Державний торговельно-економічний університет  
Кафедра інженерії програмного забезпечення та кібербезпеки

**ЛАБОРАТОРНА РОБОТА №6**

**З ДИСЦИПЛІНИ «БАЗИ ДАНИХ»**

**НА ТЕМУ: «УПРАВЛІННЯ ДОСТУПОМ ДО СИСТЕМ БД»**

**Виконала**: студентка факультету

інформаційних технологій

групи\_курсу 3-4

Авєріна Наталія Ігорівна

**Перевірила**: Рзаєва Світлана Леонідівна

Київ 2024

**Лабораторна робота №6**

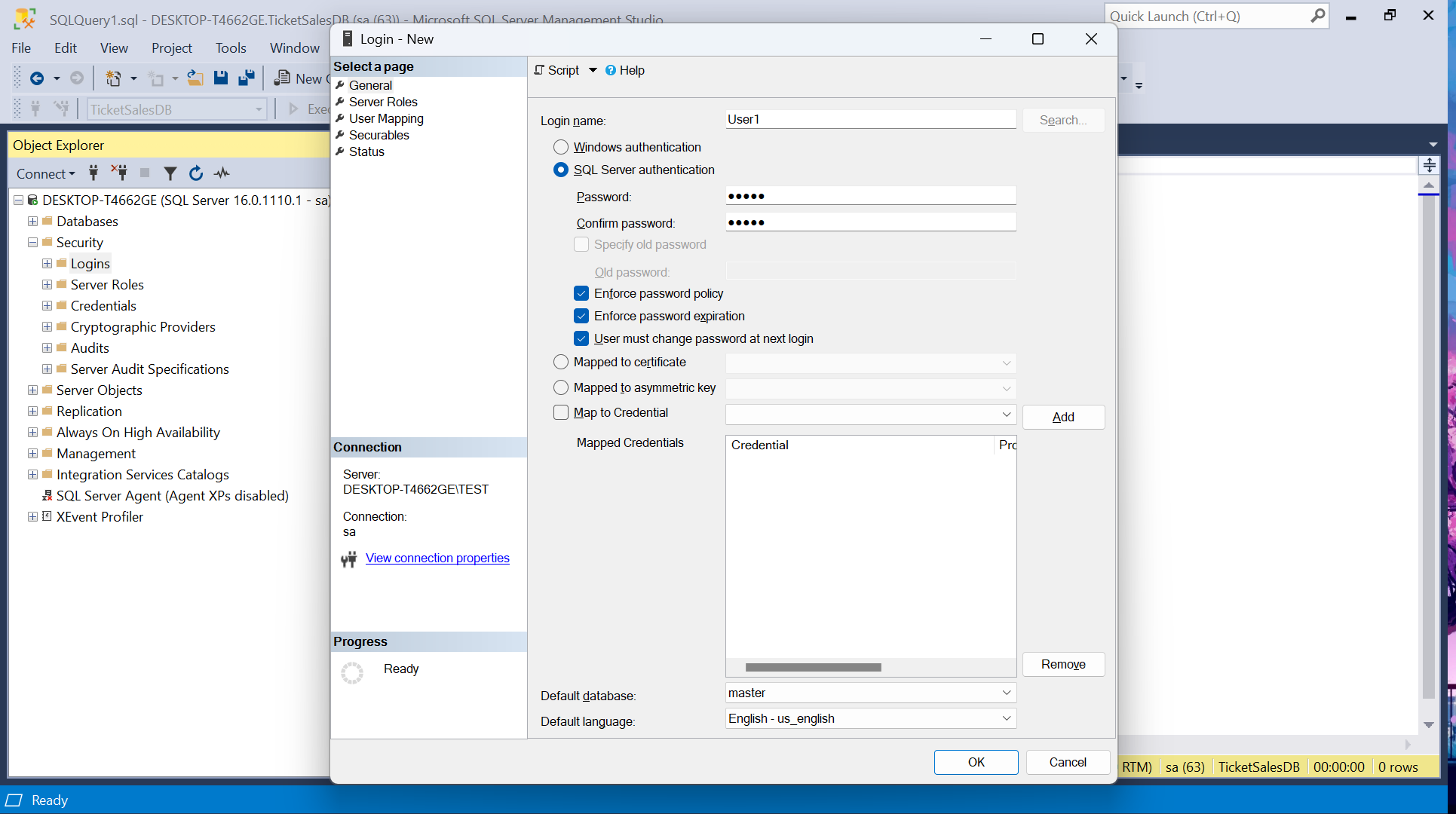
**Тема: «Управління доступом до систем БД»**

**Мета:** набути практичних навичок щодо встановлення режимів аутентифікації користувачів і об'єктів баз даних, особливостей авторизації користувачів, надання їм привілеїв.

**Хід роботи:**

1. Створення імені входу з використанням SSMS.

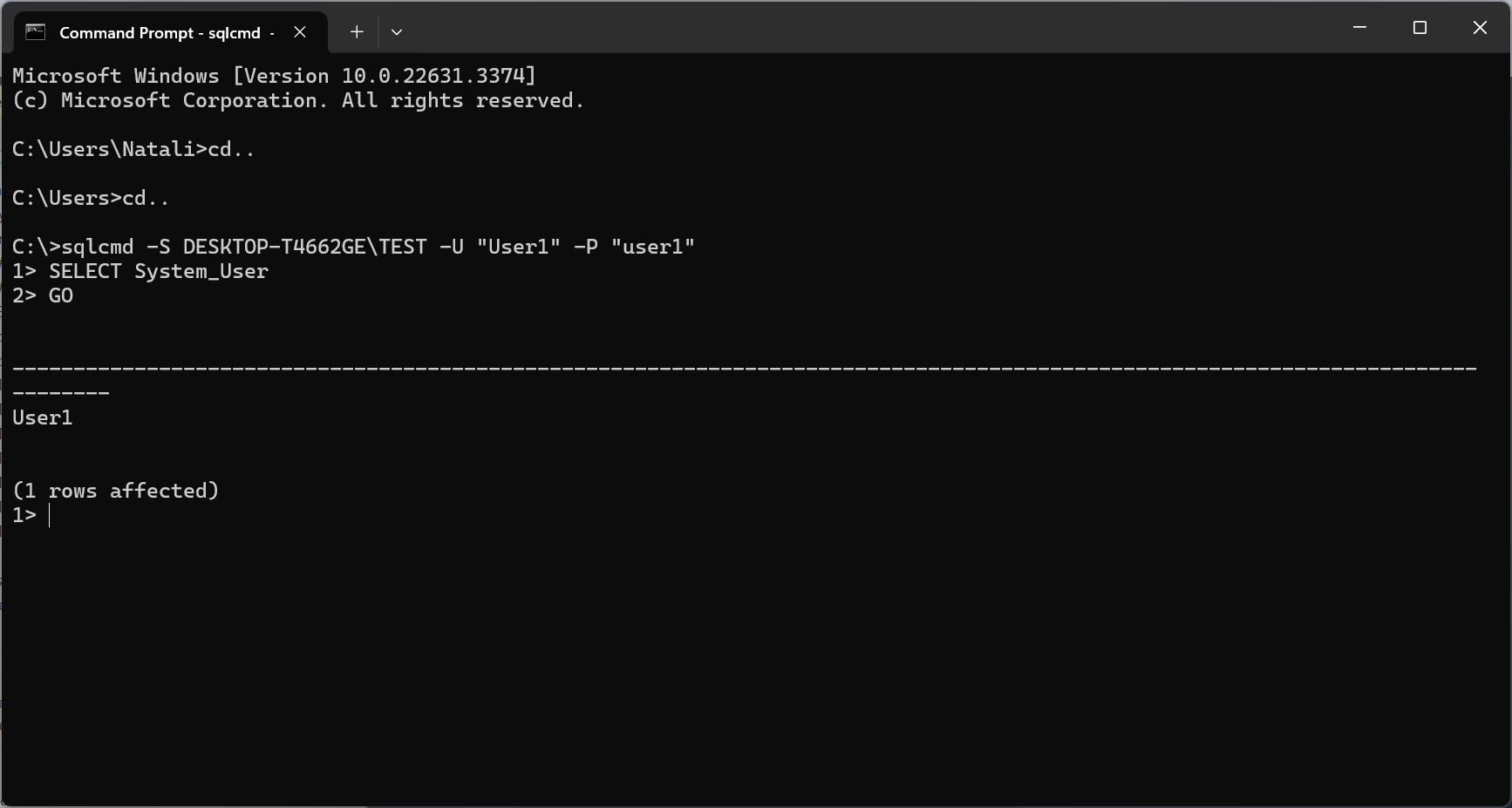
Створюємо нового користувача. В браузері об’єктів розкриваємо папку примірника сервера, далі обираємо ***Security***, натискаємо правою кнопкою миші на ***Login*** і обираємо ***New Login***. Вводимо ім’я користувача, пароль та обираємо параметри ***Enforce password policy*** та ***Enforce password expiration***. Також оберемо параметр ***User must change password at next login***, щоб користувач міг створити щоб користувач міг створити новий пароль при першому вході в систему. Обираємо в рядку *Default database* – ***Master*** та в рядку *Default language* – ***English***.

****

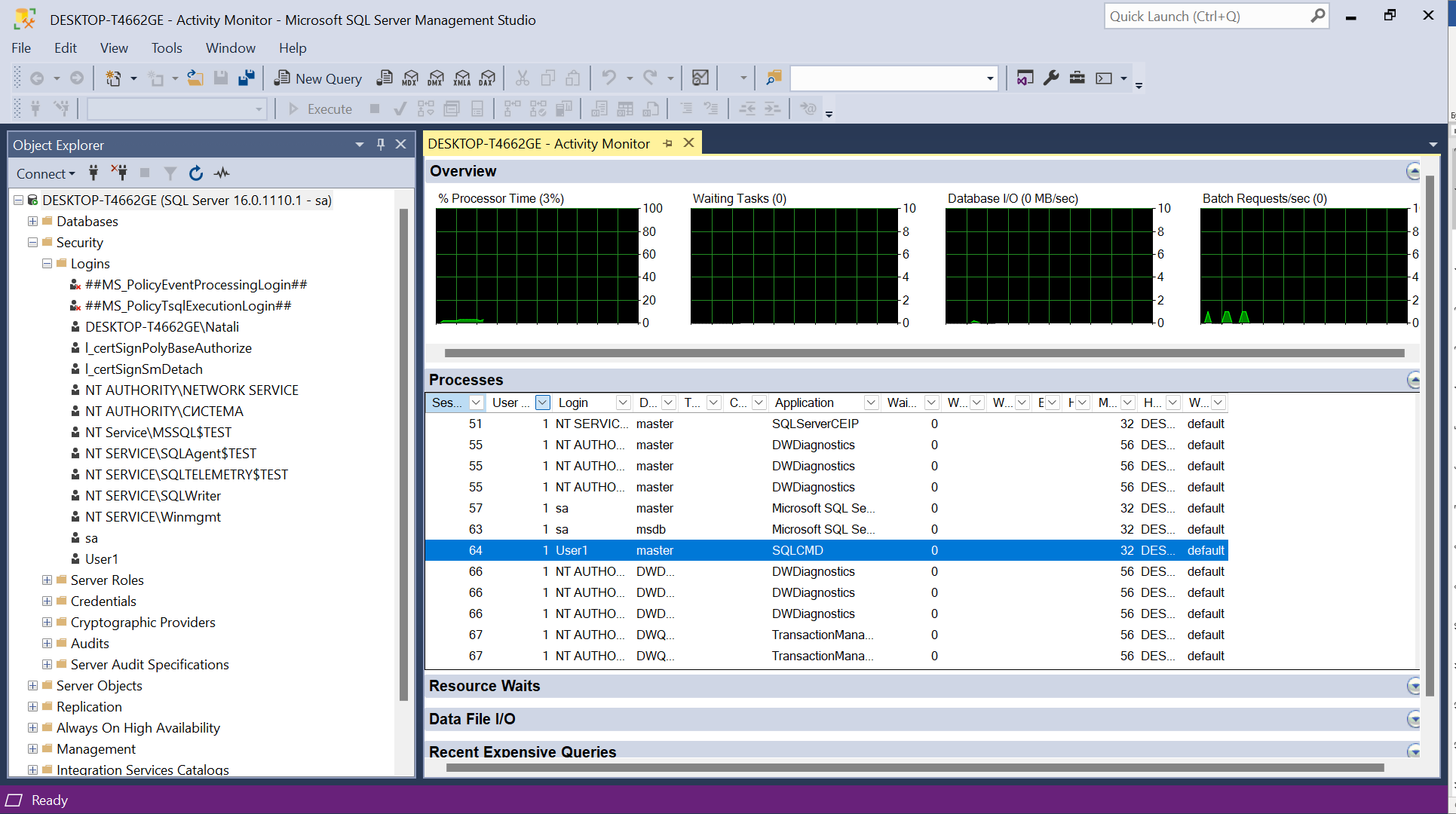
Залогінимо користувача. Виконуємо команду cmd та з командного рядку запускаємо команду:

*C:\>sqlcmd -S DESKTOP-T4662GE\TEST -U "User1" -P "user1"*

Запускаємо функцію *System\_User*, щоб повернути значення поточного імені входу.

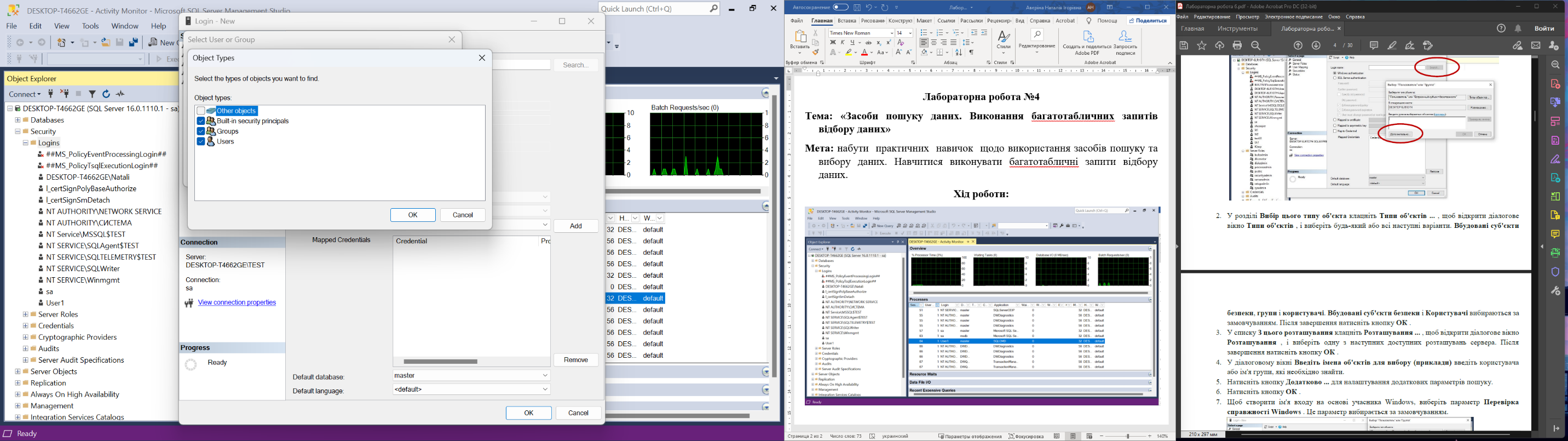
****

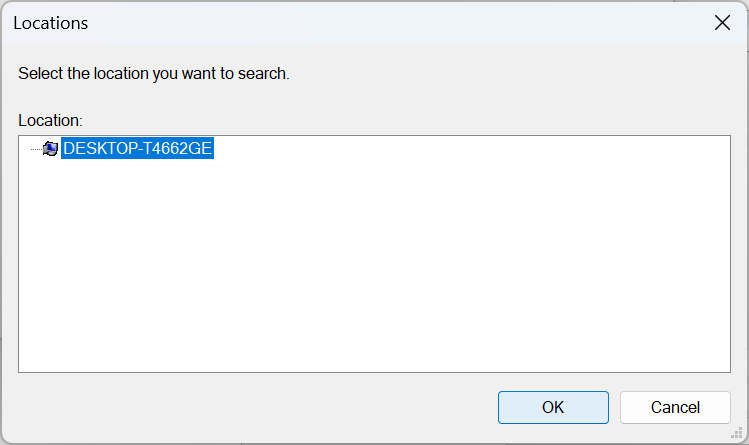
Запускаємо монітор активності та бачимо активні імена входу, серед яких *User1*.



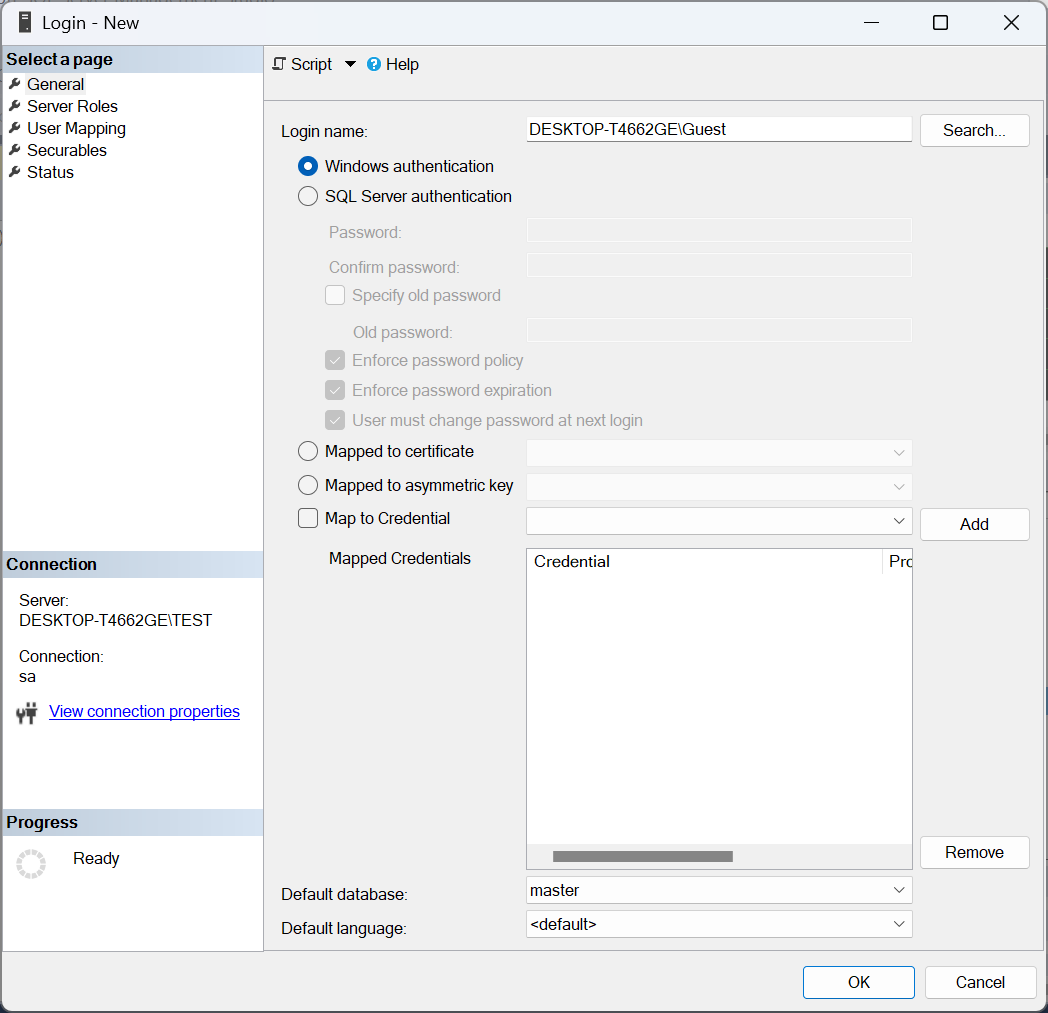
1. Використання Windows аутентифікації

Відкриваємо діалогове вікно створення користувача. Натискаємо кнопку *Search*. Обираємо типи об’єктів та розташування.





В *Advanced* обираємо зі списку обираємо потрібного користувача Windows.



1. Створення імені входу при використанні перевірки автентичності Windows за допомогою cmd.

