UNIVERZITET U SARAJEVU
**ELEKTROTEHNIČKI FAKULTET**
**ODSJEK ZA TELEKOMUNIKACIJE**

# Syslog - rsyslog (zabbix)

Projektni zadatak iz predmeta Upravljanje telekomunikacijskim mrežama

Praktični dio

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

Sarajevo, 2021. godina

# Sadržaj

# Uvod

U teorijskom dijelu projektnog zadatka detaljno je analiziran rad Syslog (engl. *System Logging Protocol*) alata za centralizirani monitoring mreže. Syslog je prije svega uveden zbog prikupljanja velike količine podataka koja dolazi sa uređaja različitih proizvođača, a koji služe za različite namjene. Pored toga, omogućeno je i slanje notifikacija i alarma u slučaju pojave problema, kako bi administratori imali bolji uvid u rad i ponašanje sistema.

Syslog 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. Dostupan je na Unix i Linux operativnim sistemima i mnogim web aplikacijama, uključujući Apache. Syslog je klijent server protokol koji koristi UDP na portu 514 bez mehanizma za provjeru spremnosti uređaja da primi podatke.

U ovom dijelu rada cilj je praktično pokazati rad syslog alata. Inicijalno je zamišljeno kombinovanje syslog i zabbix alata na način da se syslog logovi prosljeđuju u zabbix. Međutim, zbog problema sa prosljeđivanjem logova u zabbix, iako je na zabbix serveru odrađena adekvatna konfiguracija, implementirana su druga rješenja koja koriste alate za obradu velike količine podataka. U radu su pokazani rezultati dobiveni korištenjem *Splunk Enterprise* te *Splunk Forwarder*, koji su vršili sakupljenje i nadgledanje log zapisa. Također, pri izradi zadatka je korišten rsyslog (engl. *Rocket-fast Syslog*) koji predstavlja raketno-brzi sistem za procesiranje log-ova, a nudi visoke performanse, dobre sigurnosne funkcije i modularni dizajn.

Rad se sastoji iz jedinostvenog poglavlja koji je podijeljen na dva dijela. Prvi dio poglavlja predstavlja opis implementacije syslog alata, tačnije splunk syslog rješenja koristeći rsyslog. Drugi dio poglavlja daje pregled prikupljenih logova i statistika. U poglavlju su pobrojane i svi problemi i greške koje su javljenje prilikom implementacije. Na kraju rada izveden je zaključak, dat je popis slika i korištene literature.

# 1. Syslog implementacija

Kao inicijalno rješenje je bilo zamišljeno kombinovanje zabbix-a i syslog-a na način da se syslog logovi proslijeđuju direktno u zabbix. Međutim, korištene skripte dostupne na [1], nisu dale željene rezultate. Naime logovi sa nadgledanog OPNSense Firewall/Router-a koji se nalazi na adresi 192.168.1.40 su dolazili na syslog server koji se nalazi na adresi 192.168.1.115, međutim nije dolazilo do prosljeđivanja logova u zabbix iako je na zabbix serveru napravljena adekvatna konfiguracija. Također, iz još uvijek neutvrđenog razloga nije bilo moguće niti jednostavno nadgledanje log file-a koji se nalazi u $var/log/192.168.1.40/zabbix - syslog.log$.

Za rješenje koje podrazumijeva nadgledanje log file-a su korištene upute iz zabbix dokumentacije te je polje *key* konfigurisano kao lokacija log file-a na serveru, IP adresa kako klijenta, tako i servera, kombinacije UDP porta 514, te 10050, te su pokušane kombinacije u kojima je zabbix korišten kao zabbix trapper te zabbix agent. Sve navedene kombinacije su oprobane i za slučaj kada je korištena skripta trebala da preko agenta proslijedi podatke direktno u zabbix, s tom razlikom da je *key* morao biti postavljen na vrijednost "Log". Ograničavajuća okolnost je bila štura dokumentacija, te dosta kontradiktornih rješenja na koje smo nailazili (u određenim izvorima je trebalo na suprotne načine postavljati polje *key*, u odnosu na već pomenute). Također, nisu jasno naznačene ni postavke syslog konfiguracije na serveru, značenje određenih polja template-a.

