Course Overview

View Discussion

Chapter 1: Authentication

Homework 1.6: Enabling LDAP Authentication on a Replica Set

‹ Back to the Question

Here are the commands needed to successfully enable LDAP authentication on a replica set referencing the steps outlined in the instructions. These commands will be ran on the **database** VM unless otherwise specified.

- Configure `saslauthd` to automatically start and use LDAP as its mechanism.

  Edit `/etc/default/saslauthd` such that it looks like this.

  ```
  START=yes
  DESC="SASL Authentication Daemon"
  NAME="saslauthd"
  MECHANISMS="ldap"
  MECH_OPTIONS=""
  THREADS=5
  OPTIONS="-m /var/run/saslauthd"
  ```

- Configure `saslauthd` to talk to the LDAP server. The information below will be very useful.

  Create `/etc/saslauthd.conf` such that it looks like this.

  ```
  ldap_servers:
  ldap://infrastructure.m310.mongodb.university:389
  ldap_search_base: ou=Users,dc=mongodb,dc=com
  ldap_filter: (cn=%u)
  ```

- Start the `saslauthd` service.

  ```
  $ sudo service saslauthd start
  ```

- Fix the permissions on the `saslauthd` socket directory.

  ```
  $ sudo chmod 755 /var/run/saslauthd
  ```

- Start three mongods on ports 31160, 31161, and 31162 with LDAP support enabled.

```
$ mkdir -p ~/M310-HW-1.6/{r0,r1,r2}
$ cd ~/M310-HW-1.6

$ openssl rand -base64 755 > shared_key
$ chmod 400 shared_key

$ mongod --dbpath r0 --logpath r0/mongodb.log --port 31160 \
         --replSet LDAP --auth --setParameter
authenticationMechanisms=PLAIN \
         --setParameter
saslauthdPath="/var/run/saslauthd/mux" \
         --keyFile shared_key --fork

$ mongod --dbpath r1 --logpath r1/mongodb.log --port 31161 \
         --replSet LDAP --auth --setParameter
authenticationMechanisms=PLAIN \
         --setParameter
saslauthdPath="/var/run/saslauthd/mux" \
         --keyFile shared_key --fork

$ mongod --dbpath r2 --logpath r2/mongodb.log --port 31162 \
         --replSet LDAP --auth --setParameter
authenticationMechanisms=PLAIN \
         --setParameter
saslauthdPath="/var/run/saslauthd/mux" \
         --keyFile shared_key --fork
```

- Connect to the primary and initiate the replica set.

```
$ mongo --port 31160
rs.initiate()
```

- Create an account for **adam**.

```
db.getSiblingDB("$external").createUser({
  user: 'adam',
  roles: [
    {role: "userAdminAnyDatabase", db: "admin"},
    {role: "dbAdminAnyDatabase", db: "admin"},
    {role: "clusterAdmin", db: "admin"}
  ]
})
```

- Verify that you can authenticate to MongoDB with the username **adam** and his LDAP password of **password**.

```
db.getSiblingDB("$external").auth({
  mechanism: "PLAIN",
  user: 'adam',
  pwd: 'password',
  digestPassword: false
})
```

- Add the other members of the replica set.

COPY

```
rs.add('database.m310.mongodb.university:31161');
rs.add('database.m310.mongodb.university:31162');
```

- Connect to the **infrastructure** VM and change Adam's password to "**webscale**" by issuing the following command.

COPY

```
$ vagrant ssh infrastructure
$ cd ~/shared
$ python ldapconfig.py passwd -u adam -op password -np
webscale
```

- Reconnect to the **database** VM and verify that adam's new password works.

COPY

```
$ vagrant ssh database
$ mongo --port 31160

db.getSiblingDB("$external").auth({
  mechanism: "PLAIN",
  user: 'adam',
  pwd: 'webscale',
  digestPassword: false
})
```

Proceed to next section