

# LAB 1

<b>Introduction</b>	<b>1</b>
<b>Local Laptop Installation</b>	<b>1</b>
Synopsis	1
Software Download	2
Windows Instructions	2
Metricbeat	2
Filebeat	6
Mac/Linux Instructions	10
Metricbeat	10
Filebeat	12
<b>Data Loader</b>	<b>15</b>
Introduction	15
<b>Validate Data in Kibana</b>	<b>16</b>
<b>Stretch Goal</b>	<b>20</b>
Synopsis	20

## Introduction

In this lab guide we will walk you through how to ingest multiple logs files and metrics into the Elastic stack.

## Local Laptop Installation

### Synopsis

Beats agents are data shippers that are designed to be lightweight. Each beat targets a specific type of data set. For the purposes of our lab we will use Metricbeat which will send important metrics like CPU and memory utilization into Elasticsearch. We will also use Filebeat which will not only send log files from services like NGINX and Apache, but also system authorization logs.

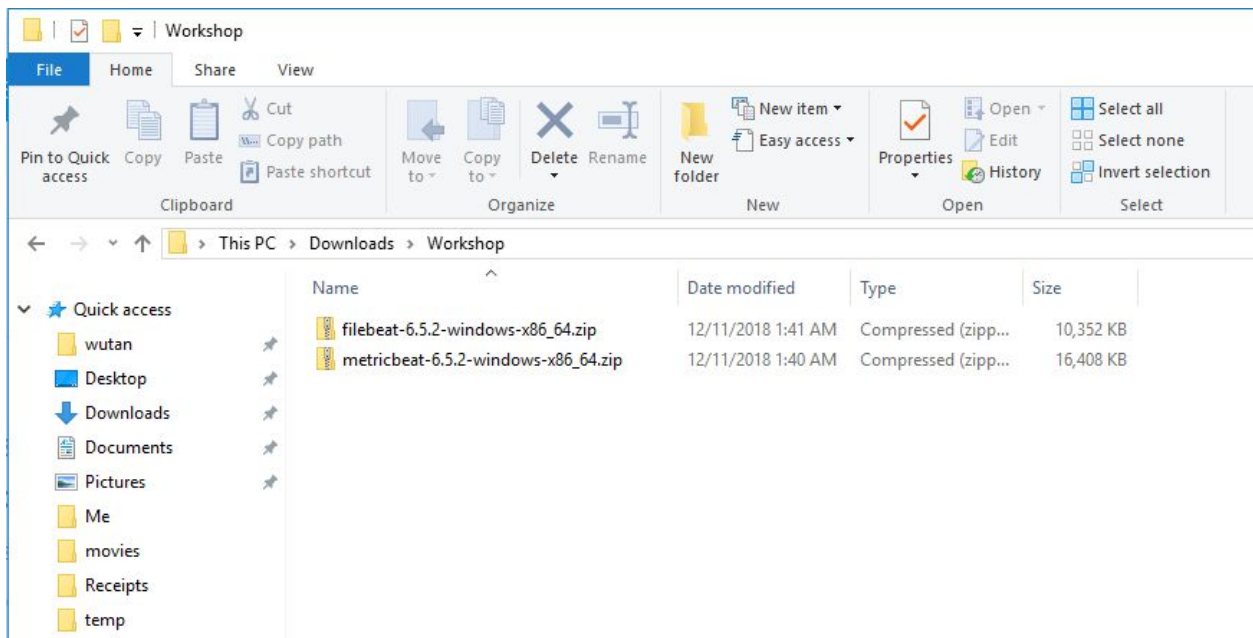
## Software Download

Software	URL
Metricbeat	<a href="https://www.elastic.co/downloads/beats/metricbeat">https://www.elastic.co/downloads/beats/metricbeat</a>
Filebeat	<a href="https://www.elastic.co/downloads/beats/filebeat">https://www.elastic.co/downloads/beats/filebeat</a>

