Microsoft® SQL Server 2012 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. 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

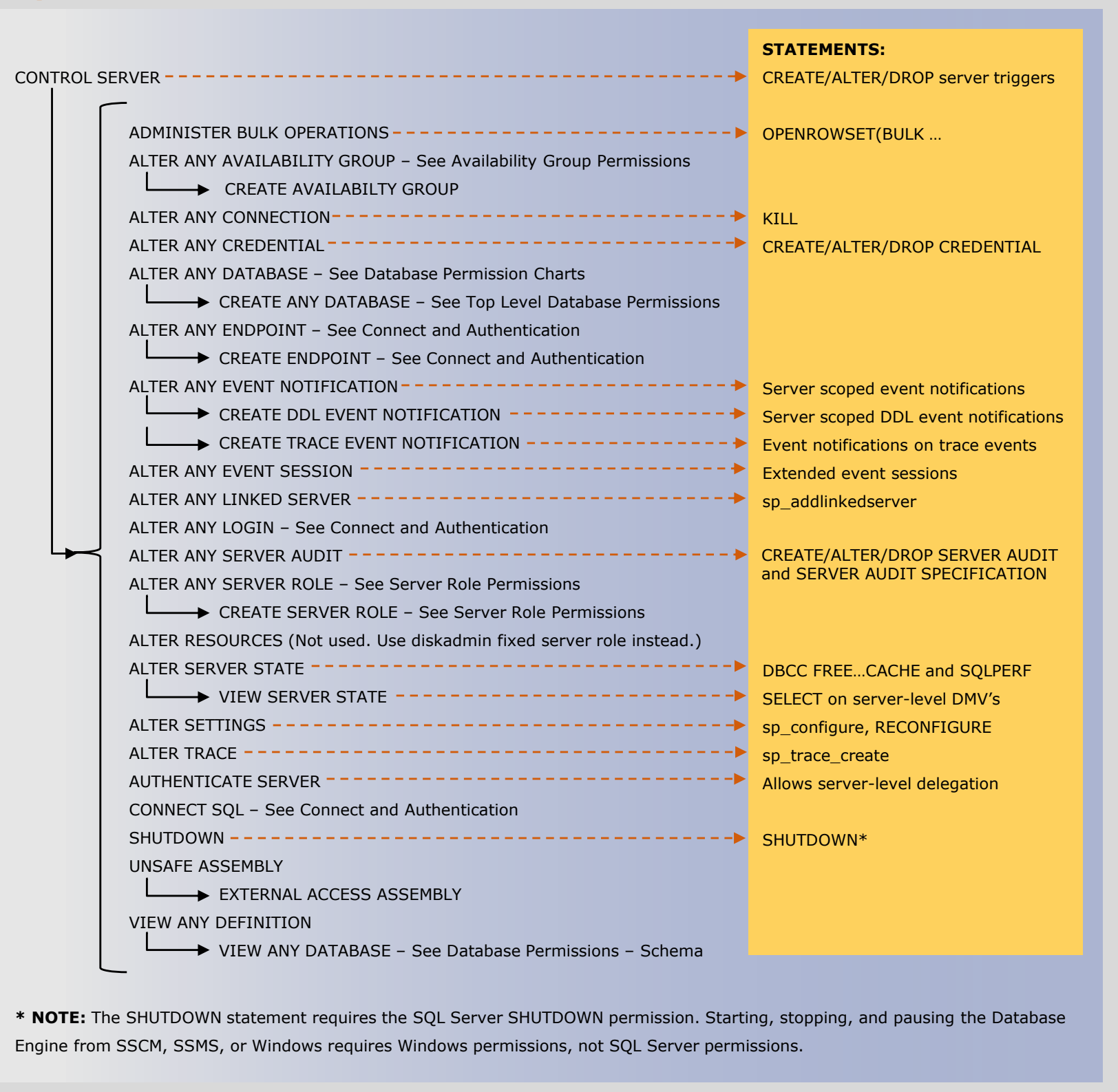
- Most of the more granular permissions are included in more than one higher level scope permission. So permissions can be inherited from more than one type of higher scope.
- Black, green, and blue arrows and boxes point to subordinate permissions that are included in the scope of higher a level permission.
- Brown arrows and boxes indicate some of the statements that can use the permission.

NOTES:

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

Server Level Permissions

Top Level Server Permissions

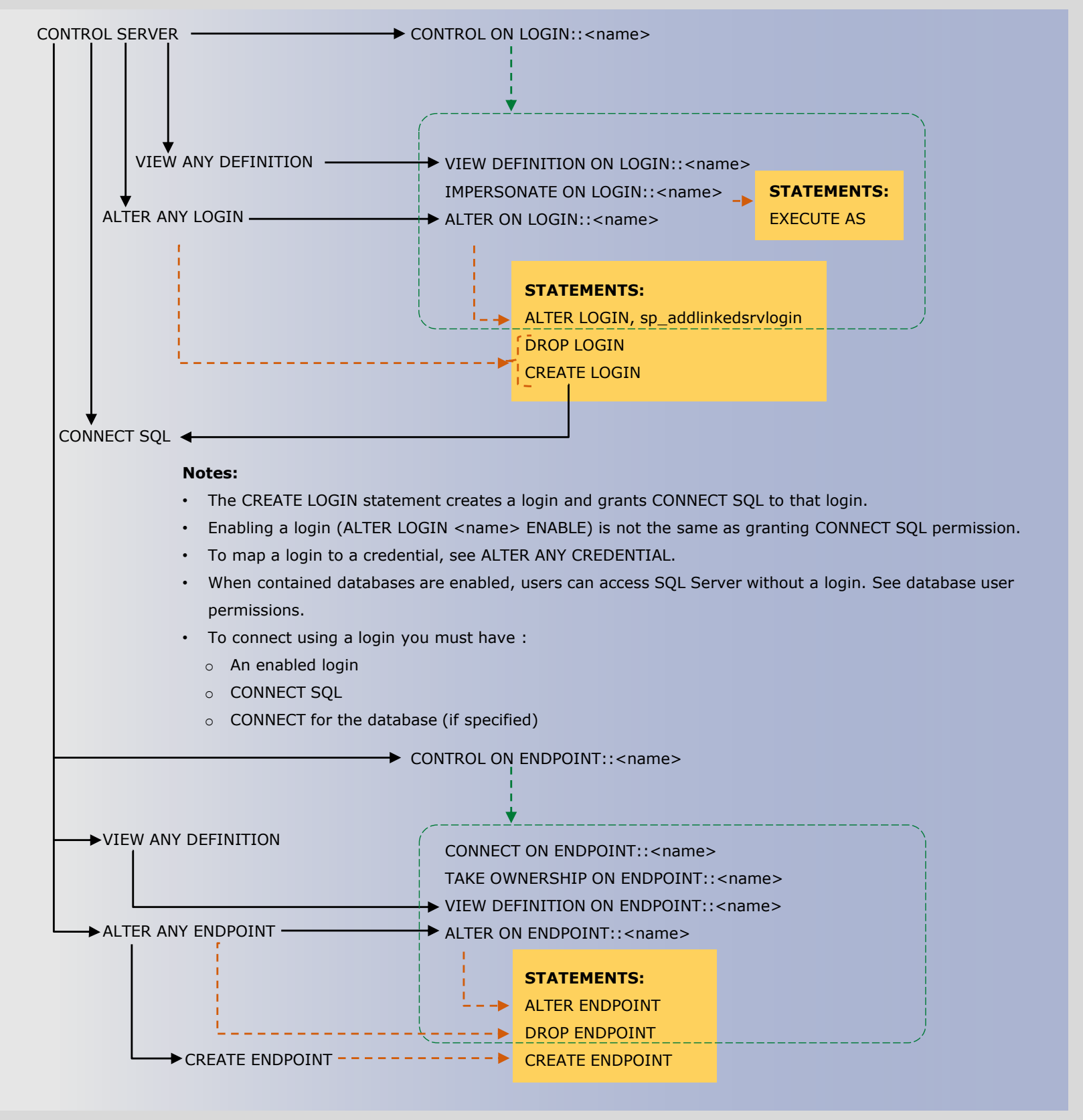


CONTROL SERVER
ADMINISTER BULK OPERATIONS
ALTER ANY AVAILABILITY GROUP – See Availability Group Permissions
CREATE AVAILABILTY GROUP
ALTER ANY CONNECTION
ALTER ANY CREDENTIAL
ALTER ANY DATABASE – See Database Permission Charts
CREATE ANY DATABASE – See Top Level Database Permissions
ALTER ANY ENDPOINT – See Connect and Authentication
CREATE ENDPOINT – See Connect and Authentication
ALTER ANY EVENT NOTIFICATION
CREATE DDL EVENT NOTIFICATION
CREATE TRACE EVENT NOTIFICATION
ALTER ANY EVENT SESSION
ALTER ANY LINKED SERVER
ALTER ANY LOGIN – See Connect and Authentication
ALTER ANY SERVER AUDIT
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.)
ALTER SERVER STATE
VIEW SERVER STATE
ALTER SETTINGS
ALTER TRACE
AUTHENTICATE SERVER
CONNECT SQL – See Connect and Authentication
SHUTDOWN
UNSAFE ASSEMBLY
EXTERNAL ACCESS ASSEMBLY
VIEW ANY DEFINITION
VIEW ANY DATABASE – See Database Permissions – Schema

STATEMENTS:
CREATE/ALTER/DROP server triggers
OPENROWSET(BULK ...
KILL
CREATE/ALTER/DROP CREDENTIAL
Server scoped event notifications
Server scoped DDL event notifications
Event notifications on trace events
Extended event sessions
sp_addlinkedserver
CREATE/ALTER/DROP SERVER AUDIT and SERVER AUDIT SPECIFICATION
DBCC FREE...CACHE and SQLPERF
SELECT on server-level DMV's
sp_configure, RECONFIGURE
sp_trace_create
Allows server-level delegation
SHUTDOWN*

* **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.

