
interia

# “A needle in a logstack” – analyzing data from mobile users around the globe to verify a successful deployment and swift problem recognition

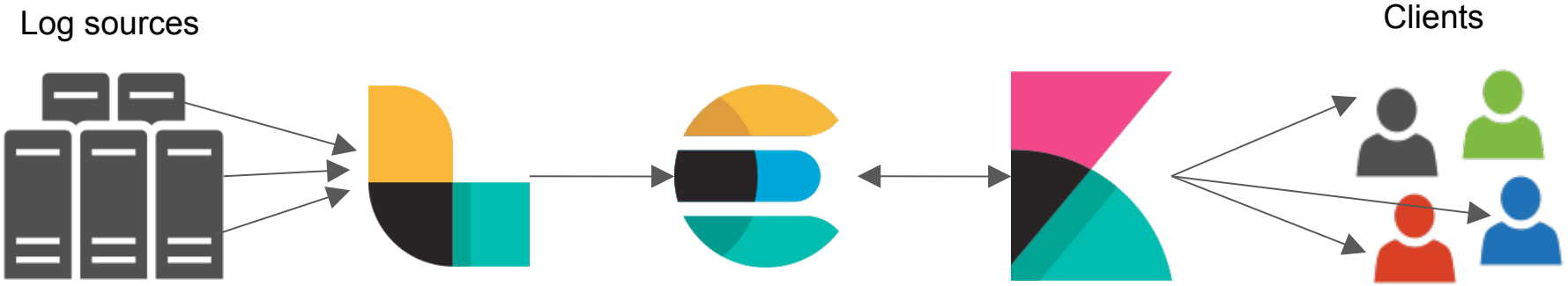
Tomasz Gągor - Senior System Administrator
Paweł Torbus - System Architect

# ELK Stack

Logstash - Log pre-processor

Elasticsearch - Storage, indexing and searching

Kibana - Elasticsearch front-end



# ELK Stack family

Filebeat - lightweight log shipper
(logstash-frowarder successor)

Marvel - Elasticsearch monitor

Shield - protect access
to elasticserch data with authorization

Reporting - generate,
schedule, email reports

Watcher - alerting for elasticsearch

# Logstash

- Written in Ruby, executed in JRuby
- Receive logs from agents in numerous formats (49 currently)
- Parse them to JSON format
- Can render additional data (like geographical coordinates from IP address, useragent)
- Store in Elasticsearch on daily indexes
- Can use other “data stores” like Mail, Graphite and more
- All events reside in the singe index

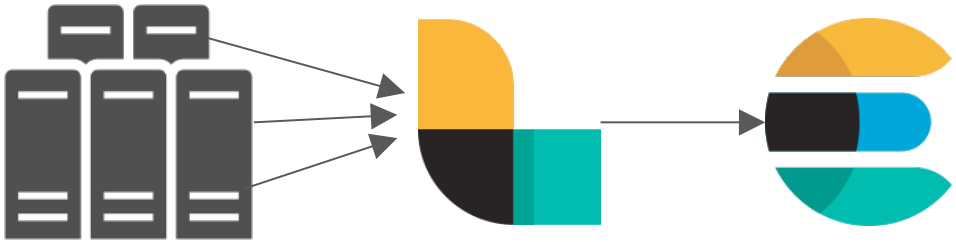
# Logstash - deployment

Accepts syslog, JSON and XML data

Parses those to JSON

Store data in singe Elasticsearch cluster

We have up to 6 logstash nodes in single cluster (gathering data from 100 hosts)



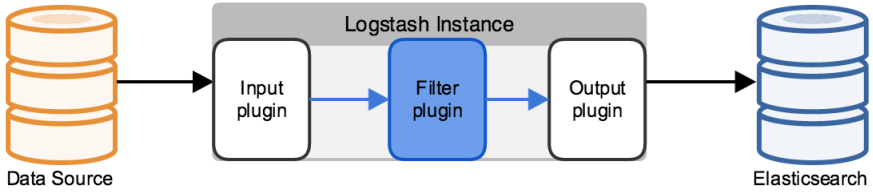
Log sources

# Logstash - problems we faced

Avoid multilines

Always use `date` filter to have proper event timestamps

Be careful naming fields - you don't want to overwrite your data




```
filter{
  if [message] == '<!DOCTYPE log SYSTEM
"logger.dtd">' { drop {} }
  if [message] == '<log>' { drop {} }
  if [message] == '</log>' { drop {} }
  if [message] =~ '^ *<' {
    multiline {
      pattern => "^</record>$"
      what => "next"
      negate => true
    }
    xml {
      source => "message"
      target => "java_xml"
    }
    date {
      match => ["[java_xml][millis]", "UNIX_MS"]
    }
```

# Logstash - problems we faced

Syslog is not reliable, favor logstash-forwarder/filebeat

Always configure `dead time` in logstash-forwarder

```
{"network": {
  "servers": [ "logstash1.xxx:5959",
"logstash2.xxx:5959" ],
  "timeout": 15,
  "ssl ca": "/etc/pki/tls/certs/ca.crt"
  },
  "files": [{
    "paths": [
    "/var/log/tomcat6/localhost.*-*-*.log",
    "/var/log/tomcat/localhost.*-*-*.log"],
    "fields": {
      "type": "java_xml",
      "forwarder_tags":"tomcat"
    },
    "dead time": "10m"
   },
...
```

# Logstash - problems we faced

Carrefully calibrate memory usage for better performance and stability

```
LS_HEAP_SIZE="3043m" or -Xmx3043m
```

Set proper field type in grok to be able to use statistics

```
grok {
  match => [
  "message",
  # Common Log Format
  # "10.0.2.2 - - [22/Apr/2015:11:58:06 +0000] "GET /some/redirect HTTP/1.1" 302 -"
  "^%{IP:[access_log][clientip]} - (-|%{USER:[access_log][user]}) \[%{HTTPDATE:
[access_log][timestamp]}\] \"%{DATA:[access_log][request]}\" %{POSINT:[access_log]
[status]:int} (%{INT:size:int}|-)$"
  ]
  add_tag => [ "access_log" ]
}
```

# Elasticsearch

Elasticsearch is schemaless Lucene based search engine.

- Distributed (availability, scalability, durability)
- JSON-based objects
- HTTP-based client API
- Data grouped in Indexes
- Indexes are stored daily

# Elasticsearch - deployment

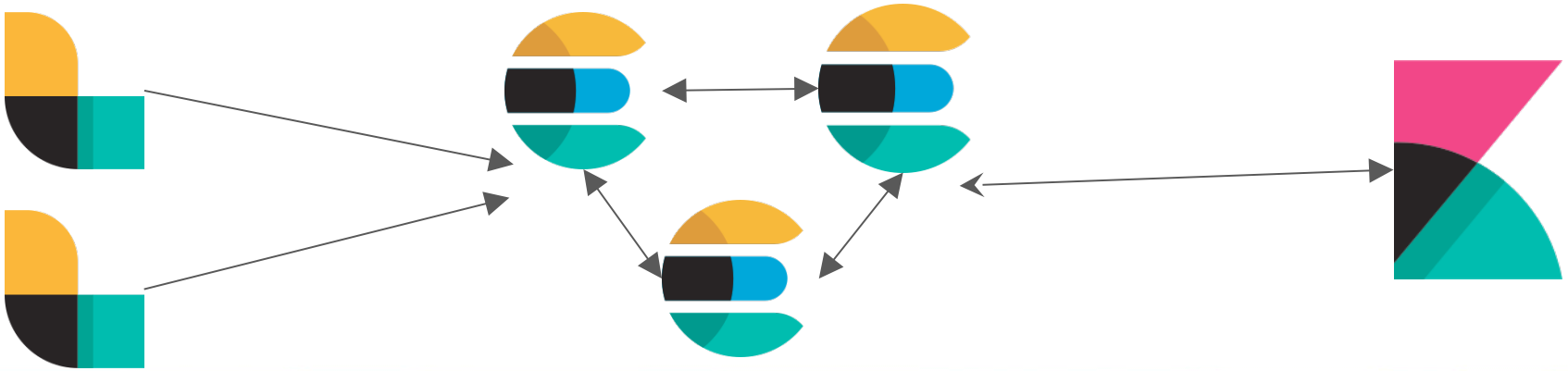
We have three clusters for two different clients, one internal

They’re in separate subnet and gather logs from all environments (prod/itg/stg/qa/…)

First cluster consists of 3 elasticsearch nodes, 250GB of storage each

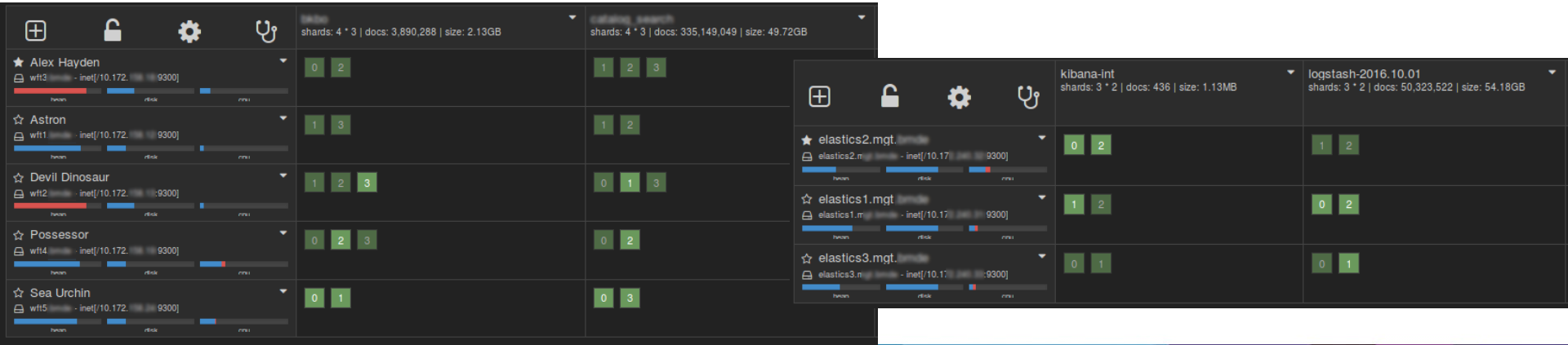
Second cluster consists of 5 nodes, 250GB each

Third cluster consists of 6 nodes, 200GB each



# Elasticsearch - problems we faced

Configure shards and replicas number according to amount of your machines
Keep track of free disk space and have enough of it
Bigger nodes will synchronise longer
Cluster autodiscovery mostly works, mostly
Disable shard allocation during node restarts/upgrades



