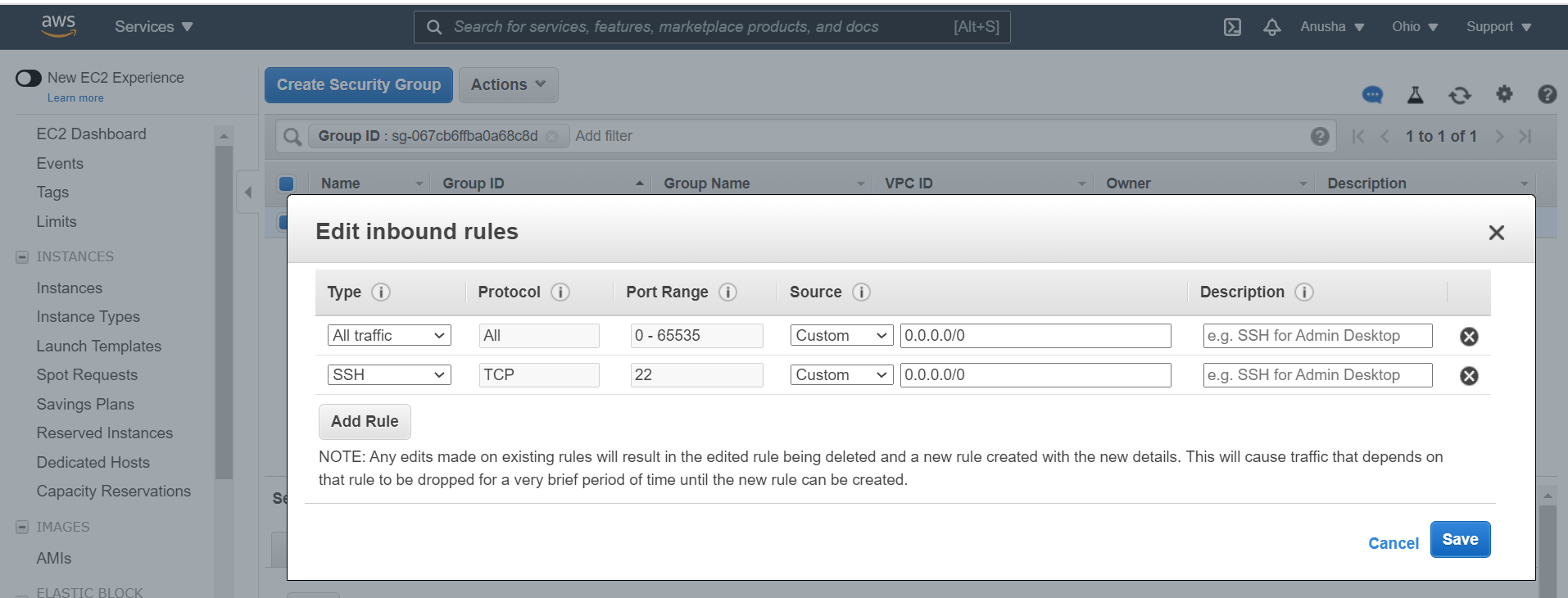
Setup elk

**Prerequisites:**

* Create Ec2 server and enable security group like below.

****

**Java 8**

sudo yum install java-11-openjdk-devel -y

**Nginx**

sudo yum install epel-release -y

sudo yum install nginx -y

sudo systemctl start nginx

sudo systemctl enable nginx

**Elasticsearch**

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

vi /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-6.x]

