AttributeManagementPilot

Introduction

The purpose of the demonstrator is to show with a practical implementation how group membership attributes or other attributes from multiple sources can be used in a federated environment to regulate access to services.

The use of COmanage, as an attribute source, for managing the users' attributes allows to regulate the authorization on services based on externally provided attributes. Such a service can be entirely managed by the research community, independently from service providers or identity providers. It simplifies the configuration at both the service provider and attribute authority level.

Detailed description

A detailed description can be found in this wiki page.

The setup consist of:

- an IdP proxy based on SimpleSAMLphp
- a COmanage server (configured as service provider) as aggregation service
- a cloud framework (OpenStack) as service provider.

For the purpose of this pilot, we have enabled federated access to the dashboard of a demo OpenStack Cloud deployment and we are using a set of dummy users registered in the testbed IdP. Specifically, the pilot IdP proxy has been configured to authenticate users and communicate the result of the authentication to an OpenStack's Identity service (Keystone) using SAML assertions. Before passing the authentication results to OpenStack, the pilot IdP proxy contacts a COmanage instance, on which some collaborations (COs) have been created that have a corresponding project in OpenStack for the mapping of users: it attaches additional entitlement regarding the user's membership of the COs to the SAML assertion. At this point the new SAML assertion is passed to OpenStack and it is mapped to keystone user groups, based on which, the authenticated user can access cloud resources using his /her federated ID.

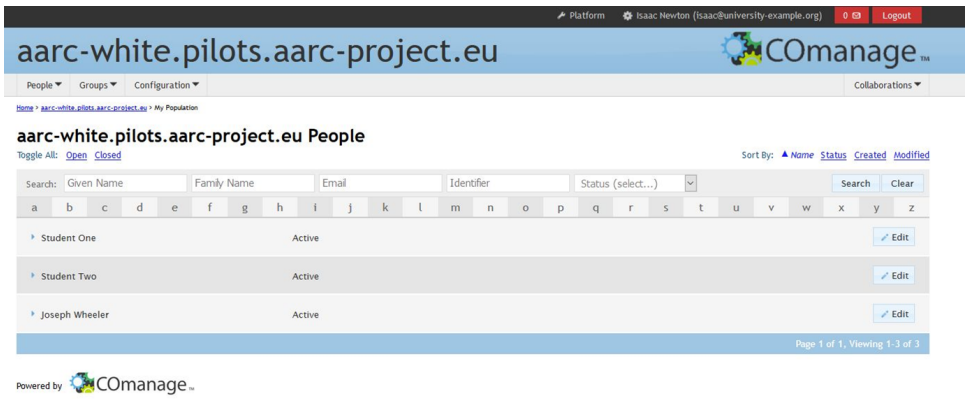
There was no need to create local accounts on the cloud framework, ephemeral users are used instead: we created a set of mapping rules that, depending on the entitlements provided by COmanage (managing COs and groups with users having specific rules in the CO), associate the external users to the right group defined into openstack, after which each of them can access a particular OpenStack project with different user rights (either admin or simple user).

Demonstration workflow

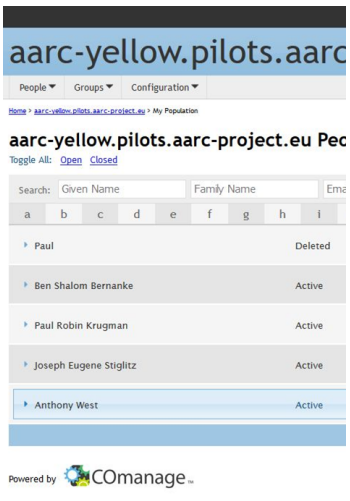
The research collaborations on COmanage

a) some research collaborations who want to access OpenStack services were created on a COmanage instance. In our case:

aarc-white.pilots.aarc-project.eu

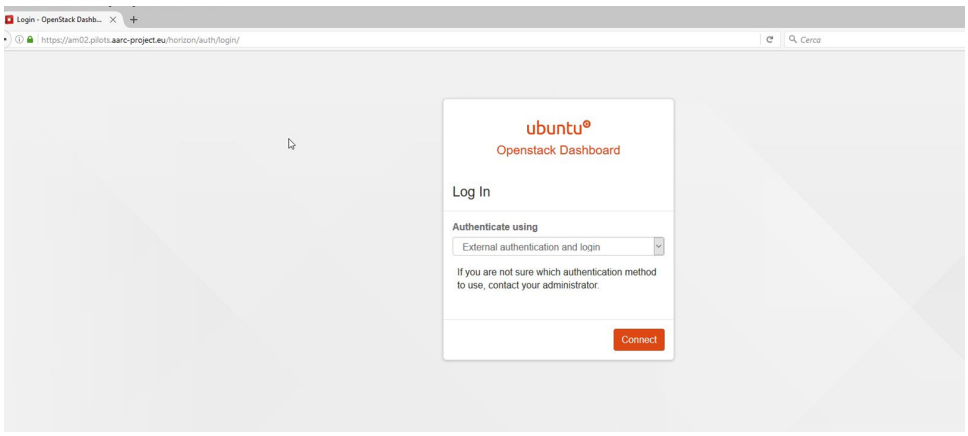
