Лабораторная работа №10
Реализация доступа пользователей к базе данных

1Цель работы

1.1 Научиться использовать системные хранимые процедуры и DDL-команды для управления именами входа и пользователями БД в СУБД;

1.2 Научиться назначать привилегии пользователю БД;

1.3 Закрепить навык создания объектов БД.

2Литература

2.1 Култыгин, О.П. Администрирование баз данных. СУБД MS SQL Server: учеб. пособие. – Москва: МФПА, 2012. – с.188-202.

3Подготовка к работе

3.1 Повторить теоретический материал (см. п.2).

3.2 Изучить описание практической работы.

4Основное оборудование

4.1 Персональный компьютер.

5Задание

Все скрипты сохранить в одном файле. Все задания кроме 1.2 выполнять на prserver.

Задание 1.2 выполняется в СУБД, созданной на ЛР №4 (если не создана – подключиться к СУБД одногруппников, создавших её на ЛР №4).

5.1 Создание имен входа и пользователей

5.1.1 Через контекстное меню создать скрипт для своего имени входа, используя CREATE. Объяснить сгенерированную команду (добавить комментарии).

5.1.2 Написать и выполнить следующие команды (в СУБД с ЛР №4)

- команду для создания нового имени входа isppLoginNN1 (вместо NN свой номер) для входа в MS SQL Server. Пароль: Password! Пароль не должен проверяться, политику смены пароля отключить (для этого в команде создания логина указать CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF).
- команду, использующую хранимую процедуру для создания нового имени входа isppLoginNN2 (вместо NN свой номер) для входа в MS SQL Server. Пароль: Password!
- команду, использующую хранимую процедуру для назначения имени входа роли для управления пользователями сервера.

5.1.3 Создать в БД новых пользователей:

- user1 и user2, используя системную хранимую процедуру sp_adduser,
- user3 и user4, используя команду CREATE USER.

В задании использовать для создания пользователей существующие имена входа login1, login2, login3, login4 соответственно. Пароль у логинов – 1.

5.2 Назначение и отзыв привилегий пользователей

5.2.1 Назначить пользователям следующие привилегии уровня БД:

- user1 – все привилегии, используя sp_addrolemember,

- user2 – чтение и запись данных, используя sp_addrolemember,
- user3 – права на удаление и вставку данных в таблицу Билеты, используя GRANT,
- user4 – права на чтение данных в таблице Посетители и обновление данных в столбцах имя и email, используя GRANT.

Проверить настройки прав доступа, выполнив в БД различные действия от имени созданных пользователей.

5.2.2 Отозвать привилегии у следующих пользователей:
- user2 – право на запись данных, используя sp_droprolemember,
- user2 – право на чтение данных из таблицы Посетители, используя DENY,
- user4 – право на обновление данных в столбце имя, используя DENY.

Проверить настройки прав доступа, выполнив в БД различные действия от имени созданных пользователей.

5.2.3 Изучить отображение привилегий пользователей в оконном интерфейсе назначения прав доступа SSMS.

5.3 Одновременное назначение прав доступа множеству пользователей

Выдать право на чтение данных таблиц БД для пользователей reader1, reader2, reader3, reader4 с существующими логинами reader1, reader2, reader3, reader4 соответственно, используя цикл, написанный на SQL. Пароль у логинов – 1.

5.4 Создание таблиц пользователей для использования в приложении

5.4.1 Создать и заполнить набор таблиц для хранения данных пользователей и их ролей.

В таблицах должны быть следующие данные: логин и пароль пользователя, название роли. У созданных таблиц название должно начинаться с префикса Task1 (например: Task1Users и Task1Roles). В таблицах должно быть 3 роли и 5 пользователей.

5.4.2 Создание таблиц пользователей для использования в приложении

Создать и заполнить набор таблиц для хранения данных пользователей. Требуется хранить логин и пароль пользователя. Для каждой роли должны указываться свои дополнительные данные:
- роль администратор: без дополнительных атрибутов,
- роль менеджер: email,
- роль клиент: телефон, баланс на карте и заблокирован ли пользователь.

У созданных таблиц название должно начинаться с префикса Task2 (например: Task2Users). Пользователей должно быть по 2 для каждой роли.

5.5 Шифрование данных

5.5.1 Добавить в одну из таблиц пользователей из п.5.4 необязательный столбец EncryptedPassword для хранения хэша пароля. Тип данных: BINARY(32).

Создать скрипт для заполнения столбца EncryptedPassword хэшем пароля, используя HASHBYTES, алгоритм: SHA256.

5.5.3 Создать скрипт проверяющий, что есть пользователем с указанным логином и паролем (для проверки сравнивать хэшированный введенный пароль с хэшами паролей в таблице.

5.5.4 Создать триггер для того, чтобы в таблице пользователей при вставке и изменении пароля менялся его хэш.

6 Порядок выполнения работы

6.1 Запустить SSMS

6.2 Выполнить задания из п.5.1-5.2.

6.3 Выполнить задание п.5.2.3, используя графический интерфейс SSMS.

6.3.1 Подключиться под пользователем-владельцем БД и сделать ее текущей БД;

6.3.2 Открыть вкладку Безопасность — Пользователи. Выбрать из контекстого меню «Создать пользователя».

6.3.3 Указать во вкладке «Общие» требуемое имя пользователя и имя входа. Назначить схему по умолчанию dbo.

6.3.4 Во вкладке «Защищаемые объекты» нажать кнопку «Добавить» и выдать и забрать разрешения на объекты типа таблиц. Для разных таблиц выдать разрешения на выполнение DML команд на уровне таблиц и столбцов.

6.4 Выполнить задания из п.5.3-5.5.

6.5 Ответить на контрольные вопросы.

7Содержание отчета

7.1 Титульный лист

7.2 Цель работы

7.3 Ответы на контрольные вопросы

7.4 Вывод

8Контрольные вопросы

8.1 В чем отличие между именами входа и пользователями БД?

8.2 Как идентифицируются пользователи в MS SQL Server?

8.3 На какие уровни разделяется система безопасности MS SQL Server?

8.4 Каково назначение ролей сервера?

8.5 Каково назначение ролей БД?