Kroz naš primjer smo uvidjeli da čak i da onemogućimo logovanje kroz konfiguraciju u $etc/rsyslog.conf$, i dalje se neće pokretati skripta u $etc/rsyslog.d/zabbix - rsyslog.conf$, nego je bilo potrebno zamijeniti imena kao i lokacije navedenih skripti (pokušano je i pokretanje rsyslog servisa u *daemon* modu, te kroz debugging same konfiguracije nije utvrđen jasan problem).

Kako syslog u određenim situacijama može da generiše ogromnu količinu podataka, okrenuli smo se ka rješenju koje koristi alate za obradu velike količine podataka. Implementirani su Splunk Enterprise te Splunk Forwarder, koji su vršili sakupljanje i nadgledanje log zapisa, dostupnog u $var/log/192.168.1.40/forwarded - logs.log$. U nastavku ćemo detaljnije opisati postupak implementacije te dobijene rezultate.

## 1.1. Splunk Syslog rješenje koristeći rsyslog

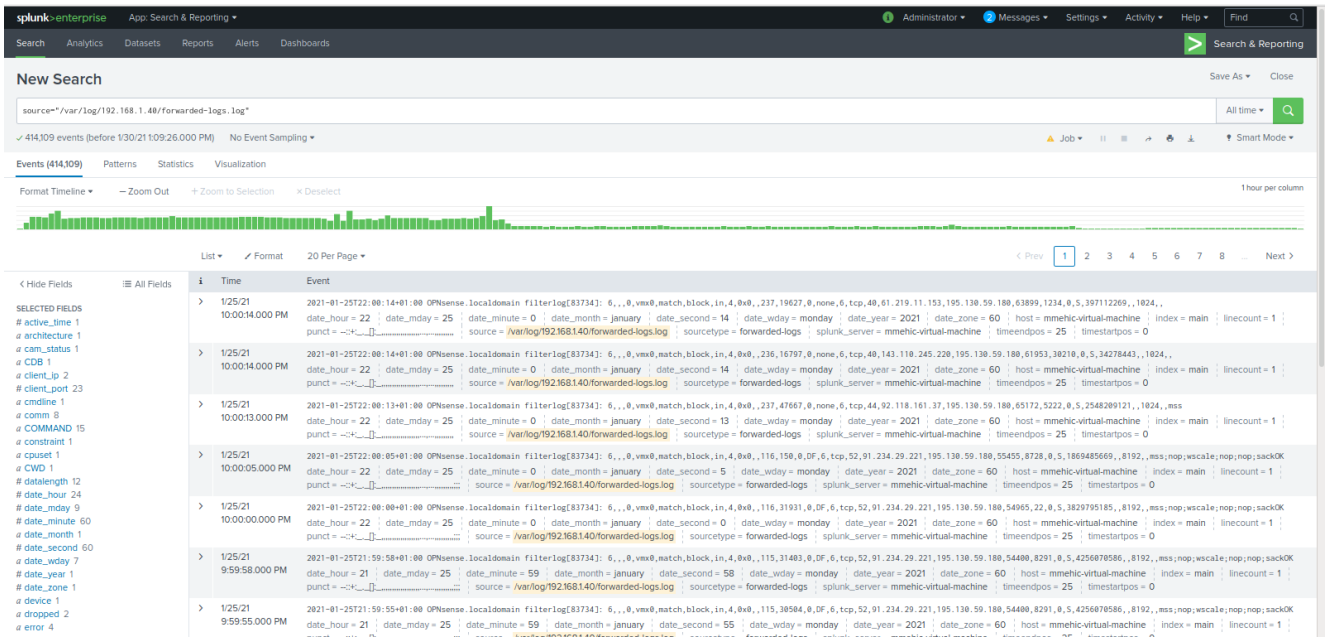
Splunk predstavlja softversko rješenje za pretragu, monitoring i analizu mašinski generisanih velikih setova podataka. Kao takav je izuzetno pogodan za kombiniranje sa syslog-om koji generište ogromnu količinu podataka. Kroz user-friendly web interface je