Connect and Authentication – Server Permissions



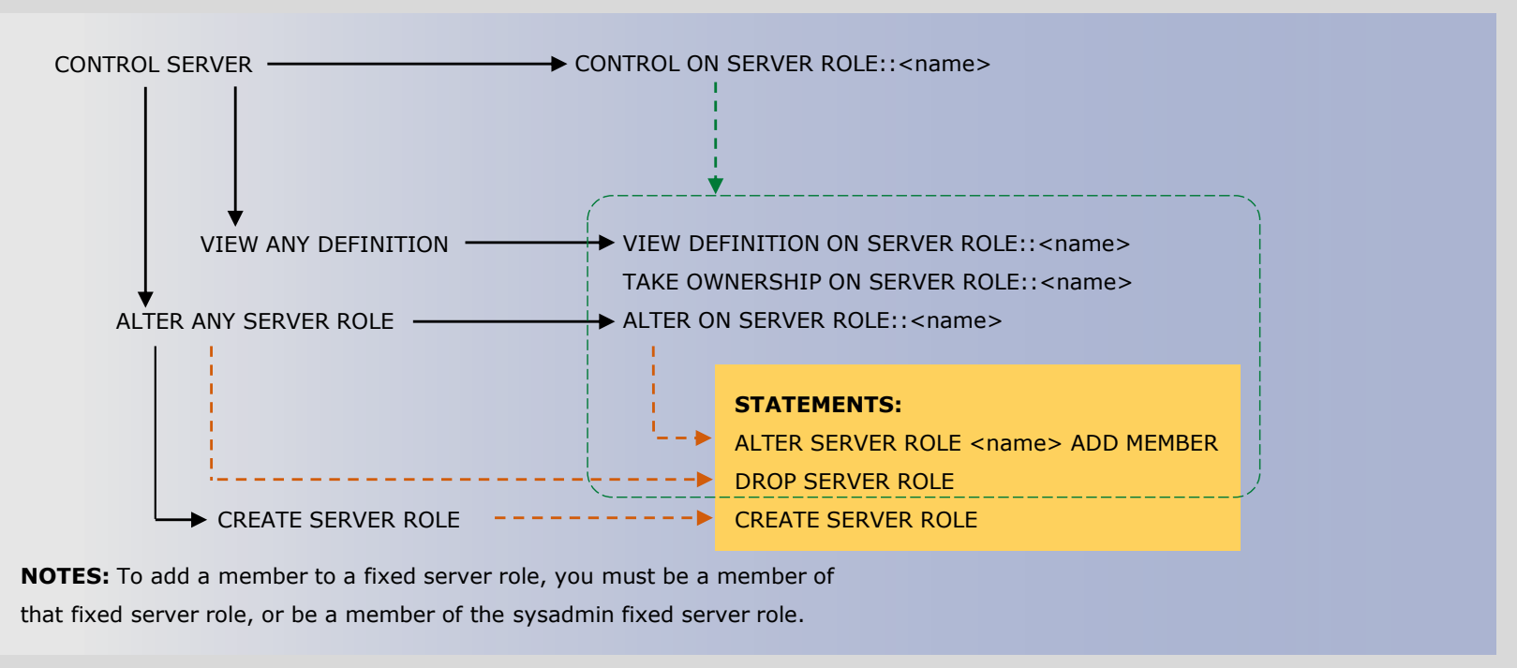
CONTROL SERVER
CONTROL ON LOGIN::<name>
VIEW ANY DEFINITION
ALTER ANY LOGIN
VIEW DEFINITION ON LOGIN::<name>
IMPERSONATE ON LOGIN::<name>
ALTER ON LOGIN::<name>
STATEMENTS:
EXECUTE AS
STATEMENTS:
ALTER LOGIN, sp_addlinkedsrvlogin
DROP LOGIN
CREATE LOGIN
CONNECT SQL

Notes:

- The CREATE LOGIN statement creates a login and grants CONNECT SQL to that login.
- Enabling a login (ALTER LOGIN <name> ENABLE) is not the same as granting CONNECT SQL permission.
- To map a login to a credential, see ALTER ANY CREDENTIAL.
- When contained databases are enabled, users can access SQL Server without a login. See database user permissions.
- To connect using a login you must have :
  - An enabled login
  - CONNECT SQL
  - CONNECT for the database (if specified)

CONTROL ON ENDPOINT::<name>
VIEW ANY DEFINITION
ALTER ANY ENDPOINT
CONNECT ON ENDPOINT::<name>
TAKE OWNERSHIP ON ENDPOINT::<name>
VIEW DEFINITION ON ENDPOINT::<name>
ALTER ON ENDPOINT::<name>
STATEMENTS:
ALTER ENDPOINT
DROP ENDPOINT
CREATE ENDPOINT
CREATE ENDPOINT

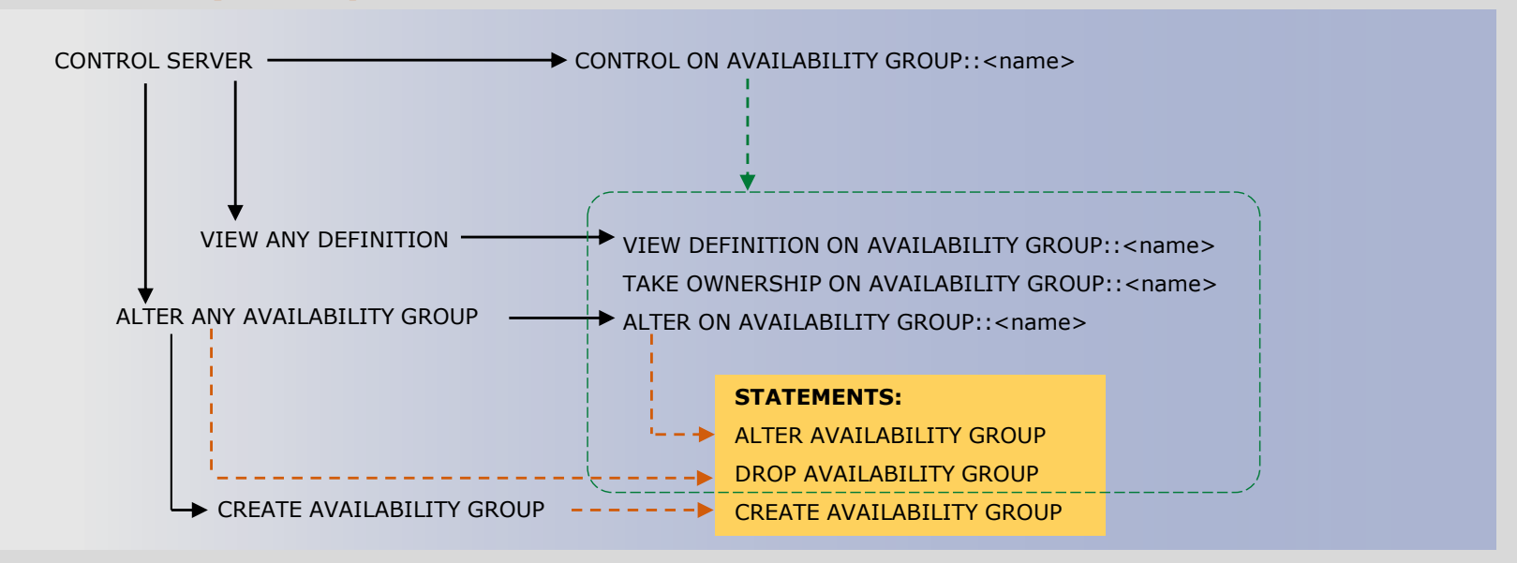
Server Role Permissions



CONTROL SERVER
CONTROL ON SERVER ROLE::<name>
VIEW ANY DEFINITION
ALTER ANY SERVER ROLE
VIEW DEFINITION ON SERVER ROLE::<name>
TAKE OWNERSHIP ON SERVER ROLE::<name>
ALTER ON SERVER ROLE::<name>
STATEMENTS:
ALTER SERVER ROLE <name> ADD MEMBER
DROP SERVER ROLE
CREATE SERVER ROLE
CREATE SERVER ROLE

NOTES: To add a member to a fixed server role, you must be a member of that fixed server role, or be a member of the sysadmin fixed server role.

