МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Казанский национальный исследовательский технический университет

им. А. Н. Туполева – КАИ»

Институт компьютерных технологий и защиты информации

Отделение СПО ИКТЗИ (Колледж информационных технологий)

ЛАБОРАТОРНАЯ РАБОТА №3

по дисциплине

“Информационная безопасность”

Тема: “Реализация доступа пользователей к базе данных”

Работу выполнил

Студент гр.4238

Константинович А.А.

Преподаватель

Кожевников К. Д.

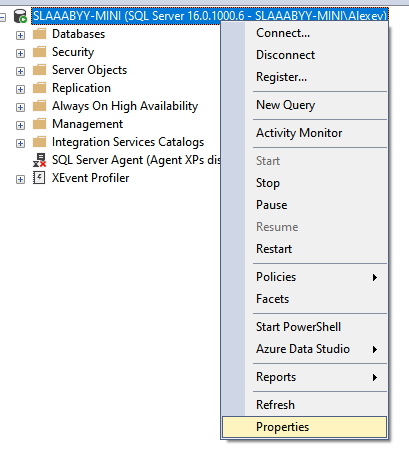
Казань 2024

**Цель работы**

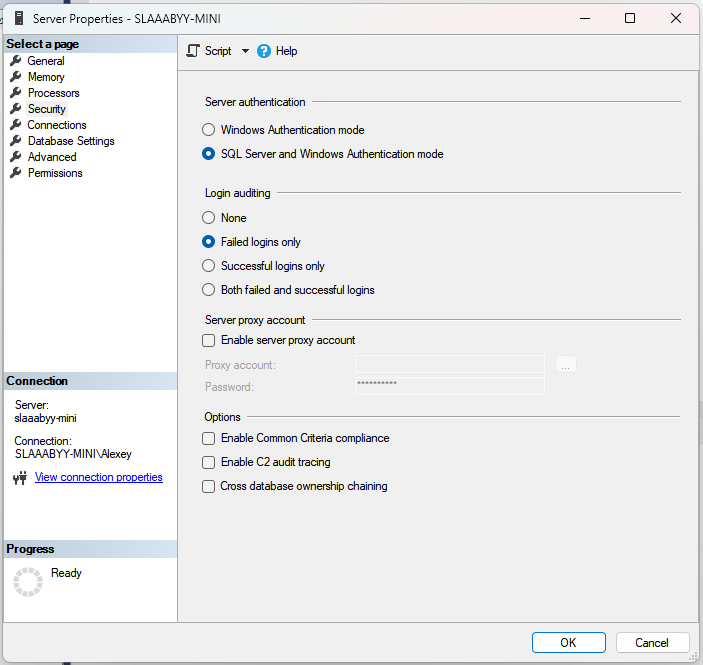
Научиться выполнять реализацию доступа пользователей к базе данных.

