

Domain Name Basics

DNS Zone Files

Tobias Sattler
tobiassattler.com

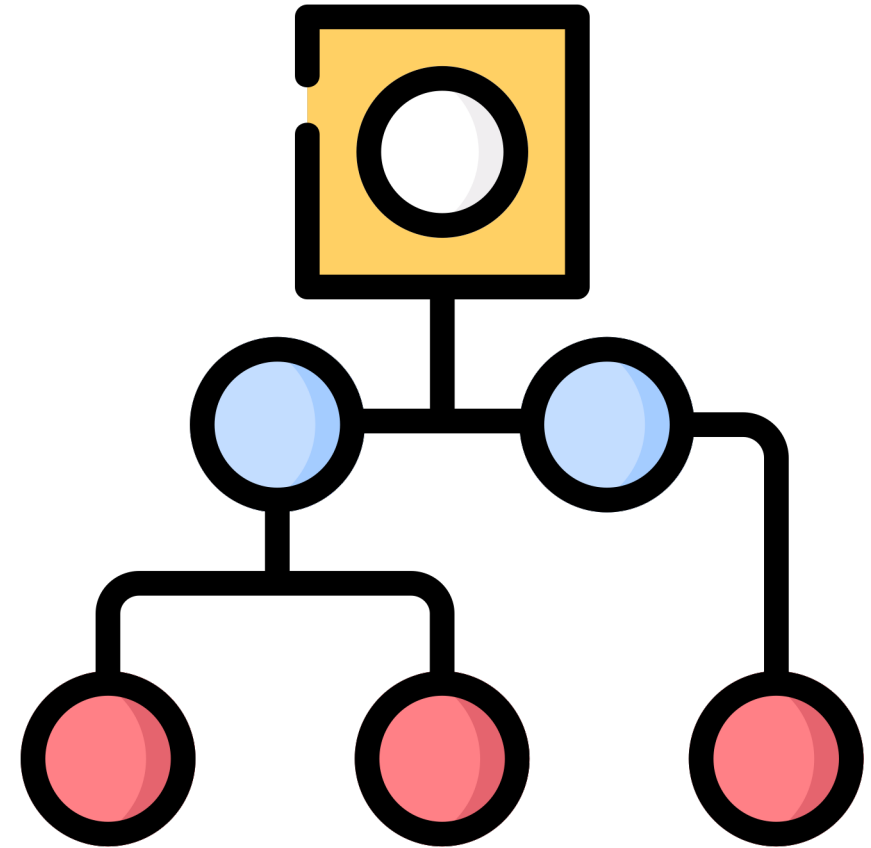
Domain Name System (DNS)

DNS is a hierarchical distributed naming system to **translate domain names** into **IP addresses**, which makes websites easier to remember, such as

- tobiassattler.com instead of 78.46.19.133

The domain namespace is a tree, and its root is a dot.

- www.tobiassattler.com.



What is a zone file?

A **zone file** is a text file that describes a DNS zone.

Such a file contains **mappings** between **domain names** and **IP addresses** and other resources. A TLD zone file contains only domain names **that are resolving**.

The format of a zone file is defined in RFC 1035 and RFC 1034 and was originally used by the Berkeley Internet Domain Name (BIND) software package.

A zone file is a sequence of entries for resource records (RR).



