Benchmarking di server e protocolli DNS sicuri

Nicolapio Gagliarde, Alessandro Macaro, Alberto Montefusco
A.A. 2023/2024

Abstract

DNS è uno dei protocolli fondamentali di Internet, ma a causa della mancanza di politiche di sicurezza sono nati un insieme di attacchi (sia su larga scala che mirati a determinate vittime) contro la privacy, alla disponibilità e all'integrità dei sistemi. Di conseguenza sono state proposte estensioni e varianti di DNS come DNSSEC per garantire l'autenticazione e l'integrità e DNS-over-TLS e DNS-over-HTTPS per garantire anche la riservatezza. Inoltre per ottenere anche l'affidabilità sono state progettate varianti di DNS basate sui due protocolli di trasporto TCP e QUIC. Tuttavia l'utilizzo di algoritmi crittografici, protocolli di trasporto più sofisticati e protocolli situati nei livelli ISO/OSI superiori al trasporto potrebbero causare un incremento delle latenza di risoluzione delle query DNS, incidendo sull'esperienza di navigazione dell'utente. L'obiettivo di questo lavoro è analizzare le prestazioni dei server DNS Bind9, PowerDNS e Techinitium, e di come cambiano al variare dei protocolli: DNS-over-UDP, DNS-over-TCP, DNSSEC, DNS-over-TLS e DNS-over-HTTPS. In particolare, ognuno di questi protocolli è stato testato su ogni server, quindi i dati sono stati analizzati e confrontati considerando uno specifico protocollo su tutti i server e poi uno specifico server per tutti i protocolli. I risultati ottenuti dimostrano che il server più efficiente e più costante nelle risposte in tutti i casi è BIND, inoltre in tutti i test viene riportato l'aumento della latenza media per i protocolli DNSSEC, DNS-over-HTTPS e DNS-over-TLS rispetto DNS-over-UDP e DNS-over-TCP. Inoltre si evince che all'aumentare del numero di richieste si ha un aumento minimo della latenza media in tutti i casi, tranne con DNS-over-TCP eseguito su Technitium, siccome in questo caso l'aumentare del numero di richieste implica una diminuzione della latenza media rispetto DNS-over-UDP. Riguardo Technitium risulta anche che con DNSSEC i primi tre dataset mostrano una latenza media inferiore rispetto DNS-over-UDP. Un altro risultato particolare è dovuto PowerDNS con DNS-over-TCP che presenta una latenza media inferiore rispetto DNS-over-UDP, questo fenomeno avviene anche in Technitium. Infine considerando le latenze massime ottenute, tali latenze risultano comunque in linea con i tempi di risposta riportati nei lavori correlati.

1 Introduzione

1.1 Il protocollo DNS

Il protocollo Domain Name System (DNS) permette di risolvere domini WEB comprensibili dall'uomo in indirizzi IPv4, con l'avvento di IPv6 si è aggiunta anche la risoluzione dei domini associati alla nuova versione del protocollo IP. DNS però non si occupa soltanto di risolvere i domini dei siti WEB, infatti permette anche il corretto funzionamento della posta elettronica, ha un ruolo fondamentale nella "gestione di Internet", ad esempio ogni Internet Service Provider, per rispettare le norme dettate dal RIPE, deve dichiarare i propri server DNS con i record PTR relativi ai propri indirizzi IP. Questo protocollo, con il crescere della rete Internet, è stato reinventato dandogli anche la responsabilità di gestire blacklist anti-spam, favorisce la transizione da IPv4 a IPv6 grazie a DNS64, permette la gestione di sistemi complessi generando alias, record CNAME e logiche di bilanciamento del carico come Round-robin DNS. Quindi DNS ha un ruolo fondamentale nella rete Internet e nel WEB, purtroppo però non è stato progettato con un approccio orientato alla sicurezza. Infatti si basa principalmente sul protocollo di trasposrto UDP che non offre nessuna garanzia di sicurezza, in alternativa è possibile utilizzare TCP che offre affidabilità, ma anche in questo caso la sicurezza è pari a zero. Quindi con l'aumentare delle problematiche di sicurezza in Internet e nel WEB, e viste le gravi implicazioni che un attacco contro un sistema DNS potrebbe avere anche in intere nazioni, è nato DNSSEC che offre principalmente integrità e autenticità delle risposte DNS. Per completare il modello Confidentiality Integrity and Availability si sono aggiunti i protocolli DNS-over-TLS e DNS-over-HTTPS che offrono anche la confidenzialità.

1.2 Lo scopo di questo lavoro

Utilizzare DNS aggiungendo tecniche crittografiche per il controllo dei certificati e di firme digitali, suite di protocolli crittografici e aggiungendo protocolli orientati alla connessione significa avere inevitabilmente un overhead maggiore rispetto DNS basato su UDP, tale overhead si potrebbe riscontrare ad esempio in latenze di risoluzione maggiori, sovraccarico dei server DNS e quindi riduzione del numero di query risolvibili in un certo tempo. Lo scopo di questo lavoro è selezionare tre server DNS in base alla popolarità di utilizzo, configurare i protocolli DNS-over-UDP, DNS-over-TCP, DNS-over-HTTPS, DNS-over-TLS e DNSSEC e analizzare le differenze prestazionali dei protocolli, in particolare analizzare l'overhead aggiunto dovuto alla sicurezza. Ma allo stesso tempo analizzare il comportamento e le prestazioni dei server DNS e di come variano all'aumentare del numero di richieste e al variare del protocollo utilizzato, e quindi determinare la capacità di gestire le versioni sicure di DNS.

1.3 Risultati

I risultati ottenuti si dividono in due gruppi: i risultati ottenuti dal benchmarking di uno specifico protocollo testato su tutti i server e i risultati ottenuti analizzando l'output del benchmarking dal punto di vista opposto, cioè dato uno specifico server analizzare il suo comportamento testando tutti i protocolli. Riguardo al primo gruppo si evince che BIND è il server più efficiente, infatti in tutti i casi risolve il 95% delle richieste in un range di latenze molto minore rispetto agli altri server. Ad esem-

pio prendendo il caso di DNS-over-UDP, dato il range di latenze in cui BIND risolve il 95% delle richieste, gli altri server risolvono il 300% di richieste in meno. Anche considerando l'andamento delle risposte BIND risulta il più costante siccome non presenta incrementi di latenza improvvisi e ingiustificati come avviene con PowerDNS e Technitium. Tali risultati vengono riassunti dalle CDF, infatti in tutti i grafici CDF il server che raggiunge prima degli altri il valore 1 all'aumentare della latenza è BIND. Riguardo le differenze in termini di efficienza di tutti i protocolli eseguito su un singolo server è ben osservabile l'overhead aggiunto per garantire la sicurezza, infatti in generale si evince un aumento della latenza media di DNS-over-HTTPS rispetto DNS-over-TLS, di DNS-over-TCP rispetto DNS-over-UDP, di DNSSEC rispetto DNS-over-UDP. Anche osservando le CDF si può notare ad esempio che la CDF di DNS-over-HTTPS è identica a DNS-over-TLS tranne per il fatto che risulta traslata verso destra indicando appunto l'aumento della latenza. Inoltre si evince che all'aumentare del numero di richieste si ha un aumento minimo della latenza media in tutti i casi. I risultati non attesi sono: DNS-over-TCP su Technitium con l'aumentare del numero di richieste si ha una diminuzione della latenza media rispetto DNS-over-UDP; anche con DNSSEC per i primi tre dataset succede lo stesso fenomeno. Un altro risultato particolare è dovuto a PowerDNS con DNS-over-TCP che presenta una latenza media inferiore rispetto DNS-over-UDP, questo fenomeno avviene anche in Technitium. Infine anche considerando le latenze massime ottenute, tali latenze risultano comunque in linea con i tempi di risposta riportati nei lavori correlati.

1.4 Struttura del paper

Oltre questo capitolo introduttivo il paper è strutturato come segue:

2. Background: una brevissima introduzione al protocollo DNS e ai protocolli UDP, TCP, TLS, HTTPS e DNSSEC;
3. Related Works: una descrizione di due lavori recenti che si avvicinano al nostro scopo in cui viene useguito il benchmarking di alcuni server e resolver DNS;
4. Metodi, tools e configurazioni:
   - 4.1. nella prima sezione vengono vengono riportati i dataset utilizzati, quindi il dataset di partenza, il formato dei records, il dataset per il file di zona dei server DNS e i cinque dataset utilizzati per il benchmarking;
   - 4.2. nella seconda sezione vengono riportate le caratteristiche delle macchine usate al fine di garantire la replicabilità delle sperimentazioni;
   - 4.3. nella terza sezione vengono descritti i tools utilizzati per verificare il corretto funzionamento dei server e per effettuare il benchmarking, in particolare dnsperf, dig, kdig e uno script creato ad-hoc utilizzando kdig;
   - 4.4. nella quarta sezione vengono descritti i metodi utilizzati per calcolare dati statistici e matematici dai risultati ottenuti dai tools di benchmarking e vengono descritti i grafici utilizzati per visualizzare tali dati;
   - 4.5. nella sezione finale vengono descritti i server DNS scelti, cioè BIND9, PowerDSN e Technitium, e per ognuno di essi vengono riportate le configurazioni dei protocolli suddetti.
5. Benchmarking:
   - 5.1. Un protocollo su tutti i server: in questa sezione vengono descritti i dati ottenuti dal benchmarking di uno specifico protocollo testato su tutti i server;
   - 5.2. Un server testato con tutti i protocolli: in questa sezione i dati vengono analizzati dal punto di vista opposto, quindi dato uno specifico server si osserva il variare del comportamento in base ai protocolli.
6. Limitazioni dello studio e sviluppi futuri: vengono descritte le limitazioni presenti in questo studio, limitazioni che coincidono con i possibili sviluppi futuri.
7. Data availability: vengono riportati gli URL in cui è possibile trovare le macchine virtuali, gli script, i dataset, i grafici e altri documenti utilizzati in questo lavoro.

