Technická univerzita v Košiciach
Fakulta elektrotechniky a informatiky

Hĺbková analýza paketov prostredníctvom protokolu IPFIX

Príloha A

Používateľská príručka

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra počítačov a informatiky (KPI)
Školiteľ:	Ing. Adrián Pekár, PhD.
Konzultant:	Ing. Ján Juhár

Košice 2015 **Bc. Dávid Farkas**

Obsah

1 Funkcia programu

Program MyBeem reprezentuje najnižšiu vrstvu architektúry BasicMeter. Predstavuje monitorovací a exportovací proces. Tieto procesy slúžia na monitorovanie sieťovej prevádzky a jej parametrov s následným exportovaním nameraných hodnôt do vyššej vrstvy. Program exportuje tieto hodnoty vo formáte konfrontujúcim so štandardami IPFIX a PSAMP. Je to konzolová aplikácia a nemá žiadne grafické rozhranie. Rôzne výpisy programu je možné sledovať priamo v konzole. Program Syncserv reprezentuje synchronizačný server nástroja BasicMeter. Je určený pre synchronizáciu hodín nástroja MyBeem. Takisto ako nástroj MyBeem je tento program konzolová aplikácia a jeho výpisy je možné sledovať v konzole. Programy boli vyvíjané použitím open-source technológií.

2 Súpis obsahu dodávky

Program je dodávaný na CD médiu, ktoré obsahuje nasledujúce adresáre:

- adresár **/doc/**
  - Používateľská príručka programov MyBeen a Syncserv vo formáte pdf;
  - Systémová príručka programov MyBeem a Syncserv vo formáte pdf;
- adresár **/src/**
  - zdrojové kódy programu MyBeem;
- adresár **/bin/**
  - skompilovaná forma programu MyBeem;
- adresár **/lib/**
  - knižnice pre správne fungovanie programov;

- adresár **/deb/**
  - .deb balíček obsahujúci programy MyBeem a Syncserv;
- súbor **/readme.txt**- textový súbor popisujúciu obsah CD;

3 Inštalácia programov

Programy MyBeem a Syncserv sú určené pre operačné systémy s linuxovým jadrom. Inštalácia programov spočíva v nainštalovaní z inštalačného deb balíka.

3.1 Požiadavky na technické vybavenie

Požiadavky na technické vybavenie závisia od množstva odchytávanej premávky a tým pádom od rýchlosti pripojenia meracieho bodu k počítačovej sieti. Preto je ťažké povedať, aká má byť optimálna konfigurácia.

3.1.1 Minimálna konfigurácia

- procesor Pentium 100MHz
- 128MB operačnej pamäte
- 10MB voľného miesta na pevnom disku
- sieťová karta

3.1.2 Optimálna konfigurácia (pre 100Mbit linku)

- 2 jádrový procesor 2GHz a viac
- 512MB operačnej pamäte a viac

- 10MB voľného miesta na pevnom disku
- sieťová karta

3.2 Požiadavky na programové vybavenie

Pre úspešné skompilovanie zdrojových súborov a správne fungovanie programu sú potrebné:

- operačný systém s linuxovým jadrom verzie 2.4 a vyššej
- kompilátor zdrojových súborov jazyka C - gcc prípadne g++ verzie 3.3 alebo vyššej
- knižnica libpcap-dev verzie 0.8.3 alebo vyššej
- knižnica libxml2-dev verzie 2.6.23 alebo vyššej
- knižnica openssl verzie 0.9.1 alebo vyššej
- knižnica libsctp-dev verzie 1.0.9 alebo vyššej
- knižnica libxml2-utils verzie 2.7.8 alebo vyššej
- knižnica libnDPI verzie 1.5.2 (iné verzie nie sú podporované)

3.3 Vlastná inštalácia

Táto podkapitola predstaví možnosti inštalácie programu MyBeem: inštalácia z deb balíka, inštalácia prekladom zdrojových kódov.

3.3.1 Inštalácia z deb balíka

Jedným zo spôsobov inštalácie programu MyBeem je priama inštalácia deb balíčka do systému. Avšak ešte skôr, ako začneme týmto spôsobom program inštalovať

je nutné mať v operačnom systéme nainštalované knižnice libcap-dev,libxml2-dev, libssl-dev, libsctp-dev a libssl0.9.8 . Tieto knižnice je možné získať z repozitárov operačného systému príkazom:

```
sudo apt-get install libpcap-dev libxml2-dev libssl-dev libsctp-dev
  libssl0.9.8
```

Okrem predošlých balíkov je potrebné mať nainštalovať aj balík nDPI z oficiálneho SVN repozitára spoločnosti ntop. Postup inštalácie balíka nDPI:

```
svn co https://svn.ntop.org/svn/ntop/trunk/nDPI/
sudo su
apt-get install gawk gcc autoconf build-essential libtool
cd nDPI
sh autogen.sh
make
make install
export LD_LIBRARY_PATH="/usr/local/lib:$LD_LIBRARY_PATH"
```

Po zadaní predošlého príkazu môžeme prejsť k samotnému získaniu deb balíčka v aktuálnej verzií. Pre získanie aktuálnej verzie programu je nutné modifikovať príkaz, to znamená číselný identifikátor verzie `mybeem_1.1-6`. Následne pre samotné stiahnutie deb balíka je potrebné do príkazového riadku uviesť:

```
wget https://svn.cnl.tuke.sk/monica/BasicMeter/Exporter/MyBeem/deb/
   mybeem_1.1-6_i386.deb --no-check-certificate
```

Samotné prevedenie inštalácie sa vykoná príkazom:

```
sudo dpkg -i mybeem_1.1-6_i386.deb
```

Atribút dpkg s parametrom `-i` nad súborom mybeem_1.1-6_i386.deb vykoná priamu inštaláciu deb balíčka do systému z tohto `.deb` súboru.

