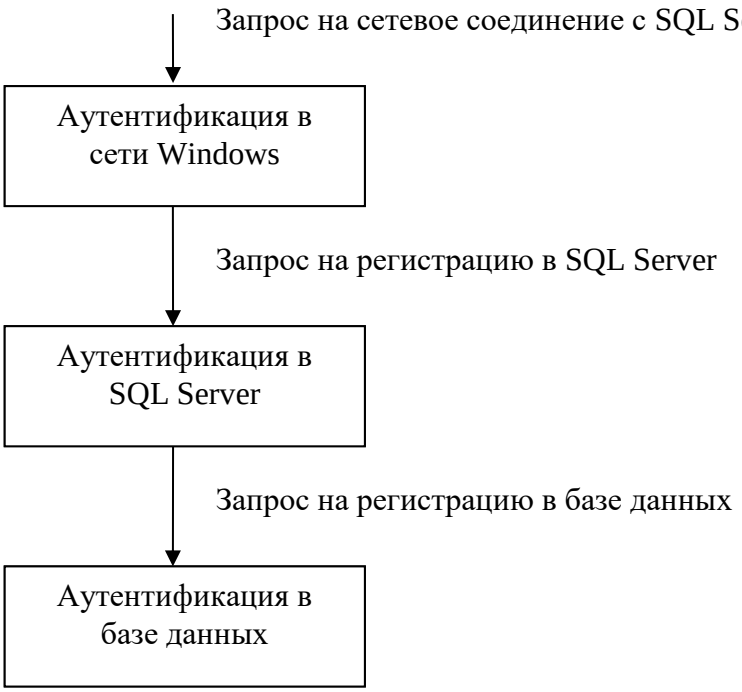
Уровни защиты данных в системе Windows 2X **– SQL Server** 2X



SQL Server оснащен двумя режимами защиты данных: интегрированным режимом защиты данных Windows 2X (integrated mode) и смешанным (mixed mode). В каждом из режимов пользователи с помощью учетных записей только Windows или Windows 2X и SQL Server 2X подтверждают свое право на использование среды SQL Server.

При подключении клиентского компьютера к серверу, на котором запущен SQL Server 2X, операционная система проводит проверку сетевого соединения. В зависимости от используемой сетевой библиотеки это соединение устанавливается по-разному.

При использовании в SQL Server протокола Named Pipes или многопротокольной библиотеки (Multiprotocol) устанавливается доверительное соединение с Windows 2X, с помощью которого SQL Server и общается с клиентом. Соединение, устанавливаемое с помощью Named Pipes или Multiprotocol, обязательно проходит проверку в Windows 2X Server. Протокол TCP/IP не позволяет устанавливать доверительные соединения, поэтому регистрацию в Windows 2X можно не проводить, а перейти непосредственно к регистрации в SQL Server.

Роли уровня сервера и баз данных

Роли применяются для организации учетных записей. С помощью ролей отдельные пользователи баз данных объединяются в единые группы. Роли могут включать в себя не только отдельных пользователей баз данных, но и другие роли.

При установке SQL Server создается учетная запись **sa**, принадлежащая к роли сервера sysadmin. Удалить учетную запись sa из роли sysadmin удалению не подлежит. Пользователь sa является владельцем или совладельцем любых баз данных, создаваемых на сервере.

Заданные роли уровня сервера

Sysadmin – пользователи, отнесенные к этой роли выполняют любые операции в SQL Server, определяют настройки системы защиты и права доступа к объектам базы данных.

Serveradmin – пользователи настраивают параметры SQL Server с помощью хранимой процедуры sp_configure и завершают работу сервера с помощью оператора SHUTDOWN. Обычно это операторы SQL Server, занимающиеся поддержкой сервера.

Setupadmin – роль определена для пользователей, устанавливающих и настраивающих связанные серверы и определяющих хранимые процедуры, которые выполняются при запуске SQL Server.

Securityadmin – роль для пользователей, создающих и управляющих учетными записями SQL Server, а также правами доступа к базам данных. Пользователи данной роли переназначают пароли учетных записей SQL Server всех пользователей, за исключением sa.

Proccessadmin – управляют процессами, запущенными в текущем экземпляре SQL Server. В их обязанности входит удаление «заблудившихся» запросов.

Dbcreator – роль для создания, удаления и изменения баз данных. Кроме того, пользователи, отнесенные к этой роли, занимаются резервным копированием и восстановлением данных на сервере. Владельцы баз данных – кандидаты на получение этой роли.

