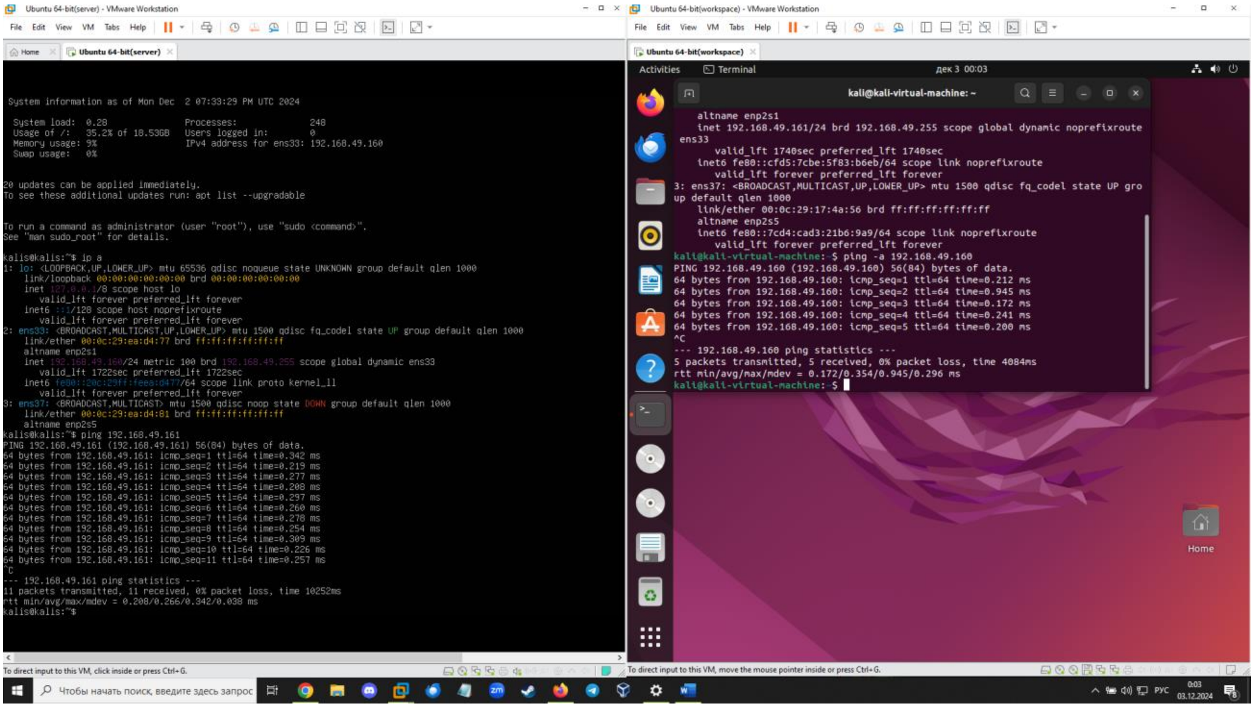
ПРЗ 5 Threat Hunting

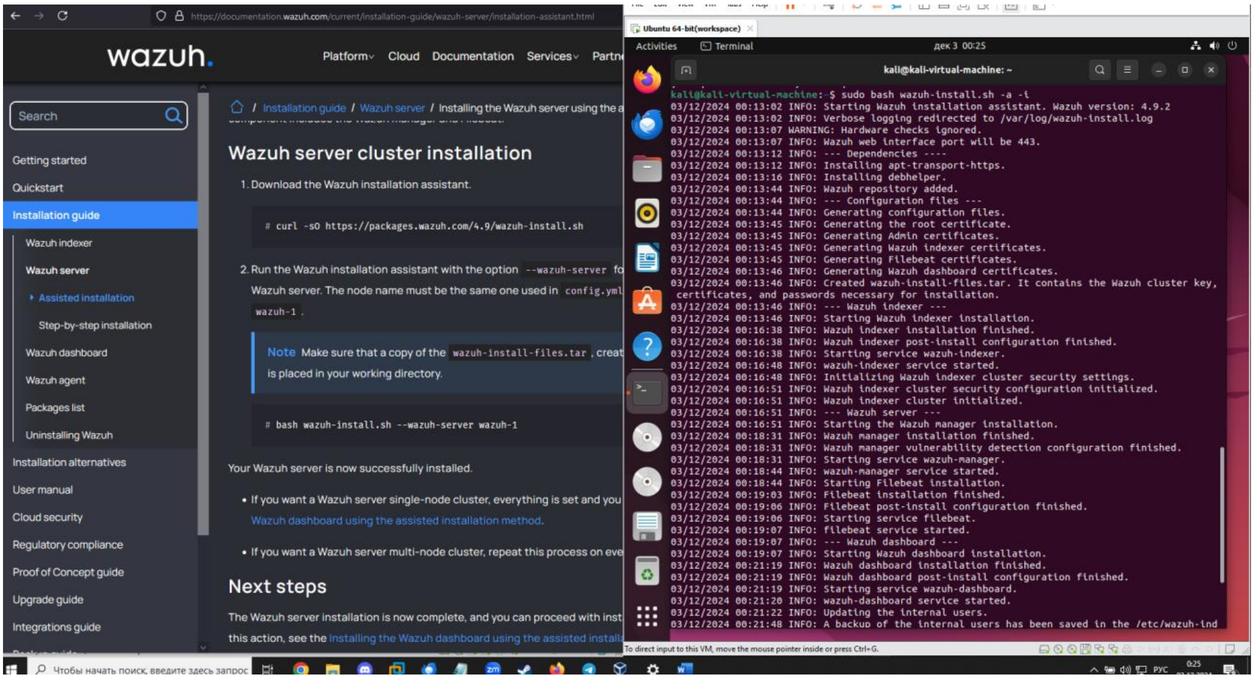
1) Разверните виртуальные машины (минимум 2 – сервер и агенты)
2) Обеспечить между ними сетевой обмен.


Ubuntu 64-bit(server) - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 64-bit(server)
To direct input to this VM, click inside or press Ctrl+G.
Чтобы начать поиск, введите здесь запрос
Ubuntu 64-bit(workspace) - VMware Workstation
Ubuntu 64-bit(workspace)
Activities
Terminal
дек 3 00:03
kali@kali-virtual-machine: ~
Home
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
РУС
0:03
03.12.2024

```
 System information as of Mon Dec  2 07:33:29 PM UTC 2024

  System load:  0.28               Processes:             248
  Usage of /:   35.2% of 18.53GB   Users logged in:       0
  Memory usage: 9%                 IPv4 address for ens33: 192.168.49.160
  Swap usage:   0%


20 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kalis@kalis:~$ ip a
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 noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ea:d4:77 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.49.160/24 metric 100 brd 192.168.49.255 scope global dynamic ens33
       valid_lft 1722sec preferred_lft 1722sec
    inet6 fe80::20c:29ff:feea:d477/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:ea:d4:81 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
kalis@kalis:~$ ping 192.168.49.161
PING 192.168.49.161 (192.168.49.161) 56(84) bytes of data.
64 bytes from 192.168.49.161: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 192.168.49.161: icmp_seq=2 ttl=64 time=0.219 ms
64 bytes from 192.168.49.161: icmp_seq=3 ttl=64 time=0.277 ms
64 bytes from 192.168.49.161: icmp_seq=4 ttl=64 time=0.208 ms
64 bytes from 192.168.49.161: icmp_seq=5 ttl=64 time=0.297 ms
64 bytes from 192.168.49.161: icmp_seq=6 ttl=64 time=0.260 ms
64 bytes from 192.168.49.161: icmp_seq=7 ttl=64 time=0.278 ms
64 bytes from 192.168.49.161: icmp_seq=8 ttl=64 time=0.254 ms
64 bytes from 192.168.49.161: icmp_seq=9 ttl=64 time=0.309 ms
64 bytes from 192.168.49.161: icmp_seq=10 ttl=64 time=0.226 ms
64 bytes from 192.168.49.161: icmp_seq=11 ttl=64 time=0.257 ms
^C
--- 192.168.49.161 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10252ms
rtt min/avg/max/mdev = 0.208/0.266/0.342/0.038 ms
kalis@kalis:~$
```

```
    altname enp2s1
    inet 192.168.49.161/24 brd 192.168.49.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1740sec preferred_lft 1740sec
    inet6 fe80::cfd5:7cbe:5f83:b6eb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:17:4a:56 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 fe80::7cd4:cad3:21b6:9a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@kali-virtual-machine:~$ ping -a 192.168.49.160
PING 192.168.49.160 (192.168.49.160) 56(84) bytes of data.
64 bytes from 192.168.49.160: icmp_seq=1 ttl=64 time=0.212 ms
64 bytes from 192.168.49.160: icmp_seq=2 ttl=64 time=0.945 ms
64 bytes from 192.168.49.160: icmp_seq=3 ttl=64 time=0.172 ms
64 bytes from 192.168.49.160: icmp_seq=4 ttl=64 time=0.241 ms
64 bytes from 192.168.49.160: icmp_seq=5 ttl=64 time=0.200 ms
^C
--- 192.168.49.160 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.172/0.354/0.945/0.296 ms
kali@kali-virtual-machine:~$
```

3) Развернуть на одной из ВМ сервер Wazuh



/ Installation guide / Wazuh server / Installing the Wazuh server using the a

Wazuh server cluster installation

1. Download the Wazuh installation assistant.

```
# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

2. Run the Wazuh installation assistant with the option `--wazuh-server` fo
Wazuh server. The node name must be the same one used in `config.yml`
`wazuh-1` .

Note Make sure that a copy of the `wazuh-install-files.tar` , creat
is placed in your working directory.

```
# bash wazuh-install.sh --wazuh-server wazuh-1
```

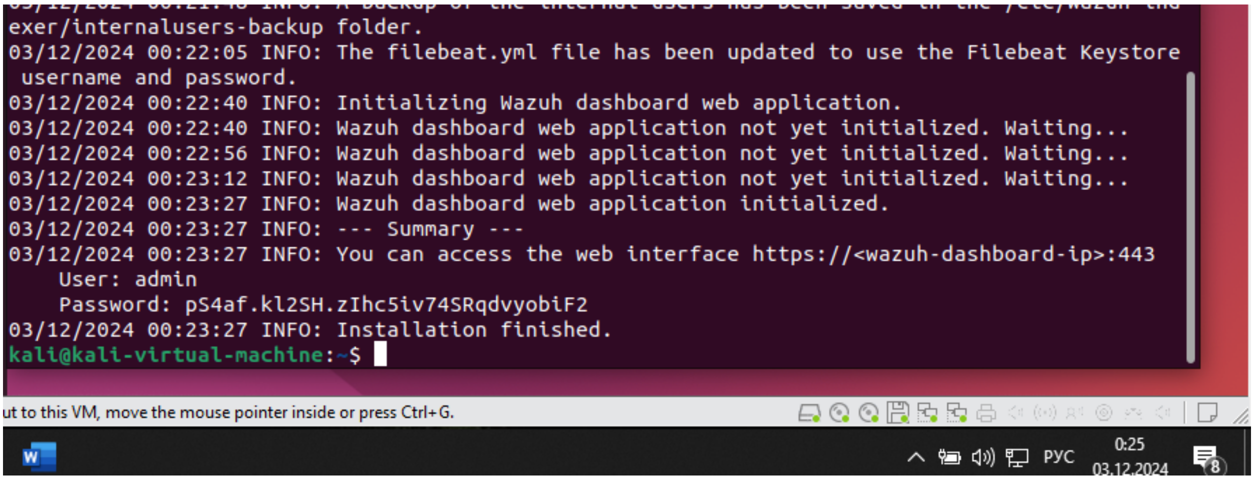
Your Wazuh server is now successfully installed.

- If you want a Wazuh server single-node cluster, everything is set and you
Wazuh dashboard using the assisted installation method.
- If you want a Wazuh server multi-node cluster, repeat this process on eve

Next steps

The Wazuh server installation is now complete, and you can proceed with inst
this action, see the Installing the Wazuh dashboard using the assisted installa

