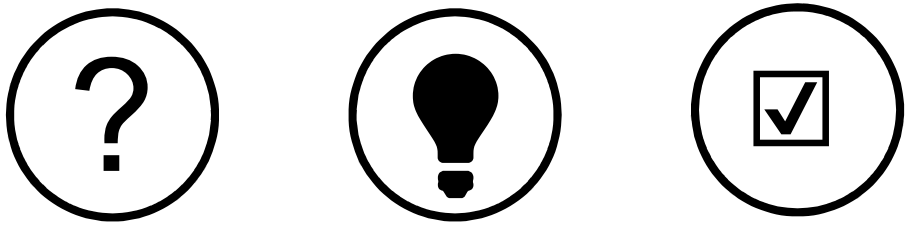
Visualize Server Logs with Kibana

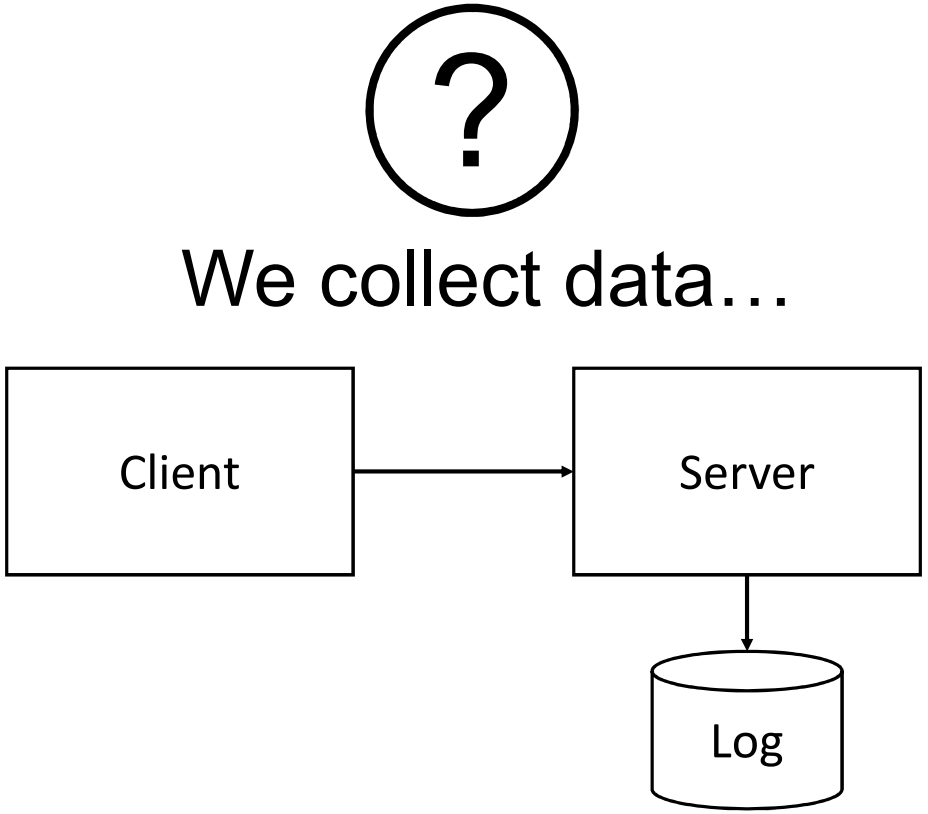
Thomas Alexander Ritter, SAP (PI Tech Core ABAP Server)

Disclaimer

Views expressed in this talk
are not necessarily SAP's

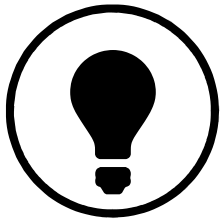


2010 - 2016


?
We collect data…
Client
Server
Log

Lots of data...

