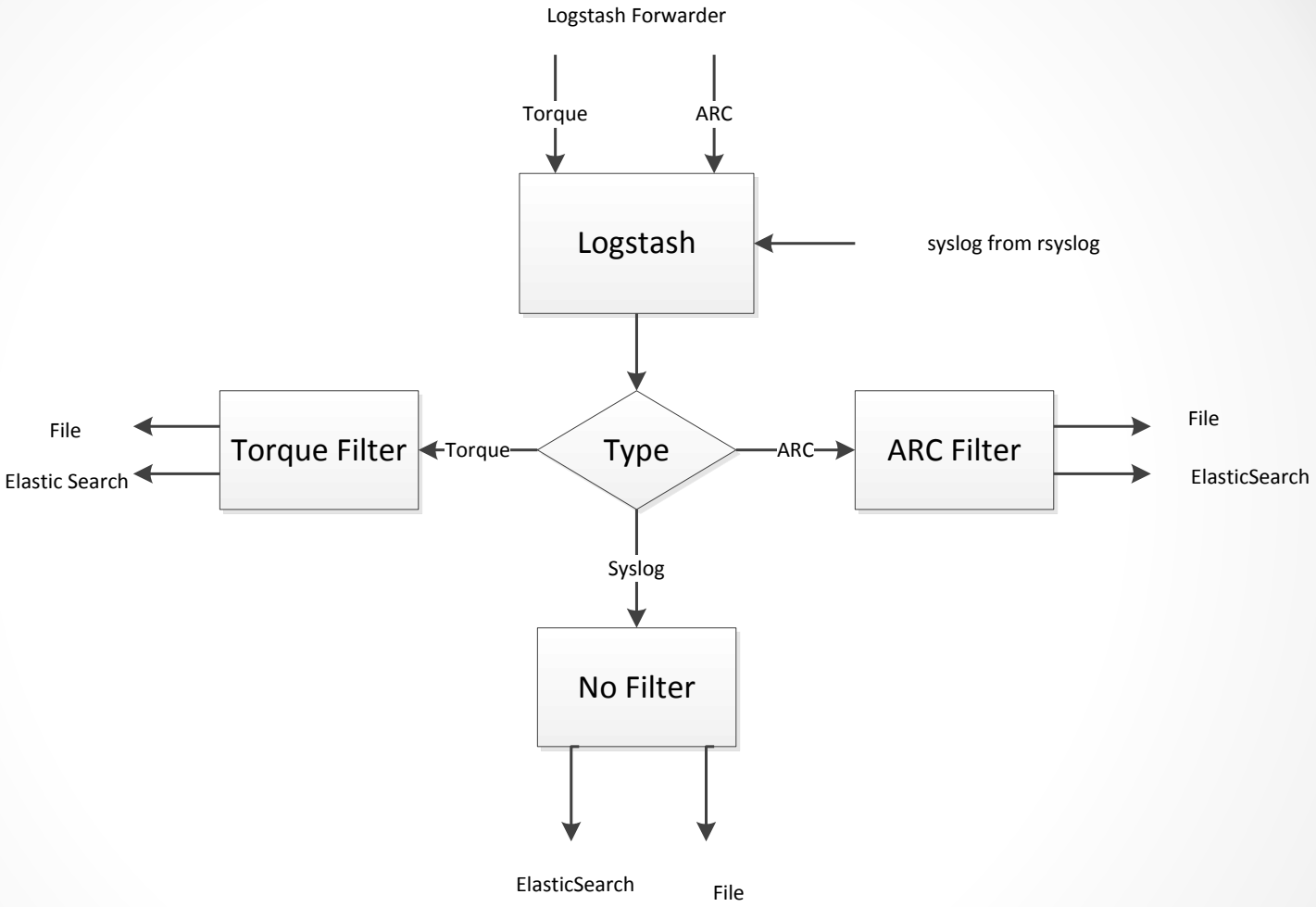
ELK Stack

Kashif Mohammad
University of Oxford

Motivations

- Looks cool
- Planning to use as Central Sys-Logger
- Accounting
- Look for interesting patterns
- Easy to extend


