Adding Custom Attributes to User Schema

1. Import Directory service certificate to JDK

* Export the Directory service certificate

echo "" | openssl s\_client -connect localhost:50636 -showcerts | openssl x509 -out D:\certfile.txt

* Import the Directory certificate to JDK

keytool -importcert -alias server-cert -file <certificate path>certfile.txt -trustcacerts -keystore "<JAVA\_HOME path>\lib\security\cacerts" -storetype JKS

keytool -importcert -alias server-cert -file D:\certfile.txt -trustcacerts -keystore "C:\Program Files\Java\jdk-11.0.15\lib\security\cacerts" -storetype JKS

1. Set JAVA environment for SSL - Add to end of tomcat/bin/setenv.sh file like below

export CATALINA\_OPTS="$CATALINA\_OPTS

-Djavax.net.ssl.trustStore=/usr/lib/jvm/jdk-11/lib/security/cacerts \

-Djavax.net.ssl.trustStorePassword=changeit \

-Djavax.net.ssl.trustStoreType=jks"

\*\* where /usr/lib/jvm/jdk-11/lib/security/cacerts is path to jdk cacerts file

\*\* where “changeit” is the default password for java cacerts file

1. Add a Custom Attribute to Directory Services/LDAP

* Create a custom attribute ldif file - “custom-attribute.ldif”

Example content for this file -

dn: cn=schema

changetype: modify

add: attributeTypes

attributeTypes: ( temp-custom-attr-oid NAME 'customAttribute' EQUALITY case

IgnoreMatch ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstrings

Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )

-

add: objectClasses

objectClasses: ( temp-custom-oc-oid NAME 'customObjectclass' SUP top AUXILIARY

MAY customAttribute )

* Add custom attribute (Modify LDAP)

ldapmodify.bat --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword <amadmin Paasowrd> "<path to your ldif file>\custome-attribute.ldif"

Example - *ldapmodify.bat --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword 12345678 "C:\tomcat\webapps\openam\WEB-INF\template\ldif\custom\custome-attribute.ldif"*

Once run the command the attribute will be added.

1. Add the custom attribute to Open AM Identity store

* In the AM console, browse to Realms > Realm Name > Identity Stores > Identity Store Name > User Configuration.
* Add the object class, for example customObjectclass, to the LDAP User Object Class list.
* Add the attribute type, for example customAttribute, to the LDAP User Attributes list.
* Save your work.
* Add the attribute type to the profile attribute whitelist.

