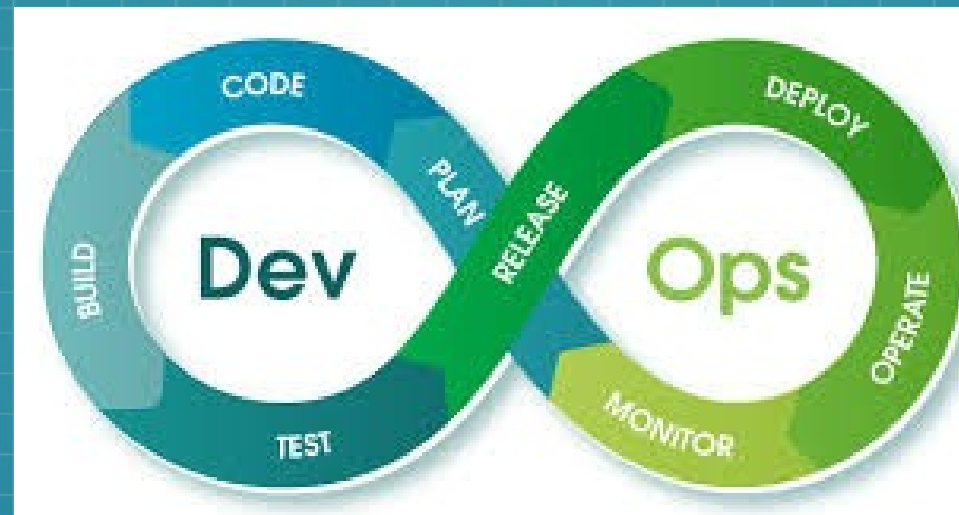
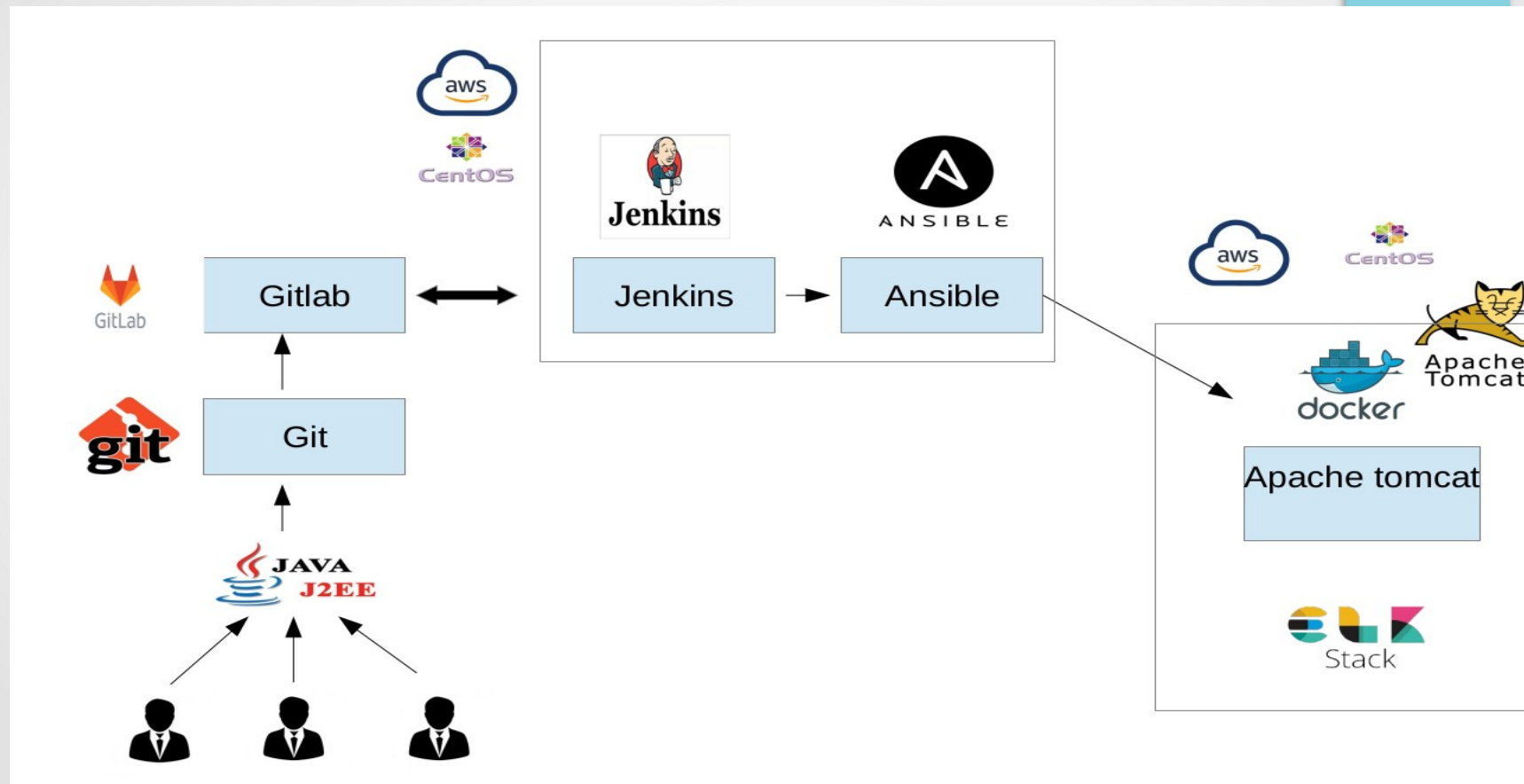


Formation Devops par la pratique



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

Objectif : Réaliser une pipeline Git-Gitlab-Jenkins-Ansible-Docker



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

Objectif : Réaliser une pipeline Git-Gitlab-Jenkins-Ansible-Docker

Pour atteindre l'objectif, on va décomposer le pipeline en plusieurs projets pour bien comprendre comment ça passe.

Projets :

- 1)- Déploiement Manuelle
- 2)- Git-Gitlab-Jenkins
- 3)- Git-Gitlab-Jenkins-Tomcat
- 4)- Git-Gitlab-Jenkins-Ansible-Tomcat
- 5)- Git-Gitlab-Jenkins-Ansible-Docker
- 6)- ELK Stack
- 7)- kubernetes
- 8)- Prometheus-Graphana



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

Parcours de Formation DEVOPS

- Révision commande Linux
- Git, Gitlab
- Jenkins
- Ansible
- Docker
- ELK stack
- Kubernetes
- Prometheus-Graphana



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Collectez et analysez les journaux Docker à l'aide de Filebeat et Elastic Stack (ELK)

Les messages de journal Docker sont un outil très utile pour une variété de tâches informatiques, mais le simple fait d'utiliser la commande **docker logs** ne sont souvent pas suffisants. Même avec quelques conteneurs en cours d'exécution, il est très difficile de trouver quelque chose d'utile dans les journaux et encore plus difficile lorsque vous exécutez docker sur plusieurs machines. La meilleure solution est d'agréger les journaux de toutes les machines et conteneurs, puis vous pouvez facilement les rechercher, les analyser ou faire tout ce que vous voulez avec eux. L'un des outils les plus utilisés pour ce type de problème est Elastic Stack, également connu sous le nom d'ELK.

Qu'est-ce que ELK? ELK est un acronyme pour une collection étonnante et puissante de trois projets open source développés par Elastic.co: Elasticsearch, Logstash et Kibana.

ELK ou également connu sous le nom d'Elastic Stack est une solution complète d'analyse de journal de bout en bout qui aide à rechercher, analyser et visualiser en profondeur le journal généré à partir de différentes machines.

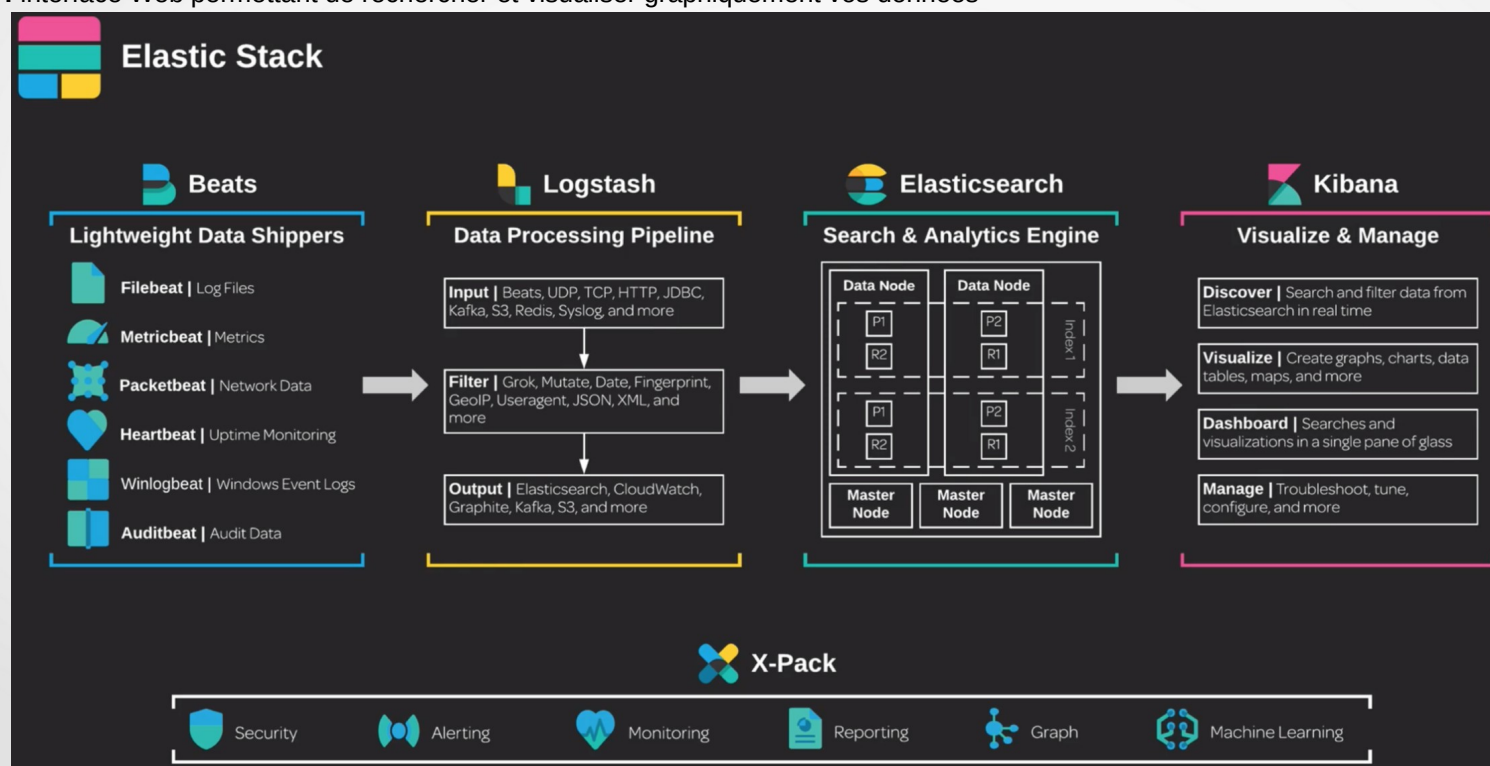


Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

La suite ELK est composée de 3 applications : **logstash**, **Elastic Search** et **Kibana** :

- 1- **LOGSTASH** : extrait les données des fichiers de log, les filtre et les envoie dans Elasticsearch.
- 2- **ELASTIC SEARCH** : stocke et indexe les données. C'est une base No-SQL permettant de gérer un grand nombre de données.
- 3- **KIBANA** : interface Web permettant de rechercher et visualiser graphiquement vos données



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Beats : est un grand projet développé par Elastic.co, la même société qui a développé la pile ELK, et son objectif est d'envoyer des données de centaines ou de milliers de machines et de systèmes à Logstash, Kafka, Redis ou Elasticsearch. La famille Beats a des expéditeurs pour tout type de données, par exemple:

Filebeat - Journaux de fichiers

Metricbeat - Métriques

Auditbeat - Données d'audit

Packetbeat - Données réseau

Heartbeat - Données de disponibilité

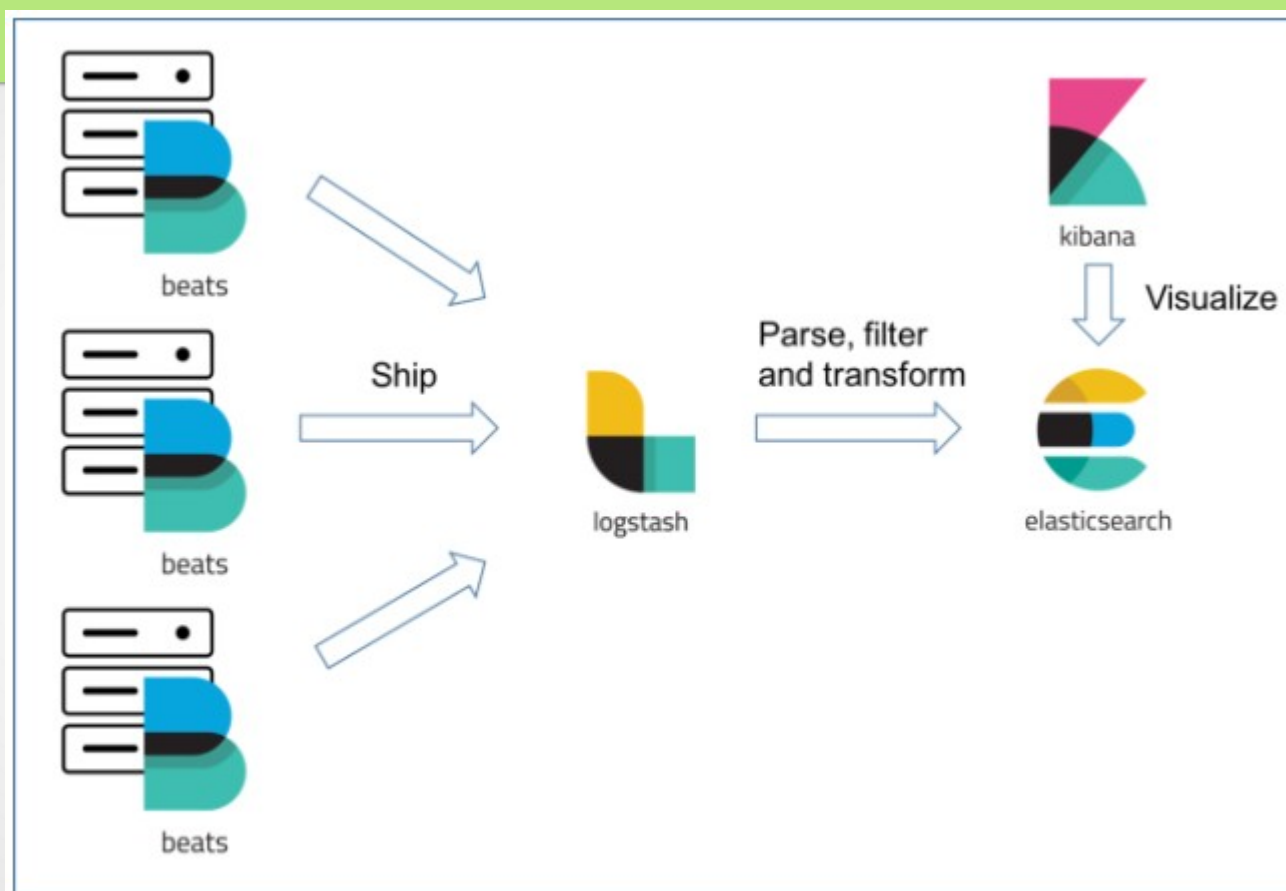
Winlogbeat - Journaux d'événements Windows

FILEBEAT : permet un transfert léger et centralisé des logs et fichiers. Si nous voulons extraire system métrics comme le CPU, memory nous installerons **Metricbeat**



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Filebeat avec ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Architecture

Par défaut, la sortie standard (stdout) de tous les conteneurs Docker est écrite dans des fichiers JSON. Ces fichiers journaux sont stockés sur l'hôte sur lequel s'exécute le moteur Docker et se trouvent sous le chemin suivant `/var/lib/docker/containers/{container-id}/{container-id}-json.log`.

```
ubuntu@vps-c59c6930:~$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                    NAMES
37008a29ae44   myapp          "docker-php-entrypoi..." 3 days ago    Up 3 days    0.0.0.0:8080->80/tcp      myapp_c
b6fe93e878b7   mysql:5.7      "docker-entrypoint.s..." 3 days ago    Up 3 days    3306/tcp, 33060/tcp      mysql_c

ubuntu@vps-c59c6930:~$ sudo ls /var/lib/docker/containers
37008a29ae44cb61c6ee2d9df0497b8d6d2900bb8d93c347cecea7a1f29d9903
b6fe93e878b79fd528a92c8cdc08599ab2bd3d64a6041d910f1bdf904c58050

ubuntu@vps-c59c6930:~$ sudo ls /var/lib/docker/containers/37008a29ae44cb61c6ee2d9df0497b8d6d2900bb8d93c347cecea7a1f29d9903/
37008a29ae44cb61c6ee2d9df0497b8d6d2900bb8d93c347cecea7a1f29d9903-json.log  hostconfig.json  mounts
checkpoints                                                                    hostname         resolv.conf
config.v2.json                                                                hosts            resolv.conf.hash

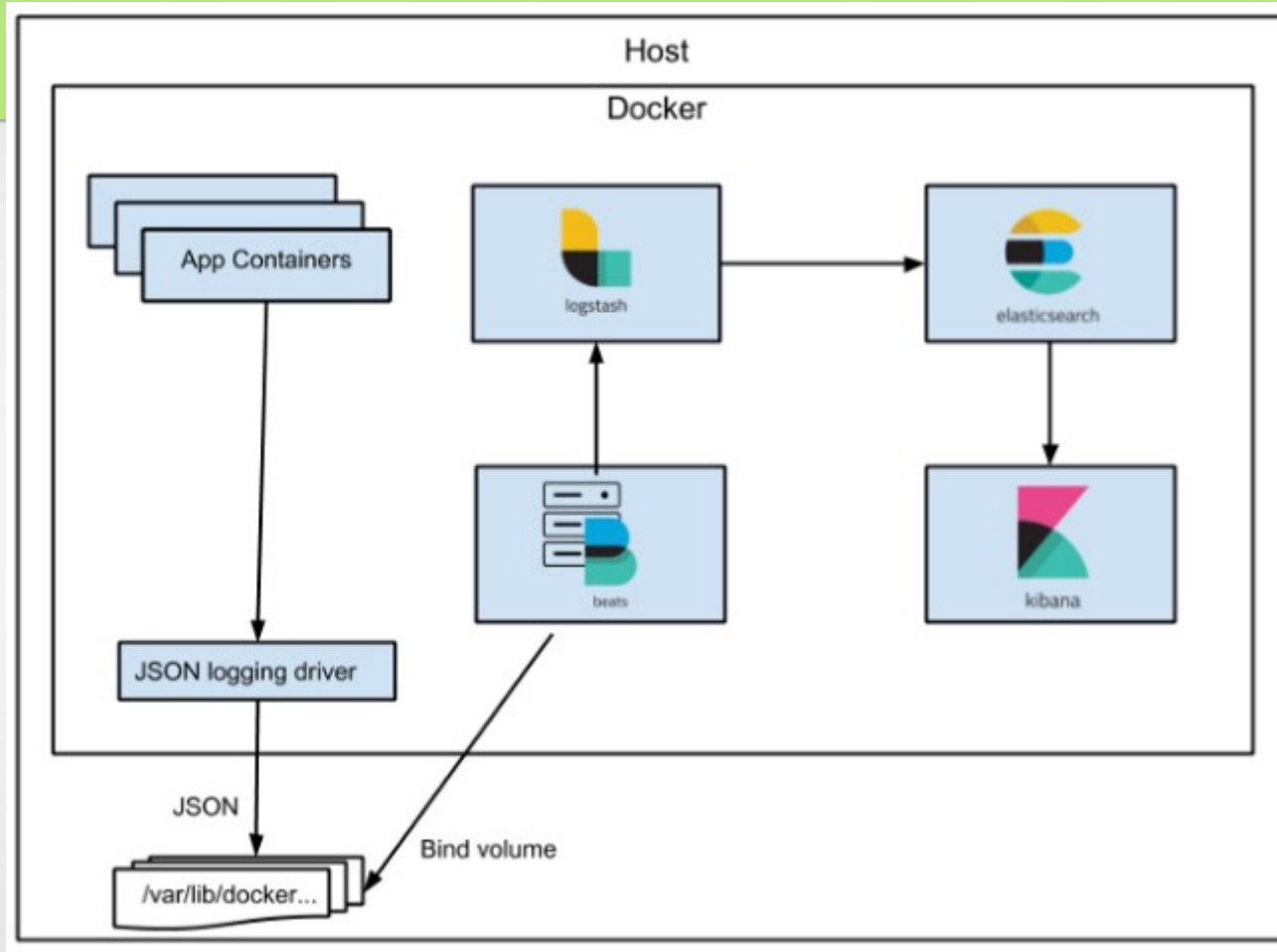
ubuntu@vps-c59c6930:~$
```

Filebeat analysera les fichiers qui correspondent au chemin suivant `/var/lib/docker/containers/*/*-json.log`, transformera les journaux, puis les transmettra à **Logstash**. **Logstash** les filtrera, les transformera et les transmettra finalement à **Elasticsearch**. Une fois les journaux stockés dans **Elasticsearch**, vous pouvez utiliser **Kibana** pour créer des tableaux de bord, rechercher dans les journaux et toutes les autres fonctionnalités prises en charge par **Kibana**.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Exemple1 : installer ELK stack avec docker-compose et dockerfile : Elasticsearch, Logstash, Kibana et Fielbeat

1- Elasticsearch Dockerfile

```
FROM docker.elastic.co/elasticsearch/elasticsearch:6.5.2

COPY --chown=elasticsearch:elasticsearch elasticsearch.yml /usr/share/elasticsearch/config/

CMD ["elasticsearch", "-Elogger.level=INFO"]
```

2- Elasticsearch.yml

```
1 cluster.name: ${cluster.name}
2 network.host: 0.0.0.0
3
4 # minimum_master_nodes need to be explicitly set when bound on a public IP
5 # set to 1 to allow single node clusters
6 # Details: https://github.com/elastic/elasticsearch/pull/17288
7 discovery.zen.minimum_master_nodes: 1
```

3- Logstash Dockerfile

```
FROM docker.elastic.co/logstash/logstash:6.5.2

RUN rm -f /usr/share/logstash/pipeline/logstash.conf

COPY pipeline/ /usr/share/logstash/pipeline/
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

4- Logstash conf

```
input {
  beats {
    port => 5044
    host => "0.0.0.0"
  }
}

output {
  elasticsearch {
    hosts => elasticsearch
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}
```

Le fichier de configuration ci-dessus indique à Logstash d'accepter les journaux d'entrée des beats sur le port 5044 et de les transmettre au cluster Elasticsearch. Les instances Elasticsearch peuvent être trouvées dans un cluster avec des hôtes nommés «elasticsearch». Dans Elasticsearch, les journaux sont stockés dans des index avec le modèle de nom suivant beat- {beat version} - {YYYY.MM.dd}



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

5- Filebeat Dockerfile

```
FROM docker.elastic.co/beats/filebeat:6.5.2

# Copy our custom configuration file
COPY filebeat.yml /usr/share/filebeat/filebeat.yml

USER root

# Create a directory to map volume with all docker log files
RUN mkdir /usr/share/filebeat/dockerlogs

RUN chown -R root /usr/share/filebeat/

RUN chmod -R go-w /usr/share/filebeat/
```

6- Filebeat conf

Le fichier de configuration Filebeat, identique à la configuration Logstash, nécessite une entrée et une sortie. Cette fois, l'entrée est un chemin où les fichiers journaux du docker sont stockés et la sortie est Logstash.

Filebeat est également configuré pour transformer les fichiers de manière à ce que les clés et les clés imbriquées des journaux json soient stockées sous forme de champs dans Elasticsearch. De cette façon, nous pouvons les interroger, créer des tableaux de bord, etc. Une autre chose intéressante que Filebeat peut faire est d'ajouter des métadonnées de docker à chaque journal, ces métadonnées peuvent être: image docker, nom de service de docker compose, identifiant de conteneur et plus encore.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

```
filebeat.inputs:
- type: docker
  combine_partial: true
  containers:
    path: "/usr/share/dockerlogs/data"
    stream: "stdout"
    ids:
      - "*"
  exclude_files: ['.gz$']
  ignore_older: 10m

processors:
  # decode the log field (sub JSON document) if JSON encoded, then maps it's fields to elasticsearch fields
  - decode_json_fields:
      fields: ["log", "message"]
      target: ""
      # overwrite existing target elasticsearch fields while decoding json fields
      overwrite_keys: true
  - add_docker_metadata:
      host: "unix:///var/run/docker.sock"

# setup filebeat to send output to logstash
output.logstash:
  hosts: ["logstash"]
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

7- application test dockerfile

```
1 FROM ubuntu:18.04
2
3 CMD while true; do sleep 2 ; echo "{\"app\": \"dummy\", \"foo\": \"bar\"}"; done
```

Je vais créer un conteneur nommé 'app' est un simple script bash qui imprime le message json {"app": "dummy", "foo": "bar"} toutes les deux secondes. Ce message sera transformé pour que dans Elasticsearch, les clés json «app» et «foo» soient des champs dans l'index et que nous puissions les utiliser.

