CUSTOMER GUIDE

Wazuh Threat Detection Server

by Code Creator

Launch securely. Enroll your first endpoint. Start seeing security events.

Wazuh 4.14.5	Ubuntu 26.04 LTS	Docker-based single node

START HERE

This AMI gives you a self-managed Wazuh security monitoring environment. Your first success is simple: sign in, enroll one Linux, Windows, or macOS endpoint, and confirm that it becomes Active in the dashboard.

What is already prepared for you

- Wazuh Dashboard, Wazuh manager, and Wazuh indexer installed as a Docker-based single-node stack.
- A unique dashboard password and instance-specific TLS certificate generated automatically at first boot.
- Public service ports limited to HTTPS dashboard access and Wazuh agent enrollment/communication. The indexer and Wazuh API are not published to the Internet.
- A customer-friendly health command that shows first-boot state, dashboard address, and service status.

What this product is

This is a self-managed security monitoring server. You decide which endpoints to enroll, which alerts matter to your organization, who reviews them, and how long you retain data.

Your first success path

1	2	3	4
Launch	**Wait**	**Sign in**	**Enroll**
Use a restricted security group.	Run the first-boot status command.	Retrieve the per-instance admin password.	Confirm your first agent is Active.

1. Prepare a secure EC2 launch

Security group first. Create or select an EC2 security group before launch. Restrict inbound access to the smallest practical source: your administrator IP, VPN, private network, or the specific network ranges hosting agents.

Port / protocol	Open when needed	Recommended source	Purpose
22 / TCP	Yes	Your administrator IP or VPN	SSH administration
443 / TCP	Yes	Trusted administrators and dashboard users	Wazuh Dashboard over HTTPS
1514 / TCP	For agents	Only networks hosting enrolled Wazuh agents	Ongoing agent communication
1515 / TCP	For agents	Only networks hosting Wazuh agents	Automatic agent enrollment
23 / TCP	No	Do not open	Telnet is not used
9200 / TCP	No	Do not open	Wazuh indexer is internal-only
55000 / TCP	No	Do not open	Wazuh API is internal-only in this AMI

DO NOT USE OPEN-TO-THE-INTERNET RULES FOR ADMINISTRATION

Do not use 0.0.0.0/0 for SSH, port 1514, or port 1515. Restrict HTTPS (443) as well whenever your operating model allows it. The AMI does not publish ports 9200 or 55000, and your security group should not open them.

1 **Launch from AWS Marketplace**

Choose the instance type, key pair, VPC, subnet, and security group. Keep the default 100 GiB root volume or use a larger volume. Wazuh stores event and index data locally, so storage needs grow with endpoint count, alert volume, and retention.

2 **Use a stable address before broad agent enrollment**

For a public deployment, associate an Elastic IP or configure stable DNS before enrolling many agents. Otherwise, a public IPv4 address can change after an EC2 stop/start cycle. For private deployments, use a private IP address or private DNS reachable by the endpoints.

3 **Wait for the instance to finish starting**

Wait for EC2 status checks to pass. The Wazuh first-run service then generates instance-specific credentials and certificates, initializes the services, and starts the dashboard.

2. Connect and wait for first boot

SSH username: ubuntu. Use this account for SSH; root login is not used.

```
ssh -i /path/to/your-key.pem ubuntu@YOUR_INSTANCE_PUBLIC_IP
```

Replace **YOUR_INSTANCE_PUBLIC_IP** with the IPv4 address or public DNS name shown in the EC2 console. Use the private key selected when you launched the instance. Do not use root.

1 **Check first-boot status**

Run this after SSH connects. The correct next step is determined by the status message, not by a fixed timer.

```
codecreator-wazuh-status
```

WAIT FOR THE READY MESSAGE

Continue only after the command reports: First boot: ready. While it reports starting or running, leave the instance up and check again in a few minutes. Do not restart Docker or manually reset passwords during first boot.

2 **Retrieve the dashboard URL and unique credentials**

After first boot reports ready, retrieve the sign-in details through your encrypted SSH session.

```
sudo cat /home/ubuntu/FIRST_LOGIN.txt
```

Protect this file. The file shows the dashboard URL, the admin username, and the unique password for this running instance. Treat the password as a secret. Do not paste it into tickets, screenshots, chat messages, shell history, or shared notes.

3 **Open the dashboard**

Open the URL shown by codecreator-wazuh-url or FIRST_LOGIN.txt. The default address is https://YOUR_INSTANCE_PUBLIC_IP. A browser certificate warning is expected because a self-signed certificate is created at first boot. Confirm the address is the server you intended to open before continuing.

```
codecreator-wazuh-url
```

SIGN-IN

Use the dashboard username admin and the generated password from FIRST_LOGIN.txt. The password is unique to this launched instance and is not built into the AMI.

