

Just 'Google' for flaws

Will operational analytics cause a paradigm shift?



October 6th 2015
Dutch testing days

Albert Witteveen

5 years BG?

Google



A paradigm shift

- Information before:
 - Limited
 - Office hours
 - Outdated
- Information after:
 - The whole world
 - Fresh
 - Search engines index continuously



Data tells a story

```

<Order>
<Timestamp>2015-30-9 10:43:58.001</Timestamp>
<CustID>B366547</CustID>
<BusID>C012548689</BusID>
<Product>Banana</Product>
<Amount>5</Amount>
<Discount>0</Discount>
<Price>2.50</Price>
<SalesPerson>John Slick</SalesPerson>
<Unit>Piece</Unit>
<Option></Option>
</Order>
    
```

```

<Message>
<Response>ERROR</Response>
<Messageid>5fd13a50836b024390cba3a7f9c916d7</Messageid>
<Replay>Unit Piece not available for Banana</Replay>
<Timestamp>2015-30-9 10:44:20.001</Timestamp>
<CustID>B366547</CustID>
<BusID>C012548689</BusID>
    
```

CO12548689	2015-30-9 10:43:58.001	Order placed	5 Bananas
CO12548689	2015-30-9 10:44:20.001	Reply from logistics	Bananas not by piece
CO12548689	2015-30-9 10:45:02	Order registered in Order DB	Status failed



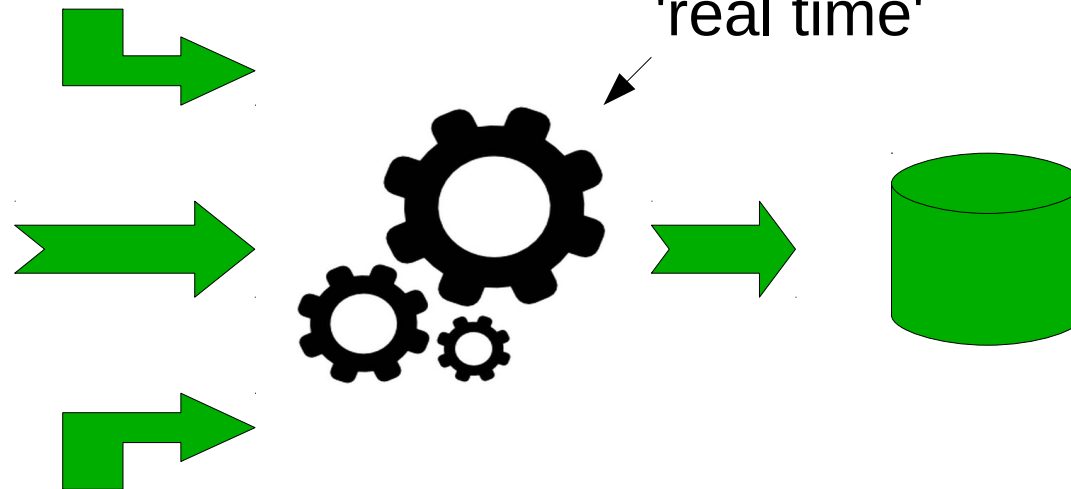
DateTime	Status	CustID	CorID	Product	#	Unit	Discount	Option
09/30/2015 10:45:00	succes	B254788	CorID12548687	Apple	1	Kg	10	sliced
09/30/2015 10:45:01	pending	B356489	CorID12548688	Carrot	5	Piece	0	na
09/30/2015 10:45:02	failed	B366547	CorID12548689	Banana	5	Piece	0	na
09/30/2015 10:45:10	succes	B112554	CorID12548690	Apple	2	Kg	5	na
09/30/2015 10:45:12	succes	R45456	CorID12548691	Orange	1	Kg	5	none

Operational intelligence system

```
64.242.88.10 -- [07/Mar/2015:16:05:49 -0800] "GET /twiki/bin/edit/Main/Double_bounce_sender?topicparent=Main.ConfigurationVariables HTTP/1.1" 401 12846
64.242.88.10 -- [07/Mar/2015:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
64.242.88.10 -- [07/Mar/2015:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
64.242.88.10 -- [07/Mar/2015:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
64.242.88.10 -- [07/Mar/2015:16:20:55 -0800] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253
64.242.88.10 -- [07/Mar/2015:16:23:12 -0800] "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382
64.242.88.10 -- [07/Mar/2015:16:24:16 -0800] "GET /twiki/bin/view/Main/PeterThoeny HTTP/1.1" 200 4924
64.242.88.10 -- [07/Mar/2015:16:29:16 -0800] "GET /twiki/bin/edit/Main/Header_checks?topicparent=Main.ConfigurationVariables HTTP/1.1" 401
```

