Частное учреждение образования
«Колледж бизнеса и права»

УТВЕРЖДАЮ
Ведущий методист
колледжа
_____ Е.В. Паскал
«___»_____2022

Специальность: «Программное обеспечение информационных технологий»	Учебная дисциплина: «Базы данных и системы управления базами данных»

ЛАБОРАТОРНАЯ РАБОТА № 27

Инструкционно-технологическая карта

Тема: Исследование системы безопасности Microsoft SQL Server.
Цель работы: научиться организовывать сохранность данных в Microsoft SQL Server.
Время выполнения: 2 часа

Содержание работы

1. Теоретические сведения для выполнения работы
2. Порядок выполнения работы
3. Пример выполнения работы
4. Контрольные вопросы
5. Литература

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

Система хранения информации должна быть максимально защищена как от случайного, так и от злонамеренного повреждения, искажения или утечки информации. С этой целью, прежде всего, надо определить круг пользователей, которые будут иметь доступ к базам данных. Далее, для этих пользователей необходимо создать учетные записи в домене Windows, а также в соответствующем экземпляре сервера SQL Server, чтобы разрешить им обращаться к этому серверу. Разрешение доступа к серверу не дает автоматически доступа к его базам данных и их объектам.

Второй этап планирования безопасности использования баз данных сервера заключается в определении действий, который может выполнить конкретный пользователь. Полный доступ к базам данных и всем их объектам имеет администратор – ему позволено все. Второе лицо после администратора – это владелец объекта. При создании любого объекта в любой базе данных ему назначается владелец, который может устанавливать права доступа к этому объекту, моди-

фицировать и удалять его. Все остальные пользователи, составляющую третью, основную группу, имеют права доступа, выданные администратором или владельцем объекта. Эти права должны быть тщательно спланированы в соответствии с занимаемой должностью и необходимостью выполнения конкретных действий.

Для работы с базами данных пользователи любой категории проходят следующие два этапа проверки системой безопасности. На первом этапе пользователь идентифицируется по имени учетной записи и паролю, т. е. проходит аутентификацию. Если данные введены правильно, то пользователь подключается к требуемому серверу, выбрав его из списка серверов и исполнив команду подключения либо с помощью Enterprise Manager, либо исполнив команды Transact –SQL в Query Analyzer. Пользователю при этом будут предоставлены те права доступа к серверу, которые имеют роль сервера, содержащая данного пользователя. Подключение к выбранному серверу, или регистрация, не дает автоматического доступа к базам данных.

На втором этапе по регистрационному имени находится имя пользователя базы данных, которое было создано администратором, и пользователь получает права доступа к выбираемой базе данных в соответствии с той ролью базы данных, в которую был включен этот пользователь администратором базы на этапе конфигурирования системы без опасности. В разных базах данных один и тот же пользователь может иметь одинаковые или разные имена пользователя базы данных с разными правами доступа, как правило. Таким образом, пользователь имеет одно имя, которое он задает при входе в систему, и, возможно, несколько имен для доступа к базам данных и их объектам.

Для доступа приложений к базам данных им также понадобятся права. Чаще всего приложениям выдаются те же права, которые предоставлены пользователям, запускающим эти приложения. Однако для работы некоторых приложений необходимо иметь фиксированный набор прав доступа, не зависящих от прав доступа пользователя. Это обеспечивается использованием специальных ролей приложения.

Итак, компонентами системы безопасности SQL Server 2012 на уровне сервера являются: система аутентификации средствами Windows и средствами SQL Server, учетные записи пользователей и встроенные роли сервера. На уровне базы данных компонентами системы безопасности являются: идентификация пользователей баз данных, фиксированные и пользовательские роли баз данных, а также роли приложений.

Фиксированными ролями сервера являются:

Sysadmin – для выполнения любых действий в сервере;

Sereradmin– для конфигурирования и выключения сервера;

Setupadmin– для управления связанными серверами и процедурами, автоматически запускающимися при старте сервера;

Securityadmin– для управления учетными записями и правами на создание базы данных, а также для контроля журнала ошибок;

Processadmin - для управления процессами, запущенными на сервере;

Dbcreator – для создания и модификации баз данных;

Diskadmin– для управления файлами сервера;

Bulcadmin– для массивного копирования баз данных.

Фиксированную роль сервера нельзя удалить или модифицировать. Нельзя также создать новую фиксированную роль. Предоставить права доступа к серверу можно только путем включения пользователя в требуемую роль сервера. Таким образом, роли сервера позволяют объединять пользователей, выполняющих одинаковые функции, для упрощения администрирования системы безопасности SQL Server. В предыдущих версиях SQL Server можно было использовать только учетную запись sa, которая предоставляла все права доступа к серверу.

