（new in v2.0） 角色是将一组具有相同权限的用户组织在一起，便于对用户及权限进行管理。

目前可使用如下SQL语句进行角色和权限的管理：

* [CREATE ROLE (企业版特性)](https://www.cockroachlabs.com/docs/stable/create-role.html)
* [DROP ROLE (企业版特性)](https://www.cockroachlabs.com/docs/stable/drop-role.html)
* [GRANT <roles> (企业版特性)](https://www.cockroachlabs.com/docs/stable/grant-roles.html)
* [REVOKE <roles> (企业版特性)](https://www.cockroachlabs.com/docs/stable/revoke-roles.html)
* [GRANT <privileges>](http://doc.cockroachchina.baidu.com/#develop/sql-statements/GRANT-%3Cprivileges%3E/)
* [REVOKE <privileges>](https://www.cockroachlabs.com/docs/stable/revoke.html)
* [SHOW ROLES](https://www.cockroachlabs.com/docs/stable/show-roles.html)
* [SHOW GRANTS](https://www.cockroachlabs.com/docs/stable/show-grants.html)

相关术语

| **英文** | **中文** | **简介** |
| --- | --- | --- |
| Role | 角色 | 一个包含任意数量的用户和其他角色的组合 |
| Role admin | 角色管理员 | 能够授予其他用户角色的特殊用户，可以使用指令WITH ADMIN OPTION授予权限成为角色管理员 |
| Superuser/Admin | 超级管理员 | 拥有admin角色的用户，能够[创建](https://www.cockroachlabs.com/docs/stable/create-role.html)和[删除角色](https://www.cockroachlabs.com/docs/stable/drop-role.html)，数据库默认创建了admin角色且不可删除。 |
| root | root | 数据库默认有一个授予admin角色的用户 |
| Inherit | 继承 | 将角色授予用户或其他角色的行为 |
| Direct member | 直接成员 | 一个角色的直接成员 |
| Indirect member | 间接成员 | 一个角色的间接成员 |

示例

准备

* 申请[企业版license](http://doc.cockroachchina.baidu.com/#deploy/enterprise-licensing/)。
* 非安全模式启动一个节点

cockroach start --insecure --store=roles --host=localhost

创建用户、角色与授权

* 开启新终端，使用root用户登陆，创建maxroach用户

cockroach user set maxroach --insecure

* 以root用户启动[内置shell](http://doc.cockroachchina.baidu.com/#quick-start/learn-cockroachdb-sql/use-the-built-in-sql-client/)

cockroach sql --insecure

* 创建数据库并设置为默认数据库

**CREATE** **DATABASE** test\_roles;

**SET** **DATABASE** = test\_roles;

* 创建角色system\_ops

**CREATE** ROLE system\_ops;

* 查看所有角色

**SHOW** ROLES;

+*------------+*

| rolename |

+*------------+*

| admin |

| system\_ops |

+*------------+*

* 为system\_ops角色授权

**GRANT** **CREATE**, **SELECT** **ON** **DATABASE** test\_roles **TO** system\_ops;

**SHOW** **GRANTS** **ON** **DATABASE** test\_roles;

+*------------+--------------------+------------+------------+*

| Database | Schema | User | Privileges |

+*------------+--------------------+------------+------------+*

| test\_roles | crdb\_internal | admin | ALL |

| test\_roles | crdb\_internal | root | ALL |

| test\_roles | crdb\_internal | system\_ops | **CREATE** |

| test\_roles | crdb\_internal | system\_ops | **SELECT** |

| test\_roles | information\_schema | admin | **ALL** |

| test\_roles | information\_schema | root | **ALL** |

| test\_roles | information\_schema | system\_ops | **CREATE** |

| test\_roles | information\_schema | system\_ops | **SELECT** |

| test\_roles | pg\_catalog | admin | **ALL** |

| test\_roles | pg\_catalog | root | **ALL** |

| test\_roles | pg\_catalog | system\_ops | **CREATE** |

| test\_roles | pg\_catalog | system\_ops | **SELECT** |

| test\_roles | **public** | admin | **ALL** |

| test\_roles | **public** | root | **ALL** |

| test\_roles | **public** | system\_ops | **CREATE** |

| test\_roles | **public** | system\_ops | **SELECT** |

+*------------+--------------------+------------+------------+*

* 赋予用户角色

**GRANT** system\_ops **TO** maxroach;

测试

退出当前shell，尝试用maxroach用户操作数据库test\_roles

* 启动内置shell

cockroach sql --user=maxroach --database=test\_roles --insecure

* 创建表

**CREATE** **TABLE** employees (

id **UUID** **DEFAULT** uuid\_v4()::**UUID** **PRIMARY** **KEY**,

**profile** JSONB

);

* 删除表

**DROP** **TABLE** employees;

pq: user maxroach does not have **DROP** privilege **on** relation employees

maxroach用户不能删除employees表，因为system\_ops角色只有该表的CRETAE和SELECT语句权限，没有删除该表的权限。

* 查看表关联的用户和权限

**SHOW** **GRANTS** **ON** **TABLE** employees;

+*------------+--------+-----------+------------+------------+*

| Database | Schema | Table | User | Privileges |

+*------------+--------+-----------+------------+------------+*

| test\_roles | public | employees | admin | ALL |

| test\_roles | public | employees | root | ALL |

| test\_roles | public | employees | system\_ops | **CREATE** |

| test\_roles | **public** | employees | system\_ops | **SELECT** |

+*------------+--------+-----------+------------+------------+*

* 退出当前shell，以root用户启动交互式shell

cockroach sql --insecure

* 尝试删除角色system\_ops的权限

**REVOKE** **ALL** **ON** **DATABASE** test\_roles **FROM** system\_ops;

**SHOW** **GRANTS** **ON** **DATABASE** test\_roles;

+*------------+--------------------+-------+------------+*

| Database | Schema | User | Privileges |

+*------------+--------------------+-------+------------+*

| test\_roles | crdb\_internal | admin | ALL |

| test\_roles | crdb\_internal | root | ALL |

| test\_roles | information\_schema | admin | ALL |

| test\_roles | information\_schema | root | ALL |

| test\_roles | pg\_catalog | admin | ALL |

| test\_roles | pg\_catalog | root | ALL |

| test\_roles | public | admin | ALL |

| test\_roles | public | root | ALL |

+*------------+--------------------+-------+------------+*

**REVOKE** **ALL** **ON** **TABLE** test\_roles.\* **FROM** system\_ops;

**SHOW** **GRANTS** **ON** **TABLE** test\_roles.\*;

+*------------+--------+-----------+-------+------------+*

| Database | Schema | Table | User | Privileges |

+*------------+--------+-----------+-------+------------+*

| test\_roles | public | employees | admin | ALL |

| test\_roles | public | employees | root | ALL |

+*------------+--------+-----------+-------+------------+*

* 删除角色

**DROP** ROLE system\_ops;