Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney
jbasney@ncsa.illinois.edu
https://sciauth.org/workshop/2022/
tokens for science

OpenID Connect (OIDC) ID Tokens (e.g., SCiMMA)
containing user attributes and group memberships
from the research community (via COmanage)
and from the researcher's home institution (via InCommon)

SciTokens (e.g., LIGO)
containing authorization scope values
determined by per client/subscriber policy

WLCG Tokens (e.g., Fermilab)
support for wlcg.groups and storage.*|compute.* scopes

GA4GH Passports (e.g., Australian BioCommons)
support for AffiliationAndRole, AcceptedTermsAndPolicies, ResearcherStatus,
ControlledAccessGrants, and LinkedIdentities

https://www.cilogon.org/jwt

www.cilogon.org
token standards

- RFC 6749: OAuth 2.0 Authorization Framework
  - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
  - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
  - token signing keys, policies, endpoint URLs
- RFC 8693: OAuth 2.0 Token Exchange
  - token delegation, drop privileges (reduce "scope")
- RFC 9068: JWT Profile for OAuth 2.0 Access Tokens
  - authorization claims using JWT "scope" and "aud"

https://www.cilogon.org/jwt
SciTokens for LIGO

dedicated https://cilogon.org/ligo token issuer
migrating to https://cilogon.org/igwn soon
vault.ligo.org server for token management
HTCondor token management for workflows
target applications: OSDF/CVMFS/XRootD, GWDataFind, DQSegDB, GraceDB
# current LIGO AuthZ policies

<table>
<thead>
<tr>
<th>scope (old)</th>
<th>scope (new)</th>
<th>group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>read:/frames</td>
<td>read:/frames gwdatafind.read</td>
<td>Communities: LSCVirgoLIGOGroupMembers gw-astronomy: KAGRA-LIGO: members</td>
</tr>
<tr>
<td>write:/frames</td>
<td>write:/frames</td>
<td>Services: XRootD: SciTokens: write-frames: authorized</td>
</tr>
<tr>
<td>query:/DQSegDB</td>
<td>dqsegdb.read</td>
<td>Communities: LSCVirgoLIGOGroupMembers gw-astronomy: KAGRA-LIGO: members</td>
</tr>
<tr>
<td>insert:/DQSegDB</td>
<td>dqsegdb.create</td>
<td>Communities: LVC: SegDB: SegDBWriter</td>
</tr>
<tr>
<td>read:/GraceDB</td>
<td>gracedb.read</td>
<td>Communities: LSCVirgoLIGOGroupMembers gw-astronomy: KAGRA-LIGO: members</td>
</tr>
<tr>
<td>write:/GraceDB</td>
<td>N/A</td>
<td>N/A (managed via service ACLs)</td>
</tr>
</tbody>
</table>
Robot: unattended, long-lived process with its own identity & capabilities

Robot operators are authorized via
"Services:Robots:<robot-name>:SciTokens:authorized" groups

Operator authenticates to CILogon to issue Robot refresh token to Vault

CILogon verifies that 1) operator is authorized to manage the Robot and 2) Robot is authorized to obtain SciToken

Vault obtains fresh SciTokens (access tokens) using refresh tokens

Robot obtains SciTokens from Vault (using Kerberos) for long-lived operation
LIGO current status

CVMFS HTCondor access in operation
GraceDB & GWDataFind support implemented and being deployed
DQSegDB support under development
Robot support under development
Bi-weekly coordination calls to prepare for tokens in next LIGO Observing Run (O4) - March 2023
Very grateful for Dave's Vault assistance
Thanks!

contact:
help@cilogon.org

subscribe for updates:
https://groups.google.com/a/cilogon.org/g/announce