Практическая работа №4
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.

5.1 Создание имен входа и пользователей

5.1.1 Создать в БД новых пользователей:

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

CREATE USER пользовательБД FOR LOGIN имяВхода.

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

5.1.2 Через контекстное меню «Безопасность – Имена для входа» создать скрипт для своего имени входа, используя CREATE.

Добавить в сгенерированную команду комментарии:

- почему пароль выводится не в исходном виде,
- для чего настройка CHECK_EXPIRATION=OFF,
- для чего настройка CHECK_POLICY=OFF.

5.1.3 Написать вызов хранимых процедур (работу не проверять, нет прав доступа):

- sp_addlogin для создания нового имени входа isppLoginNN2 (вместо NN свой номер). Пароль: Password!
- sp_addsrvrolemember для назначения созданному имени входа роли securityadmin (управление пользователями сервера).

5.2 Назначение и отзыв привилегий пользователей с использованием процедур

5.2.1 Назначить пользователям следующие привилегии уровня БД:

- user1 – все привилегии (db_owner), используя sp_addrolemember,
- user2 – чтение и запись данных (db_datareader, db_datawriter), используя sp_addrolemember.

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.

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 Назначение и отзыв привилегий пользователей с использованием команд

5.3.1 Назначить пользователям следующие привилегии уровня БД:

- 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.

5.3.2 Отозвать привилегии у следующих пользователей:

- 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.

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

5.4 Одновременное назначение прав доступа множеству пользователей

EXEC('строка с SQL-командой') – позволяет выполнить команду SQL. Если в команде используется меняющийся текст, вместо него использовать переменные.

Пример команды:

'CREATE USER [' + @имяВхода + '] FOR LOGIN [' + @имяВхода + '] WITH DEFAULT_SCHEMA=[БД] '

5.4.1 Используя цикл, написанный на SQL, создать пользователей БД на основе существующих логинов reader1, reader2, reader3, reader4 (пароль у логинов – 1).

5.4.2 Добавить право на чтение данных таблиц БД для созданных пользователей.

5.5 Шифрование данных на стороне БД

5.5.1 Добавить в БД таблицу PW4Users (id, логин, пароль) и добавить в нее необязательный столбец EncryptedPassword для хранения хэша пароля. Тип данных: BINARY(32).

5.5.2 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.

6Порядок выполнения работы

6.1 Запустить SSMS

6.2 Выполнить задания из п.5.1-5.3.

6.3 Выполнить задание п.5.2.3 и 5.3.3, 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.5.4-5.5.

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?