dCache Billing Log Analysis with ELK

9th International dCache Workshop
Amsterdam, NL, 19/5/2015, Johan Guldmyr

CSC–IT CENTER FOR SCIENCE

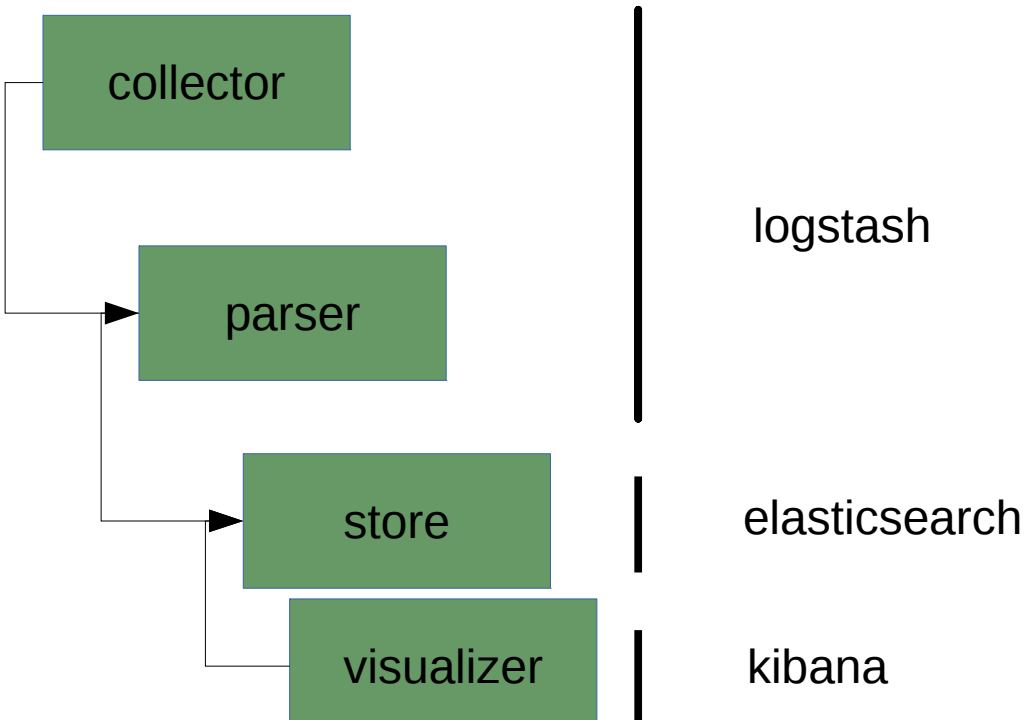
Outline

1) Introduction to the ELK stack
2) Start elasticsearch and kibana3 + kibana4
3) Use logstash to (and in-between look what is in elasticsearch/kibana):
    1) stdin/stdout some events
    2) stdin/elasticsearch some events
    3) file/elasticsearch some billing logs
    4) file/elasticsearch backfill billing logs
4) Make some cool dashboards in the kibanas
5) Bonus Material

Intro2

- Other tools
- Elastic.co
- Uses
  - Correlation
  - Finding patterns
  - Access for non-sysadmins
  - Anonymizing

