UNIVERZITET U SARAJEVU
ELEKTROTEHNIČKI FAKULTET
ODSJEK ZA TELEKOMUNIKACIJE

Syslog - rsyslog (zabbix)

Projektni zadatak iz predmeta Upravljanje telekomunikacijskim mrežama

Teorijski dio

Ćutahija Zerina, 1685/17085
Hasanbegović Selma, 1574/17753
Mahovac Nerman, 1575/17919
Repeša Almin, 1684/17550
Velić Nejra, 1634/17313

Sarajevo, 2020. godina

Sadržaj

Uvod

U svim komplikovanijim mrežama koriste se uređaji različitih proizvođača i koji služe za razne namjene, što prikupljanje podataka čini kompleksnim i zahtijeva korištenje protokola i direktni pristup opremi. Također, potrebno je omogućiti i slanje notifikacija i alarma u slučaju pojave problema, kako bi administratori imali uvid u ponašanje sistema. Upravo zbog toga, pored ostalih, uveden je Syslog, kao protokol za nadzor mreže.

Syslog (engl. *System Logging Protocol*) je osnovni pristup za centralizirani monitoring mreže. Standardizovan je 2009. godine od strane IETF, a koristi se kao način prenosa poruka od mrežnih uređaja prema log, odnosno syslog serveru. Syslog omogućava slanje syslog poruka na centralnu lokaciju za pohranu, filtriranje, vizualizaciju i upozororavanja (engl. *alerting*). Syslog poruke se generišu periodički, a uključuju informaciju o IP adresi, vremenskom žigu (engl. *timestamp*), kao i log poruku zajedno sa njenim nivoom ozbiljnosti (engl. *severity*) u rasponu od hitnih slučajeva pa do potrebe za otklanjanjem greške. Na ovaj način, syslog pruža uvid u nadzor mreže.

Zbog svoje popularnosti i dugovječnosti većina glavnih operativnih sistema podržava syslog, uključujući macOS, Linux i Unix, a korištenjem *third-party* alata moguća je i podrška na Microsoft Windows sistemu.

Cilj ovog rada jeste teoretski obraditi syslog protokol. Rad se sastoji iz dva poglavlja. Prvo poglavlje predstavlja opis rješenja u sklopu kojeg je detaljno opisan syslog protokol, njegovi entiteti i poruke, a napravljen je i kratki pregled rsyslog-a kao syslog implementacije. Drugo poglavlje daje pregled postojećih syslog rješenja. Na kraju rada izveden je generalni zaključak, dat je popis slika, tabela i korištene literature.

1. Opis rješenja

1.1. Syslog

Syslog (engl. *System Logging Protocol*) je standardizirani protokol koji se koristi za slanje sistemskih log poruka te drugih event poruka prema syslog serveru. Primarno je korišten za sakupljanje informacija sa različitih uređaja do centralne lokacije (syslog servera) zbog monitoringa i upravljanja. Ovaj protokol je implementiran na većini mrežnih elemenata (ruteri, switchevi, firewalli), čak i na nekim printerima i skenerima, što predstavlja jednu od njegovih prednosti. Dodatno, Syslog je dostupan na Unix i Linux operativnim sistemima i mnogim web aplikacijama, uključujući Apache. Nije instaliran na default-nom Windows operativnom sistemu, jer Windows ima svoj protokol za ovu namjenu (Windows Event Log) [1]. Međutim, Microsoft Windows putem third-party alata može podržati syslog.

Syslog je klijent server protokol. Na klijentskoj strani aplikacije izvršava se softver koji generiše poruku na osnovu događaja na uređaju, a na serverskoj strani servisa izvršava se softver koji obrađuje, analizira i skladišti poruke pristigle sa različitih IP uređaja.

Syslog koristi UDP protokol na portu 514, te ne podržava potvrde o isporuci poruka. Prenos podataka u Syslog-u je asinhron. Za razliku od drugih protokola za monitoring mreže, poput SNMP-a, ne postoji mehanizam koji provjerava spremnost uređaja da primi podatke [1].

