mongoDB® 存取權限

朱克剛

建立管理者

```
test> use admin
admin> db.createUser(
  {
    user: 'myAdmin',
    pwd: passwordPrompt(),
    roles: [
      { role: 'userAdminAnyDatabase', db: 'admin' },
      { role: 'readWriteAnyDatabase', db: 'admin' }
    ]
  }
)
```

開啟存取管理功能

```
$ mongod --auth
```

登入授權使用者

```
$ mongosh  -u  myAdmin  -p  1234
```

```
test> use admin
admin> db.auth("myAdmin", "1234")
```

建立某資料庫管理者

```
admin> use opendata
opendata> db.createUser(
  {
    user: 'opendataDbAdmin',
    pwd: '1234',
    roles: [
        { role: 'dbAdmin', db: 'opendata' },
        { role: 'userAdmin', db: 'opendata' }
    ]
  }
)
```

使用資料庫管理者管理資料庫

```
test> use opendata
opendata> db.auth('opendataDbAdmin', '1234')
opendata> db.createUser(
  {
    user: 'user',
    pwd: '1234',
    roles: [
        { role: 'readWrite', db: 'opendata' }
    ]
  }
)
```

PYTHON 登入

```
import pymongo

uri = 'mongodb://user:1234@localhost:27017/opendata'
client = pymongo.MongoClient(uri)
```

刪除使用者

```
use opendata
db.dropUser("user")
```

列出所有使用者

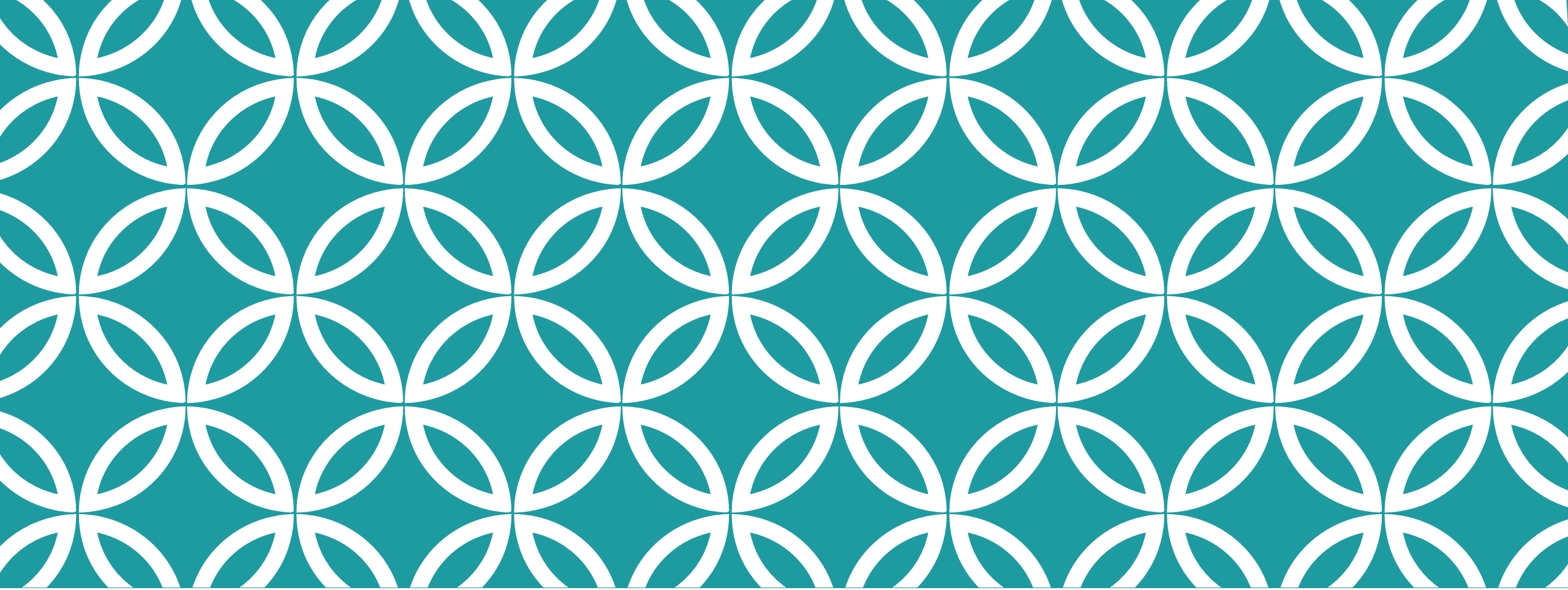
```
use admin
db.system.users.find().pretty()
```

修改密碼

```
use opendata
db.changeUserPassword("user", "new_password")
```

其餘內建角色

https://docs.mongodb.com/manual/reference/built-in-roles/#built-in-roles



覆寫與分片的存取權限

KEYFILE

產生 keyfile

```
$ openssl rand -base64 756 > <path-to-keyfile>
$ chmod 400 <path-to-keyfile>
```

複寫集設定

```
rs0 [direct: primary] test> use admin
rs0 [direct: primary] admin> db.createUser(
  {
    user: 'rs0Admin',
    pwd: passwordPrompt(),
    roles: [
      { role: 'clusterAdmin', db: 'admin' },
      { role: 'userAdminAnyDatabase', db: 'admin' },
      { role: 'readWriteAnyDatabase', db: 'admin' }
    ]
  }
)
```

```
$ mongod --port 20000 --dbpath data/dbA --replSet rs0 --keyFile <path-to-keyfile>
$ mongod --port 20001 --dbpath data/dbB --replSet rs0 --keyFile <path-to-keyfile>
$ mongod --port 20002 --dbpath data/dbC --replSet rs0 --keyFile <path-to-keyfile>
```

分片

覆寫集啟動時設定權限參數（參考上一頁）

Config Server啟動時不設定權限參數

mongos啟動時不設定權限參數

進入後建立超級管理者

```
use admin
db.createUser(
   {
     user: "admin",
     pwd: "1234",
     roles: [
        { role: "clusterManager", db: "admin" },
        { role: "userAdminAnyDatabase", db: "admin" }
     ]
   }
)
```

建立資料庫管理者

分片有分片的資料庫管理者，獨立於覆寫或單一主機的管理權限

```
use opendata
db.createUser(
  {
    user: "ckk",
    pwd: "1234",
    roles: [ { role: "dbOwner", db: "opendata" } ]
  }
)
```

ENABLE權限設定

Configure Server

```
$ mongod --port 30000 --dbpath data/cfg/dbA --replSet cs0 --configsvr --keyFile <path-to-keyfile>
$ mongod --port 30001 --dbpath data/cfg/dbB --replSet cs0 --configsvr --keyFile <path-to-keyfile>
$ mongod --port 30002 --dbpath data/cfg/dbC --replSet cs0 --configsvr --keyFile <path-to-keyfile>
```

Router

```
$ mongos --configdb cs0/localhost:30000 --keyFile <path-to-keyfile>
```