

Campus Identity Providers: Providing and Using toolkits to deploy



Marco Malavolti, 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 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

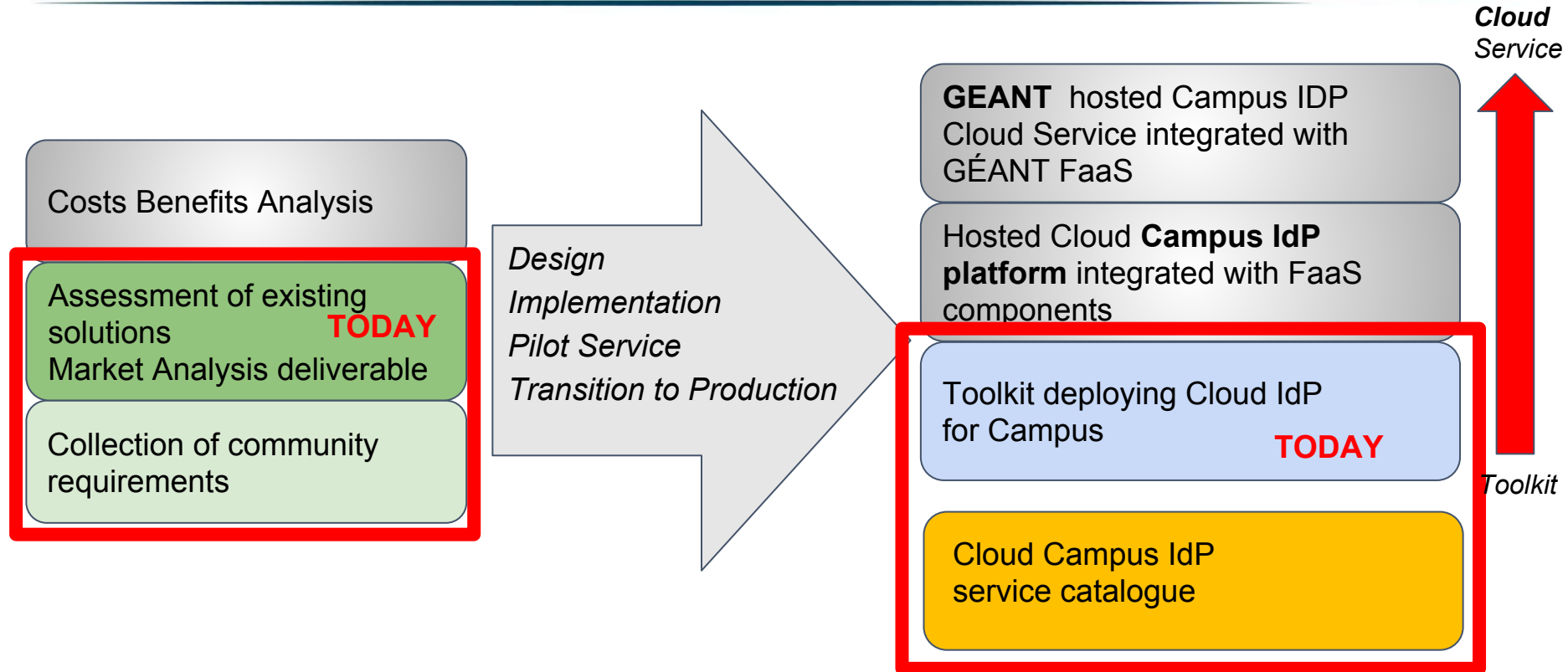


Federations

- Support Federation Operators in their role of Cloud IdP providers



Approach adopted



SIRTFI email contact verification tool

<https://campus-idp-test.geant.org/>



Campus IdP task

[Home](#) [IdP](#) [Contact](#) [Mailer](#) [User Management](#) [Logout \(Mario\)](#)

List of all eduGain entities(2018-06-04)

Select

Entity Type

☐ SP

☐ IdP

☐ AA

Alternative Type

☐ noAltType

☐ SP

Validator

☐ warn

☐ ok

ECCS Status

☐ non_eccs_entity

☐ green

☐ red

☐ yellow

Contact Type

☐ other

☐ technical

☐ administrative

First

«

1

2

3

4

5

6

7

8

9

10

»

Last

Showing 1-100 of 7,928 items.

#	Entity Name	Contact Type	Contact Email	Contact Name	Last Checked	
1	12Twenty SP	technical	kevin.chu@12twenty.com	Kevin Chu	(not set)	<input type="checkbox"/>
2	12Twenty SP	support	support@12twenty.com	General Support	(not set)	<input type="checkbox"/>
3	12Twenty Test SP	technical	kevin.chu@12twenty.com	Kevin Chu	(not set)	<input type="checkbox"/>
4	12Twenty Test SP	support	support@12twenty.com	General Support	(not set)	<input type="checkbox"/>
5	3D Labs at Stony Brook	other	DoIT_Security@stonybrook.edu	DoIT Information Security	(not set)	<input type="checkbox"/>
6	3D Labs at Stony Brook	administrative	gary.halada@stonybrook.edu	Gary Halada	(not set)	<input type="checkbox"/>
7	3D Labs at Stony Brook	technical	paul.st.denis@stonybrook.edu	Paul St. Denis	(not set)	<input type="checkbox"/>
8	missing	technical	chris.olver@3plearning.com	Chris	(not set)	<input type="checkbox"/>
9	missing	support	techsupport@3plearning.com	3P Learning Technical Support	(not set)	<input type="checkbox"/>
10	missing	support	techsupport@3plearning.co.uk	Technical Support	(not set)	<input type="checkbox"/>

<https://sirtfi-check.swamid.se/>

SWAMID - REFEDS R&S and REFEDS SIRTFI requirement test

[About SWAMID](#)

[Contact](#)

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.

