2024

Installation et configuration de ELK

Client :	Tous
Rédigé le :	17/06/2024
Auteur :	Allen
Version :	1.0

Modifié le :	Auteur :	Version :

Brown Allen
INFOTECH
17/06/2024

Sommaire :

Installation de elasticsearch……..……...…..2

Installation de kibana……...…4

Installation de logstash……...…….5

Installation de filebeat……..6

I. Installation de elasticsearch

Ordre d'installation :

1. Elasticsearch
2. Kibana
3. Logstash

Ajouter la clé de signature d'élastic pour que le package téléchargé puisse être vérifié.

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

Installer le paquet "**apt-transport-https**"

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

Ajouter le dépôt elasticsearch sur le 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
```

Installer elasticsearch

```
sudo apt-get update -y && sudo apt-get install elasticsearch
```

Configuration elasticsearch

créer un fichier ce nommant "**ram.options**" dans le répertoire
"/etc/elasticsearch/jvm.options.d/ram.options"

Exécuter la commande suivante :

```
sudo nano /etc/elasticsearch/jvm.options.d/ram.options
```

Ajouter les lignes suivante dans le fichier "**ram.options**"

```
-Xms4g
-Xmx4g
```

Enregistrer en appuyant sur Ctrl + O puis entrée, faite ensuite un Ctrl + X pour quitter le fichier de configuration.

Modifier le fichier de configuration d'elasticsearch pour attribuer une adresse ip, un port et ajouter quelques options.

Procédé comme suit :

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

Ajouter ou décommenter les options et fonctions suivante :

```
cluster.name: srv-elk
network.host: 192.168.20.75
http.port: 9200
discovery.type: single-node
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
```

Enregistrer en appuyant sur Ctrl + O puis entrer, quitter ensuite le fichier de configuration en appuyant sur Ctrl + X

Lancer le service elasticsearch avec la commande suivante :

```
sudo systemctl start elasticsearch
```

Pour vérifier le bon fonctionnement de elasticsearch, lancer la commande suivante :

```
curl 192.168.20.75:9200
```

Résultat :

```
{
  "name" : "hatim-linux",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "U1zH_yFqTUmdMRckR1gHLQ",
  "version" : {
```

```
    "number" : "7.8.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "757314695644ea9a1dc2fecd26d1a43856725e65",
    "build_date" : "2020-06-14T19:35:50.234439Z",
    "build_snapshot" : false,
    "lucene_version" : "8.5.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Exécuter ensuite la commande suivante afin de lancer elasticsearch à chaque démarrage.

```
sudo systemctl enable elasticsearch
```

II. Installation de kibana

Exécuter la commande suivant :

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

Modifier le fichier de configuration de kibana

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

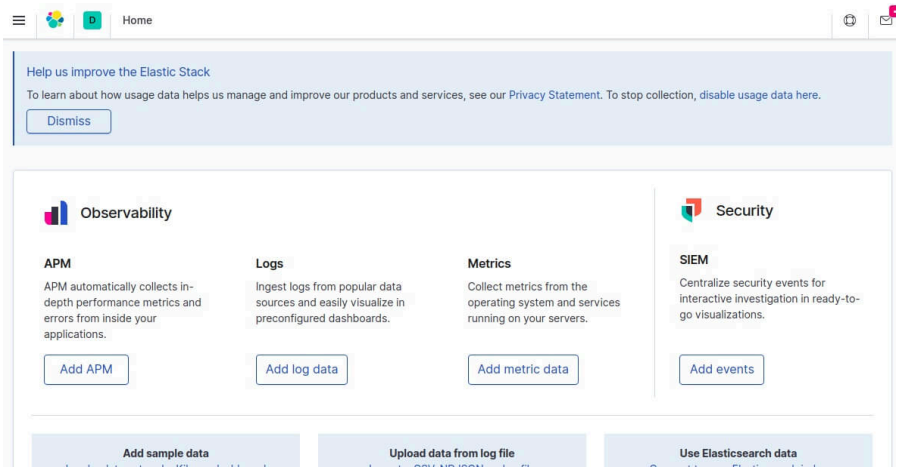
Ajouter ou décommenter les options et fonctions suivante :

```
server.port: 5601
server.host: “192.168.20.75”
server.name: “srv-elk”
elasticsearch.hosts: [“http://192.168.20.75:9200”]
elasticsearch.username: “elastic”
elasticsearch.password: “Infotech2024#!$%”
```

Lancé kibana :

```
sudo systemctl start kibana
```

Tester kibana en entrant “http://192.168.20.75:5601” dans un navigateur web



Lancé la commande suivante pour démarrer le service kibana à chaque démarrage

```
sudo systemctl enable kibana
```

III. Installation de logstash

Installer java 8 :

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

vérification de l’installation de java :

```
java -version
```

Résultat :

```
openjdk version "11.0.7" 2020-04-14
...
```

Installer ensuite logstash :

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

lancé logstash :

```
sudo systemctl start logstash
```

exécuter la commande suivante :

```
sudo systemctl enable logstash
```

Installer apache2 :

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

lancé apache2 :

```
sudo systemctl start apache2
```

IV Installation de filebeat

Installer filebeat :

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

Modifier le fichier de configuration de filebeat :

```
sudo nano /etc/filebeat/filebeat.yml
```

Ajouter ou décommenter les options suivante :

```
- type: filestream
  enabled: true
filebeat.config.modules:
reload.enabled: true
reload.period: 15s
```

```
setup.kibana:
host: “192.168.20.75”
output.elasticsearch:
hosts: [“192.168.20.75:9200”]
username: “elastic”
password: “Infotech2024#!$%”
```

Modifier ensuite le modules **“fortinet.yml**” ce trouvant dans le répertoire “**/etc/filebeat/modules.d/fortinet.yml**”

Ajouter ou décommenter les options suivante :

```
- module: fortinet
firewall:
enabled: true
var.input: udp
var.syslog_host: 192.168.20.75
var.syslog_port: 9004
```

désactiver tout les options suivante :

```
clentendpoint:
enabled: false
fortimail:
enabled: false
fortimanager:
enabled: false
```

Activer le setup filebeat :

```
filebeat setup -e
```

Activer ensuite filebeat :

```
sudo systemctl start filebeat
```

Ouvrir kibana puis entrer vos identifiant et mot de passe soit “elastic” et “Infotech2024#!$%”
Une fois à l’intérieur de kibana, cliquez sur les trois trait en haut à gauche puis sélectionner la rubrique “**Discover**” puis choisir “**filebeat-***” afin de visualiser les logs transmis.