Authentication and Authorisation for Research and Collaboration

Revamping IdP in the Cloud pilot activities

Proposal for the forthcoming months

Mario Reale, Maria Laura Mantovani, Davide Vaghetti, Marco Malavolti

AARC JRA1, SA1, NA2
GARR

AARC All Hands F2F CERN Geneva
November 30, 2016

Agenda

- IdP in the Cloud as an answer for AARC Requirements and Policy assurance
- IdP in the Cloud in the Blueprint Architecture
- The current existing solution - Proposal for a new implementation
- Required developments for the pilot
- Estimated efforts and timeline
- Outcome

Requirements addressed by IdP in the Cloud

Best Practices

Attribute Release

Persistent Unique Id

Levels of Assurance

Incident Response

Guest Users

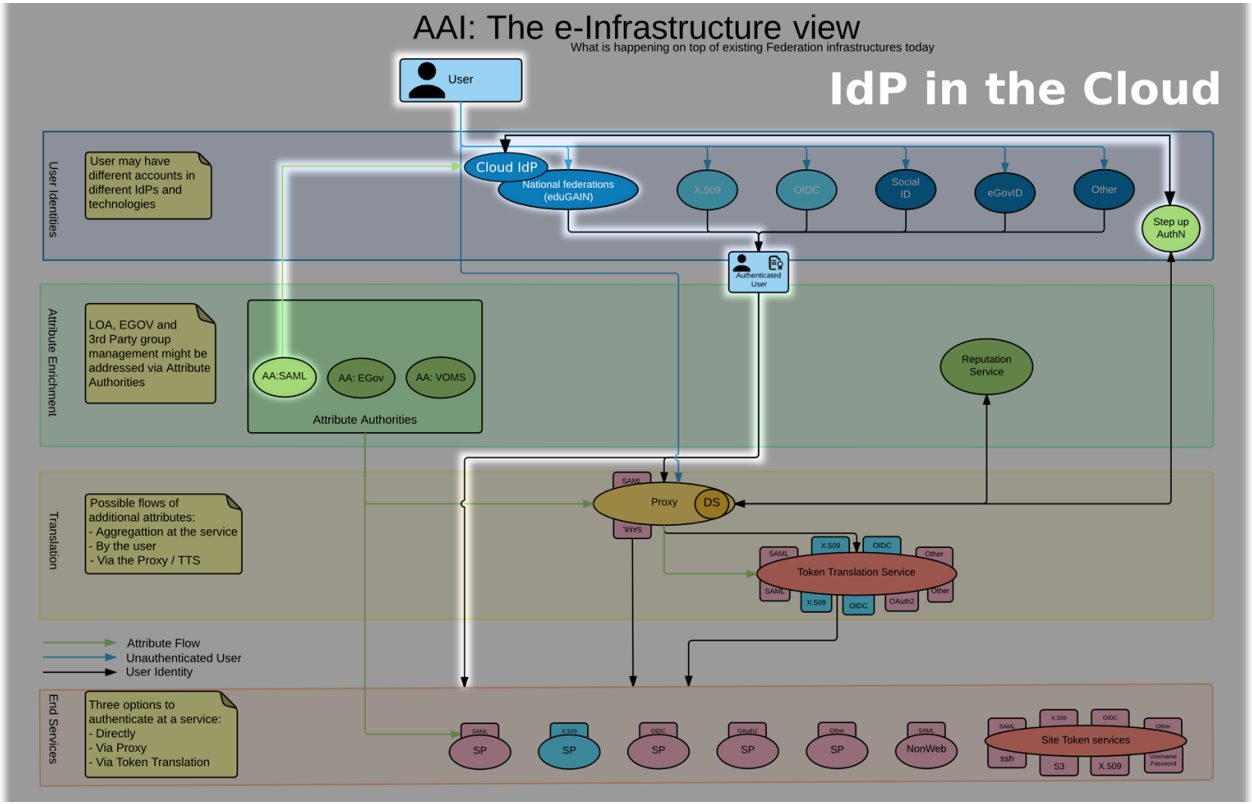
1. Availability of well-configured, secure and schema compliant IDPs in the federation
   a. SIRTFI enforcement (Operational Security, Incident Response, Traceability, Participant Responsibilities)
   b. Entity Category (R&S, CoCo) support/Attribute release enforcement
2. Ease the implementation of predefined assurance profiles (LoA)
3. Reduce required effort to interface additional components possibly needed by SPs in the Federation
   a. Attribute Authorities
   b. Step-Up Authentication
4. Provisioning of IDPs to poorly skilled/attended Home Organizations
   a. Enrollment of new identities in the Federation (guest users zero target)

