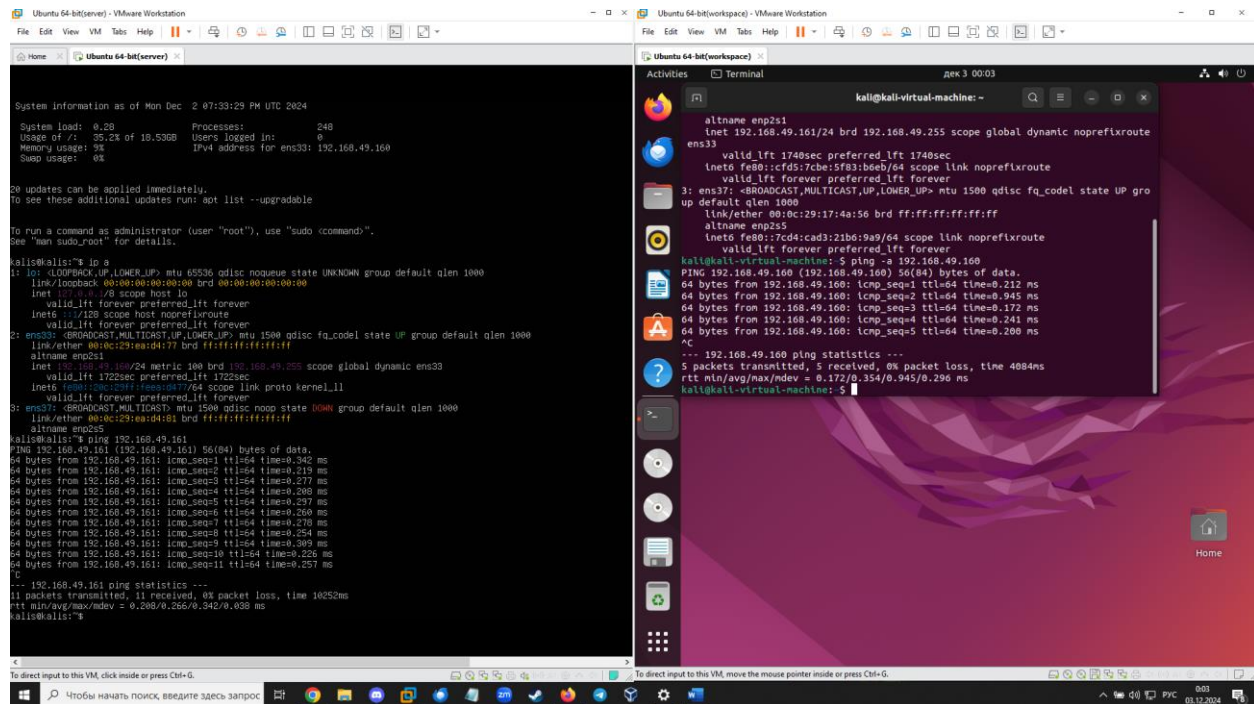
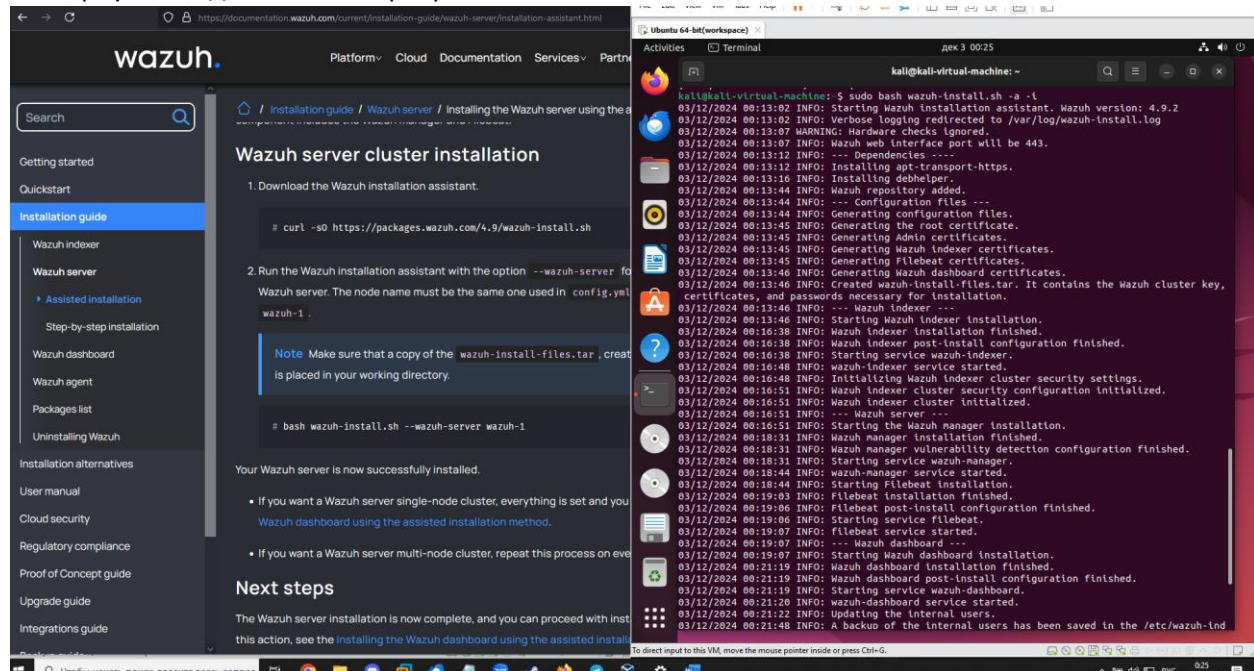


