Промышленные СУБД

Лабораторная работа №2

Лабораторная работа №2
Система безопасности Microsoft SQL Server

Цель: научить использовать системные хранимые процедуры для управления именами входа MS SQL Server и пользователями баз данных, а также разрешать и запрещать выполнение определенных действий некоторому пользователю.

Требования к отчету: по результатам работы представить отчёт со скриншотами, содержащими SQL-команды и результаты их выполнения для каждой задачи из раздела «Самостоятельная работа».

Задание 1. Подключитесь к серверу *SDB-SRV\DION* с помощью утилиты *Management Studio*.

Указания к выполнению:

1. Запустите *SQL Server Management Studio* через меню **Пуск –Программы – Microsoft SQL Server 2008**.
2. Выберите тип аутентификации: Windows *Authentication*. Укажите *User name*: Student, и *Password*: 123321123 и нажмите кнопку **Connect**.

Задание 2. Определите список ролей сервера.

Указания к выполнению:

1. Создайте новый запрос или через команду меню **File – New – Query with Current Connection** или при помощи кнопки **New Query** на панели инструментов.
2. Во вкладке *SQLQuery1.sql* выполните команду **sp_helpsrvrole** (см. рис. 1).

Results | Messages

	ServerRole	Description
1	sysadmin	System Administrators
2	securityadmin	Security Administrators
3	serveradmin	Server Administrators
4	setupadmin	Setup Administrators
5	processadmin	Process Administrators
6	diskadmin	Disk Administrators
7	dbcreator	Database Creators
8	bulkadmin	Bulk Insert Administrators

Рис. 1. Серверные роли MS SQL Server

Замечание. Для более наглядного представления данных используйте способ отображения информации в виде таблицы (кнопки **Results to Grid/Results to Text** на панели инструментов или через команды меню **Query – Results To**).

Задание 3. Создайте и настройте новую учетную запись *TempUser* для входа в SQL Server.

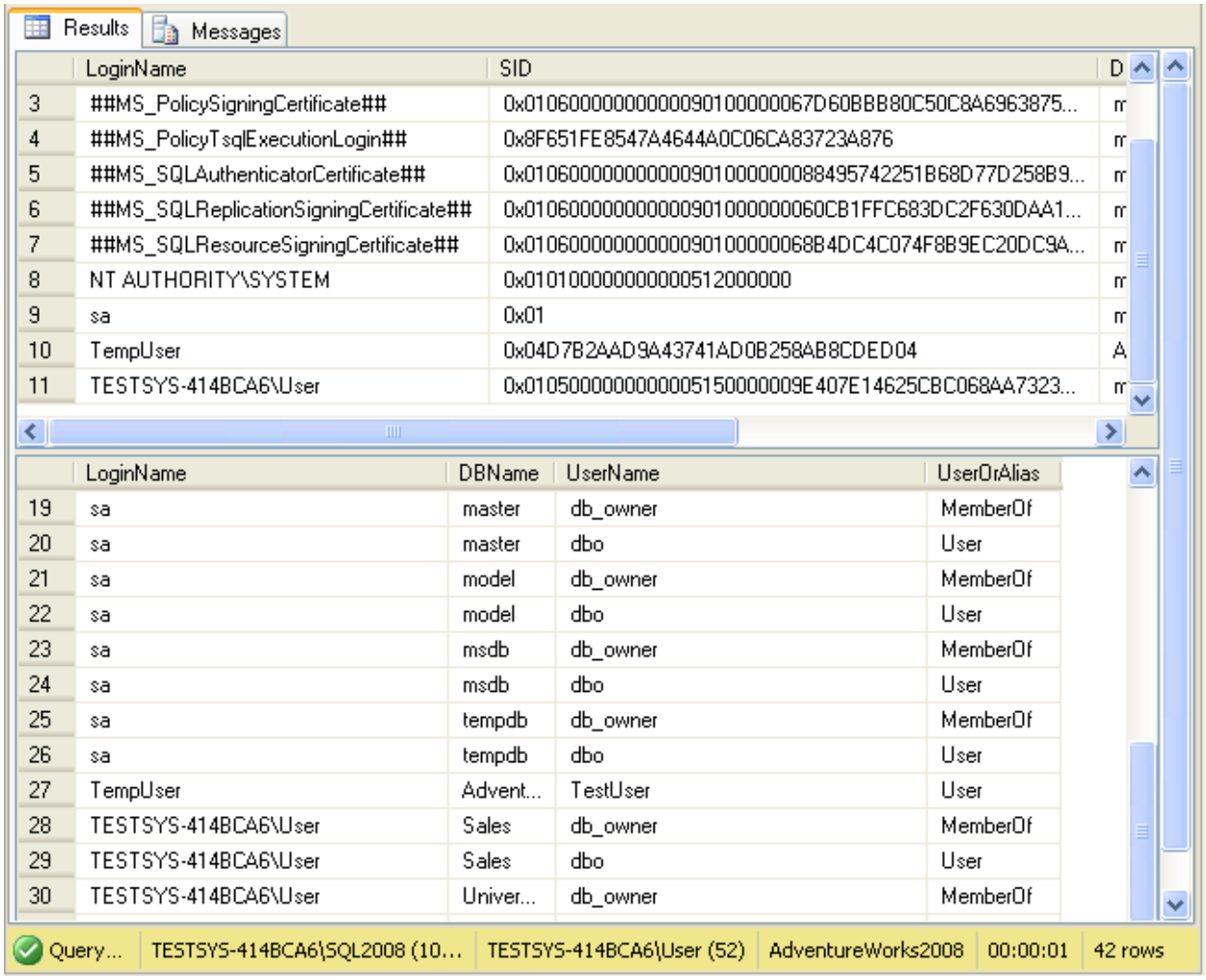
Указания к выполнению:

1. Для добавления учетной записи используйте хранимую процедуру **sp_addlogin:**

```
sp_addlogin 'TempUser', 'Password!'
```

Замечание. Для получения справки по командам Transact-SQL и хранимым процедурам можно воспользоваться утилитой *SQL Server Management Studio*. Для этого необходимо выделить имя оператора и нажать клавишу **F1**.

2. Убедитесь, что учетная запись была добавлена при помощи хранимой процедуры **sp_helplogins** (см. рис. 2).



Results | Messages

	LoginName	SID	D
3	##MS_PolicySigningCertificate##	0x010600000000000090100000067D60BBB80C50C8A6963875...	m
4	##MS_PolicyTsqlExecutionLogin##	0x8F651FE8547A4644A0C06CA83723A876	m
5	##MS_SQLAuthenticatorCertificate##	0x010600000000000090100000008849574225 1B68D77D258B9...	m
6	##MS_SQLReplicationSigningCertificate##	0x010600000000000090100000060CB1FFC683DC2F630DAA1...	m
7	##MS_SQLResourceSigningCertificate##	0x010600000000000090100000068B4DC4C074F8B9EC20DC9A...	m
8	NT AUTHORITY\SYSTEM	0x01010000000000512000000	m
9	sa	0x01	m
10	TempUser	0x04D7B2AAD9A43741AD0B258AB8CDED04	A
11	TESTSYS-414BCA6\User	0x010500000000000515000000 9E407E14625CBC068AA7323...	m

	LoginName	DBName	UserName	UserOrAlias
19	sa	master	db_owner	MemberOf
20	sa	master	dbo	User
21	sa	model	db_owner	MemberOf
22	sa	model	dbo	User
23	sa	msdb	db_owner	MemberOf
24	sa	msdb	dbo	User
25	sa	tempdb	db_owner	MemberOf
26	sa	tempdb	dbo	User
27	TempUser	Advent...	TestUser	User
28	TESTSYS-414BCA6\User	Sales	db_owner	MemberOf
29	TESTSYS-414BCA6\User	Sales	dbo	User
30	TESTSYS-414BCA6\User	Univer...	db_owner	MemberOf

Query... | TESTSYS-414BCA6\SQL2008 (10... | TESTSYS-414BCA6\User (52) | AdventureWorks2008 | 00:00:01 | 42 rows

Рис. 2. Список имен пользователей MS SQL Server

3. Попробуйте войти на сервер под созданной учетной записью.
4. Зайдите снова под учетной записью **sa**, т.к. для дальнейших действий снова потребуются права администратора.
5. Для присвоения учетной записи для входа встроенной серверной роли используется процедура:

sp_addsrvrolemember ‘TempUser’, ‘securityadmin’

Задание 4. Определите список ролей базы данных и членов роли *db_owner*.

