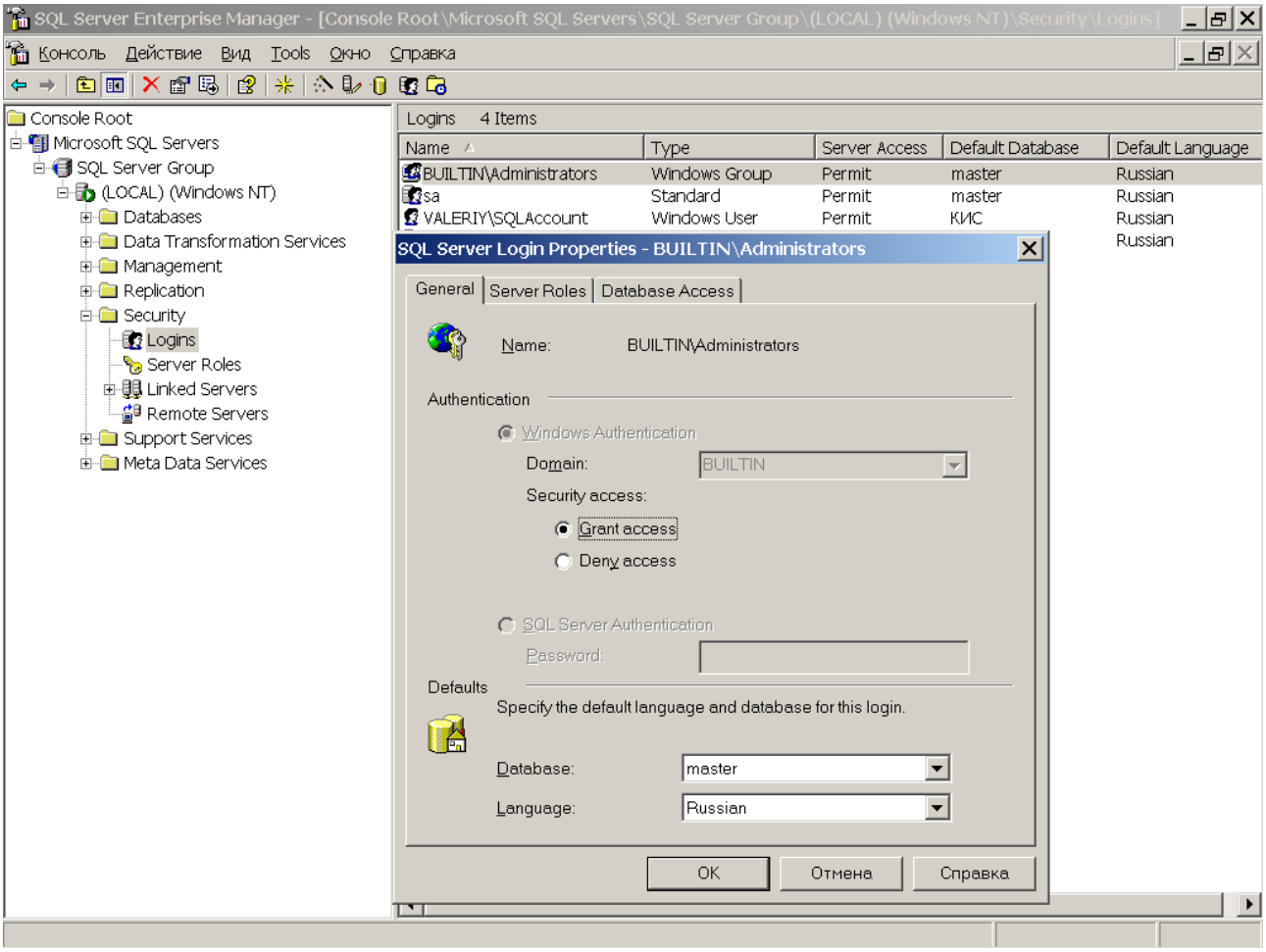
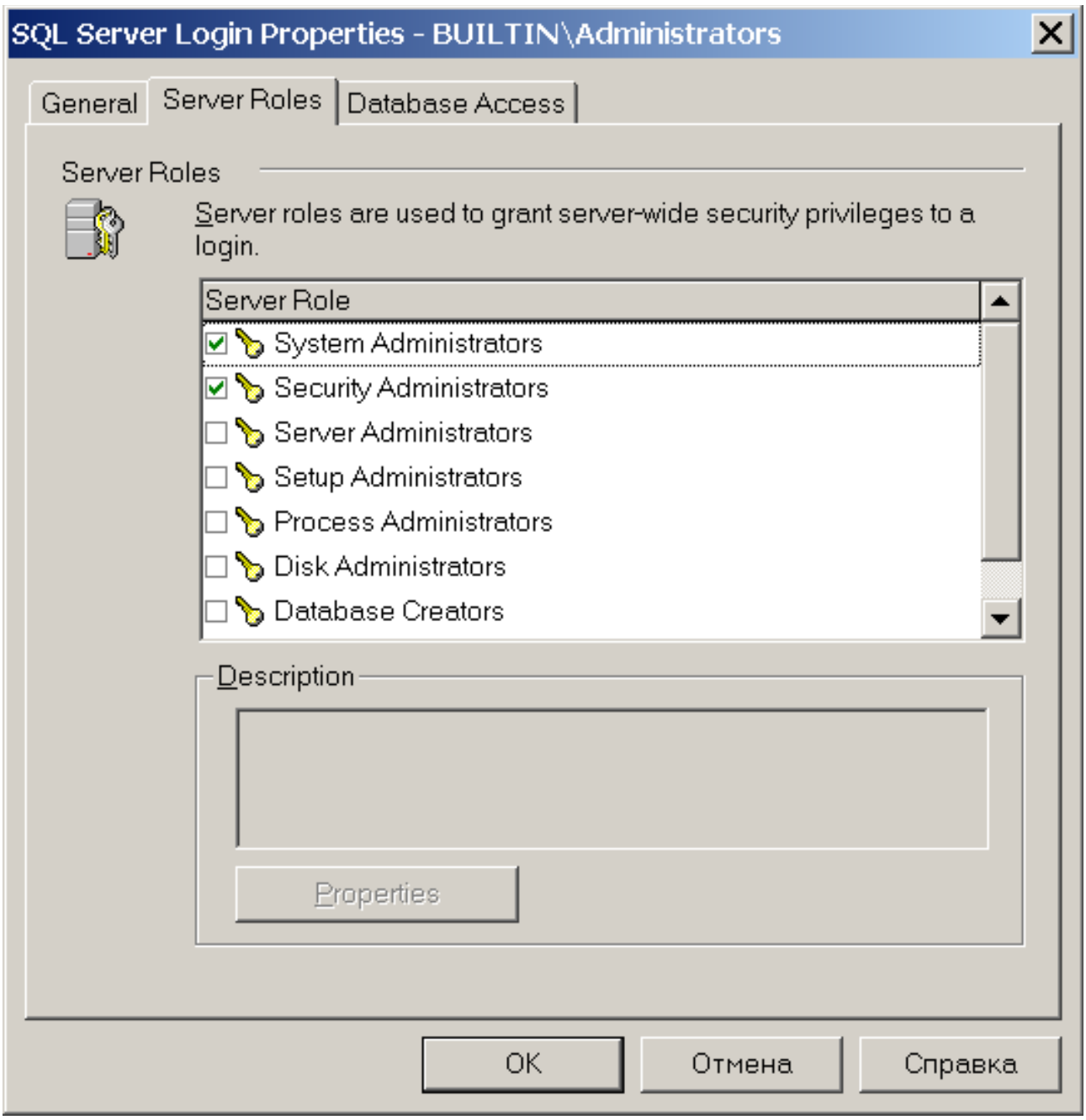
Архитектура системы безопасности СУБД SQL Server 2000

