HOW TO CONNECT KEYCLOAK OF CORE SERVICES WITH ENTERPRISE LDAPS IN HTTP

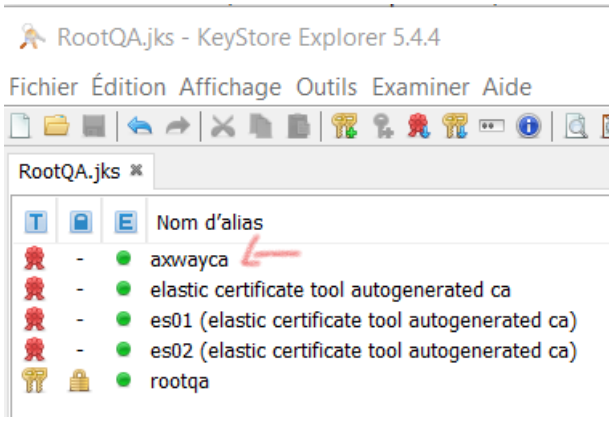
This document is in “work” state and does not replace the official documentation of Keycloak.

- **SETP 1 :**
  Uncomment and specify the truststore in the .env file:

  AUTOM_TRUSTSTORE=RootQA.jks

  AUTOM_TRUSTSTORE_PWD=1234

- **STEP2**
  This truststore file must contain the LDAPS certificate. Copy it into the CERTS_DIR directory indicated in the .env file :



In the appendix, you will find an example of creating a truststore in a few clicks.

- **STEP 3**
  Add these 2 green lines in the docker-compose.yml file :

  ….
  keycloak-itopsvision:
  # container_name: keycloak-itopsvision
  image: axway.jfrog.io/itom-release/itops-keycloak:${PACKAGE_VERSION}
  restart: unless-stopped
  user: ${USR}:${GRP}
  environment:
  …..
  - JAVA_OPTS=-Djavax.net.ssl.trustStore=/opt/jboss/keycloak-basedir/CERTS/${AUTOM_TRUSTSTORE} -Djavax.net.ssl.trustStorePassword=${AUTOM_TRUSTSTORE_PWD}
  …
  volumes:
  …
  - ${CERTS_DIR}:/opt/jboss/keycloak-basedir/CERTS

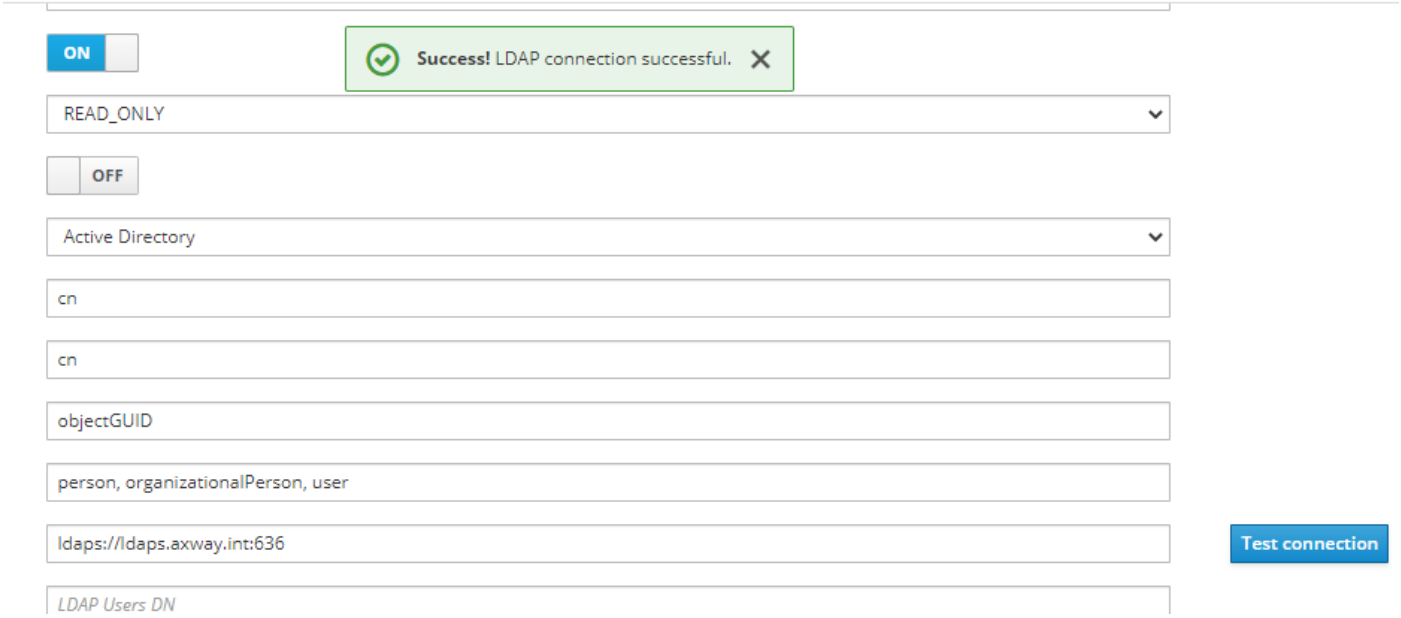
- **STP 4**
  Stop and restart Keycloak :

