

Sending Suricata Logs in Wazuh

Step 1: Install Suricata in the host computer

- ✓ `sudo apt update`
- ✓ `Sudo apt install suricata -y`

Check the Status of Suricata

- ✓ `Sudo systemctl status suricata`

```
systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-06-20 15:38:11 EDT; 57min ago
     Invocation: dca24e651c7d406eb0e432824a4aa2a5
       Docs: man:suricata(8)
             man:suricata-sc(8)
             https://suricata.io/documentation/
   Process: 71734 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
  Main PID: 71735 (Suricata-Main)
    Tasks: 7 (limit: 2211)
   Memory: 44.1M (peak: 44.9M)
      CPU: 58.41s
   CGroup: /system.slice/suricata.service
           └─71735 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Jun 20 15:38:11 kali systemd[1]: suricata.service: Deactivated successfully.
Jun 20 15:38:11 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.
Jun 20 15:38:11 kali systemd[1]: suricata.service: Consumed 29.409s CPU time, 54.6M memory peak.
Jun 20 15:38:11 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Jun 20 15:38:11 kali suricata[71734]: Info: conf-yaml-loader: Configuration node 'HOME_NET' redefined.
Jun 20 15:38:11 kali suricata[71734]: Info: conf-yaml-loader: Configuration node 'EXTERNAL_NET' redefined.
Jun 20 15:38:11 kali suricata[71734]: i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Jun 20 15:38:11 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

Now that suricata is running, let us deploy wazuh agents on Suricata machine.

Copy the generated commands and run the command in the suricata machine,

Server address: This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: 172.17.0.8

Optional settings: By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ab

Select one or more existing groups: default

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER=172.17.0.8 WAZUH_AGENT_GROUP=default WAZUH_AGENT_NAME=ab dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb
```

Requirements:

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

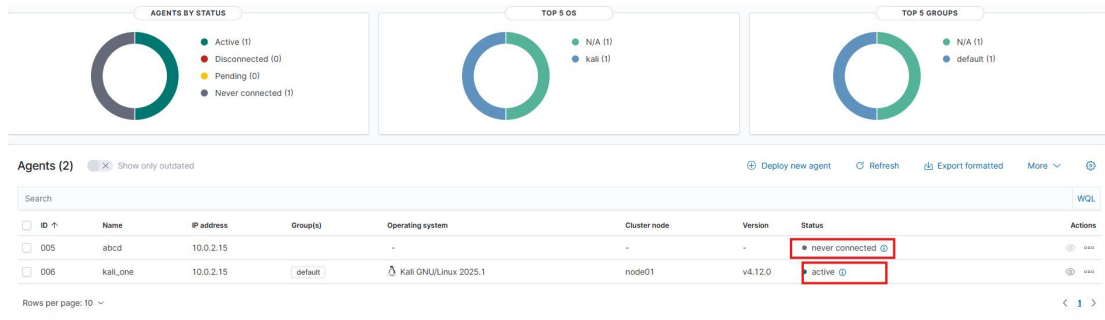
Copy the generated commands and run the command in the suricata machine.

```
(root@kali) ~#  
# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb  
# sudo WAZUH_MANAGER="172.17.0.0" WAZUH_AGENT_GROUP="default" WAZUH_AGENT_NAME="ab" dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb
```

Once the agent is installed reload and start the agent.

```
root@ramz:/home/ramz# sudo systemctl daemon-reload  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent  
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.  
root@ramz:/home/ramz#
```

Once the agent starts we can view the agent information in the wazuh dashboard.



