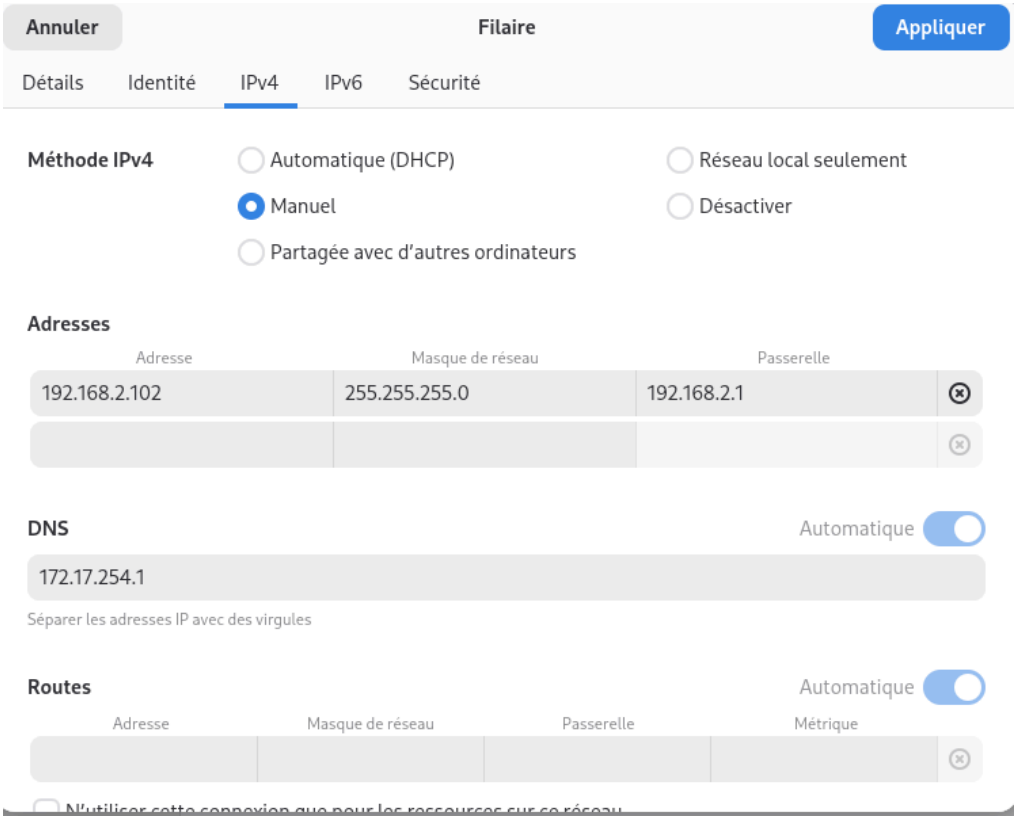
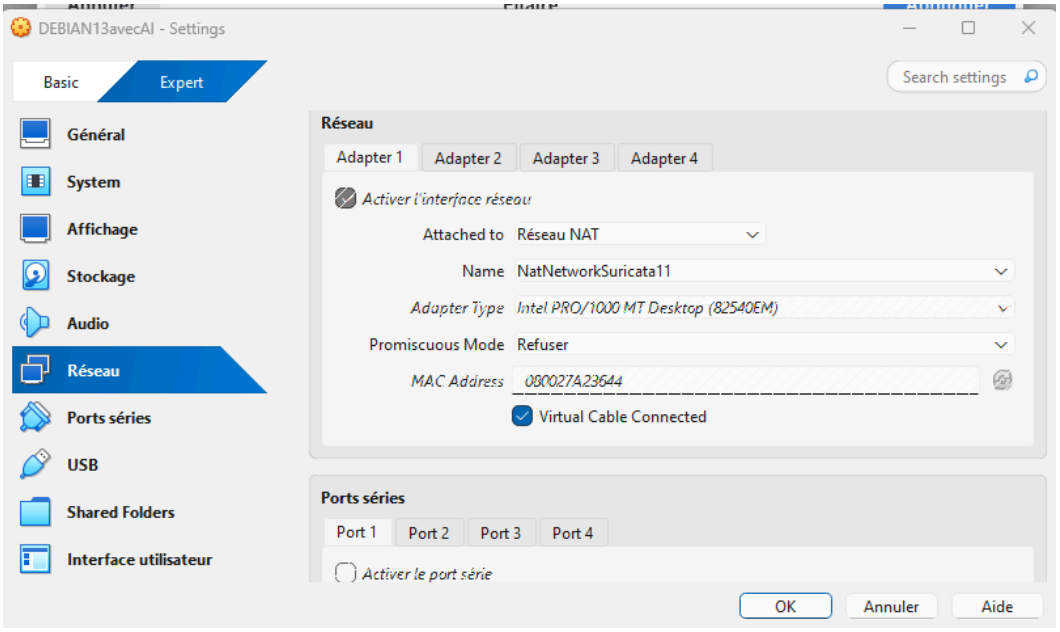
Chapitre 2 - Suricata Partie 2 : Solution SIEM avec la Suite Elastic Stack (Suite ELK)

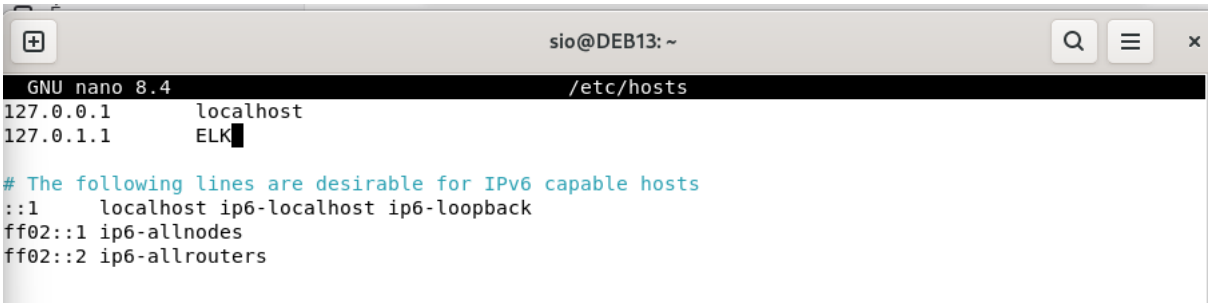
Table des Matières :

1. Les VM.

➢ Une VM Debian 13 nommée Suricata.
➢ Une VM Kali Linux 2025.
➢ Une VM Debian 13 nommée ELK.





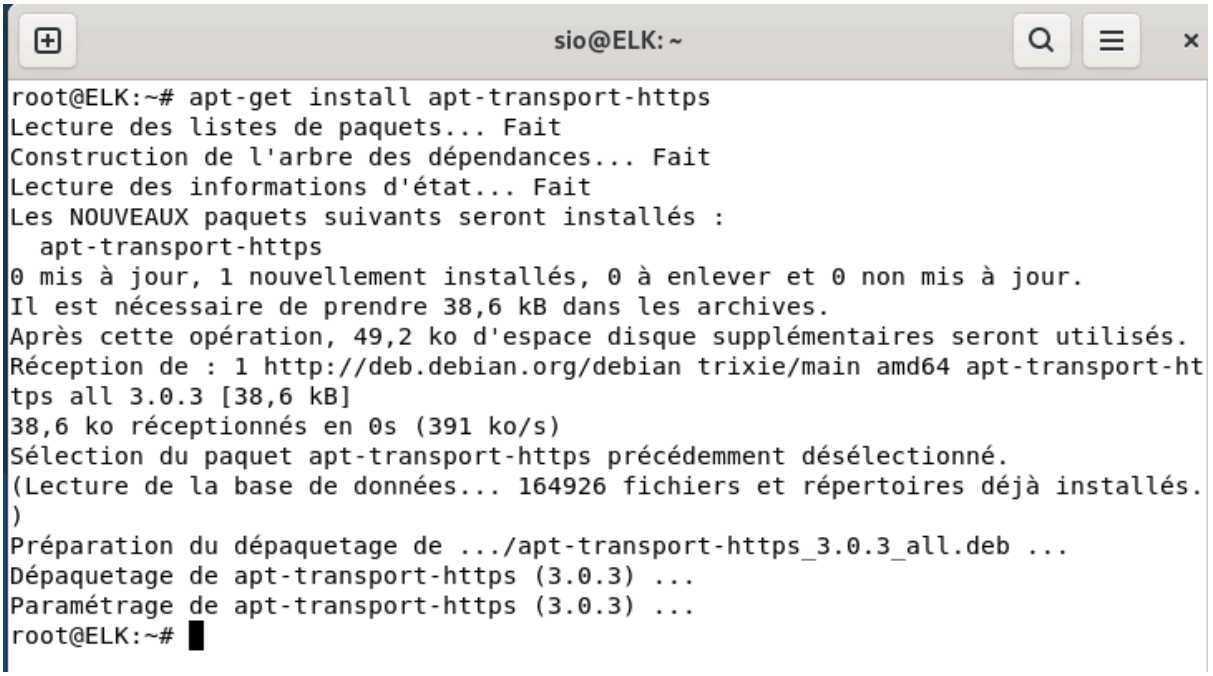

sio@DEB13: ~
GNU nano 8.4 /etc/hosts
127.0.0.1 localhost
127.0.1.1 ELK
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


sio@DEB13: ~
GNU nano 8.4 /etc/hostname
ELK

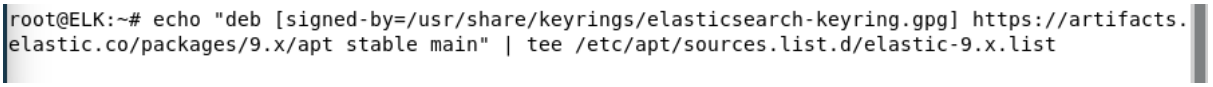
4. Installation d'Elasticsearch et Kibana sur la VM ELK.