Index and time stamp in 'real time'

Order_ID	Status	CorrelationID
O1254486	completed	C24ec540d000ee0b7d2304bc34c769a4
O1254487	in progress	a2a551a6458a8de22446cc76d639a9e9
O1254488	in progress	be121740bf988b2225a313fal107ca1
O1254489	error	b0293108cc2a2aa7c88738c2215b1a05
O1254490	completed	68c4283db8074b12df1660b31c0220a9
O1254491	completed	9a1f30943126974075dbd4d13c8018ac



```
<?xml version="1.0" standalone="yes" ?>
- <shop location="Birmingham" size="Large">
- <food>
  <Name>Apple</Name>
  <type>fruit</type>
  <cost>15</cost>
</food>
- <food>
  <Name>Carrot</Name>
  <type>vegetable</type>
  <cost>10</cost>
</food>
</shop>
```

```
01 server CRON[14748]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
01 server CRON[15493]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
04 server dbus[426]: [system] Activating service name='org.freedesktop.ConsoleKit' (using servicehelper)
05 server dbus[426]: [system] Activating service name='org.freedesktop.PolicyKit1' (using servicehelper)
05 server polkitd[15604]: started daemon version 0.105 using authority implementation 'local' version '0.105'
05 server dbus[426]: [system] Successfully activated service 'org.freedesktop.PolicyKit1'
05 server dbus[426]: [system] Successfully activated service 'org.freedesktop.ConsoleKit'
:/var/log$
```

Search

Search | Actions ▾

404 AND NOT favicon.ico Last 24 hours ▶

✔ 8,639 matching events Save search Build report

Timeline: zoom in zoom out Scale: linear log 1 bar = 1 hour

78 fields | Pick fields

Selected fields (4)

- host (1)
- method (1)
- source (4)
- sourcetype (5)

Other interesting fields (6)

- index (1)
- linecount (n) (1)
- punct (x100)
- splunk_server (1)
- timeendpos (n) (14)
- timestartpos (n) (14)

