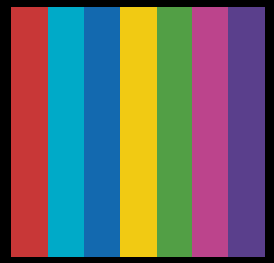
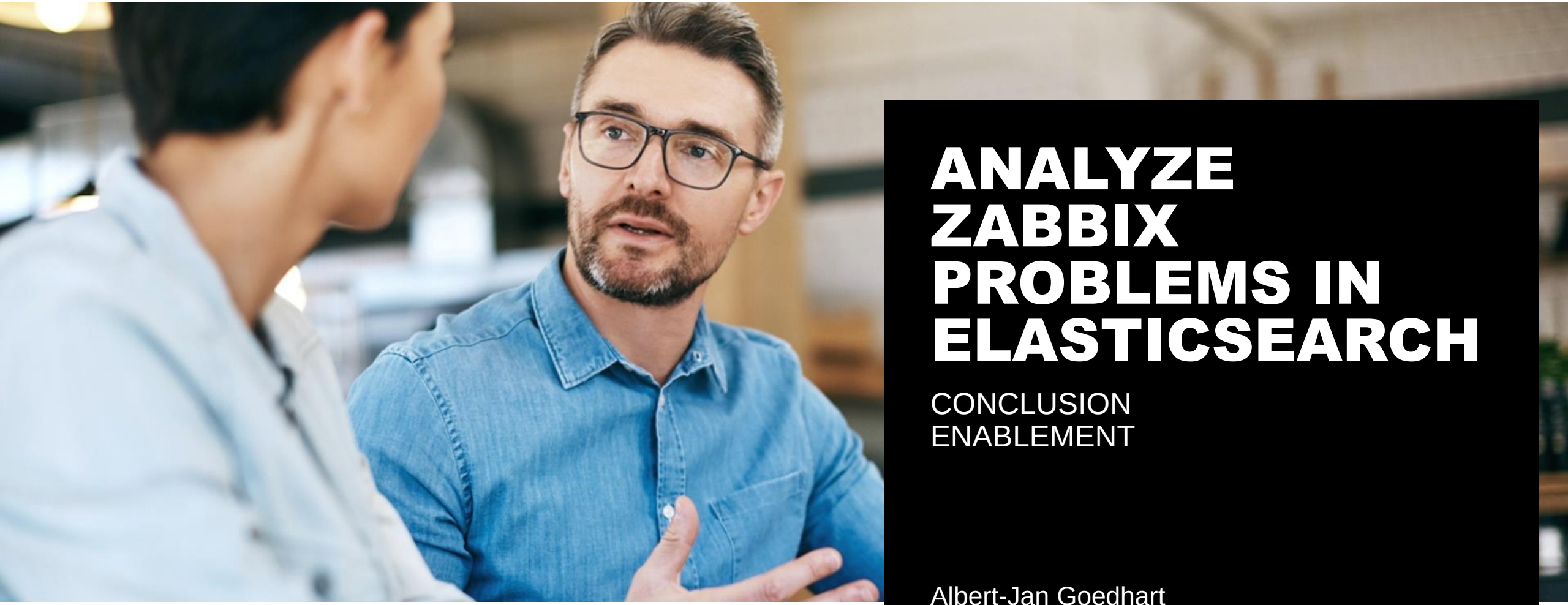


