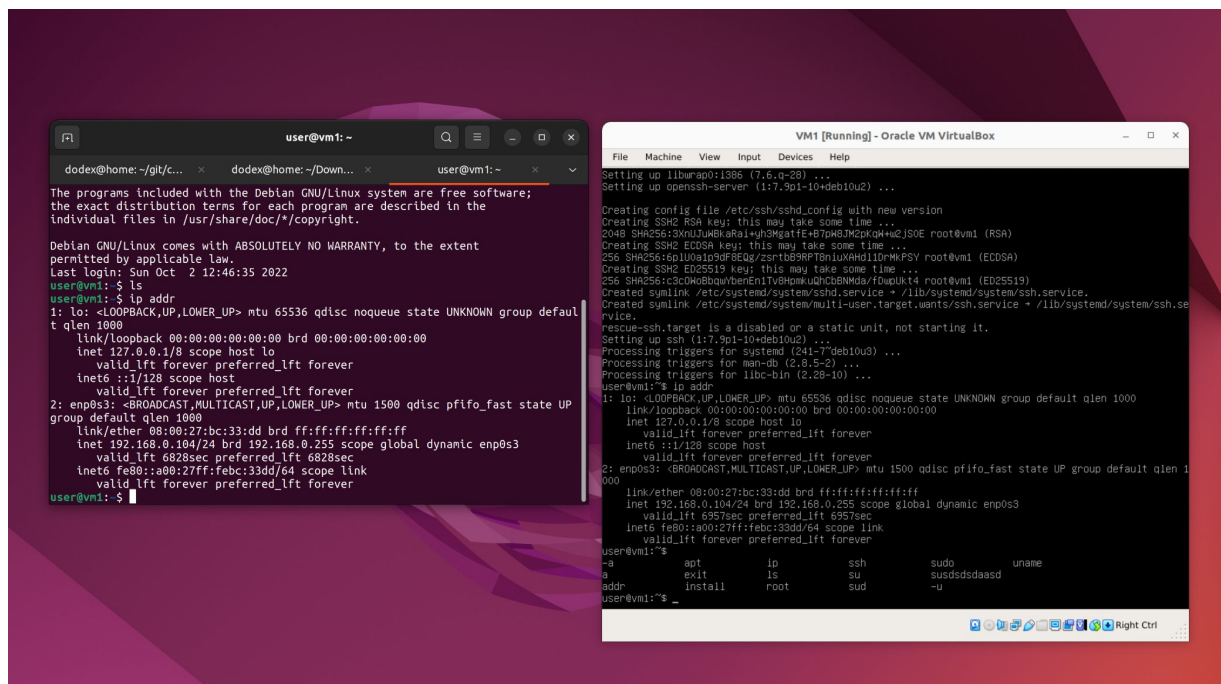


## 1. Удаленное подключение к Linux по ssh

- Установка на локальном ПК ssh-клиент и подключитесь к VM1



## 2. Безопасная аутентификация в Linux

- Настройте доступ через ключевую пару, запретите доступ к VM1 по логину и паролю `./userdata/vm1/etc/ssh/sshd config`

## Редактирование конфиг /etc/ssh/sshd\_config (./userdata)

## PermitRootLogin no – запрет логина по ssh из под root

PasswordAuthentication no – запрет логина по pass.

Добавили authorized keys с хоста подключения

pubkeyс хоста поместили в ~/.ssh

### 3. Сканирование сети

```
./userdata/vm1/netcat scan vm2.txt
```

```
./userdata/vm1/nmap scan vm2.txt
```

## 4. Анализ трафика

- Установите на локальном ПК Wireshark
- Проанализируйте трафик VM2
- Заблокируйте вредоносный трафик VM2 с помощью встроенных средств операционной системы

Блокировка по протоколу "tcp" INPUT - iptables -A INPUT -p tcp -j DROP

Отдельный IP - Iptables -A INPUT -s 76.23.12.11 -j DROP

Wireshark packet capture showing TCP traffic on interface wlo1. The capture shows a sequence of packets, including SYN, ACK, and retransmissions. The packet list pane shows details for packet 4459, which is a TCP segment from 192.168.0.106 to 192.168.0.106, port 443. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