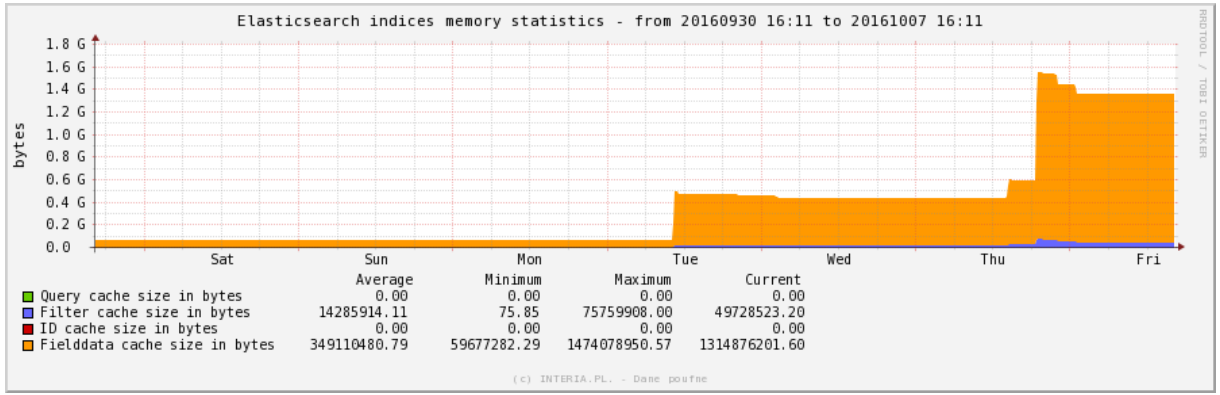
# Elasticsearch - problems we faced

Allocate max 50% of RAM for elasticsearch

Don’t use more than 32GB RAM for elasticsearch

Set `bootstrap.mlockall` to `true` to keep elasticsearch in RAM

Set `indices.fielddata.cache.size` to any value, ex. 30~40%



# Kibana

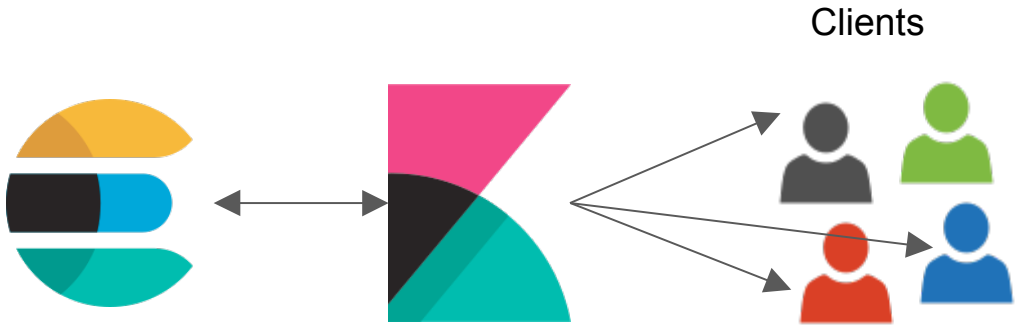
Kibana is open source analytics and visualization platform designed to work with Elasticsearch.

- Querying Elasticsearch
- Visualizing data
- Filtering and inspecting events

# Kibana - deployment

Single Kibana instance

Available in version 3.x and 4.x



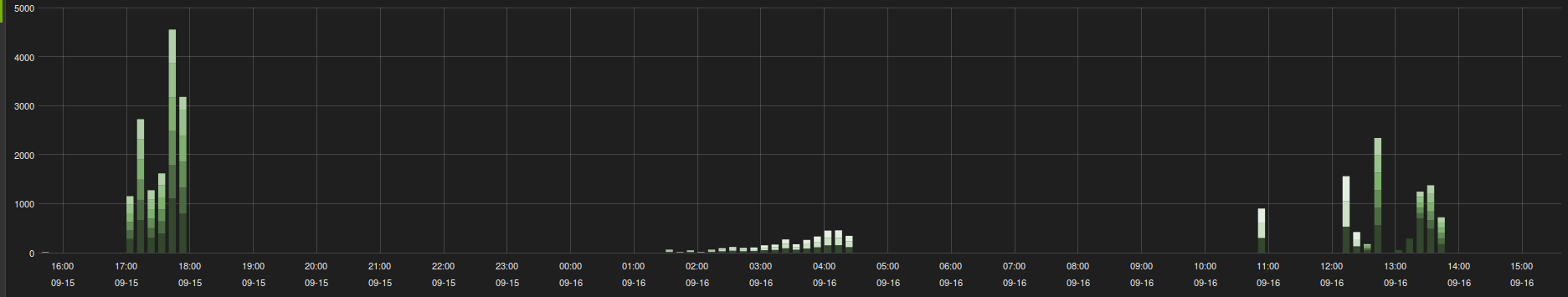
# SFTP Delivery PROD

a day ago to a few seconds ago

QUERY | FILTERING

## EVENTS OVER TIME

View | Zoom Out | @json.deliver_destination.raw:"" AND (*) (7873) newspaperdirect (3035) wewant (3020) stratoserver (3020) readly-de (3020) nook (2750) readly-uk (2030) newspaperdirect-uk (2030) count per **10m** | (**26778** hits)




## ALL EVENTS

### Fields

All (592) / Current (26)

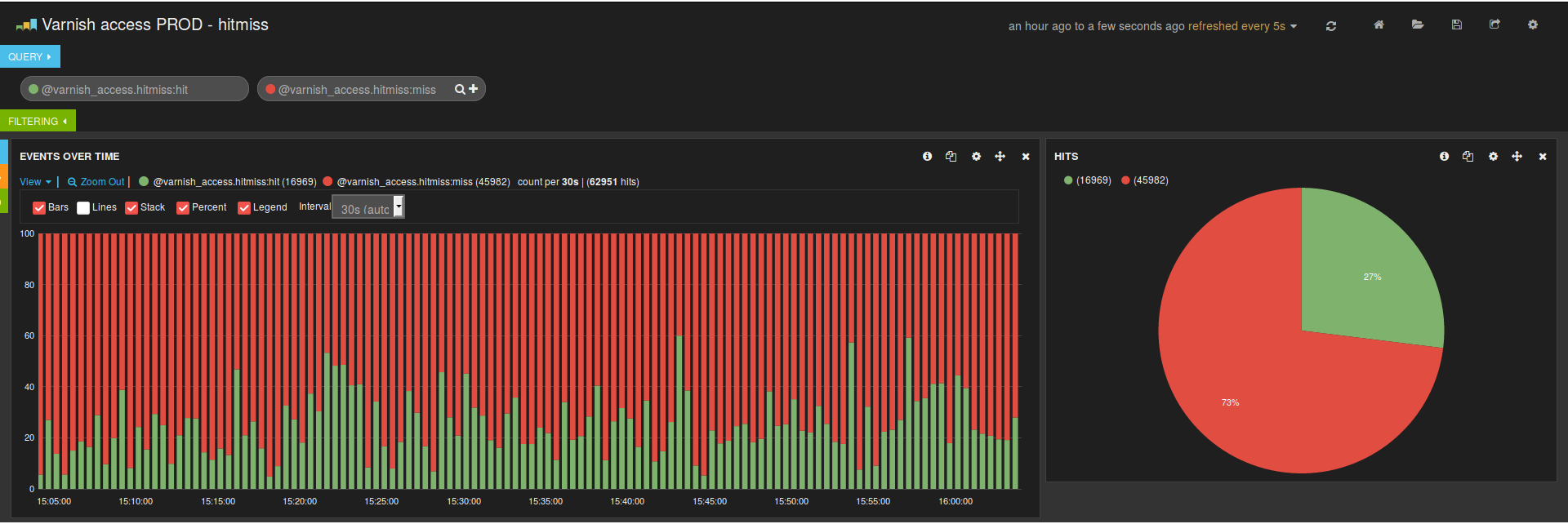
Type to filter...

- [ ] @json.asciTime
- [x] @json.deliver_destination
- [ ] @json.fileName
- [x] @json.functionName
- [ ] @json.job
- [ ] @json.levelName
- [ ] @json.levelNo
- [ ] @json.lineNo
- [ ] @json.loggerName
- [ ] @json.logRecordCreationTime
- [x] @json.message
- [ ] @json.time
- [x] @timestamp
- [ ] @version
- [ ] _id
- [ ] _index
- [ ] _type
- [ ] file
- [ ] forwarder_tags
- [ ] host
- [ ] host_addr

**0** to **100** of 500 available for paging

| @json.deliver_destination | @timestamp | @json.functionName | @json.message |
|---|---|---|---|
| newspaperdirect | 2016-09-16T13:45:30.628+02:00 | deliver | Job b54f6078-613a-41f9-9905-6492295a205c finished |
| newspaperdirect | 2016-09-16T13:45:30.628+02:00 | deliver | Listing of file sent: ['09-16-16 04:45AM 37626312 [redacted]2016_S001.pdf'] |
| newspaperdirect | 2016-09-16T13:45:30.627+02:00 | deliver | Sending done with rsponse: 226 Transfer complete. |
| newspaperdirect | 2016-09-16T13:44:25.617+02:00 | deliver | Successfully connected to service 207.34.140.19 21, from 10.172.158.20 52287 |
| newspaperdirect | 2016-09-16T13:43:18.119+02:00 | deliver | Job 4293a700-86b6-4dd2-8d07-959db5605072 finished |
| newspaperdirect | 2016-09-16T13:43:18.118+02:00 | deliver | Listing of file sent: ['09-16-16 04:43AM 1947712 [redacted]2016_S051.pdf'] |
| newspaperdirect | 2016-09-16T13:43:13.123+02:00 | deliver | Listing of file sent: ['09-16-16 04:43AM 2601497 [redacted]2016_S020.pdf'] |
| newspaperdirect | 2016-09-16T13:43:13.123+02:00 | deliver | Sending done with rsponse: 226 Transfer complete. |
| newspaperdirect | 2016-09-16T13:43:13.123+02:00 | deliver | Job 136da700-22cd-4e87-b481-4f6d104bf22d finished |
| newspaperdirect | 2016-09-16T13:43:13.122+02:00 | deliver | Sending done with rsponse: 226 Transfer complete. |
| readly-de | 2016-09-16T13:43:13.121+02:00 | deliver | Sending done with rsponse: 226-File successfully transferred<br>226 0.954 seconds (measured here), 1.95 Mbytes per second |
| nook | 2016-09-16T13:43:13.121+02:00 | deliver | Sending done with rsponse: 226-File successfully transferred<br>226 1.324 seconds (measured here), 1.40 Mbytes per second |
| readly-de | 2016-09-16T13:43:13.121+02:00 | deliver | Job da570da6-2a2e-490c-b465-422fc26f18b6 finished |
| nook | 2016-09-16T13:43:13.121+02:00 | deliver | Job 021097b6-6dc1-40bb-b7bd-6729e9848d54 finished |