CONCLUSION

ZABBIX

CONCLUSION
ENABLEMENT



ANALYZE ZABBIX PROBLEMS IN ELASTICSEARCH

CONCLUSION
ENABLEMENT

Albert-Jan Goedhart

ZABBIX

CONCLUSION ENABLEMENT

INTRODUCTION

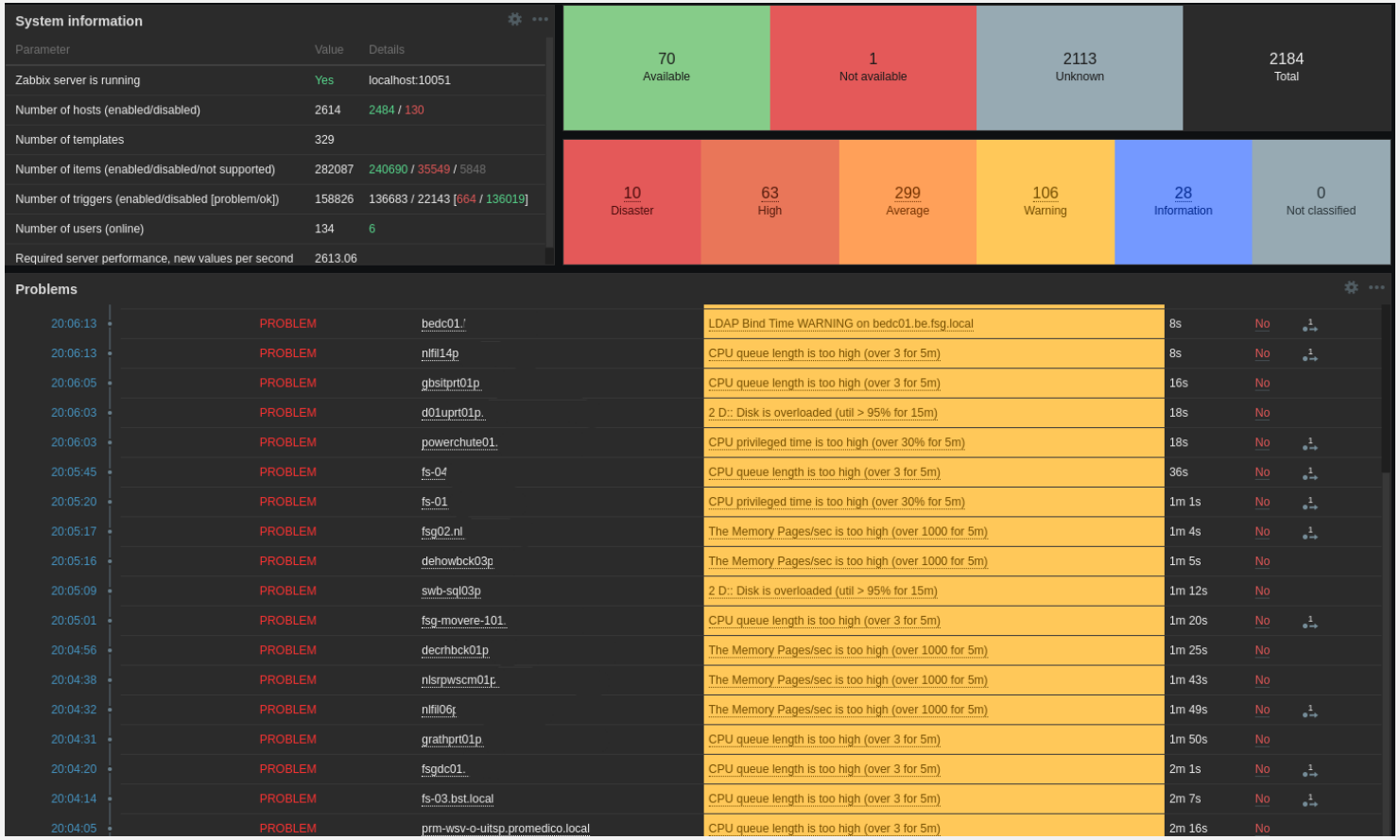
ALBERT-JAN GOEDHART

SOLUTION ENGINEER AT CONCLUSION ENABLEMENT

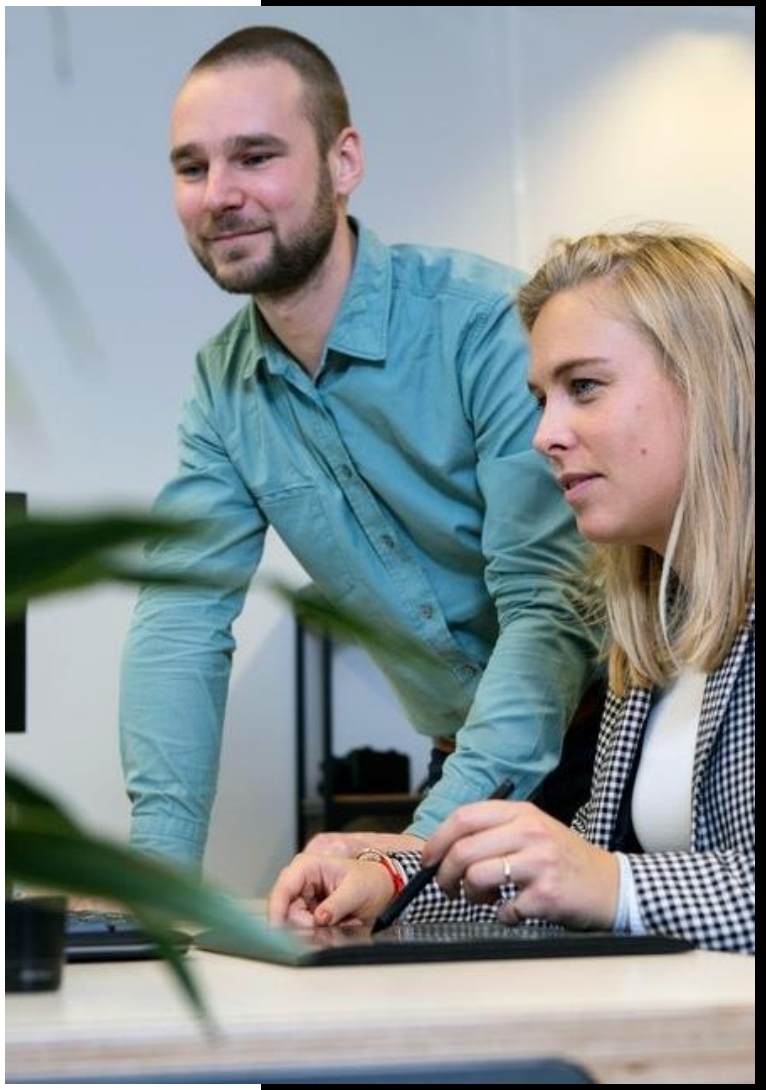
ZABBIX

CONCLUSION ENABLEMENT

ARRGGHHH!