General flow



Logs

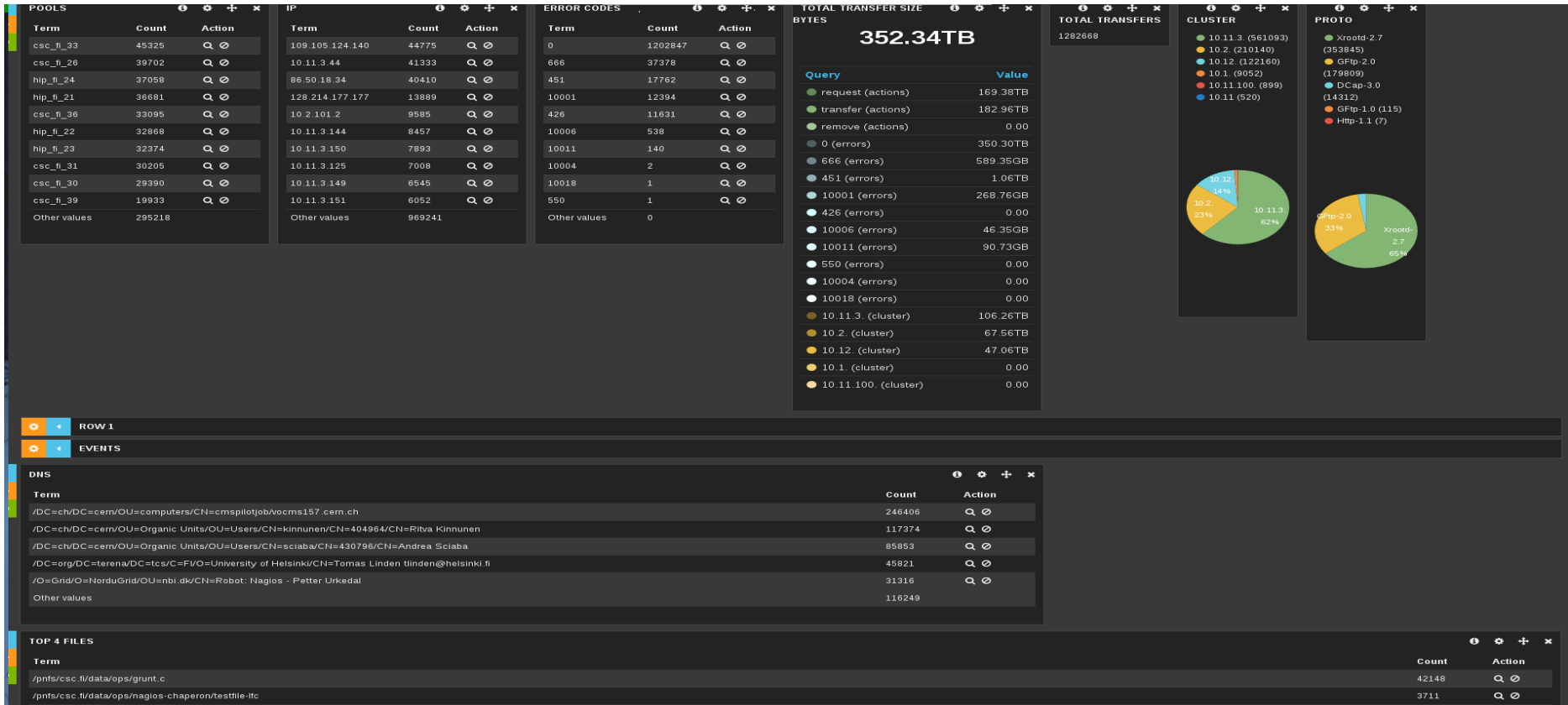
11.01 12:28:59 [pool:hip_fi_22:transfer] [00006D82705A658A4B959C82A4A2ED50C986,647254212] [/upload/464d06dd-98ed-4df5-bc13-51ee34cff076/244B6348-C476-E411-B3BC-001E67398CB9.root] myStore:STRING@osm 647254212 55339 true {GFtp-2.0 192.108.47.136 33631} [door:GFTP-madhatter-61533@ftp-madhatterDomain:1417429681425-1417429682628] {0:""}

11.17 08:46:13 [door:GFTP-pacific01-<unknown>-28729@gridftp-pacific01Domain:request] ["/DC=org/DC=terena/DC=tcs/C=FI/O=CSC/CN=Johan Guldmyr jguldmyr@csc.fi":190:190:10.11.3.1] [000030A4D6AACE2F44AB97F3BB5A05986558,0] [/pnfs/csc.fi/data/cms/test/GLITE] myStore:STRING@osm 60
0 {0:""}

