

Object Type	Applicable Privileges	Notes / Description
System (Cluster-wide)	ALL, BACKUP, CANCELQUERY, CONNECT, CONTROLJOB, CREATEDB, CREATELOGIN, CREATEROLE, MODIFYCLUSTERSETTING, MODIFYSQLCLUSTERSETTING, NOSQLLOGIN, REPAIRCLUSTER, REPAIRCLUSTERMETADATA, RESTORE, VIEWACTIVITY, VIEWACTIVITYREDACTED, VIEWCLUSTERMETADATA, VIEWCLUSTERSETTING, VIEWDEBUG, VIEWJOB, VIEWSYSTEMTABLE, EXTERNALCONNECTION, EXTERNALIOIMPLICITACCESS	Cluster-wide super-privileges. Granted with GRANT SYSTEM <priv> TO role;. ALL grants every system privilege.
Database	ALL, BACKUP, CONNECT, CREATE, CREATEDB, DROP, RESTORE, ZONECONFIG	Controls database-level actions (e.g., CONNECT allows login, CREATE allows object creation inside).
Schema	ALL, CREATE, USAGE	USAGE allows looking up objects in the schema; CREATE allows new objects in it.
Table (incl. views, materialized views)	ALL, BACKUP, BYPASSRLS, CHANGEFEED, DELETE, DROP, INSERT, REPLICATIONDEST, REPLICATIONSOURCE, SELECT, UPDATE, ZONECONFIG	Core DML/DDL privileges. CHANGEFEED for CDC, BYPASSRLS for row-level security bypass, replication privileges for physical cluster replication.
Sequence	ALL, DELETE, DROP, INSERT, SELECT, USAGE, ZONECONFIG	USAGE allows NEXTVAL/CURRVAL; SELECT also works for reading.
Function (incl. procedures)	ALL, EXECUTE	EXECUTE is the only specific privilege; ALL includes it plus DROP rights.
Type (user-defined)	ALL, USAGE	USAGE allows using the type in table definitions, casts, etc.
External Connection	ALL, DROP, USAGE	For storage connections (S3, GCS, etc.). USAGE allows the connection to be referenced in BACKUP/RESTORE/IMPORT.

Object Type	Applicable Privileges	Notes / Description
System (Cluster-wide)	ALL, BACKUP, CANCELQUERY, CONTROLJOB, CREATEDB, CREATELOGIN, CREATEROLE, EXTERNALCONNECTION, EXTERNALIOIMPLICITACCESS, MODIFYCLUSTERSETTING, MODIFYSQLCLUSTERSETTING, NOSQLLOGIN, REPAIRCLUSTER, REPAIRCLUSTERMETADATA, RESTORE, VIEWACTIVITY, VIEWACTIVITYREDACTED, VIEWCLUSTERMETADATA, VIEWCLUSTERSETTING, VIEWDEBUG, VIEWJOB, VIEWSYSTEMTABLE	Cluster-wide privileges. ALL grants every system privilege. EXTERNALCONNECTION enables creating external connections (e.g., to S3, Kafka). VIEWSYSTEMTABLE provides read access to system tables (v23.1+). NOSQLLOGIN blocks SQL access.
Database	ALL, CONNECT, CREATE, DROP, ZONECONFIG	CONNECT allows metadata viewing and connections. CREATE permits object creation inside the database and multi-region zone configs.
Schema	ALL, CREATE, USAGE	USAGE enables object lookup in the schema. CREATE allows new objects (may be restricted by cluster setting).
Table (incl. views, materialized views)	ALL, BACKUP, BYPASSRLS, CHANGEFEED, DELETE, DROP, INSERT, REPLICATIONDEST, REPLICATIONSOURCE, SELECT, UPDATE, ZONECONFIG	DML/DDI actions. BYPASSRLS bypasses row-level security (needs separate read/write privs). CHANGEFEED for change data capture. REPLICATIONDEST/SOURCE for logical replication (replaces deprecated REPLICATION).
Sequence	ALL, CREATE, DELETE, DROP, INSERT, SELECT, UPDATE, USAGE, ZONECONFIG	USAGE for NEXTVAL/CURRVAL. UPDATE for SETVAL. CREATE may apply to default privileges for new sequences.
Type (user-defined)	ALL, USAGE	USAGE allows type usage in definitions, casts, etc. Applies to ENUMs and composite types.
Function (incl. procedures)	ALL, EXECUTE	EXECUTE permits calling the function/procedure.
External Connection	ALL, USAGE	USAGE allows referencing in BACKUP, RESTORE, IMPORT, EXPORT, CHANGEFEED. Creation requires SYSTEM

Object Type	Applicable Privileges	Notes / Description
		EXTERNALCONNECTION privilege. ALL includes DROP rights.

Public Role and its privileges:

Public Role exist in CockroachDB and it is invisible to any of the catalog objects, by default all users belongs to PUBLIC role. Any privilege granted to PUBLIC role is like granting that to all current/future roles.

Below table provide details of default privileges granted to PUBLIC role on each object

Object Type	Default Privileges for PUBLIC	Notes
System (Cluster-wide)	None	PUBLIC has no system-level privileges by default; all users start with minimal access.
Database	CONNECT	Automatically granted on all databases to allow metadata viewing and connection. Revoking this would prevent access to the database entirely.
Schema	USAGE (on the default public schema in each database)	Enables lookup of objects within the default schema. For user-defined schemas, USAGE must be explicitly granted.
Table (incl. views, materialized views)	None	No DML/DDI privileges (e.g., no SELECT, INSERT); must be explicitly granted.
Sequence	None	No access (e.g., no USAGE, SELECT); explicit grants required.
Function (incl. procedures)	None	No EXECUTE; explicit grant needed.
Type (user-defined)	None	No USAGE; explicit grant required, though examples may show grants for specific types.
External Connection	None	No USAGE or creation rights; requires SYSTEM EXTERNALCONNECTION privilege for creation.

SHOW GRANTS ON DATABASE ; or SHOW GRANTS ON SCHEMA .;