© 2017 SPLUNK INC.

splunk> .conf2017

Tracking Logs at Zillow with Lookups & JIRA

Seth Thomas, Jon Wentworth

September 27 | Washington, DC

© 2017 SPLUNK INC.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

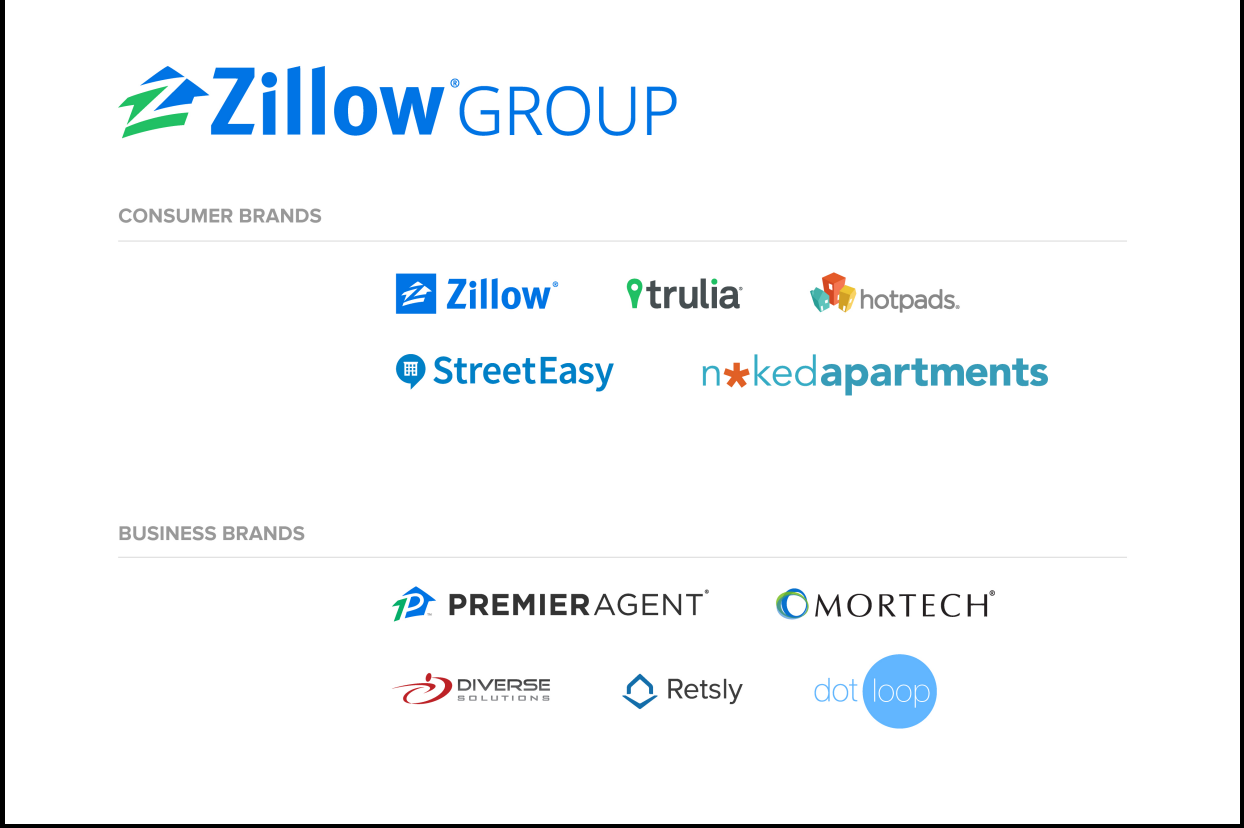
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

© 2017 SPLUNK INC.

What is Zillow?

About Zillow

- Zillow Group operates the largest real estate network on the web.
- Zillow Group Rentals is the largest rental network on the web, composed of the millions of rental shoppers on Zillow, Trulia, HotPads and MyNewPlace.
- 4 out of 5 U.S. homes have been viewed on Zillow.
- Zillow Group captured nearly two-thirds of the total market share for the online real estate category.
- Zillow has data on more than 110 million U.S. homes, with Zestimates and Rent Zestimates on more than 100 million U.S. homes.
- More than 70 million homes on Zillow have been updated by our community of users.
- 166 million average monthly unique users visited Zillow Group brands' mobile apps and websites
- mobile apps and websites reached an all-time high of nearly 180 million unique users
- More than 36 million rental visitors come to Zillow Group's rental sites and apps each month



© 2017 SPLUNK INC.

Zillow Group Splunk

How does Zillow use Splunk?

- Operations Center & Systems Engineering
- Customer Service
- Product & Engineering Teams
- Performance Team
- SEO Team
- Native Mobile Apps (iOS, Android) with MiNT

© 2017 SPLUNK INC.

Our Problem

Our services can produce a lot of errors, which do we care about, how do we track them, what are the metrics, how well is the process working?

splunk> .conf2017

© 2017 SPLUNK INC.

Evolution of Error Event Tracking

Top 10 – quantifies noise

Leaderboard – shows movement between 2 periods

Assigning Identity – is there a JIRA ticket

- Creates an Error Dictionary
- Assigns accountability
- Provides context upon regression
- Maps to all environments (prod & pre-prod)
- Allows for quality gates between code promotions

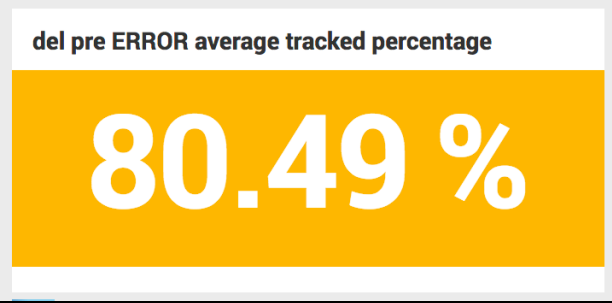
splunk> .conf2017

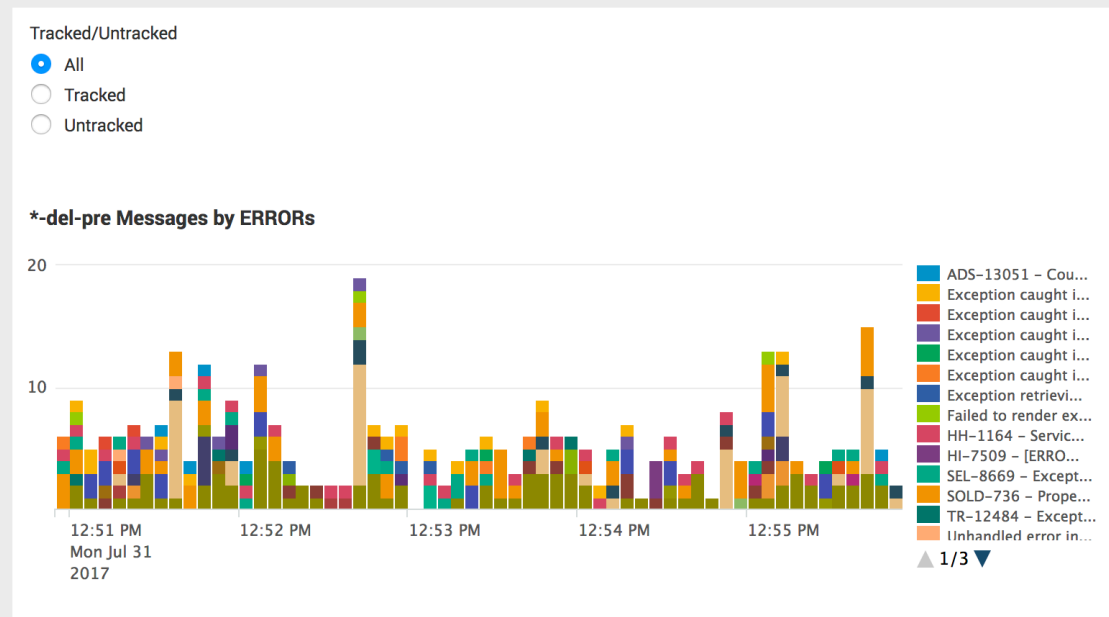
© 2017 SPLUNK INC.

