Contribution ID: **145** Type: **Oral Presentation**

Argus, the EMI Authorization Service

Tuesday, 12 April 2011 15:00 (30 minutes)

Overview

Authorization across the EMI middleware stacks (gLite, ARC and UNICORE) is currently not homogeneous, and components often have their own mechanisms of handling it. To address this inconsistency and to unify the authorization process, the Argus Authorization Service was chosen as the EMI solution.

The Argus Authorization Service renders consistent authorization decisions for distributed services (e.g., user interfaces, portals, computing elements, storage elements). The service is based on the XACML standard, and uses authorization policies to determine if a user is allowed or denied to perform a certain action on a particular service.

This presentation introduces the Argus service. Different deployment scenarios are presented, as well as the tools that Argus provide to administrators to manage authorization policies. Furthermore, an update on the status of the integration of Argus with other EMI components is given.

Impact

The Argus Authorization Service is based on XACML; using a standard for authorization eases the integration with other grid components, and provides interoperability across the EMI middleware stacks. Interfacing Argus into Compute Elements as well as Storage Elements will enable to maintain the authorization policies in one service for an entire site. The chaining of different PAPs at the international as well as national level will lead to effective global banning of malicious users during incident handling.
A special focus on the site administrator will be given in this presentation that will allow him/her to better understand the advantages of deploying Argus at his site and the roadmap of integration into other services over the lifetime of the EMI project.

Description of the work

The Argus Authorization Service is composed of three main components.

The Policy Administration Point (PAP) provides the tools to author authorization policies, organize them in the local repository and configure policy distribution among remote PAPs.

The Policy Decision Point (PDP) implements the authorization engine and is responsible for the evaluation of the authorization requests against the XACML policies.

The Policy Enforcement Point Server (PEP Server) ensures the integrity and consistency of the authorization requests received from the PEP clients. Lightweight PEP client libraries are also provided to ease the integration an interoperability with other EMI services or components.

An infrastructure-wide user banning mechanism is a major security feature currently missing in existing deployments despite its importance. This feature can be effectively implemented leveraging the modularity of Argus that allows linking together PAP services deployed at different levels of the infrastructure. Leveraging

the Argus policy distribution mechanism, banning lists can be defined at various levels (european, NGI, institutional etc...) and sites can import such lists so that local authorization mechanisms are aware of malicious users. In order to preserve site autonomy, Argus allows to override policies imported from remote PAPs with local ones, leaving the control of local resources authorization in site administrators' hands.

Authoring XACML policies in XACML itself is not straightforward: XML per se is perceived by many users as difficult to read, and editing can be prone to error. Argus solution to this issue is the Simplified Policy Language (SPL), which facilitates the authoring of policies. Site administrators can write policies in the SPL and import them in the PAP. Polcies are then converted in XACML and stored in the local repository. Command line tools are also provided to add and manipulate commonly used policies.

URL

https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework

Conclusions

The Argus Authorization Service is the solution to render and enforce consistent authorization decisions across the different EMI middleware stacks. Using a standard XACML based authorization service facilitates the integration and interoperability between the different EMI services and eases the authorization management at individual sites.

Primary authors: CECCANTI, Andrea (INFN-CNAF); TSCHOPP, Valery (SWITCH)

Presenters: CECCANTI, Andrea (INFN-CNAF); TSCHOPP, Valery (SWITCH)

Session Classification: Technologies for Distributed Computing

Track Classification: DCI - Implementation