1. Удаление rsyslog (пример Ubuntu)

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

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

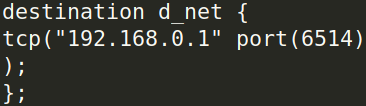
* wget –q0 – <http://download/opensuse.org/repositories/home:/laszlo_budai:/syslog-ng/xUbuntu_17.04/Release.key> | sudo apt-key add –
* sudo vim /etc/apt/source.list.d/syslog-ng.list [*http://download.opensuse.org/repositories/home:/laszlo\_budai:/syslog-ng/xUbuntu\_17.04 ./*](http://download.opensuse.org/repositories/home:/laszlo_budai:/syslog-ng/xUbuntu_17.04%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

linux-event-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.

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