Technická univerzita v Košiciach
Fakulta elektrotechniky a informatiky
Katedra počítačov a informatiky

Aplikačný rámec pre sprostredkovanie IPFIX správ v nástroji SLAmeter

Diplomová práca

Príloha B

POUŽÍVATEĽSKÁ PRÍRUČKA Mediator v1.0

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

Košice 2013 **Bc. Rastislav Kudla**

Obsah

1 Funkcia programu **6**

2 Súpis obsahu dodávky **7**

3 Inštalácia programu **8**

3.1 Požiadavky na technické prostriedky 8

3.2 Požiadavky na programové prostriedky 8

3.3 Vlastná inštalácia 9

3.3.1 Inštalácia Java 7 pod OS Ubuntu/Debian 9

3.3.2 Inštalácia samotnej aplikácie Mediator pod OS Ubuntu/Debian 9

4 Použitie programu **10**

4.1 Popis dialógu s používateľom 11

4.2 Popis konfiguračného súboru 11

4.3 Popis správ pre systémového programátora 15

5 Obmedzenia programu **15**

6 Chybové hlásenia **17**

7 Príklad použitia **22**

Zoznam použitej literatúry **23**

Zoznam obrázkov

Zoznam tabuliek

4 – 1 Voľby konfiguračného súboru 1 13
4 – 2 Voľby konfiguračného súboru 2 14
4 – 3 Logovacie úrovne programu 15

1 Funkcia programu

Program Mediátor je implementáciou aplikačného rámca pre problém sprostredkovania správ v protokole IPFIX *(IP Flow Information Export (IPFIX) Mediation Problem)* vyvíjaný výskumnou skupinou MONICA sídliacou v Laboratóriu počítačových sietí *(CNL)* na Technickej Univerzite v Košiciach. Je súčasťou meracej architektúry SLAmeter, ktorej úlohou je pasívne meranie parametrov sieťovej prevádzky na báze tokov. Na základe nameraných hodnôt určuje triedu kvality služieb a Internetového pripojenia poskytovateľov Internetu. Trieda kvality vypovedá o dodržiavaní zmluvy o úrovni poskytovanej služby - *SLA*.

Komponentmi architektúry IPFIX (IP Flow Information Export) podľa RFC 5470 [1] sú exportéry a kolektory komunikujúce protokolom IPFIX. Vzhľadom k trvalému rastu IP prevádzky v heterogénnych sieťových prostrediach, tieto exportér-kolektor systémy môžu viesť k problémom škálovateľnosti. Naviac, neposkytujú flexibilitu potrebnú pre široký rad meracích aplikácii.

Sprostredkovateľské moduly Mediátora môžu z pohľadu manipulácie s dátami poskytovať agregáciu, koreláciu, filtrovanie, anonymizáciu a iné úpravy záznamov o tokoch za účelom šetrenia výpočtových zdrojov meracieho systému a vykonávania predspracovania úloh pre kolektor. Z hľadiska interoperability nástrojov rôznych vývojárov, môžu poskytovať konverziu z iných protokolov na IPFIX, respektíve zvyšovať spoľahlivosť exportov napríklad prevodom z nespoľahlivého, bezspojovo orientovaného protokolu UDP na spoľahlivý SCTP.

Program bol v roku 2013 vytvorený Rastislavom Kudlom v rámci jeho diplomovej práce.

2 Súpis obsahu dodávky

Program je dodávaný na jednom inštalačnom CD médiu (Príloha C - CD), ktoré obsahuje nasledujúce súčasti:

- zdrojové súbory programu
- samostatne spustiteľné binárne súbory
- knižnice potrebné pre funkčnosť programu
- DEB inštalačný balík
- dokumentáciu zloženú z:

  diplomovej práce (PDF, LaTeX)

  systémovej príručky (PDF, LaTeX)

  tejto používateľskej príručky (PDF, LaTeX)

3 Inštalácia programu

3.1 Požiadavky na technické prostriedky

Spoľahlivý beh samotného programu si vyžaduje nasledovnú hardvérovú konfiguráciu:

- CPU Intel Pentium III 1Ghz alebo ekvivalent
- operačná pamäť 256MB
- pevný disk s 1GB a viac voľného miesta
- sieťová karta 100Mbit/s

Program pre spoľahlivý beh vyžaduje minimálne 32MB voľnej pamäte RAM. Nainštalovaný program zaberá približne 3.9MB na pevnom disku. Uvedené voľné miesto na pevnom disku je potrebné, kvoli logovacim vystupom. Je potrebné si uvedomiť, že pri prepinaci `--logtofile` program loguje do /var/log/mediator/ a pri nastavenej úrovni logovania DEBUG, môžu logovacie súbory mať značnú veľkosť. Pri dosiahnutí veľkosti 100MB sa obsah log súboru zálohuje a skomprimuje. Archivuje sa posledných 10 rotácií (1GB log výstupu). Monitorovanie rozsiahlejšej siete (napr. sieť poskytovateľa komunikačných služieb) si vyžaduje podstatne vyššie hardvérové nároky.

3.2 Požiadavky na programové prostriedky

- operačný systém GNU/Linux s verziou jadra 2.6 a vyššou
- Java Runtime Environment (JRE) verzie 1.7.0_03 a vyššej
- knižnice dodávané na inštalačnom médiu

3.3 Vlastná inštalácia

Vlastná inštalácia sa skladá z inštalácie DEB balíka v prostredí operačného systému Ubuntu alebo Debian. V prostredí iného operačného systému inštalácia pozostáva z nakopírovania spustiteľného Java archívu (`mediator.jar`) do priečinka podľa vlastnej voľby spoločne s adresárom knižníc. Následne treba do tohto priečinka nakopírovať súbor popisujúci podporované informačné elementy protokolu IPFIX programom Mediator (`ipfixFields.xml`) a ukážkový konfiguračný súbor (`config.xml`), ktorý je potrebné upraviť pre vlastné prostredie meraní.

3.3.1 Inštalácia Java 7 pod OS Ubuntu/Debian

```
sudo apt-get update
sudo apt-get install openjdk-7-jre-headless
```

3.3.2 Inštalácia samotnej aplikácie Mediator pod OS Ubuntu/Debian

Instalacia je velmi jednoducha. Staci stiahnut inštalačny DEB balík zo SVN repozitára:

```
wget https://svn.cnl.tuke.sk/monica/BasicMeter/Mediator/deb/mediator
_1.0_i386.deb --no-check-certificate
```

Spustiť stiahnutý DEB balík pomocou príkazu

```
sudo dpkg -i mediator_1.0_i386.deb
```

Nakoniec je potrebne nastavenie konfiguračného súboru `/etc/mediator/config.xml`. Najdôležitejšie je nastaviť spravny port, na ktorom bude Mediator ocakavat IPFIX spravy a parametre exportovacieho procesu. Nemenej dolezita je konfiguracia sprostredkovateslkych procesov.

4 Použitie programu

Mediator je konzolová aplikácia. Spustenie programu na operačných systémoch Ubuntu/Debian pri inštalácii pomocou DEB balíka je nasledovné:

```
mediator [/cesta/ku/konf./súboru/config.xml] [--logtofile]
```

Ak sa nezadá cesta ku konfiguračnému súboru, resp. subor sa na zadanej ceste nenachadza, aplikácia oznami tuto situaciu pouzivatelovi a automaticky hlada konfiguracny subor v `/etc/mediator/config.xml`. Ak konfiguračný súbor nie je nájdený ani na vychodiskovom mieste, aplikácia skončí s chybovým hlásením.

Ak zadáme nepovinný argument `--logtofile`, výstup programu bude presmerovaný do log súboru

```
/var/log/mediator/YYYYMMDD-HHmmss/mediator.log
```

,

kde Y-rok, M-mesiac, D-deň, H-hodina, m-minúta, s-sekunda spustenej inštancie programu Mediator.

