

CONCLUSION



ANALYZE ZABBIX PROBLEMS IN ELASTICSEARCH

CONCLUSION
ENABLEMENT

Albert-Jan Goedhart

INTRODUCTION

ALBERT-JAN GOEDHART

SOLUTION ENGINEER AT CONCLUSION ENABLEMENT

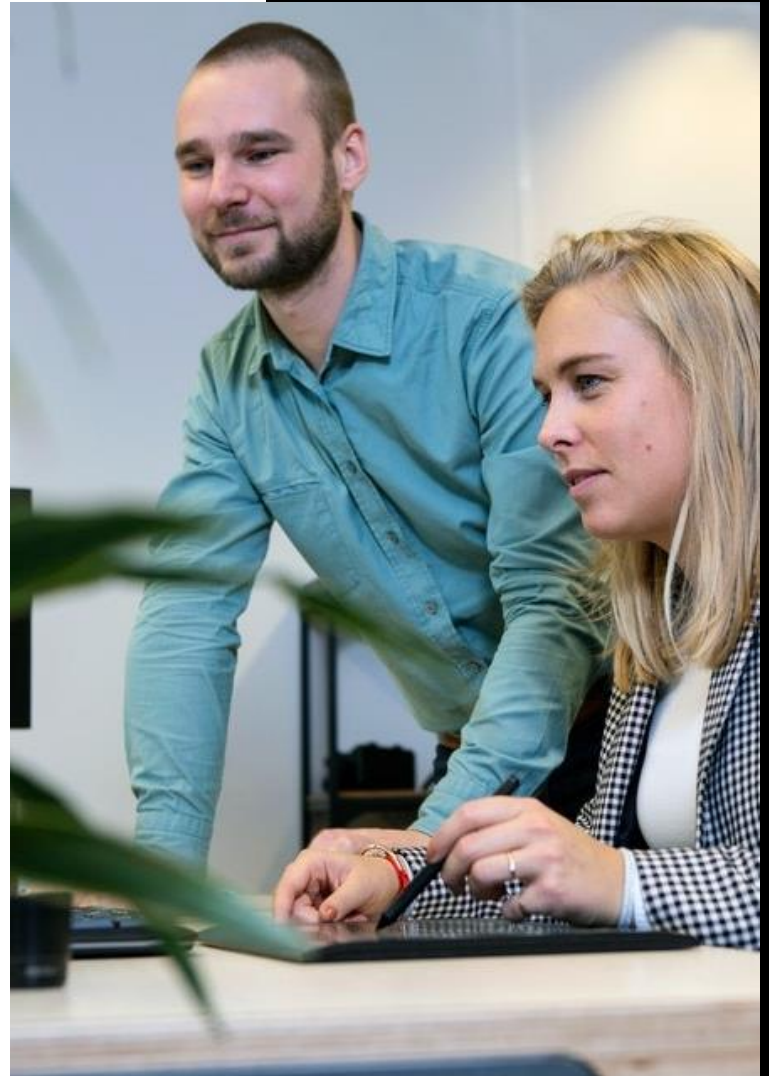
ARRGGHHH!