CLIENT	GUID	TIMESTAMP	METHOD	URL	SERVER_TIME	AGGREGATION_URL	BY_TEST_USER	STATUS_CODE
000	0000...	20160703...	GET	/sap/...	10,851,370	/sap/bc/adt/core/d...		200
000	0000...	20160703...	GET	/sap...	1,104,852	/sap/bc/adt/comp...		200
000	0000...	20160703...	GET	/sap...	87,889,016	/sap/bc/adt/disco...		200
000	0000...	20160703...	GET	/sap...	7,384,755	/sap/bc/adt/reposi...		200
000	0000...	20160703...	GET	/sap...	8,247	/sap/bc/adt/core/...		200
000	0000...	20160703...	GET	/sap...	7,456	/sap/bc/adt/comp...		200
000	0000...	20160703...	GET	/sap...	1,225,745	/sap/bc/adt/disco...		200
000	0000...	20160703...	GET	/sap...	3,436,578	/sap/bc/adt/debu...		200
000	0000...	20160703...	GET	/sap...	13,622,574	/sap/bc/adt/feeds		200
000	0000...	20160703...	GET	/sap...	262,720	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	GET	/sap...	13,583,237	/sap/bc/adt/feeds		200
000	0000...	20160703...	GET	/sap...	230,820	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	GET	/sap...	40,359	/sap/bc/adt/runti...		200
000	0000...	20160703...	POST	/sap...	11,928,039	/sap/bc/adt/debu...		200
000	0000...	20160703...	GET	/sap...	18,783,899	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	8,258	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	1,129,701	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	494,529	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	1,101,619	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	15,792,354	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	POST	/sap...	72,211,150	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	8,881,053	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	4,550,067	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	4,341,281	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	664,340	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	29,201	/sap/bc/adt/reposi...		200



Dashboard

Dec 1, 2009 - Nov 24, 2010

Visits

Graph by:

Site Usage

2,364 Visits	**67.39%** Bounce Rate
4,497 Pageviews	**00:02:17** Avg. Time on Site
1.90 Pages/Visit	**80.58%** % New Visits

Visitors Overview

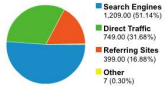
1,926 Visitors

view report

Map Overlay

view report

Traffic Sources Overview



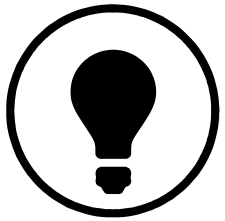
- **Search Engines** 1,209.00 (51.14%)
- **Direct Traffic** 749.00 (31.68%)
- **Referring Sites** 399.00 (16.88%)
- **Other** 7 (0.30%)

