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:

🌶 Platform 🛭 🏘 Isaac I	wwton (isaar@university.example.org)			
	terror (source and even preven			
arc-project.eu	🥻 COmanage 🛛 🖉	aarc-yellow.pilots.aa		
	Collaborations 🕶	People ▼ Groups ▼ Configuration ▼		
		Home > aarc-vellow.pilots.aarc-project.eu > My Population		
People	Sort By: A Name Status Created Modified	aarc-yellow.pilots.aarc-project.eu		
Email Identifier Status (select)	v Search Clear	search: Given Name Family Name		
i j k l m n o p q r	s t u v w x y z	a b c d e f g h		
ctive	✓ Edit	Paul Dele		
ctive	✓ Edit	Ben Shalom Bernanke Activ		
tive	🖌 Edit	Paul Robin Krugman Activ		
	Page 1 of 1, Viewing 1-3 of 3	Joseph Eugene Stiglitz Activ		
		Anthony West Activ		
		Powered by 🍓 COmanage		
	rc-project.eu People Imai Identifier Status (select) i j k t m n o p q r tive tive tive	Image: State of the state		

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

A	Access to the cloud resources							
1.	Access OpenStack's Dashboard (Horizon)	I togin- Operated Danka. X + 0 ● Intro://wr/info2.piots.aarc.project.eu/horizon/wr/infojin/						
	Select "External authentication and login" and click on "Connect".	be buttue openstack Dashboard Denstack Dashboard Log In attenticate using External authentication method to use, contact your administrator. 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	Steds your identity provider Y Image: Steds your identity provider Steds your identity provider Image: Steds your identity provider Image: Steds your identity provider Image: Steds your identity provider Steds your identity your identity provider Steds your identity your identity provider Steds your identity your identity your identity your identity your identy your identity your identi						
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	Integration and the set of the production productin production production production pr						

4 b.	member of aarc-yellow CO without any priviledged role	AARC AAI Attribute Management Pilot Home • Consent about releasing personal information						
		https://am02.pilots.aarc-project.eu/shibboleth requires that the information below is transferred.						
	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).	Remember						
		Yes, continue No, cancel						
		Information that will be sent to https://am02.pilots.aarc-project.eu/shibboleth						
		User ID						
	Among the data that will be	jstiglitz						
	passed to the Service Provider, there are the Entitlements released by the attribute authority COmanage regarding the ownership in the COs and the roles.	Given name						
		Joseph						
		Surname						
		Stightz						
		Common name						
	In this case the Entitlement contains this piece of							
	information:	J.E.Stiglitz@harvard-example.edu						
		Joseph.Stiglitz@harvard-example.edu						
	am03.pilots.aarc-project.eu:	• jstiglitz@narvaro-example.edu						
	members:member@aarc-	Uispiay name						
	yellow.pilots.aarc-project.eu	Juseph Sugniz						
	That is the piece of information	harvard-example.edu						
	used for properly mapping the	Person's principal name at home organization						
	users to the OpenStack	jstiglitz@harvard-example.edu						
	p.0j00.0.	Affiliation						
	Click on "yes" for going on.	• member						
		employee faculty						
		Group membership						
		um:collab:org:aarc-project.eu						
		Entitlement regarding the service						
		umimace:incommon.org:reg:education-example umimace:asc-project au:pmm/acc-pare-pailore.asc-project au						
	urit.mace.aarc-project.eu.am03.pilots.aarc-project.eu.members.member@aarc-yeilow.pilots.aarc-project.eu uri.mace:aarc-project.eu:am03.pilots.aarc-project.eu:members:member@aarc-yellow.pilots.aarc-project.eu							
		um mace:aarc-project.eu:am03.pilots.aarc-project.eu:members:member@aarc-yellow.pilots.aarc-project.eu						
5	The user is successfuly	□ Instance Greene × 3 + ◆ ① @ Instance Greene x + + ◆ ① @ Instance Greene x + +						
D.	Dashboard, mapped to a	ubuntu [®] The username Aptitz@havard.example.edu •						
	Keystone user group based on	Project OVerview The Project						
	the values of the Entitlement	Overview Limit Summary Le						
	username.	Instances						
	In this same the user is	Images Instances VCPUs RAM Floating IPs Security Groups Access & Security Used 0 of 10 Used 0 of 20 Used 0 of 51,200 Used 0 of 50 Used 1 of 10						
	In this case the user is accessing the aarc-vellow	Network Usage Summary						
	project with the rights for a	Identity Select a period of time to query its usage:						
	"regular user" (no administrative	From: 2017.01.01 To: 2017.01.11 Submit: Te dam should be a YYYYam-54 foread. Active Instances: 0 Active RAM: 08yles This Period's VCPU-Hours: 0.00 This Period's GB-Hours: 0.00 This Period's 0.00 This Per						
	ngma).	Usage 🔺 Deverteat CDV Summary 🕹 Operated App Environment File						
		Instance Name VCPUs Disk RAM Time since created No terms to display						
		Deploying titems						

