1. Удаление rsyslog (пример Ubuntu)

* systemctl disable rsyslog
* systemctl stop rsyslog
* sudo apt purge rsyslog –y

1. Установка и настройка syslog-ng (пример Ubuntu)

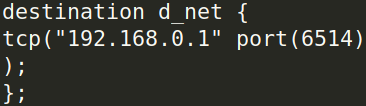
* wget –q0 – <http://download/opensuse.org/repositories/home:/laszlo_budai:/syslog-ng/xUbuntu_17.04/Release.key> | sudo apt-key add –
* sudo vim /etc/apt/source.list.d/syslog-ng.list [*http://download.opensuse.org/repositories/home:/laszlo\_budai:/syslog-ng/xUbuntu\_17.04 ./*](http://download.opensuse.org/repositories/home:/laszlo_budai:/syslog-ng/xUbuntu_17.04%20./)
* sudo apt update
* sudo apt install syslog-ng-core
* update /etc/syslog-ng/syslog-ng.conf

syslog-ng.conf.template

* create /etc/syslog-ng/conf.d/linux-example-file-log.conf

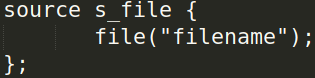
linux-example-file-log.conf.template

* Отредактировать следующую часть конфигурационного файла:



Первым параметром функции tcp должен быть указан IP адрес или доменное имя, по которому для данной машины доступен сервер логов.

* Отредактировать следующую часть конфигурационного файла:



Параметр функции file, должен указывать путь к файлу из которого необходимо читать логи.

Первым параметров функции tcp должен быть указан IP адрес или доменное имя, по которому для данной машины доступен сервер логов.

* systemctl enable syslog-ng
* systemctl start syslog-ng

1. Пояснения

При данной конфигурации каждая строка файла, будет читаться как цельное сообщение. Для дополнительного разбиения на под поля необходимо дополнить файлы linux-example-file-log.conf на клиентской и на серверной машинах соответствующими настройками. Рекомендуется для передачи формат csv (пример windows event log). Для дополнительной информации изучите документацию по следующим ссылкам:

* <https://syslog-ng.com/documents/html/syslog-ng-ose-3.13-guides/en/syslog-ng-ose-guide-admin/html/configuring-sources-file.html>
* <https://syslog-ng.com/documents/html/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/reference-parsers-csv.html>
* <https://syslog-ng.com/documents/html/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/json-parser.html>

Пример парсинга nginx логов:

* <https://habrahabr.ru/post/345968/>