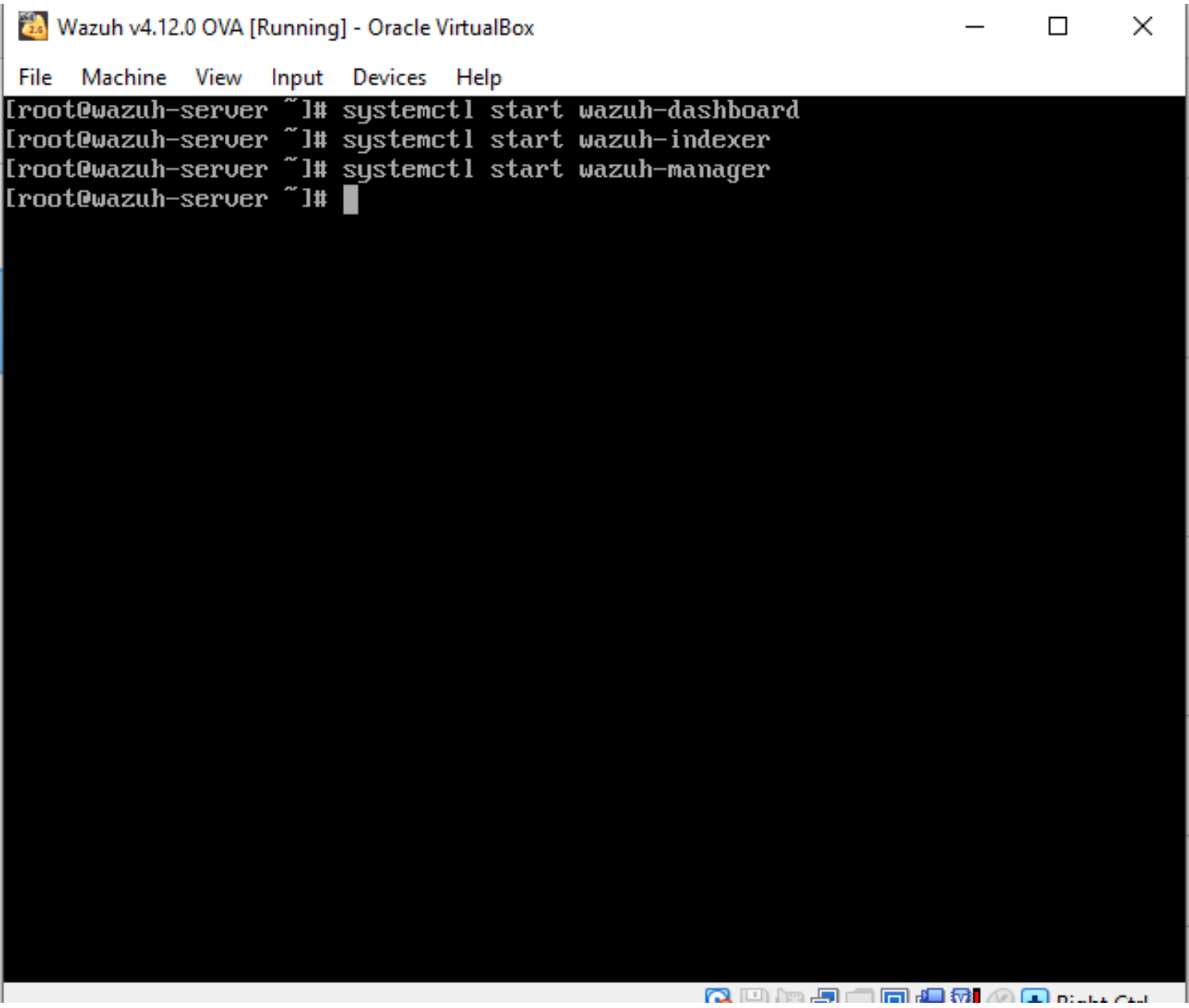
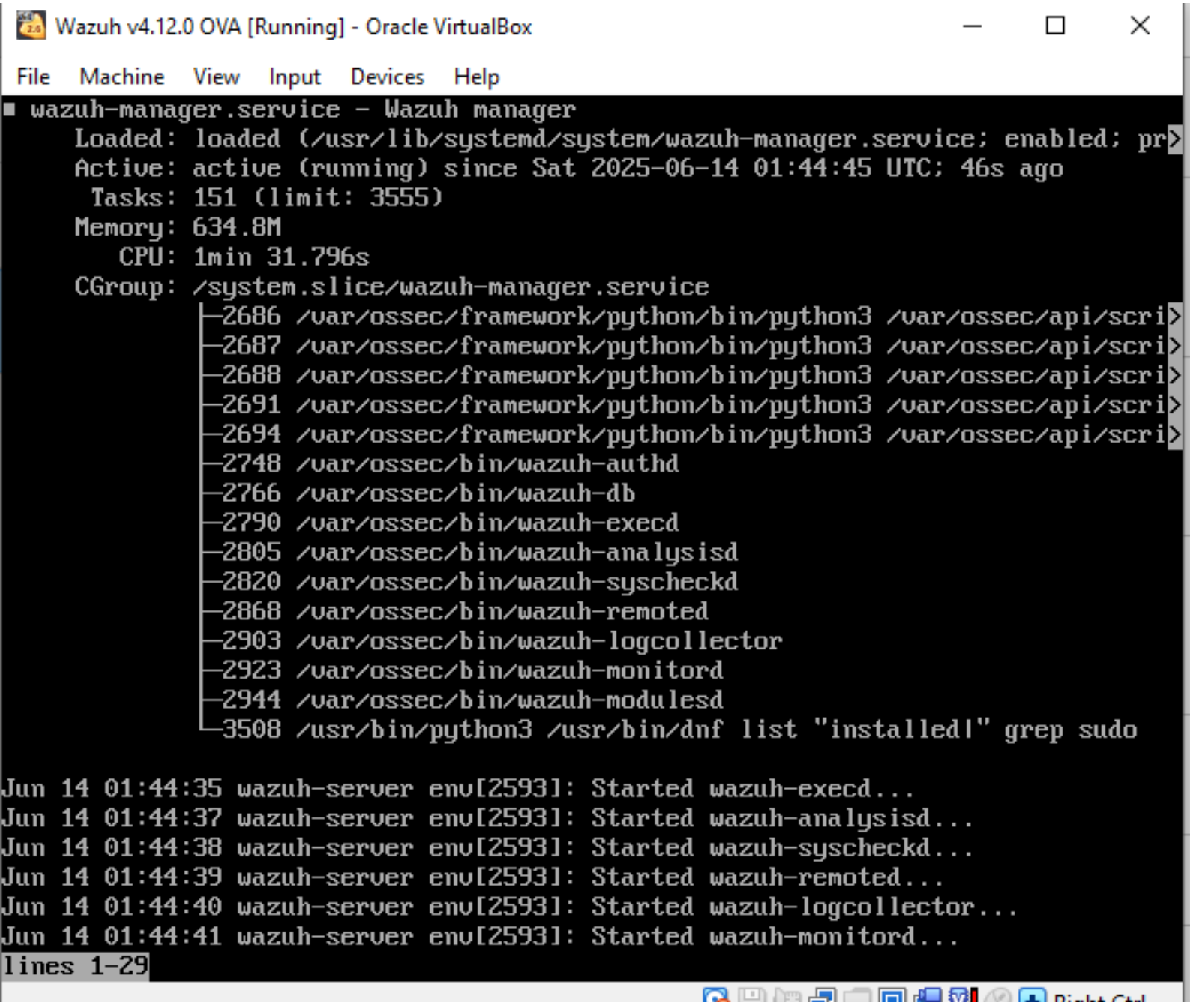
