

**МИНЦИФРЫ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Институт магистратуры

Кафедра Защищенных систем связи

Дисциплина: Технологии обеспечения информационной безопасности
больших данных

**ОТЧЕТ
ПО ПРАКТИЧЕСКОЙ РАБОТЕ 5**

Установка Falco, Falco -экспортера, Prometheus, Grafana и dashboard
(тема отчета)

Направление/специальность подготовки:

10.04.01 Информационная безопасность

(код и наименование направления/специальности)

Выполнил:

Коновалова В.В., ИКТБ -17м

(Ф.И.О., № группы)

(подпись)

Проверил:

Виткова Л.Н., ст. преп.

(Ф.И.О., должность)

(подпись)

Ход выполнения работы

1. Находим на сайте <https://falco.org/docs/getting-started/installation/> нужные нам команды для установки Falco. Затем вводим их в командной строке.

```
root@user-virtual-machine:/home/viktoria#
root@user-virtual-machine:/home/viktoria#
root@user-virtual-machine:/home/viktoria#
root@user-virtual-machine:/home/viktoria# curl -s https://falco.org/repo/falcosecurity-3672BA8F.asc | apt-key add -
OK
root@user-virtual-machine:/home/viktoria# echo "deb https://download.falco.org/packages/deb stable main" | tee -a /etc/apt/sources.l
ist.d/falcosecurity.list
deb https://download.falco.org/packages/deb stable main
root@user-virtual-machine:/home/viktoria# apt-get update -y
Суд:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Пон:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Пон:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Пон:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Пон:5 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1 393 kB]
Суд:6 https://download.docker.com/linux/ubuntu focal InRelease
Мир:7 https://download.falco.org/packages/deb stable InRelease
Пон:8 https://download.falco.org/packages/deb stable Release [1 908 B]
Пон:9 https://download.falco.org/packages/deb stable Release.gpg [833 B]
Пон:10 https://download.falco.org/packages/deb stable/main amd64 Packages [3 174 B]
Пон:11 http://ru.archive.ubuntu.com/ubuntu focal-updates/main 1386 Packages [572 kB]
Пон:12 http://security.ubuntu.com/ubuntu focal-security/main 1386 Packages [344 kB]
Пон:13 http://ru.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [282 kB]
Пон:14 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1 065 kB]
Пон:15 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [278 kB]
Пон:16 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [35,7 kB]
Пон:17 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [9 896 B]
Пон:18 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [606 kB]
Пон:19 http://security.ubuntu.com/ubuntu focal-security/universe 1386 Packages [523 kB]
Пон:20 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [112 kB]
Пон:21 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [64,7 kB]
Пон:22 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [12,9 kB]
Пон:23 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [2 464 B]
Пон:24 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [14,6 kB]
Пон:25 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [881 kB]
Пон:26 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe 1386 Packages [652 kB]
Пон:27 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [191 kB]
Пон:28 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [302 kB]
Пон:29 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [19,6 kB]
```

```
root@user-virtual-machine:/home/viktoria# apt-get -y install linux-headers-$(uname -r)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет linux-headers-5.11.0-38-generic самой новой версии (5.11.0-38.42-20.04.1).
linux-headers-5.11.0-38-generic помечен как установленный вручную.
Следующие пакеты устанавливались автоматически и больше не требуются:
  libfprint-2-tod1 libllvm9
Для их удаления используйте «sudo apt autoremove».
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 46 пакетов не обновлено.
root@user-virtual-machine:/home/viktoria#
root@user-virtual-machine:/home/viktoria# apt-get install -y falco
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libfprint-2-tod1 libllvm9
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential dctrl-tools dkms dpkg-dev fakeroot g++ g++-9 gcc gcc-9
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev
  libcrypt-dev libctf-nobfd0 libctf0 libfakeroot libgcc-9-dev libitm1 liblsan0 libquadmath0 libstdc++-9-dev libtsan0 libubsan1
  linux-libc-dev make manpages-dev
Предлагаемые пакеты:
  binutils-doc debtags menu debian-keyring g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf automake libtool flex bison
  gcc-doc gcc-9-multilib gcc-9-localles glibc-doc libstdc++-9-doc make-doc
Следующие НОВЫЕ пакеты будут установлены:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential dctrl-tools dkms dpkg-dev fakeroot falco g++ g++-9 gcc gcc-9
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils libc-dev-bin libc6-dev
  libcrypt-dev libctf-nobfd0 libctf0 libfakeroot libgcc-9-dev libitm1 liblsan0 libquadmath0 libstdc++-9-dev libtsan0 libubsan1
```