2 Background

Un server DNS è principalmente un registro di domini che quando viene interrogato da un client risolve il dominio richiesto inviando l'IP corrispondente. DNS è stato progettato inizialmente su UDP e TCP, il primo è connectionless e offre alte performance però non offre affidabilità, TCP invece offre affidabilità ma causa un overhead maggiore dovuto all'handshake della connessione. Inoltre con la creazione del protocollo QUIC che è basato su UDP, si utilizza TLS e varie tecniche per migliorare l'affidabilità ed è stato realizzato DNS-over-QUIC.

Per risolvere i problemi di sicurezza di DNS sono stati creati i seguenti protocolli:

- DNS-over-TLS: usa una connessione TLS, e quindi TCP, per garantire integrità e confidenzialità. Vengono scambiati due messaggi per derivare dalle chiavi asimmetriche una chiave simmetrica che viene utilizzata per cifrare le richieste e le risposte DNS. Durante il processo il client verifica l'identità del server utilizzando i certificati digitali
- DNS-over-HTTPS: prevede un layer addizionale sopra TLS, una volta che la connessione TLS viene stabilita vengono creati streams multipli del protocollo HTTP su cui vengono scambiate richieste e risposte DNS

- DNSSEC: utilizzando certificati e firme digitali questo protocollo fornisce autenticazione dei dati, autenticazione di denial of existence, e integrità

3 Related works

In questa sezione vengono analizzati lavori presenti in letteratura incentrati sulle performance di alcune implementazioni di server DNS e protocolli.
Nel lavoro di [7] viene misurato il tempo di risposta di una query DNS e il tempo di caricamento della pagina WEB utilizzando il protocollo DNS-over-UDP, DNS-over-TLS e DNS-over-HTTPS. Il tool utilizzato per salvare il tempo di caricamento della pagine è Selenium, invece per i tempi di risposta delle query DNS sono state utilizzate le due librerie C: getdns e libcurl. L'obiettivo di questo lavoro è quello di analizzare le performance dei protocolli DNS-over-UDP, DoT e DoH utilizzando i resolver di Google, Cloudflare e Quad9 con una rete in condizioni non ottimali. Per simulare le condizioni non ottimali è stato configurato il traffic shape, il loss rate dei pacchetti e la latenza. Riguardo i siti web visitati gli autori hanno collezionato gli HTTP Archive objects e le query DNS dei primi 1000 siti della Tranco top-list [10], inoltre sono stati presi gli ultimi 1000 siti dei primi 100000 per analizzare le differenze tra i siti più usati e i meno usati. Tra i vari confronti ci sono due risultati sorprendenti: per le query più lente DoH ha tempo di risposta medio e deviazione standard migliori di DNS-over-UDP dovuto probabilmente alla cache del DNS wire format, e con una rete che perde pacchetti il tempo di caricamento della pagina è più veloce usando DoT e DoH rispetto DNS-over-UDP grazie all'utilizzo di TCP.
In questo lavoro [8] vengono esaminate le performance dei server BIND, NSD, Knot DNS e YADIFA utilizzati con il protocollo DNS64. Vengono prese in considerazione diverse condizioni come il numero di core attivi, la taglia del file di zona, i timeout e il tipo di processore. Il tool di benchmarking utilizzato è dns64perf++, per quanto riguarda la metodologia gli autori seguono l'RFC 8219. Vengono inviate richieste AAAA a un rate costante per almeno 60 secondi, si attendono le risposte e si controlla se sono valide (cioè devono contenere un record AAAA e non deve essere scaduto il timeout).

- Se il numero di risposte valide è uguale al numero di richieste inviate viene aumentato il rate e rieseguito il test;

- Se il numero di risposte valide è inferiore al numero di richieste il rate viene decrementato e rieseguito il test.

Dai risultati del test di scalabilità risulta che all'umentare dei core aumentano le prestazioni dei server tranne di YADIFA, dai test in cui si raddoppia la taglia del file di zone si evince una degradazione delle performance solo con BIND, infine risulta che NSD e KnotDNS offrono performance migliori di BIND e YADIFA

4 Metodi, tools e configurazioni

In questa sezione vengono descritti i dataset utilizzati per creare la zona e per creare i dataset di benchmarking, le caratteristiche delle macchine usate, i tools utilizzati per effettuare il benchmarking, i grafici utilizzati per descrivere i risultati ottenuti e la configurazione dei tre server DNS testati.

4.1 Dataset usati

Il dataset utilizzato in questo lavoro è stato creato a partire dalla lista di URL "italy" presente in [1]. Ogni URL è stato innanzittutto sottoposto a un processo di pulizia per rimuovere caratteri non ammessi dallo standard URL e poi utilizzato per creare un record di tipo A nel file di zona presente nei server DNS, per un totale di due milioni di record. Il formato del record A è il seguente: "url IN A indirizzoIP", dove "url" è l'URL preso dalla lista "italy" e "indirizzoIP" è un indirizzo IPv4 generato randomicamente. Il record è di tipo A siccome in questo lavoro ci concentriamo sulla risoluzione di domini associati a indirizzi IPv4, l'indirizzo IP viene generato randomicamente siccome si è interessati a testare il server DNS e non il server WEB su cui è ospitato il sito. Per la costruzione dei dataset di richieste utilizzati da dnsperf sono state seguite le specifiche del tool stesso [9], quindi ogni dataset ha un insieme di records inseriti precedentemente nei server DNS e un insieme di records NON inseriti nei server che quindi causano risposte NXDOMAIN. Sono stati creati i seguenti dataset:

- Dataset_50_10: 50mila records presenti nei server DNS e 10mila non presenti

- Dataset_100_20: 100mila records presenti nei server DSN e 20mila non presenti

- Dataset_200_40: 200mila records presenti nei server DSN e 40mila non presenti

- Dataset_400_80: 400mila records presenti nei server DSN e 80mila non presenti

- Dataset_800_160: 800mila records presenti nei server DSN e 160mila non presenti

4.2 Caratteristiche Hardware, Virtual Machine e versioni

Per effettuare il benchmarking si è deciso di utilizzare le Virtual Machine, una decisione motivata da diversi test precedentemente effettuati.
Inizialmente, è stato condotto un test utilizzando due PC differenti (uno per il lato client e uno per il lato server), ma si sono manifestati diversi problemi nella comunicazione tra le due macchine e nelle schede di rete delle Virtual Machine, oltre a una latenza di rete troppo variabile. Successivamente si è optato per un approccio diverso, in cui il test veniva eseguito su un singolo PC, ma con due Virtual Machine differenti (una configurata come client e l'altra

come server). Anche qui si sono riscontrati numerosi problemi dovuti al troppo carico computazionale.
Infine, si è giunti alla soluzione definitiva di utilizzare una singola Virtual Machine (di seguito "VM") con funzionalità sia server che client per effettuare i test. Quindi per ogni server e per ogni protocollo si è utilizzata una VM differente, per un totale di 15. L'ambiente di virtualizzazione utilizzato è VirtualBox versione 7.0.4. Le caratteristiche di ogni VM sono:

- Sistema operativo: Debian 12 64-bit
- Memoria RAM: 4GB
- Numero processori: 3
- Execution cap: 100%

Le caratteristiche del PC utilizzato sono:

- Sistema operativo: Windows 10 Home
- Memoria RAM: 8GB
- Processore: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
- Numero di core logici: 4

Tra ogni sessione di benchmarking è stato eseguito uno spegnimento del server seguito dal riavvio della macchina virtuale, al fine di eliminare eventuali residui di buffer, cache e file temporanei, garantendo così una valutazione più accurata delle prestazioni. Inoltre i benchmark sono stati sempre eseguiti in modo sequenziale, quindi mai contemporaneamente. Per ridurre ulteriormente l'overhead sono stati terminati i processi non necessari sia sul PC utilizzato che sulla VM.

4.3 Tools per il benchmarking: dnsperf, dig e kdig

Per testare il corretto funzionamento e configurazione dei server è stato usato il tool dig [2] siccome permette di effettuare anche controlli relativi ai protocolli crittografici utilizzati da DoT, DoH e DNSSEC.

