

Creating a Threat Hunting Lab with Wazuh and Google Cloud Platform

SNORT | WAZUH | GOOGLE CLOUD | UBUNTU

Azhar Ghafoor

Cybersecurity Analyst - MS Scholar

[Azhar Ghafoor | LinkedIn](#)

Azharghafoor39@gmail.com

Contents

- 1. Tools and Techs1
 - a. Google Cloud Platform.....1
 - b. Snort IDS1
 - c. Wazuh SIEM.....1
- 2. Steps To Follow1
 - a. Creating a Virtual Machine on GCP.....1
 - b. Installing Snort IDS on VM.....5
 - i. To detect ICMP (used for ping) packets, follow these steps:..... 7
 - c. Wazuh Integration..... 8
 - i. To access WAZUH SIEM, follow these steps:..... 8
 - ii. To add an agent, follow these steps:9

1. Tools and Techs

a. Google Cloud Platform

Google Cloud Platform (GCP) is a powerful cloud computing platform that enables users to build, test, and deploy applications on a global scale. Snort IDS is a popular open-source Intrusion Detection System (IDS) that is capable of detecting and preventing various network-based attacks. Wazuh is a cloud-based Security Information and Event Management (SIEM) solution that provides real-time threat detection and response capabilities. In this article, we will discuss how to set up a virtual machine (VM) on GCP and install Snort IDS on it. We will also cover how to integrate this cloud-based VM with Snort to connect it to Wazuh.

b. Snort IDS

Snort is a free and open-source network intrusion detection and prevention system. It is capable of analyzing network traffic and detecting various types of attacks, such as port scans, buffer overflows, and stealthy probing attempts. Snort uses a rule-based language to define the conditions under which a particular attack should be detected, making it highly customizable and adaptable to different network configurations. Snort is a widely used tool in cybersecurity and plays a crucial role in safeguarding networks against malicious activities.

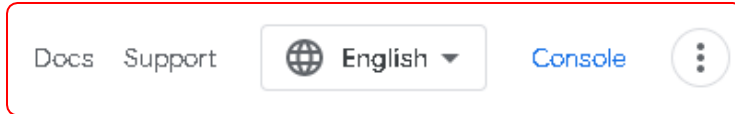
c. Wazuh SIEM

Wazuh is an open-source security monitoring solution that provides comprehensive visibility into the security status of an organization's IT infrastructure. Wazuh integrates with various security tools and technologies, such as Snort, to collect and analyze security data from different sources. Wazuh provides real-time alerts, visualization dashboards, and compliance reports to help organizations proactively manage their security posture. Wazuh is highly scalable and can be deployed on-premises or in the cloud, making it a versatile solution for organizations of different sizes and industries.