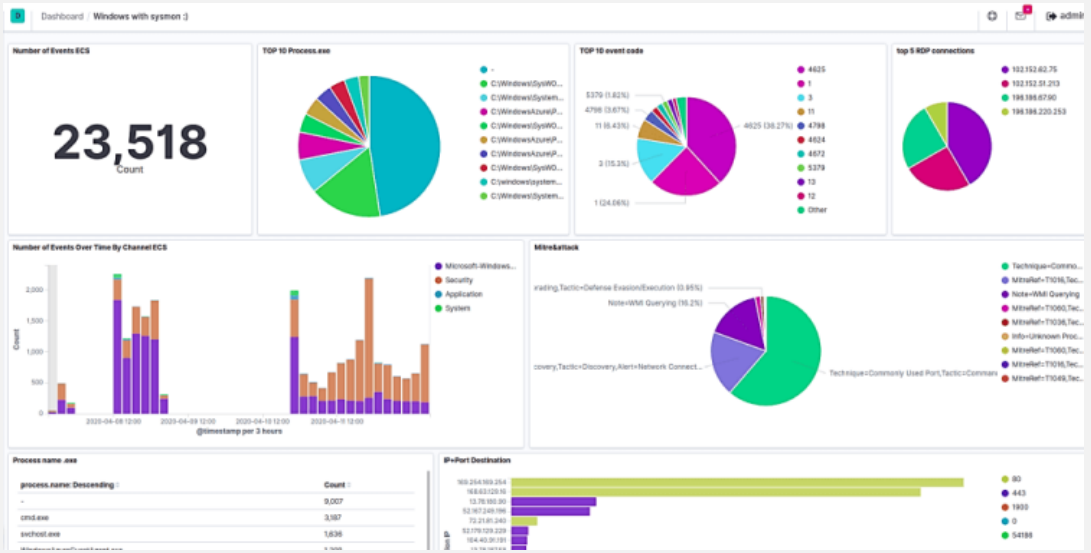
elasticsearch



ZABBIX

CONCLUSION ENABLEMENT

WHAT IS ELASTICSEARCH



Expanded document

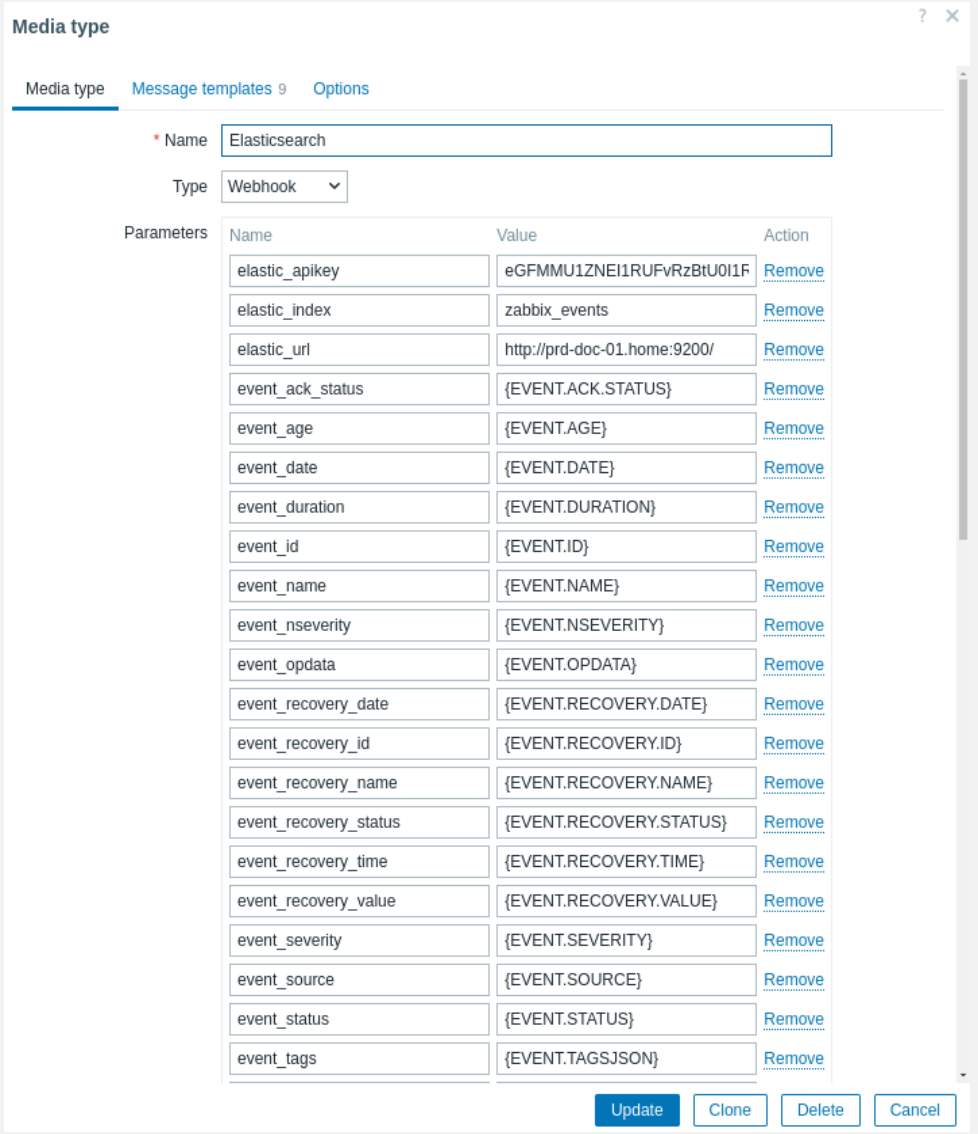
View: Single document | Surrounding documents