Výsledkom sú spustiteľné súbory `mybeem` a `syncserv`, ktoré sa nachádzajú v adresári /usr/sbin. Inštalácia pridá aj konfiguračný súbor, ktorý sa nachádza v adresári /etc/mybeem. Rovnako pridá aj init.d skript ktorý zabezpečuje spúštanie a zastavovanie programu MyBeem.

3.3.2 Inštalácia prekladom zdrojových textov

Tento spôsob je pre bežného používateľa tohto nástroja zrejme najmenej pohodlný, avšak ak má používateľ aj isté programátorské skúsenosti, jednoducho môže modifikovať zdrojové súbory programu. Pre preklad resp. kompiláciu programu je nutné, aby sa v knižničnej databáze operačného systému nachádzali nasledujúce knižnice:

- libpcap-dev verzie 0.8.3 alebo vyššej
- libxml2-dev verzie 2.6.23 alebo vyššej
- libxml2-utils verzie 2.7.8 alebo vyššej
- openssl verzie 0.9.1 alebo vyššej
- libndpi verzie 1.5.2 (iné verzie zatiaľ nie sú podporované)

Ich inštalácia je jednoduchá a vyžaduje si zadanie nasledujúcu postupnosť príkazov do povelového riadku operačného systému:

```
sudo su
apt-get install libpcap-dev libxml2-dev libssl-dev libxml2-utils
  gawk gcc autoconf build-essential libtool
svn co https://svn.ntop.org/svn/ntop/trunk/nDPI/
cd nDPI
sh autogen.sh
make
make install
export LD_LIBRARY_PATH="/usr/local/lib:$LD_LIBRARY_PATH"
```

Po úspešnej inštalácii knižníc nasleduje stiahnutie zdrojových kódov z svn repozitára. Stačí, ak do povelového riadku zadáme príkaz:

```
svn export https://svn.cnl.tuke.sk/monica/BasicMeter/Exporter/
MyBeem/src/mybeem/
```

Atribútom export sa zabezpečí vyexportovanie zdrojových textov zo zadaného svn repozitára. Ak svn resp. subversion nie je nainštalované v operačnom systéme, čo zistíme, ak vykonanie predošlého príkazu skončí chybou, je potrebné zadať nasledujúci príkaz pre jeho inštaláciu:

```
sudo apt-get install subversion
```

Po úspešnom stiahnutí zdrojových textov sa presunieme do adresára s týmito zdrojovými kódmi a to príkazom:

```
cd mybeem
```

Následne už len stačí zadať do povelového riadku príkaz pre kompiláciu zdrojových textov:

```
make
```

4 Použitie programu MyBeem

Pred spustením programu je potrebné ho najprv nakonfigurovať. Konfiguračný súbor je vo formáte xml.

Spustiť program môžeme dvoma spôsobmi:

1. **spustením samotného programu** - pri spúšťaní je možné zadať názov konfiguračného xml súboru ako parameter, alebo sa bude brať do úvahy prednastavený konfiguračný súbor `/etc/mybeem/config.xml`. Pre spustenie programu sú potrebné práva administrátora. Spustenie sa prevedie nasledujúcim

príkazom:

```
mybeem -c config.xml
```

Ak chceme MyBeem spustiť prekladom zdrojových súborov, je nutné zadať cestu k binárnemu súboru, ktorý vznikol prekladom zdrojových textov. Teda ak sa nachádzame v priečinku so zdrojovými textami a používame konfiguračný súbor, ktorý sa nachádza v adresári `/etc/mybeem/`, tak stačí pre spustenie exportéra príkaz:

```
sudo ./beem
```

Pre manuálne zadanie konfiguračného súboru a následné spustenie exportéra je potrebné zadať príkaz:

```
sudo ./beem -c config.xml
```

2. **spustením init.d skriptu** - skript prechádza adresár /etc/mybeem a ku každému xml súboru spúšťa inštanciu programu MyBeem. Spustenie programu sa prevedie zadaním nasledujúceho príkazu:

```
service mybeemd start
```

Kedže program je konzolová aplikácia, neposkytuje žiadne grafické rozhranie pre používateľa. Chybové a informačné hlásenia sú zobrazované v rovnakej konzole, v akej bol tento program spustený, alebo sú uložené v log súbore, ktorý sa nachádza v adresári `/var/log/mybeem` v prípade spustenia pomocou skriptu na pozadí. Ukončenie programu sa vykoná stlačením kombinácie kláves CTRL + C v prípade, že program nebol spustený cez skript. Ak bol program spustený cez skript jeho ukončenie sa realizuje pomocou príkazu

```
service mybeemd stop
```

Pomocou príkazu

```
service mybeemd status
```

vieme zistiť, či je exportér spustený alebo nie a zadaním príkazu

```
service mybeemd restart
```

dokážeme reštartovať všetky bežiace inštancie programu MyBeem.

