5

Managing Users and Securing the Database

Establish a security policy for every database.

- The Importance of Establishing a Security Policy for Your Database
  It is important to develop a security policy for every database. The security policy establishes methods for protecting your database from accidental or malicious destruction of data or damage to the database infrastructure.
- Managing Users and Resources
  To connect to the database, each user must specify a valid user name that has been previously defined to the database. An account must have been established for the user, with information about the user being stored in the data dictionary.
- User Privileges and Roles
  Privileges and roles are used to control user access to data and the types of SQL statements that can be executed.
- Auditing Database Activity
  You can monitor and record selected user database actions, including those performed by administrators. You can monitor system-wide actions as well as actions performed on individual database objects. This type of monitoring is called database auditing.
- Predefined User Accounts
  Oracle Database includes several predefined user accounts.

5.1 The Importance of Establishing a Security Policy for Your Database

It is important to develop a security policy for every database. The security policy establishes methods for protecting your database from accidental or malicious destruction of data or damage to the database infrastructure.

Each database can have an administrator, referred to as the security administrator, who is responsible for implementing and maintaining the database security policy If the database system is small, the database administrator can have the responsibilities of the security administrator. However, if the database system is large, a designated person or group of people may have sole responsibility as security administrator.

For information about establishing security policies for your database, see *Oracle Database Security Guide*.

5.2 Managing Users and Resources

To connect to the database, each user must specify a valid user name that has been previously defined to the database. An account must have been established for the user, with information about the user being stored in the data dictionary.

When you create a database user (account), you specify the following attributes of the user:

- User name

- Authentication method
- Default tablespace
- Temporary tablespace
- Other tablespaces and quotas
- User profile

To learn how to create and manage users, see *Oracle Database Security Guide*.

5.3 User Privileges and Roles

Privileges and roles are used to control user access to data and the types of SQL statements that can be executed.

The table that follows describes the three types of privileges and roles:

Type	Description
System privilege	A system-defined privilege usually granted only by administrators. These privileges allow users to perform specific database operations.
Object privilege	A system-defined privilege that controls access to a specific object.
Role	A collection of privileges and other roles. Some system-defined roles exist, but most are created by administrators. Roles group together privileges and other roles, which facilitates the granting of multiple privileges and roles to users.

Privileges and roles can be granted to other users by users who have been granted the privilege to do so. The granting of roles and privileges starts at the administrator level. At database creation, the administrative user `SYS` is created and granted all system privileges and predefined Oracle Database roles. User `SYS` can then grant privileges and roles to other users, and also grant those users the right to grant specific privileges to others.

To learn how to administer privileges and roles for users, see *Oracle Database Security Guide*.

5.4 Auditing Database Activity

You can monitor and record selected user database actions, including those performed by administrators. You can monitor system-wide actions as well as actions performed on individual database objects. This type of monitoring is called database auditing.

You can create unified audit policies and manage these audit policies using SQL statements. Oracle Database provides default unified audit policies that contain the standard audit settings, and you can create custom unified audit policies. You can also create fine-grained audit policies using the `DBMS_FGA` PL/SQL package.

> **See Also:**
>
> *Oracle Database Security Guide* for more information about database auditing

> **Note:**
>
> Starting with Oracle Database Release 21c, traditional auditing is desupported. Oracle recommends that you use unified auditing, which enables selective and more effective auditing inside Oracle Database.

5.5 Predefined User Accounts

Oracle Database includes several predefined user accounts.

The three types of predefined accounts are:

- Administrative accounts (`SYS`, `SYSTEM`, `SYSBACKUP`, `SYSDG`, `SYSKM`, `SYSRAC`, `SYSMAN`, and `DBSNMP`)

  `SYS`, `SYSTEM`, `SYSBACKUP`, `SYSDG`, `SYSKM`, and `SYSRAC` are described in "About Database Administrator Security and Privileges". `SYSMAN` is used to perform Oracle Enterprise Manager Cloud Control (Cloud Control) administration tasks. The management agent of Cloud Control uses the `DBSNMP` account to monitor and manage the database. You must not delete these accounts.

- Sample schema accounts

  These optional accounts are used for examples in Oracle Database documentation and instructional materials. The sample schema accounts are – `HR`, `SH`, and `OE`.

- Internal accounts

  These accounts are created so that individual Oracle Database features or components can have their own schemas. You must not delete internal accounts, and you must not attempt to log in with them.

> **Note:**
>
> Starting with Oracle Database 19c, most of the Oracle Database supplied user accounts, except `SYS` and sample schemas are *schema only* accounts, that is, these accounts are created without passwords. This prevents malicious users from logging into these accounts. You can assign passwords to these accounts whenever you want them to be authenticated, but Oracle recommends that for better security, you should change these accounts back to schema only accounts, when you do not need to authenticate them anymore.

> **See Also:**
>
> - *Oracle Database Security Guide* for information about all the predefined accounts provided by Oracle Database
> - *Oracle Database Security Guide* for information about schema only accounts
> - *Oracle Database Sample Schemas* for information about all the sample schemas provided by Oracle Database