Применение элементов управления безопасностью в СУБД

Основные средства обеспечения безопасности в SQL Server

Основные средства обеспечения безопасности в SQL Server

- **Аутентификация** — это процесс входа в SQL Server, когда пользователь отправляет свои данные на сервер. Аутентификация устанавливает личность пользователя, который проходит аутентификацию;
- **Авторизация** — это процесс определения того, к каким защищаемым объектам может обращаться пользователь, и какие операции разрешены для этих ресурсов.

Аутентификация в SQL Server

Аккаунт SQL Server можно разделить на 2 части: **Имя входа** и **Пользователь**.

- **Имя входа –** это глобальный логин для всего экземпляра SQL Server. С помощью него вы проходите процесс аутентификации;
- **Пользователь –** это участник базы данных, привязанный к определенному Имени Входа.

SQL Server поддерживает 2 режима **аутентификации**:

- **Аутентификация Windows** (Windows Authentication) – аутентификация осуществляется с помощью системы безопасности Windows. Пользователям, которые уже аутентифицированы в Windows и имеют права на SQL Server не нужно предоставлять дополнительные учетные данные.
- **Смешанный режим аутентификации** (Mixed Mode Authentication) – в этом режиме помимо аутентификации Windows поддерживается аутентификация самого SQL Server через логин и пароль.

SQL Server поддерживает три типа Login Name (имен входа):

- **Локальная учетная запись** пользователя Windows или учетная запись **домена**/доверенного домена.
- **Группа Windows**. Предоставление доступа локальной группе Windows или группе из AD домена. Позволяет предоставить доступ ко всем пользователям, которые являются членами группы.
- **Логин SQL Server** (SQL Server authentication). SQL Server хранит имя пользователя и хэш пароля в базе данных **master**, используя методы внутренней аутентификации для проверки входа в систему.

Авторизация в SQL Server

Для авторизации SQL Server использует безопасность на основе ролей, которая позволяет назначать разрешения для роли или группы Windows/домена, а не отдельным пользователям.

В SQL Server есть встроенные роли сервера и баз данных, у которых есть предопределенный набор разрешений.

В SQL Server есть 3 уровня безопасности, их можно представить, как иерархию от высшего к низшему:

- **Уровень сервера –** на этом уровне можно раздать права на базы данных, учетные записи, роли сервера и группы доступности;
- **Уровень базы данных** включают в себя схемы, пользователи базы данных, роли базы данных и полнотекстовые каталоги;
- **Уровень схемы** включают такие объекты, как таблицы, представления, функции и хранимые процедуры.

Встроенные роли сервера

Роль	Описание
sysadmin	Участник роли имеет полные права ко всем ресурсам SQL Server.
serveradmin	Участники роли могут изменять параметры конфигурации на уровне сервера и выключать сервер.
securityadmin	Участники роли управляют логинами и их свойствами. Они могут предоставлять права доступа GRANT, DENY и REVOKE на уровне сервера и на уровне базы данных, если имеют к ней доступ. securityadmin мало чем отличается от роли sysadmin, потому что участники этой роли потенциально могут получить доступ ко всем ресурсам SQL Server.
processadmin	Участники роли могут завершать процессы, запущенные в SQL Server.

Роль	Описание
setupadmin	Участники роли могут добавлять и удалять связанные серверы с помощью TSQL.
bulkadmin	Участники роли могут запускать BULK INSERT операции.
diskadmin	Участники роли могут управлять устройствами резервного копирования. На практике эта роль практически не применяется.
dbcreator	Участники роли могут создавать, изменять, удалять и восстанавливать базы данных.
public	Каждый логин SQL Server находится в этой роли. Изменить членство public нельзя. Когда у пользователя нет разрешения для объекта, к которому он получает доступ, пользователь наследует разрешения public роли для этого объекта.

Встроенные роли базы данных

Роль	Описание
db_owner	Участники роли могут выполнять все действия по настройке и обслуживанию базы данных, включая удаление.
db_securityadmin	Участники роли могут менять членство других ролей. Участники этой группы потенциально могут увеличить свои права до db_owner, поэтому стоит считать эту роль эквивалентной db_owner.
db_accessadmin	Участники роли могут управлять доступом к базе данных для существующих на сервере логинов.
db_backupoperator	Участники роли могут выполнять резервное копирование базы данных.
db_ddladmin	Участники роли могут выполнять любую DDL команду в базе данных.
db_datawriter	Участники роли могут создавать/изменять/удалять данные во всех пользовательских таблицах в базе данных.
db_datareader	Участники роли могут считывать данные со всех пользовательских таблиц.
db_denydatawriter	Участникам роли запрещен доступ к пользовательским таблицам базы данных.
db_denydatareader	Участникам роли запрещен доступ к пользовательским таблицам базы данных.

Роли приложений

Роль приложения – это объект базы данных (такой же, как и обычная роль базы данных), который позволяет с помощью аутентификации через пароль менять контекст безопасности в базе данных. В отличие от ролей баз данных, роли приложений по умолчанию находятся в неактивном состоянии и активируются, когда приложение выполняет процедуру sp_setapprole и вводит соответствующий пароль.

Фильтрация данных в SQL Server

через хранимые процедур/представления/функции можно отнести к реализации принципу наименьших привилегий, так как вы предоставляете доступ не ко всем данным в таблице, а лишь к некоторой их части.

Безопасность на уровне строк или **Row-Level Security** (**RLS**) позволяет фильтровать данные таблицы для разных пользователей по настраиваемому фильтру.

Шифрование данных средствами SQL Server

SQL Server может шифровать данные, процедуры и соединения с сервером. Шифрование возможно с использованием сертификата, асимметричного или симметричного ключа. В SQL Server используется иерархичная модель шифрования, то есть каждый слой иерархии шифрует слой под ним. Поддерживаются все известные и популярные алгоритмы шифрования. Для реализации алгоритмов шифрования используется Windows Crypto API.

Прозрачное шифрование данных

Прозрачное шифрование данных или **Transparent Data Encryption** шифрует всю базу целиком. При краже физического носителя или .mdf/.ldf файла, злоумышленник не сможет получить доступ к информации в базе данных.

Always Encrypted

Эта технология позволяет хранить шифрованные данные в SQL Server без передачи ключей шифрования самому SQL Server.

Always Encrypted так же как и TDE шифрует данные в базе данных, но не на уровне базы, а на уровне столбца.