**Дәріс 10**

 **Тақырыбы: Серверлер және деректер қорының рольдері. Деректер қоры мен нысандарының құқықтарын тағайындау.**

**Жоспар:**

**10.1 Қауіпсіздік жүйесін администрациялау**

**10.2 MS SQL Server ортасында деректер қорының объектілеріне жету құқығы**

 **Мақсаты:** Серверлер және деректер қорына привилегиялар беру, рольдерді тағайындау. Деректер қоры мен нысандарының құқықтарын білу.

**Негізгі түсініктер: привилегия, сервер және деректер қорының рольдері, нысандар құқығы.**

Негізгі әдебиет: [1-5]

Қосымша әдебиет: [6-7]

**10.1 Қауіпсіздік жүйесін администрациялау**

MS SQL Server ортасында қолданушыны құру үшін келесідей қадамдар жасау керек:

1. Деректер қорында қолданушыны тіркеу керек, ол үшін оған пароль беру керек және үнсіздікпен тұрған деректер қорының атын алу керек (**sp\_addlogin процедурасы**).
2. Осы қолданушыны барлық қажет деген деректер қорына қосу керек (**sp\_adduser процедурасы**).
3. Оған әрбір деректер қорында сәйкес привилегиясын беру керек (**GRANT бұйрығы**).

Жаңа тіркеу жазбасын құру жүйелік сақталатын процедура көмегімен іске асады:

**Sp\_addlogin [@login=] ‘тіркеу\_жазбасы’**

 **[, [@password=] ‘пароль’ ]**

 **[, [@defdb= ] ‘үнсіздікпен\_алынған\_деректер\_қоры’ ]**

Аутентификация аяқталғаннан кейін және тіркеу жазбасының идентификаторын (login ID) алғаннан кейін қолданушы тіркелген деп есептеледі және оған серверге жол ашылады. Әрбір деректер қоры үшін, оның объектілеріне енуге рұқсат алуда, қолданушының тіркеу жазбасы (login) нақты деректер қоры үшін қолданушымен (user) ассоциациаланады да келесі процедурамен жүзеге асады:

**Sp\_adduser [@loginame=] ‘тіркеу\_жазбасы’**

 **[, [@name\_in\_db=] ‘қолданушы\_аты’ ]**

 **[, ]@grpname= ] ‘рөл\_аты’ ]**

Windows NT –дің тіркеу жазбасын қолданушының атында бейнелеу үшін сақталатын процедура қолданылады:

**Sp\_grantdbaccess [@login=] ‘тіркеу\_жазбасы’**

 **[, [@name\_in\_db=] ‘қолданушы\_аты’ ]**

Деректер қорын құрушы (кестелер, сақталатын процедуралар, көрсетулер) оның иесі болады. Объектінің иесі (database object owner dbo) өзі құрған барлық объектілерге енуіне құқығы болады. Қолданушы объект құру үшін деректер қорының (.dbo) иесі оған сәйкес құқық беруі керек. Құрылатын объектінің толық атында оны құрушының аты көрсетілуі керек.

Объектінің иесінің арнайы паролі немесе ену құқығы болмайды. Ол анықталмаған түрде толық ену құқығына ие, тек ол қолданушылардың анық енуін беруі керек.

SQL Server төмендегідей процедура арқылы иелену құқығын басқаға бере алады:

**Sp\_changeobjectowner [@objname=] ‘объект\_аты’**

 **[@newowner=] ‘иесінің\_аты’**

Бірдей функцияларды орындайтын қолданушылар тобын біріктіру үші рөл қолданылады.

SQL Server – де стандартты екі рөл жүзеге асырылады:

* сервер деңгейінде;
* деректер қоры деңгейінде.

SQL Server – ді орнату кезінде сервердің фиксирленген рөлдері құрылады (мысалы, SQL Server – дің кез келген функциясын орындайтын құқығы бар **sysadmin рөлі**) және деректер қорының фиксирленген рөлдері (мысалы, деректер қорына толық енуге құқықты **db\_owner рөлі** немесе қолданушыларды қосып-алатын **db\_accessadmin рөлі**). Деректер қорының рөлдерінің ішінде **public рөлінің** өзіндік қолданысы бар, деректер қорына енуге рұқсаты бар барлық қолданушылар оның мүшесі бола алады.