ПРЗ 3. WAZUH.

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



- 3) Развернуть на одной из ВМ сервер Wazuh



```

03/12/2024 00:21:18 INFO: A backup of the internal users has been saved in the /etc/wazuh-
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:~$

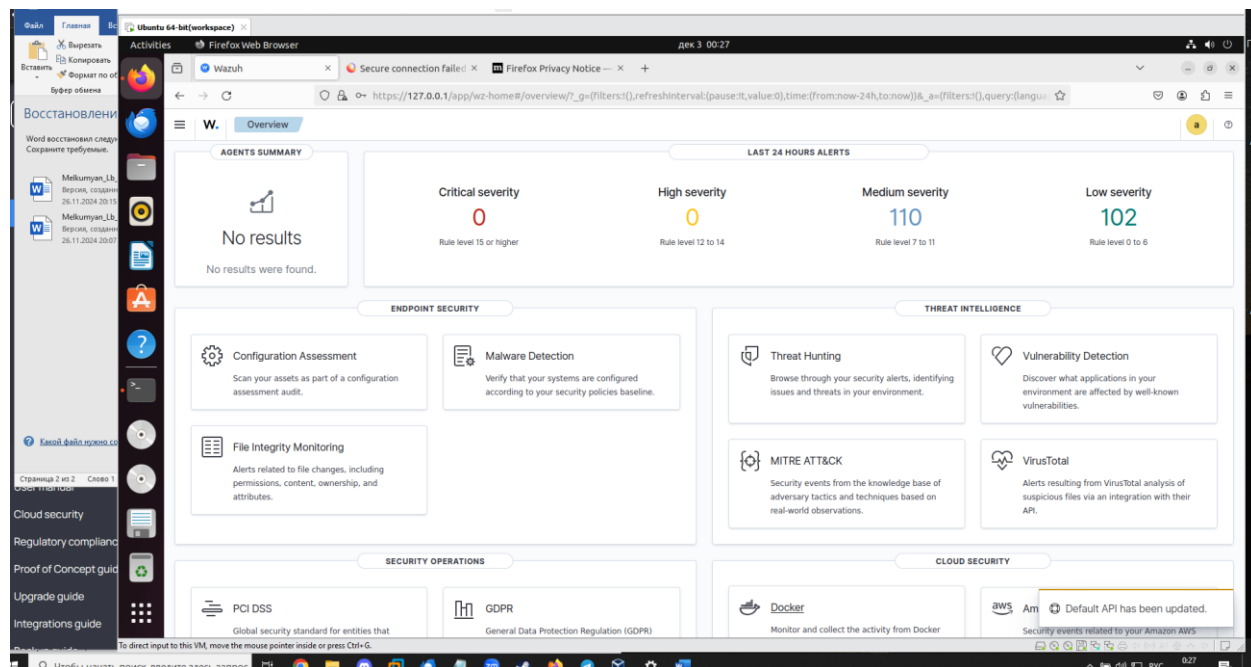
```