System information

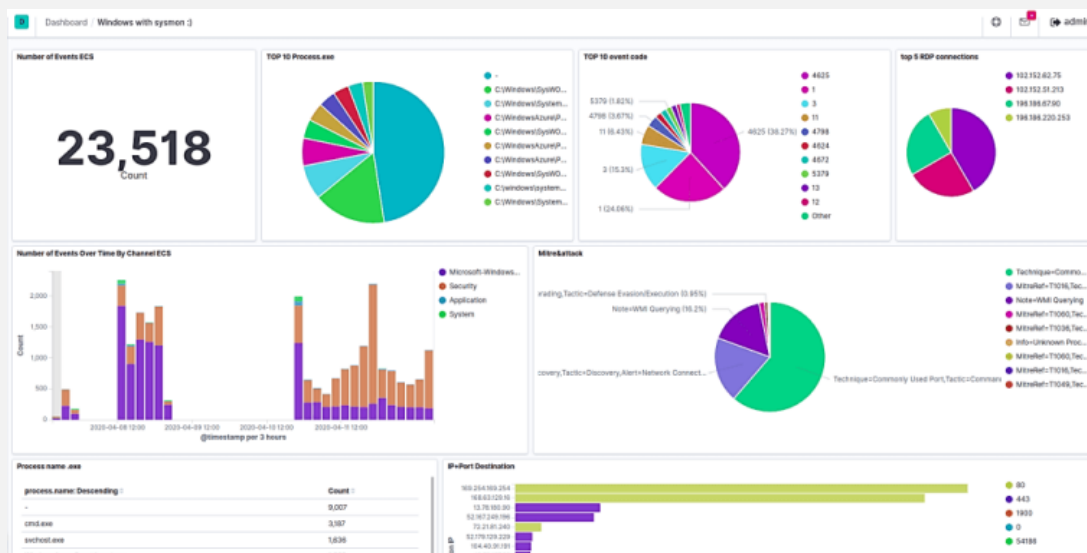
Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled)	2614	2484 / 130
Number of templates	329	
Number of items (enabled/disabled/not supported)	282087	240690 / 35549 / 5848
Number of triggers (enabled/disabled [problem/ok])	158826	136683 / 22143 [664 / 136019]
Number of users (online)	134	6
Required server performance, new values per second	2613.06	

Problems

Time	Severity	Host	Problem	Duration	Priority	Actions
20:06:13	PROBLEM	bedc01	LDAP Bind Time WARNING on bedc01.be.fsg.local	8s	No	1
20:06:13	PROBLEM	nfil14p	CPU queue length is too high (over 3 for 5m)	8s	No	1
20:06:05	PROBLEM	gbsitprt01p	CPU queue length is too high (over 3 for 5m)	16s	No	
20:06:03	PROBLEM	d01uprt01p	2 D:: Disk is overloaded (util > 95% for 15m)	18s	No	
20:06:03	PROBLEM	powerchute01	CPU privileged time is too high (over 30% for 5m)	18s	No	1
20:05:45	PROBLEM	fs-04	CPU queue length is too high (over 3 for 5m)	36s	No	1
20:05:20	PROBLEM	fs-01	CPU privileged time is too high (over 30% for 5m)	1m 1s	No	1
20:05:17	PROBLEM	fsg02.nl	The Memory Pages/sec is too high (over 1000 for 5m)	1m 4s	No	1
20:05:16	PROBLEM	dehowbck03p	The Memory Pages/sec is too high (over 1000 for 5m)	1m 5s	No	
20:05:09	PROBLEM	swb-sql03p	2 D:: Disk is overloaded (util > 95% for 15m)	1m 12s	No	
20:05:01	PROBLEM	fsg-movere-101	CPU queue length is too high (over 3 for 5m)	1m 20s	No	1
20:04:56	PROBLEM	dechrhck01p	The Memory Pages/sec is too high (over 1000 for 5m)	1m 25s	No	
20:04:38	PROBLEM	nlsrpwscm01p	The Memory Pages/sec is too high (over 1000 for 5m)	1m 43s	No	
20:04:32	PROBLEM	nfil06f	The Memory Pages/sec is too high (over 1000 for 5m)	1m 49s	No	1
20:04:31	PROBLEM	grathprt01p	CPU queue length is too high (over 3 for 5m)	1m 50s	No	
20:04:20	PROBLEM	fsgdc01	CPU queue length is too high (over 3 for 5m)	2m 1s	No	1
20:04:14	PROBLEM	fs-03.bst.local	CPU queue length is too high (over 3 for 5m)	2m 7s	No	1
20:04:05	PROBLEM	prn-wsv-o-uitsp.promedico.local	CPU queue length is too high (over 3 for 5m)	2m 16s	No	