Ak používateľ nie je root, je potrebné mať v systéme pridelené sudo právo a Mediator spustiť príkazom:

```
sudo mediator [/cesta/ku/konf./súboru/config.xml] [--logtofile]
```

Tak ako väčšina aplikácií v prostredí operačného systému Linux, aj Mediator má k dispozícii manuálové stránky (man), ktoré je možné zobraziť pomocou príkazov:

```
man mediator
```

```
man mediator_config
```

V prostredí iného operačného systému ako Ubuntu/Debian, alebo pri potrebe manuálneho spustenia, sa program spúšťa pomocou Java interpretéra s voliteľným pa-

rametrom pozostávajúcim z cesty (relatívnej alebo absolútnej) ku konfiguračnému súboru a s volitelnym prepinacom `--logtofile`:

```
java -jar mediator.jar [/cesta/ku/konf./súboru/config.xml]
                       [--logtofile]
```

Ďalšou podmienkou spustenia progrmau Mediator je súbor *ipfixFields.xml*. Cesta k tomuto súboru sa nastavuje v konfiguračnom súbore *config.xml*. Ak pri spustení sa súbor ipfixFields nenachádza v adresári definovanom v konfiguračnom súbore, aplikácia skončí s chybovým hlásením. V prípade absencie riadku s cestou k *ipfixFields.xml* v konfiguračnom súbore, Mediator automaticky predpokladá túto cestu: `/etc/mediator/ipfixFields.xml`. Ak sa ani tu XML súbor nenachádza, Mediator ukončí svoju činnosť. Bez tohto súboru nie je možné rozpoznať údaje z prijatých IPFIX paketov.

4.1 Popis dialógu s používateľom

Kedže program je konzolová aplikácia, neposkytuje žiadne grafické zobrazenie dialógu pre používatela. Chybové a informacné hlásenia sú zobrazované v rovnakej konzole v ktorej bol program spustený, prípadne v log súbore ak bol program spustený s voliteľným argumentom `--logtofile`.

Ukončenie programu sa vykoná stlačením kombinácie kláves *CTRL + C* alebo poslaním signálu *SIGTERM* alebo *SIGINT* konkrétnemu procesu:

```
kill -SIGTERM pid_procesu_mediator
```

4.2 Popis konfiguračného súboru

Vychodiskovy adresar, kde sa nachadza konfiguracny subor je `/etc/mediator/`. Jednotlivé konfiguračné parametre sa triedia podľa typu modulov, ktorých sa nastavenia

týkajú. Tieto typy ako aj zoznam všetkých možných parametrov, ich popis, štandardné hodnoty a možné voľby sa nachádzajú v tabuľkách 4 – 1, **??**, 4 – 2 a **??**. V prípade, že daná hodnota pre akýkoľvek parameter nie je uvedená v konfiguračnom súbore, parameter sa nastaví na štandardnú hodnotu. Ukážkový konfiguračný súbor na inštalačnom médiu obsahuje približné popisy parametrov a ich štandardné hodnoty. Parameter sa zapisuje vo formáte:

```
<meno_parametra>hodnota</meno_parametra>
```

Vynimku tvori len konfiguracia sprostredkovatelskych procesov. Tie sa zapisuju vo formate:

```
<process name="ExampleProcess">
  <input>exporter</input>
</process>
```

Konfiguračný súbor môže obsahovať komentár, ktorý musí byť ohraničený znakmi:

```
<!-- komentár -->
```

Tabuľka 4 – 1 Voľby konfiguračného súboru 1

Parameter	**Štandardná hodnota**	**Prípustné hodnoty**	**Popis**
Modul: Všeobecné nastavenia celého programu (global)			
logLevel	ERROR	ALL, DEBUG, INFO, WARN, TRACE, ERROR, FATAL, OFF	úroveň logovania programu
ipfixFieldsXML	/etc/mediator/ipfixFields.xml	platná cesta v rámci súborového systému	cesta k XML súboru popisujúceho IPFIX informačné elementy
ipfixTemplateTimeout	300	prirodzené celé číslo väčšie ako 0	čas, po ktorom sa čablóna pre IPFIX paket považuje za neplatnú
observationDomainID	1	prirodzené celé číslo väčšie ako 0	ID pozorovacej domény
Modul: Zhromažďovací modul (collecting)			
listenPort	6666	prir. číslo z intervalu <0-65535> (kt. nie je obsadené)	port, na ktorom beží vlákno čítajúce dáta zo siete
receiveUDP	yes	yes, no	príjem pomocou transportného protokolu UDP
Modul: Modul pre sprostredkovateľské procesy (processes)			
name	–	názov hlavnej triedy sprost. procesu v baliku IntermediateProcesses	meno sprostredkovateľského procesu
input	–	exporter, názov hlavnej triedy sprost. procesu v baliku IntermediateProcesses	nazov procesu, od ktorého tento proces prijíma záznamy o tokoch. hodnota je buď exporter, alebo akýkoľvek sprostredkovateľský proces - jeho „name“