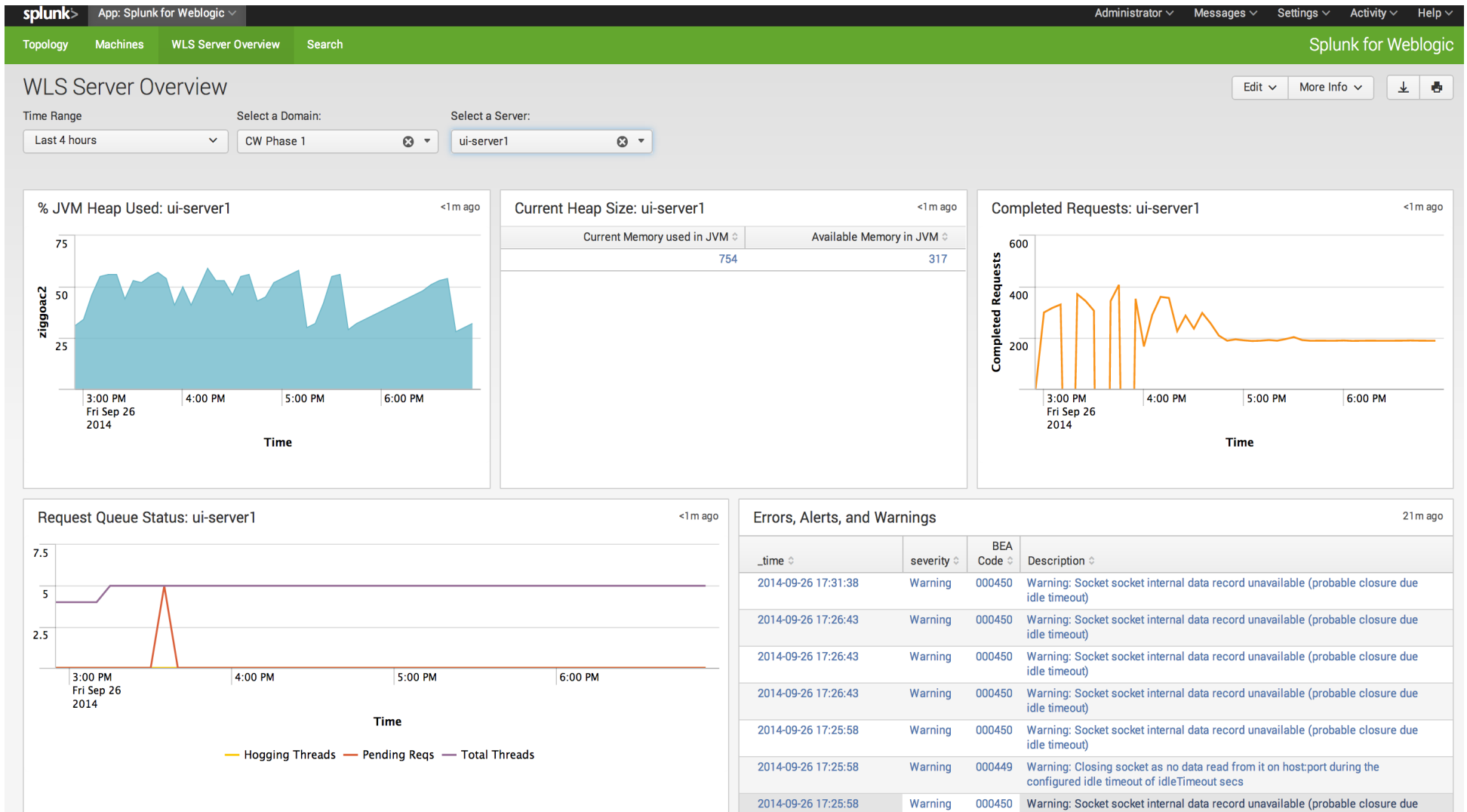
All 78 Fields

8,639 events in the last 24 hours (from 4:00:00 PM June 12 to 4:35:16 PM June 13, 2010)

Results per page 10

1	6/13/10 4:34:57.000 PM	99.91.15.28 - - [13/Jun/2010:16:34:57 -0500] "GET /global/js/jquery.simplemodal-1.2.2.min.js HTTP/1.1" 404 13477 "http://www.pittstate.edu/" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6.4; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; Zune 4.0)" host=www.pittstate.edu sourcetype=access_combined source=Asr/local/dotcms/ogs/dotcms_access.2010-06-13.log method=GET
2	6/13/10 4:34:56.000 PM	216.129.119.46 - - [13/Jun/2010:16:34:56 -0500] "GET /robots.txt HTTP/1.1" 404 - "null" "Mozilla/5.0 (Twiceler-0.9 http://www.cuil.com/twiceler/robot.html)" host=www.pittstate.edu sourcetype=access_combined source=Asr/local/dotcms/ogs/dotcms_access.2010-06-13.log method=GET
3	6/13/10 4:34:55.000 PM	10.21.10.232 - - [13/Jun/2010:16:34:55 -0500] "GET /global/js/jquery.simplemodal-1.2.2.min.js HTTP/1.1" 404 13477 "http://www.pittstate.edu/" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" host=www.pittstate.edu sourcetype=access_combined source=Asr/local/dotcms/ogs/dotcms_access.2010-06-13.log method=GET
4	6/13/10 4:34:50.000 PM	24.119.142.69 - - [13/Jun/2010:16:34:50 -0500] "GET /global/js/jquery.simplemodal-1.2.2.min.js HTTP/1.1" 404 10230 "http://www.pittstate.edu/" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.0.30618; .NET CLR 3.5.30729)" host=www.pittstate.edu sourcetype=access_combined source=Asr/local/dotcms/ogs/dotcms_access.2010-06-13.log method=GET

Correlate



Apps

splunk App: Tibco awitteveen Messages Settings Activity Help

Search Pivot reports Alerts dashboards Tibco

T1 - Tibco Detail page

Transaction ID Job ID Severity Time Stamp

RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a 1367859 All 2014-09-11T10:50:46.163+02:00