Запускаємо командний рядок як адміністратор. Перевіряємо це за допомогою команди *WhoAmI*. Для приєднання до SQL Server від імені поточного облікового запису Windows необхідно виконати команду:

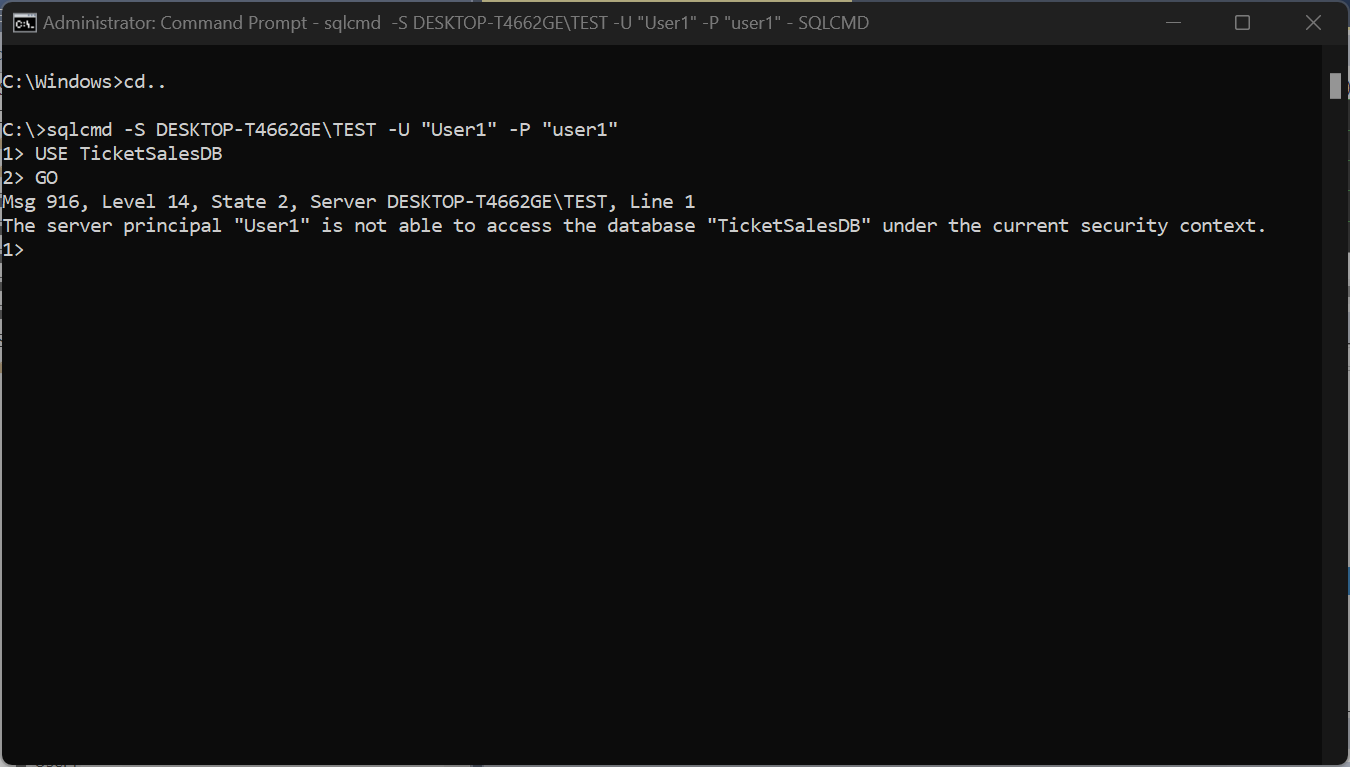
C:\> sqlcmd -S DESKTOP-T4662GE -E

Далі викликаємо команду System\_User.



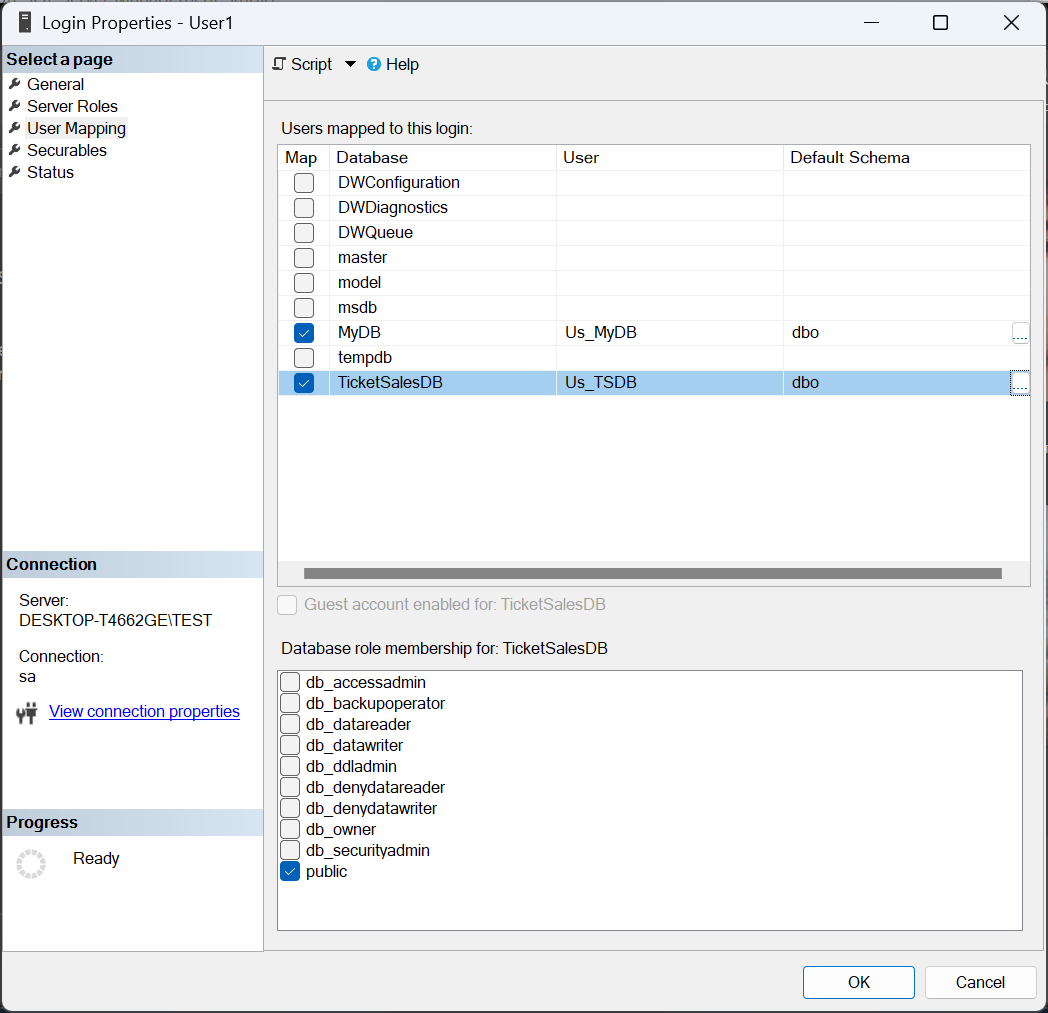
1. Авторизація

Авторизуємося за допомогою командного рядка за логіном *User1* та спробуємо активізувати базу даних *TicketSalesDB*.

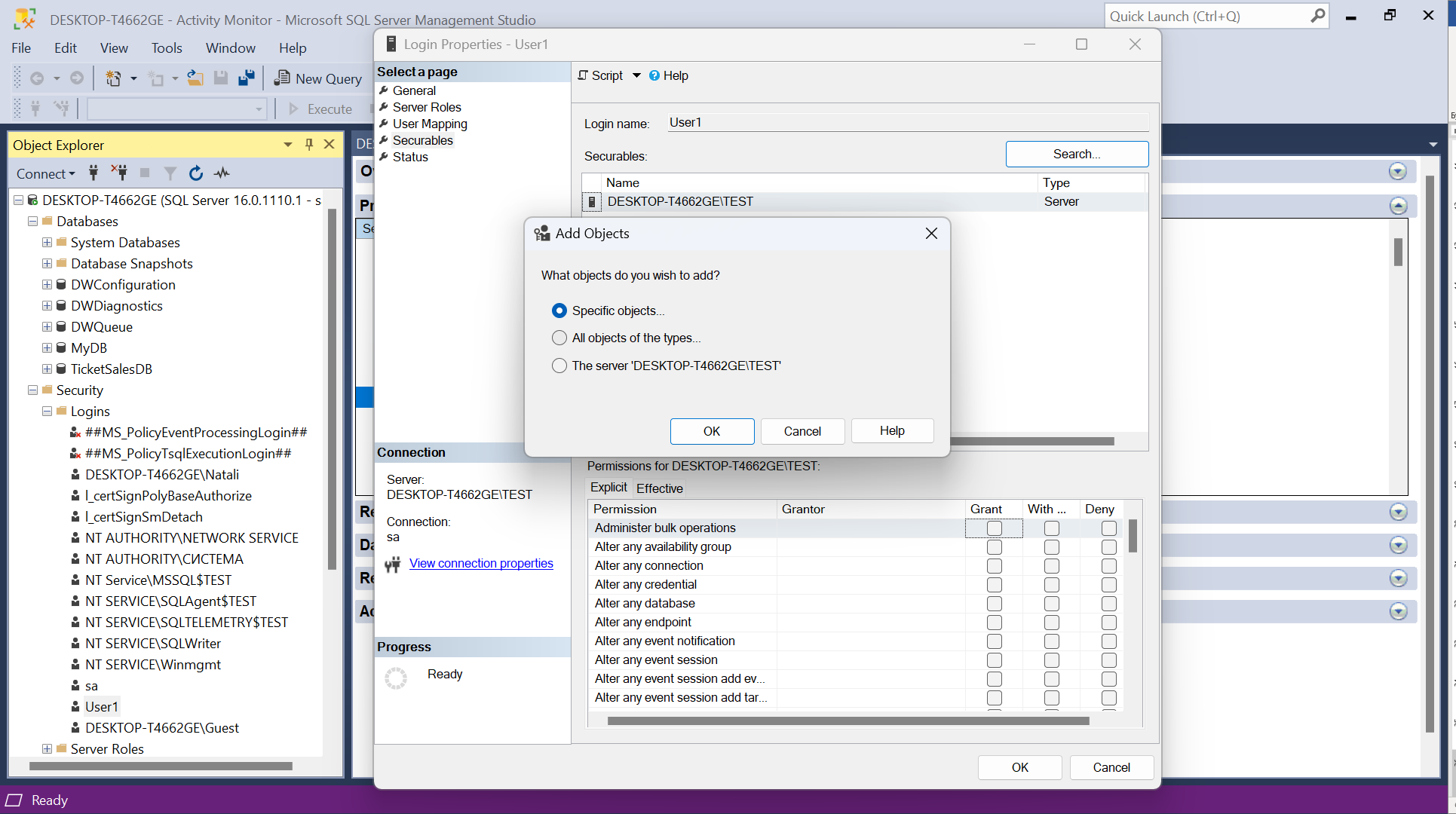


Виникає помилка, бо користувач не має прав доступу до бази даних.

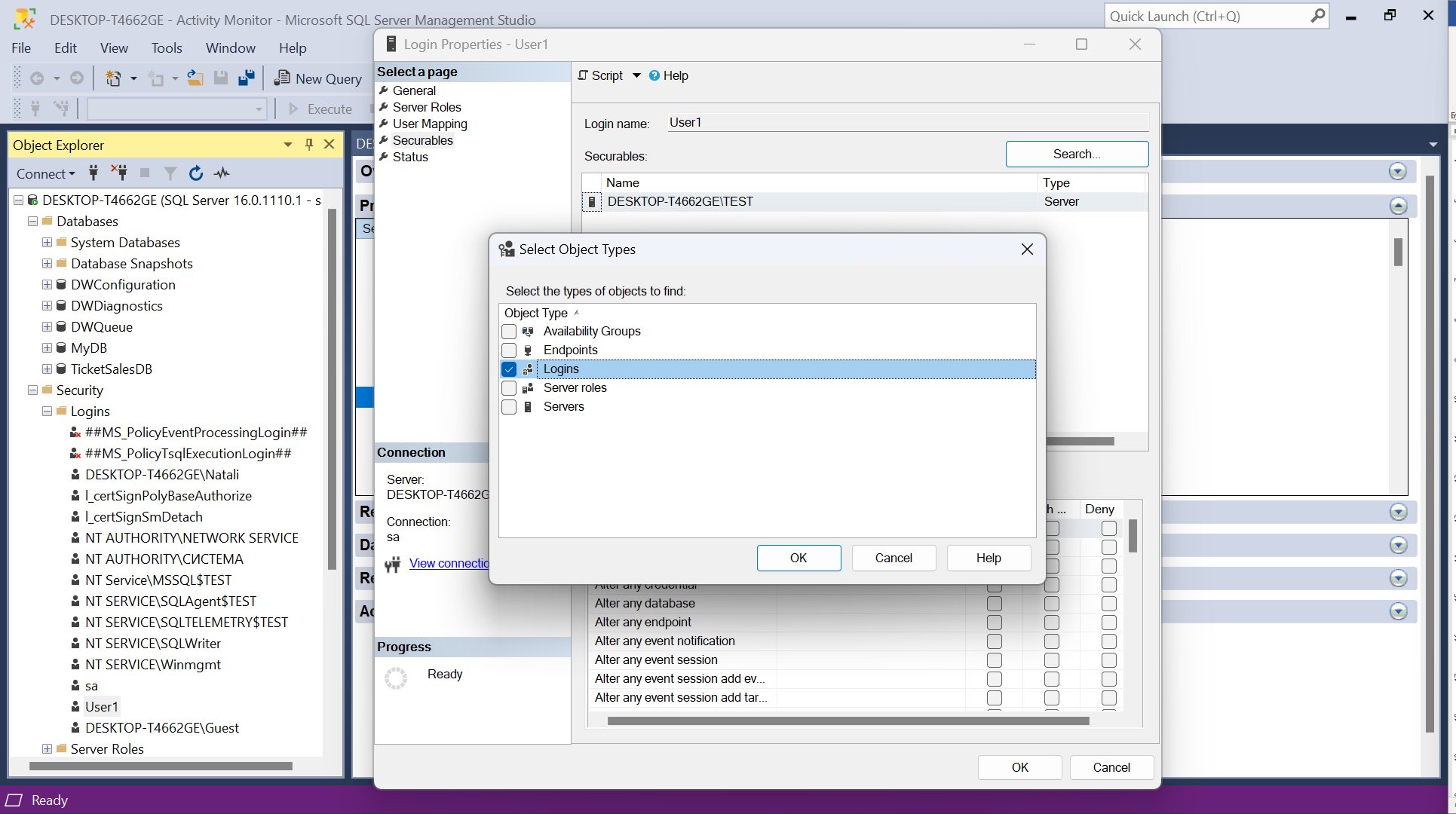
Надамо такі права користувачу за допомогою графічного інтерфейсу SSMS. Це необхідно зробити на рівні серверу. У вікні *User Mapping* відмічаємо БД, які будуть надаватися для даного логіну і створюємо нових користувачів для кожної з БД. Обираємо роль ***public***.



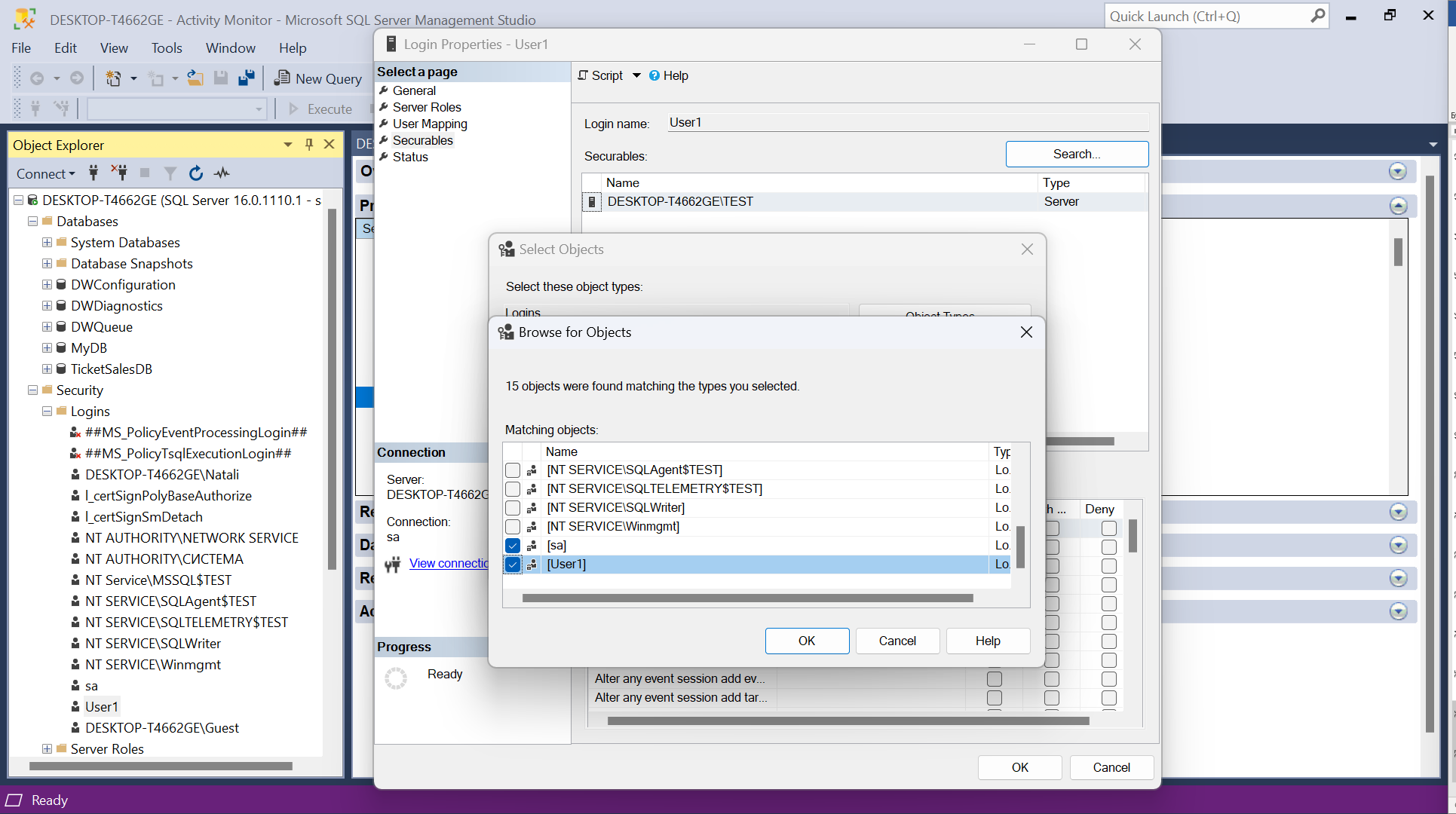
На вкладці *Securables* обираємо кнопку *Search*. У вікні *Add objects* обираємо ***Specific objects***.



Обираємо типи об’єктів.

