Microsoft SQL Server vNext and Azure SQL Database
Database Engine Permissions

Permission Syntax
Most permission statements have the format :

AUTHORIZATION PERMISSION ON SECURABLE::NAME TO PRINCIPAL

- AUTHORIZATION must be GRANT, REVOKE or DENY.
- PERMISSION is listed in the charts below.
- ON SECURABLE::NAME is the server, server object, database, or database object and its name. (ON SECURABLE::NAME is omitted for server-wide and database-wide permissions.)
- PRINCIPAL is the login, user, or role which receives or loses the permission. Grant permissions to roles whenever possible.

Sample grant statement: GRANT UPDATE ON OBJECT::Production.Parts TO PartsTeam

Denying a permission at any level, overrides a related grant.

To remove a previously granted permission, use REVOKE, not DENY.

How to Read this Chart
- Most of the more granular permissions are included in more than one higher level scope permission. So permissions can be inherited from more than one type of higher scope.
- Black, green, and purple arrows and boxes point to subordinate permissions that are included in the scope of higher a level permission.
- Brown arrows and boxes indicate some of the statements that can use the permission.
- Permissions in black apply to both SQL Server 2016 and Azure SQL Database
- Permissions in red apply only to SQL Server 2016
- Permissions marked with ‡ apply to SQL Server vNext and Azure SQL Database
- Permissions in blue apply only to Azure SQL Database
- The newest permissions are underlined

NOTES:
- The CONTROL SERVER permission has all permissions on the instance of SQL Server or SQL Database.
- The CONTROL DATABASE permission has all permissions on the database.
- Permissions do not imply role memberships and role memberships do not grant permissions. (E.g. CONTROL SERVER does not imply membership in the sysadmin fixed server role. Membership in the db_owner role does not grant the CONTROL DATABASE permission.) However, it is sometimes possible to impersonate between roles and equivalent permissions.
- Granting any permission on a securable allows VIEW DEFINITION on that securable. It is an implied permissions and it cannot be revoked, but it can be explicitly denied by using the DENY VIEW DEFINITION statement.
- SQL Database permissions refer to version 12.
- Object owners can delete them but they do not have full permissions on them.
- A DENY on a table is overridden by a GRANT on a column. However, a subsequent DENY on the table will remove the column GRANT.

Azure SQL Database Permissions Outside the Database

Notes:
- Server-Level Principal Logins are the Server admin and Azure Active Directory Admin accounts
- Server-level permissions cannot be granted on SQL Database. Use the **loginmanager** and **dbmanager** roles in the master database instead.

Top Level Server Permissions

Server Level Permissions for SQL Server

Top Level Server Permissions

*** NOTE:** The SHUTDOWN statement requires the SQL Server SHUTDOWN permission, Starting, stopping, and pausing the Database Engine from SSCM, SSMS, or Windows requires Windows permissions, not SQL Server permissions.

public role

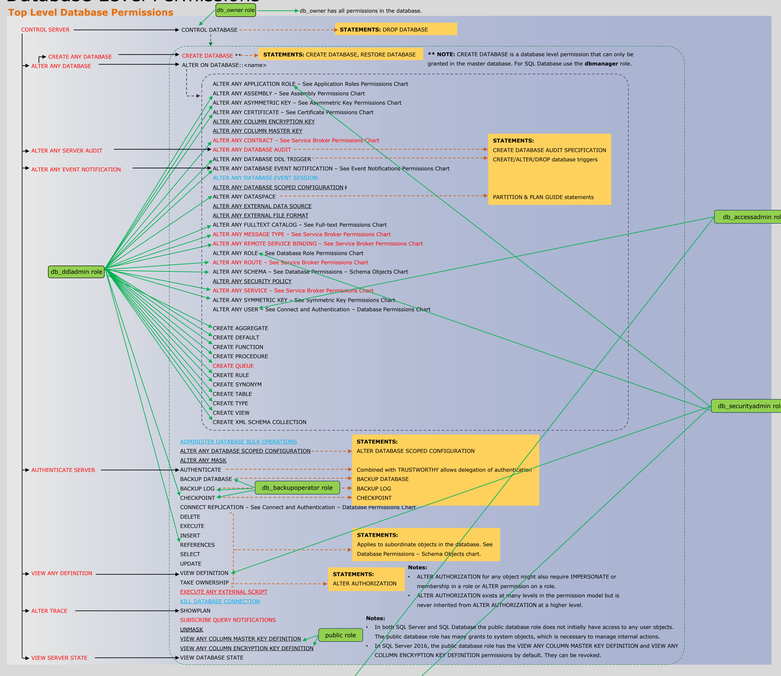
Connect and Authentication – Server Permissions