veoma jednostavno iz dostupnih podataka generisati razne statistike te ih prezentovati u željenom formatu. Takođe je moguće kreiranje "uzbuna", koje mogu mrežnom administratoru biti dojavljene putem maila u slučaju da se one dese. Također je korišten rsyslog, raketno-brzi syslog, koji je na Debian sistemima default i preinstaliran. Instalacija i konfiguracija je provedena na sljedeći način:

1. Modificiranje *rsyslog.conf* na način da dinamički kreira pomenuti file, te da na navedenu lokaciju sprema log zapise (detaljnije na [2]). Konfigurisanje klijenta (OPNSense Firewall/Router) da prosljeđuje log zapise na korišteni server [3]. Na transportnom sloju je korišten UDP.

2. Preuzimanje i instalacija Splunk Enterprise i Splunk forwardera [4], na Debian distribuciju (Linux Mint OS). Razlika u korištenoj implementaciji u odnosu na pomenutu jeste što nije vršena promjena dozvola i korisnika fileova ("sudo -u splunk splunk start –accept-license" i slične linije), kako ne bi došlo do sukoba da jedan korisnik (u našem slučaju root) instalira Splunk, a da drugi (Splunk) pokreće skriptu koja treba da prihvati licencu, omogući pokretanje pri boot-anju te sami monitoring željenog file-a. Prilikom inicijalnog pokretanja Forwardera može doći do sukoba portova (npr. 8089 koji je management port već korišten u Enterprise), te je potrebno odabrati drugi port (instalacija će se sama pobrinuti o modificiranoj konfiguraciji).

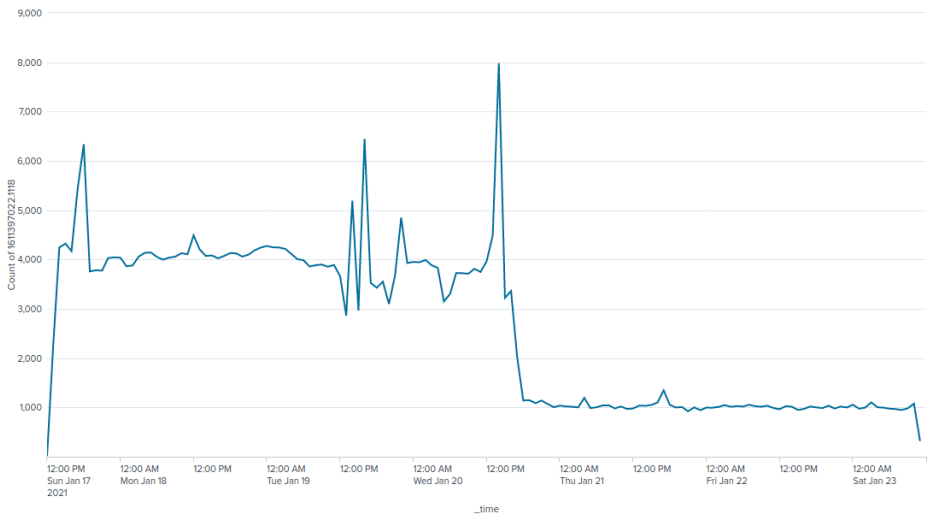
3. Forwarder je konfigurisan da nadgleda log file, koji putem porta 9997 prosljeđuje u Splunk Enterprise, te se korištenjem Web interface-a pristupa nadgledanim fileovima 1.1.




Slika 1.1: Splunk prikaz

## 1.2. Prikaz prikupljenih logova i statistika

Prvi pokazatelj stanja sistema i početna tačka jeste sam broj generisanih evenata od strane nadgledanog sistema. U kartici *Searches* je moguće odabrati vremenski period koji će se uzeti u razmatranje. U našem slučaju je to bilo 6 dana, to jeste od samog početka monitoringa. Na sljedećoj slici (slika 1.2) je prikazana raspodjela broja evenata po satima unutar navedenog perioda.

