



## Oracle 11g – Sécurité

---

<b>Objectif</b>	After completing this course, students will be able to : use basic Oracle Database security features, choose a user authentication model, secure the database and the listeners, use the Enterprise Security Manager tool, manage users using proxy authentication, implement Enterprise User Security, describe the benefits and requirements associated with the Oracle Advanced Security option, manage secure application roles, implement fine-grained access control, manage Virtual Private Database, implement fine-grained auditing, use Transparent Data Encryption, use file encryption, encrypt and decrypt table columns, set up Oracle Label Security policies
<b>Pré requis</b>	Pour suivre ce stage, il est nécessaire de maîtriser Oracle administration
<b>Durée</b>	3 jours

## Contenu

---

### Niveau 1 : Besoins en sécurité

- Introduction à la sécurité des données
- Composants de renforcement de la sécurité
- Les risques de sécurité
- Définition d'une stratégie de sécurité
- Implémentation d'une stratégie de sécurité

### Module 2 : Choix de solutions de sécurité

- Maintient de l'intégrité des données
- Surveillance de l'accès aux données
- Protection des données
- Aperçu de Audit Vault
- Combinaison de plusieurs options de sécurité

### Module 3 : Sécurité de premier niveau d'une base de données

- Points de contrôle de la sécurité d'une base de données
- Installation des composants minimum
- Application des patches de sécurité
- Paramètres de sécurité par défaut dans Oracle 11g
- Renforcement de la gestion des mots de passe
- Privilèges sur le système et les objets
- Restrictions des répertoires accessibles à l'utilisateur
- Séparation des responsabilités

### Module 4 : Audit de bases de données

- Audit standard de bases de données
- Surveillance d'activité suspecte
- Analyse des résultats d'audit
- Configuration de l'audit et syslog
- Déclencheurs et transactions autonomes

### Module 5 : Audit des instructions DML

- Audit FGA (Fine-Grained Auditing)
- Déclenchement des événements d'audit
- Vues du dictionnaire de données
- Activation et désactivation d'une stratégie FGA

### Module 6 : Authentification de base d'un utilisateur

- Authentification d'un utilisateur
- Identification d'un utilisateur par un mot de passe
- Identification externe d'un utilisateur
- Protection des mots de passe
- Audit avec des liens de bases de données

### Module 7 : Utilisation d'une authentification renforcée

- Single Sign On (SSO)
- Utilisation de certificats pour l'authentification
- Configuration de SSL
- Utilitaire orapki
- Utilisation de Kerberos pour l'authentification
- Authentification RADIUS

### Module 8 : Sécurité des utilisateurs d'entreprise

- Infrastructure Oracle Identity Management
- Authentification des utilisateurs d'entreprise
- Utilitaire de migration des utilisateurs d'entreprise
- Audit des utilisateurs d'entreprise

### Module 9 : Authentification avec proxy

- Considération sur la sécurité des applications n-tiers
- Implémentation courantes de l'authentification
- Utilisation de l'authentification par proxy pour les utilisateurs de bases de données
- Utilisation de l'authentification par proxy pour les utilisateurs d'entreprise
- Révocation de la sécurité par proxy
- Vues du dictionnaire de données pour l'authentification par proxy

### Module 10 : Méthodes d'autorisation

- Autorisation
- Assignation de privilèges
- Utilisation des rôles d'entreprise
- Implémentation de rôles d'application



**Module 11 : Utilisation du contexte de l'application**

- Généralités sur le contexte d'application
- Implémentation d'un contexte local
- Accès global au contexte d'application

**Module 12 : Implémentation d'une base de données virtuelle privée**

- Base de données privée virtuelle
- Implémentation de stratégies VPD
- Gestion des stratégies VPD

**Module 13 : Oracle Label Security**

- Contrôle d'accès discrétionnaire
- Oracle Label Security
- Comparaison d'Oracle Label Security et de VPD
- Gestion des Labels
- Gestion des niveaux, groupes et compartiments

**Module 14 : Utilisation du cryptage dans l'application**

- Le package DBMS\_CRYPTO
- Génération de clés avec RANDOMBYTES
- Utilisation d'ENCRYPT et DECRYPT
- Hash et code d'authentification de message

**Module 15 : Cryptage de données transparent**

- Composants du cryptage de données
- Utilisation du cryptage de données
- Utilisation de modules HSM
- Cryptage de tablespaces

**Module 16 : Cryptage au niveau fichier**

- Sauvegarde RMAN cryptée
- Restauration de sauvegardes cryptées

**Module 17 : Sécurité de Oracle Net Services**

- Restrictions par adresses IP
- Restrictions des ports ouverts
- Cryptage du trafic réseau
- Fichiers de logs de Oracle Net Services