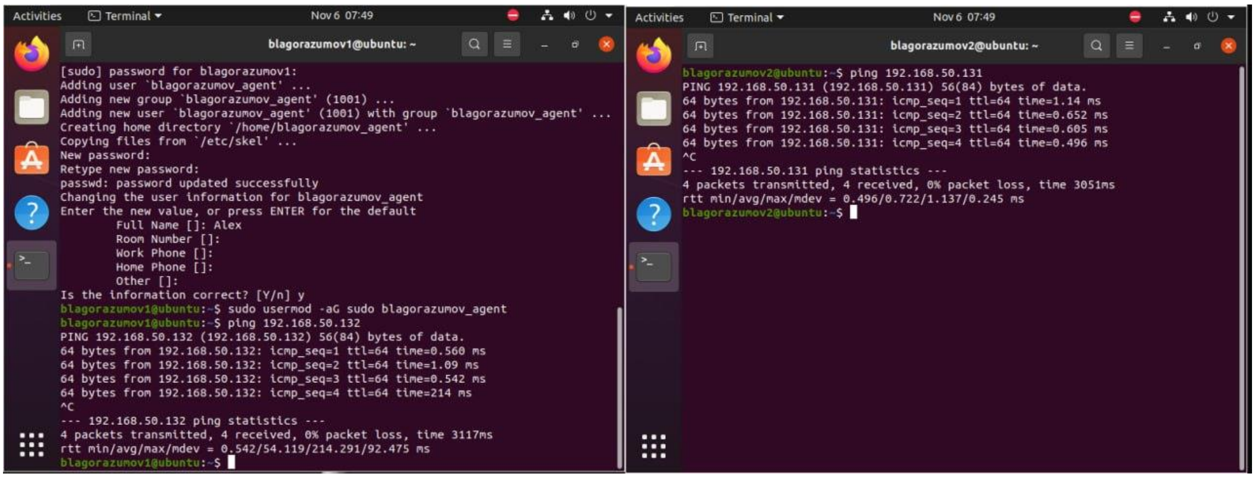
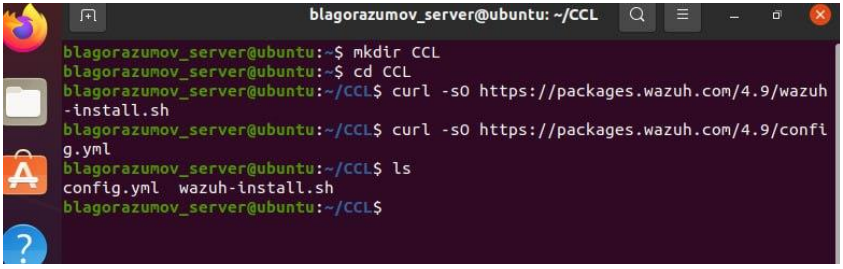


