Chapter 1: Authentication

Homework 1.6: Enabling LDAP Authentication on a Replica Set

Problem:

In this lab, you will create a replica set that uses LDAP for authentication.

In the previous exercises for this course, you may have noticed that we have been specifying `database` as the hostname after the `vagrant ssh` command. This is because our Vagrantfile, which contains instructions to vagrant on how to set up the VMs, contains instructions for a second VM with the hostname of `infrastructure`.

For this assignment, you will need to use the two VMs which will communicate over your computer's local network.

Your MongoDB replica set cluster will be on the `database` VM and the OpenLDAP server will be on the `infrastructure` VM.

Note: These are not real Internet public hostnames. The hostname resolution for each is specified in the `/etc/hosts files` on each of the VMs.

In order to start the OpenLDAP on the *infrastructure* VM, run the following commands.

COPY

```
$ cd m310-vagrant-env
$ vagrant up
$ vagrant ssh infrastructure
```

Part of your provided scripts in the handout setup OpenLDAP and add a user named **adam** with the password **password**. After you've copied the handout's files to the shared folder your file structure should look like:

COPY

```
~
`-- shared
    |-- ldap
    |   |-- Domain.ldif
```

```
|   |-- pw.ldif
|   `-- Users.ldif
|-- ldapconfig.py
|-- setup-hw-1.6.sh
`-- validate-hw-1.6.sh
```

On `infrastructure` go ahead and configure OpenLDAP by running:

```
$ cd ~/shared
$ ./setup-hw-1.6.sh
```

After you've got OpenLDAP up and running your ready to do your part! In order to enable LDAP authentication on this running replica set you're going to need to figure out how to perform the following tasks.

- Configure `saslauthd` to automatically start and use LDAP as its mechanism.
- Configure `saslauthd` to talk to the LDAP server. The information below will be very useful.

  ```
  LDAP Server IP: infrastructure.m310.mongodb.university
  LDAP Search Base: ou=Users,dc=mongodb,dc=com
  LDAP Search Filter: (cn=%u)
  ```

- Start the `saslauthd` service.
- Fix the permissions on the `saslauthd` socket directory.
- Start three `mongod` instances on ports **31160**, **31161**, and **31162** with LDAP support enabled.
- Connect to the primary and initiate the replica set.
- Create an account for **adam**.
- Verify that you can authenticate to MongoDB with the username **adam** and his LDAP password of **password**.
- Add the other members of the replica set.
- Connect to the LDAP VM and change Adam's password to "**webscale**" by issuing the following command.

  ```
  $ python ldapconfig.py passwd -u adam -op password -np
  ```

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

Note: It's probably a good idea to test that your Ubuntu VM can talk to your LDAP server with `testsaslauthd` before you create your replica set. It's also important to point out that `saslauthd` caches credentials. When you change the password on infrastructure you might need to restart the `saslauthd` service in order to use the new password.

After you've enabled LDAP authentication on your replica set you can run the following script and copy the output into the submission area below.

COPY

```
$ cd ~/shared
$ ./validate-hw-1.6.sh
```

Note: If you've successfully enabled authentication on the replica set, then the validation script should output a JSON object with two keys: `unauthorizedStatus` and `memberStatuses`. The first key confirms that authentication is enabled, and the second verifies that all members are still up and running.

Attempts Remaining: Correct Answer

Enter answer here:

```
{ unauthorizedStatus: { "ok" : 0, "errmsg" : "not authorized on admin
to execute command { replSetGetStatus: 1.0 }", "code" : 13 },
memberStatuses: ["PRIMARY","SECONDARY","SECONDARY"] }
```

Correct!

See detailed answer

Proceed to next section

Assignment is Due

12d:02hr:39m
Dec 17, 17:00 UTC

Your Grade

PASS/FAIL
Submitted