HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza LIRE alata za analizu log datoteka

CCERT-PUBDOC-2004-05-75

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

Gotovo svi poslužiteljski programi na modernim operacijskim sustavima posjeduju ugrađenu podršku za praćenje i nadzor rada, korištenjem log datoteka. Sadržaj ovih datoteka ovisi o poslužitelju, operacijskom sustavu i formatu log datoteke, a u nju se najčešće upisuju specifični podaci vezani uz rad poslužitelja. Tako se na primjer kod poslužitelja za prijenos elektroničke pošte u ove datoteke upisuje svako slanje i primanje poruka elektroničke pošte, podaci o odbijenim porukama te brojne druge slične informacije.

Ovakve datoteke najčešće sadrže ogromnu količinu informacija koje nije moguće interpretirati letimičnim pregledom pojedinih datoteka i zapisa, što znatno otežava ručno praćenje stanja sustava i servisa. Budući da je za sigurnost sustava redovito praćenje log datoteka od ključnog značaja, u tu svrhu se najčešće koriste automatizirani alati. Lire je jedan od takvih alata, koji posjeduje ugrađenu podršku za velik broj formata log datoteka, što omogućuje praćenje gotovo svih važnijih servisa na sustavu. Trenutno je pomoću ovog alata moguće analizirati sadržaje log datoteka različitih programa, odnosno servisa:

- **WWW:** Apache, Boa, Microsoft IIS;
- **E-mail:** Exim, Postfix, Sendmail, Qmail;
- **DNS:** Bind 8 i 9;
- **FTP:** ProFTPD, Wu-Ftpd, BSD ftpd;
- **Baze podataka:** MySQL;
- **Dialup veze:** isdn4linux;
- **Vatrozid:** Cisco IOS, ipchains, iptables;
- **Print servisi:** CUPS, LPRng;
- **Proxy:** Squid, Microsoft ISA;
- Syslog.

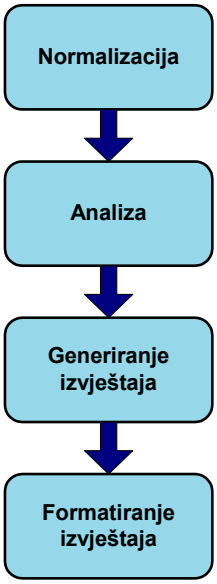
Također je ugrađena i mogućnost kreiranja vlastitih izvještaja koji prikazuju sažetak važnih podataka sadržanih u log datotekama, koji mogu biti u čistom tekstualnom, HTML, DocBook, PDF ili LogML formatu. Činjenica da je izvorni kod programa objavljen pod GPL (eng. *General Public License*) licencom osigurava brz razvoj podrške (praktički svakodnevno) za nove formate log datoteka i izvještaja.

Lire je trenutno moguće instalirati na GNU/Linux, BSD, Solaris, HP-UX, AIX i GNU/Hurd operacijske sustave.

Ovaj dokument opisati će osnovne postupke instalacije i upravljanja Lire alatom, uz kratak prikaz podešavanja oblika izvještaja za neke od važnijih servisa.

2. Arhitektura

Arhitektura Lire analizatora nastoji slijediti koncept univerzalnog alata za analizu log poruka. Zbog ovakve arhitekture, Lire je u mogućnosti analizirati log datoteke gotovo svih servisa pokrenutih na današnjim heterogenim računalnim mrežama, što ga čini jednostavnijim rješenjem za razvoj i upotrebu od danas često korištenih skripata koje se pokreću zasebno za svaki servis. **Slika 1** prikazuje proces obrade log datoteka.



Slika 1: Mehanizam obrade log datoteka korišten kod Lire alata

Koraci obrade su sljedeći:

- **Normalizacija** – u prvom koraku obrade, svi oblici log datoteka određenih skupina poslužitelja svode se na jedinstveni oblik. Tako će se npr. log datoteke svih ftp poslužitelja, bez obzira na proizvođača ili inačicu, svesti na identičan oblik, koji je u potpunosti u stanju opisati sve moguće log podatke prisutne kod ftp poslužitelja.
- **Analiza** – normalizirane datoteke analiziraju se u skladu sa konfiguracijom Lire alata i kreira se izlazna datoteka koja pobliže opisuje tražene podatke.
- **Generiranje izvještaja** – izlazni podaci analize uobličavaju se u izvještaj koji korisniku donosi pregled željenih podataka. U ovom koraku izvještaj je u XML formatu.
- **Formatiranje izvještaja** – posljednji korak u analizi log datoteka je pretvaranje izvještaja iz XML oblika u neki od oblika koji odgovara korisniku. Na raspolaganju je nekoliko formata izlaznih datoteka poput tekstualnog, PDF ili HTML.

