EPICODE

ESERCIZIO W20D1 EXTRA

INCIDENT RESPONSE

Mungiovì Fabio

TASK

Installare Wazuh (SIEM/XDR) in versione OVA nella rete laboratorio e il suo agent su Kali.

Collegare l'agent a Wazuh e interpretare le informazioni raccolte (appena avviato le informazioni saranno poche e Wazuh necessita di ulteriori configurazioni di cui non ci occuperemo).

Wazuh OVA (impostare correttamente la rete in modo che Wazuh e Kali siano nella stessa rete):
https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/enrollment-methods/via-agent-configuration/linux-endpoint.html

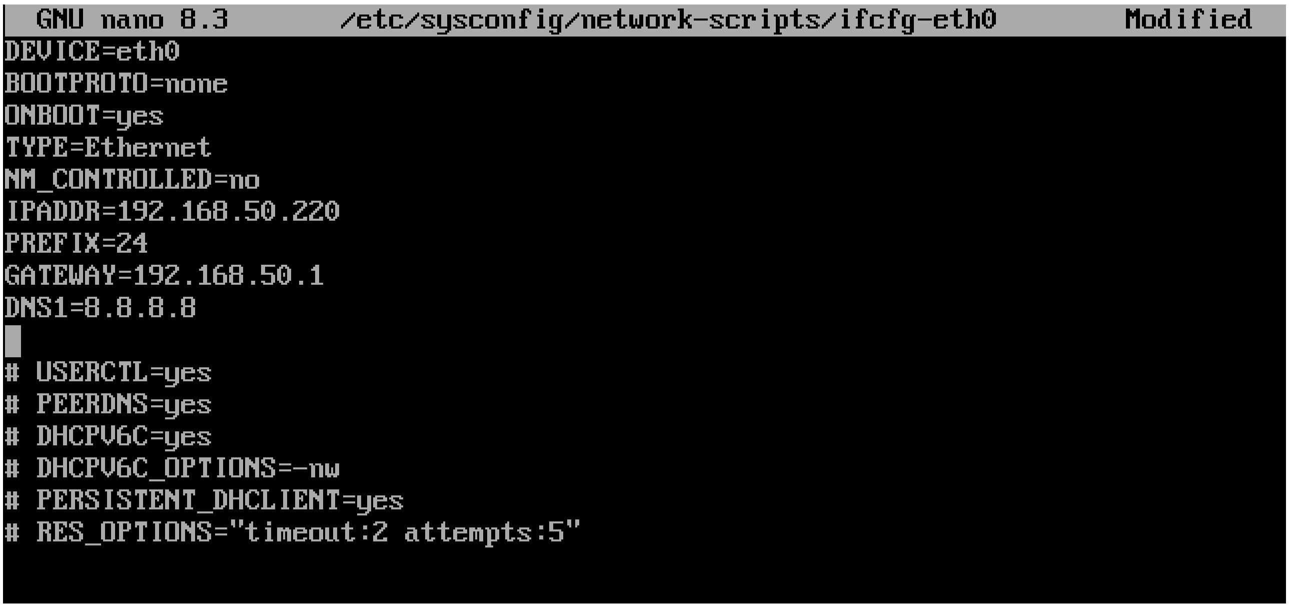
Wazuh Agent (seguire APT e Systemd):
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html

Enrollment dell'agent suggerito:
https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/enrollment-methods/via-agent-configuration/linux-endpoint.html