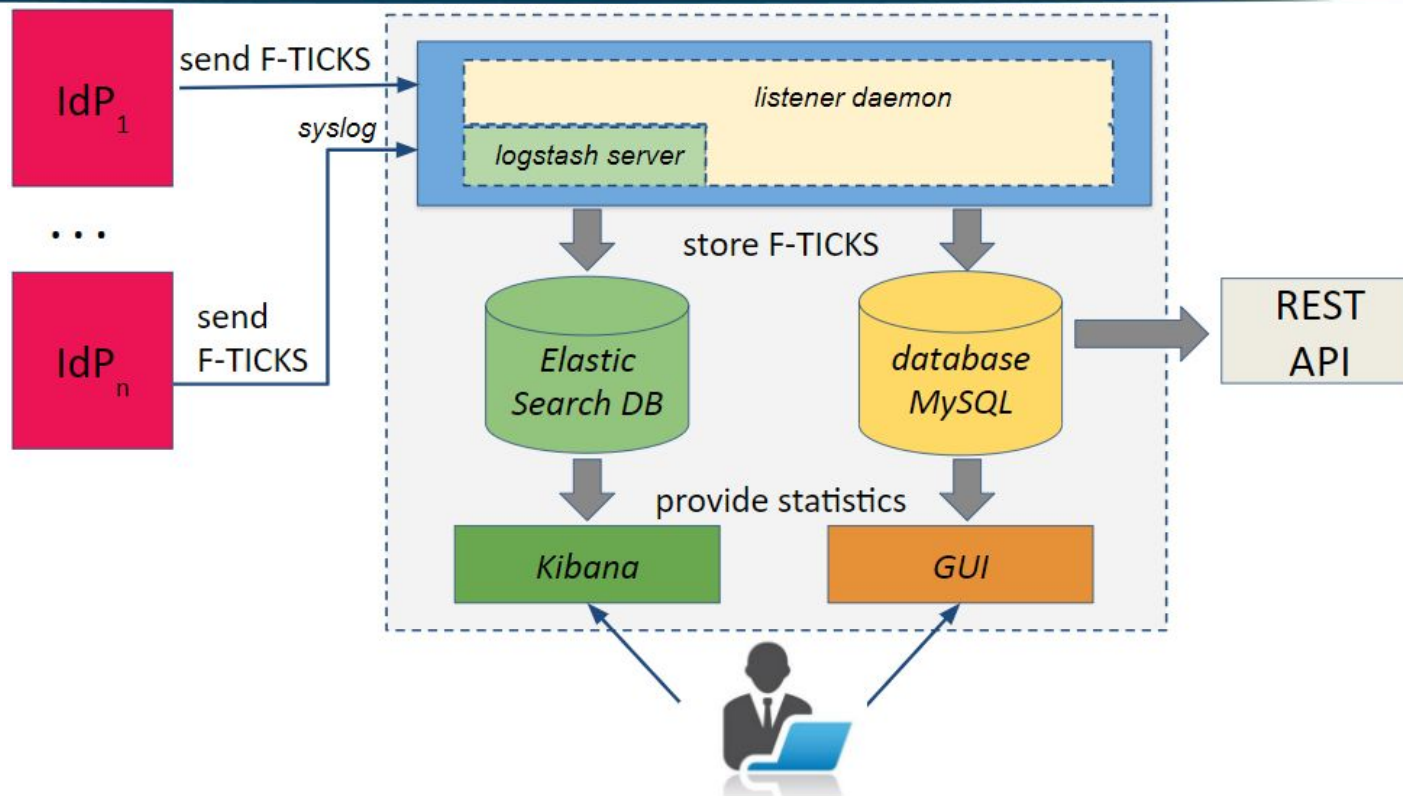
The Identity Provider is tested for

- metadata declaration for support of [REFEDS SIRTFI](#); and
- attribute release based on [REFEDS R&S](#).

