1. 编译安装：

1.configure的命令如下：

./configure --enable-bdb --libdir=/usr/app/BerkeleyDB/lib --includedir=/usr/app/BerkeleyDB/include --prefix=/usr/app/openldap-2.4.47 --enable-modules

2.make depend

3.make

4.make install

1. 把slapd.conf传统配置形式转换为olc形式。
2. 启动slapd服务

/usr/app/openldap-2.4.47/libexec/slapd -h "ldap:/// ldapi:///"。

/usr/app/openldap-2.4.47/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd/dicom.ldif

/usr/app/openldap-2.4.47/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd/dcm4che.ldif

/usr/app/openldap-2.4.47/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd/dcm4chee-archive.ldif

/usr/app/openldap-2.4.47/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd/dcm4chee-archive-ui.ldif

返回的信息如：

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry "cn=dcm4chee-archive-ui,cn=schema,cn=config"

ldap\_add: Insufficient access (50)

1. vi modify-baseDN.ldif

写入：

dn: olcDatabase={1}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=dcm4che,dc=org

-

replace: olcRootDN

olcRootDN: cn=admin,dc=dcm4che,dc=org

-

然后再实行修改：

/usr/app/openldap-2.4.47/bin/ldapmodify -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/modify-baseDN.ldif

返回了以下信息：

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

modifying entry "olcDatabase={1}hdb,cn=config"

ldap\_modify: No such object (32)

matched DN: cn=config

这里是不行的，需要把modify-baseDN.ldif中的olcDatabase={1}hdb改成olcDatabase={1}mdb。然后再：

/usr/app/openldap-2.4.47/bin/ldapmodify -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/modify-baseDN.ldif

返回了以下信息：

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

modifying entry "olcDatabase={1}mdb,cn=config"

ldap\_modify: Insufficient access (50)

1. vi slapd\_setup\_basic.ldif

写入：

dn: dc=dcm4che,dc=org

changetype: add

objectClass: top

objectClass: dcObject

objectClass: organization

o: Example Organisation name

dc: dcm4che

dn: cn=admin,dc=dcm4che,dc=org

changetype: add

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

description: LDAP administrator

userPassword:

然后再实行修改：

/usr/app/openldap-2.4.47/bin/ldapmodify -x -W -D cn=admin,dc=dcm4che,dc=org -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd\_setup\_basic.ldif

如果有

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)

这样的错误，则可能表示cn=admin,dc=dcm4che,dc=org这个dn是不存在的。

那样就是上一步：

/usr/app/openldap-2.4.47/bin/ldapmodify -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/modify-baseDN.ldif

出了问题，毕竟返回了ldap\_modify: Insufficient access (50)。

甚至更早的步骤如：

/usr/app/openldap-2.4.47/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd/dcm4chee-archive-ui.ldif

都出了问题。

同时执行/usr/app/openldap-2.4.47/bin/ldapsearch -x -D cn=config -w secret -b cn=config

都找不到dcm4chee，dicom，admin这些信息，很可能就是说Insufficient access (50)就已经代表失败。

网上查了这是代表权限问题不允许操作，因此操作是无效的。

原因是由于：

cat /usr/app/openldap-2.4.47/etc/openldap/slapd.d/cn\=config/olcDatabase={0}config.ldif

看到的是olcAccess: {0}to \* by \* none这一行

而如果是：

olcAccess: {0}

to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"

manage

by \* none

这样的则代表只有root才能访问configuration database。

解决办法：

用强硬办法，只能（虽然文件里说不要手动修改它，但现在没办法。）：

把/usr/app/openldap-2.4.47/etc/openldap/slapd.d/cn\=config/olcDatabase={0}config.ldif文件中的

olcAccess: {0}to \* by \* none这一行改为：

olcAccess: {0} to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage by \* none

否则就是root也无法修改，无法执行任何的ldapmodify命令。

1. 修改了之后把dicom.ldif这些导入了之后，再

/usr/app/openldap-2.4.47/bin/ldapsearch -x -D cn=config -w secret -b cn=config|grep dcm4che

就看到了东西，以前就是Insufficient access (50)所以没东西的。

1. 命令：

/usr/app/openldap-2.4.47/bin/ldapsearch -H ldapi:/// -Y EXTERNAL -b "cn=config" -LLL -Q "olcDatabase=\*" dn

找到后端的Database。

编写文件：

[root@localhost cn=config]# cat /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/modify-baseDN.ldif

dn: olcDatabase={1}mdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=dcm4che,dc=org

-

replace: olcRootDN

olcRootDN: cn=admin,dc=dcm4che,dc=org

实施修改：

[root@localhost cn=config]# /usr/app/openldap-2.4.47/bin/ldapmodify -Y EXTERNAL -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/modify-baseDN.ldif

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

modifying entry "olcDatabase={1}mdb,cn=config"

cat /usr/app/openldap-2.4.47/etc/openldap/slapd.d/cn\=config/olcDatabase={1}mdb.ldif

看到里面被修改了。

1. /usr/app/openldap-2.4.47/bin/ldapmodify -x -W -D cn=admin,dc=dcm4che,dc=org -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd\_setup\_basic.ldif

如果出现：

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)怎样输入密码都不对的情况，则修改密码：

进入交互模式：/usr/app/openldap-2.4.47/bin/ldapmodify -Y EXTERNAL -H ldapi:///

输入：

dn: olcDatabase={1}mdb,cn=config

replace: olcRootPW

olcRootPW: {SSHA}hEj911HKkeFtXFjVKAO4WK1VKzQ1MLPI

三行

Ctrl+d退出

而RootPW是执行：slappasswd命令后自己输入密码后返回的信息。

如果成功修改则会返回：

modifying entry "olcDatabase={1}mdb,cn=config"

再次执行：

/usr/app/openldap-2.4.47/bin/ldapmodify -x -W -D cn=admin,dc=dcm4che,dc=org -H ldapi:/// -f /usr/app/dcm4chee-arc-5.17.1-mysql-secure/ldap/slapd\_setup\_basic.ldif

输入刚才的密码，成功则返回：

Enter LDAP Password:

adding new entry "dc=dcm4che,dc=org"

adding new entry "cn=admin,dc=dcm4che,dc=org"

1. 安装ApacheDS:

./apacheds-2.0.0.AM25-64bit.bin

启动/etc/init.d/apacheds-2.0.0.AM25-default start

然而以前已经安装过，以前安装过的在搞过一些配置后出了问题，启动了之后自动退出，重新安装问题也没有解决。

把安装的那些文件目录都删掉重新安装：

[root@localhost app]# rm -rf /opt/apacheds-2.0.0.AM25

[root@localhost app]# rm -rf /var/lib/apacheds-2.0.0.AM25

[root@localhost app]# rm -rf /etc/init.d/apacheds-2.0.0.AM25-default

问题解决。

端口号为10389：

tcp6 0 0 :::10389 :::\* LISTEN 5153/java

1. 用Apache Directory Studio 2.0.0-M9在10389端口进行配置：

建立连接：

Network Parameter:

Hostname: localhost

Port: 10389

Authentication Parameter:

Bind DN or user: uid=admin,ou=system

Bind password: secret

导入：

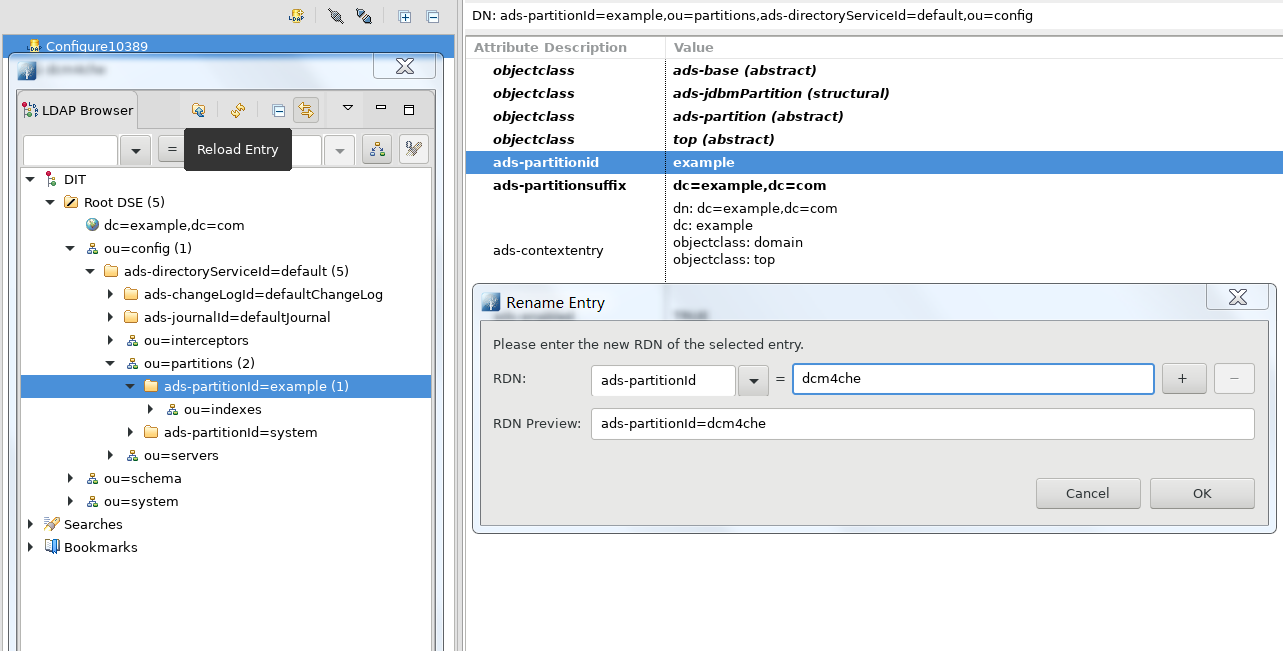
$DCM4CHEE\_ARC/ldap/apacheds/dicom.ldif

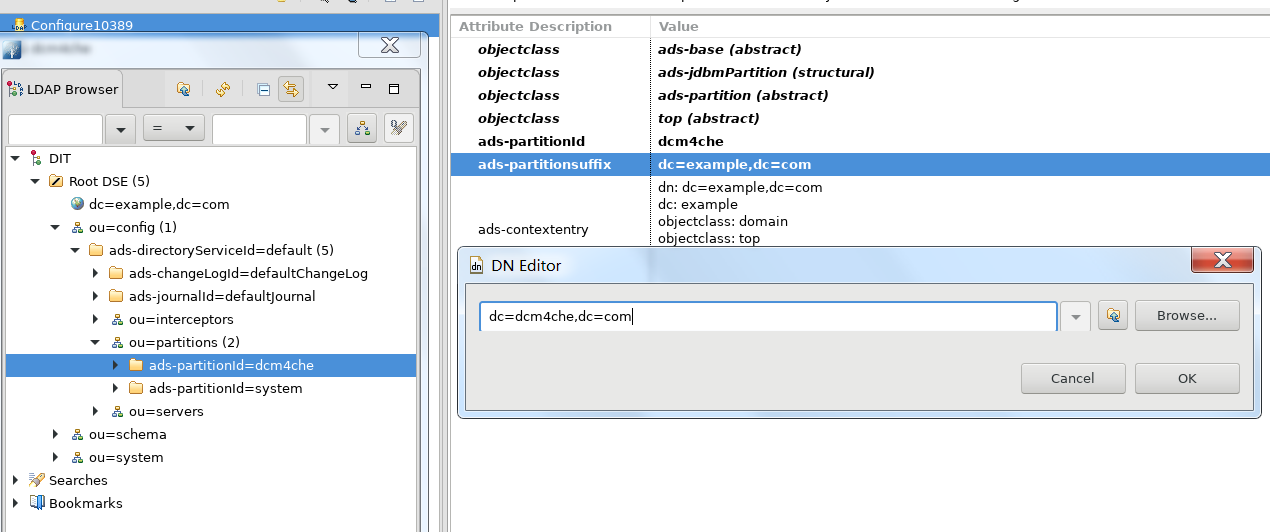
$DCM4CHEE\_ARC/ldap/apacheds/dcm4che.ldif

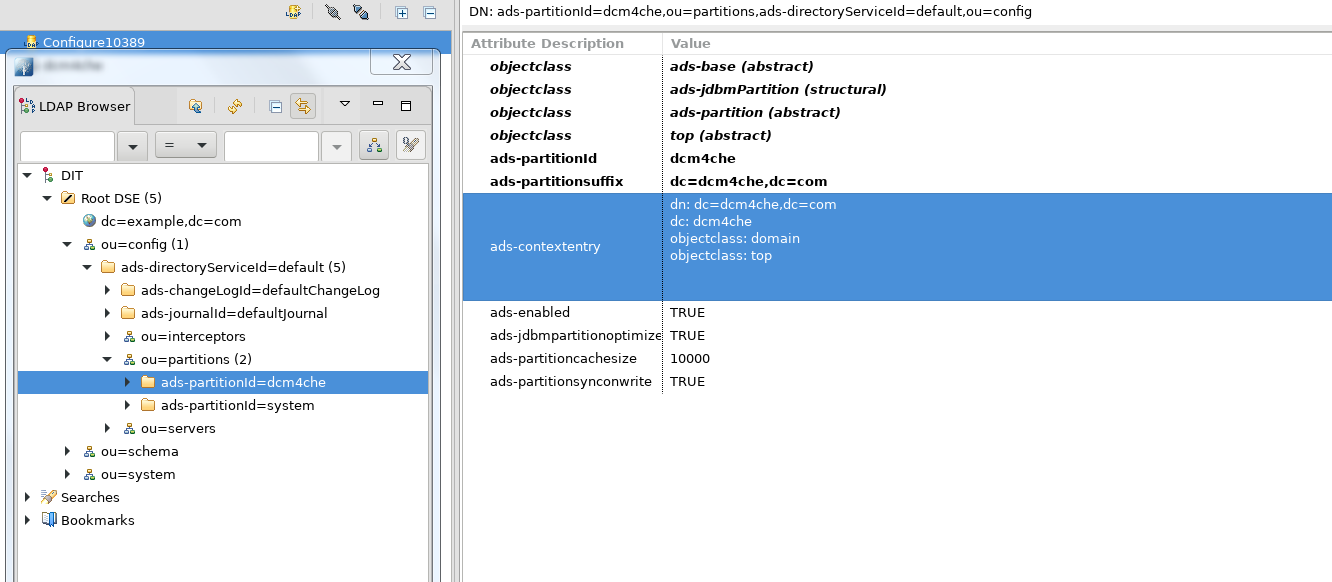
$DCM4CHEE\_ARC/ldap/apacheds/dcm4chee-archive.ldif

$DCM4CHEE\_ARC/ldap/apacheds/dcm4chee-archive-ui.ldif

然后对一些值进行修改：







然而在重启apacheds的时候报错(日志文件在/var/lib/apacheds-2.0.0.AM25/default/log/apacheds.log或者/etc/init.d/apacheds-2.0.0.AM25-default console)：

jvm 1 | [18:14:38] ERROR [org.apache.directory.api.ldap.schema.loader.LdifSchemaLoader] - ERR\_16009\_LDIF\_LOAD\_FAIL Failed to load schema LDIF file cn=dicom.ldif

jvm 1 | org.apache.directory.api.ldap.model.exception.LdapInvalidAttributeValueException: ERR\_13215\_VALUE\_EXPECT\_STRING The value is expected to be a String

jvm 1 | at org.apache.directory.api.ldap.model.entry.DefaultAttribute.getString(DefaultAttribute.java:517)

jvm 1 | at org.apache.directory.api.ldap.model.schema.registries.AbstractSchemaLoader.getSchema(AbstractSchemaLoader.java:171)

jvm 1 | at org.apache.directory.api.ldap.schema.loader.LdifSchemaLoader.initializeSchemas(LdifSchemaLoader.java:141)

jvm 1 | at org.apache.directory.api.ldap.schema.loader.LdifSchemaLoader.<init>(LdifSchemaLoader.java:111)

jvm 1 | at org.apache.directory.server.ApacheDsService.initSchemaManager(ApacheDsService.java:288)

jvm 1 | at org.apache.directory.server.ApacheDsService.start(ApacheDsService.java:183)

jvm 1 | at org.apache.directory.server.ApacheDsService.start(ApacheDsService.java:152)

jvm 1 | at org.apache.directory.server.wrapper.ApacheDsTanukiWrapper.start(ApacheDsTanukiWrapper.java:175)

jvm 1 | at org.tanukisoftware.wrapper.WrapperManager$12.run(WrapperManager.java:2788)

jvm 1 | [18:14:38] ERROR [org.apache.directory.server.wrapper.ApacheDsTanukiWrapper] - Failed to start the service.

jvm 1 | org.apache.directory.api.ldap.model.exception.LdapInvalidAttributeValueException: ERR\_13215\_VALUE\_EXPECT\_STRING The value is expected to be a String

jvm 1 | at org.apache.directory.api.ldap.model.entry.DefaultAttribute.getString(DefaultAttribute.java:517)

jvm 1 | at org.apache.directory.api.ldap.model.schema.registries.AbstractSchemaLoader.getSchema(AbstractSchemaLoader.java:171)

jvm 1 | at org.apache.directory.api.ldap.schema.loader.LdifSchemaLoader.initializeSchemas(LdifSchemaLoader.java:141)

jvm 1 | at org.apache.directory.api.ldap.schema.loader.LdifSchemaLoader.<init>(LdifSchemaLoader.java:111)

jvm 1 | at org.apache.directory.server.ApacheDsService.initSchemaManager(ApacheDsService.java:288)

jvm 1 | at org.apache.directory.server.ApacheDsService.start(ApacheDsService.java:183)

jvm 1 | at org.apache.directory.server.ApacheDsService.start(ApacheDsService.java:152)

jvm 1 | at org.apache.directory.server.wrapper.ApacheDsTanukiWrapper.start(ApacheDsTanukiWrapper.java:175)

jvm 1 | at org.tanukisoftware.wrapper.WrapperManager$12.run(WrapperManager.java:2788)

