WLCG Pre-GDB Authorization Working Group

Mine Altunay, Jeny Teheran

WLCG Authorization Working Group

10 September 2019

Outline

- Fermilab's progress towards Federated Identities and standing issues.
- DUNE computing problems: CILogon Basic CA acceptance.
- VOMS future

Federated Identities at Fermilab

- Started the Federation Project, our goal is to incorporate federated access tokens into the Fermilab computing infrastructure. Have another more detailed talk about this during FIM4R meeting.
- Already completed a demo project, where we built federation with CERN users and allow them access to Fermilab web based resources.
  - The resource was wiki.dunescience.org
  - We showed that CERN users could read the website with just their CERN credentials
- Access to grid resources is still in its early stages.
- Our standing problems
  - If we continue with SciTokens, how can we express the group privileges?
  - How can we ensure that SciTokens and Indigo AIM are fully compatible?

Federation Project Issues

- SciTokens do not express group membership and privileges associated with groups. Our infrastructure is very dependent on using the group membership information.
  - SciTokens generates capabilities based tokens
  - We can find different solutions to remedy this, but want to understand the reasons for this design decision
- Indigo IAM-SciToken interoperability
  - We are also hopeful that this should be a non-issue
  - But, want to understand what tests/process we should undergo to ensure there are no problems

Which Services to be Transitioned First

- We are first focusing on DUNE and its services
- wiki.dunescience.org
- Main dune web site (dunescience.org and friends)
- cdcvs.fnal.gov (redmine) operated SCD
- github
- SAM operated SCD
- Jobsub operated SCD (gateway to FermiGrid and OSG)
- POMS operated SCD
- Rucio operated SCD
- dCache/Enstore operated SCD
- ECL operated SCD
- EDMS operated CERN
- E-log operated CERN
- EOS operated CERN
- Castor operated CERN
- Fermi-FTS joint operated DUNE and SCD
- CERN FTS3 operated CERN

CILogon Basic CA and DUNE Computing Challenges

- DUNE computing uses CILogon Basic CA certificates for analysis jobs that requires access to CERN and other sites.
- Although CILogon Basic CA is an IGTF accredited CA, it is accredited under IOTA profile, which is not accepted by CERN and some other sites.
- This causes a major issue for DUNE.
- We will discuss our potential solutions for this problem.

Solution#1

- Work with CERN and provide a set of extra documentation to have CILogon Basic CA accepted at CERN and other sites.
- Documentation showing compliance with following documents or prove equivalent mechanisms at work.
  - WLCG Authentication Assurance Policy
  - Authentication Assurance Policy
  - Community Membership Management Policy
  - WLCG will review our documents and make a decision on CILogon Basic CA.

Solution #2

- We found many sites already supported all IGTF Classic CAs and no IOTA CAs
- Multiple sites, mainly in the UK, added during an on boarding campaign before protoDUNE started taking data
- Sites had to be contacted one by one to add CILogon Basic even after they had enabled the DUNE CAs (CILogon Basic CA) in response to the general UK request for sites.
- Some sites were able to add CILogon Basic immediately. Others (eg RAL Tier-1) had policy or technical reasons why it took much longer (up to many weeks)
- There are likely to be ongoing issues as this exceptional configuration is lost in upgrades etc.
- So, one idea is to upgrade to CILogon Silver CA

Solution#2

- Upgrade to CILogon Silver CA, which is accredited under IGTF Classical profile and accepted everywhere.
  - This entails changes to how Fermilab does identity vetting
  - Silver CA requires face-face identity vetting for all users. Fermilab already does this for majority of Fermilab users except for remote users, who cannot come to the lab.
  - Fermilab needs to incorporate either an online form of identity vetting for such remote users or find other equivalent vetting processes.
  - Either case, it is a change to Fermilab's current vetting workflow, which will take time and effort

VOMS Future

- Since Indigo IAM and SciToken ecosystem also provides user management systems, will we need VOMS in the near future?
- Token systems can generate tokens (at least SciTokens) from an ldap based user management system
- Tokens also do not need the X.509 extended proxy credential capability
- Under these circumstances, do we still need the VOMS?
- Are there any other plans in WLCG/CERN and other organizations?

Summary

- Either solution has difficulties and will take some time.
- Any insight and guidance is appreciated.