



LIGO Laboratory / LIGO Scientific Collaboration

LIGO-T1200490-v2

LIGO

Wednesday, October 31, 2012

LIGO Mailing List Group Configuration

Warren G. Anderson

Distribution of this document:

LIGO Scientific Collaboration and others authorized to access LSC computing resources

California Institute of Technology
LIGO Project – MS 100-36
1200 E. California Blvd.
Pasadena, CA 91125
Phone (626) 395-2129
Fax (626) 304-9834
E-mail: info@ligo.caltech.edu

Massachusetts Institute of Technology
LIGO Project – NW22-295
185 Albany St
Cambridge, MA 02139
Phone (617) 253-4824
Fax (617) 253-7014
E-mail: info@ligo.mit.edu

LIGO Hanford Observatory
P.O. Box 159
Richland WA 99352
Phone 509-372-8106
Fax 509-372-8137

LIGO Livingston Observatory
P.O. Box 940
Livingston, LA 70754
Phone 225-686-3100
Fax 225-686-7189

<http://www.ligo.caltech.edu/>

1 Abstract

This document describes the interactions between two core pieces of LIGO identity management infrastructure, the LIGO LDAP directory and Grouper, and the LIGO Sympa mailing list service.

2 Introduction

LIGO, composed of the LIGO Laboratory and the LIGO Scientific Collaboration, consists of almost 1000 scientists in almost 100 institutions around the world. In order to achieve its scientific goals, LIGO scientists need to be able to communicate with one another on a daily (or sometimes much more frequent) basis. LIGO employs a variety of collaboration tools to allow this communication, but none are more important to the efficiency and productivity of LIGO than mailing lists.

Mailing lists are created on a per-list request basis in LIGO – committees, working groups, etc are not automatically given mailing lists. Some organizational groups within LIGO require no mailing lists, others require a single mailing list, and still others require several mailing lists. There are three models employed within LIGO for subscription to mailing lists – mandatory subscription (if you meet certain criteria you must be subscribed to the list), controlled subscription (a list administrator decides who may and may not subscribe or unsubscribe to the list), and voluntary subscription (you may subscribe and unsubscribe to the list as you wish). There are no secret mailing lists in LIGO – all members of LIGO are allowed to know of the existence of all mailing lists. Lists can, however, have different levels of access control on knowledge about list specifics, for instance who is subscribed to the list or access to email message archives.

Previously, when there was an order of magnitude fewer LIGO scientists and institutions involved, LIGO employed a number of mailman servers hosted in an ad-hoc manner around the world to provide mailing list services. This solution, however, does not scale – users have trouble figuring out where to go to request help with subscriptions, administrators may or may not know who should be allowed to subscribe, or even if a given user requesting access is a member of LIGO, and many subscriptions never expired, despite the fact that the user had left the collaboration, perhaps years ago.

Currently, LIGO employs a centralized Sympa server that ties into the centralized identity management of LIGO. This provides more transparency for users, improved ability to administer and manage lists, and a scalability that were absent from the previous ad hoc solution. This document gives an overview of how mailing list authorizations are configured and managed in LIGO.

3 Tools

The mailing list service currently employed by LIGO is Sympa. As of this writing, the version we are using is Sympa 5.3.4-2ubuntu2. Sympa typically uses an internal database to track subscriptions and other user information used in authorization scenarios. LIGO minimizes the reliance on this database by using the LIGO.ORG Kerberos realm as an authentication mechanism and by drawing authorization information from the LIGO LDAP service.

There are three components of the LIGO identity management (IdM) infrastructure that interact to provide authorizations. The first is Sympa itself, which is easily configured to draw information from many backend IdM tools, including and LDAP directory. The second is the LIGO

LDAP directory, which stores information about groups of individuals in LIGO who are authorized to use various services. Finally, group information is managed via grouper, which reads user entity information from the `ou=people` stem of the LIGO LDAP directory and writes group information back into the LDAP directory in the `ou=grouper` stem of the stem of the directory.

