QFX5100 Guest VM:

Data Monitoring Application Setup Guide

Revision 2

Table of Contents

1 Objectives

Using combinations of data acquired from the infrastructure's components and network elements, Junos Network Analytics applies sophisticated data analysis algorithms, control systems techniques, and reporting in order to provide visibility into the aspects of the data center infrastructure’s performance and behavior. These aspects can now be directly visualized through a Guest VM application, called the Data Monitoring Application.

This application can be used to process and report the traffic and queue statistics collected from Junos. The analyzed report can then be visualized graphically using third-party visualization tools (like Kibana) running on a desktop or laptop.

The Data Monitoring application uses the Guest VM infrastructure and internally relies on the below third-party tools/libraries:

- Fluentd - Open source data collector designed for processing data streams
- Elasticsearch – Provides distributed RESTful search and analytics
- Kibana - Visualize logs and time-stamped data

This document aims to serve as a step-by-step installation and configuration guide for the Data Monitoring application.

2 Scope

This document describes how to leverage QFX5100 Guest VM infrastructure to build applications using third-party software. Juniper Networks is not liable for support of any issues reported with third-party software.

3 Steps to build the Data Monitoring Application

The following are the steps that need to be followed for building and using the Data Monitoring application:

1. Guest VM creation using JunosV App Engine configuration
2. Junos AnalyticsD configuration
3. Installation of Fluentd, Elasticsearch and AnalyticsD plugin on the Guest VM created in Step 1
4. Launching Fluentd and Elasticsearch on the Guest VM
5. Configuring Kibana on the PC or laptop to view the Traffic/Queue statistics graphically

3.1 Step 1: Guest VM creation using a JunosV App Engine configuration

A Guest VM needs to be created by building a Guest VM package, installing the Guest VM package with the help of the Junos OS CLI, and committing the Guest VM configurations in the Junos configuration mode.

The following document provides a step-by-step guide for creating a Guest VM and can be followed for creating the Guest VM:

http://www.juniper.net/techpubs/en_US/junos13.2/topics/task/installation/qfx-series-guest-vmm.html

3.2 Step 2: Junos AnalyticsD Configuration

For the purpose of reporting the Traffic and Queue statistics from the Junos VM to the Guest VM, CLI options must be configured under the "**`set services analytics`**" hierarchy in the Junos configuration mode.

The following is the sample configuration that can be used.

```
set groups datamon services analytics export-profiles p1 stream-format json

set groups datamon services analytics export-profiles p1 interface statistics
traffic

set groups datamon services analytics export-profiles p1 interface statistics
queue

set groups datamon services analytics export-profiles p1 system information

set groups datamon services analytics export-profiles p1 system status
traffic

set groups datamon services analytics export-profiles p1 system status queue

set groups datamon services analytics resource-profiles rp1 queue-monitoring

set groups datamon services analytics resource-profiles rp1 traffic-
monitoring

set groups datamon services analytics resource system resource-profile rp1

set groups datamon services analytics resource system polling-interval
traffic-monitoring 10

set groups datamon services analytics resource system polling-interval queue-
monitoring 10
```

```
set groups datamon services analytics collector local file datamon.stat

set groups datamon services analytics collector local file size 10m

set groups datamon services analytics collector address 10.204.38.76 port
24224 transport tcp export-profile p1

set apply-groups datamon
```

NOTE: In the above configuration, in “`set groups datamon services analytics collector address 10.204.38.76 port 24224 transport tcp export-profile p1`,” the IP address `10.204.38.76` needs to be replaced with the IP address that will be configured on the management interface of the Guest VM. The port number `24224` should be kept as it is as the same is used by the third party application Fluentd running on the Guest VM.

Please note that the traffic and queue monitoring intervals can also be modified in the configuration depending on your requirements.

- “`set groups datamon services analytics resource system polling-interval traffic-monitoring 10`”
- “`set groups datamon services analytics resource system polling-interval queue-monitoring 10`”

3.3 Step 3: Installation of Fluentd, Elasticsearch and AnalyticsD plugin

- Log into the Guest VM and assign the IP address on the external Management interface of the Guest VM. For example, if `eth6` is the external management interface on the Guest VM, then

  ```
  ifconfig eth6 inet <IP-address> netmask <netmask>
  ```

- Configure the default gateway on the Guest VM

  ```
  route add default gw <gateway>
  ```

- After the above configurations are done, PING from the Guest VM to the Junos VM should start working. Confirm this by executing the following command on the Guest VM:

  ```
  ping <Junos-VM-IP-address>
  ```

  where `<Junos-VM-IP-address>` is the IP address configured on the Management Interface assigned to the Junos VM.

NOTE: Third party applications need to be downloaded through the Internet, so please make sure that Internet connectivity is enabled on the above IP address configured for the Guest VM external management interface.

3.3.1 Fluentd Installation and Configuration

1. Install the Fluentd Td-agent:

```
curl -L http://toolbelt.treasuredata.com/sh/install-redhat.sh | sh
```

2. Install the Elasticsearch plugin for Fluentd Td-agent:

```
cd ~
```

```
curl -L https://github.com/uken/fluent-plugin-elasticsearch/archive/v0.2.0.zip > ~/master.zip
```

```
yum -y install unzip
```

```
unzip master.zip
```

```
cd fluent-plugin-elasticsearch-0.2.0
```

`vi fluent-plugin-elasticsearch.gemspec` and modify the field `s.files` to set it to ["`lib/fluent/plugin/out_elasticsearch.rb`"]

```
/usr/lib64/fluent/ruby/bin/fluent-gem build fluent-plugin-
elasticsearch.gemspec
```

```
/usr/lib64/fluent/ruby/bin/fluent-gem install fluent-plugin-elasticsearch-
0.2.0.gem --no-rdoc --no-ri
```

Execute the following command to confirm that fluent-plugin-elasticsearch has been installed.

```
/usr/lib64/fluent/ruby/bin/fluent-gem list| grep elasticsearch
```

```
cd ~
```

```
rm -rf master.zip
```

3. Obtain the contents of `td-agent.conf` from Appendix A and set up the Td-agent configuration for AnalyticsD:

```
vi ~/td-agent.conf
```

Next, copy and paste the contents of `td-agent.conf` from Appendix A into the above created new file `~/td-agent.conf`.

Replace the Td-agent configuration with the above `~/td-agent.conf` with the following command:

```
cp ~/td-agent.conf /etc/td-agent/td-agent.conf
```

4. Make sure `/var/log/fluentd` exists and is owned by the Td-agent:

```
mkdir /var/log/fluentd

chown td-agent /var/log/fluentd

chgrp td-agent /var/log/fluent
```

5. Additional details on Fluentd can be found at:

- http://www.fluentd.org/
- https://github.com/fluent/fluentd

3.3.2 Elasticsearch Installation and Configuration

1. Install JVM version 6 or higher, as this is a prerequisite for Elasticsearch:

```
yum install java-1.6.0-openjdk
```

2. Download and install Elasticsearch and its service wrapper:

```
cd ~

curl https://download.elasticsearch.org/elasticsearch/elasticsearch/elasticsearch-1.0.1.tar.gz | tar xvz

mkdir /etc/elasticsearch

mv ~/elasticsearch-1.0.1/* /etc/elasticsearch

rm -rf  ~/elasticsearch-1.0.1

yum -y install unzip

curl -L https://github.com/elasticsearch/elasticsearch-servicewrapper/archive/master.zip > master.zip

unzip master.zip

cd elasticsearch-servicewrapper-master/

mv service /etc/elasticsearch/bin
```

```
cd ~
```

```
rm -rf elasticsearch-servicewrapper-master master.zip
```

```
/etc/elasticsearch/bin/service/elasticsearch install
```

3. Obtain the contents of `default-mapping.json` from Appendix A and place it into Elasticsearch:

```
vi ~/default-mapping.json
```

Next, copy and paste the contents of `default-mapping.json` from Appendix A into the above created new file `~/default-mapping.json`.

```
cp ~/default-mapping.json /etc/elasticsearch/.
```

4. Edit the `cluster.name` entry in the Elasticsearch yml file to give Elasticsearch a name:

```
vi /etc/elasticsearch/config/elasticsearch.yml
```

Edit the `cluster.name` entry (for example: `cluster.name: DataMonitoringVM!`).

```
cp ~/elasticsearch.yml /etc/elasticsearch/config/elasticsearch.yml
```

5. Elasticsearch is now ready to use and the following commands can be executed when needed:

```
service elasticsearch start
```

```
service elasticsearch stop
```

```
service elasticsearch restart
```

```
service elasticsearch status
```

6. Additional details on Elasticsearch can be found at:

- http://www.elasticsearch.org/
- https://github.com/elasticsearch/elasticsearch

3.3.3 AnalyticsD Plugin Installation

1. Edit ~/.bash_profile to add a few paths for ruby gems:

```
PATH=$PATH:$HOME/bin:/usr/share/elasticsearch/bin:/usr/lib64/fluent/
ruby/bin/

GEM_HOME="/usr/lib64/fluent/ruby/lib/ruby/gems/1.9.1/"

GEM_PATH="/usr/lib64/fluent/ruby/lib/ruby/gems/1.9.1/"

export PATH

export GEM_PATH

export GEM_HOME
```

2. Export the paths by executing the following command:

```
source ~/.bash_profile
```

3. Generate the file `in_AnalyticsD.rb` and place that in the home directory:

```
mkdir ~/AnalyticsD_utility

cd ~/AnalyticsD_utility
```

Place the files `build-plugin` and `build-wrapper` (provided along with this setup guide) in the current directory. Make sure that these two files are executable:

```
chmod +x build-plugin

chmod +x build-wrapper
```

Obtain the file `in_forward.rb` from Github:

```
curl -L https://github.com/fluent/fluentd/archive/skip-nil-record.zip > skip-
nil-record.zip

unzip skip-nil-record.zip

cp fluentd-skip-nil-record/lib/fluent/plugin/in_forward.rb .
```

Install **csh** if it is not already installed on the Guest VM:

```
yum install csh
```

Generate `in_AnalyticsD.rb` using `in_forward.c` and `build-wrapper:`

```
./build-wrapper in_forward.rb
```

Open the file `in_AnalyticsD.rb` and modify lines 161 and 162:

```
record = msg

return if record.nil?

time = msg[1]                  <<<<< Remove this statement

time = Engine.now if time == 0 <<<<< Remove the condition “if time == 0″

Engine.emit(tag, time, record)
```

Thus, the above code snippet in **`in_AnalyticsD.rb`** would now appear as:

```
record = msg

return if record.nil?

time = Engine.now

Engine.emit(tag, time, record)
```

Copy **`in_AnalyticsD.rb`** to the home directory:

```
cp in_AnalyticsD.rb ~/
```

Clean up the directory **`AnalyticsD_utility`**:

```
rm -rf AnalyticsD_utility
```

4. Obtain the contents for **`fluent-plugin-AnalyticsD-0.1.0.gemspec`** from Appendix A and create this file in the home directory:

```
vi ~/fluent-plugin-AnalyticsD-0.1.0.gemspec
```

Copy the contents for this file from Appendix A and paste the same into this new file.

5. Build a directory structure for the Juniper Networks AnalyticsD plugin:

```
mkdir ~/fluent-plugin-AnalyticsD-0.1.0

mkdir ~/fluent-plugin-AnalyticsD-0.1.0/lib

mkdir ~/fluent-plugin-AnalyticsD-0.1.0/lib/fluent

mkdir ~/fluent-plugin-AnalyticsD-0.1.0/lib/fluent/plugin

cp ~/in_AnalyticsD.rb ~/fluent-plugin-AnalyticsD-0.1.0/lib/fluent/plugin/.

cp ~/fluent-plugin-AnalyticsD-0.1.0.gemspec ~/fluent-plugin-AnalyticsD-0.1.0/.
```

6. Build the AnalyticsD gem:

```
cd ~/fluent-plugin-AnalyticsD-0.1.0

fluent-gem build fluent-plugin-AnalyticsD-0.1.0.gemspec
```

```
"NOTE: a warning like the below might be produced. It is harmless.

WARNING:  no homepage specified

  Successfully built RubyGem

  Name: fluent-plugin-AnalyticsD

  Version: 0.1.0

  File: fluent-plugin-AnalyticsD-0.1.0.gem

"
```

7. Install the AnalyticsD gem:

```
fluent-gem install fluent-plugin-AnalyticsD-0.1.0.gem --no-rdoc --no-ri
```

```
"NOTE: a warning like the below will be produced. It is harmless.

WARNING:  Error fetching data: Errno::ETIMEDOUT: Connection timed out -
connect(2) (http://rubygems.org/specs.4.8.gz)

Successfully installed fluent-plugin-AnalyticsD-0.1.0

1 gem installed
```

"

8. Execute the following command to view the list of installed gems and verify that the AnalyticsD gem has been successfully installed:

```
fluent-gem list
```

3.4 Step 4: Launch Fluentd and Elasticsearch on Guest VM

Execute the following commands on the Guest VM in order to launch Elasticsearch and then Fluentd:

```
service iptables stop

service elasticsearch stop

service elasticsearch start

service td-agent restart
```

After the above commands are executed on the Guest VM, the command "**`show analytics collector`**" in the Junos OS CLI should confirm that the connection to the Guest VM has been established.