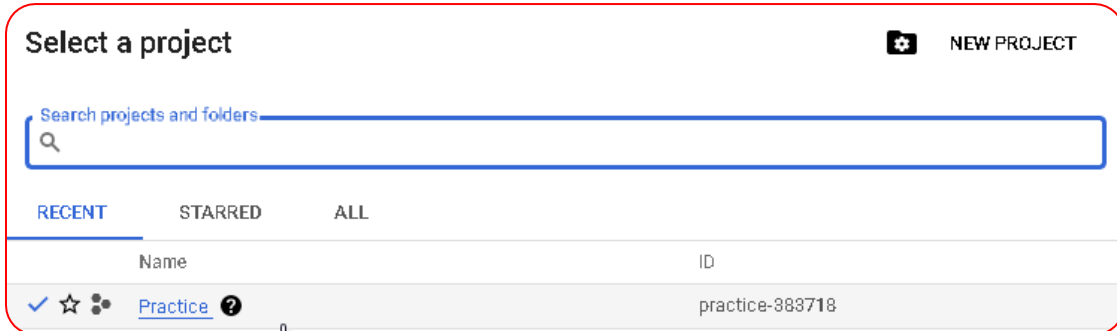
2. Steps To Follow

a. Creating a Virtual Machine on GCP

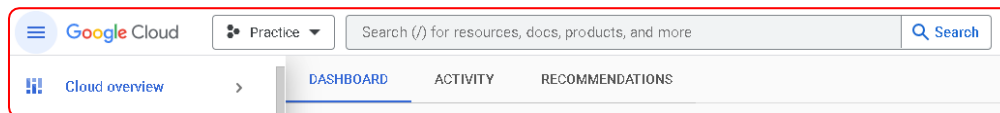
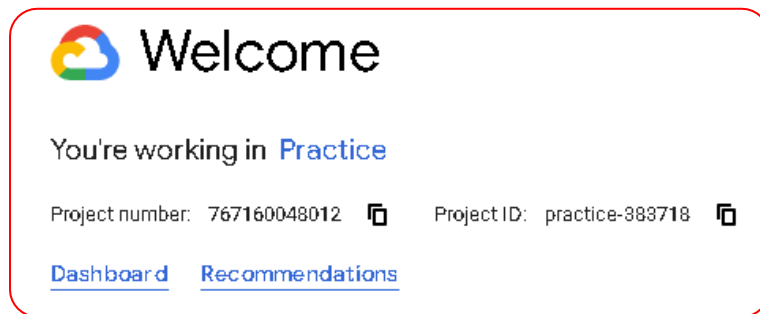
- I. Login to your account at <https://cloud.google.com/>
- II. Click on Console at the top right corner of the screen.



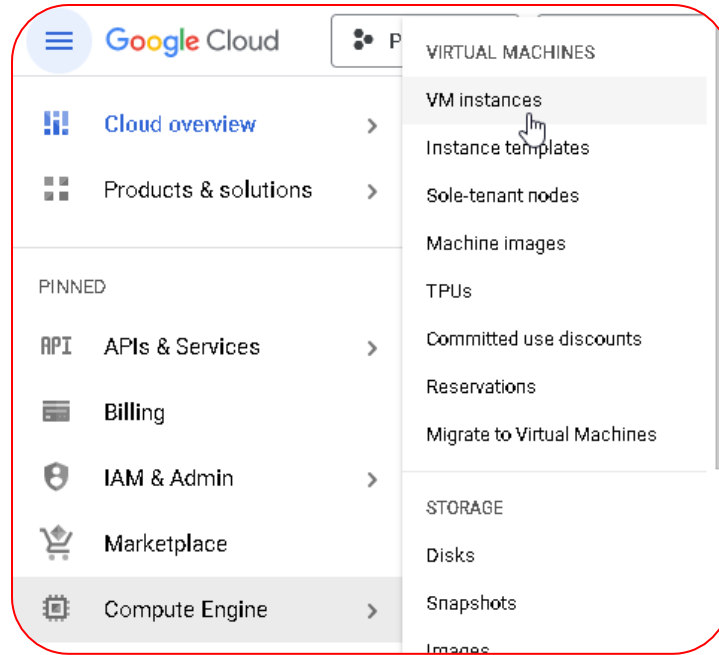
- III. From the Welcome page, click on Select the Project from the top dropdown menu or create a new project (in this case, we have already created a project named "Practice").



- IV. Click on "Dashboard" or it will automatically take you to the Dashboard page if you have created a new project.
- V. From here, you can manage your virtual machines and other resources.



- VI. From the menu, select "Compute Engine" and then "VM instances".



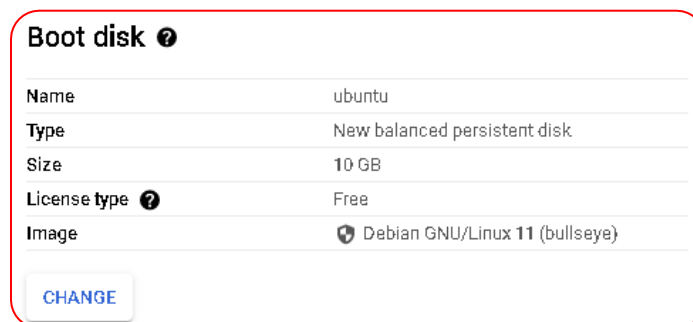
VII. It will open a new page. From the top of the page, click on "CREATE INSTANCE".