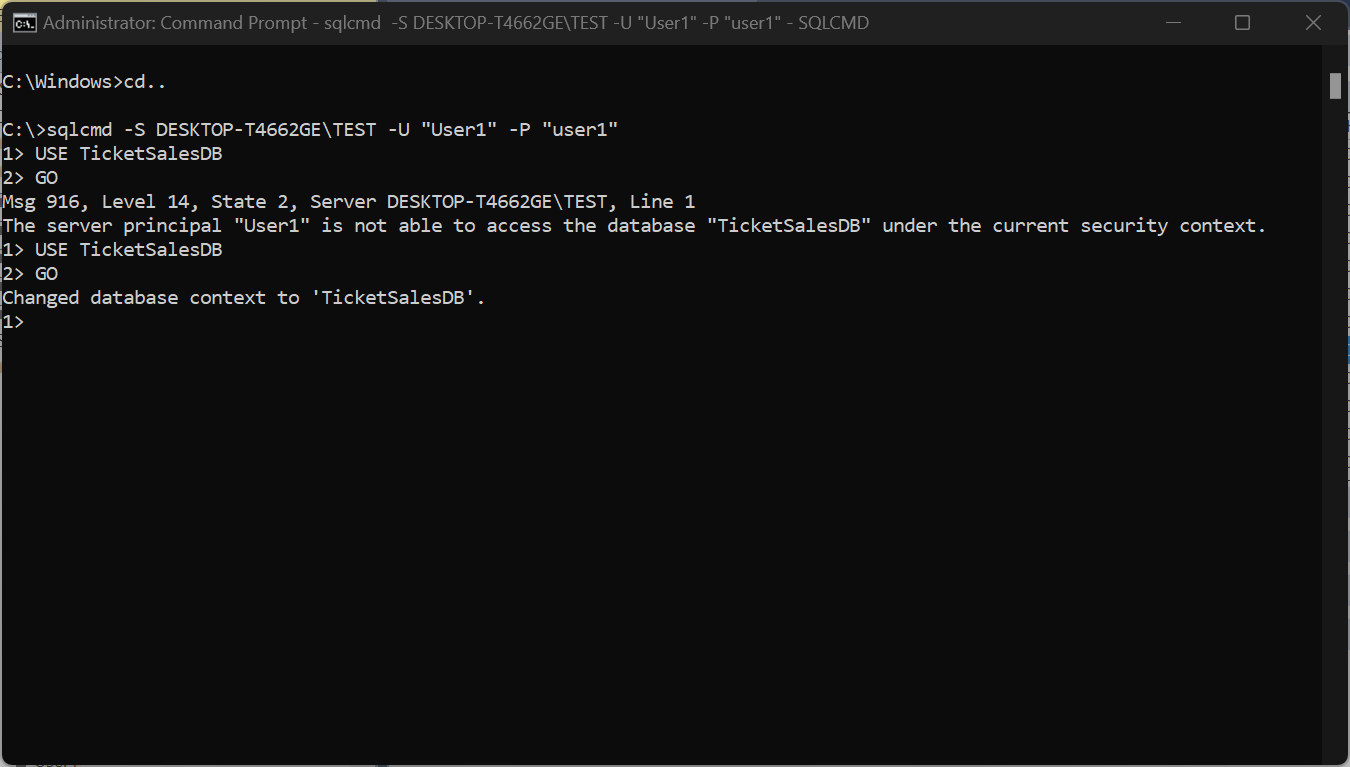


Натискаємо кнопку *Browse* та обираємо доступні об’єкти.

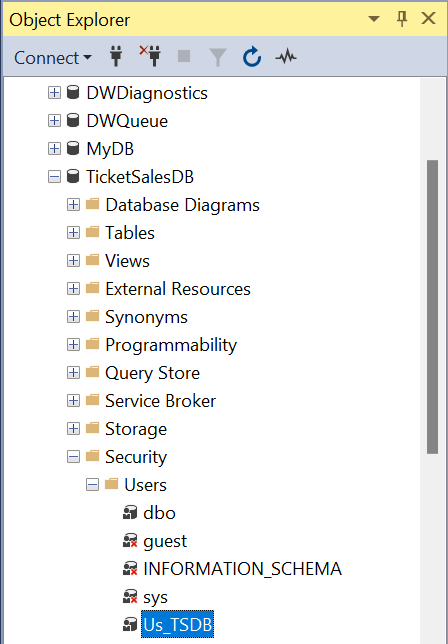


Надаємо імені входу дозвіл ***Connect SQL*** та ***Alter any login.***

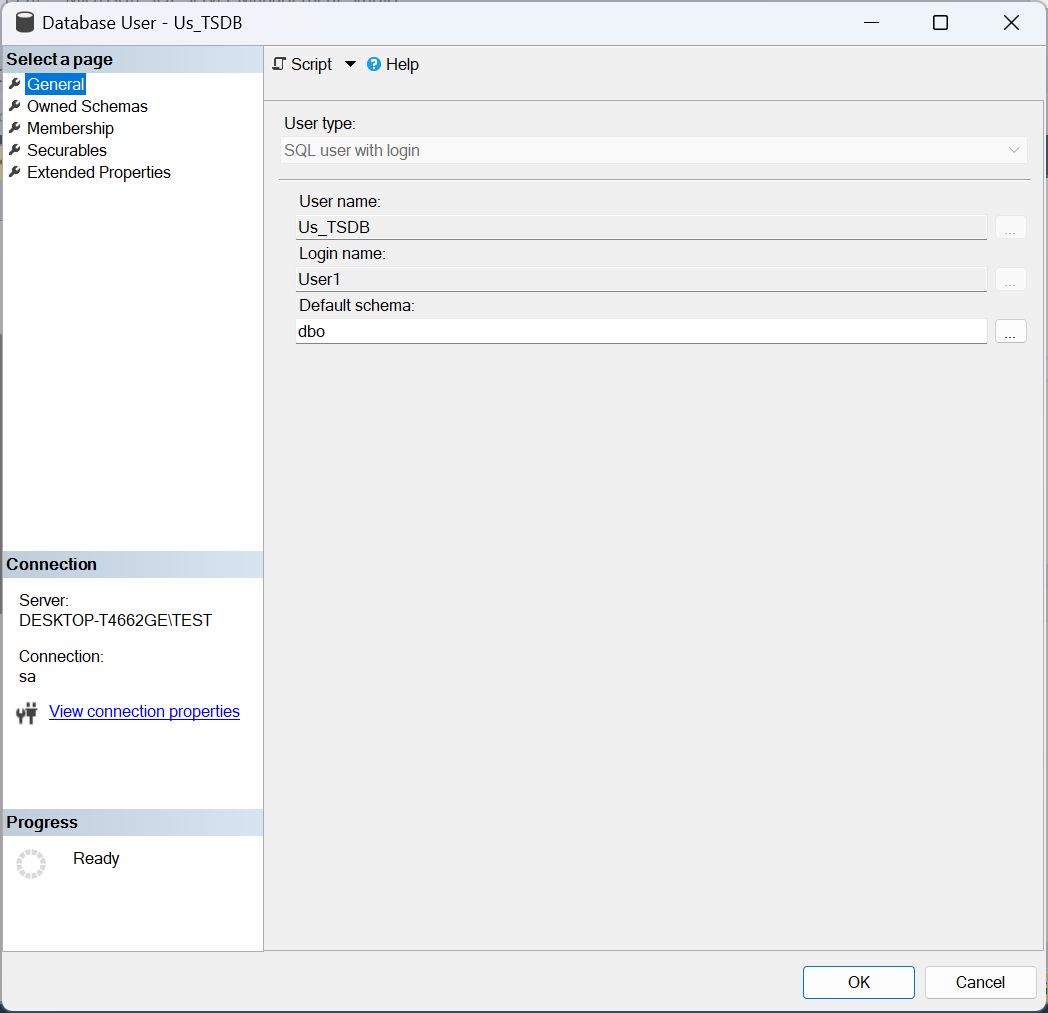
Тепер ми можемо через командний рядок активізувати базу даних TicketSalesDB.



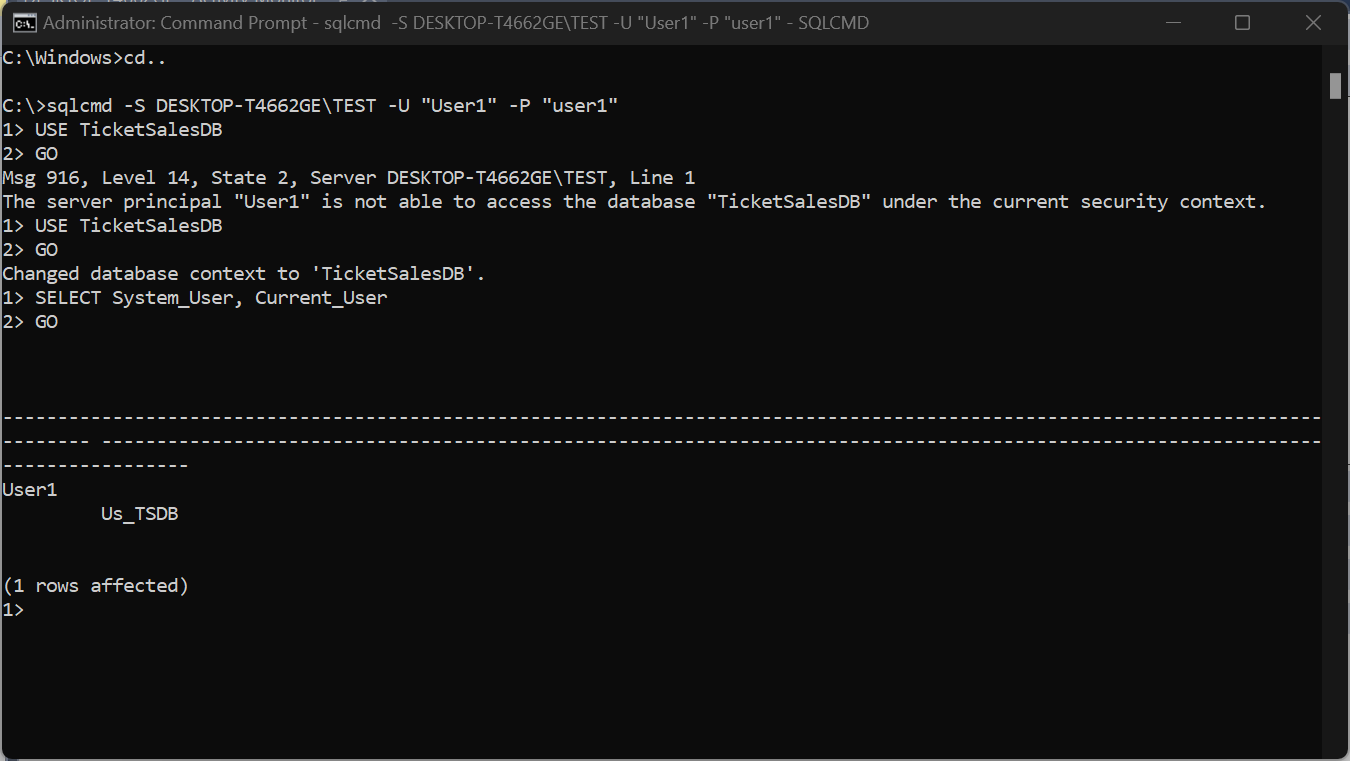
В базі даних створився користувач.



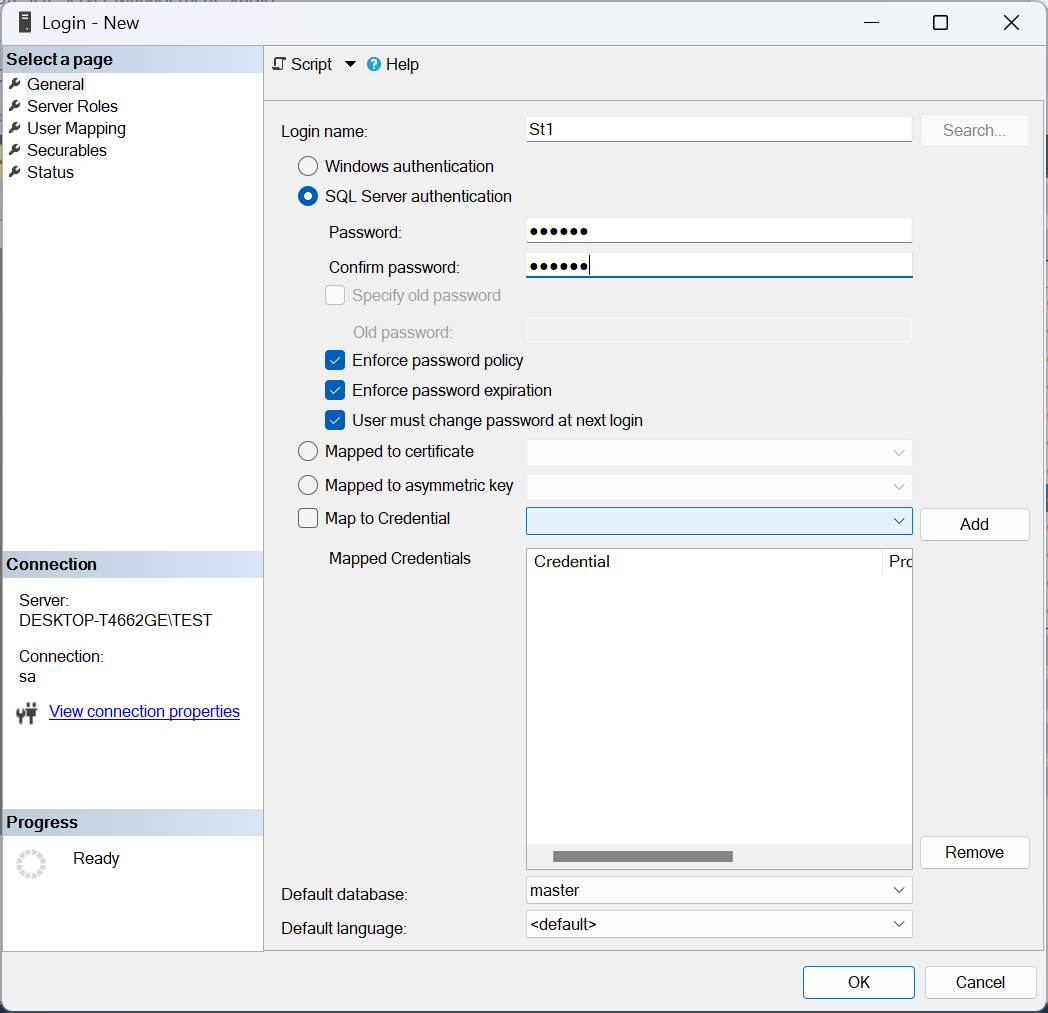
Якщо зайти у властивості користувача ***Us\_TSDB***, то ми побачимо його зв’язок з логіном.



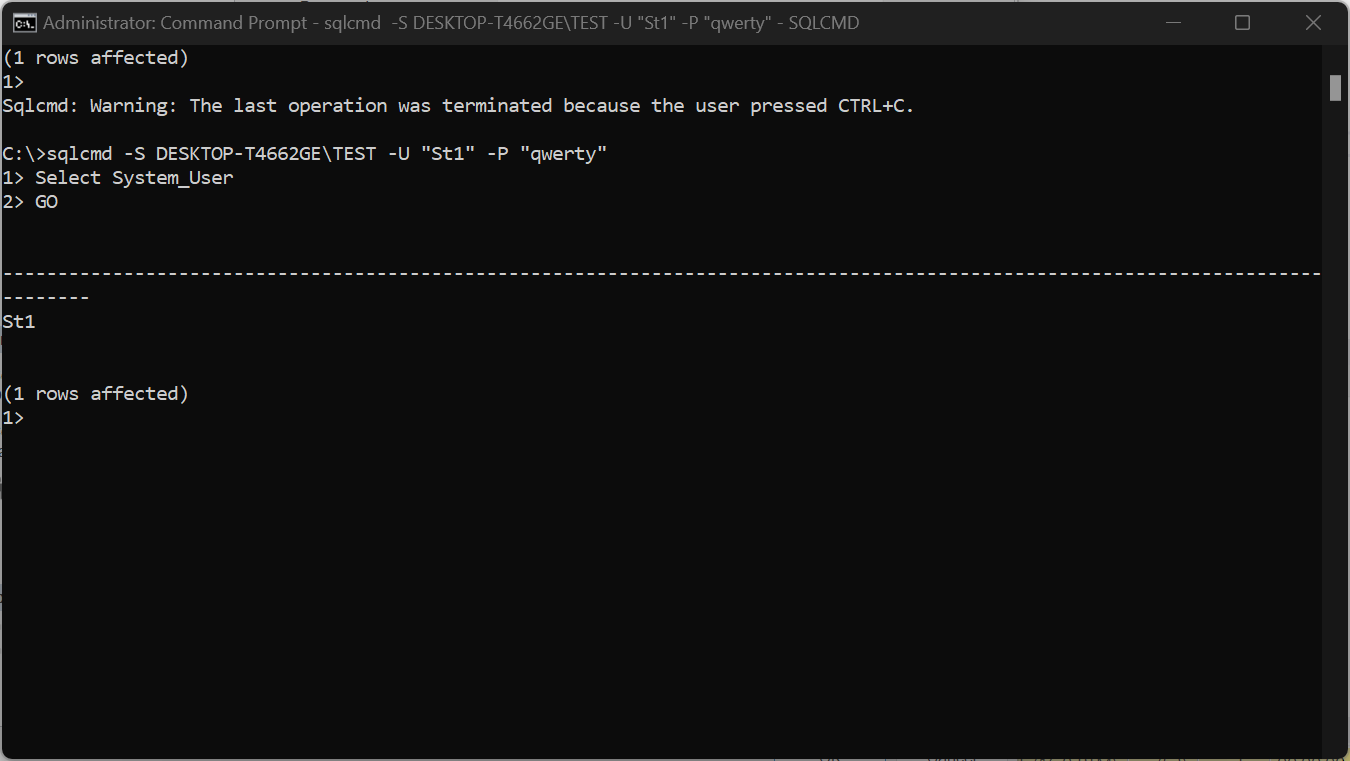
В командному рядку передивляємося системного користувача – Login name та поточного – User name.



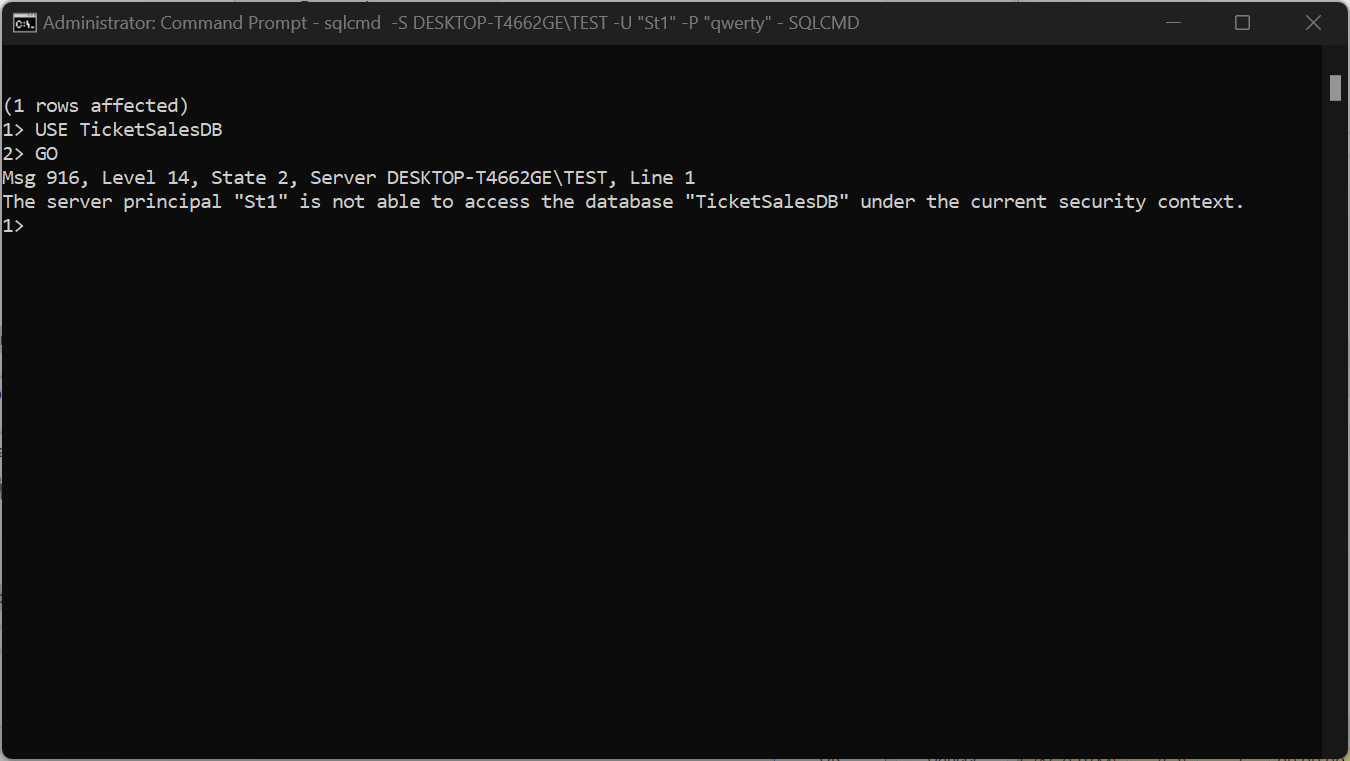
Створюємо новий логін.



