GEANT

Strategy on Campus Identity Provider

Campus IdP session with Internet2 at TechEx 2018

Mario Reale (GARR) - Michael Schmidt (DFN/LRZ)

On behalf of the GEANT Campus IdP task team

TechEx 2018 - Orlando - October 17, 2018
Agenda

• **Goals**
• **Adopted Strategy**
• **Current offer to Home Organizations and ID Federation**

• **Campus IdP Platform architecture**
  • Demo video
The GEANT TEAM of Campus IdP

Valentin Pocotilenco, Marco Malavolti, Jan Oppolzer, Janusz Ulanowski, Dick Visser, Anass Chabli, Michael Schmidt, Jule Ziegler, Miroslav Milinovic, Dubravko Penezic, Brook Schofield, Marko Eremija, Boro Jakimovski, Valeria Ardizzone, Davide Vaghetti, Mario Reale, Pal Axelsson

GEANT Gn4.2 Jra3 Task 1
Goals for Campus IdP task

**Home Organizations:**
- Support local administrators in spawning their HO Identity Provider

**Federations:**
- Support Federation Operators in their role of Cloud IdP providers

=> Community survey:
There is high desire but little or no internal ability for institutions to deliver identity provider services to their users (~ 40% of answers)
Q2: What is the desire and ability of institutions to deliver IdP services

Q3: What are the main barriers to adoption of federated Identity services?

- Survey Still online on http://tinyurl.com/z33jond
- Detailed answers report available at https://goo.gl/XA4eqy

Relevant outcome: there is high desire but little or no internal ability for institutions to deliver identity provider services to their users (~ 40% of answers)
Q8: How interested would your individual institutions be in outsourcing the provisioning of a local IdP to a managed service provider?

- Survey Still online on [http://tinyurl.com/z33jond](http://tinyurl.com/z33jond)
- Detailed answers report available at [https://goo.gl/XA4eqy](https://goo.gl/XA4eqy)

Relevant outcome: **there is high desire but little or no internal ability for institutions to deliver identity provider services to their users (~ 40% of answers)**

Q11: Principle advantages of a GEANT provided and managed Cloud based solution for the IDP?

- Interested, provided is the National ID Federation providing a solution within a compatible data protection environment
- Long term sustainability of provided solution
Approach adopted

[ skept (hidden) slide ]

- Hosted Cloud Campus IdP platform integrated with FaaS components
- Toolkit deploying Cloud IdP for Campus
- Cloud Campus IdP service catalogue
- GEANT hosted Campus IDP Cloud Service integrated with GÉANT FaaS

Cloud Service

Toolkit
Adopted strategy: what do we offer to...

...Federations:
- To support Federation Operators in their role of Cloud IdP providers:
  - Campus IDP Ansible Toolkit
  - Campus IDP Platform (In development - see demo)
  - F-ticks: Measurement and Statistics gathering
  - SIRTFI email contacts verification tool

...Home Organizations:
- To support local administrators in spawning their HO Identity Provider:
  - Campus IDP Ansible toolkit - Localhost deploy + Config support scripts
    - Including basic local IdP statistics
  - Docker deployment of Shibboleth Identity Provider
Gathering authentication statistics: F-ticks pilot architecture

F-TICKS format:

F-TICKS/<federation-id>/1.0#
VISCOUNTRY=<tld-country-of-F-tick-origin>#
AP=<SAML-IdP-entityID>#
RP=<SAML-SP-entityID>#
RESULT=<authentication-result-code>#
CSI=<SAML-session-id-hash>#
PN=<depersonalised-ePTID>#
TS=<timestamp>#
Gathering authentication statistics: F-ticks pilot results

Currently piloting with 7 federations

Gathered so far 18 Million records in 6 months
ELK stack to gather FTicks prototype

National Identity aggregation layer + GEANT collector

- Prototype for ELK-based infrastructure to gather FTicks from national federations, provide a national aggregation layer and a global GEANT collector
- Complete deployment suite based on Docker swarm
- [https://github.com/GEANT/FTicks-ELK](https://github.com/GEANT/FTicks-ELK)
Docker deployment of Shibboleth IDP

- Docker based deployment of Shibboleth IdP
  - **Docker-compose** based install and config of IdP
  - Shared volumes to keep persistent information
    - Idp configuration files
    - Certificates
    - Log file
  - Provides targeted user identifier ePTID
- https://github.com/GEANT/CampusIdP/tree/master/DOCKER
The GEANT Ansible Toolkit allows to:

1. Create/Delete Virtual Machines on an OpenStack Cloud (ansible-openstack)
2. Deploy the monitoring system to check the IdPs (ansible-monitoring)
3. Deploy an entire Shibboleth Identity Provider(IdP) (ansible-shibboleth)
GARR IdP-in-the-Cloud Example

[ skept (hidden) slide ]
Demo Introduction

Demo workflow:
1. Log in on the Campus IdP platform
2. Fill configuration form
3. Request and approve creation of new IdP
4. Spawn (Install & Config) the Shib IdP
5. Check the newly deployed IdP
Demo Video on GEANT Campus IDP Platform is available at

https://gbox.garr.it/garrbox/index.php/s/dDZPPsbyN5SZG2h
References:

1. Task wiki on https://wiki.geant.org/display/gn42jra3/Task+1%3A+Campus+and+Federation
2. GEANT Campus IdP Ansible toolkit https://goo.gl/rjuN2u
3. FTicks ELK pilot - Implementation https://github.com/GEANT/FTicks-ELK
5. SIRTFI email contacts verification tool: https://campus-idp-test.geant.org/
6. Docker deployment of IdP https://github.com/GEANT/CampusIdP/tree/master/DOCKER

Contact: gn4-2-jra3-t1@lists.geant.org
1. Docker based deployment of IdP:
   a. Add functionality and complete the Docker-based deployment module
2. Campus IdP platform:
   a. Complete the development and consolidate the Campus IdP Platform Architecture
3. SIRTFI email contacts verification tool
   a. Define 2 time zones (EU, US) to send check email at 10 AM in Europe and America
4. Measurement and Statistics
   a. Implement landing page at https://f-ticks.edugain.org
   b. Provide scripts for upgrading individual components
   c. Pilot with some GEANT federations
   d. HA swarm based infrastructure
Input 2 to discussion: Possible Items for collaboration

1. Testing new Shibboleth versions - IdP 3.4 - Share results and feedback
2. Docker developments for deployment of IdP
   a. Share code
   b. Beta testing of provided solutions
   c. Envisage a common Docker deployment module / packaging?
   d. Moving towards Kubernetes
3. Gathering of F-ticks/Statistics
   a. Share code and experience / feedback on current implementations
   b. User profiling / Access to data / Authorization model
4. Functional Monitoring of IdP instances
   a. Check_MK / Nagios / Zabbix …
5. IdP configuration management APIs - Implementation and results
   a. Campus IdP platform results
   b. GUI
   c. Architecture
   d. Scalability of solutions / user feedback