Per effettuare il benchmarking dei protocolli DNS-over-UDP, DNS-over-TCP e DNS-over-TLS, si è deciso di utilizzare il tool *dnsperf* [9] versione 2.13.1 in quanto il suo utilizzo risulta molto semplice, fornisce metriche accurate come latenza e throughput e viene considerato uno dei tool più utilizzato a questo scopo siccome è stato sviluppato da Nominum/Akamai e DNS-OARC. Inoltre è possibile fornire al tool liste di richieste DNS salvate in file. Purtroppo dnsperf non permette di eseguire richieste DNSSEC e DNS-over-HTTPS (in realtà supporta HTTPS ma dopo un certo numero di query va in uno stato di errore), quindi dopo aver valutato varie alternative come shotgun [4], Domain Name Speed Benchmark [3] e dnsjit [6] risultate poco efficaci, si è deciso di utilizzare kdig [5] versione 3.2.6 all'interno di uno script realizzato ad hoc per effettuare richieste multiple e tenere traccia dei nanosecondi necessari per risolvere la richiesta, di seguito di farà riferimento a tale script con "scriptKdig".

Infine riportiamo il fatto che i suddetti tool sono soggetti a errori, infatti durante i vari benchmarking si sono presentate latenze di valore negativo o con valori troppo alti per essere veri. Ad esempio in molti casi per alcune richieste veniva riportato una latenza in nanosecondi convertibile in vari giorni. Per motivi di visualizzazione dei dati si è deciso di rimuovere la parte intera e considerare solo le cifre dopo la virgola, è stata presa questa decisione siccome il numero di richieste con latenza errata era insignificante rispetto alla taglia del dataset intero. Ad esempio poche centinaia di richieste per dataset da centinaia di migliaia. Inoltre prima di modificare le latenze errate si è cercato di identificare eventuali pattern nei domini che causavano tali anomalie, ma non sono stati trovati pattern significativi.

4.4 Visualizzazione e analisi dei dati

In questa sezione si descrivono i risultati immediati ottenuti dai tool descritti nella sezione 4.3 e i risultati ottenuti mediante tecniche di manipolazione, estrazione e visualizzazione.

Il tool dnsperf utilizzato per il benchmarking dei protocolli DNS-over-UDP, DNS-over-TCP e DNS-over-TLS, fornisce i seguenti dati: il tempo di risposta per ogni richiesta effettuata, numero di richieste inviate, completate e perse, il numero di risposte NOERROR e NXDOMAIN, il numero di query per secondo, latenza minima, massima, media e deviazione standard. Inoltre dnsperf fornisce un insieme di bins, ogni bin è caratterizzato da un range di latenze e il numero di richieste il cui tempo di risposta è compreso nel range, in questo caso la latenza viene quantizzata in bins con una risoluzione di circa il 3% e il range della latenza per ogni bins viene incrementato logaritmicamente. Questo viene fatto da dnsperf per permettere all'utente di mostrare i bins in appositi grafici senza ulteriori elaborazioni.

Riguardo il benchmark dei protocolli DNSSEC e DNS-over-HTTPS è stato utilizzato scriptKdig, il cui output è una lista di latenze. Quindi sono stati creati ulteriori script per estrarre la latenza minima, massima, la media e la deviazione standard. Dopodiché è stato realizzato uno script che, applicando lo stesso procedimento statistico di dnsperf, ha permesso l'estrazione dei bins.

Dopodiché per permettere il confronto tra protocolli e server, i dati vengono presentati attraverso quattro tipi di grafici. In particolare:

- Grafici a barre dei bins: i bins vengono rappresentati utilizzando dei grafici a barre in cui ogni barra rappresenta un bin, quindi sull'asse delle ordinate è presente il numero di richieste nel bin e sull'asse delle ascisse è presente il range di latenza del bin. Tale grafico permette di visualizzare immediatamente la distribuzione dei bins, di conseguenza permette di capire quante richieste vengono risolte in un determinato range di latenze da un determinato server;

- Grafico delle latenze: ogni punto di questo grafico rappresenta una determinata richiesta e il suo tempo di risoluzione. Quindi sull'asse delle ascisse è presenta la latenza e sull'asse delle ordinate troviamo il numero di richieste. Tale grafico permette di visualizzare l'andamento delle risposte DNS e anomalie nelle risposte come picchi di latenze troppo alte;

- Cumulative Distribution Function (CDF): una CDF indica la probabilità che il tempo di risoluzione di una query DNS sia minore di una certa soglia. Di conseguenza avendo sull'asse delle ordinate la probabilità e sull'asse delle ascisse la latenza è possibile vedere quale server offre una certa prestazione con una certa probabilità;

- Grafico a barre per valore minimo, massimo, medio e deviazione standard: in questo grafico si ha una barra per ogni server, la barra indica la media della latenza di risoluzione delle query. Per ogni barra sono presenti tre elementi grafici per rappresentare la richiesta DNS con tempo di risoluzione minima, massima e la deviazione standard.

4.5 Server DNS

Considerando vari fattori come la popolarità, la facilità di utilizzo, la disponibilità e la qualità della documentazione e i lavori già presenti in letteratura sono state scelte le tre implementazioni di server DNS: BIND9, Technitium e PowerDNS con dnsdist.

4.5.1 Bind9

BIND è una suite di software mantenuta dalla Internet Systems Consortium per implementare sistemi DNS. Nella suite è presente il componente named che funge sia da server DNS autoritativo per le zone DNS che da resolver ricorsivo. Con questo server sono stati configurati i seguenti protocolli:

- DNS-over-UDP e DNS-over-TCP: dopo aver installato BIND è stato creato il file di zona contente i due milioni di records come detto sopra, il file di zona è stato poi aggiunto al file named.conf.local. Inoltre è stato modificato il file named.conf.option per configurare l'interfaccia di loopback e l'IP su cui ricevere le richieste DNS.

- DNSSEC: innanzitutto è stata generata la zone-signing key (ZSK) e la key-signing key (KSK) con il comando dnssec-keygen settando l'algoritmo ECDSA P-256 e SHA256. Queste chiavi sono state poi utilizzate per firmare la zona con il comando dnssec-signzone, è stato fatto il reload della zona e poi aggiunta al file named.conf.local

- DNS-over-TLS: per configurare questo protocollo sono state aggiunte le righe "tls-port 853;" e "listen-on port 853 tls ephemeral {127.0.0.1;10.0.2.15;};" nel file named.conf.options

- DNS-over-HTTPS: in questo caso è stata aggiunta la riga " listen-on tls ephemeral http local {any;};" in named.conf.options e " http local {endpoints{"/dns-query";}};" nel file named.conf.local

La versione utilizzata in questo lavoro è BIND9, di seguito verrà indicata con "BIND" o con "BIND9".

4.5.2 Technitium

Anche Technitium è un server DNS autoritativo e open source, inoltre può essere usato come resolver ricorsivo. E' possibile installarlo con una configurazione minima ed offre un interfaccia web avanzata. Con questo server sono stati configurati i seguenti protocolli:

- DNS-over-UDP e DNS-over-TCP: dopo aver installato technitium sono stati caricati 1,4 milioni di record utilizzando l'interfaccia web e il tool xclip. Purtroppo technitium non permette di inserire il dataset completo di due milioni di record.

- DNSSEC: è stata creata una zona vuota, dall'interfaccia web è stata poi firmata impostando ECDSA, P256 e SHA256, per la Proof of non-existence è stato impostato NSEC. Successivamente sono stati importati i record.

- DNS-over-TLS: innanzitutto sono stati generati i certificati usando il comando "openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem", attraverso l'interfaccia web sono stati poi configurati nel sistema, sono state impostate le porte e nella sezione forwarder è stato aggiunto "tls-certificate-domain:853"

- DNS-over-HTTPS: la configurazione di questo protocollo è identica a quella di DoT con la differenza che in forwarders va inserita la riga "https://tls-certificate-domain/dns-query"

La versione di Technitium utilizzata in questo lavoro è la 11.5.3.

4.5.3 PowerDNS e dnsdist

PowerDNS è un server DNS leader in ambito commerciale e open source, offre un alta scalabilità ed è in grado di funzionare con vari backend. In questo lavoro è stato scelto gsqlite3 siccome è quello più utilizzato e inoltre è stato installato DNSdist per attivare l'uso di DoH e DoT.

Con questo server sono stati configurati i seguenti protocolli:

- DNS-over-UDP e DNS-over-TCP: è stato installato PowerDNS e aggiunto il file di zona nel file named.conf

- DNSSEC: è stato modificato il file pdns.conf aggiungendo le istruzioni: launch=gsqlite3, gsqlite3-database=/var/lib/powerdns/pdns.sqlite3 e gsqlite3-dnssec=yes

- DNS-over-TLS: dopo aver installato dnsdist è stato creato il file dnsdist.conf in cui è stata aggiunta la riga "addTLSLocal('127.0.0.1', '/etc/ssl/certs/certificate.pem', '/etc/ssl/certs/key.pem')" quindi poi sono stati creati i certificati usando "openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem"

- DNS-over-HTTPS: anche in questo caso è stato utilizzato dnsdist, il file dnsdist.conf con la riga "addDOHLocal('127.0.0.1', '/etc/ssl/certs/certificate.pem', '/etc/ssl/certs/key.pem'" e i certificati generati anche per DoT.