ut to this VM, move the mouse pointer inside or press Ctrl+G.

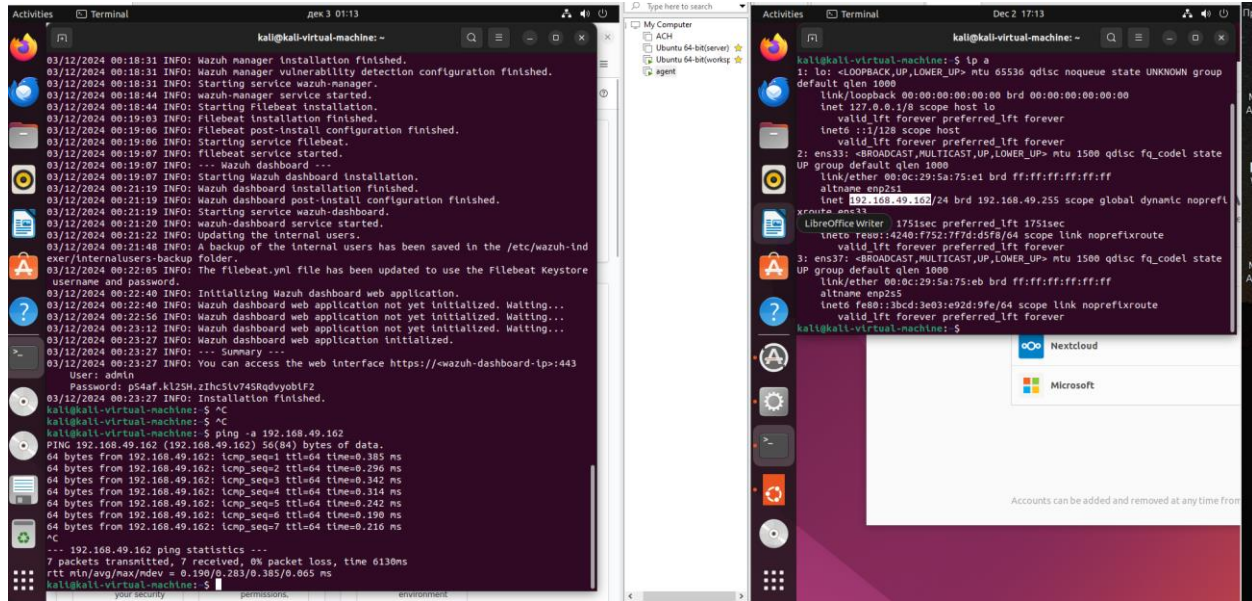
User: admin

Password: pS4af.kl2SH.zIhc5iv74SRqdvYobiF2

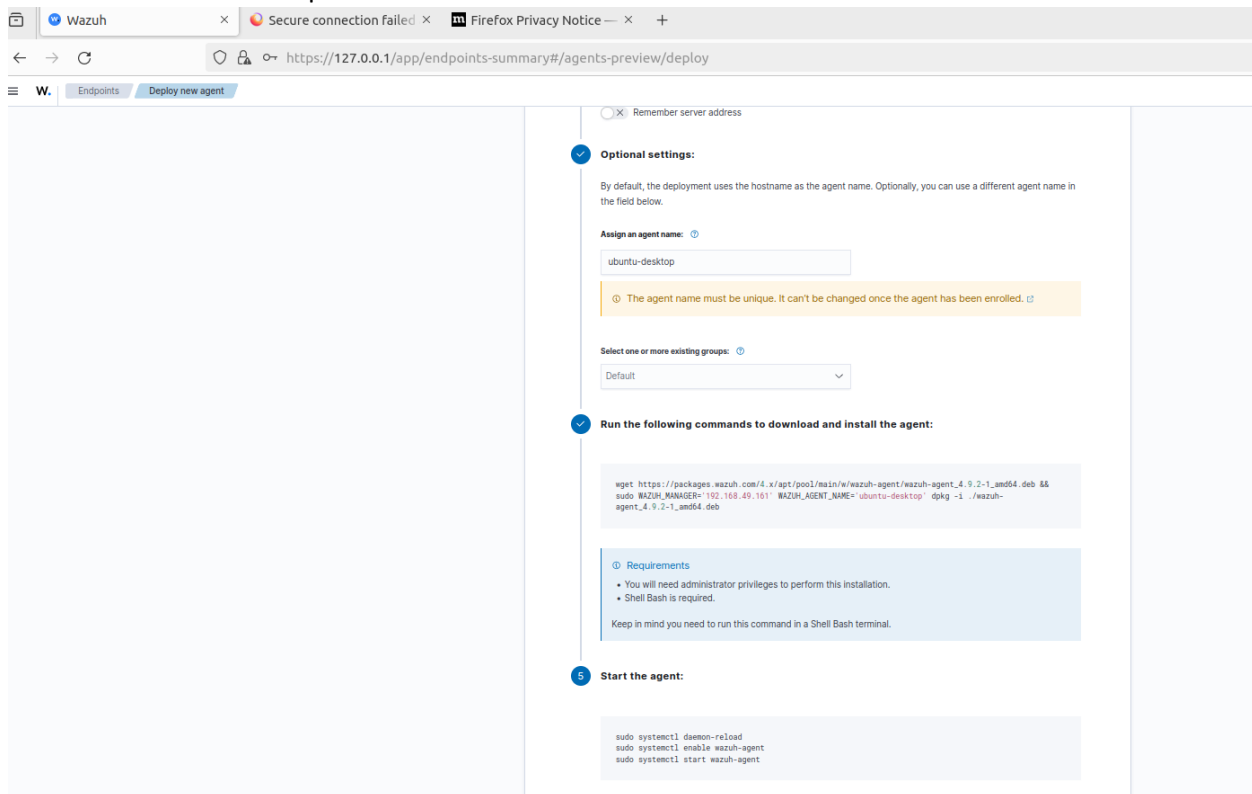
Зашли на сам Wazuh



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



4) Подключите агента используя документацию Устанавливаю агента через Wazuh



The image displays two side-by-side screenshots of a desktop environment, likely Ubuntu, showing the process of installing and configuring the Wazuh agent.

Left Screenshot (Firefox Web Browser):

- The browser window is titled "Wazuh" and shows the "Deploy new agent" page.
- The page contains instructions for assigning an agent name, with a default value of "ubuntu-desktop".
- A note states: "The agent name must be unique. It can't be changed once the agent has been enrolled."
- Below the name field, there is a section for "Select one or more existing groups" with a dropdown menu.
- A section titled "Run the following commands to download and install the agent:" provides a terminal command to download the Wazuh agent package and install it.
- A "Requirements" section lists: "You will need administrator privileges to perform this installation." and "Shell Bash is required."
- A note states: "Keep in mind you need to run this command in a Shell Bash terminal."
- A section titled "Start the agent:" provides a terminal command to start the Wazuh agent.
- A "Close" button is visible at the bottom right of the page.

