1. Настройка оповещений средствами Elastic Watcher (должен быть установлен x-pack (см. secure.docx)):

* update /etc/elasticsearch/elasticsearch.yml

elasticsearch.yml.template

* В учетной записи gmail разрешить доступ для «ненадежных» приложений.
* В интерфейсе kibana перейти в раздел Managment, выбрать вкладку Watcher, нажать на кнопку Create new watch и сконфигурировать параметры уведомлений (Рисунок 1).

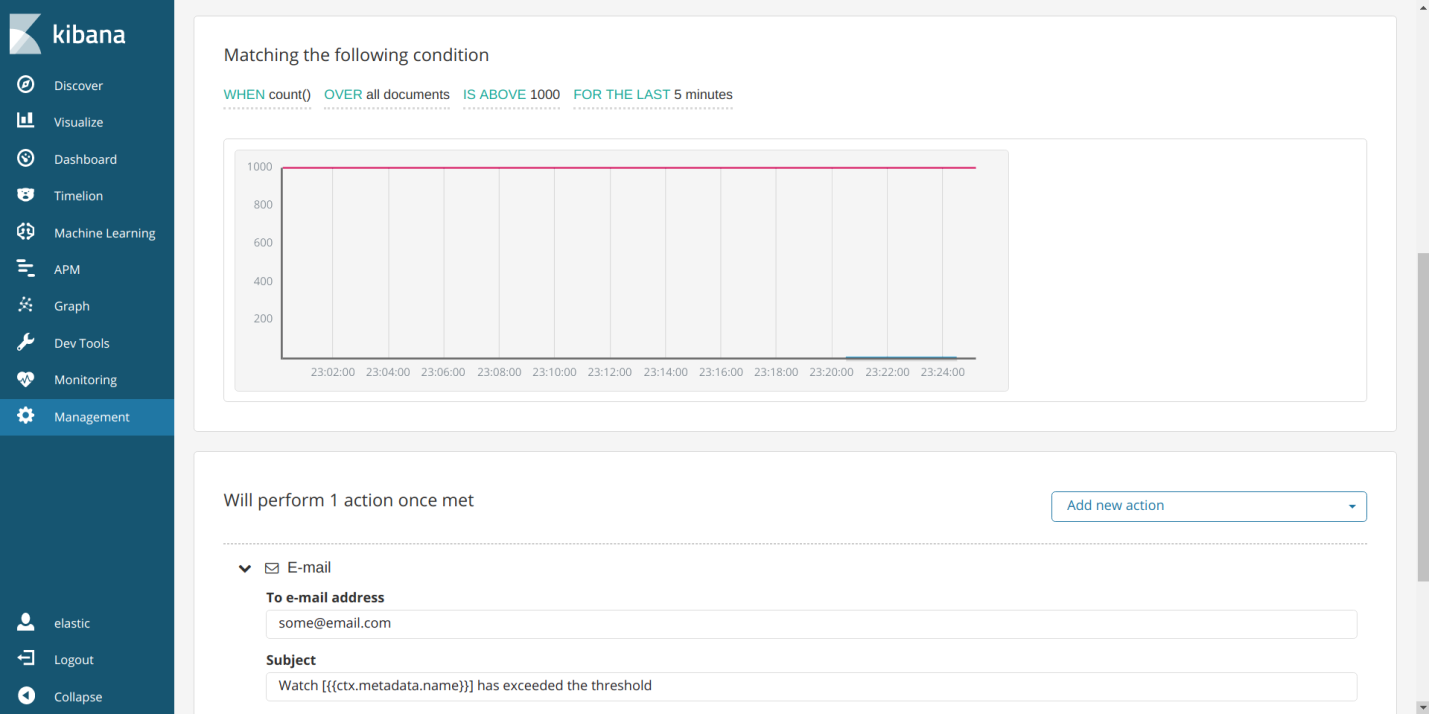


Рисунок 1 – Watcher

Функционал Elastic Watcher не отличается гибкостью, поэтому рекомендуется ознакомиться с функциональностью elastalert.

1. Установка elastalert:

* sudo yum install python2-pip
* sudo yum install gcc
* sudo yum install python-devel
* sudo pip install --upgrade pip
* sudo pip install «setuptools>=11.3»
* sudo pip install «elasticsearch>=5.0.0»
* sudo pip install «urllib3<1.23,>=1.21.1»
* sudo pip install elastalert
* sudo mkdir /etc/elasticalert
* create /etc/elasticalert/config.yaml

config.yaml.template

* create /etc/elasticalert/email.yaml

email.yaml.template

* В учетной записи gmail разрешить доступ для «ненадежных» приложений.
* elastalert-create-index
* sudo mkdir /etc/elasticalert/rules
* create /etc/elasticalerts/rules/example\_alert.yaml

example\_alert.yaml.template

* sudo chown -R elasticsearch:elasticsearch /etc/elasticalert/
* create /etc/systemd/system/elastalert.service

elastalert.service.template

* systemctl daemon-reload
* systemctl enable elastalert
* systemctl start elastalert

В данном примере elastalert настроен на отправку уведомления по email и telegram при появлении в индексе u-i-event-linux-log, новой записи со значением info поля PRIORITY. Elastalert куда более гибкий инструмент, чем Watcher, он позволяет писать условия высокой логической сложности и отправлять уведомления множеством способов включая bash (curl), HTTP REST, email, telegram и другие. Для лучшего понимания конфигурационных файлов этой утилиты обращаться к документации:

* <https://elastalert.readthedocs.io/en/latest/elastalert.html>
* <https://habrahabr.ru/company/southbridge/blog/255845/>