Most permission statements have the format :

• PERMISSION is listed in the charts below.

require ON SECURABLE::NAME

How to Read this Chart

AUTHORIZATION must be GRANT, REVOKE or DENY.

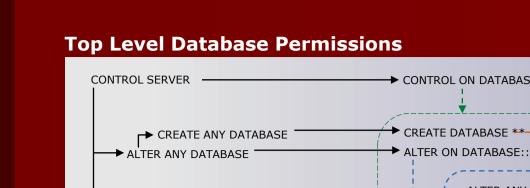
Denying a permission at any level, overrides a related grant.

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

SQL Server 2008 R2 Database Engine Permissions

Includes SQL Server Code Named 'Denali'

Database Level Permissions



Server Level Permissions

Brown arrows and boxes indicate some of the statements that can use the permission.

So permissions can be inherited from more than one type of higher scope.

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

Most of the more granular permissions are included in more than one higher level scope permission.

<u>AUTHORIZATION</u> <u>PERMISSION</u> <u>ON SECURABLE::NAME</u> <u>TO PRINCIPAL</u>

Top Level Server Permissions STATEMENTS: CREATE/ALTER/DROP server triggers OPENROWSET(BULK ... ALTER ANY AVAILABILITY GROUP - See Availability Group Permissions CREATE AVAILABILTY GROUP ALTER ANY CREDENTIAL - -CREATE/ALTER/DROP CREDENTIAL ALTER ANY DATABASE – See Database Permission Charts CREATE ANY DATABASE – See Top Level Database Permissions ALTER ANY ENDPOINT – See Connect and Authentication CREATE ENDPOINT – See Connect and Authentication ALTER ANY EVENT NOTIFICATION ------Server scoped event notifications Server scoped DDL event notifications CREATE TRACE EVENT NOTIFICATION -----ALTER ANY EVENT SESSION (New in SQL Server Code-named 'Denali') - - -> ALTER ANY LINKED SERVER ------ALTER ANY LOGIN – See Connect and Authentication CREATE/ALTER/DROP SERVER AUDIT and SERVER AUDIT SPECIFICATION ALTER ANY SERVER ROLE - See Server Role Permissions CREATE SERVER ROLE – See Server Role Permissions ALTER RESOURCES (Not used. Use diskadmin fixed server role instead.) DBCC FREE...CACHE and SQLPERF SELECT on server-level DMV's Allows server-level delegation CONNECT SQL – See Connect and Authentication UNSAFE ASSEMBLY EXTERNAL ACCESS ASSEMBLY

• ON SECURABLE::NAME is the server, server object, database, or database object and its name. Some permissions do not

• PRINCIPAL is the login, user, or role which receives or loses the permission. Grant permissions to roles whenever possible.

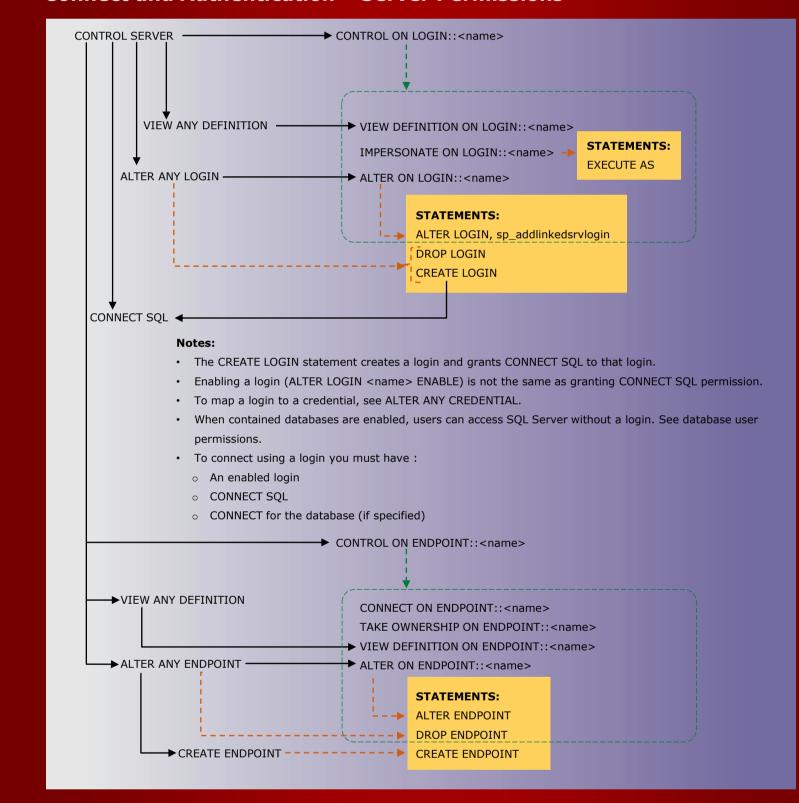
• Black, green, and blue arrows and boxes point to subordinate permissions that are included in the scope of higher a level