Кез келген SQL Server - дің тіркеу жазбасын (login) немесе Windows – тің тіркеу жазбасын сервердің кез келген рөліне енгізуге болады.

Деректер қорының рөлдері қолданушыларды бір администрациялық бірлікке біріктіреді және онымен кәдімгі қолданушы ретінде жұмыс істеуге мүмкіншілік береді. Нақты бір рөлге деректер қорының объектілеріне жетуіне құқық беруге болады, бұл рөлдің барлық мүшелері аутоматты түрде бірдей құқыққа ие болады.

Деректер қорына SQL Server – ді, SQL Server – дің рөлдерін, Windows-тың қолданушыларын қосуға болады.

Рөлге байланысты әртүрлі іс-амалдар арнайы процедуралар арқылы жүзеге асады:

• жаңа рөлді құру:

**sp\_addrole [@rolename=] ‘рөл\_аты’**

 **[, [@owername= ] ‘қолданушы\_аты’ ]**

• рөлге қолданушыны қосу:

**sp\_addrolemember [@rolename=] ‘рөл\_аты’,**

 **[ @membername=] ‘қолданушы\_аты’**

• рөлден қолданушыны алып тастау:

**sp\_droprolemember [@rolename=] ‘рөл\_аты’,**

 **[ @membername=] ‘қолданушы\_аты’**

• рөлді жою:

**sp\_droprole [@rolename=] ‘рөл\_аты’**

**10** Брандмауер қызметі.**.2 MS SQL Server ортасында деректер қорының объектілеріне жету құқығы**

ДҚБЖ-де сәйкес рұқсаттары бар ғана қолданушыларды деректер қорымен жұмыс істеуге мүмкіншілік беретін механизм бар. SQLтіліндедеректер қорын қорғауды ұйымдастыратын **GRANT** және **REVOKE** атты екі оператор бар.Қорғау механизмі қолданушы идентификаторына, оған берілетін құқыққа және привилегияға байланысты құрылады.

Қолданушы идентификаторы деп - деректер қорын қолданушыны белгілеуге қолданылатын SQLтілінің кәдімгі идентификаторын айтады. Әрбір қолданушының администратор беретін өзіндік жеке идентификаторы болады. Қауіпсіздік түсінігіне байланысты қолданушы идентификаторы кейбір парольмен байланыстырылады. Қолданушы идентификаторы қандай деректер қорына сүйене алатынын және қандай амалдар орындай алатынына құқығы барлығын анықтайды.

Әрбір құрылған объекттің оның барлығын білетін және онымен амалдар қолдана алуға құқығы бар жалғыз иесі болады.

Привилегия немесе құқық деп – қолданушының сол деректер қорының кестелерімен немесе көрсетулеріне байланысты жұмыс істеуге құқығы бар амалдарды айтады.

**Құқық категориялары**

SQL Server-ге қосылудағы қолданушының барлық іс-әрекеттері тіркеу жазбасында, рөлде берілген құқықтармен (привилегиялармен, рұқсаттармен) анықталады.

Құқықты үш категорияға бөлуге болады:

* объектілерге енуге болатын құқық;
* бұйрықтарды орындайтын құқық;
* ашық емес құқық.

*Тұжырым:* MS SQL Server ортасында деректер қорының объектілеріне жету құқығы және MS SQL Server ортасында қолданушыларды басқару

Бақылау сұрақтары:

1. MS SQL Server ортасында қолданушыларды басқару.

2. Аутентификация режимдері. Қауіпсіздік жүйесін администрациялау туралы айтыңыз.

3. MS SQL Server ортасында деректер қорының объектілеріне жету құқығы қалай жүзеге асырылады.

4. Құқық категориялары. Құқықты беру. Деректерге енудегі конфликтер туралы айтыңыз.