

In this documentation, we detail the deployment of the Wazuh Security Information and Event Management (SIEM) solution using the official assisted installation method. The deployment is carried out on a single Ubuntu server hosted on Google Cloud Platform (GCP), where the three core components Wazuh Indexer, Wazuh Server, and Wazuh Dashboard are installed on the same machine. This setup is ideal for testing environments or small-scale production deployments, allowing users to quickly implement Wazuh with minimal configuration. Throughout this documentation, each step of the installation process is explained in detail, including configuration guidelines, command examples, and best practices to ensure a smooth and successful deployment.

Use Case

- **Lab or Testing Setup** Good for setting up **Wazuh** in a test environment to learn how it works and try out its features.
- **Home SOC Practice** Ideal for building a small home lab to practice monitoring, detecting threats, and analyzing security logs.
- **Trying Out Wazuh Before Full Setup** Useful if you just want to see how Wazuh works before using it in a bigger or real company environment.

Why GCP?


Google Cloud Platform (GCP) is a powerful and flexible cloud provider that offers scalable virtual machines for different needs. For this lab setup, GCP makes it easy to deploy and test **Wazuh on demand**, giving you full control over the infrastructure while keeping costs predictable.

One of the biggest advantages is that **GCP offers a \$300 free credit valid for 90 days** when you sign up. This is perfect for setting up and running your Wazuh lab environment without any upfront cost—ideal for students, professionals, or anyone experimenting with security tools.

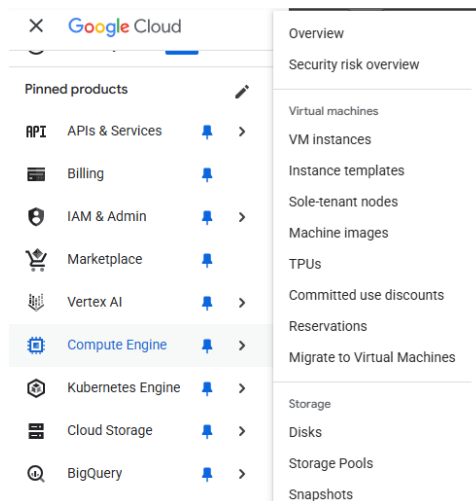
Step 1: Infrastructure Preparation

Create a Virtual Machine (VM) on GCP

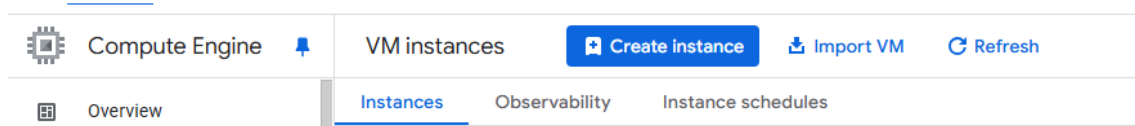
Follow these steps to create a virtual machine that will host your Wazuh environment:

1. Log in to GCP Console Go to the Google Cloud Console at: 
<https://console.cloud.google.com>

2. Access VM Instances In the left-hand menu, navigate to: **Compute Engine** → **VM Instances**



3. Click on “Create Instance” This will open the configuration screen for a new VM.



4. Configure Your VM

- **Name:** wazuh (you can choose any name, but wazuh keeps it organized)
- **Region:** us-central1-c (Selected for **E2 machine type** availability and **lower cost** compared to other regions. Ideal for budget-friendly lab setups.)
- **Machine type:** e2-medium (includes 2 vCPUs and 4 GB RAM, which is suitable for basic or lightweight single-node Wazuh deployments)
- **Boot Disk:**

Basic information

Name	bd-conector
Instance Id	
Description	None
Type	Instance
Status	✓ Running
Creation time	Aug 14, 2025, 8:32:09 AM UTC-05:00
Location ?	us-central1-a
Boot disk source image	ubuntu-2404-noble-amd64-v20250805

5. Allow Firewall Access Under the **Firewall** section, make sure to check both:

- Allow HTTP traffic
- Allow HTTPS traffic

To allow external access to Wazuh services (such as the dashboard and agent communication), you’ll need to create a firewall rule in GCP.

6.Navigate to the Firewall Section Go to **VPC Network → Firewall** in the Google Cloud Console.

Firewall policies

[+ Create firewall policy](#)

[+ Create firewall rule](#)

7.Click “Create Firewall Rule” This will open the configuration page to define your custom firewall rule.

