Lire: Integrated Analysis of all your Internet and Intranet Services

Joost van Baal <joostvb@logreport.org>
LogReport http://www.logreport.org/

FOSDEM, Brussels, 17 february 2002

Who does not speak Dutch?

Table of Contents

This talk will discuss the technical aspects of Lire as well as the organisational aspects of LogReport as an open source project.

Log file analysis

Log file analysis is

- too often neglected, but
- giving access to invaluable information; however
- tedious and time-consuming, so
- in need for both flexible and generic software.

Why use Lire**?**

Lire is

- generic
- flexible
- free, in both senses of the word
- actively maintained, in an open environment
- highly configurable
- very portable
- secure

Lire's users

Lire is valuable for both

- system administrators, and
- business managers

Lire **supported log files**

Lire currently supports log files from

- www (apache, IIS, ...)
- dns (bind)
- firewall (cisco IOS, Linux, IP Filter, WELF)
- email (Exim, Postfix, qmail, sendmail, NMS)
- print (CUPS, LPRng)
- ftp (ProFTPD, WU-FTPD, MS IIS)
- proxy (squid, WELF, MS ISA)
- database (MySQL)

Ease of installation

Lire is GPL-ed, and comes as a tarball ("autoconfiscated"), as an RPM and as a Debian package. Written in Perl and shell, so runs on any Unix-like OS.

