

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

## Table des Matières :

1. Les VM.....	2
4. Installation d'Elasticsearch et Kibana sur la VM ELK.....	4
5. Installation de Filebeat sur la VM Suricata.....	16

# 1. Les VM.

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

**Annuler** **Filaire** **Appliquer**

Détails Identité **IPv4** IPv6 Sécurité

**Méthode IPv4**

Automatique (DHCP)  Réseau local seulement

Manuel  Désactiver

Partagée avec d'autres ordinateurs

**Adresses**

Adresse	Masque de réseau	Passerelle	
192.168.2.102	255.255.255.0	192.168.2.1	✕
			✕

**DNS** Automatique

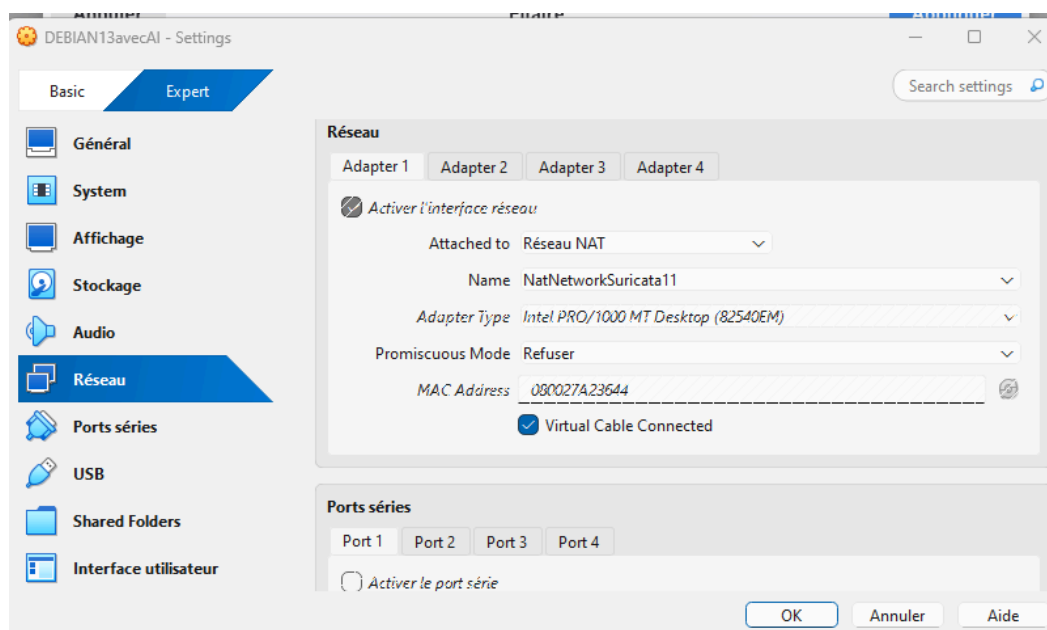
172.17.254.1

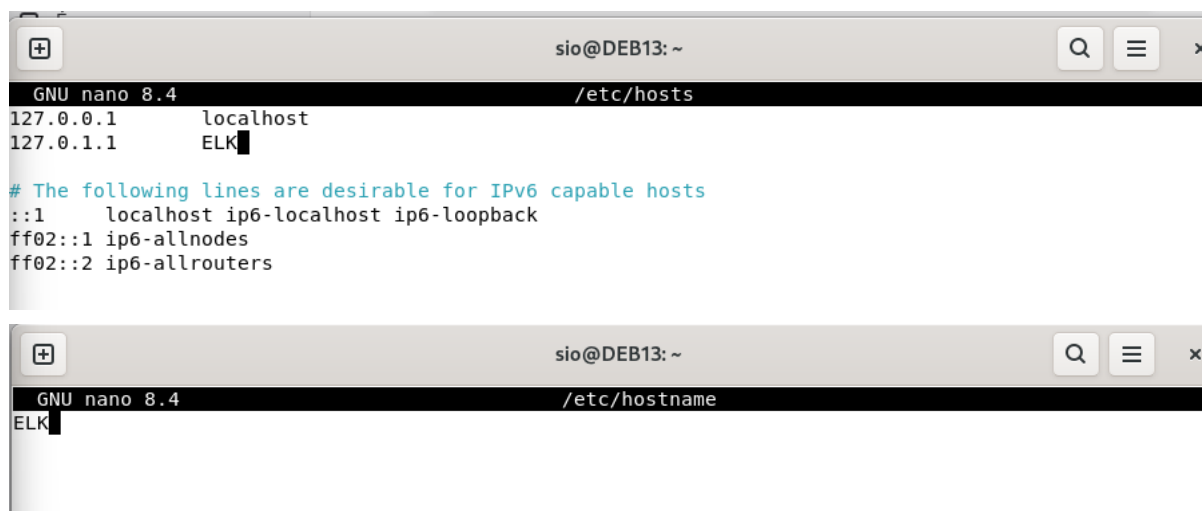
Séparer les adresses IP avec des virgules

