

Администрирование в информационных системах

Администрирование баз данных
Управление доступом к данным

Управление доступом

- При решении вопроса о разворачивании сервера БД необходимо решить вопросы защиты данных и установить определенную политику безопасности доступа к объектам базы данных для пользователей и администраторов системы.
- MS SQL Server 2005 позволяет обеспечить защиту информации в БД и разграничить доступ на основе ролевой политики безопасности.

Проверка подлинности

- Для того, чтобы пользователь мог работать с БД или выполнять задания на уровне сервера, СУБД первоначально проверяет его подлинность (выполняется аутентификация пользователя).
- SQL Server 2005 поддерживает два режима проверки подлинности:
 - Проверка подлинности средствами Windows;
 - Проверка подлинности средствами SQL Server.

Проверка подлинности средствами Windows

- Если пользователь прошел проверку подлинности в домене и является зарегистрированным пользователем, то операционная система предлагаем экземпляру SQL Server 2005 доверять результатам этой проверки и предоставлять доступ на основании и указанных имени и пароля.
- Для подтверждения подлинности в Windows 2000/2003 передается билет Kerberos.
 - SQL Server проверяет полученный билет и предоставляет или отказывает в доступе.

Проверка подлинности средствами SQL Server 2005

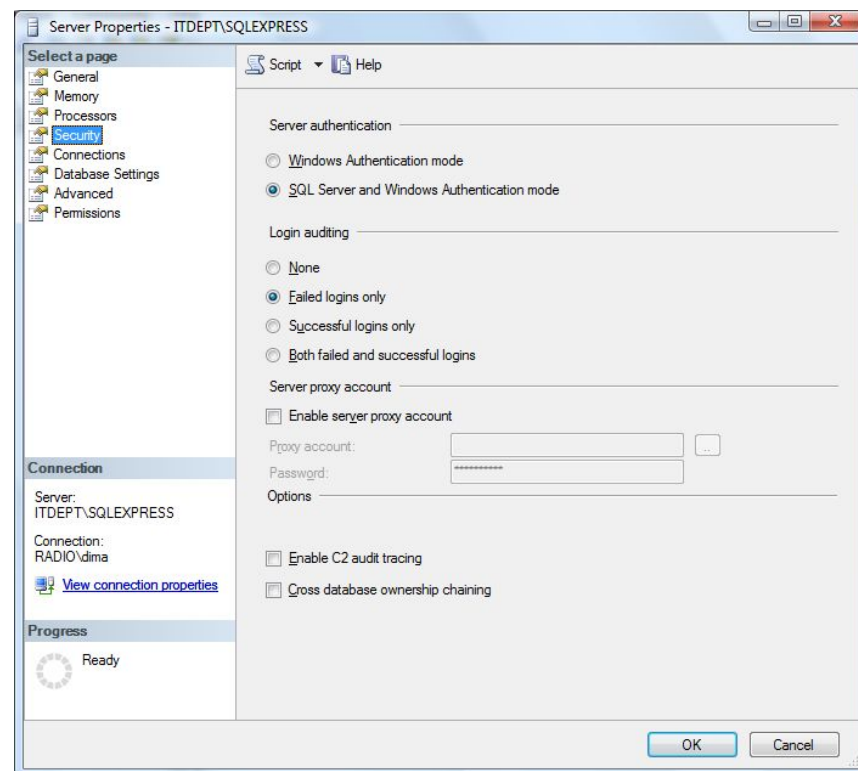
- При использовании проверки подлинности средствами SQL Server 2005 пользователь передает серверу свои имя и пароль.
- При проверке имени SQL Server сравнивает переданное имя со списком зарегистрированных пользователей, далее зашифровывает пароль и сравнивает с зашифрованным паролем в таблице.

