Course Outline

Oracle 12c/18c Database Security (Hardening, Detective and Audit Control)

Course Summary

Description

Oracle Database 12c Security helps DBAs, developers, and architects to better understand database security challenges.

This course will guide you through the process of implementing appropriate security mechanisms, helping you to ensure you are taking proactive steps to keep your data safe. Featuring solutions for common security problems in the new Oracle Database 12c, with this course you can be confident about securing your database from a range of different threats and problems.

Topics

- Security Considerations in Multitenant Environment
- PL/SQL Security
- Virtual Private Database
- Data Redaction
- Transparent Sensitive Data Protection
- Privilege Analysis
- Transparent Data Encryption
- Database Vault
- Unified Auditing
- Additional Topics
- Appendix – Application Contexts
- Resources

Prerequisite

Required: Basic computer skills, internet access, basic analytic or programming skills.

Duration

Three Days

Course Outline

Oracle 12c/18c Database Security (Hardening, Detective and Audit Control)

Course Outline

I. *Security Considerations in Multitenant Environment*

A. Creating a common user
- LAB01. Creating a common user

B. Creating a local user
- LAB02. Creating a local user

C. Creating a common role
- LAB03. Creating a common role

D. Creating a local role
- LAB04. Creating a local role

E. Granting privileges and roles commonly
- LAB05. Granting privileges and roles commonly

F. Granting privileges and roles locally
- LAB06. Granting privileges and roles locally

G. Effects of plugging/unplugging operations on users, roles, and privileges
- LAB07. Effects of plugging/unplugging operations on users, roles, and privileges

II. *PL/SQL Security*

A. Creating and using definer's rights procedures
- LAB01. Creating and using definer's rights procedures

B. Creating and using invoker's right procedures
- LAB02. Creating and using invoker's right procedures

C. Using code-based access control
- LAB03. Using code-based access control

D. Restricting access to program units by using accessible by
- LAB04. Restricting access to program units by using accessible by

III. *Virtual Private Database*

A. Creating different policy functions
- LAB01. Creating different policy functions

B. Creating Oracle Virtual Private Database row-level policies
- LAB02. Creating Oracle Virtual Private Database row-level policies

C. Creating column-level policies
- LAB03. Creating column-level policies

D. Creating a driving context
- LAB04. Creating a driving context

E. Creating policy groups
- LAB05. Creating policy groups

F. Setting context as a driving context
- LAB06. Setting context as a driving context

G. Adding policy to a group
- LAB07. Adding policy to a group

H. Exempting users from VPD policies
- LAB08. Exempting users from VPD policies

IV. *Data Redaction*

A. Creating a redaction policy when using full redaction
- LAB01. Creating a redaction policy when using full redaction

B. Creating a redaction policy when using partial redaction
- LAB02. Creating a redaction policy when using partial redaction

C. Creating a redaction policy when using random redaction
- LAB03. Creating a redaction policy when using random redaction

D. Creating a redaction policy when using regular expression redaction
- LAB04. Creating a redaction policy when using regular expression redaction

E. Using Oracle Enterprise Manager Cloud Control 12c to manage redaction policies

Course Outline

Oracle 12c/18c Database Security (Hardening, Detective and Audit Control)

Course Outline (cont.)

- LAB05. Using Oracle Enterprise Manager Cloud Control 12c to manage redaction policies

F. Changing the function parameters for a specified column
- LAB06. Changing the function parameters for a specified column

G. Add a column to the redaction policy
- LAB07. Add a column to the redaction policy

H. Enabling, disabling, and dropping redaction policy
- LAB08. Enabling, disabling, and dropping redaction policy

I. Exempting users from data redaction policies
- LAB09. Exempting users from data redaction policies

V. *Transparent Sensitive Data Protection*

A. Creating a sensitive type
- LAB01. Creating a sensitive type

B. Determining sensitive columns
- LAB02. Determining sensitive columns

C. Creating transparent sensitive data protection policy
- LAB03. Creating transparent sensitive data protection policy

D. Associating transparent sensitive data protection policy with sensitive type
- LAB04. Associating transparent sensitive data protection policy with sensitive type

