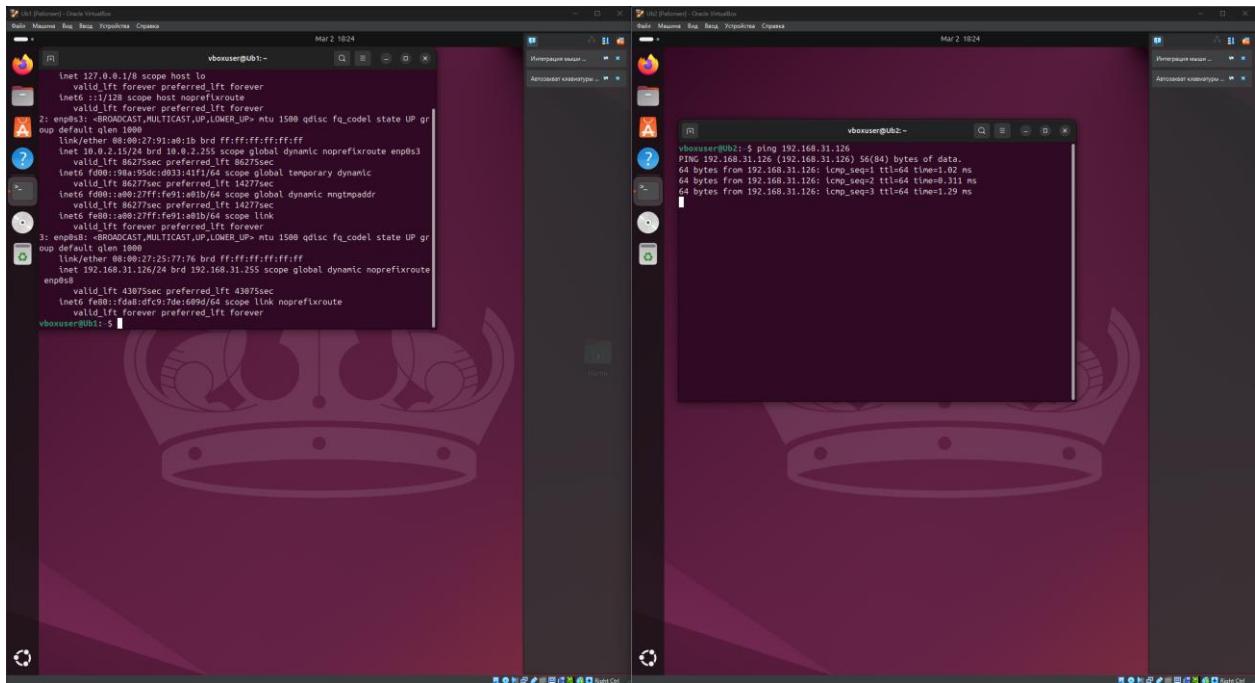


## Разворачиваем 2 ВМ и пингуем на проверку связи



## Инициализация wazuh на Ub1

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -o
```

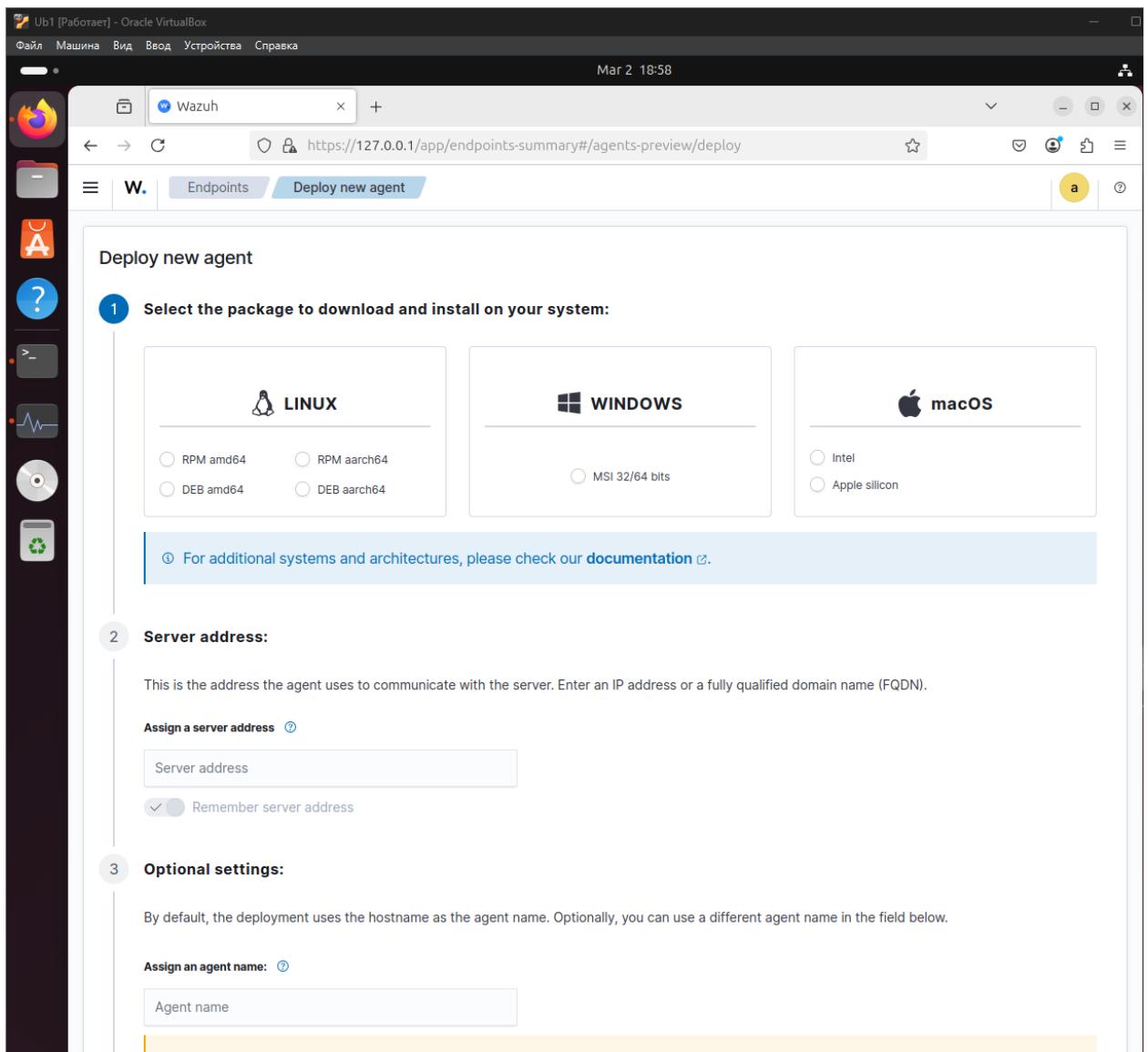
The screenshot shows a terminal window titled "vboxuser@Ub1: ~/Downloads" running on an Oracle VM VirtualBox instance of Ubuntu 22.04 LTS. The terminal displays the output of the command "sudo bash ./wazuh-install.sh -a -o". The log output is as follows:

```
vboxuser@Ub1:~/Downloads$ sudo bash ./wazuh-install.sh -a -o
02/03/2025 18:48:16 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.0 (x86_64/AMD64)
02/03/2025 18:48:16 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/03/2025 18:48:18 INFO: --- Removing existing Wazuh installation ---
02/03/2025 18:48:18 INFO: Removing Wazuh manager.
02/03/2025 18:48:25 INFO: Wazuh manager removed.
02/03/2025 18:48:25 INFO: Installation cleaned.
02/03/2025 18:48:25 INFO: Verifying that your system meets the recommended minimum hardware requirements.
02/03/2025 18:48:25 INFO: Wazuh web interface port will be 443.
02/03/2025 18:48:28 INFO: --- Dependencies ---
02/03/2025 18:48:28 INFO: Installing apt-transport-https.
02/03/2025 18:48:29 INFO: Installing debhelper.
02/03/2025 18:48:37 INFO: Wazuh repository added.
02/03/2025 18:48:38 INFO: --- Configuration files ---
02/03/2025 18:48:38 INFO: Generating configuration files.
02/03/2025 18:48:38 INFO: Generating the root certificate.
02/03/2025 18:48:38 INFO: Generating Admin certificates.
02/03/2025 18:48:38 INFO: Generating Wazuh indexer certificates.
02/03/2025 18:48:39 INFO: Generating Filebeat certificates.
02/03/2025 18:48:39 INFO: Generating Wazuh dashboard certificates.
02/03/2025 18:48:39 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
02/03/2025 18:48:39 INFO: --- Wazuh indexer ---
02/03/2025 18:48:39 INFO: Starting Wazuh indexer installation.
02/03/2025 18:50:11 INFO: Wazuh indexer installation finished.
02/03/2025 18:50:11 INFO: Wazuh indexer post-install configuration finished.
02/03/2025 18:50:11 INFO: Starting service wazuh-indexer.
02/03/2025 18:50:18 INFO: wazuh-indexer service started.
02/03/2025 18:50:18 INFO: Initializing Wazuh indexer cluster security settings.
02/03/2025 18:50:20 INFO: Wazuh indexer cluster security configuration initialized.
02/03/2025 18:50:20 INFO: Wazuh indexer cluster initialized.
02/03/2025 18:50:20 INFO: --- Wazuh server ---
02/03/2025 18:50:20 INFO: Starting the Wazuh manager installation.
02/03/2025 18:52:09 INFO: Wazuh manager installation finished.
```

### Разворачиваем дашборд и получаем креды

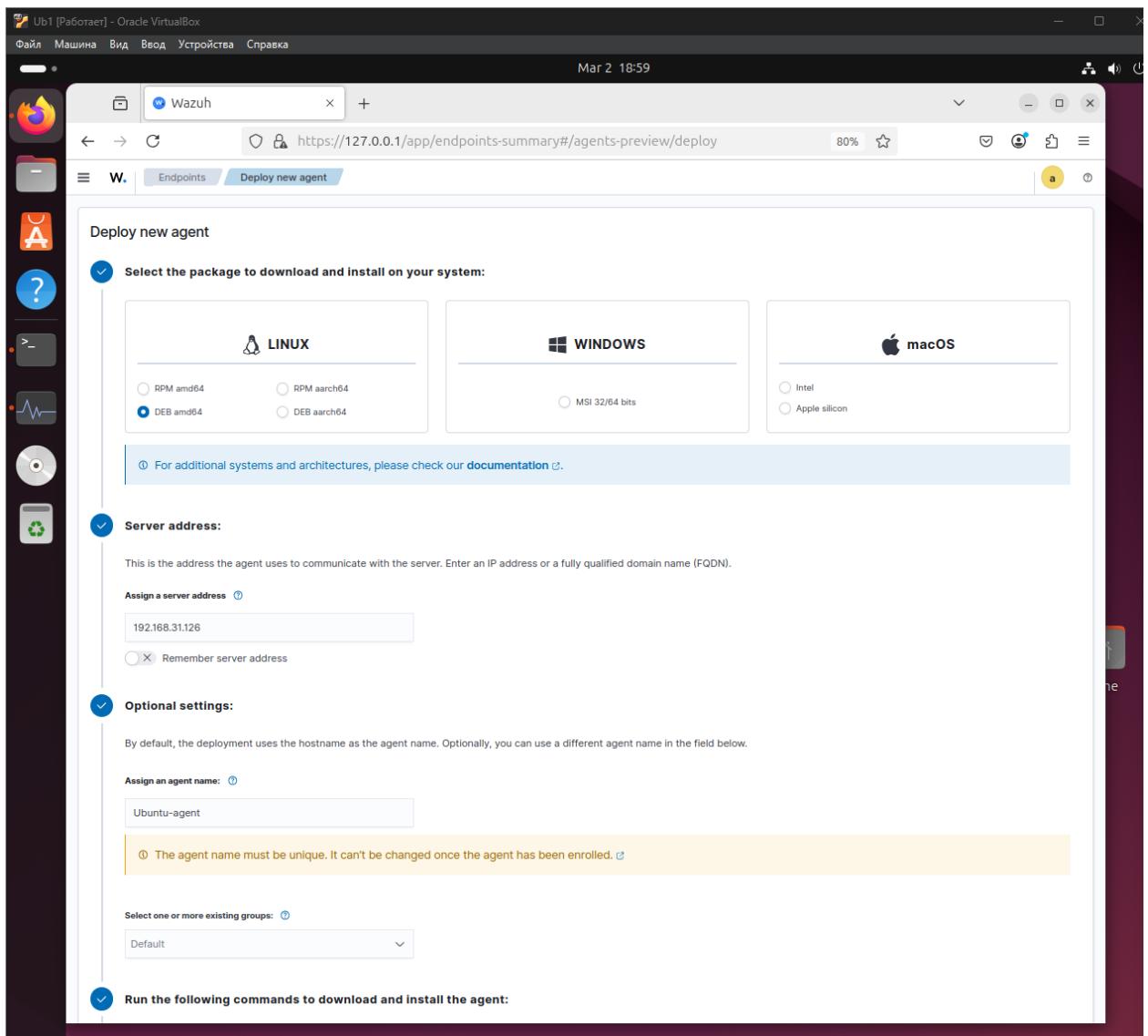
User: admin

Password: ?yjorfR4LTI7c5T8ZP4EokICuRAG?0EA



## Получаем пресет для агента

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.31.126' WAZUH_AGENT_NAME='Ubuntu-agent' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb
```



Устанавливаем агента по пресету

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.31.126' WAZUH_AGENT_NAME='Ubuntu-agent' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb
```

```

vboxuser@Ub2:~$ sudo wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.31.126' WAZUH_AGENT_NAME='Ubuntu-agent' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb
[sudo] password for vboxuser:
--2025-03-02 19:00:52-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 18.244.18.7, 18.244.18.42, 18.244.18.25, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.244.18.7|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11078824 (11M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.11.0-1_amd64.deb'

wazuh-agent_4.11.0- 100%[=====] 10.57M 9.43MB/s in 1.1s

2025-03-02 19:00:54 (9.43 MB/s) - 'wazuh-agent_4.11.0-1_amd64.deb' saved [11078824/11078824]

Selecting previously unselected package wazuh-agent.
(Reading database ... 149750 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.11.0-1_amd64.deb ...
Unpacking wazuh-agent (4.11.0-1) ...
Setting up wazuh-agent (4.11.0-1) ...
vboxuser@Ub2:~$
```

## Запускаем демона на агенте

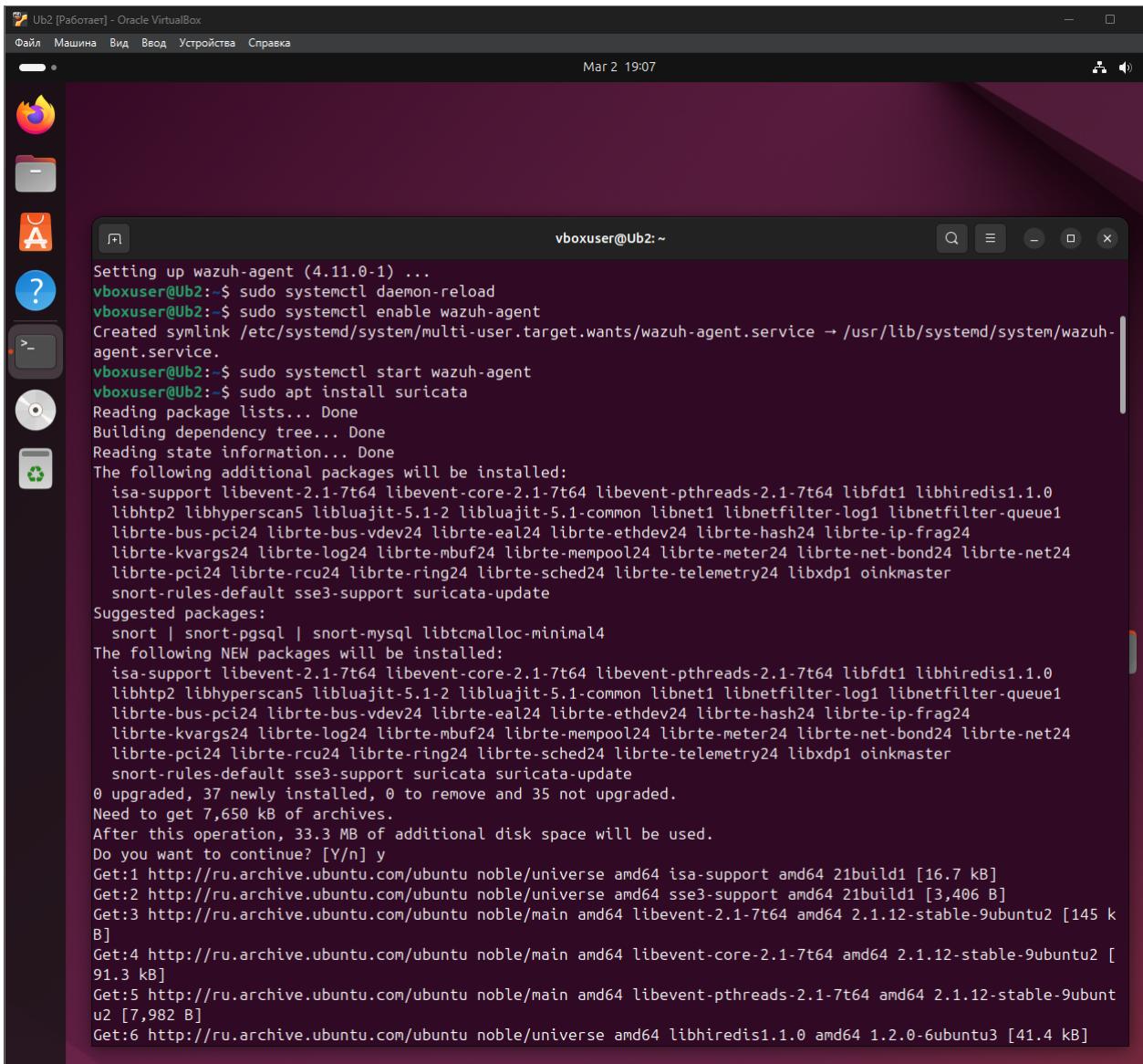
```

