Администрирование многопользовательских систем управления баз данных

ФИО преподавателя: Смирнов Михаил Вячеславович

e-mail: smirnovmgupi@gmail.com

Лекция 6

Модель безопасности СУБД.

Общие принципы обеспечения безопасности СУБД

- Поставить СУБД под защиту брандмауэра, но планировать меры безопасности в предположении, что брандмауэр был обойден.
- Своевременно устанавливать пакеты исправлений операционной системы и СУБД.
- Использовать как можно меньше функций:

  - свести к минимуму число поддерживаемых сетевых протоколов;

  - удалить системные хранимые процедуры, которые не нужны или не используются;

  - по возможности запретить вход в систему по умолчанию и с гостевыми правами;

  - не позволять пользователям работать с СУБД в интерактивном режиме (если в этом нет насущной необходимости).

Общие принципы обеспечения безопасности СУБД

- Защита компьютера, на котором работает СУБД:

  - не позволять никому из пользователей работать за компьютером, на котором работает СУБД;

  - компьютер, на котором располагается СУБД, должен находиться в помещении, запираемом на замок;

  - все визиты в помещение, где находится компьютер с работающей СУБД, должны записываться в журнал.

Общие принципы обеспечения безопасности СУБД

- Управление учетными записями и паролями:

- использовать для СУБД учетную запись операционной системы с наименьшими возможными привилегиями;

- защищать учетные записи базы данных сильными паролями;

- отслеживать неудачные попытки входа в систему;

- регулярно проверять членство в группах и роли;

- проверять учетные записи без паролей;

- назначать учетным записями наименьшие возможные привилегии;

- ограничивать привилегии учетной записи администратора базы данных.

Учетная запись пользователя

- Пользователь – успешно прошедший проверку по логину, сертификату или ассиметричному ключу пользователь БД, наделяемый правами работы с данными.
- CREATE USER user_name [FOR {LOGIN…}, {CERTIFICATE…}, {ASSYMETRIC_KEY}] [WITH DEFAULT_SCHEMA = schema_name]

Схемы БД по умолчанию

- guest
  - минимальные права
- dbo
  - владелец БД
- INFORMATION_SCHEMA
  - доступ к метаданным всех объектов БД
- Sys
  - доступ к системным представлениям (например просмотр каталогов)

Пользовательская схема

- Создается администратором БД при необходимости.
- CREATE SCHEMA my_schema AUTORIZATION [user]
  - Создание таблиц
  - Создание представлений
  - Раздача прав доступа другим пользователям.
- Процесс создания схемы является атомарным.

Роли

- Фиксированные системные или пользовательские группы пользователей или приложений, имеющие одинаковые права на действия в рамках БД
- Фиксированные серверные роли, роли базы данных или пользовательские роли.
- Права раздаются аналогично раздаче отдельным пользователям

Фиксированные серверные роли

Серверная роль	Описание
sysadmin	Выполняет любые действия в СУБД (учетная запись sa)
serveradmin	Конфигурирует экземпляры серверов
setupadmin	Управление репликациями и процедурами
securityadmin	Управляет учетными записями, мониторит отчетность сервера
processadmin	Управление системными процессами
dbcreator	Создает и изменяет базы данных
discadmin	Управляет файлами БД

Фиксированные роли БД

Роль БД	Описание
db_owner	Доступ к функциям БД
db_accessadmin	Возможность добавлять и удалять пользователей
db_datareader	Возможность просматривать данные в БД
db_datewriter	Возможность добавлять, модифицировать, удалять данные в БД
db_denydatareader	Невозможность просматривать данные в БД
db_denydatewriter	Невозможность добавлять, модифицировать, удалять данные в БД
public	Полномочия по умолчанию

Общая модель безопасности (пример)

