Openfire/Spark Installation and Configuration

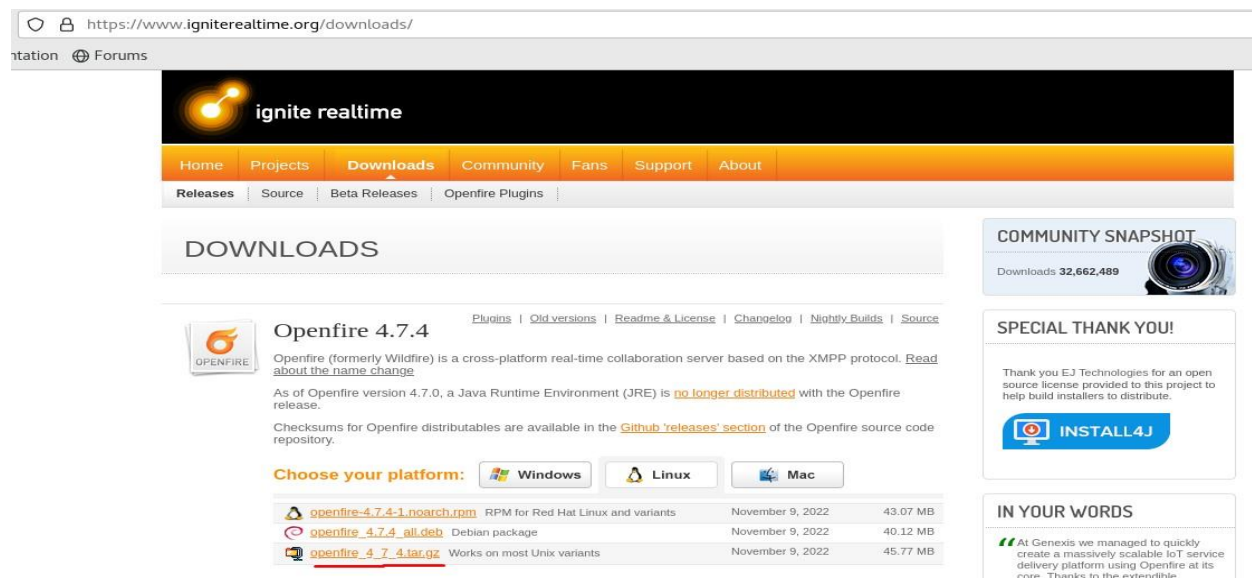1) What is Openfire & what spark ignite??

Openfire and Spark are two separate software applications developed by the same organization, Ignite Realtime, for real-time collaboration using the XMPP protocol.

Openfire is a server application that provides the backend infrastructure for real-time messaging and collaboration. It enables the creation of user accounts, groups, chat rooms, and other administrative functions. Openfire supports various authentication mechanisms and can integrate with other systems such as LDAP and Active Directory.

Spark, on the other hand, is a desktop client application that provides a user interface for messaging and collaboration. It is designed to work with Openfire and supports various features such as group chat, file transfer, and screen sharing. Spark is available for Windows, Linux, and macOS.

Together, Openfire and Spark provide a complete solution for real-time messaging and collaboration that can be used by organizations to build their own internal chat networks or by developers to create custom chat applications. The combination of Openfire and Spark is a popular choice among organizations that value open-source, extensibility, and security.

