

THE EVOLUTION OF WEB MONITORING



@EMANUIL_TOLEV

HISTORY PRESENT INNOVATION FUTURE

```
ess {inet[/93.93.131.120:9200]}
```

[2013-07-01 00:41:38,099][INFO][node] [Starsmore, Jonothon] {0.90.2}[23645]: started
[2013-07-01 00:42:18,604][INFO][node] [Starsmore, Jonothon] {0.90.2}[23645]: stopping ...
[2013-07-01 00:42:18,809][INFO][node] [Starsmore, Jonothon] {0.90.2}[23645]: stopped
[2013-07-01 00:42:18,809][INFO][node] [Starsmore, Jonothon] {0.90.2}[23645]: closing ...
[2013-07-01 00:42:19,846][INFO][node] [Starsmore, Jonothon] {0.90.2}[23645]: closed
[2013-07-01 01:19:43,108][INFO][node] [Blind Justice] {0.90.2}[24266]: initializing ...
[2013-07-01 01:19:43,114][INFO][plugins] [Blind Justice] loaded [], sites []
[2013-07-01 01:19:45,340][INFO][node] [Blind Justice] {0.90.2}[24266]: initialized
[2013-07-01 01:19:45,340][INFO][node] [Blind Justice] {0.90.2}[24266]: starting ...
[2013-07-01 01:19:45,449][INFO][transport net[/93.93.131.120:9300]] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:9300]}, publish_address {inet[/93.93.131.120:9300]}
[2013-07-01 01:19:48,484][INFO][cluster.service] [Blind Justice] new_master [Blind Justice][Jca598CqRXyBGk5Ns0T_7A][inet[/93.93.131.120:9300]], reason: zen-disco-join (elected_as_master)
[2013-07-01 01:19:48,522][INFO][discovery] [Blind Justice] elasticsearch/Jca598CqRXyBGk5Ns0T_7A
[2013-07-01 01:19:48,656][INFO][http net[/93.93.131.120:9200]] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:9200]}, publish_address {inet[/93.93.131.120:9200]}
[2013-07-01 01:19:48,657][INFO][node] [Blind Justice] {0.90.2}[24266]: started
[2013-07-01 01:19:49,826][INFO][gateway] [Blind Justice] recovered [9] indices into cluster_state
[2013-07-01 01:19:49,826][WARN][cluster.metadata] [Blind Justice] [swap] re-syncing mappings with cluster state for types [[student, account, archive]]
[2013-07-01 01:19:51,223][WARN][cluster.metadata] [Blind Justice] [leaps] re-syncing mappings with cluster state for types [[school, level, advancedlevel, student, subject, grade, account, simd, archive, institution]]
[2013-07-01 01:19:51,330][WARN][cluster.metadata] [Blind Justice] [xcri] re-syncing mappings with cluster state for types [[course, provider]]
[2013-07-01 01:19:55,562][WARN][cluster.metadata] [Blind Justice] [gtr] re-syncing mappings with cluster state for types [[project, person, organisation, publication]]
[2013-07-01 01:19:55,755][WARN][cluster.metadata] [Blind Justice] [occ] re-syncing mappings with cluster state for types [[record]]
[2013-07-01 01:20:26,822][INFO][node] [Blind Justice] {0.90.2}[24266]: stopping ...
[2013-07-01 01:20:26,937][INFO][node] [Blind Justice] {0.90.2}[24266]: stopped
[2013-07-01 01:20:26,937][INFO][node] [Blind Justice] {0.90.2}[24266]: closing ...
[2013-07-01 01:20:26,949][INFO][node] [Blind Justice] {0.90.2}[24266]: closed

```

2. cloo@pinky: /opt/elasticsearch/logs (ssh)
[2013-07-01 01:19:45,449][INFO ][transport        ] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:93]} File "/usr/lib/python2.7/socket.py", line 303, in flush
00}, publish_address {inet[/93.93.131.120:9300]}      self._sock.sendall(view[write_offset:write_offset+buffer_size])
[2013-07-01 01:19:48,484][INFO ][cluster.service    ] [Blind Justice] new_master [Blind Justice][Jca598CqRXyB] error: [Errno 32] Broken pipe
Gk5Ns0T_7A[inet[/93.93.131.120:9300]], reason: zen-disco-join (elected_as_master) 127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/vendor/jquery-ui/jquery-ui.css HTTP/1.0" 200 -
[2013-07-01 01:19:48,522][INFO ][discovery       ] [Blind Justice] elasticsearch/Jca598CqRXyB[Gk5Ns0T_7A] 127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/css/idfind.css HTTP/1.0" 200 -
[2013-07-01 01:19:48,656][INFO ][http           ] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:92]} 127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/vendor/bootstrap/1.3.0/bootstrap.min.css HTTP/1.0" 200 -
00}, publish_address {inet[/93.93.131.120:9200]}      127.0.0.1 - - [19/Sep/2014 05:00:15] "GET /static/vendor/jquery.tinysort.js HTTP/1.0" 200 -
[2013-07-01 01:19:48,657][INFO ][node           ] [Blind Justice] {0.90.2}[24266]: started 127.0.0.1 - - [19/Sep/2014 05:00:18] "GET /static/vendor/bootstrap/1.3.0/bootstrap-alerts.js HTTP/1.0" 200 -
[2013-07-01 01:19:49,826][INFO ][gateway       ] [Blind Justice] recovered [9] indices into cluster_stat 127.0.0.1 - - [19/Sep/2014 05:00:19] "GET /static/vendor/jquery-ui/jquery-ui.min.js HTTP/1.0" 200 -
e
[2013-07-01 01:19:49,826][WARN ][cluster.metadata] state for types [[student, account, archive]]  Traceback (most recent call last):
] [Blind Justice] [swap] re-syncing mappings with cluster: File "/usr/lib/python2.7/SocketServer.py", line 284, in _handle_request_noblock
state for types [[school, level, advancedlevel, student, subject, grade, account, simd, archive, institution]] self.process_request(request, client_address)
