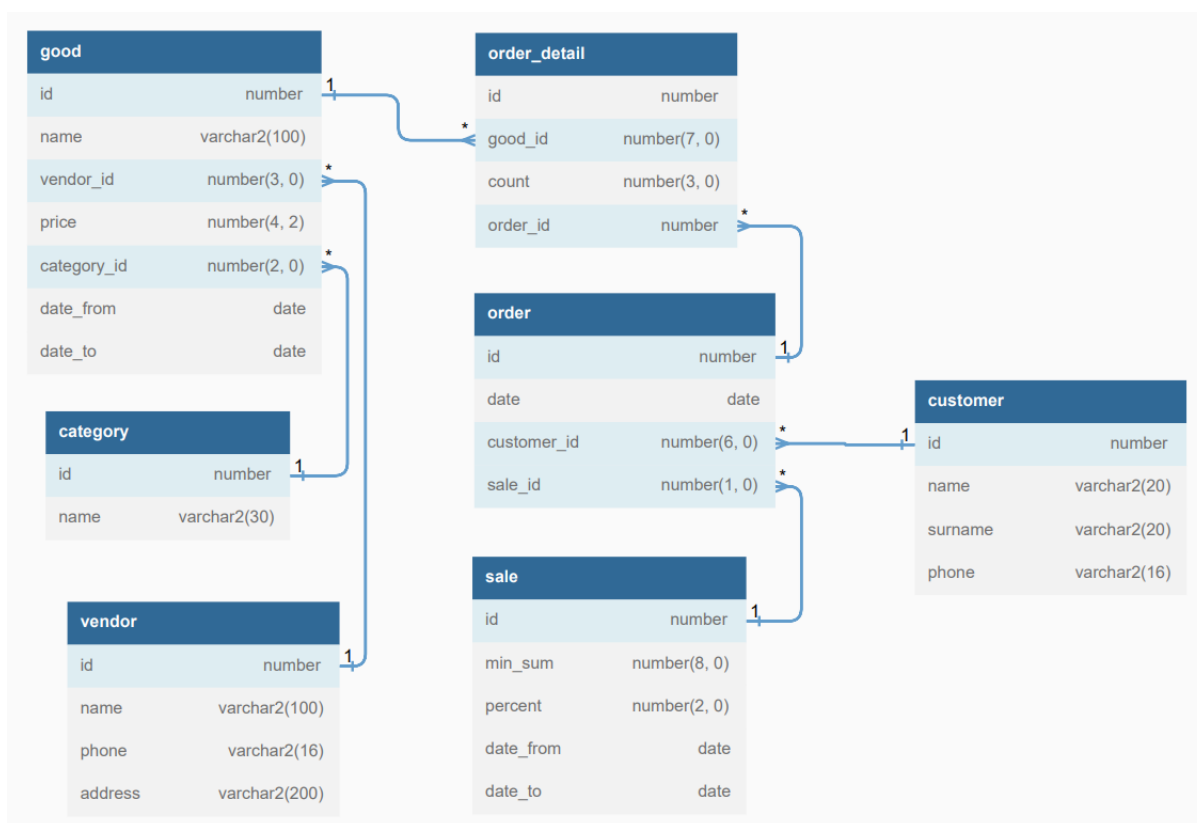


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №2-4:
«Аутентификация и базовый контроль доступа.»



Выполнила студентка группы Б19-515
Щербакова Александра

Москва, 2023 г.

1. Создание schema-only пользователей.

1) Обоснование необходимости.

