

Identity Management for the LIGO Project

Part Two: Campus support for LIGO IdM

Scott Koranda for LIGO

LIGO and University of Wisconsin-Milwaukee

February 17, 2011
LIGO-G1100137-v2



LIGO Identity Management Project

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
 - ▶ roster drives creation of principal for each member
 - ▶ roster pushes principal and details into LDAP

Single authoritative source of membership

Decided to leverage Grouper from I2

- ▶ Flexible enough to reflect community structure
- ▶ Ready-to-use web front-end
- ▶ SOAP and RESTful WS APIs
- ▶ Privilege support
- ▶ Reflect into LDAP



Welcome Scott Koranda

Act as admin

Change

My tools

Explore

Search

Group workspace

Entity workspace

Help

LIGO

Roster

MyLIGO

EXPLORE

Browse groups hierarchy

You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)

Browse or list groups

Current location is:

Root Communities LVC LSC MOU

10

Change page size

Showing 1-10 of 51 items

- BalearicIslands
- UOregion
- McNeese
- SanJoseState
- MoscowState
- HobartWilliamSmith
- GEO
- UWM
- Northwestern
- UMiss

[Next page](#)

LIGO group management based on
Grouper from



Search groups

[Advanced groups search](#)

```
[root@oregano ~]# ldapsearch -LLL -b "ou=people,dc=ligo,dc=org"  
-H ldap://ldasdata4.ligo.caltech.edu -x '(cn=Scott Koranda)'  
isMemberOf  
dn: employeeNumber=882,ou=people,dc=ligo,dc=org  
isMemberOf: Communities:LVC:LSC:MOU:UWM:UWMGroupMembers  
isMemberOf: Communities:LVC:LVCGroupMembers  
isMemberOf: Communities:LVC:LSC:LSCGroupMembers  
isMemberOf: Communities:LVC:LSC:CompComm:CompCommGroupMembers  
isMemberOf: Communities:LVC:LSC:MOU:UWM:UWMGroupManagers
```

LIGO Roster

- ▶ Students, post-docs, can apply for membership
- ▶ Managers approve & add/remove members
 - ▶ Access control derived from Grouper privileges
- ▶ Members manage password for LIGO identity (Kerberos principal)



LSC Member Management

My Information

Manage Group

LSC Group:

LSC - UW Milwaukee ▼

Actions:

- [Act on Pending Membership Requests](#)
- [Manage Members](#)
- [Manage Council Delegates](#)

Act on Pending Membership Requests

There are currently no pending membership requests for this group.



Single identity and authoritative membership is key

LIGO Roster, Grouper, and Kerberos a powerful combination

- ▶ Kerb principal enables single identity
- ▶ Roster enables management of those identities
- ▶ Grouper enables management of memberships

With this foundation we could tackle web, grid, and command line spaces...

Single sign-on for LIGO web space



Deploy I2 Shibboleth System

- ▶ Single sign-on across LIGO web tools/pages
- ▶ LIGO Identity Provider (IdP)
 - ▶ Authenticate via `REMOTE_USER` and `mod_auth_kerb`
 - ▶ Attributes pulled from LDAP master server
 - ▶ Focus mainly on `IsMemberOf` (via Grouper)
- ▶ Look to federate in future (soon!)
 - ▶ InCommon for many U.S. institutions
 - ▶ European federations (UK, DFN-AAI)
 - ▶ Virgo?



A username and password are being requested by <https://login.ligo.org>. The site says: "This content is viewable by only LIGO/Virgo personnel and authorized guests. Please enter your LIGO Directory name, e.g. albert.einstein, and password..."