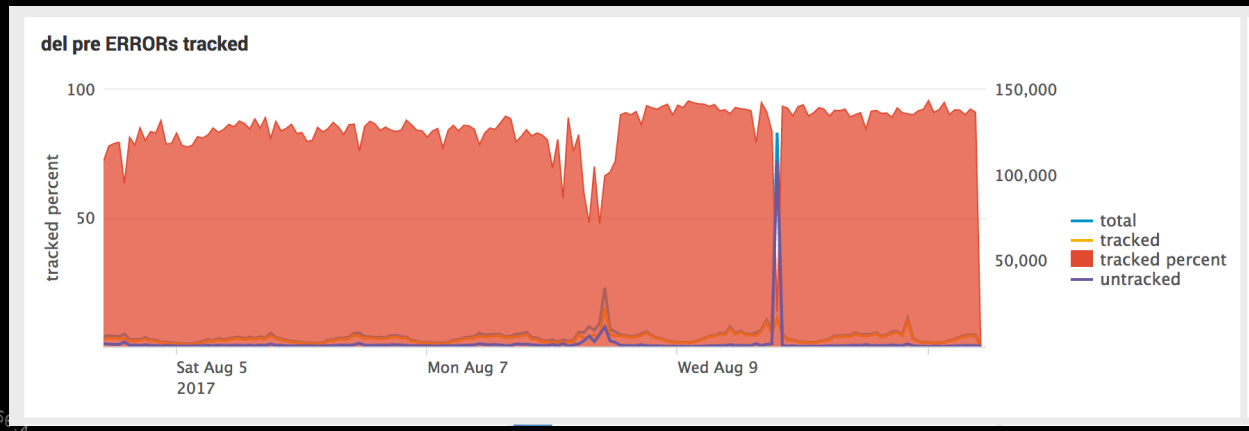
Tracking Progress with Metrics

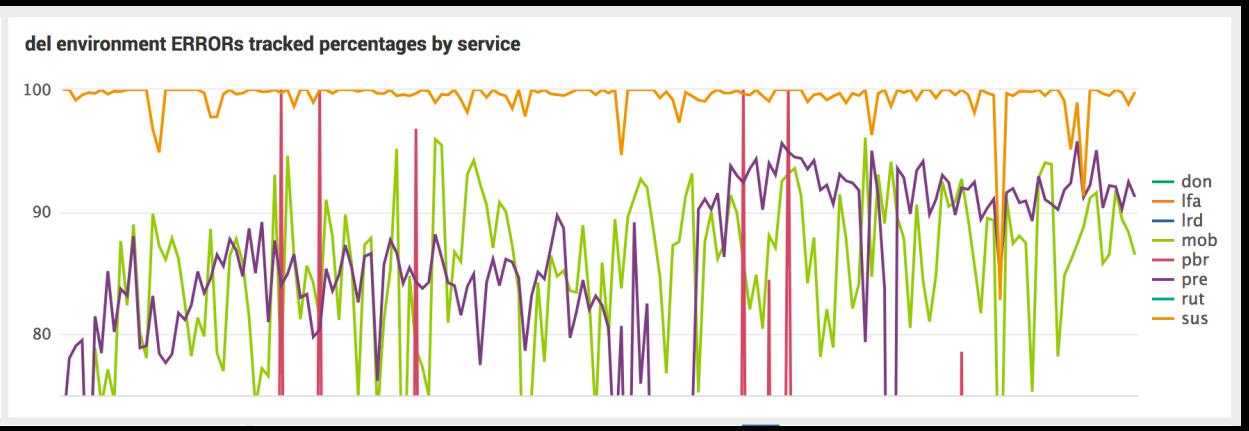
ERROR % bug Tracking

Defined Goal 80%









splunk> .conf2017

© 2017 SPLUNK INC.

Implementation Logistics

- This is a simple project IF you have the required rights and permissions.
  - JIRA requires access to API
  - Splunk access to Transforms and Apps
- No cost, doesn't index data, only populates a lookup.csv

- Who benefits? – Everyone!
  - ERROR messages are assigned to teams, tracked and triaged
  - Alarms triggered for new ERROR events
  - Regressions are caught early

© 2017 SPLUNK INC.

ZOC

Zillow Operations Center responsibilities

- Monitor Site Health
  - Routine Eyes on Glass
  - Code Deployments
  - Outages
- Protect and Defend
  - Site Error Rates
  - Log Level Rates
  - Perception of Unhealthiness

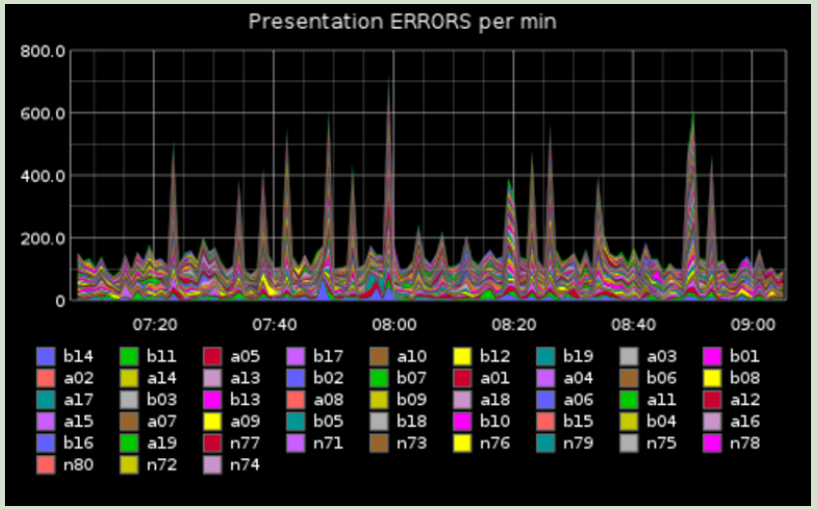
© 2017 SPLUNK INC.

