МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение

высшего образования

**«Северный (Арктический) федеральный университет имени М.В. Ломоносова»**

|  |
| --- |
| Высшая школа информационных технологий и автоматизированных систем |

**ЛАБОРАТОРНАЯ РАБОТА №4**

|  |  |  |
| --- | --- | --- |
| По дисциплине: | | Защита информации в системах управления базами данных |
|  | | |
|  | | |
| На тему | ELK | |
|  | | |
|  | | |

|  |  |
| --- | --- |
|  | Выполнил обучающийся:  Грозов Илья Владимирович |
|  |  |
|  | Направление подготовки / специальность:  10.03.01 Информационная безопасность |
|  |  |
|  | Курс: 3 |
|  | Группа: 151113 |
|  | Руководитель: Зубарев Александр Андреевич, ст. |
|  | преподаватель |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отметка о зачете |  |  |  |  |
|  |  |  |  |  |
| Руководитель |  |  |  | А.А. Зубарев. |
|  |  |  |  |  |

Архангельск 2024

##### Задание

Получить практический навык при работе с ELK

ХОД РАБОТЫ

**1. ELK**

1.1 Конфигурация контейнера с docker

На момент выполнения данной работы установка и работа с docker невозможна. Работа будет выполнена на виртуальной машине с именем huguenot-lr4. Перед установкой выполним установку java при помощи команды: sudo apt install-jre. Установка java отображена на рисунке 1

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 – Установка java

Завершение установки java на виртуальную машину отображено на рисунке 2

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 2 – Завершение установки java

Для работы с пакетами deb небоходимо выполнить установку apt-transport-https. Выполним установку apt-transport-https при помощи команды: sudo apt install apt-transport-https. Установка apt-transport-https отображена на рисунке 3

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Установка apt-transport-https

ElasticSearch невозможно загрузить и установить из России. Воспользуемся зеркалом. Добавим репозиторий в систему при помощи команды: echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list. Добавление репозитория в систему отображено на рисунке 4



Рисунок 4 – Добавление репозитория в систему

Добавим apt ключ при помощи комадны: wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add -. Добавление ключа отображено на рисунке 5

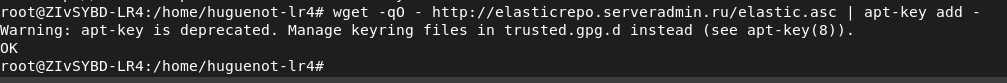


Рисунок 5 – Добавление ключа

Выполним установку из добавленного репозитория при помощи команды: apt update && apt install elasticsearch. Выполнение установки из репозитория отображено на рисунке 6

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 6 – Выполнение установки из репозитория

Процесс установки отображен на рисунке 7

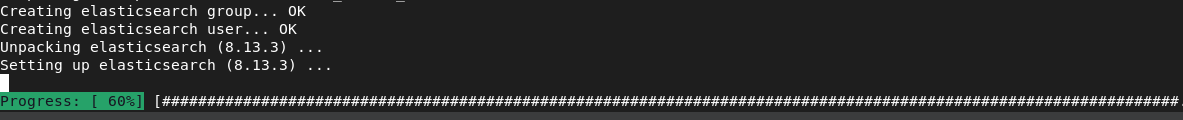


Рисунок 7 – Процесс установки

Добавим ElasticSearch в автозагрузку при помощи последовательного выполнения команд: systemctl daemon-reload, systemctl enable elasticsearch.service, systemctl start elasticsearch.service. Добавление ElasticSearch в автозагрузку отображено на рисунке 8

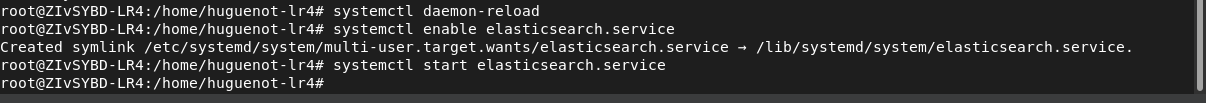


Рисунок 8 – Добавление ElasticSearch в автозагрузку

При помощи команды systemctl status elasticsearch.service проверим запустился ли ElasticSearch. Проверка запуска ElasticSearch отображена на рисунке 9

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 9 – Проверка запуска ElasticSearch

ElasticSearch запущен. Для дальнейшей работы нам потребуется выполним установку curl при помощи команды: apt-get install curl. Установка curl отображена на рисунке 10