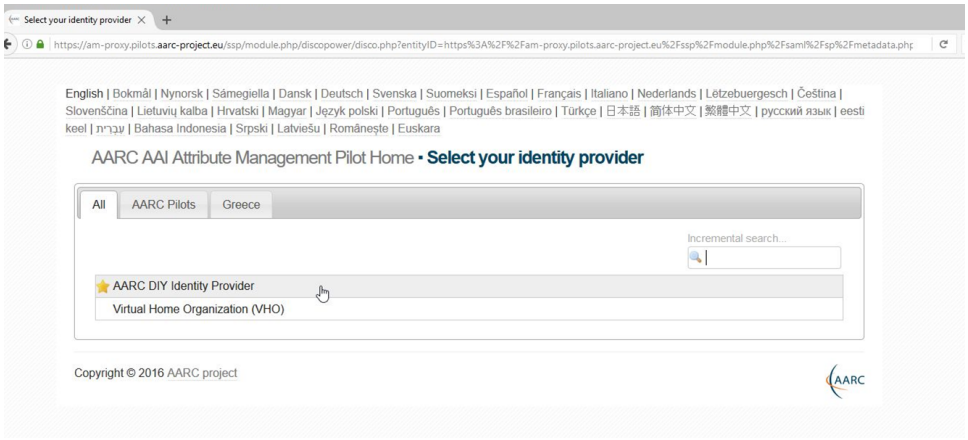
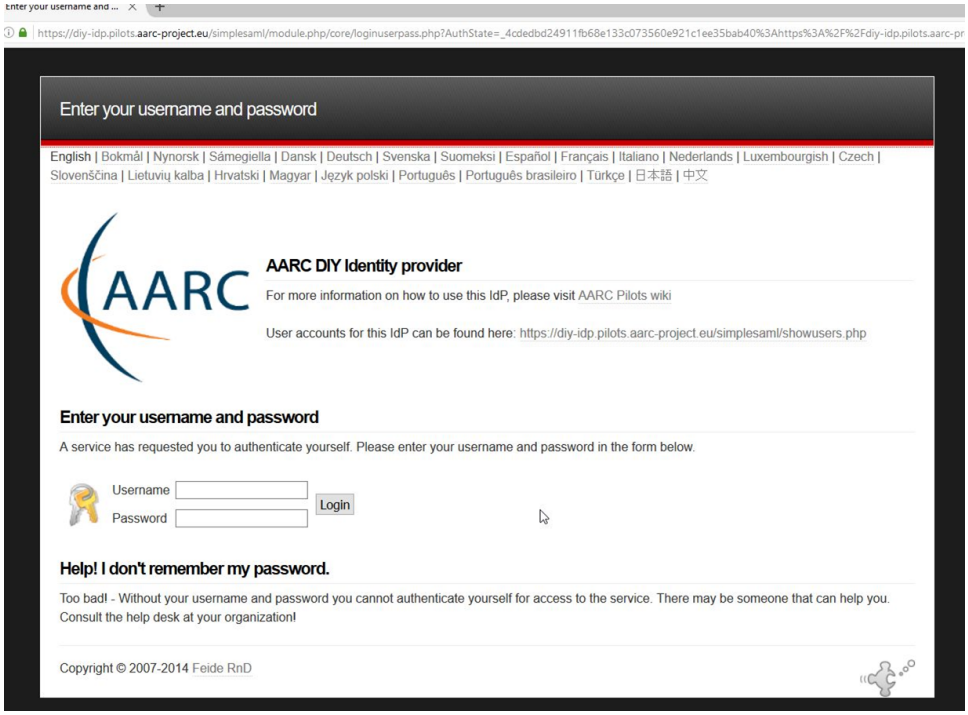


