

Oracle Security

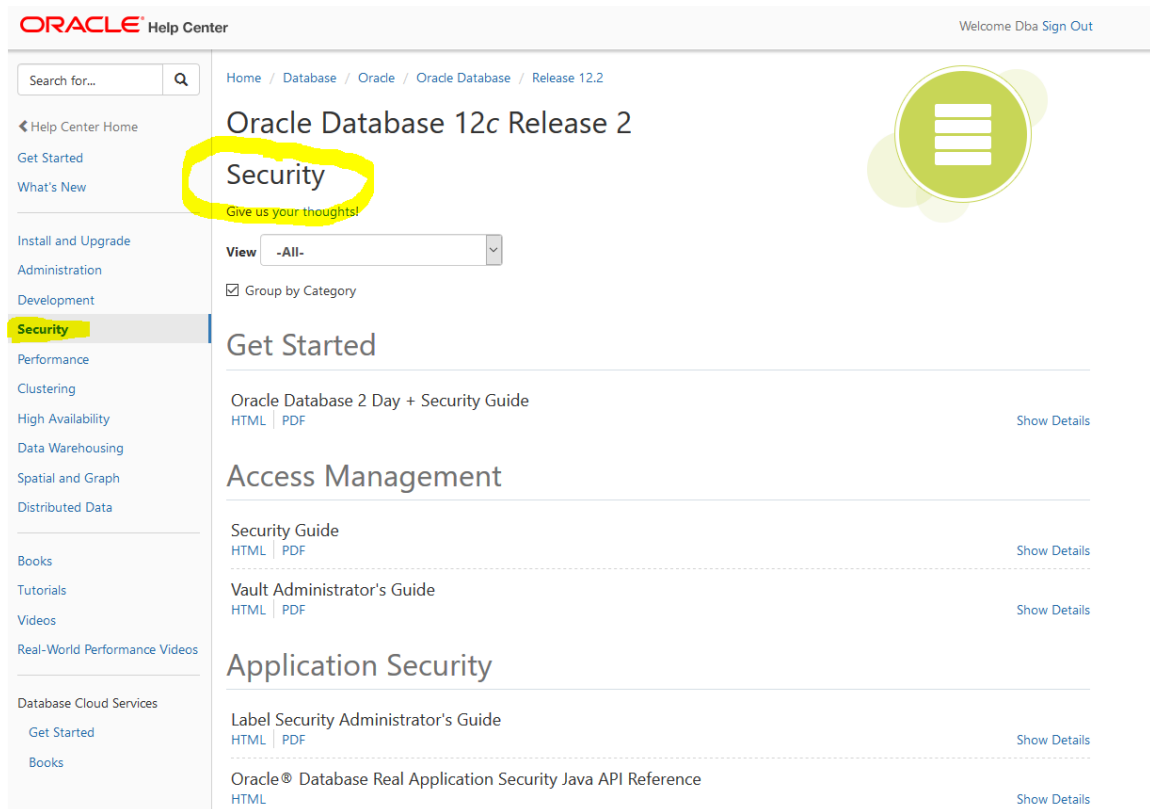
WEEK 10

What do you think of
when you're asked
about security?

The Most Important Security Concepts



In Depth Documentation



The screenshot shows the Oracle Help Center interface for Oracle Database 12c Release 2. The left sidebar contains a navigation menu with categories like 'Help Center Home', 'Get Started', 'What's New', 'Install and Upgrade', 'Administration', 'Development', 'Security' (highlighted), 'Performance', 'Clustering', 'High Availability', 'Data Warehousing', 'Spatial and Graph', 'Distributed Data', 'Books', 'Tutorials', 'Videos', 'Real-World Performance Videos', 'Database Cloud Services', 'Get Started', and 'Books'. The main content area is titled 'Oracle Database 12c Release 2' and features a 'Security' section highlighted with a yellow circle. Below this, there are links to 'Get Started', 'Access Management', and 'Application Security'.

ORACLE® Help Center

Welcome Db

Search for...

Home / Database / Oracle / Oracle Database / Release 12.2

Oracle Database 12c Release 2

Security

Give us your thoughts!