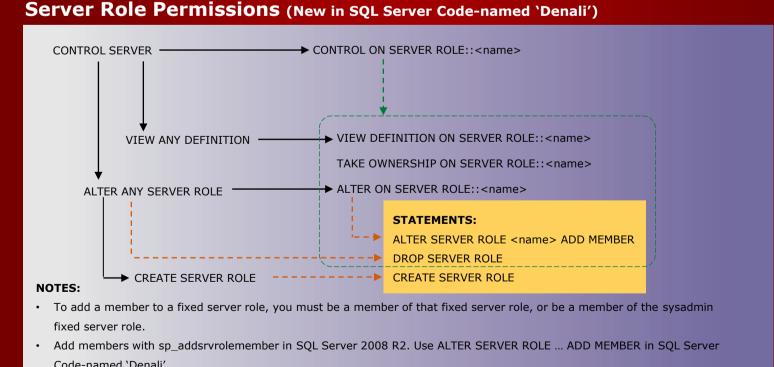
* NOTE: The SHUTDOWN statement requires the SQL Server SHUTDOWN permission. Starting, stopping, and pausing the Database Engine from SSCM, SSMS, or Windows requires Windows permissions, not SQL Server permissions.

► VIEW ANY DATABASE – See Database Permissions – Schema

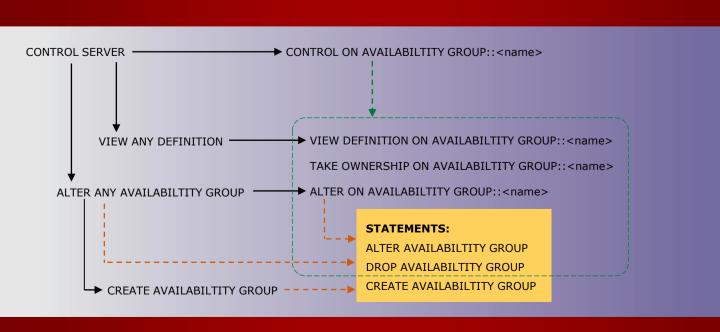
Connect and Authentication – Server Permissions

VIEW ANY DEFINITION





Availability Group Permissions (New in SQL Server Code-named 'Denali')