La versione di PowerDNS utilizzata in questo lavoro è la 4.8.3, la versione di dnsdist è 1.8.2.

5 Benchmarking

Questa sezione si divide in due parti: nella prima vengono riportati i dati ottenuti dal benchmarking effettuato su tutti i server dato uno specifico protocollo; nella seconda sezione vengono riportati i dati dal punto di vista opposto cioè dato uno specifico server vengono riportati i dati di ogni protocollo testato sul server.

5.1 un protocollo su tutti i server

5.1.1 DNS over UDP

Innanzitutto sono stati analizzati i grafici dei bins dei benchmarking di DNS-over-UDP sui tre server, da questi grafici si evince che il server in grado di risolvere il 95% delle richieste in un range di latenze più basso rispetto agli altri server è BIND. Quindi prendendo come riferimento tale range risultano enormi differenze in termini di numero di richieste risolte da PowerDNS e Technitium. Queste differenze vengono riassunte nella seguente tabella:

	Dataset	Range di latenze	Numero di Risposte
BIND	**60000**	0.000496 - 0.003263	59404
PowerDNS			14377
Technitium			13337
BIND	**120000**	0.000384 - 0.003775	118544
PowerDNS			37419
Technitium			21159
BIND	**240000**	0.000504 - 0.003903	236575
PowerDNS			72122
Technitium			40942
BIND	**480000**	0.000400 - 0.003519	475272
PowerDNS			142853
Technitium			53373
BIND	**960000**	0.000448 - 0.003775	950013
PowerDNS			287386
Technitium			107791

Table 1: DNS over UDP

Osservando il numero di richieste, con l'aumentare della dimensione del dataset la differenza di risposte è notevole

- Prendendo in considerazione Bind e PowerDNS si passa da una percentuale del 313.19% nel dataset più piccolo ad una percentuale del 230.57% nel dataset più grande

- Prendendo in considerazione PowerDNS e Technitium si passa da una percentuale del 7.8% nel dataset più piccolo ad una percentuale del 166.61% nel dataset più grande

Tuttavia ricordiamo che il grafico dei bins non considera l'ordine cronologico delle richieste, ma soltanto la loro distribuzione. Quindi risulta essere utile analizzare anche il grafico delle latenze per vedere l'andamento delle richieste nel tempo.
In particolar modo, dal grafico delle latenze (Figura 9) si può notare chiaramente che BIND rimane costante nella parte più inferiore del grafico, mentre Technitium e PowerDNS presentano molteplici picchi che variano da latenze paragonabili a quelle di BIND fino a latenze superiori senza però evidenziare pattern ben definiti. L'unico pattern ben visibile in questo grafico è dato da Technitium, in particolare dalle ultime 100000 richieste. Siccome nei grafici delle latenze per i dataset precedenti tale pattern non si presenta crediamo che ciò sia dovuto a errori (discussi nella sezione 4.3) del tool dnsperf.
Anche il grafico delle CDF conferma quanto detto in precedenza: BIND converge molto rapidamente a 1, mentre gli altri due server convergono ad uno più lentamente. In particolare Technitium risulta essere il più lento.

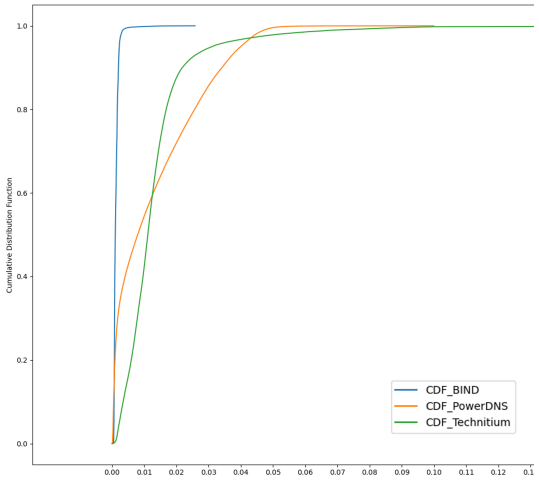

Figure 1: Cumulative Distribution Function di DNS-over-UDP sui tre server - Dataset da 960000

5.1.2 DNS over TCP

Innanzitutto la prima differenza sostanziale rispetto al confronto precedente è che il protocollo TCP offre affidabilità e ciò causa un overhead maggiore causato dall'handshake della connessione.
Analizzando i grafici dei bins dei benchmarking di DNS-over-TCP sui tre server è evidente che il server in grado di risolvere il 95% delle richieste in un range di latenze più

basso rispetto agli altri server si riconferma essere BIND. Quindi prendendo come riferimento tale range risultano enormi differenze in termini di numero di richieste risolte da PowerDNS e Technitium. Queste differenze vengono riassunte nella seguente tabella:

	Dataset	Range di latenze	Numero di Risposte
BIND	**60000**	0.002752 - 0.010751	59302
PowerDNS			43790
Technitium			31962
BIND	**120000**	0.002688 - 0.007679	110028
PowerDNS			94994
Technitium			41174
BIND	**240000**	0.002496 - 0.012031	236212
PowerDNS			236004
Technitium			160177
BIND	**480000**	0.002816 - 0.012287	476014
PowerDNS			453099
Technitium			297147
BIND	**960000**	0.002432 - 0.011007	954716
PowerDNS			729664
Technitium			595255

Table 2: DNS over TCP

Osservando il numero di richieste, con l'aumentare della dimensione del dataset la differenza di risposte è notevole

- Prendendo in considerazione Bind e PowerDNS si passa da una percentuale del 35.42% nel dataset più piccolo ad una percentuale del 30.84% nel dataset più grande

- Prendendo in considerazione PowerDNS e Technitium si passa da una percentuale del 37.01% nel dataset più piccolo ad una percentuale del 22.58% nel dataset più grande

In questo caso i grafici delle latenze (in particolare la Figura 10) non si discostano molto da quelli di UDP a parte il fatto di avere latenze più alte giustificate dal protocollo sottostante. Si rende solo più evidente che Technitium presenta picchi più alti e più numerosi rispetto a PowerDNS.
Anche il grafico delle CDF conferma quanto detto in precedenza: BIND converge molto rapidamente a 1, mentre gli altri due server convergono ad uno più lentamente. In particolare Technitium risulta essere il più lento.

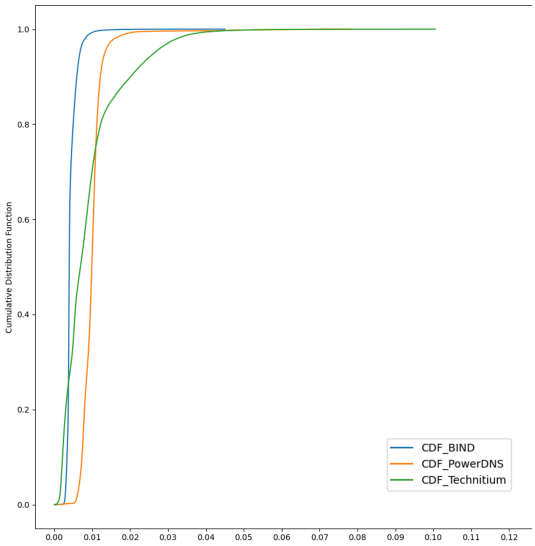

Figure 2: Cumulative Distribution Function di DNS-over-TCP sui tre server - Dataset da 960000

5.1.3 DNSSEC

Analizzando i grafici dei bins dei benchmarking di DNSSEC sui tre server è evidente che il server in grado di risolvere il 95% delle richieste in un range di latenze più basso rispetto agli altri server risulta essere sempre BIND. Quindi prendendo come riferimento tale range risultano enormi differenze in termini di numero di richieste risolte da PowerDNS e Technitium. Queste differenze vengono riassunte nella seguente tabella:

	Dataset	Range di latenze	Numero di Risposte
BIND	**60000**	0.002817 - 0.006472	59651
PowerDNS			18872
Technitium			16503
BIND	**120000**	0.002768 - 0.007451	118983
PowerDNS			47367
Technitium			29117
BIND	**240000**	0.002802 - 0.007187	238461
PowerDNS			95638
Technitium			49513
BIND	**480000**	0.002724 - 0.006688	477072
PowerDNS			181669
Technitium			60074
BIND	**960000**	0.002748 - 0.007253	954383
PowerDNS			382356
Technitium			133959

Table 3: DNS over DNSSEC

Osservando il numero di richieste, con l'aumentare della dimensione del dataset la differenza di risposte è notevole

- Prendendo in considerazione Bind e PowerDNS si passa da una percentuale del 216.08% nel dataset più piccolo ad una percentuale del 149.61% nel dataset più grande

- Prendendo in considerazione PowerDNS e Technitium si passa da una percentuale del 14.35% nel dataset più piccolo ad una percentuale del 185.43% nel dataset più grande

Analizzando anche il grafico delle latenze, in particolar modo la Figura 13, si può notare chiaramente che BIND rimane costante nella parte più inferiore del grafico, mentre le latenze di Technitium e PowerDNS non sono minimamente paragonabili a quelle di BIND, in quanto raggiungono picchi molto alti e senza seguire un pattern.
Ciò che si evince da questo grafico è che il peggiore risulta essere PowerDNS e che Technitium nelle ultime 100000 richieste raggiunge latenze di gran lunga più alte, ma si ipotizza che ciò sia dovuto al tool dnsperf.
Anche il grafico delle CDF conferma quanto detto in precedenza: BIND converge molto rapidamente a 1, mentre gli altri due server convergono ad uno più lentamente. In particolare, la probabilità che la latenza di una risoluzione di una qualsiasi query assuma un valore minore o uguale ad una latenza di 0.02 è maggiore in PowerDNS inizialmente, ma successivamente Technitium supera tale andamento.

