Table des matières

Pour ce TP nous formons le binôme LEGER Lucas + LAFORGE Samuel. Nous avons décidé de faire l'installation de la suite ELK et de comparer son installation et son utilisation à celle de Loki

Nous avons suivi le site d'elastic pour procéder aux différentes installations :
https://www.elastic.co/fr/downloads/

Pour les configurations de fichier nous avons suivi le site suivant :
https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-20-04-fr

1. Installation et configuration d'ElasticSearch

Avant de commencer le TP nous allons désactiver le firewall car nous allons utiliser plusieurs ports donc soit nous désactivons le firewall soit nous ouvrons tous les ports dont nous avons besoin sur chaque machine :

```
systemctl disable firewalld.service && systemctl stop firewalld.service
```

L'installation d'ElasticSearch et de Kibana se fait sur notre machine Rocky

Pour effectuer l'installation du serveur ElasticSearch nous avons plusieurs solutions possibles. Télécharger un fichier zip et le décompresser ou alors créer un dépôt RPM et installer directement ElasticSearch. Nous avons décidé d'installer avec le dépôt RPM en suivant ce site :
https://www.elastic.co/fr/downloads/elasticsearch

Tout d'abord nous devons récupérer et installer la clé publique :

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

Création du dépôt RPM :

```
nano /etc/yum.repos.d/elasticsearch.repo
```

Contenu du fichier :

```
[elasticsearch]
name=Elasticsearch repository for 7.x packages
```

```
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
autorefresh=1
type=rpm-md
```

Maintenant que nous avons le dépôt nous pouvons installer le serveur :

```
sudo yum install --enablerepo=elasticsearch elasticsearch
```

Durant l'installation un utilisateur elasticsearch est créé et est ajouté au groupe elasticsearch

L'installation est faite nous pouvons procéder à la configuration de l'hôte dans le fichier yml :

```
nano /etc/elasticsearch/elasticsearch.yml
```

Décommenter les lignes suivantes dans les onglets Network et Discovery :

```
network.host: 0.0.0.0
discovery.seed_hosts: ["0.0.0.0:9300"]
```

Ici nous avons autorisé toutes les IP de la machine comme serveur

Elasticsearch est bien installé. Maintenant nous pouvons activer le service et le démarrer :

```
systemctl enable elasticsearch.service && systemctl start elasticsearch.service
```

Nous pouvons vérifier son bon fonctionnement :

```
[root@localhost ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
  Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
  Active: active (running) since Fri 2022-01-21 09:17:45 CET; 30min ago
    … … … … … … … … … … … …
```

Puis :

```
[root@localhost ~]# curl http://localhost:9200/
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "m_Vxx3cNQFO_8AVOk0VG_Q",
  "version" : {
    "number" : "7.16.3",
    "build_type" : "rpm",
… … … … … … … … … … …
```

2. Installation et configuration de Kibana

Pour effectuer l'installation de Kibana nous avons plusieurs solutions possibles. Télécharger un fichier zip et le décompresser ou alors créer un dépôt RPM et installer directement Kibana. Nous avons décidé d'installer avec le dépôt RPM en suivant ce site : https://www.elastic.co/fr/downloads/kibana

La clé publique ayant déjà été récupéré pour l'installation d'ElasticSearch nous n'avons pas besoin de la retélécharger

Création du dépôt RPM :

```
nano /etc/yum.repos.d/kibana.repo
```

Contenu du fichier :

```
[kibana-7.x]
name=Kibana repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Nous pouvons maintenant installer kibana :

```
sudo yum install kibana
```

Durant l'installation un utilisateur kibana est créé et est ajouté au groupe kibana

Nous pouvons maintenant modifier le fichier de configuration :

```
nano /etc/kibana/kibana.yml
```

Décommenter les lignes suivantes :

