FeduShare Update

AuthNZ the SAML way for VOs

FeduShare Goals:

- Provide transparent sharing of **campus** resources in support of (multi-institutional) collaboration
- Support both HTTP and **non-web** access using federated authentication and Shib ECP
- Leverage the knowledge and talents of campus IAM staff
- Eliminate GUEST/AFFILIATE identities
- Commence/increase communication between IAM experts at NCSA, GeNI, XSEDE, OSG and campus

Assumptions

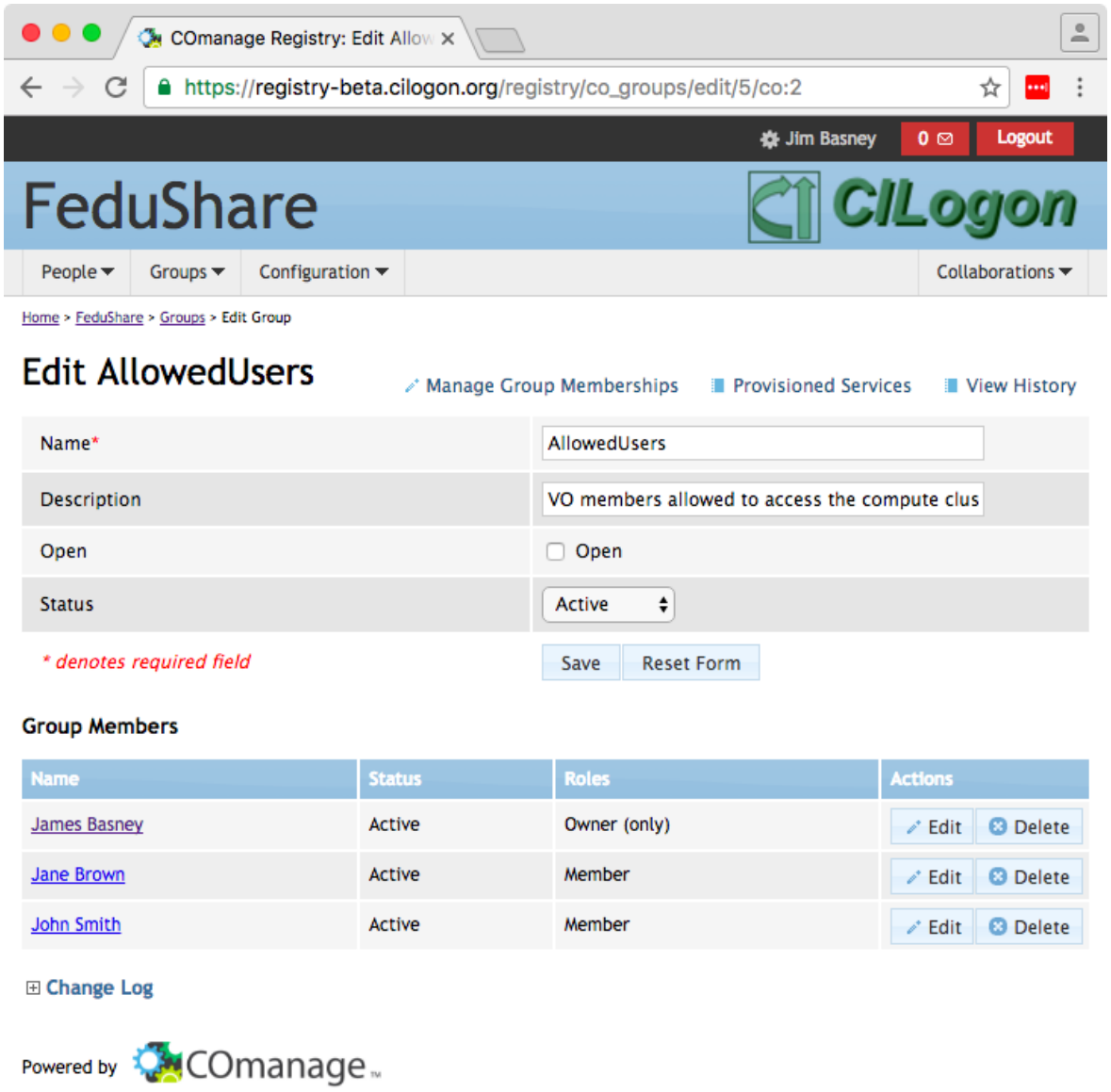
- Campus supports Shibboleth
  - Campus may support OAuth
  - Shib ECP + R&S
- Resource owner sets policy and controls access to shared resource
- There is a federated Virtual Organization management service
- Resource owner authorization processes should make use of the federated VO service

FeduShare use case 1: Shared use of campus HPC

- Federated SSH (non-web)
  - Demonstrated Utah login to Clemson Palmetto cluster in October 2015, using Shib-ECP and modified OpenSSH (gss-mechsaml-ECP)
- Partnership with JISC Moonshot Project
  - Uses gss-mechsaml-EAP
- Partnership with GeNI project office
  - Have implemented a Shibboleth Attribute Authority that can assert a subset of information such as GeNi Project membership or role as a SAML assertion

Today's Demo:

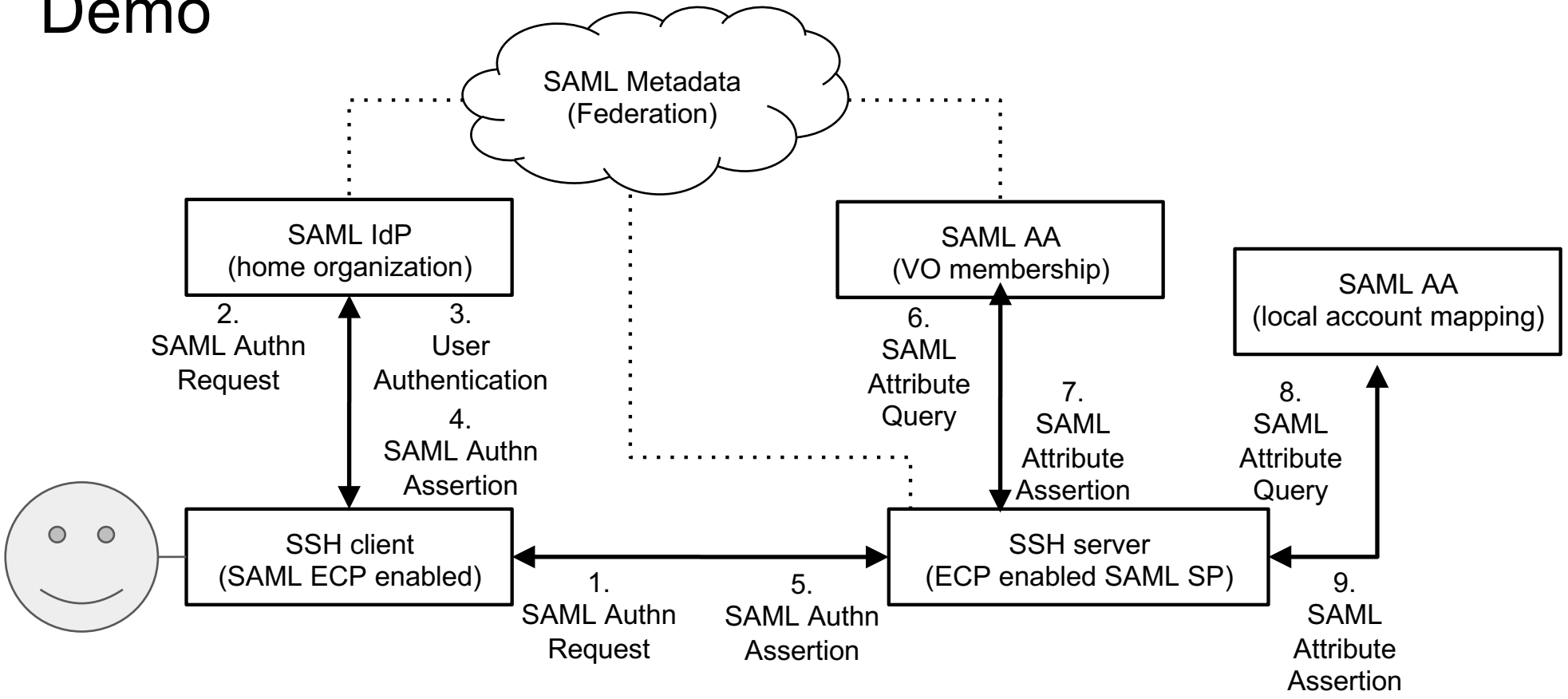
- We will demonstrate integration with MoonShot ssh client GUI
- Authorization will use attribute(s) from an Attribute Authority separate from campus
  - CILogon 2.0
  - GENI RBAC infrastructure
- We have fixed prior need to store password in a local file
- We will review security concerns



Attribute based access control

- Access denied by clearing local-login-user attribute
- Shibboleth SP and IdP provide configurable rules for denying attributes
- Examples:
  - #1
    - SP queries AA with EPPN
    - AA releases list of identifiers of VOs user is a member of
    - SP denies access if list does not include resource owner's VO
  - #2

Demo


SAML Metadata
(Federation)
SAML IdP
(home organization)
SAML AA
(VO membership)
SAML AA
(local account mapping)
2.
SAML Authn
Request
3.
User
Authentication
4.
SAML Authn
Assertion
6.
SAML
Attribute
Query
7.
SAML
Attribute
Assertion
8.
SAML
Attribute
Query
SSH client
(SAML ECP enabled)
SSH server
(ECP enabled SAML SP)
1.
SAML Authn
Request
5.
SAML Authn
Assertion
9.
SAML
Attribute
Assertion

SSH ECP Security: Distributed Trust

Federation signs metadata containing IdP/SP/AA identities and public keys

IdP verifies signature on authentication request from SP

IdP informs the client of the SP's verified identity

SP verifies signatures on assertions from IdP/AAs

GSS channel binding connects SAML flows with SSH session

User trusts client to send password securely to home IdP

SP trusts IdP to authenticate the user

How does this relate to TIER

- Shibboleth for federated authentication
- Co-Manage is a proven VO management service (LIGO)
  - Co-Manage already supports OAuth
- Look at Co-Manage as a vehicle for replacing GUEST/AFFILIATE identities
- Conversation about stand-alone Attribute Authorities needed in InCommon

Moonshot updates and use cases

- macOS support is coming!
  - Mac development house engaged, contracts are being exchanged
  - Initial support expected in early 2017
- SSH forwarding (ProxyCommand etc)
  - Proven to work with Moonshot
  - Chained multiple levels and it happily works
  - Used by eMedLab project in the UK
- New projects + federations looking at Moonshot

FeduShare Futures

- Observation: a shared campus resource might exist in one or more clouds
- Co-Manage is being integrated with CILogon for access to XSEDE and OSG resources; how can this service be used by campuses?
- If campuses set up local Co-Manage instances, can we establish common practices so that there is consistency across campuses and with CILogon?
- Will we need a “WIYVO” (Where is your VO?) service akin to WAYF?
- Sustainability: Will JISC adopt gss-mechsaml-ECP? Would there be any US funding to do this?
- Will campuses discuss shared resource policies in campus silos, or will there