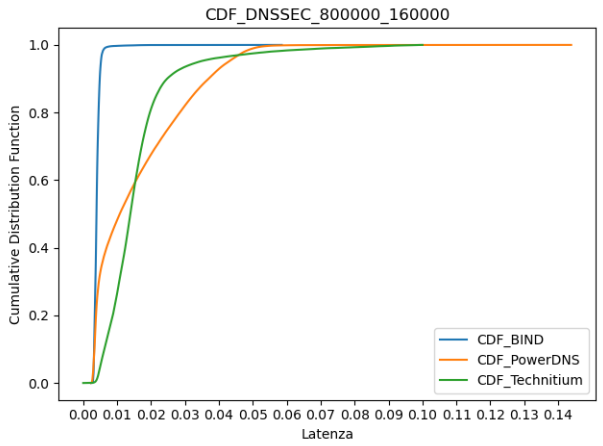

Figure 3: Cumulative Distribution Function di DNSSEC sui tre server - Dataset da 960000

5.1.4 DNS over TLS

Analizzando i grafici dei bins dei benchmarking di TLS sui tre server è evidente che il server in grado di risolvere il 95% delle richieste in un range di latenze più basso rispetto agli altri server risulta essere sempre BIND. Quindi prendendo come riferimento tale range risultano enormi differenze in termini di numero di richieste risolte da PowerDNS e Technitium. Queste differenze vengono riassunte nella seguente tabella:

	Dataset	Range di latenze	Numero di Risposte
BIND	**60000**	0.002016 - 0.010751	59177
PowerDNS			3040
Technitium			16366
BIND	**120000**	0.001632 - 0.012287	118783
PowerDNS			2538
Technitium			32198
BIND	**240000**	0.001728 - 0.011007	237598
PowerDNS			4129
Technitium			55758
BIND	**480000**	0.001696 - 0.012032	465199
PowerDNS			8897
Technitium			120387
BIND	**960000**	0.001664 - 0.012799	931366
PowerDNS			10504
Technitium			266725

Table 4: DNS over TLS

Osservando il numero di richieste, con l'aumentare della dimensione del dataset la differenza di risposte è notevole

- Prendendo in considerazione Bind e Technitium si passa da una percentuale del 261.58% nel dataset più piccolo ad una percentuale del 249.19% nel dataset più grande

- Prendendo in considerazione Technitium e PowerDNS si passa da una percentuale del 438.36% nel dataset più piccolo ad una percentuale del 2439.27% nel dataset più grande

A differenza degli altri protocolli, il peggiore si rivela essere PowerDNS.

Dai grafici delle latenze (in particolare Figura 11) si può notare chiaramente:

- BIND rimane costante nella parte più inferiore del grafico

- Technitium ha latenze più alte, ma mantiene buone prestazioni

- PowerDNS ha picchi molto alti e conferma la sua ultima posizione

Anche il grafico delle CDF conferma quanto detto in precedenza: BIND converge molto rapidamente a 1, Technitium si discosta di poco e PowerDNS converge molto lentamente a 1.

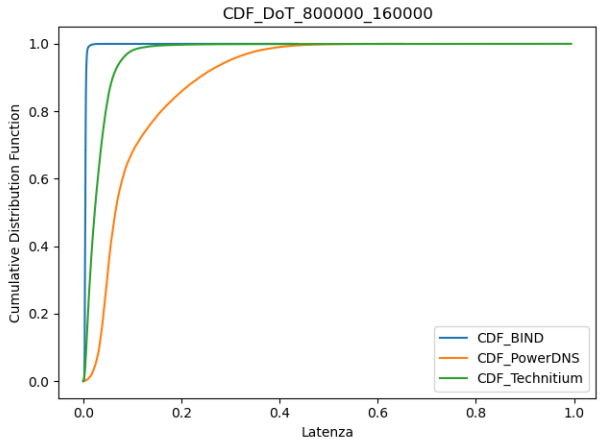

Figure 4: Cumulative Distribution Function di TLS sui tre server - Dataset da 960000

5.1.5 DNS over HTTPS

Analizzando i grafici dei bins dei benchmarking di HTTPS sui tre server è evidente che il server in grado di risolvere il 95% delle richieste in un range di latenze più basso rispetto agli altri server risulta essere BIND. Quindi prendendo come riferimento tale range risultano enormi differenze in termini di numero di richieste risolte da PowerDNS e Technitium. Queste differenze vengono riassunte nella seguente tabella:

	Dataset	Range di latenze	Numero di Risposte
BIND	**60000**	0.004372 - 0.013136	59237
PowerDNS			2963
Technitium			15996
BIND	**120000**	0.003908 - 0.016122	119178
PowerDNS			2960
Technitium			36222
BIND	**240000**	0.004013 - 0.014986	238707
PowerDNS			5074
Technitium			64915
BIND	**480000**	0.004002 - 0.016047	476545
PowerDNS			11127
Technitium			138047
BIND	**960000**	0.004101 - 0.016802	954281
PowerDNS			13074
Technitium			297094

Table 5: DNS over HTTPS

Osservando il numero di richieste, con l'aumentare della dimensione del dataset la differenza di risposte è notevole

- Prendendo in considerazione Bind e Technitium si passa da una percentuale del 270.32% nel dataset più piccolo ad una percentuale del 221.21% nel dataset più grande
- Prendendo in considerazione Technitium e PowerDNS si passa da una percentuale del 439.86% nel dataset più piccolo ad una percentuale del 2172.4% nel dataset più grande

Anche in questo protocollo il peggiore si rivela essere PowerDNS.

Dai grafici delle latenze (in particolare Figura 12) si può notare chiaramente:

- BIND rimane costante nella parte più inferiore del grafico
- Technitium ha latenze alte e presenta anche dei picchi, ma raramente
- PowerDNS tocca picchi di latenze di gran lunga superiore rispetto agli altri due server

Anche il grafico delle CDF conferma quanto detto in precedenza: BIND converge molto rapidamente a 1, Technitium converge in maniera simile alla curva di BIND e PowerDNS converge molto lentamente a 1.

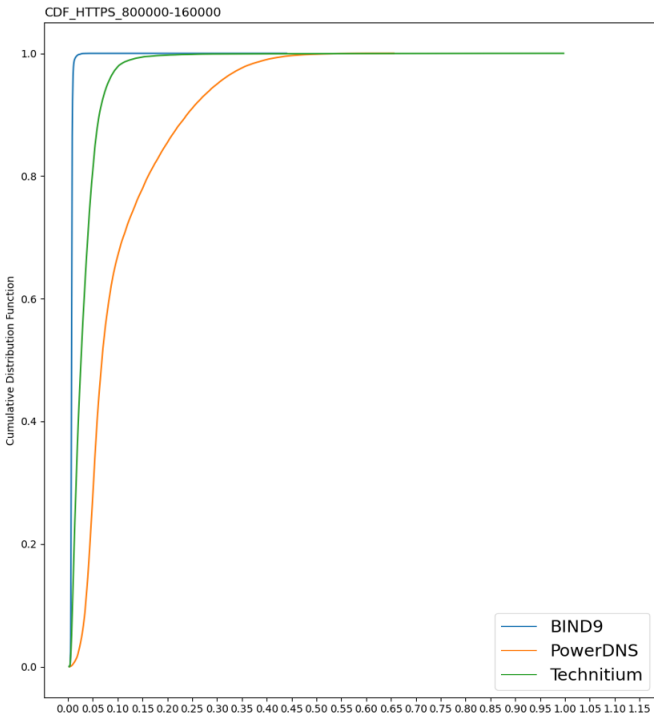

Figure 5: Cumulative Distribution Function di HTTPS sui tre server - Dataset da 960000