Указания к выполнению:

1. Выполните хранимую процедуру **sp_helprole** для получения списка как встроенных, так и определенных пользователем ролей базы данных.

2. При помощи команды **sp_helprolemember ‘db_owner’** определите членов роли *db_owner* (см. рис. 3).

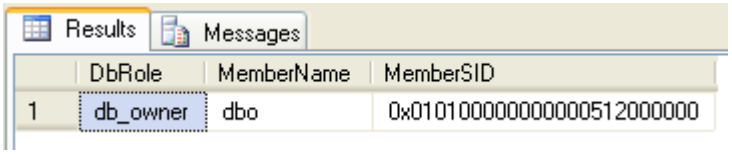


Рис. 3. Список членов роли *db_owner*

Задание 5. Создайте нового пользователя базы данных для логина *TempUser*.

Указания к выполнению:

1. При помощи хранимой процедуры добавьте пользователя:

```
sp_adduser 'TempUser', ‘MyFirstUser’
```

2. При помощи процедуры **sp_helpuser** убедитесь, что пользователь был добавлен. Какая роль ему была присвоена?
3. Добавьте пользователю роль *db_datareader:*

```
sp_addrolemember 'db_datareader, ‘MyFirstUser’
```

Задание 6. Настройте права доступа пользователю *Andy*: предоставьте явным образом право только для выборки из таблицы *Product* и обновления только полей *Name* и *ListPrice* этой таблицы.

Указания к выполнению:

1. С помощью следующей команды пользователю *TestUser* базы данных ***AdventureWorks2008*** предоставляются права выборки и изменения данных таблицы *Orders* этой базы данных:

```
GRANT select, update on AdventureWorks2008.Production.WorkOrder to TestUser
```

2. Следующая команда предоставляет пользователю *Andy* права только выборки данных полей *Name* и *ListPrice* таблицы *Product* базы данных ***AdventureWorks2008:***

```
GRANT select on AdventureWorks2008.Production.Product (Name, ListPrice) to Andy
```

Задание 7. Изучите выполнение вышеупомянутых функций при помощи графического интерфейса утилиты *Management Studio*.

Указания к выполнению:

1. Просмотр списка имеющихся учетных записей и их параметров осуществляется выбором группы *Logins* в папке **Security** сервера.

2. Для создания новой учетной записи для входа необходимо выполнить команду **New Login…** контекстного меню узла **Logins,** в появившемся диалоговом окне указать:

- вкладка *General*: имя пользователя, тип аутентификации (при аутентификации средствами MS SQL Server – задать пароль), базу данных, к которой пользователь подключается автоматически, язык по умолчанию;
- вкладка *Server Roles*: роли сервера, в которые будет входить создаваемая учетная запись;
- вкладка *User Mapping*: доступ к одной из созданных на сервере базе данных, в поле *User* ввести имя пользователя базы данных и включить создаваемого пользователя в одну существующих ролей.

Замечание. Для изменения параметров существующей учетной записи пользователя для входа необходимо выбрать ее из списка и выполнить команду контекстного меню **Properties**, для удаления – **Delete.**

3. Для отображения списка ролей сервера необходимо выбрать группу *Server Roles* в папке **Security** сервера. Просмотр пользователей, входящих в эту роль и разрешений, присвоенный ей, осуществляется выполнением команды контекстного меню **Свойства.**

Замечание. Встроенные роли сервера не могут быть удалены из системы, и нельзя изменить определенные для них разрешения. Также запрещено создавать и собственные серверные роли.

4. Для просмотра и управления параметрами пользователей некоторой базы данных предназначена группа *Security/Users* этой базы. Учетные записи отображаются в поле *User Name,* а в поле *Login Name* – соответствующие им учетные записи для входа.

Для создания нового пользователя базы данных необходимо выполнить команду **New User…,** затем в поле *User name* ввести имя пользователя, а в списке *Login Name* выбрать соответствующую учетную запись для входа. Можно также включить пользователя в роли базы данных.

Замечание. Для изменения параметров учетной записи служит команда

Properties, а для удаления – **Delete.**

5. Для отображения списка ролей базы данных используется группа *Roles*. Для просмотра пользователей, входящих в эту группу, необходимо выполнить команду **Properties.**

6. Чтобы назначить полномочия объекту безопасности необходимо выбрать его в группе *Users* (для изменения разрешения конкретного пользователя базы данных) или в группе *Roles* (для разрешений определенной роли). Для этих целей используется вкладка **Securables**.