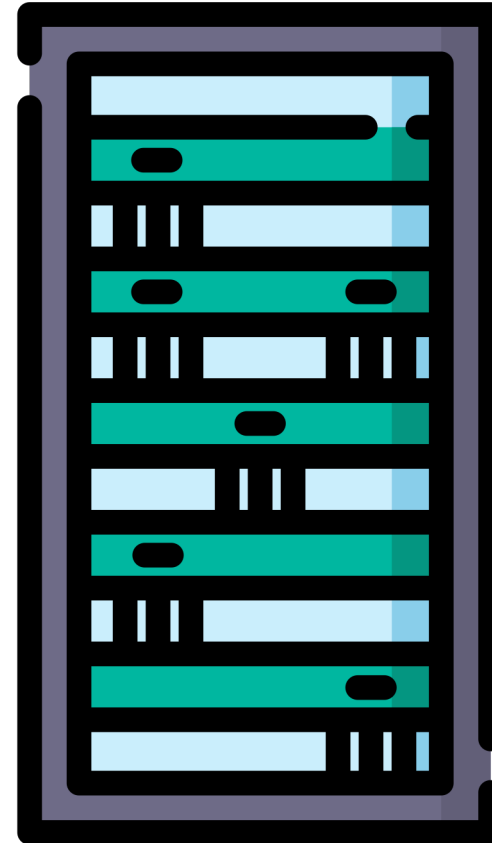
Resource Records #1

There are many DNS Resource Records. This list is an overview of the most commonly used records:

A – Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

AAAA – Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.

CNAME – Redirect to another name: the DNS lookup will continue by retrying the lookup with the new name.



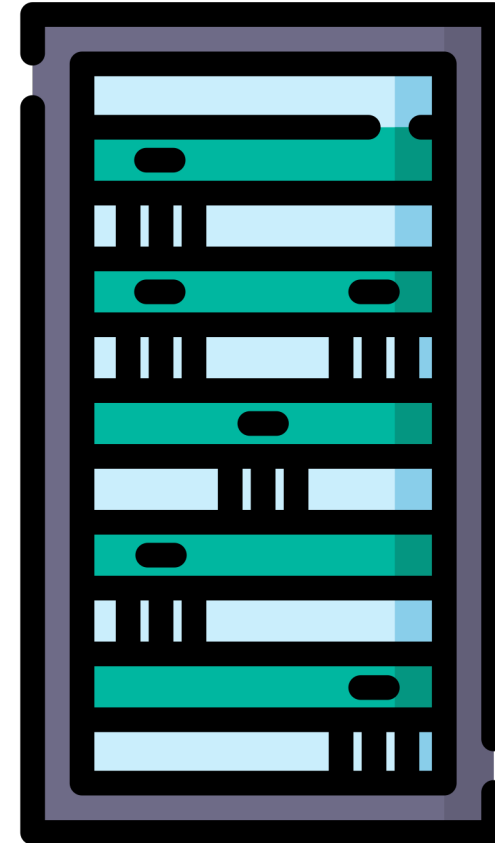
Resource Records #2

DNSKEY – The key record used in DNSSEC.

DS – The record used to identify the DNSSEC signing key of a delegated zone.

MX – Maps a domain name to a list of message transfer agents for that domain. Used for email.

NS – Delegates a DNS zone to use the given authoritative name servers.

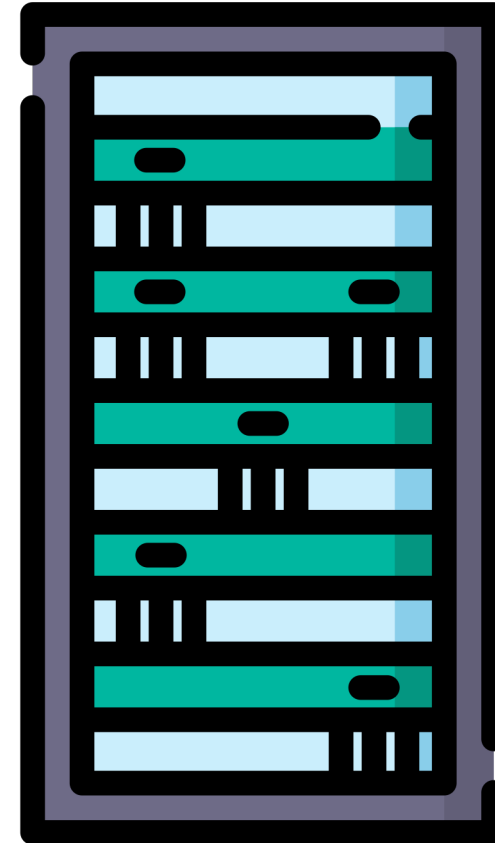


Resource Records #3

PTR – Pointer to a canonical name. Unlike a CNAME, DNS processing stops, and just the name is returned and used for reverse DNS lookups.

