# PUBLIC Role in Oracle

blog.netwrix.com/2022/12/02/public-roles-in-oracle

Kevin Joyce

Roles make it easier to grant and revoke privileges for users of a relational database. Rather than managing privileges for each user individually, you manage privileges for each role and all changes apply to all users who are assigned that role. Organizations often create multiple roles to suit their unique needs.

Handpicked related content:

[Free Download] Sysadmin Magazine: The Power of Permissions

However, most databases come with a pre-defined role called PUBLIC. In this blog, we explain what the PUBLIC role means in Oracle and key best practices for using it.

## What is the PUBLIC role in Oracle?

PUBLIC role is a special role that every database user implicitly inherits on creation. The Oracle 11g documentation states that the PUBLIC role is accessible to every database user, and therefore all privileges and roles granted to the PUBLIC role are accessible to every database user. While an administrator can issue a command to grant the PUBLIC role to or revoke it from a particular user, these commands have no practical effect; the user will always have this role.

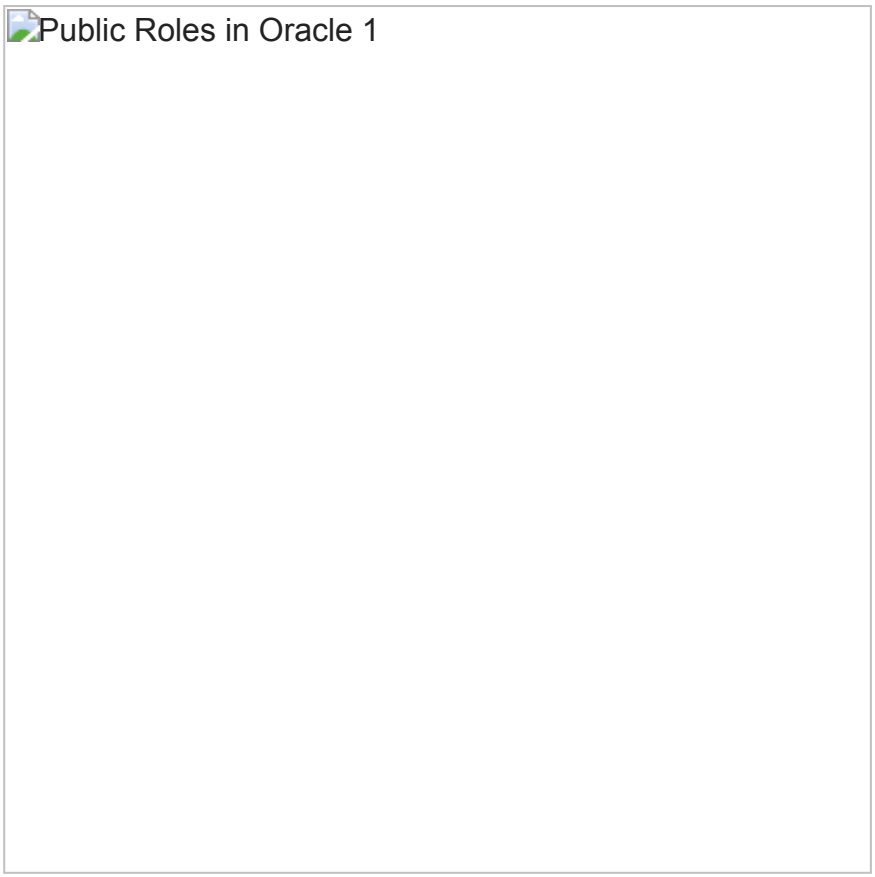
It is interesting to note the DBA_ROLES view does not list the PUBLIC role:

```
SQL> SELECT * FROM DBA_ROLES WHERE ROLE ='PUBLIC';

no rows selected
```

However, querying the SYS.USER$ table shows that PUBLIC does exist and its type# value of 0 indicates that it is a role:

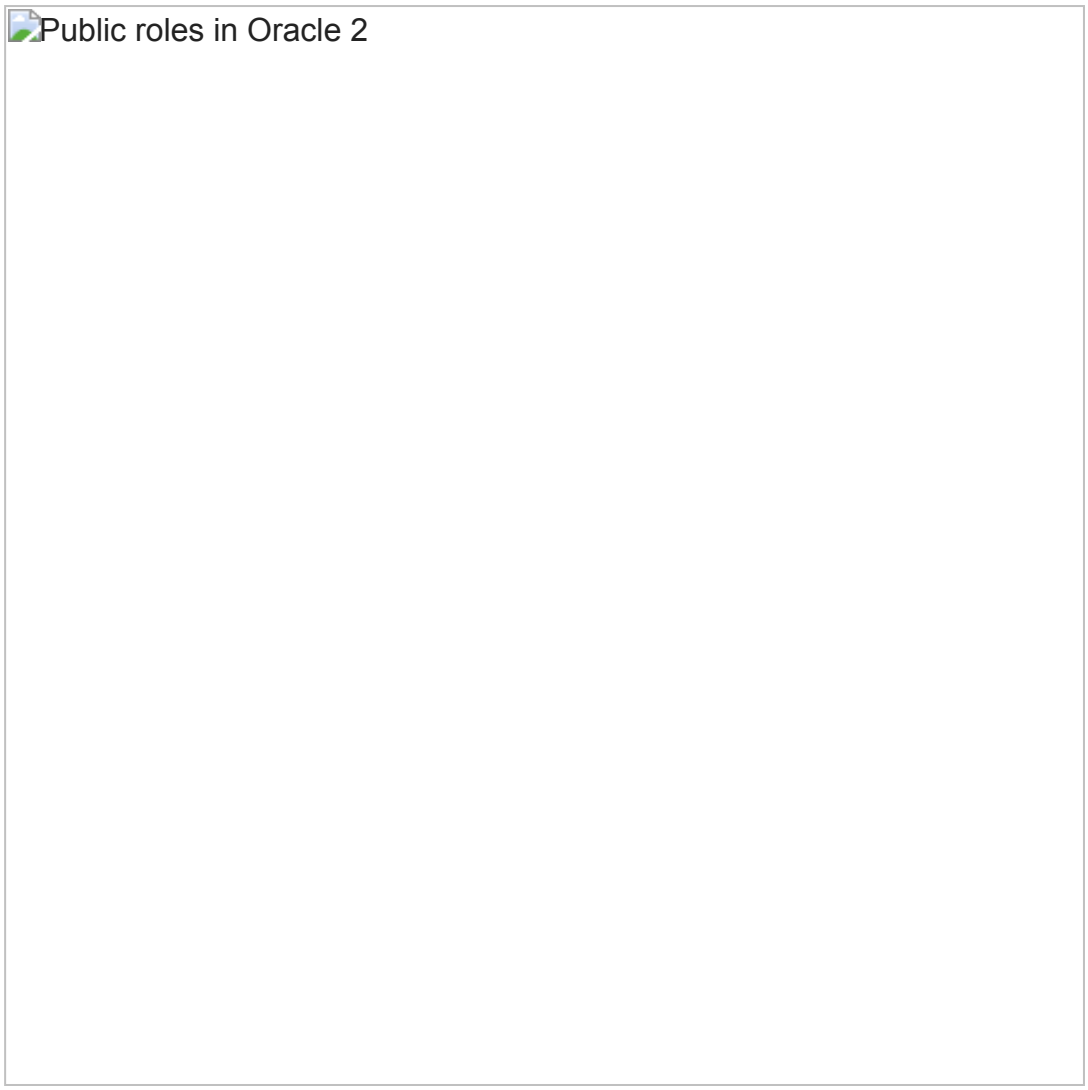
```
SQL> SELECT user#, type#, name FROM SYS.USER$ WHERE type# = 0 ORDER BY 1;
```




The implicit nature of PUBLIC role assignment to all database users can be seen in the following example. Granting the CONNECT privilege to the PUBLIC role will allow it to be inherited by the new user without being granted explicitly.

```
SQL> CREATE USER bob IDENTIFIED BY MyPassword;

SQL> conn bob/MyPassword;
```




## Best practices for the PUBLIC role

The PUBLIC role should not be used for user privilege management. In other words, never assign a privilege or role to PUBLIC unless the intent is to grant those privileges and roles to all current database users and to any new users that might be created in the future.

Indeed, granting privileges and roles directly to the PUBLIC role is classified as a *finding* by the Defense Information Systems Agency (DISA): DISA Security Technical Implementation Guide (STIG) vulnerability ID **V-61435** states that database or system privileges should not be granted to PUBLIC, and **V-61443** states that application role permissions should not be assigned to PUBLIC.

Understanding why requires some context. In a container database (CDB) or pluggable database (PDB) environment, there is a concept of common roles and local roles. In a CDB, common roles are created in the root and are known to all current and future containers. In A PDB environment, local roles are local to a specific PDB; they can be used only within the PDB they are defined in.

However, in an Oracle multi-tenant environment, roles are a bit more complicated. By default, all the privileges that Oracle grants to the PUBLIC role are granted locally and commonly. According to Oracle, privileges should never be granted to PUBLIC commonly. In other words, never grant any type of privilege to the PUBLIC role in the root or CDB. While it is possible to modify the PUBLIC role within each CDB separately, this is not recommended unless it is necessary.

Any user-granted privileges to the PUBLIC role can be revoked with no adverse consequences. But care should be taken when revoking default privileges granted to the PUBLIC role as part of database creation, since those privileges might be re-granted during a future upgrade or patching process.

For help enumerating all Oracle roles and privileges, including the PUBLIC role, consider investing in a third-party solution such as Netwrix StealthAUDIT, which can produce detailed entitlement reports out of the box.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.