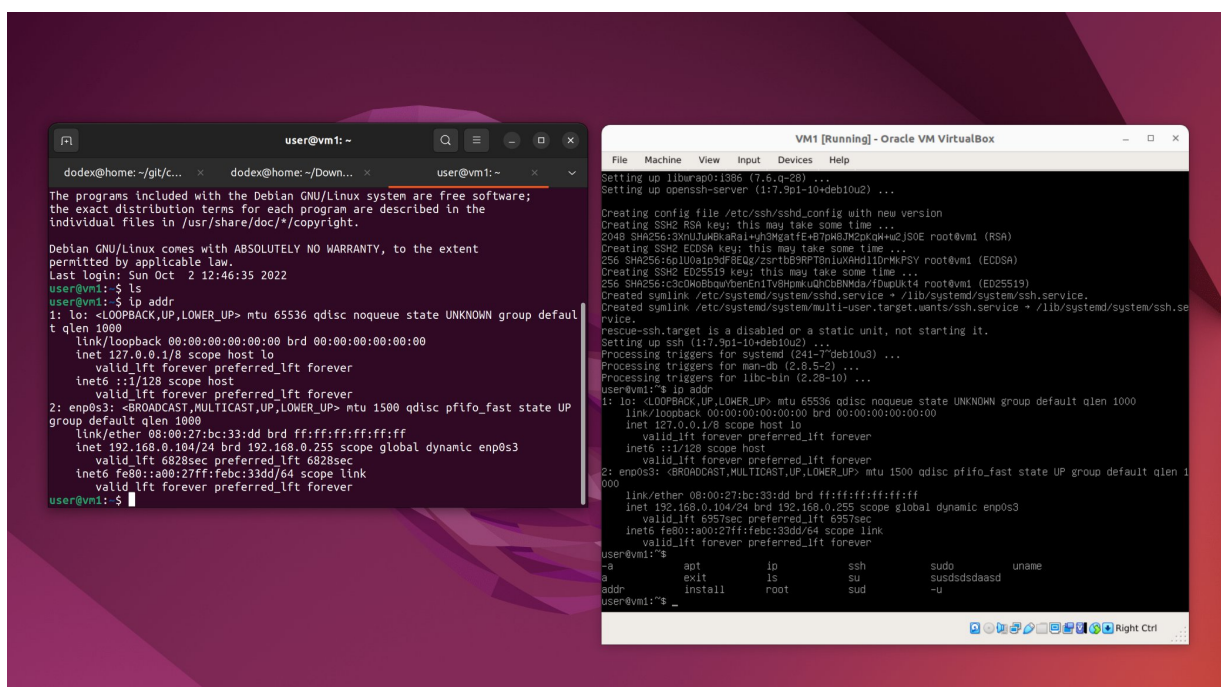


## 1. Удаленное подключение к Linux по ssh

- Установка на локальном ПК ssh-клиент и подключиться 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

`pubkey` 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 a TCP connection from 192.168.0.106 to 192.168.0.106. The capture shows a SYN flood attack where the source IP 192.168.0.106 sends multiple SYN packets to the destination 192.168.0.106. The destination responds with RST packets. The capture is filtered by 'ip.addr == 192.168.0.106'.

No.	Time	Source	Destination	Protocol	Length	Info
4455	1129.7418551	192.168.0.106	192.168.0.106	TCP	60	48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164415748 TSecr=0 WS=128
4456	1129.9070215	192.168.0.106	192.168.0.106	TCP	60	443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4457	1130.9702938	192.168.0.106	192.168.0.106	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4458	1130.9705470	192.168.0.106	192.168.0.106	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164416975 TSecr=0 WS=...
4459	1131.1342042	192.168.0.106	192.168.0.106	TCP	60	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4460	1133.9585887	192.168.0.106	192.168.0.106	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164419963 TSecr=0 WS=...
4461	1134.1475011	192.168.0.106	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=...
4462	1135.2690600	192.168.0.106	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4465	1138.4532350	192.168.0.106	192.168.0.106	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164424850 TSecr=0 WS=...
4466	1139.4448431	192.168.0.106	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=...
4470	1140.0755534	192.168.0.106	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4475	1147.8201714	192.168.0.106	192.168.0.106	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48592 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164433824 TSecr=0 WS=...
4476	1148.0070916	192.168.0.106	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=...
4477	1149.0957667	192.168.0.106	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 48592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4495	1165.0924524	192.168.0.106	172.67.140.53	TCP	74	57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422969369 TSecr=0 WS=128
4496	1165.1838199	172.67.140.53	192.168.0.106	TCP	66	[TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4497	1166.1803630	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422970385 TSecr=0 WS=...
4498	1166.2002297	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4502	1167.3246382	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4503	1168.1169729	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422972394 TSecr=0 WS=...
4504	1168.2110993	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4509	1172.3727028	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422976649 TSecr=0 WS=...
4510	1172.4647225	172.67.140.53	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=...
4511	1173.5689721	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192
4512	1180.5710042	192.168.0.106	172.67.140.53	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 57762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2422984848 TSecr=0 WS=...
4513	1180.6033113	172.67.140.53	192.168.0.106	TCP	66	[TCP Previous segment not captured] [TCP Port numbers reused] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=...
4514	1181.7556620	172.67.140.53	192.168.0.106	TCP	66	[TCP Retransmission] 443 → 57762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=8192