2. Затем, скачиваем файл falco_rules.yaml с репозитория https://github.com/falcosecurity/falco/blob/master/rules/falco_rules.yaml для того, чтобы добавить правила для обнаружения событий информационной безопасности. Добавляем файл в каталог /etc/falco. Или меняем старый файл из этого каталога, на новый, скаченный нами.

3. Изменим конфигурацию falco.yaml следующим образом:

```
# Whether to output events in json or text
json_output: true

syslog_output:
  enabled: true

http_output:
  enabled: true
  url: http://localhost:2801
```

Последний адрес необходим для будущей интеграции с Dashboard

4. Проверка работы Falco:

Запускаем falco:

```
root@user-virtual-machine:/etc/falco#
root@user-virtual-machine:/etc/falco#
root@user-virtual-machine:/etc/falco#
root@user-virtual-machine:/etc/falco#
root@user-virtual-machine:/etc/falco# falco
Tue Dec 14 19:22:26 2021: Falco version 0.30.0 (driver version 3aa7a83bf7b9e6229a3824e3fd1f4452d1e95cb4)
Tue Dec 14 19:22:26 2021: Falco initialized with configuration file /etc/falco/falco.yaml
Tue Dec 14 19:22:26 2021: Loading rules from file /etc/falco/falco_rules.yaml:
Tue Dec 14 19:22:26 2021: Loading rules from file /etc/falco/k8s_audit_rules.yaml:
```

Запускаем docker-compose:

```
viktor@user-virtual-machine:~/docker$
viktor@user-virtual-machine:~/docker$ sudo docker-compose up -d
Creating network "docker_app-network" with the default driver
Creating volume "docker_greafana-storage" with local driver
WARNING: Found orphan containers (docker_web_1, redisdb, docker_redis_1) for this project. If you removed or renamed this service in your compose file, you can run this command with the --remove-orphans flag to clean it up.
Pulling node_exporter (quay.io/prometheus/node-exporter:latest)...
a27a809b84c: Pull complete
b45d31e027f: Pull complete
b5db1e299295: Pull complete
Digest: sha256:f2268e731240d0f60a7d19a2ce1204d1308a955e0b0e00b9d081e478592cd
Status: Downloaded newer image for quay.io/prometheus/node-exporter:latest
Pulling prometheus (prom/prometheus:latest)...
latest: Pulling from prom/prometheus
30b53b0a8a2: Pull complete
c4d1a94ab1d1: Pull complete
41c8079f1eb7: Pull complete
100be10c01f3: Downloading [=====] 20.43MB/34.0MB
44af030a0a67: Download complete
101005400520: Download complete
e70892487524: Download complete
920f29a8210e: Download complete
```

Получаем результат:

```
root@user-virtual-machine: /
viktor@user-virtual-machine: ~/docker
[{"output": "19:33:37.129829108: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.129829108\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617129829108\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.159801422: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.159801422\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617159801422\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.190958334: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.190958334\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617190958334\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.221901508: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.221901508\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617221901508\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.253207644: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.253207644\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617253207644\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.284835158: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.284835158\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617284835158\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
[\"output\": \"19:33:37.314933749: Error File below / or /root opened for writing (user=root user.loginid=1801 command=falco parent=bash file=/e
vents.txt program=falco container_id=host image=nginx), \"priority\": \"Error\", \"rule\": \"Write below root\", \"source\": \"syscall\", \"tags\": [\"filesystem\"],
\"mitre_persistence\": {}, \"time\": \"2021-12-14T18:33:37.314933749\", \"output_fields\": { \"container.id\": \"host\", \"container.image.repository\": null, \"evt.t
ime\": \"16394999617314933749\", \"fd.name\": \"/events.txt\", \"proc.cmdline\": \"falco\", \"proc.name\": \"falco\", \"proc.pname\": \"bash\", \"user.loginid\": 1801, \"user.na
me\": \"root\"}}]
```