▪ Téléchargement et installation de la clé publique GPG d'Elastic :

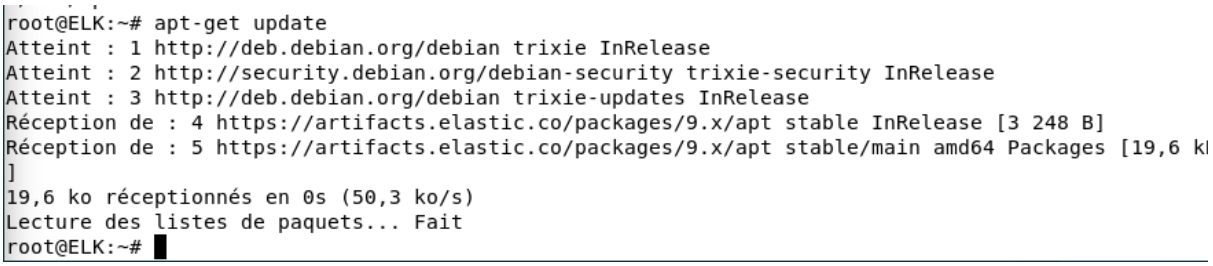
▪ Installation du paquet apt-transport-https :



▪ Nous ajoutons le dépôt de paquets Elastic au répertoire sources.list.d :



▪ Nous mettons à jour nos listes de paquets depuis les différents dépôts y compris les nouveaux paquets Elastic :



▪ Installation de Elasticsearch et Kibana :

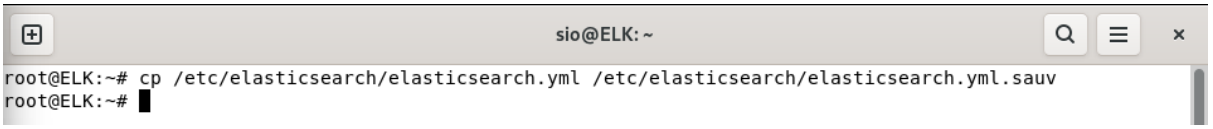
```
sio@ELK: ~
root@ELK:~# apt-get install elasticsearch kibana
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  elasticsearch kibana
0 mis à jour, 2 nouvellement installés, 0 à enlever et 20 non mis à jour.
Il est nécessaire de prendre 1 047 MB dans les archives.
Après cette opération, 2 472 Mo d'espace disque supplémentaires seront utilisés.
Réception de : 1 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 elasticsearch amd64 9.2
.0 [687 MB]
Réception de : 2 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 kibana amd64 9.2.0 [360
 MB]
1 047 Mo réceptionnés en 29s (35,5 Mo/s)
Sélection du paquet elasticsearch précédemment désélectionné.
(Lecture de la base de données... 164930 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../elasticsearch_9.2.0_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Dépaquetage de elasticsearch (9.2.0) ...
Sélection du paquet kibana précédemment désélectionné.
Préparation du dépaquetage de .../kibana_9.2.0_amd64.deb ...
Dépaquetage de kibana (9.2.0) ...
Paramétrage de elasticsearch (9.2.0) ...
```

▪ Nous obtenons la sortie suivante :

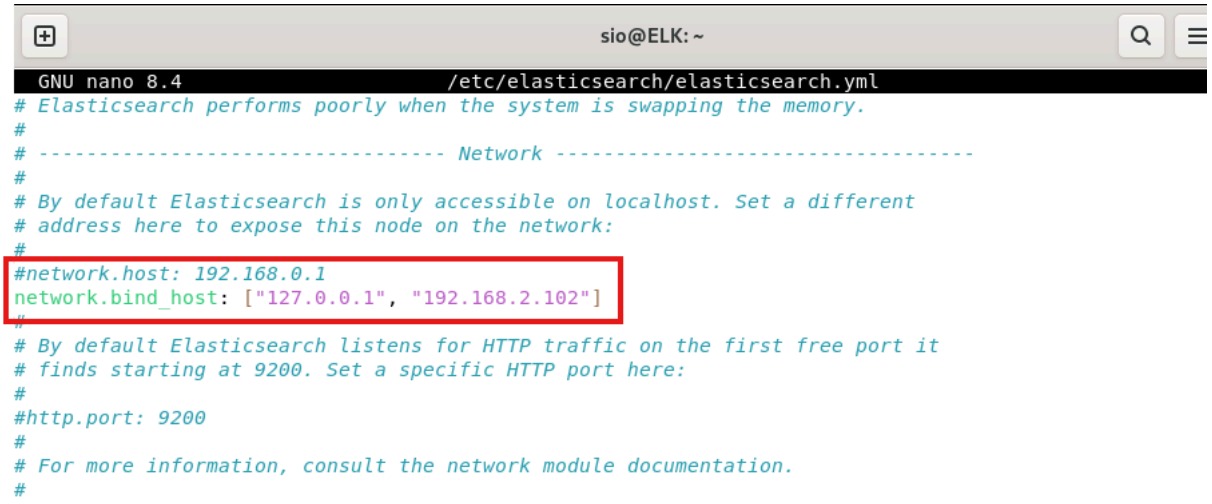
```
-------------------------- Security autoconfiguration information ------------------------------

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : fbvdrekbZy9hIO0X+4Wk

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------------------------
### NOT starting on installation, please execute the following statements to configure elasticsearch ser
vice to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Paramétrage de kibana (9.2.0) ...
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
Traitement des actions différées (« triggers ») pour procps (2:4.0.4-9) ...
Traitement des actions différées (« triggers ») pour systemd (257.8-1~deb13u2) ...
root@ELK:~#
```

MDP Elastic :
fbvdrekbZy9hI00X+4Wk

▪ Nous effectuons une sauvegarde du fichier de configuration yaml d'Elasticsearch :

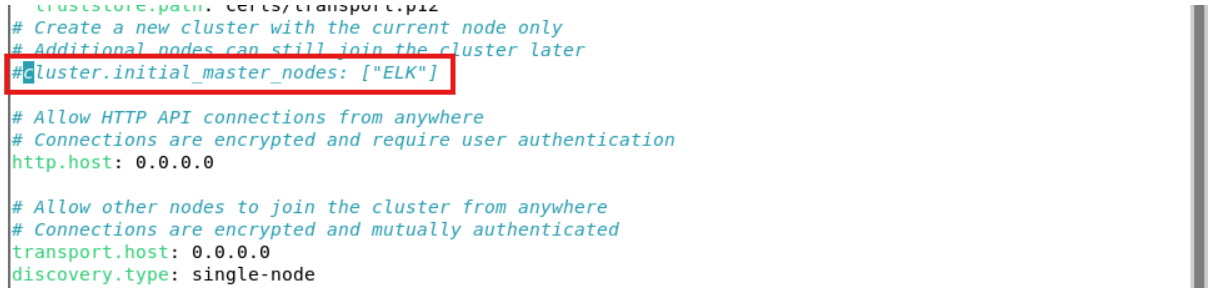


▪ Nous décommentons la ligne #network.host : 192.168.0.1 et nous remplaçons l'adresse par défaut par 0.0.0.0. Nous ajoutons la ligne encadrée ci-après :

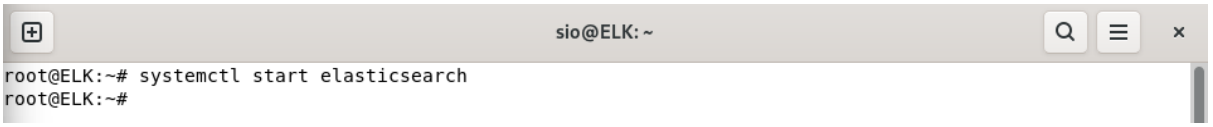


▪ Nous décommentons la ligne #transport.host : 0.0.0.0 et nous ajoutons la ligne discovery.type : single-node :

▪ Nous veillez à ce que la ligne #cluster.initial_master_nodes : [« ELK »] soit commentée.