Frame 4459: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0  
Ethernet II, Src: Tp-LinkT.80:7b:18 (c0:c9:e3:80:7b:18), Dst: Chongjin.b7:9f:65 (4c:d5:77:b7:9f:65)  
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.106  
Transmission Control Protocol, Src Port: 443, Dst Port: 48592, Seq: 0, Ack: 1, Len: 0

Wireshark packet capture showing a TCP connection from 192.168.0.106 to 192.168.0.106. The capture shows a SYN flood attack where the source IP 192.168.0.106 sends multiple SYN packets to the destination 192.168.0.106. The destination responds with RST packets. The capture is filtered by 'ip.addr == 192.168.0.106'.

## 5. Мониторинг nginx

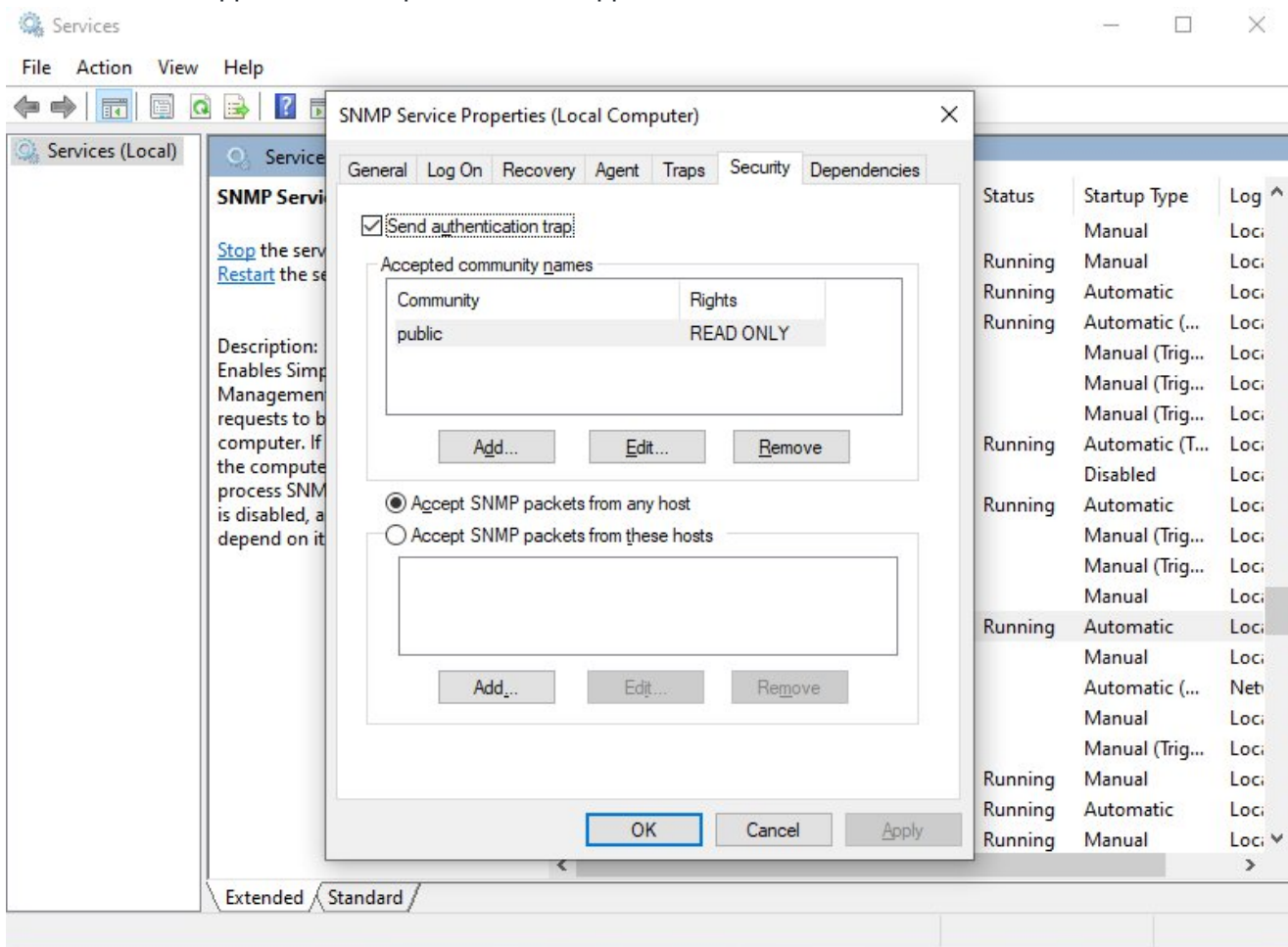
Zabbix monitoring dashboard for nginx. The dashboard shows a graph of nginx item values over time, with a red area chart indicating a significant increase in requests. Below the graph, a table provides summary statistics for various nginx metrics.