  docker-compose stop keycloak-itopsvision

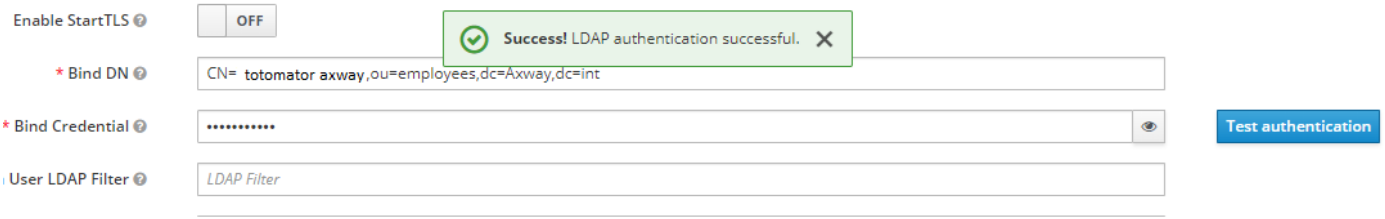
  docker-compose up -d keycloak-itopsvision

STEP 5

Connect to Keycloak then go to the menu “User Federation” - “ldap” then fill in "URL Connection" and do "Connection Test"



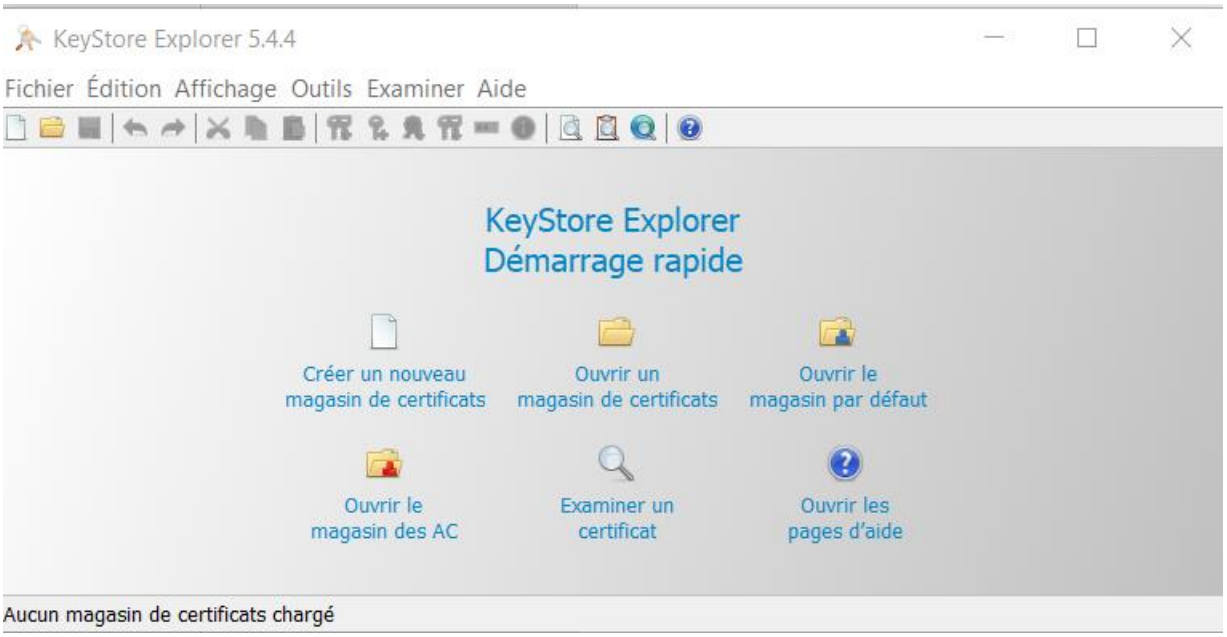
Then test the LDAPS login



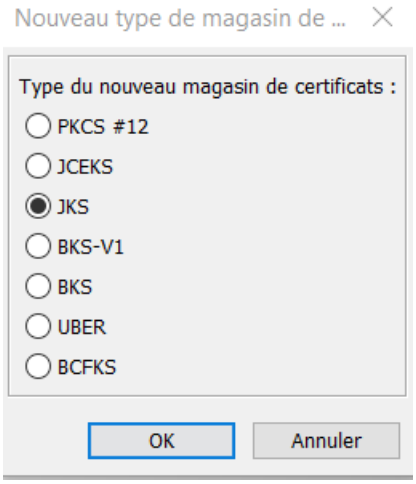