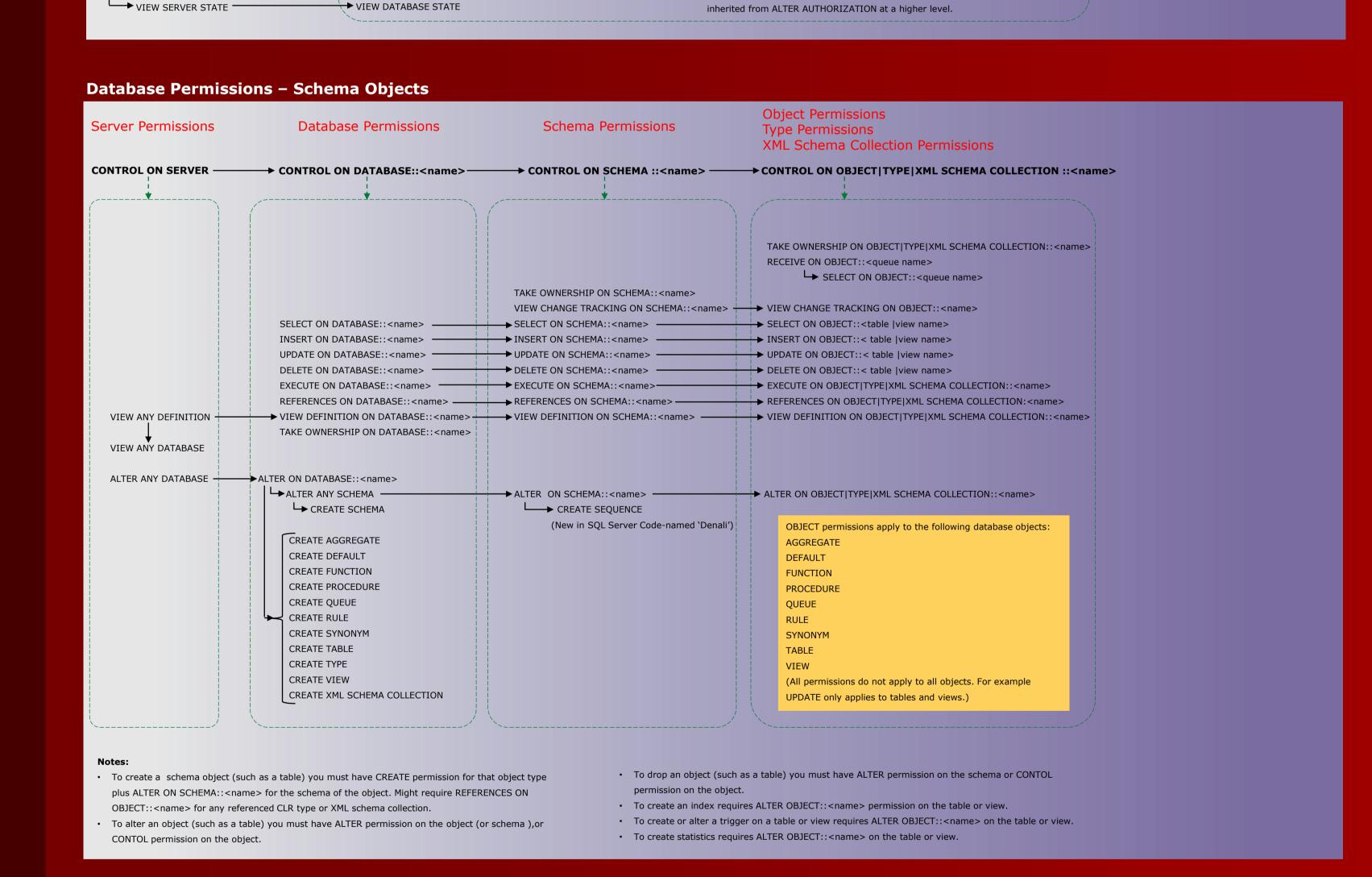


──► CONTROL ON DATABASE::<name> - - - - - - - - - STATEMENTS: DROP DATABASE CREATE DATABASE **----- STATEMENTS: CREATE DATABASE, RESTORE DATABASE ALTER ANY APPLICATION ROLE ALTER ANY ASSEMBLY

