LAB 4 – Elastic Alerting

Estimated Time for This Lab: 30 Min

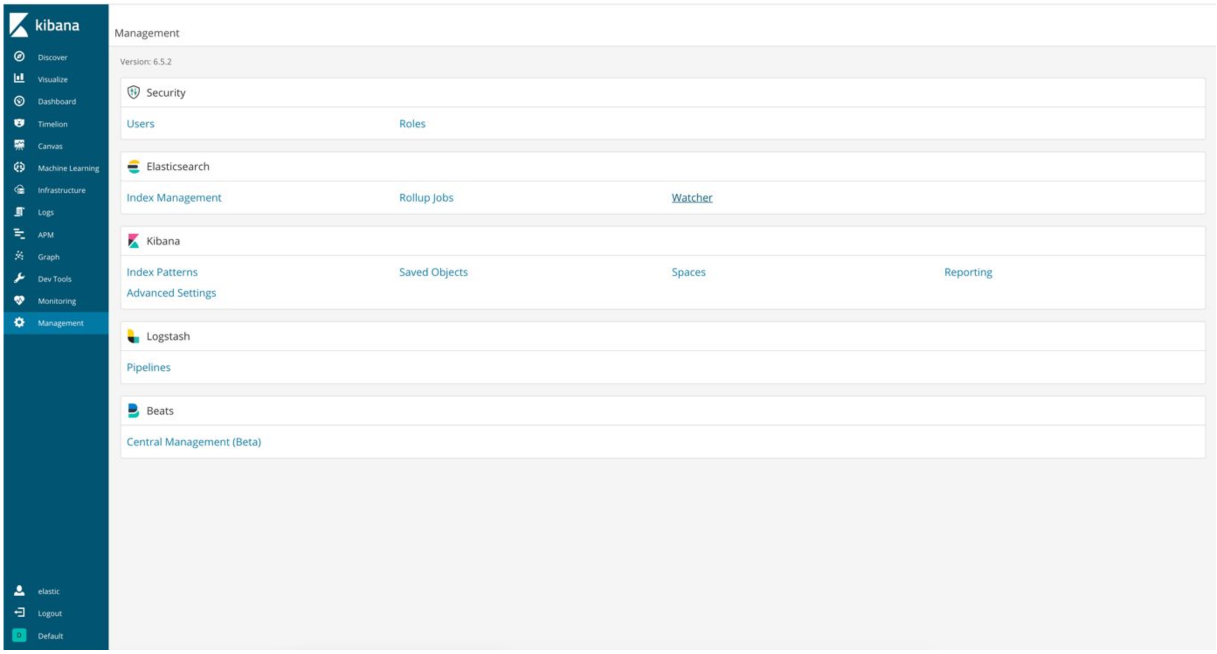
Introduction

Log data can tell you all sorts of things about your applications and infrastructure. Once we have data flowing into Elastic most companies want to be Alerted when specific patterns or conditions are seen in the data. Elastic Alerting allows you to define the data/events that are of interest so that Elastic and send an Alert to notify you.

