

DNS-Zonen

Im Jahr 1987 veröffentlichte die Internet Engineering Task Force (IETF) in ihrer Spezifikation namens RFC 1035 „Domain Names - Implementation And Specification“ den Begriff der DNS-Zone. In diesem Dokument wird der Zusammenhang zwischen Nameservern und DNS-Zonen erläutert.

Alle Informationen zum Thema DNS-Zonen sind im betreffenden RFC-Dokument ersichtlich:
<https://www.rfc-editor.org/rfc/rfc1035>

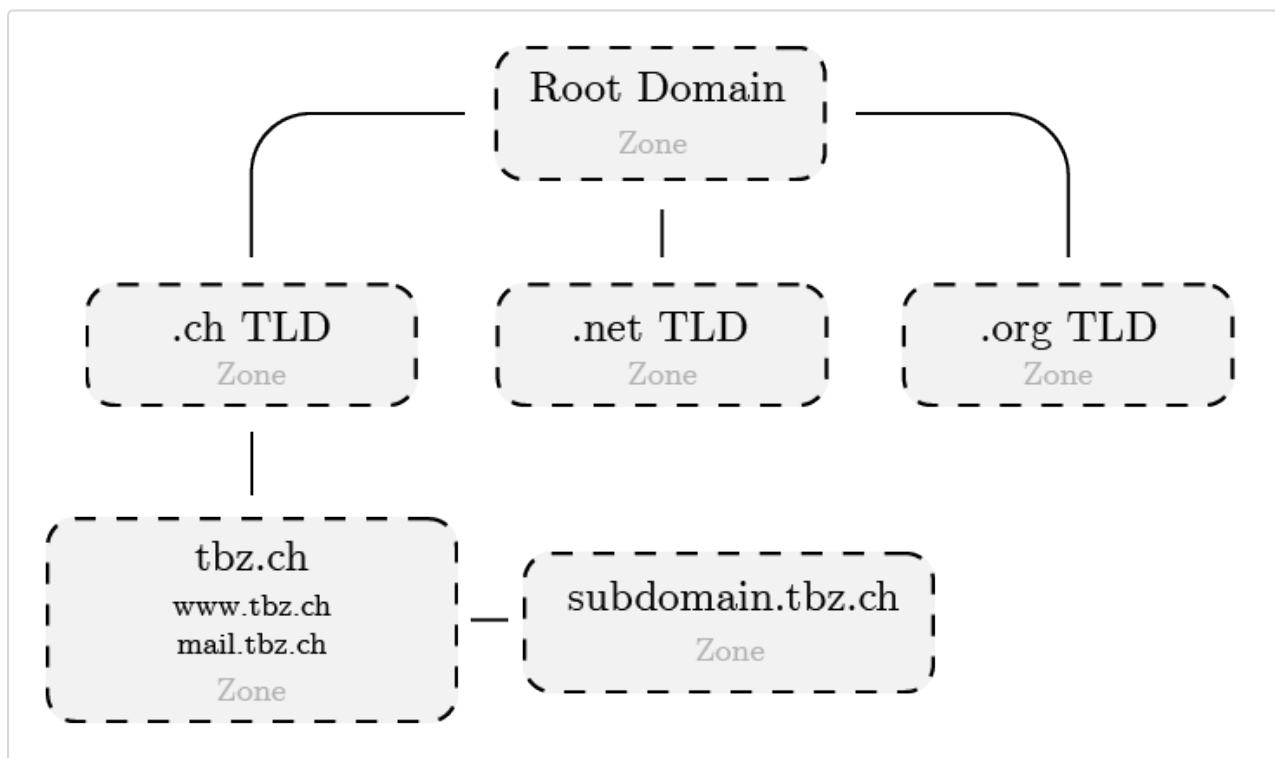
Der DNS-Namensraum wird durch DNS-Zonen definiert, die von einer spezifischen Organisation oder Person verwaltet werden. Eine Zone ist eine administrative Einheit, die mindestens eine Domain und ggf. weitere Subdomains umfasst. Subdomains können jedoch auch als eigene Zonen konfiguriert werden.

