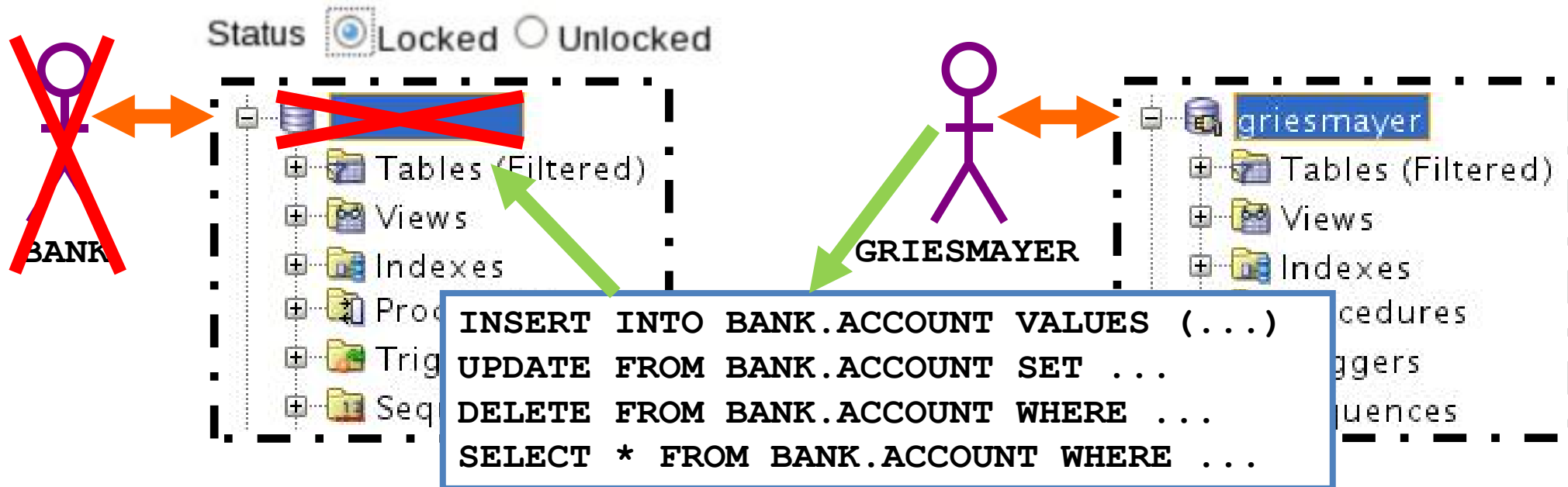


Rights

Mag. Thomas Griesmayer

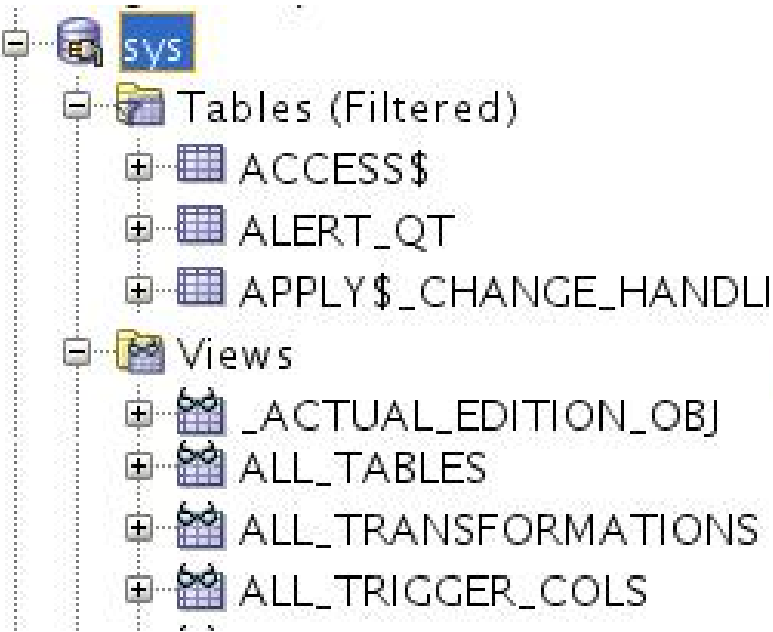
schema

- By creating a user, Oracle implicit creates a schema.
- A schema is a logical container (same name as the user) for database objects such as tables, views, triggers and so on.
- Deleting a user, all his objects has to be deleted.
- Never create database objects in a production environment in a schema owned by a real user.