Tabuľka 4 – 2 Voľby konfiguračného súboru 2

Parameter	**Štandardná hodnota**	**Prípustné hodnoty**	**Popis**
Modul: Exportovací proces (exporting)			
version	10	10	verzia IPFIX protokolu
host	127.0.0.1	názov alebo IP adresa kolektora-/ineho mediatora	IP adresa IPFIX kolektora/mediatora
port	4739	prir. číslo z intervalu <0-65535> (kt. nie je obsadené)	port, na ktorom pocuva kolektor/iny mediator
protocol	UDP	UDP	názov transportného protokolu
refreshTemplateTime	5	prirodzené celé číslo väčšie ako 0	čas (s) po ktorom Mediator exportuje príslušnú šablónu (ak sa nastaví vyššia hodnota ako je v exportéri, tak reálne platí hodnota daná exportérom)
exportTime	RENEW	KEEP, RENEW	sposob, akym Mediator naraba s casom v poli hlavicky spravy - „exportTime“
Modul: Expertné nastavenia (expertsOnly)			
packetCacheSize	25	prirodzené celé číslo väčšie ako 0	velkost cache pre IPFIX pakety na vstupe
inputBufferSize	75	prirodzené celé číslo väčšie ako 0	velkost vstupneho buffera sprostredkovatelskych procesov
exportCacheSize	25	prirodzené celé číslo väčšie ako 0	velkost exportovacej cache
maxInputPacketSize	65540	prirodzené celé číslo väčšie ako 0	maximalna povolena velkost jedneho IPFIX paketu

4.3 Popis správ pre systémového programátora

V dodanej verzii JXColl sa zmenil aj spôsob zobrazovania správ. Logovací subsystém však zostal nedotknutý. Správy oproti starej verzie programu sú teraz prehľadnejšie a kratšie.

Počas behu programu sa vypisujú rôzne hlásenia od chybových až po informačné. Logovací subsystém programu je možné inicializovať rôznymi úrovňami. Ich popis je uvedený v tabuľke 4 – 3. Každá úroveň zahŕňa v sebe aj úrovne na nižšom stupni, takže napr. pre úroveň ERROR sa budú zobrazovať aj hlásenia typu FATAL. Na reálnu prevádzku je vhodné nastaviť úroveň ERROR.

Tabuľka 4 – 3 Logovacie úrovne programu

Typ hlásenia	**Popis**
ALL	vypisuje sa všetko
DEBUG	zobrazujú sa kompletné výpisy celého diania v programe
INFO	program informuje o svojej činnosti a akcii, INFO ktorú práve vykonáva
WARN	vypíšu sa informácie o upozorneniach programu na možné chyby alebo zlú interpretáciu vstupných dát
TRACE	zobrazia sa informácie o stave programu
ERROR	sú vypísané hlásenia chýb majúcich vplyv na dáta
FATAL	hlásenia, ktoré sú pre beh programu smrteľné a zvyčajne znamenajú nezotaviteľnú chybu programu
OFF	vypnú sa všetky hlásenia programu

5 Obmedzenia programu

Program sa bude na pomalších počítačoch jednoznačne pomalšie spúšťať, keďže Java je jazyk interpretovaný a bežiaci vo vlastnom virtuálnom stroji. Rýchlosť programu

tiež závisí na množstve prijatých dát. Ďalšie obmedzenie je dané schémou databázy, ktorá je vopred daná, a pre jej zmenu je nutné zmeniť aj samotný zdrojový kód.

6 Chybové hlásenia

Počas používania programu môže dôjsť k nasledujúcim chybám. Časové známky boli odstránené kvôli zvýšeniu prehľadnosti.