RRSIG – Signature for a DNSSEC-secured record set.

SOA – Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the zone serial number, and several timers relating to refreshing the zone.

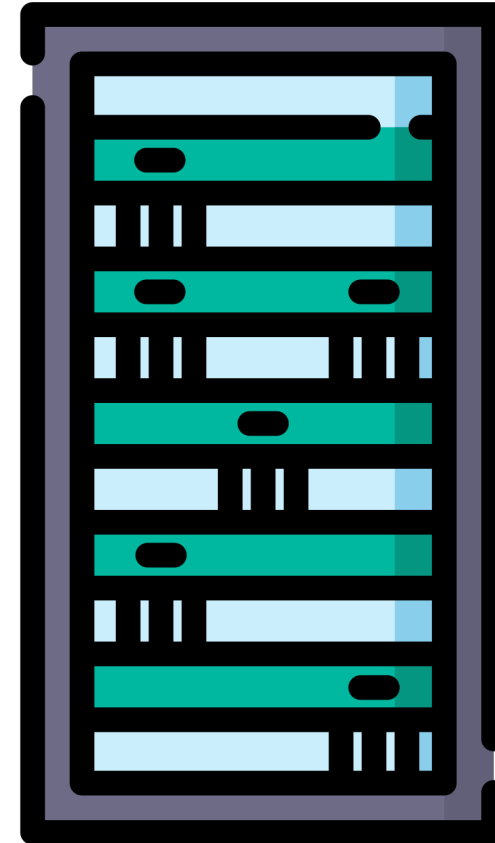


Resource Records #4

SRV – Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX. Commonly used for SIP (VoIP) and XMPP (Jabber / Instant Messenger).

TLSA – A record for DANE. This resource record is used to associate a TLS server certificate or public key with the domain name where the record is found.

TXT – Originally for arbitrary human-readable text in a DNS record. By now, they are usually used for DKIM, DMARC, SPF, etc.



DNS Zone File Example

```
;; QUESTION SECTION:
;tobiassattler.com.      IN      ANY

;; ANSWER SECTION:
tobiassattler.com.      3600    IN      RRSIG   HINFO 13 2 3789 20160823084652 20160821064652 35273 tobiassattler.com. IQqodcX0A5C0KaK1tPYtcN+WNqVWGLa16P6ih6YF
egR9M3qmkB/Y9S+ Wq3Ty1bMoUiM+A0V4+j7ZHQW012Llw==
tobiassattler.com.      3600    IN      HINFO   "Please stop asking for ANY" "See draft-ietf-dnsop-refuse-any"
tobiassattler.com.      3600    IN      RRSIG   DNSKEY 13 2 3600 20160910150750 20160712150750 2371 tobiassattler.com. nF88qNPyn7MEms5F6GjslMbDj17Wn5Km/ANava+uN
BUXXu15KAnLs290 qXZaVgcLvECeRxs1gJ39E83xDf70BQ==
tobiassattler.com.      3600    IN      DNSKEY  257 3 13 mdsswUyr3DPW132m0i8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+ KkxLbxILfDLUT0rAK9iUzy1L53eKGQ==
tobiassattler.com.      3600    IN      DNSKEY  256 3 13 koPbw9wmYZ7ggcJnQ6ayHyhHaDNMYELKTqT+qRGrZpWSccr/lBcrml0Z 1PuQHB3Azhii+sb0PYFkH1ruxLhe5g==
tobiassattler.com.      3600    IN      RRSIG   DS 8 2 86400 20160829043125 20160822032125 27452 com. eYrDZtZKYM4catcGZkwY78/0QJLmAZCr5+U7ywFSZpCUQsQahhFNHfm/ N
9lBL30hK8ASK8U2jIxshpqr2N7o7lBfqhetWsIre6J5G8mL6yyWwcj gLbbYDUelRhprf4vhBZ6PTqXlHNhdoiUdz4qtKRkFhBu3pApYBhx7dR4 mgc=
tobiassattler.com.      3600    IN      DS      2371 13 2 AEC28A9CE09F9D5EA2244D5D4ED4B732F79D0D6E2F2C0048E1C428A1 844A62CB
tobiassattler.com.      3600    IN      NS      kip.ns.cloudflare.com.
tobiassattler.com.      3600    IN      NS      ruth.ns.cloudflare.com.

;; AUTHORITY SECTION:
tobiassattler.com.      3600    IN      NS      ruth.ns.cloudflare.com.
tobiassattler.com.      3600    IN      NS      kip.ns.cloudflare.com.

;; ADDITIONAL SECTION:
kip.ns.cloudflare.com.  3600    IN      A      173.245.59.128
kip.ns.cloudflare.com.  3600    IN      AAAA   2400:cb00:2049:1::adf5:3b80
ruth.ns.cloudflare.com. 1361    IN      A      173.245.58.143
ruth.ns.cloudflare.com. 1361    IN      AAAA   2400:cb00:2049:1::adf5:3a8f
```


