

Elastic Lab

Let's explore the Elastic Stack

Table of Contents

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

Section 1: Build an Elastic Cluster


- Elastic Cluster 는 최신 버전(7.5)으로 구성하시기 바랍니다.

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.



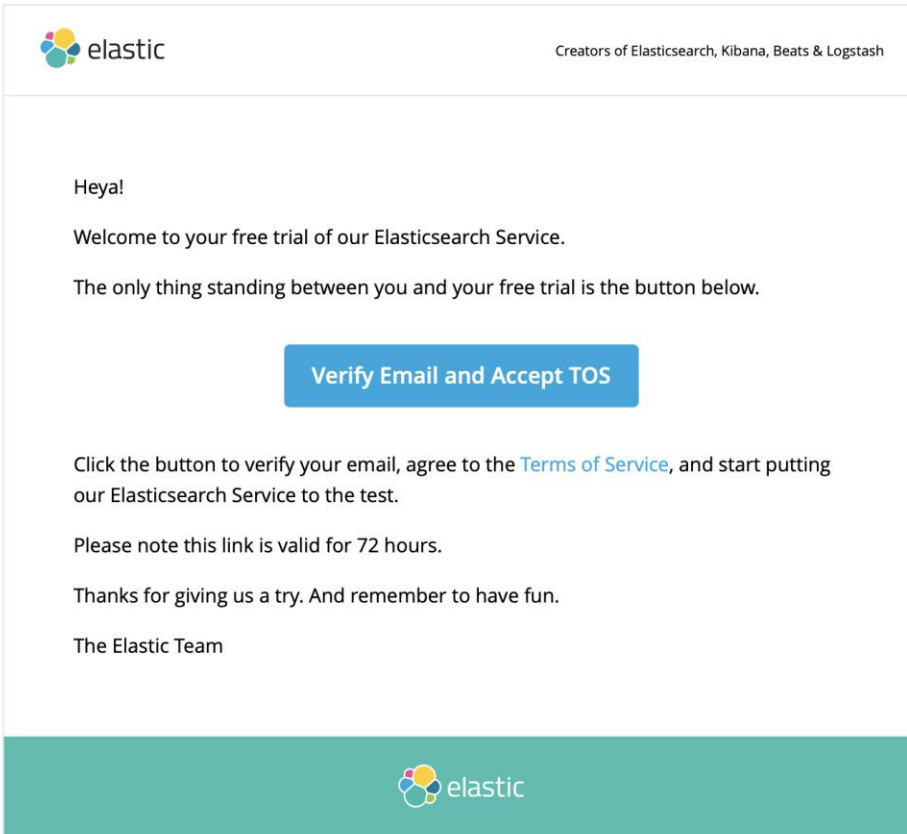
Deploy Elasticsearch in 3 Minutes or Less

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.



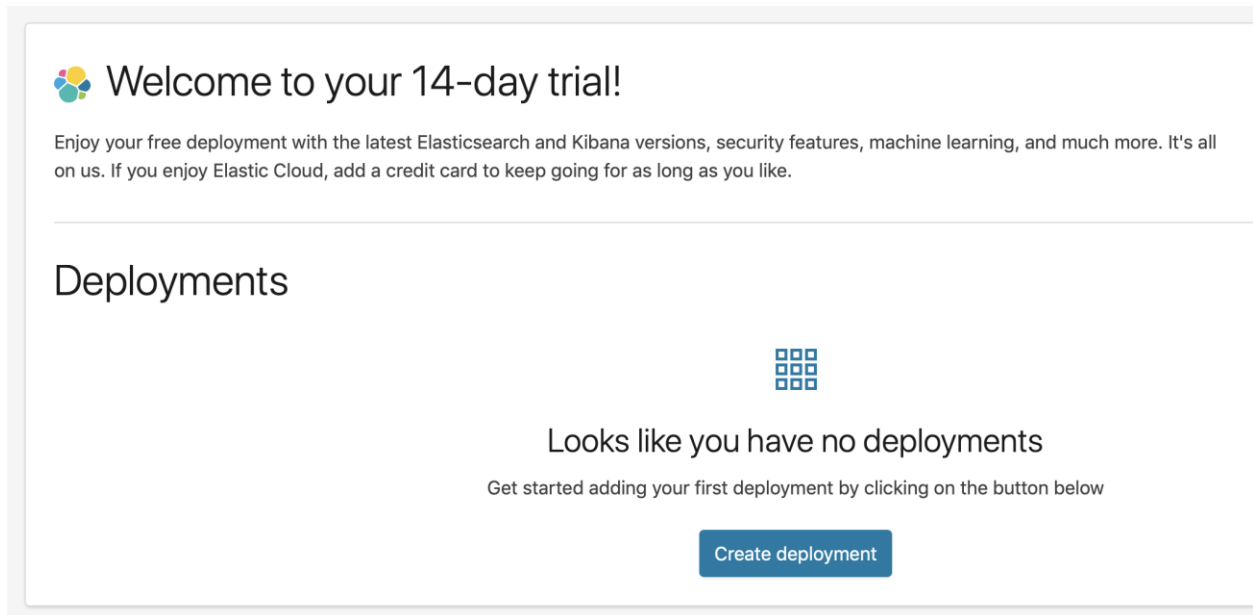
4. Log in and create give your account a strong password.

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". It has two input fields. The first is labeled "Password" and contains a lock icon and a series of dots. The second is labeled "Repeat password" and also contains a lock icon and a series of dots. Below these fields is a blue button labeled "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

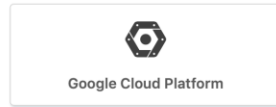
Workshop

7. Pick the cloud platform of your choice.

You may pick AWS or GCP. Once your provider is selected. You may pick a Region. (AWS / Tokyo 리전을 선택하시기 바랍니다.)

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.
(최신 버전으로 선택하시기 바랍니다.)

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](#)

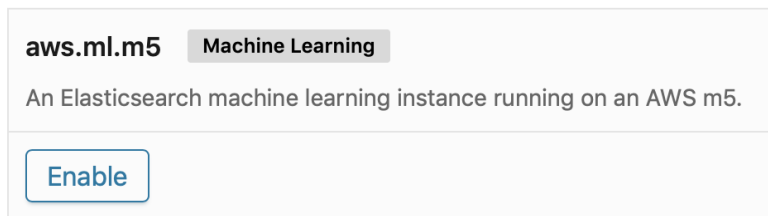
Elastic Cloud supports many more options to cater to your specific use case such as hot-warm architecture optimized for logging, compute-focused setup optimized for analytics etc. [Learn more ...](#)

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



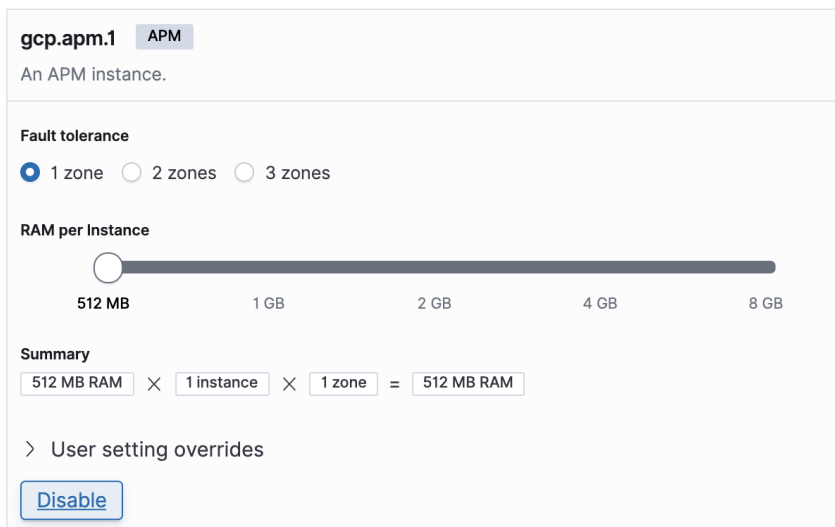
12. Turn on “Machine Learning” by clicking “Enable”.

