**Authentication and Authorization in Cassandra**

**Authentication**

By default authentication is disabled you enable authentication through configuring cassandra.yaml file

When enables you have to provide credentials username and password

Example cqlsh -u cassandra -p cassandra

In cassandra.yaml file you have to do some configurations

| //default value  #authenticator: AllowAllAuthenticator  // set the authenticator value  authenticator:PasswordAuthenticator |
| --- |

After this restart cassandra and then login cassandra with these credentials

| cqlsh -u cassandra -p cassandra |
| --- |

But this username and password is known to everyone we can also change the password for the username cassandra

| cqlsh -u cassandra -p cassandra  AlTER USER cassandra with PASSWORD ‘db\_123’;  cqlsh -u cassandra -p db\_123  LIST ROLES |
| --- |



To prevent security breaches, replace the default superuser, *cassandra*, with another superuser with a different name

| CREATE ROLE <new\_super\_user> WITH PASSWORD = '<some\_secure\_password> AND SUPERUSER = true AND LOGIN = true; |
| --- |

Log in as the newly created superuser

| cqlsh -u db\_team -p dbteam123 |
| --- |

The cassandra superuser cannot be deleted from Cassandra. To neutralize the account, change the password to something long and incomprehensible, and alter the user's status to NOSUPERUSER

**Authorization**

By default authorization is disabled you enable authorization through configuring cassandra.yaml file

In cassandra.yaml file you have to do some configurations

| //default value  #authorizer: AllowAllAuthorizer  //set the authorizer value  authorizer: CassandraAuthorizer |
| --- |

After this restart cassandra and then login cassandra

CQL supports these authorization statements:

* GRANT
* LIST PERMISSIONS
* REVOKE

**GRANT**

In Cassandra's authorization system, the "GRANT" command is used to assign specific permissions to roles or users. It allows you to explicitly grant privileges to roles, specifying the actions they are authorized to perform on specific resources such as keyspaces, tables, or columns.

**Syntex**

| GRANT <privilege/permission> ON <resource> TO <role> |
| --- |

<resource>: This refers to the specific resource on which you want to grant permissions. It can be a keyspace, table, or even an individual column. You need to specify the keyspace and table name, optionally followed by the column name in the format <keyspace>.<table>[.<column>].

<role/user>: This represents the role or user to whom you want to grant the permissions. You can specify a role name or a username, depending on your authentication setup. The granted permissions will be applicable to all users or clients associated with the specified role.

**Privilege**

This represents the specific action or operation that you want to grant. It can be one of the available permissions in Cassandra, such as SELECT, INSERT, UPDATE, DELETE, MODIFY, CREATE, ALTER, DROP, and more. You can grant multiple permissions in a single GRANT statement, separating them with commas.

These are the available privileges:

* ALL PERMISSIONS
* ALTER
* AUTHORIZE
* CREATE
* DESCRIBE
* DROP
* EXECUTE
* MODIFY
* SELECT

**Permissions can be granted on:**

* CREATE - keyspace, table, function, role, index
* ALTER - keyspace, table, function, role
* DROP - keyspace, table, function, role, index
* SELECT - keyspace, table
* MODIFY - INSERT, UPDATE, DELETE, TRUNCATE - keyspace, table
* AUTHORIZE - GRANT PERMISSION, REVOKE PERMISSION - keyspace, table, function, and role
* DESCRIBE - LIST ROLES
* EXECUTE - SELECT, INSERT, UPDATE - functions

**Resource**

This refers to the specific resource on which you want to grant permissions. It can be a keyspace, table, or even an individual column. You need to specify the keyspace and table name, optionally followed by the column name in the format <keyspace>.<table>[.<column>]

These are the available resources

* ALL FUNCTIONS
* ALL FUNCTIONS IN KEYSPACE keyspace\_name
* FUNCTION function\_name
* ALL KEYSPACES
* KEYSPACE keyspace\_name
* TABLE table\_name
* ALL ROLES
* ROLE role\_name

**Roles**

This represents the role to whom you want to grant the permissions. You can specify a role name ,depending on your authentication setup.