Master

_time	businessTransactionID	job_id	message_type	filename	operation	severity	classification	message
2014-09-11 10:49:53	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	97122	DEBUG	adpRtcis-adpRtcis.log	RtcGetRoutingConfiguration_1	DEBUG		Request to SmpGetRoutingConfiguration_1
2014-09-11 10:49:53	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	97122	INFO	adpRtcis-adpRtcis.log	RtcGetRoutingConfiguration_1	INFO		REQUEST message received
2014-09-11 10:49:53	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	1367859	INFO	adpSmp-adpSmp.log	SmpGetRoutingConfiguration_1	INFO		REQUEST message received
2014-09-11 10:49:53	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	1367859	DEBUG	adpSmp-adpSmp.log	SmpGetRoutingConfiguration_1	DEBUG		Log request message to Sigma SMP
2014-09-11 10:50:16	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	1367859	DEBUG	adpSmp-adpSmp.log	SmpGetRoutingConfiguration_1	DEBUG		ConsersationID to get message form SMP Topic
2014-09-11 10:50:16	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	1367859	DEBUG	adpSmp-adpSmp.log	SmpGetRoutingConfiguration_1	DEBUG		Log Response from Sigma SMP
2014-09-11 10:50:33	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	97122	ERROR	adpRtcis-adpRtcis.log	RtcGetRoutingConfiguration_1	ERROR	TECHNICAL	Timed out waiting for a response
2014-09-11 10:50:46	RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a	1367859	ERROR	adpSmp-adpSmp.log	SmpGetRoutingConfiguration_1	ERROR	TECHNICAL	Timed out waiting for a response

Transaction ID: RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a Job-ID: 1367859 Time: 2014-09-11T10:50:46.163+02:00

i	Time	Event
>	9/11/14 10:50:46.163 AM	<LoggingEvent <severity>ERROR</severity> <message>Error RESPONSE sent</message> <sourceContext> <host>ESB-BM-WAV01</host> <application>adpSmp</application> <operation>SmpGetRoutingConfiguration_1</operation> </sourceContext> <keyFields> <attribute> <key-cmm:businessTransactionID</key> <value>RTCIS_diagnose_d864fad5-c6f9-4e38-80a0-d9e05353697a</value> </attribute> <attribute> <key-cmm:externalCorrelationID</key> <value>e1dbb908-5861-4dba-9b9e-91eff34776bb</value> </attribute> <attribute> <key-cmm:messageID</key> <value>5f1c8d40-85eb-4ff7-9e0d-32c24f341dcc</value> </attribute> <attribute> <key-cmm:correlationID</key> <value>28c4f23e-f405-44bc-b7a5-9e79da503fc4</value> </attribute> </keyFields> </LoggingEvent>

Dashboards

graylog Search Streams Dashboards Sources System In 7,367 / Out 7,369 msg/s Albert Witteveen

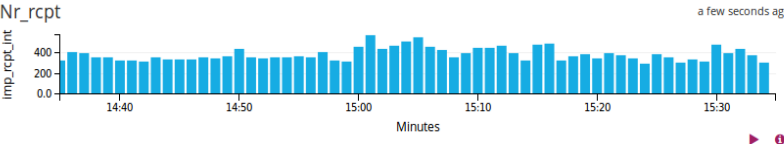
MX platform

Update in background Fullscreen Unlock / Edit

Drag widgets to any position you like in [unlock / edit mode](#).

Nr_rcpt


imp_rcpt_int a few seconds ago



Minutes

MX Actions Yesterday


a few seconds ago



Value	%	Count
DELIVERY	88.18%	20,372,460
Spam	11.40%	2,634,573
LOG	0.28%	63,634
FAILURE	0.08%	18,742