8- Deploy containers

Git clone <https://gitlab.com/bileli/docker-log-elk.git>

```
ubuntu@vps-c59c6930:~$ ls
projet  projet_dockecompose  projet_dockerfile  projet_dockerfile_volume
ubuntu@vps-c59c6930:~$ git clone https://gitlab.com/bileli/docker-log-elk.git
Cloning into 'docker-log-elk'...
Username for 'https://gitlab.com': bileli
Password for 'https://bileli@gitlab.com':
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 15 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (15/15), 2.62 KiB | 535.00 KiB/s, done.
ubuntu@vps-c59c6930:~$ ls
docker-log-elk  projet_dockecompose  projet_dockerfile_volume
projet          projet_dockerfile
ubuntu@vps-c59c6930:~$ cd docker-log-elk/
ubuntu@vps-c59c6930:~/docker-log-elk$ ls
docker-compose.yml  dummy-app  elasticsearch  filebeat  logstash
ubuntu@vps-c59c6930:~/docker-log-elk$
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Créer et démarrer des conteneurs en utilisant **docker-compose up -d**

Vérification de l'état des conteneurs en utilisant **docker-compose ps** et vous devriez avoir 5 conteneurs

```
ubuntu@vps-c59c6930:~/docker-log-elk$ docker-compose up -d
Creating network "docker-log-elk_default" with the default driver
Creating docker-log-elk_app_1          ... done
Creating docker-log-elk_elasticsearch_1 ... done
Creating docker-log-elk_kibana_1       ... done
Creating docker-log-elk_logstash_1     ... done
Creating docker-log-elk_filebeat_1     ... done
ubuntu@vps-c59c6930:~/docker-log-elk$ docker-compose ps
```

Name	Command	State	Ports
docker-log-elk_app_1	/bin/sh -c while true; do ...	Up	
docker-log-elk_elasticsearch_1	/usr/local/bin/docker-entr ...	Up	0.0.0.0:9200->9200/tcp, 9300/tcp
docker-log-elk_filebeat_1	/usr/local/bin/docker-entr ...	Up	
docker-log-elk_kibana_1	/usr/local/bin/kibana-docker	Up	0.0.0.0:5601->5601/tcp
docker-log-elk_logstash_1	/usr/local/bin/docker-entr ...	Up	0.0.0.0:5044->5044/tcp, 9600/tcp

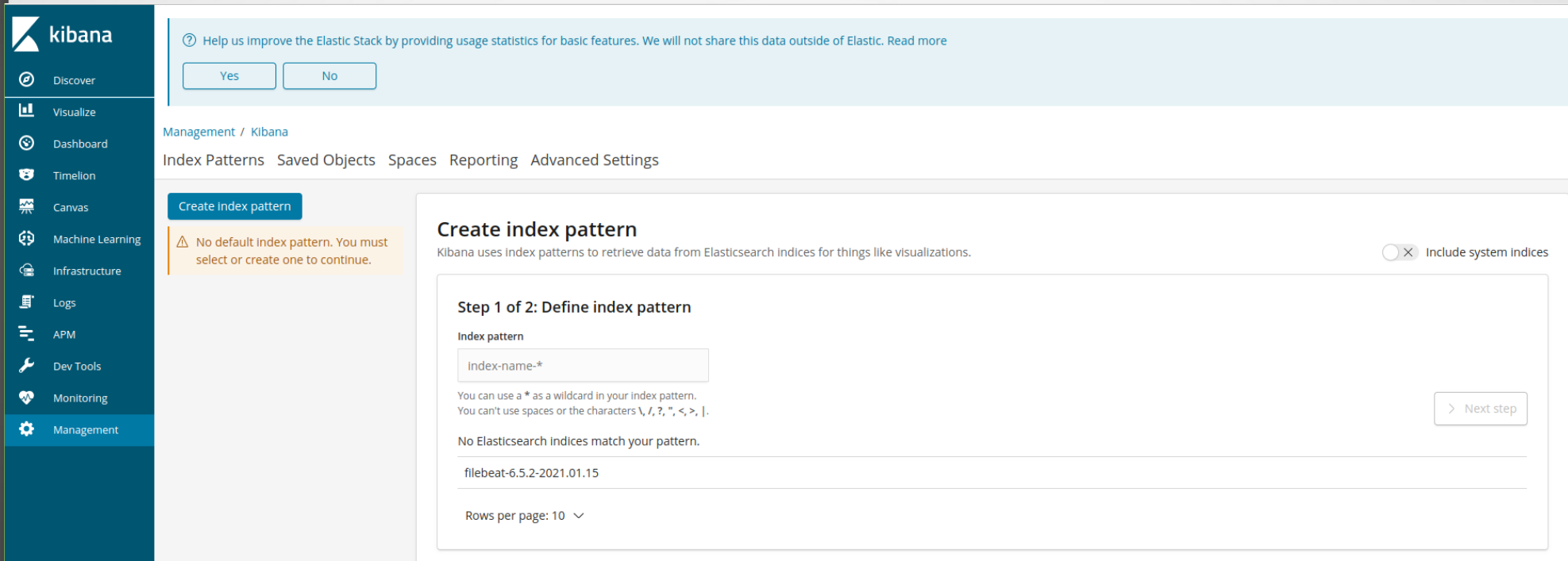
```
ubuntu@vps-c59c6930:~/docker-log-elk$
```

En utilisant Kibana, qui peut être utilisé accédé **http://@ip_serveur:5601** , sous l'onglet Découvrir, écrivez dans la zone de recherche «foo: bar», puis appuyez sur Entrée. Vous devriez voir les messages imprimés à partir du conteneur Docker comme dans l'image ci-dessous.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



The screenshot shows the Kibana Management interface. On the left is a sidebar with the Kibana logo and navigation links: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management (highlighted). The main content area has a top bar with a help message and 'Yes/No' buttons. Below this is a breadcrumb 'Management / Kibana' and a navigation menu with 'Index Patterns', 'Saved Objects', 'Spaces', 'Reporting', and 'Advanced Settings'. The 'Create index pattern' button is highlighted. A warning message states: 'No default index pattern. You must select or create one to continue.' The main section is titled 'Create index pattern' with a sub-header 'Step 1 of 2: Define index pattern'. It includes a text input for 'Index pattern' with the value 'index-name-*'. Below the input, it says: 'You can use a * as a wildcard in your index pattern. You can't use spaces or the characters \, /, ?, *, <, >, |.' A message below the input states: 'No Elasticsearch indices match your pattern.' Below this is a text input with the value 'filebeat-6.5.2-2021.01.15'. At the bottom left, it says 'Rows per page: 10' with a dropdown arrow. At the bottom right, there is a 'Next step' button. A toggle switch for 'Include system indices' is also present.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Create index pattern

Kibana uses Index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 1 of 2: Define index pattern

Index pattern

filebeat*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

> Next step

✓ **Success!** Your index pattern matches **1 index**.

filebeat-6.5.2-2021.01.15

Rows per page: 10 ▾



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 2 of 2: Configure settings

You've defined **filebeat*** as your Index pattern. Now you can specify some settings before we create it.

Time Filter field name

[Refresh](#)

@timestamp

The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

[Show advanced options](#)

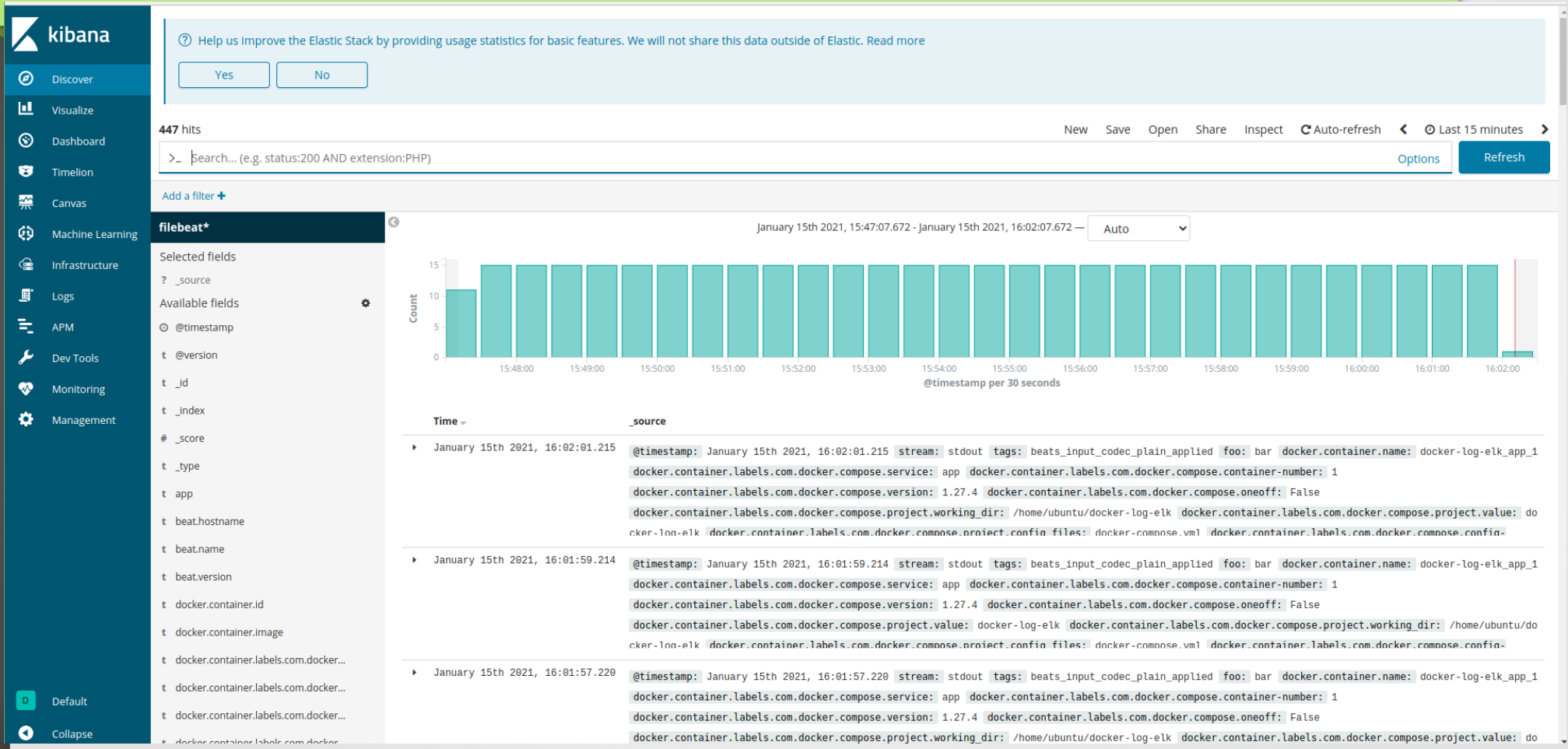
[Back](#)

Create Index pattern



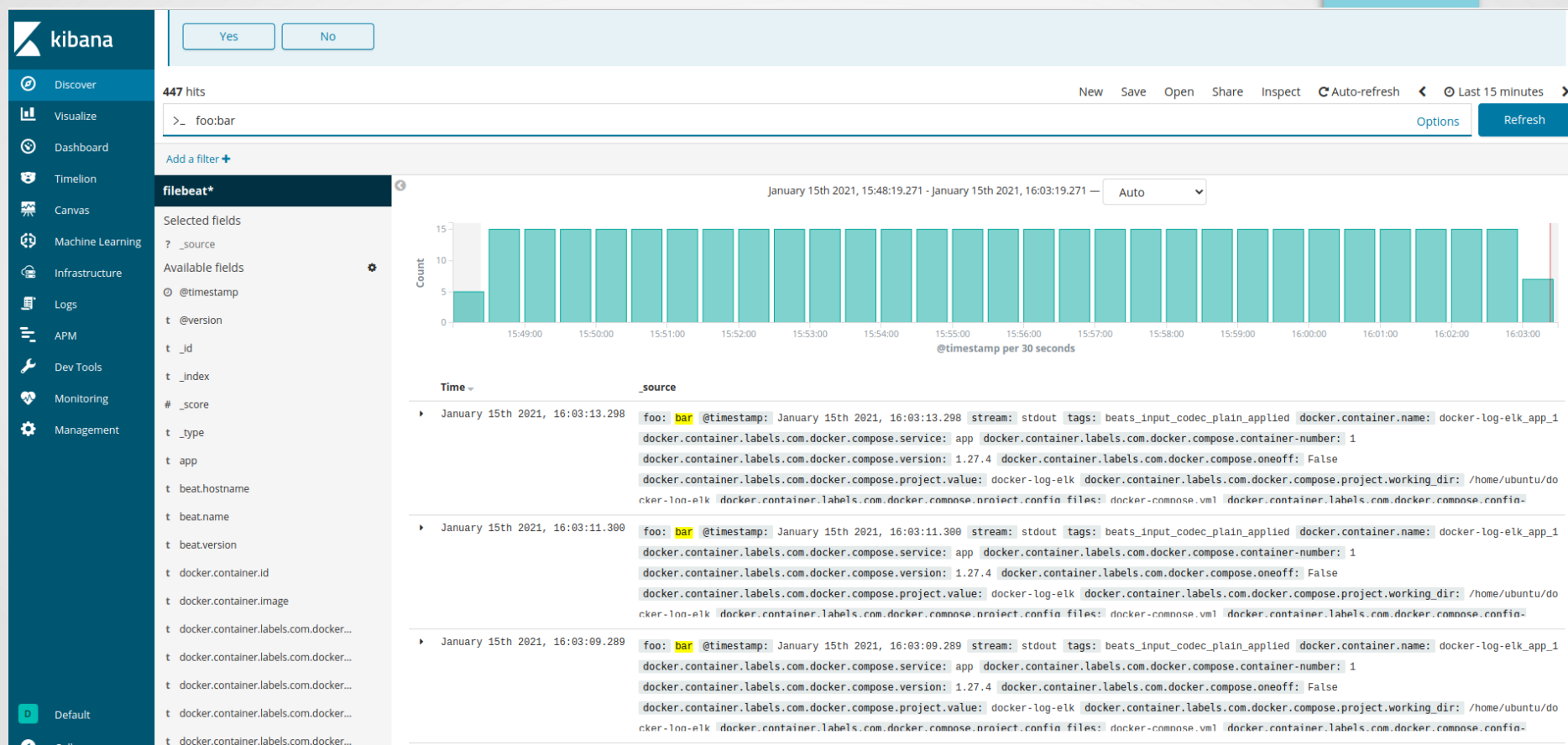
Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Visualisation log du conteneur myapp_c qu'on utilise dans le cours docker-compose

