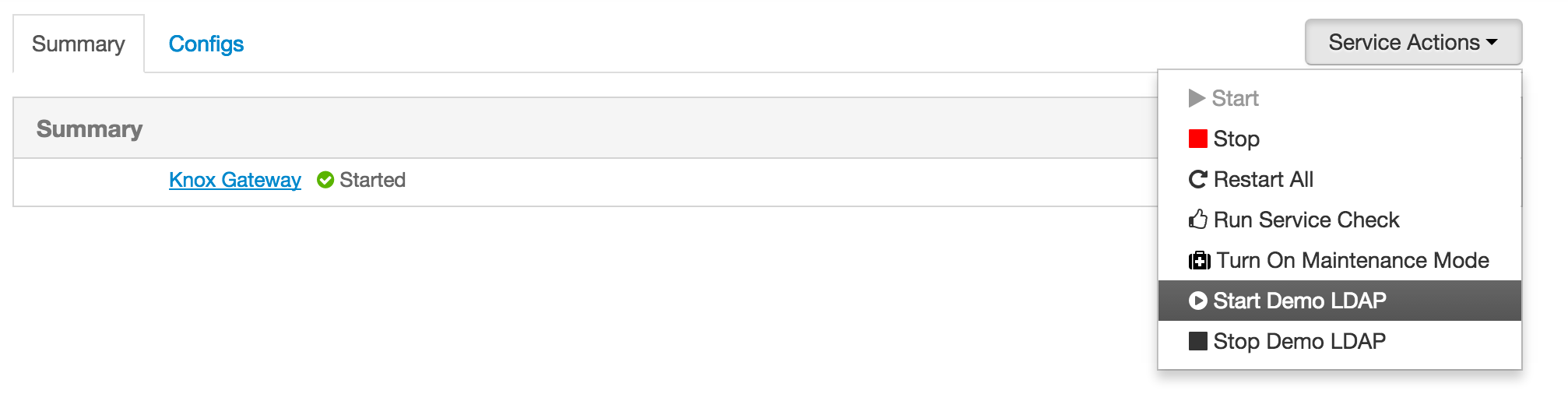
NiFi User Authentication with LDAP

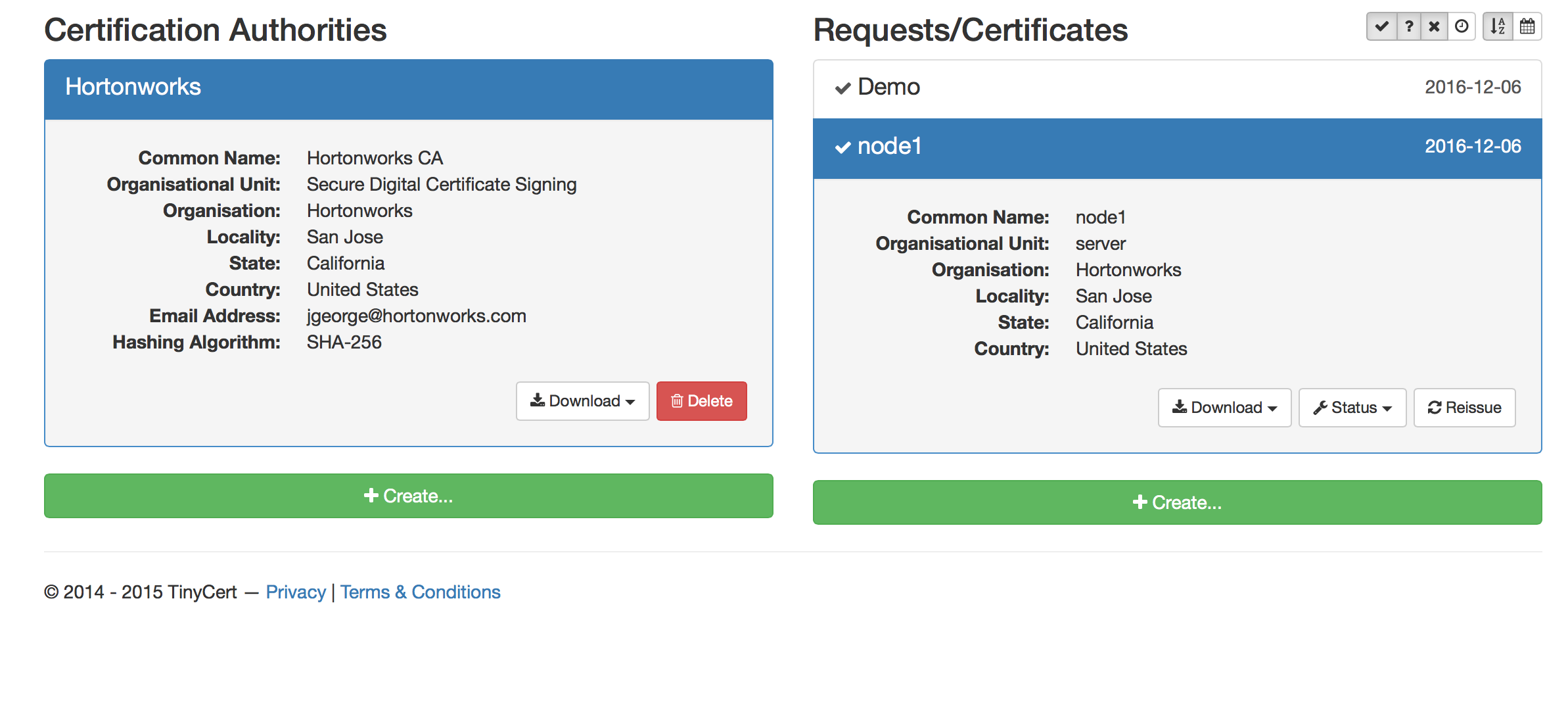
Prerequisite

Make sure Knox is installed on your sandbox and demo LDAP is started.



Steps:

1. I already did created Certification Authorities and client certificates at www.tinycert.org



2. My keystore is saved as *‘/root/scripts/cert.p12’* and a truststore is saved as *‘/root/scripts/cacert.jks’*. and password is set as **hadoop.**

3. Below are the configuration updates you have to do in *nifi.properties* file in sandbox:

# vi /opt/nifi-1.1.0.0-10/conf/nifi.properties

4. Once opened in editor update below properties to given values [updating https port and certificate details]:

*nifi.web.http.host=*

*nifi.web.http.port=*

*nifi.web.https.host=sandbox*

*nifi.web.https.port=9090*

*nifi.security.keystore=/root/scripts/cert.p12*

*nifi.security.keystoreType=PKCS12*

*nifi.security.keystorePasswd=hadoop*

*nifi.security.keyPasswd=hadoop*

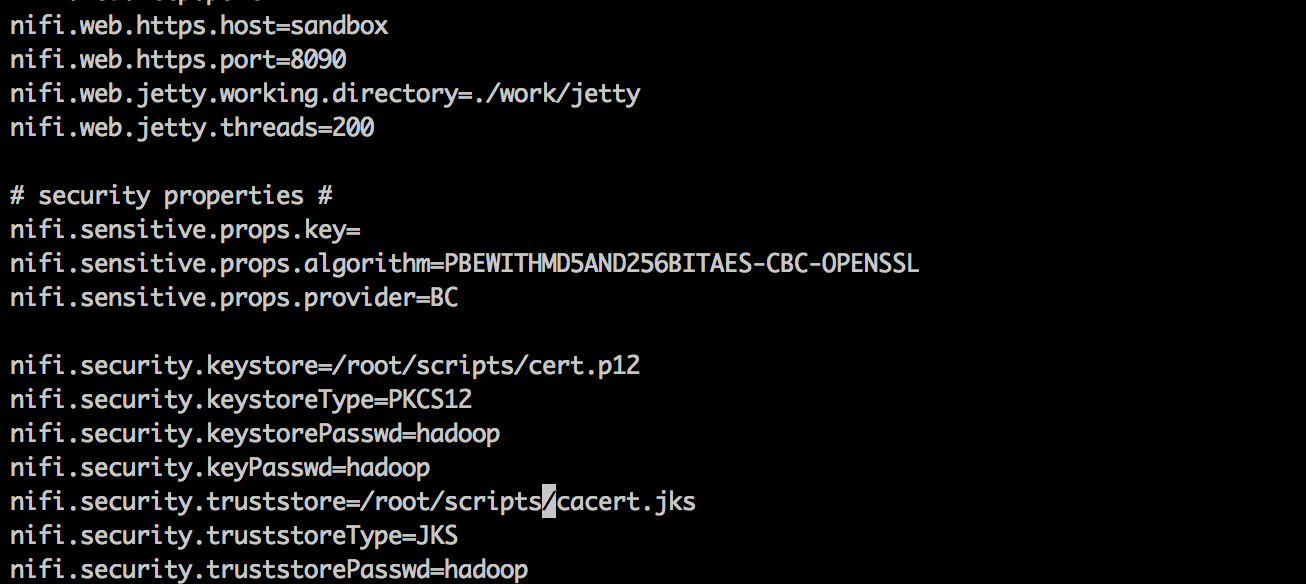
*nifi.security.truststore=/root/scripts/cacert.jks*