name=Elasticsearch repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

sudo yum install elasticsearch -y

sudo systemctl start elasticsearch  
sudo systemctl enable elasticsearch

sudo systemctl status elasticsearch

**Kibana Dashboard**

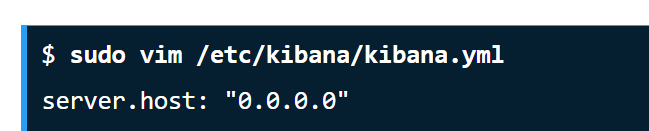
sudo yum install kibana -y

sudo systemctl enable kibana

sudo systemctl start kibana

vi /etc/kibana/kibana.yml

add below line in kibana.yml



systemctl restart kibana

systemctl status kibana

**Logstash**

sudo yum install logstash -y

sudo vi /etc/logstash/conf.d/02-beats-input.conf

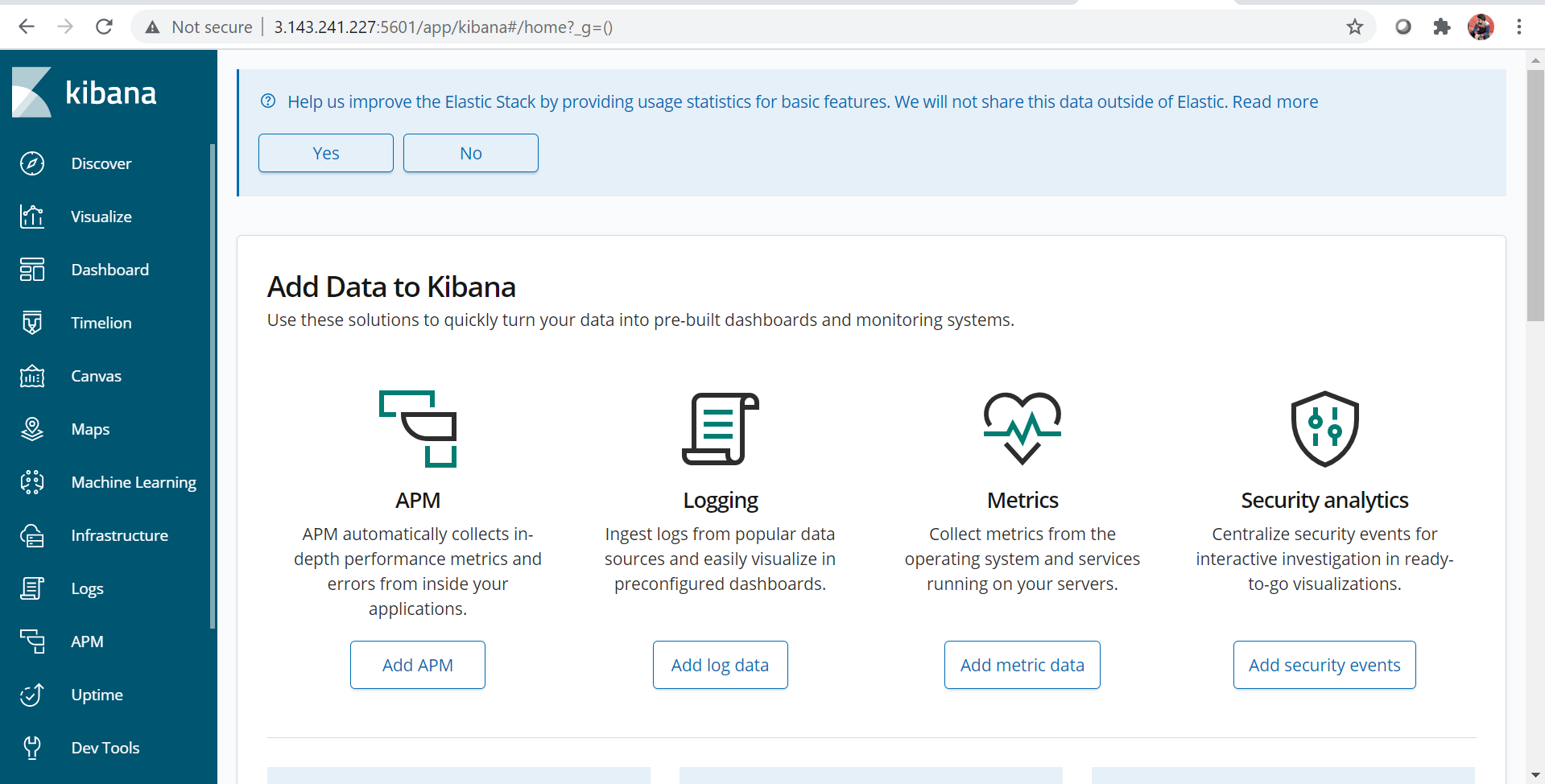
sudo systemctl start logstash

sudo systemctl enable logstash

sudo systemctl status logstash

Open browser and search below URL

[http://3.143.241.227:5601/](http://3.143.241.227:5601/app/kibana#/home?_g=())



Metricbeat Configuration:

* Go to Jenkins Server and Install Metricbeat using below Commands.
* Before installing Metricbeat install below dependency packages.
* **Java 8**
* sudo yum install java-11-openjdk-devel -y
* **Nginx**

sudo yum install epel-release -y

sudo yum install nginx -y

sudo systemctl start nginx

sudo systemctl enable nginx

* **Elasticsearch**

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

vi /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-6.x]