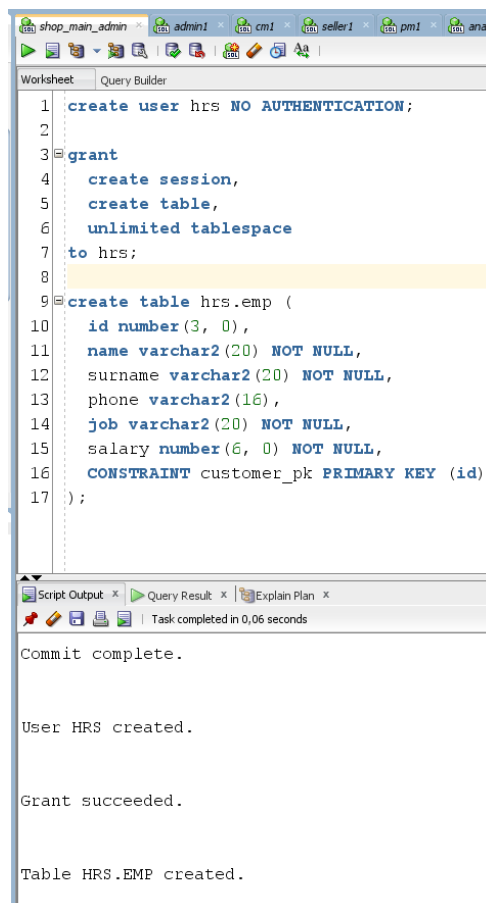
С расширением базы данных возникает необходимость создания нескольких схем для более простой процедуры создания ролей и выдачи привилегий пользователям. Таблицы должны быть физически (методом создания schema-only пользователей) разделены в соответствии с логикой БД: каждое приложение использует свою схему. Если несколькими приложениям требуется доступ к одной и той же схеме, надо выбрать тип разделяемой среды, например, «несколько схем» или «разделяемая схема».

// Источник: <https://www.interface.ru/fset.asp?Url=/oracle/0003.htm>

Все таблицы, существующие в рассматриваемой БД, тесно связаны между собой, так как типичные запросы требуют соединений их всех. Допустим, есть первое приложение в инфраструктуре магазина, имеющее доступ к семи имеющимся таблицам.

2) Тестирование (весь код в приложении А)

Расширим БД – пусть есть таблица сотрудников emp, а для работы с сотрудниками нужно второе приложение. Для этого организуем новую схему путем создания schema-only пользователя hrs (от имени shop_main_admin):



```
1 create user hrs NO AUTHENTICATION;
2
3 grant
4   create session,
5   create table,
6   unlimited tablespace
7 to hrs;
8
9 create table hrs.emp (
10  id number(3, 0),
11  name varchar2(20) NOT NULL,
12  surname varchar2(20) NOT NULL,
13  phone varchar2(16),
14  job varchar2(20) NOT NULL,
15  salary number(6, 0) NOT NULL,
16  CONSTRAINT customer_pk PRIMARY KEY (id)
17 );
```

Script Output x Query Result x Explain Plan x

Task completed in 0,06 seconds

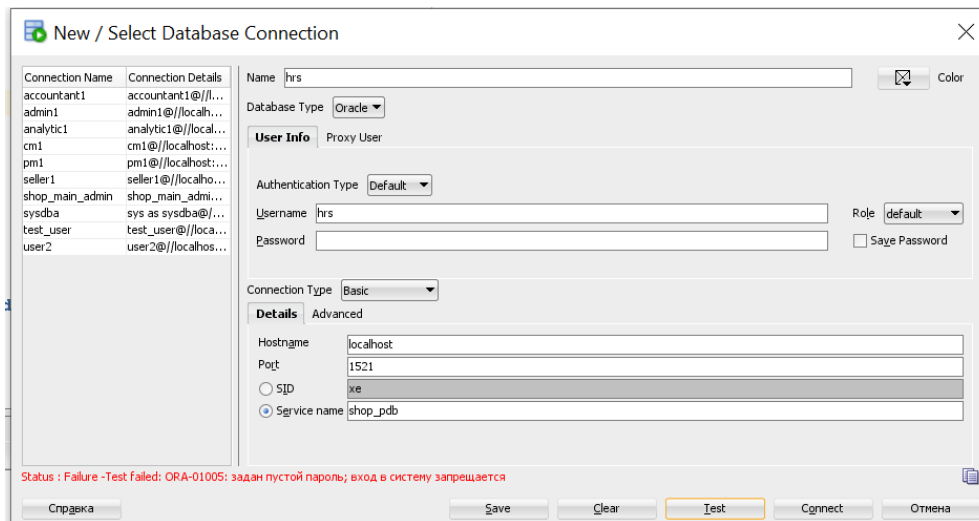
Commit complete.