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

## И видим агента на сервере

## Устанавливаем suricata на агента

```
sudo apt install suricata
```



Ubuntu 20.04 LTS [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Mar 2 19:07

vboxuser@Ub2:~

```
Setting up wazuh-agent (4.11.0-1) ...
vboxuser@Ub2:~$ sudo systemctl daemon-reload
vboxuser@Ub2:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
vboxuser@Ub2:~$ sudo systemctl start wazuh-agent
vboxuser@Ub2:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
isa-support libevent-2.1-7t64 libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0
libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common libnet1 libnetfilter-log1 libnetfilter-queue1
librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24 librte-hash24 librte-ip-frag24
librte-kvargs24 librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24 librte-net24
librte-pci24 librte-rcu24 librte-ring24 librte-sched24 librte-telemetry24 libxdp1 oinkmaster
snort-rules-default sse3-support suricata-update
Suggested packages:
snort | snort-pgsql | snort-mysql libtcmalloc-minimal
The following NEW packages will be installed:
isa-support libevent-2.1-7t64 libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libfdt1 libhiredis1.1.0
libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common libnet1 libnetfilter-log1 libnetfilter-queue1
librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24 librte-hash24 librte-ip-frag24
librte-kvargs24 librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24 librte-net24
librte-pci24 librte-rcu24 librte-ring24 librte-sched24 librte-telemetry24 libxdp1 oinkmaster
snort-rules-default sse3-support suricata-update
0 upgraded, 37 newly installed, 0 to remove and 35 not upgraded.
Need to get 7,650 kB of archives.
After this operation, 38.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu noble/universe amd64 isa-support amd64 21build1 [16.7 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu noble/universe amd64 sse3-support amd64 21build1 [3,406 B]
Get:3 http://ru.archive.ubuntu.com/ubuntu noble/main amd64 libevent-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [145 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu noble/main amd64 libevent-core-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [91.3 kB]
Get:5 http://ru.archive.ubuntu.com/ubuntu noble/main amd64 libevent-pthreads-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [7,982 B]
Get:6 http://ru.archive.ubuntu.com/ubuntu noble/universe amd64 libhiredis1.1.0 amd64 1.2.0-6ubuntu3 [41.4 kB]
```

sudo suricata-update

vboxuser@Ub2:~\$ sudo suricata-update

```
2/3/2025 -- 19:08:54 - <Info> -- Using data-directory /var/lib/suricata.
2/3/2025 -- 19:08:54 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/3/2025 -- 19:08:54 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
2/3/2025 -- 19:08:54 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
2/3/2025 -- 19:08:54 - <Info> -- Loading /etc/suricata/suricata.yaml
2/3/2025 -- 19:08:54 - <Info> -- Disabling rules for protocol postgresql
2/3/2025 -- 19:08:54 - <Info> -- Disabling rules for protocol modbus
2/3/2025 -- 19:08:54 - <Info> -- Disabling rules for protocol dnp3
2/3/2025 -- 19:08:54 - <Info> -- Disabling rules for protocol enip
2/3/2025 -- 19:08:54 - <Info> -- No sources configured, will use Emerging Threats Open
2/3/2025 -- 19:08:54 - <Info> -- Fetching https://rules.emergin.../suricata-7.0.3/emerging.rules.t
ar.gz.
100% - 4792661/4792661
2/3/2025 -- 19:08:57 - <Info> -- Done.
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Ignoring file rules/emerging-deleted.rules
2/3/2025 -- 19:08:58 - <Info> -- Loaded 57156 rules.
2/3/2025 -- 19:08:58 - <Info> -- Disabled 14 rules.
2/3/2025 -- 19:08:58 - <Info> -- Enabled 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Modified 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Dropped 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Enabled 136 rules for flowbit dependencies.
2/3/2025 -- 19:08:58 - <Info> -- Backing up current rules.
```

## Запускаем suricata и проверяем статус – всё ок

sudo systemctl start suricata

sudo systemctl status suricata

Ubuntu 22.04 LTS (Ubuntu 22.04 LTS) [Работает] - Oracle VM VirtualBox

Файл Машинка Вид Ввод Устройства Справка

Mar 2 19:10

```
vboxuser@Ub2:~
```

```
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
2/3/2025 -- 19:08:57 - <Info> -- Ignoring file rules/emerging-deleted.rules
2/3/2025 -- 19:08:58 - <Info> -- Loaded 57156 rules.
2/3/2025 -- 19:08:58 - <Info> -- Disabled 14 rules.
2/3/2025 -- 19:08:58 - <Info> -- Enabled 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Modified 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Dropped 0 rules.
2/3/2025 -- 19:08:58 - <Info> -- Enabled 136 rules for flowbit dependencies.
2/3/2025 -- 19:08:58 - <Info> -- Backing up current rules.
2/3/2025 -- 19:08:58 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 57156; enabled: 42828; added: 57156; removed: 0; modified: 0
2/3/2025 -- 19:08:58 - <Info> -- Writing /var/lib/suricata/rules/classification.config
2/3/2025 -- 19:08:58 - <Info> -- Testing with suricata -T.
2/3/2025 -- 19:09:13 - <Info> -- Done.
vboxuser@Ub2:~$ sudo systemctl start suricata
vboxuser@Ub2:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-03-02 19:10:26 UTC; 9s ago
    Docs: man:suricata(8)
           man:suricatas(8)
           https://suricata.io/documentation/
   Process: 8246 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suri...
 Main PID: 8249 (Suricata-Main)
   Tasks: 1 (limit: 14034)
  Memory: 264.5M (peak: 264.6M)
    CPU: 9.103s
   CGroup: /system.slice/suricata.service
           └─8249 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Mar 02 19:10:26 Ub2 systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Mar 02 19:10:26 Ub2 suricata[8246]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Mar 02 19:10:26 Ub2 suricata[8246]: W: ioctl: Failure when trying to get MTU via ioctl for 'eth0': No such device
Mar 02 19:10:26 Ub2 systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

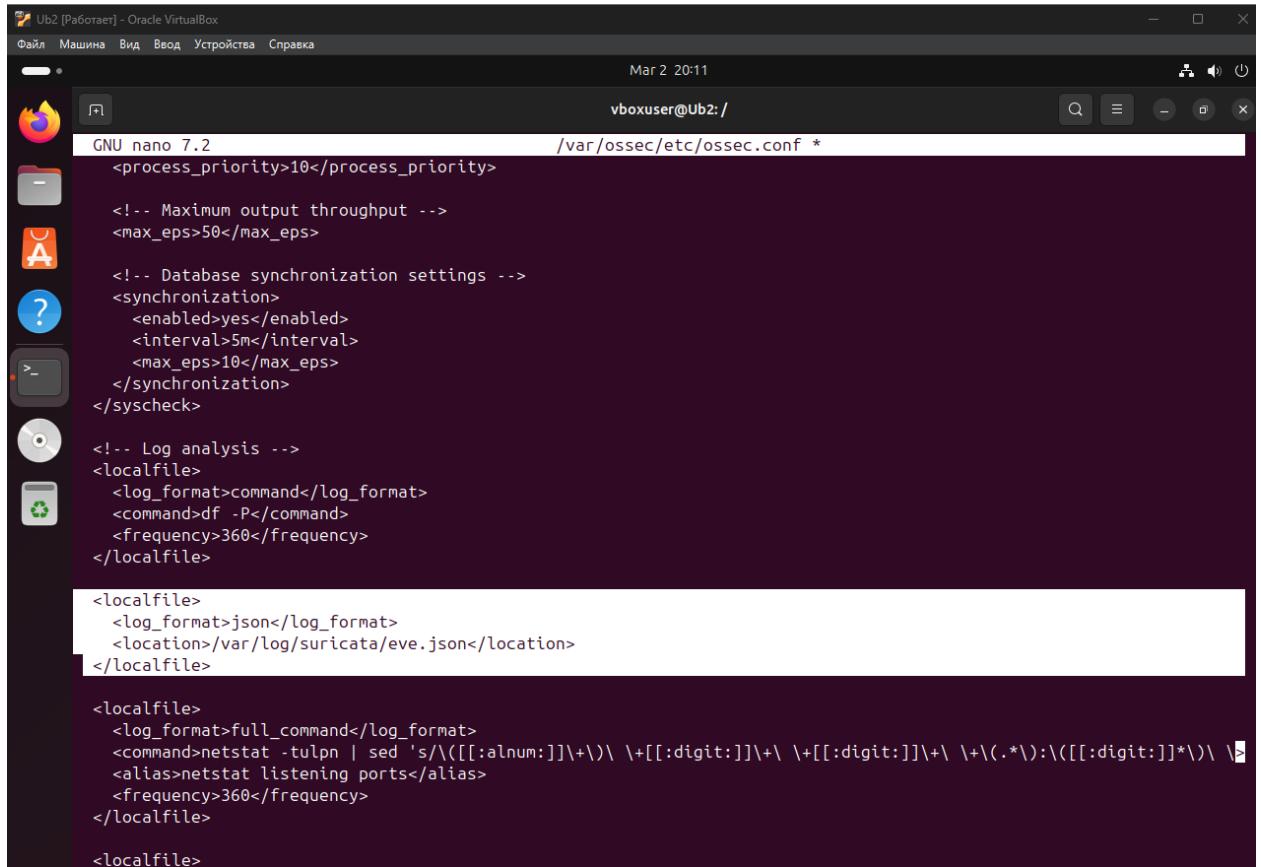
lines 1-18/18 (END)

## Добавляем логи к сурикате