SWAMID and eduGAIN

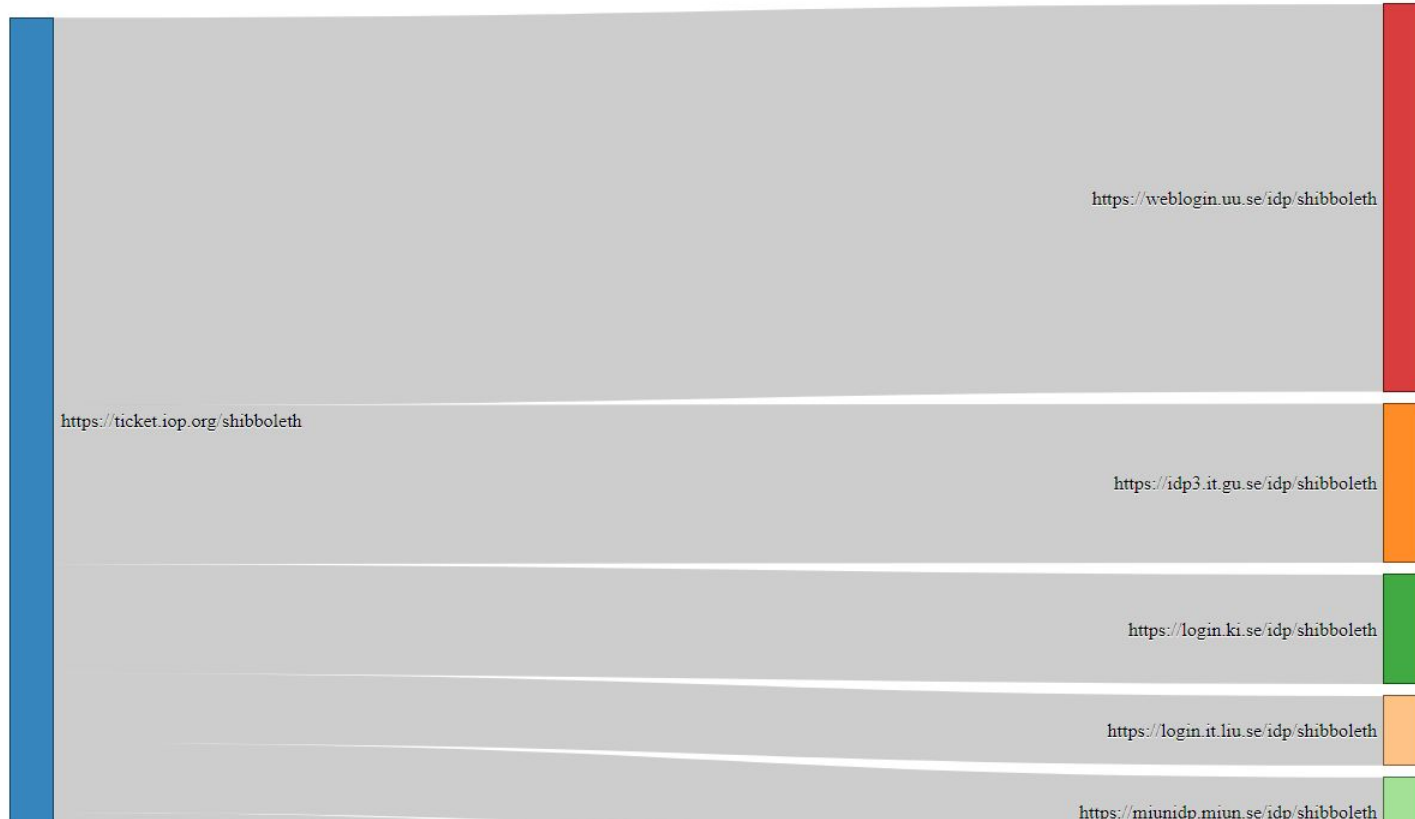
Log in via SWAMID or eduGAIN

Gathering authentication statistics: Fticks pilot



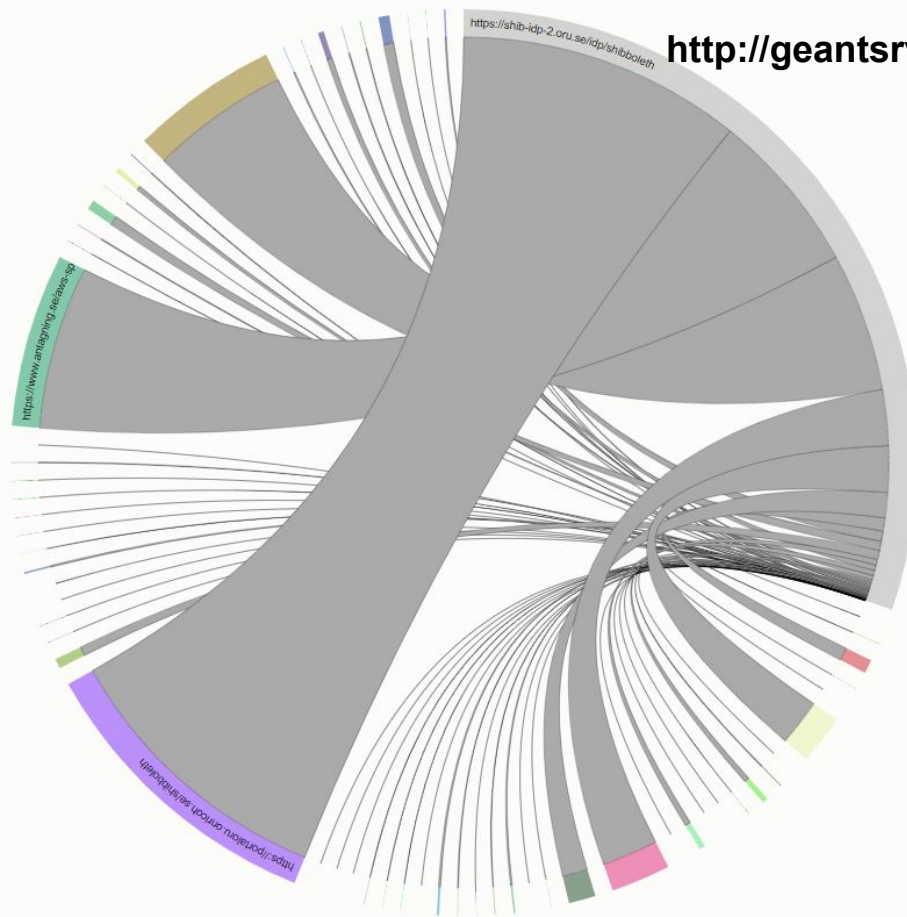
Gathering authentication statistics: Fticks pilot