ESECUZIONE

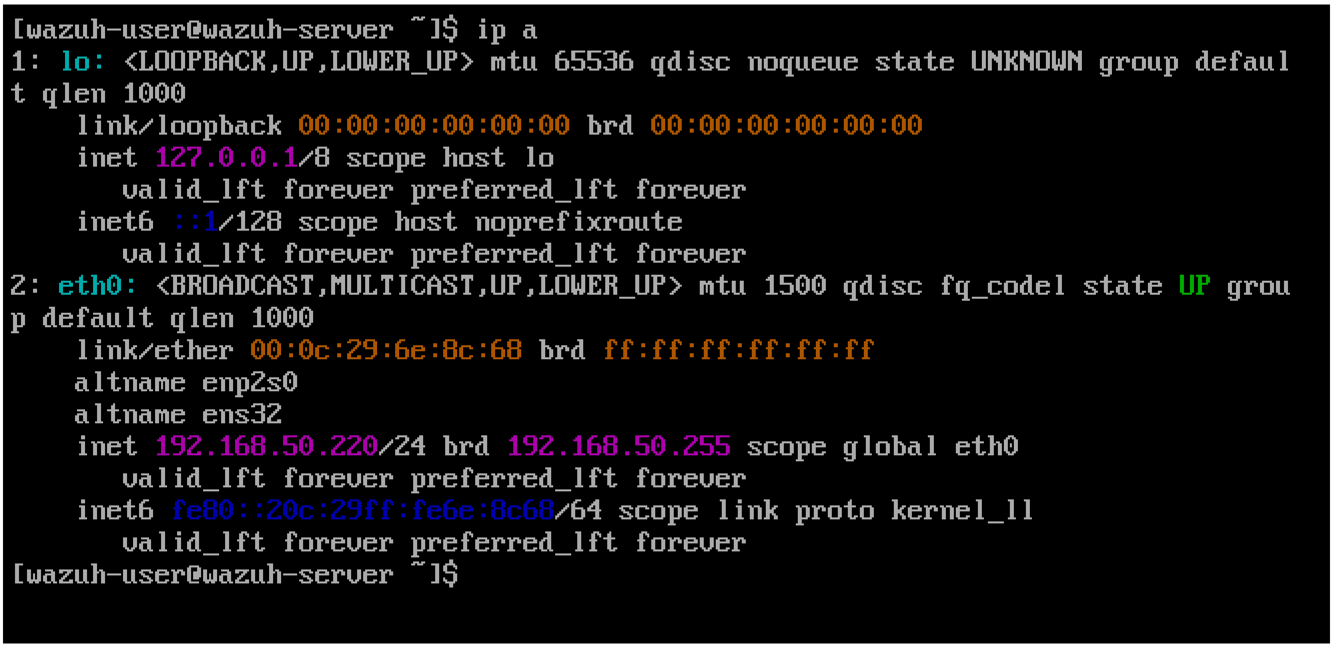
Configurazione

Una volta installato l'OVA di Wazuh sulla Virtual Machine, avviamola e configuriamo il servizio di rete statico (modificando il file al percorso: `/etc/sysconfig/network-scripts/ifcfg-eth0`) con le impostazioni presenti in figura



```
  GNU nano 8.3        /etc/sysconfig/network-scripts/ifcfg-eth0        Modified
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
NM_CONTROLLED=no
IPADDR=192.168.50.220
PREFIX=24
GATEWAY=192.168.50.1
DNS1=8.8.8.8

# USERCTL=yes
# PEERDNS=yes
# DHCPV6C=yes
# DHCPV6C_OPTIONS=-nw
# PERSISTENT_DHCLIENT=yes
# RES_OPTIONS="timeout:2 attempts:5"
```

