Campus Identity Providers: Providing and Using toolkits to deploy

Marco Malavoliti, Mario Reale, Jack Suess, Ann West, Steven Zoppi

TNC 2018
1. GEANT context
2. GEANT example deployment (Federations)
3. Internet2/TIER context
4. Internet2/TIER example deployment (Home Organizations)
5. Wrap up
GEANT context: Campus IdP supporting services activities

- GEANT task on Campus IdP is working on the following items:
  - An **ANSIBLE toolkit** aimed at automating the deployment of the Shibboleth IdP
  - A **Docker-based** deployment solution to provide Shibboleth IdP
  - A tool to gather **Fticks** from IdPs and display related authentication statistics for eduGAIN federations
  - A tool to **gather email address of IdP security contacts** and verify their validity, to support **SIRTFI**
  - A general GEANT IdP platform as an eduGAIN SP accessible by FedOps and HO managers to manage their Identity providers:
    - Install
    - Configure
    - Update
    - ..
Two main customers: Home Organizations and Federations

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

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

Costs Benefits Analysis

Assessment of existing solutions
Market Analysis deliverable

Collection of community requirements

Design
Implementation
Pilot Service
Transition to Production

GEANT hosted Campus IDP
Cloud Service integrated with GÉANT FaaS

Hosted Cloud Campus IdP platform integrated with FaaS components

Toolkit deploying Cloud IdP for Campus
TODAY

Cloud Campus IdP service catalogue
## List of all eduGain entities (2018-06-04)

Showing 1-10 of 7,029 items.

<table>
<thead>
<tr>
<th>#</th>
<th>Entity Name</th>
<th>Contact Type</th>
<th>Contact Email</th>
<th>Contact Name</th>
<th>Last Checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12Twenty SP</td>
<td>technical</td>
<td><a href="mailto:kevin.chu@12twenty.com">kevin.chu@12twenty.com</a></td>
<td>Kevin Chu</td>
<td>(not set)</td>
</tr>
<tr>
<td>2</td>
<td>12Twenty SP</td>
<td>support</td>
<td><a href="mailto:support@12twenty.com">support@12twenty.com</a></td>
<td>General Support</td>
<td>(not set)</td>
</tr>
<tr>
<td>3</td>
<td>12Twenty Test SP</td>
<td>technical</td>
<td><a href="mailto:kevin.chu@12twenty.com">kevin.chu@12twenty.com</a></td>
<td>Kevin Chu</td>
<td>(not set)</td>
</tr>
<tr>
<td>4</td>
<td>12Twenty Test SP</td>
<td>support</td>
<td><a href="mailto:support@12twenty.com">support@12twenty.com</a></td>
<td>General Support</td>
<td>(not set)</td>
</tr>
<tr>
<td>5</td>
<td>3D Labs at Stony Brook</td>
<td>other</td>
<td><a href="mailto:DoIT_Security@stonybrook.edu">DoIT_Security@stonybrook.edu</a></td>
<td>DoIT Information Security</td>
<td>(not set)</td>
</tr>
<tr>
<td>6</td>
<td>3D Labs at Stony Brook</td>
<td>administrative</td>
<td><a href="mailto:gary.halada@stonybrook.edu">gary.halada@stonybrook.edu</a></td>
<td>Gary Halada</td>
<td>(not set)</td>
</tr>
<tr>
<td>7</td>
<td>3D Labs at Stony Brook</td>
<td>technical</td>
<td><a href="mailto:paul.st.donis@stonybrook.edu">paul.st.donis@stonybrook.edu</a></td>
<td>Paul St. Denis</td>
<td>(not set)</td>
</tr>
<tr>
<td>8</td>
<td>missing</td>
<td>technical</td>
<td><a href="mailto:chris.oliver@3plearning.com">chris.oliver@3plearning.com</a></td>
<td>Chris</td>
<td>(not set)</td>
</tr>
<tr>
<td>9</td>
<td>missing</td>
<td>support</td>
<td><a href="mailto:techsupport@3plearning.com">techsupport@3plearning.com</a></td>
<td>3P Learning Technical Support</td>
<td>(not set)</td>
</tr>
<tr>
<td>10</td>
<td>missing</td>
<td>support</td>
<td><a href="mailto:techsupport@3plearning.co.uk">techsupport@3plearning.co.uk</a></td>
<td>Technical Support</td>
<td>(not set)</td>
</tr>
</tbody>
</table>
SWAMID - REFEDS R&S and REFEDS SIRTFI requirement test

This service is a simple proof of concept test with Shibboleth SP Attribute Checker. If the test is successful you will see a very simple page with all attributes echoed.

The Identity Provider is tested for

- metadata declaration for support of REFEDS SIRTFI; and
- attribute release based on REFEDS R&S.

