Sistem za praćenje promena na fajl sistem Linux servera

Mentor: Prof. dr. Bratislav Predić

Student: Đorđe Cvetković

Zadatak rada:

Praćenje faj sitema, prikaz informacija, zastita veb servera

Alati za praćenje i obrade logova Audit, Filebeat, ELK stek

Implementacija sistema za praćenje promena na fajl sistem Linux servera

Značaj praćenja fajl sistema

Porast konfiguracionih fajlova

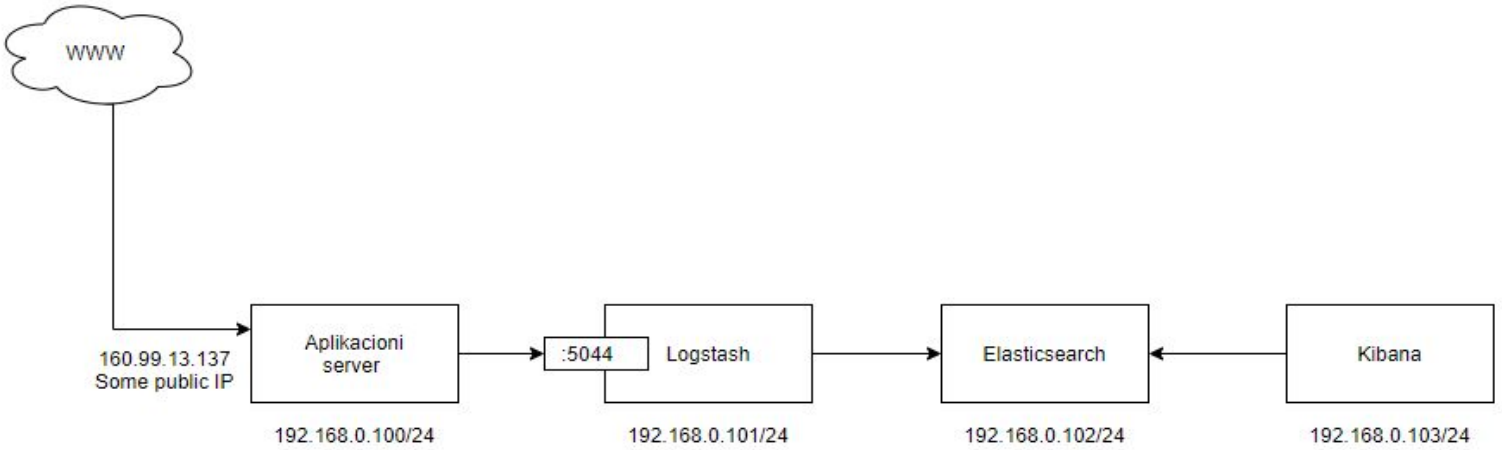
Povećane aktivnosti na serveru

Prevencija otkaza sistema

Prepoznavanje nelegalnog korišćenja

Prepoznavanje napada na sistem

Arhitektura implementiranog sistema



Audit

Prati i evidentira doagađaje na serveru

Set pravila određuje koje događaje prati

Pravila mogu biti: Kontrolna pravila

Pravila nadgledanja direktorijuma

Pravila sistemskih poziva

Podatke o događaju smesta u *audit.log* fajlu

Audit

Pravila:

-w /var/www/ -p rwxa -k aplication_directorium

Audit log

type=SYSCALL msg=audit(1648776363.437:328): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c

a1=7ffd6c661768 a2=941 ... ppid=1170 pid=1743 ... uid=1000 gid=1000 ... sgid=1000 fsgid=1000 tty=pts1 ses=3 comm="touch" exe="/usr/bin/touch"

key="aplication_directory"

Filebeat

Prosleđivanje i centralizacija logova

Prikuplja logove *acces.log*, *error.log* i *audit.log*

Održava poziciju čitanja podataka

Dodaje polje koje označava tip loga i sa kog je servera

Prikupljene logove šalje ka Logstash serveru

Filebeat konfiguracija

```
filebeat.inputs
        enabled: true
        paths:
                - /var/log/audit/audit.log
        fields:
                datatype: audit
                source: cs_elfak_ni_ac_rs
```

```
output.logstash:
        hosts: ["192.168.0.101:5044"]
```

Logstash

Prikupljanje, obrada i slanje podataka

Novi server za Logstash (Ubuntu 20.1)

Tri faze obrade i konfiguracije: ulaz -> filter -> izlaz

Konfiguracija regularnog izraza koji izdvaja polja iz logova

Obrada nestruktuiranog teksta

Konfiguracija ulaza

```
input {
  beats {
    port => 5044
    include_codec_tag => false
  }
}
```

Konfiguracija filtera

Primer regularnog izraza za izvlačenje podataka iz loga

```
filter {
        grok {
            match => [ "message", "type=%{WORD:audit_type}
msg=audit\(%{NUMBER:audit_epoch}:%{NUMBER:audit_counter}\):%{GREEDYDATA:msg}" ]
        }
        grok {
            patterns_dir => "/etc/logstash/patterns"
            match => [
                "msg", "%{AUDITD_1}",
                "msg", "%{AUDITD_2}",
                "msg", "%{AUDITD_3}",
```

Konfiguracija filtera

Deo za izmenu i filtriranje polja

```
mutate {
  add_field => {"logstash_time" => "%{@timestamp}" }
  remove_field => [ "agent", "ref", "input@", "file", "eps" ]
}
"host", "log", "ident", "rawrequest", "tags" ]
```

Konfiguracija izlaza

Konfiguracija izlaza sa određenim *indexom*

```
output {
        elasticsearch {
                hosts => ["192.168.0.102:9200"]
                user => "elasticUser"
                password => "Password!!"
                index => "audit"
        }
}
```

Elasticsearch

Distribuirani sistem baze podataka

Vrši indeksiranje podataka

Pruža pretragu i analiziranje svih vrsta podataka

Radi u realnom vremenu

Kibana

Vizualizacija podataka

Kreiranje upita ka Elasticsearch-u

Struktuirani i nestruktuirani podaci