Opisani modularan dizajn programerima olakšava izradu modula za podršku novih formata log datoteka. Detaljan opis rada pojedinih modula, kao i upute za izradu novih, nalazi se u dokumentu pod nazivom „*Lire Developer's Manual*“ koji se nalazi u poddirektoriju `doc` paketa s izvornim kodom programa ili na web stranicama proizvođača (http://www.logreport.org).

3. Instalacija

Lire je moguće instalirati prevođenjem izvornog kôda ili korištenjem gotovih binarnih paketa. Budući da je proces mnogo jednostavniji, manje iskusnim korisnicima se preporučuje korištenje binarnih paketa. Trenutno su na raspolaganju binarni .deb paketi za Debian distribuciju Linux sustava i RPM paketi za RedHat i sve ostale distribucije koje se temelje na RPM paketima (npr. Mandrake, Suse, ...). Instalacija binarnih paketa obavlja se standardnim postupkom za pojedinu vrstu paketa te se u ovom dokumentu neće pobliže opisivati.

Ukoliko se Lire instalira na operacijski sustav koji nije podržan navedenim binarnim paketima, prevođenje izvornog kôda jedini je način instalacije. Prije prevođenja, potrebno je osigurati postojanje određenih aplikacija i biblioteka na sustavu. Neophodno su potrebni sljedeći programi, odnosno moduli:

- GNU zip aplikacija za arhiviranje;
- Perl interpreter inačice 5.6.1 ili noviji (preporučuje se interpreter inačice 5.8.0);
- Expat inačice 1.9.x i XML::Parser inačice 2.29 ili noviji;
- Digest::MD5 modul (samo za inačice perl interpretera starije od 5.8.0);
- DBI modul za perl interpreter;
- DBD::SQLite0.29 modul ili noviji;
- Curses::UI modul;
- Libintl-perl grupa modula;
- Standardne Unix naredbe poput sh, cut, head, sort, grep i cat (naredbe se moraju nalaziti u stazi (engl. *path*) korisnika koji pokreće LIRE).

Za generiranje izvještaja u bilo kojem obliku drukčijem od čistog tekstualnog, potrebno je instalirati sljedeće alate:

- Xsltproc inačice 1.0.10 (ili kasniji);
- DocBook XML DTD (Document Type Definition) inačice 4.1.2;
- Jade ili OpenJade;
- XSL stylesheet za DocBook;
- TeX;
- JadeTeX;
- Ploticus;
- Libpng i zlib biblioteke;
- Libgd i libjpeg biblioteke.

U slučaju da postoji potreba za procesiranjem log datoteka većih od 2 gigabajta, perl interpreter na sustavu mora imati uključenu podršku za velike datoteke. To se može provjeriti izdavanjem naredbe '`perl -V`' koja bi u svom ispisu trebala sadržavati oznaku '`uselargefiles`'.

Proces instalacije Lire alata iz paketa s izvornim kodom započinje pokretanjem standardne `./configure` skripte, koja ispituje parametre sustava i priprema podatke potrebne za uspješno prevođenje koda. Kôd se prevodi pokretanjem naredbe `make`, a prevedene datoteke se kopiraju u odgovarajuće direktorije izdavanjem naredbe `make install`. Sve datoteke se automatski instaliraju unutar `/usr/local` direktorija, ukoliko parametrom `–prefix`, prilikom pokretanja `configure` skripte, nije specificirana proizvoljna lokacija.

Ukoliko na sustavu ne može pronaći neku od željenih datoteka, `configure` skripta će prijaviti grešku. Budući da je broj paketa o kojima ovisi uspješno funkcioniranje Lire-a popriličan, greške prilikom konfiguracije su vrlo česte. Paketi o kojima Lire ovisi trebali bi, za uspješan postupak konfiguracije, biti instalirani na uobičajenim mjestima. Ukoliko to nije slučaj, `configure` skripti potrebno je dati do znanja gdje se aplikacije nalaze. U tu svrhu najčešće se koriste varijable okoline. Tako je na primjer stazu do SGML/XML komponenata moguće podesiti uvođenjem sljedećih varijabli okoline:

```
DBK_XML_DTD=staza_do_docbook_direktorija/docbookx.dtd \,
DBK_DSSSL_STYLESHEETS= staza_do_docbook_dsssl_direktorija \,
DBK_XSL_STYLESHEETS= staza_do_docbook_xsl_direktorija \ ,
```

a staze za ostale aplikacije, pomoću sljedećih varijabli:

- PATHTOPERL - perl interpreter;
- PATHTOJADE - jade DSSSL interpreter;
- PATHTOPDFJADETEX - pdfjadetex naredba;
- PATHTOXSLTPROC - xsltproc XSLT procesor.