Die Zonendatei, auch als DNS Zone File bezeichnet, ist die technische Grundlage zur Speicherung der DNS Informationen einer Zone. Sie ist eine Textdatei, die auf einem Server gespeichert wird. Der Aufbau einer DNS Zone File ist im bereits erwähnten RFC 1035 definiert. Jede Zone File ist zeilenbasiert strukturiert und enthält je Zeile eine „Directive“ oder einen „Resource Record“.

Auf der untenstehenden Grafik ist ersichtlich, dass jeder Teil des DNS-Namespaces über eine eigene Zonen-Datei verfügt. Die Root-Zone enthält eine eigene Zonendatei. In dieser Datei sind die DNS-Einträge vorhanden, welche auf die Nameserver für die Top-Level-Domains verweisen. So ist z. B. ein Verweis auf die Nameserver der TLD .ch enthalten.

Die Nameserver der Top-Level-Domains enthalten wiederum eine eigene Zonendatei, in der die Nameserver-Informationen aller untergeordneten Domains enthalten sind. Die Zonendatei der .ch-Zone enthält somit alle .ch Domains wie tzb.ch, google.ch, coop.ch u.s.w.

Die eigentlichen DNS-Information von tbz.ch liegen dann in der Zonendatei von tbz.ch. Darin enthalten sind all die DNS-Informationen für die verschiedenen Hosts wie www.tbz.ch und mail.tbz.ch. In gewissen Fällen sind Subdomains in eigenen Zonendateien ausgelagert und die Zonendatei der übergeordneten Zone enthält einen Verweis für diese Subdomain.



Auftrag 1: Die Zonendatei der Root-Zone ist öffentlich einsehbar. Es handelt sich genau um jene Datei, welche auf allen 13 Root-Nameserver (inkl. deren Spiegelungen) verteilt ist.

<https://www.iana.org/domains/root/files>

Öffnen Sie das Root Zone File (HTTP) und suchen Sie darin die Informationen zur .CH Zone. Wie lauten diese?

```
ch.      172800  IN  NS  a.nic.ch.
ch.      172800  IN  NS  b.nic.ch.
ch.      172800  IN  NS  d.nic.ch.
```

```
ch.      172800  IN   NS    e.nic.ch.
ch.      172800  IN   NS    f.nic.ch.
ch.      86400   IN   DS    10 13 2
0E175543A74D9083EA977BAB2BEE98A771995F80982FB796B2B0B9CC6413D1A6
ch.      86400   IN   RRSIG  DS 8 1 86400 20221227050000 20221214040000 18733 .
D39MuhB3NqrjbpFLj+L/Guws9+ROsLIBe6AuD1uf3X4s2k+YHgZGKZPVzRwNc97cjY5l6lbubSWMc50mtCy
DCEoMYgQHI3GpinKitY2r6AWGJJeYcgDI6M7Q0YjdCO9AX3gbGEXw0ixlBoALgXxB3/GYF0nfM1vmgBW3qC
FL14ruj691UgtD/rb0f1RpFCrFSF4EuNL5F/P+v1spPpoAmrVbiovdTy6GejvLJlnpZ96y+Leg9te1J61MUI/Hh6
gFrBNB6zBl+wLI2gOrup8ajxiC5IGEDRI/5gisb9mA7gkAz/psNCSakKlqR51qx Cf/fS+a48t4Ma0j/9SMQUbRa
g==
ch.      86400   IN   NSEC   chanel. NS DS RRSIG NSEC
ch.      86400   IN   RRSIG  NSEC 8 1 86400 20221227050000 20221214040000 18733 .
3IKglUDT/CBIMwfkSP9MdNLARS1UyZWNgj41TAftS0hB4ZlappbJgTEhQpFNssjAVipHC6wGodv5sZkj/SLUD
Zb8AGZAh6O66X58SONmx0LDBmLj5vpzCi+ivQHB89whi1En18y/92INeZW0lx8eEWD4XaZSqveu/EidN4
qyDLpdKin3acsY1wAV8+3TL7cRAKCEnRB7B5xJshZH7DThUyUb3tdok4Kw8Csi6XSiGIFW30JfLeX+1bla7H
wcbfyzMbDnawt2lfMKVzl9quGVvoykgSiSMHO/idGfiH44fSWOtt7nkQh8lQLqQfirvr5amKepEylGm1HCgdp
q32Xk2A==
ns.itu.ch. 172800  IN   A     156.106.192.121
ns.itu.ch. 172800  IN   AAAA   2a00:7580:60:2141:0:0:0:10
a.nic.ch.  172800  IN   A     130.59.31.41
a.nic.ch.  172800  IN   AAAA   2001:620:0:ff:0:0:0:56
b.nic.ch.  172800  IN   A     130.59.31.43
b.nic.ch.  172800  IN   AAAA   2001:620:0:ff:0:0:0:58
d.nic.ch.  172800  IN   A     194.0.25.39
d.nic.ch.  172800  IN   AAAA   2001:678:20:0:0:0:0:39
e.nic.ch.  172800  IN   A     194.0.17.1
e.nic.ch.  172800  IN   AAAA   2001:678:3:0:0:0:0:1
f.nic.ch.  172800  IN   A     194.146.106.10
f.nic.ch.  172800  IN   AAAA   2001:67c:1010:2:0:0:0:53
```

