

Elastic Lab

Let's explore the Elastic Stack

Table of Contents

Section 1: Build an Elastic Cluster
Section 2: Setup Linux
Section 3: Metricbeat
Section 4: Filebeat
Section 5: Alerting
Section 6: Machine Learning
Section 7: Conclusion


Section 1: Build an Elastic Cluster

- 이 Workshop 의 Elastic Stack 버전은 6.5.2 를 기준으로 되어 있습니다. Elasticsearch, Kibana 및 Beats 는 버전이 맞아야 하므로 Elasticsearch 최신 버전의 클러스터를 구성한 경우에는 Beats 도 최신 버전을 사용해야 하므로 이 부분을 반드시 체크하시기 바랍니다. 현재 어떤 버전으로 운영하고 있는 지 Lab 을 진행하는 동안 숙지하시기 바랍니다.

In this section, we will provision an Elastic Cluster using **cloud.elastic.co**.

1. Sign up for the Elastic Cloud Trial

Visit <https://cloud.elastic.co> and click "Sign up now"




Email

Password

[Log in](#) [Forgot password?](#)

Don't have an account? [Sign up now.](#)

2. Enter your business email (no credit card is required). The cluster you build will be hosted for free for 14 days.



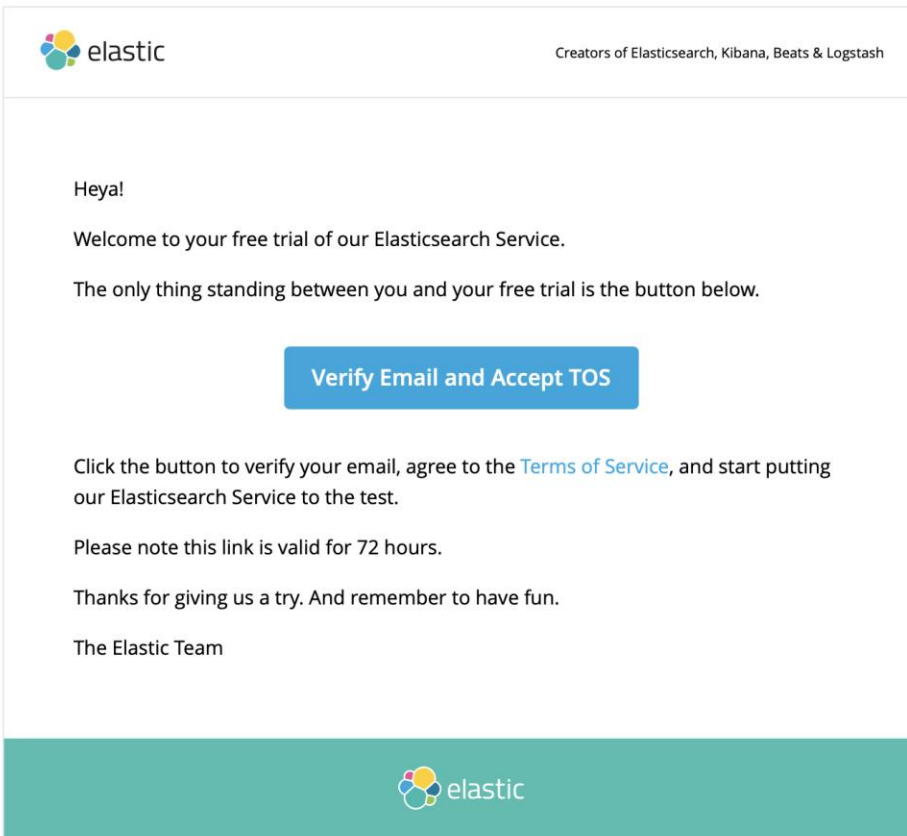
Deploy Elasticsearch in 3 Minutes or Less

14-day trial. All free. No credit card required.

Business Email Address:

By submitting you agree to the [Elastic Cloud Standard Terms and Policies](#) and agree to receive occasional emails.

3. Check your email to verify your account.



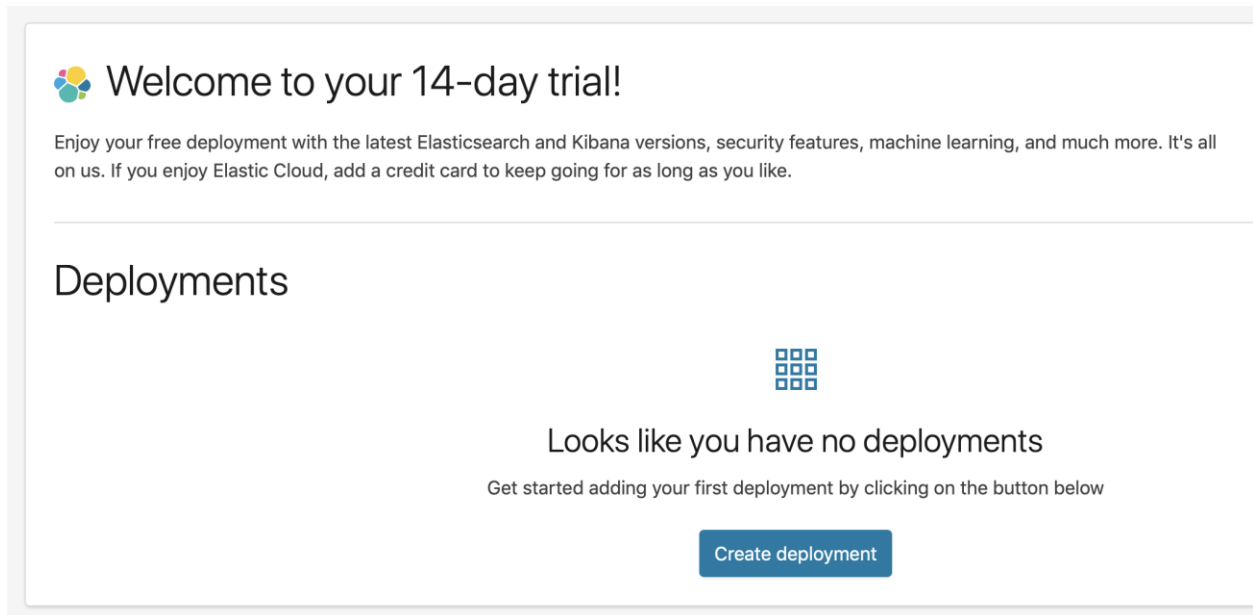
4. Log in and create give your account a strong password.

Note: The form will have what looks like a password already filled in. Click the input box and it will disappear. Enter a new *strong* password to secure your account.

Tip: You will have to manage 2 passwords in this lab. They will be different. Securely note them somewhere so you can easily copy & paste them as needed.

A form titled "Welcome to Elastic Cloud" on a light gray background. It has two input fields, each with a lock icon on the left and a series of dots representing a password. The first field is labeled "Password" and the second is labeled "Repeat password". Below these fields is a blue button with white text that says "Set password".

5. You should now be looking at the dashboard. Click “Create deployment”.



6. Give your deployment a name.

1 Name your deployment

Give your deployment a name

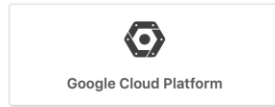
Workshop

7. Pick the cloud platform of your choice.

You may pick AWS or GCP. Once your provider is selected. You may pick a Region.

2 Select a cloud platform

Pick your cloud and let us handle the rest. No additional accounts required.