If these tests work fine, configure the other fields by following this documentation :
https://docs.axway.com/bundle/Automator_41_Documentation_allOS_en_HTML5/page/tips___keycloak_-_ldap_synchronization.html

APPENDIX: Creation of a Truststore

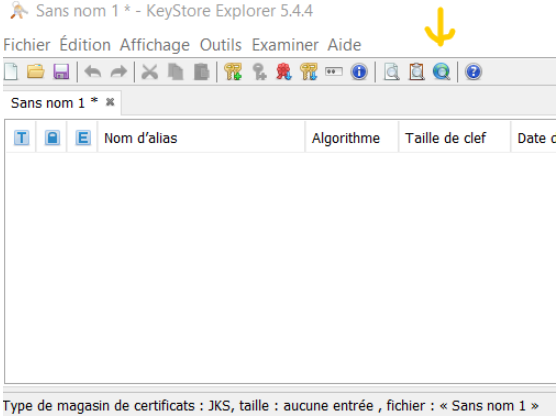
1/ Launch the Keystore Explorer utility



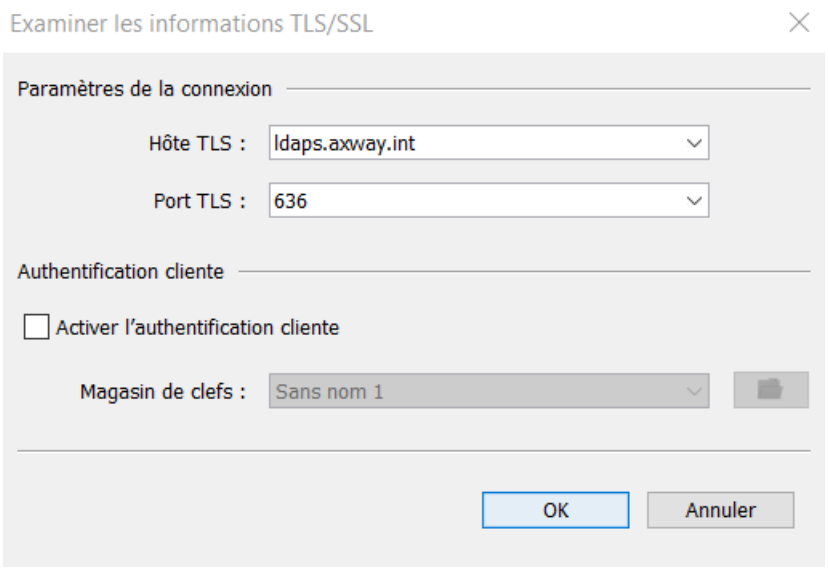
2/ Select "create a new certificate store" and choose JKS :