ZOC

Our traditional tools before Splunk

terminal	Graphite	log rollups

```
'2017-04-03T15:48:55.511889Z' '[hi_api.controllers.api.collections_controller] _update_collection_order_and_details called with
 user_id: 56451544, collection_id: 2285921'
'2017-04-03T15:48:55.598456Z' '[elasticsearch] HEAD /hi_search/image/9523396527 [status:404 request:0.002s]'
'2017-04-03T15:48:55.598825Z' '[boto3.resources.action] Calling sqs:send_message with {u\'QueueUrl\': \'https://us-west-2.queue
.amazonaws.com/150122898372/HI_prod_ElasticSearchBoard\', \'MessageBody\': \'{"id": 2285921, "time": 1491234535.598739}\'}'
'2017-04-03T15:48:55.600975Z' '[botocore.vendored.requests.packages.urllib3.connectionpool] Resetting dropped connection: us-we
st-2.queue.amazonaws.com'
'2017-04-03T15:48:57.204575Z' '[boto3.resources.action] Calling sqs:send_message with {u\'QueueUrl\': \'https://us-west-2.queue
.amazonaws.com/150122898372/HI_prod_EmailSubscribe\', \'MessageBody\': \'{"job_data": {"email_address": null, "user_id": 564515
44, "subscription_ids": [42, 41], "is_buzz_check": true}}\'}'
'2017-04-03T15:48:57.206735Z' '[botocore.vendored.requests.packages.urllib3.connectionpool] Resetting dropped connection: us-we
st-2.queue.amazonaws.com'
'2017-04-03T15:49:01.082308Z' '[hi_api.controllers.api.collections_controller] post called with user_id 76897548, collection_id
 None, image_id None'
'2017-04-03T15:49:01.082560Z' '[hi_api.controllers.api.collections_controller] _create_collection called with user_id: 76897548
'
'2017-04-03T15:49:01.105946Z' '[hi_api.controllers.api.collections_controller] Missing user from pogo! Requested: 1, Returned:
0, Missing: [76897548]'
'2017-04-03T15:49:01.123261Z' '[hi_api.controllers.api.collections_controller] Missing user from pogo! Requested: 1, Returned:
0, Missing: [76897548]'
'2017-04-03T15:49:01.125609Z' '[hi_api.controllers.api.collections_controller] Missing user from pogo! Requested: 1, Returned:
0, Missing: [76897548]'
'2017-04-03T15:49:01.125813Z' '[hi_api.lib.application_common] data not found in pogo using empty data with zuid 76897548'
'2017-04-03T15:49:01.322873Z' '[hi_api.controllers.api.collections_controller] post called with user_id 76897548, collection_id
 3137238, image_id 9499223622'
'2017-04-03T15:49:01.325298Z' '[hi_api.controllers.api.collections_controller] _save_image_to_collection called with user_id: 7
6897548, collection_id: 3137238, image_id: 9499223622'
'2017-04-03T15:49:01.332170Z' '[hi.db.image] There is no row for image_id = 9499223622'
'2017-04-03T15:49:01.660312Z' '[hi_api.controllers.api.images_v2] Missing user from pogo! Requested: 262, Returned: 261, Missin
g: [37361976]'
'2017-04-03T15:49:04.132177Z' '[boto3.resources.action] Calling sqs:send_message with {u\'QueueUrl\': \'https://us-west-2.queue
.amazonaws.com/150122898372/HI_prod_EmailSubscribe\', \'MessageBody\': \'{"job_data": {"email_address": null, "user_id": 581368
50, "subscription_ids": [42, 41], "is_buzz_check": true}}\'}'
'2017-04-03T15:49:04.155737Z' '[boto3.resources.action] Calling sqs:send_message with {u\'QueueUrl\': \'https://us-west-2.queue
.amazonaws.com/150122898372/HI_prod_UserSavedSearch\', \'MessageBody\': \'{"job_data": {"update_time": 1491234544.155594, "emai
l_frequency_id": 4, "user_id": 58136850, "subscription_type_id": 1, "search_object": {"room_type_id": 34, "style_id": null, "ta
g_ids": [], "grade_id": null, "color": null, "text": null, "tag_count": 0}}}\'}'
'2017-04-03T15:49:04.157989Z' '[botocore.vendored.requests.packages.urllib3.connectionpool] Resetting dropped connection: us-we
st-2.queue.amazonaws.com'
```



lyn-del-pre-errors Error Counters

1386647	Info
681216	Warn
53541	Errors
0	Fatals

lyn-del-pre-errors Errors

17539	web.service.homedetail.PropertyLinkFactoryImpl AddressObject is null for zpid #
4202	[I/O dispatcher #]service.account.FutureLoginImpl
1802	web.ZillowEngine org.apache.hivemind.ApplicationRuntimeException: Proxied content call returned an internal server error.####activationPath=/contacts/AddContactStatusUpdate.htm##Path=/contacts/AddContactStatusUpdate.htm##Content-Length=###
1032	web.ZillowEngine java.lang.RuntimeException: com.google.common.util.concurrent.UncheckedExecutionException: com.zillow.service.asset.StaticsAssetFetchException: Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/calculator/payment/hdp/app.config.json - Error: Read
1006	web.pages.search.SearchDispatcher
887	database.utils.PropertySetter Property 'valueByCode' threw exception; nested exception is java.lang.IllegalArgumentException: No enumeration element for type:Type ID:# Base:Enum elements:Baseboard(#,#),Forced air(#,#),Geothermal(#,#),Heat pump(#,#),Radiant(#,#),Stove(#,#),Wall(#,#),Other(#,#), code:
871	web.ZillowEngine java.lang.RuntimeException: com.google.common.util.concurrent.UncheckedExecutionException: com.zillow.service.asset.StaticsAssetFetchException: Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/after-bal-contact/app.config.json - Error: Read timed
827	service.asset.StaticsAssetFetcher Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/calculator/payment/hdp/app.config.json - Error: Read timed out
771	web.pages.personalization.api.PersonalizationJsonResponsePage Error getting personalization data
767	web.components.homedetail.facts.CompareWithPublicFacts Could not get detailed propertyInformation from property database for id: #
758	database.utils.PropertySetter Property 'valueByCode' threw exception; nested exception is java.lang.IllegalArgumentException: No enumeration element for type:Type ID:# Base:Enum elements:Brick(#,#),Cement / Concrete(#,#),Composition(#,#),Metal(#,#),Shingle(#,#),Stone(#,#),Stucco(#,#),Vinyl(#,#),Wood
749	service.asset.StaticsAssetFetcher Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/after-bal-contact/app.config.json - Error: Read timed out
744	service.asset.StaticsAssetFetcher Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/calculator/payment/hdp-summary/app.config.json - Error: Read timed out
707	service.asset.StaticsAssetFetcher Exception retrieving from http://zgm-frontend-prod.s#-website-us-west-#.amazonaws.com/calculator/affordability/hdp/app.config.json - Error: Read timed out
706	database.utils.PropertySetter Property 'valueByCode' threw exception; nested exception is java.lang.IllegalArgumentException: No enumeration element for type:Type ID:# Base:Enum elements:Carport(#,#),Garage - Attached(#,#),Garage - Detached(#,#),Off-street(#,#),On-street(#,#),None(#,#), code:#skippi
684	database.utils.PropertySetter Property 'valueByCode' threw exception; nested exception is java.lang.IllegalArgumentException: No enumeration element for type:Type ID:# Base:Enum elements:Coal(#,#),Electric(#,#),Gas(#,#),Oil(#,#),Propane / Butane(#,#),Solar(#,#),Wood / Pellet(#,#),Other(#,#),None(#,#
599	service.account.FutureLoginImpl
515	service.imaging.ImagingServiceImpl Exception invoking image conversion service
515	service.imaging.ImagingServiceImpl ERROR upload to CLOUD
510	service.imaging.ImagingServiceImpl Error Converting ImageId #// Returned # for addImageWorkitemStream but: HTTP/#.# # Not Implemented
507	web.ZillowEngine java.lang.NullPointerException####activationPath=/search/Unsubscribed.htm##Path=/search/Unsubscribed.htm##
481	web.pages.search.GetResults Unhandled error in pageBeginRender:
480	web.ZillowEngine java.lang.NullPointerException####activationPath=/profile##Path=/profile/Eric-Buersken/##
467	service.user.auth.ExternalAccountProviderWrapper AUTH: Failed to reload login session: ResponseImpl{code=#, host did not accept the connection within timeout of # ms'}
457	web.components.profiles.reviews.ReviewListJSON error retrieving data from review-display api
453	web.ZillowEngine java.lang.RuntimeException: Encoded url identifier has no valid type: AjaxRender.htm####activationPath=/url-shortener/AjaxRender.htm##Param:
426	web.service.homedetail.logic.contact.PropertyContactRecipientLogicImpl Couldn't find posting contact emails in the database for property: #