 **Machine Learning** 1 configuration



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

 **APM** 1 configuration



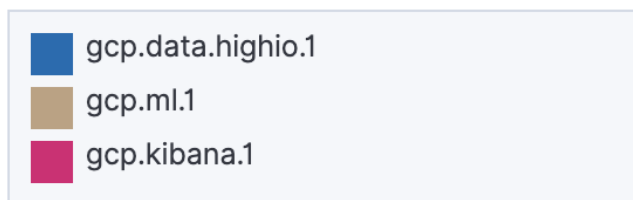
Your cluster’s Architecture should look similar to this:

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
j1mNWU0YW== 

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

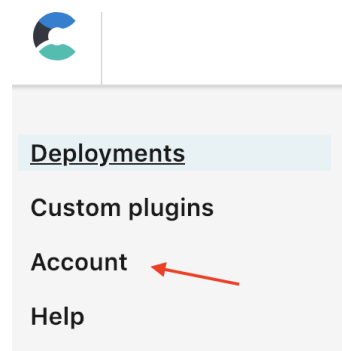
[Cancel](#)

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.

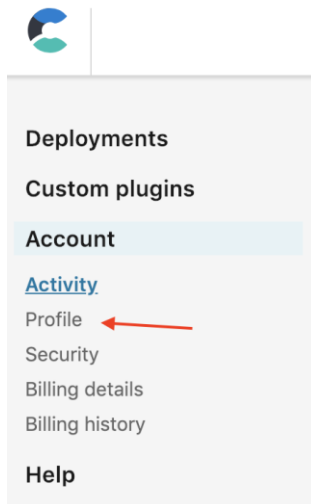
Note: This is your *cluster's* password, *not* your account password to log into cloud.elastic.co. You should now have 2 passwords. Securely record them somewhere.

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".



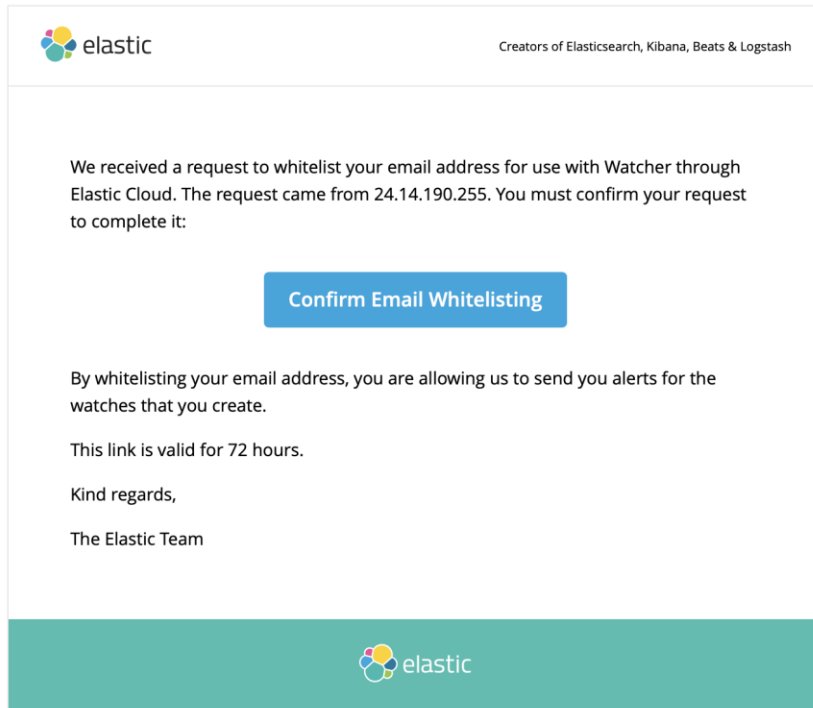
22. Add your email to “Monitoring email whitelist”.

Monitoring email whitelist

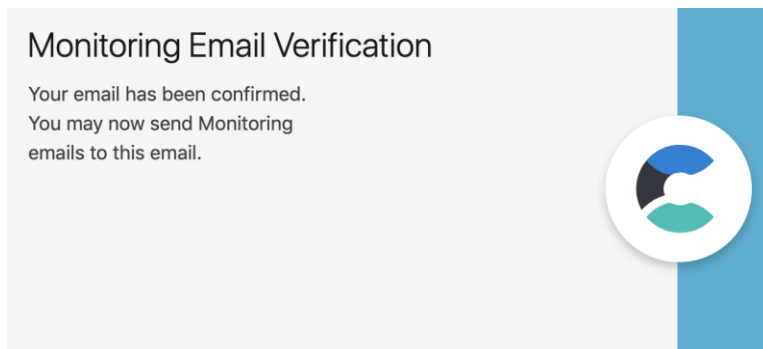
Whitelist an email address that should receive monitoring alerts. You must confirm the email address to start receiving these alerts.

Add

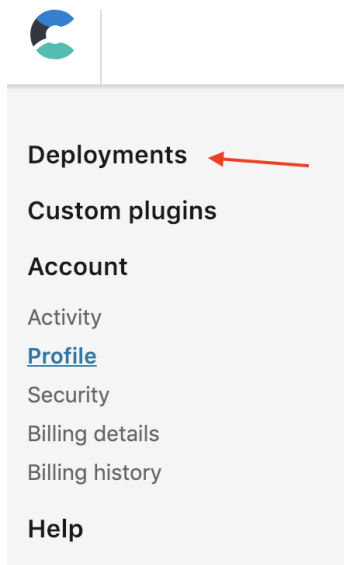
23. Check your email for a confirmation and click on the button “Confirm Email Whitelisting.”



