**Engineer**

# DNS

das Verzeichnis, das Namen in Adressen auflöst

## Was es ist

DNS, das Domain Name System, ist das verteilte Verzeichnis, das das Internet vor fast allem anderen abfragt. Ein Programm, das einen Namen wie `example.com` kennt, fragt dort nach der Adresse, zu der es sich verbinden soll. Dasselbe System beantwortet einige weitere Fragen zu diesem Namen: welche Server seine E-Mails annehmen, welchen Text sein Inhaber veröffentlicht hat und welche Server dafür zuständig sind.

Das Verzeichnis ist ein von rechts nach links gelesener Baum. Oben steht die Wurzel, darunter Top-Level-Domains wie `.com` oder `.dk`, darunter die von Menschen registrierten Domains und darunter alle von ihren Inhabern angelegten Subdomains. Kein einzelner Server enthält den gesamten Baum. Jede Ebene übergibt die Verantwortung für die nächste an benannte Server. Der Teil des Baums, für den eine Servergruppe antwortet, heißt Zone. Wer eine Zone kontrolliert, entscheidet, auf welche Ziele ihre Namen aufgelöst werden.

Zwei Serverarten erledigen die Arbeit. Autoritative Server halten eine Zone und geben für sie die verbindliche Antwort. Rekursive Resolver von Internetanbietern, Unternehmen oder öffentlich zugänglichen Diensten gehen den Weg für einen Client: Sie fragen einen Rootserver nach `.com`, `.com` nach `example.com`, die Server dieser Domain nach dem Eintrag und geben die Antwort zurück. Ihr Betriebssystem betreibt nur einen kleinen Stub-Resolver, der die Frage an einen rekursiven weitergibt und wartet.

Die Antworten sind typisierte Einträge. Die klassische Schreibweise dafür ist eine Zonendatei:

```
$ORIGIN example.com.
$TTL 3600
@     IN  SOA    ns1.example.net. hostmaster.example.com. (
                 2026101701 7200 900 1209600 300 )
@     IN  NS     ns1.example.net.
@     IN  A      192.0.2.10
@     IN  AAAA   2001:db8::10
www   IN  CNAME  example.com.
@     IN  MX     10 mail.example.net.
@     IN  TXT    "v=spf1 include:_spf.example.net -all"
```

`A` und `AAAA` liefern IPv4- und IPv6-Adressen. `CNAME` macht einen Namen zum Alias eines anderen. `MX` benennt den empfangenden Mailserver; `TXT` enthält freien Text, in der Praxis Richtlinien zur Mailauthentifizierung und Nachweise der Kontrolle über die Domain. `NS` und `SOA` beschreiben die Zone selbst.

Jeder Eintrag hat eine Gültigkeitsdauer, hier 3.600 Sekunden. Diese Zahl ist der Schlüssel zum Verhalten von DNS. Ein Resolver darf eine abgerufene Antwort bis zum Ablauf ihrer TTL wiederverwenden, ohne erneut zu fragen. So beantwortet das System die meisten Abfragen aus einem Cache nahe am Client und antwortet weiter, wenn ein autoritativer Server kurz nicht erreichbar ist. Der Preis: Niemand kann die Welt zwingen, eine alte Antwort vorzeitig zu vergessen.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist DNS?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. WLAN, Firewalls und Fernzugriff werden so eingerichtet, dass Mitarbeitende von überall arbeiten können und nur Berechtigte Zugang erhalten.

**Unsere Leistungen entdecken** Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 30 Ubuntu-Linux-VPS-Instanzen verwaltet — 30 verwaltete Linux-Server mit geplantem Wiederherstellungsweg

**30 Ubuntu-Linux-VPS-Instanzen verwaltet** Kontakt aufnehmen →

## Warum es wichtig ist

Jede Verbindung zu einem benannten Dienst beginnt mit einer Abfrage. Ist DNS falsch, können die Server völlig gesund sein, während Website, API und Mail trotzdem ausgefallen wirken, weil nichts sie erreicht. Funktioniert DNS, bemerkt es niemand. Deshalb ist es oft der am wenigsten dokumentierte Systemteil.