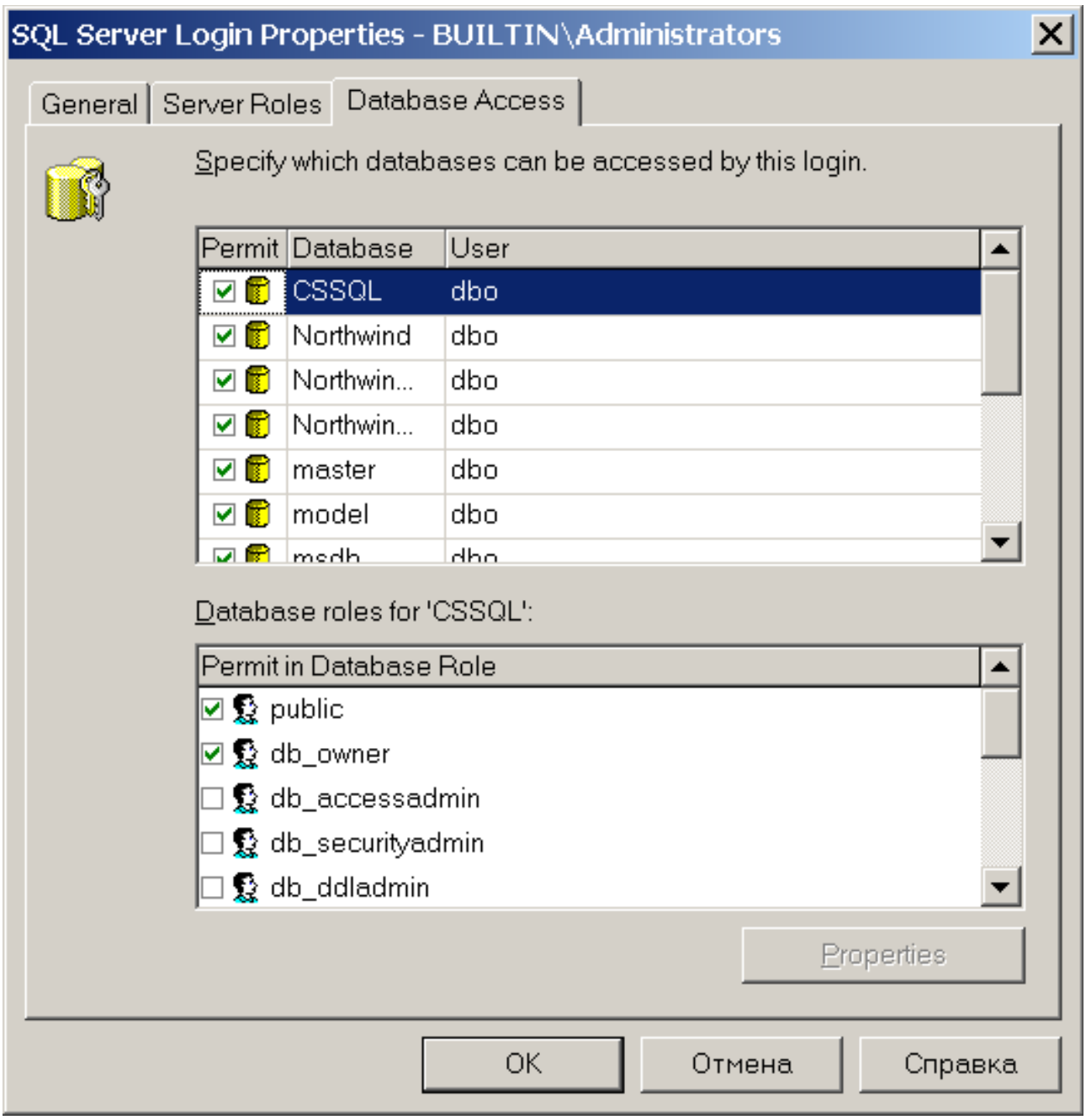
На уровне сервера система безопасности оперирует следующими понятиями: аутентификация, учетная запись (логин), роль сервера.
Сервер может работать в двух режимах аутентификации – Windows NT и SQL Server. В режиме Windows NT сервер для идентификации пользователя использует учетную запись пользователя (группы пользователей) Windows. В режиме аутентификации SQL Server пользователю для подключения к серверу требуется дополнительно пройти процедуру идентификации с указанием своего логина и пароля, зарегистрированных на сервере.