```
server.host: "10.44.19.200"
elasticsearch.hosts: ["http://localhost:9200"]
```

Ici nous avons défini l'IP de l'hôte sur laquelle nous accédons par pont pour pouvoir autoriser les connexions à distances depuis notre machine physique et éviter de faire un reverse proxy et l'IP du serveur hôte afin de récupérer les données dessus

Nous pouvons maintenant activer et démarrer le service kibana :

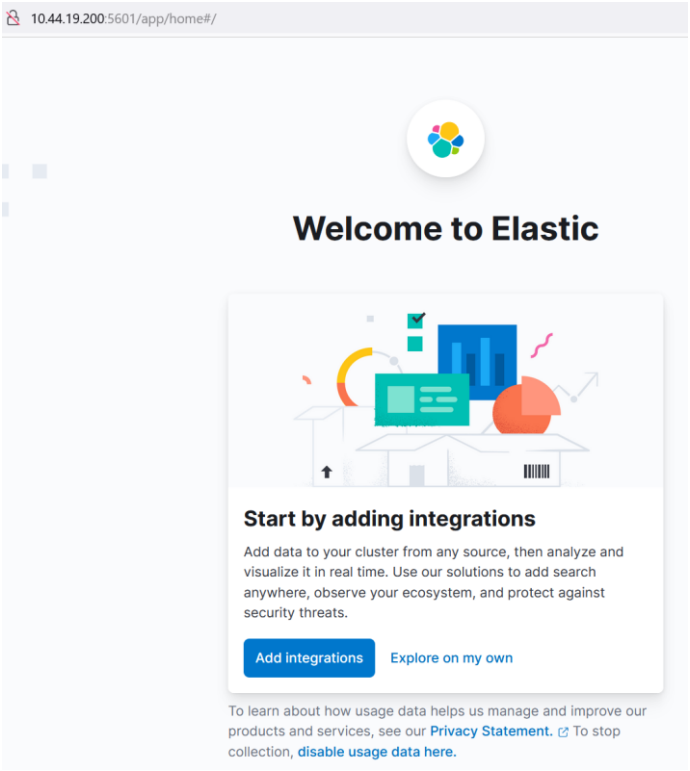
```
systemctl enable kibana.service && sytemctl start kibana.service
```

Nous pouvons vérifier son bon fonctionnement :

```
[root@localhost ~]# systemctl status kibana.service
● kibana.service - Kibana
```

```
Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
Active: active (running) since Fri 2022-01-21 09:56:35 CET; 11min ago
  Docs: https://www.elastic.co
Main PID: 4809 (node)
  Tasks: 11 (limit: 49498)
```

Tout est maintenant configuré. Nous pouvons ouvrir un navigateur et y entrer l'IP de notre serveur ainsi que son port pour accéder à kibana :



3. Installation et configuration de Logstash sur la Debian

Cette installation s'effectue sur la machine sur laquelle nous récupérons les données avant de les envoyer sur le serveur (ici sur notre machine Debian). Installer Logstash va nous permettre de traiter les données avant de les envoyer vers le serveur avec FileBeat. Ceci augmentera la flexibilité des données pour les collecter depuis différentes sources, les transformer dans un format commun et les exporter vers une autre base de données.

Pour effectuer l'installation de Logstash nous avons plusieurs solutions possibles. Télécharger un fichier zip et le décompresser ou alors ajouter la source et installer directement Logstash. Nous avons décidé d'installer en ajoutant la source à notre machine et en installant le paquet en suivant ce site : https://www.elastic.co/fr/downloads/logstash

Tout d'abord nous devons télécharger et ajouter la clé publique :

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

Nous devons installer le paquet suivant si jamais ce n'est pas déjà le cas :

```
sudo apt-get install apt-transport-https
```

Ajout de la source elastic (c'est elle qui nous permettra d'installer le paquet Logstash) :

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

Nous mettons à jour les paquets de la machine et nous installons Logstash :

```
sudo apt-get update && sudo apt-get install logstash
```

Nous devons maintenant configurer Logstash pour ajouter une entrée Filebeat afin qu'il puisse recevoir les données :

```
nano /etc/logstash/conf.d/02-beats-input.conf
```

Contenu du fichier :

```
input {
  beats {
    port => 5044
  }
}
```

Nous avons ici spécifié une entrée de beats qui écoutera sur le port 5044

Nous devons maintenant configurer la sortie des données vers le serveur :