4 Authorizations in Sympa

There are a variety of access control knobs that can be set in the Sympa. In principal, LIGO wishes to set all of these using groups managed in Grouper and exported from the LIGO LDAP directory. Two of these controls are global to the Sympa service – the group of Sympa admins and the group of recipients of Sympa service level email alerts. Both of these are controlled through the “listmaster” sympa parameter. In Sympa, the listmaster is a configuration parameter that is composed of an email address and a password. Logging into the web interface with this email address and password gives Sympa administrator level access, which allows superuser privileges throughout the Sympa interface. When system level alerts are created, they are sent by default to the listmaster email address. These functions could be separated, if desired, by creating an email alias that is drawn from one Grouper group but creating a different group that can authenticate to the Sympa web interface as listmaster. Currently, neither of these access controls are managed in our system via groups. Two individuals are aliased to receive the listmaster emails and these same individuals know the Sympa listmaster password.

All other access controls are created on a per list basis. The following table lists the authorization groups used by LIGO for access controls:

| Authorization | Description | Default Value | Notes |
|---------------|---|-----------------|---|
| subscriber | Group of list subscribers. | None. | Group membership can be controlled by individual users or by list administrators. ¹ |
| moderator | Group of list moderators. | None. | Group membership is assigned when list is requested. |
| post-only | Group who can send mail to the list without moderation. | All LIGO users. | Other values in use include subscribers only, subscribers plus guests only, all LIGO users plus automated service emails. |
| view-archive | Group who can view list's email archives. | All LIGO users. | Only other value in use at present is subscribers only |
| admin | Group who can change list configurations through the web interface. | listmaster | Currently, all list configuration goes through listmaster as other options have proved untenable in the past. This is not a group, but should be. |

¹ Although in principal we would like subscriber list admin to be handled by members of a subscriber-admin group, we do not have an interface that is suitable at the present time.

Because of LIGO mailing list policies, there are some authorizations that are set through default policies in Sympa and that we therefore do not need separate authorization groups for. For instance, because we have a policy of no secret lists, the view-list-info authorization is always set to “everyone can view”. Because only LIGO users can access the web interface, this is in practice equivalent to “all LIGO users can view”. Likewise, we have a policy that anyone who can post to a list should be able to view the recipients, so view-member-info is set to be the same as post-only from the table above. Finally, LIGO does not use the shared documents feature of Sympa, so view-shared-docs and edit-shared-docs are set to Sympa’s defaults.

Finally, there are a number of Sympa access controls that are made irrelevant by virtue of the fact that we use our LDAP directory rather than Sympa’s internal database to store subscription information. These are add-subscribers, delete-subscribers, and invite-subscribers. As mentioned above, subscribers are added via two mechanisms – user’s may add or delete their own membership to the subscriber group for the list through a custom built web interface to Grouper, or list requestors can maintain subscriber groups through requests to listmaster (who is assumed to have administrative access to the appropriate functions in Grouper). Also, we do not initiate remind processes, so Sympa’s remind-subscribers authorization is also not used. All of the values for these parameters are set to “closed”, as though the list was closed, so that no subscription options appear for users within the Sympa web interface.