Chyba:

```
DEBUG [main] DBExport  -
Connecting to postgres@jdbc:postgresql://127.0.0.3:5432/bm...

ERROR [main] DBExport  -
Connection refused. Check that the hostname and port are correct and
that the postmaster is accepting TCP/IP connections.

INFO [main] DBExport  -
Login failed. org.postgresql.util.PSQLException: Connection refused. Check
that the hostname and port are correct and that
the postmaster is accepting TCP/IP connections. SQL error

INFO [main] DBExport  -
Login failed. org.postgresql.util.PSQLException: FATAL: password authentication
failed for user "postgres" SQL error
```

Popis a riešenie: V týchto prípadoch sa JXColl nedokáže napojiť na databázu. Buď je zle zadaná adresa, port servera, prihlasovacie údaje alebo je spojenie blokované/nefunkčné.

Chyba:

```
INFO  [main] Config  - Loading config file: /zla/cesta/k/jxcoll_config.xml
ERROR [main] Config  - Could not load config file: /zla/cesta/k/jxcoll_config.xml !
```

Popis a riešenie: Nie je možné načítať konfiguračný súbor. Treba sa uistiť, či súbor /etc/jxcoll/jxcoll.conf existuje, alebo či je k nemu správne zadaná cesta.

Chyba:

```
FATAL [main] IpfixElements  - XML file "/etc/jxcoll/ipfixFields.xmla"
was not found!
FATAL [main] JXColl  - JXColl could not start because of an error while
```

```
processing XML file!
```

Popis a riešenie: Nenašiel sa ipfixFields.xml súbor, ktorý slúži na rozpoznanie údajov z IPFIX paketu. Treba sa uistiť, či sa súbor nachádza v priečinku definovanom v konfiguračnom súbore alebo v predvolenej ceste (/etc/jxcoll/ipfixFields.xml).

Chyba:

```
ERROR [ACP Thread 4] ACPIPFIXWorker  - IO EXCEPTION :null
DEBUG [ACP Thread 4] ACPIPFIXWorker  - Closing connection in try-catch
```

Popis a riešenie: V tomto prípade modul, ktorý používa protokol ACP na priame sprístupnenie nameraných dát, nečakane prerušil spojenie. JXColl sa automaticky zotaví a bude naďalej čakať pripojenie cez protokol ACP.

Chyba:

```
ERROR [UDP Processor] DBExport  - Check if is DB connected failed:
java.lang.NullPointerException
```

Popis a riešenie: Počas spracovania údajov sa došlo k prerušení spojenia s databázou. Treba sa uistiť, či chyba nenastala v spojení.

Chyba:

```
ERROR [Net Parser] RecordDispatcher  - Element with ID: 74 is not supported,
skipped! Update XML file!
```

Popis a riešenie: Počas spracovania údajov sa narazilo na nepodporovaný informačný element. JXColl tento element preskočí. Treba aktualizovať XML súbor ipfixFields.xml o informácie o tomto elemente, prípadne doimplementovať jeho podporu v JXColl.

Chyba:

```
ERROR [UDP Processor] RecordDispatcher  - i.e. 'icmpTypeCodeIPv6' (unsigned16) -
received data has wrong datatype! (10 bytes)
ERROR [UDP Processor] RecordDispatcher  - Skipping this element DB exportation!
```

Popis a riešenie: Počas spracovania údajov sa narazilo na informačný element, ktorého veľkosť nekorešponduje s očakávaným dátovým typom podľa XML súboru. JXColl tento element preskočí. Nápravu je nutné vykonať pravdepodobne na strane exportéra.

Chyba:

```
ERROR [UDP Processor] RecordDispatcher  - "i.e. 'subTemplateMultiList' -
Cannot decode datatype: subTemplateMultiList
ERROR [UDP Processor] RecordDispatcher  - Skipping this element DB exportation!
```

Popis a riešenie: Počas spracovania údajov sa narazilo na informačný element, ktorého dátový typ JXColl nevie dekódovať. JXColl tento element preskočí. Nápravu je nutné vykonať na strane JXColl.