SYS SYSTEM user

- SYS is the owner of the database and the owner of the data dictionary.
- SYSTEM is a privileged administration user, and typically owns Oracle provided tables other than the dictionary.
- Don't create objects in the schema of SYS or SYSTEM.

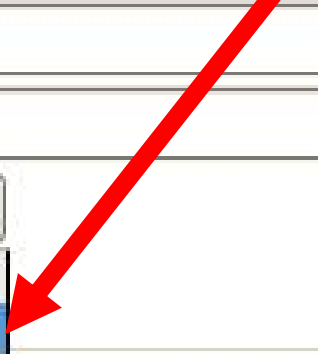


A tree view of the SYS schema in an Oracle database. The root is 'SYS', which contains two folders: 'Tables (Filtered)' and 'Views'. Under 'Tables (Filtered)', there are three tables: 'ACCESS\$', 'ALERT_QT', and 'APPLY\$_CHANGE_HANDLI'. Under 'Views', there are four views: '_ACTUAL_EDITION_OBJ', 'ALL_TABLES', 'ALL_TRANSFORMATIONS', and 'ALL_TRIGGER_COLS'.

INSTANCE:

- STARTUP
- SHUTDOWN
- BACKUP
- RECOVER
- CREATE

* User Name	<input type="text" value="SYS"/>
* Password	<input type="password" value="*****"/>
Connect As	<input type="text" value="Normal"/>
	<input type="text" value="Normal"/>
	<input type="text" value="SYSDBA"/>
	<input type="button" value="Login"/>