После прохождения аутентификации пользователь получает доступ к серверу. При этом его учетная запись (учетная запись Windows, учетная запись группы Windows, или учетная запись SQL Server) может быть использована в той или иной роли сервера.
В СУБД имеются две стандартные учетные записи:

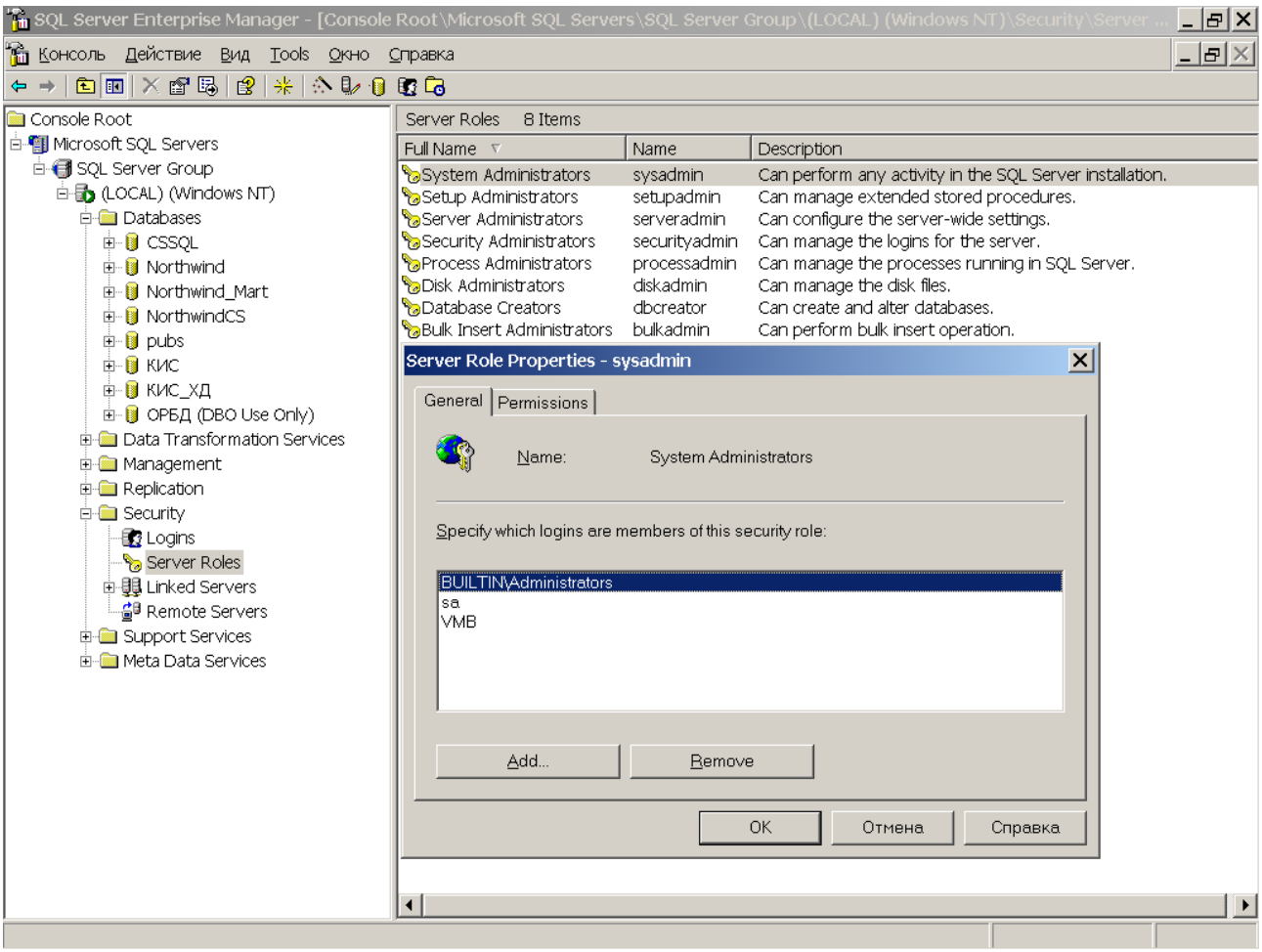
- BUILTIN\Administrators – это учетная запись Windows, обеспечивающая автоматический доступ всем членам группы Administrators к SQL Server, и являющаяся по умолчанию членом встроенной роли сервера sysadmin. Таким образом, системные администраторы получают полный доступ к серверу и ко всем БД.
- sa – специальная учетная запись для администратора, по умолчанию присвоена системной роли сервера sysadmin.