*nifi.security.truststoreType=JKS*

*nifi.security.truststorePasswd=hadoop*

***nifi.login.identity.provider.configuration.file=./conf/login-identity-providers.xml***

***nifi.security.user.login.identity.provider=ldap-provider***



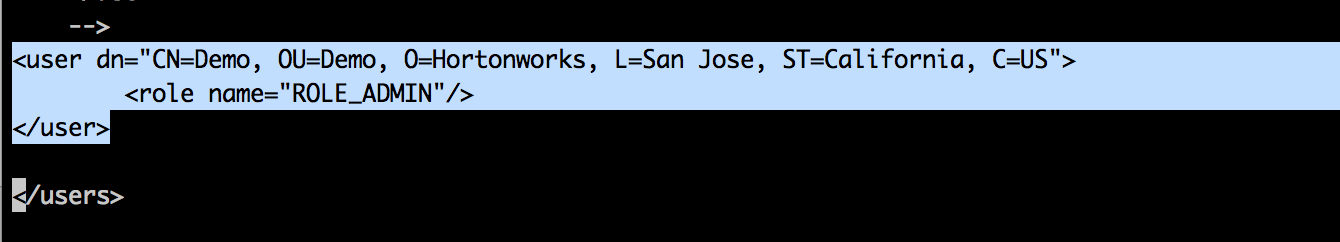
5. Now configure the authorized users in ‘*authorized-users.xml’* file, configuration of user is based on certificate. Configure it exactly as you have in your certificate. Following is my configuration:

vi /opt/nifi-1.1.0.0-10/conf/authorized-users.xml

*<user dn="CN=Demo, OU=Demo, O=Hortonworks, L=San Jose, ST=California, C=US">*

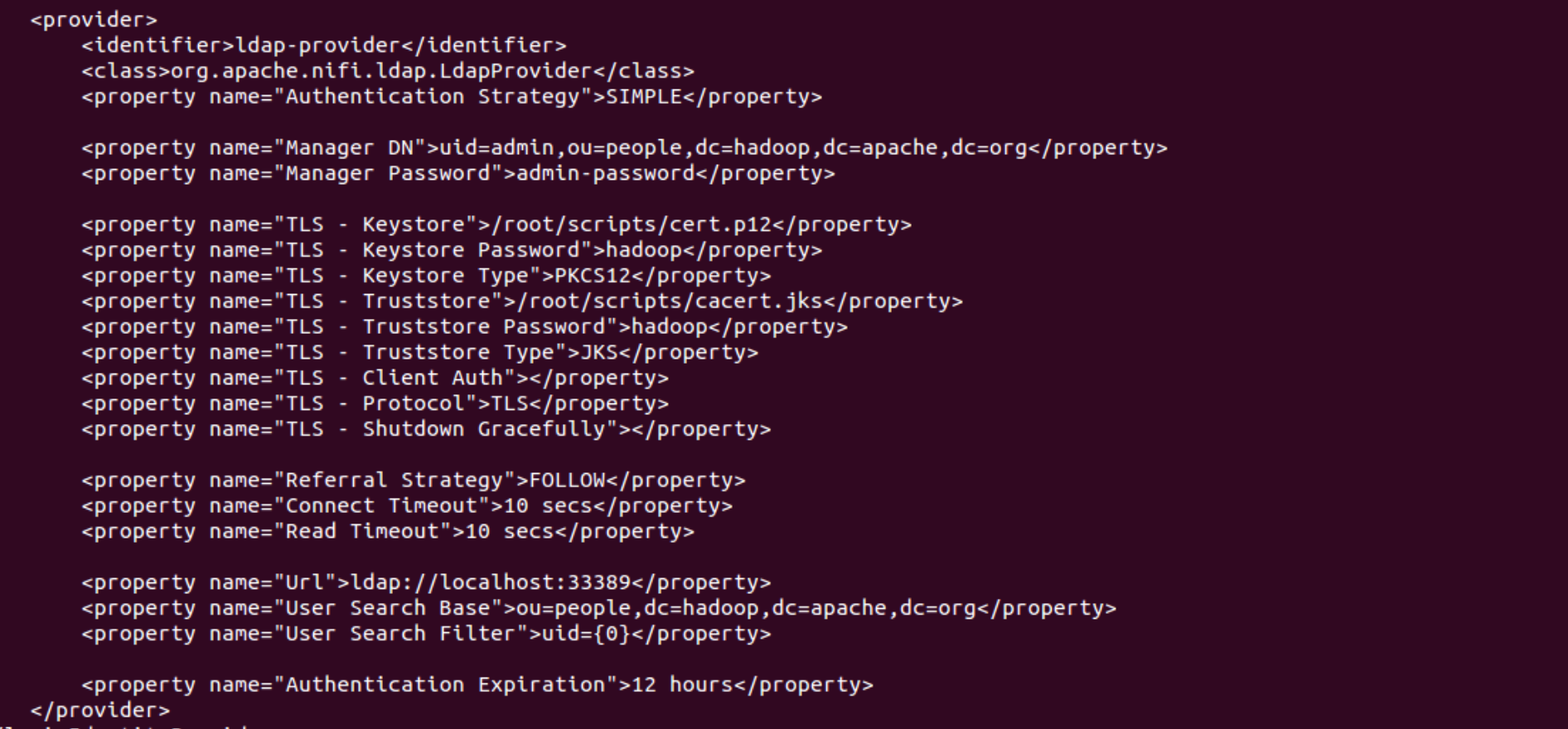
*<role name="ROLE\_ADMIN"/>*

*</user>*



6. Above configuration is to login as NiFi Administrator, every other users can be pulled from LDAP after this administrator assigns roles on request.

7. Configure ./*conf/login-identity-providers.xml* as below with reference to Knox Demo LDAP Server.



<provider>

<identifier>ldap-provider</identifier>

<class>org.apache.nifi.ldap.LdapProvider</class>

<property name="Authentication Strategy">**SIMPLE**</property>

<property name="Manager DN">**uid=admin,ou=people,dc=hadoop,dc=apache,dc=org**</property>

<property name="Manager Password">**admin-password**</property>

<property name="TLS - Keystore">***/root/scripts*/cert.p12**</property>

<property name="TLS - Keystore Password">**hadoop**</property>

<property name="TLS - Keystore Type">**PKCS12**</property>

<property name="TLS - Truststore">***/root/scripts/*cacert.jks**</property>

<property name="TLS - Truststore Password">**hadoop**</property>

<property name="TLS - Truststore Type">**JKS**</property>

<property name="TLS - Client Auth"></property>

<property name="TLS - Protocol">**TLS**</property>

<property name="TLS - Shutdown Gracefully"></property>

<property name="Referral Strategy">FOLLOW</property>

<property name="Connect Timeout">10 secs</property>

<property name="Read Timeout">10 secs</property>

<property name="Url">**ldap://localhost:33389**</property>

<property name="User Search Base">**ou=people,dc=hadoop,dc=apache,dc=org**</property>

<property name="User Search Filter">**uid={0}**</property>

<property name="Authentication Expiration">12 hours</property>

</provider>

8. Once configured, restart NiFi server.

# /opt/nifi-1.1.0.0-10/bin/nifi.sh restart

9. Now say open ‘**Chrome’** browser and load client certificate associated with ADMIN user and login to secure https url of NiFi running on sandbox:

<https://sandbox:9090/nifi>

10. When asked, confirm for security exception and proceed. Now you are securely logged in as Demo user with admin privileges. You can now grant access to any user requesting access who are part of LDAP Directory.