```
ubuntu@vps-c59c6930:~/docker-log-elk$ docker ps
```

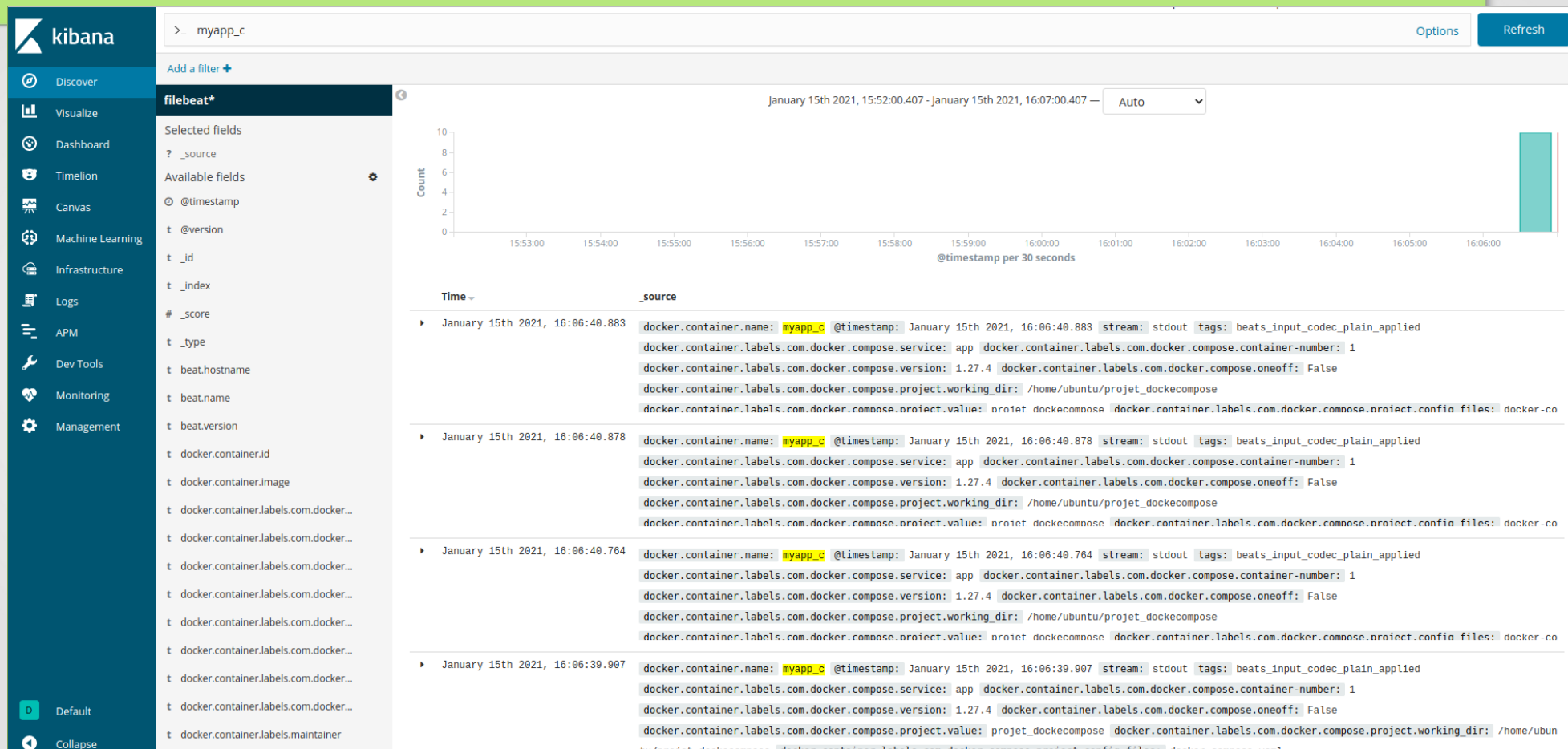
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
78d74dade241	docker-logs-elk/filebeat:1.0.0	"/usr/local/bin/dock..."	30 minutes ago	Up 30 minutes		docker-log-elk
ilebeat_1						
4cd8a34be5f6	docker-logs-elk/logstash:1.0.0	"/usr/local/bin/dock..."	30 minutes ago	Up 30 minutes	0.0.0.0:5044->5044/tcp, 9600/tcp	docker-log-elk
ogstash_1						
6a5021721ddb	kibana:6.5.2	"/usr/local/bin/kiba..."	30 minutes ago	Up 30 minutes	0.0.0.0:5601->5601/tcp	docker-log-elk
ibana_1						
41d7f47073c7	docker-logs-elk/elasticsearch:1.0.0	"/usr/local/bin/dock..."	30 minutes ago	Up 30 minutes	0.0.0.0:9200->9200/tcp, 9300/tcp	docker-log-elk
lasticsearch_1						
0861971f9b91	docker-logs-elk/dummy-app:1.0.0	"/bin/sh -c 'while t..."	30 minutes ago	Up 30 minutes		docker-log-elk
pp_1						
37008a29ae44	myapp	"docker-php-entrypoi..."	5 days ago	Up 29 hours	0.0.0.0:8080->80/tcp	myapp_c
b6fe93e878b7	mysql:5.7	"docker-entrypoint.s..."	5 days ago	Up 29 hours	3306/tcp, 33060/tcp	mysql_c

```
ubuntu@vps-c59c6930:~/docker-log-elk$
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Ressources:

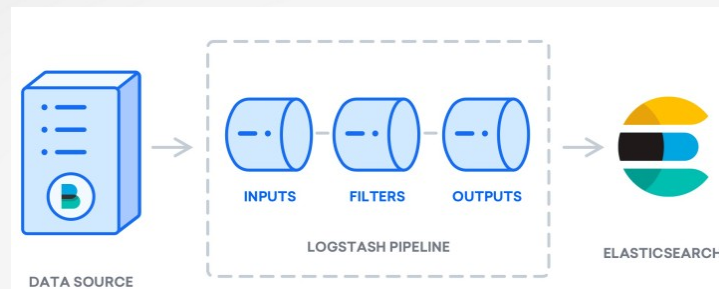
- 1- <https://docs.docker.com/>
- 2- <https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html>
- 3- <https://www.elastic.co/guide/en/beats/filebeat/current/index.html>
- 4- <https://www.elastic.co/guide/en/kibana/current/index.html>
- 5- <https://www.elastic.co/guide/en/logstash/current/index.html>
- 6- <https://docs.docker.com/compose/>



ELK

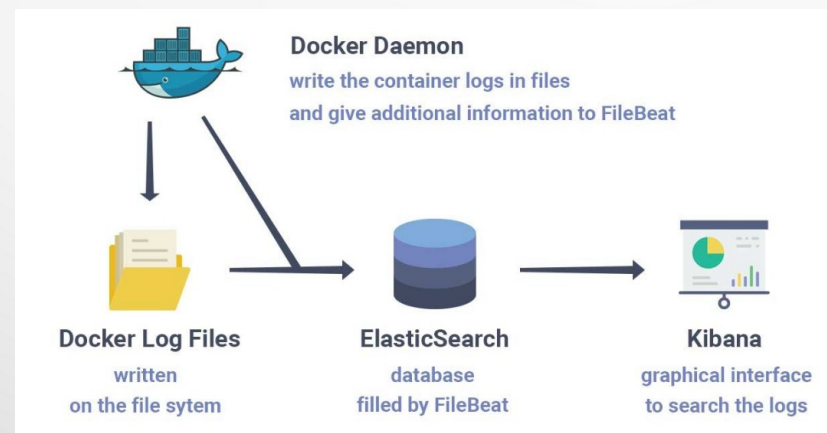
Exemple2 : Envoi de journaux Docker à ElasticSearch et Kibana avec Logstash sans filebeat

<https://gitlab.com/bileli/elk.git>



Exemple3 : Envoi de journaux Docker à ElasticSearch et Kibana avec filebeat sans Logstash

<https://www.sarulabs.com/post/5/2019-08-12/sending-docker-logs-to-%20elasticsearch-and-kibana-with-filebeat.html>



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Utilisation de la stack ELK (installation from scratch) sur les logs Apache from scratch

Chap1 : Dans ce chapitre, nous allons procéder à l'installation et la configuration des différents composants de la suite ELK.

La stack ELK peut être installée à l'aide d'une variété de méthodes et sur un large éventail de systèmes d'exploitation et d'environnements différents. Vous pouvez installer ELK localement, sur le cloud, à l'aide de Docker et de systèmes de gestion de configuration comme Ansible, Puppet et Chef. La pile peut être également installée à l'aide de votre gestionnaire de paquets ou manuellement depuis les binaires officiels. Voici le lien pour la page officielle des multiples méthodes d'installation d'ELK. <https://www.elastic.co/guide/en/elasticsearch/reference/7.8/install-elasticsearch.html>

De nombreuses étapes d'installation sont similaires d'un environnement à l'autre et comme nous ne pouvons pas couvrir tous les différents scénarios, je vais vous fournir un exemple d'installation de tous les composants de la pile Elasticsearch, Logstash, Kibana sous une seule machine Linux à l'aide du gestionnaire de paquets APT

Note : Lors de l'installation d'ELK, vous devez utiliser la même version sur l'ensemble de la pile. Par exemple, si vous utilisez Elasticsearch 7.10.2 alors Kibana doit être aussi sous sa version 7.10.2 et même pour Logstash en version 7.10.2.

1- Elasticsearch

1.1:installation

Tout d'abord, vous devez ajouter la clé de signature d'Elastic pour que le package téléchargé puisse être vérifié

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  
sudo apt-get install apt-transport-https
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

L'étape suivante consiste à ajouter le dépôt Elasticsearch sur votre système :

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list  
sudo apt-get update -y && sudo apt-get install elasticsearch
```

1.2-Configuration

Par défaut à son lancement Elasticsearch consomme 1go de mémoire de la JVM (machine virtuelle java), si votre machine n'est pas assez puissante vous pouvez modifier les valeurs Xms et Xmx situé dans le fichier **/etc/elasticsearch/jvm.options** pour une consommation réduite:

```
# Avant (1go)  
-Xms1g  
-Xmx1g  
# Après (512 mo)  
-Xms512mo  
-Xmx512mo
```

Les configurations Elasticsearch sont effectuées à l'aide du fichier de configuration **/etc/elasticsearch/elasticsearch.yml** qui vous permet de configurer les paramètres généraux comme par exemple le nom du nœud, ainsi que les paramètres réseau comme par exemple l'hôte et le port, l'emplacement des données stockées, la mémoire, les fichiers de logs, etc... Pour ce cours nous laisserons la configuration par défaut.

1.3-Lancement et test

Pour exécuter Elasticsearch, utilisez la commande suivante (l'initialisation peut prendre un peu de temps) :

```
sudo systemctl start elasticsearch
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Si jamais vous rencontrez des problèmes d'initialisation, veuillez vérifier les logs du service elasticsearch à l'aide de la commande suivante :

```
sudo journalctl -f -u elasticsearch
```

Pour confirmer que tout fonctionne comme prévu, pointez votre commande curl ou votre navigateur sur l'adresse <http://localhost:9200>, et vous devriez voir quelque chose comme la sortie suivante :

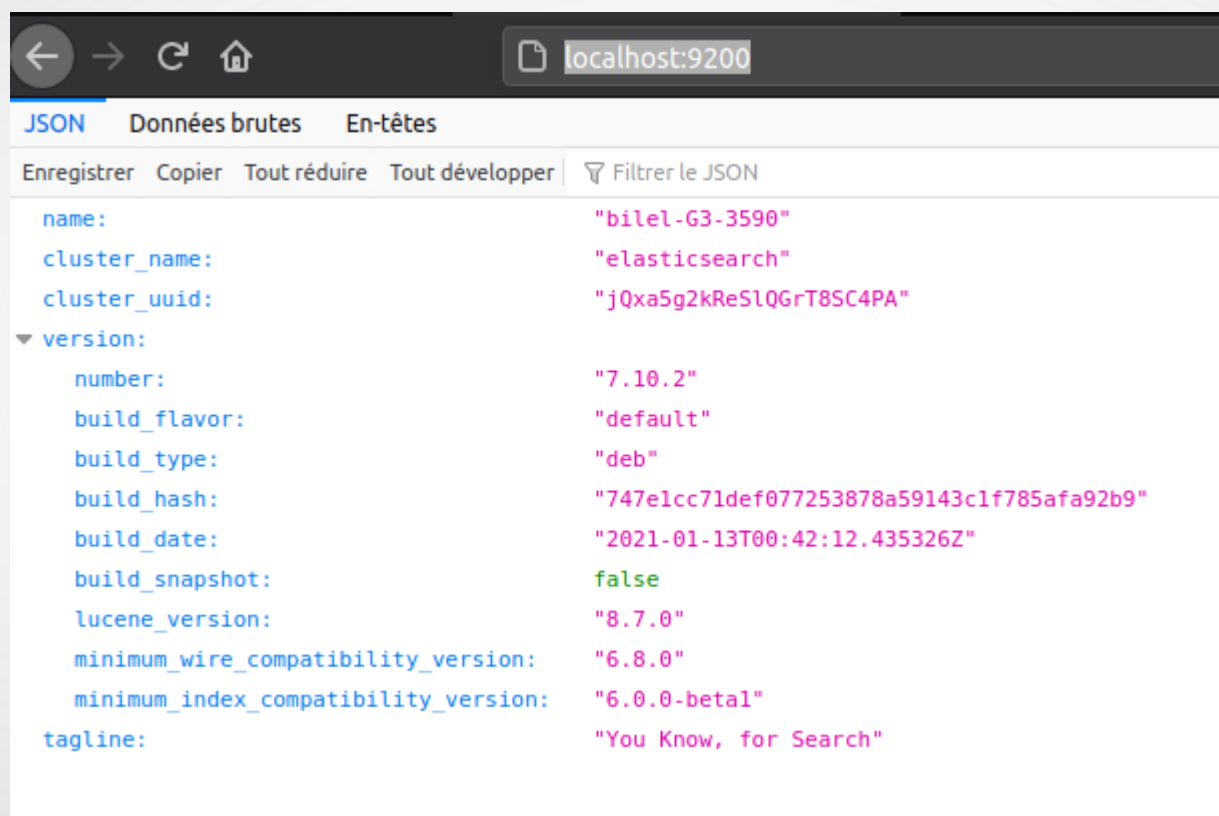
```
curl localhost:9200
```

```
bilel@bilel-G3-3590:~$ sudo systemctl start elasticsearch
bilel@bilel-G3-3590:~$ curl localhost:9200
{
  "name" : "bilel-G3-3590",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "jQxa5g2kReSlQGrT8SC4PA",
  "version" : {
    "number" : "7.10.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "747e1cc71def077253878a59143c1f785afa92b9",
    "build_date" : "2021-01-13T00:42:12.435326Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
bilel@bilel-G3-3590:~$
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