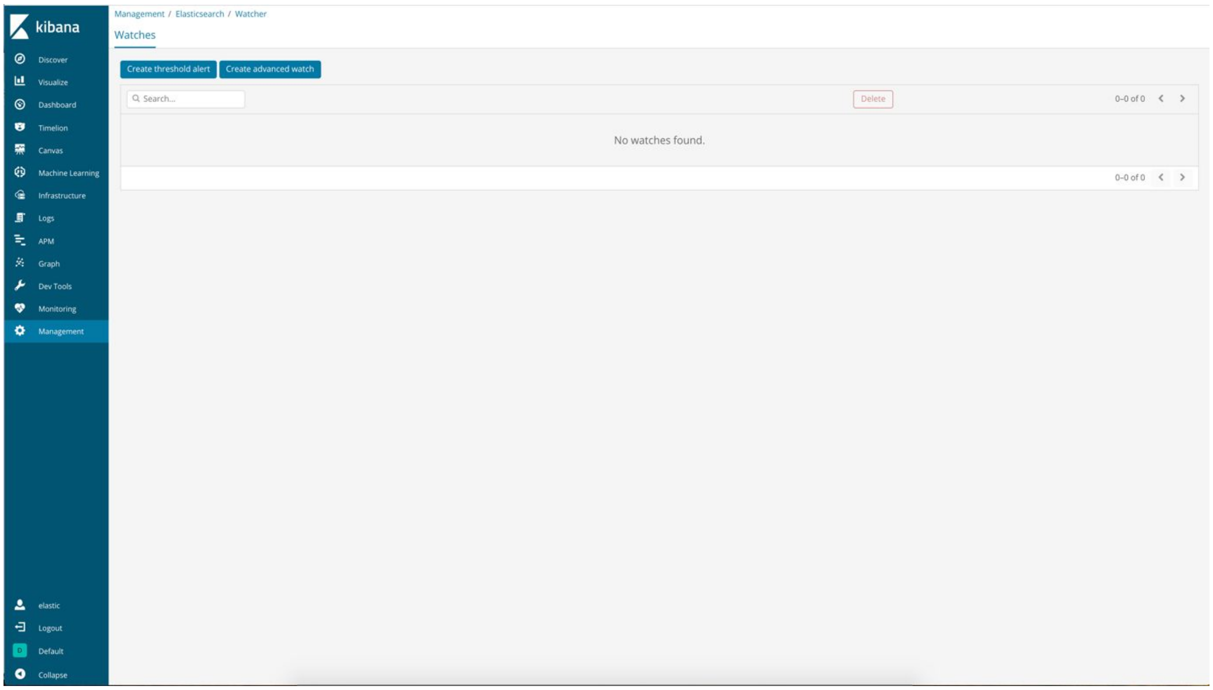
In this lab we will look at setting up basic threshold alerts and also defining more advanced Alerts.

Let’s get started!

1. In Kibana click on “Management” item in the menu and then click on “Watcher”.



2. First let’s create a simple threshold alert. Click on “Create threshold alert” button.



Management / Elasticsearch / Watcher

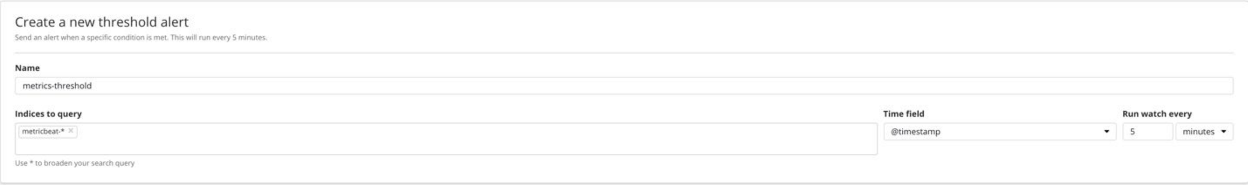
Watches

0-0 of 0

No watches found.

0-0 of 0

3. Give it a name and in the indices section fill out the following conditions:
   Indices to query: metricbeat-*
   Time field: @timestamp
   Run watch every: 5 min



Create a new threshold alert

Send an alert when a specific condition is met. This will run every 5 minutes.

