Практическое задание №1. Сбор логов

Выполнил студент - Князева Анастасия Михайловна группы: ББМО-01-23

rsyslog

Установка rsyslog на сервер

```
knya@debian-server: $ sudo apt install rsyslog
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
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 829 kB of archives.
After this operation, 2,280 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 libestr0 amd64 0.1.11-1 [9,204 B]
Get:2 http://deb.debian.org/debian bookworm/main amd64 libfastjson4 amd64 1.2304.0-1 [28.9 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 liblognorm5 amd64 2.0.6-4 [67.2 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 rsyslog amd64 8.2302.0-1 [723 kB]
Fetched 829 kB in 0s (1,790 kB/s)
Selecting previously unselected package libestr0:amd64.
(Reading database ... 157621 files and directories currently installed.)
Preparing to unpack .../libestr0_0.1.11-1_amd64.deb ...
Unpacking libestr0:amd64 (0.1.11-1) ...
Selecting previously unselected package libfastjson4:amd64.
Preparing to unpack .../libfastjson4_1.2304.0-1_amd64.deb ...
Unpacking libfastjson4:amd64 (1.2304.0-1) ...
```

Настройка модулей rsyslog

```
#################
#### 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")
```

Настройка модулей rsyslog

```
#################
#### 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")
```

Добавление правил сбора логов

```
#
# Rules for processing remote logs from client
#
template(name="RemoteLogs" type="string" string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
*.* ?RemoteLogs
& stop
```

Применение конфигурации rsyslog на сервере

```
knya@debian-server:~$ sudo nano /etc/rsyslog.conf
knya@debian-server:~$ sudo systemctl restart rsyslog
knya@debian-server:~$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2023-11-09 08:27:10 GMT; 17s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 3283 (rsyslogd)
      Tasks: 10 (limit: 2252)
     Memory: 1.1M
        CPU: 7ms
     CGroup: /system.slice/rsyslog.service
             └─3283 /usr/sbin/rsyslogd -n -iNONE

Nov 09 08:27:10 debian-server systemd[1]: rsyslog.service: Deactivated successfully.
Nov 09 08:27:10 debian-server systemd[1]: Stopped rsyslog.service - System Logging Service.
Nov 09 08:27:10 debian-server systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 09 08:27:10 debian-server systemd[1]: Started rsyslog.service - System Logging Service.
Nov 09 08:27:10 debian-server rsyslogd[3283]: imuxsock: Acquired UNIX socket '/run/systemd/journa
Nov 09 08:27:10 debian-server rsyslogd[3283]: [origin software="rsyslogd" swVersion="8.2302.0" x-
lines 1-20/20 (END)
```

```
knya@debian-server:~$ sudo ss -tulnp | grep rsyslog
udp   UNCONN 0      0            0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid=3283,fd=6))
udp   UNCONN 0      0               [::]:514           [::]:*    users:(("rsyslogd",pid=3283,fd=7))
tcp   LISTEN 0      25           0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid=3283,fd=8))
tcp   LISTEN 0      25              [::]:514           [::]:*    users:(("rsyslogd",pid=3283,fd=9))
```

Установка rsyslog на клиент

```
root@debian-client:/home/m20a# apt update && apt install -y rsyslog
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://security.debian.org/debian-security bookworm-security InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
13 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl | rsyslog-gnutl
The following NEW packages will be installed:
  rsyslog
0 upgraded, 1 newly installed, 0 to remove and 13 not upgraded.
Need to get 723 kB of archives.
After this operation, 1,989 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 rsyslog amd64 8.2302.0-1 [723 kB]
Fetched 723 kB in 0s (1,852 kB/s)
Selecting previously unselected package rsyslog.
(Reading database ... 157590 files and directories currently installed.)
Preparing to unpack .../rsyslog_8.2302.0-1_amd64.deb ...
Unpacking rsyslog (8.2302.0-1) ...
```

Добавление правила пересылки логов на сервер

```
#
# Rule for sending all logs to server
#

*.* @@192.168.248.132:514
```