Prilikom instalacije Lire-a iz ranije spomenutih binarnih paketa, u slučaju nepostojanja potrebnih komponenata, instalacijski program će navesti koje dodatne pakete je potrebno instalirati kako bi se zadovoljile ovisnosti.

Radi lakše deinstalacije i nadogradnje Lire paketa preporučuje se, nakon prevođenja, na sustavu ostaviti direktorij sa izvornim kodom i datotekama koje konfiguriraju proces prevođenja. Radi optimiranja korištenja diskovnog prostora, poželjno je izdati naredbu `make clean` koja će ukloniti suvišne datoteke nastale u procesu prevođenja. Program se sa sustava uklanja naredbom `make uninstall`.

Nadogradnja Lire paketa vrlo je jednostavna, a sastoji se od ponovne instalacije softvera i kopiranja starih konfiguracijskih datoteka. Konfiguracijski parametri, a samim time i konfiguracijske datoteke, su u načelu jednaki onima iz prethodnih inačica (ukoliko u dokumentaciji nije napomenuto drugačije).

3.1. Instalacija Lire-a u klijent-poslužitelj načinu rada

U okruženju sa velikim brojem poslužitelja, posebice ukoliko je u pitanju i velik broj različitih operacijskih sustava, instalacija, nadogradnja i korištenje Lire servisa mnogo su jednostavniji ukoliko se koristi klijent-poslužitelj ili tzv. *responder* način rada. Princip je jednostavan: Lire se instalira na jedno od računala kao centralni poslužitelj za analizu log datoteka, a ostali poslužitelji putem elektroničke pošte šalju svoje log datoteke na obradu centralnom poslužitelju. Budući da na klijentskoj strani nije potrebno instalirati nikakav specifičan softver, već samo podesiti lokalni program za slanje elektroničke pošte da ispravno šalje log datoteke udaljenom poslužitelju na obradu, moguće je obavljati analizu i za one poslužitelje koji su pokrenuti na platformama na kojima nije podržana instalacija Lire alata (npr. Microsoft IIS na Microsoft Windows operacijskom sustavu).

Osnovna procedura instalacije Lire-a, kao centralnog poslužitelja za obradu, identična je „*standalone*“ instalacijskom postupku, uz napomenu da je na sustavu potrebno imati MIME-Tools modul za Perl interpreter.

Po završenoj instalaciji i konfiguraciji prilikom pokretanja Lire-a podiže se `lr_spoold` poslužitelj, koji je zadužen za nadzor direktorija elektroničke pošte unutar kojih se smještaju zahtjevi za obradu.

Pod pojmom direktorija elektroničke pošte smatra se format *mailboxa* razvijen kao dio Qmail projekta, u kojem se pristigle poruke elektroničke pošte smještaju u direktorij kao zasebne datoteke. Za svaki od servisa čije se log datoteke žele analizirati potrebno je napraviti ovakav direktorij. Popis direktorija čiji se sadržaj nadgleda, kao i tip log datoteka koje se nalaze u pristiglim porukama, specificira se unutar `lire/address.cf` direktorija.

Za uspostavu osnovne infrastrukture potrebne za rad Lire-a kao poslužitelja za obradu log datoteka putem poruka elektroničke pošte koristi se `lr_setup_responder` skripta koja automatizira cjelokupan postupak.

Alternativno, moguće je i izdavanje sljedećih naredbi:

```
$ cd ~/lire
$ mkdir -p var/spool/lire/common
$ maildirmake var/spool/lire/common/Maildir
$ cd ~/lire/var/spool/lire
$ mkdir bind8_query postfix qmail sendmail
$ maildirmake bind8_query/Maildir
$ maildirmake postfix/Maildir
$ maildirmake qmail/Maildir
$ maildirmake sendmail/Maildir
```

Naredba `maildirmake` distribuira se unutar Qmail i Courier Mail Server paketa (http://www.courier-mta.org).