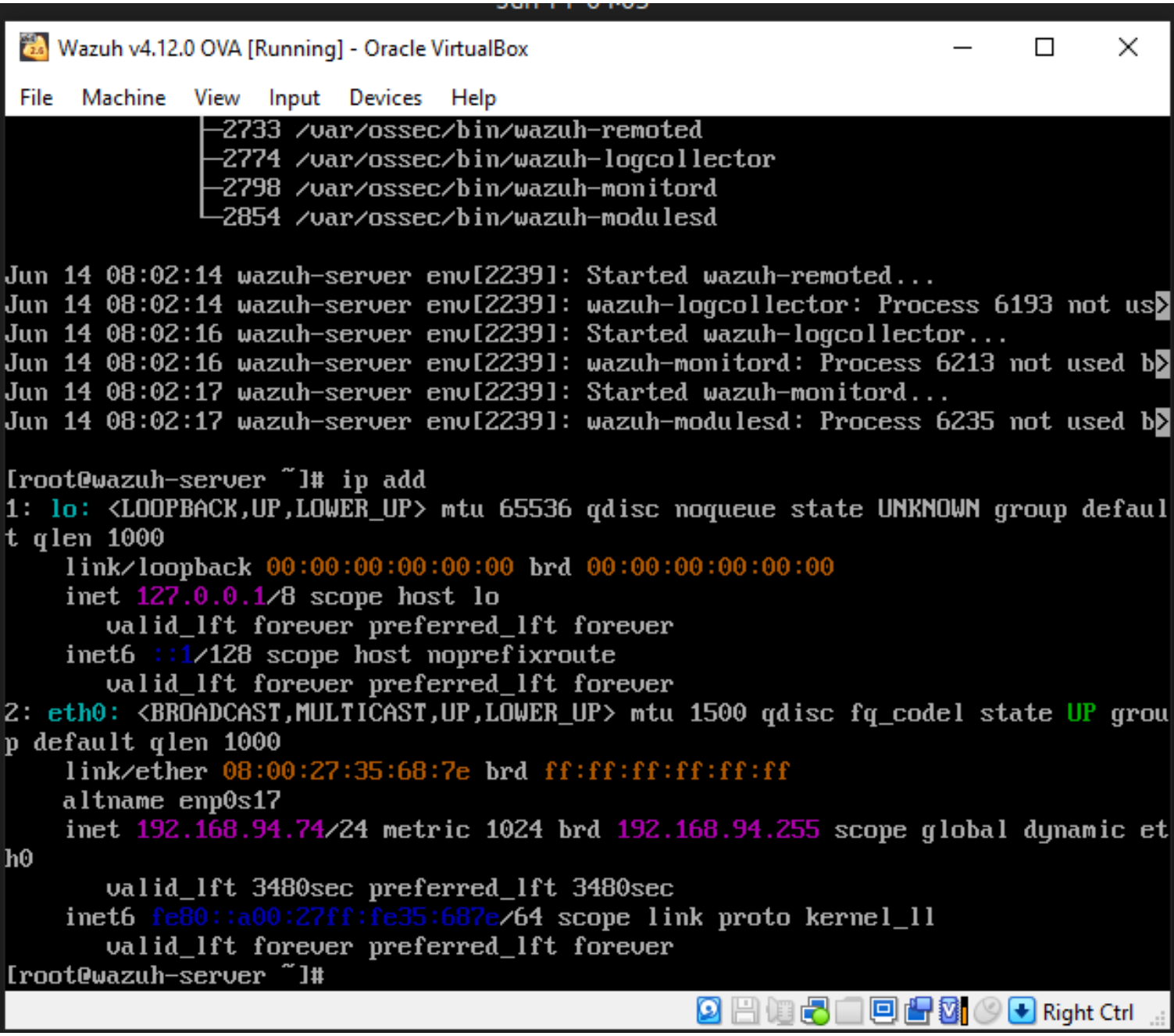
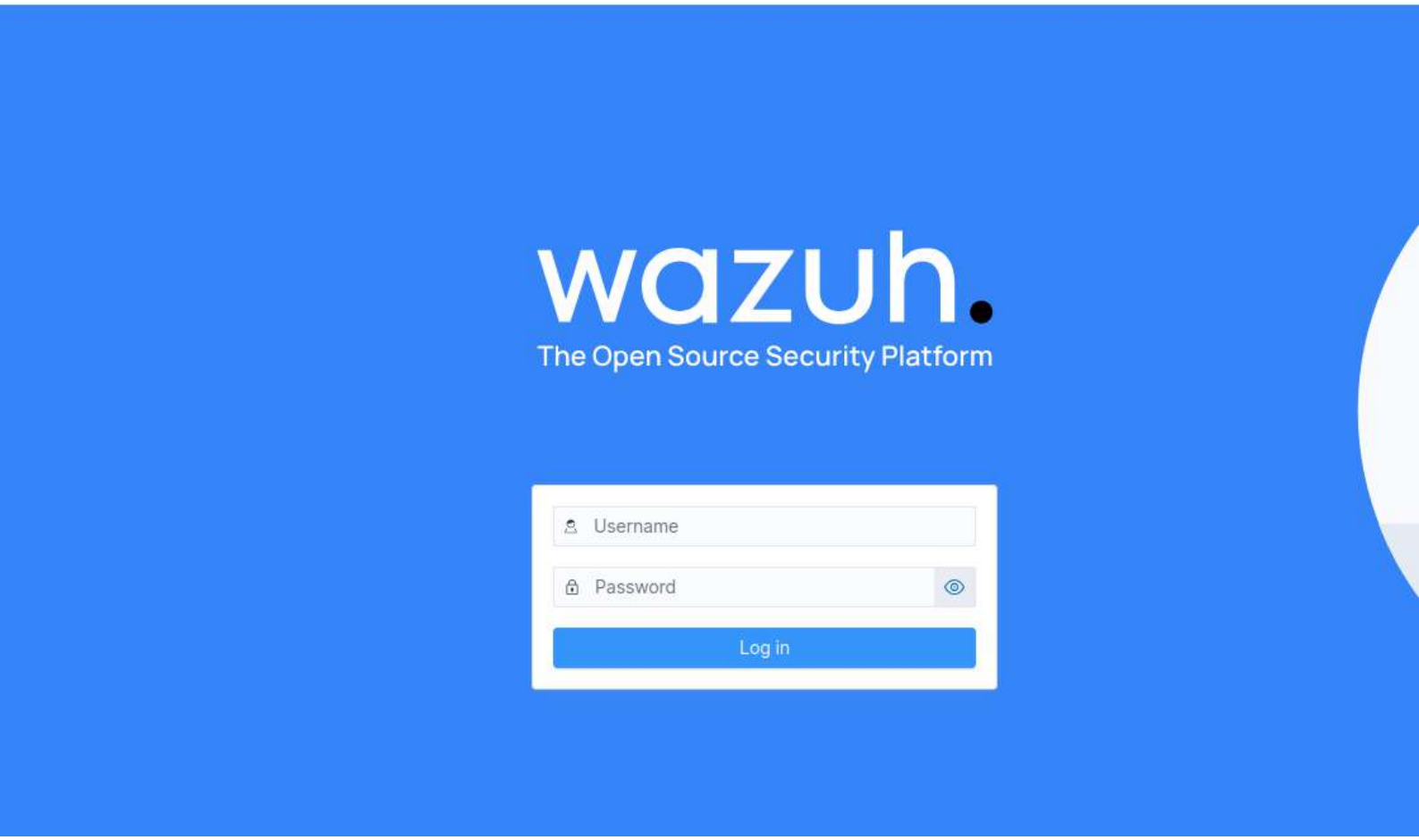
