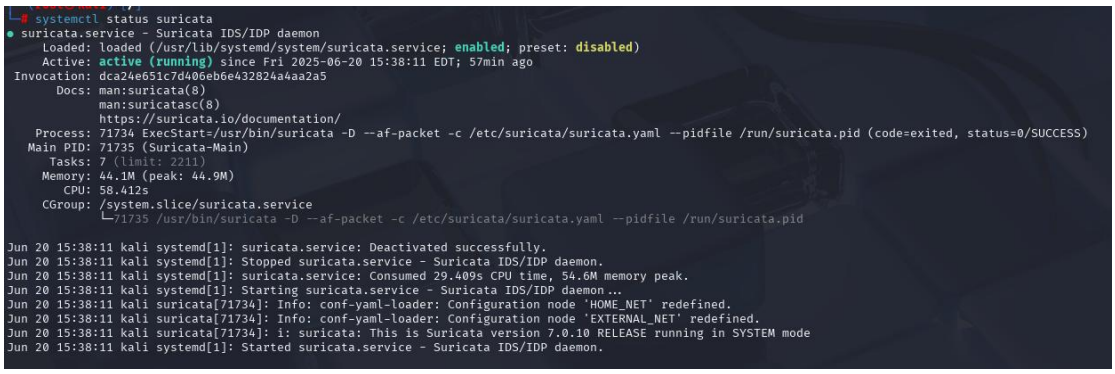
Sending Suricata Logs in Wazuh

Step 1: Install Suricata in the host computer

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

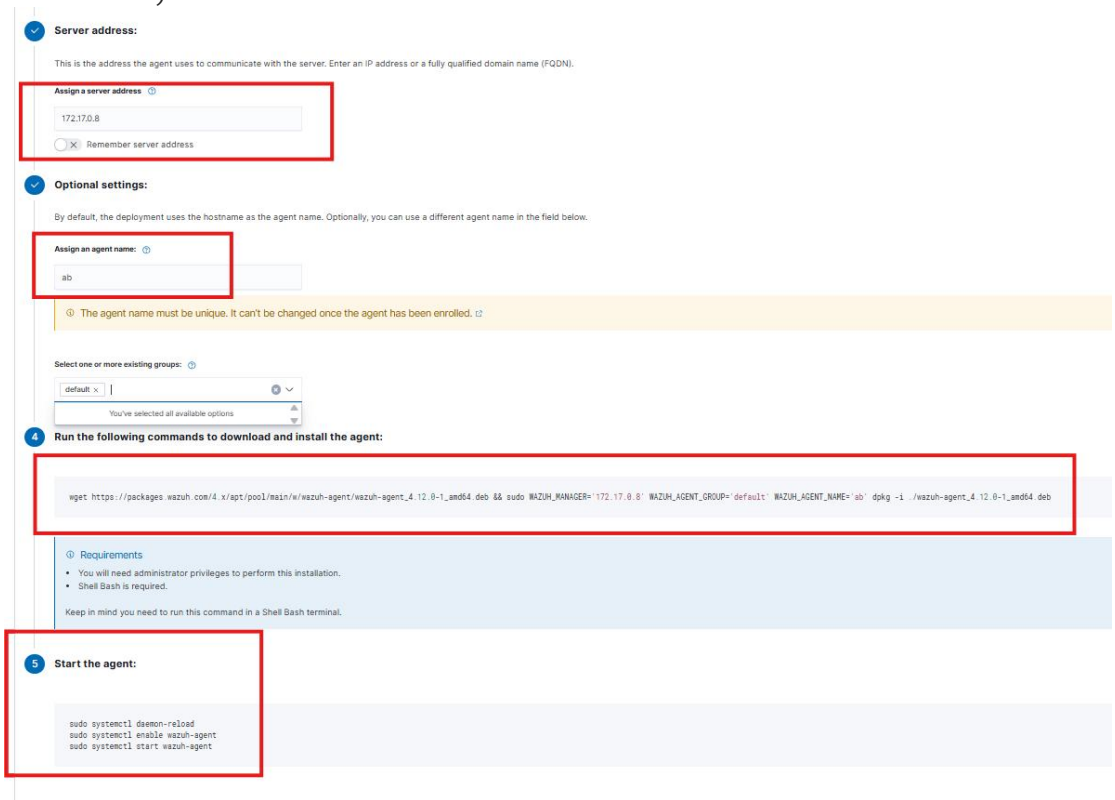
Check the Status of Suricata

- ✓ Sudo systemctl status suricata



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,

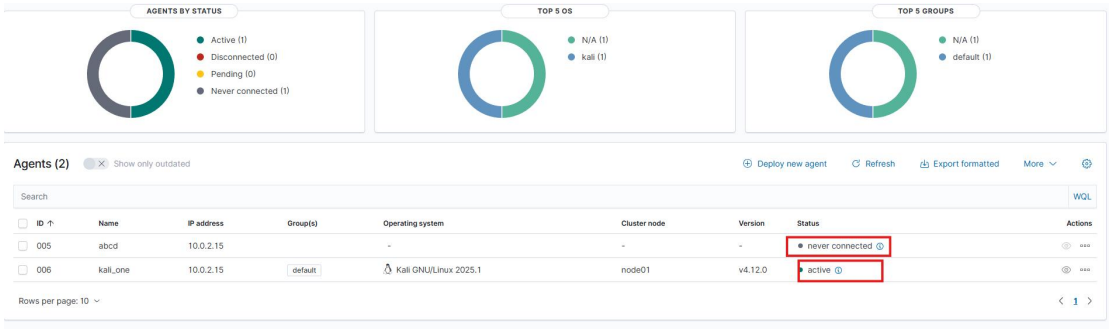


Copy the generated commands and run the command in the suricata machine.

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.serv
ice.
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