**Ход работы**

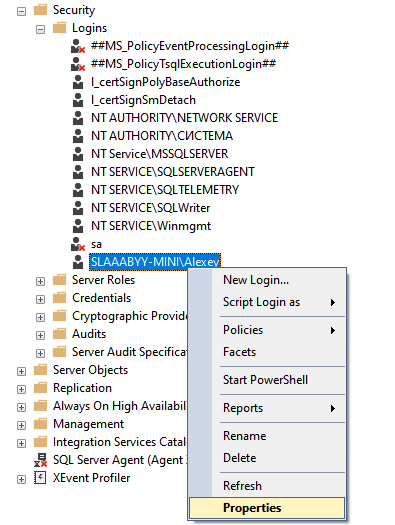
1. Заходим в свойства

  
Рисунок 1 –Свойства

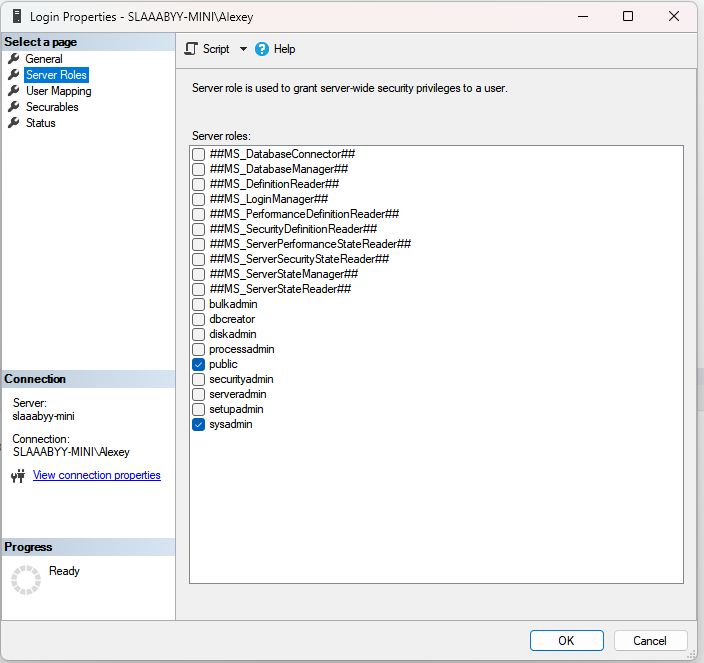
2. В графе “Серверная проверка подлинности” нужно изменить на проверки подлинности SQL Server и Windows

  
Рисунок 2 – Проверка подлинности

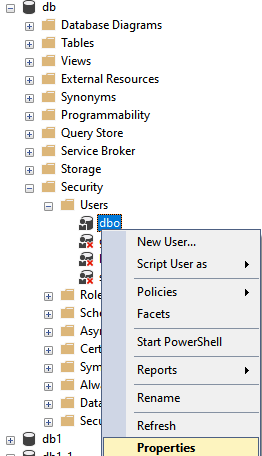
3. Нажимаем ПКМ на свою учетную запись и выбираем опцию “Свойства”

  
Рисунок 3 – Свойства учетной записи

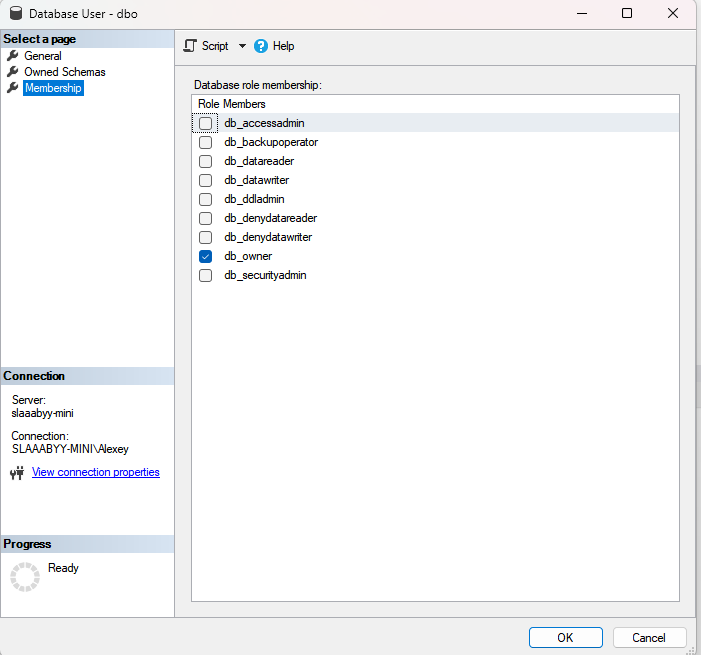
4. Во вкладе “Роли сервера” можно увидеть, на выполнение каких серверных ролей авторизована учетная запись

  
Рисунок 4 - Проверка роли сервера.