Logstash Forwarder
Torque
ARC
Logstash
syslog from rsyslog
File
Elastic Search
Torque Filter
Torque
Type
ARC
ARC Filter
File
ElasticSearch
Syslog
No Filter
ElasticSearch
File

Client configuration

/etc/logstash-forwarder.conf

```
{
  "network": {
    "servers": ["logger.physics.ox.ac.uk:5004"],

    "ssl ca": "/etc/pki/tls/certs/logger.crt",

    "timeout": 15
  },

  "files": [
  {
      "paths": ["/var/torque/server_priv/accounting/*"],

      "fields": { "type": "torquelogs" }
  }
 ]
}
```

/etc/rsyslog.conf.d/local.conf

```
*.*                                    @logger:5514
```

Server configuration

```
input {
  lumberjack {
      port => 5004
      type => "torquelogs"
      ssl_certificate => "/etc/grid-security/logger.crt"
      ssl_key => "/etc/grid-security/logger.key"

    }

}

filter{
    if [type] == "torquelogs" {
    grok {
     match => [ "message", "%{DATESTAMP:date};E;%{GREEDYDATA:job}.t2torque03.physics.ox.ac.uk;%{GREEDYDATA:KVTOTAL}" ]
     }

     kv {
       source => ["KVTOTAL"]
       remove_field => [ "ctime", "etime", "Resource_List.nodect", "Resource_List.nodes", "session", "end" ]
       }
       grok { match => [ "resources_used.cput", "%{INT:cpu_used_h:int}:%{INT:cpu_used_m:int}:%{INT:cpu_used_s:int}" ] }
       grok { match => [ "resources_used.walltime", "%{INT:walltime_used_h:int}:%{INT:walltime_used_m:int}:%{INT:walltime_used_s:int}" ] }
        if [Resource_List.walltime] { grok { match => [ "Resource_List.walltime", "%{INT:walltime_asked_h:int}:%{INT:walltime_asked_m:int}:%{INT:walltime_asked_s:int}" ] } }
       grok { match => [ "resources_used.mem", "%{INT:mem_used_kb:int}" ] }
       grok { match => [ "resources_used.vmem", "%{INT:vmem_used_kb:int}" ] }
       if [Resource_List.mem] { grok { match => [ "Resource_List.mem", "%{INT:mem_ask:int}%{GREEDYDATA:mem_ask_unit}" ] } }
       if [Resource_List.neednodes] and [Resource_List.neednodes] =~ "ppn" {
          grok { match => [ "Resource_List.neednodes", "%{INT:nodes_asked:int}:ppn=%{INT:cpus_asked:int}" ] }
       }
       if "_grokparsefailure" not in [tags] {
       if [mem_ask_unit] == "gb" { ruby { code => "event['mem_ask_kb'] = event['mem_ask']*1048576" } }
          else if [mem_ask_unit] == "mb" { ruby { code => "event['mem_ask_kb'] = event['mem_ask']*1024" } }
          else if [mem_ask_unit] == "b" { ruby { code => "event['mem_ask_kb'] = event['mem_ask']/1024" } }
          else if [mem_ask_unit] == "kb" { ruby { code => "event['mem_ask_kb'] = event['mem_ask']" } }
       ruby { code => "event['cpu_used_tot'] = (event['cpu_used_h']*3600)+(event['cpu_used_m']*60)+event['cpu_used_s']" }
       ruby { code => "event['walltime_used_tot'] = (event['walltime_used_h']*3600)+(event['walltime_used_m']*60)+event['walltime_used_s']" }
       if [Resource_List.walltime] { ruby { code => "event['walltime_asked_tot'] = (event['walltime_asked_h']*3600)+(event['walltime_asked_m']*60)+event['walltime_asked_s']" } }
       if [walltime_used_tot] != 0 { ruby { code => "event['cpu_efficiency'] = Float(event['cpu_used_tot']) / Float(event['walltime_used_tot'])" } }
       ruby { code => "event['wait_for_start'] = Integer(event['start']) - Integer(event['qtime'])" }
  }
### Cleaning...
       mutate { remove_field => [ "cpu_used_h", "cpu_used_m", "cpu_used_s", "walltime_used_h", "walltime_used_m", "walltime_used_s", "walltime_asked_h", "walltime_asked_m",
"walltime_asked_s", "mem_ask", "qtime", "start", "mem_ask_unit", "Resource_List.mem", "resources_used.cput", "resources_used.walltime", "resources_used.mem",
"resources_used.vmem", "Resource_List.neednodes", "Exit_status", "Resource_List.walltime", "KVTOTAL", "host" ] }
       date {
         match => [ "date" , "MM/dd/YYYY HH:mm:ss" ]
       }
}

}
```