Die Root-Zone wird von der Organisation IANA verwaltet. <https://www.iana.org/domains> Sämtliche Anpassung an der Zone werden von dieser Organisation koordiniert. Berechtigt für Änderungen sind alle Betreiber einer Top-Level-Domain wie z. B. die SWITCH für .ch und die DENIC für .de.

Auftrag 2: Auch die Zonendatei der .CH Zone kann öffentlich abgerufen werden. Diese ist mit rund einem Gigabyte aber wesentlich grösser und enthält mit rund 11 Millionen Einträge, wesentlich mehr Informationen als die Root-Zone.

Nicht jede Zone einer TLD ist öffentlich einsehbar. Dies hängt ganz von der Organisation ab, welche die betreffende Zone betreut.

Frage: Auf welchen Nameservern ist die Zonendatei der .CH Zone genau abgelegt? Geben Sie mindestens 3 Nameserver an. (Tipp: Insgesamt sind es 5 Nameserver auf denen die Datei abgelegt ist)

a.nic.ch.	172800	IN	A	130.59.31.41
b.nic.ch.	172800	IN	A	130.59.31.43
d.nic.ch.	172800	IN	A	194.0.25.39
e.nic.ch.	172800	IN	A	194.0.17.1
f.nic.ch.	172800	IN	A	194.146.106.10

Auftrag 3: Finden Sie heraus, wer für die Betreuung der .CH Zone zuständig ist. (Tipp. schauen Sie sich mal die TLD-Nameserver von .CH an) Wie müssen Sie vorgehen, wenn Sie eine eigene Domain in der .CH Zone hinterlegt haben möchten?

In der Schweiz ist die Organisation SWITCH für die Verwaltung zuständig.

Möchte man eine Domain in der .CH Zone hinterlegt haben, so muss man die gewünschte Domain zu erst kaufen (registrieren). Der Reigstrar hinterlegt dann die gewünschten Nameserver-Informationen in der .CH Zone.

Die Zonen-Datei der .CH Zone ist mit einem Gigabyte wesentlich grösser als die Zonendatei der Root-Zone. Aus diesem Grund ist die nachfolgende Aufgabe **freiwillig**.

Auftrag optional:

Diesen Auftrag schauen wir uns in der Klasse gemeinsam am Beamer an.

Laden Sie die Zonen-Datei [hier](#) herunter und öffnen Sie diese in einem geeigneten Editor. Manche Editoren kommen mit der grossen Dateigrösse nicht zurecht. Der Editor Visual Studio Code funktioniert

jedoch recht gut.

Öffnen Sie die Datei und suchen Sie die Informationen zur Domain tbz.ch. Wie lauten diese:

```
tbz.ch.      3600  IN   NS   ns1.hosting.ch.  
tbz.ch.      3600  IN   NS   ns2.hosting.ch.
```

Nehmen Sie sich 5 Minuten Zeit und stöbern Sie etwas in der Zonen-Datei. Können Sie anhand der Daten ungefähr herausfinden wie viele Tennis-Clubs (tc-) es in der Schweiz gibt, was die Migros (migros) alles für Domains verwendet oder es Domains mit Ihrem Namen gibt.

