1. Расширение репозитория

* wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
* sudo rpm -Uvh epel-release-latest-7.noarch.rpm

1. Удаление rsyslog

* sudo yum erase rsyslog

1. Установка JDK-8

* sudo yum install java-1.8.0-openjdk.x86\_64
* sudo vim /etc/ld.so.conf.d/java.conf

*/usr/lib/jvm/jre/lib/amd64/server*

* sudo ldconfig

1. Подключение репозитория syslog-ng

* cd /etc/yum.repos.d/
* sudo wget <https://copr.fedorainfracloud.org/coprs/czanik/syslog-ng313/repo/epel-7/czanik-syslog-ng313-epel-7.repo>

1. Подключение репозитория elastic

* cd /etc/yum.repos.d/
* sudo vim elastic.repo

*[elasticsearch-6.x]*

*name=Elasticsearch repository for 6.x packages*

*baseurl=https://artifacts.elastic.co/packages/6.x/yum*

*gpgcheck=1*

*gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch*

*enabled=1*

*autorefresh=1*

*type=rpm-md*

1. Установка и настройка elasticsearch

* sudo yum install elasticsearch
* sudo mkdir /elasticsearchdata/ && sudo chown -R elasticsearch:elasticsearch /elasticsearchdata/
* sudo /sbin/chkconfig --add elasticsearch
* update usr/lib/systemd/system/elasticsearch.service

elasticsearch.service.template

* systemctl daemon-reload
* sudo vim /etc/elasticsearch/jvm.options

*-Xms6g*

*-Xmx6g*

* update /etc/elasticsearch/elasticsearch.yml

elasticsearch.yml.template

* systemctl enable elasticsearch
* systemctl start elasticsearch

1. Установка и настройка kibana

* sudo yum install kibana
* update /etc/kibana/kibana.yml

kibana.yml.template

* systemctl enable kibana
* systemctl start kibana

1. Установка и настройка syslog-ng

* sudo yum install syslog-ng
* sudo yum install syslog-ng-java
* update /usr/lib/systemd/system/syslog-ng.service

syslog-ng.service.template

* systemctl daemon-reload
* 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

* create /etc/syslog-ng/conf.d/windows-event-log.conf

windows-event-log.conf.template

* create /etc/syslog-ng/conf.d/windows-old-event-log.conf

windows-old-event-log.conf.template

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

linux-example-file-log.conf.template

Данный файл содержит пример конфигурации для приема логов из текстовых файлов (см. linix-example-file-client).

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

windows-example-file-log.conf.template

Данный файл содержит пример конфигурации для приема логов из текстовых файлов (см. windows-example-file-client).

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

1. Пояснения

При необходимости индексы и другие конфигурации elasticsearch в конфигурационных файлах syslog-ng могут быть отредактированы. Для лучшего понимания обратитесь к документации:

* <https://syslog-ng.com/documents/html/syslog-ng-pe-latest-guides/en/syslog-ng-pe-guide-admin/html/configuring-destinations-elasticsearch2.html>
* <https://habrahabr.ru/post/280488/>
* <https://www.elastic.co/guide/en/kibana/current/index.html>