Availability Group Permissions



CONTROL SERVER
CONTROL ON AVAILABILITY GROUP::<name>
VIEW ANY DEFINITION
ALTER ANY AVAILABILITY GROUP
VIEW DEFINITION ON AVAILABILITY GROUP::<name>
TAKE OWNERSHIP ON AVAILABILITY GROUP::<name>
ALTER ON AVAILABILITY GROUP::<name>
STATEMENTS:
ALTER AVAILABILITY GROUP
DROP AVAILABILITY GROUP
CREATE AVAILABILITY GROUP
CREATE AVAILABILITY GROUP

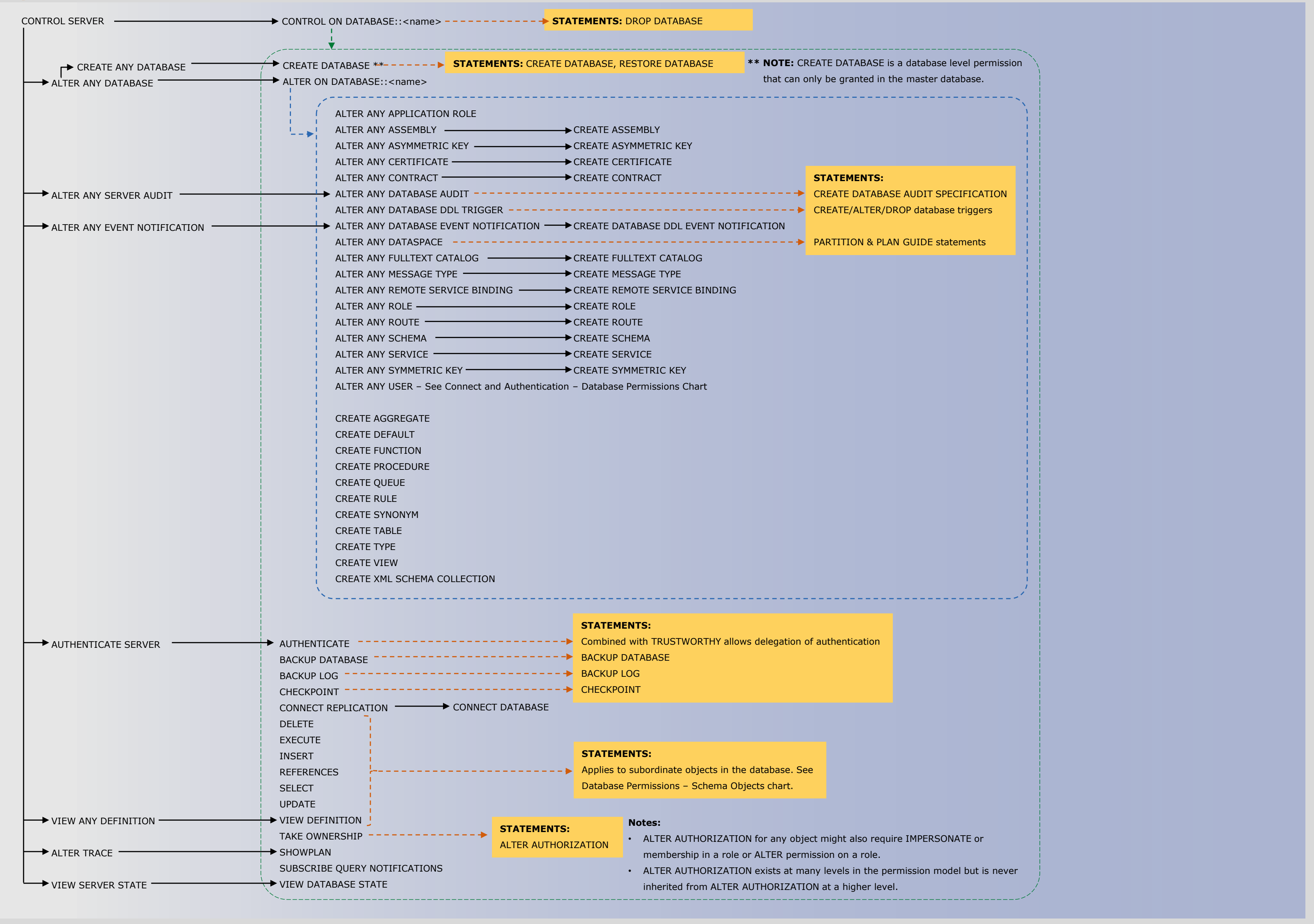
Questions and comments to **Rick.Byham@Microsoft.com**