splunk> .conf2017

© 2017 SPLUNK INC.

ZOC

Limitations

- Graphs only show basic volume trends
- Strong cmd line foo to tail logs meaningfully
- Log rollups lack time dimension

Is that error new? Intro'd with release? Regression?

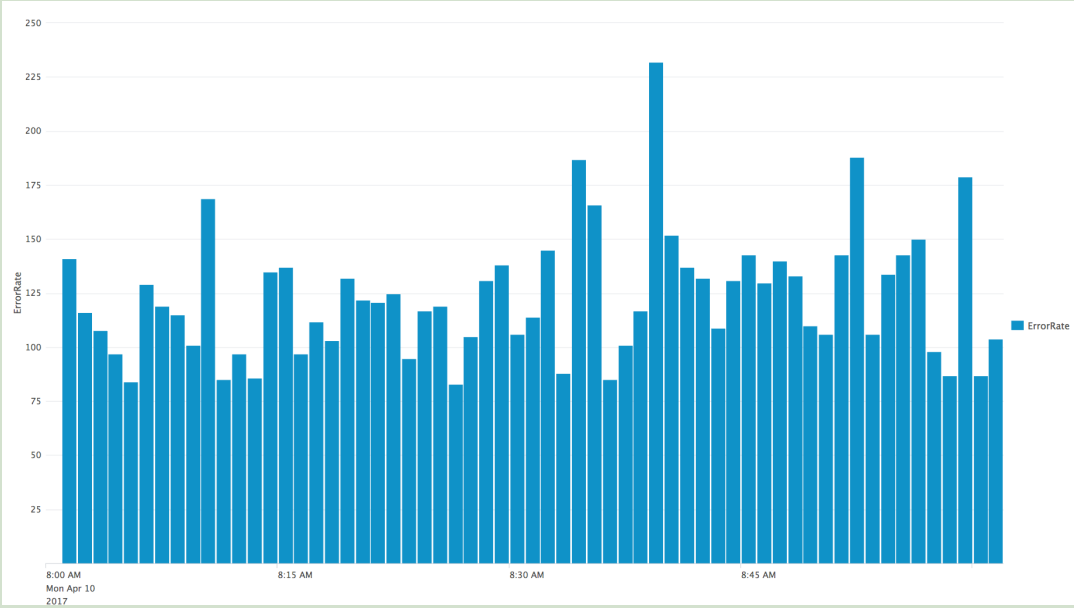
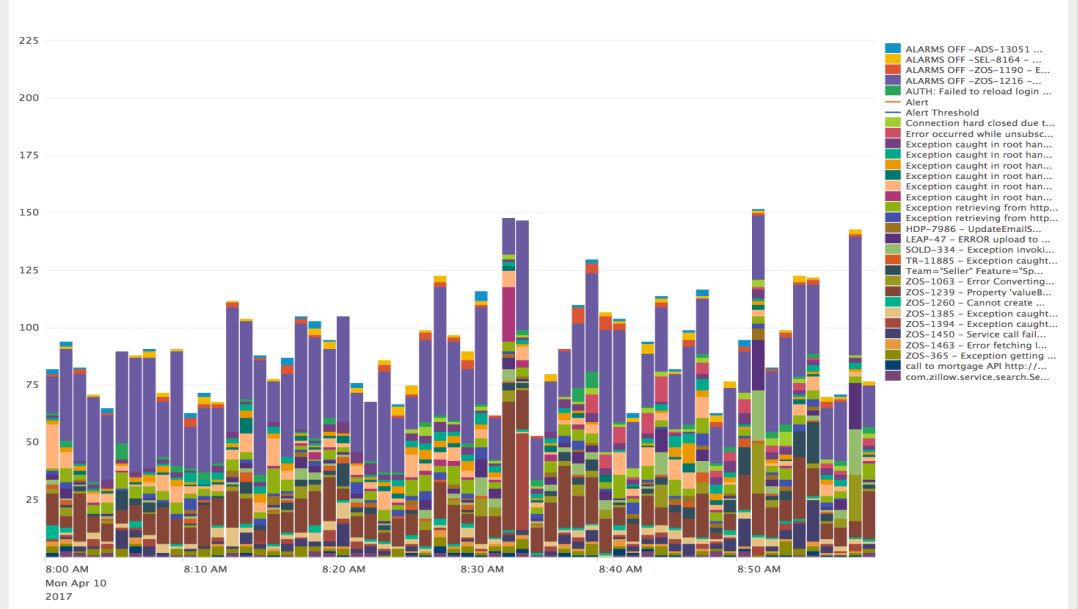
Who owns that?

What just happened?

© 2017 SPLUNK INC.

ZOC

Needed a solution

to turn this	into this… automatically
	

splunk> .conf2017

© 2017 SPLUNK INC.

Lexicon

Java service error log

- 2017-07-12T18:14:50.205813+00:00 WARN [com.zillow.web.pages.myzillow.SavedSearchEdit] no saved search available for XXXXXXXXXX
- 2017-07-12T18:14:50.661995+00:00 ERROR [com.zillow.db.InnerPool] Connection hard closed due to exception:java.sql.SQLException: Invalid state, the Connection object is closed. src:{ call dbo.XXXXXXXXXX(XXXXXXXXXX) } on jdbc:jtds:sqlserver://XXXXXXXXXX
- 2017-07-12T18:14:50.662739+00:00 ERROR [org.springframework.transaction.support.TransactionTemplate] Application exception overridden by rollback exception

© 2017 SPLUNK INC.