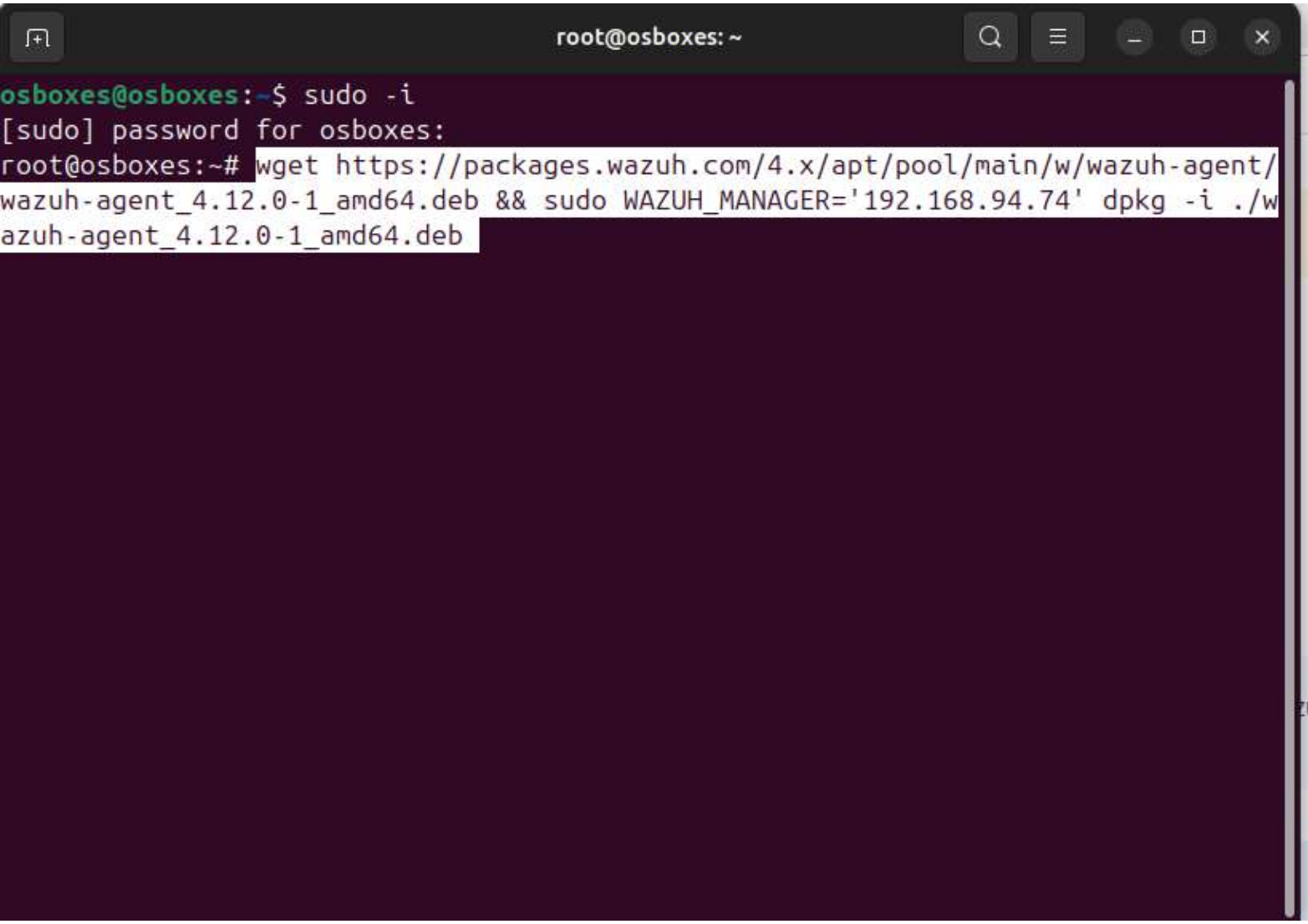
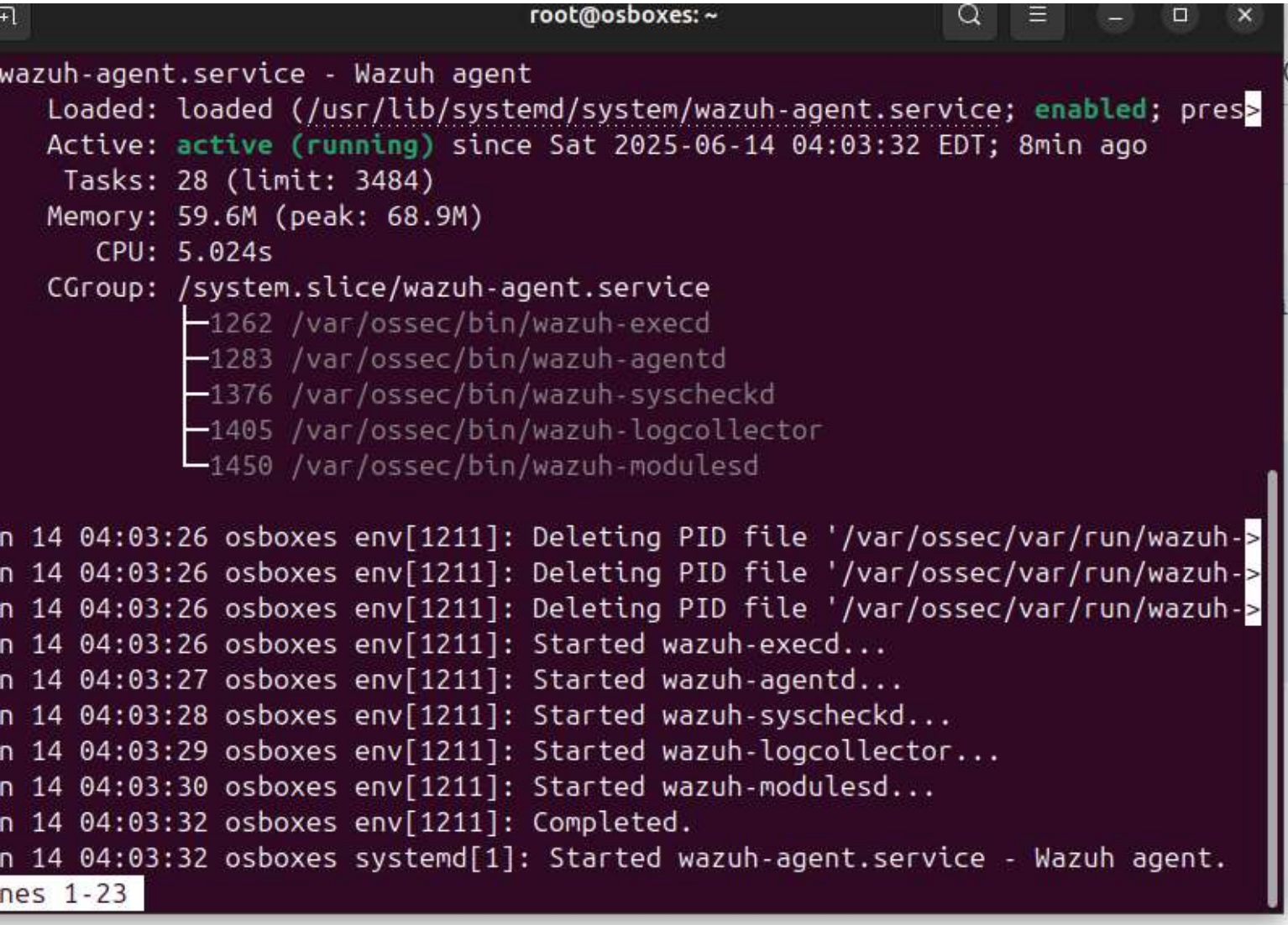

Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[root@wazuh-server ~]# systemctl start wazuh-dashboard
[root@wazuh-server ~]# systemctl start wazuh-indexer
[root@wazuh-server ~]# systemctl start wazuh-manager
[root@wazuh-server ~]#


Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
● wazuh-manager.service - Wazuh manager
Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; pr
Active: active (running) since Sat 2025-06-14 01:44:45 UTC; 46s ago
Tasks: 151 (limit: 3555)
Memory: 634.8M
CPU: 1min 31.796s
CGroup: /system.slice/wazuh-manager.service
├─2686 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri
├─2687 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri
├─2688 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri
├─2691 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri
├─2694 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri
├─2748 /var/ossec/bin/wazuh-authd
├─2766 /var/ossec/bin/wazuh-db
├─2790 /var/ossec/bin/wazuh-execd
├─2805 /var/ossec/bin/wazuh-analysisd
├─2820 /var/ossec/bin/wazuh-syscheckd
├─2868 /var/ossec/bin/wazuh-remoted
├─2903 /var/ossec/bin/wazuh-logcollector
├─2923 /var/ossec/bin/wazuh-monitord
├─2944 /var/ossec/bin/wazuh-modulesd
└─3508 /usr/bin/python3 /usr/bin/dnf list "installed|" grep sudo
Jun 14 01:44:35 wazuh-server env[2593]: Started wazuh-execd...
Jun 14 01:44:37 wazuh-server env[2593]: Started wazuh-analysisd...
Jun 14 01:44:38 wazuh-server env[2593]: Started wazuh-syscheckd...
Jun 14 01:44:39 wazuh-server env[2593]: Started wazuh-remoted...
Jun 14 01:44:40 wazuh-server env[2593]: Started wazuh-logcollector...
Jun 14 01:44:41 wazuh-server env[2593]: Started wazuh-monitord...
lines 1-29


Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
├─2733 /var/ossec/bin/wazuh-remoted
├─2774 /var/ossec/bin/wazuh-logcollector
├─2798 /var/ossec/bin/wazuh-monitord
└─2854 /var/ossec/bin/wazuh-modulesd
Jun 14 08:02:14 wazuh-server env[2239]: Started wazuh-remoted...
Jun 14 08:02:14 wazuh-server env[2239]: wazuh-logcollector: Process 6193 not us>
Jun 14 08:02:16 wazuh-server env[2239]: Started wazuh-logcollector...
Jun 14 08:02:16 wazuh-server env[2239]: wazuh-monitord: Process 6213 not used b>
Jun 14 08:02:17 wazuh-server env[2239]: Started wazuh-monitord...
Jun 14 08:02:17 wazuh-server env[2239]: wazuh-modulesd: Process 6235 not used b>
[root@wazuh-server ~]# ip add
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 08:00:27:35:68:7e brd ff:ff:ff:ff:ff:ff
altname enp0s17
inet 192.168.94.74/24 metric 1024 brd 192.168.94.255 scope global dynamic et
h0
valid_lft 3480sec preferred_lft 3480sec
inet6 fe80::a00:27ff:fe35:687e/64 scope link proto kernel_ll
valid_lft forever preferred_lft forever
[root@wazuh-server ~]#
Right Ctrl