| **Privilege** | **Resource** | **Permissions** |
| --- | --- | --- |
| ALL | resource\_name | All operations that are applicable to the resource and its ancestors. |
| CREATE | ALL KEYSPACES | CREATE KEYSPACE and CREATE TABLE in any keyspace. |
| CREATE | KEYSPACE keyspace\_name | CREATE TABLE in specified keyspace. |
| CREATE | ALL FUNCTIONS | CREATE FUNCTION in any keyspace and CREATE AGGREGATE in any keyspace. |
| CREATE | ALL FUNCTIONS IN KEYSPACE keyspace\_name | CREATE FUNCTION and CREATE AGGREGATE in specified keyspace. |
| CREATE | ALL ROLES | CREATE ROLE |
| ALTER | ALL KEYSPACES | ALTER KEYSPACE and ALTER TABLE in any keyspace. |
| ALTER | KEYSPACE keyspace\_name | ALTER KEYSPACE and ALTER TABLE in specified keyspace. |
| ALTER | TABLE table\_name | ALTER TABLE specified table. |
| ALTER | ALL FUNCTIONS | CREATE FUNCTION and CREATE AGGREGATE, also replace existing. |
| ALTER | ALL FUNCTIONS IN KEYSPACE keyspace\_name | CREATE FUNCTION and CREATE AGGREGATE: , also replace existing in specified keyspace |
| ALTER | FUNCTION function\_name | CREATE FUNCTION and CREATE AGGREGATE, also replace existing. |
| ALTER | ALL ROLES | ALTER ROLE on any role |
| ALTER | ROLE role\_name | ALTER ROLE specified role. |
| DROP | ALL KEYSPACES | DROP KEYSPACE and DROP TABLE in any keyspace |
| DROP | KEYSPACE keyspace\_name | DROP TABLE in specified keyspace |
| DROP | TABLE table\_name | DROP TABLE specified. |
| DROP | ALL FUNCTIONS | DROP FUNCTION and DROP AGGREGATE in any keyspace. |
| DROP | ALL FUNCTIONS IN KEYSPACE keyspace\_name | DROP FUNCTION and DROP AGGREGATE in specified keyspace. |
| DROP | FUNCTION function\_name | DROP FUNCTION specified function. |
| DROP | ALL ROLES | DROP ROLE on any role. |
| DROP | ROLE role\_name | DROP ROLE specified role. |
| SELECT | ALL KEYSPACES | SELECT on any table. |
| SELECT | KEYSPACE keyspace\_name | SELECT on any table in specified keyspace. |
| SELECT | TABLE table\_name | SELECT on specified table. |
| SELECT | ALL MBEANS | Call getter methods on any mbean. |
| SELECT | MBEANS pattern | Call getter methods on any mbean matching a wildcard pattern. |
| SELECT | MBEAN mbean\_name | Call getter methods on named mbean. |
| MODIFY | ALL KEYSPACES | INSERT, UPDATE, DELETE and TRUNCATE on any table. |
| MODIFY | KEYSPACE keyspace\_name | INSERT, UPDATE, DELETE and TRUNCATE on any table in specified keyspace. |
| MODIFY | TABLE table\_name | INSERT, UPDATE, DELETE and TRUNCATE on specified table. |
| MODIFY | ALL MBEANS | Call setter methods on any mbean. |
| MODIFY | MBEANS pattern | Call setter methods on any mbean matching a wildcard pattern. |
| MODIFY | MBEAN mbean\_name | Call setter methods on named mbean. |
| AUTHORIZE | ALL KEYSPACES | GRANT PERMISSION and REVOKE PERMISSION on any table. |
| AUTHORIZE | KEYSPACE keyspace\_name | GRANT PERMISSION and REVOKE PERMISSION on any table in specified keyspace. |
| AUTHORIZE | TABLE table\_name | GRANT PERMISSION and REVOKE PERMISSION on specified table. |
| AUTHORIZE | ALL FUNCTIONS | GRANT PERMISSION and REVOKE PERMISSION on any function. |
| AUTHORIZE | ALL FUNCTIONS IN KEYSPACE keyspace\_name | GRANT PERMISSION and REVOKE PERMISSION in specified keyspace. |
| AUTHORIZE | FUNCTION function\_name | GRANT PERMISSION and REVOKE PERMISSION on specified function. |
| AUTHORIZE | ALL ROLES | GRANT ROLE and REVOKE ROLE on any role. |
| AUTHORIZE | ROLES | GRANT ROLE and REVOKE ROLE on specified roles |
| DESCRIBE | ALL ROLES | LIST ROLES on all roles or only roles granted to another, specified role. |
| DESCRIBE | ALL MBEANS | Retrieve metadata about any mbean from the platform's MBeanServer. |
| EXECUTE | ALL FUNCTIONS | SELECT, INSERT and UPDATE using any function, and use of any function in CREATE AGGREGATE. |
| EXECUTE | ALL FUNCTIONS IN KEYSPACE keyspace\_name | SELECT, INSERT and UPDATE using any function in specified keyspace and use of any function in keyspace in CREATE AGGREGATE. |
| EXECUTE | FUNCTION function\_name | SELECT, INSERT and UPDATE using specified function and use of the function in CREATE AGGREGATE. |
| role\_name | resource\_name | Roles are a collection of privileges; grant all the privileges in a role on any resource. |

LIST PERMISSION:

In Cassandra's authorization system, the "LIST PERMISSIONS" command is used to view the permissions granted to roles or users. It allows you to retrieve the list of permissions assigned to a specific role or user, providing visibility into their authorized actions on various resources.