Name: metrics-threshold

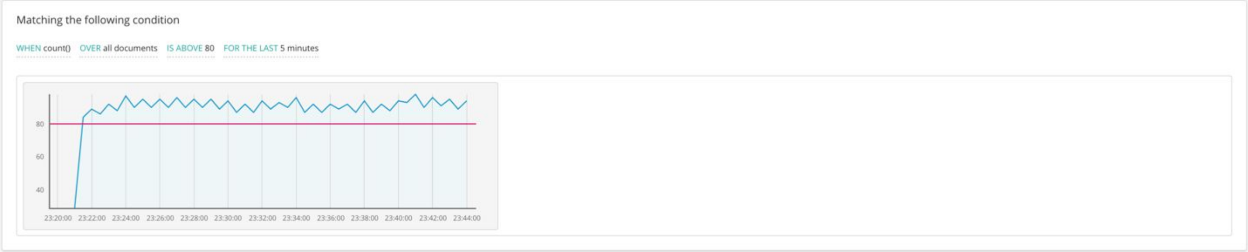
Indices to query: metricbeat-*

Use * to broaden your search query

Time field: @timestamp

Run watch every: 5 minutes

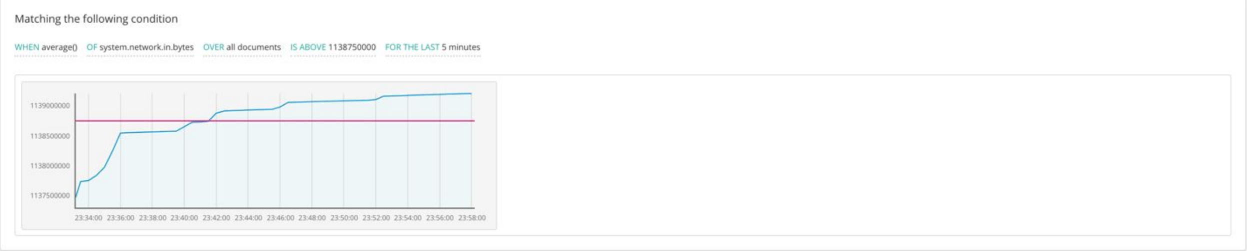
In the Matching condition section first try count() for function over all the documents over the last 5 minutes and play with the threshold so that the aggregation value goes over the red line:



Matching the following condition

WHEN count() OVER all documents IS ABOVE 80 FOR THE LAST 5 minutes

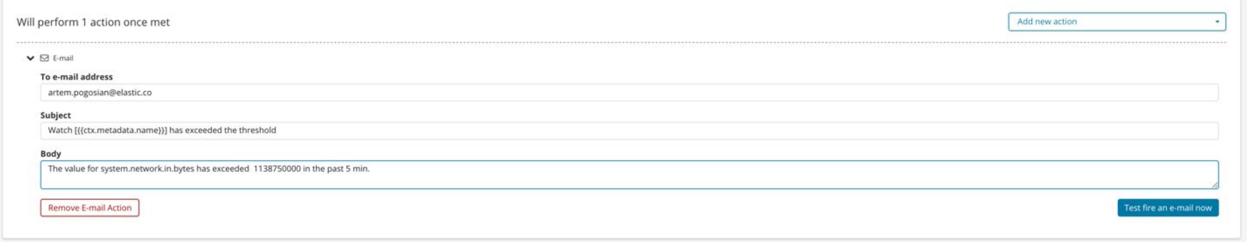
Now to get an idea what other kinds of conditions are possible select average of system.network.in.bytes over the last 5 min and play with the threshold so that the aggregation value goes over the line:



Matching the following condition

WHEN average() OF system.network.in.bytes OVER all documents IS ABOVE 1138750000 FOR THE LAST 5 minutes

Define an action for the scenario where the threshold gets bypassed. Select email action, specify your email that you've whitelisted in Lab 0, and put in email text in a body. Click on "Test fire an email", you should get this email your inbox in a few min.



Will perform 1 action once met

E-mail

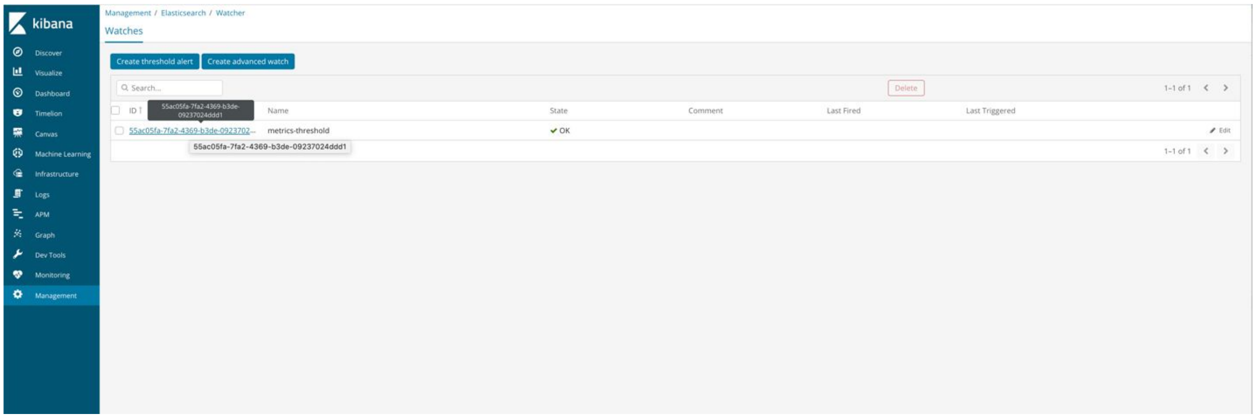
To e-mail address
artem.pogosian@elastic.co