<http://geantsrv17.ct1.garrservices.it/>

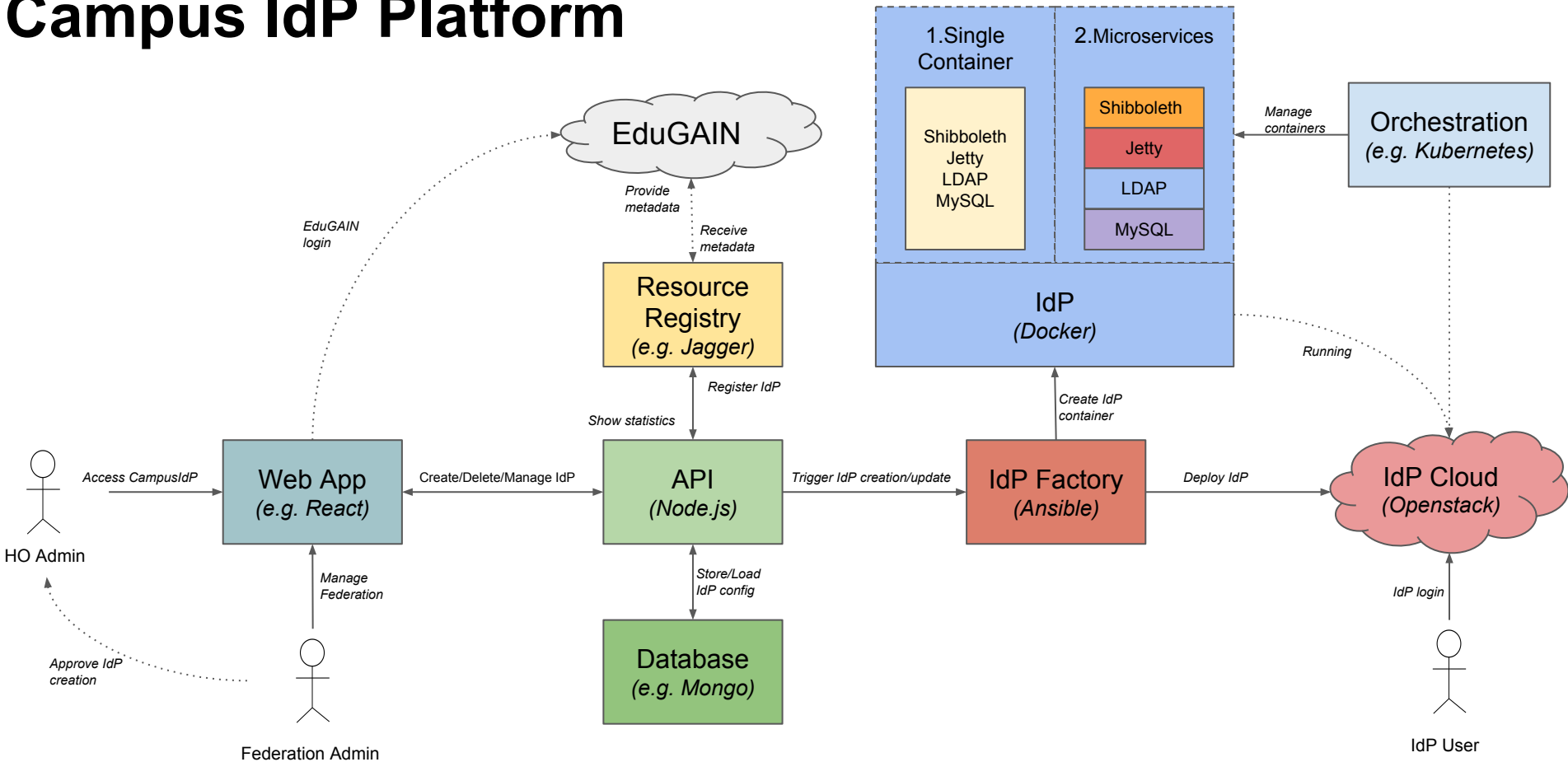


Gathering authentication statistics: Fticks pilot

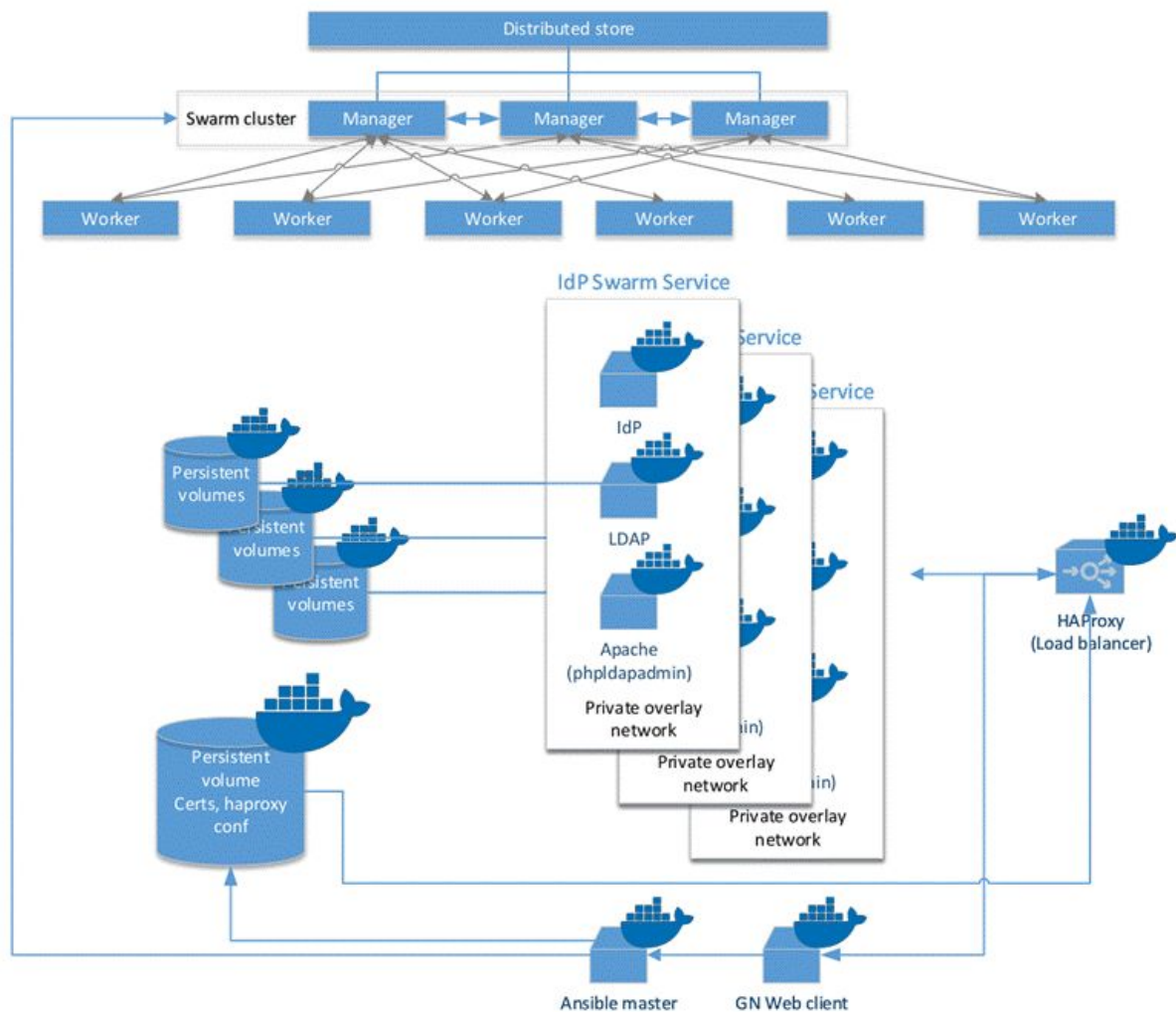
<http://geantsrv17.ct1.garrservices.it/>



Campus IdP Platform



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 GÉANT 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

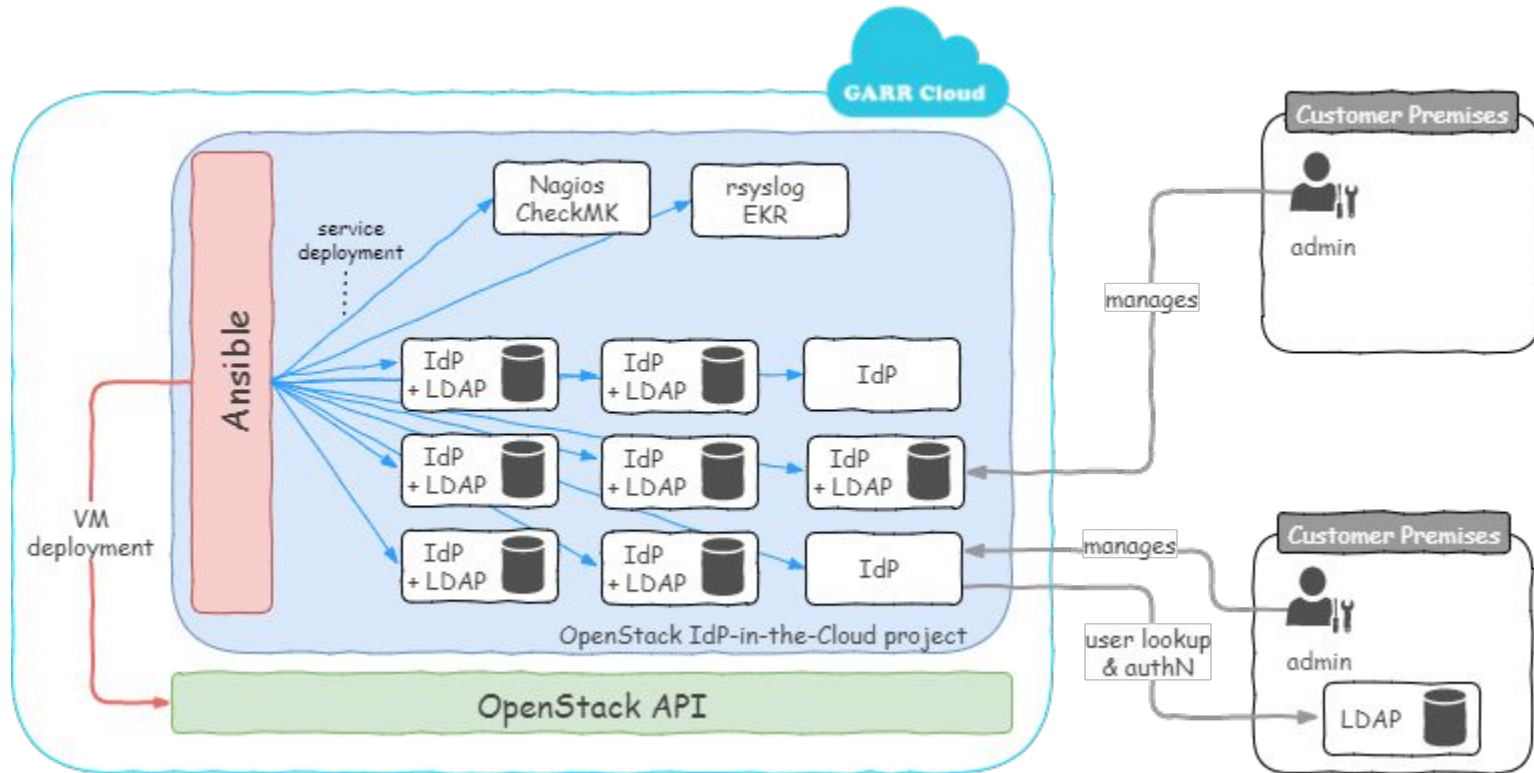
How?