name=Elasticsearch repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

sudo yum install elasticsearch -y

sudo systemctl start elasticsearch  
sudo systemctl enable elasticsearch

sudo systemctl status elasticsearch

yum install metricbeat -y

systemctl enable metricbeat

systemctl start metricbeat

systemctl status metricbeat

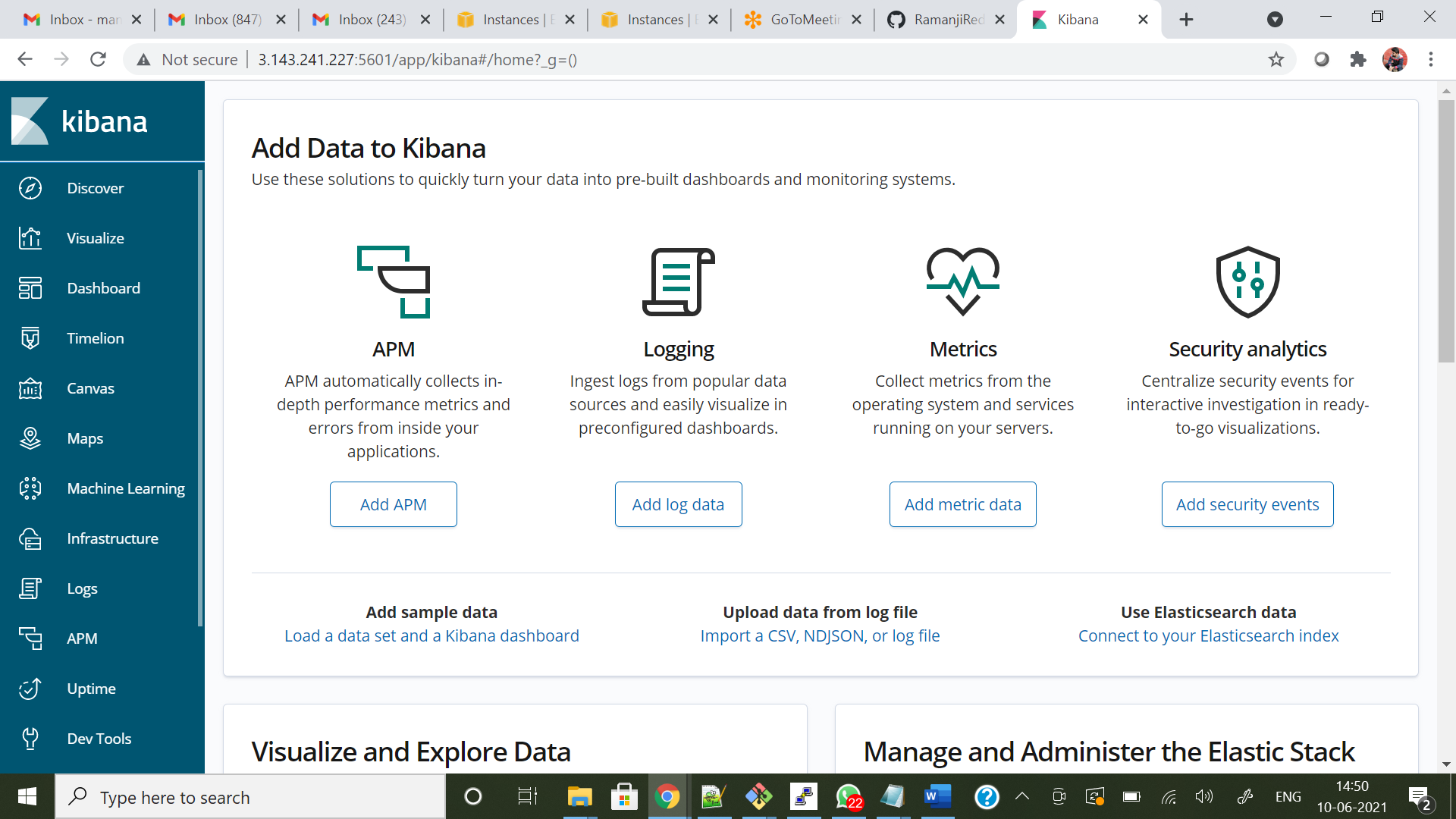
