Mysql with ssl

Do the steps identified at:


I started with 6.3.9.5 to generate my certs/keys and stuff, then I did section 6.3.9.3. Instead of starting the server with command line arguments I just uncommented the section in `/etc/mysql/my.cnf` like so:

```bash
ssl-ca=/etc/mysql/newcerts/ca-cert.pem
ssl-cert=/etc/mysql/newcerts/server-cert.pem
ssl-key=/etc/mysql/newcerts/server-key.pem
```

Before restarting mysql I added the following line to `/etc/apparmor.d/usr.sbin.mysqld`:

```bash
/etc/mysql/newcerts/*.pem r,
```

Before the closing curly brace.

Then you should be able to restart mysql. You will probably want to create a new user and make sure that you can connect remotely. From the mysql prompt:

```bash
grant all privileges on *.* to joe@'%' identified by 'foobar!';
```

Then back in `my.cnf` file, comment out the line that refers to bind-address, restart mysql again.

Now when you look at your server and issue the following command, you should see that it is using ssl:

```bash
show variables like 'have_ssl';
```

To connect from a client do:

```bash
mysql -u joe -p -h it4500-2.cs.dixie.edu -ssl-cert client-cert.pem -ssl-key client-key.pem
```

After copying over the client files that you created earlier. In a session from a client you can now do the `ls` and it should show it is using ssl.

```bash
Current user:       joe@yavin.cs.dixie.edu
SSL:               Cipher in use is DHE-RSA-AES256-SHA
Current pager:     stdout
```

If you try to login as a normal user, without all the ssl garbage, you can also do `ls` and see that SSL is not being used.

```bash
mysql -u joe -p -h it4500-2.cs.dixie.edu
```