2015-09-16 - WebAccessControl Authorization Delegate Planning Meeting

Time/Place

- Time: 3:00pm Eastern Daylight Time US (UTC-4)
- Call-in:
  - U.S.A/Canada toll free: 866-740-1260, participant code: 2257295
  - International toll free: http://www.readytalk.com/intl

Attendees

- David Wilcox
- Andrew Woods
- Nick Ruest
- Ben Wallberg
- Unknown User (acoburn)
- Jared Whiklo

Agenda

1. Collect stakeholder feedback on Sprint 1
2. Review Phase1 scope/use-cases
   a. Allow admin agent to always have full access to resources and ACLs
   b. Allow admin agent to CRUD ACLs
   c. Allow admin agent to assign ACLs to resources
   d. Allow a specific agent to READ a resource
   e. Allow a specific agent to READ and WRITE a resource
   f. Allow a specific agent to CREATE a resource, but not update it
   g. Allow a specific agent to assign an ACL
   h. Allow a class of agent to do the above (d - g)
   i. Allow a specific agent to do the above over a class of resources (d - g)
   j. Allow a class of agent to do the above over a class of resources (d - g)
   k. When access is denied return a 403 and a body (or link header) with cause
3. What Phase1 requirements must be addressed in Sprint2?
   a. Link header
   b. Remote ACLs
   c. ...
4. Schedule second sprint
5. Discuss Phase2 scope/use-cases
   a. Allow a request from a specific I.P. address (or range?) to do the above for a resource and a class of resources (2.d - g)
   b. Enforce authorization policy on a resource (or class of resources) based on that resource's association to a licenses (or tag)
   c. Enforce datetime sensitive authorization polices (i.e. embargos / leases)
   d. Allow authorization decisions based on nested ACLs (i.e. acl:include)
   e. Demonstrate pattern for enforcing the same authorization decisions as found in the repository in the context of Solr queries

Related Documents

- https://www.w3.org/wiki/WebAccessControl
- https://github.com/duraspace/pcdm/wiki#webacl
- Authorization Delegates
- http://www.w3.org/ns/auth/acl

Minutes

Facilitate Stakeholder Verification

- Enable WebAC feature in fcrepo4-vagrant
- Script the creation of resources and ACLs that correspond to stakeholder use cases
  - **Stakeholders should provide additional use cases/scenarios as needed to help round out the verification**

Sprint 2 Items to address

1. Allow a specific agent to CREATE a resource, but not update it
2. Currently, ACL resources are protected like other repository resources. Add special protection for ACL resources
3. Implement "agent class" support:

    a. For agent classes that are found within the repository
    b. For agent classes that are found external to the repository (*stretch, do stakeholders want this?*)
    c. Allow repository admins to turn of "agent class" capability
4. Implement "remote ACLs", *if stakeholders view it as a priority*
5. *Stretch goal:* acl:include

Note: Since the WebAC "specification" does not have provisions for time-based authorization, the proposal is to move logic for policies such as leases or embargoes up into the application layer. Question for stakeholders, *Is that reasonable?*