```
sudo nano /var/ossec/etc/ossec.conf
```

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

</localfile>

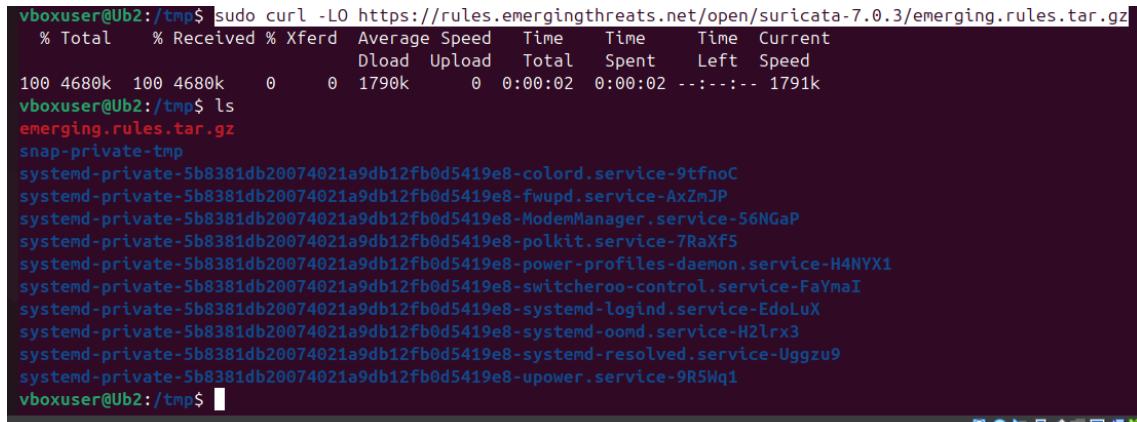


```
GNU nano 7.2          vboxuser@Ub2:/var/ossec/etc/ossec.conf *  
<process_priority>10</process_priority>  
  
<!-- Maximum output throughput -->  
<max_eps>50</max_eps>  
  
<!-- Database synchronization settings -->  
<synchronization>  
  <enabled>yes</enabled>  
  <interval>5m</interval>  
  <max_eps>10</max_eps>  
</synchronization>  
</syscheck>  
  
<!-- Log analysis -->  
<localfile>  
  <log_format>command</log_format>  
  <command>df -P</command>  
  <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>netstat -tulpn | sed 's/([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(\.\*\):\(\[[[:digit:]]*\)\) \>  
  <alias>netstat listening ports</alias>  
  <frequency>360</frequency>  
</localfile>  
  
<localfile>
```

### Скачиваем рулы для сурикаты

```
cd /tmp/
```

```
sudo curl -LO https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz
```



```
vboxuser@Ub2:/tmp$ sudo curl -LO https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz  
% Total    % Received % Xferd  Average Speed   Time   Time     Current  
          Dload  Upload Total Spent   Left Speed  
100 4680k  100 4680k    0      0  1790k      0  0:00:02  0:00:02  ---:-- 1791k  
vboxuser@Ub2:/tmp$ ls  
emerging.rules.tar.gz  
snap-private-tmp  
systemd-private-5b8381db20074021a9db12fb0d5419e8-colord.service-9tfnoC  
systemd-private-5b8381db20074021a9db12fb0d5419e8-fwupd.service-AxZmJP  
systemd-private-5b8381db20074021a9db12fb0d5419e8-ModemManager.service-56NGaP  
systemd-private-5b8381db20074021a9db12fb0d5419e8-polkit.service-7RaXf5  
systemd-private-5b8381db20074021a9db12fb0d5419e8-power-profiles-daemon.service-H4NYX1  
systemd-private-5b8381db20074021a9db12fb0d5419e8-switcheroo-control.service-FaYmaI  
systemd-private-5b8381db20074021a9db12fb0d5419e8-systemd-logind.service-EdoLuX  
systemd-private-5b8381db20074021a9db12fb0d5419e8-systemd-oomd.service-H2lrx3  
systemd-private-5b8381db20074021a9db12fb0d5419e8-systemd-resolved.service-Uggzu9  
systemd-private-5b8381db20074021a9db12fb0d5419e8-upower.service-9R5Wq1  
vboxuser@Ub2:/tmp$
```

### Разорхивируем их

```
sudo tar -xvf emerging.rules.tar.gz
```

vboxuser@Ub2 [Работает] - Oracle VirtualBox

Файл Машинка Вид Ввод Устройства Справка

Mar 2 20:22

vboxuser@Ub2:/tmp\$ sudo tar -xvf emerging.rules.tar.gz

rules/  
rules/BSD-License.txt  
rules/LICENSE  
rules/botcc.portgrouped.rules  
rules/botcc.rules  
rules/ciarmy.rules  
rules/classification.config  
rules/compromised-ips.txt  
rules/compromised.rules  
rules/drop.rules  
rules/dshield.rules  
rules/emerging-activex.rules  
rules/emerging-adware\_pup.rules  
rules/emerging-attack\_response.rules  
rules/emerging-chat.rules  
rules/emerging-coinminer.rules  
rules/emerging-current\_events.rules  
rules/emerging-deleted.rules  
rules/emerging-dns.rules  
rules/emerging-dos.rules  
rules/emerging-dyn\_dns.rules  
rules/emerging-exploit.rules  
rules/emerging-exploit\_kit.rules  
rules/emerging-file\_sharing.rules  
rules/emerging-ftp.rules  
rules/emerging-games.rules  
rules/emerging-hunting.rules  
rules/emerging-icmp.rules  
rules/emerging-imap.rules  
rules/emerging-inappropriate.rules  
rules/emerging-info.rules  
rules/emerging-ja3.rules  
rules/emerging-malware.rules  
rules/emerging-misc.rules  
rules/emerging-mobile\_malware.rules  
rules/emerging-netbios.rules  
rules/emerging-p2p.rules  
rules/emerging-phishing.rules  
rules/emerging-pop3.rules  
rules/emerging-remote\_access.rules  
rules/emerging-retired.rules  
rules/emerging-rpc.rules  
rules/emerging-scada.rules  
rules/emerging-scan.rules  
rules/emerging-shellcode.rules  
rules/emerging-smtp.rules  
rules/emerging-snmp.rules  
rules/emerging-sql.rules  
rules/emerging-ta\_abused\_services.rules  
rules/emerging-telnet.rules  
rules/emerging-tftp.rules  
rules/emerging-user\_agents.rules  
rules/emerging-voip.rules  
rules/emerging-web\_client.rules  
rules/emerging-web\_server.rules

**Перемещение правил в /etc/suricata/rules/**

`sudo mv rules/*.rules /etc/suricata/rules/`

+ проверка

`cd /etc/suricata/rules/`

ls

```
vboxuser@Ub2:/tmp$ sudo mv rules/*.rules /etc/suricata/rules/
vboxuser@Ub2:/tmp$ cd /etc/suricata/rules/
vboxuser@Ub2:/etc/suricata/rules$ ls
app-layer-events.rules      emerging-hunting.rules      emerging-voip.rules
botcc.portgrouped.rules     emerging-icmp.rules      emerging-web_client.rules
botcc.rules                 emerging-imap.rules      emerging-web_server.rules
clarmy.rules                emerging-inappropriate.rules emerging-web_specific_apps.rules
compromised.rules           emerging-info.rules      emerging-worm.rules
decoder-events.rules         emerging-ja3.rules      files.rules
dhcp-events.rules           emerging-malware.rules   ftp-events.rules
dnsp3-events.rules          emerging-misc.rules      http2-events.rules
dns-events.rules            emerging-mobile_malware.rules http-events.rules
drop.rules                  emerging-netbios.rules   ipsec-events.rules
dshield.rules               emerging-p2p.rules      kerberos-events.rules
emerging-activex.rules      emerging-phishing.rules modbus-events.rules
emerging-adware_pup.rules    emerging-pop3.rules    mqtt-events.rules
emerging-attack_response.rules emerging-remote_access.rules nfs-events.rules
emerging-chat.rules          emerging-retired.rules  ntp-events.rules
emerging-coinminer.rules     emerging-rpc.rules      quic-events.rules
emerging-current_events.rules emerging-scada.rules   rfb-events.rules
emerging-deleted.rules       emerging-scan.rules    smb-events.rules
emerging-dns.rules           emerging-shellcode.rules smtp-events.rules
emerging-dos.rules           emerging-smtp.rules    ssh-events.rules
emerging-dyn_dns.rules       emerging-snmp.rules    stream-events.rules
emerging-exploit_kit.rules   emerging-sql.rules     threatview_CS_c2.rules
emerging-exploit.rules       emerging-ta_abused_services.rules tls-events.rules
emerging-file_sharing.rules  emerging-telnet.rules   tor.rules
emerging-ftp.rules           emerging-tftp.rules
emerging-ames.rules
vboxuser@Ub2:/etc/suricata/rules$
```

## Выдача прав рулам

sudo chmod 640 /etc/suricata/rules/\*.rules

```
vboxuser@Ub2:/etc/suricata/rules$ sudo chmod 640 /etc/suricata/rules/*.rules
vboxuser@Ub2:/etc/suricata/rules$
```

## Правим yaml сурикаты

sudo nano /etc/suricata/suricata.yaml

Ub2 [Работает] - Oracle VirtualBox

Файл Машина Вид Ввод Устройства Справка Mar 2 20:46

vboxuser@Ub2: /var/log/suricata

vboxuser@Ub2: /var/log/suricata

vboxuser@Ub2: /etc/suricata/suricata.yaml \*

```
GNU nano 7.2 /etc/suricata/suricata.yaml *
#level: Info ## possible levels: Emergency, Alert, Critical,
## Error, Warning, Notice, Info, Debug
#ethernet: no # log ethernet header in events when available
#redis:
#   server: 127.0.0.1
#   port: 6379
#   async: true ## if redis replies are read asynchronously
#   mode: list ## possible values: list/lpush (default), rpush, channel/publish
#   #
## lpush and rpush are using a Redis list. "list" is an alias for
## publish is using a Redis channel. "channel" is an alias for pu
#   key: suricata ## key or channel to use (default to suricata)
# Redis pipelining set up. This will enable to only do a query every
# 'batch-size' events. This should lower the latency induced by network
# connection at the cost of some memory. There is no flushing implemented
# so this setting should be reserved to high traffic Suricata deployments.
#   pipelining:
#     enabled: yes ## set enable to yes to enable query pipelining
#     batch-size: 10 ## number of entries to keep in buffer

# Include top level metadata. Default yes.
#metadata: no

# include the name of the input pcap file in pcap file processing mode
pcap-file: false

# Community Flow ID
# Adds a 'community_id' field to EVE records. These are meant to give
# records a predictable flow ID that can be used to match records to
# output of other tools such as Zeek (Bro).
#
# Takes a 'seed' that needs to be same across sensors and tools
# to make the id less predictable.