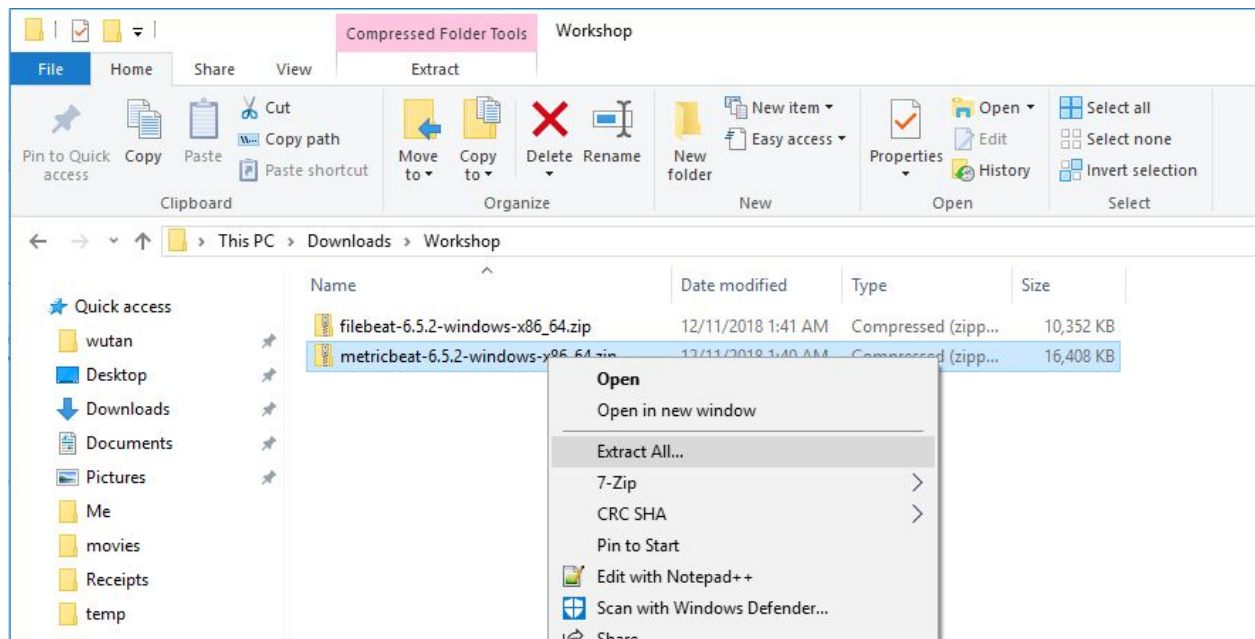
## Windows Instructions

### Metricbeat

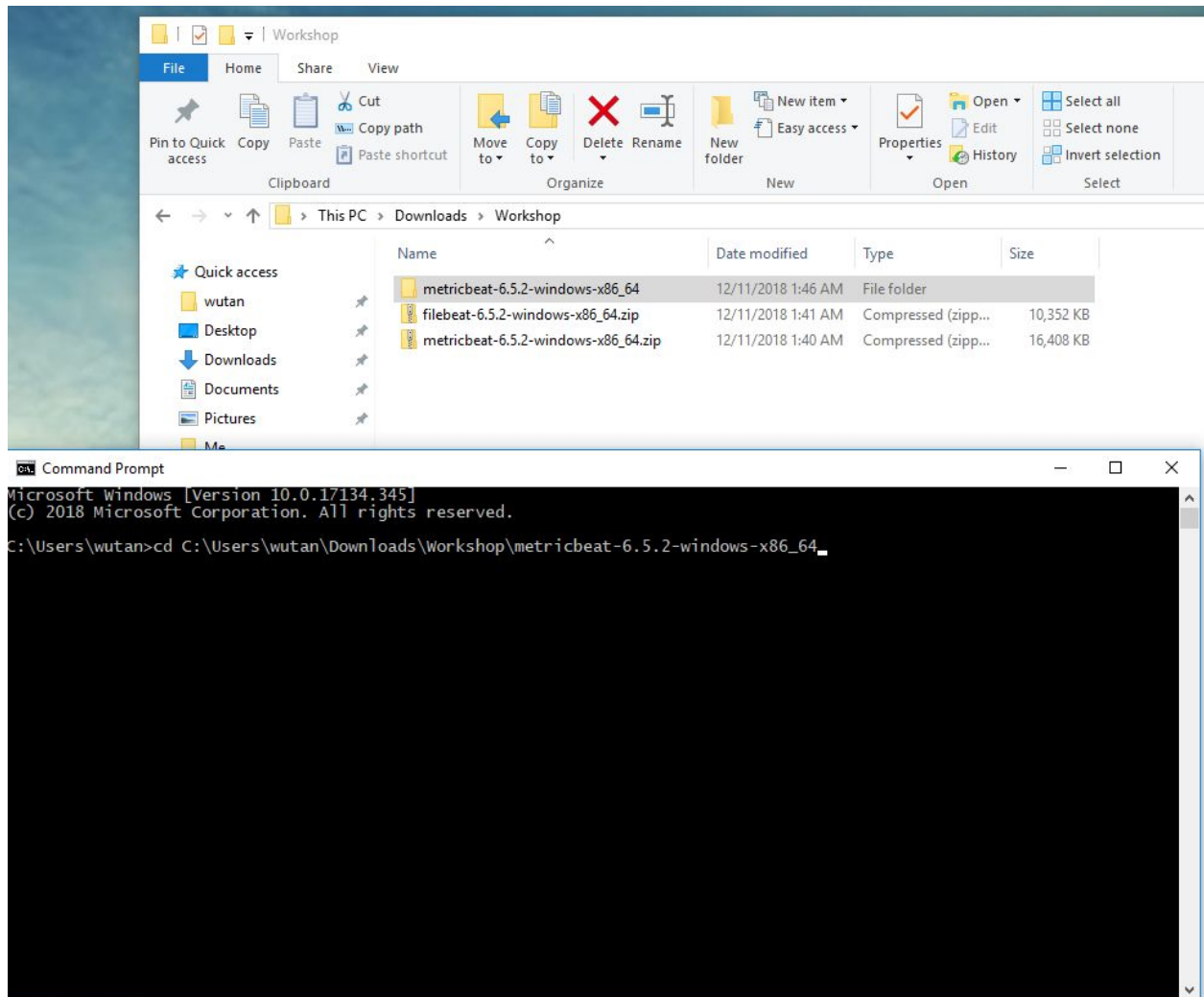
- 1) Open a Windows Explorer and navigate to the location that you downloaded metricbeat to



- 2) Expand the file that you downloaded



- 3) Open up a command prompt and type in `cd + a space`. Now drag-n-drop the extracted folder from step #2 to the command prompt window. Notice how it filled out the full path for you in the command prompt window? You can also type out the full path if you are a glutton for pain. Hit enter.



4) Now list modules that are available

```
metricbeat.exe modules list
```

You should see which modules are **enabled** and which modules are **disabled**. Out of the box the **system** module is the only one that is enabled.

```
Command Prompt
C:\Users\wutan\Downloads\Workshop\metricbeat-6.5.2-windows-x86_64>metricbeat.exe modules list

Enabled:
system

Disabled:
aerospike
apache
ceph
couchbase
docker
dropwizard
elasticsearch
envoyproxy
etcd
golang
graphite
haproxy
http
jolokia
kafka
kibana
kubernetes
kvm
logstash
memcached
mongodb
munin
mysql
nginx
php_fpm
postgresql
prometheus
rabbitmq
redis
traefik
uwsgi
vsphere
windows
zookeeper
```

- 5) Before we setup Elasticsearch to accept system metrics we need to tell Metricbeat where Elasticsearch is and provide credentials to login. We do this by editing the configuration file for Metricbeat called `metricbeat.yml`

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 .yml file because they will cause errors. To learn more about .yml files see this link: <https://en.wikipedia.org/wiki/YAML>

Example:

```
73 #===== Elastic Cloud =====
74
75 # These settings simplify using metricbeat with the Elastic Cloud (https://cloud.elastic.co/)
76
77 # The cloud.id setting overwrites the 'output.elasticsearch.hosts' and
78 # 'setup.kibana.host' options.
79 # You can find the 'cloud.id' in the Elastic Cloud web UI.
80 cloud.id: "CentralizedBeatsMgmt:dXhtZWfZdCoxLmF3cy5mb3VuZC5pbyRkZmR1ZTEwOWY2MmI0MTMxODhhZTRmM2U4ODYzNTVlZiRjYTEzMlQ0MGFkMzc0OWZjYThkZWZhZTU5OWE0NjY2OQ=="
81
82 # The cloud.auth setting overwrites the 'output.elasticsearch.username' and
83 # 'output.elasticsearch.password' settings. The format is 'user:pass'.
84 cloud.auth: "elastic:uB2AxEXuR1G900WwiteZ8VLT"
85
86 #===== Outputs =====
87
88
```

- 6) Now we are ready to setup Elasticsearch to receive the system metric data, visualize it, and create Machine Learning jobs to detect anomalies. Fortunately it only takes one command!