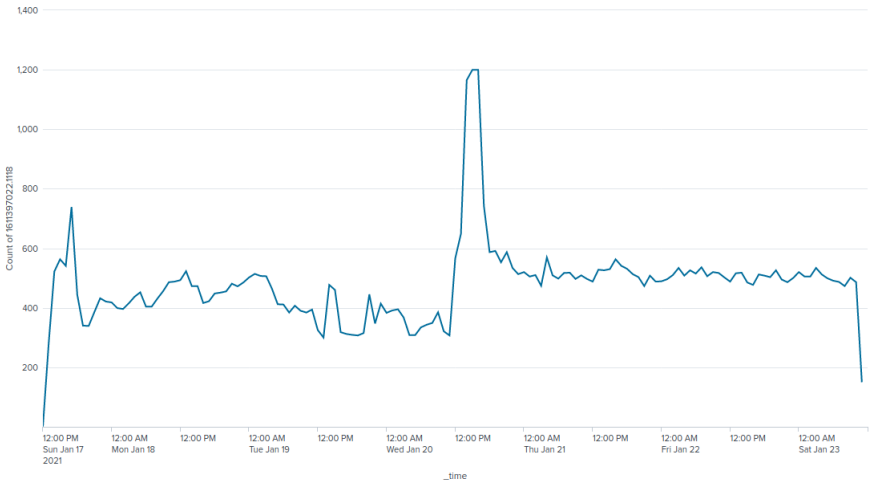



Slika 1.2: Raspodjela događaja

Navedena statistika je korisna iz razloga što (in)direktno ukazuje na potrošnju i upotrebu resursa, kao što su CPU i memorija. Također ukazuje na potencijalne probleme u slučaju kao što je prikazan na slici. Vidimo peak-ove u određenim vremenskim trenucima, što je, kasnije će se ispostaviti nakon ispitivanja log sadržaja, ukazivalo na određeni problem u našem sistemu. Splunk je faktički u mogućnosti da filteriše evente po identificiranom polju. Cilj je bio prije svega prepoznati koja su to polja koja se vežu za događaje određene greške. Tako smo dobili sljedeći prikaz.

| i | Time | Event |
|---|---|---|
| › | 1/19/21 1:59:59.000 PM | 2021-01-19T13:59:59+01:00 OPNsense.localdomain devd[91733]: message repeated 9 times: [ Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " '] host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |
| › | 1/19/21 1:59:32.000 PM | 2021-01-19T13:59:32+01:00 OPNsense.localdomain devd[91733]: Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " ' host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |
| › | 1/19/21 1:59:29.000 PM | 2021-01-19T13:59:29+01:00 OPNsense.localdomain devd[91733]: message repeated 6 times: [ Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " '] host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |
| › | 1/19/21 1:59:11.000 PM | 2021-01-19T13:59:11+01:00 OPNsense.localdomain devd[91733]: Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " ' host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |
| › | 1/19/21 1:59:08.000 PM | 2021-01-19T13:59:08+01:00 OPNsense.localdomain devd[91733]: message repeated 2 times: [ Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " '] host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |
| › | 1/19/21 1:59:02.000 PM | 2021-01-19T13:59:02+01:00 OPNsense.localdomain devd[91733]: Processing event '!system=CAM subsystem=periph type=error device=cd0 serial="00000000000000000001" cam_status="0xcc" scsi_status=2 scsi_sense="70 02 3a 00" CDB="00 00 00 00 00 00 " ' host = mmehic-virtual-machine source = /var/log/192.168.1.40/forwarded-logs.log sourcetype = forwarded-logs |

