МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

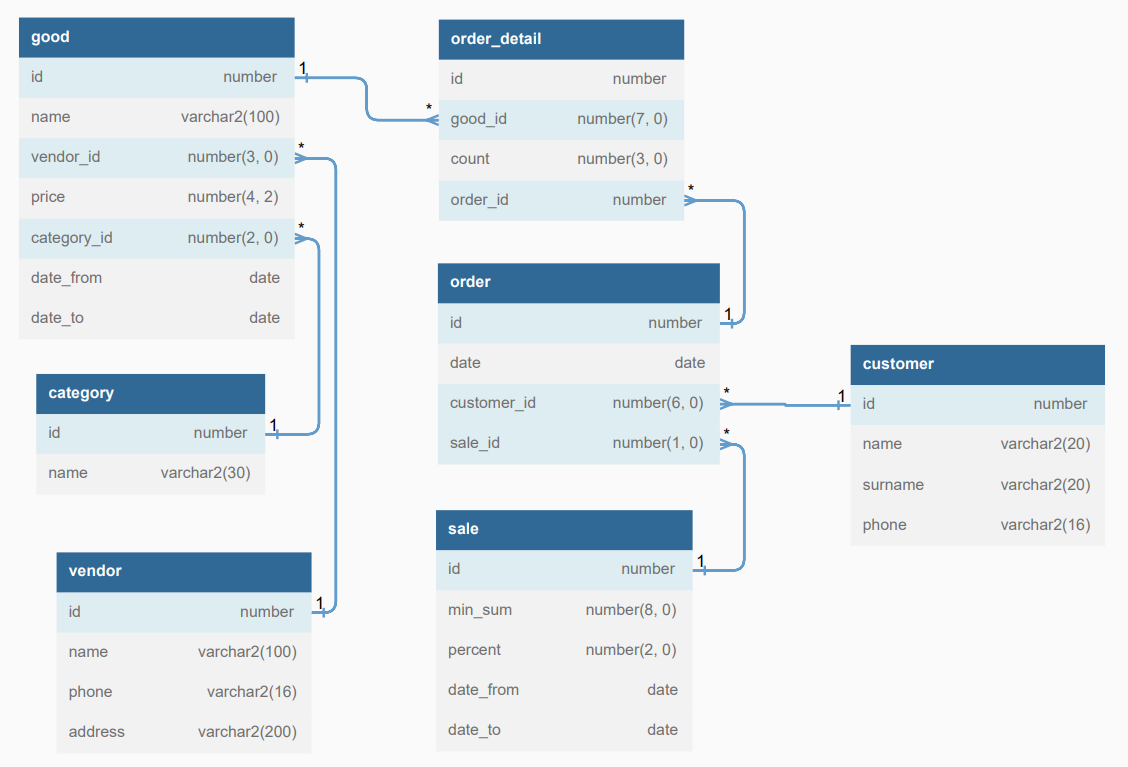
Федеральное государственное автономное образовательное учреждение

высшего образования

«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №2-2:

«Пользователи. Роли. Привилегии. Профили.»



Выполнила студентка группы Б19-515

Щербакова Александра

Москва, 2022 г.

**1. Создание PDB.**

Создана новая PDB shop\_pdb с администратором shop\_main\_admin, которому предоставлены все возможные привилегии внутри shop\_pdb (код см. в Приложении А).

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

**2. Создание схем и таблиц.**

В данной лабораторной вся работа будет производиться в одной схеме, потому что это было бы существенным усложнением для базы данных текущего размера.

------------------------------------------------------------------------------------------------

Лирическое отступление – фантазии об увеличении базы данных.

Тем не менее, если пофантазировать насчет расширения базы данных, то встанет вопрос о разделении схем. Выдавать каждому приложению привилегии на каждую таблицу по отдельности достаточно трудоемко. Поэтому (не в данной лабе, а в теории) в качестве метода создания разделяемой среды базы данных был бы выбран метод «несколько схем». Предположим, что на данный момент в инфраструктуре не предполагается наличие приложений, которые будут пользоваться объектами из одной и той же схемы. Таким образом, при необходимости можно легко переделать базу данных на тип «разделяемая схема».