**Syntex**

| LIST privilege ON resource\_name OF role\_name NORECURSIVE |
| --- |

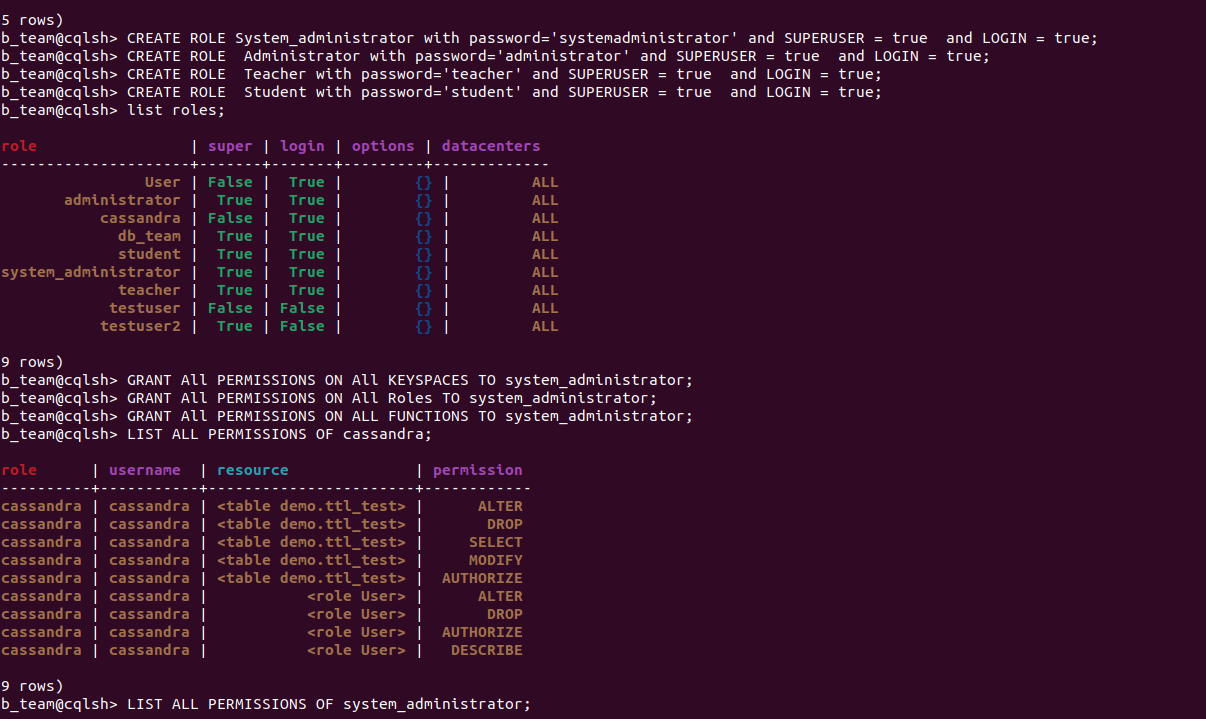
**NON RECURSIVE**

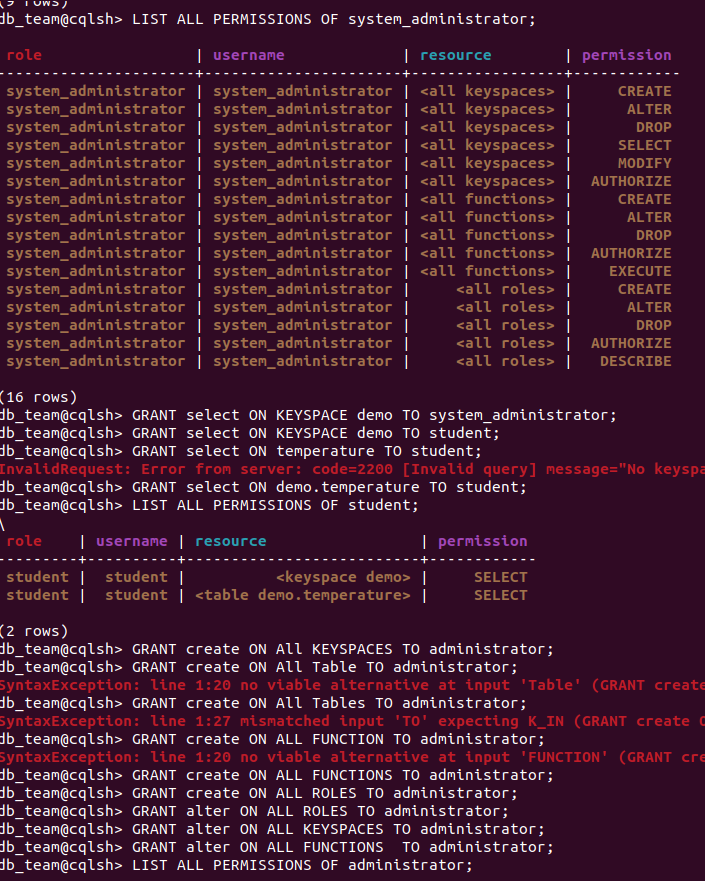
Only display permissions granted to the role. By default permissions checks are recursive; it shows direct and inherited permissions.