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 10 – Установка curl

После установки curl выполним запрос к ElasticSearch при помощи команды: curl -k --user elastic:'N0f4jpvLM2WxQILMMMWM' <https://127.0.0.1:9200>. Ответ кластера отображен на рисунке 11

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 11 – Ответ кластера

1.2 Установка паролей и логинов к системе

Для создания пользователей, установки логинов и паролей в системе нам необходимо дополнительно установить curl jq при помощи команды apt-get install curl jq. Выполнение установки curl jq отображено на рисунке 12

Изображение выглядит как текст, снимок экрана, Шрифт, меню

Автоматически созданное описание

Рисунок 12 – Выполнение установки curl jq

Во время создания пользователей был ошибочно создан пользователь по команде листинга 1

Листинг 1 – Команда

curl -k --user elastic:elastic123 -X POST "https://192.168.100.7:9200/\_security/user/bruno?pretty" -H 'Content-Type: application/json' -d'

{

"password" : "kamisama123",

"roles" : [ "superuser" ],

"full\_name" : "Bruno Ricci",

"email" : "bruno@techexpert.tips"

}

'

Ошибочное создание пользователя отображено на рисунке 13

Изображение выглядит как текст, снимок экрана, черный, Шрифт

Автоматически созданное описание

Рисунок 13 – Ошибочное создание пользователя

Создание нового пользователя было невозможно. Виртуальная машина была возвращена в состояние до изменения настроек пользователя. В дальнейшем была использована предыдущая команда для создания пользователя huguenot. Создание пользователя huguenot отображено на рисунке 14

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 14 – Создание пользователя huguenot

При попытке авторизации было выяснено, что huguenot не является именем пользователя им остается bruno. Данные в команде об имени пользователя не изменялись. Пошлем запрос к ElasticSearch при помощи команды curl -k --user bruno:huguenot123 -X GET "<https://127.0.0.1:9200/_security/user?pretty>" с именем пользователя bruno и паролем huguenot123. Выполнение запроса к ElasticSearch от пользователя bruno отображен на рисунке 15



Рисунок 15 – Выполнение запроса к ElasticSearch от пользователя bruno

Мы получили информацию о пользователях в системе. Ответ на запрос отображен на рисунке 16

Изображение выглядит как текст, снимок экрана, Шрифт, меню

Автоматически созданное описание

Рисунок 16 – Ответ на запрос

1.3 Изменение параметров cluster\_name

Чтобы изменить имя кластера воспользуемся командой: nano /etc/elasticsearch/elasticsearch.yml. Необходимо выполнить редактирование конфигурационного файла. Открытие файла отображено на рисунке 17



Рисунок 17 – Открытие конфигурационного файла

В файле elasticsearch.yml изменим строку cluster.name предварительно раскоментировав ее. Изменим название на huhguenotcluster. Изменение названия кластера отображено на рисунке 18

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 18 – Изменение название кластера

Для вступления в силу изменений остановим ElasticSearch при помощи команды systemctl stop elasticsearch.service и запустим его при помощи команды systemctl start elasticsearch.service. Остановка и запуск ElasticSearch отображены на рисунке 19



Рисунок 19 – Остановка и запуск ElasticSearch

При помощи команды systemctl status elasticsearch.service проверим запустился ли ElasticSearch. Проверка запуска ElasticSearch отображена на рисунке 20

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 20 – Проверка запуска ElasticSearch

Выполним запрос к кластеру для проверки смены его имени при помощи команды: curl -k --user elastic:N0f4jpvLM2WxQILMMMWM -X GET <https://127.0.0.1:9200> Проверка смены имени кластера отображена на рисунке 21

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 21 – Проверка смены имени кластера

Для альтернативного способа проверки имени кластера можно воспользоваться командой: curl -k --user elastic:N0f4jpvLM2WxQILMMMWM -X GET "https://127.0.0.1:9200/\_security/\_cluster/health?pretty Альтернативный способ проверки имени кластера отображен на рисунке 22

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Рисунок 22 – Альтернативный способ проверки имени кластера

1.4 Дополнительные настройки и конфигурация ElasticSearch

Данный раздел зарезервирован под дополнительную настройку ElasticSearch для связи с другими приложениями

**2 KIBANA**

2.1 Установка kibana

Добавим публичный ключ Kibana в систему при помощи команды: wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add – Добавление публичного ключа Kibana отображено на рисунке 23