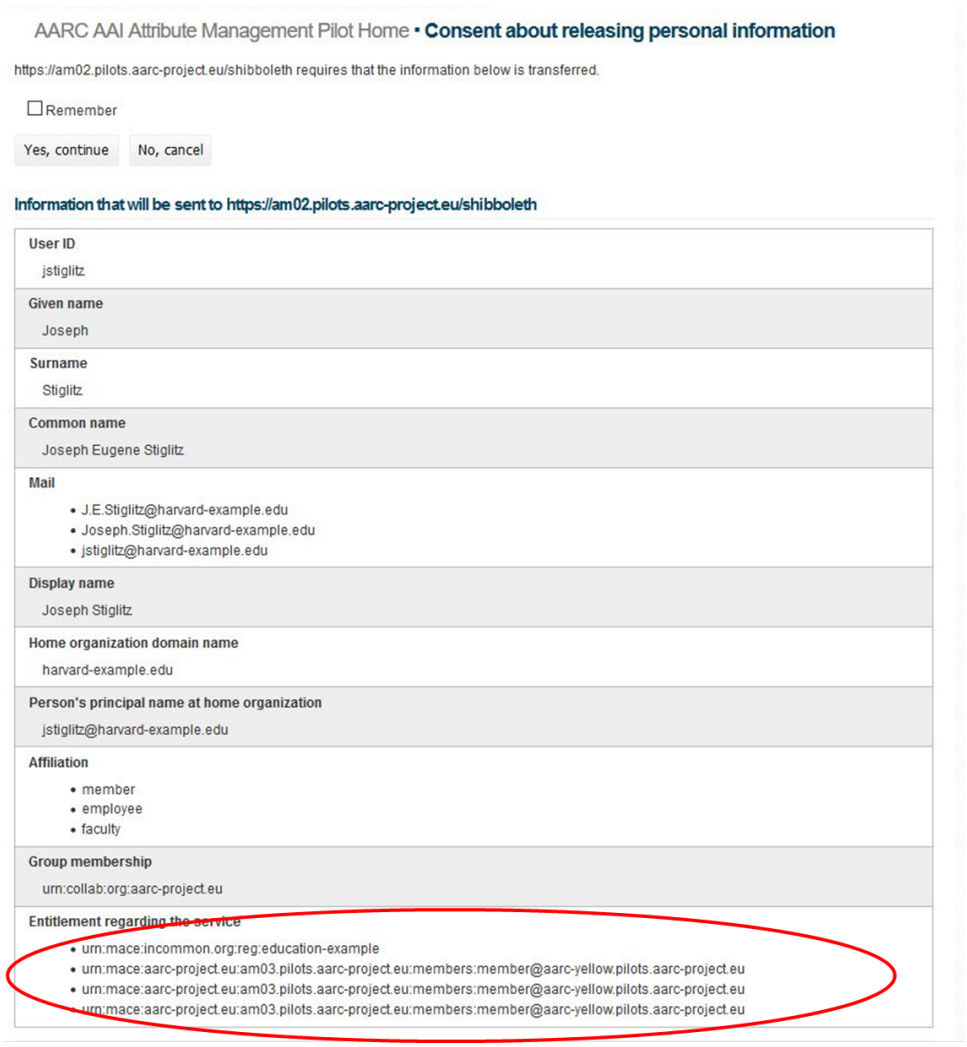
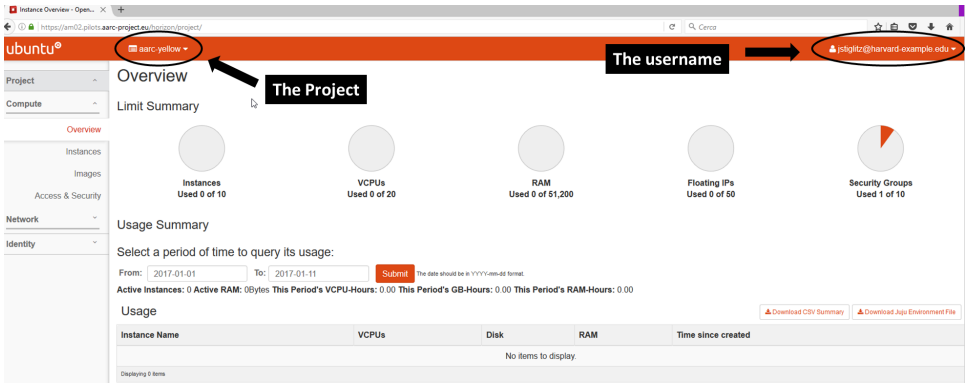
aarc-yellow.pilots.aarc-project.eu

