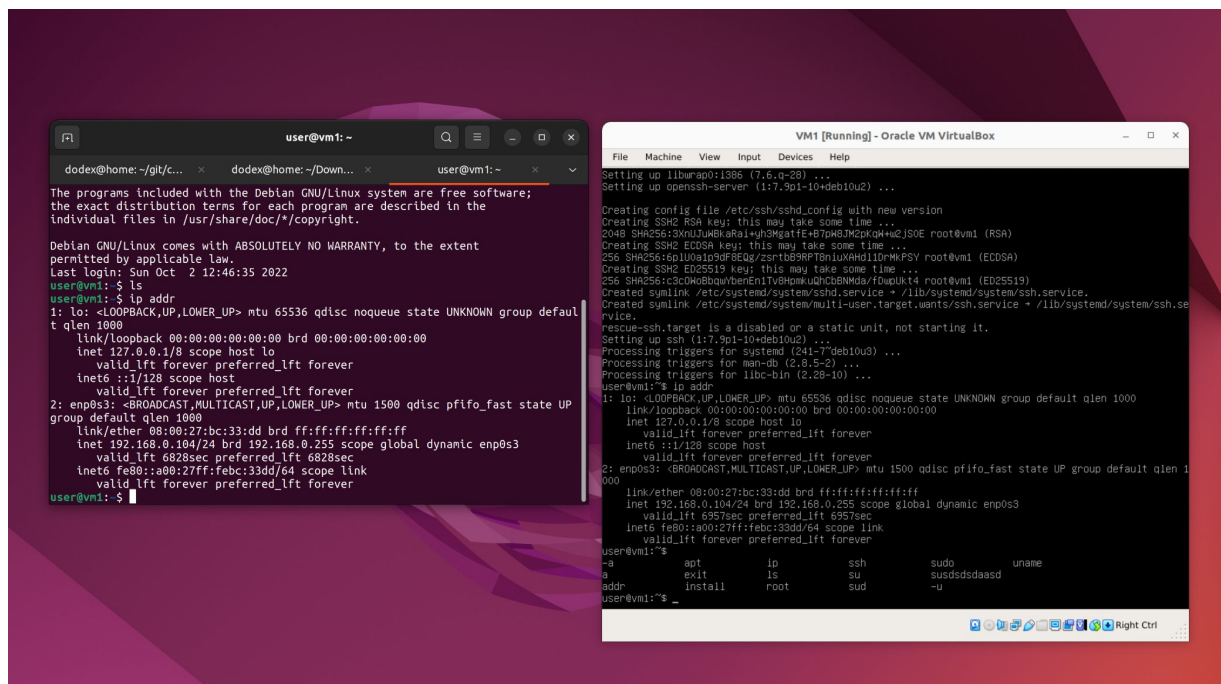


1. Удаленное подключение к Linux по ssh

- 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 analysis 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 repeatedly sends SYN packets to the destination IP, which responds with RST packets. The packet list shows multiple 'Previous segment not captured' and 'Retransmission' entries. The packet details pane shows the TCP header with Seq=0, Win=64240, Len=0, MSS=1460, SACK_PERM=1, TSval=1164415746, TSecr=0, WS=128. The packet bytes pane shows the raw data in hexadecimal and ASCII.