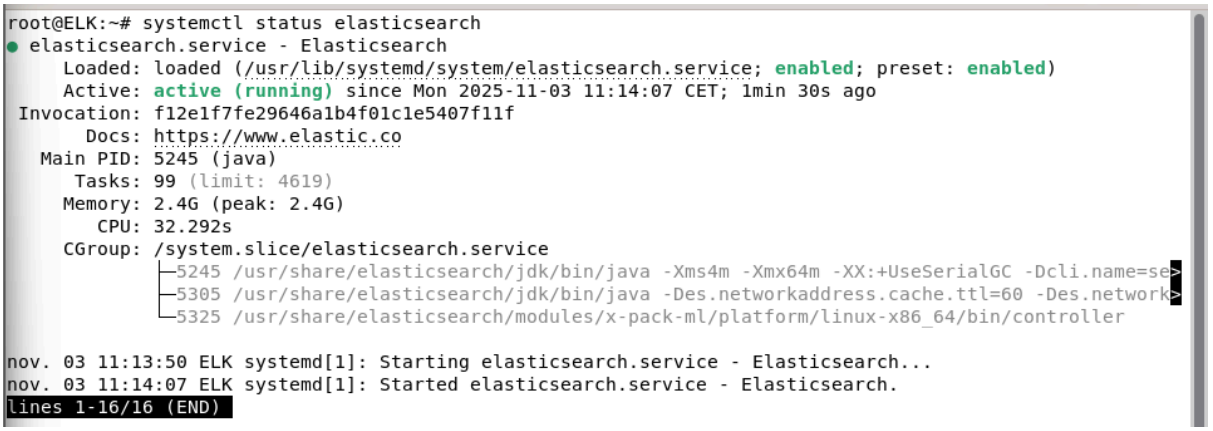


Démarrage du service Elasticsearch avec systemctl :

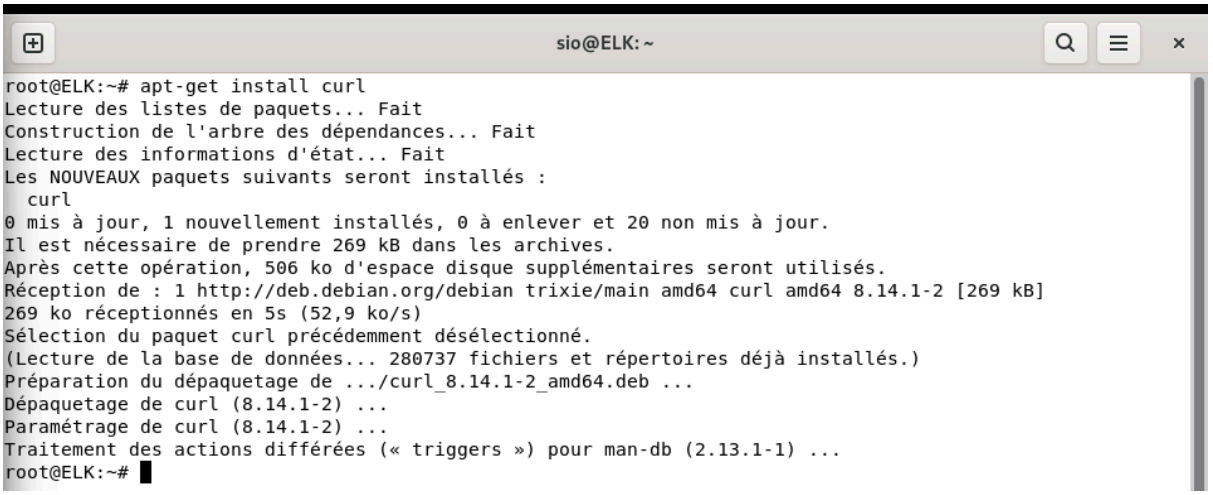


Nous permettons à Elasticsearch de démarrer automatiquement à chaque redémarrage de la machine :

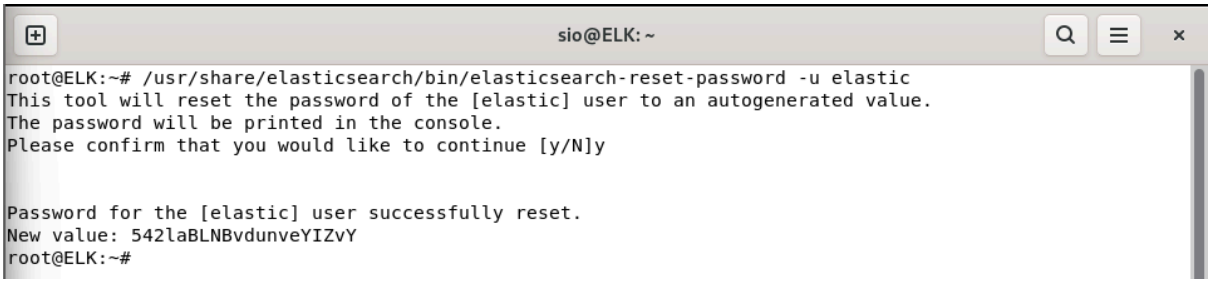
▪ Nous vérifions l'état du service :



▪ Installation du paquet curl :

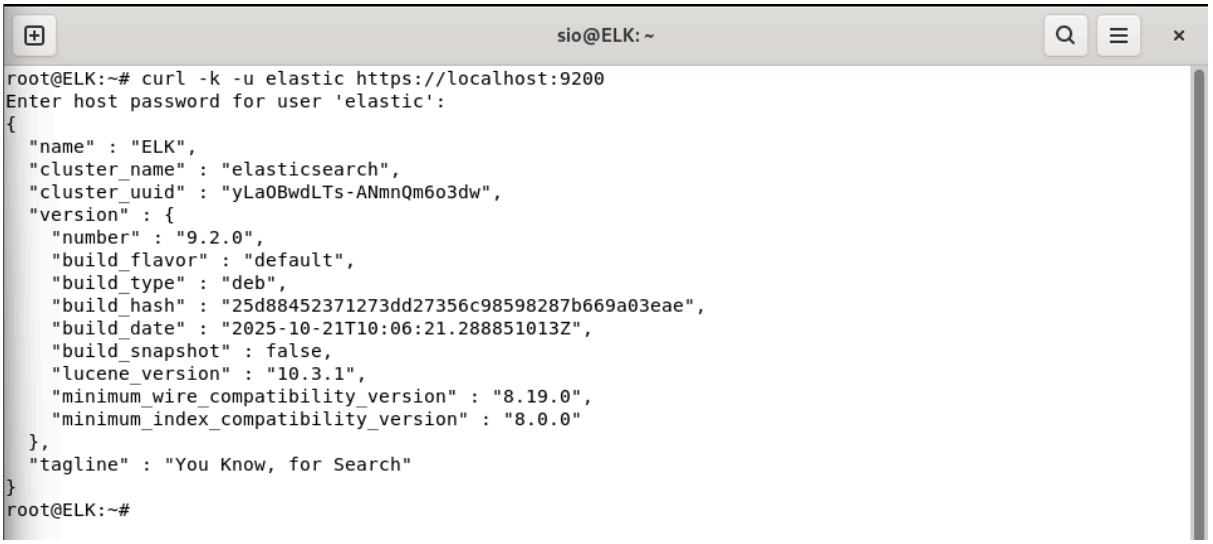


▪ Possibilité de modifier le mot de passe du superutilisateur d'Elasticsearch :

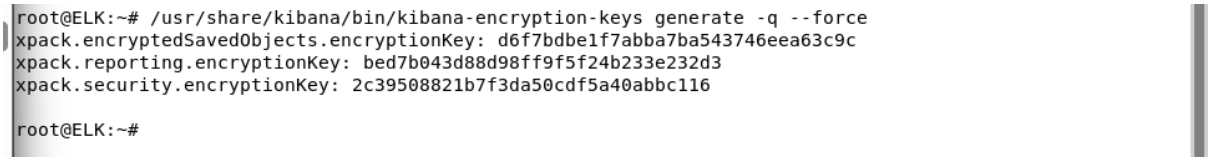


MDP :
542laBLNBvdunveYIZvY

▪ Nous vérifions si Elasticsearch répond aux requêtes https sur le port 9200 :

