ELK Stack

Visualize Apache Logs With Elastic Stack on Ubuntu

- Update system package and install java runtime

```
$ sudo apt-get update && sudo apt-get upgrade

$ sudo apt-get install default-jre-headless
```

- Install the Elastic APT Repository → this package repositories contain all of the necessary packages include Elasticsearch, log stash and kibana

```
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elastics
sudo apt-key add -
$ echo "deb https://artifacts.elastic.co/packages/7.x/apt
sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
$ sudo apt-get update
```

- Install Elasticsearch
  1. `sudo apt-get install elasticsearch`
  2. Set up heap size for JVM

```
File: /etc/elasticsearch/jvm.options

-Xmx(one-quarter of your server's available memory)m

Ex.
-Xmx1g (if host have 4g of memory)
```

  3. Start elasticsearch

```
 $ sudo systemctl enable elasticsearch
 $ sudo systemctl start elasticsearch
```

  4. confirm that the Elasticsearch API is available

```
$ curl localhost:9200

response should be :

{
  "name" : "vm-module",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "TZ0bzoEGSaKuUaktiQQLQQ",
  "version" : {
    "number" : "7.17.21",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "d38e4b028f4a9784bb74de339ac1b877e2d
    "build_date" : "2024-04-26T04:36:26.745220156Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta
  },
  "tagline" : "You Know, for Search"
}
```

- Install logstash and cabana
  - `sudo apt-get install logstash`
  - `sudo apt-get install kibana`
- Configure the Elastic Stack
  - Overwrite Elasticsearch setup from create multiple shard to use only one shard.
    - Create a temporary JSON

```
{
  "index_patterns": ["*"],
  "template": {
    "settings": {
      "index": {
        "number_of_shards": 1,
```

```
        "number_of_replicas": 0
      }
    }
  }
}
```

- Use `curl` to create an index template with these settings that is applied to all indices created hereafter:

```
$ curl -XPUT -H'Content-type: application/json' ht
tp://localhost:9200/_index_template/defaults -d @t
emplate.json
```

- Configure Logstash

  collect Apache access logs, Logstash must be configured to watch any necessary files and then process them, eventually sending them to Elasticsearch.

  - Set up heap size for logstash at `/etc/logstash/jvm.options`
  - Create the following Logstash configuration

```
File: /etc/logstash/conf.d/apache.conf

input {
  file {
    path => '/var/www/*/logs/access.log'
    start_position => 'beginning'
  }
}

filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
}

output {
```

```
  elasticsearch { }
}
```

- Start all service

```
$ sudo systemctl enable logstash
$ sudo systemctl start logstash

$ sudo systemctl enable kibana
$ sudo systemctl start kibana
```

- Install apache2 for test log collecting
  - `sudo apt-get install apache2`
  - change logs dir to appropriate with logstash configuration

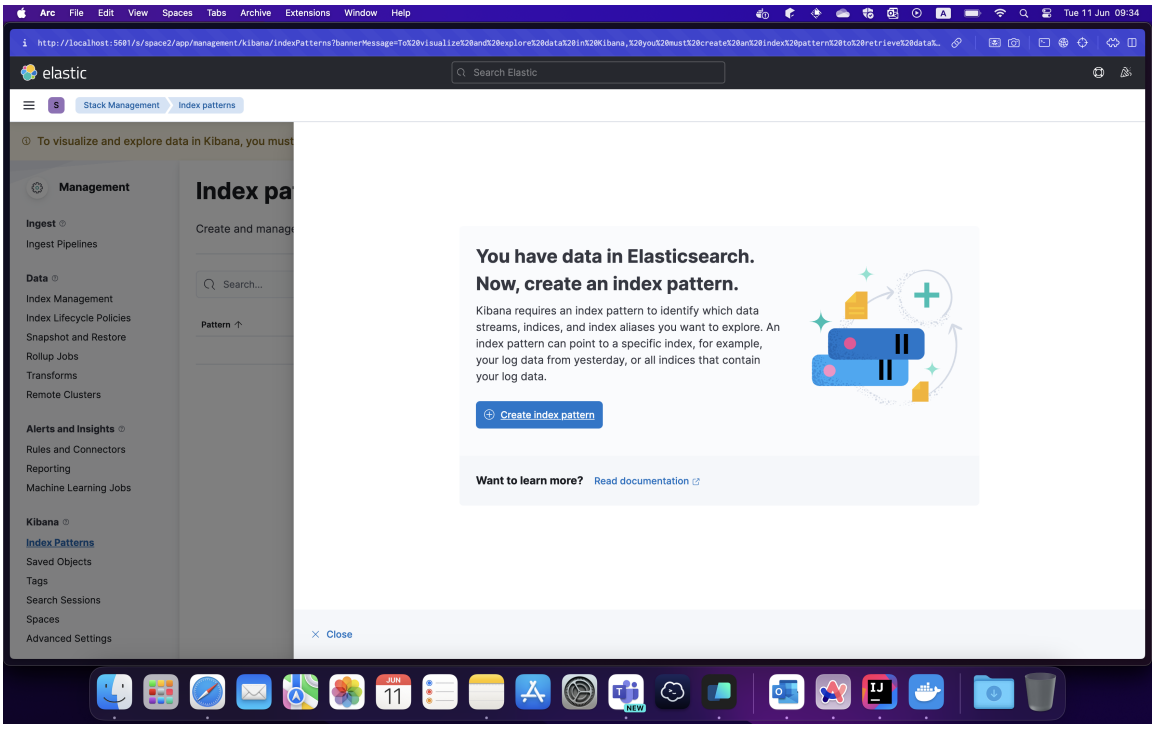
```
$ vim /etc/apache2/sites-available/000-default.conf

ErrorLog /var/www/html/logs/error.log
CustomLog /var/www/html/logs/access.log combined

$ sudo mkdir /var/www/html/logs

$ sudo systemctl restart apache2
```