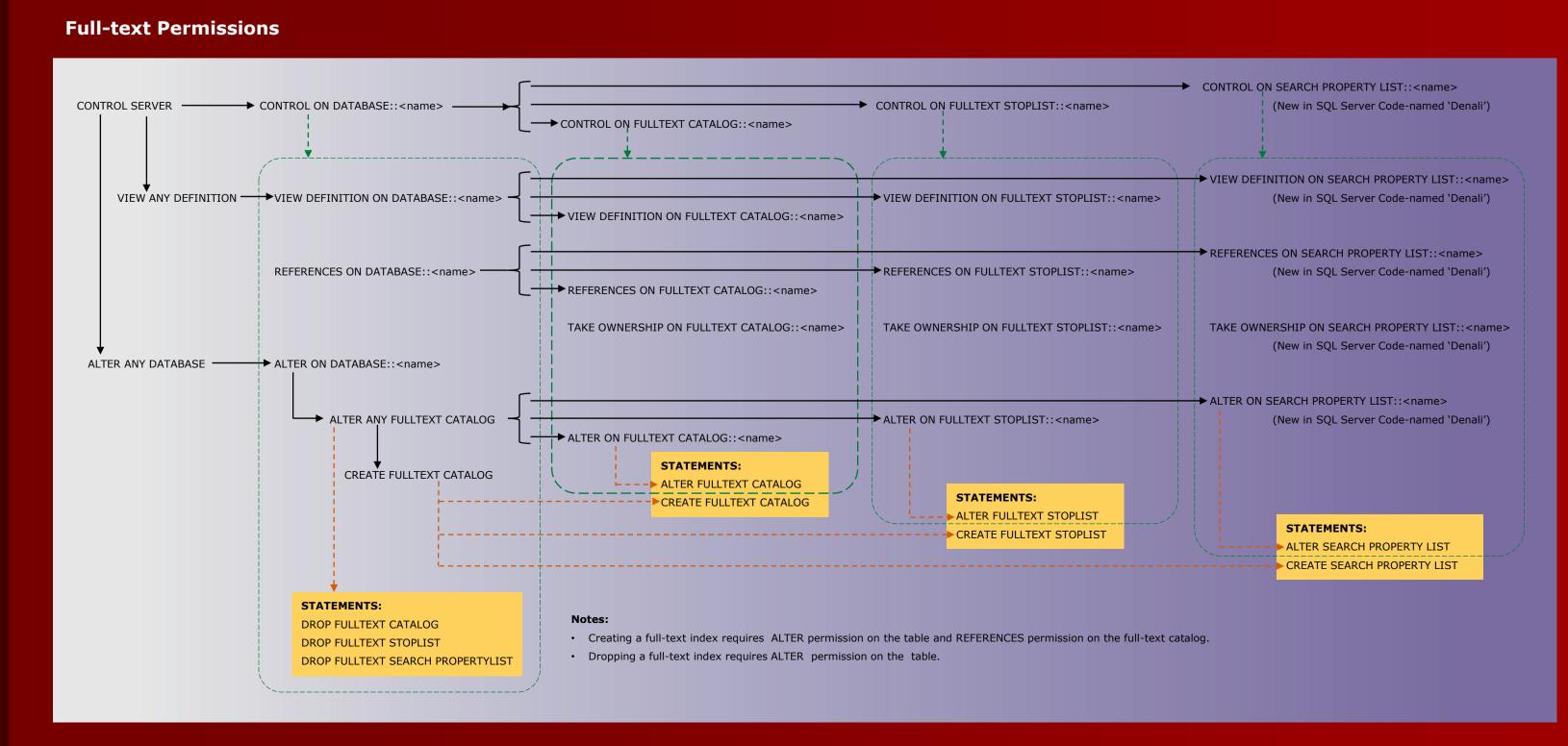
→ CREATE ASSEMBLY ALTER ANY ASYMMETRIC KEY — CREATE ASYMMETRIC KEY ALTER ANY CERTIFICATE
→ CREATE CERTIFICATE ALTER ANY DATABASE AUDIT -------CREATE DATABASE AUDIT SPECIFICATION ALTER ANY SERVER AUDIT ALTER ANY DATABASE DDL TRIGGER ------CREATE/ALTER/DROP database triggers → ALTER ANY DATABASE EVENT NOTIFICATION → CREATE DATABASE DDL EVENT NOTIFICATION ALTER ANY EVENT NOTIFICATION PARTITION & PLAN GUIDE statements ALTER ANY FULLTEXT CATALOG