Nakon uspostave osnovne infrastrukture direktorija, potrebno je podesiti poslužitelj elektroničke pošte na sustavu tako da ispravno isporučuje poruke u zadane direktorije elektroničke pošte. Ukoliko se na sustavu koristi poslužitelj koji podržava opisani format direktorija elektroničke pošte (npr.

Qmail), podešavanje se svodi na izradu ispravnih *aliasa* pomoću kojih se poruke isporučuju u zadani direktorij. Prije podešavanja Lire-a kao *responder* poslužitelja, preporučuje se detaljno proučavanje dokumentacije poslužitelja elektroničke pošte instaliranog na sustavu.
Pojedini poslužitelji elektroničke pošte ne podržavaju oblik pohrane poruka putem direktorija elektroničke pošte. Kod takvih poslužitelja, najlakše je iskoristiti njihovu mogućnost integracije s procmail MDA (*Mail Delivery Agent*) agentom za isporuku elektroničke pošte. U datoteku `.procmailrc` unutar korijenskog direktorija Lire alata moguće je upisati sljedeći sadržaj:

```
:0:
* ^To:*combined-log@
<LR_SPOOLDIR>/combined/Maildir/new
:0:
* ^To:.*sendmail-log@
<LR_SPOOLDIR>/sendmail/Maildir/new
```

Ovakav oblik `.procmailrc` datoteke rezultirati će preusmjeravanjem pošte u zasebne datoteke u odgovarajućim direktorijima. Pri tome je potrebno pripaziti da (u ovom slučaju) adrese `combined-log` i `sendmail-log` budu podešene kao *aliasi* koji pokazuju na korisnika lire. Kao što se može primijetiti, svaki oblik log datoteke mora biti predstavljen odgovarajućom adresom elektroničke pošte i pripadajućim direktorijem.

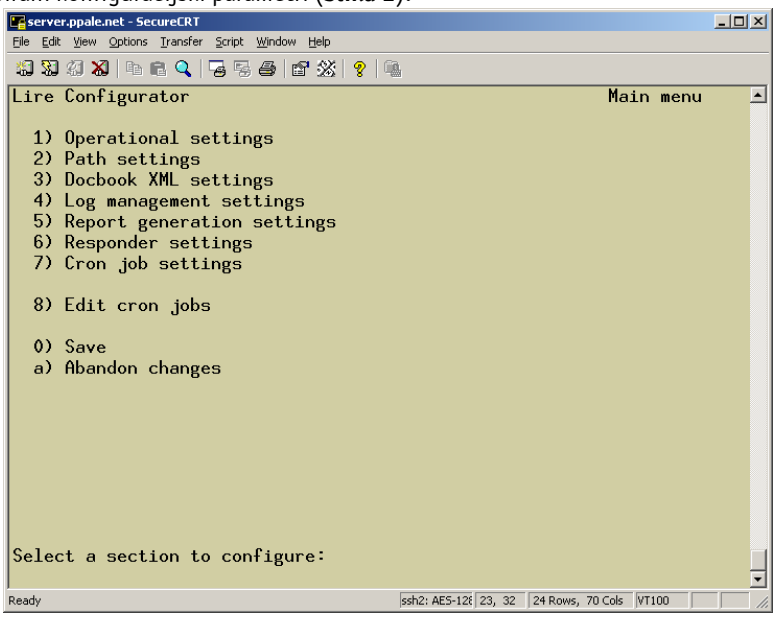
3.2. Podrška za „anonimiziranje“ log datoteka

Iako je klijent-poslužitelj način rada jednostavan i u mnogo slučajeva pogodan za korištenje, slanje log datoteka, koje sadrže određene povjerljive podatke o stanju sustava, na javni poslužitelj nije poželjno sa stanovišta sigurnosti. Iz tog razloga, Lire podržava „anonimiziranje“, tj. postupak uklanjanja svih povjerljivih podataka iz sadržaja log datoteka prije njihovog slanja javnom servisu za obradu. Vraćeni izvještaj u XML formatu se potom „deanonimizira“ tj. u njega se vraćaju potrebni podaci i transformira se u konačan format izvještaja.
Podrška za anonimiziranje log datoteka uključena je u standardnoj instalaciji Lire paketa, no potrebno je obratiti pozornost na postojanje BerkleyDB i DB_File Perl modula koji su neophodni za ovaj proces. Ovi moduli su uključeni u gotovo većinu standardnih instalacija Perl interpretara, što znači da (osim u slučaju nekih *proprietary* UNIX sustava) nema potrebe za instalacijom dodatnih paketa.