For example:

```
root@qfx5100-c6-sys> show analytics collector
Address        Port   Transport  Stream format  State        Sent
10.204.38.76   24224  tcp        json           Established  2
```

3.5 Step 5: Configure Kibana on the PC to view the Traffic/Queue statistics

Download Kibana from the following website and place it on the Desktop:

https://download.elasticsearch.org/kibana/kibana/kibana-3.0.0.zip

Unzip the above file. Then a directory structure will get created. In the top level of the directory structure you will find a "config.js" file. Put a line similar to

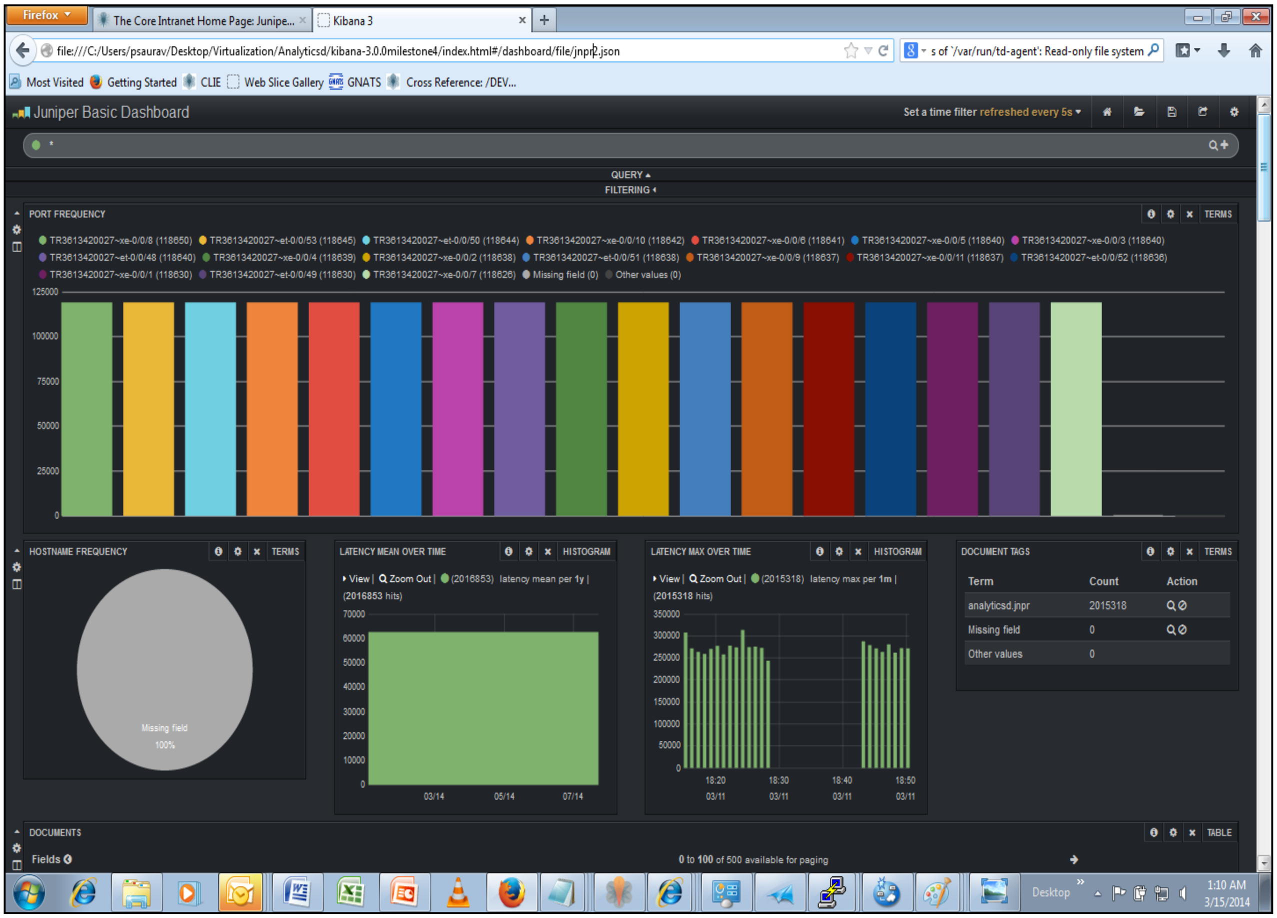
```
elasticsearch: "http://<IP_ADDRESS>:9200"
```

Here, **`IP_ADDRESS`** is the external Management IP address of the Guest VM. Here the port number `9200` is associated to Elasticsearch and should be kept as it is.

Start up either Microsoft Internet Explorer or Mozilla Firefox (these are the only browsers supported). Point the browser to a Kibana dashboard to visualize the traffic and queue statistics. For example, if the Kibana directory structure for a user <*username*> is located at "C:/Users/<username>/Desktop/kibana-3.0.0milestone4", the browser can be pointed to the Kibana dashboard *guided.json* by specifying the path as:

file:///C:/Users/<username>/Desktop/kibana-3.0.0milestone4/index.html#/dashboard/file/guided.json

Sample output taken from Kibana


file:///C:/Users/psaurav/Desktop/Virtualization/Analyticsd/kibana-3.0.0milestone4/index.html#/dashboard/file/jnpr2.json

s of '/var/run/td-agent': Read-only file system

Term	Count	Action
analyticsd.jnpr	2015318	
Missing field	0	
Other values	0	

▸ View | Zoom Out | ● (2016853) latency mean per 1y | (2016853 hits)

▸ View | Zoom Out | ● (2015318) latency max per 1m | (2015318 hits)

0 to 100 of 500 available for paging

Firefox
The Core Intranet Home Page: Junipe...
Kibana 3
Most Visited
Getting Started
CLIE
Web Slice Gallery
GNATS
Cross Reference: /DEV...
Juniper Basic Dashboard
Set a time filter refreshed every 5s
QUERY
FILTERING
PORT FREQUENCY
TERMS
TR3613420027~xe-0/0/8 (118650)
TR3613420027~et-0/0/53 (118645)
TR3613420027~et-0/0/50 (118644)
TR3613420027~xe-0/0/10 (118642)
TR3613420027~xe-0/0/6 (118641)
TR3613420027~xe-0/0/5 (118640)
TR3613420027~xe-0/0/3 (118640)
TR3613420027~et-0/0/48 (118640)
TR3613420027~xe-0/0/4 (118639)
TR3613420027~xe-0/0/2 (118638)
TR3613420027~et-0/0/51 (118638)
TR3613420027~xe-0/0/9 (118637)
TR3613420027~xe-0/0/11 (118637)
TR3613420027~et-0/0/52 (118636)
TR3613420027~xe-0/0/1 (118630)
TR3613420027~et-0/0/49 (118630)
TR3613420027~xe-0/0/7 (118626)
Missing field (0)
Other values (0)
125000
100000
75000
50000
25000
0
HOSTNAME FREQUENCY
TERMS
Missing field
100%
LATENCY MEAN OVER TIME
HISTOGRAM
70000
60000
50000
40000
30000
20000
10000
0
03/14
05/14
07/14
LATENCY MAX OVER TIME
HISTOGRAM
350000
300000
250000
200000
150000
100000
50000
0
18:20 03/11
18:30 03/11
18:40 03/11
18:50 03/11
DOCUMENT TAGS
TERMS
DOCUMENTS
TABLE
Fields
Desktop
1:10 AM
3/15/2014

Figure 1. Sample Output from Kibana

For additional sample output, see Appendix B – Additional Sample Output.

Additional details on Kibana can be found at:

- http://www.elasticsearch.org/overview/kibana/
- https://github.com/elasticsearch/kibana

4 Appendix A – Code Samples

Contents of td-agent.conf

```
####

## Output descriptions:

##

<source>

  type monitor_agent

  bind 0.0.0.0

  port 24220

</source>

<match td.*.*>

  type tdlog

  apikey YOUR_API_KEY


  auto_create_table

  buffer_type file

  buffer_path /var/log/td-agent/buffer/td

</match>


<match debug.**>

  type file

  path /var/log/fluentd/debug

  flush_interval 1s

</match>


####

## Source descriptions:
```

```
##

<source>
  type AnalyticsD
  port 24224
  bind 0.0.0.0
</source>
<match analyticsD.jnpr>
  type elasticsearch
  logstash_format true
  include_tag_key true
  tag_key _jnpr
  flush_interval 1s
</match>

<source>
  type http
  port 8888
  bind 0.0.0.0
</source>
<match curl.test>
  type elasticsearch
  logstash_format true
  include_tag_key true
  flush_interval 1s
</match>

<source>
```

```
  type debug_agent

  bind 127.0.0.1

  port 24230

</source>
```

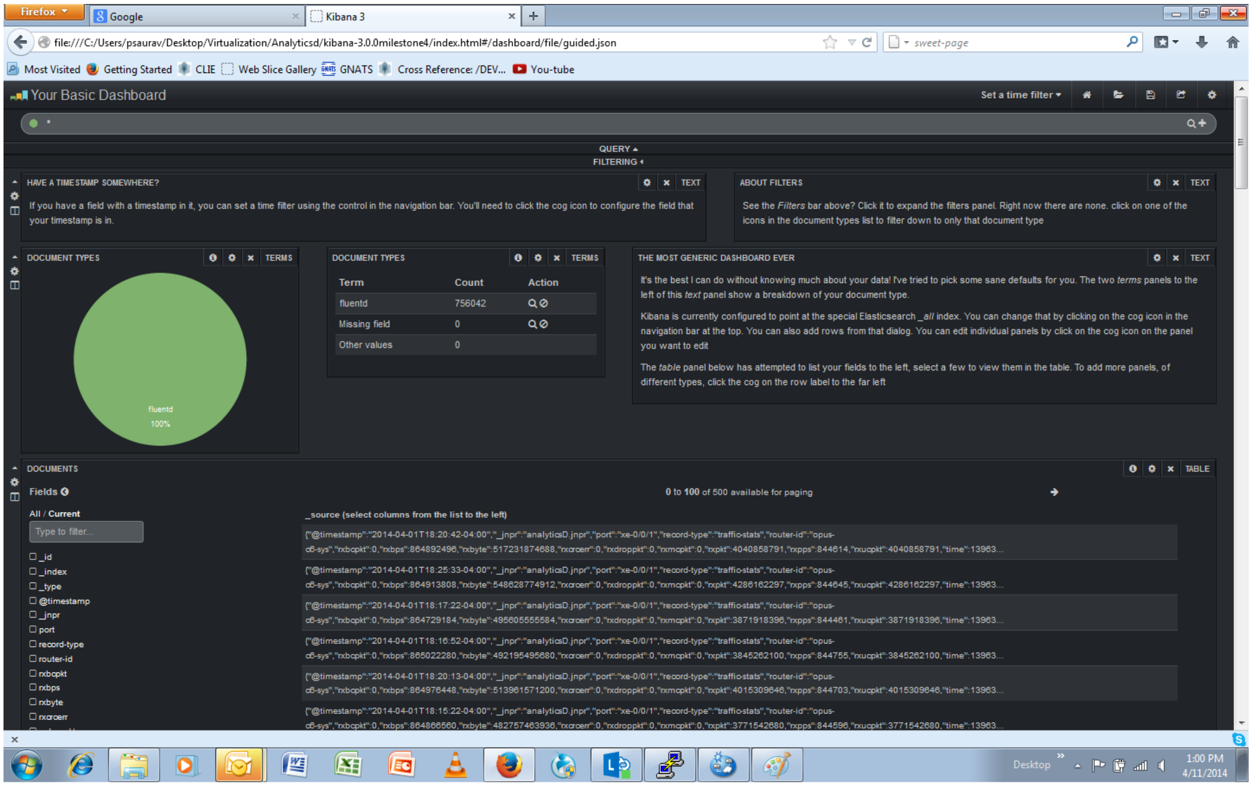
Contents of default-mapping.json

```
{

  "_default_" : {

    "properties" : {

        "port" : { "type":"string","index":"not_analyzed"},

        "hostname" : { "type":"string","index":"not_analyzed"},

        "router-id" : { "type":"string","index":"not_analyzed"},

        "queue-depth" : { "type":"string","index":"not_analyzed"},

        "record-type" : { "type":"string","index":"not_analyzed"},

        "zhtpt" : { "type":"string","index":"not_analyzed"}

    }

  }

}
```

Contents of fluent-plugin-AnalyticsD-0.1.0.gemspec

```
Gem::Specification.new do |gem|

  gem.name        = 'fluent-plugin-AnalyticsD'

  gem.version     = '0.1.0'

  gem.date        = '2014-01-08'

  gem.summary     = "JNPR!"

  gem.description = "Fluentd Input Plugin for JNPR Devices"

  gem.authors     = ["Jay A. Wilson"]

  gem.email       = 'jayw@juniper.net'

  gem.files       = ["lib/fluent/plugin/in_AnalyticsD.rb"]
  gem.require_paths = ["lib"]
  gem.has_rdoc    = false


  gem.required_ruby_version = '>= 1.9.2'


  gem.add_dependency "fluentd", "~> 0.10.7"
end
```

5 Appendix B – Additional Sample Output



HAVE A TIMESTAMP SOMEWHERE?

