

Настройка Alertmanager

Общие сведения

Настройка Alertmanager производится как с помощью ключей, так и с помощью конфигурационного файла. Формат – yaml. В конфигурационном файле настраивается вся обработка алертов. Конфигурационный файл может содержать 5 блоков. Далее рассмотрим каждый блок отдельно.

Блок global

resolve_timeout

default: 5m Время, через которое алерт считается решенным, если в течение этого времени он не был обновлен.

smtp_from default: – email адрес, который будет использован в качестве адреса отправителя. В блоке global объявляются значения по умолчанию, переопределить которые можно в блоке receiver.

smtp_smarthost

default:

Адрес SMTP сервера, который используется для отправки. Формат: ip:port . В блоке global объявляются значения по умолчанию, переопределить которые можно в блоке receiver.

smtp_require_tls

default: true

Задает, использовать ли tls при подключении к SMTP. **NB!** Обратите внимание, что значение по умолчанию true и при использовании с локально установленным postfix без дополнительных настроек работать не будет.

Также в этой секции возможно настроить отправку уведомлений в: slack, hipchat, pagerduty и другие мессенджеры. Но для настройки получателей рекомендуется использовать webhook. Его настройка возможна только в разделе receivers.

Блок route

В блоке `route` производится маршрутизация сообщений. В результате получается древовидная структура.

receiver

Имя конфигурации, которая будет использована для отправки уведомлений.

group_by

Набор меток, по которым производится агрегация. Значение `['...']` отключает группировку.

continue

default: `false`

Если значение `false`, обработка уведомления прекращается при первом совпадении. Если значение `true`, обработка продолжается и выбирается последний `route`, удовлетворяющий условиям.

match

Список меток `key: value`, при точном совпадении с которыми выбирается этот маршрут.

match_re

Список меток `key: regex`, при совпадении с которыми выбирается этот маршрут.

group_wait

Default: `30s`

Время задержки перед отправкой сообщений для группы. Позволяет дождаться поступления большего числа алертов и произвести эффективную группировку.

group_interval

default: `5m`

Время задержки для отправки новых уведомлений, по которым первоначальное уведомление уже было отправлено.

repeat_interval

default: `4h`

Время задержки для повторной отправки уведомления.

routes

Дополнительные маршруты. Не являются обязательными.

Пример:

```
route:
  receiver: 'default-receiver'
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 4h
  group_by: [cluster, alertname]
  routes:
  - receiver: 'db-team'
    group_wait: 10s
    match_re:
      service: mysql|postgres
  - receiver: 'frontend-team'
    group_by: [product, environment]
    match:
      team: frontend
```

В этом примере все уведомления labels service со значениями mysql или postgres будут отправлены db-team. Уведомления, имеющие label team со значением frontend, будут отправлены frontend-team. Остальные уведомления будут отправлены получателю по умолчанию.

Блок receivers

Receiver – это именованная конфигурация одного или нескольких получателей уведомлений. На данный момент имеется интеграция с несколькими мессенджерами: slack, hipchat, pagerduty и др. Но для настройки получателей рекомендуется использовать webhook. В настройках указываются данные для отправки. Пример настройки email будет рассмотрен в следующем шаге.

Блок inhibit_rules

Блок inhibit_rules позволяет отключить уведомления для алертов, у которых labels соответствуют набору labels, указанных в target_match(_re), и при условии, что уже есть уведомление, у которого набор labels соответствуют набору labels, указанных в source_match(_re).

target_match

Список labels, при совпадении с которым сообщение будет отключено.

target_match_re

Список labels, при совпадении с которым сообщение будет отключено. Для проверки используется регулярное выражение.

source_match

Набор меток, для которых уже должен существовать алерт, чтобы правило подавления работало.

source_match_re

Набор меток, для которых уже должен существовать алерт, чтобы правило подавления работало. Для проверки используется регулярное выражение.

equal

Набор label, которые должны совпадать в alert и inhibit alert, чтобы подавление работало.

Блок templates

В данном блоке задается список путей для файлов с пользовательскими шаблонами уведомлений. Допускается использование маски.

Пример:

templates:

- 'templates/*.tmpl'