找到cn=dicom.ldif文件的位置：

/var/lib/apacheds-2.0.0.AM25/default/partitions/schema/ou=schema/cn=dicom.ldif

解决办法(https://issues.apache.org/jira/browse/DIRAPI-326)：

/var/lib/apacheds-2.0.0.AM25/default/partitions/schema/ou=schema/cn=dicom.ldif

/var/lib/apacheds-2.0.0.AM25/default/partitions/schema/ou=schema/cn=dcm4che.ldif

/var/lib/apacheds-2.0.0.AM25/default/partitions/schema/ou=schema/cn=dcm4chee-archive.ldif

/var/lib/apacheds-2.0.0.AM25/default/partitions/schema/ou=schema/cn=dcm4chee-archive-ui.ldif

四个文件。

把：

creatorsName:: MC45LjIzNDIuMTkyMDAzMDAuMTAwLjEuMT0gYWRtaW4gLDIuNS40LjExPSBzeXN0Z

W0g

改为：

creatorsname: uid=admin,ou=system

之后ApacheDS就能成功启动。

1. 用ApacheDS Browser连接：

Network Parameter:

Hostname: localhost

Port: 389

Authentication Parameter:

Bind DN or user: cn=admin,dc=dcm4che,dc=org

Bind password: secret

Browser Options:

Base DN: dc=dcm4che,dc=org

其中密码是自己设置的admin的密码，是用slappasswd设置的那个。

导入：

$DCM4CHEE\_ARC/ldap/init-baseDN.ldif

$DCM4CHEE\_ARC/ldap/init-config.ldif

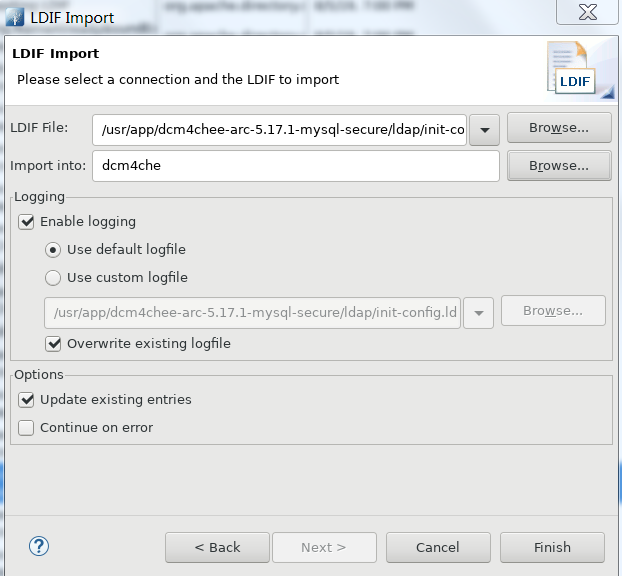
$DCM4CHEE\_ARC/ldap/default-config.ldif

$DCM4CHEE\_ARC/ldap/default-ui-config.ldif

$DCM4CHEE\_ARC/ldap/add-vendor-data.ldif

如果报错：

javax.naming.NameAlreadyBoundException:



则把Update existing entries选上。

1. 在keycloak服务器配置好后，先停掉keycloak服务器。
2. 现在尝试用LDAP联动的方式来配置Keycloak的用户。

如果在389端口导入的话，会报错：

Error while importing LDIF

- [LDAP: error code 21 - objectClass: value #0 invalid per syntax]

java.lang.Exception: [LDAP: error code 21 - objectClass: value #0 invalid per syntax]

如果在10389端口导入的话，也会报错：

Error while importing LDIF

- [LDAP: error code 32 - NO\_SUCH\_OBJECT: failed for MessageType : ADD\_REQUES

java.lang.Exception: [LDAP: error code 32 - NO\_SUCH\_OBJECT: failed for MessageType : ADD\_REQUEST

Message ID : 11

Add Request :

Entry

dn: ou=users,dc=dcm4che,dc=org

objectClass: organizationalUnit

objectClass: top

ou: users

: ERR\_268 Cannot find a partition for ou=users,dc=dcm4che,dc=org]

通过官网后面的给出的信息，推测是在389端口导入而不是10389端口导入的（经过后面确认，的确是从389端口导入）。

objectClass: value #0指的是objectClass: organizationalUnit

然而：

[root@localhost cn=schema]# /usr/app/openldap-2.4.47/bin/ldapsearch -x -D cn=config -w secret -b cn=config|grep organizationalUnit

olcAttributeTypes: {8}( 2.5.4.11 NAME ( 'ou' 'organizationalUnitName' ) DESC '

olcObjectClasses: {3}( 2.5.6.5 NAME 'organizationalUnit' DESC 'RFC2256: an org

是有的。

同时以前的操作也有过成功的信息：

#!RESULT OK

#!CONNECTION ldap://localhost:10389

#!DATE 2019-08-05T09:51:54.382

dn: ou=syntaxes, cn=dcm4chee-archive-ui, ou=schema

changetype: add

ou: syntaxes

objectclass: organizationalUnit

objectclass: top

其实也可以通过命令行来添加：

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -D cn=admin,dc=dcm4che,dc=org -W -f /home/ftpuser/df-user.ldif

Enter LDAP Password:

adding new entry "ou=users,dc=dcm4che,dc=org"

adding new entry "uid=admin,ou=users,dc=dcm4che,dc=org"

ldap\_add: Invalid syntax (21)

additional info: objectClass: value #0 invalid per syntax

用交互的方法来添加也不行：

[root@localhost bin]# ./ldapadd -Y EXTERNAL -H ldapi:///

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

dn: ou=users,dc=dcm4che,dc=org

ou: users

objectClass: organizationalUnit

objectClass: top

adding new entry "ou=users,dc=dcm4che,dc=org"

ldap\_add: Insufficient access (50)

additional info: no write access to parent

然而报了另外的错误。

实际上说的是：

[root@localhost bin]# ./ldapadd -Y EXTERNAL -H ldapi:///

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

dn: uid=admin,ou=users,dc=dcm4che,dc=org

uid: admin

objectClass: inetOrgPerson

objectClass: organizationalPerson

sn:: IA==

cn:: IA==

userPassword:: YWRtaW4=

adding new entry "uid=admin,ou=users,dc=dcm4che,dc=org"

ldap\_add: Invalid syntax (21)

additional info: objectClass: value #0 invalid per syntax

inetOrgPerson这个Object找不到，刚才认为organizationalUnit有问题，其实不是，是inetOrgPerson有问题。

找遍了(grep inetOrgPerson \*)dcm4che给的文件夹都看不到，ldapsearch也找不到，inetOrgPerson没有导入，因此报错。

在/usr/app/openldap-2.4.47/etc/openldap/schema/inetorgperson.ldif找到了inetOrgPerson。

然而尝试导入的时候遇到问题：

[LDAP: error code 50 - Insufficient Access Rights]

java.lang.Exception: [LDAP: error code 50 - Insufficient Access Rights]

无论是从Browser还是命令行都不行。

做了几次尝试：

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -D cn=admin,dc=dcm4che,dc=org -H ldapi:/// -f /home/ftpuser/inetorgperson.ldif

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -H ldapi:/// -f /home/ftpuser/inetorgperson.ldif

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -H ldapi:/// -f /home/ftpuser/inetorgperson.ldif

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -D cn=config -H ldapi:/// -f /home/ftpuser/inetorgperson.ldif

Enter LDAP Password:

ldap\_bind: Invalid credentials (49)

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -D cn=config -H ldapi:/// -f /home/ftpuser/inetorgperson.ldif

Enter LDAP Password:

adding new entry "cn=inetorgperson,cn=schema,cn=config"

ldap\_add: Other (e.g., implementation specific) error (80)

additional info: olcObjectClasses: AttributeType not found: "audio"

其中改了dn: olcDatabase={0}config,cn=config的密码。

解决办法：

需要把另外一个ldif导入：

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -D cn=config -H ldapi:/// -f /usr/app/openldap-2.4.47/etc/openldap/schema/cosine.ldif

Enter LDAP Password:

adding new entry "cn=cosine,cn=schema,cn=config"

[root@localhost bin]# /usr/app/openldap-2.4.47/bin/ldapadd -x -W -D cn=config -H ldapi:/// -f /usr/app/openldap-2.4.47/etc/openldap/schema/inetorgperson.ldif

Enter LDAP Password:

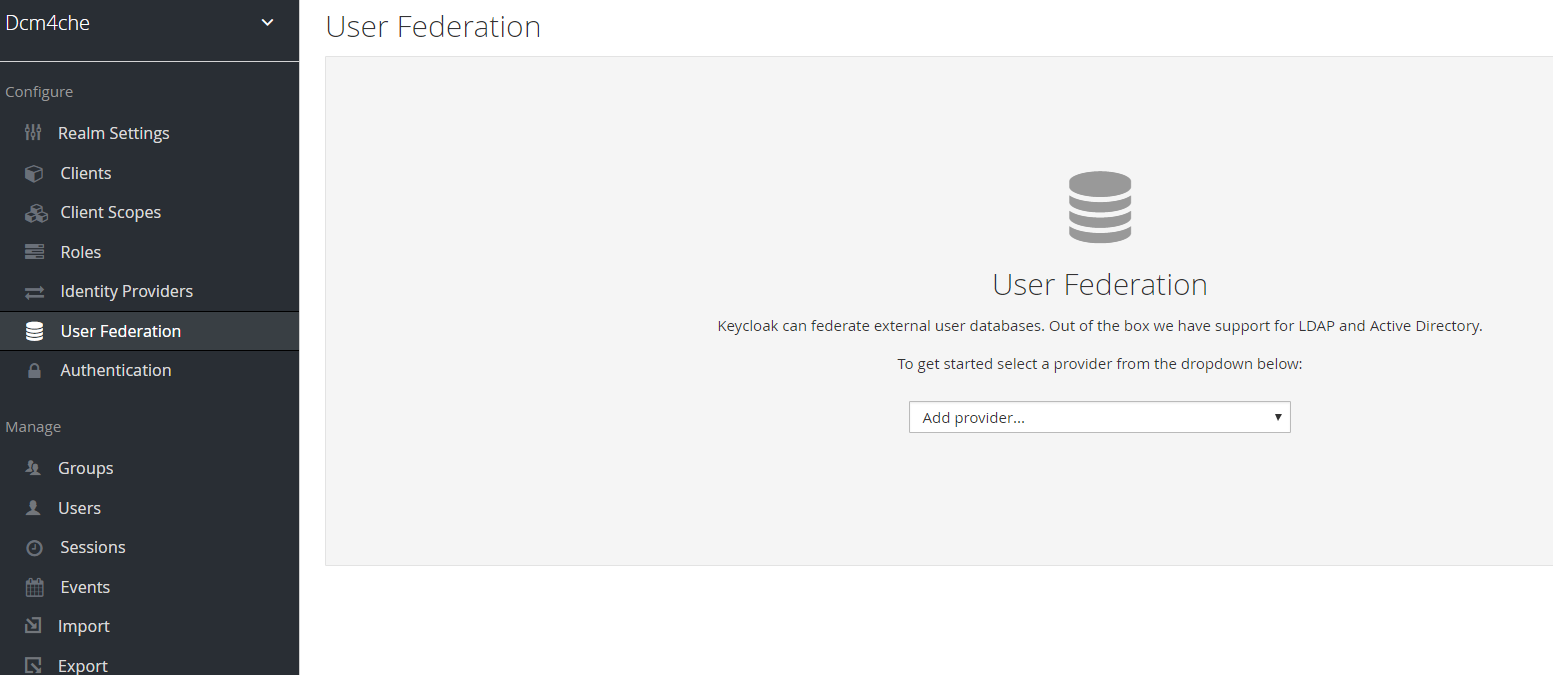
adding new entry "cn=inetorgperson,cn=schema,cn=config"

