NA62 Electronic Logbook

Phil Rubin

August 10, 2012

1 Introduction

THE PSI ELOG [1] electronic logbook has been implemented for NA62. Its installation, configuration as of the date of this note, and basic usage are here described.

2 Installation

An experiment's logbook should probably be reliable, simple to use, accessible, and secure. The PSI ELOG was chosen not just because it can to some extent be characterized in these terms, but also because of its extended history of use as a logbook for experiments, it's continued maintenance and support at PSI, its employment at CERN (LHCb and ATLAS, and formerly CMS), and its familiarity to the author.

For the logbook to be accessible from outside the NA62 private network (PN), its server should be on the CERN general purpose network (GPN), but, for the sake of security, CERN required that access then be shielded by CERN's Single Sign On protocol, ssl encryption, and appropriate firewall protection.

2.1 CERN Virtual Machine

The networking requirement was met without dedicated hardware through the computer center's virtual machine arrangement. The self-service kiosk

`https://vmm.cern.ch/vmm/`

made available on 27 July 2012, a single-processor, 2-GByte memory, virtual machine with a 40-GByte system disk, running slc6-x86_64. Its DNS designation is

`vmna62s1.cern.ch`

Its root filesystem contains the full array of CERN utilities, including AFS. The author is presently the designated owner and main user. By default, the machine

is considered a development machine, and its service level is the lowest available (bronze), which dictates a six-month lifetime (expiration date, 26 January 2013) and no candidacy for automatic computer center backups. Once the functionality of the logbook is verified, the service level can be raised, by "creating an incident in ServiceNow," to gold (there's also a silver level, at which backups are possible), which entails elimination of an expiration date and institution of automatic backups.

2.2 Security

CERN computer security required that external access to the logbook server, residing in the GPN but accessible from the PN, be shielded by the CERN Single Sign On (SSO) protocol. Installation directions at

`http://linux.web.cern.ch/linux/scientific6/docs/shibboleth.shtml`

were followed.

The following packages were installed:

- shibboleth
- log4shib
- xmltooling-schemas
- opensaml-schemas
- mod_ssl

User and host certificates and keys were obtained from http://cern.ch/ca. The host certificate was placed in /etc/httpd/conf/ssl_crt, and the host key was placed in /etc/httpd/conf/ssl_key.

In addition, the following files were downloaded and placed in /etc/shibboleth/

- `http://linux.web.cern.ch/linux/scientific6/docs/shibboleth/shibboleth2.xml`
- `http://linux.web.cern.ch/linux/scientific6/docs/shibboleth/ADFS-metadata.xml`
- `http://linux.web.cern.ch/linux/scientific6/docs/shibboleth/attribute-map.xml`
- `http://linux.web.cern.ch/linux/scientific6/docs/shibboleth/wsignout.gif`

The file /etc/shibboleth/shibboleth2.xml was modified as follows:

- the listener host (localhost) was set

  ```
  <TCPListener address="127.0.0.1" port="1600" acl="127.0.0.1"/>
  ```

- all occurrences of somehost.cern.ch were replaced by vmna62s1.cern.ch:
  - `<Site id="1" name="somehost.cern.ch"/>`

- `<Host name="somehost.cern.ch"/>`
- `<ApplicationDefaults id="default" policyId="default" entityID="https://somehost.cern.ch/Shibboleth.sso/ADFS" homeURL="https://somehost.cern.ch" ....`
- `<saml:Audience>https://somehost.cern.ch/Shibboleth.sso/ADFS</saml:Audience>`

SELINUX enforcement was modified by changing SELINUX=enforcing to SELINUX=permissive in /etc/sysconfig/selinux. The change was effected by

```
/usr/sbin/setenforce Permissive
```

The file /etc/sysconfig/shibd was created to contain the two lines:

```
LD_PRELOAD=/opt/shibboleth/lib64/libcurl.so.4
export LD_PRELOAD
```

The following was added to the file /etc/httpd/conf.d/shib.conf:

```
SSLRequireSSL   # The modules only work using HTTPS
AuthType shibboleth
ShibRequireSession On
ShibRequireAll On
ShibExportAssertion Off

Require valid-user
Require ADFS_GROUP "na62-news"
```

Note that this limits access to NICE password holders in the na62-news egroup.

