**Securing MongoDB server (as a service)**

1/ Uninstall the existing version of MongoDB--

2/ Start a DOS command window as an administrator

Microsoft Windows [Version 10.0.14393]

(c) 2016 Microsoft Corporation. All rights reserved.

3/ Create these directories under c:\

--

C:\WINDOWS\system32>mkdir c:\data\db

C:\WINDOWS\system32>mkdir c:\data\log

4/ Install mongodb to C:\mongodb and not the default path

--

5/ Add c:\mongodb\bin to the windows path

--

6/ Use NotePad++ in admin mode and create a config file called, C:\mongod.cfg containing the following lines. Do not use Tabs, only line breaks and spaces. YML does not like tabs.

systemLog:

destination: file

path: c:\data\log\mongod.log

storage:

dbPath: c:\data\db

security:

authorization: enabled

net:

bindIp: 127.0.0.1

port: 25514

7/ copy this file to c:\mongodb\mongod.cfg

C:\WINDOWS\system32>copy c:\mongod.cfg C:\MongoDB\

1 file(s) copied.

10/ Start mongodb from command line

--

C:\WINDOWS\system32>mongod --port=25514

2017-03-02T21:57:59.386-0600 I CONTROL [initandlisten] MongoDB starting : pid=5

376 port=25514 dbpath=C:\data\db\ 64-bit host=HP-Saeed

2017-03-02T21:57:59.386-0600 I CONTROL [initandlisten] targetMinOS: Windows 7/W

indows Server 2008 R2

2017-03-02T21:57:59.387-0600 I CONTROL [initandlisten] db version v3.2.8

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] git version: ed70e33130c

977bda0024c125b56d159573dbaf0

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] OpenSSL version: OpenSSL

1.0.1p-fips 9 Jul 2015

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] allocator: tcmalloc

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] modules: none

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] build environment:

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] distmod: 2008plus-ss

l

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] distarch: x86\_64

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] target\_arch: x86\_64

2017-03-02T21:57:59.388-0600 I CONTROL [initandlisten] options: {}

2017-03-02T21:57:59.388-0600 I - [initandlisten] Detected data files in C

:\data\db\ created by the 'wiredTiger' storage engine, so setting the active sto

rage engine to 'wiredTiger'.

2017-03-02T21:57:59.389-0600 I STORAGE [initandlisten] wiredtiger\_open config:

create,cache\_size=8G,session\_max=20000,eviction=(threads\_max=4),config\_base=fals

e,statistics=(fast),log=(enabled=true,archive=true,path=journal,compressor=snapp

y),file\_manager=(close\_idle\_time=100000),checkpoint=(wait=60,log\_size=2GB),stati

stics\_log=(wait=0),

2017-03-02T21:57:59.560-0600 I NETWORK [HostnameCanonicalizationWorker] Startin

g hostname canonicalization worker

2017-03-02T21:57:59.560-0600 I FTDC [initandlisten] Initializing full-time d

iagnostic data capture with directory 'C:/data/db/diagnostic.data'

2017-03-02T21:57:59.991-0600 I NETWORK [initandlisten] waiting for connections

on port 25514

11/ Leave this window alone and start a new DOS command window and start the mongo client. Once mongo client starts type the commands indicated in the Mongo shell. These are indicated by >

--

C:\Users\Saeed>mongo 127.0.0.1:25514/admin

MongoDB shell version: 3.2.8

connecting to: 127.0.0.1:25514/admin

> use admin

switched to db admin

>

-- run the following command by copying these lines to the mongo client shell

> db.createUser (

{

user: "mongoadmin",

pwd: "StrongPassWord$12",

roles:

[

{

role: "userAdminAnyDatabase",

db: "admin"

}

]

}

)

-- This is mongo response. If you do not get this response, you have done something wrong.

Successfully added user: {

"user" : "mongoadmin",

"roles" : [

{

"role" : "userAdminAnyDatabase",

"db" : "admin"

}

]

}

>

12/ Now exit from the client shell by typing in

> exit

13/ on the mongod command window, press CTRL-C to stop the mongod server

--

8/ Configure mongodb as a windows service

--

C:\ C:\MongoDB\bin\mongod.exe --config c:\mongodb\mongod.cfg --install

9/ Start the service

--

C:\WINDOWS\system32>net start mongodb

The MongoDB service was started successfully.