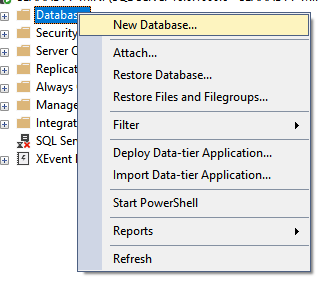
5. В папке “Security” в интересующей базе данных разворачиваем папку “Users”. Нажимаем ПКМ на пользователе и выбираем опцию “Свойства”

  
Рисунок 5 – Свойства пользователя.

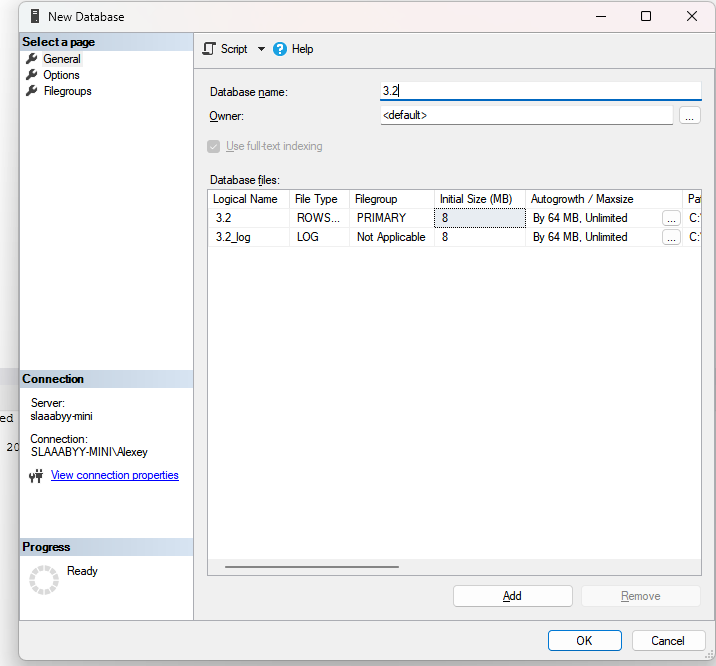
6. Во вкладке “Членство” можно ознакомиться с информацией о ролях, к которым пользователь авторизован в базе данных

  
Рисунок 6 – Членство.

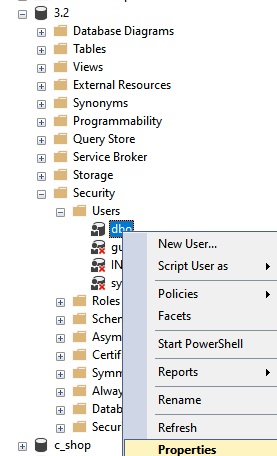
7. Создаем новую базу данных

  
Рисунок 7 – Создание БД.

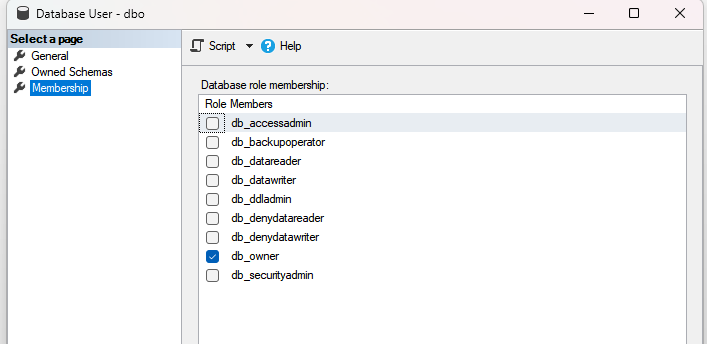
8. В появившемся окне вводим имя для новой базы данных

  
Рисунок 8 – Имя БД.

