

test meeting notes transfer from google docs

CIFER Provisioning and Integration Team Meeting, Tuesday, April 15, 4:00 pm Eastern, 1:00 pm Pacific

Dial-in numbers:

+1-734-615-7474 (Please use if you do not pay for Long Distance),

+1-866-411-0013 (toll free US/Canada Only)

Access code: 0145272# NOTE: New pin for all calls going forward

Paired with an Adobe Connect Meeting for screen sharing:

<http://wisc.adobeconnect.com/cifer-prov/> open for presentation

Participants: KeithH, BillT, JimmyV, DavidL, PatrickR, GaryW,

AGENDA

<http://wisc.adobeconnect.com/cprmessaging/>

1) Affiliation lifecycles at U Chicago (Adobe Connect slides from David Langenberg)

<https://docs.google.com/presentation/d/1W-7WNnULPOYv2I5oacq84CSYt4brTyPEe5h0gqRG2xM/edit?usp=sharing>

<https://answers.uchicago.edu/page.php?id=16003> closure rules at U Chicago

- since 2008, NetIDs not "closed", access to services is revoked instead (via Grouper)
- closure grace period now 45 days instead of two weeks; partial lockouts begin at 10 days to get users' attention
- two trees of affiliations: current and effective (current plus transition)
- how do you catch "fell out of eligibility" events? Current_individual master group: when you disappear from that view, that triggers entrance into closure process;
- division of labor between Grouper and Closure app? Mostly has to do with evolution of Grouper since 2008;
- "Person Reg tracks eligibility": for an eduPerson affiliation; underpinnings are data feeds from across campus; 50 views of registry: current affiliations pushed into Grouper; Grouper controls ePAffil values in LDAP; Open Reg. terminology for this process is "calculation"; how does overall system know what services a particular affil grants user? e.g. affil:effective:postdoc gets you into "modem pool eligible" group;
- Have lawyers ever challenged rules for closure grace period? Not really;
- Pushing people from using LDAP for AuthZ to using Grouper;
- Do you get asked for broad audit for who has audit to what services? Maintain an external audit report, short of digging into Grouper logs and hierarchies; DavidL: IdM Services Dashboard has big services listed with their status; Where do I go to see what the rule is? Call DavidL; BillT: potential customers always asking about what kind of audit reports are available; what policies are in effect; DavidL: Registrar gets a spreadsheet that shows them the detailed breakdown;
- Most of provisioning coming out of Grouper is to the affiliation and eligibility groups; direct provisioning to services: Portal uses grouper web services; if you're shibbed, we push isMemberOf; federated, we can push entitlement;
- Google apps: we're good at creating services when you show up; not so good at adding a services somewhere later; we try to anticipate what services you might ever need; Not many need pre-provisioning; Many are just in time; SAML assertion is what gets you in; or it will have the entitlement that maps to the site license; closure process does apply to the Google case and does a deprovisioning step;

2) CPR --> LDAP; Grouper LDAP provisioning in IAM Testbed:

- Build out more unix-style simple tools for simple tasks; LDAP provisioner would just talk to LDAP, maybe for version 2.3;

3) Scott Koranda question to grouper-users list on Grouper LDAP via Messaging

Hello,

At the recent Grouper BOF held at the Internet2 Global Summit a number of campuses indicated they have or will be writing custom Grouper change log consumers that write some change log entries into message brokers so that consumers may read the messages and take appropriate provisioning actions. Provisioning into Google was mentioned a number of times. The message broker mentioned most often during the meeting was ActiveMQ.

If your campus is taking this approach I would be grateful if you could reply with the flavor of message broker you are using or planning on using. I am curious to see if there is a consensus on the message broker of choice. I am happy to record the results in the Grouper wiki.

I am also curious to understand what format campuses are using for the messages themselves? Is there an emerging standard or best practice?

Thank you for your consideration.

Cheers, Scott K

UPCOMING CALLS:

29 April 2014