To create statistics requires ALTER OBJECT::<name> on the table or view. When contained databases are enabled, creating an object (such as a table) you must have ALTER permission on the schema or CONTROL permission.

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

To connect using a login you must have:

- ALTER AUTHORIZATION
- EXECUTE
- REPLICATION
- SELECT

Permission exists at many levels in the permission model but is never inherited from ALTER AUTHORIZATION at a higher level.

Note:
- The CONNECT permission is required only when connecting using a login.
- To create an object, you must have the appropriate permission.
- To connect using a login, you must have the appropriate permission.

Permission inheritance:
- Permissions can be granted or denied at various levels, and these permissions are inherited by the lower-level objects.
- Permissions can be denied at any level to override the permissions inherited from a higher level.

Permission propagation:
- Permissions can be propagated from a higher level to lower levels, and these permissions are inherited by the lower-level objects.
- Permissions can be denied at any level to override the permissions propagated from a higher level.

How to Read This Chart:
- Each box in the chart represents a permission or permission level.
- The color of the box indicates the level of the permission:
  - Red indicates a higher level of permission.
  - Yellow indicates a lower level of permission.
- The arrows connecting the boxes indicate the flow of permission inheritance or propagation.
- The permission names are listed in the boxes, and the permission levels are listed in the boxes.
- The chart includes the following features:
  - Server level permissions
  - Database level permissions
  - Schema object permissions
  - Object permissions
  - Role permissions
  - Server role permissions
  - Login permissions
  - Certificate permissions
  - Assembly permissions
  - Symmetric key permissions
  - Database role permissions
  - Event notification permissions
  - Database permission chart
  - Full text permission chart
  - Schedule permission chart
  - Server role permissions chart
  - Login role permissions chart
  - Certificate role permissions chart
  - Event notification role permissions chart
  - Full text role permissions chart
  - Schedule role permissions chart
  - Server role permission chart
  - Login role permission chart
  - Certificate role permission chart
  - Event notification role permission chart
  - Full text role permission chart
  - Schedule role permission chart

When contained databases are enabled, users can access SQL Server without a login. See database user.