

Wazuh is a free and open source security platform that combines XDR and SIEM features. Protects workloads in on-premises, virtualized, containerized, and cloud-based environments. The solution consists of a single universal agent and three central components: Wazuh server, Wazuh indexer and Wazuh dashboard.

Wazuh Server: The Wazuh server is responsible for analyzing data received from Wazuh agents, triggering alerts when threats or anomalies are detected. It is also used to remotely manage the configuration of agents and monitor their status.

Elastic Stack: Elastic stack is a unified suite of popular open source projects including Elasticsearch, Kibana, Filebeat and others for log management. Indexes and stores alerts generated by the Wazuh server. In addition, the integration between Wazuh and Kibana* provides a user interface for data visualization and analysis. This interface is also used to manage the Wazuh configuration and monitor its status.

There are three main components related to Wazuh:

Filebeat: Used in Wazuh server to send events and alerts to Elasticsearch. It reads the output of the Wazuh analysis engine and sends the events in real time via an encrypted channel.

Elasticsearch: It is a highly scalable, full-text search and analytics engine. Elasticsearch is distributed, meaning data indices are split into chunks and each chunk can have zero or more copies. Wazuh uses different indices for alert data, raw events and condition monitoring information

Kibana: It is a flexible and intuitive web interface for data mining, analysis and visualization. It runs on top of indexed content in an Elasticsearch cluster. The Wazuh web UI is fully embedded in Kibana as a plugin. Security events include out-of-the-box dashboards for regulatory compliance (e.g. PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration evaluation results, cloud infrastructure monitoring events.

Wazuh Dashboard: This central component is a flexible and intuitive web interface for mining, analysis and visualization of data. Provides ready-to-use dashboards that allow you to navigate the user interface seamlessly. Users can quickly visualize security events, detect vulnerable applications, file integrity monitoring data, configuration evaluation results, cloud infrastructure monitoring events, and PCI DSS, GDPR, CIS, HIPAA, and NIST It can detect legal compliances such as 800-53 standards.

Wazuh Indexer: Wazuh indexer is a highly scalable, full-text search and analytics engine. This Wazuh central component indexes and stores alerts generated by the Wazuh server and provides near real-time data search and analytics capabilities.

Wazuh Agent: Wazuh agent is multiplatform and runs on the hosts the user wants to monitor. It communicates with the Wazuh administrator, sending data in near real-time via an encrypted and authenticated channel. The agent was developed with the need to monitor a wide variety of different endpoints without affecting their performance. It requires an average of 35 MB of RAM. Therefore, it is supported on most popular operating systems.

Wazuh agent provides key features to increase the security of your system.

Log collector	Command execution
File integrity monitoring (FIM)	Security configuration assessment (SCA)
System inventory	Malware detection
Active response	Container security
Cloud security	

WAZUH INSTALLATION

There are many alternative ways to download the Wazuh tool. The first of these ways and the installation featured on its page; To complete the download process step by step from <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html>.

As an alternative to this method, the following can be shown:

Deployment in Docker:

Docker is an open platform for building, delivering, and running applications in software containers. Docker containers bundle software, including everything needed to run it: code, runtime, system tools, system libraries, and settings. Docker enables to separate applications from infrastructure. This ensures that the application will always run the same regardless of the environment the container is running in. Containers can run in the cloud or on-premises. You can install Wazuh using Docker images such as wazuh/wazuh-manager, wazuh/wazuh-indexer, and wazuh/wazuh-dashboard. All these Wazuh Docker images are available in the Docker hub.

Installing from Packages:

Wazuh manager and agent can be installed via sources as an alternative to installing from packages.

Amazon Machine Images (AMI):

Wazuh provides a prebuilt Amazon Machine Image (AMI). AMI is a ready-to-use, preconfigured template for creating a virtual computing environment in Amazon Elastic Compute Cloud (Amazon EC2).

In addition to these alternative ways, we preferred the installation of OVA 4.2 version, which is another alternative way in this project.

Virtual Machine (OVA):

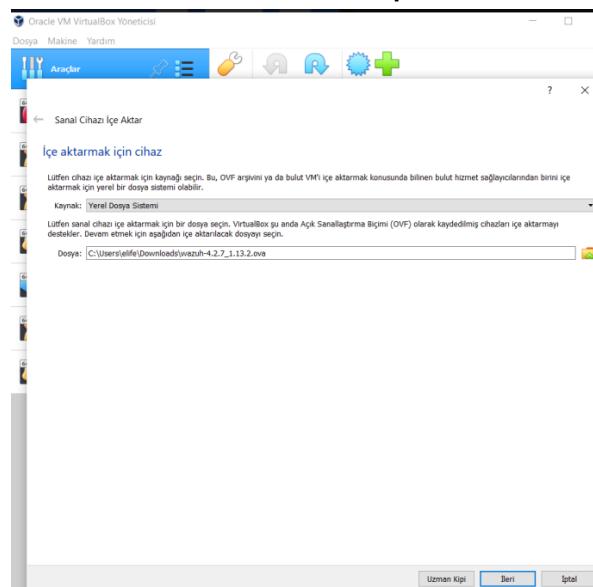
Wazuh provides a prebuilt virtual machine image (OVA) that you can import directly using VirtualBox or other OVA compatible virtualization systems. Note that this VM only works on 64-bit systems and does not provide high availability and scalability of the product.

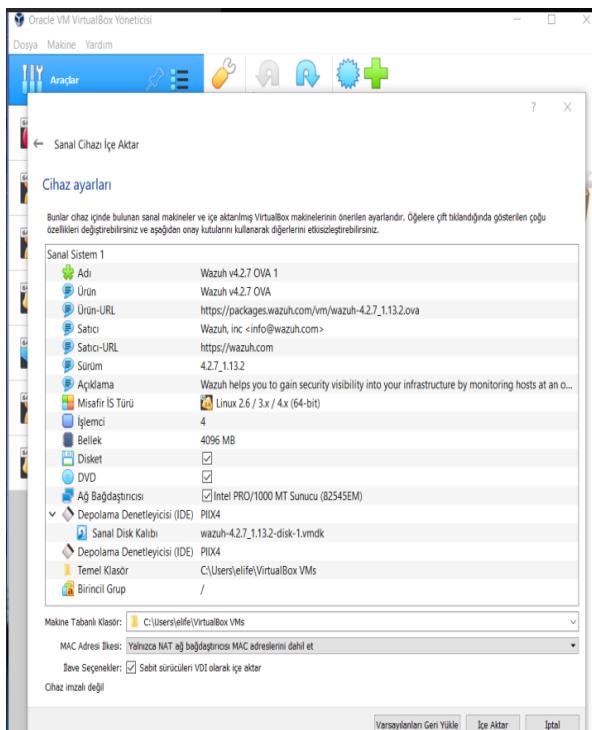
The OVA includes the following components:

- CentOS 7
- Wazuh manager: 4.2.7
- Open Distro for Elasticsearch: 1.13.2
- Filebeat-OSS: 7.10.2
- Kibana: 7.10.2
- Wazuh Kibana plugin: 4.2.7-7.10.2

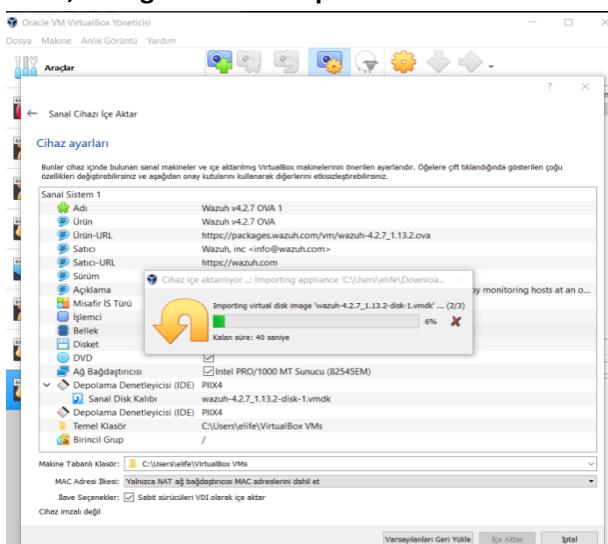
After downloading the above mentioned OVA in our project, we followed these steps for installation:

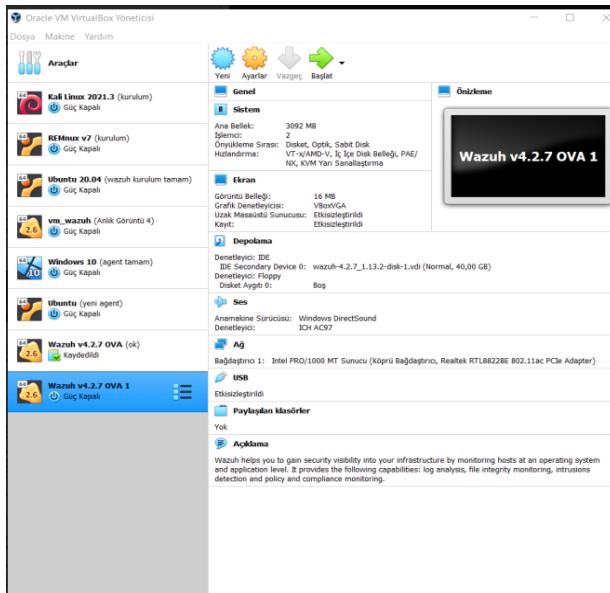
The downloaded OVA file is imported into VirtualBox.





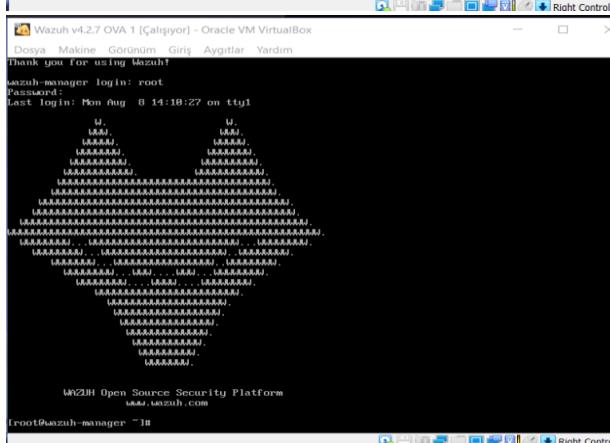
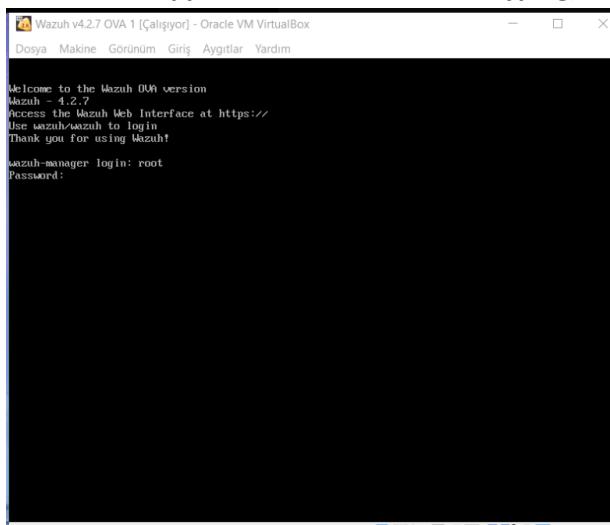
Default values can be changed during the installation process. After the import process is done, changes cannot be performed.