3 Select a region

US East (N. Virginia)

US West (N. California)

US West (Oregon)

EU (Ireland)

Asia Pacific (Singapore)

Asia Pacific (Tokyo)

South America (Sao Paulo)

Asia Pacific (Sydney)

EU (Frankfurt)

8. Pick the latest version of Elastic. It will be newer than 6.5.2 as shown in the screenshot.

4 Set up your deployment

Elastic Stack version

6.5.2 [Edit](#)

☐ Select a deployment to restore from its latest snapshot

9. Select the **I/O Optimized**:

5 Optimize your deployment

I/O Optimized
Recommended
Use for search and general all-purpose workloads. Includes a balance of compute, memory, and storage.
[Default specs](#)

Compute Optimized
Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage.
[Default specs](#)

Memory Optimized
Perform memory-intensive operations efficiently, including workloads with frequent aggregations.
[Default specs](#)

Hot-Warm Architecture
Use for time-series analytics and logging workloads that benefit from automatic index curation.
[Default specs](#)

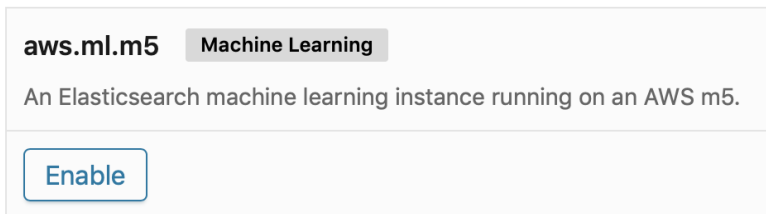
Elastic Cloud supports many more options to cater to your specific use case such as hot-warm architecture optimized for logging, compute-focused setup optimized for analytics etc. [Learn more ...](#)

10. Click “Customize deployment”. We want to make a few more changes before creating the deployment.



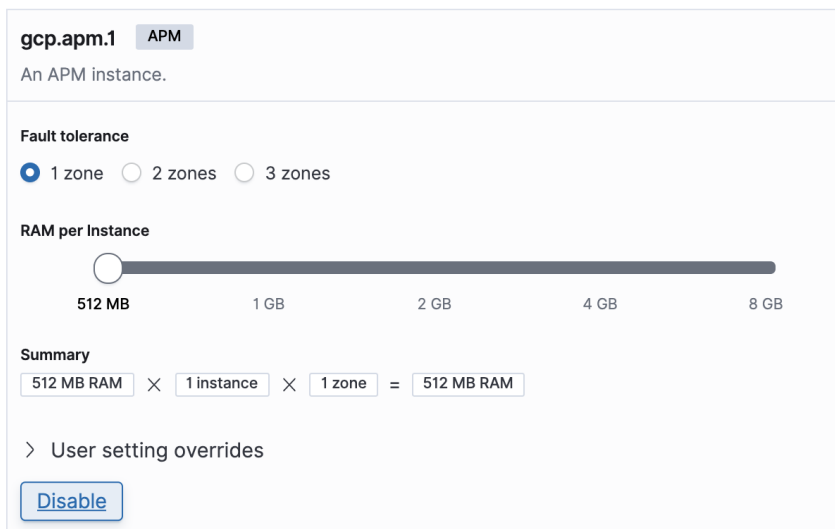
12. Turn on “Machine Learning” by clicking “Enable”.

 **Machine Learning** 1 configuration



13. Turn off “APM” by clicking “Disable”.

 **APM** 1 configuration



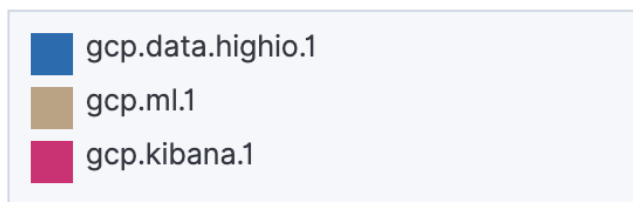
Your cluster’s Architecture should look similar to this:

Architecture

Zone 1



Zone 2





18. Your cluster will begin to spin up. It will take several minutes for your cluster to spin up.

[Elasticsearch](#) Kibana

Generated user

You can use the credentials below to login to Elasticsearch or Kibana. Make sure to save the password somewhere as this is the only time we can show it to you.

Username elastic**Password** wM0D6RBSjA4UG3xnqC4qzhZh **Cloud ID** Workshop:dXMtZWZdC0xLmF3cy5mb3VuZC5pbyQ3YmIxYTU5OWYwODk0OT
EzYWU3M2ExNWVjNzI2Mjd1ZCQyOGJkZTNhMzY4ZjM0ODViODJhMDM1M2QxM
j1mNWU0YWw== 

Get started with Beats and Logstash quickly. The Cloud ID simplifies sending data to your cluster on Elastic Cloud. [Learn more ...](#)

Updating deployment configuration

- ☒ Started 23 seconds ago
☐ Waiting until instances are running

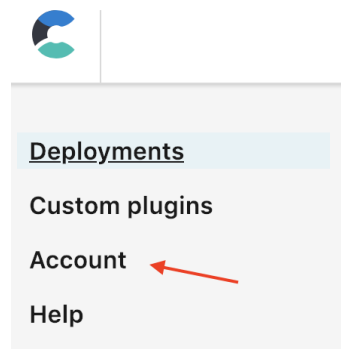
[Cancel](#)

Important: Copy the auto generated Password by clicking the clipboard icon. We'll need it in the future and it won't be shown again after this screen.

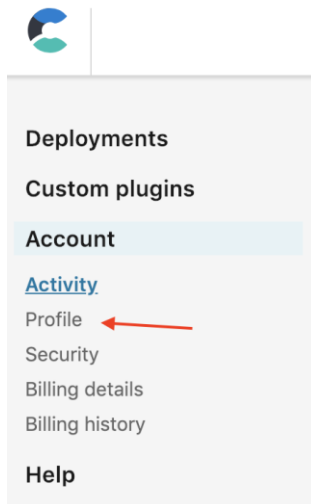
Note: This is your *cluster's* password, *not* your account password to log into cloud.elastic.co. You should now have 2 passwords. Securely record them somewhere.

19. While the cluster is being provisioned, we will add your email to a whitelist so we can send Alerts to it later in the lab.

20. Click on "Account".



21. Click on "Profile".



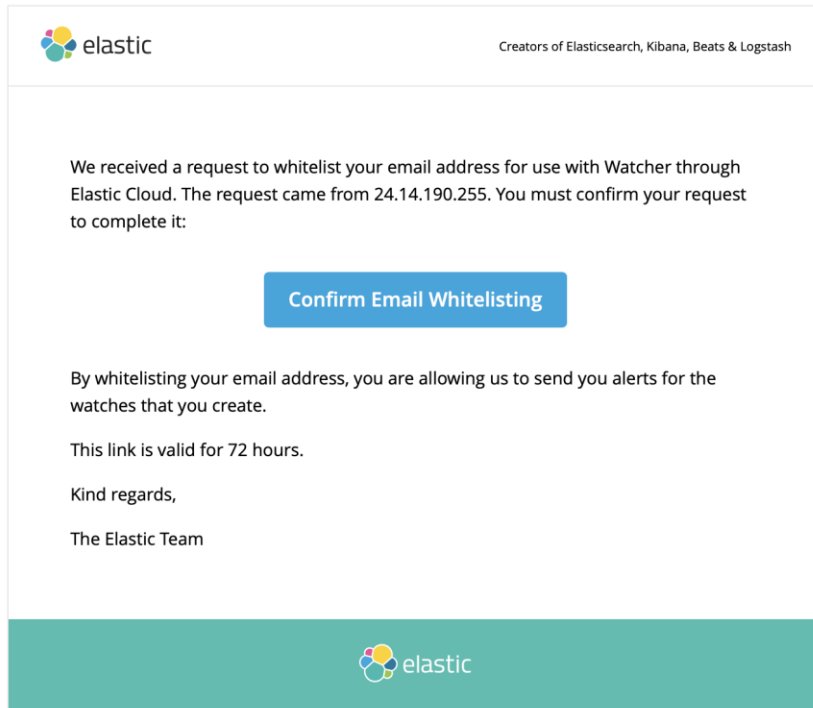
22. Add your email to “Monitoring email whitelist”.

Monitoring email whitelist

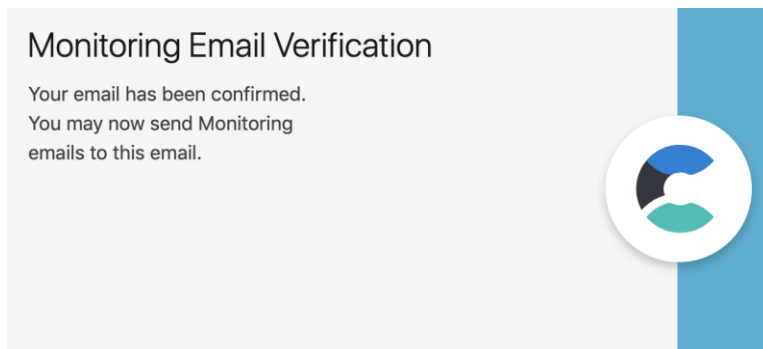
Whitelist an email address that should receive monitoring alerts. You must confirm the email address to start receiving these alerts.