Slika 1.3: Konstantno prisutna greška

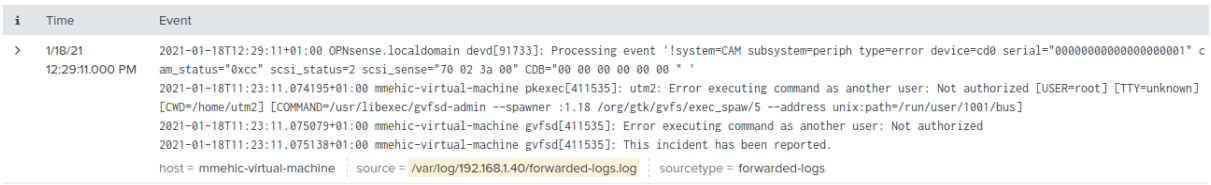



Slika 1.4: Raspodjela CDB događaja

Nakon očiglednog prepoznavanja polja *error* preko kojeg je bilo moguće filtrirati događaje, došli smo do polja CDB (*command descriptor block*), koje je skupa statusnim kodom "scsi status=2" (*check condition*), tipom poruke error, te "scsi sense" porukom, ukazivala na neočekivanu SCSI komandu. Naime, navedena kombinacija polja je ukazivala na neispravnost određene konfiguracije te nemogućnost pisanja na određenu lokaciju. Raspodjela CBD događaja je prikazana na slici 1.4.

Naime, istovremeno sa prikupljanjem logova na već opisani način, tekli su konstantni pokušaji implementacije i integracije zabbix-a i syslog-a, te je problem uzrokovalo podešavanje te razne konfiguracije kako klijenta, tako i servera. Praktično smo kroz logove mogli vidjeti našu aktivnost i pokušaje te način na koji je sve navedeno uticalo na rad samog sistema.

Dodatni sistemski događaji koji su se javljali jesu neautorizovan pristup izvršavanju određenih komandi kao što je prikazano na slici 1.5.



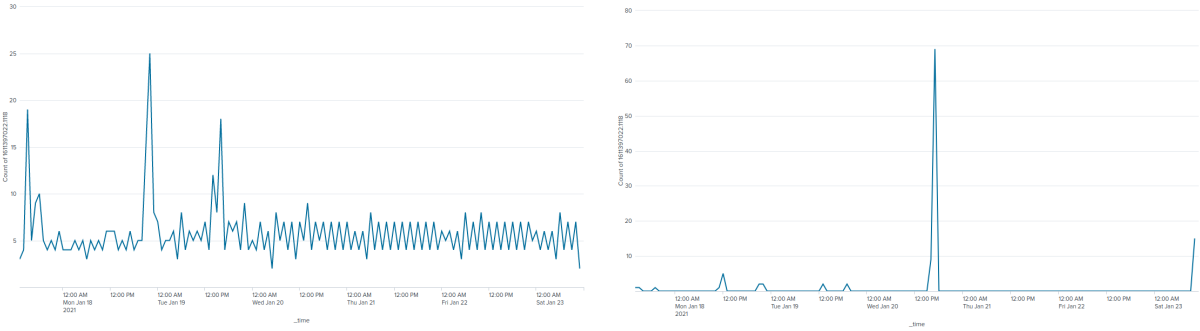

Slika 1.5: Neautorizovan pristup

Jedna od značajki korištenog rješenja jeste *Quick Report* koji omogućava sumiranje događaja od interesa, te njihovo razvrstavanje. Kroz navedenu funkcionalnost nam je bilo omogućeno da direktno filtriramo logove te napravimo izvještaj za događaje od interesa. Jedan od tih događaja jesu nesistemske greške a koje je generisao sam klijent. Navedene greške generisane *Quick Report*-om su date na slici 1.6.