Fill in the following details:

Name: allow-wazuh-services

Network: default (or the VPC you're using)

Targets: All instances in the network

Source IP Ranges: 0.0.0.0/0 (for public access)

Protocols & Ports: Check "Specified protocols and ports", then add:

- tcp:443

- tcp:9200

- tcp:1514

- udp:1514

- tcp:1515

- tcp:514 (optional if you are going to receive data from an external source to Wazuh)

This will allow you to access the Wazuh web interface and other services later.

8.Click “Create” Once the VM is configured, click the **Create** button at the bottom to launch your virtual machine.After the VM is ready, you’ll be able to **SSH into it directly** from the browser or by using the gcloud CLI to begin installing Wazuh.

Now that the infrastructure is ready, let's begin our Wazuh deployment

Step 2: Set Up the Servers

1. Initial Configuration (Single-Node Setup)

```
ssh root@inderex.ip
```

Download Wazuh Installation Assistant and Configuration File

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
```

```
curl -sO https://packages.wazuh.com/4.12/config.yml
```

```
chmod +x wazuh-install.sh
```

1. What does curl do

- curl is a command-line tool used to download files from the Internet.
- The -s option means **silent** → it runs without showing progress.
- The -O option means save with the same name as the remote file.

2. Files that are downloaded

1. wazuh-install.sh

- It is an automatic installation script.
- It handles the installation of the main Wazuh components: **Indexer**, **Wazuh Server**, and **Dashboard**.

2. config.yml

- It is a configuration file that defines:
 - Node names
 - IP addresses
 - Components to be installed
- You must edit it before installation if you need to customize the setup (for example, change the IP address or node name).

Edit the configuration file

nano ./config.yml

```
nodes:
# Wazuh indexer nodes
indexer:
  - name: node-1
    ip: "10.128.0.6"
  #- name: node-2
  # ip: "<indexer-node-ip>"
  #- name: node-3
  # ip: "<indexer-node-ip>"

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
  - name: wazuh-1
    ip: "10.128.0.6"
    # node_type: master
  #- name: wazuh-2
  # ip: "<wazuh-manager-ip>"
  # node_type: worker
  #- name: wazuh-3
  # ip: "<wazuh-manager-ip>"
  # node_type: worker

# Wazuh dashboard nodes
dashboard:
  - name: dashboard
    ip: "10.128.0.6"
```

Update the name and IP address of the nodes for the Wazuh indexer, server, and dashboard as shown in the previous snippet. Since I am using a single-node setup, I have assigned the same internal IP address to all components Wazuh manager, indexer, and dashboard. If you are using a multi-node configuration, make sure to assign the corresponding IP address to each component.

Generate SSL Certificates and Passwords

```
bash wazuh-install.sh --generate-config-files
```

The command `bash wazuh-install.sh --generate-config-files` creates the SSL certificates, cluster key, and secure passwords required for secure communication between the Wazuh components. It prepares everything necessary before starting the installation.

2. Install All Wazuh Components

Install Wazuh Indexer

```
bash wazuh-install.sh --wazuh-indexer node-1
```

This installs OpenSearch (the Wazuh indexer) to store and manage security data.

It sets up secure communication and indexing for Wazuh alerts.

Initialize the Cluster Security:

```
sudo bash wazuh-install.sh --wazuh-indexer node-1 --start-cluster
```

This command configures the internal users, keys, and SSL certificates required for secure communication between the Dashboard and the Indexer.

Install the Wazuh Server

```
bash wazuh-install.sh --wazuh-server wazuh-1
```

This installs the Wazuh Manager, which collects and analyzes logs from the agents.

It connects to the Indexer to send processed alerts and events.

Install the Wazuh Dashboard

```
bash wazuh-install.sh --wazuh-dashboard dashboard
```

This installs the Wazuh web interface used to view alerts, logs, and configurations.

It connects to the Indexer and the Wazuh API to display real-time data.

Once the installation is complete, the output shows the login credentials and a confirmation message indicating that the installation was successful.

```
INFO: --- Summary ---
```

```
INFO:      You      can      access      the      web      interface  
https://<WAZUH_DASHBOARD_IP_ADDRESS>
```

```
User: admin
```

```
Password: <ADMIN_PASSWORD>
```

```
INFO: Installation finished.
```

1. Verify that the services are active:

```
sudo systemctl status wazuh-manager
```

```
sudo systemctl status wazuh-indexer
```

```
sudo systemctl status wazuh-dashboard
```