Part III

Controlling Access to Data

Part III describes how to control access to data.

- Using Application Contexts to Retrieve User Information
  An application context stores user identification that can enable or prevent a user from accessing data in the database.

- Using Oracle Virtual Private Database to Control Data Access
  Oracle Virtual Private Database (VPD) enables you to filter users who access data.

- Using Transparent Sensitive Data Protection

- Encryption of Sensitive Credential Data in the Data Dictionary
  You can encrypt sensitive credential information, such as passwords that are stored in the data dictionary.

- Securing and Isolating Resources Using DbNest
  You can secure and isolate instance-level and operating system resources by using dbNest.

- On-Demand Encryption of Data
  You can use the `DBMS_CRYPTO` PL/SQL package to perform on-demand encryption of data.