Microsoft®

March 28, 2012

Database Level Permissions

Top Level Database Permissions

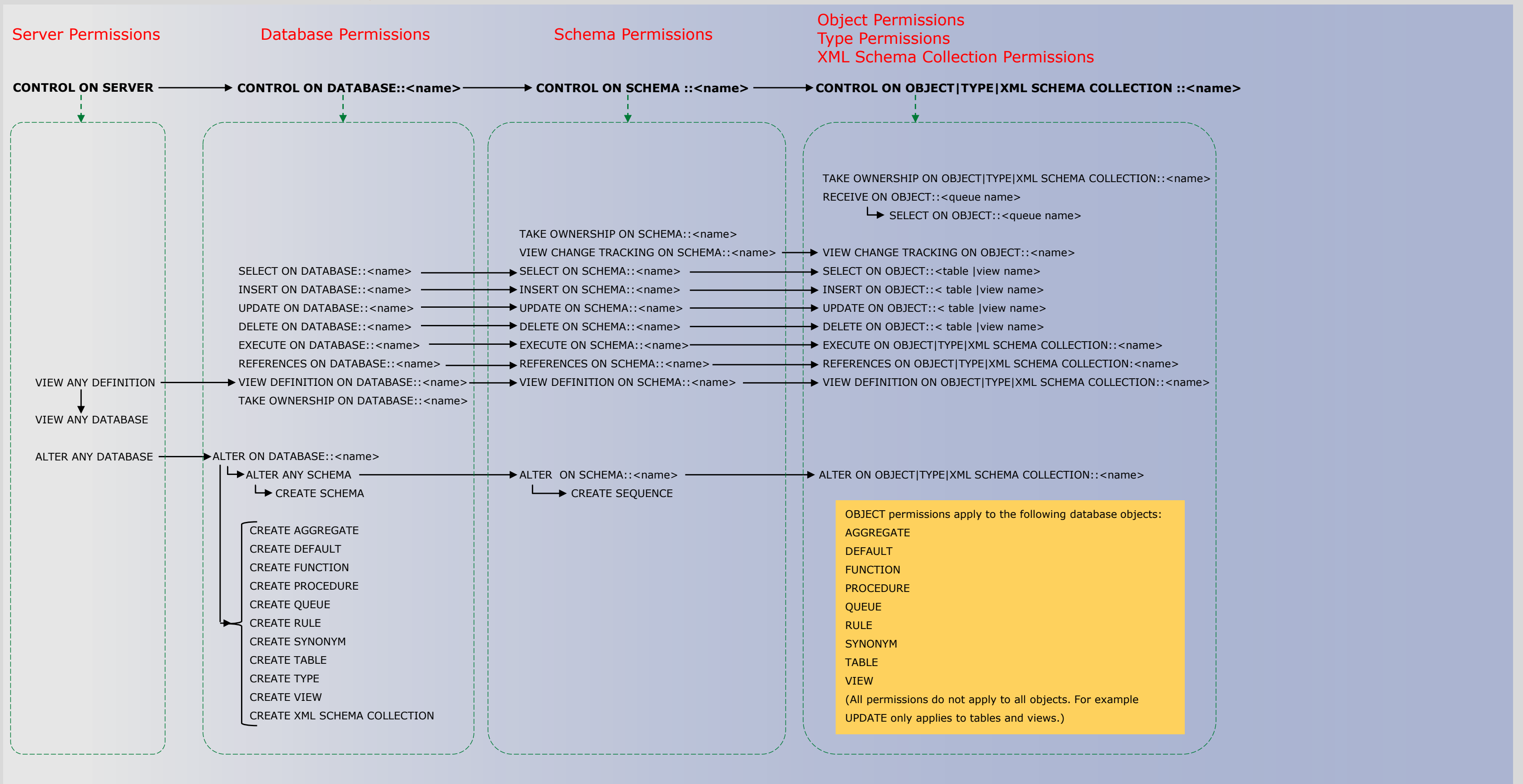


CONTROL SERVER
CONTROL ON DATABASE::<name>
STATEMENTS: DROP DATABASE
CREATE ANY DATABASE
ALTER ANY DATABASE
CREATE DATABASE **
ALTER ON DATABASE::<name>
STATEMENTS: CREATE DATABASE, RESTORE DATABASE
** **NOTE:** CREATE DATABASE is a database level permission that can only be granted in the master database.
ALTER ANY SERVER AUDIT
ALTER ANY EVENT NOTIFICATION
ALTER ANY APPLICATION ROLE
ALTER ANY ASSEMBLY → CREATE ASSEMBLY
ALTER ANY ASYMMETRIC KEY → CREATE ASYMMETRIC KEY
ALTER ANY CERTIFICATE → CREATE CERTIFICATE
ALTER ANY CONTRACT → CREATE CONTRACT
ALTER ANY DATABASE AUDIT
ALTER ANY DATABASE DDL TRIGGER
ALTER ANY DATABASE EVENT NOTIFICATION → CREATE DATABASE DDL EVENT NOTIFICATION
ALTER ANY DATASPACE
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
STATEMENTS:
CREATE DATABASE AUDIT SPECIFICATION
CREATE/ALTER/DROP database triggers
PARTITION & PLAN GUIDE statements
CREATE AGGREGATE
CREATE DEFAULT
CREATE FUNCTION
CREATE PROCEDURE
CREATE QUEUE
CREATE RULE
CREATE SYNONYM
CREATE TABLE
CREATE TYPE
CREATE VIEW
CREATE XML SCHEMA COLLECTION
AUTHENTICATE SERVER
AUTHENTICATE
BACKUP DATABASE
BACKUP LOG
CHECKPOINT
CONNECT REPLICATION → CONNECT DATABASE
DELETE
EXECUTE
INSERT
REFERENCES
SELECT
UPDATE
VIEW ANY DEFINITION
VIEW DEFINITION
TAKE OWNERSHIP
ALTER TRACE
SHOWPLAN
SUBSCRIBE QUERY NOTIFICATIONS
VIEW SERVER STATE
VIEW DATABASE STATE
STATEMENTS:
Combined with TRUSTWORTHY allows delegation of authentication
BACKUP DATABASE
BACKUP LOG
CHECKPOINT
STATEMENTS:
Applies to subordinate objects in the database. See Database Permissions – Schema Objects chart.
STATEMENTS:
ALTER AUTHORIZATION

Notes:

- ALTER AUTHORIZATION for any object might also require IMPERSONATE or membership in a role or ALTER permission on a role.
- ALTER AUTHORIZATION exists at many levels in the permission model but is never inherited from ALTER AUTHORIZATION at a higher level.

Database Permissions – Schema Objects

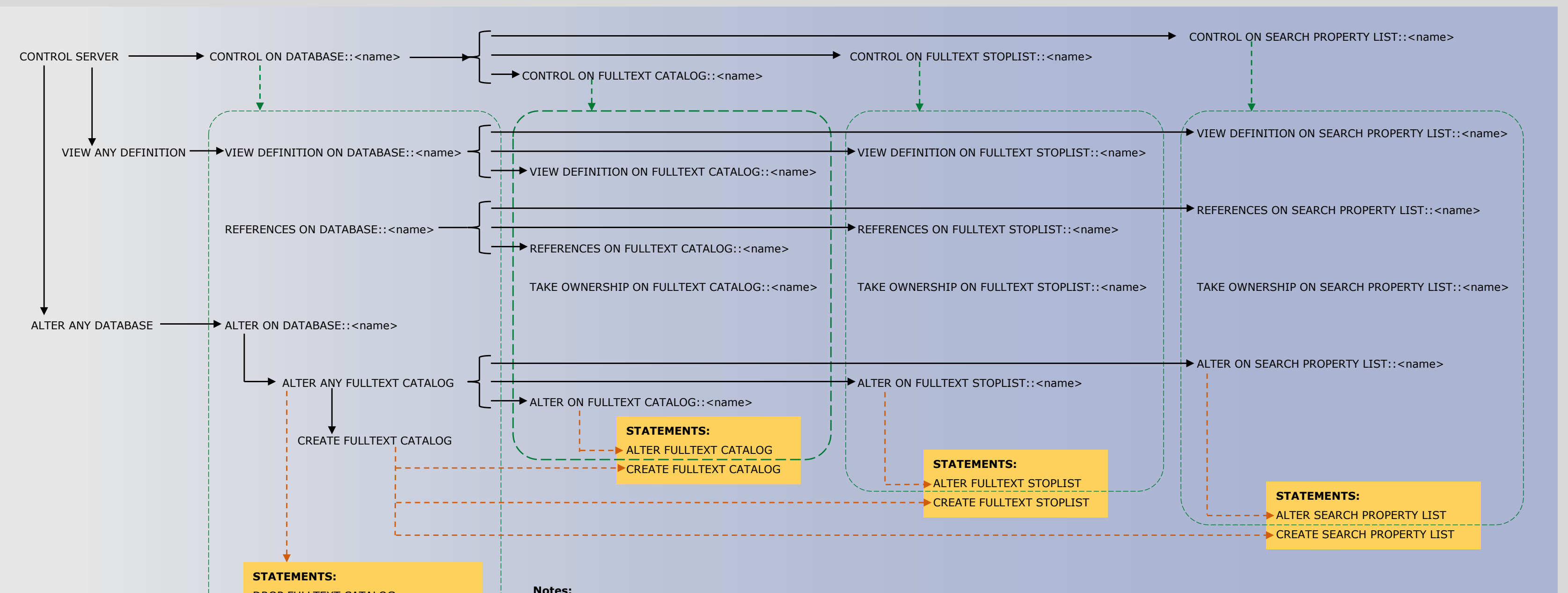


Server Permissions
Database Permissions
Schema Permissions
Object Permissions
Type Permissions
XML Schema Collection Permissions
CONTROL ON SERVER → **CONTROL ON DATABASE::<name>** → **CONTROL ON SCHEMA ::<name>** → **CONTROL ON OBJECT|TYPE|XML SCHEMA COLLECTION ::<name>**
TAKE OWNERSHIP ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>
RECEIVE ON OBJECT::<queue name>
SELECT ON OBJECT::<queue name>
TAKE OWNERSHIP ON SCHEMA::<name>
VIEW CHANGE TRACKING ON SCHEMA::<name> → VIEW CHANGE TRACKING ON OBJECT::<name>
SELECT ON DATABASE::<name> → SELECT ON SCHEMA::<name> → SELECT ON OBJECT::<table |view name>
INSERT ON DATABASE::<name> → INSERT ON SCHEMA::<name> → INSERT ON OBJECT::< table |view name>
UPDATE ON DATABASE::<name> → UPDATE ON SCHEMA::<name> → UPDATE ON OBJECT::< table |view name>
DELETE ON DATABASE::<name> → DELETE ON SCHEMA::<name> → DELETE ON OBJECT::< table |view name>
EXECUTE ON DATABASE::<name> → EXECUTE ON SCHEMA::<name> → EXECUTE ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON SCHEMA::<name> → REFERENCES ON OBJECT|TYPE|XML SCHEMA COLLECTION:<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON SCHEMA::<name> → VIEW DEFINITION ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>
VIEW ANY DATABASE
TAKE OWNERSHIP ON DATABASE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY SCHEMA → ALTER ON SCHEMA::<name> → ALTER ON OBJECT|TYPE|XML SCHEMA COLLECTION::<name>
CREATE SCHEMA
CREATE SEQUENCE
CREATE AGGREGATE
CREATE DEFAULT
CREATE FUNCTION
CREATE PROCEDURE
CREATE QUEUE
CREATE RULE
CREATE SYNONYM
CREATE TABLE
CREATE TYPE
CREATE VIEW
CREATE XML SCHEMA COLLECTION
OBJECT permissions apply to the following database objects:
AGGREGATE
DEFAULT
FUNCTION
PROCEDURE
QUEUE
RULE
SYNONYM
TABLE
VIEW
(All permissions do not apply to all objects. For example UPDATE only applies to tables and views.)

