**ISS Technologies**

**Document Name: Wazuh Cluster Setup on VMs**

**Version No: 1.0**

**Created by: Ram Moahan**

**Reviewed & Approved by: Sasidhar.**

**Version Control:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description of change** | **Prepared by** | **Reviewed and Approved by** |
| **07/03/2025** | **1.0** | **Original – created** | **Ram Mohan** | **Sasidhar B** |

**Prerequisites**

1. **Three Virtual Machines**:

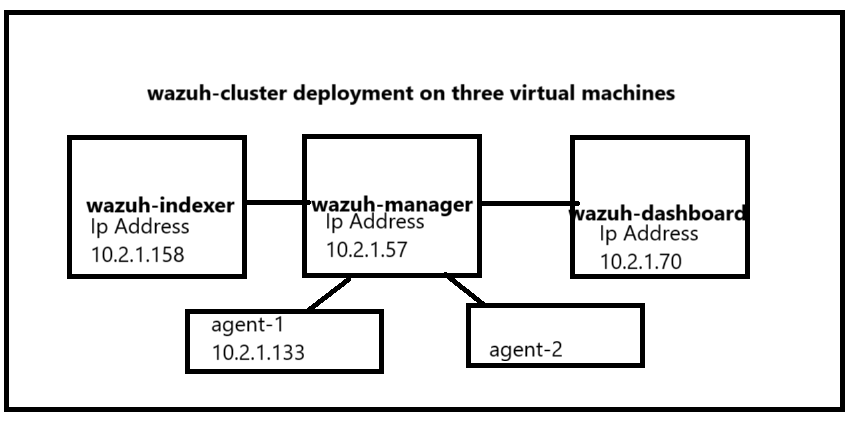
* VM1: Wazuh Indexer
* VM2: Wazuh Manager
* VM3: Wazuh Dashboard
* Ensure each VM has network connectivity and can communicate with the others.

1. **System Requirements** (minimum for small-scale deployment):

* 4 GB RAM per VM (8 GB recommended for production).
* 2 CPU cores per VM.
* At least 20 GB of disk space per VM (more for production based on alert volume).

1. **Operating System**: A supported 64-bit Linux OS (e.g., Ubuntu 20.04).
2. **Root Access**: You’ll need root or sudo privileges on all VMs.
3. **Network Configuration**:

* VM1 (Indexer): e.g., 10.2.1.158
* VM2 (Manager): e.g., 10.2.1.57
* VM3 (Dashboard): e.g., 10.2.1.70



**Step 1: Prepare Certificates for Secure Communication**

Since the components will run on separate VMs, you need to generate and distribute SSL certificates to secure communication between them. Perform this step on one VM (e.g., VM3) and then copy the certificates to the others.

**1. Certificates creation**

*curl -sO https://packages.wazuh.com/4.11/wazuh-certs-tool.sh*

*curl -sO https://packages.wazuh.com/4.11/config.yml*

**Edit the config.yml File**: Open config.yml in a text editor (e.g., nano config.yml) and update it with your VM details:

nodes:

  # Wazuh indexer nodes

  indexer:

    - name: node-1

      ip: "<indexer-node-ip>"

    #- 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: "<wazuh-manager-ip>"

    #  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: "<dashboard-node-ip>"

Save and exit.

**Generate Certificates**: Run the certificate tool:

*bash wazuh-certs-tool.sh*

This creates a wazuh-certificates.tar file containing the certificates.

**Compress all the necessary files**

*tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .*

*rm -rf ./wazuh-certificates*

**Distribute Certificates**: Copy wazuh-certificates.tar to VM1 and VM2 using scp or another method:

*scp wazuh-certificates.tar w-server@1o.2.1.57:/home/w-server/*

*scp wazuh-certificates.tar dashboard@10.2.1.70:/home/dashboard/*

Shape

**Step 2: Install Wazuh Indexer on VM1**

The Wazuh Indexer stores and indexes alerts generated by the Wazuh Manager.

1. **Add the Wazuh Repository**:

*apt-get install gnupg apt-transport-https*

*curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -*

*echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list*

*sudo apt-get update*

(For CentOS, use rpm --import and edit /etc/yum.repos.d/wazuh.repo as per the documentation.)