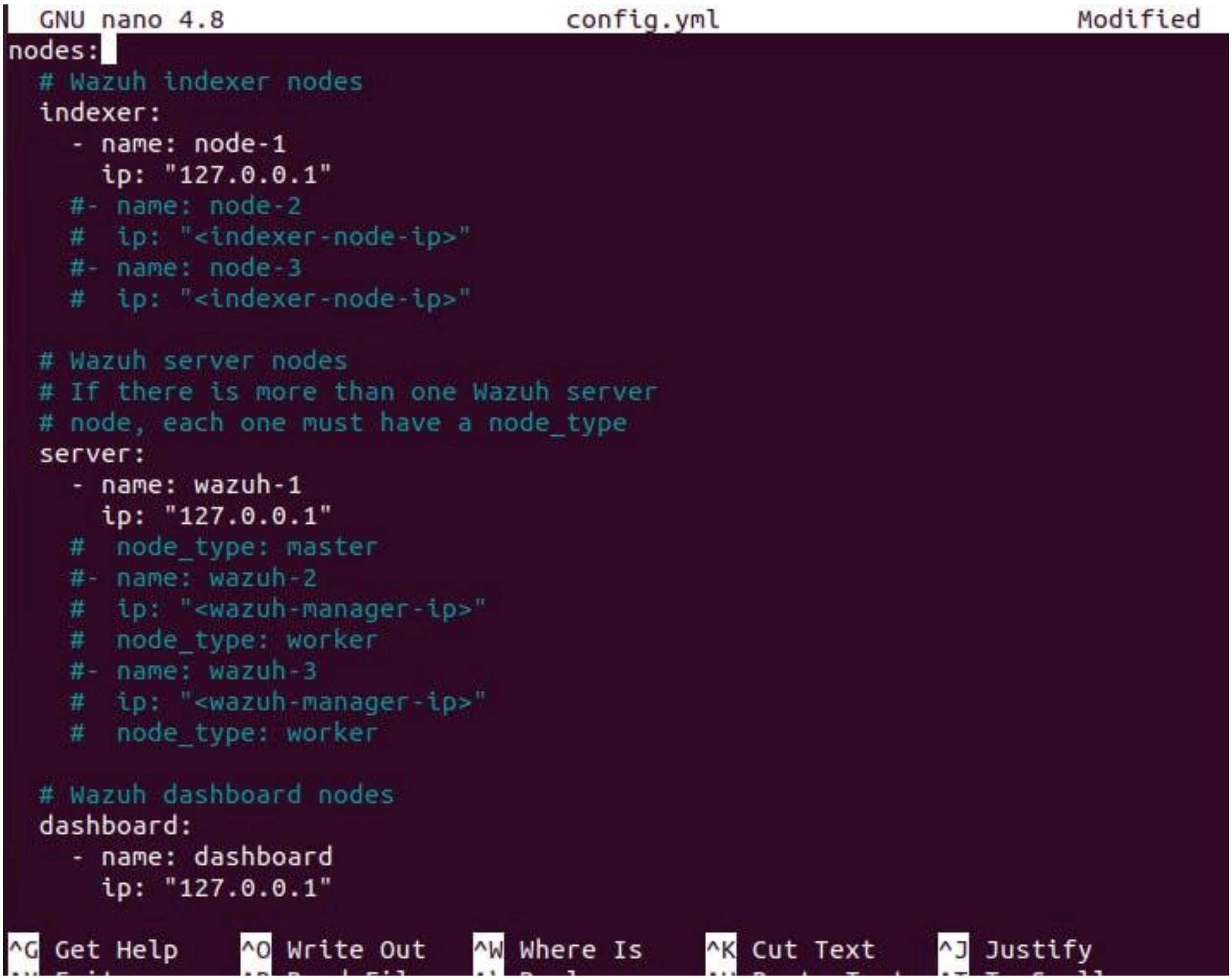
```
[sudo] password for blagorazumov1:
Adding user `blagorazumov_agent' ...
Adding new group `blagorazumov_agent' (1001) ...
Adding new user `blagorazumov_agent' (1001) with group `blagorazumov_agent' ...
Creating home directory `/home/blagorazumov_agent' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for blagorazumov_agent
Enter the new value, or press ENTER for the default
        Full Name []: Alex
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
blagorazumov1@ubuntu:~$ sudo usermod -aG sudo blagorazumov_agent
blagorazumov1@ubuntu:~$ ping 192.168.50.132
PING 192.168.50.132 (192.168.50.132) 56(84) bytes of data.
64 bytes from 192.168.50.132: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 192.168.50.132: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.50.132: icmp_seq=3 ttl=64 time=0.542 ms
64 bytes from 192.168.50.132: icmp_seq=4 ttl=64 time=214 ms
^C
--- 192.168.50.132 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3117ms
rtt min/avg/max/mdev = 0.542/54.119/214.291/92.475 ms
blagorazumov1@ubuntu:~$
```

```
blagorazumov2@ubuntu:~$ ping 192.168.50.131
PING 192.168.50.131 (192.168.50.131) 56(84) bytes of data.
64 bytes from 192.168.50.131: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.50.131: icmp_seq=2 ttl=64 time=0.652 ms
64 bytes from 192.168.50.131: icmp_seq=3 ttl=64 time=0.605 ms
64 bytes from 192.168.50.131: icmp_seq=4 ttl=64 time=0.496 ms
^C
--- 192.168.50.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.496/0.722/1.137/0.245 ms
blagorazumov2@ubuntu:~$
```

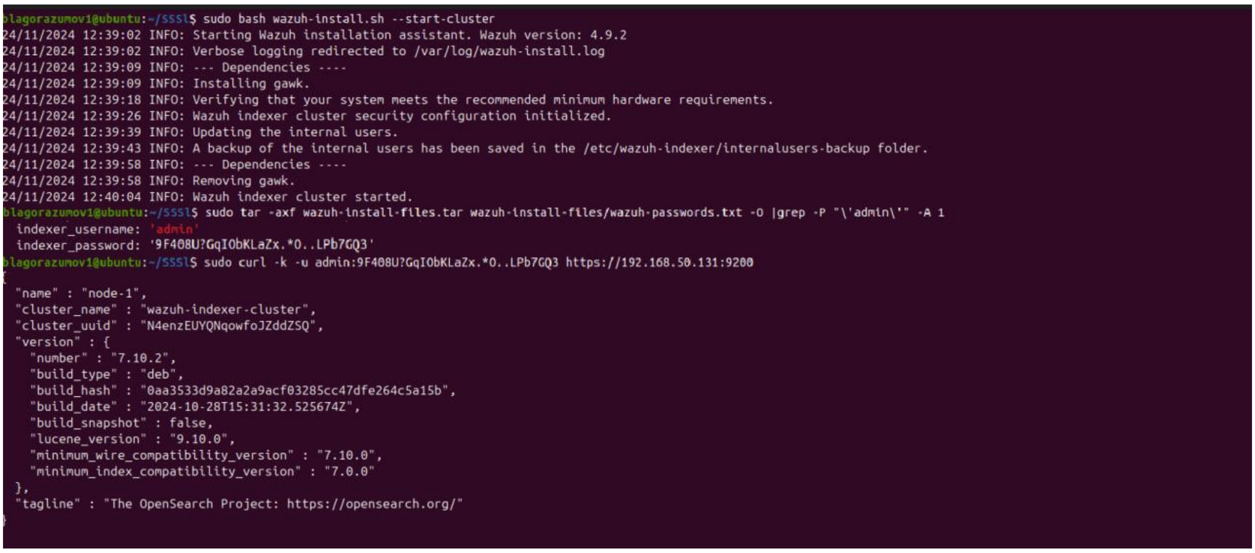
Развернули 2 ВМ и обеспечили между ними сетевой обмен



```
blagorazumov_server@ubuntu:~$ mkdir CCL
blagorazumov_server@ubuntu:~$ cd CCL
blagorazumov_server@ubuntu:~/CCL$ curl -sO https://packages.wazuh.com/4.9/wazuh
-install.sh
blagorazumov_server@ubuntu:~/CCL$ curl -sO https://packages.wazuh.com/4.9/confi
g.yml
blagorazumov_server@ubuntu:~/CCL$ ls
config.yml  wazuh-install.sh
blagorazumov_server@ubuntu:~/CCL$
```