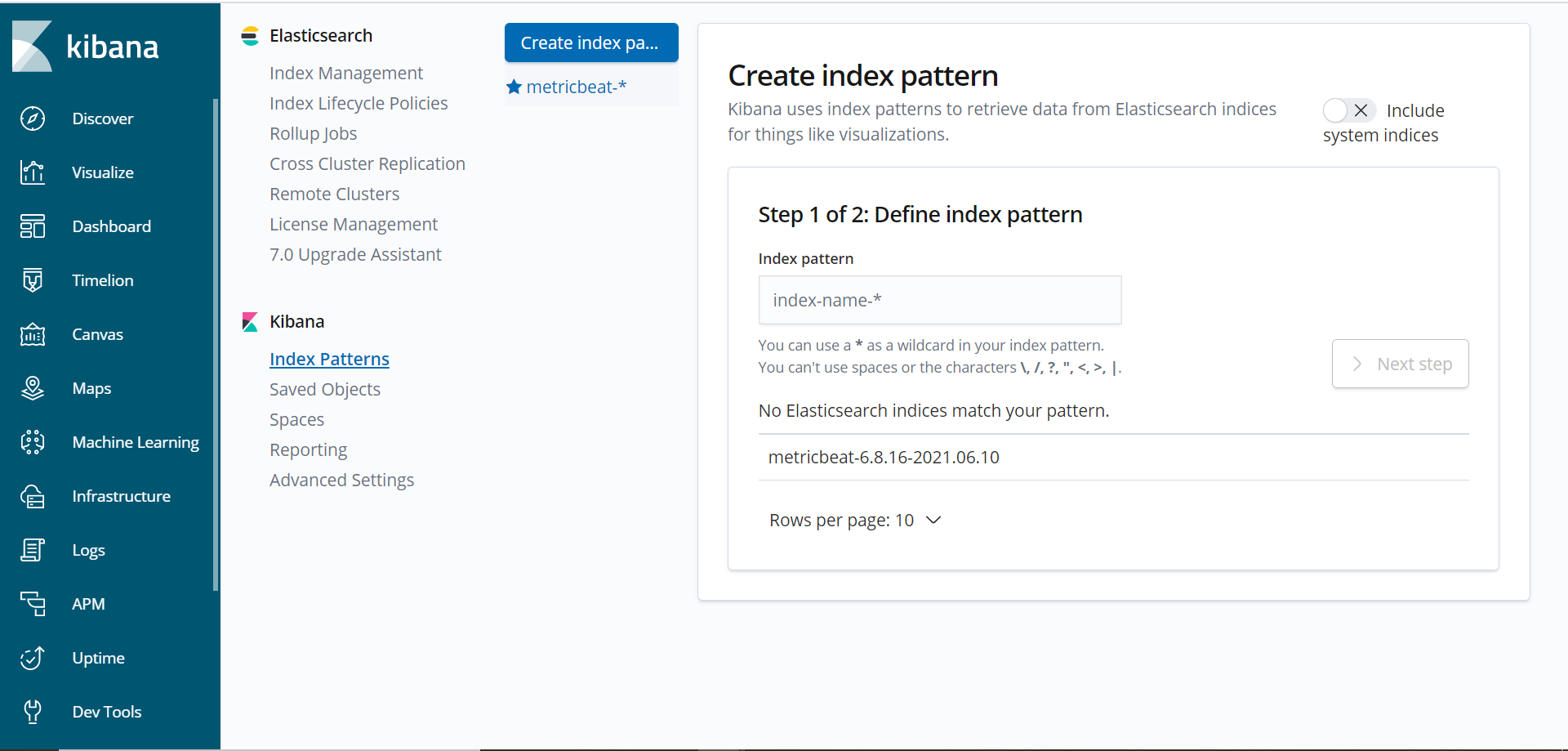
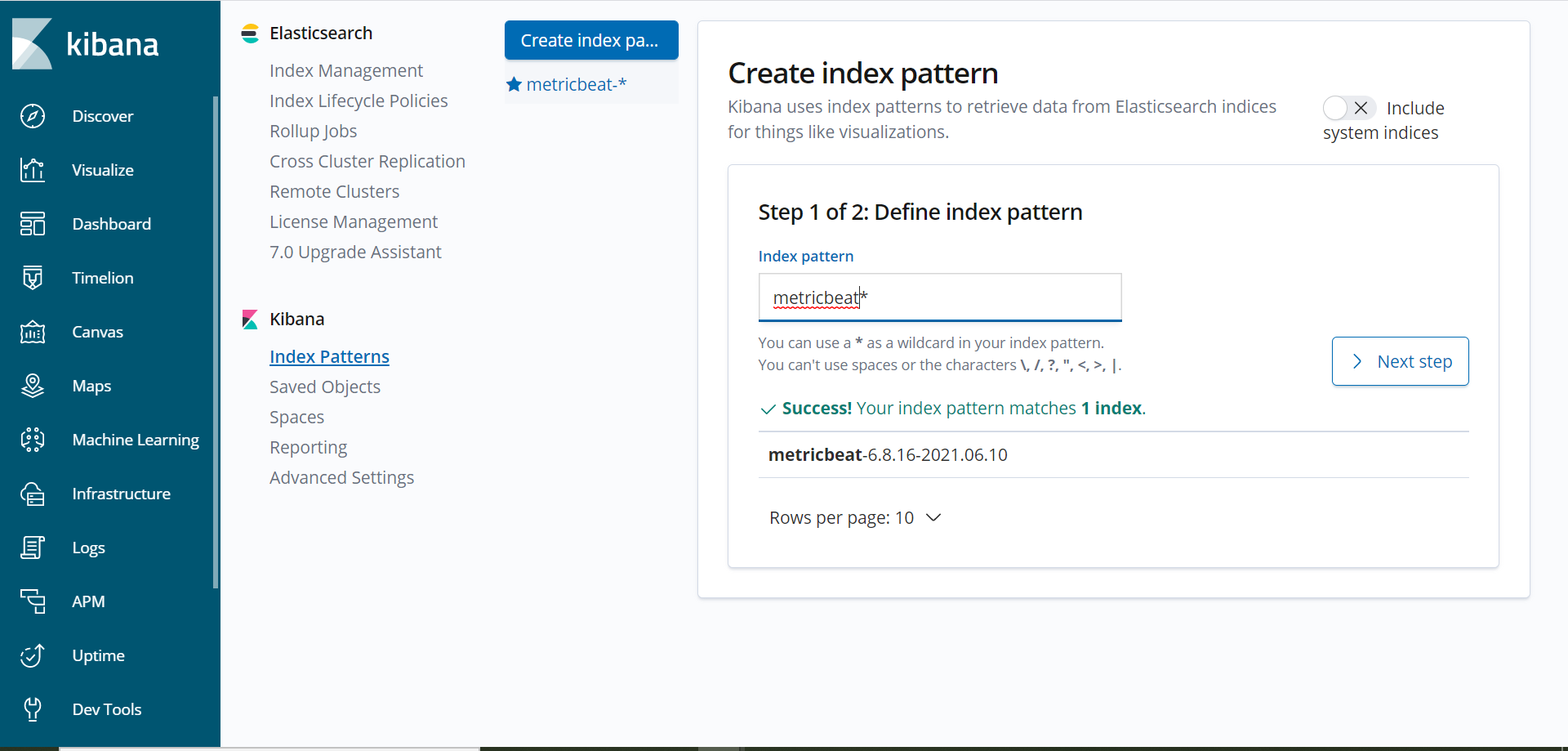
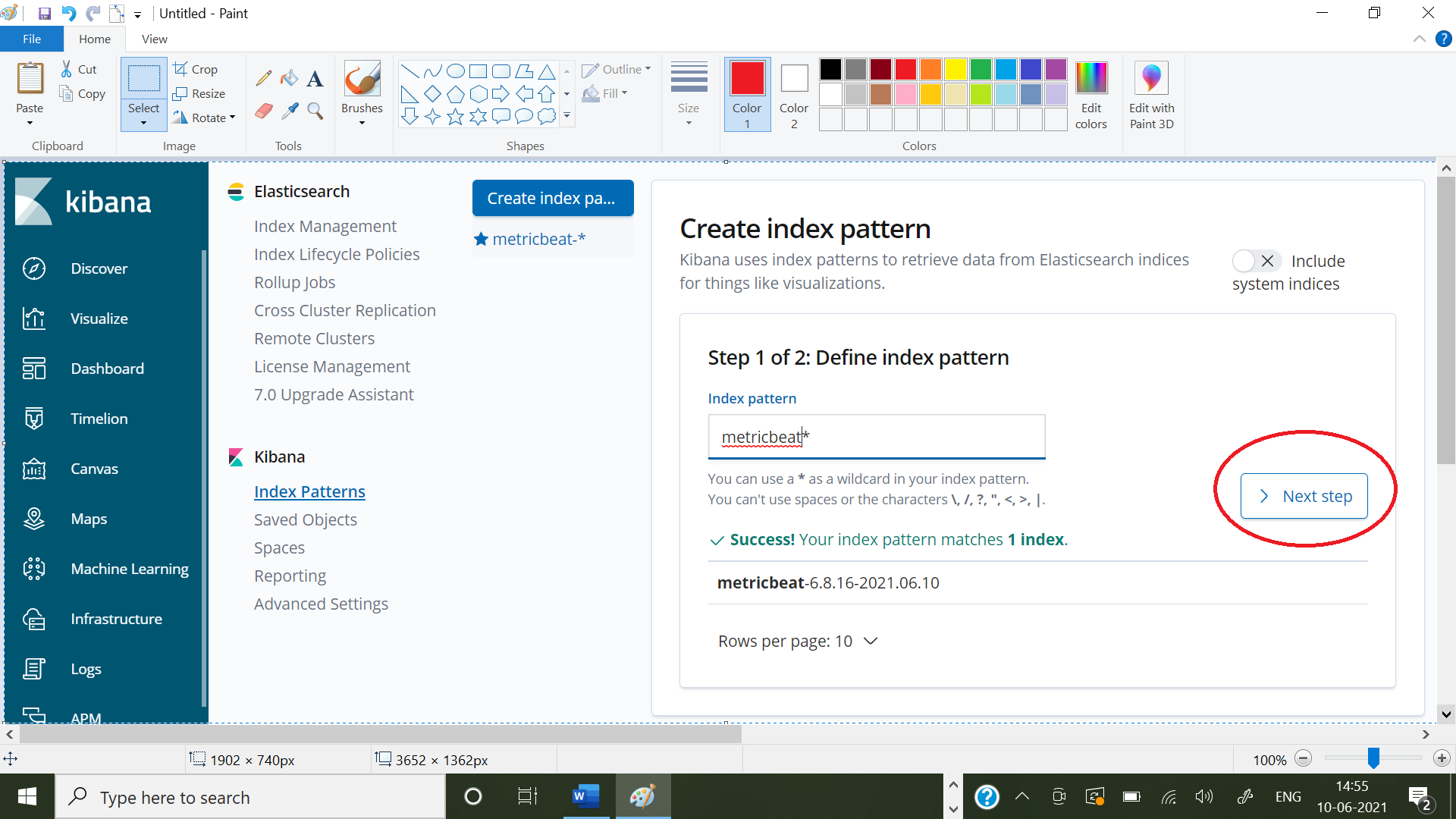