Add

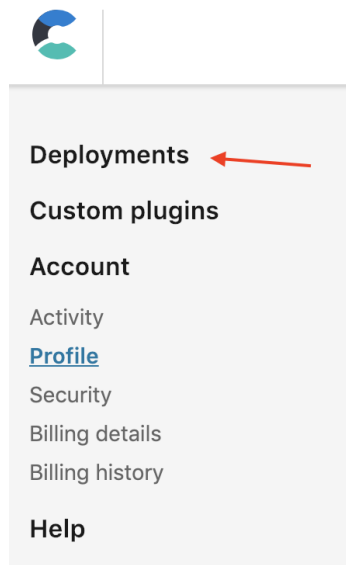
23. Check your email for a confirmation and click on the button “Confirm Email Whitelisting.”



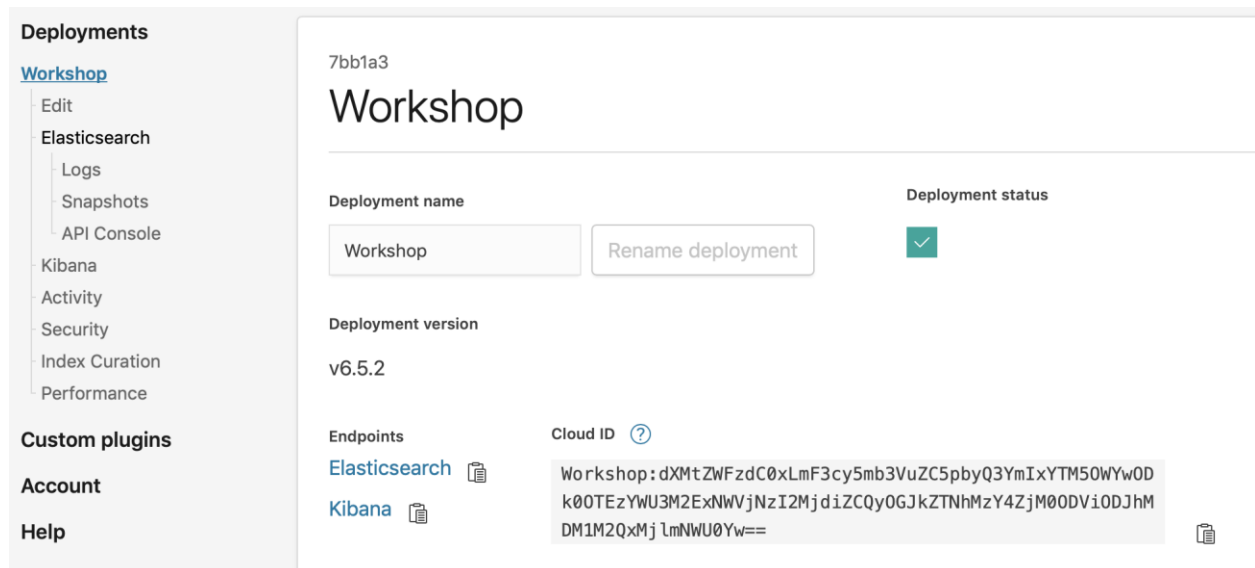
24. You should see the following confirmation in your web browser.



25. Let's check on the state of your cluster. Click on "Deployments".

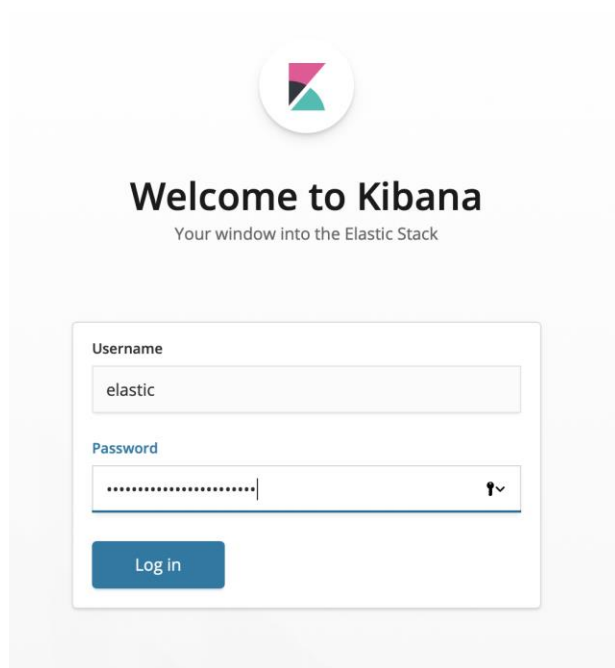


26. When the cluster is ready, select your cluster name in the top left.

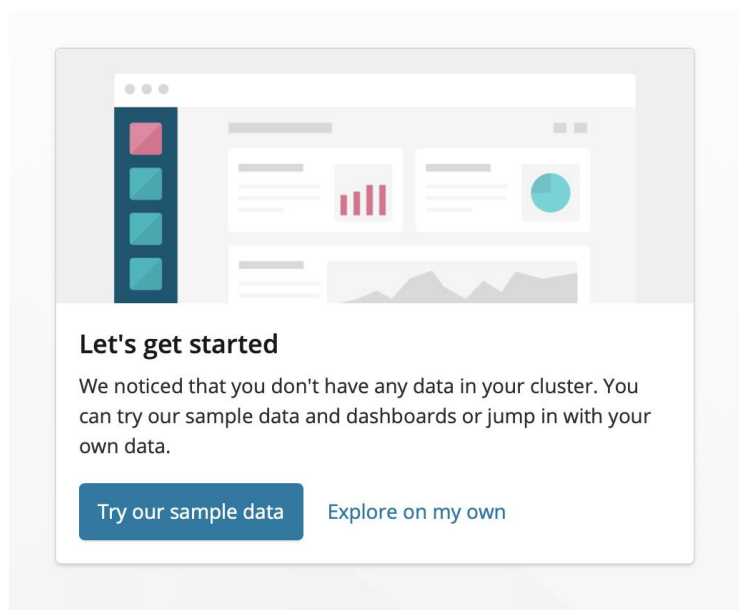


27. Click on Kibana to launch Kibana in a new tab. Log in with the username “elastic” and your password.

Note: Use the long password you copied in Step 18 that is for your cluster. Do *not* use your cloud.elastic.co account password.



28. You are now in Kibana. Click on “Try our sample data” and load one or more of the sample data sets. Each data set comes with a Dashboard and Canvas. The data loaded is isolated so it will not affect the rest of the lab.



29. Congratulations! In the next section we'll put the Elastic Stack to work.

Section 3: Metricbeat

- Metricbeat 를 인스톨하는 방법은 APT, YUM 이외에도 다양한 방법이 있습니다.

인스톨 레퍼런스(<https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-installation.html>) 와 LAB1 문서를 참조하시기 바랍니다.

- Add the beats repositories : <https://www.elastic.co/guide/en/beats/metricbeat/current/setup-repositories.html> 참조

In this section, we will install Metricbeat to monitor our OS “system” metrics.

1. Install metricbeat.

```
$ sudo apt-get install metricbeat
```

2. Edit the metricbeat.yml file to point it to Logstash.

```
$ sudo nano /etc/metricbeat/metricbeat.yml
```

Look for the “Elastic Cloud” section and comment out “cloud.id” (line 81) and the “cloud.auth” line (line 85) below it.

Tip: In nano, use the keyboard shortcut “esc-g” to jump to line 81.

Add your Cloud ID and your cluster’s credentials in the format shown:

```
#===== Elastic Cloud

# You can find the `cloud.id` in the Elastic Cloud web UI.
cloud.id: your_cloud_id

# The format is `<user>:<pass>`.
cloud.auth: elastic:your_cluster_password
```

Hit control-x to exit nano, and follow the prompts to save your file.

3. Load the index templates and dashboards.

```
$ sudo metricbeat setup
```

This command takes about 20 seconds to run. The output should match:

```
Loaded index template
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

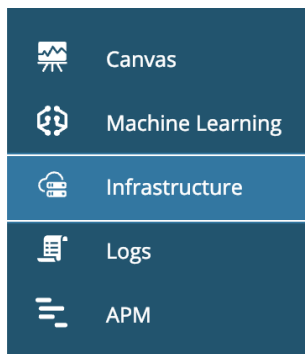
4. Configure metricbeat to start on reboot.