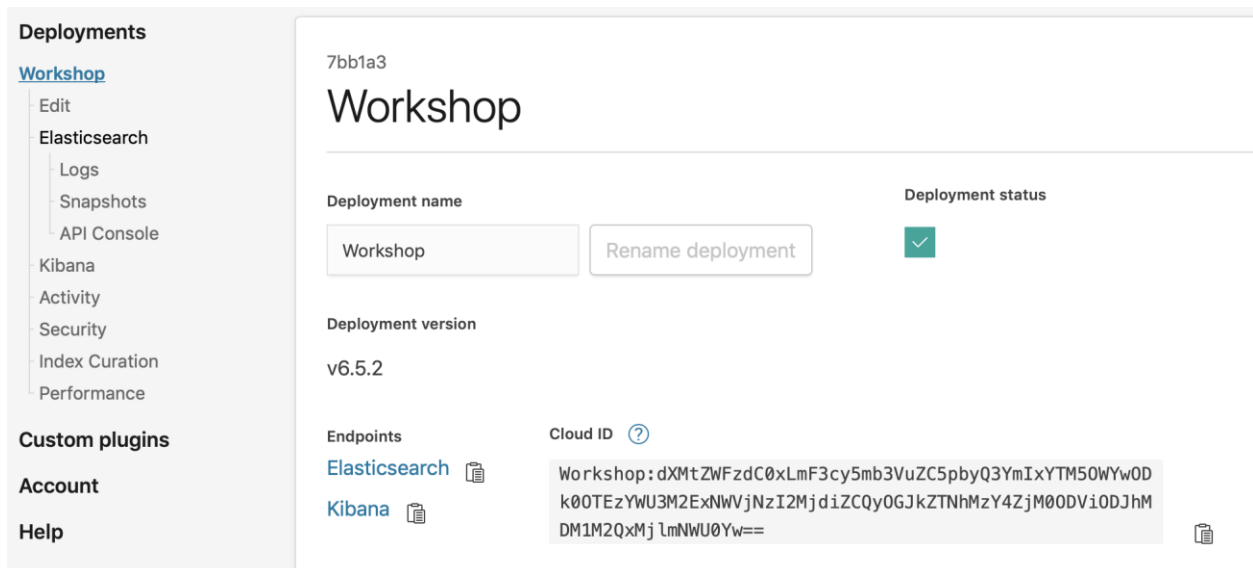
24. You should see the following confirmation in your web browser.



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

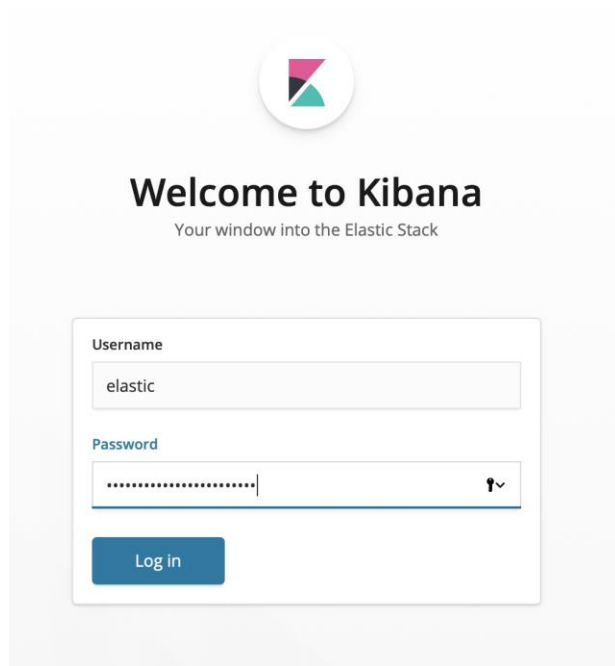


26. When the cluster is ready, select your cluster name in the top left.

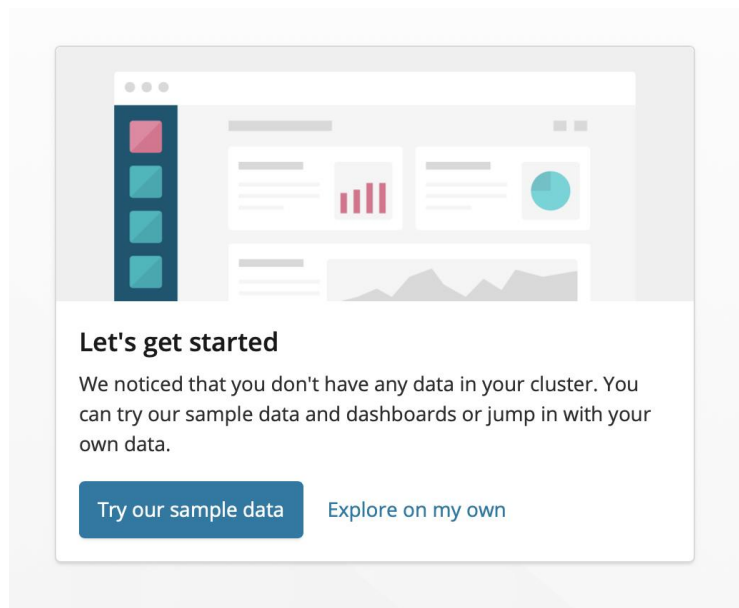


27. Click on Kibana to launch Kibana in a new tab. Log in with the username “elastic” and your password.

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 2: Metricbeat

- 각 운영체제 별 자세한 인스톨 방법은 LAB01 – Install Guide 문서를 참조하시기 바랍니다.
- 이 문서는 Mac/Linux 를 디폴트로 설명합니다. (윈도우에서 인스톨 방법은 위 가이드문서 참조)

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

* 인스톨 가이드 문서 : <https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-installation.html>

mac:

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-
7.5.0-darwin-x86_64.tar.gz
```

linux:

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-
7.5.0-linux-x86_64.tar.gz
```

1. Expand the file that you downloaded:

```
$ tar -zxvf metricbeat-<version>-x86_64.tar.gz
```

2. Change directory into the metricbeat

```
$ cd metricbeat-<version>-x86_64
```

(* Directory layout : <https://www.elastic.co/guide/en/beats/metricbeat/current/directory-layout.html>)

2.1. List modules that are available

```
$ ./metricbeat modules list
```

System module is enabled

3. Edit the metricbeat.yml file to point it to Elastic Cloud

- Use your favorite text editor to open metricbeat.yml and replace cloud.id and cloud.auth with values obtained from Lab 0.

(YAML files don't like hard tabs. Do not use them if you are editing a .yaml file because they will cause errors. To learn more about .yaml files see this link: <https://en.wikipedia.org/wiki/YAML>)

```
$ sudo vi ./metricbeat.yml
```

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

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: "testcluster:dXMtZWZdC0xLmF3cy5mb3VuZC5pbyRkZmRiZTEwOWY2MmI0MTMxODhh
ZTRmM2U4ODYzNTVlZiRjYTEzMTg0MGFkMzc0OWZjYThkZWRhZTU5OWE0MjY2OQ=="

# The format is `
```

4. Load the index templates and dashboards.

```
$ ./metricbeat -e 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
```

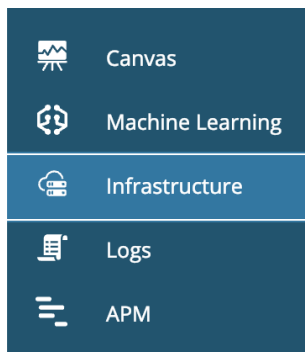
5. Start metricbeat

