Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Oracle Database 12c : Security

Date et durée

Code formation : ORA176FR
Durée : 5 jours
Nombre d'heures : 35 heures

Description

Votre organisation doit être en conformité avec ses obligations de sécurité de l'information en termes de confidentialité, d'intégrité et de conformité avec les contraintes imposées par les règlementations internationales ou nationales, voire sectorielles.
Ce cours vous expliquera comment optimiser les fonctionnalités de sécurité d'Oracle et comment sécuriser un Système de Gestion de Base de Données Relationnel (SGBDR).
Vous saurez comment assurer la confidentialité et l'intégrité des données, comment mettre en œuvre des contrôles d'accès – au réseau, à la base de données, aux données - , comment procéder à des audits et comment apporter la preuve de la conformité de votre SGBDR avec les normes de sécurité imposées.
Seront aussi abordés lors de cette formation :

- Le contrôle d'accès aux données sensibles basé sur des labels (étiquettes) avec Oracle Label security
- Le chiffrement avec Transparent Data Encryption (TDE)
- La gestion des droits et privilèges spéciaux des utilisateurs avec Oracle Database Vault
- La création d'espaces d'archivage pour les données sensibles avec Flasback Data Archive (FDA)
- L'audit et la conservation des traces des activités de la base de données avec Oracle Audit Vault

Les stagiaires seront mis en situation au travers des exercices pratiques.

Objectifs

- Répondre aux exigences de sécurité en mettant en œuvre et en gérant les solutions de sécurité Oracle
- Contrôler les accès aux données
- Apprendre à configurer et implémenter des mesures d'authentification forte
- Découvrir les possibilités offertes par les solutions de cryptage : protection des données stockées ou archivées, sécurités des informations en transit via les réseaux de communication
- Savoir déterminer des stratégies d'audit : auditer les actions des utilisateurs et auditer les activités au sein de la base de données

Pré-requis

Il est aussi fortement conseillé de savoir :

- Configurer et administrer processus d'écoute Listener Oracle
- Gérer des utilisateurs : création et maintenance des rôles et privilèges
- Utiliser RMAN pour la sauvegarde et la restauration de données
- Transférer des données en masse avec fonctionnalités d'export import d'Oracle

Les formations ci-dessous sont recommandées.

Public

Cette formation s'adresse :

- Administrateurs de bases de données
- Administrateurs réseaux
- Analystes système
- Ingénieurs supports
- Administrateurs de sécurité
- Auditeurs de la conformité à la sécurité

Cette formation s'adresse aux profils suivants

Administrateur système
Technicien Support / HelpDesk

Programme

- Identifier les exigences de sécurité de l’information
    - La sécurité des données
    - Identifier les risques de sécurité de l’information
    - Détecter les failles de sécurité et prévenir les vulnérabilités
    - Mettre en œuvre les mesures de sécurité
- Eléments de base de la sécurité d’une base de données
    - Lister les points de contrôle de sécurité d’une base de données
    - Préparer l’administration d’une base de données
    - Sécurité physique
- Sécuriser les données en réseaux
    - Contrôler les accès au réseau
    - Créer, configurer et contrôler processus d’écoute Oracle Database
- Mettre en œuvre et gérer les accès des utilisateurs
    - Authentification forte ou de base
    - Méthode d’authentification sur un serveur Oracle Secure Global Desktop (SGD)
    - Enterprise User Security (EUS) : infrastructure de gestion des identités d’Oracle
    - Concepts et architecture d’Oracle Internet Directory (OID)
    - Authentification des utilisateurs par proxy
- Administrer les profils, les rôles et les privilèges des utilisateurs d’Oracle
    - Schéma de base de données relationnel avec modèle relationnel des données : tables, colonnes et lignes
    - Création de l’utilisateur propriétaire du catalogue privé virtuel
    - L’analyse de privilèges de Oracle Database 12c : flux de l’analyse et mise en œuvre
- Utiliser les contextes d’application
    - Politiques de sécurité des accès aux bases de données
    - Mettre en œuvre la base de données privée virtuelle (VPD : Virtual Private Database)
    - Mettre en œuvre Fine-Grained Access Control (FGAC)
- Mettre en œuvre Oracle Label Security
    - Stratégies et politiques d’OLS
- Utiliser Oracle Data Masking
    - Protéger les données à caractère personnel (DCP)
    - Stratégie et processus de masquage de données
- Fonctionnalité de protection transparente des données sensibles

    - Une option de sécurité avancée : le chiffrement
    - Protéger les données lors de leur stockage : Transparent Data Encryption (TDE)
    - Clés maîtres et fichier de clés
    - Sauvegarde RMAN et OSB
    - Modes de cryptage RMAN
    - Exportation et importation de données cryptées via Data Pump
- Implémenter des audits de bases de données
    - Les fonctions d’audit de base
    - Gestion des audits unifiés
    - Situations d’audit spéciales
    - Fonctionnalité d’audit de niveau fin (FGA : Fine Grained Auditing)