

## Практическая работа № 1: Сбор логов

Выполнил Ионов Максим Сергеевич, группа ББМО-02-23

### Цель работы:

- Создать 2 виртуальные машины на базе ОС Debian 12
- Обеспечить между ними сетевой обмен
- Включить на 1й из ВМ передачу логов по протоколу rsyslog на 2ю ВМ
- Установить и настроить получение логов на сервер с использованием Loki
- Установить и настроить получение логов на сервер с использованием Loki (signoz.io)

### Ход работы

,

### Установка `rsyslog` на сервер

```
(mrx@mrx)-[~]  
$ sudo apt-get install rsyslog  
[sudo] password for mrx:  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
The following packages were automatically installed and are no longer required:  
  libavfilter9 libjsoncpp25 libkf5guiaddons-bin libplacebo338 libpostproc57  
  openjdk-17-jre openjdk-17-jre-headless rwho rwhod  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libestr0 libfastjson4 liblognorm5  
Suggested packages:  
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl  
  | rsyslog-gnutls rsyslog-gssapi rsyslog-relp  
The following NEW packages will be installed:  
  libestr0 libfastjson4 liblognorm5 rsyslog  
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.  
Need to get 818 kB of archives.  
After this operation, 4208 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

### Настройка модулей и добавление правил `rsyslog`

```
(mrx@mrx)-[~]  
$ sudo nano /etc/rsyslog.conf
```

```

GNU nano 8.1 /etc/rsyslog.conf *
# /usr/share/doc/rsyslog-doc/html/configuration/index.html

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

$template RemoteLogs, "/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
*. * ?RemoteLogs
& ~
#####

```

## Применение конфигурации `rsyslog`

```

(mrx@mx)-[~]
$ sudo nano /etc/rsyslog.conf

(mrx@mx)-[~]
$ sudo systemctl restart rsyslog

(mrx@mx)-[~]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; prese>
   Active: active (running) since Thu 2024-09-12 18:33:48 MSK; 10s ago
 Invocation: 0038b1e5db71461cbbdda3e17fdf86c9
  TriggeredBy: ● syslog.socket
             Docs: man:rsyslogd(8)
                  man:rsyslog.conf(5)
                  https://www.rsyslog.com/doc/
   Main PID: 7358 (rsyslogd)
    Tasks: 10 (limit: 2206)
   Memory: 2.1M (peak: 2.6M)
      CPU: 27ms
   CGroup: /system.slice/rsyslog.service
           └─7358 /usr/sbin/rsyslogd -n -iNONE

```

```

(mrx@mx)-[~]
$ sudo nano /etc/rsyslog.conf

(mrx@mx)-[~]
$ sudo systemctl restart rsyslog

(mrx@mx)-[~]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; prese
   Active: active (running) since Mon 2025-01-22 18:33:48 MSK; 10s ago
   Invocation: 0038b1e5db71461cbbdda3e17fdf86c9
   TriggeredBy: ● syslog.socket
     Docs: man:rsyslogd(8)
           man:rsyslog.conf(5)
           https://www.rsyslog.com/doc/
   Main PID: 7358 (rsyslogd)
     Tasks: 10 (limit: 2206)
    Memory: 2.1M (peak: 2.6M)
       CPU: 27ms
    CGroup: /system.slice/rsyslog.service
            └─7358 /usr/sbin/rsyslogd -n -iNONE

```

## Установка `rsyslog` на клиент

```

(mrx@mx)-[~]
$ sudo apt-get install rsyslog
[sudo] password for mrx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
d:
  libavfilter9 libjsoncpp25 libkf5guiaddons-bin libplacebo338 libpostproc57
  openjdk-17-jre openjdk-17-jre-headless rwho rwhod
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libestr0 libfastjson4 liblognorm5
Suggested packages:
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl
  | rsyslog-gnutls rsyslog-gssapi rsyslog-relp
The following NEW packages will be installed:
  libestr0 libfastjson4 liblognorm5 rsyslog
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 818 kB of archives.
After this operation, 4208 kB of additional disk space will be used.
Do you want to continue? [Y/n] █

```

## Добавление правила пересылки логов на сервер