```
kali@kali-virtual-machine:~$ sudo bash wazuh-install.sh -a -i
03/12/2024 00:13:02 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
03/12/2024 00:13:02 INFO: Verbose logging redirected to /var/log/wazuh-install.log
03/12/2024 00:13:07 WARNING: Hardware checks ignored.
03/12/2024 00:13:07 INFO: Wazuh web interface port will be 443.
03/12/2024 00:13:12 INFO: --- Dependencies ----
03/12/2024 00:13:12 INFO: Installing apt-transport-https.
03/12/2024 00:13:16 INFO: Installing debhelper.
03/12/2024 00:13:44 INFO: Wazuh repository added.
03/12/2024 00:13:44 INFO: --- Configuration files ---
03/12/2024 00:13:44 INFO: Generating configuration files.
03/12/2024 00:13:45 INFO: Generating the root certificate.
03/12/2024 00:13:45 INFO: Generating Admin certificates.
03/12/2024 00:13:45 INFO: Generating Wazuh indexer certificates.
03/12/2024 00:13:45 INFO: Generating Filebeat certificates.
03/12/2024 00:13:46 INFO: Generating Wazuh dashboard certificates.
03/12/2024 00:13:46 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key,
 certificates, and passwords necessary for installation.
03/12/2024 00:13:46 INFO: --- Wazuh indexer ---
03/12/2024 00:13:46 INFO: Starting Wazuh indexer installation.
03/12/2024 00:16:38 INFO: Wazuh indexer installation finished.
03/12/2024 00:16:38 INFO: Wazuh indexer post-install configuration finished.
03/12/2024 00:16:38 INFO: Starting service wazuh-indexer.
03/12/2024 00:16:48 INFO: wazuh-indexer service started.
03/12/2024 00:16:48 INFO: Initializing Wazuh indexer cluster security settings.
03/12/2024 00:16:51 INFO: Wazuh indexer cluster security configuration initialized.
03/12/2024 00:16:51 INFO: Wazuh indexer cluster initialized.
03/12/2024 00:16:51 INFO: --- Wazuh server ---
03/12/2024 00:16:51 INFO: Starting the Wazuh manager installation.
03/12/2024 00:18:31 INFO: Wazuh manager installation finished.
03/12/2024 00:18:31 INFO: Wazuh manager vulnerability detection configuration finished.
03/12/2024 00:18:31 INFO: Starting service wazuh-manager.
03/12/2024 00:18:44 INFO: wazuh-manager service started.
03/12/2024 00:18:44 INFO: Starting Filebeat installation.
03/12/2024 00:19:03 INFO: Filebeat installation finished.
03/12/2024 00:19:06 INFO: Filebeat post-install configuration finished.
03/12/2024 00:19:06 INFO: Starting service filebeat.
03/12/2024 00:19:07 INFO: filebeat service started.
03/12/2024 00:19:07 INFO: --- Wazuh dashboard ---
03/12/2024 00:19:07 INFO: Starting Wazuh dashboard installation.
03/12/2024 00:21:19 INFO: Wazuh dashboard installation finished.
03/12/2024 00:21:19 INFO: Wazuh dashboard post-install configuration finished.
03/12/2024 00:21:19 INFO: Starting service wazuh-dashboard.
03/12/2024 00:21:20 INFO: wazuh-dashboard service started.
03/12/2024 00:21:22 INFO: Updating the internal users.
03/12/2024 00:21:48 INFO: A backup of the internal users has been saved in the /etc/wazuh-ind
```



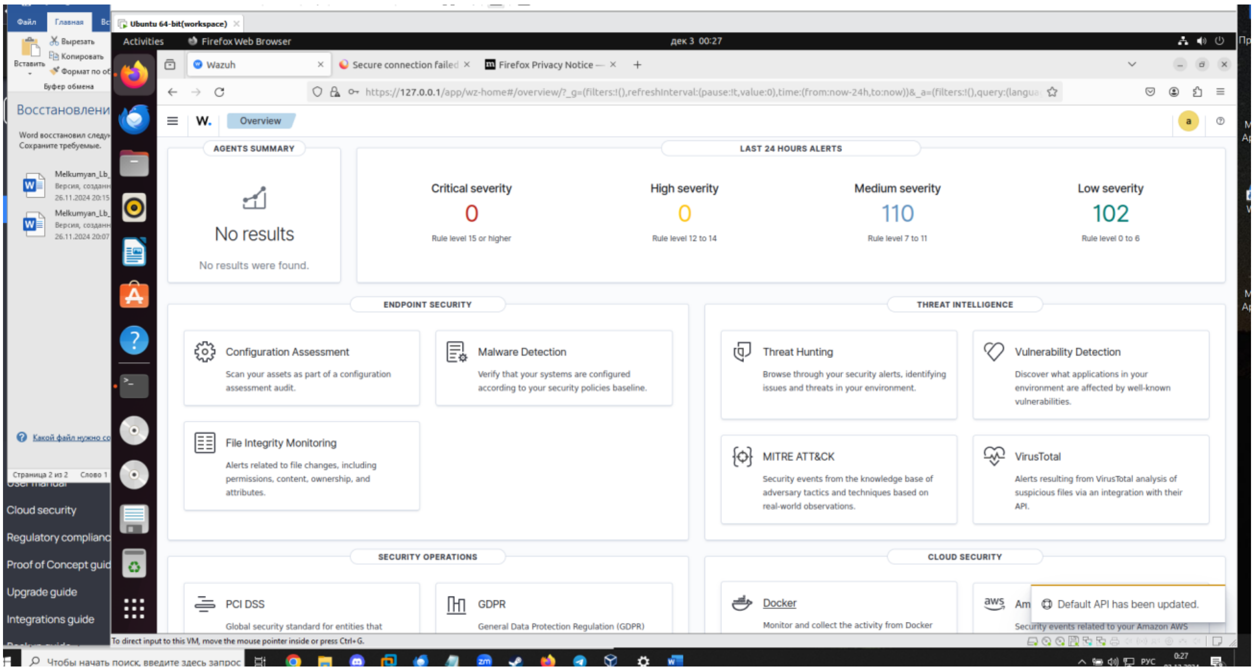
```
exer/internalusers-backup folder.
03/12/2024 00:22:05 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore
 username and password.
03/12/2024 00:22:40 INFO: Initializing Wazuh dashboard web application.
03/12/2024 00:22:40 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:22:56 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:23:12 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:23:27 INFO: Wazuh dashboard web application initialized.
03/12/2024 00:23:27 INFO: --- Summary ---
03/12/2024 00:23:27 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2
03/12/2024 00:23:27 INFO: Installation finished.
kali@kali-virtual-machine:~$
```

ut to this VM, move the mouse pointer inside or press Ctrl+G.
РУС
0:25
03.12.2024

User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Зашли на сам Wazuh



Ubuntu 64-bit(workspace)

Activities — Firefox Web Browser — дек 3 00:27

Wazuh | Secure connection failed | Firefox Privacy Notice —

https://127.0.0.1/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(langua

W. Overview

AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity 0 Rule level 15 or higher

High severity 0 Rule level 12 to 14

Medium severity 110 Rule level 7 to 11

Low severity 102 Rule level 0 to 6

ENDPOINT SECURITY

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

Malware Detection — Verify that your systems are configured according to your security policies baseline.

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 — Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal — Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

SECURITY OPERATIONS

PCI DSS — Global security standard for entities that

GDPR — General Data Protection Regulation (GDPR)

CLOUD SECURITY

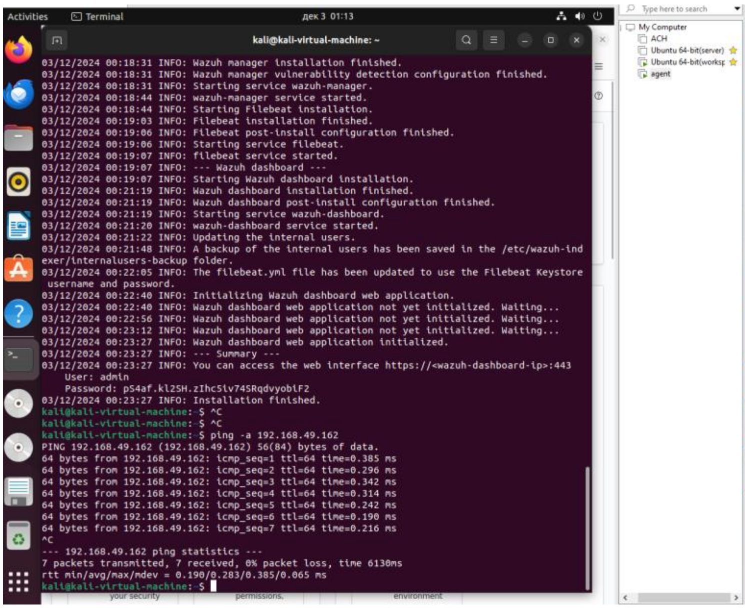
Docker — Monitor and collect the activity from Docker

Am — Security events related to your Amazon AWS

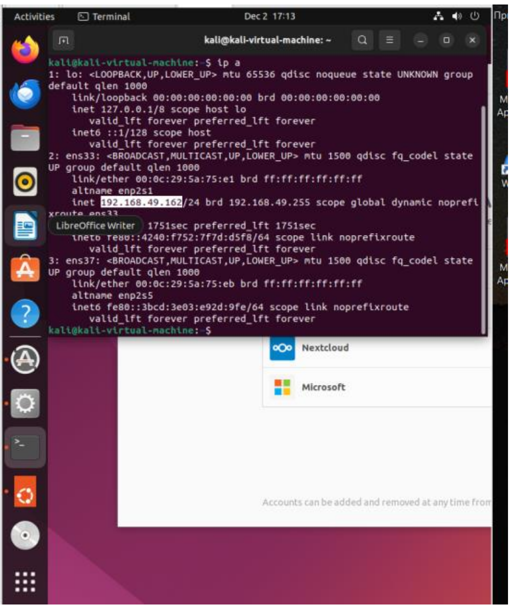
Default API has been updated.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Еще раз проверил сетевую связанность между машинами потому что будучи сонным установил не туда,и пришлось еще одну машину разворачивать



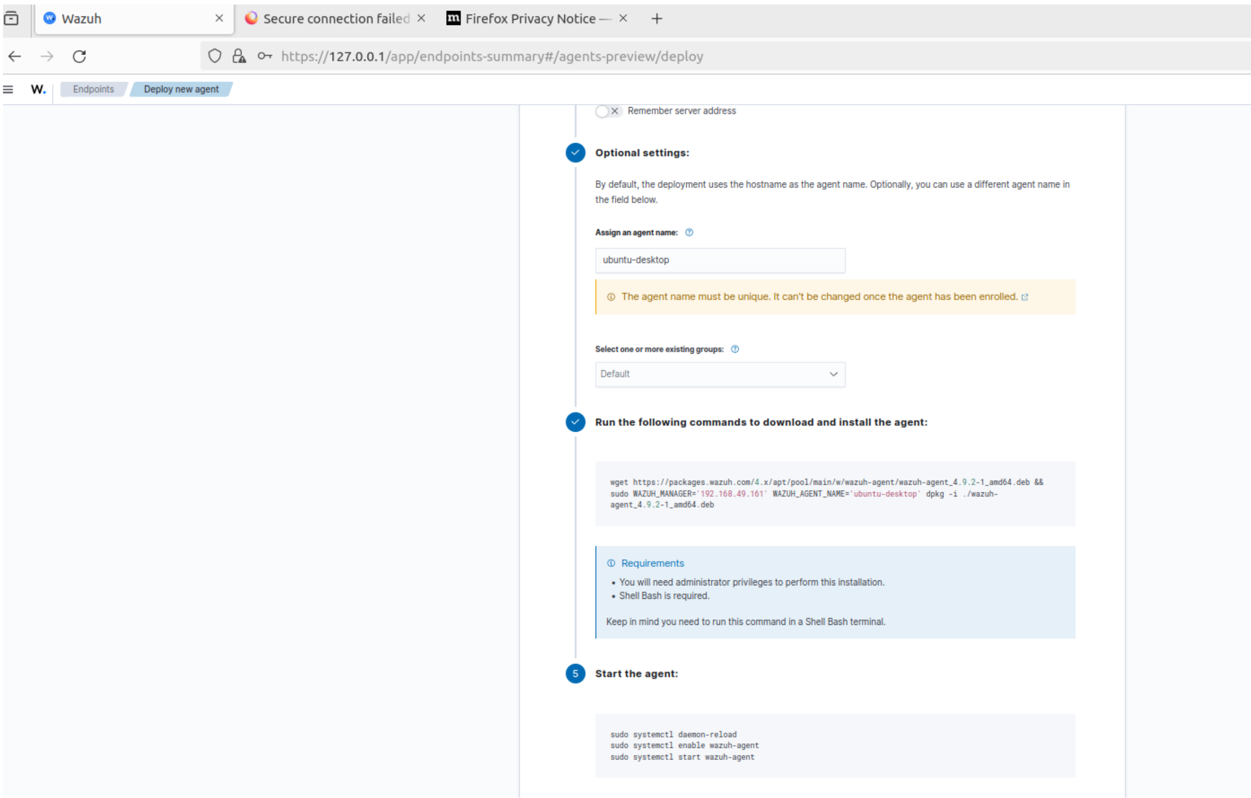
```
03/12/2024 00:18:31 INFO: Wazuh manager installation finished.
03/12/2024 00:18:31 INFO: Wazuh manager vulnerability detection configuration finished.
03/12/2024 00:18:31 INFO: Starting service wazuh-manager.
03/12/2024 00:18:44 INFO: wazuh-manager service started.
03/12/2024 00:18:44 INFO: Starting Filebeat installation.
03/12/2024 00:19:03 INFO: Filebeat installation finished.
03/12/2024 00:19:06 INFO: Filebeat post-install configuration finished.
03/12/2024 00:19:06 INFO: Starting service filebeat.
03/12/2024 00:19:07 INFO: filebeat service started.
03/12/2024 00:19:07 INFO: --- Wazuh dashboard ---
03/12/2024 00:19:07 INFO: Starting Wazuh dashboard installation.
03/12/2024 00:21:19 INFO: Wazuh dashboard installation finished.
03/12/2024 00:21:19 INFO: Wazuh dashboard post-install configuration finished.
03/12/2024 00:21:19 INFO: Starting service wazuh-dashboard.
03/12/2024 00:21:20 INFO: wazuh-dashboard service started.
03/12/2024 00:21:22 INFO: Updating the internal users.
03/12/2024 00:21:48 INFO: A backup of the internal users has been saved in the /etc/wazuh-ind
exer/internalusers-backup folder.
03/12/2024 00:22:05 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore
 username and password.
03/12/2024 00:22:40 INFO: Initializing Wazuh dashboard web application.
03/12/2024 00:22:40 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:22:56 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:23:12 INFO: Wazuh dashboard web application not yet initialized. Waiting...
03/12/2024 00:23:27 INFO: Wazuh dashboard web application initialized.
03/12/2024 00:23:27 INFO: --- Summary ---
03/12/2024 00:23:27 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2
03/12/2024 00:23:27 INFO: Installation finished.
kali@kali-virtual-machine:~$ ^C
kali@kali-virtual-machine:~$ ^C
kali@kali-virtual-machine:~$ ping -a 192.168.49.162
PING 192.168.49.162 (192.168.49.162) 56(84) bytes of data.
64 bytes from 192.168.49.162: icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from 192.168.49.162: icmp_seq=2 ttl=64 time=0.296 ms
64 bytes from 192.168.49.162: icmp_seq=3 ttl=64 time=0.342 ms
64 bytes from 192.168.49.162: icmp_seq=4 ttl=64 time=0.314 ms
64 bytes from 192.168.49.162: icmp_seq=5 ttl=64 time=0.242 ms
64 bytes from 192.168.49.162: icmp_seq=6 ttl=64 time=0.190 ms
64 bytes from 192.168.49.162: icmp_seq=7 ttl=64 time=0.216 ms
^C
--- 192.168.49.162 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6130ms
rtt min/avg/max/mdev = 0.190/0.283/0.385/0.065 ms
kali@kali-virtual-machine:~$
```


Activities
Terminal
Dec 2 17:13
kali@kali-virtual-machine: ~
LibreOffice Writer
Nextcloud
Microsoft
Accounts can be added and removed at any time from