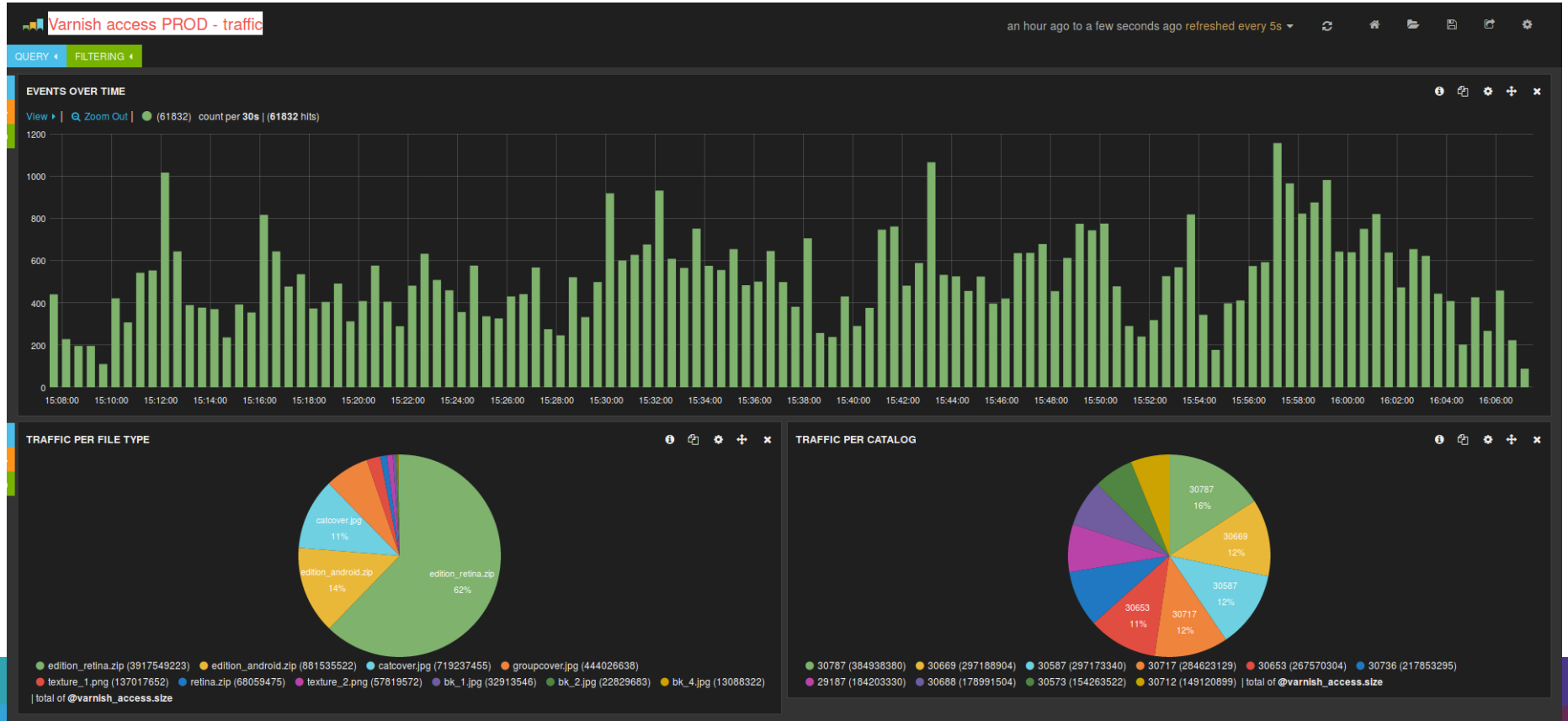
# Simple HIT/MISS statistics






interia

# Varnish traffic per file type



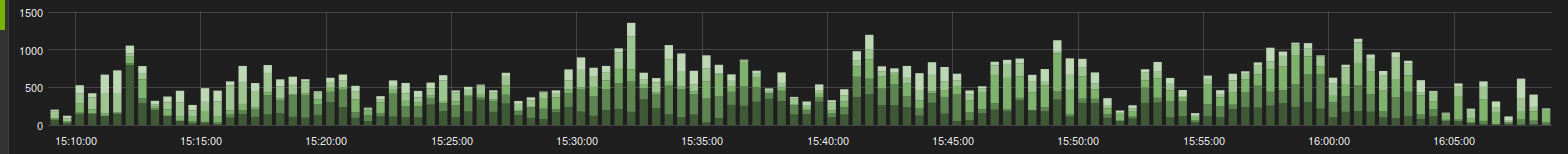
# WFT accesses

an hour ago to a few seconds ago refreshed every 30s

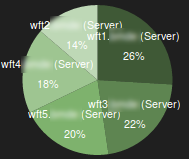
QUERY FILTERING

## HTTP REQUESTS

View | Zoom Out | wft1 (Server) (19888) wft3 (Server) (16634) wft5 (Server) (15472) wft4 (Server) (14129) wft2 (Server) (10517) count per **30s** | (**76640** hits)

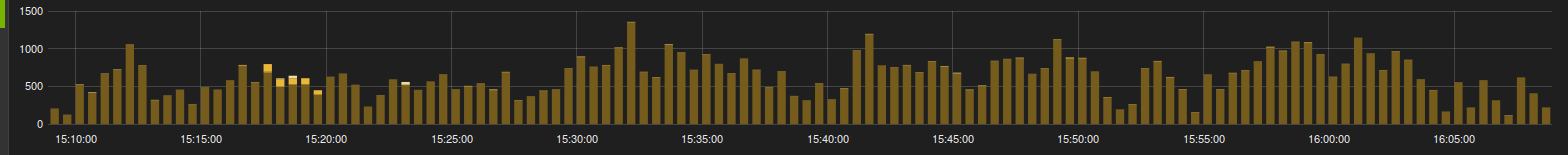



## REQUESTS PER HOST

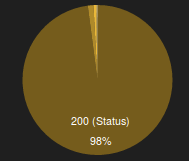



## STATUSES

View | Zoom Out | 200 (Status) (75053) 404 (Status) (932) 302 (Status) (451) 403 (Status) (131) 304 (Status) (73) count per **30s** | (**76640** hits)




## RESPONSE STATUSES




## ALL EVENTS

**0** to **100** of 500 available for paging

| host_addr | @access_log.request | @access_log.status |
|---|---|---|
| wft4 | POST /[redacted]erxmlforapp.do?groupId=7 HTTP/1.1 | 200 |
| wft5 | GET /[redacted]ce/getrecipeinfo.do?auth=[TOKEN]&action=overview&catalog=30438 HTTP/1.1 | 200 |
| wft2 | GET /[redacted]e/getrecipeinfo.do?auth=[TOKEN]&action=overview&catalog=30438 HTTP/1.1 | 200 |
| wft4 | POST /[redacted]xmlforapp.do?groupId=6 HTTP/1.1 | 200 |
| wft3 | GET /[redacted]e/getappcatalogdata.do?path=img&f=catcover.jpg&catalogid=28259 HTTP/1.1 | 200 |
| wft2 | POST /[redacted]/downloadstatus.do HTTP/1.1 | 200 |
| wft5 | GET /[redacted]e/getrecipeinfo.do?action=recipe_of_the_day HTTP/1.1 | 200 |
| wft3 | GET /[redacted]/getappcatalogdata.do?path=img&f=catcover.jpg&catalogid=28414 HTTP/1.1 | 200 |
| wft5 | GET /[redacted]/getappcatalogdata.do?auth=[redacted]784fa20f8d85&catalogid=30656&... | 200 |
| wft5 | GET /[redacted]e/getappcatalogdata.do?auth=[redacted]784fa20f8d85&catalogid=30656&... | 200 |
| wft5 | GET /[redacted]e/getappcatalogdata.do?auth=[redacted]784fa20f8d85&catalogid=30656&... | 200 |
| wft5 | GET /[redacted]e/varnish.do?auth=[redacted]784fa20f8d85&catalogid=30656&path=tile... | 200 |
| wft5 | GET /[redacted]e/getappcatalogdata.do?auth=[redacted]784fa20f8d85&catalogid=30656&... | 200 |
| wft5 | GET /[redacted]e/getappcatalogdata.do?auth=[redacted]784fa20f8d85&catalogid=30656&... | 200 |
| wft5 | GET /[redacted]e/varnish.do?auth=[redacted]784fa20f8d85&catalogid=30656&path=tile... | 200 |

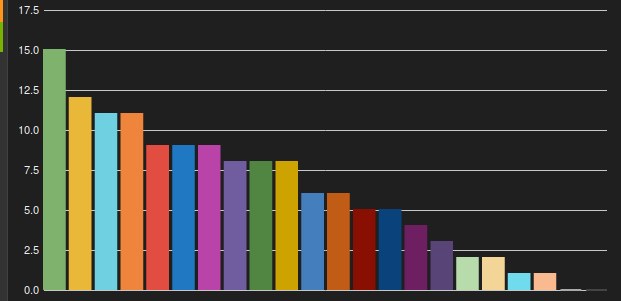
# access_log HTTP 500

an hour ago to a few seconds ago refreshed every 30s

QUERY FILTERING

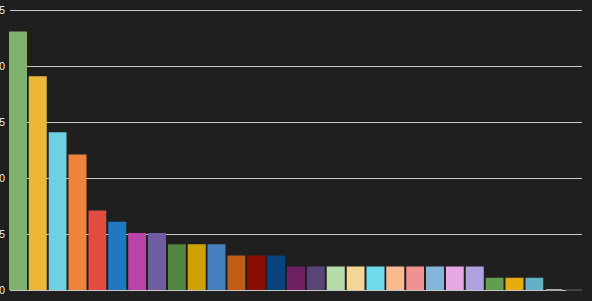
GRAPH

## BY SERVER



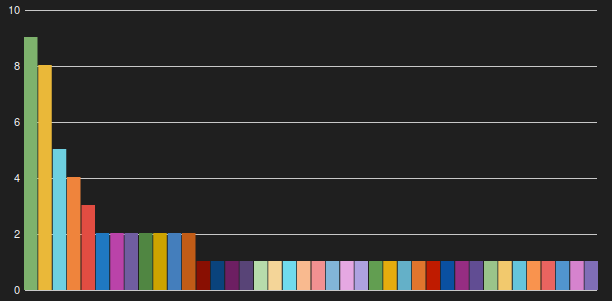

| | |
|---|---|
| 56w[redacted] | 15 |
| 56w[redacted] | 12 |
| 56w[redacted] | 11 |
| 56w[redacted].pl | 11 |
| 56w[redacted] | 9 |
| 56w[redacted] | 9 |
| 56w[redacted] | 9 |
| wfin[redacted].pl | 8 |
| 56w[redacted] | 8 |
| 56w[redacted].pl | 8 |
| wfin[redacted].pl | 6 |
| 56w[redacted].pl | 6 |
| wfin[redacted].pl | 5 |
| 56w[redacted].pl | 5 |
| 56w[redacted] | 4 |
| 56w[redacted].pl | 3 |
| wfrn[redacted].pl | 2 |
| 56w[redacted].pl | 2 |
| form[redacted]ia.pl | 1 |
| 56w[redacted].pl | 1 |
| Missing field | 0 |
| Other values | 0 |