4. Pokretanje i upravljanje

4.1. Konfiguracija

Konfiguracijski parametri lire alata smješteni su u nekoliko datoteka, koje se nalaze na različitim lokacijama u datotečnom sustavu. Unutar direktorija `/usr/share/lire/defaults` nalazi se inicijalna konfiguracija Lire alata i eventualnih dodatnih komponenata koje su instalirane uz sam alat. Ove datoteke se ne preporučuje uređivati, budući da će svaka nadogradnja alata ili dodatnih komponenata uzrokovati ponovno prepisivanje ovih datoteka inicijalnim vrijednostima. Korisnička konfiguracija lire alata nalazi se unutar `/etc/lire/config/config.xml` datoteke i unutar ove datoteke je potrebno unijeti sve izmjene u konfiguraciji. Prilikom pokretanja Lire alata prvo se provjeravaju parametri u inicijalnim datotekama, koji se potom po potrebi prilagođavaju korisničkim postavkama iz `/etc/lire/config/config.xml` datoteke.
Budući da je konfiguracijska datoteka zapisana u XML formatu, koji je teško razumljiv većini korisnika, podešavanje parametara najlakše je izvesti pomoću `lr_config` aplikacije koja se isporučuje kao standardan dio Lire paketa. Nakon pokretanja aplikacije, korisniku se nudi nekoliko izbornika unutar kojih su grupirani konfiguracijski parametri (**Slika 2**).



Slika 2: Konfiguracijsko sučelje Lire alata

4.2. Generiranje izvještaja

Za generiranje izvještaja iz zadane log datoteke koristi se `lr_log2report` naredba, koja sa standardnog ulaza uzima log datoteku, a na standardni izlaz vraća gotov izvještaj u tekstualnom obliku. Kao dodatni parametar ovoj naredbi se zadaje format zapisa obrađivane log datoteke. Naredbom `lr_check_service -l` moguće je dobiti ispis podržanih formata, a njihovo detaljnije objašnjenje nalazi se unutar `lr_log2report` *manual* stranice.
Kao primjer može se uzeti sljedeća naredba, koja će obraditi log datoteku Apache web poslužitelja (*common log format*) i izvještaj spremiti u `report.txt` datoteku unutar korijenskog direktorija korisnika koji je pokrenuo Lire.

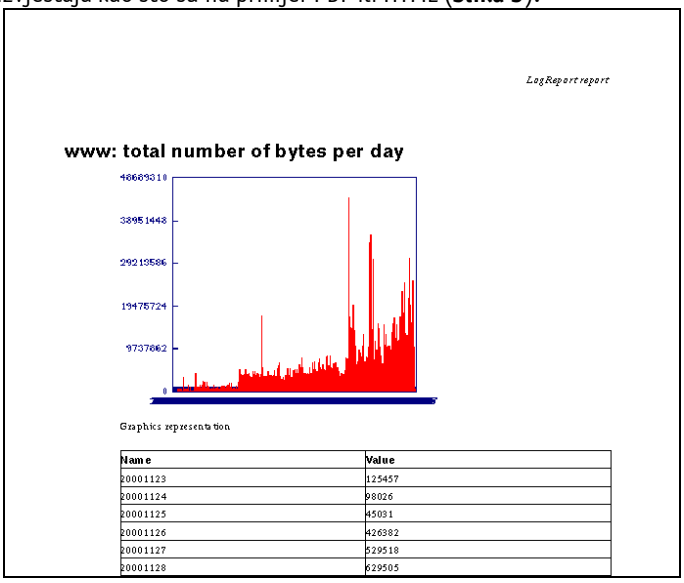
```
lr_log2report combined < /var/log/apache/access_log > ~/report.txt
```

Generirani izvještaj imati će sljedeći oblik:

```
Report generated: 2004-05-11 06:08:56 EDT
Reporting on period:
2004-02-05 15:09:07 EST - 2004-05-11 12:27:06 EDT
```