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

|  |  |  |  |
| --- | --- | --- | --- |
| *Название схемы* | *Таблицы, входящие в схему* | *Назначение* | *Дополнительные таблицы, если предположить, что модель БД будет расширена* |
| prchdpt | vendor | (purchasing\_department)  Отдел закупок. Вся информация о поставщиках и поставках на склад | Количество, наименования товаров в поставках; время поставок |
| cstsvc | customer | (customer\_service)  Отдел по работе с клиентами. Информация о покупателях | Адрес для доставки на дом; выбранные покупателем категории скидки/кешбека |
| warehouse | good, category | Информация о товарах | Наличие товаров на складе |
| orders | Order, order\_detail, sale | Информация о совершенных покупках |  |

Пользователи prchdpt, cstsvc, warehouse, orders обладают всеми привилегиями внутри своей схемы. Это уникальные пользователи, для них роли не будут создаваться. Однако этим пользователям реальный человек не соответствует – ими всеми управляет shop\_main\_admin.

Также для каждой схемы нужно создать роль администратора (обязательно с правом на создание ролей и новых пользователей в этой схеме). И дальше уже можно создавать пользователей, описанных с следующей части лабораторной работы.

------------------------------------------------------------------------------------------------

Лирическое отступление закончено – вернемся к примеру с одной схемой.

1. От имени пользователя shop\_main\_admin созданы все таблицы, согласно erd-диаграмме (приложение B).
2. Созданы и заполнены тестовыми данными все таблицы (код в приложении С).
3. Для некоторых таблиц созданы представления, чтобы ограничить доступ пользователей к полям, которые им не требуются. Для всех таблиц и представлений созданы публичные синонимы для удобства использования (приложение D).

**3. Создание ролей для новых пользователей.**

Разработана ролевая модель в соответствии с задачами пользователей.

Код для создания ролей, а также одного тестового пользователя для каждой роли в приложении E.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Роль | Задачи | Привилегии |
| 1 | admin | Любая администраторская деятельность. Создание новых ролей и пользователей. Любая работа с объектами. | Встроенная в Oracle роль DBA. Все привилегии: SELECT \* FROM ROLE\_SYS\_PRIVS where role = 'DBA'; |
| 2 | accounting | Бухгалтерия. Вычисляет суммарные доходы и расходы (такой таблицы пока нет). Read only. | Select from orders, order\_detail, goodV, saleV |
| 3 | client\_manager | Менеджер по работе с клиентами. Добавляет и изменяет информацию о клиентах. Может вычислить сумму покупок клиента | Select, insert, update on customer  Select on orders, order\_detail, goodV, saleV |
| 4 | seller | Продавец. Добавляет новые заказы. Нужно знать сумму покупок клиента, чтобы применить правильную скидку. | Select, insert, update on order, order\_detail  Select on customer, good, sale |
| 5 | prch\_manager | Менеджер по работе с поставщиками. Добавляет, изменяет информацию о поставщиках. Добавляет новые товары и категории. | Select, insert, update on vendor, category, good |
| 6 | analytic | Анализ продаж: какие товары/категории товаров лучше продаются. В какое время дня больше покупок. Read only. | Select on good, category, order\_detail, ordersV, saleV |

1. Создан один из админов базы данных admin1 (от лица пользователя shop\_main\_admin):

Изображение выглядит как текст

Автоматически созданное описание

Войдем в бд от лица admin1 и посмотрим, какие привилегии ему предоставлены. Роли – только DBA, привилегий всего 235 штук (не поместилось на скрине).

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как стол

Автоматически созданное описание

Протестируем работоспособность привилегий create any table, drop any table:

Изображение выглядит как текст

Автоматически созданное описание

Протестируем работу привилегии grant any role, создав второго админа с аналогичными правами:

Изображение выглядит как текст

Автоматически созданное описание

1. От лица admin1 создадим роль для бухгалтера, а также одного пользователя с этой ролью.