Utilizziamo il comando `ip a` per visualizzare la corretta impostazione dell' IP

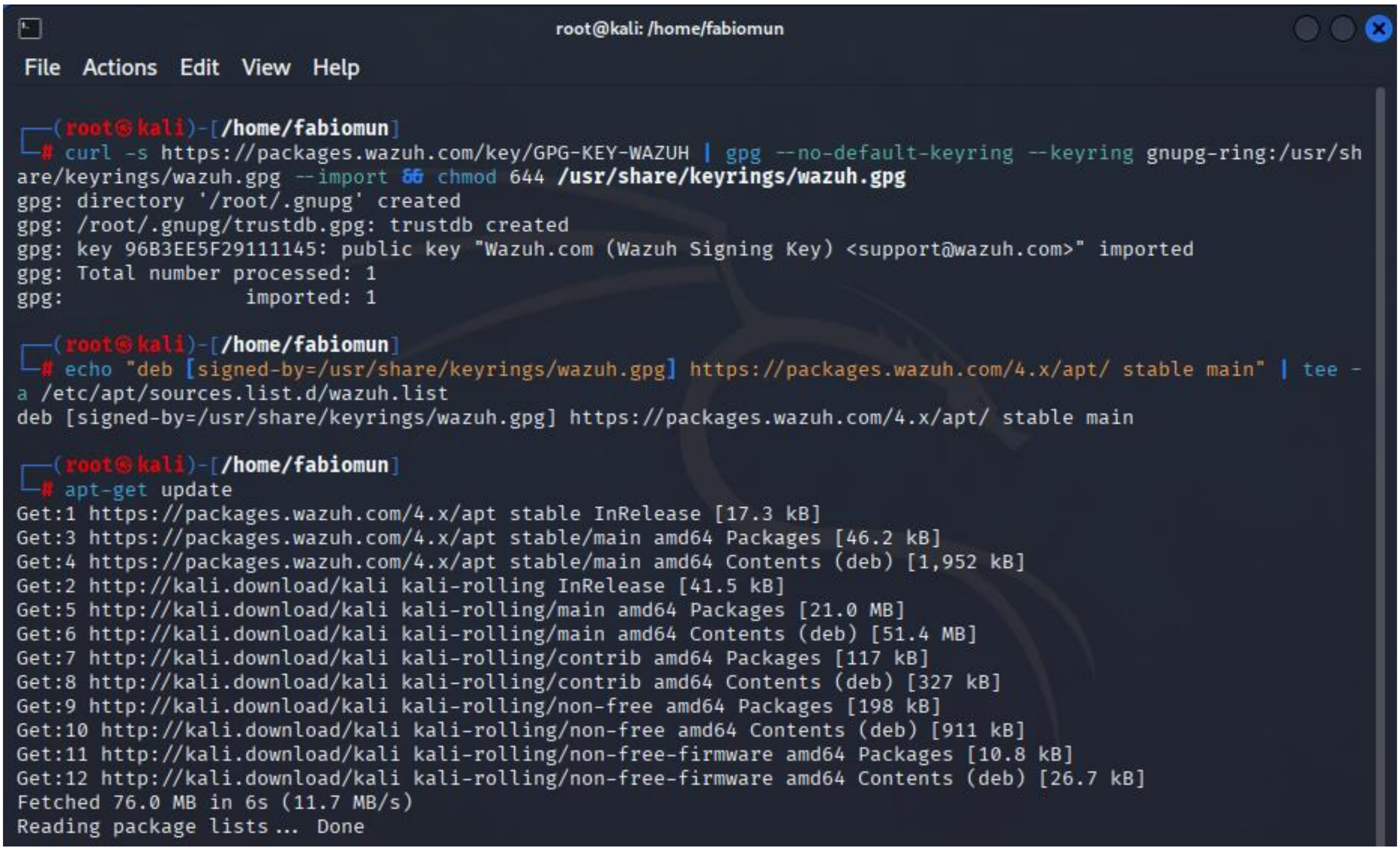


```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       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 00:0c:29:6e:8c:68 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname ens32
    inet 192.168.50.220/24 brd 192.168.50.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:8c68/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