2)We can download both from https://www.igniterealtime.org/downloads/ .
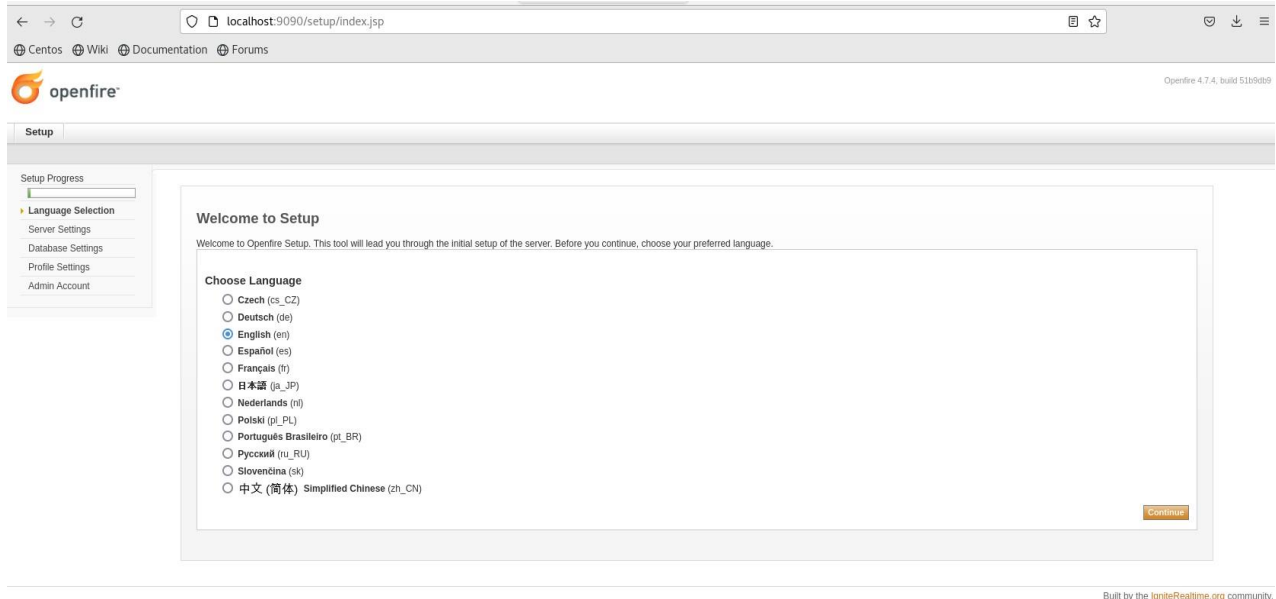

We install Openfire from RPM and or we can directly download ta.gz file and create custom installtion if we want to.

In Our case we do the custom installation from the downloaded tar.gz file we keep downloaded file on our /opt/soft folder and untar it.
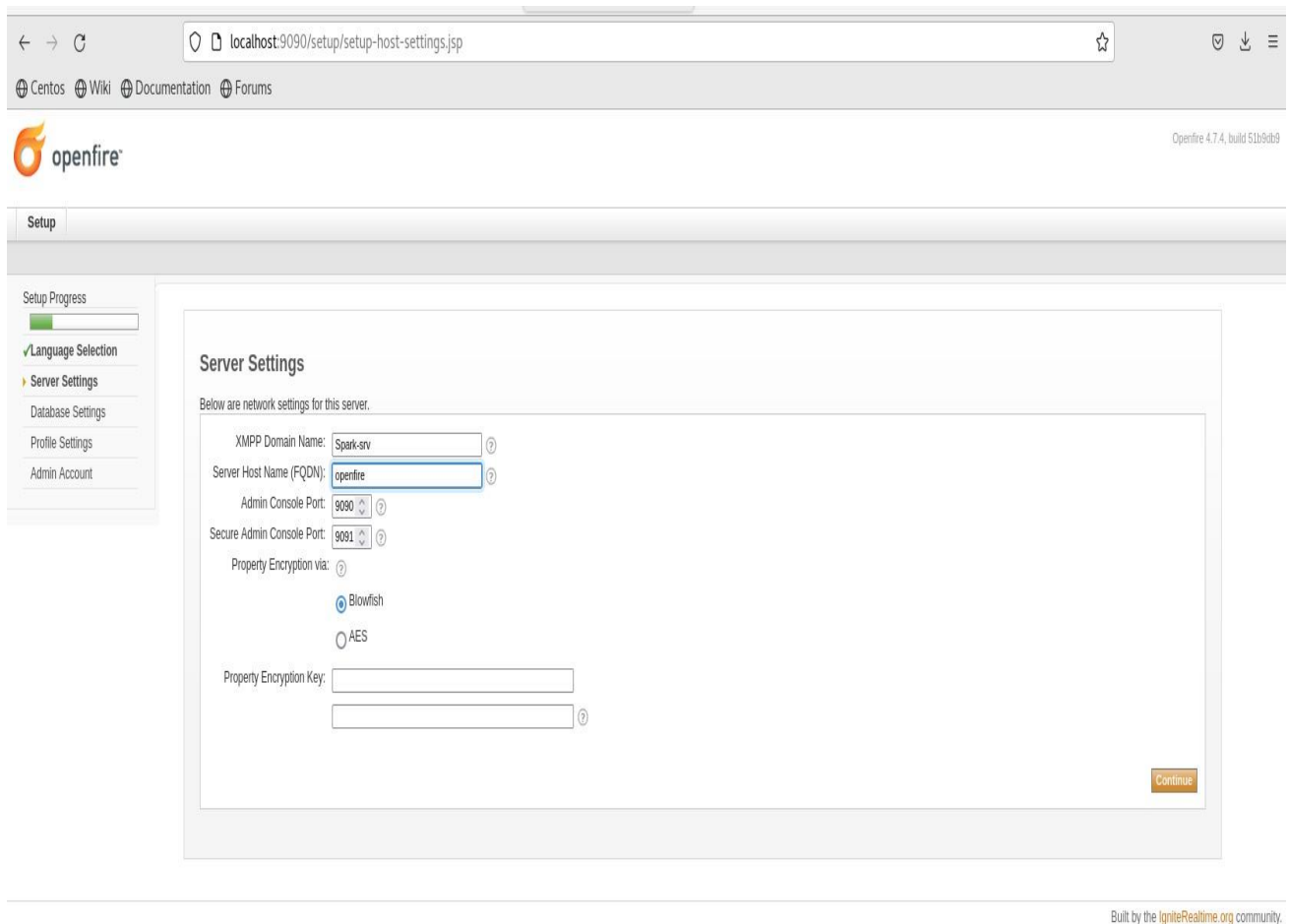
After keeping Openfire in a custom location, we start the application by going /opt/soft/openfire/bin and fire command "./openfire start" or We can shoot from the current terminal "/opt/soft/openfire/bin/openfire start" so application will run, or we can say start.