02.11 00:25:27 [pool:csc_fi_30:transfer] [0000DEE949BFA3AB4AB6A7ECB863CFF4C129,2684354560] [/pnfs/csc.fi/data/cms/store/PhEDEx_LoadTest07/LoadTest07_Debug_HIP/LoadTest07_HIP_05] myStore:STRIN
G@osm 2684354560 469699 false {GFtp-2.0 128.142.18.164 20383} [door:GFTP-madhatter-142884@ftp-madhatterDomain:1423606656955-1423606657869] {0:""}
02.11 00:25:27 [door:GFTP-madhatter-142884@ftp-madhatterDomain:request] ["/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=mtaze/CN=752482/CN=Meric Taze":27098:194:128.142.132.64] [0000DEE949BFA3A
B4AB6A7ECB863CFF4C129,2684354560] [/pnfs/csc.fi/data/cms/store/PhEDEx_LoadTest07/LoadTest07_Debug_HIP/LoadTest07_HIP_05] myStore:STRING@osm 469820 0 {0:""}
02.11 00:25:29 [door:SRM-madhatter@srm-madhatterDomain:remove] ["/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=amaltaro/CN=718748/CN=Alan Malta Rodrigues":194:194:10.11.3.147] [00009718DCF32D38
4E929AF00F248AEC37F9,0] [/pnfs/csc.fi/data/cms/store/unmerged/logs/prod/2015/2/8/dmason_FSQ-RunIIFall14GS-Backfill-00001_00004_v1__150203_211737_7102/Production/0007/0/9915e7c0-af45-11e4-b599
-a0369f23d01e-204-0-logArchive.tar.gz] <Unknown> 0 0 {0:""}
02.11 00:25:29 [pool:csc_fi_35:transfer] [0000B99135AAECDA482CA5197D10DABD0385,186811] [/upload/9a57f25a-1b37-4ec2-80c7-ac69247374ad/28d9f920-b115-11e4-93aa-001e67abf094-41-0-logArchive.tar.g

Not readable

Into this


POOLS
Term Count Action
csc_fi_33 45325
csc_fi_26 39702
hip_fi_24 37058
hip_fi_21 36681
csc_fi_36 33095
hip_fi_22 32868
hip_fi_23 32374
csc_fi_31 30205
csc_fi_30 29390
csc_fi_39 19933
Other values 295218
IP
Term Count Action
109.105.124.140 44775
10.11.3.44 41333
86.50.18.34 40410
128.214.177.177 13889
10.2.101.2 9585
10.11.3.144 8457
10.11.3.150 7893
10.11.3.125 7008
10.11.3.149 6545
10.11.3.151 6052
Other values 969241
ERROR CODES
Term Count Action
0 1202847
666 37378
451 17762
10001 12394
426 11631
10006 538
10011 140
10004 2
10018 1
550 1
Other values 0
TOTAL TRANSFER SIZE BYTES
352.34TB
Query Value
request (actions) 169.38TB
transfer (actions) 182.96TB
remove (actions) 0.00
0 (errors) 350.30TB
666 (errors) 589.35GB
451 (errors) 1.06TB
10001 (errors) 268.76GB
426 (errors) 0.00
10006 (errors) 46.35GB
10011 (errors) 90.73GB
550 (errors) 0.00
10004 (errors) 0.00
10018 (errors) 0.00
10.11.3. (cluster) 106.26TB
10.2. (cluster) 67.56TB
10.12. (cluster) 47.06TB
10.1. (cluster) 0.00
10.11.100. (cluster) 0.00
TOTAL TRANSFERS
1282668
CLUSTER
10.11.3. (561093)
10.2. (210140)
10.12. (122160)
10.1. (9052)
10.11.100. (899)
10.11 (520)
10.12. 14%
10.2. 23%
10.11.3. 62%
PROTO
Xrootd-2.7 (353845)
GFtp-2.0 (179809)
DCap-3.0 (14312)
GFtp-1.0 (115)
Http-1.1 (7)
GFtp-2.0 33%
Xrootd-2.7 65%
ROW 1
EVENTS
DNS
Term Count Action
/DC=ch/DC=cern/OU=computers/CN=cmspilotjob/vocms157.cern.ch 246406
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=kinnunen/CN=404964/CN=Ritva Kinnunen 117374
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=sciaba/CN=430796/CN=Andrea Sciaba 85853
/DC=org/DC=terena/DC=tcs/C=FI/O=University of Helsinki/CN=Tomas Linden tlinden@helsinki.fi 45821
/O=Grid/O=NorduGrid/OU=nbi.dk/CN=Robot: Nagios - Petter Urkedal 31316
Other values 116249
TOP 4 FILES
Term Count Action
/pnfs/csc.fi/data/ops/grunt.c 42148
/pnfs/csc.fi/data/ops/nagios-chaperon/testfile-lfc 3711
/pnfs/csc.fi/data/cms/store/mc/SAM/GenericTTbar/GEN-SIM-RECO/CMSSW_5_3_1_START53_V5-v1/0013/CE4D66FB-5AAF-E111-96D6-003048D37524.root 3556

