http://aob01.aob.net:5150/auth/realms/sampler-realm/account

in keycloak federation settings:

#SEE the drive folders.

!!! hardcoded-attribute-mapper type is not available in the current version, for email-verified=true for all new users.

- reasons for -probable- ldap authentication fails => settings in dc

- minimum admin account permissions for keycloak federation user.

- kerberos auth (learn)

- minimum dc settings

### #NOTICE can NET-NAT commands be also used ?

## NOTE: does not respond, sometimes.. remove/reset and add again..

## to forward physical port to local virtualboz port:

netsh interface portproxy add v4tov4 listenaddress=192.168.1.101 listenport=5150 connectaddress=aob01.aob.net connectport=5150

## to list all:

netsh interface portproxy show all

## to remove:

netsh interface portproxy delete v4tov4 listenport=5150 listenaddress=192.168.1.101

## to remove all:

netsh interface portproxy reset

## on dc server, add a user and run the following commands:

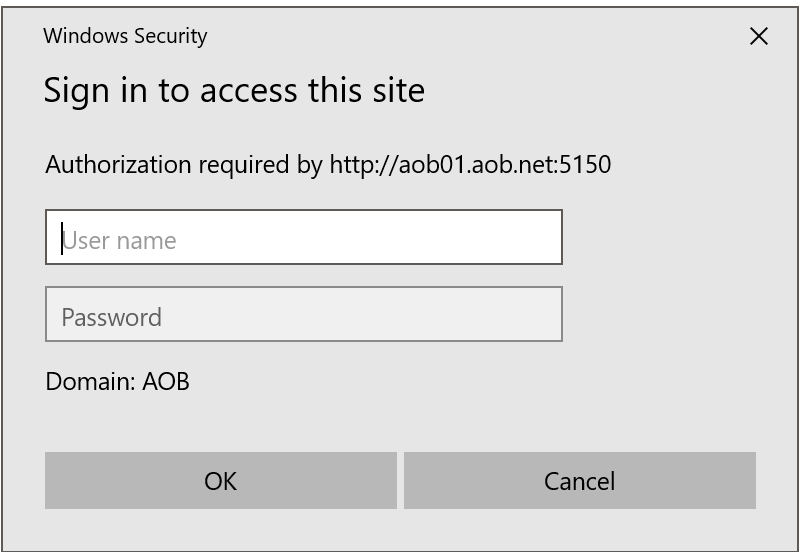
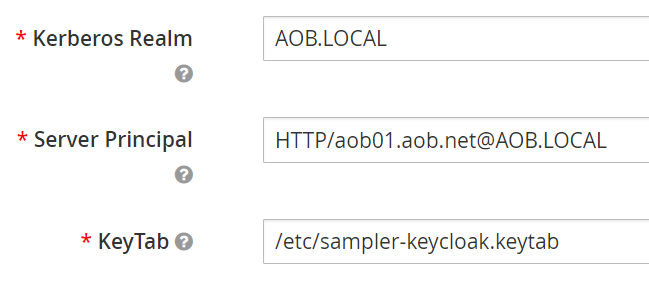
# acc to <http://matthewcasperson.blogspot.com/2015/07/authenticating-via-kerberos-with.html> :

ktpass -out keycloak.keytab -princ HTTP/virtual.local@VIRTUAL.LOCAL -mapUser Keycloak@VIRTUAL.LOCAL -pass password1! -kvno 0 -ptype KRB5\_NT\_PRINCIPAL -crypto RC4-HMAC-NT

setspn -l Keycloak

## on the client computerL

Internet Options -> Local intranet > Sites , add the site..



KEYCLOAK\_IDENTITY => token

KEYCLOAK\_SESSION => url path including uuid/AUTH\_SESSION\_ID

AUTH\_SESSION\_ID => uuid

-- can join a k8s pod to a windows domain ??

-- what clients (may) need ldap/kerberos ...etc

# Firefox automatically logs in the current user, via applying: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system-level_authentication_guide/configuring_applications_for_sso>

about:config => network.negotiate-auth.trusted-uris

# Fixes domain user automatic (passwordless) login in chrome:

<https://specopssoft.com/blog/configuring-chrome-and-firefox-for-windows-integrated-authentication/>

C:\Users\domainuser1\AppData\Local\Google\Chrome\Application\chrome.exe –auth-server-whitelist=”.AOB.NET” –auth-schemes=”negotiate”

or, use registry settings:

Software\Policies\Google\Chrome\AuthSchemes (negotiate)  and  Software\Policies\Google\Chrome\AuthServerWhitelist

# IE and Edge:

site should be added to trusted zones, trusted zone settings may need to be customized.. (allow with current uname passwd)

# secure ldap (ldaps):

##TODO copy from sublime

# group/role mapping from ldap:

##TODO copy from sublime

====================  LDAP Düzenlenecek =======================

Authorization: Negotiate 'spnego-token'

