

Installing and configuring SIEM

Roozah Khan

In this and the next lab you will be installing and using Wazuh, an agent-based security monitoring and Security Information and Events Management (SIEM) system.

Wazuh is a free, open source and enterprise-ready security monitoring solution that provides a variety of functions, including security monitoring and analysis, log analysis, and intrusion detection, etc. In this lab you will be installing and configuring Wazuh so a Wazuh manager and a Wazuh agent can communicate, and you will be using its monitoring and log analysis functions in the next lab.

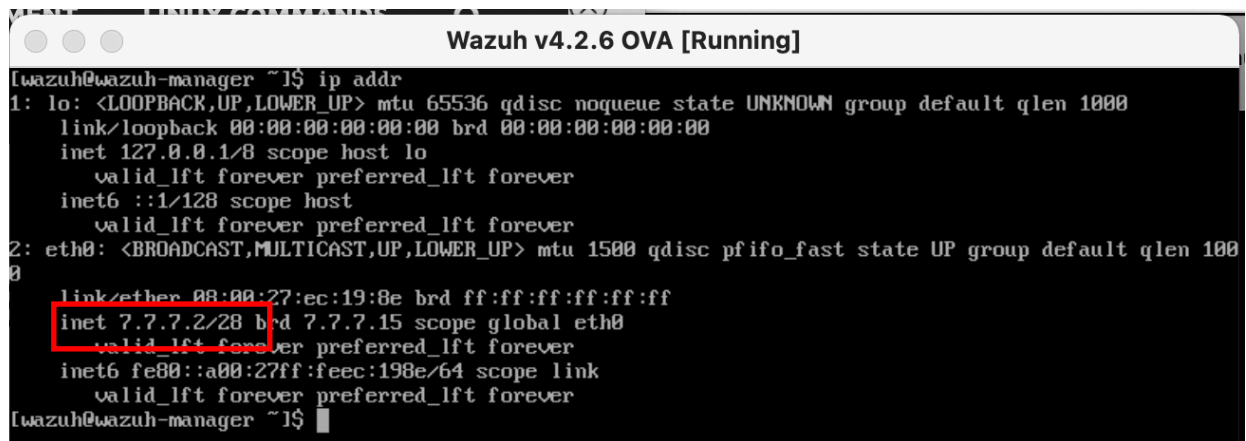
Wazuh works based on a agent-manager structure. Where multiple Wazuh agents can be installed on different operating systems, such as Linux or Windows, and a Wazuh manager communicates and manages those agents. Each agent can be configured to monitor a variety of security events on the host operating system, such as user login and file creating/deleting/modification, and sends those events to the manager. The manager can then aggregate the received logs and display them in a user-friendly graphical interface for human operators.

1. Find Wazuh manager installation guide from here: <https://documentation.wazuh.com/current/installation-guide/index.html>. You will be following the “all-in-one” installation. In specific, you will download the OVA image and import it into your Virtualbox, instead of installing all necessary components in a plain Linux environment.
2. Before power one the virtual machine, change its network adapter to “internal” and put it in LANnet that you have created in the previous lab.
3. Power on the virtual machine. Now we need to give Wazuh an IP address so it can connect to other hosts in this network. Wazuh is based on CentOS Linux, do a search online to find out how to configure IP addresses on CentOS, and the following are the configuration that you need to do:
 - a. You are going to configure the `eth0` interface.
 - b. Set the IP to be static (AKA manual), or, not using DHCP.
 - c. Set the IP address to be `7.7.7.2/28`
 - d. Set the gateway to be `7.7.7.1`.

Depending on how did you configured the IP addresses, you may need to restart the network interface to allow it be in effect, run command `systemctl restart network` after your configuration.

