Sécurité Oracle 11g 12c

Référence : BASO | Niveau : Intermédiaire | Durée : 3 jours (21h.)

Tarif: Nous Contacter | Date: Juin, Juillet, Aout | Contact: +225 22469017 / 74622582

Objectifs

La nécessité de sécuriser les données n'est plus à démontrer. Les risques englobent le piratage des comptes utilisateurs, l'exploitation des vulnérabilités des applications, le vol de supports physique de sauvegarde et d'autres attaques comme des menaces persistantes avancées ou APT.
Les administrateurs de base de données ont une responsabilité directe ou indirecte pour :
• Sécuriser l'installation et la configuration des bases de données (y inclus le téléchargement et l'installation des correctifs de sécurité)
• Gérer les comptes utilisateurs (Identification et Authentification)
• Sécuriser les connexions réseaux
• Sécuriser les données sensibles (chiffrement)
• Auditer régulièrement les composants base de données au niveau approprié.
Le cours Sécurité Oracle 11g 12c rappelle les techniques et les ressources disponibles pour renforcer la sécurité au niveau des bases de données.
À l'issue de cette formation, vous aurez acquis les connaissances et les compétences pour:
• Mettre en œuvre une méthodologie de travail
• Appréhender la complémentarité des actions
• Proposer des axes d'amélioration et d'optimisation.
Très orientée sur la pratique, cette formation est composée d'une première journée consacrée aux principes de la sécurité, puis de deux journées de travaux pratiques spécifiques à la base de données Oracle.

Public

Cette formation Sécurité Oracle 11g 12c s'adresse aux responsables sécurité, administrateurs de bases de données, développeurs SQL, chefs de projets souhaitant obtenir une vision d'ensemble des outils de sécurité des bases de données et mettre en pratique la sécurité sur une base Oracle.

Pré-requis

Il est recommandé d'avoir des connaissances Oracle

Contenu du cours

La feuille de route (1 jour)

Les 9 étapes pour orchestrer une défense raisonnée
Étape1:Sécuriserl'accèsauxbasesdedonnéesàl'aidedesparamètresd'initialisation et des protections réseau Étape2:Créerdesrôlesetdesprivilègespourl'Identification et l'Authentification
Créer un rôle de sécurité
Les comptes Utilisateur prédéfinis
Les privilèges
L'authentification forte
Étape3:Chiffrerlesdonnées qui se déplacent à travers le réseau
Le chiffrement
Étape4:Protégerl'accès aux données sensibles
Réduire la surface
Les contextes d'application
Étape5:Restreindre l'affichage des données sensibles
Étape6:Limiter l'accès aux données sensibles
Étape7:Partager les données en toute sécurité
Étape8:Renforcer la sécurité avec des outils intégrés ou externes
Étape9:Configurerl'audit pour tracer l'activité sur la base de données
Les stratégies d'audit prédéfinies

Travaux Pratiques avec les bases de données Oracle 11g et 12c (2 jours)

Travaux Pratiques Étape 1:
Définir le rôle des paramètres de sécurité par défaut de la version Oracle 12c
Comment chiffrer des données sur le réseau
Comment contrôler l'expiration et le verrouillage des comptes Utilisateur
Travaux Pratiques Étape 2:
Comment renforcer la sécurité avec les clauses ACCESSIBLE BY, AUTHID CURRENT_USER et AUTHID DEFINER ainsi que la clause BEQUEATH dans les vues et INHERIT [ANY] PRIVILEGES
Travaux Pratiques Étape 3:
Les méthodes d'authentification et de chiffrement avec Oracle Net Manager
Travaux Pratiques Étape 4:
Comment réduire la surface d'exposition
Mise en œuvre des contextes d'application
Travaux Pratiques Étape 5:
Mise en œuvre de la limitation d'affichage des données sensibles avec Oracle Data Redaction
Travaux Pratiques Étape 6:
Une feuille de route détaillée avec DataMasking
Une feuille de route détaillée avec VDP
Travaux Pratiques Étape 7:

Comment générer des clés de chiffrement
Le chiffrement avec package DBMS_CRYPTO
Utilisation de TDE (Transparent Database Encryption)

Travaux Pratiques Étape 8:

Configurer et activer Oracle Database Vault

Travaux Pratiques Étape 9:

L'audit FGA