

# Cluster Elasticsearch with Ansible

## Advanced NoSQL



# elasticsearch

**Réalise par :**

- CHAKOUKI El Hassan.
- DAHAMOU Abdelilah.
- DAHOUCHE Zaineb.

**DATA-INE3 2022**

## ElasticSearch:

Elasticsearch est un puissant moteur de recherche et d'analyse en temps réel open source, RESTful et distribué qui offre la possibilité d'effectuer une recherche en texte intégral. Elasticsearch est basé sur Apache Lucene et le logiciel est disponible gratuitement sous la licence Apache 2. Dans cet article, nous allons installer un cluster Elasticsearch sur CentOS 8/7 et Ubuntu 20.04/18.04 à l'aide de l'outil d'automatisation Ansible.

### Step 1: Installation d'Ansible on VM ubuntu:

Pour se faire on tape les commandes suivant dans notre machine virtual ubuntu :

```
sudo apt update  
sudo apt install software-properties-common  
sudo apt-add-repository --yes --update ppa:ansible/ansible  
sudo apt install ansible
```

### Step 2: Importation de Elasticsearch ansible role:

Après l'installation d'Ansible, on va désormais importer le rôle ansible Elasticsearch sur notre système local à l'aide de galaxy. On tape :

```
$ ansible-galaxy install elastic.elasticsearch
```

Puis on configure notre ssh avec les hôtes de cluster Elasticsearch.

```
Connection to 3.237.99.222 closed.  
hassan@hassan:~$ sudo cat ~/.ssh/config  
# Elasticsearch master nodes  
Host elk_node01  
  Hostname 3.239.37.225  
  User ubuntu  
  IdentityFile /home/hassan/VM1_Key.pem  
  
Host elk_node02  
  Hostname 3.237.99.222  
  User ubuntu  
  IdentityFile /home/hassan/VM1_Key.pem  
  
Host elk_node03  
  Hostname 3.238.76.108  
  User ubuntu  
  IdentityFile /home/hassan/VM1_Key.pem  
...
```