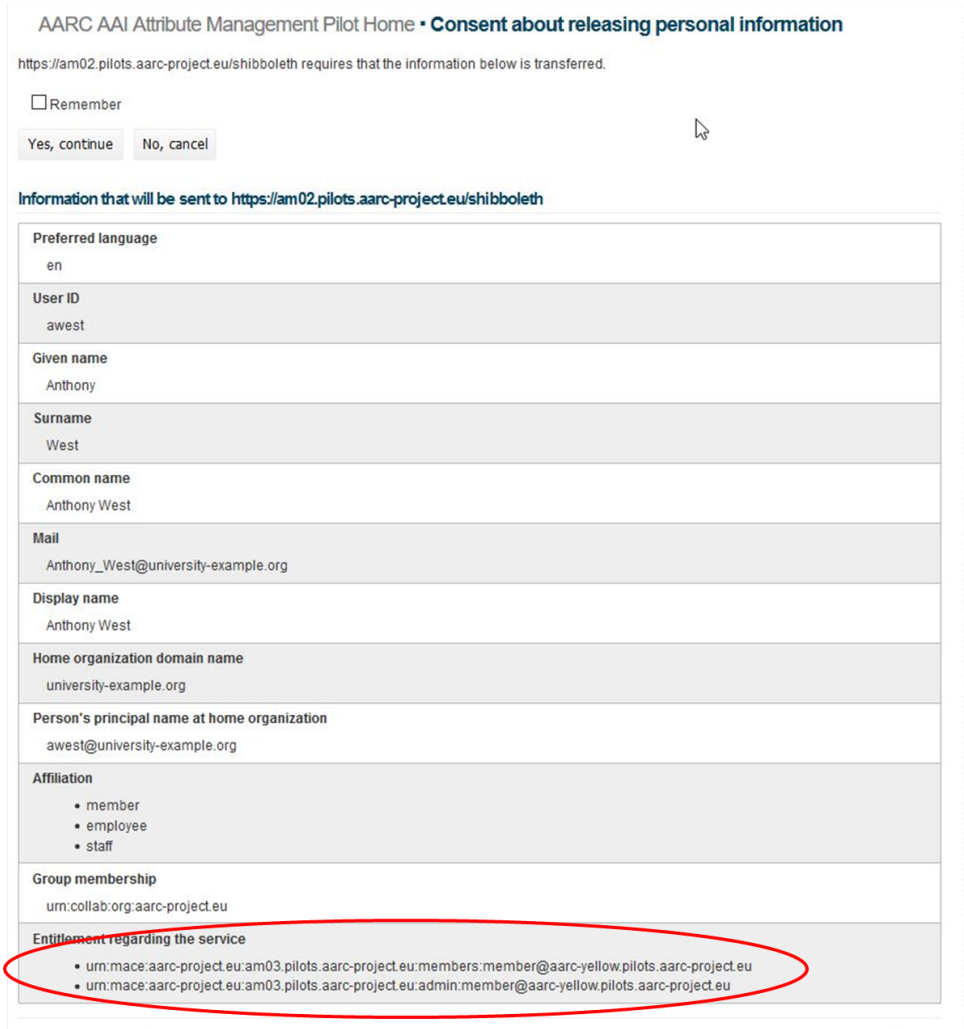
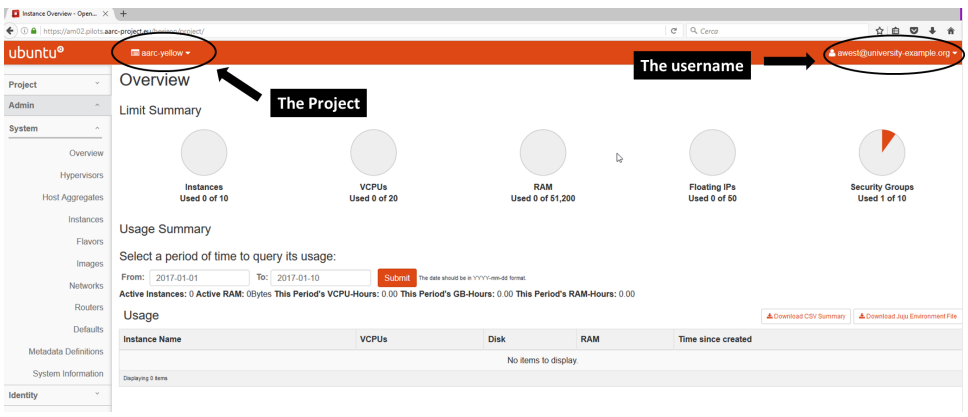