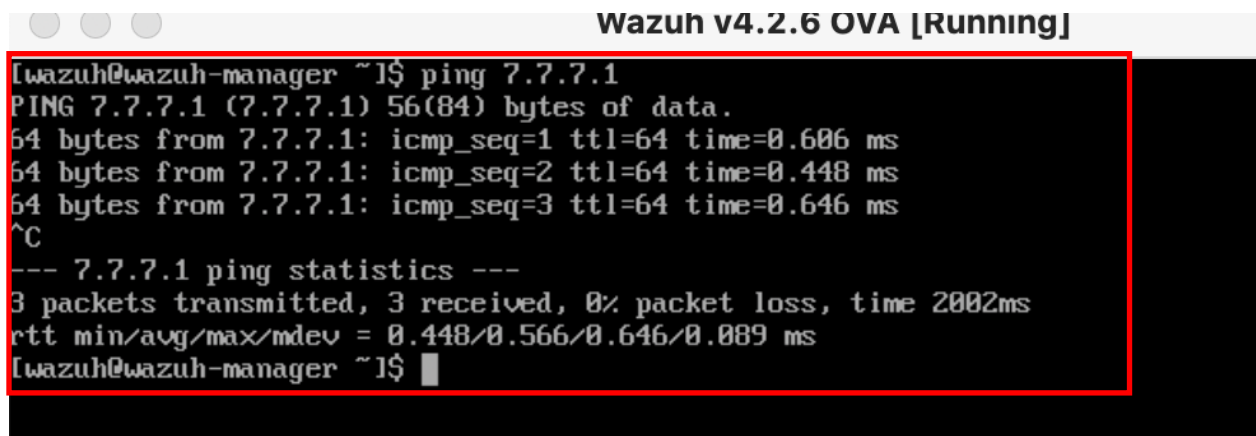
4. After the configuration and the network interface is restarted, type `ip addr` to display the network configuration. You should see the new IP address being listed on `eth0` interface. And you should be able to communicate with pfSense.

Provide a screenshot of the output of `ip addr` command, which should display the correctly configured IP addresses. – Screenshot 1.



```
[wazuh@wazuh-manager ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ec:19:8e brd ff:ff:ff:ff:ff:ff
    inet 7.7.7.2/28 brd 7.7.7.15 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feec:198e/64 scope link
        valid_lft forever preferred_lft forever
[wazuh@wazuh-manager ~]$
```

