateur
Authentification
Privilège
Rôle
Profil
Mot de passe
> Quota

## Affecter des quotas aux utilisateurs

- Vous ne devez pas accorder de quota aux utilisateurs sur les tablespaces **SYSTEM** et **SYSAUX**. En général, seuls les utilisateurs **SYS** et **SYSTEM** doivent pouvoir créer des objets dans les tablespaces SYSTEM et SYSAUX.
- Vous n'avez pas besoin de quota pour un tablespace temporaire qui vous est affecté ou pour un tablespace d'annulation.




## Affecter des quotas aux utilisateurs

- **Quand l'instance Oracle utilise-t-elle des quotas ?**
- Les quotas sont employés lorsqu'un utilisateur crée ou étend un segment.
- **Quelles activités n'ont pas d'incidence sur les quotas ?**
- Les activités qui n'utilisent pas l'espace disponible dans le tablespace désigné n'affectent pas les quotas. Il s'agit, par exemple, de la création de vues ou de l'utilisation du tablespace temporaire.
- **Quand le quota est-il renouvelé ?**
- Le quota est renouvelé lorsque les objets dont l'utilisateur est le propriétaire sont supprimés à l'aide de la clause **PURGE** ou lorsque les objets contenus dans la corbeille sont purgés automatiquement.

## Synthèse



- Ce cours vous a permis d'apprendre à :
  - créer et gérer des comptes utilisateur de base de données
    - authentifier les utilisateurs
    - affecter des zones de stockage par défaut (tablespaces)
  - accorder et révoquer des privilèges
  - créer et gérer des rôles
  - créer et gérer des profils
    - implémenter des fonctionnalités standard de sécurité utilisant des mots de passe
    - contrôler l'utilisation des ressources par les utilisateurs