_index	zabbix_events
_score	-
@timestamp	Apr 7, 2024 @ 09:32:05.580
customer	Peek-a-Boo Surveillance Co
environment	Productie
event.date	2024.04.07
event.duration	3s
event.id	171968331
event.name	High memory utilization (>90% for 5m)
event.nseverity	2
event.operational.data	91.79 %
event.severity	Warning
event.source	0
event.status	PROBLEM
event.time	09:32:01
event.update.status	0
event.value	1
host.group	Peek-a-Boo Surveillance Co Servers Windows
host.ip	10.250.0.180
host.name	ftp-01.bst.local
site	undefined

ZABBIX

CONCLUSION ENABLEMENT

MEDIATYPE



MEDIATYPE

- AS MUCH DATA AS POSSIBLE
- FILTER ELASTIC_ PARAMETERS
- FILTER ALL VALUES WHICH START AND END WITH { }
- ADDED EVENT SOURCE AS TEXT
- CONVERT EVENT DURATION TO SECONDS
- SPLIT ALL TAGS TO SEPARATE FIELDS

MEDIATYPE

- FILTER ELASTIC_ PARAMETERS

```
4  //Function to filter non-empty keys, keys starting with elastic_ and filter values start/ending with {}
5  function printObject(obj, indent) {
6    for (var key in obj) {
7      if (obj.hasOwnProperty(key)) {
8        if (!key.startsWith("elastic_") && key !== "event_tags" && obj[key] !== "" && !/^{.*}$/.test(obj[key])) {
9          body[indent + key] = obj[key];
10         console.log("Opt2: " + indent + key + ": " + obj[key]);
11       }
12     }
13   }
14 }
```

MEDIATYPE

- FILTER ALL VALUES WHICH START AND END WITH { }

```
4  //Function to filter non-empty keys, keys starting with elastic_ and filter values start/ending with {}
5  function printObject(obj, indent) {
6    for (var key in obj) {
7      if (obj.hasOwnProperty(key)) {
8        if (!key.startsWith("elastic_") && key !== "event_tags" && obj[key] !== "" && !/^{.*}$/.test(obj[key])) {
9          body[indent + key] = obj[key];
10         console.log("Opt2: " + indent + key + ": " + obj[key]);
11       }
12     }
13   }
14 }
```

MEDIATYPE

- ADDED EVENT SOURCE AS TEXT

```
16 //Function to convert numeric eventsource to text
17 function EventSourceText(eventsource) {
18   switch(eventsource) {
19     case 0:
20       eventSourceText = "Trigger";
21       break;
22     case 1:
23       eventSourceText = "Discovery";
24       break;
25     case 2:
26       eventSourceText = "Autoregistration";
27       break;
28     default:
29       eventSourceText = "Internal";
30   }
31   return eventSourceText;
32 }
```

MEDIATYPE

- CONVERT EVENT DURATION TO SECONDS

```
//Function to convert event duration to seconds
//Makes duration searches possible in Elastic
function convertDurationToSeconds(duration) {
const regex = /(\d+)([smhdwMy])/g;
totalSeconds = 0;
while ((match = regex.exec(duration)) !== null) {
  const value = parseInt(match[1]);
  const unit = match[2];
  switch (unit) {
    case 's':
      totalSeconds += value;
      break;
    case 'm':
      totalSeconds += value * 60;
      break;
    case 'h':
      totalSeconds += value * 3600;
      break;
    case 'd':
      totalSeconds += value * 86400;
      break;
    case 'w':
      totalSeconds += value * 604800;
      break;
    case 'M':
      totalSeconds += value * 2592000;
      break;
    case 'y':
      totalSeconds += value * 31536000;
      break;
    default:
      // Ignore unknown units
      break;
    }
```