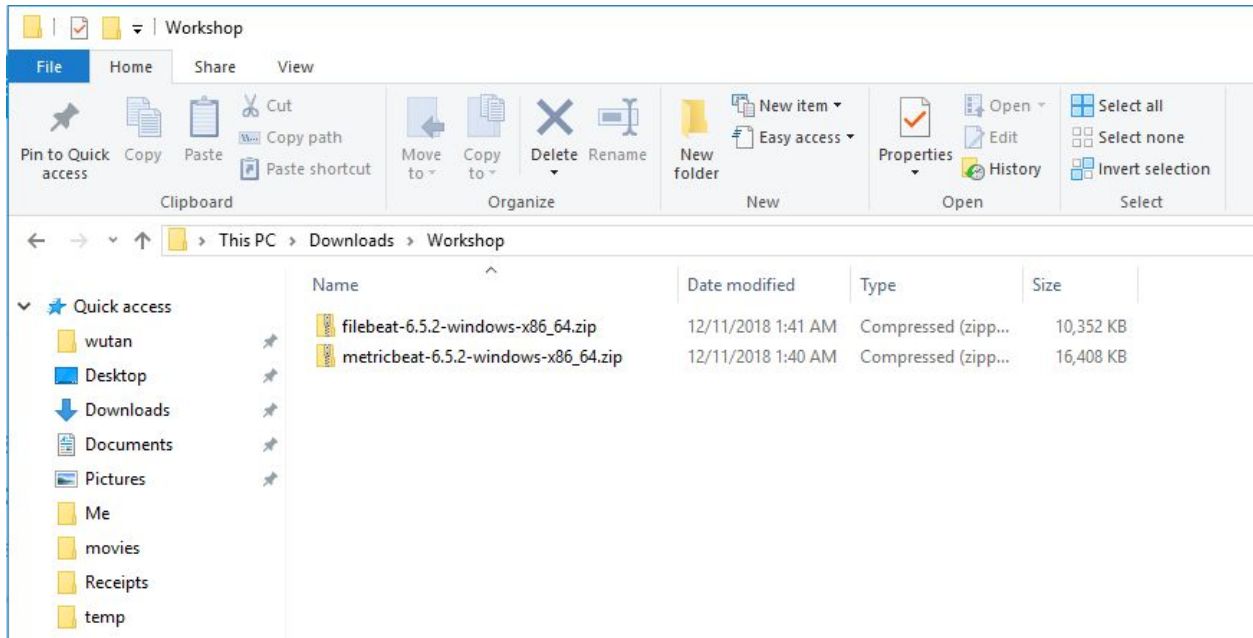
```
metricbeat.exe -e setup system
metricbeat.exe -e
```

Make sure you see the following text at the end of the output:

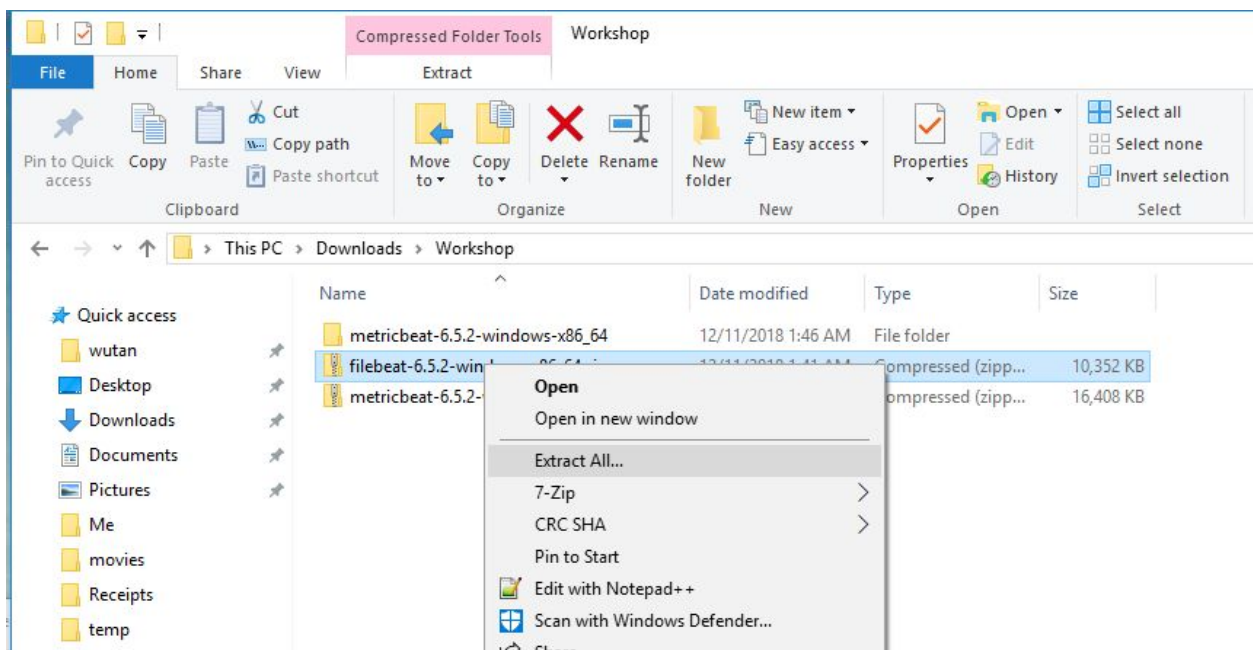
```
2018-12-11T02:09:03.985-0500 INFO [beat] instance/beat.go:825 Beat info {"system_info": {"beat": {"path": {"config": "C:\\Users\\wutan\\Downloads\\Workshop\\metricbeat-6.5.2-windows-x86_64\\data", "home": "C:\\Users\\wutan\\Downloads\\Workshop\\metricbeat-6.5.2-windows-x86_64\\logs", "type": "metricbeat", "uuid": "9d2a40fd-5971-4d16-9edc-7576152e6f23"}}}}
2018-12-11T02:09:03.985-0500 INFO [beat] instance/beat.go:834 Build info {"system_info": {"build": {"commit": "b48d073b84e874a182c122d8ef2bad867f714a11", "l1": "6.5.2", "time": "2018-11-29T23:11:55.000Z", "version": "6.5.2"}}}}
2018-12-11T02:09:03.985-0500 INFO [beat] instance/beat.go:837 Go runtime info {"system_info": {"go": {"os": "windows", "arch": "amd64", "max_procs": 4, "version": "go1.10.3"}}}}
2018-12-11T02:09:04.002-0500 INFO [beat] instance/beat.go:841 Host info {"system_info": {"host": {"architecture": "x86_64", "boot_time": "2018-11-02T01:15:12-04:00", "name": "ShawnDesktop", "ip": [{"169.254.7.121/16", "169.254.87.244/16", "169.254.121.200/16", "169.254.12.134/16", "192.168.75.1/24", "192.168.91.1/24", "192.168.1.200/24"}], "kernel_version": "10.0.17134.345 (winBuild.160101.0800)", "mac": [{"40:8d:5c:c7:62:09", "00:ff:95:af:0d:72", "16:f2:6d:b5:41:94", "26:f2:6d:b5:41:94", "00:50:56:c0:00:00", "00:50:56:c0:00:01", "f4:f2:6d:b5:41:94"}], "os": {"family": "windows", "platform": "windows", "name": "Windows 10 Home", "version": "10.0", "major": 10, "minor": 0, "patch": 0}, "build": "17134.345", "timezone": "EST", "timezone_offset_sec": -18000, "id": "b57d999f-d214-4d04-a4e7-9726d4d40d8d"}}}}
2018-12-11T02:09:04.004-0500 INFO [beat] instance/beat.go:870 Process info {"system_info": {"process": {"cwd": "C:\\Users\\wutan\\Downloads\\Workshop\\metricbeat-6.5.2-windows-x86_64", "exe": "C:\\Users\\wutan\\Downloads\\Workshop\\metricbeat-6.5.2-windows-x86_64\\metricbeat.exe", "name": "metricbeat.exe", "pid": 19536, "ppid": 9348, "start_time": "2018-12-11T02:09:03.082-0500"}}}}
2018-12-11T02:09:04.004-0500 INFO instance/beat.go:278 Setup Beat: metricbeat; Version: 6.5.2
2018-12-11T02:09:07.020-0500 INFO add_cloud_metadata/add_cloud_metadata.go:319 add_cloud_metadata: hosting provider type not detected.
2018-12-11T02:09:07.020-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T02:09:07.020-0500 INFO [publisher] pipeline/module.go:110 Beat name: ShawnDesktop
2018-12-11T02:09:07.020-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T02:09:07.281-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.2
2018-12-11T02:09:07.315-0500 INFO template/load.go:82 Loading template for Elasticsearch version: 6.5.2
2018-12-11T02:09:07.786-0500 INFO template/load.go:145 Elasticsearch template with name 'metricbeat-6.5.2' loaded
Loaded index template
Loading dashboards (Kibana must be running and reachable)
2018-12-11T02:09:07.787-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T02:09:07.928-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.2
2018-12-11T02:09:07.928-0500 INFO kibana/client.go:118 Kibana url: https://ca131840ad3749fca8ddedae599a42669.us-east-1.aws.found.io:443
2018-12-11T02:09:33.566-0500 INFO instance/beat.go:717 Kibana dashboards successfully loaded.
Loaded dashboards
C:\\Users\\wutan\\Downloads\\Workshop\\metricbeat-6.5.2-windows-x86_64>
```

## Filebeat

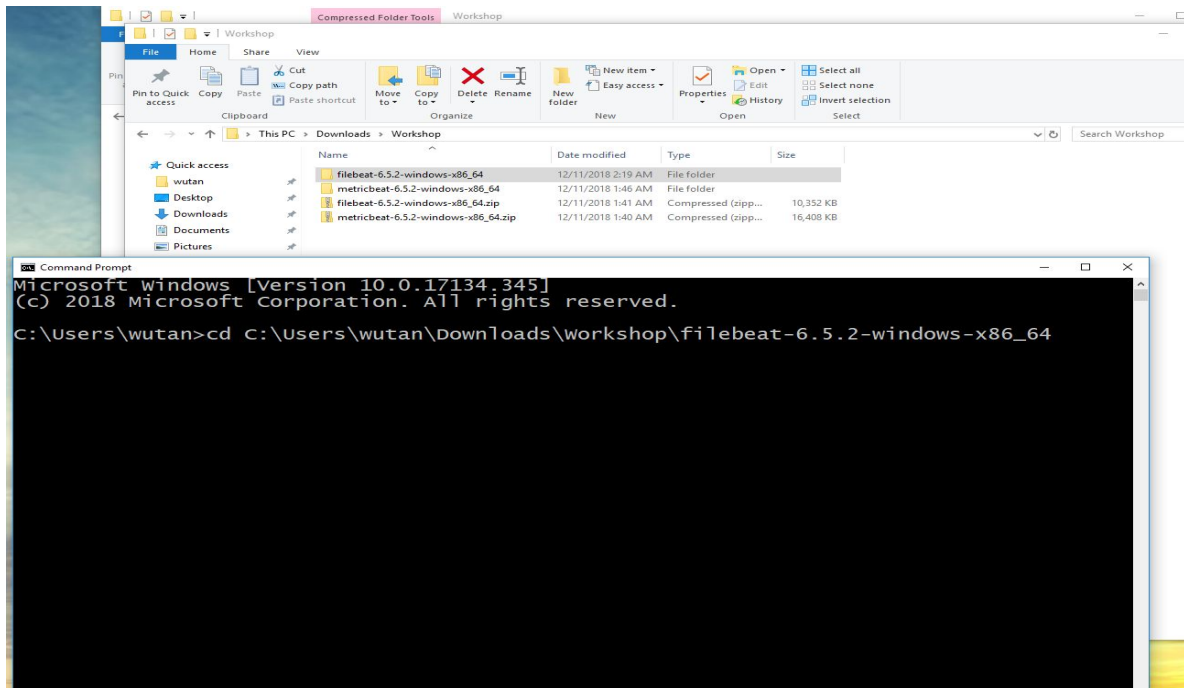
- 1) Open a Windows Explorer and navigate to the location that you downloaded metricbeat to



2) Expand the file that you downloaded



3) Open up a command prompt and type in `cd + a space`. Now drag-n-drop the extracted folder from step #2 to the command prompt window. Notice how it filled out the full path for you in the command prompt window? You can also type out the full path if you are a glutton for pain. Hit enter.