11. Open another browser say ‘**Safari’** to establish another session

<https://sandbox:9090/nifi>

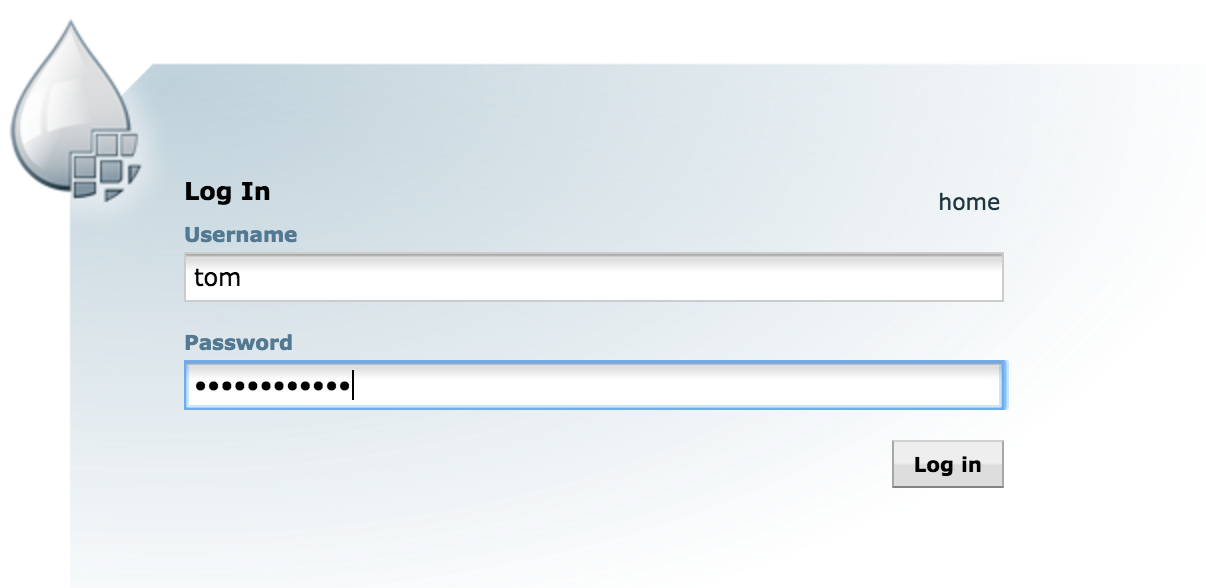
It will popup below screen for login, enter credentials for accounts part of LDAP. Below are credentials part of knox demo ldap we have configured.