5 Použitie programu Syncserv

Program je možné spustiť zadaním príkazu

```
syncserv <CISLO_PORTU>
```

Pri spustení je potrebné špecifikovať číslo portu, ktoré bude program používať pre komunikáciu so synchronizačným klientom. Ukončenie programu sa vykoná stlačením kombinácie kláves CTRL + C. Program po každom obdržaní synchronizačnej správy vypíše hlásenie obsahujúce hodnotu času, ktorý odosiela synchronizačnému klientovi.

6 Použitie zasielania výpisov na syslog server

Predtým ako je MyBeem spustený s parametrom príkazového riadku `-logserv` je nutné, aby bola v systéme nainštalovaná syslog-ng aplikácia. Tento proces sa vykoná zadaním príkazu:

```
sudo apt-get install syslog-ng
```

Po úspešnom nainštalovaní aplikácie vznikne v adresári `/etc/syslog-ng/` konfiguračný súbor `syslog-ng.conf`. MyBeem si však pri inicializácii, ak je zapnutá možnosť zasielania výpisov na syslog server, vytvára vlastný konfiguračný súbor pre tento program a následne ho s ním spúšťa. Dôležitá je však konfigurácia syslogd daemona na strane servera, kde je potrebné vykonať zmeny v konfiguračnom súbore `syslog-ng.conf`. Príklad konfiguračného súboru:

```
options {
   chain_hostnames(0);
   time_reopen(10);
   time_reap(360);
   log_fifo_size(2048);
   create_dirs(yes);
   group(adm);
   perm(0640);
   dir_perm(0755);
   use_dns(no);
   stats_freq(0);
   bad_hostname("^gconfd$");
   };

   source s_net {tcp(ip(147.232.241.139) port(4739));};
   destination df_beem {file("/var/log/mybeem/$HOST/
   $YEAR-$MONTH-$DAY-$HOUR.00.log" template("$MSG\n"));};

log{
   source(s_net);
   destination(df_beem);
   };
```

Najpodtatnejšou časťou je konfigurácia zdroja a cieľa. V tomto prípade je ako zdroj IP adresa rozhrania, na ktoré sú zasielané správy syslog-ng klientom a cieľom je súbor v zložke, ktorej názov je IP adresa klienta (parameter `$HOST` v ceste cieľa). Bližšie informácie o možnostiach konfigurácie syslogd daemona je možné nájsť na príslušných manuáových stránkach.

7 Generovanie programu šitého na mieru

Táto funkcionalita sa dá použiť len v prípade ak program MyBeem používame prostredníctvom prekladu zdrojových kódov. Poskytuje pre používateľa možnosť vygenerovania takej verzie programu MyBeem, z ktorej určitá sada informačných elementov a/alebo doplňujúcich služieb je vynechaná pre účel zníženia požiadaviek na systémové prostriedky. Teda používateľ ho môže "zašiť na mieru".

Požiadavky použitia tejto funkcionality sú:

- balík libxml2-utils verzie 2.7.8 alebo vyššej,
- úplna sada zdrojových modulov programu MyBeem a súbory config.xml, Makefile a beem_adjuster.sh.

Inštalácia balíka libxml2-utils sa dá vykonať jednoducho zadaním nasledujúceho príkazu do príkazového riadku operačného systému:

```
sudo apt-get install libxml2-utils
```

O spôsobe obstarávaní zdrojových kódov a dodatočných súborov (beem_adjuster.sh, Makefile, config.xml) z SVN repozitára sa táto používateľská príručka zaoberá v sekcii 3.3.2 .

Po nainštalovaní potrebného balíka a stiahnutí potrebných súborov používateľ už má všetko k dispozícii k tomu, aby vygeneroval svoju vlastnú verziu programu MyBeem. Prvým krokom je nastavenie vlastností novej verzie, kto sa dosiahne modifikáciou

konfiguračného súboru (config.xml).

V sekcii /configuration/templates/template id=”257” sa nachádza zoznam podporovaných informačných elementov. Vymazaním alebo vykomentovaním ľubovoľného riadku tohto zoznamu používateľ ”vypne”daný informačný element pre novú verziu programu.

Doplňujúce služby sa nachádzajú v sekcii /configuration/mediator (sekcia mediačného servera), /configuration/synchronization (sekcia synchronizačného servera) a /configuration/logging (sekcia logovacieho servera). Používateľ môže vypnúť ľubovoľný počet z týchto služieb pomocou prvej položky danej sekcie, ktorej hodnotu prepíše na hodnotu false.

Druhým a posledným krokom generovania upravenej verzie programu MyBeem je schválenie vykonaných zmien pomocou skriptu beem_adjuster.sh. Po uložení vykonaných zmien v konfiguračnom súbore, spomínaný skript sa dá spustiť nasledujúcim príkazom príkazového riadku:

```
./beem_adjuster.sh
```

Generovanie chvíľku potrvá, skript počas svojej práce hláškami informuje používateľa o stave a úspešnosti generovania. V prípade neúspechu treba pokračovať v riešení inštrukcií chybovej hlášky. Popis jednotlivých chybových hlášok sa nachádza v sekcii 11.1 . Po úspešnom skončení skriptu používateľ ďalej môže postupovať podľa bodov kapitoly 4 .