Рисунок 23 – Добавление публичного ключа Kibana

Если официальный репозиторий недоступен, добавим репозиторий с зеркала при помощи команды: echo "deb http://elasticrepo.serveradmin.ru bullseye main" | tee /etc/apt/sources.list.d/elasticrepo.list Добавление репозитория Kibana с зеркала в систему отображено на рисунке 24



Рисунок 24 – Добавление репозитория Kibana с зеркала в систему

Для добавления публичного ключа Kibana с зеркала воспользуемся командой: wget -qO - http://elasticrepo.serveradmin.ru/elastic.asc | apt-key add – Добавление публичного ключа Kibana с зеркала отображено на рисунке 25



Рисунок 25 – Добавление публичного ключа Kibana с зеркала

Выполним установку Kibana при помощи команды: apt install kibana. Выполнение установки Kibana отображена на рисунке 26

Изображение выглядит как текст, снимок экрана, черный

Автоматически созданное описание

Рисунок 26 – Выполнение установки Kibana

Дополнительно произведем установку утилиты net-tools. Установка утилиты net-tools отображена на рисунке 27

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 27 – Установка утилиты net-tools

При помощи последовательного выполнения команд: systemctl daemon-reload, systemctl enable kibana.service, systemctl start kibana.servic добавим kibana в автозагрузку и запусти его

При помощи команды: netstat -tulnp | grep 5601 что Kibana запущена на порту 5601. Проверка запуска Kibana на порту 5601 отображена на рисунке 28



Рисунок 28 - Проверка запуска Kibana на порту 5601

Выполним GET запрос к Kibana при помощи команды: curl -X GET http://127.0.0.1:5601/\_security /\_cluster/health?pretty. Результат выполненного запроса отображен на рисунке 29

**Изображение выглядит как текст, снимок экрана, черный

Автоматически созданное описание**

Рисунок 29 – Результат выполненного запроса

2.1 Настройка Kibana

Для настройки Kibana выполним редактирование файла конфигурации при помощи команды: nano /etc/kibana/kibana.yml. Открытие файла конфигурации отображено на рисунке 30



Рисунок 30 – Открытие файла конфигурации

Раскоментируем параметр server.host и укажем адрес 0.0.0.0 чтобы было прослушивание всех соединений. Редактирование параметра server.host отображено на рисунке 31

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 31 – Редактирование параметра

Выполним перезагрузку. При помощи команды: /usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana\_system создадим пароль для встроенного пользователя kibana\_system. Создание пароля для пользователя kibana\_system отображено на рисунке 32

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 32 – Создание пароля для пользователя kibana\_system

Укажем автоматически сгенерированный сертификат во время установки elasticsearch. Выполним копирование созданного сертификата из директории /etc/elasticsearch/certs в директорию /etc/kibana при помощи команды: cp -R /etc/elasticsearch/certs /etc/kibana. Для прав используем команду: chown -R root:kibana /etc/kibana/certs. Копирование сертификатов и настройка прав отображено на рисунке 33



Рисунок 33 – Копирование сертификатов и настройка прав

В ранее изменяемом конфигурационном файле kibana добавив информацию о сертификате. Добавление информации о сертификате в конфигурационный файл kibana отображена на рисунке 34

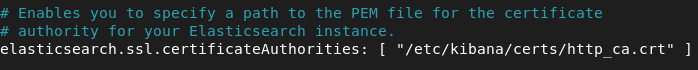


Рисунок 34 – Добавление информации о сертификате в конфигурационный файл kibana

В конфигурационный файл kibana добавим учетную запись пользователя kibana\_system со сгенерированным паролем. Добавление учетной записи пользователя kibana\_system со сгенерированным паролем отображена на рисунке 35

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 35 – Добавление учетной записи пользователя kibana\_system со сгенерированным паролем

В конфигурационный файл kibana укажем подключение по HTTPS. Указание подключения по HTTPS в конфигурационном файле kibana отображено на рисунке 36

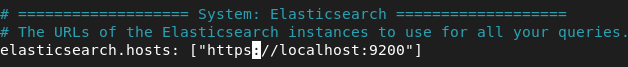


Рисунок 36 – Указание подключения по HTTPS в конфигурационном файле kibana

После чего перезагрузим kibana при помощи команды: systemctl restart kibana.service

Зайдем в web – интерфейс по адресу: 127.0.0.1:5601. Вход в интерфейс по адресу 127.0.0.1:5601 отображен на рисунке 37

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Автоматически созданное описание

Рисунок 37 – Вход в интерфейс по адресу 127.0.0.1:5601

Вход выполняется под учетной записью elastic.