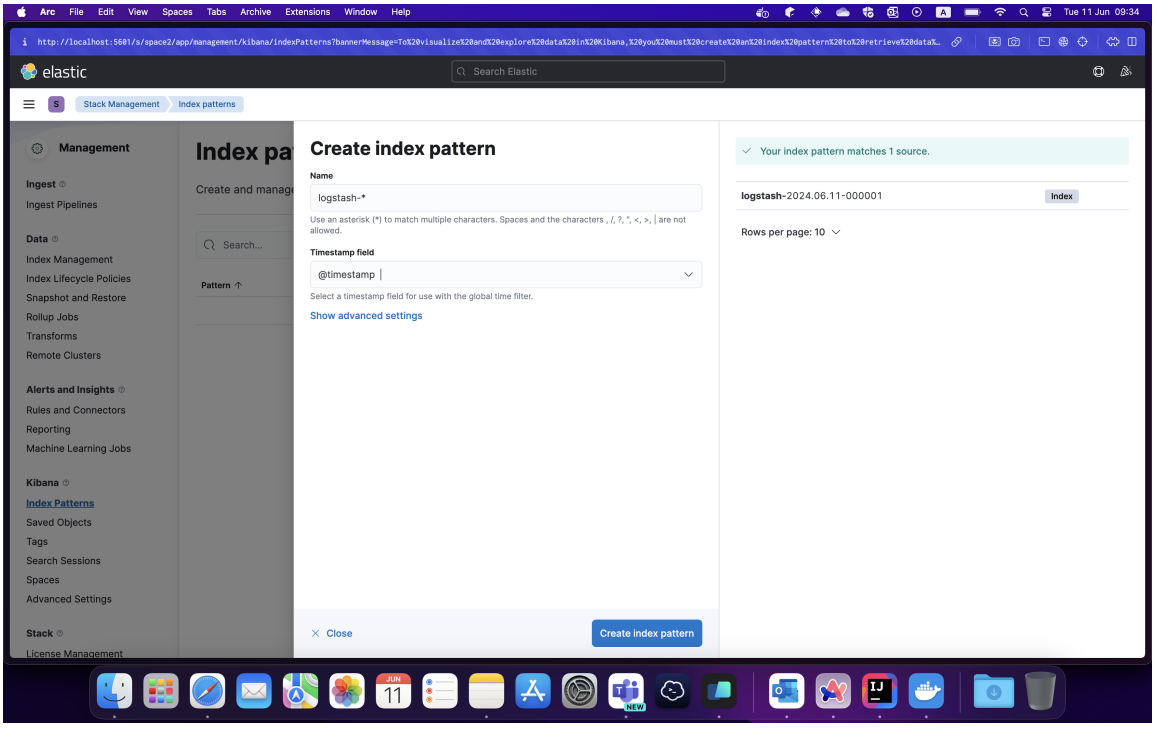
- For testing we need some logs data so that we need to enter apache2 landing page to get logs via : `for i in `seq 1 5` ; do curl localhost ; sleep 0.2 ; done`