WHAT IS ELASTICSEARCH



Expanded document

View: [Single document](#) [Surrounding documents](#) [🔍](#)

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

MEDIATYPE

Media type

Media type Message templates 9 Options

* Name

Type

Parameters

Name	Value	Action
<input type="text" value="elastic_apikey"/>	<input type="text" value="eGFMMU1ZNEI1RUFvRzBtU01F"/>	Remove
<input type="text" value="elastic_index"/>	<input type="text" value="zabbix_events"/>	Remove
<input type="text" value="elastic_url"/>	<input type="text" value="http://prd-doc-01.home:9200/"/>	Remove
<input type="text" value="event_ack_status"/>	<input type="text" value="{EVENT.ACK.STATUS}"/>	Remove
<input type="text" value="event_age"/>	<input type="text" value="{EVENT.AGE}"/>	Remove
<input type="text" value="event_date"/>	<input type="text" value="{EVENT.DATE}"/>	Remove
<input type="text" value="event_duration"/>	<input type="text" value="{EVENT.DURATION}"/>	Remove
<input type="text" value="event_id"/>	<input type="text" value="{EVENT.ID}"/>	Remove
<input type="text" value="event_name"/>	<input type="text" value="{EVENT.NAME}"/>	Remove
<input type="text" value="event_nseverity"/>	<input type="text" value="{EVENT.NSEVERITY}"/>	Remove
<input type="text" value="event_opdata"/>	<input type="text" value="{EVENT.OPDATA}"/>	Remove
<input type="text" value="event_recovery_date"/>	<input type="text" value="{EVENT.RECOVERY.DATE}"/>	Remove
<input type="text" value="event_recovery_id"/>	<input type="text" value="{EVENT.RECOVERY.ID}"/>	Remove
<input type="text" value="event_recovery_name"/>	<input type="text" value="{EVENT.RECOVERY.NAME}"/>	Remove
<input type="text" value="event_recovery_status"/>	<input type="text" value="{EVENT.RECOVERY.STATUS}"/>	Remove
<input type="text" value="event_recovery_time"/>	<input type="text" value="{EVENT.RECOVERY.TIME}"/>	Remove
<input type="text" value="event_recovery_value"/>	<input type="text" value="{EVENT.RECOVERY.VALUE}"/>	Remove
<input type="text" value="event_severity"/>	<input type="text" value="{EVENT.SEVERITY}"/>	Remove
<input type="text" value="event_source"/>	<input type="text" value="{EVENT.SOURCE}"/>	Remove
<input type="text" value="event_status"/>	<input type="text" value="{EVENT.STATUS}"/>	Remove
<input type="text" value="event_tags"/>	<input type="text" value="{EVENT.TAGSJSON}"/>	Remove

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

```
34 //Function to convert event duration to seconds
35 //Makes duration searches possible in Elastic
36 function convertDurationToSeconds(duration) {
37   const regex = /(\d+)([smhdwMy])/g;
38   totalSeconds = 0;
39   while ((match = regex.exec(duration)) !== null) {
40     const value = parseInt(match[1]);
41     const unit = match[2];
42     switch (unit) {
43       case 's':
44         totalSeconds += value;
45         break;
46       case 'm':
47         totalSeconds += value * 60;
48         break;
49       case 'h':
50         totalSeconds += value * 3600;
51         break;
52       case 'd':
53         totalSeconds += value * 86400;
54         break;
55       case 'w':
56         totalSeconds += value * 604800;
57         break;
58       case 'M':
59         totalSeconds += value * 2592000;
60         break;
61       case 'y':
62         totalSeconds += value * 31536000;
63         break;
64       default:
65         // Ignore unknown units
66         break;
67     }
68   }
69 }
```