Or this

sum of transfers

185495

Sum of transfer_size_gigabytes

billing_top_dn

Top 5 dn.raw	Count of documents
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=amaltaro/CN=718748/CN=Alan Malta Rodrigues	123254
/DC=org/DC=terena/DC=tcs/C=FI/O=University of Helsinki/CN=Tomas Linden tlinden@helsinki.fi	42028
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=sciaba/CN=430796/CN=Andrea Sciaba	16051
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=jlee/CN=661342/CN=Jason Lee	13618
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=hyunyong/CN=693411/CN=Hyunyong Kim	11649

Top 15 Hosts sorted by transfer_size_gigabytes

Top 15 remote_host	Sum of transfer_size_gigabytes
130.246.183.202	5234
130.246.181.19	5106
130.246.183.213	4971
130.246.181.33	4868
130.246.183.210	4864
130.246.183.214	4800
130.246.181.22	4667
130.246.181.32	4566
194.190.165.2	2276
194.190.165.15	1945

Export

« 1 2 »

Get all the things for this demo

Two options:

1) Run on localhost

2) Run in a VM

TCP ports for localhost: 9200, 9292, 5601

Run on localhost 1

Get: Elasticsearch, Logstash and Kibana4 tar balls

- JAVA (8 or 7 openjdk works) is needed
- Tested on Ubuntu 15.04 (localhost)

TCP ports: 9200, 9292, 5601

- Some billing files
- Configs and patterns:
  - git clone https://github.com/CSC-IT-Center-for-Science/ELK-demo
  - git clone https://github.com/dCache/logstash4dcache.git
- There are better ways of installing the ELK stack for production (see notes)

Run on localhost 2

wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.5.2.tar.gz

wget https://download.elastic.co/logstash/logstash/logstash-1.4.2.tar.gz

wget https://download.elastic.co/kibana/kibana/kibana-4.0.2-linux-x64.tar.gz

Run in a VM

- JAVA (8 or 7 openjdk works) is needed
- Tested with CentOS6 (in an openstack)
- Some billing files

TCP ports: 9200, 9292, 5601

- Ansible: git clone https://github.com/CSC-IT-Center-for-Science/ELK-demo
- Configs: git clone https://github.com/dCache/logstash4dcache.git

Run in a VM 2 – configure with ansible

git clone https://github.com/CSC-IT-Center-for-Science/ELK-demo

Launch a VM

TCP ports: 9200, 9292, 5601

modify ansible-inventory file - it should have the DNS to the VM - not the IP

Follow instructions in
https://github.com/CSC-IT-Center-for-Science/ELK-demo/wiki/Install-the-ELK-demo-VM-with-ansible

ansible-playbook -i ansible-inventory setup.yml

Logstash stdin/stdout:

http://logstash.net/docs/latest

tar -xvf logstash-1.4.2.tar.gz

Input from stdin / output to stdout:
./logstash-1.4.2/bin/logstash agent -f ELK-demo/logstash/config/01-logstash.conf

CTRL+C and then ENTER to stop

Outputs in json format – copy paste some dCache billing into there:
./logstash-1.4.2/bin/logstash agent -f ELK-demo/logstash/config/02-logstash.conf

Elasticsearch:

```
tar -xvf elasticsearch-1.5.2.tar.gz

echo 'http.cors.allow-origin: "*"' >> elasticsearch-1.5.2/config/elasticsearch.yml
echo 'http.cors.enabled: true' >> elasticsearch-1.5.2/config/elasticsearch.yml

./elasticsearch-1.5.2/bin/elasticsearch
curl localhost:9200/_search
curl localhost:9200/_cluster/health
```

- For production: Filter it **heavily**, for example:
  - Limit PUT/POST/DELETE commands from trusted network, allow only from localhost
  - Only allow access to /*/(_search|_aliases) etc, which are used by scripts/kibanas.