1.1.1. Syslog entiteti

Syslog koristi tri entiteta (sloja):

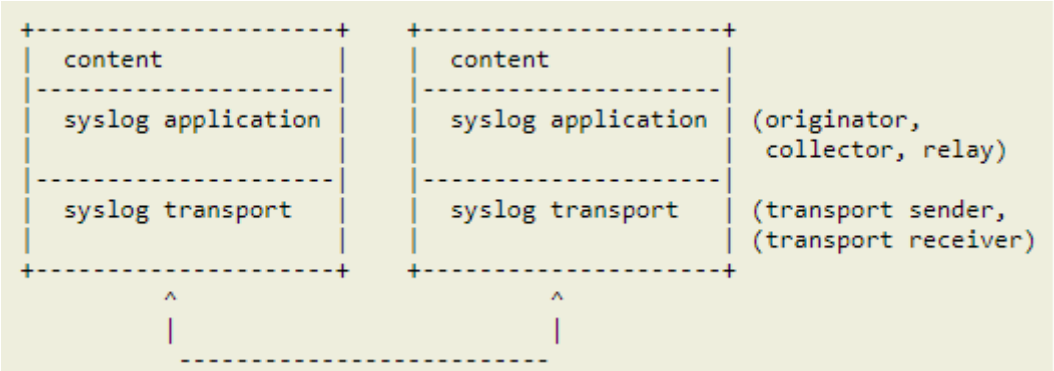
- **Syslog sadržaj** - (engl. *Syslog content*) upravlja informacijama iz syslog poruke
- **Syslog aplikacijski sloj** - (engl. *Syslog application layer*) generiše, interpretira, prosljeđuje i pohranjuje syslog poruke
- **Syslog transportni sloj** (engl. *Syslog transport layer*) - transport poruke u mrežu

Sljedeće funckije se izvršavaju na pojedinim syslog slojevima:

- **Originator** - generiše syslog sadržaj koji će se prenositi u poruci
- **Collector** - prikuplja syslog sadržaj za dalju analizu

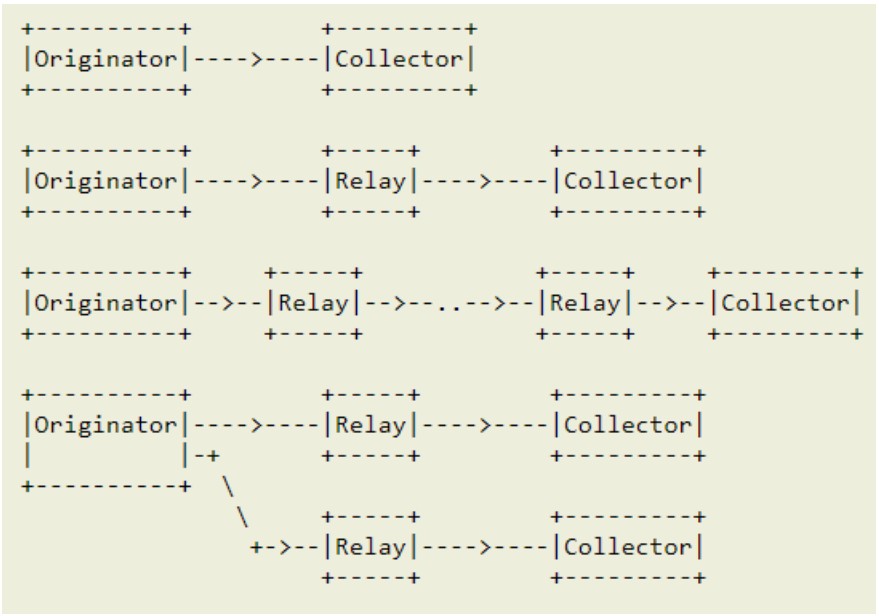
- **Reley** - prosljeđuje poruke, prihvata poruke od pokretača (*originator*) ili drugih releja, te ih šalje kolektorima ili drugim relejima
- **Transport sender** - prosljeđuje syslog poruke transportnom protokolu
- **Transport receiver** - preuzima syslog poruke od gore navedenog transportnog protokola

Na slici 1.1 je su prikazani syslog slojevi i odgovarajuće funkcije koje se na njima izvršavaju.



