2014-04-22 XACML AuthZ Design Meeting

Date

Apr 21, 2014, 2:00pm - Google Hangout

Attendees

- Greg Jansen
- Unknown User (bbpennel)
- Mike Daines
- Kevin S. Clarke
- Eric James

Goals

- Address concerns with current design:
  - persistence of ACLs for external nodes
  - limitations of implemented inheritance/override model
- Overview of XACML policies and policy sets
- peek at the JBOSS policy engine
- Begin a new XACML design page, i.e. mapping XACML to fedora authz delegate, etc..
  - How to specify effective XACML policies for a given node/region?
  - How and where to persist policy objects?
- How to map Fedora metadata into XACML request/context attributes
  - which attributes are always in the XACML request context?
  - which attributes are also available to policies via the attribute finder?
- More???

Discussion Items

Time	Item	Who	Notes
5min	Overview, review goals & wiki page	Greg	
5min	Review AuthZ delegate api	Mike	
5min	XACML Policies and JBoss PDP	Greg	
20min	Identify some XACML implementation alternatives	All	Starting out we favor an internal PDP (configured as a bean within the webapp). The code can be in a separate project.
15min	Role inheritance/persistence (Hydra rights, rbacl, XACML etc..)	Greg	
15min	What can we do in this sprint?	All	

Action Items

- Kevin S. Clarke Investigate what data is available on incoming authz requests for newly created objects, i.e. in Session
- Do we have enough information via the Path parameter to determine access for metadata? (Implementation-specific identification of readable metadata)
- Eric James Identify trade-offs for different acl persistence strategies.
- Greg Jansen Elaborate on the design enough to make it a topic of the commiter call. (Outline the APIs used and take a use case through the entire sequence of events.)