WBS 2.3.2 Open OnDemand OAuth Design 2021-09-10 Meeting

Dates

10 Sep 2021

Agenda, Discussion, and Action Items

Agenda & Discussion

Topic(s)

Review OOD web architecture:

- Apache with mod_auth_openidc
- Per-user Nginx (PUN) runs the user's dashboard and applicationsAn OOD configuration selects OAuth tokens to pass to a PUN pre-hook that runs as root
    - Like: OIDC_ACCESS_TOKEN,OIDC_ID_TOKEN,OIDC_SESSION,OIDC_CLAIM_EMAIL,OIDC_CLAIM_PREFERRED_USERNAME
- The PUN pre-hook (script) does whatever it wants with the OAuth tokens
    - Could securely save them to files owned by the user
    - Could put them in a token service

Discussion

Which OAuth Tokens

- xyz

Where to store them

- xyz

Which OAuth Tokens for SSH to SP resources

- Per Lee's e-mail

Managing OOD portal local accounts

- By hand for development
- By XCDB query and sync tool like login.xsede.org
- By CoManage directory

What about Scott Sakai's concerns

As an aside, a -major- hurdle to getting some other kind of authentication adopted is that it requires maintaining and running non-standard software in the critical path of authentication. If none of the capability-restricting features of SciTokens will be used, pursuing an SSH CA would speed adoption immensely. This is NOT an x509 PKI.
Rather than requiring extra binaries on the system, to accept SSH certificates, modern OpenSSH requires one or two lines to the sshd config file, and a file with the CA's public key.
I have developed an identity bridge that consumes Globus Auth access tokens, and produces SSH CA certificates, with the intent that it can be used for our OOD deployment. It's specific to SDSC's NSF resources, but the process might be adapted to something that would work XSEDE-wide.

Try to fund OOD staff to help?

- Use unspent funds

Action Items

- [ ] xyz

Attendees

- Lee Liming ✅
- Jim Basney ✅
- Eric Blau ✅
- Derek Simmel ✅
- JP Navarro ✅
- Shava Smallen ❌