User Name:

Password:

Cancel

OK

[File](#) [Edit](#) [View](#) [History](#) [Bookmarks](#) [Tools](#) [Help](#)

Wiki_Home - DASWG Wiki

LVC PortalGEOLIGOLSCVIRGOHelp

LIGO Data Grid Wiki

welcome: [ScottKoranda](#) | [settings](#)
Refresh my LIGO group memberships

[LDGWiki](#) >

Quick Links

- [recentchanges](#)
- [findpage](#)
- [helpcontents](#)
- [wiki home](#)

Search Wiki

Search

[Titles](#) [Text](#)

Page Tools

- [edit \(text\)](#)
- [edit \(gui\)](#)
- [page history](#)
- [email me changes](#)
- [add to quicklinks](#)
- [upload & manage files](#)

[\[more options \]](#)

Contents

- [1. Organizational](#)
- [2. Projects](#)
- [3. Help, Howto, FAQs](#)
- [4. Technical Documents](#)

Welcome to the LIGO Data Grid wiki which compliments the [LIGO Data Grid](#) and [DASWG](#) websites.

Organizational

- Telecons and Minutes
- LIGO Data Grid Team
- Version Control Systems Advisory Committee (2008)
- OS Selection Committee (2007)

Projects

- S6 Online Working Group
- Advanced LIGO Data and Computing
- GPU Development in LSC/Virgo
- CondorC for LIGO Data Grid

12 / 31

Center for Gravitation and Cosmology Wiki

welcome: [ScottKoranda](#) | [settings](#)
Refresh my LIGO group memberships

CGCWiki >

Quick Links

[recentchanges](#)
[findpage](#)
[helpcontents](#)
[wiki home](#)

Search Wiki

Page Tools

[edit \(text\)](#)
[edit \(gui\)](#)
[page history](#)
[email me changes](#)
[add to quicklinks](#)
[upload & manage files](#)

[\[more options \]](#)

Contents

1. [Administrative](#)
2. [Projects/Events](#)
3. [MOU Reports and Attachments](#)
4. [Computing](#)
5. [Proposals](#)
6. [General HowTo's URL](#)
7. [UWMLSC Document Center](#)

Administrative

- [Information for new group members](#)
- [Useful links and resources for LSC members](#)
- [Information for travellers](#)
- [Information for visitors](#)

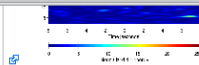
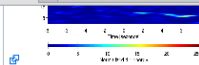
Projects/Events

- [Schedule of Departure/Return times for LIGO/VIRGO meeting 2010](#)
- [projects/GWDAW15](#)

MOU Reports and Attachments

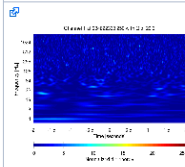


- ▶ Only deploying Shibboleth 2.x
- ▶ Only supporting SAML2
- ▶ Rely heavily on SAML2 artifact resolution
- ▶ Helps with a specific use case
 - ▶ Wiki include IMG from multiple servers
 - ▶ Browsers won't push attributes via JS when fetching IMG
 - ▶ SAML2 artifact resolution requires no JS

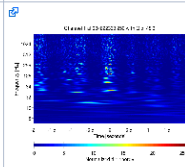


L1:OMC-QPD1_Y_OUT_DAQ and L1:OMC-QPD2_Y_OUT_DAQ have some noise at higher frequencies:

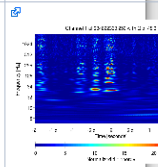
LSC-DARM_ERR



OMC-QPD1_Y_OUT_DAQ



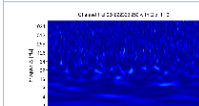
OMC-QPD2_Y_OUT_DAQ



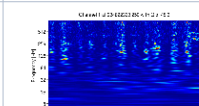
H1: There is a H1:DMT-PRE_LOCKLOSS_1800_SEC flag.

Looks like some H1:OMC-QPD1 channels had some noise at higher frequencies:

LSC-DARM_ERR



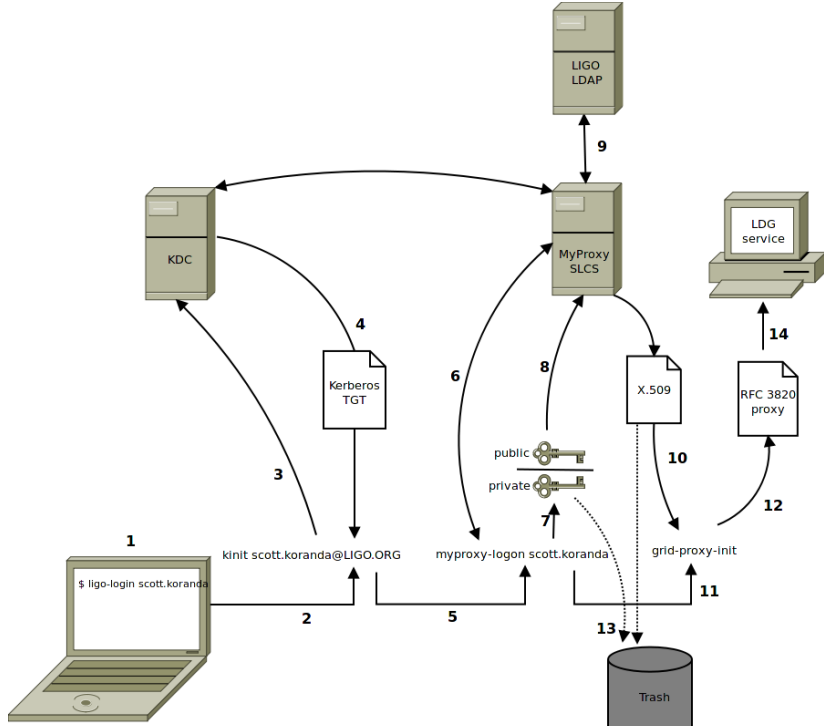
H1:OMC-QPD1_Y_OUT_DAQ



MyProxy and GridShib CA integrate LIGO Data Grid



- ▶ MyProxy exchanges Kerb ticket for X.509 cert
- ▶ GridShib CA exchanges SAML2 for X.509 cert
- ▶ User “sees” @LIGO.ORG cred required for both
- ▶ X.509 certs are “short-lived”
- ▶ Can also be converted to RFC 3820 proxy cert



LIGO Certificate Authorities

MyProxy and GridShib expose LIGO CA

- ▶ SLCS = short lived credential service
- ▶ The Americas Grid Policy Management Authority (TAGPMA)
- ▶ TAGPMA provides SLCS profile
- ▶ Plan to accreditate LIGO SLCSs



LIGO Data Grid Authorization

Grid authorization driven by Grouper and LDAP

- ▶ ACL files derived from IsMemberOf
- ▶ Simple LDAP query with local caching
- ▶ X.509 DN and login pulled from LDAP

```
# isMemberOf Communities:LVC:LSC:LSCGroupMembers
"/DC=org/DC=ligo/O=LIGO/OU=People/CN=scott.koranda@LIGO.ORG" skoranda
"/DC=org/DC=ligo/O=LIGO/OU=People/CN=sergey.klimenko@LIGO.ORG" klimenko
"/DC=org/DC=ligo/O=LIGO/OU=People/CN=sukanta.bose@LIGO.ORG" bose
"/DC=org/DC=ligo/O=LIGO/OU=People/CN=szabolcs.marka@LIGO.ORG" smarka
"/DC=org/DC=ligo/O=LIGO/OU=People/CN=teviet.creighton@LIGO.ORG" teviet
```

Integrating the command line

CVS, SVN, git tunnel through SSH

- ▶ Most Linux OpenSSH sshd GSS-API + Kerberos
- ▶ Grid-enabled OpenSSH also deployed
- ▶ NCSA “mechglue” enables Kerb + GSI
- ▶ PAM also work with Kerberos

This pattern same for other command line tools

(note that curl works well with SAML2/artifact)

Integrating email



- ▶ LDAP queries define lists
- ▶ Fairly complex queries possible
- ▶ `mailAlternateAddress` LDAP attribute enables posts from multiple accounts
- ▶ Lists can accept posts from any person in collaboration
- ▶ Web access to list management pages and archives via Shib

Putting it all together

Within 15 minutes of joining LIGO Albert Einstein using his `albert.einstein@LIGO.ORG` credential can...