## BY HOST




| | |
|---|---|
| forum.interia.pl | 23 |
| motoryzacja.interia.pl | 19 |
| ding.interia.pl | 14 |
| swiatseriali.interia.pl | 12 |
| www.pomponik.pl | 7 |
| dzikikraj.interia.pl | 6 |
| praca.interia.pl | 5 |
| konto.interia.pl | 5 |
| mamdziecko.interia.pl | 4 |
| magazynauto.interia.pl | 4 |
| ifr-lib.interia.pl | 4 |
| szukaj.interia.pl | 3 |
| quizy.interia.pl | 3 |
| olimpiada.interia.pl | 3 |
| zdjecia.interia.pl | 2 |
| www.styl.pl | 2 |
| www.rmf24.pl | 2 |
| www.interia.tv | 2 |
| pogoda.interia.pl | 2 |
| poczta-api.interia.pl | 2 |
| ifr-lib.smaker.pl | 2 |
| firma.interia.pl | 2 |
| film.interia.pl | 2 |
| fakty.interia.pl | 2 |
| www.poboczem.pl | 1 |
| m.interia.pl | 1 |
| janusz.pyzio.antyspam.forms.interia.pl.ds.iplv2.bauer-pl.bauermedia.group | 1 |
| Missing field | 0 |

## BY PATH




| | |
|---|---|
| /robots.txt | 9 |
| /_vti_bin/owssvr.dll | 8 |
| / | 5 |
| /https://ifr-lib.interia.pl/ | 4 |
| /pokaz-komentarz,pId,84872424,dId,2483306 | 3 |
| /v1/attachment/fileUpload | 2 |
| /szukaj | 2 |
| /s/images/star.png | 2 |
| /poczta/nowe-konto | 2 |
| /mapa-serwisu | 2 |
| /komentarze/odpowiedz/formularz | 2 |
| /iframe.html | 2 |
| /wyloguj | 1 |
| /wyjete-z-sieci/memy-po-debacie-blad-404-hitem-internetu-zdjecie,iId,1946612,iAId,177058 | 1 |
| /wyjete-z-sieci/memy-po-debacie-blad-404-hitem-internetu-zdjecie,iId,1946609,iAId,177058 | 1 |
| /wyjete-z-sieci/memy-po-debacie-blad-404-hitem-internetu-zdjecie,iId,1946606,iAId,177058 | 1 |
| /wiadomosci,nPack,2 | 1 |
| /wiadomosci,4040,0,85,895167 | 1 |
| /watek-chronologicznie/trace-ochote-do-zycia,9373,616312,0,c,4,122,0,0 | 1 |
| /watek-chronologicznie/ogloszenia-towarzyskie,8024,1010008,,c,1,2,0,0 | 1 |
| /uczucia/news-w-malzenstwie-trzeba-umiec-sie-klocic,nId,2285501 | 1 |
| /testy/pierwsze-jazdy/news-honda-cr-z-pierwsza-jazda,nId,613676 | 1 |
| /tagi-jezyk-francuski,tId,105309 | 1 |
| /sport | 1 |
| /serwis/forum/a6w-opinie-wady-i-zalety-tematy,dId,2727256 | 1 |
| /rss/komentarze,dId,2264227,srvId,1035 | 1 |
| /rss/komentarze,dId,2262989,th,65036119,srvId,1035 | 1 |
| /rss/komentarze,dId,2229788,srvId,1 | 1 |

# Varnish access PROD - hitmiss - separated

a day ago to a few seconds ago

QUERY

@http_request.@uri.path:

@http_request.@uri.path:"/

@http_request.@uri.path:"/

@http_request.@uri.path:"/

@http_request.@uri.path:"/

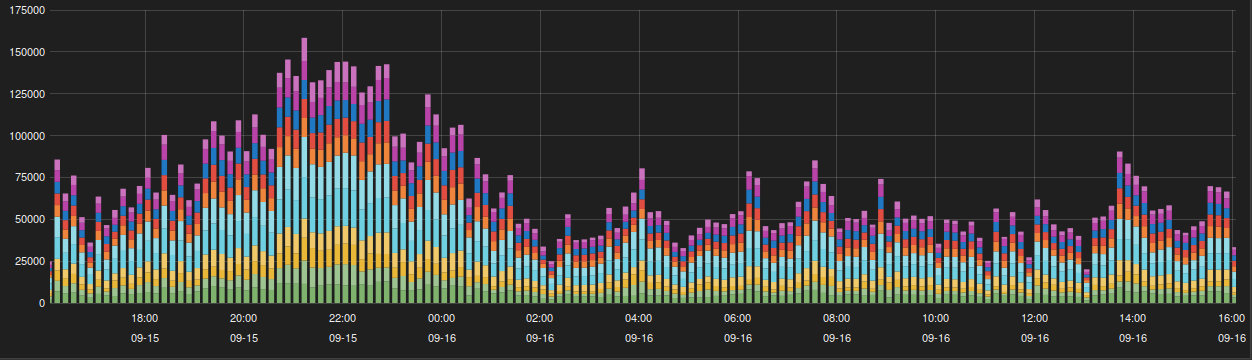
@http_request.@uri.path:"/

NOT @http_request.@uri.path:b

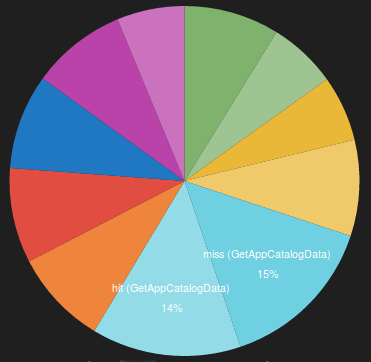
FILTERING

## EVENTS OVER TIME

View | Zoom Out | miss ('' space') (877814) hit ('' space') (628199) hit (GetAppData) (606182) miss (GetAppData) (884499) miss (GetAppCatalogData) (1466071) hit (GetAppCatalogData) (1376222) miss (GetRecipeInfo) (874631) miss (XMLForApp) (874631) miss (GetWebData) (874631) miss (Other) (874652) hit (Other) (622479) count per **10m** | (**9960011** hits)



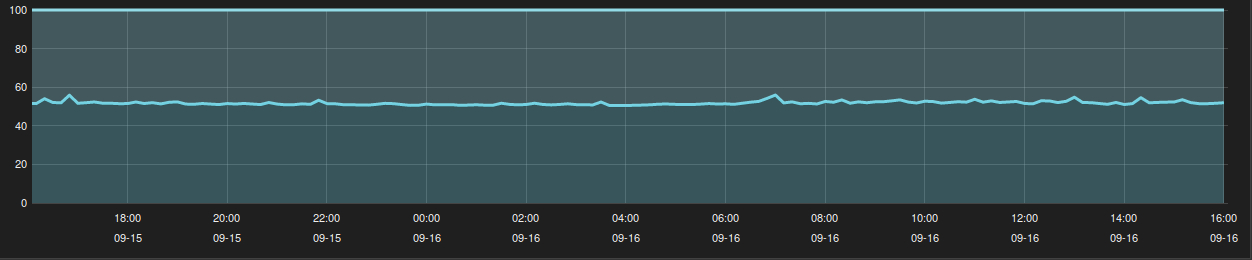

## HITS



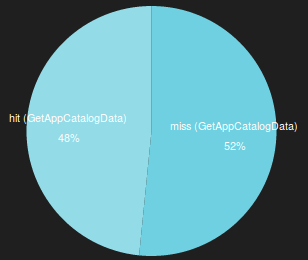

miss ('' space') (877825) hit ('' space') (628204) hit (GetAppData) (606186) miss (GetAppData) (884510) miss (GetAppCatalogData) (1466086) hit (GetAppCatalogData) (1376235) miss (GetRecipeInfo) (874642) miss (XMLForApp) (874642) miss (GetWebData) (874642) miss (Other) (874663) hit (Other) (622484)

## HIT-MISS RATIO

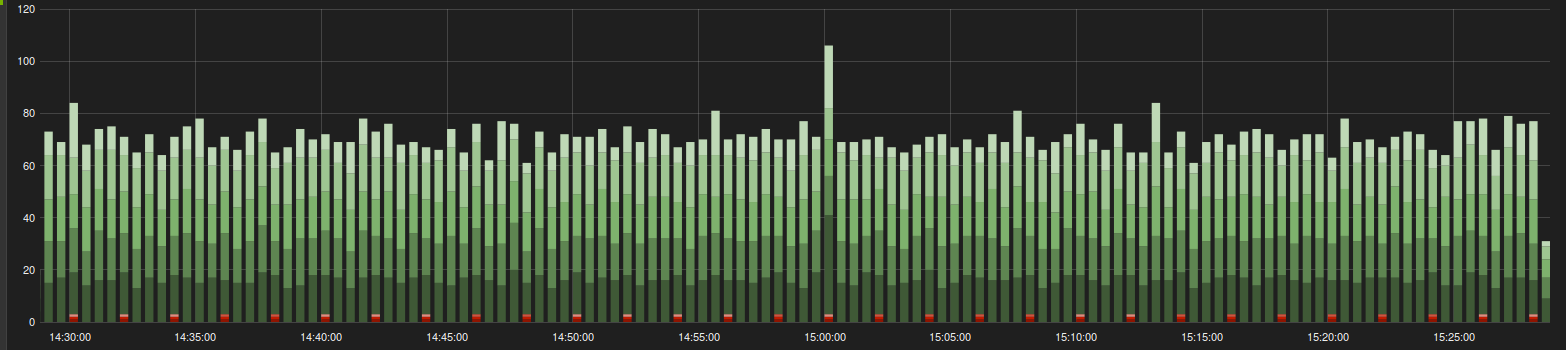
View | Zoom Out | miss (GetAppCatalogData) (1466011) hit (GetAppCatalogData) (1376157) count per **10m** | (**2842168** hits)