Log in via SWAMID or eduGAIN
Gathering authentication statistics: Fticks pilot

- IdP_1
  - send F-TICKS
  - syslog

- IdP_n
  - send F-TICKS

- listener daemon
  - logstash server
  - store F-TICKS

- Elastic Search DB
  - provide statistics

- database MySQL

- Kibana

- GUI

- REST API
Gathering authentication statistics: Fticks pilot

http://geantsrv17.ct1.garrservices.it/
Gathering authentication statistics: Fticks pilot

http://geantsrv17.ct1.garrservices.it/
Campus IdP Platform

Web App (e.g. React) → Access CampusIdP
HO Admin → Manage Federation

EduGAIN

Resource Registry (e.g. Jagger)

API (Node.js) → Create/Delete/Manage IdP
Trigger IdP creation/update
Store/Load IdP config

Database (e.g. Mongo)

IdP Factory (Ansible)

1. Single Container
   IdP Cloud (Openstack)

2. Microservices
   IdP Cloud (Openstack)

Orchestration (e.g. Kubernetes)

Manage containers

Running

IdP Cloud (Openstack) → IdP Cloud (Openstack)
IdP login

IdP User

EduGAIN login

Provide metadata
Receive metadata

Manage
containers

Manage
containers

Manage
Federation

Approve IdP creation

Federation Admin

Create IdP container

Create IdP container

Deploy IdP

Show statistics

Register IdP

Create/Delete/Manage IdP

Store/Load IdP config

Trigger IdP creation/update

Register IdP
Campus IdP
Platform: microservices
On going work and further developments

On going

- Design and implementation of Web Client application (GUI) [React] & corresponding SP
- Further development of Docker microservices based solution by adding offered functionality
- Addition of functionality to the SIRTFI email checker tool [https://campus-idp-test.geant.org]
- Extend the Measurement and Statistics pilot to include additional IdPs from Federations
The GEANT Ansible toolkit to deploy Identity Providers

Marco Malavolti
IDEM Federation Operator
marco.malavolti@garr.it
1. **Help** research institutions lacking of manpower, hardware, knowledge, to install and configure their Identity Providers Shibboleth.

2. **Increase** the number of IdPs joining identity federations.

3. **Break down the effort** needed to join an identity federation
How?

With the Géant **Ansible-Toolkit**.

The 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](#))
<table>
<thead>
<tr>
<th>Instance Name</th>
<th>Image Name</th>
<th>IP Address</th>
<th>Size</th>
<th>Key Pair</th>
<th>Status</th>
<th>Availability Zone</th>
<th>Task</th>
<th>Power State</th>
<th>Time since created</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>idp-portal.iks.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.93.37</td>
<td>Floating P=99 147.155.106</td>
<td>idem-idcloud</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 minutes</td>
</tr>
<tr>
<td>garr-idp-prod.rccs.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.10</td>
<td>Floating P=99 147.155.82</td>
<td>idem-idcloud</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>1 month, 1 week</td>
</tr>
<tr>
<td>garr-idp-best.rccs.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.36</td>
<td>Floating P=99 147.157.145</td>
<td>idem-idcloud</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
<tr>
<td>checmk.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.7</td>
<td>m1.medium</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
<td>Create Snapshot</td>
</tr>
<tr>
<td>kibana.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.36</td>
<td>Floating P=99 147.155.215</td>
<td>idem-elk</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
<tr>
<td>data-backups.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.9</td>
<td>Floating P=99 147.155.36</td>
<td>idem-idcloud</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
<tr>
<td>logs.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.8</td>
<td>Floating P=99 147.155.172</td>
<td>idem-idcloud</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
<tr>
<td>elasticsearch2.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.5</td>
<td>Floating P=99 147.155.12</td>
<td>idem-elk</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
<tr>
<td>elasticsearch1.aai.garr.it</td>
<td>Debian 8.2</td>
<td>192.168.90.4</td>
<td>Floating P=99 147.155.82</td>
<td>idem-elk</td>
<td>idpcloud-key</td>
<td>Active</td>
<td>nova</td>
<td>None</td>
<td>Running</td>
<td>2 months, 1 week</td>
</tr>
</tbody>
</table>
Check HTTPS:
Check SSL Certificate Expiration

Check IDP MD:
Check IDP Metadata (/idp/shibboleth/) availability

check_aacci: Check the capacity of sending attributes from the IdP to a test SP

check_mysql:
Check that all needed database for the IdPs are active

- Check IDM page,
- Check IDM-TOOLS,
- Check LOCKUSER,
- check_coco,
- check_rs,
- check_lidap
Ansible-monitoring result: Install and Configure monitoring tools
ansible-shibboleth result: Install and Configure a Shibboleth IDP completely

Clear User Consent

Password Management

Information Web Page

Privacy Policy Web Page

Multi Language Support

Links to Federation and Interfederation web page whom the organisation belongs to

Footer Background Color and Footer Text are customizable
Ansible-shibboleth result: Install and Configure a Shibboleth IDP completely

SP Information (retrieved from its metadata)

SP Description
Test Service Provider v2.5.3 hosted by OpenStack Milano

- Go back to login page
- SP Service Name: Test SP v2.5.3
- SP Organization: TEST Shib SP v2.5.3
- SP Contacts: Marco Malavolti
- SP Privacy Policy
- SP Information Page
The IDP Manager can view the usage of the IDP with a simple “Statistics” page.
Identity Management provided by a customized and corrected version of phpLDAPadmin 1.2.3 (latest available)
The IdP manager can lock out the users immediately by pressing on “Lock” button, or “Set an expiration date” in the future.
Results