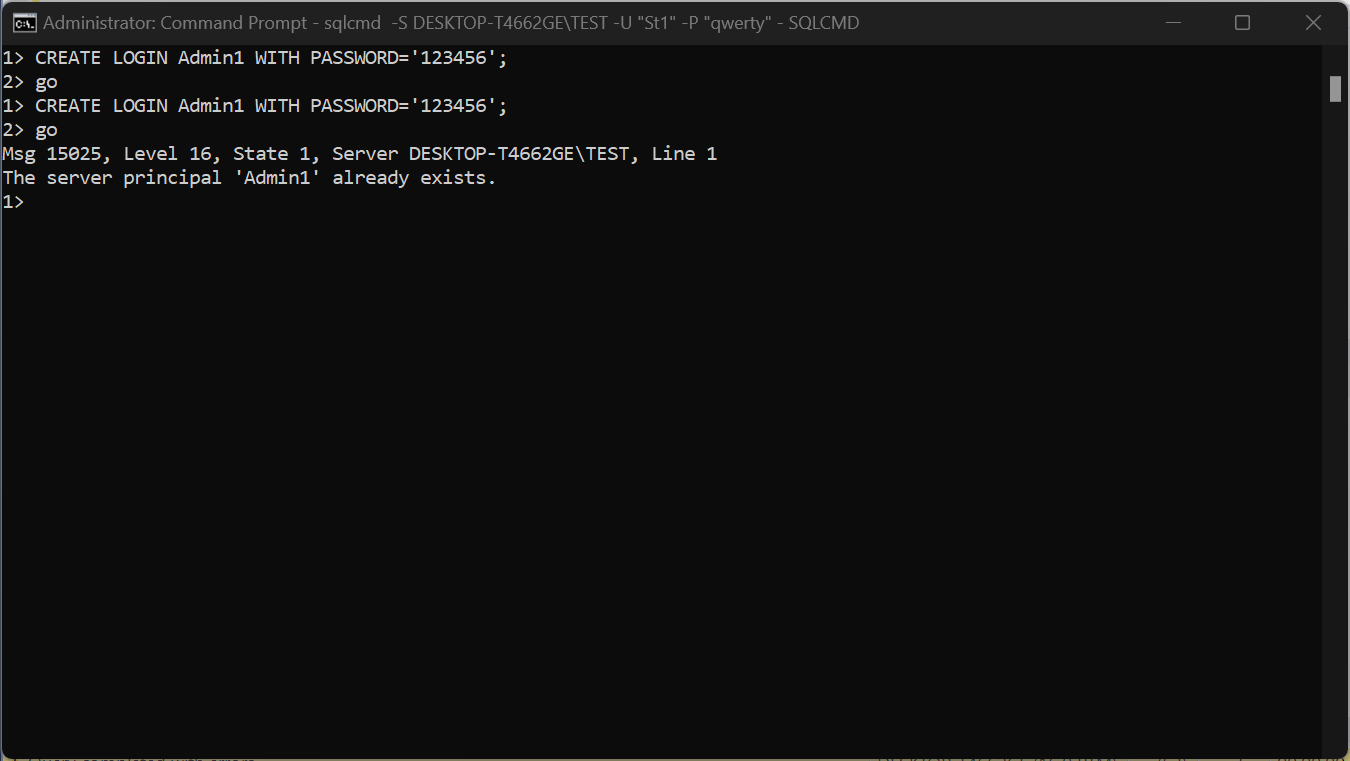
Через командний рядок входимо за цим логіном у систему.

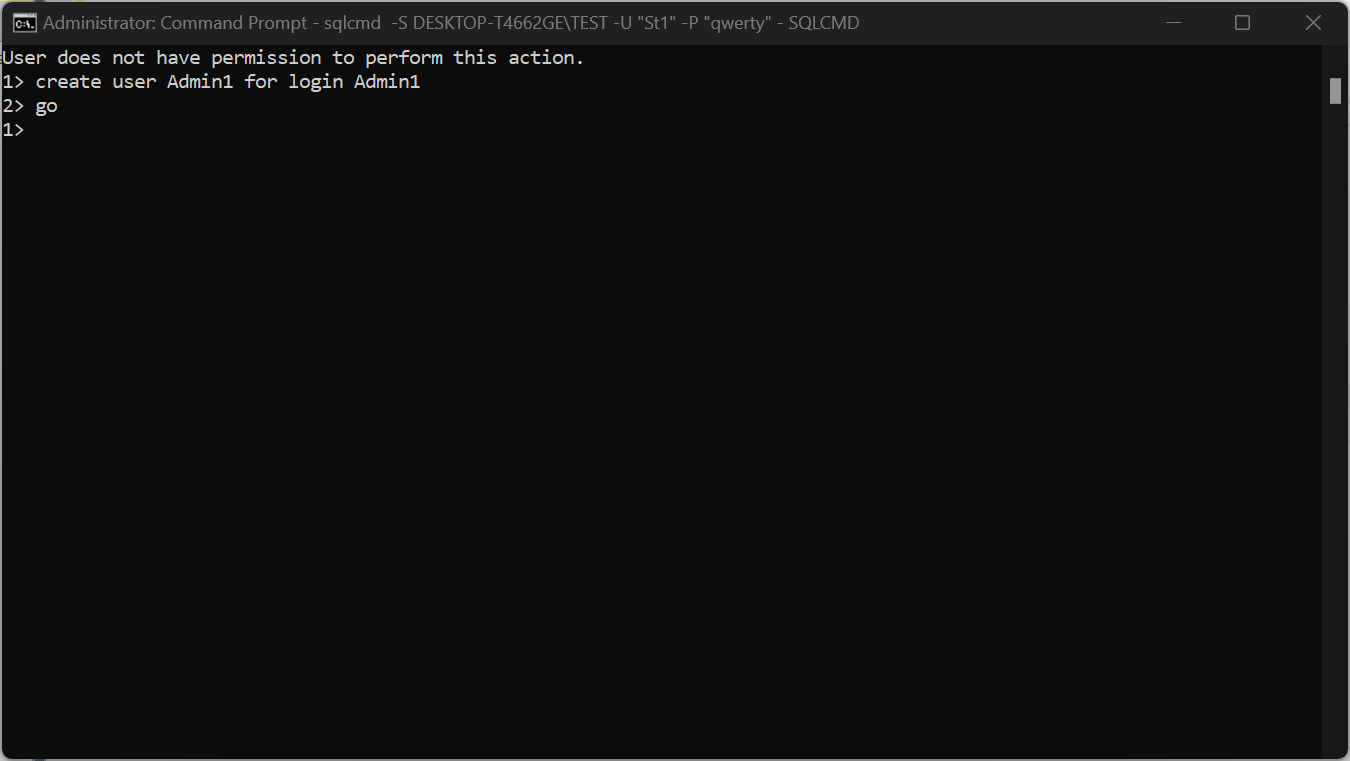


Робимо спробу входу до БД.

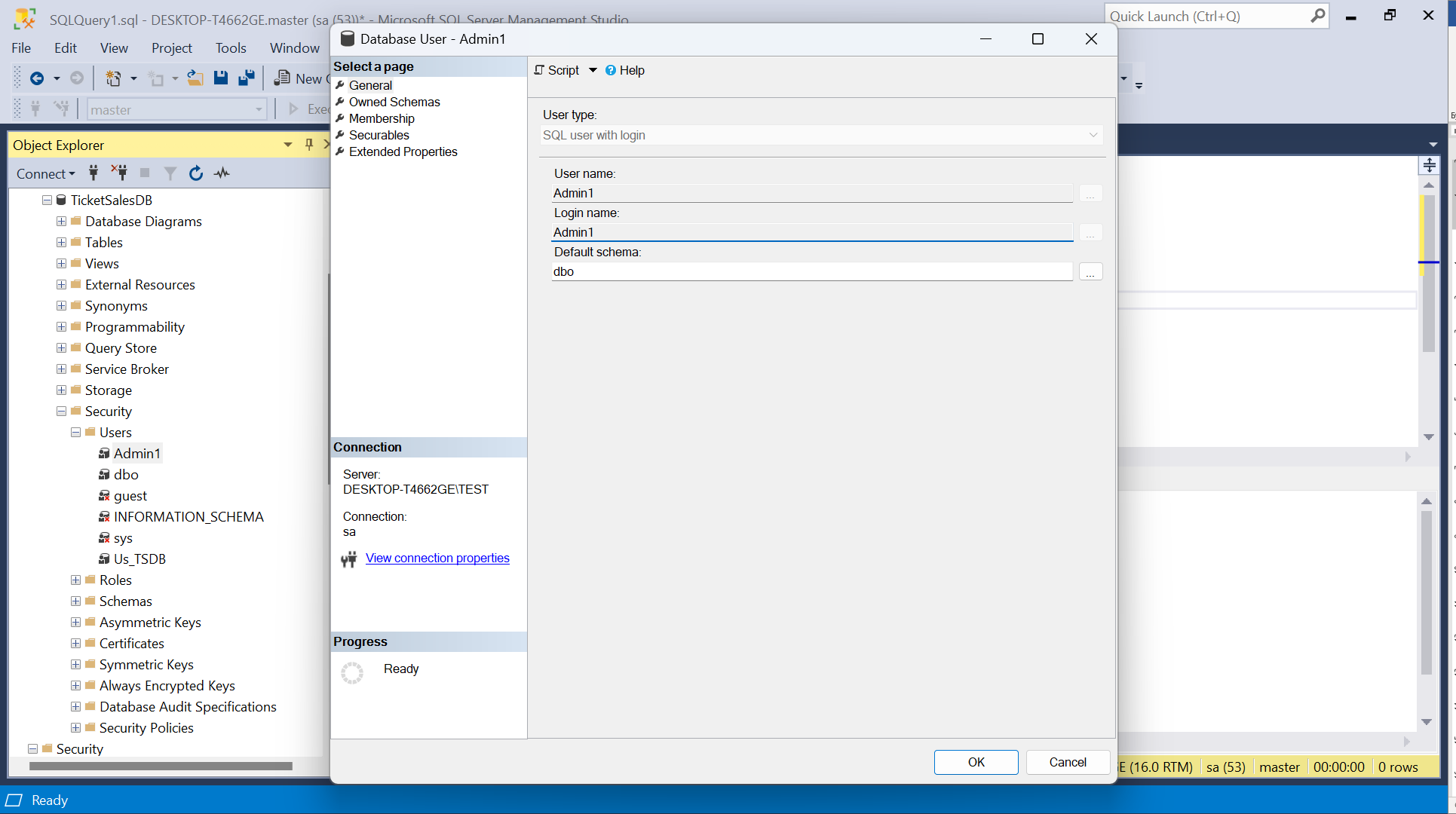


1. Створення нового користувача бази даних і зв'язування його з існуючим логіном

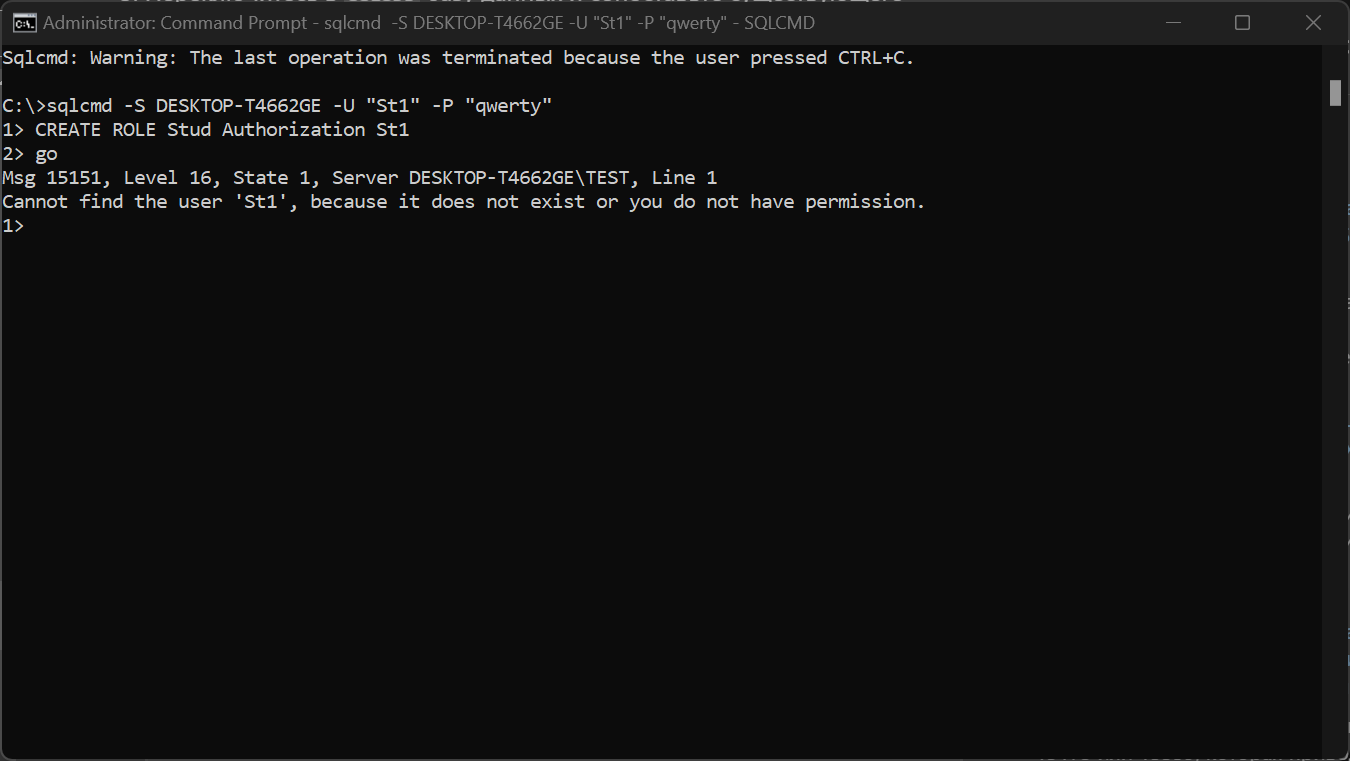


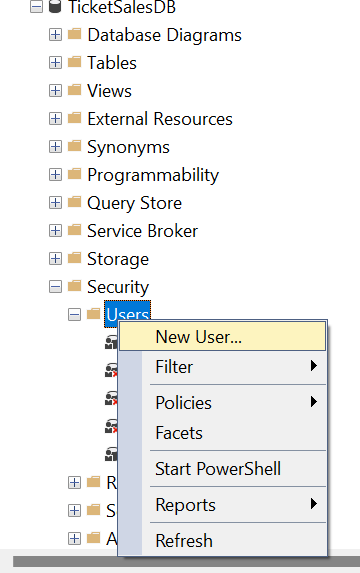


Можемо побачити, що у користувача *Admin1* бази даних *TicketSalesDB* є взаємозв’язок з системним користувачем *Admin1*.

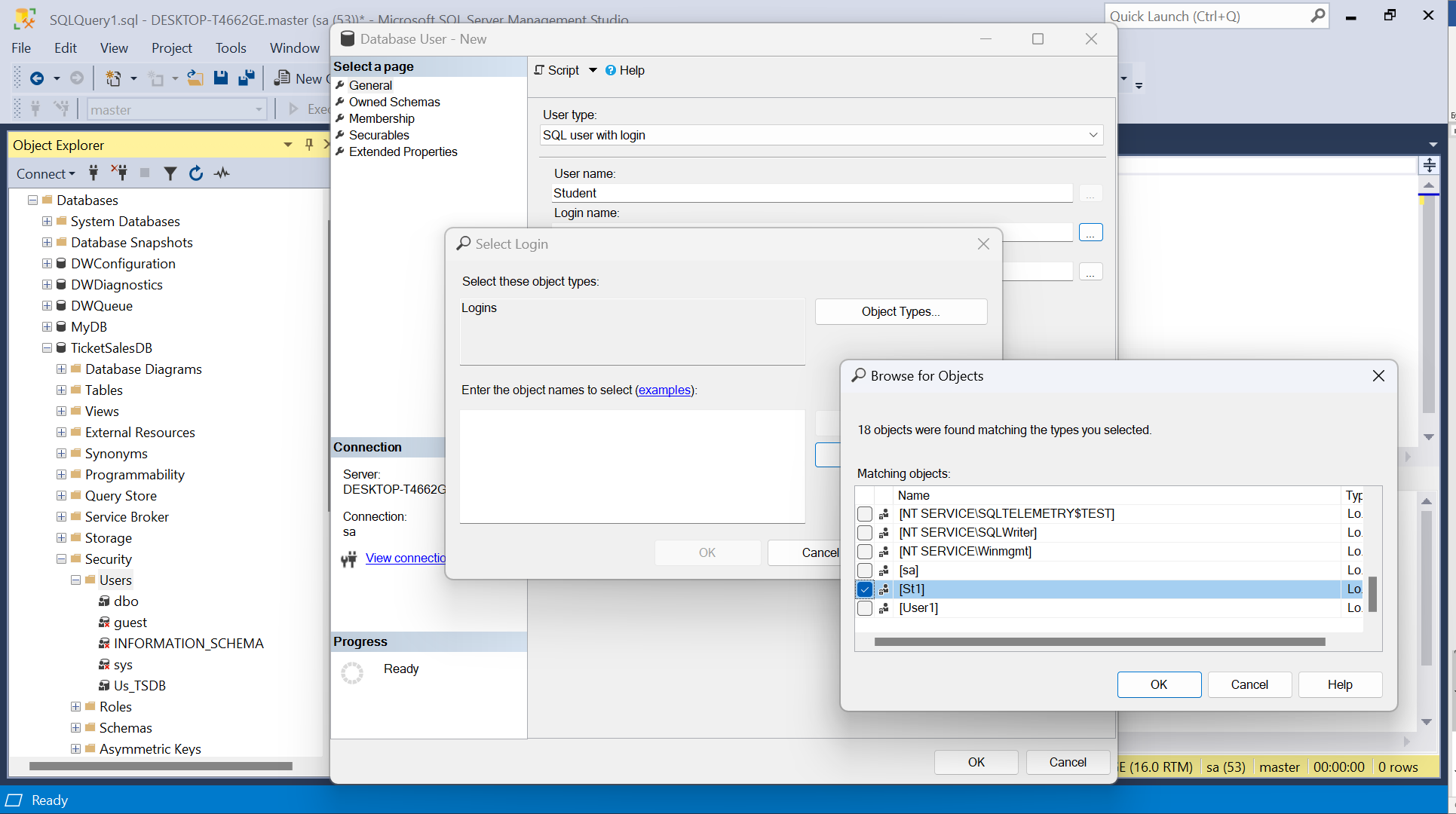


1. Створення ролі для користувача за допомогою cmd

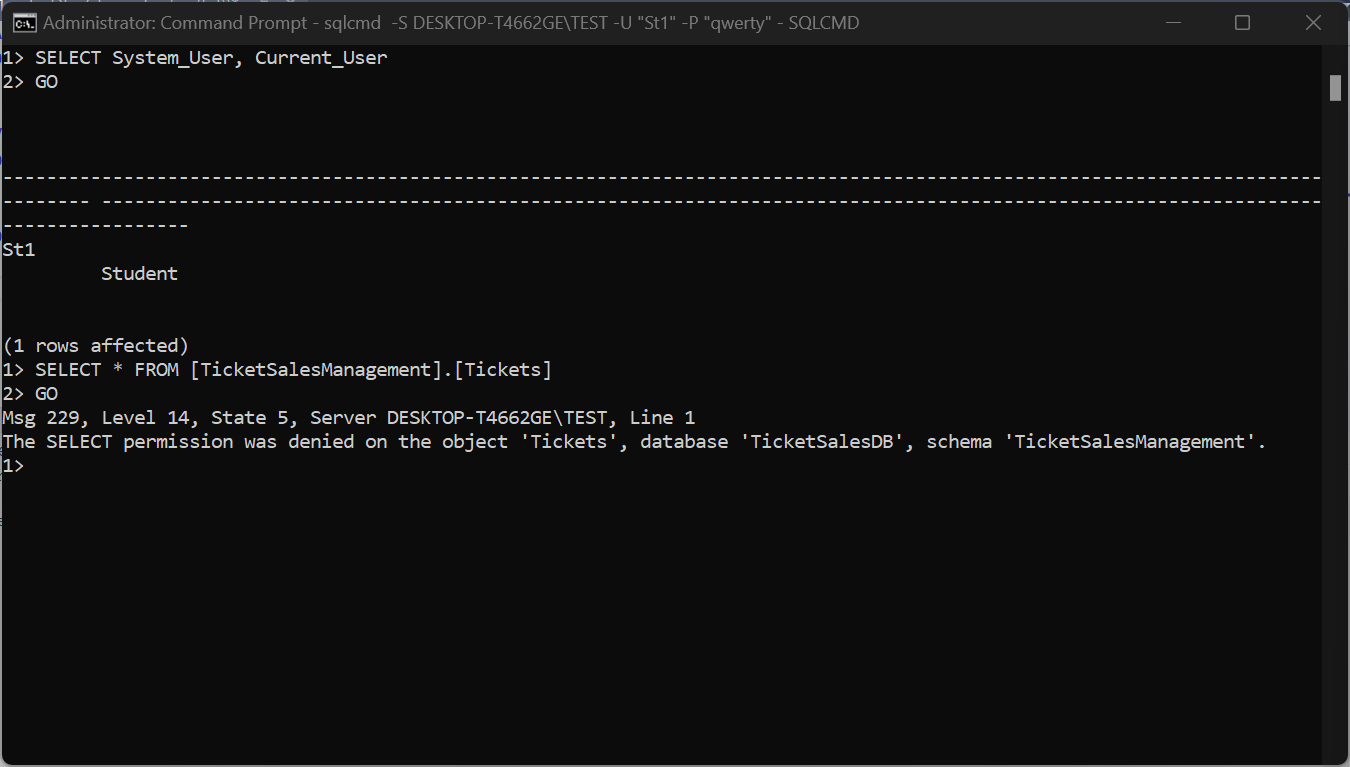




Вказуємо ім’я користувача, додаємо логін ***St1*** та натискаємо ОК.