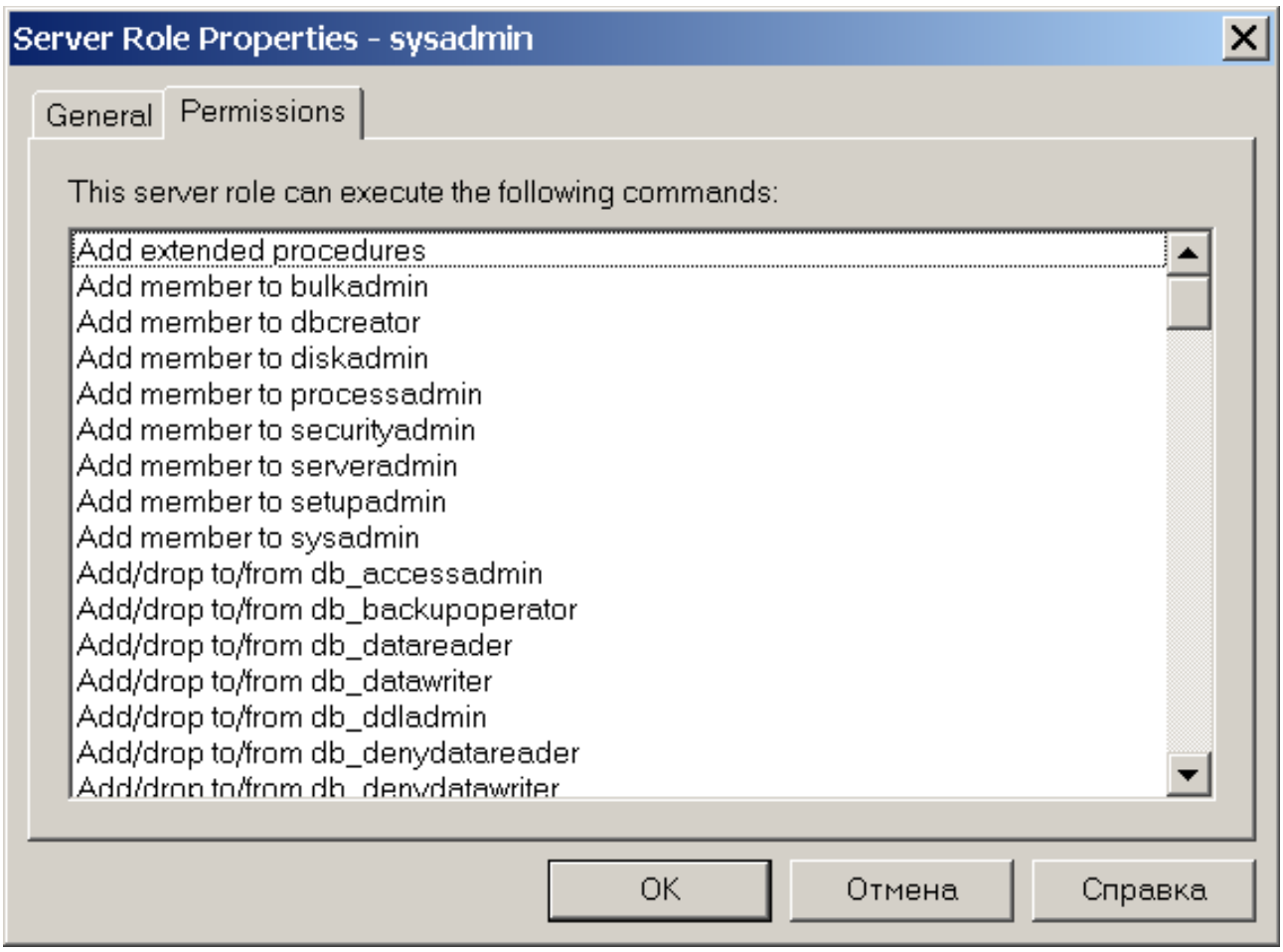

SQL Server Enterprise Manager - [Console Root\Microsoft SQL Servers\SQL Server Group\(LOCAL) (Windows NT)\Security\Logins]
Консоль Действие Вид Tools Окно Справка
Console Root
Microsoft SQL Servers
SQL Server Group
(LOCAL) (Windows NT)
Databases
Data Transformation Services
Management
Replication
Security
Logins
Server Roles
Linked Servers
Remote Servers
Support Services
Meta Data Services
Logins 4 Items
Name Type Server Access Default Database Default Language
BUILTIN\Administrators Windows Group Permit master Russian
sa Standard Permit master Russian
VALERIY\SQLAccount Windows User Permit КИС Russian
Russian
SQL Server Login Properties - BUILTIN\Administrators
General Server Roles Database Access
Name: BUILTIN\Administrators
Authentication
Windows Authentication
Domain: BUILTIN
Security access:
Grant access
Deny access
SQL Server Authentication
Password:
Defaults
Specify the default language and database for this login.
Database: master
Language: Russian
OK Отмена Справка


SQL Server Login Properties - BUILTIN\Administrators
General
Server Roles
Database Access
Server Roles
Server roles are used to grant server-wide security privileges to a login.
Server Role
System Administrators
Security Administrators
Server Administrators
Setup Administrators
Process Administrators
Disk Administrators
Database Creators
Description
Properties
OK
Отмена
Справка



В SQL Server существует 9 фиксированных ролей сервера:


SQL Server Enterprise Manager - [Console Root\Microsoft SQL Servers\SQL Server Group\(LOCAL) (Windows NT)\Security\Server ...
Консоль Действие Вид Tools Окно Справка
Console Root
Microsoft SQL Servers
SQL Server Group
(LOCAL) (Windows NT)
Databases
CSSQL
Northwind
Northwind_Mart
NorthwindCS
pubs
КИС
КИС_ХД
ОРБД (DBO Use Only)
Data Transformation Services
Management
Replication
Security
Logins
Server Roles
Linked Servers
Remote Servers
Support Services
Meta Data Services
Server Roles 8 Items
Full Name
Name
Description
System Administrators sysadmin Can perform any activity in the SQL Server installation.
Setup Administrators setupadmin Can manage extended stored procedures.
Server Administrators serveradmin Can configure the server-wide settings.
Security Administrators securityadmin Can manage the logins for the server.
Process Administrators processadmin Can manage the processes running in SQL Server.
Disk Administrators diskadmin Can manage the disk files.
Database Creators dbcreator Can create and alter databases.
Bulk Insert Administrators bulkadmin Can perform bulk insert operation.
Server Role Properties - sysadmin
General
Permissions
Name: System Administrators
Specify which logins are members of this security role:
BUILTIN\Administrators
sa
VMB
Add...
Remove
OK
Отмена
Справка



