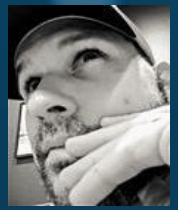
IT/Dev CONNECTIONS

It's Called ElasticSearch

what do you mean you use it for analytics?



Adam Dockter
VP of Engineering
ServiceTarget

Delivered by KNect365 TMT an Informa business

Who are we?

ServiceTarget

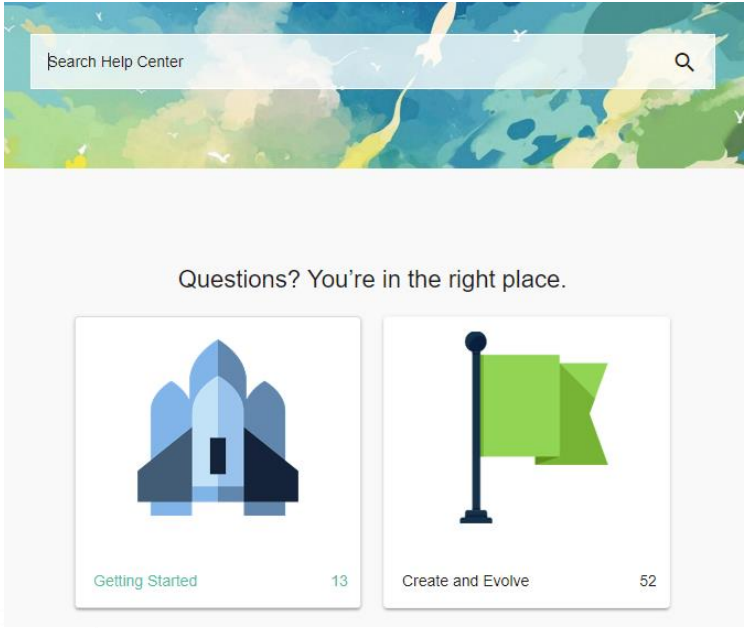
Small Company 4 Developers

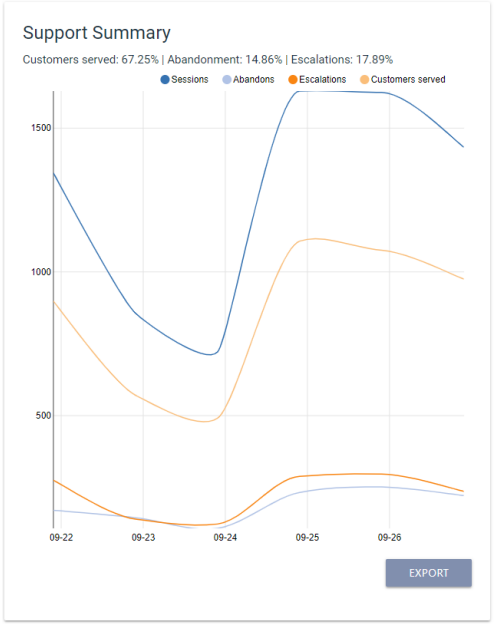
AWS Infrastructure

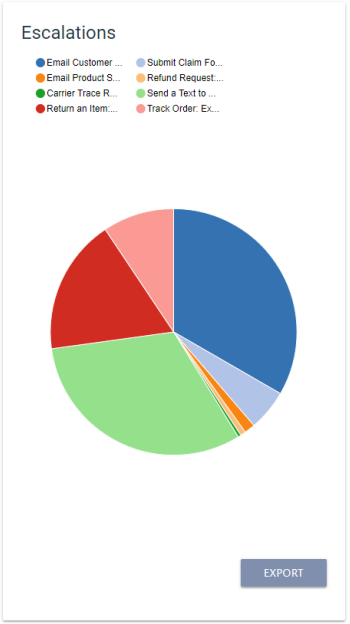
NO QA!!