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

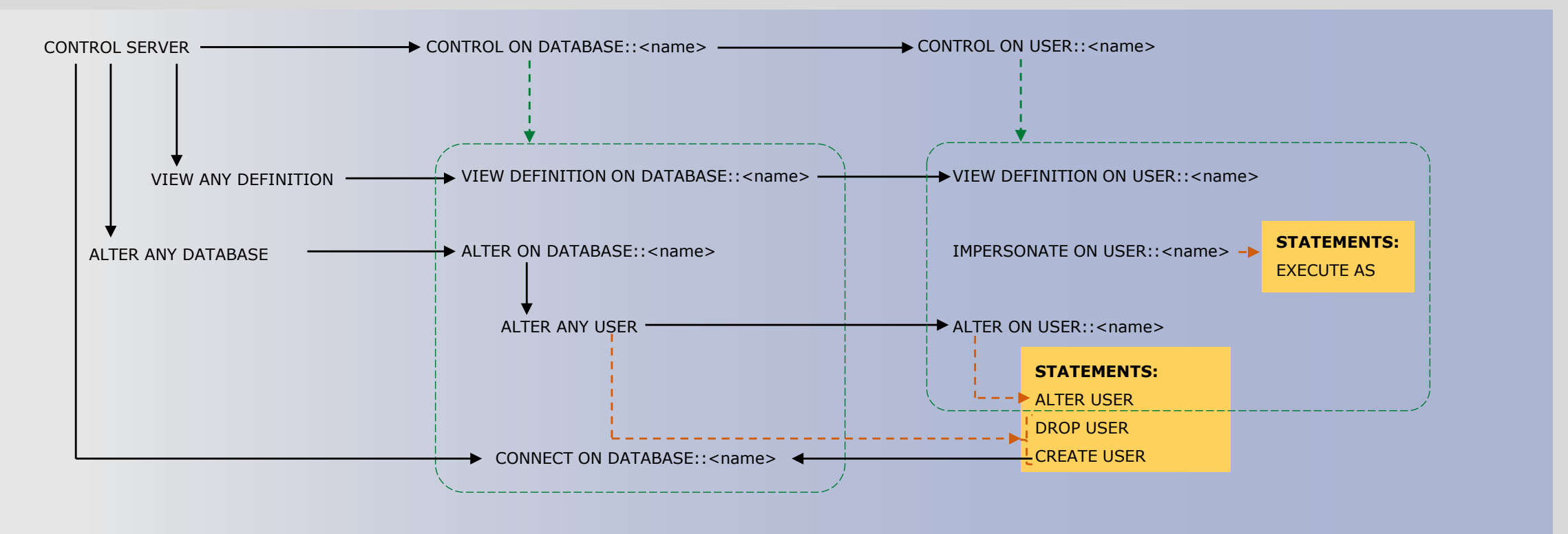


CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON SEARCH PROPERTY LIST::<name>
CONTROL ON FULLTEXT STOPLIST::<name>
CONTROL ON FULLTEXT CATALOG::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name>
VIEW DEFINITION ON SEARCH PROPERTY LIST::<name>
VIEW DEFINITION ON FULLTEXT STOPLIST::<name>
VIEW DEFINITION ON FULLTEXT CATALOG::<name>
REFERENCES ON DATABASE::<name>
REFERENCES ON SEARCH PROPERTY LIST::<name>
REFERENCES ON FULLTEXT STOPLIST::<name>
REFERENCES ON FULLTEXT CATALOG::<name>
TAKE OWNERSHIP ON FULLTEXT CATALOG::<name>
TAKE OWNERSHIP ON FULLTEXT STOPLIST::<name>
TAKE OWNERSHIP ON SEARCH PROPERTY LIST::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY FULLTEXT CATALOG
ALTER ON SEARCH PROPERTY LIST::<name>
ALTER ON FULLTEXT STOPLIST::<name>
ALTER ON FULLTEXT CATALOG::<name>
CREATE FULLTEXT CATALOG
STATEMENTS:
ALTER FULLTEXT CATALOG
CREATE FULLTEXT CATALOG
STATEMENTS:
ALTER FULLTEXT STOPLIST
CREATE FULLTEXT STOPLIST
STATEMENTS:
ALTER SEARCH PROPERTY LIST
CREATE SEARCH PROPERTY LIST
STATEMENTS:
DROP FULLTEXT CATALOG
DROP FULLTEXT STOPLIST
DROP FULLTEXT SEARCH PROPERTYLIST

Notes:

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

Connect and Authentication – Database Permissions

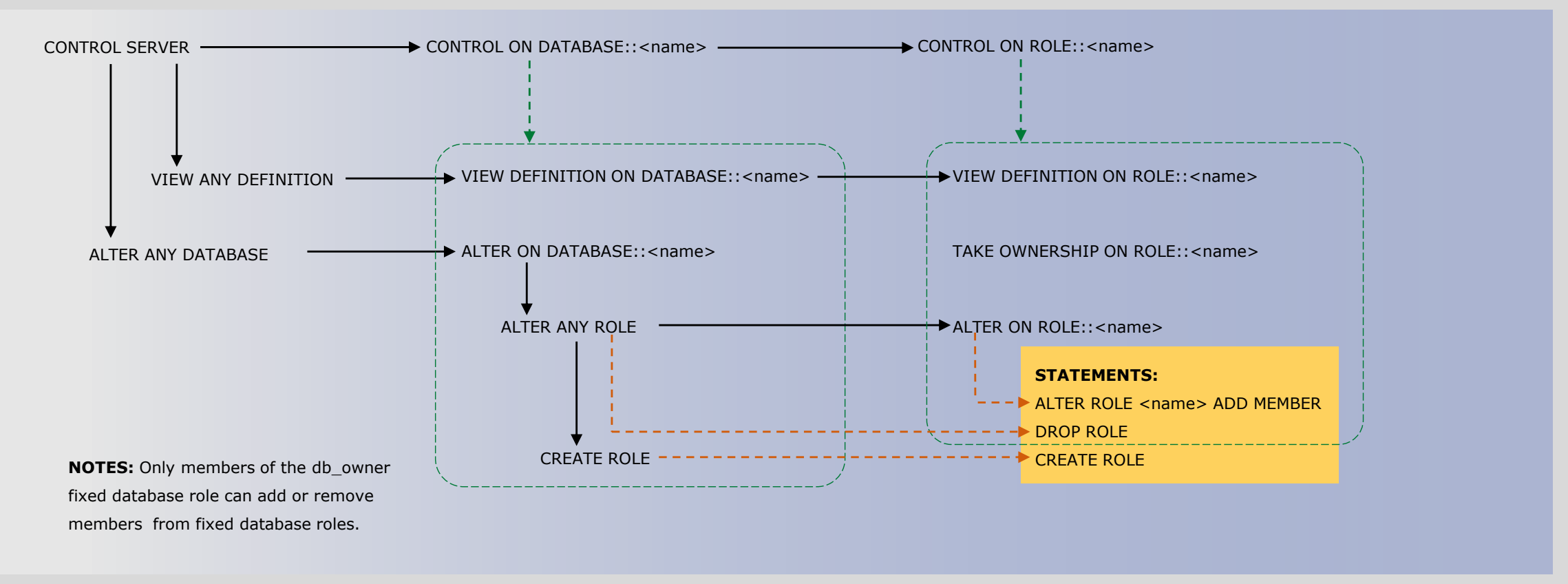


CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON USER::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON USER::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
IMPERSONATE ON USER::<name>
STATEMENTS:
EXECUTE AS
ALTER ANY USER → ALTER ON USER::<name>
STATEMENTS:
ALTER USER
DROP USER
CREATE USER
CONNECT ON DATABASE::<name>

NOTES:

- When contained databases are enabled, creating a database user that authenticates at the database, grants CONNECT DATABASE to that user, and it can access SQL Server without a login.
- Granting ALTER ANY USER allows a principal to create a user based on a login, but does not grant the server level permission to view information about logins.