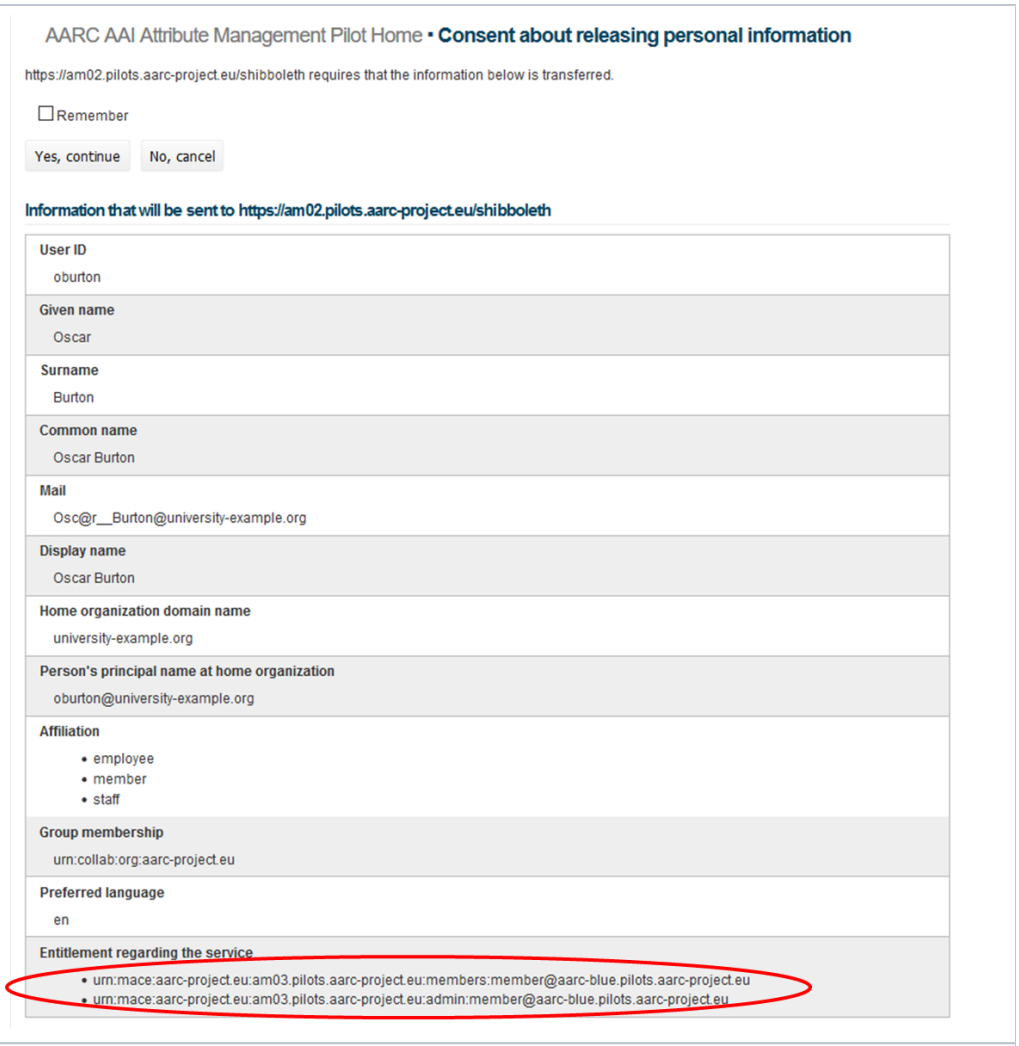
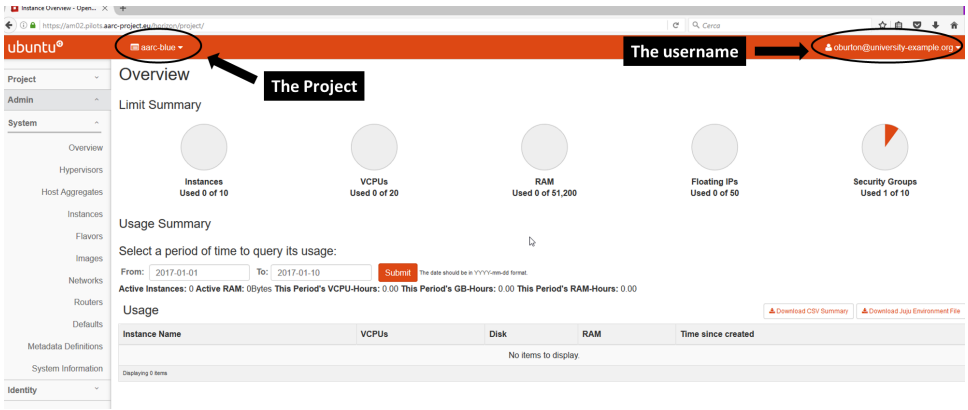
b) Each CO has got an admin who approves the membership requests and several users registered

