ELASTALERT

DOCUMENTAZIONE

E’ un **framework** per l’ alerting a seguito di anomalie o pattern di interesse rilevati nei dati in **Elasticsearch**. Esso combina Elasticsearch con due diversi componenti: *rule types* e *alerts.*

Elasticsearch viene sottoposto periodicamente a *queries*; in seguito i dati raccolti vengono passati al rule type che consente di individuare i match. Dopodiché se un match viene individuato, esso viene passato ad uno o più alert i quali generano azioni basate su tale match.

E’ un servizio che, con una frequenza settata nel file di configurazione, sottopone elasticsearch (i log che esso gestisce) a delle query. Il tipo di query dipende dai parametri che sono stati settati nella regola; lo stesso vale per il tipo di azione da eseguire nel momento in cui viene rilevato un match.

RULE TYPES

1. “Match where there are X events in Y time” (frequency type)
2. “Match when the rate of events increases or decreases” (spike type)
3. “Match when there are less than X events in Y time” (flatline type)
4. “Match when a certain field matches a blacklist/whitelist” (blacklist and whitelist type)
5. “Match on any event matching a given filter” (any type)
6. “Match when a field has two different values within some time” (change type).

ALERT TYPES

Alerta, Alertmanager, AWS SES (Amazon Simple Email Service), AWS SNS (Amazon Simple Notification Service), Chatwork, Command, Datadog, Debug, Dingtalk, Discord, Email, Exotel, Gitter, GoogleChat, HTTP POST, HTTP POST 2, Jira, Line Notify, Mattermost, Microsoft Teams, OpsGenie, PagerDuty, PagerTree, Rocket.Chat, Squadcast,

ServiceNow, Slack, Splunk On-Call (Formerly VictorOps), Stomp, Telegram, Tencent SMS, TheHive, Twilio, Zabbix.

RUNNING AS A PYTHON PACKAGE

Prerequisiti:

- Elasticsearch.
- ISO8601 or Unix timestamped data.

Installazione:

```
$ sudo apt-get install -y python
$ sudo apt-get install python3-pip python3-dev libffi-dev libssl-dev
$ git clone https://github.com/Yelp/elastalert.git
$ cd elastalert
$ sudo pip install "setuptools>=11.3"
$ sudo pip install pyOpenSSL
$ sudo pip install "elasticsearch>=5.0.0"
$ cp config.yaml.example config.yaml
```

Configurazione:

Nella directory *elastalert* creare una nuova cartella *rules*.

Nel file di configurazione *config.yaml:*

- rules_folder: *rules*
- run_every: *frequenza*
- es_host: *localhost*
- es_port: *9200*

Creare un indice per ElastAlert:

```
$ elastalert-create-index
```

Copiare una delle regole, in base all'obiettivo che si vuole raggiungere, presenti in *example_rules*, nella cartella *rules*. Modificarne opportunamente i parametri relativi ai match e alle azioni da mettere in atto.

Testare la regola inserita per capire se il file di configurazione la carica in maniera opportuna.

```
$ elastalert-test-rule --config config.yaml rules/example_frequency.yaml
```

Infine se tutto è andato a buon fine è possibile invocare ElastAlert direttamente tramite python:

```
$ python -m elastalert.elastalert --verbose --rule example_frequency.yaml
```