Part I

Managing User Authentication and Authorization

Part I describes how to manage user authentication and authorization.

- Managing Security for Oracle Database Users
  You can manage the security for Oracle Database users in many ways, such as enforcing restrictions on the way that passwords are created.

- Configuring Authentication
  Authentication means to verify the identity of users or other entities that connect to the database.

- Configuring Privilege and Role Authorization
  Privilege and role authorization controls the permissions that users have to perform day-to-day tasks.

- Performing Privilege Analysis to Identify Privilege Use
  Privilege analysis dynamically analyzes the privileges and roles that users use and do not use.

- Configuring Centrally Managed Users with Microsoft Active Directory
  Oracle Database can authenticate and authorize Microsoft Active Directory users with the database directly without intermediate directories or Oracle Enterprise User Security.

- Authenticating and Authorizing IAM Users for Oracle DBaaS Databases
  Identity and Access Management (IAM) users can be configured to connect to an Oracle Database as a service (Oracle DBaaS) instance.

- Authenticating and Authorizing Microsoft Azure Users for Oracle Databases
  An Oracle database can be configured for Microsoft Azure users of Microsoft Entra ID (previously called Microsoft Azure AD) to connect using single sign-on authentication.

- Managing Security for Definer's Rights and Invoker's Rights
  Invoker's rights and definer's rights have several security advantages when used to control access to privileges during user-defined procedure executions.

- Managing Fine-Grained Access in PL/SQL Packages and Types
  Oracle Database provides PL/SQL packages and types for fine-grained access to control access to external network services and wallets.

- Managing Security for a Multitenant Environment in Enterprise Manager
  You can manage common and local users and roles by using Oracle Enterprise Manager.

ORACLE®