If you have a field with a timestamp in it, you can set a time filter using the control in the navigation bar. You'll need to click the cog icon to configure the field that your timestamp is in.

ABOUT FILTERS

See the *Filters* bar above? Click it to expand the filters panel. Right now there are none. click on one of the icons in the document types list to filter down to only that document type

DOCUMENT TYPES

DOCUMENT TYPES

Term	Count	Action
fluentd	756042	🔍 ⊘
Missing field	0	🔍 ⊘
Other values	0	

THE MOST GENERIC DASHBOARD EVER

It's the best I can do without knowing much about your data! I've tried to pick some sane defaults for you. The two *terms* panels to the left of this *text* panel show a breakdown of your document type.

Kibana is currently configured to point at the special Elasticsearch *_all* index. You can change that by clicking on the cog icon in the navigation bar at the top. You can also add rows from that dialog. You can edit individual panels by click on the cog icon on the panel you want to edit

The *table* panel below has attempted to list your fields to the left, select a few to view them in the table. To add more panels, of different types, click the cog on the row label to the far left

DOCUMENTS

Fields

0 to 100 of 500 available for paging

All / Current

Type to filter...

- ☐ _id
- ☐ _index
- ☐ _type
- ☐ @timestamp
- ☐ _jnpr
- ☐ port
- ☐ record-type
- ☐ router-id
- ☐ rxbcpkt
- ☐ rxbps
- ☐ rxbyte
- ☐ rxcrcerr

_source (select columns from the list to the left)

```
{"@timestamp":"2014-04-01T18:20:42-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":864892496,"rxbyte":517231874688,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4040858791,"rxpps":844614,"rxucpkt":4040858791,"time":13963...
{"@timestamp":"2014-04-01T18:25:33-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":864913808,"rxbyte":548628774912,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4286162297,"rxpps":844645,"rxucpkt":4286162297,"time":13963...
{"@timestamp":"2014-04-01T18:17:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":864729184,"rxbyte":495605555584,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3871918396,"rxpps":844461,"rxucpkt":3871918396,"time":13963...
{"@timestamp":"2014-04-01T18:16:52-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":865022280,"rxbyte":492195495680,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3845262100,"rxpps":844755,"rxucpkt":3845262100,"time":13963...
{"@timestamp":"2014-04-01T18:20:13-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":864976448,"rxbyte":513961571200,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4015309646,"rxpps":844703,"rxucpkt":4015309646,"time":13963...
{"@timestamp":"2014-04-01T18:15:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c8-sys","rxbcpkt":0,"rxbps":864866560,"rxbyte":482757463936,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3771542680,"rxpps":844596,"rxucpkt":3771542680,"time":13963...
```

Figure 2. Basic Kibana Dashboard (guided.json)

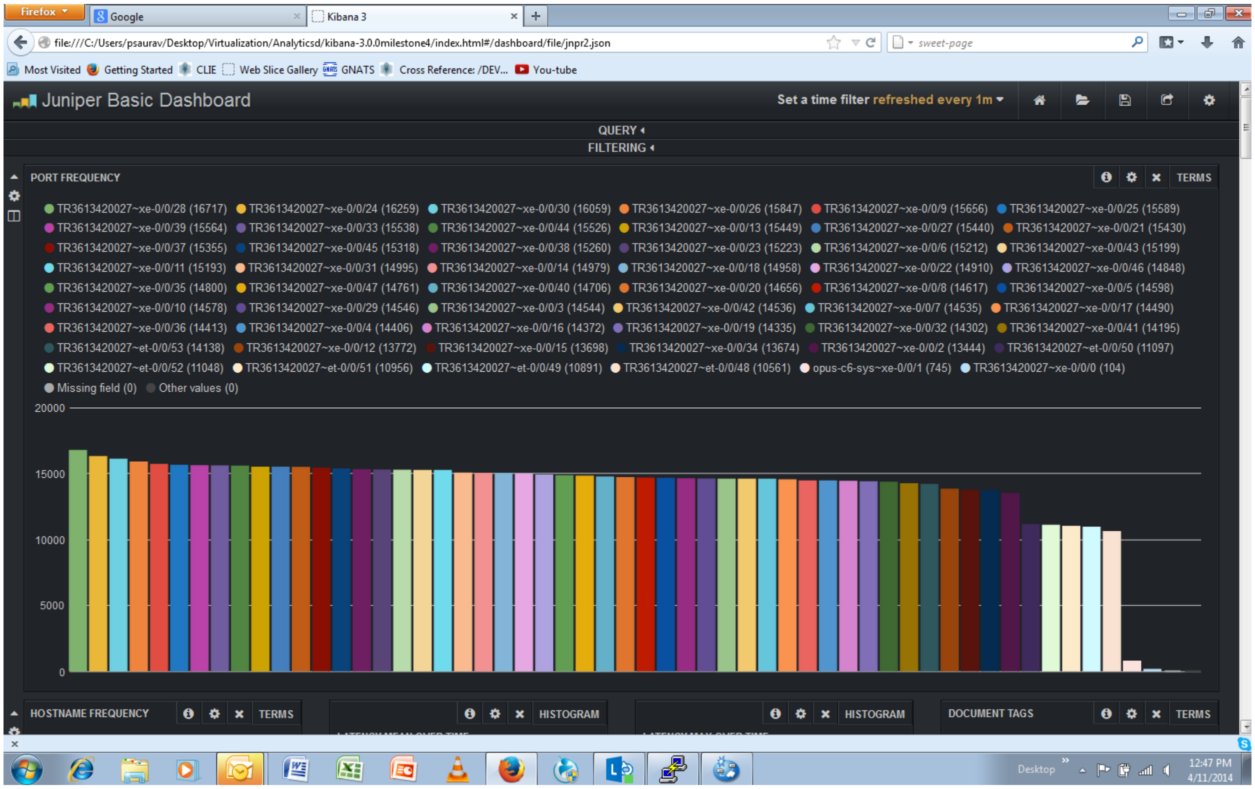

Juniper Basic Dashboard
Set a time filter refreshed every 1m
QUERY
FILTERING
PORT FREQUENCY
TERMS
TR3613420027~xe-0/0/28 (16717)
TR3613420027~xe-0/0/24 (16259)
TR3613420027~xe-0/0/30 (16059)
TR3613420027~xe-0/0/26 (15847)
TR3613420027~xe-0/0/9 (15656)
TR3613420027~xe-0/0/25 (15589)
TR3613420027~xe-0/0/39 (15564)
TR3613420027~xe-0/0/33 (15538)
TR3613420027~xe-0/0/44 (15526)
TR3613420027~xe-0/0/13 (15449)
TR3613420027~xe-0/0/27 (15440)
TR3613420027~xe-0/0/21 (15430)
TR3613420027~xe-0/0/37 (15355)
TR3613420027~xe-0/0/45 (15318)
TR3613420027~xe-0/0/38 (15260)
TR3613420027~xe-0/0/23 (15223)
TR3613420027~xe-0/0/6 (15212)
TR3613420027~xe-0/0/43 (15199)
TR3613420027~xe-0/0/11 (15193)
TR3613420027~xe-0/0/31 (14995)
TR3613420027~xe-0/0/14 (14979)
TR3613420027~xe-0/0/18 (14958)
TR3613420027~xe-0/0/22 (14910)
TR3613420027~xe-0/0/46 (14848)
TR3613420027~xe-0/0/35 (14800)
TR3613420027~xe-0/0/47 (14761)
TR3613420027~xe-0/0/40 (14706)
TR3613420027~xe-0/0/20 (14656)
TR3613420027~xe-0/0/8 (14617)
TR3613420027~xe-0/0/5 (14598)
TR3613420027~xe-0/0/10 (14578)
TR3613420027~xe-0/0/29 (14546)
TR3613420027~xe-0/0/3 (14544)
TR3613420027~xe-0/0/42 (14536)
TR3613420027~xe-0/0/7 (14535)
TR3613420027~xe-0/0/17 (14490)
TR3613420027~xe-0/0/36 (14413)
TR3613420027~xe-0/0/4 (14406)
TR3613420027~xe-0/0/16 (14372)
TR3613420027~xe-0/0/19 (14335)
TR3613420027~xe-0/0/32 (14302)
TR3613420027~xe-0/0/41 (14195)
TR3613420027~et-0/0/53 (14138)
TR3613420027~xe-0/0/12 (13772)
TR3613420027~xe-0/0/15 (13698)
TR3613420027~xe-0/0/34 (13674)
TR3613420027~xe-0/0/2 (13444)
TR3613420027~et-0/0/50 (11097)
TR3613420027~et-0/0/52 (11048)
TR3613420027~et-0/0/51 (10956)
TR3613420027~et-0/0/49 (10891)
TR3613420027~et-0/0/48 (10561)
opus-c6-sys~xe-0/0/1 (745)
TR3613420027~xe-0/0/0 (104)
Missing field (0)
Other values (0)
20000
15000
10000
5000
0
HOSTNAME FREQUENCY
TERMS
HISTOGRAM
HISTOGRAM
DOCUMENT TAGS
TERMS