```
$ sudo systemctl enable metricbeat
```

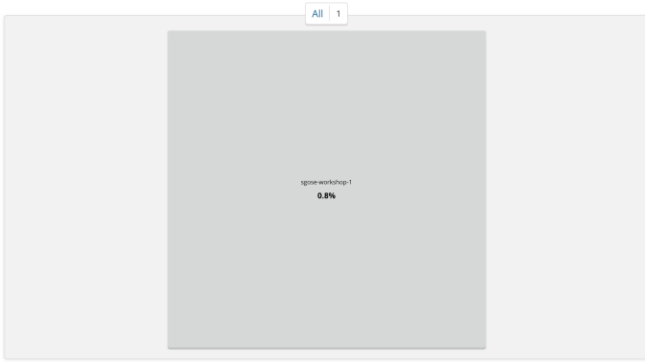
5. Start metricbeat.

```
$ sudo service metricbeat start
```

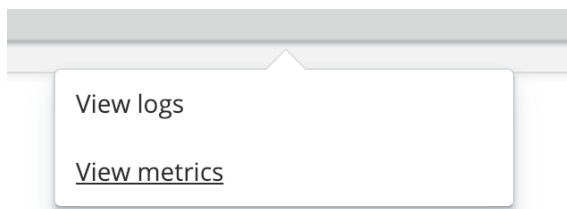
6. Go to your Kibana instance and click on the “Infrastructure” tab.



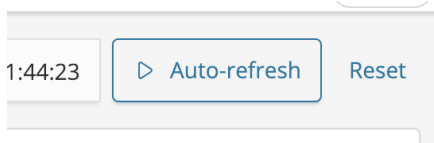
You should see your host show up as a tile.



7. Click on your host and then “View metrics”



8. Click on “Auto-refresh”.



9. You should see metrics flowing in.

Host

Overview

CPU Usage

Load

MemoryUsage

Network Traffic

sgose-workshop-1



12/23/2018 10:46:40



12/23/2018 11:4

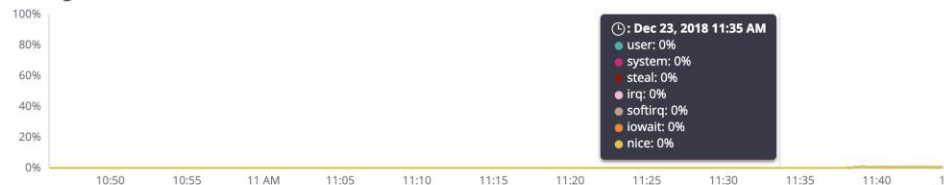
|| Stop refreshing

Reset

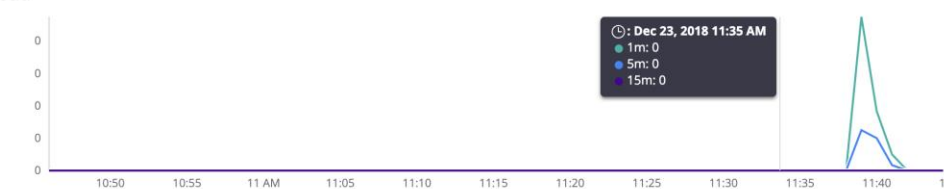
Host Overview



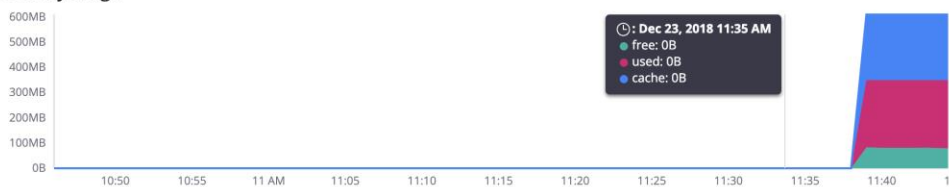
CPU Usage



Load



MemoryUsage



10. Congratulations! You have successfully installed and configured Metricbeat.

Section 4: Filebeat

In this section, we will install Filebeat to grab logs from `/var/log/*.log`

1. Install filebeat.

```
$ sudo apt-get install filebeat
```

2. Edit the filebeat.yml file to point it to Logstash.


```
$ sudo nano /etc/filebeat/filebeat.yml
```

Look for the “Elastic Cloud” section and comment out “cloud.id” (line 137) and “cloud.auth” (lines 141).

Tip: In nano, use the keyboard shortcut “esc-g” to jump to line 137.

Add your Cloud ID and your cluster’s credentials in the format shown:

```
#===== Elastic Cloud

# You can find the `cloud.id` in the Elastic Cloud web UI.
cloud.id: your_cloud_id

# The format is `:<pass>`.
cloud.auth: elastic:your_cluster_password
```

Hit control-x to exit nano, and follow the prompts to save your file.

3. View the list of modules enabled. Notice that there are no modules enabled.

```
$ sudo filebeat modules list
Enabled:

Disabled:
apache2
auditd
elasticsearch
haproxy
icinga
iis
kafka
kibana
logstash
mongodb
mysql
nginx
osquery
postgresql
redis
suricata
```

```
system
traefik
```

4. Enable the “system” module.

```
$ sudo filebeat modules enable system
```

Now you should see:

```
$ sudo filebeat modules list
Enabled:
system

Disabled:
apache2
auditd
elasticsearch
haproxy
...
```

5. Load the index templates and dashboards.

```
$ sudo filebeat setup
```

This command takes about 20 seconds to run. The output should match:

```
Loaded index template
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
```

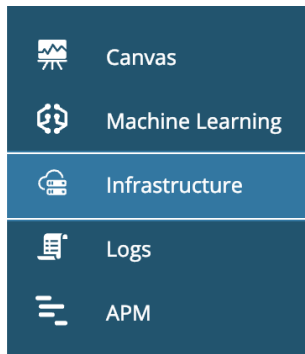
6. Configure filebeat to start on reboot.

```
$ sudo systemctl enable filebeat
```

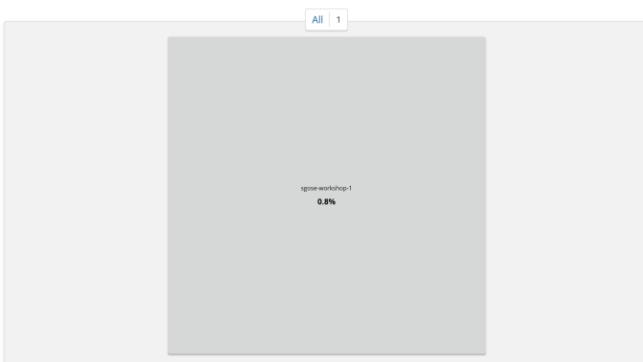
7. Start filebeat

```
$ sudo service filebeat start
```

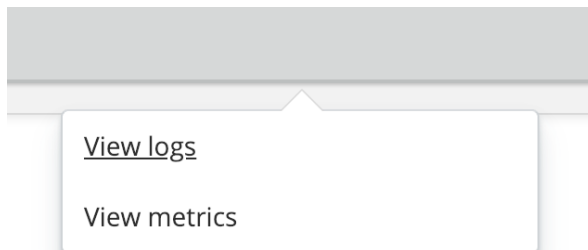
8. Go to your Kibana instance and click on the “Infrastructure” tab.



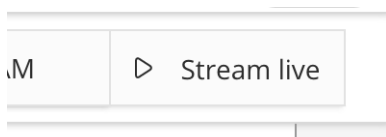
9. You should see your host tile.



10. Click on your host and then “View logs”



11. Click on “Stream live”.



You should see a live tail of all your log output flowing in. There are two log files streaming in: syslog and auth.log. We'll need to filter them to isolate a single one.

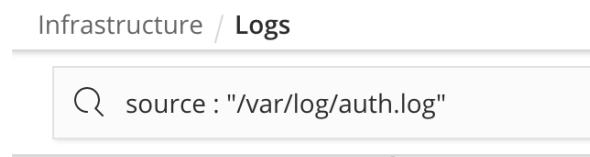
12. Filter the stream to just show auth.log by typing the following in the search bar.

- 최신 버전의 Beats 는 Elastic Common

Schem(<https://www.elastic.co/guide/en/ecs/current/index.html>) 에 맞춰서 필드네임과 타입이 업그레이드 되었습니다. log.file.path: "/var/log/auth.log"

```
source : "/var/log/auth.log"
```

Your search bar should look like the following.



13. Let's try an SSH login attempt to get the auth.log file to update. Replace IP_ADDRESS with the Public IP address of your lab machine (output from Step 13 above).

Note: Be sure to type "yes" when prompted by SSH.