User HRS created.

Grant succeeded.

Table HRS.EMP created.

Попробуем подключиться к БД в качестве пользователя hrs – невозможно.



Создадим новую роль hr и пользователя с этой ролью hr1. Выдадим новой роли привилегию на выборку из таблицы emp:

```
19 create public synonym emp for hrs.emp;
20
21 create role hr;
22 grant create session to hr;
23 grant select on emp to hr;
24
25 CREATE USER hr1
26     IDENTIFIED BY pas
27     DEFAULT TABLESPACE SHOP_PDB_USERS
28     TEMPORARY TABLESPACE temp
29     QUOTA 500M ON SHOP_PDB_USERS;
30 grant hr to hr1;
```

Grant succeeded.

Grant succeeded.

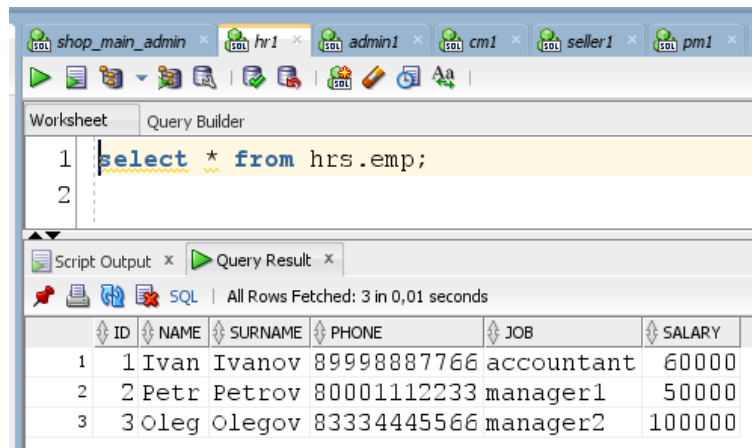
User HR1 created.

Grant succeeded.

Заполним от имени админа пару строк в таблице, не забыв выдать место в табличном пространстве для схемы.

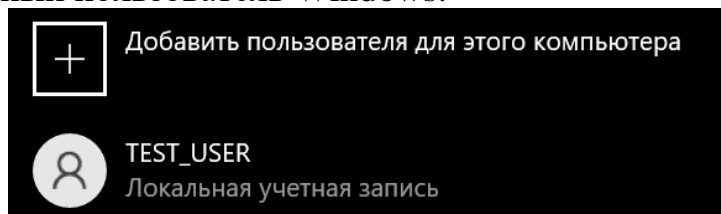
```
11 alter user hrs quota 100M on shop_pdb_users;
12
13 insert into emp values (1, 'Ivan', 'Ivanov', '89998887766', 'accountant', 60000);
14 insert into emp values (2, 'Petr', 'Petrov', '80001112233', 'manager1', 50000);
15 insert into emp values (3, 'Oleg', 'Olegov', '83334445566', 'manager2', 100000);
16
```

Теперь пользователь hr1 может работать с таблицей emp в пределах своих привилегий.

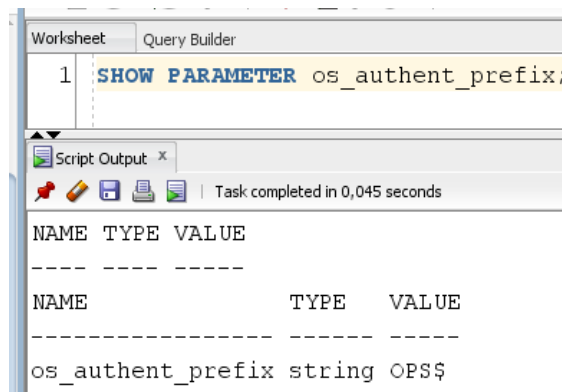


2. Аутентификация средствами ОС.