На уровне базы данных используются понятия:

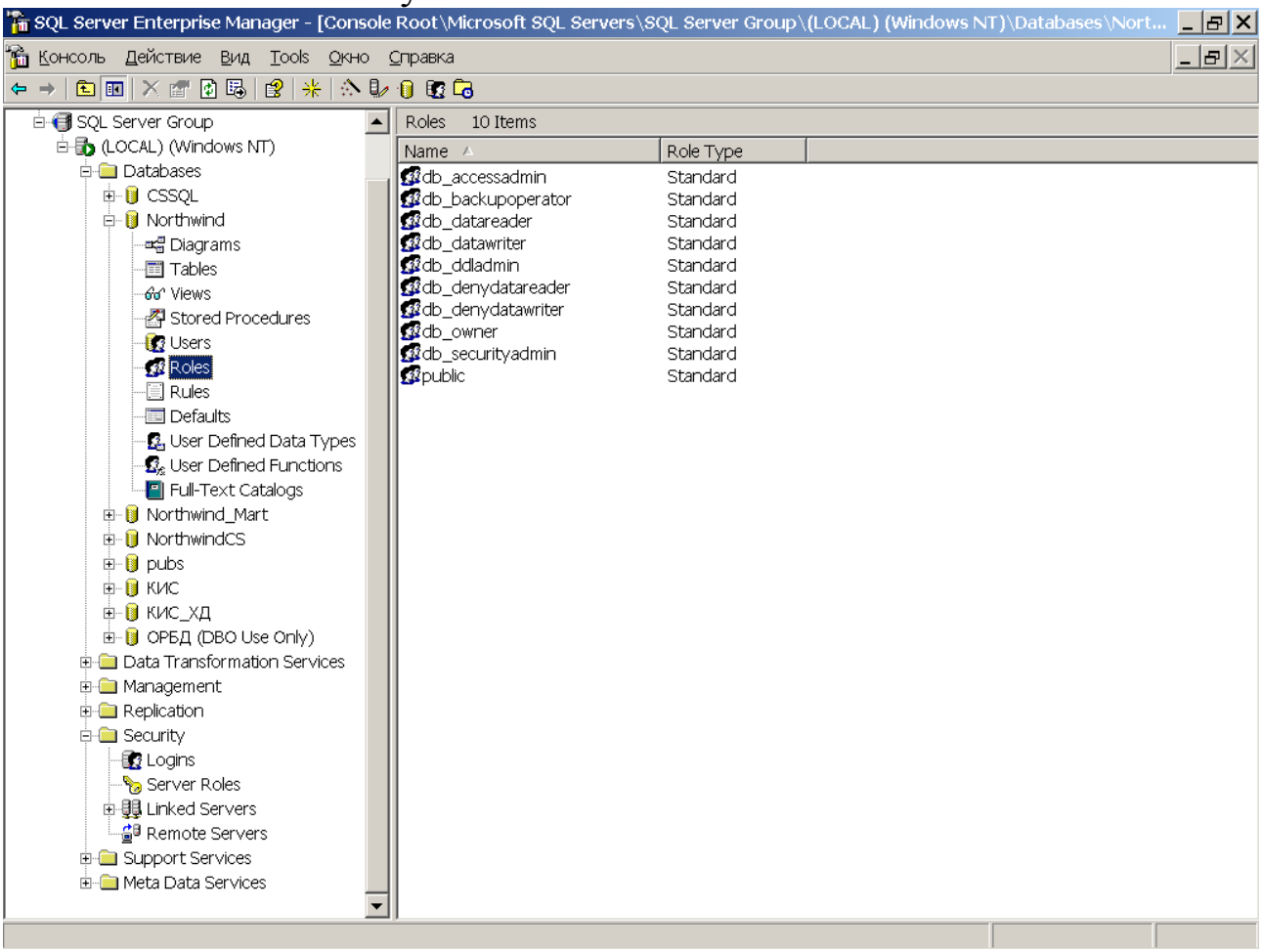
- пользователь базы данных;
- фиксированная роль БД;
- пользовательская роль БД;
- роль приложения.

