MAGIC Meeting Minutes

May 6, 2015

Attendees

Basney, Jim jbasney@ncsa.uiuc.edu
Carlson, Richard Richard.carlson@science.doe.gov
Gemmill, Jill Clemson University
Harmsen, Meg NITRD/NCO
Love, Paul epl@sover.net
Lyles, Bryan jlyles@nsf.gov
Navarro, J.P. Argonne
Riley, Don drriley@umd.edu
Simmel, Derek dsimmel@psc.edu
Tuecke, Steve tuecke@ci.uchicago.edu

Action Items

1. Jill Gemmill will provide access to the FeduShare site and presentation materials from today's meeting.
2. Request to Grant Miller to add a link to the FeduShare slides from the MAGIC site.

Proceedings

The meeting was held May6, 2015 at Stafford II-535 in Arlington, VA, and chaired by Rich Carlson, DOE.

The April MAGIC minutes were approved. Rich Carlson asked that Grant Miller post them to the MAGIC website.

FeduShare

Jill Gemmill provided an overview of FeduShare and the current status of the project. The documentation used for the presentation is located at https://sites.google.com/site/fedushare.

FeduShare is a research project to bridge campus and research identity and access management for self-managed collaboration. It is funded by an NSF research grant under the Campus Cyberinfrastructure-Infrastructure, Innovation, and Engineering (CC*IIE) program. It is a collaboration among Clemson Univ., Univ. Illinois/NCSA, GENI, and Univ. of Utah.

FeduShare is a user-managed collaboration framework. It is based on four fundamental ideas: 1) access management for national infrastructure, to date, has been built by a small number of skilled experts, 2) researchers do their work at campuses, but need their resources to be available across campuses and national and international borders; they need to set up their collaborations quickly, 3) university campuses have talented IT staff in place, mostly focused on administrative identity and access management, 4) control over resources has been siloed and managed by resource administrators. It is time to turn the model upside-down and design infrastructure to support user-managed collaborations.

While campus Identity and Access Management (IAM) and the new Trust and Identity in Research and Education (TIER) program show promise, there is a need to go further and enable ways to be self-managed. Building blocks are needed, e.g., taking Shibboleth, etc., packaging it up, putting out a regular release of code, and providing a user interface and installation. The focus should be on collaboration versus control.

Referring to the FeduShare schematic (https://sites.google.com/site/fedushare/the-fedushare-framework), Jill described several components of FeduShare. These included the "actors" (researcher, PI, VO manager, and resource manager) and the "event flow" for setting up a virtual organization, listing collaborators, and requesting and accessing resources through a Resource Request Protocol. This setup allows those collaborators who are members of the VO to be authorized for access to resources through their local campus authentication (EPPN) and VO membership. One assumption is that the InCommon trust fabric is behind the process, and all actors and resources are part of InCommon. Each campus uses Shibboleth and can provide SAML assertions. A VO manager service must also exist. Possible federated resources could be accessed through, e.g., a service portal or science gateway.

To ground this approach in reality, they are using the use case, "SSH Login to Campus Cluster using Federated Identity." Jill noted a number of scenarios where logging in via a federated identity is useful. One genre is Guest Accounts. For example, to enable collaboration across campuses, an HPC investigator at one campus may want to allow an HPC investigator from another campus access to a local HPC cluster (Clemson and Utah have HPC clusters and both use campus IAM systems.) Since the remote investigator is not in the local IAM, they can request a guest account for this purpose. Other guest account examples included parents viewing a student's grade or parents paying a bill. Another genre for using federated identity is for access to Regional Clusters, which are becoming a way to aggregate HPC resources and operate them economically. Users' local campus GUIDs would be the way to connect.

Jill described five candidate approaches to enabling users to have SSH logins to a remote cluster by using their InCommon EPPN. She discussed the pros and cons of each, and the one they selected.

1. CILogon
2. ECP SSH (ECP profile = Enhanced Client or Proxy Profile)
3. ECP PAM
4. SSH KEYS
5. STAY IN THE BROWSER

They chose #2 ECP SSH. In this case, one needs to have ECPSSH installed. It is based on GSSAPI and leverages Shibboleth.

The next steps will be to 1) implement the use case with ECP SSH. This will probably be a cloud lab, using a bioinformatics workflow – campus to cloud lab – and an SDN administrative domain; 2) complete the VO manager; 3) map current software solutions to the framework and identify gaps; and 4) summarize in final report.

Q&A and discussion:
What were the leading criteria for deciding which login approach to select? Jill said they had not documented the criteria, but provided the following response. They will add criteria to the document for future reference:

- Put the user in control
- Have a console window login (user request)
- Quick. Do not want to wait too long to get set up
- Preferred to not have to remember another user name
- Cloud/virtual instead of batch approach
- Preferred federated identity (e.g., SAML) versus external certificate (This was more important than requiring user to install special software. They thought it would be a moon shot project to get GSSAPI into SSH clients.)

How will you distribute the client software? This is still to be determined.

Jill invited participants to contact her (or Jim Basney) with any questions or comments.

Next MAGIC Meeting
June 3, 2015, NSF, Room TBD.