DELEG - RENOVIERTE WEGWEISER

DDI User Group 09/26

CARSTEN STROTMANN

Created: 2026-09-24 Thu 09:10

DELEG - RENOVIERTE WEGWEISER

Carsten Strotmann

DNS(SEC)/DANE/DHCP/IPv6/Linux/xBSD/Security Trainer und Berater

DNS UND DELEGATION

- Kaum ein anderes Feature ist so definierend für DNS wie die Delegation
  - Die Delegation ermöglicht die verteilte DNS-Datenbank
  - Die Vorgänger-Technologie von DNS, die Datei `hosts.txt`, kannte keine Delegation

WAS GENAU IST "DELEGATION"

VERTEILTER NAMENSRAUM

- DNS bildet einen verteilten Namensraum
- Die DNS-Informationen sind über verschiedene Server im Internet verteilt
- DNS-Resolver finden die DNS-Authoritative-Server über die DNS-Delegation

NS-RECORDS

- Die NS-Records im DNS verweisen auf die DNS-Authoritative-Server einer DNS-Domain
    - Verweis = eng. "Referral"

```
example.com.      3600  IN NS  ns01.example.net.
example.com.      3600  IN NS  ns02.example.net.
```

NS-RECORDS

- Die NS-Records für eine DNS-Domain finden sich auf zwei Ebenden in der DNS-Hierarchie:
  - In der Zone oberhalb der DNS-Domain (Elternzone) = delegierende Zone
  - In der Zone für die DNS-Domain (Kindzone) = delegierte Zone
- Die NS-Records an beiden Stellen sollten inhaltlich identisch sein (gleiche Anzahl, gleiche Server-Namen)
- NS-Records liefern immer einen (Host-)Domain-Namen für einen DNS-Server, nicht die IP-Adressen

GLUE-RECORDS

- Liegen die DNS-Domain-Namen der DNS-Server für eine DNS-Domain innerhalb der delegierten Domain, so besteht ein "Henne-Ei-Problem":
  - Ein DNS-Resolver braucht die IP-Adressen der DNS-Server der Zone
  - Um diese IP-Adressen zu bekommen, muss der mit den DNS-Servern der Zone sprechen
  - Ohne die IP-Adressen kann er noch nicht mit den DNS-Servern sprechen