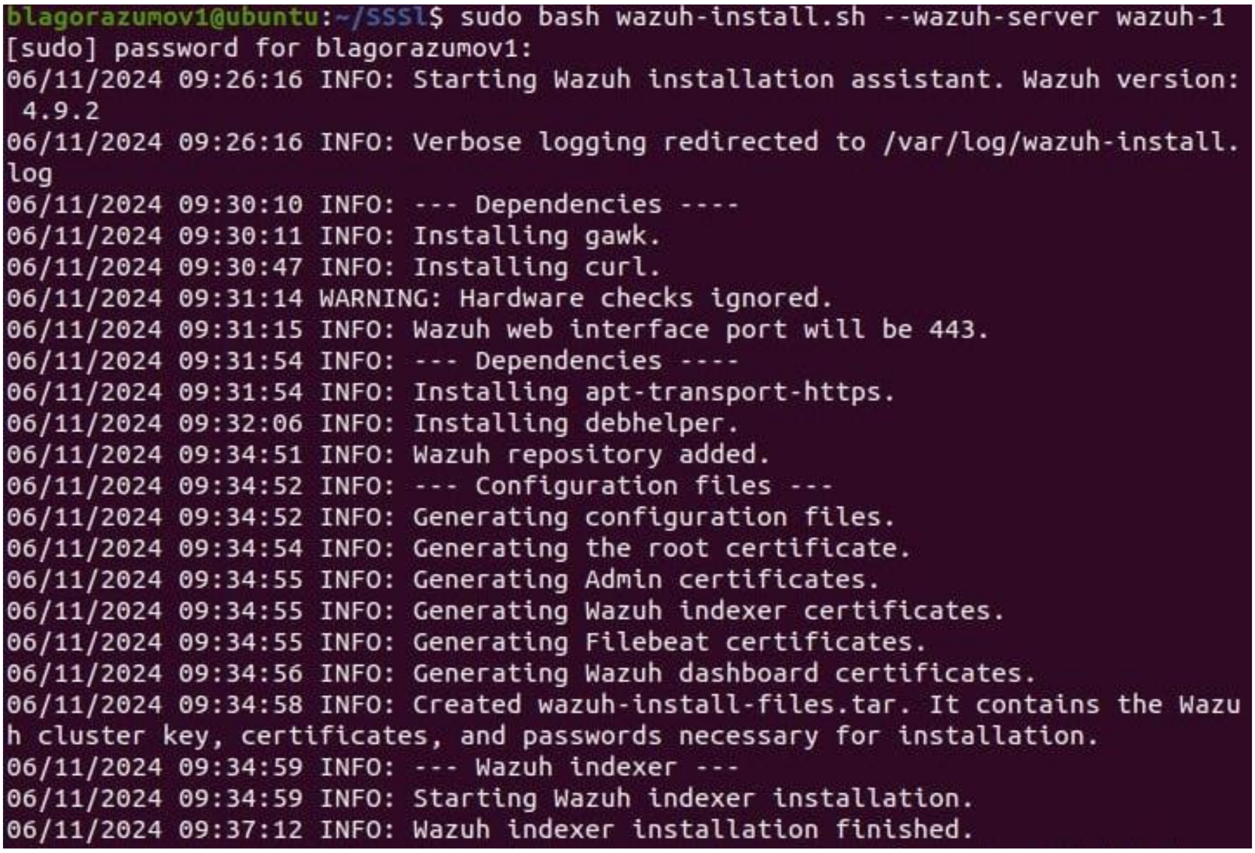


```
  GNU nano 4.8                     config.yml                           Modified
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "127.0.0.1"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "127.0.0.1"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "127.0.0.1"

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
```



