The Argus authorization service: a status update

Andrea Ceccanti for the Argus Collaboration

GDB, Apr. 12th 2017

Argus collaboration: alive and kicking!

Steers Argus maintenance, evolution and release

Members

- INFN, NIKHEF, CERN,IN2P3 (maintenance & evolution)
- EGI (release)

Meets regularly on a monthly basis since March 2015

- https://indico.cern.ch/category/6364/
- minutes for each meeting attached to the agenda

Argus 1.7.0

Current release in UMD

- CENTOS 7 and CENTOS 6

Stable

- No GGUS tickets for the Argus SU

Improved performance and scalability

- Especially for large sites (i.e., CERN)

Documentation migrated to ReadTheDocs

- http://argus-documentation.readthedocs.io/en/latest/index.html

Updated dependencies

- Java 8, recent versions of core libraries (Jetty, OpenSAML, VOMS, CANL)
- New integration and load testing test suites

Argus 1.7.1: authentication profiles support

Problem:

- in 2017 not all CAs are equal, different authentication profiles (Level Of Assurance) require different authorization policies

Requirements:

- It should be possible to enable/disable CA LoA for a given supported VO
- CA LoA support should have minimal performance impact
- It should be possible to define complicated policies matching combined LoAs
- A VO must NOT automatically become eligible for all LoAs when new assurance profiles are enabled on the infrastructure

Argus 1.7.1: authentication profiles support

After long discussions, consensus was reached on this proposal

Objectives

- Only allow IOTA CAs for certain VOs (those explicilty allowed by the infrastructure)
  - currently only LHC VOs
- Existing policies continue to work as expected
- Easy upgrade procedure

Implementation under testing

- >80% unit test coverage for the new code, new tests in the integration test suite targeting new functionality
- load testing ongoing

ETA:

- end of April in Argus PT repository, May UMD release

Argus 1.7.1: upgrade procedure

Argus 1.7.1 is a drop-in replacement for 1.7.0

- yum update + reconfiguration + services restart will give a working system that implements the same authorization policies
  - access to resources is only granted to certificates issued by CAs in the classic, slcs and mics IGTF profiles

To enable IOTA CA support for selected VOs, you'll need to:

- install the IOTA CA RPM
- install another, yet-to-be-named RPM providing a VO-CA-AP policy file which states which authentication profiles are enabled for VOs and trusted certificates
- Point your Argus PEPD server to the VO-CA-AP policy file

Detailed instructions on how to do the above will be included in Argus 1.7.1 release notes and documentation

INDIGO-Datacloud AAI/OpenID Connect support

Objective:

- integrate INDIGO-Datacloud AAI to provide consistent and centralized authorization for services that “speak” OpenID Connect
  - any service using OpenID Connect for authN could leverage this integration

Plan:

- Write a PIP to extract authN and authZ information from the OpenID Connect token
- Write a profile that defines how these attributes can be used to write policies

ETA

- September 2017

Argus sustainability

INDIGO-DataCloud funding ends in September

EOSC-Hub (if approved) has some effort for Argus maintenance and “integration”

3PM over 36 months

Clearly not much, but is good that Argus is recognized as a valuable part of EOSC-Hub and there are plans for integration with core EGI AAI services

Currently no major developments are on the todo list besides what will be delivered before September (Authentication Profiles/LoA support, INDIGO AAI integration)

Conclusions

Argus was is non-ideal shape in 2015

- Difficult-to-debug issues and race conditions in some parts of the code made the service potentially unstable, as experienced at CERN
- Unclear sustainability, due to a key partner (SWITCH) leaving the development team

Two years later we are in a much better shape

- A productive collaboration has been set up to coordinate Argus maintenance and evolution
- All known problems have been fixed; Argus has been ported to CENTOS7
- Argus has been evolved to support CA authentication profiles and is being integrated with INDIGO AAI
- Funding (if EOSC-hub is approved) has been secured for the next 3 years for basic maintenance and integration activities