wazuh.
The Open Source Security Platform
Username
Password
Log in


root@osboxes: ~
osboxes@osboxes:~$ sudo -i
[sudo] password for osboxes:
root@osboxes:~# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.94.74' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb


root@osboxes: ~
wazuh-agent.service - Wazuh agent
Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; pres>
Active: active (running) since Sat 2025-06-14 04:03:32 EDT; 8min ago
Tasks: 28 (limit: 3484)
Memory: 59.6M (peak: 68.9M)
CPU: 5.024s
CGroup: /system.slice/wazuh-agent.service
├─1262 /var/ossec/bin/wazuh-execd
├─1283 /var/ossec/bin/wazuh-agentd
├─1376 /var/ossec/bin/wazuh-syscheckd
├─1405 /var/ossec/bin/wazuh-logcollector
└─1450 /var/ossec/bin/wazuh-modulesd
n 14 04:03:26 osboxes env[1211]: Deleting PID file '/var/ossec/var/run/wazuh->
n 14 04:03:26 osboxes env[1211]: Deleting PID file '/var/ossec/var/run/wazuh->
n 14 04:03:26 osboxes env[1211]: Deleting PID file '/var/ossec/var/run/wazuh->
n 14 04:03:26 osboxes env[1211]: Started wazuh-execd...
n 14 04:03:27 osboxes env[1211]: Started wazuh-agentd...
n 14 04:03:28 osboxes env[1211]: Started wazuh-syscheckd...
n 14 04:03:29 osboxes env[1211]: Started wazuh-logcollector...
n 14 04:03:30 osboxes env[1211]: Started wazuh-modulesd...
n 14 04:03:32 osboxes env[1211]: Completed.
n 14 04:03:32 osboxes systemd[1]: Started wazuh-agent.service - Wazuh agent.
nes 1-23

Pending (0)

Never connected (0)

TOP 5 GROUPS

default (1)

Agents (1)