5.2 un server testato con tutti i protocolli

5.2.1 Bind

Analizzando i dati del benchmarking dei protocolli DNS-over-UDP, DNS-over-TCP, DNS-over-TLS, DNSSEC e DNS-over-HTTPS, sul server BIND risulta che: le latenze di DNS-over-TCP sono superiori di circa 0.004 secondi rispetto le latenze di DNS-over-UDP con tutti i dataset, questo non ci sorprende siccome TCP è un protocollo orientato alla connessione quindi con overhead maggiore; la stessa differenza di latenze si ha tra DNS-over-UDP e DNSSEC, probabilmente l'aumento di latenze è causato dai controlli crittografici effettuati per garantire l'autenticità e l'integrità; DNS-over-HTTPS presenta delle latenze superiori del 45% circa rispetto DNS-over-TLS, anche questo risultato è un risultato atteso siccome HTTPS utilizza TLS, quindi HTTPS aggiunge overhead

ProtocolloBIND	Dataset	Latenza minima	Latenza massima	Media	Deviazione Standard	Query al secondo
DNS-over-UDP	60000	0.000074	0.013901	0.001111	0.000742	72839
	120000	0.000139	0.019272	0.001166	0.001003	71686
	240000	0.000036	0.021055	0.001286	0.000878	65231
	480000	0	0.0551614	0.001196	0.000868	70014
	960000	0	0.0551615	0.001214	0.000850	69407
DNS-over-TCP	60000	0.000211	0.046138	0.005718	0.001368	16635
	120000	0.000155	0.041497	0.004668	0.001567	20416
	240000	0.000181	0.035257	0.005137	0.002134	18532
	480000	0.000074	0.039776	0.004465	0.005625	20881
	960000	0.000163	0.045033	0.004372	0.001348	21941
DNS-over-TLS	60000	0.000174	0.471178	0.004385	0.001960	19795
	120000	0.000279	0.067095	0.004181	0.001771	20894
	240000	0.000162	0.044604	0.004068	0.001606	21976
	480000	0.000292	0.043098	0.004337	0.001984	20437
	960000	0.000210	0.436309	0.004447	0.002280	20077
DNS-over-HTTPS	60000	0.002638	0.050066	0.007209	0.001986	/
	120000	0.002566	0.070032	0.007006	0.001798	/
	240000	0.002844	0.047929	0.006893	0.001637	/
	480000	0.002631	0.048867	0.007161	0.002008	/
	960000	0.002711	0.439635	0.007270	0.002302	/
DNSSEC	60000	0.0023942	0.019115	0.003932	0.00080	/
	120000	0.0025783	0.0225401	0.003990	0.00105	/
	240000	0.0023379	0.0242727	0.004109	0.00093	/
	480000	0.0022919	0.0585243	0.004027	0.00112	/
	960000	0.0022856	0.0585269	0.004042	0.00102	/

protocollare a TLS che si ripercuote anche in DNS-over-TLS e DNS-over-HTTPS;

Riguardo la distribuzione dei bins si evince che circa il 95% delle richieste di trova nei seguenti range:

- Le latenze DNS-over-UDP presentano una latenza di risoluzione compresa nel range 0.000512 - 0.003135
- le richieste DNS-over-TCP hanno una latenza compresa nel range 0.002688 - 0.011007
- Le richiede DNS-over-TLS hanno una latenza compresa nel range 0.001728 - 0.012543
- Le richieste DNSSEC hanno una latenza compresa nel range 0.002828 - 0.007321
- Le richieste DNS-over-HTTPS hanno una latenza compresa nel range 0.004151 - 0.017582

Analizzando la latenza minima, la latenza massima, la media e la deviazione standard si può osservare che: la latenza media è correlata al numero di records, ad esempio prendendo il protocollo con maggiore overhead cioè HTTPS e quello con il minore overhead cioè UDP e calcolando l'indice di correlazione tra la latenza media di DNS-over-HTTPS e la taglia dei dataset risulta un indice pari a 0,77, per DNS-over-UDP invece tale indice cala a 0,33; l'aumento del numero di records nel dataset implica un aumento di circa 0.0001 secondi della latenza media, quindi anche avendo un indice di correlazione forte come nel caso di HTTPS la latenza media cresce molto lentamente; a sostegno di ciò si può osservare la deviazione standard che nel caso peggiore (DNS-over-TCP dataset 48000) è pari a 0.005625 Dal numero di query al secondo risulta un throughput di circa 70000 query al secondo per DNS-over-UDP, tale cifra scende a 20000 per i protocolli DNS-over-TCP e DNS-over-TLS. Riguardo ai protocolli DNSSEC e DNS-over-HTTPS non si ha il numero di query al secondo siccome il loro benchmarkin è stato eseguito utilizzando scriptKdig.

Infine osservando anche le Cumulative Distribution Function possiamo dire che BIND offre prestazioni eccellenti con tutti i protocolli testati

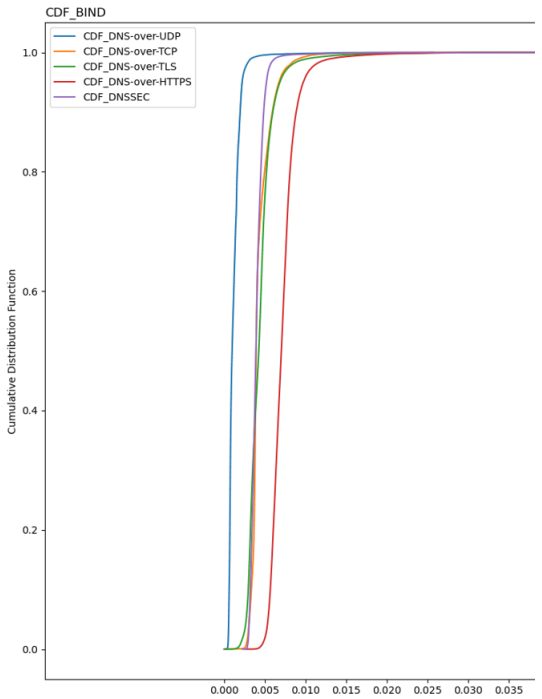

Figure 6: CDF di tutti i protocolli su BIND (dataset da 960000)

5.2.2 PowerDNS e dnsdist

Analizzando i dati del benchmarking dei protocolli DNS finora riportati sul server PowerDNS con la sua estensione dnsdist, per permettere l'utilizzo di DNSSEC, DNS-over-TLS e DNS-over-HTTPS, risulta che: DNS-over-TCP ha una latenza media inferiore di DNS-over-UDP, in particolare con i dataset 120000, 240000 e 480000 la latenza media di DNS-over-TCP è inferiore di un ordine di grandezza rispetto DNS-over-UDP sugli stessi dataset. Questo risultato non è affatto un risultato attesso siccome come anche detto nei paragrafi precedenti TCP ha un overhead protocollare maggiore di UDP. Riguado i due protocolli DNS sicuri possiamo notare che rispetto agli altri hanno una media e una deviazione standard ben maggiore (anche in questo di un ordine di grandezza), questo risultato viene ben rappresentato dall'andamento delle CDF. Inoltre dalle CDF di HTTPS e TLS è possibile notare lo stesso andamento con un leggero aumento della latenza in HTTPS, questo a conferma del fatto che HTTPS (basato su TLS) presenta una latenza maggiore di 0.0030 secondi rispetto TLS (come osservabile dalla tabella). Lo stesso fenomeno di verifica con DNSSEC (basato su UDP), anche in questo caso le due CDF hanno lo stesso andamento ma DNSSEC presenta un aumento delle latenze pari a 0.0020 secondi.

ProtocolloPDNS	Dataset	Latenza minima	Latenza massima	Media	Deviazione Standard	Query al secondo
DNS-over-UDP	60000	0.000010	0.060898	0.011496	0.010857	8232
	120000	0.000007	0.0551610	0.012723	0.020099	7379
	240000	0	0.621478	0.011545	0.011960	8168
	480000	0	0.0551604	0.012605	0.012792	7710
	960000	0.000002	0.0551615	0.012940	0.013464	7529
DNS-over-TCP	60000	0.000292	0.078802	0.010970	0.005248	8945
	120000	0.000097	0.282269	0.007531	0.008450	12994
	240000	0.000104	0.0696429	0.007358	0.013827	13338
	480000	0.000217	0.064662	0.007977	0.004281	12226
	960000	0.000080	0.078075	0.010028	0.003450	9803
DNS-over-TLS	60000	0.000431	0.436976	0.053293	0.056625	1791
	120000	0.001249	0.498664	0.076835	0.071649	1242
	240000	0.000748	0.602001	0.091005	0.082070	1056
	480000	0.000501	0.773330	0.086077	0.079871	1118
	960000	0.000276	0.653104	0.102050	0.087765	948
DNS-over-HTTPS	60000	0.0029155	0.440252	0.056119	0.056626	/
	120000	0.0037513	0.501567	0.079657	0.071649	/
	240000	0.0033559	0.605095	0.093829	0.082070	/
	480000	0.0029973	0.776448	0.088900	0.079872	/
	960000	0.0027836	0.655488	0.104874	0.087766	/
DNSSEC	60000	0.002391	0.063711	0.014321	0.010861	/
	120000	0.002307	0.092534	0.015293	0.012447	/
	240000	0.002300	0.062473	0.014367	0.011901	/
	480000	0.002290	0.114460	0.015429	0.012796	/
	960000	0.002301	0.143832	0.015764	0.013468	/