```
$ ssh hAx0R@IP_ADDRESS
...
Are you sure you want to continue connecting (yes/no)? yes
```

15. Switch back to Kibana to see your attempted SSH login.

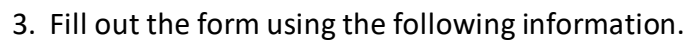
2018-12-26 08:30:00.459	Dec 26 14:29:58 ip-172-31-30-159 sshd[8462]: input_userauth_request: invalid user hAx0R [preauth]
2018-12-26 08:30:00.459	Dec 26 14:29:58 ip-172-31-30-159 sshd[8462]: Connection closed by 35.158.221.127 port 52020 [preauth]
2018-12-26 08:30:00.459	Dec 26 14:29:58 ip-172-31-30-159 sshd[8462]: Invalid user hAx0R from 35.158.221.127

16. Congratulations! You have successfully installed Filebeat and began threat-hunting.

Section 5: Alerting

In this section, we will explore the logs & metrics streaming in. We'll set up Alerts to notify us when there's an issue on a machine.

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




Create a new threshold alert

Send an alert when a specific condition is met. This will run every 1 minute.


Name

High CPU



Indices to query


metricbeat-* 

Time field

@timestamp 

Run watch every

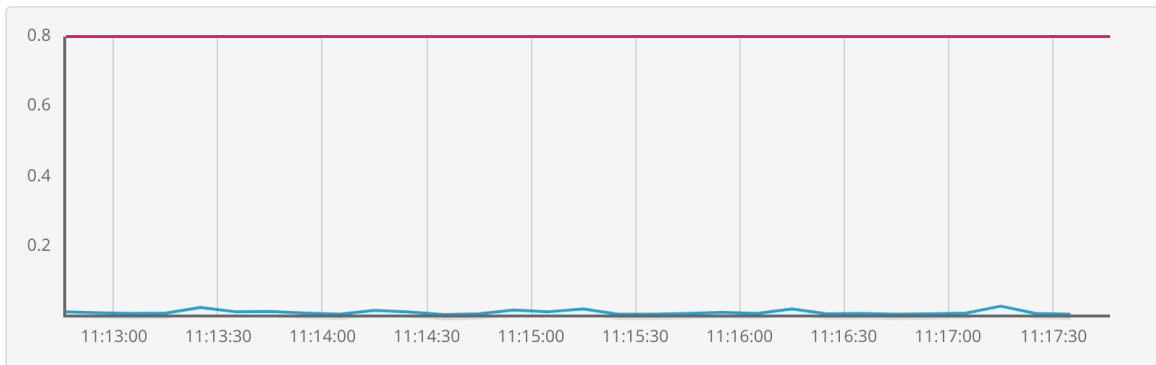
1  


minutes 


Use * to broaden your search query


Matching the following condition

WHEN average() OF system.cpu.total.pct OVER all documents IS ABOVE 0.8 FOR THE LAST 1 minute



 E-mail
Send out an e-mail from your server.

 Logging
Add a new item to the logs.

 Slack
Send a message to a slack user or channel.

Will perform 1 action once met

Add new action

▼  E-mail

To e-mail address

YOUR_EMAIL_ADDRESS

Subject

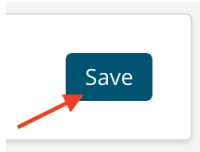
Watch [{{ctx.metadata.name}}] has exceeded the threshold

Body

High CPU Alert

Remove E-mail Action

Test fire an e-mail now

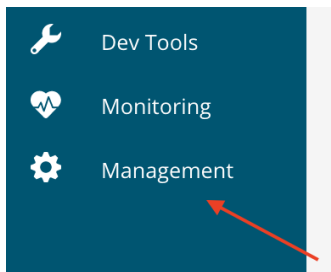


4. Now let's generate some load to get this Alert to trigger.
5. Go to your Linux host and run the following command.

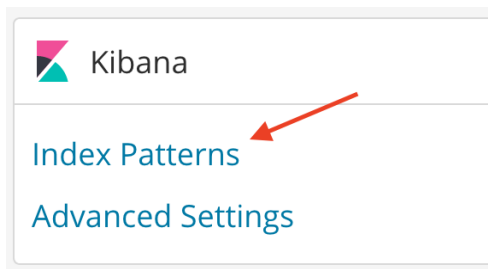
```
$ dd if=/dev/zero of=/dev/null
```

This command will generate a lot of load on your linux host. It will not return, so let it run for 2-3 minutes. During this time, you should receive a few emails, alerting you to the high load.

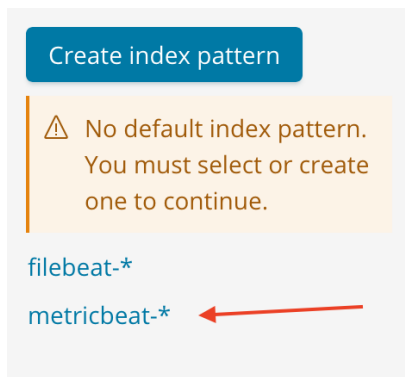
6. Switch back to Kibana and click on "Management".



7. Click on "Index Patterns" in the Kibana section.



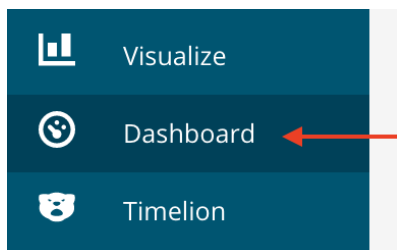
8. Click on the "metricbeat-*" index pattern.



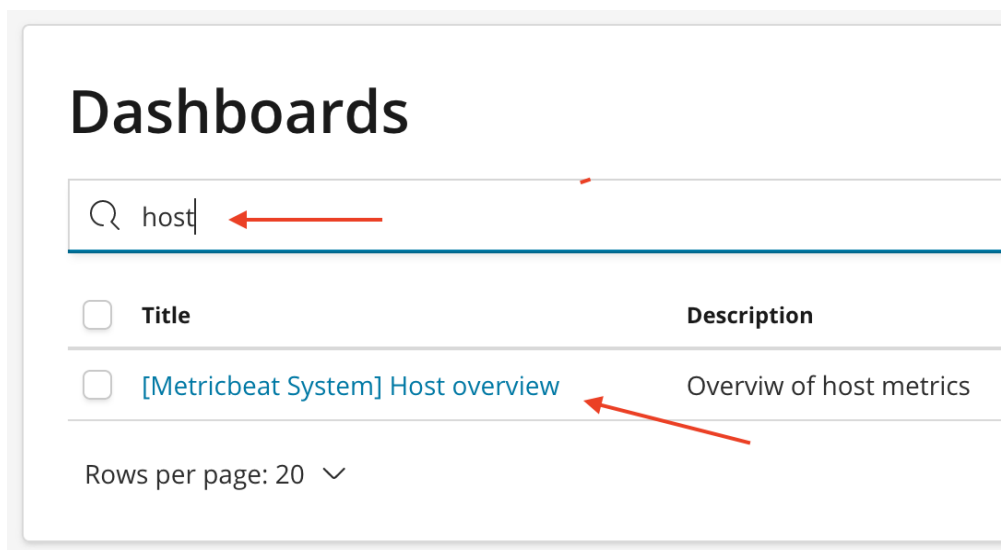
9. Click on the star icon which will set this index pattern as the default.



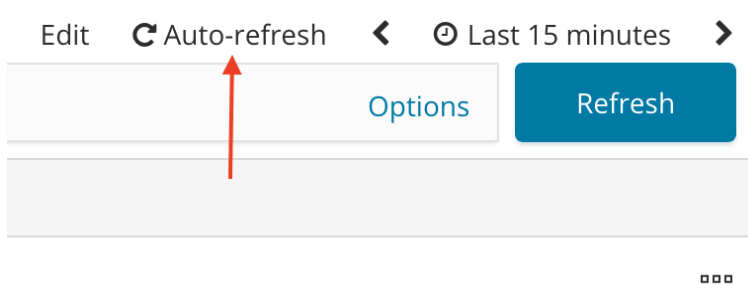
10. Click on the “Dashboard” tab in Kabana.



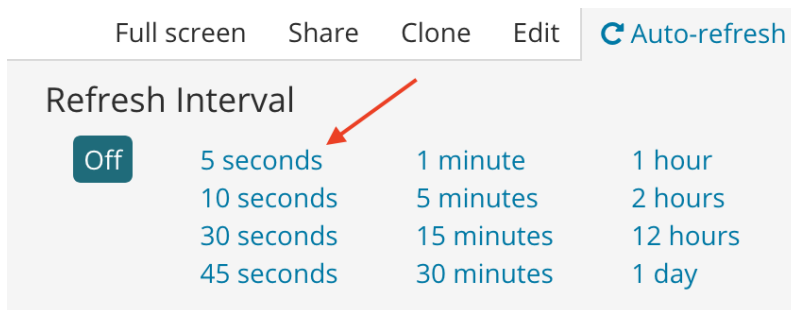
11. Search for “host” and click on the [Metricbeat System] Host overview link.



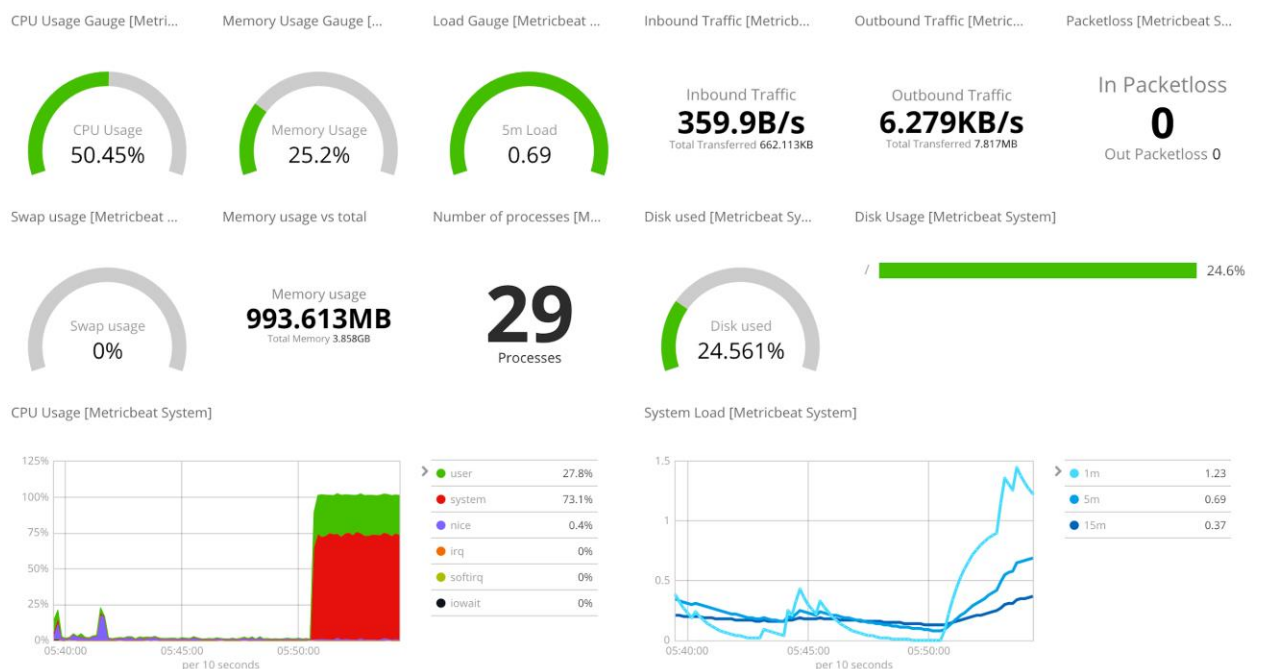
12. Click on “Auto-refresh” at the top of the page.



13. Click on “5 seconds” in the dropdown.



14. Verify you see the CPU Load has increased.



15. Verify several emails in your inbox alerting you to the high CPU load.

Watch [High CPU] has exceeded the threshold Inbox x



Watcher Alert <noreply@watcheralert.found.io>

to me ▾

High CPU Alert



--

This email is sent via a Watcher alert on a Found hosted cluster. Your email address was previously whitelisted. To stop receiving any Watcher alerts, click on the link below:
nd.io/u/eJwVxDEOwyAMAMDXhl3lBoNhYMgfOnVBCZgWKQ1Sw_9V9YariWsDr3qSz97PjDn36-yX1JyJBW7H4TQWZk0Rmo4UQle4OxfG8V_tALzU71TDN57KGygEd9qJBRib50F76oLqL7pLmPO9TVuWQjk3O_Zy1qGmmkx2w_8Kixb

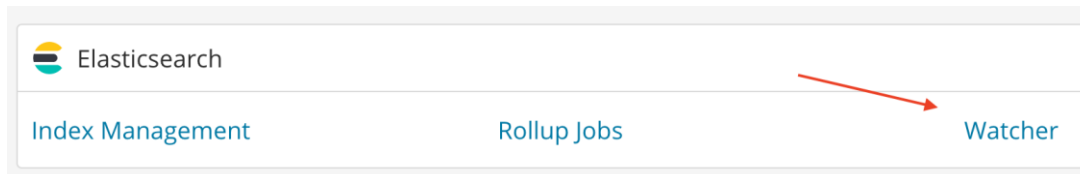
16. Kill the “dd” command that is generating a high CPU load by hitting **control-c**.