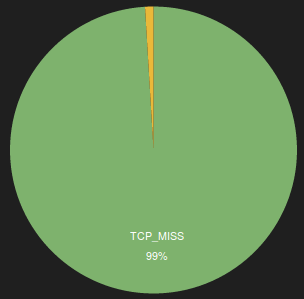



## HIT-MISS RATIO




GETAPPDATA





# Proxy access_log

**time** must ●
**field** : @timestamp
**from** : now-1h
**to** : now

**field** must ●
**field** : forwarder_tags
**query** : "squid_access"

**field** mustNot ●
**field** : @squid_access.user_agent
**query** : check_http nagios-plugins

**field** mustNot ●
**field** : @http_request.uri
**query** : "cache_object://info/info"

**field** mustNot ●
**field** : @http_request.uri
**query** : "[redacted]
/-/0003D[redacted]"

## EVENTS OVER TIME

View ▸ | Zoom Out | ● proxy1.stg[redacted] (Failed Requests) (30) ● proxy1.itg[redacted] (Failed Requests) (30) ● proxy2[redacted] (Failed Requests) (15) ● proxy1[redacted] (Failed Requests) (15) ● proxy1.itg[redacted] (SucessRequests) (1882) ● proxy2.stg[redacted] (SucessRequests) (1857) ● proxy1.stg[redacted] (SucessRequests) (1857) ● proxy2.itg[redacted] (SucessRequests) (1855) ● proxy2[redacted] (SucessRequests) (987) count per **30s** | (**8528** hits)

## CACHE HIT RATIO

## ALL EVENTS

**0** to **100** of 500 available for paging

| @squid_access.clientip | @squid_access.request | @squid_access.request_status | @squid_access.hierarchy_status | @squid_access.user_agent | @squid_access.referer |
|---|---|---|---|---|---|
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v2.0.3 (nagios-plugins 2.0.3) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v2.0.3 (nagios-plugins 2.0.3) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v1.4.16 (nagios-plugins 1.4.16) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v2.0.3 (nagios-plugins 2.0.3) | |
| 127.0.0.1 | GET cache_object://info/info HTTP/1.0 | TCP_MISS | NONE | check_http/v2.0.3 (nagios-plugins 2.0.3) | |

# Proxy apple errors

6 hours ago to 2 minutes ago refreshed every 15m

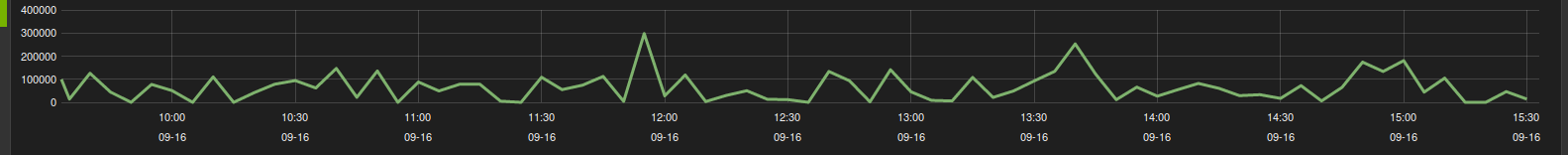
QUERY

id_access.response_time:[0 TO 1000] | cess.response_time:[1001 TO 10000] | sponse_time:[10001 TO 100000]

FILTERING

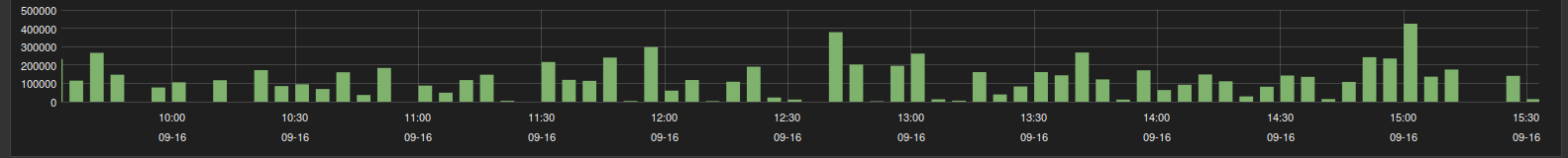
## MEAN TRANSACTION TIME [MS]

View | Zoom Out | 200 (status) (554) **@squid_access.response_time** mean per **5m** | (**554** hits)



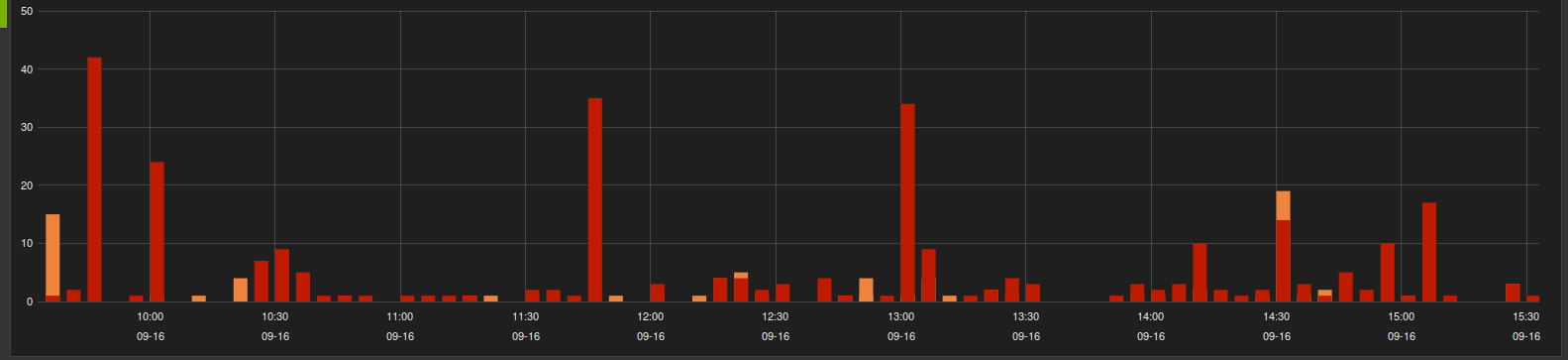

## MAX TRANSACTION TIME [MS]

View | Zoom Out | 200 (status) (554) **@squid_access.response_time** max per **5m** | (**554** hits)



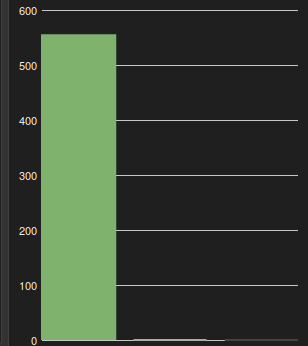

## MAX TRANSACTION TIME [MS]

View | Zoom Out | 0-1s (8) 1-10s (77) 10-100s (295) count per **5m** | (**380** hits)




## STATUS

200 (554) Missing field (0)
Other values (0)



kibana | Discover | Visualize | Dashboard | Settings | Last 24 hours

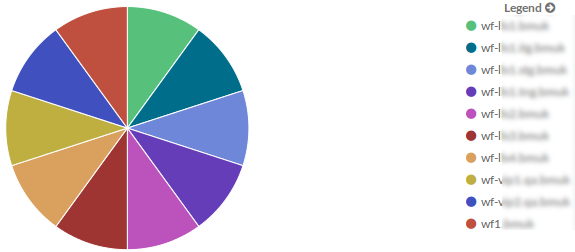
logstash-forwarder errors | *

## logstash-forwarder errors count

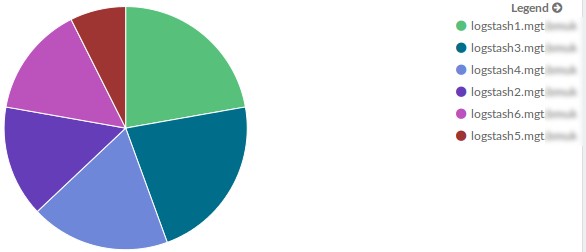
27

Count

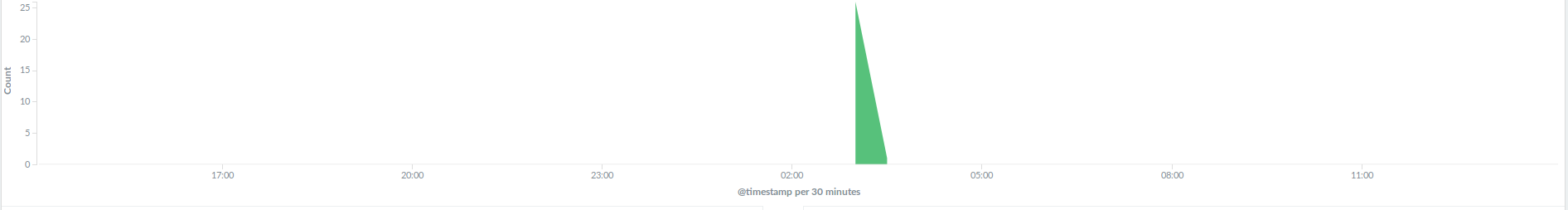
## logstash-forwarder errors per host




## logstash-forwarder errors per logstash



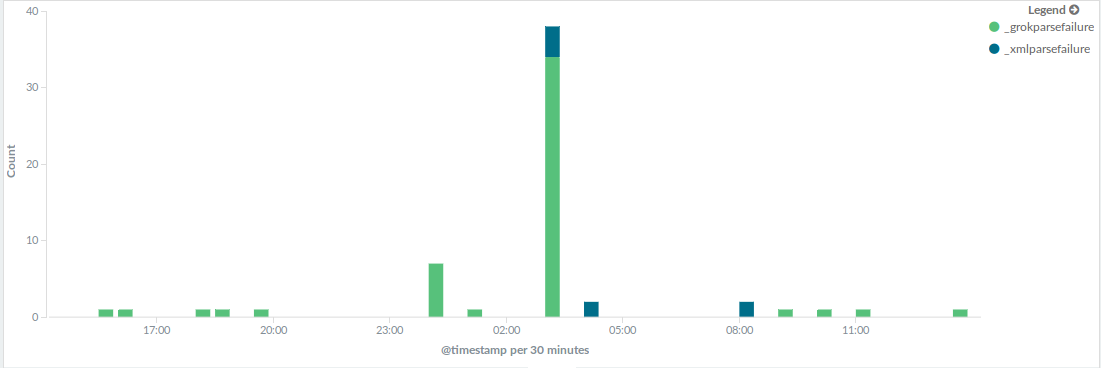

## logstash-forwarder errors histogram




## logstash_forwarder errors

| Time | tags | host | logstash_node | message |
|---|---|---|---|---|
| October 6th 2016, 03:40:04.391 | multiline | wf-l | logstash6.m | { "network": { "ssl ca": "/etc/ssl/logstash-forwarder.crt", "timeout": 60, "servers": [ "logstash1.mgt.bmuk:5959", |
| October 6th 2016, 03:10:09.059 | multiline | wf1 | logstash6.m | { "network": { "ssl ca": "/etc/ssl/logstash-forwarder.crt", "timeout": 60, "servers": [ "logstash1.mgt.bmuk:5959", |

