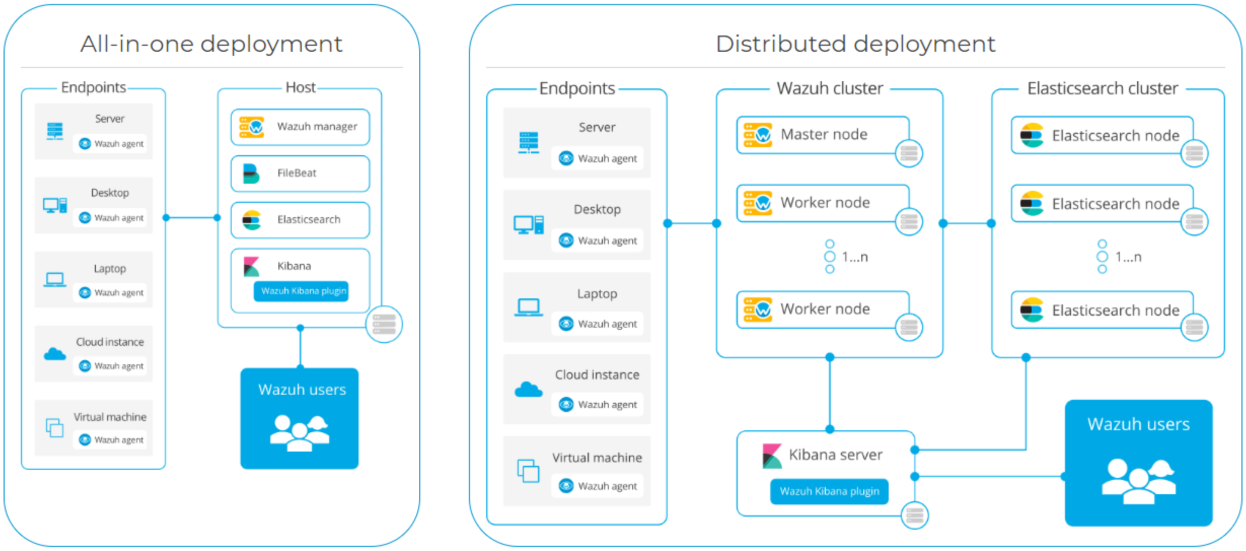
Installing and configuring SIEM

Roozah Khan

As you have successfully install Wazuh, we will now explore some basic functions of it. Wazuh is an integrated security monitoring system that is able to collect and aggregate security data, those data are then send to Elastic Stack for better analysis. As shown in the following, as we have taken the All-in-one deployment, the Elastic Stack has already been integrated in the virtual machine image and ready to work.



In the following we will explore a few basic Wazuh functions for security monitoring.

1. File integrity check

Part I: FIM (file integrity monitoring) configuration

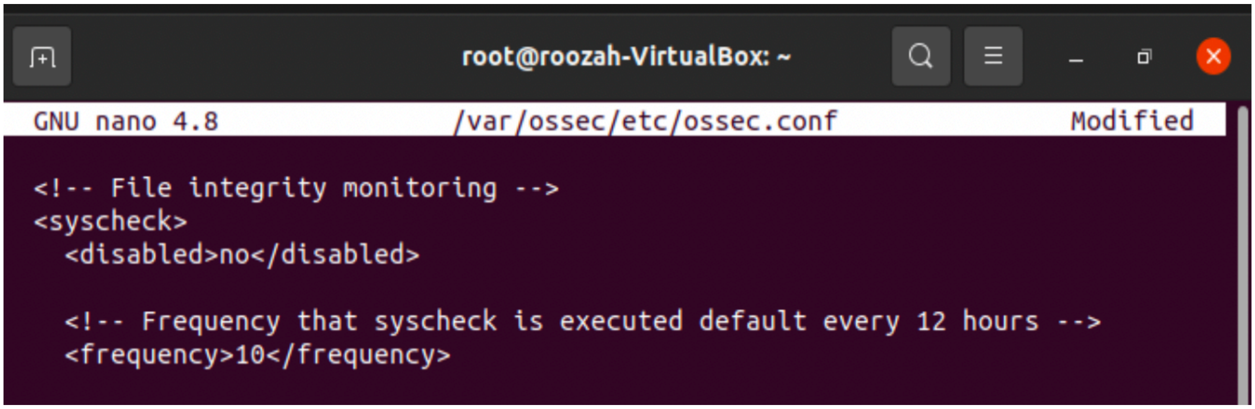
Wazuh agent is able to monitor the change of files in any specified path on the system. If any file is created/deleted/modified in the monitored path, Wazuh agent will record such action and send corresponding log to Wazuh manager.