[2013-07-01 01:19:51,223][WARN ][cluster.metadata] state for types [[course, provider]]  File "/usr/lib/python2.7/SocketServer.py", line 310, in process_request
] [Blind Justice] [leaps] re-syncing mappings with cluster: self.finish_request(request, client_address)
File "/usr/lib/python2.7/SocketServer.py", line 323, in finish_request
state for types [[project, person, organisation, publication]]  self.RequestHandlerClass(request, client_address, self)
] [Blind Justice] [gtr] re-syncing mappings with cluster: File "/usr/lib/python2.7/SocketServer.py", line 640, in __init__
state for types [[record]]  self.finish()
File "/usr/lib/python2.7/SocketServer.py", line 693, in finish
] [Blind Justice] [occ] re-syncing mappings with cluster: self.wfile.flush()
] [Blind Justice] {0.90.2}[24266]: stopping ...  File "/usr/lib/python2.7/socket.py", line 303, in flush
] [Blind Justice] {0.90.2}[24266]: stopped  self._sock.sendall(view[write_offset:write_offset+buffer_size])
] [Blind Justice] {0.90.2}[24266]: closing ...  error: [Errno 32] Broken pipe
] [Blind Justice] {0.90.2}[24266]: closed  127.0.0.1 - - [19/Sep/2014 05:00:21] "GET /static/js/idfind.js HTTP/1.0" 200 -
cloo@pinky:/opt/elasticsearch/logs$ []

4. root@pinky: /var/log/nginx (ssh)
89.248.169.12 - - [07/Jun/2019:13:11:25 +0100] "GET / HTTP/1.1" 404 150 "-" "Mozilla/5.0 zgrab/0.x" 42.162 LEN=125 TOS=0x00 PREC=0x00 TTL=61 ID=1841 DF PROTO=UDP SPT=59284 DPT=51413 LEN=105
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "POST /RPC2_Login HTTP/1.1" 404 177 "-" "Dahua/2.0; Dahua/3.0" [17132187.845631] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=5.189.157.90 DST=178.62.242.
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /System/configurationFile/?auth=YWRtaW46MTEKY0BA HTTP/1.1" 404 162 LEN=125 TOS=0x00 PREC=0x00 TTL=60 ID=40139 DF PROTO=UDP SPT=11989 DPT=51413 LEN=105
177 "-" "-" [17132206.040731] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=173.249.33.72 DST=178.62.242
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /device.rsp?opt=user&cmd=list HTTP/1.1" 404 177 "-" "Mozilla/7.0 (911; Linux x86_128; rv:9743.0)" .162 LEN=125 TOS=0x00 PREC=0x00 TTL=61 ID=42539 DF PROTO=UDP SPT=11989 DPT=51413 LEN=105
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /system.ini?loginuse&loginpas HTTP/1.1" 404 177 "-" "-" [17132225.988443] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=207.180.192.205 DST=178.62.2
62.212.86.141 - - [07/Jun/2019:14:56:56 +0100] "GET /web/cgi-bin/hi3510/param.cgi?cmd=getuser HTTP/1.1" 404 177 "-" [17132246.933916] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=5.189.185.57 DST=178.62.242.
" "-" [17132246.933916] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=5.189.185.57 DST=178.62.242.
62.212.86.141 - admin [07/Jun/2019:14:56:56 +0100] "POST /queryUserList HTTP/1.1" 404 177 "-" "ApiTool" [17132266.106187] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=207.180.192.206 DST=178.62.2
191.255.180.172 - - [07/Jun/2019:16:08:36 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" [17132285.918792] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=173.249.33.72 DST=178.62.242
17.58.96.167 - - [07/Jun/2019:17:06:20 +0100] "GET /robots.txt HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.com/go/applebot)" [17132306.472372] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=207.180.192.205 DST=178.62.2
17.58.96.167 - - [07/Jun/2019:17:06:20 +0100] "GET / HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.co [17132328.394056] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=91.90.11.116 DST=178.62.242.
m/go/applebot)" [17132346.559219] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=1.55.47.122 DST=178.62.242.1
51.38.12.21 - - [07/Jun/2019:17:19:13 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36" [17132367.550827] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=177.180.136.152 DST=178.62.2
61.219.11.153 - - [07/Jun/2019:19:12:44 +0100] "\x01\x00\x00\x00" 400 181 "-" [17132362.134 TOS=0x00 PREC=0x00 TTL=51 ID=0 DF PROTO=UDP SPT=9441 DPT=51413 LEN=114
193.232.106.88 - - [07/Jun/2019:21:09:49 +0100] "GET /.env HTTP/1.1" 404 177 "-" "curl/7.35.0" [17132386.036685] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a:7d:08:00 SRC=207.180.210.81 DST=178.62.24
189.68.51.105 - - [07/Jun/2019:22:33:05 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" [17132406.922815] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=5.189.160.21 DST=178.62.242.
152.249.138.6 - - [07/Jun/2019:23:38:04 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" [17132426.078611] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82:7d:08:00 SRC=59.45.20.178 DST=178.62.242.
root@pinky:/var/log/nginx# cloo@pinky:/var/log$ []

5. cloo@pinky: /var/log (ssh)