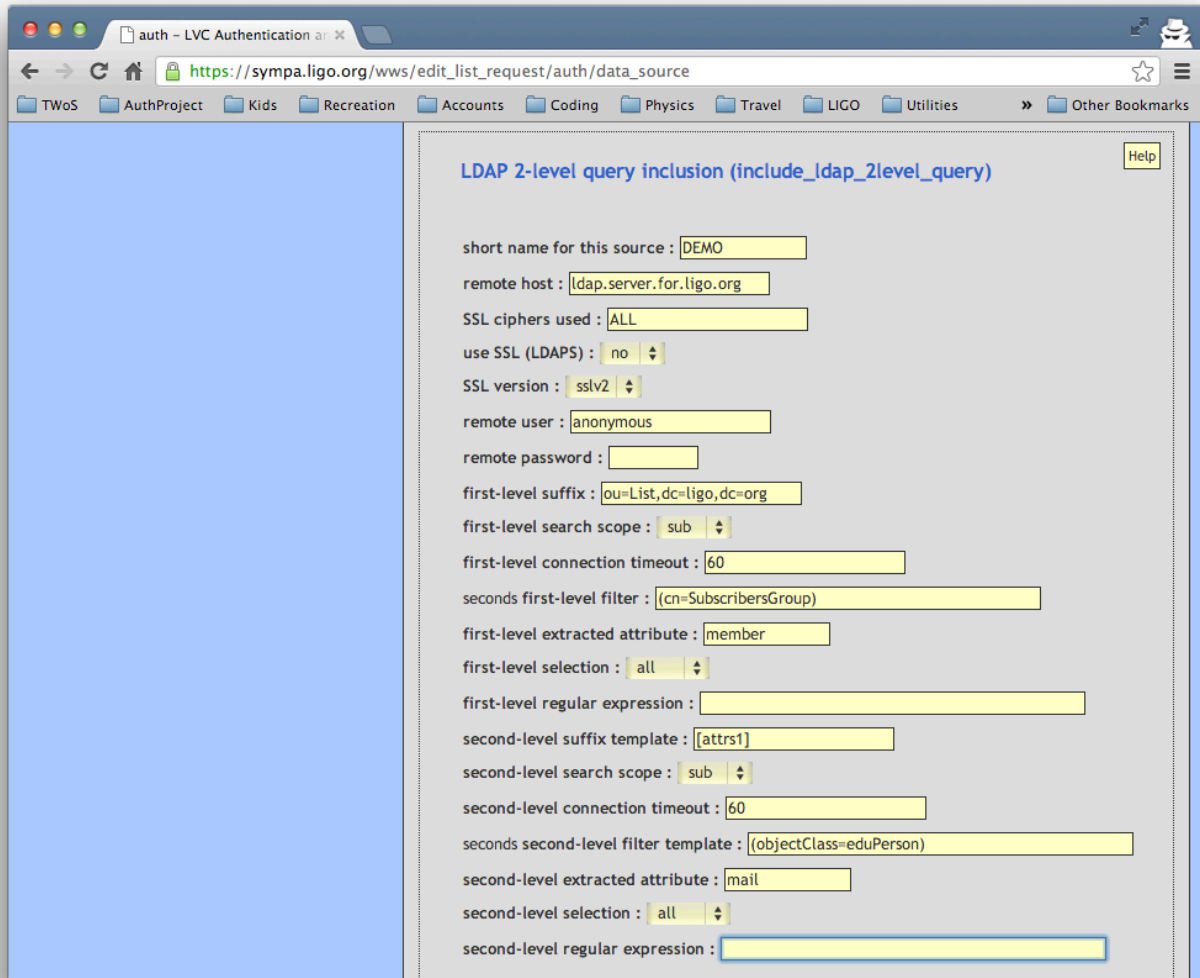
This is the current state of authorizations for Sympa within LIGO, however, as mentioned above, there are two further per-list authorization groups that we wish to make in the future:

| Authorization | Description | Default Value | Notes |
|------------------|--|---------------|---|
| subscriber-admin | Group responsible for adding and deleting subscribers for non-self-subscribed lists. | None | Membership to this group will be assigned when list is requested. |
| admin | Group who can change list configurations through the web interface. | Sympa admins | |

5 Importing LDAP Groups into Sympa

Setting up access control groups in the LIGO LDAP directory via Grouper is relatively straightforward. Furthermore, Sympa has facilities built into it to draw information from an LDAP directory for a large variety of authorization scenarios. Nonetheless, the configuration of Sympa needed to import group information from the LIGO LDAP is sufficiently opaque that it is worth elaborating on the process here. We describe the configuration on a per-authorization basis.

subscribers – subscribers is the most straightforward group to import into Sympa. We use the two-level LDAP query built into Sympa to first find the members of the appropriate group and then to find the email addresses of the members. The relevant Sympa configuration parameters and how they are set are shown in the following configuration screen capture.



The screenshot shows a web browser window with the URL `https://sympa.ligo.org/wws/edit_list_request/auth/data_source`. The page title is "LDAP 2-level query inclusion (include_ldap_2level_query)". The configuration parameters are as follows:

- short name for this source : DEMO
- remote host : ldap.server.for.ligo.org
- SSL ciphers used : ALL
- use SSL (LDAPS) : no
- SSL version : sslv2
- remote user : anonymous
- remote password : (empty)
- first-level suffix : ou=List,dc=ligo,dc=org
- first-level search scope : sub
- first-level connection timeout : 60
- seconds first-level filter : (cn=SubscribersGroup)
- first-level extracted attribute : member
- first-level selection : all
- first-level regular expression : (empty)
- second-level suffix template : [attrs1]
- second-level search scope : sub
- second-level connection timeout : 60
- seconds second-level filter template : (objectClass=eduPerson)
- second-level extracted attribute : mail
- second-level selection : all
- second-level regular expression : (empty)