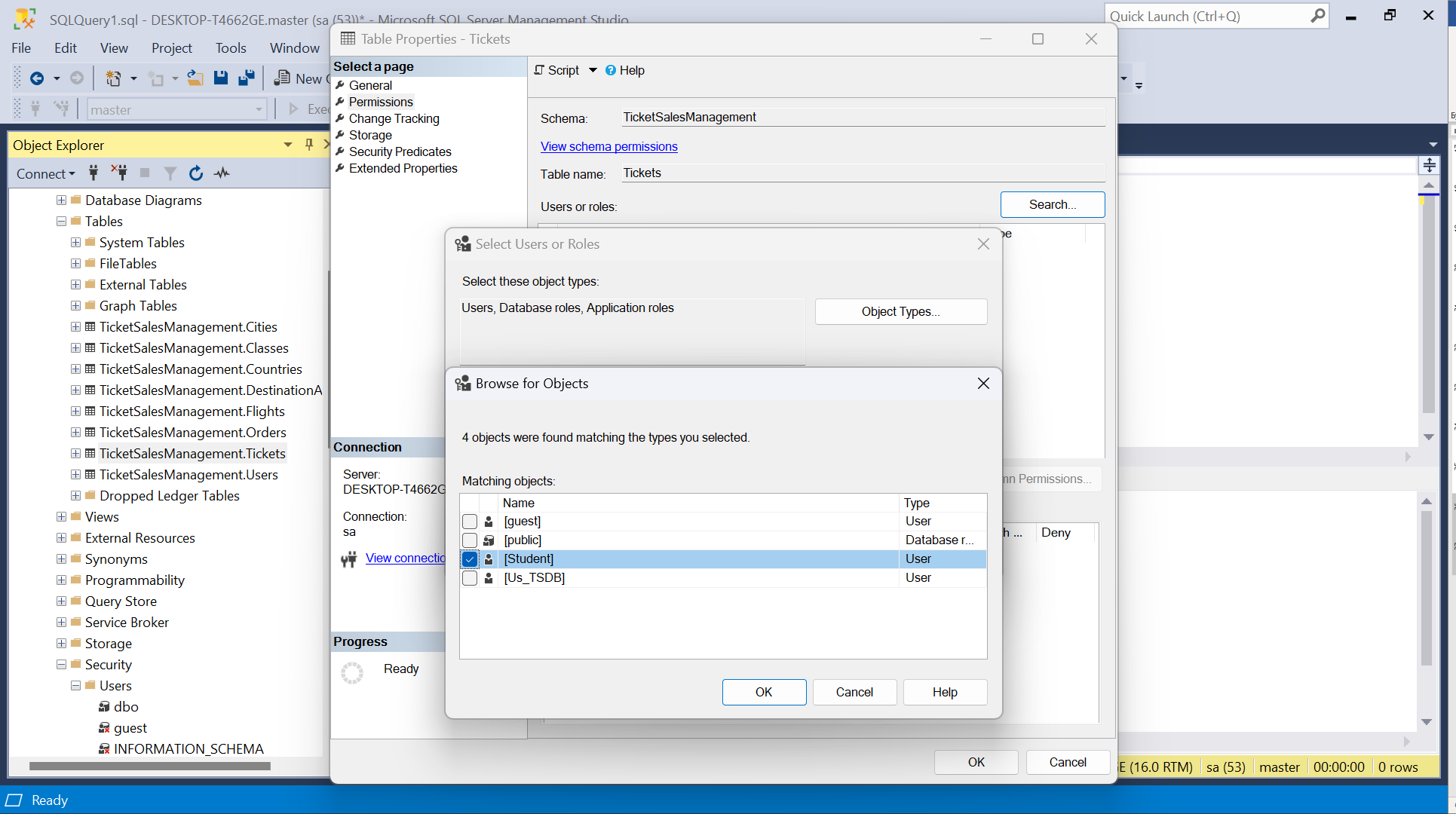


З’єднання з даною базою даних відбулося. Але даний користувач не може переглянути вміст таблиць, бо не має дозволу.

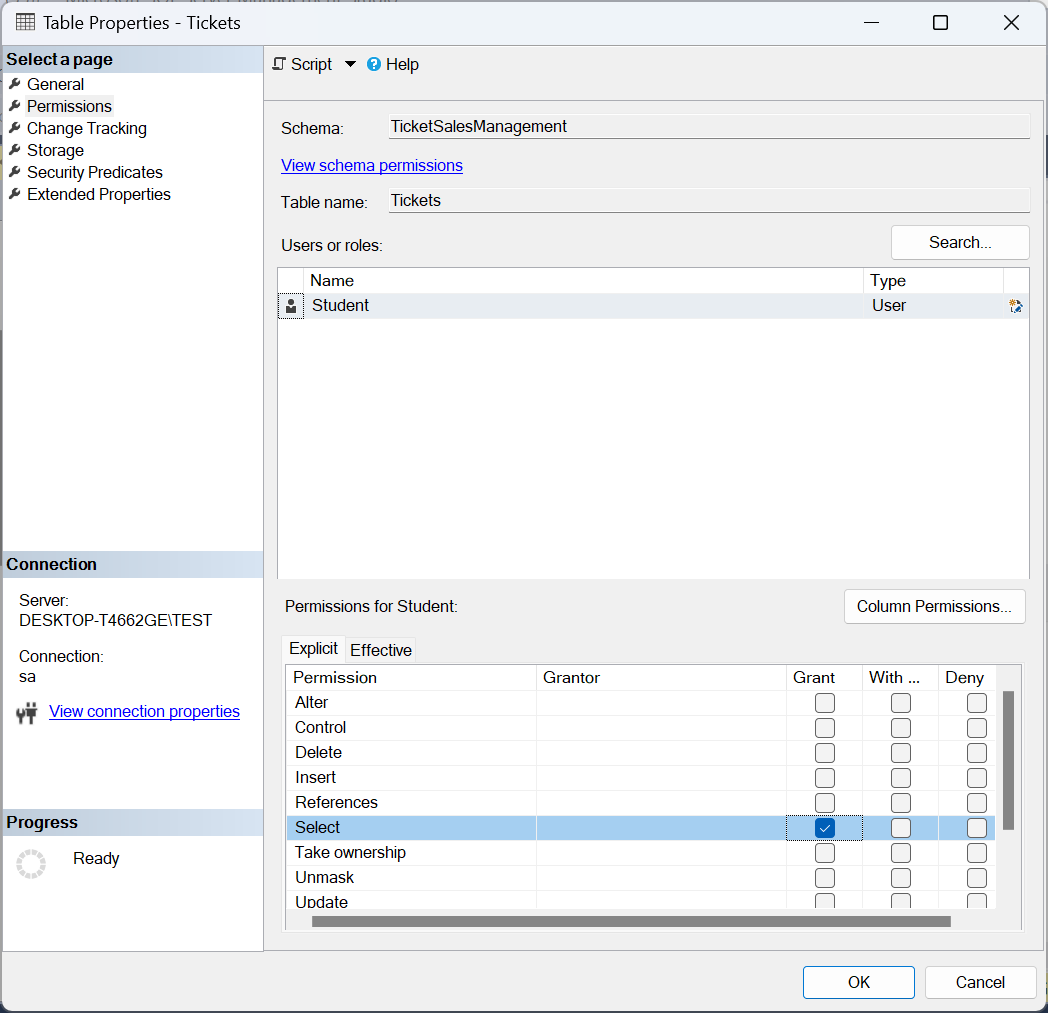


1. Надання доступу для користувачів в графічному інтерфейсі SSMS

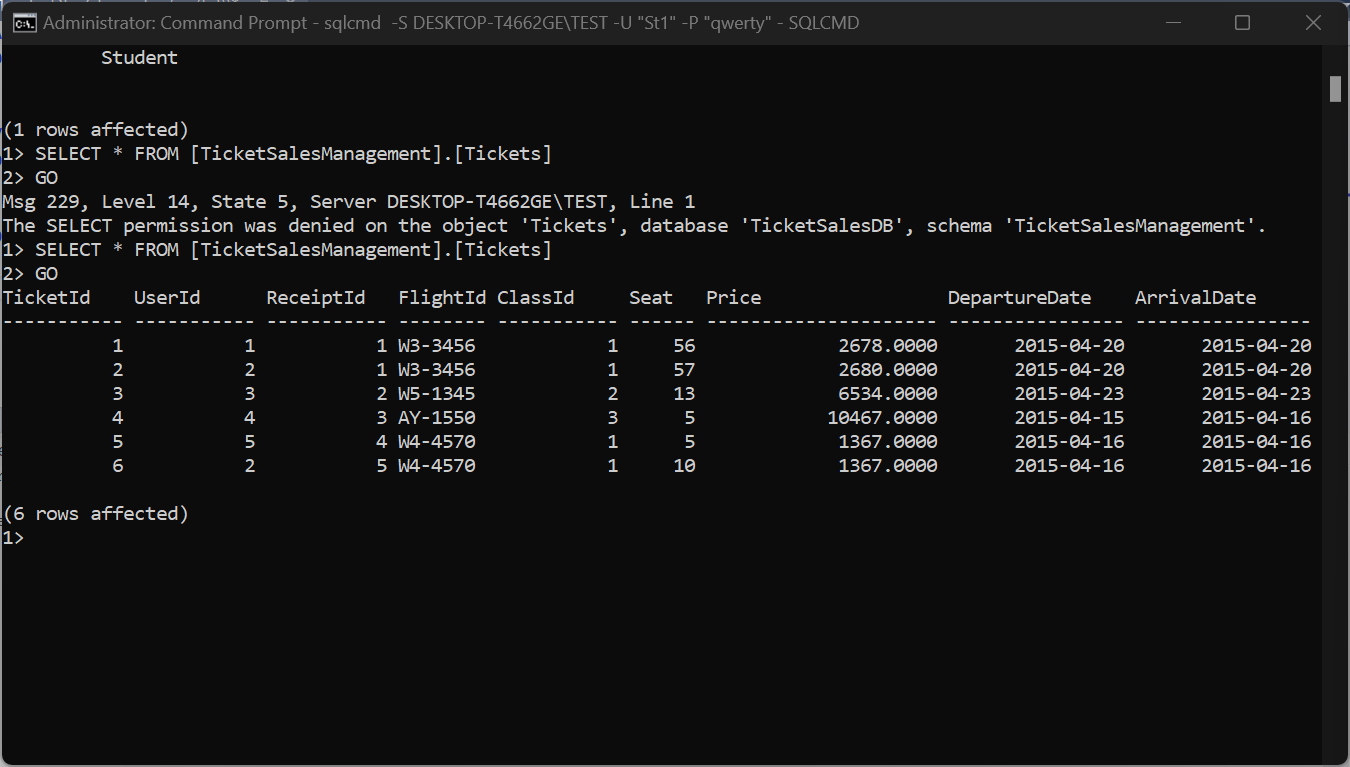
Обираємо БД та відповідну таблицю та заходимо в *Properties*. В діалоговому вікні обираємо опцію *Permissions* – *Search* – *Browse*. Обираємо користувача ***Student***.



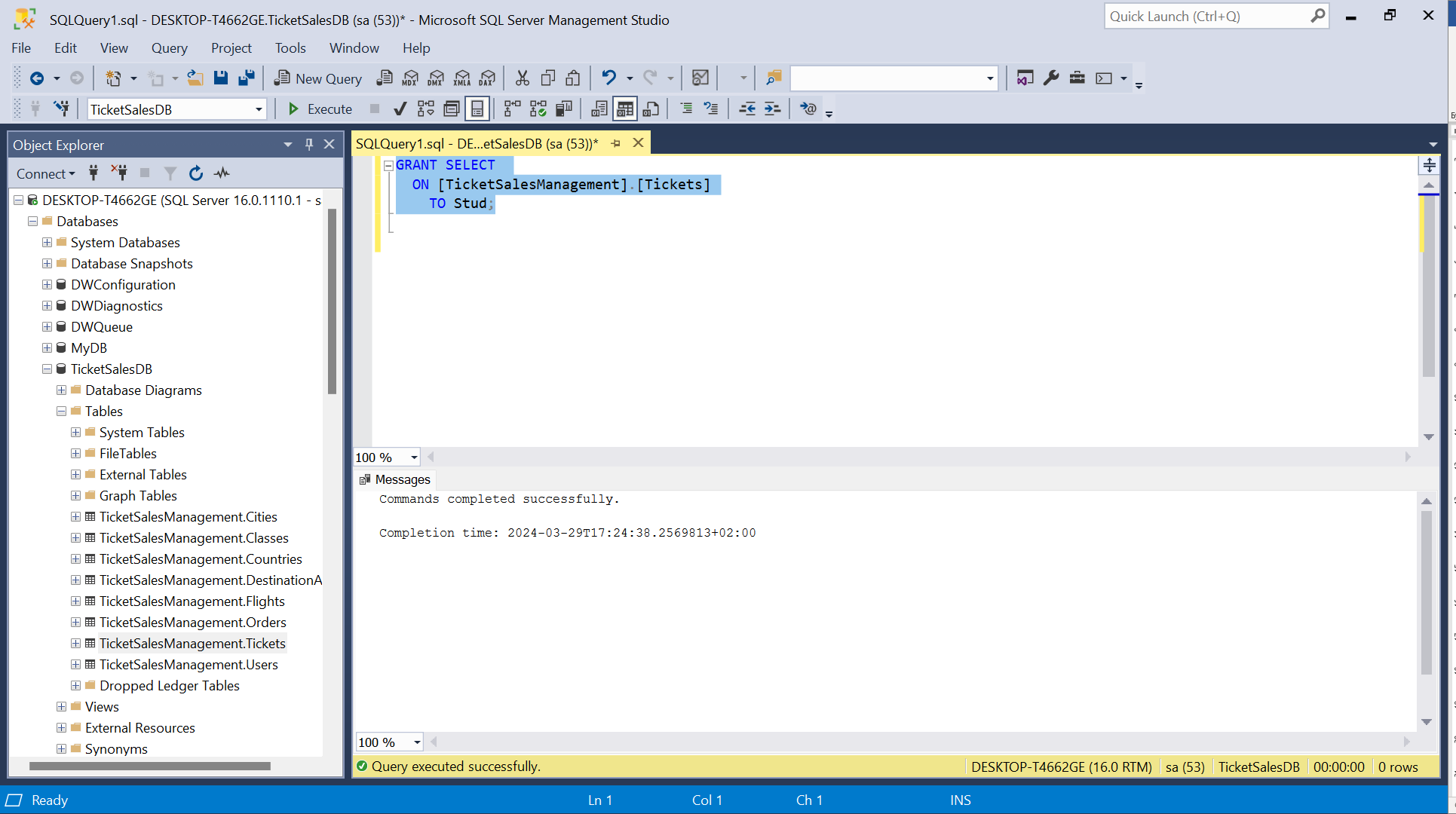
Далі надаємо дозвіл виконувати команду ***Select***.



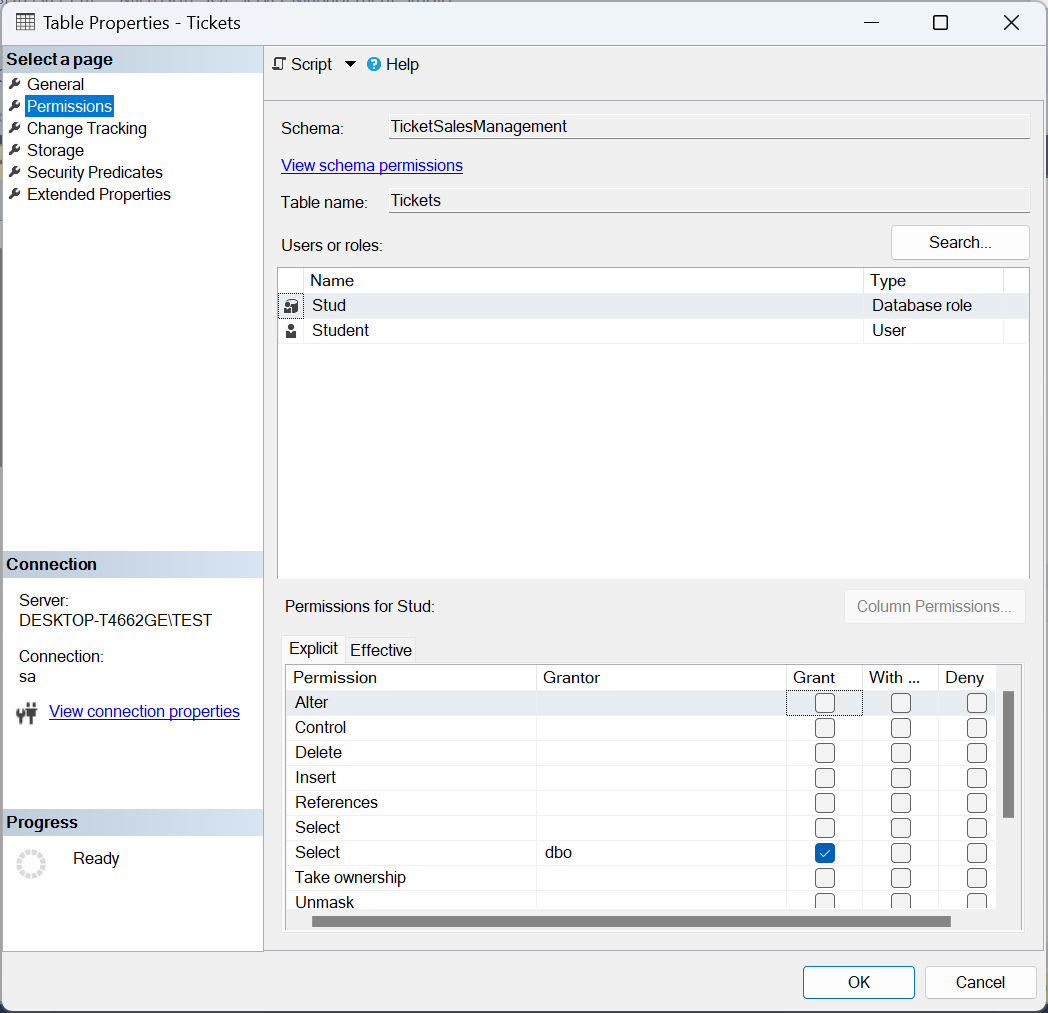
Перевіряємо. Сервер дозволив виконання команди для даної таблиці.



