COmanage Call 2-Sep-2011

Minutes: COmanage-TAC call 2-Sept-2011

Attending

Heather Flanagan, Internet2 (Chair)
Ken Klingenstein, Internet2
Benn Oshrin, Internet2
Keith Hazelton, University of Wisconsin
Steven Carmody, Brown
Tom Barton, U. Chicago
Steve Olshansky, Internet2
Emily Eisbruch, Internet2 (scribe)

New Action Items

[AI] (Heather) will adjust the MACE glossary definitions of "action" and "inheritance" based on the discussion on the call.

[AI] (Heather) will check that everything in simple glossary is also in MACE glossary.   https://spaces.at.internet2.edu/display/macepaccman/Another+Glossary+Page

Carry Over Action Items

[AI] (Steven) will send Ken details on the Commerce Dept. safe harbor issue.

[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] (Ken) will send out a link to the Eve Maler presentation from the July 2011 Cloud Identity Summit.

[AI] (Keith) will start a problem statement on the need for a "virtual Switzerland."
[AI] (Keith) will send a pointer to OpenSearch information

[AI] (Ken) will provide a link to the French listing regarding applications and sets/bundles of attributes.

[AI] (Steven) will develop a one-page write-up on attribute aggregation.

DISCUSSION

Glossary

Heather and TomD have been working on the MACE glossary and the Simple Glossary:

- https://spaces.at.internet2.edu/display/macepaccman/Another+Glossary+Page
  (in particular, "action" and "inheritance")

Current Definitions:

Inheritance: An object can imply indirect privileges due to inherited privileges of another object. Inheritance can be found in roles, resources, or actions. e.g. the role SeniorAdmin inherits all the privileges from the role Admin, and adds a few more.

Action: Describes the access to a resource e.g. "delete","add" , "reserve". Often used interchanged with function and verb

- TomB commented that this definition of inheritance could be too specific, too Grouper centric.
- We want a broad community to be able to understand the definitions.
- TomB noted that an inheritance generally flows down a tree, there is a hierarchy along which things are inherited, and this is what should be stated in the glossary (drop the part about roles, resources or actions)

[AI] (Heather) will adjust the MACE glossary definitions of "action" and "inheritance" based on the discussion on the call.

TomB asked if everything in the simple glossary should also be in the MACE glossary. Currently "Action" does not appear in the MACE glossary.

[AI] (Heather) will check that everything in simple glossary is also in MACE glossary.

Feedback on Statement of Work for Tom Zeller

TomZ is now working for Unicon, and they have provided for 20-24 hours per week of TomZ's time to be devoted to Internet2 work. What are the projects and priorities for TomZ's Internet2 time? Heather is coordinating a call to discuss this with Ken and TomB. She would like the COmanage-TAC group's input.

Currently on the list:
* Continue to develop, maintain, and support provisioning software and projects .
(estimated 10 hours per week, which includes dev calls)
* Contribute to the development of Shibboleth. (estimated 10 hours per week, which
includes dev calls)
* Participate in standards work related to provisioning, including OASIS PSTC, OASIS
SSTC, and SCIM. (estimated 2 hours per week)
* Participate in Internet2 working groups as needed, including OSIDM4HE, MACE-dir,
MACE-paccman, etc. (estimated 2 hours per week)

- StevenC: What do we want to see in the Middleware Initiative 12 months from now? Released code? Standards pushed forward? Proof of concept implementations?
- Heather noted that the SURFnet team has been discussing an enterprise provisioning tool that could fit in a VO context.

Q:: How is that enterprise provisioning tool different from what could come out of the OSIdM4HE initiative? https://spaces.at.internet2.edu/display/OSIdM4HE/OSIdM4HE+Initiative
A: We don't know yet, since OSIdM4HE is in such early stages.

- TomB noted that TomZ has been the maintainer of LDAPPC-NG with the Grouper project
- LDAPPC-NG is a provisioning tool that goes beyond Grouper
- LDAPPC-NG builds on the Nexus work of Walter Hoehn http://www.internet2.edu/presentations/spring06/20060425-middleware-hoehn.pdf
- Steven commented that Brown does not use LDAPPC-NG, and is headed towards an event driven design, using a message bus and a variety of listeners
- TomB said that LDAPPC-NG is composed of different parts and has several distinct functions
- The parts that update targets are separable from the parts that announce there is an update that needs to be done
- The front end of LDAPPC-NG -- the part that picks up that an event needs to be done --- will be event based with Grouper 2.1
- Grouper 2.1 will have real time incremental provisioning
- Can potentially put that directly on an ESB
- There is a need to be able to create some rules that control provisioning, whether for provisioning groups info or for permissions info

- Benn: the Dutch are interested in the enterprise provisioning level (as opposed to federated provisioning level)
- There is a the central repository of info and it is used to drive actions, such as adding or removing info from target systems
- This describes what COmanage is going to do
- Federated provisioning is more of a point to point process
- Steven: when I register at a VO site, accompanied by attributes asserted by my home organization, that might be done via the federated mechanism
- Within the VO, once I'm registered, the event-driven approach would be used, with rules engines and SPML or SCIM on outboard side
- The first part, where you register with attributes is a complicated issue, but Steven is engaged in working groups looking at ways to simplify it

- TomB: thinking of federated provisioning and the SDCI grant, a VO member comes on board and VO resources (such as a wiki) need to be provisioned to enable their participation, so it's like enterprise provisioning

- Ken: Does account linking play a part in these issues? Account linking has been discussed related to box.net
- WIth Box.net, there is the issue of a user who used box.net with an email from their institution
- How to handle that when their institution becomes a box.net account?

- Benn: Yes, there is overlap w account linking issues.
- Use case: I have one identity from this IdP and I log in with another identity from another IdP
- TomB: With federated attributes, it has been scoped down to display name, email address and a persistent identifier -- those are the 3 main things people are concerned with for VOs
- Ken: class enrollments will play a role as well

- Heather: it's clear that Enterprise Provisioning is an area the TomZ could continue work on.
- This will be discussed further at a call next week.

InCommon Access to Research.gov

Heather reported that she looked into the issue of using InCommon credentials to gain authenticated access to the www.research.gov site.
She found that Mike LaHaye was already working on this. It has now been set up. See details at:

https://www.research.gov/research-portal/appmanager/base/desktop?_nfpb=true&_pageLabel=research_node_display&_nodePath=/researchGov/Generic/Common/InCommonURLS.html

Project Bamboo

Keith asked which version of COmanage he should use for the Project Bamboo work currently going on.
Benn suggested version 0.2

Keith is interested in the SURFconext integration, in drafting SURFconext onto the comanage gears (registry).
Benn said there is not work on this right now. Keith may become the expert in this area.

Next COmanage Call: Friday, Sept. 16 at 2pm ET