```
$ dd if=/dev/zero of=/dev/null  
^C  
12651700+0 records in  
12651699+0 records out  
6477669888 bytes (6.5 GB, 6.0 GiB) copied, 3.73029 s, 1.7 GB/s
```

Note that threshold Alerts are great for keeping an eye on any kind of metric, like disk space filling up, extended network transfers, low uptime, and more.

Next, we'll setup an Alert to notify us of any login attempts through SSH.

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



18. Back in Kibana, click the “Create advanced watch” button. You might need to navigate back to the Management tab and then Watcher.

[Management](#) / [Elasticsearch](#) / [Watcher](#)

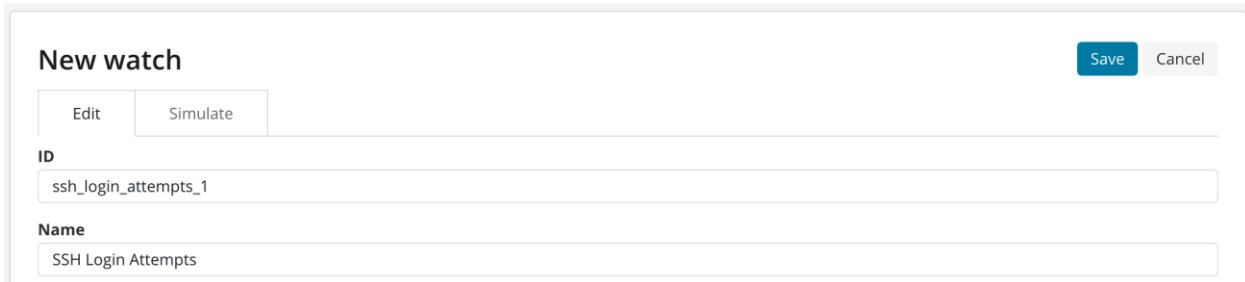
[Watches](#)

Create threshold alert

Create advanced watch

We're going to use a query this time, to find any SSH login attempts.

19. Insert the following for ID and Name.



New watch Save Cancel

Edit Simulate

ID
ssh_login_attempts_1

Name
SSH Login Attempts

20. Copy and paste the following JSON into the "Watch JSON" text area of your Alert.

The motto with Elastic Alerting is, "If you can query it, you can Alert on it."

Take a few minutes to read through this JSON. An Alert is constructed of 4 sections:

- Schedule
- Query
- Condition
- Actions

See if you can identify these sections in the alert below.

Note: Replace YOUR_EMAIL_ADDRESS in the JSON snippet below with the email address you whitelisted in Section 1, Step 22 of this lab.