Возможности защиты при проверке различными методами подлинности

Проверка подлинности Windows	Проверка подлинности SQL Server 2005
Имя и пароль при входе в систему передаются контроллеру домена в зашифрованном виде	Windows не проверяет подлинность пользователя
Пользователь, прошедший проверку подлинности передает имя и пароль SQL Server 2000, билет Kerberos зашифровывается	Имя и пароль передается в незашифрованном виде
В Windows 2000/2003 действует политика паролей	Политики паролей нет
В Windows 2003/2003 действует политика блокирования записей	Политики блокирования учетных записей нет

Выбор режима проверки подлинности

- Выбор проверки подлинности выбирается, как правило, при установке SQL Server 2005.
- Смена режима проверки подлинности после установки может быть выполнена с помощью SQL Server Management Studio.
- Для этого необходимо выбрать нужный экземпляр SQL Server 2005 и в контекстном меню открыть раздел Security в свойствах экземпляра SQL Server.



Авторизация пользователей

- После завершения проверки подлинности пользователь может выполнять операции с данными или административные задачи только с теми БД, для которых ему предоставлены соответствующие разрешения доступа.
- SQL Server имеет несколько предопределенных ролей уровня сервера, обладающих правами администрирования.
 - Данные роли не могут быть удалены или изменены их права.
- Чтобы предоставить данные права пользователю, необходимо добивать его учетную запись в состав роли сервера.

Роли сервера SQL Server 2005

Роль сервера	Права члена роли
Sysadmin	Может выполнять любую задачу в любой БД SQL Server. По умолчанию учетная запись sa и все члены группы Windows Administrator являются членами данной роли
Serveradmin	Конфигурировать SQL Server с помощью системной хранимой процедуры sp_configure и перезапускать службы SQL Server
Setupadmin	Устанавливать и изменять параметры конфигурации удаленных и связанных сервисов и параметры репликации. Могут включать некоторые хранимые процедуры в число исполняемых при запуске системы
Securityadmin	Выполнять все операции, связанные с управлением, защитой, контролем над учетными записями сервера и чтение журнала ошибок SQL Server

Роли сервера SQL Server 2005

Роль сервера	Права члена роли
Processadmin	Управлять процессами в системе SQL Server, удалять пользовательские процессы, применяющие некорректные запросы
Dbcreator	Создавать, изменять и удалять БД
Diskadmin	Управлять файлами и устройствами резервного копирования
Bulkadmin	Выполнять операторы BULK INSERT (распределять задачи резервного копирования и восстановления данных)

Информация об участниках ролей сервера БД

- Для получения сведений об участниках серверной роли используется системное представление:
 - `sys.server_role_members`
- Для добавления существующего логина в число участников роли используется системная хранимая процедура:
 - `EXECUTE sp_addsrvrolemember login, fix_server_role`
- Для удаления пользователя из числа участников роли:
 - `EXECUTE sp_dropsrvrolemember login, fix_server_role`

Разрешение уровня базы данных

- При подключении к SQL Server автоматически не предоставляется право доступа к БД.
 - Кроме участников роли `sysadmin` никто не имеет прав на уровне БД.
- Для работы с БД необходимо предоставление специальных прав (разрешений) на уровне БД.
- Разрешение можно предоставлять (`grant`), блокировать (`deny`) и отзывать (`revoke`).
- К разрешениям уровня БД относятся:
 - разрешение на создание объектов,
 - администрирование БД,
 - выполнение операторов T-SQL,
 - вставка и изменение данных в таблицы,
 - просмотр данных.