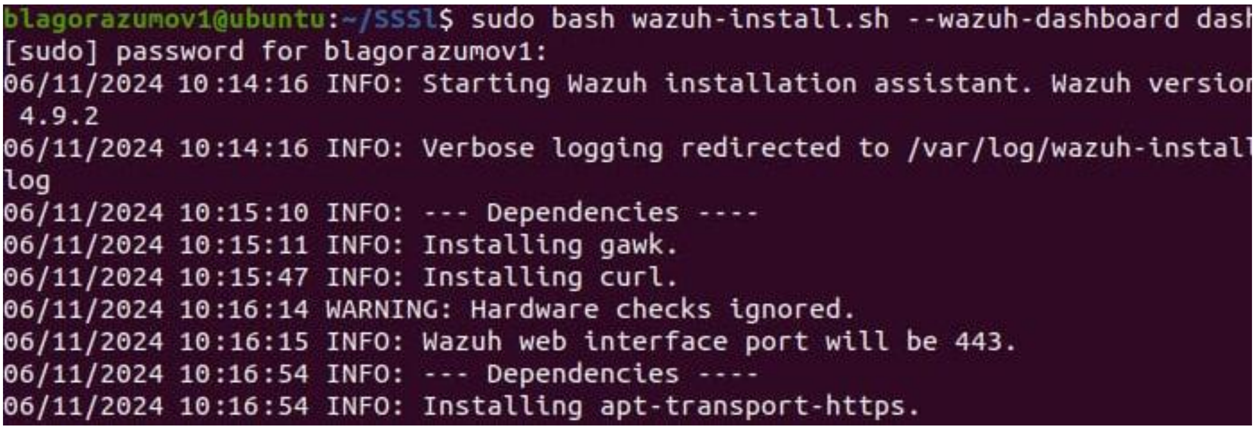
```
blagorazumov1@ubuntu:~/SSSl$ sudo bash wazuh-install.sh --start-cluster
24/11/2024 12:39:02 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.2
24/11/2024 12:39:02 INFO: Verbose logging redirected to /var/log/wazuh-install.log
24/11/2024 12:39:09 INFO: --- Dependencies ----
24/11/2024 12:39:09 INFO: Installing gawk.
24/11/2024 12:39:18 INFO: Verifying that your system meets the recommended minimum hardware requirements.
24/11/2024 12:39:26 INFO: Wazuh indexer cluster security configuration initialized.
24/11/2024 12:39:39 INFO: Updating the internal users.
24/11/2024 12:39:43 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
24/11/2024 12:39:58 INFO: --- Dependencies ----
24/11/2024 12:39:58 INFO: Removing gawk.
24/11/2024 12:40:04 INFO: Wazuh indexer cluster started.
blagorazumov1@ubuntu:~/SSSl$ sudo tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O |grep -P "\'admin\'" -A 1
  indexer_username: 'admin'
  indexer_password: '9F408U?GqIObKLaZx.*O..LPb7GQ3'
blagorazumov1@ubuntu:~/SSSl$ sudo curl -k -u admin:9F408U?GqIObKLaZx.*O..LPb7GQ3 https://192.168.50.131:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "N4enzEUYQNqowfoJZddZSQ",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "0aa3533d9a82a2a9acf03285cc47dfe264c5a15b",
    "build_date" : "2024-10-28T15:31:32.525674Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Установка wazuh-indexer и старт wazuh-cluster



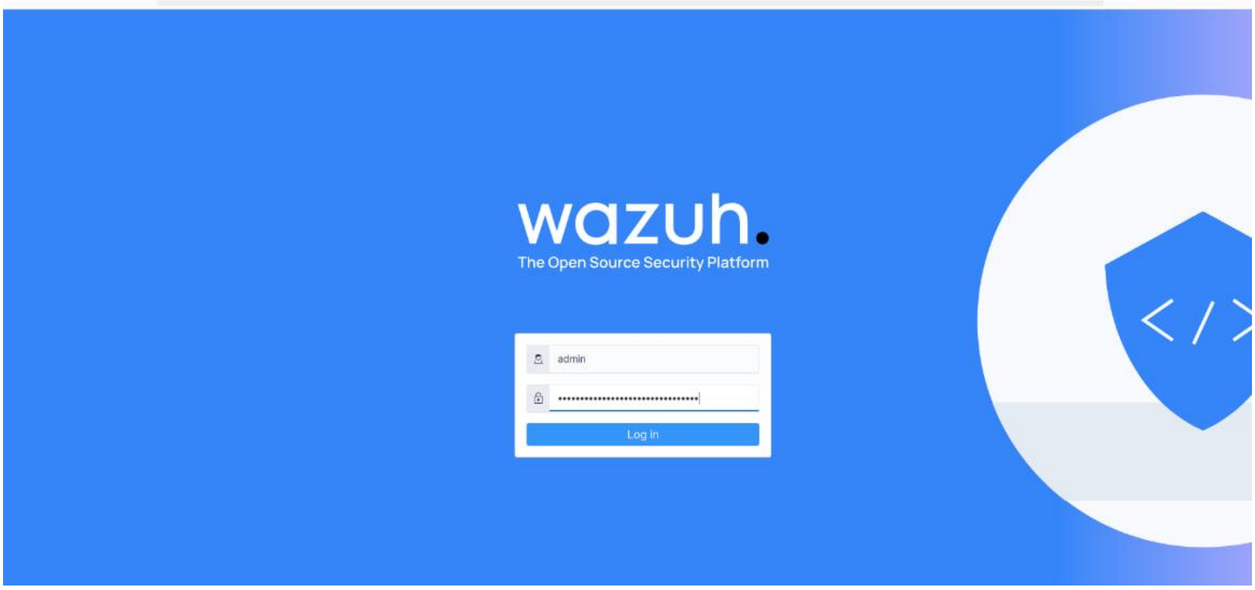
```
blagorazumov1@ubuntu:~/SSSl$ sudo bash wazuh-install.sh --wazuh-server wazuh-1
[sudo] password for blagorazumov1:
06/11/2024 09:26:16 INFO: Starting Wazuh installation assistant. Wazuh version:
 4.9.2
06/11/2024 09:26:16 INFO: Verbose logging redirected to /var/log/wazuh-install.
log
06/11/2024 09:30:10 INFO: --- Dependencies ----
06/11/2024 09:30:11 INFO: Installing gawk.
06/11/2024 09:30:47 INFO: Installing curl.