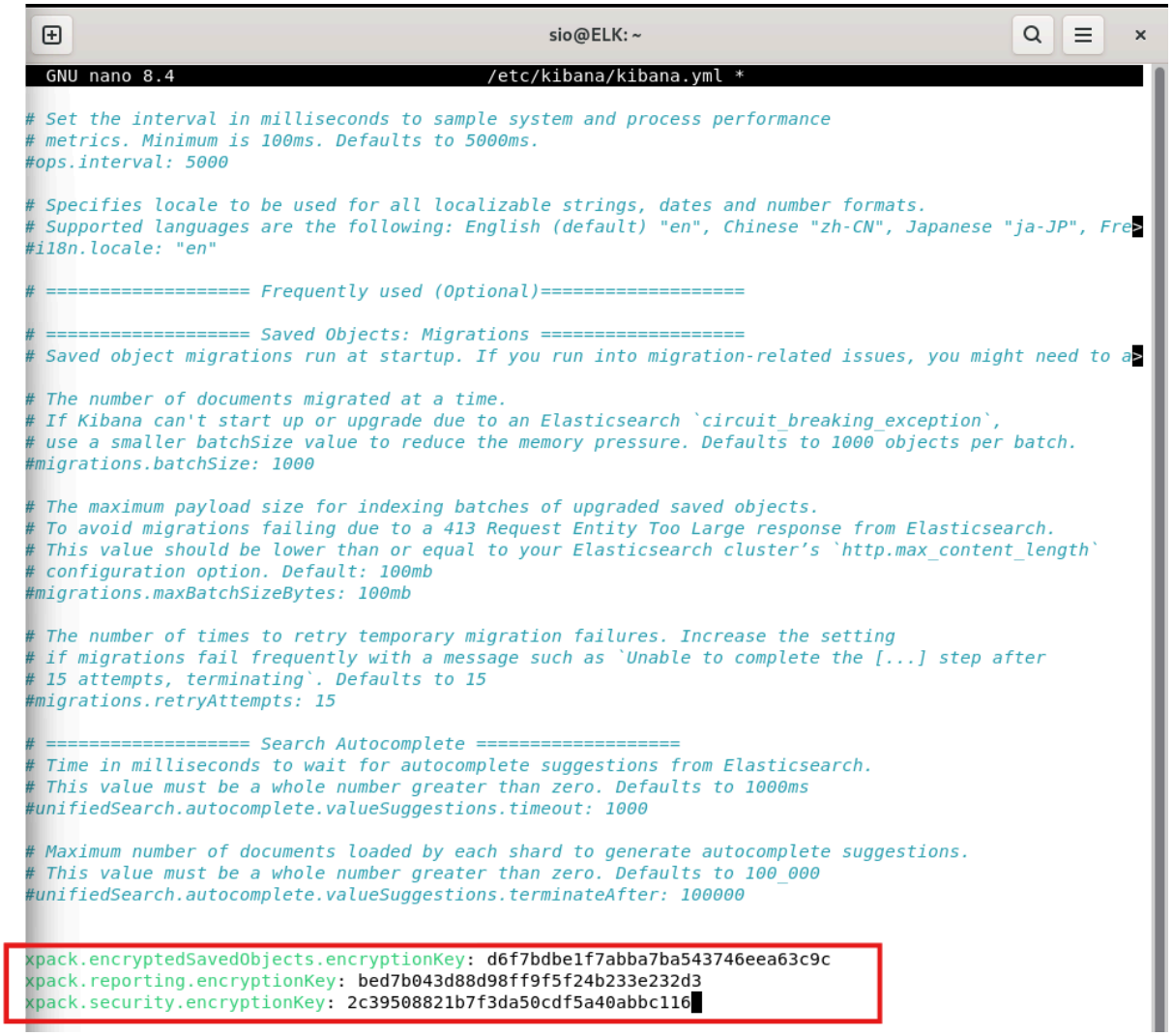


▪ Configuration KIBANA



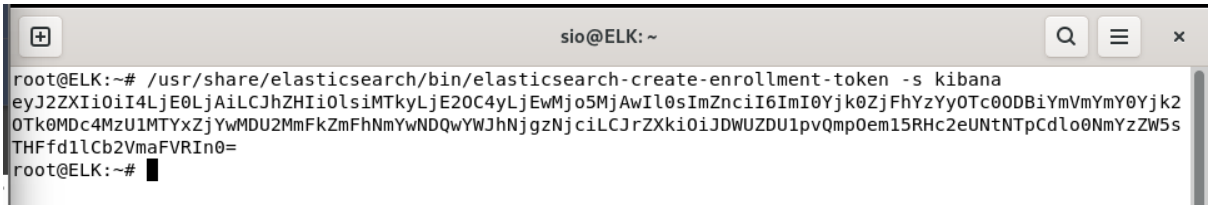
xpack.encryptedSavedObjects.encryptionKey: d6f7bdbe1f7abba7ba543746eea63c9c
xpack.reporting.encryptionKey: bed7b043d88d98ff9f5f24b233e232d3
xpack.security.encryptionKey: 2c39508821b7f3da50cdf5a40abbc116

▪ Nous collons la configuration qui a été donnée à la fin du fichier de configuration kibana.yml :



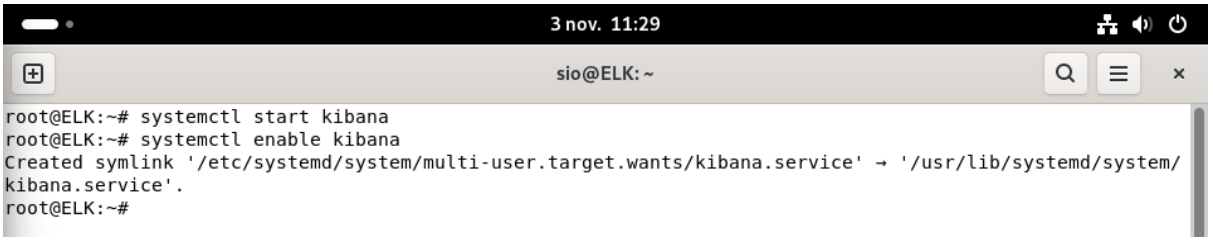
▪ Nous configurons Kibana pour être accessible sur l'adresse IP privée du serveur :

▪ Nous configutons l'accès à Kibana en générant un jeton d'inscription qui servira pour se connecter à l'interface web de Kibana :

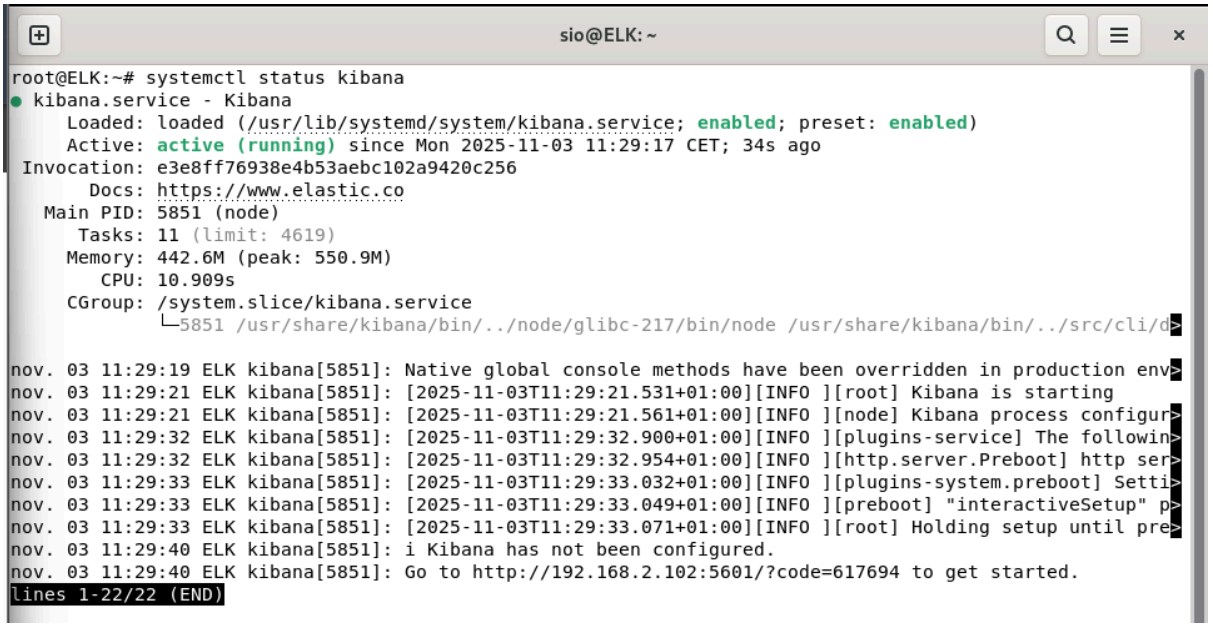


Copiez/collez la sortie sur votre document :
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC4yLjEwMjo5MjAwIl0sImZnciI6ImI0Yjk0ZjFhYzYyOTc0ODBiYmVmYmY0Yjk2OTk0MDc4MzU1MTYxZjYwMDU2MmFkZmFhNmYwNDQwYWJhNjgzNjciLCJrZXkiOiJDWUZDU1pvQmpOem15RHc2eUNtNTpCdlo0NmYzZW5sTHFfd1lCb2VmaFVRIn0=

