

Škálování DNS resolverů

pro UDP, TLS a HTTPS provoz

Petr Špaček • petr.spacek@nic.cz • 2020-09-08



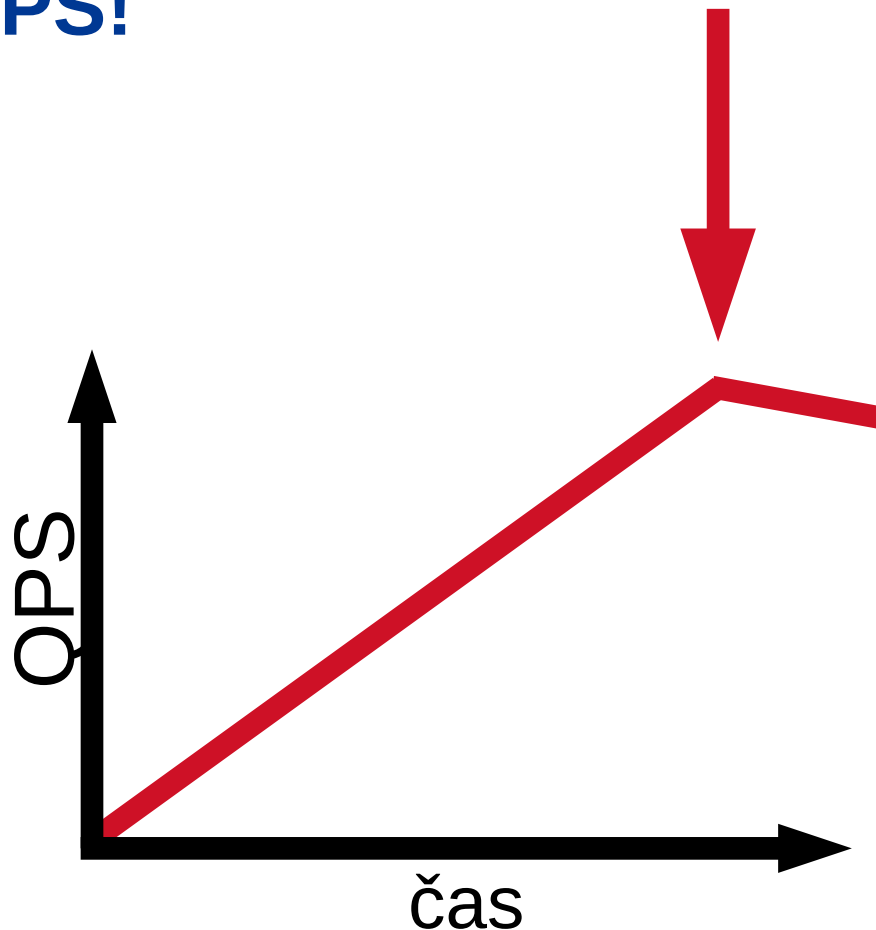
Obsah

- Klasický přístup – QPS
- DNS Shotgun – realistické měření
- Nové protokoly



Klasický přístup: QPS QPS QPS!

- \$ man resperf
- Hledá maximální QPS
 - Vyřízené dotazy/sekunda
- Seznam dotazů
 - tcpdump $\Rightarrow$ text
 - **ztráta informace**
 - čas, EDNS, flagy, ...