Imp_rcpt_int Mean Value Graph Day

imp_rcpt_int a few seconds ago



Days

Failure MX Incomming

a few seconds ago

0

Message Count

a few seconds ago

285,502

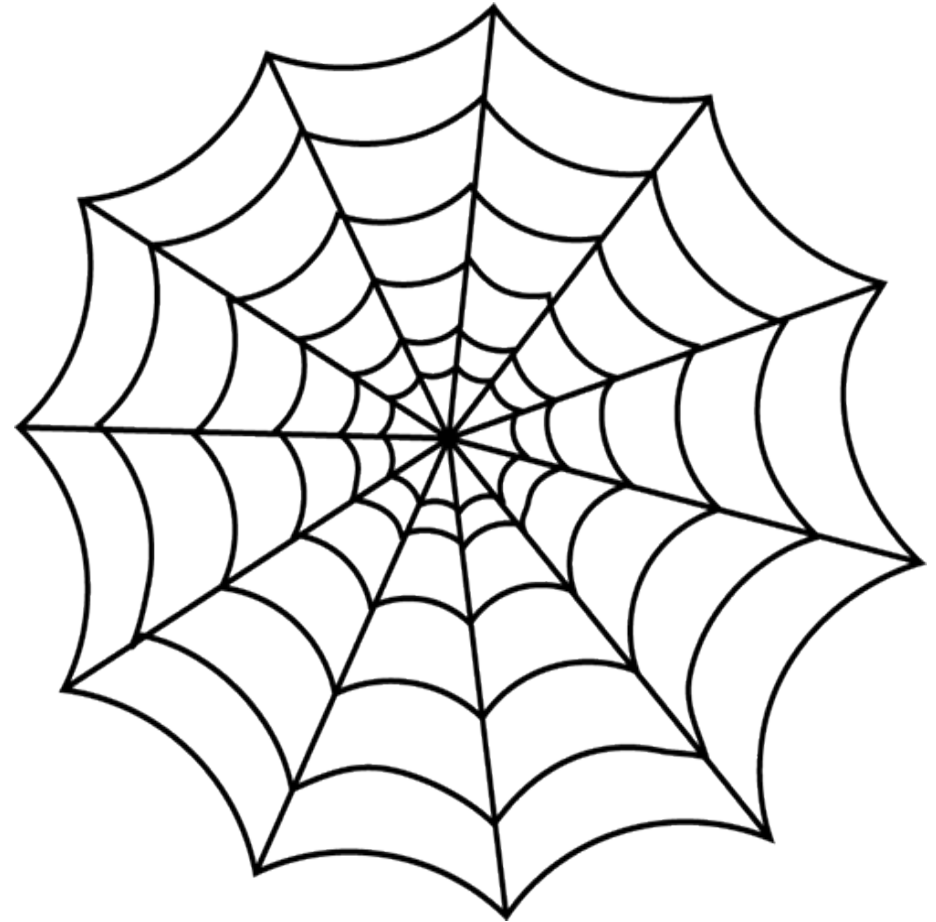
graylog-web-interface v1.1.5 (2a39def) (Oracle Corporation 1.7.0_79 / Linux 3.13.0-61-generic) on kibana1

Find: spam Previous Next Highlight all Match case Done

The challenge

You can't check each log for each test!

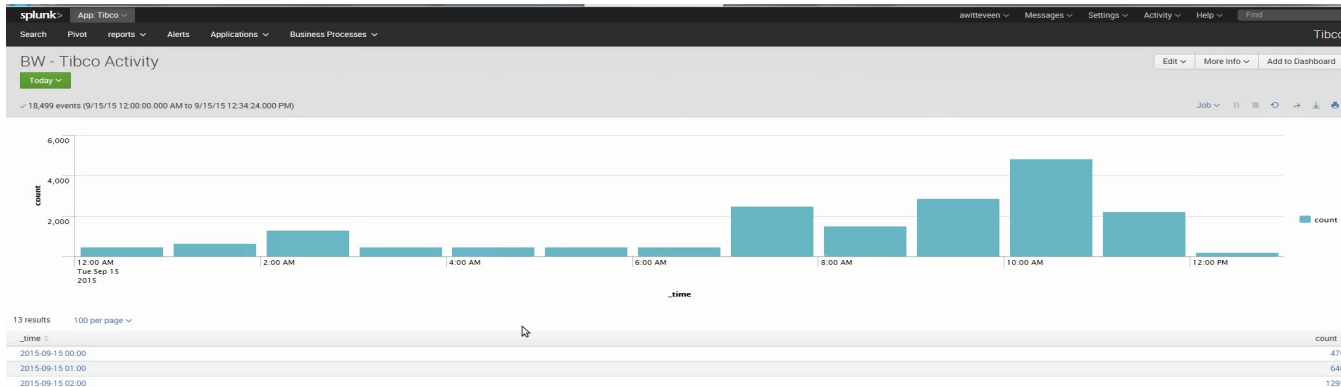
- SOA: from chain to web
- Multiple teams change
- Change based specs
- Logs hidden
- Integration drama
- Too much...



Expected result???

Operational intelligence

- Finds issues before complaints come in
- Is a great for root cause analysis
- Provides facts and figures on the quality of the system