8 Použitie hĺbkovej analýzy paketov

Program MyBeem vo verzii 1.9 bol rozšírení o funkcionalitu hĺbkovej analýzy paketov, čo spočíva v tom, že vo fáze merania sa analyzuje aj dátová časť paketov za účelom získania aplikačného protokolu. Hĺbková analýza sa vykoná pomocou API rozhrania knižnice nDPI. Teda požiadavkou použitia tejto funkcionality je to, aby

bola nainštalovaná knižnica libndpi verzie 1.5.2. Postup tejto inštalácie sa nachádza v podkapitole 3.3.1.

Keďže služba hĺbkovej analýzy paketov má vysoké náklady ohľadom systémových prostriedkov, preto je možné túto službu vypnúť prostredníctvom konfiguračného súboru config.xml. Konfigurácie hĺbkovej analýzy paketov sú nasledovné:

```
<dpi>
  <doDpi>true</doDpi>
  <protofile>NULL</protofile>
</dpi>
```

Popis jednotlivých konfigurácií:

- **doDPI** – vypínanie/zapínanie služby hĺbkovej analýzy paketov. Hodnota true znamená, že sa služba má použiť, hodnota false službu vypne.
- **protofile** – cesta k súboru aplikačných protokolov. Hodnota NULL znamená, že sa súbor aplikačných protokolov nemá použiť. Účel a štruktúra tohoto súboru je popísaná v podkapitole 10.2.

Základná sada podporovaných aplikačných protokolov pozostáva zo 188 protokolov, ktoré sú vymenované na oficiálnej stránke knižnice nDPI[1].

9 Konfigurácia exportéra nainštalovaného na meracom bode

V tomto kapitole budú predstavené možnosti nakonfigurovania programu MyBeem pred jeho spustením: konfigurácia priamym pozmenením konfiguračného súboru, konfigurácia pomocou parametrov príkazového riadku.

[1] http://www.ntop.org/products/ndpi/

9.1 Konfigurácia exportéra priamym pozmenením konfiguračného súboru config.xml

Po úspešnom nainštalovaní exportéra na merací bod, môžme zahájiť jeho konfiguráciu. Konfigurácia zmenou konfiguračného súboru je narozdiel od konfigurácie prostredníctvom parametrov príkazového riadku trvalá, teda pri každom ďalšom zapnutí exportéra budú aplikované uložené nastavenia, ak nebudú prostredníctvom príkazového riadku zadané iné.

Pre pozmenenie konfiguračného súboru je potrebné ho otvoriť v niektorom z editorov, ktoré ponúka operačný systém. Ako príklad uvediem pozmenenie súboru v editore vim. Otvorenie súboru v tomto editore je možné príkazom:

```
vim /etc/mybeem/config.xml
```

Ak toto otvorenie skončí chybovým hlásením, je možné, že v systéme tento editor ešte nainštalovaný nie je. Preto je pre jeho inštaláciu potrebné zadať:

```
sudo apt-get install vim
```

Následne po otvorení súboru v editore vim je pre editáciu obsahu nutné stlačiť kláves `i`. Kurzorom sa presunieme do sekcie `/configuration/collector` kde môžme vykonať príslušné nastavenia pre pripojenie sa na kolektor. Základom je nastavenie položiek z obrázka 9 – 1.

```
<configuration>
   <collector>
        <host> </host>              <!-- IP adresa kolektora, teda zhromažďovača, kde
                                         sa budú údaje získané zo siete zasielať -->
        <port> </port>              <!-- číslo portu, na ktorom bude exportér
                                         komunikovať s kolektorom -->
        <protocol> </protocol>      <!-- protokol, akým sa bude pripájať exportér na
                                         kolektor (MyBeem podporuje protokoly TCP,UDP a SCTP) -->
   </collector>
</configuration>
```

Obr. 9 – 1 Kľúčové položky konfiguračného súboru pre nastavenie exportéra

Aby sa vykonané zmeny konfiguračného súboru prejavili v praxi, je nutné ich uložiť.

Pre uloženie je nutné sa prepnúť v editore s editovacieho do riadiaceho režimu. Tento stav dosiahneme stlačením klávesu `Esc`. Následne sa v ľavom dolnom rohu okna objaví možnosť zadať príkaz. Preto pre uloženie vykonaných zmien a návrat do adresára s konfiguračným súborom zadáme nasledujúci príkaz `:wq`.

9.2 Konfigurácia zadaním parametrov príkazového riadku pri spúšťaní exportéra

Konfigurácia zadaná do parametrov príkazového riadku ma vyššiu prioritu, teda je uprednostnená, pred konfiguráciou z konfiguračného súboru. Tento spôsob nastavení nie je trvalý, teda je nutné uviesť príslušné hodnoty pri každom spustení exportéra. Pričom platí, že zvyšné hodnoty, ktoré do parametrov neuvedieme sú čítané z príslušného konfiguračného súboru.