```

```
2. cloo@pinky: /opt/elasticsearch/logs (ssh)
[2013-07-01 01:19:51,330][WARN ][cluster.metadata      ] [Blind Justice] [xcr :7d:
vel, student, subject, grade, account, simd, archive, institution]
[2013-07-01 01:19:51,330][WARN ][cluster.metadata      ] [Blind Justice] [xcr ID=:
[2013-07-01 01:19:51,330][WARN ][cluster.metadata      ] [Blind Justice] [xcr [171:
i] re-syncing mappings with cluster state for types [[course, provider]]
[2013-07-01 01:19:55,562][WARN ][cluster.metadata      ] [Blind Justice] [gtr :7d:
] re-syncing mappings with cluster state for types [[project, person, organisati ID=:
on, publication]]
[2013-07-01 01:19:55,755][WARN ][cluster.metadata      ] [Blind Justice] [occ [171:
] re-syncing mappings with cluster state for types [[record]]
[2013-07-01 01:20:26,822][INFO ][node                ] [Blind Justice] {0.9 :7d:
0.2}[24266]: stopping ...
[2013-07-01 01:20:26,937][INFO ][node                ] [Blind Justice] {0.9 =51
] [Blind Justice] {0.9 [171:
0.2}[24266]: stopped
[2013-07-01 01:20:26,937][INFO ][node                ] [Blind Justice] {0.9 :7d:
0.2}[24266]: closing ...
[2013-07-01 01:20:26,949][INFO ][node                ] [Blind Justice] {0.9 [171:
0.2}[24266]: closed
[2013-07-01 01:20:26,949][INFO ][node                ] [Blind Justice] {0.9 :7d:
0.2}[24266]: closed
[2013-07-01 01:20:26,949][INFO ][node                ] [Blind Justice] {0.9 ID=:
0.2}[24266]: closed
```

```
5.cloo@pinky: /var/log (ssh) | ● ● ● 8.root@pinky: /var/log/nginx (ssh)
DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL=57 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML,
67 DPT=51413 LEN=105 like Gecko) Version/9.1.2 Safari/601.7.7"
[K] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a : 216.245.193.10 - - [01/Jun/2019:23:04:09 +0100] "HEAD /robots.txt HTTP/1.0"
ST=178.62.242.162 LEN=129 TOS=0x00 PREC=0x00 TTL=111 , 404 0 "-" "-"
55 DPT=51413 LEN=109 77.247.110.106 - - [02/Jun/2019:00:49:40 +0100] "HEAD /robots.txt HTTP/1.0"
[K] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a : 404 0 "-" "-"
52 DST=178.62.242.162 LEN=134 TOS=0x00 PREC=0x00 TTL= 190.186.82.207 - - [02/Jun/2019:05:35:16 +0100] "GET / HTTP/1.1" 404 579 "-"
441 DPT=51413 LEN=114 ; Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
[K] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a : Chrome/51.0.2704.103 Safari/537.36"
1 DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL= 183.129.160.229 - - [02/Jun/2019:06:54:30 +0100] "GET / HTTP/1.1" 404 177 "-"
=41189 DPT=51413 LEN=105 ; Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0"
[K] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82 : efox/47.0"
DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL=60 58.250.125.114 - - [02/Jun/2019:07:10:03 +0100] "GET /robots.txt HTTP/1.1" 5
2205 DPT=51413 LEN=105 ; 02 181 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
[K] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82 : html#07"
DST=178.62.242.162 LEN=143 TOS=0x00 PREC=0x00 TTL=47 58.250.125.114 - - [02/Jun/2019:07:10:03 +0100] "GET / HTTP/1.1" 502 181 "-"
1 DPT=51413 LEN=123 ; "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
```

```
4. root@pinky: /var/log/nginx (ssh)
17.58.96.167 - - [07/Jun/2019:17:06:20 +0100] "GET / HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.com/go/applebot)"
51.38.12.21 - - [07/Jun/2019:17:19:13 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.228.0 Safari/537.36"
61.219.11.153 - - [07/Jun/2019:19:12:44 +0100] "\x01\x00\x00\x00" 400 181 "-" "-"
193.232.106.88 - - [07/Jun/2019:21:09:49 +0100] "GET /.env HTTP/1.1" 404 177 "-" "curl/7.35.0"
189.68.51.105 - - [07/Jun/2019:22:33:05 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
152.249.138.6 - - [07/Jun/2019:23:38:04 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
root@pinky:/var/log/nginx#
```

```
@pinky: /opt/elasticsearch/logs (ssh) 9.cloo@pinky: /opt/idfind (ssh)
[INFO ][node] [Black Fox] {0.90.2} 127.0.0.1 - - [19/Sep/2014 02:47:09] "GET / HTTP/1.0" 200 -
[INFO ][transport] [Black Fox] bound_a 0 -
[INFO ][cluster.service] [Black Fox] new_mas 0 -
[INFO ][discovery] [Black Fox] cl_test Traceback (most recent call last):
[INFO ][http] [Black Fox] bound_a lock
[INFO ][node] [Black Fox] {0.90.2}
[INFO ][gateway] [Black Fox] recover
```

```
3. cloo@pinky: /opt/idfind (ssh)
js HTTP/1.0" 200 -
Traceback (most recent call last):
  File "/usr/lib/python2.7/SocketServer.py", line 284, in _handle_request_noblock
    self.process_request(request, client_address)
  File "/usr/lib/python2.7/SocketServer.py", line 310, in process_request
    self.finish_request(request, client_address)
  File "/usr/lib/python2.7/SocketServer.py", line 323, in finish_request
    self.RequestHandlerClass(request, client_address, self)
  File "/usr/lib/python2.7/SocketServer.py", line 640, in __init__
    self.finish()
  File "/usr/lib/python2.7/SocketServer.py", line 693, in finish
    self.wfile.flush()
  File "/usr/lib/python2.7/socket.py", line 303, in flush
    self._sock.sendall(view[write_offset:write_offset+buffer_size])
error: [Errno 32] Broken pipe
127.0.0.1 - - [19/Sep/2014 05:00:21] "GET /static/js/idfind.js HTTP/1.0" 200 -
cloo@pinky:/opt/idfind$
```

```
7. cloo@pinky: /var/log (ssh) 10. cloo@pinky: /opt/elasticsearch/logs (ssh)
: pam_unix(sudo:session): session closed for user root STATUS | wrapper | 2018/11/21 15:43:21 | http://wrapper.tanukisoftware.com
[32355]: Received disconnect from 104.248.148.6: 11: B
: pam_unix(sudo:session): session opened for user root STATUS | wrapper | 2018/11/21 15:43:21 | Launching a JVM...
log INFO | jvm 1 | 2018/11/21 15:43:22 | WrapperManager: Initializing...
: pam_unix(sudo:session): session closed for user root STATUS | wrapper | 2019/04/12 11:37:54 | TERM trapped. Shutting down.
: pam_unix(sudo:session): session opened for user root STATUS | wrapper | 2019/04/12 11:37:56 | <-- Wrapper Stopped
: pam_unix(sudo:session): session closed for user root STATUS | wrapper | 2019/04/12 13:06:36 | --> Wrapper Started as Daemon
: pam_unix(sudo:session): session opened for user root STATUS | wrapper | 2019/04/12 13:06:36 | Java Service Wrapper Community Edition 64-bit 3.5.14
: pam_unix(sudo:session): session closed for user root STATUS | wrapper | 2019/04/12 13:06:36 | Copyright (C) 1999-2011 Tanuki Software, Ltd. All Rights Reserved.
: pam_unix(sudo:session): session closed for user root STATUS | wrapper | 2019/04/12 13:06:36 | http://wrapper.tanukisoftware.com
: pam_unix(sudo:session): session opened for user root STATUS | wrapper | 2019/04/12 13:06:36 | Launching a JVM...
: pam_unix(sudo:session): session closed for user root INFO | jvm 1 | 2019/04/12 13:06:36 | WrapperManager: Initializing...
: cloo@pinky:/opt/elasticsearch/logs$
```



