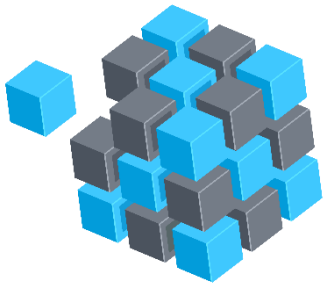

# Сопровождение и эксплуатация ИндексЛог

# Оглавление

# Проверка работоспособности компонентов стека

## Проверка работоспособности ИндексЛог_Поиск.

Проверку доступности ИндексЛог_Поиск можно осуществлять по настроенному порту (по умолчанию 9200). При включенном шифровании HTTP-соединений (включено по умолчанию) убедитесь, что используете HTTPS запрос, иначе запрос будет отклонен. --cacert это путь к сгенерированному сертификату http_ca.crt

```
curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic
https://localhost:9200
```

Введите автоматически сгенерированный пароль пользователя elastic. Вы должны получить следующий ответ:

```
{
  "name" : "Cp8oag6",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "AT69_T_DTp-1qgIJlatQqA",
  "version" : {
    "number" : "8.6.2",
    "build_type" : "tar",
    "build_hash" : "f27399d",
    "build_flavor" : "default",
    "build_date" : "2016-03-30T09:51:41.449Z",
    "build_snapshot" : false,
    "lucene_version" : "9.4.2",
    "minimum_wire_compatibility_version" : "1.2.3",
    "minimum_index_compatibility_version" : "1.2.3"
  },
  "tagline" : "You Know, for Search"
}
```

Более подробные данные о состоянии кластера можно получить с помощью API-запросов. Удобнее всего их отправлять через консоль разработчика в ИндексЛог_Аналитика:

```
GET _cluster/health

GET /_health_report
```

## Проверка работоспособности ИндексЛог_Аналитика.

Проверка работоспособности ИндексЛог_Аналитика осуществляется путем проверки доступности веб-интерфейса. Доступ к интерфейсу Kibana можно получить через браузер по адресу http://<mydomain>:5601. Для доступа в интерфейс Kibana используется логин и пароль от учетной записи пользователя ИндексЛог.

## Проверка работоспособности агента ИндексЛог и сервера ЦУА.

Проверка доступности всех агентов ИндексЛог и сервера централизованного управления осуществляется в веб-интерфейсе ИндексЛог Аналитика во вкладку Управление > Агенты. В этой вкладке выводится информация об управляемых с помощью сервера агентах ИндексЛог, а именно: имя хоста, статус, политика, версия и время последней активности.Сервер ЦУА отображается в этом интерфейсе как агент с политикой сервера централизованного управления.

## Проверка состояния кластера с помощью Наблюдателя.

ИндексЛог_Наблюдатель это инструмент для выполнения автоматических действий при соблюдении заданных условий. Проверка (watch) состоит из следующих компонентов:

- Trigger – определяет, при каком условии активируется проверка;
- Input – загружает данные в буфер проверки;
- Condition – определяет, при каком условии будут выполняться действия;
- Transform – преобразует содержание буфера перед действием;
- Action – определяет действия, выполняемые при соблюдении условий.

Пример проверки состояния кластера каждые 10 секунд:

```
PUT _watcher/watch/cluster_health_watch
{
  "trigger" : {
    "schedule" : { "interval" : "10s" }
  },
  "input" : {
    "http" : {
      "request" : {
       "host" : "localhost",
       "port" : 9200,
       "path" : "/_cluster/health"
      }
    }
  },
  "condition" : {
    "compare" : {
      "ctx.payload.status" : { "eq" : "red" }
    }
  },
  "actions" : {
    "send_email" : {
      "email" : {
        "to" : "username@example.org",
        "subject" : "Cluster Status Warning",
        "body" : "Cluster status is RED"
      }
    }
  }
}
```

Чтобы Watcher мог отправлять электронные письма, необходимо задать конфигурацию электронной почты в elasticsearch.yml.

```
xpack.notification.email.account:
  work:
    profile: gmail
    email_defaults:
      from: <email>
    smtp:
      auth: true
      starttls.enable: true
      host: smtp.gmail.com
      port: 587
      user: <username>
```

```
      password: <password>
```
в данном примере <email> отвечает за адрес электронной почты, с которого будут отправляться сообщения, <username> обозначает имя пользователя аккаунта (обычно адрес gmail), а <password> - пароль от аккаунта gmail.

## Логирование стека ИндексЛог

Логи каждой ноды ИндексЛог_Поиск находятся в /var/log/elasticsearch. Для ИндексЛог_Аналитика - /var/log/kibana.

Логирование каждого агента ИндексЛог и сервера централизованного управления агентами осуществляется отдельно. Для записи лога при установке агента разрешите сбор логов и метрик агента. Удобнее всего просматривать логи агентов в интерфейсе ИндексЛог_Аналитика во вкладке Управление > Агенты.

### Инструкция по выводу лога

Можно посмотреть содержимое логов следующими способами:

Вывод всего текста лога в консоль (лог пролистывается полностью с начала и до конца)

```
cat имя_лога
```
Пример:

```
cat /var/log/elasticsearch/elasticsearch.log
```
Вывод последних 10 строк файла.

```
tail имя_лога
```
Вывод произвольного количества строк файла (для примера 50)

```
tail -т 50 имя_лога
```
Вывод строк в режиме реального времени (вывод строк по мере их добавления)

```
tail -f имя_лога
```
Просмотр списка файлов в директории

```
ls -lah путь_к_директории
```
Например:

```
ls -lah /var/log/
```
Также для просмотр могут быть использованы текстовые редакторы вроде nano, vi,vim, mcview

## Мониторинг стека ИндексЛог

Так как ИндексЛог представляет собой в том числе решение по мониторингу логов и инфраструктуры, мониторинг стека ИндексЛог можно осуществлять его же инструментами.

Среди интеграций для унифицированного агента ИндексЛог присутствуют интеграции для мониторинга компонентов стека. Установите эти интеграции так же, как любые другие и используйте встроенные дэшборды или собственные визуализации для мониторинга стека.

Рекомендуется в продуктивных средах отслеживать основной кластер ИндексЛог с помощью дополнительного кластера, предназначенного только для мониторинга ИндексЛог. При такой конфигурации в случае отказа основного кластера, кластер мониторинга будет работать и зафиксирует сбой в работе основного кластера.