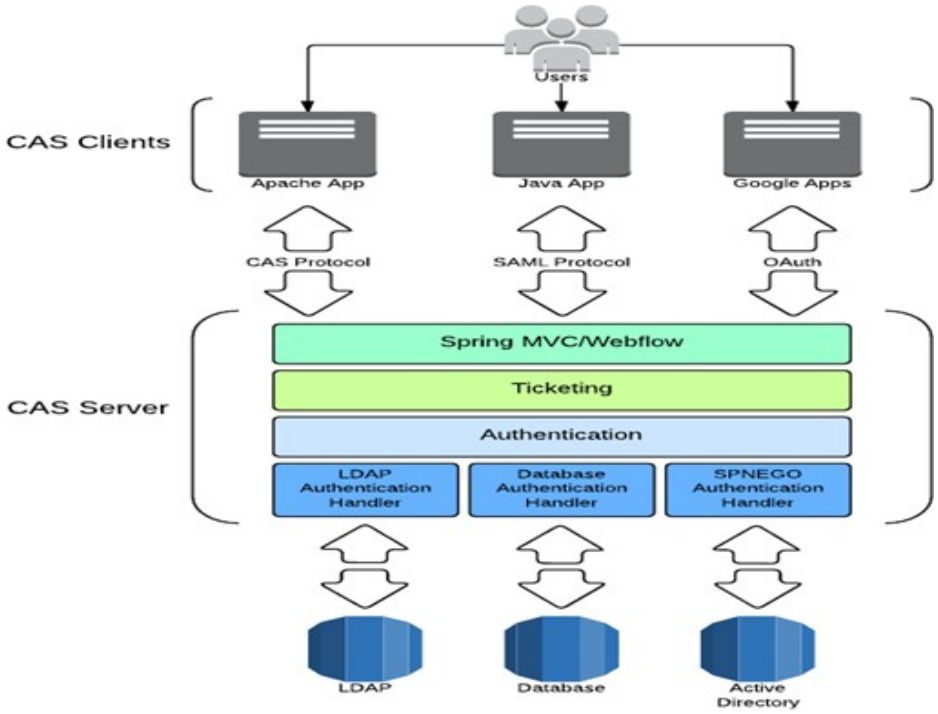
Here are three of the methods used and the difficulties encountered on CAS SSO: As well as its architecture:



To implement the sso single sign-on we need to proceed as follows:

- Install and configure a CAS server: Here

the only big problem is the lack of the

- One and configure CAS client:

As a CAS client I chose :

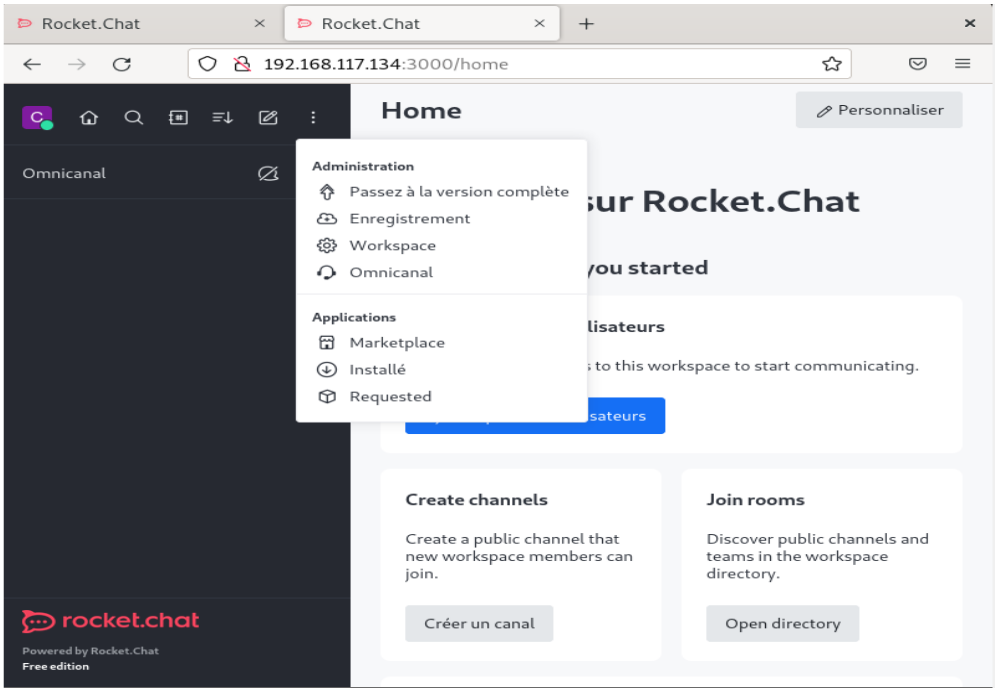
- java-cas-client :

