Schatten DNS - Überblick

06.07.2025 07:50:15

FAQ-Artikel-Ausdruck

Kategorie:	Datennetz::DNS	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	19:07:15 - 26.02.2025

Schlüsselwörter

Schatten-DNS DNS DNS-Resolver DNS-Server

Lösung (öffentlich)

Grundlagen: Von Domains, Zonen und DNS-Servern

Das "Domain Name System" (kurz DNS) ist das Telefonbuch des Internets. Es wird hauptsächlich dazu genutzt, damit Computer herausfinden können unter welcher IP-Adresse sie einen anderen Computer mit einem bestimmten Namen erreichen können.

Der DNS-Namensraum ist hierarchisch in einer Baum-Struktur aufgebaut, wobei ein Punkt die jeweiligen Ebenen trennt. Der Einstiegspunkt (Wurzel des Baums) ist die sog. Root-Zone, gekennzeichnet durch den Punkt ".". Darunter befinden sind die sogenannten "Top Level Domains" (TLD) wie "de." oder "org." und darunter schließlich was gemeinhin "Domain" genannt wird, wie zum Beispiel "tu-dresden.de." oder "example.org." Alles darunter wird gemeinhin als "Subdomain" bezeichnet, beispielsweise "www.tu-dresden.de." oder "blog.example.org.". Es gibt keine Limitierung wie viele Ebenen es geben kann, allerdings ist die Gesamtlänge eines Namens (Punkte eingeschlossen) auf 255 Zeichen begrenzt. Da der finale Punkt am Ende Teil jedes (absoluten) DNS-Namens ist, wird er außerhalb von DNS-Software zumeist weggelassen und impliziert.

Zonen dienen dazu, den oben beschriebenen gewaltigen DNS-Namensraum in sinnvoll verwaltbare Teilbereiche zu unterteilen. Diese Trennung ist rein organisatorisch und hat keine Auswirkung auf die Bedeutung eines DNS-Namens. Jeder Punkt in einem DNS-Namen ist potenziell eine Zonen-Grenze; muss es aber nicht sein. Analog zum DNS-Namensraum sind auch die Zonen hierarchisch in einer Baum-Struktur angeordnet. Die "Root Zone" ist die Wurzel, darunter kommen die Zonen der TLDs, und darunter jeweils die Zonen der Domains, und noch ggf. weitere Subzonen.

Das DNS ist eine Client-Server-Architektur: Der Client fragt einen Server nach Einträgen (Resource Records) eines bestimmten Typs (z.B. Typ A für IPv4-Adressen) für einen Namen, und dieser antwortet. DNS-Server (auch "Nameserver" genannt) werden strikt in zwei Rollen unterteilt: autoritative und rekursive. Autoritative DNS-Server stellen die Zonen bereit, und können Anfragen zu diesen Zonen definitiv und endgültig beantworten; allerdings nur genau für diese Zonen. Rekursive DNS-Server (auch Resolver genannt) hingegen haben selbst keine Zonen, können aber für einen angefragten DNS-Namen den zuständigen autoritativen DNS-Server ausfindig machen und von diesem die endgültige Antwort einholen. Ältere DNS-Server-Implementierungen erlauben es, gleichzeitig beide Rollen wahrzunehmen, moderne Implementierungen trennen diese Rollen aus Sicherheitsgründen vollständig. Endgeräte kommunizieren idR nicht direkt mit einem autoritativen DNS-Server, sondern implementieren lediglich einen sog. Stub Resolver, der Anfragen an einen oder mehrere vollwertige, rekursive DNS-Server weiterleitet; und dieser kümmert sich darum, die Frage zu beantworten.

Um eine Zone im DNS zu veröffentlichen, muss Sie in der darüber liegenden Zone mittels einer Delegation vermerkt werden. Eine Delegation besteht aus NS-Einträgen, welche festlegt, welche DNS-Server für diese Zone autoritativ sind. In der "Root Zone" gibt es deshalb Delegationen für jede TLD, und in den jeweiligen TLD-Zonen gibt es Delegationen für die second-level Domains usw. Wenn rekursive DNS-Server den autoritativen DNS-Server für einen DNS-Namen suchen, dann starten diese immer in der Root-Zone und hangeln sich anhand der Delegationen durch den Baum bis es keine weitere Subzone mehr gibt. Und da die Zonen alle öffentlich sind, haben alle rekursiven DNS-Server Zugang zu den gleichen Daten und kommen unabhängig voneinander für eine gegeben Frage zur gleichen Antwort.

Was ist Schatten-DNS?

Kontrolliert man einen rekursiven DNS-Server könnte man in Versuchung kommen, dort unabhängig von der tatsächlichen Delegationskette von der Root-Zone aus lokal eine eigene Zone "mysecretzone.example.org." zu konfigurieren. Obwohl es in der Eltern-Zone "example.org." keine Delegation gibt und damit diese Zone eigentlich nicht existiert, würde dieser DNS-Server auch alle Anfragen zu "mysecretzone.example.org." beantworten. Eine derartige Konfiguration bezeichnen wir als Schatten-DNS: Spezielle DNS-Server antworten auf Anfragen für Zonen, für die keine gültige Delegationskette von der Root-Zone aus existiert.