Frage: Wie finden Domains mit Umlauten (äöü) oder z. B. Emojis 🇨🇭 in der Zonen-Datei? Denken Sie an die letzte Übung mit den Domain-Namen.

Wenn die Domain mit xn-- beginnt, wird diese ein Sonderzeichen oder Emoji enthalten.

Die Zone einer Domain

Die Zone einer spezifischen Domain ist in der Regel nicht öffentlich einsehbar, da diese mitunter sensible Informationen enthalten kann. Sie sehen aber nun nachfolgend ein Beispiel, wie die Zonendatei der DNS-Zone von tbz.ch aussehen könnte:

```
$TTL      600
@         IN      SOA      ns1.hosting.ch hostmaster.tbz.ch. (
                                2125762      ; Serial
                                604800      ; Refresh Time
                                86400      ; Retry Time
                                2419200     ; Expire Time
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       ns1.hosting.ch.
@         IN      NS       ns2.hosting.ch.
@         IN      A        149.126.4.25
@[]      IN      MX[]      tbz-ch.mail.protection.outlook.com.
@[]      IN      TXT       "MS=ms26028428"
@[]      IN      TXT       "0hh6wyw3v2cqrmmmyv7lfhpx5xtnsy3"
@[]      IN      TXT       "v=spf1 a: edge-mta001.tam.ch a: edge-mta002.tam.ch ip4: 91.250.83.194
ip4: 80.74.157.0/24 include:spf.protection.outlook.com a: mail01.refline.ch a: mail02.refline.ch -all"
intranet IN      CNAME     intranet.tam.ch.
www       IN      CNAME     s016.cyon.net.
```

Der erste Block von Zeile 1 bis Zeile 8 enthält den SOA-Eintrag mit den grundlegenden Zonen-Informationen. Dieser Eintrag steuert, wie lange die Datei im Cache bleiben darf und wie die Regeln bei einem Sync zwischen einem Primary- und Secondary-Nameserver sind. Dies wird gemacht, wenn zwei Nameserver zur besseren Redundanz existieren und die Daten zwischen den beiden Nameservern abgeglichen werden müssen. Dies ist aber nicht Teil dieses Moduls, hier arbeiten wir der Einfachheit halber nur mit einem Nameserver.

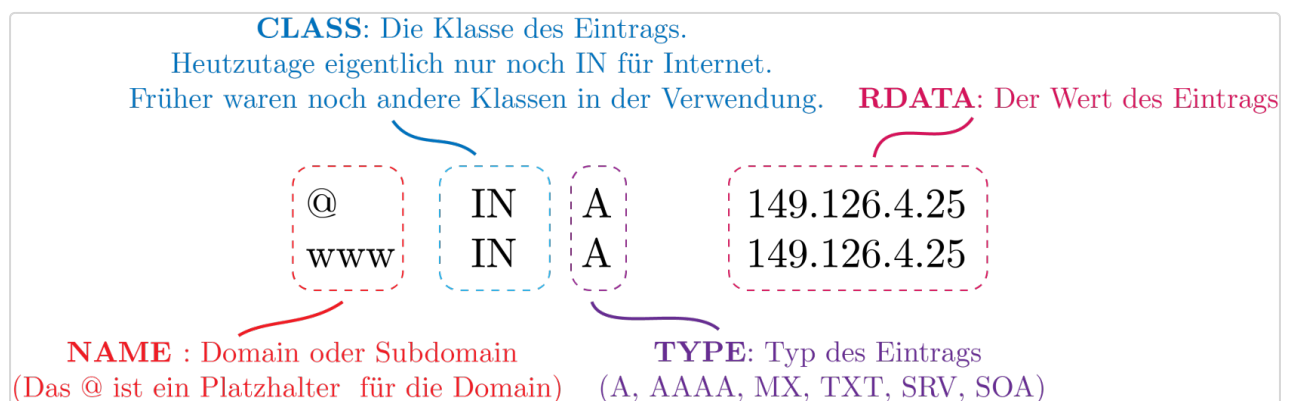
- **TTL (Time to live):** Die Dauer, wie lange diese Zone von einem DNS-Client oder Resolver im Cache behalten werden kann. Je kürzer diese TTL gehalten ist, desto schneller propagieren Änderungen an der DNS-Zone, jedoch verursacht dies auch eine höhere Last auf dem Server.
- **Primary Master** für diese Zone (ns1.hosting.ch):
 - er definiert, an wen dynamische Updates gesendet werden sollen (siehe: [Dynamisches Update](#))
 - er gibt an, an wen keine Notifies gesendet werden (siehe: [Zonentransfer](#))