- 10 minutes to deploy a Shibboleth IdP
- **Hidden** the complexity of installation and configuration of SAML Shibboleth IdP
- **Simplified user management operations** for IdP managers
- **Simplified the management** of an IdP for operators: security updates, bugfix, software updates, …
- **Matched** the required **federation standards** in terms of security, reliability, compliance with required policies:
  - SSL credentials, Metadata, Privacy and Information pages, Logos, Entity Categories …
- **Eased the process of joining a federation for IdPs**

We can add Identity Providers to the Identity Federation more quickly
Thank you!

Are you interesting in a pilot?  
Contact us!

Marco Malavolti - marco.malavolti@garr.it
Mario Reale - mario.reale@garr.it
Internet2 / Trust and Identity Initiatives

TIER Program Summary ...
TIER Program Expectations

• Primary:

  Long-term sustainability

• Informed By:

  Requirements were prioritized with a Three Year scope in-mind

Driven by IT and Research Use Cases
Institutionalized Work Plan and Results

2018 TIER WORK PLAN AND PROGRESS REPORT BY THEMATIC GROUPING

AS OF 5 MAY 2018 FOR THE 2018 GLOBAL SUMMIT
Scope of Sustainability

- Pre-configured for Multilateral Federated Participants and Research Communities.
- Long-term support agreements will have been established with the Subject Matter Experts, Agencies and Consortia and will be managed on behalf of the community by Internet2
- International Collaborative Development, support and implementation models will continue to be evaluated
The portfolio will be “frozen” to contain “DevOps Friendly” (operationally-oriented), pre-packaged solutions:

- Group Management (Grouper+UI), Collaborative Organizations Management (COmanage+UI), SAML-based Identity Provider and related Service Provider (Shibboleth+UI), InCommon Federation Manager (FM+UI), Entity Registry Storage + Provisioning and Deprovisioning (midPoint), AMQP Compliant messaging middleware (RabbitMQ), Relational Database Solution to support deployment (MariaDB); Solution Packaging (Docker Containers)
Getting Started with Internet2 Trust and Identity

- **TIER Package Delivery**
  - Docker Containers
  - Virtual Machine Images

- **TIER 101**
  - Basic and Background Information
  - Resources to help understand TIER

- **TIER Reference Architecture**
Facets of TIER Program Deliverables

Commercial Offering Contrast
- Offerings are **Solid, Well-Supported**, but **Limited**
- Orientation
  - Application WebSSO
  - Enterprise WebSSO
- Un(der) Served
  - Global Multilateral Federation
  - No Useable AuthZ
  - No Community Policy expression

Unique Program Orientation:
- Community-Requirements Driven
- DevOps, Common APIs, Configuration
- User Interfaces are Core to ALL Functional Deliverables
- Training and Connecting Community Subject Matter Expertise are crucial
- Development process that span ALL types of contributors (Campus Assignees, Contractors, Collaborators, Development Partners)
Campus Success Program
Helping to Mature the Platform

- Identifying future development and support models
- Collaborating around vendor engagements
- Standardized attribute feeds from Ellucian Banner
- Investigating new / future use cases
- SCIM Schemas, API’s, ...
- Deployment Guide(s)
- Identifying, resolving, and documenting institutional implementation challenges
Next Steps and Work In Progress...
Project Name: UMBC TIER Campus Success Program

Project Goals:
- The Tier Campus Success Program is a one year effort to rethink our IDMS and service provisioning strategy.
- UMBC will collaborate with other universities to develop and adopt best practices in IDMS and Federation.

Key Project Milestones:
- Develop Project Plan (11/17)
- Integrate myUMBC groups 5/25
- Test Midpoint registry in testing 4/15
- Develop configuration management tools to streamline integration of UMBC specific needs

Expected Campus or DoIT Impact or Deliverables:
- Create a unified approach to group management across services
- Streamline integration of services by making group management easier.
- Lessen custom business logic in our IDMS environment.

Evaluation or Assessment Criteria:
- We have integrated group management across DoIT services.
- This is used to streamline administrative access to services.
- User satisfaction is rated at least a 4 on our bi-annual survey.
UMBC TIER CSP Results

- CSP has been very helpful in building a community of practitioners for TIER.
- Completed testing of TIER Shibboleth container, will begin deployment for some services in June and complete by fall.
- Working with TIER CSP schools, we have integrated Box and Google into the TIER grouper effort.
- Waiting for Rabbit/MQ -- we are in process of integrating all 500 or our portal groups into grouper and keeping them in sync through Rabbit/MQ -- this will be a big win.
- We will launch our sponsored account provisioning service through midPoint this fall and begin planning for the full deployment over the next 16 months with completion planned for January 2020.
- Beginning some national discussions with IMS about a standard API for SIS.
Thank you