```
kali@kali-virtual-machine:~$ ip a
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 00:0c:29:5a:75:e1 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.49.162/24 brd 192.168.49.255 scope global dynamic noprefi
xroute ens33
               1751sec preferred_lft 1751sec
    inet6 fe80::4240:f752:7f7d:d5f8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 00:0c:29:5a:75:eb brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet6 fe80::3bcd:3e03:e92d:9fe/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@kali-virtual-machine:~$
```

4) Подключите агента используя документацию

Устанавливаю агента через Wazuh



○ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ubuntu-desktop

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: Default

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.49.161' WAZUH_AGENT_NAME='ubuntu-desktop' dpkg -i ./wazuh-
agent_4.9.2-1_amd64.deb
```

Requirements

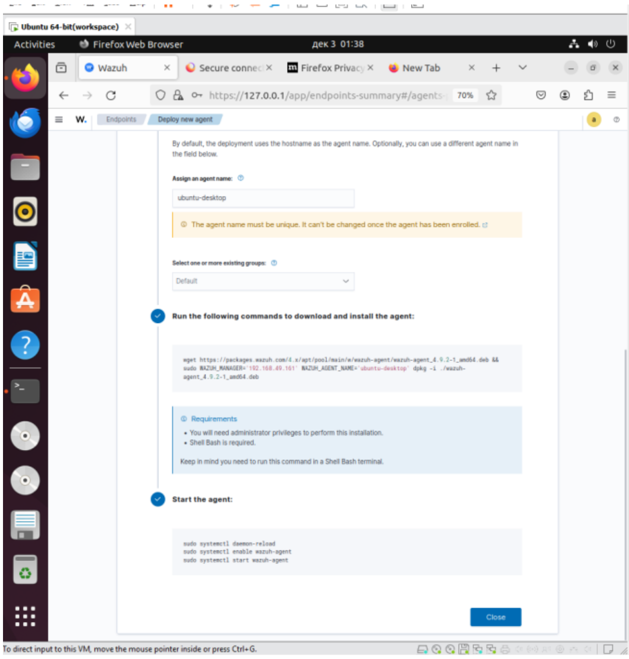
- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

5 **Start the agent:**

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Ввели все команды и установили



By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ubuntu-desktop

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: Default

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.49.161' WAZUH_AGENT_NAME='ubuntu-desktop' dpkg -i ./wazuh-
agent_4.9.2-1_amd64.deb
```

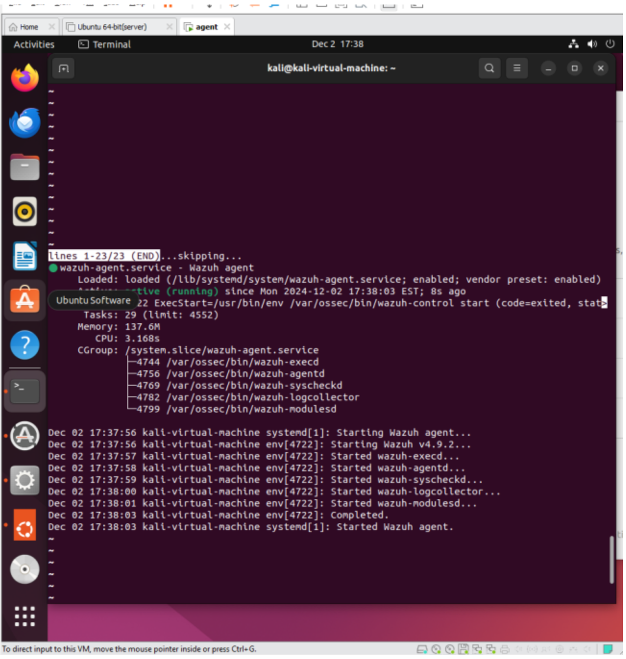
Requirements
- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Close
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Home
Ubuntu 64-bit(server)
agent
Activities
Terminal
Dec 2 17:38
kali@kali-virtual-machine: ~
Ubuntu Software
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

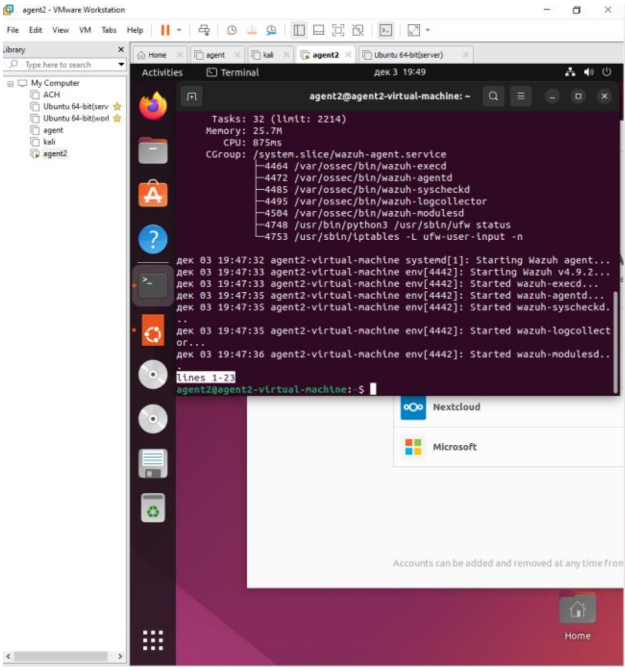
```
lines 1-23/23 (END)...skipping...
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-12-02 17:38:03 EST; 8s ago
    Process: 4722 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, stat>
      Tasks: 29 (limit: 4552)
     Memory: 137.6M
        CPU: 3.168s
     CGroup: /system.slice/wazuh-agent.service
             ├─4744 /var/ossec/bin/wazuh-execd
             ├─4756 /var/ossec/bin/wazuh-agentd
             ├─4769 /var/ossec/bin/wazuh-syscheckd
             ├─4782 /var/ossec/bin/wazuh-logcollector
             └─4799 /var/ossec/bin/wazuh-modulesd