VIII. In the new page, you can set VM values such as VM name, region of the server, zone, machine type, etc.



IX. To select the operating system, click on the CHANGE button under "Boot disk".



X. It will open a new window. From here, select your desired OS, such as Ubuntu OS.

Operating system
Ubuntu

Version *
Ubuntu 20.04 LTS
x86/64, amd64 focal image built on 2023-03-02, supports Shielded VM features

Boot disk type *
Balanced persistent disk

COMPARE DISK TYPES

Size (GB) *
20

- XI. Under "Access scopes", select Allow default access and under "Firewall", check both checkboxes to allow both HTTP and HTTPS traffic for the instance.

Access scopes ⓘ

- Allow default access
- Allow full access to all Cloud APIs
- Set access for each API

Firewall ⓘ

Add tags and firewall rules to allow specific network traffic from the Internet

- Allow HTTP traffic
- Allow HTTPS traffic

- XII. Once all values are selected as per the need, navigate to the bottom and click on "CREATE" to create a new VM.

Advanced options ▾
Networking, disks, security, management, sole-tenancy

CREATE CANCEL [EQUIVALENT CODE](#)

- XIII. It will open a new window of VM Instances where you can find your newly created VM with IPs (hidden for secrecy).

VM instances

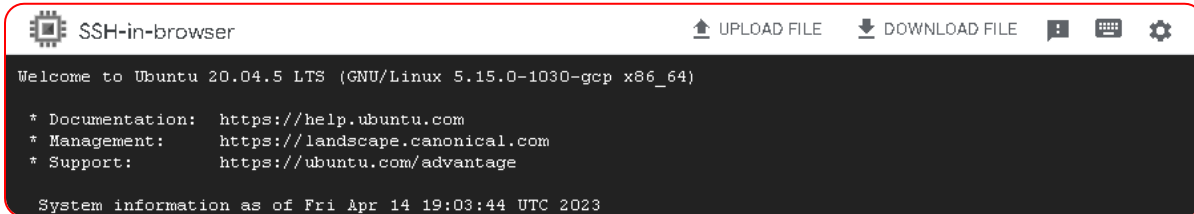
Filter Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	◀	ubuntu	us-west4-b					SSH ▾ ⋮

- XIV. Your VM is now ready to be used, and you can use SSH to connect to it.

b. Installing Snort IDS on VM

- I. Click on SSH option to start using it. It will open a new browser tab and establish a connection with the VM.



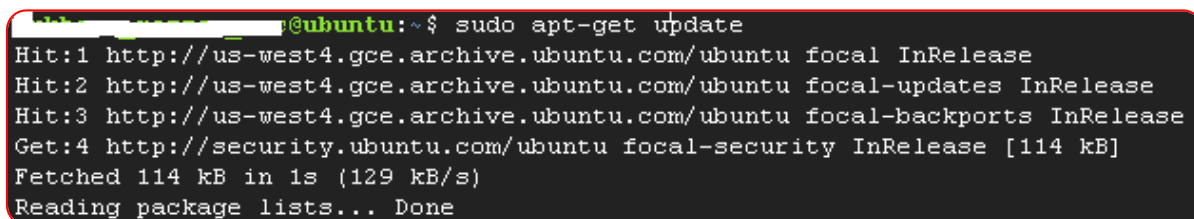
```
SSH-in-browser  UPLOADED FILE  DOWNLOADED FILE  [Icons]

Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1030-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

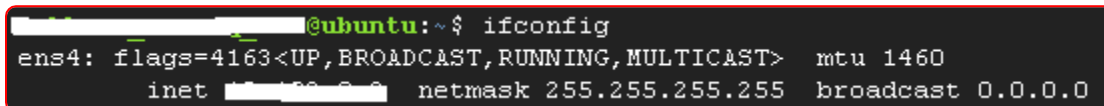
System information as of Fri Apr 14 19:03:44 UTC 2023
```

- II. Now, you can use it as a simple Ubuntu terminal. First, update the packages using the command "sudo apt-get update".