Tabuľka 9 – 1: Paleta implementovaných parametrov príkazového riadku

-v	zobrazí aktuálnu verziu programu
-h	zobrazí informácie
-p [PROTO TYPE]	nastaví typ protokolu na hodnotu špecifikovanú v [PROTO TYPE]
-i [INTERFACE]	nastaví rozhranie na typ špecfikovaný v [INTERFACE]
-c [CONFIG FILE]	nastaví kofiguračný súbor na súbor špecfikovaný v [CONFIG FILE]
-l [LOG FILE]	nastaví logovací súbor na súbor špecfikovaný v [LOG FILE]
-pc [PCAP FILTER]	nastaví PCAP filter na filter špecifikovaný v [PCAP FILTER]

-po [PORT NUMBER]	nastaví číslo portu na číslo špecifikované v [PORT NUMBER]
-ho [HOST IP]	nastaví host IP adresu na adresu špecifikovanú v [HOST IP]
-llvl [LOG LEVEL]	nastaví úroveň výpisov na hodnotu špecifikovanú v [LOG LEVEL]
-opid [OBS POINT ID]	nastaví observationPointId na hodnotu špecifikovanú v [OBSERVATION POINT ID]
-odid [OBS DOM ID]	nastaví observationDomainId na hodnotu špecifikovanú v [OBSERVATION DOMAIN ID]
-logserv	zapne logovanie na syslog server pri použití konfigurácie z konfiguračného súboru config.xml
-logprot [PROTO TYPE]	nastaví protokol pre prenos syslog správi na hodnotu špecifikovanú v [PROTO TYPE]
-logaddr [IP ADDRESS]	nastaví IP adresu syslog servra na hodnotu špecifikovanú v [IP ADDRESS]
-logport [PORT NUMBER]	nastaví port pre komunikáciu so syslog servrom na hodnotu špecifikovanú v [PORT NUMBER]
-aggreg	zapne proces agregácie v programe MyBeem

Príklad použitia nastavení:

```
sudo mybeem -ho 192.168.24.3 -p TCP -po 2345 -opid 23 -odid 3
```

Uvedené parametre nastavia IP adresu, na ktorej sa pripojí exportér ku kolektoru, na 192.168.24.3, protokol, ktorým sa bude exportér pripájať na kolektor na TCP, port na hodnotu 2345, identifikátor meracieho bodu observationPointID na hodnotu 23 a identifikátor pozorovacej domény observationDomainID na hodnotu 3.

10 Popis vstupných a výstupných súborov programu MyBeem

Vstupom programu je samotná sieťová prevádzka a výstup tvoria exportované dáta. Zároveň programe poskytuje možnosť presmerovať svoje výpisy do logovacieho súboru v adresári /var/log/mybeem.

10.1 Konfiguračný súbor

V tejto podkapitole sú predstavené položky konfiguračného súboru programu MyBeem členené do nasledujúcich skupín: konfigurovateľné parametre, vzorkovacie metódy, informačné elementy.

10.1.1 Konfigurovateľné parametre

Program je konfigurovateľný pomocou konfiguračného súboru `config.xml`. Konfigurovateľné parametre znázorňuje nasledujúca tabuľka 10 – 1.

Tabuľka 10 – 1: Zoznam značiek konfiguračného súboru config.xml

configuration	koreňová značka, ktorá ohraničuje všetky konfiguračné parametre konfiguračného súbor

observationPointId	jedinečný identifikátor pozorovacieho bodu (celočíselná kladná hodnota 1-32767)
observationDomainId	jedinečný identifikátor pozorovacej domény
sync_port	port, použitý pri synchronizácii nástrojom MyBeem
readfile	ak true, príznak čítania zo súboru. Ak false, "číta"sa zo zvoleného sieťového rozhrania
dumpFile	názov súboru z ktorého sa v prípade nastavenia readFile na true bude čítať
interface	sieťové rozhranie, z ktorého sa majú odchytávať pakety
pcapFilter	typ BPF filtra pre filtrovanie paketov
flows	značka ohraničujúca parametre ovplyvňujúce nastavenie tokov
biflows	prepínač na zapnutie/vypnutie podpory obojsmerných tokov exportérom, false-uniflow true-biflow
passiveTimeout	nastavenie času v milisekundách pre pasívny timeout. Pasívny timeout je čas, za ktorý keď pre príslušný tok nie je obdržaný žiaden paket, tak daný tok je expirovaný.

activeTimeout	nastavenie času v milisekundách pre aktívny timeout. Aktívny timeout je čas, po uplynutí ktorého je príslušný tok expirovaný a údaje exportované aj napriek tomu, že pakety pre príslušný tok sú stále zachytávané. Musí byť väčší ako pasívny timeout.
sampling	značka ohraničujúca nastavenia týkajúce sa vzorkovania
type	celočíselná hodnota z intervalu 0 až 5 špecifikujúca spôsob vzorkovania
parameter1	prvý parameter pre vzorkovacie funkcie.
parameter2	druhý parameter pre vzorkovacie funkcie.
templates	značka ohraničujúca nastavenia týkajúce sa šablón
template	značka ohraničujúca nastavenia týkajúce sa jednej konkrétnej šablóny
field	definícia poľa v rámci jednej šablóny prostredníctvom identifikačného čísla informačného elementu *elementID* . Ak je tento element skupinovo (enterprise) špecifický, značka field sa zadáva spolu s atribútom enterprise.
mediator	značka ohraničujúca nastavenia pre mediátor
doMediation	prepínač na zapnutie/vypnutie služby
collector	značka ohraničujúca nastavenia pre kolektor
version	špecifikácia verzie kolektora/mediátora (verzia IPFIX protokolu)