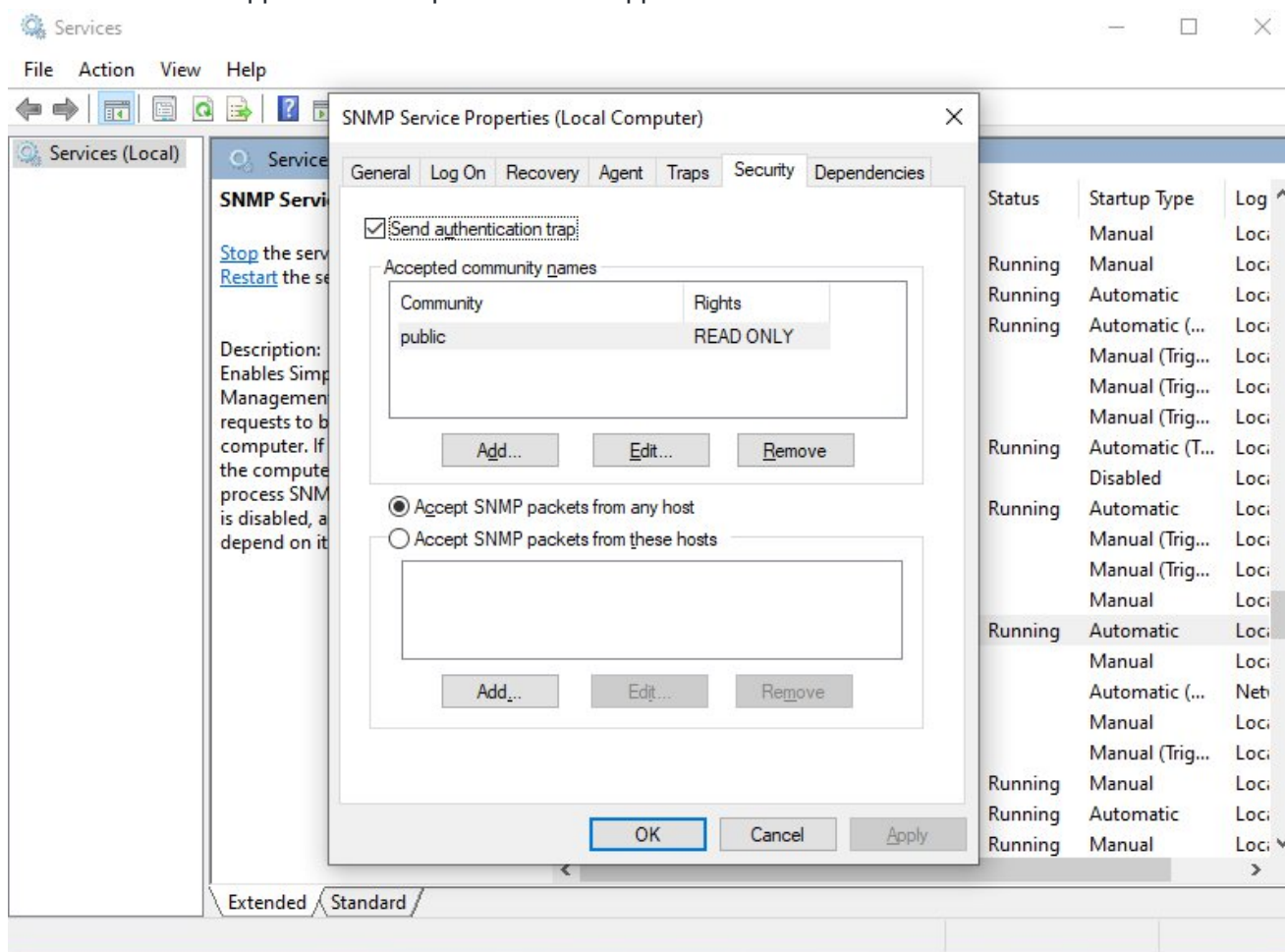
## 5. Мониторинг nginx

Zabbix monitoring dashboard for nginx. The dashboard shows a list of items for nginx, including Service status, Service response time, Requests total, Requests per second, Connections writing, Connections waiting, Connections reading, Connections handled per second, Connections dropped per second, Connections active, and Connections accepted per second. A graph shows the item values over time, with a red area representing the data. The graph shows a steady increase in the number of connections over time.

Item	last	min	avg	max
Nginx: Service status	[no data]			
Nginx: Service response time	[avg]	0,1ms	0,1ms	0,1ms
Nginx: Requests total	[avg]	141	108	116,4
Nginx: Requests per second	[avg]	0,4498	0,0167	0,1133
Nginx: Connections writing	[avg]	1	1	1
Nginx: Connections waiting	[avg]	4	0	1,2
Nginx: Connections reading	[avg]	0	0	0
Nginx: Connections handled per second	[avg]	0,1	0,05	0,0667
Nginx: Connections dropped per second	[avg]	0	0	0
Nginx: Connections active	[avg]	5	1	2,2
Nginx: Connections accepted per second	[avg]	0,1	0,05	0,0667

## 6. Мониторинг Windows

- Настройте SNMP для принятия пакетов с любого хоста
- Создайте сообщество SNMP для чтения.