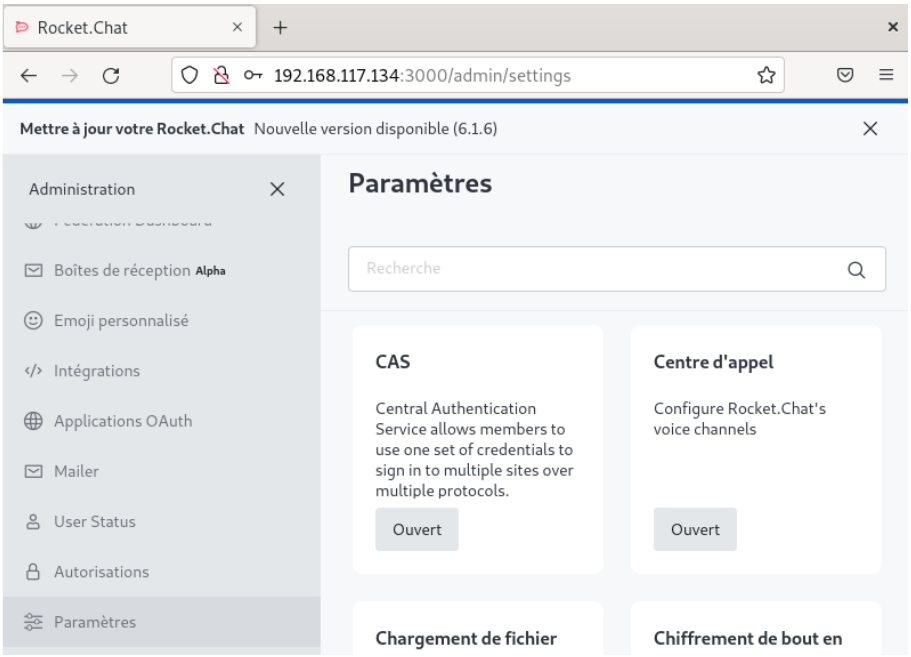
  I have installed it but I have not yet managed to configure the test web applications that CAS offers because of the non-working of some configurations.

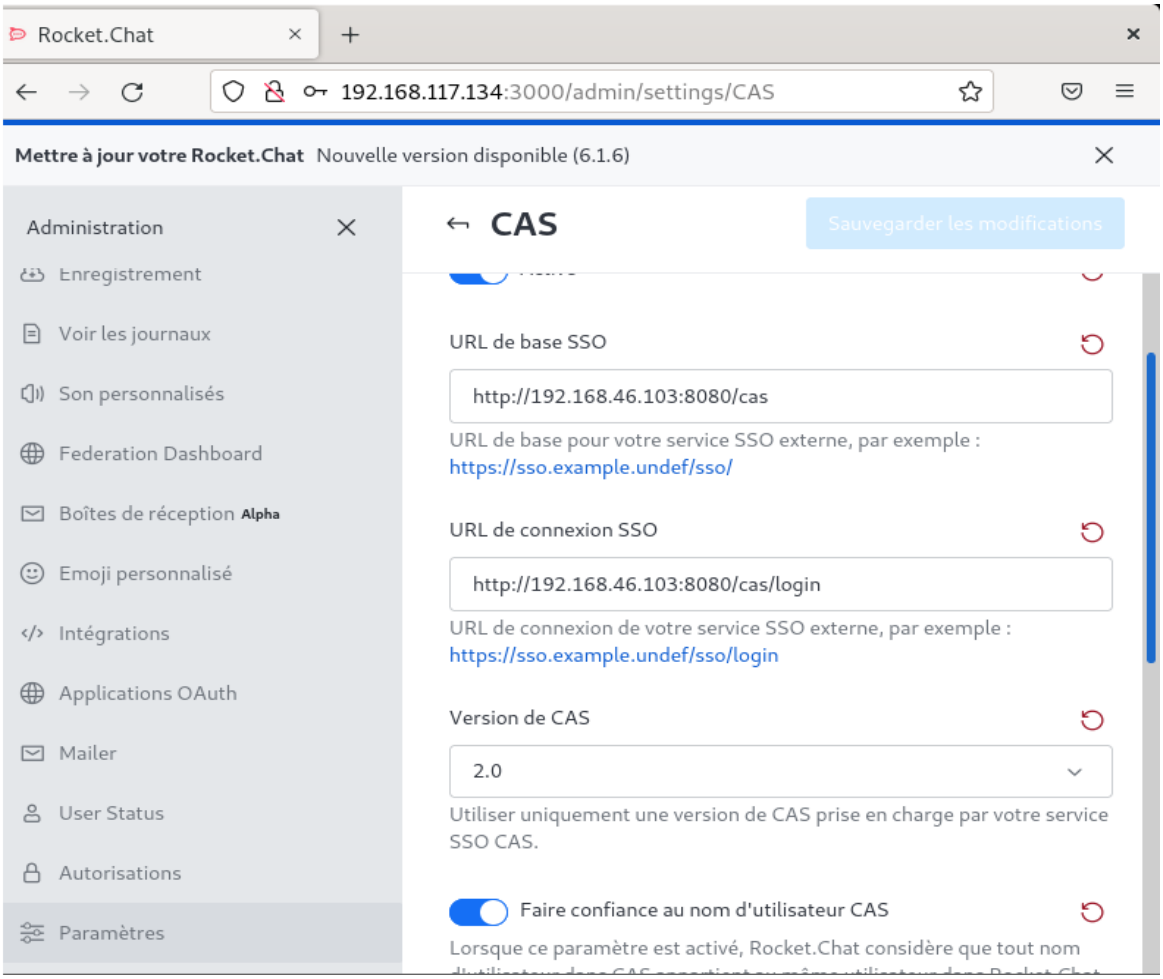
- Bootiful-cas-client : Same difficulties as CAS