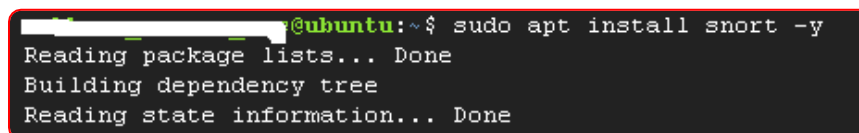
```
@ubuntu:~$ sudo apt-get update
Hit:1 http://us-west4.gce.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us-west4.gce.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://us-west4.gce.archive.ubuntu.com/ubuntu focal-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Fetched 114 kB in 1s (129 kB/s)
Reading package lists... Done
```

- III. Snort installation will ask to enter an interface, so it is better to first check the interface using the ifconfig command.
 - a. Note the IP address of the interface that you want to use for monitoring traffic. In this case, we will use **X.X.X.X**

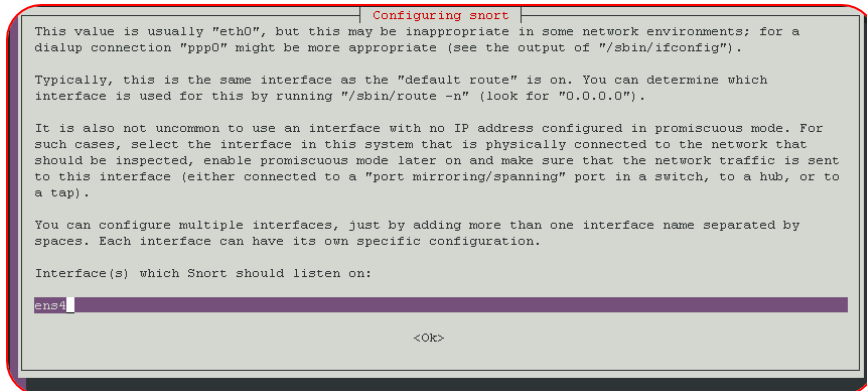


```
@ubuntu:~$ ifconfig
ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
    inet X.X.X.X netmask 255.255.255.255 broadcast 0.0.0.0
```

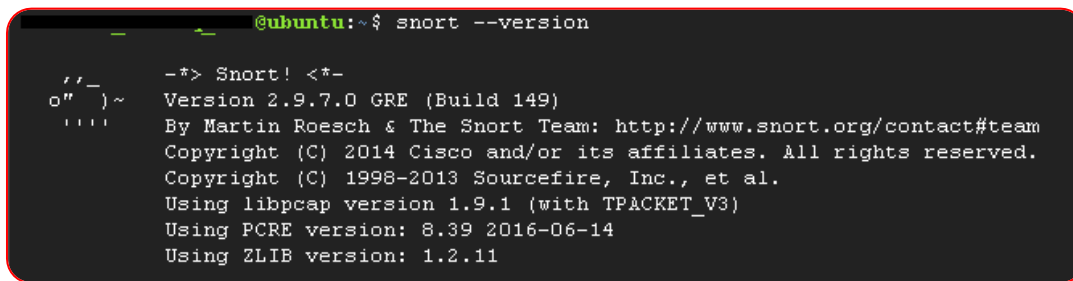
- IV. Now use command "sudo apt install snort -y" to install the Snort IDS.



