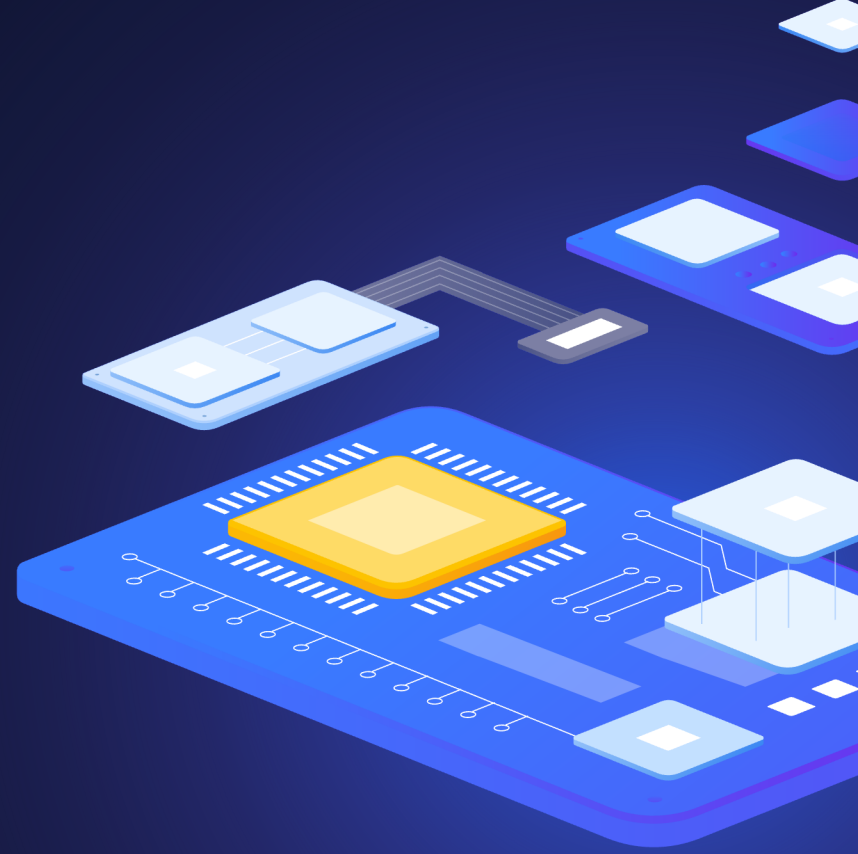
initMAX

Wazuh: Installation & Configuration

all our microphones are muted
ask your questions in Q&A, not in the Chat
use Chat for discussion, networking or applause