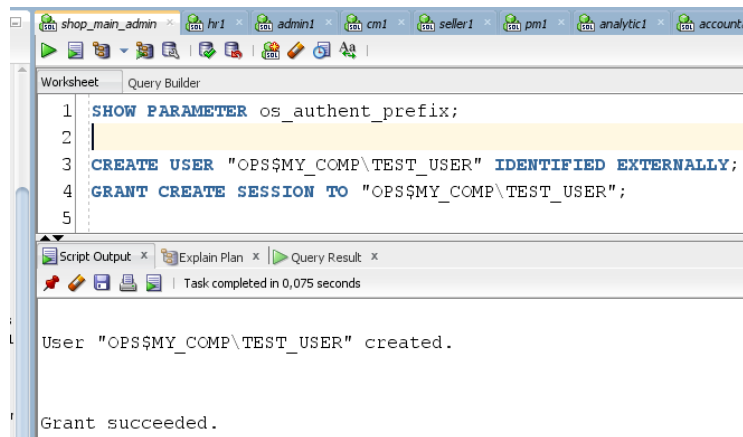
Создан локальный пользователь Windows:



Необходимо узнать префикс аутентификации. Он дефолтный, менять не будем, хотя можно сделать равным нулю, если кому-то не нравится писать лишние буквы.



Создаем пользователя с параметром внешней аутентификации и даем ему возможность подключаться к БД.



Логинимся как TEST_USER, через командную строку можно создать сессию без ввода логина и пароля.

```

C:\> Командная строка - sqlplus /@"localhost:1521/shop_pdb"
Microsoft Windows [Version 10.0.19044.1889]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\TEST_USER>sqlplus /@"localhost:1521/shop_pdb"

SQL*Plus: Release 18.0.0.0.0 - Production on Thu Jan 19 14:13:28 2023
Version 18.4.0.0.0

Copyright (c) 1982, 2018, Oracle. All rights reserved.

Connected to:
Oracle Database 18c Express Edition Release 18.0.0.0.0 - Production
Version 18.4.0.0.0

SQL> show user
USER is 'OPS$DESKTOP-9N078RD\TEST_USER'
SQL>

```

3. Использование представлений.

В лабораторной работе 2-2 представления уже были применены для ограничения доступа пользователей/ролей к данным, не требующимся им для работы.

В задании сказано «ограничить доступ к особо важным данным». Особо важных данных в разрабатываемой таблице на данный момент нет, поэтому приведу часть отчета из лабораторной 2-2.

Имеется роль analytic. Пользователи этой роли занимаются анализом продаж: какие товары/категории лучше продаются, в какое время дня / день недели лучше продажи и тому подобное.

Привилегии для роли analytic:

```

grant create session      to analytic;
grant select on ordersV   to analytic;
grant select on order_detail to analytic;
grant select on good       to analytic;
grant select on saleV      to analytic;
grant select on category   to analytic;

```

SaleV и ordersV – это представления, созданные для ограничение доступа пользователя к полям таблиц, которые им не требуются.

Рассмотрим подробнее: для анализа продаж важно знать только процент предоставленных скидок, а не условия их применения. Из таблицы orders в представление не попал столбец customer_id, потому что на таблицу customer у этой роли нет прав даже чтения, да и ей незачем знать данные покупателя.