File Edit View History Bookmarks Tools Help

Kibana 3 - Torque

https://logger.physics.ox.ac.uk/#/dashboard/elasticsearch/Torque

logstash kiban

Torque

7 days ago to a few seconds ago

QUERY

*

FILTERING

querystring must
query : *

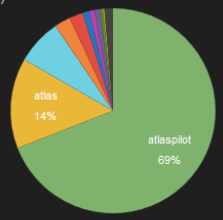
querystring must
query : _type=torquelogs

time must
field : @timestamp
from : now-7d
to : now

querystring mustNot
query : tags=_grokparsefailure

TOP 10 TERMS IN FIELD GROUP

atlaspilot (32175) atlas (6647) cmspilot (3343) alice (1184) lhcbpilot (1016) cms (476) ops (394) snoplus (364) lhcb (241)
alicepilot (125) Missing field (0) Other values (622)



TORQUE

Fields

All (1) / Current (25)

Type to filter...

- @timestamp
- @version
- _id
- _index
- _type
- cpu_efficiency
- cpu_used_tot
- date
- exec_host
- file
- group
- job
- jobname
- mem_used_kb
- message
- offset
- owner
- queue
- Resource_List.cput

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

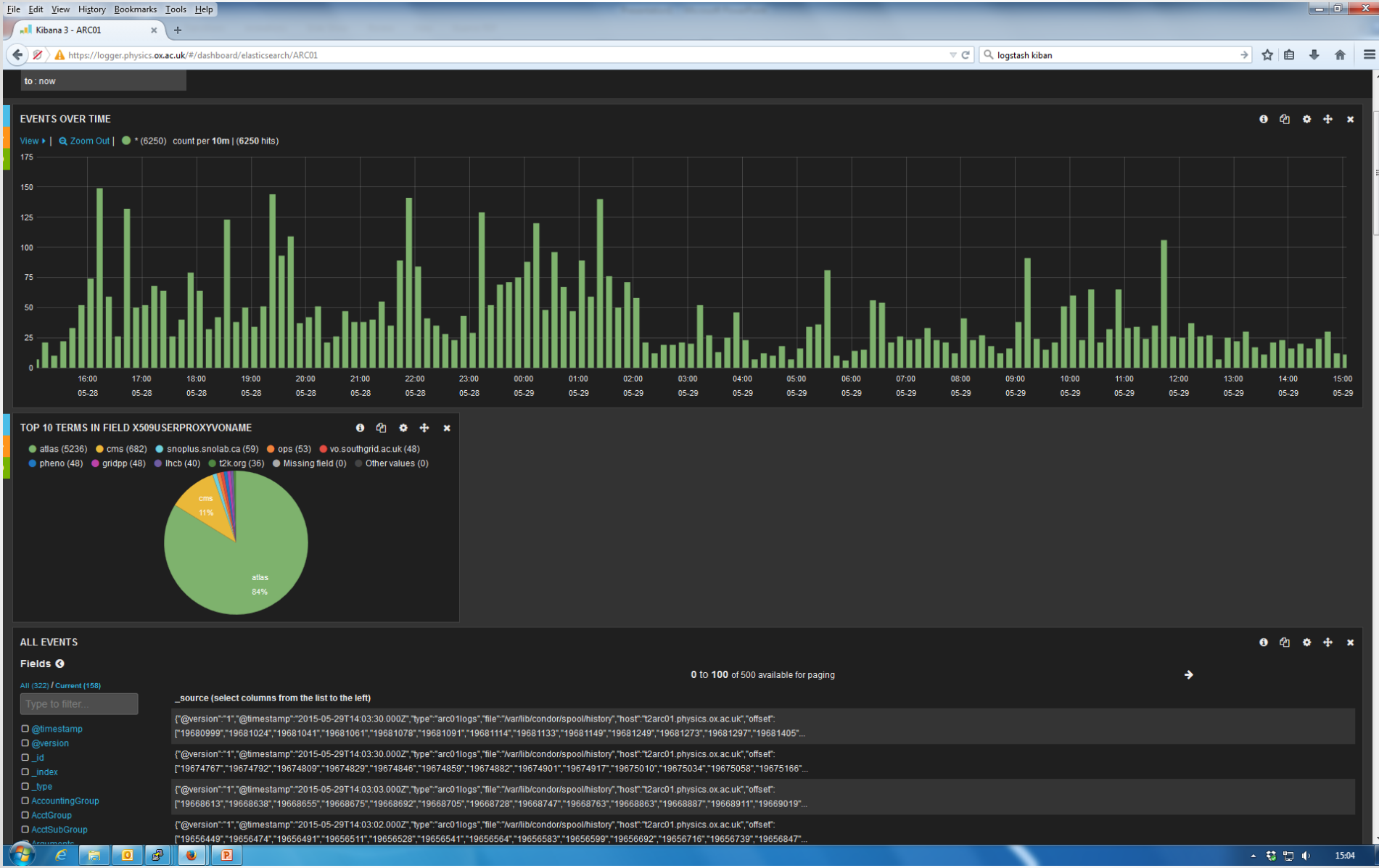
_source (select columns from the list to the left)