```
{
  "trigger": {
    "schedule": {
      "interval": "1m"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "metricbeat-*"
        ]
      },

```

```

    "rest_total_hits_as_int": true,
    "body": {
      "size": 0,
      "query": {
        "bool": {
          "filter": {
            "range": {
              "@timestamp": {
                "gte": "now-1m",
                "lte": "now",
                "format":
"strict_date_optional_time||epoch_millis"
              }
            }
          }
        }
      },
      "aggs": {
        "metricAgg": {
          "avg": {
            "field": "system.cpu.total.pct"
          }
        }
      }
    }
  },
  "condition": {
    "script": {
      "source": "if (ctx.payload.aggregations.metricAgg.value >
params.threshold) { return true; } return false;",
      "lang": "painless",
      "params": {
        "threshold": 1.6
      }
    }
  },
  "actions": {

```

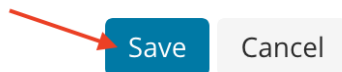
```

    "send_email": {
      "email": {
        "profile": "standard",
        "to": [
          "YOUR_EMAIL_ADDRESS"
        ],
        "subject": "[Elastic Alert] High-CPU Usage Alert",
        "body": {
          "text": "{{ctx.payload.aggregations.metricAgg.value}} %
High CPU USAGE"
        }
      }
    }
  }
}

```

21. Replace YOUR_EMAIL_ADDRESS in the JSON snippet you pasted with the email address you whitelisted in Section 1, Step 22 of this lab. If you don't, this alert won't work!

22. Click on "Save".



23. Now let's generate some load to get this Alert to trigger.

24. Check your email for an Alert.

25. Congratulations! You have successfully set up Alerts.

Though these examples are contrived, you can easily extend them to watch more interesting things in your environment. For some example alerts, visit:

<https://github.com/elastic/examples/tree/master/Alerting/Sample%20Watches>

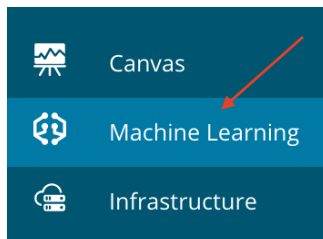
A great overview of Alerting (a.k.a., Watcher) is available here:

<https://www.elastic.co/guide/en/elastic-stack-overview/6.5/xpack-alerting.html>

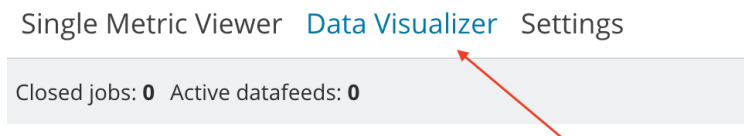
Section 6: Machine Learning

In this section, we will learn about Machine Learning. We're going to use the new "Data Visualizer" in Kibana to load data into an index and then analyze it.

1. Open Kibana and click on the Machine Learning tab.



2. Click on "Data Visualizer"



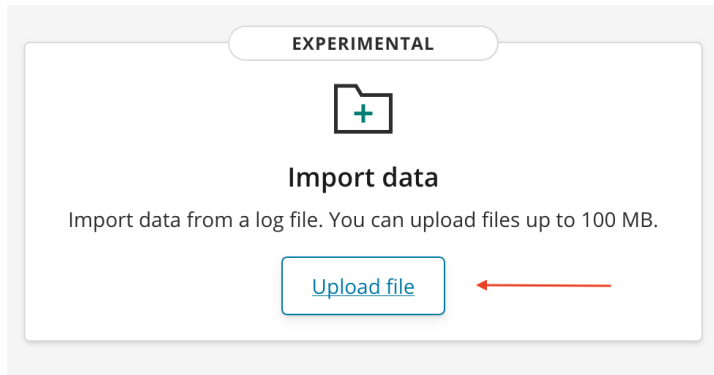
3. Click on the following link which will download a CSV file called "**flights.csv**" to your laptop. It contains all US Commercial flights between October and November 2017 (2 months).

Note: The file downloaded will be "flights.csv" and should be 33MB in size.

<https://bit.ly/elastic-data>

<https://github.com/codingogre/logging-workshop>

4. Upload the file into the Data Visualizer.

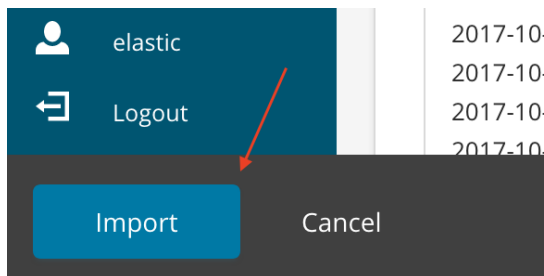


5. Drag and drop the file into the upload area or select it using a file picker.