moderators – moderators are set through the `editor_include` parameter, which imports a data-source file in the directory `/etc/sympa/data_sources`. This file gives the parameters for a two-level query like the one above. An example is shown here:

```
include_ldap_2level_query
    host ldap.server.for.ligo.org
    port 389
    user anonymous
    suffix1 ou=List,dc=ligo,dc=org
    scope1 sub
    filter1 (cn=ModeratorsGroup)
    attrs1 member
    select1 all
    suffix2 [attrs1]
    scope2 sub
    filter2 (objectClass=eduPerson)
    attrs2 mail
    select2 all
```

post-only – this is one of the most complicated groups to use. There are two Sympa configuration files involved in creating the authorization to post to a list. The first is an LDAP search filter definition file, located in `/etc/sympa/search_filters/`. An example is shown here:

```
# myListPostOnlyFilter.ldap – example LDAP filter file.

host      ldap.server.for.ligo.org:389
suffix    ou=people,dc=ligo,dc=org
filter    (&(|(mail = [sender])
              (mailAlternateAddress = [sender])
              (mailForwardingAddress = [sender])))
              (isMemberOf=Path:To:List:PostOnlyGroup))
scope     sub
```

This file identifies if a posting is from any email address that is stored in the `mail`, `mailAlternateAddress` or `MailForwardingAddress` attributes of any member of the post-only group for the mailing list.

The second configuration file for post-only is a scenario file, located in `/etc/sympa/scenari/`. An example is shown here:

```
# send.myList - configuration for who can post to myList

title.gettext Members of List:PostOnly group can post
                without moderation, all others held.

search(myListPostOnlyFilter.ldap)  smtp,smime,md5    -> do_it
is_editor([listname],[sender])     smtp,smime,md5    -> do_it
true()                             smtp,smime,md5    -> editorkey
```

Details of the syntax and semantics of these scenario files are found in the Sympa documentation, the essential element demonstrated here is that scenario files use the LDAP filter files located in `/etc/sympa/search_filters/` to pull group information out of LDAP and create authorizations for particular actions, in this case posting to a list without being held for moderation.

view-archive – this group is accessed by Sympa in the same way that the post-only group is, via an LDAP filter in `/etc/sympa/search_filters/` like:

```
# myListViewArchiveFilter.ldap - another example LDAP filter file.

host    ldap.server.for.ligo.org:389
suffix  ou=people,dc=ligo,dc=org
filter  (&(mail = [sender])
        (isMemberOf=Path:To:List:ViewArchiveGroup))
scope   sub
```

and a scenario file is located in `/etc/sympa/scenari/` like this:

```
# viewArchives.myList - configuration for who can view myList
#                               archives.

title.gettext restricted to List:ViewArchiveGroup members

is_listmaster([sender])          md5,smime -> do_it
search(myListViewArchiveFilter.ldap) smtp,smime,md5 -> do_it
true() md5,smime -> reject(reason='web_archive_local_user_sub')
```

This example takes advantage of the fact that for LIGO users the Apache `REMOTE_USER` environment variable is populated by the Kerberos principal, which happens to be identical to the `mail` attribute for all LIGO users. In a federated model, where `REMOTE_USER` cannot be guaranteed to match the email address, one would have to make a more sophisticated filter. Nonetheless, given a sufficiently well designed LDAP, there is nothing preventing us from using the same general mechanism.

6 Future Group Imports

As mentioned in a previous section, there are two other authorization groups we would like to implement going forward. The first is for an authorization that is already in use, the **admin** authorization for each list. In our Sympa installation, this authorization defaults to `listmaster`, and we do not override it. However, Sympa provides a mechanism to import an LDAP group for the **admin** authorization that is identical to the one for the **moderator** authorization, so it will be easy to implement the **admin** authorization via grouper on a group-by-group basis going forward.

The second new authorization that we will be implementing via groups in the future is **subscriber-admin**. Since in our model subscription lists are not kept in Sympa itself, the **subscriber-admin** group would not be imported into Sympa. Rather, our plan is to create a web services interface for Grouper that allows management of the **subscriber** group for each Sympa list. The **subscriber-admin** group for a Sympa list would then be used to define who had permission to use the web services interface to manage the **subscriber** group for that list. Authorization checking will likely be implemented via standard Shibboleth mechanisms.