```
$ sudo chown root metricbeat.yml
$ sudo chown root modules.d/system.yml
$ sudo ./metricbeat -e
```

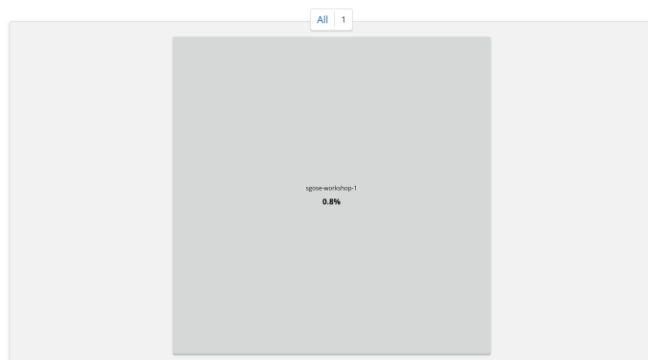
(You'll be running Metricbeat as root, so you need to change ownership of the configuration file and any configurations enabled in the `modules.d` directory, or run Metricbeat with `--strict.perms=false` specified. See [Config File Ownership and Permissions](#) in the *Beats Platform Reference*)

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

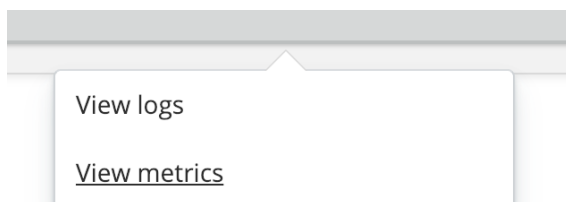
(Metric Tab 으로 이름이 바뀌었습니다. Metric tab 으로 이동하시면 됩니다.)



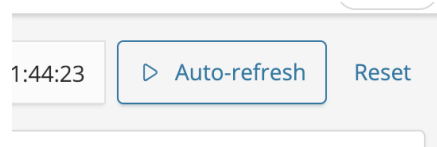
You should see your host show up as a tile.



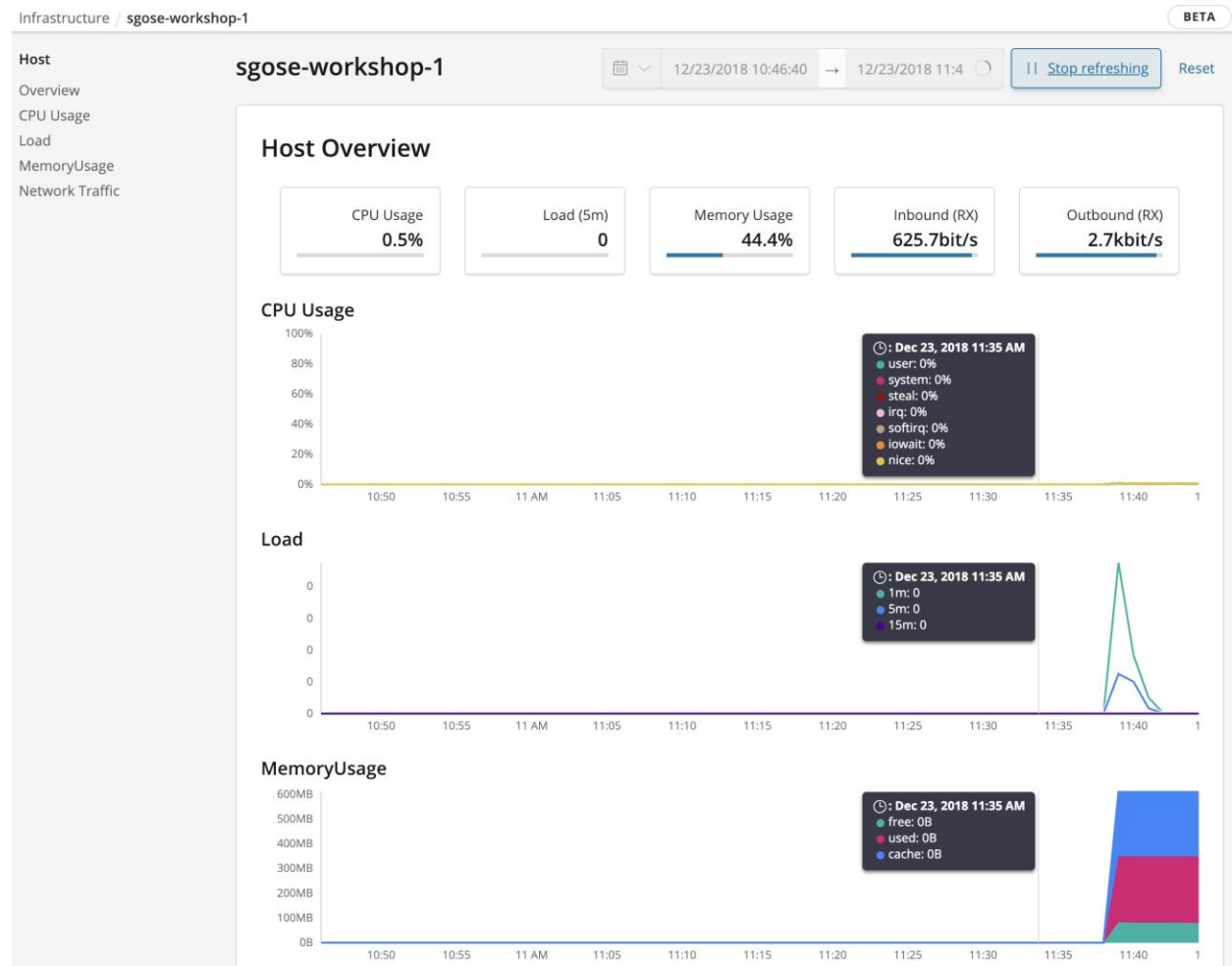
7. Click on your host and then “View metrics”



8. Click on “Auto-refresh”.



9. You should see metrics flowing in.



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

Section 3: Filebeat

In this section, we will install Filebeat to grab nginx log files.

* 인스톨 가이드 문서 : <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation.html>

mac:

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-
darwin-x86_64.tar.gz
```

linux:

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.5.0-
linux-x86_64.tar.gz
```

1. Expand the file that you downloaded:

```
$ tar -zxvf filebeat-<version>-x86_64.tar.gz
```

2. List modules

```
$ ./filebeat modules list
```

3. Enable nginx module

```
$ ./filebeat modules enable nginx
```

4. Edit the filebeat.yml file to point it to Elastic Cloud.

```
$ sudo vi ./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
```

5. Download the NGINX logs from the following URL and extract the log file:

<https://drive.google.com/file/d/1RUDsDI5WOkVAnLw1xRR3H9zX3slqAHt/view?usp=sharing>

6. Change directory to the following location

```
$ cd modules.d
```

7. Now let us modify the NGINX module to point to the log file location. We do this by modifying the nginx.yml file and creating an entry for the access logs. Add the following configuration to the nginx.yml file.

```
$ sudo vi nginx.yml
```

Note: Use the directory you expanded the NGINX log file to

```
- [module:nginx]
  # Access logs
  access:
    enabled: true
    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:
    var.paths: ["/Users/shh/Development/logs/nginx/nginx.log"]

  # Error logs
  error:
    enabled: true
    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:
```

8. Now we are ready to setup Elasticsearch to receive the NGINX logs, visualize it, and create Machine Learning jobs to detect anomalies.