最终通过命令行成功导入inetorgperson.ldif。

导入inetorgperson.ldif后就能够在Browser成功导入default-users.ldif。

1. 启动keycloak服务器。

进入<http://192.168.15.31:8080/auth/>



下拉选择ldap。

然后填写信息：

Edit Mode : WRITABLE

Sync Registrations : ON

Vendor : Other

Connection URL : ldap://<host>:<port>

Users DN : ou=users,dc=dcm4che,dc=org

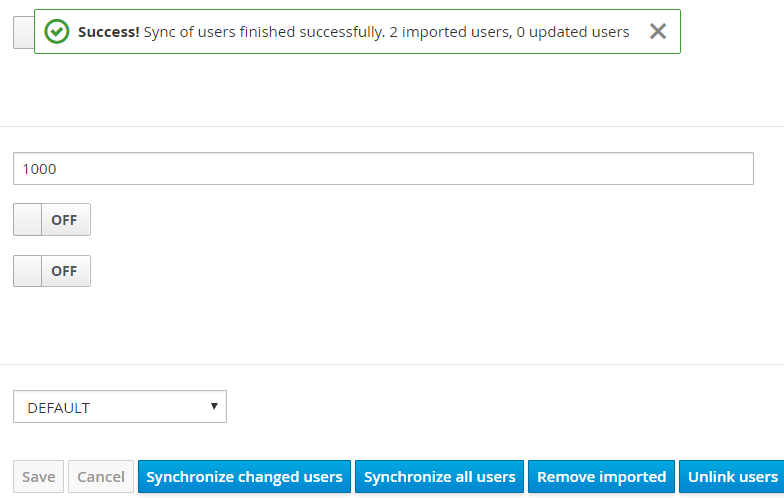
Bind DN : cn=admin,dc=dcm4che,dc=org

Bind Credential : <rootpw>

Validate Password Policy : ON

保存之前先测试下连通性和是否成功授权。

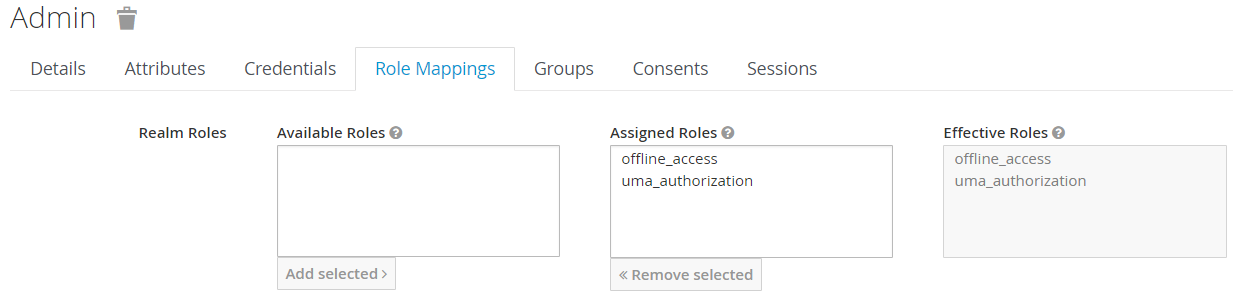
然后点击：Synchronize all users，成功则会如下图所示：

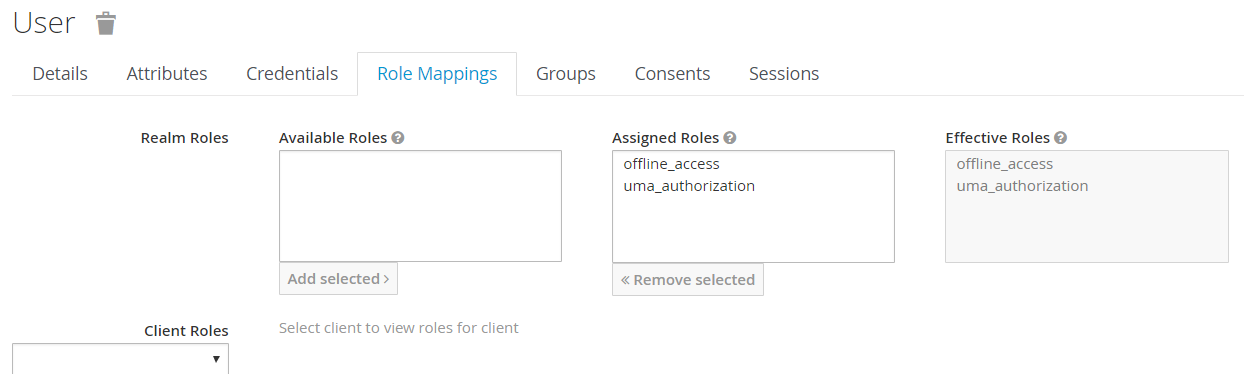


可以看到新增了两个Users(Admin和User)：

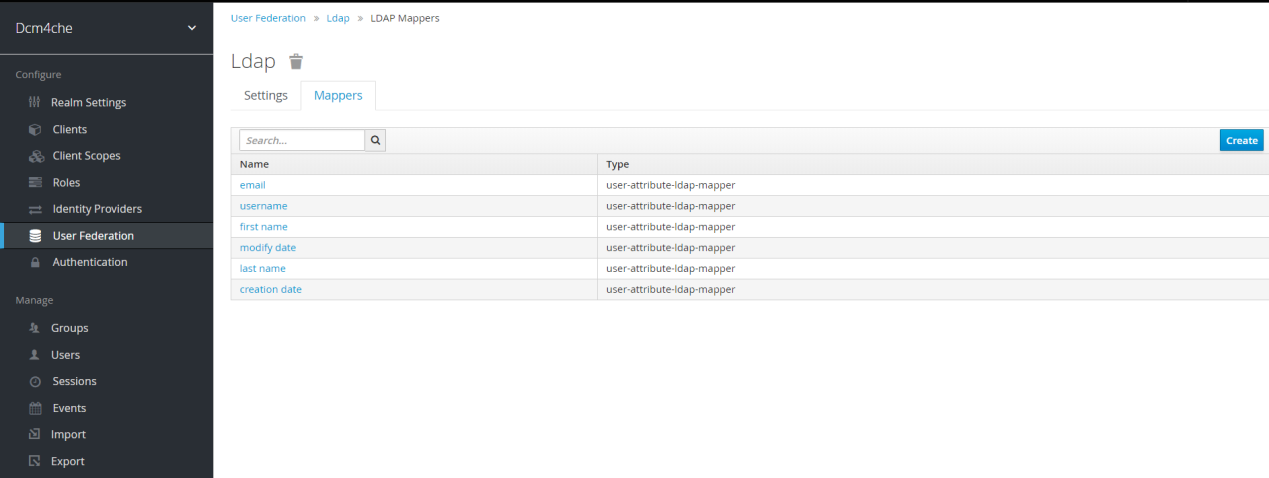


然后查看两个Users都有什么Roles(offline\_access和uma\_authorization)：

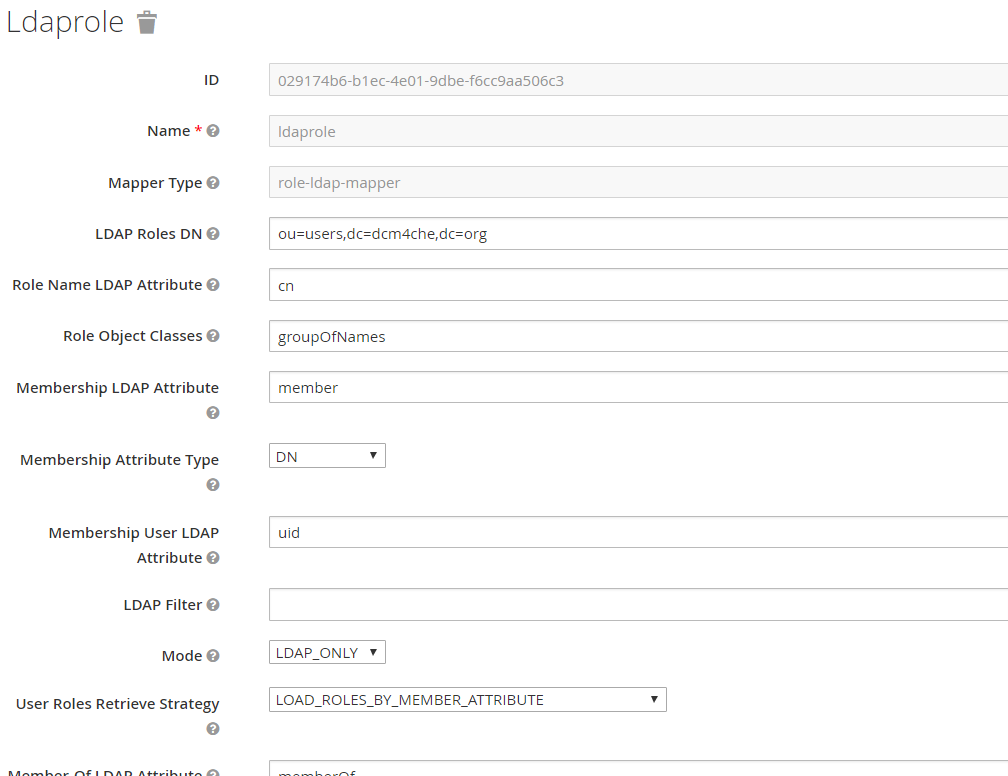
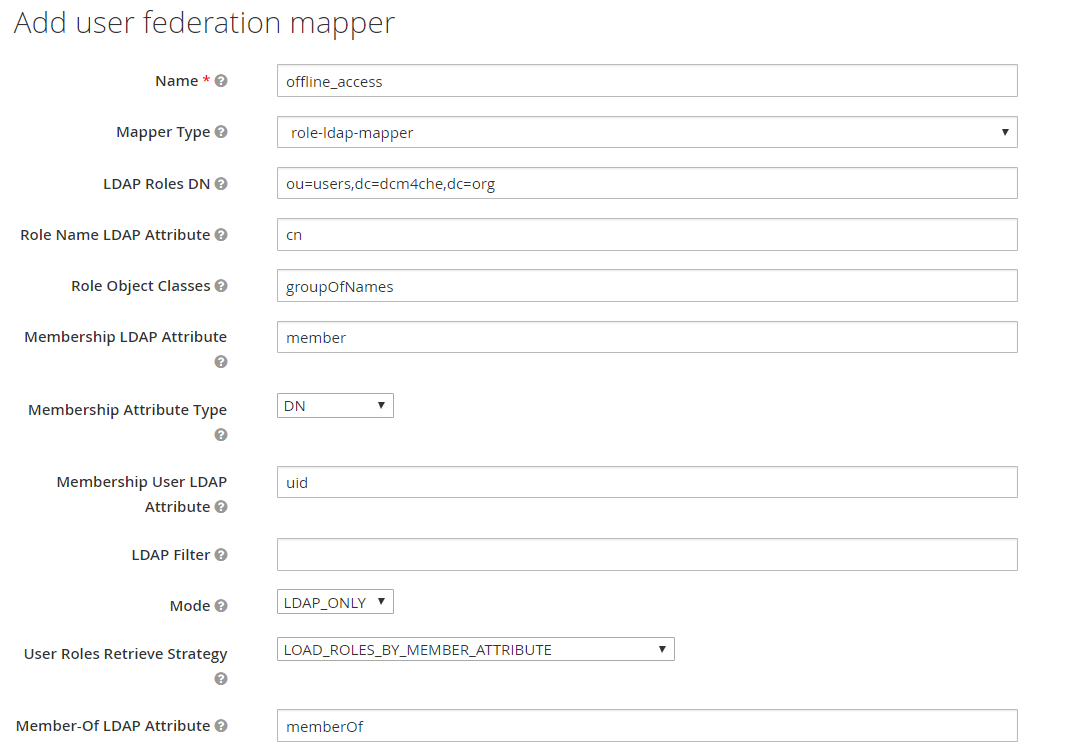




然后去LDAP那里，选择Mappers：

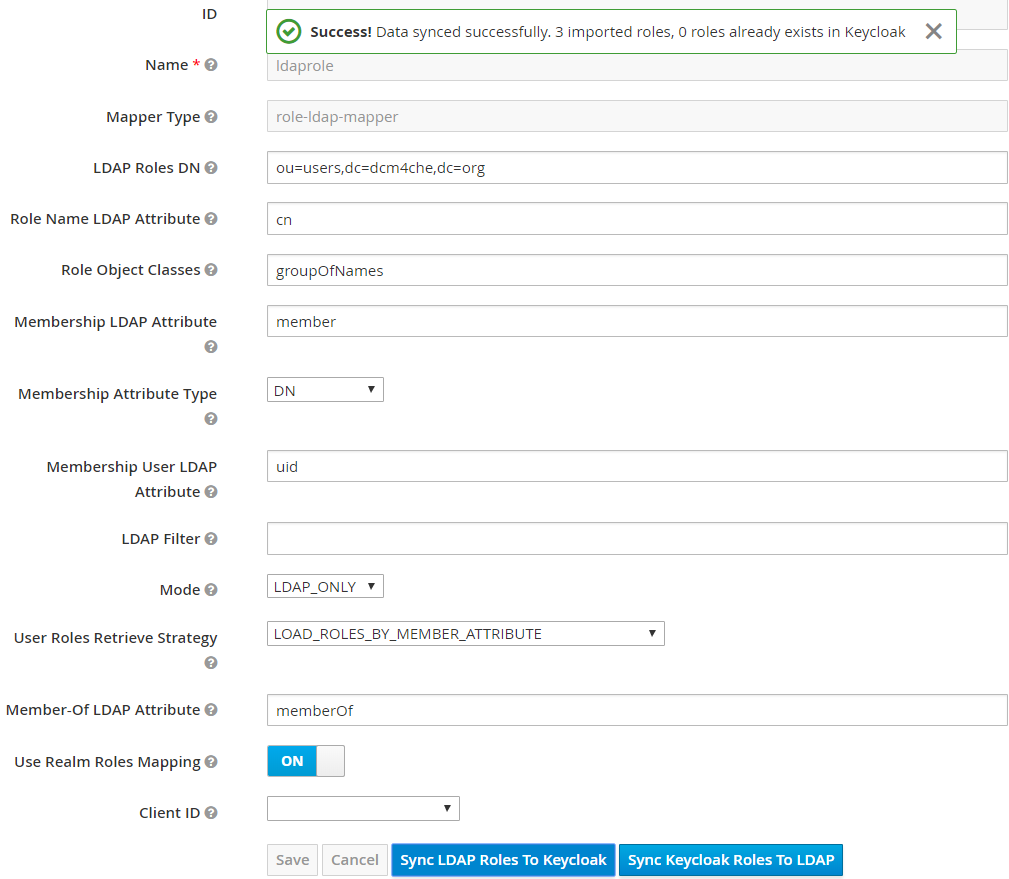


然后选择Create。

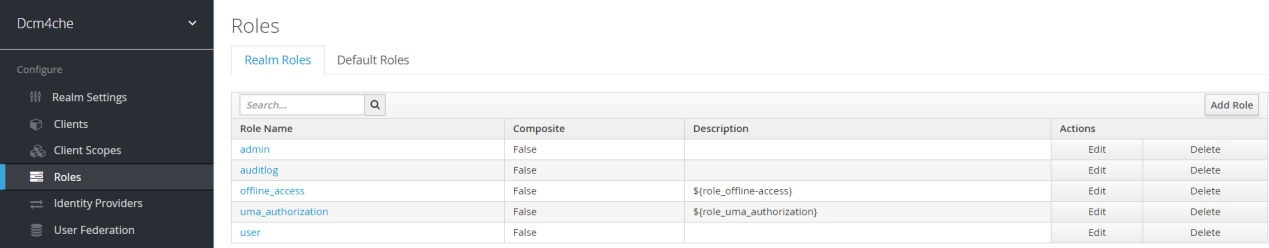
 

Name就自己起一个合适的名字，Mapper Type选择：role-ldap-mapper，LDAP Roles DN则填写：ou=users,dc=dcm4che,dc=org 其它不变。