Добавление пользователя БД

- Для предоставления доступа к БД необходимо создать учетную запись пользователя БД и связать с логином на уровне сервера БД:
 - `CREATE USER user_name FOR LOGIN login_name`
- Для изменения свойств учетной записи:
 - `ALTER USER`
- Для удаления учетной записи пользователя БД:
 - `DROP USER`

Разрешения, назначаемые на уровне БД

Разрешение	Описание
Database owner	Если пользователь является владельцем БД, то он может выполнять любые операции над ней
DBO role	Все участники sysadmin являются членами роли dbo и могут выполнять над БД любые действия
User	Пользователи и группы получают доступ к БД. Зарегистрированные пользователи получают права database owner, роли public и специально определенные права
Guest	Если пользователь прошел проверку подлинности на SQL Server, но не имеет пользовательского доступа к БД, он может получить права guest
Public role	Все пользователи, которым разрешен доступ к некоторой БД, становятся участниками роли public и получают определенные права для работы с БД

Разрешения, назначаемые на уровне БД

Разрешение	Описание
Fixed database role	Зарегистрированные пользователи могут стать участниками постоянных ролей БД
User-defined database role	Зарегистрированные пользователи могут стать участниками роли, определенной пользователем. Эти роли создаются администратором.
Statement permissions	Право выполнения административных операторов может быть предоставлено пользователям
Object permissions	Право доступа к объектам может быть предоставлено пользователям, группам
Application role	Право выполнять операции с БД может быть предоставлено приложению

Фиксированные роли базы данных

Роль БД	Права участника роли
Db_owner	Может выполнять любые задачи в БД
Db_accessadmin	Может добавлять в БД и удалять из нее пользователей (с помощью процедуры sp_grantdbaccess)
Db_securityadmin	Может управлять разрешениями, ролями, записями участников ролей (используя операторы GRANT, REVOKE, DENY)
Db_ddladmin	Может добавлять, изменять и удалять объекты (CREATE, ALTER, DROP)
Db_backupoperator	Может выполнять команды DBCC, инициировать процессы фиксации транзакций, создавать резервные копии

