Oracle Database 11g : Sécurité Release 2

Durée: 5 Jours

Description

Dans ce cours, les stagiaires apprennent à utiliser les fonctionnalités de la base de données Oracle pour répondre aux exigences de sécurité, de confidentialité et de conformité réglementaire de leur organisation. 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 la base de données et comment utiliser les fonctionnalités de celle-ci pour améliorer la sécurité. Il décrit différentes architectures permettant de répondre à des besoins spécifiques. Il présente les fonctionnalités suivantes : audit, cryptage pour Payment Card Industry Data Security Standard (PCI DSS) incluant le cryptage au niveau colonne, tablespace ou fichier, Virtual Private Database (VPD), Oracle Label Security (OLS) et Enterprise User Security (EUS). Par ailleurs, il explique comment protéger un réseau Oracle en sécurisant le processus d'écoute et en restreignant les connexions en fonction de l'adresse IP.

Learn To:

Implémenter les fonctionnalités de sécurité de la base de données Oracle pour assurer la protection des données
Implémenter les fonctionnalités de sécurité de la base de données Oracle pour assurer la conformité réglementaire

Audience

Administrateurs de base de données
Administrator
Analystes système
Database Administrators
Ingénieurs support
Security Administrators
Support Engineer
System Analysts
Technical Administrator

Cours pré-requis

Cours pré-requis obligatoire(s)

Oracle Database 11g: Administration Workshop I
Oracle Database 11g: Administration Workshop I Release 2

Cours pré-requis conseillé(s)

Oracle Database 11g : Administration Workshop II Release 2
Oracle Database 11g: Administration Workshop II Release 2
Oracle Database 11g: Administration Workshop II

Objectifs

Choisir un modèle d'authentification pour les utilisateurs
Décrire les avantages et les exigences liés à l'option Oracle Advanced Security
Crypter et décrypter des colonnes de table
Implémenter Enterprise User Security (EUS)

Implémenter le contrôle d'accès de niveau fin
Implémenter un audit détaillé (FGA - Fine Grained Auditing)
Gérer Virtual Private Database
Gérer les rôles applicatifs sécurisés
Gérer les utilisateurs authentifiés par proxy
Sécuriser la base de données et son processus d'écoute
Implémenter une stratégie Oracle Label Security
Utiliser Transparent Data Encryption
Utiliser d'autres fonctions de sécurité de base de données
Utiliser le cryptage des fichiers
Utiliser Enterprise Manager Security

Thèmes abordés

Introduction à la sécurité des bases de données
Exigences élémentaires en matière de sécurité des données
Problèmes liés à la sécurité des données
Conformité réglementaire
Risques en matière de sécurité
Développer une stratégie de sécurité
Définir une stratégie de sécurité
Implémenter une stratégie de sécurité
Techniques de mise en œuvre de la sécurité

Choisir les solutions de sécurité
Préserver l'intégrité des données
Contrôler l'accès aux données
Présentation d'Oracle Database Vault
Présentation d'Oracle Audit Vault
Combiner les fonctionnalités de sécurité facultatives
Analyseur de conformité
Enterprise Manager Database Control : Evolution des stratégies
Sécurité de la base de données : Règles élémentaires

Sécurité de la base de données : Règles élémentaires
Sécurité de la base de données : Règles élémentaires
Réduire l'effort d'administration
Appliquer les patches de sécurité
Paramètres de sécurité par défaut
Prise en charge des mots de passe sécurisés
Mettre en oeuvre la gestion des mots de passe
Protéger le dictionnaire de données
Privilèges système et privilèges sur les objets

Auditer les utilisateurs, les privilèges et les objets de base de données
Surveiller les activités suspectes
Audit de base de données standard
Définir le paramètre AUDIT_TRAIL
Définir les options d'audit
Visualiser les options d'audit
Auditer les utilisateurs SYSDBA

Auditer les fichiers XML
Audit basé sur les données

Auditer les instructions LMD
Audit détaillé (FGA)
Utiliser le package DBMS_FGA
Stratégie d'audit détaillé
Déclencher des événements d'audit
Vues du dictionnaire de données
DBA_FGA_AUDIT_TRAIL
Activer et désactiver une stratégie d'audit détaillé
Gérer la trace d'audit

Utiliser l'authentification de base des utilisateurs
Authentification des utilisateurs
Protéger les mots de passe
Créer des liens de base de données fixes
Crypter les mots de passe dans les liens de base de données
Utiliser des liens de base de données sans informations d'identification et de connexion
Modifier les mots de passe dans les liens de base de données
Auditer des opérations via les liens de base de données
Protéger un lien de base de données à l'aide de vues

Utiliser l'authentification forte
Authentification forte
Accès avec connexion unique (SSO)
Outils de l'infrastructure PKI
Configurer la technologie SSL sur le serveur
Certificats
Employer l'utilitaire orapki
Utiliser Kerberos pour l'authentification
Configurer le "wallet"