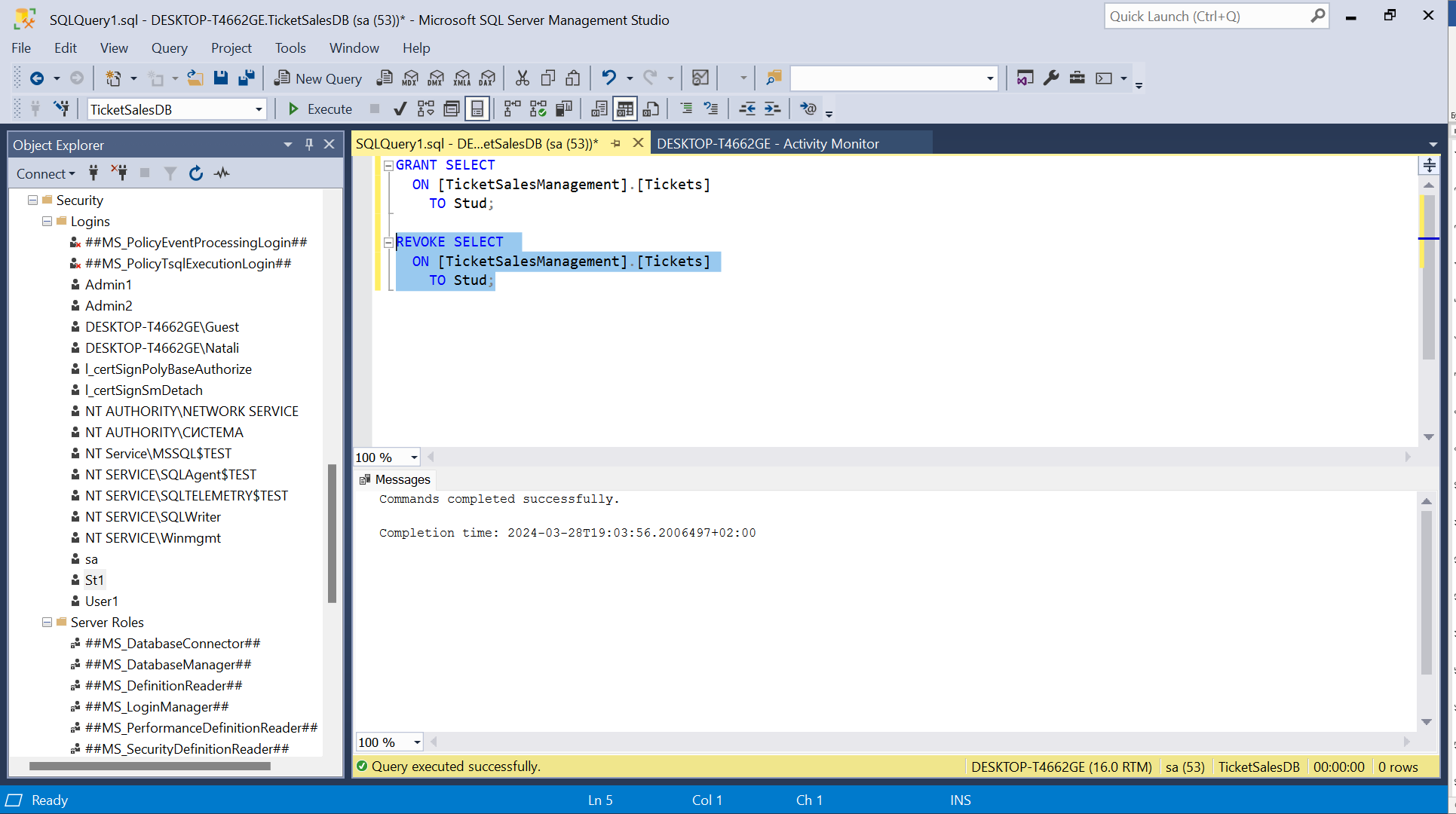
Надамо доступ ролі *Stud* на виконання команди ***Select***.



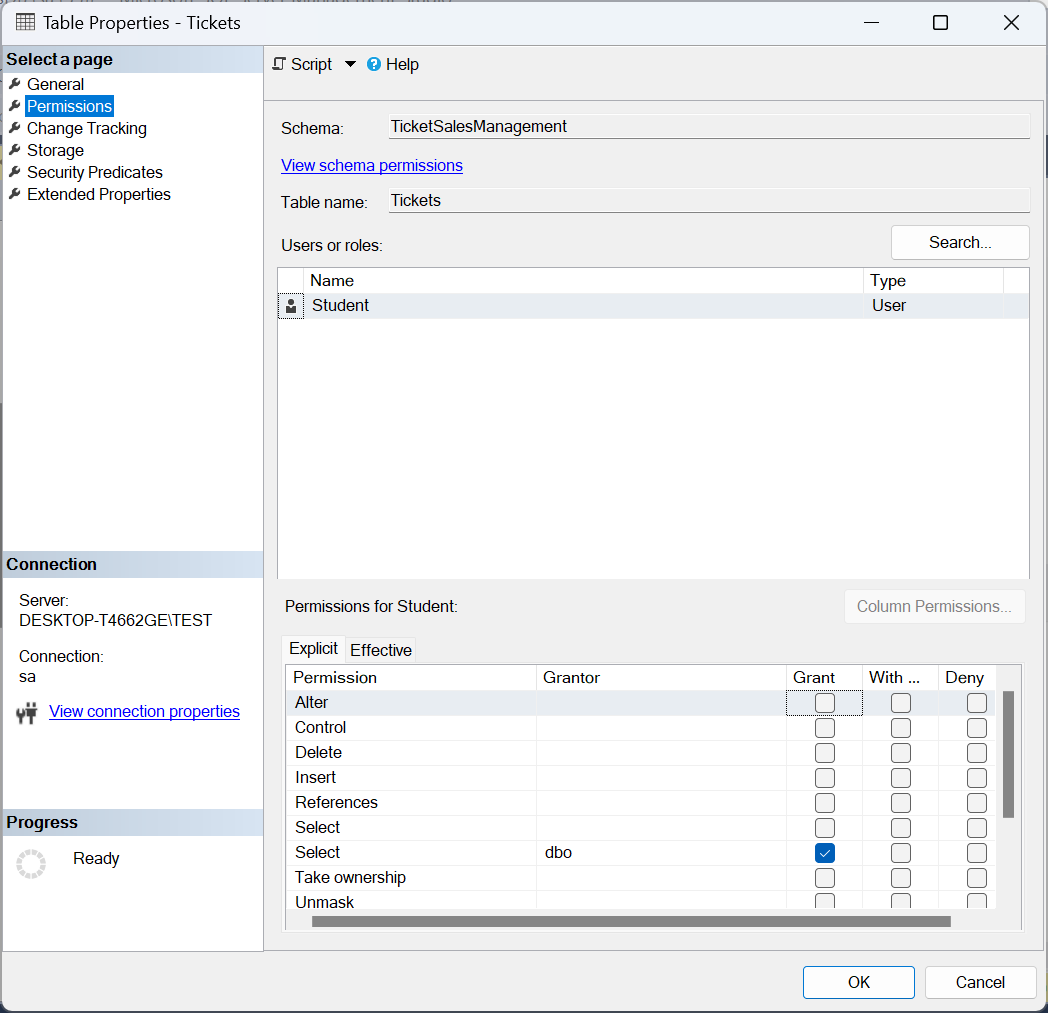
Результат виконання:



Тепер скасуємо доступ на виконання команди ***SELECT*** ролі *Stud*.

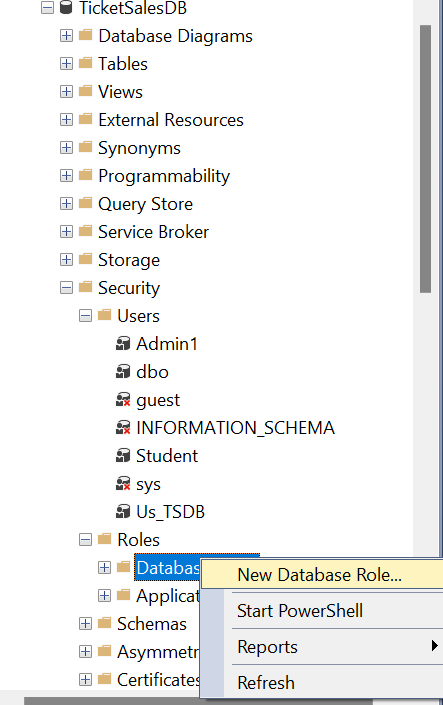


Результат виконання:

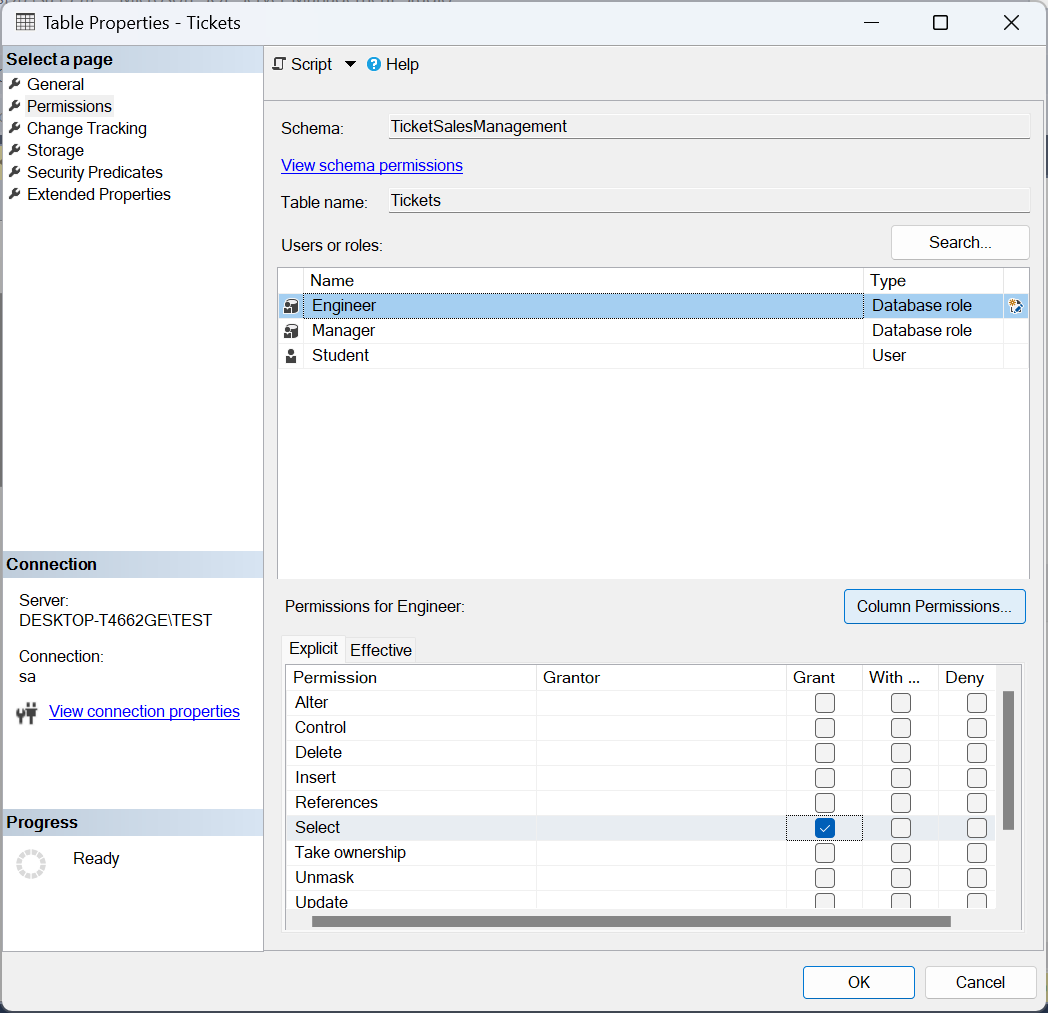
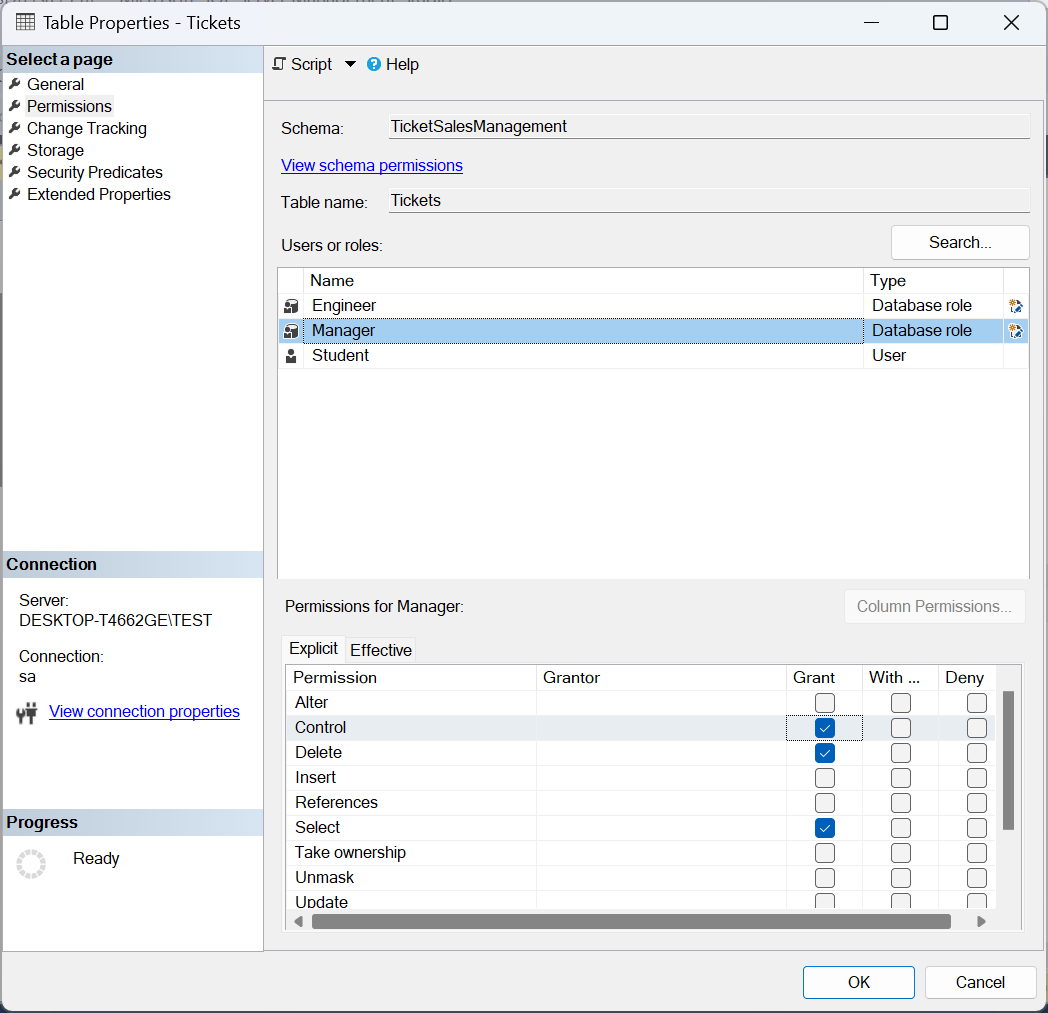


1. Створення нової ролі для БД за допомогою графічного інтерфейсу SSMS

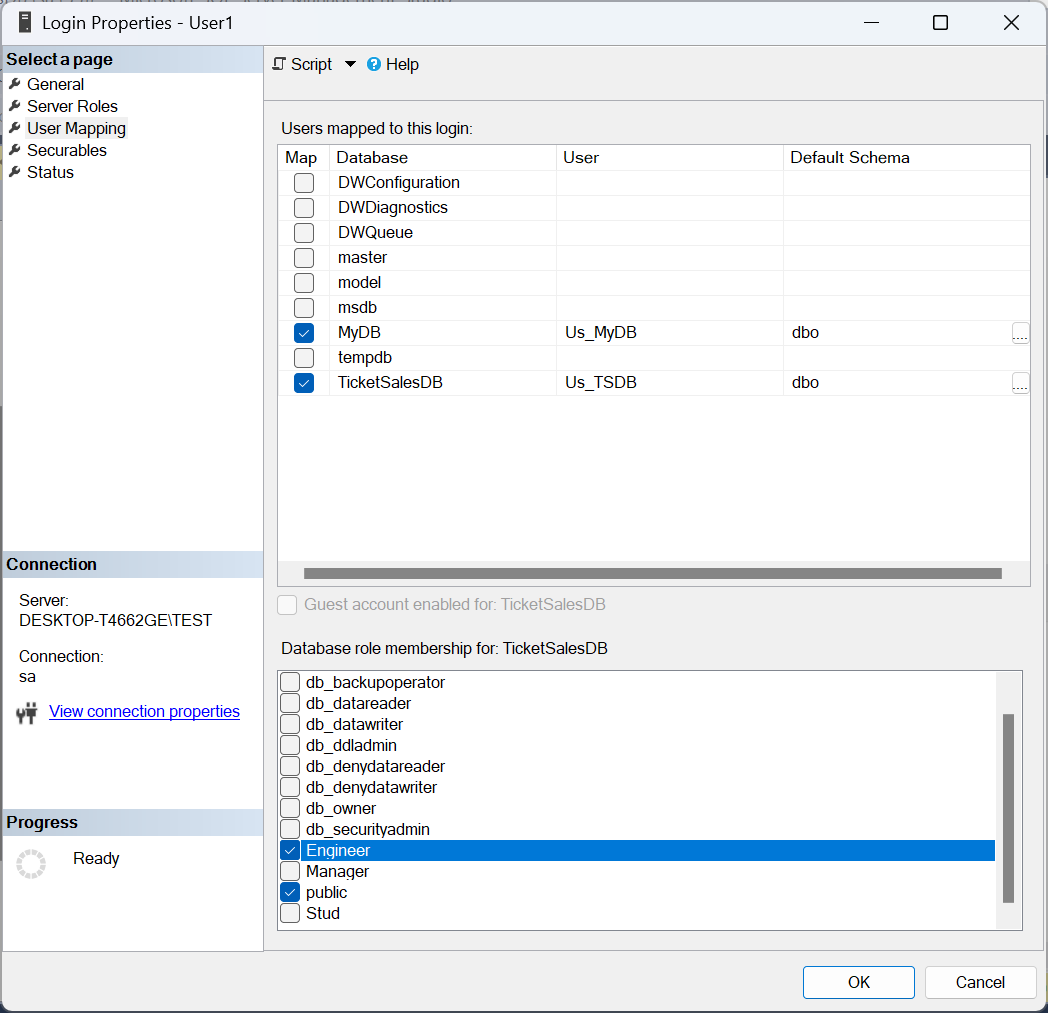
Обираємо БД, в ній переходимо до *Security* – *Roles* – *Database Roles*. Натискаємо правою кнопкою миші та обираємо *New Database Role*.



