Auditing in MongoDB

Enable and Configure Audit Output

- Use the --auditDestination option to enable auditing and specify where to output the audit events . This option is set while starting the mongod using command line
- The same can be set in the mongod.conf ,using the following parameter
- auditLog:
- destination:<value>

What all being audited

MongoDB will be auditing the following actions

- schema (DDL),
- replica set and sharded cluster,
- authentication and authorization, and
- CRUD operations (requires auditAuthorizationSuccess set to true).

What are the audit destination

MongoDB can write the audit information to any of the following output

Syslog (Not available on Windows)
Console
JSON file
BSON File

Writing the audting information to SYSLOG

```
$ mongod --dbpath /u01/data  --auditDestination syslog
```

Or in the configuration file

```
storage:
  dbPath: /u01/data
auditLog:
  destination: syslog
```

Writing the audit information to console

```
$ mongod --dbpath /data/db --auditDestination console
```

Or

Update the configuration file with the following information

```
 storage:
   dbPath: /data/db
auditLog:
   destination: console
```

Writing the audit information to json

```
$ mongod --dbpath /data/db --auditDestination file --auditFormat JSON --auditPath data/db/auditLog.json
```

Or

```
storage:
  dbPath: /data/db
auditLog:
  destination: file
  format: JSON
  path: /data/db/auditLog.json
```

Writing the audit information to bson

```
$ mongod --dbpath /data/db --auditDestination file --auditFormat BSON --auditPath data/db/auditLog.bson
```

Or update in the configuration file

```
storage:
  dbPath: /data/db
auditLog:
  destination: file
  format: BSON
  path: /data/db/auditLog.bson
```

Auditing CURD Operations

```
$ mongod --port 27018 --dbpath /u01/data --auth --setParameter auditAuthorizationSuccess=true --auditDestination file --auditFilter '{ atype: "authCheck", "param.command": { $in: [ "find", "insert", "delete", "update", "findandmodify" ] } }' --auditFormat JSON --auditPath /u01/data/auditLog.json
```

Or update in the configuration file

```
storage:
dbPath: data/db
security:
authorization: enabled
auditLog:
destination: file
format: BSON
path: data/db/auditLog.bson
filter: '{ atype: "authCheck", "param.ns": "test.orders", "param.command": { $in: [ "find", "insert", "delete", "update", "findandmodify" ] } }'
```