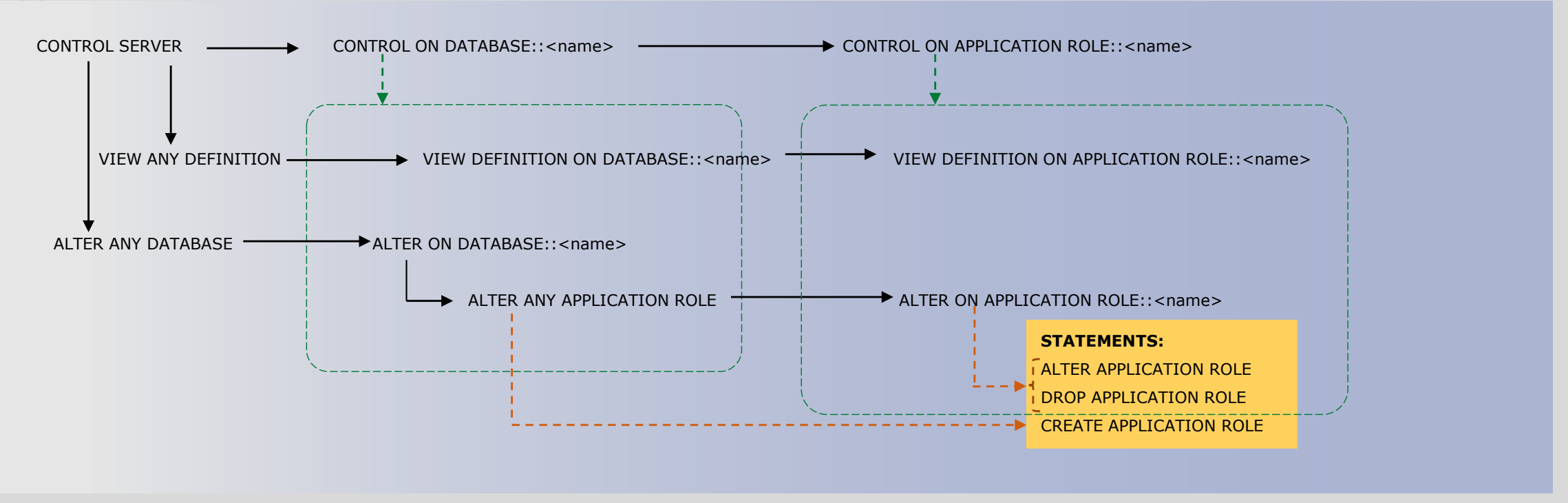
Database Role Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON ROLE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON ROLE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
TAKE OWNERSHIP ON ROLE::<name>
ALTER ANY ROLE → ALTER ON ROLE::<name>
CREATE ROLE
STATEMENTS:
ALTER ROLE <name> ADD MEMBER
DROP ROLE
CREATE ROLE

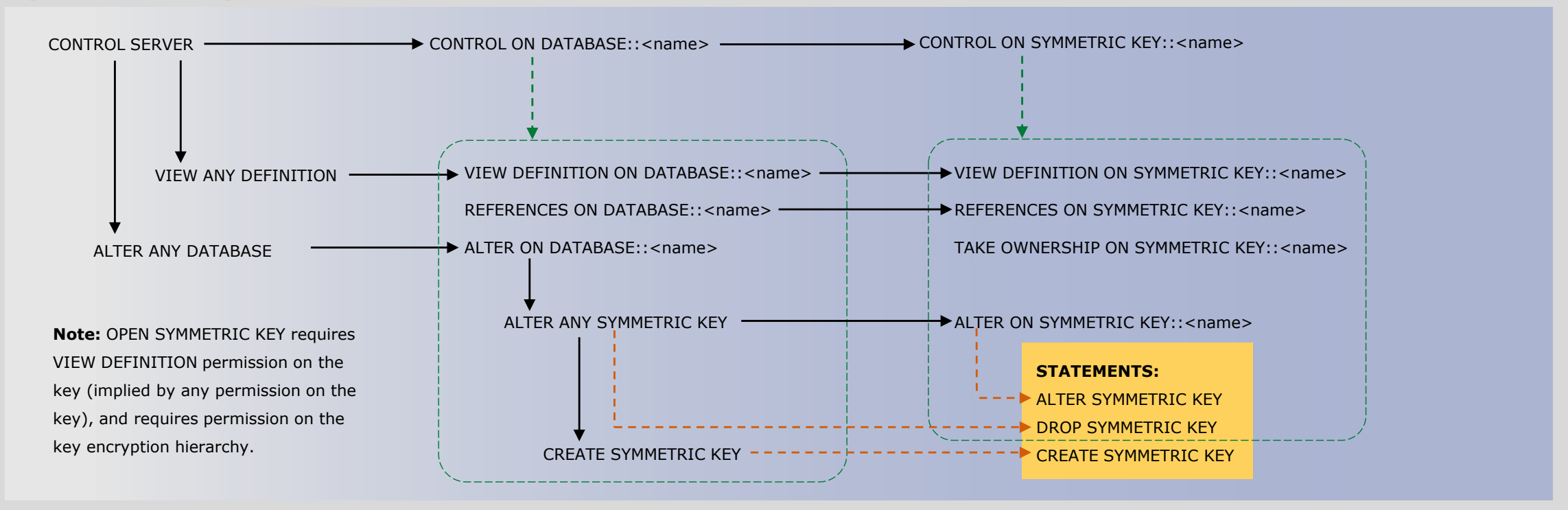
NOTES: Only members of the db_owner fixed database role can add or remove members from fixed database roles.

Application Role Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON APPLICATION ROLE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON APPLICATION ROLE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY APPLICATION ROLE → ALTER ON APPLICATION ROLE::<name>
STATEMENTS:
ALTER APPLICATION ROLE
DROP APPLICATION ROLE
CREATE APPLICATION ROLE

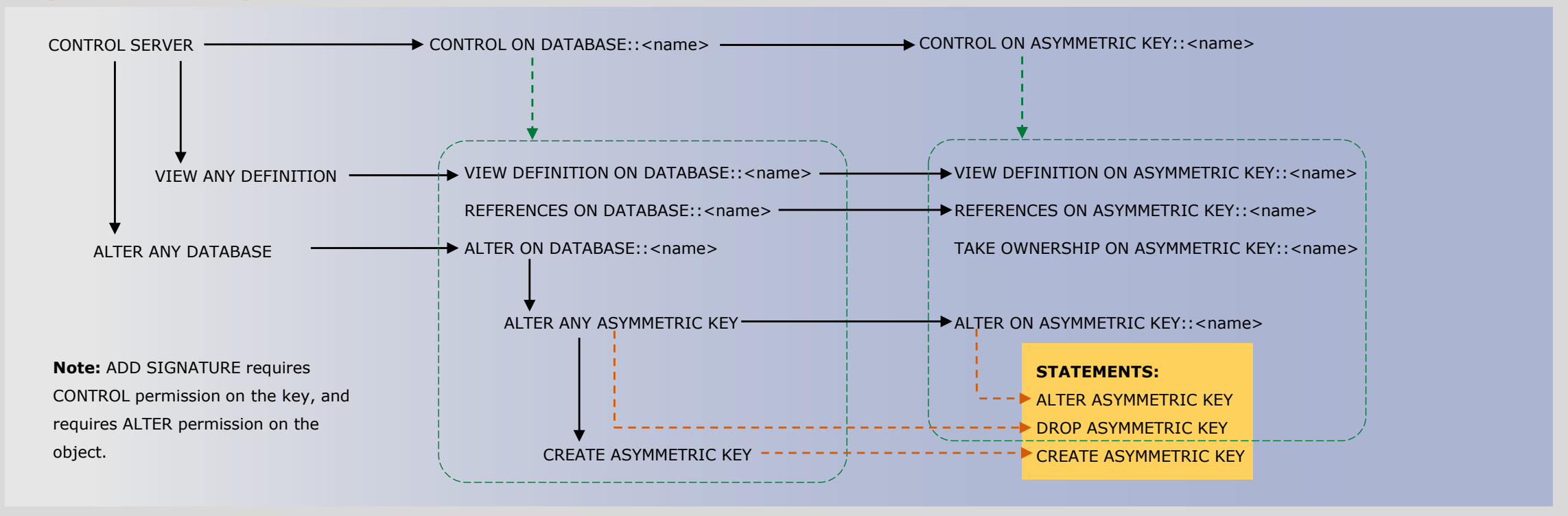
Symmetric Key Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON SYMMETRIC KEY::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON SYMMETRIC KEY::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON SYMMETRIC KEY::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
TAKE OWNERSHIP ON SYMMETRIC KEY::<name>
ALTER ANY SYMMETRIC KEY → ALTER ON SYMMETRIC KEY::<name>
CREATE SYMMETRIC KEY
STATEMENTS:
ALTER SYMMETRIC KEY
DROP SYMMETRIC KEY
CREATE SYMMETRIC KEY

Note: OPEN SYMMETRIC KEY requires VIEW DEFINITION permission on the key (implied by any permission on the key), and requires permission on the key encryption hierarchy.