# enable/disable the community id feature.
community-id: true
# Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0

# HTTP X-Forwarded-For support by adding an extra field or overwriting
# the source or destination IP address (depending on flow direction)
```

```
vboxuser@Ub2:/etc/suricata/rules          x          vboxuser@Ub2:/etc/suricata/rules          x          ~
GNU nano 7.2                               /etc/suricata/suricata.yaml *
%YAML 1.1
---
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.31.76]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[HTTP_PORTS,110,143]"
    FTP_PORTS: 21
    GENEVE_PORTS: 6081

^G Help      ^O Write Out     ^W Where Is      ^K Cut      ^T Execute      ^C Location      M-U Undo
^X Exit      ^R Read File     ^\ Replace      ^U Paste      ^J Justify      ^/ Go To Line    M-E Redo
```

как видно на этом скриншоте я неправильно указал интерфейс добавив в конце S делая скрин... (

```
vboxuser@Ub2: /etc/suricata/rules
vboxuser@Ub2: /etc/suricata/rules
GNU nano 7.2 /etc/suricata/suricata.yaml *

# Requires libunwind to be available when Suricata is configured and built.
# If a signal unexpectedly terminates Suricata, displays a brief diagnostic
# message with the offending stacktrace if enabled.
#stacktrace-on-signal: on

# Define your logging outputs. If none are defined, or they are all
# disabled you will get the default: console output.
outputs:
- console:
    enabled: yes
    # type: json
- file:
    enabled: yes
    level: info
    filename: suricata.log
    # format: "[%i - %m] %z %d: %S: %M"
    # type: json
- syslog:
    enabled: no
    facility: local5
    format: "[%i] <%d> -- "
    # type: json

## Step 3: Configure common capture settings
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##

# Linux high speed capture support
af-packet:
- interface: enp0s8S
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
```

### Рестарт сурикаты

```
sudo systemctl restart suricata
```

```
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl restart suricata
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-03-02 20:34:44 UTC; 4s ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
  Process: 12986 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid
 Main PID: 12989 (Suricata-Main)
    Tasks: 1 (limit: 14034)
   Memory: 173.7M (peak: 173.7M)
      CPU: 4.088s
     CGroup: /system.slice/suricata.service
             └─12989 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Failed with result 'exit-code'.
Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Consumed 17.155s CPU time.
Mar 02 20:34:44 Ub2 systemd[1]: suricata.service: Scheduled restart job, restart counter is at 1.
Mar 02 20:34:44 Ub2 systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Mar 02 20:34:44 Ub2 suricata[12986]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Mar 02 20:34:44 Ub2 suricata[12986]: W: ioctl: Failure when trying to get MTU via ioctl for 'enp0s8S': No such device
Mar 02 20:34:44 Ub2 systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-21/21 (END)
```

### Перезапуск wazuh-agent

```
sudo systemctl restart wazuh-agent
```

```
vboxuser@Ub2:/etc/suricata/rules$ sudo systemctl restart wazuh-agent
vboxuser@Ub2:/etc/suricata/rules$
```

### Пингуем агента и получаем события от суриката

Ubuntu [Работает] - Oracle VirtualBox

Файл Машина Вид Ввод Устройства Справка

Discover - Wazuh Discover - Wazuh Mar 2 20:53

Wazuh Discover

Discover - Wazuh https://127.0.0.1/app/data-explorer/discover#?\_a=(discover:(columns:!(\_source),isDirty:!f,sort:\_score,order:desc))&\_index=wazuh-alerts-\*&\_source=\_source&\_size=100

New Save Open Share Reporting Inspect

wazuh-alerts-\*

Selected fields

- \_index
- agent.id
- agent.ip
- agent.name
- data.arch
- data.command
- data.dpkg\_status
- data.dsuser
- data.extra\_data
- data.id
- data.package
- data.pwd
- data.srcuser
- data.status
- data.timestamp
- data.tty
- data.uid
- data.version
- decoder.ftcomment
- decoder.name
- decoder.parent
- full\_log
- id
- input.type
- location
- manager.name
- predecoder.hostname
- predecoder.program\_name
- predecoder.timestamp
- rule.description
- rule.firetimes
- rule.gdpr
- rule.gpg13
- rule.groups
- rule.hipaa

Expanded document

Table JSON

↳	_index
	wazuh-alerts-4.x-2025.03.02
↳	agent.id
	001
↳	agent.ip
	192.168.31.76
↳	agent.name
	Ubuntu-agent
↳	data.alert.action
	allowed
↳	data.alert.category
	Misc activity
↳	data.alert.gid
	1
↳	data.alert.metadata.confidence
	Medium
↳	data.alert.metadata.created_at
	2010-09-23
↳	data.alert.metadata.signature_severity
	Informational
↳	data.alert.metadata.updated_at
	2019-07-26
↳	data.alert.rev
	8
↳	data.alert.severity
	3
↳	data.alert.signature
	GPL ICMP PING *NIX
↳	data.alert.signature_id
	2100366
↳	data.community_id
	1:RhCjXNbKzhV+Ur5JE08GIdfPJQ=
↳	data.dest_ip
	192.168.31.76
↳	data.dest_port
	8
↳	data.direction
	to_server
↳	data.event_type
	alert
↳	data.flow.bytes_toclient
	1078
↳	data.flow.bytes_toserver
	1176
↳	data.flow.dest_ip
	192.168.31.76
↳	data.flow.pkts_toclient
	11

View surrounding documents View single document

The screenshot shows the Wazuh Data Explorer interface within an Oracle VirtualBox window titled 'Ub1 [Работает] - Oracle VirtualBox'. The main window displays a list of discovered fields under the 'Discover' tab. The left sidebar contains a navigation tree with sections like 'wazuh-alerts-\*', 'Selected fields', and 'Available fields'. The right pane lists the discovered fields with their types and values. A status bar at the bottom indicates 'Mar 2 20:53'.

Field	Type	Value
data.flow.bytes_toclient	number	1078
data.flow.bytes_toserver	number	1176
data.flow.dest_ip	string	192.168.31.76
data.flow.pkts_toclient	number	11
data.flow.pkts_toserver	number	12
data.flow.src_ip	string	192.168.31.126
data.flow.start	date	2025-03-02T20:50:30.691559+0000
data.flow_id	number	1844327657444973.000000
data.icmp_code	number	0
data.icmp_type	number	8
data.in_iface	string	enp0s8
data.pkt_src	string	wire/pcap
data.proto	string	ICMP
data.src_ip	string	192.168.31.126
data.src_port	number	0
data.timestamp	date	Mar 2, 2025 @ 20:50:41.890
t_decoder.name	string	json
t_id	number	1740948641.214933
t_input.type	string	log
t_location	string	/var/log/suricata/eve.json
t_manager.name	string	ub1
t_rule.description	string	Suricata: Alert - GPL ICMP PING +NIX
# rule.firedtimes	number	12
t_rule.groups	string	ids, suricata
t_rule.id	number	86601
# rule.level	number	3
t_rule.mail	boolean	false
timestamp	date	Mar 2, 2025 @ 20:50:41.556

## Установка yara