```
#
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

#sending all logs
*. * @10.211.55.28
```

## Применение конфигурации `rsyslog`

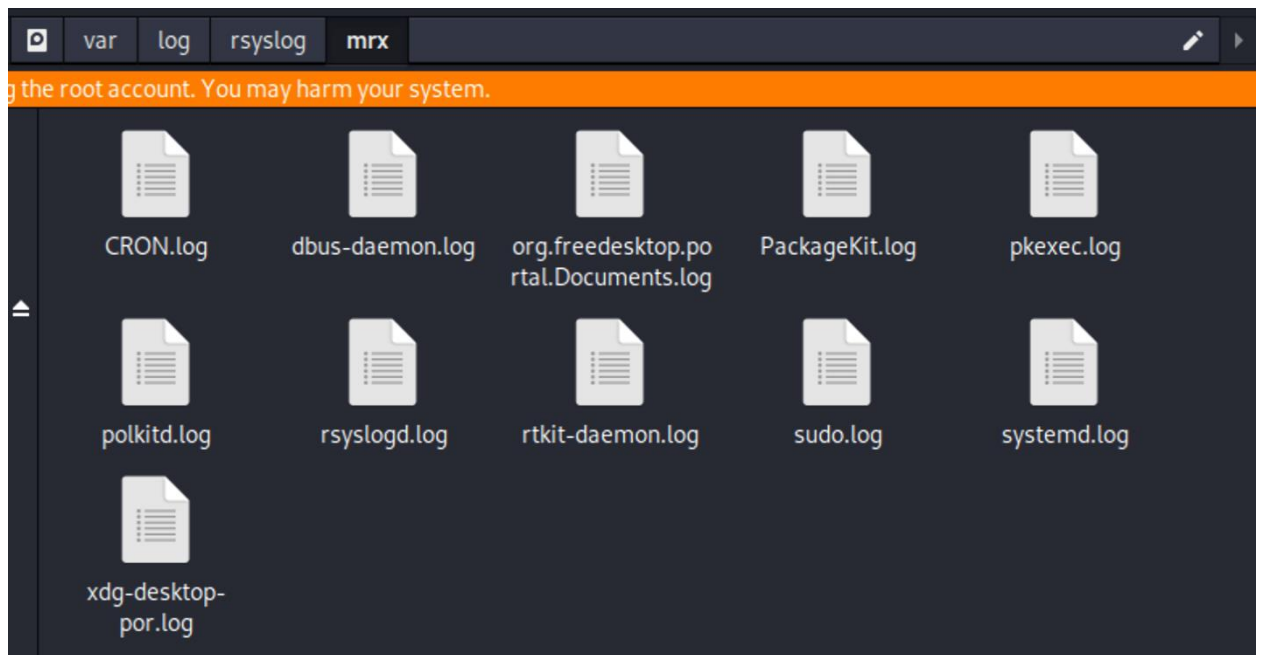
```
(mrx@mrx)-[~]
$ sudo systemctl restart rsyslog

(mrx@mrx)-[~]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; prese>
   Active: active (running) since Thu 2024-09-12 18:37:24 MSK; 5s ago
     Invocation: 77e845d7cf4248d3a25e3843f2ee6e4c
   TriggeredBy: ● syslog.socket
        Docs: man:rsyslogd(8)
              man:rsyslog.conf(5)
              https://www.rsyslog.com/doc/
   Main PID: 6638 (rsyslogd)
     Tasks: 10 (limit: 2206)
    Memory: 1.2M (peak: 1.5M)
       CPU: 27ms
    CGroup: /system.slice/rsyslog.service
            └─6638 /usr/sbin/rsyslogd -n -iNONE
```