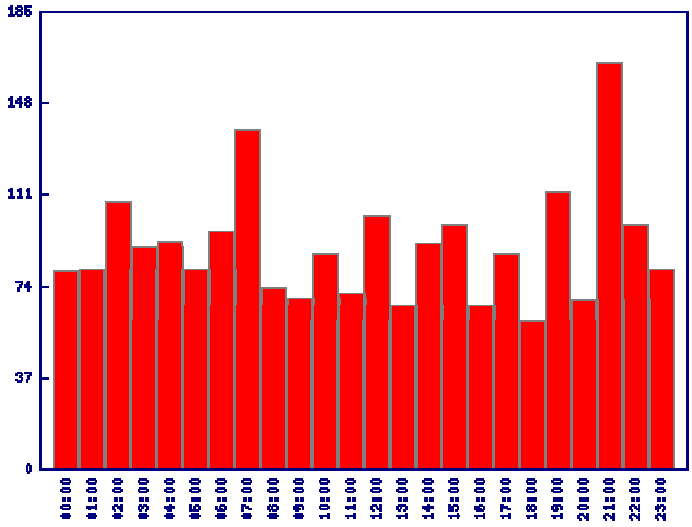
```
                        Activity Reports
                        ----------------

Number of Requests Served by 1d Period

Period                                              Requests % Total
--------------------------------------------------- -------- -------
2004-02-05                                                 8     0.0
2004-02-06                                               249     1.4
2004-02-07                                                34     0.2
2004-02-08                                                85     0.5
2004-02-09                                               216     1.3
2004-02-10                                                59     0.3
2004-02-11                                                57     0.3
2004-02-12                                                 8     0.0
2004-02-13                                               168     1.0
2004-02-14                                                34     0.2
2004-02-15                                                 4     0.0
2004-02-16                                               111     0.6
2004-02-17                                               480     2.8
2004-02-18                                               187     1.1
2004-02-19                                               120     0.7
2004-02-20                                               113     0.7
2004-02-21                                               225     1.3
2004-02-22                                                65     0.4
2004-02-23                                                45     0.3
2004-02-24                                                24     0.1
2004-02-25                                                64     0.4
```

Ukoliko su izvještaji iscrpni, tekstualni oblik nije najpogodniji za njihovo prikazivanje. Korištenjem opcije `-o` u kombinaciji sa `lr_log2report` naredbom, moguće je odabrati neki od alternativnih izlaznih formata izvještaja kao što su na primjer PDF ili HTML (**Slika 3**).



Slika 3: Izvještaj u PDF obliku

Kao što je vidljivo iz prethodne slike, u izvještaje je moguće ubacivati i grafičke prikaze rezultata analize. Lire podržava generiranje *pie chart*, *bar chart* (**Slika 4**), grafova i različitih histograma.



Slika 4: Grafički prikaz broja pristupa Web poslužitelju, u rezoluciji od jednog sata

Korištenje grafičkog prikaza čini izvještaje preglednijima i olakšava uočavanje anomalija u radu poslužitelja. Ova opcija uključuje se pomoću parametra `-i` prilikom pokretanja `lr_log2report` naredbe. Grafički prikaz je trenutno moguće dodati isključivo u HTML, PDF, XHTML i DocBook XML tipove izvještaja.

4.3. Korištenje klijent-poslužitelj modela

Najlakši način generiranja izvještaja je, kao što je već spomenuto, putem klijent-poslužitelj načina rada. Log datoteka se šalje unutar poruke elektroničke pošte na posebnu adresu na poslužitelju, specifičnu za taj oblik datoteke. Generirani izvještaj šalje se natrag na adresu navedenu u `Repy-To` polju pristigle poruke. Ukoliko poruka ne sadrži `Reply-To` polje, iskoristiti će se adresa iz `From` polja poruke. Vidljivo je da je za generiranje izvještaja u *responder* načinu rada potreban Lire poslužitelj i standardni *e-mail* program na strani klijenta.

Kako bi slanje poruka bilo što efikasnije, *responder* prihvaća gzip ili zip formate datoteka, a datoteka se može nalaziti u tijelu poruke ili u privitku. Iako se za slanje poruka može iskoristiti bilo koji standardni klijent elektroničke pošte, ipak je potrebno pripaziti na neke detalje u njegovom radu. Potrebno je obratiti pozornost na sljedeće:

- Korišteni program nikako ne smije ubacivati nove retke, nastale kako rezultat formatiranja predugih redaka u log datotekama. Zbog ovoga je najbolje log datoteku slati u privitku poruke.
- Potrebno je provjeriti da klijent postavlja standardno MIME zaglavlje poruke.
- Ukoliko se log datoteka šalje kao privitak, poruka ne smije sadržavati dodatne privitke.

Ispravan rad klijenta vrlo lako se može provjeriti slanjem poruka na javni *online responder* servis održavan od strane LogReport organizacije. Popis adresa elektroničke pošte za pojedine formate log datoteka može se pronaći na adresi http://logreport.org/lire/or.