Select or drag and drop a file

6. Click the “Import” button in the bottom left of the screen.



7. Import the data into an index named “flights”.

Import data

EXPERIMENTAL

[Simple](#) [Advanced](#)

Index name

flights

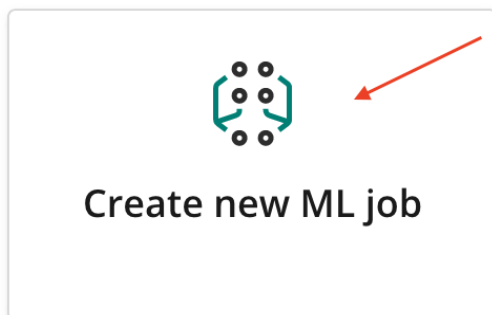
☒ Create index pattern

Import

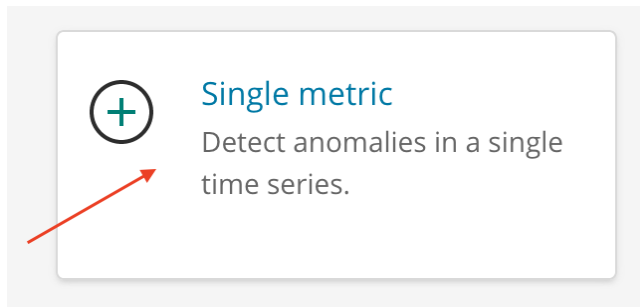
8. After clicking “Import”, you should see an “Import complete” confirmation.

✓ Import complete	
Index	flights
Index pattern	flights
Ingest pipeline	flights-pipeline
Documents ingested	933959

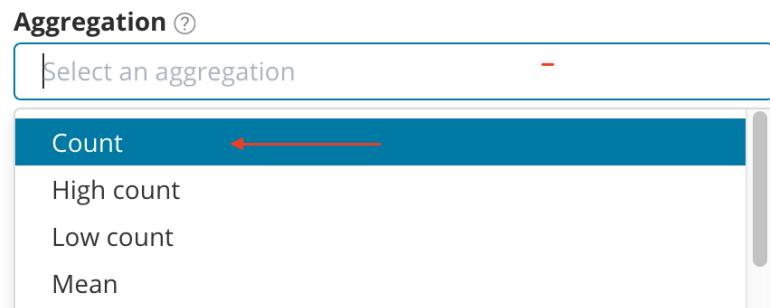
9. Click on “Create new ML job”.



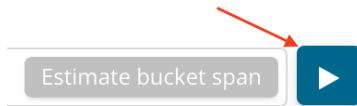
10. Click on “Single metric”.



11. For the Aggregation, select “Count”.



12. Click the Play button to see an overview of the data.



13. Name your job “flights” and click “Create Job”.

Name ?

flights ←

Description ?

Job description

Job Groups ?

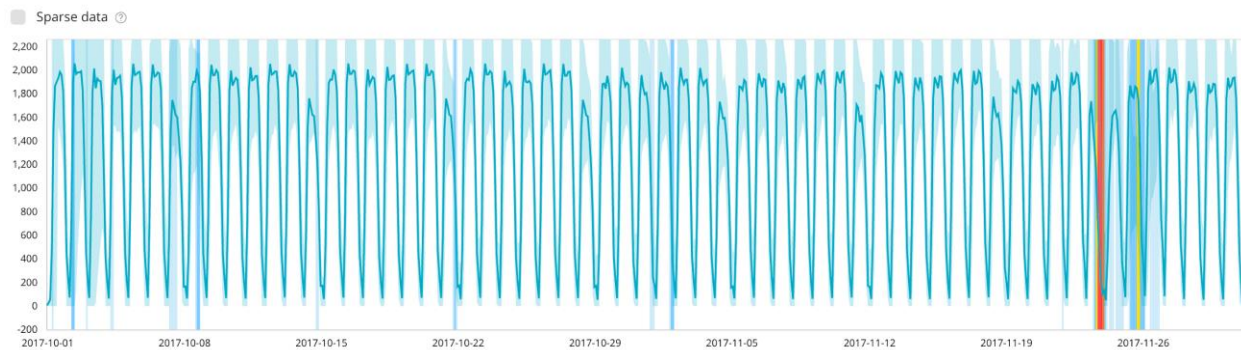
Job Group

▶ **Advanced** ?

Move to advanced job configuration

Validate Job ? Create Job

14. When your job finishes, you should see the data model filled in over the data stream.

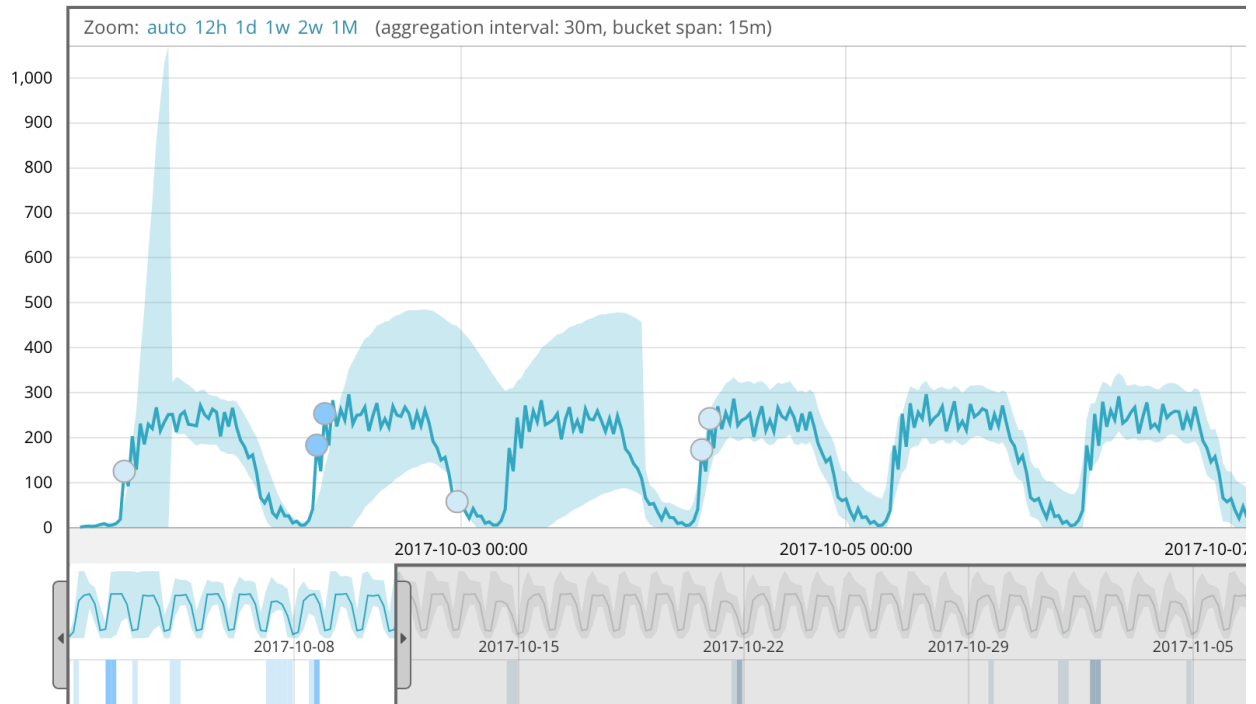


15. Click on “View Results”.

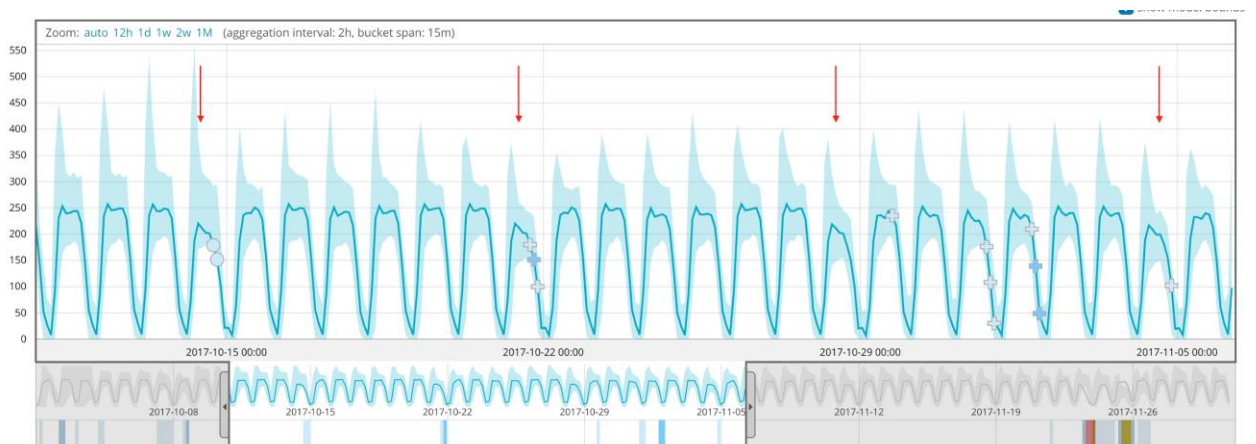
Job flights created ✓



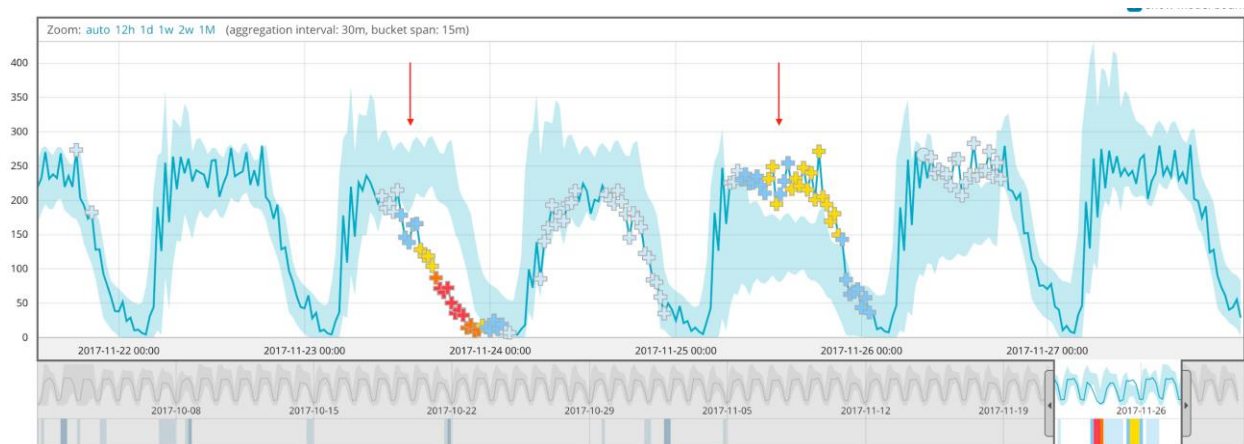
16. You should now be looking at the “Single Metric Viewer” in Kibana. Drag the time window to cover only the first week of data. Notice how the data model picks up a pattern after about 3 days.



17. Adjust the time window again to cover about 4 weeks worth of data. Can you pick out a weekly pattern in US Commercial flight activity? What day of the week always has less flights than the others?



18. Adjust the time window to look at the week starting on 11/22. Why is the detector throwing high anomaly scores on Thursday, 11/23? Why is it throwing high anomaly scores on Saturday, 11/25?



The power of Machine Learning with Elastic is you can let a machine watch hundreds, even thousands, of different data streams you're collecting. It will build a unique data model for each one. And when a given data stream starts to misbehave (from its past behavior), you can get an alert.

16. Congratulations! You have successfully used Machine Learning in Elastic.

Section 7: Conclusion

Thank you for taking the Elastic Workshop.

The cluster you provisioned in cloud.elastic.co will be hosted for free for 2 weeks.

Your lab Linux machine will be deleted after the lab ends.

You can retake this lab at home or work using any Linux, Windows, or Mac host. The instructions in this Lab are for Linux but you can also install Metricbeat, & Filebeat on Windows or Mac.

The Elastic Stack can be used for Monitoring, Analytics, SIEM, Search, and more. The flexibility of the Elastic Stack is what makes it so powerful. Let it empower you to find answers in your own environment.