



kimssster 30 мар 2016 в 12:16

## Опять про IDS или ELK для suricata

4 мин 29К

Информационная безопасность\*, Open source\*

Привет, привет!

Сегодня хочу поделиться с вами опытом по настройке ELK и IDS Suricata. В инете много мануалов, но ни один из них не позволит «завезти» связку этих продуктов в текущих версиях. Также есть готовый дистрибутив SELKS — [www.stamus-networks.com/open-source/#selks](http://www.stamus-networks.com/open-source/#selks) или же, в качестве альтернативы, связка snort, snorby и barnyard2 в SecOnion — [blog.securityonion.net](http://blog.securityonion.net). Для остальных прошу под кат.

Итак, что нам надо:

Систему, которая будет наглядно отображать события с IDS, и чтобы это не был ArcSight, OSSIM, QRadar и т.п.

Для начала найдем что-нибудь из RHEL7 или CentOS7. Можно и Ubuntu LTS, что вам больше нравится для продакшена.

А также сами компоненты ELK и IDS.

Suricata — [suricata-ids.org](http://suricata-ids.org)

ElasticSearch — [www.elastic.co/products/elasticsearch](http://www.elastic.co/products/elasticsearch)

Logstash — [www.elastic.co/products/logstash](http://www.elastic.co/products/logstash)

Kibana — [www.elastic.co/products/kibana](http://www.elastic.co/products/kibana)

Ну и дунуть, чтобы получилось чудо... В смысле, думать!

### IDS

Для начала доустановим необходимые компоненты (java, json):

```
yum -y install java-1.8.0-openjdk-devel.x86_64
yum -y install gcc libpcap-devel pcre-devel libyaml-devel file-devel  zlib-devel jansson-dev
```

Скачиваем и устанавливаем ids suricata:

```
wget http://www.openinfosecfoundation.org/download/suricata-3.0.tar.gz
tar -xvzf suricata-3.0.tar.gz
cd suricata-3.0
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lu
```

Далее



```
make; sudo make install; sudo ldconfig
```

Или следующие команды для автоматического конфигурирования: `make install-conf; make install-rules`

`make install-full` —если вам не нужно что-то тонко настраивать, рекомендую использовать данную команду. Автоматически будут созданы переменные, папки и правила докачаются соответственно в директорию `/rules`

При автоматической установке нужная нам директория с логами будет располагаться в:

```
@srv-ids ~]# cd /var/log/suricata/
```

Здесь будут файлы: `eve.json fast.log http.log stats.log`. Но не все файлы одинаково полезны. Нам нужен тот у которого хвост `json`

Теперь необходимо настроить IDS. Мы остановимся только на том, чтобы alerts попадали в `json` файл. Идем в `/etc/suricata/suricata.yaml` и находим там блок вывода логов или alerts. Для вывода в `json` нужен такой конфиг:

```
- eve-log:
  enabled: yes
  filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
  filename: eve.json
```

Остальной конфиг на ваше усмотрение. Благо там есть над чем задуматься.

## ELK

Далее `elasticsearch`:

Проверяем что там с `java`:

```
java -version
echo $JAVA_HOME
```

Если все ок, продолжаем (иначе, в начало заметки).

Скачиваем и устанавливаем `elasticsearch`:

```
wget https://download.elasticsearch.org/elasticsearch/release/org/elasticsearch/distribution/
sudo rpm -Uvh ./elasticsearch-2.2.1.rpm
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service
sudo systemctl status elasticsearch.service
```

Status —OK? Поехали за Logstash



```
wget https://download.elastic.co/logstash/logstash/packages/centos/logstash-2.2.2-1.noarch.rpm
sudo rpm -Uvh ./logstash-2.2.2-1.noarch.rpm
```

Тверь нужно его настроить, идем в /etc/logstash/conf.d/

Вот так выглядит рабочий конфиг logstash для текущих версий компонентов ПО:

```
input {
  file {
    path => ["/var/log/suricata/eve.json"]
    #sincedb_path => ["/var/lib/logstash/"]
    codec => json
    type => "SuricataIDPS-logs"
    start_position => "beginning"
  }
}
filter {
  if [type] == "SuricataIDPS-logs" {
    date {
      match => [ "timestamp", "ISO8601" ]
    }
  }
  ruby {
    code => "if event['event_type'] == 'fileinfo'; event['fileinfo']['type']=event['fileinfo']['type'];"
  }
  if [src_ip] {
    geoip {
      source => "src_ip"
      target => "geoip"
      #database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat"
      add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
      add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
    }
    mutate {
      convert => [ "[geoip][coordinates]", "float" ]
    }
  }
}
output {
  elasticsearch { hosts => ["localhost:9200"] }
  #stdout { codec => rubydebug }
}
```