### Steep 3 : Créer un Playbook Elasticsearch et l'exécuter :

Maintenant que tous les prérequis sont configurés, créons un fichier Playbook 'elk\_configuration.yml' pour le déploiement :

```
hassan@hassan:~$ cat ClusterELK/elk_configuration.yml
- hosts: elk_master_nodes
  roles:
    - role: elastic.elasticsearch
  vars:
    es_version: 7.10.0
    es_enable_xpack: false
    es_data_dirs:
      - "/data/elasticsearch/data"
    es_log_dir: "/data/elasticsearch/logs"
    es_java_install: true
    es_heap_size: "1g"
    es_config:
      cluster.name: "elk-cluster-chakouki-dahamou-dahouch"
      cluster.initial_master_nodes: ["3.239.37.225:9300"]
      discovery.seed_hosts: ["3.239.37.225:9300", "3.237.99.222:9300", "3.238.76.108:9300"]
      http.port: 9200
      node.data: false
      node.master: true
      bootstrap.memory_lock: false
      network.host: '0.0.0.0'
    es_plugins:
      - plugin: ingest-attachment

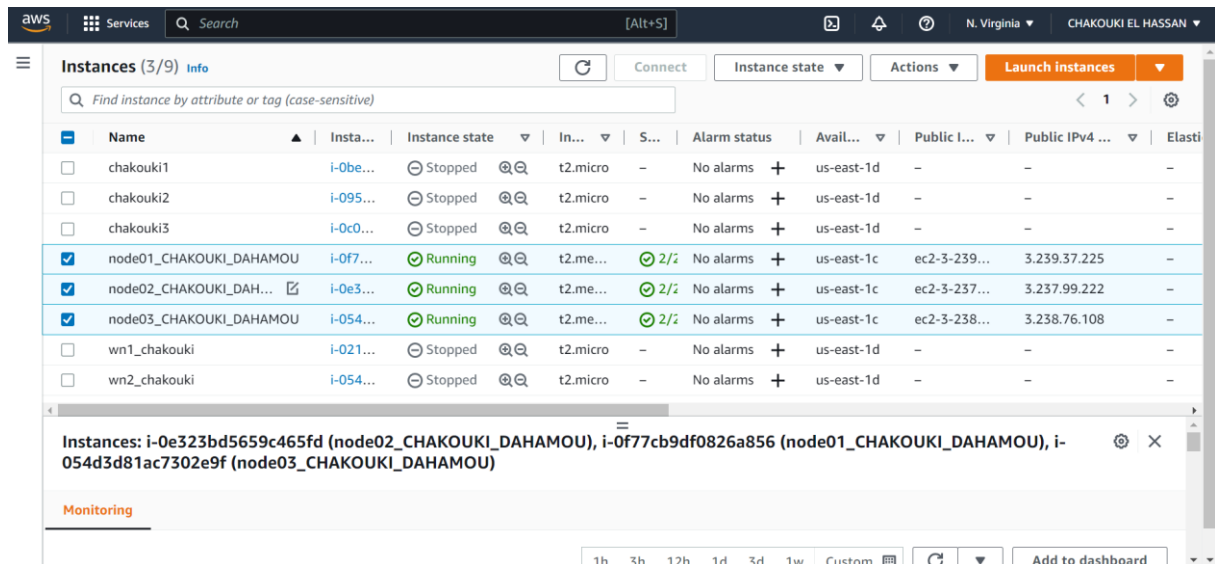
- hosts: elk_data_nodes
  roles:
    - role: elastic.elasticsearch
  vars:
    es_version: 7.10.0
    es_enable_xpack: false
    es_data_dirs:
      - "/data/elasticsearch/data"
    es_log_dir: "/data/elasticsearch/logs"
    es_java_install: true
    es_config:
      cluster.name: "elk-cluster-chakouki-dahamou-dahouch"
      cluster.initial_master_nodes: ["3.239.37.225:9300"]
      discovery.seed_hosts: ["3.239.37.225:9300", "3.237.99.222:9300", "3.238.76.108:9300"]
      http.port: 9200
      node.data: true
      node.master: false
      bootstrap.memory_lock: false
      network.host: '0.0.0.0'
    es_plugins:
      - plugin: ingest-attachment
hassan@hassan:~$
```

puis on va créer un inventory file qu'on appel 'config\_hosts' :

```
hassan@hassan:~$ cat ClusterELK/config_hosts
[servers]
elk_node01 ansible_host=3.239.37.225 ansible_user=ubuntu ansible_ssh_private_key_file=/home/hassan/VM1_Key.pem
elk_node02 ansible_host=3.237.99.222 ansible_user=ubuntu ansible_ssh_private_key_file=/home/hassan/VM1_Key.pem
elk_node03 ansible_host=3.238.76.108 ansible_user=ubuntu ansible_ssh_private_key_file=/home/hassan/VM1_Key.pem

[elk_master_nodes]
elk_node01
[elk_data_nodes]
elk_node02
elk_node03
```

Ce file est fait référence au machine virtual sur aws qui vont jouer le rôle des nœuds d'Elasticsearch :



Lorsque tout est défini, on va exécuter le Playbook 'elk\_configuration.yml' avec la commande :

```
$ ansible-playbook -i config_hosts elk_configuration.yml
```

```
hassan@hassan:~$ ansible-playbook -i ~/ClusterELK/config_hosts ~/ClusterELK/elk_configuration.yml

PLAY [elk_master_nodes] *****

TASK [Gathering Facts] *****
ok: [elk_node01]

TASK [elastic.elasticsearch : set_fact] *****
ok: [elk_node01]

TASK [elastic.elasticsearch : os-specific vars] *****
ok: [elk_node01]

TASK [elastic.elasticsearch : Set fact oss_version when using es_enable_xpack] *****
ok: [elk_node01]

TASK [elastic.elasticsearch : Warn about deprecated es_enable_xpack variable] *****
ok: [elk_node01] => {
```