Server Role Permissions

Availability Group Permissions

Database Level Permissions

Top Level Database Permissions

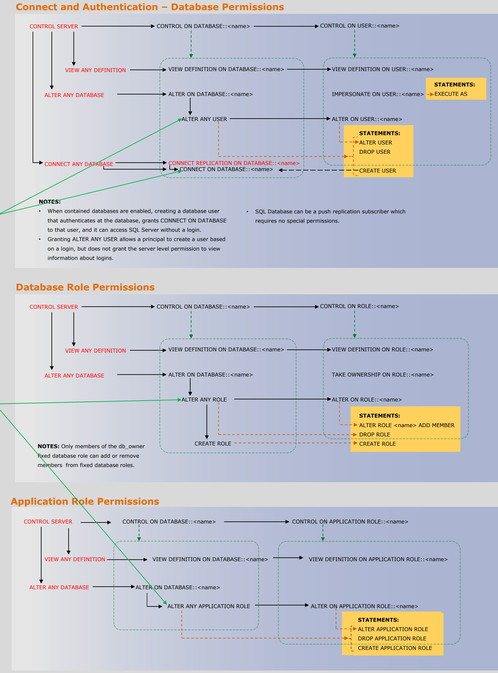


Database Permissions – Schema Objects

Notes:
- To create a schema object (such as a table) you must have CREATE permission for that object type plus ALTER ON SCHEMA::<name> for the schema of the object. Might require REFERENCES ON OBJECT::<name> for any referenced CLR type or XML schema collection.
- To alter an object (such as a table) you must have ALTER permission on the object (or schema), or CONTROL permission on the object.
- To drop an object (such as a table) you must have ALTER permission on the schema or CONTROL permission on the object.
- To create an index requires ALTER OBJECT::<name> permission on the table or view.
- To create or alter a trigger on a table or view requires ALTER OBJECT::<name> on the table or view.
- To create statistics requires ALTER OBJECT::<name> on the table or view.

Full-text Permissions

Connect and Authentication – Database Permissions



Database Role Permissions

Application Role Permissions

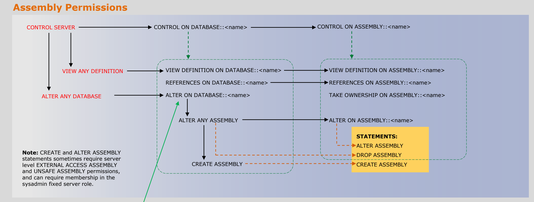
Symmetric Key Permissions

Asymmetric Key Permissions

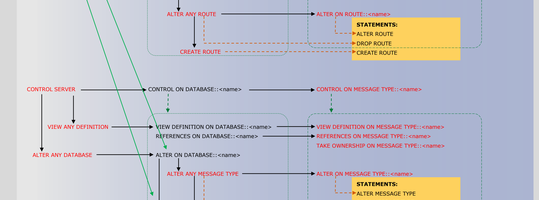
Certificate Permissions

Database Scoped Credential Permissions ‡

Assembly Permissions



Event Notification Permissions (SQL Server only)



Service Broker Permissions (SQL Server only)

Notes:
- The user executing the CREATE CONTRACT statement must have REFERENCES permission on all message types specified.
- The user executing the CREATE SERVICE statement must have REFERENCES permission on the queue and all contracts specified.
- To execute the CREATE REMOTE SERVICE BINDING the user must have REFERENCES permission on the service specified in the statement.
- When the CREATE or ALTER MESSAGE TYPE statement specifies a schema collection, the user executing the statement must have REFERENCES permission on the schema collection specified.
- See the ALTER ANY EVENT NOTIFICATION chart for more permissions related to Service Broker.
- See the SCHEMA OBJECTS chart for QUEUE permissions.
- The ALTER CONTRACT permission exists but at this time there is no ALTER CONTRACT statement.

Questions and comments to
Rick.Byham@Microsoft.com

Microsoft

January 19, 2017