

Oracle Database Security Administrator



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. Overview

- Assess security needs (risk reduction, regulatory compliance)
- Assess the typical attack points for a database
- Deploy the Maximum-Security Architecture

2. Manage Database Users

- Administer OS Authentication
- Administer Kerberos Authentication
- Administer PKI Certificate Authentication
- Administer Enterprise User Security
- Administer Centrally Managed Users
- Identify Inactive accounts

3. Manage and Secure passwords

- Secure Passwords in scripts and applications
- Change a user's password securely
- Administer a secure external password store to secure passwords
- Administer the Database Password File
- Control the use of a password file



Oracle Database Security Administrator

4. Configure and Use Contexts

- Understand and use USERENV variables
- Understand and Use Client Identifiers
- Extend Unified Auditing with Context information
- Use context information with Secure Application Roles

5. Manage Authorization

- Administer System and Object Privileges
- Assign Administrative Privileges
- Configure Secure Application Roles
- Configure Global Roles (EUS/CMU)
- Perform Privilege Analysis

6. Configure Fine Grained Access Control

- Configure Fine Grained Access Control (FGAC)
- Configure FGAC with Real Application Security
- Configure FGAC with Virtual Private Database
- Configure FGAC with Oracle Label Security



Oracle Database Security Administrator

7. Configure and Manage Database Vault

- Describe the Default Separation of Duties with Database Vault
- Configure Database Vault Factors, Rules, and Rule Sets
- Configure Database Vault Mandatory and non-Mandatory Realms
- Configure Database Vault Command Rules
- Configure Realms, Command Rules, and Application Context
- Perform Database Vault Operations Control

8. Configure and Use Auditing

- Perform Privileged User Audit
- Configure Standard Audit
- Configure Fine Grained Auditing
- Configure and use Unified Audit

9. Configure Network Security

- Assess the need for Network access control (ACL)
- Manage Network ACLs in relation to microservice deployments
- Configure ACLs to access passwords in a wallet
- Configure Network Service Profiles
- Configure and use Listener Valid-Node Checking
- Enhance Database Communication Security with SEC_ parameters



10. Configure and Implement Encryption

- Encrypt data in motion
- Configure Native Network Encryption
- Configure TLS Encryption
- Encrypt data at rest with Transparent Database Encryption
- Configure Column level and Tablespace level Encryption
- Encrypt the Data Dictionary
- Migrate unencrypted to encrypted data
- Manage Encryption Keys
- Administer and use the SYSKM Administrative Privilege
- Administer Encryption Wallets

11. Implement Data Masking and Data Redaction

- Implement Data Redaction
- Implement Enterprise Manager Data Masking Pack
- Configure and use the Application Data Model
- Perform Sensitive Data Discovery
- Deploy Data Masking Formats
- Compare In-Database -vs- At-Source execution
- Automate Masking operations with EMCLI
- Configure Transparent Sensitive Data Protection (TSDP)



Oracle Database Security Administrator

For Enquiry: +91 8680961847

12. Invoke the Database Security Assessment Tool

- Run the Database Security Assessment Tool

13. Patch Databases

- Assess the need for of a CVE
- Decode CVSS Risk Scoring

14. Manage Database Security in the Cloud

- Assess the Shared Responsibility Model
- Manage hybrid cloud scenarios
- Assess Autonomous Database Self Securing

Zetlan Technologies

Free Advice: +91 9600579474

www.zetlantech.com



**LEARN
REMOTELY!!**

**The efficiency of online learning
in terms of time management,
flexibility, and the ability
to access resources anytime,
anywhere can be compelling.**



ZETLAN TECHNOLOGIES
www.zetlantech.com

**For contact: +91 8680961847
+91 9600579474**