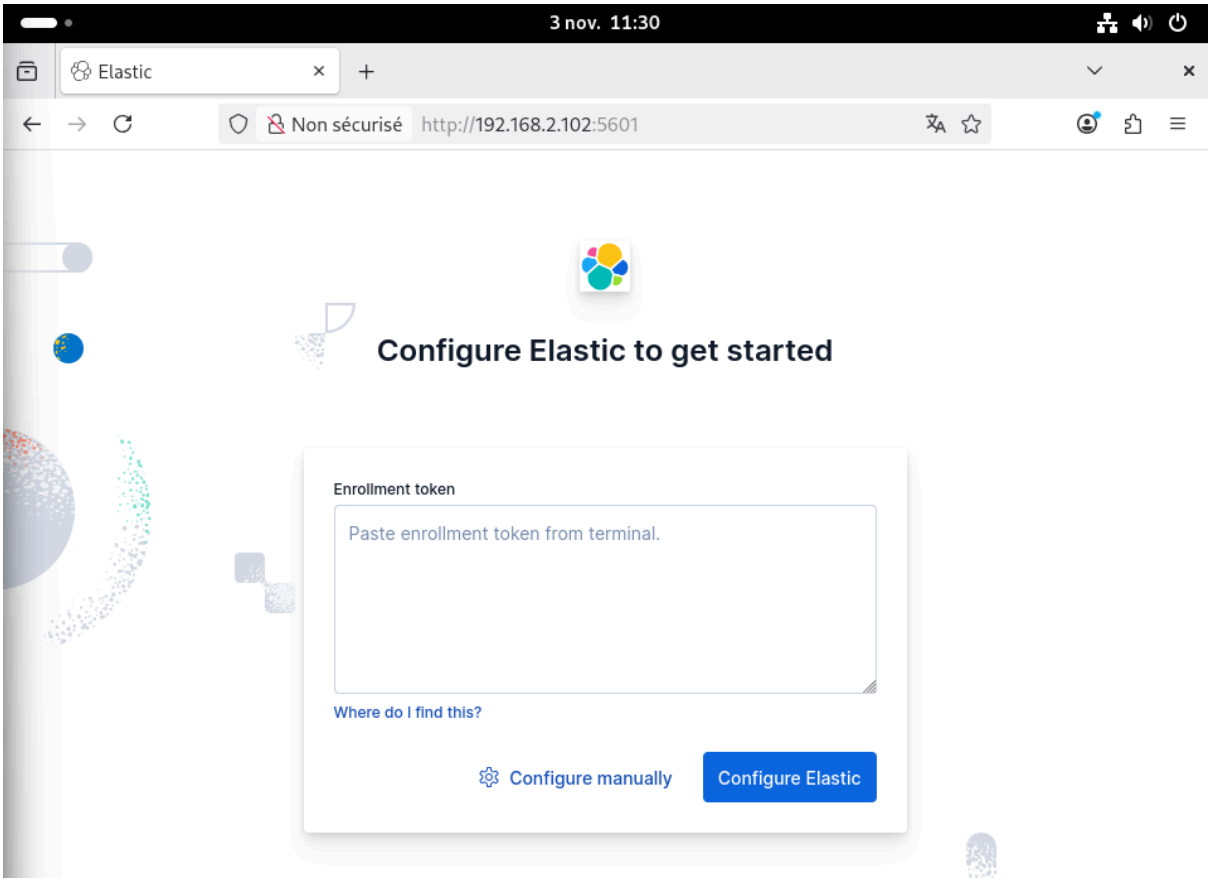
Nous démarrons et activons le service Kibana :



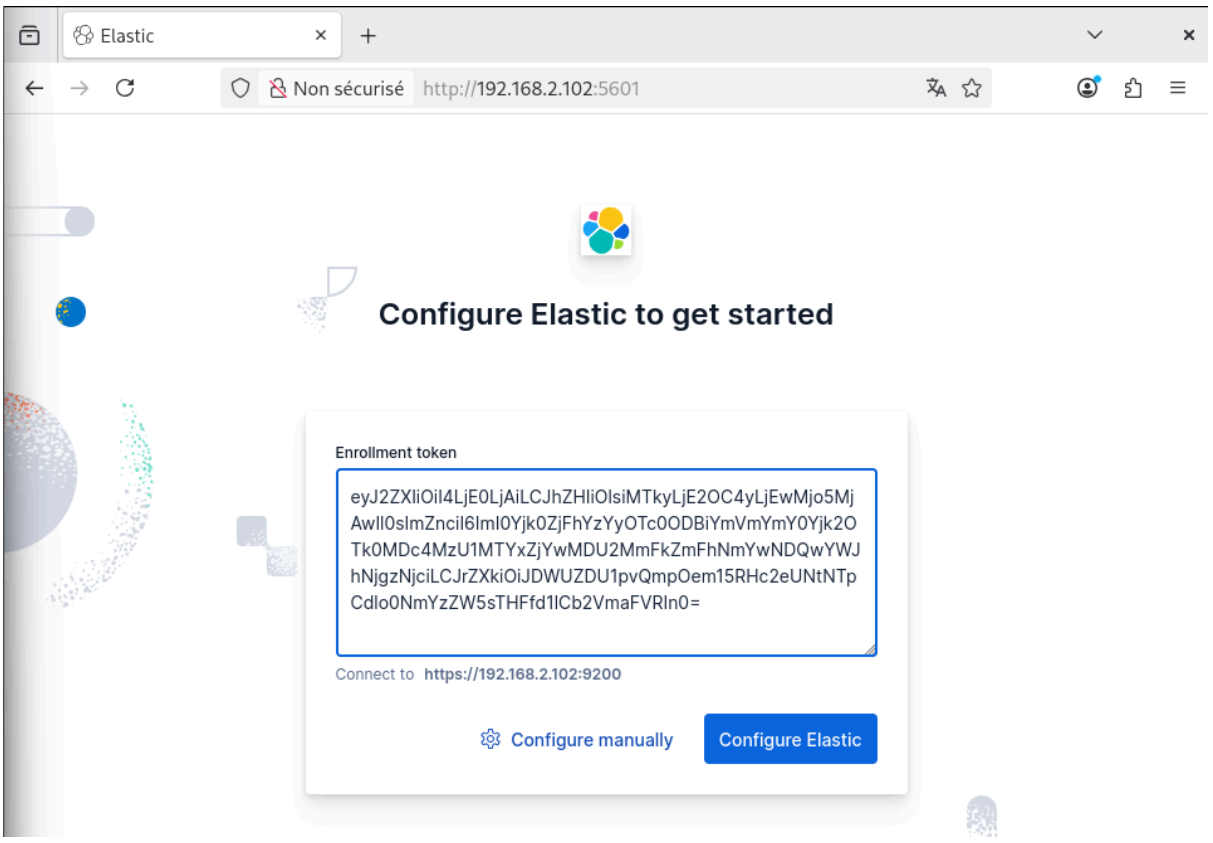
▪ Vérification de son état :



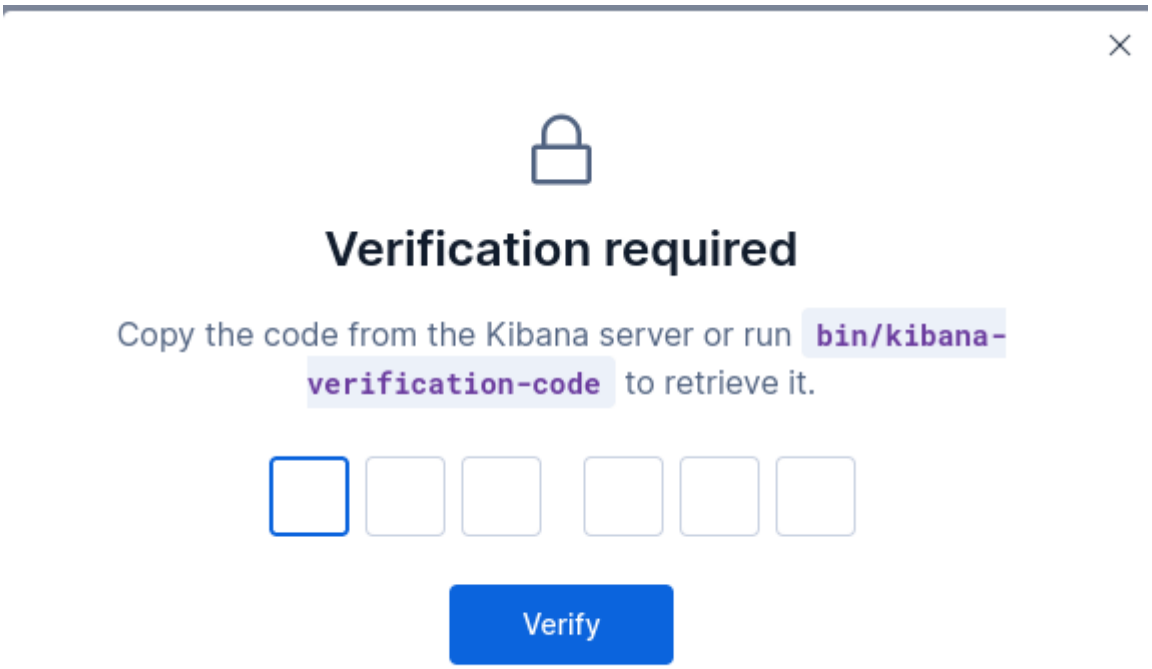
▪ Nous accédons à la page de Kibana :



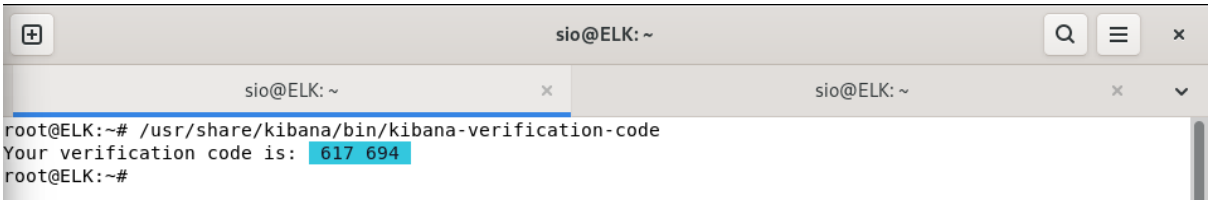
▪ Nous collons le jeton d'inscription et cliquons sur Configure Elastic :