```
(mrx@mrx)-[~]
$ sudo systemctl restart rsyslog

(mrx@mrx)-[~]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; prese>
   Active: active (running) since Mon 2025-01-22 18:37:24 MSK; 5s ago
     Invocation: 77e845d7cf4248d3a25e3843f2ee6e4c
   TriggeredBy: ● syslog.socket
        Docs: man:rsyslogd(8)
              man:rsyslog.conf(5)
              https://www.rsyslog.com/doc/
   Main PID: 6638 (rsyslogd)
     Tasks: 10 (limit: 2206)
    Memory: 1.2M (peak: 1.5M)
       CPU: 27ms
    CGroup: /system.slice/rsyslog.service
            └─6638 /usr/sbin/rsyslogd -n -iNONE
```

## Просмотр полученных логов на сервере

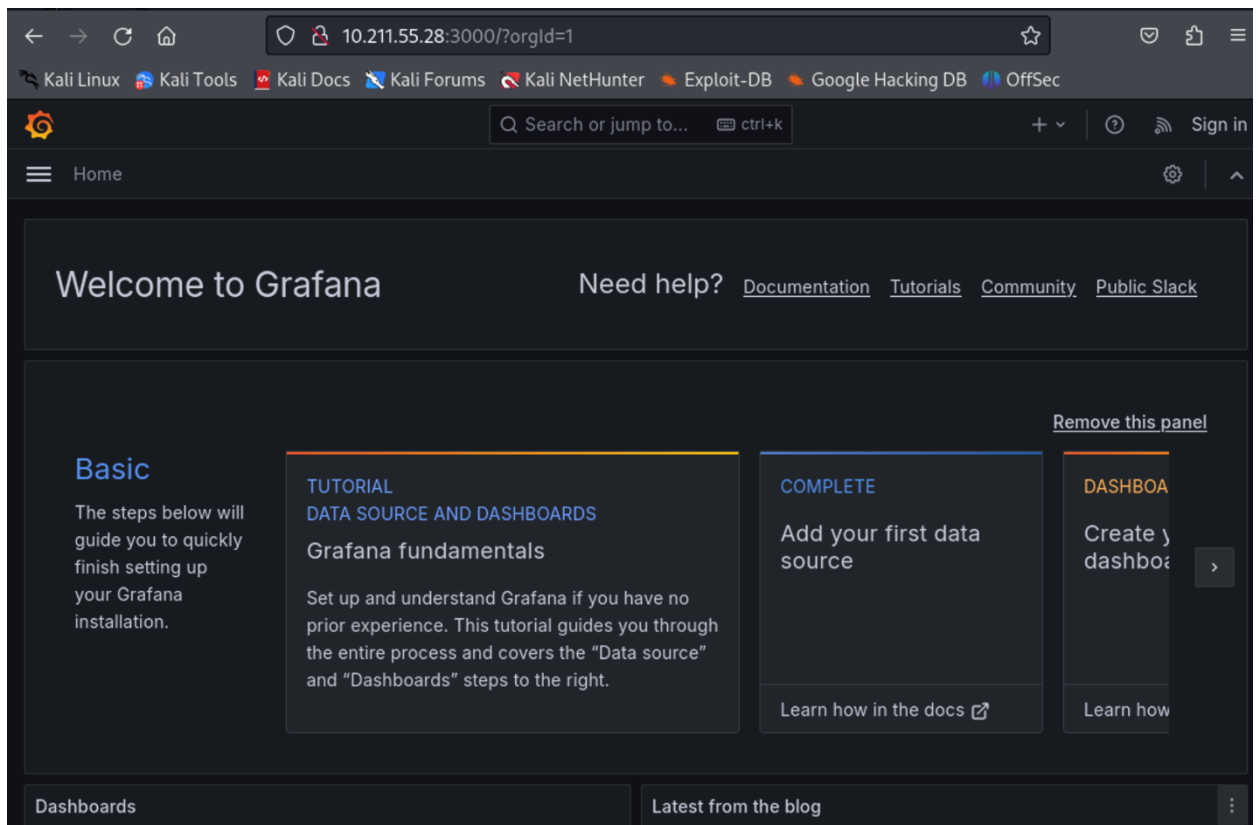


## Loki

Загружаем compose-файл от разработчика

Запуск Loki

```
(mrx@mrx)~[~]
$ sudo docker-compose up -d
Creating network "mrx_loki" with the default driver
Pulling loki (grafana/loki:2.9.10) ...
2.9.10: Pulling from grafana/loki
690e87867337: Pull complete
ca788e42cccc: Pull complete
0dc7266e3fe0: Pull complete
d70bc2ed4e18: Pull complete
28a9aefadd6d: Pull complete
a222aaaff35d: Pull complete
Digest: sha256:35b02acc67654ddc38273e519b4f26f3967a907b9db5489af300c21f37ee1ae7
Status: Downloaded newer image for grafana/loki:2.9.10
Pulling promtail (grafana/promtail:2.9.10) ...
2.9.10: Pulling from grafana/promtail
bd2a3a2ed82d: Pull complete
03c97452ef13: Pull complete
59c8c08a04c5: Pull complete
98d74d043369: Pull complete
af66105f2cbd: Pull complete
19fb7c316c21: Pull complete
Digest: sha256:63a2e57a5b1401109f77d36a49a637889d431280ed38f5f885eedcd3949e52cf
Status: Downloaded newer image for grafana/promtail:2.9.10
Pulling grafana (grafana/grafana:latest) ...
latest: Pulling from grafana/grafana
bca4290a9639: Pull complete
35ffea0c044a: Pull complete
fbbaca673c19: Pull complete
73d7d01a1d2c: Pull complete
f257bec43f81: Pull complete
15e31fbc4904: Pull complete
8ff0366d982d: Pull complete
1e825da9c63a: Pull complete
ffca16271da6: Pull complete
27a3c8ebdfbf: Pull complete
Digest: sha256:408afb9726de5122b00a2576763a8a57a3c86d5b0eff5305bc994ceb3eb96c3f
Status: Downloaded newer image for grafana/grafana:latest
Creating mrx_loki_1 ... done
Creating mrx_grafana_1 ... done
Creating mrx_promtail_1 ... done
```



## Редактирование конфигурации `promtail` на клиенте