Применение конфигурации rsyslog на клиенте

```
knya@debian-client:~$ sudo nano /etc/rsyslog.conf
knya@debian-client:~$ sudo systemctl restart rsyslog
knya@debian-client:~$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2023-11-09 08:36:42 GMT; 19s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 4560 (rsyslogd)
      Tasks: 10 (limit: 2252)
     Memory: 1.1M
        CPU: 8ms
     CGroup: /system.slice/rsyslog.service
             └─4560 /usr/sbin/rsyslogd -n -iNONE

Nov 09 08:36:42 debian-client systemd[1]: rsyslog.service: Deactivated successfully.
Nov 09 08:36:42 debian-client systemd[1]: Stopped rsyslog.service - System Logging Service.
Nov 09 08:36:42 debian-client systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 09 08:36:42 debian-client systemd[1]: Started rsyslog.service - System Logging Service.
Nov 09 08:36:42 debian-client rsyslogd[4560]: imuxsock: Acquired UNIX socket '/run/systemd/journa
Nov 09 08:36:42 debian-client rsyslogd[4560]: [origin software="rsyslogd" swVersion="8.2302.0" x-
lines 1-20/20 (END)
```

Просмотр логов клиента на сервере

```
knya@debian-server:/var/log/debian-client$ ls -la
total 24
drwxr-xr-x  2 root root 4096 Nov  9 08:38 .
drwxr-xr-x 11 root root 4096 Nov  9 08:36 ..
-rw-r-----  1 root adm    64 Nov  9 08:38 PackageKit.log
-rw-r-----  1 root adm   465 Nov  9 08:36 rsyslogd.log
-rw-r-----  1 root adm  1147 Nov  9 08:40 sudo.log
-rw-r-----  1 root adm   705 Nov  9 08:38 systemd.log
knya@debian-server:/var/log/debian-client$ sudo cat sudo.log
2023-11-09T08:36:42+00:00 debian-client sudo: pam_unix(sudo:session): session closed for user root
2023-11-09T08:37:02+00:00 debian-client sudo:     m20a : TTY=pts/0 ; PWD=/home/m20a ; USER=root ; COMMAND=/usr/bin/syst
status rsyslog
2023-11-09T08:37:02+00:00 debian-client sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
2023-11-09T08:38:37+00:00 debian-client sudo: pam_unix(sudo:session): session closed for user root
2023-11-09T08:39:46+00:00 debian-client sudo:     m20a : TTY=pts/0 ; PWD=/home/m20a ; USER=root ; COMMAND=/usr/bin/ls
2023-11-09T08:39:46+00:00 debian-client sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
2023-11-09T08:39:46+00:00 debian-client sudo: pam_unix(sudo:session): session closed for user root
2023-11-09T08:40:09+00:00 debian-client sudo:     m20a : TTY=pts/0 ; PWD=/home/m20a ; USER=root ; COMMAND=/usr/bin/cat
history
2023-11-09T08:40:09+00:00 debian-client sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
2023-11-09T08:40:09+00:00 debian-client sudo: pam_unix(sudo:session): session closed for user root
```

Графана Локи

Загрузка compose-файла Loki

```
knya@debian-server:~/loki$ wget https://raw.githubusercontent.com/grafana/loki/v2.9.1/production/docker-compose.yaml
--2023-11-09 10:27:20--  https://raw.githubusercontent.com/grafana/loki/v2.9.1/production/docker-compose.yaml
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ..
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1073 (1.0K) [text/plain]
Saving to: 'docker-compose.yaml'

docker-compose.yaml            100%[=============================================>]   1.05K  --.-KB/s    in 0s

2023-11-09 10:27:20 (70.7 MB/s) - 'docker-compose.yaml' saved [1073/1073]
```

```yaml
version: "3"

networks:
  loki:

services:
  loki:
    image: grafana/loki:2.9.0
    ports:
      - "3100:3100"
    command: -config.file=/etc/loki/local-config.yaml
    networks:
      - loki

  grafana:
    environment:
      - GF_PATHS_PROVISIONING=/etc/grafana/provisioning
      - GF_AUTH_ANONYMOUS_ENABLED=true
      - GF_AUTH_ANONYMOUS_ORG_ROLE=Admin
    entrypoint:
      - sh
      - -euc
      - |
        mkdir -p /etc/grafana/provisioning/datasources
        cat <<EOF > /etc/grafana/provisioning/datasources/ds.yaml
        apiVersion: 1
        datasources:
        - name: Loki
          type: loki
          access: proxy
          orgId: 1
          url: http://loki:3100
```