view report

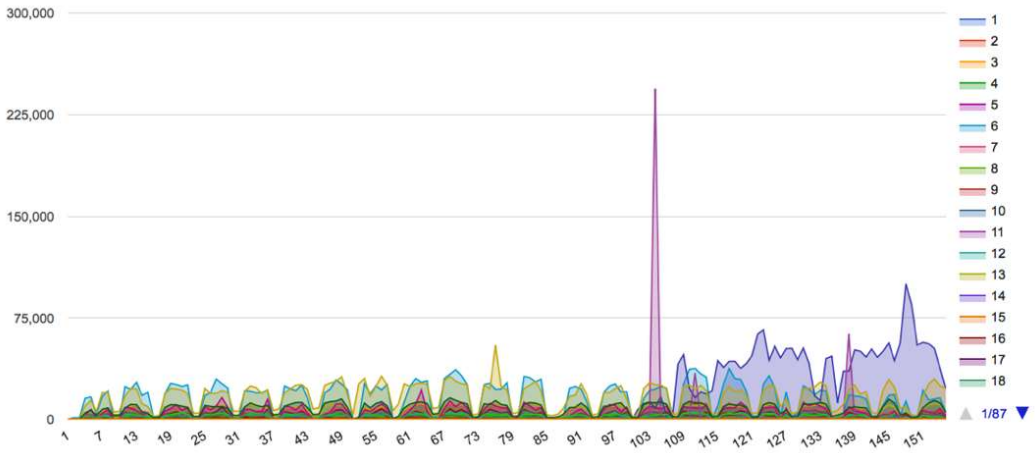
Content Overview

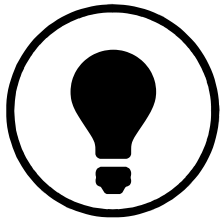
Pages	Pageviews	% Pageviews
/	1,030	22.90%
/public/item/216330	274	6.09%
/public/blog/214788	238	5.29%
/public/aggregate/214840	157	3.49%
/public/item/216329	152	3.38%

view report



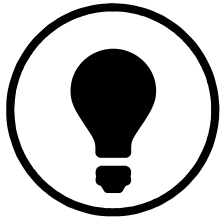
First ideas...


300,000
225,000
150,000
75,000
0
1
7
13
19
25
31
37
43
49
55
61
67
73
79
85
91
97
103
109
115
121
127
133
139
145
151
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
1/87



ELK Stack

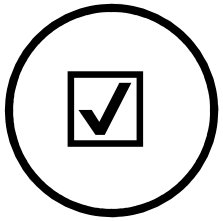
(Thanks Marco!)

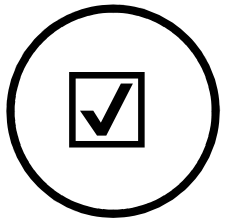


apache lucene powered, full textsearch, distributed, nosql

collect, format, dispatch

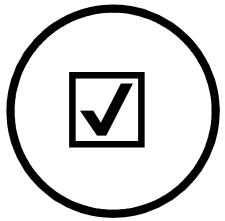
visualize





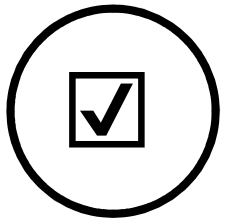
How to setup a system?

1. Trial at https://www.elastic.co/cloud
2. Lots of how to guides just Google
3. We use BOSH for deployments



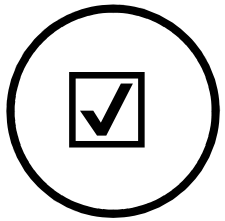
How to?

CLIENT	GUID	TIMESTAMP	METHOD	URL	SERVER_TIME	AGGREGATION_URL	BY_TEST_USER	STATUS_CODE
000	0000...	20160703...	GET	/sap/...	10,851,370	/sap/bc/adt/core/d...		200
000	0000...	20160703...	GET	/sap...	1,104,852	/sap/bc/adt/comp...		200
000	0000...	20160703...	GET	/sap...	87,889,016	/sap/bc/adt/disco...		200
000	0000...	20160703...	GET	/sap...	7,384,755	/sap/bc/adt/reposi...		200
000	0000...	20160703...	GET	/sap...	8,247	/sap/bc/adt/core/...		200
000	0000...	20160703...	GET	/sap...	7,456	/sap/bc/adt/comp...		200
000	0000...	20160703...	GET	/sap...	1,225,745	/sap/bc/adt/disco...		200
000	0000...	20160703...	GET	/sap...	3,436,578	/sap/bc/adt/debu...		200
000	0000...	20160703...	GET	/sap...	13,622,574	/sap/bc/adt/feeds		200
000	0000...	20160703...	GET	/sap...	262,720	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	GET	/sap...	13,583,237	/sap/bc/adt/feeds		200
000	0000...	20160703...	GET	/sap...	230,820	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	GET	/sap...	40,359	/sap/bc/adt/runti...		200
000	0000...	20160703...	POST	/sap...	11,928,039	/sap/bc/adt/debu...		200
000	0000...	20160703...	GET	/sap...	18,783,899	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	8,258	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	1,129,701	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	494,529	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	1,101,619	/sap/bc/adt/runti...		200
000	0000...	20160703...	GET	/sap...	15,792,354	/sap/bc/adt/feeds/...		200
000	0000...	20160703...	POST	/sap...	72,211,150	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	8,881,053	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	4,550,067	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	4,341,281	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	664,340	/sap/bc/adt/reposi...		200
000	0000...	20160703...	POST	/sap...	29,201	/sap/bc/adt/reposi...		200

