59

2.3 Oracle Database Vault-Specific Database Roles to Enforce Separation of Duties

The Oracle Database Vault configuration implements the concept of *separation of duty* so that you can improve security and meet regulatory, privacy, and other compliance requirements.

59

Oracle Database Vault makes clear separation between the account management responsibility, data security responsibility, and database management responsibility inside the database. This means that the concept of a super-privileged role (for example, `DBA`) is divided among several new database roles to ensure no one user has full control over both the data and configuration of the system. Oracle Database Vault prevents privileged users (those with the `DBA` and other privileged roles and system privileges) from accessing designated protected areas of the database called realms. It also introduces new database roles called the Oracle Database Vault Owner (`DV_OWNER`) and the Oracle Database Vault Account Manager (`DV_ACCTMGR`). These new database roles separate the data security and the account management from the traditional `DBA` role. You should map these roles to distinct security professionals within your organization.

Related Topics

- Separation of Duty Guidelines
  Oracle Database Vault is designed to easily implement separation of duty guidelines.
- Oracle Database Vault Roles
  Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

2.4 Privileges That Are Revoked from Existing Users and Roles

The Oracle Database Vault configuration revokes privileges from several Oracle Database-supplied users and roles, for better separation of duty.

Table 2-2 lists privileges that Oracle Database Vault revokes from the Oracle Database-supplied users and roles. Be aware that if you disable Oracle Database Vault, these privileges remain revoked. If your applications depend on these privileges, then grant them to application owner directly. In a multitenant environment, these privileges are revoked from the users and roles in the CDB root and its PDBs and from the application root and its PDBs.

Table 2-2 Privileges Oracle Database Vault Revokes

User or Role	Privilege That Is Revoked
`DBA` role	• `BECOME USER` • `SELECT ANY TRANSACTION` • `CREATE ANY JOB` • `CREATE EXTERNAL JOB` • `EXECUTE ANY PROGRAM` • `EXECUTE ANY CLASS` • `MANAGE SCHEDULER` • `DEQUEUE ANY QUEUE` • `ENQUEUE ANY QUEUE` • `MANAGE ANY QUEUE`