Table of Contents

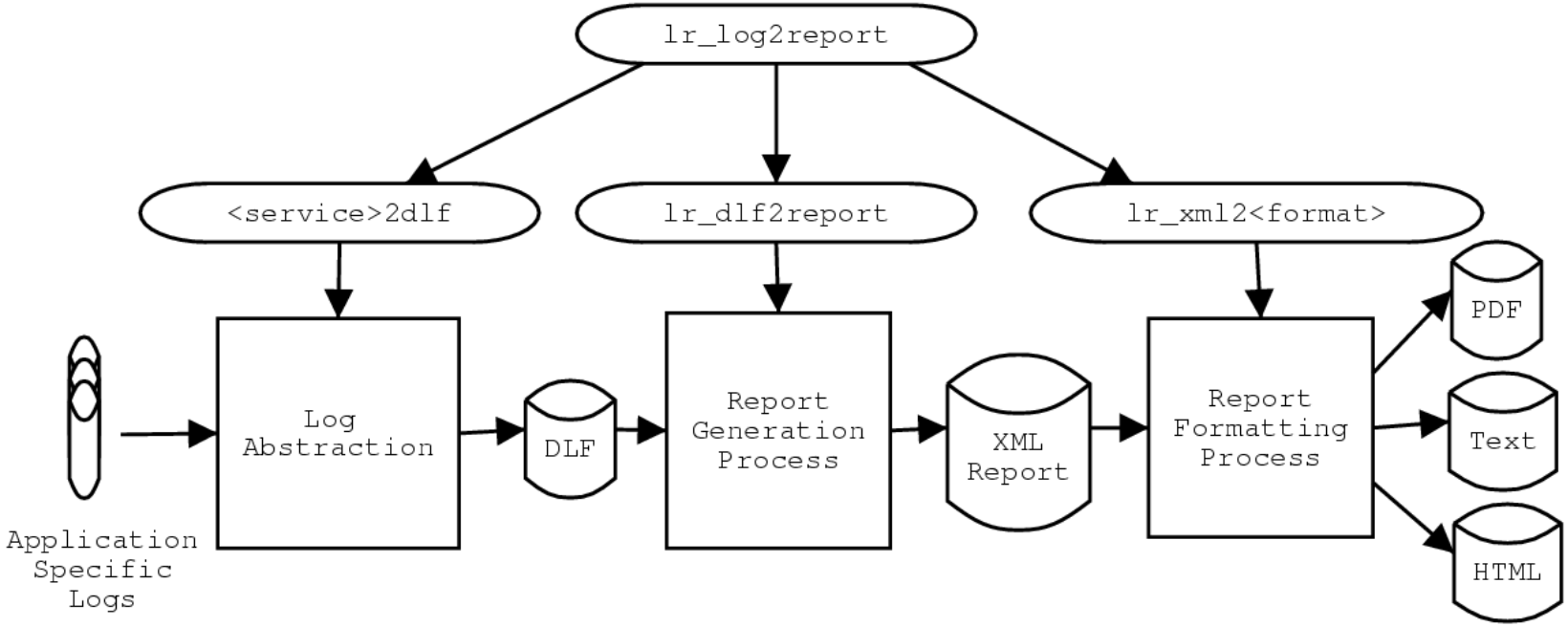
services, superservices and dlf's

dlf "distilled log format" space separated, line oriented, fixed fields

service raw log file format

superservice a class of services, sharing same dlf and report

Lire's Architecture

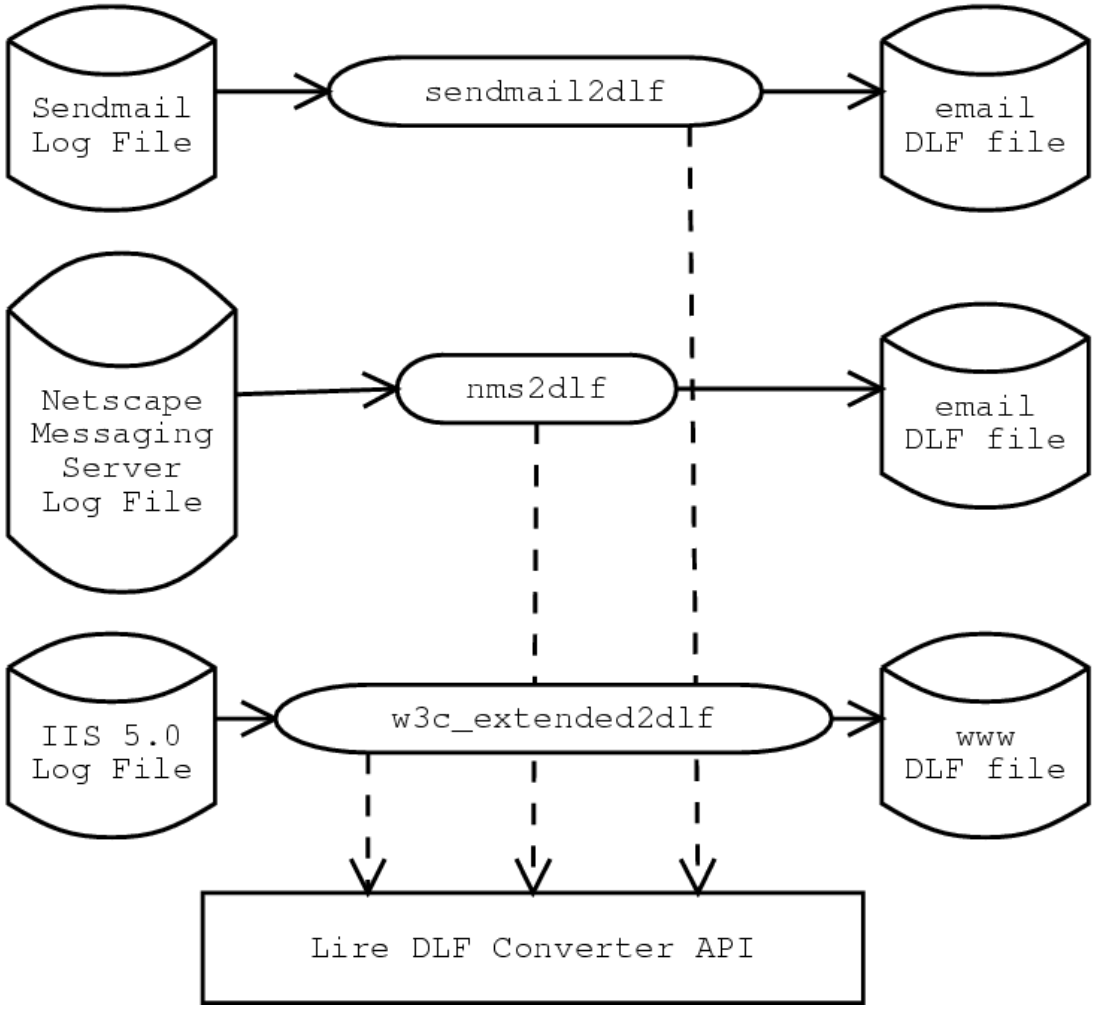


Running Lire

One can run Lire:

- as online responder
- as client
- from cron
- from command line

dlf **convertors**



Services and Superservices

A service:

- one raw log file format
- generally one service is one application
- belongs to one superservice
- example: the postfix service

A superservice:

- one dlf format
- a set of supported subreports
- a set of services
- example: the email superservice.

email dlf format

```
[...]
<lire:field name="time"        type="timestamp" default="0"/>
<lire:field name="queueid"     type="string"    default="-"/>
<lire:field name="from_user"   type="string"    default="-"/>
<lire:field name="from_domain" type="hostname"  default="-"/>
[...]
```

Report Specification

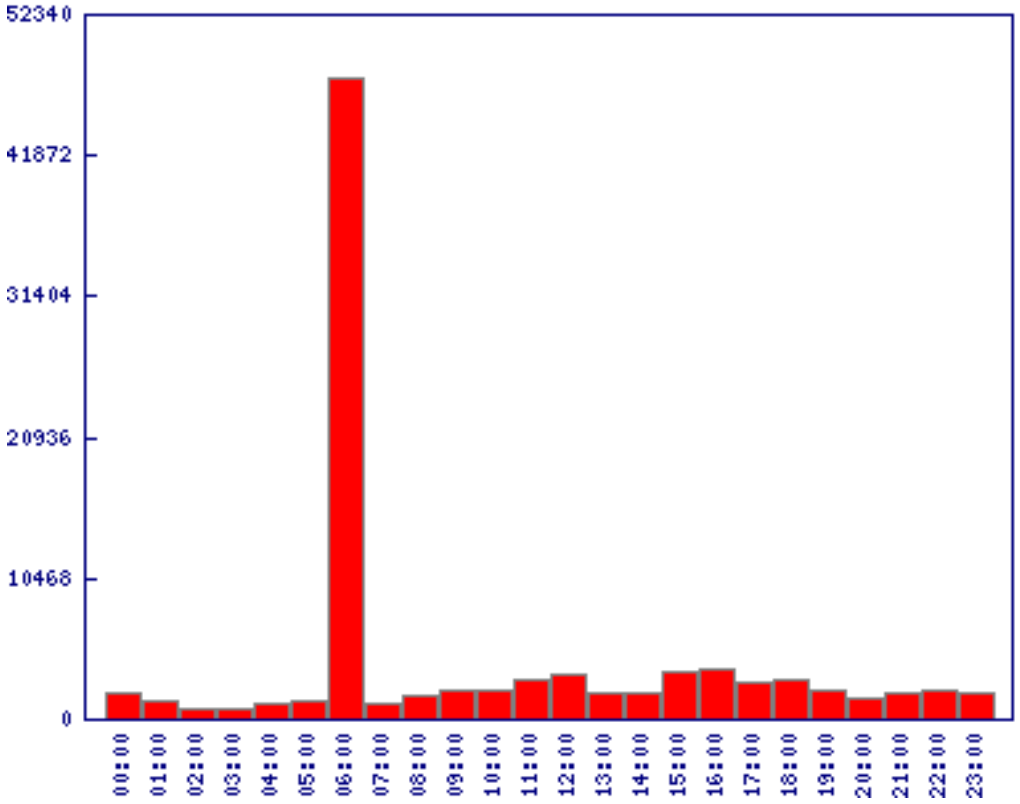
```
[...]
<lire:report-calc-spec>
 <lire:group sort="-mail_volume" limit="$domain_to_show">
  <lire:field name="to_domain"/>
  <lire:sum name="mail_volume" field="size"/>
 </lire:group>
</lire:report-calc-spec>
[...]
```

