Данное руководство описывает настройку клиент серверной системы сбора и хранения логов следующей структуры:

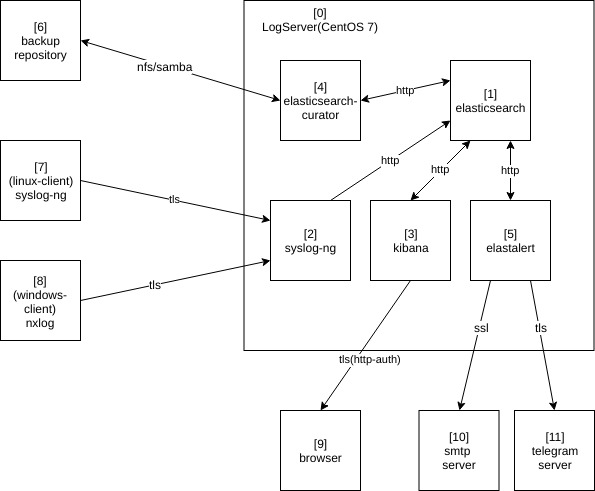


Рисунок 1 - Архитектура системы

1. Сервер логов с операционной системой CentOS 7.
2. NoSQL база данных elasticsearch

* <https://www.elastic.co/products/elasticsearch>

1. Серверная заглушка для сбора логов syslog-ng

* <https://syslog-ng.org/>

1. Web UI для elasticsearch kibana

* <https://www.elastic.co/products/kibana>

1. Command Line UI с поддержкой сценариев для elasticsearch elasticsearch-curator

* <https://www.elastic.co/guide/en/elasticsearch/client/curator/5.4/index.html>

1. Служба оповещений с поддержкой правил для elasticsearch elastalert

* <https://elastalert.readthedocs.io/en/latest/elastalert.html>

1. Удаленное хранилище резервных копий для elasticsearch под управление ОС Linux или Windows
2. Клиент для сбора логов с машин под управлением ОС Linux syslog-ng

* <https://syslog-ng.org/>

1. Клиент для сбора логов с машин под управлением ОС Window nxlog

* <https://nxlog.co/>

1. Пользовательский браузер
2. Почтовый сервер Google

* <https://support.google.com/a/answer/176600?hl=ru>

1. Сервер программы для обмена сообщениями Telegram

* <https://telegram.org/>

Протоколы, с помощью которых составные части обмениваются информацией, изображены на рисунке (Рисунок 1).

Руководство разбито на поддиректории, в которых расположены подруководства для настроек определенных частей системы (Рисунок 2):

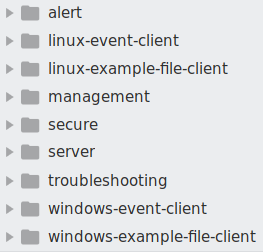


Рисунок 2 – Структура руководства

1. Каталог server содержит руководство по установке и настройке [1], [2] и [3].
2. Каталог linux-event-client содержит руководство по настройке [7] для сбора системных событий ОС Linux
3. Каталог linux-example-file-client содержит руководство по настройке [7] для сбора информации из отдельно взятого файла на ОС Linux
4. Каталог windows-event-client содержит руководство по настройке [8] для сбора системных событий OC Windows
5. Каталог windows-example-file-client содержит руководство по настройке [8] для сбора информации из отдельного взятого файла на ОС Windows
6. Каталог secure содержит руководство по настройке tls соединений между сервером и клиентами, конфигурацией ssl для [3], а также конфигурацией плагина x-pack для включения http аутентификации.
7. Каталог management содержит руководство по настройке [4] для автоматизации создания резервных копий базы данных в хранилище [6], а также по очистке устаревшей информации. Также указанное руководство включает в себя ручное создание резервных копий средствами [3] и плагина x-pack.
8. Каталог alert содержит руководство по настройке [5] для уведомлений о наступлении определенных событий в собираемых логах. Email уведомления реализуются средствами smtp [10], уведомления в telegram средствами сервера [11].
9. Каталог troubleshooting содержит руководство, которое должно помочь преодолеть проблемы, возникающие при настройке сервера.

Внимание: прежде чем приступать к настройке необходимо изучить содержимое всех руководств, чтобы не выполнять одну и туже работу несколько раз!

Далее в данном руководстве (подруководствах) могут встречаться фрагменты текста следующего формата:

* username: user – информация, которой необходимо дополнить целевой конфигурационный файл.
* сonf.template – путь к шаблону конфигурационного файла, начинающийся от файла руководства, в котором он используется. На основе шаблона необходимо сформировать или дополнить целевой конфигурационный файл.
*  - изображение, на основе которого необходимо дополнить целевой конфигурационный файл.

Приступать к изучению руководств в выше указанном порядке.