2.3 Составление и отправка запросов

Выполним тестовый запрос предложенный elastic. Предложенный запрос отображен на рисунке 38

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 38 – Предложенный запрос

Результат выполненного тестового предложенного запроса отображен на рисунке 39

**Изображение выглядит как текст, программное обеспечение, снимок экрана, Значок на компьютере

Автоматически созданное описание**

Рисунок 39 – Результат выполненного тестового предложенного запроса

Выполним запрос предложенный лабораторной работой. Предложенный запрос: GET /\_cluster/health?pretty. Результат выполненного запроса отображен на рисунке 40

**Изображение выглядит как текст, программное обеспечение, снимок экрана, веб-страница

Автоматически созданное описание**

Рисунок 40 – Результат выполненного запроса

**3 LOGTASH**

3.1 Установка logtash

Выполним установку logtash при помощи команды: apt install logtash. Выполнение установки logtash отображено на рисунке 41

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

Рисунок 41 – Выполнение установки logtash

Добавим logtash в автозагрузку при помощи команды systemctl enable logstash.service. Добавление logtash в автозагрузку отображено на рисунке 42

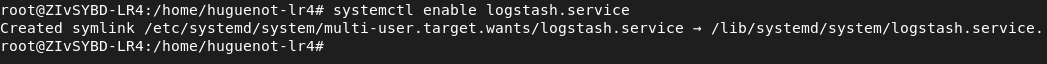
****

Рисунок 42 – Добавление logtash в автозагрузку

3.2 Настройка logtash

Выполним настройку logtash перейдя в папку при помощи команды: cd /etc/logtash/conf.d и создадим файл touch input.conf. Переход в папку conf.d и создание файла input.conf отображено на рисунке 43

****

Рисунок 43 – Переход в папку conf.d и создание файла input.conf

Откроем созданный файл conf.d при помощи команды nano input.conf. Открытие файла conf.d отображено на рисунке 44

****

Рисунок 44 – Открытие файла input.conf

Конфигурация файла input.conf отображена на рисунке 45

**Изображение выглядит как текст, снимок экрана, черный, Шрифт

Автоматически созданное описание**

Рисунок 45 – Открытие файла input.conf

Создадим файл output.conf при помощи команды: touch output.conf. Создание файла output.conf отображено на рисунке 46

****

Рисунок 46 - Создание файла output.conf

Конфигурация файла output.conf отображена на рисунке 47

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

Рисунок 47 – Конфигурация файла output.conf

Выполним копирование сертификатов и назначим права при помощи команд: cp -R /etc/elasticsearch/certs /etc/logstash и chown -R root:logstash /etc/logstash/certs. Копирование сертификатов и назначение прав отображено на рисунке 48

****

Рисунок 48 – Копирование сертификатов и назначение прав

При помощи команды: touch создадим файл filter.conf. Создание файла filter.conf отображено на рисунке 49

****

Рисунок 49 – Создание файла filter.conf

Конфигурация файла filter.conf отображена на рисунке 50

**Изображение выглядит как текст, черный, снимок экрана

Автоматически созданное описание**

Рисунок 50 – Конфигурация файла filter.conf

Настройка logtash завершена. Перезапустим logtash при помощи команды: ystemctl start logstash.service. Перезапуск logtash отображен на рисунке 51

****

Рисунок 51 – Перезапуск logtash

При помощи команды: cat /var/log/logstash/logstash-plain.log проверим лог logtash. Лог logtash отображен на рисунке 52

**Изображение выглядит как текст, снимок экрана, черно-белый, Шрифт

Автоматически созданное описание**

Рисунок 52 – Лог logtash

Успешный запуск logtash отображен на рисунке 53

****

Рисунок 53 – Успешный запуск logtash

3.3 Данный пункт зарезервирован под дополнительные настройки

**4 NGINX**

4.1 Установка и настройка nginx

Выполним установку nginx при помощи команды: apt install nginx. Установка nginx отображена на рисунке 54

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

Рисунок 54 – Установка nginx

Установленный nginx отображен на рисунке 55

**Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание**

Рисунок 55 – Установленный nginx

Добавим nginx в автозагрузку при помощи команды: systemctl enable nginx. Добавление nginx в автозагрузку отображено на рисунке 56