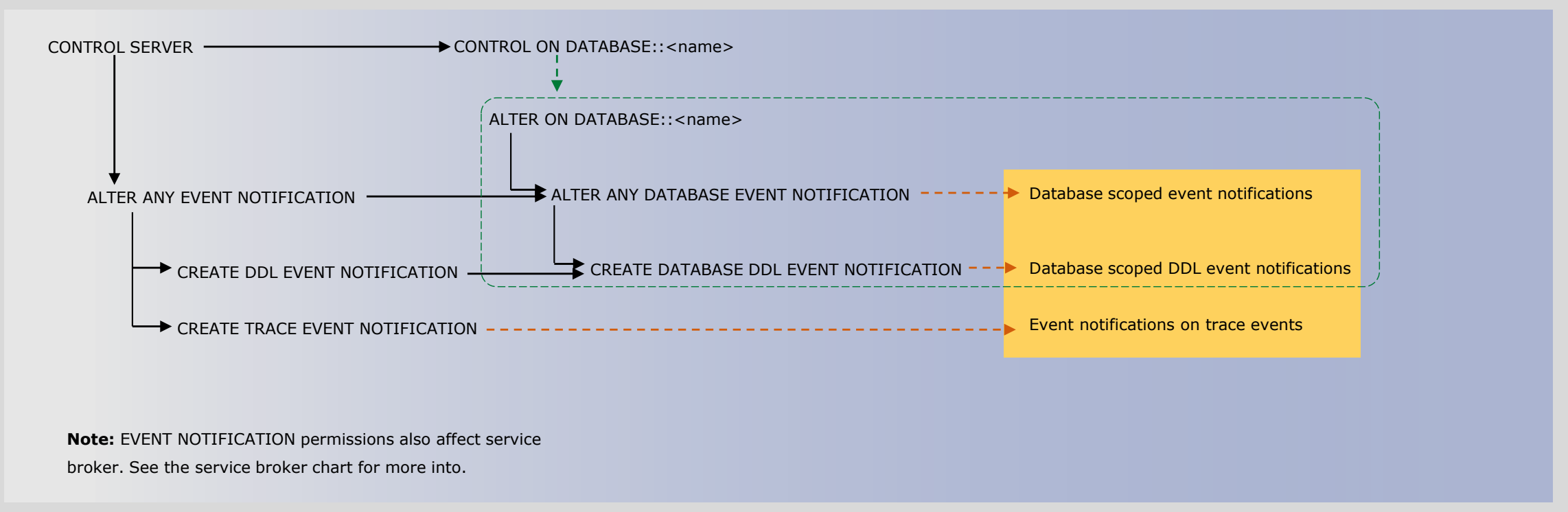
Asymmetric Key Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON ASYMMETRIC KEY::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON ASYMMETRIC KEY::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON ASYMMETRIC KEY::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
TAKE OWNERSHIP ON ASYMMETRIC KEY::<name>
ALTER ANY ASYMMETRIC KEY → ALTER ON ASYMMETRIC KEY::<name>
CREATE ASYMMETRIC KEY
STATEMENTS:
ALTER ASYMMETRIC KEY
DROP ASYMMETRIC KEY
CREATE ASYMMETRIC KEY

Note: ADD SIGNATURE requires CONTROL permission on the key, and requires ALTER permission on the object.

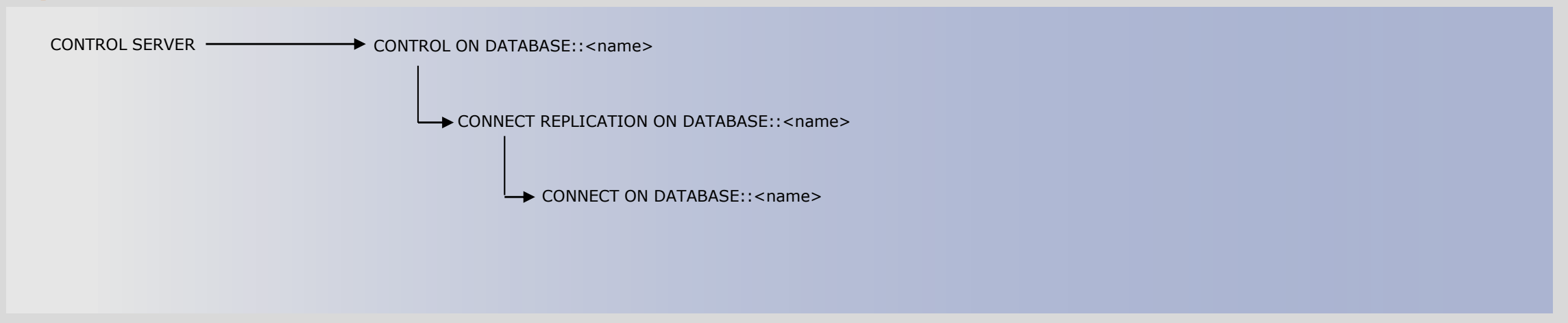
Event Notification Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
ALTER ON DATABASE::<name>
ALTER ANY EVENT NOTIFICATION → ALTER ANY DATABASE EVENT NOTIFICATION
CREATE DDL EVENT NOTIFICATION → CREATE DATABASE DDL EVENT NOTIFICATION
CREATE TRACE EVENT NOTIFICATION
Database scoped event notifications
Database scoped DDL event notifications
Event notifications on trace events

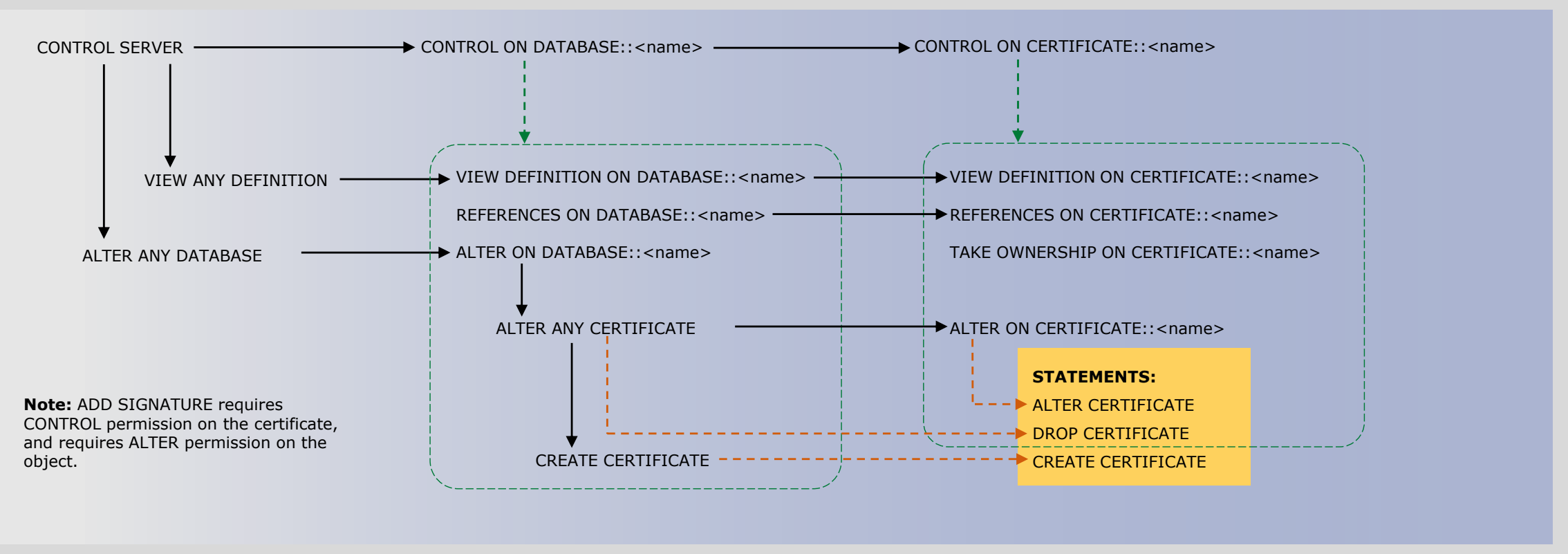
Note: EVENT NOTIFICATION permissions also affect service broker. See the service broker chart for more into.

Replication Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONNECT REPLICATION ON DATABASE::<name>
CONNECT ON DATABASE::<name>

