Installation ELK

supervision, ELK

Note : ELK est en version 7.x au moment de la rédaction de cette page, c'est la raison pour laquelle nous utilisons le dépôt de cette branche.

Méthode 1 : ajout dépôt APT

Nous créons le fichier elasticsearch.list, et ajoutons le dépôt pour Elasticsearch :

```
sudo nano /etc/apt/sources.list.d/elasticsearch.list
```

```
##
# Elasticsearch repository
# Version: 7.x
##

deb http://HTTPS///artifacts.elastic.co/packages/7.x/apt stable main
```

Note : le lien APT est de la forme “http://HTTPS///” pour pouvoir passer par le proxy APT local, bien qu'étant à la base un dépôt en HTTPS.

Nous importons la clé GPG du dépôt :

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

Méthode 2 : utilisation du dépôt local

Une copie de paquets est faite sur notre dépôt APT local OPLV. C'est la solution qui est privilégiée.
Nous récupérons la clé GPG du dépôt :

```
wget -q -O - http://repo.oplv-france.pro/oplv-apt.pub | sudo apt-key add -
```

Nous créons le fichier /etc/apt/sources.list.d/oplv.list

```
##
# OPLV repository
```

```
# Version: Stretch
##

deb http://repo.oplv-france.pro/debian stretch main
```

Nous mettons le cache à jour

```
sudo aptitude update
```

Installation des paquets

Nous installons les paquets nécessaires :

```
sudo aptitude update && sudo aptitude install openjdk-8-jdk-headless
elasticsearch kibana logstash
```

Configuration

Nous configurons elasticsearch :

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

Nous renseignons les paramètres suivants:

```
cluster.name: oplv-infra
node.name: node01
network.host: 127.0.0.1
http.port: 9200
```

Nous configurons kibana :

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

Nous renseignons les paramètres suivants:

```
server.port: 5601
server.host: "localhost"
elasticsearch.url: "http://localhost:9200"
```

Installation Nginx comme reverse proxy

Nous installons Nginx qui va servir de reverse proxy :

```
sudo aptitude install nginx
```

Nous créons le vhost

```
sudo nano /etc/nginx/sites-available/rsyslog.neotion.pro
```

Et nous insérons :

```
##
# Nginx vHost
# rsyslog.neotion.pro
##

server {
        listen 80;
        server_name rsyslog.neotion.pro;
        return 301 https://$host$request_uri;
}

server {
        listen 443;
        server_name rsyslog.neotion.pro;

        access_log /var/log/nginx/rsyslog.neotion.pro_access.log;
        error_log /var/log/nginx/rsyslog.neotion.pro_error.log;

        root html;
        index index.html index.htm;

        ssl on;
        ssl_certificate /etc/ssl/certs/neotion.pro.crt;
        ssl_certificate_key /etc/ssl/private/neotion.pro.key;
        ssl_trusted_certificate /etc/ssl/certs/neotion.pro.root.crt;
        ssl_session_timeout 1d;
        ssl_session_cache shared:SSL:50m;

        ssl_protocols TLSv1.2;
        ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256';
        ssl_prefer_server_ciphers on;

        location / {
                proxy_pass http://127.0.0.1:5601;
                include proxy_params;
        }
}
```

Nous activons le vhost :

```
cd /etc/nginx/sites-enabled
```

```
sudo ln -s /etc/nginx/sites-available/rsyslog.neotion.pro
```

Nous redémarrons nginx :

```
sudo systemctl restart nginx
```

Démarrage de l'ensemble

Nous activons les services pour qu'ils se lancent au démarrage :

```
sudo systemctl enable elasticsearch
sudo systemctl enable logstash
sudo systemctl enable kibana
```

Nous démarrons les services :

```
sudo systemctl start elasticsearch
sudo systemctl start logstash
sudo systemctl start kibana
```

Test

Pour contrôler depuis l'API Rest d'Elasticsearch

```
curl -X GET http://localhost:9200
```

Vous devriez avoir un retour de ce type

```
{
  "name" : "node01",
  "cluster_name" : "oplv-infra",
  "cluster_uuid" : "lPbKK-s9Qkm6DgOFxQyQvA",
  "version" : {
    "number" : "7.3.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "4749ba6",
    "build_date" : "2019-08-19T20:19:25.651794Z",
    "build_snapshot" : false,
    "lucene_version" : "8.1.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Liens

- https://www.elastic.co site ELK
- install Elasticsearch with Debian Package
- https://blog.schermi.fr/2017/08/31/install-elk/ Install ELK on debian 9
- https://www.4armed.com/blog/installing-the-elk-stack-on-ubuntu/ installing the elk stack on Ubuntu