Lexicon

Java service error log

- Timestamp
- Severity level
- Class – hierarchical code template
- Message – verbose return

- 2017-07-12T18:14:50.205813+00:00 WARN [com.zillow.web.pages.myzillow.SavedSearchEdit] no saved search available for XXXXXXXXXX
- 2017-07-12T18:14:50.661995+00:00 ERROR [com.zillow.db.InnerPool] Connection hard closed due to exception:java.sql.SQLException: Invalid state, the Connection object is closed. src:{ call dbo.XXXXXXXXXX(XXXXXXXXXX) } on jdbc:jtds:sqlserver://XXXXXXXXXX
- 2017-07-12T18:14:50.662739+00:00 ERROR [org.springframework.transaction.support.TransactionTemplate] Application exception overridden by rollback exception

splunk> .conf2017

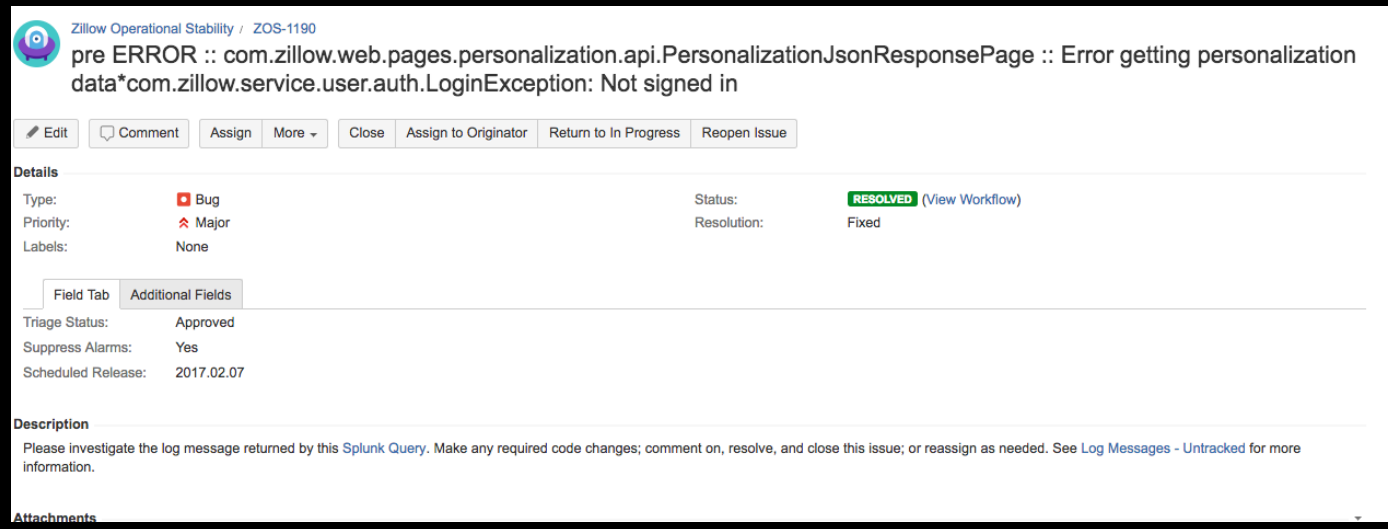
© 2017 SPLUNK INC.

Lexicon

JIRA

A commercial issue tracking product, developed by Atlassian.

- **JIRA is a component of Zillow's code development tool suite**
  - Provides bug tracking, issue tracking, and project management functions.



© 2017 SPLUNK INC.

Lexicon

jirarest

Add-on used to query JIRA's API

| jirarest jqlsearch "LogTrackingEnabled=Yes"

→ **Using https://github.com/firebus/splunk-jira** ←

Version 2.1 handles auto-pagination for production-scale Jira implementations, jirarest command

Not using official Splunk version https://splunkbase.splunk.com/app/1438/

Provides only jira command to live query JIRA REST API. Deprecated jirarest commands.

splunk> .conf2017

© 2017 SPLUNK INC.

Lexicon

lookup

| lookup <lookup-table-name> <lookup-field1> AS <event-field1>, <lookup-field2> AS <event-field2> OUTPUTNEW <lookup-destfield1> AS <event-destfield1>, <lookup-destfield2> AS <event-destfield2>

| lookup update=true MyLookup msg, cls, java_svc OUTPUT bug java_svc cls lvl msg Priority

© 2017 SPLUNK INC.

Lexicon

cluster

For rollups, regex has it’s limitations…

rex field=msg mode=sed "s/\S+@\S+.\w+/*@*.*x/g" | rex field=msg mode=sed "s/token = \S+\w+/token = */g" | rex field=msg mode=sed "s/screenname=.+\w+/screenname=*/g" | rex field=msg mode=sed "s/(?s)(.{200}).+/\1*/g" | rex field=msg mode=sed "s/\d+/*/g" | rex field=msg mode=sed "s/\"/ /g" | rex field=msg mode=sed "s/zws-id=[^&].+\w+/zws-id=*/g”

→ | eval msg=substr(msg,1,200)

| cluster t=0.8 labelonly=t field=msg

splunk> .conf2017

© 2017 SPLUNK INC.

Lexicon

cluster

```
<base_search> lvl=ERROR
| eval msg=substr(msg,1,200)
| cluster t=0.8 labelonly=t field=msg
| top limit=0 msg cluster_label
| where count > 60
| sort cluster_label
```

Last 15 minutes

✓ 3,809 events (7/18/17 10:54:37.000 AM to 7/18/17 11:09:37.000 AM) No Event Sampling Job Verbose Mode

Events (3,809) | Patterns | Statistics (8) | Visualization

100 Per Page Format Preview

msg	cluster_label	count	percent
AddressObject is null for zpid 2093526210	2	84	2.205303
AddressObject is null for zpid 79905228	2	64	1.680231
Asset not found at http://zgm-frontend-prod.s3-website-us-west-2.amazonaws.com/calculator/payment/hdp-summary/app.config.json	28	122	3.202940
Unhandled exception from call. : hdpHomeValues com.zillow.pogo.client.impl.IOExceptionUnrecoverable: Request to <http://pogo-collator.del.zillow.local> failed for query: <return{bedrooms,zestimate,pri	91	116	3.045419
Unhandled exception from call. : recentlySoldComps com.zillow.pogo.client.impl.IOExceptionUnrecoverable: Request to <http://pogo-collator.del.zillow.local> failed for query: <return{videoIds,zestimate	91	72	1.890260
Unhandled exception from call. : forSaleComps com.zillow.pogo.client.impl.IOExceptionUnrecoverable: Request to <http://pogo-	91	68	1.785245

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

1. Create and fill fields in JIRA tickets
1. Search JIRA with jirarest to populate lookup file
1. Enable wildcard searching - transforms.conf
1. Create searches against fields using lookups
1. Enhance with evals and conditionals

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

1. Create and fill fields in JIRA tickets

- LogTrackingEnabled
- LogTrackingMessage
- LogTrackingClass
- LogTrackingLevel
- LogTrackingService

LogTrackingEnabled	☑ Yes
LogTrackingMessage	no saved search available for *
LogTrackingService	pre
LogTrackingClass	com.zillow.web.pages.myzillow.SavedSearchEdit
LogTrackingLevel	WARN