Wazuh OVA is run.

**In the window that opens, type “root” in the wazuh-manager login section and “wazuh” in the Password section and press the enter key to login.
(password does not appear on the screen while typing)**



After the system is turned on, "systemctl status kibana", "systemctl status wazuh-manager", "systemctl status elasticsearch" should be typed and kibana, wazuh-manager and elasticsearch should be running actively. If the status is not active, for example, "systemctl start elasticsearch" should be typed and the status of elasticsearch should be checked again.

```

Wazuh v4.2.7 OVA 1 [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görüntüm Giriş Aygıtlar Yardım
WAZUH Open Source Security Platform
www.wazuh.com

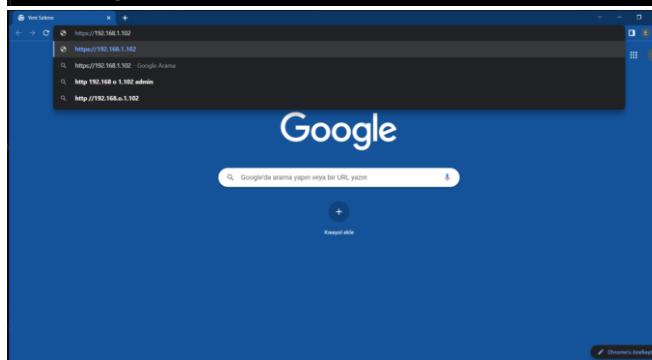
root@wazuh-manager:~# systemctl status wazuh-manager
root@wazuh-manager:~# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
  Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2022-08-08 11:29:41 UTC; 7s ago
    Process: 826 ExecStart=/usr/bin/cron /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           └─826 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py

Aug 08 11:29:29 wazuh-manager env[826]: Started wazuh-authd...
Aug 08 11:29:30 wazuh-manager env[826]: Started wazuh-db...
Aug 08 11:29:31 wazuh-manager env[826]: Started wazuh-execd...
Aug 08 11:29:32 wazuh-manager env[826]: Started wazuh-analysisd...
Aug 08 11:29:33 wazuh-manager env[826]: Started wazuh-syscheckd...
Aug 08 11:29:34 wazuh-manager env[826]: Started wazuh-remoted...
Aug 08 11:29:37 wazuh-manager env[826]: Started wazuh-logger...
Aug 08 11:29:38 wazuh-manager env[826]: Started wazuh-monitord...
Aug 08 11:29:38 wazuh-manager env[826]: Started wazuh-modulesd...
Aug 08 11:29:40 wazuh-manager env[826]: Completed.

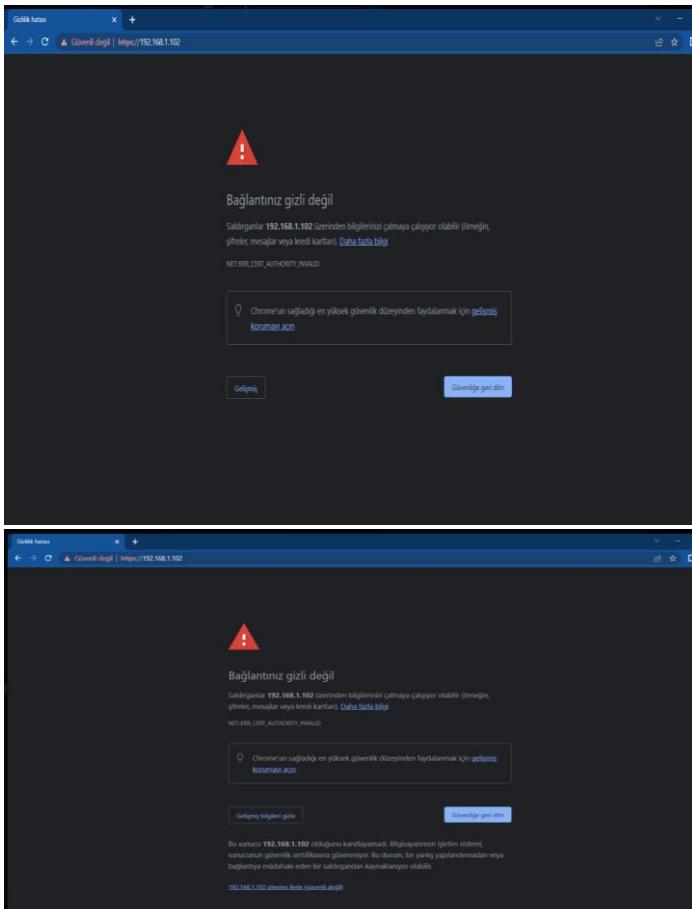
root@wazuh-manager:~# systemctl status elasticsearch
root@wazuh-manager:~# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
  Loaded: loaded (/etc/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/elasticsearch.service.d
            └─elasticsearch.conf
  Active: active (running) since Mon 2022-08-08 11:29:47 UTC; 1min 28s ago
    Docs: https://www.elastic.co
  Main PID: 828 (java)
     CGroup: /system.slice/elasticsearch.service
             └─828 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl...
```

```

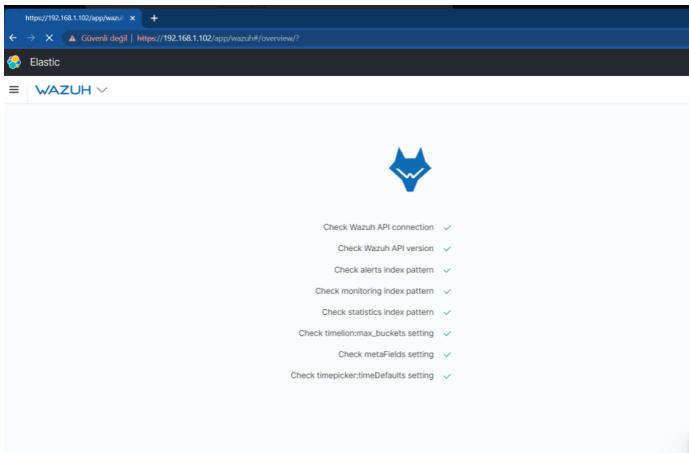
root@wazuh-manager:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:00:27:15:a5:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 3351sec preferred_lft 3351sec
    inet6 fe80::a00:27ff:fe15:a565/64 scope link
        valid_lft forever preferred_lft forever
root@wazuh-manager:~#
```



On the page that opens, if a warning such as "your connection is not confidential" is encountered, this warning should not be taken into account, by clicking on the "hide advanced information" button and clicking the "advance to the received IP address" button.



When an error such as “kibana server is not ready yet” is given in the interface that opens, step 4 should be returned and the statuses should be checked. All links must be complete on the page that opens.



After all connections are completed, login to wazuh dashboard is made automatically. After these stages, agent adding processes can be started. First, click on the “add agent” section and select the operating system that we want to add an agent to from the page that appears. Then “wazuh address server” Finally, the command in the "install and enroll agent" section is copied and pasted into the command line of the operating system in which the agent is desired to be installed, and press enter.

Deploy a new agent

- Choose the Operating system
 - Red Hat / CentOS
 - Debian / Ubuntu
 - Windows**
 - MacOS
- Wazuh server address

You can predefine the Wazuh server address with the `envClient.json` Wazuh app setting.
- Assign the agent to a group

Select one or more existing groups
- Install and enroll the agent

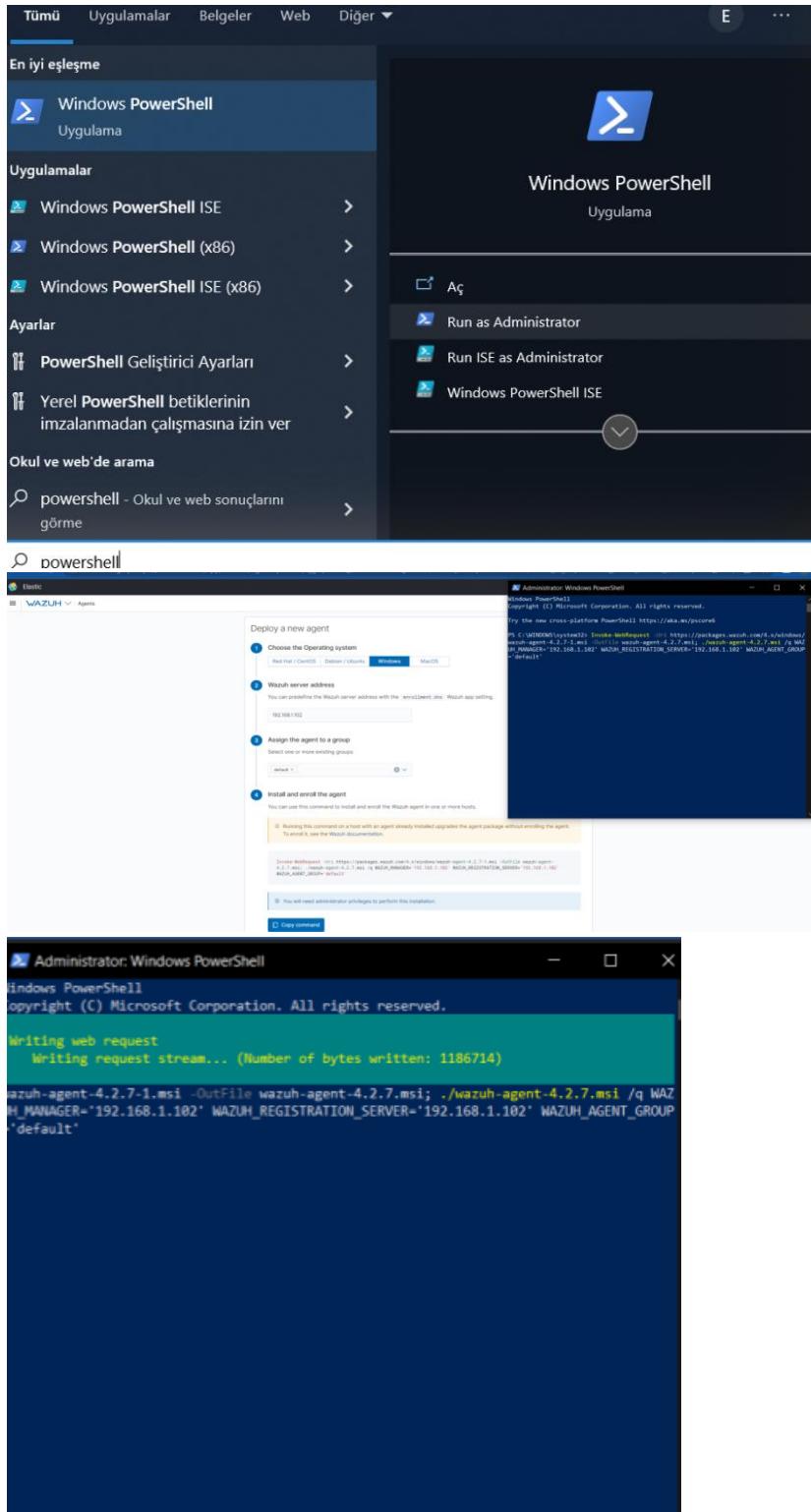
You can use the command or a tool with an agent already installed upgrade the agent package without enrolling the agent.