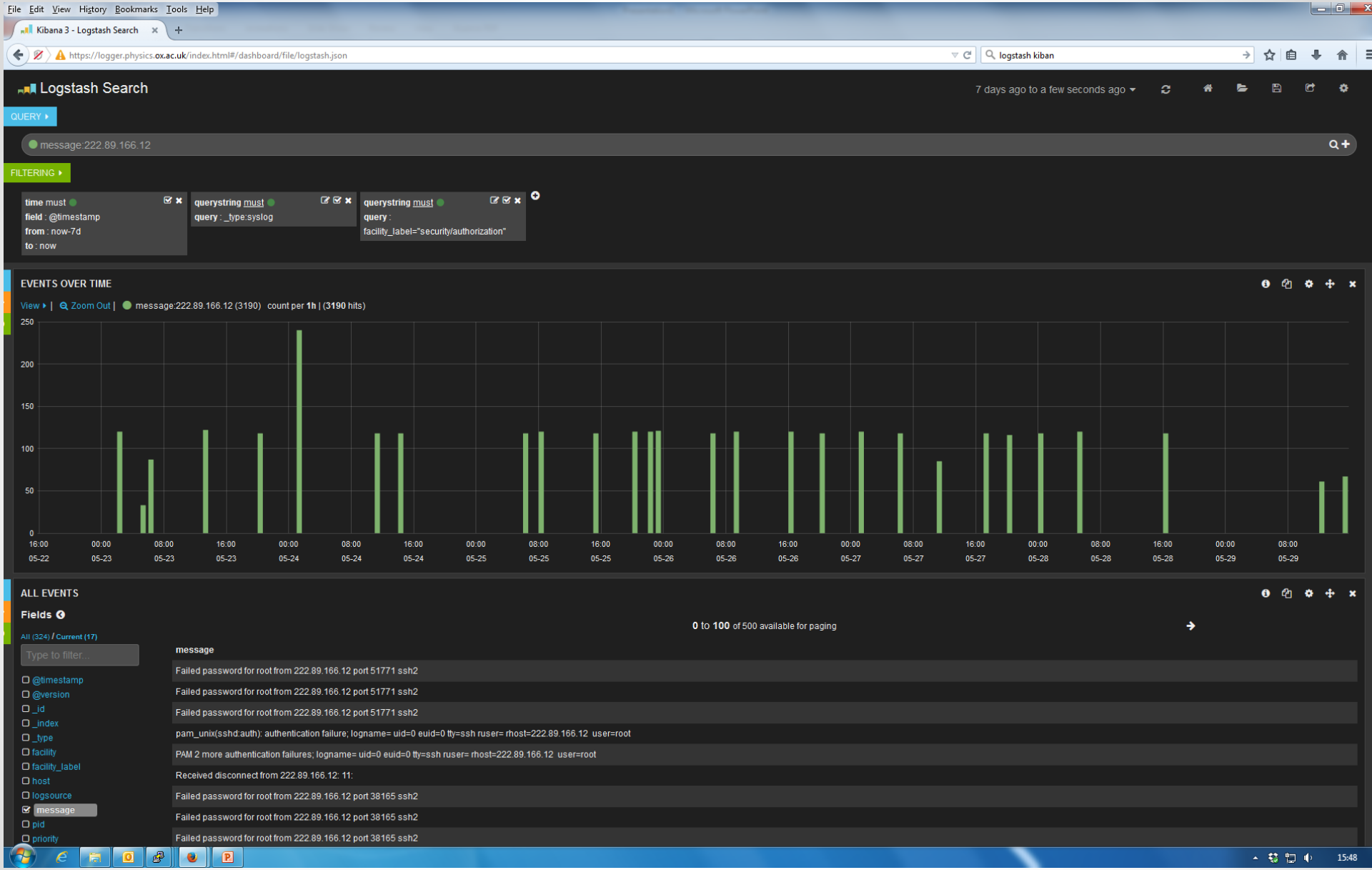
{"message":"05/23/2015 02:08:56;E;4213381.t2torque03.physics.ox.ac.uk;user=atlaspilot018 group=atlaspilot jobname=cream_742971667 queue=longfive ctime=1432341962 qtime=1432341962 etime=1432341962 start=1432342833 owner=atlaspilot018@t2ce06.physics.ox.ac.uk exec_host=t2wn58.physics.ox.ac.uk/0 Resourc...

View: Table / JSON / Raw

Field	Action	Value
@timestamp		2015-05-23T01:08:56.000Z
@version		1
Resource_List.cput		48:00:00
_id		elmlS1hWRYO09GVAbuGyHQ
_index		t2torque-2015.05.00
_type		torquelogs
cpu_efficiency		0.5944333996023857
cpu_used_tot		299
date		05/23/2015 02:08:56
exec_host		t2wn58.physics.ox.ac.uk/0

