Logstash - Tips and Troubleshooting

Tips

Key=Value

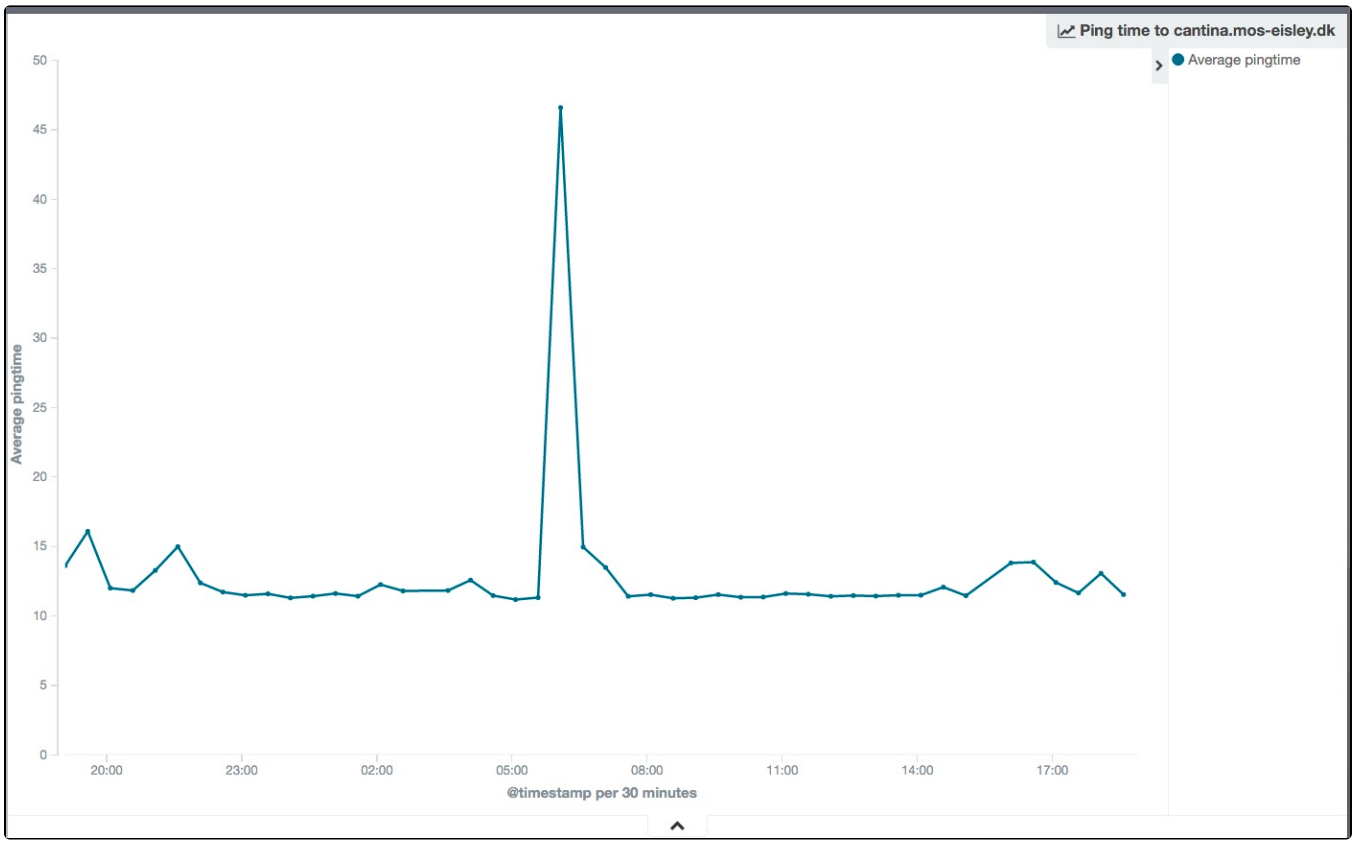
to get Key=Value out from and input, I use this in a filter:

```
.....
if [type] == "pinglog" {
        kv {}
        mutate {
          convert => { "pingtime" => "float" }
        }
      }
      else
      {
        if [type] == "syslog"
        {
          kv
          {
            include_keys => ["OUT","IN","SRC","SPT","DST","DPT","PROTO","ACTION"]
            trim => "<>\[\],"
            trimkey => "<>\[\],"
          }

.....
```

According to http://logz.io/blog/5-logstash-pitfalls-and-how-to-avoid-them/ there a danger in using "kv" without adding specific fields

As my "pingtime" is a value I want to visualize and use for an Y-Axis, it must be numeric - hence the mutate to a float:



Drop something

THis is how I drop part of the syslog (google DNS lookup) after it has been "kv" (:

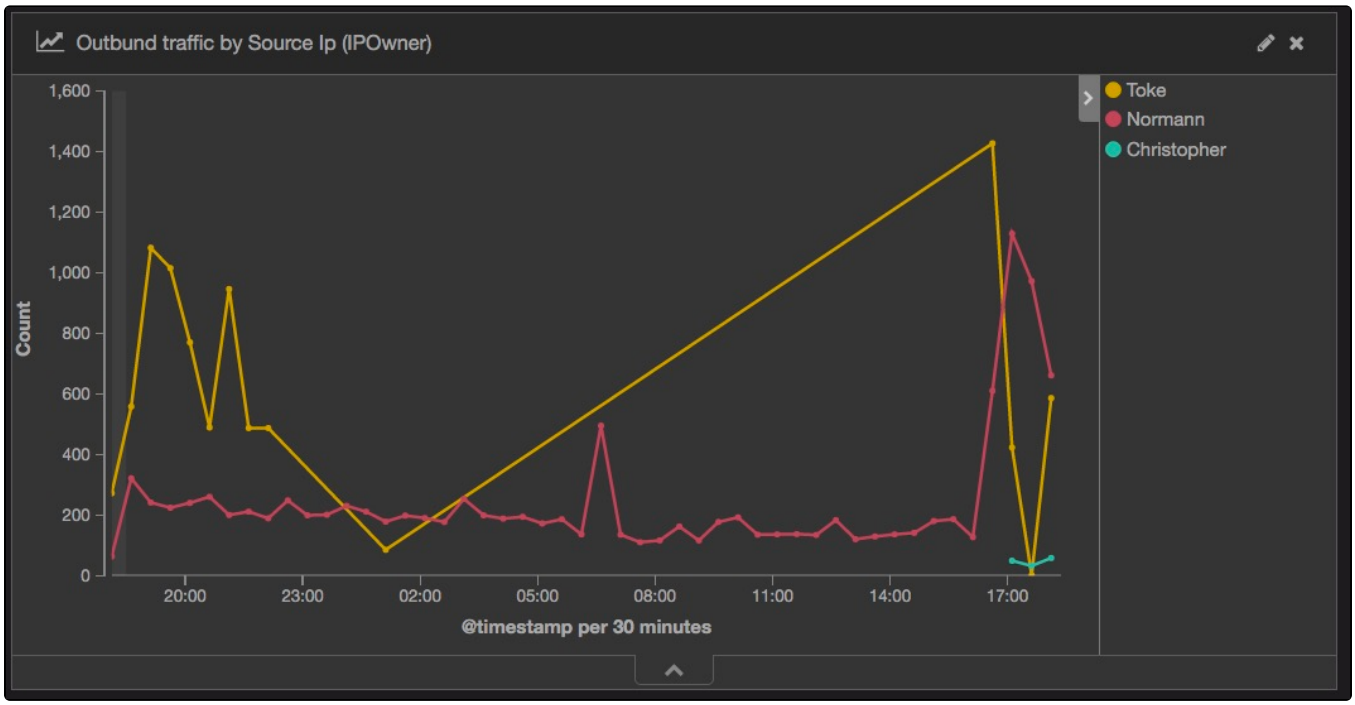
```
if [DST] == "8.8.8.8"
{
  drop {}
}
```

Adding fields/metadata

From the Router Syslog, I would like to add an owner and device of the Source (Identified by Source IP "SRC") - I have static IP's for the devices:

```
if [SRC] == "10.0.0.102" {
  mutate
  {
    add_field => { "IPOwner" => "Toke" "Device" => "iPad" }
  }
}
...
...
if [SRC] == "10.0.0.109" {
  mutate
  {
    add_field => { "IPOwner" => "Christopher" "Device" => "Laptop LAN" }
  }
}
```

These metadata give me a possibility to Visualize traffic by IPOwner:



Trobleshooting

Cant send data to Elasticsearch - Elasticsearch wont recieve

The /var/log/logstash/logstash.log shows:

```
{:timestamp=>"2016-04-08T08:32:32.217000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:32.721000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:33.232000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:33.733000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:34.282000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:34.783000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
```

My Elasticseach was down - status "red":

```
curl localhost:9200/_cluster/health?pretty
{
  "cluster_name" : "moselk",
  "status" : "red",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 421,
  "active_shards" : 421,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 25,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 94.39461883408072
}
```

See Elasticsearch - Tips and Troubleshooting

Can send data to Elasticsearch - Congestion

The /var/log/logstash/logstash.log shows:

```
{:timestamp=>"2016-04-08T08:32:32.217000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:32.721000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:33.232000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:33.733000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:34.282000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
{:timestamp=>"2016-04-08T08:32:34.783000+0200", :message=>"Beats input: the pipeline is blocked, temporary
refusing new connection.", :reconnect_backoff_sleep=>0.5, :level=>:warn}
```

I have seen this twice, the first time setting `congestion_threshold` in the beats input to more than 5 (I use 25) - https://github.com/elastic/logstash/issues/4368 - helped

```
input {
  beats {
    port => 5044
    ssl => true
    ssl_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"
    ssl_key => "/etc/pki/tls/private/logstash-forwarder.key"
    congestion_threshold => 25
  }
}
```

And restart logstash