****

Рисунок 56 – Добавление nginx в автозагрузку

Запустим nginx при помощи команды: systemctl start nginx. Запуск nginx отображен на рисунке 57

****

Рисунок 57 – Запуск nginx

При помощи команды: systemctl status nginx проверим, запущен ли nginx. Проверка запуска nginx отображена на рисунке 58

**Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание**

Рисунок 58 - Проверка запуска nginx

Перейдем по адресу: 127.0.0.1:80. Переход на адрес 127.0.0.1:80 отображен на рисунке 59

**Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание**

Рисунок 59 – Переход на адрес 127.0.0.1:80

4.2 Отправка access-лог nginx в Elasticsearch с помощью Logstash

Для отправки access-лог nginx в Elasticsearch с помощью Logstash изменим файл конфигурации input.conf. Измененная конфигурация файла input.conf отображена на рисунке 60

Изображение выглядит как текст, программное обеспечение, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 60 – Измененная конфигурация файла input.conf

Остановим и запустим logtash.service при помощи команд systemctl stop logtash.service и systemctl start logtash.service тем самым выполнив перезапуск. Перезапуск logtash.service отображен на рисунке 61



Рисунок 61 – Перезапуск logtash.service

При помощи команды: cat /var/log/logstash/logstash-plain.log проверим лог logtash. Лог logtash отображен на рисунке 62



Рисунок 62 – Лог logtash

В логе logtash замечена ошибка на доступ к файлу из-за прав, по этой причине нету доступа к логам. Исправим ошибку выдав необходимые права при помощи команды: sudo chmod o+r /var/log/nginx/access.log. Выдача необходимых прав отображена на рисунке 63



Рисунок 63 – Выдача необходимых прав

Остановим и запустим logtash.service при помощи команд systemctl stop logtash.service и systemctl start logtash.service тем самым выполнив перезапуск. Перезапуск logtash.service отображен на рисунке 64



Рисунок 64 – Перезапуск logtash.service

Перейдем в панель управления ElasticSearch. Переход в панель управления ElasticSearch отображен на рисунке 65

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 65 – Переход в панель управления ElasticSearch

Продолжим настройку. В поле name укажем nginx, а в поле index pattern укажем websrv-\*. Продолжение настроек отображено на рисунке 66

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 66 – Продолжение настроек

Перейдем в раздел Discover в который начали поступать логи от nginx. Поступающих логи отображены на рисунке 67

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 67 – Поступающие логи

Логи nginx отображены на рисунке 68

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 68 – Логи nginx

**5 FILEBEAT ДЛЯ ОТПРАВКИ ЛОГОВ В LOGSTASH**

5.1 Установка filebeat

Выполним установку filebeat при помощи команды: apt install filebeat. Установка filebeat отображена на рисунке 69

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 69 – filebeat

5.2 Настройка filebeat

Для настройки filebeat вернемся к редактированию файла конфигурации logstash. Удалим активную конфигурацию и раскомментируем предыдущую. Изменение файла конфигурации logstash отображено на рисунке 70

Изображение выглядит как текст, программное обеспечение, Мультимедийное программное обеспечение, снимок экрана

Автоматически созданное описание

Рисунок 70 – Изменение файла конфигурации

Измененная конфигурация logstash файла input.conf отображена на рисунке 71

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 71 – Измененная конфигурация logstash файла input.conf

Для вступления изменений в силу выполним перезагрузку logstash при помощи команды: systemctl reload logstash.service. Выполнение перезагрузки logstash отображено на рисунке 72

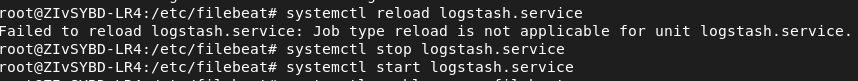


Рисунок 72 – Выполнение перезагрузки logstash

5.3 Настройка поставки логов через filebeat

Выполним настройку конфигурационного файла filebeat.yml находящегося в директории /etc/filebeat при помощи команды nano. Открытие файла конфигурации отображено на рисунке 73



Рисунок 73 – Открытие файла конфигурации

В разделе filebeat inputs файла конфигурации filebeat.yml установим значение enable на true. Укажем путь до файла с логами nginx. Редактирование раздела filebeat inputs файла конфигурации filebeat.yml отображено на рисунке 74