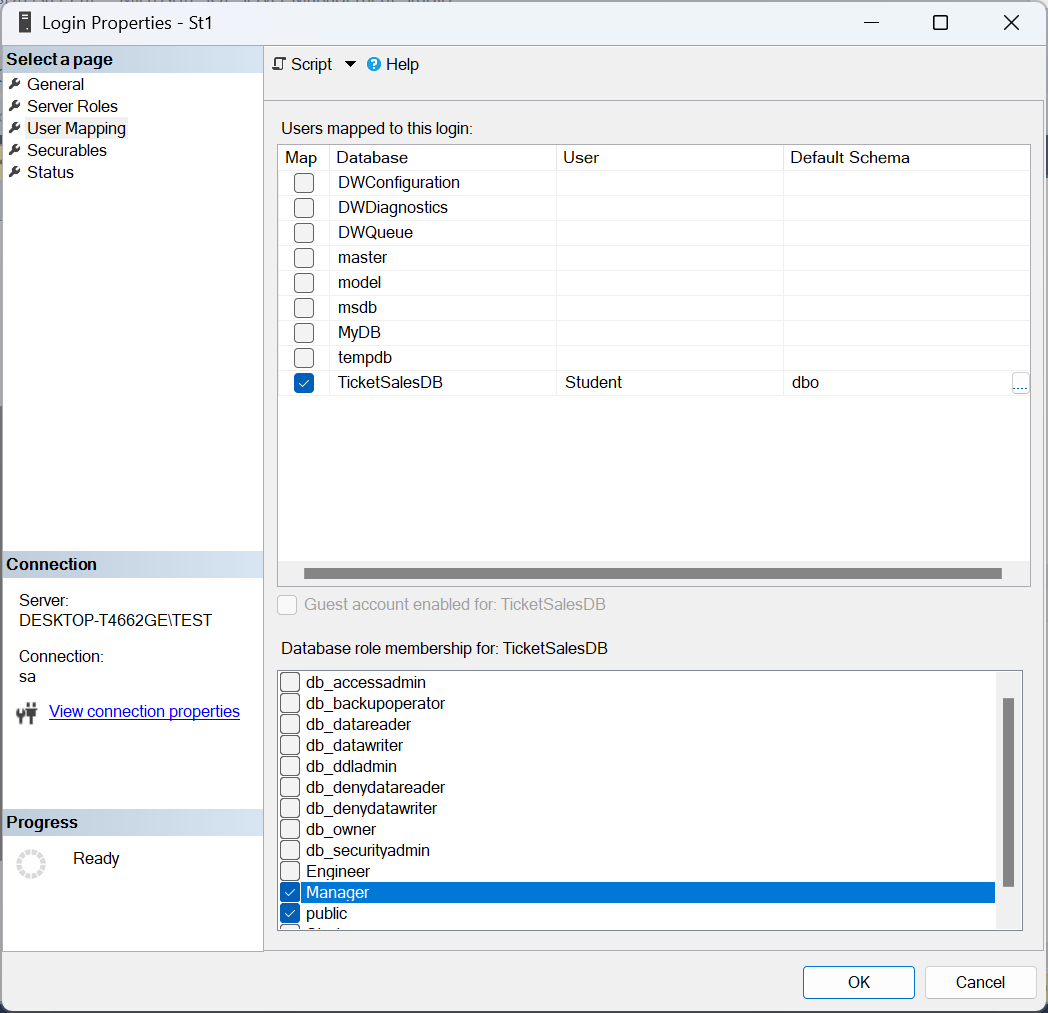
Створюємо роль для менеджера та розробника. Присвоюємо кожній ролі конкретні права: інженеру – *Select*, менеджеру – *Select*, *Alter*, *Delete*.

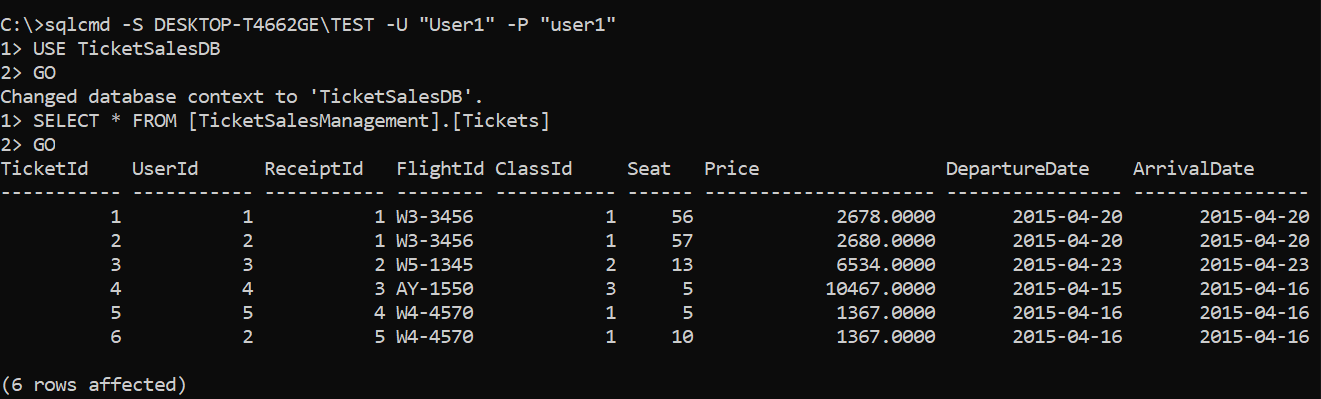
 

Присвоюємо конкретним користувачам конкретні ролі. Обираємо *User1* – *Properties* – *User Mapping*. Обираємо базу даних та ставимо прапорець навпроти Engineer.

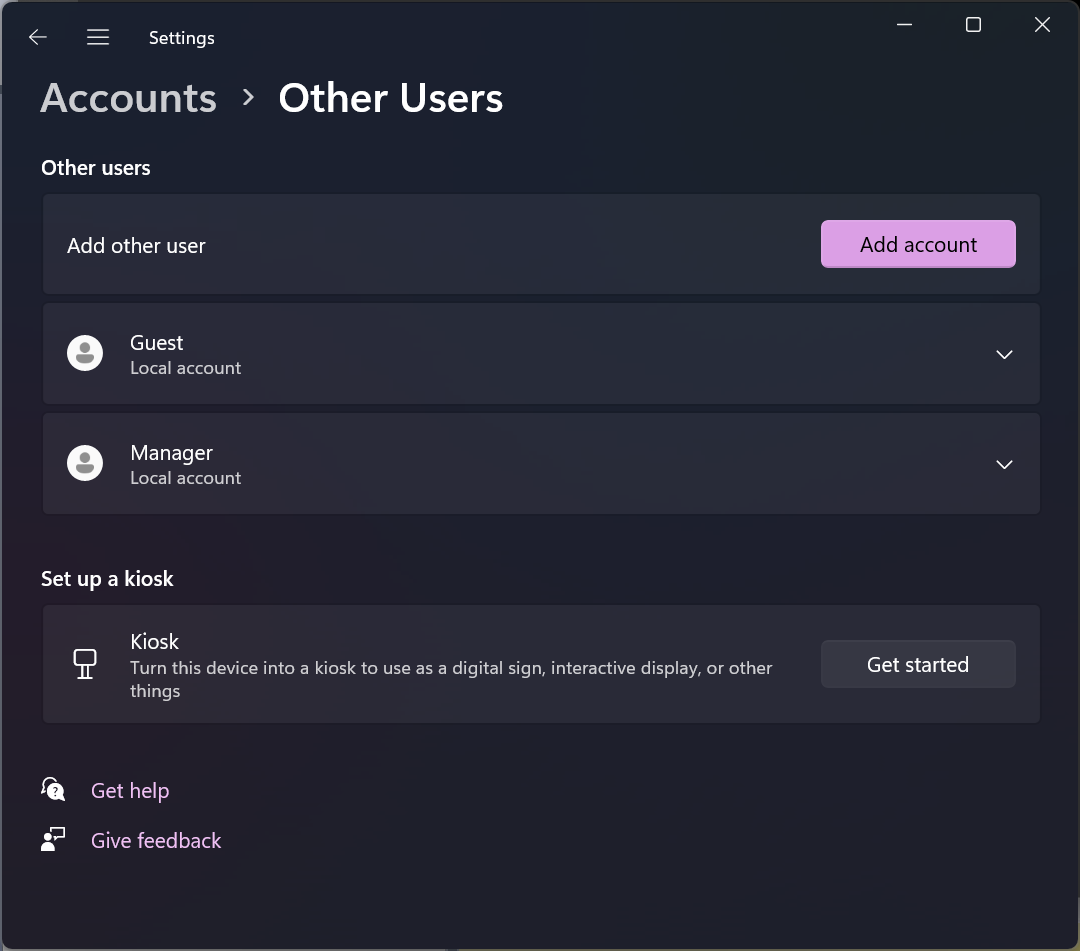


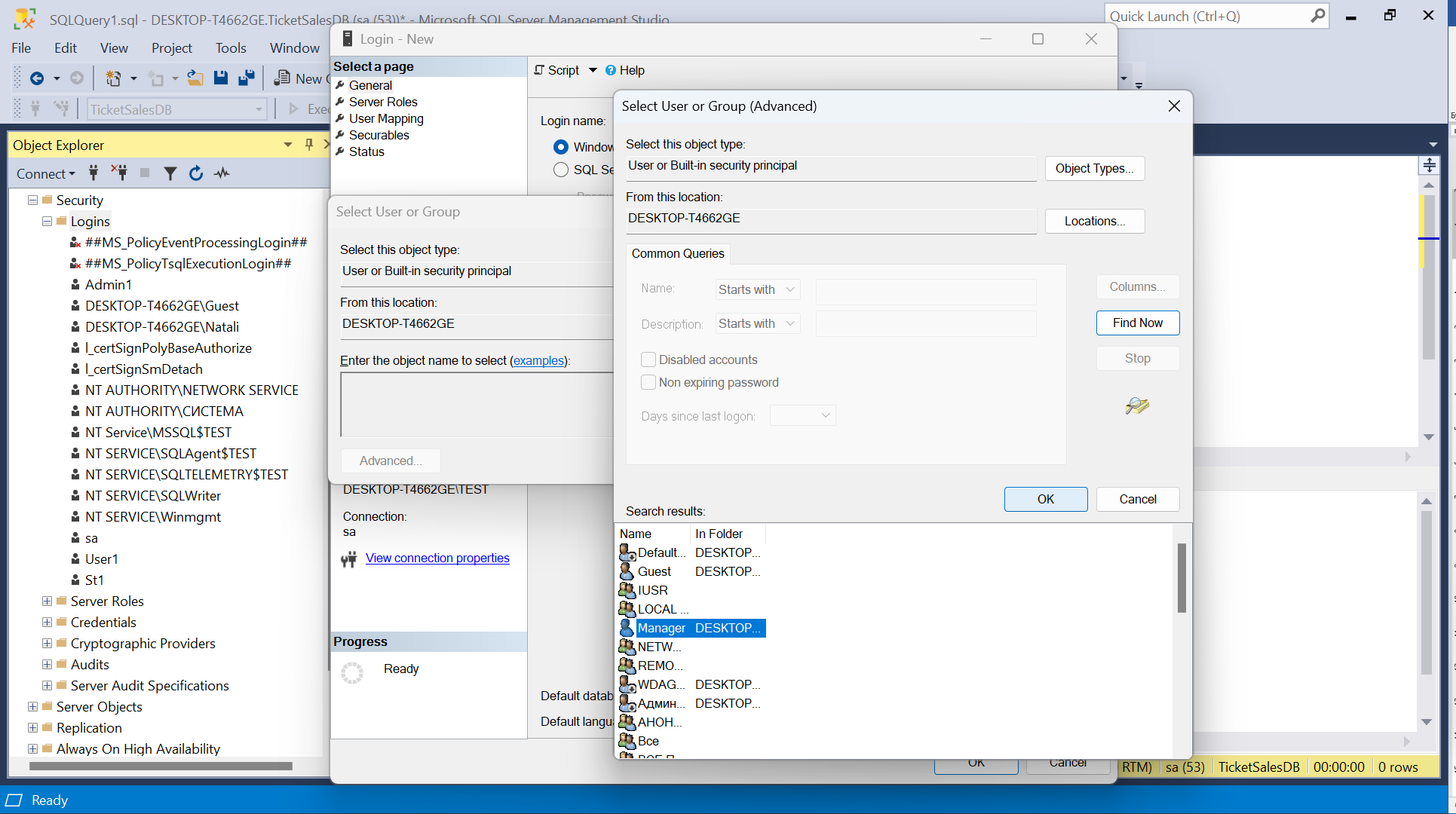
*St1* буде менеджером.

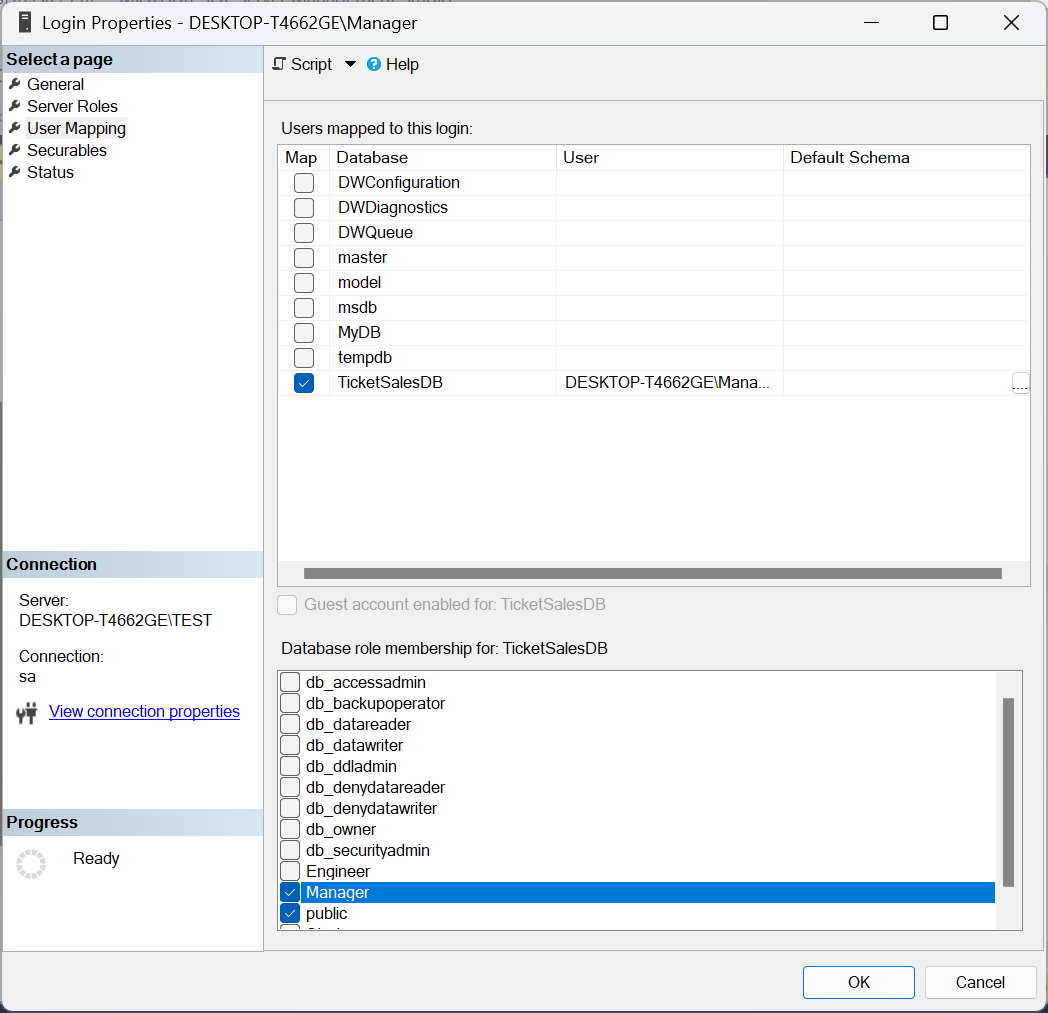
За допомогою cmd перевіряємо виконані дії. Заходимо як *User1*. Дозвіл у користувача *User1* використовувати команду *SELECT* є.



1. Створення локального користувача в обліковому записі Windows

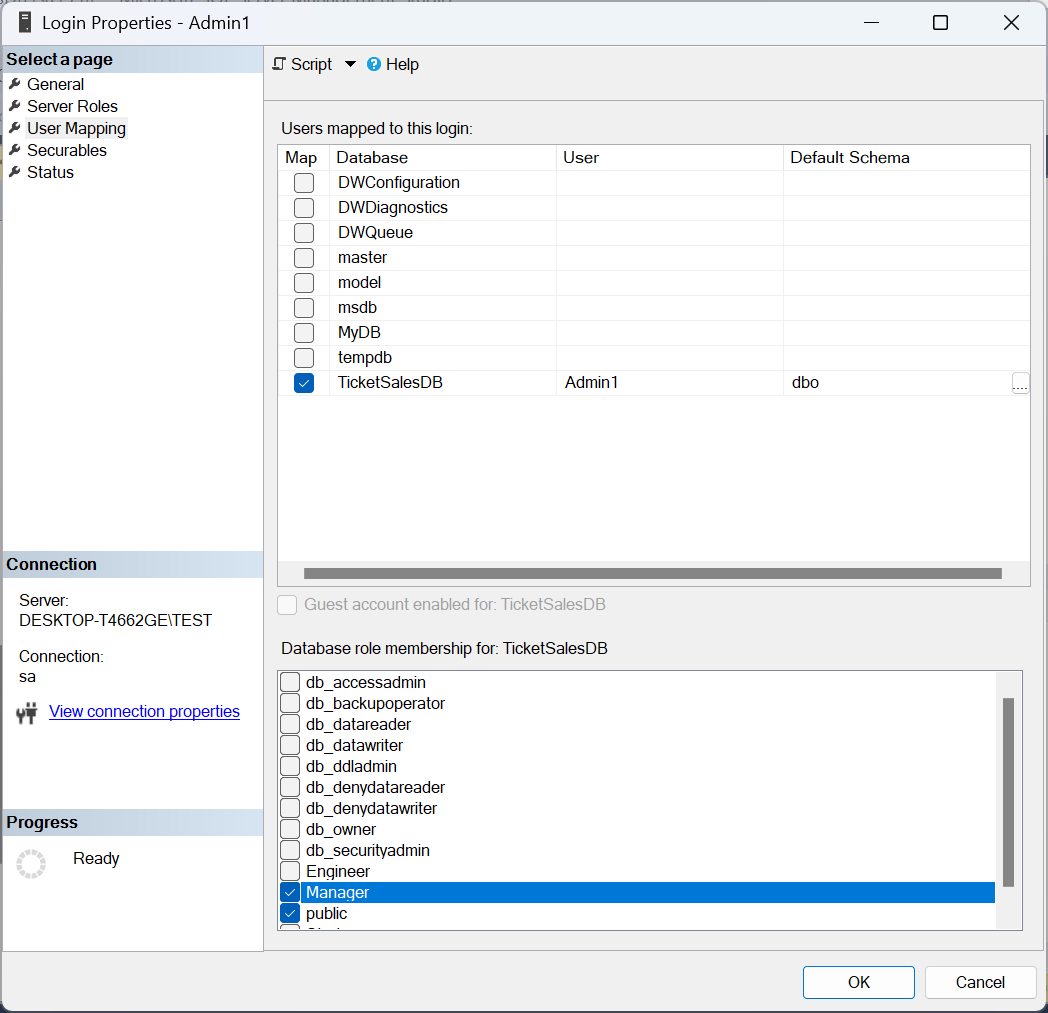




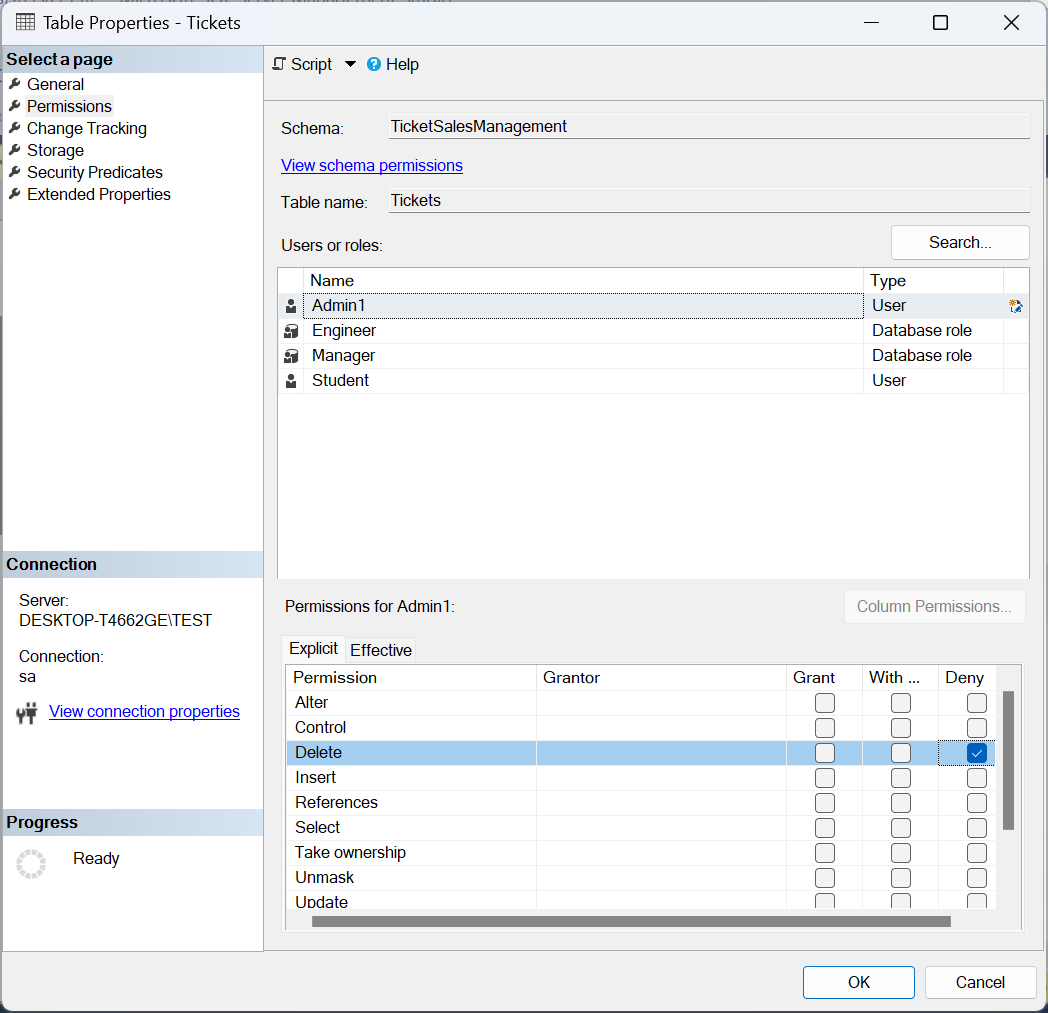


1. Створення явної заборони (Deny) за допомогою графічного інтерфейсу SSMS

Додамо до ролі менеджера користувача *Admin1*.