E. Enabling, disabling, and dropping policy
- LAB05. Enabling, disabling, and dropping policy

F. Altering transparent sensitive data protection policy
- LAB06. Altering transparent sensitive data protection policy

VI. *Privilege Analysis*

A. Creating database analysis policy
- LAB01. Creating database analysis policy

B. Creating role analysis policy
- LAB02. Creating role analysis policy

C. Creating context analysis policy
- LAB03. Creating context analysis policy

D. Creating combined analysis policy
- LAB04. Creating combined analysis policy

E. Starting and stopping privilege analysis
- LAB05. Starting and stopping privilege analysis

F. Reporting on used system privileges
- LAB06. Reporting on used system privileges

G. Reporting on used object privileges
- LAB07. Reporting on used object privileges

H. Reporting on unused system privileges
- LAB08. Reporting on unused system privileges

I. Reporting on unused object privileges
- LAB09. Reporting on unused object privilege

J. How to revoke unused privileges
- LAB10. How to revoke unused privileges

K. Dropping the analysis
- LAB11. Dropping the analysis

VII. *Transparent Data Encryption*

A. Configuring keystore location in sqlnet.ora
- LAB01. Configuring keystore location in sqlnet.ora

B. Creating and opening the keystore
- LAB02. Creating and opening the keystore

C. Setting master encryption key in software keystore

Course Outline

Oracle 12c/18c Database Security (Hardening, Detective and Audit Control)

Course Outline (cont.)

- LAB03. Setting master encryption key in software keystore

D. Column encryption - adding new encrypted column to table
- LAB04. Column encryption - adding new encrypted column to table

E. Column encryption - creating new table that has encrypted column(s)
- LAB05. Column encryption - creating new table that has encrypted column(s)

F. Using salt and MAC
- LAB06. Using salt and MAC

G. Column encryption - encrypting existing column
- LAB07. Column encryption - encrypting existing column

H. Auto-login keystore
- LAB08. Auto-login keystore

I. Encrypting tablespace
- LAB09. Encrypting tablespace

J. Rekeying
- LAB10. Rekeying

K. Backup and Recovery
- LAB11. Backup and Recovery

VIII. *Database Vault*

A. Registering Database Vault

B. Preventing users from exercising system privileges on schema objects

C. Securing roles

D. Preventing users from executing specific command on specific object

E. Creating a rule set

F. Creating a secure application role

G. Using Database Vault to implement that administrators cannot view data
- LAB01. Registering Database Vault
- LAB02. Preventing users from exercising system privileges on schema objects
- LAB03. Securing roles
- LAB04. Preventing users from executing specific command on specific object
- LAB05. Creating a rule set
- LAB06. Creating a secure application role
- LAB07. Using Database Vault to implement that administrators cannot view data
- LAB08. Running Oracle Database Vault reports
- LAB09. Disabling Database Vault
- LAB10. Re-enabling Database Vault

H. Running Oracle Database Vault reports

I. Disabling Database Vault

J. Re-enabling Database Vault

IX. *Unified Auditing*

A. Enabling Unified Auditing mode
- LAB01. Enabling Unified Auditing mode

B. Configuring whether loss of audit data is acceptable
- LAB02. Configuring whether loss of audit data is acceptable

C. Which roles do you need to have to be able to create audit policies and to view audit data?
- LAB03. Which roles do you need to have to be able to create audit policies and to view audit data?

D. Auditing RMAN operations
- LAB04. Auditing RMAN operations

E. Auditing Data Pump operations
- LAB05. Auditing Data Pump operations

F. Auditing Database Vault operations
- LAB06. Auditing Database Vault operations

G. Creating audit policies to audit privileges, actions and roles under specified conditions

Course Outline

Oracle 12c/18c Database Security (Hardening, Detective and Audit Control)

Course Outline (cont.)

- LAB07. Creating audit policies to audit privileges, actions and roles under specified conditions

H. Enabling audit policy
- LAB08. Enabling audit policy

I. Finding information about audit policies and audited data
- LAB09. Finding information about audit policies and audited data

J. Auditing application contexts
- LAB10. Auditing application contexts

K. Purging audit trail
- LAB11. Purging audit trail

L. Disabling and dropping audit policies
- LAB12. Disabling and dropping audit policies

X. *Additional Topics*

A. Exporting data using Oracle Data Pump in Oracle Database Vault environment
- LAB01. Exporting data using Oracle Data Pump in Oracle Database Vault environment

B. Creating factors in Oracle Database Vault
- LAB02. Creating factors in Oracle Database Vault

C. Using TDE in a multitenant environment
- LAB03. Using TDE in a multitenant environment

XI. *Appendix – Application Contexts*

A. Exploring and using built-in contexts
- LAB01. Exploring and using built-in contexts

B. Creating an application context
- LAB02. Creating an application context

C. Setting application context attributes
- LAB03. Setting application context attributes

D. Using an application context
- LAB04. Using an application context

XII. *Resources*

A. Resources