Logstash – to elasticsearch:

Input from stdin – billing entry to elasticsearch:
./logstash-1.4.2/bin/logstash agent -f 03-logstash.conf

curl localhost:9200/_search?pretty

```
$ curl localhost:9200/
{
  "status" : 200,
  "name" : "Jennifer Kale",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.5.2",
    "build_hash" : "62ff9868b4c8a0c45860bebb259e21980778ab1c",
    "build_timestamp" : "2015-04-27T09:21:06Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
```

Kibana3:

./logstash-1.4.2/bin/logstash web

firefox http://localhost:9292

Notice:

- The whole event is in “message” field
- The timestamp in @timestamp field is not the same as the timestamp in the message field
- For production put kibana3 behind an httpd(DocumentRoot in apache's), no need to proxy

Kibana4:

tar -xvf kibana-4.0.2-linux-x64.tar.gz

./kibana-4.0.2-linux-x64/bin/kibana

firefox http://localhost:5601

For production:

Put kibana4 behind an http proxy. Not in a package yet, see

https://github.com/elastic/kibana/issues/1811

Grok patterns

https://grokdebug.herokuapp.com/

04-logstash.conf

```
...
filter {
 grok {
        # 04.28 00:00:46 [pool:csc_fi_31:transfer] ...
        patterns_dir => "./logstash4dcache/patterns"
        match => [ "message", "%{BILLING_TIME:local_time} %{GREEDYDATA:message}" ]
        overwrite => [ "message" ]
  }
}
...
```

logstash4dcache:

You don't have to write all the logstash/grok patterns!

Contribute :)

Many are already done in https://github.com/dCache/logstash4dcache

Some standard ones are already in logstash:

https://grokdebug.herokuapp.com/patterns#

or /opt/logstash/patterns/

Logstash date matching:

Date matching – important for backfilling

./logstash-1.4.2/bin/logstash agent -f 05-logstash.conf

Logstash backfilling:

$EDITOR 06-logstash-bf.conf and update:

- Path to match your billing files
- Gsub filter if using dCache <= 2.9

./logstash-1.4.2/bin/logstash agent -w 8 -f 06-logstash-bf.conf

Kibana3:

firefox http://localhost:9292

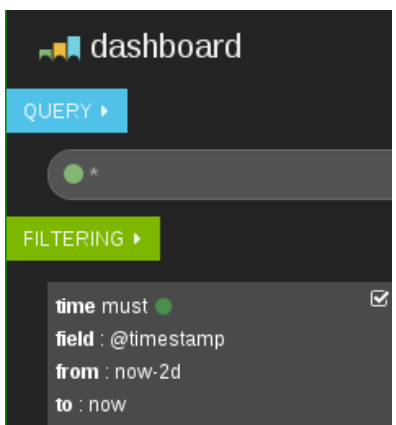
- Anything with _grokparsefailure or _parse_dcache_failure10 tags?
  - Room for improvement :)
- message field is gone
- Let's make some dashboards!

Kibana3:

Lucene search syntax examples:

- pool_name:pool_name_*
- pool_name:[pool_name_01 TO pool_name_35]

Change to **topN Queries** by clicking on the green circle in the query box.