При создании базы данных сервер автоматически создает для нее фиксированные роли, которые, как и фиксированные роли сервера, нельзя удалить или модифицировать:

Db_owner – для выполнения любых действий в базе данных;

Db_accessadmin – для добавления и удаления пользователей;

Db_securityadmin – для управления всеми разрешениями, объектами, ролями и именами ролей;

Db_ddladmin – для выполнения любых команд DDL, кроме GRANT, DENY и REVOKE;

Db_backupoperator– для выполнения команд DBCC, CHECK, POINT и BACKUP;

Db_datareader – для контроля данных во всех таблицах базы данных и и чтения;

Db_datawriter – для модификации данных в любых таблицах базы данных;

Db_denydatareader – для запрета просмотра данных в любой таблице базы данных;

Db_denydatawriter – для запрета модификации данных во всех таблицах базы данных.

Кроме этих фиксированных ролей любой базы данных есть еще одна роль public, членами которой автоматически становятся все пользователи, имеющие тот или иной доступ к базе данных. Эта роль имеет специальное назначение и обеспечивает минимальные права доступа к базе данных тем пользователям, для которых их права не определены явно. Эта роль имеется во всех базах данных, включая системные master, tempdb, msdbu model и не может быть удалена.

Если в базе данных разрешен пользователь quest, то установленный для public доступ будут иметь все пользователи, получившие доступ к SQL Server.

В отличие от сервера базы данных могут иметь пользовательские роли и роли приложения, которые создает администратор с помощью Enterprise Manager или Transact_SQL индивидуально для групп пользователей и групп приложений, наделяя их необходимыми правами доступа к конкретной базе данных.

В любую роль базы данных можно включать:

а) пользователей сервера;

б) роли сервера;

в) пользователей Windows;

г) группы пользователей Windows.

Средствами Enterprise Manager можно включать только пользователей сервера. Процедура SQL Server sp_addrolemember ‘role’, ‘security_account’ позволяет включать как роли сервера, так и пользователей Windows, в том числе и групп пользователей с помощью задания их учетной записи в SQL Server или Windows ‘security_account’ и указания требуемой роли ‘role’.

Работа с данными и выполнение хранимых процедур требуют наличия класса доступа, называемого правами на доступ к объектам баз данных: таблицам и ее столбцам, представлениям и хранимых процедурам.

Такими правами являются:

SELECT, INSERT, UPDETE, DELETE, RFERENCES – для таблиц и представлений, а SELECT и для столбца (тоже и для UPDETE), SELECT и UPDETE – для столбца таблицы или представления;

EXECUTE – для хранимых процедур и функций.

Здесь право RFERENCES разрешает создавать внешние ключи и представления для таблиц.

Командой GRANT можно разрешать пользователям определенные права доступа к объектам, командой **DENI** – запрещать их.

Помимо прав доступа к объектам имеются еще и права, на создание объектов базы данных и самой базы данных:

CREATE DATABASE – на создание базы данных ;

CREATE TABLE – на создание таблиц;

CREATE VIEW – на создание представлений;

CREATE DEFAULT – на создание умолчаний;

CREATE RULE – на создание правил;

CREATE PROCEDURE – на создание хранимых процедур;

BACKUP DATABASE – на резервное копирование баз данных;

BACKUP LOG – на резервное копирование журнала транзакций;

ALL – на создание любых объектов.

При установке SQL Server имеется возможность выбрать один из двух режимов аутентификации:

а) средствами Windows ;

б) средствами Windows и/или средствами SQL Server.

В первом случае после успешной аутентификации с помощью Windows SQL Server автоматически обеспечивает доступ пользователя к требуемому экземпляру сервера и к нужной базе данных. Этот метод подключения называется методом установления доверительного подключения. В этом случае член стандартной роли sysadmin или securityadmin должен указать серверу, какие группы или пользователи Windows имеют доступ к серверу. Во время подключения пользователя его имя и пароль запрашиваются только один раз при входе в систему Windows.

Во втором режиме системным администратором, входящим в роль sysadmin или securityadmin, должна быть создана и сконфигурирована учетная запись в SQL Server для каждого пользователя. Эта запись будет содержать собственное имя, имя экземпляра сервера и пароль. Две такие записи с именем BUILTIN\Administrators и sa создаются автоматически при установке сервера.

