Настройка alertmanager

Практика выполняется на monitoring сервере, доступ к нему осуществляется по **IP** адресу и выполняется с root привилегиями.

1. Сохраним конфигурационный файл

Перед началом настройки, необходимо подтвердить пользовательское соглашение для email, с которого будут отправляться email уведомления. Для этого перейдите по ссылке, авторизируйтесь и подтвердите соглашение. Для авторизации - имя пользователя <user name>@edu-prom.slurm.io, а пароль совпадает с паролем ssh. Данные можно посмотреть в личном кабинете.

Выполним команду для создания правил алертинга. Перед выполнением необходимо поменять: <email_1> и <email_2> на реальные email (если нет двух разных email, можно указать один), а так же заменить <user name>, <Password>. Значения можете посмотреть в личном кабинете.

```
cat <<EOF > /etc/alertmanager/alertmanager.yml
global:
  smtp_smarthost: smtp.yandex.ru:465
  smtp_from: '<user name>@edu-prom.slurm.io'
  smtp_auth_username: '<user name>@edu-prom.slurm.io'
  smtp_auth_password: '<Password>'


route:
  group_by: ['alertname', 'service']
  group_wait: 30s
  group_interval: 5m
  repeat_interval: 1h
  receiver: team-monitoring

  routes:
  - match:
      service: prom
    receiver: team-ops
  - match:
      severity: (warnings|error|critical)
    receiver: team-monitoring

inhibit_rules:
- source_match:
```

```
    severity: 'critical'
    alertname: PrometheusConfigurationReload
  target_match:
    severity: 'error'

receivers:
- name: 'team-ops'
  email_configs:
    - to: '<email_1>'
      send_resolved: true
      require_tls: false
- name: 'team-monitoring'
  email_configs:
    - to: '<email_2>'
      send_resolved: true
EOF
```

Данная конфигурация использует группировку по alertname и service. Все сообщения с label service: prom будут отправлены на email_1, все алерты с label severity: critical, error и warning будут отправлены на email_2. Если есть алерт с label service: prom и alertname: PrometheusConfigurationReload, остальные алерты отправляться не будут.

NB! В реальной жизни routing будет намного сложнее, и для его визуализации можно воспользоваться сайтом.

2. Выполните reload для Alertmanager, чтобы применить новые настройки:

systemctl reload alertmanager.service

3. Тестирование.

3.1 Исправляем конфиг Prometheus.

Добавляем в начало конфигурационного файла Prometheus: 1. И выполняем:

systemctl reload prometheus.service

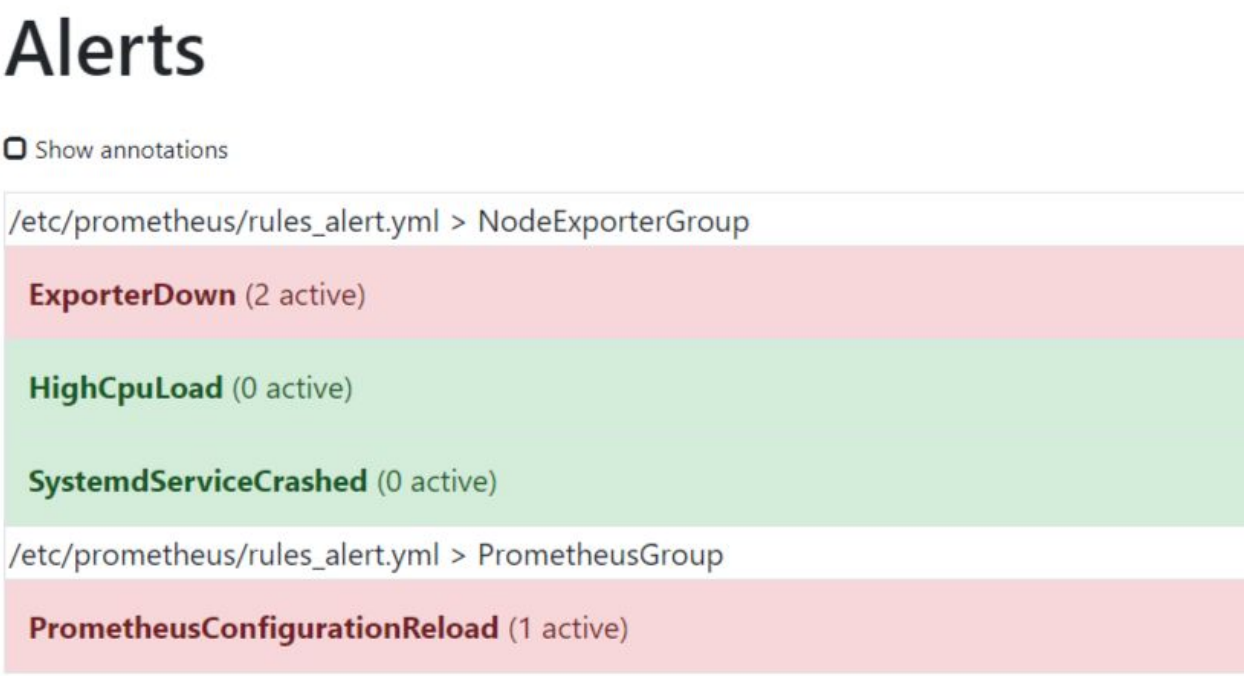
Это приведет к отправке алерта об ошибке в конфигурационном файле Prometheus.

3.2 Останавливаем node exporter.

Останавливаем node exporter на monitoring и server1, выполнив команду.

systemctl stop node_exporter.service

Теперь необходимо дождаться, пока отработает alert rule. Для проверки перейдите: http://<monitoring_IP>:9090/alerts. Должно быть активно два алерта.



При этом новых алертов приходить не должно, так как работает подавление.

3.3 Исправляем конфигурационный файл: /etc/prometheus/prometheus.yml, удаляем 1. И выполняем:

systemctl reload prometheus.service

Теперь должно прийти еще 2 уведомления: первое – об исправлении с конфигурацией Prometheus, второе – о недоступности двух exporters.