1. **Install Wazuh Indexer**:

*sudo apt-get install wazuh-indexer*

1. **Configure Wazuh Indexer**: *Edit /etc/wazuh-indexer/opensearch.yml:*

*network.host: "10.2.1.158"  # VM1 IP*

*node.name: "indexer-1"*

*cluster.initial\_master\_nodes:*

*- "indexer-1"*

Ensure certificates are in place:

*NODE\_NAME=<INDEXER\_NODE\_NAME>*

*mkdir /etc/wazuh-indexer/certs*

*tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem*

*mv -n /etc/wazuh-indexer/certs/$NODE\_NAME.pem /etc/wazuh-indexer/certs/indexer.pem*

*mv -n /etc/wazuh-indexer/certs/$NODE\_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem*

*chmod 500 /etc/wazuh-indexer/certs*

*chmod 400 /etc/wazuh-indexer/certs/\**

*chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs* ***Start Wazuh* Indexer**:

*sudo systemctl daemon-reload*

*sudo systemctl enable wazuh-indexer*

*sudo systemctl start wazuh-indexer*

Verify it’s running:

*sudo systemctl status wazuh-indexer*

Execute the following command to disable the Wazuh repository:

*sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list*

*apt update*

**Cluster initialization**

*/usr/share/wazuh-indexer/bin/indexer-security-init.sh*

***Testing the cluster installation***

*curl -k -u admin:admin https://<WAZUH\_INDEXER\_IP\_ADRESS>:9200*

**Step 3: Install Wazuh Manager on VM2**

The Wazuh Manager analyzes data from agents and forwards alerts to the Indexer.

1. **Add the Wazuh Repository**: (Same as above for VM1.)
2. **Install Wazuh Manager**:

*sudo apt-get install wazuh-manager*

1. **Install Filebeat**: Filebeat forwards alerts to the Indexer:

*sudo apt-get install filebeat*

1. **Configure Filebeat**: Download the preconfigured Filebeat config:

*curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.x/tpl/wazuh/filebeat/filebeat.yml*

*Edit /etc/filebeat/filebeat.yml:*

output.elasticsearch:

*hosts: ["192.168.1.101:9200"]  # VM1 IP*

*username: "admin"*

*password: "<indexer-admin-password>"  # Default from installation or set manually*

Add certificates:

*mkdir /etc/filebeat/certs*

*tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./root-ca.pem*

*mv -n /etc/filebeat/certs/$NODE\_NAME.pem /etc/filebeat/certs/filebeat.pem*

*mv -n /etc/filebeat/certs/$NODE\_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem*

*chmod 500 /etc/filebeat/certs*

*chmod 400 /etc/filebeat/certs/\**

*chown -R root:root /etc/filebeat/certs*

***Configuring the Wazuh indexer connection***

*echo '<INDEXER\_USERNAME>' | /var/ossec/bin/wazuh-keystore -f indexer -k username*

*echo '<INDEXER\_PASSWORD>' | /var/ossec/bin/wazuh-keystore -f indexer -k password*

*vim /var/ossec/etc/ossec.conf*

*give the public ip address of vazuh indexer*

*/etc/filebeat/filebeat.yml*

*Replace 0.0.0.0 with your Wazuh indexer node IP address*

***Starting the Wazuh manager***

*systemctl daemon-reload*

*systemctl enable wazuh-manager*

*systemctl start wazuh-manager*

**5.Start Services**:

systemctl daemon-reload

systemctl enable filebeat

systemctl start filebeat

filebeat test output

Execute the following command to disable the Wazuh repository:

*sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list*

*apt update*

**Step 4: Install Wazuh Dashboard on VM3**

The Wazuh Dashboard provides the web interface for visualization and management.

1. **Add the Wazuh Repository**: (Same as above for VM1.)

*apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later*

*apt-get install gnupg apt-transport-https*

*curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg*

*echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list*

*apt-get update*

1. **Install Wazuh Dashboard**:

sudo apt-get install wazuh-dashboard -y

**Configuring the Wazuh dashboard**

/etc/wazuh-dashboard/opensearch\_dashboards.yml

*server.host: 0.0.0.0*

*server.port: 443*

*opensearch.hosts: https://localhost:9200*

*opensearch.ssl.verificationMode: certificate*

*replace local host with indexer ip*

***Deploying certificates***

*NODE\_NAME=<DASHBOARD\_NODE\_NAME>*

*mkdir /etc/wazuh-dashboard/certs*

*tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./root-ca.pem*

*mv -n /etc/wazuh-dashboard/certs/$NODE\_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem*

*mv -n /etc/wazuh-dashboard/certs/$NODE\_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem*

*chmod 500 /etc/wazuh-dashboard/certs*

*chmod 400 /etc/wazuh-dashboard/certs/\**

*chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs*

***Starting the Wazuh dashboard service***

*systemctl daemon-reload*

*systemctl enable wazuh-dashboard*

*systemctl start wazuh-dashboard*

Edit */usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml*

hosts:

   - default:

      url: https://<WAZUH\_SERVER\_IP\_ADDRESS>

      port: 55000

      username: wazuh-wui

      password: wazuh-wui