```
nano /etc/logstash/conf.d/30-elasticsearch-output.conf
```

Contenu du fichier :

```
output {
  if [@metadata][pipeline] {
    elasticsearch {
    hosts => ["10.44.19.200:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    pipeline => "%{[@metadata][pipeline]}"
    }
  } else {
    elasticsearch {
    hosts => ["10.44.19.200:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    }
  }
}
```

Globalement, cette sortie configure Logstash pour stocker les données des Beats dans Elasticsearch, qui tourne sur `10.44.19.200:9200` qui est l'IP de notre serveur, dans un index nommé en fonction du Beat utilisé. Le Beat utilisé dans ce tutoriel est Filebeat

Nous pouvons tester sa configuration :

```
sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t
```

Après quelques secondes voir 1 minute nous devrions avoir une sortie comme celle-ci :

```
Configuration OK
[2022-01-21T10:37:45,639][INFO ][logstash.runner          ] Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

Si la configuration est OK nous pouvons activer et démarrer le service :

```
systemctl enable logstash.service && systemctl start logstash.service
```

4. Installation et configuration de Filebeat

L'Elastic Stack utilise plusieurs expéditeurs de données légers appelés Beats pour collecter des données de diverses sources et les transporter vers Logstash ou Elasticsearch. Voici les Beats qui sont actuellement disponibles chez Elastic :

Filebeat : recueille et expédie les fichiers journaux.

Metricbeat : collecte les métriques de vos systèmes et services.

Packetbeat : recueille et analyse les données du réseau.

Winlogbeat : collecte les journaux des événements Windows.

Auditbeat : collecte les données du framework de vérification Linux et surveille l'intégrité des fichiers.

Heartbeat : surveille activement la disponibilité des services.

Pour effectuer l'installation de Filebeat nous avons plusieurs solutions possibles. Télécharger un fichier zip et le décompresser ou alors ajouter la source et installer directement Filebeat. Nous avons décidé d'installer en ajoutant la source à notre machine en nous aidant des sites suivants : https://www.elastic.co/fr/downloads/beats/filebeat

Nous pouvons directement installer Filebeat car la clé publique et la source sont déjà ajoutés sur la machine :

```
sudo apt-get install filebeat
```

Nous devons modifier le fichier de configuration afin que Filebeat envoi les données vers Logstash et non vers le serveur ElasticSearch directement afin que les données soient traitées avant :

```
#output.elasticsearch:
  # Array of hosts to connect to.
#  hosts: ["localhost:9200"]


output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```

Filebeat utilise plusieurs modules qui peuvent êtres activés. Ici nous n'utiliserons que le module system qui collecte et analyse les journaux créés par le service de journalisation du système. Toutes les commandes suivantes sont à refaire pour chaque module que nous activeront. Ici nous activons le module system donc nous passons toutes les commandes mais si nous installions le module apache nous devrions repasser toutes les commandes suivantes afin de mettre en place la récupération de log et l'envoi des logs dans un dashboard pré-configuré de Kibana

```
sudo filebeat modules enable system
```

Nous pouvons vérifier que notre module est bien activé :

```
root@debian10:/home/debian# sudo filebeat modules list

Enabled:

system
```

Nous devons maintenant mettre en place les pipelines d'ingestion de Filebeat qui analysent les données du journal avant de les envoyer à notre serveur ElasticSearch via Logstash.

Nous devons d'abord charger le pipeline d'ingestion pour le module system :

```
sudo filebeat setup --pipelines --modules system
```

Ensuite charger le modèle d'index dans ElasticSearch :

```
sudo filebeat setup --index-management -E output.logstash.enabled=false -E
'output.elasticsearch.hosts=["10.44.19.200:9200"]'
```

Filebeat contient des Dashboards pré-configurés que nous pouvons importer dans Kibana. Pour se faire nous devons charger les dashboard en reliant directement Filebeat au serveur sans passer par Logstash :

```
sudo filebeat setup -E output.logstash.enabled=false -E
output.elasticsearch.hosts=['10.44.19.200:9200'] -E setup.kibana.host=10.44.19.200:5601
```

Nous devrions ressortir un résultat comme suit :

```
Index setup finished.