Figure 3. Statistics for Various Ports

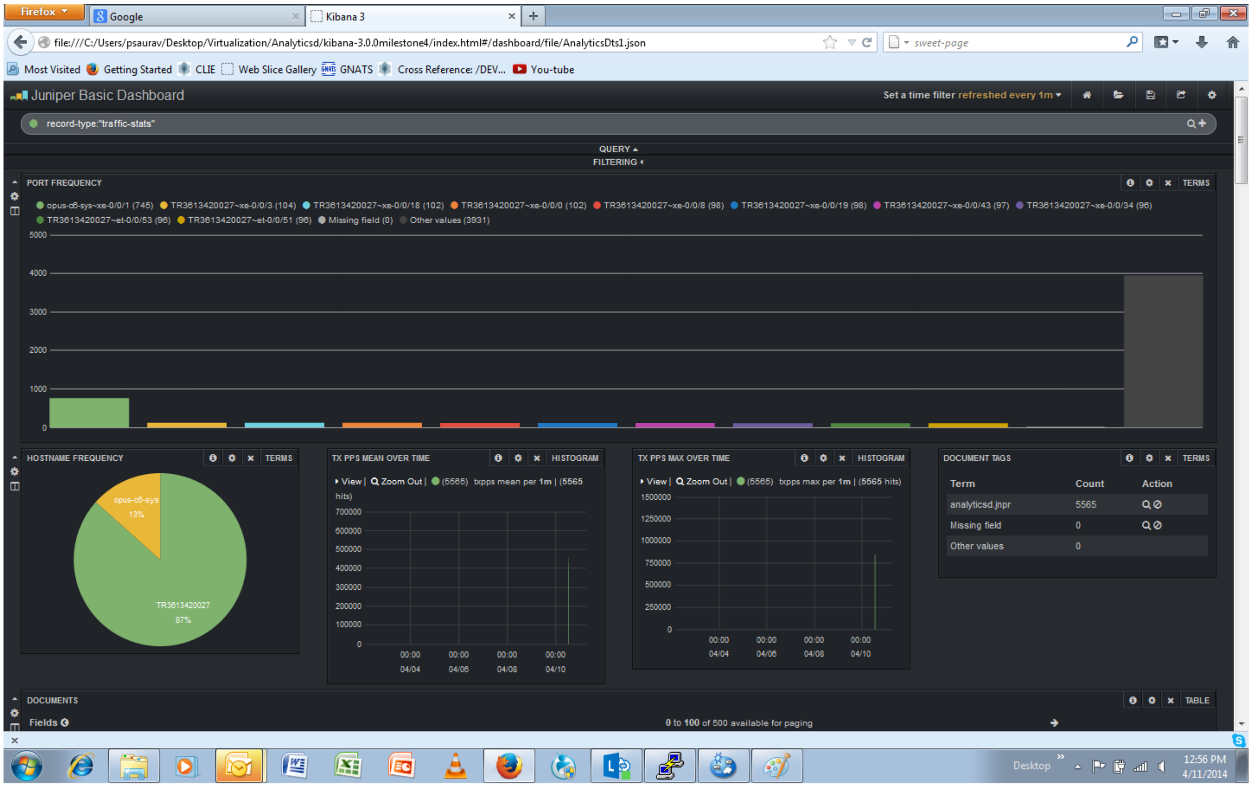

Juniper Basic Dashboard
record-type:"traffic-stats"
QUERY
FILTERING
PORT FREQUENCY
opus-c6-sys~xe-0/0/1 (745) TR3613420027~xe-0/0/3 (104) TR3613420027~xe-0/0/18 (102) TR3613420027~xe-0/0/0 (102) TR3613420027~xe-0/0/8 (98) TR3613420027~xe-0/0/19 (98) TR3613420027~xe-0/0/43 (97) TR3613420027~xe-0/0/34 (96) TR3613420027~et-0/0/53 (96) TR3613420027~et-0/0/51 (96) Missing field (0) Other values (3931)
HOSTNAME FREQUENCY
opus-c6-sys 13%
TR3613420027 87%
TX PPS MEAN OVER TIME
TX PPS MAX OVER TIME
DOCUMENT TAGS
Term Count Action
analyticsd.jnpr 5565
Missing field 0
Other values 0
DOCUMENTS
0 to 100 of 500 available for paging

Figure 4. Hostname Frequency and Tx pps Mean/Max Over Time

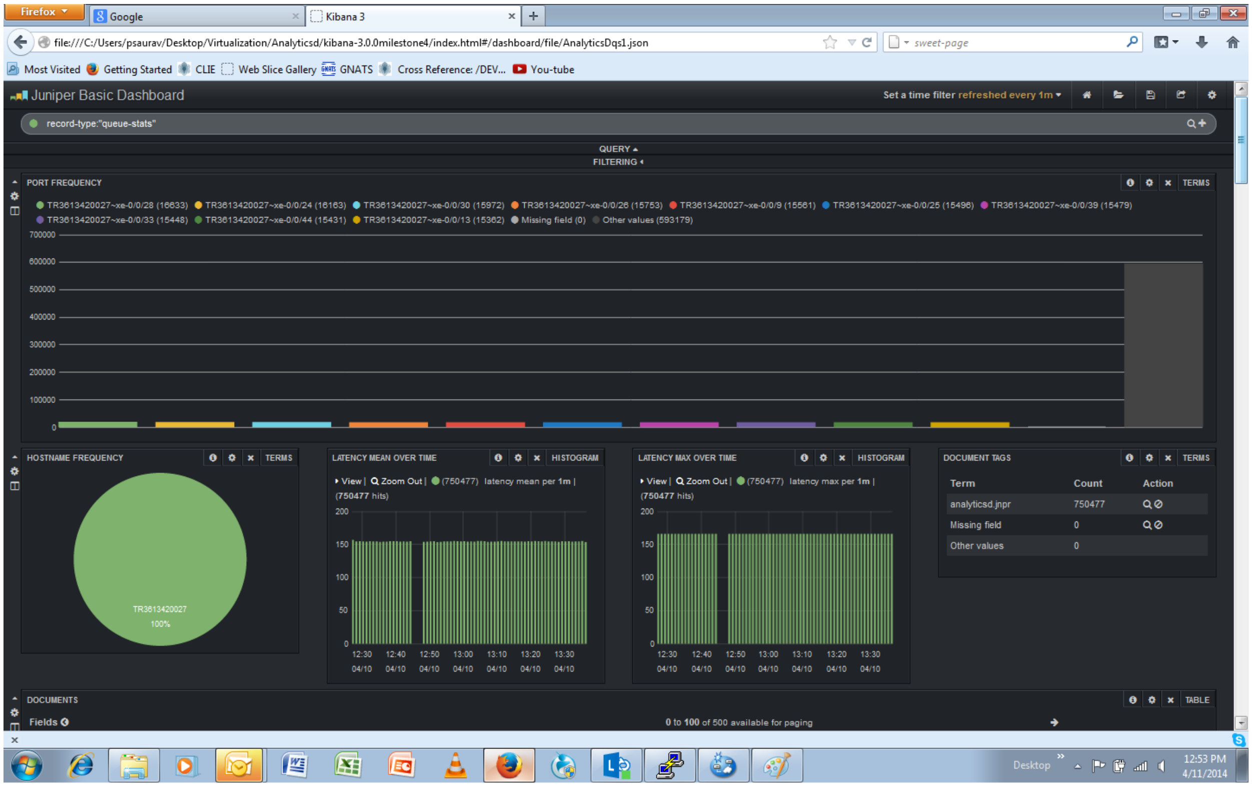
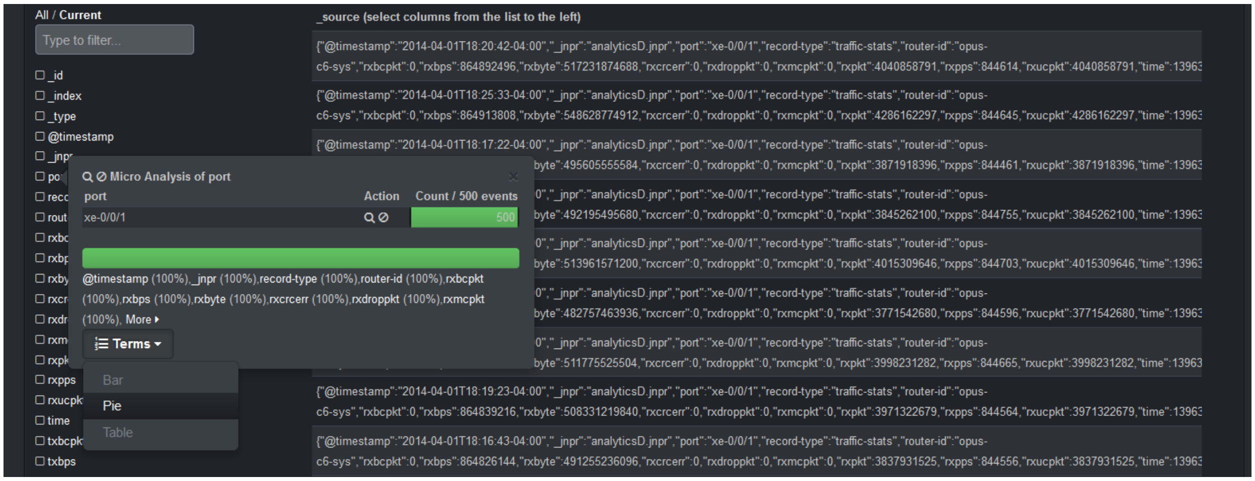

Juniper Basic Dashboard
record-type:"queue-stats"
QUERY
FILTERING
PORT FREQUENCY
TR3613420027~xe-0/0/28 (16633) TR3613420027~xe-0/0/24 (16163) TR3613420027~xe-0/0/30 (15972) TR3613420027~xe-0/0/26 (15753) TR3613420027~xe-0/0/9 (15561) TR3613420027~xe-0/0/25 (15496) TR3613420027~xe-0/0/39 (15479) TR3613420027~xe-0/0/33 (15448) TR3613420027~xe-0/0/44 (15431) TR3613420027~xe-0/0/13 (15362) Missing field (0) Other values (593179)
HOSTNAME FREQUENCY
TR3613420027 100%
LATENCY MEAN OVER TIME
LATENCY MAX OVER TIME
DOCUMENT TAGS
Term Count Action
analyticsd.jnpr 750477
Missing field 0
Other values 0
DOCUMENTS
0 to 100 of 500 available for paging

Figure 5. Latency Mean/Max Over Time



_source (select columns from the list to the left)

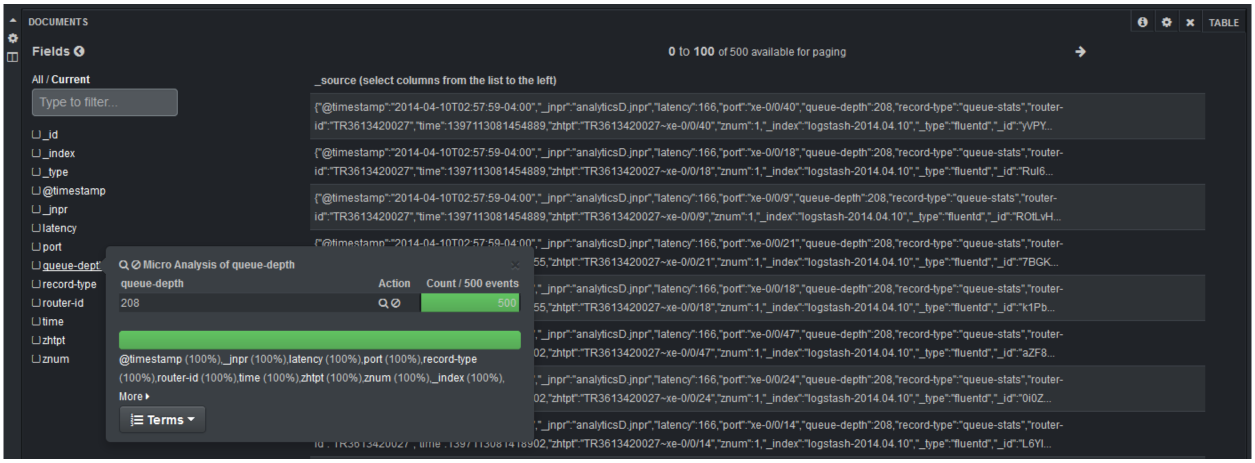
```
{"@timestamp":"2014-04-01T18:20:42-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864892496,"rxbyte":517231874688,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4040858791,"rxpps":844614,"rxucpkt":4040858791,"time":13963
{"@timestamp":"2014-04-01T18:25:33-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864913808,"rxbyte":548628774912,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4286162297,"rxpps":844645,"rxucpkt":4286162297,"time":13963
{"@timestamp":"2014-04-01T18:17:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
byte":495605555584,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3871918396,"rxpps":844461,"rxucpkt":3871918396,"time":13963
0","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
byte":492195495680,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3845262100,"rxpps":844755,"rxucpkt":3845262100,"time":13963
0","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
byte":513961571200,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4015309646,"rxpps":844703,"rxucpkt":4015309646,"time":13963
0","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
byte":482757463936,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3771542680,"rxpps":844596,"rxucpkt":3771542680,"time":13963
0","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
byte":511775525504,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3998231282,"rxpps":844665,"rxucpkt":3998231282,"time":13963
{"@timestamp":"2014-04-01T18:19:23-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864839216,"rxbyte":508331219840,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3971322679,"rxpps":844564,"rxucpkt":3971322679,"time":13963
{"@timestamp":"2014-04-01T18:16:43-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864826144,"rxbyte":491255236096,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3837931525,"rxpps":844556,"rxucpkt":3837931525,"time":13963
```

Micro Analysis of port

port	Action	Count / 500 events
xe-0/0/1		500

@timestamp (100%),_jnpr (100%),record-type (100%),router-id (100%),rxbcpkt (100%),rxbps (100%),rxbyte (100%),rxcrcerr (100%),rxdroppkt (100%),rxmcpkt (100%), More