Subject
Watch [{{ctx.metadata.name}}] has exceeded the threshold

Body
The value for system.network.in.bytes has exceeded 1138750000 in the past 5 min.

Click on "Save" button to save the watch.

4. You will end up on the main page for watches. It is likely that you will be receiving a new watch email every 5 min. You probably do not want that right now, so click on the watch.



Management / Elasticsearch / Watcher

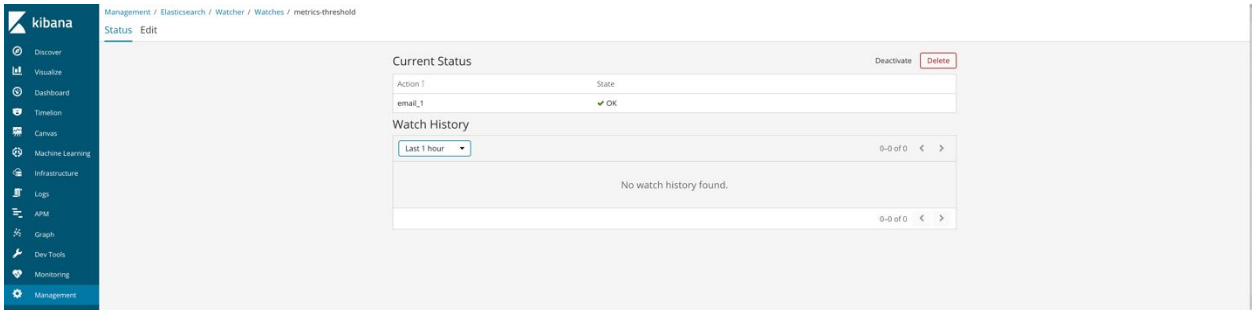
Watches

ID	Name	State	Comment	Last Fired	Last Triggered
55ac05fa-7fa2-4369-b3de-0923702...	metrics-threshold	✓ OK			

1-1 of 1

55ac05fa-7fa2-4369-b3de-09237024ddd1

Click on Deactivate button to turn off the watch for now.



Management / Elasticsearch / Watcher / Watches / metrics-threshold

Current Status

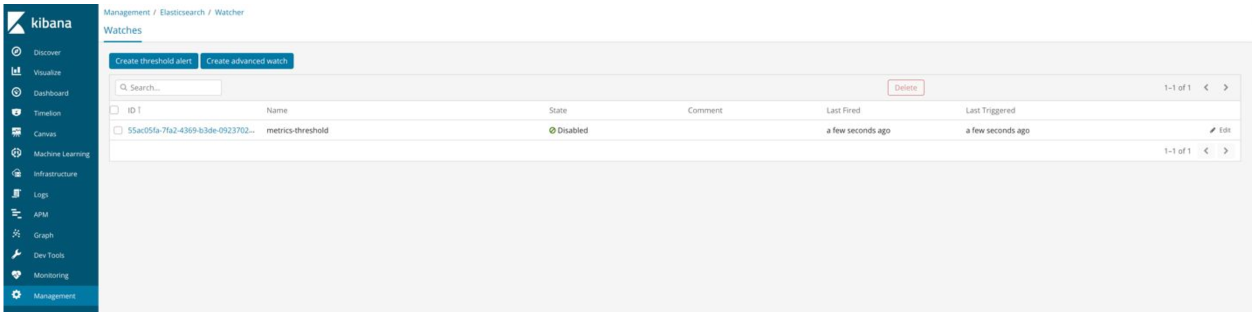
Action	State
email_1	✓ OK

Watch History

0-0 of 0

No watch history found.

