# MongoDB Security

# which mongo

/usr/bin/mongo

# netstat -ntlp | grep mongod

tcp 0 0 127.0.0.1:27017 0.0.0.0:\* LISTEN 831/mongod

### Encrypt Communication (TLS/SSL)

Windows - Secure Channel (Schannel)

Linux/BSD - OpenSSL

macOS - Secure Transport

etc/mongod.conf

#SSL configuration

# network interfaces

net:

port: 27017

bindIp: 127.0.0.1

ssl:

mode:requireSSL

PEMKeyFile: /etc/ssl/mongodb.pem <route of the signed SSL certificate .pem>

CAFile: /etc/ssl/caToValidateClientCertificates.pem <route of the certificate chain>

CRLFile: /etc/ssl/revokedCertificates.pem <route of the revoked certificates>

# allowConnectionsWithoutCertificates: true <bypass client certificate validation>

#disabledProtocols: TLS1\_0,TLS1\_1 <prevents incoming connections eitherTLS1 & TLS1\_1>

#TLS configuration

# network interfaces

net:

port: 27017

bindIp: 127.0.0.1

tls:

more: requireTLS

certificateKeyFile: /etc/ssl/mongodb.pem <route of file that contains the TLS certificate>

CAFile: /etc/ssl/caToValidateClientCertificates.pem <route of the certificate chain>

CRLFile: /etc/ssl/revokedCertificates.pem <route of the revoked certificates>

#allowConnectionsWithoutCertificates: true <bypass client certificate validation>

#disabledProtocols: TLS1\_0,TLS1\_1 <prevents incoming connections eitherTLS1 & TLS1\_1>

### Enable Access Control

# service mongod status

● mongod.service - MongoDB Database Server

Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)

Active: active (running) since Tue 2021-01-19 10:50:15 +03; 2h 45min ago

Docs: https://docs.mongodb.org/manual

Main PID: 831 (mongod)

CGroup: /system.slice/mongod.service

└─831 /usr/bin/mongod --config /etc/mongod.conf

Oca 19 10:50:15 sss-VirtualBox systemd[1]: Started MongoDB Database Server.

# mongod --port 27017

# mongod --port 27017

2021-01-19T15:16:51.129+0300 I CONTROL [main] Automatically disabling TLS 1.0, to force-enable TLS 1.0 specify --sslDisabledProtocols 'none'

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] MongoDB starting : pid=24389 port=27017 dbpath=/data/db 64-bit host=sss-VirtualBox

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] db version v4.0.22

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] git version: 1741806fb46c161a1d42870f6e98f5100d196315

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] OpenSSL version: OpenSSL 1.1.1 11 Sep 2018

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] allocator: tcmalloc

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] modules: none

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] build environment:

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] distmod: ubuntu1804

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] distarch: x86\_64

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] target\_arch: x86\_64

2021-01-19T15:16:51.145+0300 I CONTROL [initandlisten] options: { net: { port: 27017 } }

rs01:PRIMARY> show dbs

admin 0.078GB

config 0.078GB

local 2.077GB

rocketchat 0.078GB

rs01:PRIMARY> use rocketchat

switched to db rocketchat

rs01:PRIMARY> db.createUser(

... {

... user: "myAdmin",

... pwd: "test123",

... roles: [ { role: "userAdminAnyDatabase", db: "admin" } ]

... }

... )

Successfully added user: {

"user" : "myAdmin",

"roles" : [

{

"role" : "userAdminAnyDatabase",

"db" : "admin"

}

]

}

# mongo --port 27017

rs01:PRIMARY> use rocketchat

switched to db rocketchat

rs01:PRIMARY> db.auth("myAdmin", "test123")

1

rs01:PRIMARY>

# mongo -u "myAdmin" --authenticationDatabase "rocketchat" -p

MongoDB shell version v4.0.22

Enter password: \*\*\*\*

connecting to: mongodb://127.0.0.1:27017/?authSource=rocketchat&gssapiServiceName=mongodb

rs01:PRIMARY> db.foo.insert( { x: 1, y: 1 } )

WriteResult({ "nInserted" : 1 })

rs01:PRIMARY>

rs01:PRIMARY> db.foo.find()

{ "\_id" : ObjectId("6006d3bf19b80956979c52a0"), "x" : 1, "y" : 1 }

rs01:PRIMARY>

<[security.authorization](https://docs.mongodb.com/manual/reference/configuration-options/" \l "security.authorization)>

/etc/mongod.conf

security:

authorization: enabled

### Enable Auditing

dbPath: /var/lib/mongodb

/etc/mongod.conf

# where to write logging data.

systemLog:

destination: file

logAppend: true

path: /var/log/mongodb/mongod.log

storage:

dbPath: /var/lib/mongodb

auditLog:

destination: <syslog>, <console>

storage:

dbPath: /var/lib/mongodb

auditLog:

destination: file

format: JSON

path: data/db/auditLog.json

storage:

dbPath: /var/lib/mongodb

auditLog:

destination: file

format: BSON

path: data/db/auditLog.bson

### Manage Users and Roles

rs01:PRIMARY> use rocketchat

switched to db rocketchat

rs01:PRIMARY> db.runCommand({connectionStatus : 1})

{

"authInfo" : {

"authenticatedUsers" : [

{

"user" : "myAdmin",

"db" : "rocketchat"

}

],

"authenticatedUserRoles" : [

{

"role" : "userAdminAnyDatabase",

"db" : "admin"

}

]

},

"ok" : 1,

"operationTime" : Timestamp(1611062301, 4),

"$clusterTime" : {

"clusterTime" : Timestamp(1611062301, 4),

"signature" : {

"hash" : BinData(0,"AAAAAAAAAAAAAAAAAAAAAAAAAAA="),

"keyId" : NumberLong(0)

}

}

}

rs01:PRIMARY> show users

{

"\_id" : "rocketchat.myAdmin",

"userId" : UUID("73fd7588-0442-46da-a004-a95f9b953e95"),

"user" : "myAdmin",

"db" : "rocketchat",

"roles" : [

{

"role" : "userAdminAnyDatabase",

"db" : "admin"

}

],

"mechanisms" : [

"SCRAM-SHA-1",

"SCRAM-SHA-256"

]

}

{

"\_id" : "rocketchat.testUser",

"userId" : UUID("88a9398d-fc40-4ae9-988d-21fa4f2c72ad"),

"user" : "testUser",

"db" : "rocketchat",

"roles" : [

{

"role" : "read",

"db" : "test"

},

{

"role" : "readWrite",

"db" : "rocketchat"

}

],

"mechanisms" : [

"SCRAM-SHA-1",

"SCRAM-SHA-256"

]

}

rs01:PRIMARY>

rs01:PRIMARY> db.changeUserPassword("testUser", "test?")

rs01:PRIMARY> db.getRole( "read", { showPrivileges: true } )

{

"role" : "read",

"db" : "rocketchat",

"isBuiltin" : true,

"roles" : [ ],

"inheritedRoles" : [ ],

"privileges" : [

{

"resource" : {

"db" : "rocketchat",

"collection" : ""

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.indexes"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.js"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.namespaces"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

}

],

"inheritedPrivileges" : [

{

"resource" : {

"db" : "rocketchat",

"collection" : ""

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.indexes"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.js"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

},

{

"resource" : {

"db" : "rocketchat",

"collection" : "system.namespaces"

},

"actions" : [

"changeStream",

"collStats",

"dbHash",

"dbStats",

"find",

"killCursors",

"listCollections",

"listIndexes",

"planCacheRead"

]

}

]

}