Slika 1.1: Prikaz syslog slojeva

Pokretači (*originators*) i releji mogu biti konfigurisani da šalju iste poruke različitim kolektorima i relejima, a funkcija pokretača, releja i kolektora se mogu nalaziti na istom sistemu [2]. Na slici 1.2 su prikazani neki od mogućih scenarija syslog implementacije.



Slika 1.2: Primjeri scenarija implementacije

1.1.2. Syslog server

Syslog server se koristi za prikupljanje poruka na centralnoj lokaciji. On može biti fizički server, viruelna mašina ili softverski bazirani server. Da bi se omogućilo primanje, pohrana i interpretiranje poruka, syslog server se sastoji od sljedećih komponeneti [3]:

- **Syslog Listener** - omogućava primanje poruka sakupljanjem syslog podataka
- **Database** - baza podataka, važna za velike mreže da bi se izvršila pohrana podataka
- **Management and filtering software** - softver za upravljanje i filtriranje se koristi za automatizaciju i jednostavno filtriranje specifičnih log-ova, te omogućava serveru da generiše alarme, notifikacije i upozorenja kao odgovor na neke poruke, kako bi obavijestio administratore o pojavi probelma.

Dakle, syslog server omogućava prikupljanje, prikaz i filtriranje syslog poruka na jednoj lokaciji, a poruke se prikupljaju sa svih uređaja te operativnih sistema. Pored toga, omogućava obavještavanje u slučaju problema te generisanje izvještaja kojima se može pratiti statistika sistema. Neke napredne funkcije syslog servera uključuju: filtriranje poruka prema prioritetu, vremenu, IP adresi ili imenu domaćina, bufferovanje poruka, u svrhu izbjegavanja preopterećenja sistema, arhiviranje podataka da bi udovoljio zakonima HIPAA, SOX i dr [4].

1.1.3. Syslog poruka

Veličina syslog poruke mora da bude 1024B ili manja, pri čemu ne postoji ograničenje na minimalnu dužinu poruke, s tim da se prazne syslog poruke ne bi trebale prenositi.
Syslog poruka (engl. *Syslog message*) sastoji se od tri dijela, a koja su objašnjena u nastavku [1], [5].

1. PRI

PRI dio poruke mora imati tri, četiri ili pet karaktera, pri čemu su prvi i zadnji karakter ugaone zadrade ("<", ">"). Dakle, PRI dio poruke počinje sa "<", nakon čega slijedi broj, te završava sa znakom ">". Interpretira se kao 7-bitna ASCII vrijednost u 8-bitnom polju. Broj koji se nalazi između zagrada je poznat kao Prioritetna vrijednost (engl. *Priority value*) te predstavlja *Facility* i *Severity*. Vrijednosti su prikazane u tabelama 1.1 i 1.2. PRI vrijednost (engl. *Priority value*) se računa kao:

$$PRI = (Facility\_vrijednost * 8) + Severity\_vrijednost$$

2. HEADER

Zaglavlje poruke je, kao i kod PRI vrijednosti, 7-bitna ASCII vrijednost u 8-bitnom polju. Zaglavlje sadrži *timestamp* i indikator IP adrese uređaja ili imena domaćina (engl. *hostname*). Nakon završetka PRI polja, odmah slijedi *timestamp* zaglavlja poruke, a nakon svakog *timestamp* i *hostname* polja mora uslijediti razmak (engl. *space*).

Tablica 1.1: Facilities syslog poruke

Numerical Code	**Facility**
0	Kernel message
1	User-level message
2	Mail system
3	System daemons
4	Security/authorization messages
5	Messages generated internally by syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Clock daemon
16 - 23	Local use 0 - Local use 7

Tablica 1.2: Severities syslog poruke

Numerical Code	**Severity**
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Hostname polje sadrži ime uređaja, a ukoliko uređaj nema ime, polje sadrži njegovu IP adresu. *Timestamp* polje je lokalno vrijeme koje se piše u formatu "*Mmm dd hh:mm:ss*", pri čemu: *Mmm* i *dd* predstavlja mjesec i dan u godini, respektivno, a *Hh:mm:ss* lokalno vrijeme [5].