```
$ cd ..  
$ sudo chown root filebeat.yml  
$ sudo chown root modules.d/nginx.yml  
$ ./filebeat -e setup  
$ sudo ./filebeat -e
```

(* You'll be running Filebeat as root, so you need to change ownership of the configuration file, or run Filebeat with `--strict.perms=false` specified. See [Config File Ownership and Permissions](#) in the *Beats Platform Reference*.)

9. Check the logs in Kibana -> Discovery tab

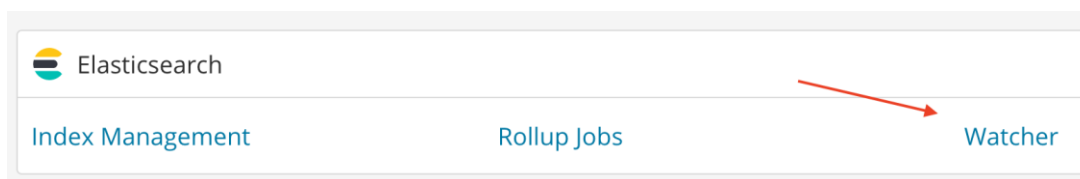
Congratulations! You have successfully installed Filebeat and began threat-hunting.

Section 4: 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.

Let's begin with a simple threshold Alert.

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



2. Click on "Create threshold alert" button.

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

Watches

[Create threshold alert](#) [Create advanced watch](#)

3. Fill out the form using the following information.

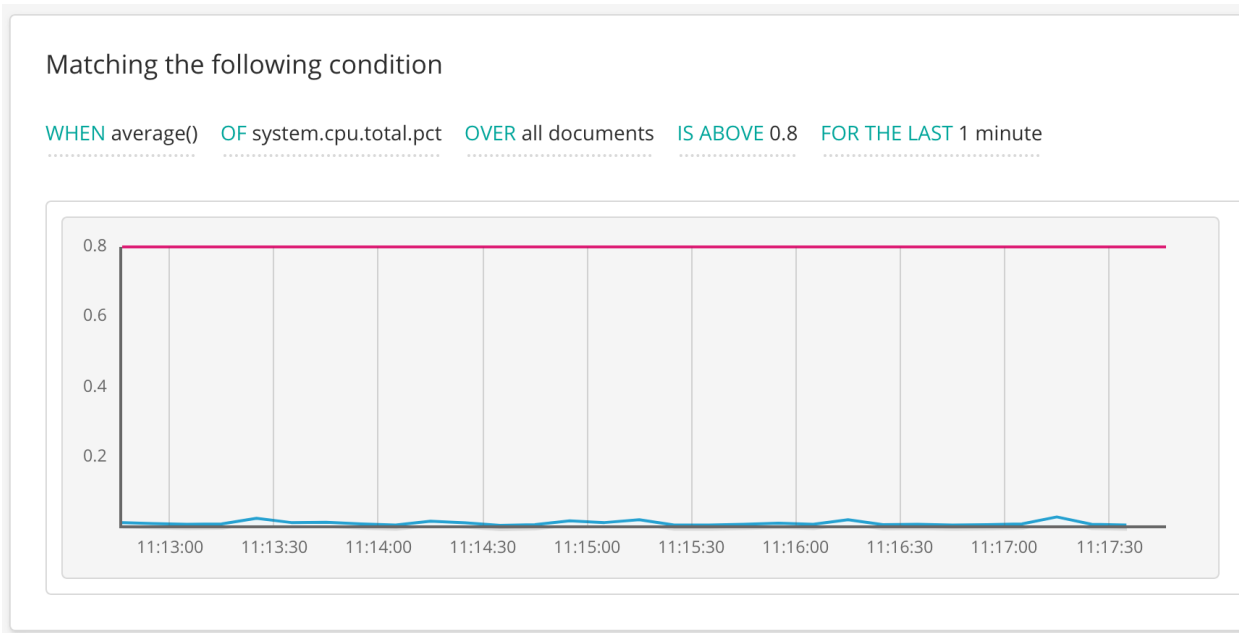
Create a new threshold alert

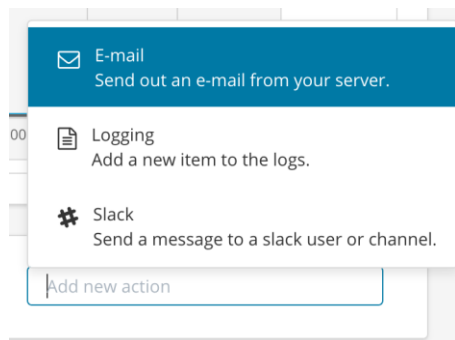
Send an alert when a specific condition is met. This will run every 1 minute.

Name

Indices to query **Time field** **Run watch every**

Use * to broaden your search query





Will perform 1 action once met Add new action

▼ E-mail

To e-mail address

YOUR_EMAIL_ADDRESS

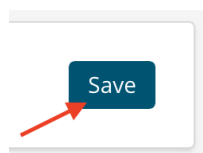
Subject

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

Body

High CPU Alert

Remove E-mail Action Test fire an e-mail now



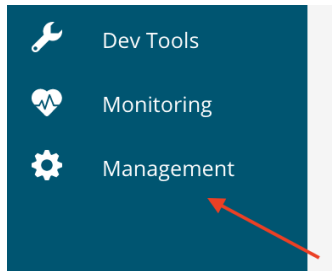