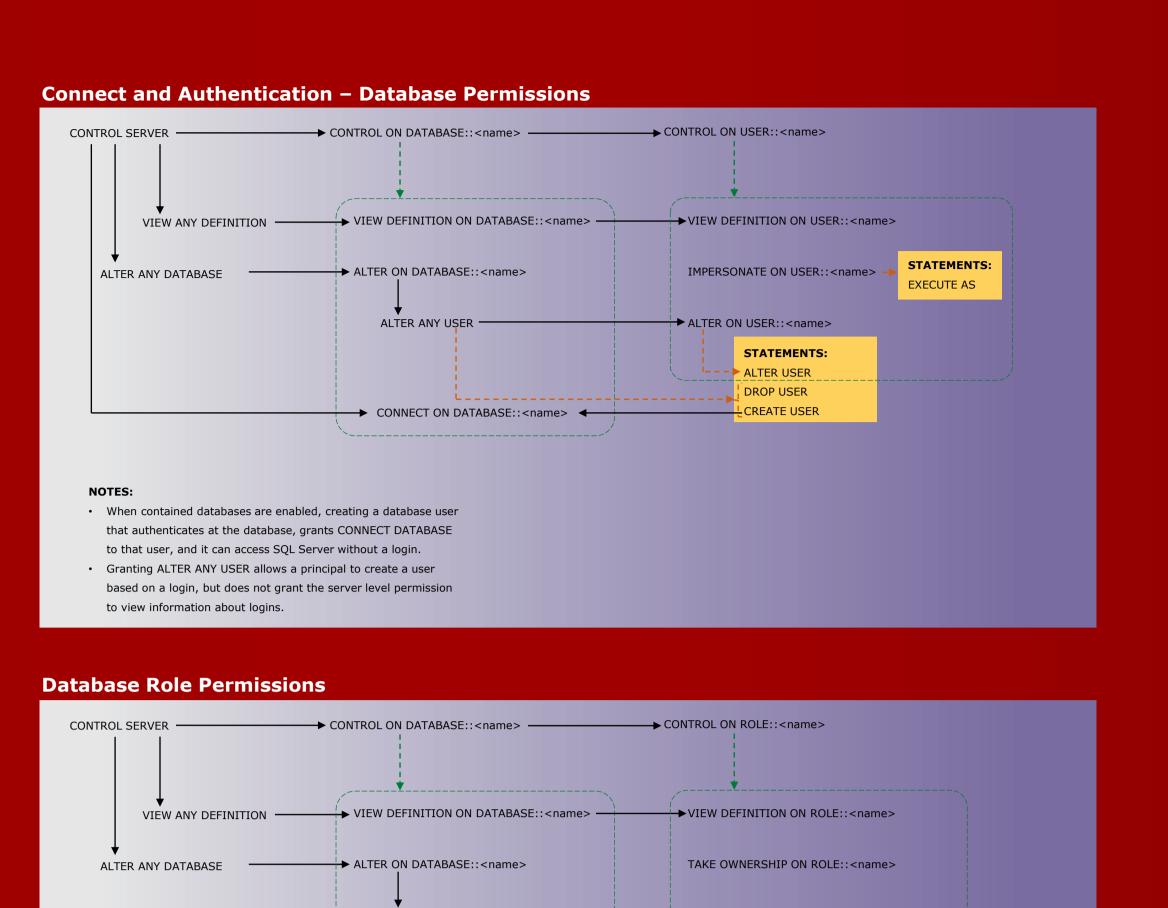
→ CREATE FULLTEXT CATALOG ALTER ANY MESSAGE TYPE CREATE MESSAGE TYPE ALTER ANY REMOTE SERVICE BINDING ———— CREATE REMOTE SERVICE BINDING ALTER ANY ROLE
→ CREATE ROLE ALTER ANY ROUTE