Figure 6. Micro Analysis of a Given Port



0 to 100 of 500 available for paging

_source (select columns from the list to the left)

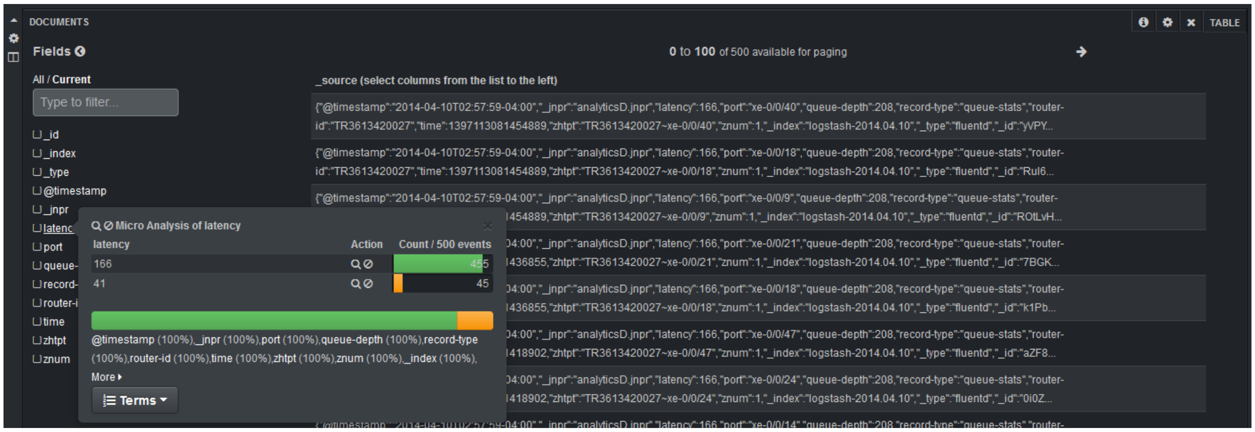
```
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/40","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/40","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"yVPY...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"Rul6...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/9","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/9","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"ROtLvH...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/21","queue-depth":208,"record-type":"queue-stats","router-
55,"zhtpt":"TR3613420027~xe-0/0/21","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"7BGK...
","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
55,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"k1Pb...
","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/47","queue-depth":208,"record-type":"queue-stats","router-
02,"zhtpt":"TR3613420027~xe-0/0/47","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"aZF8...
","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/24","queue-depth":208,"record-type":"queue-stats","router-
02,"zhtpt":"TR3613420027~xe-0/0/24","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"0i0Z...
","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/14","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081418902,"zhtpt":"TR3613420027~xe-0/0/14","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"L6Yl...
```

Micro Analysis of queue-depth

queue-depth	Action	Count / 500 events
208		500

@timestamp (100%),_jnpr (100%),latency (100%),port (100%),record-type (100%),router-id (100%),time (100%),zhtpt (100%),znum (100%),_index (100%), More

Figure 7. Micro Analysis of Queue Depth



0 to 100 of 500 available for paging

_source (select columns from the list to the left)

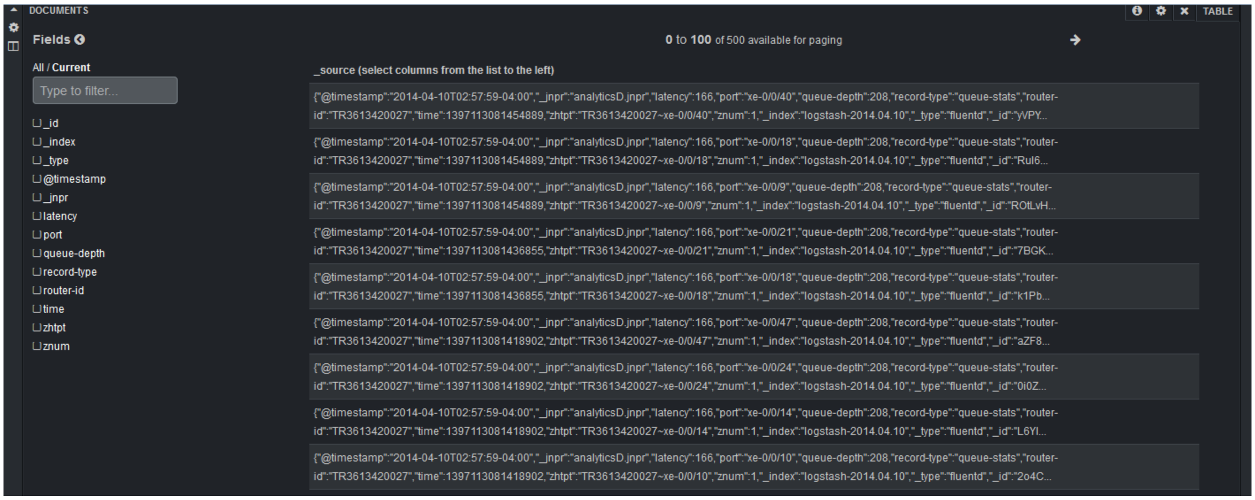
```
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/40","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/40","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"yVPY...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"Rul6...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/9","queue-depth":208,"record-type":"queue-stats","router-
1454889,"zhtpt":"TR3613420027~xe-0/0/9","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"ROtLvH...
04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/21","queue-depth":208,"record-type":"queue-stats","router-
1436855,"zhtpt":"TR3613420027~xe-0/0/21","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"7BGK...
04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
1436855,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"k1Pb...
04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/47","queue-depth":208,"record-type":"queue-stats","router-
1418902,"zhtpt":"TR3613420027~xe-0/0/47","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"aZF8...
04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/24","queue-depth":208,"record-type":"queue-stats","router-
1418902,"zhtpt":"TR3613420027~xe-0/0/24","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"0i0Z...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/14","queue-depth":208,"record-type":"queue-stats","router-
```

Micro Analysis of latency

latency	Action	Count / 500 events
166		455
41		45

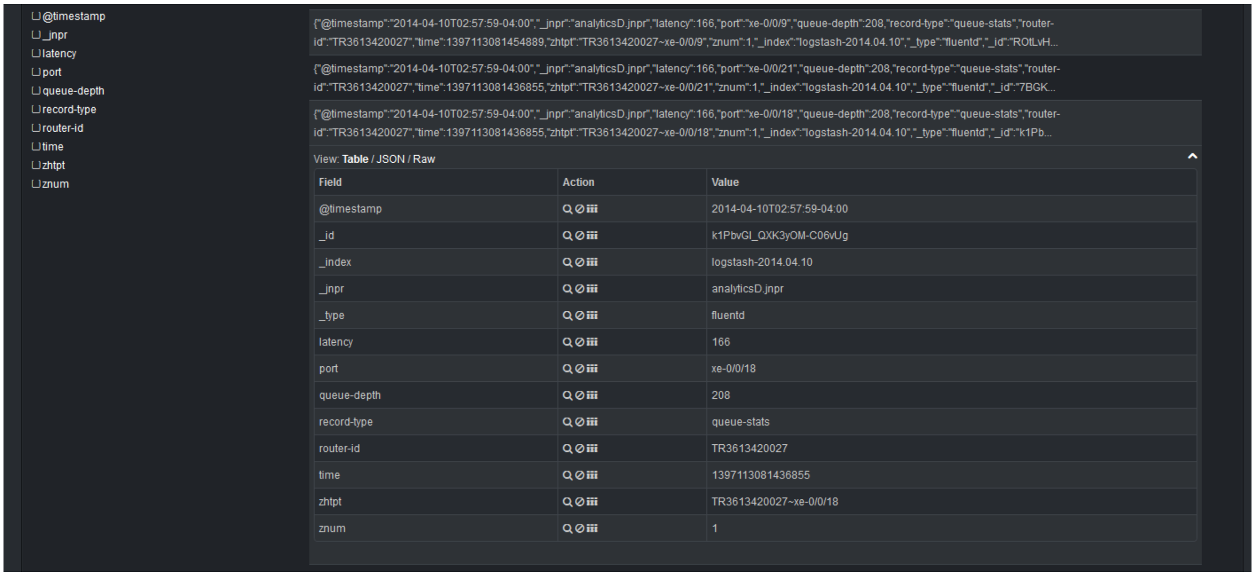
@timestamp (100%),_jnpr (100%),port (100%),queue-depth (100%),record-type (100%),router-id (100%),time (100%),zhtpt (100%),znum (100%),_index (100%), More

Figure 8. Micro Analysis of Latency



```
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/40","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/40","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"yVPY...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"Rul6...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/9","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/9","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"ROtLvH...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/21","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081436855,"zhtpt":"TR3613420027~xe-0/0/21","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"7BGK...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081436855,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"k1Pb...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/47","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081418902,"zhtpt":"TR3613420027~xe-0/0/47","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"aZF8...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/24","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081418902,"zhtpt":"TR3613420027~xe-0/0/24","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"0i0Z...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/14","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081418902,"zhtpt":"TR3613420027~xe-0/0/14","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"L6Yl...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/10","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081418902,"zhtpt":"TR3613420027~xe-0/0/10","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"2o4C...
```

Figure 9. Queue Records



```
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/9","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081454889,"zhtpt":"TR3613420027~xe-0/0/9","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"ROtLvH...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/21","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081436855,"zhtpt":"TR3613420027~xe-0/0/21","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"7BGK...
{"@timestamp":"2014-04-10T02:57:59-04:00","_jnpr":"analyticsD.jnpr","latency":166,"port":"xe-0/0/18","queue-depth":208,"record-type":"queue-stats","router-
id":"TR3613420027","time":1397113081436855,"zhtpt":"TR3613420027~xe-0/0/18","znum":1,"_index":"logstash-2014.04.10","_type":"fluentd","_id":"k1Pb...
```

Field	Action	Value
@timestamp	🔍⊘▥	2014-04-10T02:57:59-04:00
_id	🔍⊘▥	k1PbvGI_QXK3yOM-C06vUg
_index	🔍⊘▥	logstash-2014.04.10
_jnpr	🔍⊘▥	analyticsD.jnpr
_type	🔍⊘▥	fluentd
latency	🔍⊘▥	166
port	🔍⊘▥	xe-0/0/18
queue-depth	🔍⊘▥	208
record-type	🔍⊘▥	queue-stats
router-id	🔍⊘▥	TR3613420027
time	🔍⊘▥	1397113081436855
zhtpt	🔍⊘▥	TR3613420027~xe-0/0/18
znum	🔍⊘▥	1