4. Now let's generate some load to get this Alert to trigger.

5. Go to your Linux host and run the following command.

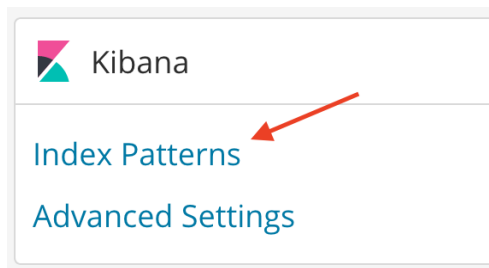
```
$ dd if=/dev/zero of=/dev/null
```

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.

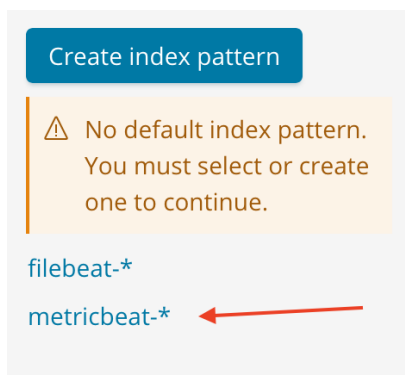
6. Switch back to Kibana and click on "Management".



7. Click on “Index Patterns” in the Kibana section.



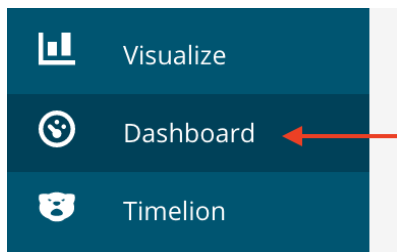
8. Click on the “metricbeat-*” index pattern.



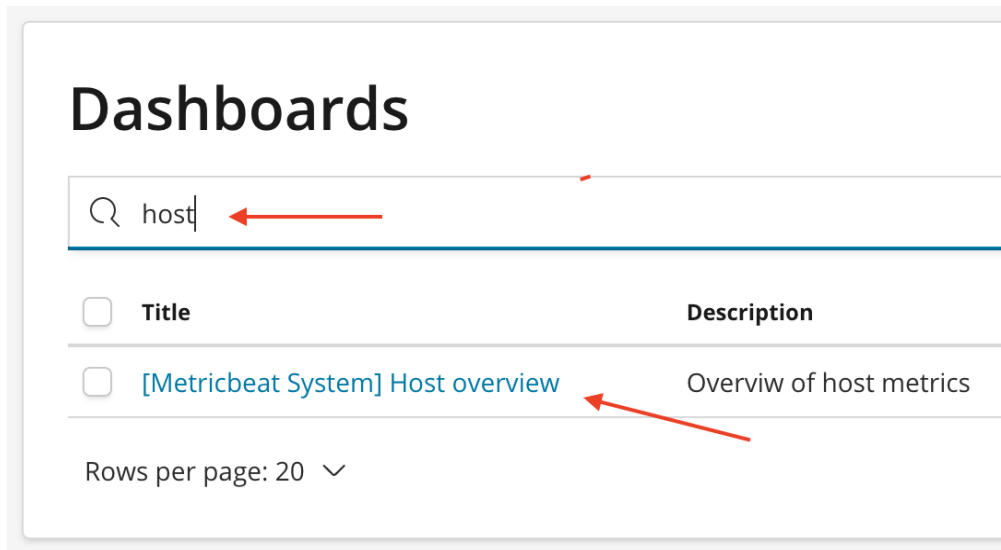
9. Click on the star icon which will set this index pattern as the default.



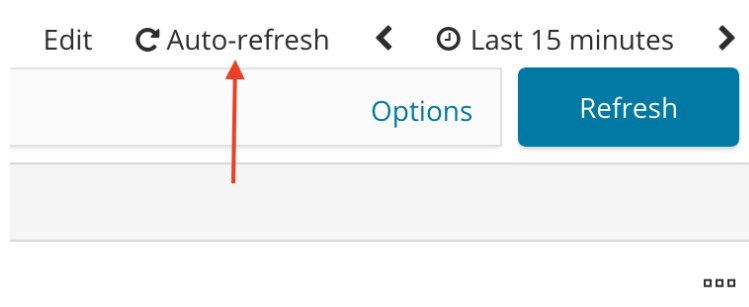
10. Click on the “Dashboard” tab in Kibana.



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



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



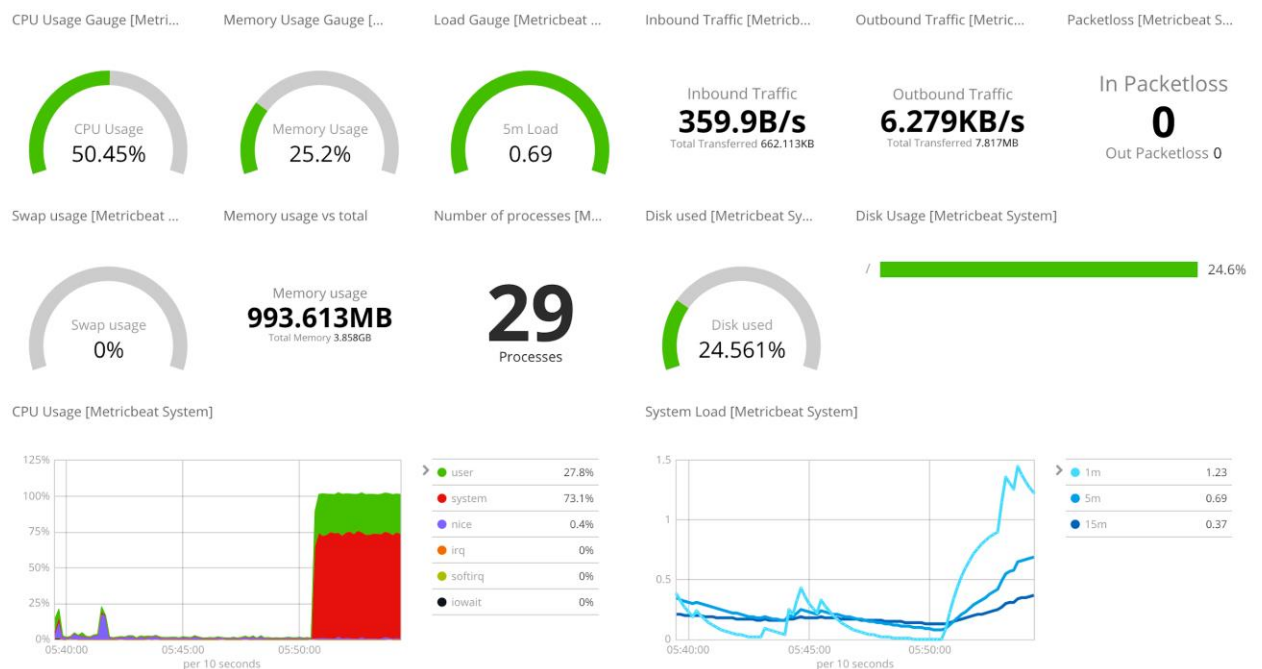
13. Click on “5 seconds” in the dropdown.

Full screen Share Clone Edit [Auto-refresh](#)

Refresh Interval

Off 5 seconds 1 minute 1 hour
 10 seconds 5 minutes 2 hours
 30 seconds 15 minutes 12 hours
 45 seconds 30 minutes 1 day

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

...

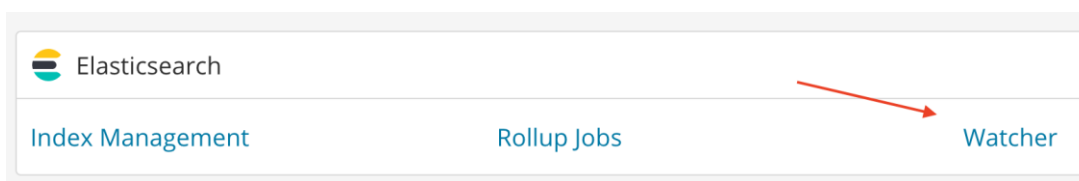
This email is sent via a Watcher alert on a Found hosted cluster. Your email address was previously whitelisted. To stop receiving any Watcher alerts, please visit nd.io/u/eJwVxDEOwyAMAMDXhI3lBoNhYMgfOnVBCZgWKQ1Sw_9V9YariWsDr3qSz97PjDn36-yX1JyJBW7H4TQWZk0Rmo4UQle4Oxfg8V_tALzU71TDN57KGygEd9qJBRib50F76oLqL7pLmPO9TVuWQjk3O_Zy1qGmmkx2w_8Kixb