Обе эти записи автоматически включаются также во встроенную роль сервера sysadmin, в результате системные администраторы получают полный доступ ко всем базам данных с именем пользователя dbo (DataBase Owner). Если функции системного администратора и администратора баз данных выполняют разные люди, следует исключить учетную запись BUILTIN\Administrators. Запись sa не следует использовать, так как она предназначена для совместимости со старыми версиями SQL Server и для входа в сервер, если администратор баз данных забыл пароль. Как правило, для администратора баз данных создается отдельная учетная запись с ролью сервера sysadmin.

После того как пользователь прошел аутентификацию и получил идентификатор учетной записи (LoginID), он считается зарегистрированным и ему предоставляется доступ к серверу.

Учетная запись при создании была связана с конкретной базой данных, а пользователь – с конкретным именем пользователя базы данных. Именно пользователи баз данных являются специальными объектами, которым предоставляются права доступа к данным. Если учетная запись не связывается с конкретным пользователем, то такому пользователю предоставляется неявный доступ с использованием гостевого имени quest, которому даются минимальные права владельцами баз данных. Все учетные записи связаны с quest.

Если в базе данных разрешен пользователь quest, то установленный для роли public доступ будут иметь все пользователи, получившие доступ к SQL Server.

Для управления системой безопасности сервера SQL Server можно использовать следующие хранимые процедуры и команды языка Transact_SQL:

sp_addapprole – создать роль для приложения ;

sp_addlogin – создать новую учетную запись сервера;

sp_addrole – создать новую роль в базе данных;

sp_addrolemember – добавить члена в роль базы данных;

sp_addsrvrolemember – добавить члена в фиксированную роль сервера; sp_approlepassword – изменить пароль для роли приложения;

sp_defaultldb – изменить базу данных по умолчанию для учетной записи;

sp_defaultlanguage – изменить язык по умолчанию для учетной записи;

p_denylogin – запретить доступ пользователю или группе Windows;

sp_dropapprole – удалить роль приложения;

sp_droplinkedsrvlogin – удалить отображения учетной записи с другого сервера;

sp_droplogin – удалить учетную запись сервера;

sp_droprole – удалить роль базы данных;

sp_droprolemember – удалить пользователя из роли базы данных; sp_dropsrordemember – удалить члена из роли сервера;

sp_grantdbaccess – разрешить доступ к базе данных учетной записи сервера, пользователям и группам пользователей Windows;

sp_grantlogin – разрешить доступ к серверу;

sp_helpdbfixedrole – выдать список фиксированных ролей в базе данных; sp_helplogins – посмотреть учетную запись;

sp_helpntgraep – посмотреть группы NT в сервере;
sp_helprole – посмотреть роли, определенные в базе данных;
sp_helpsrvrole – выдать список фиксированных ролей сервера;
sp_helpsrvrolemember – выдать информацию о члене роли сервера;
sp_helpuser – просмотреть информацию о пользователе;
sp_password – изменить пароль учетной записи сервера;
sp_setapprole – инициализировать роль приложения;
GRANT – предоставить доступ;
DENI – запретить доступ;
REVOKE – неявно отключить доступ.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить теоретическую часть настоящей инструкционно-технологической карты.
2. Рассмотреть работу создания пользователей, описанную в разделе «Примеры выполнения работы» инструкционно-технологической карты №25.
3. Получить у преподавателя индивидуальное задание и выполнить лабораторную работу в соответствии с вариантом задания согласно описанной в разделе «Пример выполнения работы» методике настоящей инструкционно-технологической карты.
4. Ответить на контрольные вопросы.

3. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Задание 1. Создать учетную запись SQL сервера, используя графическую утилиту Enterprise Manager, выполнив следующие действия:

1. Выбрать нужный сервер.
2. Открыть папку Security этого сервера.
3. Выбрать объект Logins, щелкнув по соответствующему значку.
4. В правом окне просмотреть список учетных записей данного сервера: Name – имя учетной записи сервера; Type – происхождение учетной записи:

User W– пользователь Windows;
Group W– группа пользователей Windows; Standard – пользователь SQL сервера;
Server Access – доступ к серверу SQL:
Permit – разрешен;
Deny – запрещен;
Default Database – база данных по умолчанию, к которой подключен пользователь(обязательный параметр)
User – имя пользователя базы данных;
Default Language – язык по умолчанию для данной учетной записи.

5. Для создания новой учетной записи сервера открыть контекстное меню объекта Logins, щелкнув по нему правой клавишей мыши или по значку на панели инструментов левой клавишей мыши.

6. В появившемся диалоговом окне на вкладе General (общие) ввести имя учетной записи в поле Name.

7. Выбрать тип аутентификации: Windows Authentication или SQL Server

Authentication.