Dec 02 17:37:56 kali-virtual-machine systemd[1]: Starting Wazuh agent...
Dec 02 17:37:56 kali-virtual-machine env[4722]: Starting Wazuh v4.9.2...
Dec 02 17:37:57 kali-virtual-machine env[4722]: Started wazuh-execd...
Dec 02 17:37:58 kali-virtual-machine env[4722]: Started wazuh-agentd...
Dec 02 17:37:59 kali-virtual-machine env[4722]: Started wazuh-syscheckd...
Dec 02 17:38:00 kali-virtual-machine env[4722]: Started wazuh-logcollector...
Dec 02 17:38:01 kali-virtual-machine env[4722]: Started wazuh-modulesd...
Dec 02 17:38:03 kali-virtual-machine env[4722]: Completed.
Dec 02 17:38:03 kali-virtual-machine systemd[1]: Started Wazuh agent.
```

Видим что сервер «увидел» агента

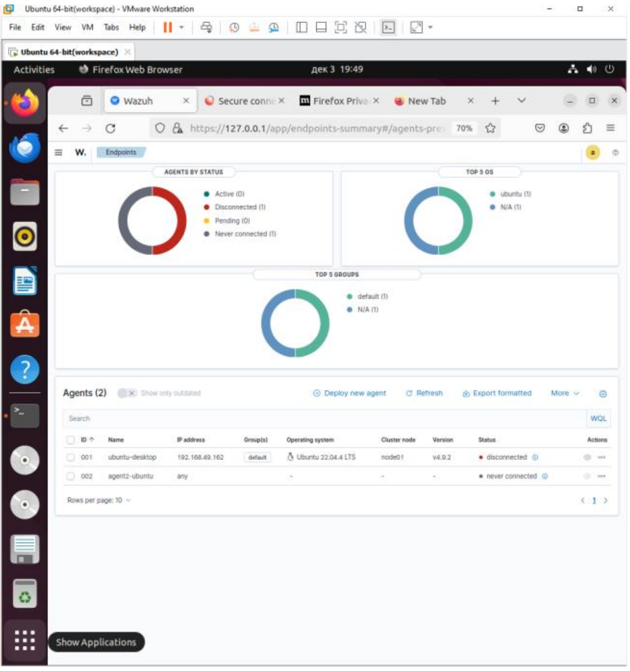
User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvyobiF2

Добавил еще одну машину потому что прошлая почему-то решила больше не работать



```
      Tasks: 32 (limit: 2214)
     Memory: 25.7M
        CPU: 875ms
     CGroup: /system.slice/wazuh-agent.service
             ├─4464 /var/ossec/bin/wazuh-execd
             ├─4472 /var/ossec/bin/wazuh-agentd
             ├─4485 /var/ossec/bin/wazuh-syscheckd
             ├─4495 /var/ossec/bin/wazuh-logcollector
             ├─4504 /var/ossec/bin/wazuh-modulesd
             ├─4748 /usr/bin/python3 /usr/sbin/ufw status
             └─4753 /usr/sbin/iptables -L ufw-user-input -n

дек 03 19:47:32 agent2-virtual-machine systemd[1]: Starting Wazuh agent...
дек 03 19:47:33 agent2-virtual-machine env[4442]: Starting Wazuh v4.9.2...
дек 03 19:47:33 agent2-virtual-machine env[4442]: Started wazuh-execd...
дек 03 19:47:35 agent2-virtual-machine env[4442]: Started wazuh-agentd...
дек 03 19:47:35 agent2-virtual-machine env[4442]: Started wazuh-syscheckd.
..
дек 03 19:47:35 agent2-virtual-machine env[4442]: Started wazuh-logcollect
or...
дек 03 19:47:36 agent2-virtual-machine env[4442]: Started wazuh-modulesd..
.
lines 1-23
agent2@agent2-virtual-machine:~$ 
```

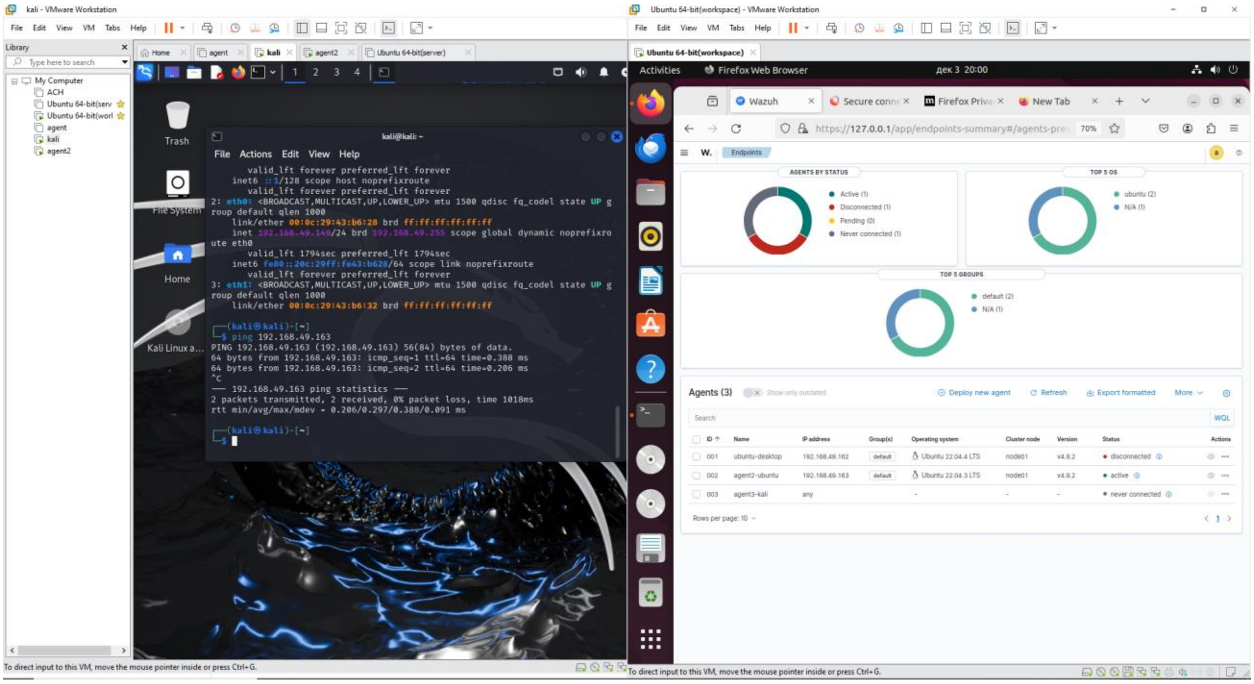


Agents (2)

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	ubuntu-desktop	192.168.49.162	default	Ubuntu 22.04.4 LTS	node01	v4.9.2	● disconnected	
002	agent2-ubuntu	any		-	-	-	● never connected	

Rows per page: 10

Добавил еще кали линукс,его события тоже можно будет посмотреть



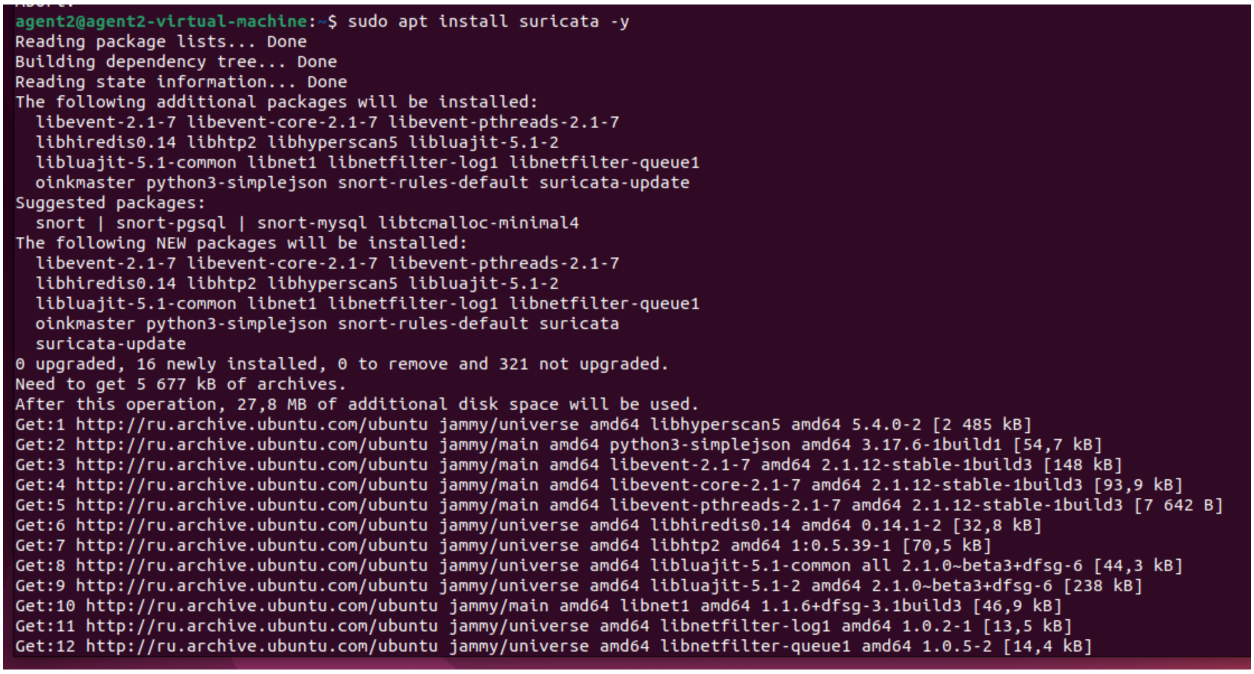
```
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:43:b6:28 brd ff:ff:ff:ff:ff:ff
    inet 192.168.49.149/24 brd 192.168.49.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1794sec preferred_lft 1794sec
    inet6 fe80::20c:29ff:fe43:b628/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:43:b6:32 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ ping 192.168.49.163
PING 192.168.49.163 (192.168.49.163) 56(84) bytes of data.
64 bytes from 192.168.49.163: icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from 192.168.49.163: icmp_seq=2 ttl=64 time=0.206 ms
^C
─── 192.168.49.163 ping statistics ───
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.206/0.297/0.388/0.091 ms

┌──(kali㉿kali)-[~]
└─$ 
```

Agents (3)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	ubuntu-desktop	192.168.49.162	default	Ubuntu 22.04.4 LTS	node01	v4.9.2	● disconnected	···
002	agent2-ubuntu	192.168.49.163	default	Ubuntu 22.04.3 LTS	node01	v4.9.2	● active	···
003	agent3-kali	any		-	-	-	● never connected	···

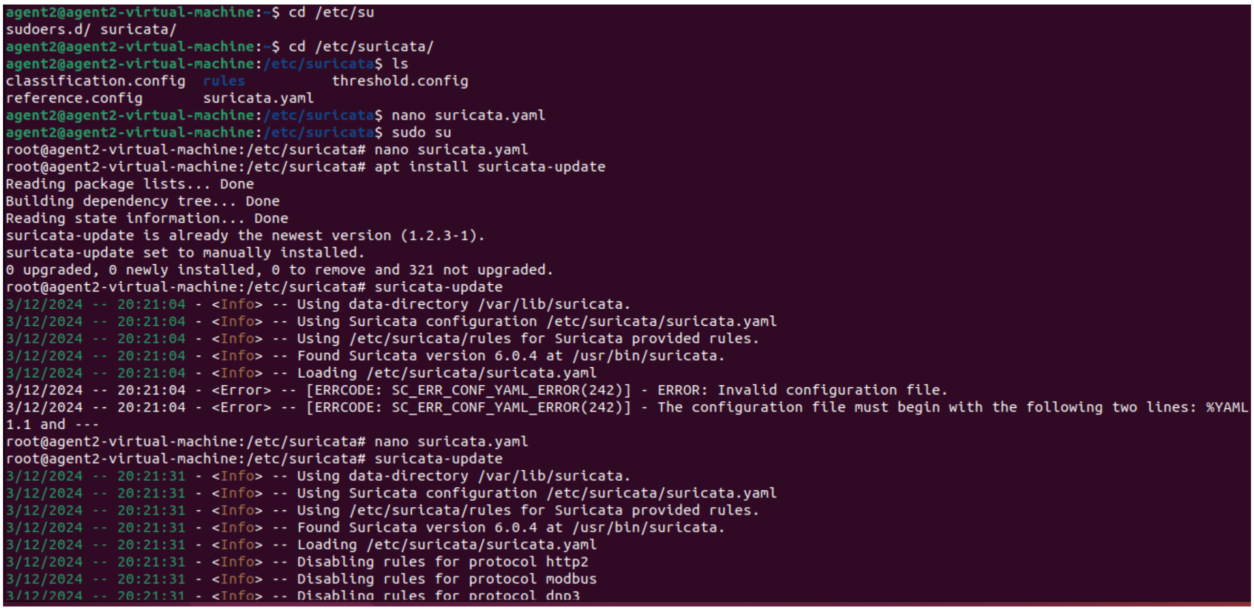
Rows per page: 10

Скачали сурикату



