

## Wazuh Kurulum ve Dağıtım

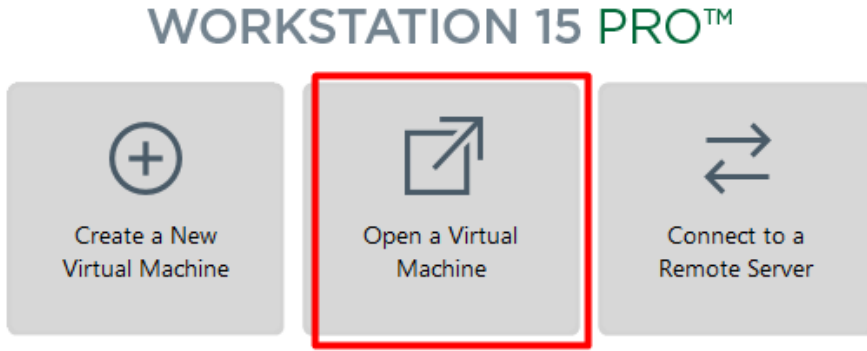
Wazuh açık kaynaklı güvenlik izleme çözümdür. Wazuh ile tehdit algılama vb. süreçleri takip edebilirsiniz. Detaylı bilgiye aşağıda adresten ulaşabilirsiniz.

<https://wazuh.com/>

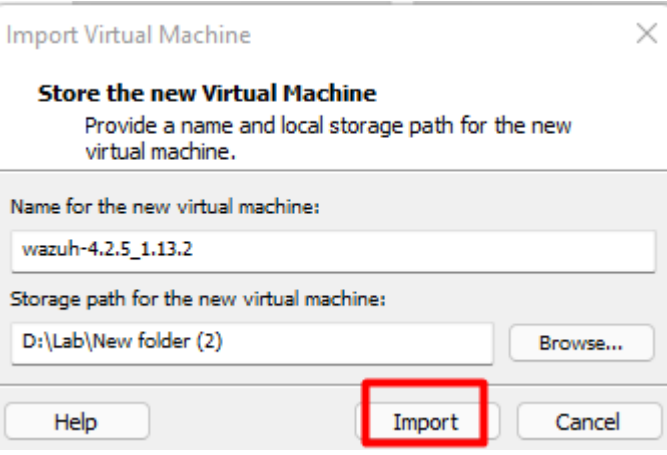
Aşağıdaki adresten \*.ova olarak indirme işlemini yapabilirsiniz.

<https://documentation.wazuh.com/current/virtual-machine/virtual-machine.html>

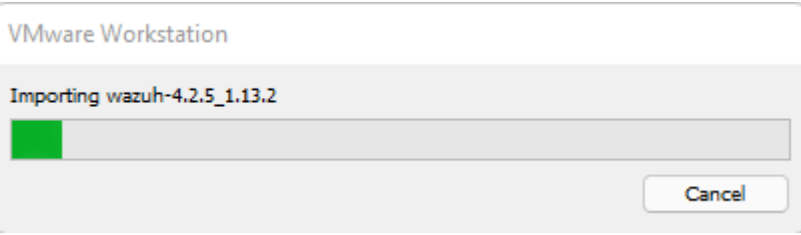
Ortamımızda VMware Workstation bulunmaktadır. Open a Virtual Machine ile indirmiş olduğumuz ova dosyamızı gösterelim.



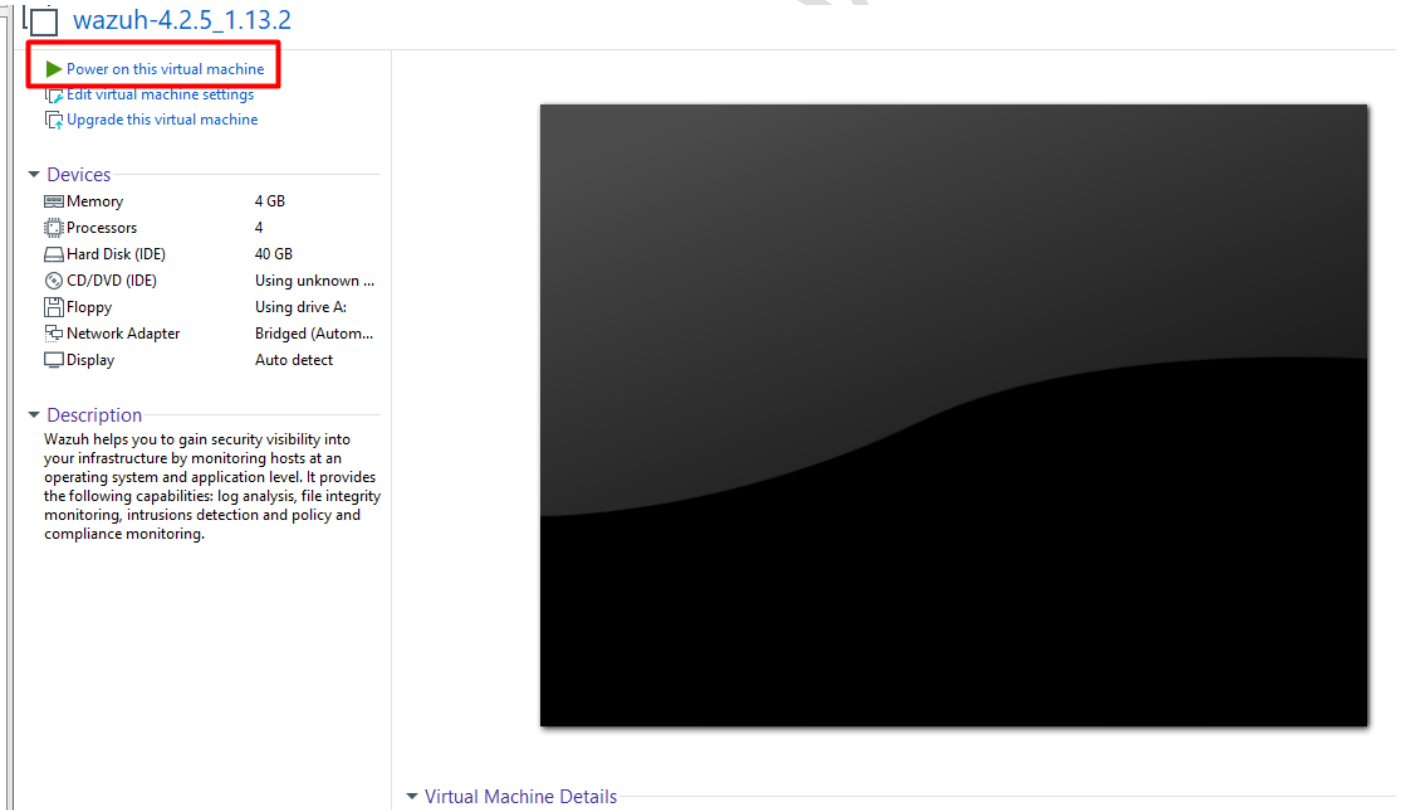
İmport işlemini gerçekleştirelim.



İşlemimiz başladı.



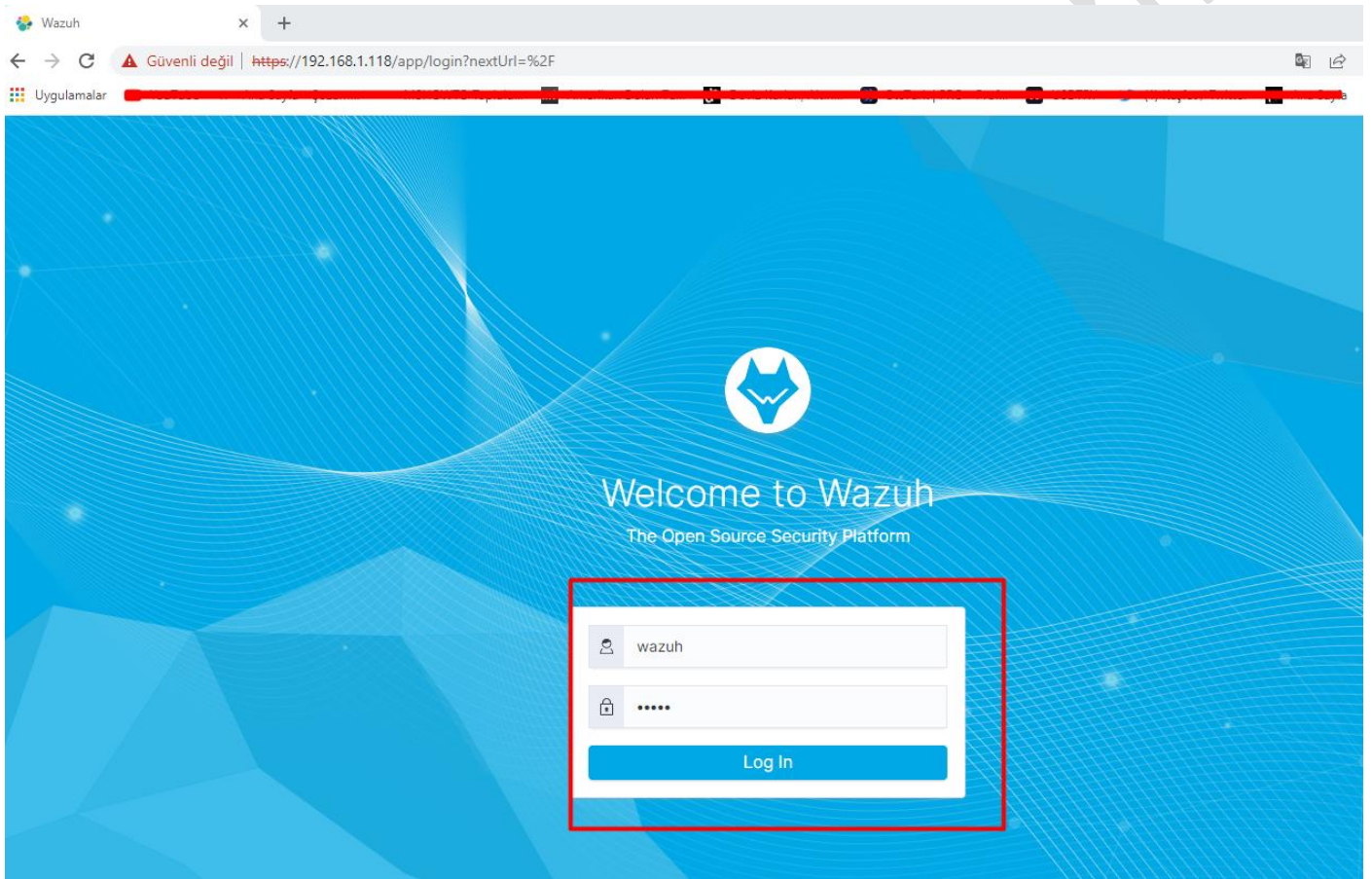
Aktarma işlemimiz tamamlandıktan sonra sunucumuzu açalım.



Ekranımız açıldı ve default olarak user/pass wazuh olarak gelmektedir. Giriş yapalım ve ip address komutunu çalıştırdık ip adresini öğrenelim.

```
[wazuh@wazuh-manager ~]# ip address
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 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        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 00:0c:29:3d:91:fe brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.118/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 86328sec preferred_lft 86328sec
    inet6 fd34:7e00:8193:3800:20c:29ff:fe3d:91fe/64 scope global mngtmpaddr dynamic
        valid_lft 7128sec preferred_lft 3528sec
    inet6 fe80::20c:29ff:fe3d:91fe/64 scope link
        valid_lft forever preferred_lft forever
[wazuh@wazuh-manager ~]#
```

Ip adresimiz ile web üzerinden https:\\ipadresini ile giriş yapalım. User/pass:wazuh



Ekranımız açıldı.

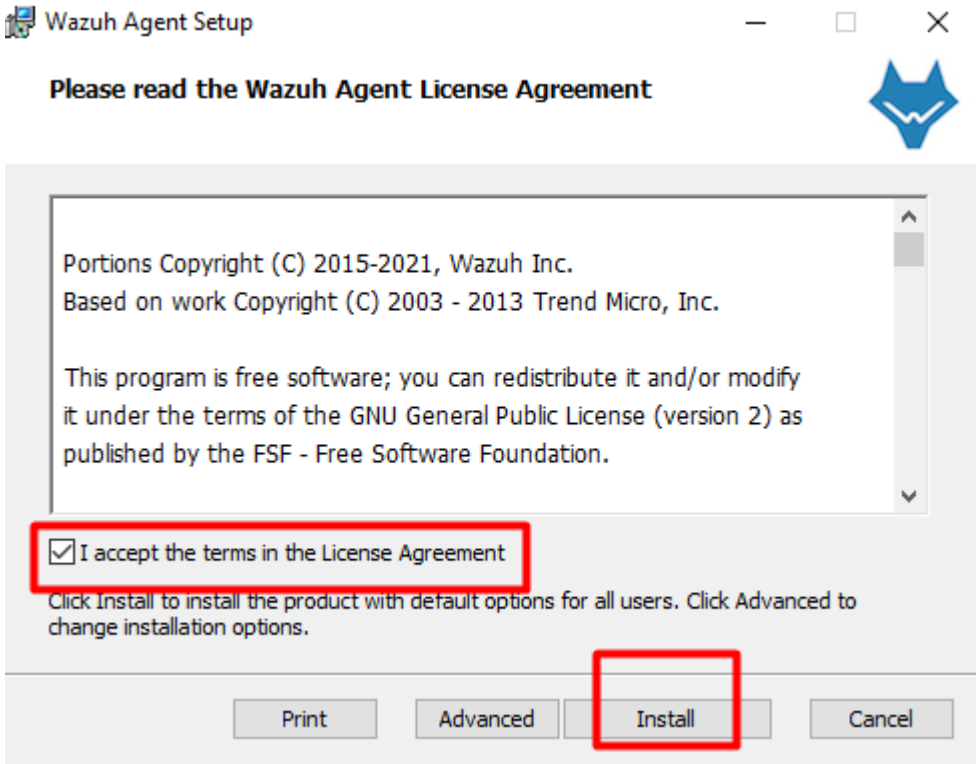
The screenshot shows the Wazuh dashboard interface. At the top, there are four status indicators: Total agents (0), Active agents (0), Disconnected agents (0), and Never connected agents (0). Below these, a yellow banner states "No agents were added to this manager. Add agent". The main content is divided into two sections: "SECURITY INFORMATION MANAGEMENT" and "AUDITING AND POLICY MONITORING". Under "SECURITY INFORMATION MANAGEMENT", there are three cards: "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.), and "Policy monitoring" (Verify that your systems are configured according to your security policies baseline.). Under "AUDITING AND POLICY MONITORING", there are two cards: "System auditing" (Audit users behavior, monitoring command execution and alerting on access to critical files.) and "Security configuration assessment" (Scan your assets as part of a configuration assessment audit.).

Şimdi agent ekleme işlemimiz yapalım. Örnek olarak AD sunucumu açıyoruz ve aşağıdaki adresten msi paketini indirip çalıştırıyoruz.

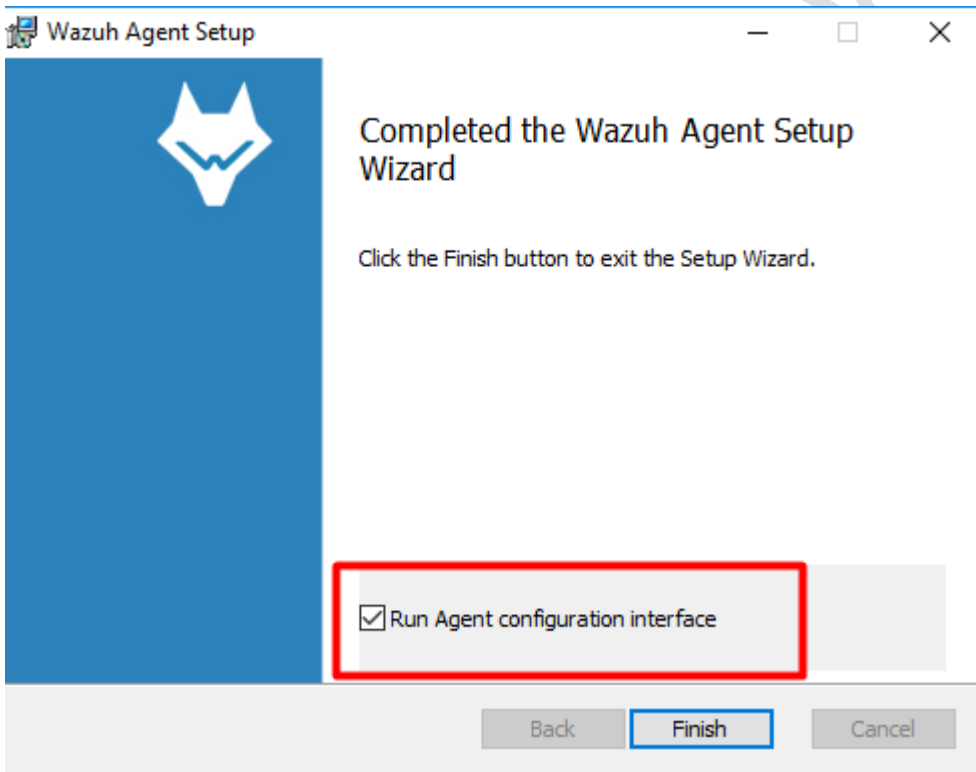
<https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>

The screenshot shows the Wazuh documentation page for Windows agent installation. The page title is "WAZUH Docs" and the version is "4.2 (current)". The left sidebar contains a navigation menu with items like "Getting started", "Installation guide", "Requirements", "Wazuh server", "Wazuh agent", "Linux", "Windows", "macOS", "AIX", "HP-UX", "Solaris", "Deployment variables", "Packages list", "More installation alternatives", "Upgrade guide", "User manual", and "Wazuh cloud service". The main content area has a search bar and a search button. Below the search bar, there is a section titled "To perform the installation, administrator privileges are required." followed by two numbered steps: 1. To start the installation process, download the Windows installer. 2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI). The "CLI" tab is selected, and the content shows instructions for deploying the Wazuh agent to your system, including a note about editing the WAZUH\_MANAGER and WAZUH\_REGISTRATION\_SERVER variables. Two code blocks are provided: one for using CMD and one for using PowerShell. The CMD code is: `wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_SERVER="10.0.0.2"`. The PowerShell code is: `.\wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="10.0.0.2" WAZUH_REGISTRATION_SERVER="10.0.0.2"`. Below the code blocks, there is a note about additional deployment options and a final note stating that the installation process is now complete and the Wazuh agent is successfully installed, registered, and configured, running on your Windows system.

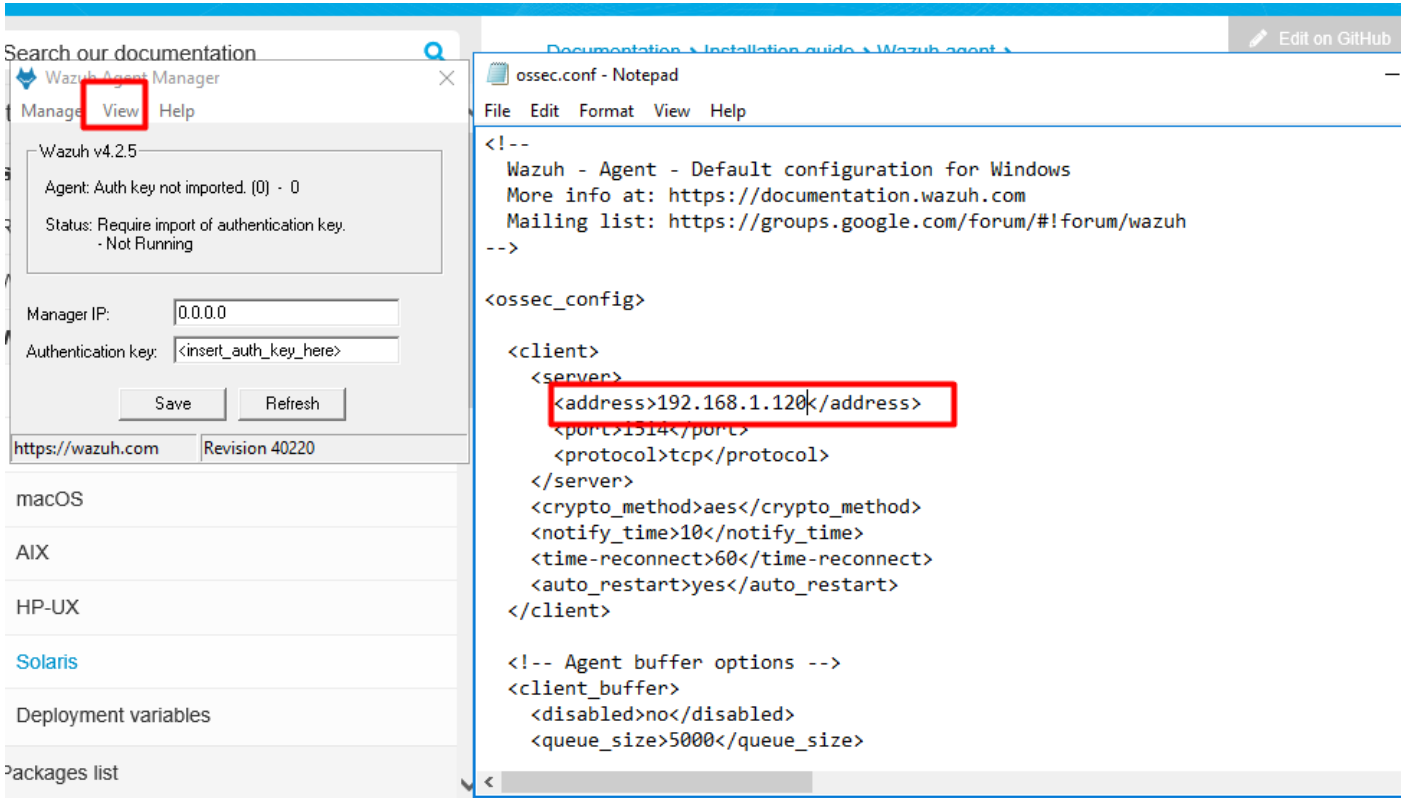
Lisans sözleşmesini kabul edip install ile kurulumu yapıyoruz.



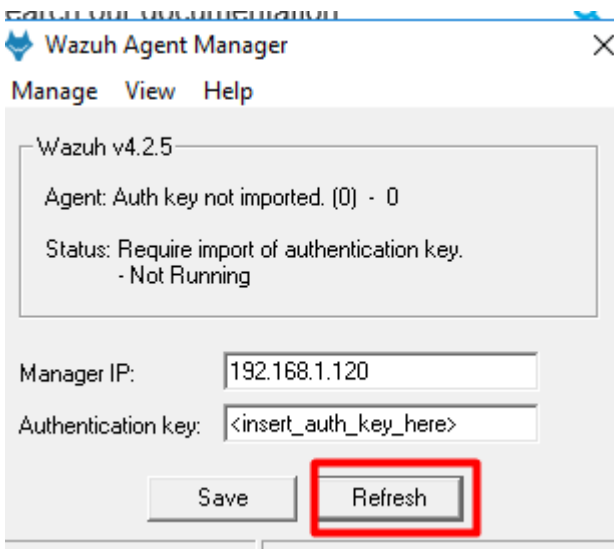
Kurulum tamamlandıktan sonra run agent configuration butonuna basıyoruz.



Karşımıza çıkan ekranda view>view config ekranına geliyoruz. Açılan ossec.conf dosyasında server kısmına wazuh server ip adresini girip kaydedip çıkıyoruz.



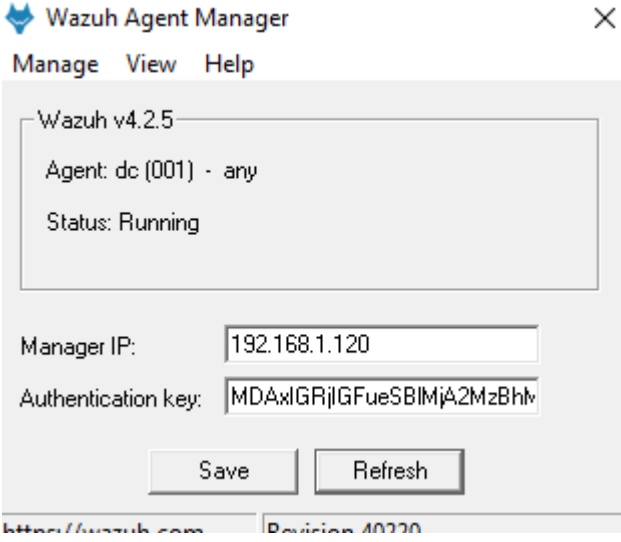
Refresh ile sunucunun geldiğini göreceğiz.



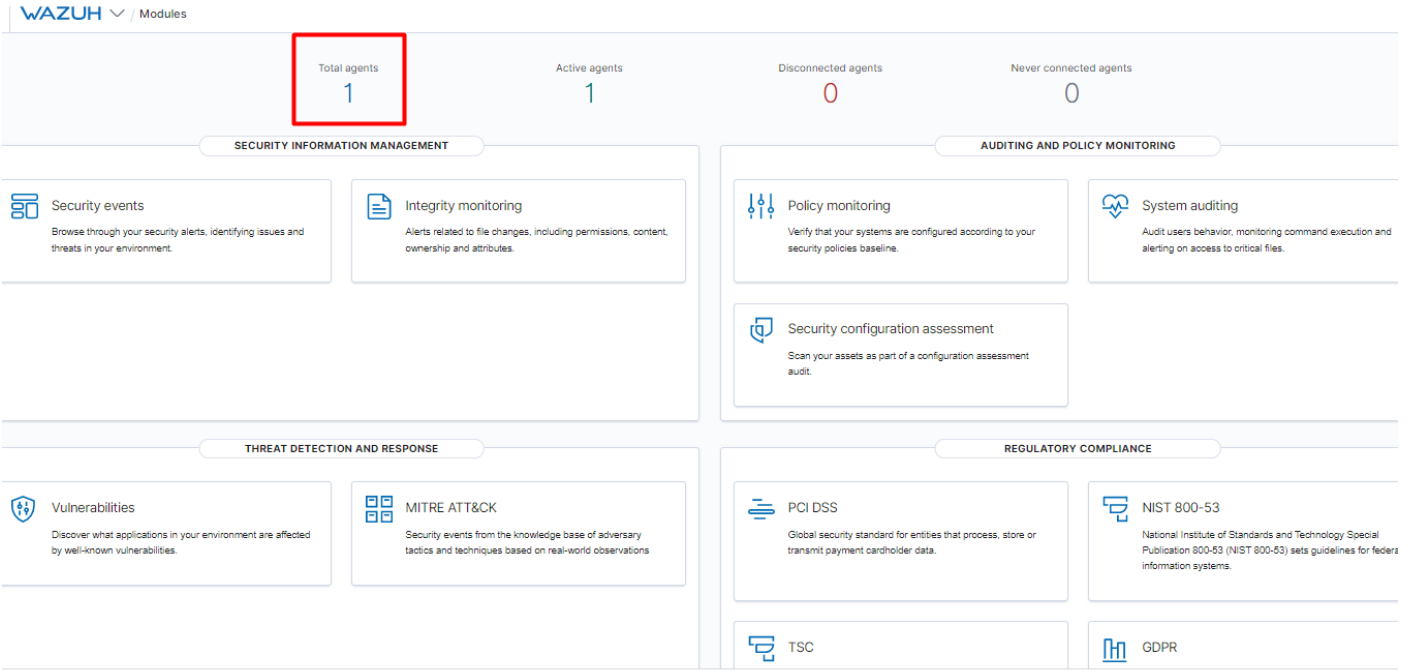
Key oluşturmak için powershell ekranında aşağıdaki komutu giriyoruz.

```
.\wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="10.0.0.2"  
WAZUH_REGISTRATION_SERVER="10.0.0.2"  
PS C:\Users\Administrator> cd..  
PS C:\Users> .\Administrator\Downloads\wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="192.168.1.120" WAZUH_REGISTRATION_SERVE  
R="192.168.1.120"  
PS C:\Users> _
```

Authentication key'in geldiğini görüyoruz.




Wazuh ekranımıza geri döneelim ve kontrol edelim. Sunucumuzun geldiğini görüyoruz.



Üzerine tıkladığımızda ayrıntılara ulaşabiliriz.

**STATUS**

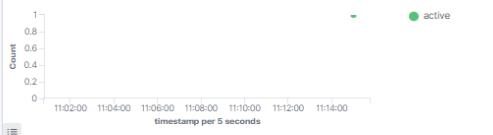


**DETAILS**

Active: 1 | Disconnected: 0 | Never connected: 0 | Agents coverage: 100.00%



Last registered agent: dc | Most active agent: dc

**EVOLUTION**



Filter or search agent Refresh

Agents (1) Deploy new agent | Export formatted

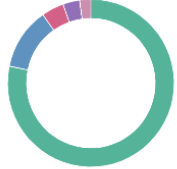
ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	dc	192.168.1.114	default	Microsoft Windows Server ...	node01	v4.2.5	Feb 28, 2022 @ 11:...	Feb 28, 2022 @ 11:...	active	 

Status: active | IP: 192.168.1.114 | Version: Wazuh v4.2.5 | Groups: default | Operating system: Microsoft Windows Serv... | Cluster node: node01 | Registration date: Feb 28, 2022 @ 11:13:50.000 | Last keep alive: Feb 28, 2022 @ 11:16:20.000

**MITRE**

- Active
- Access
- Escalation

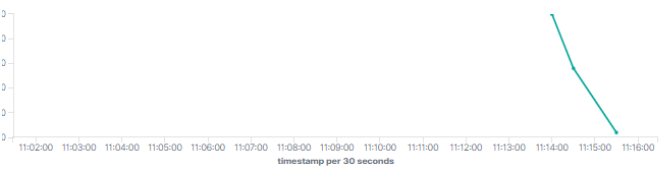
**Compliance** (PCI DSS)



**FIM: Recent events**

Time ↓	Path	Action	Rule description	Rule Level	Rule Id
No recent events					

**Agents count evolution**



**SCA: Last scan**

Benchmark for Windows audit: sca\_wir\_audit

This document provides a way of ensuring the security of the Windows systems.

Pass	Fail	Total checks	Score
27	7	71	79%

Start time: Feb 28, 2022 @ 11:14:19.000 | Duration: < 1s

Faydalı olması dileğiyle...

WWW