```
{
  "name": "bilel-G3-3590",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "jQxa5g2kReSlQGrT8SC4PA",
  "version": {
    "number": "7.10.2",
    "build_flavor": "default",
    "build_type": "deb",
    "build_hash": "747e1cc71def077253878a59143c1f785afa92b9",
    "build_date": "2021-01-13T00:42:12.435326Z",
    "build_snapshot": false,
    "lucene_version": "8.7.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour initialiser le service à chaque démarrage de la machine, lancez la commande suivante :

```
sudo systemctl enable elasticsearch
```

2- Kibana

1.1: installation

Puisque nous avons déjà défini le dépôt dans le système, tout ce que nous avons à faire pour installer kibana est d'exécuter la commande suivante:

```
sudo apt-get install kibana
```

2.2- Configuration

Le fichier de configuration de kibana se retrouve dans **/etc/kibana/kibana.yml** . Si jamais vous avez modifié avec ce fichier, assurez-vous juste que la configuration kibana possède les bonnes informations pour communiquer avec Elasticsearch :

```
elasticsearch.hosts: ["http://localhost:9200"]
```

2.3- Lancement et test

Voici la commande pour démarrer Kibana :

```
sudo systemctl start kibana
```

Si jamais vous rencontrez des problèmes d'initialisation, veuillez vérifier les logs du service kibana comme suit :

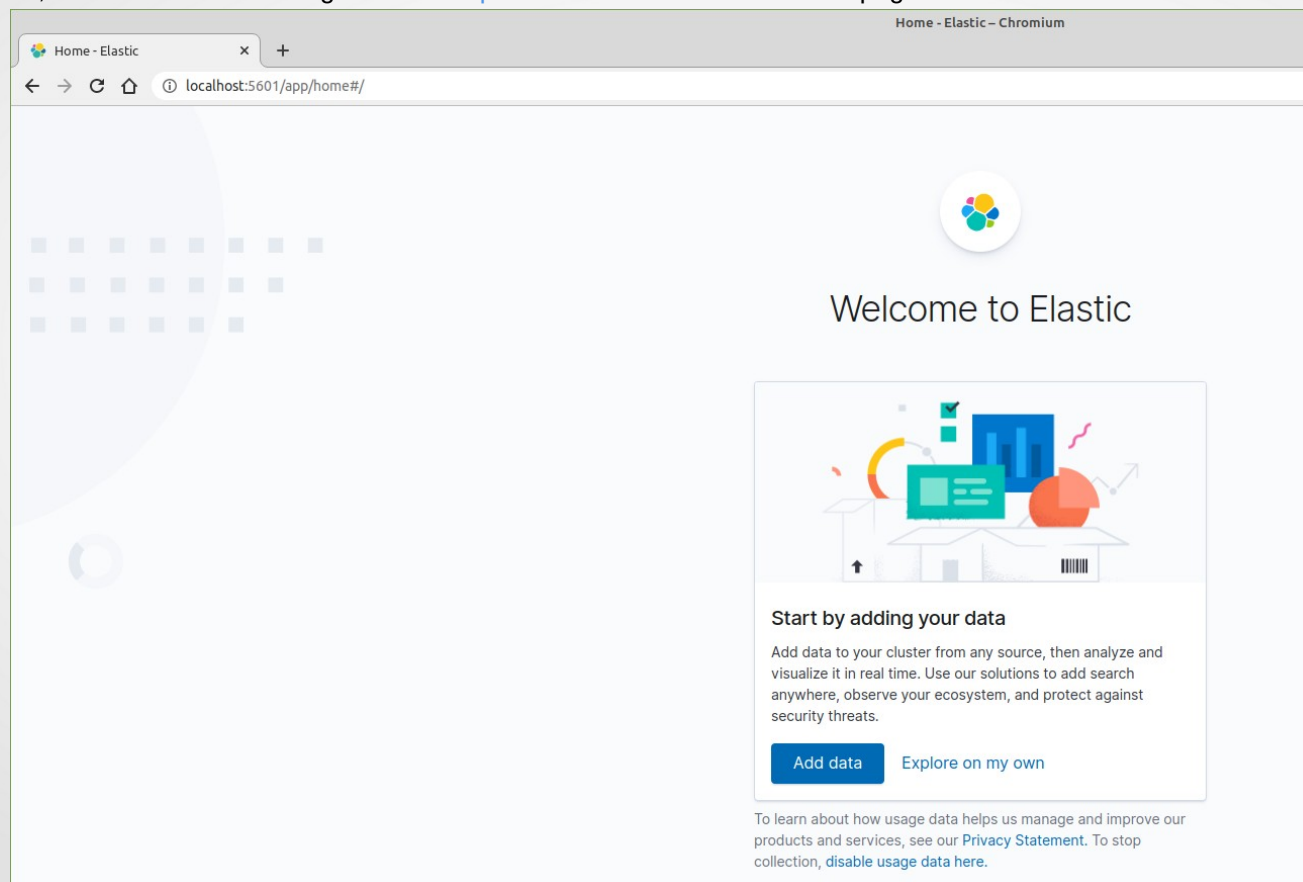
```
sudo journalctl -f -u kibana
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour tester Kibana, ouvrez dans votre navigateur l'url <http://localhost:5601> afin de voir la page d'accueil Kibana :



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour initialiser le service Kibana à chaque démarrage de la machine, lancez la commande suivante :

```
sudo systemctl enable kibana
```

3- Logstash

3.1: installation

Logstash nécessite au minimum la version 8 de java pour fonctionner, nous allons donc commencer le processus de configuration de Logstash avec:

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

vérifiez que java est installé:

```
bilel@bilel-G3-3590:~$ java --version
openjdk 11.0.9.1 2020-11-04
OpenJDK Runtime Environment (build 11.0.9.1+1-Ubuntu-0ubuntu1.20.04)
OpenJDK 64-Bit Server VM (build 11.0.9.1+1-Ubuntu-0ubuntu1.20.04, mixed mode, sharing)
bilel@bilel-G3-3590:~$
```

Comme pour kibana, puisque nous avons déjà défini le dépôt dans le système, tout ce que nous avons à faire pour installer Logstash est d'exécuter:

```
sudo apt-get install logstash
```

3.2-Configuration

Le fichier de configuration de Logstash est le suivant : **/etc/logstash/logstash.yml** et permet de configurer des paramètres généraux comme par exemple le nom du nœud, le port, le niveau des logs etc... Pour ce cours nous laisserons la configuration par défaut.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

3.3-Lancement et test

Voici la commande pour démarrer logstash :

```
sudo systemctl start logstash
```

Si jamais vous rencontrez des problèmes d'initialisation, vérifiez les logs du service Logstash comme suit :

```
sudo journalctl -f -u logstash
```

Pour initialiser le service à chaque démarrage de la machine, lancez la commande suivante :

```
sudo systemctl enable logstash
```

Pour tester votre installation Logstash, vous devez configurer un pipeline de données. Nous aborderons cette partie dans le prochain chapitre.

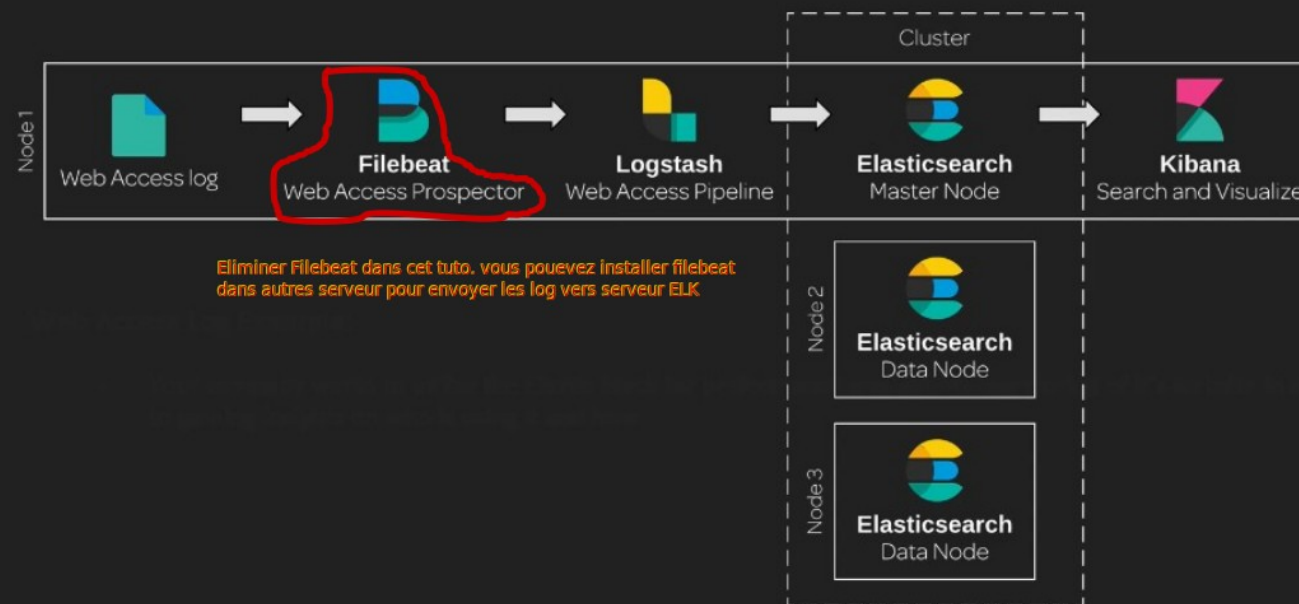


ELK

Chap2 : Dans ce chapitre, nous allons apprendre à utiliser la stack ELK en analysant en temps réel les logs d'accès Apache.

Après avoir installé la suite ELK dans la chapitre précédent. Nous allons dans cet chap pratiquer et s'initier à l'utilisation des différents composants de la stack ELK en analysant en temps réel les logs d'accès Apache.

Web Access Log Aggregation Example



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour bien suivre cet tuto, vous devez au préalable installer et démarrer le package d'Apache sur votre machine ELK. Pour cela, lancez les commandes suivantes :

```
sudo apt-get install -y apache2
```

Utilisez l'outil systemctl pour démarrer le service Apache :

```
sudo systemctl start apache2
```

Enfin, très important, n'oubliez pas de rajouter l'utilisateur logstash au groupe adm :

```
sudo usermod -aG adm logstash
```

Logstash

La première étape à effectuer est le traitement des logs sous forme d'un ou plusieurs pipelines avec l'outil Logstash.

Comment fonctionne de Logstash ? Il est capable d'extraire des données de presque n'importe quelle source de données à l'aide des plugins d'entrée, et d'appliquer une grande variété de transformations et d'améliorations de données à l'aide de plugins de filtre et enfin d'expédier ces données vers un grand nombre de destinations à l'aide de plugins de sortie. Vous comprendrez alors que Logstash joue un rôle très important dans la pile en récupérant, filtrant et expédiant vos données afin de les utiliser plus facilement sur le reste des composants.

Pour utiliser Logstash, il faut créer des fichiers de configuration qui contiendront trois sections principales que nous allons par passer en revue ci-dessous. À savoir que chacune de ces sections est responsable de différentes fonctions et utilisant différents plugins Logstash.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Commencez déjà par créer un fichier **apache.conf** dans le dossier de configuration Logstash situé dans **/etc/logstash/conf.d/** et rajoutez-y les trois sections de configuration principales qui seront pour le moment vide :

```
input {}  
filter {}  
output {}
```

- **Entrées Logstash** : Les points de départ de toute configuration Logstash sont vos entrées. Les entrées sont des plugins Logstash responsables de la récupération des données de différentes sources de données. Vous trouverez l'intégralité des plugins d'entrée dans le site officiel <https://www.elastic.co/guide/en/logstash/current/input-plugins.html>. Pour notre exemple, nous avons besoin de récupérer les données depuis un fichier donc nous utiliserons le plugin d'entrée file , comme suit :

```
input {  
  file { path => "/var/log/apache2/access.log" }  
}  
...
```

En regardant la documentation du [plugin d'entrée file](#) , vous remarquerez que vous pouvez utiliser différents paramètres pour cette entrée. Comme par exemple, le paramètre **start_position** qui permet de choisir où Logstash doit commencer sa lecture initiale des fichiers, soit au début ou à la fin. La valeur par défaut est **end** qui traite les fichiers comme des flux direct en temps réel (comme la commande **tail -f**) et comme son nom l'indique, la lecture débutera à partir de la fin du fichier, mais si vous souhaitez lire un fichier depuis le début, forcez alors la valeur à **beginning** :

```
input {  
  file {  
    path => "/var/log/apache2/access.log"  
    start_position => "beginning"  
    sincedb_path => "/dev/null"  
  }  
}  
...
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Par défaut, logstash écrit la dernière position de lecture dans un fichier log qui réside généralement dans **\$HOME/.sincedb** ou dans le dossier **/var/lib/logstash/plugins/inputs/file/**. Afin de forcer la relecture complète d'un fichier à chaque exécution de **logstash**, il faut changer le chemin du fichier de logs de position en valorisant **sincedb_path** à **/dev/null**. Ou sinon vous pouvez supprimer uniquement la ligne correspondante de votre fichier .sincedb et redémarrez le service logstash.