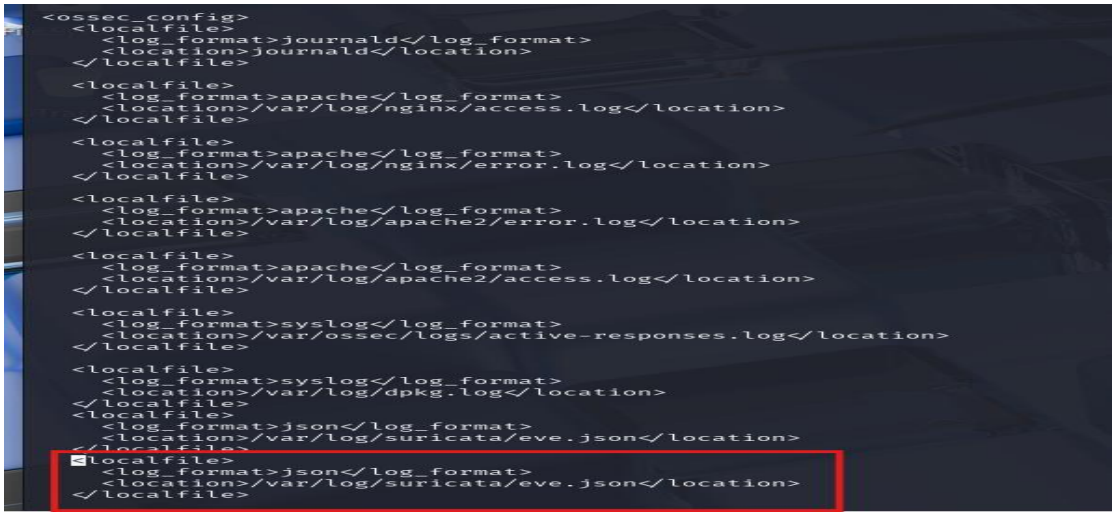
sudo nano /var/ossec/etc/ossec.conf

✓

```
┌──(root㉿kali)-[/]
└─# sudo nano /var/ossec/etc/ossec.conf
```

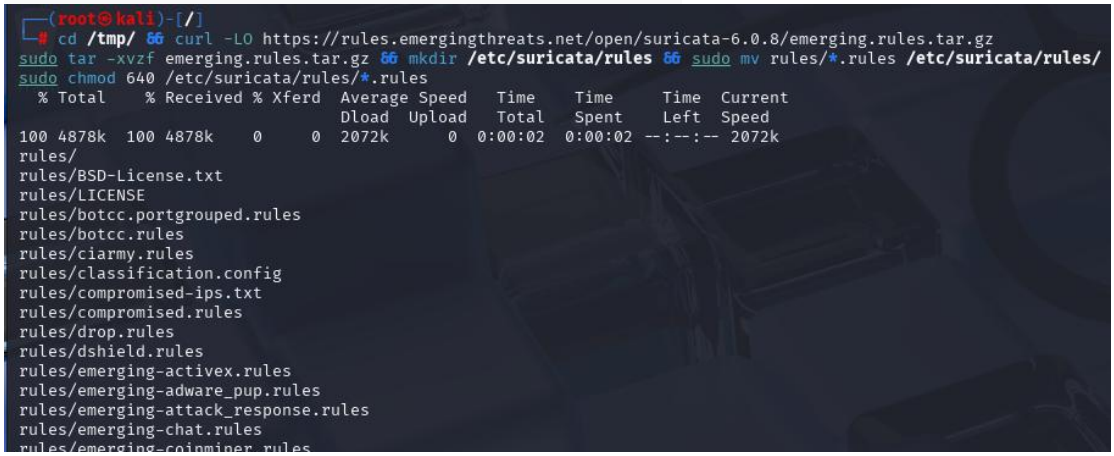
✓ Add the suricata eve.json file path as shown below.

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