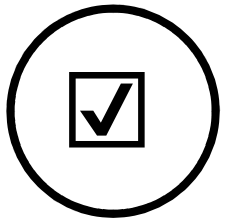


REST APIs

- Index url → <host>/<your_index>?pretty
- Batch import url → <host>/requests/request/_bulk
- Admin urls e.g. → <host>/_cluster/health/<your_index>?pretty



API DEMO



Index design 101

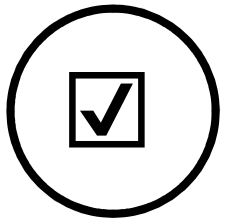
Index name

Type name

/requests-yi3?pretty

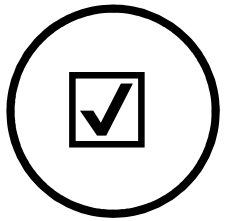
```
{
  "requests-yi3" : {
    "aliases" : { },
    "mappings" : {
      "request" : {
        "properties" : {
          "@timestamp" : {
            "type" : "date",
            "format" : "strict_date_optional_time||epoch_millis"
          },
          "@version" : {
            "type" : "string"
          },
          "agent" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
          "aggregatedUrl" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
          "clientId" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
          "host" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
          "httpversion" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
          "response" : {
            "type" : "string",
            "index" : "not_analyzed"
          },
```

Analysed: /my/url/my → my, url, my



More on index design...

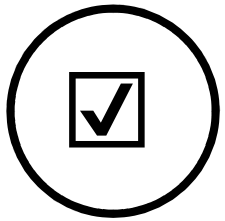
- One index per day (requests-06.10.16, requests-07.10.16, … → requests-*)
- Sharding
- …



How to transfer logs via ABAP?

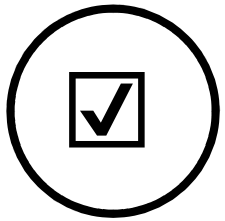
1. ABAP report
2. HTTP Client API (cl_http_client)
3. Use REST batch APIs
4. ABAP Jobs (SM36)
5. Be aware of system proxy settings! (SICF)

Example request



…/request/_bulk


```
{
  "create":{
    "_index":"requests-yi3",
    "_type":"request"
  }
}\n{
  "message":"FB0F9A87D546600E860CB2E1 - - [15/Dec/2016:00:01:45 -
0800] \"POST /sap/bc/adt/abapsource/codecompletion/elementinfo HTTP/1.1 200 3891 \"http://uia\" \"Eclipse/4.5.2.v20160212-
1500 ADT/2.59.0.dev\"",
  "@timestamp":"2016-03-15T08:01:45.000Z",
  "@version":"1",
  "host":"http://uia",
  "clientId":"FB0F9A87D5D60CB2E1",
  "timestamp":"15/Dec/2016:00:01:45 -0800",
  "verb":"POST",
  "request":"/sap/bc/adt/abapsource/codecompletion/elementinfo",
  "httpversion":"1.1",
  "response":"200",
  "serverTime":"148240",
  "agent":"Eclipse/4.5.2.v20160212-1500 ADT/2.59.0"
}\n
```



Configuring and using Kibana

Demo

Experience / Outlook

1. Great documentation for elasticsearch
2. Authorization can be added via proxy
3. Long term strategy for data integrity/backups
4. Use it for all kinds of data (Twitter, Blogs, …)

Links

https://www.elastic.co/guide/en/elasticsearch/reference/current/_basic_concepts.html
http://joelabrahamsson.com/elasticsearch-101/

Questions?

@thomasritter