Wazuh Agent

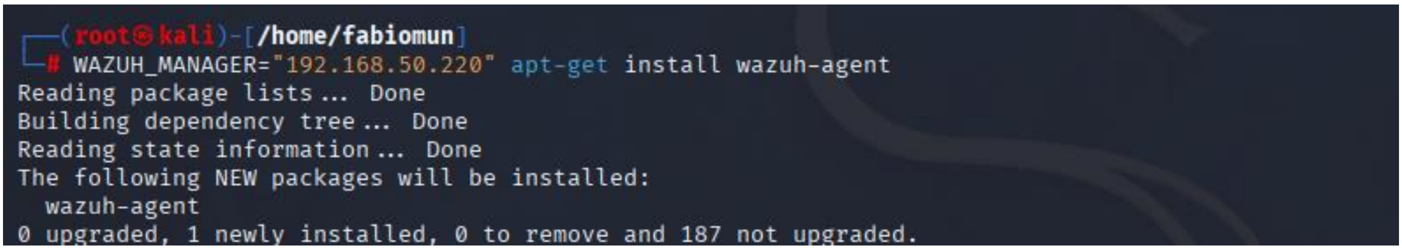
Spostiamoci ora sulla macchina Kali.
Seguendo le istruzioni della guida all'installazione procediamo con:

- Installazione della GPG key
- Aggiunta repository
- Update dei pacchetti



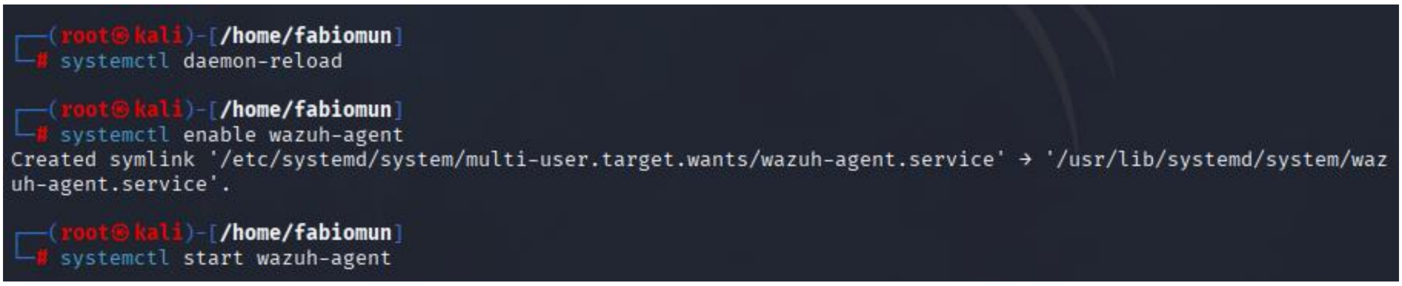
```
┌──(root㉿kali)-[/home/fabiomun]
└─# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/sh
are/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb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