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 74 – Редактирование раздела filebeat inputs файла конфигурации filebeat.yml

В разделе filebeat modules файла конфигурации filebeat.yml оставляем все значения без изменений Редактирование раздела filebeat modules файла конфигурации filebeat.yml отображено на рисунке 75

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 75 – Редактирование раздела filebeat modules файла конфигурации filebeat.yml

В разделе outputs файла конфигурации filebeat.yml необходимо обязательно закомменитировать строки относящиеся к elasticsearch иначе при запуске возникнет ошибка не позволяющая передавать логи. Строки logstash необходимо раскомментировать и указать ip адрес или localhost в нашем случае. Редактирование раздела outputs файла конфигурации filebeat.yml отображено на рисунке 76

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 76 – Редактирование раздела outputs файла конфигурации filebeat.yml

В разделе processor файла конфигурации filebeat.yml конфигурацию оставляем без изменений. Редактирование раздела outputs файла конфигурации filebeat.yml отображено на рисунке 77

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 77 – Редактирование раздела outputs файла конфигурации filebeat.yml

Добавим filebeat в автозагрузку при помощи команды: systemctl enable –now filebeat. Добавление filebeat в автозагрузку отображено на рисунке 78

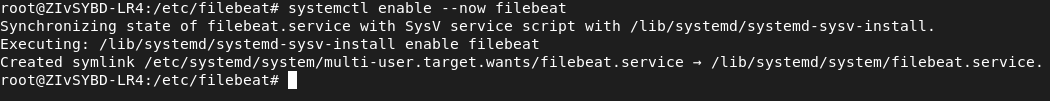


Рисунок 78 – Добавление filebeat в автозагрузку

Проверим статус filebeat при помощи команды systemctl statuss filebeat. Проверка статуса filebeat отображена на рисунке 79

Изображение выглядит как текст, черный, Мультимедийное программное обеспечение, снимок экрана

Автоматически созданное описание

Рисунок 79 – Проверка статуса filebeat

Filebeat запущен и работает. Все данные об log access nginx передаются в elasticsearch. Вернемся в панель elasticsearch, обновим страницу. Данные log access nginx поступают исправно. Поступающие данные log access nginx отображены на рисунке 80

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описание

Рисунок 80 – Поступающие данные log access nginx

Один из логов nginx access приведен на рисунке 81

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 81 – Лог nginx access

**6 НАСТРОЙКА ПОСТАВКИ ЛОГА В ELASTICSEARCH ЧЕРЕЗ LOGSTASH И FILEBEAT**

6.1 Раздел был зарезервирован для настойки поставки логов с Windows при помощи Winlogbeat

Во время настройки возникли неполадки не позволяющие продолжить сбор и поставку логов при помощи Winlogbeat в ElasticSearch. Описательная часть отсутствует

6.2 Парсинг лога и разложение на поля

Дополнительный раздел к предыдущим пунктам, описывающий процесс парсинга лога и разложение его на поля

{

"@timestamp": [

"2024-06-06T16:39:17.717Z"

],

"@version": [

"1"

],

"@version.keyword": [

"1"

],

"event.original": [

"127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0\""

],

"event.original.keyword": [

"127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0\""

],

"host.name": [

"ZIvSYBD-LR4"

],

"host.name.keyword": [

"ZIvSYBD-LR4"

],

"log.file.path": [

"/var/log/nginx/access.log"

],

"log.file.path.keyword": [

"/var/log/nginx/access.log"

],

"message": [

"127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0\""

],

"message.keyword": [

"127.0.0.1 - - [06/Jun/2024:19:39:17 +0300] \"GET / HTTP/1.1\" 200 396 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0\""

],

"tags": [

"\_geoip\_lookup\_failure"

],

"tags.keyword": [

"\_geoip\_lookup\_failure"

],

"\_id": "x3Rr7o8BudhOdipTQ6pu",

"\_index": "websrv-2024.06",

"\_score": null

}

6.3 Изменение файлов конфигурации

6.3.1 Изменение файла конфигурации

6.3.2 Изменение файла конфигурации

6.3.3 Изменение файла конфигурации

6.3.4 Изменение файла конфигурации

6.4 Проверка поступающих логов в ElascticSearch

КОНТРОЛЬНЫЕ ВОПРОСЫ

ВЫВОД

В ходе выполнения лабораторной работы по теме: «ELK» получили практический навык при работе с ELK