```
sudo apt install -y make gcc autoconf libtool libssl-dev pkg-config
```

```
sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
```

Ub2 [Работает] - Oracle VirtualBox

Файл Машина Вид Ввод Устройства Справка

Mar 2 21:03

vboxuser@Ub2: /var/log/suricata

(Reading database ... 150659 files and directories currently installed.)

Preparing to unpack .../00-m4\_1.4.19-4build1\_amd64.deb ...

Unpacking m4 (1.4.19-4build1) ...

Selecting previously unselected package autoconf.

Preparing to unpack .../01-autoconf\_2.71-3\_all.deb ...

Unpacking autoconf (2.71-3) ...

Selecting previously unselected package autotools-dev.

Preparing to unpack .../02-autotools-dev\_20220109.1\_all.deb ...

Unpacking autotools-dev (20220109.1) ...

Selecting previously unselected package automake.

Preparing to unpack .../03-automake\_1%3a1.16.5-1.3ubuntu1\_all.deb ...

Unpacking automake (1:1.16.5-1.3ubuntu1) ...

Selecting previously unselected package libltdl-dev:amd64.

Preparing to unpack .../04-libltdl-dev\_2.4.7-7build1\_amd64.deb ...

Unpacking libltdl-dev:amd64 (2.4.7-7build1) ...

Selecting previously unselected package libpkgconf3:amd64.

Preparing to unpack .../05-libpkgconf3\_1.8.1-2build1\_amd64.deb ...

Unpacking libpkgconf3:amd64 (1.8.1-2build1) ...

Selecting previously unselected package libssl-dev:amd64.

Preparing to unpack .../06-libssl-dev\_3.0.13-0ubuntu3.5\_amd64.deb ...

Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...

Selecting previously unselected package libtool.

Preparing to unpack .../07-libtool\_2.4.7-7build1\_all.deb ...

Unpacking libtool (2.4.7-7build1) ...

Selecting previously unselected package pkgconf-bin.

Preparing to unpack .../08-pkgconf-bin\_1.8.1-2build1\_amd64.deb ...

Unpacking pkgconf-bin (1.8.1-2build1) ...

Selecting previously unselected package pkgconf:amd64.

Preparing to unpack .../09-pkgconf\_1.8.1-2build1\_amd64.deb ...

Unpacking pkgconf:amd64 (1.8.1-2build1) ...

Selecting previously unselected package pkg-config:amd64.

Preparing to unpack .../10-pkg-config\_1.8.1-2build1\_amd64.deb ...

Unpacking pkg-config:amd64 (1.8.1-2build1) ...

Setting up m4 (1.4.19-4build1) ...

Setting up autotools-dev (20220109.1) ...

Setting up libpkgconf3:amd64 (1.8.1-2build1) ...

Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...

Setting up pkgconf-bin (1.8.1-2build1) ...

Setting up autoconf (2.71-3) ...

Setting up automake (1:1.16.5-1.3ubuntu1) ...

update-alternatives: using /usr/bin/automake-1.16 to provide /usr/bin/automake (automake) in auto mode

Setting up libtool (2.4.7-7build1) ...

Setting up pkgconf:amd64 (1.8.1-2build1) ...

Setting up libltdl-dev:amd64 (2.4.7-7build1) ...

Setting up pkg-config:amd64 (1.8.1-2build1) ...

Processing triggers for libc-bin (2.39-0ubuntu8.4) ...

Processing triggers for man-db (2.12.0-4build2) ...

Processing triggers for install-info (7.1-3build2) ...

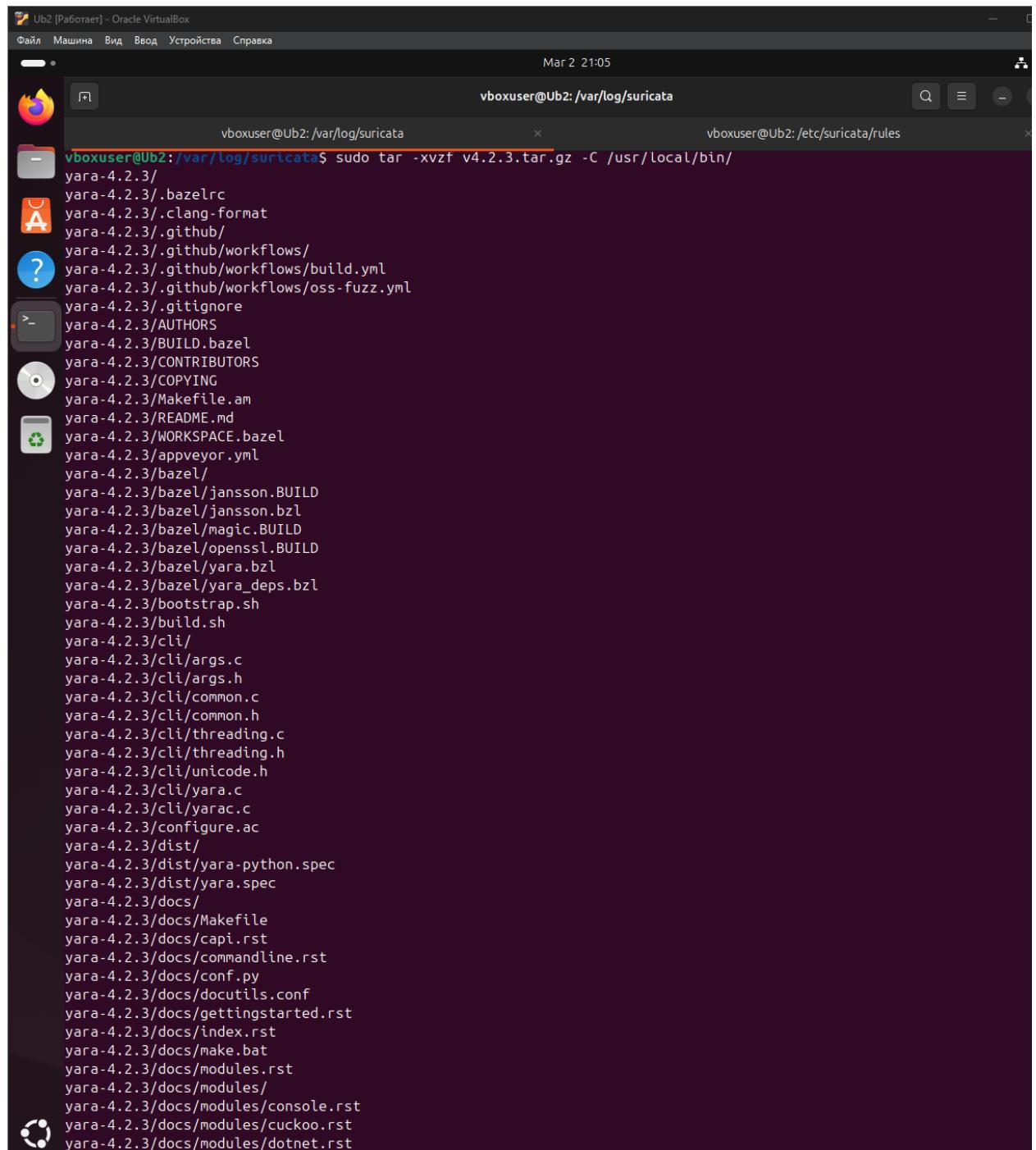
vboxuser@Ub2: /var/log/suricata\$ sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
Dload	Upload	Total	Spent	Left	Speed		
0	0	0	0	0	0	0	0
100	1258k	0	1258k	0	0	423k	0
						0:00:02	759k

vboxuser@Ub2: /var/log/suricata\$

Right Ctrl

```
sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/  
sudo rm -f v4.2.3.tar.gz
```



The screenshot shows a terminal window titled "vboxuser@Ub2: /var/log/suricata" running on a virtual machine named "Ub2". The command "sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/" was entered, followed by "yara-4.2.3". The terminal output lists all the files and directories extracted from the tar archive into the "/usr/local/bin" directory. The files listed include various configuration files, build scripts, and header files for the YARA project version 4.2.3.

```
vboxuser@Ub2: /var/log/suricata$ sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/  
yara-4.2.3/  
yara-4.2.3/.bazelrc  
yara-4.2.3/.clang-format  
yara-4.2.3/.github/  
yara-4.2.3/.github/workflows/  
yara-4.2.3/.github/workflows/build.yml  
yara-4.2.3/.github/workflows/oss-fuzz.yml  
yara-4.2.3/.gitignore  
yara-4.2.3/AUTHORS  
yara-4.2.3/BUILD.bazel  
yara-4.2.3/CONTRIBUTORS  
yara-4.2.3/COPYING  
yara-4.2.3/Makefile.am  
yara-4.2.3/README.md  
yara-4.2.3/WORKSPACE.bazel  
yara-4.2.3/appveyor.yml  
yara-4.2.3/bazel/  
yara-4.2.3/bazel/jansson.BUILD  
yara-4.2.3/bazel/jansson.bzl  
yara-4.2.3/bazel/magic.BUILD  
yara-4.2.3/bazel/openssl.BUILD  
yara-4.2.3/bazel/yara.bzl  
yara-4.2.3/bazel/yara_deps.bzl  
yara-4.2.3/bootstrap.sh  
yara-4.2.3/build.sh  
yara-4.2.3/cli/  
yara-4.2.3/cli/args.c  
yara-4.2.3/cli/args.h  
yara-4.2.3/cli/common.c  
yara-4.2.3/cli/common.h  
yara-4.2.3/cli/threading.c  
yara-4.2.3/cli/threading.h  
yara-4.2.3/cli/unicode.h  
yara-4.2.3/cli/yara.c  
yara-4.2.3/cli/yarac.c  
yara-4.2.3/configure.ac  
yara-4.2.3/dist/  
yara-4.2.3/dist/yara-python.spec  
yara-4.2.3/dist/yara.spec  
yara-4.2.3/docs/  
yara-4.2.3/docs/Makefile  
yara-4.2.3/docs/capi.rst  
yara-4.2.3/docs/commandline.rst  
yara-4.2.3/docs/conf.py  
yara-4.2.3/docs/docutils.conf  
yara-4.2.3/docs/gettingstarted.rst  
yara-4.2.3/docs/index.rst  
yara-4.2.3/docs/make.bat  
yara-4.2.3/docs/modules.rst  
yara-4.2.3/docs/modules/  
yara-4.2.3/docs/modules/console.rst  
yara-4.2.3/docs/modules/cuckoo.rst  
yara-4.2.3/docs/modules/dotnet.rst
```