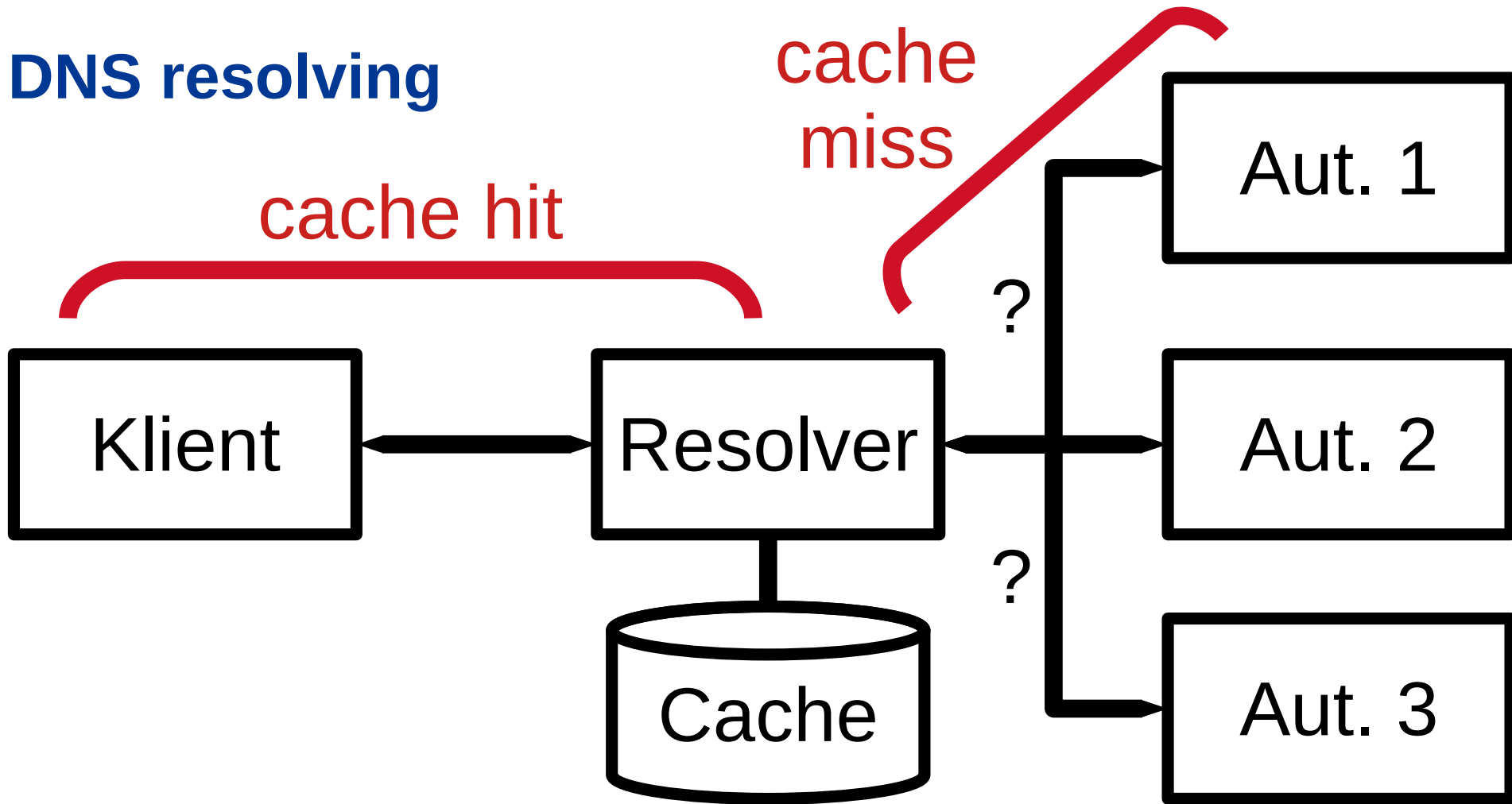
Klasický přístup



- Chybí prodlevy mezi dotazy
 - Ignoruje TTL $\Rightarrow$ nerealistický cache hit rate
- Ignoruje správu spojení
 - TCP, TLS, DoH!
- Postupné zvyšování zátěže
 - $\Rightarrow$ nerealistické
- **Přeceňuje QPS a ignoruje ostatní vlastnosti!**



DNS resolving



DNS Shotgun: Představení

- Nástroj pro **realistické** měření výkonu DNS resolverů
- Vývoj CZ.NIC Labs
- Open-source
 - <https://gitlab.nic.cz/knot/shotgun/>
- Zatím nemá uživatelské rozhraní :-)



DNS Shotgun: Nový přístup

- Kolik klientů resolver zvládne obsloužit?
 - Nepočítá "jen" QPS
- Záleží na chování klientů
 - IoT, mobil, desktop, mail server, ...