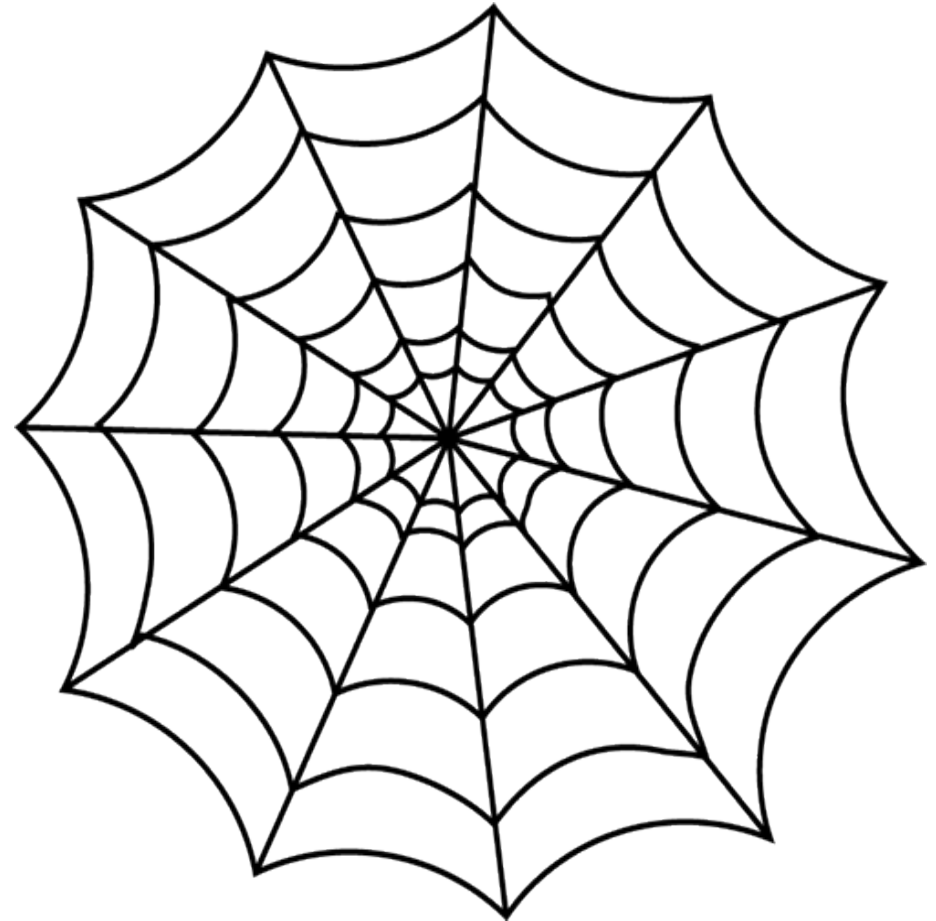


Wait, isn't that our job?

The challenge

You can't check each log for each test!

- SOA: from chain to web
- Multiple teams change
- Change based specs
- Logs hidden
- Integration drama
- Too much...



Expected result???

Unexpected result

- Frontends provide limited feedback
- Feedback is in the logs, in the tables, in the messages
- Can we still predict the result?

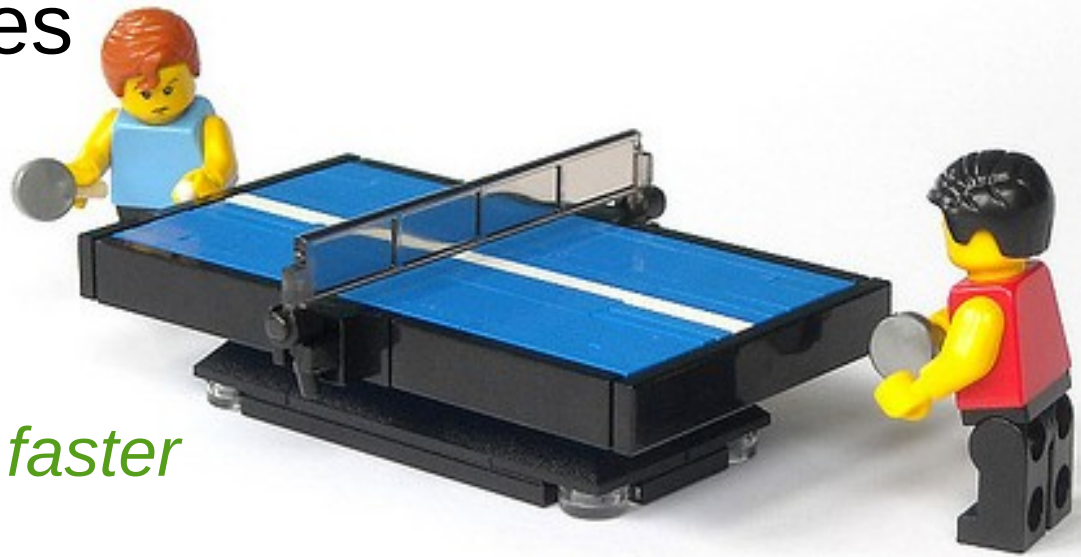
Are we sure we checked every log?



Doable to do this manually?