c) Each CO has got a corresponding project into OpenStack, reserved to its members

Access to the cloud resources		
1.	Access OpenStack's Dashboard (Horizon) Select "External authentication and login" and click on "Connect".	
2.	Select your Identity Provider from the discovery page (WAYF). The institutional IdP to select (considered for demo purposes only) is: **AARC DIY Identity Provider**	
3.	Enter your login credentials to authenticate yourself with the IdP of your Home Organisation. We will show three cases: a) an user belonging to aarc-yellow CO with admin role b) an user belonging to aarc-yellow CO with no particular roles c) an user belonging to aarc-blue CO with admin role	

4 b.	-- member of aarc-yellow CO without any priviledged role -- After successful authentication, the user needs to give the consent for releasing your personal information to the Service Provider mentioned in the page (the OpenStack framework in our case). Among the data that will be passed to the Service Provider, there are the Entitlements released by the attribute authority COmanage regarding the ownership in the COs and the roles. In this case the Entitlement contains this piece of information: ***urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:members:member@aarc-yellow.pilots.aarc-project.eu*** That is the piece of information used for properly mapping the users to the OpenStack projects. Click on "yes" for going on.	
5 b.	The user is successfuly redirected to the OpenStack Dashboard, mapped to a Keystone user group based on the values of the Entitlement attribute, with the eppn as username. In this case the user is accessing the aarc-yellow project with the rights for a "regular user" (no administrative rights).	

4 a.	-- user belonging to aarc-yellow CO and with admin role -- After successful authentication, the user needs to give the consent for releasing your personal information to the Service Provider mentioned in the page (the OpenStack framework in our case). Among the data that will be passed to the Service Provider, there are the Entitlements released by the attribute authority COmanage regarding the ownership in the COs and the roles. In this case the Entitlement contains these pieces of information: ***urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:members:member@aarc-yellow.pilots.aarc-project.eu*** ***urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:admin:member@aarc-yellow.pilots.aarc-project.eu*** That is the piece of information used for properly mapping the users to the OpenStack projects. Click on "yes" for going on.	
5 a.	The user is successfuly redirected to the OpenStack Dashboard, mapped to a Keystone user group based on the values of the Entitlement attribute, with the eppn as username. In this case the user is accessing to the aarc-yellow project with administrative rights.	

4 c.	-- user belonging to aarc-blue CO and with admin role -- After successful authentication, the user needs to give consent for releasing personal information to the Service Provider mentioned in the page (the OpenStack framework in our case). Among the data that will be passed to the Service Provider, there are the Entitlements released by the attribute aggregatore COmanage regarding the ownership in the COs and the roles. In this case the Entitlement contain these pieces of information: ***urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:members:member@aarc-blue.pilots.aarc-project.eu*** ***urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:admin:member@aarc-blue.pilots.aarc-project.eu*** That is the piece of information used for properly mapping the users to the OpenStack projects. Click on "yes" for going on.	
5 c.	The user is successfuly redirected to the OpenStack Dashboard, mapped to a Keystone user group based on the values of the Entitlement attribute, with the eppn as username.. In this case the user is accessing the aarc-blue project with administrative rights.	

Mapping rules: an example

{
"local": [
{
"user": {
"name": "{0}"
}
},
{
"group": {
"id": "3b609a4da6654625a3789d1a6bd1fdc7"
}
}
],
"remote": [
{
"type": "eppn"
},
{
"type": "entitlement",
"any_one_of": [
"urn:mace:aarc-project.eu:am03.pilots.aarc-project.eu:admin:member@aarc-blue.pilots.aarc-project.eu"
]
}
]
},
	The mapping rules are passed in Keystone as a json file. Each set of rules is made of a local and a remote section.
	
	In the remote part it is specified the external attributes to take into account and that we want to map to the local ones, following the order in which they are listed.
	
	In our case, as local username, it will be used the eppn, and any SAML assertion presenting that particular value in the entitlement attribute will be mapped to the local group qith that particular ID.