MEDIATYPE

- SPLIT ALL TAGS TO SEPARATE FIELDS

```
77 //Iterate over all tags and add them to Elastic
78 //these 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

User Media 1 Permissions

Media	Type	Send to	When active	Use if severity	Status	Action
	Elasticsearch	Elastic	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
Add						

[Update](#) [Delete](#) [Cancel](#)

TRIGGER ACTION

- CREATE TRIGGER ACTION

Action **Operations 3**

* Default operation step duration

Operations	Steps	Details	Start in	Duration	Action
	1	Send message to users: Elasticsearch via Elasticsearch	Immediately	Default	Edit Remove

[Add](#)

Recovery operations

Details	Action
Notify all involved	Edit Remove

[Add](#)

Update operations

Details	Action
Notify all involved	Edit Remove

[Add](#)

Pause operations for symptom problems

Pause operations for suppressed problems

Notify about canceled escalations

* At least one operation must exist.

[Add](#) [Cancel](#)

New action

Action **Operations**

* Name

Conditions

Label	Name	Action
Add		

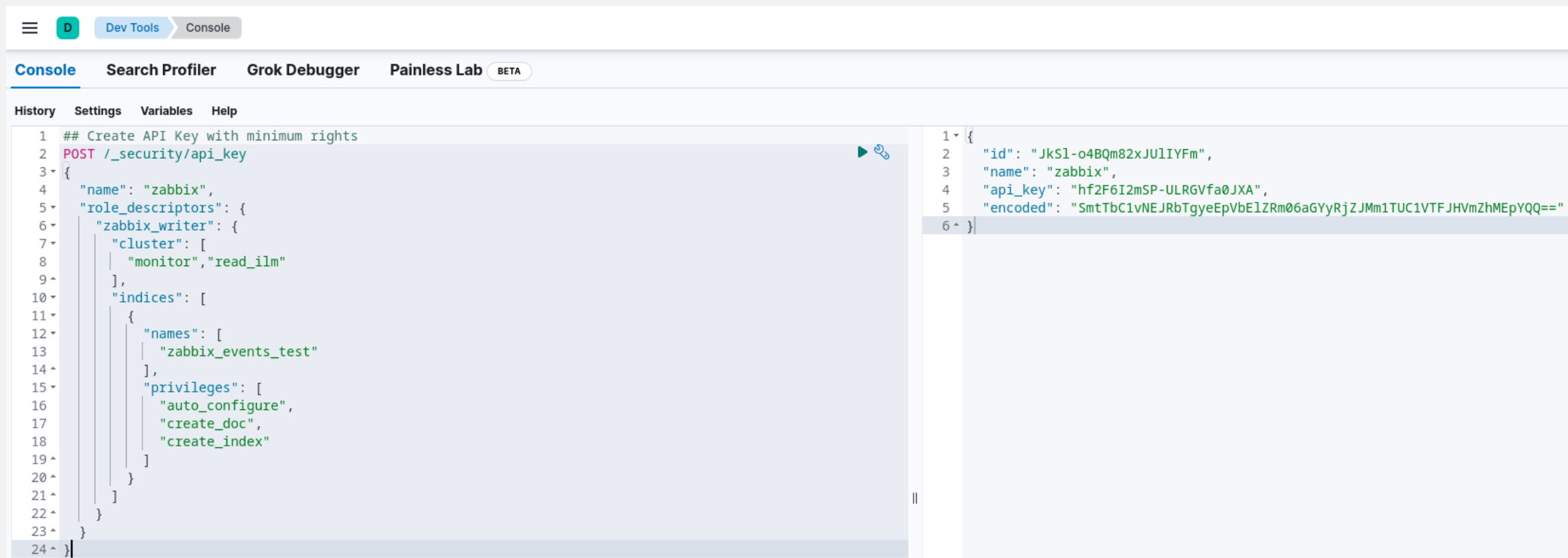
Enabled

* At least one operation must exist.

[Add](#)

API TOKEN

- CREATE API TOKEN



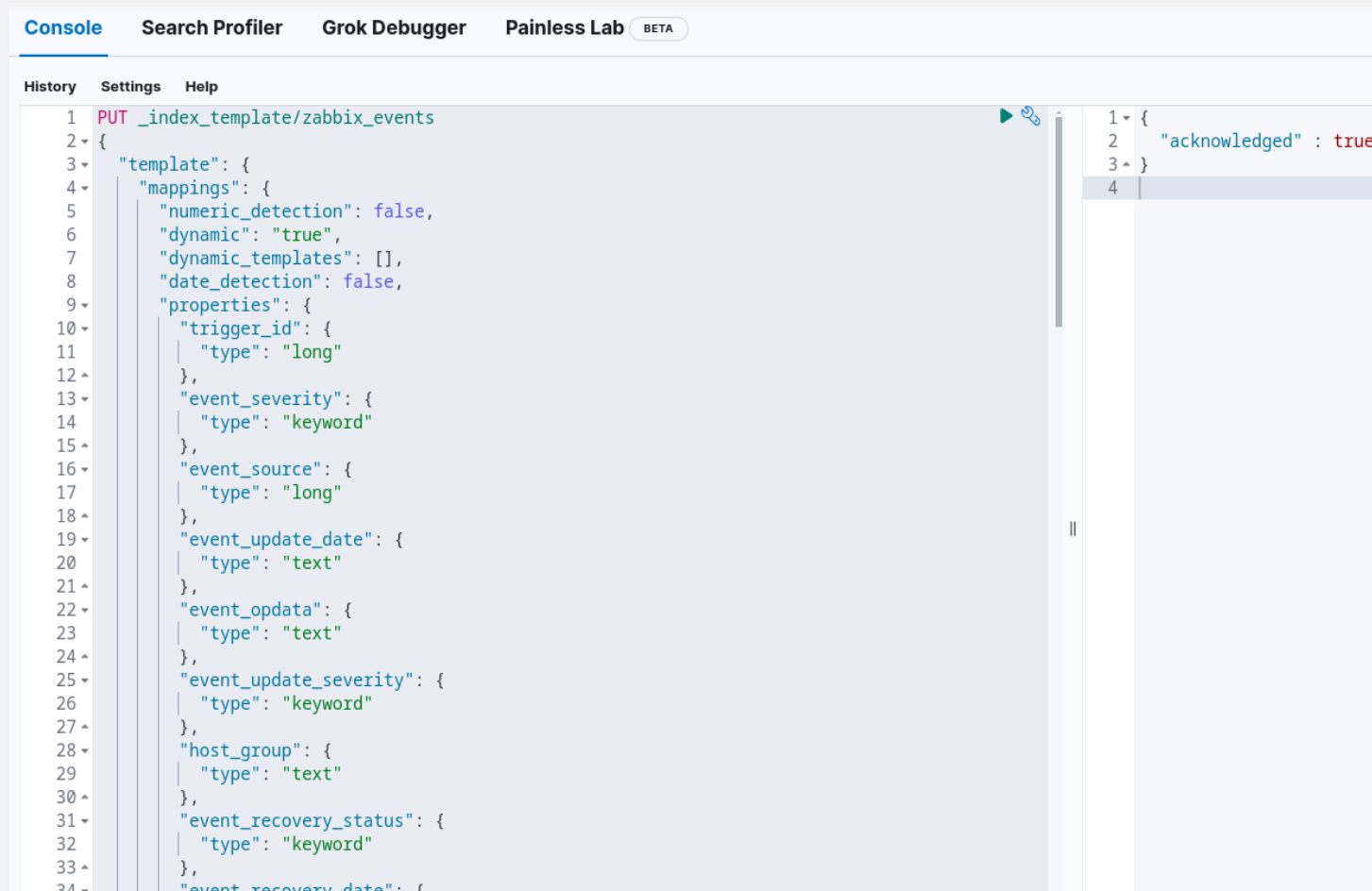
The screenshot shows a web browser's developer console with the 'Console' tab selected. The console displays a REST client request and its corresponding JSON response. The request is a POST to the endpoint `/_security/api_key` with a JSON body defining a role for 'zabbix' with specific permissions. The response is a JSON object containing the created role's details, including its ID, name, API key, and an encoded version of the role configuration.