Show only outdated

Deploy new agent | Refresh | Export formatted | More

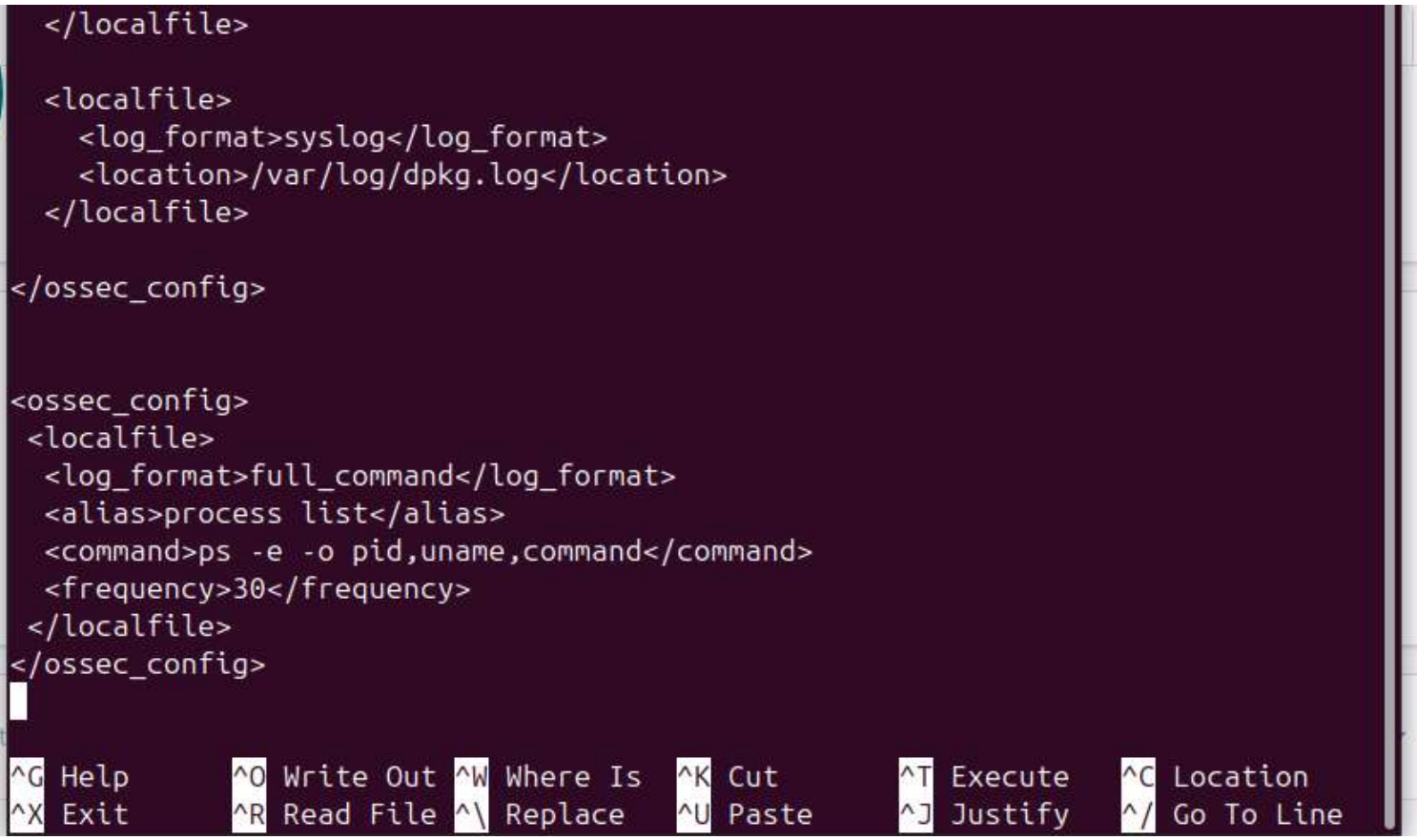
Search

WQL

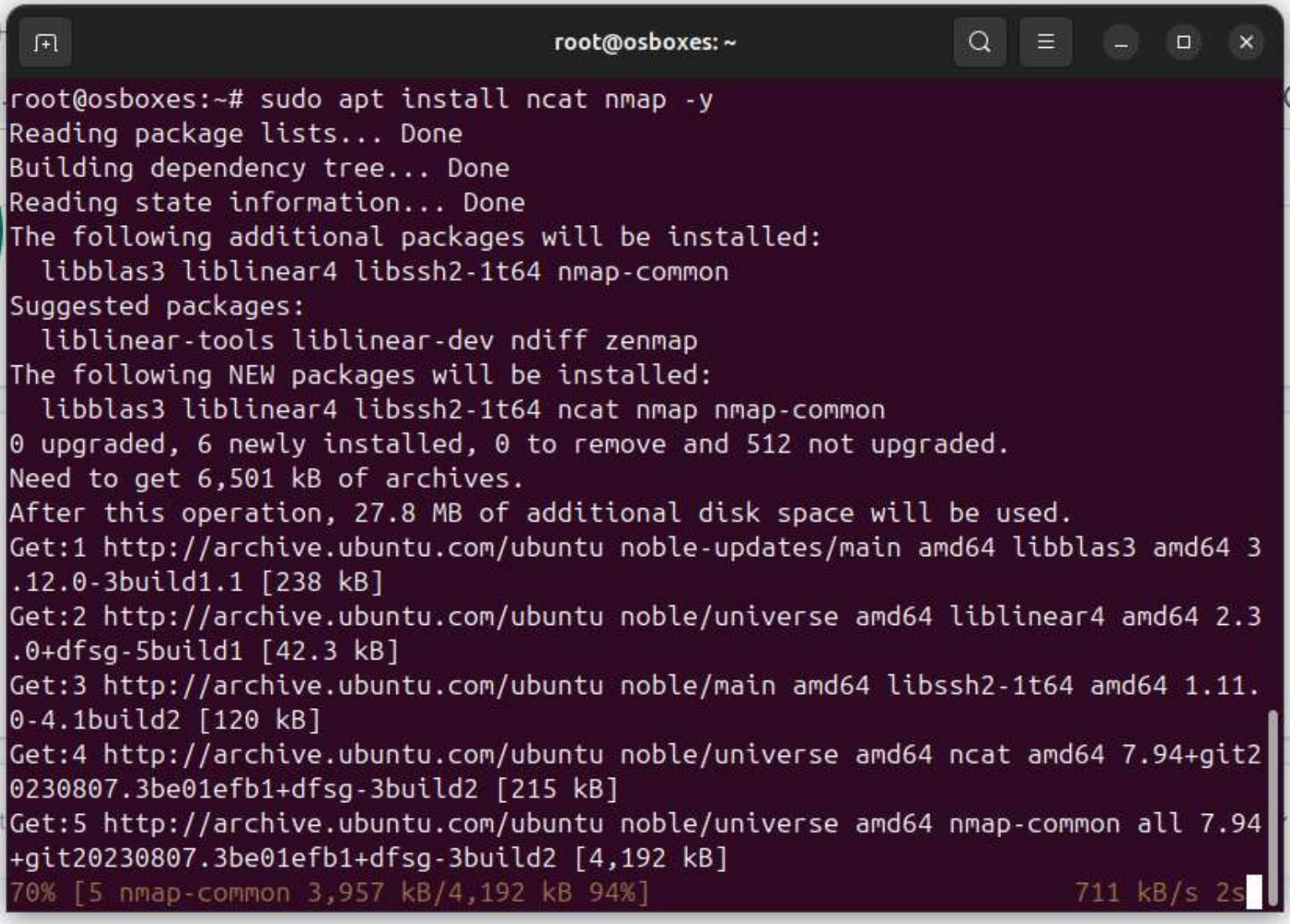
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	osboxes	192.168.94.59	default	Ubuntu 24.04 LTS	node01	v4.12.0	active	

