



Oracle Database 19c : Fondamentaux de la S curit 

Description

Prix : 750  -HT

Dur e : 1 jour

Code de R f rence  : SECU19

Catalogue Database

Ce cours couvre les principales fonctionnalit s de s curisation des bases de donn es Oracle 19c (authentification/autorisation, chiffrement, audit). A l'issue de la formation, les stagiaires disposent d'une bonne connaissance de l'offre disponible et sont en mesure d' valuer ce qu'il est opportun de mettre en  uvre dans leur contexte de travail.

Objectifs de la formation

A l'issue de cette formation Oracle, vous serez capable de :

- Choisir des solutions appropri es pour r pondre aux exigences en mati re de s curit , de confidentialit  et de conformit 
- Mettre en  uvre la s curit  de base de la base de donn es
- Configurer l'authentification pour la base de donn es
- Contr ler l'acc s et l'int grit  des donn es
- Trouver des solutions pour s curiser l'acc s   la base de donn es via le r seau
- Auditer les actions des utilisateurs
- Assurer la confidentialit  des donn es en utilisant une solution de chiffrement

Public

Cette formation s'adresse aux administrateurs de base de donn es / DBA, administrateurs/consultants s curit .



PrÃ©requis

Ãªtre sensibilisÃ© aux concepts gÃ©nÃ©raux de sÃ©curitÃ©, avoir des connaissances basique de l'architecture et du fonctionnement d'Oracle Database.

Programme de la formation

Administration des utilisateurs, authentification et autorisation

- Objectifs
- Utilisateurs locaux
- Utilisateurs communs par rapport aux utilisateurs locaux
- ParamÃªtres de profil : verrouillage et mots de passe
- Mots de passe et vÃ©rificateurs de mots de passe
- Utilisateurs de schÃ©ma uniquement
- Utilisateurs proxy
- Authentification du systÃªme d'exploitation
- SÃ©curitÃ© des utilisateurs d'entreprise
- Structure du rÃ©pertoire : aperÃ§u
- Utilisateurs d'entreprise
- Utilisation des rÃªles d'entreprise
- Audit des utilisateurs d'entreprise
- Gestion des comptes : verrouiller et dÃ©verrouiller des comptes
- Gestion des comptes : expiration des mots de passe
- Gestion des comptes : identification des comptes inactifs

SÃ©curisation des mots de passe

- Protection des mots de passe
- Utilisation d'un magasin de mots de passe externe sÃ©curisÃ© pour protÃ©ger les mots de passe
- Conception d'applications pour gÃ©rer les mots de passe de maniÃªre sÃ©curisÃ©e
- Gestion sÃ©curisÃ©e des mots de passe dans les scripts
- Gestion du fichier de mots de passe de la base de donnÃ©es
- AmÃ©liorations du fichier de mots de passe
- Migration du fichier de mots de passe
- VulnÃ©rabilitÃ©s du fichier de mots de passe



Autorisation

- Analyse des privilèges
- Flux d'analyse des privilèges
- Résultats des privilèges utilisés
- Comparaison des privilèges utilisés et non utilisés
- Listes de captures
- Suppression d'une analyse
- Profils de verrouillage de PDB (base de données à partitionnement physique)
- Restriction des opérations dans un profil de verrouillage de PDB
- Héritage des profils de verrouillage de PDB (base de données à partitionnement physique)
- Profils de verrouillage de PDB statiques et dynamiques

Sécurité réseau

- Contrôle d'accès réseau pour les services externes
- Relation entre les listes de contrôle d'accès réseau et les déploiements de microservices
- Utilisation des listes de contrôle d'accès (ACL) pour accéder aux mots de passe dans un portefeuille
- Vérification de nœuds valides pour le gestionnaire d'écoute
- Profils de services réseau
- SEC_USER_UNAUTHORIZED_ACCESS_BANNER
- SEC_USER_AUDIT_ACTION_BANNER
- FALLBACK_AUTHENTICATION
- ALLOWED_LOGON_VERSION_CLIENT
- ALLOWED_LOGON_VERSION_SERVER
- Restriction des adresses IP réseau : vérification des nœuds valides
- Amélioration de la sécurité de la communication de la base de données
- SEC_PROTOCOL_ERROR_TRACE_ACTION
- SEC_PROTOCOL_ERROR_FURTHER_ACTION
- SEC_MAX_FAILED_LOGIN_ATTEMPTS
- SEC_RETURN_SERVER_RELEASE_BANNER

Chiffrement du stockage de la base de données

- Compréhension du chiffrement
- Coût du chiffrement



- Gestion des clés de chiffrement
- Chiffrement transparent des données
- Chiffrement des tablespaces
- Chiffrement des colonnes
- Chiffrement des LOB (grands objets) SECUREFILE
- Sauvegardes chiffrées RMAN
- Chiffrement des exports de données

Chiffrement du trafic réseau

- Chiffrement de bout en bout
- Configuration du chiffrement réseau
- Vérification de l'intégrité des données (Checksumming)
- Configuration de la vérification de l'intégrité des données (Checksumming)

Utilisation de l'audit unifié

- Présentation de l'audit
- Architecture de l'audit unifié
- Politique d'audit
- Mise en œuvre de l'audit unifié
- Gestion de l'audit unifié
- Situations d'audit spécifiques

Méthodes pédagogiques

Apports théoriques et démonstrations, des exercices pratiques permettent de mettre en œuvre les connaissances acquises.

Méthodes d'évaluation des acquis

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.