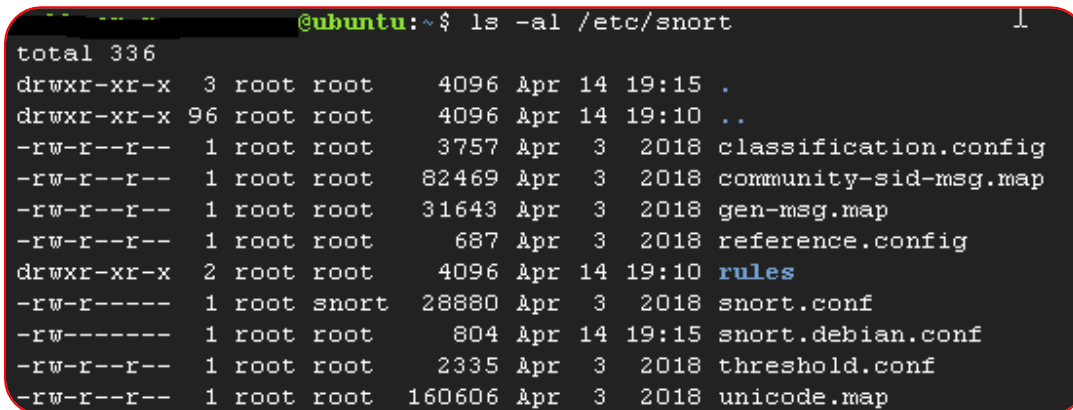
```
@ubuntu:~$ sudo apt install snort -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```



- V. After installation is complete, use the command shown in the image below to check the version of Snort.



- VI. Snort is installed in the /etc/snort/ directory, and all of its files and folders are placed in there. To check them, use the command below:



- a. In these files, **snort.conf** is the most important file which allows enabling and disabling rules, changing the mode of Snort, etc.
- VII. Let's open (using the command "`sudo nano /etc/snort/snort.conf`") the **snort.conf** file and change the HOME_NET address. This is the value that makes Snort either Host-based IDS or Network-based IDS. By default, it is set to any, which means Snort inspects all of the traffic in that particular subnet in which it is installed. If you want to modify it so it only inspects a single device, then modify the highlighted value from any to IP (or IP range).


```
GNU nano 4.8 /etc/snort/snort.conf
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any
```

- VIII. By default, most of the rules of Snort are enabled that detect intrusions. If you want to create custom rules, that can also be done under the rules directory.
- IX. Now, let's start Snort, but before we start it, it is best practice to always test for errors after making changes to the config file. Use this command **sudo snort -T -i ens4 -c /etc/snort/snort.conf** to test for successful compilation of Snort.

```
Snort successfully validated the configuration!
Snort exiting
```

- X. So, if validation of configurations is successful, now let's start the Snort IDS. Use the following command "**sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens4**"
 - **-A console**: When you choose the 'console' option, alerts concerning fast mode will be sent to the stdout stream.
 - **-q**: This is the silent mode, in which both the banner and the status report will not be shown.
 - **-u snort**: After the operating system has finished booting up, you should execute Snort as the following user.
 - **-g snort**: After the computer has finished booting up, you should start Snort while logged in as the following group.
 - **-c /etc/snort/snort.conf**: We are able to define the path of our snort.conf file by using this flag.
 - **-i ens4**: The medium that one might use in order to listen on (change to your interface if different).

```
@ubuntu:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens4
```

- XI. After running the command, Snort will start looking for intrusions.
 - i. To detect ICMP (used for ping) packets, follow these steps:
- XII. To begin, access any system and ping the IP address, preferably the public IP address displayed under "External IP".

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
☑	ubuntu	us-west4-b			(nic0)	(nic0)	SSH