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
```



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,

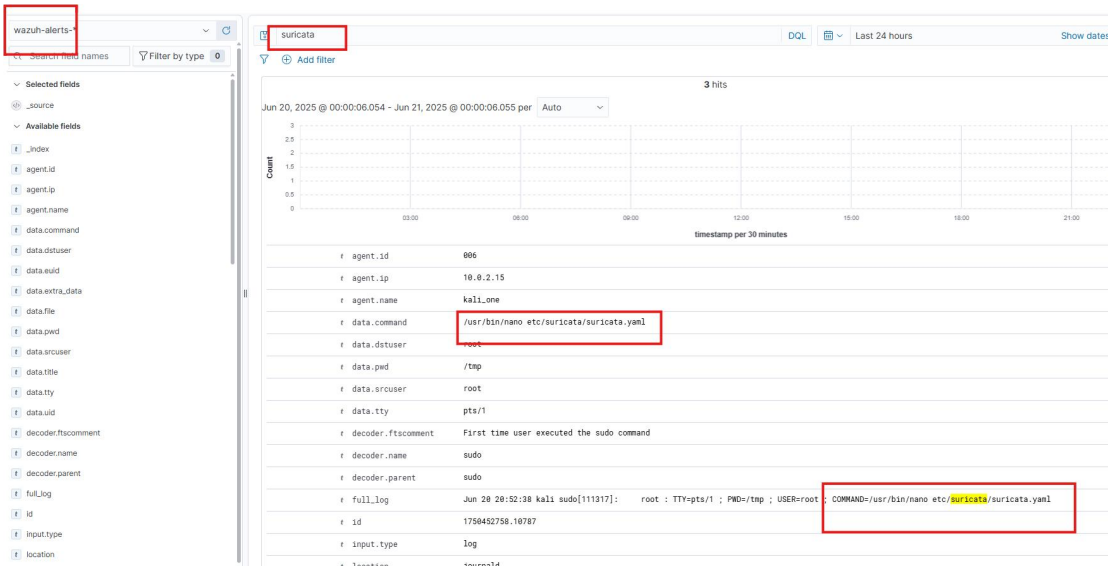
```
systemctl restart suricata
```

```
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