```
sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check
```

```
vboxuser@Ub2:~$ cd /usr/local/bin/yara-4.2.3/
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$ sudo ./bootstrap.sh && sudo ./configure && sudo make && sudo make install && sudo make check
[sudo] password for vboxuser:
libtoolize: putting auxiliary files in AC_CONFIG_AUX_DIR, 'build-aux'.
libtoolize: copying file 'build-aux/ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt-obsolete.m4'
configure.ac:23: warning: The macro `AC_PROG_CC_C99' is obsolete.
configure.ac:23: You should run autoupdate.
./lib/autoconf/c.m4:1659: AC_PROG_CC_C99 is expanded from...
configure.ac:23: the top level
configure.ac:25: warning: AC_PROG_LEX without either yywrap or noyywrap is obsolete
./lib/autoconf/programs.m4:716: _AC_PROG_LEX is expanded from...
./lib/autoconf/programs.m4:709: AC_PROG_LEX is expanded from...
aclocal.m4:1072: AM_PROG_LEX is expanded from...
configure.ac:25: the top level
configure.ac:79: warning: The macro `AC_LANG_C' is obsolete.
configure.ac:79: You should run autoupdate.
./lib/autoconf/c.m4:72: AC_LANG_C is expanded from...
m4/acx_pthread.m4:63: ACX_PTHREAD is expanded from...
configure.ac:79: the top level
configure.ac:79: warning: The macro `AC_TRY_LINK' is obsolete.
configure.ac:79: You should run autoupdate.
./lib/autoconf/general.m4:2920: AC_TRY_LINK is expanded from...
m4/acx_pthread.m4:63: ACX_PTHREAD is expanded from...
configure.ac:79: the top level
configure.ac:369: warning: AC_C_BIGENDIAN should be used with AC_CONFIG_HEADERS
configure.ac:20: installing 'build-aux/compile'
configure.ac:8: installing 'build-aux/missing'
Makefile.am: installing 'build-aux/depcomp'
checking whether make supports nested variables... yes
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether the compiler supports GNU C... yes
checking whether gcc accepts -g... yes
checking for gcc option to enable C11 features... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
```

Установка завершена

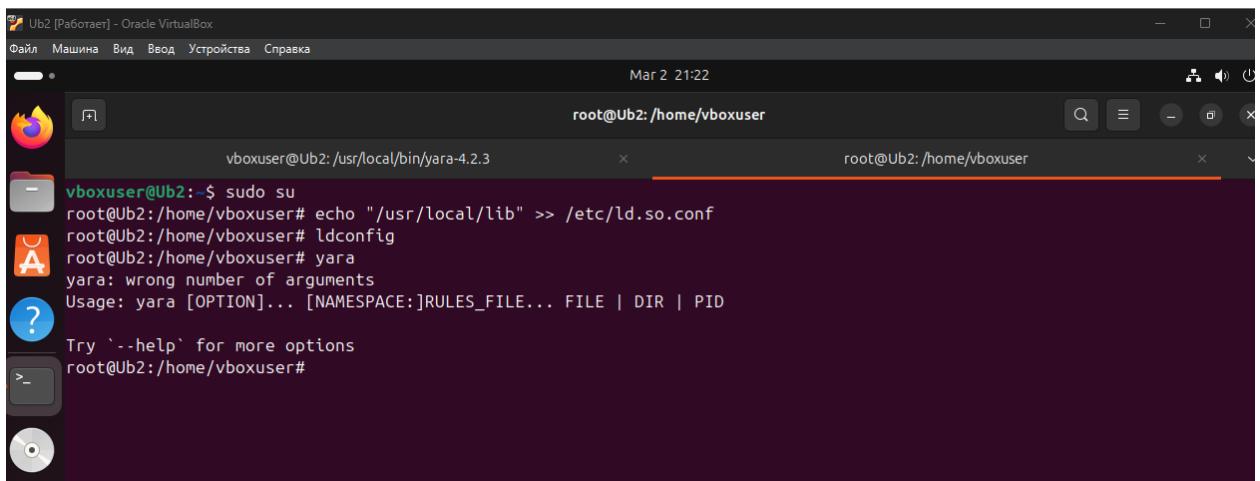
```
vboxuser@Ub2: /usr/local/bin/yara-4.2.3
vboxuser@Ub2: ~
vboxuser@Ub2: /usr/local/bin/yara-4.2.3

CC      tests/test-pe.o
CCLD    test-pe
CC      tests/test-elf.o
CCLD    test-elf
CC      tests/test-version.o
CCLD    test-version
CC      tests/test-bitmask.o
CCLD    test-bitmask
CC      tests/test-math.o
CCLD    test-math
CC      tests/test-stack.o
CCLD    test-stack
CC      tests/test-re-split.o
CCLD    test-re-split
CC      tests/test-async.o
CCLD    test-async
CC      tests/test-exception.o
CCLD    test-exception
CC      tests/test-dotnet.o
CCLD    test-dotnet
make[2]: Leaving directory '/usr/local/bin/yara-4.2.3'
make check-TESTS
make[2]: Entering directory '/usr/local/bin/yara-4.2.3'
make[3]: Entering directory '/usr/local/bin/yara-4.2.3'
PASS: test-area
PASS: test-alignment
PASS: test-atoms
PASS: test-api
PASS: test-rules
PASS: test-pe
PASS: test-elf
PASS: test-version
PASS: test-bitmask
PASS: test-math
PASS: test-stack
PASS: test-re-split
PASS: test-async
PASS: test-exception
PASS: test-dotnet
=====
Testsuite summary for yara 4.2.3
=====
# TOTAL: 15
# PASS: 15
# SKIP: 0
# XFAIL: 0
# FAIL: 0
# XPASS: 0
# ERROR: 0
=====
make[3]: Leaving directory '/usr/local/bin/yara-4.2.3'
make[2]: Leaving directory '/usr/local/bin/yara-4.2.3'
make[1]: Leaving directory '/usr/local/bin/yara-4.2.3'
vboxuser@Ub2: /usr/local/bin/yara-4.2.3$
```

Ошибка при проверки уара

```
vboxuser@Ub2: /usr/local/bin/yara-4.2.3$ yara
yara: error while loading shared libraries: libyara.so.9: cannot open shared object file: No such file or directory
vboxuser@Ub2: /usr/local/bin/yara-4.2.3$
```

```
echo "/usr/local/lib" >> /etc/ld.so.conf
ldconfig
```



```
vboxuser@Ub2:~$ sudo su
root@Ub2:/home/vboxuser# echo "/usr/local/lib" >> /etc/ld.so.conf
root@Ub2:/home/vboxuser# ldconfig
root@Ub2:/home/vboxuser# yara
yara: wrong number of arguments
Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID
Try `--help` for more options
root@Ub2:/home/vboxuser#
```

```
root@Ub2:/home/vboxuser#
```

```
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$ yara
yara: wrong number of arguments
Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID
Try `--help` for more options
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$
```

### Создание директории под рулы

```
sudo mkdir -p /tmp/yara/rules
```

Через sudo curl 'https://valhalla.nextron-systems.com/api/v1/get' не удалось скачать

```
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$ sudo curl 'https://valhalla.nextron-systems.com/api/v1/get'
curl: (7) Failed to connect to valhalla.nextron-systems.com port 443 after 21015 ms: Couldn't connect to server
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$
```

### Установка через гит

```
sudo apt install git
```

```
vboxuser@Ub2:~$ sudo apt install git
[sudo] password for vboxuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 35 not upgraded.
Need to get 4,804 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu noble amd64 liberror-perl all 0.17029-2 [25.6 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man all 1:2.43.0-1ubuntu7.2 [1,100 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu noble-updates/main amd64 git amd64 1:2.43.0-1ubuntu7.2 [3,679 kB]
Fetched 4,804 kB in 0s (9,986 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 151193 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-2_all.deb ...
Unpacking liberror-perl (0.17029-2) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.43.0-1ubuntu7.2_all.deb ...
Unpacking git-man (1:2.43.0-1ubuntu7.2) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.43.0-1ubuntu7.2_amd64.deb ...
Unpacking git (1:2.43.0-1ubuntu7.2) ...
Setting up liberror-perl (0.17029-2) ...
Setting up git-man (1:2.43.0-1ubuntu7.2) ...
Setting up git (1:2.43.0-1ubuntu7.2) ...
Processing triggers for man-db (2.12.0-4build2) ...
vboxuser@Ub2:~$
```

## Установка правил с гита

```
sudo git clone https://github.com/Yara-Rules/rules.git
```

```
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$ sudo git clone https://github.com/Yara-Rules/rules.git
Cloning into 'rules'...
remote: Enumerating objects: 7274, done.
remote: Counting objects: 100% (161/161), done.
remote: Compressing objects: 100% (83/83), done.
remote: Total 7274 (delta 81), reused 134 (delta 69), pack-reused 7113 (from 1)
Receiving objects: 100% (7274/7274), 4.18 MiB | 7.50 MiB/s, done.
Resolving deltas: 100% (4463/4463), done.
vboxuser@Ub2:/usr/local/bin/yara-4.2.3$
```

## Создаю правило для с изменением файла (установка/удаление)

```
cd /tmp/yara/rules
sudo nano monitor_desktop.yara
```

```
rule monitor_desktop_changes {
```

```
meta:
```

```
description = "Monitor changes in Desktop directory"
```

```
author = "Sapoff"
```

```
date = "2025-03-02"
```

```
strings:
```

```
$desktop_path = "/home/Ubuntu-agent/Desktopop"
```

condition:

any of them

```
}
```

```
rule FileCreationOrDeletion
```

```
{
```

meta:

```
description = "Detect file creation or deletion"
```

```
author = "Sapof"
```

strings:

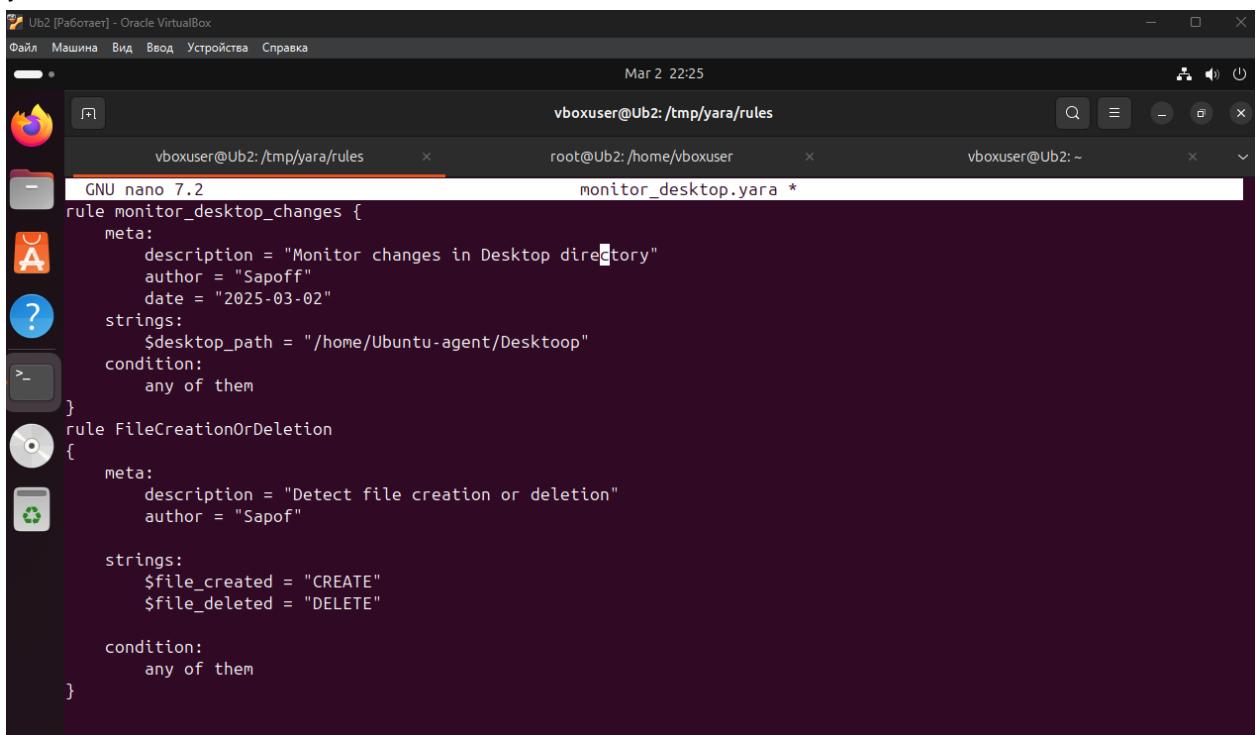
```
$file_created = "CREATE"
```

```
$file_deleted = "DELETE"
```

condition:

any of them

```
}
```



The screenshot shows a terminal window titled 'monitor\_desktop.yara \*' with the command 'vboxuser@Ub2: /tmp/yara/rules'. The window displays two YARA rules: 'monitor\_desktop\_changes' and 'FileCreationOrDeletion'. The 'monitor\_desktop\_changes' rule monitors the desktop directory for changes, while the 'FileCreationOrDeletion' rule detects file creation or deletion. Both rules include meta-information such as description, author, and date, along with strings and condition definitions.

```
GNU nano 7.2
rule monitor_desktop_changes {
    meta:
        description = "Monitor changes in Desktop directory"
        author = "Sapoff"
        date = "2025-03-02"
    strings:
        $desktop_path = "/home/Ubuntu-agent/Desktopop"
    condition:
        any of them
}
rule FileCreationOrDeletion
{
    meta:
        description = "Detect file creation or deletion"
        author = "Sapof"

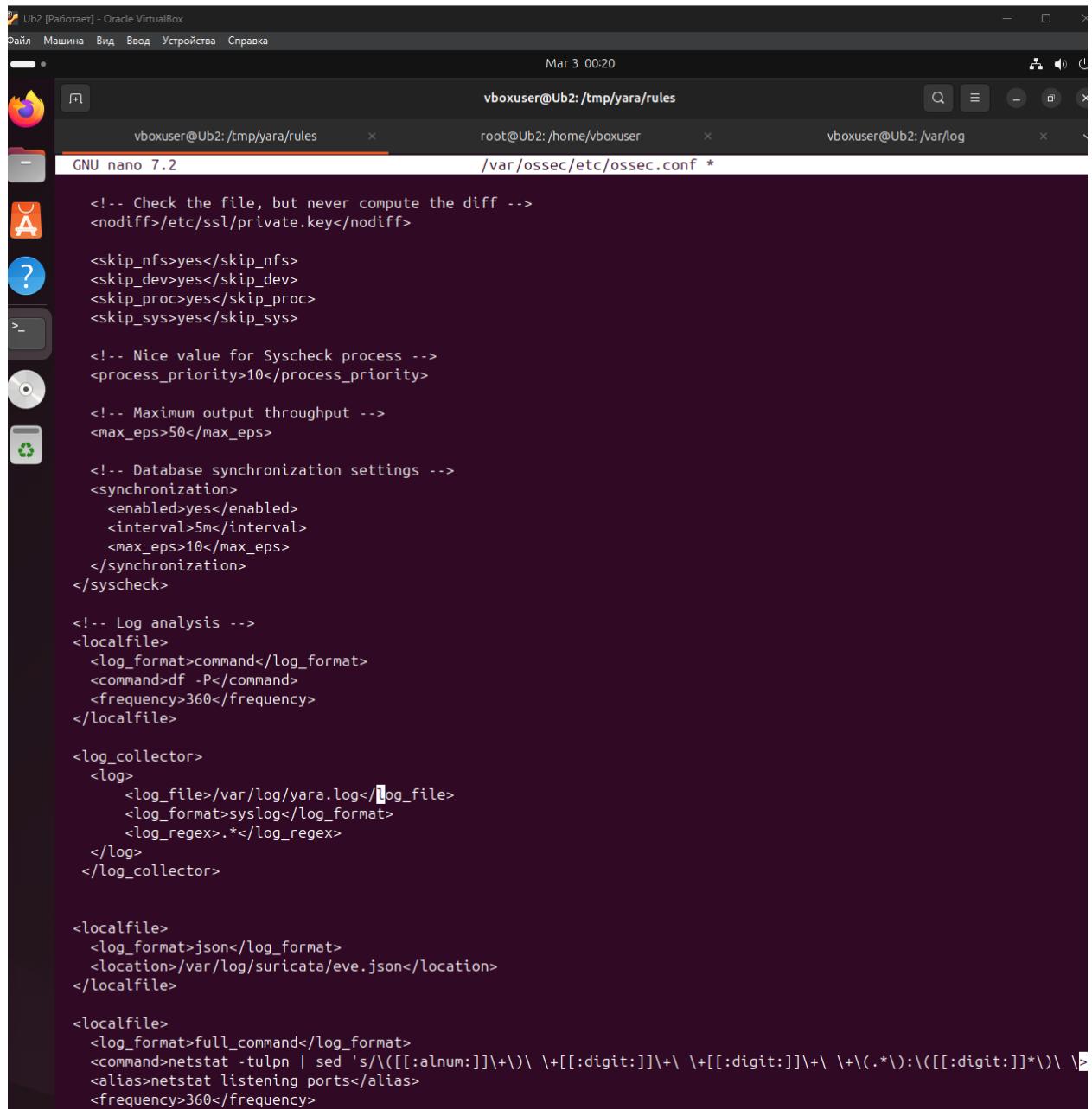
    strings:
        $file_created = "CREATE"
        $file_deleted = "DELETE"

    condition:
        any of them
}
```

## Указываю логи в конфиге агента

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<log_collector>
  <log>
    <log_file>/var/log/yara.log</log_file>
    <log_format>syslog</log_format>
    <log_regex>.*</log_regex>
  </log>
</log_collector>
```



```
GNU nano 7.2
vboxuser@Ub2: /tmp/yara/rules
root@Ub2: /home/vboxuser
vboxuser@Ub2: /var/log


<nodiff>/etc/ssl/private.key</nodiff>

<skip_nfs>yes</skip_nfs>
<skip_dev>yes</skip_dev>
<skip_proc>yes</skip_proc>
<skip_sys>yes</skip_sys>


<process_priority>10</process_priority>


<max_eps>50</max_eps>


<synchronization>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <max_eps>10</max_eps>
</synchronization>
</syscheck>


<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>

<log_collector>
  <log>
    <log_file>/var/log/yara.log</log_file>
    <log_format>syslog</log_format>
    <log_regex>.*</log_regex>
  </log>
</log_collector>

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

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tulpn | sed 's/(\[[[:alnum:]]\+\)\| \+[[[:digit:]]\+\| \+[[[:digit:]]\+\| \+\(.*\):\| \([[:digit:]]*\)\| \>
```

## Проверка правила