```
C:\Users\PsychicPowers>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=292ms TTL=59
Reply from 10.0.0.4: bytes=32 time=290ms TTL=59
Reply from 10.0.0.4: bytes=32 time=291ms TTL=59
```

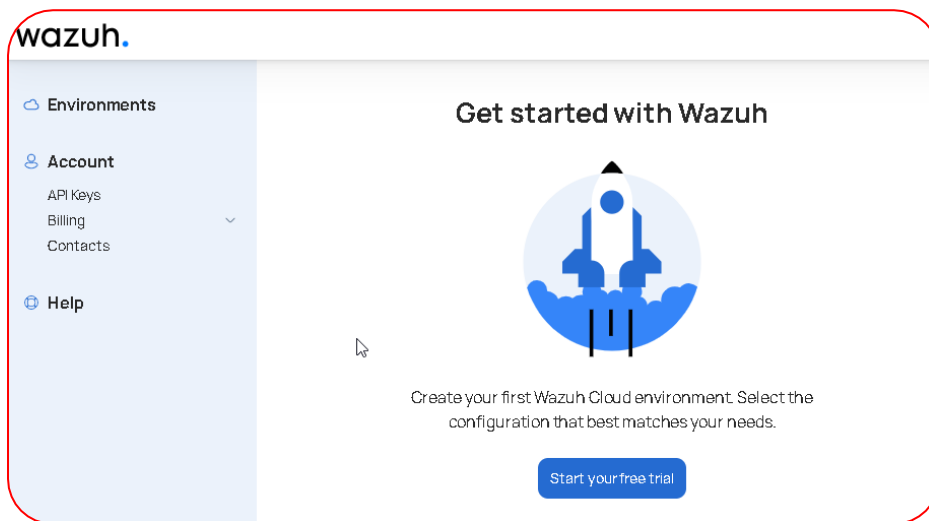
XIII. Check the SNORT console, and you will see that it has successfully detected the ICMP packets.