┌──(root㉿kali)-[/home/fabiomun]
└─# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable 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/fabiomun]
└─# apt-get update
Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:3 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [46.2 kB]
Get:4 https://packages.wazuh.com/4.x/apt stable/main amd64 Contents (deb) [1,952 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [117 kB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Packages [198 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:11 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:12 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [26.7 kB]
Fetched 76.0 MB in 6s (11.7 MB/s)
Reading package lists... Done
```

Ora settiamo l'IP del server Wazuh modificando la variabile WAZUH_MANAGER



```
┌──(root㉿kali)-[/home/fabiomun]
└─# WAZUH_MANAGER="192.168.50.220" apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 187 not upgraded.
```

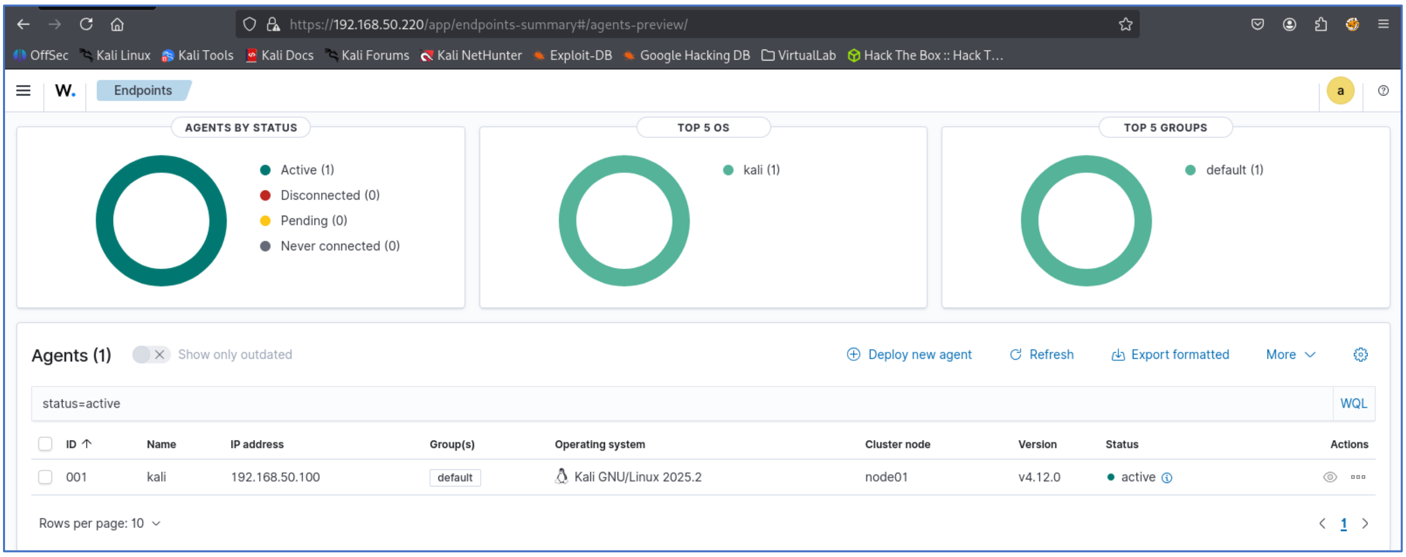
Infine abilitiamo il servizio con i seguenti comandi