Изображение выглядит как текст

Автоматически созданное описание

// далее скриншоты создания пользователей приводиться не будут, чтобы не перегружать отчет. Код для создания всех ролей и пользователей в приложении E.

Подключимся к базе как бухгалтер. Можно посмотреть все таблицы, к которым есть доступ. SaleV здесь не отображается, так как это представление, а не таблица.

Изображение выглядит как текст

Автоматически созданное описание

Протестируем работу бухгалтера. Стандартный запрос для этой роли – вычислить сумму продаж (за определенное время, например, январь).

Изображение выглядит как текст

Автоматически созданное описание

1. Роль client\_manager и пользователь cm1

Стандартный запрос – добавить пользователя.

Изображение выглядит как текст

Автоматически созданное описание

Еще запрос: вычислить сумму покупок клиента.

Изображение выглядит как текст

Автоматически созданное описание

1. Роль seller и пользователь seller1.

Добавить новый заказ. Для этого сначала вычисляется сумма предыдущих покупок клиента, выбирается соответствующая скидка, и только потом добавляется заказ.

Изображение выглядит как текст

Автоматически созданное описание Изображение выглядит как текст

Автоматически созданное описание

Теперь добавляются детали (сколько и каких товаров куплено) в order\_details.

Изображение выглядит как стол

Автоматически созданное описание

1. Роль prch\_manager и пользователь pm1.

Изменить информацию о поставщике.

Изображение выглядит как текст

Автоматически созданное описание

Добавить новый товар из существующей категории.

Изображение выглядит как стол

Автоматически созданное описание

1. Роль analytic и пользователь analytic1.

Вычислить сумму проданных товаров из всех категорий.

Изображение выглядит как текст

Автоматически созданное описание

**4. Заключение**

В данной работе реализована сегментация работы пользователей с базой данных магазина. Созданы базовые роли для работы с данными, созданы пользователи для каждой роли, для них протестирована работа привилегий.

Если БД содержит на порядки больше таблиц, выдавать объектные привилегии, как сделано в данной лабораторной, слишком трудозатратно. Поэтому в теории следовало бы расширить БД и, продумав, какие приложения будут использовать какие таблицы, разбить БД на схемы.

Также можно было бы сделать представления из соединения нескольких таблиц, так как соединение, например, order-order\_detail-good используется для похожих целей пользователями различных ролей.

**Приложение A. Создание базы данных.**

/ as sysdba

create pluggable database SHOP\_PDB admin user shop\_main\_admin identified by pas

default tablespace SHOP\_PDB\_USERS

datafile 'C:\APP\ALEXM\PRODUCT\18.0.0\ORADATA\XE\SHOP\_PDB\SHOP\_PDB\_USERS01.dbf' size 250m autoextend on

file\_name\_convert=('C:\APP\ALEXM\PRODUCT\18.0.0\ORADATA\XE\pdbseed','C:\APP\ALEXM\PRODUCT\18.0.0\ORADATA\XE\SHOP\_PDB');

show pdbs;

alter pluggable database SHOP\_PDB open;

show pdbs;

ALTER SESSION SET CONTAINER=shop\_pdb;

GRANT

all privileges

to shop\_main\_admin

CONTAINER=CURRENT;

**Приложение B. Создание таблиц.**

-- shop\_main\_amdin/pas@"localhost:1521/shop\_pdb"

CREATE TABLE sale (

id number(3, 0),

min\_sum number(8, 0) NOT NULL,

percent number(3, 1) NOT NULL,

date\_from date NOT NULL,

date\_to date NOT NULL,

CONSTRAINT sale\_pk PRIMARY KEY (id)

);

CREATE TABLE vendor (

id number(4, 0),

name varchar2(100) NOT NULL,

phone varchar2(16) NOT NULL,

address varchar2(200),

CONSTRAINT vendor\_pk PRIMARY KEY (id)

);

CREATE TABLE category (

id number(3, 0),

name varchar2(30) NOT NULL,

CONSTRAINT category\_pk PRIMARY KEY (id)

);