`curl -s https://packages.wazuh.com/4.2/wazuh-agent-4.2.7-1_amd64.deb --output wazuh-agent-4.2.7_amd64.deb & apt install ./wazuh-agent-4.2.7_amd64.deb`

To run it, see the Wazuh documentation.

You will need administrator privileges to perform this installation.

For the Window operating system, click the “PowerShell” “run as administrator” button, then the device is approved to make changes and the command received is pasted here and the enter key is pressed.



```

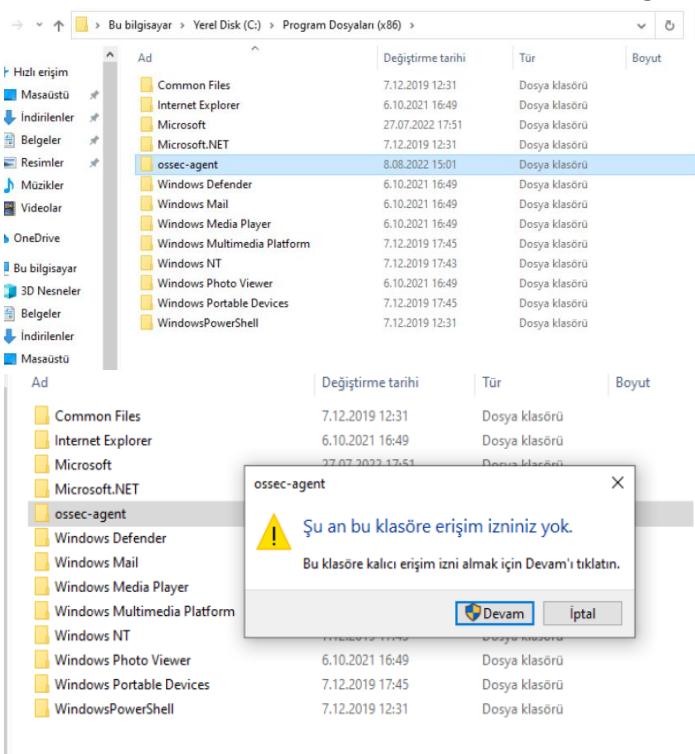
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.2.7-1.msi -Outfile wazuh-agent-4.2.7.msi; ./wazuh-agent-4.2.7.msi /q WAZUH_MANAGER='192.168.1.102' WAZUH_REGISTRATION_SERVER='192.168.1.102' WAZUH_AGENT_GROUP='default'
PS C:\WINDOWS\system32>

```

After the download is complete, the following path must be followed to access the Window agent: C:\Program Files (x86). From this folder section, the “ossec-agent” folder where the Windows agent is located is found and opened. Then, from the "view" tab on the screen, click the "view config" button and from the opened page, the ip address given to us before is written to the address section and the save button is clicked. The agent installation process is completed.



Yerel Disk (C:) > Program Dosyaları (x86) > ossec-agent

Ara: ossec-agent

Ad	Değiştirme tarihi	Tür	Boyut
queue	5.08.2022 15:37	Dosya klasörü	
rds	8.08.2022 15:01	Dosya klasörü	
ruleset	5.08.2022 15:37	Dosya klasörü	
shared	5.08.2022 15:37	Dosya klasörü	
syscheck	5.08.2022 15:37	Dosya klasörü	
tmp	8.08.2022 15:02	Dosya klasörü	
upgrade	5.08.2022 15:37	Dosya klasörü	
wodles	5.08.2022 15:37	Dosya klasörü	
agent_info	8.08.2022 15:00	AGENT_INFO Dosyası	1 KB
agent-auth	30.05.2022 16:00	Uygulama	984 KB
agent-auth.exe.manifest	30.05.2022 13:00	MANIFEST Dosyası	1 KB
client.keys	8.08.2022 15:01	KEYS Dosyası	1 KB
dbsync.dll	30.05.2022 13:55	Uygulama uzantısı	1.287 KB
help	30.05.2022 13:55	Metin Belgesi	2 KB
internal_options.conf	30.05.2022 13:55	CONF Dosyası	14 KB
libgc_c_59f-1.dll	30.05.2022 13:54	Uygulama uzantısı	1.090 KB
libwazuhext.dll	30.05.2022 13:54	Uygulama uzantısı	5.506 KB
libwazuhshared.dll	30.05.2022 13:55	Uygulama uzantısı	820 KB
libwazuhthread-1.dll	30.05.2022 13:54	Uygulama uzantısı	522 KB
LICENSE	30.05.2022 13:55	Metin Belgesi	25 KB
local_internal_options.conf	30.05.2022 13:55	CONF Dosyası	1 KB
manage_agents	30.05.2022 16:00	Uygulama	980 KB
ossec.conf	5.08.2022 15:37	CONF Dosyası	10 KB
ossec	8.08.2022 15:02	Metin Belgesi	24 KB
REVISION	30.05.2022 13:55	Dosya	1 KB
rsync.dll	30.05.2022 13:55	Uygulama uzantısı	1.152 KB
syscollector.dll	30.05.2022 13:55	Uygulama uzantısı	1.322 KB
sysinfo.dll	30.05.2022 13:55	Uygulama uzantısı	1.237 KB
VERSION	30.05.2022 13:55	Dosya	1 KB
vista_sec	30.05.2022 13:00	Metin Belgesi	92 KB
wazuh-agent	30.05.2022 16:00	Uygulama	1.798 KB
wazuh-agent.state	8.08.2022 15:04	STATE Dosyası	1 KB
wazuh-logcollector.state	8.08.2022 15:03	STATE Dosyası	2 KB
win32ui	30.05.2022 16:00	Uygulama	909 KB
win32ui.exe.manifest	30.05.2022 13:00	MANIFEST Dosyası	1 KB

Ad	Değiştirme tarihi	Tür	Boyut
queue	5.08.2022 15:37	Dosya Klasörü	
rds	8.08.2022 15:01	Dosya Klasörü	
ruleset	5.08.2022 15:37	Dosya Klasörü	
shared	5.08.2022 15:38	Dosya Klasörü	
syscheck	5.08.2022 15:37	Dosya Klasörü	
tmp	8.08.2022 15:02	Dosya Klasörü	
upgrade	5.08.2022 15:37	Dosya Klasörü	
wodles	5.08.2022 15:37	Dosya Klasörü	
agent_info	8.08.2022 15:00	AGENT_INFO Dosyası	1 KB
agent-auth	30.05.2022 16:00	Uygulama	984 KB
agent-auth.exe.manifest	30.05.2022 13:00	MANIFEST Dosyası	1 KB
client.keys	8.08.2022 15:01	KEYS Dosyası	1 KB
dbsync.dll	30.05.2022 13:55	Uygulama uzantısı	1.287 KB
help	30.05.2022 13:55	Metin Belgesi	2 KB
internal_options.conf	30.05.2022 13:55	CONF Dosyası	14 KB
libgc_c_59f-1.dll	30.05.2022 13:54	Uygulama uzantısı	1.090 KB
libwazuhext.dll	30.05.2022 13:54	Uygulama uzantısı	5.506 KB
libwazuhshared.dll	30.05.2022 13:55	Uygulama uzantısı	820 KB
libwazuhthread-1.dll	30.05.2022 13:54	Uygulama uzantısı	522 KB
LICENSE	30.05.2022 13:55	Metin Belgesi	25 KB
local_internal_options.conf	30.05.2022 13:55	CONF Dosyası	1 KB
manage_agents	30.05.2022 16:00	Uygulama	980 KB
ossec.conf	5.08.2022 15:37	CONF Dosyası	10 KB
ossec	8.08.2022 15:02	Metin Belgesi	24 KB
REVISION	30.05.2022 13:55	Dosya	1 KB
rsync.dll	30.05.2022 13:55	Uygulama uzantısı	1.152 KB
syscollector.dll	30.05.2022 13:55	Uygulama uzantısı	1.322 KB
sysinfo.dll	30.05.2022 13:55	Uygulama uzantısı	1.237 KB
VERSION	30.05.2022 13:55	Dosya	1 KB
vista_sec	30.05.2022 13:00	Metin Belgesi	92 KB
wazuh-agent	30.05.2022 16:00	Uygulama	1.798 KB
wazuh-agent.state	8.08.2022 15:04	STATE Dosyası	1 KB
wazuh-logcollector.state	8.08.2022 15:03	STATE Dosyası	2 KB
win32ui	30.05.2022 16:00	Uygulama	909 KB
win32ui.exe.manifest	30.05.2022 13:00	MANIFEST Dosyası	1 KB

Wazuh Agent Manager

Manage View Help

Wazuh v4.2.7

Agent DESKTOP-LELRB8 (002) - any

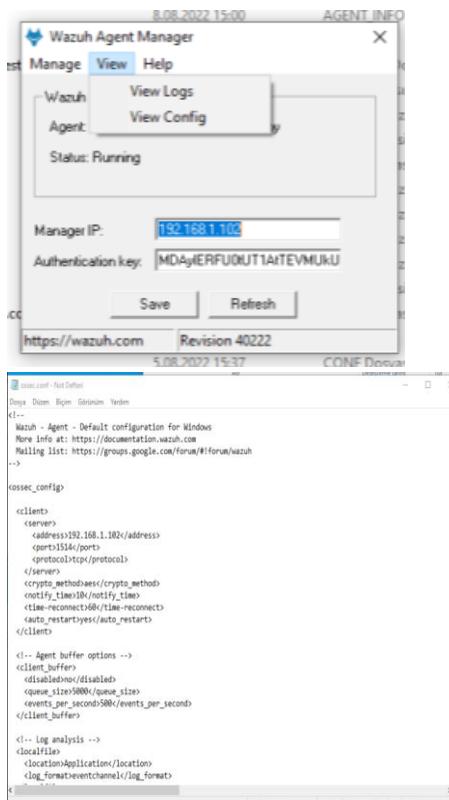
Status: Running

Manage IP: 192.168.1.105

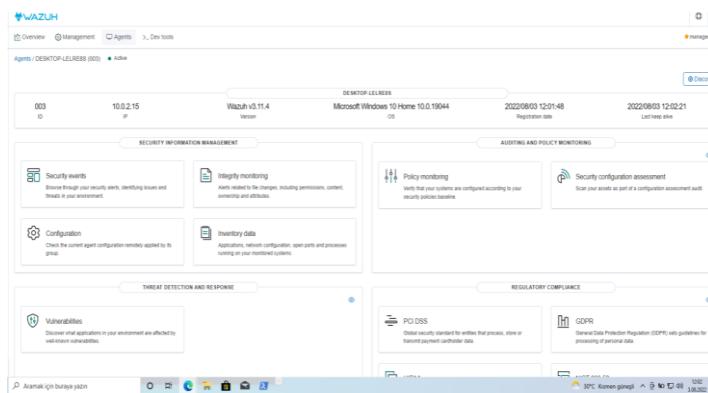
Authentication key: MD5d4ERFU0U1TATEVM/RU

Save Refresh

https://wazuh.com Revision 40222



After all the processes are completed, when the wazuh interface is entered, it will be seen that the agent is installed.



After the received ip address, "this site cannot be reached" error in the wazuh interface can be encountered because the ip address given to us in the wazuh ova section is a dynamic rip address and can change. In this case, a new ip address can be taken with ip add and the process can be taken under control.

The process of installing agents on Ubuntu operating system is the same. Users who want to install agents on Ubuntu can do the same steps.

WAZUH		Agents									
STATUS		DETAILS									
		Active	Disconnected								
001	elf-VirtualBox	10.0.2.15	IP								
		Active	Disconnected								
003	DESKTOP-LELRE8S	10.0.2.15	IP								
		Active	Disconnected								
Last registered agent		Never connected	Agents coverage								
HP-Elf		0	33.33%								
Most active agent		DESKTOP-LELRE8S									
No results found											
Filter or search agent		Refresh									
Agents (3)											
ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions	
001	elf-VirtualBox	10.0.2.15	default	Ubuntu 20.04.4 LTS	node01	v4.2.7	Aug 4, 2022 @ ...	Aug 7, 2022 @ ...	● disconnected		
003	DESKTOP-LELRE8S	10.0.2.15	default	Microsoft Windows 1...	node01	v4.2.7	Aug 5, 2022 @ ...	Aug 8, 2022 @ ...	● disconnected		

After all the stages are completed, the "security event" overview in the wazuh tool is as follows.

The screenshots illustrate the Wazuh security event overview across three main sections:

- Security events:** Shows a summary of alerts, including a bar chart of alert counts over time, a pie chart of alert groups, and a list of top 5 alerts with their descriptions, levels, and counts.
- Actions:** Shows a summary of file changes, including a pie chart of file types (modified vs. added), a list of most active users, and a timeline of file modifications.
- Network interfaces:** Shows a table of network interfaces with columns for Name, MAC, State, MTU, and Type. It also includes a table of network ports and windows update logs.

The screenshot shows the Wazuh Management interface. In the top navigation bar, there are tabs for Overview, Management, Agents, and Dev Tools. The main content area is divided into three sections:

- Network settings:** Shows two network interfaces: Ethernet and Wireless. Ethernet has an IP of 192.168.1.15, subnet mask 255.255.255.0, and broadcast 192.168.1.255. Wireless has an IP of 192.168.1.100 and subnet mask 255.255.255.0.
- Windows updates:** A list of pending updates from Microsoft, including Security updates, Cumulative Updates, and Microsoft Edge updates.
- Packages:** A table of installed packages from Oracle Corporation, Microsoft Corporation, and Wazuh, Inc., including Oracle VM VirtualBox Guest Additions, Windows PC System, Microsoft Update Health Tools, Microsoft Edge, Microsoft Edge Update, and Wazuh Agent.

INSTALLING WAZUH IN CLOUD ENVIRONMENT

Wazuh tool can be installed on a cloud environment as well as on a VirtualBox. Wazuh tool should have the following requirements in general;

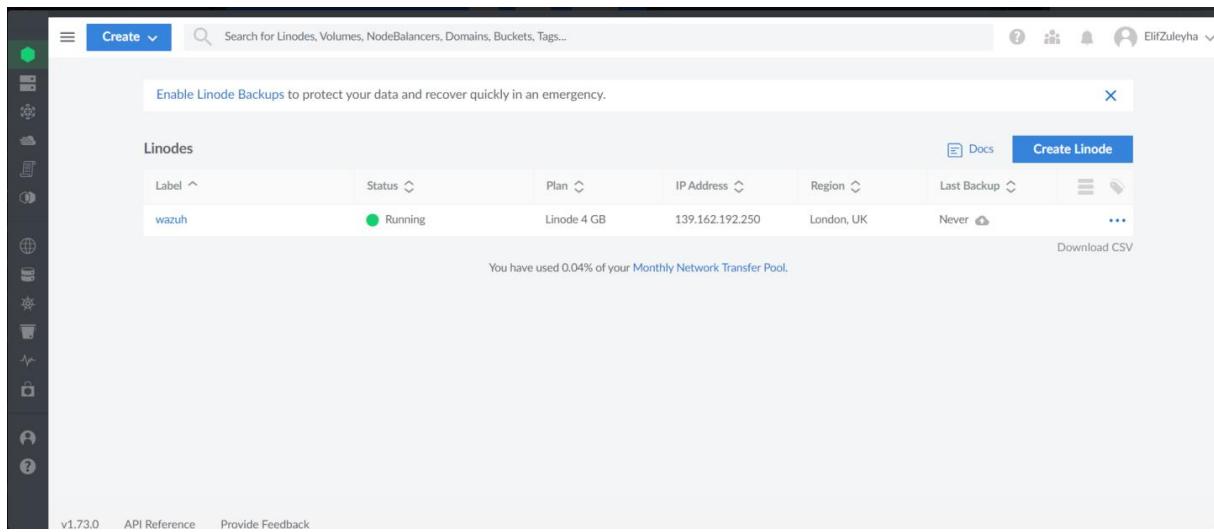
Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

When we used Wazuh Ova in this project, we encountered events such as system slowdowns, contractions, so we preferred to install the wazuh tool in a cloud environment called linode, which provides a virtual server, in order to prevent these problems and to prevent each team member from downloading wazuh ova separately.

INSTALL WAZUH ON LINODE:

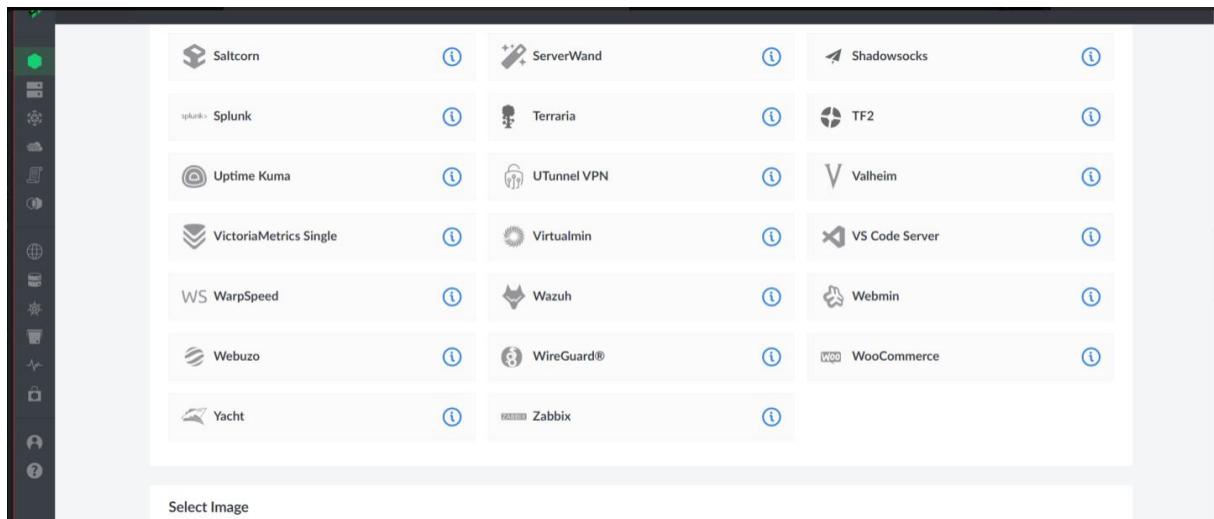
Go to <https://cloud.linode.com/linodes> and open an account to use the cloud environment. If a virtual card is used in the payment information section when opening an account on Linode, the Linode system automatically rejects the account. Therefore, physical card information should be used in this section. Opening an account After the application is made, an account is created if the necessary conditions are met.

After logging into the account, click on the 'Create Linode' button from the 'Linodes' tab.



The screenshot shows the Linode dashboard with the 'Linodes' tab selected. A table lists a single node named 'wazuh'. The columns include Label, Status, Plan, IP Address, Region, and Last Backup. The 'wazuh' node is listed as 'Running' on a 'Linode 4 GB' plan with the IP address '139.162.192.250' in the 'London, UK' region, with its last backup taken 'Never'. There is a 'Create Linode' button in the top right corner of the table header.

From the page that opens, go to the “marketplace” tab. In this section, there are tools that can be used on Linode. Among these tools, the Wazuh tool is selected.



The screenshot shows the 'Marketplace' tab on the Linode dashboard. It displays a grid of tool icons and names. The 'Wazuh' tool is clearly visible in the middle row, second column. Other tools shown include Saltcorn, ServerWand, Shadowsocks, Splunk, Terraria, TF2, Uptime Kuma, UTunnel VPN, Valheim, VictoriaMetrics Single, Virtualmin, VS Code Server, WarpSpeed, Webmin, Webuzo, WireGuard®, WooCommerce, Yacht, and Zabbix. A 'Select Image' button is located at the bottom left of the grid.

Fill in the information in the "Wazuh options" section on the page that opens.

The screenshot shows two stacked configuration screens from the Linode WordPress setup wizard.

Wazuh Options:

- Email address (for the Let's Encrypt SSL certificate) (required): user@domain.tld
- Advanced Options:** These fields are additional configuration options and are not required for creation.
- The limited sudo user to be created for the Linode: (empty input field)
- The password for the limited sudo user: an0th3r_s3cure_p4ssw0rd (Weak)
- The SSH Public Key that will be used to access the Linode: (empty input field)
- Disable root access over SSH? (radio buttons: Yes [unchecked], No [checked])

Your Linode API token. This is needed to create your WordPress server's DNS records:

- Enter a password: (empty input field)
- Subdomain: (empty input field)
- The subdomain for the DNS record: www (Requires Domain)
- Domain: (empty input field)
- The domain for the DNS record: example.com (Requires API token)

Select an Image:

- Images: Ubuntu 20.04 LTS

Region:

- You can use [our speedtest page](#) to find the best region for your current location.
- Region: Select a Region

After the information is frozen, go to the “Shared Cpu” section in the “Linode Plan” section and select the CPU and RAM.

The screenshot shows the Linode Plan section with the "Shared CPU" tab selected.

Shared CPU instances are good for medium-duty workloads and are a good mix of performance, resources, and price.

	Monthly	Hourly	RAM	CPUs	Storage	Transfer	Network In / Out
Nanode 1 GB	\$5	\$0.0075	1 GB	1	25 GB	1 TB	40 Gbps / 1 Gbps
Linode 2 GB	\$10	\$0.015	2 GB	1	50 GB	2 TB	40 Gbps / 2 Gbps
Linode 4 GB	\$20	\$0.03	4 GB	2	80 GB	4 TB	40 Gbps / 4 Gbps
Linode 8 GB	\$40	\$0.06	8 GB	4	160 GB	5 TB	40 Gbps / 5 Gbps
Linode 16 GB	\$80	\$0.12	16 GB	6	320 GB	8 TB	40 Gbps / 6 Gbps
Linode 32 GB	\$160	\$0.24	32 GB	8	640 GB	16 TB	40 Gbps / 7 Gbps
Linode 64 GB	\$320	\$0.48	64 GB	16	1280 GB	20 TB	40 Gbps / 9 Gbps
Linode 96 GB	\$480	\$0.72	96 GB	20	1920 GB	20 TB	40 Gbps / 10 Gbps
Linode 128 GB	\$640	\$0.96	128 GB	24	2560 GB	20 TB	40 Gbps / 11 Gbps

After all the processes are completed, the wazuh tool is installed on Linode. An "ip" address is given for users to access the Wazuh interface. This IP address is searched by typing https:// on the browser.

Enable Linode Backups to protect your data and recover quickly in an emergency.

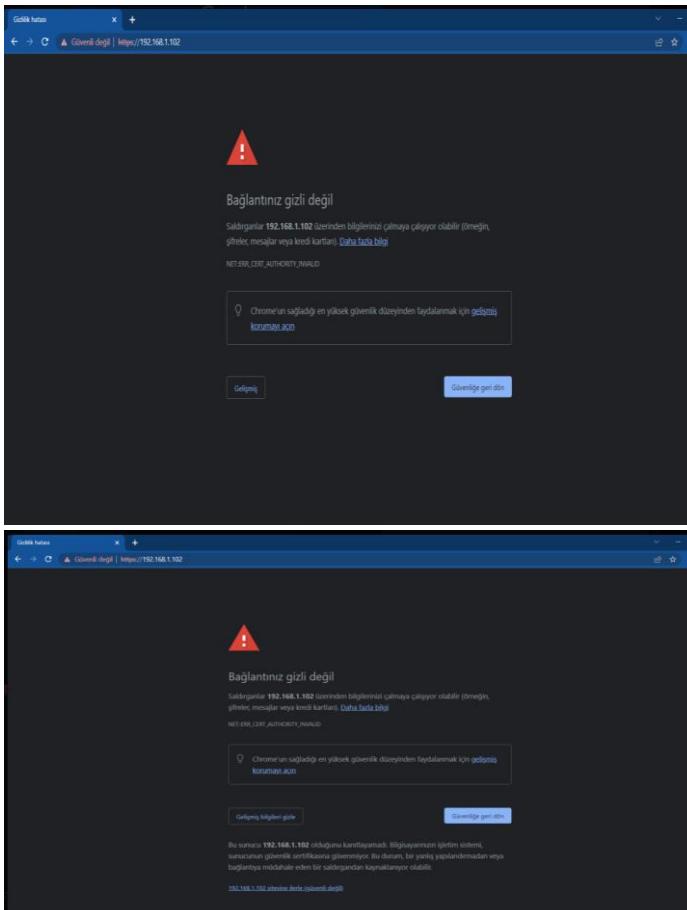
Linodes

Label ^	Status ^	Plan ^	IP Address ^	Region ^	Last Backup ^	...
wazuh	Running	Linode 4 GB	139.162.192.250	London, UK	Never	

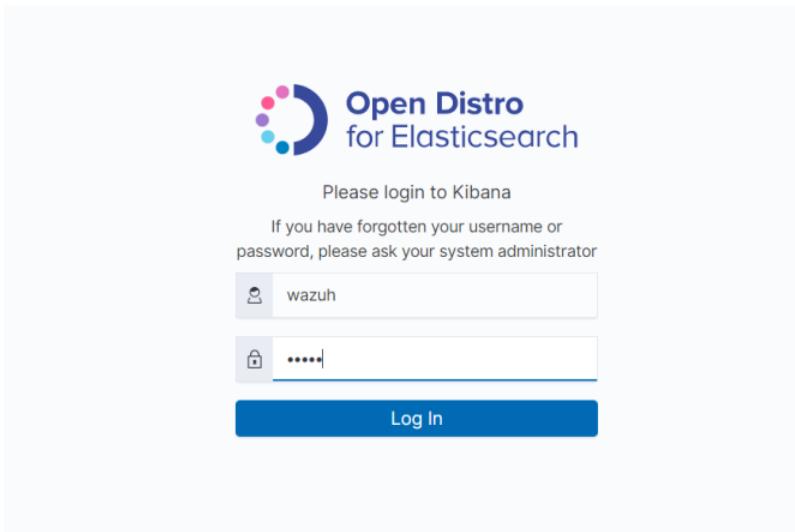
Download CSV

You have used 0.04% of your Monthly Network Transfer Pool.

On the page that opens, if a warning such as “your connection is not confidential” is encountered, this warning should not be taken into account.



Açılan sayfada wazuh aracına giriş yapmak için username ve password kısımlarına “wazuh” yazılır ve sisteme giriş yapılır.



WAZUH / Modules

Total agents	Active agents	Disconnected agents	Never connected agents
4	0	4	0

SECURITY INFORMATION MANAGEMENT

- Security events: Browse through your security alerts, identifying issues and threats in your environment.
- Integrity monitoring: Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

- Policy monitoring: Verify that your systems are configured according to your security policies baseline.
- System auditing: Audit users behavior, monitoring command execution and alerting on access to critical files.

THREAT DETECTION AND RESPONSE

- Vulnerabilities: Discover what applications in your environment are affected by well-known vulnerabilities.
- MITRE ATT&CK: Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

REGULATORY COMPLIANCE

- PCI DSS: Global security standard for entities that process, store or transmit payment cardholder data.
- NIST 800-53: National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

Wazuh agent kurma kısmı wazuh ova kurma kısmında anlatıldığı gibidir.

WAZUH / Agents

STATUS

Active: 0
Disconnected: 4
Never connected: 0

DETAILS

Last registered agent: DESKTOP-UQEOKRL
Most active agent: compeng

EVOLUTION

Count: 4
timestamp per 10 minutes

Filter or search agent Refresh

Agents (4)										
ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	DESKTOP-LELREBS	10.0.2.15	default	Microsoft Windows 10...	node01	v4.3.6	Jan 1, 1970 @ 0...	Aug 12, 2022 @...	● disconnected	Deploy Logs
002	elf-VirtualBox	10.0.2.15	default	Ubuntu 20.04.4 LTS	node01	v4.3.6	Aug 11, 2022 @...	Aug 11, 2022 @...	● disconnected	Deploy Logs
003	compeng	10.0.2.15	default	Ubuntu 20.04.4 LTS	node01	v4.3.6	Aug 11, 2022 @...	Aug 13, 2022 @...	● disconnected	Deploy Logs
004	DESKTOP-UQEOKRL	10.0.2.15	default	Microsoft Windows 10...	node01	v4.3.6	Aug 12, 2022 @...	Aug 12, 2022 @...	● disconnected	Deploy Logs

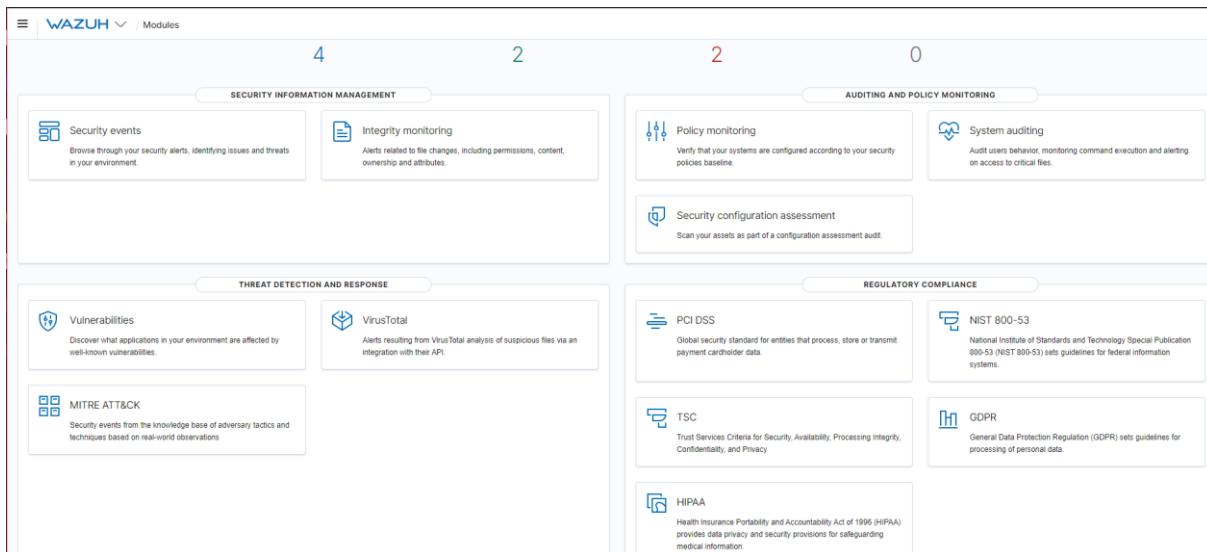
WAZUH MODULES

1. Security Event

2. Integrity Monitoring

3. Vulnerabilities

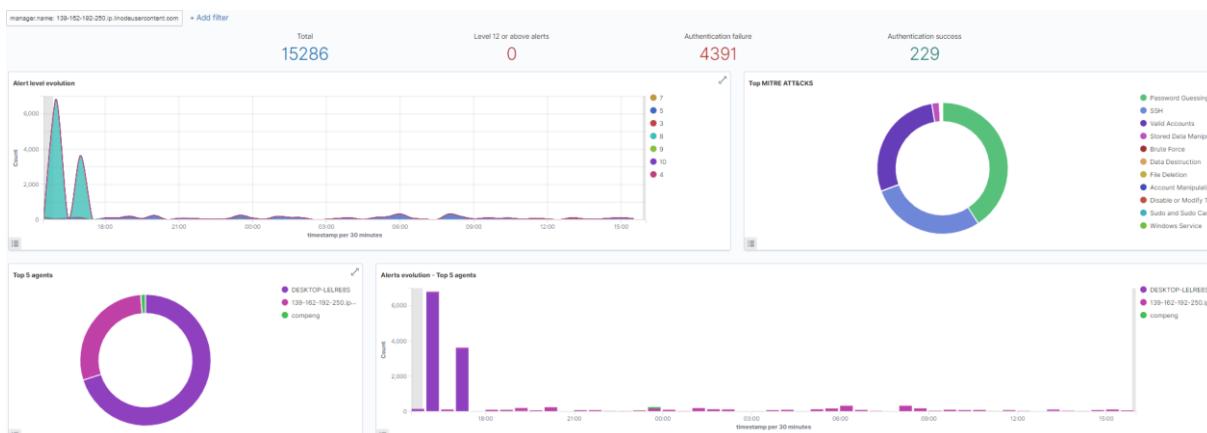
4. MITRE ATT&CK



1. SECURITY EVENT:

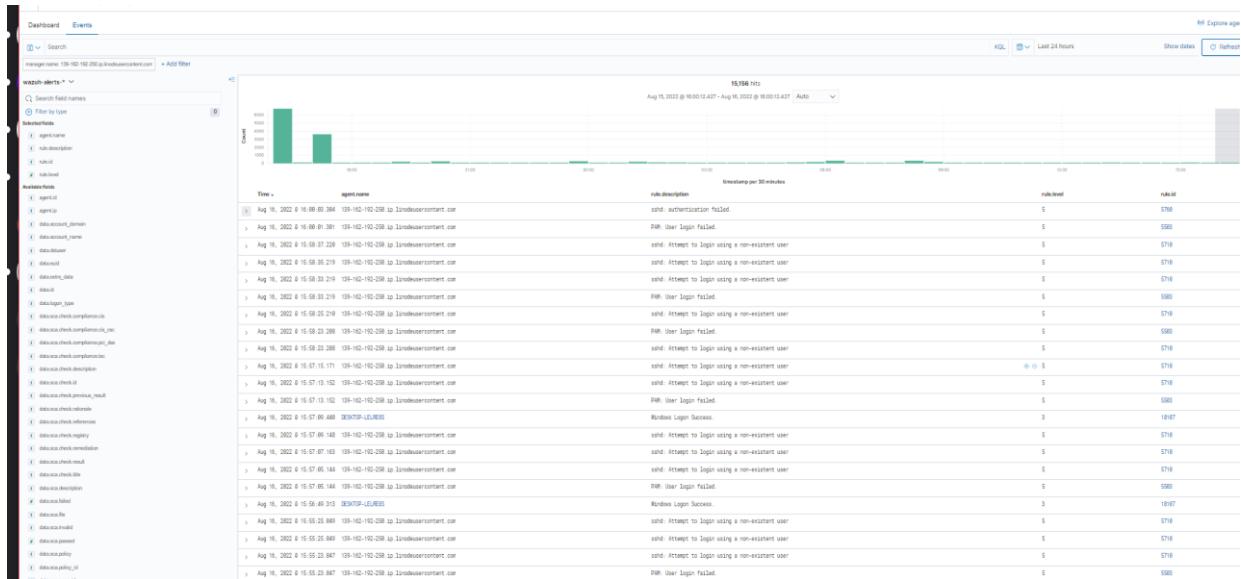
It provides security warnings by identifying problems and threats in the environment. It consists of 2 components. Dashboard and Events.

The warnings given in the Dashboard and the threats found are displayed more graphically and there are Security warnings, we can examine these warnings in the form of tables, JSON and rules in this section.



Security Alerts																																																			
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID																																												
> Aug 16, 2022 @ 15:52:26.886	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710																																												
> Aug 16, 2022 @ 15:52:24.884	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710																																												
> Aug 16, 2022 @ 15:52:20.879	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710																																												
> Aug 16, 2022 @ 15:52:20.878	000	139-162-192-250.ip.linodeusercontent.com	T1110.001	Credential Access	PAM: User login failed.	5	5503																																												
> Aug 16, 2022 @ 15:51:58.859	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760																																												
> Aug 16, 2022 @ 15:51:56.856	000	139-162-192-250.ip.linodeusercontent.com	T1110.001	Credential Access	PAM: User login failed.	5	5503																																												
> Aug 16, 2022 @ 15:51:30.831	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760																																												
> Aug 16, 2022 @ 15:51:26.827	000	139-162-192-250.ip.linodeusercontent.com	T1110.001	Credential Access	PAM: User login failed.	5	5503																																												
> Aug 16, 2022 @ 15:51:02.804	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710																																												
> Aug 16, 2022 @ 15:51:02.804	000	139-162-192-250.ip.linodeusercontent.com	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710																																												
Table JSON Rule																																																			
<table border="1"> <tr> <td>agent.name</td><td>139-162-192-250.ip.linodeusercontent.com</td></tr> <tr> <td>agent.id</td><td>000</td></tr> <tr> <td>manager.name</td><td>139-162-192-250.ip.linodeusercontent.com</td></tr> <tr> <td>rule.mail</td><td>false</td></tr> <tr> <td>rule.level</td><td>5</td></tr> <tr> <td>rule.hipaa</td><td>164.312.b</td></tr> <tr> <td>rule.pci_dss</td><td>10.2.4, 10.2.5, 10.6.1</td></tr> <tr> <td>rule.tsc</td><td>C00.1, C00.8, C07.2, C07.3</td></tr> <tr> <td>rule.description</td><td>sshd: Attempt to login using a non-existent user</td></tr> <tr> <td>rule.groups</td><td>syslog, sshd, authentication_failed, invalid_login</td></tr> <tr> <td>rule.nist_800_53</td><td>AU.14, AC.7, AU.6</td></tr> <tr> <td>rule.gdrp</td><td>N_25.7.d, N_32.2</td></tr> <tr> <td>rule.firetimes</td><td>100</td></tr> <tr> <td>rule.mitre.technique</td><td>Password Guessing, SSH, Valid Accounts</td></tr> <tr> <td>rule.mitre.id</td><td>T1110.001, T1021.004, T1078</td></tr> <tr> <td>rule.mitre.tactic</td><td>Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access</td></tr> <tr> <td>rule.id</td><td>5710</td></tr> <tr> <td>rule.gpg13</td><td>7.1</td></tr> <tr> <td>decoder.parent</td><td>sshd</td></tr> <tr> <td>decoder.name</td><td>sshd</td></tr> <tr> <td>full_log</td><td>Aug 16 12:52:25 139-162-192-250 sshd[812512]: Disconnected from invalid user admin@143.135.157.113 port 49420 [preauth]</td></tr> <tr> <td>location</td><td>/var/log/auth.log</td></tr> </table>								agent.name	139-162-192-250.ip.linodeusercontent.com	agent.id	000	manager.name	139-162-192-250.ip.linodeusercontent.com	rule.mail	false	rule.level	5	rule.hipaa	164.312.b	rule.pci_dss	10.2.4, 10.2.5, 10.6.1	rule.tsc	C00.1, C00.8, C07.2, C07.3	rule.description	sshd: Attempt to login using a non-existent user	rule.groups	syslog, sshd, authentication_failed, invalid_login	rule.nist_800_53	AU.14, AC.7, AU.6	rule.gdrp	N_25.7.d, N_32.2	rule.firetimes	100	rule.mitre.technique	Password Guessing, SSH, Valid Accounts	rule.mitre.id	T1110.001, T1021.004, T1078	rule.mitre.tactic	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	rule.id	5710	rule.gpg13	7.1	decoder.parent	sshd	decoder.name	sshd	full_log	Aug 16 12:52:25 139-162-192-250 sshd[812512]: Disconnected from invalid user admin@143.135.157.113 port 49420 [preauth]	location	/var/log/auth.log
agent.name	139-162-192-250.ip.linodeusercontent.com																																																		
agent.id	000																																																		
manager.name	139-162-192-250.ip.linodeusercontent.com																																																		
rule.mail	false																																																		
rule.level	5																																																		
rule.hipaa	164.312.b																																																		
rule.pci_dss	10.2.4, 10.2.5, 10.6.1																																																		
rule.tsc	C00.1, C00.8, C07.2, C07.3																																																		
rule.description	sshd: Attempt to login using a non-existent user																																																		
rule.groups	syslog, sshd, authentication_failed, invalid_login																																																		
rule.nist_800_53	AU.14, AC.7, AU.6																																																		
rule.gdrp	N_25.7.d, N_32.2																																																		
rule.firetimes	100																																																		
rule.mitre.technique	Password Guessing, SSH, Valid Accounts																																																		
rule.mitre.id	T1110.001, T1021.004, T1078																																																		
rule.mitre.tactic	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access																																																		
rule.id	5710																																																		
rule.gpg13	7.1																																																		
decoder.parent	sshd																																																		
decoder.name	sshd																																																		
full_log	Aug 16 12:52:25 139-162-192-250 sshd[812512]: Disconnected from invalid user admin@143.135.157.113 port 49420 [preauth]																																																		
location	/var/log/auth.log																																																		

In the Events section, detailed examination of incoming warnings and threats can be made. Warnings of the desired nature can be found by filtering processes. In this section, threat analysis can also be performed by looking at the values such as location, hash, and full log of the incoming alert.



For example; We received a warning as follows when an attempt was made to gain unauthorized access to our Wazuh server.

Time	agent.name	rule.description	rule.level	rule.id
Aug 16, 2022 @ 16:00:03.304	139-162-192-250.ip.linodeusercontent.com	sshd: authentication failed.	5	5760
View expanded document				
View surrounding documents				
View single document				
Table JSON				
<pre>t GeoLocation.city_name Duluth t GeoLocation.country_name United States @ GeoLocation.location { "lon": -92.1998, "lat": 46.8147 } t GeoLocation.region_name Minnesota t _index wazuh-alerts-4.x-2022.08.16 t agent.id 000 t agent.name 139-162-192-250.ip.linodeusercontent.com t data.dstuser root t data.srcip 143.110.179.172 t data.srcport 60690 t decoder.name sshd t decoder.parent sshd t full_log Aug 16 13:00:03 139-162-192-250 sshd[635092]: Failed password for root from 143.110.179.172 port 60690 ssh2 t id 1660654803.1632522 t input.type log</pre>				

```

t input.type      log
t location        /var/log/auth.log
t manager.name    139-162-192-250.ip.linodeusercontent.com
t predecoder.hostname 139-162-192-250
t predecoder.program_name sshd
t predecoder.timestamp Aug 16 13:00:03
t rule.description sshd: authentication failed.
# rule.firedtimes 1
t rule.gdpr       IV_35.7.d, IV_32.2
t rule.gpg13      7.1
t rule.groups     syslog, sshd, authentication_failed
t rule.hipaa      164.312.b
t rule.id         5768
# rule.level      5
@ rule.mail       false
t rule.mitre.id   T1110, 001, T1021, 004
t rule.mitre.tactic Credential Access, Lateral Movement
t rule.mitre.technique Password Guessing, SSH
t rule.nist_800_53 AU.14, AC.7
t rule.pc1_dss    10.2.4, 10.2.5
t rule.tsc        CC6.1, CC6.8, CC7.2, CC7.3

```

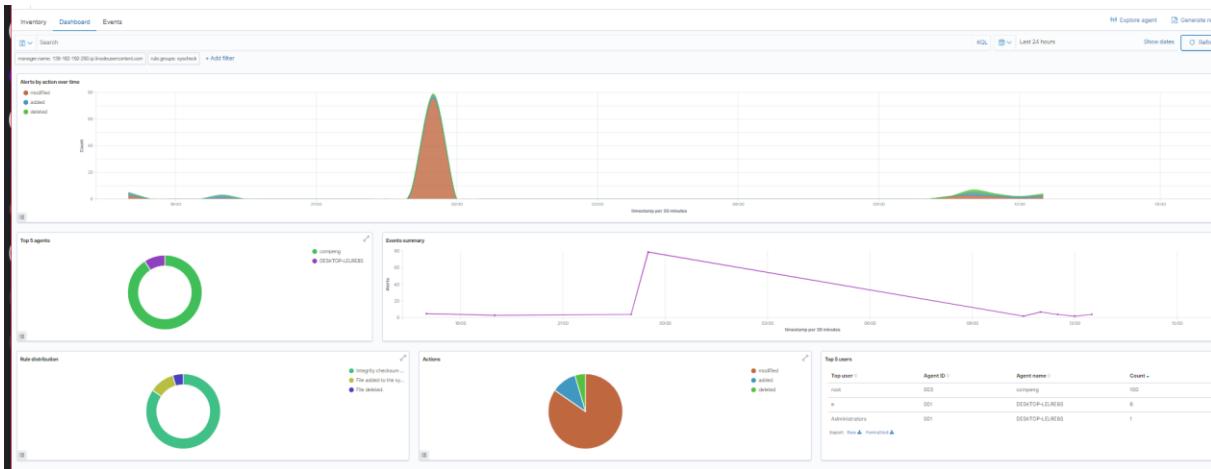
```

l e m f t rule.id      5768
# rule.level      5
@ rule.mail       false
t rule.mitre.id   T1110, 001, T1021, 004
t rule.mitre.tactic Credential Access, Lateral Movement
t rule.mitre.technique Password Guessing, SSH
t rule.nist_800_53 AU.14, AC.7
t rule.pc1_dss    10.2.4, 10.2.5
t rule.tsc        CC6.1, CC6.8, CC7.2, CC7.3
f timestamp       Aug 16, 2022 @ 16:00:03.384

```

2.Integrity Monitoring:

Warnings about file changes including permission, content, ownership and attributes can be seen in this section. For example, when a file is added to the system, the content of the file is changed, deleted or a file is downloaded to the system, we can perform detailed inspections from the Integrity Monitoring section. Dashboard, Inventory and Events. It consists of 3 parts. We can monitor graphically from the Dashboard part.

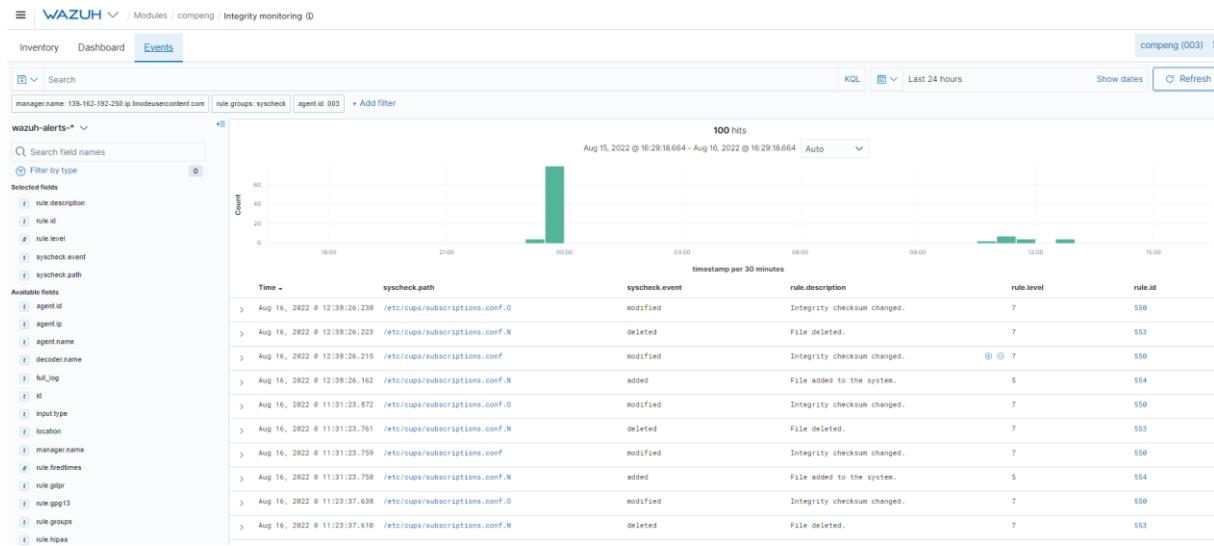


In the Inventory section, it is shown when and by whom the last change of which file was made.

The Events section provides detailed information about file modifications. The table includes the following data:

File	Last Modified	User	User ID	Group	Group ID	Permissions	Size
/bin	Aug 11, 2022 @ 17:56:01.000	root	0	root	0	rwxrwxrwx	7
/boot/System.map-5.13.0-30-generic	Feb 7, 2022 @ 17:01:37.000	root	0	root	0	r-----	5960334
/boot/System.map-5.15.0-46-generic	Aug 4, 2022 @ 21:40:38.000	root	0	root	0	r-----	6220961
/boot/config-5.13.0-30-generic	Feb 7, 2022 @ 17:01:37.000	root	0	root	0	r--r--r--	257734
/boot/config-5.15.0-46-generic	Aug 4, 2022 @ 21:44:36.000	root	0	root	0	r--r--r--	262223
/boot/grub/fonts/unicode.pf2	Aug 11, 2022 @ 18:39:17.000	root	0	root	0	r--r--r--	2395475
/boot/grub/gfxblacklist.txt	Feb 23, 2022 @ 11:50:58.000	root	0	root	0	r--r--r--	712
/boot/grub/grub.cfg	Aug 11, 2022 @ 19:24:15.000	root	0	root	0	r--r--r--	10019
/boot/grub/grubenv	Aug 16, 2022 @ 10:20:58.000	root	0	root	0	r--r--r--	1024
/boot/grub/386-pc/915resolution.mod	Aug 11, 2022 @ 18:39:14.000	root	0	root	0	r--r--r--	8016
/boot/grub/386-pc/acpi.mod	Aug 11, 2022 @ 18:39:08.000	root	0	root	0	r--r--r--	10764
/boot/grub/386-pc/adler32.mod	Aug 11, 2022 @ 18:38:59.000	root	0	root	0	r--r--r--	1396
/boot/grub/386-pc/affs.mod	Aug 11, 2022 @ 18:39:14.000	root	0	root	0	r--r--r--	5856
/boot/grub/386-pc/afs.mod	Aug 11, 2022 @ 18:38:59.000	root	0	root	0	r--r--r--	6308
/boot/grub/386-pc/ahci.mod	Aug 11, 2022 @ 18:39:11.000	root	0	root	0	r--r--r--	15640

In the Events section, we can monitor in more detail. As preparation for our project, we customized our agents by editing the ossec.conf file and the agents sent a warning to the wazuh server when there were file adding, deleting, content modification and download processes in the system by looking at the files we want to look at. as such;



In this section, all the details of the transactions can be examined.

This screenshot shows a detailed view of a single syscheck alert transaction. It includes a timestamp, path, event type, rule description, level, and ID. Below this, there is an 'Expanded document' section containing JSON data with various fields like index, agent.id, and rule.description. The rule.description field contains a detailed log of file changes, including mode, mtime, inode, md5, sha1, sha256, and file paths.

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Aug 16, 2022 @ 12:38:26.238	/etc/cups/subscriptions.conf.O	modified	Integrity checksum changed.	7	550

