Oracle Database Security: Preventive Controls

Le cours "Oracle Database Security: Preventive Controls" explique comment utiliser les produits et technologies Oracle Database Security pour satisfaire aux exigences de sécurité, de confidentialité et de conformité des entreprises.

Les mesures réglementaires dictées par des textes tels que les lois Sarbanes-Oxley, HIPAA et UK Data Protection Act imposent une sécurité accrue au niveau de la base de données. Ce cours explique comment sécuriser l'accès aux bases de données et comment utiliser les produits et technologies Oracle Database Security pour améliorer l'accès aux données et la confidentialité. Il recommande des solutions Oracle permettant de répondre à des problèmes courants.

Audience

- Administrator
- Datbase Administrators
- Network Administrator
- Systems Administrator

Bénéfices de cette formation

Ce cours décrit les fonctionnalités de sécurité suivantes de la base de données : authentification, contrôle d'accès aux données via des autorisations utilisateur basées sur des privilèges et des rôles, confidentialité des données via la protection par occultation, le masquage des données et la création de sous-ensembles de données, la protection transparente des données confidentielles (TSDP), le cryptage transparent des données au niveau colonne, tablespace et fichier. Il présente par ailleurs l'utilisation d'Oracle Key Vault pour centraliser la gestion des clés dans toute l'entreprise. Oracle Database Vault est utilisé pour mettre en oeuvre la séparation des fonctions au niveau de l'administrateur de base de données.

Des exercices pratiques et des démonstrations permettent d'apprendre à utiliser la plupart des fonctionnalités d'Oracle Database 12c pour sécuriser le centre de données, à l'aide d'Oracle Enterprise Manager Cloud Control ou d'autres outils simples comme SQL*Plus.

Learn To:

- Choisir les produits et technologies oracle database security pour satisfaire aux exigences de sécurité.
- Sécuriser l'accès à la base de données par les utilisateurs de la base ou de l'entreprise à l'aide de fonctions d'authentification de base ou fortes telles que ssl, kerberos et radius.
- Se protéger contre le contournement de la base de données à l'aide du cryptage transparent.
- Utiliser des portefeuilles Oracle et Oracle Key Vault pour gérer les clés de cryptage.
- Repérer les colonnes confidentielles, telles que les numéros de carte de crédit, à l'aide de la modélisation des données d'application.
- Limiter la prolifération des données confidentielles dans les environnements de test/développement grâce au masquage des données.
- Limiter les coûts de stockage dans les environnements de test/développement grâce à la création de sous-ensembles de données.
- Réduire l'exposition des données confidentielles dans les applications grâce à la protection par occultation de données