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.

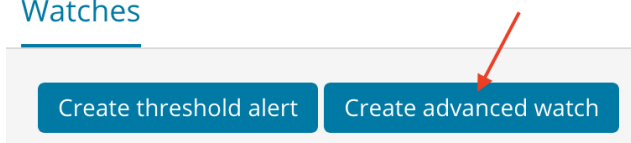
17. In Kibana, click on “Management” item in the menu and then click on “Watcher”.



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



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

19. Insert the following for ID and Name.

A screenshot of the 'New watch' form in Kibana. The form has a title 'New watch' and two buttons, 'Save' and 'Cancel', in the top right corner. Below the title are two tabs: 'Edit' and 'Simulate'. The 'ID' field contains the text 'ssh_login_attempts_1'. The 'Name' field contains the text '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>

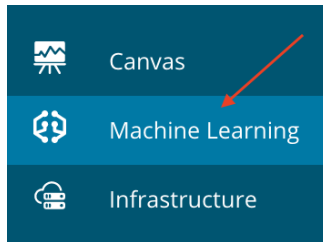
A great overview of Alerting (a.k.a., Watcher) is available here:

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

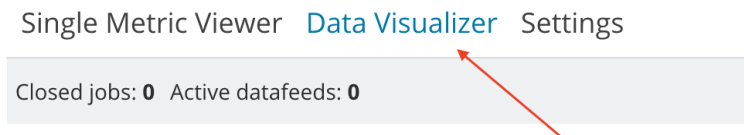
Section 5: Machine Learning

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”



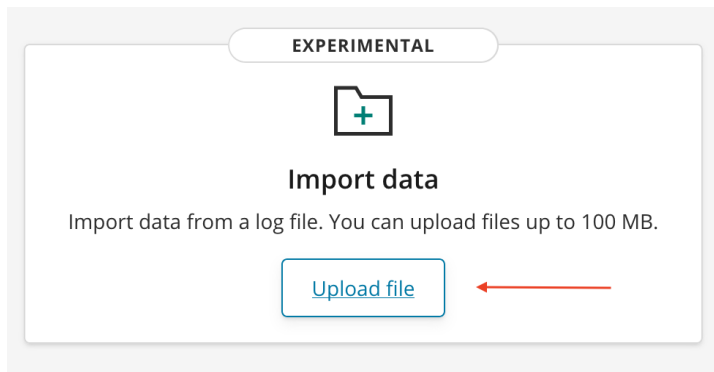
3. Click on the following link which will download a CSV file called “**flights.csv**” to your laptop. It contains all US Commercial flights between October and November 2017 (2 months).

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.

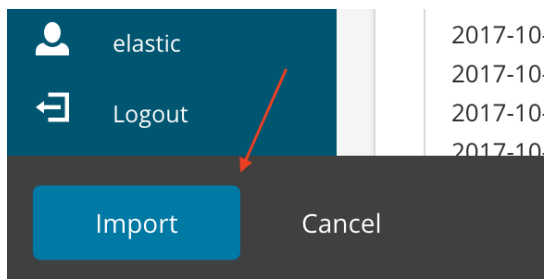


5. Drag and drop the file into the upload area or select it using a file picker.



Select or drag and drop a file

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



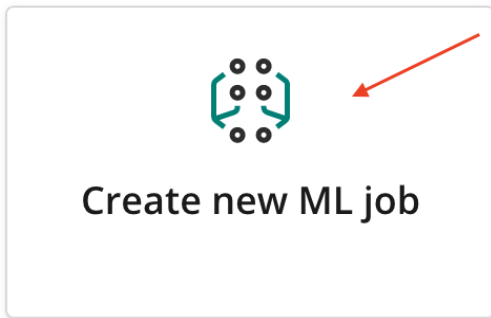