host	internetová adresa zhromažďovača/mediátora, prípadne localhost
port	port, na ktorom kolektor/mediátor očakáva IPFIX správy
protocol	transportný protokol, ktorý sa použije pri odosielaní IPFIX správ
refreshTemplateTime	čas, po ktorom má byť používaná šablóna opätovne preposielaná kolektoru/mediátoru. (Nastavenie zavisí od nastavenia "default template lifetime"v kolektore.)
reconnectFrequency	počet sekúnd, po ktorých sa nástroj MyBeem bude pokúšat o znovupripojenie ku zhromažďovaču/mediátoru
connectionTimeout	počet sekúnd, po ktorých vyprší timeout spojenia so zhromažďovačom/mediátorom
synchronization	značka ohraničujúca nastavenia pre synchronizačný server
doSync	prepínač na zapnutie/vypnutie synchronizácie voči synchronizačnému serveru, false-zapnutá synchronizácia true-vypnutá synchronizácia
port	port, na ktorom MyBeem očakáva synchronizačné správy
serverAddress	internetová adresa synchronizačného servera
serverPort	port, na ktorom synchronizačný server očakáva synchronizačné správy

logging	značka ohraničujúca nastavenia pre správu logov
sendingProtocol	protocol, pomocou ktorého budú zasielané výpisy na syslog server
syslogServIP	internetová adresa syslog servera
syslogServPort	port, na ktorom bude komunikovať exportér so syslog serverom
messageLogLevel	nastavenie úrovne výpisov programu
aggregation	značka ohraničujúca nastavenie pre agregačný proces
aggregationTrigger	časový interval, po ktoreho ubehnutí bude stále prechádzaná vyrovnávacia pamäť tokov
octetTotalCountForAggregation	minimálny počet oktetov, ktorý ak tok spĺňa, tak nedôjde k jeho agregácii
doAggregation	prepínač na zapnutie/vypnutie procesu agregácie
automaticAggregation	prepínač na zapnutie/vypnutie procesu automatickej agregácie
first	kľúčový element s najvyššou hodnotou priority, ktorý bude agregovaný
second	kľúčový element s druhou najvyššou hodnotou priority, ktorý bude agregovaný
third	kľúčový element s treťou najvyššou hodnotou priority, ktorý bude agregovaný
fourth	kľúčový element so štvrtou najvyššou hodnotou priority, ktorý bude agregovaný

dpi	značka ohraničujúce konfigurácie pre hĺbkovú analýzu paketov
doDPI	prepínač na zapnutie/vypnutie služby
protfile	cesta k súboru aplikačných protokolov

10.1.2 Podporované vzorkovacie metódy

Nasleduje charakteristika podporovaných vzorkovacích metód. Každá metóda má dva parametre. Význam dvoch spomínaných parametrov pri vykonávaní jednotlivých vzorkovacích funkcií je nasledovný:

Charakteristika typov vzorkovania

- **typ 0 - všetky odchytené pakety sú spracovávané.**
- **typ 1 - Systematické vzorkovanie podľa počtu.**
  parameter1 - počet vyberaných paketov z radu prichádzajúcich.
  parameter2 - počet následne nevyberaných paketov z radu prichádzajúcich.
- **typ 2 - Systematické vzorkovanie podľa času.**
  parameter1 - čas v sekundách počas ktorého sú pakety pre ďalšie spracovanie vyberané.
  parameter2 - čas v sekundách počas ktorého pakety pre ďalšie spracovanie vyberané nie sú.
- **typ 3 - Náhodné vzorkovanie n z N.**
  parameter1 - (n) počet náhodne vybraných paketov z N-prvkovej množiny prichádzajúcich paketov.
  parameter2 - (N) počet prichádzajúcich paketov, z ktorých sa má vybrať náhodnych n paketov. Tento parameter musí byť väčší ako parameter1 a zároveň menší ako 1000.

- **typ 4 - Vzorkovanie na základe náhodnej uniformnej pravdepodobnosti.**
  parameter1 - pravdepodobnosť, celočíselná hodnota z intervalu 0 až 100. parameter2 - v tomto prípade nepožadovaný a jeho hodnota sa nebude brať do úvahy.
- **typ 5 - Vzorkovanie na základe náhodnej neuniformnej pravdepodobnosti.**
  parameter1 - začiatok intervalu istého výberu (sure-sampled interval) udávaný v počte sekúnd od začiatku unixovej epochy (0:00:00 1.1.1970).
  parameter2 - koniec intervalu istého výberu paketov. Zadáva sa rovnakým spôsobom ako parameter1.