3) openfire will listen on 9090 on http for 1st time for installation.

Select language hit next.
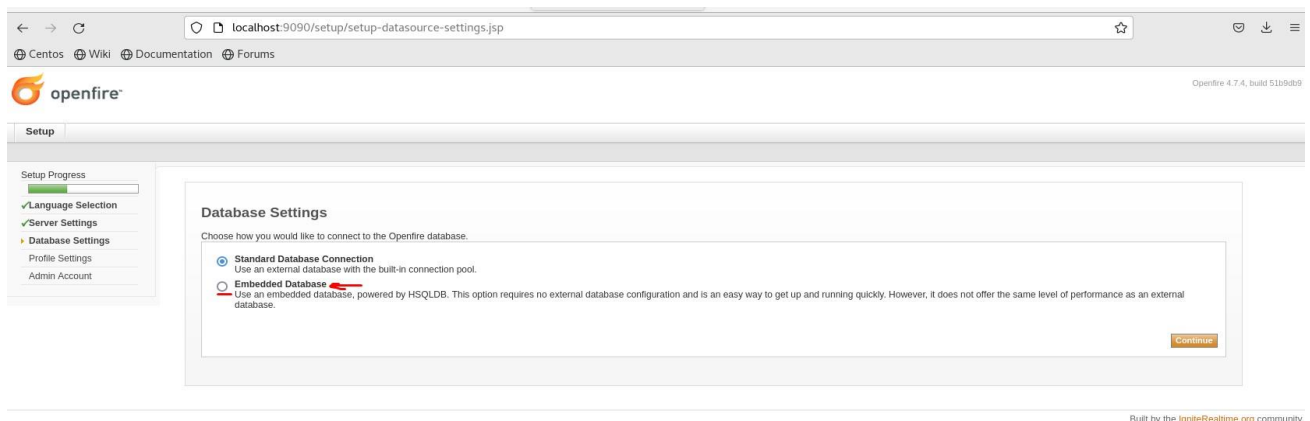
 We can setup server settings like Domain name and FQDN and hit next.

Admin port 9090 and secure admin port is 9091 on https.

Select database embedded one because we do not maintain database of openfire server.

In Our earlier and easy usage, we create a local environment so need to create and delete, update user from openfire server but now we use active directory feature so if user exists on AD then we can directly import user from the AD and maintain from AD only.

