Argus Authorization Framework and SCAS transitional service in gLite

In this note, we attempt to explain the different options for a back-end authorization service in gLite. LCAS and LCMAPS were used as an authorization system for many components. These two services were deployed locally on each host where the authorization decision needed to be made. Some level of site-wide synchronisation was provided by using a shared gridmapdir and pool accounts served by LDAP. LCAS and LCMAPS provide Grid-to-Unix credential mapping using local or VOMS-based input; user, VO and group banning; authentication validation; and credential life time limitations, etc. Also, several third parties have extended LCMAPS with site-local or nationally developed plug-ins.

There are many scenarios where a *centralised* authorization service, that spans multiple site resources (compute, resource brokering, etc.), is preferable. The most urgent use case for such a central service is the use of identity switching and Unix-level sandboxing on the worker nodes in multi-user pilot job (MUPJ) scenarios, implemented through the use of gLExec 'on the worker node'.

Within gLite, two alternatives are currently available to sites: *Argus* and *SCAS* ('site-central authorisation service'). It is not always clear which of these two solutions (or both) should be preferred. *Argus* is the new gLite authorization service, developed in EGEE-III, which is being interfaced to other gLite services to provide a single authorization service at a site as part of the EMI work plan. *SCAS* is a networked service which allows remote invocation of LCAS/LCMAPS instances for central evaluation and mapping. Of these, SCAS is intended as a *transitional solution*, allowing sites to use site-central authorization whilst leveraging the existing infrastructure and configuration known from the LCAS/LCMAPS system.

At this point in time Argus 1.1 provides all functionality that is needed for a 'standard' site in the EGEE grid to perform site-central authorization, and at the same time provides a clear path forward for richer and more flexible authorization decisions, also incorporating off-site policy if so desired.

Suggested deployment options

- If: Sites that currently use Yaim exclusively for installing gLite

➢ Then: continue to use Yaim as provided and deploy an Argus service node.

- If: Sites that use LCAS/LCMAPS with only basic and VOMS plugins and only default ordering of the LCMAPS policies, including those where secondary groups are used for authorization or accounting

➢ Then: choose Argus as the preferred solution.

Then there are several exceptional cases:

- Sites that rely on additional node-local credential mapping (e.g. AFS/K5 integration), or
- Sites that use LCAS/LCMAPS modules that have site-wide effects (such as dynamic groups and automatic LDAP updating),

➢ Then: should consider to either *(i)* keep their node-local system but deploy in addition an Argus node and use the LCMAPS PEP-C plug-in to support central banning, or *(ii)* deploy both SCAS and Argus and use the (Yaim) functionality of 'dual-call' to both systems, if their credential mapping support and benefits from a central service.

- Sites that rely on complicated mappings such as many-to-one account mappings without VOMS and ordering of mapping sequences

➢ should contact the team to see if their use case is already supported by Argus. Some use cases may already be supported. For use cases where non-VOMS proxies are used with pool account mappings, or other more complex mappings, support will be prioritized following mutual agreement.

- Sites that use independently (third-party) developed LCAS/LCMAPS modules for credential mapping based on local or national non-XACML policy systems or attributes that benefit from central evaluation

➢ should consider SCAS, but preferably configure also the 'dual-call' solution from the worker node.

Sites that fall in the category of the above described "exceptional cases" and deploy SCAS should contact the Argus product team and describe their use-case such that the missing functionality can be added to Argus. The Argus PT is committed to make Argus cover all possible deployment options.

When deploying SCAS with central credential mapping in conjunction (sequentially) with Argus, make sure to call Argus first and disable the credential mapping features of Argus. The Argus 'PEP daemon' caches results so that dual call is not expected to add significant overhead.

Issues and remarks

Through the standard use of LCMAPS plugins (pep-c client for Argus or the scas-client for SCAS), and in some cases through service-native calls, all central authorization services (Argus or SCAS) can also be used in other places where the authorization is currently done locally. On the other hand, not all possible scenarios and combination have been (stress) tested. The use of Argus (or SCAS) with gLExec is a certified combination. The use of SCAS with the lcg-CE (Globus GK/GridFTP) has been tested but is not certified, Argus in the same position should work equally well. The integration of Argus into CREAM is currently been done and should become available in fall 2010. In case desired site-local functions or capabilities are not (yet) present in Argus Yaim supports configuring calls to both Argus and SCAS in selected configurations.

For local services that currently use LCMAPS, or when locally developed LCMAPS plug-ins are being used, adding an additional call to Argus for additional (site-central) decision making is a straight-forward and sustainable solution. Argus will over time add more advanced functionality, including execution environment customisations and support for authorizing access to more diverse site-local resources such as VMs. Based on site input and the issues reported, these features can be designed and prioritized for inclusion in Argus. However, such services will not become available for SCAS, which has entered maintenance mode. Meanwhile, SCAS will remain a supported component for as long as customers have it deployed in the operational infrastructure and reported incidents will be analysed and processed.

Summary

Sites should install Argus 1.1, except in the special cases listed. Sites that have special LCAS/LCMAPS plug-ins or configurations deployed as described in "suggested deployment options" should contact the Argus PT and describe their use-case. The PT will then either recommend installing SCAS or Argus or both and advise on the custom installation. If Argus lacks a required functionality, then it will be prioritized together with the site and added in a future release.

A quick-selection guide for site administrators is also available on-line at
https://www.nikhef.nl/grid/gridwiki/index/Central_authorization_service

Support for gLite authorization issues is available at
argus-support@cern.ch