With Operation intelligence

- All the logging information in one overview
- Errors in unexpected systems
- Trends and history
- Avoid ping pong issues

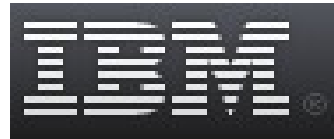


Solve integration issues much faster

Find issues that would be overlooked

Solutions

Commercial



Predictive Maintenance

Open Source



An Open-Source
Community Site

E



elastic

L



logstash

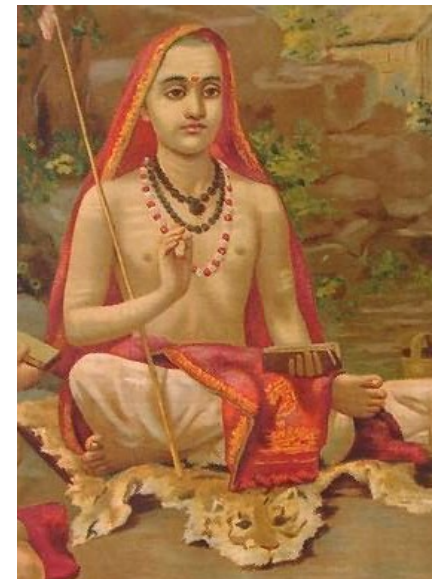
K

Kibana | Explore & Visualize Your Data

Experience

- Large multimillion € programme:
 - Integration issues solved
 - Testers: 'I see what is happening'
 - Significant decrease in 'test issues'
 - End of ping pong issues
 - Fast issue resolving
 - Insight for management
 - Guru essential

Stop bickering

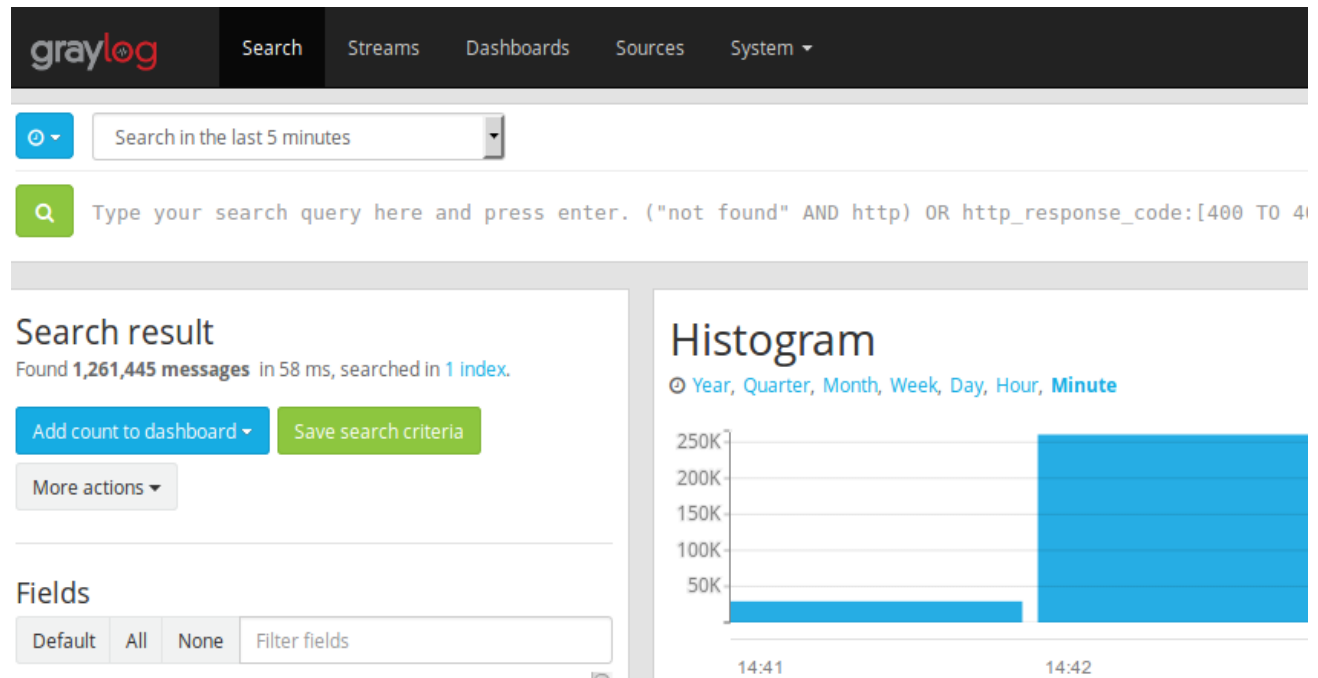


Issue manager: don't log before Splunking...

Paradigm shift?