What is the DNS root zone?

The DNS root zone is the top-level zone in the hierarchical namespace. This zone is served by 13 root server clusters, in total 929 instances, which are authoritative for queries to the TLD.

Thus, every name resolution either starts with a query or uses information that was once obtained from a root server.

Therefore, the root DNS servers are essential to the function of the Internet, as most Internet services are based on domains.

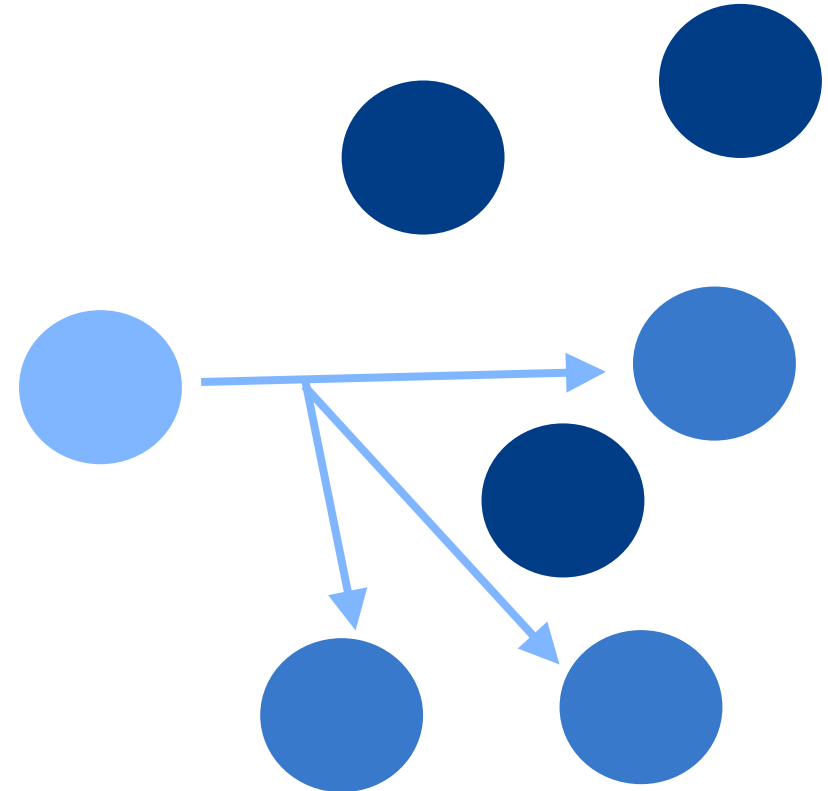


Anycast Name Servers

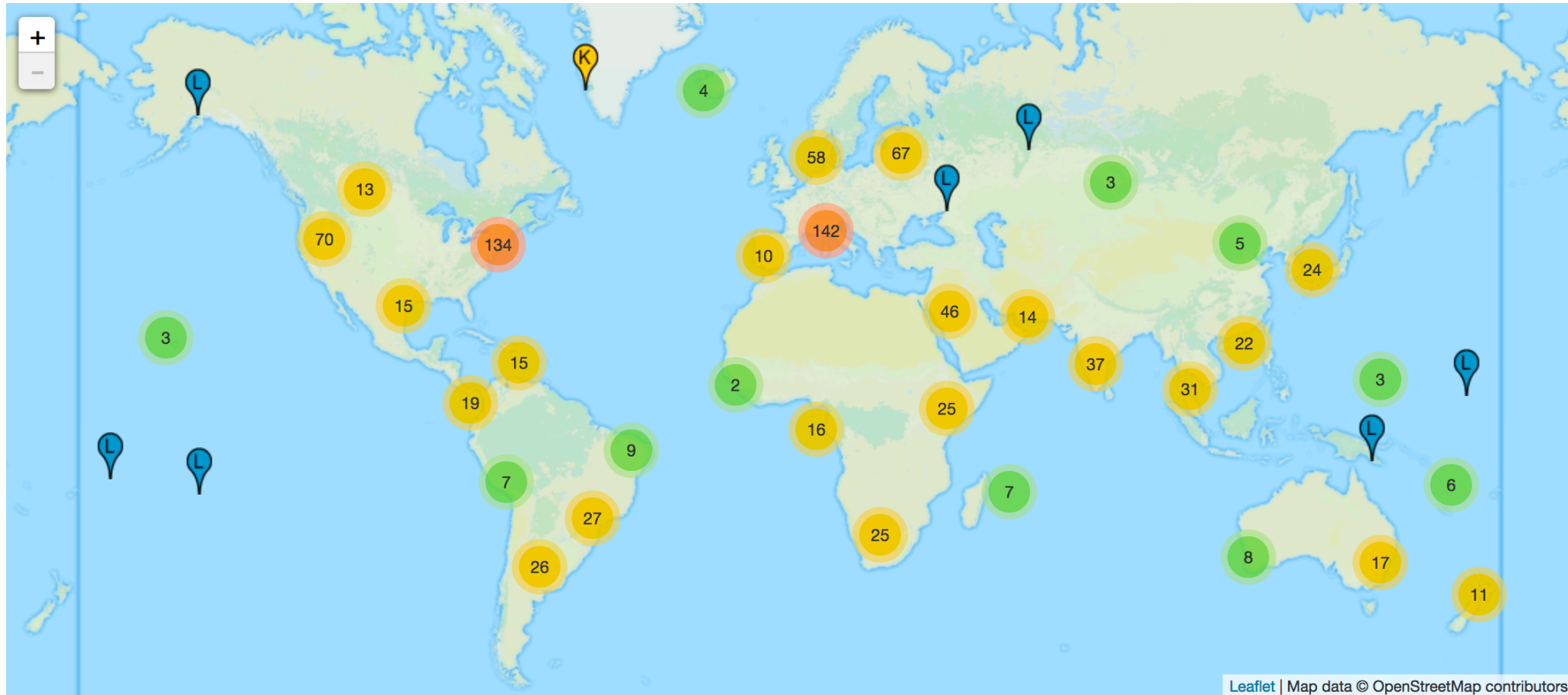
Anycast is a **network addressing** and **routing** methodology in which one source can 'talk' to a service that is advertised or hosted on multiple nodes configured with the same IP address.

It announces the same IP address **simultaneously** from different servers on the web.

Network routing will route the packets to the '**nearest**' **target** based upon topology.