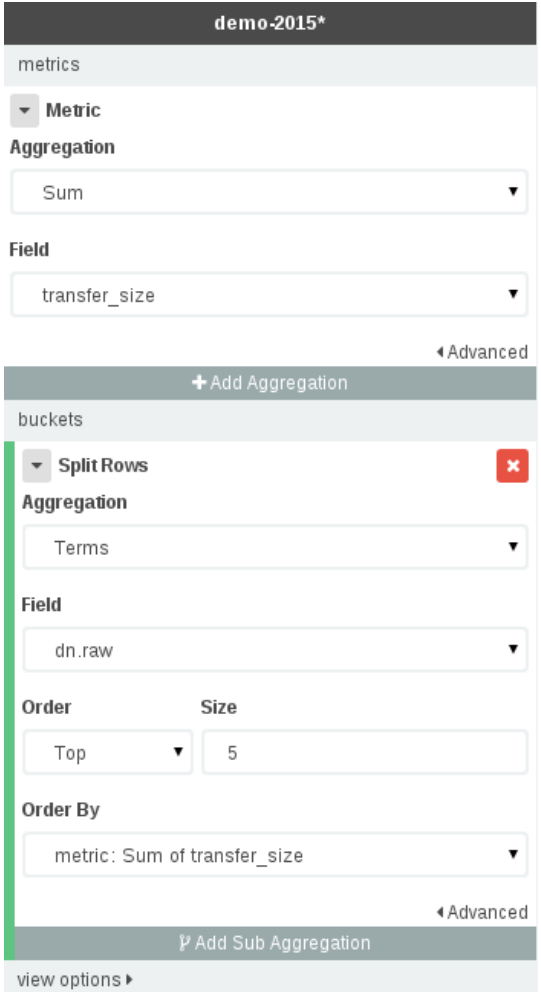


Kibana4:

firefox http://localhost:5601

- More advanced visualizations
- All the development is happening here

Kibana4:


demo-2015*
metrics
Metric
Aggregation
Sum
Field
transfer_size
Advanced
Add Aggregation
buckets
Split Rows
Aggregation
Terms
Field
dn.raw
Order
Size
Top
5
Order By
metric: Sum of transfer_size
Advanced
Add Sub Aggregation
view options

Kibana4:

Top 5 dn.raw	Sum of transfer_size
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=fanzago/CN=610896/CN=Federica Fanzago	93695479402871
/C=IT/O=INFN/OU=Personal Certificate/L=Pisa/CN=Silvio Donato	10526854158452
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=sciaba/CN=430796/CN=Andrea Sciaba	4016821102391
/DC=org/DC=terena/DC=tcs/C=FI/O=University of Helsinki/CN=Tomas Linden tlinden@helsinki.fi	3701436216864
/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=acelik/CN=747146/CN=Ali Celik	2502041315910

dCache workshop Demo:

Might be available during the workshop:

Kibana3: http://vm0444.kaj.pouta.csc.fi:443/ or http://elkdemo.csc.fi:443

Kibana4: http://vm0444.kaj.pouta.csc.fi:80 or http://elkdemo.csc.fi

Ansible & logstash for setting up the demo:

https://github.com/CSC-IT-Center-for-Science/ELK-demo

Extra – if time

- dCache
  - access
  - cell logs
  - postgresql to elasticsearch? Maybe https://github.com/logstash-plugins/logstash-input-jdbc
- ELK scaling
- Elasticsearch tips

dCache cell logs

- logback.xml: https://gist.github.com/martbhell/09bacc51d4df9e83f3a6
- There are ready made patterns for JAVA exceptions

1) Setup rsyslog to receive syslogs and write to a file
2) Configure logback to write to a remote syslog
3) Configure logstash to read rsyslogs files
   - Patterns: https://github.com/dCache/logstash4dcache/blob/master/patterns/dcache-logs

