Users and Roles

User Syntax

Simplified syntax for creating users (10g, 11g, 12c)

CREATE USER user\_name

IDENTIFIED BY *password*

DEFAULT TABLESPACE *tablespace\_name*

TEMPORARY TABLESPACE *temporary\_tablespace\_name*;

user\_name is the unique name of the new user that you are creating

*password* means the password that the user must specify to connect to the database

*tablespace\_name* specifies where the user’s objects (e.g. tables and sequences) are created

*temporary\_tablespace\_name* specifies the tablespace where the user’s temporary segments (used for sort and join operations) are stored

All identifiers (user\_name, *password, tablespace\_name, and temporary\_tablespace\_name*) must be between 1 and 30 characters, contain only alpha-numeric and the underscore, hashtag and dollar sign characters, must start with an alpha character, and cannot be a reserved word. Double quotes can be used to circumvent these rules but it is definitely not recommended.

Note: Oracle recommends a password with a minimum of 8 characters with at least one lowercase letter, one uppercase letter, and one digit; and the password should not be an actual word

Privileges

Authorization includes primarily two processes:

* Permitting only certain users to access, process, or alter data.
* Applying varying limitations on user access or actions. The limitations placed on (or removed from) users can apply to objects such as schemas, tables, or rows.

A user privilege is the right to run a particular type of SQL statement, or the right to access an object that belongs to another user, run a PL/SQL package, etc.

Roles

Roles are created by users (usually administrators) to group together privileges or other roles, Roles are used to streamline the granting / revoking of multiple privileges or roles to users

Role Syntax

CREATE ROLE *role\_name*

[ { NOT IDENTIFIED | IDENTIFIED BY password } ];

*role\_name* is the name of the new role that you are creating. This is how you will refer to the grouping of privileges.

*NOT IDENTIFIED* means that the role is immediately enabled. No password is required to enable the role.

*IDENTIFIED BY password* means that a user must supply a password to enable the role.

Grant Syntax

GRANT { system\_privilege | role\_name | ALL PRIVILEGES }

TO user\_name [ IDENTIFIED BY password ] [ WITH ADMIN OPTION ];

role\_name is the name of the role that you wish to grant.

*user\_name* is the name of the user that will be granted the role.

*IDENTIFIED BY* *password* resets the user’s password if the user exists; otherwise the user is created with that password and the role is granted to the new user

*WITH ADMIN OPTION* enables the grantee to:

* Grant the privilege or role to another user or role, unless the role is a GLOBAL role
* Revoke the privilege or role from another user or role
* Alter the privilege or role to change the authorization needed to access it
* Drop the privilege or role

Granting standard roles

GRANT connect, resource TO user\_name;

Granting extra roles needed to use the Debugger in SQL Developer

GRANT debug connect session, debug any procedure TO user\_name;

Granting extra role needed in 12c to allow users to allocate an extent (a number of contiguous data blocks allocated for storing information) in their tablespace

ALTER USER user\_name QUOTA UNLIMITED ON *tablespace\_name*;

The following three roles are provided to maintain compatibility with previous versions of Oracle and may not be created automatically in future versions of Oracle. Oracle recommends that you design your own roles for database security, rather than relying on these roles which may change or be deprecated or possibly discontinued.

| **Role Name** | **Description** |
| --- | --- |
| CONNECT | Probably includes the following system privileges: CREATE SESSION, SET CONTAINER  May include the following system privileges: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW |
| RESOURCE | Probably includes the following system privileges: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE |
| DBA | Probably includes all system privileges (approx. 241) WITH ADMIN OPTION |

Explanations taken wholly, or in part, from Oracle ® Database Security Guide 12c Release 1 (12.1) E17607-25 (<http://docs.oracle.com/cd/E16655_01/network.121/e17607.pdf>)