Title:
Campus Identity Providers: Providing and Using Toolkits for Deployments

Presenters' names: Marco Malavolti, Mario Reale, Jack Suess, Ann West
Affiliation*:* GARR, UMBC
Authors names:
Marco Malavolti, Davide Vaghetti, Mario Reale / GARR, Anass Chabli /RENATER, Jan Oppolzer / CESNET, Marko Eremija / AMRES, Janusz Ulanowski / HEANet, Michael Schmidt / LRZ, Valentin Pocotilenco / RENAM, Jack Suess / University of Maryland-Baltimore County, Ann West / Internet2

Five keywords*:* Shibboleth IdP, Ansible, Docker, Toolkit, GEANT Platform

Description:
In this joint presentation by GEANT and Internet2 the tools developed by the Campus IdP task of GEANT will be presented, together with the TIER deployment suite by Internet2. Both solutions are aimed at easing the deployment of Campus Identity Providers by Home Organizations and support and include:

- A comprehensive Ansible suite has been developed to spawn a dedicated Virtual Machine on OpenStack private cloud, install and configure the Shibboleth IdP and all related monitoring, logging and statistics tools .
- An alternative Docker based approach developed in the US by the Internet2 TIER Program and a campus IdP adoption case study of what this is like to deploy.

Background
Campus IdP supporting services task of GEANT project (Gn4.2) has been developing deployment tools for the Shibboleth identity provider, for Home Organizations and interested NRENs to automate the SAML Identity Provider deployment process.
In this presentation the comprehensive toolkit developed in Ansible to spawn Virtual Machines on Openstack Private Cloud, deploy a Shibboleth IdP on top of them, and integrate the Identity Provider with Identity Management tools and a complete monitoring suite based on Check_MK and Elasticsearch, Kibana and Rsyslog will be presented.

The Ansible toolkit is available for the GEANT community to make use of it, targeting specifically less skilled Home Organizations and Campuses, to enable them to join Federated Identity management within eduGAIN.
The Ansible toolkit has been extensively used to deploy at scale IdP instances for the major Research Hospitals in Italy, in the context of GARR involved in a task for the Italian Ministry of Health.
The toolkit will also be the core component of a pilot in GEANT aimed at evaluating the feedback by federation operators on the tool and at demonstrating interoperation with the GEANT Federation-as-a-Service platform.

Beyond the toolkit itself, the current architecture and prototype of the GEANT Campus IdP platform will be sketched. The Platform is based on the toolkit but further aims at consistently integrate the toolkit in a unique system, offered as ad eduGAIN SP to Federation Operators,

by means of which they will be able to automatically spawn IdPs for the Home Institutions and Campuses requiring them, and for HO admins to request their creation.

The Docker-based deployment tools and procedures to spawn the Campus IdP was developed in the US by the Internet2 TIER Program, which is a response to the need for a comprehensive suite of identity services tools and software, and consistent campus identity practices culminating in a common deployment scenario and interoperation at the deployment and operational level. Docker is offered to the GEANT Community as an alternative deployment option with the same goal of easing the Shibboleth IdP deployment for Campuses.

University of Maryland-Baltimore County (UMBC) is an early adopter of the TIER work and a participant in the Campus Success Program; which includes a diverse group of higher education institutions committed to adopting and deploying the TIER software components and helping to accelerate adoption for the rest of the trust and identity community. The goal of the program is work together to define effective practices and enable other campuses to learn from the lessons of the early adopters. UMBC will be presenting their findings during the session, paying particular attention to the challenges associated with replacing legacy systems with modern technology.

Both the Ansible and Docker solutions are aimed at integrating relevant IdP complementary features in a single deployment, like statistics, support for SIRTFI Assurance profile, and Entity Categories and gathering of FTicks for reporting relevant IdP-related information to Federation Operators and HO IdP administrators.

Internet2 and GEANT are in close contact to leverage synergies in addressing Campus IdP related matters, to maximize the positive outcome of collaboration within their users communities, starting by sharing experiences, best practices and tools in the context of REFEDS: the main collaboration items in this domain will be presented.

Marco Malavolti Short Biography

Marco is a software developer and a Federation Operator at GARR, the Italian NREN, and IDEM, the national identity federation.
Marco joined GARR in 2013, where he provided support to the IDEM federation, developing specific recipes for the deployment of SAML Identity and Service providers
He graduated in computer science in 2012 with a thesis on a Comparative study on different Metadata Registries at the University of Bologna, Italy.
During the last years he worked for IDEM GARR AAI on the IdP-in-the-Cloud project (with Ansible) allowing an Organization to create an Identity Provider Shibboleth with minimal effort or specific expertise and he has taken care all recent tutorials provided to the IDEM community for the installation and configuration of several identity and service provider.
He has installed, configured, maintained and updated the current IDEM Entity Registry (based on Edugate Jagger Metadata Registry) and the Shibboleth Metadata Aggregator (MDA) for the generation of IDEM metadata: in particular, Marco has been involved in the automation of the production of federation metadata by means of the MD Registry and MDA.

Mario Reale Short Biography

Mario is a cloud engineer at GARR. He has an educational background in experimental high energy physics, graduation in 1992 and Ph.D in 1997. He then moved to the domain of Grid Computing, joining the first major EU project on Grid in 2001 (DataGrid), working in the domain of grid middleware testing. In the years 2006 to 2011 worked on the IPv6 compliance of Grid middleware and acted as Networking Support task coordinator for the EGI (2009-2013). Since 2014 he works in Cloud computing as a Cloud Engineer at GARR on the OpenStack platform. He is currently task coordinator in the AARC2 project for supporting user communities in the adoption of AAI solutions, liaising with eInfrastructures. He is currently task coordinator of the “Campus IdP Supporting Services” in the GEANT Gn4.2 project.

Jack Suess, Short Biography

Jack Suess is Vice President of Information Technology and Chief Information Officer (CIO) for the University of Maryland, Baltimore County (UMBC). As Vice President, he provides university leadership for information technology at UMBC and serves on the executive leadership team of the university and is responsible for providing information technology services in support of teaching and scholarship, research computing, and administrative support.

Mr. Suess has been active in the R&E community. He was the Principal Investigator (PI) for UMBC in two National Science Foundation advanced networking grants: vBNS (1997) and CC*IIE (2014). He has served as co-Chair of the Higher Education Information Security Council (2003-2006), chaired the REN-ISAC Executive Advisory Board (2006-2013), served on InCommon Steering (2009-2014), Internet2 Board of Directors 2009-2011, IMSglobal Board of Directors (2014-present), and EDUCAUSE Board of Directors (2014-present).

Ann West, Internet2

Ann West serves as the Associate Vice President for Trust and Identity for Internet2. In this role, she works on the InCommon Federation and with the international Research and Education community and corporate partners on collaborative projects and services related to identity services. She also engages the community on TIER, the Internet2 Trust and Identity for Education Program.