	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

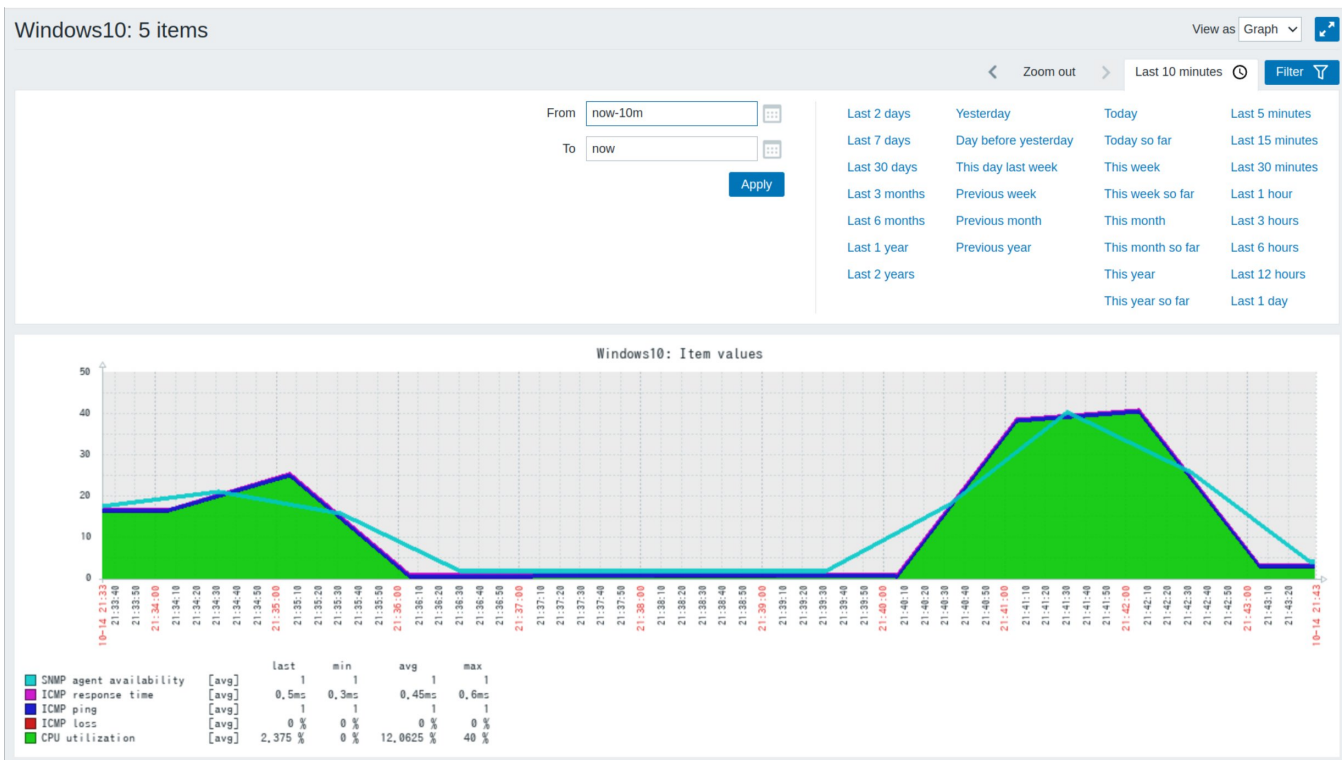
Zabbix 4.4.8. © 2001–2020, Zabbix SIA

## 6. Мониторинг Windows

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



- Свяжите хост с шаблоном сетевого монитора
- Запустите мониторинг

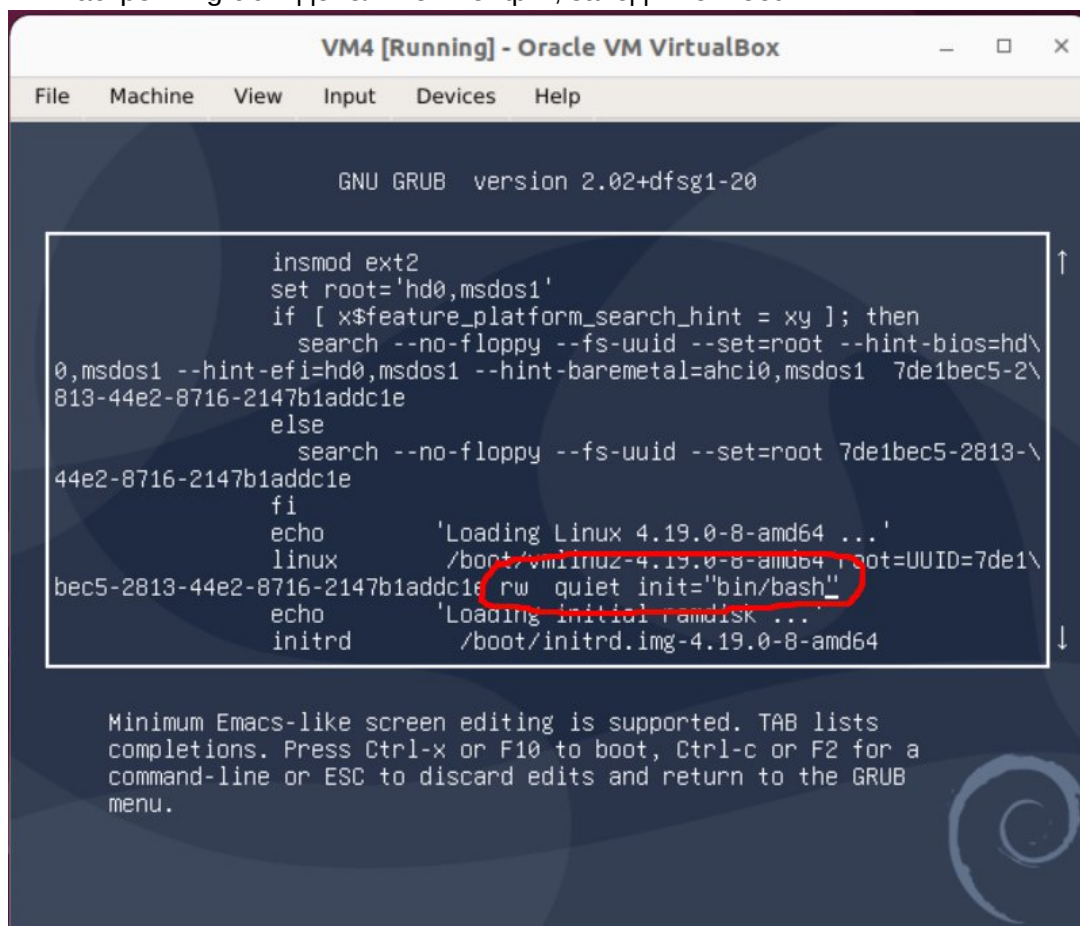


## Windows10 + Nginx

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



```
GNU GRUB version 2.02+dfsg1-20

insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd\
0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 7de1bec5-2\
813-44e2-8716-2147b1addc1e
else
  search --no-floppy --fs-uuid --set=root 7de1bec5-2813-\
44e2-8716-2147b1addc1e
fi
echo          'Loading Linux 4.19.0-8-amd64 ...'
linux         /boot/vmlinuz-4.19.0-8-amd64 root=UUID=7de1\
bec5-2813-44e2-8716-2147b1addc1e rw quiet init="bin/bash"
echo          'Loading initial ramdisk ...'
initrd        /boot/initrd.img-4.19.0-8-amd64

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```



- Сбрасываем пароль