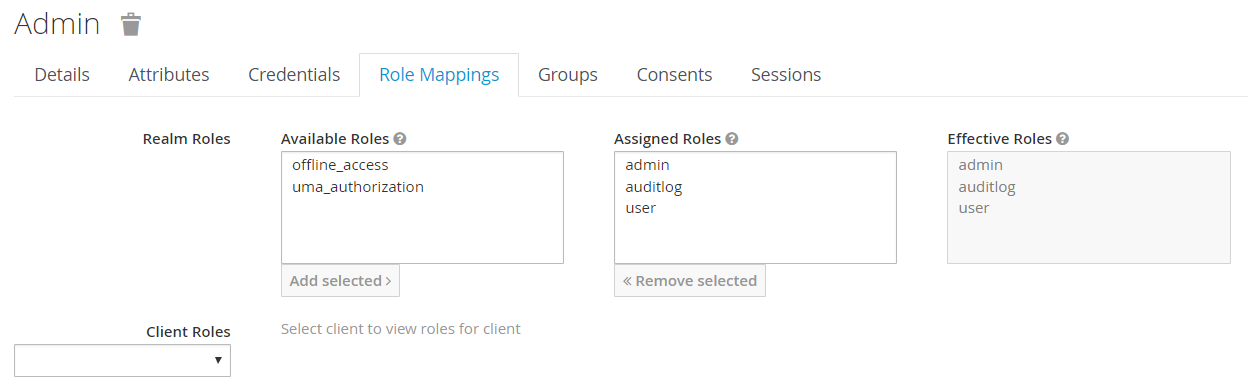
然后点击Sync LDAP Roles to Keycloak，如果成功则如下图所示。

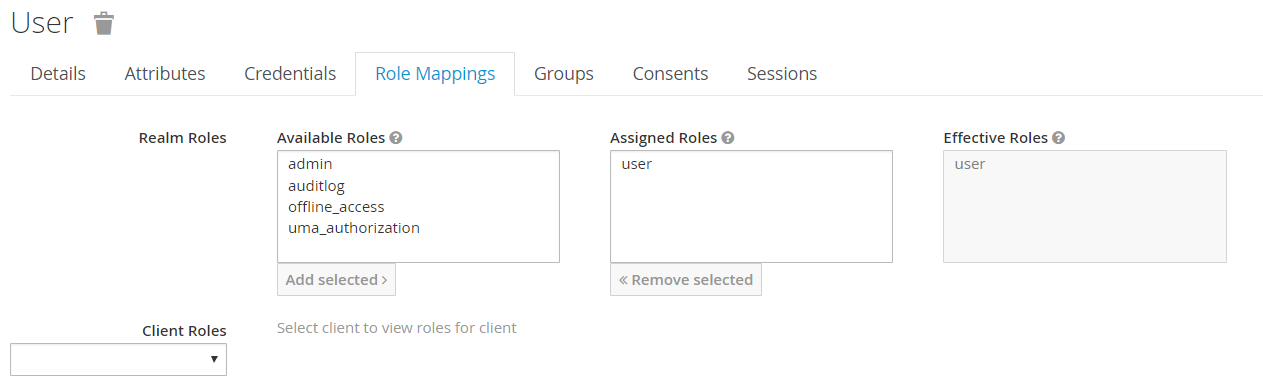


之后到Role那里查看可以看到多了三行(admin,user和auditlog)：



然后查看Users的Role Mappings发生了变动：





如果想让这个admin用户成为Keycloak的管理员用户的话，回到LDAP Mappers那里，点击create，起一个合适的名字，如：realm-management，Mapper Type选择role-ldap-mapper，然后修改以下三项：

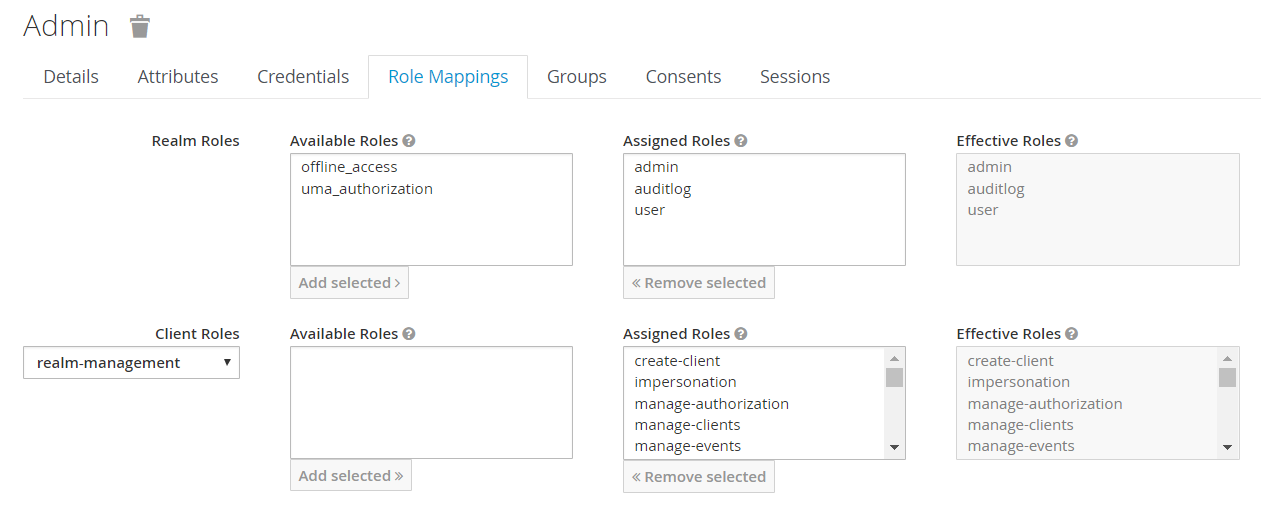
LDAP Roles DN : ou=realm-management,dc=dcm4che,dc=org

Use Realm Roles Mapping : OFF

Client ID : realm-management

其它保持不变，然后保存，再Sync LDAP Roles to Keycloak。

然后可以在Admin用户Role Mappings的页面看到：



多了19个realm-management的roles。

1. 设置Wildfly服务器（不是keycloak的Wildfly）以配置secure dcm4che：

1.

cd $WILDFLY\_HOME

unzip /home/ftpuser/keycloak-wildfly-adapter-dist-6.0.1.zip

cd bin

cp adapter-elytron-install-offline.cli adapter-elytron-install-offline.cli.bak

vi adapter-elytron-install-offline.cli

把--server-config=${server.config:standalone.xml}改成--server-config=${server.config:standalone-full.xml}

[root@localhost bin]# ./jboss-cli.sh --file=adapter-elytron-install-offline.cli

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

{"outcome" => "success"}

2.

cp -r $DCM4CHEE\_ARC/configuration/dcm4chee-arc $WILDFLY\_HOME/standalone/configuration

可能需要修改：/usr/app/wildfly-16.0.0.Final/standalone/configuration/dcm4chee-arc/ldap.properties(dcm4che服务器上)

$KEYCLOAK\_HOME/standalone/configuration/keycloak/ldap.properties(keycloak服务器上)

保证里面的配置和自己配置ldap的时候是一致的。

3.

cd $WILDFLY\_HOME/standalone/configuration/

cp standalone-full.xml dcm4chee-arc.xml

4.

cd $WILDFLY\_HOME/

unzip $DCM4CHEE\_ARC/jboss-modules/dcm4che-jboss-modules-5.17.1.zip

最终需要在同样目录，把$DCM4CHEE\_ARC/jboss-modules/的所有zip都解压到那里，该版本有五个：

dcm4che-jboss-modules-5.17.1.zip jai\_imageio-jboss-modules-1.2-pre-dr-b04.zip jdbc-jboss-modules-1.0.0-mysql.zip

ecs-object-client-jboss-modules-3.0.0.zip jclouds-jboss-modules-2.1.2-noguava.zip

5.

cp /home/ftpuser/mysql-connector-java-5.1.47/mysql-connector-java-5.1.47-bin.jar /usr/app/wildfly-16.0.0.Final/modules/com/mysql/main/

vi /usr/app/wildfly-16.0.0.Final/modules/com/mysql/main/module.xml

修改resource-root path=这一行为刚才拷过去的文件。

6.

vi /usr/app/wildfly-16.0.0.Final/standalone/configuration/dcm4chee-arc.xml

把里面所有的127.0.0.1改成0.0.0.0(这里仅为做测试用，但如果严格安全考虑应该不会那样设置。)

7.

启动dcm4che的Wildfly服务：

$WILDFLY\_HOME/bin/standalone.sh -c dcm4chee-arc.xml

8.