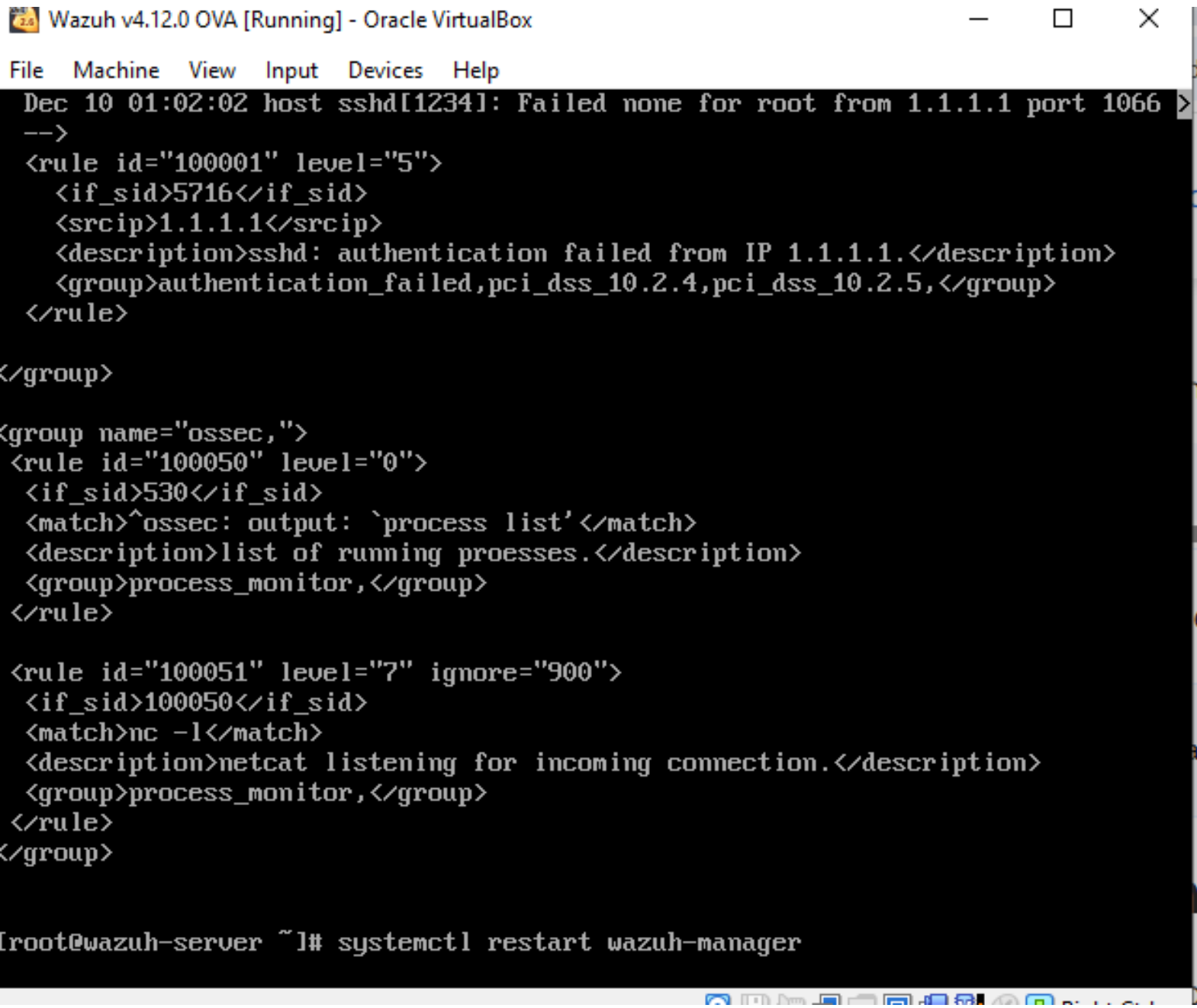
Rows per page: 10

1


  </localfile>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>
</ossec_config>
<ossec_config>
 <localfile>
  <log_format>full_command</log_format>
  <alias>process list</alias>
  <command>ps -e -o pid,uname,command</command>
  <frequency>30</frequency>
 </localfile>
</ossec_config>
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

```
wazuh-agent_4.12.0-1_amd64.deb~
Command '~wget' not found, did you mean:
  command 'wget' from deb wget (1.21.4-1ubuntu4.1)
  command 'owget' from deb ow-shell (3.2p4+dfsg1-4.2)
  command 'pwget' from deb pwget (2016.1019+git75c6e3e-8)
Try: apt install <deb name>
root@osboxes:~# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/
wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.94.74' dpkg -i ./w
azuh-agent_4.12.0-1_amd64.deb
--2025-06-14 04:17:30--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-ag
ent/wazuh-agent_4.12.0-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 108.139.200.42, 2600:9000:2
846:a600:8:fed3:b0c0:93a1
Connecting to packages.wazuh.com (packages.wazuh.com)|108.139.200.42|:443... con
nected.
^C
root@osboxes:~# sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
root@osboxes:~# nano /var/ossec/etc/ossec.conf
root@osboxes:~# nano /var/ossec/etc/ossec.conf
root@osboxes:~# nano /var/ossec/etc/ossec.conf
root@osboxes:~# sudo systemctl restart wazuh-agent
root@osboxes:~#
```


root@osboxes: ~
root@osboxes:~# sudo apt install ncat nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libblas3 liblinear4 libssh2-1t64 nmap-common
Suggested packages:
liblinear-tools liblinear-dev ndiff zenmap
The following NEW packages will be installed:
libblas3 liblinear4 libssh2-1t64 ncat nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 512 not upgraded.
Need to get 6,501 kB of archives.
After this operation, 27.8 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3
.12.0-3build1.1 [238 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3
.0+dfsg-5build1 [42.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.
0-4.1build2 [120 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 ncat amd64 7.94+git2
0230807.3be01efb1+dfsg-3build2 [215 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94
+git20230807.3be01efb1+dfsg-3build2 [4,192 kB]
70% [5 nmap-common 3,957 kB/4,192 kB 94%] 711 kB/s 2s


Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066
-->
<rule id="100001" level="5">
<if_sid>5716</if_sid>
<srcip>1.1.1.1</srcip>
<description>sshd: authentication failed from IP 1.1.1.1.</description>
<group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
</group>
<group name="ossec,">
<rule id="100050" level="0">
<if_sid>530</if_sid>
<match>^ossec: output: `process list'</match>
<description>list of running proesses.</description>
<group>process_monitor,</group>
</rule>
<rule id="100051" level="7" ignore="900">
<if_sid>100050</if_sid>
<match>nc -l</match>
<description>netcat listening for incoming connection.</description>
<group>process_monitor,</group>
</rule>
</group>
[root@wazuh-server ~]# systemctl restart wazuh-manager