**Routes** Automatique

Adresse	Masque de réseau	Passerelle	Métrieque	
				✕

N'utiliser cette connexion que pour les ressources sur ce réseau





The image displays two terminal windows from a Linux system. The top window shows the nano text editor editing the /etc/hosts file. The content includes IPv4 localhost entries, an IPv4 entry for 'ELK', and IPv6 localhost and allnodes/allrouters entries. The bottom window shows the nano text editor editing the /etc/hostname file, with 'ELK' entered as the system's hostname.

```
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 :

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

- Installation du paquet apt-transport-https :

```
sio@ELK: ~  
root@ELK:~# apt-get install apt-transport-https  
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 :  
  apt-transport-https  
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.  
Il est nécessaire de prendre 38,6 kB dans les archives.  
Après cette opération, 49,2 ko d'espace disque supplémentaires seront utilisés.  
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 apt-transport-https all 3.0.3 [38,6 kB]  
38,6 ko réceptionnés en 0s (391 ko/s)  
Sélection du paquet apt-transport-https précédemment désélectionné.  
(Lecture de la base de données... 164926 fichiers et répertoires déjà installés.)  
Préparation du dépaquetage de .../apt-transport-https_3.0.3_all.deb ...  
Dépaquetage de apt-transport-https (3.0.3) ...  
Paramétrage de apt-transport-https (3.0.3) ...  
root@ELK:~#
```

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

```
root@ELK:~# 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
```

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

```
root@ELK:~# apt-get update  
Atteint : 1 http://deb.debian.org/debian trixie InRelease  
Atteint : 2 http://security.debian.org/debian-security trixie-security 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 kiB]  
19,6 ko réceptionnés en 0s (50,3 ko/s)  
Lecture des listes de paquets... Fait  
root@ELK:~#
```

- 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 : fbvdrekBZy9hI00X+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 :

```
sio@ELK: ~  
root@ELK:~# cp /etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/elasticsearch.yml.sauv  
root@ELK:~#
```

- 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 :

```
sio@ELK: ~  
GNU nano 8.4 /etc/elasticsearch/elasticsearch.yml  
# Elasticsearch performs poorly when the system is swapping the memory.  
#  
# ----- Network -----  
#  
# By default Elasticsearch is only accessible on localhost. Set a different  
# address here to expose this node on the network:  
#  
#network.host: 192.168.0.1  
network.bind_host: ["127.0.0.1", "192.168.2.102"]  
#  
# By default Elasticsearch listens for HTTP traffic on the first free port it  
# finds starting at 9200. Set a specific HTTP port here:  
#  
#http.port: 9200  
#  
# For more information, consult the network module documentation.  
#
```

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

```
# Allow other nodes to join the cluster from anywhere  
# Connections are encrypted and mutually authenticated  
transport.host: 0.0.0.0  
discovery.type: single-node
```

- Nous veillons à ce que la ligne `#cluster.initial_master_nodes : [« ELK »]` soit commentée.

```
cluster.initial_master_nodes: ["ELK"]  
# Create a new cluster with the current node only  
# Additional nodes can still join the cluster later  
# Allow HTTP API connections from anywhere  
# Connections are encrypted and require user authentication  
http.host: 0.0.0.0  
# Allow other nodes to join the cluster from anywhere  
# Connections are encrypted and mutually authenticated  
transport.host: 0.0.0.0  
discovery.type: single-node
```

Démarrage du service Elasticsearch avec `systemctl` :

```
sio@ELK: ~  
root@ELK:~# systemctl start elasticsearch  
root@ELK:~#
```

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

```
sio@ELK: ~  
root@ELK:~# systemctl daemon-reload  
root@ELK:~# systemctl enable elasticsearch  
Created symlink '/etc/systemd/system/multi-user.target.wants/elasticsearch.service' → '/usr/lib/systemd/system/elasticsearch.service'.  
root@ELK:~#
```

▪ Nous vérifions l'état du service :