```
agent2@agent2-virtual-machine:~$ sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2
  libluajit-5.1-common libnet1 libnetfilter-log1 libnetfilter-queue1
  oinkmaster python3-simplejson snort-rules-default suricata-update
Suggested packages:
  snort | snort-pgsql | snort-mysql libtcmalloc-minimal4
The following NEW packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2
  libluajit-5.1-common libnet1 libnetfilter-log1 libnetfilter-queue1
  oinkmaster python3-simplejson snort-rules-default suricata
  suricata-update
0 upgraded, 16 newly installed, 0 to remove and 321 not upgraded.
Need to get 5 677 kB of archives.
After this operation, 27,8 MB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libhyperscan5 amd64 5.4.0-2 [2 485 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 python3-simplejson amd64 3.17.6-1build1 [54,7 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-2.1-7 amd64 2.1.12-stable-1build3 [148 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-core-2.1-7 amd64 2.1.12-stable-1build3 [93,9 kB]
Get:5 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1build3 [7 642 B]
Get:6 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libhiredis0.14 amd64 0.14.1-2 [32,8 kB]
Get:7 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libhtp2 amd64 1:0.5.39-1 [70,5 kB]
Get:8 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-6 [44,3 kB]
Get:9 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-6 [238 kB]
Get:10 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 libnet1 amd64 1.1.6+dfsg-3.1build3 [46,9 kB]
Get:11 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libnetfilter-log1 amd64 1.0.2-1 [13,5 kB]
Get:12 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libnetfilter-queue1 amd64 1.0.5-2 [14,4 kB]
```

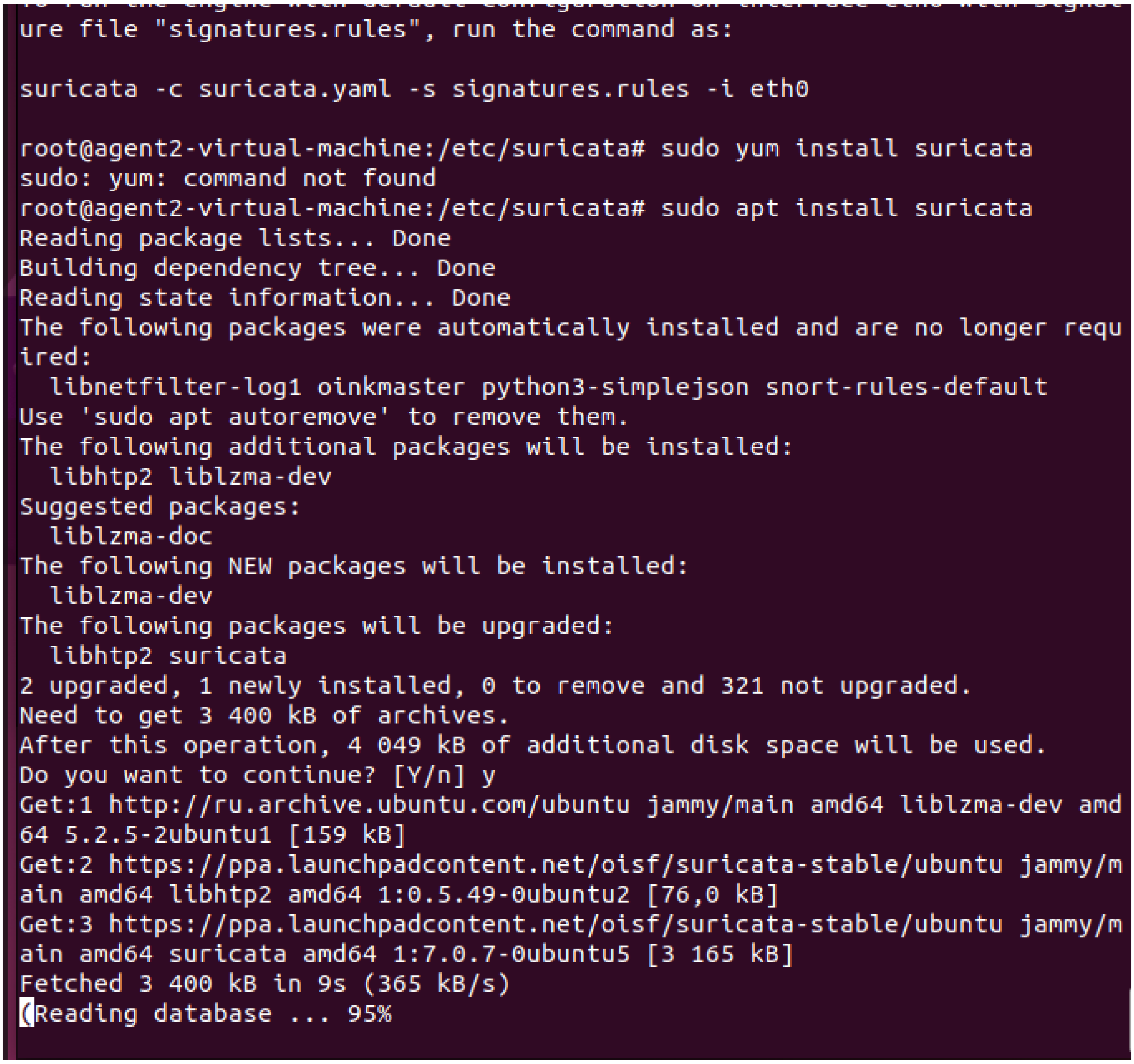
Установили правила



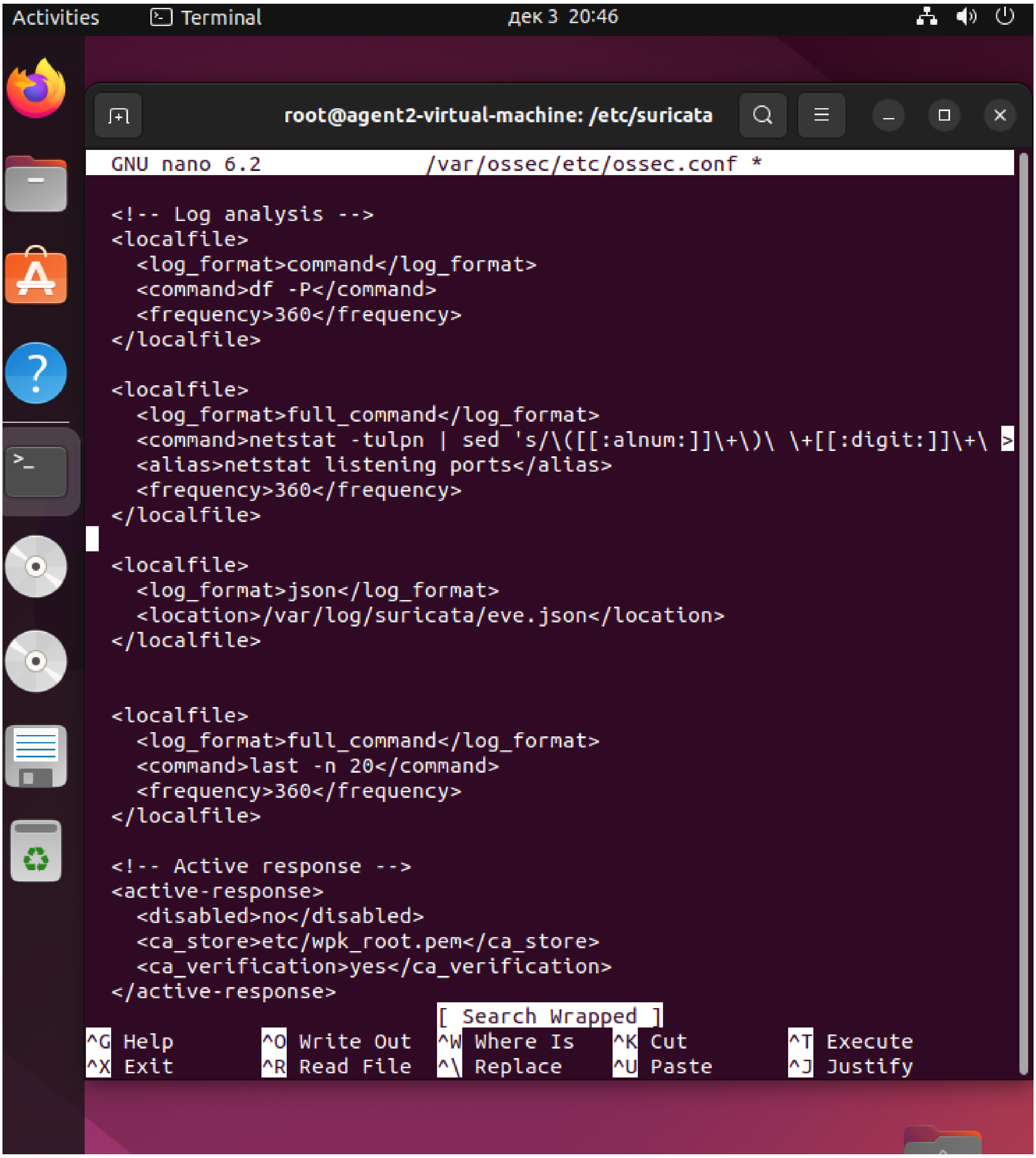
```
agent2@agent2-virtual-machine:~$ cd /etc/su
sudoers.d/ suricata/
agent2@agent2-virtual-machine:~$ cd /etc/suricata/
agent2@agent2-virtual-machine:/etc/suricata$ ls
classification.config  rules          threshold.config
reference.config       suricata.yaml
agent2@agent2-virtual-machine:/etc/suricata$ nano suricata.yaml
agent2@agent2-virtual-machine:/etc/suricata$ sudo su
root@agent2-virtual-machine:/etc/suricata# nano suricata.yaml
root@agent2-virtual-machine:/etc/suricata# apt install suricata-update
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata-update is already the newest version (1.2.3-1).
suricata-update set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 321 not upgraded.
root@agent2-virtual-machine:/etc/suricata# suricata-update
3/12/2024 -- 20:21:04 - <Info> -- Using data-directory /var/lib/suricata.
3/12/2024 -- 20:21:04 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/12/2024 -- 20:21:04 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/12/2024 -- 20:21:04 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
3/12/2024 -- 20:21:04 - <Info> -- Loading /etc/suricata/suricata.yaml
3/12/2024 -- 20:21:04 - <Error> -- [ERRCODE: SC_ERR_CONF_YAML_ERROR(242)] - ERROR: Invalid configuration file.
3/12/2024 -- 20:21:04 - <Error> -- [ERRCODE: SC_ERR_CONF_YAML_ERROR(242)] - The configuration file must begin with the following two lines: %YAML
1.1 and ---
root@agent2-virtual-machine:/etc/suricata# nano suricata.yaml
root@agent2-virtual-machine:/etc/suricata# suricata-update
3/12/2024 -- 20:21:31 - <Info> -- Using data-directory /var/lib/suricata.
3/12/2024 -- 20:21:31 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
3/12/2024 -- 20:21:31 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
3/12/2024 -- 20:21:31 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
3/12/2024 -- 20:21:31 - <Info> -- Loading /etc/suricata/suricata.yaml
3/12/2024 -- 20:21:31 - <Info> -- Disabling rules for protocol http2
3/12/2024 -- 20:21:31 - <Info> -- Disabling rules for protocol modbus
3/12/2024 -- 20:21:31 - <Info> -- Disabling rules for protocol dnp3
```

Установили на агенте чтобы была интеграция событий с сурикаты в вазух (брал json)

Обновляю сурикату,в связи с многочисленными ошибками

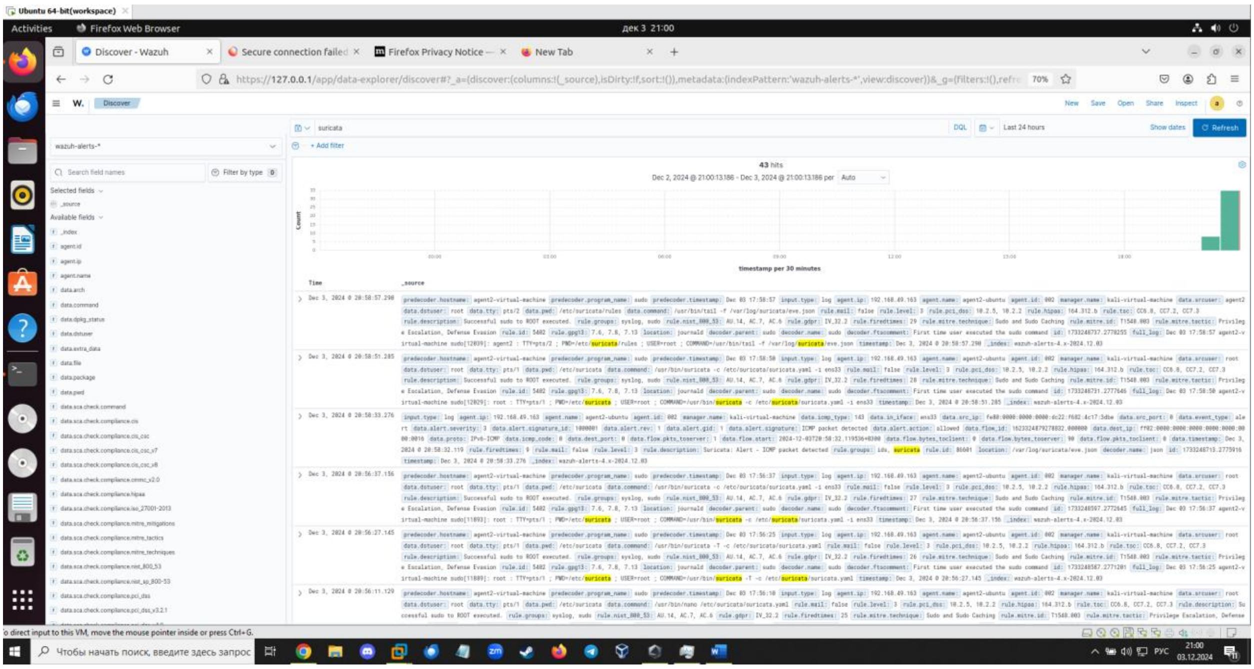