- **Filtres Logstash** : Les filtres sont des modules qui vont traiter les données récupérées depuis l'input en s'aidant lui aussi de différents plugins de filtrage (<https://www.elastic.co/guide/en/logstash/current/filter-plugins.html>). Pour notre exemple, nous utiliserons le plugin **grok** (<https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html>) qui vous permet d'analyser facilement des données de logs non structurées en quelque chose de plus exploitable en utilisant des expressions régulières. Cet outil est parfait pour tout format de logs généralement écrit pour les humains comme les logs applicatifs (ex: mysql, apache, nginx, etc ...).

La syntaxe d'un pattern grok est la suivante : **%{SYNTAX:SEMANTIC}**

- **SYNTAX** : nom du pattern qui correspond à un filtre prédéfini, comme par exemple le pattern **NUMBER** qui prend en compte des nombres tel quel 3 ou 3.55 ou le pattern **IP** qui correspond à une IP comme 192.168.1.20.

- **SEMANTIC** : est l'identifiant de la valeur récupérée par votre SYNTAX.

Par exemple pour traiter la ligne de log suivante : **55.3.244.1 GET /index.html 15824 0.043** Le pattern grok sera le suivant :

```
filter {
  grok {
    match => { "message" => "%{IP:client} %{WORD:method} %{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}" }
  }
}
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Après traitement du filtre grok, nous obtiendrons les champs suivants :

```
client: 55.3.244.1
method: GET
request: /index.html
bytes: 15824
duration: 0.043
```

Pour notre besoin, nous allons plutôt découvrir et utiliser des patterns **APACHE grok** pré-configurés. Vous pouvez utiliser soit le pattern **COMMONAPACHELOG** qui récupère des informations de base (IP source, code HTTP, etc ...) ou le pattern **COMBINEDAPACHELOG** qui récupère des informations supplémentaires comme le user-agent.

Pour tester vos patterns, vous pouvez soit utiliser un plugin de sortie que nous verrons dans la section suivante, ou bien utilisez un débogueur grok en ligne, comme [grokdebug](#). Pour utiliser l'exactitude d'exécution de votre pattern sur votre débogueur, vous n'avez qu'à copier quelques lignes de vos logs apaches :

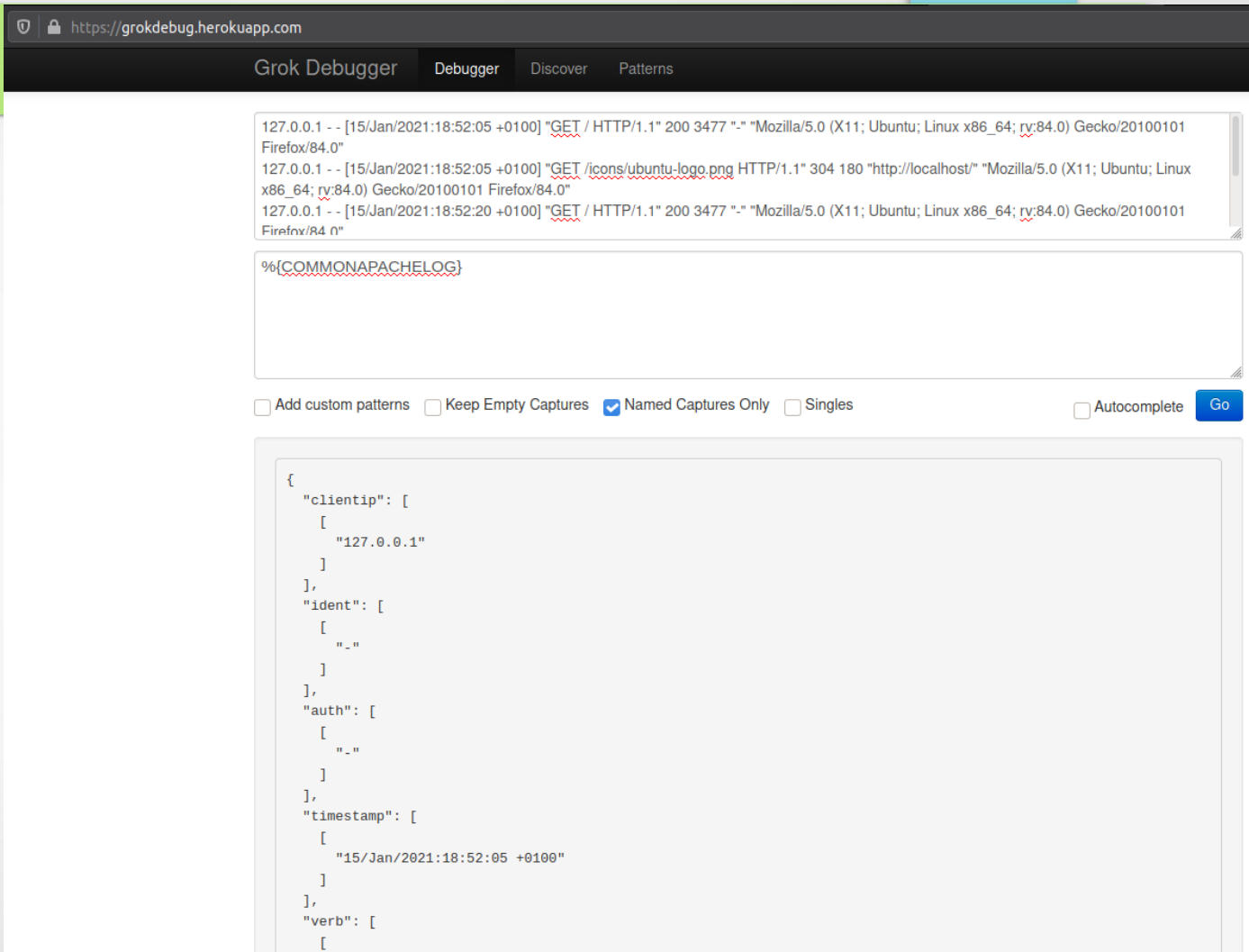
```
bilel@bilel-G3-3590:~$ tail -f /var/log/apache2/access.log
127.0.0.1 - - [15/Jan/2021:18:50:53 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:50:53 +0100] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:50:53 +0100] "GET /favicon.ico HTTP/1.1" 404 487 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:51:50 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:51:50 +0100] "GET /icons/ubuntu-logo.png HTTP/1.1" 304 180 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:05 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:05 +0100] "GET /icons/ubuntu-logo.png HTTP/1.1" 304 180 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:20 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:20 +0100] "GET /icons/ubuntu-logo.png HTTP/1.1" 304 180 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Une fois vos lignes de logs copiées,
collez les dans votre débogueur avec votre
pattern du plugin grok, exemple :



The screenshot shows the Grok Debugger interface at <https://grokdebug.herokuapp.com>. The interface has a dark theme with a top navigation bar containing "Grok Debugger", "Debugger", "Discover", and "Patterns".

The main area displays three log lines from a web server:

```
127.0.0.1 - - [15/Jan/2021:18:52:05 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:05 +0100] "GET /icons/ubuntu-logo.png HTTP/1.1" 304 180 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
127.0.0.1 - - [15/Jan/2021:18:52:20 +0100] "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0"
```

Below the logs, a Grok pattern is entered in a text box:

```
%{COMMONAPACHELOG}
```

At the bottom, there are checkboxes for "Add custom patterns", "Keep Empty Captures", "Named Captures Only" (which is checked), and "Singles". There is also an "Autocomplete" checkbox and a "Go" button.

The bottom section shows the resulting JSON output of the Grok pattern:

```
{
  "clientip": [
    [
      "127.0.0.1"
    ]
  ],
  "ident": [
    [
      "-"
    ]
  ],
  "auth": [
    [
      "-"
    ]
  ],
  "timestamp": [
    [
      "15/Jan/2021:18:52:05 +0100"
    ]
  ],
  "verb": [
    [
      "GET"
    ]
  ]
}
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Cool notre pattern grok fonctionne! Revenons alors maintenant sur notre fichier apache.conf et complétons la section filtre, comme suit :

```
input {
  file { path => "/var/log/apache2/access.log" }
}
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
  mutate {
    convert => {
      "response" => "integer"
      "bytes" => "integer"
    }
  }
}
```

J'ai fait exprès de rajouter deux nouveaux filtre [date](#) et [mutate](#), car ils nous serviront plus tard pour nos visualisations sur Kibana :

Par défaut, logstash basera son horodatage sur l'heure à laquelle l'entrée du fichier de log a été lue et non sur l'horodatage fourni par le fichier de logs Apache. D'où l'utilisation du filtre de date qui basera son horodatage sur les dates des champs filtrés par grok, soit l'horodatage réel fourni par le fichier de log Apache.

J'utilise également le filtre mutate avec l'action convert afin de convertir la réponse HTTP et la taille de la requête qui sont par défaut en type string vers le type entier, car en effet, Kibana gère ses visualisations différemment selon le type de données que vous lui envoyez.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Sorties Logstash : Les points d'arrivée de toute configuration Logstash sont vos sorties, lui-même utilise différents plugins de sortie (<https://www.elastic.co/guide/en/logstash/current/output-plugins.html>) qui envoient les données traitées par la phase de filtrage à une destination particulière (ex: elasticsearch). Par ailleurs, les sorties sont la dernière étape du pipeline Logstash.

Pour cet article, je vais vous dévoiler comment récupérer les événements sur la sortie standard avec le plugin de sortie **stdout** (<https://www.elastic.co/guide/en/logstash/current/plugins-outputs-stdout.html>) avant de les envoyer plus tard à **elasticsearch**. Le plugin **stdout** propose différents formats de sortie, dans notre exemple nous utiliserons le format **rubydebug**, comme ceci :

```
input {
  file { path => "/var/log/apache2/access.log" }
}
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
  mutate {
    convert => {
      "response" => "integer"
      "bytes" => "integer"
    }
  }
}
output {
  stdout { codec => rubydebug }
}
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Debug : Dans cette partie je souhaite vous montrer comment vous pouvez debug votre pipeline Logstash afin d'utiliser du mieux ce plugin, pour cela il faut commencer par stopper le service logstash : `sudo systemctl stop logstash`

Ensuite, nous allons vérifier la syntaxe de notre code **Logstash** avec le binaire **logstash** situé dans **/usr/share/logstash/bin/logstash** en utilisant l'option **-t**

```
sudo /usr/share/logstash/bin/logstash --path.settings /etc/logstash -f /etc/logstash/conf.d/apache.conf -t
```

Résultat :

```
Configuration OK
[2021-01-15T18:59:40,886][INFO ][logstash.runner           ] Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
bilel@bilel-G3-3590:~$
```

Les différents options du binaire logstash sont disponibles [ici](https://www.elastic.co/guide/en/logstash/current/running-logstash-command-line.html). <https://www.elastic.co/guide/en/logstash/current/running-logstash-command-line.html>

Une fois la syntaxe validée, relancez la commande sans l'option **-t** mais avec l'option **--debug**

```
sudo /usr/share/logstash/bin/logstash -debug --path.settings /etc/logstash -f /etc/logstash/conf.d/apache.conf
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Visitez ensuite depuis votre navigateur la page d'accueil <http://localhost/> et revenez sur la sortie standard de votre logstash pour observer le résultat suivant :

```
[2021-01-15T19:03:35,007][DEBUG][logstash.filters.grok][main][7b20cb5be07f2a5a2c3b62f5efc78d54dbf9e1cf8b89dbc13df4f30b928e1223] Event now: {:event=>#<LogStash::Event:0x50ffc76c>}
{
  "message" => "127.0.0.1 - - [15/Jan/2021:19:03:34 +0100] \"GET /icons/ubuntu-logo.png HTTP/1.1\" 304 180 \"http://localhost/\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0\"",
  "@timestamp" => 2021-01-15T18:03:34.000Z,
  "clientip" => "127.0.0.1",
  "host" => "bilel-63-3590",
  "agent" => "\"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0\"",
  "ident" => "-",
  "httpversion" => "1.1",
  "verb" => "GET",
  "@version" => "1",
  "response" => 304,
  "timestamp" => "15/Jan/2021:19:03:34 +0100",
  "auth" => "-",
  "bytes" => 180,
  "request" => "/icons/ubuntu-logo.png",
  "referrer" => "\"http://localhost/\"",
  "path" => "/var/log/apache2/access.log"
}
[2021-01-15T19:03:37,469][DEBUG][org.logstash.execution.PeriodicFlush][main] Pushing flush onto pipeline.
[2021-01-15T19:03:39,451][DEBUG][logstash.instrument.periodicpoller.jvm] collector name {:name=>"ParNew"}
[2021-01-15T19:03:39,456][DEBUG][logstash.instrument.periodicpoller.jvm] collector name {:name=>"ConcurrentMarkSweep"}
[2021-01-15T19:03:42,469][DEBUG][org.logstash.execution.PeriodicFlush][main] Pushing flush onto pipeline.
```

Passons maintenant à la communication avec elasticsearch.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

ElasticSearch : Modifions ensuite notre fichier apache.conf pour communiquer avec elasticsearch :

```
input {
  file { path => "/var/log/apache2/access.log" }
}
filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }

  date {
    match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
  }

  mutate {
    convert => {
      "response" => "integer"
      "bytes" => "integer"
    }
  }
}
output {
  elasticsearch {
    hosts => "localhost:9200"
    index => "apache-%{+YYYY.MM.dd}"
  }
}
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Vous remarquerez que j'utilise un index dans le bloc de code de sortie elasticsearch car c'est le moyen pour **elasticsearch** de structurer ses données et de les gérer plus rapidement. Le nommage utilisé dans notre index actuel est dynamique grâce au pattern `%{+YYYY.MM.dd}`, ce qui aura pour effet de créer un index par jour, permettant à l'administrateur de facilement s'y retrouver en affichant par exemple que les logs d'une date précise dans Kibana, supprimer que les indexs d'une plage de dates , etc ...