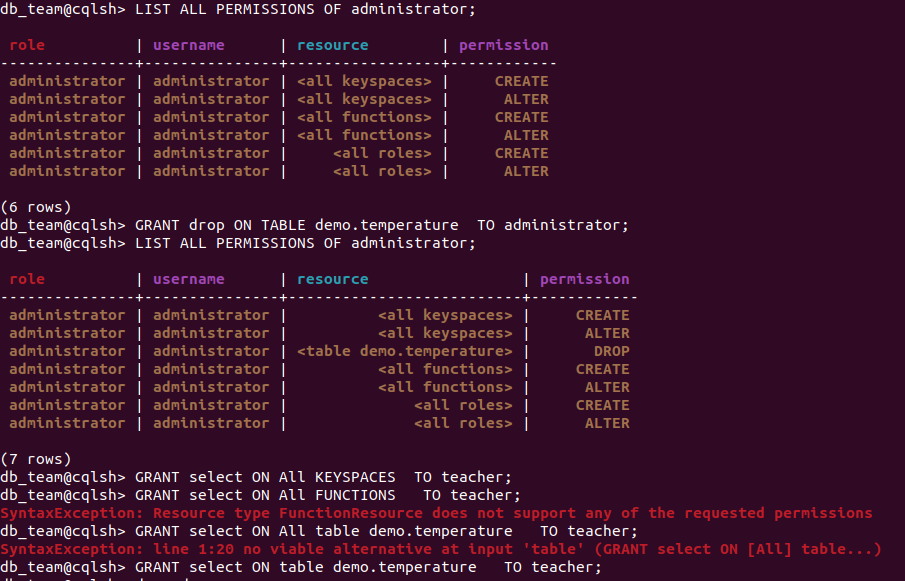
# **REVOKE** In Cassandra's authorization system, the "REVOKE" command is used to revoke or remove specific permissions from roles or users. It allows you to explicitly revoke privileges that were previously granted, thereby restricting the actions that can be performed on specific resources within the database.