Just 'Google' in stead of test?

$2+2=5$?



So

- Do(n't) go out and try for yourself
- It can help change our work
- We still need to test



Find any question?

```
[ 0.000000] efi: mem60: type=6, attr=0x800000000000000f, range=[0x00000000da0a9000-0x00000000da109000) (0MB)
[ 0.000000] efi: mem61: type=5, attr=0x800000000000000f, range=[0x00000000da109000-0x00000000da123000) (0MB)
[ 0.000000] efi: mem62: type=6, attr=0x800000000000000f, range=[0x00000000da123000-0x00000000da126000) (0MB)
[ 0.000000] efi: mem63: type=6, attr=0x800000000000000f, range=[0x00000000da126000-0x00000000da14d000) (0MB)
[ 0.000000] efi: mem64: type=0, attr=0xf, range=[0x00000000da14d000-0x00000000da2a0000) (1MB)
[ 0.000000] efi: mem65: type=0, attr=0xf, range=[0x00000000da2a0000-0x00000000da64d000) (3MB)
[ 0.000000] efi: mem66: type=10, attr=0xf, range=[0x00000000da64d000-0x00000000da71a000) (0MB)
[ 0.000000] efi: mem67: type=10, attr=0xf, range=[0x00000000da71a000-0x00000000da8b7000) (1MB)
[Question: should I be introducing operational intelligence?]
[ 0.000000] efi: mem68: type=10, attr=0xf, range=[0x00000000da8b7000-0x00000000da8b8000) (0MB)
[ 0.000000] efi: mem69: type=10, attr=0xf, range=[0x00000000da8b8000-0x00000000da8cd000) (0MB)
[ 0.000000] efi: mem70: type=9, attr=0xf, range=[0x00000000da8cd000-0x00000000da8d2000) (0MB)
[ 0.000000] efi: mem71: type=4, attr=0xf, range=[0x00000000da8d2000-0x00000000da8d3000) (0MB)
[ 0.000000] efi: mem72: type=10, attr=0xf, range=[0x00000000da8d3000-0x00000000da916000) (0MB)
[ 0.000000] efi: mem73: type=4, attr=0xf, range=[0x00000000da916000-0x00000000daa62000) (1MB)
[ 0.000000] efi: mem74: type=3, attr=0xf, range=[0x00000000daa62000-0x00000000dacfa000) (2MB)
[ 0.000000] efi: mem75: type=4, attr=0xf, range=[0x00000000dacfa000-0x00000000dacff000) (0MB)
[ 0.000000] efi: mem76: type=3, attr=0xf, range=[0x00000000dacff000-0x00000000dad03000) (0MB)
[ 0.000000] efi: mem77: type=4, attr=0xf, range=[0x00000000dad03000-0x00000000dad10000) (0MB)
[ 0.000000] efi: mem78: type=3, attr=0xf, range=[0x00000000dad10000-0x00000000dad22000) (0MB)
[ 0.000000] efi: mem79: type=4, attr=0xf, range=[0x00000000dad22000-0x00000000dad29000) (0MB)
[ 0.000000] efi: mem80: type=6, attr=0x800000000000000f, range=[0x00000000dad29000-0x00000000daff4000) (2MB)
[ 0.000000] efi: mem81: type=4, attr=0xf, range=[0x00000000daff4000-0x00000000db000000) (0MB)
[ 0.000000] efi: mem82: type=7, attr=0xf, range=[0x00000000100000000-0x0000000011f200000) (498MB)
[ 0.000000] efi: mem83: type=0, attr=0x8000000000000000, range=[0x00000000dbc00000-0x00000000dfe00000) (66MB)
[ 0.000000] efi: mem84: type=11, attr=0x8000000000000001, range=[0x00000000f8000000-0x00000000fc000000) (64MB)
[ 0.000000] efi: mem85: type=11, attr=0x8000000000000001, range=[0x00000000fec00000-0x00000000fec01000) (0MB)
[ 0.000000] efi: mem86: type=11, attr=0x8000000000000001, range=[0x00000000fed00000-0x00000000fed04000) (0MB)
[ 0.000000] efi: mem87: type=11, attr=0x8000000000000001, range=[0x00000000fed1c000-0x00000000fed20000) (0MB)
[ 0.000000] efi: mem88: type=11, attr=0x8000000000000001, range=[0x00000000fee00000-0x00000000fee01000) (0MB)
[ 0.000000] efi: mem89: type=11, attr=0x8000000000000001, range=[0x00000000fff00000-0x0000000100000000) (16MB)
```