Geographical distribution of Root Servers



Source: <http://root-servers.org> - Effective 06/2018

Root Zone File Example

```
.           86400   IN       SOA      a.root-servers.net. nstld.verisign-grs.com. 2018062800 1800 900 604800 86400
.           86400   IN       RRSIG   SOA 8 0 86400 20180711050000 20180628040000 39570 .
VHxsBXG4qpOsNEWLC/Wm16SOGZqgf2J8+3urAO1Pm043izqPYQKfKw0z4NjfxGn9GSdCnRR+pt00gdllPUcCih9jqteaIeQcXzW+nmvV3AwpULZ8tGfG1blzJOuz5d7KfH
/1+oktGxhGWkAko1BgnSKu63m4ewoi4Ba7yl5sCcRFn6+cEQOSsHq10V0+oppPIYDNaPnqx+sytkCkx09vn5TD6afHqsGBzzlINatCRWfF+6rzJ/0FnIYZ7Vm2osSdyxbzkExiInpQvxpEHlholVaqOAijDxmODx3DI
.           518400  IN       NS        a.root-servers.net.
.           518400  IN       NS        b.root-servers.net.
.           518400  IN       NS        c.root-servers.net.
.           518400  IN       NS        d.root-servers.net.
.           518400  IN       NS        e.root-servers.net.
.           518400  IN       NS        f.root-servers.net.
.           518400  IN       NS        g.root-servers.net.
.           518400  IN       NS        h.root-servers.net.
.           518400  IN       NS        i.root-servers.net.
.           518400  IN       NS        j.root-servers.net.
.           518400  IN       NS        k.root-servers.net.
.           518400  IN       NS        l.root-servers.net.
.           518400  IN       NS        m.root-servers.net.
.           518400  IN       RRSIG   NS 8 0 518400 20180711050000 20180628040000 39570 . Yqgln/27yrJSwJWX0r92QtlgXMsADvrawLpeYeda+FjEjRTy8NUgBMK5oEmIuu
/Nb6bA+ZHz+ZZwVuxCcHbk8UmUn6sQX3a1T8XvNQgW9nvBVKh3ymycq26AL4pYRVxZzgw1xRDBX3o/8qhNp6zFrEKoUpda9B2EmxrMpvypSSdyK9rX/nqYa+X88SvkeY9ud/1z6s/HIIsYPYxPUwwawLp7sItO0mqj
/5bcTU7+FVVWxxMuPlRHkKfwwAHodpsJnV9oTe5YXYRs206dXIPQ==
.           86400   IN       NSEC     aaa. NS SOA RRSIG NSEC DNSKEY
.           86400   IN       RRSIG   NSEC 8 0 86400 20180711050000 20180628040000 39570 .
DIdwGayG4W1vHlR7NBU1hQNVpYOhR80Rk6fYhfTe+i2goO56yYlDhPMV0z1C7VTL3P7Z10LtirFu0Wn3WztFa6G+B8GX09mt7XBtWKGBI212TsYMufPH5b4bGpv74GkLmk/e/x1LG2Vg3BegUW+i
/SKGh4o7VUlowI+MRd5pw4Dawb1R5uh29xEV5aR6VZ+KDiw17tF9+0AaWiK1+jtxyxSy9cQrxNdmdKblwzCuf+rHVvDv1BIwpBb4B8pG6sGWbf+FlvvLjOz/nnYaBBOTVnagzrzw8JOnmkEmnr3nShz4ERYvY9v4i
.           172800  IN       DNSKEY   256 3 8 AwEAAU4aK1DgEpXWWpH5aXHJZi1Vm9Cm42mGAsqkz3akFctS6zsZHC3pNNMug99fKa7OW+tRHIwZEc//mX8Jt6bcw5bPgRHG6u2eT8vUj
/ZP+VdrhWZDeEWZRRPBLjByBWTH1+v/f+xtvTJ3Stcq2tEqnzS2CCOr6RTJepprYhu+5Yl6aRzmEVbK27WCW1Zrk1LekJvJXfcyKSKk19C5M5JWX58px6nB1IS0pMs6aCIK2yaQQVNUEg9XyQzBSv/rMxVNNy3VAqO:
.           172800  IN       DNSKEY   256 3 8 AwEAAfaiFsqh+9ItxYRCwuiY0FY2NkaEwd/zmyVvakixDgT0kgG
/PUz1EauAiKz1xGwezjqbKFPswrY3qHmbbsSTY6G8hZtna8k26eCwy59Chh573cu8qtBkmUIXMYG3fSdlUREp+uhBWBfKI2aGwhRmQYR0zSmg7PGode34c/rOItKlebJhjTAJ6TmnON7qMfk/1KvH4qOvYtzstLhr:
/nEyFyTduRbz1nzqkp6yMuHwWVsABK81UYXSaUrDasuMSldhafmR/A15BxNhv9M7mzJj7UH2RVME9JbYinBEzWwW9GpnY+ZmBWgZiRVTaDuemCTJ5ZJWLRs=
.           172800  IN       DNSKEY   257 3 8 AwEAAgAIK1VZrpC6Ia7gEzahOR+9W29euxhJhVVL0yQbSEW008gcCjFFVQUTf6v5f8LjwBd0YI0EzrAcQqBGCzh/RStIo08g0NfnfL2M:
/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjr0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGlcGOYl70yQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqj
```