10.1.3 Podporované informačné elementy

Program MyBeem podporuje nasledujúce informačné elementy (podrobný popis jednotlivých informačných elementov sa nachádza na stránke registra IPFIX informačných elementov[2]):

Tabuľka 10 – 2: Podporované informačné elementy

elementID	názov elementu
1	octetDeltaCount
2	packetDeltaCount
4	protocolIdentifier
5	ipClassOfService
7	sourceTransportPort
8	sourceIPv4Address
11	destinationTransportPort

[2]http://www.iana.org/assignments/ipfix/ipfix.xhtml

12	destinationIPv4Address
21	flowEndSysUpTime
22	flowStartSysUpTime
27	sourceIPv6Address
28	destinationIPv6Address
31	flowLabelIPv6
32	icmpTypeCodeIPv4
33	igmpType
36	flowActiveTimeout (activeTimeout)
37	flowIdleTimeout (passiveTimeout)
54	fragmentIdentification
55	postIpClassOfService
56	sourceMacAddress
60	ipVersion
80	destinationMacAddress
85	octetTotalCount
86	packetTotalCount
88	fragmentOffset
95	applicationId
96	applicationName
130	exporterIPv4Address
131	exporterIPv6Address
132	droppedOctetDeltaCount
133	droppedPacketDeltaCount
136	flowEndReason
138	observationPointId
139	icmpTypeCodeIPv6

148	flowID
149	observationDomainID
152	flowStartMilliseconds
153	flowEndMilliseconds
154	flowStartMicroseconds
155	flowEndMicroseconds
156	flowStartNanoseconds
157	flowEndNanoseconds
158	flowStartDeltaMicroSeconds
159	flowEndDeltaMicroSeconds
160	systemInitTimeMilliseconds
161	flowDurationMilliseconds
162	flowDurationMicroseconds
173	flowKeyIndicator
176	icmpTypeIPv4
177	icmpCodeIPv4
178	icmpTypeIPv6
179	icmpCodeIPv6
184	tcpSequenceNumber
185	tcpAcknowledgementNumber
186	tcpWindowSize
187	tcpUrgentPointer
189	ipHeaderLength
190	totalLengthIPV4
192	ipTTL
193	nextHeaderIPV6
195	ipDiffServCodePoint

196	ipPrecedence
197	fragmentFlags
198	octetDeltaSumOfSquares
199	octetTotalSumOfSquares
204	ipPayloadLength
206	isMulticast
207	ipv4IHL
211	collectorIPv4Address
212	collectorIPv6Address
213	exportInterface
214	exportProtocolVersion
215	exportTransportProtocol
216	collectorTransportPort
217	exporterTransportPort
218	tcpSynTotalCount
219	tcpFinTotalCount
220	tcpRstTotalCount
221	tcpPshTotalCount
222	tcpAckTotalCount
223	tcpUrgTotalCount
224	ipTotalLength
240	roundTripTimeNanoseconds
241	packetPairsTotalCount
242	firstPacketID
243	lastPacketID
244	flowStartAfterExport
375	originalFlowsPresent

376	originalFLowsInitiated
377	originalFLowsCompleted
378	distinctCountOfSourceIPAddress
379	distinctCountOfDestinationIPAddress
380	distinctCountOfSourceIPv4Address
381	distinctCountOfDestinationIPv4Address
382	distinctCountOfSourceIPv6Address
383	distinctCountOfDestinationIPv6Address

10.2 Súbor aplikačných protokolov

Súbor aplikačných protokolov sa využíva v rámci služby hĺbkovej analýzy paketov. Používateľ prostredníctvom tohto súboru môže rozšíriť základnú sadu podporovaných aplikačných protokolov. Je to obyčajný textový súbor, ktorý musí mať nasledujúcu štruktúru:

```
<tcp|udp>:<port>,<tcp|udp>:<port>,...@<protocol_name>
```

Prostredníctvom tohto súboru sa dajú definovať aj podprotokoly pre aplikačný protokol HTTP. Ich definícia musí mať nasledujúcu štruktúru:

```
host:"<value>",host:"<value>",...@<subprotocol_name>
```

Ďalej sú uvedené príklady pre obe definície (prvý riadok predstavuje definíciu nového aplikačného protokolu a druhý riadok definíciu nového podprotokolu):

```
tcp:3000@ntop
host:"fei.tuke.sk"@TUKE FEI
```

11 Chybové hlásenia

Počas behu programu môže dôjsť k neočakávaným chybám. Používateľ je o všetkých chybách informovaný prostredníctvom chybových hlásení, ktoré budú uvedené v tejto kapitole. Neuvádzajú sa však hlásenia, ktoré môžu byť vyvolané podpornými knižnicami. Okrem týchto hlásení MyBeem vypisuje na konzolu aj hlásenia, ktoré majú čisto informatívny charakter. Ich účelom je iba informovať používateľa o aktuálnej činnosti vykonávanej programom.

Zoznam chybových hlásení:

- `Flow cache full. Consider increasing MAXFLOWCACHE` - preplnená pamäť tokov. Pravdepodobne je nastavený príliš veľký interval expirácie, alebo príliš malá veľkosť pamäte tokov (flow-cache).
- `Forcing program to stop(not waiting for pcap loop to finish)` - Násilné ukončenie programu dvojitím stlačením kombinácie CTRL + C.
- `IP address conversion error` - Chyba pri konverzii na bodkovú notáciu.
- `IP address netmask conversion error` - chyba pri konverzii sieťovej masky na bodkovú notáciu.
- `Filter compilation error. Filter deactivated` - Syntaktická chyba vo filtri. Filter deaktivovaný.
- `Filter pcap application error. Filter deactivated` - Chyba pri kompilácii filtra. Filter deaktivovaný.
- `Error in xmlXPathNewContext` - Chyba pri vytváraní nového XPath kontextu.
- `Error in xmlXPathEvalExpression` - Chyba pri vyhodnocovaní XPath výrazu.
- `Configuration not parsed succesfully` - Chyba v konfiguračnom súbore.

