

FORMATION ORACLE DATABASE 12C SECURITY : PREVENTIVE CONTROLS ED1

Durée: 5jours

Description

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.

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.

Compétences à acquérir:

- 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.

TRUST-SYSTEMS CONSULTING SARL

N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala

BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331

Email : contact@trust-systems.net – site web : www.trust-systems.net

- 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 des données.

Prérequis suggérés

- Utiliser l'exportation et l'importation d'Oracle Data Pump et exécuter RMAN en retour
- Utiliser Flashback Data Archive et Créer des procédures PL/SQL
- Familiarité avec SQL*Plus, SQL*Developer
- Familiarité avec Oracle Enterprise Manager Cloud Control

Prérequis exigés

- Introduction à Oracle Database Security Ed 1
- Créer et gérer des utilisateurs, des rôles et des privilèges
- Créer et gérer des tables et des espaces de table
- Créer des procédures PL/SQL

Audience

- Administrateur
- Administrateur de base de données
- Administrateur réseau
- Administrateur des systèmes

Objectifs

- Configurer et utiliser le cryptage transparent des données
- Configurer et utiliser la protection transparente des données confidentielles
- Configurer les fonctions générales d'authentification et d'autorisation
- Installer et utiliser Oracle Database Vault
- Configurer et gérer un portefeuille simple
- Comprendre la protection par occultation Oracle
- Comprendre et mettre en oeuvre des utilisateurs globaux
- Comprendre et utiliser le masquage et la création de sous-ensembles de données Oracle
- Comprendre et utiliser Oracle Key Vault
- Comprendre les risques pour la sécurité et identifier les solutions Oracle appropriées

Thèmes

- Introduction
- Objectifs du cours
- Cours connexes et où cela s'inscrit
- Calendrier des cours et annexes
- Utilisation de l'authentification utilisateur de base et renforcée
- Authentification de base
- Authentification forte
- Protection des mots de passe des liens de base de données
- Sécurité des rôles
- Configuration de l'authentification globale des utilisateurs
- À propos de la gestion des utilisateurs d'entreprise (EUS)
- Intégration EUS et LDAP
- Utilisation de l'authentification proxy
- Défis de sécurité de l'informatique à trois niveaux
- Solutions d'authentification proxy
- Concepts et solutions de chiffrement
- Notions
- Solutions
- Solutions Oracle
- Utilisation du chiffrement intégré dans les applications
- *Usage
- *Utilisation du chiffrement transparent des données (TDE)
- *Aperçu
- Les clés principales et le magasin de clés
- Keystore matériel
- Chiffrement
- Sécurité du stockage de la base de données
- Sauvegardes RMAN et OSB
- Modes de chiffrement RMAN
- Data Pump Exportation et importation de données cryptées
- Présentation d'Oracle Key Vault
- Qu'est-ce qu'Oracle Key Vault ?
- Utilisation d'Oracle Key Vault
- Installation d'Oracle Key Vault
- Installation
- Points finaux
- Utilisation d'Oracle Key Vault
- Réviser ou rafraîchir les connaissances préalables

TRUST-SYSTEMS CONSULTING SARL

N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala

BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331

Email : contact@trust-systems.net – site web : www.trust-systems.net

- Portefeuilles Oracle et portefeuilles virtuels OKV contrastés
- Administration d'Oracle Key Vault
- Rôles en détail
- Conseils sur les meilleures pratiques pour Oracle Key Vault
- Découverte automatisée des données sensibles
- Aperçu
- Modélisation des données d'application
- Gestion des modèles de données d'application
- Présentation du masquage de données et des sous-ensembles Oracle
- Aperçu
- Masquage des données sensibles dans les environnements de non-production
- Exploration de la bibliothèque de formats de masquage de données
- Transformations de masquage des données de sous-ensemble
- Exploration des définitions de sous-ensembles de données
- Gestion du masquage des données et des sous-ensembles
- Administration du masquage des données et des sous-ensembles
- Masquage hétérogène et sous-ensemble
- Les meilleures pratiques Oracle Advanced Security
 - Rédaction des données
- Besoin de caviarder ou de masquer dynamiquement des données
- Mise en œuvre de la rédaction des données
- Consignes d'utilisation de la rédaction des données
- Oracle Transparent Sensitive Data Protection (TSDP)
- Mise en œuvre du TSDP
- Présentation d'Oracle Database Vault
- Comprendre les contrôles du coffre-fort de base de données
- Qu'est-ce qu'un royaume ? Un ensemble de règles ? Une règle de commande ? Un rôle d'application sécurisé ?
- Que sont les Facteurs et les Identités ? Relations entre les composants et évaluation ?
- Effets et exemple du coffre-fort de base de données
- Présentation du logiciel : API, vues et intégration avec d'autres produits Oracle
- Configuration de Database Vault
- Rôles et schéma du coffre-fort de base de données
- À quoi s'attendre après l'activation de Database Vault
- Sécurisation des données dans les environnements mutualisés
- Configuration des utilisateurs de Database Vault dans Cloud Control 12c
- Analyse des privilèges
- Présentation et fonctionnalités de l'analyse des privilèges
- Comment ça marche?
- Quels sont les types d'analyse, les outils et les prérequis ?

TRUST-SYSTEMS CONSULTING SARL

N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala

BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331

Email : contact@trust-systems.net – site web : www.trust-systems.net

- Gestion des politiques d'analyse des privilèges
- Cas d'utilisation

TRUST-SYSTEMS CONSULTING SARL
N°A6.4, Résidence J, 210 Rue FOCH, AKWA, Douala
BP: 1184 Douala, Cameroun – Tel +237 233 430 911 / +241 03130331
Email : contact@trust-systems.net – site web : www.trust-systems.net