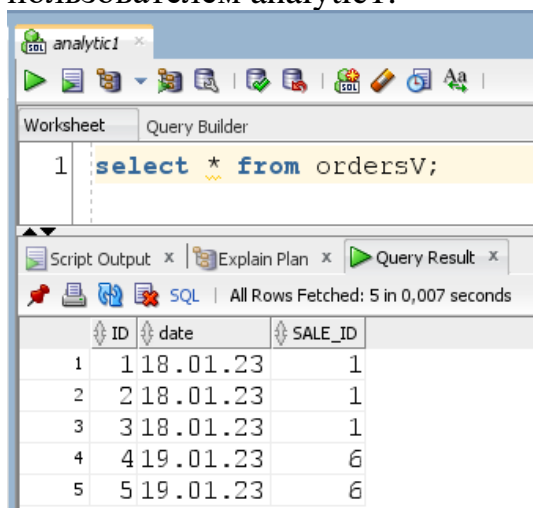
```

-- create views
create view saleV as
  select id, percent
  from sale;

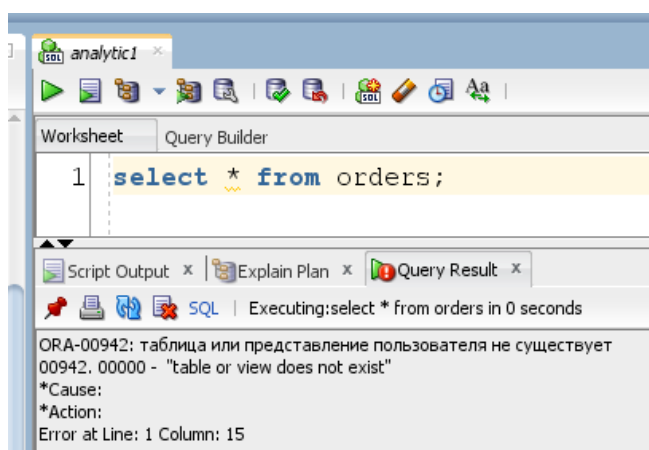
create view ordersV as
  select id, "date", sale_id
  from orders;

```

Попробуем прочесть представление ordersV и всю таблицу orders пользователем analytic1:



ID	date	SALE_ID
1	18.01.23	1
2	18.01.23	1
3	18.01.23	1
4	19.01.23	6
5	19.01.23	6



4. Заключение

В лабораторной работе рассмотрены подходы к аутентификации пользователей (schema-only accounts и внешняя идентификация).

Протестирована работа schema-only пользователя. Сделан вывод, что в разрабатываемой базе данных создание нескольких схем (и schema-only пользователей) нецелесообразно из-за слишком малого количества объектов. Однако при расширении модели БД создание разделяемой среды и дополнительных схем будет необходимо.

Выполнена аутентификация пользователя средствами ОС Windows.

Рассмотрено использование представлений для ограничения доступа пользователей к важным или не нужным для них данным.

Приложение А. Работа со schema-only пользователем.

```
create user hrs NO AUTHENTICATION;
```

```
grant  
  create session,  
  create table,  
  unlimited tablespace  
to hrs;
```

```
create table hrs.emp (  
  id number(3, 0),  
  name varchar2(20) NOT NULL,  
  surname varchar2(20) NOT NULL,  
  phone varchar2(16),  
  job varchar2(20) NOT NULL,  
  salary number(6, 0) NOT NULL,  
  CONSTRAINT customer_pk PRIMARY KEY (id)  
);
```

```
create public synonym emp for hrs.emp;
```

```
create role hr;  
grant create session to hr;  
grant select on emp to hr;  
alter user hrs quota 100M on shop_pdb_users;
```

```
CREATE USER hr1  
  IDENTIFIED BY pas  
  DEFAULT TABLESPACE SHOP_PDB_USERS  
  TEMPORARY TABLESPACE temp  
  QUOTA 500M ON SHOP_PDB_USERS;  
grant hr to hr1;
```

```
insert into emp values (1, 'Ivan', 'Ivanov', '89998887766', 'accountant', 60000);  
insert into emp values (2, 'Petr', 'Petrov', '80001112233', 'manager1', 50000);  
insert into emp values (3, 'Oleg', 'Olegov', '83334445566', 'manager2', 100000);
```