Za primjer se može iskoristiti slanje log datoteke bind8 poslužitelja pomoću standardne „`mail`“ naredbe na Unix sustavima.

```
$ mail -s "Bind8 Log" log@bind8-query.logreport.org < \
/var/log/query.log
```

U slučaju slanja većih log datoteka, poželjno je koristiti neki od formata za kompresiju datoteka, kao npr. gzip.

```
$ mutt -s "`hostname` `date`" -a \
/var/log/apache/common.log.1.gz log@common.logreport.org < \
/dev/null
```

Kao što je već prije spomenuto, log datoteke je prije slanja moguće anonimizirati. U tom slučaju potrebno je koristiti naredbu `lr_anonymize` koja će ukloniti sve osjetljive podatke iz zadane log datoteke. Mapiranje stvarnih vrijednosti u odnosu na zamijenjene sprema se na tvrdi disk, tako da je

prilikom primanja izvještaja moguće proces provesti u suprotnom smjeru. Polje `Subject` poruke elektroničke pošte koja sadrži anonimiziranu log datoteku mora započinjati znakovnim nizom '`anon`'.
Primjer:
Za slanje anonimizirane log datoteke Postfix poslužitelja na javni *responder* Logreport organizacije, može se iskoristiti sljedeća naredba:

```
$ grep ' postfix/' /var/log/mail.log | \
lr_run lr_anonymize /tmp/anon | \
mail -s "anon Daily Report" log@postfix.logreport.org
```

Pri tome `/tmp/anon` datoteka predstavlja bazu sa mapom stvarnih i anonimiziranih vrijednosti. Budući da će pri sljedećem izdavanju ovakve naredbe `lr_anonymize` skripta obrisati ovu bazu, potrebno je pripaziti da se ne pokrene više paralelnih zahtijeva za anonimiziranjem, jer u tom slučaju postoji rizik od gubljenja podataka.

5. Automatizacija zadataka

Jednom kada je Lire podešen i ispravno funkcionira, poželjno je podesiti periodičko, automatsko generiranje izvještaja. Automatizacija zadataka ovakvoga tipa na Unix i Linux sustavima najlakše se izvodi korištenjem cron poslužitelja. U sklopu Lire paketa postoji skripta pod nazivom `lr_cron`, čija namjena je izvršavanje unaprijed definiranih setova naredbi nad zadanim log datotekama. Generirani izvještaji mogu biti u ASCII ili bilo kojem drugom formatu podržanom od Lire alata, uz uvjet da su sve potrebne datoteke za takvu akciju prisutne na sustavu. Po izvođenju `lr_cron` skripte, generirani izvještaji se administratoru šalju putem elektroničke pošte ili se spremaju na proizvoljnu lokaciju na tvrdom disku. Za korištenje `lr_cron` skripte neophodno je potrebno imati ispravno konfigurirane DLF (*Distilled Log Format*) spremnike detaljnije opisane u „*Lire Developer's Manual*" dokumentu.
Podešavanje se sastoji od dva dijela:

- Konfiguriranje poslova vezanih uz spremnik;
- Konfiguriranje cron poslužitelja tako da pokreće `lr_cron` skriptu u određeno vrijeme i nad određenim spremnicima

Prvi korak postiže se pomoću Lire naredbe. DLF spremnik otvara se korištenjem *Store->Open* ili *Store New* izbornika u kojima se nalaze opcije *Import jobs* i *Report jobs*. Opcije je potrebno konfigurirati tako da se podesi frekvencija izvođenja i tip svakog od poslova.
Opcija *Import jobs* zadužena je za dohvaćanje log datoteka i njihovo spremanje unutar DLF spremnika, dok opcija *Report jobs* definira procese koji analiziraju prikupljene podatke i u konačnici daju gotov izvještaj. Svako pokretanje `lr_cron` skripte povlači za sobom pokretanje *Import jobs* i *Report jobs* sekvence.
Kako bi se skripta izvršavala periodički, potrebno je ispravno podesiti cron poslužitelj. Taj postupak je relativno lagan budući da su jedini parametri koje je potrebno zadati skripti period pokretanja i odgovarajući spremnik.
Primjer:

```
0 0 * * * /usr/bin/lr_cron daily /var/lib/lire/www_store
0 0 * * 0 /usr/bin/lr_cron weekly /var/lib/lire/email_store
```

Gornji primjer pokrenuti će generiranje izvještaja za Web poslužitelj na dnevnoj osnovi i izvještaja za poslužitelj elektroničke pošte na tjednoj osnovi.