3. MESSAGE

Ostatak syslog paketa čini sama poruka. Najčešće se sastoji od teksta poruke te nekih dodatnih informacija o procesu koji je generisao tu poruku. Kao i u prethodnim slučajevima, kod je 7-bitni ASCII u 8-bitnom polju. Sastoji se od dva dijela: *Tag* i *Content*. *Content* dio poruke sadrži detalje same poruke i daje detaljne informacije o događaju. *Tag* je string ABNF (engl. *Augmented Backus-Naur Form*) alfanumeričkih karaktera koje ne smije premašiti 32 karaktera [5].

1.1.4. Nedostaci

Kod syslog-a se javlja problem sigurnosti jer ne uključuje mehanizam za autentifikaciju. Također, bog korištenja UDP transportnog protokola, postoji mogućnost gubitka syslog poruka. Postoji i problem nekonzistentnosti kada je riječ o formatiranju sadržaja syslog poruka. Navedeno dovodi do problema da su pojedine poruke važnije od drugih, zbog nečitljivosti istih (u smislu razumljivosti ljudima) [6].

1.2. Rsyslog

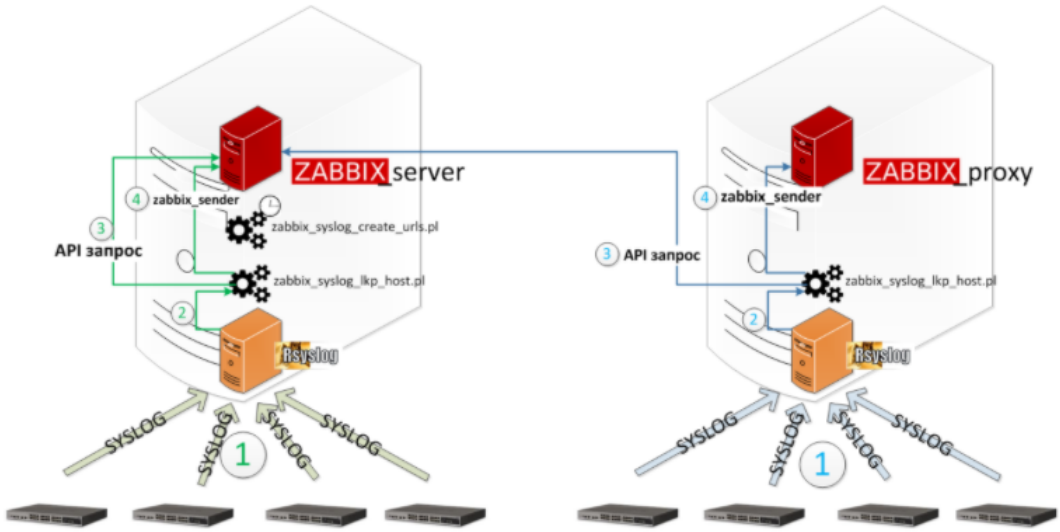
Rsyslog (engl. *Rocket-fast Syslog*) jeste raketno-brzi (engl. *rocket-fast*) sistem za procesiranje log-ova koji nudi visokre performanse, dobre sigurnosne funkcije i modularni dizajn. To je open source program za prenos log poruka preko IP mreže [7]. Rsyslog implementira jezgru Syslog protokola i proširuje je sljedećim mogućnostima:

- Filtriranje na bazi sadržaja,
- Napredne karakteristike filtriranja,
- Korištenje TCP, SSL, TLS, RELP za transport,
- Filtriranje bilo kojeg dijela syslog poruke,
- Fleksibilne konfiguracione opcije.

Rsyslog ima mogućnost dostavljanja preko milion poruka po sekundi lokalnim odredištima pri ograničenom precesiranju. Čak i ukoliko je riječ o udaljenim odredištima i složenijim procesiranjem, performanse Rsyslog-a se smatraju 'zadivljujućim' [8].

2. Postojeća rješenja

2.1. Zabbix Syslog rješenje koristeći rsyslog



Slika 2.1: Prikaz Zabbix Syslog rješenja [9]

Način realizacije navedenog rješenja:

1. Konfiguracija mrežnih uređaja da rutiraju sve syslog poruke do Zabbix servera i Zabbix proxy-ja koristeći rsyslog.

2. Rsyslog pokreće odgovarajuće skripte i određuje sa kojeg Zabbix-host-a dolazi poruka (koristeći Zabbix API).

3. Zabbix-sender protokol se koristi za spremanje poruka unutar samog Zabbix-a.

Osobine navedenog rješenja:

IP to host rješenja se keširaju da bi se minimizirao broj Zabbix API upita Zabbix pošiljatelj je ovdje u *perl* funkciji, tako da *cli* Zabbix-sender alat nije zahtijevan [9].