Der riesige Nachteil ist, dass das nur solange funktioniert wie man diesen speziellen, "richtigen" DNS-Server verwendet. Sobald ein anderer rekursiver DNS-Server verwendet wird, der sich von der Root-Zone aus über die Delegationen durcharbeitet, können die Namen aus der Schatten-Zone nicht mehr aufgelöst werden. Es müssen also auf allen relevanten Geräten die "richtigen" DNS-Server konfiguriert sein; vom Desktop-PC über Laptop, Tablet, Smartphone bis zum Server. Schnell mal ins WLAN? Eduroam verwendet standardmäßig die "falschen" DNS-Server (die vom ZIH). Ein Zertifikat von LetsEncrypt ausstellen? Keine Chance, die verwenden definitiv die "falschen" DNS-Server.

Und das sind nur einige Beispiele.

Mit dem Einsatz von DNSSEC wird das Problem noch viel schlimmer. DNSSEC ist eine Technik bei der Zonen und deren Inhalt kryptografisch signiert werden, damit wird es möglich Manipulationen in DNS-Antworten zu entdecken. Denn genau das ist Schatten-DNS.

Wie macht man es besser

Die naheliegendste Lösung ist es alle Zonen ordentlich im DNS per Delegation zu verankern. Ebenso wie das Telefonbuch öffentlich einsehbar ist, sollte auch das DNS öffentlich einsehbar sein. Den eigentlichen Zugriffsschutz übernimmt dann (hoffentlich korrekt konfigurierte) Firewall(s). Damit wird es wieder egal welchen rekursiven DNS-Server man verwendet, da alle für eine gegebene Frage zur gleichen Antwort kommen; es gibt keinen "richtigen" DNS-Server mehr (bzw. jeder DNS-Server ist der "richtige").

Die einfachste Variante ist es, die Verwaltung der Zone vollständig an das ZIH abzugeben. Wir verwalten bereits die Zonen für die gesamte "tu-dresden.de" Domain sowie einer großen Anzahl weiterer Domains, und haben dafür die notwendige Infrastruktur und Prozesse. Jegliche Änderung an der Zone kann über ein Ticket beim ServiceDesk angefordert werden.

Das ist aber nicht immer möglich und/oder praktikabel, da man die direkte Kontrolle über Verwaltung der Zone und deren Inhalt abgibt. Als zweite Variante besteht die Möglichkeit, stattdessen mit Hilfe des "Zonen-Transfer" genannten Mechanismus die Zone automatisch von dem eigenen DNS-Server auf die DNS-Server des ZIH zu transferieren. Das ZIH stellt dabei die Verfügbarkeit der Zone sicher, und übernimmt zukünftig auch die DNSSEC-Signierung und die damit zusammenhängende Schlüsselverwaltung.

Wenn es doch sehr sensitiv ist

In bestimmten Fällen gibt es ein berechtigtes Interesse, Zonen nicht öffentlich zugänglich zu machen. Ähnlich wie in der vorherigen Variante wird eine ordentliche Delegation im DNS eingetragen und die Zone automatisch via Zonen-Transfer zum ZIH transferiert. Die Zone selbst wird aber von separaten autoritativen DNS-Servern bereitgestellt, welche nicht aus dem Internet sondern nur aus den TUD-Netzen erreichbar sind. Diese Lösung mag auf den ersten Blick nicht viel besser erscheinen als Schatten-DNS, hat aber signifikante Vorteile:

- Aus dem Internet sieht man (anhand der Delegation) nur, dass die Zone existiert aber nicht ihren Inhalt
- Da es eine korrekte Delegations-Kette gibt, können alle rekursiven DNS-Server in den TUD-Netzen (nicht nur die des ZIH!) ohne zusätzliche Konfiguration Namen aus dieser Zone auflösen
- Durch die ebenfalls korrekt vorhandene DNSSEC-Kette können alle Endgeräte die Richtigkeit der Antwort verifizieren, es sind keine mutwilligen Manipulationen notwendig
- Anfragen aus dem Internet werden mit einem expliziten "Keine Berechtigung" Fehler beantwortet

Funktioniert das auch mit Windows-Domänen?

Ja, und entgegen allgemeiner Annahmen auch ohne negative Auswirkungen oder Einbußen von Funktionen.