N'oubliez pas de démarrer votre service logstash avec la commande suivante :

```
sudo systemctl start logstash
```

Après démarrage de votre service, logstash va lancer votre pipeline. Ensuite vous pouvez vérifier si l'index s'est correctement créé, pour cela appelez l'API REST fournie par elasticsearch, comme suit :

```
curl "localhost:9200/_cat/indices?v"
```

```
bilel@bilel-G3-3590:~$ curl "localhost:9200/_cat/indices?v"
health status index      uuid                                pri rep docs.count docs.deleted store.size pri.store.size
yellow open   apache-2021.01.15 HHm0RMiGQuqv6_TlITj9tA             1   1      12             0    99.9kb         99.9kb
```



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

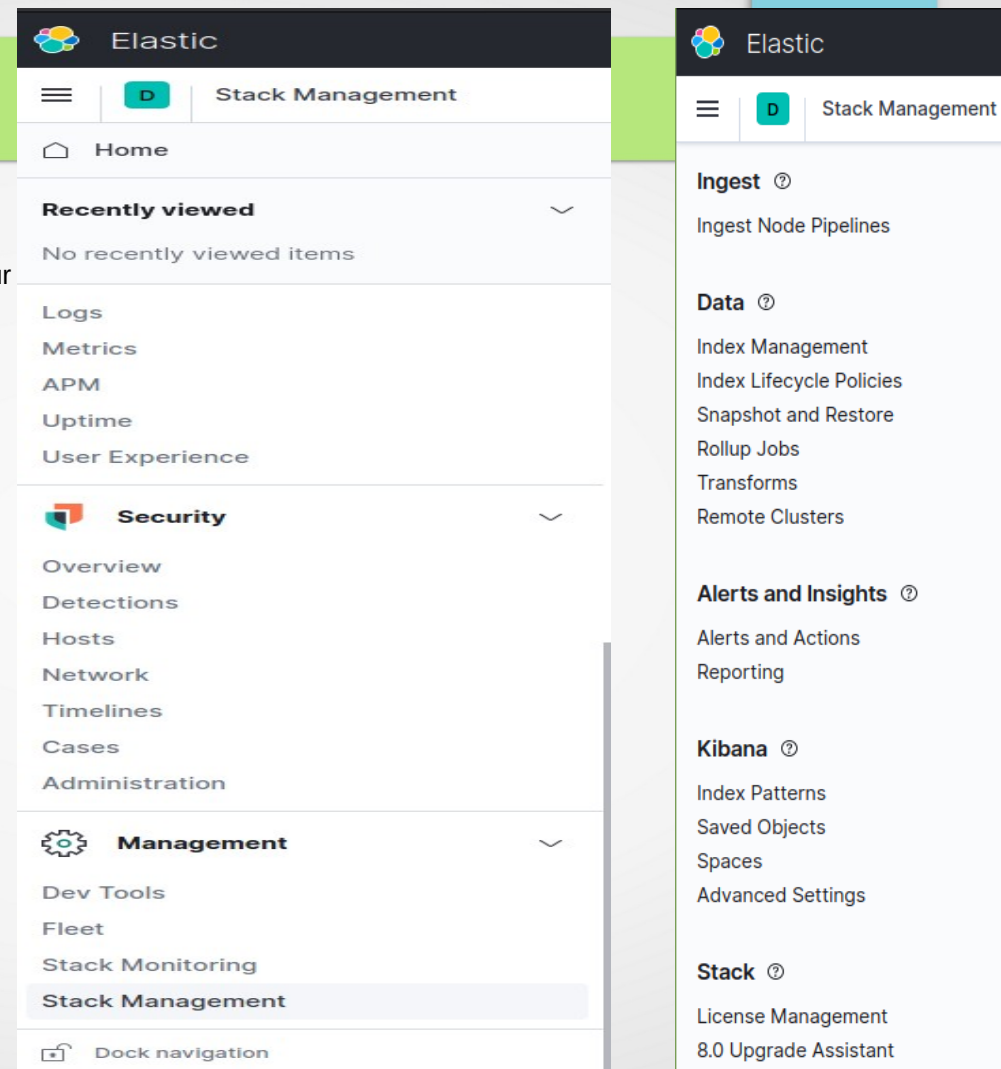
ELK

- Kibana

1- Index Patterns

Rendez-vous ensuite sur Kibana depuis l'url <http://localhost:5601/>. Pour visualiser notre index, allez sur le menu à gauche et cliquez sur "Stack Management" :

Par la suite, vous devez ajouter un pattern index dans kibana afin de prendre en considération vos indexs quotidiens Apache récupérés par elasticsearch. Cliquez sur "Index Patterns" sur le volet à gauche et cliquez sur le bouton "Create index pattern" :



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Dans notre cas le préfix de nos indexs apache est "apache-", donc le pattern index à créer dans kibana sera apache-* :

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .

[Read documentation](#) 

Step 1 of 2: Define an index pattern

Index pattern name

Next step >

Use an asterisk (*) to match multiple indices. Spaces and the characters `\,/,?,",<,>|` are not allowed.

☐ Include system and hidden indices

✓ Your index pattern matches 1 source.

apache-2021.01.15

Index

Rows per page: 10 ▾




Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Cliquez ensuite sur "Next Step". Ensuite il nous demande par quel moyen il doit gérer le filtre temporel (timestamp). Ce filtre est utile pour filtrer et affiner nos données par plage horaire. Nous avons prévu le coup sur notre configuration logstash en créant un champ @timestamp, et c'est celui là qu'on sélectionnera :

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .

[Read documentation](#) 

Step 2 of 2: Configure settings

Specify settings for your **apache*** index pattern.

Select a primary time field for use with the global time filter.

Time field

[Refresh](#)

@timestamp



[> Show advanced settings](#)

[< Back](#)

Create index pattern



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Enfin, cliquez sur le bouton "Create index pattern" et vous verrez apparaître tous vos champs :

apache*

Time field: '@timestamp'

This page lists every field in the **apache*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#)

Fields (34) Scripted fields (0) Source filters (0)

Search

All field types

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	
@version	string		•		
@version.keyword	string		•	•	
_id	string		•	•	
_index	string		•	•	
_score	number				
_source	_source				
_type	string		•	•	
agent	string		•		
agent.keyword	string		•	•	

Rows per page: 10

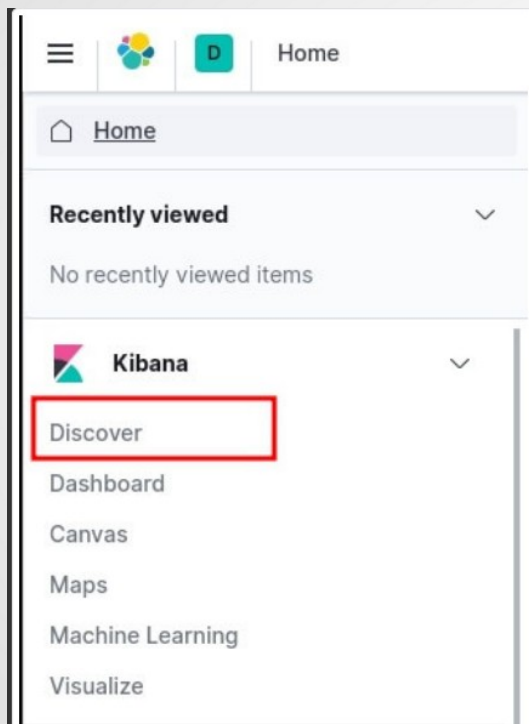
< 1 2 3 4 >



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Découvrir vos logs : Pour découvrir vos logs, sur le menu à gauche cliquez sur Discover :



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



















Ensuite, Faites quelques visites depuis votre navigateur sur la page d'accueil d'apache <http://localhost/> et revenez sur la page de discover :



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Vous avez également la possibilité de filtrer vos logs par champ depuis la barre de recherche du Discover :

Search	
 <code>_id</code>	Filter results that contain <code>_id</code>
 <code>_index</code>	Filter results that contain <code>_index</code>
 <code>_type</code>	Filter results that contain <code>_type</code>
 <code>@timestamp</code>	Filter results that contain <code>@timestamp</code>
 <code>@version.keyword</code>	Filter results that contain <code>@version.keyword</code>
 <code>@version</code>	Filter results that contain <code>@version</code>
 <code>agent.keyword</code>	Filter results that contain <code>agent.keyword</code>
 <code>agent</code>	Filter results that contain <code>agent</code>
 <code>auth.keyword</code>	Filter results that contain <code>auth.keyword</code>
 <code>auth</code>	Filter results that contain <code>auth</code>
 <code>bytes</code>	Filter results that contain <code>bytes</code>
 <code>clientip.keyword</code>	Filter results that contain <code>clientip.keyword</code>
 <code>clientip</code>	Filter results that contain <code>clientip</code>
 <code>host.keyword</code>	Filter results that contain <code>host.keyword</code>
 <code>host</code>	Filter results that contain <code>host</code>
 <code>httpversion.keyword</code>	Filter results that contain <code>httpversion.keyword</code>
 <code>httpversion</code>	Filter results that contain <code>httpversion</code>
 <code>ident.keyword</code>	Filter results that contain <code>ident.keyword</code>

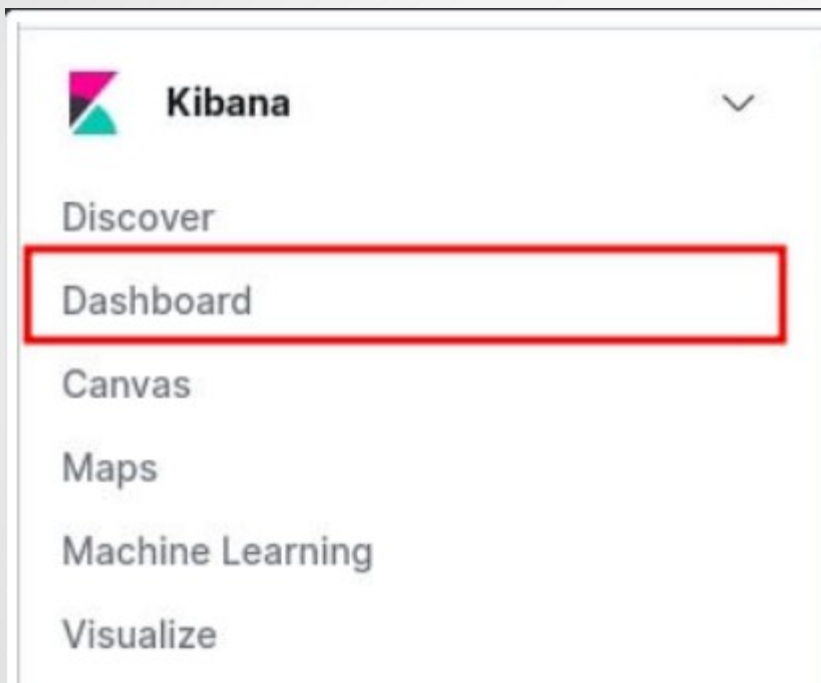
Exemple : "response : 404" pour
n'afficher que les requêtes en
erreur 404.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Dashboard : L'étape suivante est de créer un tableau de bord afin de visualiser une collection de visualisations en temps réel. Pour commencer, ouvrez le menu, accédez à Dashboard , puis cliquez sur "Create dashboard" :