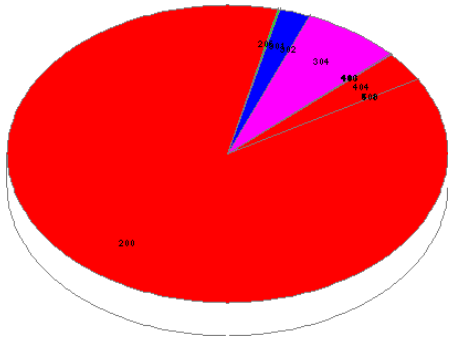
Report configuration file

```
# Report configuration for the proxy superservice

=section General
requests-summary

=section Denied Sites Reports
|select-cache_result result=TCP_DENIED
top-destinations            dsts_to_show=50
top-users-by-destinations   users_to_show=30 dsts_to_show=50
[...]
```

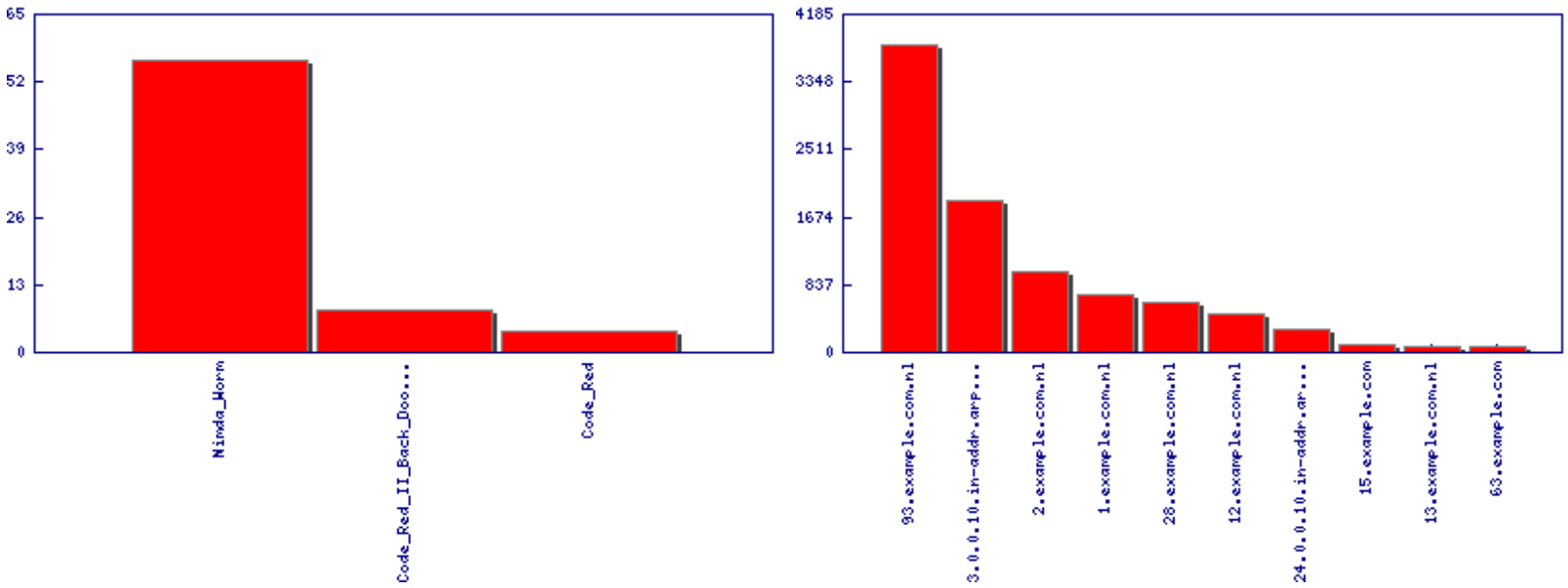
Example Graphical Reports

Some reports from the www superservice





Some reports from the www and dns superservices



Lire's Scripts

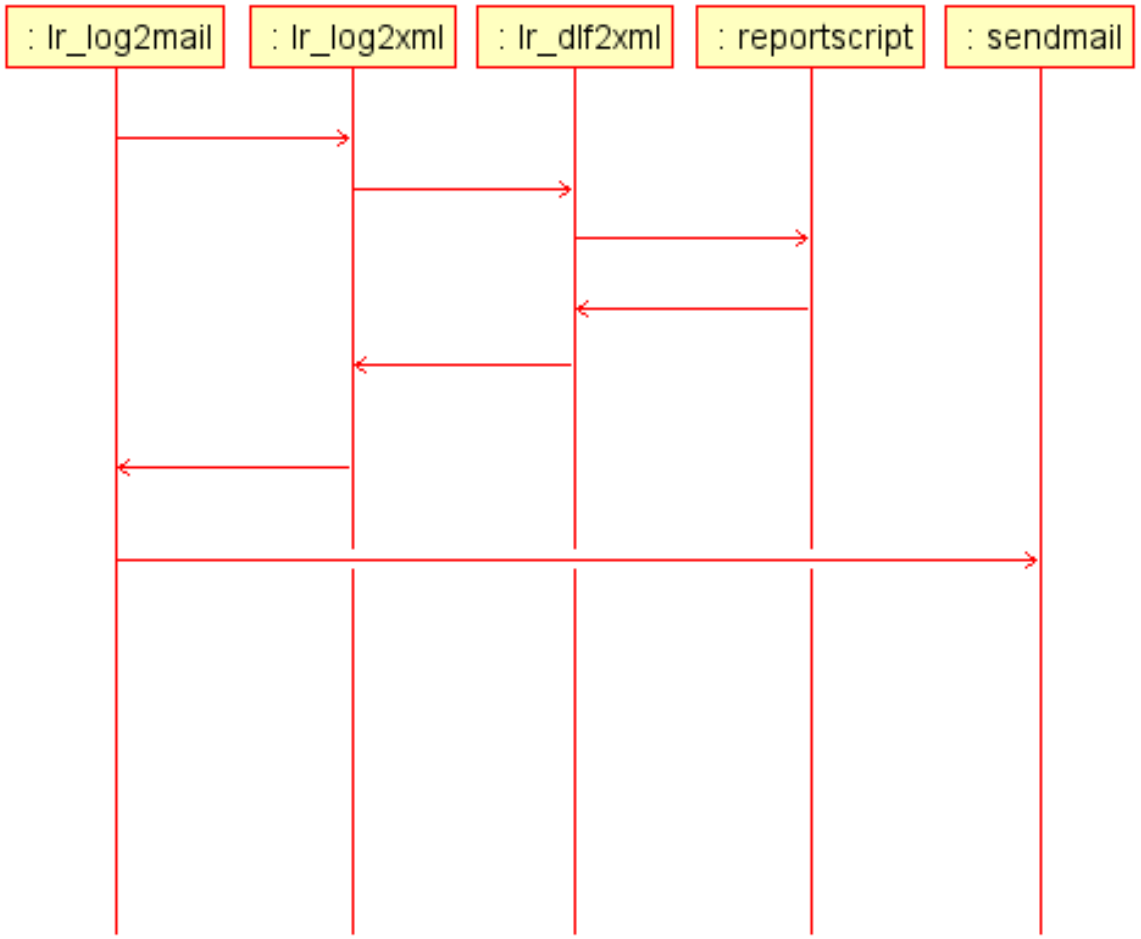


Table of Contents

- Log file analysis
- Lire Overview
- Lire's Architecture
- Lire's Future
- The LogReport Project
- More information, contact, questions

Release, Roadmap

lire-20020214.tar.gz is realised!

But we have more plans:

- merging and splitting of reports and log files
- display
- performance: jade
- more services
- online responder
- configuration interface

LogReport people

LogReport developers

- Joost van Baal
- Wessel Dankers
- Josh Koenig
- Francis Lacoste
- Egon Willighagen

LogReport board

- Teus Hagen (chairman)
- Wytze van der Raay (treasurer)
- Jakob Schripsema (secretary)

How to help

- Use our Online Responder
- Sent (anonimized) log files
- Download Lire, and use it
- Give feedback on our mailinglists: feature requests, bug reports, help other people
- Even better: send patches and add support for other services
- Promote Lire: via webpages and mailinglists
- Fund us.

More information, contact info

website `http://www.logreport.org/`

mailing lists (archived) `questions@logreport.org`, `development@logreport.org`

irc `#logreport` on OPN

announcements `announcement@logreport.org`

Questions?