Запуск Loki

```
knya@debian-server:~/loki$ sudo docker-compose up -d
[+] Building 0.0s (0/0)
[+] Running 3/3
 ✔ Network loki_loki         Created
 ✔ Container loki-grafana-1  Started
 ✔ Container loki-loki-1     Started
knya@debian-server:~/loki$ sudo docker-compose ps
NAME               IMAGE                  COMMAND                  SERVICE             CREATED
TUS              PORTS
loki-grafana-1     grafana/grafana:latest   "sh -euc 'mkdir -p /…"   grafana             34 seconds ago
31 seconds       0.0.0.0:3000->3000/tcp, :::3000->3000/tcp
loki-loki-1        grafana/loki:2.9.0       "/usr/bin/loki -conf…"   loki                34 seconds ago
31 seconds       0.0.0.0:3100->3100/tcp, :::3100->3100/tcp
```

Файл конфигурации promtail на клиенте

```yaml
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://192.168.248.132:3100/loki/api/v1/push

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

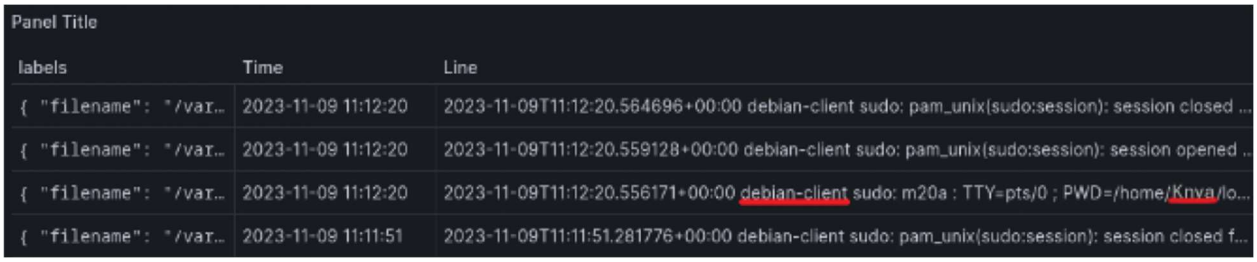
Compose-файл promtail

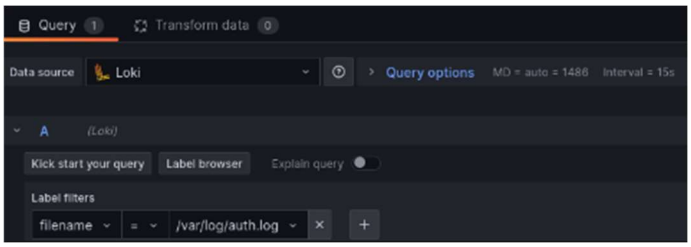
```
version: "3.9"

services:
  promtail:
    image: grafana/promtail:2.9.0
    volumes:
      - /var/log:/var/log
      - ./promtail-config.yaml:/etc/promtail/config.yml
    command: -config.file=/etc/promtail/config.yml
```

Запуск promtail на клиенте