@emanuil_tolev



D

Infrastructure

[Inventory](#)[Metrics Explorer](#)

Search for infrastructure data... (e.g. host.name:host-1)

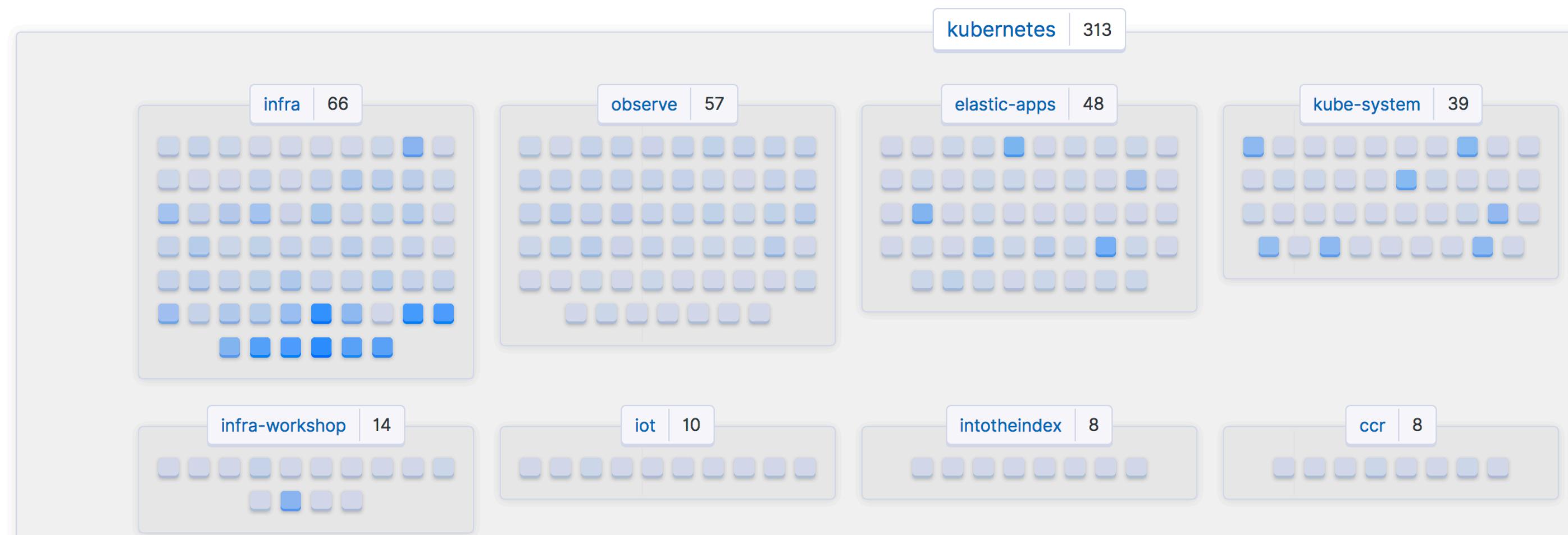
[Hosts](#)[Kubernetes](#)[Docker](#)

Metric: CPU Usage ▾

Group By: Service Type Namespace ▾

[Configuration](#)[Map View](#)[Table View](#)

Showing





THE STORY OF MONITORING IS A STORY
OF FRUSTRATION, FACEPALMING AND
PAINFUL MOMENTS OF REFLECTION

NOW:

- > MONITORING
- > LOGGING
- > METRICS
- > TRACING
- > SECURITY?
- > OBSERVABILITY

WAF - Metrics

1,021

Total Attacks

4

Unique Rules Hit

5

Unique Sources

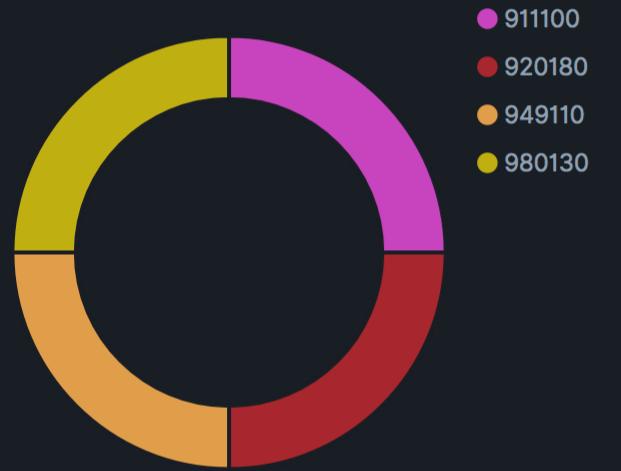
3

Source Attack Countries

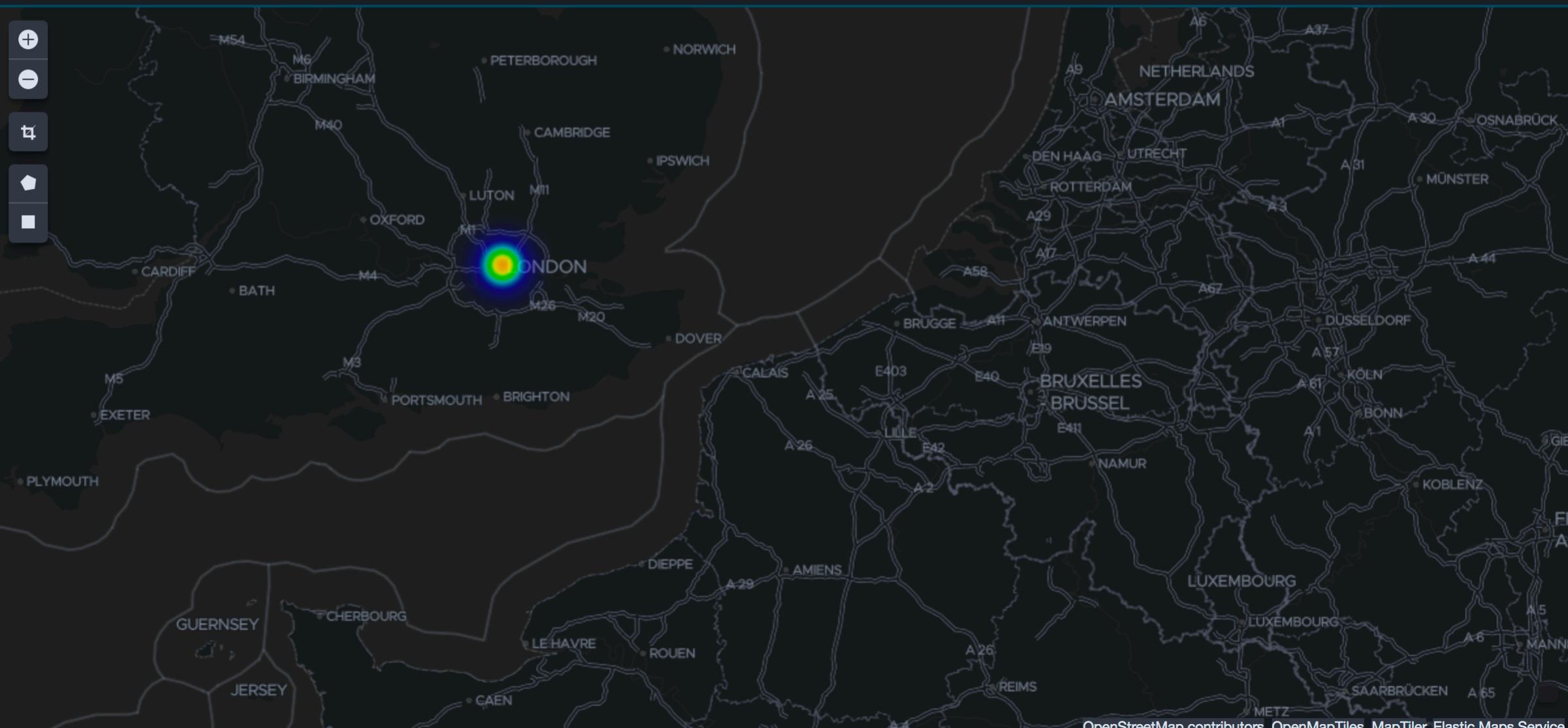
2

Reporting Hosts

WAF - Chart of Top 10 Rules



WAF - Attack Heat Map



WAF - Chart Of Severities





Best Log Management Tools: 51 Useful Tools for Log Management, Monitoring, Analytics, and More

STACKIFY | MAY 26, 2017 | DEVELOPER TIPS, TRICKS & RESOURCES



@emanuil_tolev

OBSERVABILITY

[HTTPS://WWW.HONEYCOMB.IO/BLOG/
OBSERVABILITY-A-MANIFESTO/](https://www.honeycomb.io/blog/observability-a-manifesto/)

PRESENT INNOVATION

- > FEATURES
- > BUSINESS MODELS
- > STRATEGIC VIEW OF OPS PAIN & RELIEF

service: iOS

operation: /api/get-sto ...