## parsefailure histogram




## logstash-forwarder files

| Top 100 file.raw | Count |
|---|---|
| /var/log/varnish/access.log | 23,244,864 |
| /var/log/apache2/access_log | 6,587,297 |
| /var/log/[redacted]Service.xml | 5,688,627 |
| /var/log/varnish/varnishncsa.log | 2,205,003 |
| /var/log/[redacted]Service.xml | 1,738,478 |
| /var/log/[redacted]/frontend/[redacted].xml | 1,488,257 |
| /var/log/nginx/access_log | 679,958 |
| /var/log/[redacted]/frontend/[redacted].xml | 373,796 |
| /var/log/gearmand/gearmand.log | 315,415 |
| /var/log/[redacted]le1.xml | 240,918 |

## logstash-forwarder types

| Top 100 type.raw | Count |
|---|---|
| varnish_access_log | 25,463,546 |
| [redacted] | 13,285,704 |
| apache_access_log | 6,587,297 |
| nginx_access_log | 901,599 |
| gearmand | 315,415 |
| gearman_clients | 130,296 |
| php_error_log | 127,259 |
| nginx_error_log | 120,573 |
| pound | 25,009 |
| logstash_forwarder | 12,198 |

## grokparsefailure

1 2 »

| Time | host | type | message |
|---|---|---|---|
| October 6th 2016, 13:33:42.702 | wf6[redacted] | apache_error_log | zend_mm_heap corrupted |
| October 6th 2016, 11:29:10.775 | wf5[redacted] | apache_error_log | zend_mm_heap corrupted |
| October 6th 2016, 10:12:26.371 | wf-l[redacted] | apache_access_log | 10.172.135.27 - - [06/Oct/2016:10:12:24 +0200] [redacted] "ea/fb324/62d06/fbeca/maxineashley2_466x466.jpg?1431960528 HTTP/1.1 " 400 226 "-" "-" [-] 0 69 226 |
| October 6th 2016, 09:23:53.809 | wf1[redacted] | apache_error_log | zend_mm_heap corrupted |
| October 6th 2016, 03:10:13.230 | wf1[redacted] | logstash_forwarder | vice.xml |
| October 6th 2016, 03:10:09.883 | wf-l[redacted] | logstash_forwarder | etc/logstash-forwarder.conf |

## xmlparsefailure

| Time | host | file | message |
|---|---|---|---|
| October 6th 2016, 08:05:15.757 | grmq2.[redacted] | /var/log/gearman/worker/Search.xml | </message><priority>6</priority><priorityName>INFO</priorityName><pid>12615</pid></logEntry> |
| October 6th 2016, 08:05:10.285 | grmq2.[redacted] | /var/log/gearman/worker/Search.xml | <logEntry><timestamp>2016-10-06T06:05:09+00:00</timestamp><message>Updated 41-news-98038 |
| October 6th 2016, 04:05:31.356 | grmq2.[redacted] | /var/log/gearman/work | </message><priority>6</priority><priorityName>INFO</priorityName><pid>12615</pid></logEntry> |

sources

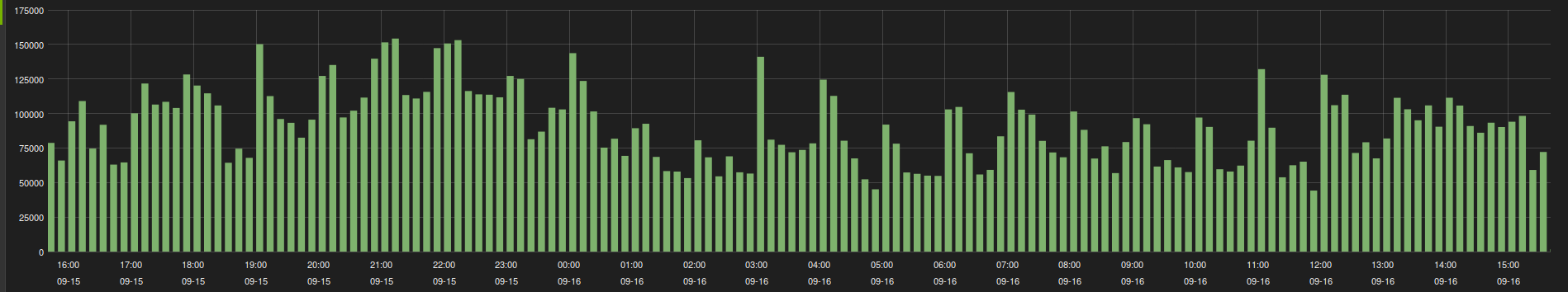
# Analyzing log sources

a day ago to a few seconds ago

QUERY FILTERING

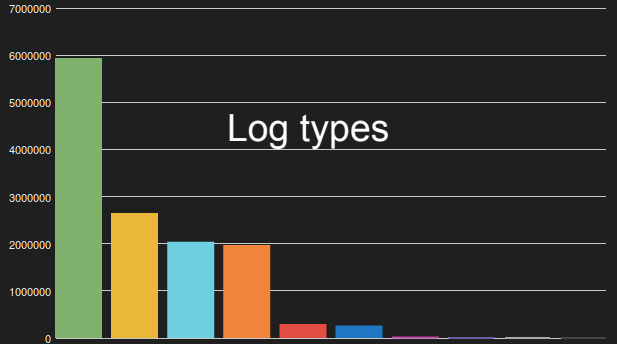
## EVENTS OVER TIME

View | Zoom Out | (13051294) count per **10m** | (**13051294** hits)



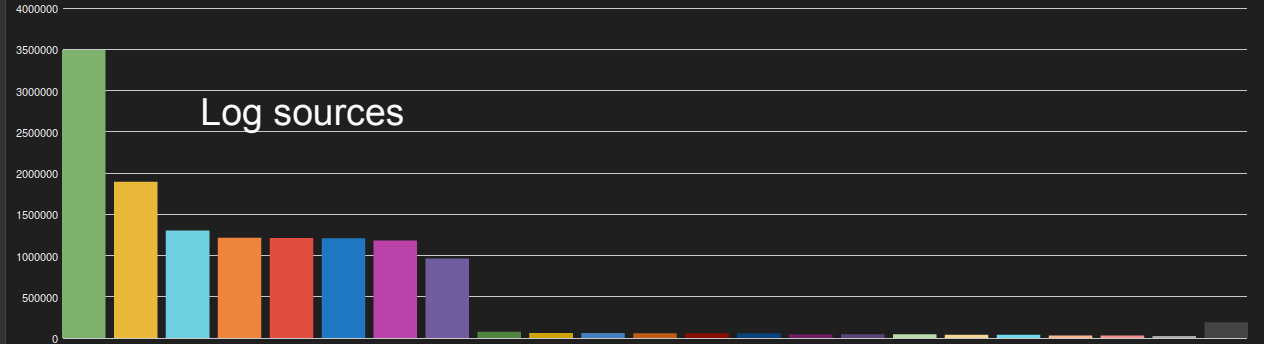

## TERMS

_rolling_info (5916065) access_log (2632759) json (2020118)
varnish_access (1953806) server_xml (276427) squid_access (241727) java_gc (10389)
java_xml (90) Missing field (0) Other values (0)



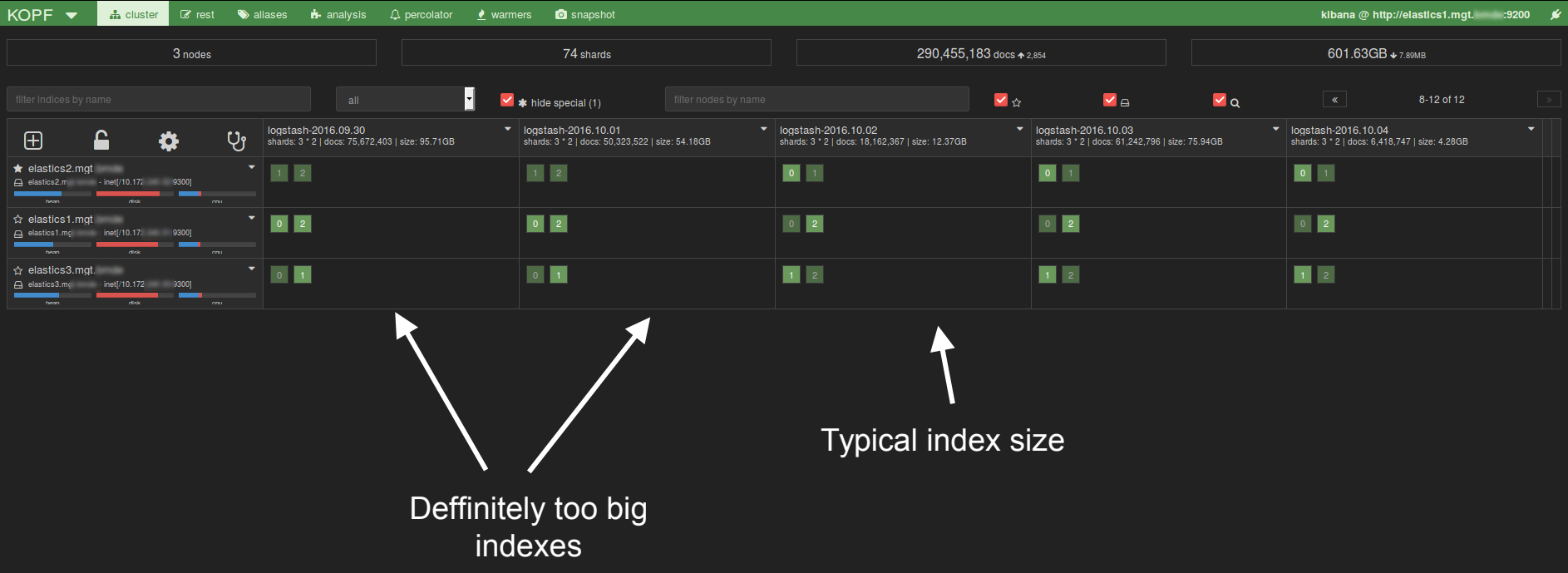

## TERMS

bft1 (3478943) vc1 (1881953) wft4 (1291555) wft3. (1202152) wft5 (1199825) wft2 (1197989) wft1 (1170143) bft1.itg. (951432)
vc2 (62642) proxy1.itg. (48155) proxy1.stg (47502) proxy2.stg. (46064) proxy2.itg. (46064) sftp1. (45982) bkl4. (33753) bkl7 (32984)
bkl5. (32964) bkl8. (28726) bkl2 (27455) bkl6. (18332) bkl3 (18024) Missing field (11048) Other values (177739)




