Hi Ranpal, Veronica, Ben,

Per discussion Victor's decision in the Monday management meeting, you three plus Victor, Iain, and I are the "team" that will define the answers to the questions posed below for the IDM effort.

Based on our LSST Master Information Policy (LPM-121) and LSST Information Classification Policy (LPM-122), I have made some annotations to the questions below. We need to follow the information classification categories as we consider the questions, and map profile information to the categories. I took some guesses as examples below. Ultimately the IDM team needs to know this for every profile field.

I suggest we have a short meeting to discuss and finalize answers. I've set up a doodle poll to pick a day next week if possible:

https://doodle.com/poll/97qye6w2mrvzuxxm

Once we get the days narrowed down, I'll update the poll with possible times.

Also, as Brian Selvy pointed out in the management meeting, AURA has a web-based staff directory for AURA employees that includes LSST staff, but you have to know the person's name to look them up, then you can find email and address. I think that is too narrow for us, as it only applies to AURA staff.

Please respond to the poll, thanks!

Jeff

> On Apr 26, 2018, at 8:12 AM, Jeff Kantor <jkantor@lsst.org> wrote:
>
> Hi all,
>
> We are in the process of working with NCSA to stand up the new Identity Management System (IMS). This is a Kerberos and LDAP-based system that will permit unified management of all logins, groups, access profiles, etc. for LSST. There will be a master database at NCSA, and distributed servers in Tucson and Chile.
>
> The Identity Management (IDM) home page in confluence is:
>
> https://confluence.lsstcorp.org/display/LAAIM/LSST+Authentication%2C+Authorization%2C+and+Identity+Management+Home
>
> Applications of the new IMS include providing authentication and authorization services for users and software services, providing a database and web-portal for identity management administration, and providing a replacement for the current Contacts Database on the LSST project site.
>
> This new IMS provides an opportunity to further "engineer" our access policies to various information. In particular, we need clarity on what profile information for known identities is:
>
> - accessible to the general public

Categories: Shareable (e.g. name, organization/affiliation, public contact information)

> - accessible to registered/vetted LSST users (e.g. Science Collaboration Members, exact definition of various groups is TBD)

Categories: Shareable, Protected User (e.g. collaboration membership information)

> - accessible to LSST staff (of various levels, such as individuals, supervisors, directors, etc.)

Categories: Shareable, Internal (AMCL membership, Builder status?), Sensitive (e.g. emergency contact list), Highly Sensitive (only to management as needed, shouldn't be any of this in profiles)

> - accessible to AURA staff who support LSST (e.g. CISS)

Categories: Shareable (some of these people may also be added to LSST staff group to give more access)

> Currently it appears that no information in the LSST Contacts Database is accessible to the general public. Is that to be the case going forward or do we want a public directory of some kind? For example, a variety of information about NCSA staff (but not NCSA users) is published publicly in the NCSA directory: http://www.ncsa.illinois.edu/about/directory.

> Similarly, do we want to change the information accessible to LSST users of all types, and to project staff in particular? Are there fields that should or should not be self-editable other than those currently editable?

Shareaable and Protected User information should be self-editable by an authenticated user, other levels require someone on project staff with appropriate group membership.

> A confluence page was created underneath this for these more detailed questions and answers.
>
> https://confluence.lsstcorp.org/display/LAAIM/LSST+Contacts+Information+and+Profiles
>
> I will mention this on the management call on Monday, thanks!
>
> Jeff