5. Go back to the main Watcher screen again. This time click on “Create advanced watch”.



Management / Elasticsearch / Watcher

Watches

ID	Name	State	Comment	Last Fired	Last Triggered
55ac05fa-7fa2-4369-b3de-0923702...	metrics-threshold	Disabled		a few seconds ago	a few seconds ago

1-1 of 1

You will end up on the screen where you can enter any query again Elasticsearch and alert on it. This gives you a lot of flexibility to create whatever alert based on the data you have. The way we describe this functionality is “If you can search on it, you can alert on it”.

Imagine you would like to get notified if the past month you had more that 1000 accesses from an IP that you suspect is trying to do something malicious with your site.

First, specify how often you want it to run:

```
{
  "trigger": {
    "schedule": {
      "interval": "1d"
    }
  }
```

Then the search:

```
"input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "filebeat*"
        ],
        "types": [],
        "body": {
          "size": 0,
          "query": {
            "bool": {
              "must": {
                "match": {
                  "nginx.access.remote_ip": "1.190.172.233"
                }
              },
              "filter": {
                "range": {
                  "@timestamp": {
                    "gte": "now-30d/d",
                    "lt": "now/d"
                  }
                }
              }
            }
          }
        }
      }
    }
  }
```

Now you need to specify the condition:

```
"condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 1000
      }
    }
  }
```

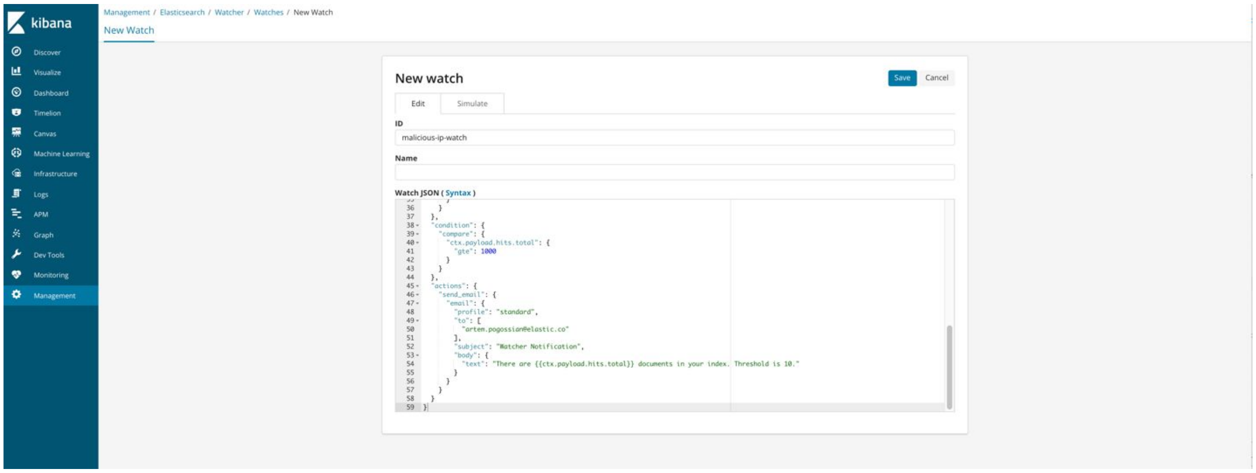
And action:

```
"actions": {
    "send_email": {
      "email": {
        "profile": "standard",
        "to": [
          "artem.pogossian@elastic.co"
        ],
        "subject": "Watcher Notification",
        "body": {
          "text": "There are {{ctx.payload.hits.total}} documents in your index. Threshold is 1000."
        }
      }
    }
  }
```