Bulkadmin – пользователи этой роли ответственны за выполнение обмена данными между серверами с помощью оператора BULK INSERT.

Diskadmin – роль определяется для пользователей, которым разрешено управлять файлами и их увеличением в SQL Server. Обычно в эту роль включают владельцев баз данных.

Заданные роли уровня базы данных

Заранее определенные роли уровня базы данных предоставляют пользователям права в пределах только отдельно взятой базы данных.

Роль *public* существует в каждой базе данных и не может быть удалена. Каждый пользователь базы данных относится к этой роли и получает набор прав, определенных для нее: право на использование оператора SELECT, EXECUTE и многих системных хранимых процедур для всех системных таблиц каждой базы данных. Задавая дополнительные права для роли *public* необходимо помнить, что они будут распространяться на всех пользователей, включая и тех, которые будут добавлены в будущем.

Db_owner – роль назначается для владельцев базы данных. Пользователи получают самые обширные права в базе данных и выполняют любые

операции, которые только позволяет выполнять SQL Server в пределах одной базы данных, в том числе относить пользователей к этой роли и удалять из других ролей.

Db_accessadmin – пользователи назначают и закрывают доступ к базе данных.

Db_securityadmin – пользователи администрируют систему защиты данных в базе данных: управляют правами, ролями и доступом к объектам базы данных.

Db_ddladmin – пользователи этой роли создают, изменяют и удаляют все объекты базы данных, но не могут пользоваться командами их защиты (например: grant, revoke, deny).

Db_backupoperator – пользователи, отнесенные к этой роли, выполняют команды DBCC, управляют контрольными точками и проводят резервное копирование.

Db_datareader – пользователи имеют полный доступ к выборке данных (с помощью оператора SELECT) из любой таблицы, функции или представления базы данных.

Db_datawriter – эта роль позволяет выполнять операторы INSERT, DELETE, UPDATE для любой таблицы базы данных.

Db_denydatareader – эта роль запрещает выполнение оператора SELECT для всех таблиц базы данных.

Db_denydatawriter – роль запрещает выполнение операторов модификации данных (INSERT, DELETE, UPDATE) для любых таблиц базы данных.

Резервное копирование

Виды резервного копирования

1. *Полное резервное копирование базы данных* – включает создание резервных копий всех таблиц, индексов, системных таблиц и объектов базы данных. Во время полного резервного копирования создается копия журнала транзакций, но при этом не сохраняются пустые строки, а записи журнала после копирования не удаляются.
2. *Распределенное резервное копирование*. Создаются резервные копии только данных, которые изменились во время последнего резервного копирования.
3. *Резервное копирование файлов и групп файлов*. Производится создание резервных копий только выбранных фалов или групп файлов, а не всей базы.
4. *Резервное копирование журнала транзакций*. Все изменения в базе данных фиксируются в специальном журнале транзакций. В нем фиксируются все выполненные пользователями команды, а также операции, автоматически выполняемые сервером. Журнал транзакций используется для повторного выполнения всех ранее выполненных операций.

Для баз данных размером в несколько гигабайт резервное копирование производится один раз в день, а журнал транзакций - несколько раз в день в строго определенные моменты.

Резервное копирование базы данных MASTER выполняется после каждого изменения, но не чаще одного раза в день.

Резервное копирование базы данных MSDB проводится ежедневно, а журнала транзакций – раз в неделю.

Модели восстановления

Полное восстановление – используется для любых видов резервного копирования. Как модель по умолчанию используется в выпусках SQL Server Standard и Enterprise.

Простое восстановление – используется, когда базу необходимо восстановить до предыдущего состояния с помощью любой резервной копии.

Создание устройства резервного копирования

Устройство резервного копирования – это простой указатель в системном каталоге MS SQL (системной таблицы *sysdevices* базы данных *master*), содержащий логическое имя и физический путь расположения файла на локальном жестком диске удаленного компьютера. При выполнении команды BACKUP производится ссылка на логическое имя устройства резервного копирования, а не указывается его физическое месторасположение. Можно создать несколько устройств логического копирования со ссылкой на одно и то же физическое устройство.

Для создания устройства резервного копирования используется хранимая процедура
sp_addumpdevice.

