

MongoDB 权限认证

李焕贞

河北师范大学软件学院

MongoDB权限认证

1、创建管理员账号

```
db.createUser({ user: "zhangsan", pwd: "zhangsan123", roles: [{ role: "userAdminAnyDatabase", db: "admin" }] })
```

2、修改MongoDB安装目录中的配置文件 bin/mongod.cfg，重启服务 security:

authorization: enabled

注意：authorization前面要有两个空格

3、show dbs，会报错

```
> show dbs
2019-02-12T15:41:30.812+0800 E QUERY [js] Error: listDatabases failed:
  "ok" : 0,
  "errmsg" : "command listDatabases requires authentication",
  "code" : 13,
  "codeName" : "Unauthorized"
> :
_getErrorWithCode@src/mongo/shell/utils.js:25:13
Mongo.prototype.getDBs@src/mongo/shell/mongo.js:124:1
shellHelper.show@src/mongo/shell/utils.js:876:19
shellHelper@src/mongo/shell/utils.js:766:15
@<shellhelp2>:1:1
```

MongoDB权限认证

4、密码认证:

```
db.auth("zhangsan","zhangsan123")
```

返回1, 表示成功登录

5、创建普通用户

```
db.createUser({ user: "lisi",pwd: "lisi123", roles: [{ role:  
"read", db: "student"}]})
```

```
6. db.auth("testAdmin","123456")
```

```
db.class2.insert({name:"tom"})
```

```
> db.class2.insert<<name:'aaa'>>  
WriteCommandError<{  
  "ok" : 0,  
  "errmsg" : "not authorized on student to execute command { insert: \"cla  
ss2\", ordered: true, lsid: { id: UUID<\"901325ab-c8f3-47d6-a554-57a543e3eda7\">  
>, $db: \"student\" } }",  
  "code" : 13,  
  "codeName" : "Unauthorized"  
>>  
>
```

roles: 指定用户的角色, 可以用一个空数组给新用户设定空角色; 在roles字段, 可以指定内置角色和用户定义的角色。role里的角色可以选:

- Read: 允许用户读取指定数据库
- readWrite: 允许用户读写指定数据库
- dbAdmin: 允许用户在指定数据库中执行管理函数, 如索引创建、删除, 查看统计或访问system.profile
- userAdmin: 允许用户向system.users集合写入, 可以找指定数据库里创建、删除和管理用户
- clusterAdmin: 只在admin数据库中可用, 赋予用户所有分片和复制集相关函数的管理权限。

MongoDB权限认证

- readAnyDatabase: 只在admin数据库中可用，赋予用户所有数据库的读权限
- readWriteAnyDatabase: 只在admin数据库中可用，赋予用户所有数据库的读写权限
- userAdminAnyDatabase: 只在admin数据库中可用，赋予用户所有数据库的userAdmin权限
- dbAdminAnyDatabase: 只在admin数据库中可用，赋予用户所有数据库的dbAdmin权限。
- root: 只在admin数据库中可用。超级账号，超级权限

MongoDB权限认证

- 修改用户密码

`db.changeUserPassword("accountUser", "S0h3TbYhx8ypJPxmt1o0fL")` 删除用户(只删除当前数据中的football用户)

`db.dropUser("football");`

- 授权

`use products`

`db.grantRolesToUser("accountUser01", ["readWrite" , { role: "read", db: "stock" }], { w: "majority" , wtimeout: 4000 })`

- 关闭MongoDB服务

`use admin;`

`db.shutdownServer();`