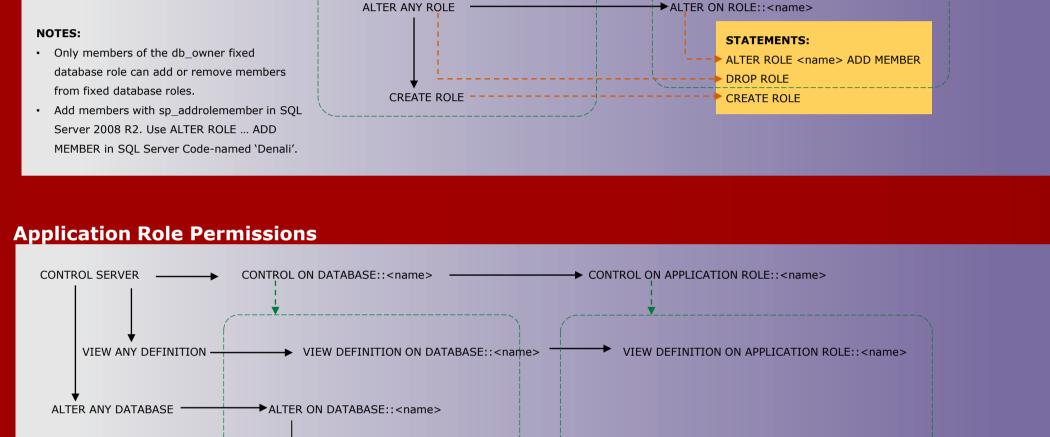
→ CREATE ROUTE ALTER ANY SCHEMA ← CREATE SCHEMA ALTER ANY SERVICE CREATE SERVICE ALTER ANY SYMMETRIC KEY
→ CREATE SYMMETRIC KEY ALTER ANY USER - See Connect and Authentication - Database Permissions Chart CREATE AGGREGATE CREATE DEFAULT CREATE FUNCTION CREATE PROCEDURE CREATE QUEUE CREATE RULE CREATE SYNONYM CREATE TABLE CREATE TYPE CREATE VIEW CREATE XML SCHEMA COLLECTION STATEMENTS: --- Combined with TRUSTWORTHY allows delegation of authentication → AUTHENTICATE AUTHENTICATE SERVER BACKUP DATABASE CONNECT REPLICATION CONNECT DATABASE EXECUTE Applies to subordinate objects in the database. See Database Permissions – Schema Objects chart. → VIEW ANY DEFINITION — ALTER AUTHORIZATION for any object might also require IMPERSONATE or SUBSCRIBE QUERY NOTIFICATIONS



ALTER AUTHORIZATION exists at many levels in the permission model but is never





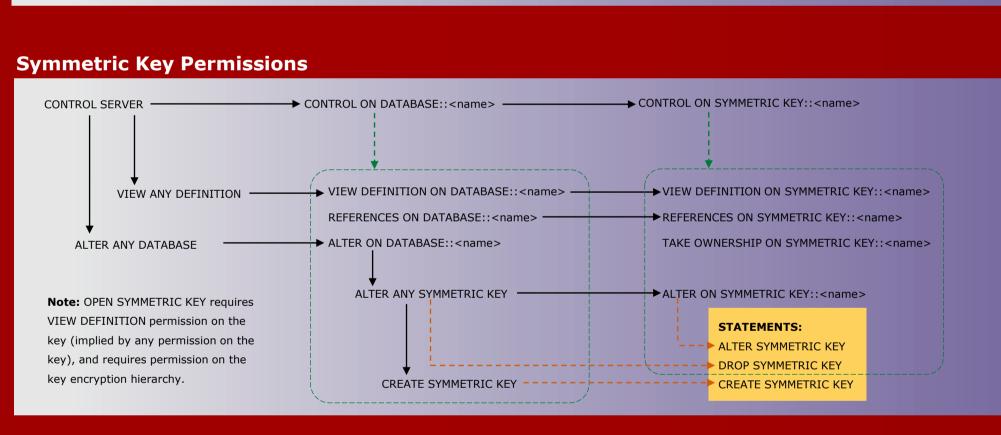


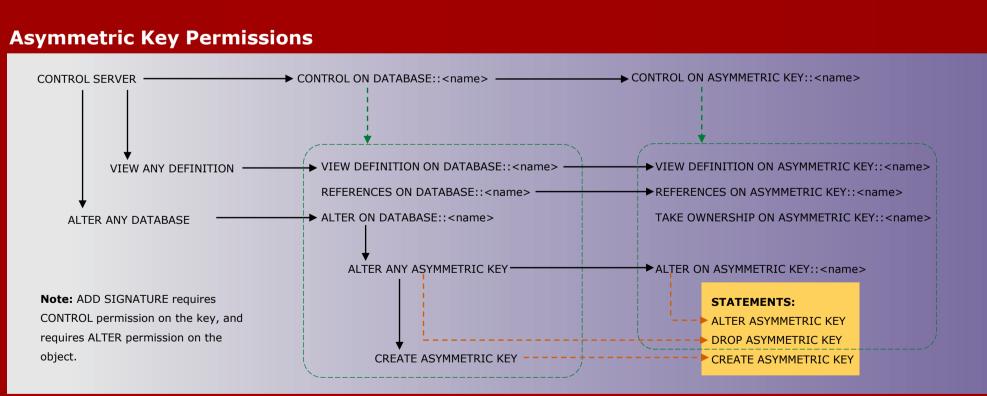
ALTER ANY APPLICATION ROLE ALTER ON APPLICATION ROLE::<name>