By default, file integrity monitoring is turned off in the Wazuh agent, and you need to turn it on to enable such function.

1. From the Ubuntu instance, use your preferred editor, open and edit the file `/var/ossec/etc/ossec.conf` (you will need root access to edit it).
2. Scroll down the file till you find the section `<!-- File integrity monitoring -->`, modify the property `<disabled>` from `yes` to `no` (to turn it on).

In the `<frequency>` section, set it to `600` or any value you consider proper (unit is in seconds).
Pay attention to the `<directories>` section, those are the paths the agent will keep monitoring. We do not need to make any changes here.

Provide a screenshot focusing on your modified part of ossec.conf file to show your modification. – screenshot 1.



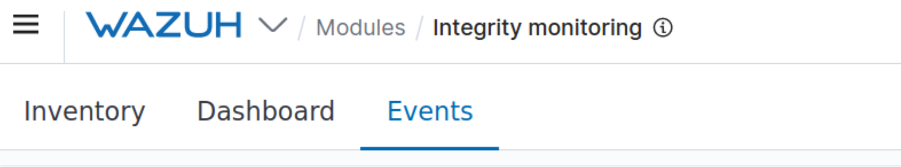
```
GNU nano 4.8                /var/ossec/etc/ossec.conf                Modified

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>10</frequency>
```

After this configuration, save the file, and restart wazuh-agent by typing `systemctl restart wazuh-agent`.

Part II: FIM in action.

1. Create a file `firstName_lastname.txt` in the path `/etc`. for example, I created a file `/etc/mingkui_wei.txt`.

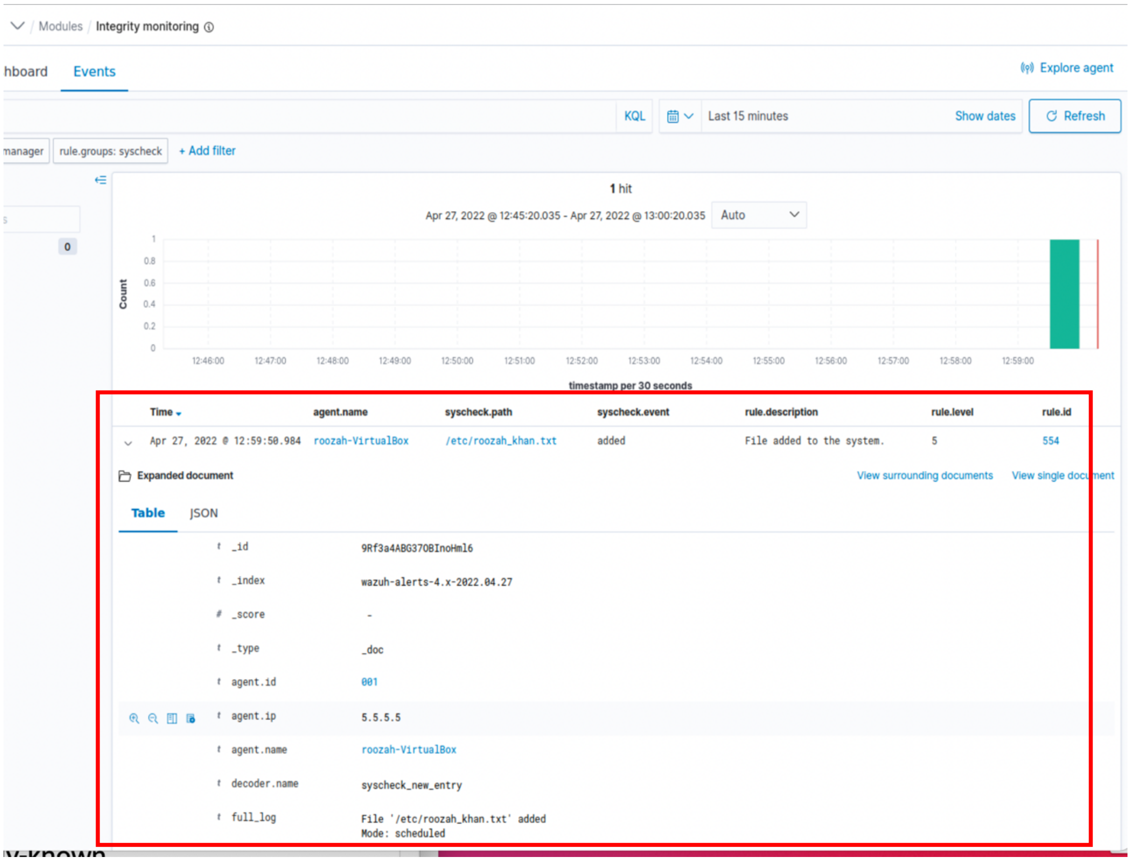
2. After the period you have set in the "frequency" section of the agent (we set it to 600 seconds unless you set it to other values), this event should be reflected in Wazuh manager. Now open Wazuh manager, from "modules", choose "Integrity monitoring, and switch to "Events" tab, as the following figure shows.