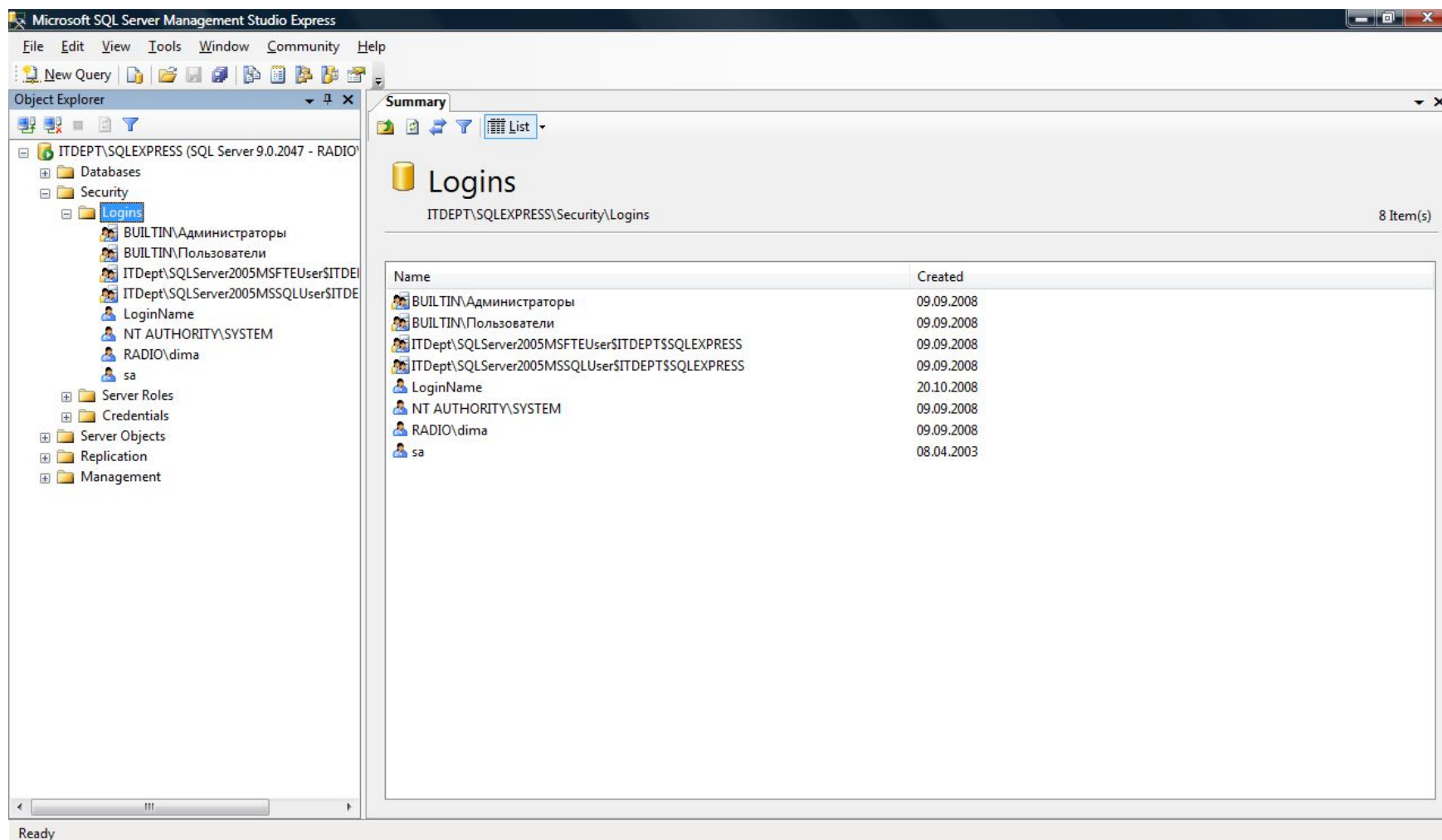
Фиксированные роли базы данных

Роль БД	Права участника роли
Db_datareader	Может считывать данные из пользовательских таблиц и представлений в БД
Db_datawriter	Может изменять или удалять данные из пользовательских таблиц и представлений
Db_denydatareader	Не может считывать данные из пользовательских таблиц представлений в БД
Db_denydatawriter	Не может изменять или удалять данные из пользовательских таблиц в БД