Über DNS wird auch die Kontrolle über eine Domain ausgeübt und nachgewiesen. Mailanbieter lesen SPF-, DKIM- und DMARC-Richtlinien aus `TXT`-Einträgen, um über die Echtheit einer angeblich von Ihrer Domain stammenden Nachricht zu entscheiden. Ein falscher oder fehlender Eintrag schickt deshalb legitime E-Mails in den Spam. Zertifizierungsstellen und gehostete Dienste verlangen einen Eintrag mit einem bestimmten Wert als Nachweis des Namensbesitzes. Wer die Zone bearbeiten kann, kann die Website umleiten, Mail abfangen und Zertifikate für die Domain erhalten. Der Zugang zum DNS-Konto ist deshalb genauso sensibel wie der Serverzugang.

Caching prägt jede Änderung. Die sogenannte Propagation besteht tatsächlich aus Tausenden Resolvern, die jeweils auf den Ablauf ihrer eigenen Kopie warten. Für einen Websiteumzug mit wenigen Unterbrechungen senkt man die TTL etwa einen Tag vorher, wartet die alte TTL ab, nimmt die Änderung vor und erhöht die TTL wieder, sobald sich alles eingependelt hat.

Klassisches DNS überträgt Klartext. Weder Antworten noch Fragen sind vertraulich. Mit DNSSEC kann ein Resolver prüfen, ob eine Antwort wirklich vom Zoneninhaber stammt und unverändert blieb. Laut eigener Spezifikation fügt es keine Vertraulichkeit hinzu. Verschlüsselte Übertragungswege wie DNS over HTTPS verbergen die Fragen auf dem Netzwerkweg. Der Resolver am anderen Ende sieht trotzdem jeden angefragten Namen. Wer einen Resolver wählt, entscheidet, wer diese Liste bekommt.

## Wie es in der Praxis aussieht

Die eigene Zone des Unternehmens zeigt den üblichen Ausgangspunkt und einen Weg daraus. Sie enthielt etwa zwanzig Einträge in der Webkonsole eines Anbieters: für den Webauftritt, eine git-Subdomain, zwei persönliche Weiterleitungen, Mail über einen gehosteten Postfachanbieter, eine Domain für Transaktionsmails und die Authentifizierungseinträge für beide Mailbereiche. In einer Konsole ist der aktuelle Stand das, was die Person hinterlassen hat, die dort zuletzt geklickt hat. Die Zone liegt jetzt als Daten in einem Repository: aktive Einträge, Anwendungseinträge, Einträge für Transportrichtlinien und eine getrennte Liste zu entfernender Einträge. Ein Play bringt den Zustand beim Anbieter über dessen API mit dieser Deklaration in Einklang. Zwei weitere Einstiegspunkte liegen hinter Tags, die ausdrücklich aktiviert werden müssen: ein Audit, das Unterschiede meldet, ohne etwas zu ändern, und ein Export, der die Zone im Standardformat einer Zonendatei schreibt, damit auch etwas anderes als das Repository sie lesen kann. Das Audit wird am häufigsten genutzt. Denn häufiger geht es darum, den Unterschied zu kennen, als ihn zu beseitigen.

Derselbe Anbieter hat bewusst eine eng begrenzte Aufgabe. Die Credits-Seite erklärt, dass Cloudflare DNS-Anfragen für die Website beantwortet und sonst nichts, ohne vorgeschalteten Proxy. Sie nennt die Serveradresse offen, weil DNS sie ohnehin jedem Anfragenden gibt.

DNS zu lesen gehört auch zur regelmäßigen Beschreibung der Systemlandschaft. Zu sieben nur lesenden Berichtsrollen, die den laufenden Host in Markdown abbilden gehört ein Anbieterinventar, das DNS neben zwei Cloud-APIs und einer API für dedizierte Server liest. Dabei gilt die Regel, dass kein Bericht eine Zahl ausgibt, die sein Lauf nicht gemessen hat.

## Wo es schiefgeht

DNS-Ausfälle treten oft verzögert auf, bleiben im Cache bestehen oder wirken sich je nach Nutzer unterschiedlich aus. Derselbe Name funktioniert deshalb für eine Person und für eine andere nicht. Diese Fälle kehren wieder.