4 a.	user belonging to aarc-yellow CO and with admin role	AARC AAI Attribute Management Pilot Home • Consent about releasing personal information								
	After successful authentication, the user needs to give the	ht	tps://am02.pilots	s.aarc-project.eu/shibbo	leth requires that the informa	tion below is transferred.				
	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	24	Yes, continue	No, cancel			\$			
		In	Information that will be sent to https://am02.pilots.aarc-project.eu/shibboleth							
			Preferred langue	uage						
		2-	User ID							
			awest							
	authority COmanage regarding the ownership in the COs and		Anthony							
	the roles.	-	Surname							
	In this case the Entitlement contains these pieces of	-	West							
	information:		Anthony West	t						
	urn:mace:aarc-project.eu: am03.pilots.aarc-project.eu: members:member@aarc- yellow.pilots.aarc-project.eu		Mail Anthony_Wes	st@university-example.o	rg					
			Display name Anthony West	t						
	urn:mace:aarc-project.eu: am03.pilots.aarc-project.eu: admin:member@aarc-yellow. pilots.aarc-project.eu		Home organiza	tion domain name						
		-	Person's principal name at home organization							
			awest@unive	ersity-example.org						
	That is the piece of information used for properly mapping the users to the OpenStack projects.		member employee staff							
	Click on "yes" for going on.		Group member urn:collab:org	rship g:aarc-project.eu						
		<	Entitlement reg • urn:ma • urn:ma	arding the service ace:aarc-project.eu:am0; ace:aarc-project.eu:am0;	3.pilots.aarc-project.eu:memi 3.pilots.aarc-project.eu:admir	bers:member@aarc-yellow.pilo n:member@aarc-yellow.pilots.a	is.aarc-project.eu arc-project.eu	>		
5 a.	The user is successfuly redirected to the OpenStack Dashboard, mapped to a Keystone user group based on the values of the Entitlement	 Ins Ins 	ance Overview - Open × +	oject eu doeison (project/			C Q. Cerco			
		Proje		Verview		1	he username	awest@university-example.org •		
		Admi Syste	m ^ Li	mit Summary	The Project					
	username.		Overview			ø				
	In this case the user is		Host Aggregates	Instances Used 0 of 10	VCPUs Used 0 of 20	RAM Used 0 of 51,200	Floating IPs Used 0 of 50	Security Groups Used 1 of 10		
	accessing to the aarc-yellow project with administrative rights.		Flavors Images Se	sage Summary elect a period of time to quer	y its usage:					
			Networks Ac	rom: 2017-01-01 To: tive Instances: 0 Active RAM: 0Bytes 1	2017-01-10 Submit The date shou This Period's VCPU-Hours: 0.00 This Period's	d be in YYYY-mm-4d format. GB-Hours: 0.00 This Period's RAM-Hours: 0.00				
			Defaults In	Jsage	VCPUs	Disk RAM	▲ Down Time since created	nload CSV Summary		
			Metadata Definitions System Information	splaying 0 šema		No items to display.				
		Identi	ity ~							

4 c.	user belonging to aarc-blue CO and with admin role	AARC AAI Attribute Management Pilot Home - Consent about releasing personal information							
	After successful authentication,	https://am02.pilots.aarc-project.eu/shibboleth requires that the information below is transferred.							
	the user needs to give consent for releasing personal information to the Service Provider mentioned in the page	Ves continue No cancel							
		res, contaitue no, cantei							
	(the OpenStack framework in our case).	Information that will be sent to https://am02.pilots.aarc-project.eu/shibboleth							
	Among the data that will be	oburton							
	passed to the Service Provider, there are the Entitlements released by the attribute	Given name							
		Oscar Sumame							
	regarding the ownership in the	Surname Burton							
	COs and the roles. In this case the Entitlement contain these pieces of	Common name							
		Oscar Burton Mail							
	information:	Osc@rBurton@university-ex	kample.org						
	urn:mace:aarc-project.eu:	Display name Oscar Burton							
	members:member@aarc-blue.	Home organization domain name							
	phots.aarc-project.eu	university-example.org	a organization						
	urn:mace:aarc-project.eu: am03.pilots.aarc-project.eu: admin:member@aarc-blue. pilots.aarc-project.eu	oburton@university-example.org							
		Affiliation							
	That is the piece of information used for properly mapping the users to the OpenStack projects.	• member • staff							
		Group membership							
		um:collab:org:aarc-project.eu							
	Click on "yes" for going on.	en							
		Entitlement regarding the service	ce						
		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							
~		Datase Universe - Upies X 📪							
с.	redirected to the OpenStack	De https://am02.pilots.aarc-project.au/backgor/project/ Jbuntu [®] I asarc-blue →			د مردست The username				
	Keystone user group based on	Admin	The Project	-					
	the values of the Entitlement attribute, with the eppn as								
	username	Hypervisors Instances	VCPUs	RAM	Floating IPs	Security Groups			
	In this case the user is accessing the aarc-blue project	Instances Usage Summary	Used 0 01 20	0360 0 01 51,200	Used U of SU	Used t of to			
	with administrative rights.	Select a period of time From: 2017-01-01	to query its usage: To: 2017-01-10 Submit The date should	لي d be in ۱٬۱۹۹۷-mm-dd format.					
		Routers Usage	4: 0Bytes This Period's VCPU-Hours: 0.00 This Period's 0	3B-Hours: 0.00 This Period's RAM-Hours: 0.00	D 📥 Downfor	ad CSV Summary			
	Time since created								
		dentity *							

Mapping rules: an example