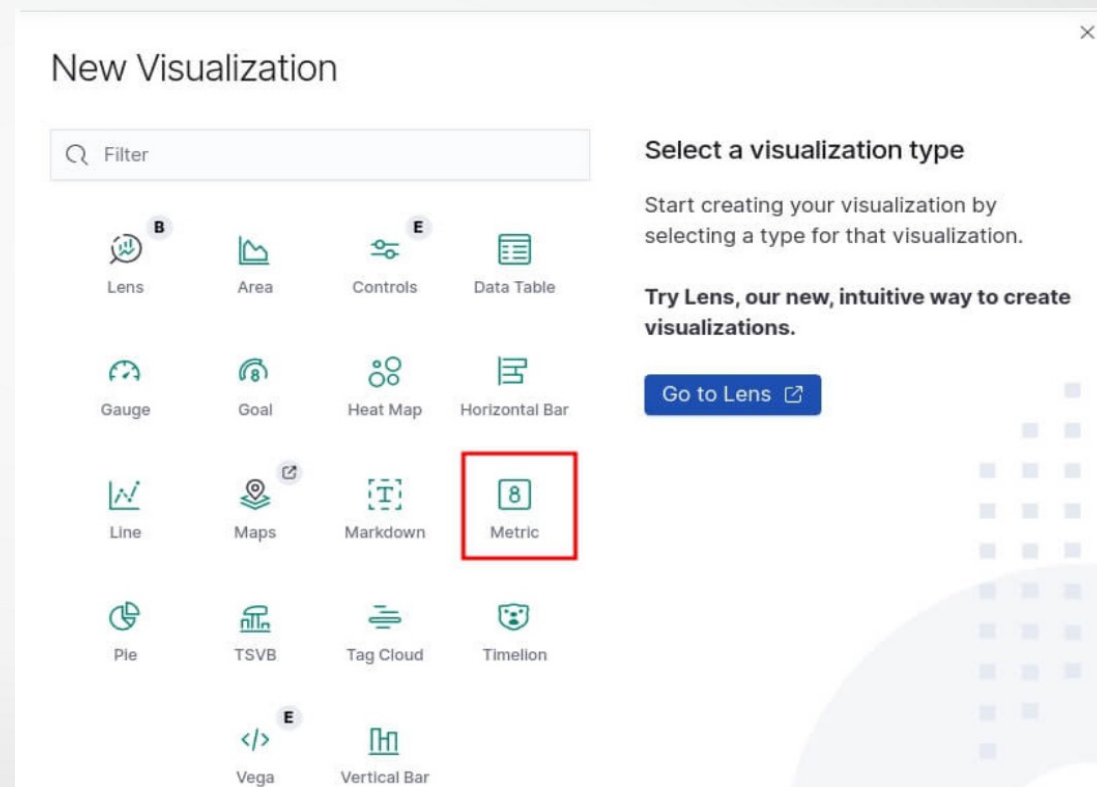
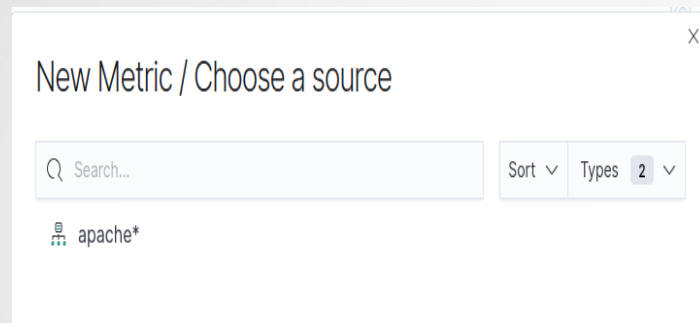
Pour ajouter des éléments à votre dashboard vous devez créer des visualisations Kibana que vous pouvez déplacer et redimensionner dans votre dashboard. Vous pouvez ajouter des visualisations à partir de plusieurs index patterns et la même visualisation peut apparaître dans plusieurs tableaux de bord.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Dans notre exemple nous allons commencer par créer une visualisation qui permet d'afficher la taille moyenne des requêtes temporellement, Pour ce faire, créez une visualisation en cliquant sur "Create new" et dans la fenêtre de "New visualisation" nous allons choisir le type de visualisation "area".



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour information, voici la liste des types de visualisations Kibana les plus fréquemment utilisées :

- **Line, area, et bar charts** : compare différentes métriques sur l'axe X et Y.
- **Pie chart** : graphique circulaire.
- **Data table** : données en format de tableau.
- **Metric** : affiche une seule métrique.
- **Goal and gauge** : affiche un nombre avec des indicateurs de progression.
- **Tag cloud** : affiche les mots dans un nuage, où la taille du mot correspond à son importance.

On vous demande ensuite de paramétrer votre visualisation, vous devez choisir d'abord votre agrégation qui correspond aux métriques extraites pour générer des valeurs de données. Voici les valeurs les plus communes :

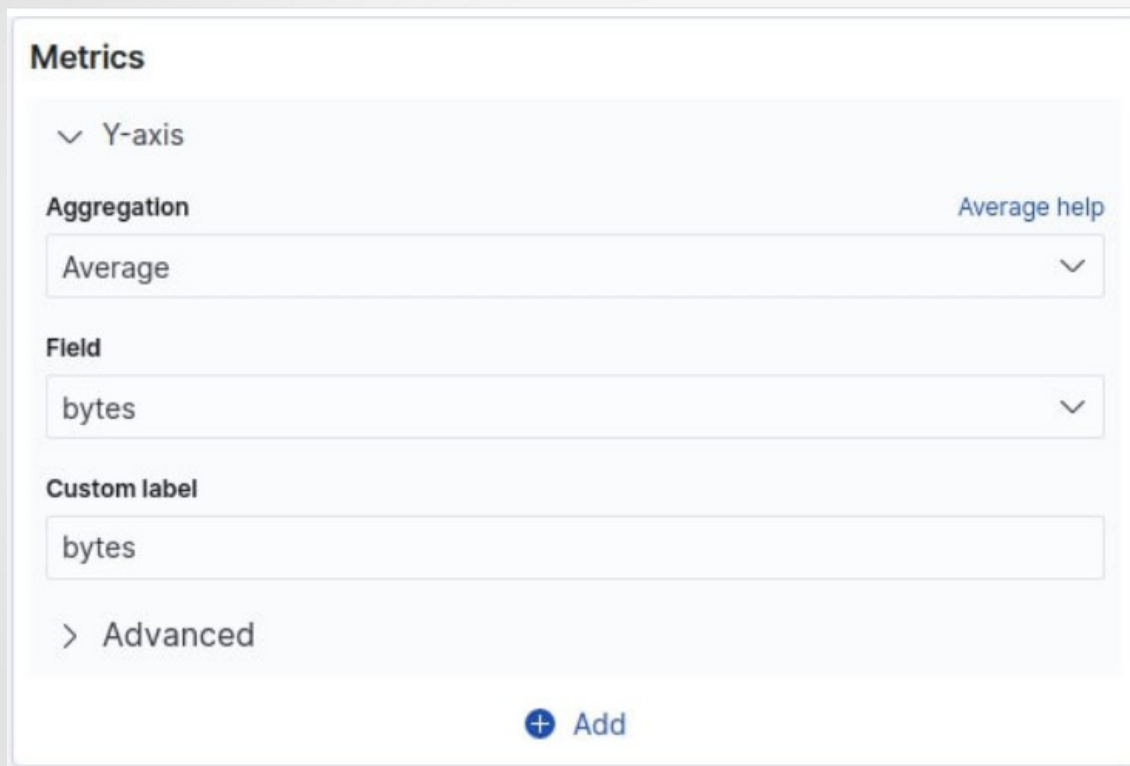
- **Average** : valeur moyenne.
- **Count** : nombre total de documents correspondant à une requête.
- **Max** : la valeur la plus élevée.
- **Median** : médiane.
- **Min** : la valeur la plus basse.
- **Sum** : La valeur totale.
- **Unique Count** : nombre unique d'une métrique.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuelle de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Pour l'axe Y nous allons utiliser une agrégation de type "Average" sur le champ byte :



The screenshot shows the 'Metrics' configuration panel in the ELK stack. It includes a 'Y-axis' section with a dropdown for 'Aggregation' set to 'Average' (with a link to 'Average help'), a 'Field' dropdown set to 'bytes', and a 'Custom label' field containing 'bytes'. There is an 'Advanced' link and an 'Add' button at the bottom.

Pour l'axe X ça sera un peu différent car nous utiliserons les Bucket aggregations qui trient les documents en compartiments selon le contenu du document. Voici les valeurs les plus communes :

Date histogram : fractionne un champ de date en compartiments par intervalle.

Date range : valeurs comprises dans une plage de dates que vous spécifiez.

Filter : filtre les données récupérées (ex : traiter que les erreurs 404).

IPv4 range : plages d'adresses IPv4.

Range : plages de valeurs pour un champ numérique.

Terms : Spécifiez le nombre d'éléments supérieurs ou inférieurs d'un champ donné à afficher, classés par nombre ou par une métrique personnalisée.





Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155


ELK

Pour notre cas nous utiliserons le type "Date histogram" :


Buckets

☒ X-axis  



Aggregation [Date Histogram help](#)

Date Histogram 

Field

@timestamp 

Minimum Interval


Auto  

Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

☐ Drop partial buckets

Custom label

[> Advanced](#)

 Add



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Nous allons cette fois-ci afficher le top des requêtes en erreur sous forme d'un tableau. Créez une nouvelle visualisation de type "Data table" avec comme configuration une agrégation de type "Count" (par défaut) et une Bucket aggregation de type "Terms" sur le champ "request" et trier par ordre décroissant par l'agrégation "Count", ce qui nous affichera pour le moment que les pages web les plus visitées. Cette partie de la configuration ressemblera à ceci :

The screenshot shows the Kibana configuration for a new visualization. In the 'Aggregation' section, 'Count' is selected. In the 'Buckets' section, 'Split rows' is checked, 'Terms' is selected for aggregation, 'request.keyword' is the field, and it is ordered by 'Metric: Count' in descending order with a size of 5.

Ensuite pour récupérer que les requêtes en erreur, nous filtrerons ces requêtes si elles ont une réponse différente au code HTTP 200. Pour cela, vous devez cliquer sur le bouton situé en haut à gauche nommé "+ Add filter" et ajouter le filtre suivant :

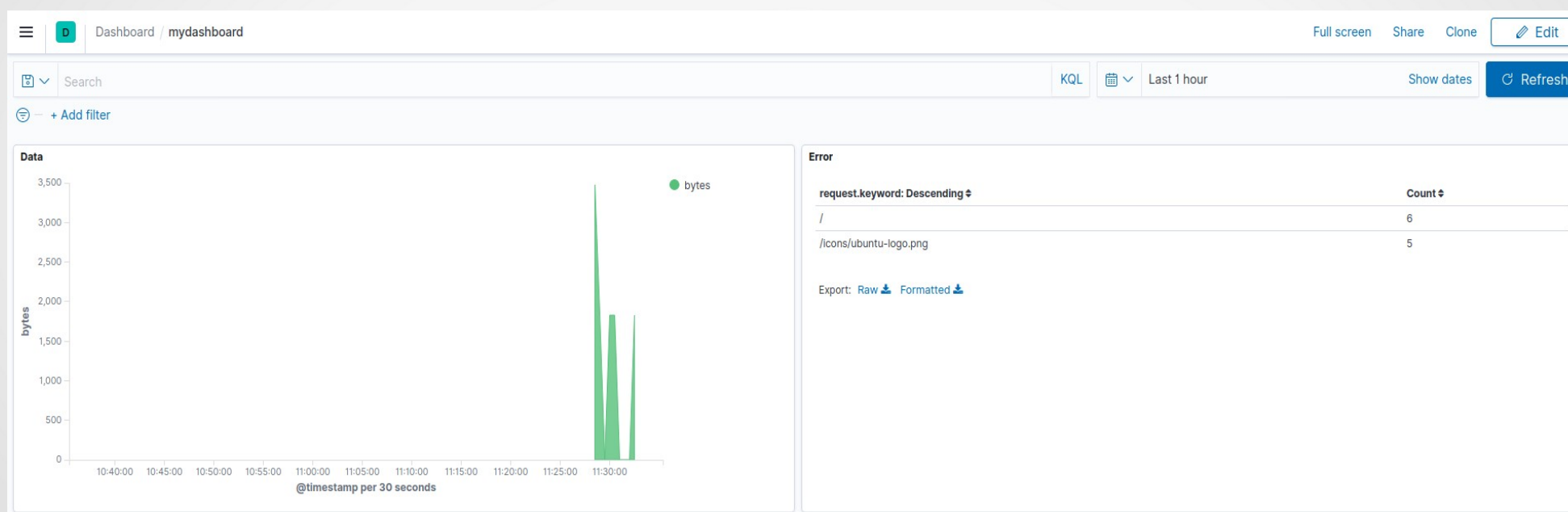
The screenshot shows the 'EDIT FILTER' dialog box. The field is 'response', the operator is 'is not', and the value is '200'. The 'Save' button is highlighted.



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK

Lorsque vous avez terminé d'ajouter et d'organiser les panneaux, enregistrez le tableau de bord. Dans la barre d'outils Kibana, cliquez sur "Save" et saisissez ensuite le titre du tableau de bord et la description facultative, puis enregistrez votre tableau de bord. Le dashboard final ressemble à ceci :



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155

ELK



Mr. BILEL Issaoui, Formateur DevOps chez Ghazela Technology Academy, www.ghazelatc.com. Tél. +21654260000. Le support est à usage personnel, il est propriété intellectuel de l'académie, il n'est pas à usage commercial, contact@ghazelatc.com, +21671866142, +21654828018, +21627862155