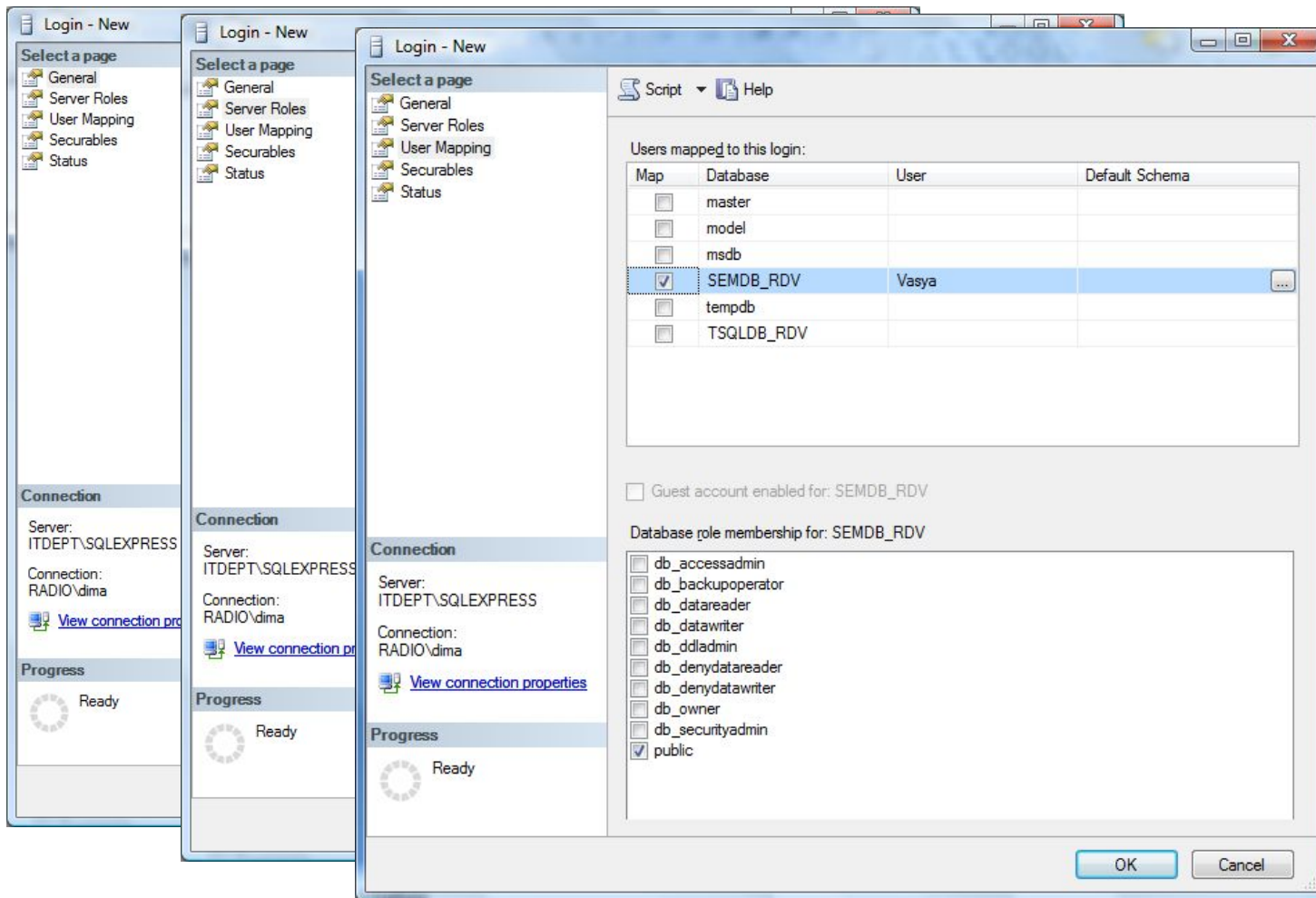
Создание и управление учетными записями

- SQL Server Management Studio позволяет в интерактивном режиме сопоставить учетную запись пользователя с регистрационной записью сервера, создавать регистрационную запись.
- Для создания учетной записью можно воспользоваться мастером средствами Management Studio или операторами T-SQL