```
To run the engine with default configuration on interface eth0 with signat
ure file "signatures.rules", run the command as:

suricata -c suricata.yaml -s signatures.rules -i eth0

root@agent2-virtual-machine:/etc/suricata# sudo yum install suricata
sudo: yum: command not found
root@agent2-virtual-machine:/etc/suricata# sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requ
ired:
  libnetfilter-log1 oinkmaster python3-simplejson snort-rules-default
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libhtp2 liblzma-dev
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  liblzma-dev
The following packages will be upgraded:
  libhtp2 suricata
2 upgraded, 1 newly installed, 0 to remove and 321 not upgraded.
Need to get 3 400 kB of archives.
After this operation, 4 049 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 liblzma-dev amd
64 5.2.5-2ubuntu1 [159 kB]
Get:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/m
ain amd64 libhtp2 amd64 1:0.5.49-0ubuntu2 [76,0 kB]
Get:3 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/m
ain amd64 suricata amd64 1:7.0.7-0ubuntu5 [3 165 kB]
Fetched 3 400 kB in 9s (365 kB/s)
(Reading database ... 95%
```



```
  GNU nano 6.2              /var/ossec/etc/ossec.conf *

  <!-- Log analysis -->
  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ >
    <alias>netstat listening ports</alias>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>


  <localfile>
    <log_format>full_command</log_format>
    <command>last -n 20</command>
    <frequency>360</frequency>
  </localfile>

  <!-- Active response -->
  <active-response>
    <disabled>no</disabled>
    <ca_store>etc/wpk_root.pem</ca_store>
    <ca_verification>yes</ca_verification>
  </active-response>
                            [ Search Wrapped ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

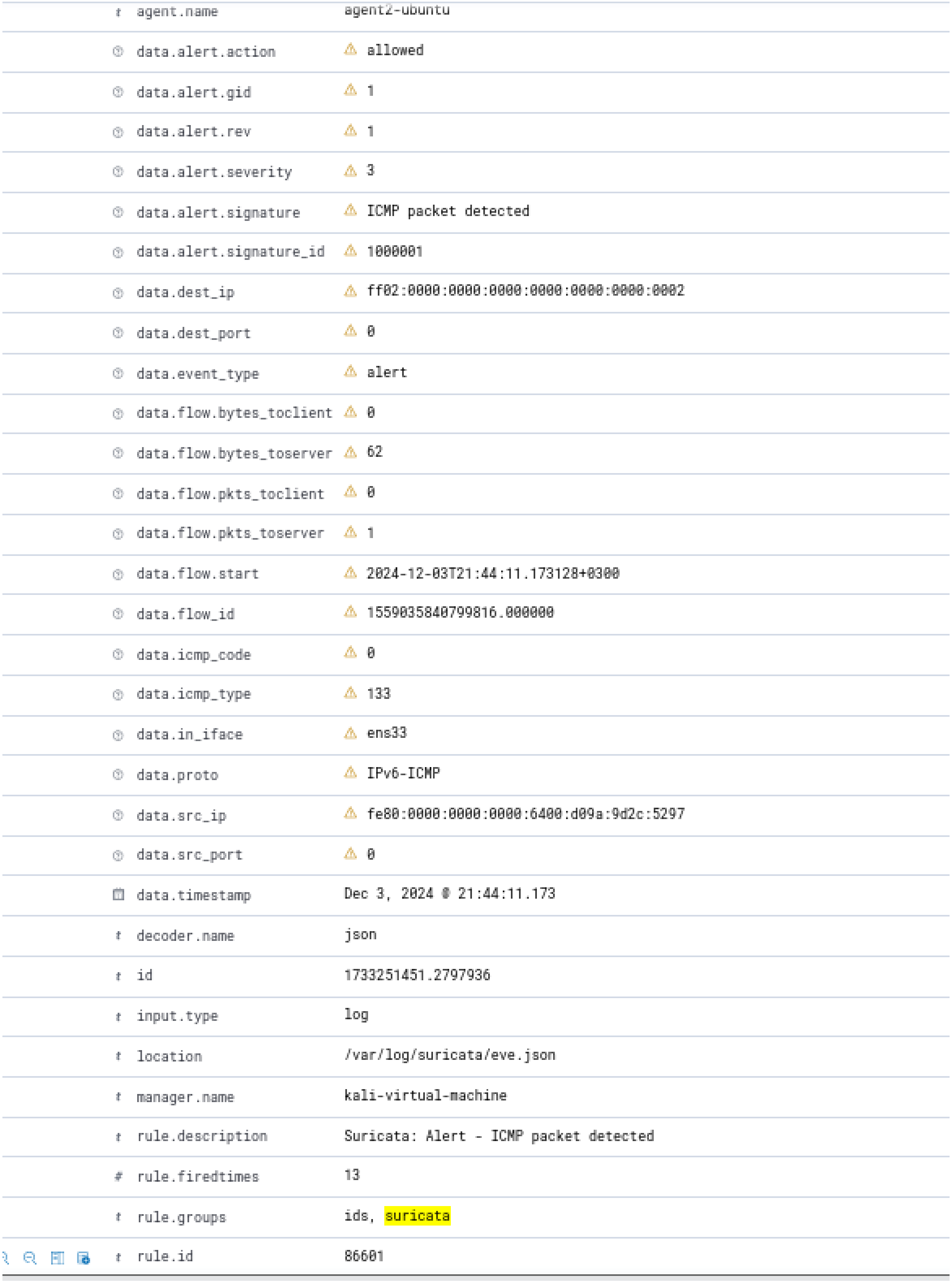
События приходят в вазух



Ubuntu 64-bit(workspace)
Activities
Firefox Web Browser
дек 3 21:00
Discover - Wazuh
Secure connection failed
Firefox Privacy Notice —
New Tab
https://127.0.0.1/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:'wazuh-alerts-*',view:discover))&_g=(filters:!(),refre
70%
W.
Discover
New
Save
Open
Share
Inspect
suricata
DQL
Last 24 hours
Show dates
Refresh
wazuh-alerts-*
+ Add filter
Search field names
Filter by type 0
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.arch
data.command
data.dpkg_status
data.dstuser
data.extra_data
data.file
data.package
data.pwd
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc
data.sca.check.compliance.cis_csc_v7
data.sca.check.compliance.cis_csc_v8
data.sca.check.compliance.cmmc_v2.0
data.sca.check.compliance.hipaa
data.sca.check.compliance.iso_27001-2013
data.sca.check.compliance.mitre_mitigations
data.sca.check.compliance.mitre_tactics
data.sca.check.compliance.mitre_techniques
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.nist_sp_800-53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.pci_dss_v3.2.1
43 hits
Dec 2, 2024 @ 21:00:13.186 - Dec 3, 2024 @ 21:00:13.186 per
Auto
Count
35
30
25
20
15
10
5
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
timestamp per 30 minutes
Time
_source
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Чтобы начать поиск, введите здесь запрос
РУС
21:00
03.12.2024