06/11/2024 09:31:14 WARNING: Hardware checks ignored.
06/11/2024 09:31:15 INFO: Wazuh web interface port will be 443.
06/11/2024 09:31:54 INFO: --- Dependencies ----
06/11/2024 09:31:54 INFO: Installing apt-transport-https.
06/11/2024 09:32:06 INFO: Installing debhelper.
06/11/2024 09:34:51 INFO: Wazuh repository added.
06/11/2024 09:34:52 INFO: --- Configuration files ---
06/11/2024 09:34:52 INFO: Generating configuration files.
06/11/2024 09:34:54 INFO: Generating the root certificate.
06/11/2024 09:34:55 INFO: Generating Admin certificates.
06/11/2024 09:34:55 INFO: Generating Wazuh indexer certificates.
06/11/2024 09:34:55 INFO: Generating Filebeat certificates.
06/11/2024 09:34:56 INFO: Generating Wazuh dashboard certificates.
06/11/2024 09:34:58 INFO: Created wazuh-install-files.tar. It contains the Wazu
h cluster key, certificates, and passwords necessary for installation.
06/11/2024 09:34:59 INFO: --- Wazuh indexer ---
06/11/2024 09:34:59 INFO: Starting Wazuh indexer installation.
06/11/2024 09:37:12 INFO: Wazuh indexer installation finished.
```

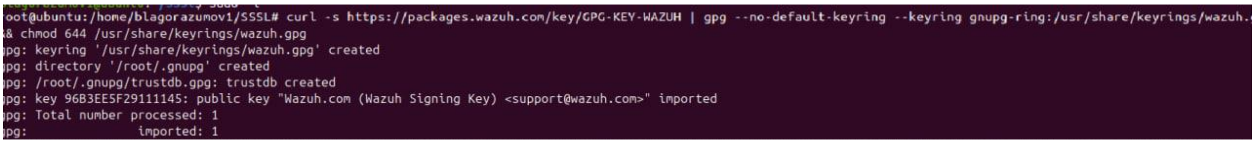
Установка wazuh-server



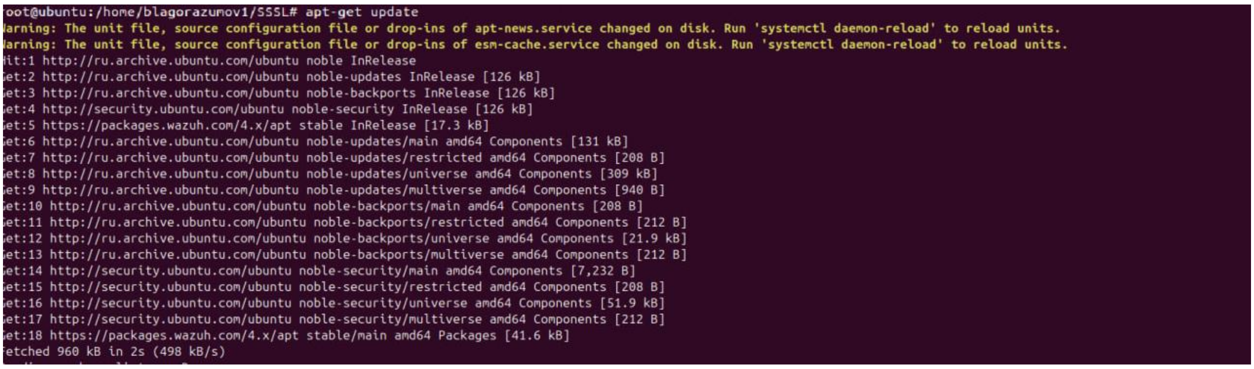
```
blagorazumov1@ubuntu:~/SSSl$ sudo bash wazuh-install.sh --wazuh-dashboard dash
[sudo] password for blagorazumov1:
06/11/2024 10:14:16 INFO: Starting Wazuh installation assistant. Wazuh versior
 4.9.2
06/11/2024 10:14:16 INFO: Verbose logging redirected to /var/log/wazuh-install
log
06/11/2024 10:15:10 INFO: --- Dependencies ----
06/11/2024 10:15:11 INFO: Installing gawk.
06/11/2024 10:15:47 INFO: Installing curl.
06/11/2024 10:16:14 WARNING: Hardware checks ignored.
06/11/2024 10:16:15 INFO: Wazuh web interface port will be 443.
06/11/2024 10:16:54 INFO: --- Dependencies ----
06/11/2024 10:16:54 INFO: Installing apt-transport-https.
```

Установка wazuh dashboard



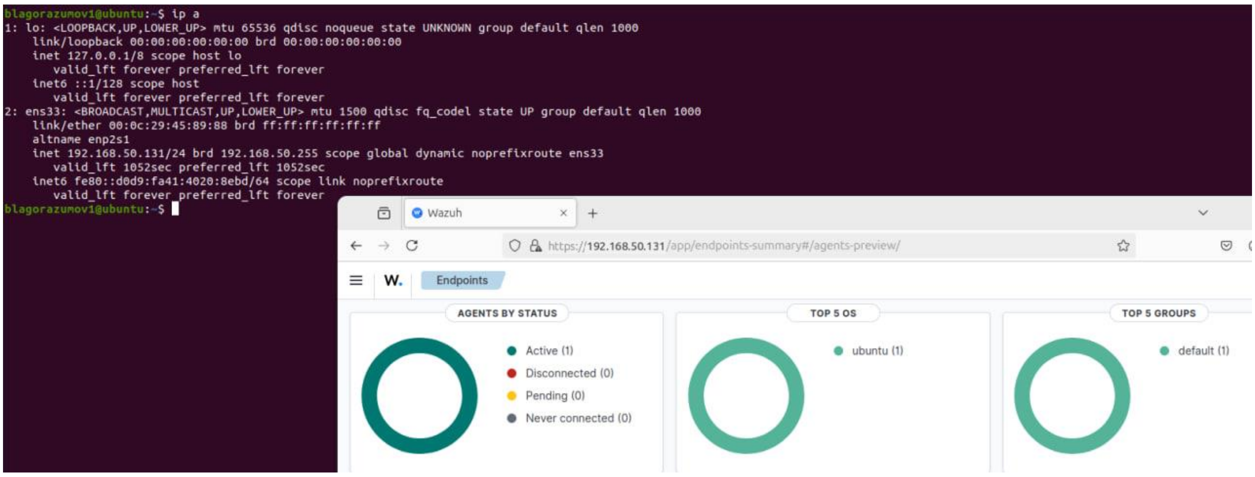