Сохраняем, проверяем конфигурацию:

```
@srv-ids ~]# service logstash configtest
Configuration OK
```



Напоследок устанавливаем web-лицо нашей системы IDS — Kibana4.

```
wget https://download.elastic.co/kibana/kibana/kibana-4.4.2-linux-x64.tar.gz
```

Распаковываем в папку, например так: /opt/kibana4/ или /var/www/html/. В директории /opt/kibana4/bin/ запускаем веб-интерфейс. Можно сделать службу, как — описано здесь [discuss.elastic.co/t/run-kibana-as-service-on-centos/23971/2](https://discuss.elastic.co/t/run-kibana-as-service-on-centos/23971/2). Я не делал.

Бывает, что при запуске kibana появляется ошибка «kibana is still indexing», это можно увидеть в консоли или на вэбке в дашборде «Status». Для устранения ошибки делаем следующие команды с проверкой успешности:

```
curl -XDELETE http://localhost:9200/.kibana
curl -XDELETE http://localhost:9200/*
```

Теперь нам нужны индексы. Идем сюда [github.com/StamusNetworks/KTS](https://github.com/StamusNetworks/KTS). Здесь мы найдем уже подготовленные индексы и дашборды.

```
git clone https://github.com/StamusNetworks/KTS.git
patch -p1 -d /opt/kibana4/ < /opt/kibana4/KTS/patches/kibana-integer.patch
patch -p1 -d /opt/kibana4/ < /opt/kibana4/KTS/patches/timelion-integer.patch
./load.sh
```

**Go, go, go!**

Для запуска движка IDS вводим:

```
@srv-ids ~]# /usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth0
```

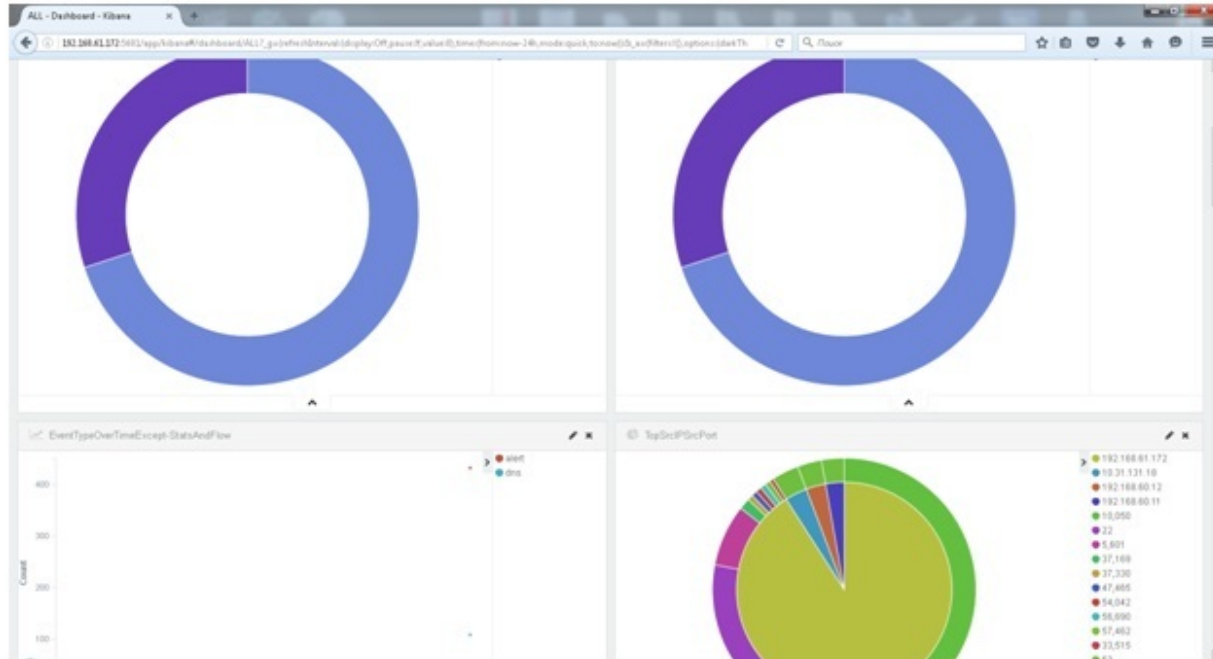
Обратите внимание на название интерфейса и режим его работы. Для пассивного анализа, необходимо перевести интерфейс в режим promisc и SPAN сессией тоже лучше обзавестись:

```
@srv-ids ~]# ifconfig eth0 promisc
```

После запуска IDS, размер лог-файлов должен существенно увеличиваться.