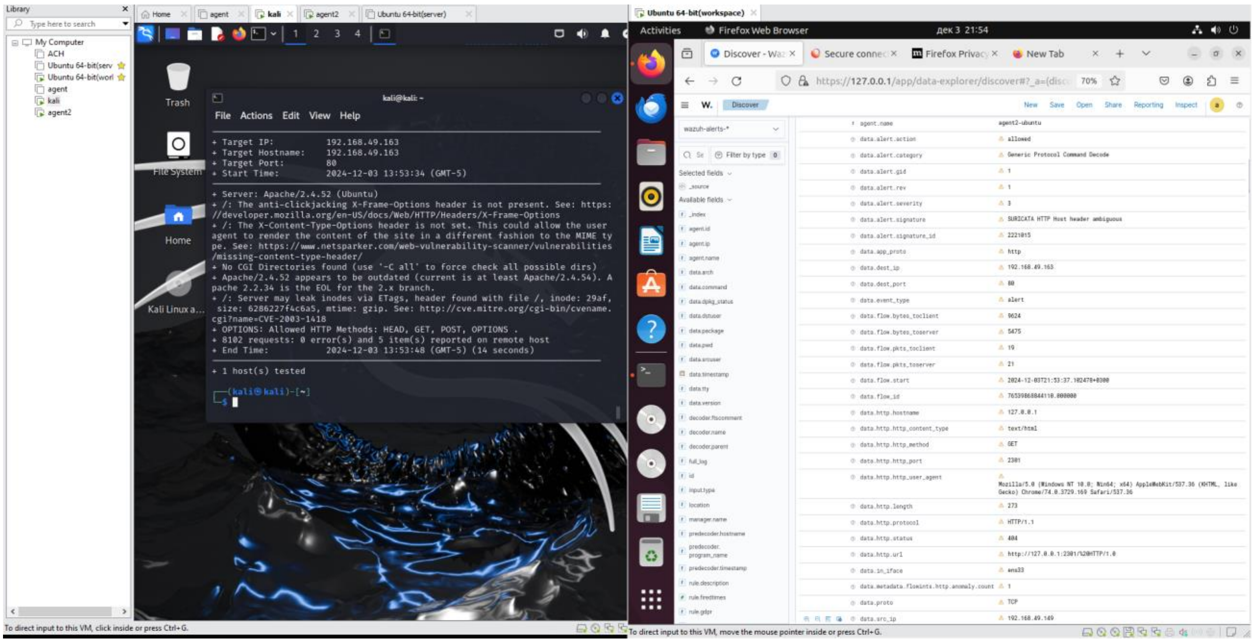
```
Dec 3, 2024 @ 20:58:57.290  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 17:58:57 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: agent2
                            data.dstuser: root data.tty: pts/2 data.pwd: /etc/suricata/rules data.command: /usr/bin/tail -f /var/log/suricata/eve.json rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3
                            rule.description: Successful sudo to ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 29 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privileg
                            e Escalation, Defense Evasion rule.id: 5402 rule.gpg13: 7.6, 7.8, 7.13 location: journald decoder.parent: sudo decoder.name: sudo decoder.ftscomment: First time user executed the sudo command id: 1733248737.2778255 full_log: Dec 03 17:58:57 agent2-v
                            irtual-machine sudo[12039]: agent2 : TTY=pts/2 ; PWD=/etc/suricata/rules ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/suricata/eve.json timestamp: Dec 3, 2024 @ 20:58:57.290 _index: wazuh-alerts-4.x-2024.12.03
Dec 3, 2024 @ 20:58:51.285  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 17:58:50 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: root
                            data.dstuser: root data.tty: pts/1 data.pwd: /etc/suricata data.command: /usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33 rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3
                            rule.description: Successful sudo to ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 28 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privileg
                            e Escalation, Defense Evasion rule.id: 5402 rule.gpg13: 7.6, 7.8, 7.13 location: journald decoder.parent: sudo decoder.name: sudo decoder.ftscomment: First time user executed the sudo command id: 1733248731.2777646 full_log: Dec 03 17:58:50 agent2-v
                            irtual-machine sudo[12029]: root : TTY=pts/1 ; PWD=/etc/suricata ; USER=root ; COMMAND=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33 timestamp: Dec 3, 2024 @ 20:58:51.285 _index: wazuh-alerts-4.x-2024.12.03
Dec 3, 2024 @ 20:58:33.276  input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.icmp_type: 143 data.in_iface: ens33 data.src_ip: fe80:0000:0000:0000:dc22:f682:4c17:3dbe data.src_port: 0 data.event_type: ale
                            rt data.alert.severity: 3 data.alert.signature_id: 1000001 data.alert.rev: 1 data.alert.gid: 1 data.alert.signature: ICMP packet detected data.alert.action: allowed data.flow_id: 1623324879278832.000000 data.dest_ip: ff02:0000:0000:0000:0000:0000:00
                            00:0016 data.proto: IPv6-ICMP data.icmp_code: 0 data.dest_port: 0 data.flow.pkts_toserver: 1 data.flow.start: 2024-12-03T20:58:32.119536+0300 data.flow.bytes_toclient: 0 data.flow.bytes_toserver: 90 data.flow.pkts_toclient: 0 data.timestamp: Dec 3,
                            2024 @ 20:58:32.119 rule.firedtimes: 9 rule.mail: false rule.level: 3 rule.description: Suricata: Alert - ICMP packet detected rule.groups: ids, suricata rule.id: 86601 location: /var/log/suricata/eve.json decoder.name: json id: 1733248713.2775916
                            timestamp: Dec 3, 2024 @ 20:58:33.276 _index: wazuh-alerts-4.x-2024.12.03
Dec 3, 2024 @ 20:56:37.156  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 17:56:37 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: root
                            data.dstuser: root data.tty: pts/1 data.pwd: /etc/suricata data.command: /usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33 rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3
                            rule.description: Successful sudo to ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 27 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privileg
                            e Escalation, Defense Evasion rule.id: 5402 rule.gpg13: 7.6, 7.8, 7.13 location: journald decoder.parent: sudo decoder.name: sudo decoder.ftscomment: First time user executed the sudo command id: 1733248597.2772645 full_log: Dec 03 17:56:37 agent2-v
                            irtual-machine sudo[11893]: root : TTY=pts/1 ; PWD=/etc/suricata ; USER=root ; COMMAND=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33 timestamp: Dec 3, 2024 @ 20:56:37.156 _index: wazuh-alerts-4.x-2024.12.03
Dec 3, 2024 @ 20:56:27.145  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 17:56:25 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: root
                            data.dstuser: root data.tty: pts/1 data.pwd: /etc/suricata data.command: /usr/bin/suricata -T -c /etc/suricata/suricata.yaml rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3
                            rule.description: Successful sudo to ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 26 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privileg
                            e Escalation, Defense Evasion rule.id: 5402 rule.gpg13: 7.6, 7.8, 7.13 location: journald decoder.parent: sudo decoder.name: sudo decoder.ftscomment: First time user executed the sudo command id: 1733248587.2771201 full_log: Dec 03 17:56:25 agent2-v
                            irtual-machine sudo[11889]: root : TTY=pts/1 ; PWD=/etc/suricata ; USER=root ; COMMAND=/usr/bin/suricata -T -c /etc/suricata/suricata.yaml timestamp: Dec 3, 2024 @ 20:56:27.145 _index: wazuh-alerts-4.x-2024.12.03
Dec 3, 2024 @ 20:56:11.129  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 17:56:10 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: root
                            data.dstuser: root data.tty: pts/1 data.pwd: /etc/suricata data.command: /usr/bin/nano /etc/suricata/suricata.yaml rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: Su
                            ccessful sudo to ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 25 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privilege Escalation, Defense
```

Это я отправлял пакет с кали на убунту



t	agent.name	agent2-ubuntu
◷	data.alert.action	⚠ allowed
◷	data.alert.gid	⚠ 1
◷	data.alert.rev	⚠ 1
◷	data.alert.severity	⚠ 3
◷	data.alert.signature	⚠ ICMP packet detected
◷	data.alert.signature_id	⚠ 1000001
◷	data.dest_ip	⚠ ff02:0000:0000:0000:0000:0000:0000:0002
◷	data.dest_port	⚠ 0
◷	data.event_type	⚠ alert
◷	data.flow.bytes_toclient	⚠ 0
◷	data.flow.bytes_toserver	⚠ 62
◷	data.flow.pkts_toclient	⚠ 0
◷	data.flow.pkts_toserver	⚠ 1
◷	data.flow.start	⚠ 2024-12-03T21:44:11.173128+0300
◷	data.flow_id	⚠ 1559035840799816.000000
◷	data.icmp_code	⚠ 0
◷	data.icmp_type	⚠ 133
◷	data.in_iface	⚠ ens33
◷	data.proto	⚠ IPv6-ICMP
◷	data.src_ip	⚠ fe80:0000:0000:0000:6400:d09a:9d2c:5297
◷	data.src_port	⚠ 0
📅	data.timestamp	Dec 3, 2024 @ 21:44:11.173
t	decoder.name	json
t	id	1733251451.2797936
t	input.type	log
t	location	/var/log/suricata/eve.json
t	manager.name	kali-virtual-machine
t	rule.description	Suricata: Alert - ICMP packet detected
#	rule.firedtimes	13
t	rule.groups	ids, suricata
t	rule.id	86601

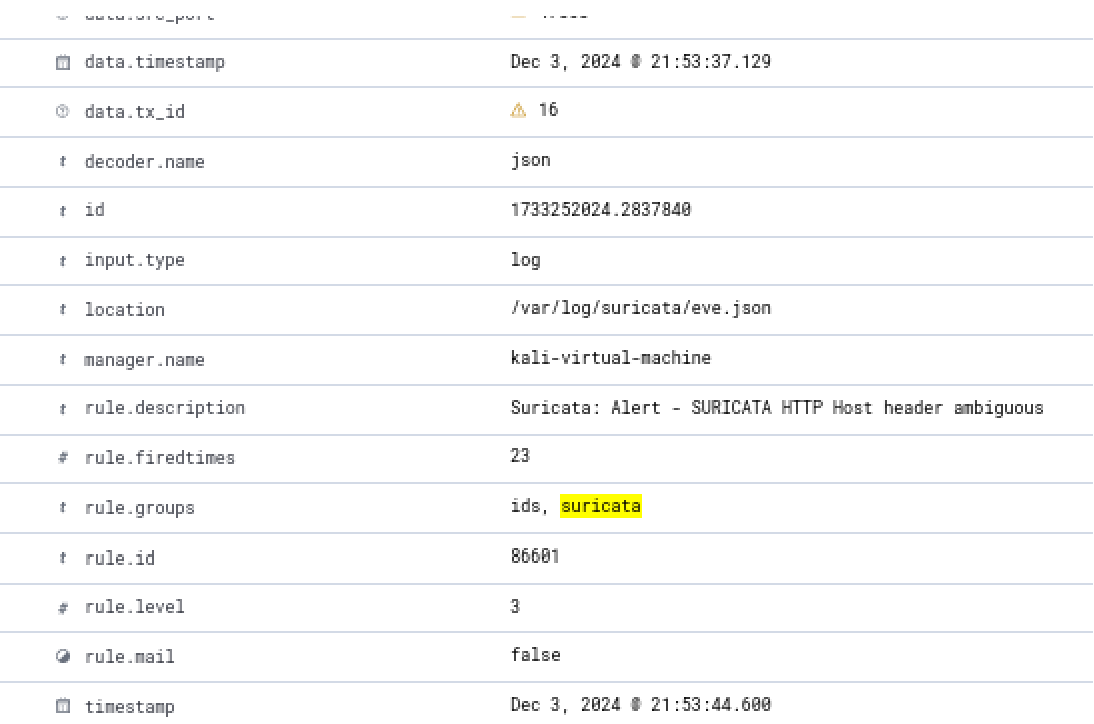
Проверка получения событий



```
+ Target IP:          192.168.49.163
+ Target Hostname:    192.168.49.163
+ Target Port:        80
+ Start Time:         2024-12-03 13:53:34 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af,
 size: 6286227f4c6a5, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ 8102 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-12-03 13:53:48 (GMT-5) (14 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$
```