4) List the modules that are available

```
filebeat.exe modules list
```

You should see which modules are **enabled** and which modules are **disabled**. Out of the box there are no modules enabled.



```
Command Prompt
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\wutan>cd C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64

C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64>filebeat modules list
Enabled:

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

C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64>
```

5) Now let us enable the NGINX module so we can ingest NGINX logs

```
filebeat.exe modules enable nginx
```

```
Command Prompt
traefik

C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64>filebeat.exe modules enable nginx
Enabled nginx

C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64>filebeat.exe modules list
Enabled:
nginx

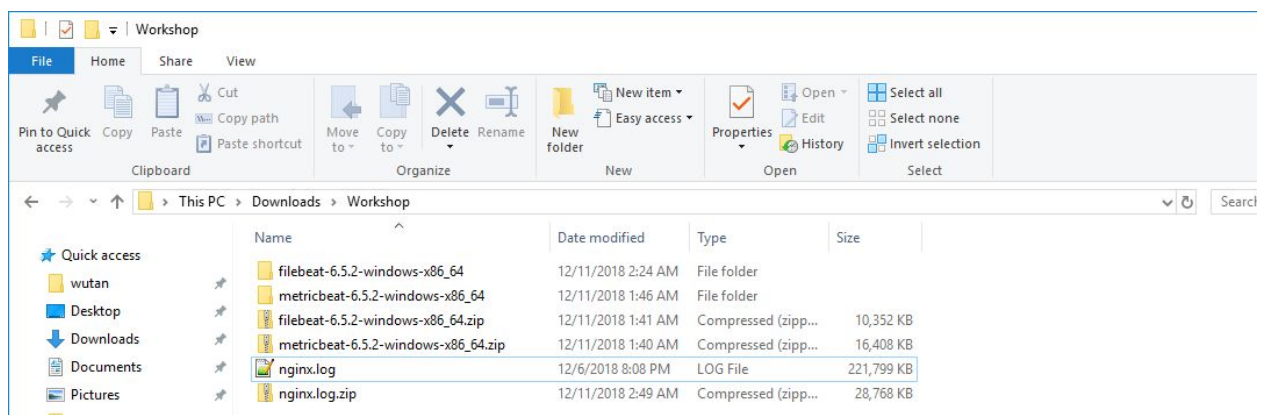
Disabled:
apache2
auditd
elasticsearch
haproxy
icinga
iis
kafka
kibana
logstash
mongodb
mysql
osquery
postgresql
redis
suricata
system
traefik

C:\Users\wutan\Downloads\workshop\filebeat-6.5.2-windows-x86_64>
```

- 6) Before we setup Elasticsearch to accept NGINX logs we need to tell Filebeat where Elasticsearch is and provide credentials to login. We do this by editing the configuration file for Filebeat called `filebeat.yml`.
- 7) Follow the exact same procedure that you did in step #5 when you setup Metricbeat and add the **cloud.id** and **cloud.auth** to `filebeat.yml` using the values from [Lab 0](#)
- 8) Normally Filebeat would scan your system in several common locations for NGINX log files. Since we don't actually have NGINX installed we are going to copy some real NGINX log files to the filesystem and tell the NGINX module where they are located.

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

[https://drive.google.com/file/d/1RUDsDI5WOkVAnLw1xRR3H9zX3slqAht\\_/view?usp=sharing](https://drive.google.com/file/d/1RUDsDI5WOkVAnLw1xRR3H9zX3slqAht_/view?usp=sharing)



- 9) Change directory to the following location

```
cd modules.d
```

- 10) 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.

```

1  - module: nginx
2  # Access logs
3  access:
4    enabled: true
5
6  # Set custom paths for the log files. If left empty,
7  # Filebeat will choose the paths depending on your OS.
8  var.paths: ["C:/Users/wutan/Downloads/Workshop/nginx.log"]
9
10 # Error logs
11 error:
12   enabled: true
13
14 # Set custom paths for the log files. If left empty,
15 # Filebeat will choose the paths depending on your OS.
16 #var.paths:
17

```



- Change all backslashes in your Windows path to forward slashes
- Use the directory you expanded the NGINX log file to

11) Now we are ready to setup Elasticsearch to receive the NGINX logs, visualize it, and create Machine Learning jobs to detect anomalies. Fortunately it only takes one command!

```

cd ..
filebeat.exe -e setup nginx
filebeat.exe -e

```

## Mac/Linux Instructions

### Metricbeat

- 1) Open a terminal and navigate to the location that you downloaded metricbeat to

```
cd ~/Downloads/
```

- 2) Expand the file that you downloaded:

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

- 3) Change directory into the metricbeat

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

- 4) List models that are available

```
./metricbeat modules list
```

You should see which modules are **enabled** and which modules are **disabled**. Out of the box the **system** module is the only one that is enabled.

- 5) Before we setup Elasticsearch to accept system metrics we need to tell Metricbeat where Elasticsearch is and provide credentials to login. We do this by editing the configuration file for Metricbeat called `metricbeat.yml`.

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 .yml file because they will cause errors. To learn more about .yml files see this link: <https://en.wikipedia.org/wiki/YAML>

Example:

```
#cloud.id:
```

to

```
cloud.id:  
"testcluster:dXMtZWZdC0xLmF3cy5mb3VuZC5pbyRkZmRiZTEwOWY2MmI0MTMxODhh  
ZTRmM2U4ODYzNTVlZiRjYTEzMTg0MGFkMzc0OWZjYThkZWRhZTU5OWE0MjY2OQ=="
```

and

```
#cloud.auth:
```

to

```
cloud.auth: "elastic:uB2AxBXuR1GM00WwiteZ8VLt"
```

- 6) Now we are ready to setup Elasticsearch to receive the system metric data, visualize it, and create Machine Learning jobs to detect anomalies. Fortunately it only takes one command!

```
./metricbeat -e setup system
```