```
oot@ubuntu:/home/blagorazumov1/SSSL# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.
& chmod 644 /usr/share/keyrings/wazuh.gpg
pg: keyring '/usr/share/keyrings/wazuh.gpg' created
pg: directory '/root/.gnupg' created
pg: /root/.gnupg/trustdb.gpg: trustdb created
pg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
pg: Total number processed: 1
pg:               imported: 1
```



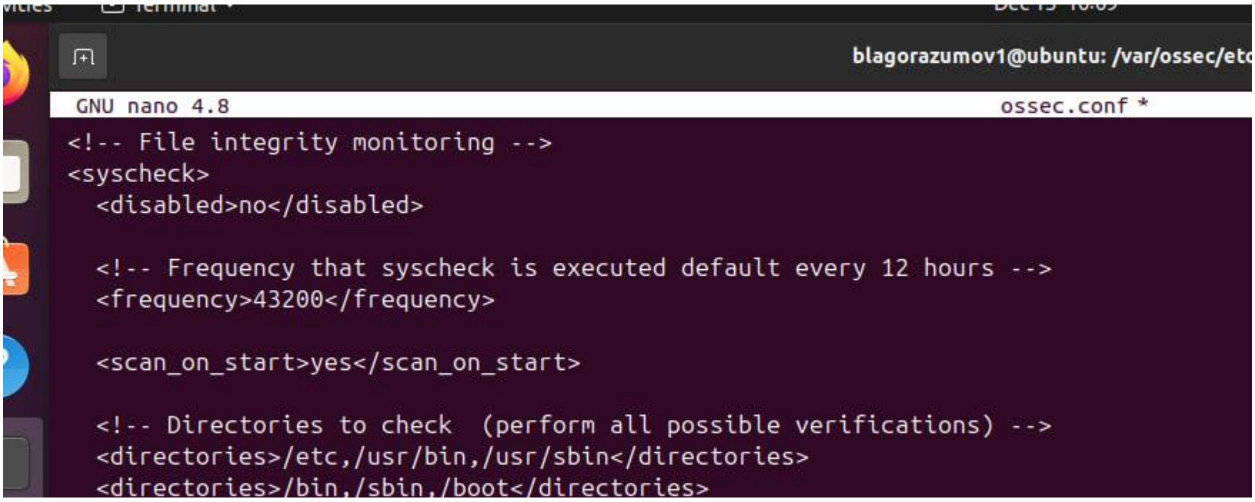
```
oot@ubuntu:/home/blagorazumov1/SSSL# apt-get update
arning: The unit file, source configuration file or drop-ins of apt-news.service changed on disk. Run 'systemctl daemon-reload' to reload units.
arning: The unit file, source configuration file or drop-ins of esm-cache.service changed on disk. Run 'systemctl daemon-reload' to reload units.
it:1 http://ru.archive.ubuntu.com/ubuntu noble InRelease
et:2 http://ru.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
et:3 http://ru.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
et:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
et:5 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
et:6 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [131 kB]
et:7 http://ru.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [208 B]
et:8 http://ru.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [309 kB]
et:9 http://ru.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
et:10 http://ru.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
et:11 http://ru.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
et:12 http://ru.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [21.9 kB]
et:13 http://ru.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
et:14 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7,232 B]
et:15 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [208 B]
et:16 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
et:17 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
et:18 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [41.6 kB]
etched 960 kB in 2s (498 kB/s)
```

Подключение агента по документации



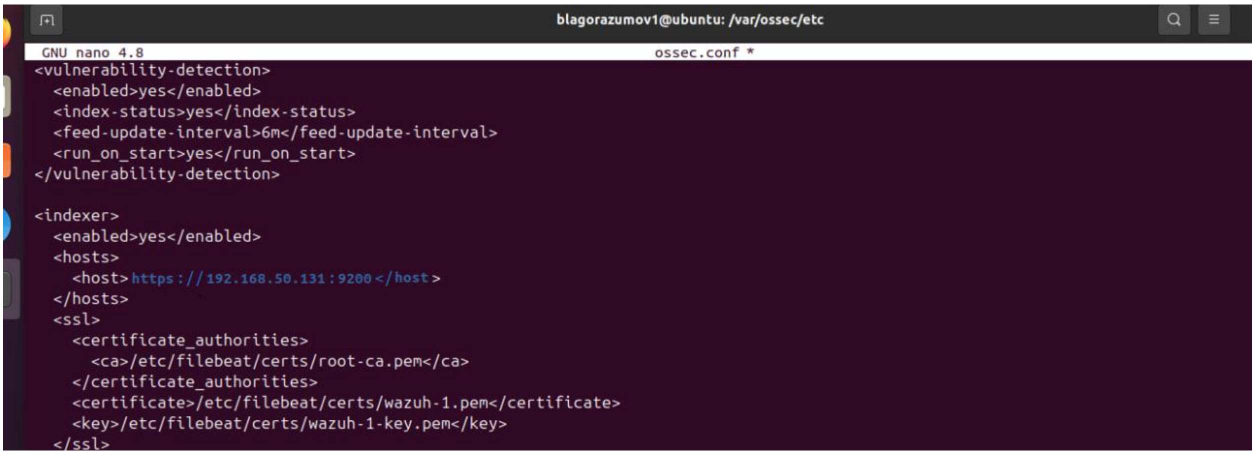
```
blagorazumov1@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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:29:45:89:88 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.50.131/24 brd 192.168.50.255 scope global dynamic noprefixroute ens33
       valid_lft 1052sec preferred_lft 1052sec
    inet6 fe80::d0d9:fa41:4020:8ebd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
blagorazumov1@ubuntu:~$
```

Демонстрация успешного подключения



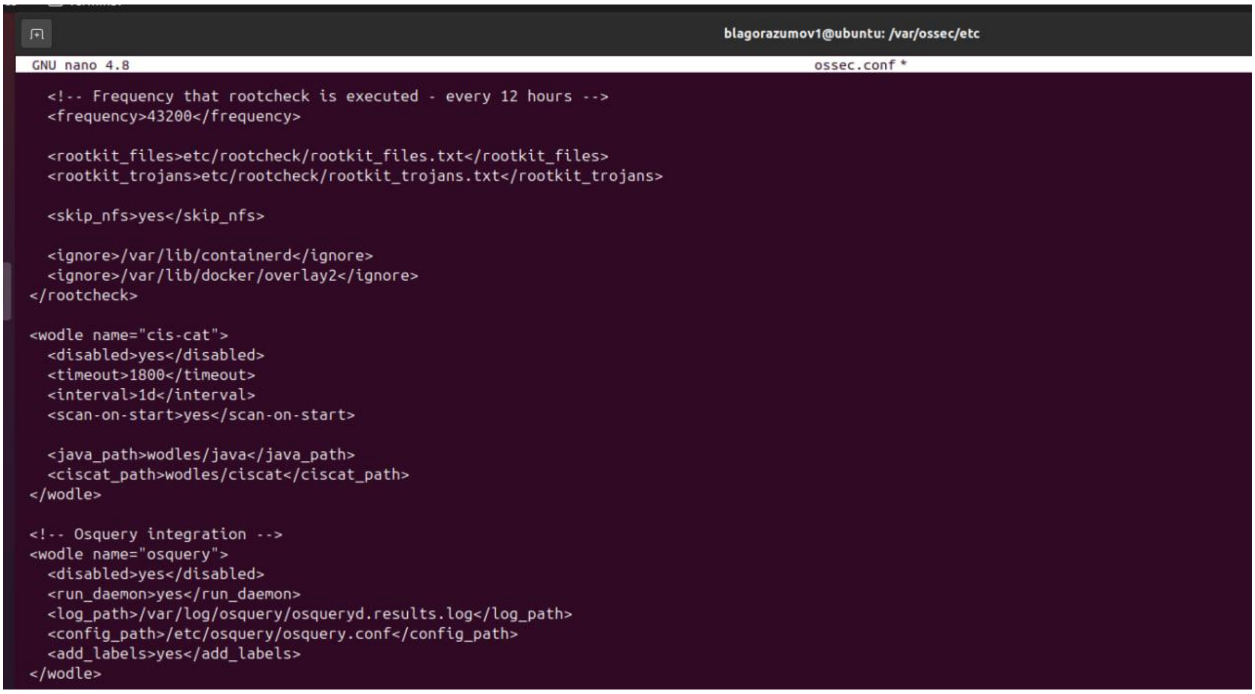
```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
```

Создаем проверку на целостность файлов



