Chapter 3: Auditing and Best Practices

Homework 3.2 : Change audit filters to audit specific user

Back to the Question

This homework is similar to the last one. The key difference this time is that we need to also build an audit filter.

One way to build audit filters is to start up a test server with auditing enabled, then run the command that you're trying to filter for. Here's an example audit log, for an operation performed by `steve`:

COPY

```
{
  "atype": "createCollection",
  "ts": {
    "$date": "2006-04-30T10:40:53.751+0000"
  },
  "local": {
    "ip": "127.0.0.1",
    "port": 31311
  },
  "remote": {
    "ip": "127.0.0.1",
    "port": 46314
  },
  "users": [
    {
      "user": "steve",
      "db": "admin"
    }
  ],
  "roles": [
    {
      "role": "root",
      "db": "admin"
    }
  ],
  "param": {
    "ns": "production.myCollection"
```

```
  },
  "result": 0
}
```

From this document we can derive our filter document:

```
{ "users.user": "steve" }
```

COPY

First, we need to set up our directory structure:

```
$ mkdir -p ~/M310-HW-3.2/{r0,r1,r2}
```

COPY

After that, we can go ahead and start each member of our replica set with our new audit filter:

COPY

```
$ mongod --dbpath ~/M310-HW-3.2/r0 --logpath ~/M310-HW-
3.2/r0/mongo.log --port 31320 \
         --fork --replSet HW-3.2 --auditDestination file --
auditFormat JSON \
         --auditPath ~/M310-HW-3.2/r0/auditLog.json --auditFilter
'{ "users.user": "steve" }'
$ mongod --dbpath ~/M310-HW-3.2/r1 --logpath ~/M310-HW-
3.2/r1/mongo.log --port 31321 \
         --fork --replSet HW-3.2 --auditDestination file --
auditFormat JSON \
         --auditPath ~/M310-HW-3.2/r1/auditLog.json --auditFilter
'{ "users.user": "steve" }'
$ mongod --dbpath ~/M310-HW-3.2/r2 --logpath ~/M310-HW-
3.2/r2/mongo.log --port 31322 \
         --fork --replSet HW-3.2 --auditDestination file --
auditFormat JSON \
         --auditPath ~/M310-HW-3.2/r2/auditLog.json --auditFilter
'{ "users.user": "steve" }'
```

From here, all we need to do is connect to the **mongod** running on port **31320**, initiate the replica set, add the other members, and create an account for Steve.

COPY

```
$ mongo --port 31320
use admin
rs.initiate()
rs.add('database.m310.mongodb.university:31321')
rs.add('database.m310.mongodb.university:31322')
db.createUser({user: 'steve', pwd: 'secret', roles: ['root']})
```

Proceed to next section