15:0


File Edit View History Bookmarks Tools Help
Kibana 3 - ARC01
https://logger.physics.ox.ac.uk/#/dashboard/elasticsearch/ARC01
logstash kiban
to : now
EVENTS OVER TIME
View | Zoom Out | * (6250) count per 10m | (6250 hits)
175
150
125
100
75
50
25
0
16:00 05-28
17:00 05-28
18:00 05-28
19:00 05-28
20:00 05-28
21:00 05-28
22:00 05-28
23:00 05-28
00:00 05-29
01:00 05-29
02:00 05-29
03:00 05-29
04:00 05-29
05:00 05-29
06:00 05-29
07:00 05-29
08:00 05-29
09:00 05-29
10:00 05-29
11:00 05-29
12:00 05-29
13:00 05-29
14:00 05-29
15:00 05-29
TOP 10 TERMS IN FIELD X509USERPROXYVONAME
atlas (5236) cms (682) snoplus.snolab.ca (59) ops (53) vo.southgrid.ac.uk (48)
pheno (48) gridpp (48) lhcb (40) t2k.org (36) Missing field (0) Other values (0)
cms
11%
atlas
84%
ALL EVENTS
Fields
0 to 100 of 500 available for paging
All (322) / Current (158)
Type to filter...
_source (select columns from the list to the left)
@timestamp
@version
_id
_index
_type
AccountingGroup
AcctGroup
AcctSubGroup
{"@version":"1","@timestamp":"2015-05-29T14:03:30.000Z","type":"arc01logs","file":"/var/lib/condor/spool/history","host":"t2arc01.physics.ox.ac.uk","offset":
["19680999","19681024","19681041","19681061","19681078","19681091","19681114","19681133","19681149","19681249","19681273","19681297","19681405"...
{"@version":"1","@timestamp":"2015-05-29T14:03:30.000Z","type":"arc01logs","file":"/var/lib/condor/spool/history","host":"t2arc01.physics.ox.ac.uk","offset":
["19674767","19674792","19674809","19674829","19674846","19674859","19674882","19674901","19674917","19675010","19675034","19675058","19675166"...
{"@version":"1","@timestamp":"2015-05-29T14:03:03.000Z","type":"arc01logs","file":"/var/lib/condor/spool/history","host":"t2arc01.physics.ox.ac.uk","offset":
["19668613","19668638","19668655","19668675","19668692","19668705","19668728","19668747","19668763","19668863","19668887","19668911","19669019"...
{"@version":"1","@timestamp":"2015-05-29T14:03:02.000Z","type":"arc01logs","file":"/var/lib/condor/spool/history","host":"t2arc01.physics.ox.ac.uk","offset":
["19656449","19656474","19656491","19656511","19656528","19656541","19656564","19656583","19656599","19656692","19656716","19656739","19656847"...
15:04


File Edit View History Bookmarks Tools Help
Kibana 3 - Logstash Search
https://logger.physics.ox.ac.uk/index.html#/dashboard/file/logstash.json
logstash kiban
Logstash Search
7 days ago to a few seconds ago
QUERY
message:222.89.166.12
FILTERING
time must
field : @timestamp
from : now-7d
to : now
querystring must
query : _type:syslog
querystring must
query :
facility_label="security/authorization"
EVENTS OVER TIME
View | Zoom Out | message:222.89.166.12 (3190) count per 1h | (3190 hits)
250
200
150
100
50
0
16:00 05-22
00:00 05-23
08:00 05-23
16:00 05-23
00:00 05-24
08:00 05-24
16:00 05-24
00:00 05-25
08:00 05-25
16:00 05-25
00:00 05-26
08:00 05-26
16:00 05-26
00:00 05-27
08:00 05-27
16:00 05-27
00:00 05-28
08:00 05-28
16:00 05-28
00:00 05-29
08:00 05-29
ALL EVENTS
Fields
All (324) / Current (17)
Type to filter...
@timestamp
@version
_id
_index
_type
facility
facility_label
host
logsource
message
pid
priority
0 to 100 of 500 available for paging
message
Failed password for root from 222.89.166.12 port 51771 ssh2
Failed password for root from 222.89.166.12 port 51771 ssh2
Failed password for root from 222.89.166.12 port 51771 ssh2
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.89.166.12 user=root
PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.89.166.12 user=root
Received disconnect from 222.89.166.12: 11:
Failed password for root from 222.89.166.12 port 38165 ssh2
Failed password for root from 222.89.166.12 port 38165 ssh2
Failed password for root from 222.89.166.12 port 38165 ssh2
15:48

Thanks