Loading dashboards (Kibana must be running and reachable)

Loaded dashboards

Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app
instead.

See more: https://www.elastic.co/guide/en/machine-learning/current/index.html

It is not possble to load ML jobs into an Elasticsearch 8.0.0 or newer using the Beat.

Loaded machine learning job configurations

Loaded Ingest pipelines
```

Nous pouvons maintenant activer et démarrer le service Filebeat :

```
systemctl enable filebeat && systemctl start filebeat
```

Si notre Logstash ainsi que le serveur sont bien configurés nous devrions avoir des données qui partent vers le serveur :

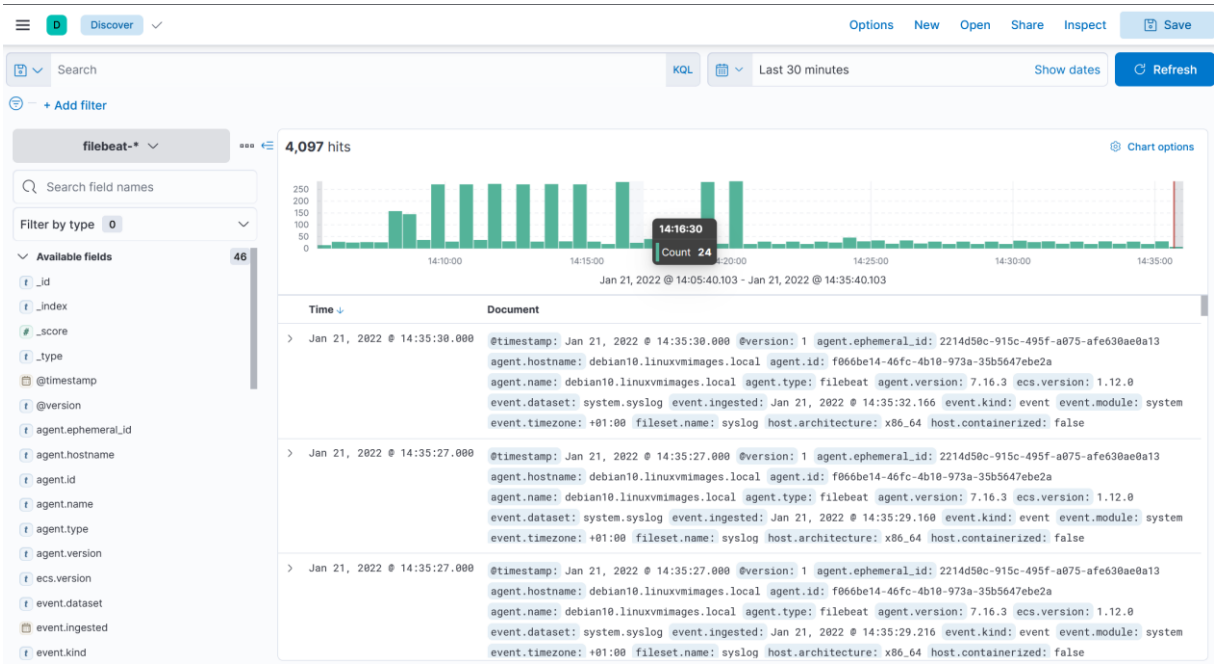
```
curl -XGET 'http://10.44.19.200:9200/filebeat-*/_search?pretty'
```

5. Visualisation des Dashboards

Commande pour vider tous les logs qui sont récupérés par Kibana :

