Oracle Database 10g Security

Course information

Days : 4
Total lessons : 20
Suggested Prerequisites :

- Oracle Database 10g: Administrator Workshop I
- Oracle Database 10g: Administrator Workshop II

Training includes :

- Experienced trainer(s)
- Pre-test and Post-test
- Practices, and solutions
- Trainer Assistant(s)

In-house price for 4 days

- 82,000 baht(THB) : Small Class : 1 - 10 persons
- 100,000 baht(THB) : Medium Class : 11 - 20 persons
- 118,000 baht(THB) : Big Class : 21 - 30 persons
- All prices exclude VAT 7 %

Course details

Day 1

- Introduction
- Lesson 1 : Understanding Security Requirements
- Lesson 2 : Choosing Security Solutions
- Lesson 3 : Applying Internal Database Security
- Lesson 4 : Auditing Database Users, Privileges, and Objects
- Lesson 5 : Auditing DML Statements

Day 2

- Lesson 6 : Using Basic User Authentication
- Lesson 7 : Using Strong Authentication
- Lesson 8 : Using Enterprise User Security
- Lesson 9 : Using Proxy Authentication
- Lesson 10 : Using Privileges and Roles

Day 3

- Lesson 11 : Using Application Contexts
- Lesson 12 : Implementing Fine-Grained Access Control
- Lesson 13 : Installing Oracle Label Security
- Lesson 14 : Implementing Oracle Label Security
- Lesson 15 : Encryption Concepts

Day 4

- Lesson 16 : Using Application-Based Encryption
- Lesson 17 : Applying Transparent Data Encryption
- Lesson 18 : Applying File Encryption
- Lesson 19 : Oracle Net Services: Security Checklists
- Lesson 20 : Securing the Listener

Lesson details

Lesson 1 : Understanding Security Requirements

- Describe fundamental security requirements
- Define the following terms:
    - Least privilege
    - Authorization
    - Authentication
- Describe security policies
- Describe security policies
- Describe the concept of in-depth security

Lesson 2 : Choosing Security Solutions

- Preventing exploits
- Maintaining data integrity
- Protecting data
- Controlling data access

Lesson 3 : Applying Internal Database Security

- Apply the principle of least privilege to the database
- Apply security patches (Critical Patch Update)
- Lock and expire default user accounts
- Change default user passwords
- Create strong passwords
- Enforce password management
- Protect the data dictionary

Lesson 4 : Auditing Database Users, Privileges, and Objects

- Implement basic database auditing
- Implement auditing of the privileged user
- Implement DML and DDL auditing
- Send audit records to OS files

Lesson 5 : Auditing DML Statements

- Implement fine-grained auditing (FGA)
- Maintain FGA policies
- Implement an FGA audit event handler
- Read FGA audit events from the FGA audit trail

Lesson 6 : Using Basic User Authentication

- Authenticate users with passwords
- Protect passwords
- Authenticate users with the operating system (OS)
- Restrict remote OS authentication
- Protect database link passwords

Lesson 7 : Using Strong Authentication

- Describe strong authentication by using:
  - Certificates
  - Kerberos
  - RADIUS
- Describe a setup for strong authentication by using:
  - Certificates
  - Kerberos
  - KDC
- Implement the secure external password store

Lesson 8 : Using Enterprise User Security

- Describe Enterprise User Security
- Set up Enterprise User Security
- Create an enterprise user
- Use shared schemas
- Use enterprise roles
- Audit enterprise users
- Enable enterprise roles
- Migrate users from the database to Oracle Internet Directory

Lesson 9 : Using Proxy Authentication

- Describe how proxy authentication works
- Manage users being authenticated by using proxy authentication
- Audit users authenticated by proxy

Lesson 10 : Using Privileges and Roles

- Implement roles
- Implement the securing of objects through procedures
- Describe how secure application roles work
- Manage roles and users by using secure application roles

Lesson 11 : Using Application Contexts

- Describe how an application context is used
- Describe the sources of application context values
- Implement a local context
- Implement an application context that is accessed globally

Lesson 12 : Implementing Fine-Grained Access Control I

- Describe how fine-grained access control (FGAC) and the Virtual Private Database (VPD) work
- Implement FGAC or the VPD
- Group policies

Lesson 13 : Installing Oracle Label Security

- Describe Oracle Label Security
- Install Oracle Label Security

Lesson 14 : Implementing Oracle Label Security

- Creating policies
- Defining labels
- Setting up user authorizations
- Applying policies to tables

Lesson 15 : Encryption Concepts

- Understand the issues of encryption
- Discuss challenges of encryption
- Describe key management solutions
- Describe the encryption options available with Oracle Database 10g

Lesson 16 : Using Application-Based Encryption

- Use DBMS_CRYPTO to:
    - Generate random encryption keys
    - Encrypt and decrypt table columns

Lesson 17 : Applying Transparent Data Encryption

- Set up the database master encryption key
- Implement Transparent Data Encryption
- Encrypt column data

Lesson 18 : Applying File Encryption

- Use RMAN encrypted backups
- Oracle Secure Backup
- Use Data Pump export encryption

Lesson 19 : Oracle Net Services: Security Checklists

- Describe the items on the client, listener, and network security checklists
- Secure administration of the network
- Restrict access by IP address
- Encrypt network traffic

Lesson 20 : Securing the Listener

- Describe how to limit the privileges of the listener
- Administer the listener securely
- Analyze listener log files

For more information please contact :
VT Technology Co.,Ltd.
Tel +66 0 2594 5185 Fax +66 0 2101 9725
contact@vttech.co.th

To see other available Oracle courses
please go to www.vttech.co.th/course.html