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

2. Search JIRA with jirarest to populate lookup file

```
| jirarest jqlsearch "LogTrackingEnabled=Yes"
| eval bug=Key
| eval msg=LogTrackingMessage
| eval cls=LogTrackingClass
| eval lvl=LogTrackingLevel
| eval java_svc=LogTrackingService
| table bug msg cls lvl java_svc "Suppress Alarms"
| fillnull value="NULL"
| outputlookup MyLookup.csv
```

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

2. Search JIRA with jirarest to populate lookup file

```
| jirarest jqlsearch "LogTrackingEnabled=Yes"
| eval bug=Key
| eval msg=LogTrackingMessage
| eval cls=LogTrackingClass
| eval lvl=LogTrackingLevel
| eval lava_svc=LogTrackingService
| table bug msg cls lvl java_svc "Suppress Alarms"
| fillnull value="NULL"
```

Last 15 minutes

✓ 674 events (7/18/17 9:25:11.000 AM to 7/18/17 9:40:11.000 AM) No Event Sampling

Job Verbose M

Events (674) Patterns Statistics (674) Visualization

100 Per Page Format Preview

Prev 1 2 3 4 5 6 7

bug	msg	cls	lvl	java_svc	Suppress Alarms
ZPID-8656	Connection hard closed due to exception:java.sql.SQLException: Procedure or function 'PropertyLatLongUserMrg*' expects parameter *@*.*x was not supplied. src:{call dbo.PropertyLatLongUserMrg*(?, ?, *	com.zillow.db.InnerPool	ERROR		NULL
ZPID-8655	org.springframework.jdbc.BadSqlGrammarException: CallableStatementCallback; bad SQL grammar []; nested exception is java.sql.SQLException: Procedure or function 'PropertyLatLongUserMrg*' expects para*	com.zillow.web.pages.ajax.property.AddProperty	ERROR		NULL
ZPID-7038	java.lang.NoSuchFieldException: ZillowCSskipping property initialization for:dataSourceType	com.zillow.database.utils.PropertySetter	ERROR		NULL
ZPID-6653	OCP operation took*	com.zillow.service.overlapped.OverlappedCallManager	WARN		NULL
ZOS-1712	Unhandled error in pageBeginRender*com.zillow.pogo.client.impl.IOExceptionUnrecoverable*Request to*http*//pogo-collator.del.zillow.local*failed for query*	com.zillow.web.pages.search.GetResults	ERROR		NULL
ZOS-1711	Unhandled exception from call*com.zillow.pogo.client.impl.IOExceptionUnrecoverable*Request to*http*//collator-pog.del.zillow.local*failed for query*	com.zillow.service.overlapped.OverlappedCallManager	ERROR		NULL
ZOS-1710	Unhandled exception from call*com.zillow.pogo.client.impl.IOExceptionUnrecoverable*Request to *http*//pogo-collator.del.zillow.local*	com.zillow.service.overlapped.OverlappedCallManager	ERROR		NULL
ZOS-1709	Exception caught in root handler* java.lang.NullPointerException*Request received at Fri Jul * PDT *Method*GET* activationPath*/ui/ClientProfile.htm*Path*/ui/ClientProfile.htm*Memory* Free*983MB* Total*2437MB* Max*2534MB*java.lang.NullPointerException*	com.zillow.web.ZillowEngine	ERROR		Yes

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

2. Search JIRA with jirarest to populate lookup file

```
| jirarest jqlsearch "LogTrackingEnabled=Yes"
| eval bug=Key
| eval msg=LogTrackingMessage
| eval cls=LogTrackingClass
| eval lvl=LogTrackingLevel
| eval java_svc=LogTrackingService
| table bug msg cls lvl java_svc "Suppress Alarms"
| fillnull value="NULL"
| outputlookup MyLookup.csv
```

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

3. Enable wildcard searching - transforms.conf

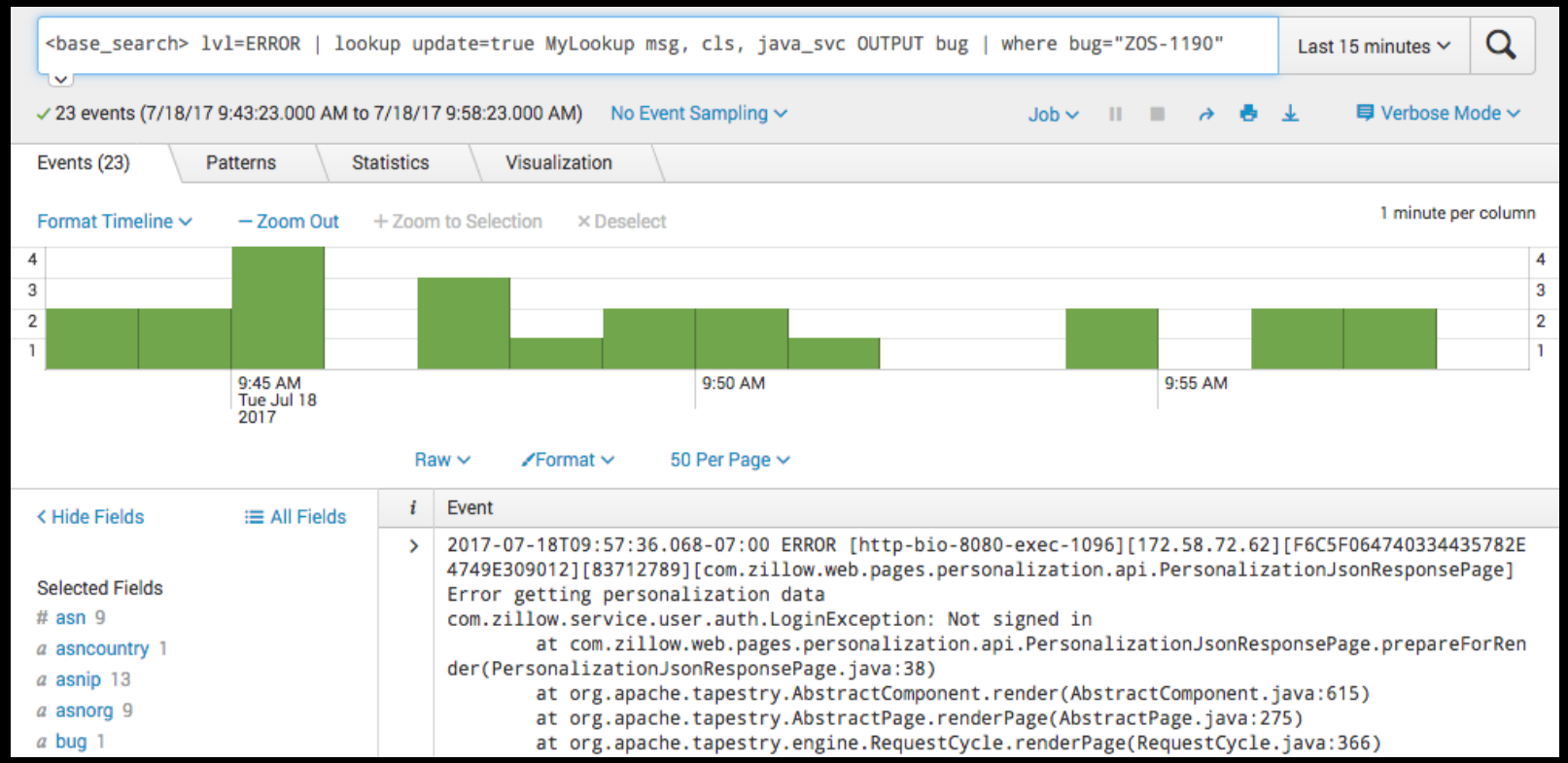
```
[MyLookup]
filename = MyLookup.csv
case_sensitive_match=false
match_type = WILDCARD(msg)
```

© 2017 SPLUNK INC.