*tom/tom-password*

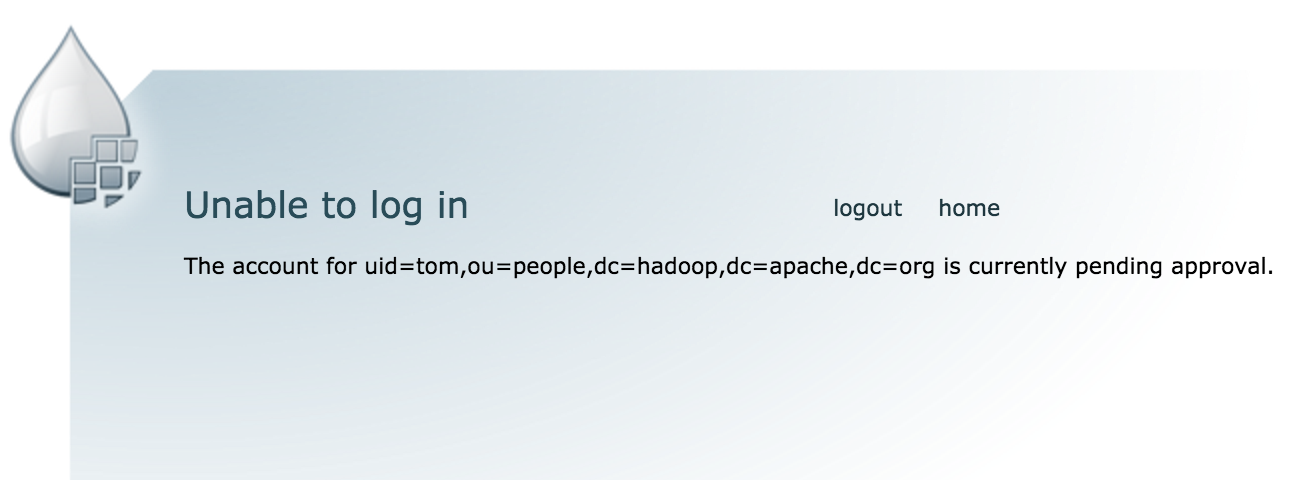
*admin/admin-password*

*sam/sam-password*

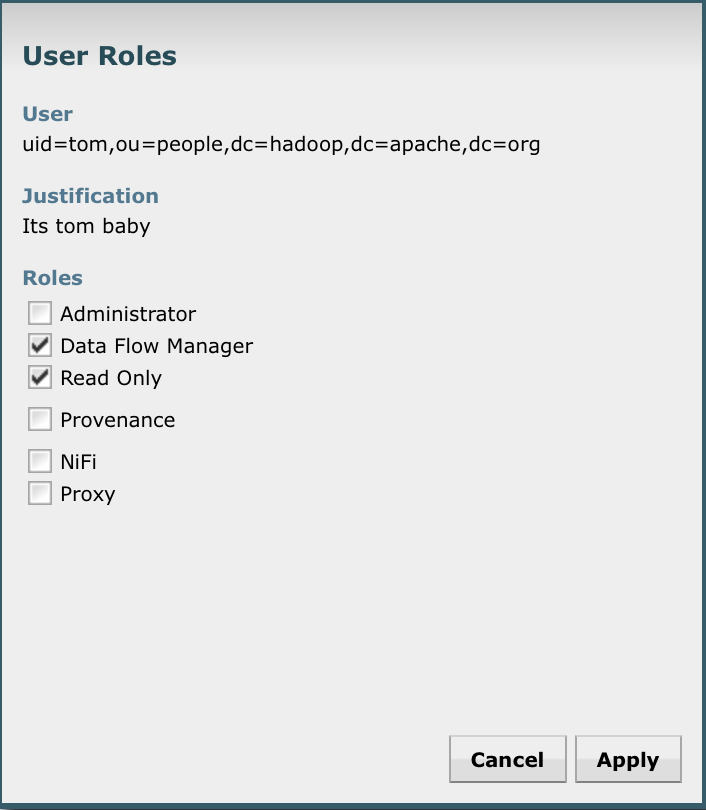
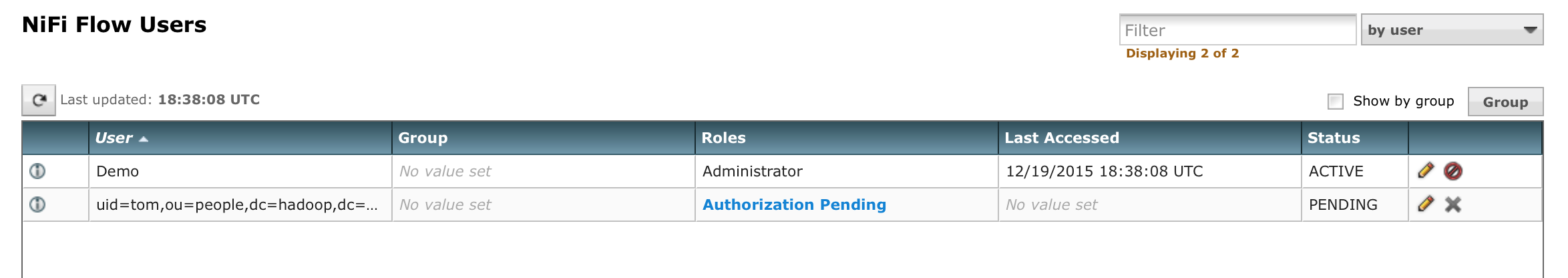
*guest/guest-password*



12. Enter the password and hit login, enter justification and it will show up below screen that request is pending with Admin who already have access using certificates.



13. Now go back to chrome browser where ‘Demo’ user is NiFi Administrator and assign role to Tom



14. Go back to the old session as tom in **safari**, refresh the browser and you will be logged in as tom with privileges assigned by NiFi administrator. You can test if for other users as well.