CREATE TABLE customer (

id number(6, 0),

name varchar2(20) NOT NULL,

surname varchar2(20) NOT NULL,

phone varchar2(16),

CONSTRAINT customer\_pk PRIMARY KEY (id)

);

CREATE TABLE good (

id number(9, 0),

name varchar2(100) NOT NULL,

vendor\_id number(4, 0) NOT NULL,

price number(6, 2) NOT NULL,

category\_id number(3, 0) NOT NULL,

date\_from date NOT NULL,

date\_to date NOT NULL,

CONSTRAINT good\_pk PRIMARY KEY (id),

CONSTRAINT good\_fk\_category

FOREIGN KEY (category\_id)

REFERENCES category (id),

CONSTRAINT good\_fk\_vendor

FOREIGN KEY (vendor\_id)

REFERENCES vendor (id)

);

CREATE TABLE orders (

id number(7, 0),

"date" date NOT NULL,

customer\_id number(6, 0) NOT NULL,

sale\_id number(3, 0),

CONSTRAINT orders\_pk PRIMARY KEY (id),

CONSTRAINT orders\_fk\_cistomer

FOREIGN KEY (customer\_id)

REFERENCES customer (id),

CONSTRAINT orders\_fk\_sale

FOREIGN KEY (sale\_id)

REFERENCES sale (id)

);

CREATE TABLE order\_detail (

id number(8, 0),

good\_id number(9, 0) NOT NULL,

count number(3, 0) NOT NULL,

order\_id number(7, 0) NOT NULL,

CONSTRAINT order\_detail\_pk PRIMARY KEY (id),

CONSTRAINT order\_detail\_fk\_good

FOREIGN KEY (good\_id)

REFERENCES good (id),

CONSTRAINT order\_detail\_fk\_order

FOREIGN KEY (order\_id)

REFERENCES orders (id)

);

**Приложение C. Заполнение таблиц.**

-- category

insert into category values (1, 'fruit');

insert into category values (2, 'vegetables');

insert into category values (3, 'chocolate');

insert into category values (4, 'water');

-- vendor

insert into vendor values (1, 'fruit vendor', '81234567788', 'Moscow');

insert into vendor values (2, 'fruit and vegetables vendor', '81234568899', 'Krasnodar');

insert into vendor values (3, 'chocolate vendor 1', '81112223344', 'Podolsk');

insert into vendor values (4, 'chocolate vendor 2', '83334445566', 'Minsk');

insert into vendor values (5, 'water vendor 1', '89998887766', 'Yaroslavl');

-- customer

insert into customer values (1, 'Ivan', 'Ivanov', '91115556677');

insert into customer values (2, 'Petr', 'Petrov', '91115556688');

insert into customer values (3, 'Kirill', 'Kirilenko', '91115556699');

insert into customer values (4, 'Anton', 'Antonov', '91115556600');

insert into customer values (5, 'Olga', 'Olegova', '91115556666');

insert into customer values (6, 'Yan', 'Portnov', '91115556655');

declare

c\_date\_to date := to\_date('01-01-2023', 'dd-mm-yyyy');

c\_date\_from date := to\_date('01-01-2022', 'dd-mm-yyyy');

begin

-- good

insert into good values (1, 'apple', 1, 30, 1, c\_date\_from, c\_date\_to);

insert into good values (2, 'banana', 1, 20, 1, c\_date\_from, c\_date\_to);

insert into good values (3, 'cucumber', 2, 25, 2, c\_date\_from, c\_date\_to);

insert into good values (4, 'alionka', 3, 70, 3, c\_date\_from, c\_date\_to);

insert into good values (5, 'alpen gold', 4, 70, 3, c\_date\_from, c\_date\_to);

insert into good values (6, 'sviatoy istochnik', 5, 50, 4, c\_date\_from, c\_date\_to);

-- sale

insert into sale values (1, 0, 0.5, c\_date\_from, c\_date\_to);

insert into sale values (2, 30000, 1, c\_date\_from, c\_date\_to);

insert into sale values (3, 50000, 2, c\_date\_from, c\_date\_to);

insert into sale values (4, 100000, 5, c\_date\_from, c\_date\_to);

insert into sale values (5, 2000000, 7, c\_date\_from, c\_date\_to);

end;