Browser needs to have SPNEGO enabled. Different browsers do that differently. You enable a specific URL for SPNEGO

 -pass password1!

ktpass -out sampler-keycloak.keytab -princ HTTP/aob01.aob.net@AOB.LOCAL -mapUser sampler-keycloak@AOB.LOCAL -kvno 0 -ptype KRB5\_NT\_PRINCIPAL -crypto RC4-HMAC-NT

ldifde /f sampler\_keycloak\_keytab\_principal.ldf /d "CN=sampler keycloak,CN=Users,DC=aob,DC=local" /p base /l samaccountname,userprincipalname

kerberos udp 88 by default

Keycloak renders HTML login screen together with status 401 and HTTP header WWW-Authenticate: Negotiate

In case that the browser has Kerberos ticket from desktop login, it transfers the desktop sign on information to the Keycloak in header Authorization: Negotiate 'spnego-token' . Otherwise it just displays the login screen.

the name:

Windows Integrated Authentication

enabled for IE ??

C:\Users\domainuser1\AppData\Local\Google\Chrome\Application\chrome.exe –auth-server-whitelist=”.AOB.NET” –auth-negotiate-delegatewhitelist=”.AOB.NET” –auth-schemes=”digest,ntlm,negotiate”

# minimum working:

C:\Users\domainuser1\AppData\Local\Google\Chrome\Application\chrome.exe –auth-server-whitelist=”.AOB.NET” –auth-schemes=”negotiate”

## ldaps:

## import root cert to store

$ keytool -import -keystore keycloak.jks -file root.crt -alias root

# import certificate (key and cert should have the same alias) :

keytool -import -alias yourdomain -keystore keycloak.jks -file your-certificate.cer

keytool -list -keystore /home/mposolda/tmp/dev1xy.truststore

## put custom scripts in keycloak:

/opt/jboss/startup-scripts/

## java opts env variable in keycloak:

JAVA\_OPTS\_APPEND="-Dkeycloak.profile.feature.upload\_script=enabled"

-Djavax.net.debug=all ??

##

tls.crt & tls.key in /etc/x509/https/ auto enables https

  => volumemounts may be inappropriate: @see https://hub.docker.com/r/jboss/keycloak/

aob-local-root-ca

389

ldaps 636

asl project management:

sap - primera - bv

DDS:

cilium multicast desteklemiyor, weavenet destekliyor (Bryan Boreham).

hikikomori

https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf\_files/krb5\_conf.html

 keytool -import -trustcacerts -alias aob-local-root-ca -file aob-local-root-ca.cer -keystore keycloak.jks

<spi name="truststore">

    <provider name="file" enabled="true">

        <properties>

            <property name="file" value="/etc/aob-local.jks"/>

            <property name="password" value="password"/>

            <property name="hostname-verification-policy" value="WILDCARD"/>

            <property name="disabled" value="false"/>

        </properties>

    </provider>

</spi>

 /opt/jboss/tools/docker-entrypoint.sh

 /opt/jboss/keycloak/standalone/configuration/standalone.xml

 /opt/jboss/keycloak/standalone/configuration/standalone-ha.xml

 /etc/aob-local.jks

 Keystore /opt/jboss/keycloak/standalone/configuration/application.keystore not found, it will be auto generated on first use with a self signed certificate for host localhost

## custom user federtion mapper:

https://github.com/keycloak/keycloak-documentation/blob/master/server\_development/topics/user-federation-mapper.adoc

https://github.com/keycloak/keycloak/blob/master/federation/ldap/src/main/java/org/keycloak/storage/ldap/LDAPStorageProvider.java

Roles:

realm vs client roles

## Mappers:

MSAD mapper: userAccountControl, pwdLastSet in ldap.

  if pwdLastSet is 0, UPDATE\_PASSWORD required action is added.

  userAccountControl = 514, == user is disabled.

dn: CN=Administrators,CN=Builtin,DC=aob,DC=local

objectClass: group

member: CN=Domain Admins,CN=Users,DC=aob,DC=local

member: CN=Enterprise Admins,CN=Users,DC=aob,DC=local

member: CN=Administrator,CN=Users,DC=aob,DC=local

Keycloak does not list users if it cannot reach ldap server..? :

  Note: Users are already in DB.

Caused by: org.keycloak.models.ModelException: Querying of LDAP failed org.keycloak.storage.ldap.idm.query.internal.LDAPQuery@512d78b6

keycloak04\_1     |      at org.keycloak.storage.ldap.idm.store.ldap.LDAPIdentityStore.fetchQueryResults(LDAPIdentityStore.java:207)

keycloak04\_1     |      at org.keycloak.storage.ldap.idm.query.internal.LDAPQuery.getResultList(LDAPQuery.java:164)

keycloak04\_1     |      ... 87 more

keycloak04\_1     | Caused by: javax.naming.CommunicationException: windcserver.aob.local:636 [Root exception is java.net.ConnectException: Connection timed out (Connection timed out)]