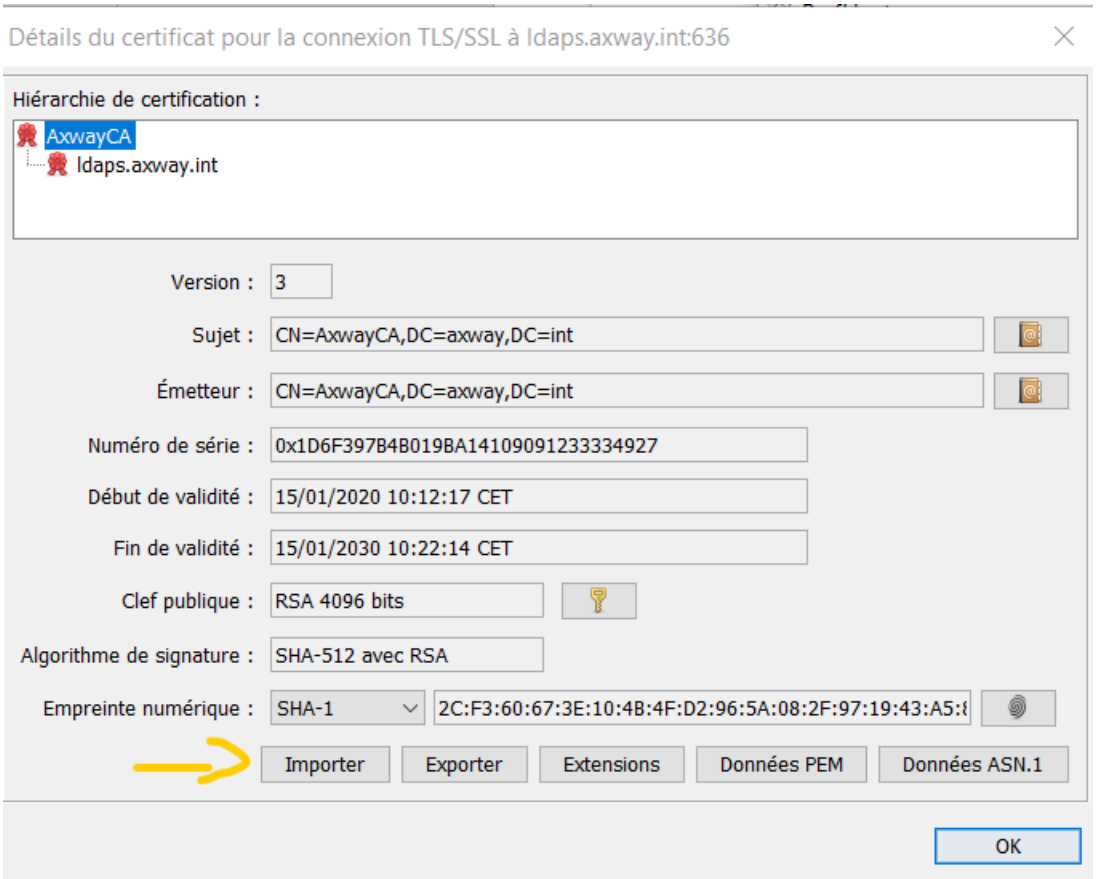
3 / Click on this icon to retrieve the certificate of the site to be trusted :



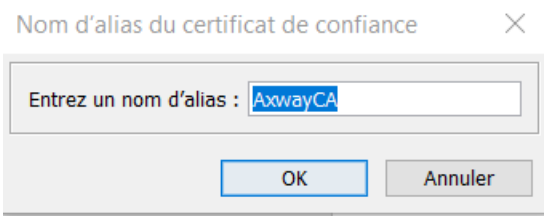
4/ Put the coordinates of the site :



5/ Click "ok" then "import" when the certificate is displayed:



6/ Then click “ok” on the proposed alias:



7/ Last step: save the trust by indicating a password and the name of the file with the extension .jks :