About our product

Self service web application powered by analytics







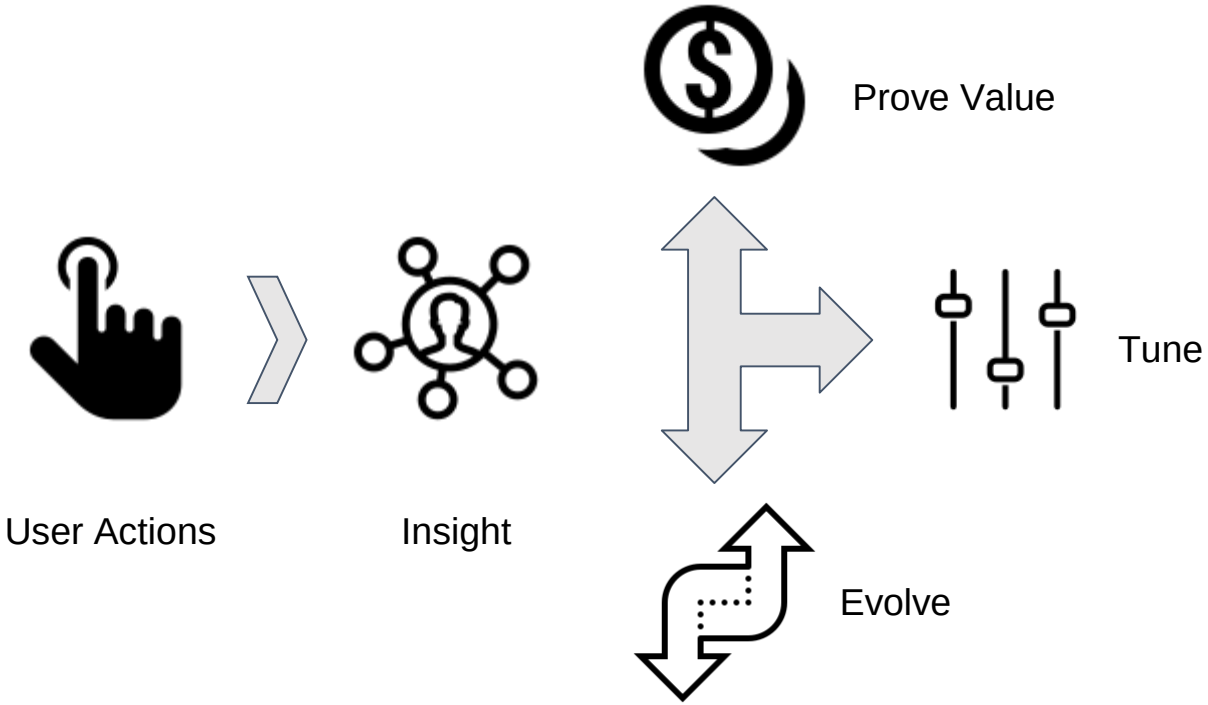
Why Elasticsearch for analytics

A familiar product and infrastructure

fast near real time queries
full visibility and control of data

testability - e2e, unit test and integration tests

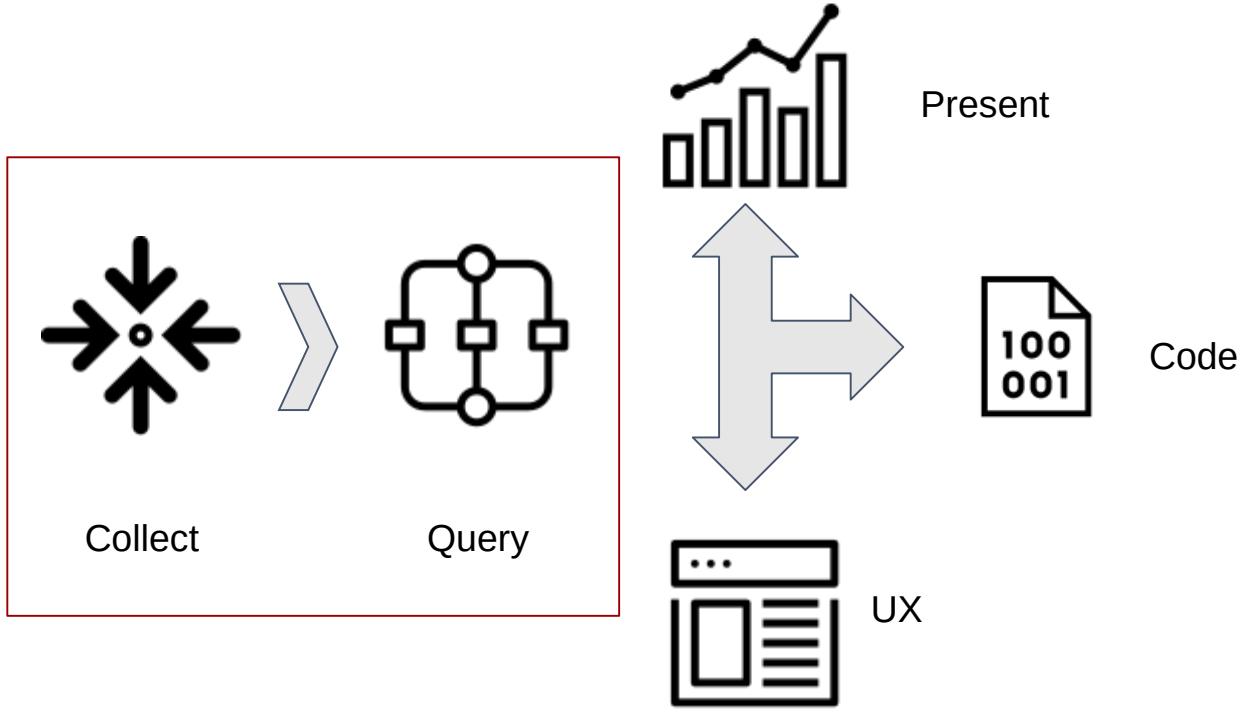
What are our analytics?



