
Fine-grained Authorization for Job and Resource Management using Akenti and Globus

Mary Thompson^{LBL}, Kate Keahey^{ANL},
Sam Lang^{ANL}, Bo Liu^{ANL}, Von Welch^{ANL},
Sam Meder^{ANL}, Abdelilah Essiari^{LBL}



Motivation for Fine-grained Authorization

- A Virtual Organization (VO) wants to provide limited services to its members
 - Allow most users to only run a small number of services but possibly with high resource limits
 - Allow developers to run a wider range of programs such as compilers or debuggers but with stricter resource limits
 - Administrators may want to monitor jobs and kill misbehaving user jobs



Globus GT2 GRAM only does admission control

- Users in the grid-mapfile have the equivalent of a login account on the host.
 - No limit on binaries that can be executed.
 - No limit on compute time or disk resources.
 - All fine-grain authorization is done by OS on the basis of the local user id assigned to the job.
- Users can kill or manage their own jobs, but no other party can.



GRAM (Grid Resource Acquisition and Management) modules

- Gatekeeper
 - Does the admission control based on a static grid-mapfile entry
 - Starts the requested service, e.g. job manager
- Job Manager
 - Parses the Resource Specification Language (RSL) that specifies the binary to be executed, and may specify additional parameters such as CPU time or number of processors needed.
 - Handles requests pertaining to executing jobs
 - Suspend, stop, query



Job Manager authorization

- Does no authorization on job startup
 - Gatekeeper verified that the user has privileges to run on the machine before starting the job manager
- Only allows the initiator of the job to issue job control directives
- Runs with uid of the user so it can only control jobs started by the initial user.



Add authorization callouts from the Job Manager

- Add a generic authorization callout at the points where a job is started
- And when one of the following job managements requests is made
 - Cancel, suspend, resume, ask for status, change priority of job
 - register or deregister a call-back contact
 - stop or restart the job manager process that is watching the job



Information Passed to Authorization Call

- gss_context of job initiator
- gss_context of requester
- Static job-group, dynamic job id
- action requested
- RSL for the request
 - On job start the RSL may specify parameters that need to be controlled such as:
 - Number of CPUs requested
 - CPU time needed
 - Queue (or priority) desired



GSS Context

- Generic Security Service Context (IETF RFC 2744)
- For GSI implementations this contains
 - Requestor's X.509 proxy certificate
 - Requestor's Distinguished Name
 - Acceptor's name
 - Intended use
 - Cryptographic state – shared session keys



Akenti Authorization Server

- Authorization policy created by independent stakeholder as digitally signed certificates.
- Requestors are identified by X.509 certificates or DN and CA's DN.
- Resource gateway asks for a authorization decision based on a resource name and the requestor's identity.
- Akenti finds (pulls) all the relevant authorization policy and returns allowed actions and conditional actions.
- Conditional actions may specify runtime conditions that the resource gateway must evaluate.



Akenti Authorization plug-in

- Handles the interface between the Job Manager and the Akenti authorization service.
- Extracts X.509 proxy certificate from GSS_CTX
- Maps Globus resource name e.g. pathname of binary or job tag to an Akenti policy resource name.
- Interprets Akenti response.
 - Evaluates runtime conditions
 - Policy might limit number of CPUs used
 - Maps Akenti actions to Globus actions
 - e.g. “control job” to cancel job, get job status, suspend, resume, etc.
- Returns allowed or disallowed answer to Job Manager and a Globus Error object.



Status

- Two prototypes with progressively refined functionalities have been built and were demonstrated at Fusion Physics meetings (TTF and Sherwood Theory) Apr. '02 and SC02 in Nov.'02
- Production version currently under development
- Plan to release modified Job manager as part of a future GT2 release. (hopefully 2.4)
- Akenti interface module will be released as a user contributed plug-in to GT2
- Akenti server currently released as open source software by LBNL



Future Work

- Globus Tool kit is evolving to Open Grid Services
- Globus is working with input from GGF to define a generic authorization service API.
- Akenti has been wrapped by Python as a Grid service and a SOAP interface to the server has recently been added.
- It will become an instance of a pull model Grid Authorization service.



Project web sites

- Akenti
 - <http://www-itg.lbl.gov/Akenti>
- Globus
 - <http://www.globus.org>
- Fusion Grid
 - <http://www.fusiongrid.org>