The line

```
LoadModule ssl_module modules/mod_ssl.so
```

was added to /etc/httpd/conf/httpd.conf.

The SSO/ADFS application was then registered with CERN at

```
http://www.cern.ch/winservices/SSO/registerapplication.aspx
```

Once registration was acknowledged, the daemons shibd and httpd were (re)started:

```
chkconfig --levels 345 shibd on
service shibd start
service httpd restart
```

3 Configuration

An account elog, with associated group elog, was created on vmna62s1. The ELOG daemon will not run in the root group, for security reasons, and therefore a local user and group was created. ELOG source files were downloaded into the elog home directory, /home/elog/:

```
svn checkout svn+ssh://svn@savannah.psi.ch/repos/meg/elog/trunk elog
svn@midas.psi.ch's password: svn

svn checkout svn+ssh://svn@savannah.psi.ch/repos/meg/mxml/trunk mxml
svn@midas.psi.ch's password: svn
```

It should be noted that the password had to be entered twice in each case.

In the directory, /home/elog/elog, Makefile was modified to include Kerberos integration with AFS, so that NICE passwords would be the default for ELOG: `USE_KRB5 = 0` ⇒ `USE_KRB5 = 1`.

ELOG was built and installed.

```
make
make install
```

The default base directory is /usr/local. The ELOG daemon script is placed in /etc/init.d/

3.1 Configuration File

A configuration file, /usr/local/elog/elogd.cfg, controls the behavior and look of ELOG. The complete syntax of the file can be found at

`http://midas.psi.ch/elog/config.html`

The NA62 configuration as of the date of this note was:

```
[global] ; general instructions for the ELOG server
Port = 8080 ; 8080 is the default port, so this need not be here
SMTP host = cernmx.cern.ch ; CERN's anonymous mail server
Usr = elog ; daemon account
Grp = elog ; daemon group
Logbook Tabs = 0 ; turn of quick switch between logbooks
Page title = NA62 Logbook
List Page title = NA62 Logbook
Protect Selection page = 1 ; require login to access logbook
Password file = na62.pwd
Logfile = elog.log
Logging level = 2 ; log logins, logouts, and write accesses
URL = https://vmna62s1.cern.ch/elog
Admin user = rubinp
Authentication = Kerberos ; use NICE passwords

[NA62Logbook]
Theme = default ; use default skin
Title image = <img border=0 src="NA62logo.gif" alt="NA62 logo">
Comment = NA62 Logbook
Time format = %A, %d %B %Y, %H:%M
```

```
Page Title = NA62 Logbook - $subject
Menu commands = List, New, Find, Help
List Menu commands = New, Find, Help, Logout
Attributes = Author, Type, Category, Subject
Options Type = Routine, Problem(s), Other
Options Category = General, Beam, Hardware, Software, Trigger, Computer/Network
Extendable Options = Category
Required Attributes = Author, Type, Category, Subject
Quick filter = Type, Category, Subject
Self register = 1 ; users register on their own
Allow password change = 0
Reverse sort = 1 ; start list page with newest entry
Default encoding = 1 ; default display font is plain text
Allowed encoding = 3 ; allow plain text and ELCode, not html
                     ; (http://midas.psi.ch/elog/ELcode_en.html)
List after submit = 1 ; return to list after adding new entry
Fix text = 1 ; disallow entry editing after submission
Refresh = 1800
Bottom text login = <center><img src='lock.png'>
<a href="https://login.cern.ch/adfs/ls/?wa=wsignout1.0" target="_top">
CERN SSO logout</a></center>
```

The ELOG service is a daemon process:

```
chkconfig --level 345 elogd on
service elogd start
```

3.2 Attachments

Uploading of attachments is enabled. ELOG converts images with ImageMagick to png format for viewing in the logbook. Clicking on the image file opens the default image utility. ImageMagick had to be installed on mvna62s1.

3.3 Backups

ELOG entries are saved in plain ASCII format in files by day. Specifically, each day's entries, if there are any, are save in a single file created that day and labeled YYMMDDa.log (YY is the year, MM the month, and DD the day). Individual entries in a file are separated by the string @MID@. Should this string for some reason be written into an entry, it is converted automatically so as to preserve the validity of the database structure. Entry files are located in /usr/local/elog/logfiles/NA62Logbook/

3.3.1 cron jobs

A daily backup of entry files is made and stored in /usr/local/logbook_backups. A full backup of most of /usr/local/elog and, separately, of the ELOG password

file, na62.pwd, is done once a week and stored in the same directory. The latest of these weekly backups is copied to /afs/cern.ch/user/r/rubinp/private/elog/. The daily backups are purged after 30 days, and the weekly backups are purged after 90 days.