В появившейся вкладке перечислены все объекты базы данных, с возможными правами доступа. Можно установить одно из трех состояний доступа: *предоставление* (галочка), *запрещение* (крестик) и *неявное отклонение* (пустое поле) – в соответствующем поле.

Задание 8. Отмените присвоение роли учетной записи и удалите учетную запись *TempUser*.

Указания к выполнению:

1. Отмена присвоенной пользователю роли может быть выполнена с помощью процедуры:

```
sp_droprolemember ‘db_datareader’, ‘MyFirstUser’
```

2. Для удаления пользователя БД используются процедуры:

```
sp_dropuser ‘MyFirstUser’
```

3. Отмена присвоения учетной записи определенной роли выполняется с помощью хранимой процедуры:

```
sp_dropsrvrolemember 'TempUser', ‘securityadmin’
```

4. Для удаления учетной записи выполните хранимую процедуру:

```
sp_droplogin 'TempUser'
```

Самостоятельная работа

1. Определите список всех ролей сервера и действия, разрешенные пользователям роли *dbcreator*.

2. Установите, какая серверная роль присвоена системной учетной записи ***sa***.

3. Определите, пользователь какой роли имеет возможность создания и удаления учетных записей для входа.

4. Изменение пароля учетной записи пользователя для входа выполняется с помощью процедуры *sp_password*.

5. Создайте собственную учетную запись для входа с подключением к вашей базе данных, докажите правильность выполненных действий. Созданной учетной записи присвойте права на создание и изменение баз данных, докажите правильность выполненных действий. Подключитесь к MS SQL Server, используя созданную учетную запись, и создайте еще одну учетную запись пользователя для входа, результат объясните.

6. Создайте пользователя *Admin* и присвойте ему роль, обладающую полным доступом к базе данных.

7. Создайте пользователя *User* и присвойте ему роль, обладающую доступом к базе данных только для чтения.

8. Пользователю *manager* присвойте роль, обладающую только возможностью просмотра содержимого вашей базы данных.

Замечание. Для проверки правильности выполненных действий можно выполнить произвольный запрос к этой базе данных, например, отображающий содержимое таблицы *таблицца1(пример)*:

```
SELECT * FROM таблица1.
```

9. Пользователю *manager* запретите просмотр данных БД, присвоив необходимую роль. Как доказать правильность внесенных изменений?

10. Какое количество пользователей базы данных может быть создано на основе одной учетной записи пользователя для входа? Ответ обоснуйте.

11. Средствами *SQL Server Management Studio* создайте учетную запись пользователя для входа на основе аутентификации SQL, подключающегося по умолчанию к вашей базе данных, имеющего права серверной роли *diskadmin*.

12. Определите список пользователей, входящих в роль *diskadmin* и ее разрешения.

13. В базе данных создайте пользователя на основе созданной ранее учетной записи для входа.

14. Для созданного ранее пользователя базы данных определите, членом какой роли он является и каково ее назначение. Имеет ли данный пользователь право выборки данных из *таблицы1* этой базы данных? Ответ обоснуйте и проверьте, выполнив извлечение данных командой SELECT * *from таблица1(пример)*.

15. В базе данных создайте роль *managers*. Для этой роли определите право выборки данных из таблицы *таблица1* базы данных. Присвойте роль *managers* созданному ранее пользователю. Имеет ли теперь этот пользователь право выборки данных? Проверьте сделанный вывод. К каким еще объектам базы данных имеет право доступа этот пользователь? Обоснуйте и проверьте вывод.

16. Создайте пользователя, имеющего доступ к вашей базе данных и принадлежащего роли *clerks*. Для этой роли определите возможность выборки данных из таблицы *таблица2* только для определенных полей, например полей *Имя* и *Количество*. Для проверки правильности выполненных действий выполните команды:

- SELECT * *from Таблица1* – чтение данных из всех полей таблицы *Authors*;
- SELECT *Имя, Количество from Таблица1* – чтение данных таблицы *Таблица1* только из указанных полей.

17. Для роли *clerks* запрещена выборка данных из таблицы *Таблица1* базы данных. Пользователь *Andy* принадлежит пользовательской роли *clerks* и системной роли *db_datareader*. Может ли этот пользователь получить данные из этой таблицы?