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](#))

GARR IdP-in-the-Cloud Example



Ansible-openstack result: Add/Remove VM on OpenStack Cloud



cloudusers • idpcloud

idpcloud-ops

Project

Compute

Overview

Instances

Volumes

Images

Access & Security

Network

Object Store

Identity

Instances

Instance Name = Filter [Launch Instance](#) [Delete Instances](#) [More Actions](#)

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/>	idp-portici.izs.garr.it	Debian-8.8.2	192.168.80.37 Floating IPs: 90.147.166.106	idem-idpcloud	idpcloud-key	Active	nova	None	Running	2 minutes	Create Snapshot
<input type="checkbox"/>	garr-idp-prod.irccs.garr.it	Debian-8.8.2	192.168.80.10 Floating IPs: 90.147.166.82	idem-idpcloud	idpcloud-key	Active	nova	None	Running	1 month, 1 week	Create Snapshot
<input type="checkbox"/>	garr-idp-test.irccs.garr.it	Debian-8.8.2	192.168.80.36 Floating IPs: 90.147.167.145	idem-idpcloud	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	checkmk.aai.garr.it	Debian-8.8.2	192.168.80.7 Floating IPs: 90.147.166.123	m1.medium	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	kibana.aai.garr.it	Debian-8.8.2	192.168.80.6 Floating IPs: 90.147.167.215	idem-elk	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	data-backups.aai.garr.it	Debian-8.8.2	192.168.80.9 Floating IPs: 90.147.166.36	idem-idpcloud	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	logs.aai.garr.it	Debian-8.8.2	192.168.80.8 Floating IPs: 90.147.167.172	idem-idpcloud	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	elasticsearch2.aai.garr.it	Debian-8.8.2	192.168.80.5 Floating IPs: 90.147.167.12	idem-elk	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot
<input type="checkbox"/>	elasticsearch1.aai.garr.it	Debian-8.8.2	192.168.80.4 Floating IPs:	idem-elk	idpcloud-key	Active	nova	None	Running	2 months, 1 week	Create Snapshot

Ansible-monitoring result: Install and Configure monitoring tools

Check MK
1.4.0p9

Tactical Overview

Quicksearch

Views

Overview

Hosts & Services Problems

Main Overview

Network Topology

Hosts

All hosts

All hosts (Mini)

All hosts (lined)

Favorite hosts

Host search

Host Groups

Host Groups

Host Groups (Grid)

Host Groups (Summary)

Services

All services

Favorite services

Recently changed services

Save by host groups

Service search

Unmonitored services

Service Groups

Service Groups (Grid)

Service Groups (Summary)

Services by group

Metrics

Search Time Graphs

Search performance data

Business Intelligence

Problems

Alert Statistics

Host problems

Pending Services

Pending service discovery

Service problems

State services

Event Console

Events

Recent Event History

Inventory

CPU Related Inventory of all Hosts

Search Backplanes

Search Fans

Search Modules

Search Network interfaces

Search Oracle datapoint statistics

Search Oracle instances

Search Oracle recovery areas

Search Oracle tolerances

All services

73 rows malavolti (admin) 12:23

Local site idpcloud, ansible-slave-1.ircrc.garr.it

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - Agent version 1.4.0p9, execution time 0.7 sec	2017-06-20 14:20:03	19.6 s	707 ms
OK	Check_MK Discovery		OK - no unmonitored services found, no vanished services found	2017-06-01 12:35:48	36 m	
OK	Check HTTPS		OK - Certificate 'ansible-slave-1.ircrc.garr.it' will expire on Sun Nov 29 07:48:08 2026 +0000.	2017-06-20 14:15:37	45.6 s	
OK	Check IDP MD		HTTP OK: HTTP/1.1 200 OK - 14093 bytes in 0.046 second response time	2017-06-20 14:17:29	11.6 s	46.3 ms
OK	check_aacli		OK - SUCCESS - IdP has retrieved metadata of Test SP and is sending attributes to it	2017-06-20 14:15:37	18.6 s	
OK	check_mysql		OK - SUCCESS - IdP has all needed databases	2017-06-01 12:35:20	18.6 s	
OK	CPU load		OK - 15 min load 0.05 at 2 Cores (0.03 per Core)	2017-04-13 20:22:33	18.6 s	0.0400
OK	CPU utilization		OK - user: 0.7%, system: 0.4%, wait: 0.1%, steal: 0.0%, guest: 0.0%, total: 1.1%	2017-04-13 20:22:33	18.6 s	1.13%
OK	Disk IO SUMMARY		OK - Utilization: 0.1%, Read: 0.00 B/s, Write: 8.53 KB/s, Average Read Wait: 0.00 ms, Average Write Wait: 0.66 ms, Latency: 0.66 ms, Average Queue Length: 0.00	2017-04-13 20:22:33	18.6 s	0 B/s / 8.53 KB/s
OK	Filesystem /		OK - 15.6% used (3.06 of 19.65 GB), trend: +8.20 MB / 24 hours	2017-04-13 20:22:33	18.6 s	15.6%
OK	Interface 2		OK - [eth0] (up) speed unknown, in: 425.38 B/s, out: 1.10 KB/s	2017-04-13 20:22:33	18.6 s	425.38 B/s / 1.10 KB/s
OK	Kernel Context Switches		OK - 144/s	2017-04-13 20:22:33	18.6 s	144.47/s
OK	Kernel Major Page Faults		OK - 0/s	2017-04-13 20:22:40	18.6 s	0/s
OK	Kernel Process Creations		OK - 2/s	2017-04-13 20:22:40	18.6 s	1.55/s
OK	Memory		OK - RAM used: 889.41 MB of 3.87 GB (22.4%).	2017-04-13 20:22:33	18.6 s	889.41 MB
OK	Mount options of /		OK - Mount options exactly as expected	2017-04-13 20:22:33	18.6 s	
OK	NTP Time		OK - sys.peer - stratum 1, offset -2.12 ms, jitter 0.94 ms, last reached 968 secs ago (synchronized on 1667-06-20 14:15:37)	2017-04-13 20:22:33	18.6 s	1667 ms
OK	Number of threads		OK - 148 threads	2017-04-13 20:22:33	18.6 s	148
OK	SSH		SSH OK - OpenSSH_6.7p1 Debian-5+deb8u3 (protocol 2.0)	2017-06-22 14:19:46	36.7 s	
OK	TCP Connections		OK - ESTABLISHED: 5, SYN_RECV: 1, CLOSE_WAIT: 7, TIME_WAIT: 3, LISTEN: 7	2017-04-13 20:22:33	18.7 s	
OK	Uptime		OK - Up since Tue Jun 20 13:54:58 2017 (85d 20:17:23)	2017-04-13 20:22:33	18.7 s	86 d