修改add-data-source-mysql.cli文件，让里面内容和自身构建数据库时是一致的：

/subsystem=datasources/jdbc-driver=mysql:add(driver-module-name=com.mysql,driver-name=mysql)

data-source add --name=PacsDS --driver-name=mysql --jndi-name=java:/PacsDS \

--connection-url=jdbc:mysql://localhost:3306/pacsdb \

--user-name=pacsuser --password=123456

$WILDFLY\_HOME/bin/jboss-cli.sh -c --file=/usr/app/wildfly-16.0.0.Final/add-data-source-mysql.cli

{"outcome" => "success"}

10.

$WILDFLY\_HOME/bin/jboss-cli.sh -c --file=$DCM4CHEE\_ARC/cli/add-jms-queues.cli

11.

$WILDFLY\_HOME/bin/jboss-cli.sh -c

加入：

[standalone@localhost:9990 /] /subsystem=ee/managed-executor-service=default:undefine-attribute(name=hung-task-threshold)

[standalone@localhost:9990 /] /subsystem=ee/managed-executor-service=default:write-attribute(name=long-running-tasks,value=true)

[standalone@localhost:9990 /] /subsystem=ee/managed-executor-service=default:write-attribute(name=core-threads,value=2)

[standalone@localhost:9990 /] /subsystem=ee/managed-executor-service=default:write-attribute(name=max-threads,value=100)

[standalone@localhost:9990 /] /subsystem=ee/managed-executor-service=default:write-attribute(name=queue-length,value=0)

[standalone@localhost:9990 /] /subsystem=ee/managed-scheduled-executor-service=default:undefine-attribute(name=hung-task-threshold)

[standalone@localhost:9990 /] /subsystem=ee/managed-scheduled-executor-service=default:write-attribute(name=long-running-tasks,value=true)

[standalone@localhost:9990 /] /subsystem=ee/managed-scheduled-executor-service=default:write-attribute(name=core-threads,value=2)

12.

由于要使用keycloak，还要在dcm4che的wildfly的console加入：

[standalone@localhost:9990 /] /system-property=super-user-role:add(value=admin)

[standalone@localhost:9990 /] /system-property=realm-name:add(value=dcm4che)

[standalone@localhost:9990 /] /system-property=auth-server-url:add(value=http://192.168.15.31:8080/auth)

注：需要和设置的keycloak一致。

13. 在DCM4CHEE Archive's Wildfly的console加入：

/subsystem=keycloak/secure-deployment=dcm4chee-arc-ui2-5.17.1-secure.war/:add(realm=dcm4che,resource=dcm4chee-arc-ui,auth-server-url=http://192.168.15.31:8080/auth,ssl-required=external,public-client=true)

/subsystem=keycloak/secure-deployment=dcm4chee-arc-war-5.17.1-secure.war/:add(realm=dcm4che,resource=dcm4chee-arc-rs,auth-server-url=http://192.168.15.31:8080/auth,ssl-required=external,bearer-only=true)

成功则返回：

{

"outcome" => "success",

"response-headers" => {"process-state" => "reload-required"}

}

14.

先启动ldap服务器：

/usr/app/openldap-2.4.47/libexec/slapd -h "ldap:/// ldapi:///"

最终部署：

[standalone@localhost:9990 /] deploy /usr/app/dcm4chee-arc-5.17.1-mysql-secure/deploy/dcm4chee-arc-ear-5.17.1-mysql-secure.ear

成功则返回：

18:31:25,202 INFO [org.hibernate.hql.internal.QueryTranslatorFactoryInitiator] (ServerService Thread Pool -- 102) HHH000397: Using ASTQueryTranslatorFactory

18:31:27,408 INFO [io.smallrye.metrics] (MSC service thread 1-2) MicroProfile: Metrics activated

18:31:31,596 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 102) WFLYUT0021: Registered web context: '/dcm4chee-arc/xsl' for server 'default-server'

18:31:32,196 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 134) WFLYUT0021: Registered web context: '/dcm4chee-arc/xdsi' for server 'default-server'

18:31:33,606 WARN [io.undertow.servlet] (ServerService Thread Pool -- 139) UT015020: Path /\* is secured for some HTTP methods, however it is not secured for [OPTIONS]

18:31:33,608 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 139) WFLYUT0021: Registered web context: '/dcm4chee-arc' for server 'default-server'

18:31:33,624 INFO [org.wildfly.extension.undertow] (ServerService Thread Pool -- 143) WFLYUT0021: Registered web context: '/dcm4chee-arc/ui2' for server 'default-server'

18:31:37,169 INFO [org.opencv.osgi] (ServerService Thread Pool -- 147) Successfully loaded OpenCV native library.

18:31:38,311 INFO [org.dcm4che3.net.Connection] (ServerService Thread Pool -- 147) No TCP Protocol Handler for protocol HTTP

18:31:38,368 INFO [org.dcm4che3.net.Connection] (EE-ManagedExecutorService-default-Thread-2) Start TCP Listener on /0.0.0.0:11112

18:31:38,364 INFO [org.dcm4che3.net.Connection] (EE-ManagedExecutorService-default-Thread-1) Start TCP Listener on /0.0.0.0:2575

18:31:39,491 INFO [org.jboss.as.server] (management-handler-thread - 1) WFLYSRV0010: Deployed "dcm4chee-arc-ear-5.17.1-mysql-secure.ear" (runtime-name : "dcm4chee-arc-ear-5.17.1-mysql-secure.ear")

1. 进行测试：

1.如果没有开启keycloak服务器，直接登录dcm4che的PACS页面(http://192.168.15.32:8080/dcm4chee-arc/ui2)，会报错。

地址会跳转到(192.168.15.31:8080是keycloak服务器的地址和端口)：

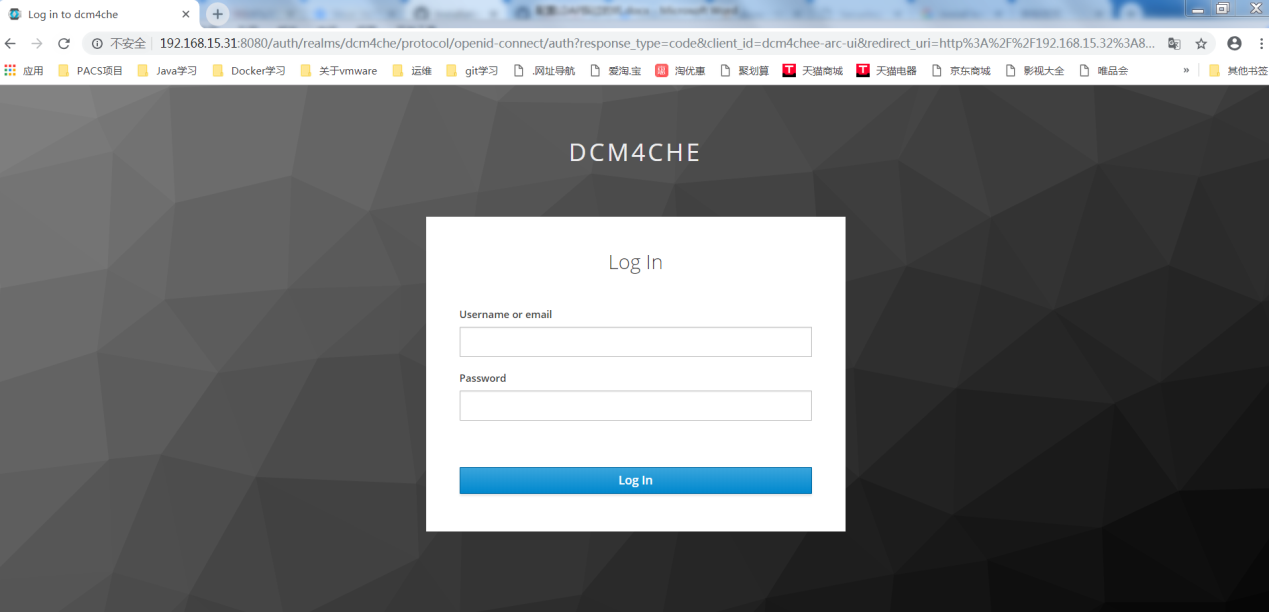
<http://192.168.15.31:8080/auth/realms/dcm4che/protocol/openid-connect/auth?response_type=code&client_id=dcm4chee-arc-ui&redirect_uri=http%3A%2F%2F192.168.15.32%3A8080%2Fdcm4chee-arc%2Fui2%2F&state=8fcd2ac7-08f2-4590-acbb-855558c1ac8f&login=true&scope=openid>