- **RNAME** (hostmaster.tbz.ch): Mail-Adresse des Verantwortlichen für diese Zone. (Das @ wird durch . ersetzt. Punkte vor dem @ werden durch \. ersetzt; beispielsweise max\. mustermann. wikipedia. org für die E-Mail Adresse max. mustermann@wikipedia. org)
- **Serial**: Seriennummer, die bei jeder Änderung um den Wert ein erhöht wird (vorzugsweise JJJJMMTTVV; dient als Hinweis, wann die Zone zuletzt aktualisiert wurde)
- **REFRESH**: Sekundenabstand, in dem sekundäre Nameserver die Seriennummer vom primären Master abfragen sollen, um Änderungen der Zone festzustellen. Empfehlung vom RIPE NCC für kleine und stabile Zonen: 86400 $\pm$ 24 Stunden.
- **RETRY**: Sekundenabstand, in dem, bei ausbleibender Antwort des Masters, sekundäre Nameserver nochmals seine Seriennummer abfragen sollen. Dieser Wert muss kleiner als jener zum Refresh sein. Empfehlung vom RIPE NCC für kleine und stabile Zonen: 7200 $\pm$ 2 Stunden.
- **EXPIRE**: Sekundenabstand, nach dem bei ausbleibender Antwort des Masters sekundäre Nameserver keine Antworten über die Zone mehr geben sollen. Dieser Wert muss größer als die Summe jener zum Refresh und Retry sein. Empfehlung vom RIPE NCC für kleine und stabile Zonen: 3600000 $\pm$ 1000 Stunden.

Nun folgen auf den Zeilen 9 bis 17 die DNS-Informationen der Zone tbz.ch. Beachten Sie die Regeln auf folgender Wikipedia-Seite zum Aufbau der DNS-Informationen:

<https://de.wikipedia.org/wiki/Zonendatei>

Ein einzelner DNS-Eintrag ist jeweils wie folgt aufgebaut:



Auftrag: Recherchieren Sie nun die Bedeutung der folgenden Ressource-Typen (TYPE).

Der A-Eintrag verweist auf eine IPv4 Adresse

Der AAAA-Eintrag verweist auf eine IPv6 Adresse

Der CNAME-Eintrag (Canonical Name) verweist auf einen anderen DNS-Eintrag z. B.

tbz.ch	IN	A	149.126.4.25
www.tbz.ch	IN	CNAME	tbz.ch

Der Eintrag **www.tbz.ch** verweist auf **tbz.ch**, welcher wiederum auf die IP-Adresse **149.126.4.25**. Somit verweist der DNS-Eintrag **www.tbz.ch** auf die IP-Adresse **149.126.4.25**

Der MX-Eintrag (Mail Exchange) verweist auf den Hostnamen (nicht die IP-Adresse) eines Mailservers. Der MX-Eintrag wird somit nur von Mailservern abgefragt. Hat der Mailserver nur eine IP-Adresse, so muss ein A-Eintrag erstellt werden, auf den der MX-Eintrag verweisen kann. z .B

tbz.ch	IN	MX	mail.tbz.ch.
mail.tbz.ch	IN	A	104.47.11.74

Der TXT-Eintrag beinhaltet eine Text-Information. Diese wird in der DNS-Zone hinterlegt und kann z. B. zur Domainbasierten Verifikation oder Bereitstellung zusätzlicher Informationen wie SPF und DKIM verwendet werden.

Revision #7

Created 14 December 2022 15:56:03 by Admin

Updated 15 December 2022 07:36:13 by Admin