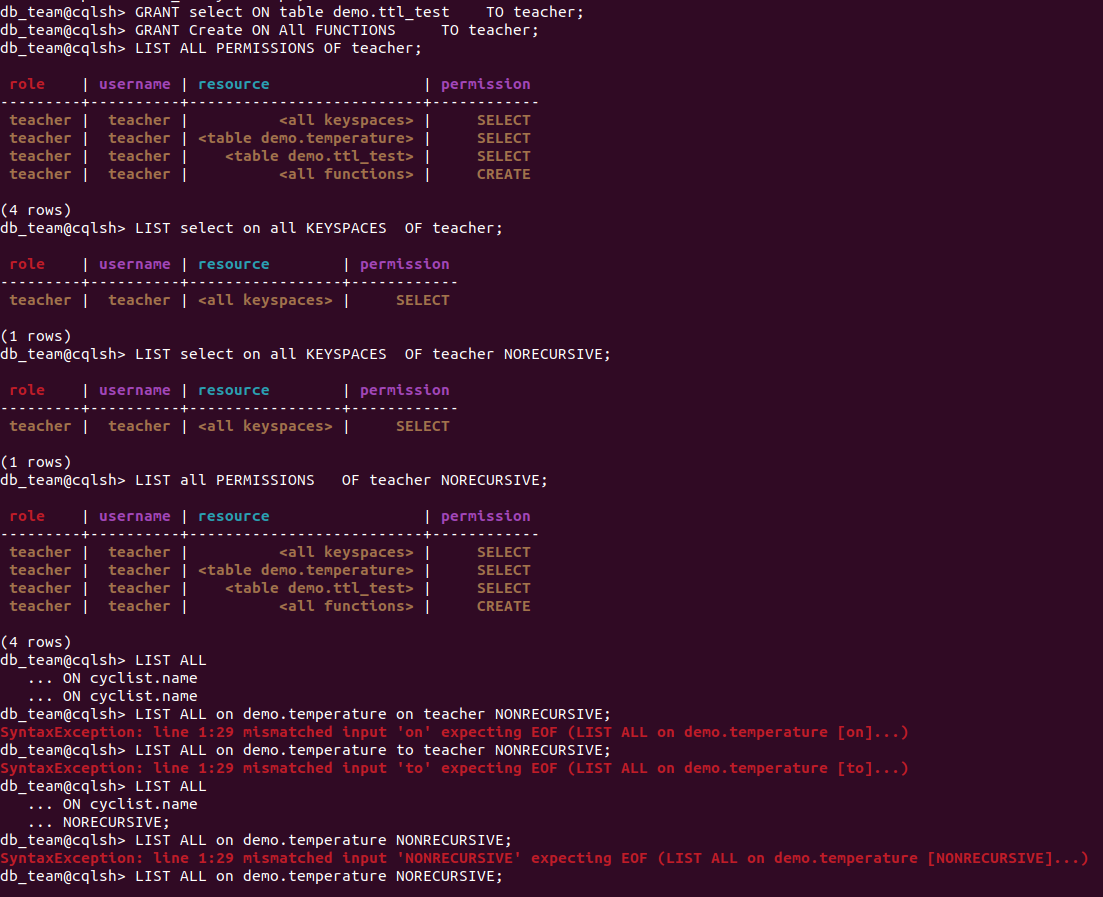
| REVOKE privilege ON resource\_name FROM role\_name |
| --- |

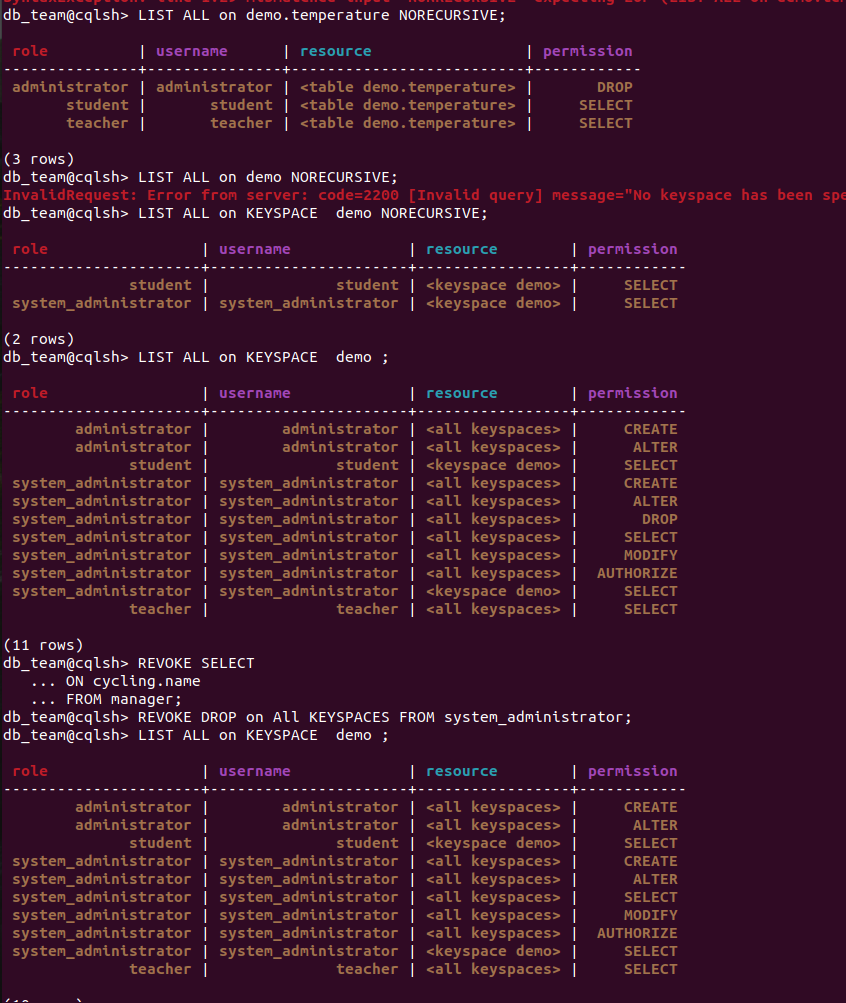
**Example:**

****

****

****

****

****