## EVENTS

ADD A ROW


KOPF
cluster
rest
aliases
analysis
percolator
warmers
snapshot
kibana @ http://elastics1.mgt.:9200
3 nodes
74 shards
290,455,183 docs 2,854
601.63GB 7.89MB
filter indices by name
all
hide special (1)
filter nodes by name
8-12 of 12
logstash-2016.09.30
shards: 3 * 2 | docs: 75,672,403 | size: 95.71GB
logstash-2016.10.01
shards: 3 * 2 | docs: 50,323,522 | size: 54.18GB
logstash-2016.10.02
shards: 3 * 2 | docs: 18,162,367 | size: 12.37GB
logstash-2016.10.03
shards: 3 * 2 | docs: 61,242,796 | size: 75.94GB
logstash-2016.10.04
shards: 3 * 2 | docs: 6,418,747 | size: 4.28GB
elastics2.mgt
elastics1.mgt
elastics3.mgt
Deffinitely too big indexes
Typical index size

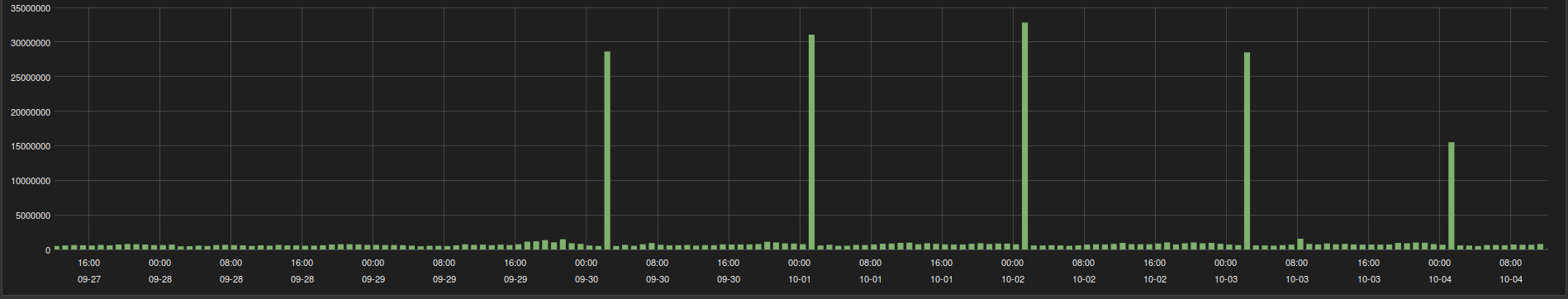
sources

7 days ago to 8 minutes ago

QUERY | FILTERING

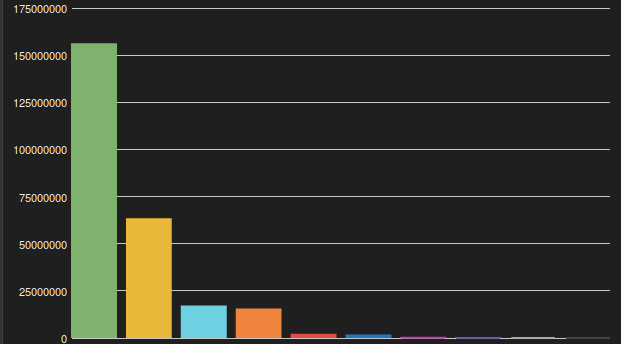
## EVENTS OVER TIME

View | Zoom Out | (253757521) count per **1h** | (**253757521** hits)



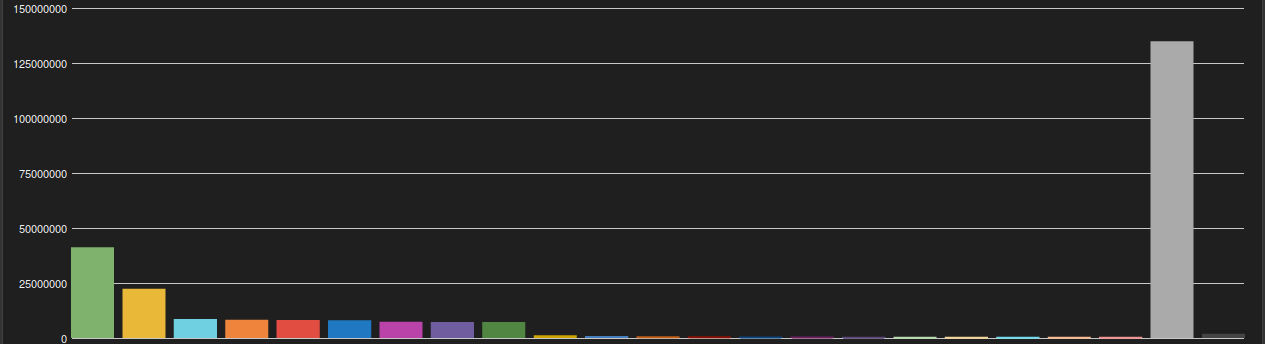

## TERMS

json (155768934) [illegible]_rolling_info (62993976) access_log (16727805)
varnish_access (15081230) squid_access (1687875) [illegible]ver_xml (1341219)
java_gc (155400) java_xml (3012) Missing field (0) Other values (0)



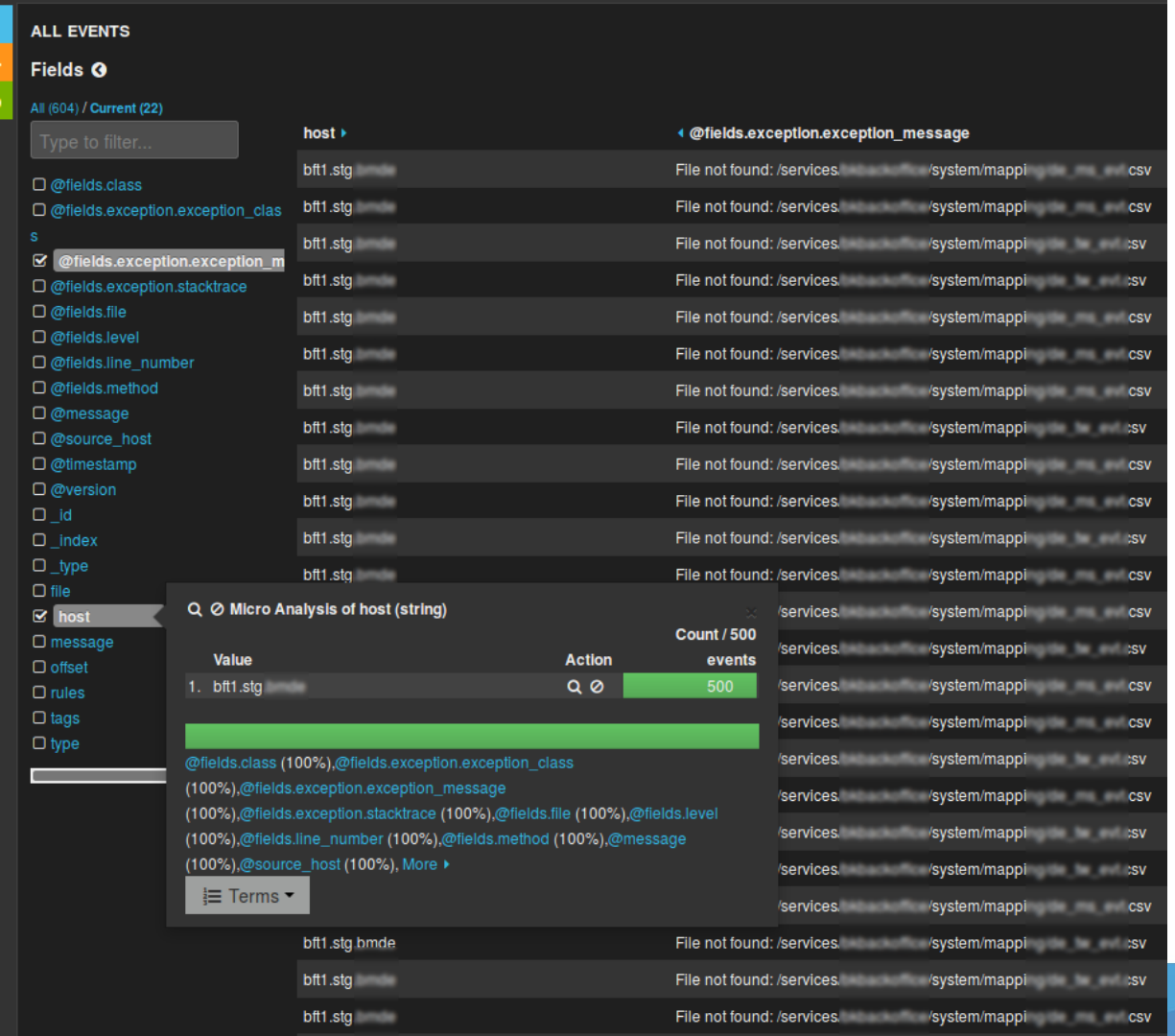

## TERMS

bft1 [illegible] (40771919) wft1 [illegible] (21971977) wft3 [illegible] (8156372) wft2 [illegible] (7837738) wft4 [illegible] (7692345) wft5 [illegible] (7647671) vc3 [illegible] (6966245) vc4 [illegible] (6867944)
bft1.itg [illegible] (6806075) vc1 [illegible] (744019) vc2 [illegible] (438434) proxy1.itg [illegible] (336735) proxy1.stg [illegible] (285049) proxy2.itg [illegible] (276417) proxy2.stg [illegible] (276413) sftp1 [illegible] (153984)
bkl5 [illegible] (142836) bkl2 [illegible] (137099) bkl4 [illegible] (133495) proxy1 [illegible] (124681) wft1.itg [illegible] (124418) Missing field (134404271) Other values (1466213)