Run ⌘ ↵

Wed Oct 16, 23:01:48



Latency Histogram

Show percentile

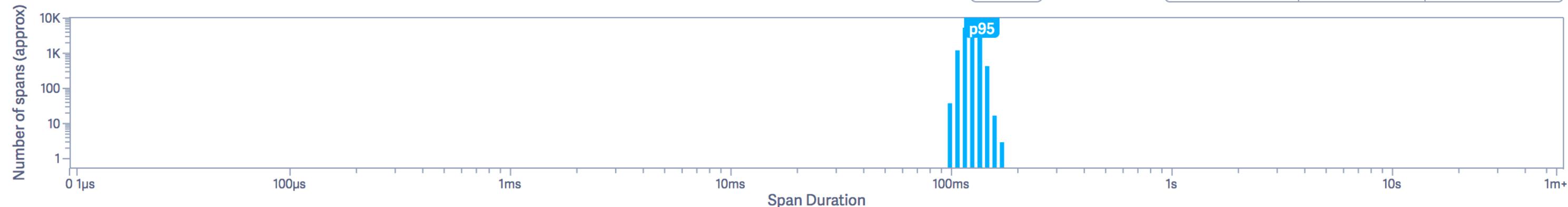
p95

Compare to

1 hour prior

1 day prior

1 week prior



Trace Analysis Service Diagram

SERVICE

iOS