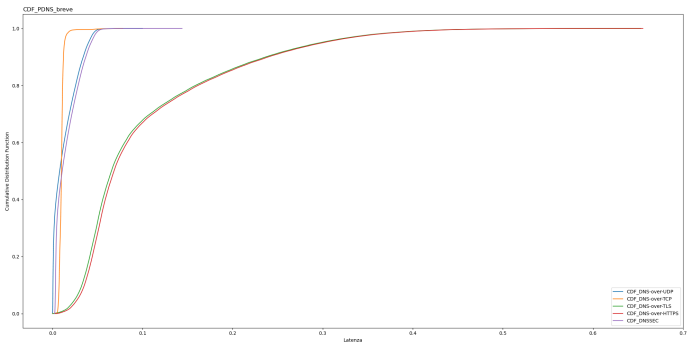

Figure 7: CDF di tutti i protocolli su PDNS (dataset da 960000)

Riguardo la distribuzione dei bins si evince che circa il 95% delle richieste di trova nei seguenti range:

- Le latenze DNS-over-UDP presentano una latenza di risoluzione compresa nel range 0.000128 - 0.045391
- le richieste DNS-over-TCP hanno una latenza compresa nel range 0.005248 - 0.020991
- Le richieste DNS-over-TLS hanno una latenza compresa nel range 0.003072 - 0.409599 con una maggiore presenza nel range 0.030208 - 0.129023
- Le richieste DNSSEC hanno una latenza compresa nel range 0.002406 - 0.056186
- Le richieste DNS-over-HTTPS hanno una latenza compresa nel range 0.006478 - 0.50598 con una maggiore presenza nel range 0.028234 - 0.070873

Anche in questo caso l'aumento del numero di records nel dataset è correlato con la latenza media, infatti in tutti i protocolli (tranne DNS-over-TCP) l'indicie di correlazione è superiore al 0.65. Anche qui il caso peggiore si con HTTPS siccome la latenza media passa da 0.056 a 0.104 secondi. Riguardo DNS-over-TCP l'indice di correlazione è pari a 0.19 quindi una correlazione debole e infatti la latenza media è pari a 0.007 per i tre dataset 120000, 240000 e 480000, per i dataset 60000 e 960000 è pari a 0.010. Dal numero di query al secondo risulta un throughput di circa 8000 query al secondo per DNS-over-UDP, 12000 per DNS-over-TCP e solo 1000 per DNS-over-TLS. Riguardo ai protocolli DNSSEC e DNS-over-HTTPS non si ha il numero di query al secondo siccome il loro benchmark è stato eseguito utilizzando scriptKdig.

5.2.3 Technitium

Dai dati ottenuti dai benchmarking effettuati sul server Technitium anche in questo caso risulta che DND-over-TCP in alcuni test presenta una latenza media inferiorie a DNS-over-UDP, in particolare con i dataset 480000 e 960000 la latenza media di DNS-over-TCP è pari a 0.0095 invece con UDP la latenza sale a 0.017 e 0.021, tale incremento è osservabile anche nelle CDF. Lo stesso fenomeno però non si verifica con i dataset 60000 e 120000. Anche in questo caso le latenze di HTTPS e TLS si differenziano di poco e anche in questo caso l'andamento delle CDF è identico se non per un leggero scostamento di HTTPS dovuto all'aggiunta di overhead al protocollo TLS. Un risultato molto interessante è dato da DNSSEC, infatti per i primi tre dataset la latenza media rispetto a UDP è inferiore di 0.0050 secondi invece nei dataset 480000 e 960000 DNSSEC ha latenze inferiori di 0,017 secondi.

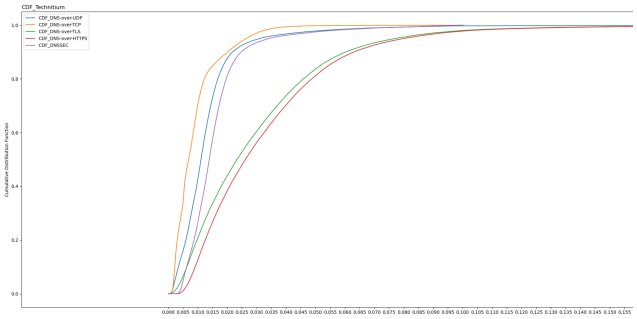

Figure 8: CDF di tutti i protocolli su Technitium (dataset da 960000)

Riguardo la distribuzione dei bins si evince che circa il 95% delle richieste di trova nei seguenti range:

- Le latenze DNS-over-UDP presentano una latenza di risoluzione compresa nel range 0.001319 - 0.092567;
- le richieste DNS-over-TCP hanno una latenza compresa nel range 0.001280 - 0.059916 con maggiore presenza nel range 0.002067 - 0.013823;
- Le richiede DNS-over-TLS hanno una latenza compresa nel range 0.0026785 - 0.092782 con una maggiore presenza nel range 0.008192 - 0.056319;
- Le richieste DNSSEC hanno una latenza compresa nel range 0.003250 - 0.0556712;
- Le richieste DNS-over-HTTPS hanno una latenza compresa nel range 0.004179 - 0.106413

Anche con Techniutium si ha una forte correlazione tra la taglia del dataset e la latenza media tuttavia la latenza non subisce forti aumenti, nel caso peggiore cioè DNS-over-UDP l'aumento è pari a 0,013. Un caso molto particolare è dato da DNS-over-TCP infatti in questo caso

ProtocolloTECH	Dataset	Latenza minima	Latenza massima	Media	Deviazione Standard	Query al secondo
DNS-over-UDP	60000	0.000231	0.051895	0.008399	0.007036	10771
	120000	0.000246	0.057467	0.008985	0.005359	5615
	240000	0.000034	1.139794	0.009863	0.023835	5905
	480000	0.000195	1.439380	0.017266	0.025609	1560
	960000	0	0.0551612	0.021412	0.147457	1334
DNS-over-TCP	60000	0.000388	0.091362	0.010676	0.010769	8854
	120000	0.000125	0.073314	0.010840	0.009071	8794
	240000	0.000157	0.671400	0.009485	0.013058	10034
	480000	0.000114	0.060340	0.009536	0.014529	9970
	960000	0.000040	0.056360	0.009538	0.038124	1003
DNS-over-TLS	60000	0	0.0551603	0.025787	0.020249	3273
	120000	0.000034	0.0551523	0.028833	0.025248	2961
	240000	0.000030	0.0551580	0.027995	0.073974	3035
	480000	0	0.0551611	0.029597	0.049873	2828
	960000	0	0.0551615	0.032276	0.086735	2710
DNS-over-HTTPS	60000	0.002641	0.1679537	0.028614	0.020248	/
	120000	0.002465	0.3316686	0.031659	0.025248	/
	240000	0.002404	0.2223731	0.029390	0.020271	/
	480000	0.00236	0.4405274	0.031801	0.023609	/
	960000	0.002312	0.9971559	0.033256	0.031381	/
DNSSEC	60000	0.0025374	0.054948	0.003932	0.007043	/
	120000	0.0026433	0.060667	0.003990	0.005367	/
	240000	0.002541	0.117014	0.004109	0.006752	/
	480000	0.002487	0.346790	0.004027	0.018942	/
	960000	0.000001	0.099995	0.004042	0.011464	/

la correlazione, pari a -0.67, è negativa e infatti aumentando la taglia del dataset la latenza media si abbassa di 0,0005 Dal numero di query al secondo risulta un throughput di circa 3000 query al secondo per DNS-over-TLS. Per DNS-over-UDP si registra un andamento inversamente proporzionale alla taglia del dataset infatti con il dataset da 60000 il numero di query al secondo è pari a 10771, per i dataset da 120000 e 240000 il numero di query scende a 5615 e 5905, per poi arrivare a 1560 e 1334 con i restanti due dataset. A conferma di questo andamento c'è l'indice di correlazione pari a -0.81. Riguardo DNS-over-TCP il throughput cala drasticamente solo con il dataset da 960000. Riguardo ai protocolli DNSSEC e DNS-over-HTTPS non si ha il numero di query al secondo siccome il loro benchmark è stato eseguito utilizzando scriptKdig.