Если критичных ошибок при старте не было, заходим на 5601 порт. Выбираем индексы logstash-\*, идем в Dashboards и создаем интерфейс отображения под себя. Может получиться что-нибудь похожее на это:

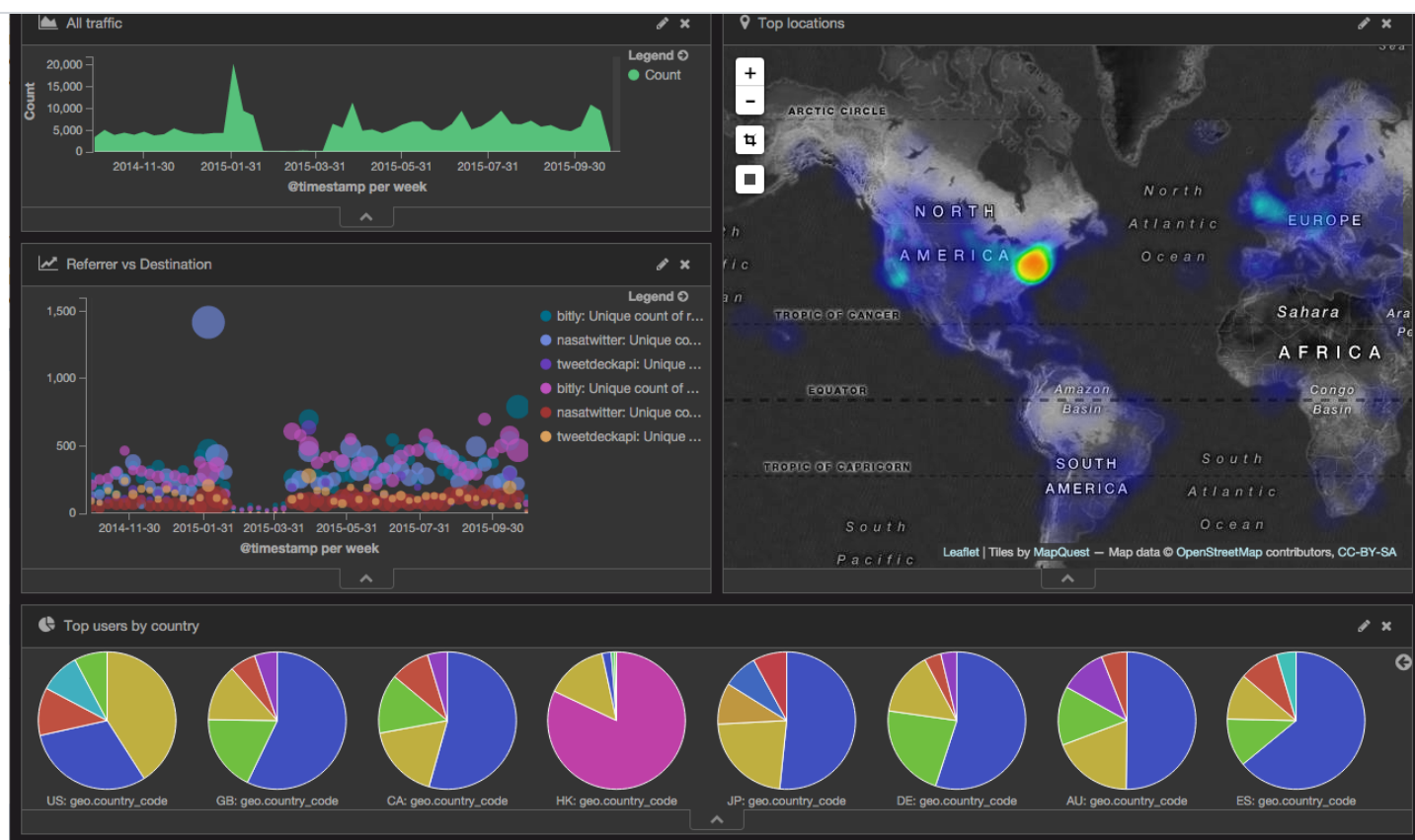




Или на это (скрин не мой):



Моя лента Все потоки Разработка Администрирование Дизайн Менеджмент Маркетинг Научпоп  Войти



Для того чтобы смотреть на карту, нужно раскомментировать в конфиге logstash эту строку:

#database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat" и скачать собственно указанный или аналогичный файл с геолокацией по IP.

Да еще не забудьте про Log rotation.