View -All-

☒ Group by Category

Get Started

Oracle Database 2 Day + Security Guide

HTML | PDF

Show Details

Access Management

Security Guide

HTML | PDF

Show Details

Vault Administrator's Guide

HTML | PDF

Show Details

Application Security

Label Security Administrator's Guide

HTML | PDF

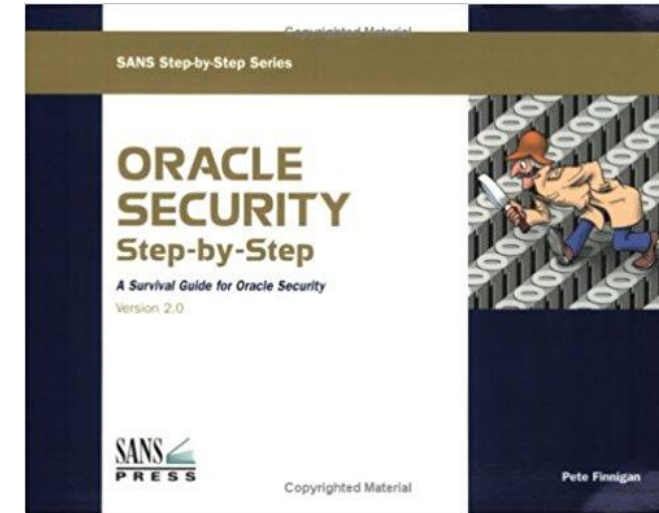
Show Details

Oracle® Database Real Application Security Java API Reference

HTML

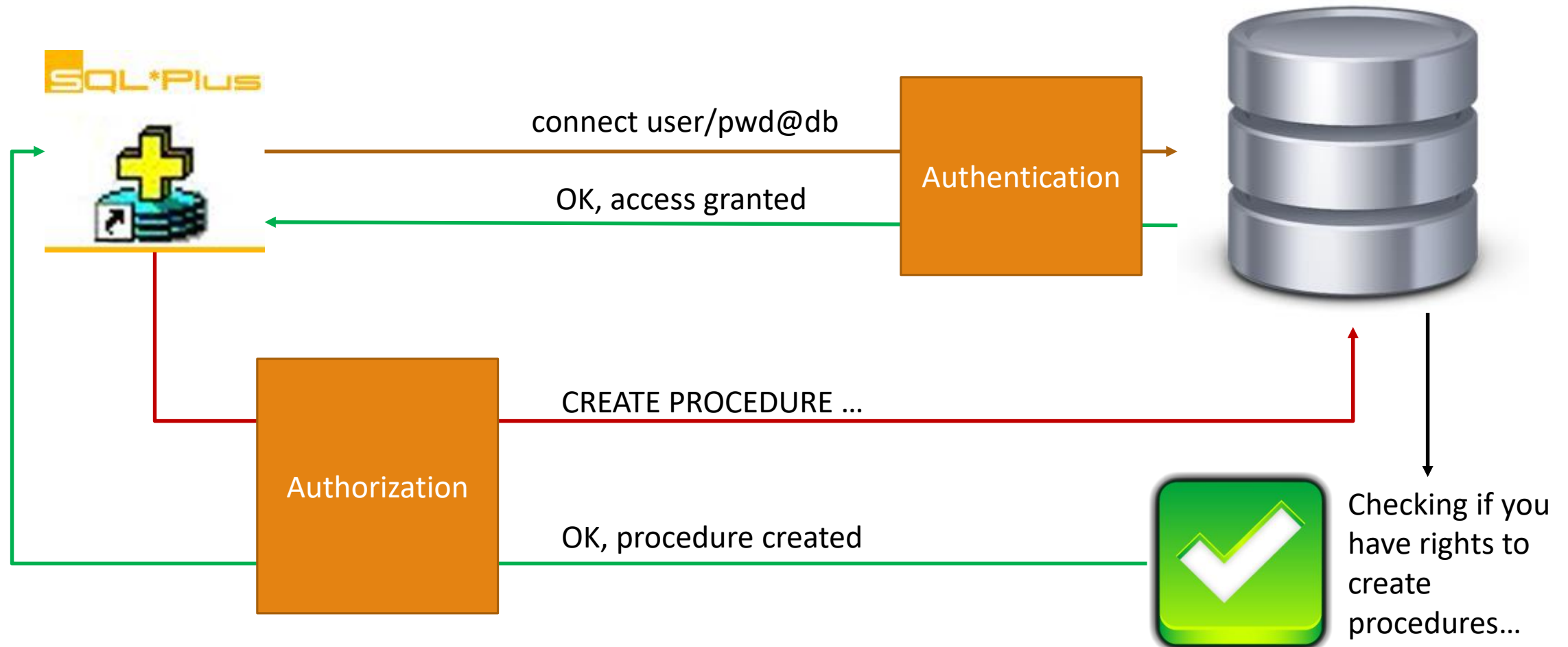
Show Details

<https://docs.oracle.com/en/database/oracle/oracle-database/12.2/security.html>



<https://www.amazon.com/gp/product/0974372749>

Authentication vs. Authorization



User Accounts

