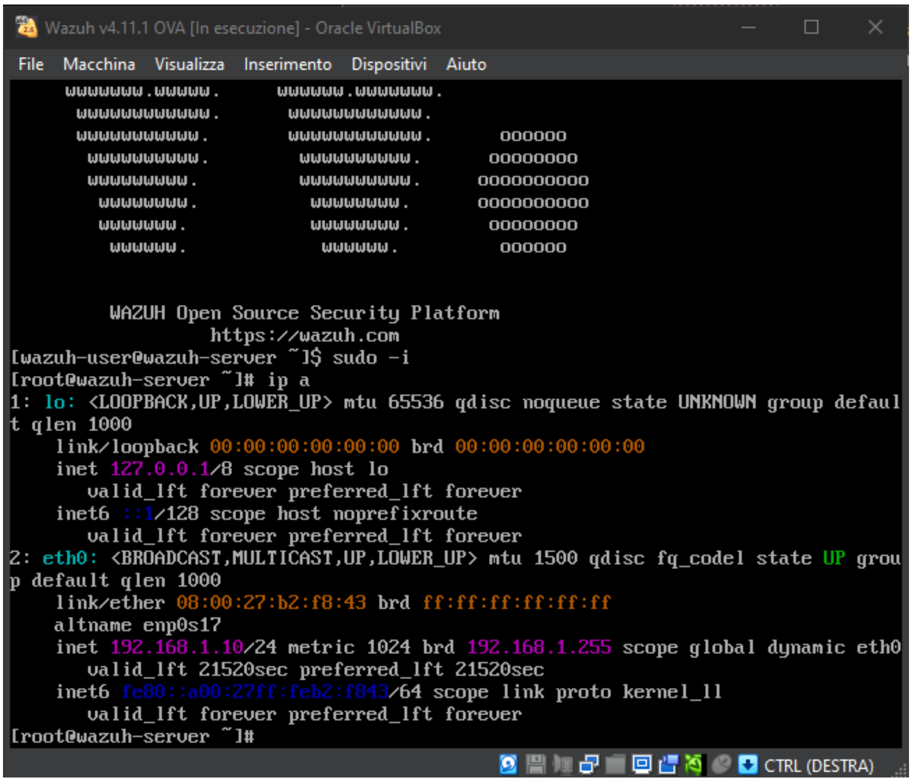
Installazione Wazuh Extra

Iniziamo con il download di wazuh tramite il sito ufficiale, installiamo l'ova sulla nostra VirtualBox e procediamo con la configurazione seguendo la guida online.

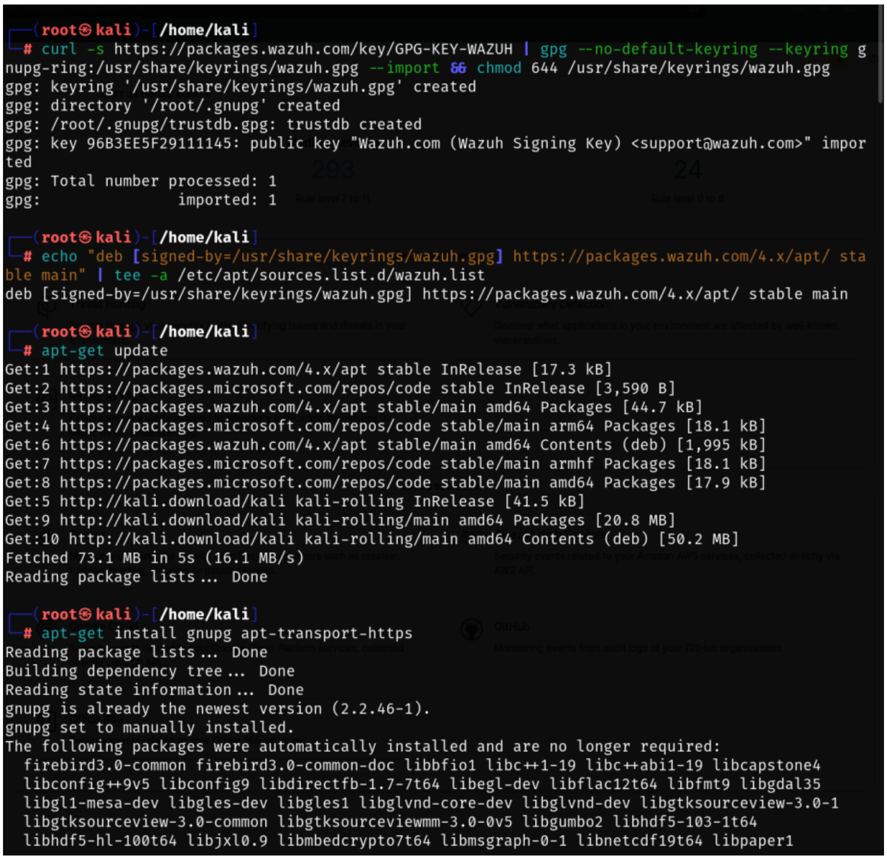


```
     wwwwwww.wwwww.      wwwwww.wwwwwww.
      wwwwwwwwwwwww.      wwwwwwwwwwwww.
      wwwwwwwwwwww.       wwwwwwwwwwwww.       oooooo
       wwwwwwwwwww.        wwwwwwwwwww.      oooooooo
       wwwwwwwwww.         wwwwwwwwwww.     oooooooooo
        wwwwwwww.           wwwwwwww.       oooooooooo
        wwwwwww.            wwwwwwww.        oooooooo
         wwwwww.             wwwwww.          oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 08:00:27:b2:f8:43 brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 192.168.1.10/24 metric 1024 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 21520sec preferred_lft 21520sec
    inet6 fe80::a00:27ff:feb2:f843/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@wazuh-server ~]#
```

Le macchine sono sulla stessa rete e comunicano tra loro.