В /etc/logrotate.d/ создаем файл suricata со следующим содержанием:

```
/var/log/suricata/*.log /var/log/suricata/*.json
{
    rotate 3
    missingok
    nocompress
    create
```



```
sharedscripts
postrotate
    /bin/kill -HUP $(cat /var/run/suricata.pid)
endscript
}
```

Буду рад вашим комментариям.

Если будете пробовать и не заведется ELK или suricata, пишите, может что и выйдет=)

**Теги:** elk, suricata, ids, kibana

**Хабы:** Информационная безопасность, Open source

↑ +7 ↓

📖 51



💬 4 +4

## Редакторский дайджест



Присылаем лучшие статьи раз в месяц

Электронная почта



30

0

Карма

Рейтинг

**Герман @kimssster**

Пользователь

Подписаться



## Комментарии 4



👤 **nikerossxp** 30 мар 2016 в 12:37

Да, совместимость продуктов меня повергла в смятение. Пытался поднять ELK "родным" методом — репозиторий, установка, конфигурация — фигли, последние версии продуктов друг друга не видят! Нашел готовый SELKS, а там используются более старые пакеты :) Попробовал их же вручную — с полпинка завелись.

Где я свернул невтуды на последних версиях? Или это не баг, а фича?



Ответить



👤 **kimssster** 30 мар 2016 в 12:42




Это open source=), приходится читать про те малюсенькие изменения, которые делают разработчики, так сказать своеобразная плата за продукты.



Ответить



 **nikerossxp** 30 мар 2016 в 12:44 ^

да у того же logstash уже так просто порт на прослушку не откроешь :D А если откроешь, он не будет отдавать их в elasticsearch..

↑  ↓ Ответить  ...

 **porutchik** 29 июл 2017 в 22:10

Тверь => Теперь

↑  ↓ Ответить  ...

Зарегистрируйтесь на Хабре , чтобы оставить комментарий

## Публикации

ЛУЧШИЕ ЗА СУТКИ    ПОХОЖИЕ



**ntsaplin** 22 часа назад

### Десантируем арктический ЦОД и орбитального сисадмина на дрейфующую льдину

 6 мин     4.4K

 +57     24     29 +29



**DRoman0v** 21 час назад

### Самые неприятные поломки ноутбуков в моей практике. Чинить или не чинить — тот еще вопрос

 4 мин     8.7K

 +55     22     8 +8



**Lex98** 11 часов назад

### Rust — это не «memory safe C»

 Средний     25 мин     10K

Из песочницы

 +51     77     60 +60





timyrik20 23 часа назад

## Об одной изящной задаче



Простой



4 мин



7.8K



+30



45



35 +35



andrey\_nado 22 часа назад

## Нет у меня никакого первого имени



Простой



4 мин



7.8K

Мнение



+28



37



76 +76



leonik 22 часа назад

## Выращиваем тимлидов в домашних условиях



Простой



8 мин



3.4K

Мнение



+21



35



4 +4



roman-gorb 22 часа назад

## Ускорение инференса LLM



Средний



13 мин



2.2K



+20



33



1 +1



Parker0 23 часа назад

## Структура объекта в JavaScript движках



20 мин



2.3K



+20



52



0



markshevchenko вчера в 10:09

## 1. Почему вам стоит попробовать Nix (Nix в пилюлях)



Средний



6 мин



5.4K

Тutorial

Перевод



+19



28



6 +6







Kilor 19 часов назад

## Курс «PostgreSQL для начинающих»: #4 — Анализ запросов (ч.1 — как и зачем читать планы)

Средний

16 мин

5.4K

Тutorial

+17

140

0

## Как исправить раздвоение встреч в конференциях на базе Jitsi: опыт команды Телемоста

Интересно

Показать еще

### МИНУТОЧКУ ВНИМАНИЯ



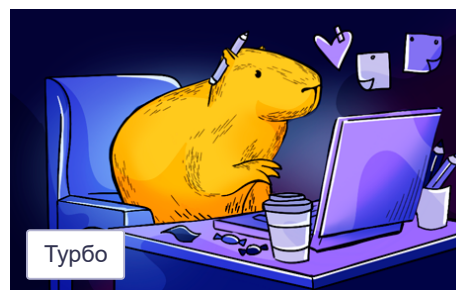
Интересно

IT-события, которые ты ищешь, тоже ищут тебя



Турбо

Как бессонница в час ночной, меняет промокодище облик твой



Турбо

Tinkoff CTF 2024: готовимся к соревнованию по хакингу

### ЗАКАЗЫ

Scada Alpha platforma

2000 руб./в час · 1 отклик · 10 просмотров

Написать 2 sql запроса на 2 простые таблички с json полем

1000 руб./за проект · 6 откликов · 38 просмотров

Соединить Revenuecat и Appsflyer Firebase

10000 руб./за проект · 1 отклик · 15 просмотров

Сверстать 2 страницы на react

1000 руб./за проект · 7 откликов · 36 просмотров

Полный редизайн мобильного приложения с добавлением нового функционала

50000 руб./за проект · 5 откликов · 18 просмотров



## ЧИТАЮТ СЕЙЧАС

Признаки рака можно заметить за несколько лет до появления симптомов, утверждает новый исследовательский институт