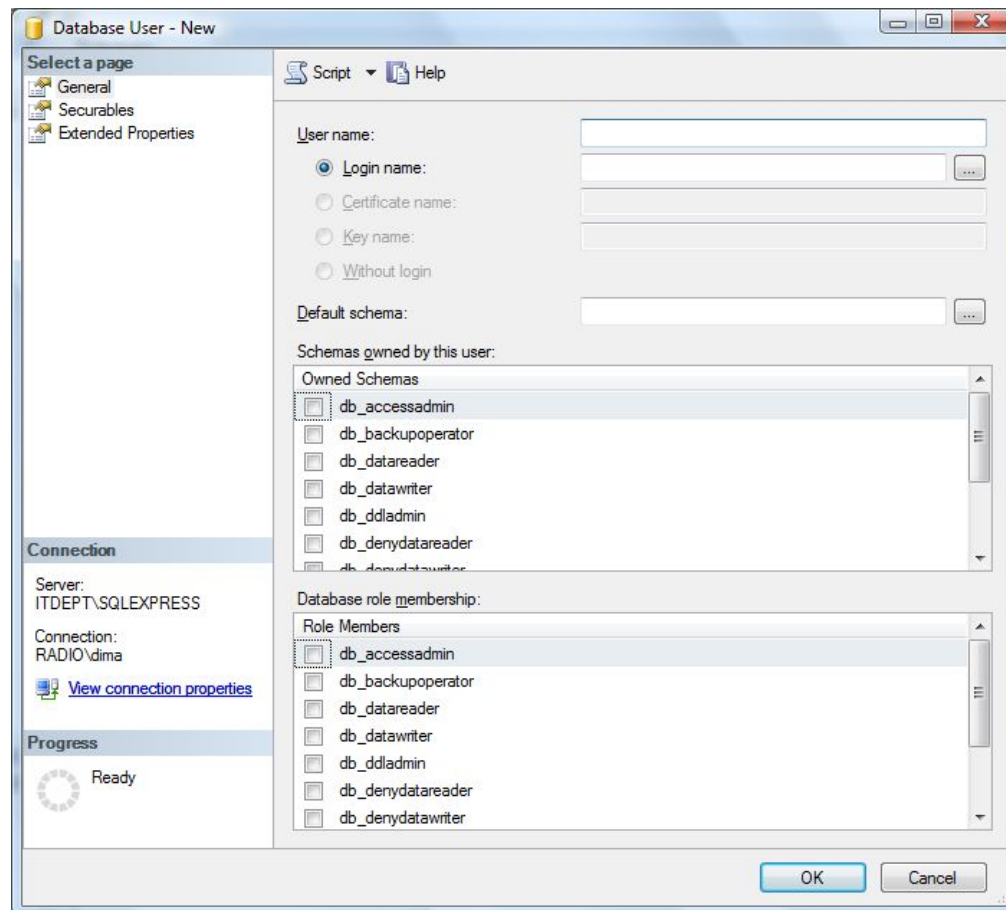
Использование Management Studio



Создание учетной записи средствами Management Studio

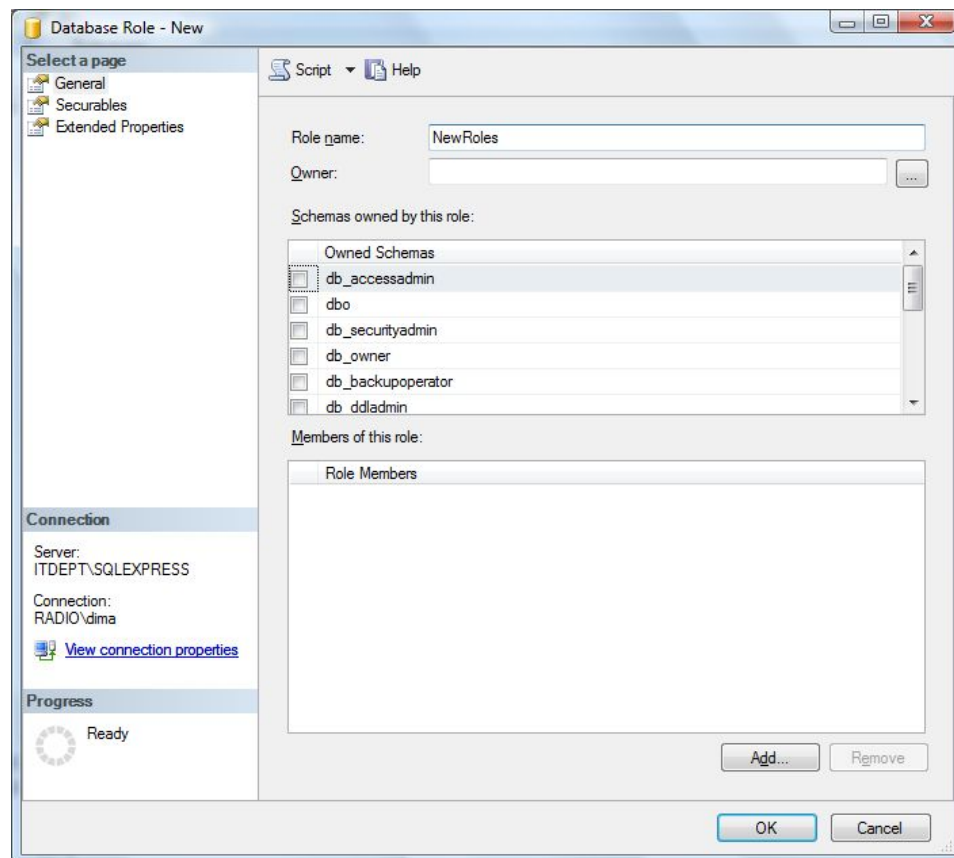


Создание учетной записи пользователя БД



Создание пользовательской роли БД

- Для создания пользовательской роли базы данных, выберите необходимую базу данных.
- Раскройте список объектов и выберите объект Roles.
- С помощью контекстного меню вызывается команда New Database Role.



