Wazuh Security Monitoring Platform

Complete installation and configuration guide for Wazuh - Open source security monitoring solution.

Table of Contents

Overview

Wazuh is a free, open source security monitoring solution that provides:
- Intrusion detection
- Log data analysis
- File integrity monitoring
- Vulnerability detection
- Configuration assessment
- Incident response
- Regulatory compliance

Architecture

[Wazuh Agents] → [Wazuh Server] → [Elastic Stack]
↓ ↓ ↓
[Endpoints] [Management] [Dashboard & Visualization]

Prerequisites

Hardware Requirements:

- Wazuh Server: 8GB RAM, 4 CPU cores, 50GB storage minimum
- Elasticsearch Node: 8GB RAM, 4 CPU cores, 100GB storage minimum
- Network: Stable connectivity between components

Software Requirements:
- OS: CentOS 7/8, RHEL 7/8, Ubuntu 16.04/18.04/20.04, Amazon Linux 2
- Docker (for containerized deployment)
- Python 3.x
- curl and tar utilities

Installation Methods

Method 1: All-in-One Installation (Quick Start)

```
curl -so wazuh-install.sh https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh --generate-config-files
sudo bash wazuh-install.sh --wazuh-indexer --wazuh-server --wazuh-dashboard
--start-cluster
```

Method 2: Single Node Installation

Step 1: Install Wazuh Indexer
```
apt install wazuh-indexer
systemctl enable wazuh-indexer
systemctl start wazuh-indexer
```

Step 2: Install Wazuh Server
```
apt install wazuh-manager
systemctl enable wazuh-manager
systemctl start wazuh-manager
```

Step 3: Install Wazuh Dashboard
```
apt install wazuh-dashboard
systemctl enable wazuh-dashboard
systemctl start wazuh-dashboard
```

Method 3: Docker Installation

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.7.0
cd wazuh-docker
docker-compose -f generate-indexer-certs.yml run --rm generator
docker-compose up -d
```

Distributed Deployment

Multi-Node Cluster Setup

Indexer Cluster Nodes: Configure opensearch.yml for clustering
Manager Cluster Nodes: Configure ossec.conf cluster section

Agent Deployment

Linux Agents
---
curl -so wazuh-agent-4.7.0.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.0-1_amd64.deb
sudo WAZUH_MANAGER='wazuh-server-ip' dpkg -i wazuh-agent-4.7.0.deb
systemctl enable wazuh-agent
systemctl start wazuh-agent

Windows Agents

Invoke-WebRequest -Uri "https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.0-1.msi" -OutFile "wazuh-agent.msi"
msiexec.exe /i wazuh-agent.msi /q WAZUH_MANAGER="wazuh-server-ip" WAZUH_REGISTRATION_SERVER="wazuh-server-ip"

macOS Agents
---
curl -o wazuh-agent-4.7.0.pkg https://packages.wazuh.com/4.x/macos/wazuh-agent-4.7.0-1.pkg
sudo installer -pkg wazuh-agent-4.7.0.pkg -target /
sudo /Library/Ossec/bin/wazuh-control set-manager wazuh-server-ip

Configuration

Wazuh Manager (/var/ossec/etc/ossec.conf)
---

yes
admin@yourcompany.com
smtp.yourcompany.com
wazuh@yourcompany.com

Elasticsearch (/etc/wazuh-indexer/opensearch.yml)

```
------------------------------------------------
cluster.name: wazuh-indexer
node.name: wazuh-indexer-1
network.host: 0.0.0.0
discovery.type: single-node
```

Usage

```
Access Dashboard
----------------
URL: https://your-server-ip:5601
Username: admin
Password: admin

Management Commands
-------------------
systemctl status wazuh-manager
systemctl restart wazuh-manager
/var/ossec/bin/agent_control -l
systemctl restart wazuh-agent
```

Monitoring

```
Health Check
------------
systemctl is-active wazuh-manager
systemctl is-active wazuh-indexer
systemctl is-active wazuh-dashboard

Log Monitoring
--------------
tail -f /var/ossec/logs/ossec.log
tail -f /var/ossec/logs/active-responses.log
tail -f /var/log/wazuh-indexer/wazuh-indexer.log
```

Troubleshooting

```
Connection Issues
-----------------
iptables -L
telnet wazuh-server-ip 1514

Certificate Issues
```

/usr/share/wazuh-indexer/bin/indexer-security-init.sh
openssl x509 -in /etc/wazuh-indexer/certs/admin.pem -text -noout

Performance Issues
---
top
df -h
curl -k -u admin:admin https://localhost:9200/_cat/indices?v

Maintenance

Backup
---
tar -czf wazuh-backup-$(date +%Y%m%d).tar.gz /var/ossec/etc/ /etc/wazuh-indexer/

Update
---
apt update
apt install wazuh-manager wazuh-indexer wazuh-dashboard
systemctl restart wazuh-manager wazuh-indexer wazuh-dashboard

Log Rotation
---
logrotate -f /etc/logrotate.d/wazuh

Resources

- Wazuh Documentation: https://documentation.wazuh.com/current/
- GitHub: https://github.com/wazuh
- Community Forum: https://wazuh.com/community/
- Support: https://wazuh.com/support/

License