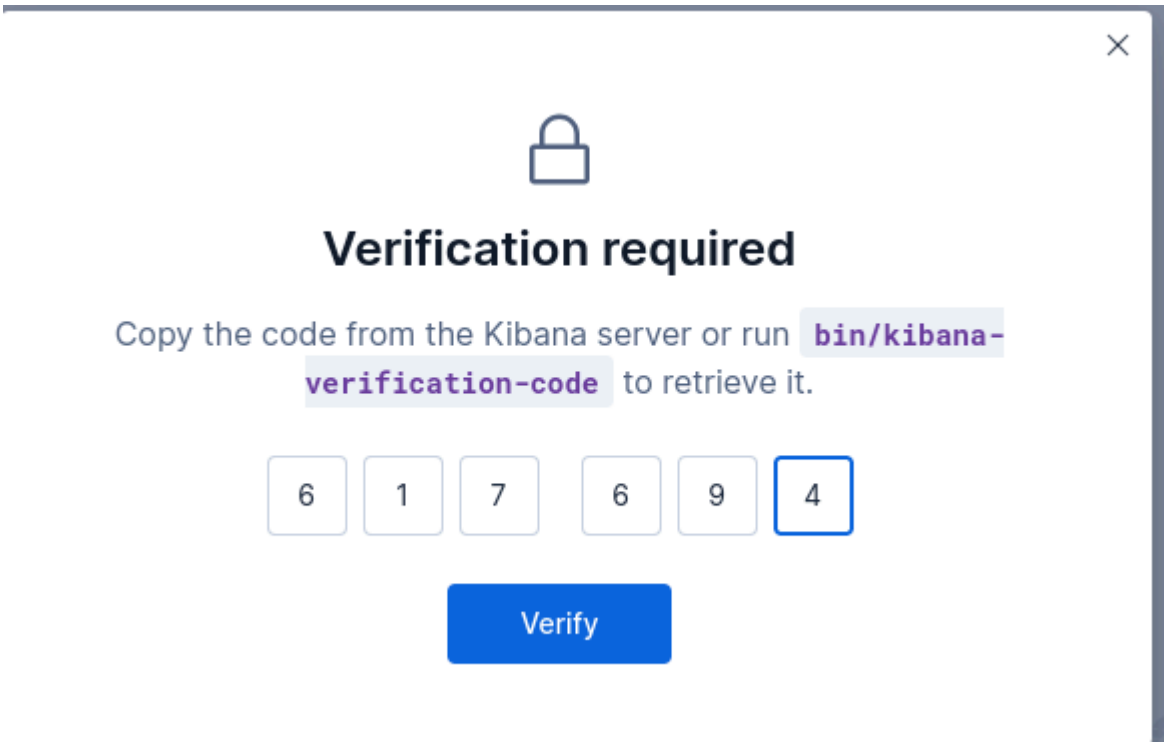


▪ Un code de vérification nous est demandé :

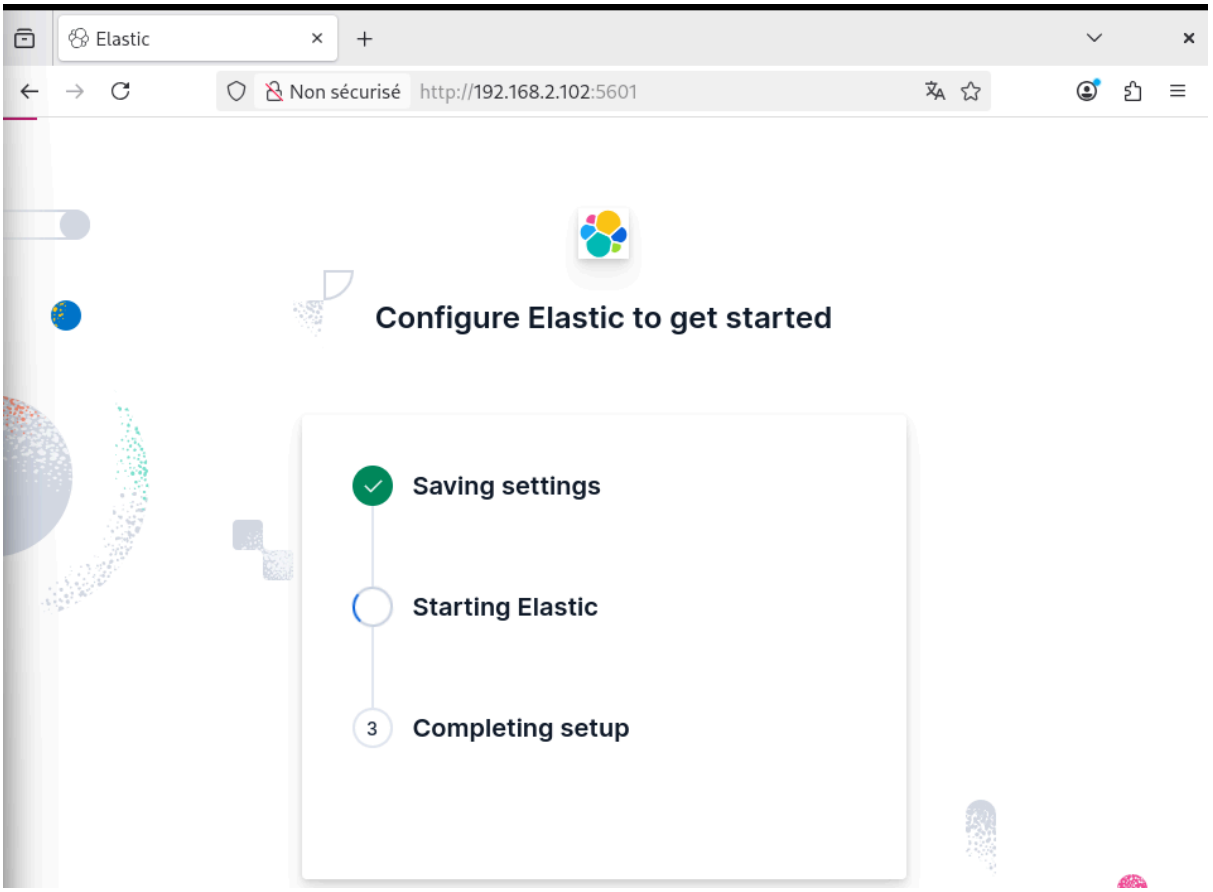


▪ Nous générons le code et nous l'entrons :