Step-up AuthN

Attribute Aggregation

User Managed Information

IdP in the Cloud in the Blueprint Architecture



Proposal for improvement of current GARR IdP in the Cloud (1/2)

IdP in the Cloud Features	version 1 (current)	version 2.0 (pilot)	version X (evolution)
Cloud Infrastructure	Openstack	Any docker-enabled cloud infrastructure	• Any docker-enabled cloud infrastructure • Openstack (private cloud) • Public cloud (Azure, AWS, etc.)
Cloud Infrastructure integration	manual	manual	Juju, Vagrant
Container support	(none)	Docker (with persistent storage for DB, custom config, and logs)	Kubernetes
Deploy management	Puppet	Ansible	Ansible
OpSys	Ubuntu 12.04.5	Debian (latest)	• Debian (latest) • Ubuntu • CentOS
IdP SW	Shibboleth v3.2.1(latest)	Shibboleth v3.3.x (latest)	Shibboleth v3.3.x (latest)
Flavours	- IdP only - IdP + IDM	• IdP only • IdM+Directory+IdP	• IdP only • IdM+Directory+IdP

Proposal for improvement of current GARR IdP in the Cloud (2/2)

IdP in the Cloud Features	version 1 (current)	version 2.0 (pilot)	version X (evolution)
IdM	OpenLDAP+phpLDAPadmin (mySQL)	OpenLDAP+phpLDAPadmin	OpenLDAP+phpLDAPadmin OpenLDAP+PERUN OpenLDAP+midPoint OpenLDAP+Apache Syncope
System monitoring	Nagios, collectd	Nagios, collectd	Nagios, collectd Zabbix
System security	-		Fail2ban or alternatives
Statistics and accounting	PHP script based on loganalysis script		
Added values	Entity category support Managed Attribute filter	Entity category support Managed Attribute filter Federation integration	Entity category support Managed Attribute filter Managed LoA Federation integration

Pilot tasks breakout

- Setup docker environment
- Development of Ansible playbooks to
  - Create the HomeOrg IdP including all required customizations
  - Spawn and management of IdPs through Docker containers
- Support for english and local language (according to partners' participation)
- We will evaluate other container types (e.g. LXC/LXD) and other Linux distributions (e.g. Ubuntu, CentOS) if of interest for pilot participants/community
- Set up of a testbed, possibly involving different infrastructures / hosting environments
  - We encourage the participation of 1-2 AARC additional partners to the pilot
- Publish ansible playbooks and Docker recipes on public repos
- Publish the Docker image on Docker Hub

Draft estimated effort and timeline

- Setup of required clusters at the sites (0.5 week , 2 persons)
- Creation of test Docker environment (0.5 week, 2 persons)
- Writing Ansible playbooks to carry out required tasks (4 weeks, 2 persons)
  - Including local language support
- Tests against test SP-instances (1 week, 1 person)
- Writing comprehensive guide for providers, in collaboration with NA2 (2 weeks , 1 person)
- Writing Leaflet for HO, in collaboration with NA2 (1 week, 1 person)
- Showcasing everything on the SA1 wiki / Cockpit panel (2 weeks, 1 person)

Timeline:

- Start : January 1, 2017 - End: March 31, 2017

Outcome

1. Demonstrate feasibility and effectiveness of providing IdP in the Cloud via containers deployable, possibly on different cloud infrastructures
2. Production of an handbook for Cloud providers in order to offer the service
3. Leaflet for Home Organizations about needs and benefits of the IdP in the Cloud solution

AARC vs GN4-2 approach in supporting IdP deployment

AARC NA2/SA1 proposed activities	GN4-2 JRA3 Task 1 planned / ongoing activities
1. Demonstrate feasibility for IdP in the Cloud 2. Howto handbook for Cloud providers 3. Leaflet for Home Organizations about needs and benefits of the IdP in the Cloud solution	1. On-going survey on NRENs/Feds requirements around IdPs and level of appreciation for a Cloud-based solution 2. Cost-Benefit Analysis to be provided for a Campus IdP platform .Its goal is supporting a GEANT decision on future transition to service for a a. Deployment toolkit b. NREN/GEANT hosted Cloud IdP platform 3. Sketching an initial design for a comprehensive platform aimed at a. Providing IdP MD management b. Spawning IdPs on Containers c. Plugging private cloud infrastructures

Thank you

Any Questions?

mario.reale@garr.it
marialaura.mantovani@garr.it
davide.vaghetti@garr.it
marco.malavolti@garr.it

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).