ДЗ-06: ELK

Настройка

<https://www.dmosk.ru/miniinstruktions.php?mini=rsyslog>

<https://www.8host.com/blog/centralizaciya-logov-s-pomoshhyu-rsyslog-logstash-i-elasticsearch-v-ubuntu-14-04/>

# Authentication credentials - either API key or username/password.

#api\_key: "id:api\_key"

username: "elastic"

password: "10DM27XoI52iiDxXZa78"

ssl.verification\_mode: none

nano modules.d/system.yml

**/etc/logstash/logstash.yml**

xpack.monitoring.enabled: true

xpack.monitoring.elasticsearch.url: http://X.X.X.X:9200

**/etc/rsyslog.conf**

# provides UDP syslog reception

module(load="imudp")

input(type="imudp" port="514")

# provides TCP syslog reception

module(load="imtcp")

input(type="imtcp" port="514")

**/etc/ssh/sshd\_config**

SyslogFacility AUTH

LogLevel INFO

### Конфиги

**/etc/rsyslog.d/rsyslog-json-template.conf –** форматирование в json для отправки в logstash

template(name="json-template"

type="list") {

constant(value="{")

constant(value="\"@timestamp\":\"") property(name="timereported" dateFormat="rfc3339")

constant(value="\",\"@version\":\"1")

constant(value="\",\"message\":\"") property(name="msg" format="json")

constant(value="\",\"sysloghost\":\"") property(name="hostname")

constant(value="\",\"severity\":\"") property(name="syslogseverity-text")

constant(value="\",\"facility\":\"") property(name="syslogfacility-text")

constant(value="\",\"programname\":\"") property(name="programname")

constant(value="\",\"procid\":\"") property(name="procid")

constant(value="\"}\n")

}

**/etc/rsyslog.d/rsyslog-sshd-output.conf –** отправка логов sshd в logstash

if $programname == 'sshd' then @127.0.0.1:10514;json-template

& ~

**/etc/logstash/conf.d/logstash-rsyslog.conf**

input {

udp {

host => "127.0.0.1"

port => 10514

codec => "json"

type => "rsyslog"

}

}

filter { }

output {

if [programname] == "sshd" {

elasticsearch {

index => "sshd-%{+YYYY.MM.dd}"

ssl => true

ssl\_certificate\_verification => false

user => "elastic"

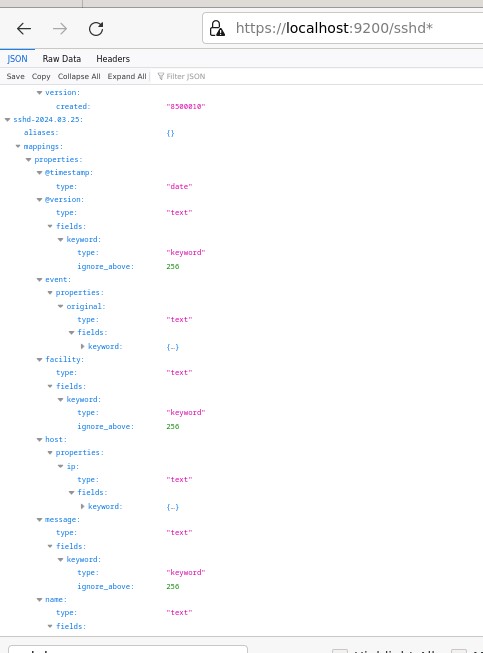
password => "10DM27XoI52iiDxXZa78"

}

}

}

Index



Kibana