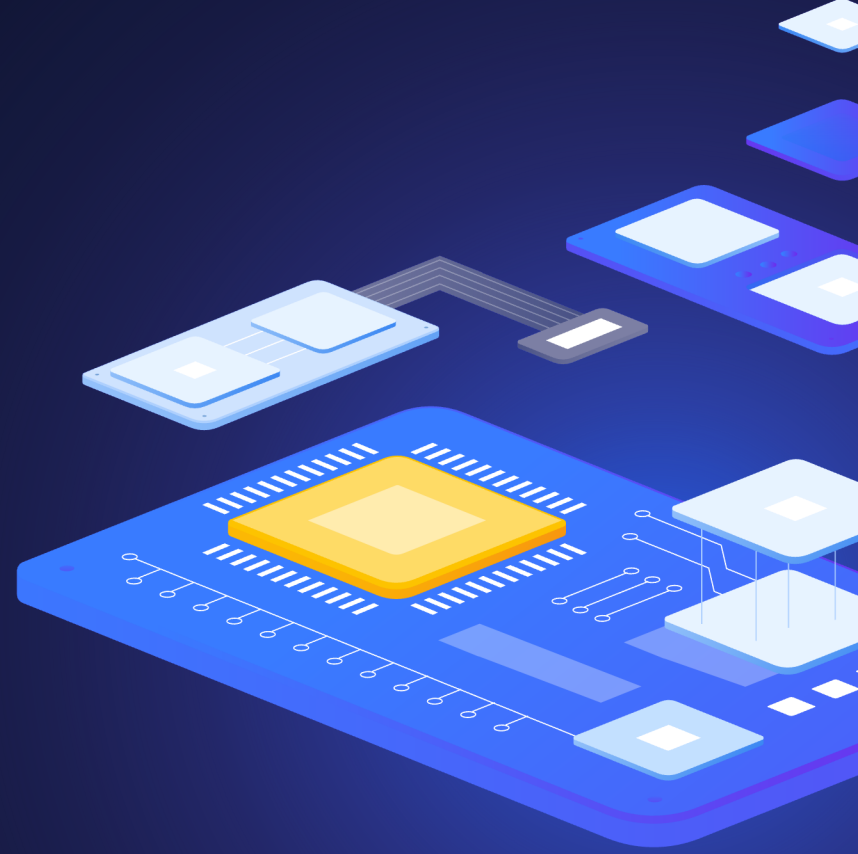
Agenda

1. Intro
2. Wazuh Indexer
3. Wazuh Manager
4. Wazuh Dashboard & Agents
5. Demo



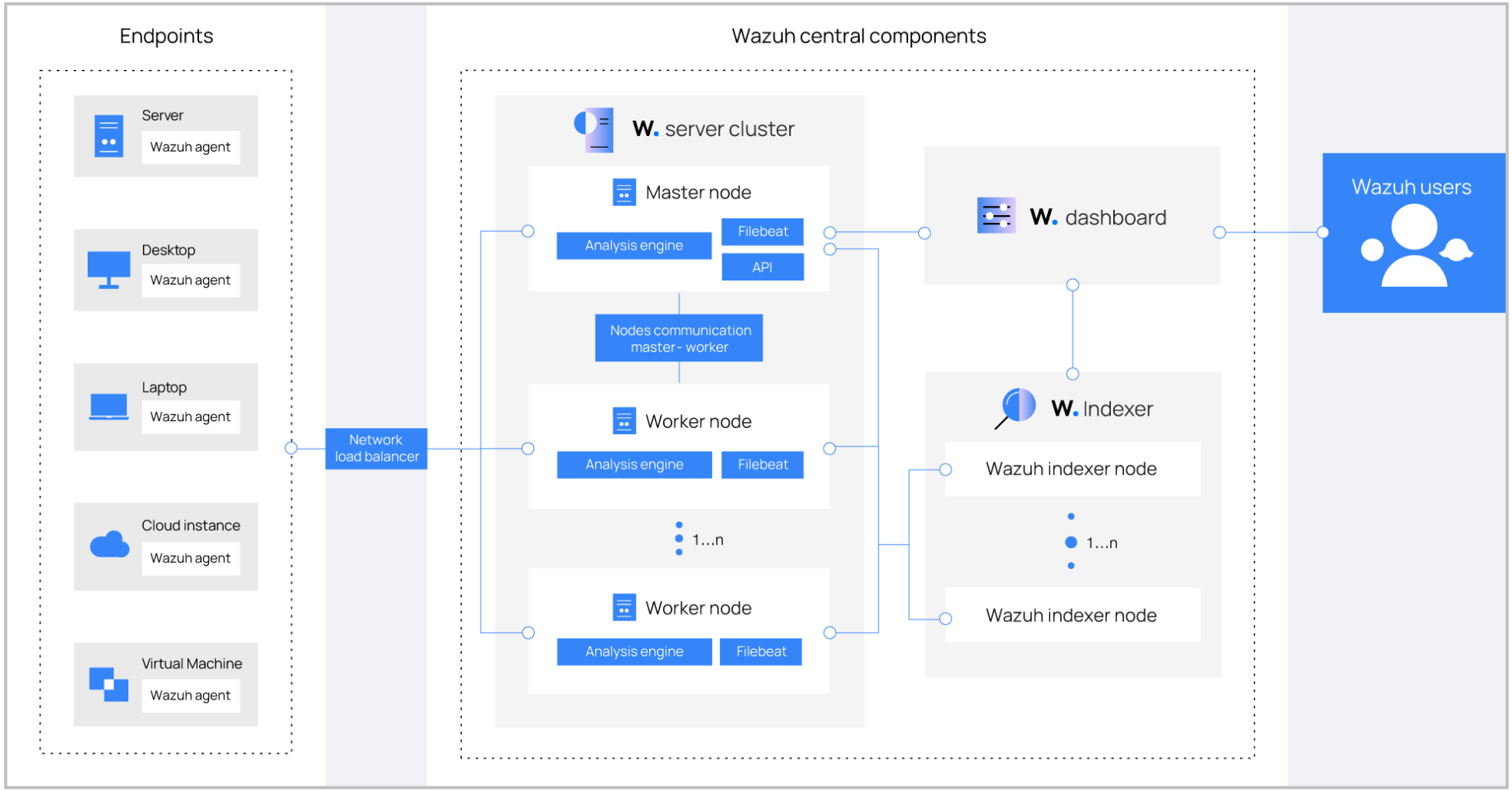
1

Intro



initMAX

Architecture



initMAX

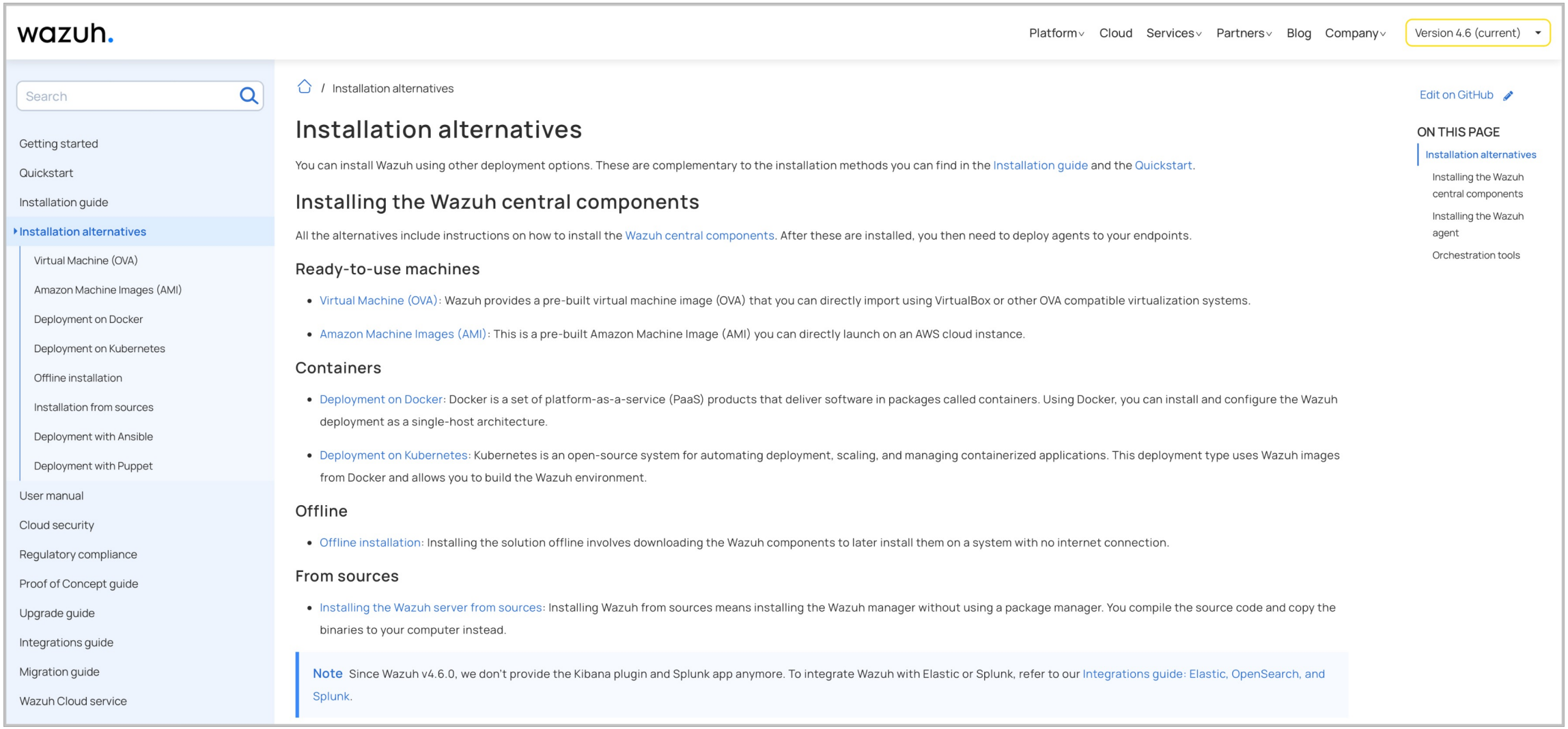
Requirements

- Hardware – all in one
  - The minimum requirements for 25 agents and 90 days of history are as follows:
    - 4 CPU
    - 8 GB RAM
    - 50 GB available disk space – preferably SSD

- Recommended operating systems
  - CentOS 7, 8
  - Red Hat Enterprise Linux 7, 8, 9
  - Amazon Linux 2, Amazon Linux 2023
  - Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

initMAX

Installation alternatives



wazuh.

Platform Cloud Services Partners Blog Company Version 4.6 (current)

Search

Getting started
Quickstart
Installation guide
Installation alternatives
- Virtual Machine (OVA)
- Amazon Machine Images (AMI)
- Deployment on Docker
- Deployment on Kubernetes
- Offline installation
- Installation from sources
- Deployment with Ansible
- Deployment with Puppet

User manual
Cloud security
Regulatory compliance
Proof of Concept guide
Upgrade guide
Integrations guide
Migration guide
Wazuh Cloud service

/ Installation alternatives

Edit on GitHub

ON THIS PAGE
- Installation alternatives
- Installing the Wazuh central components
- Installing the Wazuh agent
- Orchestration tools

Installation alternatives

You can install Wazuh using other deployment options. These are complementary to the installation methods you can find in the Installation guide and the Quickstart.

Installing the Wazuh central components

All the alternatives include instructions on how to install the Wazuh central components. After these are installed, you then need to deploy agents to your endpoints.

Ready-to-use machines

- Virtual Machine (OVA): Wazuh provides a pre-built virtual machine image (OVA) that you can directly import using VirtualBox or other OVA compatible virtualization systems.
- Amazon Machine Images (AMI): This is a pre-built Amazon Machine Image (AMI) you can directly launch on an AWS cloud instance.

Containers

- Deployment on Docker: Docker is a set of platform-as-a-service (PaaS) products that deliver software in packages called containers. Using Docker, you can install and configure the Wazuh deployment as a single-host architecture.
- Deployment on Kubernetes: Kubernetes is an open-source system for automating deployment, scaling, and managing containerized applications. This deployment type uses Wazuh images from Docker and allows you to build the Wazuh environment.

Offline

- Offline installation: Installing the solution offline involves downloading the Wazuh components to later install them on a system with no internet connection.