```
root@ELK:~# systemctl status elasticsearch  
● elasticsearch.service - Elasticsearch  
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)  
   Active: active (running) since Mon 2025-11-03 11:14:07 CET; 1min 30s ago  
 Invocation: f12e1f7fe29646a1b4f01c1e5407f11f  
    Docs: https://www.elastic.co  
   Main PID: 5245 (java)  
    Tasks: 99 (limit: 4619)  
  Memory: 2.4G (peak: 2.4G)  
     CPU: 32.292s  
   CGroup: /system.slice/elasticsearch.service  
           └─5245 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=se  
             └─5305 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.network  
               └─5325 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller  
  
nov. 03 11:13:50 ELK systemd[1]: Starting elasticsearch.service - Elasticsearch...  
nov. 03 11:14:07 ELK systemd[1]: Started elasticsearch.service - Elasticsearch.  
lines 1-16/16 (END)
```

▪ Installation du paquet curl :

```
sio@ELK: ~  
root@ELK:~# apt-get install curl  
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 :  
  curl  
0 mis à jour, 1 nouvellement installés, 0 à enlever et 20 non mis à jour.  
Il est nécessaire de prendre 269 kB dans les archives.  
Après cette opération, 506 ko d'espace disque supplémentaires seront utilisés.  
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 curl amd64 8.14.1-2 [269 kB]  
269 ko réceptionnés en 5s (52,9 ko/s)  
Sélection du paquet curl précédemment désélectionné.  
(Lecture de la base de données... 280737 fichiers et répertoires déjà installés.)  
Préparation du dépaquetage de .../curl_8.14.1-2_amd64.deb ...  
Dépaquetage de curl (8.14.1-2) ...  
Paramétrage de curl (8.14.1-2) ...  
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...  
root@ELK:~#
```

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

```
sio@ELK: ~  
root@ELK:~# /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic  
This tool will reset the password of the [elastic] user to an autogenerated value.  
The password will be printed in the console.  
Please confirm that you would like to continue [y/N]y  
  
Password for the [elastic] user successfully reset.  
New value: 542laBLNBvdunveYIZvY  
root@ELK:~#
```

MDP :

542laBLNBvdunveYIZvY

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

```
sio@ELK: ~  
root@ELK:~# curl -k -u elastic https://localhost:9200  
Enter host password for user 'elastic':  
{  
  "name" : "ELK",  
  "cluster_name" : "elasticsearch",  
  "cluster_uuid" : "yLa0BwdLTs-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"  
}  
root@ELK:~#
```

- Configuration KIBANA

```
root@ELK:~# /usr/share/kibana/bin/kibana-encryption-keys generate -q --force  
xpack.encryptedSavedObjects.encryptionKey: d6f7bdbe1f7abba7ba543746eea63c9c  
xpack.reporting.encryptionKey: bed7b043d88d98ff9f5f24b233e232d3  
xpack.security.encryptionKey: 2c39508821b7f3da50cdf5a40abbc116  
root@ELK:~#
```

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 :

```
sio@ELK: ~
GNU nano 8.4 /etc/kibana/kibana.yml *
# Set the interval in milliseconds to sample system and process performance
# metrics. Minimum is 100ms. Defaults to 5000ms.
#ops.interval: 5000

# Specifies locale to be used for all localizable strings, dates and number formats.
# Supported languages are the following: English (default) "en", Chinese "zh-CN", Japanese "ja-JP", Fre
#i18n.locale: "en"

# ===== Frequently used (Optional)=====

# ===== Saved Objects: Migrations =====
# Saved object migrations run at startup. If you run into migration-related issues, you might need to a
# The number of documents migrated at a time.
# If Kibana can't start up or upgrade due to an Elasticsearch `circuit_breaking_exception`,
# use a smaller batchSize value to reduce the memory pressure. Defaults to 1000 objects per batch.
#migrations.batchSize: 1000

# The maximum payload size for indexing batches of upgraded saved objects.
# To avoid migrations failing due to a 413 Request Entity Too Large response from Elasticsearch.
# This value should be lower than or equal to your Elasticsearch cluster's `http.max_content_length`
# configuration option. Default: 100mb
#migrations.maxBatchSizeBytes: 100mb

# The number of times to retry temporary migration failures. Increase the setting
# if migrations fail frequently with a message such as `Unable to complete the [...] step after
# 15 attempts, terminating`. Defaults to 15
#migrations.retryAttempts: 15

# ===== Search Autocomplete =====
# Time in milliseconds to wait for autocomplete suggestions from Elasticsearch.
# This value must be a whole number greater than zero. Defaults to 1000ms
#unifiedSearch.autocomplete.valueSuggestions.timeout: 1000

# Maximum number of documents loaded by each shard to generate autocomplete suggestions.
# This value must be a whole number greater than zero. Defaults to 100_000
#unifiedSearch.autocomplete.valueSuggestions.terminateAfter: 100000

xpack.encryptedSavedObjects.encryptedKey: d6f7bdbe1f7abba7ba543746eea63c9c
xpack.reporting.encryptedKey: bed7b043d88d98ff9f5f24b233e232d3
xpack.security.encryptedKey: 2c39508821b7f3da50cdf5a40abbc116
```