Figure 10. Queue Record Expanded

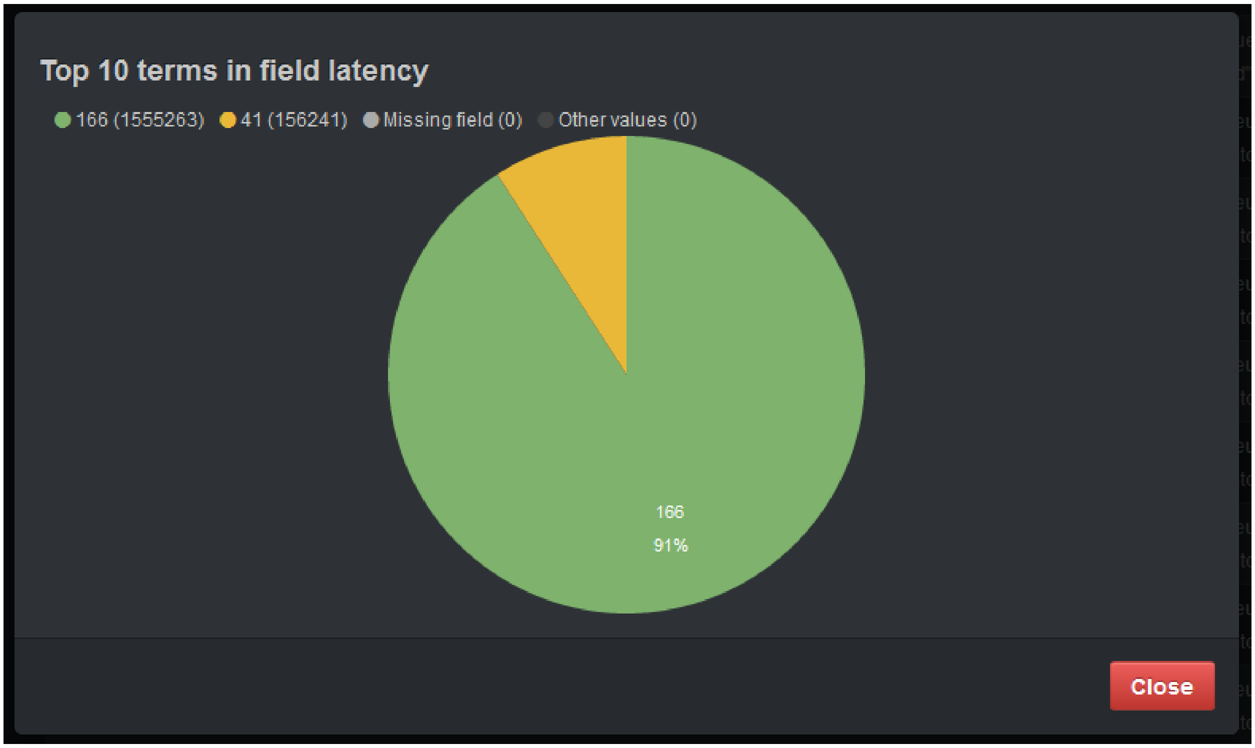
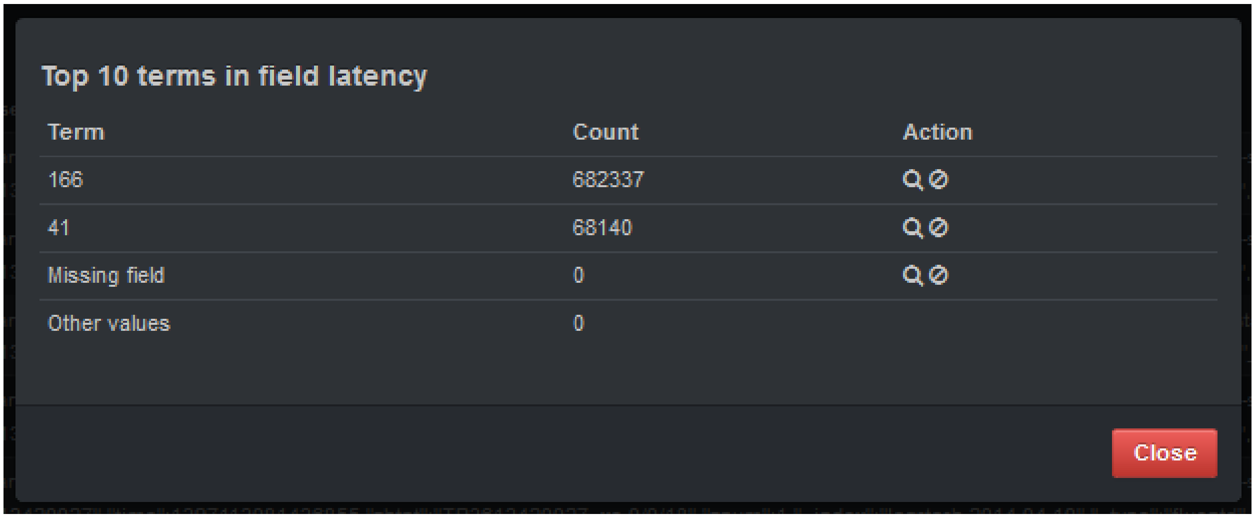


Figure 11. Top Ten Latency in a Pie Chart



Top 10 terms in field latency

Term	Count	Action
166	682337	🔍⊘
41	68140	🔍⊘
Missing field	0	🔍⊘
Other values	0	

Figure 12. Top Ten Latency in a Table

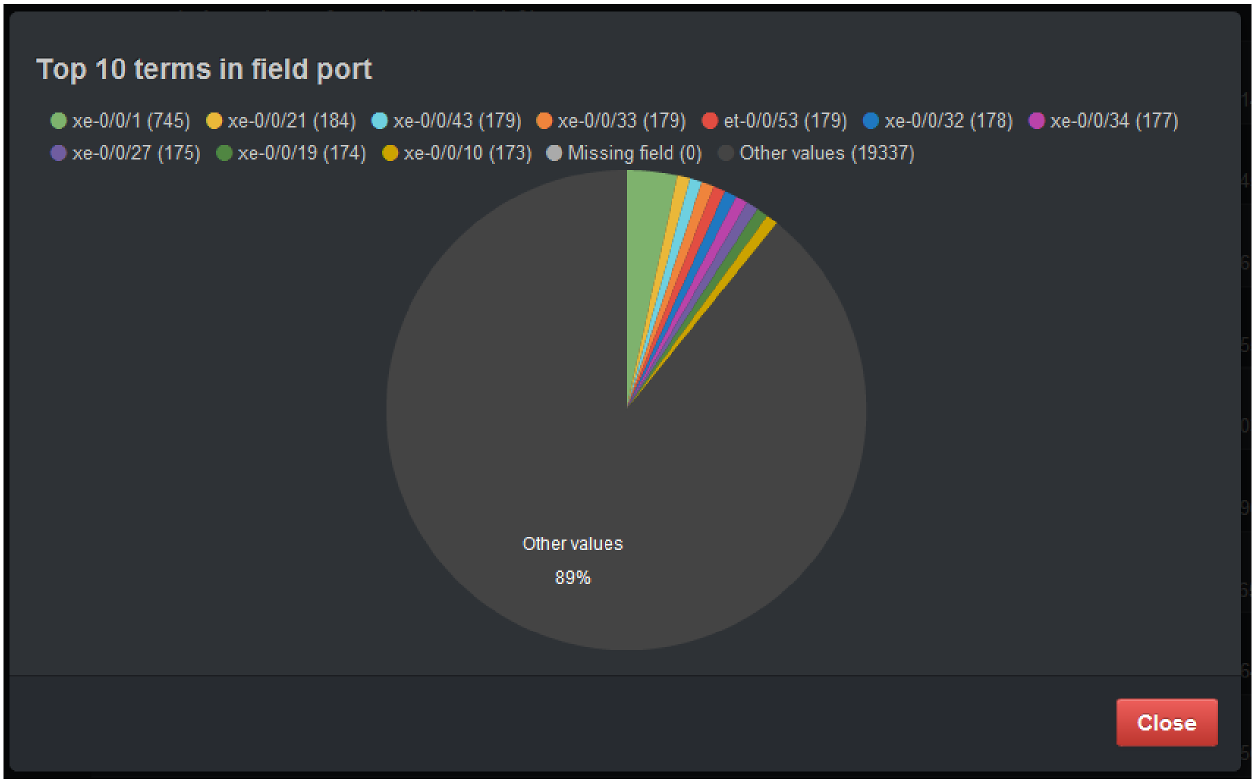
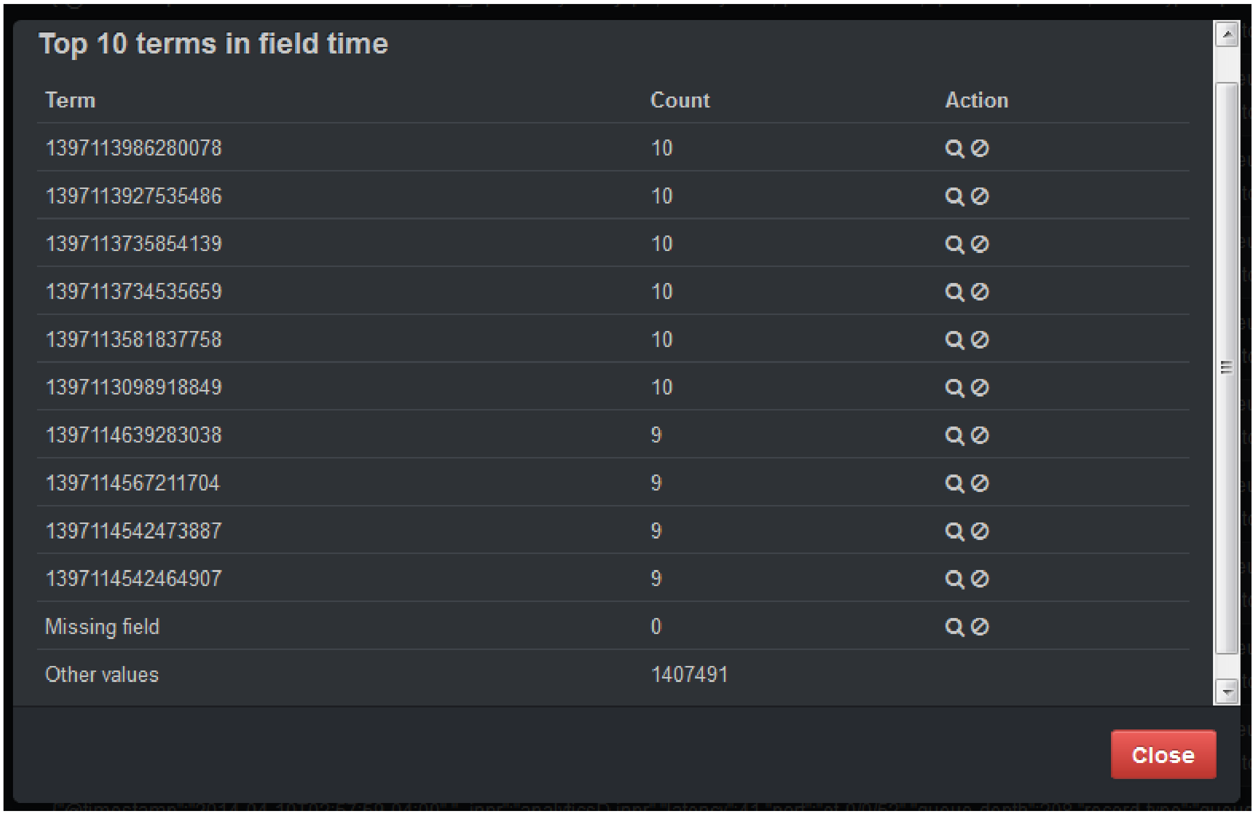


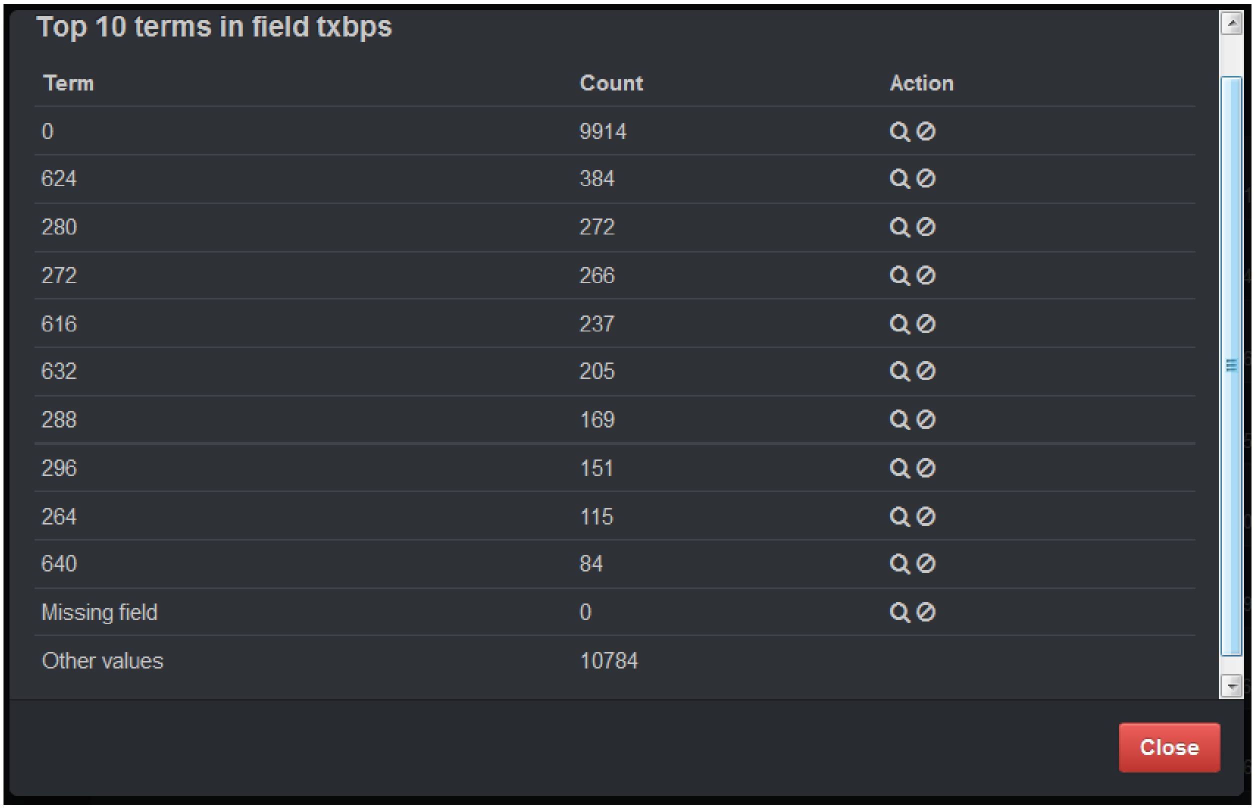
Figure 13. Top Ten Ports in a Pie Chart



Top 10 terms in field time

Term	Count	Action
1397113986280078	10	🔍 ⊘
1397113927535486	10	🔍 ⊘
1397113735854139	10	🔍 ⊘
1397113734535659	10	🔍 ⊘
1397113581837758	10	🔍 ⊘
1397113098918849	10	🔍 ⊘
1397114639283038	9	🔍 ⊘
1397114567211704	9	🔍 ⊘
1397114542473887	9	🔍 ⊘
1397114542464907	9	🔍 ⊘
Missing field	0	🔍 ⊘
Other values	1407491	