--

16/ Now connect to the server again

--

C:\WINDOWS\system32>mongo 127.0.0.1:25514/admin

MongoDB shell version: 3.2.8

connecting to: 127.0.0.1:25514/admin

17/ Run the following command inside the shell.

> db

admin

> show databases

2017-03-02T22:12:04.873-0600 E QUERY [thread1] Error: listCollections failed:

{

"ok" : 0,

"errmsg" : "not authorized on admin to execute command { listCollections: 1.0, filter: {} }",

"code" : 13

} :

\_getErrorWithCode@src/mongo/shell/utils.js:25:13

DB.prototype.\_getCollectionInfosCommand@src/mongo/shell/db.js:773:1

DB.prototype.getCollectionInfos@src/mongo/shell/db.js:785:19

DB.prototype.getCollectionNames@src/mongo/shell/db.js:796:16

shellHelper.show@src/mongo/shell/utils.js:754:9

shellHelper@src/mongo/shell/utils.js:651:15

@(shellhelp2):1:1

-- As you can see if you try to get data out of the system it gives

-- you an error since you have not logged in with a username and password.

--

However using the following to connect, you will be able view the databases:

C:\Users\Saeed>mongo 127.0.0.1:25514/admin --username mongoadmin --password SEIS737$0Spr17

MongoDB shell version: 3.2.8

connecting to: 127.0.0.1:25514/admin

> show databases

admin 0.000GB

local 0.000GB

>

18/ Creating a New Database

Now that you finally have your MongoDB service up and running, the next step is to create a new database called seis737, add an admin user and a unique user.

> use seis737

switched to db seis737

> db.createUser(

{

user: "mongoadmin",

pwd: "StrongPassWord$12",

roles:

[

{

role: "dbOwner",

db: "seis737"

}

]

}

)

Successfully added user: {

"user" : "mongoadmin",

"roles" : [

{

"role" : "dbOwner",

"db" : "seis737"

}

]

}

> db.createUser(

{

user: "seisuser",

pwd: "Abcd1234",

roles:

[

{

role: "dbOwner",

db: "seis737"

}

]

}

)

Successfully added user: {

"user" : "seisuser",

"roles" : [

{

"role" : "dbOwner",

"db" : "seis737"

}

]

}

19/ To test the created user, quit the current mongo shell

> exit

20/ Log back in using the new database user as follows:

C:\Users\Saeed>mongo --username seisuser --password Abcd1234 seis737

MongoDB shell version: 3.2.8

connecting to: seis737

21/ in the mongo shell run the following steps:

> db.test.insert({"name":"test value"})

WriteResult({ "nInserted" : 1 })

> db.test.find()

{ "\_id" : ObjectId("58b8f2daccd7c66ca907387e"), "name" : "test value" }

> show collections

test

>

22/ The db is ready to be used and it is secured. Close the client shell

> exit

C:\WINDOWS\system32>

23/ You can leave the server running, but for now, we will stop it

C:\WINDOWS\system32> net stop mongodb

The MongoDB service is stopping.

The MongoDB service was stopped successfully.

Extras:

-- To get help you can run the following from command line

--

C:\WINDOWS\system32>mongod.exe --help

Options:

General options:

-h [ --help ] show this usage information

--version show version information

-f [ --config ] arg configuration file specifying

additional options

-v [ --verbose ] [=arg(=v)] be more verbose (include multiple times

for more verbosity e.g. -vvvvv)

--quiet quieter output

--port arg specify port number - 25514 by default

--bind\_ip arg comma separated list of ip addresses to

listen on - all local ips by default

--ipv6 enable IPv6 support (disabled by

default)

--maxConns arg max number of simultaneous connections

- 1000000 by default

--logpath arg log file to send write to instead of

stdout - has to be a file, not

directory

--logappend append to logpath instead of

over-writing

--logRotate arg set the log rotation behavior

(rename|reopen)

--timeStampFormat arg Desired format for timestamps in log

messages. One of ctime, iso8601-utc or

iso8601-local

--pidfilepath arg full path to pidfile (if not set, no

pidfile is created)

--keyFile arg private key for cluster authentication

--noauth run without security

--setParameter arg Set a configurable parameter

--httpinterface enable http interface

--clusterAuthMode arg Authentication mode used for cluster

authentication. Alternatives are

(keyFile|sendKeyFile|sendX509|x509)

--auth run with security

--jsonp allow JSONP access via http (has

security implications)