```
knya@debian-client:~/loki$ sudo docker-compose up -d
[sudo] password for m20a:
Sorry, try again.
[sudo] password for m20a:
Creating network "loki_default" with the default driver
Pulling promtail (grafana/promtail:2.9.0)...
2.9.0: Pulling from grafana/promtail
7d97e254a046: Pull complete
39932bcaa1cc: Pull complete
4059d897dde4: Pull complete
325d59b59788: Pull complete
9e9c5b842176: Pull complete
01befd6b403e: Pull complete
Digest: sha256:c2c423196c75a2c9c26f6fe0ba7200c3167334b14975747f5dcff678bd1a32e9
Status: Downloaded newer image for grafana/promtail:2.9.0
Creating loki_promtail_1 ... done
knya@debian-client:~/loki$ sudo docker-compose ps
     Name                   Command               State   Ports
-------------------------------------------------------------------
loki_promtail_1   /usr/bin/promtail -config. ...   Up
```

Просмотр логов клиента в Grafana



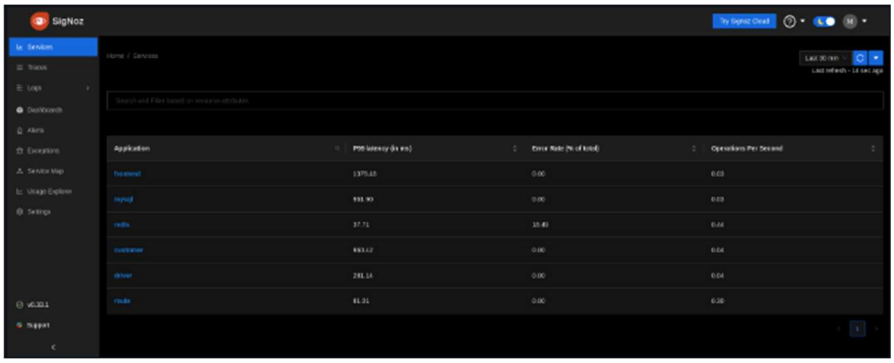


Синьоз

Запуск Signoz

```
knya@debian-server:~/signoz/deploy/docker/clickhouse-setup$ sudo docker-compose up -d
[sudo] password for m20a:
[+] Building 0.0s (0/0)
[+] Running 11/11
 ✔ Container hotrod                        Running                                 0.0s
 ✔ Container load-hotrod                   Running                                 0.0s
 ✔ Container signoz-zookeeper-1            Running                                 0.0s
 ✔ Container signoz-clickhouse             Healthy                                20.3s
 ✔ Container otel-migrator                 Exited                                 19.8s
 ✔ Container signoz-query-service          Healthy                                32.8s
 ✔ Container signoz-otel-collector-metrics Started                                 2.3s
 ✔ Container signoz-alertmanager           Started                                 2.2s
 ✔ Container signoz-otel-collector         Started                                 2.2s
 ✔ Container signoz-frontend               Started                                 3.2s
 ✔ Container signoz-logspout               Started                                 3.2s
```

Стартовая страница Signoz



Приложение, используемое на стороне клиента для отправки данных в Signoz — https://github.com/SigNoz/sample-nodejs-app/

```
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://192.168.248.132:4318/v1/traces
      - OTEL_RESOURCE_ATTRIBUTES=service.name=sample-nodejs
```

Запуск клиентского приложения

```
knya@debian-client: /nodejs$ sudo docker-compose up -d
Creating network "nodejs_default" with the default driver
Pulling web (signoz/sample-nodejs-app:latest)...
latest: Pulling from signoz/sample-nodejs-app
f56be85fc22e: Downloading [>                                                  ]
 34.76kB/3.375MBlling fs layer
60542df8b663: Pulling fs layer
f56be85fc22e: Downloading [==========>                                        ]
 703.8kB/3.375MBiting
4f4fb700ef54: Waiting
f56be85fc22e: Downloading [====================>                              ]
 1.437MB/3.375MBiting
91fc9829d156: Waiting
931b0e865bc2: Downloading [========>                                          ]
f56be85fc22e: Pull complete
931b0e865bc2: Pull complete
60542df8b663: Pull complete
062e26bc2446: Pull complete
aebace558f25: Pull complete
4f4fb700ef54: Pull complete
02b799cff739: Pull complete
d4f1f08cb98d: Pull complete
91fc9829d156: Pull complete
Digest: sha256:50c4842c41be7f2a5b00385f6d3f275f374be4e8f05bb97b8a2fced1ccf90afa
```

Информационная панель в Signoz