dCache access logs

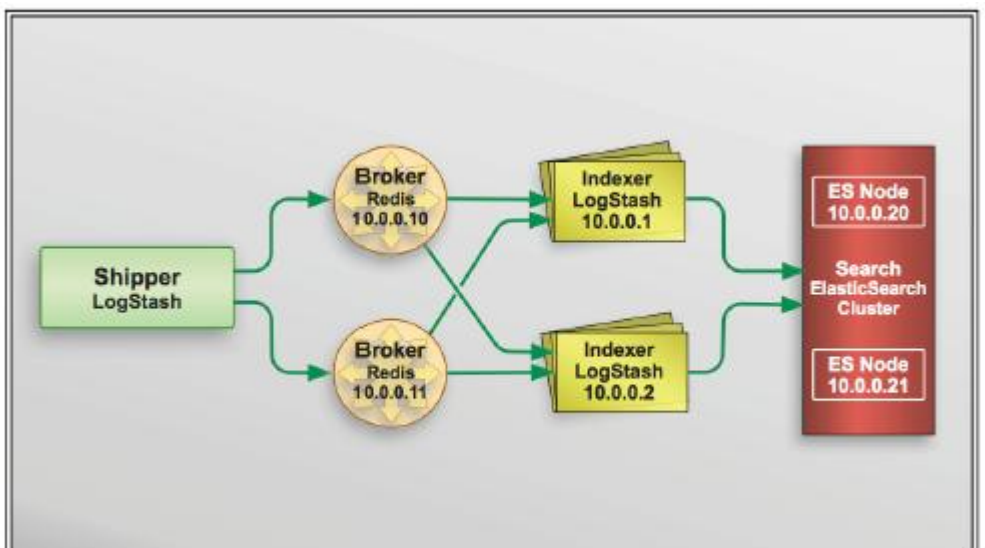
- Same as cell logs could be done – needs more modifications to logback.xml
- Look deeper into what the clients are doing
- Another way (also works for other applications)

1) Have rsyslog read the non-syslog managed files and write over syslog

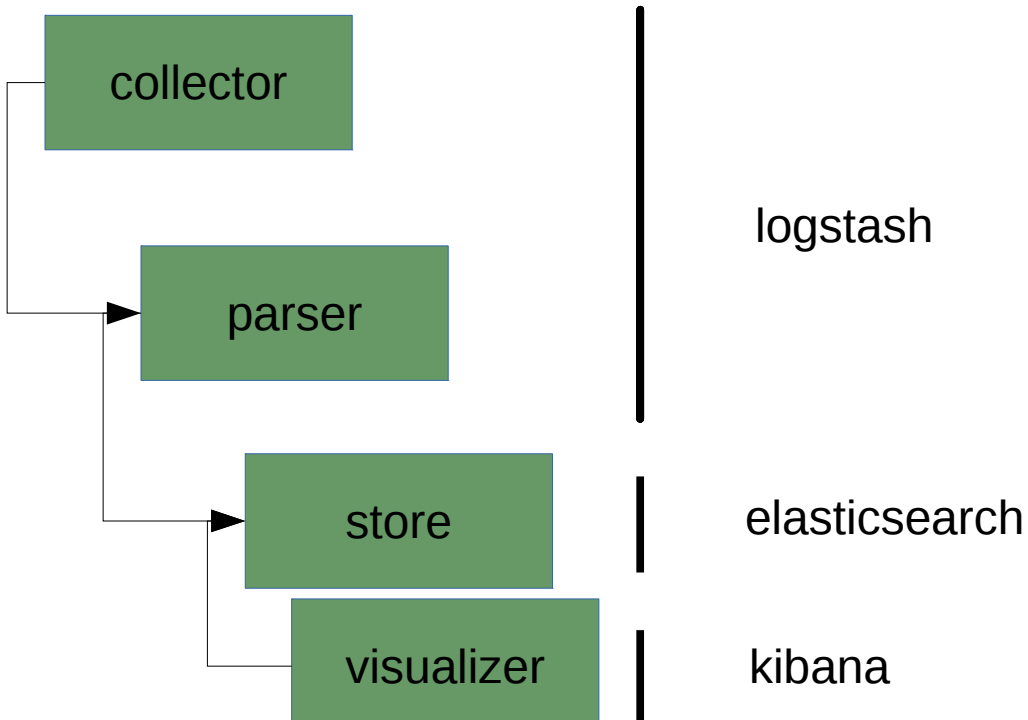
2) Install logstash/logstash forwarder on the doors