```
curl -XPUT -H "Content-Type: application/json" https://[YOUR_ELASTICSEARCH_ENDPOINT]:9200/_all/_settings -d '{"index.blocks.read_only_allow_delete": null}'
```

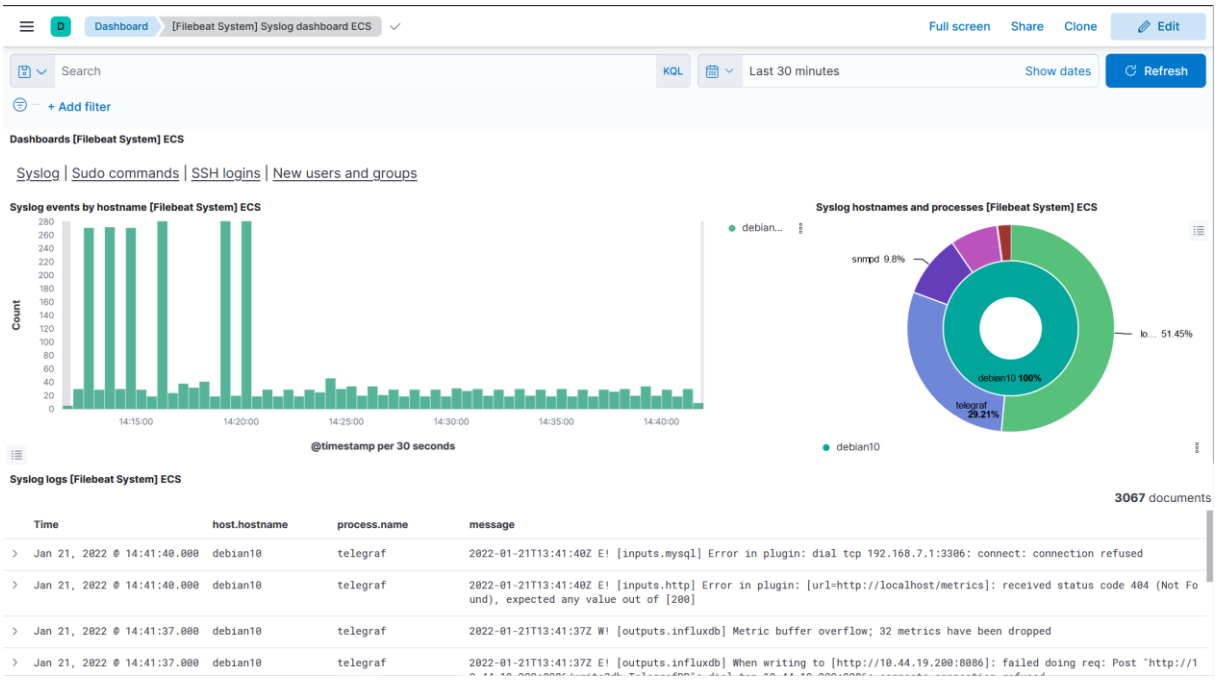
Nous pouvons maintenant aller dans notre navigateur sur la page kibana. Nous pouvons faire un discover afin de trouver notre index pattern et visualiser le nombre de logs récupérés :



Il existe aussi différents Dashboards déjà créés dans l'onglet Dashboards. Il suffit de trouver un Dashboard utilisant le module "system" que nous avons activé précédemment :

[Filebeat System] New users and groups ECS	New users and groups dashboard for the System module in Filebeat
[Filebeat System] SSH login attempts ECS	SSH dashboard for the System module in Filebeat
[Filebeat System] Sudo commands ECS	Sudo commands dashboard from the Filebeat System module
[Filebeat System] Syslog dashboard ECS	Syslog dashboard from the Filebeat System module

Par exemple nous pouvons utiliser le Dashboard Syslog ECS afin de voir les logs système :



Ce Dashboard nous affiche tous les logs systèmes en bas ainsi que les moments où il y en a eu le plus et quel processus en a créé le plus

Dashboard pour Apache :

Nous pouvons visualiser tous les logs d'apache sur ce dashboard et voir dans les erreurs ci-dessus que nous avons bien coupé et redémarré le serveur

6. Comparaison avec Loki

Lors du TP précédent nous avons mis en place une solution du même type avec Loki/Grafana/Promtail. De notre point de vu la solution ELK est légèrement plus compliqué à mettre en place mais une fois toutes les installations faites nous avons de très beaux dashboards pré-configurés dans Kibana et qui sont lisibles contrairement à Grafana où nous devions créer nous même des dashboards et les configurer