```
┌──(root㉿kali)-[/home/fabiomun]
└─# systemctl daemon-reload

┌──(root㉿kali)-[/home/fabiomun]
└─# systemctl enable wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/waz
uh-agent.service'.

┌──(root㉿kali)-[/home/fabiomun]
└─# systemctl start wazuh-agent
```

Wazuh Web UI

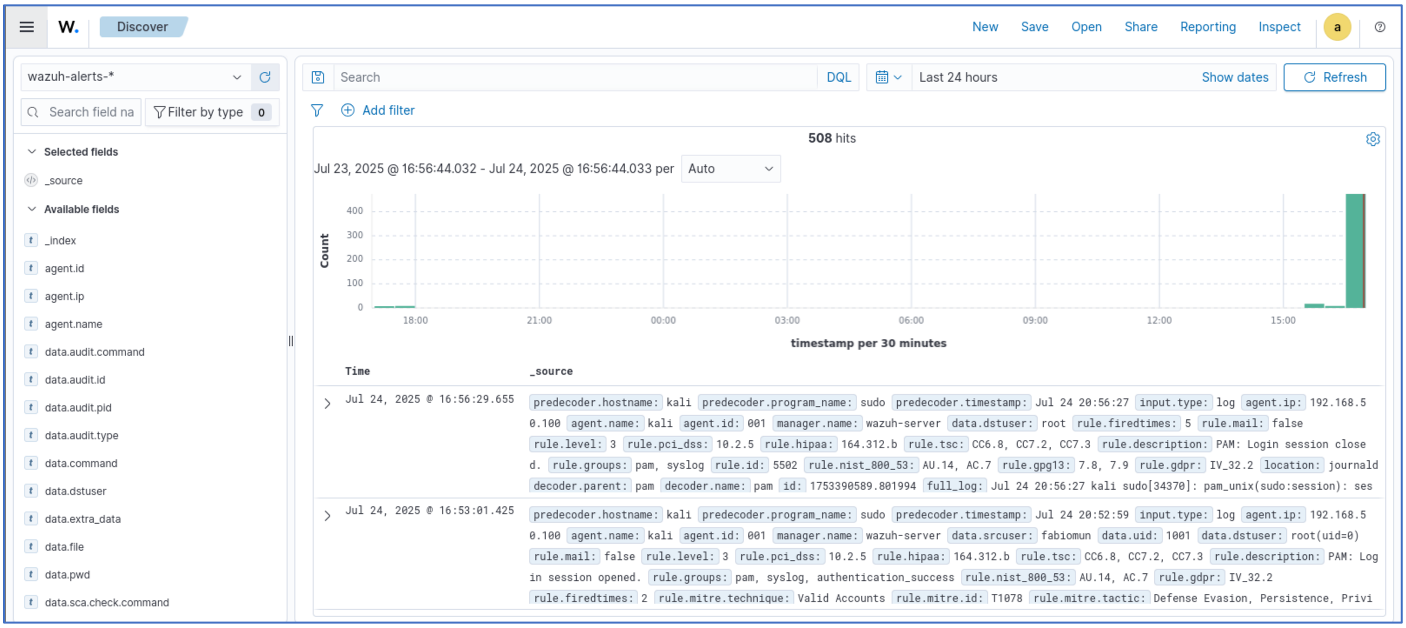
Da browser, colleghiamoci alla Web UI di Wazuh, attraverso il suo indirizzo IP.
La macchina Kali sarà ora riconosciuta come Endpoint.



status=active

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali	192.168.50.100	default	Kali GNU/Linux 2025.2	node01	v4.12.0	● active	

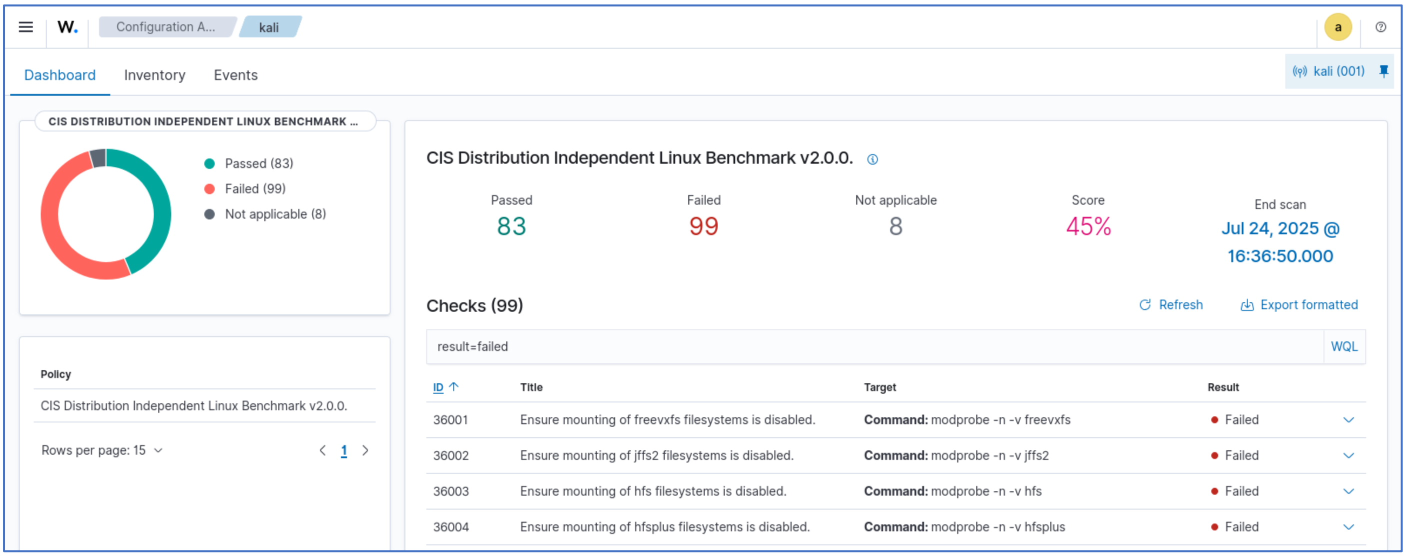
La sezione **Explore / Discover** permette di vedere i log in ingresso al SIEM



