МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

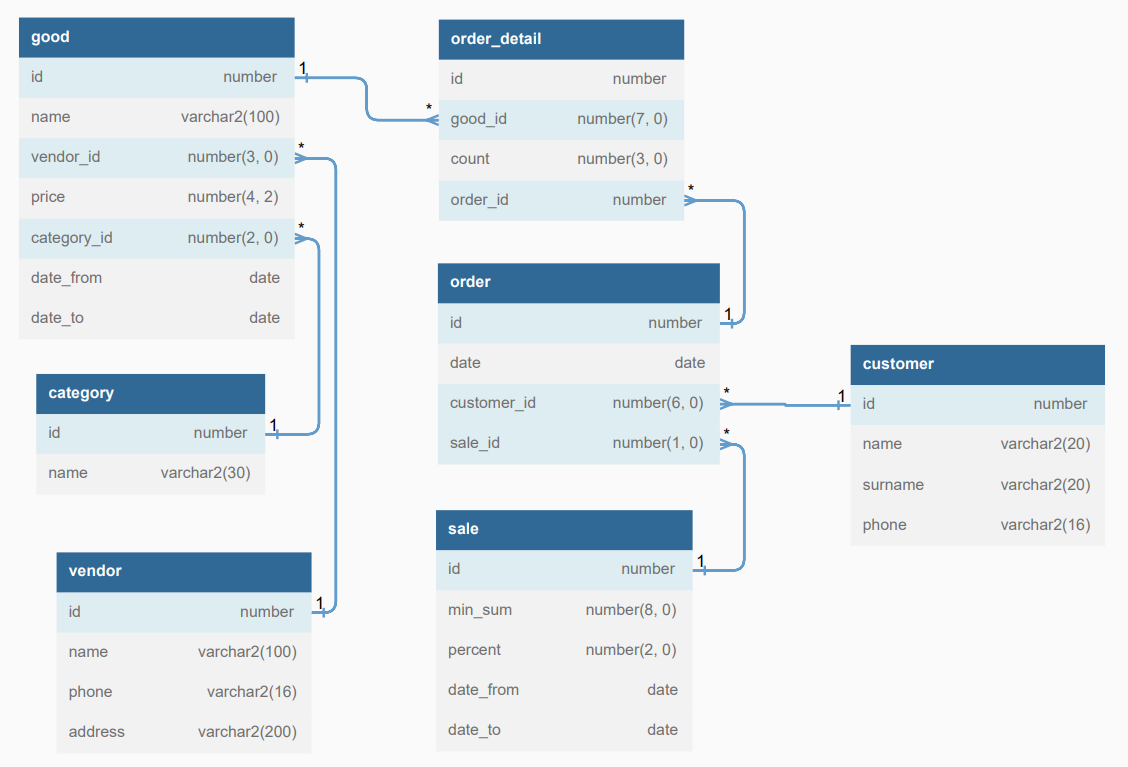
Федеральное государственное автономное образовательное учреждение

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 нескольким 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):

Изображение выглядит как текст

Автоматически созданное описание

Попробуем подключиться к БД в качестве пользователя hrs – невозможно.

Изображение выглядит как текст

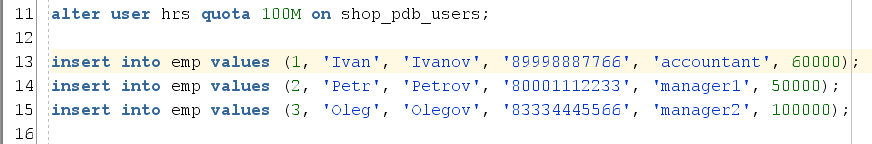
Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

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



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

Изображение выглядит как текст

Автоматически созданное описание

**2. Аутентификация средствами ОС.**

Создан локальный пользователь Windows:

Изображение выглядит как текст

Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

Логинимся как TEST\_USER, через командную строку можно создать сессию без ввода логина и пароля.

Изображение выглядит как текст

Автоматически созданное описание

**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:

Изображение выглядит как текст

Автоматически созданное описание

SaleV и ordrersV – 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.

Изображение выглядит как текст

Автоматически созданное описание

Попробуем прочитать представление ordersV и всю таблицу orders пользователем analytic1:

Изображение выглядит как текст

Автоматически созданное описание Изображение выглядит как текст

Автоматически созданное описание

**4. Заключение**

В лабораторной работе рассмотрены походы 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 данных.

**Приложение A. 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);