4 User Guide

4.1 Logging In

From any browser window, the NA62logbook book is available at

`https://vmna62s1.cern.ch/elog`

The url `https://vmna62s1.cern.ch` invokes a javascript that should bounce to the logbook page, but will work, of course, only on browsers supporting and enabled for javascript.

A certificate warning may appear if the CERN host certificate has not been permanently accepted. The accompanying dialog allows the warning to be circumvented temporarily or permanently.

Once the certificate is handled, the CERN SSO page will come up, and login with CERN username and NICE password is required.

Successful login will bring up the ELOG login page [see Figure 1]. If this is

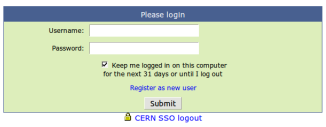

Figure 1: ELOG login page.

the first time logging in, select `Register as new user` and fill in the requested information. Use a CERN e-mail address in case of a desire for e-mail notification, as CERN-to-CERN e-mail is all that is permitted by the anonymous server. NICE passwords are assigned by default. Otherwise, login with CERN username and password. Note that the SSO logoff link is available from this page, which will reappear after ELOG logout.

The NA62 logbook listing page should then be accessible [see Figure 2].

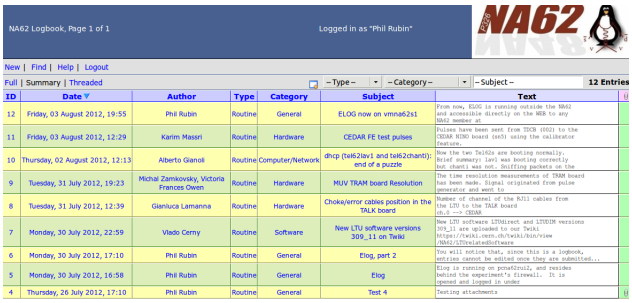

Figure 2: ELOG listing page.

4.2 Using ELOG

A link to a users' HELP menu is provided at the upper left of the listing page, just below the page header.

Notice that the listing page lists the most recent entry first. From the listing page, there are at present four options:

4.2.1 Reading

Any entry may be read by clicking on one of the active links in the listing row. From an entry page, just hit the back arrow to return to the listing page.

4.2.2 Searching

Three search methods are available:

Column Sorting The listing page may be resorted by selecting a relevant column heading. Column sorting permits both ascending and descending arrangements. By default, the listing is sorted by entry ID in descending order.

Quick Filter Selecting the type and/or category from the pull-down menus, and/or entering a subject keyword in the `--Subject--` box, and then entering a carriage return, will filter the listing to just those entries that meet the filtering criterion/criteria.

Find An advanced search facility is available by clicking the Find link.

5 Writing

An entry may be added by clicking on the New link. A timestamp is automatically included. Four required fields–author (or authors), type, category, and

subject–must be entered, or the submission will not be accepted. Text is optional, but may be written in either plain text (default) or ELCode. The latter affords font enhancements. Click on the ELCode link

(`http://midas.psi.ch/elog/ELcode_en.html`)

for additional information and guidance.

Attachments may be uploaded from local disc, with the utility provided at the bottom of the New Entry page.

Successful submission automatically returns to the listing page, which is refreshed to include the new entry.

Once submitted, entries are no longer editable or deletable.

6 Exiting

Clicking the Logout link on the listing page returns to the login page. The CERN SSO logout link is underneath the login box.

7 Additional Available Features

Possible enhancements to the basic logbook described above include e-mailing entries (working, but not implemented; this can be configured to tailor notification to different individuals by topic, category, and perhaps subject); RSS feeds; check sheet entry and logging; and automatic logging of run-control and DCS messages.

8 Acknowledgements

The installation of the logbook was expedited with the aid of Diana Scannicchio and Sergio Ballestrero of the ATLAS TDAQ SysAdmin team and Stefan Lüders, Head of Computer Security.

References

[1] http://midas.psi.ch/elog/