Su kali passiamo alla configurazione dell'agent Wazuh, sempre seguendo la guida online.



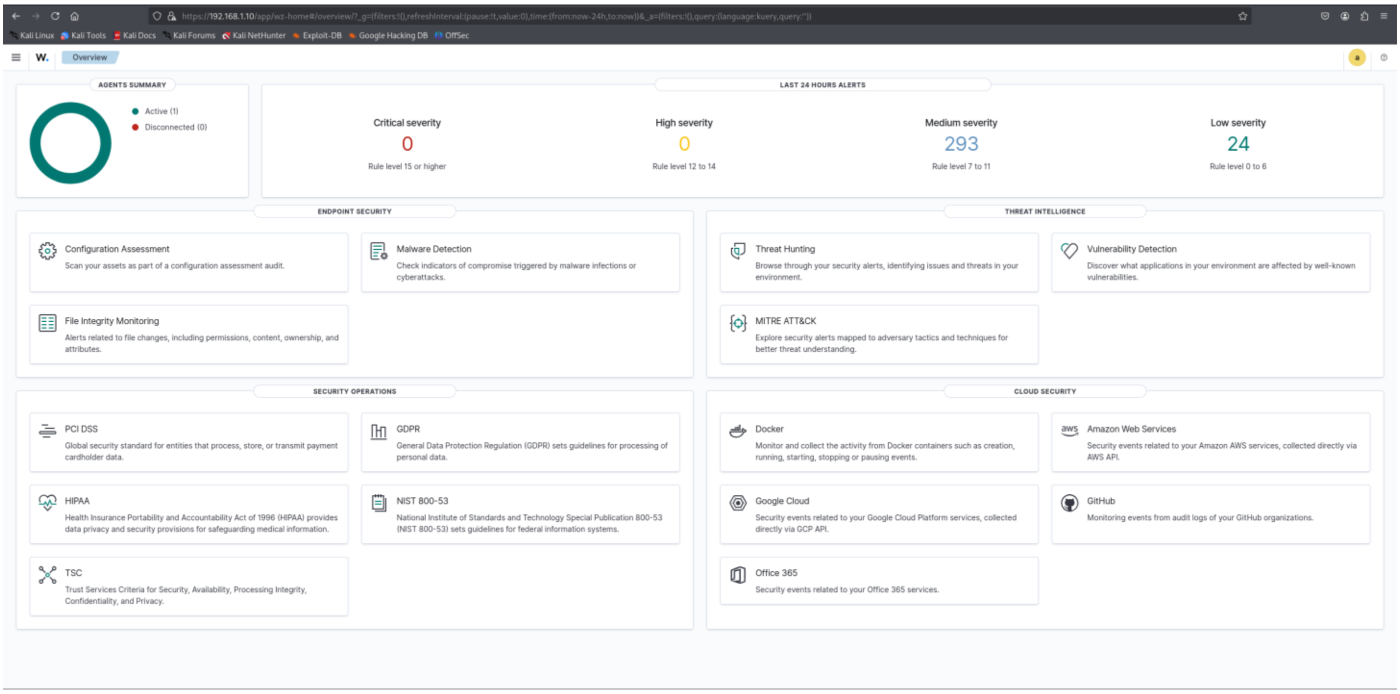
```
┌──(root㉿kali)-[/home/kali]
└─# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring g
nupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" impor
ted
gpg: Total number processed: 1
gpg:               imported: 1

┌──(root㉿kali)-[/home/kali]
└─# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ sta
ble main" | tee -a /etc/apt/sources.list.d/wazuh.list
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main

┌──(root㉿kali)-[/home/kali]
└─# apt-get update
Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:2 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:3 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [44.7 kB]
Get:4 https://packages.microsoft.com/repos/code stable/main arm64 Packages [18.1 kB]
Get:6 https://packages.wazuh.com/4.x/apt stable/main amd64 Contents (deb) [1,995 kB]
Get:7 https://packages.microsoft.com/repos/code stable/main armhf Packages [18.1 kB]
Get:8 https://packages.microsoft.com/repos/code stable/main amd64 Packages [17.9 kB]
Get:5 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 Packages [20.8 MB]
Get:10 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50.2 MB]
Fetched 73.1 MB in 5s (16.1 MB/s)
Reading package lists... Done

┌──(root㉿kali)-[/home/kali]
└─# apt-get install gnupg apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.46-1).
gnupg set to manually installed.
The following packages were automatically installed and are no longer required:
  firebird3.0-common firebird3.0-common-doc libbfio1 libc++1-19 libc++abi1-19 libcapstone4
  libconfig++9v5 libconfig9 libdirectfb-1.7-7t64 libegl-dev libflac12t64 libfmt9 libgdal35
  libgl1-mesa-dev libgles-dev libgles1 libglvnd-core-dev libglvnd-dev libgtksourceview-3.0-1
  libgtksourceview-3.0-common libgtksourceviewmm-3.0-0v5 libgumbo2 libhdf5-103-1t64
  libhdf5-hl-100t64 libjxl0.9 libmbedcrypto7t64 libmsgraph-0-1 libnetcdf19t64 libpaper1
```

Una volta configurato anche l’agent, possiamo accedere alla dashboard di Wazuh tramite browser di kali inserendo l’ip della macchina Wazuh.


https://192.168.1.10/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(language:kuery,query:''))
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
W.
Overview
a

AGENTS SUMMARY

- Active (1)
- Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	293	24
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud
Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub
Monitoring events from audit logs of your GitHub organizations.

Office 365
Security events related to your Office 365 services.