4) Domain Integration as shown as below

Same configuration should be done for active directory collaboration and AD's global administrator use authentication must be done to achieve proper success in auth.
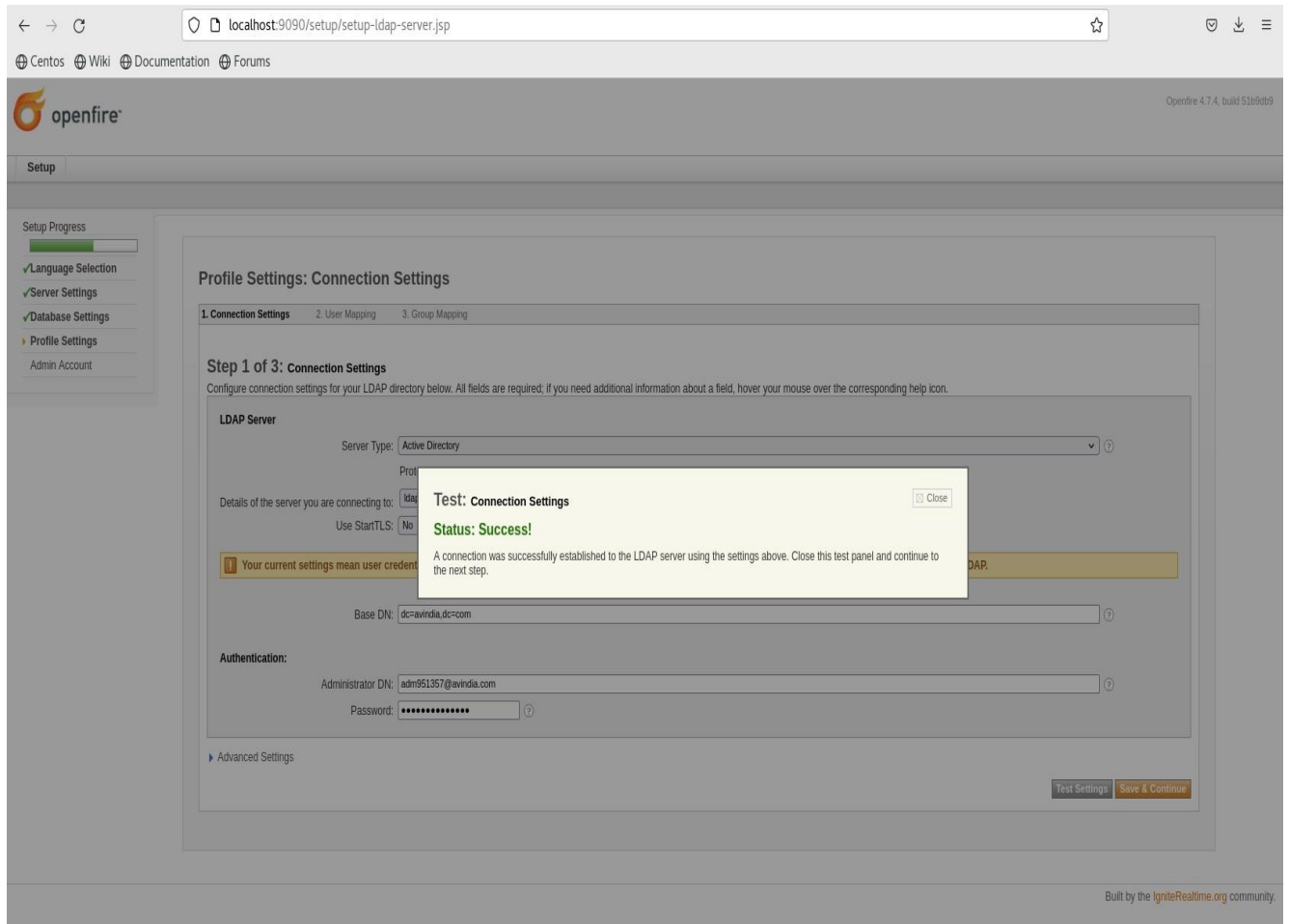
Test connection before preceding so we can achieve 100 % success in setting up server-side configuration.

5) Very important setup not to forget adding administrator of openfire server this activity done only when we configure openfire server so if want add administrator we can do after completion of openfire server.

So, add AD's server administrators at this step only so others can access openfire admin console.

6) So now setup is complete we can access openfire admin portal by http://localhost:9090 & https://localhost:9091 for secure authentication.

Now our openfire server backend is ready to use 1st thing here we can see all the details regarding server.

A few things we need to observe are that Java memory is by default allocated and we may increase if in case we face issue slowness or GC full.

We can do that by creating a file in /opt/soft/openfire/bin filename "openfire.vmoptions" contains

"-Xms8000m

-Xmx12000m

"

So, we specifically saying minimum 8 Gb to 12 GB Java memory should be used by openfire server.