Создание пользовательской роли БД

- Для создания пользовательской роли базы данных, укажите необходимую базу данных и используемую схему.
 - `USE TSQLDB;`
 - `CREATE USER NewUser FOR LOGIN NewLogin WITH DEFAULT_SCHEMA=db_datawriter;`
 - `GO`

Системные процедуры администрирования учетных записей Windows

- Данные системные процедуры могут выполняться только участниками ролей sysadmin и securityadmin

Системная хранимая процедура	Описание
Sp_grantlogin 'учетная запись'	Создает учетную запись для пользователя Windows
Sp_revokelogin 'учетная запись'	Удаляет учетную запись пользователя с SQL Server
Sp_denylogin 'учетная запись'	Запрещает пользователям подключаться к SQL Server
Sp_defaultdb 'учетная запись', 'база данных'	Изменяет БД, установленную по умолчанию для данной записи
Sp_defaultlanguage 'учетная запись', 'язык'	Изменяет язык, установленный по умолчанию

Системные процедуры администрирования учетных записей SQL Server

- Данные системные процедуры могут выполняться только участниками ролей sysadmin и securityadmin

Системная хранимая процедура	Описание
Sp_addlogin 'учетная запись', ['пароль', 'база данных', 'язык', 'sid', 'опции шифров']	Создает учетную запись SQL Server
Sp_droplogin 'учетная запись'	Удаляет учетную запись SQL Server
Sp_password 'старый пароль', 'новый пароль', 'учетная запись'	Добавляет и изменяет пароль
Sp_defaultdb 'учетная запись', 'база данных'	Изменяет БД, установленную по умолчанию для данной записи
Sp_defaultlanguage 'учетная запись', 'язык'	Изменяет язык, установленный по умолчанию

Роли сервера

- Системные хранимые процедуры, используемые для добавления и удаления участника роли сервера. Только участники роли sysadmin могут добавлять учетные записи к любой роли.

Системная хранимая процедура	Описание
Sp_addsrvrolemember 'учетная запись', 'роль'	Добавляет учетную запись, как участника роли сервера
Sp_dropsrvrolemember 'учетная запись', 'роль'	Удаляет учетную запись как участника роли сервера

Доступ к базе данных

- Системные хранимые процедуры для добавления и удаления учетных записей для доступа к БД. Могут выполняться только участниками роли db_accessadmin и db_owner

Системная хранимая процедура	Описание
Sp_grantdbaccess 'учетная запись', 'имя в БД'	Добавляет учетную запись в качестве пользователя БД
Sp_revokedbaccess 'имя'	Удаляет учетную запись как пользователя БД

Роли базы данных

- Системные хранимые процедуры для изменения владельца БД, добавления и удаления регистрационных записей.