3. Enroll your first endpoint

Your first operational result. A dashboard that opens is only the beginning. The meaningful test is an endpoint that enrolls and becomes Active. Start with one representative Linux, Windows, or macOS device before broad rollout.

1 **Open the guided enrollment screen**

In the Wazuh Dashboard, open the menu and select Agents management > Summary > Deploy new agent.

2 **Choose the correct endpoint options**

Select the endpoint operating system and architecture. For Ubuntu or Debian endpoints, select DEB amd64. Enter the Wazuh server address that the endpoint can reach: use the public IP or public DNS for Internet-reachable endpoints; use a private IP or private DNS for same-VPC or connected private-network endpoints.

3 **Run the dashboard-generated command on the endpoint**

Copy the generated command and run it with administrator privileges on the endpoint. The endpoint needs TCP 1515 to enroll and TCP 1514 for its ongoing connection to the Wazuh server.

4 **Confirm the agent becomes Active**

Return to Agents management > Summary. The new endpoint should appear as Active. Once active, review its security events and decide which alert types require action in your environment.

ADDRESS RULE

The endpoint must be able to reach the exact Wazuh manager address you entered. A private EC2 address only works from connected private networks. A public deployment should use a stable public address, such as an Elastic IP or DNS name.

4. Day-one operating habits

- Review the new endpoint in Agents management and inspect recent security events after it becomes Active.
- Begin with a small, representative group of endpoints. Confirm useful alerts, data volume, storage use, and alert-review ownership before enrolling your entire environment.
- Restrict dashboard access and agent traffic continuously. Remove temporary broad rules after testing.
- Plan backups and a recovery procedure before changing configuration, retention, or product versions.
- Use the official Wazuh Docker upgrade guidance for Wazuh upgrades. Do not change Docker image tags or run blanket Docker updates without a backup and an upgrade plan.

Useful server commands

Command	What it does
`codecreator-wazuh-status`	Shows first-boot state, service status, and the current dashboard URL.
`codecreator-wazuh-url`	Prints the dashboard address using the current public IPv4 address.
`sudo cat /home/ubuntu/FIRST_LOGIN.txt`	Shows the unique dashboard sign-in credentials after first boot is ready.
`sudo systemctl status codecreator-wazuh-firstboot.service --no-pager`	Shows first-boot service status for troubleshooting.

5. Maintenance and troubleshooting

Host operating-system updates

Keep the host patched. Apply standard Ubuntu security updates as part of your normal maintenance process. This updates the Ubuntu host; it does not automatically upgrade the Wazuh Docker version.

```
sudo apt update && sudo apt upgrade -y
[ -f /var/run/reboot-required ] && sudo reboot
```

Important: After a reboot, reconnect as ubuntu and run codecreator-wazuh-status. Follow the official Wazuh Docker upgrade documentation for product-version upgrades.

Quick troubleshooting

Symptom	What to check
First boot does not show ready	Keep the instance running. Confirm EC2 status checks pass, then run codecreator-wazuh-status. If it remains incomplete after 15 minutes, inspect: sudo systemctl status codecreator-wazuh-firstboot.service --no-pager.
Dashboard does not open	Confirm first boot is ready, use codecreator-wazuh-url, and verify inbound TCP 443 permits your current IP or approved network.
SSH does not connect	Confirm inbound TCP 22 permits your present IP, the correct key pair was selected, and you are connecting as ubuntu.
Agent is not Active	Verify that the endpoint can reach the Wazuh server on TCP 1515 for enrollment and TCP 1514 for ongoing communication. Confirm the agent uses a Wazuh manager address reachable from that endpoint.
You need a stable public server address	Associate an Elastic IP or configure DNS before enrolling agents over the Internet.

Learning resources and help URLs

- Wazuh documentation home
- Deploy a new agent from the Wazuh Dashboard
- Wazuh agent enrollment requirements and ports
- Deploy Wazuh agents on Linux endpoints
- Wazuh Docker deployment
- Wazuh Docker upgrade guide
- Wazuh Docker password-management guidance
- AWS EC2 security group rule reference
- AWS: Connect to a Linux EC2 instance using SSH

Wazuh Threat Detection Server by Code Creator helps teams establish a private security monitoring foundation quickly: launch a dedicated server, enroll endpoints, centralize security signals, and build an alert-review process that fits the organization.