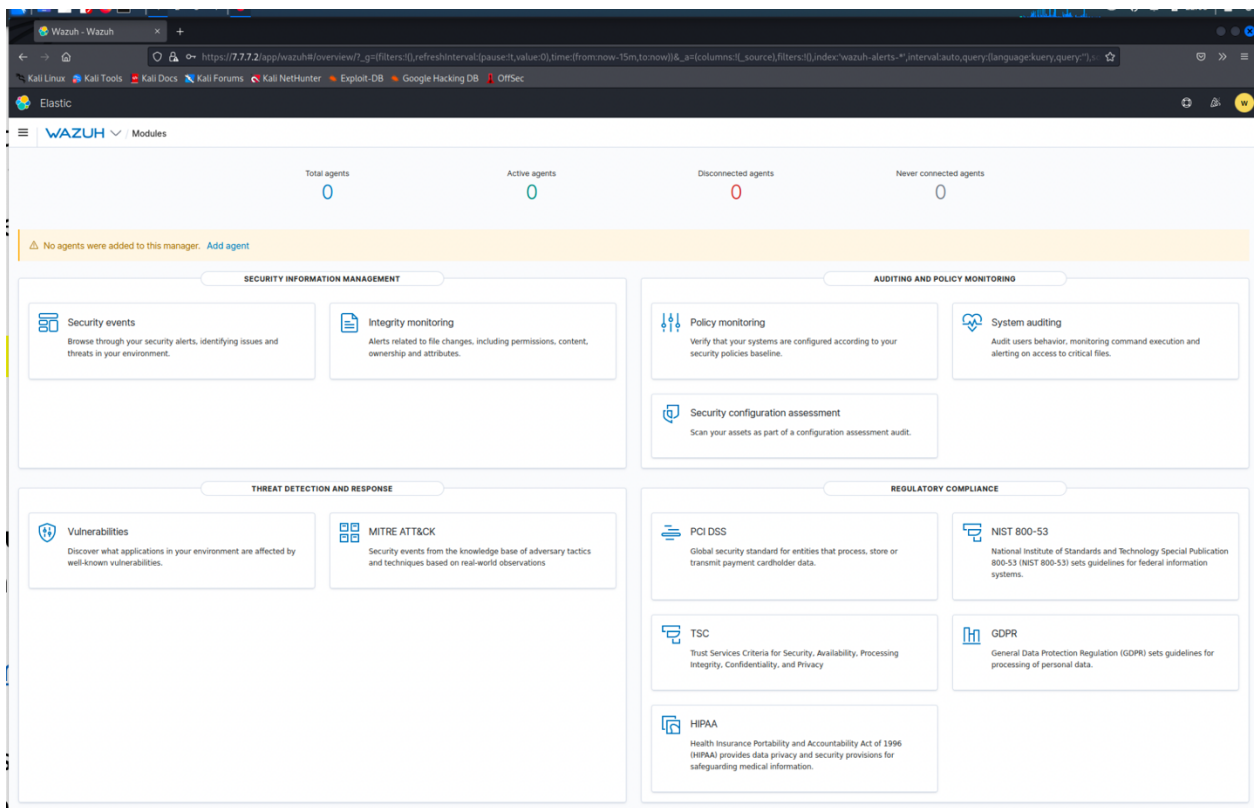
Provide a screenshot from Wazuh pinging the gateway 7.7.7.1, which should show that the ping is working. – Screenshot 2.



```
[wazuh@wazuh-manager ~]$ ping 7.7.7.1
PING 7.7.7.1 (7.7.7.1) 56(84) bytes of data.
64 bytes from 7.7.7.1: icmp_seq=1 ttl=64 time=0.606 ms
64 bytes from 7.7.7.1: icmp_seq=2 ttl=64 time=0.448 ms
64 bytes from 7.7.7.1: icmp_seq=3 ttl=64 time=0.646 ms
^C
--- 7.7.7.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.448/0.566/0.646/0.089 ms
[wazuh@wazuh-manager ~]$
```

5. If you can successfully ping the gateway, this means that you Wazuh manager is up and running. In the browser from Admin Client, enter <https://7.7.7.2>, you should now see the login page of Wazuh. Login with default username and password `wazuh:wazuh`, and you should be able to login.

Provide a screenshot to show that you have successfully logged in Wazuh manager. – Screenshot 3.



- The next step is to install a Wazuh agent on the Ubuntu server. The agent will monitor various events happens on the Ubuntu and report such events to the Wazuh manager, such that an operator can view and analyze such events from the manager.

The installation procedure of installing Wazuh agent is in this page:

<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>

For your information, Ubuntu uses `APT` to install packages, and use `systemd` to enable and disable services. Also remember, in our lab, the Wazuh_manager has address 7.7.7.2. If the installation manual is not clear enough for you, you can find more hint from watching this video (the first 8 minutes): <https://youtu.be/ASW5hHaGGGM>. Note this video is not installing the agent on Ubuntu, so you need to make necessary changes in your procedures.

- If you have followed the installation manual and set the Wazuh_manager IP during installation, and the installation is successful, the agent should be running now and trying to connect the manager. If you watched the video and have not set the manager's IP, you will need to manually set the IP, do so by editing `/var/ossec/etc/ossec.conf`. Set the

server's address to be 7.7.7.2, port to be 1514, and protocol to be tcp. Remember each time you changed anything in the configuration file, you need to restart the agent by `systemctl restart wazuh-agent`.

- The last thing is to allow the traffic between the Wazuh agent and manager. In pfSense, create a rule, allow the agent to connect to LANnet, using tcp on port 1514. If all set correctly, the agent and the manager should be able to communicate now. From the front page of Wazuh, or from the "modules" page, you should now see you have one "active agent". Click on the number "1", you will be brought to the page where detailed information of the agent is displayed, that is, your Ubuntu Server. You can also navigate to this page from the top-left of the Wazuh page, see the following.

Provide a screenshot of the "agent" page, showing that the details of the connected agent. –screenshot4.