Getting access to zone files

Access to the **root zone** file is **available** for **everyone** and can be done with different tools.

Access to top-level domain name (**TLD**) zone files is available **depending** on the **TLD**.

All **new gTLDs** are **available** at ICANN's Centralized Zone Data Service (**CZDS**).

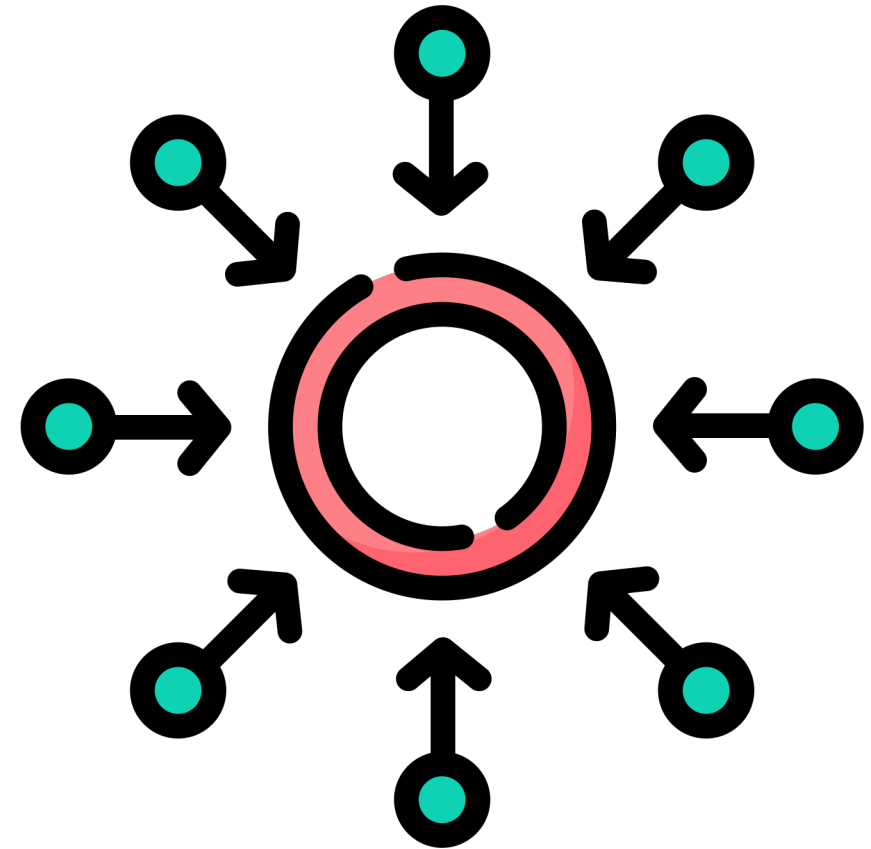
Some TLDs offer their zone files **directly**, but many **other** TLDs **do not publish** their zone files, such as .de.



Centralized Zone Data Service

The Centralized Zone Data Service (**CZDS**) provides a **centralized access** point for interested parties to request access to the Zone Files provided by **participating** TLDs.

You may sign up for CZDS at ICANN, but you will need to request access to each TLD zone file you want to access. However, Terms and Conditions are forbidding to misuse this access.



Thank you!