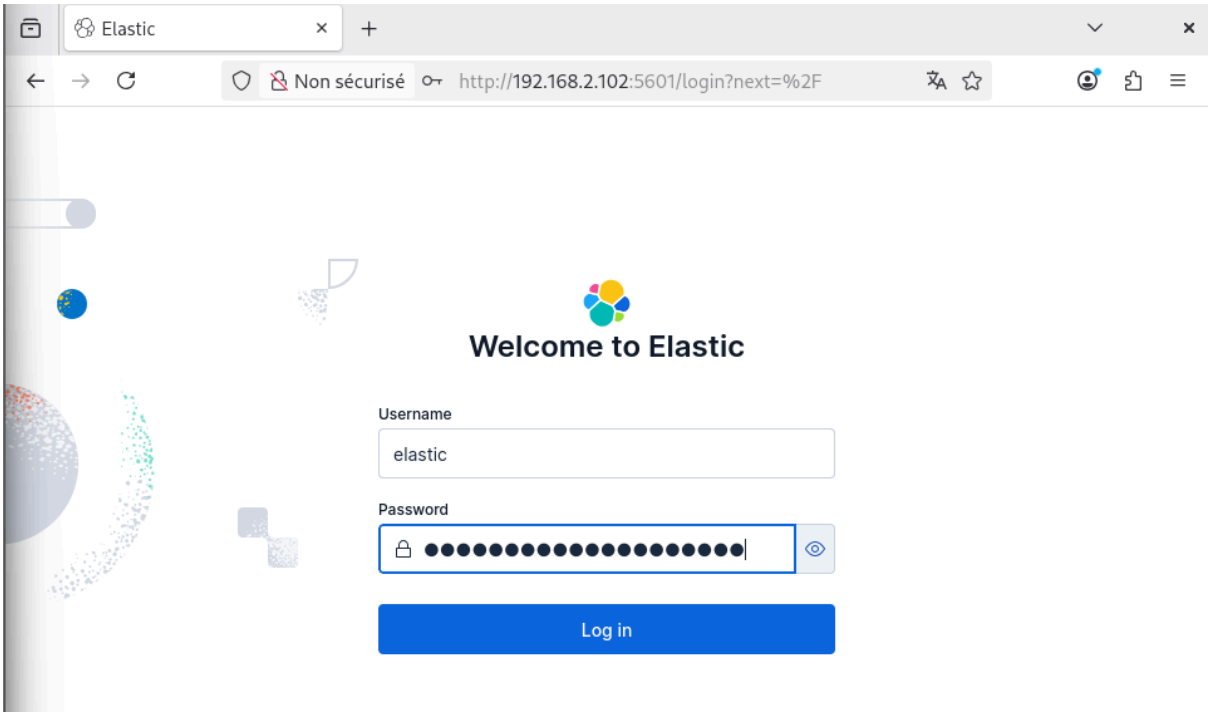


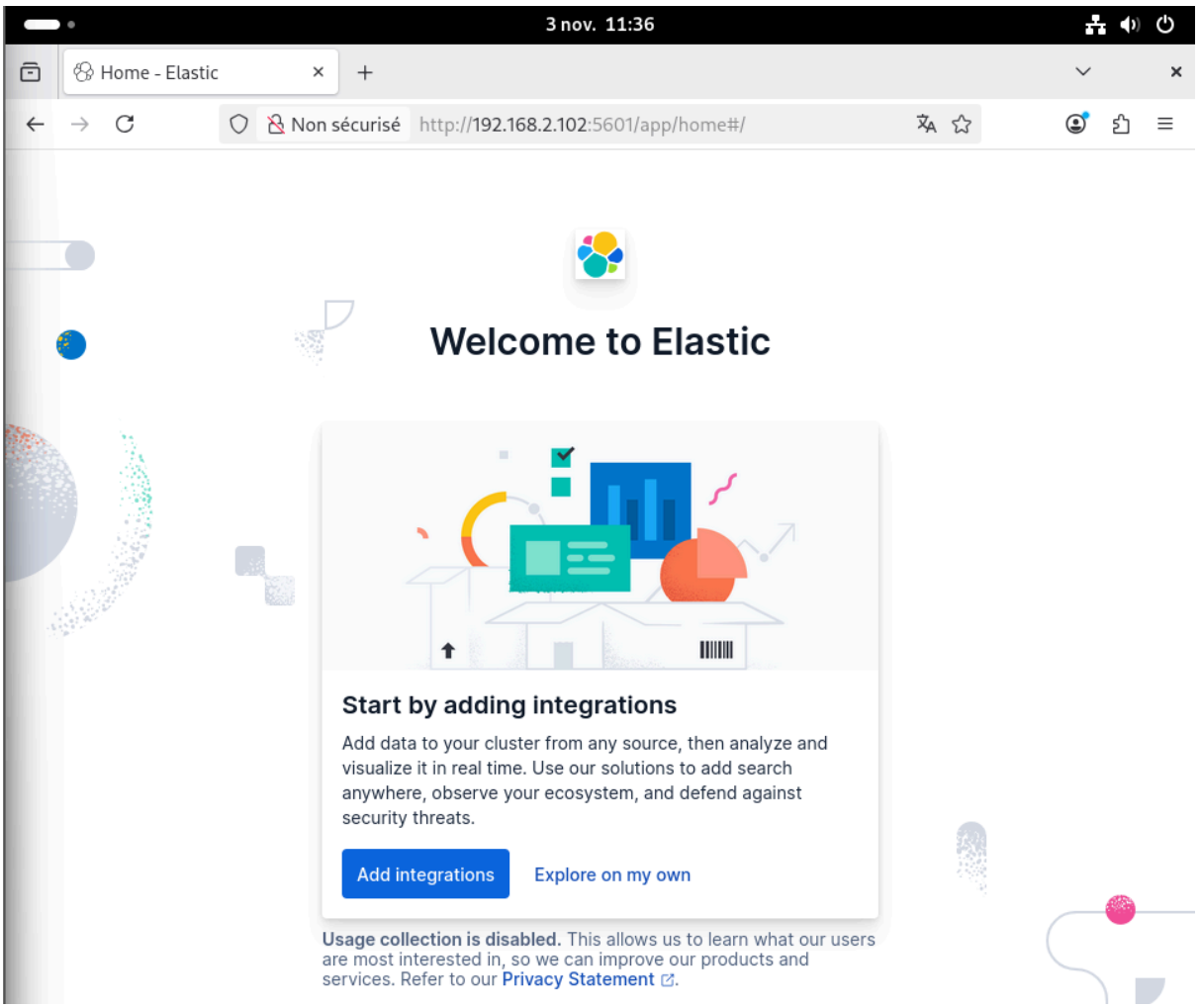


▪ Nous attendons que la configuration d'Elastic se termine :



▪ Nous nous connectons avec l'utilisateur elastic et le mot de passe que nous avions regénéré auparavant :




3 nov. 11:36
Home - Elastic
Non sécurisé
http://192.168.2.102:5601/app/home#/
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.
Add integrations
Explore on my own
Usage collection is disabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement.

5. Installation de Filebeat sur la VM Suricata.

▪ Nous téléchargeons et installons la clé publique GPG d'Elastic :

```
root@Suricata:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --dearmor -o /usr
/share/keyrings/elasticsearch-keyring.gpg
```

▪ Ajout du dépôt Elastic au répertoire sources.list.d :

```
sio@Suricata: ~
root@Suricata:~# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts
.elastic.co/packages/9.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-9.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.
x/apt stable main
root@Suricata:~#
```

▪ Mise à jour de la liste des paquets téléchargeables :

```
sio@Suricata: ~
root@Suricata:~# apt-get update
Réception de : 1 http://security.debian.org/debian-security trixie-security InRelease [43,4 kB]
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Réception de : 4 https://artifacts.elastic.co/packages/9.x/apt stable InRelease [3 248 B]
Réception de : 5 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 Packages [19,6 kB]
66,3 ko réceptionnés en 0s (291 ko/s)
Lecture des listes de paquets... Fait
root@Suricata:~#
```

▪ Installation de Filebeat :

```
sio@Suricata: ~
root@Suricata:~# apt-get install filebeat
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  filebeat
0 mis à jour, 1 nouvellement installés, 0 à enlever et 19 non mis à jour.
Il est nécessaire de prendre 67,0 MB dans les archives.
Après cette opération, 257 Mo d'espace disque supplémentaires seront utilisés.
Réception de : 1 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 filebeat amd64 9.2.0
[67,0 MB]
67,0 Mo réceptionnés en 2s (35,7 Mo/s)
Sélection du paquet filebeat précédemment désélectionné.
(Lecture de la base de données... 145215 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../filebeat_9.2.0_amd64.deb ...
Dépaquetage de filebeat (9.2.0) ...
Paramétrage de filebeat (9.2.0) ...
root@Suricata:~#
```

▪ Copie du fichier http_ca.crt du serveur Elasticsearch dans le répertoire /etc/filebeat/ :

```
sio@Suricata: ~
root@Suricata:~# scp root@192.168.2.102:/etc/elasticsearch/certs/http_ca.crt /etc/
filebeat
root@192.168.2.102's password:
http_ca.crt                                   100% 1939   407.4KB/s   00:00
root@Suricata:~#
```

▪ Section Kibana du fichier de configuration de Filebeat :

```
sio@Suricata: ~
  GNU nano 8.4                    /etc/filebeat/filebeat.yml
#  env: staging

# ================================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here or by using the `setup` command.
#setup.dashboards.enabled: false

# The URL from where to download the dashboard archive. By default, this URL
# has a value that is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:

# =================================== Kibana ========================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"
host: "192.168.2.102:5601"
protocol: "http"
ssl.enabled: true
ssl.certificate_authorities: ["/etc/filebeat/http_ca.crt"]
```

▪ Section Elasticsearch Output :

```
# ================================== Outputs ========================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.2.102:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "542laBLNBvdunveYIZvY"
  ssl.certificate_authorities: ["/etc/filebeat/http_ca.crt"]
  ssl.verification_mode: full
```

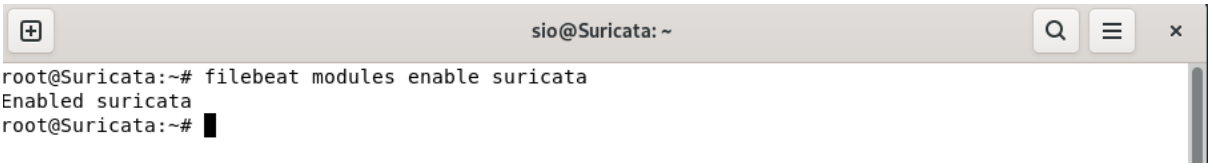
- Ajout de la ligne suivante à la fin du fichier :

```
# ================================== Migration =================================

# This allows to enable 6.7 migration aliases
#migration.6_to_7.enabled: true

setup.ilm.overwrite: true
```