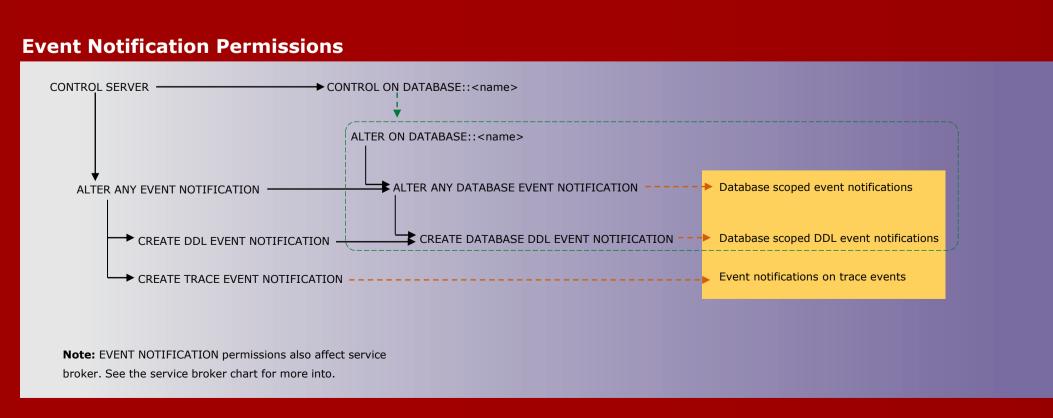
ALTER APPLICATION ROLE

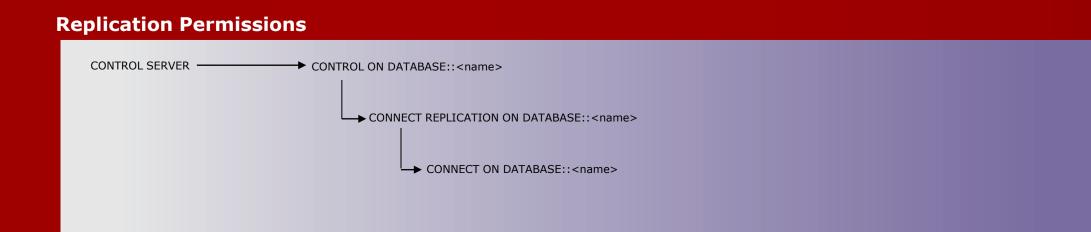
DROP APPLICATION ROLE

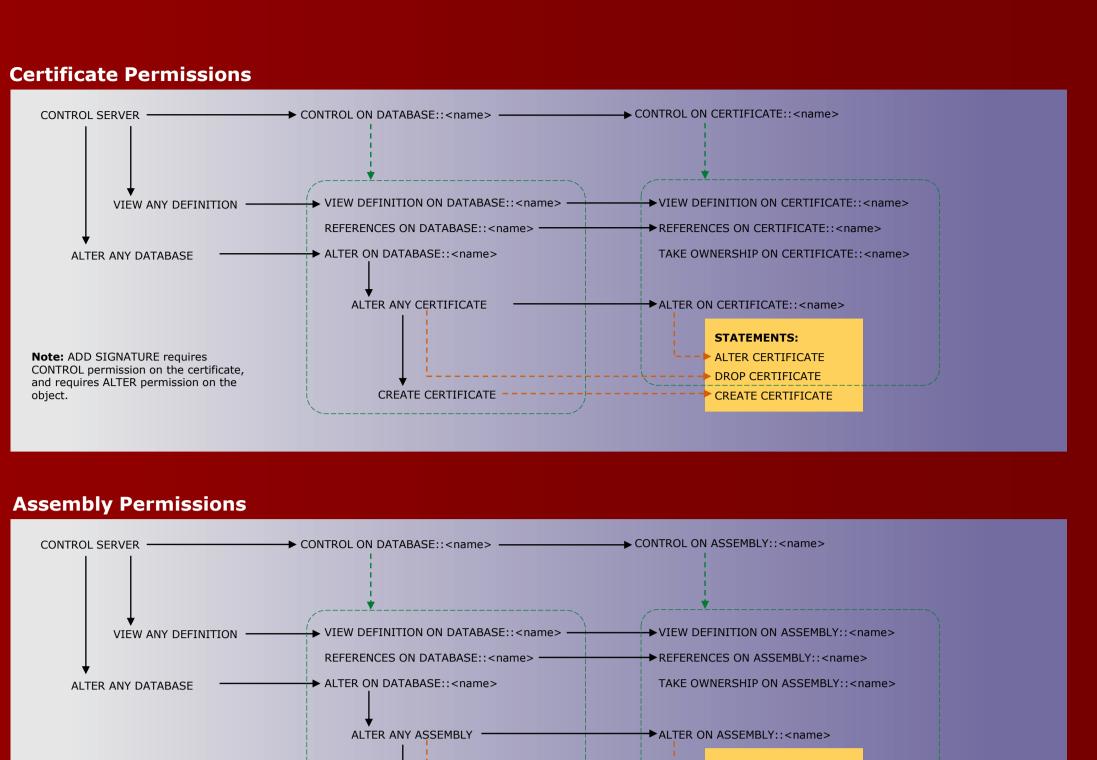
CREATE APPLICATION ROLE











STATEMENTS:

• 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

• 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

NOTES:

• The CONTROL SERVER permission has all permissions on the instance of SQL Server.

• The CONTROL DATABASE permission has all permissions on the database.

possible to impersonate between roles and equivalent permissions.

be explicitly denied by using the DENY VIEW DEFINITION statement.