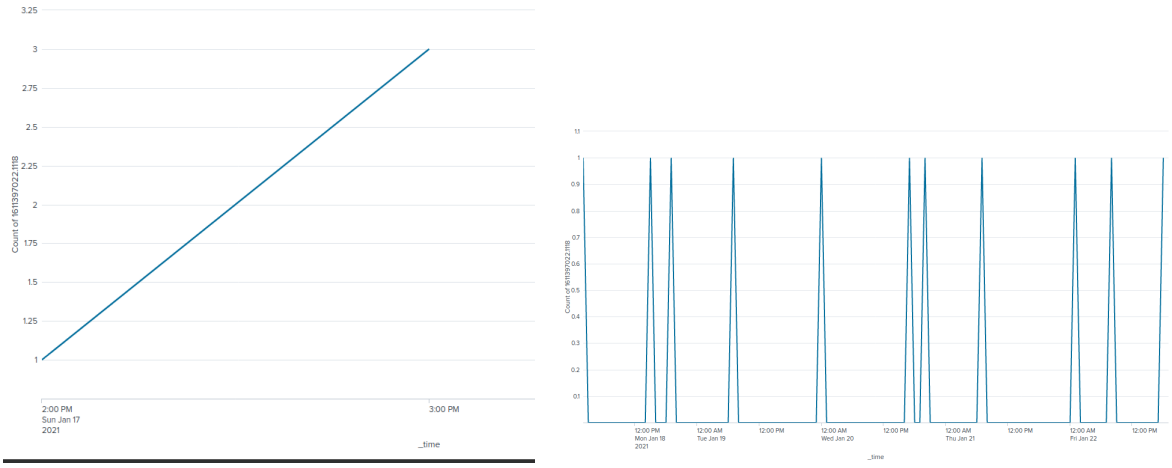
Kao što možemo vidjeti jedna od grešaka jeste 'Connection reset by peer' koja predstavlja situaciju kada jedna strana pošalje TCP paket drugoj strani, pri čemu druga strana ne prepoznaje TCP konekciju. Na ovaj način konekcije se instantno prekida umjesto standardnog *handshake*-a. Druga greška predstavlja nedostupnu mrežu, koja označava nemogućnost proslijeđivanja na željenu adresu.


Slika 1.6: Nesistemske greške

Sposobnost Splunka da izdvoji svako polje zasebno, i generiše izvještaj samo za to polje otvara nevjerovatne mogućnosti. Tu dolazimo do polja kao što su *timeendpos* i *timestartpos*. Kroz njih je moguće nadgledati da li sistem nailazi na određene probleme sa timestamping-om. Splunk kroz navedena polja određuje koliko traje timestamp unutar određenog eventa. Također, moguće je nadgledati koji korisnici su i koliko često pristupali sistemu. Kroz pomenuti pristup se u slučaju da imamo grupe korisnika u sistemu (npr. Syslog, Splunk, Root itd), možemo uvidjeti i koja aplikacija koliko koristi sistem, kao i ko od korisnika vrši izmjene na sistemu. Raspodjela evenata po korisnicima je data na slikama 1.7 i 1.8 (UID0 predstavlja root korisnika).



Slika 1.7: a) UID 0 (lijevo); b) UID 1001 (desno)