Step by Step

4. Create searches against fields using lookups

<base_search> lvl=ERROR | lookup update=true MyLookup msg, cls, java_svc OUTPUT bug | where bug="ZOS-1190"



splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

4. Create searches against fields using lookups

<base_search> lvl=ERROR | lookup update=true MyLookup msg, cls, java_svc OUTPUT bug | where bug="ZOS-1190"

bug	lvl	msg	cls	java_svc
ZOS-1190	ERROR	Error getting personalization data*com.zillow.service.user.auth.LoginException: Not signed in*	com.zillow.web.pages.personalization.api.PersonalizationJsonResponsePage	pre

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

4. Create searches against fields using lookups

<base_search> lvl=ERROR | lookup update=true MyLookup msg, cls, java_svc OUTPUT bug | where bug="ZOS-1190"

2017-07-18T09:57:36.068-07:00 ERROR [http-bio-8080-exec-1096][172.58.72.62][F6C5F064740334435782E4749E309012][83712789][com.zillow.web.pages.personalization.api.PersonalizationJsonResponsePage] Error getting personalization data com.zillow.service.user.auth.LoginException: Not signed in
at com.zillow.web.pages.personalization.api.PersonalizationJsonResponsePage.prepareForRender(PersonalizationJsonResponsePage.java:38)

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

5. Enhance with evals and conditionals

```
<base_search> lvl=ERROR
| lookup update=true MyLookup msg, cls, java_svc OUTPUT bug "Suppress Alarms”
| eval msg=substr(msg,1,200)
| cluster t=0.8 labelonly=t field=msg
| eval cluster_by = if(isnotnull(bug), bug, cluster_label)
| eventstats first(bug) as bug, first(msg) as msg by cluster_by
| eval bug = if(like('Suppress Alarms',"Yes"), "ALARMS OFF -".bug, bug)
| eval bug = if(isnotnull(bug), bug." - ".msg, msg)
| timechart count by bug usenull=f useother=f
...
```

splunk> .conf2017

© 2017 SPLUNK INC.

Step by Step

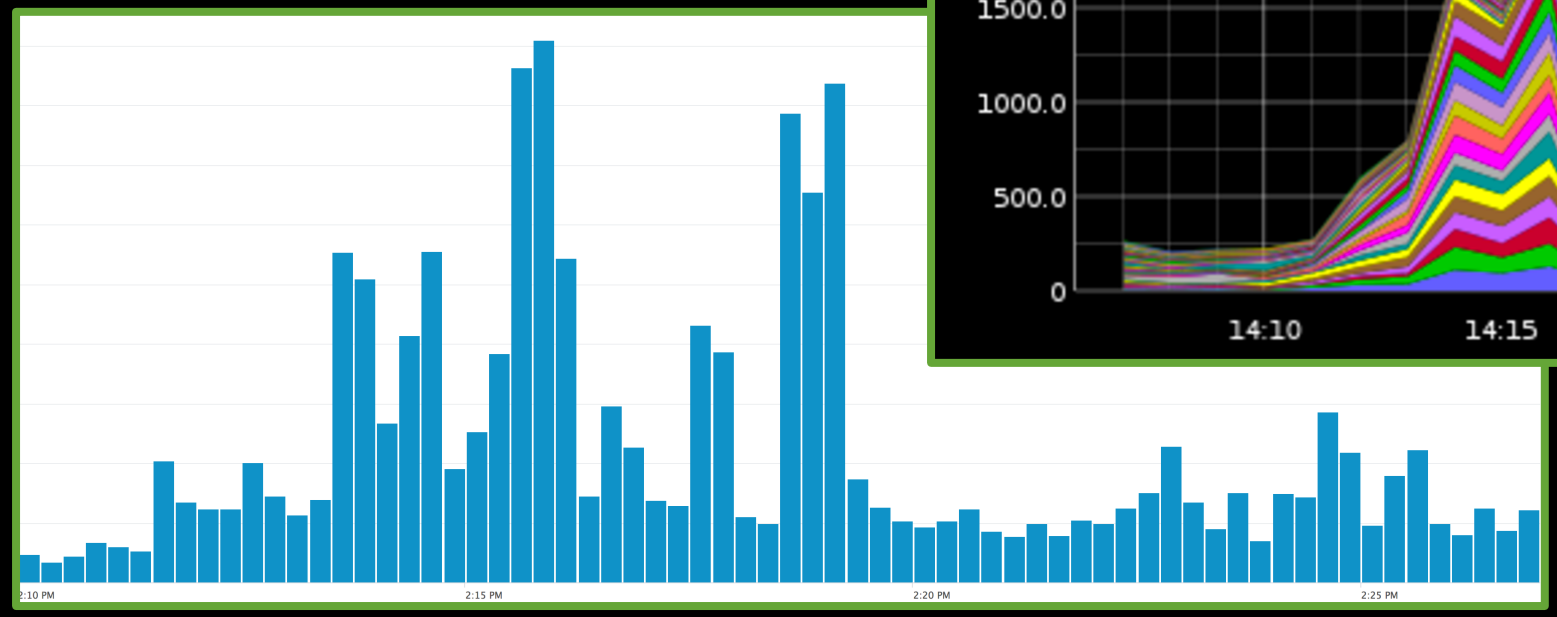
5. Enhance with evals and conditionals (cont.)