Chyba:

```
ERROR [TCP Processor] IpfixParser  - Field data is longer than remaining bytes in Data Set!
ERROR [TCP Processor] IpfixParser  - Corrupted data detected! Shutting down TCP connection to IP:port

ERROR [TCP Processor] IpfixParser  - Template Set is not long enough to hold all field specifiers!
ERROR [TCP Processor] IpfixParser  - Corrupted data detected! Shutting down TCP connection to IP:port

ERROR [TCP Processor] IpfixParser  - Options Template has field count set to 0!
ERROR [TCP Processor] IpfixParser  - Corrupted data detected! Shutting down TCP connection to IP:port

ERROR [TCP Processor] IpfixParser  - Message length (20) is not as stated in header (630)!
ERROR [TCP Processor] IpfixParser  - Corrupted data detected! Shutting down TCP connection to IP:port

ERROR [TCP Processor] IpfixParser  - Set states that it is longer than remaining data part is!!
ERROR [TCP Processor] IpfixParser  - Corrupted data detected! Shutting down TCP connection to IP:port
```

Popis a riešenie: Počas príjmu údajov cez protokol TCP boli prijaté chybné dáta, spojenie sa uzatvára a vlákno končí. Chyba bola spôsobená na strane exportéra poslaním poškodených dát. Tieto chybové správy platia a majú rovnaký význam aj pre protokol SCTP. Chyba bola spôsobená exportérom.

Chyba:

```
ERROR [TCP Processor] IpfixParser  - Attempt to withdraw Template #267, OD:0,
which does not exist in cache!
ERROR [TCP Processor] IpfixParser  - Shutting down TCP connection to IP:port
```

Popis a riešenie: Počas príjmu údajov cez protokol TCP bola prijatá správa Template Withdrawal Message, ktorá ruší už predtým zrušenú alebo neexistujúcu šablónu. Správa sa zahodí, spojenie sa násilne uzavrie (RST) a vlákno končí. Rovnaký význam platí aj pre protokol SCTP. Chyba bola spôsobená exportérom.

Chyba:

```
ERROR [TCP Processor] IpfixParser  - Template #267 is already in cache!
ERROR [TCP Processor] IpfixParser  - Shutting down TCP connection to IP:port
```

Popis a riešenie: Ide o pokus o pridanie šablóny do cache, ktorá tam už existuje. Správa sa zahodí, spojenie sa násilne uzavrie (RST) a vlákno končí. Rovnaký význam platí aj pre protokol SCTP. Chyba bola spôsobená exportérom.

Chybové hlásenia súvisiace s Java Virtual Machine (JVM)

Program je interpretovaný v Java Virtual Machine. Chyby, ktoré môžu nastať a nie sú ošetrené vlastnými chybovými hláseniami programu sú chyby, ktoré boli nepredvídané a sú ľahko rozoznateľné tým, že nie sú formátované v štýle loggera a zvyčajne sú označené ako Java Error alebo Exception. Obyčajne sa vypíše aj časť zásobníka. Bežne sú to tri riadky v hierarchii volania danej metódy, ktorá takto zlyhala. Takéto chyby znamenajú poškodenie funkcie programu a je nutné ho reštartovať. Chybu je možné opraviť len v zdrojovom kóde, teda sa berie ako programátorská chyba.

Opis známych chýb

V súčasnosti neboli v JXColl nájdené vážne chyby.

7 Príklad použitia

Program je možné primárne použiť v spojení so zariadením alebo so softvérom, ktorý je schopný exportovať informácie o tokoch v sieti vo formáte IPFIX. Takéto zariadenie môže byť napr. Cisco router schopný exportu IPFIX dát alebo z modulov BasicMetra napríklad BEEM. Analyzujúca aplikácia je primárne zastúpená BMAnalyzer-om, a v princípe môže to byť softvér, ktorý dokáže spracovávať údaje získané buď prostredníctvom protokolu ACP, alebo z databázy. Po úprave vkladacieho SQL reťazca v zdrojovom kóde je možné JXColl prispôsobiť aj k schéme inej databázy.

Literatúra

[1] SADASIVAN, G. et al.: *Architecture for IP Flow Information Export* RFC 5470. 2009