```
sio@ELK: ~
root@ELK:~# cp /etc/elasticsearc/certs/http_ca.crt /etc/kibana/
root@ELK:~#
```

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

```
sio@ELK: ~
GNU nano 8.4 /etc/kibana/kibana.yml
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
#server.host: "localhost"
server.host: "192.168.2.102"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# ===== Search Autocomplete =====
# Time in milliseconds to wait for autocomplete suggestions from Elasticsearch.
# This value must be a whole number greater than zero. Defaults to 1000ms
#unifiedSearch.autocomplete.valueSuggestions.timeout: 1000

# Maximum number of documents loaded by each shard to generate autocomplete suggestions.
# This value must be a whole number greater than zero. Defaults to 100_000
#unifiedSearch.autocomplete.valueSuggestions.terminateAfter: 100000

xpack.encryptedSavedObjects.encryptionKey: d6f7bdbe1f7abba7ba543746eea63c9c
xpack.reporting.encryptionKey: bed7b043d88d98ff9f5f24b233e232d3
xpack.security.encryptionKey: 2c39508821b7f3da50cdf5a40abbc116
telemetry.optIn: false
telemetry.allowChangingOptInStatus: false

# ===== System: Elasticsearch (Optional) =====
# These files are used to verify the identity of Kibana to Elasticsearch and are required when
# xpack.security.http.ssl.client_authentication in Elasticsearch is set to required.
#elasticsearch.ssl.certificate: /path/to/your/client.crt
#elasticsearch.ssl.key: /path/to/your/client.key

# Enables you to specify a path to the PEM file for the certificate
# authority for your Elasticsearch instance.
#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]
elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/http_ca.crt" ]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.
#elasticsearch.ssl.verificationMode: full
```

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

```
sio@ELK: ~  
root@ELK:~# /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana  
eyJ2ZXliOiI4LjE0LjAiLCJhZHliOiI0LsiMTkyLjE2OC4yLjEwMj05MjAwIl0sImZnciI6ImI0Yjk0ZjFhYzYyOTc0ODBiYmVmYmY0Yjk2OTk0MDc4MzU1MjYxZjYwMDU2MmFkZmFhNmYwNDQwYWJhNjgzNjciLCJrZXkiOiJlJDUZDU1pvQmpOem15RHc2eUNtNTpCdlo0NmYzZW5sTHFfd1lCb2VmaFVRIn0=  
root@ELK:~#
```

Copiez/collez la sortie sur votre document :

```
eyJ2ZXliOiI4LjE0LjAiLCJhZHliOiI0LsiMTkyLjE2OC4yLjEwMj05MjAwIl0sImZnciI6ImI0Yjk0ZjFhYzYyOTc0ODBiYmVmYmY0Yjk2OTk0MDc4MzU1MjYxZjYwMDU2MmFkZmFhNmYwNDQwYWJhNjgzNjciLCJrZXkiOiJlJDUZDU1pvQmpOem15RHc2eUNtNTpCdlo0NmYzZW5sTHFfd1lCb2VmaFVRIn0=
```

Nous démarrons et activons le service Kibana :

```
3 nov. 11:29  
sio@ELK: ~  
root@ELK:~# systemctl start kibana  
root@ELK:~# systemctl enable kibana  
Created symlink '/etc/systemd/system/multi-user.target.wants/kibana.service' → '/usr/lib/systemd/system/kibana.service'.  
root@ELK:~#
```


- Vérification de son état :