Minium 6 GB utilized as we have seen in observation and minimum 6 CPU core for standard 400-500 user via Active directory and if user increase then we need to increase Java memory and CPU also.

If Java memory is utilized above 80% then we must restart openfire server by "/opt/soft/openfire/bin/openfire restart".

6) User administration is an important and easy task if we use AD integration.
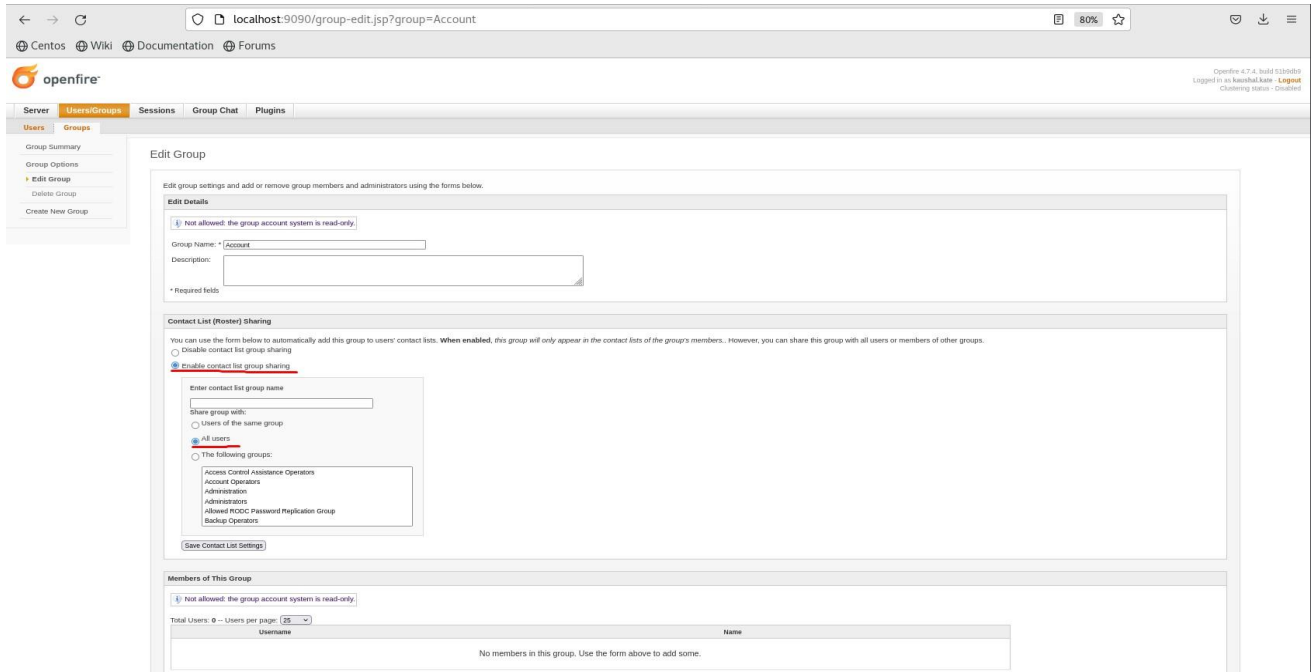
For Active directory integration we must go in groups active/enable all working security group from AD.