После аутентификации на сервере учетная запись пользователя также отображается в пользователя базы данных. Подобное отображение необходимо для каждой БД, доступ к которой хочет получить пользователь. Пользователи БД, в свою очередь, могут быть объединены в группы и роли. Если учетная запись не отображена в пользователя БД, то клиент все-таки может получить доступ к БД под гостевым именем guest, если оно имеется в БД.

Владелец БД (DataBase Owner, dbo) – специальный пользователь, обладающий максимальными правами в БД. Любой член роли sysadmin автоматически отображается в пользователя dbo.

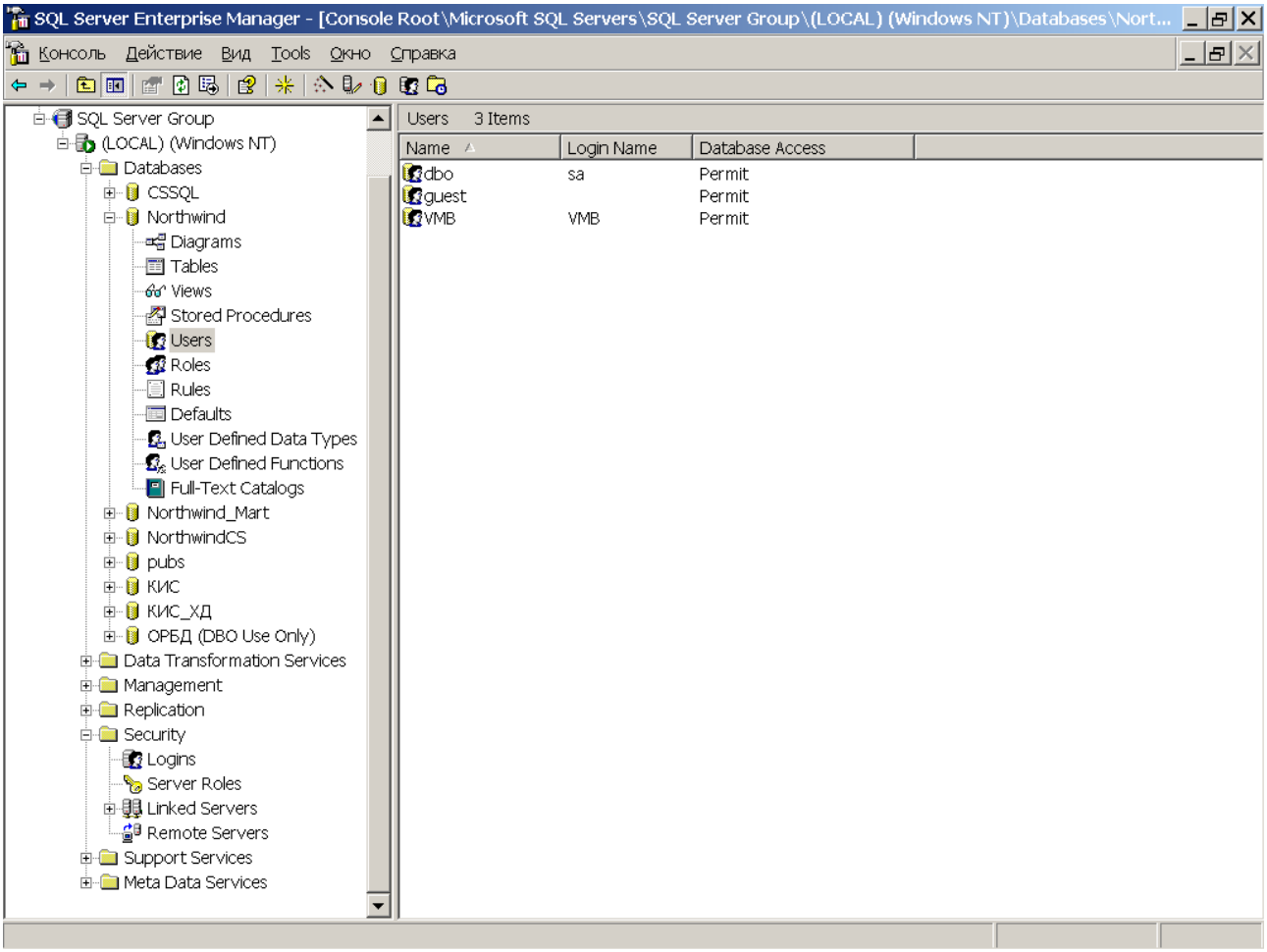
Роли БД позволяют объединить пользователей в административные единицы и работать с ними как с одним пользователем. Если назначить права доступа к объектам БД для конкретной роли, то автоматически все члены этой роли одинаково получат эти права. В роль БД можно включать пользователей SQL Server, роли SQL Server,

