УПРАВЛІННЯ ДОСТУПОМ ДО БАЗИ ДАНИХ

Лекція 9 Автор Голуб Б.Л.

Захист даних

- Несанкціонований доступ включає як доступ до даних користувачів, які мають певні обмеження щодо даних БД, так і дії, які спрямовані на недопущення несанкціонованого підключення до БД
- Захист даних у БД означає захист їх від несанкціонованого доступу
- Привілеї – це рівні повноважень, які надаються користувачеві під час доступу до БД і її об’єктам, під час маніпулювання даними і виконання різних адміністративних функцій
- Захист даних – це процес розподілення привілей для роботи у межах різних рівнів доступу, відміни привілей та прийняття мір по захисту різних даних, особливо, важливих файлів БД

Типи користувачів бази даних

- **Адміністратор бази даних.** Створює облікові записи користувачів, надає користувачеві привілеї, створює профілі для користувачів та, якщо це необхідно, видаляє їх.
- **Системний аналітик або системний адміністратор.** Відповідає за безпеку усієї обчислювальної системи, для чого і створюються облікові записи та розроблюється система привілей доступу.
- **Кінцеві користувачі.** Жоден користувач не може мати привілей доступу, які перевищують необхідні для його роботи. Головною причиною використання облікових записів користувачів та привілей є необхідність захисту даних.

Створення облікового запису

sp_addlogin [**@loginame =**] '***login***'

[**,** [**@passwd =**] '*password*']

[**,** [**@defdb =**] '*database*']

[**,** [**@deflanguage =**] '*language*']

[**,** [**@sid =**] *sid*]

[**,** [**@encryptopt =**] '*encryption_option*']

Створення користувача

sp_adduser [**@loginame** =] '***login***'
[, [**@name_in_db** =] '*user*']
[, [**@grpname** =] '*group*']

Сеанс роботи з БД

CONNECT TO

{

[server_name.]**database_name**

}

[AS connection_name]

USER [login[.password] | $integrated]

Приклад

EXEC SQL CONNECT TO gizmo.pubs USER sa;

Привілеї доступу до системи

Дають можливість користувачеві реалізовувати в межах БД адміністративні задачі, такі як створення та видалення БД, облікових записів користувачів, зміни стану об’єктів, зміни стану БД та інших подібних операцій

GRANT { *ALL* | *statement* [,...n] } TO security_account [,...n]

- **ALL** визначає, що надаються всі допустимі дозволи. У разі призначення привілеїв на рівні доступу до системи параметр ALL може використовуватися тільки для *sysadmin* ролі.
- **statement** – це оператор, для якого надається дозвіл. Список операторів може включати такі:

CREATE DATABASE CREATE DEFAULT CREATE FUNCTION CREATE PROCEDURE

CREATE RULE CREATE TABLE CREATE VIEW BACKUP DATABASE BACKUP LOG

- **n** означає, що одному користувачеві можуть надаватися декілька привілеїв, які розділяються комами.
- **TO** передує списку облікових записів.
- **n** означає, що привілеї можуть надаватися одразу декільком користувачам, назви яких відокремлюються комами.

Привілеї доступу до об’єктів

Такі привілеї – це рівні повноважень, які надаються користувачеві під час роботи з БД. Наприклад, щоби отримати дані із таблиці іншого користувача, необхідно спочатку отримати право доступу до його даних.

Надання привілеїв

```
grant
{ ALL [PRIVILEGES] | permission[,…n]}
{
        [(column[…..n])] ON {table | view}
        | ON {table | view} [(column [,…n])]
        | ON {stored_procedure | extended_procedure}
        | ON {user_defined_function}
}
TO security_account [,…n]
[WITH GRANT OPTION]
[AS {group | role}]
```

Параметри

- ALL визначає, що надаються всі допустимі дозволи. У разі призначення привілеїв на рівні доступу до об’єктів параметр ALL може використовуватися тільки для sysadmin та db_owner ролей.
- Permission визначає привілеї.

SELECT – дозволяє доступ до вказаної таблиці;

INSERT [(name_column)] – дозволяє розмістити дані у вказаному стовпці або у всі стовпці вказаної таблиці;

DELETE – дозволяє видаляти записи вказаної таблиці;

REFERENCES[(name_column)] – дозволяє посилатися в умовах цілісності на вказаний стовпець або на всі стовпці вказаної таблиці;

UPDATE [(name_column)] – дозволяє змінювати дані у вказаному стовпці або у всіх стовпцях вказаної таблиці.

- Привілеї можуть призначатися для таблиць, уявлень, збережених процедур, функцій.
- WITH GRANT OPTION означає, що власник об’єкта наділяє правами користувача самому надавати привілеї.
- AS { group | role } використовується для надання прав користувачеві, які не є членами групи або не мають вказаної ролі.

Відміна привілеїв

```
REVOKE [ GRANT OPTION FOR ]
    { ALL [ PRIVILEGES ] | permission [ ,...n ] }
    {
        [ ( column [ ,...n ] ) ] ON { table | view }
        | ON { table | view } [ ( column [ ,...n ] ) ]
        | ON { stored_procedure | extended_procedure }
        | ON { user_defined_function }
    }
{ TO | FROM }
    security_account [ ,...n ]
[ CASCADE ]
[ AS { group | role } ]
```

Спеціальні облікові записи

- **sa** (system administrator). Цей обліковий запис має абсолютні права щодо управління сервером. Програма установки включає цей запис у роль сервера *sysadmin*, надаючи йому таким чином ці права
- **BUILTIN\Administrators**. За допомогою цього облікового запису члени групи Windows Administrators домена, в якому встановлений локальний SQL Server, отримають права доступу до серверу. Обліковий запис BUILTIN\Administrators за замовченням включений до фіксованої ролі серверу, тобто адміністратори Windows за замовченням мають право на управління сервером.

Спеціальні користувачі

- **dbo** (database owner). Цей користувач БД є власником її. Власник БД має абсолютні права щодо управління нею. Користувача dbo неможливо видалити. За замовченням обліковий запис sa є відносно будь-якої БД користувачем dbo, що і дозволяє цьому обліковому запису отримати всі права на БД.
- **guest**. Всі права, що є у цього користувача, автоматично надаються всім обліковим записам, що створені на сервері, за умови, що цьому обліковому запису не наданий доступ до БД. Цей користувач може бути видалений, що рекомендується зробити з метою захисту інформації від несанкціонованого доступу.