- Свяжите хост с шаблоном сетевого монитора
- Запустите мониторинг



## Windows10 + Nginx

Windows10	CPU (1 Item)				
<input type="checkbox"/>	CPU utilization	2022-10-14 21:34:07	15.875 %	+15.875 %	Graph
Windows10	General (6 Items)				
<input type="checkbox"/>	SNMP traps (fallback)				History
<input type="checkbox"/>	System contact details				History
<input type="checkbox"/>	System description				History
<input type="checkbox"/>	System location				History
<input type="checkbox"/>	System name				History
<input type="checkbox"/>	System object ID				History
nginx	Nginx (12 Items)				
<input type="checkbox"/>	Nginx: Connections accepted per second	2022-10-14 21:34:10	0.0499	-0.0002	Graph
<input type="checkbox"/>	Nginx: Connections active	2022-10-14 21:34:10	1		Graph
<input type="checkbox"/>	Nginx: Connections dropped per second	2022-10-14 21:34:10	0		Graph
<input type="checkbox"/>	Nginx: Connections handled per second	2022-10-14 21:34:10	0.0499	-0.0002	Graph
<input type="checkbox"/>	Nginx: Connections reading	2022-10-14 21:34:10	0		Graph
<input type="checkbox"/>	Nginx: Connections waiting	2022-10-14 21:34:10	0		Graph
<input type="checkbox"/>	Nginx: Connections writing	2022-10-14 21:34:10	1		Graph
<input type="checkbox"/>	Nginx: Requests per second	2022-10-14 21:34:10	0.0166	-0.0001	Graph
<input type="checkbox"/>	Nginx: Requests total	2022-10-14 21:34:10	26	+1	Graph
<input type="checkbox"/>	Nginx: Service response time	2022-10-14 21:34:08	0.1ms	- 0.1ms	Graph
<input type="checkbox"/>	Nginx: Service status	2022-10-14 21:25:09	Up (1)		Graph
<input type="checkbox"/>	Nginx: Version	2022-10-14 21:25:10	1.14.2		History
Windows10	Status (5 Items)				
<input type="checkbox"/>	ICMP loss	2022-10-14 21:34:07	0 %		Graph
<input type="checkbox"/>	ICMP ping	2022-10-14 21:34:07	Up (1)		Graph

### 7) Выход за пределы Docker-контейнера

- На VM4 изначально дан неверный pass от пользователя user и root. Заходим в настройки grub и дополняем конфиг, заходим от root



- Сбрасываем пароль

```

VM4 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help

root@none):/# mount -rw -o remount /
root@none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@none):/# passwd user
New password:
Retype new password:
passwd: password updated successfully
root@none):/# umount /
root@none):/# reboot -f_

```

- Zabbix в Docker:

The screenshot displays the Zabbix web interface. On the left is a sidebar with navigation links: Monitoring, Dashboard, Problems, Hosts, Latest data, Maps, Discovery, Services, Inventory, Reports, Configuration, and Administration. The main content area is titled 'Global view' and includes several widgets:

- Top hosts by CPU utilization:** A table showing utilization, 1m avg, 5m avg, 15m avg, and Processes. It currently shows 'No data found.'
- Zabbix server Values per second:** A large number '0.81' with a red downward arrow.
- System information:** A table with parameters and their values.
 

Parameter	Value	Details
Zabbix server is running	Yes	zabbix-server:10051
Number of hosts (enabled/disabled)	1	1 / 0
Number of templates	311	
Number of items (enabled/disabled/not supported)	99	99 / 0 / 0
Number of triggers (enabled/disabled [problem/vok])	56	56 / 0 / 56
Number of users (online)	2	1
Required server performance, new values per second	1.45	
- Host availability:** A bar chart showing 0 Available, 0 Not available, 1 Unknown, and 1 Total.
- Problems by severity:** A bar chart showing 0 Disaster, 0 High, 1 Average, 0 Warning, 0 Information, and 0 Not classified.
- Current problems:** A table showing a problem with 'Zabbix agent is not available (for 3m)' on the 'Zabbix server' host.
- Geomap:** A map showing the location of the Zabbix server in Riga, Latvia.

At the bottom, a terminal window shows the following commands and output:

```

vagrant@debian10: /var/lib/zabbix$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        NAMES        STATUS
37cdd8b1d318   zabbix/zabbix-web-nginx-pgsql:alpine-latest   "docker-entrypoint.sh"   13 minutes ago   zabbix-web   Up 13 min
bf7af96d269b   zabbix/zabbix-server-pgsql:alpine-latest      "/sbin/tini -- /usr/_..." 13 minutes ago   zabbix-server Up 13 min
017e7c03fdd   postgres:14-bullseye                    "docker-entrypoint.s..." 14 minutes ago   zabbix-postgres Up 14 min
vagrant@debian10: /var/lib/zabbix$

```