Local site idpcloud, ansible-slave-2.izs.garr.it

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - Agent version 1.4.0p9, execution time 1.8 sec	2017-06-23 07:16:29	2.67 s	1.83 s
OK	Check_MK Discovery		OK - no unmonitored services found, no vanished services found	2017-05-31 10:35:48	36 m	
OK	Check HTTPS		OK - Certificate 'ansible-slave-2.izs.garr.it' will expire on Sun Nov 29 14:37:01 2026 +0000.	2017-06-23 07:12:29	53.7 s	
OK	Check IDM page		HTTP OK: Status line output matched "HTTP/1.1 401 Unauthorized" - 1631 bytes in 0.045 second response time	2017-07-28 14:13:30	10.7 s	44.8 ms
OK	Check IDM-TOOLS		HTTP OK: Status line output matched "HTTP/1.1 401 Unauthorized" - 1639 bytes in 0.044 second response time	2017-07-28 14:19:13	45.7 s	44.4 ms
OK	Check IDP MD		HTTP OK: HTTP/1.1 200 OK - 13943 bytes in 0.050 second response time	2017-09-11 01:21:10	30.7 s	49.8 ms
OK	Check LOCKUSER		HTTP OK: Status line output matched "HTTP/1.1 401 Unauthorized" - 1644 bytes in 0.044 second response time	2017-06-23 07:15:35	47.7 s	43.8 ms
OK	check_aacli		OK - SUCCESS - IdP has retrieved metadata of Test SP and is sending attributes to it	2017-09-07 07:12:40	698 ms	
OK	check_coco		OK - SUCCESS - IdP has retrieved metadata of Test COCO SP and is sending attributes to it	2017-06-19 16:02:35	700 ms	
OK	check_ldap		OK - SUCCESS - LDAP exists and release attributes	2017-06-19 16:02:35	702 ms	
OK	check_mysql		OK - SUCCESS - IdP has all needed databases	2017-06-19 16:02:35	705 ms	
OK	check_rs		OK - SUCCESS - IdP has retrieved metadata of Test RS SP and is sending attributes to it	2017-08-01 00:59:40	708 ms	

Check HTTPS:
Check SSL Certificate Expiration

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

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

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

- Check IDM page,

- Check IDM-TOOLS

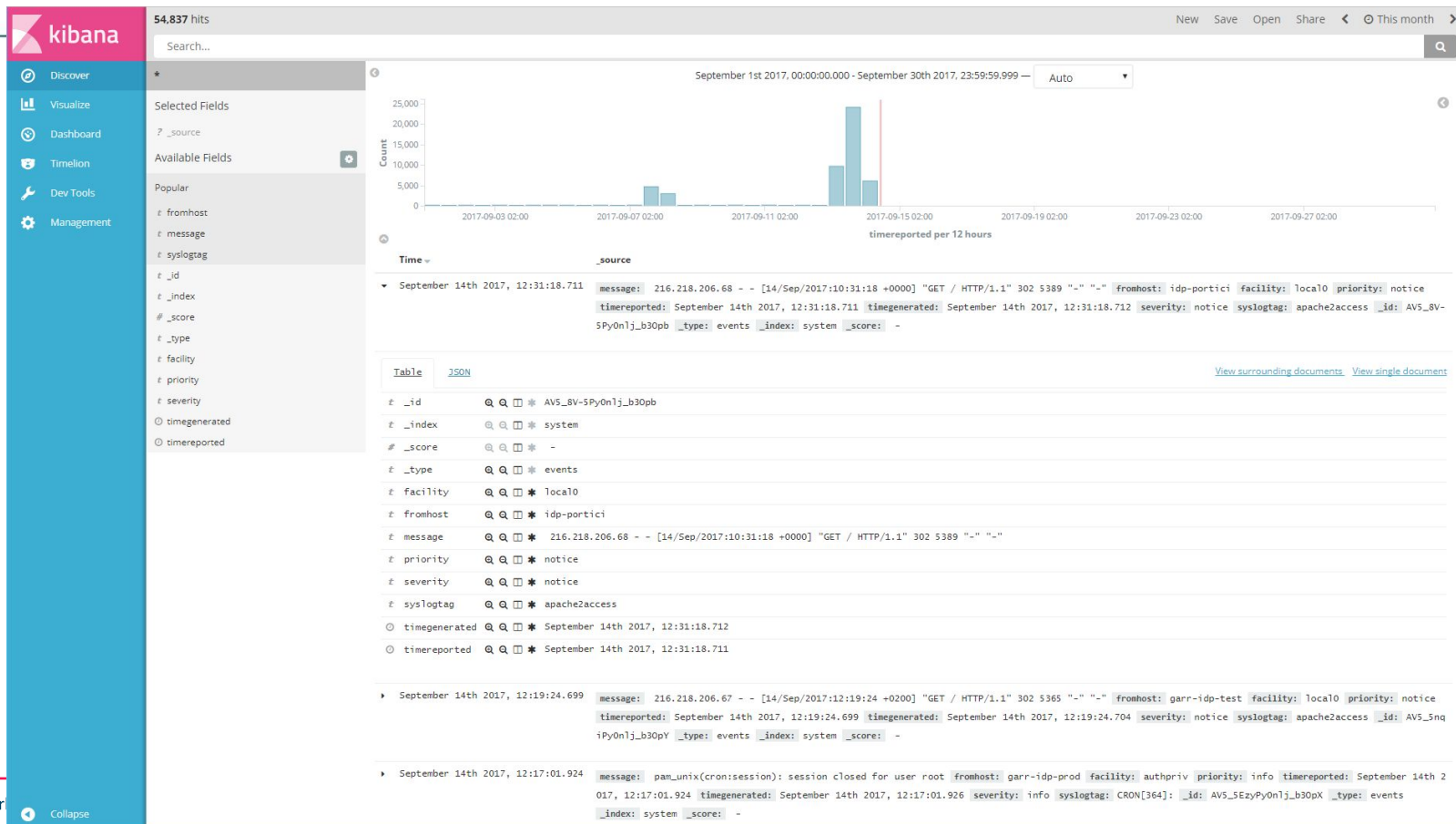
- Check LOCKUSER

- check_coco,

- check_rs,

- check_ldap

Ansible-monitoring result: Install and Configure monitoring tools



Cookie Policy



logo.png

ansible-shibboleth result: Install and Configure a Shibboleth IDP completely

Clear User Consent

Login to Test SP v2.5.3

Username

Password

☐ Don't Remember Login

☐ Clear prior granting of
permission for release of your
information to this service.

Login



SP Logo

Test Service Provider v2.5.3 hosted
by OpenStack Milano
> Resource informations

SP Informations

Password Management

> Forgot your password?

> Need Help?