Eine Windows-Domäne benötigt eine funktionierende DNS-Infrastruktur. Um das sicherzustellen hat sich Microsoft dafür entschieden, bei der Einrichtung eines Windows-Domänen-Controllers standardmäßig auch einen DNS-Server zu installieren, der sowohl als autoritativer als auch rekursiver DNS-Server agiert; und dieser wird standartmäßig von allen Domänen-Mitgliedern (inkl. der DCs selbst) verwendet. Und weil dies der Standard ist, hält sich hartnäckig die weitverbreitete Fehlannahme dass das zwangsläufig so sein muss. Aber tatsächlich ist auch das genaue Gegenteil möglich: Man kann eine voll funktionsfähige Windows-Domäne betreiben, bei der die DCs keinerlei DNS-Server-Funktionalität bereitstellen; also weder autoritativ für die DNS-Zonen sind, noch als DNS-Resolver für die Windows-Domänen-Mitglieder fungieren. Es gibt eigentlich nur zwei Bedingungen welche erüllt sein müssen: Die Windows-Domänen-Mitglieder müssen über DNSUPDATEs den Inhalt der DNS-Zonen anpassen können, und die Windows-Domänen-Mitglieder müssen den Inhalt der DNS-Zonen auflösen können. Solange dies der Fall ist, spielt es keine große Rolle was genau als DNS-Infrastruktur verwendet wird.

Im Kontext der TU Dresden werden die DCs (wie weiter oben beschrieben) nur noch als autoritative DNS-Server für ihre DNS-Zonen fungieren. Die DCs (und damit indirekt die Administrierenden der jeweiligen Windows-Domäne) behalten die Kontrolle über den Inhalt der DNS-Zonen, aber transferieren die fertige DNS-Zone zum ZIH. Da die DCs nur noch autoritativ und nicht mehr rekursiv agieren, müssen alle Windows-Domänen-Mitglieder nun dedizierte DNS-Resolver verwenden (normalerweise aber nicht zwangsläufig die des ZIH).

Ich möchte das, was muss ich tun?

Allgemein gesprochen müssen folgende Dinge eingerichtet werden:

- Ihr DNS-Server muss auf Port 53 via TCP und UDP von unserem DNS-Einliefer-Server (pdns1.zih.tu-dresden.de bzw. 141.76.10.196) erreichbar sein. Gegebenenfalls sind Firewall-Freischaltung(en) nötig.
- Ihr DNS-Server muss unserem DNS-Einliefer-Server (pdns1.zih.tu-dresden.de bzw. 141.76.10.196) erlauben, die jeweilige Zone per Zonen-Transfer (AXFR bzw. IXFR) abzufragen.
- Ihr DNS-Server sollte unserem DNS-Einliefer-Server (pdns1.zih.tu-dresden.de bzw. 141.76.10.196) mitteilen wenn es Änderung an der Zone gibt (NOTIFY).
- Dies ist nicht zwingend notwendig, stellt aber sicher das Änderungen sich zeitnah propagieren.

- In Ihrer DNS-Zone sind die korrekten Zonen-Metadaten hinterlegt (SOA-Record).
- Primär-Server (MNAME) ist Ihr DNS-Server
- Kontakt E-Mail Addresse (RNAME) ist hostmaster@tu-dresden.de (das @ wird

idR durch einen Punkt ersetzt)
- Aktualisierungsinterval (REFRESH) ist 6 Stunden (21600 Sekunden)
- Wiederholungsinterval (RETRY) ist 1 Stunde (3600 Sekunden)
- Zonengültigkeit (EXPIRE) ist 4 Wochen (28 Tage oder 2419200 Sekunden)
- Minimale Gültigkeitsdauer (MINIMUM) ist 1 Stunde (3600 Sekunden)

- In Ihrer DNS-Zone sind die korrekten autoritativen DNS-Server (NS-Records) eingetragen. Je nachdem ob die Zone öffentlich oder intern ist, müssen dies exakt die folgenden vier/zwei sein; nicht mehr und nicht weniger.
- öffentlich
- adns1.zih.tu-dresden.de
- adns2.zih.tu-dresden.de
- dns-1.dfn.de
- dns-3.dfn.de

- intern
- adns-internal1.zih.tu-dresden.de
- adns-internal2.zih.tu-dresden.de

Wir haben weitere FAQ-Artikel mit Konfigurationshilfen vorbereitet, um die Administrierenden bei der Einrichtung auf unterschiedlichen Plattformen zu unterstützen.

Außerdem bitte ein Ticket mit folgenden Informationen beim [1]ServiceDesk aufmachen, damit die Einrichtung des Zonen-Transfers sowie der DNS-Delegation durch das ZIH erfolgen kann:

- Name der zu transferierenden DNS-Zone(n)
- öffentliche oder interne Zone gewünscht
- Namen und IP-Adressen der autoritativen DNS-Server für diese Zonen (bei Windows-Domänen sind das alle DCs)
- Technische Ansprechperson (nur für interne Zwecke im Problemfall)

Natürlich können Sie sich auch jederzeit bei Fragen oder Problemen zu diesem Thema an den [2]ServiceDesk wenden.

[1] mailto:servicedesk@tu-dresden.de
[2] mailto:servicedesk@tu-dresden.de