```
GNU nano 8.1 docker-compose.yml *
version: "3"

services:
  promtail:
    image: grafana/promtail:3.0.0
    volumes:
      - ./promtail-config.yaml:/etc/promtail/promtail-config.yaml
      - /var/log:/var/log
    command: -config.file=/etc/promtail/promtail-config.yaml
```

```
GNU nano 8.1 promtail-config.yaml *
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

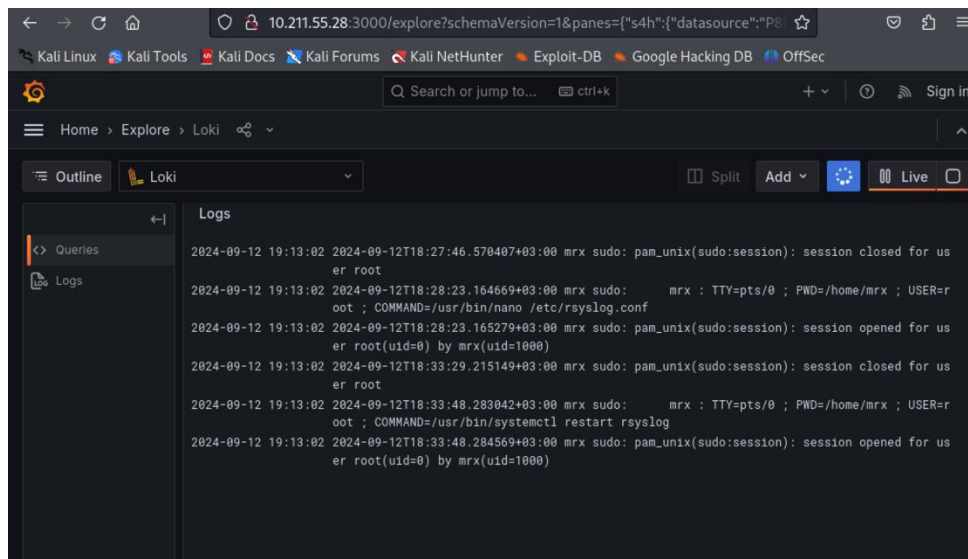
clients:
  - url: http://10.211.55.28:3100/loki/api/v1/push

scrape_configs:
  - job_name: system
    static_configs:
      - targets:
          - localhost
        labels:
          job: varlogs
          path: /var/log/*log
```

## Запуск `promtail` на клиенте

```
$ sudo docker-compose up -d
Creating network "promtail_default" with the default driver
Pulling promtail (grafana/promtail:3.0.0)...
3.0.0: Pulling from grafana/promtail
ef2fb7c49f69: Downloading [>
] 309.5kB/30.07MBng fs layer
6d00efff8967: Downloading [=====
ef2fb7c49f69: Downloading [=====>
] 2.173MB/30.07MBloading [>
ef2fb7c49f69: Pull complete
6d00efff8967: Pull complete
72e334002521: Pull complete
b571b5ee0c80: Pull complete
85a4c7b92961: Pull complete
caa973f8c036: Pull complete
Digest: sha256:d3de3da9431cfbe74a6a94555050df5257f357e827be8e63f8998d509c37af8b
Status: Downloaded newer image for grafana/promtail:3.0.0
Creating promtail_promtail_1 ... done
```

## Просмотр логов клиента в Grafana



## Signoz

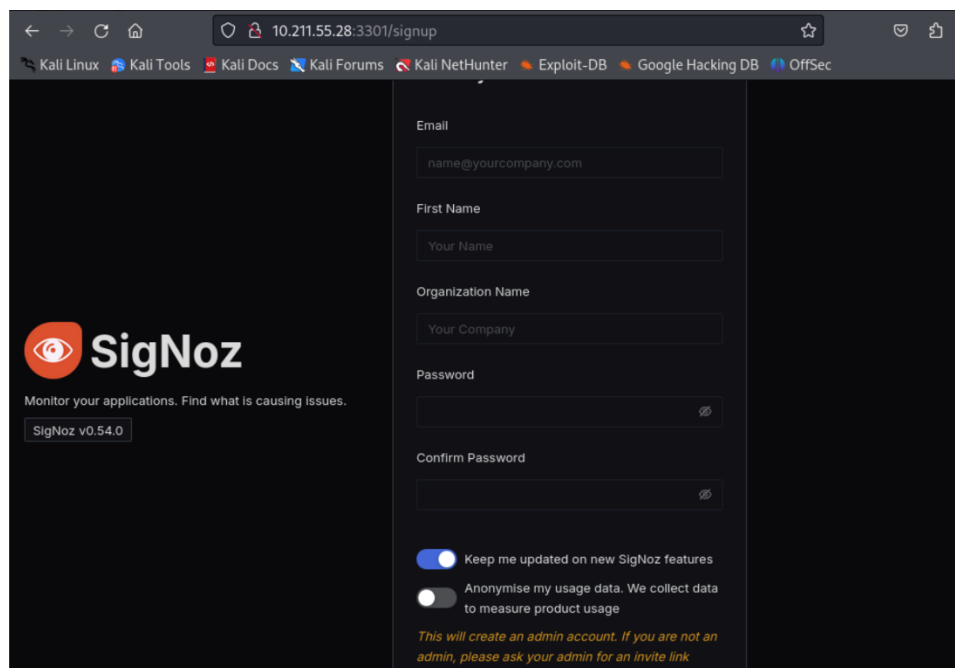
### Запуск Signoz

### Установка `Signoz` на сервер