--rest turn on simple rest api

--slowms arg (=100) value of slow for profile and console

log

--profile arg 0=off 1=slow, 2=all

--cpu periodically show cpu and iowait

utilization

--sysinfo print some diagnostic system

information

--noIndexBuildRetry don't retry any index builds that were

interrupted by shutdown

--noscripting disable scripting engine

--notablescan do not allow table scans

Windows Service Control Manager options:

--install install Windows service

--remove remove Windows service

--reinstall reinstall Windows service (equivalent

to --remove followed by --install)

--serviceName arg Windows service name

--serviceDisplayName arg Windows service display name

--serviceDescription arg Windows service description

--serviceUser arg account for service execution

--servicePassword arg password used to authenticate

serviceUser

Replication options:

--oplogSize arg size to use (in MB) for replication op

log. default is 5% of disk space (i.e.

large is good)

Master/slave options (old; use replica sets instead):

--master master mode

--slave slave mode

--source arg when slave: specify master as

<server:port>

--only arg when slave: specify a single database

to replicate

--slavedelay arg specify delay (in seconds) to be used

when applying master ops to slave

--autoresync automatically resync if slave data is

stale

Replica set options:

--replSet arg arg is <setname>[/<optionalseedhostlist

>]

--replIndexPrefetch arg specify index prefetching behavior (if

secondary) [none|\_id\_only|all]

--enableMajorityReadConcern enables majority readConcern

Sharding options:

--configsvr declare this is a config db of a

cluster; default port 27019; default

dir /data/configdb

--configsvrMode arg Controls what config server protocol is

in use. When set to "sccc" keeps server

in legacy SyncClusterConnection mode

even when the service is running as a

replSet

--shardsvr declare this is a shard db of a

cluster; default port 27018

SSL options:

--sslOnNormalPorts use ssl on configured ports

--sslMode arg set the SSL operation mode

(disabled|allowSSL|preferSSL|requireSSL

)

--sslPEMKeyFile arg PEM file for ssl

--sslPEMKeyPassword arg PEM file password

--sslClusterFile arg Key file for internal SSL

authentication

--sslClusterPassword arg Internal authentication key file

password

--sslCAFile arg Certificate Authority file for SSL

--sslCRLFile arg Certificate Revocation List file for

SSL

--sslDisabledProtocols arg Comma separated list of TLS protocols

to disable [TLS1\_0,TLS1\_1,TLS1\_2]

--sslWeakCertificateValidation allow client to connect without

presenting a certificate

--sslAllowConnectionsWithoutCertificates

allow client to connect without

presenting a certificate

--sslAllowInvalidHostnames Allow server certificates to provide

non-matching hostnames

--sslAllowInvalidCertificates allow connections to servers with

invalid certificates

--sslFIPSMode activate FIPS 140-2 mode at startup

Storage options:

--storageEngine arg what storage engine to use - defaults

to wiredTiger if no data files present

--dbpath arg directory for datafiles - defaults to

\data\db\ which is C:\data\db\ based on

the current working drive

--directoryperdb each database will be stored in a

separate directory

--noprealloc disable data file preallocation - will

often hurt performance

--nssize arg (=16) .ns file size (in MB) for new databases

--quota limits each database to a certain

number of files (8 default)

--quotaFiles arg number of files allowed per db, implies

--quota

--smallfiles use a smaller default file size

--syncdelay arg (=60) seconds between disk syncs (0=never,

but not recommended)

--upgrade upgrade db if needed

--repair run repair on all dbs

--repairpath arg root directory for repair files -

defaults to dbpath

--journal enable journaling

--nojournal disable journaling (journaling is on by

default for 64 bit)

--journalOptions arg journal diagnostic options

--journalCommitInterval arg how often to group/batch commit (ms)

WiredTiger options:

--wiredTigerCacheSizeGB arg maximum amount of memory to allocate

for cache; defaults to 1/2 of physical

RAM

--wiredTigerStatisticsLogDelaySecs arg (=0)

seconds to wait between each write to a

statistics file in the dbpath; 0 means

do not log statistics

--wiredTigerJournalCompressor arg (=snappy)

use a compressor for log records

[none|snappy|zlib]

--wiredTigerDirectoryForIndexes Put indexes and data in different

directories

--wiredTigerCollectionBlockCompressor arg (=snappy)

block compression algorithm for

collection data [none|snappy|zlib]

--wiredTigerIndexPrefixCompression arg (=1)

use prefix compression on row-store

leaf pages