Make sure you see the following text at the end of the output:

```
2018-12-07T16:29:04.189-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443  
2018-12-07T16:29:04.785-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.1  
2018-12-07T16:29:04.785-0500 INFO kibana/client.go:118 Kibana url: https://ca131840ad3749fca8dedae599a42669.us-east-1.aws.found.io:443  
2018-12-07T16:29:40.086-0500 INFO instance/beat.go:717 Kibana dashboards successfully loaded.  
Loaded dashboards {"version": {
```

- 7) Now run the metricbeat agent. Metrics from your local machine should now be flowing into Elasticsearch!

```
./metricbeat -e
```

## Filebeat

- 1) Open a terminal and navigate to the location that you downloaded filebeat to

```
cd ~/Downloads/
```

2) Expand the file that you downloaded:

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

3) Change directory into the filebeat

```
cd filebeat-<version>-x86_64
```

4) List the modules that are available

```
./filebeat modules list
```

You should see which modules are **enabled** and which modules are **disabled**. Out of the box there are no modules enabled.

```
# ./filebeat modules list  
Enabled:
```

4) List models that are available

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

```
./filebeat modules list
```

You should see which modules are **enabled** and which modules are **disabled**. Out of the box there are no modules enabled.

5) Now let us enable the NGINX module so we can ingest NGINX logs

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

```
# ./filebeat modules list
Enabled:
nginx

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

5) Now let us enable the NGINX module so we can ingest NG

- 6) Before we setup Elasticsearch to accept NGINX logs we need to tell Filebeat where Elasticsearch is and provide credentials to login. We do this by editing the configuration file for Filebeat called `filebeat.yml`.
- 7) Follow the exact same procedure that you did in step #6 when you setup Metricbeat and add the **cloud.id** and **cloud.auth** to `filebeat.yml` using the values from [Lab 0](#)
- 8) Normally Filebeat would scan your system in several common locations for NGINX log files. Since we don't actually have NGINX installed we are going to copy some real NGINX log files to the filesystem and tell the NGINX module where they are located.

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

[https://drive.google.com/file/d/1RUDsDI5WOkVAnLw1xRR3H9zX3slqAht\\_/view?usp=sharing](https://drive.google.com/file/d/1RUDsDI5WOkVAnLw1xRR3H9zX3slqAht_/view?usp=sharing)

- 9) Change directory to the following location

```
cd modules.d
```

- 10) 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.

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



```

- [module:nginx] 18
# 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:

```

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

```

cd ..
./filebeat -e setup nginx
./filebeat -e

```

```

# ./filebeat -e setup nginx
2018-12-11T01:32:03.831-0500 INFO instance/beat.go:592 Home path: [C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64] Config path: [C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64] Data path: [C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64\data] Logs path: [C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64/logs]
2018-12-11T01:32:03.831-0500 INFO instance/beat.go:599 Beat UUID: 3c16d505-9652-42d7-b7c2-547ad985cb1d
2018-12-11T01:32:03.837-0500 INFO [beat] instance/beat.go:825 Beat info {"system_info": {"path": {"config": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64", "data": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64\data", "home": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64", "logs": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64/logs"}, "type": "filebeat", "uuid": "3c16d505-9652-42d7-b7c2-547ad985cb1d"}}}
2018-12-11T01:32:03.838-0500 INFO [beat] instance/beat.go:834 Build info {"system_info": {"build": {"commit": "b48d073b84e874a182c122d8ef2bad867f714a11", "libbeat": "6.5.2", "time": "2018-11-29T23:03:04.000Z", "version": "6.5.2"}}}
2018-12-11T01:32:03.838-0500 INFO [beat] instance/beat.go:837 Go runtime info {"system_info": {"go": {"os": "darwin", "arch": "amd64", "max_procs": 8, "version": "go1.10.3"}}}
2018-12-11T01:32:03.839-0500 INFO [beat] instance/beat.go:841 Host info {"system_info": {"host": {"architecture": "x86_64", "boot_time": "2018-12-07T13:04:35.829985-05:00", "name": "Shawns-MacBook-Pro-2.local", "ip": ["127.0.0.1/8", "::1/128", "fe80::1/64", "192.168.1.13/24", "fe80::f85a:d0ff:feaa:5047/64", "fe80::56c0:da23:8d5a:7418/64", "fe80::5258:6fd:32c3:ca2d/64", "fe80::aede:48ff:fe00:1122/64"], "kernel_version": "18.0.0", "mac": ["8c:85:90:ad:2d:5e", "e2:00:28:89:84:01", "e2:00:28:89:84:00", "e2:00:28:89:84:05", "e2:00:28:89:84:04", "e2:00:28:89:84:01", "0e:85:90:ad:2d:5e", "fa:5a:d0:aa:50:47", "ac:de:48:00:11:22"], "os": {"family": "darwin", "platform": "darwin", "name": "Mac OS X", "version": "10.14", "major": 10, "minor": 14, "patch": 0, "build": "18A391"}, "timezone": "EST", "timezone_offset_sec": -18000}}}
2018-12-11T01:32:03.840-0500 INFO [beat] instance/beat.go:870 Process info {"system_info": {"process": {"cwd": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64", "exe": "C:\Users\shh\Development\filebeat-6.5.2-darwin-x86_64\filebeat", "name": "filebeat", "pid": 5719, "ppid": 2954, "start_time": "2018-12-11T01:32:03.804-0500"}}}
2018-12-11T01:32:03.840-0500 INFO instance/beat.go:278 Setup Beat: filebeat; Version: 6.5.2
2018-12-11T01:32:06.851-0500 INFO add_cloud_metadata/add_cloud_metadata.go:319 add_cloud_metadata: hosting provider type not detected.
2018-12-11T01:32:06.851-0500 INFO [publisher] pipeline/module.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T01:32:06.853-0500 INFO [publisher] pipeline/module.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T01:32:07.258-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.2
2018-12-11T01:32:07.289-0500 INFO template/load.go:129 Template already exists and will not be overwritten.
Loaded index template
Loading dashboards (Kibana must be running and reachable)
2018-12-11T01:32:07.298-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T01:32:07.536-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.2
2018-12-11T01:32:07.536-0500 INFO kibana/client.go:118 Kibana url: https://ca131840ad3749fca8dadae599a42669.us-east-1.aws.found.io:443
2018-12-11T01:32:49.235-0500 INFO instance/beat.go:717 Kibana dashboards successfully loaded.
Loaded dashboards
2018-12-11T01:32:49.235-0500 INFO elasticsearch/client.go:163 Elasticsearch url: https://dfdbe109f62b413188ae4f3e886355ef.us-east-1.aws.found.io:443
2018-12-11T01:32:49.535-0500 INFO elasticsearch/client.go:712 Connected to Elasticsearch version 6.5.2
2018-12-11T01:32:49.535-0500 INFO kibana/client.go:118 Kibana url: https://ca131840ad3749fca8dadae599a42669.us-east-1.aws.found.io:443
Loaded machine learning job configurations