ELK scaling

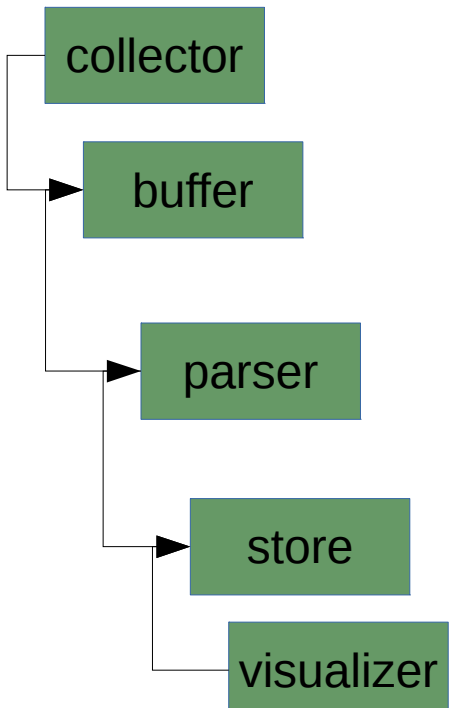
- Common way of scaling this is to add more layers and use some sort of message queue (redis/rabbitmq).



General flow



General flow – more layers



Logstash / lsf (logstash forwarder) / beaver / syslog

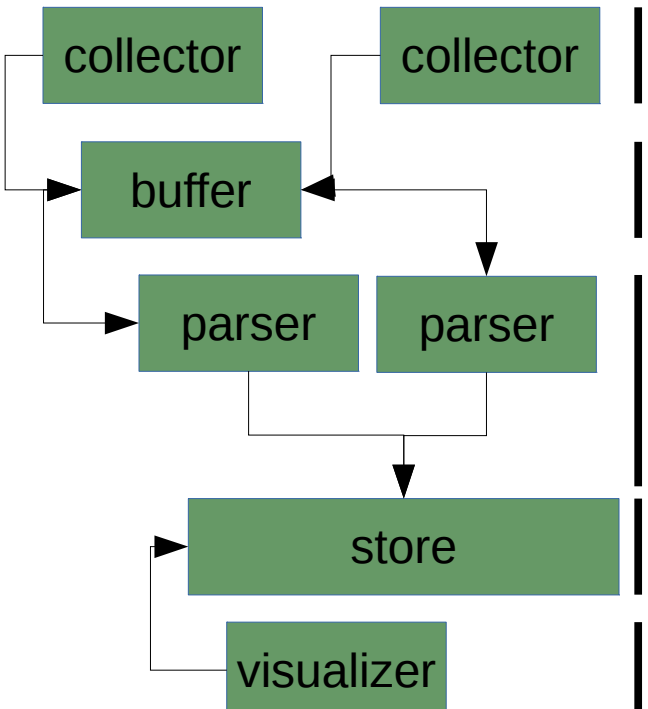
Redis, mq

Logstash

Elasticsearch

Kibana

General flow – more layers



Logstash / lsf (logstash forwarder) / beaver / syslog

Redis, mq

Logstash

Elasticsearch

Kibana

Elasticsearch plugins

Good for managing the indices and some health status

./elasticsearch-1.5.2/bin/plugin -install mobz/elasticsearch-head

./elasticsearch-1.5.2/bin/plugin -install royrusso/elasticsearch-HQ

http://localhost:9200/_plugin/head

Elasticsearch tips

- Default is 10 shards per day (5 per index and default is 1 replica so 10)
  - Overkill for only billing logs of a small T2 as T2_FI_HIP (~100k transfers/day)
  - You can't change sharding on an index after it's created
    - finite amount of shards per ES node
  - Index creation monthly (YYYY-MM instead of YYYY-MM-DD)
  - Unique _id field based on hash of billing entry
    - good if you are sure that the entry in the billing files is unique
- Max 31GB allocated to each elasticsearch node – and the same amount should be available as free RAM on the box. So max 64GB / node.
- Use elasticsearch-curator to alias/close/optimize/delete indices

elasticsearch tips 2

- Security updates – many escapes out of sandboxes
- Never put direct access to elasticsearch on the Internets

Resources

- http://logstash.net/docs/latest
- http://grokdebug.herokuapp.com
- Good introduction to ELK - http://tech.paulcz.net/ACUG-Logstash
- Kibana4 video tutorials are quite good on https://elastic.co
- Tigran's CHEP 2015 talk: http://indico.cern.ch/event/304944/session/4/contribution/45/material/slides/0.pdf
- https://github.com/CSC-IT-Center-for-Science/ELK-demo

Questions?

CSC-IT CENTER FOR SCIENCE