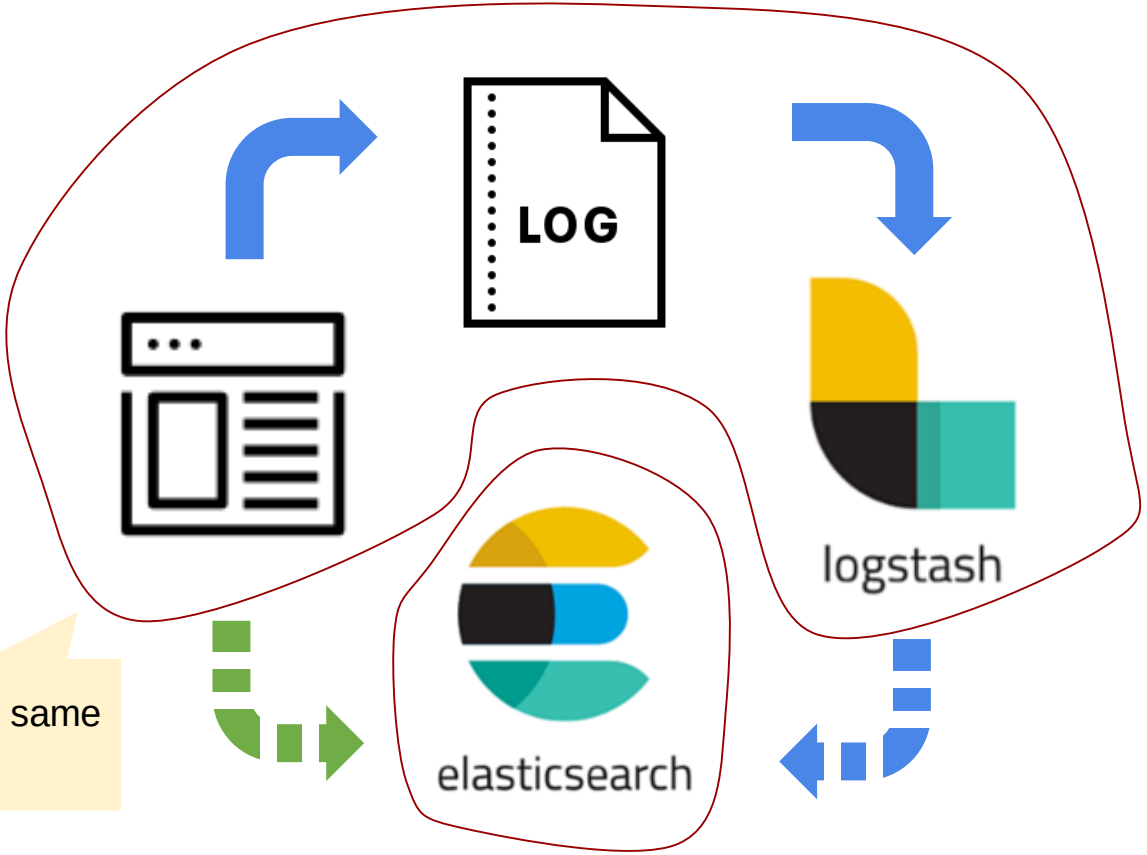
What are our analytics?

DEMO

How do we go about it?



How do we go about it?



Run on the same VM

How do we go about it?