MEDIATYPE

- SPLIT ALL TAGS TO SEPARATE FIELDS

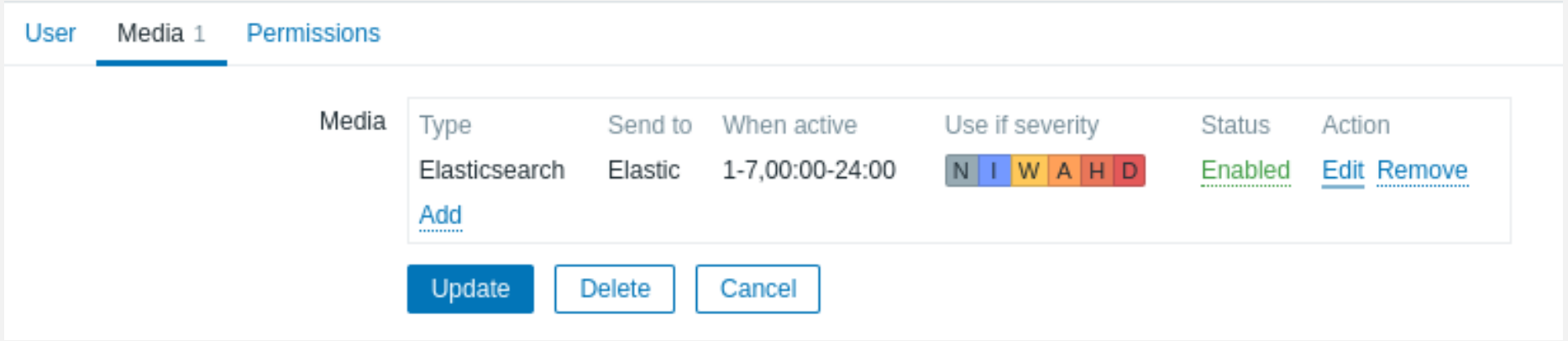
```
77  //Iterate over all tags and add them to Elastic
78  //hese tags will be parsed to Elastic, make sure to add all tag names to the
79  //index template in Elasticsearch to make them searchable
80  if (params.event_tags !== '{EVENT.TAGSJSON}') {
81    var eventTags = JSON.parse(params.event_tags);
82    for (var i = 0; i < eventTags.length; i++) {
83      body["tag." + eventTags[i].tag] = eventTags[i].value;
84    }
85  }
```

MEDIATYPE

- AS MUCH DATA AS POSSIBLE
- FILTER ELASTIC_ PARAMETERS
- FILTER ALL VALUES WHICH START AND END WITH { }
- ADDED EVENT SOURCE AS TEXT
- CONVERT EVENT DURATION TO SECONDS
- SPLIT ALL TAGS TO SEPARATE FIELDS

