# Installation de Suricata (Ubuntu)

SURICATA®

Sommaire :

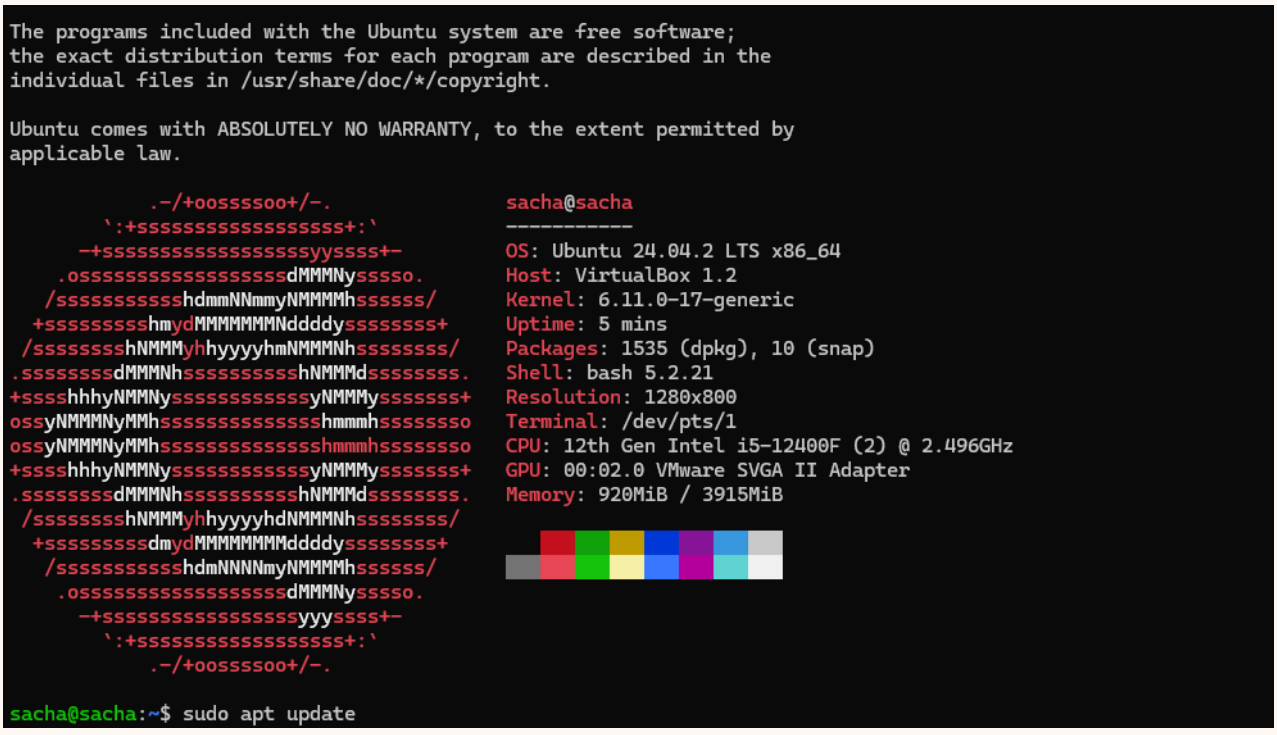
# Configuration serveur Suricata

## 1- Prérequis

Suricata est un système de détection et de prévention d'intrusions open-source, capable d'analyser en temps réel le trafic réseau pour détecter des menaces. Il supporte plusieurs protocoles et est optimisé pour des performances élevées grâce au multithreading.

## 2- Mise à jour des paquets du système :

Commencons par un update :



# Configuration serveur Suricata

## 3- Installation de Suricata :

Suricata est présent sur les dépots ubuntu un simple apt install suffit donc :

```
sacha@sacha:~$ sudo apt install suricata
```

```
sacha@sacha:~$ suricata -V
This is Suricata version 7.0.3 RELEASE
```

## 4- Configuration du serveur :

Maintenant que suricata est installé nous allons faire un test simple comme exemple pour commencer nous allons consulter le fichier de configuration suricata :

```
sacha@sacha:~$ sudo nano /etc/suricata/suricata.yaml
```

Par défaut Suricata analyse plusieurs réseau c'est à nous de modifier en fonction de nos attentes :

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
```

# Configuration serveur Suricata

Pour mon cas je vais seulement analyser mon @ ip :

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.1.51/32]"
    #HOME_NET: "[192.168.0.0/16]"
```

Puis choisir sur qu'elle interface suricata va opérer :

**pour trouver rapidement : *CTRL + W puis af - packet***

```
# Linux high speed capture support
af-packet:
  - interface: enp0s3
    # Number of receive threads. "auto" uses the number
    #threads: auto
    # Default clusterid. AF_PACKET will load balance pack
    cluster-id: 99
```

Puis modifiez avec le nom de votre interface.

Nous pouvons ensuite mettre à jour les règles par défaut de suricata en récupérant les dernières règles :

```
sacha@sacha:~$ suricata-update
```

# Configuration serveur Suricata

Avant de démarrer le serveur nous pouvons tester la configuration du serveur :

***sudo suricata -T -c /etc/suricata/suricata.yaml -v***

```
sacha@sacha:~$ suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 1 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 1 signatures processed. 1 are IP-only rules, 0 are inspecting packet payl
 0 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

Puis on démarre le serveur :

```
sacha@sacha:~$ sudo systemctl start suricata
sacha@sacha:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-02-21 00:31:24 CET; 4min 27s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 8586 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile
   Main PID: 8587 (Suricata-Main)
      Tasks: 8 (limit: 4611)
     Memory: 43.4M (peak: 43.7M)
        CPU: 2.641s
     CGroup: /system.slice/suricata.service
             └─8587 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/sur

févr. 21 00:31:24 sacha systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
févr. 21 00:31:24 sacha suricata[8586]: i: suricata: This is Suricata version 7.0.3 RELEASE running in
févr. 21 00:31:24 sacha systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-17/17 (END)
```

# Configuration serveur Suricata

## 5- Test avec une règle local :

Maintenant que nous avons configuré et démarrer le serveur suricata nous pouvons effectuer un test avec une règle local (les règles récupéré avec le update nécessite de lancer des attaques.) Pour tester nous allons donc crée une règles ICMP et examiner le comportement du serveur :

***/etc/suricata/rules/local.rules*** ***(fichier des règles locales)***

```
sacha@sacha:~$ sudo nano /etc/suricata/rules/local.rules
```

Puis on ajoute notre règle :

FORMAT : ***action protocol source_ip source_port direction destination_ip destination_port (options)***

```
 GNU nano 7.2                                  /etc/suricata/rules/local.rules
alert icmp any any -> any any (msg:"ICMP Test Detected"; sid:1000001; rev:1;)
```

# Configuration serveur Suricata

Un suricata-update pour que le serveur accepte les modifications :

```
sacha@sacha:~$ suricata-update
```

Puis on redémarre le serveur :

***sudo systemctl restart suricata***

Ensuite nous analysons les log *simplifié* Suricata

***tail -f /var/log/suricata/fast.log***

```
sacha@sacha:~$ sudo tail -f /var/log/suricata/fast.log
```

Puis on lance un ping et on observe les alertes

```
02/21/2025-00:36:34.010659  [**] [1:1000001:1] ICMP Test Detected [**] [Classification: (null)] [Priority: 3]
.168.1.4:8 -> 192.168.1.51:0
02/21/2025-00:36:34.010728  [**] [1:1000001:1] ICMP Test Detected [**] [Classification: (null)] [Priority: 3]
.168.1.51:0 -> 192.168.1.4:0
```