```
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>6m</feed-update-interval>
  <run_on_start>yes</run_on_start>
</vulnerability-detection>

<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://192.168.50.131:9200</host>
  </hosts>
  <ssl>
    <certificate_authorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/wazuh-1.pem</certificate>
    <key>/etc/filebeat/certs/wazuh-1-key.pem</key>
  </ssl>
```

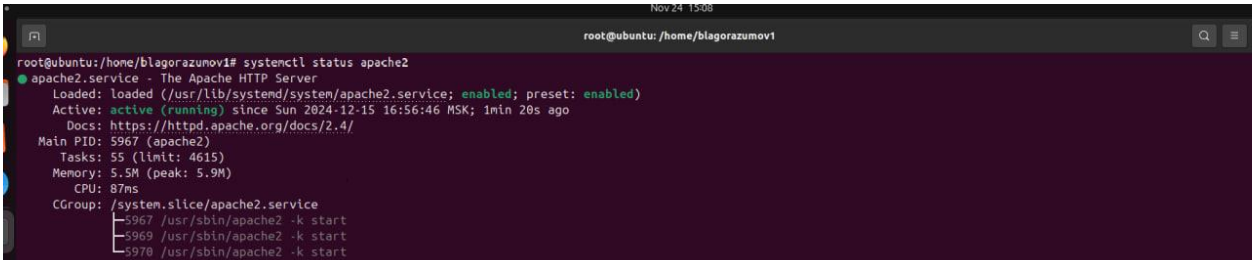
Приступаем к настройке выявления уязвимостей по документации



blagorazumov1@ubuntu: /var/ossec/etc