Au final de l'exécution on doit avoir le résultat suivant :

```
TASK [elastic.elasticsearch : set fact roles_to_modify] *****
skipping: [elk_node02]

TASK [elastic.elasticsearch : Update Native Roles] *****

TASK [elastic.elasticsearch : ensure templates dir is created] *****
skipping: [elk_node02]
skipping: [elk_node03]

TASK [elastic.elasticsearch : Copy templates to elasticsearch] *****

TASK [elastic.elasticsearch : Install templates] *****

PLAY RECAP *****
elk_node01      : ok=40    changed=0    unreachable=0    failed=0    skipped=125   rescued=0    ignored=0
elk_node02      : ok=40    changed=0    unreachable=0    failed=0    skipped=125   rescued=0    ignored=0
elk_node03      : ok=44    changed=15   unreachable=0    failed=0    skipped=90    rescued=0    ignored=0

hassan@hassan:~$ sudo nano ~/.ssh/config
```

## Steep 4 : Confirmation de l'installation d'Elasticsearch Cluster :

On a etabli une connection ssh au 1<sup>er</sup> nœud pour vérifier la bonne installation de nœud d'Elasticsearch :

```
hassan@hassan:~$ ssh elk_node01
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Nov 19 21:26:14 UTC 2022

System load:  0.0          Processes:      109
Usage of /:   6.4% of 38.58GB Users logged in:  0
Memory usage: 38%         IPv4 address for eth0: 172.31.2.164
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

https://ubuntu.com/aws/pro

69 updates can be applied immediately.
50 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 19 16:16:33 2022 from 196.200.133.172
ubuntu@ip-172-31-2-164:~$ curl -XGET 'http://localhost:9200'
{
  "name" : "elk_node01",
  "cluster_name" : "elk-cluster-chakouki-dahamou",
  "cluster_uuid" : "_na_",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "oss"
  },
  "tagline" : "You Know, for Search"
}

ubuntu@ip-172-31-2-164:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/elasticsearch.service.d
            └─override.conf
   Active: active (running) since Sat 2022-11-19 15:11:31 UTC; 6h ago
     Docs: https://www.elastic.co
    Main PID: 6167 (java)
      Tasks: 34 (limit: 4689)
     Memory: 1.1G
    CGroup: /system.slice/elasticsearch.service
            └─6167 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.neg

Nov 19 15:10:51 ip-172-31-2-164 systemd[1]: Starting Elasticsearch...
Nov 19 15:11:31 ip-172-31-2-164 systemd[1]: Started Elasticsearch.

ubuntu@ip-172-31-2-164:~$ s
```

C'est le même avec le 2eme nœud aussi :

```

hassan@hassan:~$ ssh elk_node02
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Nov 19 21:42:38 UTC 2022

System load:  0.0               Processes:    109
Usage of /:   32.5% of 7.57GB   Users logged in: 0
Memory usage: 65%              IPv4 address for eth0: 172.31.7.117
Swap usage:   0%

69 updates can be applied immediately.
50 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 19 16:11:37 2022 from 196.200.133.172
ubuntu@ip-172-31-7-117:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/elasticsearch.service.d
            └─override.conf
   Active: active (running) since Sat 2022-11-19 15:24:13 UTC; 6h ago
     Docs: https://www.elastic.co
   Main PID: 17556 (java)
    Tasks: 35 (limit: 4689)
   Memory: 2.2G
   CGroup: /system.slice/elasticsearch.service
            └─17556 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.ne

Nov 19 15:23:33 ip-172-31-7-117 systemd[1]: Starting Elasticsearch...

```

Lien vers la vidéo démonstrative :

[https://youtu.be/duRBq3p\\_rn8](https://youtu.be/duRBq3p_rn8)

**Fin.**