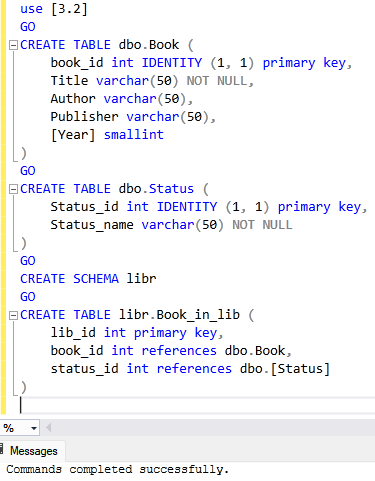
­­9. Нажимаем ПКМ на пользователе “dbo” и выбираем “Свойства”

  
Рисунок 9 –Свойства

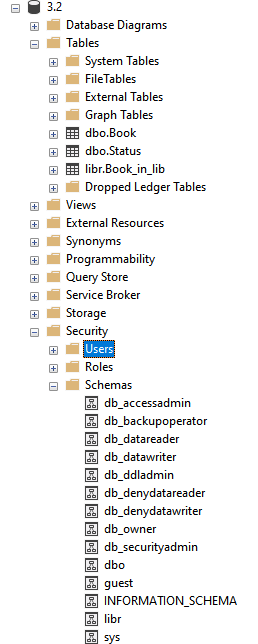
10. Открываем вкладку “Членство” и убеждаемся, что роль “db\_owner” присутствует в списке ролей, к которым пользователь авторизован.

  
Рисунок 10 – Членство.

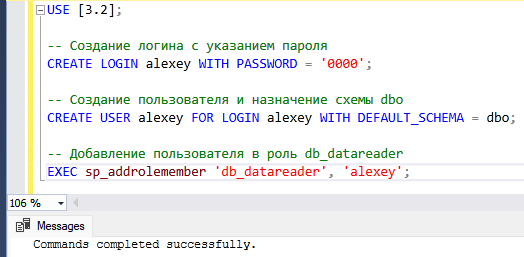
­­11. Создаем таблицы в базе данных

  
Рисунок 11 – Создание таблиц.

12. Проверяем, что таблицы созданы в нашей БД. Также можно посмотреть структуру созданных таблиц и связи между ними.

  
Рисунок 12 – Проверка.

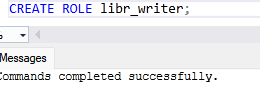
­­13. Создание пользователя, выбор схемы dbo, добавление в роль db\_datareader:

  
Рисунок 13 – Скрипт.

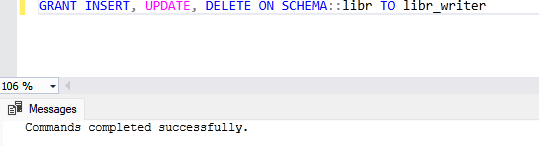
14. После подключения к серверу с учетной записью другого пользователя нужно убедиться, что новый пользователь имеет доступ только на чтение данных из всех таблиц базы данных.

  
Рисунок 14 – Проверка со стороны пользователя

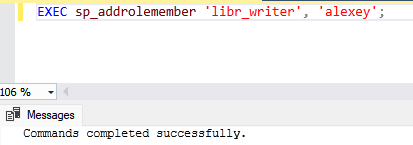
­­15. Создаем новую роль уровня базы данных

  
Рисунок 15 – Новая роль.

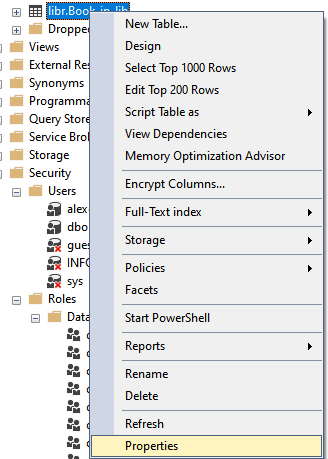
16. Предоставляем разрешения роля “libr\_writer” на выполнение операций INSERT, UPDATE, DELETE для объектов в схеме “libr”

  
Рисунок 16 – Разрешения роли.