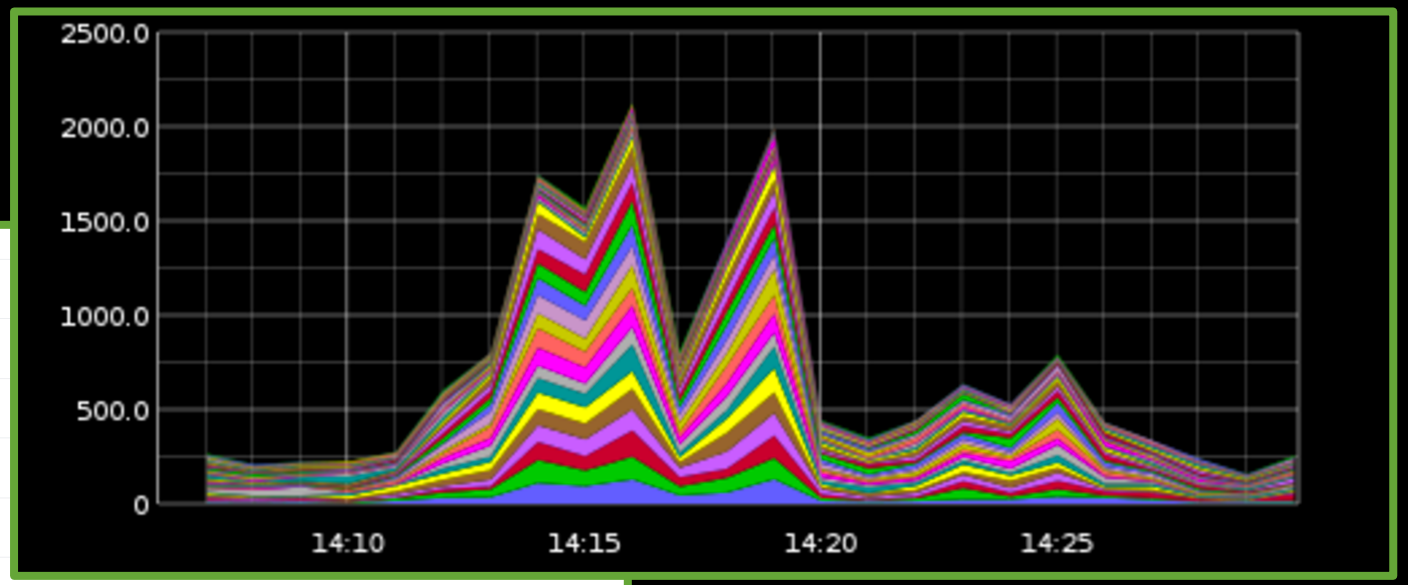
```
...
| eval alert=300 | rename alert AS "Alert Threshold"
| appendcols [ search index="_internal" sourcetype="scheduler" thread_id="AlertNotifier*" NOT
(alert_actions="summary_index" OR alert_actions="")
| where like(savedsearch_name,"%Error Rate Threshold Exceeded%")
| timechart count(savedsearch_name) AS Alert
| fields Alert | eval Alert= Alert * 350 ]
```

splunk> .conf2017

© 2017 SPLUNK INC.

To turn this…

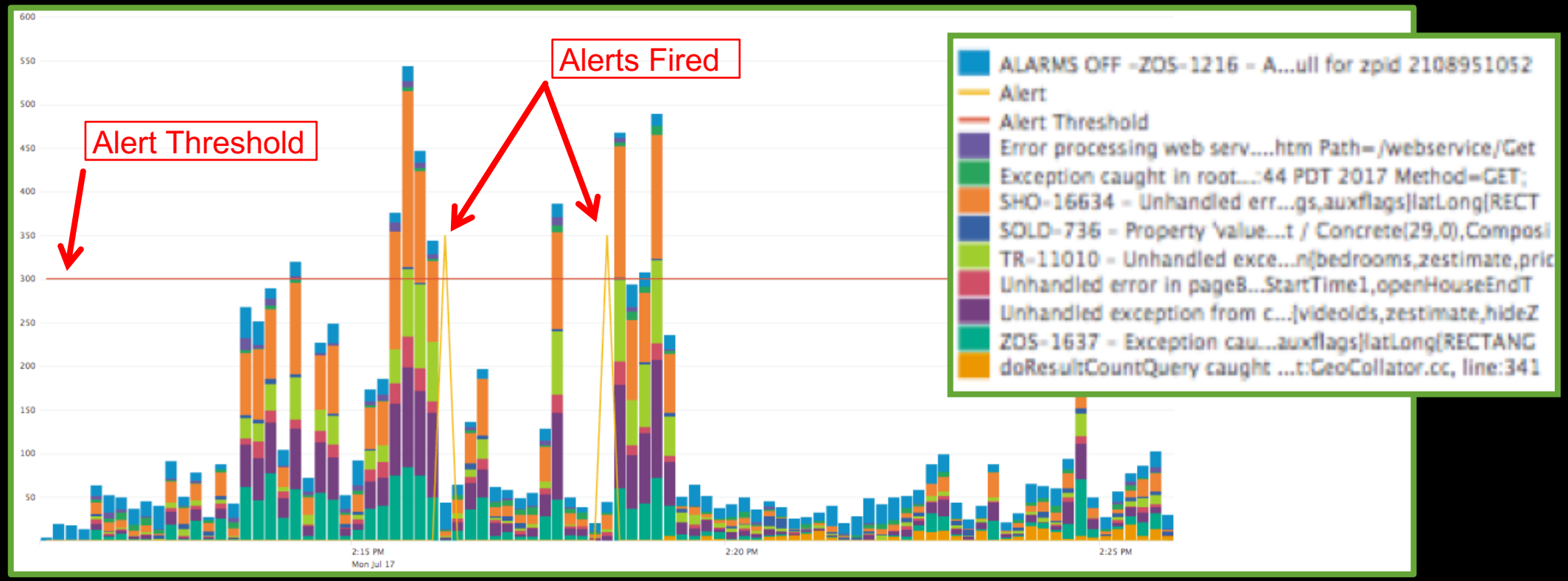




splunk> .conf2017

© 2017 SPLUNK INC.

...into this



splunk> .conf2017

© 2017 SPLUNK INC.

and this…

splunk> .conf2017

© 2017 SPLUNK INC.

and this…

_time	Top 10 Errors	Msg Count	Total Count
Wed Jul 19 22:15:00 2017	Minor - https://zbrt.atl.zillow.net/browse/PERS-5522	16596	38286
	Connection hard closed due to exception:java.sql.SQLException: The tar	7536	
	Unable to obtain pooled connection for bean 'SubscriptionReadonly': Ti	4372	
	Minor - https://zbrt.atl.zillow.net/browse/ZOS-1564	3913	
	Unable to obtain pooled connection for bean 'SubscriptionReadonly': Ne	3913	
	Major - https://zbrt.atl.zillow.net/browse/ADS-13199	494	
	Error getting latest ordinal	291	
	org.springframework.jdbc.CannotGetJdbcCon	205	
	Exception caught in root handler: org.springframework.jdbc.CannotGetJd	155	
	Exception caught in root handler: org.springframework.dao.TransientDat	139	
	Unable to obtain pooled connection for bean 'Subscription': Login time	139	
	java.sql.SQLException: Login timed out. connecting to: jdbc:jtds:sqlse		
Wed Jul 19 22:14:00 2017	Minor - https://zbrt.atl.zillow.net/browse/PERS-5522	18946	37852
	Connection hard closed due to exception:java.sql.SQLException: The tar	7869	
	Unable to obtain pooled connection for bean 'Subscription': Login time	4226	
	java.sql.SQLException: Login timed out. connecting to: jdbc:jtds:sqlse	4226	
	Major - https://zbrt.atl.zillow.net/browse/ADS-13199	579	

splunk> .conf2017

© 2017 SPLUNK INC.

Recap

1. **Create and fill fields in JIRA tickets**
   - Manual or semi-automated
2. **Search JIRA with jirarest to populate lookup file**
   - Saved Search (/10min)
3. **Enable wildcard searching - transforms.conf**
   - One-time configuration
4. **Create searches against fields using lookups**
   - Dashboards, alerts, leaderboards, etc.
5. **Enhance with evals and conditionals**
   - Many, many possibilities

splunk> .conf2017

© 2017 SPLUNK INC.

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017