```
(mrX@mrX)-[~/signoz/deploy/docker/clickhouse-setup]
$ sudo docker-compose up -d
Starting signoz-zookeeper-1 ... done
Starting hotrod ... done
Starting load-hotrod ... done
Starting signoz-clickhouse ... done
Starting otel-migrator ... done
Starting signoz-query-service ... done
Starting signoz-otel-collector ... done
Starting signoz-alertmanager ... done
Starting signoz-frontend ... done
Starting signoz-logspout ... done
```

## Рабочая панель Signoz



10.211.55.28:3301/signup

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 **SigNoz**

Monitor your applications. Find what is causing issues.

SigNoz v0.54.0

Email  
name@yourcompany.com

First Name  
Your Name

Organization Name  
Your Company

Password

Confirm Password

☒ Keep me updated on new SigNoz features

☐ Anonymise my usage data. We collect data to measure product usage

*This will create an admin account. If you are not an admin, please ask your admin for an invite link*

## Редактирование конфигурации клиентского приложения для отправки данных в Signoz

```
(mrX@mrX)-[~]
$ sudo git clone https://github.com/SigNoz/sample-nodejs-app.git
Cloning into 'sample-nodejs-app'...
remote: Enumerating objects: 200, done.
remote: Counting objects: 100% (56/56), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 200 (delta 29), reused 25 (delta 11), pack-reused 144 (from 1)
Receiving objects: 100% (200/200), 450.92 KiB | 1.45 MiB/s, done.
Resolving deltas: 100% (99/99), done.

(mrX@mrX)-[~]
$ cd sample-nodejs-app

(mrX@mrX)-[~/sample-nodejs-app]
$ sudo nano docker-compose.yaml
```



```
GNU nano 8.1 docker-compose.yml *
version: "2.4"
services:
  web:
    image: signoz/sample-nodejs-app:latest
    ports:
      - "5555:5555"
    extra_hosts:
      - signoz:host-gateway
    environment:
      - OTEL_EXPORTER_OTLP_ENDPOINT=http://10.211.55.28:4318/v1/traces # Replace with SigNoz OTLP endpoint, >
      - OTEL_RESOURCE_ATTRIBUTES=service.name=sample-nodejs
```

## Запуск клиентского приложения

```
(mrxc@mrxc) ~/sample-nodejs-app
$ sudo docker-compose up -d
Creating network "sample-nodejs-app_default" with the default driver
Pulling web (signoz/sample-nodejs-app:latest) ...
latest: Pulling from signoz/sample-nodejs-app
c41833b44d91: Pull complete
762c2470eea4: Pull complete
fefc7d195eee: Pull complete
06fc22ed341f: Pull complete
38711f466238: Pull complete
4f4fb700ef54: Pull complete
4c4d1890cf12: Pull complete
4528a0431042: Pull complete
7dee7df32563: Pull complete
Digest: sha256:50c4842c41be7f2a5b00385f6d3f275f374be4e8f05bb97b8a2fced1ccf90afa
Status: Downloaded newer image for signoz/sample-nodejs-app:latest
Creating sample-nodejs-app_web_1 ... done
```

## Информация о приложении в SigNoz

