Permission Syntax

Most permission statements have the format: AUTHORIZATION PERMISSION ON SECURABLE::NAME TO PRINCIPAL

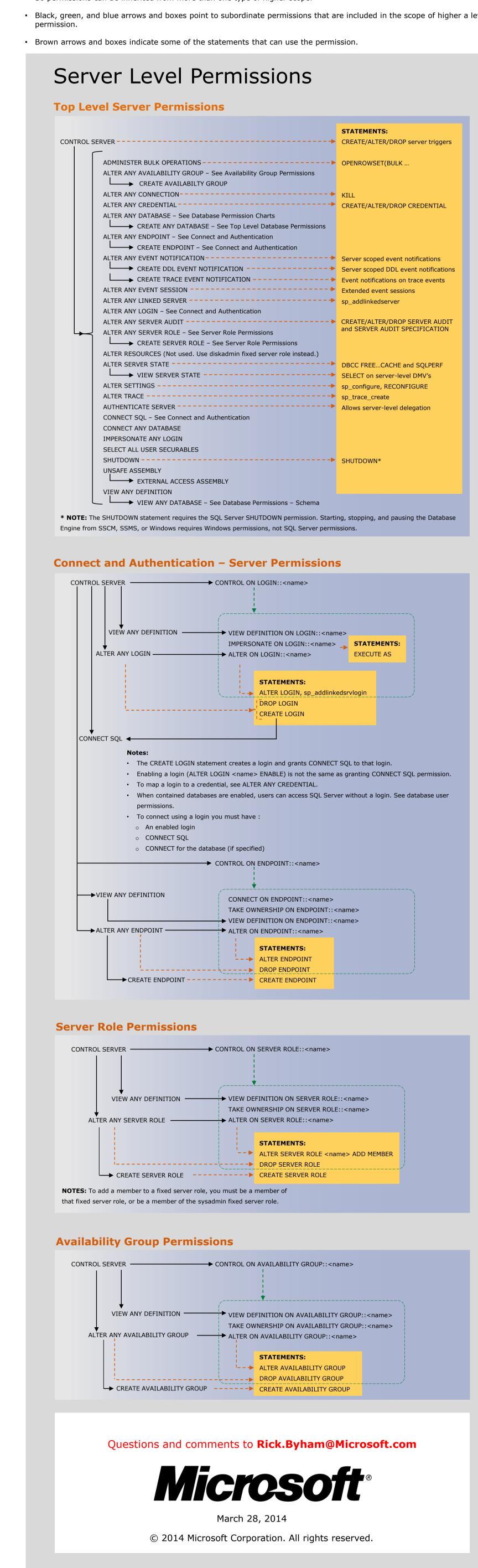
AUTHORIZATION must be GRANT, REVOKE or DENY.

- PERMISSION is listed in the charts below.
- ON SECURABLE::NAME is the server, server object, database, or database object and its name. Some permissions do not require ON SECURABLE::NAME.
- 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 blue arrows and boxes point to subordinate permissions that are included in the scope of higher a level



Microsoft SQL Server 2014

that can only be granted in the master database.

---> CREATE DATABASE AUDIT SPECIFICATION

— / → CREATE DATABASE **- - - - - > STATEMENTS: CREATE DATABASE, RESTORE DATABASE ** NOTE: CREATE DATABASE is a database level permission

---> Combined with TRUSTWORTHY allows delegation of authentication

ALTER AUTHORIZATION for any object might also require IMPERSONATE or

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

XML Schema Collection Permissions

→ SELECT ON OBJECT::<queue name>

RECEIVE ON OBJECT::<queue name>

TAKE OWNERSHIP ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>

OBJECT permissions apply to the following database objects:

(All permissions do not apply to all objects. For example

→ VIEW DEFINITION ON SEARCH PROPERTY LIST::<name>

TAKE OWNERSHIP ON FULLTEXT CATALOG::<name> | TAKE OWNERSHIP ON FULLTEXT STOPLIST::<name> TAKE OWNERSHIP ON SEARCH PROPERTY LIST::<name>

ALTER ON FULLTEXT STOPLIST::<name>

-- ALTER FULLTEXT STOPLIST

--- CREATE FULLTEXT STOPLIST

REFERENCES ON SEARCH PROPERTY LIST::<name>

ALTER ON SEARCH PROPERTY LIST::<name>

--- ALTER SEARCH PROPERTY LIST

UPDATE only applies to tables and views.)

To drop an object (such as a table) you must have ALTER permission on the schema or CONTROL

To create or alter a trigger on a table or view requires ALTER OBJECT::<name> on the table or view.

• To create an index requires ALTER OBJECT::<name> permission on the table or view.

VIEW DEFINITION ON FULLTEXT STOPLIST::<name>

• Creating a full-text index requires ALTER permission on the table and REFERENCES permission on the full-text catalog.

To create statistics requires ALTER OBJECT::<name> on the table or view.

membership in a role or ALTER permission on a role.

Object Permissions

Type Permissions

inherited from ALTER AUTHORIZATION at a higher level.

Applies to subordinate objects in the database. See

Database Permissions – Schema Objects chart.

VIEW CHANGE TRACKING ON SCHEMA::<name> → → VIEW CHANGE TRACKING ON OBJECT::<name>

AGGREGATE

DEFAULT

Database Level Permissions

CONTROL SERVER

CONTROL ON DATABASE::<name> - - - - - → STATEMENTS: DROP DATABASE

ALTER ANY APPLICATION ROLE

CREATE AGGREGATE

CREATE DEFAULT

CREATE FUNCTION

CREATE PROCEDURE

CREATE QUEUE

CREATE RULE

CREATE TABLE

CREATE TYPE

CREATE VIEW

→ AUTHENTICATE

→ VIEW DEFINITION

──\ ► VIEW DATABASE STATE

SUBSCRIBE QUERY NOTIFICATIONS

→ SHOWPLAN

Database Permissions

TAKE OWNERSHIP ON DATABASE::<name>

→ ALTER ANY SCHEMA ———

CREATE AGGREGATE

CREATE DEFAULT

CREATE FUNCTION

CREATE PROCEDURE CREATE QUEUE

CREATE SYNONYM

CREATE TABLE

CREATE TYPE

CREATE VIEW

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

To alter an object (such as a table) you must have ALTER permission on the object (or schema), or

VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> →

DROP FULLTEXT CATALOG

DROP FULLTEXT STOPLIST

DROP FULLTEXT SEARCH PROPERTYLIST

→ ALTER ANY FULLTEXT CATALOG

OBJECT::<name> for any referenced CLR type or XML schema collection.

ALTER ANY DATABASE ALTER ON DATABASE::<name>

CONTROL permission on the object.

Full-text Permissions

CREATE XML SCHEMA COLLECTION

CREATE RULE

► CREATE SCHEMA

CREATE XML SCHEMA COLLECTION

CONNECT REPLICATION CONNECT DATABASE

CREATE SYNONYM

ALTER ANY ASYMMETRIC KEY
→ CREATE ASYMMETRIC KEY ALTER ANY CERTIFICATE
→ CREATE CERTIFICATE ALTER ANY CONTRACT
→ CREATE CONTRACT

ALTER ANY FULLTEXT CATALOG

→ CREATE FULLTEXT CATALOG

ALTER ANY REMOTE SERVICE BINDING ———— CREATE REMOTE SERVICE BINDING

ALTER ANY MESSAGE TYPE
→ CREATE MESSAGE TYPE

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

Schema Permissions

CONTROL ON SERVER → CONTROL ON DATABASE::<name> CONTROL ON SCHEMA ::<name> CONTROL ON OBJECT|TYPE|XML SCHEMA COLLECTION ::<name>

TAKE OWNERSHIP ON SCHEMA::<name>

SELECT ON DATABASE::<name> → SELECT ON OBJECT::

INSERT ON DATABASE::<name> → INSERT ON SCHEMA::<name> → INSERT ON OBJECT::

UPDATE ON DATABASE::<name> UPDATE ON SCHEMA::<name> UPDATE ON OBJECT::

DELETE ON DATABASE::<name> → DELETE ON SCHEMA::<name> → DELETE ON OBJECT::

VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>

CREATE SEQUENCE

CONTROL SERVER → CONTROL ON DATABASE::<name> ← CONTROL ON FULLTEXT STOPLIST::<name>

→ CONTROL ON FULLTEXT CATALOG::<name>

VIEW DEFINITION ON FULLTEXT CATALOG::<name>

→ T REFERENCES ON FULLTEXT CATALOG::<name>

ALTER ON FULLTEXT CATALOG::<name>

REFERENCES ON DATABASE::<name> REFERENCES ON FULLTEXT STOPLIST::<name>

---- ALTER FULLTEXT CATALOG

---- CREATE FULLTEXT CATALOG

Dropping a full-text index requires ALTER permission on the table.

REFERENCES ON DATABASE::<name> → → → → REFERENCES ON SCHEMA::<name> → → → REFERENCES ON OBJECT|TYPE|XML SCHEMA COLLECTION:<name>

→ ALTER ANY DATABASE EVENT NOTIFICATION — CREATE DATABASE DDL EVENT NOTIFICATION

Top Level Database Permissions

CREATE ANY DATABASE

ALTER ANY SERVER AUDIT

AUTHENTICATE SERVER

→ VIEW ANY DEFINITION —

VIEW SERVER STATE

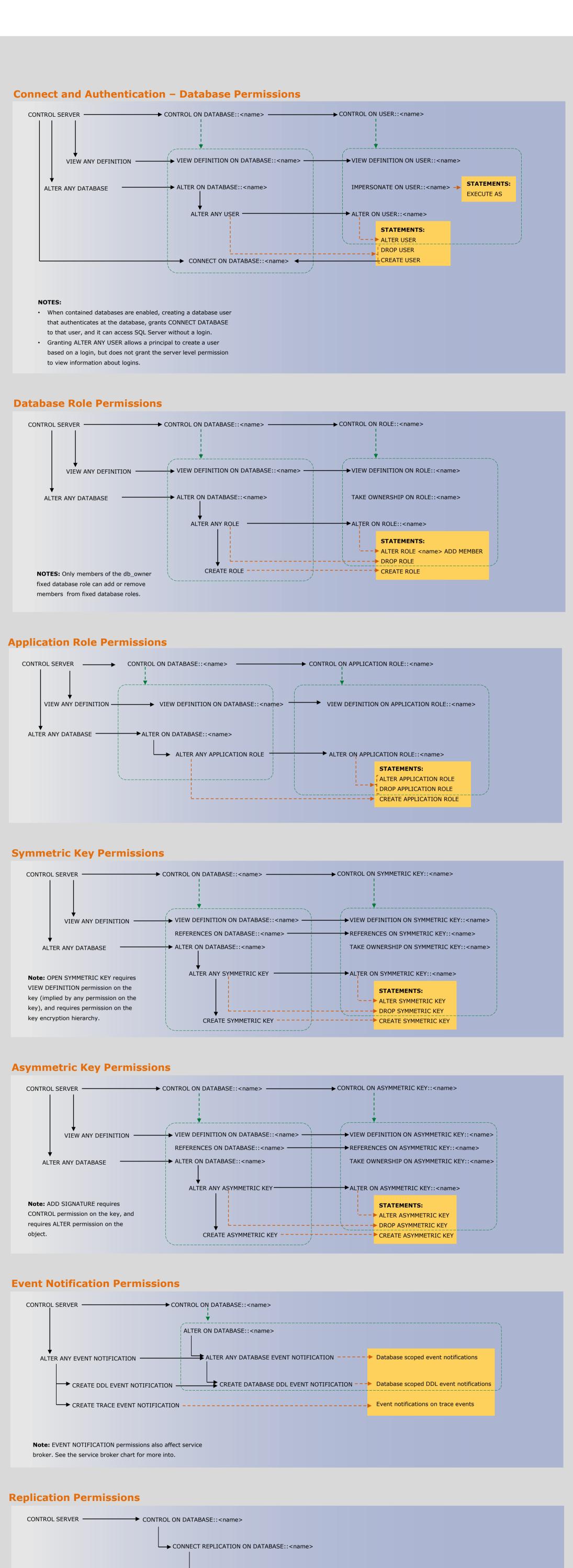
VIEW ANY DATABASE

Database Permissions – Schema Objects

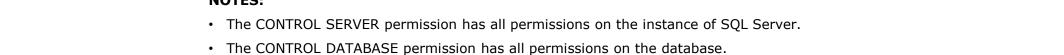
ALTER ANY EVENT NOTIFICATION

ALTER ANY DATABASE

Database Engine Permissions



→ CONNECT ON DATABASE::<name>



• 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