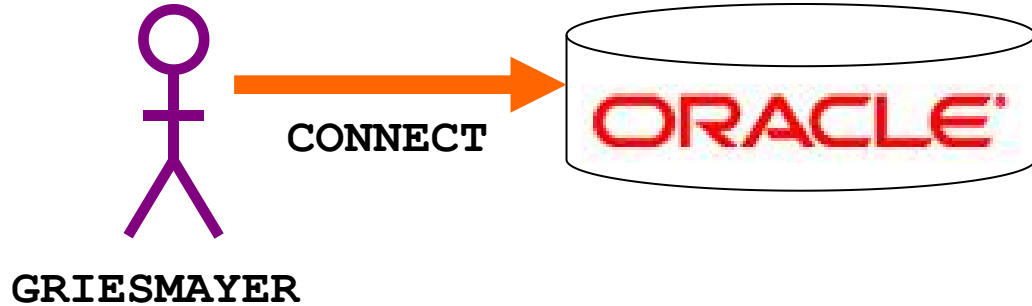


privileges

- System privileges

- › CREATE TABLE
- › CREATE ANY TABLE
- › CREATE USER
- › CONNECT

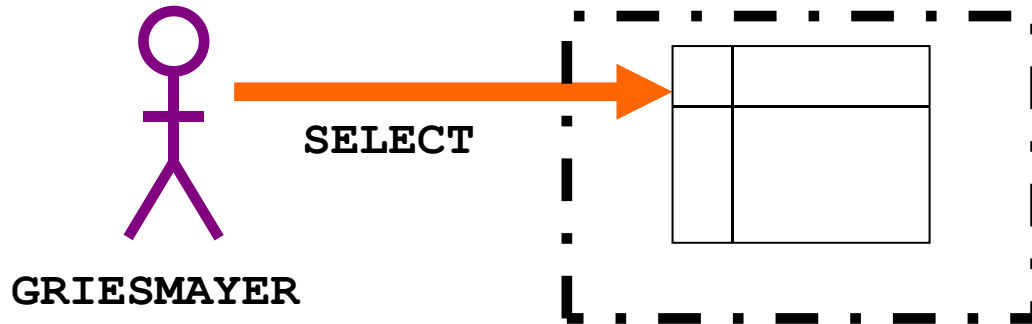
```
GRANT CONNECT TO griesmay;
```



- Object privileges

- › SELECT
- › DELETE
- › INSERT
- › UPDATE

```
GRANT SELECT ON BANK.ACCOUNT TO GRIESMAYER;  
GRANT INSERT ON BANK.ACCOUNT TO GRIESMAYER;
```



System Privileges

- A system privilege is the right to perform a particular action, or to perform an action on any schema objects of a particular type.
- For example, the privileges to create tablespaces and to delete the rows of any table in a database are system privileges.
- **ADMIN** - perform administrative tasks including checkpointing, backups, migration, and user creation and deletion.
- **ALTER ANY VIEW** - alter any view in the database.
- **CREATE ANY TABLE** - create a table owned by any user in the database.
- **CREATE ANY PROCEDURE** - create a PL/SQL procedure, function or package owned by any user in the database.
- **CREATE PROCEDURE** - create a PL/SQL procedure, function or package owned by that user.

Object Privileges

- A schema object privilege is the permission to perform a particular action on a specific schema object.
- Schema objects:
 - Table
 - View
 - Sequences
 - Procedure
 - Functions and Packages
 - Type
- Specify **WITH GRANT OPTION** to enable the grantee to grant the object privileges to other users.

GRANT SELECT ON ACCOUNT TO FRITZ WITH GRANT OPTION;

!!! uncontrollable !!!

Table

- You can grant privileges to use the **SELECT**, **DELETE**, **INSERT** and **UPDATE** DML operations on a table.
- Grant these privileges only to users and roles that need to query or manipulate data in a table.
- Alternatively, a view that excludes the salary column could satisfy this need for additional security.