8. Если выбрана аутентификация Windows, то задать в поле Domain имя домена, в котором учтен пользователь или группа Windows. Имя заданного домена добавиться впереди имени пользователя также и в поле Name (для выбора домена использовать кнопку"…").

9. В группе Security Access (безопасный доступ) установить переключатель Grant Access (доступ разрешен). Установка переключателя Deny Access навсегда запретит\ регистрацию пользователя или домена Windows.

10. Если выбрана аутентификация SQL Server, то задать только пароль для учетной записи.

11. Задав параметры аутентификации Windows или SQL Server, указать в группе Defaults (умолчания) имя базы данных в поле Database, к которой пользователь будет подключаться автоматически, и язык Language (Russian). Если имя базы данных не задать, то сервер будет автоматически подключать к базе master.

12. Включить создаваемую учетную запись в требуемую встроенную роль сервера:

Sysadmin, Serveradmin, Setupadmin, Securityadmin, Processadmin, Dbereator,

Diskadmin, Bulkadmin, установив флажок против этой роли на вкладке Server Role.

13. На вкладке Database Access выбрать требуемую базу данных, установив флажок слева от ее имени, и задать имя пользователя, в которое будет отображаться рассматриваемая учетная запись, а в нижней части вкладки с помощью флажка включить пользователя в ту или иную роль в зависимости от его работы с базой данных.

14. Щелкнув по кнопке Properties (свойства) и просмотреть список пользователей, включенных в выбранную роль рассматриваемой базы данных.

15. Щелкнув по кнопке Permissions (права) и просмотреть список прав, предоставленных выбранной роли базы данных.

16. Закрыть все окна.

17. Вновь открыть список учетных записей сервера, дважды щелкнуть по вновь созданной записи и проверить правильность введенных параметров.

18. Закрыть все окна.

Приступить к работе с базами данных, используя новую учетную запись.

Задание 2. Создать нового пользователя базы данных для учетной записи Windows с помощью Enterprise Manager, выполнив следующие действия:

1. Выбрать требуемый сервер и требуемую базу данных в левом окне Tree.
2. Открыть объекты выбранной базы данных, щелкнув по значку ”+” этой базы.
3. Выбрать в раскрывшемся списке объектов рассматриваемой базы данных объект Users (пользователи).
4. Щелкнуть правой клавишей мыши и открыть контекстное меню объекта Users (пользователи).
5. В контекстном меню исполнить команду New Database User (новый пользователь базы данных).
6. В открывшемся диалоговом окне ввести:

а) в поле Login Name – имя учетной записи пользователя или группы пользователей Windows;

б) в поле User Name – имя нового пользователя рассматриваемой базы данных.

7. Включить нового пользователя в необходимые роли базы данных: public, db – owner, db – denydatareader и т.д. Для этого требуемые роли надо отметить флажками в списке фиксированных ролей базы данных, расположенном в правой части окна.
8. Щелкнуть по кнопке Properties и, просмотрев список всех пользователей базы данных, убедиться, что новый пользователь включен этот список.
9. Щелкнуть по кнопке Permission и задать права доступа пользователя к объектам базы данных: SELECT, INSERT, UPDATE, DELET, EXEC, DRI. В окне находится полный список объектов базы данных.
10. Щелкнуть по кнопке Columns (столбцы) для выбранной базы данных и задать права доступа к конкретным столбцам таблицы: SELECT и/или UPDATE.
11. Закрыть все открытые диалоговые окна, щелкая по кнопкам ОК.
12. Проверить работу нового пользователя с рассматриваемой базой данных и его права.

4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите фиксированные роли сервера и опишите их.
2. Что можно включить в любую роль базы данных?
3. Перечислите права на доступ к объектам баз данных.
4. Перечислите хранимые процедуры языка Transact-SQL.

5. ЛИТЕРАТУРА

1. Петкович, Д. Microsoft SQL Server 2012. Руководство для начинающих: пер. с английского / Д. Петкович. – СПб.: БХВ-Петербург, 2013. – 816 с.: ил.

2. Обеспечение безопасности SQL Server [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/securing-sql-server?view=sql-server-ver15

3. Прикладное программирование и базы данных: учебно-методическое пособие для практических работ / О.В. Игнатьева; ФГБОУ ВО РГУПС. – Ростов н/Д, 2017. – 206 с.

Преподаватель В.Ю.Купцова

Рассмотрено на заседании цикловой
комиссии программного обеспечения
информационных технологий №10
Протокол № __ от «___»_____2022
ПредседательЦК В.Ю.Михалевич