```
 GNU nano 4.8                                                    ossec.conf *
    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>

    <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

    <skip_nfs>yes</skip_nfs>

    <ignore>/var/lib/containerd</ignore>
    <ignore>/var/lib/docker/overlay2</ignore>
  </rootcheck>

  <wodle name="cis-cat">
    <disabled>yes</disabled>
    <timeout>1800</timeout>
    <interval>1d</interval>
    <scan-on-start>yes</scan-on-start>

    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>

  <!-- Osquery integration -->
  <wodle name="osquery">
    <disabled>yes</disabled>
    <run_daemon>yes</run_daemon>
    <log_path>/var/log/osquery/osqueryd.results.log</log_path>
    <config_path>/etc/osquery/osquery.conf</config_path>
    <add_labels>yes</add_labels>
  </wodle>
```

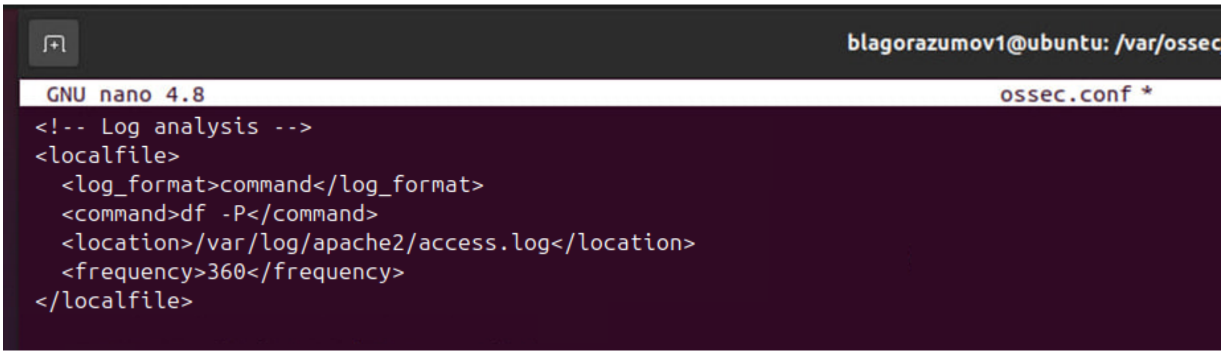
Настраиваем выявление руткитов\троянов и остальных скрытых процессов



Nov 24 15:08

root@ubuntu: /home/blagorazumov1

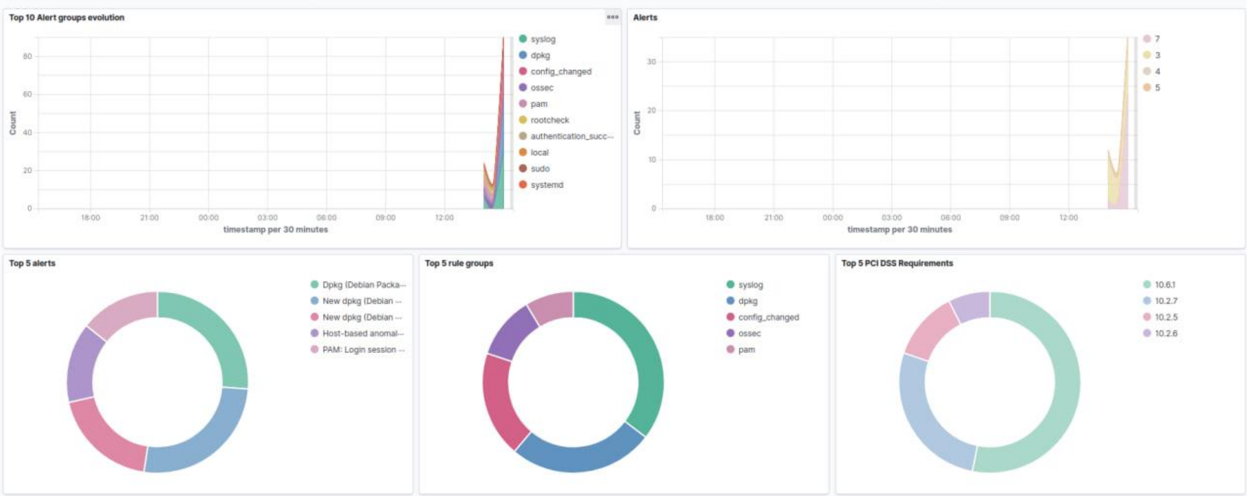
```
root@ubuntu:/home/blagorazumov1# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-12-15 16:56:46 MSK; 1min 20s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 5967 (apache2)
      Tasks: 55 (limit: 4615)
     Memory: 5.5M (peak: 5.9M)
        CPU: 87ms
     CGroup: /system.slice/apache2.service
             ├─5967 /usr/sbin/apache2 -k start
             ├─5969 /usr/sbin/apache2 -k start
             └─5970 /usr/sbin/apache2 -k start
```



blagorazumov1@ubuntu: /var/ossec

```
 GNU nano 4.8                                  ossec.conf *
 <!-- Log analysis -->
 <localfile>
   <log_format>command</log_format>
   <command>df -P</command>
   <location>/var/log/apache2/access.log</location>
   <frequency>360</frequency>
 </localfile>
```

Настраиваем выявление SQL-инъекций



Итоговая демонстрация панели срабатываний