Eine Änderung setzt sich nicht durch. Jemand bearbeitet einen Eintrag mit einem Tag TTL und erwartet die sofortige Wirksamkeit der neuen Adresse. Resolver mit der alten Antwort im Cache liefern sie jedoch bis zum Ablauf ihrer Kopie weiter aus. Eine leisere Variante trifft neue Namen: Wurde ein Name vor dem Anlegen seines Eintrags abgefragt, wird auch die negative Antwort gecacht, solange die `SOA` der Zone es erlaubt (RFC 2308). Senken Sie TTLs vor geplanten Änderungen und legen Sie Einträge an, bevor etwas sie abfragt.

Ein Alias steht an einer unzulässigen Stelle. Laut RFC 1034 darf ein Name mit `CNAME` keine anderen Daten enthalten. Die nackte Domain, `example.com` selbst, hat immer `SOA` - und `NS` -Einträge. Eine standardkonforme Zone kann die Zonenspitze deshalb nicht zum Alias machen. Ein `CNAME` auf einer Subdomain, die auch `MX` oder `TXT` benötigt, verletzt dieselbe Regel. Anbieter bieten abgeflachte oder `ALIAS` -Einträge als eigene Umgehung an. Jeder verhält sich etwas anders. Lesen Sie deshalb nach, was Ihr Anbieter tatsächlich ausliefert.

Die Mailauthentifizierung kippt. Jedes `include` eines SPF-Eintrags verursacht DNS-Abfragen, und RFC 7208 begrenzt ihre Gesamtzahl auf zehn. Das Hinzufügen eines weiteren Newsletter- oder Ticketdienstes kann den Eintrag über die Grenze bringen. Empfänger behandeln die Richtlinie dann als dauerhaften Fehler, und die eigentlich damit zu authentifizierende Mail wird ohne sie beurteilt. Zählen Sie die Abfragen bei jedem neu hinzugefügten Absender.

Ein Eintrag überlebt sein Ziel. Eine Subdomain verweist per `CNAME` auf einen inzwischen gelöschten Cloudspeicher-Bucket oder eine gehostete App. Erlaubt der Anbieter jedem, diesen Ressourcennamen zu beanspruchen, kann ein Fremder das tun und eigene Inhalte unter Ihrer Subdomain ausliefern, mit dem Ruf Ihrer Domain im Gepäck. Entfernen Sie den Eintrag in derselben Änderung wie sein Ziel.

Die Zone lebt nur in einer Konsole. Es gibt keine Historie, kein Review und keinen Diff. Eine versehentliche Löschung des `MX`-Eintrags fällt deshalb erst beim Ausbleiben der Mail auf. Der frühere Wert muss aus dem Gedächtnis rekonstruiert werden. Regelmäßige Zonenexporte oder besser ihre Deklaration als Code geben jeder Änderung einen Nachweis und einen Rückweg.

## Weiterführende Lektüre

- RFC 1035: Domain Names, Implementation and Specification — Eintragsformate, Zonendateisyntax und das Übertragungsprotokoll.
- RFC 1034: Domain Names, Concepts and Facilities — Baum, Zonen, Delegation und die Wege der Resolver.
- RFC 9499: DNS-Terminologie — genaue Definitionen der auf dieser Seite verwendeten Begriffe.
- RFC 2308: Negatives Caching von DNS-Abfragen — wie lange ein Resolver sich merken darf, dass ein Name nicht existiert.
- RFC 4033: Einführung und Anforderungen an DNS-Sicherheit — was DNSSEC schützt und was es unberührt lässt.
- RFC 8484: DNS-Abfragen über HTTPS — Namensabfragen innerhalb gewöhnlichen verschlüsselten Webverkehrs.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

**Preise ansehen** Kontakt aufnehmen →

# Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist DNS?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

**Unsere Leistungen entdecken**

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

**Mit Sorgfalt und Liebe gestaltet von D.**

**CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N**

**Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.**

**Gedruckt von https://engineer.company/de/glossary/dns/**