Мне понадобилось организовать сервер для сбора логов с удаленных устройств. Это могут быть серверы, сетевое оборудование, либо что-то еще, что поддерживает логирование в формате syslog. Я решил использовать не стандартный для большинства дистрибутивов rsyslog, а установить syslog-ng, потому что мне он показался более удобным и простым в настройке.

Содержание:

Введение

Информации на тему сбора логов с удаленных серверов и интернете достаточно много. Ничего сложного тут нет, я и сам уже описывал подобную настройку в статье про сбор логов с mikrotik. Но решение получилось кривоватое, в комментариях написаны замечания. Я и сам знал о них, но простого и быстрого решения я не смог найти, на тот момент меня устраивал и такой вариант. Сейчас же решил все сделать аккуратно и красиво, чтобы было удобно пользоваться. В процессе поиска информации в интернете решил попробовать **syslog-ng**. С ним у меня не возникло никаких затруднений, сразу получилось то, что требовалось, поэтому я остановил свой выбор на нем.

Настраивать сервер сбора логов будем на системе CentOS 7. Если у вас еще не подготовлен сервер, то читайте мою информацию по установке и базовой настройке centos. Для небольшого количества устройств, нагрузка на сервер будет незначительная, поэтому имеет смысл размещать сервер на виртуальной машине. Если у вас нет готового гипервизора, можете посмотреть мою информацию на тему настройки linux гипервизора proxmox или

бесплатного решения microsoft — Windows Hyper-V Server 2016.

Установка и настройка syslog-ng

С установкой нет ничего сложного. Установить syslog-ng можно одной командой:

```
# yum install -y syslog-ng
```

Сразу переходим к настройке. Файл конфигурации располагается по адресу */etc/syslog-ng/syslog-ng.conf*. Чтобы сервер начал принимать логи с удаленного устройства, его необходимо прописать в конфиг. Делается это просто. В самый конец конфигурационного файла добавляем информацию о новом устройстве:

```
destination d_xs-zabbix { file("/var/log/!remote/xs-zabbix.log"); };
filter f_xs-zabbix { netmask("10.1.3.29/255.255.255.255"); };
log { source(net); filter(f_xs-zabbix); destination(d_xs-zabbix); };
```

d_xs-zabbix	Название назначения для записи лога по адресу /var/log/!remote/xs-zabbix.log
f_xs-zabbix	Название фильтра по адресу сервера источника.
10.1.3.29	Адрес сервера источника логов

Соответственно для второго сервера нужно добавить еще 3 строки, например так:

```
destination d_xs-web { file("/var/log/!remote/xs-web.log"); };
filter f_xs-web { netmask("10.1.3.38/255.255.255.255"); };
log { source(net); filter(f_xs-web); destination(d_xs-web); };
```

И так далее. Добавляете столько серверов, сколько нужно. Не забудьте создать папку для логов. В моем примере это папка */var/log/!remote*, сами файлы создавать не надо, служба автоматически их создаст, когда придет информация с удаленных серверов.

Запускаем syslog-ng и добавляем в автозагрузку:

```
# systemctl start syslog-ng
# systemctl enable syslog-ng
```

Проверим, запустилась ли служба:

```
# netstat -tulnp | grep syslog
udp 0 0 0.0.0.0:514 0.0.0.0:* 25960/syslog-ng
```

Все в порядке, слушает **514 udp** порт. Не забудьте открыть этот порт в iptables, если у вас включен фаерволл. Сервер готов к приему логов.

Отправка логов syslog на удаленный сервер

Теперь идем на добавленные в syslog-ng сервера и настраиваем там отправку логов на наш сервер. Сделать это очень просто. Открываем файл конфигурации rsyslog. В CentOS он живет по адресу */etc/rsyslog.conf* и добавляем туда строку:

```
*.* @10.1.3.22
```

10.1.3.22 — ip адрес syslog-ng сервера. Перезапустите rsyslog:

```
# service rsyslog restart
```

и проверяйте логи на сервере syslog-ng в указанной папке. Правило *.* отправит все логи в указанное направление. Это не всегда нужно, можно отредактировать правила. Для этого надо ознакомиться с документацией по syslog. Там нет ничего сложного, мне не хочется на этом сейчас подробно останавливаться. В интернете есть примеры. Приведу пару своих.

```
*.*;local5.none @10.1.3.22
```

В данном случае у меня по local5.notice идет лог самбы по доступу к сетевой шаре. Мне не нужно собирать эту информацию и я ее отключил. Вот еще пример:

```
*.info @10.1.3.22
```

С этого сервера сыпалось много лишней информации уровня debug. Я ограничил отправляемые сообщения уровнем info. И так далее.

Ротация логов syslog-ng

В завершение приведу пример своего правила ротации логов. Рекомендую ротацию настроить сразу, не оставлять на потом. Создаем файл */etc/logrotate.d/syslog-ng*

```
# mcedit /etc/logrotate.d/syslog-ng
```

```
/var/log/!remote/*.log {
    daily
    rotate 180
    olddir /var/log/!remote/old
    missingok
    compress
    sharedscripts
    postrotate
    /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

По этому правилу ротация логов происходит раз в день. Старые логи перемещаются в папку /var/log/!remote/old и сжимаются. Хранятся логи за последние 180 дней.

Заключение

Я привел частный случай настройки хранения логов с удаленных устройств. Решение в лоб. В простых случаях этого достаточно. Лично мне удобно смотреть информацию в текстовых файлах. Это требуется редко, сделано на всякий случай для расследования инцидентов, если таковые возникают. Эту

же задачу, к примеру, можно решить с помощью заббикс. Я уже показывал, как мониторить с помощью zabbix лог файлы. Приведенное решение легко переделать в хранение логов.

Для более удобного сбора и последующего просмотра информации существуют готовые решения с написанными веб панелями. Я посмотрел на некоторые из них. Что-то мне показалось слишком сложным в настройке, где-то веб интерфейс не понравился. Для себя остановился на приведенном варианте.