```
sio@ELK: ~  
root@ELK:~# systemctl status kibana  
● kibana.service - Kibana  
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)  
   Active: active (running) since Mon 2025-11-03 11:29:17 CET; 34s ago  
 Invocation: e3e8ff76938e4b53aebc102a9420c256  
    Docs: https://www.elastic.co  
   Main PID: 5851 (node)  
     Tasks: 11 (limit: 4619)  
    Memory: 442.6M (peak: 550.9M)  
       CPU: 10.909s  
    CGroup: /system.slice/kibana.service  
           └─5851 /usr/share/kibana/bin/./node/glibc-217/bin/node /usr/share/kibana/bin/./src/cli/d  
nov. 03 11:29:19 ELK kibana[5851]: Native global console methods have been overridden in production env  
nov. 03 11:29:21 ELK kibana[5851]: [2025-11-03T11:29:21.531+01:00][INFO ][root] Kibana is starting  
nov. 03 11:29:21 ELK kibana[5851]: [2025-11-03T11:29:21.561+01:00][INFO ][node] Kibana process configur  
nov. 03 11:29:32 ELK kibana[5851]: [2025-11-03T11:29:32.900+01:00][INFO ][plugins-service] The followin  
nov. 03 11:29:32 ELK kibana[5851]: [2025-11-03T11:29:32.954+01:00][INFO ][http.server.Preboot] http ser  
nov. 03 11:29:33 ELK kibana[5851]: [2025-11-03T11:29:33.032+01:00][INFO ][plugins-system.preboot] Setti  
nov. 03 11:29:33 ELK kibana[5851]: [2025-11-03T11:29:33.049+01:00][INFO ][preboot] "interactiveSetup" p  
nov. 03 11:29:33 ELK kibana[5851]: [2025-11-03T11:29:33.071+01:00][INFO ][root] Holding setup until pre  
nov. 03 11:29:40 ELK kibana[5851]: i Kibana has not been configured.  
nov. 03 11:29:40 ELK kibana[5851]: Go to http://192.168.2.102:5601/?code=617694 to get started.  
lines 1-22/22 (END)
```



- Un code de vérification nous est demandé :

×



## Verification required

Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

Verify


- Nous générons le code et nous l'entrons :

sio@ELK: ~Q ☰ ×

sio@ELK: ~sio@ELK: ~