DEMO

Mappings

- logs
  - @timestamp *date*
  - @version *keyword*
  - host *keyword*
  - logLevel *keyword*
  - logType *keyword*
  - logger *keyword*
  - message *keyword*
  - metric
    - action *keyword*
    - data
    - disposition *keyword*
    - scope *keyword*
    - trigger *keyword*
  - path *keyword*
  - refererUri *keyword*
  - requestId *keyword*
  - requestMethod *keyword*
  - requestSource *keyword*
  - requestTags *keyword*
  - requestUri *keyword*
  - sessionId *keyword*
  - subdomain *keyword*
  - tags *keyword*
  - timestamp *date*

Built in Elastic Fields

Mappings

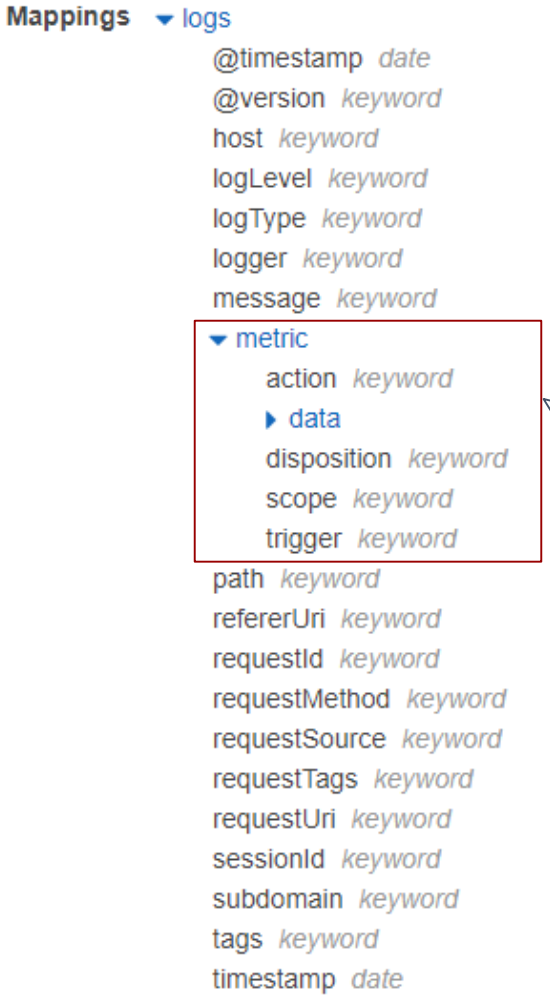
- logs
  - @timestamp *date*
  - @version *keyword*
  - host *keyword*
  - logLevel *keyword*
  - logType *keyword*
  - logger *keyword*
  - message *keyword*
  - metric
    - action *keyword*
    - data
    - disposition *keyword*
    - scope *keyword*
    - trigger *keyword*
  - path *keyword*
  - refererUri *keyword*
  - requestId *keyword*
  - requestMethod *keyword*
  - requestSource *keyword*
  - requestTags *keyword*
  - requestUri *keyword*
  - sessionId *keyword*
  - subdomain *keyword*
  - tags *keyword*
  - timestamp *date*

HTTP Request information

Mappings ▾ logs

- @timestamp *date*
- @version *keyword*
- host *keyword*
- logLevel *keyword*
- logType *keyword*
- logger *keyword*
- message *keyword*
- ▾ metric
  - action *keyword*
  - ▸ data
  - disposition *keyword*
  - scope *keyword*
  - trigger *keyword*
- path *keyword*
- refererUri *keyword*
- requestId *keyword*
- requestMethod *keyword*
- requestSource *keyword*
- requestTags *keyword*
- requestUri *keyword*
- sessionId *keyword*
- subdomain *keyword*
- tags *keyword*
- timestamp *date*

Logging information



Analytics information

scope: part of the application

action: the thing being tracked

trigger: user, timer, bot

disposition: good, bad, neutral

data: related information to the action type

Scale / Throughput

Instance type	t2.small.elasticsearch
Instance count	2
Dedicated master	Disabled
Zone awareness	Enabled
Storage type	EBS
EBS volume type	General Purpose (SSD)
EBS volume size	35 GB
Encryption at rest	Disabled
Node-to-node encryption	Disabled

▾ metric201805

Count	3646909
Size in bytes	3.36 GB
Query total	5220
Mappings	▸ logs

▾ metric201806

Count	3814822
Size in bytes	3.63 GB
Query total	5220
Mappings	▸ logs

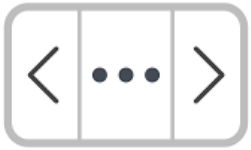
▾ metric201807

Count	3522401
Size in bytes	2.21 GB
Query total	5500
Mappings	▸ logs

What's Next?

Historical Roll Up

Elasticsearch Rollup API



Aggregation Pagination

Elasticsearch Composite Aggregations

How can we improve

DEMO

Why Elasticsearch for analytics

A familiar product and infrastructure

fast near real time queries
full visibility and control of data

testability - e2e, unit test and integration tests

Questions?