6. Uređivanje izvještaja

Generirani izvještaji za svaki od pojedinih mrežnih servisa sastavljeni su od nekoliko podizvještaja koji su spojeni u jednu cjelinu. Ovisno o tipu mrežnog servisa i informacija dostupnih u log datotekama, Lire nudi određen broj različitih podizvještaja koji se mogu uključiti u konačan izvještaj. Ukoliko korisnik nije zadovoljan sa inicijalno podešenim izvještajima, u mogućnosti je po volji dodavati ili uklanjati pojedine podizvještaje.

Konfiguracijski podaci za izvještaje čuvaju se u posebnim datotekama unutar `/etc/lire` direktorija i imaju naziv oblika `ime_servisa.cfg` (npr. `www.cfg` ili `ftp.cfg`). Ne preporučuje se izravna izmjena ovih datoteka, već je najbolje u `/etc/lire` direktorij kopirati .cfg datoteke koje se isporučuju u paketu s izvornim kodom programa i nad njima provoditi izmjene, a inicijalne .cfg datoteke sačuvati za slučaj da je nova konfiguracija neispravna ili izaziva probleme u radu alata.

Konfiguracijske datoteke podijeljene su u više odjeljaka koji počinju sa direktivom `=section` i naslovom odjeljka. U recima iza ove direktive, slijede filtri i podizvještaji specifični za taj odjeljak. Prazni reci u konfiguracijskoj datoteci, kao i oni koji počinju sa znakom # ignoriraju se. Korištenje filtara koji selektivno propuštaju log podatke koji će se koristiti u konačnom izvještaju je opcionalno, ali ukoliko se koriste obavezno moraju biti navedeni prije podizvještaja pojedinog odjeljka. Redak u kojem se nalazi filtar mora počinjati sa znakom '|' (eng. *pipe*).

Za primjer je moguće uzeti tipičnu konfiguracijsku datoteku DNS servisa:

```
=section All Requests
top-requesting-hosts       hosts_to_show=10
top-requested-names names_to_show=10
requesttype-distribution
requests-by-period         period=1d

=section Recursive Requests
|select-resolver    method="recurs"
top-requesting-hosts       hosts_to_show=10
top-requested-names names_to_show=10
requesttype-distribution
requests-by-period         period=1d

=section Non Recursive Requests
|select-resolver    method="nonrec"
top-requesting-hosts       hosts_to_show=10
top-requested-names names_to_show=10
requesttype-distribution
requests-by-period         period=1d
```

Prikazana konfiguracija sadrži tri odjeljka. Unutar prvog odjeljka ne koriste se filtri, pa će traženi podizvještaji biti generirani korištenjem svih zahtijeva upućenih DNS poslužitelju. Odjeljak `Recursive Requests` sadrži filtar koji specificira korištenje isključivo rekurzivnih upita prilikom generiranja podizvještaja, dok treći odjeljak podizvještaje generira isključivo na osnovu nerekurzivnih upita. Na ovaj način moguće je izdvojiti željene informacije u više odjeljaka i učiniti konačni izvještaj preglednijim.

Budući da se izvještaj generira redoslijedom kojim su odjeljci navedeni u konfiguracijskoj datoteci, konačan oblik izvještaja moguće je promijeniti promjenom redoslijeda odjeljaka. Također je moguće mijenjati i parametre pojedinih podizvještaja tako da odgovaraju potrebama korisnika. Pri tome je potrebno pripaziti da varijable koje definiraju parametre podizvještaja budu smještene u isti redak kao i sam podizvještaj.

Izbor filtara i podizvještaja za svaki od podržanih servisa detaljno je opisan u korisničkoj dokumentaciji Lire alata.

7. Zaključak

Lire je fleksibilan alat, s vrlo jednostavnim instalacijskim postupkom. Brojne mogućnosti, poput velikog broja podržanih formata log datoteka i rada u klijent-poslužitelj modelu, čine ga pogodnim za implementaciju u računalnim mrežama sa velikim brojem poslužitelja i servisa.

Modularan koncept i korištenje XML formata prilikom generiranja izvještaja programerima olakšava i znatno ubrzava razvoj podrške za nove formate log datoteka. Kao nedostatak može se navesti nemogućnost izvještavanja o sadržaju log datoteka u stvarnom vremenu. No, to konceptualno i nije svrha ovakvog alata, već se u tu svrhu preporučuje upotreba specijaliziranih programa kao što su swatch (http://swatch.sourceforge.net/) ili LoFiMo (http://lofimo.anzac.at/).