2.2. PIX Firewall Syslog Log

Korisne informacije o statusu mreže nalaze se u zapisnicima koje generišu *firewall-i*, međutim količina ovih podataka je jako velika što njihovu analizu čini izrazito teškom. Stoga je, na osnovu *Cisco PIX firewall*-a ovaj rad [10] prikupio zapise Sysloga koristeći tehniku spremišta niti, zatim je izvršio filtriranje i kategorizaciju zapisa ključnim riječima te konačno njihovu pohranu. Kroz TopN statističku analizu, istraživanje i otkrivanje sigurnosnih događaja na osnovu funkcije, on ostvaruje efikasno nadgledanje mrežnog saobraćaja, uslugu aplikacija, ponašanje korisnika i status pokretanja. Također, pruža osnovu za upravljanje mrežom i dizajn sigurnosne strategije za administratora, čime jača dalje upravljanje mrežom. *Firewall* je odbrambeni sistem koji je izoliran između lokalne i vanjske mreže i smatra se skupom preventivnih mjera te uključuje *software* i *hardware*. Na tržištu je *hardware firewall* vrlo raznolik, kao što su *Cisco PIX, Juniper Netscreen, SONICWALL, H3C, WatchGuard, FortiGate, 3Com* itd. *Cisco PIX firewall* preuzima Syslog. Na postojeći problem nadzora trenutne mreže, u ovom radu je implementiran sistem za analizu *log PIX firewall*-a. Sistem je prikupio i prethodno obrađivao Syslog logove koji su generirani *PIX firewall*-om, a zatim su vršili statističku analizu TopN i otkrivali sigurnosne događaje, te izvodili druge relativne operacije, kako bi se ostvario učinkovit nadzor mrežnog saobraćaja, aplikacijske usluge, ponašanja korisnika i mreže sigurnosti, tako da administrator može znati status mreže u stvarnom vremenu, ako postoji neadekvatan događaj u mreži, administrator ga može odmah obraditi kako bi efikasno poboljšao sigurnosne performanse mreže. Međutim, na osnovu konstrukcije sistema, on se također mora poboljšati u nekim aspektima. Među njima postoje dvije tačke [10]:

1. Statističke analize: Trenutno je često prihvaćena metoda opća statistika. Što se tiče obrade masovnih podataka, potrebno je dalje proučavati kako povećati njegovu efikasnost i tačnost.

2. Ispitivanje sigurnosnog događaja: Trenutno je metoda koju je sistem usvojio jednostavna i uredno se podudara sa zapisom i karakteristikom za ispitivanje sigurnosnog događaja, a njegova tačnost treba da se poboljša. Možemo koristiti neke matematičke modele, na primjer, zasnovane na modelu vremenskih serija; također možemo koristiti metodu prikupljanja podataka za ispitivanje sigurnosnog događaja.

2.3. A Prioritized Retransmission Mechanism for Reliable and Efficient Delivery of Syslog Messages

U ovom radu je raspravljano o problemima u mrežnim sistemima za prijavu i predložen je mehanizam za postizanje pouzdanosti i efikasnosti ovih sistema. Budući da Syslog protokol, koji se široko koristi za evidentiranje mreže, ne može pružiti pouzdanost, novi syslog protokol je standardiziran na IETF-u. Upotreba TCP-a smatra se obećavajućim pristupom za pouzdanu isporuku Syslog poruka. TCP ne može garantovati pouzdanost nakon prekida veze, a kontrola prijenosa TCP negativno utiče na pravovremenost važnih poruka. Tada su predloženi prioritetni mehanizmi ponovnog slanja za pouzdanu i efikasnu isporuku syslog poruka. Pretpostavljamo da predloženi mehanizmi djeluju na aplikacijskom sloju, a UDP je temeljni transportni protokol. Predložena metoda dijeli Syslog poruke u dvije grupe: važne i normalne. Razlikuje mehanizam ponovnog slanja dvije vrste poruka. Nastavljajući s tim, predloženi metod može pružiti pouzdanost za obje vrste poruka i pravovremenost za važne poruke. Simulacijama NS-2 pokazano je da je predložena metoda efikasnija od TCP-a u pružanju pouzdane isporuke Syslog poruka [11].