```

VM [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_

```

- На VM4 загрузите образ alpine и присвойте контейнеру имя "capability"
- Установить конфигурацию запрещающую выход за пределы контейнера.

```

user@debian: ~
File Edit View Search Terminal Help
root@debian:/home/user# docker run --name capability --cap-add all --cap-drop CHOWN -d -it alpine
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
213ec9aee27d: Pull complete
Digest: sha256:bc41182d7ef5ffc53a40b044e725193bc10142a1243f395ee852a8d9730fc2ad
Status: Downloaded newer image for alpine:latest
0612452e6f46aed84a77a05b8840437220261344533c04f90d172c0bb92882ba
root@debian:/home/user# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS
PORTS              NAMES
0612452e6f46        alpine             "/bin/sh"          3 seconds ago      Up 2 seconds
capability
root@debian:/home/user#

```

## 8) Злоупотребление ресурсами в docker

- В ВМ4 установите переброс портов с 80 на 8080, лимит ОП 128МБ, CPU 30%
- Запустите контейнер в фоновом режиме.

```
user@debian: ~
File Edit View Search Terminal Help
root@debian:/home/user# docker run --name nginx -d -p 8080:80 --memory 128m --cpus=0.30 nginx
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
e9995326b091: Pull complete
71689475aec2: Pull complete
f88a23025338: Pull complete
0df440342e26: Pull complete
eef26ceb3309: Pull complete
8e3ed6a9e43a: Pull complete
Digest: sha256:24a1618e0ac445d24eda699881d7de1364e45641be98e9b1db5f7cad6b7b29b2
Status: Downloaded newer image for nginx:latest
WARNING: Your kernel does not support swap limit capabilities or the cgroup is not mounted. Memory limited without swap.
9a188e980828de32a9da179b35e17a42ec4e53cfb2ab1bac34e42583dd57a5fa
root@debian:/home/user# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS
9a188e980828        nginx              "/docker-entrypoint..." 5 seconds ago       Up 4 seconds
s                   0.0.0.0:8080->80/tcp  nginx
```

- Выполните команду `curl http://localhost:8080`

```
user@debian: ~
File Edit View Search Terminal Help
root@debian:/home/user# curl http://localhost:8080
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@debian:/home/user#
```

- Zabbix в Docker:

**ZABBIX** << Zabbix docker

Global view

All dashboards / Global view

**Top hosts by CPU utilization**

Utilization 1m avg 5m avg 15m avg Processes

No data found.

**0.81** ↓  
Zabbix server  
Values per second

**System information**

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 [0 / 56]
Number of users (online)	2	1
Required server performance, new values per second	1.45	

**20:07**  
Moscow

**Host availability**

0 Available 0 Not available 1 Unknown 1 Total

**Problems by severity**

0 Disaster 0 High 1 Average 0 Warning 0 Information 0 Not classified

**Current problems**

Time 19:57:26 Info Host Problem • Severity Duration Ack Actions Tags

Zabbix server Zabbix agent is not available (for 3m) 9m 2s No class: os component: system scope: availability +++

**Geomap**

Map of Riga, Latvia, showing the location of the Zabbix server.

```
vagrant@debian10: /var/lib/zabbix$ docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS
37cdd8b1d318   zabbix/zabbix-web-nginx-pgsql:alpine-latest  "docker-entrypoint.sh"  13 minutes ago Up 13 min
b77af96d269b   zabbix/zabbix-server-pgsql:alpine-latest     "/sbin/tini -- /usr/_  13 minutes ago Up 13 min
017e7c863fdd   postgres:14-bullseye                  "docker-entrypoint.s..." 14 minutes ago Up 14 min
utes 5432/tcp
vagrant@debian10: /var/lib/zabbix$
```