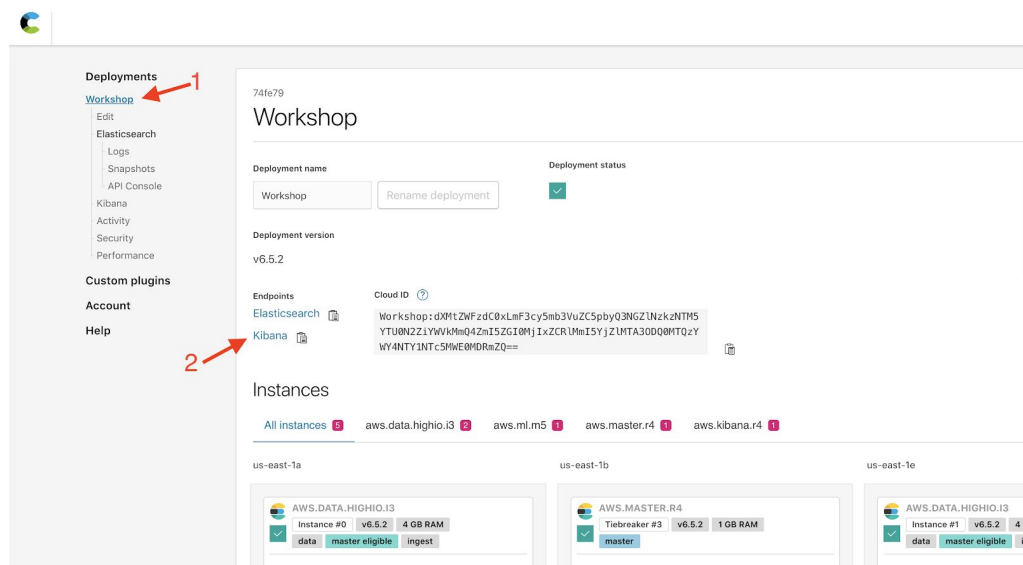
```



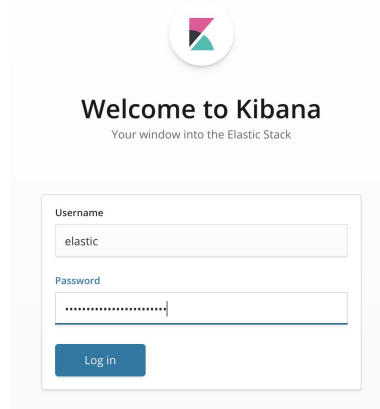
# Validate Data in Kibana

At this point let's look at the data in Kibana by looking at the index.

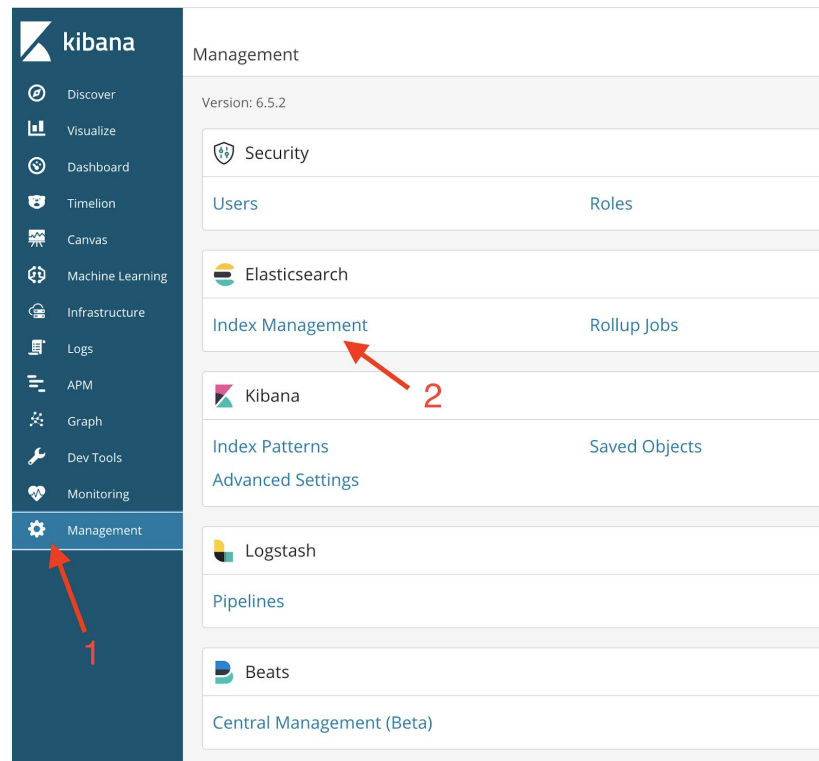
- 1) Log into your cloud console and click on the Kibana link



- 2) Log into Kibana with the credentials you obtained in [Lab 0](#).



### 3) Click on the Management Link



- 4) Look for Indexes named Metricbeat-<version>-YYYY.MM.DD where version is the current version of the product and YYYY, MM, and DD represent the year, month, and day respectively. Examine Docs Count, Storage Size, and Primary Storage Size. Realistic data like this provides a wonderful opportunity to look at your data and how much disk space it consumes to help size your environment accurately.

## Index management

Update your Elasticsearch indices individually or in bulk

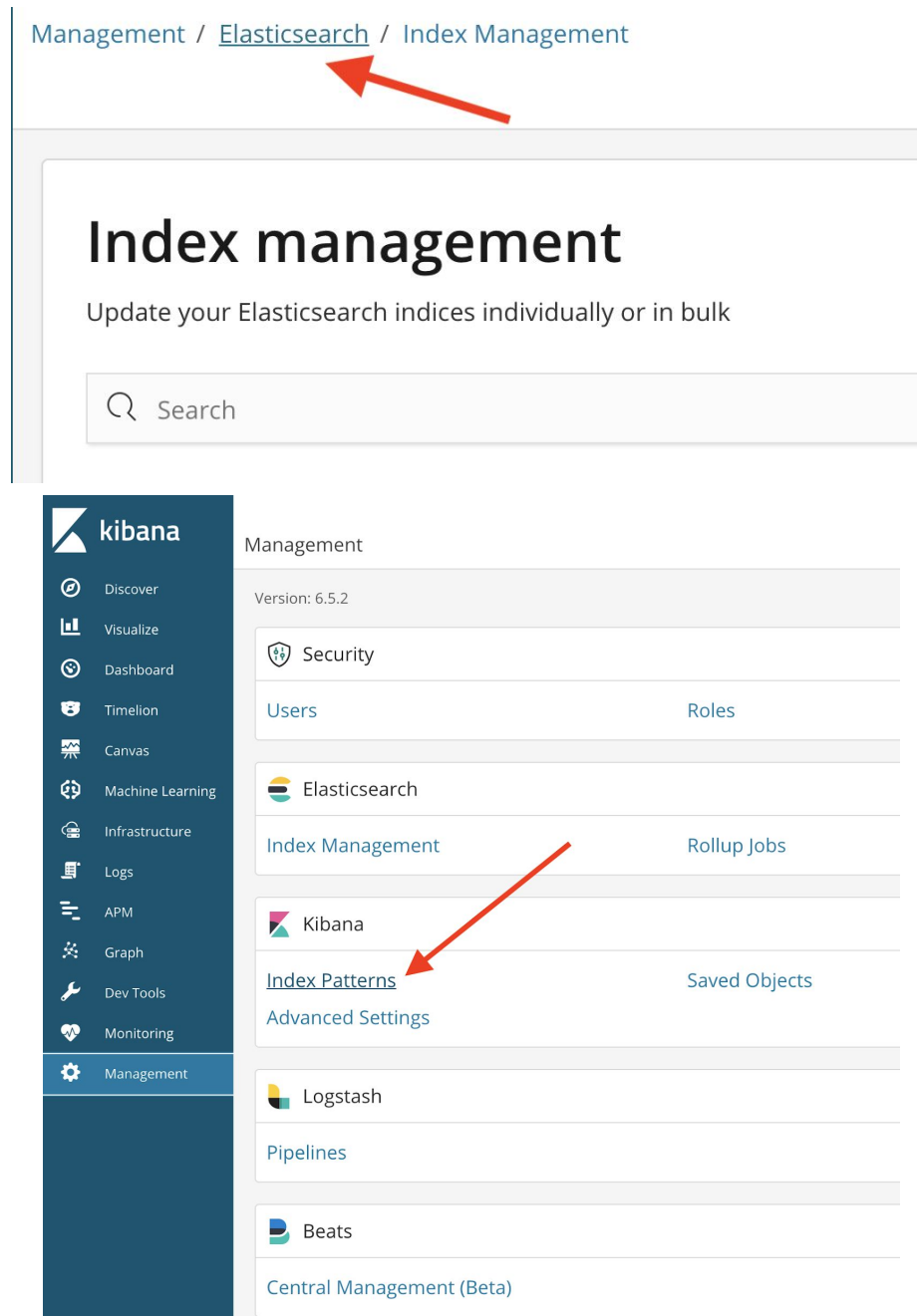
☐ ☒ Include system indices

<input type="checkbox"/> Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Primary storage size
<input type="checkbox"/> filebeat-6.5.0-2018.12.07	<span>● green</span>	open	3	1	984887	783.7mb	391.8mb
<input type="checkbox"/> metricbeat-6.5.1-2018.12.07	<span>● green</span>	open	1	1	8012	3.2mb	1.6mb
<input type="checkbox"/> divvy	<span>● green</span>	open	2	0	3829003	1.2gb	1.2gb
<input type="checkbox"/> metricbeat-6.5.0-2018.12.07	<span>● green</span>	open	1	1	10729	4.7mb	2.3mb
<input type="checkbox"/> checkpoint	<span>● green</span>	open	1	1	6000	8.2mb	4.1mb
<input type="checkbox"/> metricbeat-6.5.1-2018.11.28	<span>● green</span>	open	5	1	650346	452.7mb	226.3mb
<input type="checkbox"/> metricbeat-6.5.1-2018.12.10	<span>● green</span>	open	1	1	39088	17.2mb	9.3mb