Watching Logs

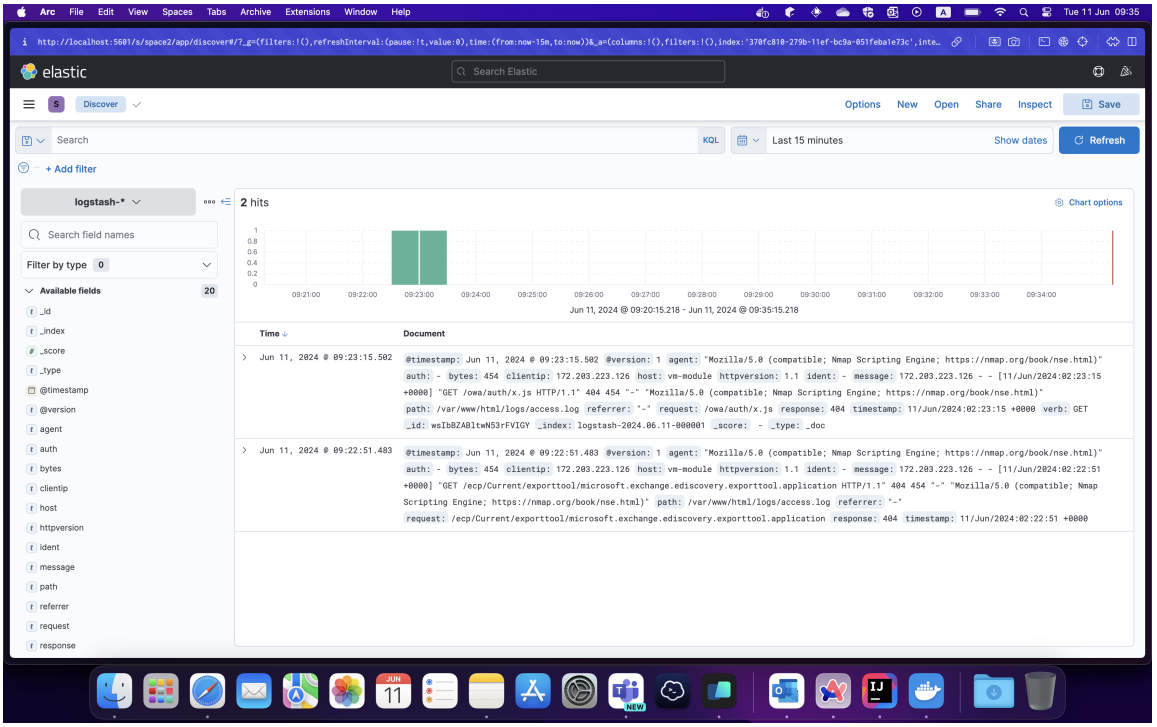
- By default, Kibana binds to the local address `127.0.0.1`. This only permits connections that originate from localhost. This is recommended in order to avoid exposing the dashboard to the public internet. use `ssh` command can forward the port to your workstation.
  - `ssh -N -L 5601:localhost:5601 Username@<IP address of kibana>`
- Open Kibana in your browser at http://localhost:5601.

- Create an index pattern to collect logs data





- Now when back to Discover page again will see


elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
logstash-*
Search field names
Filter by type 0
Available fields 20
_id
_index
_score
_type
@timestamp
@version
agent
auth
bytes
clientip
host
httpversion
ident
message
path
referrer
request
response
2 hits
Chart options
Jun 11, 2024 @ 09:20:15.218 - Jun 11, 2024 @ 09:35:15.218
Time
Document
Jun 11, 2024 @ 09:23:15.502
@timestamp: Jun 11, 2024 @ 09:23:15.502 @version: 1 agent: "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" auth: - bytes: 454 clientip: 172.203.223.126 host: vm-module httpversion: 1.1 ident: - message: 172.203.223.126 - - [11/Jun/2024:02:23:15 +0000] "GET /owa/auth/x.js HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" path: /var/www/html/logs/access.log referrer: "-" request: /owa/auth/x.js response: 404 timestamp: 11/Jun/2024:02:23:15 +0000 verb: GET _id: wsIbBZAB1twN53rFVIGY _index: logstash-2024.06.11-000001 _score: - _type: _doc
Jun 11, 2024 @ 09:22:51.483
@timestamp: Jun 11, 2024 @ 09:22:51.483 @version: 1 agent: "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" auth: - bytes: 454 clientip: 172.203.223.126 host: vm-module httpversion: 1.1 ident: - message: 172.203.223.126 - - [11/Jun/2024:02:22:51 +0000] "GET /ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" path: /var/www/html/logs/access.log referrer: "-" request: /ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application response: 404 timestamp: 11/Jun/2024:02:22:51 +0000