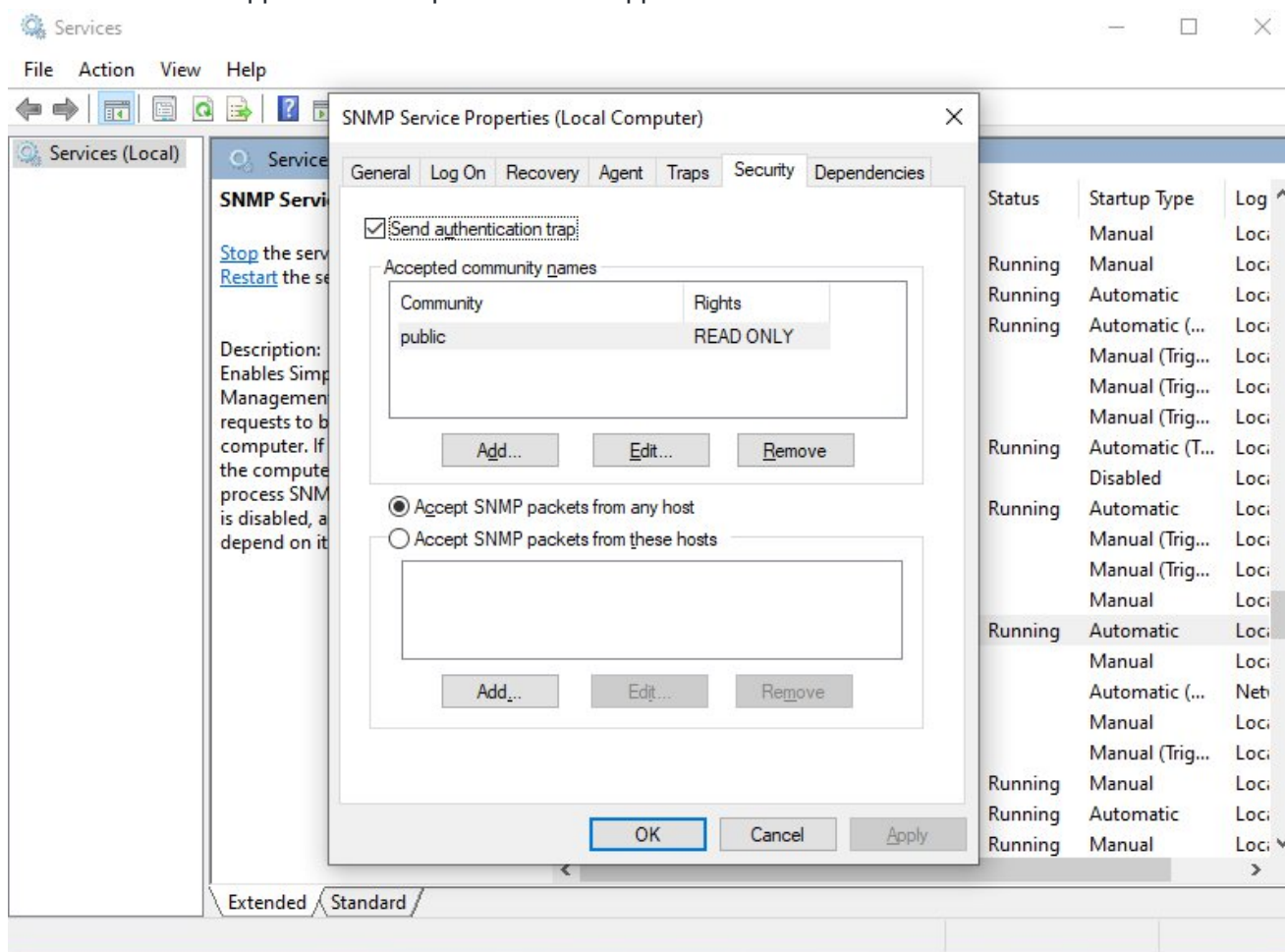
5. Мониторинг nginx

Zabbix monitoring dashboard for nginx. The dashboard shows a graph of nginx item values over time, with a red area chart showing a significant increase in values starting around 21:12:00. Below the graph, a table provides summary statistics for various nginx metrics.

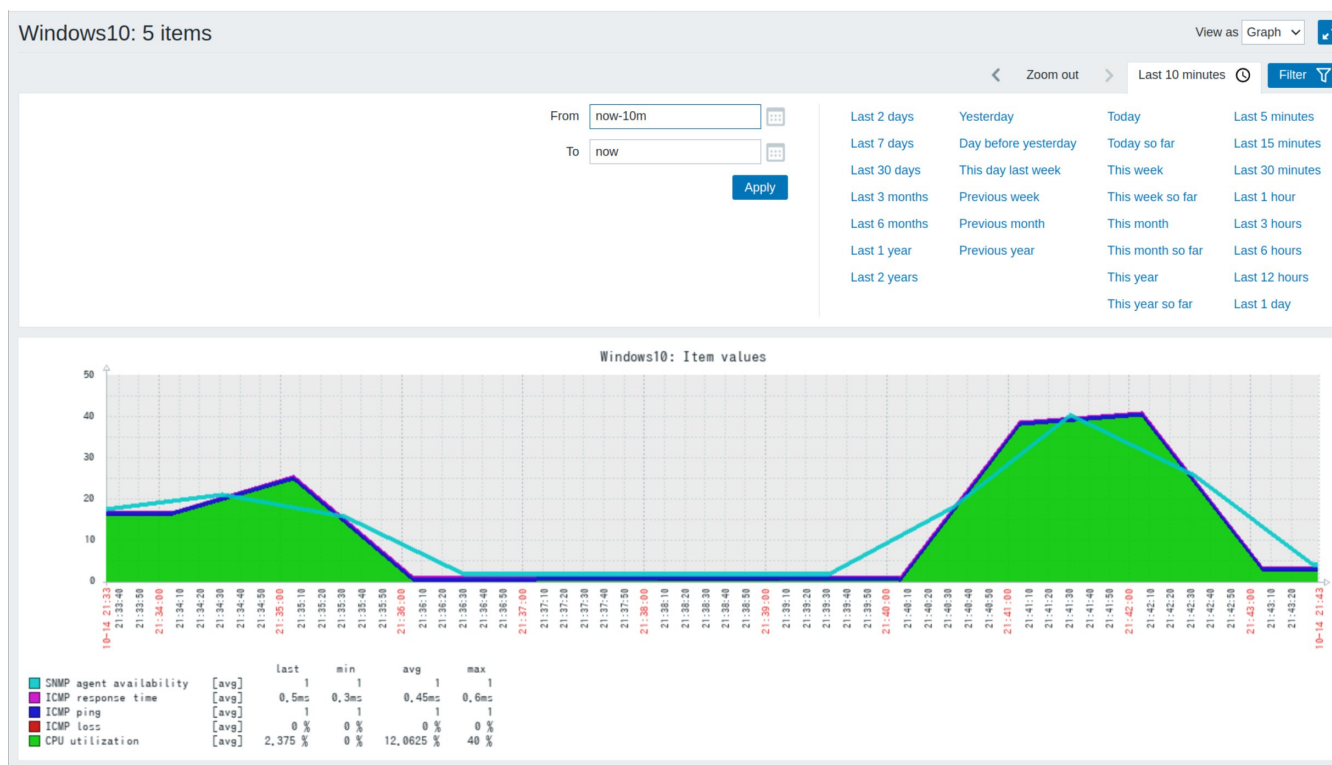
		last	min	avg	max
Nginx: Service status	[no data]				
Nginx: Service response time	[avg]	0,1ms	0,1ms	0,1ms	0,1ms
Nginx: Requests total	[avg]	141	108	116,4	141
Nginx: Requests per second	[avg]	0,4498	0,0167	0,1133	0,4498
Nginx: Connections writing	[avg]	1	1	1	1
Nginx: Connections waiting	[avg]	4	0	1,2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

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