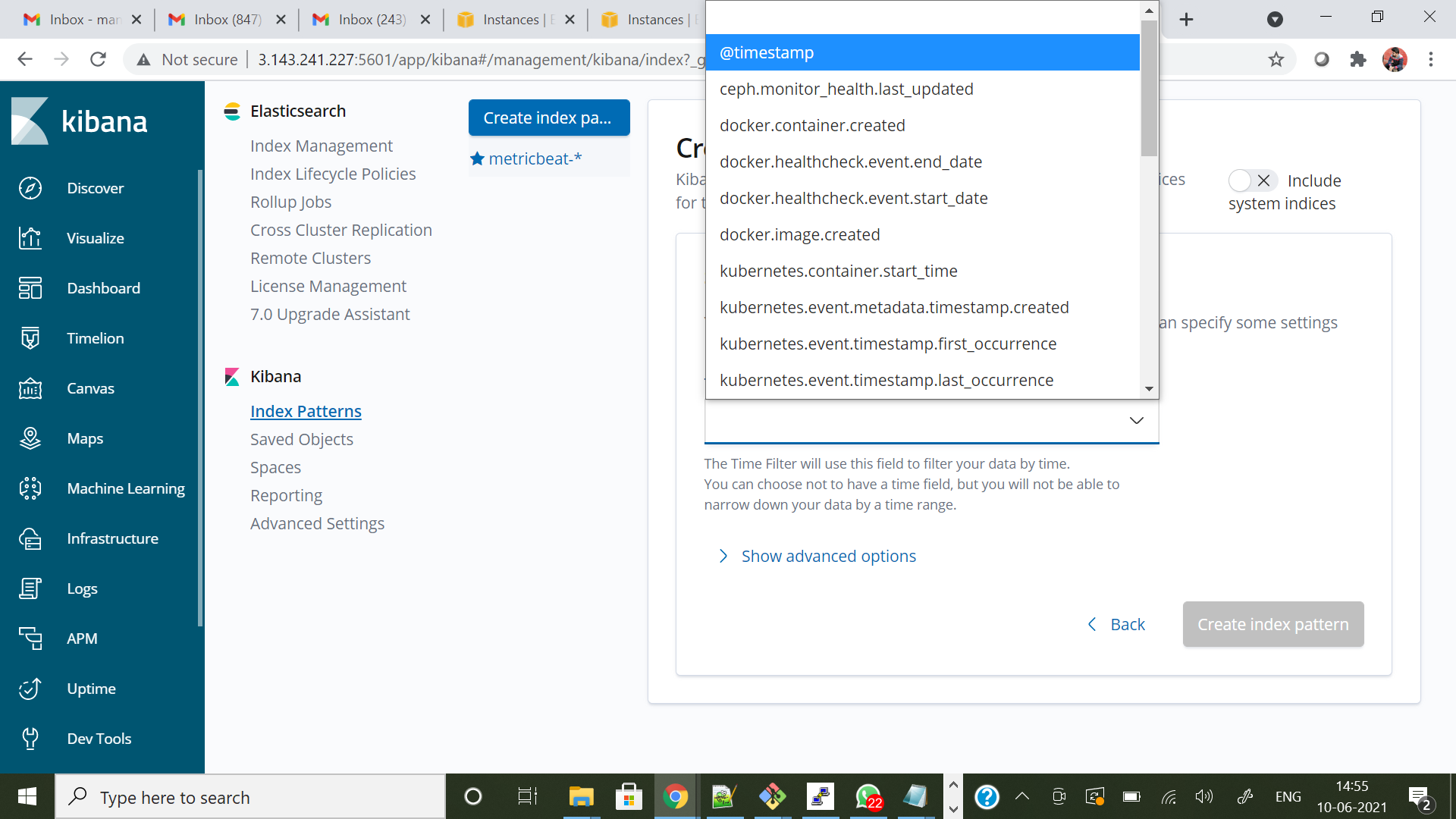
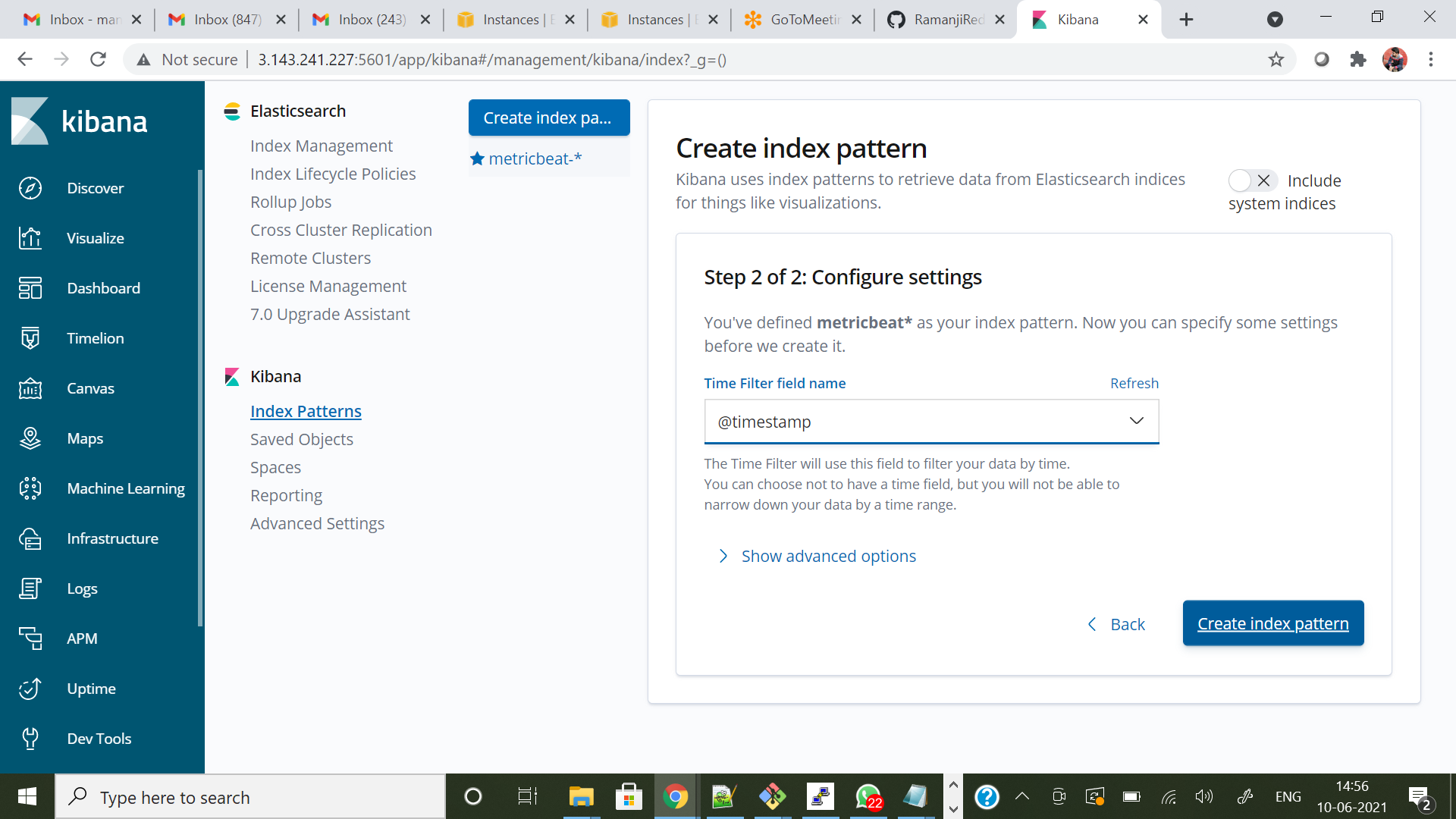
* Go to below location and add ELK server IP like below

