Meeting Notes 2015-12-03

Date
03 Dec 2015

Attendees
- Unknown User (tfleury)
- Unknown User (awithers)
- Donald Petravick
- Unknown User (jalt)
- Margaret Gelman
- Unknown User (dnthayer)
- James Basney
- Unknown User (xiuqin)
- Gregory Dubois-Felsmann
- Unknown User (jar)

Goals
- Discuss Granting Data Access Rights

Meeting Transcript

Jim B - Our focus today is on the wiki document Granting Data Access Rights. What prompted this topic? Several weeks ago, met with developers of Internet2's Comanage software. There was a conversation about onboarding users with LIGO. Any feedback from today's call can be shared with Comanage development team.

Review Granting Data Access Rights

Possibly have a light weight sign up process with post-review. Or is it better to have a pre-review process? What is the right balance?

Don - How accurate are the automatic filters? Is it a principle that we give out data rights? How is it constrained by quality of analysis?

Jim - For example, we want to have a decision in 1 business day. Or we want no more than 1 false positive per month.

don - Depends on the policy and how tight the filters are

Jason - Not comfortable with giving people access optimistically.

Don - We fail if we end up with a process like teragrid

Gregory - Echoes Don's statements. We are trying to work out the available technology. We are not going to be deciding policy.

Jim - 1st tech option - grant data rights based on campus attributes. Key attribute is eduPerson Scoped Affiliation. "member" is a person in good standing with the university. This may be good for automatic. As Gregory commented, it would be useful to have more info for additional attributes (e.g., grad student, post-doc, etc.)

Next case - if user's home campus doesn't have an InCommon Identity Provider, we need another process. User clicks "Apply for data access rights" button, fills out form. LSST admin checks form against campus registry to match email address and verifies university affiliation. LSST admin clicks "Approve", and user get access.

Another option would be to try to glean info from email address. E.g., simply check for .edu for U.S. universities. But this would be more difficult for Chile users in the.cl domain.

Don - It's possible to use IP address to get physical location?

Jim - Yes

Xiuqin - Alums may have edu address but not currently a researcher.
Don - is there a professional registry of astronomers? Did the VA tackle that?

Xiuqin - no idea

Gregory - when VAO disbanded, Venkat has info on what happened to the IdP.

Jim - sounds like just .edu isn't good enough.

Don - we need to do research on what resources are available for identity vetting. We are talking about registration authority. This needs to be done by February so policy makers know the current capabilities out there.

Xiuqin - propose this for the February agenda?

Don - Margaret can put on agenda.

Margaret - need to find out how to propose items for the agenda

Jim - next case is granting data rights based on named individuals. Email address based invitation process. E.g., "Click here to create account or add data access rights to your account". That option seems straightforward.

Next is named individuals granting rights to associates, e.g., professor adding grad students to their project, and granting data rights to them. We'll probably want a system that can be controlled per individual.

Gregory - Note that this is about getting people in the front door.

Jim - another email based process is logical for this case.

Next topic - maintaining data rights - periodic re-validation of rights, especially of designated additional individuals. XSEDE does this on an annual basis. No formal proposal for de-provisioning data rights. Technically feasible, but we need the workflows for implementation.

Don - in dark energy survey, if a person leaves, but the research is not complete, their access is not cut off, but they can't grant rights to others to their data. This is a reasonable alternative.

Jim - Similarly, LIGO has a grace period for evaporation of rights.

Don - also workflow for PI to invite 'experts' into project, and what happens when 'expert' is not .edu person.

Gregory - same issue in BaBar - late in he project, needed process to have random strangers 'anointed' for their expertise.

Don - These kind of statuses need to be recorded.

Jim - tracking how person got data access rights is important

Another topic that Gregory commented on - users being able to authenticate even when they don't have data access rights. This has been the idea, i.e., first get access, then get data rights.

Don - right, identity is separate from authorization.

Don - talking with Steve Tueke, will this scheme inter-operate with other schemes, e.g., for data movement?

Jim - we don't address that in the design doc. So far, just thinking of Globus as a provider of group/user management service, A Swiss army knife. New revision called Globus Auth, will be used to plug into XSEDE, and won't need to create a Globus user account.

Don - has anyone thought about astronomer using our data, but using another proprietary data set with a different authentication scheme, i.e., check for conflicts?

Gregory - discussed a little, but nothing technical/practical

John - if you have access to LSST and can rsync out, that seems fine

Jim - any scheme should allow for multiple ssh, oauth, etc. tokens. don't lock ourselves into single token.

John - want to be able to pull data from many different sources into your workspace.

Jim - could be that scientist ssh in and pulls down data which is now in workspace, which is then accessible by multiple access schemes.

Gregory - people would manage data access to their workspace themselves.

Don - request that this is clearly written up as a consistent use case.

Jim - in IAM policy - need to say something to the effect that if user is importing proprietary data into workspace, then user is responsible for data access rights, this would be policy that the user signs off on.

Greg - correct.

Xiuqin - can we talk about workspace and authn?

Jim - we've talked about how IAM will enable ssh, api, webapps. etc. Are you asking for another level of detail?
Xiuqin - just talked about proprietary data in local workspace.

Greg - today’s topic is just about getting in the front door. The rest of talking about L3 rights would be another topic.

Jim - this could be a topic for another meeting.

Don & John - Brief discussion about im2p3 using same AUP as us. But little has been decided. They have only 100 users, so they don’t have to support everybody.