7. Import the data into an index named “flights”.

A screenshot of the 'Import data' dialog box. The title is 'Import data' with a sub-label 'EXPERIMENTAL'. There are two tabs: 'Simple' (selected) and 'Advanced'. Under the 'Simple' tab, there is a section 'Index name' with a text input field containing 'flights'. A red arrow points to this field. Below the input field, there is a checkbox labeled 'Create index pattern' which is checked. At the bottom, there is a blue 'Import' button with a red arrow pointing to it.

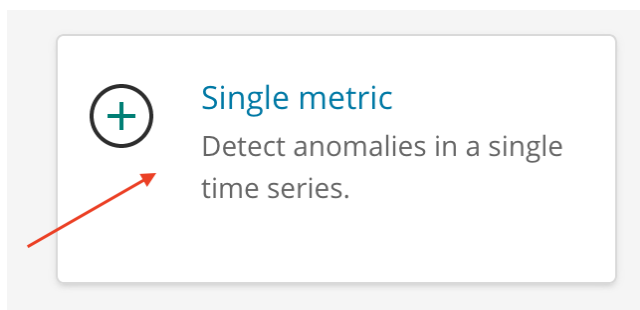
8. After clicking “Import”, you should see an “Import complete” confirmation.

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

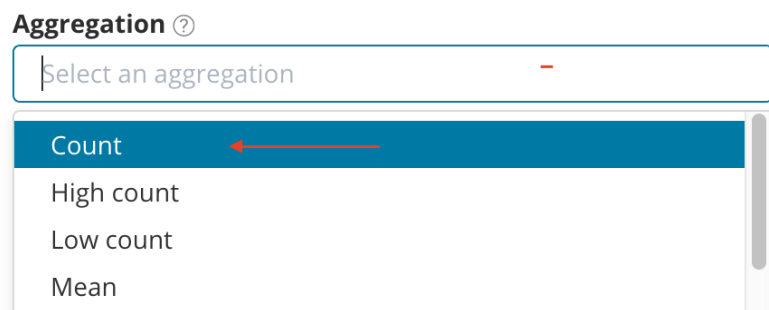
9. Click on “Create new ML job”.



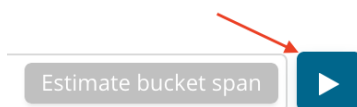
10. Click on "Single metric".



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 ?

 ←

Description ?

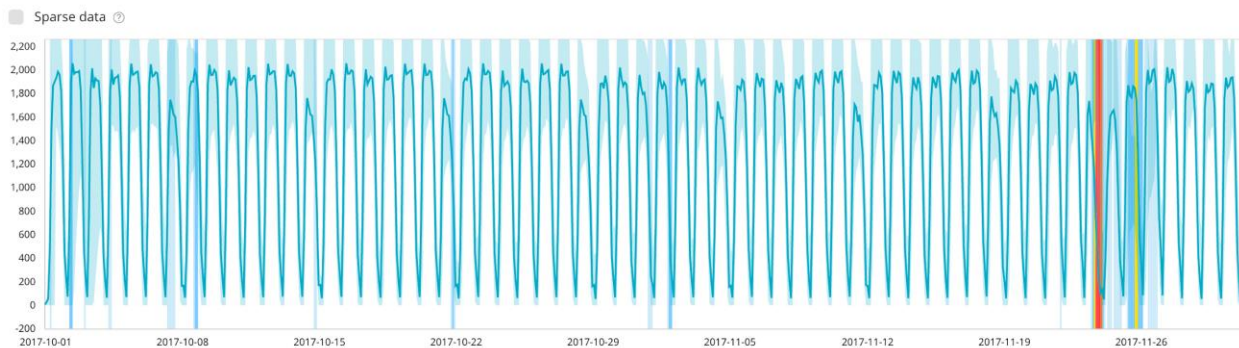
Job Groups ?

▶ **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.

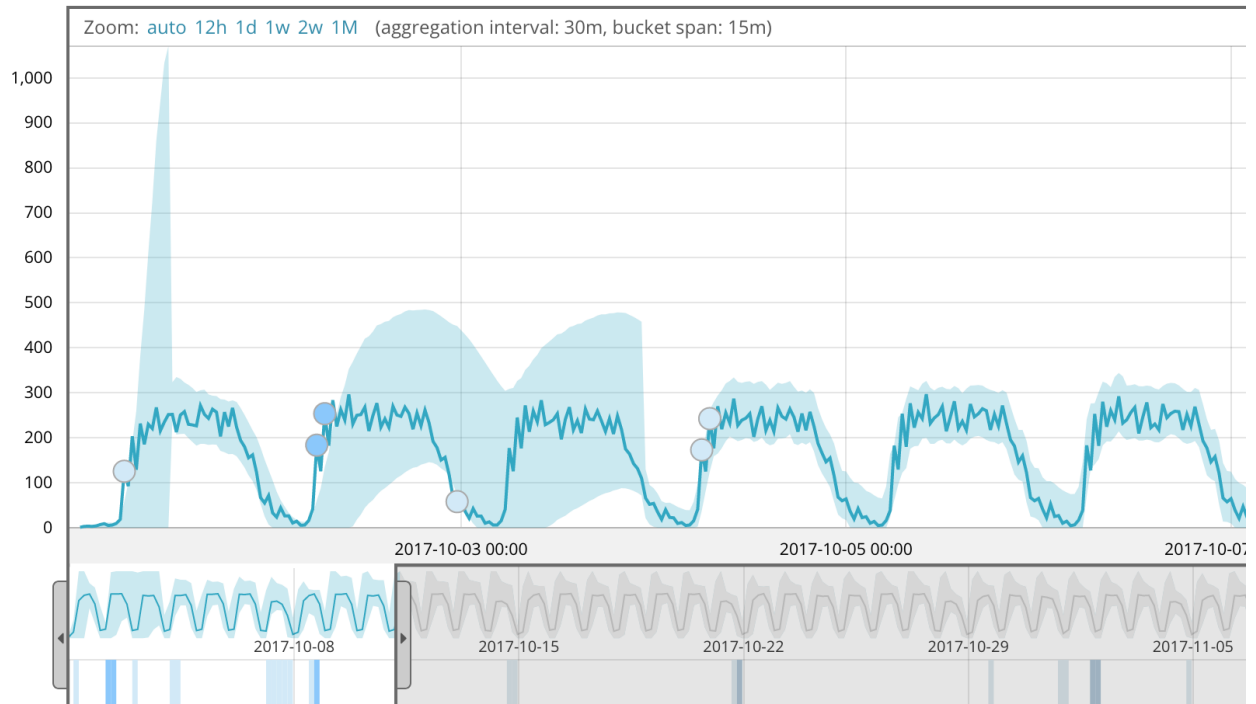


15. Click on “View Results”.

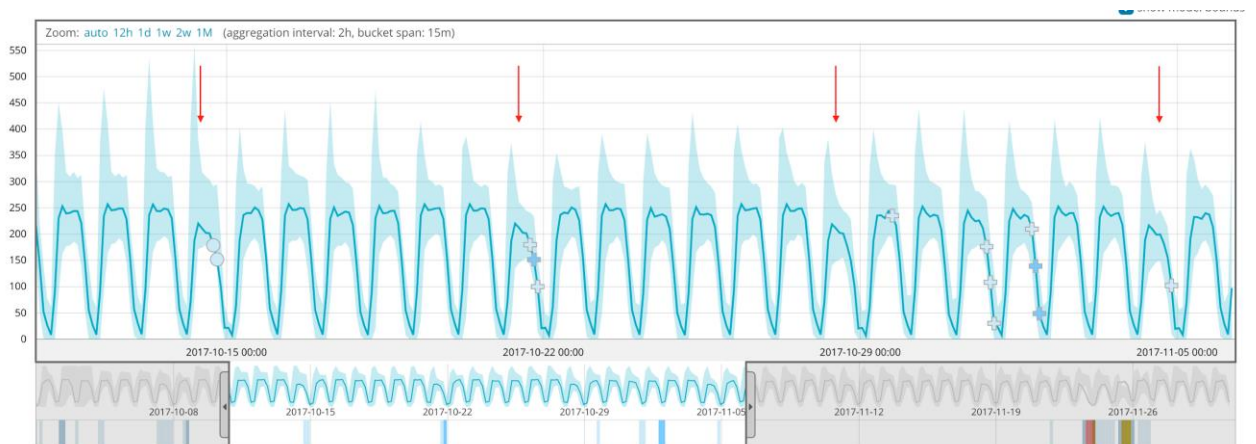
Job flights created ✓

[Reset](#) [View Results](#) ←

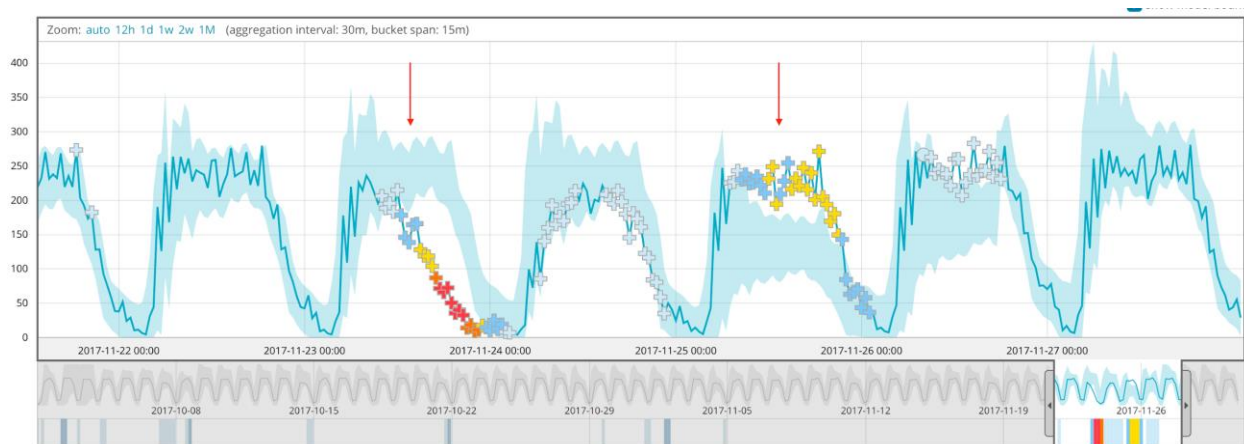
16. You should now be looking at the “Single Metric Viewer” in Kibana. Drag the time window to cover only the first week of data. Notice how the data model picks up a pattern after about 3 days.



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 6: 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.