EXEC sp_addumpdevice 'disk','master_backup',
'C:\Program Files\Microsoft SQL Server\mssql\backup\master_backup.bak'

Sp_addumpdevice ‘тип устройства’, ‘логическое_имя’, ‘физическое_имя’

Для удаления устройства резервного копирования используется следующая хранимая процедура:
Sp_dropdevice ‘логическое имя’.
Логическое_имя – имя устройства резервного копирования; используется в команде BACKUP и ссылается на физический носитель.
EXEC sp_dropdevice ‘master_backup’
Для одновременного удаления вместе с устройством и резервной копии выполняется процедура:
EXEC sp_dropdevice ‘master_backup’, ‘delfile’

Для просмотра списка всех устройств резервного копирования выполняется процедура:

```
EXEC sp_helpdevice
```

Проверка правильности базы

Прежде чем приступить к созданию резервных копий баз данных, необходимо выполнить проверку базы данных. Правильность базы данных перед резервным копированием не гарантирует правильность резервных копий, поэтому необходимо проверять и их.

Проверка правильности базы данных запускается перед резервным копированием хранимой процедурой:

проверку могут проводить только члены роли sysadmin и db_owner.

```
Use master
DBCC CHECKDB ('master') WITH NO_INFOMSGS, TABLERESULTS
```

NO_INFOMSGS позволяет выводить на экран только важные сообщения. Ни одно информационное сообщение на экран не выводится.

Создание резервных копий

Резервное копирование проводится либо на одно устройство, либо на несколько. На одном устройстве можно также создавать несколько резервных копий.

Резервное копирование выполняется командой BACKUP

```
EXEC sp_addumpdevice 'disk','master_backup',
'C:\Сервер_SQL\master_backup.bak'
GO
Use master
DBCC CHECKDB ('master') WITH NO_INFOMSGS
BACKUP DATABASE master to master_backup WITH INIT
```

Команда WITH INIT позволяет перезаписывать существующие в устройстве резервные копии новыми. Перезапись проводится только в случае, если срок действия резервной копии истек.

Настройка срока хранения

Изменение срока хранения производится с помощью процедуры

```
EXEC sp_configure ‘media retention’,30
RECONFIGURE WITH OVERRIDE/
```

Срок хранения задается длительностью 30 дней. После процедуры для вступления в силу параметров требуется перезагрузка SQL Server.

ПРИМЕРЫ КОДОВ T-SQL

Выборка данных

```
USE GGG
SELECT*FROM AUTHORS
```

Выборка данных с заданным ограничением

```
USE GGG
SELECT*FROM AUTHORS
WHERE NOT PHONE LIKE '4%'

SELECT*FROM VIEZD
WHERE  NOT (MARHRUT='ПИРС'OR MARHRUT='ГОРОД')
```

Выполнение групповых операций

```
USE GGG
SELECT VIEZD.KOD_AVTO, COUNT(KOD_AVTO) AS K  FROM VIEZD
GROUP BY KOD_AVTO
HAVING (KOD_AVTO)=2
```

Включение однопользовательского режима

```
EXEC SP_DBOPTION PUBS, 'DBO USE ONLY', TRUE
```

Выключение однопользовательского режима

```
EXEC SP_DBOPTION PUBS, 'DBO USE ONLY', FALSE
```

Перевод базы в многопользовательский режим

```
EXEC SP_DBOPTION PUBS,'DBO USE ONLY',FALSE
```

Результат выполнения команды

```
The command(s) completed successfully.
```

Информация по базе

```
EXEC SP_HELPDB GGG
```

Переименование базы данных

```
USE MASTER
GO
EXEC SP_DBOPTION GGG, 'SINGLE USER', TRUE
EXEC SP_RENAMEDB 'GGG', 'BAZA'
EXEC SP_DBOPTION BAZA, 'SINGLE USER', FALSE
GO
USE BAZA
SP_HELPDB BAZA
```

Просмотр учетных записей
SELECT SUBSTRING (NAME,1,25) AS NAME,
SUBSTRING (PASSWORD,1,20) AS PASSWORD,LANGUAGE
FROM SYSXLOGINS

Создание учетных записей
EXEC SP_ADDLOGIN 'YUKA','111'

Изменение пароля
EXEC SP_PASSWORD NULL,'LLL','YUKA'

Отображение сведений об учетных записях
EXEC SP_HELPLOGINS

Удаление учетных записей
EXEC SP_DROPLOGIN YUKA

Создание групп пользователей
EXEC SP_GRANTLOGIN YUKA

Сведения о пользователях базы данных
EXEC SP_HELPUSER

Сведения о соединениях пользователей
EXEC SP_MONITOR