DataStax Enterprise User Management and Privilege System

DataStax Enterprise (DSE) 6.9 implements Role-Based Access Control (RBAC) for secure user management and fine-grained authorization. RBAC is enabled after setting up DSE Unified Authentication (via dse.yaml and cassandra.yaml).

Roles

Definition: A role is a database entity that holds privileges for accessing resources. It can act as a user (with LOGIN=true) or a permission set (no login needed).
Properties:
LOGIN: (Default: false) Enables CQL execution (e.g., via cqlsh or drivers).
SUPERUSER: (Default: false) Grants all privileges (root-like access).
PASSWORD: For internal auth; hashed for security.
Nesting: Roles can inherit from others via GRANT ROLE, allowing reusable permission sets.

Privileges

Privilege	Description
CREATE	Create keyspaces/tables/functions.
ALTER	Modify existing objects.
DROP	Delete objects.
SELECT	Read data (queries).
MODIFY	Write data (INSERT/UPDATE/DELETE).
AUTHORIZE	Grant/revoke privileges.
DESCRIBE	View metadata (e.g., schema).
EXECUTE	Run UDFs
RESTRICT	Deny access (overrides grants; superusers only).

DSE-Specific Privileges:

Search (Solr): SOLR permissions on indices (e.g., CREATE SOLR INDEX).
Graph: VERTEX/EDGE access (e.g., MODIFY ON GRAPH.VERTEX).
Analytics (Spark): EXECUTE ON SPARK.JOB.
RPC: For CQL methods (e.g., EXECUTE ON rpc_method).

Resource Hierarchy

Permissions follow this structure (grant on higher level cascades down):

ALL KEYSPACES > **KEYSPACE <name>** > **TABLE <name>** > **ROWS** (for RLAC).
FUNCTIONS/AGGREGATES: For UDFs/UDAs.
DSE Resources: e.g., SOLR.CORE, GRAPH.KEYSPACE, SPARK.ANALYTICS.
Row-Level Access Control (RLAC) adds granular filters on partition keys for table rows.

Configuration

Enable RBAC: Set authenticator: DseAuthenticator and authorizer: DseAuthorizer in cassandra.yaml. Configure role_management_options: { mode: internal \| ldap } in dse.yaml.
LDAP Integration: Map groups to roles; no per-user roles needed.
Caching: Tune credentials_validity_in_ms, roles_validity_in_ms, permissions_validity_in_ms in cassandra.yaml for performance (default: 2000ms).
Proxy Authentication: For apps; roles execute as other roles via DSE proxy.
Initial Setup: Log in as cassandra, create superuser, then REVOKE LOGIN FROM cassandra; or DROP ROLE cassandra;.

Management Commands

All via CQL (cqlsh or drivers). Requires superuser or AUTHORIZE privilege.

Command	Description	Syntax	Example
CREATE ROLE	Creates a role/user.	CREATE ROLE <role_name> WITH [LOGIN = {true|false}] [PASSWORD = '<password>'] [SUPERUSER = {true|false}];	CREATE ROLE analyst WITH LOGIN = true AND PASSWORD = 'secretpass'; (Creates login role)
ALTER ROLE	Updates role properties.	ALTER ROLE <role_name> WITH [PASSWORD = '<password>'] [SUPERUSER = {true|false}] [LOGIN = {true|false}];	ALTER ROLE analyst WITH SUPERUSER = true; (Elevates to superuser)
DROP ROLE	Deletes role (must not be granted to others).	DROP ROLE <role_name>;	DROP ROLE analyst; (Removes role)
GRANT ROLE	Nests roles (inherits privileges).	GRANT <granted_role> TO <receiver_role>;	GRANT dba TO analyst; (Analyst inherits dba privileges)
REVOKE ROLE	Removes role nesting.	REVOKE <granted_role> FROM <receiver_role>;	REVOKE dba FROM analyst; (Removes inheritance)
LIST ROLES	Lists roles (with inheritance).	LIST ROLES [OF <role_name>] [NORECURSIVE];	LIST ROLES OF analyst; Output: ```role:disable-run

Privilege Commands

Command	Description	Syntax	Example
GRANT	Assigns privilege on resource.	GRANT <privilege> ON <resource> TO <role>;	GRANT SELECT ON KEYSPACE cycling TO analyst; (Read access to keyspace) GRANT MODIFY ON TABLE cycling.cyclist TO analyst; (Write to specific table) GRANT CREATE ON ALL KEYSPACES TO dba; (Global create) GRANT EXECUTE ON SPARK.JOB TO spark_user; (DSE Analytics)
REVOKE	Removes privilege.	REVOKE <privilege> ON <resource> FROM <role>;	REVOKE SELECT ON KEYSPACE cycling FROM analyst; (Revokes read access)
LIST PERMISSIONS	Lists effective privileges.	LIST PERMISSIONS [ON <resource>] [OF <role_name>];	LIST PERMISSIONS ON cycling OF analyst; Output: resource_type | resource | role | permission data | [cycling] | analyst | select
RESTRICT	Denies access (overrides grants).	RESTRICT <privilege> ON <resource> TO <role>;	RESTRICT MODIFY ON TABLE cycling.cyclist TO analyst; (Blocks writes even if granted)