From sources

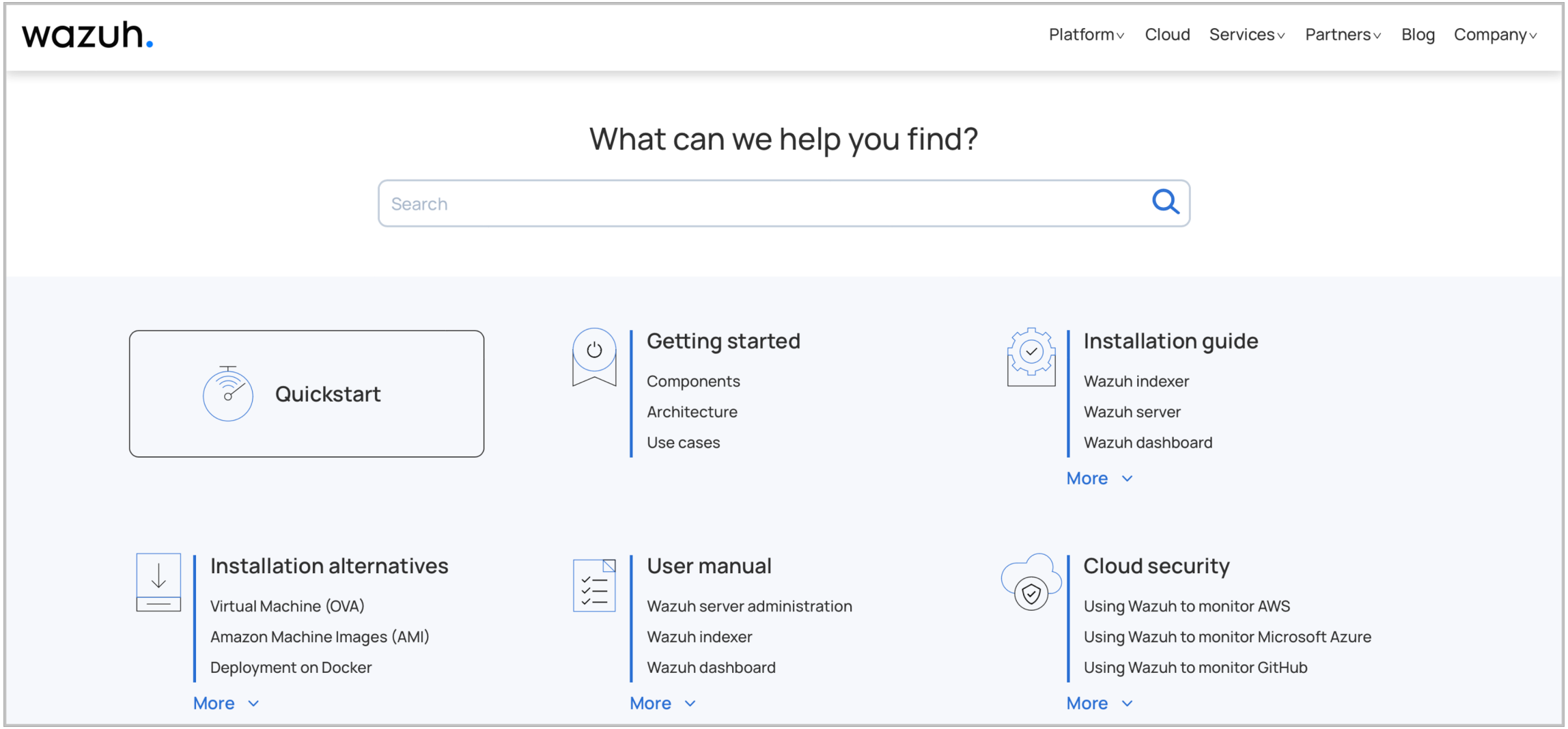
- Installing the Wazuh server from sources: Installing Wazuh from sources means installing the Wazuh manager without using a package manager. You compile the source code and copy the binaries to your computer instead.

Note Since Wazuh v4.6.0, we don't provide the Kibana plugin and Splunk app anymore. To integrate Wazuh with Elastic or Splunk, refer to our Integrations guide: Elastic, OpenSearch, and Splunk.