vim /etc/metricbeat/metricbeat.yml

|  |
| --- |
| ###################### Metricbeat Configuration Example #######################  # This file is an example configuration file highlighting only the most common  # options. The metricbeat.reference.yml file from the same directory contains all the  # supported options with more comments. You can use it as a reference.  #  # You can find the full configuration reference here:  # https://www.elastic.co/guide/en/beats/metricbeat/index.html  #========================== Modules configuration ============================  metricbeat.config.modules:  # Glob pattern for configuration loading  path: ${path.config}/modules.d/\*.yml  # Set to true to enable config reloading  reload.enabled: false  # Period on which files under path should be checked for changes  #reload.period: 10s  #==================== Elasticsearch template setting ==========================  setup.template.settings:  index.number\_of\_shards: 1  index.codec: best\_compression  #\_source.enabled: false  #================================ General =====================================  # The name of the shipper that publishes the network data. It can be used to group  # all the transactions sent by a single shipper in the web interface.  #name:  # The tags of the shipper are included in their own field with each  # transaction published.  #tags: ["service-X", "web-tier"]  # Optional fields that you can specify to add additional information to the  # output.  #fields:  # env: staging  #============================== Dashboards =====================================  # These settings control loading the sample dashboards to the Kibana index. Loading  # the dashboards is disabled by default and can be enabled either by setting the  # options here, or by using the `-setup` CLI flag or the `setup` command.  #setup.dashboards.enabled: false  # The URL from where to download the dashboards archive. By default this URL  # has a value which is computed based on the Beat name and version. For released  # versions, this URL points to the dashboard archive on the artifacts.elastic.co  # website.  #setup.dashboards.url:  #============================== Kibana =====================================  # Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.  # This requires a Kibana endpoint configuration.  setup.kibana:  # Kibana Host  # Scheme and port can be left out and will be set to the default (http and 5601)  # In case you specify and additional path, the scheme is required: http://localhost:5601/path  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601  #host: "localhost:5601"  host: "http://3.143.241.227:5601/"  # Kibana Space ID  # ID of the Kibana Space into which the dashboards should be loaded. By default,  # the Default Space will be used.  #space.id:  #============================= Elastic Cloud ==================================  # These settings simplify using metricbeat with the Elastic Cloud (https://cloud.elastic.co/).  # The cloud.id setting overwrites the `output.elasticsearch.hosts` and  # `setup.kibana.host` options.  # You can find the `cloud.id` in the Elastic Cloud web UI.  #cloud.id:  # The cloud.auth setting overwrites the `output.elasticsearch.username` and  # `output.elasticsearch.password` settings. The format is `<user>:<pass>`.  #cloud.auth:  #================================ Outputs =====================================  # Configure what output to use when sending the data collected by the beat.  #-------------------------- Elasticsearch output ------------------------------  #output.elasticsearch:  # Array of hosts to connect to.  #hosts: ["localhost:9200"]  # hosts: ["http://3.143.241.227:9200"]  # Enabled ilm (beta) to use index lifecycle management instead daily indices.  #ilm.enabled: false  # Optional protocol and basic auth credentials.  #protocol: "https"  #username: "elastic"  #password: "changeme"  #----------------------------- Logstash output --------------------------------  output.logstash:  # The Logstash hosts  hosts: ["http://3.143.241.227:5044"]  # Optional SSL. By default is off.  # List of root certificates for HTTPS server verifications  #ssl.certificate\_authorities: ["/etc/pki/root/ca.pem"]  # Certificate for SSL client authentication  #ssl.certificate: "/etc/pki/client/cert.pem"  # Client Certificate Key  #ssl.key: "/etc/pki/client/cert.key"  #================================ Processors =====================================  # Configure processors to enhance or manipulate events generated by the beat.  processors:  - add\_host\_metadata: ~  - add\_cloud\_metadata: ~  #================================ Logging =====================================  # Sets log level. The default log level is info.  # Available log levels are: error, warning, info, debug  #logging.level: debug  # At debug level, you can selectively enable logging only for some components.  # To enable all selectors use ["\*"]. Examples of other selectors are "beat",  # "publish", "service".  #logging.selectors: ["\*"]  #============================== Xpack Monitoring ===============================  # metricbeat can export internal metrics to a central Elasticsearch monitoring  # cluster. This requires xpack monitoring to be enabled in Elasticsearch. The  # reporting is disabled by default.  # Set to true to enable the monitoring reporter.  #xpack.monitoring.enabled: false  # Uncomment to send the metrics to Elasticsearch. Most settings from the  # Elasticsearch output are accepted here as well. Any setting that is not set is  # automatically inherited from the Elasticsearch output configuration, so if you  # have the Elasticsearch output configured, you can simply uncomment the  # following line.  #xpack.monitoring.elasticsearch: |
|  |
| * Restart the metricbeat using below command * systemctl restart metricbeat * Check the metricbeat status * systemctl status metricbeat |

* Restart the kibana using below command

systemctl restart kibana

* Go to Kibana Dashboard.
* 
* Click on Discover
* 
* Create Index patterns.
* 
* 
* Click on @timestapm
* 
* Create index pattern
* 
* Click on discover
* 