Server and Database Roles in SQL Server

03/30/20173 minutes to readContributors all

In this article

All versions of SQL Server use role-based security, which allows you to assign permissions to a role, or group of users, instead of to individual users. Fixed server and fixed database roles have a fixed set of permissions assigned to them.

Fixed Server Roles

Fixed server roles have a fixed set of permissions and server-wide scope. They are intended for use in administering SQL Server and the permissions assigned to them cannot be changed. Logins can be assigned to fixed server roles without having a user account in a database.

> **Important**
>
> The `sysadmin` fixed server role encompasses all other roles and has unlimited scope. Do not add principals to this role unless they are highly trusted. `sysadmin` role members have irrevocable administrative privileges on all server databases and resources.

Be selective when you add users to fixed server roles. For example, the `bulkadmin` role allows users to insert the contents of any local file into a table, which could jeopardize data integrity. See SQL Server Books Online for the complete list of fixed server roles and permissions.

Fixed Database Roles

Fixed database roles have a pre-defined set of permissions that are designed to allow you to easily manage groups of permissions. Members of the `db_owner` role can perform all configuration and maintenance activities on the database.

For more information about SQL Server predefined roles, see the following resources.

Resource	Description

Resource	Description
Server-Level Roles and Permissions of Fixed Server Roles in SQL Server Books Online	Describes fixed server roles and the permissions associated with them in SQL Server.
Database-Level Roles and Permissions of Fixed Database Roles in SQL Server Books Online	Describes fixed database roles and the permissions associated with them

Database Roles and Users

Logins must be mapped to database user accounts in order to work with database objects. Database users can then be added to database roles, inheriting any permission sets associated with those roles. All permissions can be granted.

You must also consider the `public` role, the `dbo` user account, and the `guest` account when you design security for your application.

The public Role

The `public` role is contained in every database, which includes system databases. It cannot be dropped and you cannot add or remove users from it. Permissions granted to the `public` role are inherited by all other users and roles because they belong to the `public` role by default. Grant `public` only the permissions you want all users to have.

The dbo User Account

The `dbo`, or database owner, is a user account that has implied permissions to perform all activities in the database. Members of the `sysadmin` fixed server role are automatically mapped to `dbo`.

Note

`dbo` is also the name of a schema, as discussed in Ownership and User-Schema Separation in SQL Server.

The `dbo` user account is frequently confused with the `db_owner` fixed database role. The scope of `db_owner` is a database; the scope of `sysadmin` is the whole server. Membership in the `db_owner` role does not confer `dbo` user privileges.

The guest User Account

After a user has been authenticated and allowed to log in to an instance of SQL Server, a separate user account must exist in each database the user has to access. Requiring a user account in each database prevents users from connecting to an instance of SQL Server and accessing all the databases on a server. The existence of a `guest` user account in the database circumvents this requirement by allowing a login without a database user account to access a database.

The `guest` account is a built-in account in all versions of SQL Server. By default, it is disabled in new databases. If it is enabled, you can disable it by revoking its CONNECT permission by executing the Transact-SQL REVOKE CONNECT FROM GUEST statement.

> **Important**
>
> Avoid using the `guest` account; all logins without their own database permissions obtain the database permissions granted to this account. If you must use the `guest` account, grant it minimum permissions.

For more information about SQL Server logins, users and roles, see the following resources.

Resource	Description
Identity and Access Control in SQL Server Books Online	Contains links to topics that describe principals, roles, credentials, securables and permissions.
Principals in SQL Server Books Online	Describes principals and contains links to topics that describe server and database roles.

See Also

Securing ADO.NET Applications
Application Security Scenarios in SQL Server
Authentication in SQL Server
Ownership and User-Schema Separation in SQL Server

Authorization and Permissions in SQL Server
ADO.NET Managed Providers and DataSet Developer Center