GLUE-RECORDS

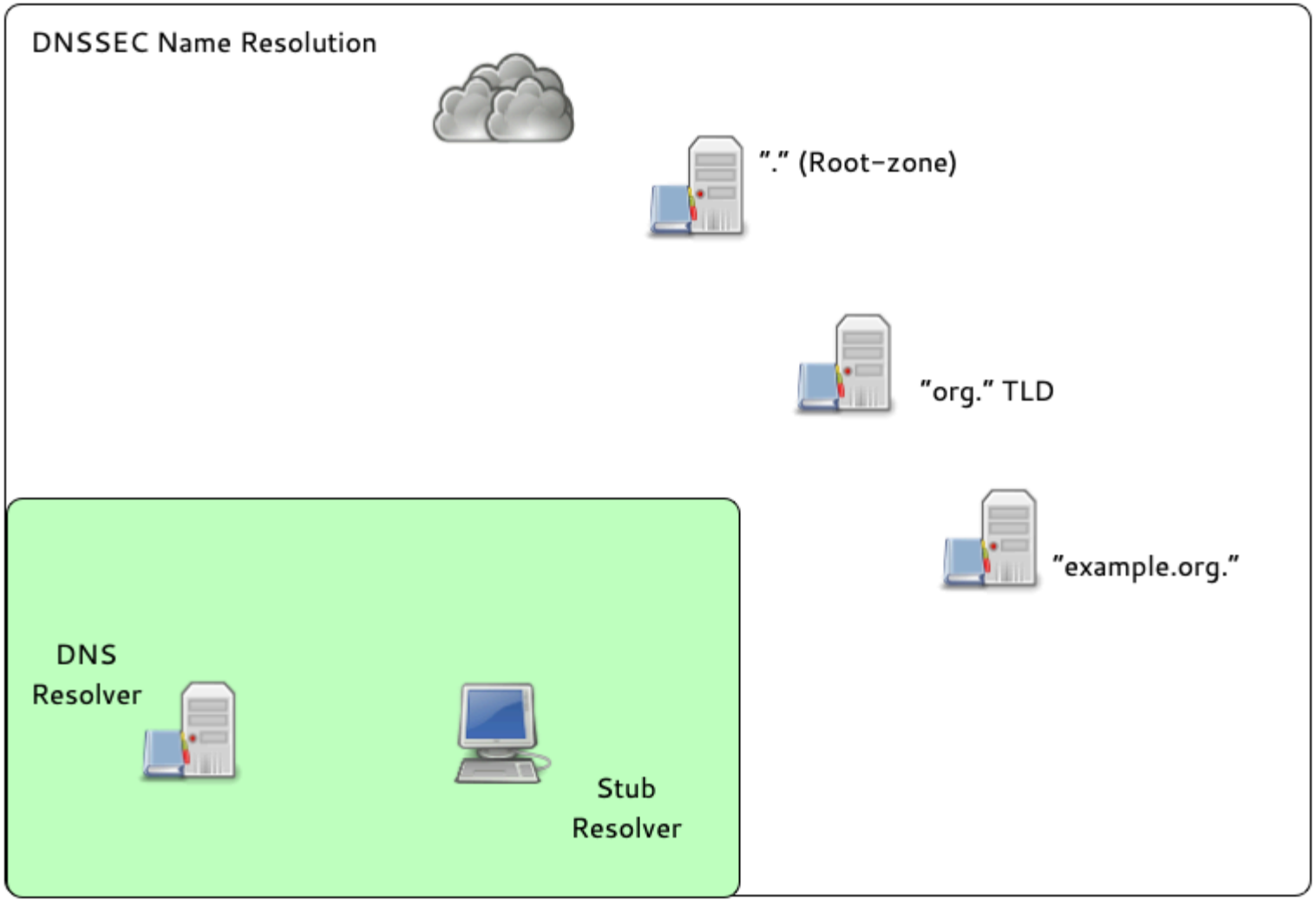
- Glue-Records helfen in diesem Fall:
  - Glue-Records sind Adressen-Records (IPv6 AAAA oder IPv4 A) für DNS-Server in einer Delegation
  - Glue-Records liegen in der delegierenden Eltern-Zone
  - Glue-Records müssen mit den Adressen-Records in der delegierten Zone synchron gehalten werden (meist manuell)

```
example.com.   3600 IN NS  dns1.example.org.
example.com.   3600 IN NS  dns2.example.info.
example.com.   3600 IN NS  dns3.example.com.
```

```
example.com.  3600 IN NS  dns1.example.org.
example.com.  3600 IN NS  dns2.example.info.
example.com.  3600 IN NS  dns3.example.com.

dns3.example.com. 3600 IN AAAA 2001:db8::53
dns3.example.com. 3600 IN A 192.0.2.53
```

DNS-NAME-RESOLUTION



DELEG

- Die IETF möchte DNS-Delegation flexibler gestalten
- Neue DELEG (und DELEGPARAM) Records

WARUM DELEG

PROBLEME MIT BISHERIGEN DNS-DELEGATION

- DNS-Delegation über NS-Records ist nicht erweiterbar
  - Keine Parameter, DNS-over-UDP Port 53 ist implizit
- NS-Records und Glue-Records sind in der delegierenden Zone nicht "authoritative", kein AA-Flag, keine DNSSEC-Signaturen (!), keine Sicherheit in der Delegation