> Informations

> Privacy Policy



eduGAIN



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

FOOTER TEXT in english language



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:

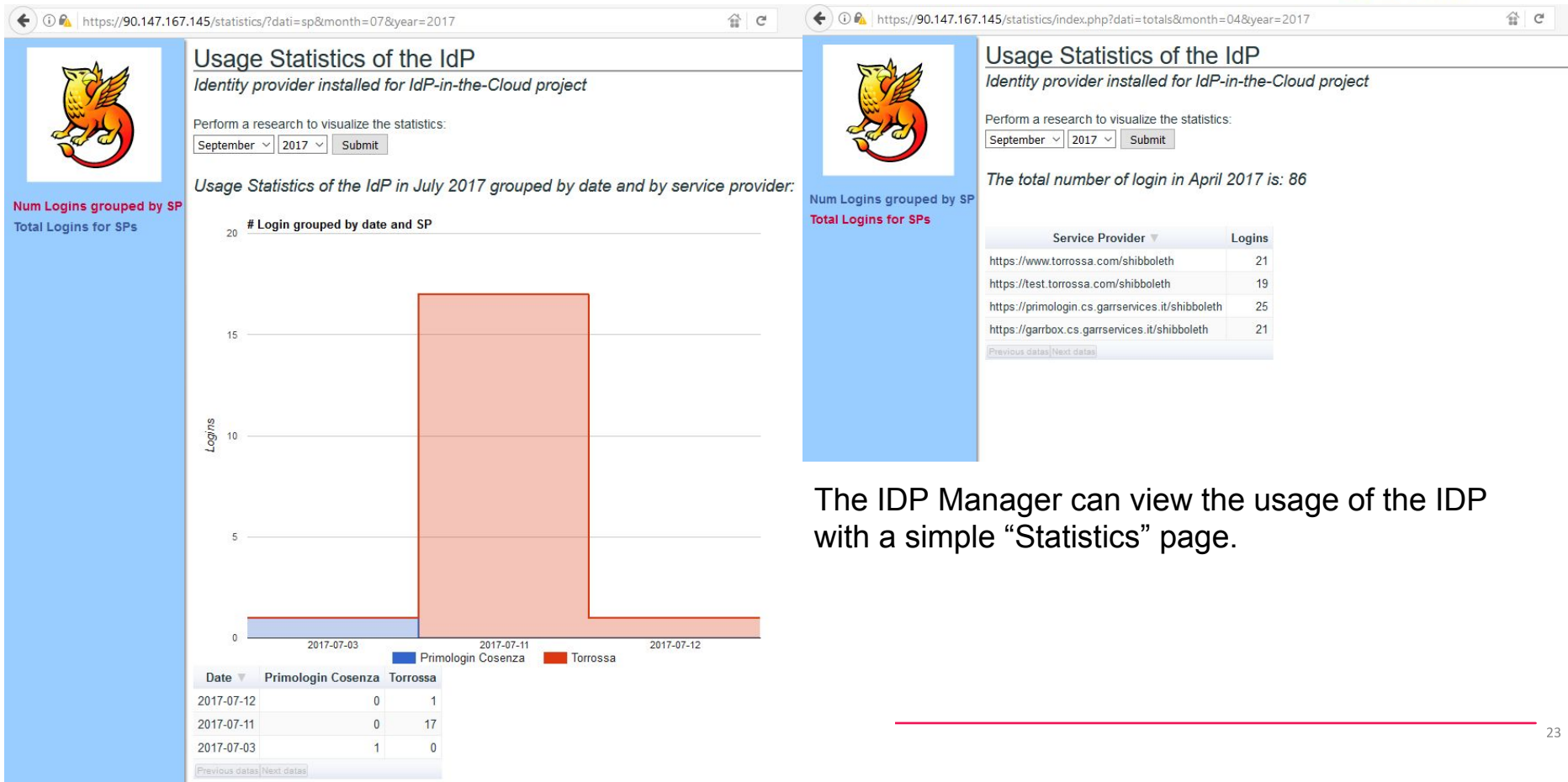
Marco Malavolti

> SP Privacy Policy

> SP Information Page

FOOTER TEXT in english language

Ansible-shibboleth result: Install and Configure a Shibboleth IDP completely



The IDP Manager can view the usage of the IDP with a simple “Statistics” page.

ansible-shibboleth result: Install and Configure a Shibboleth IDP completely

Home

Hint

Consortium GARR LDAP Server

new search refresh

Users (2)

Create Object

Server: Consortium GARR LDAP Server Container: ou=people,dc=garr,dc=it
Template: Identity Provider: New user creation (custom_idpAccount)

Identity Provider: New user creation (Step 1 of 1)

Name * Hint

Surname * Hint

Name and Surname Hint

Username * Hint

Fiscal code * Hint

ORCID Hint

eduPersonAffiliation * Hint


eduPersonEntitlement Hint

Create Object

Identity Management provided by a customized and corrected version of phpLDAPadmin 1.2.3 (latest available)

ansible-shibboleth result: Install and Configure a Shibboleth IDP completely







Start

My LDAP Server

Lock/Unlock of the users

Server: My LDAP Server Content: ou=people,dc=izs,dc=it

Identity Provider: Locking/Unlocking Users

User list	
 Marco Malavolti	User expiration date: <input type="text"/> <input type="button" value="Set user expiration date"/> <input type="button" value="Lock"/>
 Test User	User expiration date: <input type="text"/> <input type="button" value="Set user expiration date"/> <input type="button" value="Lock"/>

1.2.0.5
sourceforge

The IdP manager can lock out the users immediately by pressing on “**Lock**” button, or “**Set an expiration date**” in the future.

- **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



TIER Thematic Requirements / Prioritized

(Least Important) 1 ... 5 (Most Important)

Tuesday, April 12, 2016 2:41:42 PM

Theme / Category / (ID) Requirement

Avg Rating

Solution

Standards and Enforcement

31

The program must assert and enforce: Published / Stable APIs for ALL core components.

5.00

[Unchanged Requirement]

Dep

Rel

Solution

Federation and Inter-Federation

9

Inter-Federation and Federation needs must be held high in considerations when building core solutions and artifacts related to TIER.

4.92

[Unchanged Requirement]

Dep

16

Rel

Person Registry/Provisioning

20

Identity Matching Logic must be a part of the Person Registry Service (Directory)

4.92

[Unchanged Requirement]

Dep

31

Rel

Campus Success

Basic Communications

54

One Pager for general stakeholders (elevator speech)

4.83

[Unchanged Requirement]

Dep

Rel

Solution

De/Provisioning

8

The solutions must enable individuals to have multiple roles/affiliations/relationships/whatever with the institution, each with its own lifecycle and overlapping set of access privileges needed to undertake each role. Statefulness (consistence and preservation of state) must permeate the design goals of all solution

4.83

[Unchanged Requirement]

Dep

Rel

Standards and Enforcement

32

The program must assert and enforce: Published / Stable APIs for ALL core components.