Figure 14. Top Ten Timestamps in a Table



Top 10 terms in field txbps

Term	Count	Action
0	9914	🔍 ⊘
624	384	🔍 ⊘
280	272	🔍 ⊘
272	266	🔍 ⊘
616	237	🔍 ⊘
632	205	🔍 ⊘
288	169	🔍 ⊘
296	151	🔍 ⊘
264	115	🔍 ⊘
640	84	🔍 ⊘
Missing field	0	🔍 ⊘
Other values	10784	

Figure 15. Top Ten Tx bps in a Table

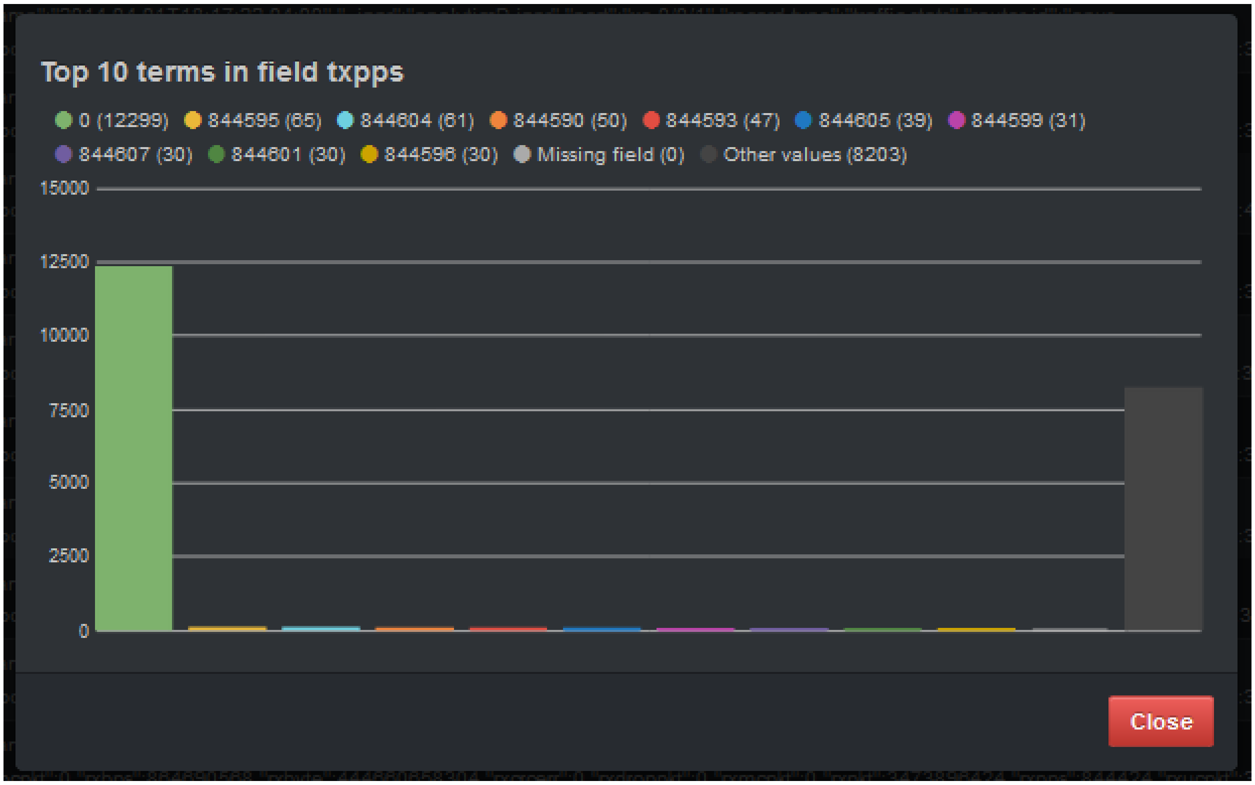


Figure 16. Top Ten Tx pps in a Bar Graph

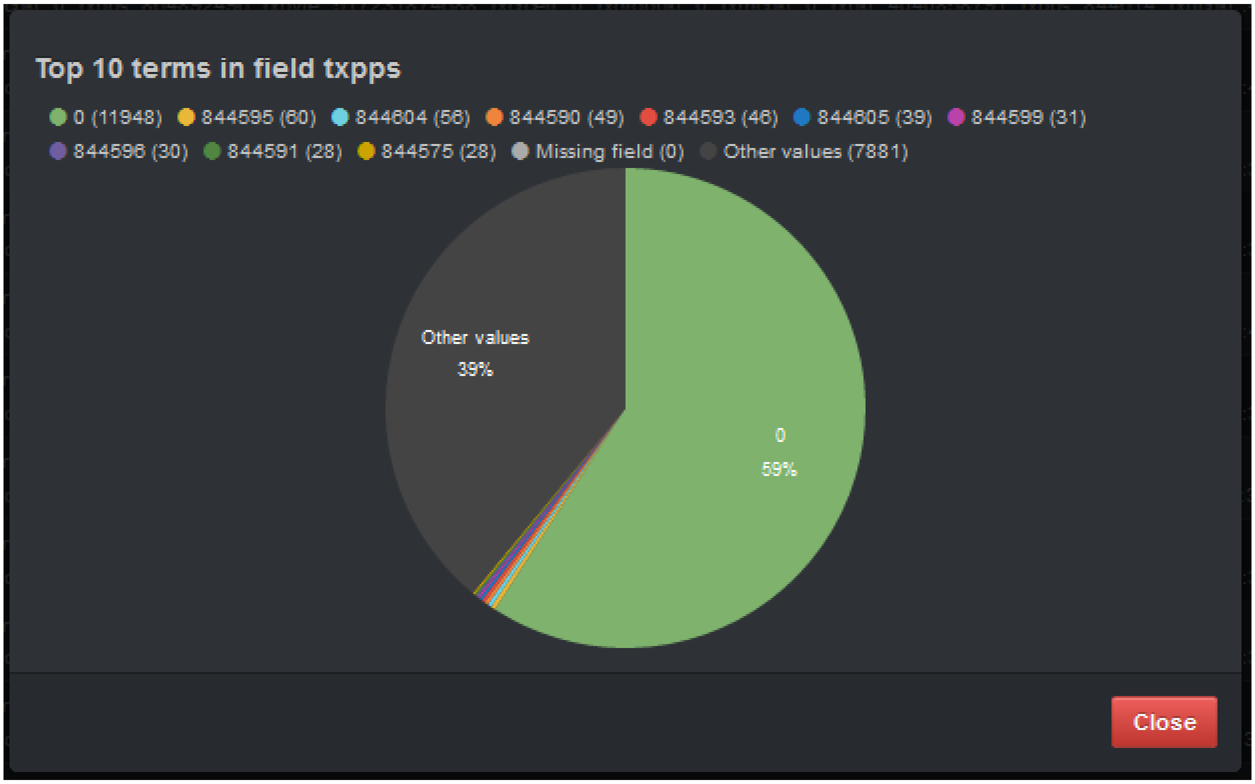
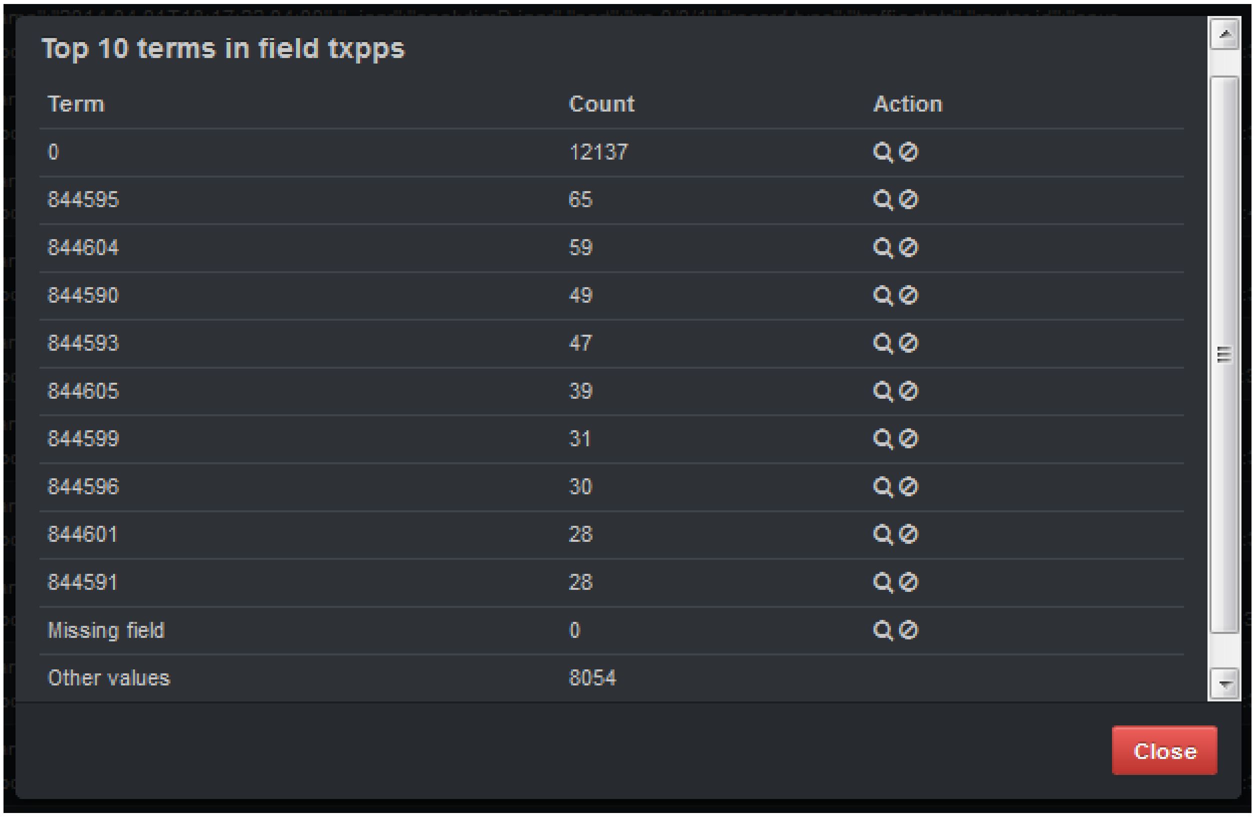


