2013-07-29 FF Tech Mtg

Attendees

- Andrew Woods ⭐
- Greg Jansen
- Osman Din
- Scott Prater
- Bruce Barton
- A. Soroka

General

- Indicates who took minutes - ⭐
- Call-in: Google-hangout at:
    - https://plus.google.com/hangouts/_/event/ccnv0ba94h3fb2je3gscunqc49g

Agenda

1. Plan Sprint b1
    a. Themes
        i. AuthN/Z - next steps
        ii. Policy driven storage - next steps

Minutes

General

1. Scott to begin participating this week: Aug
2. Scott to create diagram auth diagram and submit to mailing list
3. PivotalTracker tickets: https://www.pivotaltracker.com/s/projects/684825

AuthN/Z

1. Greg
    - Coming from f3 perspective
    - Looking for something that is pluggable, but with a strong contract
    - Interested in jboss/xacml role-based
2. Scott
    - Want loose coupling of auth and fedora
    - Fedora gets atts, pass them to pdp
    - PDP decides if item is accessible
3. Greg
    - Want at least some metadata conventions that impls can rely on
    - Need conventions for roles
    - How to determine role from shib?
4. Scott
    - What roles would f4 be interested in?
    - External pdp defines expected roles rights
    - Need a central place for all applications to check for access rights
5. Conceptual Flow
    a. Atts collected
        - atts from shib
        - obj id
        - function trying to be performed
        - ?is policy stored in f4?
    b. Some users will want a default impl
    - There may be two kinds of tasks:
        - Come up with api and default impl
            - Default impl is useful for examples for the community
        - Allow not using default impl
6. Scott
    - Interest in keeping policies external to f4
    - There is a need to make the same policy decisions in other components of the university infrastructure
7. Greg
    - Agree, concern that policy in the repo creates security risk
8. If policies are external, how to achieve fine-grained access control?
    - Policies can be written to restrict by datastream names
    - Should pdp be able to call back into the repo?
        - This could introduce a significant performance hit

9. Adam
    - OAuth allows machine to act on a resource on behalf of a user
    - Credentials last for a defined amount of time
    - We can define oauth "scopes"
        - Additional level of policy granularity will be needed
        - Use the hierarchy of jcr to drive access control
        - Scope: crud and repo geography
10. Bruce
    - Interest in possibility of not managing pdp themselves
    - (Adam) Suggestion: accessing the external pdp through F4 API may work
11. Goals from sprint b1
    - a. Greg
        - Write up contract of pdp
        - Explore jboss impl?
        - Users a,b,c can log in, and have different rights
    - b. Bruce
        - Willing to validate outcome of sprint
    - c. Adam
        - Suggest getting Michael Durbin onto the line, and Scott Turnbull
    - d. Osman
        - Need to be able to integrate CAS

Policy driven storage

Add tickets

1. Make policies hot swappable
2. Need policy validation
3. Need a "property-language" for storage
4. Need an iRODS connector

Closing Comments

1. jaychen (VaTech), is working on aptrust bagit connector
2. Bagit tickets need editing/grooming

Actions

- Greg Jansen to organize auth tickets
- Greg Jansen to connect jaychen with F4 development effort