DNS Shotgun: Princip

- Krok 1: Analyzuje provoz v PCAP souborech
- Krok 2: Simuluje N ***vašich*** klientů
- Krok 3: Srovnává jednotlivé běhy



DNS Shotgun: Simulace klientů

- Realistické použití socketů a spojení
- Časování ± 1 sekunda
 - Realistický cache hit rate
 - $\Rightarrow$ QPS dle klientů, i proměnné
- Více **klientů** $\Rightarrow$ větší zátěž



DNS Shotgun: Hledání limitů

- Simulace N klientů 
 - Počty odpovědí + jejich RCODE
- Zvýšení počtu klientů N
 - ... dokud resolver odpovídá
- **Výsledné N** = maximální počet klientů
 - ... pro daný provoz a parametry simulace

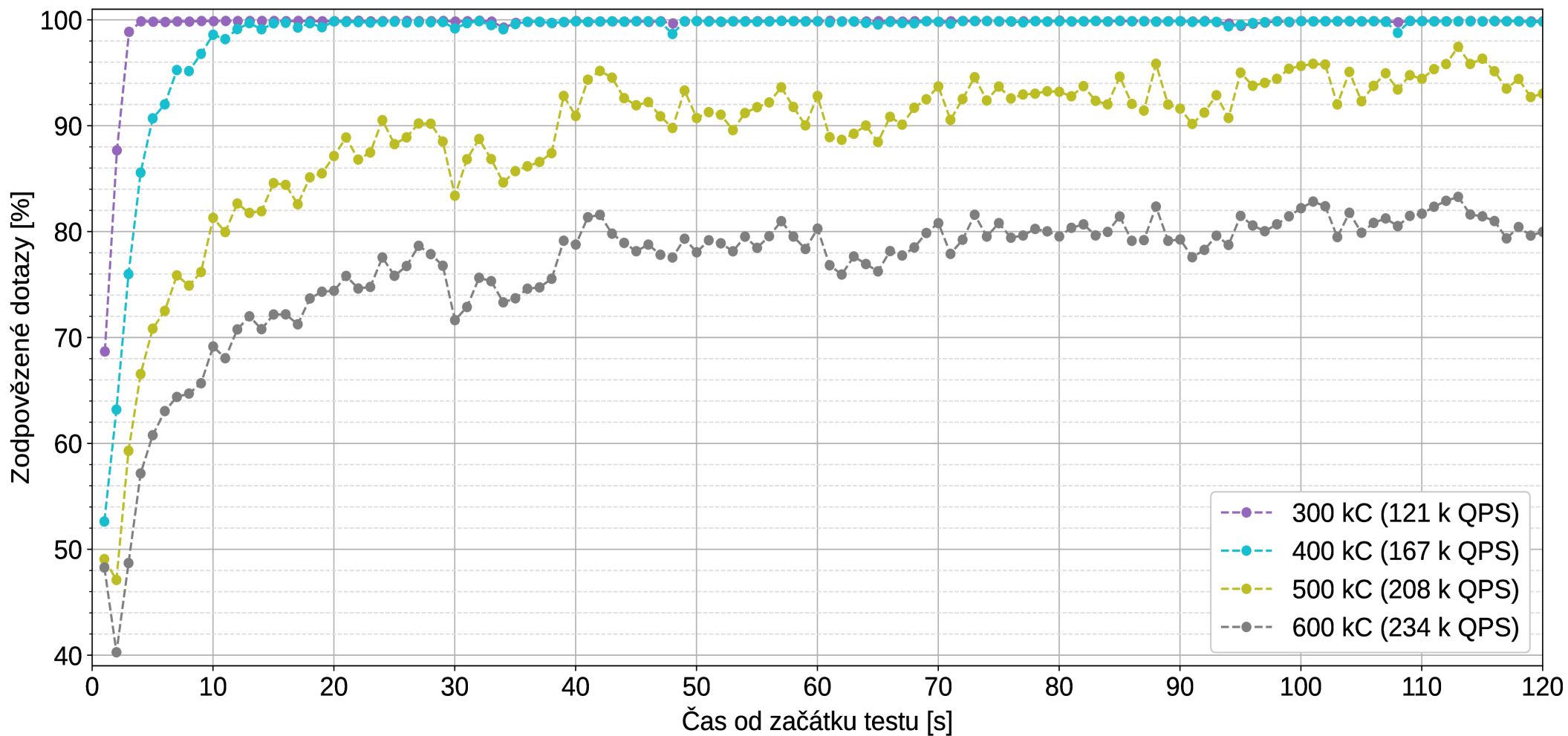


DNS Shotgun: Experiment

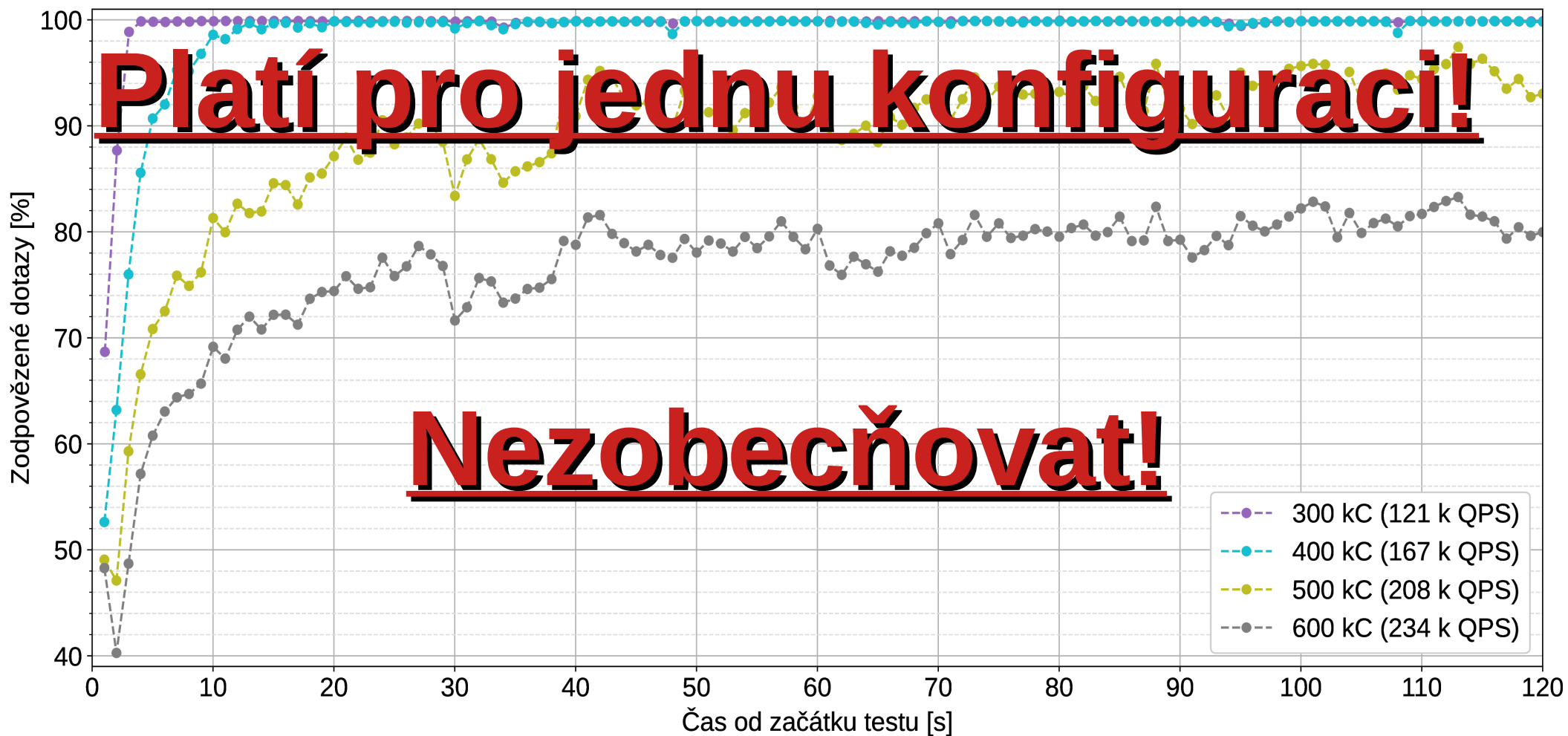
- Provoz: anonymizovaný z univerzity
- Prázdná cache
- Měření 120 s
- Poměry NOERROR/NXDOMAIN/SERVFAIL, latence
- **Zvýšení počtu klientů**
- 8 CPU, 32 GB RAM, 10 ms latence klient $\leftrightarrow$ resolver



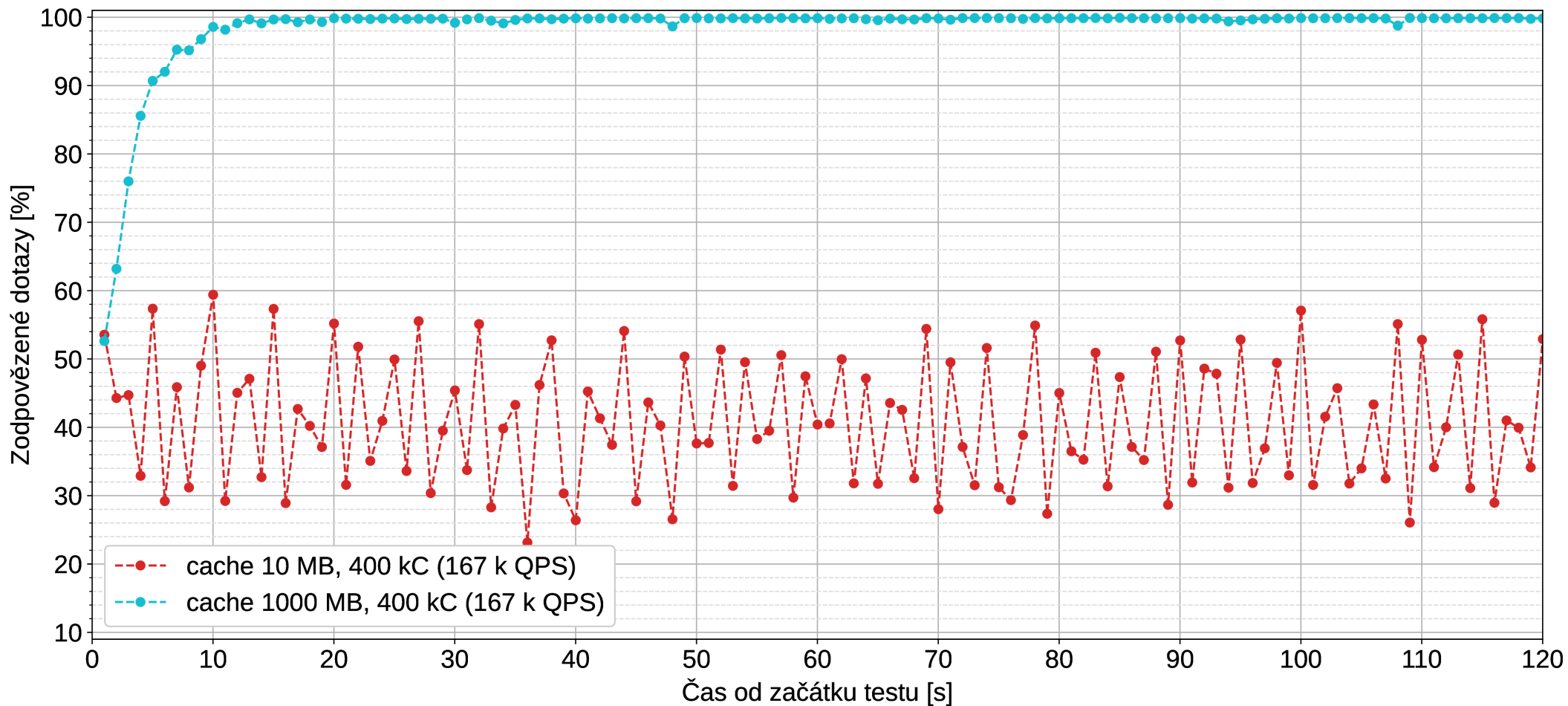
Knot Resolver 5.1.3 – UDP



Knot Resolver 5.1.3 – UDP



Experiment: Vliv velikosti cache

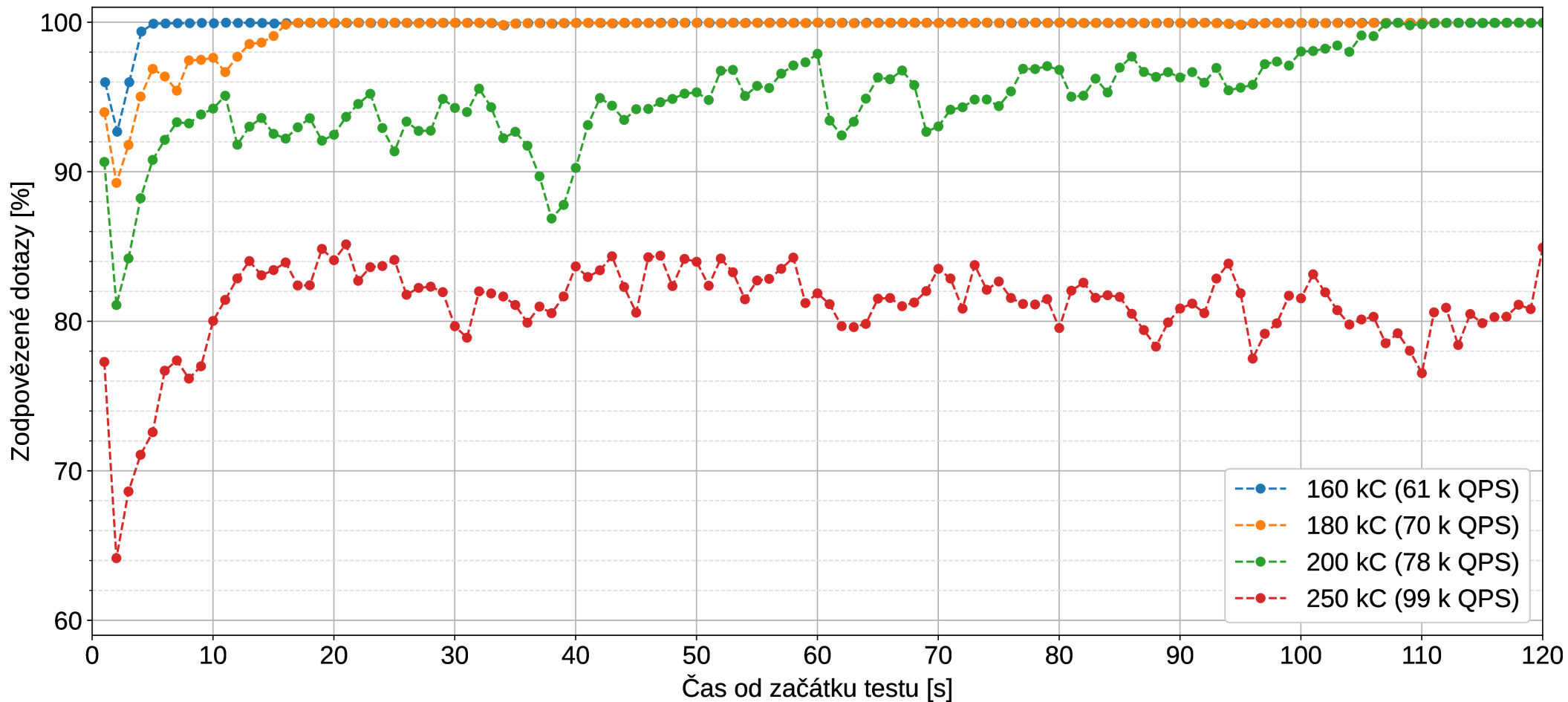


TCP

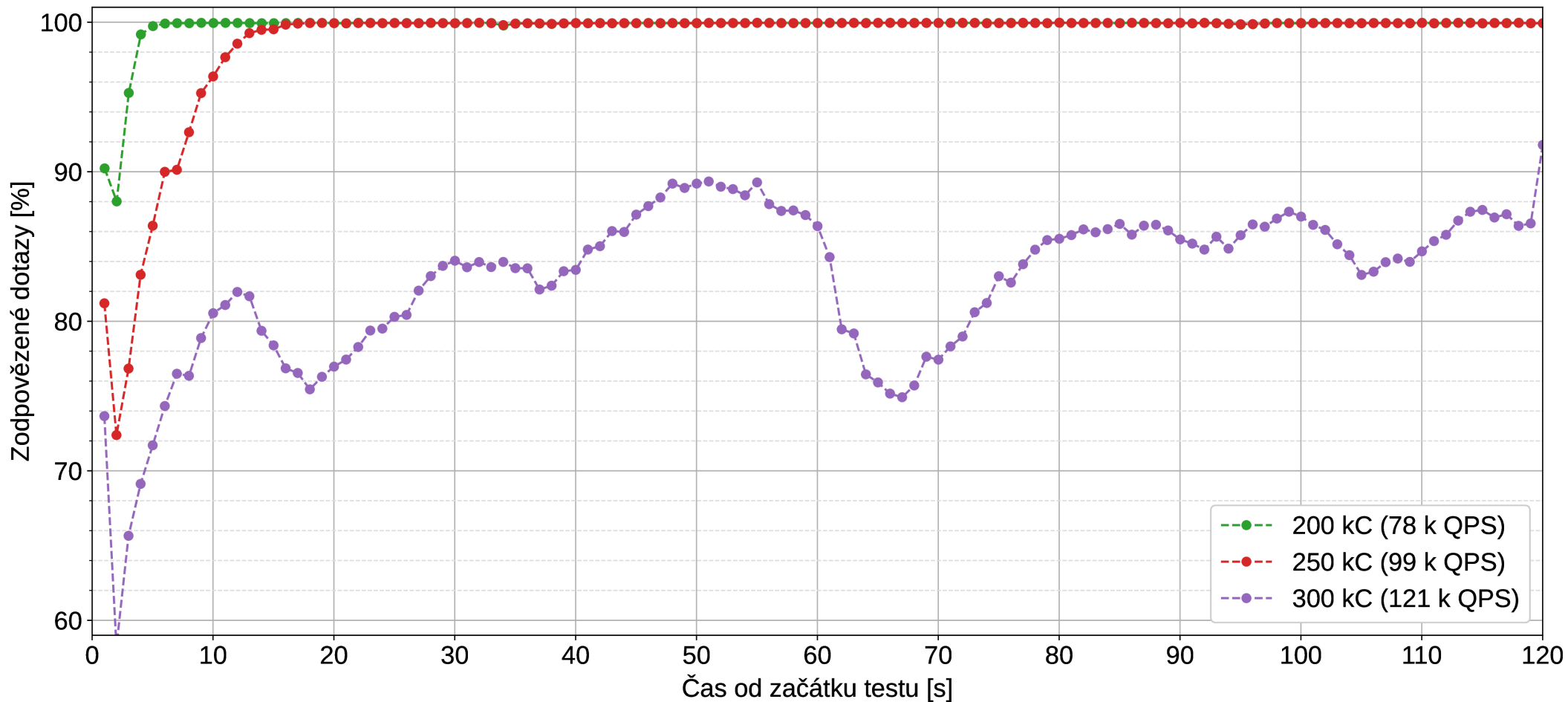
- Základ pro TLS a HTTPS
- Ladění výkonu – dle síťové karty
 - https://www.kernel.org/doc/html/latest/networking/device_drivers/ethernet/intel/ixgb.html#improving-performance
 - Zkusit explicitní CPU affinity pro RX/TX fronty
- Držení spojení ano či ne?
 - Navazování spojení $\Rightarrow$ latence + CPU