```
root@ELK:~# /usr/share/kibana/bin/kibana-verification-code
Your verification code is: 617 694
root@ELK:~#
```

×

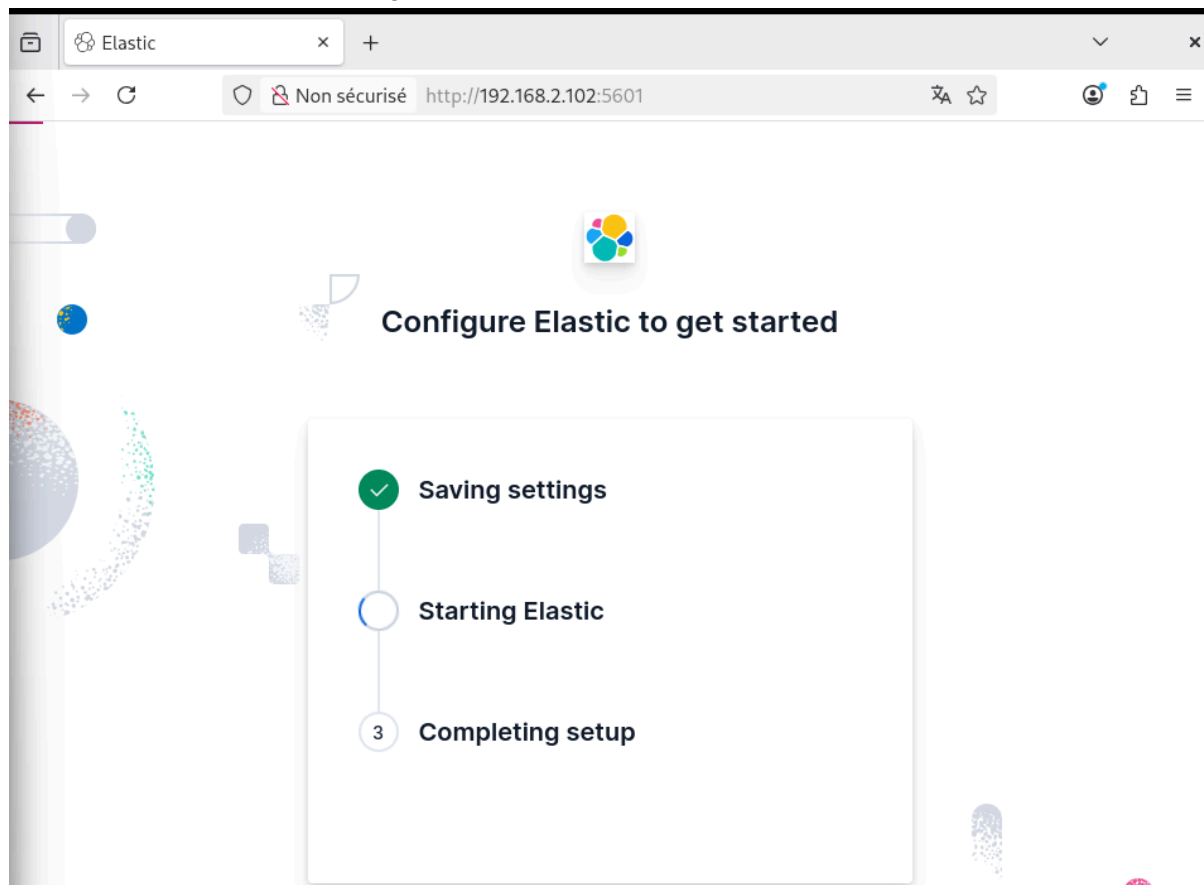


## Verification required

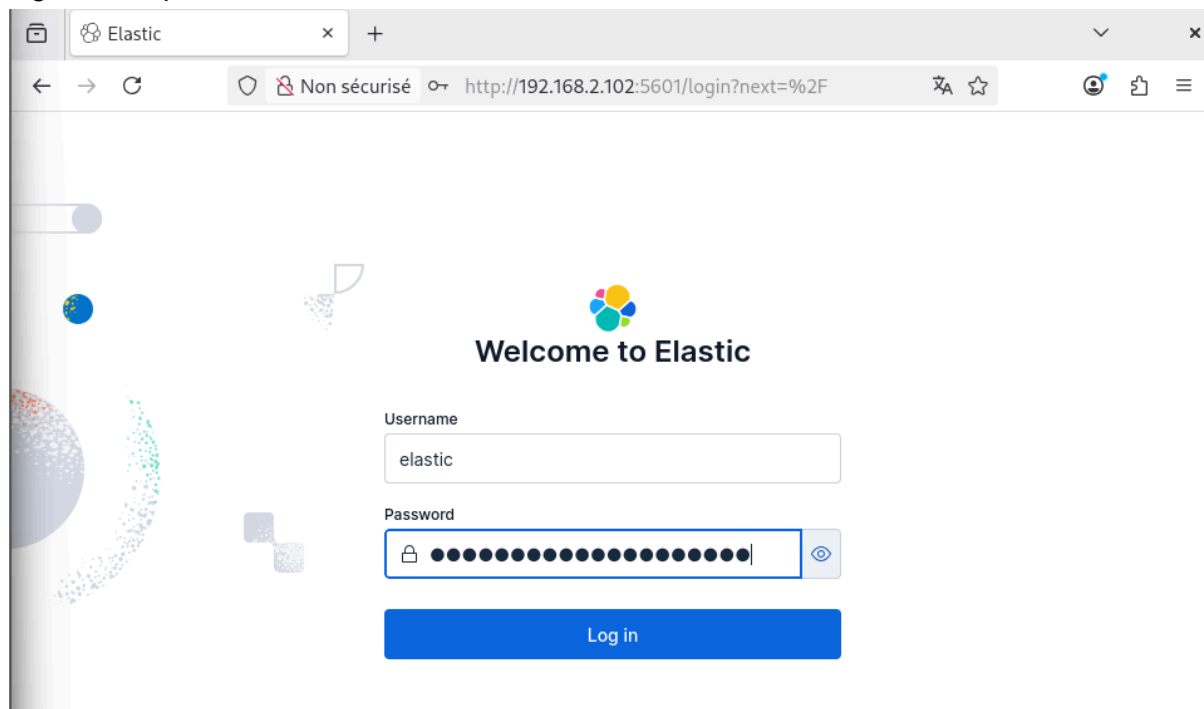
Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

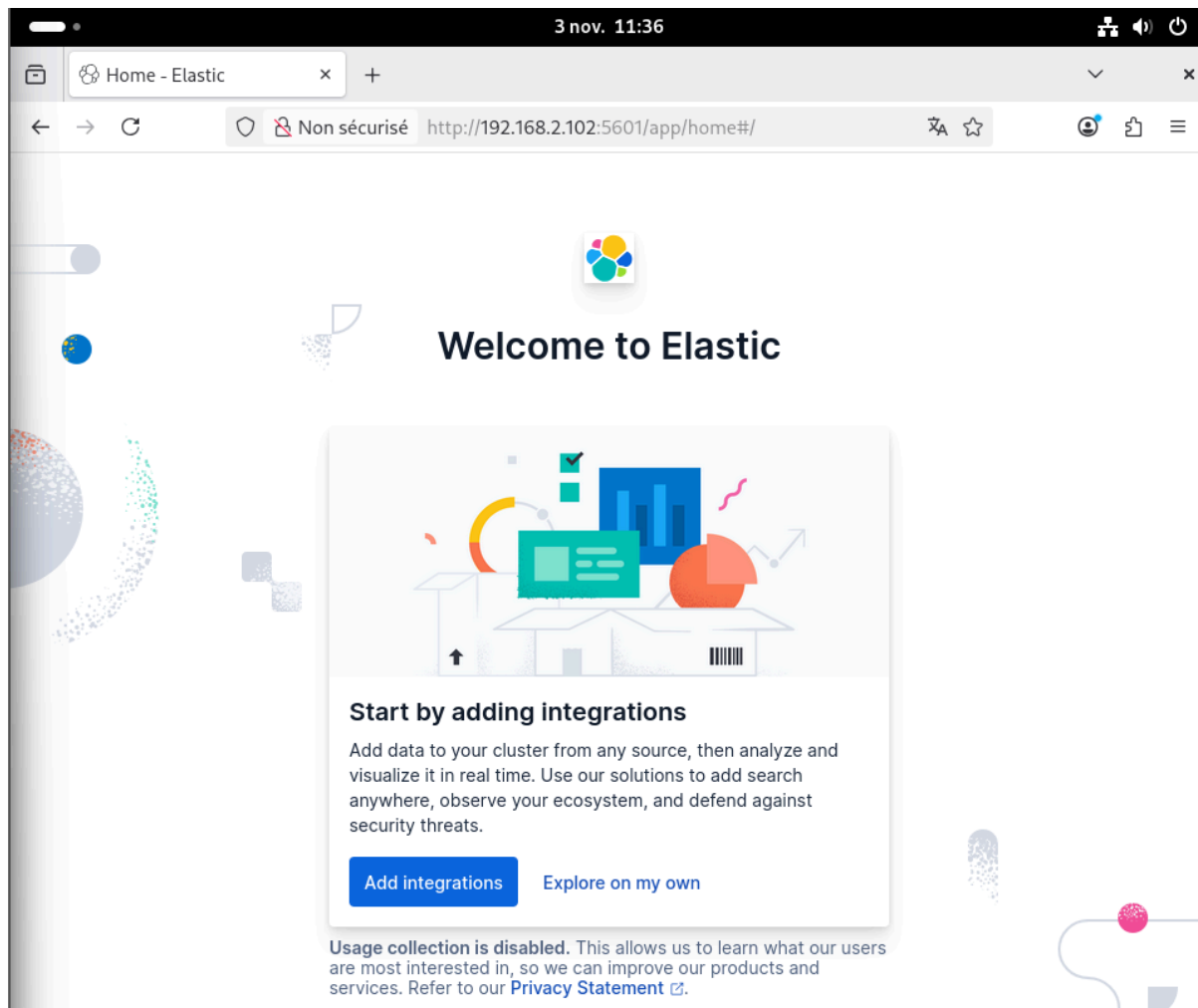
Verify

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



- Nous nous connectons avec l'utilisateur elastic et le mot de passe que nous avons régénéré auparavant :



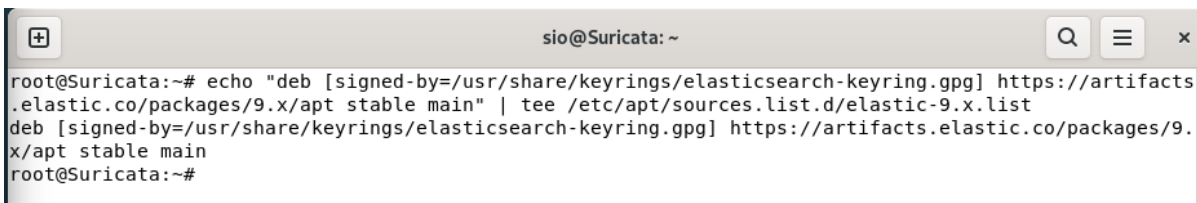