- ✓ Once the agent is successfully deployed, change the directory to /var/ossec/etc and edit ossec.conf

sudo nano /var/ossec/etc/ossec.conf

```
(root@kali) ~#  
# sudo nano /var/ossec/etc/ossec.conf
```

- ✓ Add the suricata eve.json file path as shown below.

```
<ossec_config>  
  <localfile>  
    <log_format>json</log_format>  
    <location>/var/log/suricata/eve.json</location>  
  </localfile>  
</ossec_config>
```

```

<ossec_config>
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/nginx/error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>

```

In the suricata machine, download and extract the Emerging Threats Suricata ruleset

```

cd /tmp/ && curl -LO
https://rules.emergingthreats.net/open/suricata-
6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && mkdir /etc/suricata/rules &&
sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules

```

```

(root@kali)~[~]
# cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules

```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100 4878k	100 4878k	0 0	2072k 0	0:00:02	0:00:02	--:--:--	2072k

```

rules/
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules

```

Now modify Suricata settings in the /etc/suricata/suricata.yaml file and set the following variables

```

✓ sudo nano /etc/suricata/suricata.yaml

HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"
default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"
# Global stats configuration
stats:
enabled: yes
# Linux high speed capture support

```

af-packet:

- interface: enp0s3

```
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]"
  #HOME_NET: "[10.0.0.0/8]"
  #HOME_NET: "[172.16.0.0/12]"
  #HOME_NET: "any"

  EXTERNAL_NET: "!$HOME_NET"
  EXTERNAL_NET: "any"

# Global stats configuration
stats:
  enabled: yes
  # The interval field (in seconds) controls the interval at
  # which stats are updated in the log.
  interval: 8
default-rule-path: /var/lib/suricata/rules
rule-files:
- suricata.rules
default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"[]
```

Now restart Suricata and wazuh-agent,

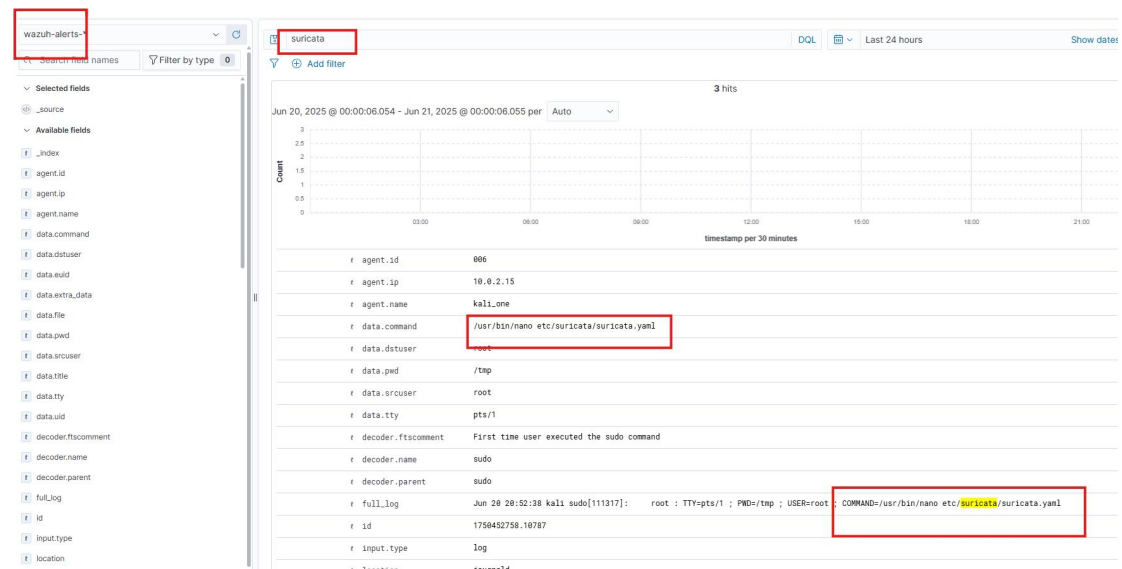
systemctl restart suricata

systemctl restart wazuh-agent

```
(root@kali)-[/tmp]
# systemctl restart suricata
systemctl restart wazuh-agent

(root@kali)-[/tmp]
#
```

Wazuh automatically parses data from /var/log/suricata/eve.json and generates related alerts on the Wazuh dashboard.



By Ambesaw Simachew Alene