https://documentation.wazuh.com/current/deployment-options/index.html

initMAX

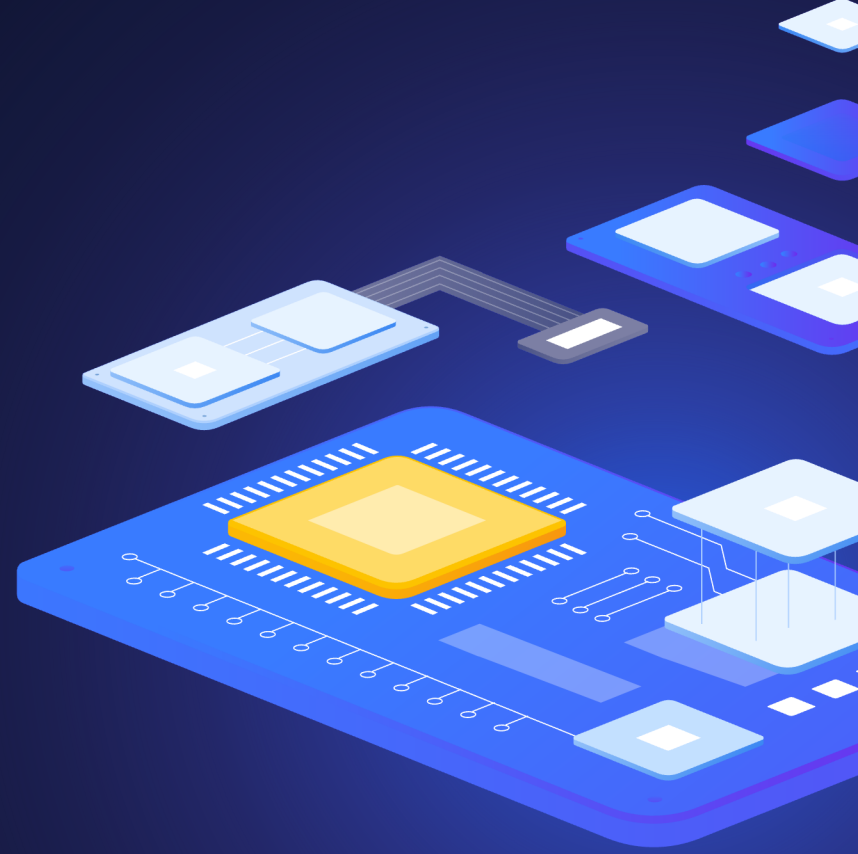
Documentation



https://documentation.wazuh.com/current/index.html

2

Wazuh Indexer



initMAX

Wazuh Indexer

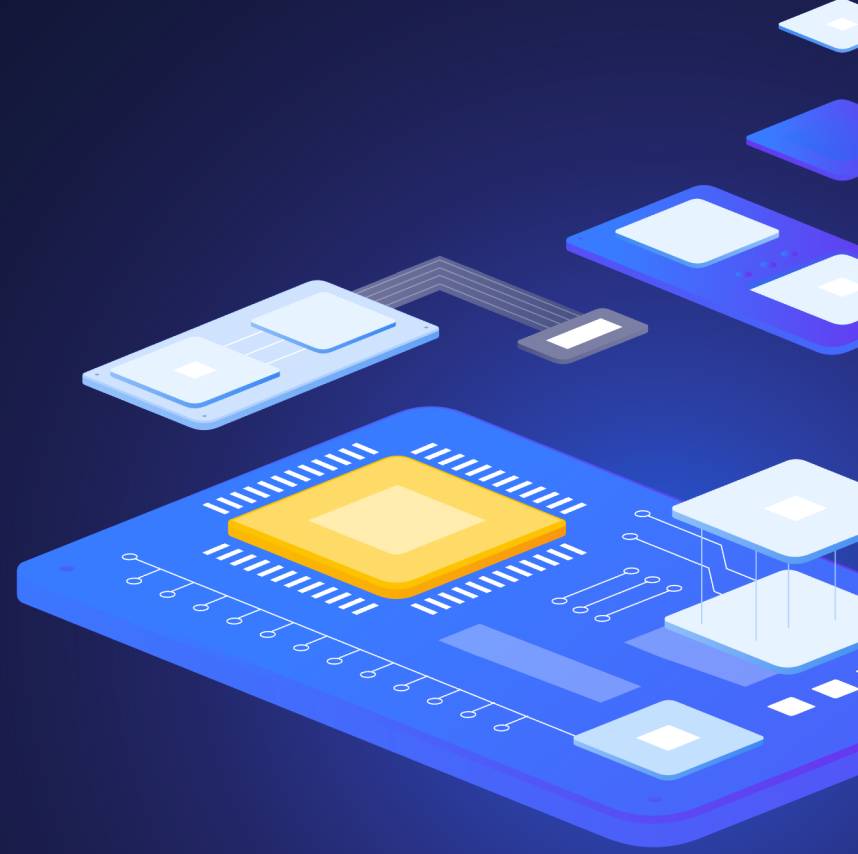
- Hardware recommendations for each node
  - Minimum
    - 2 CPU
    - 4 GB RAM
  - Recommended
    - 8 CPU
    - 16 GB RAM

Monitored endpoints	APS	Storage in Wazuh indexer (GB/90 days)
Servers	0.25	3.7
Workstations	0.1	1.5
Network devices	0.5	7.4

- Disk space requirements
  - The amount of data depends on the generated alerts per second (APS).
  - For example, for an environment with 80 workstations, 10 servers, and 10 network devices, the storage needed on the Wazuh indexer server for 90 days of alerts is 230 GB.