View

- You can grant privileges to use the **DELETE**, **INSERT**, **SELECT**, and **UPDATE** DML operations on a view.

```
CREATE VIEW BANK.ACCOUNT_PUBLIC AS
SELECT ACCOUNT_ID,
        FIRST_NAME,
        LAST_NAME
        BALANCE
FROM    BANK.ACCOUNT;

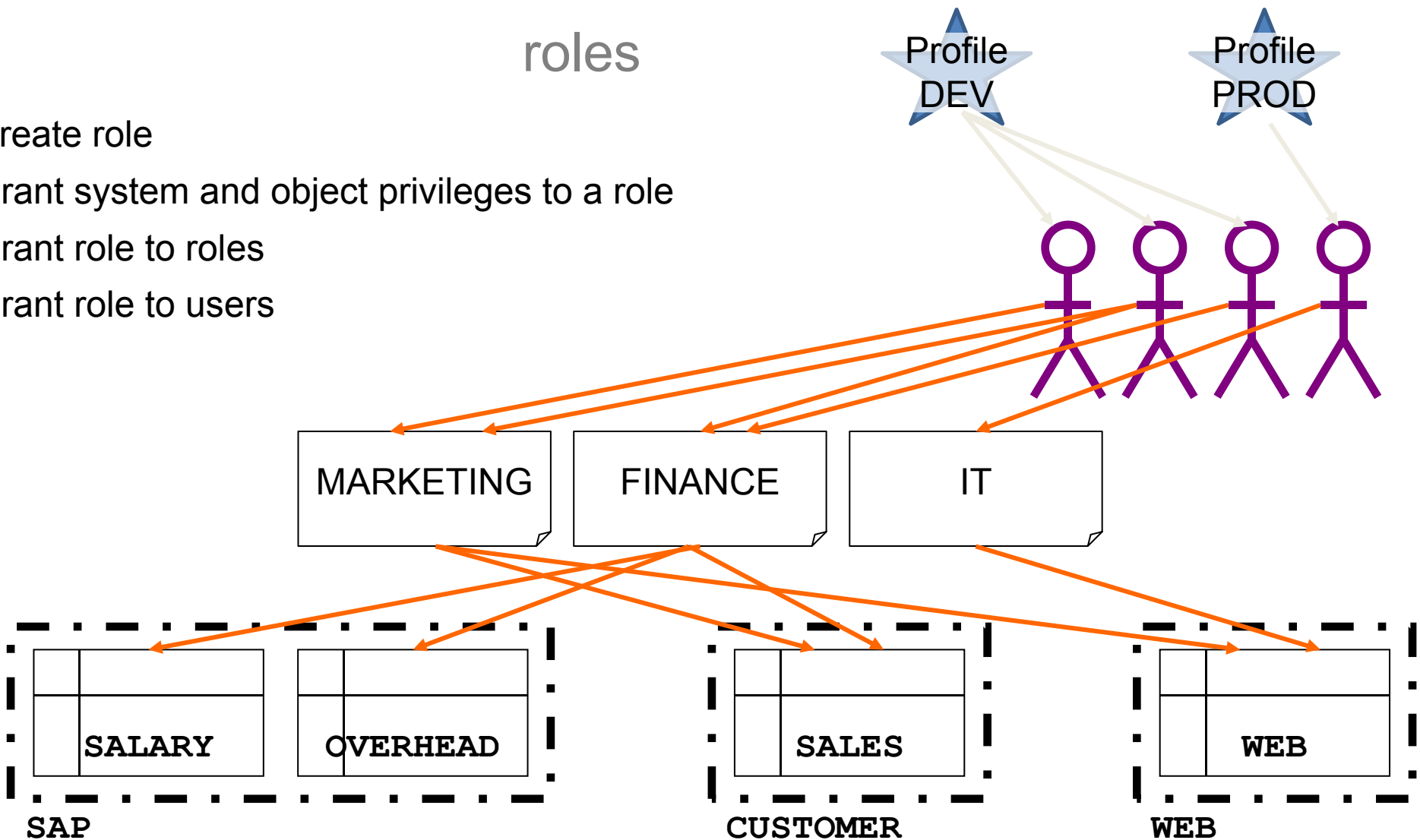
GRANT SELECT ON BANK.ACCOUNT_PUBLIC TO FRITZ;
```


Procedure

- **EXECUTE** is the only schema object privilege for procedures, including standalone procedures and functions as well as packages.

roles

- Create role
- Grant system and object privileges to a role
- Grant role to roles
- Grant role to users



predefined roles

- The **CONNECT** role enables a user to connect to the database.
- The **RESOURCE** role allows a user to create, modify and delete certain types of schema objects in his schema.

CREATE TABLE, CREATE PROCEDURE, ...

- The **DBA** role enables a user to perform most administrative functions.

DROP TABLE in any schema, CREATE USER, GRANT, ...