Utiliser Enterprise User Security
Enterprise User Security
Infrastructure Oracle Identity Management : Déploiement par défaut
Base de données Oracle : Architecture Enterprise User Security
Présentation de la structure Oracle Internet Directory
Installer Oracle Application Server Infrastructure
Gérer Enterprise User Security
Créer un objet de mise en correspondance de schéma dans l'annuaire
Créer un objet de mise en correspondance de schéma dans l'annuaire

Utiliser l'authentification par proxy
Défis liés à la sécurité avec le modèle informatique à trois niveaux
Implémentations courantes de l'authentification
Limiter les privilèges du niveau intermédiaire
Authentifier les utilisateurs de base de données et les utilisateurs entreprise
Utiliser l'authentification par proxy pour les utilisateurs de base de données
Accès par proxy via SQL*Plus
Révoquer l'authentification par proxy
Vues du dictionnaire de données pour l'authentification par proxy

Utiliser les privilèges et les rôles
Autorisation
Privilèges
Avantages des rôles
Privilèges du rôle CONNECT
Utiliser l'authentification par proxy avec les rôles
Créer un rôle entreprise
Sécuriser les objets à l'aide de procédures
Sécuriser les rôles d'application

Contrôle des accès
Description du contexte applicatif
Utiliser un contexte applicatif
Définir un contexte applicatif
Sources de données pour un contexte applicatif
Utiliser la fonction PL/SQL SYS_CONTEXT
Packages et procédures PL/SQL
Implémenter un contexte applicatif en accès global
Vues du dictionnaire de données

Implémenter Virtual Private Database
Contrôle d'accès de niveau fin
Virtual Private Database (VPD)
Fonctionnement du contrôle d'accès de niveau fin
Utiliser DBMS_RLS
Exceptions aux stratégies de contrôle d'accès de niveau fin
Implémenter une stratégie VPD
Implémenter des groupes de stratégies
Meilleures pratiques liées à VPD

Concepts Oracle Label Security
Présentation du contrôle d'accès
Contrôle d'accès discrétionnaire
Oracle Label Security
Utilisation des labels de sensibilité
Installer Oracle Label Security
Oracle Label Security : Fonctionnalités
Oracle Label Security et Virtual Private Database : Comparaison
Analyser les besoins des applications

Implémenter Oracle Label Security
Implémenter une stratégie Oracle Label Security
Créer des stratégies
Définir la présentation des labels
Définir des compartiments
Identifier les labels de données
Médiation d'accès
Ajouter des labels aux données
Affecter des labels d'autorisation à un utilisateur

Utiliser Data Masking Pack
Principe du masquage des données

Fonctionnalités de Data Masking Pack
Identifier les données sensibles à masquer
Types de primitive et de sous-programme de masquage intégrés
Masquer des données de la table EMPLOYEES
Implémenter une fonction de post-traitement
Afficher l'état d'impact relatif au masquage des données
Créer un modèle de masque d'application en exportant des définitions de masque de données

Concepts relatifs au cryptage
Comprendre les exceptions
Problèmes résolus par le cryptage
Différence entre le cryptage et le contrôle d'accès
Données à crypter
Défis liés au cryptage de données
Stockage des clés dans la base de données
Gestion des clés par les utilisateurs
Stockage des clés au niveau du système d'exploitation

Utiliser le cryptage au niveau de l'application
Présentation du package DBMS_CRYPTO
Utiliser le package DBMS_CRYPTO
Générer des clés à l'aide de RANDOMBYTES
Utiliser les fonctions ENCRYPT et DECRYPT
Renforcer la sécurité grâce aux modes de chaînage pour chiffrement par bloc
Fonctions HASH et MAC

Applying Transparent Data Encryption
Transparent Data Encryption (TDE)
Creating the Master Key
Opening the Wallet
Using Auto Login Wallet
Resetting (Rekeying) the Unified Master Encryption Key ** 11.2 **
Using Hardware Security Modules
TDE Column Encryption Support
Creating an Encrypted Tablespace

Applying File Encryption
RMAN Encrypted Backups
Oracle Secure Backup Encryption
Creating RMAN Encrypted Backups
Using Password Mode Encryption
Restoring Encrypted Backups
Data Pump Encryption
Using Dual Mode Encryption
Encrypting Dump Files

Oracle Net Services: Security Checklists
Overview of Security Checklists
Securing the Client Computer
Configuring the Browser
Network Security Checklist
Using a Firewall to Restrict Network Access

Restricting Network IP Addresses: Guidelines
Configuring IP Restrictions with Oracle Net Manager
Configuring Network Encryption

Securing the Listener
Listener Security Checklist
Restricting the Privileges of the Listener
Moving the Listener to a Nondefault Port
Preventing Online Administration of the Listener
Using the INBOUND_CONNECT_TIMEOUT Parameter
Analyzing Listener Log Files
Administering the Listener Using TCP/IP with SSL
Setting Listener Logging Parameters

Cours associé(s)

Oracle Database 11g: Security Self-Study Course