SYS: The most powerful user in the Oracle DB

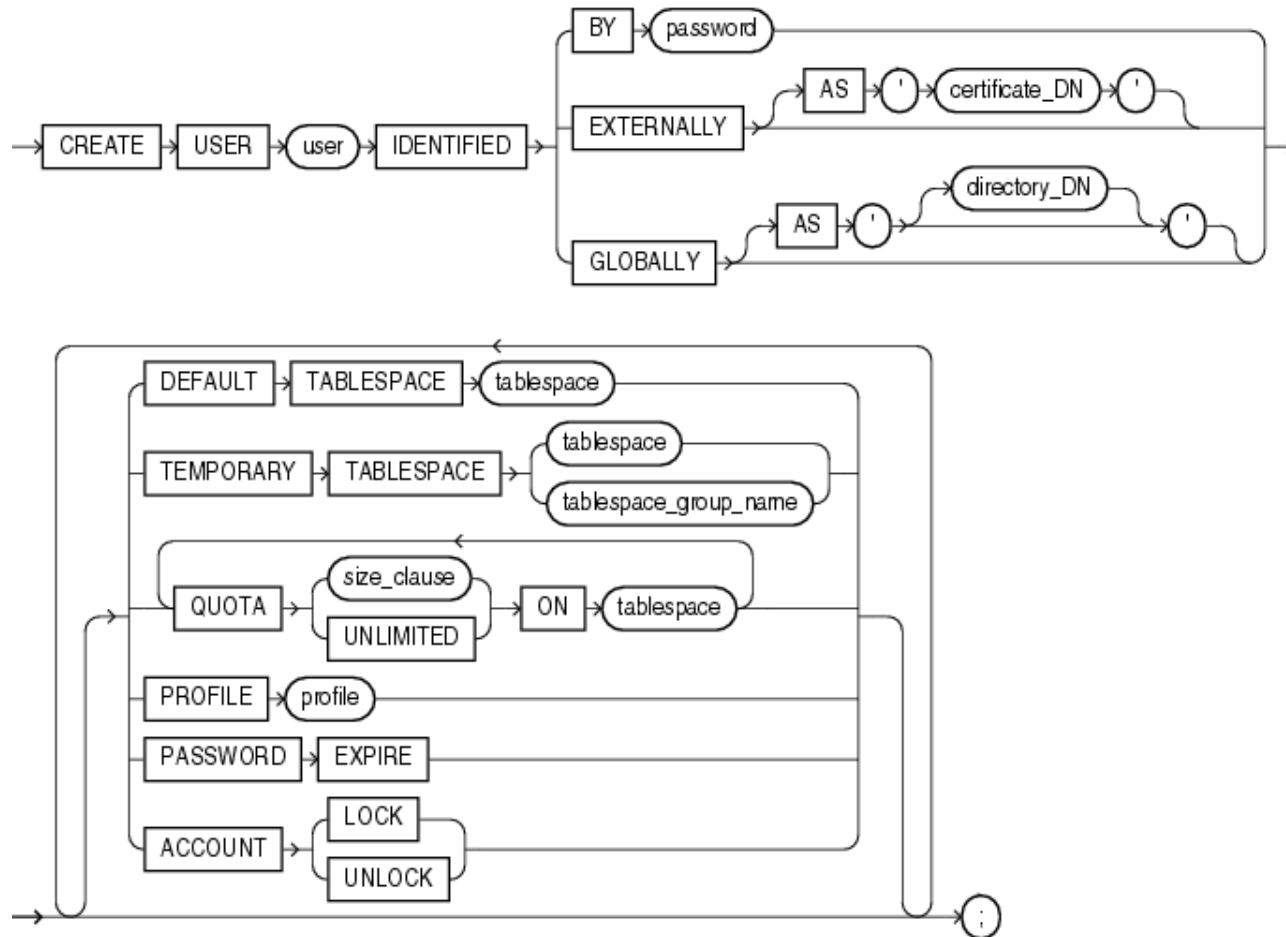
SYSTEM: A user with administrative rights, not so powerful as SYS, but still a very powerful user

Default Oracle Accounts

Account Categories

SYSDBA	Normal
SYS	SYSTEM
Allow access to the Oracle instance even though it's not opened	The DB must be opened for a normal user to be able to connect
It's mandatory to use "as sysdba" when connecting using this kind of user	A normal connect is used
Unlimited privileges including the dictionary tables	The access is controlled using Oracle privileges
The authentication is done externally (usually by the OS)	The authentication is done by the database itself

