Shibboleth Thread

Return to parent thread

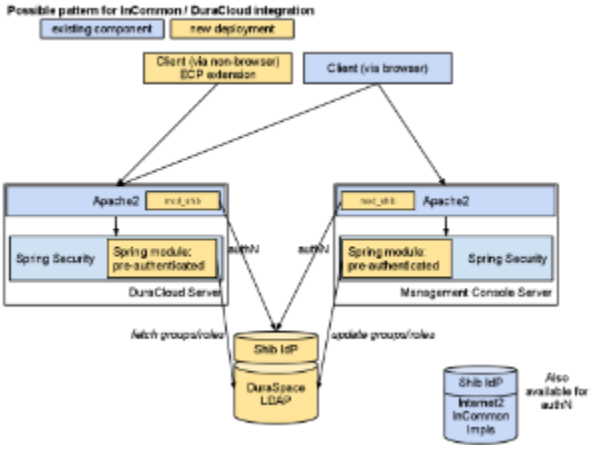
Shibboleth

Shibboleth is an implementation of SAML in use by many higher education institutions and is required by Internet2. This thread discusses the investigation of Shibboleth for use in DfR and how it could fit in the implementation.and service.

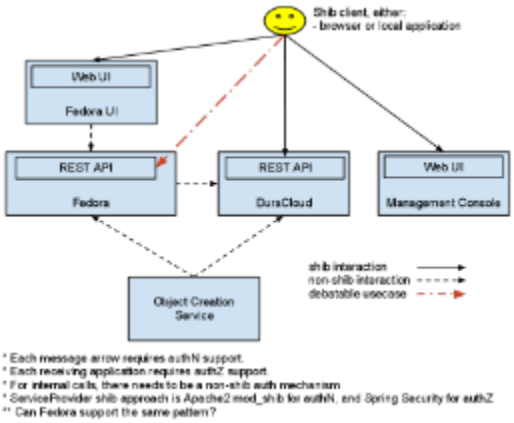
Issues

How do we handle institutions that don't have Shibboleth?

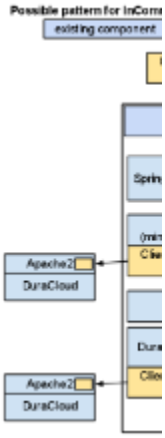
Design



Auth for Management Console



DfR Auth Interactions



Auth for DuraCloud

(Editable source DfR Auth Interactions)
(Editable source Auth for Management Console)
(Editable source Auth for DuraCloud)

Components

Identity Provider (IdP)

- DuraSpace implementation
    1. CAS Server exposed as Shib IdP
    2. or LDAP / JAAS Shib IdP

Identity Provider Discovery Service

- This service determines in an automated or user-driven manner the selection of which IdP to use.
- We will likely include InCommon and the DuraSpace IdP.

Service Provider (SP)

- Considerations
    1. Do we want the DuraCloud webapps to participate in a Shib/SAML interaction? or do we want the webapps to assume a pre-authentication context?
        - Likewise for Fedora
    2. Since we can not assume that the InCommon IdP will provide the roles and groups needed in DuraCloud, those details must be available to the DuraCloud webapps through another mechanism
        a. DuraSpace LDAP?
        b. DuraSpace CAS server, potentially over a DuraSpace LDAP?
    - Therefore, DuraCloud users would need to login to the DuraCloud Management Console (MC) to set up roles and groups... meaning the MC will also need to be Shibbolized.

Client

- In order to support browser-less Shib clients, we will likely want to leverage existing Enhanced Client or Proxies (ECP)

Discussion

1. Need to retain userId in association with content throughout DfR interactions
2. Shib not necessary with internal "system" interactions
    - object creation service
    - cloudsync
3. May be necessary to allow non-shib authN for internal calls
    - investigate support in mod_shib

Questions

1. How does authN between islandora and fedora currently work?
2. Would Islandora be interested in using/leveraging DuraCloud groups from DuraSpace LDAP with Fedora policies

h4. Related Materials

1. CAS
    - https://wiki.jasig.org/display/CASUM/Shibboleth-CAS+Integration
    - https://wiki.jasig.org/display/CASUM/RESTful+API
    - http://code.google.com/p/casshib/
2. SAML
    - https://jira.springsource.org/browse/SEC-1004
    - https://jira.springsource.org/secure/attachment/15148/SpringSecurity+SAML+-+documentation.pdf
3. Spring-Security
    - http://static.springsource.org/spring-security/site/docs/3.1.x/reference/springsecurity.html
4. Shibboleth
    - http://code.google.com/apis/apps/articles/shibboleth2.0.html
    - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig
    - https://wiki.shibboleth.net/confluence/display/SHIB2/ECP
    - http://wiki.aaf.edu.au/aaf-mini-grants/tpac/shibboleth-integration-with-spring-security
5. OAuth
    - http://code.google.com/apis/accounts/docs/OAuth2.html
    - http://code.google.com/apis/accounts/docs/OAuth.html

Return to parent thread