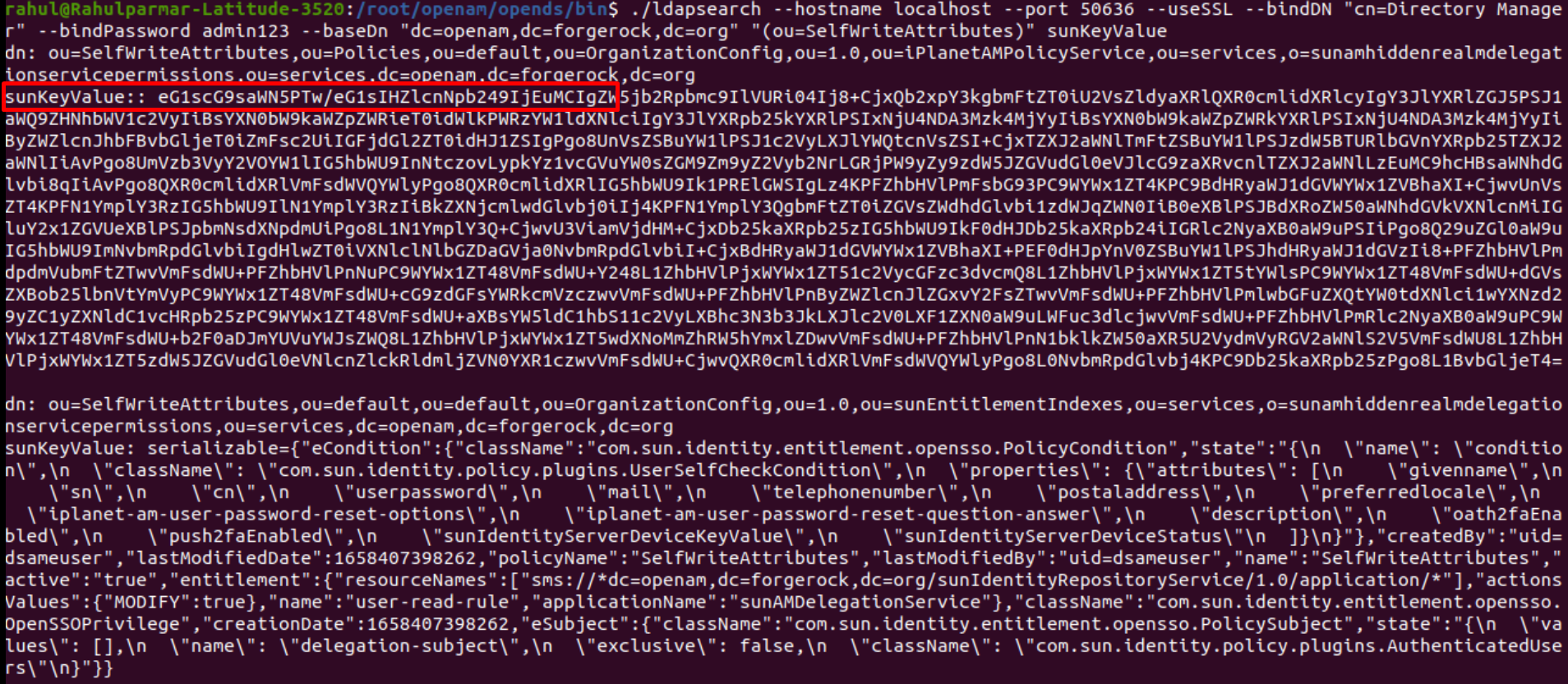
Globally: Navigate to Configure > Global Services > User Self-Service > Profile Management, and edit the Self readable attributes field.

1. Allow Users to Update the New Attribute Using the Command Line

* Search for the value of sunKeyValue in ou=SelfWriteAttributes by running the following command:

ldapsearch --hostname localhost --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword <amadmin Paasowrd> --baseDn "dc=openam,dc=forgerock,dc=org" "(ou=SelfWriteAttributes)" sunKeyValue

Copy the encrypted code after the field “sunKeyValue” and decode it with the below command



* Decode the base64 string of the iPlanetAMPolicyService DN. For example:

base64 decode --encodedData eG1scG9saWN5PTw/eG1sIHZlcnNpb249IjEuMCIgZW5 ….