Zaključak

Syslog predstavlja moćan alat koji administratorima olakšava upravljanje kompleksnim mrežama. Velika prednost ovog alata je dostupnost na Unix i Linux operativnim sistemima,a može ga podržati i Windows. Syslog server na kojeg se prikupljaju podaci mora biti dostupan kosrisnicima u svakom trenutku. Prilikom razmatranja projektnog zadatka, osim prednosti Sysloga, uočeni su i neki njegovi nedostatci, pa tako za povećanje sigurnosti komunikacije bi se mogao koristiti TCP protokol umjesto implementiranog UDP-a. Ukoliko uređaj nije spreman da primi podatke oni su trajno izgubljeni, što predstavlja problem i prepreku u korištenju ovog protokola za prikupljanje povjerljivih informacija. Pri razvoju novih verzija ovog protokola svakako treba obratiti pažnju na ove stvari ukoliko njegovi kreatori žele poboljšati kvalitete samog protokola. Iako u literaturi nigdje nismo pronašli ništa vezano za čuvanje podataka ukoliko dođe do problema u radu servera, mišljenja smo da u sljedećim verzijama protokola treba obratiti pažnju i na ovaj detalj.

Jedan od najvećih izazova Syslog-a jeste obim podataka. Logging server mora biti u mogućnosti pojednostaviti upravljanje zapisima i pomoći administratorima da ih filtriraju i fokusiraju se na poruke koje su zaista bitne.

Sljedeći korak pri realizaciji projektnog zadatka je na postojećoj virtuelnoj mašini implementirati Zabbix dodatak za Syslog protokol, i prikupljanje podataka na server.

Popis slika

Popis tablica

Bibliografija

[1] Paessler, "IT Explained: Syslog," 2020. [Online]. Available: https://www.paessler.com/it-explained/syslog

[2] R. Gerhards, "The Syslog Protocol," RFC 5424, March 2009. [Online]. Available: https://www.hjp.at/doc/rfc/rfc5424.html

[3] A. Altvater, "Syslog Tutorial: How It Works, Examples, Best Practices, and More," 2017. [Online]. Available: https://stackify.com/syslog-101/

[4] DNSstuff, "What Is Syslog? Syslog Server vs. Event Log Explained + Recommended Syslog Management Tool," 2020. [Online]. Available: https://www.dnsstuff.com/what-is-syslog

[5] C. Lonvick, "The BSD Syslog Protocol," 2001. [Online]. Available: https://dl.acm.org/doi/pdf/10.17487/RFC3164

[6] sumo logic, "What is syslog?" [Online]. Available: https://www.sumologic.com/syslog/

[7] "Rsyslog." [Online]. Available: https://github.com/rsyslog/rsyslog

[8] rsyslog, "The rocket-fast Syslog Server." [Online]. Available: https://www.rsyslog.com/

[9] "Zabbix Syslog UDP using rsyslog." [Online]. Available: https://share.zabbix.com/cat-app/zabbix-syslog-udp-using-rsyslog

[10] N. W. Gu Zhaojun, Li Yong, "Analysis and implement of pix firewall syslog log." IEEE, 2010.

[11] K. O. Y. W. G. M. K. Y. N. Hiroshi Tsunoda, Takafumi Maruyama, "A prioritized retransmission mechanism for reliable and efficient delivery of syslog messages." IEEE, 209.

[12] M. Rajiullah, R. Lundin, A. Brunstrom, and S. Lindskog, "Syslog performance: Data modeling and transport," in *2011 Third International Workshop on Security and Communication Networks (IWSCN)*. IEEE, 2011, pp. 31–37.

[13] A. Leskiw, "Syslog: Servers, Messages Security – Tutorial Guide to this System Logs!" 2020. [Online]. Available: https://www.networkmanagementsoftware.com/what-is-syslog/