-- orders

insert into orders values (1, SYSDATE, 1, 1);

insert into orders values (2, SYSDATE, 2, 1);

insert into orders values (3, SYSDATE, 2, 1);

-- order\_detail

insert into order\_detail values (1, 1, 5, 1);

insert into order\_detail values (2, 2, 10, 1);

insert into order\_detail values (3, 3, 2, 1);

insert into order\_detail values (4, 4, 7, 2);

insert into order\_detail values (5, 5, 1, 2);

insert into order\_detail values (6, 6, 2, 2);

insert into order\_detail values (7, 1, 3, 2);

insert into order\_detail values (8, 1, 20, 3);

**Приложение D. Создание представлений и публичных синонимов.**

-- create views

create view saleV as

select id, percent

from sale;

create view ordersV as

select id, "date", sale\_id

from orders;

create view goodV as

select id, name, price

from good;

-- create public synonyms for all tables

create public synonym vendor

for shop\_main\_admin.vendor;

create public synonym customer

for shop\_main\_admin.customer;

create public synonym good

for shop\_main\_admin.good;

create public synonym category

for shop\_main\_admin.category;

create public synonym orders

for shop\_main\_admin.orders;

create public synonym order\_detail

for shop\_main\_admin.order\_detail;

create public synonym sale

for shop\_main\_admin.sale;

-- create public synonyms for all views

create public synonym saleV

for shop\_main\_admin.saleV;

create public synonym ordersV

for shop\_main\_admin.ordersV;

create public synonym goodV

for shop\_main\_admin.goodV;

**Приложение E. Создание ролей и пользователей.**

-- create roles

create role accounting;

grant create session to accounting;

grant select on orders to accounting;

grant select on order\_detail to accounting;

grant select on good to accounting;

grant select on saleV to accounting;

create role client\_manager;

grant create session to client\_manager;

grant

select,

insert,

update on customer to client\_manager;

grant select on orders to client\_manager;

grant select on order\_detail to client\_manager;

grant select on goodV to client\_manager;

grant select on saleV to client\_manager;

create role seller;

grant create session to seller;

grant

select,

insert,

update on orders to seller;

grant

select,

insert,

update on order\_detail to seller;

grant select on customer to seller;

grant select on good to seller;

grant select on sale to seller;

create role prch\_manager;

grant create session to prch\_manager;

grant

select,

insert,

update on vendor to prch\_manager;

grant

select,

insert,

update on category to prch\_manager;

grant

select,

insert,

update on good to prch\_manager;

create role 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;

-- create users

CREATE USER accountant1

IDENTIFIED BY pas

DEFAULT TABLESPACE SHOP\_PDB\_USERS

TEMPORARY TABLESPACE temp

QUOTA 500M ON SHOP\_PDB\_USERS;

grant accounting to accountant1;

CREATE USER cm1

IDENTIFIED BY pas

DEFAULT TABLESPACE SHOP\_PDB\_USERS

TEMPORARY TABLESPACE temp

QUOTA 500M ON SHOP\_PDB\_USERS;

grant client\_manager to cm1;

CREATE USER seller1

IDENTIFIED BY pas

DEFAULT TABLESPACE SHOP\_PDB\_USERS

TEMPORARY TABLESPACE temp

QUOTA 500M ON SHOP\_PDB\_USERS;

grant seller to seller1;

CREATE USER pm1

IDENTIFIED BY pas

DEFAULT TABLESPACE SHOP\_PDB\_USERS

TEMPORARY TABLESPACE temp

QUOTA 500M ON SHOP\_PDB\_USERS;

grant prch\_manager to pm1;

CREATE USER analytic1

IDENTIFIED BY pas

DEFAULT TABLESPACE SHOP\_PDB\_USERS

TEMPORARY TABLESPACE temp

QUOTA 500M ON SHOP\_PDB\_USERS;

grant analytic to analytic1;