## EVENTS

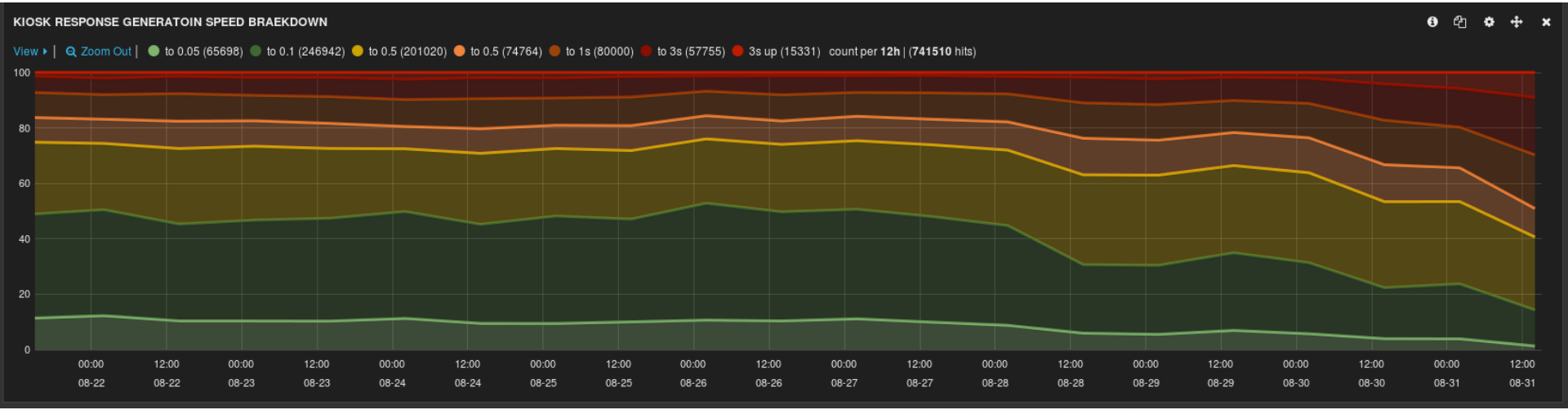
ADD A ROW




1. Few clicks and it was clear who's guilty
2. Adding another table panel with "terms" filter we were able to list all lacking files
3. I can't imagine simpler way to nail it

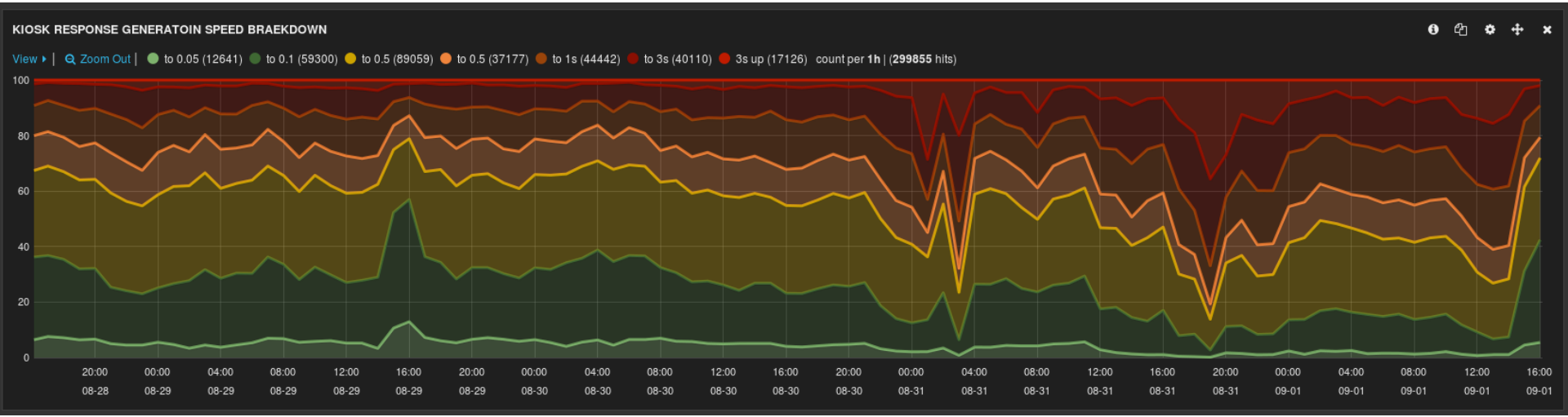
# Response time analysis

New search mechanism, full reindex required - did it and how affect performance of service?



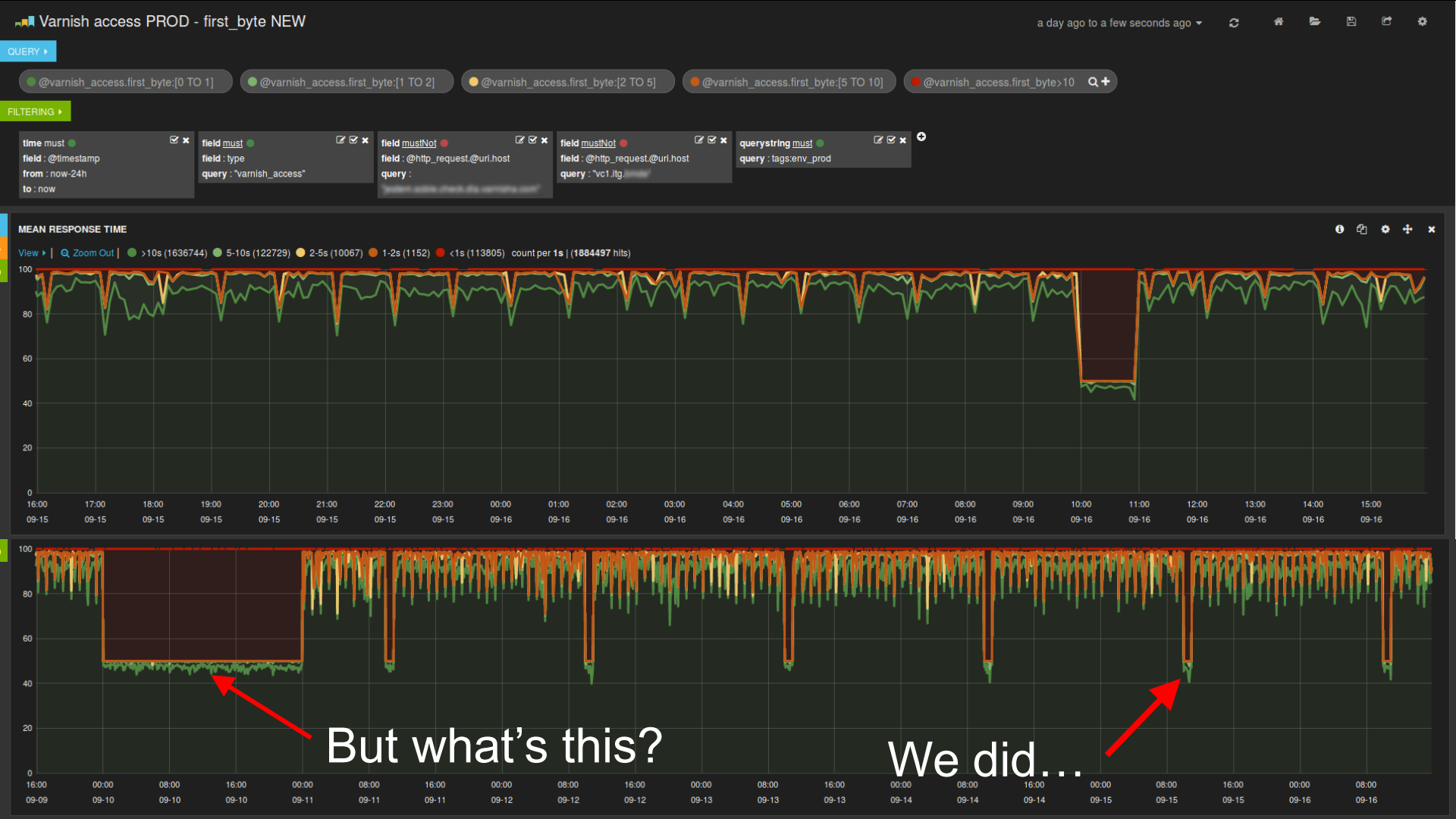
# Response time analysis

Kibana allowed us to actually see impact of our changes on application latency.




What's that hour long hole?

Do we have it more than once?


Varnish access PROD - first_byte NEW
a day ago to a few seconds ago
QUERY
@varnish_access.first_byte:[0 TO 1]
@varnish_access.first_byte:[1 TO 2]
@varnish_access.first_byte:[2 TO 5]
@varnish_access.first_byte:[5 TO 10]
@varnish_access.first_byte>10
FILTERING
time must
field : @timestamp
from : now-24h
to : now
field must
field : type
query : "varnish_access"
field mustNot
field : @http_request.@uri.host
query :
field mustNot
field : @http_request.@uri.host
query : "vc1.itg
querystring must
query : tags:env_prod
MEAN RESPONSE TIME
View | Zoom Out | >10s (1636744) 5-10s (122729) 2-5s (10067) 1-2s (1152) <1s (113805) count per 1s | (1884497 hits)
But what's this?
We did…

# WFT request types

6 hours ago to a few seconds ago

QUERY

FILTERING

**time** must
**field** : @timestamp
**from** : now-6h
**to** : now

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getrecipeinfo.do"

**field** must
**field** : type
**query** : "access_log"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/monitor.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/downloadstatus.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/bauerxmlforapp.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/login.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/manager/status?XML=true"

**querystring** mustNot
**query** : @http_request.uri:"/[redacted]/xmlforapp.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getappcatalogdata.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]varnish.do"

**field** mustNot
**field** : @http_request.uri
**query** : update.plist

**field** mustNot
**field** : @http_request.uri
**query** : banner.plist

**field** mustNot
**field** : @http_request.uri
**query** : localizationInfo.plist

**field** mustNot
**field** : @http_request.uri
**query** : localization.zip

**field** mustNot
**field** : @http_request.uri
**query** : "/favicon.ico"

**field** mustNot
**field** : @http_request.uri
**query** : banner.zip

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getappdata.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]er/"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]ets"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]resources"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/registerPush.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getCatalogPage.do"

**field** must
**field** : host
**query** : wft*

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getwebdata.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]atalog/webclient/"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/customerlogin.do"

**field** mustNot
**field** : @access_log.status
**query** : 403

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getCss.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/assets/"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getcatalogwebclient.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/favicon.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/getcatalog.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/logout.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/catalogsearch.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/atomfeed.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/sendappfeedback.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/catalogmngt.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]/customerpage.do"

**field** mustNot
**field** : @http_request.uri
**query** : "/[redacted]//multimedia/"

GRAPH

ALL EVENTS

Fields

All (554) / Current (22)

Type to filter...

- @access_log.clientip
- @access_log.request
- @access_log.status
- @access_log.timestamp
- @http_request.method
- @http_request.proto_version
- @http_request.uri
- @timestamp

**0** to **100** of 117 available for paging

| @http_request.uri | @access_log.status |
|---|---|
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]I22242BBCB564.n2?path=img&f=catcover.jpg&catalogid=578 | 404 |
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]F19386671A67D.n1?path=img&f=catcover.jpg&catalogid=280 | 404 |
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]FFF107F52332A.n3?path=img&f=catcover.jpg&catalogid=114 | 404 |
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]75A79A70A972.n1?path=img&f=catcover.jpg&catalogid=473 | 404 |
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]34621944B06A1.n2?path=img&f=catcover.jpg&catalogid=235 | 404 |
| /[redacted]/getcatalogdata.do;jsessionid=[redacted]B3E6BFBF519E.n1?path=img&f=catcover.jpg&catalogid=237 | 404 |


# Thank you for attention