```
1 ## Create API Key with minimum rights
2 POST /_security/api_key
3 {
4   "name": "zabbix",
5   "role_descriptors": {
6     "zabbix_writer": {
7       "cluster": [
8         "monitor", "read_ilm"
9       ],
10      "indices": [
11        {
12          "names": [
13            "zabbix_events_test"
14          ],
15          "privileges": [
16            "auto_configure",
17            "create_doc",
18            "create_index"
19          ]
20        }
21      ]
22    }
23  }
24 }
```

```
1 {
2   "id": "JkSl-o4BQm82xJUIYFm",
3   "name": "zabbix",
4   "api_key": "hf2F6I2mSP-ULRGVfa0JXA",
5   "encoded": "SmtTbC1vNEJRbTgyeEpVbE1ZRm06aGYyRjZJMm1TUC1VTFJHvmZhMEpYQQ=="
6 }
```

INDEX TEMPLATE

- CREATE AN INDEX TEMPLATE

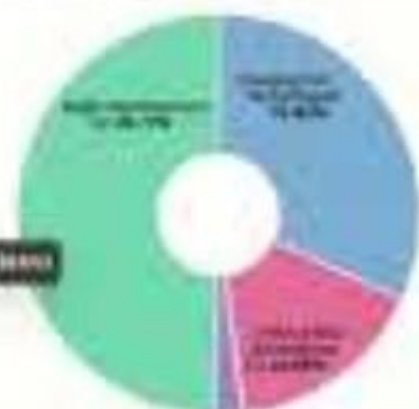


The screenshot shows the Zabbix web interface's console. The 'Console' tab is active, displaying a REST API call to create an index template. The request body is a JSON object with the following structure:

```
1 PUT _index_template/zabbix_events
2 {
3   "template": {
4     "mappings": {
5       "numeric_detection": false,
6       "dynamic": "true",
7       "dynamic_templates": [],
8       "date_detection": false,
9     "properties": {
10      "trigger_id": {
11        "type": "long"
12      },
13      "event_severity": {
14        "type": "keyword"
15      },
16      "event_source": {
17        "type": "long"
18      },
19      "event_update_date": {
20        "type": "text"
21      },
22      "event_opdata": {
23        "type": "text"
24      },
25      "event_update_severity": {
26        "type": "keyword"
27      },
28      "host_group": {
29        "type": "text"
30      },
31      "event_recovery_status": {
32        "type": "keyword"
33      },
34      "event_recovery_date": {
```

The response body is partially visible on the right side of the console, showing:

```
1 {
2   "acknowledged" : true
3 }
```



The values of Trigger name

Top 8 values of event name (events)

Count of factories

CPU queue length is too high (over 5 for 5s)	90,823
File Memory Fragmentation is too high (over 100% for 5s)	63,828
CPU privileged time is too high (over 20% for 5s)	15,049
MSMR: 100% on a resource per second that tried but couldn't get	9,819
The heap is too small	2,218
System wait policy was changed	1,807
MSMR: The heap physical usage is too high	1,703

The values of hostnames



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
1 GET /zabbix_events*/_count
2 {
3   "query": {
4     "bool": {
5       "filter": [
6         {
7           "range": {
8             "@timestamp": {
9               "gte": "now-15m"
10            }
11          }
12        }
13      ],
14      "should": [
15        {
16          "match": {
17            "event_status": "RESOLVED"
18          }
19        }
20      ],
21      "minimum_should_match": 1
22    }
23  }
24 }
```

```
1 {
2   "count" : 46,
3   "_shards" : {
4     "total" : 2,
5     "successful" : 2,
6     "skipped" : 0,
7     "failed" : 0
8   }
9 }
```

<https://github.com/Zablove>



MEDIA TYPE



LAB ZABBIX WITH ELASTICSEARCH

CONCLUSION

www.conclusion.nl



CONCLUSION
ENABLEMENT