How to Create New Users



**USER =
SCHEMA**

DBA_USERS: all
users created in a
database

V\$PWFILERS: all
SYSDBA users

Metadata
About Users

Oracle Privileges

System privileges

- The right to connect: CREATE SESSION
- The right to create tables: CREATE TABLE
- The right to create PL/SQL procedures in any schema: CREATE ANY PROCEDURE

Object privileges:

- The right to query the T1 table from SCOTT user
- The right to delete records from a table belonging to another user

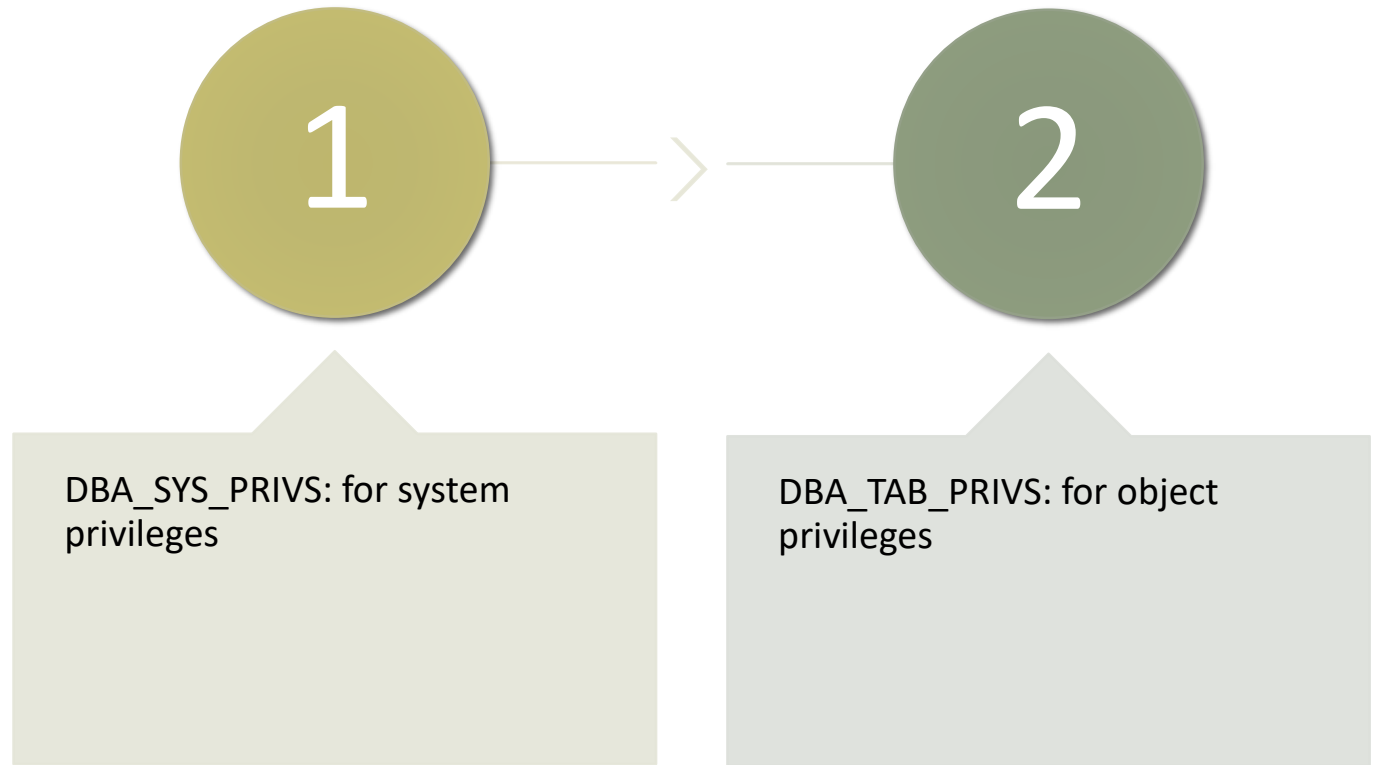
Privileges Categories

GRANT

REVOKE

DCL
Statements

Metadata About Privileges



Create a new user called
GOGU (choose
whatever password you
want)

Grant to GOGU the right
to connect to the
database and the right
to query the
MOVIES.RENTAL table

Connect with GOGU and
check if you are allowed
indeed to query the
MOVIES.RENTAL table.

How can you allow
access to just a few
columns from the
RENTAL table?