From here you should see a security event, i.e., a new file has been created in the monitored path.

3. Click on the drop-down arrow on the left side of this event, you can see much more details of this event, including who created it, when it is created, etc. You can also see the Hash value of this file is provided, which you can use to compare with known malware's Hash signatures, for example, on www.virustotal.com. We are not going to do it here since we know it won't match with any known signatures.

Make a screenshot of this event, showing that the file firstname_lastname.txt has been created and captured by the agent. – screenshot 2.



Time	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Apr 27, 2022 @ 12:59:50.984	roozah-VirtualBox	/etc/roozah_khan.txt	added	File added to the system.	5	554

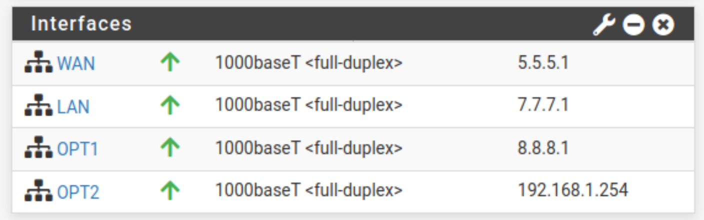
t _id	9Rf3a4ABG370BInoHml6
t _index	wazuh-alerts-4.x-2022.04.27
# _score	-
t _type	_doc
t agent.id	001
t agent.ip	5.5.5.5
t agent.name	roozah-VirtualBox
t decoder.name	syscheck_new_entry
t full_log	File '/etc/roozah_khan.txt' added Mode: scheduled

2. Vulnerability scanning

If you have explored Wazuh a bit, you may have found there is a module "Vulnerabilities". Wazuh is able to periodically scan the machine via the agent against publicly-known vulnerabilities listed in multiple sources, such as the National Vulnerability Database maintained by NIST.

However, you may also have found that the vulnerability function does not show any events now. This is because as we have confined all the virtual machines in our local network, the Wazuh manager is unable to download any vulnerability database, and thus unable to start such scanning. In the following, we are going to enable Internet access of the local network, let Wazuh manager to download those databases and scan the Ubuntu server.

