DNSSEC am Leibniz-Rechenzentrum

Bernhard Schmidt

schmidt@lrz.de
bschmidt@teleport-iabg.de
berni@birkenwald.de

16. Juni 2010

Eigenvorstellung

- aktiv im Serviceproviderumfeld seit Mitte 2001
- aktuell:
  - Student Informatik an der LMU München
  - Netzplanung am Leibniz-Rechenzentrum – HDiaG
  - Netzdesign und -betrieb des IABG Teleports
  - freiberuflicher Berater
  - ...

Das LRZ

- gemeinsames Rechenzentrum der Universität München, der Technischen Universität München und der BAdW
- weitere Kunden sind die Hochschule München (HM), Hochschule Weihenstephan-Triesdorf (HWST), Deutsches Herzzentrum München, Hochschule für Film- und Fernsehen und viele weitere
- 80.000 Studenten und 26.000 Mitarbeiter der Einrichtungen
- 150 Mitarbeiter
- Betrieb des Münchner Wissenschaftsnetzes
- zentrale IT-Dienste für die Universitäten, unter anderem DNS $\rightarrow$ **DNSSEC**

Warum DNSSEC?

- “Forscherdrang” – Umfeld für Forschung und Lehre
- Thema einschlägiger Vorlesungen und Praktikas
- Kaminsky-Vulnerability demonstriert
- Erfahrung sammeln

Struktur

- vier physikalische Server
- verteilt an verschiedenen Standorten im MWN
- Redundanz über Anycast
  - 2 Nodes für dns1 + resolver1
  - 2 Nodes für dns2 + resolver2
  - dns3 auf VM in Portugal
- komplett dualstacked

Rekursiver Dienst

- ISC BIND (aktuell 9.7.0-P2)
- zentrale Konfiguration über Subversion und scp/Makefiles
- alle eigenen Zonen als Slave
- 90% der Clients im MWN nutzen diese Resolver (DHCP, Forwarder)
- im Peak etwa 1300 Queries pro Sekunde

DNSSEC

resolver1:

- DLV (dlv.isc.org) seit Juni 2009
- IANA ITAR seit Oktober 2009
- DENIC DNSSEC-Testbed seit Anfang Mai 2010

DNSSEC

resolver1:

- DLV (dlv.isc.org) seit Juni 2009
- IANA ITAR seit Oktober 2009
- DENIC DNSSEC-Testbed seit Anfang Mai 2010

kein DNSSEC auf resolver2

Erfahrungen

- kein merkbarer Einfluss auf CPU-Last
- keine gravierenden Ausfälle
  - Testbed-Unerreichbarkeit am 9. Mai
  - DENIC-F*ckup am 12. Mai fast überlebt
- Flooding von Warnmeldungen – nicht kritisch

```
16-Jun-2010 00:43:46.242 DNS format error from
2a02:568:0:1::53#53 resolving www.sparkasse.de/A for
client 129.187.xxx.xxx#51861: sideways referral
```

There's more

IABG Teleport:

- Hauptgeschäft IP-over-Satellite in den Nahen Osten
- Resolver-Cluster basierend auf Unbound
- erste Tests auf Backup-Resolver
  - DLV und ITAR weitgehend problemfrei
  - gelegentlich Ärger mit 2nd Level in .gov
  - DENIC-Testbed mit Unbound 1.4.1 instabil – EDNS0-Problem
- Unbound 1.4.4 löst Problem im DENIC-Testbed
- seit Anfang Mai Rollen vertauscht, Hauptresolver fährt DLV+ITAR+DENIC

Authoritativ

- Kommerzielle, mandantenfähige Webschnittstelle von Nixu (Namesurfer)
- hält Zonendaten in eigener Datenbank und stellt sie per AXFR zur Verfügung
- starker Einsatz von DDNS-Updates $\rightarrow$ signierende Proxies unpraktikabel
- kann (einfaches) DNSSEC seit Anfang des Jahres
  - kein Key-Rollover, kein NSEC3, nur RSASHA1
- Closed Betaversion mit verbessertem DNSSEC-Support seit Anfang letzter Woche
  - auf gutem Weg (NSEC3, ZSK-Rollover, DS-Eintrag bei Delegation), aber ...

Authoritativ

- Kommerzielle, mandantenfähige Webschnittstelle von Nixu (Namesurfer)
- hält Zonendaten in eigener Datenbank und stellt sie per AXFR zur Verfügung
- starker Einsatz von DDNS-Updates $\rightarrow$ signierende Proxies unpraktikabel
- kann (einfaches) DNSSEC seit Anfang des Jahres
  - kein Key-Rollover, kein NSEC3, nur RSASHA1
- Closed Betaversion mit verbessertem DNSSEC-Support seit Anfang letzter Woche
  - auf gutem Weg (NSEC3, ZSK-Rollover, DS-Eintrag bei Delegation), aber ...
  - `dnssec IN RRSIG SOA 7 3 86400 19700101000000 20100607135827 ...`

Danke für die Aufmerksamkeit