Učiňme DNS opět velkým!

Automatická správa keysetů a jedno krásné výročí

Ondřej Filip • ondrej.filip@nic.cz • 24. 11. 2017

Bývaly časy, kdy bylo DNS jednoduché

- (tedy ...)
- Konfigurace nameserveru, zóny
- Vložení NS záznamů (popřípadě glue) do nadřazené zóny/registru
- A pak už nic nedělat, klidně celá léta
- (bohužel ...)

Ale pak se vše trochu zkomplikovalo

- Přišel DNSSEC
- Skvělá technologie – jediná globální důvěryhodná databáze
- Ale není jednoduchá
- Ne všichni registrátoři jsou vzorní (i když v .cz to jde)
- Pro laika těžké opakovaně přenášet kryptoklíče
- Co když registrátor a DNS operátor jsou různí?

Motivace

- Zjednodušit život triumvirátu
  - Držitel, registrátor a DNS operátor
- A čísla (!)
  - Gotta catch‘em all!

Co s tím?

- Zkusme to zautomatizovat
- Nedávno se objevily nástroje:
  - RFC 7344 - Automating DNSSEC Delegation Trust Maintenance - září 2014
  - RFC 8078 - Managing DS Records from the Parent via CDS/CDNSKEY – březen 2017
- A tak jsme se do toho hned pustili

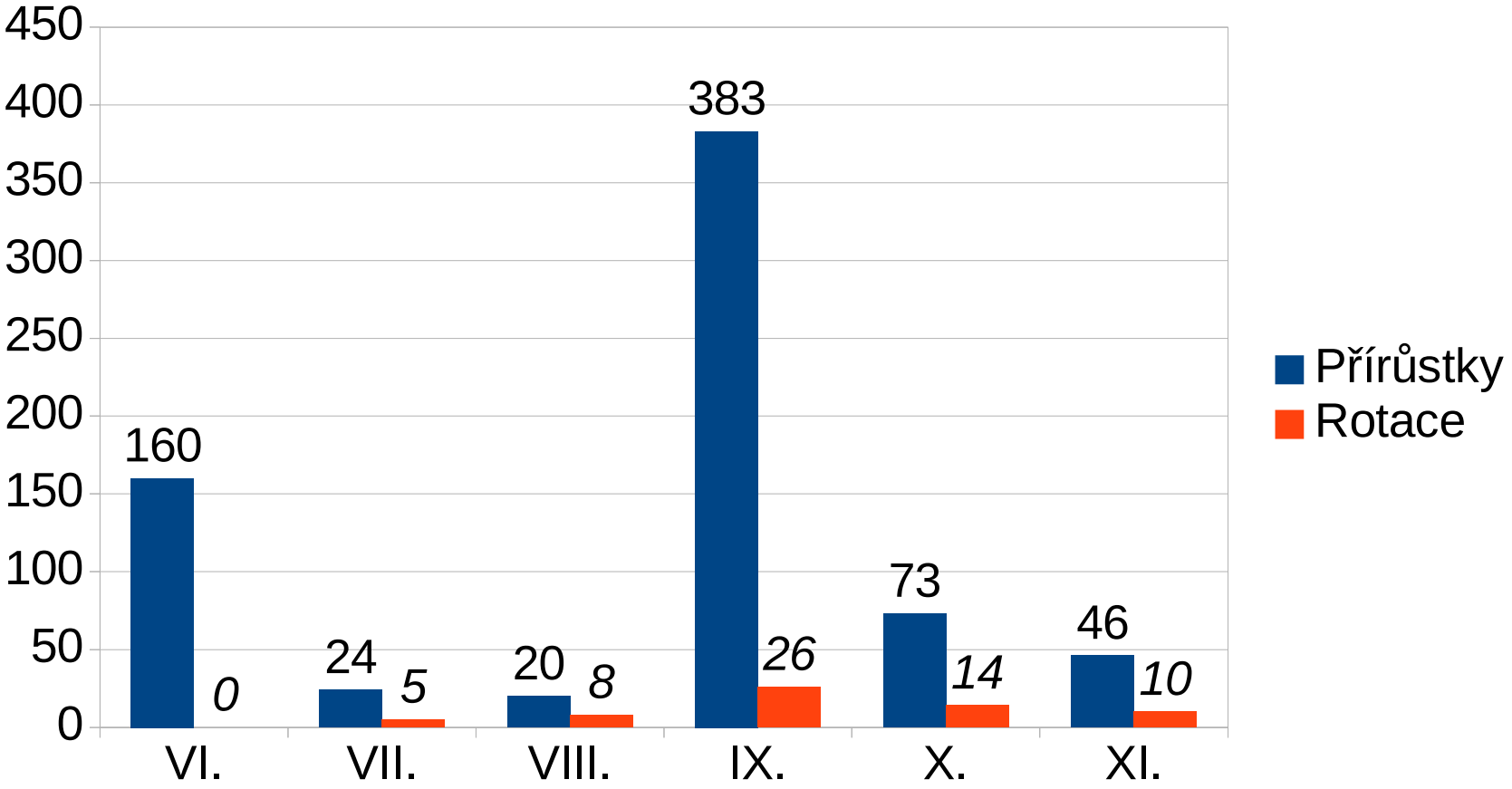
Princip

- Zvláštní signalizace v DNS zóně – **CDNSKEY**, CDS
- Provádí DNS operátor
- Zcela automatické například v Knot DNS od verze 2.5 (v současnosti 2.6.2)
- Scan zóny - TCP
- 7 dnů, notifikace
- Další změny rychle

Postupný náběh

- Těsně před IT17 – 20. 6. 2017
  - Domény bez DNSSEC (7 dní)
  - Domény s již automaticky zapnutým DNSSECem (rotace, výmaz – téměř okamžitě)
- Druhá fáze – 26. 9. 2017
  - Domény s ručně nastaveným DNSSECem (téměř okamžitě)

Měsíční operace



Co dál?