```
04/14-19:40:35.681273 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] (ICMP)
04/14-19:40:35.681273 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] (ICMP)
```

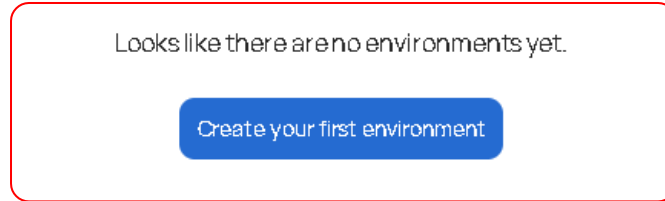
c. Wazuh Integration

i. To access WAZUH SIEM, follow these steps:

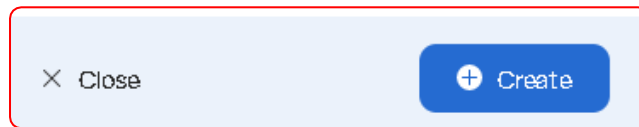
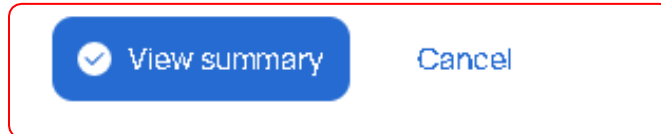
- i. Go to <https://console.cloud.wazuh.com/>.
- ii. Click on the "SIGN UP" button.
- iii. Enter the necessary details and verify your email.
- iv. After verification, log in to your account.



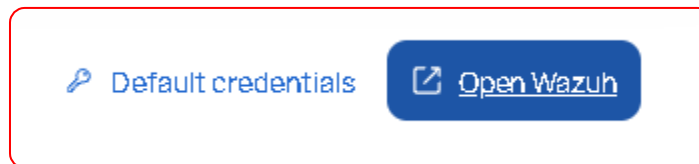
v. Click on "Environments" to create a new environment.



- vi. Add the environment's name and choose a tier, such as 100 GB.
- vii. Select the region and fill in other details.
- viii. Click on the "View Summary" button at the bottom and then on the "Create" button.



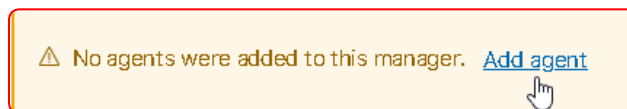
- ix. The new environment will be created, and you can access the main dashboard by clicking on the "Open Wazuh" button on the top left corner of the screen.



- x. Enter the default credentials by clicking on the "Default Credentials" button located alongside the "Open Wazuh" button.

ii. To add an agent, follow these steps:

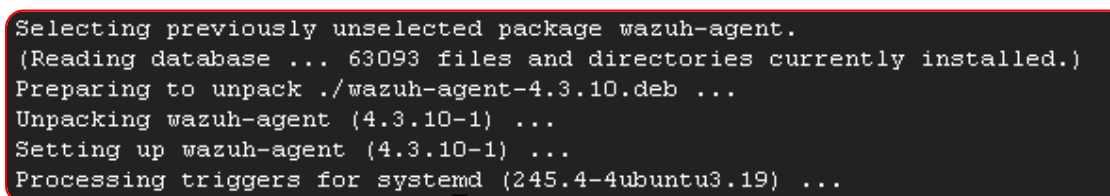
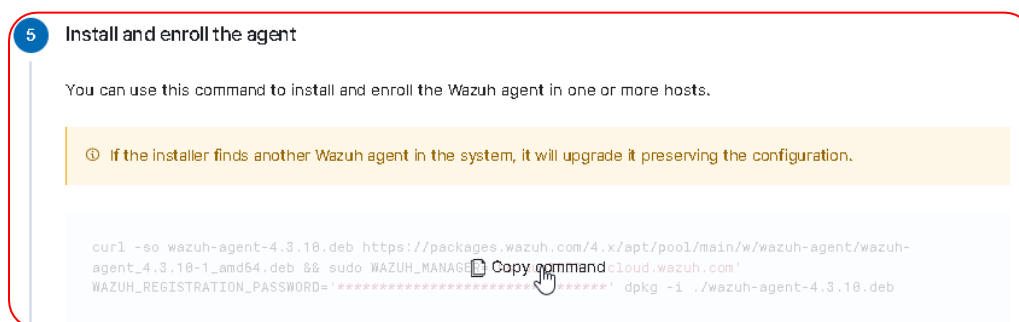
- i. Click on the "Add agent" link displayed on the main dashboard.



- ii. Select the operating system on which you want to install the agent and select its architecture.



- iii. Copy the command shown at step-5 of Wazuh agent installation windows and paste it into the terminal of the Ubuntu GCP VM to install the Wazuh agent.



- iv. Follow step-6 to start the agent in Ubuntu by entering the provided commands.



- v. Use the "status" command to check if the Wazuh agent is working in Ubuntu.

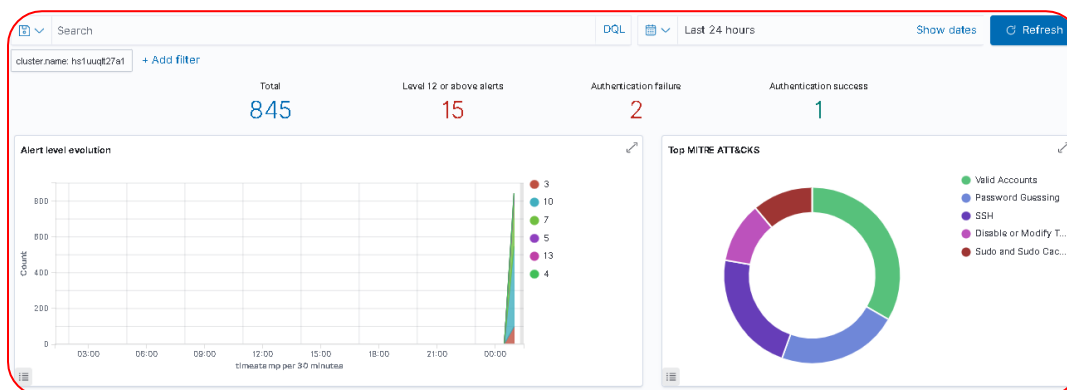
```
@ubuntu:~$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor
   Active: active (running) since Fri 2023-04-14 20:12:45 UTC; 17s ago
   Process: 17730 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start
```

- vi. After starting the Wazuh agent, proceed to verify the Wazuh dashboard by taking the following steps:
- a. Access the updated dashboard.



- vii. Reactivate the SNORT IDS and proceed to perform a ping or SSH connection. Observe that the statistics for these actions are updated in the SIEM dashboard.

```
C:\Users\PsychicPowers>ssh -i .ssh\id_rsa root@192.168.1.100
psychicpowers@192.168.1.100: Permission denied (publickey).
```



With this successful integration of SIEM Wazuh with GCP VM, intrusions are detected by Snort installed on the VM, and their corresponding events are displayed on the Wazuh dashboard.