- **Configure applications using json to connect directly to the CAS Server :**

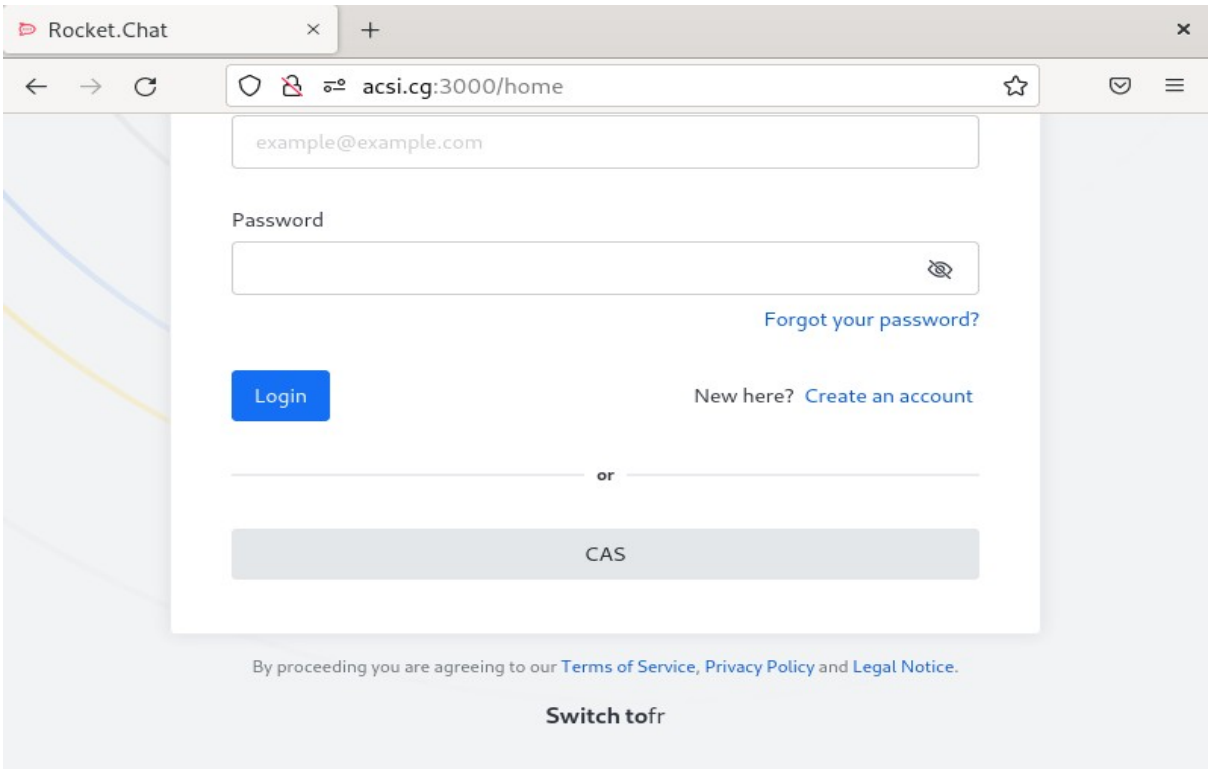
Here are the configurations:





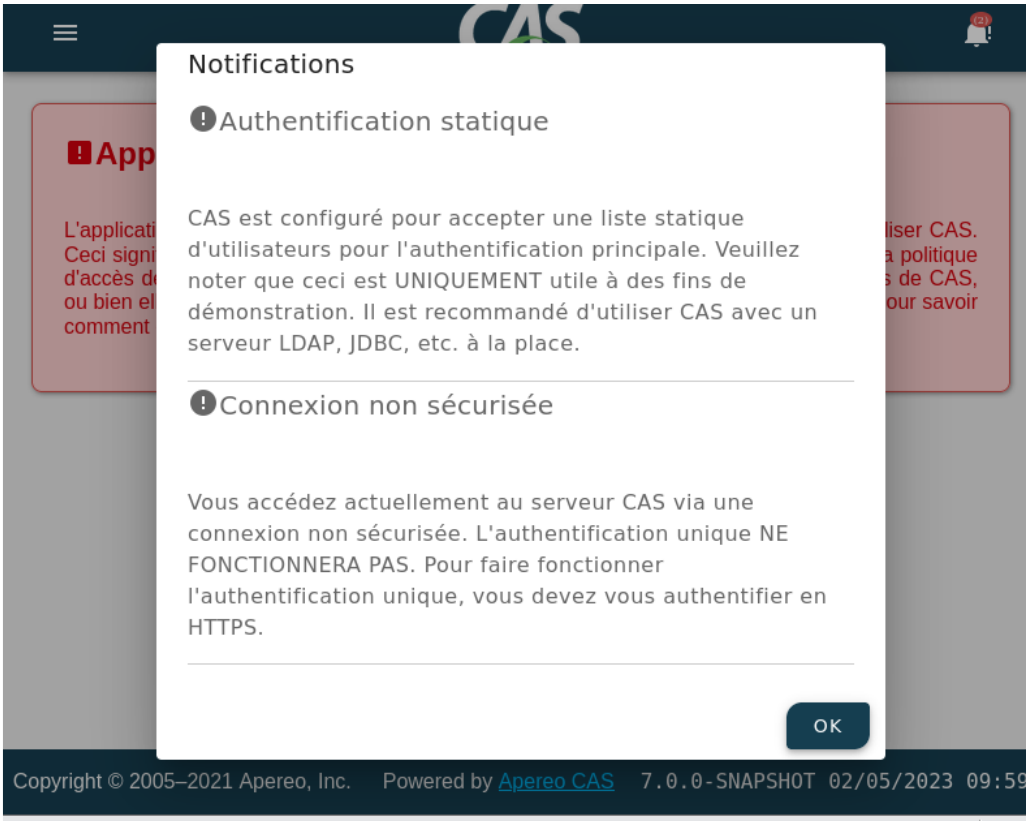


To connect via the CAS option:



Here the difficulty encountered is this:

With notifications as follows:



For the second notification:

Since CAS is deployed on tomcat, I assumed that it would be necessary to set tomcat to https so that connections to CAS Server would also be secure, but I really tried, this limits me to signing the certificate by a recognized certificate authority (CA). I tried but I still couldn't do it because many tutorials ask to use a certificate recognized by the CA.

Pac4j:

-LDAP directory:

To connect this one to CAS you have to configure the file "cas.properties" in the folder etc/cas/Config of the project, but unfortunately this file is no longer available in the new version of CAS, so I created and configured it, but just this evening I understood that LDAP is not connected to CAS, it is most likely due to this problem that LDAP users are unable to authenticate to CAS.

Here is the link where you will find all the information about the ratchet configuration. Chat and other :

https://www.esup-portail.org/wiki/pages/viewpage.action?pageId=972292097

Coeurcy MOKOKO