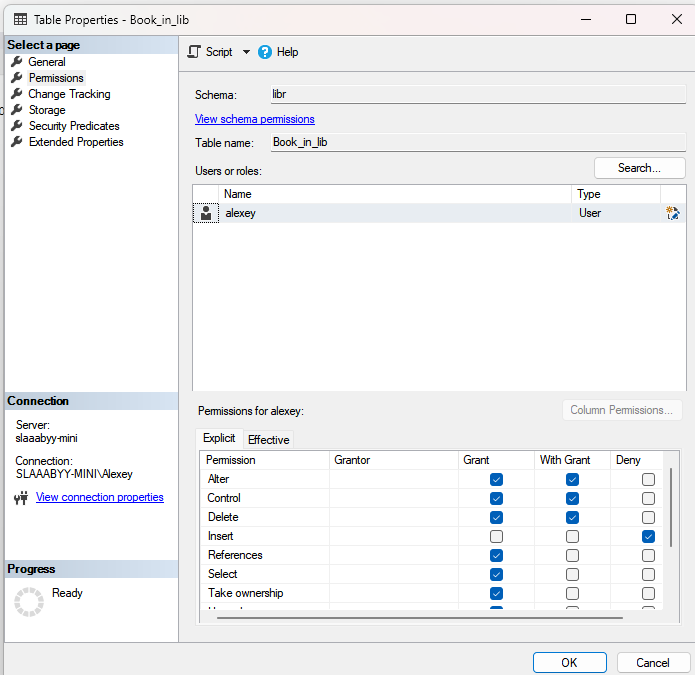
­­17. Добавляем пользователя “alexey” в роль “libr\_writer”

  
Рисунок 17 – Назначение роли

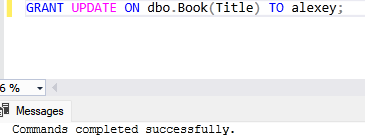
8. Заходим в свойства таблицы “Book\_in\_lib”, принадлежащей схеме “libr”:

  
Рисунок 18 – Свойства.

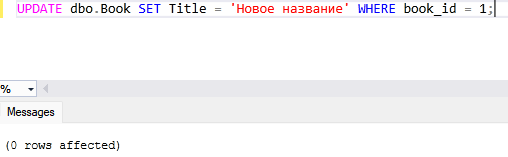
­­19. Назначаем разрешения для пользователя “alexey”

  
Рисунок 19 – Настройка разрешений.

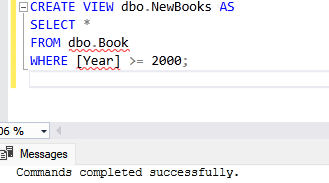
20. Предоставляем пользователю право на обновление столбца “Title” в таблице “Book”:

  
Рисунок 20 – Предоставление право

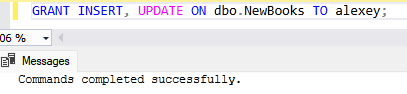
­­21. Обновляем значение в столбце “Title” таблицы “Book”

  
Рисунок 21 – Обновление столбца

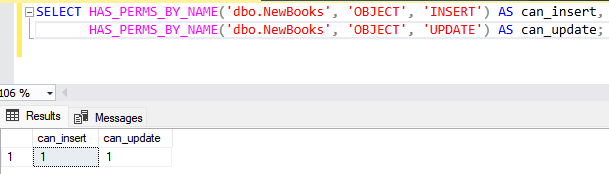
­­22. Выполняем оператор “CREATE VIEW” для создания представления. Выбираем из таблицы “Book” только те книги, которые были изданы не ранее 2000 года:

  
Рисунок 22 – Создание представления

­­23. Предоставляем пользователю права на изменение и добавление записей в представление “NewBooks”, но только для книг, изданных не ранее 2000 года:

  
Рисунок 23 – Права на изменение записей

­­24. Проверяем, что пользователь имеет права на изменение и добавление записей в представление “NewBooks”:

  
Рисунок 24 – Проверка прав пользователя.

**Вывод**

Я научился реализовывать доступ пользователей к базе данных. Все прошло успешно и без ошибок.