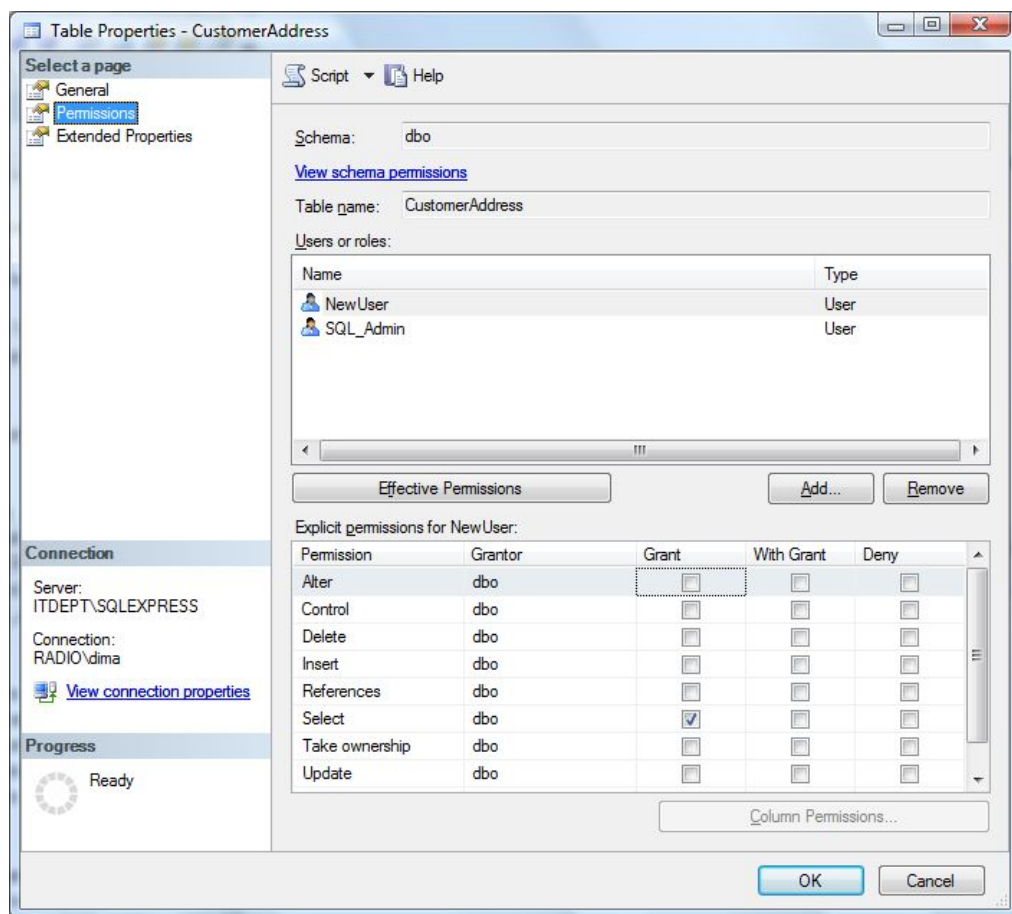
Системная хранимая процедура	Описание
Sp_changedbowner 'учетная запись'	Изменяет владельца БД (выполнять имеет право sysadmin)
Sp_addrolemember 'роль', 'регистрационная запись'	Добавляет регистрационную запись к роли БД
Sp_droprolemember 'роль', 'регистрационная запись'	Удаляет регистрационную запись из роли БД
Sp_addrole 'роль', 'владелец'	Создание новой роли в текущей БД
Sp_droprole ''	Удалять роль, определенную пользователем

Просмотр информации о правах доступа

- Системные хранимые процедуры, возвращающие информацию о правах доступа

Системная хранимая процедура	Описание
Sp_helplogins ['учетная запись']	Выводит информацию обо всех или определенной учетной записи
Sp_helpsrvrolemember ['роль']	Выводит информацию обо всех или определенной роли и ее участниках
Sp_helpuser ['регистрац_запись']	Выводит информацию обо всех или определенном пользователе
Sp_helprolemember ['роль']	Выводит информацию обо всех ролях или обо всех участниках определенной роли
Sp_helpntgroup ['имя']	Выводит информацию обо всех или определенной группе Windows

Установка разрешений на объекты базы данных



Установка разрешений на объекты базы данных средствами T-SQL

- Для установки разрешений можно воспользоваться оператором T-SQL
- Пример устанавливает разрешение выборки (SELECT) для таблицы CustomerAddress пользователю NewUser:
 - `GRANT SELECT ON OBJECT::dbo.CustomerAddress TO NewUser;`