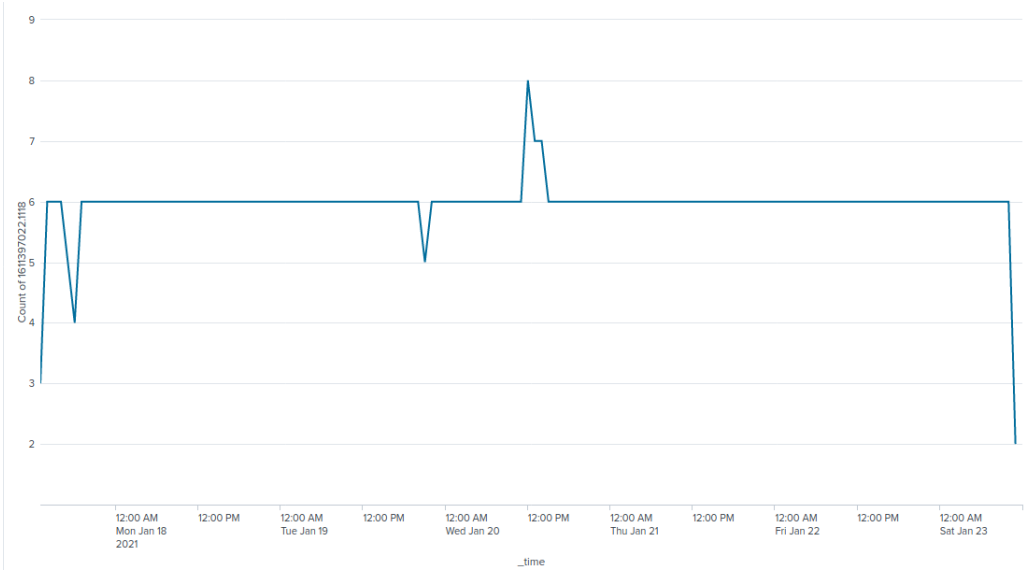


Slika 1.8: a) UID 1002 (lijevo); b) UID 62803 (desno)

Svakako neki od zanimljivih događaja jesu i broj odbačenih paketa, kao i broj paketa u redu čekanja. Primjer obrade paketa, specifičnosti vezane za spremanje u red čekanja i slično (u ovom specifičnom slučaju je to paket upravo namijenjen syslog serveru) je dat na slici 1.9.


Slika 1.9: Prikaz događaja obrade paketa

Pomenuto je izuzetno korisno za monitoring performansi samog sistema. Moguće je vršiti određene strategije implementacije redova čekanja, načina odbacivanja paketa i slično, ukoliko korelacijom dužine reda čekanja i broja odbačenih paketa utvrdimo da je moguće optimizirati sistem u skladu sa zahtjevima. Prikaz raspodjele broja odbačenih paketa je dat na slici 1.10.




Slika 1.10: Broj odbačenih paketa

# 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. Prilikom razmatranja projektnog zadatka, osim prednosti syslog-a, 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.

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. Stoga se Splunk nameće kao idealno rješenje iz razloga što omogućava kako adekvatno filtriranje, tako i spremanje, obradu i prikaz velike količine podataka u *user-friendly* formatu. Kroz web interface je moguće izvlačiti statistiku svakog polja zasebno, kao i nadgledati i uočavati promjene u radu sistema te izolirati slučajeve od interesa. Kombinacija *Big Data* alata i rsyslog-a se pokazala kao izuzetno prihvatljiva, primjenjiva i pogodna, pogotovo za neiskusne mrežne administratore koji možda i nemaju ideju kako pristupiti ovom problemu, te nisu upoznati sa time šta da očekuju od uređaja koje nadgledaju.

Zabbix kao rješenje ima svoje prednosti i mane, međutim inicijalno nije zamišljen kao skladište velike količine log podataka, te se u situacijama kada je potrebno nadgledati ogroman broj uređaja i ne preporučuje. Također je potrebno ograničiti broj događaja koje prima od mrežnih uređaja te posmatrati i filtrirati samo događaje od interesa. Korištenjem Splunk-a, te primanjem svih zapisa (uz naravno njihovo arhiviranje i kompresovanje nakon izvjesnog vremena), moguće je pratiti cjelokupni rad sistema tokom njegovog životnog vijeka, te što je osobito pogodno za neiskusne administratore, dobiti širu sliku cjelokupnog procesa rada uređaja, te istražiti dublje način njegovog funkcionisanja.

# Popis slika

# Bibliografija

[1] “zabbix-syslog.” [Online]. Available: https://github.com/v-zhuravlev/zabbix-syslog

[2] D. Garn, “How to use rsyslog to create a Linux log aggregation server,” 2020. [Online]. Available: https://www.redhat.com/sysadmin/log-aggregation-rsyslog

[3] “OPNsense - Remote Syslog Configuration.” [Online]. Available: https://techexpert.tips/opnsense/opnsense-remote-syslog-configuration/

[4] “Install Splunk and Forwarder on Linux,” 2020. [Online]. Available: https://djangocas.dev/blog/install-splunk-and-forwarder/