Combining all of that together we get the following watch:

```
{
  "trigger": {
    "schedule": {
      "interval": "1d"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "filebeat*"
        ],
        "types": [],
        "body": {
          "size": 0,
          "query": {
            "bool": {
              "must": {
                "match": {
                  "nginx.access.remote_ip": "1.190.172.233"
                }
              },
              "filter": {
                "range": {
                  "@timestamp": {
                    "gte": "now-30d/d",
                    "lt": "now/d"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gte": 1000
      }
    }
  },
  "actions": {
    "send_email": {
      "email": {
        "profile": "standard",
        "to": [
          "artem.pogossian@elastic.co"
        ],
        "subject": "Watcher Notification",
        "body": {
          "text": "There are {{ctx.payload.hits.total}} documents in your index. Threshold is 10."
        }
      }
    }
  }
}
```

Copy and paste the JSON above into Watch JSON window and give your watch a name.



ID

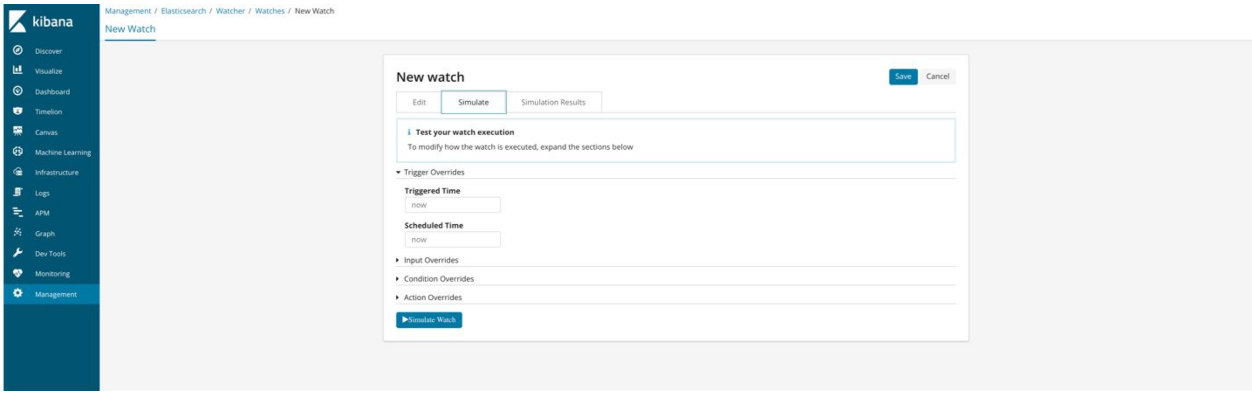
malicious-ip-watch

Name

Watch JSON (Syntax)

```
      }
    },
    "condition": {
      "compare": {
        "ctx.payload.hits.total": {
          "gte": 1000
        }
      }
    },
    "actions": {
      "send_email": {
        "email": {
          "profile": "standard",
          "to": [
            "artem.pogossian@elastic.co"
          ],
          "subject": "Watcher Notification",
          "body": {
            "text": "There are {{ctx.payload.hits.total}} documents in your index. Threshold is 10."
          }
        }
      }
    }
}
```

Before saving it click on Simulate and click on Simulate Watch test your watch.



