COmanage Call 9-Dec-2011

Minutes: COmanage-TAC call 9-Dec-2011

Attending

Heather Flanagan, Internet2 (Chair)
Ken Klingenstein, Internet2
Steven Carmody, Brown U.
Keith Hazelton, University of Wisconsin - Madison
Benn Oshrin, Internet2
Scott Koranda, U. Wisconsin - Milwaukee (LIGO)
Steve Olshansky, Internet2
Emily Eisbruch, scribe

Carry Over Action Items

[AI] (Heather) will set up meetings with IRODS/iPlant/Internet2 in January
[AI] (Keith) will check whether the Project Bamboo IAM infrastructure work plan is available on the wiki, and if yes, he will send the group a link.
[AI] (Steven) will develop a one-page write-up on attribute aggregation.

DISCUSSION

Update from LIGO Meetings in Pasadena

Benn reported that LIGO meetings in Pasadena have been going well.

- Getting close to being ready to tag the COmanage 0.3 release
- This release does not include major external facing changes
- There are some changes to how data is handled, teasing apart the person level data from role level data
- Goal is to have work to demo for the LIGO meeting in March and Internet2 SMM in April
- After the COmanage 0.3 release, the plan is to start working on the new UI and on the enrollment workflows
- There will also be work on upgrading the php framework
- Benn plans to update the Jiras: https://bugs.internet2.edu/jira/browse/CO
- There is a specific LIGO use case that is driving the current development work
- Additional LIGO use cases will be addressed in the future

A new issue "web directory" issue for the roadmap has emerged:
- LIGO's roster is their web directory
- They hope to rebuild that in the March/ April 2012 timeframe
- Web directory is not a unique problem to solve, every site seems to write their own product
- Hope is to introduce a new parallel product to the registry, called the COmanage directory
- Envision this COmanage directory as a stand-alone web people search product
- Every university has one

There are two modes:
1. Stand alone LDAP front end
2. A web directory deployed next to the COmanage registry

- should there be direct integration and ability to edit data in registry?
- that is now on the radar as a proposal
- stems from needs COmanage has re authenticated vs unauthenticated access to roster
- it's a quarter-baked idea now, with some initial requirements, have not committed to a particular path

Q: in terms of directory style service, everyone writes their own, can we just use someone else's?

A: Benn: No, have looked into this, but mostly they are not open source, not in a package state

Q: Would there be anything in OSIDM4HE that we could use for the directory?

A: Benn: Not right now, but this would belong in that space, would be good to add "web front end" to things being addressed in OSIDM4HE

ScottK commented that the recent Pasadena LIGO work, with Benn onsite, was productive, time well spent

Changing Roles (user as administrator, user as PI)

Ken: An issue that may come up in upcoming meetings with energy labs is about defining/switching roles in the COmanage environment:

The question could be stated:
- "Sometimes I want to switch roles online, for example, first doing things in my role as the lab administrator and then switching to doing things in my role as the PI.
- How does COmanage handle those in terms of authentication and privileges?"

- Keith noted that the application should be able to determine if the person signing in has the correct role to take certain actions.
- So the user should not have to be aware of switching roles
- Roles should be handled in the SAML attribute assertion process

- Ken: perhaps folks will want a GUI to make it explicit that they are switching roles (backing out of one role and into another)
- Like wanting a different physical key to drive a different vehicle or enter a different building
- But perhaps the answer is that it could be transparent, which would be great

- Would there be something in COmanage that would say which role do you want to initially step into?
- For example, you step up as Lab Administrator and you see the apps available?
- Roles can have apps associated with them, so is it possible to gather them in portals and say, you have switched roles, here are the apps you can use?
- some way of putting rubber band around those apps could be good

- Heather: switching roles has been discussed in LIGO context
- A use case involving access to documents: https://spaces.at.internet2.edu/display/macepaccman/LIGO+Document+Management
- Also there could be a case where if you want to use a certain instrument you'd need a higher level of assurance account

- ScottK noted that LIGO has one use case where people switch roles, and this is handled by group affiliation.
- Also there are some new use cases arising with collaborations involving LIGO researchers and researchers affiliated with the Japanese interferometer group.

Updates from Ken

- Ken was in Tokyo recently for an event around OpenID
- In Japan, there is a need for SAML to Social gateway
- The SAML user base is larger; there is no trusted OpenID provider
- Ken shared with the Japanese what has been done here concerning federated ID

- Ken met with the NII group, and discussed their equivalent of COmanage ,,, they work with Swiss approach
- They have not yet tackled provisioning or attribute aggregation issues
- There are questions around identity credential conversion
- We need to work together more, harness the community
- Looking tentatively at a meeting time around 2011 SMM
- Possibility of NSF or TERENA sponsorship
- Ken will know more about sponsorship after discussions next week