1. Access LIGO wikis to find HOWTOs
2. Download and install client tools
3. Login to cluster
4. Checkout code from git repository
5. Email analysis discussion list for help
6. Build code, submit analysis jobs

From 0 to science with one `@LIGO.ORG` credential

Cleaning up is easy

When Albert Einstein leaves the LIGO collaboration...

1. albert.einstein@LIGO.ORG Kerberos principal disabled
2. Removed from Grouper/LDAP groups
3. No login to Shib IdP, no web access
4. No MyProxy, GridShib, no grid access
5. No access to code repositories
6. No email lists

How can campus IT and CIC IdM support LIGO IdM?

Obvious (and easy?) first:

- ▶ Join InCommon (Done)
- ▶ Support growth of InCommon
- ▶ Continue support of technologies like Grouper and Shib
- ▶ More “brains on a stick” offerings




How can campus IT and CIC IdM support LIGO IdM?

MyCO - LIGO - Iceweasel

File Edit View History Bookmarks Tools Help













MyCO - LIGO


**LIGO Scientific Collaboration**

Alan Weinstein
Logout

MyApplications MyMailingLists MyGroups MyCollaborators MyInfo MyHistory

Invite a New COllaborator CO Directory

Identifier	Person	Role	Title	Email	Sponsor	Actions
34545	Ken Klingenstein	COmanage Developer	Sales	kjk@gmail.com	COmanage	 
31793	Steven Carmody	COmanage Developer	Architect	stc@gmail.com	Ken Klingenstein	  
45787	Heather Flanagan	COmanage Developer	Manager	hlf@gmail.com	Ken Klingenstein	  
40396	Jim Leous	COmanage Developer	Architect	jal@gmail.com	Steven Carmody	
19445	Steve Olshansky	COmanage Developer	Flywheel	steveo@gmail.com	Ken Klingenstein	  

 **COmanage™**

http://co.internet2.edu/mockup/comanage/myco-ligo.html#mycollabs

How can campus IT and CIC IdM support LIGO IdM?

Support “easy” enrollment in LIGO CO

- ▶ Expose campus LDAP (or ?) to COmanage
- ▶ Allows for pre-population of registration info
- ▶ Bind campus identity to LIGO (re-use identity)

How can campus IT and CIC IdM support LIGO IdM?

Standardize “in & out” timeframes

- ▶ Enable new campus people to come online quickly
- ▶ Harder is when to disable after people leave?
- ▶ Need a reasonable time for transition between orgs

How can campus IT and CIC IdM support LIGO IdM?

IdP and attributes

- ▶ Standardize release of (small) set of attributes
- ▶ Mostly need ePPN, givenName, sn, cn, mail
- ▶ OU, title, employeeType helpful but not required
- ▶ LIGO authz done using LIGO-specific attributes (at SP)

uApprove, if done well, seems appropriate

How can campus IT and CIC IdM support LIGO IdM?

IdP and SAML2

- ▶ Evolve to SAML2 (done?)
- ▶ Support SAML2 artifact resolution profile
 - ▶ Solves specific problem with LIGO wikis
- ▶ Support SAML ECP profile, deploy Shib IdP ECP extension
 - ▶ “Smart” command line tools for smart users
 - ▶ Simple wrappers around `curl` work well
 - ▶ Allows scientists to invoke RESTful WS with federated identity

How can campus IT and CIC IdM support LIGO IdM?

Shibboleth SP

- ▶ Help support campus deployments of LIGO SPs
- ▶ Groups want to provide LIGO web services
- ▶ Wikis common use case
- ▶ Some also want local access for colleagues
- ▶ (Some want mix of public and private pages)
- ▶ (Gets interesting for colleagues with no identity)
- ▶ Might require local discovery service

How can campus IT and CIC IdM support LIGO IdM?

InCommon certificate services

- ▶ SSL certificate service quite useful
- ▶ Caltech providing *.ligo.org for VirtualHost
- ▶ Some groups want local brand, so help is appreciated
- ▶ Consider deploying MyProxy/GridShib like service?
- ▶ Consider developing KerbShib?
 - ▶ Command line tool to get Kerb ticket via SAML2
 - ▶ Could leverage the SAML2 ECP profile