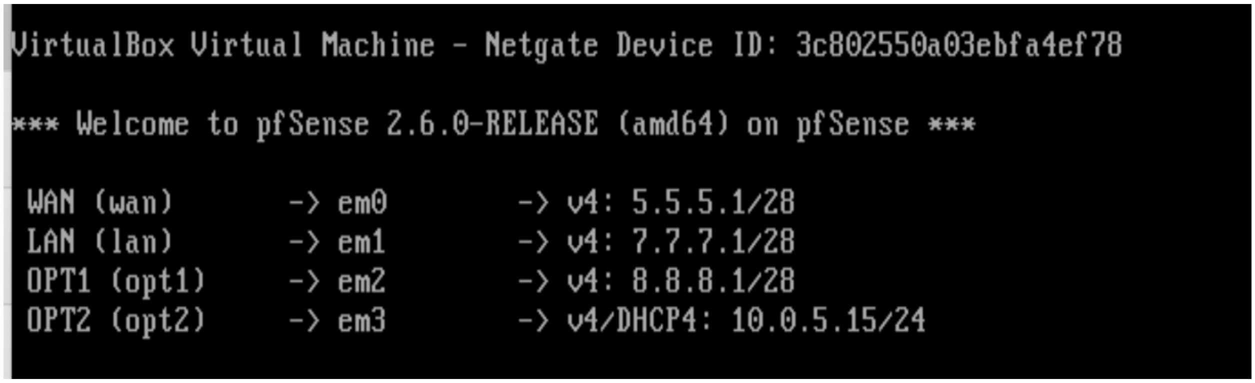
1. Make sure your host machine, i.e., the machine you are running virtualBox, has Internet access.
2. In VirtualBox, enable the 4th network interface for pfSense, set it to "NAT".
   Power on pfSense, (if already powered on, you need to reboot it). Configure its interface, without change the first 3 interfaces, assign `em3` to the new network interface `OPT2`.
   Login to pfSense GUI, in the front page, you should now see 4 interfaces: em0 – em3, like the following (your OPT2 shouldn't have an IP yet):



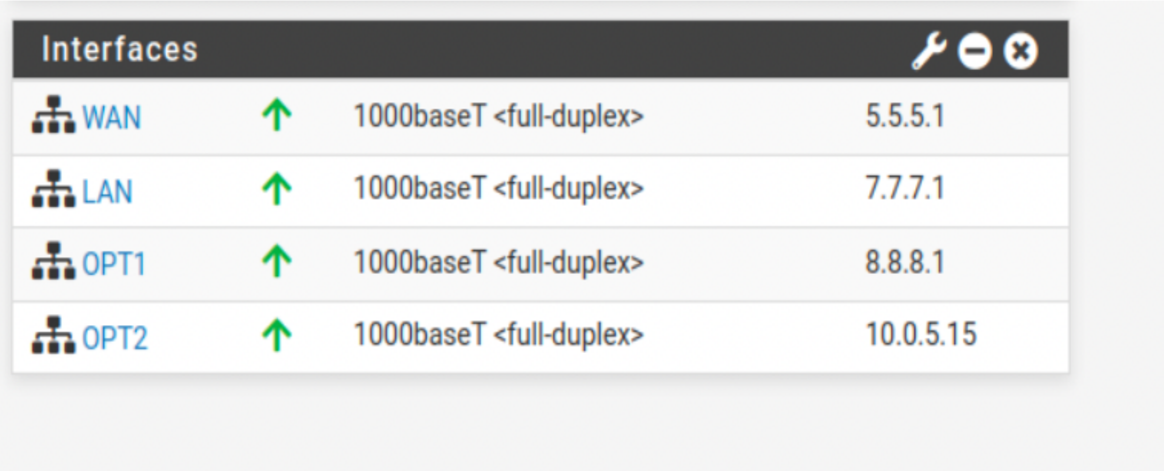
Interfaces			
WAN	↑	1000baseT <full-duplex>	5.5.5.1
LAN	↑	1000baseT <full-duplex>	7.7.7.1
OPT1	↑	1000baseT <full-duplex>	8.8.8.1
OPT2	↑	1000baseT <full-duplex>	192.168.1.254

   Click on OPT2, set its IPv4 Configuration Type to be DHCP. Save and apply change. Return back to the front page of pfSense, if all set correctly, you should now see your OPT2 network has an IP address.

   Provide a acreenshot showing the configuration of the 4 interfaces in pfSense's command line interface, showing that you have successfully obtained an IP using DHCP. – screenshot 3.



```
VirtualBox Virtual Machine - Netgate Device ID: 3c802550a03ebfa4ef78

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0       -> v4: 5.5.5.1/28
 LAN (lan)       -> em1       -> v4: 7.7.7.1/28
 OPT1 (opt1)     -> em2       -> v4: 8.8.8.1/28
 OPT2 (opt2)     -> em3       -> v4/DHCP4: 10.0.5.15/24
```



Interfaces

WAN	↑	1000baseT <full-duplex>	5.5.5.1
LAN	↑	1000baseT <full-duplex>	7.7.7.1
OPT1	↑	1000baseT <full-duplex>	8.8.8.1
OPT2	↑	1000baseT <full-duplex>	10.0.5.15