## 5. Installation de Filebeat sur la VM Suricata.

- 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 :



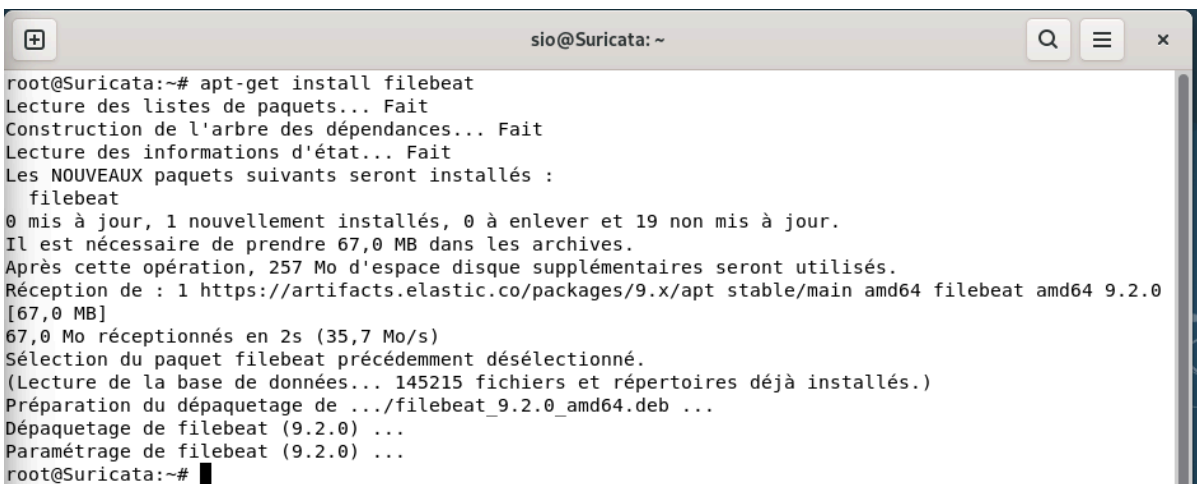
```
sio@Suricata: ~  
root@Suricata:~# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-9.x.list  
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt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

```

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 an 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 ZWxhc3RpYzo1NDJsYUJMTkZ2ZHVudmVZSVp2WQ==  
> 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" : "yLa0BwdLTs-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 :