363K 65 +65

Rust — это не «memory safe C»

10K 60 +60

Правда ли, что в Европе везде отсталые сервисы, медленные платежи и плохие онлайн-услуги?

111K 820 +820

Исследователи не смогли получить от ИИ-сервисов Midjourney и DALL-E от OpenAI картинку с чистым белым фоном

6K 29 +29

Amazon закрыла в США магазины Just Walk Out, где клиенты могли брать товары и выходить без прохода через кассу

2K 3 +3

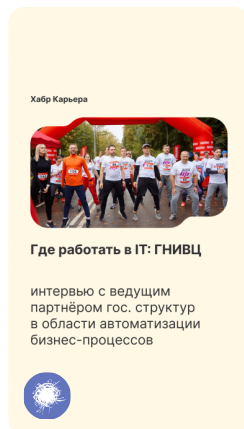
Как исправить раздвоение встреч в конференциях на базе Jitsi: опыт команды Телемоста

Интересно

## ИСТОРИИ



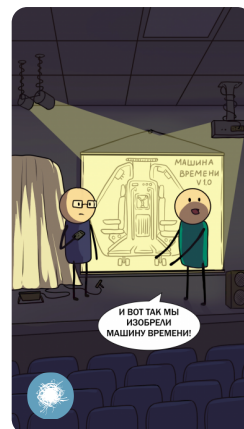
Погружение в мир LLM



Где работать в IT: ГНИВЦ



Полезные книги для библиотеки айтишника



Как продвинуть машину времени?



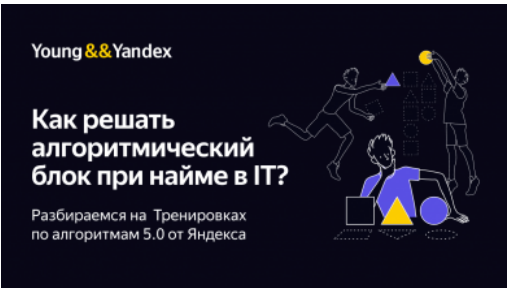
Перевернуть календарь и добавить событие



Специалист по информационной безопасности  
142 вакансии

Все вакансии

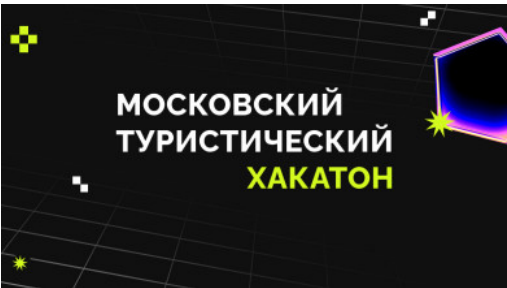
БЛИЖАЙШИЕ СОБЫТИЯ



Серия занятий «Тренировки по алгоритмам 5.0» от Яндекса

1 марта – 19 апреля  
19:00  
Онлайн

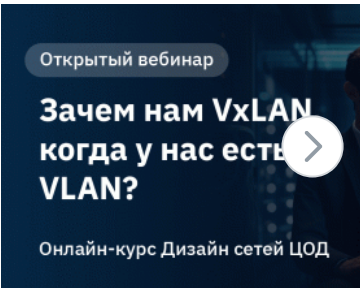
Подробнее в календаре



Московский туристический хакатон

23 марта – 7 апреля  
Москва • Онлайн

Подробнее в календаре



Вебинар «Зачем нам VxLAN, когда у нас есть VLAN?»

3 апреля 20:00  
Онлайн

Подробнее в календаре

Ваш аккаунт

Войти  
Регистрация

Разделы

Статьи  
Новости  
Хабы  
Компании  
Авторы  
Песочница

Информация

Устройство сайта  
Для авторов  
Для компаний  
Документы  
Соглашение  
Конфиденциальность

Услуги

Корпоративный блог  
Медийная реклама  
Нативные проекты  
Образовательные программы  
Стартапам



[Настройка языка](#)

[Техническая поддержка](#)

© 2006–2024, Habr