NS-RECORD REFERRAL OHNE SIGNATUREN

```
; <<>> DiG 9.18.50 <<>> @a.nic.de blog.defaultroutes.de A +norec +dnssec +multi
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53804
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1452
;; QUESTION SECTION:
;blog.defaultroutes.de. IN A

;; AUTHORITY SECTION:
defaultroutes.de.       86400 IN NS ns3.myinfrastructure.org.
defaultroutes.de.       86400 IN NS ns5.myinfrastructure.org.
defaultroutes.de.       86400 IN DS 29257 8 2 (
                                3BA14264461D9A3A8279E903085768F1FB6478C61417
                                A996C7A4E00CB4670C12 )
defaultroutes.de.       86400 IN RRSIG DS 8 2 86400 (
                                20261005071639 20260921054639 32911 de.
                                W20P7uXY58Yc5udMq9IQ5ccJ+W8wZuLNwdUJwGEYHCT3
                                G7nWX6EHdpjOECcOaJltuRvedwNwQ4UxS3aWVP4G52bD
                                YOJdMpSfm3WLwGl7cri5qlf9jHZGK8JA26oBlCLSl1Kl
                                DYLH1rNLirJHb9MDDroMgfFl8PUh2snKLQb7vxM= )

;; Query time: 107 msec
;; SERVER: 194.0.0.53#53(a.nic.de) (UDP)
;; WHEN: Thu Sep 24 07:06:40 CEST 2026
;; MSG SIZE  rcvd: 316
```

DER DELEG DNS-RECORD

```
example.   SOA ...

test.example.   DELEG server-ipv4=192.0.2.1 server-ipv6=2001:db8::1
test.example.   DELEG server-name=ns2.example.net.,ns3.example.org.

test.example.   NS    ns1.test.example.
test.example.   NS    ns2.example.net.
test.example.   NS    ns3.example.org.
```

DER DELEG DNS-RECORD

- Der DELEG DNS-Record definiert eine DNS-Delegation aus einer delegierenden (Eltern-) Zone auf die DNS-Server für die delegierte (Kind-)Zone
  - Die Delegations-Informationen werden im DELEG-Record als Key-Value Paare spezifiziert
  - DELEG-Records sind in der delegierenden Zone "authoritative" und werden DNSSEC-signiert
  - DELEG-Records können allein oder neben NS-Records in einer Zone existieren

DE-FLAG

Nein, nicht diese "DE-Flag"

DE-FLAG

- DNS-Resolver müssen mit den "DE"-Flag (EDNS-Flag) signalisieren, das sie DELEG-Records verarbeiten können
  - ohne DE-Flag werden keine DELEG-Records in einer Delegation zurückgeliefert
  - mit DE-Flag werden keine NS-Records in einer Delegation zurückgeliefert

DELEG RDATA

- `server-ipv4` und `server-ipv6`: IP-Adressen der DNS-Server einer Zone, als Ersatz für Glue-Records

DELEG RDATA

- `server-name` ein oder mehrere DNS-Hostnamen der DNS-Server einer Zone, müssen auflösbar sein

DELEG RDATA

- `include-delegparam` indirecte Konfiguration der Delegation – sehr spannend – kommen wir gleich dazu

DELEG RDATA

- `mandatory` Liste der Schlüsselwörter, welche ein DNS-Resolver verarbeiten **muss**, um diese Delegation benutzen zu dürfen

DELEGPARAM

DELEGPARAM

- DELEG Informationen können über `include-delegparam` indirect aus einer anderen Zone geladen werden
- Somit lassen sich die Delegation-Informationen für mehrere Zonen zentral verwalten (ggf. auch von einer anderen Organisation, z.B. einem ISP)
    - Wir können die Delegation delegieren 🙂
- Die Konfigurations-Zone enthält DELEGPARAM-Records
    - DELEGPARAM-Records sind identisch zu DELEG-Records, nur erzeugen sie keine Delegation in der Zone

DELEGATION DER ZONE "TEST.EXAMPLE."

```
test.example.   3600 IN DELEG   include-delegparam=Acfg.example.org.,cname.example.org.
```