пользователей и группы Windows. При создании БД для нее определяются 10 стандартных ролей, которые, как и роли сервера, изменены быть не могут:



db_owner – создатель БД, имеет все права в БД,
db_accessadmin – может добавлять и удалять пользователей,
db_securityadmin – управляет пользователями, разрешениями и ролями,
db_ddladmin – может выполнять любые команды ddl, кроме GRAND, DENY, REVOKE,
db_backupoperator – может управлять созданием резервных копий,
db_datareader – может просматривать любые данные в любой таблице,
db_datawriter – может изменять любые данные в любой таблице,
db_denydatareader – запрет на просмотр данных в любой таблице,
db_denydatawriter – запрет на изменение данные в любой таблице,
public – включает в себя всех пользователей, включая guest.
Кроме стандартных ролей существуют роли приложения, для которой обязательно должны быть определены имя и пароль, которые будут использовать приложения, подключающиеся к БД. Для подключения

и активизации таких ролей приложение должно использовать хранимую процедуру:
sp_setuprole ‘NameRole’ ‘Password’ ‘encrypt_style’
где ‘NameRole’ – имя роли; ‘Password’ – пароль; ‘encrypt_style’ – схема шифрования: ‘none’ или ‘odbc’.



5.1 Управление правами доступа в SQL Server.

Права в SQL Server можно разделить на 3 категории:

- права на доступ к объектам БД;
- права на выполнение команд T-SQL;
- неявные права.

Неявные права не предоставляются пользователю непосредственно, он получает их при определенных обстоятельствах. Так, сразу после создания новый пользователь не имеет ни каких прав, кроме тех которые разрешены для роли public. С другой стороны, создав БД, пользователь становится ее полновластным хозяином.
Права выдаются пользователю (или роли БД, в которую он входит) администратором или владельцем БД. Для различных объектов БД применяются различные наборы прав доступа:

- SELECT, INSERT, UPDATE, DELETE, REFERENCES – для таблиц и представлений,
- SELECT, UPDATE – для столбцов таблиц и представлений,
- EXECUTE – для хранимых процедур.

Предоставлять или отключать права можно при помощи встроенных ролей БД. Например, для предоставлению пользователю права чтения данных из всех таблиц БД, достаточно включить его в роль БД db_datareader.

Синтаксис оператора предоставления разрешений на языке T-SQL:

GRANT {ALL [PRIVILEGES] | разрешение1, …}
[колонка1, …]
{ON Таблица | Представление } | {ON ХранимаяПроцедура | ВнешняяПроцедура}
TO ИмяПользователя | Роль
[WITH GRANT OPTION]
[AS ИмяПользователя | Роль]

разрешение1, … – список представляемых прав доступа.

WITH GRANT OPTION – опция с помощью которой, можно предоставить не только право доступа к объекту, но и право передавать это право другим пользователям.

AS ИмяПользователя | Роль – указание участия передающего право в роли, имеющей соответствующую возможность.

Право на выполнение команд DDL-SQL предоставляется с помощью команды

GRANT {ALL | Create_Object}
TO ИмяПользователя | Роль
[WITH GRANT OPTION]
[AS ИмяПользователя | Роль]

Запрещение доступа к объектам осуществляется командой

DENY {ALL [PRIVILEGES] | разрешение1, …}
[колонка1, …]
{ON Таблица | Представление } | {ON ХранимаяПроцедура | ВнешняяПроцедура}
FROM ИмяПользователя | Роль
[CASCADE]
[AS ИмяПользователя | Роль]

А запрещение выполнения команд DDL-SQL – с помощью команды

DENY {ALL | Create_Object}
TO ИмяПользователя | Роль
[CASCADE]
[AS ИмяПользователя | Роль]

Параметр CASCADE позволяет отозвать права не только у конкретного пользователя, но и у тех пользователей, которым он успел передать это право.

Запрещение доступа к объектам для конкретного пользователя выполняется независимо от разрешений на более высоком уровне иерархии, и, наоборот, запрещение доступа на уровне группы или роли приводит к запрещению доступа для всех пользователей этой группы (роли).

В SQL Server возможно неявное отклонение доступа с помощью команды REVOKE, имеющей синтаксис, аналогичный DENY. Эта команда запрещает доступ к объектам для той или иной роли, но оставляет его для тех ее членов, которым доступ был определен явно. Т.е. для отмены прав у таких пользователей команды DENY или REVOKE должны быть применены к ним так же явно.