3

Wazuh Manager



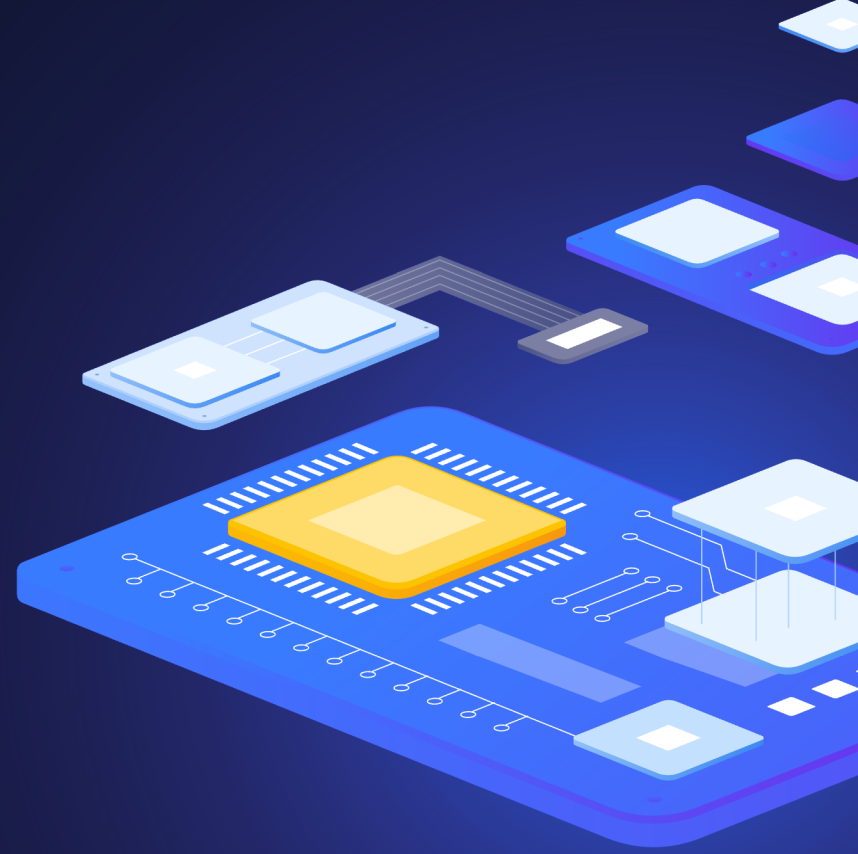
initMAX

Wazuh Manager

- Hardware recommendations for each node
  - Minimum
    - 2 CPU
    - 2 GB RAM
  - Recommended
    - 8 CPU
    - 4 GB RAM

Monitored endpoints	APS	Storage in Wazuh Server (GB/90 days)
Servers	0.25	0.1
Workstations	0.1	0.04
Network devices	0.5	0.2

- Disk space requirements
  - The amount of data depends on the generated alerts per second (APS).
  - For example, for an environment with 80 workstations, 10 servers, and 10 network devices, the storage needed on the Wazuh server for 90 days of alerts is 6 GB.



4

Wazuh Dashboard & Agents

initMAX

Wazuh Dashboard

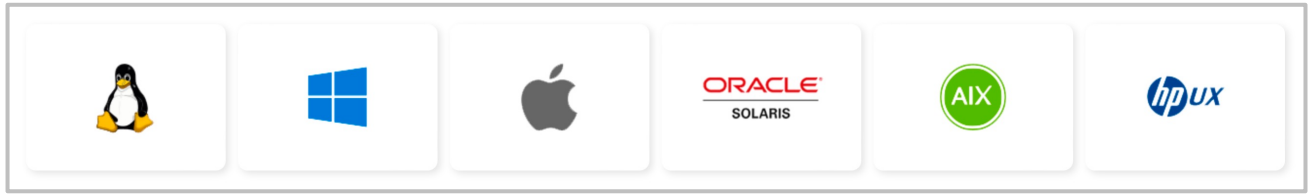
- Hardware recommendations for each node
  - Minimum
    - 2 CPU
    - 4 GB RAM
  - Recommended
    - 4 CPU
    - 8 GB RAM

- Browser compatibility
  - Chrome 95 or later
  - Firefox 93 or later
  - Safari 13.7 or later
  - Other Chromium-based browsers might also work. Internet Explorer 11 is not supported