Test your watch execution

To modify how the watch is executed, expand the sections below

▾ Trigger Overrides

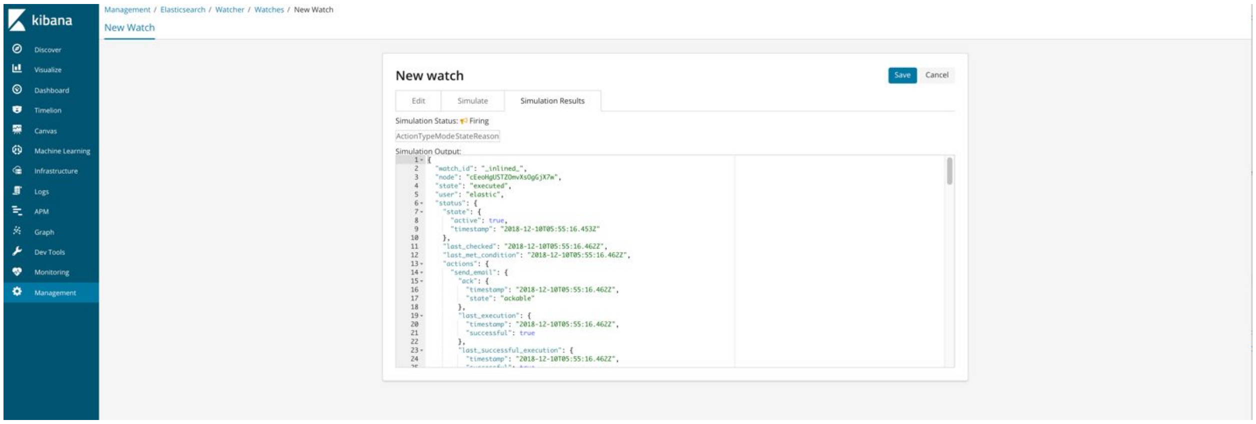
Triggered Time

now

Scheduled Time

now

Watch is shown as "Firing" which means that the condition we've specified is being met after the query gets executed.

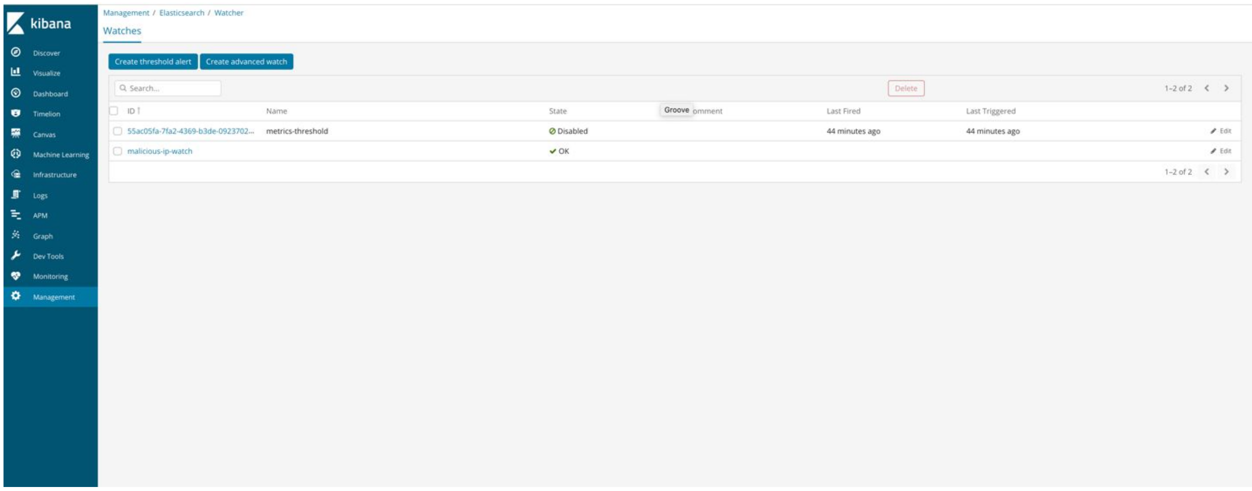


Simulation Status: Firing

Simulation Output:

```
{
  "watch_id": "_inlined_",
  "node": "cEeoHgUSTZOmvXsOgGjX7w",
  "state": "executed",
  "user": "elastic",
  "status": {
    "state": {
      "active": true,
      "timestamp": "2018-12-10T05:55:16.453Z"
    },
    "last_checked": "2018-12-10T05:55:16.462Z",
    "last_met_condition": "2018-12-10T05:55:16.462Z",
    "actions": {
      "send_email": {
        "ack": {
          "timestamp": "2018-12-10T05:55:16.462Z",
          "state": "ackable"
        },
        "last_execution": {
          "timestamp": "2018-12-10T05:55:16.462Z",
          "successful": true
        },
        "last_successful_execution": {
          "timestamp": "2018-12-10T05:55:16.462Z",
```

Click on Save button to save the watch.



ID	Name	State	omment	Last Fired	Last Triggered	
55ac05fa-7fa2-4369-b3de-0923702...	metrics-threshold	Disabled		44 minutes ago	44 minutes ago	Edit
malicious-ip-watch		✓ OK				Edit