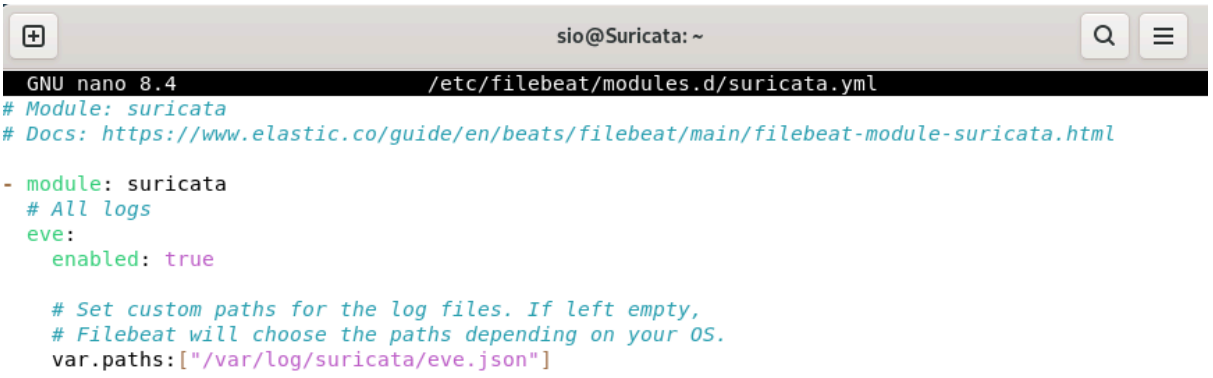
- Test de la connexion avec le serveur Elasticsearch :

```
sio@Suricata: ~
root@Suricata:~# curl -v --cacert /etc/filebeat/http_ca.crt https://192.168.2.102:9200 -u elastic
Enter host password for user 'elastic':
*   Trying 192.168.2.102:9200...
* ALPN: curl offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
*  CAfile: /etc/filebeat/http_ca.crt
*  CApath: /etc/ssl/certs
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / x25519 / RSASSA-PSS
* ALPN: server did not agree on a protocol. Uses default.
* Server certificate:
*  subject: CN=ELK
*  start date: Nov  3 10:03:36 2025 GMT
*  expire date: Nov  3 10:03:36 2027 GMT
*  subjectAltName: host "192.168.2.102" matched cert's IP address!
*  issuer: CN=Elasticsearch security auto-configuration HTTP CA
*  SSL certificate verify ok.
*   Certificate level 0: Public key type RSA (4096/152 Bits/secBits), signed using sha256WithRSAEnc
ryption
*   Certificate level 1: Public key type RSA (4096/152 Bits/secBits), signed using sha256WithRSAEnc
ryption
* Connected to 192.168.2.102 (192.168.2.102) port 9200
* using HTTP/1.x
* Server auth using Basic with user 'elastic'
> GET / HTTP/1.1
> Host: 192.168.2.102:9200
> Authorization: Basic ZWxhc3RpYzo1NDJsYUJMTkJ2ZHVudmVZSVp2WQ==
> User-Agent: curl/8.14.1
> Accept: */*
>
* Request completely sent off
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* Request completely sent off
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
< HTTP/1.1 200 OK
< X-elastic-product: Elasticsearch
< content-type: application/json
< content-length: 527
<
{
  "name" : "ELK",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "yLaOBwdLTs-ANmnQm6o3dw",
  "version" : {
    "number" : "9.2.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "25d88452371273dd27356c98598287b669a03eae",
    "build_date" : "2025-10-21T10:06:21.288851013Z",
    "build_snapshot" : false,
    "lucene_version" : "10.3.1",
    "minimum_wire_compatibility_version" : "8.19.0",
    "minimum_index_compatibility_version" : "8.0.0"
  },
  "tagline" : "You Know, for Search"
}
* Connection #0 to host 192.168.2.102 left intact
root@Suricata:~#
```

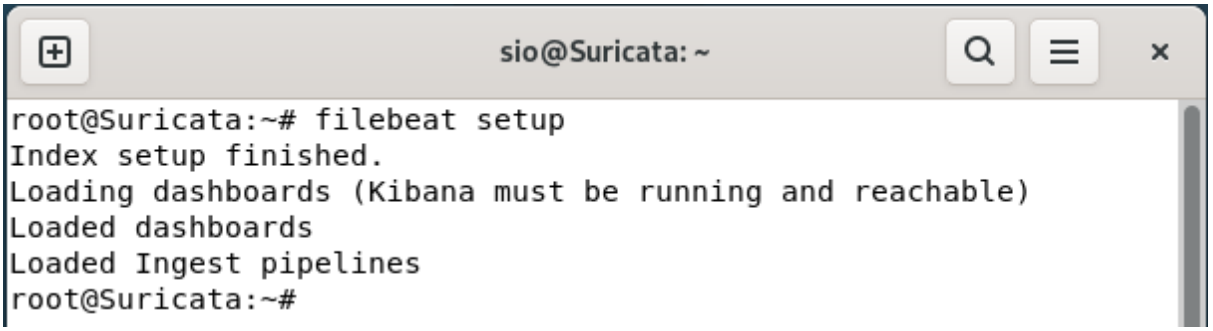
▪ Activation du module Suricata intégré de Filebeat :



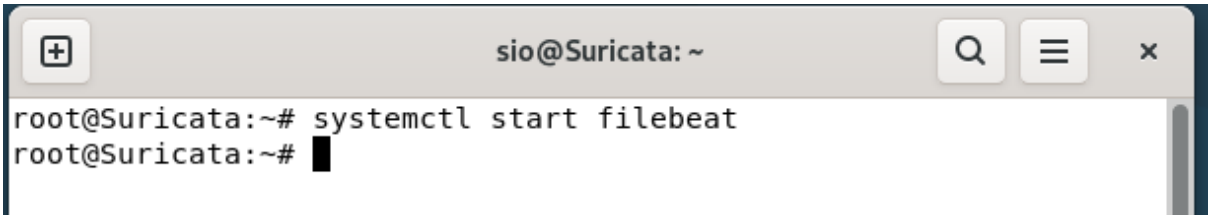
▪ Nous changeons la valeur de la variable enabled, nous devons décommenter var.paths et y spécifier le fichier de log de suricata :

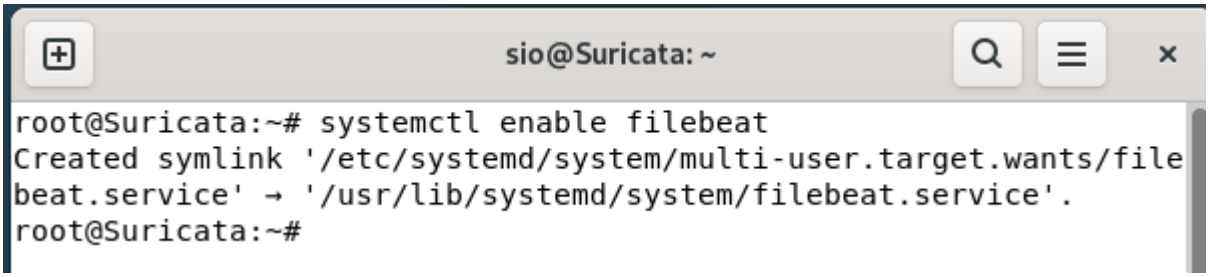


▪ Changement des tableaux de bord et les pipelines SIEM dans Elasticsearch à l'aide de la commande filebeat setup :

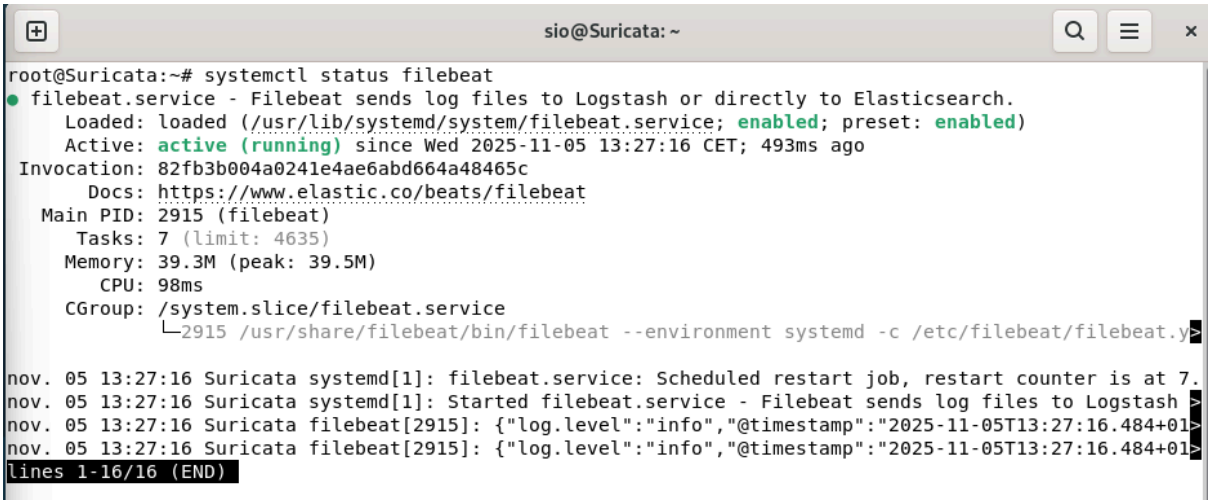


▪ Nous démarrons le service Filebeat :

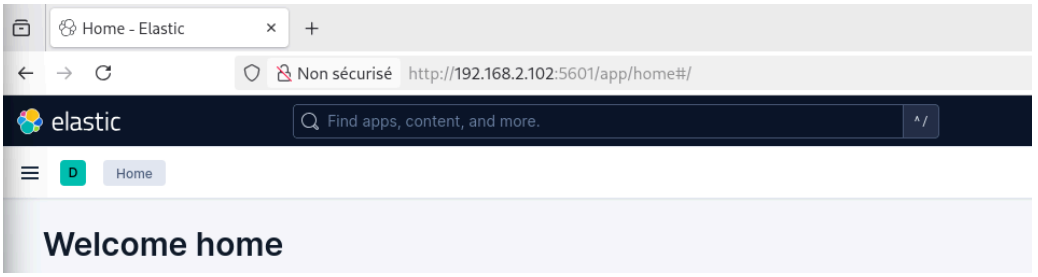




▪ Nous vérifions l'état du service :



▪ Nous accédons à Kibana :



▪ Nous tapons type:dashboard suricata dans la barre de recherche en haut pour localiser les informations sur Suricata :