USER MEDIA

- SEPARATE USER

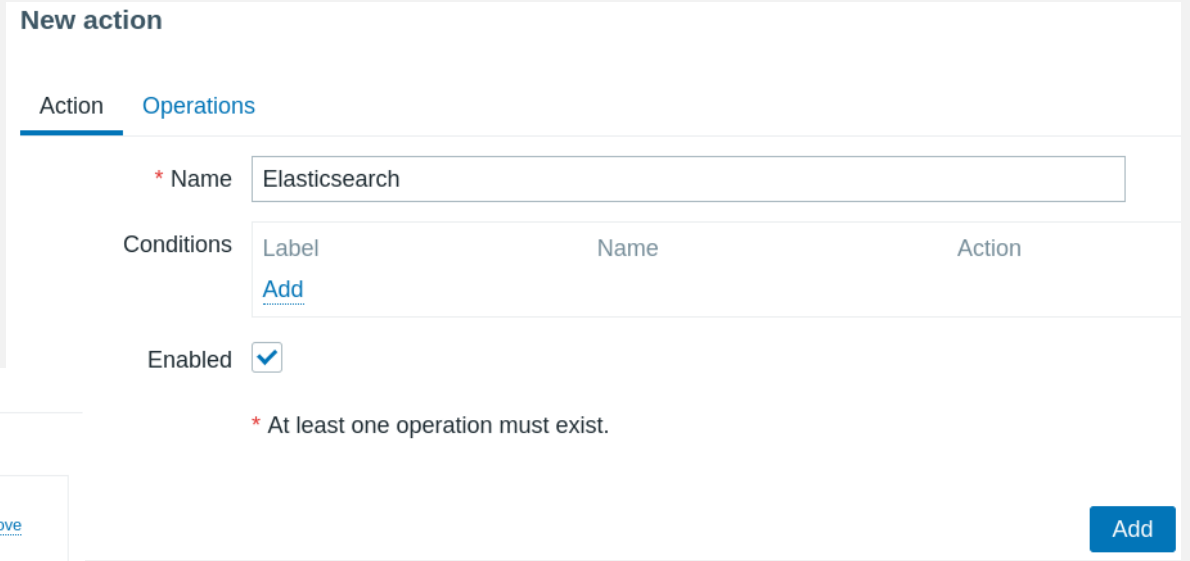


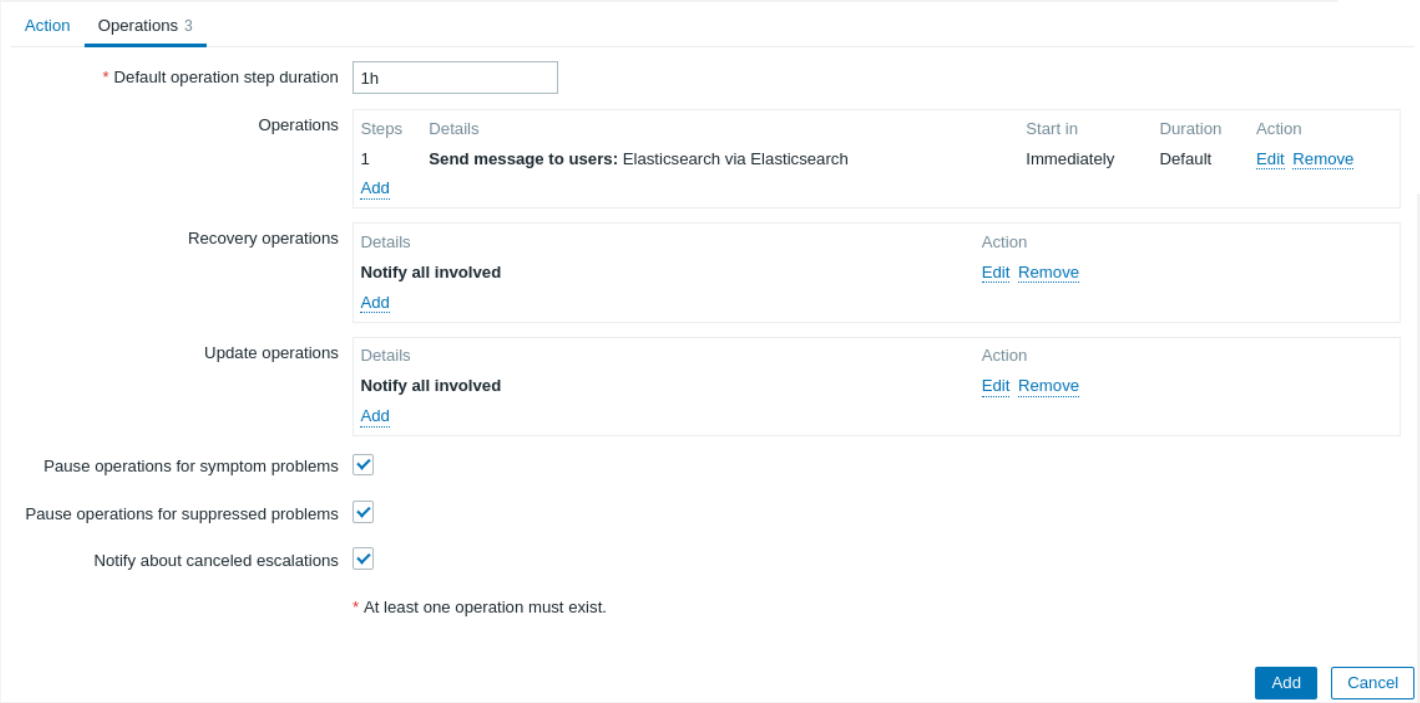
ZABBIX

CONCLUSION ENABLEMENT

TRIGGER ACTION

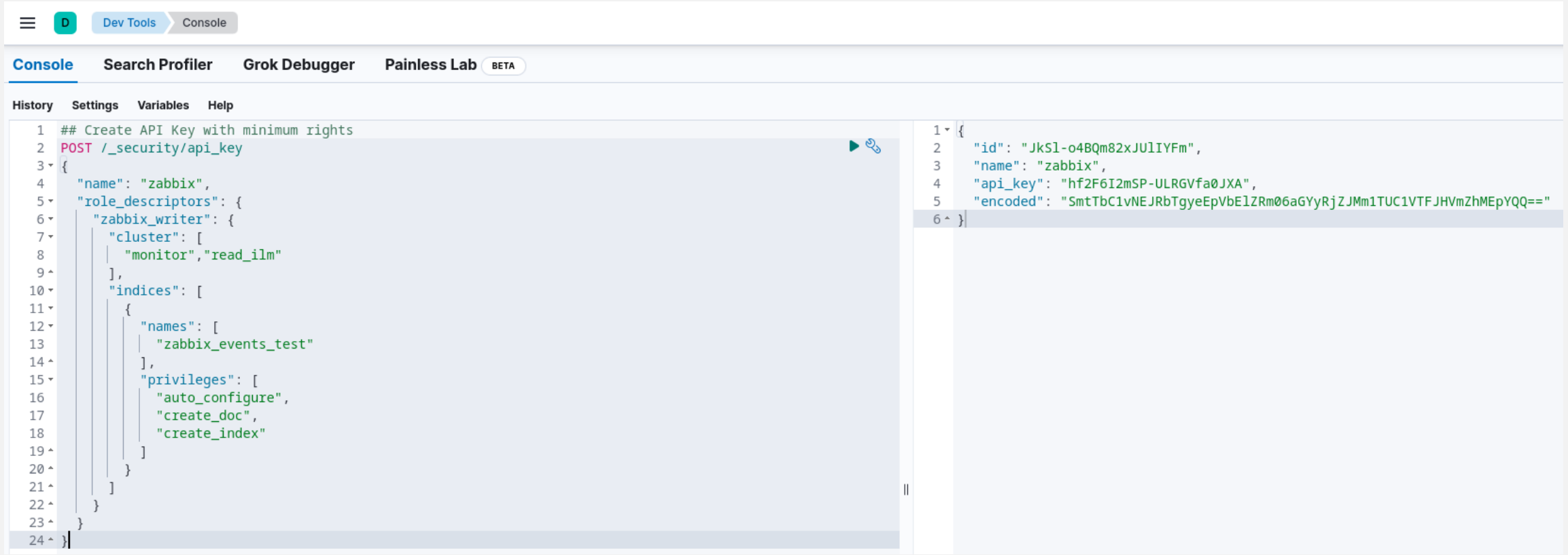
- CREATE TRIGGER ACTION





API TOKEN

- CREATE API TOKEN

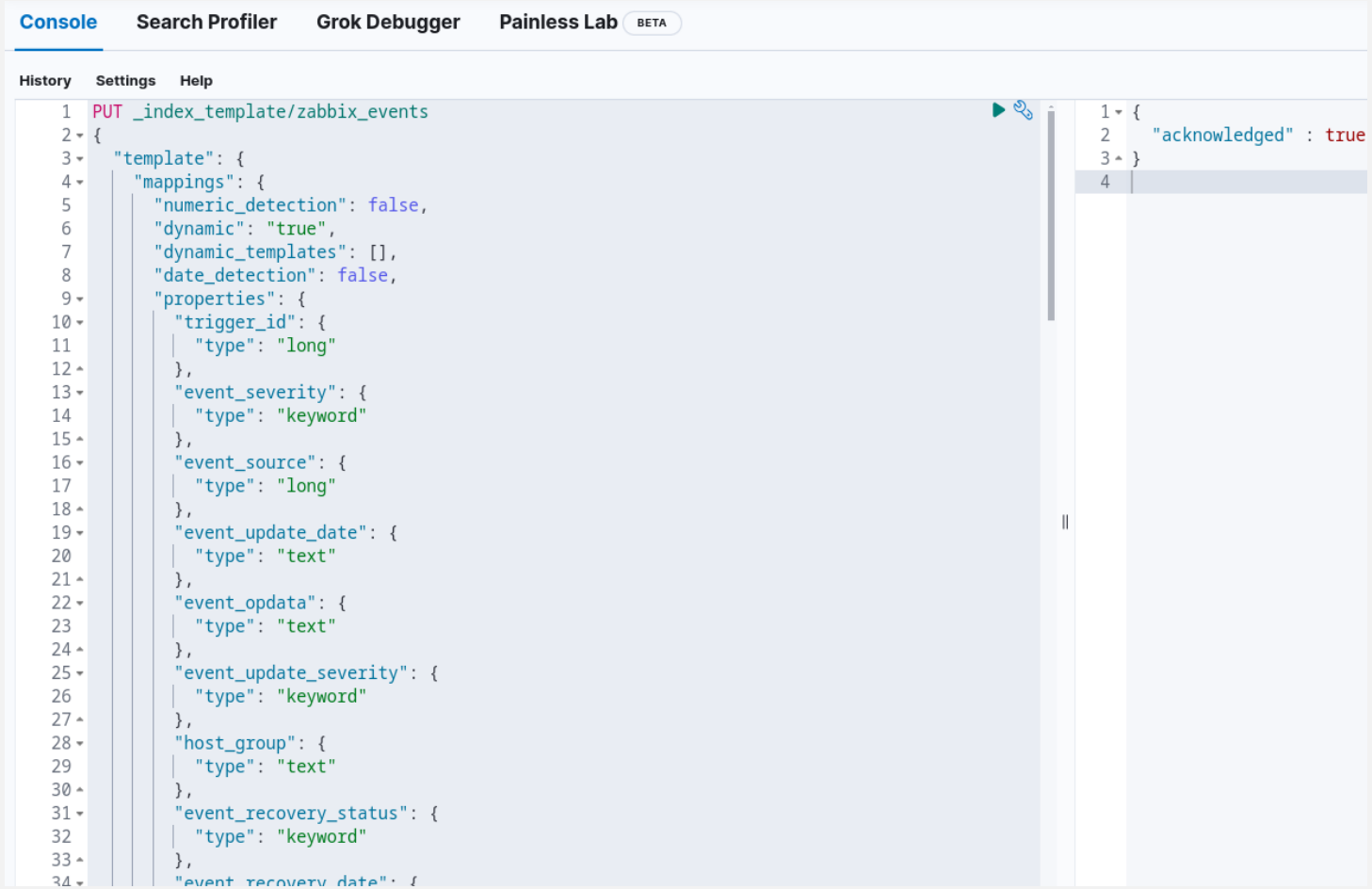


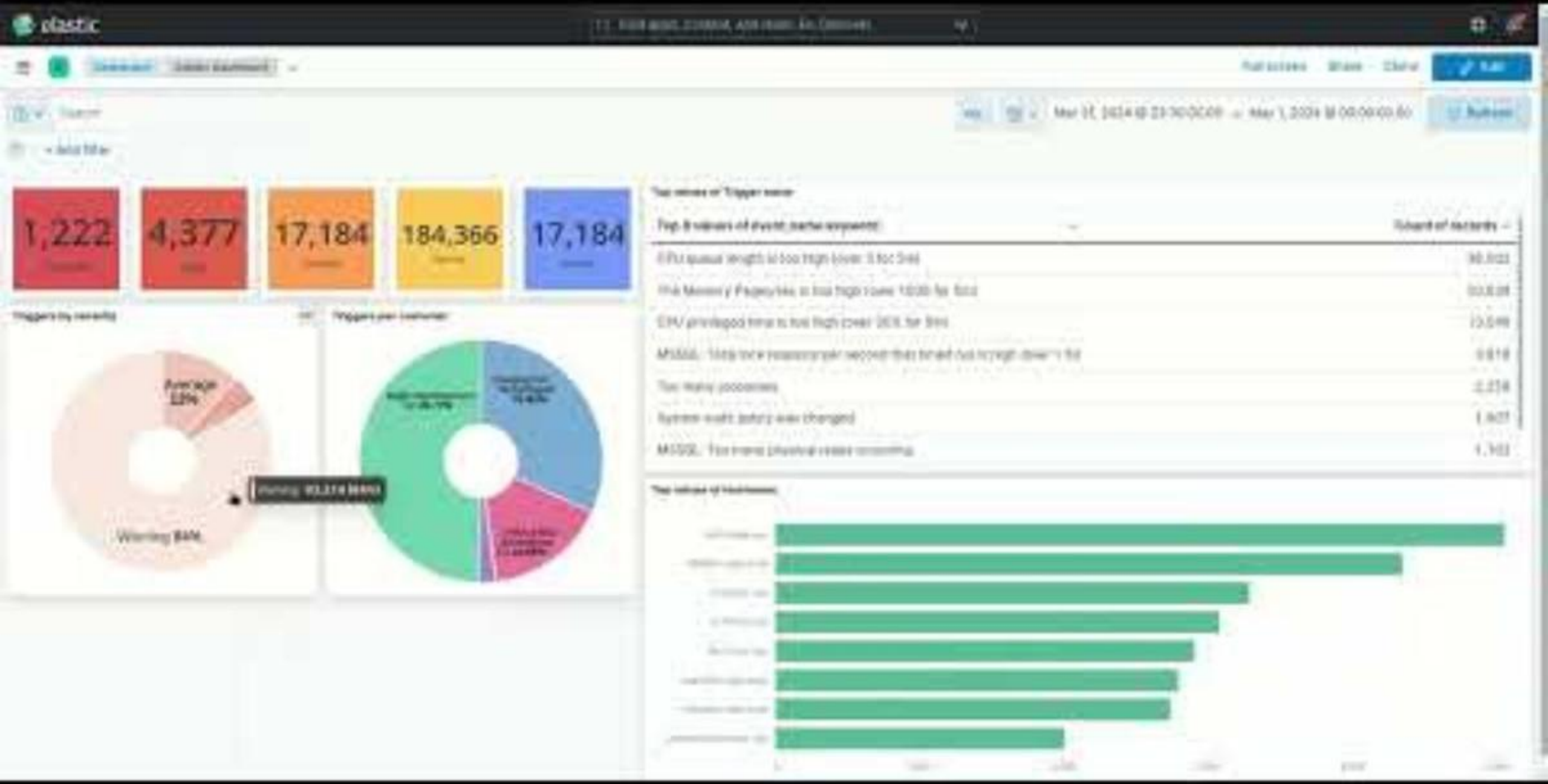
ZABBIX

CONCLUSION ENABLEMENT

INDEX TEMPLATE

- CREATE AN INDEX TEMPLATE




1,222
4,377
17,184
184,366
17,184
Warning 84K

USE CASES

- ADVANCED REPORTING TOOLS
- DISCOVERY ACTIONS
- AUTOREGISTRATION ACTIONS
- QUERY STATISTICS IN ELASTICSEARCH FROM ZABBIX
- STREAM METRICS FROM ZABBIX TO ELASTICSEARCH
  - ZBXNEXT-8704 -> IMPROVE STREAMING CAPABILITIES
  - ZBX-23400 -> ACCEPT HTTP 201 AS VALID RESPONSE

History Settings Help

```
GET /zabbix_events*/_count
{
  "query": {
    "bool": {
      "filter": [
        {
          "range": {
            "@timestamp": {
              "gte": "now-15m"
            }
          }
        }
      ],
      "should": [
        {
          "match": {
            "event_status": "RESOLVED"
          }
        }
      ],
      "minimum_should_match": 1
    }
  }
}
```

```
{
  "count" : 46,
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "skipped" : 0,
    "failed" : 0
  }
}
```

https://github.com/Zablove

MEDIA TYPE

LAB ZABBIX WITH ELASTICSEARCH

CONCLUSION

www.conclusion.nl

CONCLUSION
ENABLEMENT