OPERATIONS

/api/get-store

192.90 ms

172.27 ms

167.73 ms

167.68 ms

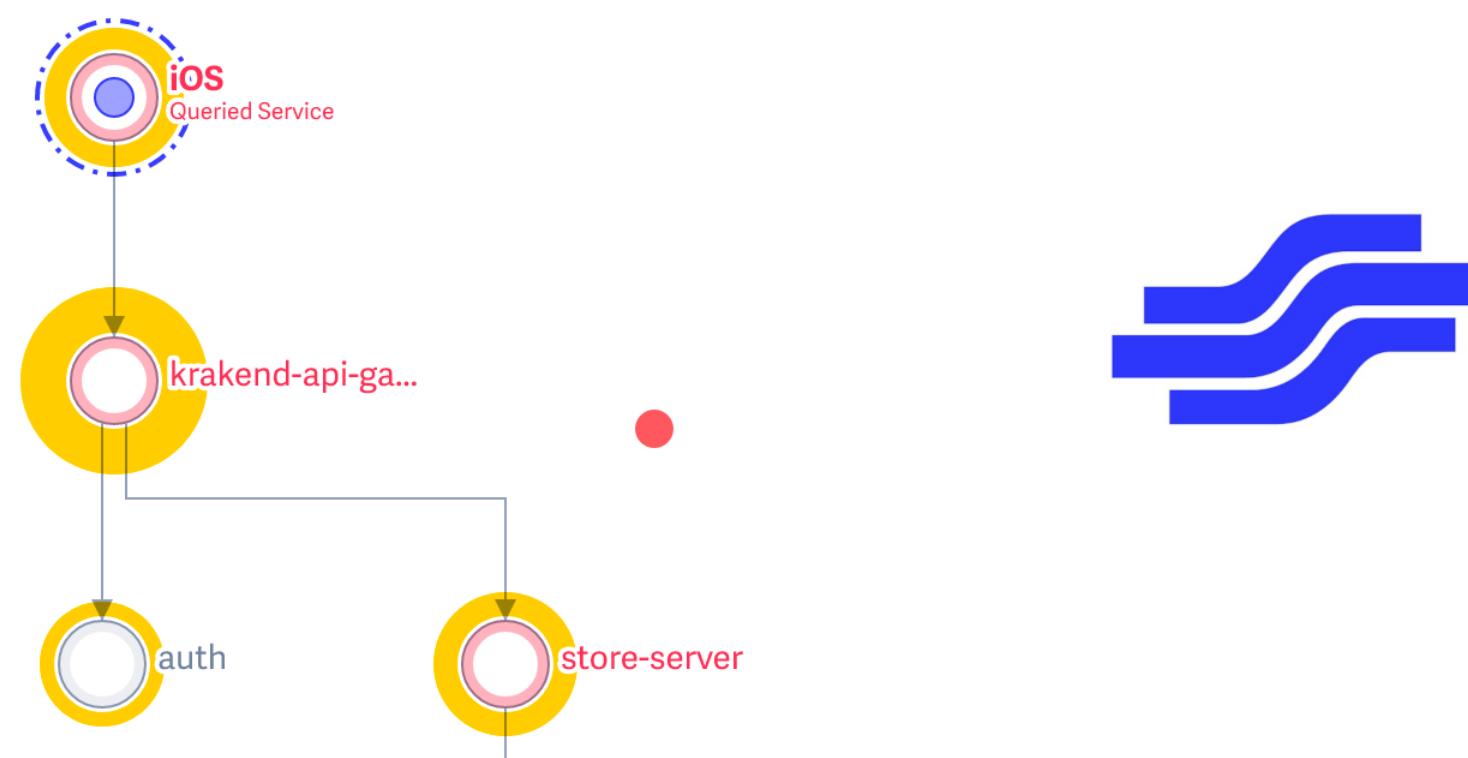
166.68 ms

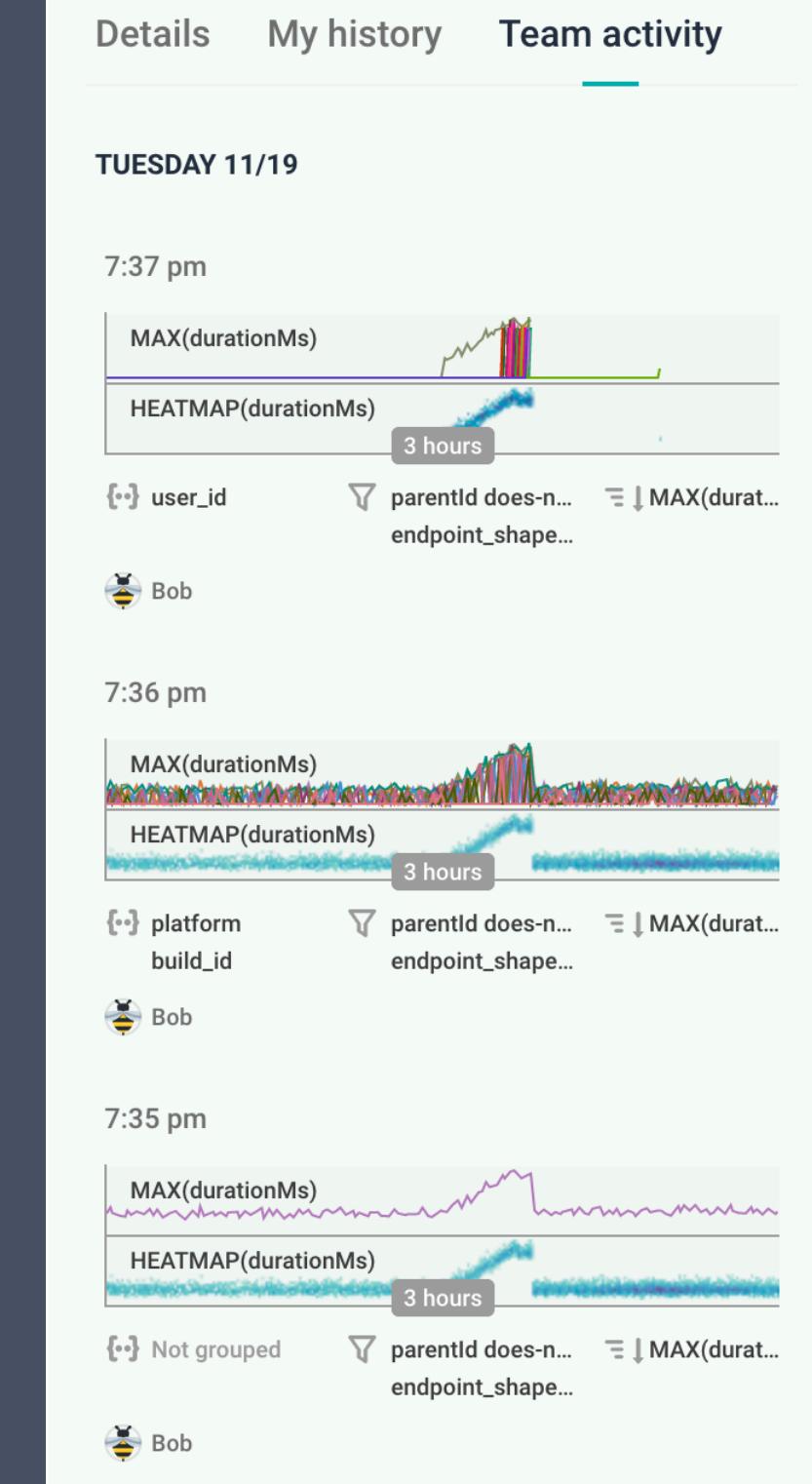
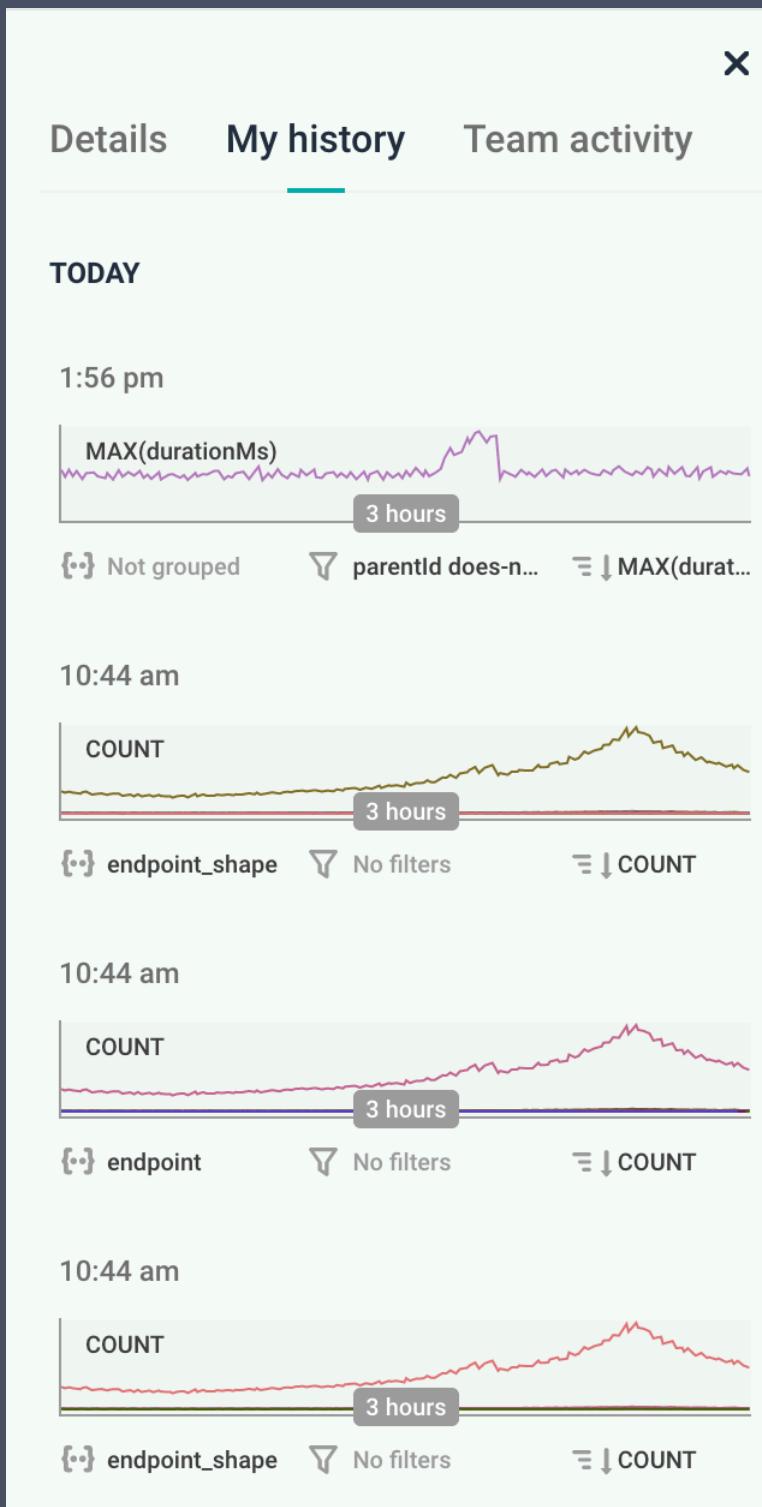
164.70 ms