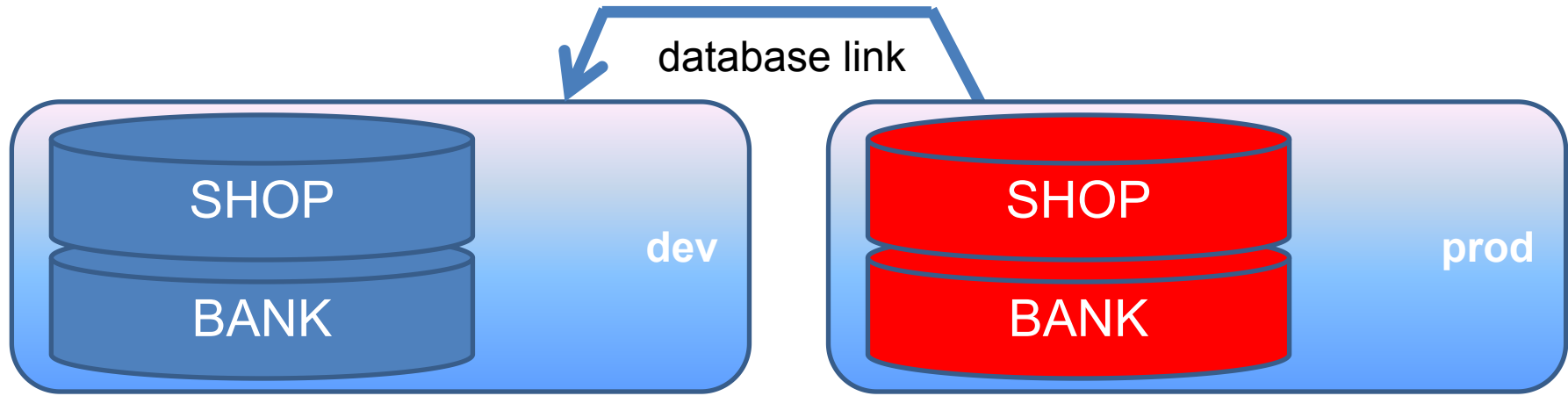
SQL

```
CREATE USER GRIESMAYER  
PROFILE STUDENT  
IDENTIFIED BY "oracle"  
DEFAULT TABLESPACE USERS  
TEMPORARY TABLESPACE TEMP  
QUOTA 1024000 K ON USERS  
ACCOUNT UNLOCK;
```

```
GRANT SELECT ANY DICTIONARY TO GRIESMAYER;  
GRANT SELECT ANY TABLE TO GRIESMAY;  
GRANT CONNECT TO GRIESMAY;
```

```
GRANT UPDATE ON BANK.ACCOUNT TO GRIESMAYER;  
GRANT INSERT ON BANK.ACCOUNT TO GRIESMAYER;
```

```
GRANT DEVELOP TO GRIESMAY;
```



GRIESMAYER

CONNECT

CREATE ANY TABLE

CREATE ANY VIEW

GRIESMAYER

CONNECT

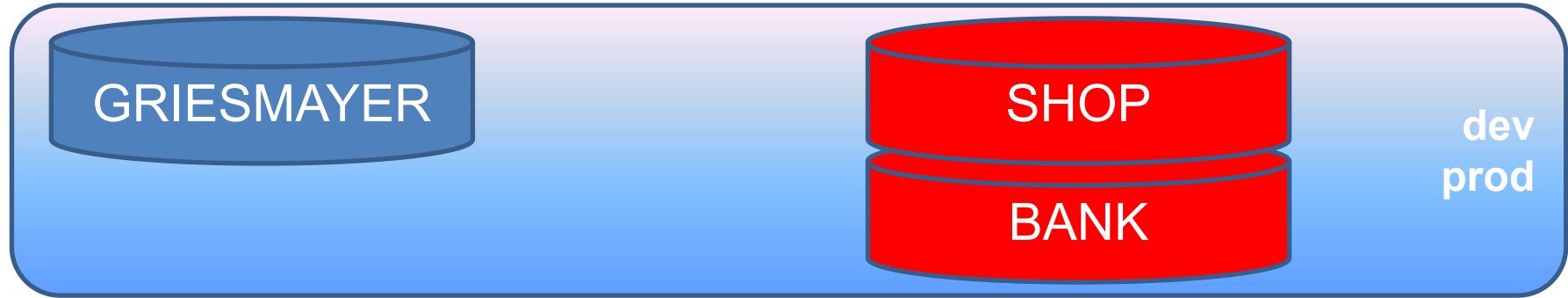
SELECT InternetShop

ADMIN

CONNECT

CREATE ANY TABLE

CREATE ANY VIEW



GRIESMAYER

CONNECT

CREATE TABLE

CREATE VIEW

SELECT BANK...

ADMIN

CONNECT

CREATE ANY TABLE

CREATE ANY VIEW