5. Настройка Falco-экспортера, Prometheus, Grafana. Для этого необходимо дописать следующие строки в файл Docker-compose:

```
node_exporter:
  image: quay.io/prometheus/node-exporter:latest
  container_name: node_exporter
  command:
    - '--path.rootfs=/host'
  pid: host
  restart: unless-stopped
  volumes:
    - '/:/host:ro,rslave'
  networks:
    app-network:
      ipv4_address: 172.20.0.2
```

```
prometheus:
  image: prom/prometheus:latest
  container_name: prometheus
  restart: unless-stopped
  ports:
    - "8080:9090"
  volumes:
    - "/etc/prometheus:/etc/prometheus"
  networks:
    app-network:
      ipv4_address: 172.20.0.3
```

```
grafana-oss:
  image: grafana/grafana-oss:latest
  container_name: grafana-oss
  restart: unless-stopped
  ports:
    - "3000:3000"
  volumes:
    - "grafana-storage:/var/lib/grafana"
  networks:
    app-network:
      ipv4_address: 172.20.0.4
```

```
falcosidekick:
  image: falcosecurity/falcosidekick
  container_name: falcosidekick
```

```

restart: unless-stopped
ports:
  - "2801:2801"
environment:
  - KAFKA_HOSTPORT=172.20.0.8:9092
  - KAFKA_TOPIC=falco-events
networks:
  app-network:
    ipv4_address: 172.20.0.5

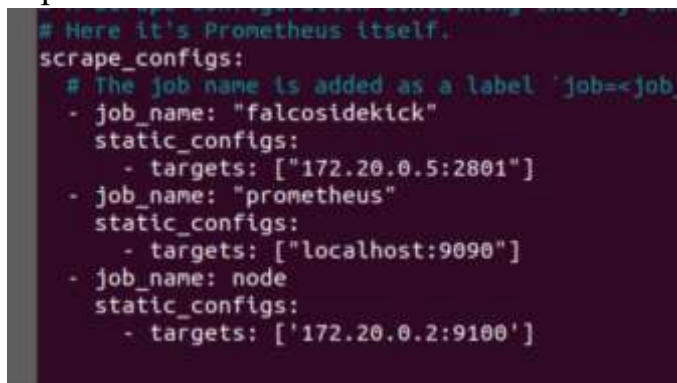
volumes:
  grafana-storage:
    driver: local
networks:
  app-network:
    ipam:
      driver: default
      config:
        - subnet: "172.20.0.0/24"

```

Node Exporter — сервис, задача которого заключается в экспорте информации о машине в формате, понятном Prometheus'у. Grafana рисует для графики, используя информацию из Prometheus. Falcosidekick - Простой демон, который поможет вам с выводами Falco. Он берет событие сокола и направляет его на разные выходы, в нашем случае на Dashboard.

6. Конфигурация Falco-экспортера (Falcosidekick):

Прописываем в файл `/etc/prometheus/Prometheus.yaml` Следующие строки:

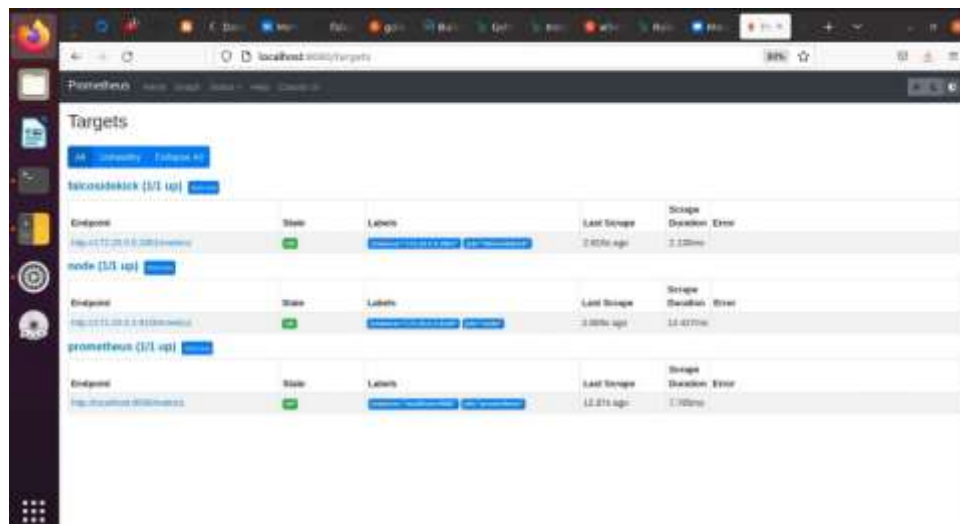


```

# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label 'job=<job_name>'
  - job_name: "falcosidekick"
    static_configs:
      - targets: ["172.20.0.5:2801"]
  - job_name: "prometheus"
    static_configs:
      - targets: ["localhost:9090"]
  - job_name: node
    static_configs:
      - targets: ['172.20.0.2:9100']

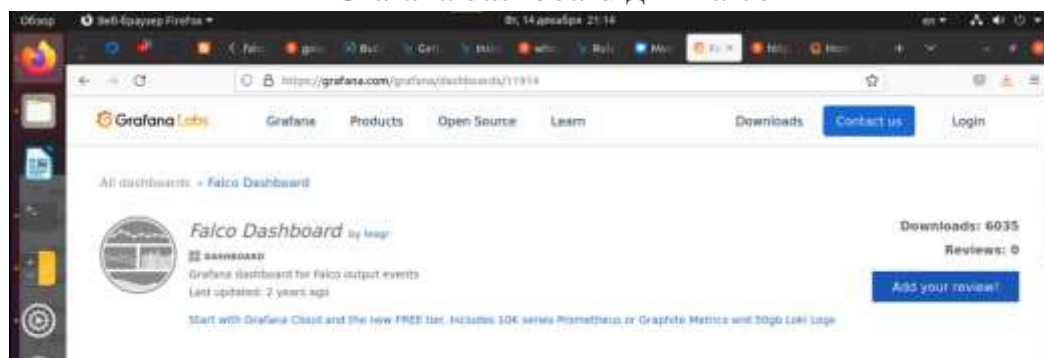
```

проверяем работу web интерфейса:

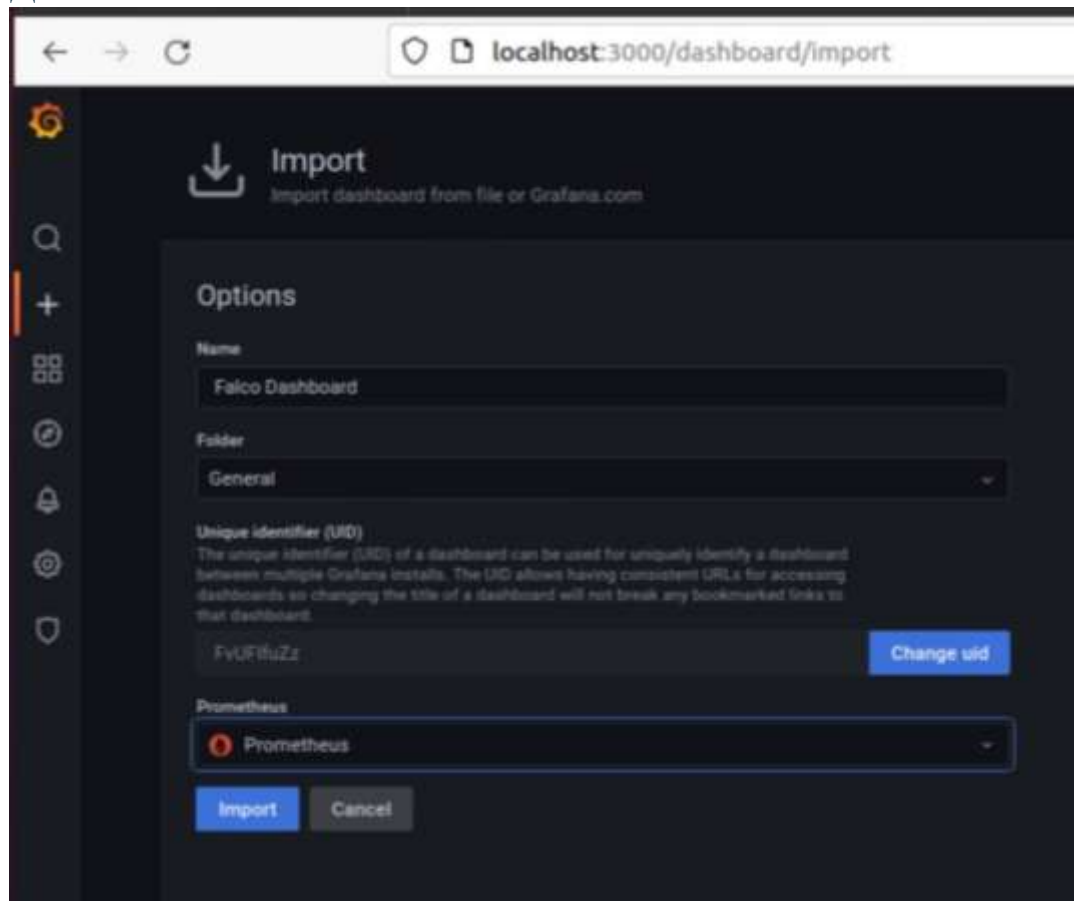


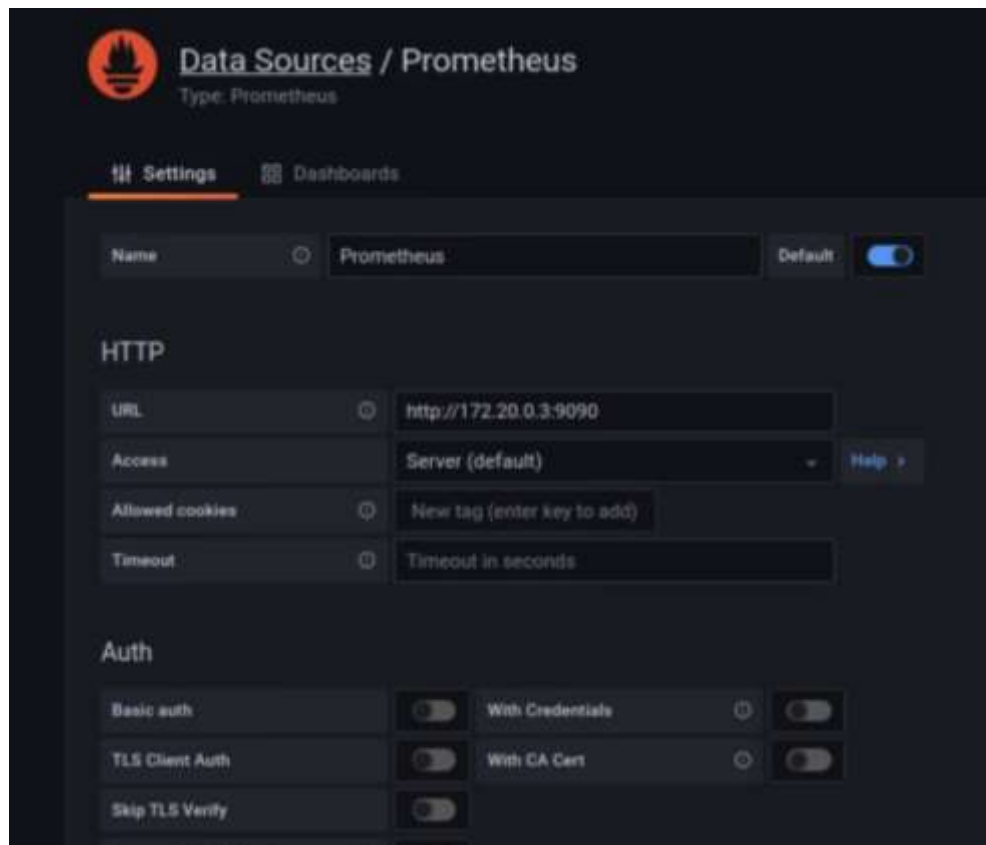
7. Настройка dashboard:

Скачиваем на сайте Grafana dashboard для Falco



Добавляем скаченный готовый dashboard:





8. Проверяем работоспособность всех установленных компонент:
Запускаем фалко, запускаем Docker-compose

```

viktoria@user-virtual-machine:~/Docker$ sudo docker-compose start
Starting web ... done
Starting redis ... done
Starting node_exporter ... done
Starting prometheus ... done
Starting grafana-oss ... done
Starting falcosidekick ... done

```

Вывод на dashboard:

