Wazuh Kurulum ve Dağıtım

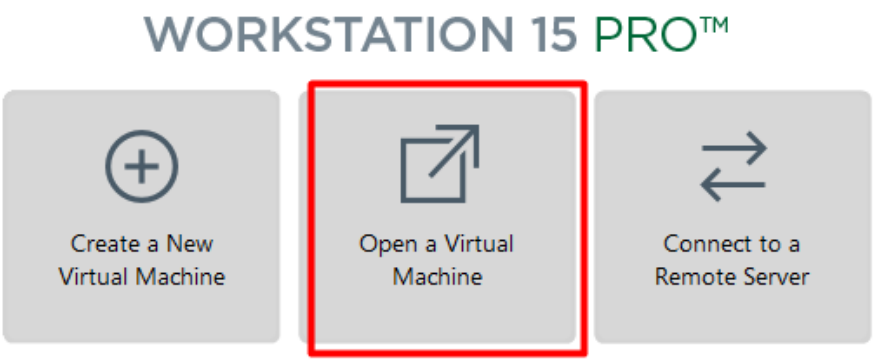
Wazuh açık kaynaklı güvenlik izleme çözümüdür. Wazuh ile tehdit algılama vb. süreçleri takip edebilirsiniz. Detaylı bilgiye aşağıda adresten ulaşabilirsiniz.

https://wazuh.com/

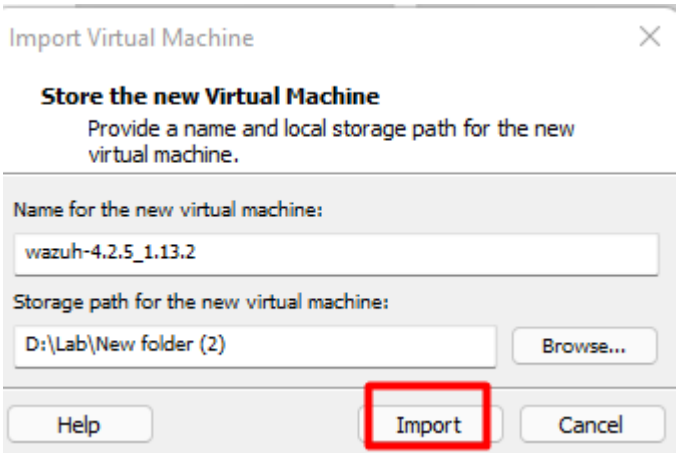
Aşağıdaki adresten *.ova olarak indirme işlemini yapabilirsiniz.

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

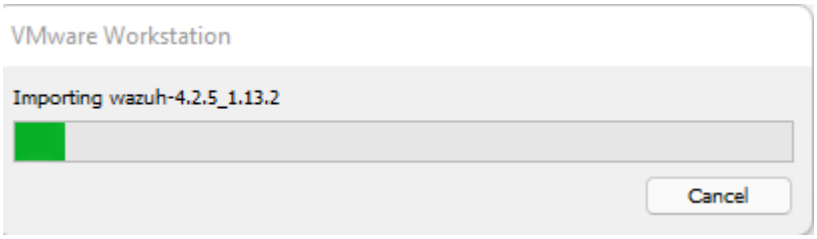
Ortamımızda VMware Workstation bulunmaktadır. Open a Virtual Machine ile indirmiş olduğumuz ova dosyamızı gösterelim.



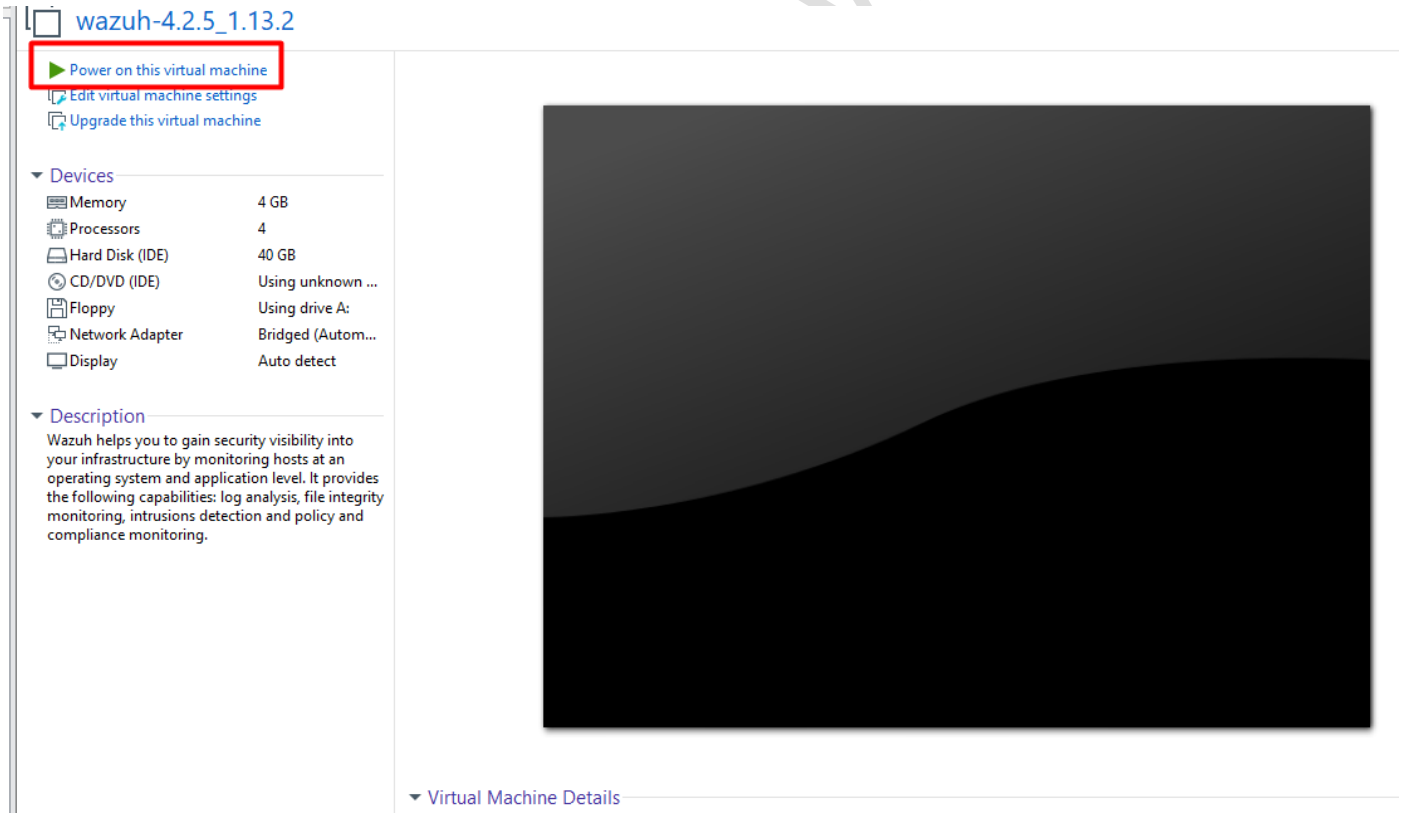
İmport işlemini gerçekleştirelim.



İşlemimiz başladı.



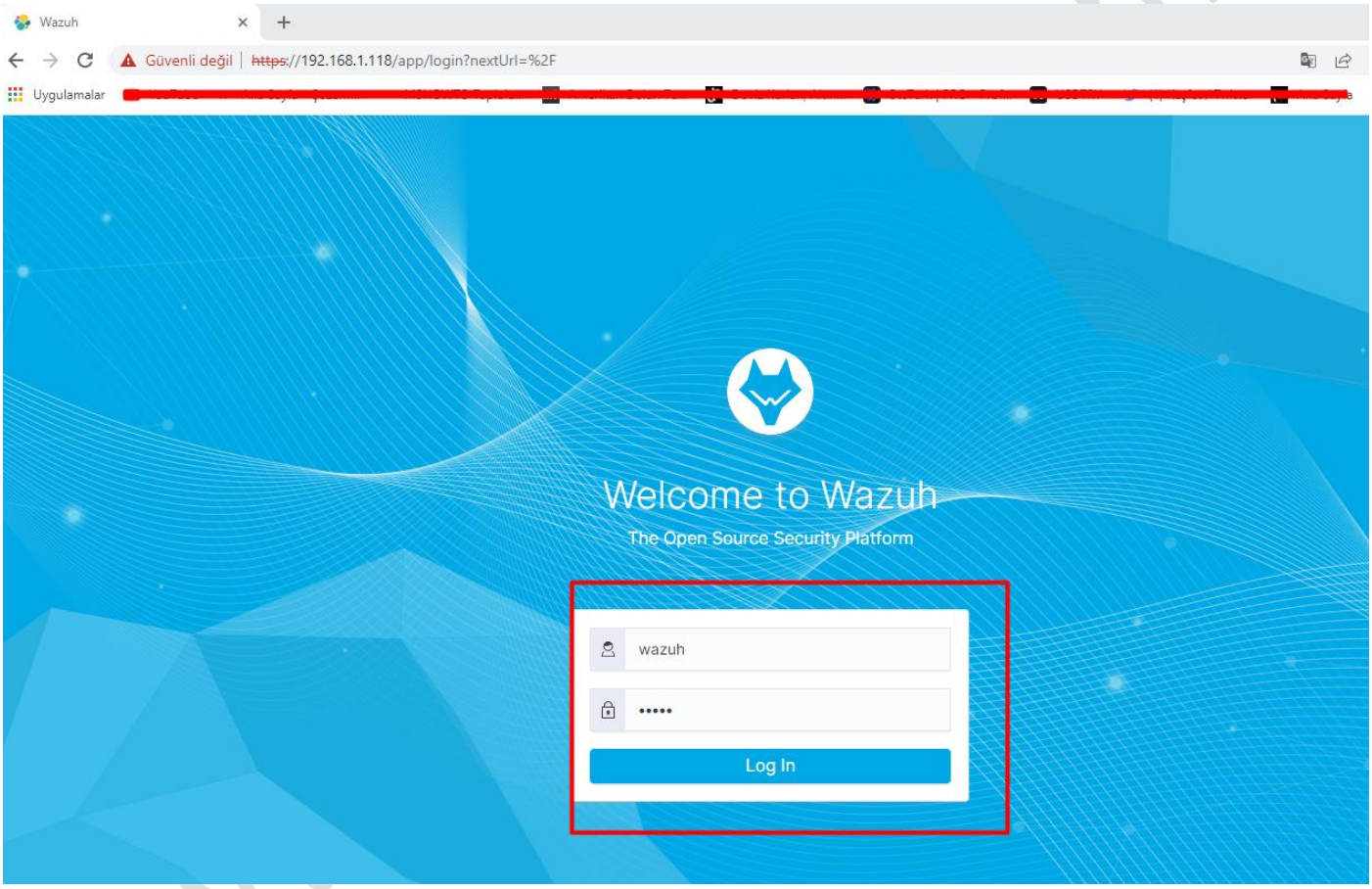
Aktarma işlemimiz tamamlandıktan sonra sunucumuzu açalım.



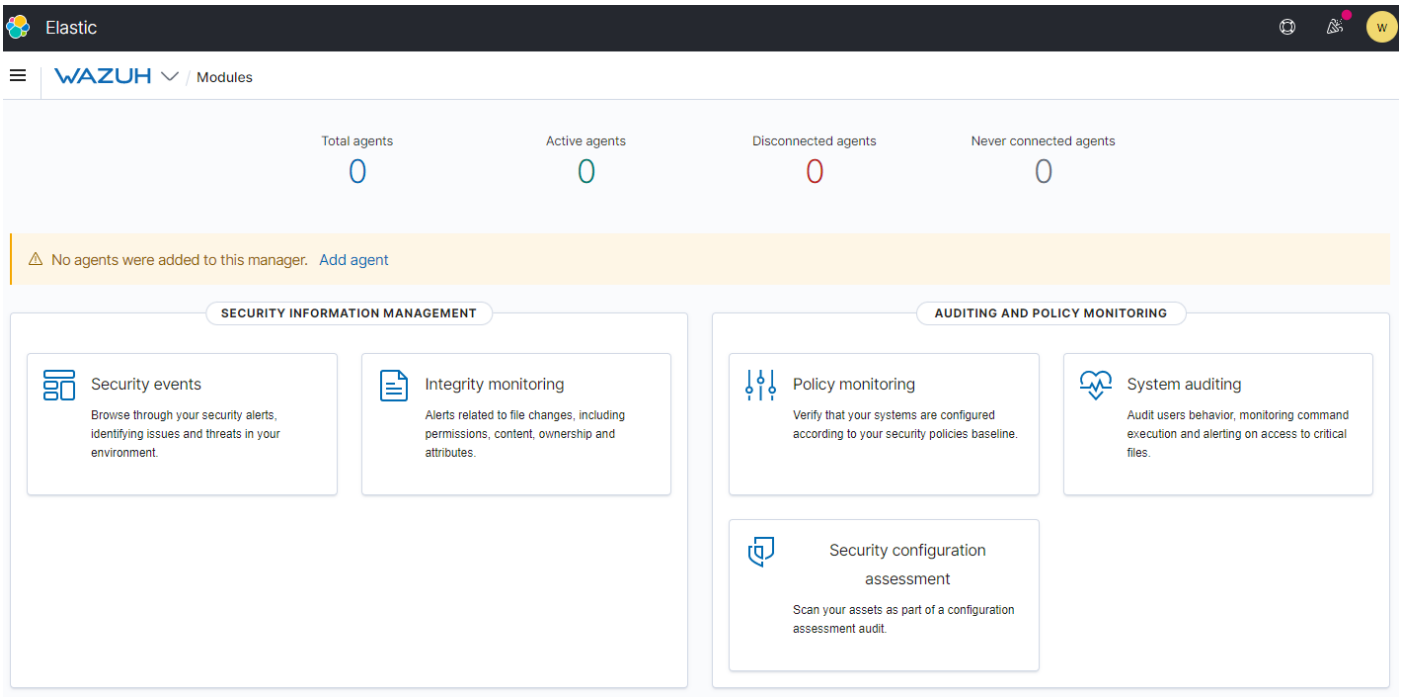
Ekranımız açıldı ve default olarak user/pass wazuh olarak gelmektedir. Giriş yapalım ve ip address komutunu çalışıtıp ip adresini öğrenelim.

```
[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 100
0
    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:\\ipadresi ile giriş yapalım. User/pass:wazuh

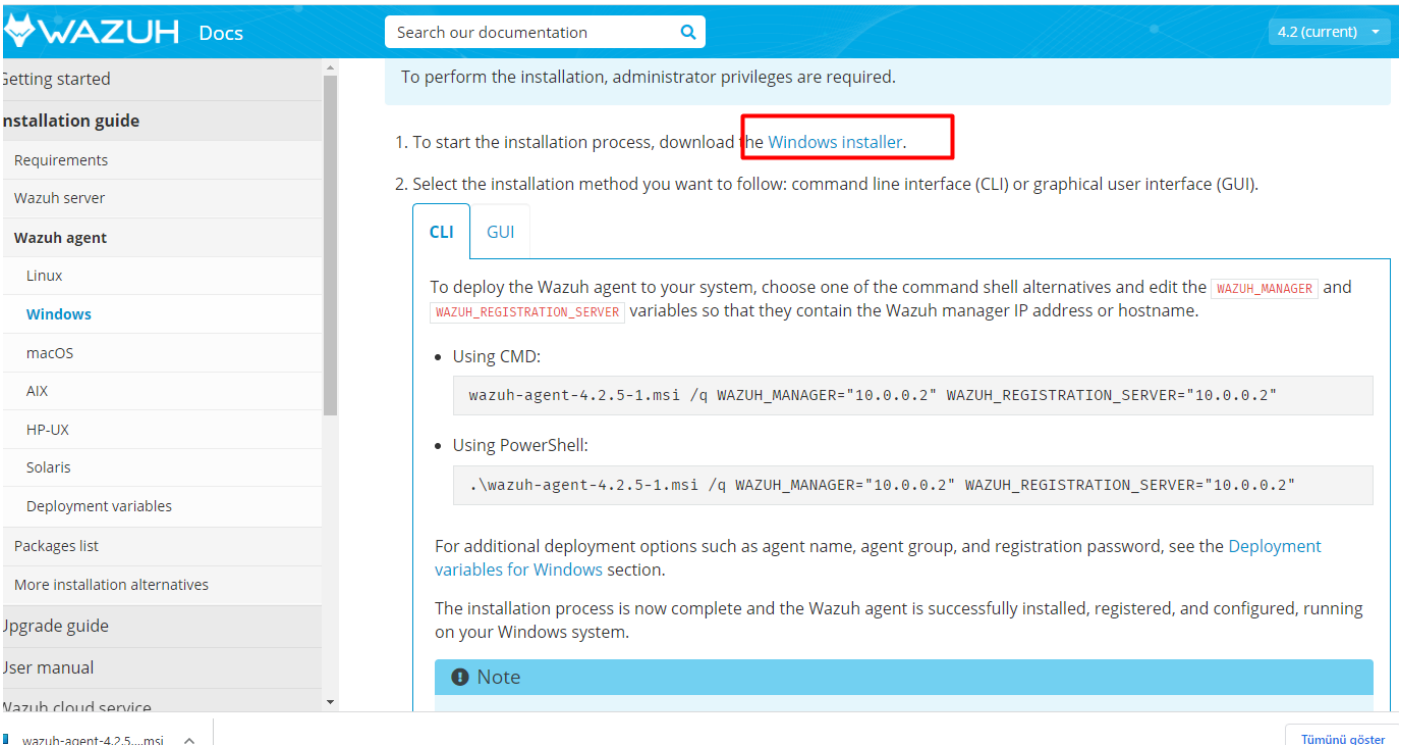


Ekranımız açıldı.

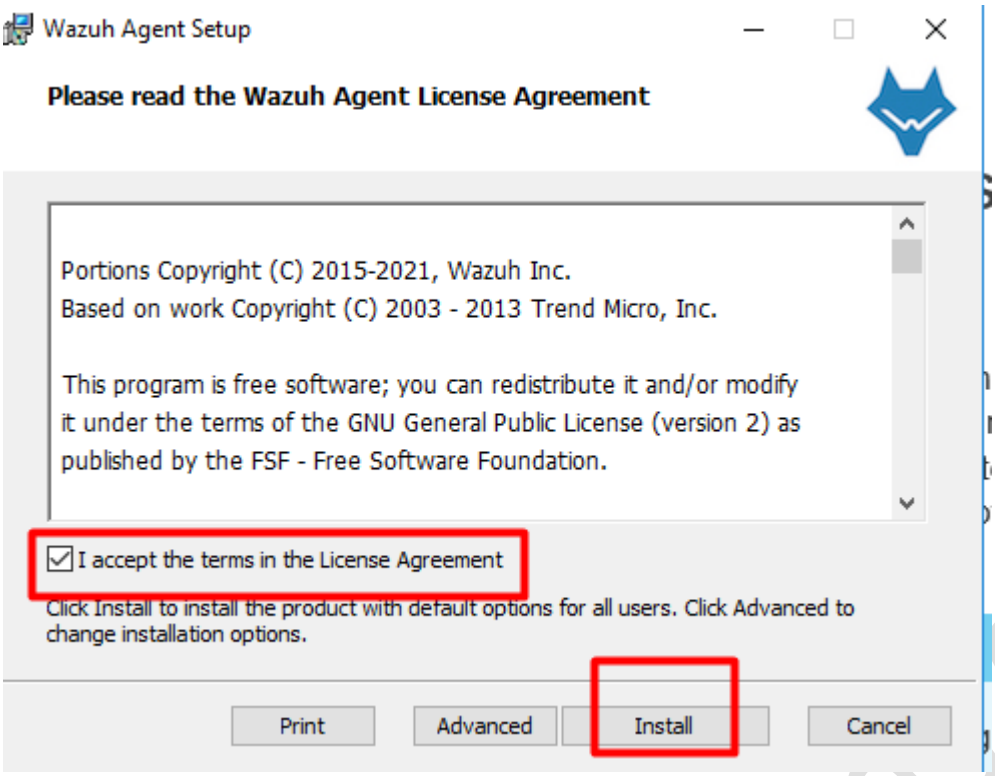


Şimdi agent ekleme işlemimiz yapalım. Örnek olarak AD sunucumu açıyoruz ve aşağıdaki adresten msi paketini indirip çalıştırıyoruz.

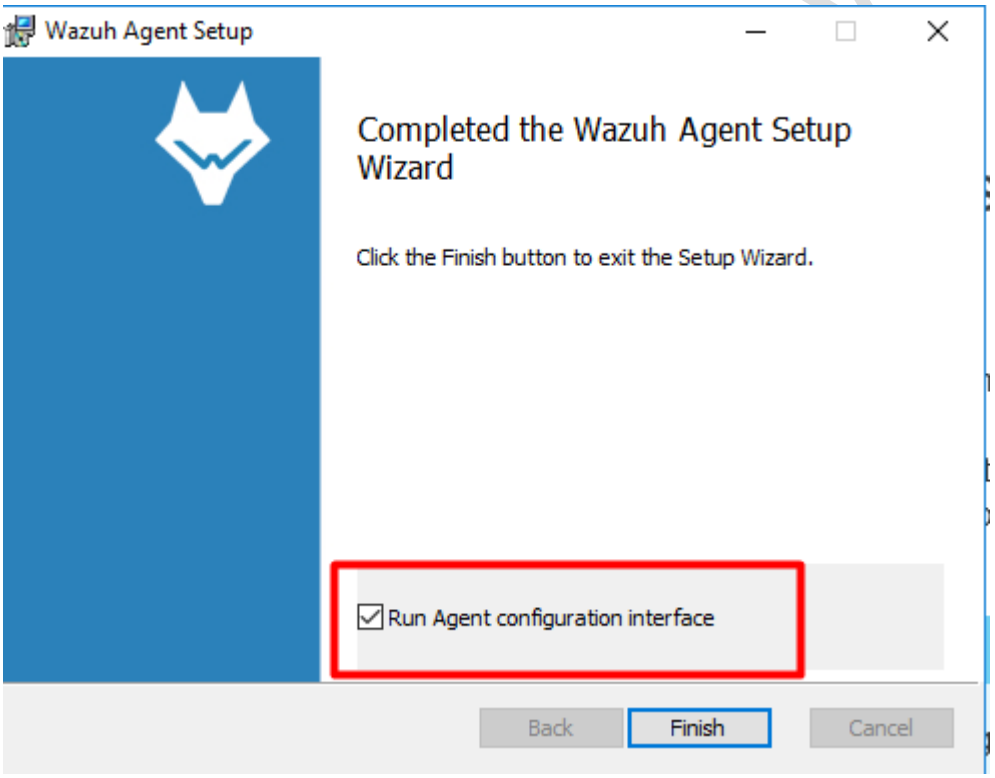
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html



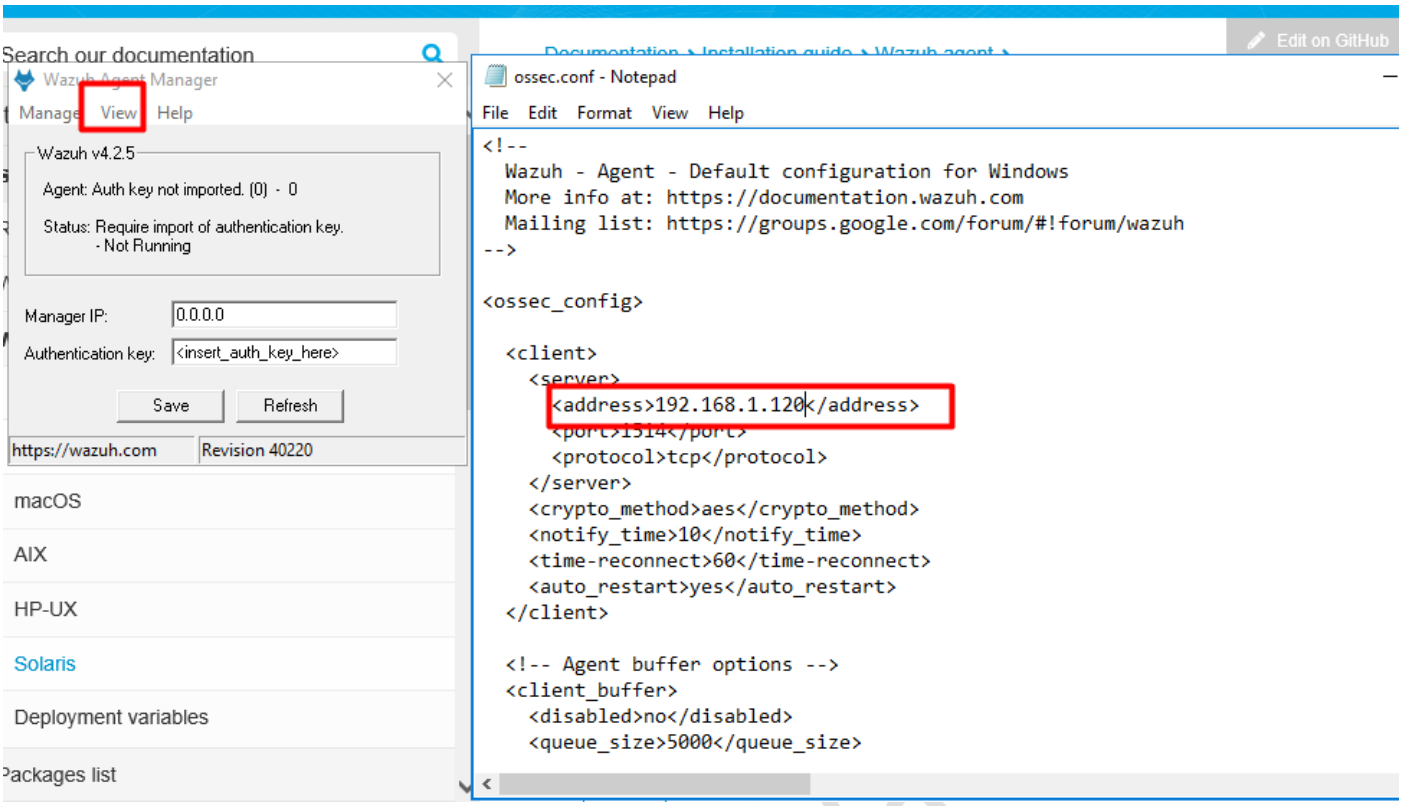
Lisans sözleşmesini kabul edip install ile kurulumu yapıyoruz.



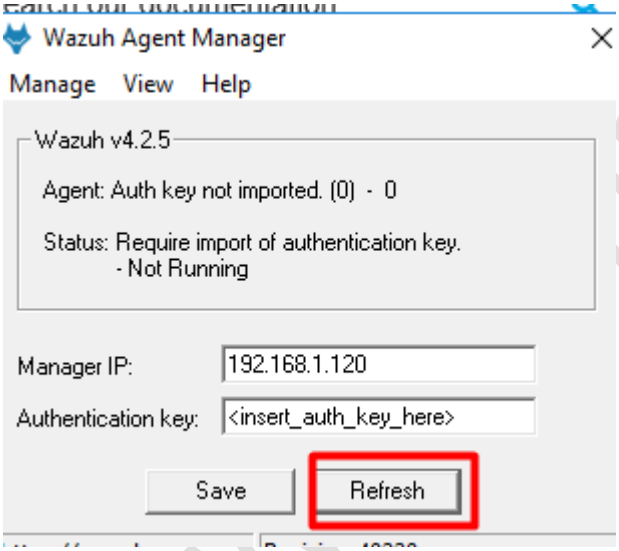
Kurulum tamamlandıktan sonra run agent configuration butonuna basıyoruz.



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.

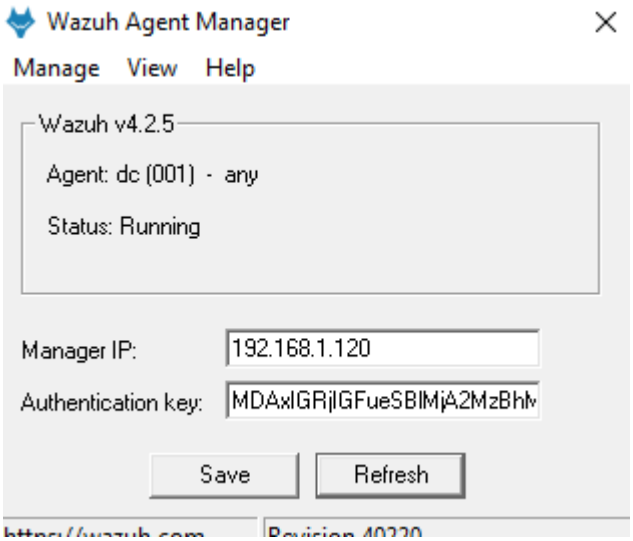


Key oluşturmak için powershell ekranında aşağıdaki komutu giriyoruz.

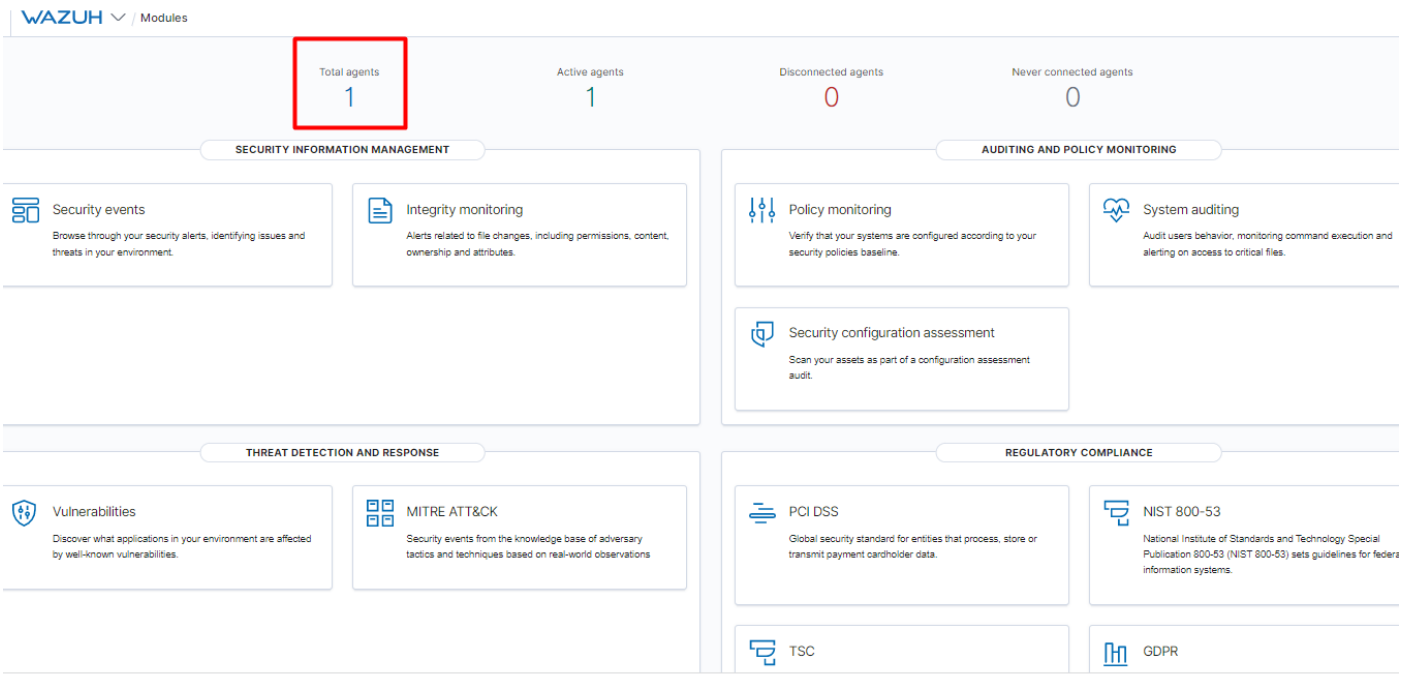
```
.\wazuh-agent-4.2.5-1.msi /q WAZUH_MANAGER="10.0.0.2"
WAZUH_REGISTRATION_SERVER="10.0.0.2"
```

```
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>
```

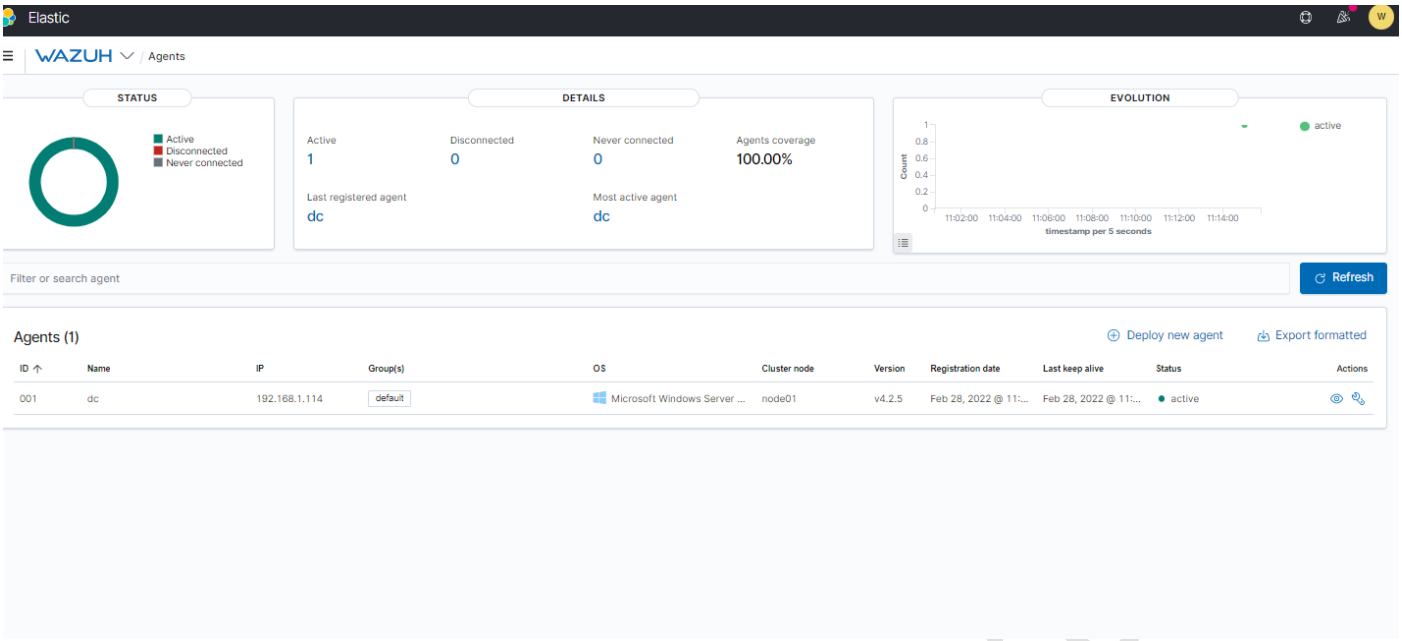
Authentication key'in geldiğini görüyoruz.

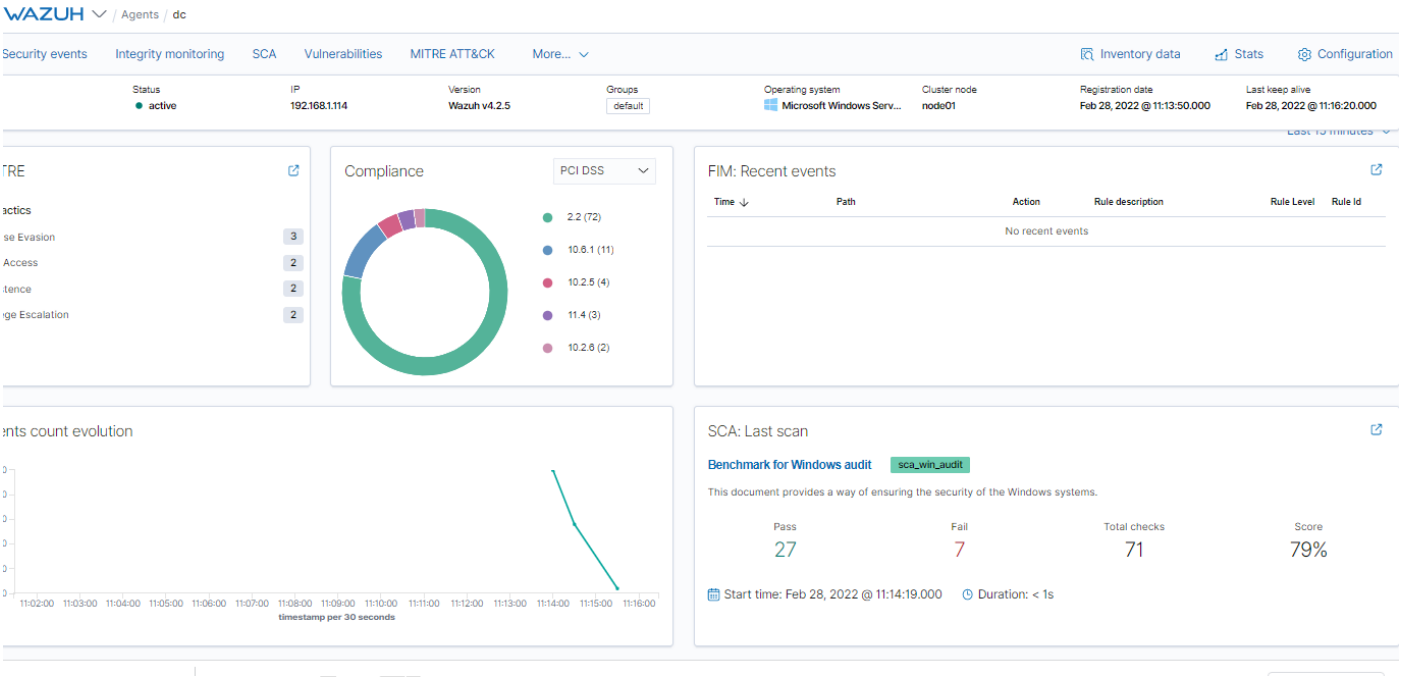


Wazuh ekranımıza geri dönelim ve kontrol edelim. Sunucumuzun geldiğini görüyoruz.



Üzerine tıkladığımızda ayrıntılara ulaşabiliriz.





Faydalı olması dileğiyle...