Right Screenshot (Terminal Window):

- The terminal window is titled "Terminal" and shows the output of the Wazuh agent installation and startup commands.
- The output shows the agent name "wazuh-agent.service - Wazuh agent" and its status as "loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)".
- The output shows the agent is "Active (running)" since Mon 2024-12-02 17:38:03 EST; 8s ago.
- The output shows the agent's resources: "Tasks: 29 (limit: 452)", "Memory: 132.6M", and "CPU: 3.168s".
- The output shows the agent's group: "Group: /system.slice/wazuh-agent.service".
- The output shows the agent's files: "/etc/ossec/bin/wazuh-execd", "/etc/ossec/bin/wazuh-agentd", "/etc/ossec/bin/wazuh-syscheckd", "/etc/ossec/bin/wazuh-logcollector", and "/etc/ossec/bin/wazuh-modulesd".
- The output shows the agent's startup logs: "Dec 02 17:37:56 kali-virtual-machine systemd[1]: Starting Wazuh agent...", "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.", and "Dec 02 17:38:03 kali-virtual-machine systemd[1]: Started Wazuh agent."

W.

Endpoints

Agents by status

Active (1)

Disconnected (0)

Pending (0)

Never connected (0)

TOP 5 OS

ubuntu (1)

TOP 5 GROUPS

default (1)

Agents (1)

Show only outdated

Deploy new agent

Refresh

Export formatted

More

status=active

WQL

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	active	

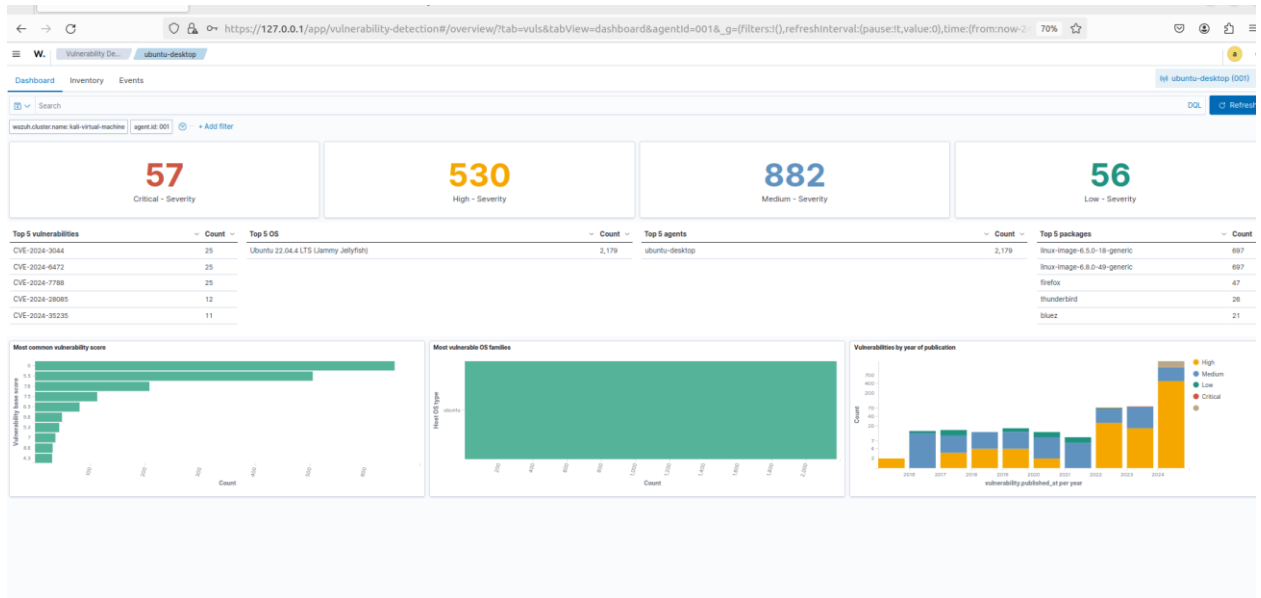
Rows per page: 10

< 1 >

Document Details

[view single document](#)[illegible]

Настройте выявление уязвимостей в соответствии с документацией



Настройте выявление скрытых процессов

```
<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- rootcheck execution frequency - every 12 hours by default-->

  <frequency>120</frequency>
```

Настройте выявление SQL-инъекций.

```
<ossec_config>
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

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

Настройте выявление web shell attack.

```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>
```