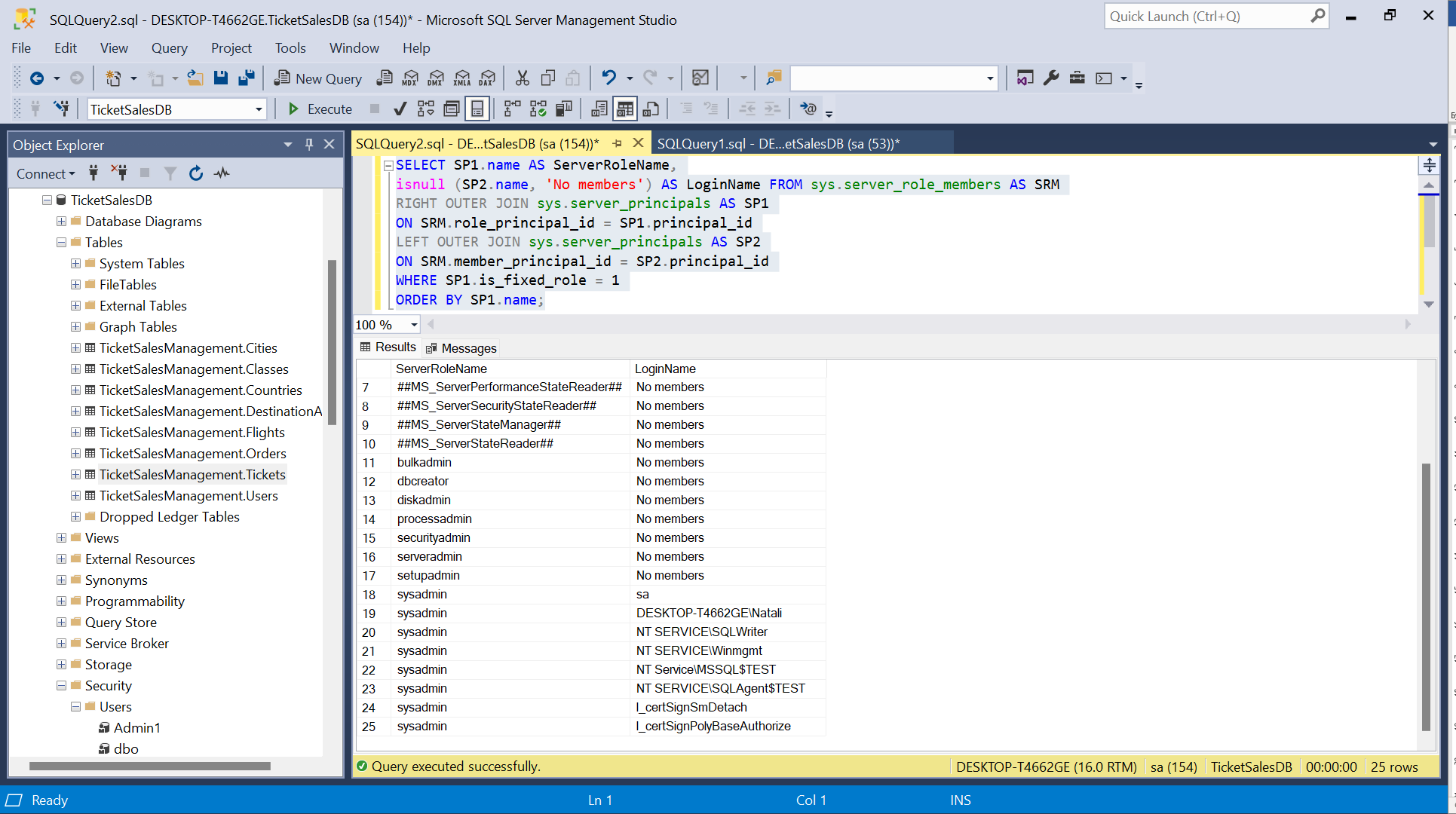


Заборонимо йому використання команди *Delete*. Відповідно всі менеджери зможуть використовувати цю команду, окрім одного.

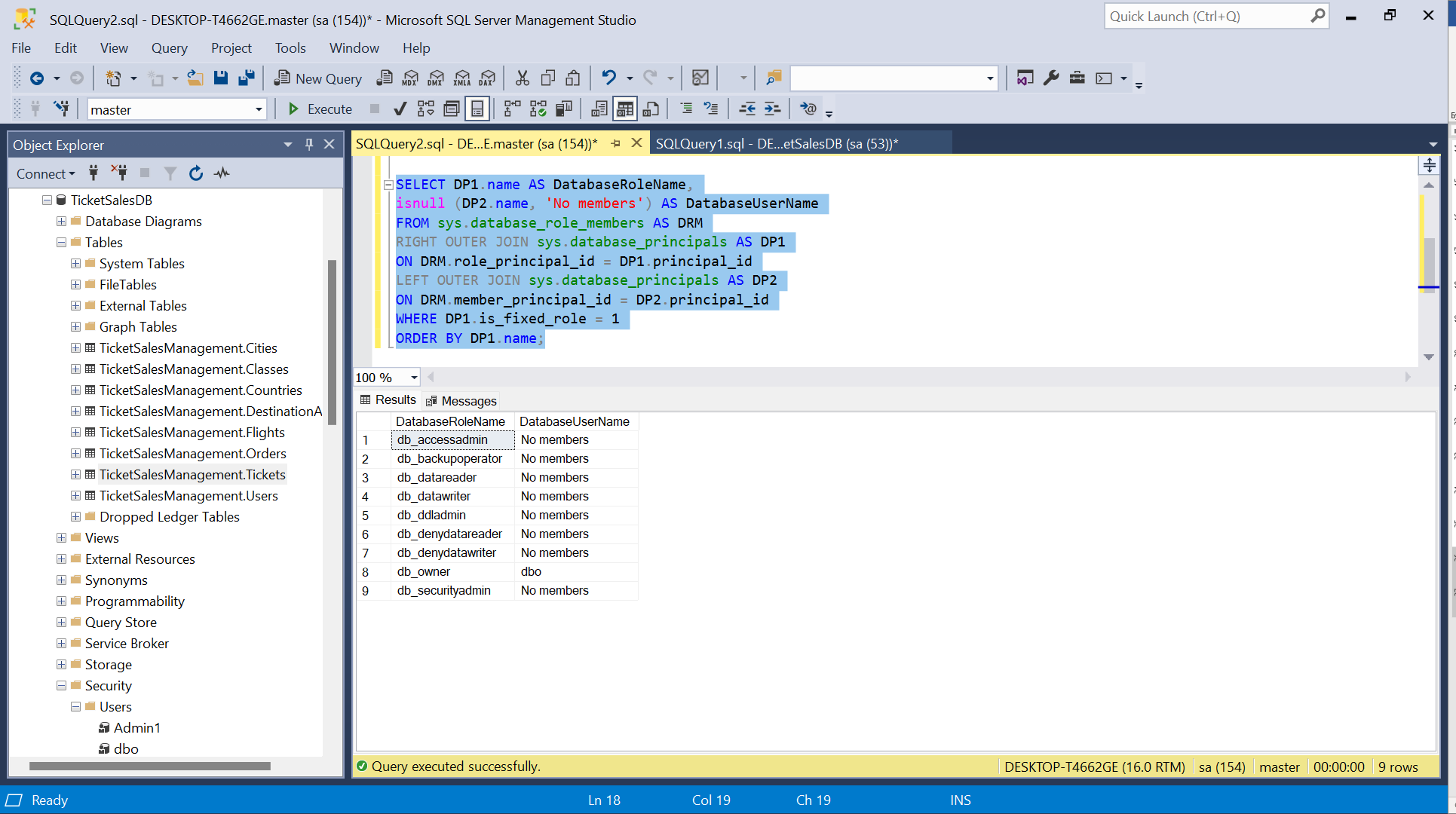


ЗАВДАННЯ НА САМОСТІЙНУ РОБОТУ

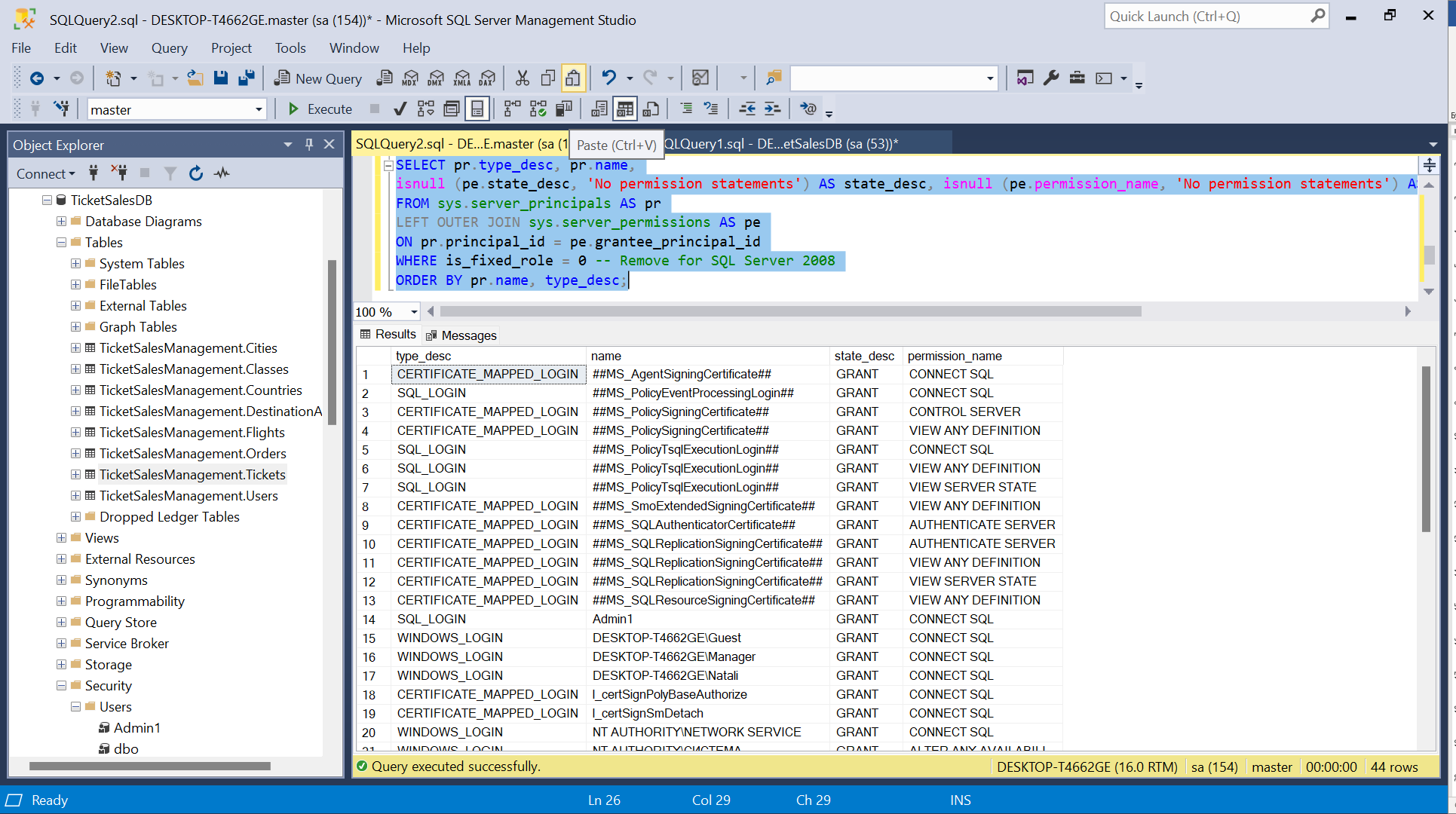
Виведемо інформацію про систему дозволів зумовленої ролі.



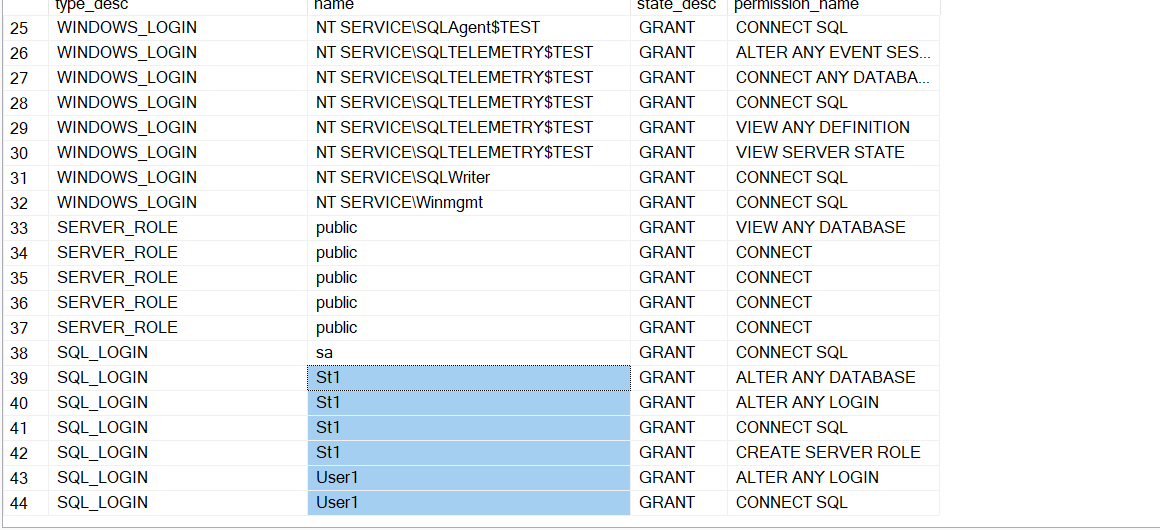
Визначимо учасників зумовленої ролі бази даних



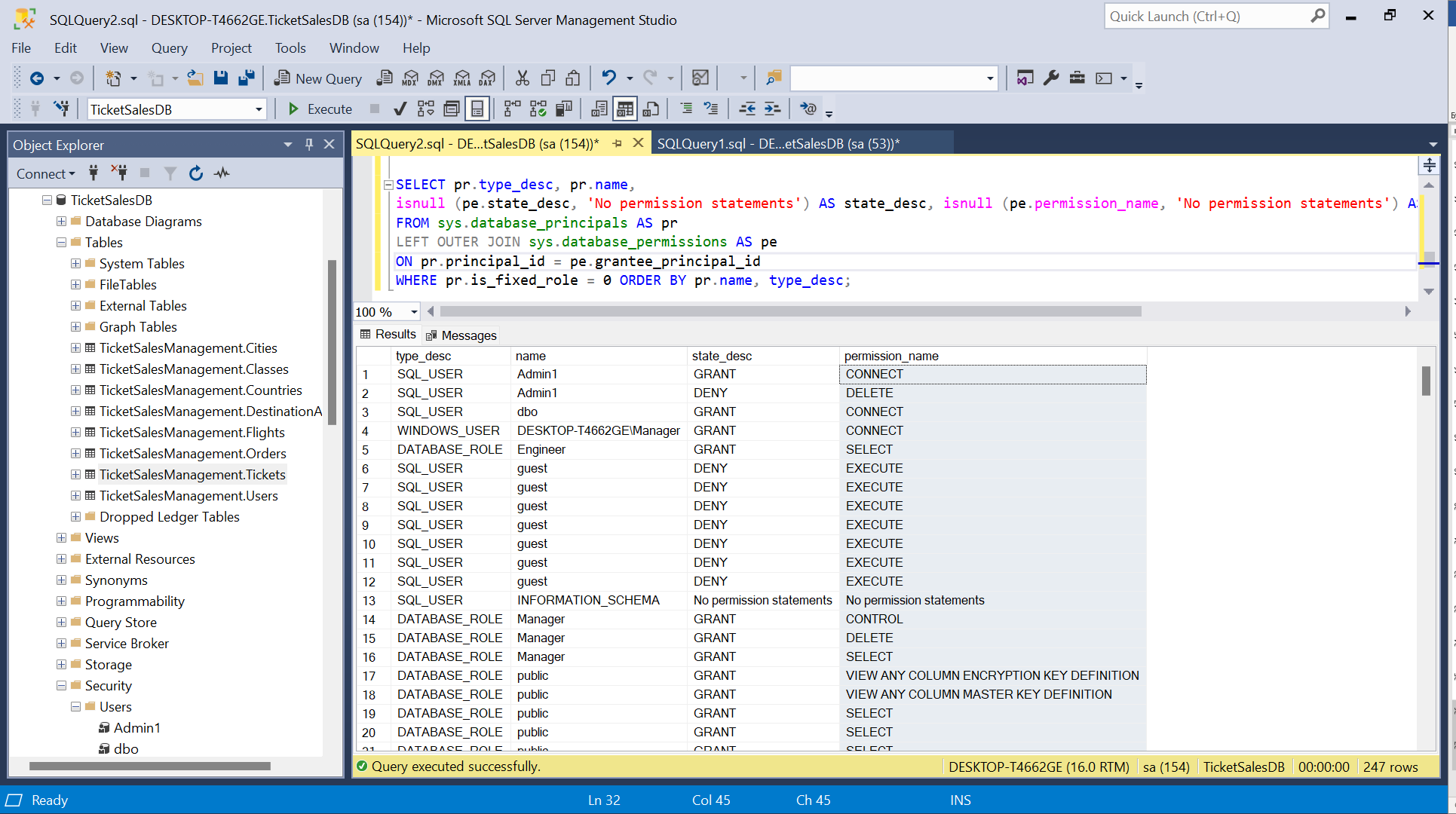
Виведемо на екран список дозволів, які надані або заборонені на рівні сервера.



Можемо побачити дозволи, які ми надавали власноруч, під час виконання лабораторної.



Виведемо список дозволів, які були надані або відхилені на рівні бази даних TicketSalesDB. Можемо знайти дозволи, які ми надали користувачам під час виконання лабораторної роботи, та інші.



Виведемо імена об’єкта бази даних TicketSalesDB, на якого поширюється дозвіл.



**Висновок:** під час виконання даної лабораторної роботи було набуто практичних навичок щодо встановлення режимів аутентифікації користувачів і об'єктів баз даних, особливостей авторизації користувачів та надання їм привілеїв.