 - Držení $\Rightarrow$ paměť



Knot Resolver 5.1.3, TCP klient nedrží spojení



Knot Resolver 5.1.3, TCP klient drží spojení 10 s



Srovnání UDP vs. TCP

Protokol	Obsloužených klientů	Škálování na výkon UDP
UDP	400 k	1
TCP klient zavírá spojení	180 k	2,3
TCP klient drží spojení 10 s	250 k	1,6



TLS

- TLS verze
 - doporučena 1.3
- Podepisovací algoritmus
 - RSA 2k, RSA 3k, P256, Ed25519, ...
- TLS session resumption
 - nový handshake – latence, CPU
 - držení TCP spojení omezuje vliv



Srovnání UDP – TCP – TLS, spojení 10 s

Protokol	Obsloužených klientů	Škálování na výkon UDP
UDP	400 k	1
TCP	250 k	1,6
TLS RSA 2k	80 k	5
TLS RSA 3k	20 k	20
TLS P256	120 k	3,4
TLS Ed25519	120 k	3,4



Srovnání UDP – TCP – TLS, ndrží spojení



Protokol	Obsloužených klientů	Škálování na výkon UDP
UDP	400 k	1
TCP	180 k	2,3
TLS Ed25519	40 k	10



HTTPS

- TCP + TLS + HTTPS
- HTTP verze
 - 1 vs. 2 – verze 1 není doporučena
 - GET / POST
- HTTP komprese
- Hlavičky
 - Content-type ...
- O řád složitější než TLS