Expanded document

Table JSON

```

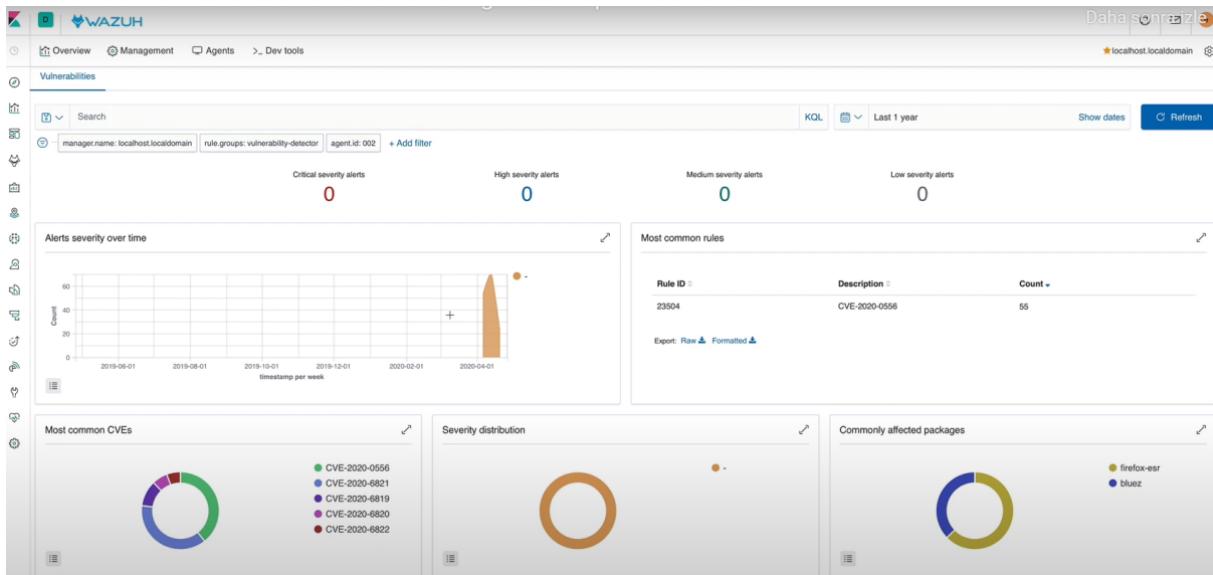
{
  "index": "wazuh-alerts-4.x-2022.08.16",
  "agent.id": "003",
  "agent.ip": "10.0.2.15",
  "agent.name": "compeng",
  "decoder.name": "syscheck_integrity_changed",
  "full_log": {
    "path": "/etc/cups/subscriptions.conf.O",
    "mode": "realtime",
    "changed_attributes": "mtime,inode,md5,sha1,sha256",
    "old_modification_time": "1660638217",
    "new_modification_time": "1660638683",
    "old_inode": "524435",
    "new_inode": "527310",
    "old_md5sum": "23d8c0217de7c72514926223190ddcbe",
    "new_md5sum": "a014a004a01f5a077774a0e0d0f54111a7"
  },
  "id": "1660642706.1214617",
  "input.type": "log",
  "location": "syscheck",
  "manager.name": "139-162-192-250.ip.linodeusercontent.com",
  "rule.description": "Integrity checksum changed.",
  "rule.firetimes": "3",
  "rule.gdpr": "II_5.1.f",
  "rule.gpg13": "4.11",
  "rule.groups": "ossec, syscheck, syscheck_entry_modified, syscheck_file"
}

```

3. Vulnerabilities:

Using the Vulnerability Detector module, Wazuh is able to detect vulnerabilities in applications installed on agents. To detect vulnerabilities, agents can collect a list of installed applications locally and periodically send it to the administrator (where it is stored in local SQLite databases, one for each agent). In addition, the administrator creates a global database of vulnerabilities from public CVE repositories, which he then uses to cross-correlate with his agent's application inventory data.

After the global vulnerability database (with CVEs) is created, the detection process searches the inventory databases (unique per agent) for vulnerable packages. Alerts are generated when a CVE (Common Vulnerabilities and Exposures) affects a package known to have been installed on one of the monitored hosts. A package is labeled as a vulnerability when its version is within the affected range of a CVE. Results are presented as alerts and are also stored in a per-agent vulnerabilities inventory. This way, you can check for recent scan alerts or query each agent's inventory of vulnerabilities.



4. MITRE ATT&CK:

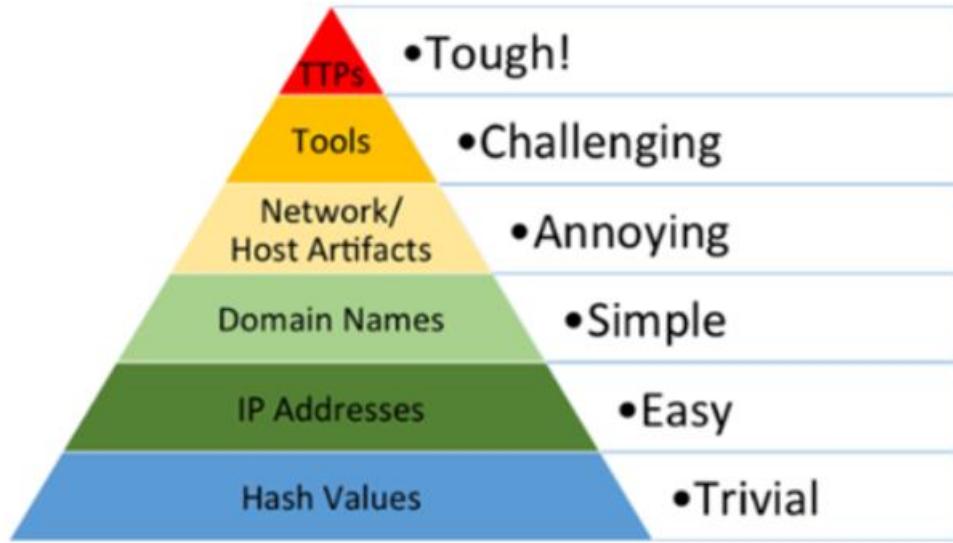
MITER stands for ATT&CK, MITER stands for Hostile Tactics, Techniques and Common Knowledge (ATT&CK). The MITER ATT&CK framework is a selected knowledge base and model for cyber attacker behavior that reflects the various stages of an adversary's attack lifecycle and the known platforms they target. Its tactical and technical abstraction in the model provides a common classification of individual enemy actions understood by both the offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for enemy action and specific ways to defend against it.

-The most up-to-date information center showing the Behavior anatomy of an attack.

- Created by Observing Attacks that occur in the real world.
- Based on Tactics, Techniques and Procedures.

It is a free, open and accessible information center.

-Community-Driven, Supported by 100+ Organizations and People

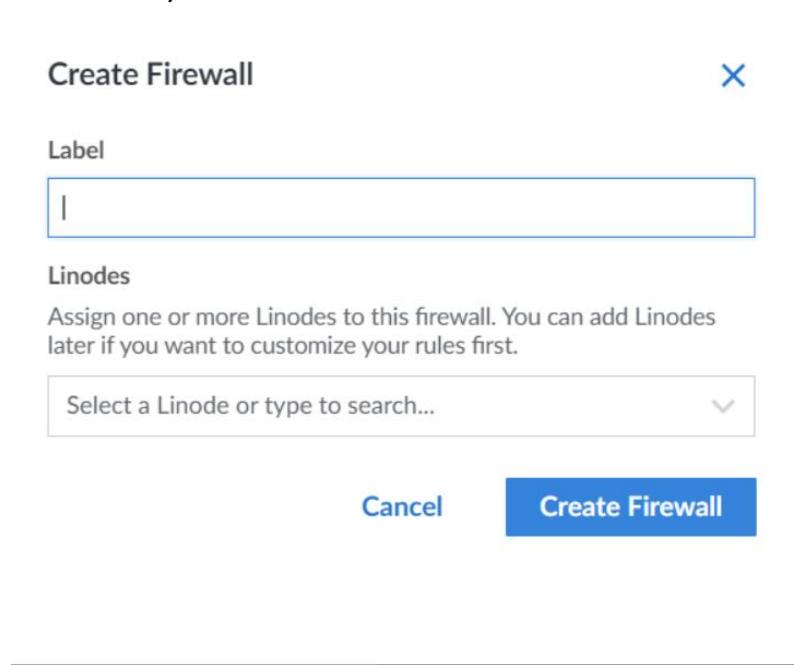


CREATING A FIREWALL ON WAZUH AND WRITE RULES

1- Click the Firewalls button.

Label	Status	Plan	IP Address	Region	Last Backup
wazuh	Running	Linode 4 GB	178.79.155.124	London, UK	Never

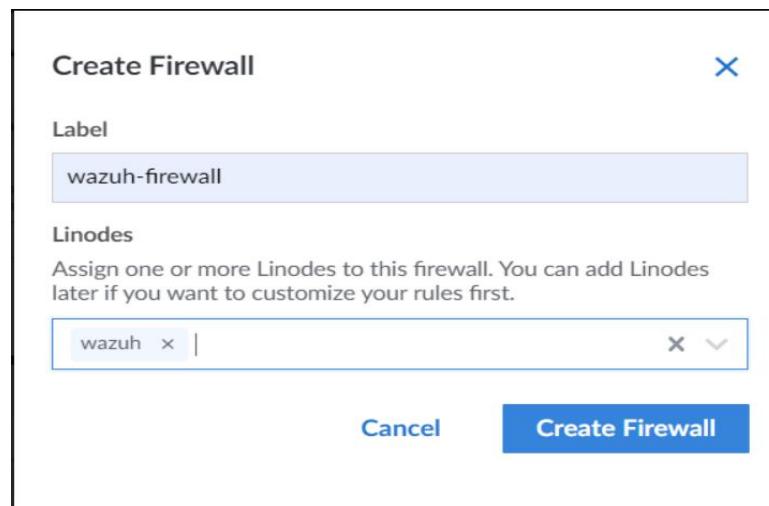
2- Click on the create firewall button from the page that appears and the following screen is encountered;



The screenshot shows a 'Create Firewall' dialog box. At the top left is the title 'Create Firewall' and at the top right is a blue 'X' button. Below the title is a 'Label' field containing a single character 'I'. Underneath is a 'Linodes' section with a descriptive text: 'Assign one or more Linodes to this firewall. You can add Linodes later if you want to customize your rules first.' Below this is a dropdown menu placeholder 'Select a Linode or type to search...'. At the bottom are two buttons: 'Cancel' on the left and a large blue 'Create Firewall' button on the right.

3- Since we will use firewall for wazuh, we filled this screen as follows;

Instead of “label”, the name for the firewall is written. In the “linode” part, the tool that we will use the firewall is selected and the create firewall button is clicked.



The screenshot shows the same 'Create Firewall' dialog box as above, but with the 'Label' field now containing 'wazuh-firewall'. In the 'Linodes' section, the dropdown menu shows 'wazuh' with a delete 'x' icon and a dropdown arrow. The 'Create Firewall' button at the bottom is still blue and prominent.

This is how it looks when the firewall occurs.

Firewalls				Docs	Create Firewall
Firewall	Status	Rules	Linodes		
wazuh-firewall	Enabled	No rules	wazuh	Disable	Delete

4- Clicking on the name of the Firewall opens the page where the rules are written. Rules can be written for the Firewall created in this section.

The screenshot shows a web-based firewall configuration interface. At the top, there's a navigation bar with 'Firewalls / wazuh-firewall' and a pencil icon, followed by 'Docs'. Below the navigation, there are two tabs: 'Rules' (which is selected) and 'Linodes'. The main area is divided into two sections: 'Inbound Rules' and 'Outbound Rules'. Each section has a table header with columns: Label, Protocol, Port Range, Sources, and Action. Under 'Inbound Rules', it says 'No inbound rules have been added.' and includes a note about the default inbound policy. Under 'Outbound Rules', it says 'No outbound rules have been added.' and includes a note about the default outbound policy. At the bottom right of each section is a blue 'Add an [Inbound/Outbound] Rule' button. At the very bottom right of the interface are two buttons: 'Discard Changes' and 'Save Changes'.

After adding any rule, click the save changes button to save the changes.