164.47 ms

Recenter Focus on service

Selected Latency Errors Documentation







D

Machine Learning



e

[Job Management](#) [Anomaly Explorer](#) [Single Metric Viewer](#) [Data Frames](#) [Data Visualizer](#) [Settings](#)

petclinic-react-events-high_mean_response_time

[Edit job selection](#)[Filter by influencer fields... \(E.g. user.name : dalem\)](#)

Top Influencers

**user.name**dalem [+](#) [-](#)

96

275

jtornkv [+](#) [-](#)
80

80

strusl... [+](#) [-](#)
80

80

dflag85 [+](#) [-](#)
72

72

kisset... [+](#) [-](#)
72

72

Anomaly timeline

Overall



2018-11-27 00:00

2018-11-27 12:00

2018-11-28 00:00

View by

Limit

transaction.name

10

UpdateOwner

EditPetPage

OwnerEditor:ZipChange



@emanuil_tolev



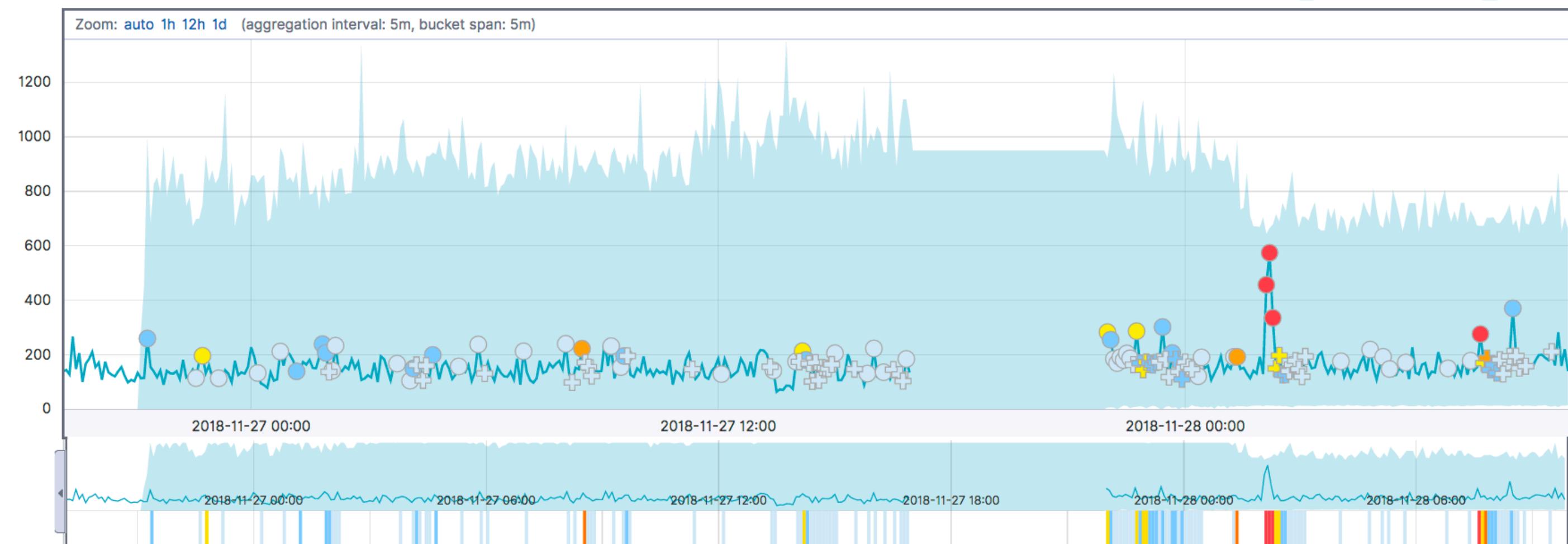
@emanuil_tolev

Detector: high_mean("transaction.duration.us")

transaction.name: Enter value

Forecast

Single time series analysis of avg transaction.duration.us (14 distinct transaction.name values)

 show model bounds annotations

Anomalies

Severity threshold

 warning

Interval

Auto

time	severity ↓	detector	found for	influenced by	actual	typical	description	actions
November 28th 2018, 02:00	● 94	high_mean("transaction.duration.us")	UpdateOwner <input type="button" value="⊕"/> <input type="button" value="⊖"/>	transaction.name: UpdateOwner user.name: dalem	4977	38	↑ More than 100x higher	<input type="button" value="⚙"/>

BUSINESS MODELS

VARIETY: CHARGE PER NODE / DATA VOLUME / DATA STORAGE / COMPUTE / OPS USER, ...

STRATEGIC VIEW

- > HONEYCOMB: EVENTS. STRUCTURED INFO RATHER THAN LOGS. UNKNOWN UNKNOWNS. THE SYSTEM TEACHES US
- > ELASTIC AND SPLUNK: ONE-STOP SHOP (BUT PRICING VARIES BY ORDERS OF MAGNITUDE IN DIFF USE CASES)
 - > MANY OTHERS

THE FUTURE

- > IN-DEPTH COMPARISON OF VENDORS?
- > TRYING EVERY TOOL AVAILABLE AND WRITING A BOOK?
- > PRODUCT MANAGERS @ VENDORS DECIDE WHERE NEXT?
- > TIME-TESTED METHOD: GO RANT AT SEVERAL CONFERENCES ABOUT YOUR OWN FRUSTRATIONS!