<input type="checkbox"/> metricbeat-6.5.1-2018.11.29	<span>● green</span>	open	5	1	852450	571mb	285.5mb
<input type="checkbox"/> kibana_sample_data_ecommerce	<span>● green</span>	open	1	0	4675	5mb	5mb
<input type="checkbox"/> filebeat-6.5.2-2018.12.10	<span>● green</span>	open	5	1	111546	93mb	46.6mb

Rows per page: 10

< 1 2 >

- 5) Now click on the “elasticsearch” breadcrumb in the upper left hand corner of the screen and click on Index Patterns. Index patterns tell Kibana which Elasticsearch indices you want to explore. An index pattern can match the name of a single index, or include a wildcard (\*) to match multiple indices.



- 6) Now verify that metricbeat and filebeat index patterns exist. Notice the wildcard pattern. Examine the fields, notice the field data type, whether it is searchable and aggregatable.

Discover

Visualize

Dashboard

Timeline

Canvas

Machine Learning

Infrastructure

Logs

APM

Graph

Dev Tools

Monitoring

Management

elastic

Logout

Management / Kibana

Index PatternsSaved ObjectsSpacesReportingAdvanced Settings

Create index pattern

★ checkpo\*

divvy\*

filebeat-\*

metricbeat-\*

metricbeat-\*

Time Filter field name: @timestamp

This page lists every field in the **metricbeat-\*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API.

Fields (1852)Scripted fields (0)Source filters (0)

Filter

All field types

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date	Date			
_id	string				
_index	string				
_score	number				
_source	_source				
_type	string				
aerospike.namespace.client.delete.error	number				
aerospike.namespace.client.delete.not_found	number				
aerospike.namespace.client.delete.success	number				
aerospike.namespace.client.delete.timeout	number				

Rows per page: 10

< 1 2 3 4 5 ... 186 >

7) Congratulations, you are now ready for Lab 2.