Identity Management for the LIGO Project

Scott Koranda for LIGO

LIGO and University of Wisconsin-Milwaukee

November 5, 2010
LIGO-XXXXXXXX-v1
LIGO Science Mission

LIGO, the Laser Interferometer Gravitational-wave Observatory, seeks to detect gravitational waves – ripples in the fabric of spacetime. First predicted by Einstein in his theory of general relativity, gravitational waves are produced by exotic events involving black holes, neutron stars and objects perhaps not yet discovered.
LIGO Hanford, WA
LIGO Livingston, LA
LIGO Laboratory

LIGO Laboratory =
LIGO Caltech + LIGO MIT +
LIGO Hanford Observatory +
LIGO Livingston Observatory
The LIGO Scientific Collaboration (LSC) is a self-governing collaboration seeking to detect gravitational waves, use them to explore the fundamental physics of gravity, and develop gravitational wave observations as a tool of astronomical discovery. The LIGO Scientific Collaboration was founded in 1997 and currently has more than 800 members from 70 institutions worldwide.
LIGO Identity Management: We Had a Mess

LIGO scientists struggle in early 2007:

- **web** Many servers, wikis, log books—multiple identities
- **grid** Request, renew, manage own X.509 certificates
- **shell** Multiple identities each with distinct credential
- **email** Each list managed separately
LIGO Identity Management: We Had a Mess

No single event precipitated new approach

It really came down to two things:

1. Sustained whining from frustrated users
2. Chatting with Ken Klingenstein over drinks
LIGO Identity Management Project

Started in Summer 2007

Knit together existing technologies and tools

Goals:

➤ Single identity for each LIGO person
➤ Single source of membership info
➤ Single credential for each LIGO person
➤ SSO across web, grid, command-line
LIGO Identity Management Project

Found we had two building blocks:

1. The nascent “LIGO Roster” project
   - PHP + Apache + MySQL

2. Kerberos principal for each LIGO member
   - unused at the time
   - scott.koranda@LIGO.ORG
   - users call it their “at LIGO.ORG login”
   - also known as their “albert.einstein” login
LIGO Identity Management Project

Building on solid foundations:

- **Kerberos** single identity and credential
- **Grouper** single source of membership info
- **OpenLDAP** solid distributed replication
- **Shibboleth** web SSO with eye towards federation
- **Sympa** sophisticated email list management
- **MyProxy** flexible and easy X.509 from Kerberos
- **CoManage** coming soon!
LIGO IdM: Status

- distributed Kerberos infrastructure in production
- distributed LDAP infrastructure in production
- Grouper 1.4.2 in production, provisions into LDAP
- 3 Shib IdPs in production (WAN configuration–2 for HA)
- LIGO custom DS in place for HA
- 21 Shib SPs deployed
- domesticated Foswiki, Moin, aLOG
- Sypma email in production
- LIGO CAs provisioned
- LHO site tightly integrated via Kerb, LDAP, Shib
- NSF SDCI grant to accelerate COManage & Grouper integration into LIGO
LIGO IdM: Stalled

- MyProxy deployment stalled—no time!
- LIGO CAs safe but not so useable
- command line integration at other sites
- no federation yet
- custom GUI work not stalled, but slow progress