initMAX

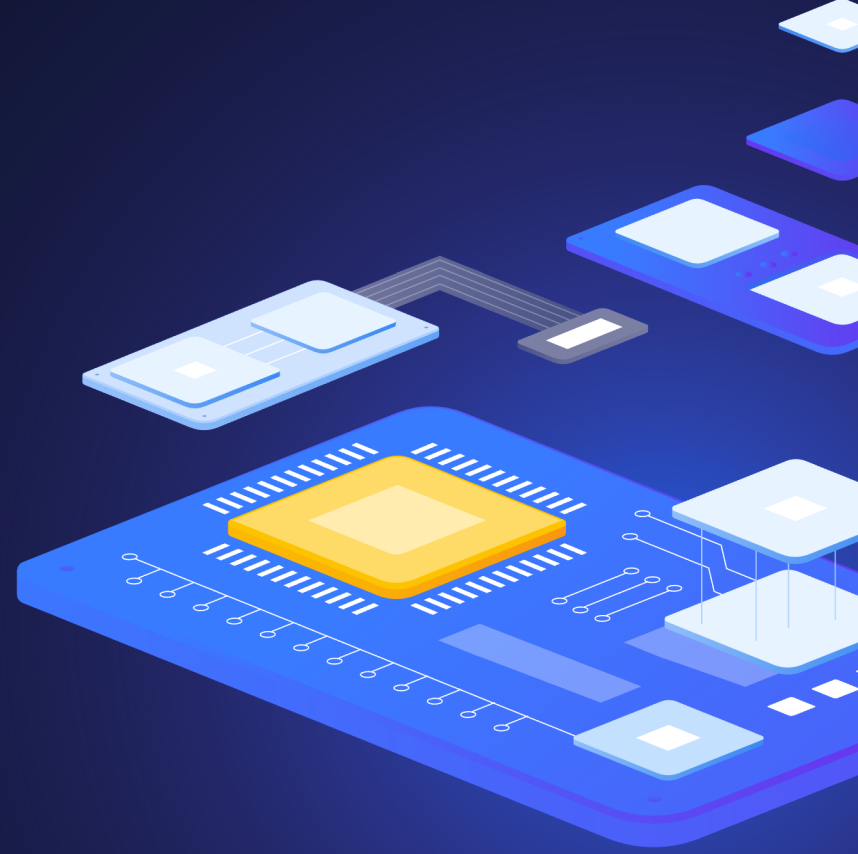
Wazuh Agents

- The agent was developed considering the need to monitor a wide variety of different endpoints without impacting their performance
- Agent supported on the most popular operating systems
- Requires 35 MB of RAM on average



initMAX

Demo time



initMAX

Wazuh Indexer installation

```
# Create firewall exceptions
firewall-cmd --permanent --add-port={443,514,1514,1515,1516,55000}/tcp
firewall-cmd --permanent --add-port={514,1514}/udp
firewall-cmd --reload

# Download the wazuh-certs-tool.sh script and the config.yml configuration file
curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh
curl -sO https://packages.wazuh.com/4.9/config.yml

# Edit ‘config.yml’ and replace example node names and IP addresses with correct ones
vim ./config.yml

# Run wazuh-certs-tool.sh to generate certificates
bash ./wazuh-certs-tool.sh -A

# Compress generated certificates into a tarball
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .

# Add Wazuh Yum repository and GPG key
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH

echo -e '[wazuh]\ngpgcheck=1\ngpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH\nenabled=1\nname=EL-$releasever -
Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1' | tee /etc/yum.repos.d/wazuh.repo
```

initMAX

Wazuh Indexer installation

```
# Install Wazuh Indexer and dependencies
yum install coreutils
yum install wazuh-indexer

# Edit ‘opensearch.yml’ configuration file according to your config.yml
vim /etc/wazuh-indexer/opensearch.yml

# Deploy certificates
mkdir /etc/wazuh-indexer/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./student-wazuh-01.pem ./student-wazuh-01-key.pem ./admin.pem ./admin-key.pem
./root-ca.pem
mv -n /etc/wazuh-indexer/certs/student-wazuh-01.pem /etc/wazuh-indexer/certs/indexer.pem
mv -n /etc/wazuh-indexer/certs/student-wazuh-01-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 and enable the service
systemctl daemon-reload
systemctl enable wazuh-indexer --now

# Initialize Wazuh Indexer cluster
/usr/share/wazuh-indexer/bin/indexer-security-init.sh

# Testing the cluster installation
curl -k -u admin:admin https://student-wazuh-01.initmax.com:9200
curl -k -u admin:admin https://student-wazuh-01.initmax.com:9200/_cat/nodes?v
```

initMAX

Wazuh Manager installation

```
# Install Wazuh manager
yum install wazuh-manager

# Install Filebeat
yum install filebeat

# Download the preconfigured Filebeat configuration file
curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.9/tpl/wazuh/filebeat/filebeat.yml

# Edit the ‘filebeat.yml’ configuration file
vim /etc/filebeat/filebeat.yml

# Create a Filebeat keystore to securely store authentication credentials
filebeat keystore create

# Add the default username and password to the secrets keystore
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force

# Download alerts template for the Wazuh indexer
curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.9.2/extensions/elasticsearch/7.x/wazuh-
template.json
chmod go+r /etc/filebeat/wazuh-template.json

# Download Wazuh module for Filebeat
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

initMAX

Wazuh Manager installation

```
# Deploy certificates
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./student-wazuh-01.pem ./student-wazuh-01-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/student-wazuh-01.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/student-wazuh-01-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

# Save Wazuh Indexer username and password into the Wazuh manager keystore
echo 'admin' | /var/ossec/bin/wazuh-keystore -f indexer -k username
echo 'admin' | /var/ossec/bin/wazuh-keystore -f indexer -k password

# Configure Wazuh Indexer connection in ‘ossec.conf’ configuration file (the same IP address as in filebeat.yml)
vim /var/ossec/etc/ossec.conf

# Enable and start both services
systemctl daemon-reload
systemctl enable wazuh-manager --now
systemctl enable filebeat --now

