

Настройка Syslog-ng на Unix системах

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Для начала необходимо проверить установлена ли нужная служба Syslog-ng, посмотрим статус службы:

```
systemctl status syslog-ng
```

В случае отсутствия службы необходимо установить следующие пакеты:

```
apt-get install syslog-ng
```

В случае если служба не запущена:

```
sudo systemctl start syslog-ng  
sudo systemctl enable syslog-ng
```

Настройка источника

Далее на источнике нужно создать файл с параметрами работы службы и изменить конфигурационный файл службы Syslog-ng.

Сначала создается файл с параметрами работы службы:

Создайте файл `/etc/syslog-ng/1-unixLogging.conf`, например с помощью nano:

```
nano /etc/syslog-ng/1-unixLogging.conf
```

Добавьте в файл строки для отправки по UDP на порт 5140:

```
filter unix_filter {
    not facility(cron, lpr, mail, news, uucp);
};

destination to_kuma_udp {
    udp("<IP_KUMA_Collector>" port(5140));
};

log {
    source(s_src);
    filter(unix_filter);
    destination(to_kuma_udp);
};
```

Добавьте в файл строки для отправки по TCP на порт 5140:

```
filter unix_filter {
    not facility(cron, lpr, mail, news, uucp);
};

destination to_kuma_tcp {
    tcp("<IP_KUMA_Collector>" port(5140) log-fifo-size(1000));
};

log {
    source(s_src);
    filter(unix_filter);
    destination(to_kuma_tcp);
    flags(flow-control);
};
```

Чтобы настроить конфигурационный файл службы с использованием настроек сделанных выше, отредактируйте файл `/etc/syslog-ng/syslog-ng.conf`, добавив в файл строку:

```
@include "1-unixLogging.conf"
```

Перезапустите службу syslog-ng:

```
systemctl restart syslog-ng
```

Проверка отправки сообщения

Для проверки получения и отправки сообщения можно воспользоваться командой с тестовым сообщением:

```
logger "testTest"
```

Это сообщение должно появиться в системном журнале, например `/var/log/messages`:

```
Oct  4 10:22:41 test-kuma systemd[1]: kuma-collector-2d8ccbfd-3990-4e
Oct  4 10:22:41 test-kuma systemd[1]: Failed to start KUMA collector.
Oct  4 10:22:43 test-kuma root[4032724]: testTest
Oct  4 10:22:44 test-kuma kuma[4393]: 2023/10/04 10:22:44 WARN: You s
Oct  4 10:22:44 test-kuma systemd[1]: kuma-collector-28a4fb00-f0e3-4f
Oct  4 10:22:44 test-kuma systemd[1]: kuma-collector-28a4fb00-f0e3-4f
```

Дополнительная информация

Обычно в конфигурации `/etc/syslog-ng/syslog-ng.conf` в `s_src` содержится 2 типа журналов

```
source s_src {
    system(); # системный журнал
    internal(); # внутренние сообщения журнала syslog-ng
};
```

Для задания шаблона сообщения можно использовать следующее:

```
template LogglyFormat { template("<${PRI}>1 ${ISODATE} ${HOST} ${PROGRAM} ${PID} ${MSGID}
[TOKEN@41058 tag=\"TAG\" ] $MSG\n");
    template_escape(no);
};
```

```
destination d_loggly {
    tcp("logs-01.loggly.com" port(514) template(LogglyFormat));
};
```