6 Limitazioni dello studio e sviluppi futuri

In questo studio si sono analizzate le performance di cinque protocolli configurati su tre server DNS, i risultati ottenuti sono conformi alla Quality Of Service e alla Quality Of Experience dei servizi web più comuni [7]. Ad esempio considerando tutti i dataset su tutti tre i server, la latenza media di una query DNS-over-UDP non supera i 20ms. Lo stesso discorso vale per DNS-over-HTTPS, che è il protocollo DNS con maggiore overhead, infatti nel caso peggiore la latenza media non supera i 100ms. Risulta fondamentale però il numero di richieste al secondo, infatti Technitium e PowerDNS che rispettivamente risolvono un numero di query DNS-over-UDP al secondo di circa 8000 e 5900 risulterebbero poco adatti a contesti su larga scala. Oltre ciò bisogna considerare il caso d'uso specifico, cioè quale protocollo DNS verrà più utilizzato. Infatti con DNS-over-TLS le migliori performance tra PowerDNS e Technitium si hanno da quest'ultimo, anche se con gli altri protocolli presenta prestazioni inferiori rispetto PowerDNS.

Tuttavia bisogna tenere conto delle numerose limitazioni riscontrate, limitazioni che combaciano con i possibili sviluppi futuri. Una su tutte i tool con cui effettuare il benchmarking: dnsperf è il tool più utilizzato in lettura però le latenze in output risultano spesso non reali come valori negativi e valori eccessivamente alti e quindi è necessario un adattamento dei dati; l'utilizzo di kdig implica l'aggiunta di un overhead superiore a dnsperf, di conseguenza anche scriptKdig presenta questa pecca; il sovraccarico del PC utilizzato per eseguire le VM su cui si effettua il benchmarking implica una forte limitazione della memoria centrale; un ulteriore limite è il dataset utilizzato per creare il file di zona, in particolare in termini di dimensione (andrebbero considerate zone molto più grandi), in questo studio si è utilizzata una zona di appena due milioni di records a causa della limitazione di memoria della VM e del PC; un alta limitazione è data dal numero di client che si collegano contemporaneamente al server, in questo studio è stato considerato un singolo client a causa delle risorse limitate del PC;

Tali limitazioni potrebbero essere affrontate in versioni successive di questo lavoro, ad esempio utilizzando diverse macchine client e macchine server con file di zona con taglie reali. Un ulteriore sviluppo futuro molto interessante è quello di analizzare DNS-over-QUIC, infatti questo nuovo protocollo di trasporto include le funzionalità di TCP aggiungendo la sicurezza TLS, tutto ciò con una latenza inferiore a TCP. In questo lavoro non è stato preso in considerazione siccome non è stato ancora implementato in BIND e Technitium.

In conclusione possiamo dire che BIND è il server che presenta le performance migliori in tutti i casi, poi troviamo PowerDNS e infine Technitium. Anche se le prestazioni di questi ultimi due server sono nettamente inferiori rispetto a BIND, vorremo spendere qualche parola in loro difesa. Innanzitutto Technitium è stato il server DNS che ha dato meno problemi, la sua installazione risulta banale, offre un interfaccia grafica web molto user friendly e utile, inoltre offre una documentazione molto chiara con tutorial molto esplicativi. Anche PowerDNS offre una buona documentazione ma risulta molto più complicato configurare i vari protocolli, inoltre per i protocolli DNS sicuri bisogna utilizzare l'estensione dnsdist. Infine BIND è il server DNS che ci ha dato più problemi durante la configurazione, non offre un'interfaccia grafica, la documentazione risulta enorme e difficile da studiare per chi è alle prime armi con i sistemi DNS e il materiale che si trova nel WEB per la configurazione di DNSSEC, DNS-over-TLS e DNS-over-HTTPS risulta essere superficiale o addirittura errato. In conclusione BIND, PowerDNS e Technitium rappresentano il classico compromesso che troviamo spesso nella vita di tutti i giorni tra efficienza e semplicità di utilizzo.

7 Data Availability

Il Dataset principale, da cui è stato ricavato il file contenente i due milioni di record utilizzato il file di zona e i diversi file per le sessioni di benchmarking, è disponibile al seguente link: https://t.ly/s-oFl. Tutte le VM utilizzate in questo lavoro sono disponibili al seguente link Google Drive: http://tiny.cc/Virtual-Machine. In questa repository GitHub (https://t.ly/Q2tT0 sono presenti:

- Il file di zona *db.it* utilizzato per ciascun server
- Per ogni sessione di benchmarking e per ogni protocollo: i file di test utilizzati per le sessioni di bench-

marking e i file ottenuti da dnsperf e scriptKdig; i grafici delle latenze, a barre per i bins e le CDF; Il grafico a barre per valore minimo, massimo, medio e deviazione standard.

- Per ogni server una CDF con tutti i protocolli
- Tutti gli script utilizzati durante il pre-processing per la visualizzazione grafica dei dati, gli script per creare i grafici e "scriptKdig.sh". Ogni script ha un README.md

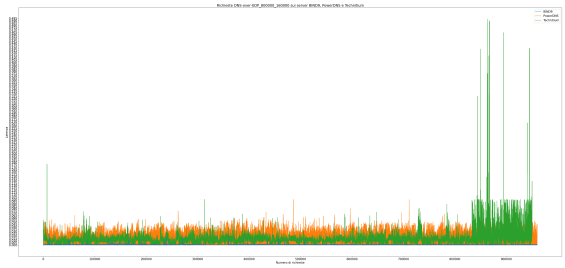

Figure 9: Grafico delle latenze DNS-over-UDP dataset 960000

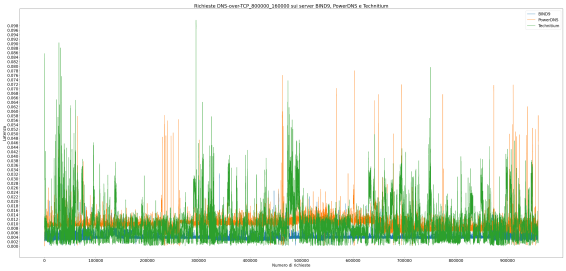

Figure 10: Grafico delle latenze DNS-over-TCP dataset 960000

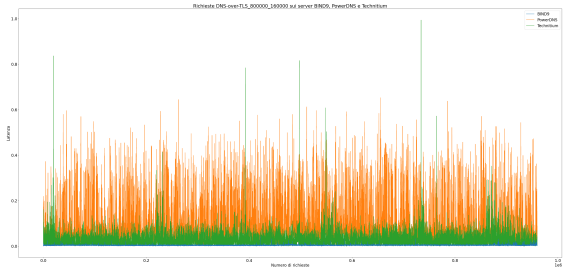

Figure 11: Grafico delle latenze DNS-over-TLS dataset 960000

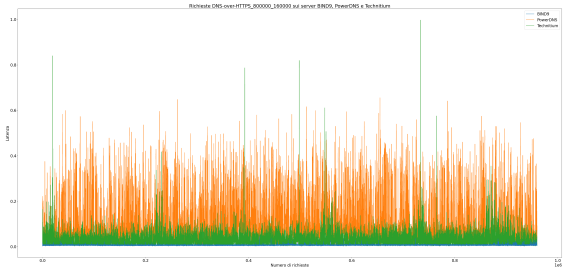

Figure 12: Grafico delle latenze DNS-over-HTTPS dataset 960000

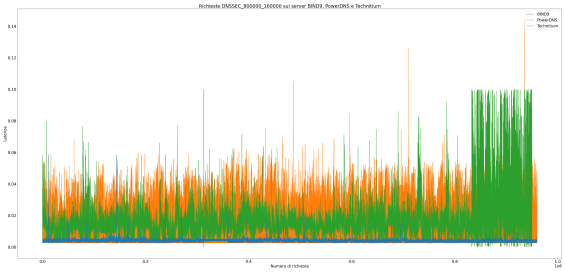

Figure 13: Grafico delle latenze DNSSEC dataset 960000

References

[1] Pavel Bohdan Turkynevych. *World's single largest Internet domains dataset*. `https://github.com/tb0hdan/domains/tree/master`. 2021.

[2] Internet Systems Consortium. *dig - DNS lookup utility*. `https://linux.die.net/man/1/dig`.

[3] Gibson Research Corporation. *Domain Name Speed Benchmark*. `https://www.grc.com/dns/benchmark.htm`.

[4] CZ.NIC. *DNS Shotgun*. `https://github.com/CZ-NIC/shotgun`.

[5] KNOT DNS. *kdig – Advanced DNS lookup utility*. `https://www.knot-dns.cz/docs/latest/html/man_kdig.html`.

[6] DNS-OARC. *dnsjit - Engine for capturing, parsing and replaying DNS*. `https://github.com/DNS-OARC/dnsjit`.

[7] Austin Hounsel et al. "Comparing the effects of DNS, DoT, and DoH on web performance". In: *Proceedings of The Web Conference 2020*. 2020, pp. 562–572.

[8] Gábor Lencse. "Benchmarking Authoritative DNS Servers". In: *IEEE Access* 8 (2020), pp. 130224–130238. DOI: `10.1109/ACCESS.2020.3009141`.

[9] Inc Nominum. *dnsperf - Man Page test the performance of a DNS server*. `https://www.mankier.com/1/dnsperf`.

[10] Victor Le Pochat et al. "Tranco: A research-oriented top sites ranking hardened against manipulation". In: *arXiv preprint arXiv:1806.01156* (2018).