No surprise—lack of FTE effort for this work
It’s (mostly) all about group memberships at this time:

```
$ ldapsearch -x -LLL -b "ou=people,dc=ligo,dc=org" \
   "(krbPrincipalName=scott.koranda@LIGO.ORG)" isMemberOf 
  dn: employeeNumber=882,ou=people,dc=ligo,dc=org
  isMemberOf: Communities:LVC:LSC:CompComm:AuthProject:AuthProjectGroupMembers
  isMemberOf: Communities:LVC:LSC:CompComm:CompCommGroupMembers
  isMemberOf: Communities:LVC:LSC:LDGSysAdmin:LDGSysAdminMail
  isMemberOf: Communities:LVC:LVCGroupMembers
  isMemberOf: Communities:LVC:LSC:MOU:UWM:UWMGroupMembers
  isMemberOf: Communities:LVC:LSC:LSCGroupMembers
  isMemberOf: Communities:LSCVirgoLIGOGroupMembers
  isMemberOf: Communities:LVC:LSC:MOU:UWM:UWMGroupManagers

Wikis also need sn, givenName

Sympa needs mail, mailAlternateAddress, mailForwardingAddress
$ ldapsearch -x -LLL -b "ou=people,dc=ligo,dc=org" \
   "(krbPrincipalName=laura.cadonati@LIGO.ORG)" isMemberOf

dn: employeeNumber=631,ou=people,dc=ligo,dc=org
isMemberOf: Communities:LVC:LSC:LSCGroupMembers
isMemberOf: Communities:LVC:LSC:MOU:UMAmherst:UMAmherstCouncilMembers
isMemberOf: Communities:LVC:LVCGroupMembers
isMemberOf: Communities:LVC:LSC:MOU:UMAmherst:UMAmherstGroupManagers
isMemberOf: Communities:LVC:LSC:MOU:UMAmherst:UMAmherstGroupMembers
isMemberOf: Communities:LVC:LSC:MOU:UMAmherst:UMAmherstSupportStaffManagers
isMemberOf: Communities:LVC:LSC:Council:LSCCouncil
isMemberOf: Communities:LVC:LSC:MOU:UMAmherst:UMAmherstPublicInformationOfficers
isMemberOf: Communities:LVC:LSC:PublicInformationOfficers
isMemberOf: Communities:LVC:SympaLists:LVCBurst:LVCBurstModerators
isMemberOf: Communities:LVC:SympaLists:LVCBurst:LVCBurstSubscribers
isMemberOf: Communities:LVC:SympaLists:GEO-DC:GEO-DCSubscribers
isMemberOf: Communities:LSCVirgoLIGOGroupMembers
Attributes for Authorization: Foswiki

AuthProject Web Preferences

The following settings are web preferences of the AuthProject web. These preferences overwrite the site-level preferences in System.DefaultPreferences and Main.SitePreferences, and can be overwritten by user preferences (your personal topic, eg: ScottKoranda in the Main web).

- Web Preferences Settings
- Help on Preferences
- Tools
- Related Topics

Web Preferences Settings

These settings override the defaults for this web only. See full list of defaults with explanation.

Many of the settings below are commented out. Remove the # sign to enable a local customisation.

* Users or groups who are not/are allowed to view/change/ rename topics in the AuthProject web: (See TWikiAccessControl)
  - Set DENYWEBVIEW =
  - Set ALLOWWEBVIEW = Communities:LSCVirgoLIGOGroupMembers
  - Set DENYWEBCHANGE =
  - Set ALLOWWEBCHANGE = Communities:LSCVirgoLIGOGroupMembers
  - Set DENYWEBRENAMES =
  - Set ALLOWWEBRENAME = Communities:LSCVirgoLIGOGroupMembers
Attributes for Authorization: Moin

Other users will be warned until 2010-11-02 13:05:00 that you are editing this page. Use the Preview button to extend the locking period.

```plaintext
# acl Communities*LVC*LVCGroupMembers: read, write, delete, revert, admin

<<TableOfContents()>>

= Foswiki Configuration =

"Debian Lenny x86 64 as deployed for wiki.ligo.org"

== General Apache configuration ==

* Install Apache and modules

```
Attributes: What to Expect When Federated?

What attribute and value to authorize IceCube scientists?

\texttt{isMemberOf: nsf.gov:IceCube:IceCubeMembers}
\texttt{isMemberOf: nsf.gov:IceCube:IceCubeManagers}

Who is going to negotiate the taxonomy for federated science?

Are the national Higher Ed federations the optimal vehicle?
Path to Federating With Smaller VOs?

Real (and in some cases urgent) science drivers

Need collaboration spaces with
  ▶ astronomers
  ▶ astrophysicists
  ▶ numerical relativists

Requirement to leverage existing @LIGO.ORG identities

Smaller VOs have no (managed) identities to offer!

Until everyone federated try to offer @LIGOGUEST.ORG identities

That is not going to scale...please help!
Use Case: GraceDB

GraceDB — Gravitational-wave Candidate Event Database

GraceDB Alpha — Overview

The gravitational-wave candidate event database (GraCEDb) is a prototype system to organize candidate events from gravitational-wave searches and to provide an environment to record information about follow-ups.

A simple client tool is provided in Glue which can submit a candidate event and query the event database. The client is a standalone Python script and will run using only standard Python libraries.

You can read about using the service at the Howto page. More details are available at the Project page.

To receive email alerts when GraCEDb events are created, sign up on the gracedb mailing list or set up your own alert under the Options menu item.
Use Case: GraceDB

- scientist uses X.509/RFC3820 authenticate to cluster
- analysis workflow runs on cluster (up to 1 week)
- last few jobs could use some credential to
  - transfer output data products (GridFTP:X509/proxy)
  - publish triggers (GraceDB:X509/proxy/SAML2)
  - publish summary results (wiki:SAML2)
  - create collaboration space (wiki?:SAML2)

How do I delegate my identity to this workflow appropriately?

(Yes, we could make the technical plumbing work. Should we have to?)
Why aren’t more (science) VOs here?

Conjecture:
- Few VOs can spare the FTE effort
- Few VOs link “federated identity” with their problems
- Science effort may be organized/centralized, but IT is not

Engaging science VOs requires different model than Higher Ed