```
sio@Suricata: ~  
root@Suricata:~# filebeat modules enable suricata  
Enabled suricata  
root@Suricata:~# █
```

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

```
sio@Suricata: ~  
GNU nano 8.4 /etc/filebeat/modules.d/suricata.yml  
# Module: suricata  
# Docs: https://www.elastic.co/guide/en/beats/filebeat/main/filebeat-module-suricata.html  
  
- module: suricata  
  # All logs  
  eve:  
    enabled: true  
  
  # Set custom paths for the log files. If left empty,  
  # Filebeat will choose the paths depending on your OS.  
  var.paths: ["/var/log/suricata/eve.json"]
```

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

```
sio@Suricata: ~  
root@Suricata:~# filebeat setup  
Index setup finished.  
Loading dashboards (Kibana must be running and reachable)  
Loaded dashboards  
Loaded Ingest pipelines  
root@Suricata:~#
```

- Nous démarrons le service Filebeat :

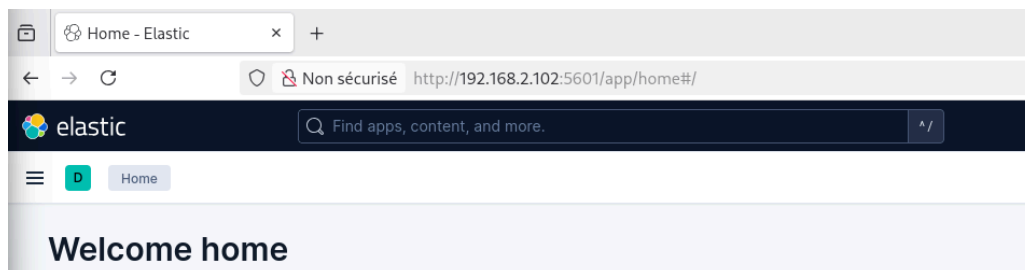
```
sio@Suricata: ~  
root@Suricata:~# systemctl start filebeat  
root@Suricata:~# █
```

```
sio@Suricata: ~  
root@Suricata:~# systemctl enable filebeat  
Created symlink '/etc/systemd/system/multi-user.target.wants/filebeat.service' → '/usr/lib/systemd/system/filebeat.service'.  
root@Suricata:~#
```

- Nous vérifions l'état du service :

```
sio@Suricata: ~  
root@Suricata:~# systemctl status filebeat  
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.  
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: enabled)  
   Active: active (running) since Wed 2025-11-05 13:27:16 CET; 493ms ago  
 Invocation: 82fb3b004a0241e4ae6abd664a48465c  
    Docs: https://www.elastic.co/beats/filebeat  
   Main PID: 2915 (filebeat)  
    Tasks: 7 (limit: 4635)  
  Memory: 39.3M (peak: 39.5M)  
     CPU: 98ms  
   CGroup: /system.slice/filebeat.service  
           └─2915 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.y  
nov. 05 13:27:16 Suricata systemd[1]: filebeat.service: Scheduled restart job, restart counter is at 7.  
nov. 05 13:27:16 Suricata systemd[1]: Started filebeat.service - Filebeat sends log files to Logstash  
nov. 05 13:27:16 Suricata filebeat[2915]: {"log.level":"info","@timestamp":"2025-11-05T13:27:16.484+01>  
nov. 05 13:27:16 Suricata filebeat[2915]: {"log.level":"info","@timestamp":"2025-11-05T13:27:16.484+01>  
lines 1-16/16 (END)
```

- Nous accédons à Kibana :



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