2.启动keycloak服务器：

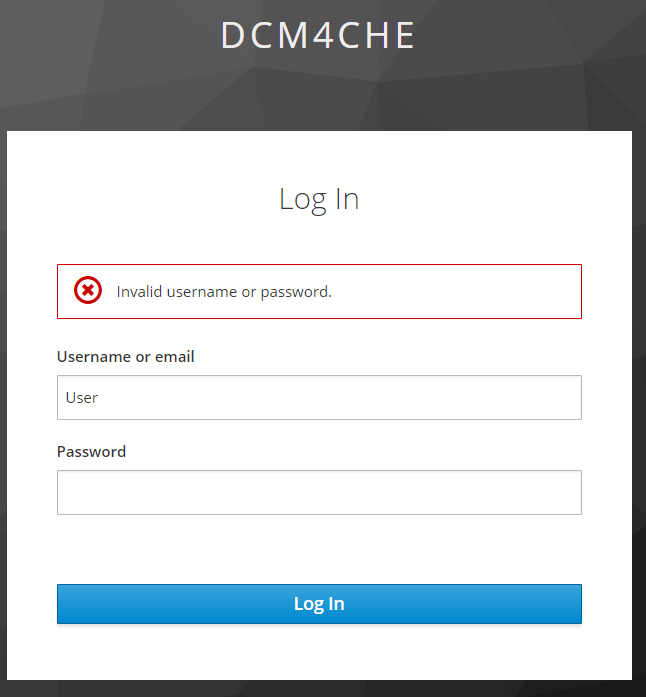
[root@keycloakserver keycloak]# /usr/app/keycloak-6.0.1/bin/standalone.sh

3.在浏览器输入<http://192.168.15.32:8080/dcm4chee-arc/ui2>

发现被跳转到以下页面：



如果输入了错误的用户名和密码，是不能进去的：

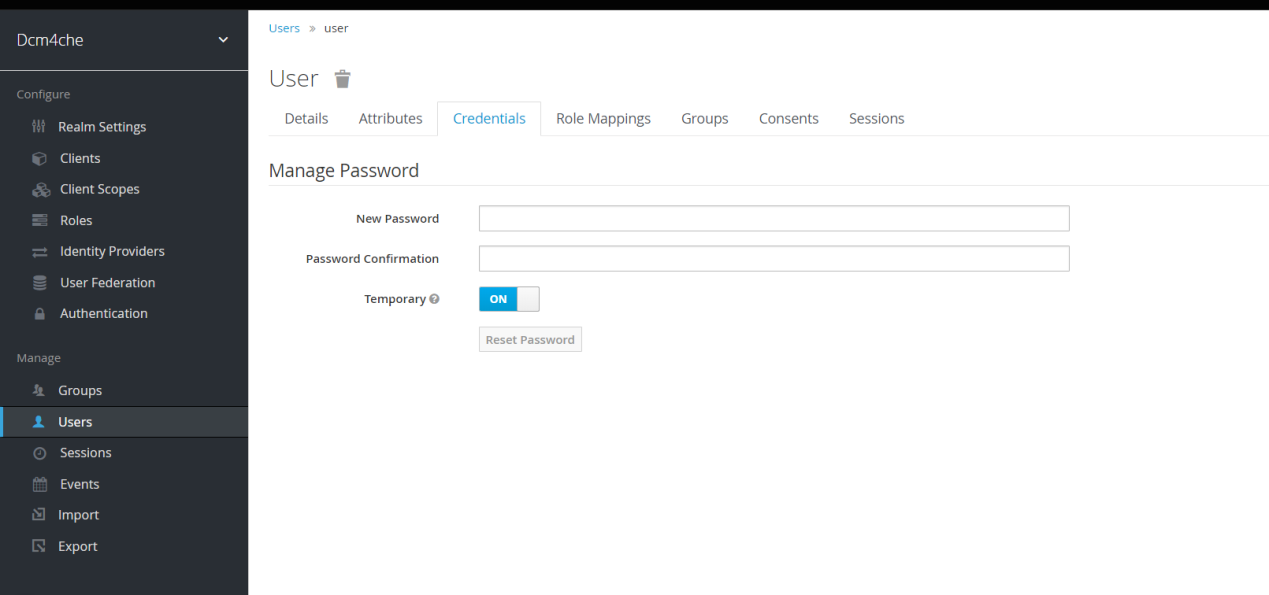


如果输入的是keycloak管理员的用户名和密码，会返回：



4.以管理员的身份登录keycloak服务器<http://192.168.15.31:8080>。

修改User用户的密码：



再尝试登录，然而返回Forbidden。

在Keycloak服务器返回：

10:48:02,731 WARN [org.keycloak.events] (default task-12) type=LOGIN\_ERROR, realmId=dcm4che, clientId=dcm4chee-arc-ui, userId=14056287-65f3-43f2-958a-34777741e085, ipAddress=192.168.15.177, error=invalid\_user\_credentials, auth\_method=openid-connect, auth\_type=code, redirect\_uri=http://192.168.15.32:8080/dcm4chee-arc/ui2/, code\_id=2990eb61-ff88-452a-9585-a94a24ffffd4, username=User

在Dcm4che Wildfly服务器返回：

18:53:42,450 ERROR [org.keycloak.adapters.OAuthRequestAuthenticator] (default task-1) failed verification of token: Token is not active

解决办法：

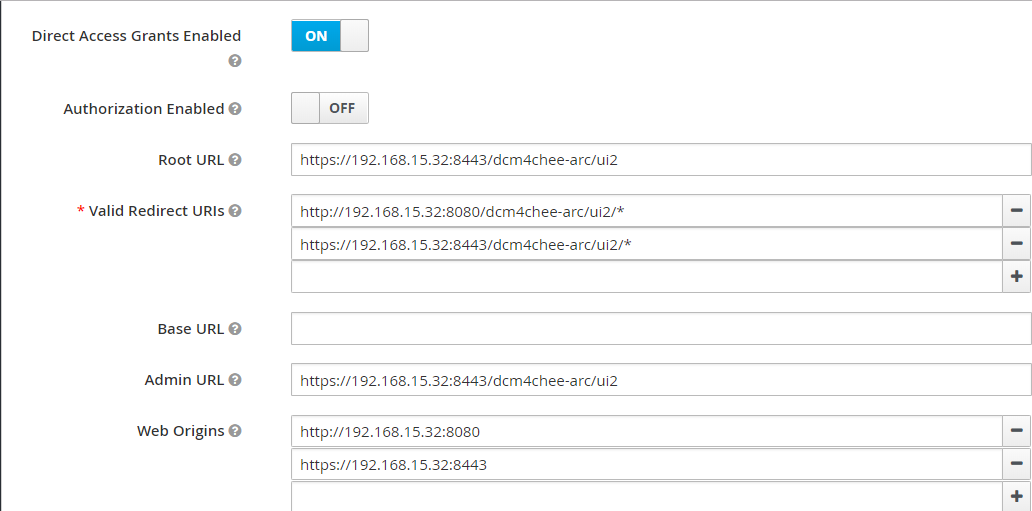
Keycloak服务器和Dcm4che Wildfly服务器的时间需要同步。

5.

之后成功登录PACS，然而点击什么都没有反应和其它显示，还是原来的页面。

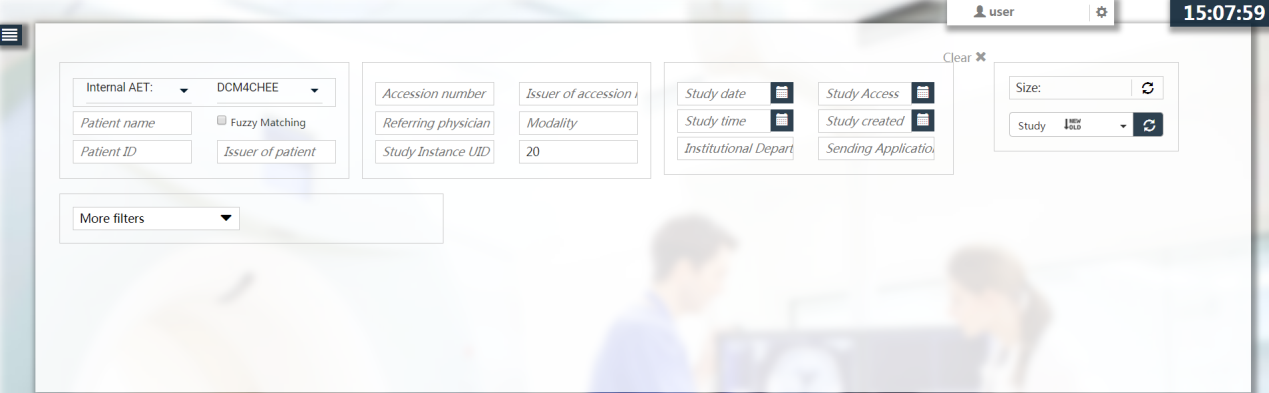
解决办法：

在keycloak服务器添加：

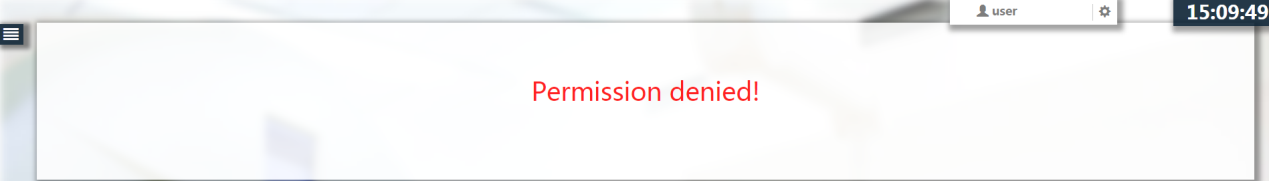


在Web Origins把<http://192.168.15.32:8080>添加进去。

如果用User作为用户登录，则只能看到Study：



Monitoring和Configuration都是”Permission Denied”的：



如果是admin作为用户登录，则都可以看到：