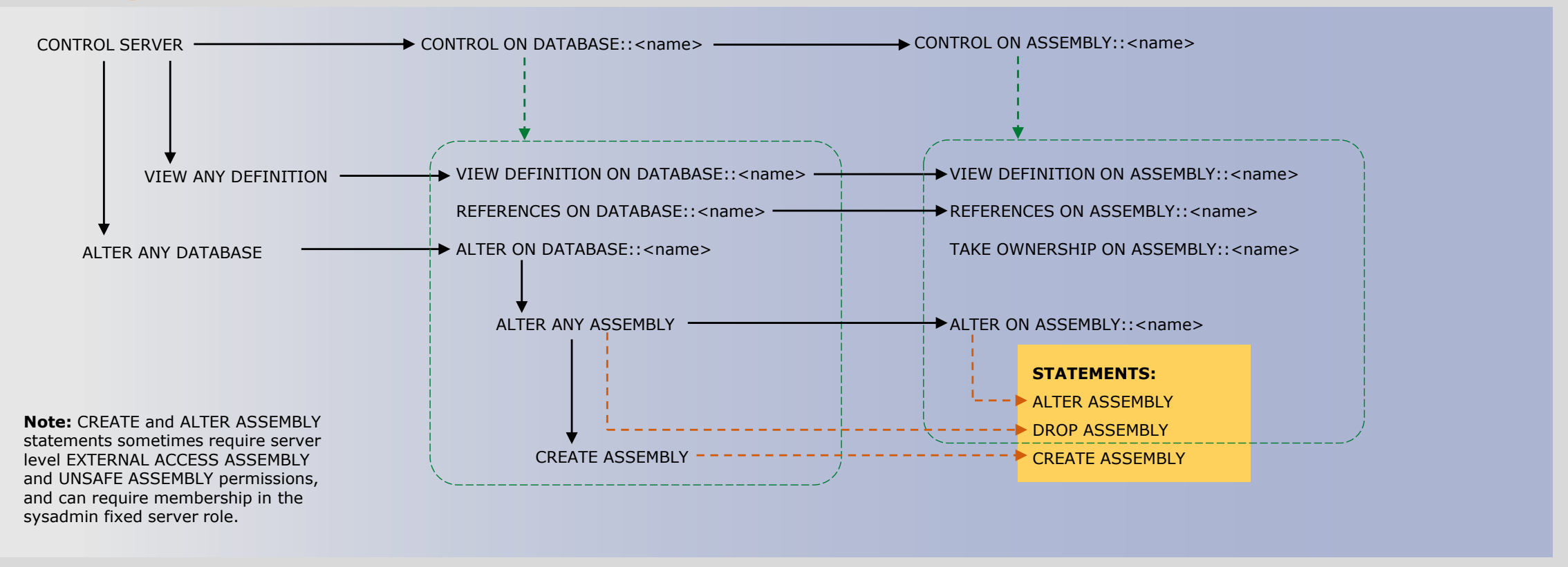
Certificate Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON CERTIFICATE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON CERTIFICATE::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON CERTIFICATE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
TAKE OWNERSHIP ON CERTIFICATE::<name>
ALTER ANY CERTIFICATE → ALTER ON CERTIFICATE::<name>
CREATE CERTIFICATE
STATEMENTS:
ALTER CERTIFICATE
DROP CERTIFICATE
CREATE CERTIFICATE

Note: ADD SIGNATURE requires CONTROL permission on the certificate, and requires ALTER permission on the object.

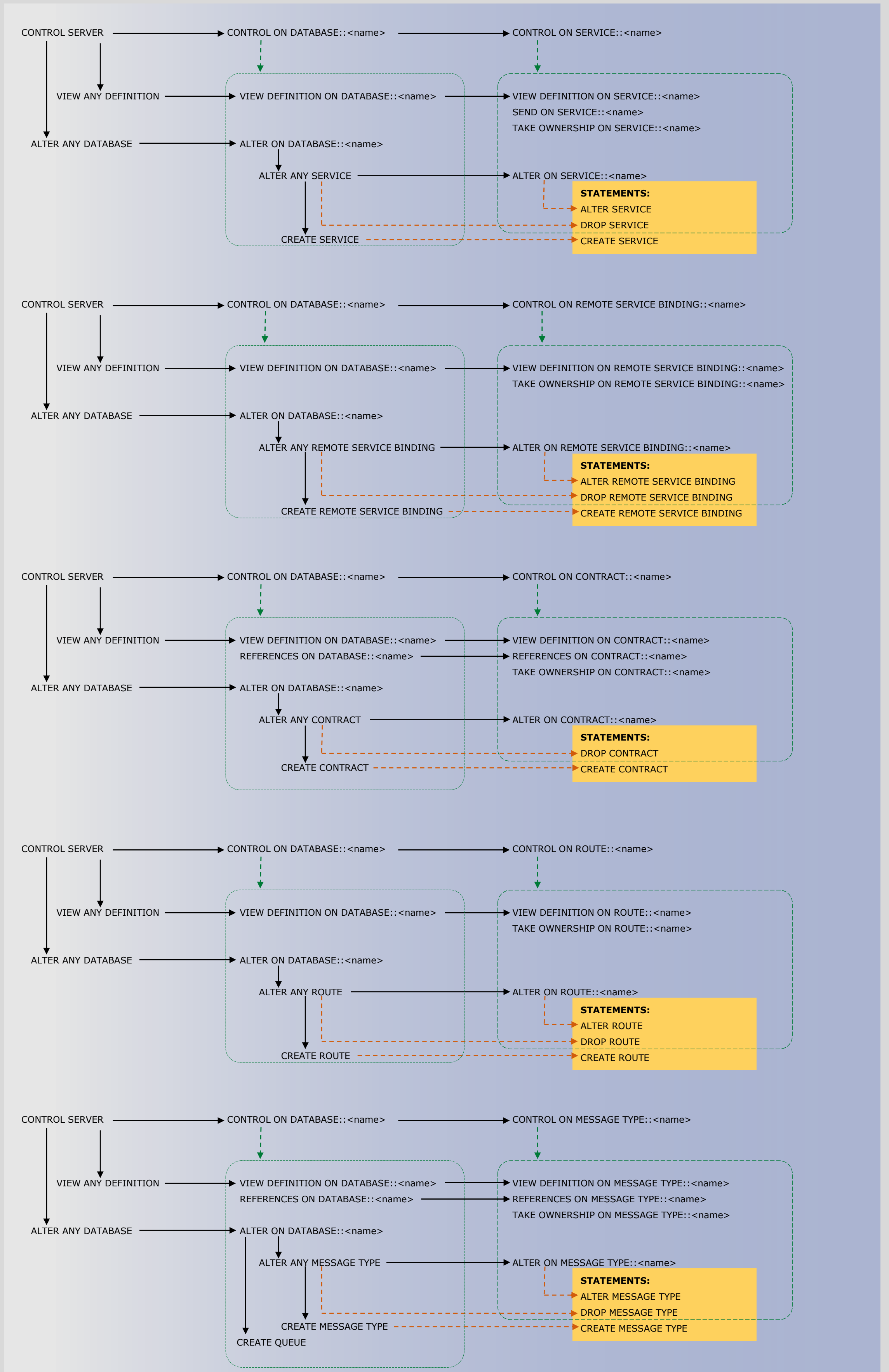
Assembly Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON ASSEMBLY::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON ASSEMBLY::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON ASSEMBLY::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
TAKE OWNERSHIP ON ASSEMBLY::<name>
ALTER ANY ASSEMBLY → ALTER ON ASSEMBLY::<name>
CREATE ASSEMBLY
STATEMENTS:
ALTER ASSEMBLY
DROP ASSEMBLY
CREATE ASSEMBLY

Note: CREATE and ALTER ASSEMBLY statements sometimes require server level EXTERNAL ACCESS ASSEMBLY and UNSAFE ASSEMBLY permissions, and can require membership in the sysadmin fixed server role.

Service Broker Permissions



CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON SERVICE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON SERVICE::<name>
SEND ON SERVICE::<name>
TAKE OWNERSHIP ON SERVICE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY SERVICE → ALTER ON SERVICE::<name>
CREATE SERVICE
STATEMENTS:
ALTER SERVICE
DROP SERVICE
CREATE SERVICE

CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON REMOTE SERVICE BINDING::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON REMOTE SERVICE BINDING::<name>
TAKE OWNERSHIP ON REMOTE SERVICE BINDING::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY REMOTE SERVICE BINDING → ALTER ON REMOTE SERVICE BINDING::<name>
CREATE REMOTE SERVICE BINDING
STATEMENTS:
ALTER REMOTE SERVICE BINDING
DROP REMOTE SERVICE BINDING
CREATE REMOTE SERVICE BINDING

CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON CONTRACT::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON CONTRACT::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON CONTRACT::<name>
TAKE OWNERSHIP ON CONTRACT::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY CONTRACT → ALTER ON CONTRACT::<name>
CREATE CONTRACT
STATEMENTS:
DROP CONTRACT
CREATE CONTRACT

CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON ROUTE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON ROUTE::<name>
TAKE OWNERSHIP ON ROUTE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY ROUTE → ALTER ON ROUTE::<name>
CREATE ROUTE
STATEMENTS:
ALTER ROUTE
DROP ROUTE
CREATE ROUTE

CONTROL SERVER
CONTROL ON DATABASE::<name>
CONTROL ON MESSAGE TYPE::<name>
VIEW ANY DEFINITION → VIEW DEFINITION ON DATABASE::<name> → VIEW DEFINITION ON MESSAGE TYPE::<name>
REFERENCES ON DATABASE::<name> → REFERENCES ON MESSAGE TYPE::<name>
TAKE OWNERSHIP ON MESSAGE TYPE::<name>
ALTER ANY DATABASE → ALTER ON DATABASE::<name>
ALTER ANY MESSAGE TYPE → ALTER ON MESSAGE TYPE::<name>
CREATE MESSAGE TYPE
CREATE QUEUE
STATEMENTS:
ALTER MESSAGE TYPE
DROP MESSAGE TYPE
CREATE MESSAGE TYPE

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 or ALTER REMOTE SERVICE BINDING the user must have impersonate permission for the principal 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.