Challenge

Oracle Roles

A named collection of privileges
and/or other roles

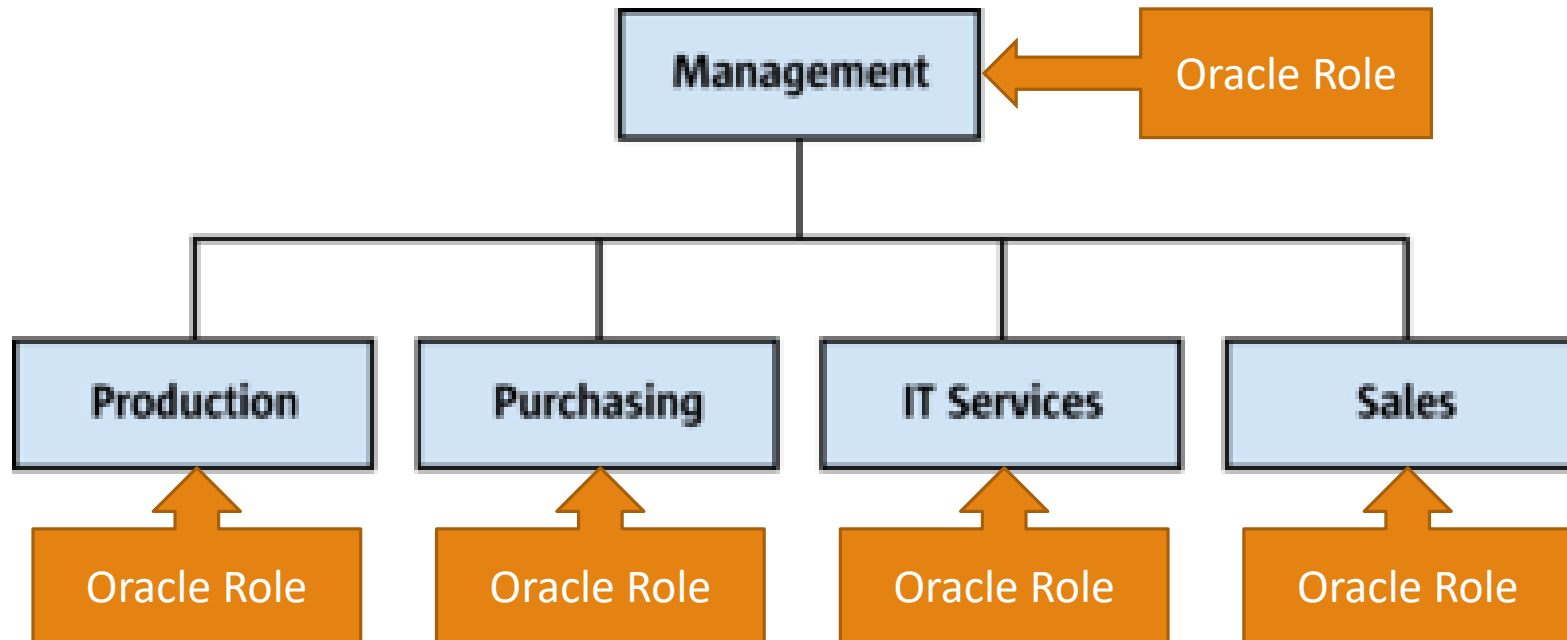
Oracle provides already a bunch
of pre-built roles: DBA,
DATAPUMP_EXP_FULL_DATABASE
etc.

The same role can be granted to
many users

A granted/revoked privilege from
a granted role becomes effective
for all users who were granted
that role

What is a Role?

Organizational Structure



How to Create a New Role

Create a new role:

```
CREATE ROLE MARKETING_ROLE;
```

Grant privileges to the role:

```
GRANT SELECT ON ERP.PROMOTIONS TO MARKETING_ROLE;
```

```
GRANT INSERT,UPDATE,DELETE ON ERP.SURVEYS TO MARKETING_ROLE;
```

Grant the role to a user:

```
GRANT MARKETING_ROLE TO GOGU;
```

DBA_ROLES

DBA_ROLES_PRIVS

DBA_SYS_PRIVS
(where GRANTEE
is the role)

DBA_TAB_PRIVS
(where GRANTEE
is the role)

Roles
Related
Dictionary
Views

Challenge

Our fictional movie store has a new SALES department.

The employees assigned to this department must be allowed to:

- Query, add, change, delete records from the MOVIES.RENTAL
- Query and add rows to MOVIES.PAYMENTS
- Query the MOVIES.STORE table

How would you design the authorization considering the above requirements?

How can you add GOGU to this new department?

That's all folks!

THANK YOU AND SEE YOU NEXT WEEK...