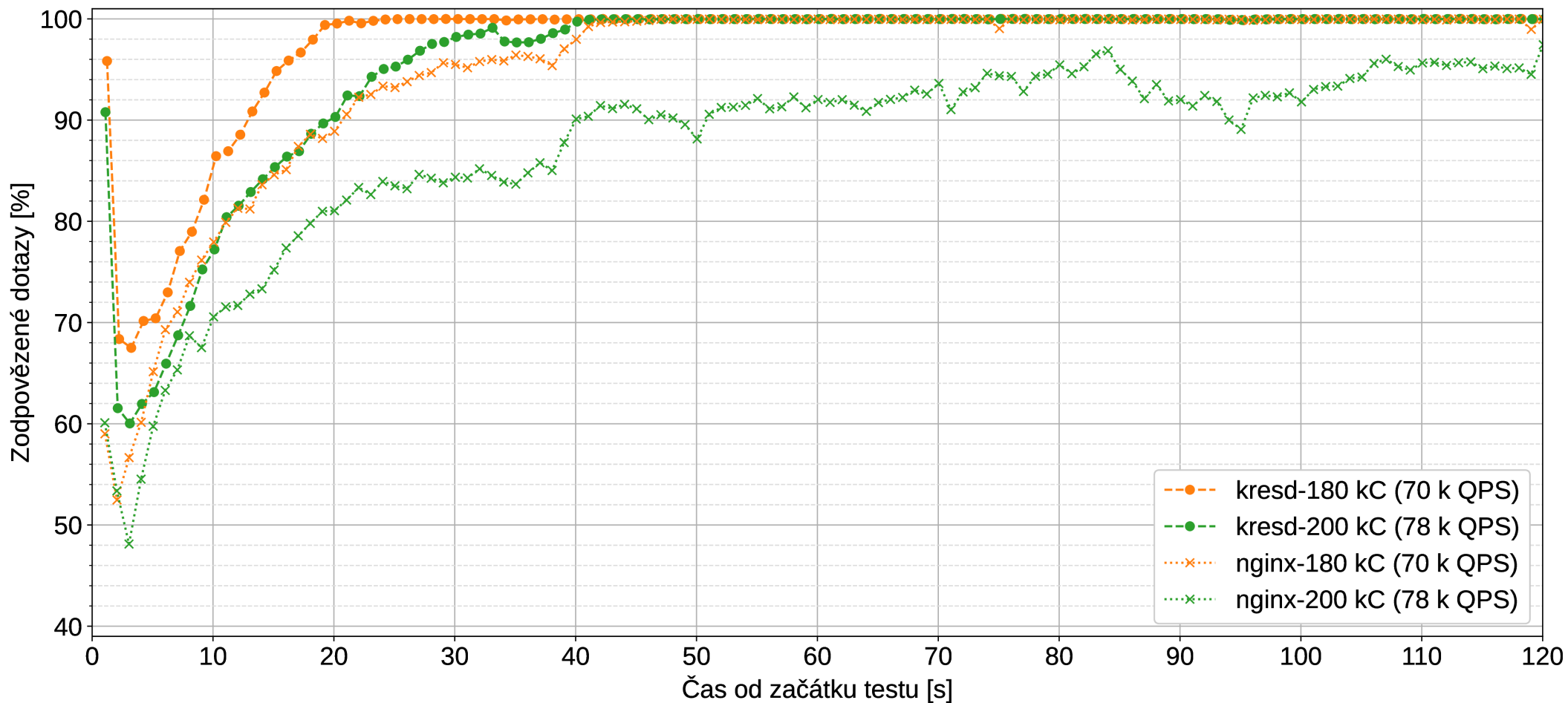


Srovnání UDP – TCP – TLS – HTTPS, spojení 10 s

Protokol	Obsloužených klientů	Škálování na výkon UDP
UDP	400 k	1
TCP	250 k	1,6
TLS Ed25519	120 k	3,4
HTTP + TLS Ed25519	100 k	4



Knot Resolver 5.2.0 HTTPS vs. Nginx: cache hit



Závěr

- TLS – P256 / Ed25519 certifikáty, RSA v nouzi
- Škálování pro DoH
 - 4x – klient musí držet spojení s P256
 - 10x – když spojení nedoručí s P256
 - RSA – když spojení nedoručí ☢
- Pozor na zobecňování
- Měření svépomocí
 - <https://gitlab.nic.cz/knot/shotgun>
- Měření na objednávku
 - knot-resolver@labs.nic.cz