```
Time                          _source
Jul 24, 2025 @ 16:56:29.655   predecoder.hostname: kali predecoder.program_name: sudo predecoder.timestamp: Jul 24 20:56:27 input.type: log agent.ip: 192.168.5
                              0.100 agent.name: kali agent.id: 001 manager.name: wazuh-server data.dstuser: root rule.firedtimes: 5 rule.mail: false
                              rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session close
                              d. rule.groups: pam, syslog rule.id: 5502 rule.nist_800_53: AU.14, AC.7 rule.gpg13: 7.8, 7.9 rule.gdpr: IV_32.2 location: journald
                              decoder.parent: pam decoder.name: pam id: 1753390589.801994 full_log: Jul 24 20:56:27 kali sudo[34370]: pam_unix(sudo:session): ses
Jul 24, 2025 @ 16:53:01.425   predecoder.hostname: kali predecoder.program_name: sudo predecoder.timestamp: Jul 24 20:52:59 input.type: log agent.ip: 192.168.5
                              0.100 agent.name: kali agent.id: 001 manager.name: wazuh-server data.srcuser: fabiomun data.uid: 1001 data.dstuser: root(uid=0)
                              rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Log
                              in session opened. rule.groups: pam, syslog, authentication_success rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_32.2
                              rule.firedtimes: 2 rule.mitre.technique: Valid Accounts rule.mitre.id: T1078 rule.mitre.tactic: Defense Evasion, Persistence, Privi
```

Endpoint security / Configuration Assessment / Dashboard

In questa sezione vediamo un riepilogo delle configurazioni su tutti gli endpoint (in questo caso è attivo solo Kali).



Policy
CIS Distribution Independent Linux Benchmark v2.0.0.

CIS Distribution Independent Linux Benchmark v2.0.0.

Passed	Failed	Not applicable	Score	End scan
83	99	8	45%	Jul 24, 2025 @ 16:36:50.000

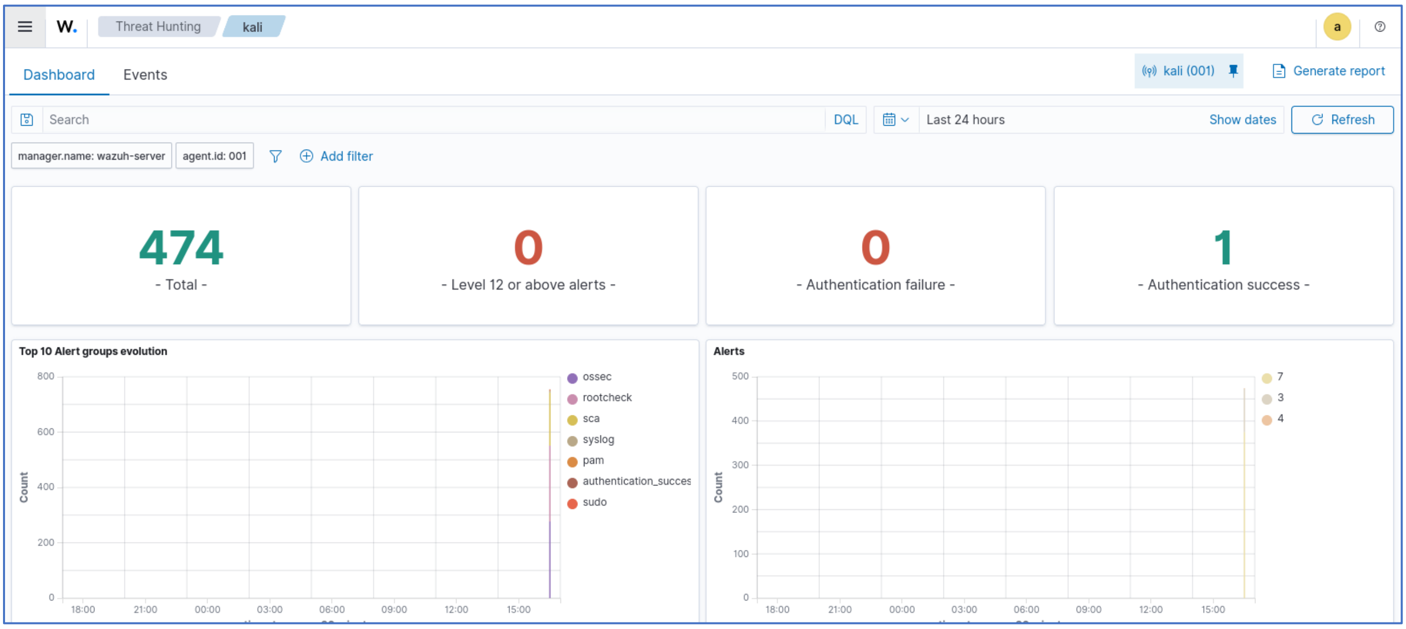
Checks (99)

result=failed

ID	Title	Target	Result
36001	Ensure mounting of freevxfs filesystems is disabled.	**Command:** modprobe -n -v freevxfs	● Failed
36002	Ensure mounting of jffs2 filesystems is disabled.	**Command:** modprobe -n -v jffs2	● Failed
36003	Ensure mounting of hfs filesystems is disabled.	**Command:** modprobe -n -v hfs	● Failed
36004	Ensure mounting of hfsplus filesystems is disabled.	**Command:** modprobe -n -v hfsplus	● Failed

Threat intelligence / Threat Hunting

Sezione dedicata al Threat hunting mettendo insieme le informazioni provenienti da tutti gli endpoint.



474	0	0	1
- Total -	- Level 12 or above alerts -	- Authentication failure -	- Authentication success -