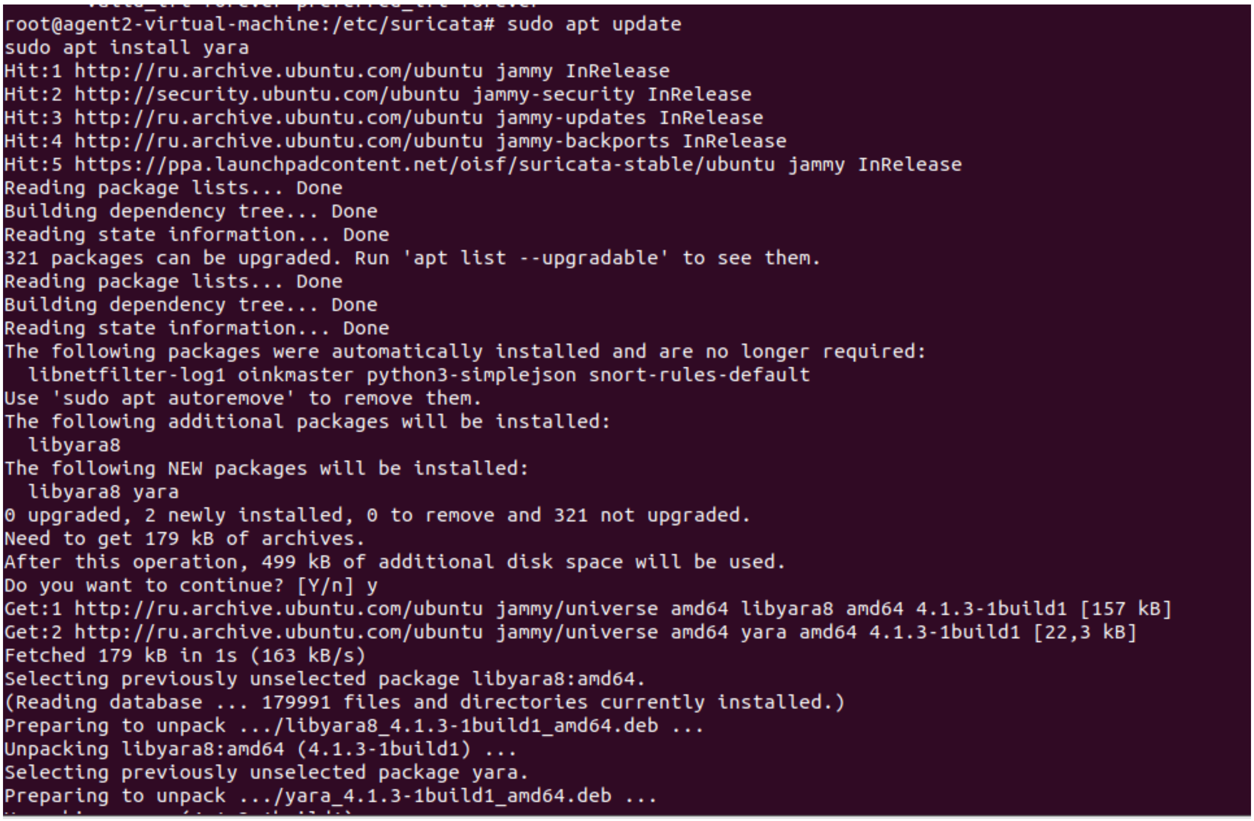
https://127.0.0.1/app/data-explorer/discover#?_a=(disc

agent.name	agent2-ubuntu
data.alert.action	⚠ allowed
data.alert.category	⚠ Generic Protocol Command Decode
data.alert.gid	⚠ 1
data.alert.rev	⚠ 1
data.alert.severity	⚠ 3
data.alert.signature	⚠ SURICATA HTTP Host header ambiguous
data.alert.signature_id	⚠ 2221015
data.app_proto	⚠ http
data.dest_ip	⚠ 192.168.49.163
data.dest_port	⚠ 80
data.event_type	⚠ alert
data.flow.bytes_toclient	⚠ 9624
data.flow.bytes_toserver	⚠ 5475
data.flow.pkts_toclient	⚠ 19
data.flow.pkts_toserver	⚠ 21
data.flow.start	⚠ 2024-12-03T21:53:37.102478+0300
data.flow_id	⚠ 765398688441l0.000000
data.http.hostname	⚠ 127.0.0.1
data.http.http_content_type	⚠ text/html
data.http.http_method	⚠ GET
data.http.http_port	⚠ 2301
data.http.http_user_agent	⚠ Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
data.http.length	⚠ 273
data.http.protocol	⚠ HTTP/1.1
data.http.status	⚠ 404
data.http.url	⚠ http://127.0.0.1:2301/%20HTTP/1.0
data.in_iface	⚠ ens33
data.metadata.flowints.http.anomaly.count	⚠ 1
data.proto	⚠ TCP
data.src_ip	⚠ 192.168.49.149

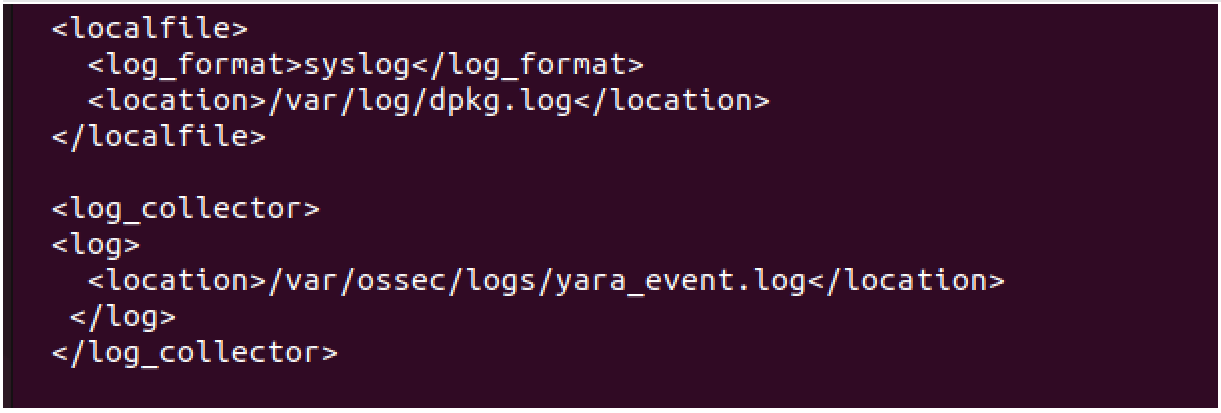


data.timestamp	Dec 3, 2024 @ 21:53:37.129
data.tx_id	⚠ 16
decoder.name	json
id	1733252024.2837840
input.type	log
location	/var/log/suricata/eve.json
manager.name	kali-virtual-machine
rule.description	Suricata: Alert - SURICATA HTTP Host header ambiguous
rule.firedtimes	23
rule.groups	ids, suricata
rule.id	86601
rule.level	3
rule.mail	false
timestamp	Dec 3, 2024 @ 21:53:44.600

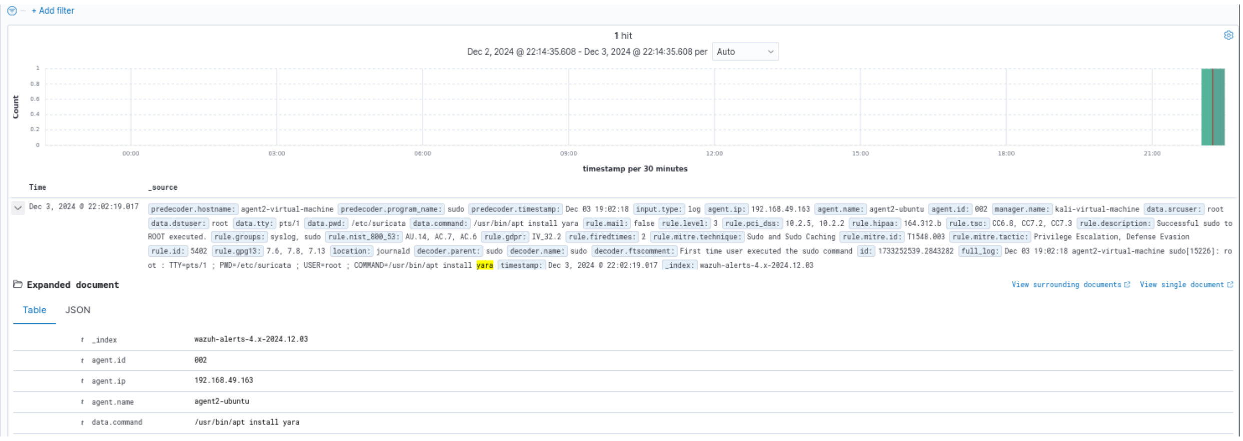
Для интегрирования событий yara



```
root@agent2-virtual-machine:/etc/suricata# sudo apt update
sudo apt install yara
Hit:1 http://ru.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://ru.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
321 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libnetfilter-log1 oinkmaster python3-simplejson snort-rules-default
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libyara8
The following NEW packages will be installed:
  libyara8 yara
0 upgraded, 2 newly installed, 0 to remove and 321 not upgraded.
Need to get 179 kB of archives.
After this operation, 499 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 libyara8 amd64 4.1.3-1build1 [157 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 yara amd64 4.1.3-1build1 [22,3 kB]
Fetched 179 kB in 1s (163 kB/s)
Selecting previously unselected package libyara8:amd64.
(Reading database ... 179991 files and directories currently installed.)
Preparing to unpack .../libyara8_4.1.3-1build1_amd64.deb ...
Unpacking libyara8:amd64 (4.1.3-1build1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_4.1.3-1build1_amd64.deb ...
```



```
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <log_collector>
  <log>
    <location>/var/ossec/logs/yara_event.log</location>
   </log>
  </log_collector>
```



```
Time                      _source
Dec 3, 2024 @ 22:02:19.017  predecoder.hostname: agent2-virtual-machine predecoder.program_name: sudo predecoder.timestamp: Dec 03 19:02:18 input.type: log agent.ip: 192.168.49.163 agent.name: agent2-ubuntu agent.id: 002 manager.name: kali-virtual-machine data.srcuser: root
data.dstuser: root data.tty: pts/1 data.pwd: /etc/suricata data.command: /usr/bin/apt install yara rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5, 10.2.2 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: Successful sudo to
ROOT executed. rule.groups: syslog, sudo rule.nist_800_53: AU.14, AC.7, AC.6 rule.gdpr: IV_32.2 rule.firedtimes: 2 rule.mitre.technique: Sudo and Sudo Caching rule.mitre.id: T1548.003 rule.mitre.tactic: Privilege Escalation, Defense Evasion
rule.id: 5402 rule.gpg13: 7.6, 7.8, 7.13 location: journald decoder.parent: sudo decoder.name: sudo decoder.ftscomment: First time user executed the sudo command id: 1733252539.2843282 full_log: Dec 03 19:02:18 agent2-virtual-machine sudo[15226]: ro
ot : TTY=pts/1 ; PWD=/etc/suricata ; USER=root ; COMMAND=/usr/bin/apt install yara timestamp: Dec 3, 2024 @ 22:02:19.017 _index: wazuh-alerts-4.x-2024.12.03
```

t _index	wazuh-alerts-4.x-2024.12.03
t agent.id	002
t agent.ip	192.168.49.163
t agent.name	agent2-ubuntu
t data.command	/usr/bin/apt install yara