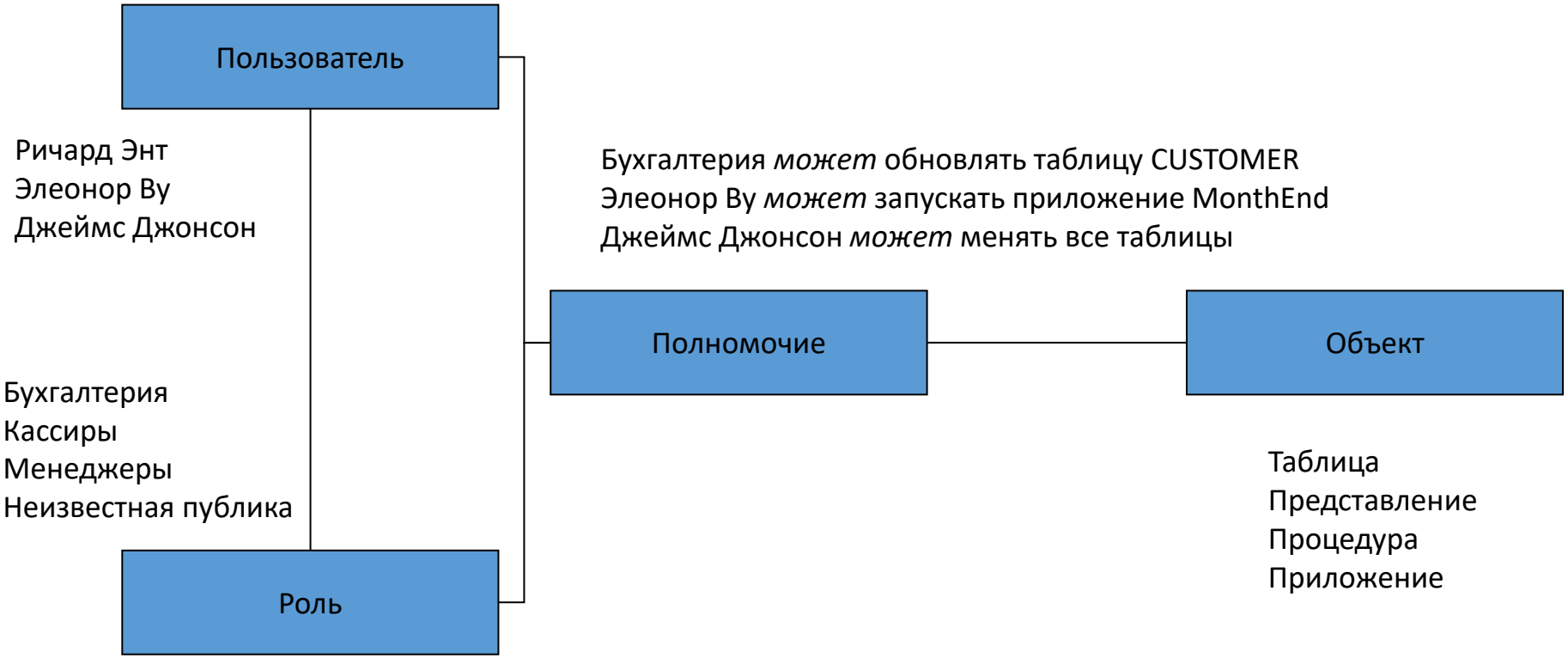

Таблица требований к ролям и пользователям (пример)

	CUSTOMER	TRANSACTION	WORK	ARTIST
Продавцы	Вставка, изменение, запрос	Изменение, запрос	Запрос	Запрос
Менеджеры	Вставка, изменение, запрос	Вставка, изменение, запрос	Вставка, изменение, запрос	Вставка, изменение, запрос
Системный администратор	Вставка, изменение, запрос, удаление, предоставление прав, модификация структуры	Вставка, изменение, запрос, удаление, предоставление прав, модификация структуры	Вставка, изменение, запрос, удаление, предоставление прав, модификация структуры	Вставка, изменение, запрос, удаление, предоставление прав, модификация структуры

Создание логина пользователя МБД (MS SQL)

```
USE master;
GO

CREATE LOGIN
[AdventureWorks\Terry.Adams]
FROM WINDOWS;
GO
```

Авторизация через OS-логин

```
CREATE LOGIN James WITH
PASSWORD = 'Pa$$w0rd';
GO
```

Авторизация через T-SQL

Создание роли и добавление пользователя МБД (MS SQL)

```
USE master;
GO

ALTER SERVER ROLE serveradmin ADD
(DROP) MEMBER Mod10Login;
GO
```

Добавление (удаление) пользователя к существующей роли

```
USE master;
GO

CREATE SERVER ROLE
srv_documenters;
GO
```

Создание новой роли сервера

Использование оператора GRANT (MS SQL)

```
GRANT SELECT ON
Marketing.CampaignBalance
TO SalesTeam;
GO
```

Разрешение выборок
из таблицы для роли

```
GRANT SELECT, UPDATE ON
Marketing.SalesTerritory
TO SalesManagers;
GO
```

Разрешение выборок и
изменений
в таблице для роли

```
GRANT EXECUTE ON
Marketing.MoveCampaignBalance
TO SalesManagers;
GO
```

Разрешение запуска процедуры
для роли

Чтение на дом

- Русский Кренке, стр. 398-407
- Петкович, Microsoft SQL Server 2012, стр. 323-366.

Вопросы для самостоятельного изучения

1. Перечислите все возможные полномочия пользователя MS SQL Server (таблица требований к ролям).
2. Что такое CERTIFICATE и ASSYMETRIC_KEY в системе безопасности MS SQL SERVER?
3. Чем USER отличается от LOGIN в MS SQL Server?
4. Чем оператор REVOKE отличается от оператора DENY?

Спасибо за внимание!