5.00

[Unchanged Requirement]

Dep

Rel

Program Success

Govt

Scale (Le

Driven by IT a

Research Us

Case

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

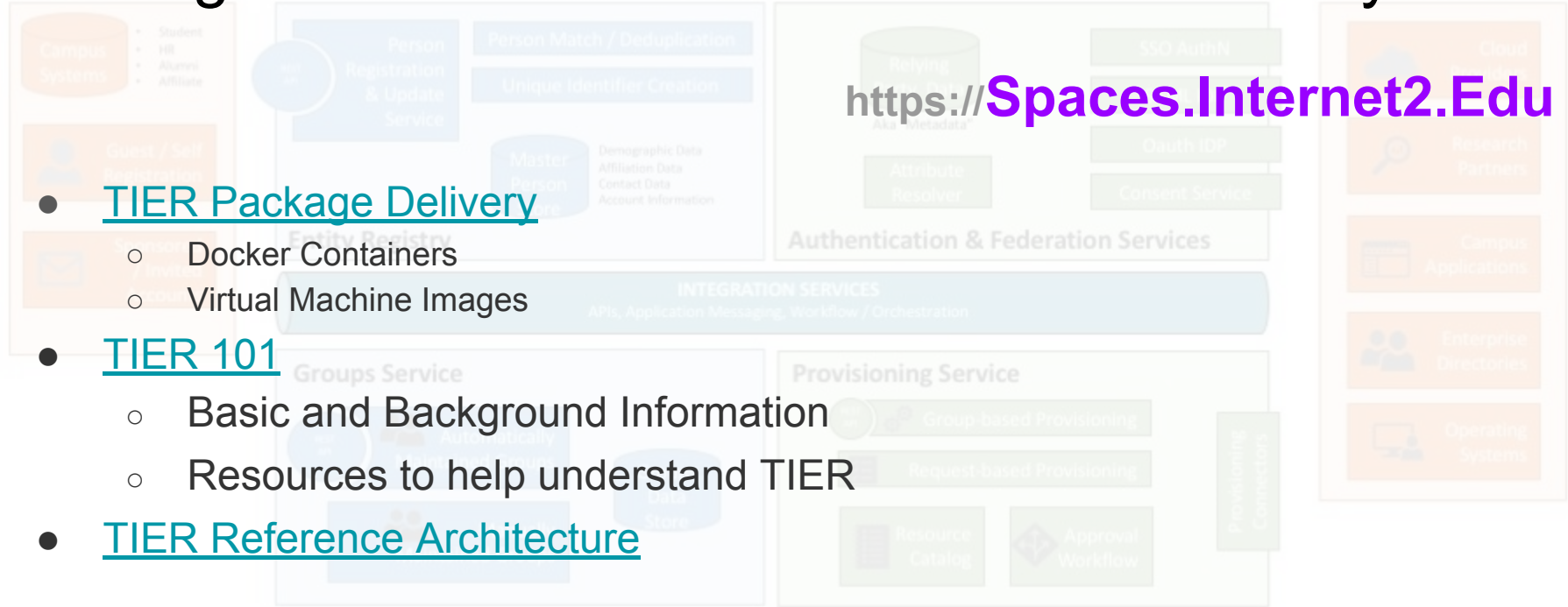
Scope of Sustainability

- The portfolio will be “frozen” to contain “DevOps Friendly” (operationally-oriented), *pre-packaged solutions*:
- Group Management (**Grouper+UI**), Collaborative Organizations Management (**CManage+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

<https://Spaces.Internet2.Edu>

- [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

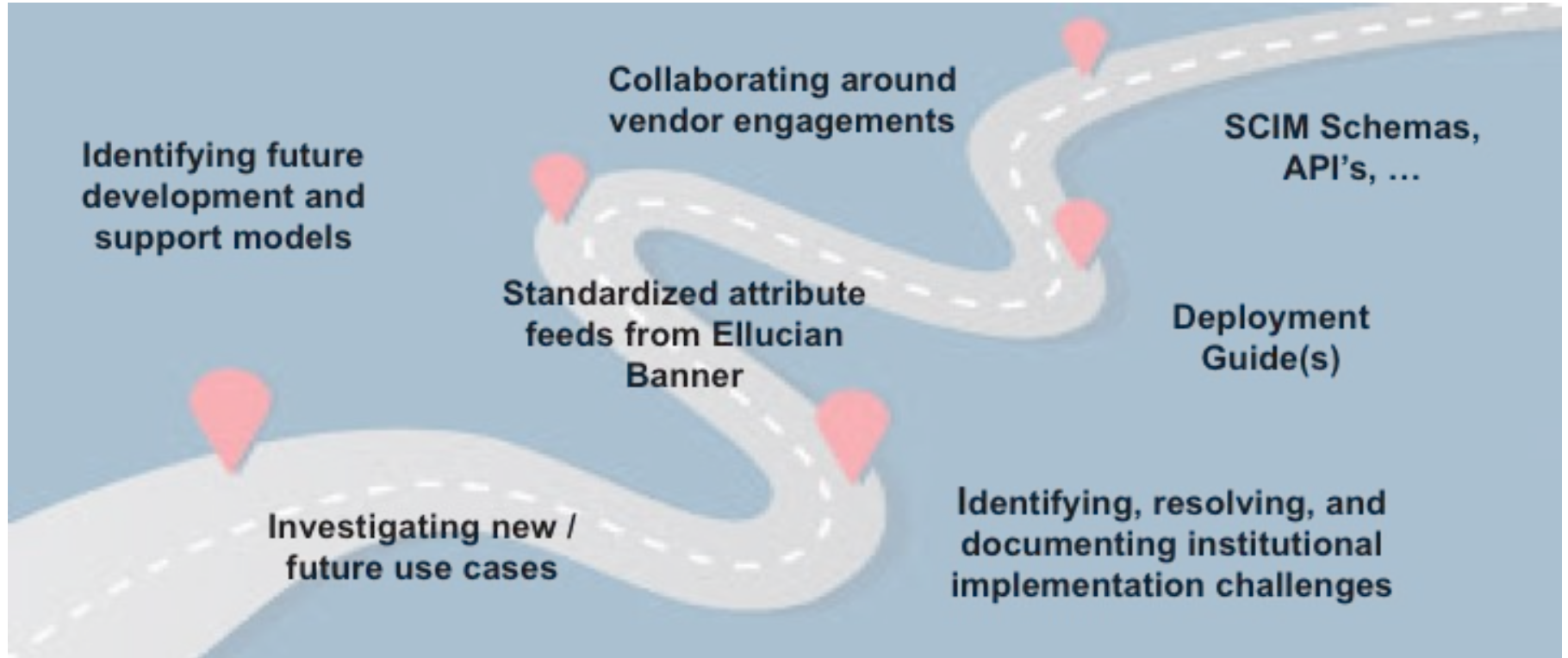
Unique Program Orientation:

- 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



Next Steps and Work In Progress...



Shibboleth®



spherical cow
group



docker
kubernetes
by Google



Division of Information Technology

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.

- 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



Networks · Services · People
www.geant.org