# Check status of Wazuh Manager service
systemctl status wazuh-manager

# Verify that Filebeat works correctly and can indeed connect to Wazuh Indexer
filebeat test output
```

initMAX

Wazuh Dashboard installation

```
# Install Wazuh Dashboard package
yum install wazuh-dashboard

# Install dependencies if missing
yum install libcap

# Configure OpenSearch dashboard (IP of Wazuh Manager master node)
vim /etc/wazuh-dashboard/opensearch_dashboards.yml

# Deploy certificates
mkdir /etc/wazuh-dashboard/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./student-wazuh-01.pem ./student-wazuh-01-key.pem ./root-ca.pem
mv -n /etc/wazuh-dashboard/certs/student-wazuh-01.pem /etc/wazuh-dashboard/certs/dashboard.pem
mv -n /etc/wazuh-dashboard/certs/student-wazuh-01-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

# Enable and start the Wazuh dashboard service
systemctl daemon-reload
systemctl enable wazuh-dashboard --now

# Edit the Wazuh Dashboard configuration file (vulnerability detection)
vim /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml

# Access the Wazuh Dashboard WUI with your credentials
https://student-wazuh-01.initmax.com
```

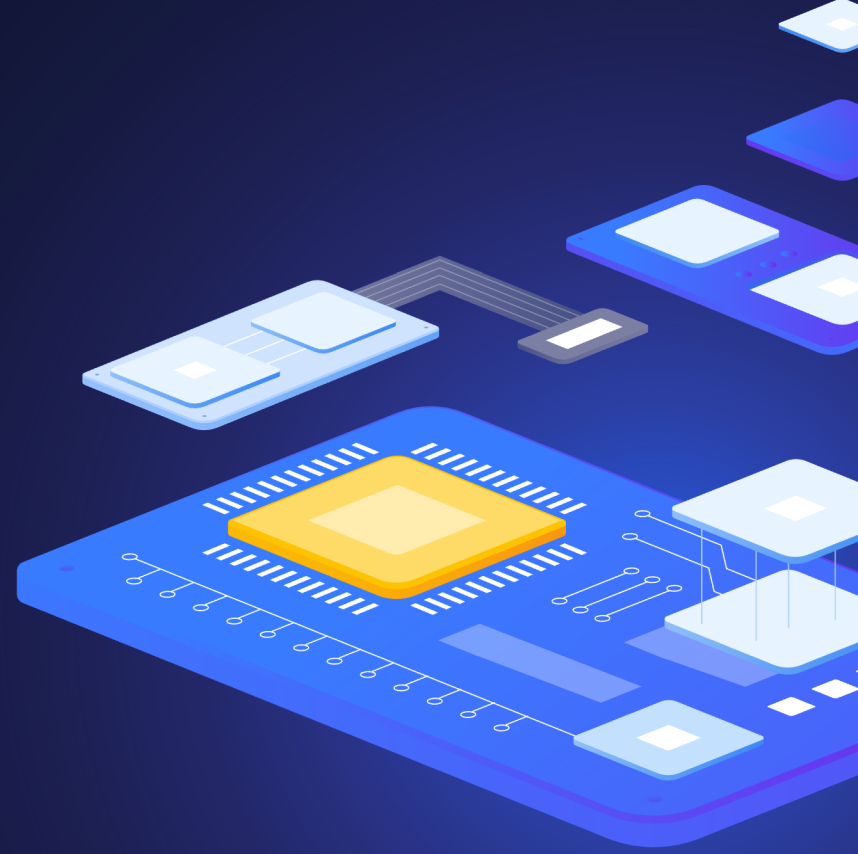
initMAX

Wazuh Dashboard installation

```
# Generate passwords for all users (all-in-one deployment)
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password
wazuh

# Generate passwords for indexer users (distributed deployment) – on any indexer node
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all

# Generate passwords for API users (distributed deployment) – on Wazuh Manager master node
curl -sO https://packages.wazuh.com/4.9/wazuh-passwords-tool.sh
bash wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password wazuh

# Update ‘admin’ password in Filebeat keystore (distributed deployment) – on EVERY Wazuh Manager node
echo %ADMIN_PASSWORD% | filebeat keystore add password --stdin –force

# Update ‘kibanaserver’ password in OpenSearch Dashboard keystore (distributed deployment) – on EVERY Wazuh Dashboard node
echo %KIBANASERVER_PASSWORD% | /usr/share/wazuh-dashboard/bin/opensearch-dashboards-keystore --allow-root add -f --stdin opensearch.password

# Update ‘wazuh-wui’ password in Wazuh Dashboard configuration (distributed deployment) – on EVERY Wazuh Dashboard node
vim /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml

# Restart all affected services to reflect the changes (watch out for cache!)
```

initMAX

Questions?



initMAX

Contact us:

Phone:	+420 800 244 442
Web:	https://www.initmax.cz
Email:	tomas.hermanek@initmax.cz
LinkedIn:	https://www.linkedin.com/company/initmax
Twitter:	https://twitter.com/initmax
Tomáš Heřmánek:	+420 732 447 184