At AD side we must create a security group in the organization unit (OU) so openfire can fetch all users and groups.
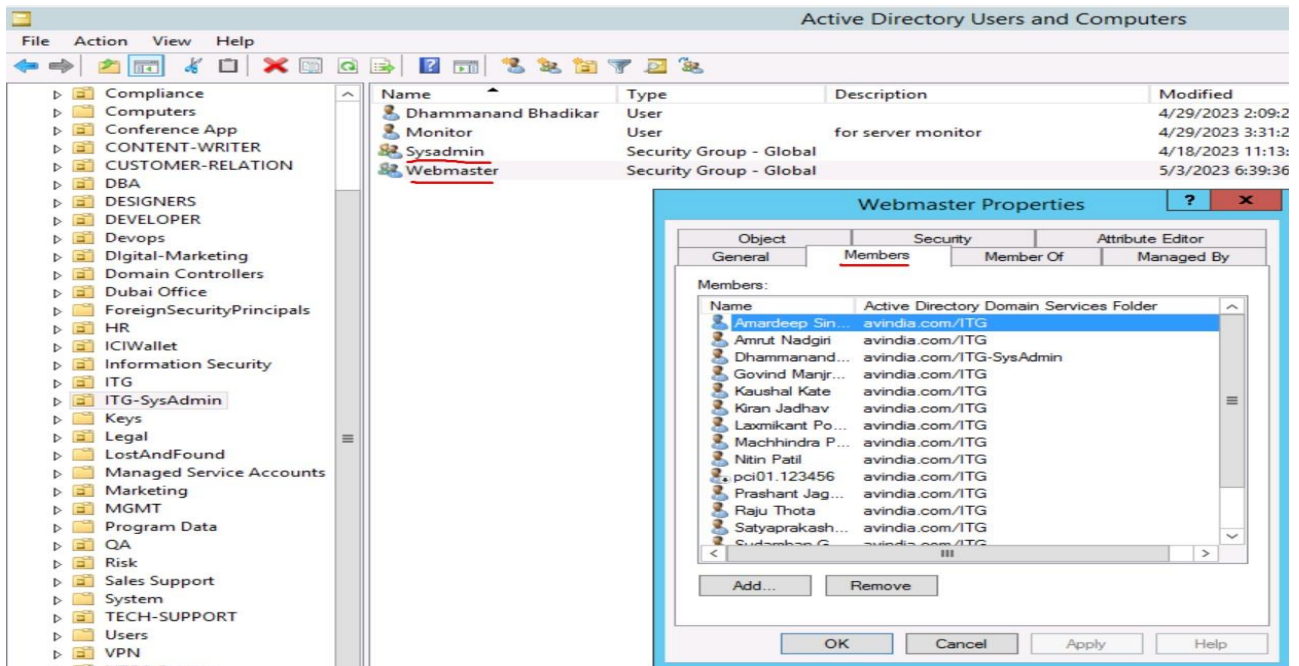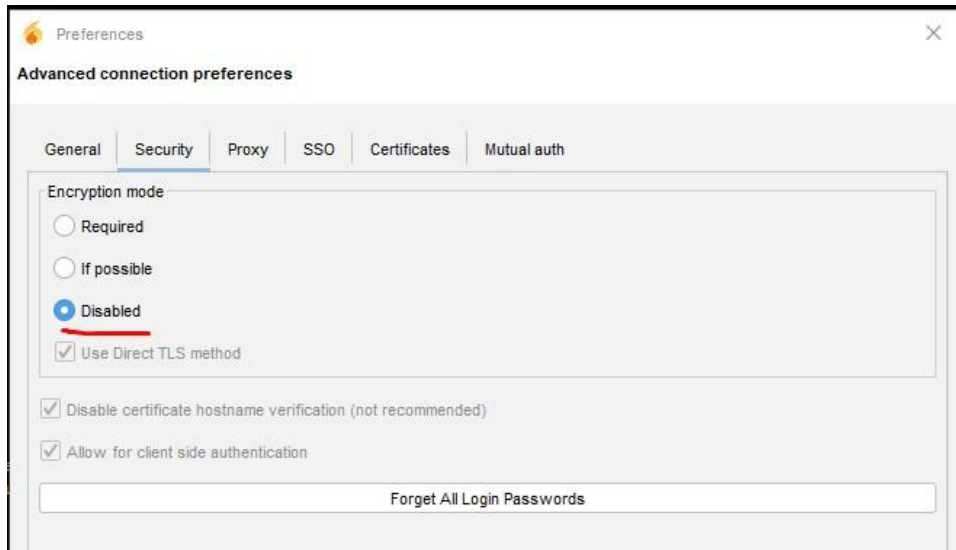
7) If we follow these above settings at openfire side, then backend is configured.

We must install spark client who can connect to openfire server. Spark clients can be windows, Linux, Mac.

Basic setting in Spark client is

Disabled TLS to connect openfire server in Spark client newer then 2.72.

Import Note:-

How to stop, start & restart Spark server??

In our case we have configured in root so take root access and fire below command

"/opt/soft/openfire/bin openfire start"

"/opt/soft/openfire/bin/openfire stop"

"/opt/soft/openfire/bin/openfire restart"

"/opt/soft/openfire/bin /openfire status"

Or we can go to path /opt/openfire/bin/ and "./openfire start "

"./openfire restart "

"./openfire stop "

"./openfire status "