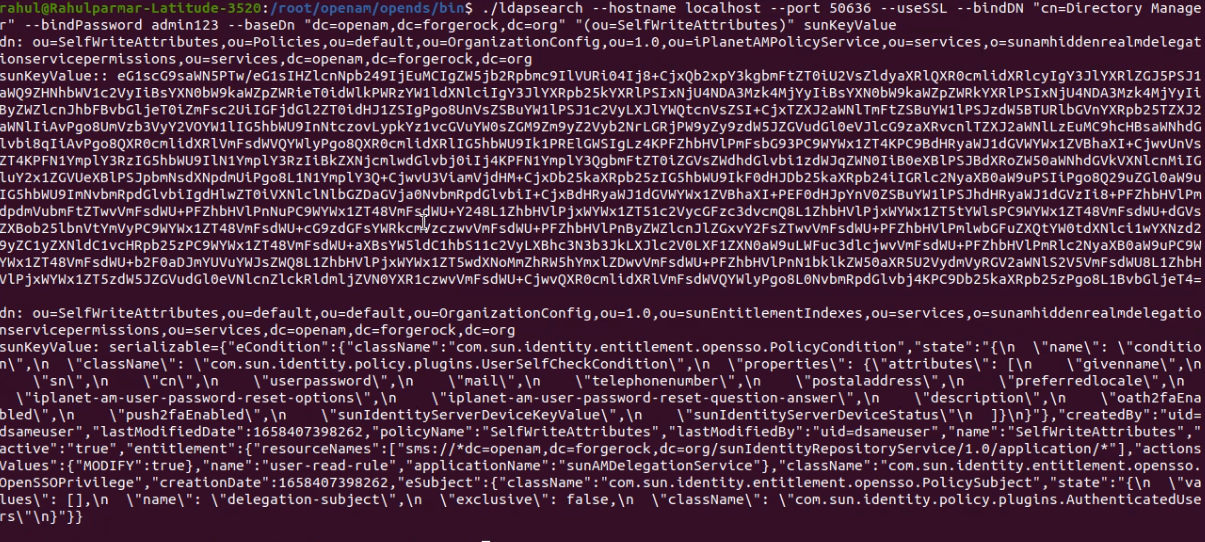


* Create a file with the decoded string. Then, add the custom attribute to the <AttributeValuePair> list. For example to-encode.xml
* Encrypt the xml file back to base 64 string

base64 encode -f "<path of the xml file>\to-encode.xml"

* Copy the resulted base64 encrypted data
* Run the ldapsearch command one more time -

ldapsearch --hostname localhost --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword <amadmin pass> --baseDn "dc=openam,dc=forgerock,dc=org" "(ou=SelfWriteAttributes)" sunKeyValue



* Copy the resulted output and create a ldif file :- “change.ldif”

Add two extra parameters as shown below

* Replace the base64 string with the new generated base64 string above
* Add the custom attribute to the attribute list in the sunKeyValue of the second part
* Add the two extra parameters in both the parts

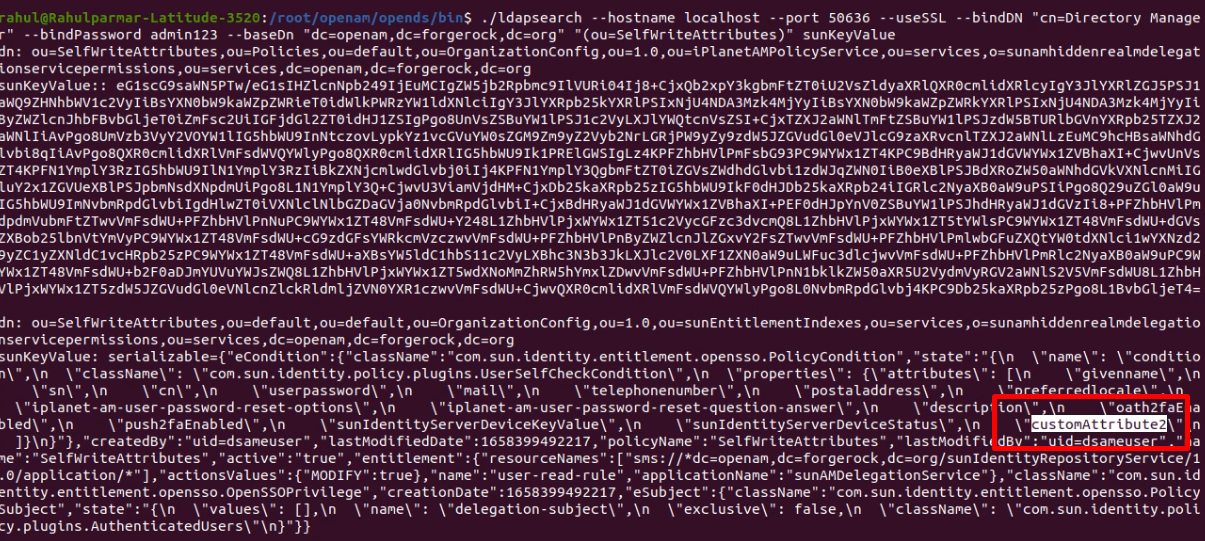


* Apply the changes in the LDIF file to the LDAP configuration store, as follows:

./ldapmodify --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword <amadmin pass> “path/to/change.ldif”

* Run ladap search one more time to verify if the new custom attribute is updated.

ldapsearch --hostname localhost --port 50636 --useSSL --bindDN "cn=Directory Manager" --bindPassword <amadmin pass> --baseDn "dc=openam,dc=forgerock,dc=org" "(ou=SelfWriteAttributes)" sunKeyValue



1. Update the amUser.xml file (located in tomcat/webapps/openam/classes)

* Add the new attribute tag under the <user></user> tag



1. Restart the Open AM. (restart the tomcat server).
2. Now you will see the new user Attribute in the identities -