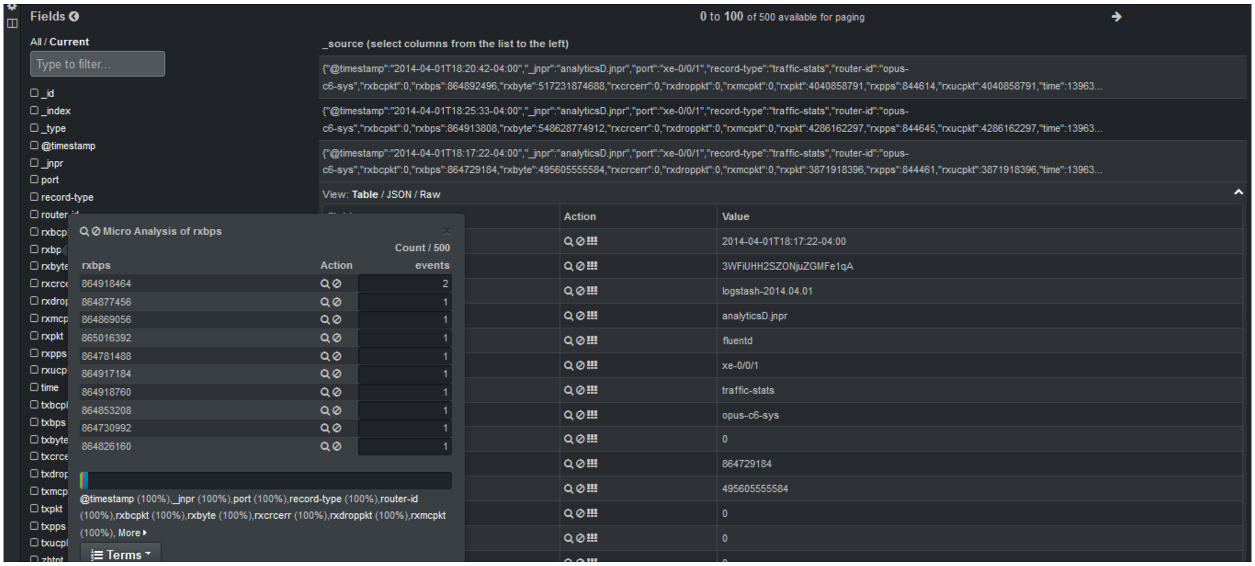
Figure 17. Top Ten Tx pps in a Pie Chart



Top 10 terms in field txpps

Term	Count	Action
0	12137	🔍 ⊘
844595	65	🔍 ⊘
844604	59	🔍 ⊘
844590	49	🔍 ⊘
844593	47	🔍 ⊘
844605	39	🔍 ⊘
844599	31	🔍 ⊘
844596	30	🔍 ⊘
844601	28	🔍 ⊘
844591	28	🔍 ⊘
Missing field	0	🔍 ⊘
Other values	8054	

Figure 18. Top Ten Tx pps in a Table



_source (select columns from the list to the left)

```
{"@timestamp":"2014-04-01T18:20:42-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864892496,"rxbyte":517231874688,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4040858791,"rxpps":844614,"rxucpkt":4040858791,"time":13963...
{"@timestamp":"2014-04-01T18:25:33-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864913808,"rxbyte":548628774912,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4286162297,"rxpps":844645,"rxucpkt":4286162297,"time":13963...
{"@timestamp":"2014-04-01T18:17:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864729184,"rxbyte":495605555584,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3871918396,"rxpps":844461,"rxucpkt":3871918396,"time":13963...
```

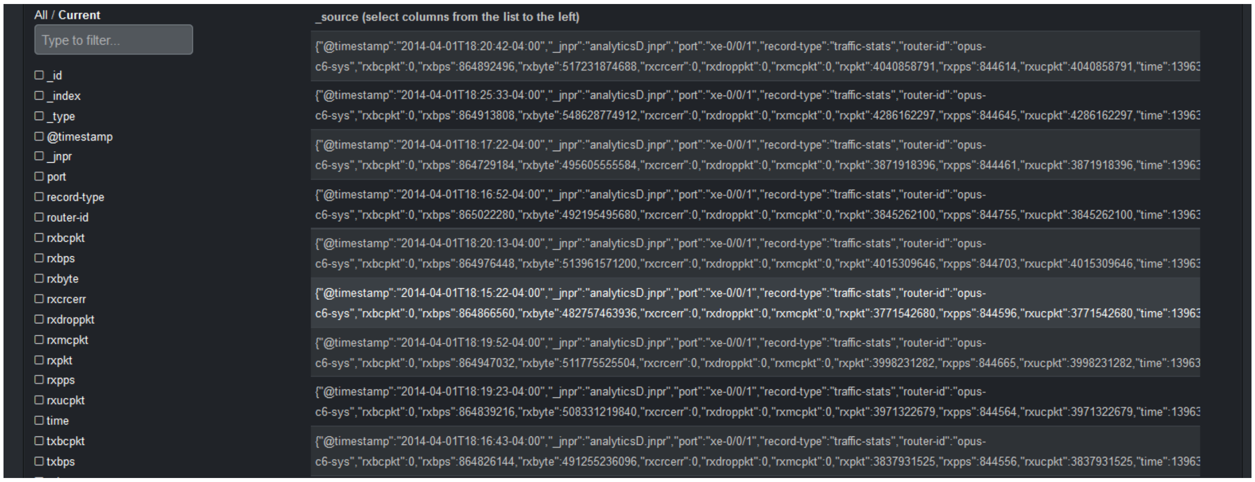
Action	Value
🔍 ⊘ ▦	2014-04-01T18:17:22-04:00
🔍 ⊘ ▦	3WFiUHH2SZONjuZGMFe1qA
🔍 ⊘ ▦	logstash-2014.04.01
🔍 ⊘ ▦	analyticsD.jnpr
🔍 ⊘ ▦	fluentd
🔍 ⊘ ▦	xe-0/0/1
🔍 ⊘ ▦	traffic-stats
🔍 ⊘ ▦	opus-c6-sys
🔍 ⊘ ▦	0
🔍 ⊘ ▦	864729184
🔍 ⊘ ▦	495605555584
🔍 ⊘ ▦	0
🔍 ⊘ ▦	0

🔍 ⊘ Micro Analysis of rxbps

rxbps	Action	Count / 500 events
864918464	🔍 ⊘	2
864877456	🔍 ⊘	1
864869056	🔍 ⊘	1
865016392	🔍 ⊘	1
864781488	🔍 ⊘	1
864917184	🔍 ⊘	1
864918760	🔍 ⊘	1
864853208	🔍 ⊘	1
864730992	🔍 ⊘	1
864826160	🔍 ⊘	1

@timestamp (100%),_jnpr (100%),port (100%),record-type (100%),router-id (100%),rxbcpkt (100%),rxbyte (100%),rxcrcerr (100%),rxdroppkt (100%),rxmcpkt (100%), More ▸

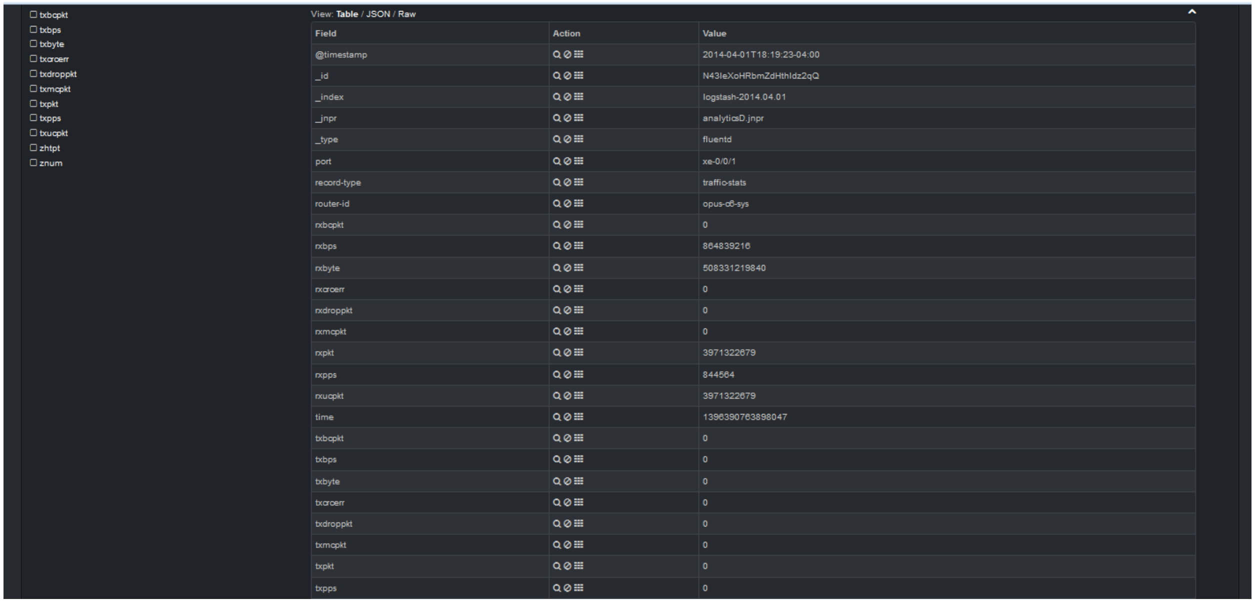
Figure 19. Micro Analysis of Rx bps



_source (select columns from the list to the left)

```
{"@timestamp":"2014-04-01T18:20:42-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864892496,"rxbyte":517231874688,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4040858791,"rxpps":844614,"rxucpkt":4040858791,"time":13963
{"@timestamp":"2014-04-01T18:25:33-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864913808,"rxbyte":548628774912,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4286162297,"rxpps":844645,"rxucpkt":4286162297,"time":13963
{"@timestamp":"2014-04-01T18:17:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864729184,"rxbyte":495605555584,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3871918396,"rxpps":844461,"rxucpkt":3871918396,"time":13963
{"@timestamp":"2014-04-01T18:16:52-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":865022280,"rxbyte":492195495680,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3845262100,"rxpps":844755,"rxucpkt":3845262100,"time":13963
{"@timestamp":"2014-04-01T18:20:13-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864976448,"rxbyte":513961571200,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":4015309646,"rxpps":844703,"rxucpkt":4015309646,"time":13963
{"@timestamp":"2014-04-01T18:15:22-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864866560,"rxbyte":482757463936,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3771542680,"rxpps":844596,"rxucpkt":3771542680,"time":13963
{"@timestamp":"2014-04-01T18:19:52-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864947032,"rxbyte":511775525504,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3998231282,"rxpps":844665,"rxucpkt":3998231282,"time":13963
{"@timestamp":"2014-04-01T18:19:23-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864839216,"rxbyte":508331219840,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3971322679,"rxpps":844564,"rxucpkt":3971322679,"time":13963
{"@timestamp":"2014-04-01T18:16:43-04:00","_jnpr":"analyticsD.jnpr","port":"xe-0/0/1","record-type":"traffic-stats","router-id":"opus-
c6-sys","rxbcpkt":0,"rxbps":864826144,"rxbyte":491255236096,"rxcrcerr":0,"rxdroppkt":0,"rxmcpkt":0,"rxpkt":3837931525,"rxpps":844556,"rxucpkt":3837931525,"time":13963
```

Figure 20. Traffic Records



☐ txbcpkt
☐ txbps
☐ txbyte
☐ txcrcerr
☐ txdroppkt
☐ txmcpkt
☐ txpkt
☐ txpps
☐ txucpkt
☐ zhtpt
☐ znum

View: **Table** / JSON / Raw

Field	Action	Value
@timestamp	🔍 ⊘ ▦	2014-04-01T18:19:23-04:00
_id	🔍 ⊘ ▦	N43IeXoHRbmZdHthIdz2qQ
_index	🔍 ⊘ ▦	logstash-2014.04.01
_jnpr	🔍 ⊘ ▦	analyticsD.jnpr
_type	🔍 ⊘ ▦	fluentd
port	🔍 ⊘ ▦	xe-0/0/1
record-type	🔍 ⊘ ▦	traffic-stats
router-id	🔍 ⊘ ▦	opus-c6-sys
rxbcpkt	🔍 ⊘ ▦	0
rxbps	🔍 ⊘ ▦	864839216
rxbyte	🔍 ⊘ ▦	508331219840
rxcrcerr	🔍 ⊘ ▦	0
rxdroppkt	🔍 ⊘ ▦	0
rxmcpkt	🔍 ⊘ ▦	0
rxpkt	🔍 ⊘ ▦	3971322679
rxpps	🔍 ⊘ ▦	844564
rxucpkt	🔍 ⊘ ▦	3971322679
time	🔍 ⊘ ▦	1396390763898047
txbcpkt	🔍 ⊘ ▦	0
txbps	🔍 ⊘ ▦	0
txbyte	🔍 ⊘ ▦	0
txcrcerr	🔍 ⊘ ▦	0
txdroppkt	🔍 ⊘ ▦	0
txmcpkt	🔍 ⊘ ▦	0
txpkt	🔍 ⊘ ▦	0
txpps	🔍 ⊘ ▦	0

Figure 21. Various Fields of a Traffic Record