- `Cannot init ipfix module:-` Chyba pri inicializácii ipfix exportného modulu.
- `Ipfix_open() failed:` *dôvod* - Chyba pri otváraní spojenia s ipfix kolektorom.
- `Ipfix_add_collector() host,port failed:` *dôvod* - Chyba pri pridávaní kolektora.
- `Ipfi_new_template() failed:` *dôvod* - Chyba pri pridávaní šablóny.
- `Ipfix_add_field() failed:` *dôvod* - chyba pri pridávaní poľa šablóny.
- `Ipfix_export() failed:` *dôvod* - zlyhanie ipfix exportu.
- `Ipfix_export_flush() failed:` *dôvod* - Zlyhanie pri ukončovaní ipfix exportu
- `Select error_ sockfd not set` - Chyba pri výbere soketu pre komunikáciu
- `Fnctl failed:` *dôvod* - chyba pri nastavovaní príznakov pre soket.
- `Cannot get address of host` *'IP adresa': dôvod* - Zlyhal preklad DNS mena na IP adresu.
- `Socket() failed:` *dôvod* - všeobecné zlyhanie soketu.
- `Cannot conntect to host:` *dôvod* - Zlyhanie spojenia s kolektorom.
- `Connection lost. Reconect.` - Zlyhanie TCP, alebo SCTP transportu. Spojenie bude obnovené.
- `Connection timed out` - Vypršal timeout spojenia so zhromažďovačom.
- `Ipfix message dropped. Size:` *veľkosť*, `Sequence number:` *sekvenčné číslo* - IPFIX správa s danou veľkosťou a sekvenčným číslom bola zahodená.
- `INTERNAL ERROR: ipfix node not found!` - Interná chyba programu. Neexistencia uzla struktúry šablón.

- `Wrong type of sampling specified` - chybne špecifikovaný typ vzorkovania.
- `Wrong sampling parameter #1` - Chybne definovaný 1.parameter vzorkovania
- `Wrong sampling parameter #2` - Chybne definovaný 2.parameter vzorkovania
- `Error: gethostbyname..` *dôvod* - Nakonfigurovaný host neznámy.
- `Error: bind failed` *dôvod* - Operácia bind zlyhala.

11.1 Chybové hlásenia nástroja beem_adjuster.sh

Počas vytvorenia programu "šitého na meru"môže dôjsť k prerušeniu práce nástroja. Používateľ je o všetkých chybách informovaný prostredníctvom chybových hlásení, ktoré budú uvedené v tejto kapitole.

Zoznam chybových hlásení:

- **The script needs to be in the same directory as the beem project is!** – skript sa nenachádza v adresári, v ktorom sú zdrojové kódy a dodatočné súbory programu MyBeem.
- **You need to install package libxml2-utils to use this script!** – na systéme nie je nainštalovaný balík libxml2-utils.
- **You can not start Beem with an empty Information Model...** – prostredníctvom konfiguračného súboru boli "vypnuté"všetky informačné elementy. Je potrebné povoliť aspoň jeden.
- **COMPILATION FAILURE!** – počas prekladu sa odhalili syntaktické chyby programovacieho jazyka C. Súčasťou tejto hlášky sa uvádza aj miesto vzniku chyby v zdrojových kódoch.

Referencie

[1] MONICA: *SLAmeter.* 2012. Dostupné na internete: <`http://wiki.cnl.sk/Monica/SLAmeter`>

[2] TREMKO, S.: *Meracie body pre nástroj SLA Meter: Bakalárska práca.* Košice: KPI FEI TUKE, 2012. 62 s.

[3] KECSEY, T.: *Konformita nástroja BasicMeter s architektúrou IPFIX: Bakalárska práca.* Košice: KPI FEI TUKE, 2010. 59 s.

[4] HUSIVARGA, Ľ.: *Identifikácia paketových párov: Bakalárska práca.* Košice: KPI FEI TUKE, 2008. 43 s.

[5] HUSIVARGA, Ľ.: *Meranie časových charakteristík sieťovej prevádzky: Diplomová práca.* Košice: KPI FEI TUKE, 2010. 64 s.

[6] KECSEY, T.: *Optimalizácia meracieho a exportovacieho procesu nástroja BasicMeter: Diplomová práca.* Košice: KPI FEI TUKE, 2012. 90 s.

[7] TREMKO, S.: *Redukcia informácií o IP tokoch za účelom zníženia záťaže monitorovacích systémov: Diplomová práca.* Košice: KPI FEI TUKE, 2014. 85 s.

[8] FARKAS, D.: *Hĺbková analýza paketov prostredníctvom protokolu IPFIX: Diplomová práca.* Košice: KPI FEI TUKE, 2015. 78 s.