ZONE MIT DELEGATIONS-DATEN (DELEGPARAM)

```
Acfg.example.org.  3600 IN  DELEGPARAM server-ipv6=2001:db8::6666
Acfg.example.org.  3600 IN  DELEGPARAM server-name=ns3.example.org.
Acfg.example.org.  3600 IN  DELEGPARAM include-delegparam=subcfg.example.org.

; unhelpful but technically legal CNAME
cname.example.org.   3600 IN CNAME     Acfg.example.org.

ns3.example.org.     3600 IN AAAA      3fff::33

subcfg.example.org.  3600 IN DELEGPARAM server-ipv4=203.0.113.1 server-ipv6=3fff::33
```

DNSKEY-ADT FLAG

DOWNGRADE ANGRIFFE AUF DELEG

- Ein MITM-Angreifer kann aus einer signierten Eltern-Zone alle DELEG Records und die dazugehörigen RRSIG-Records (Signaturen) entfernen und stattdessen unsignierte NS-Records liefern (Legacy-Delegation)
- Ohne Hilfsmittel kann ein DNS-Resolver diesen Angriff nicht erkennen

ADT-FLAG AUF DEM DNSKEY

- Die DNSKEY-Records (öffentliche DNSSEC-Schlüssel in der Zone) bekommen ein neues Flag: ADT (Bit 14)
  - ADT = *Authoritative Delegation Types*
- Das ADT-Flag kann auf einem beliebigen DNSKEY gesetzt sein (KSK, ZSK, SSK …)
- Kommt eine Delegation nur mit NS-Record aus einer Zone mit DNSKEY-ADT Flag
  - … so muss der Resolver prüfen, das es einen NSEC(3) Record gibt, welcher für den Delegations-Namen beweist, das es keinen DELEG-Record gibt

ADT-FLAG AUF DEM DNSKEY

```
;; ANSWER SECTION:
defaultroutes.de.       3600 IN DNSKEY 385 3 8 (    ; 256 (SEP) + 128 (ADT) + 1 (KSK)
                                AwEAAcIXCMZtPnBQcIAVuu2PZk0Tr0rYtcWJtigrdyBH
                                eFDk44pXTp6Pk9Wdet9oNU7Jumr8sij3tGNS6zy3uzlE
                                DkRiha8qmF3wbXNezm9Ym8jGKST5I+yisn6eMRhrPaBE
                                Mr4Z0KqzAmLbfHorM8APgNTPPeZJt0mV5J6nzwni8h8+
                                gKf0GVzpIthr985SB9e/9Jxdl9/JWAfiX6DQhUfbE0kw
                                hYniEMlSIqahF5TYAX5jhsC3wD/kJoyoJFFRY/N4RzKT
                                Ml5tqa2V1vQX/ZAb7ZehpRU4O37hJ3fBPOwHn/LXszIx
                                jddOYx0ckRIf9a0nK8dEF0Qv5bJQMnCExG/G2gk=
                                ) ; KSK; ADT; alg = RSASHA256 ; key id = 29257
```

STATUS DER DELEG IETF-DRAFTS

- Die DELEG IETF-Drafts sind schon sehr weit fortgeschritten, es wird erwartet, dass die DELEG-Drafts noch in diesem Jahr RFC-Status erlangen
- Einige DNS-Software-Hersteller legen die Grundlagen für DELEG in den Produkten (z.B. BIND 9.21.x)

HERAUSFORDERUNGEN/AUFGABEN

- NS und DELEG Records werden für absehbare Zeit gleichzeitig benutzt werden
- Es wir DELEG-only Domains geben, welche von Legacy-DNS-Resolvern nicht gesehen werden (-> Support Anfragen)
- IPAM- und DNS-Management-Software muss DELEG-Records unterstützen (Updates)
- DNS-Monitoring muss erweitert werden

INFORMATIONEN

- IETF-Draft: Extensible Delegation for DNS https://datatracker.ietf.org/doc/html/draft-ietf-deleg
- IETF-Draft: DNS Protocol Modifications for Delegation Extensions https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-delext

VIELEN DANK!

Kontakt:

carsten@dnsworkshop.de