- Zatím jsme jediní na světě
- Další registry následují
  - Switch - .ch/.li
  - CIRA - .ca
- Cloudflare – diskuse - OPT-IN → OPT-OUT (~ 3000)
- Vyhodnocení provozu – PUSH pro FRED a Knot DNS
- Lokace

FRED

KNOT DNS

Oslava narozenin!

- Víte kdo má tento měsíc kulatiny?

Oslava narozenin!

- Víte kdo má tento měsíc kulatiny?
- RFC-1034 & RFC-1035 – autor Paul Mockapetris
- Dosud platná RFC (!) - nahradila starší 882 a 883
- Konec RFC-952, RFC-953
- Konec hosts.txt

RFC-1034

- Víte, kolik typů záznamů definuje toto RFC?

RFC-1034

- Víte, kolik typů záznamů definuje toto RFC?

```
www.nic.cz      IN      A       217.31.205.50
```

RFC-1034

- Víte, kolik typů záznamů definuje toto RFC?

www.nic.cz IN A 217.31.205.50

RFC-1034

- Víte, kolik typů záznamů definuje toto RFC?

```
This memo uses the following types:

A               a host address

CNAME           identifies the canonical name of an
                alias

HINFO           identifies the CPU and OS used by a host

MX              identifies a mail exchange for the
                domain.  See [RFC-974 for details.

NS
the authoritative name server for the domain

PTR
a pointer to another part of the domain name space

SOA
identifies the start of a zone of authority]
```

RFC-1035

- Víte, kolik tříd záznamů definuje toto RFC?

RFC-1035

- Víte, kolik tříd záznamů definuje toto RFC?

```
www.nic.cz      IN      A       217.31.205.50
```

RFC-1035

- Víte, kolik tříd záznamů definuje toto RFC?

www.nic.cz IN A 217.31.205.50

RFC-1035

- Víte, kolik tříd záznamů definuje toto RFC?

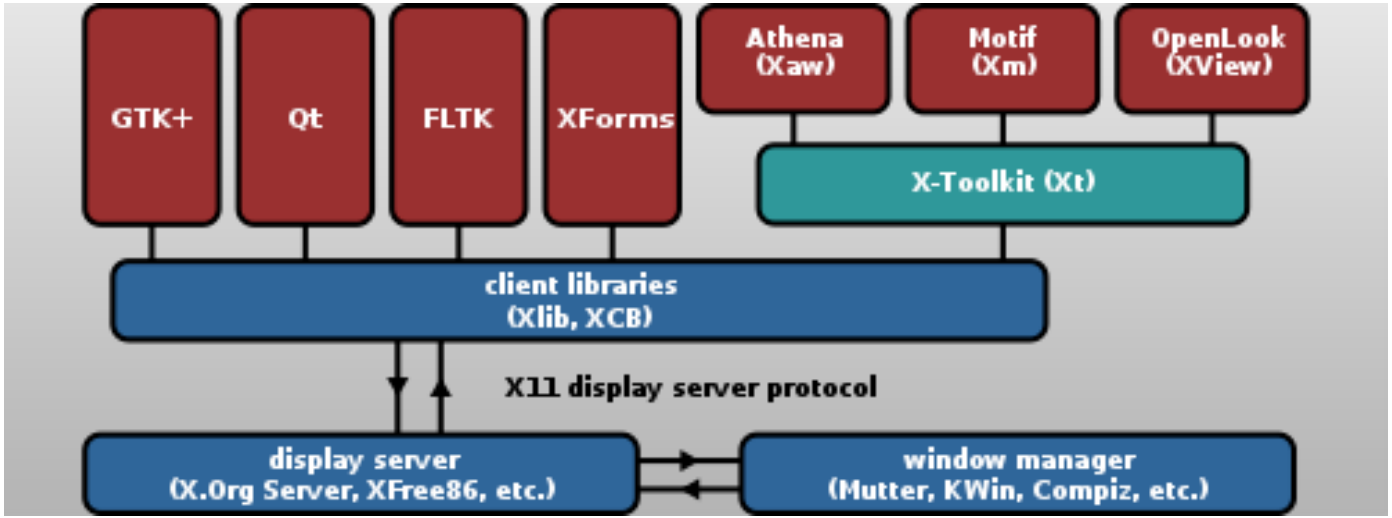
```
3.2.4. CLASS values

CLASS fields appear in resource records.  The following CLASS mnemonics
and values are defined:

IN              1 the Internet

CS              2 the CSNET class (Obsolete - used only for examples in
                some obsolete RFCs)

CH              3 the CHAOS class

HS              4 Hesiod [Dyer 87]
```

Hesiod

- Víte, kde se používá třída hesiod?

Hesiod

- Víte, kde se používá třída hesiod?
- Project Athena – MIT, DEC a IBM – distribuovaný výukový systém – vznik X-Windows, Kerberos, ...



Hesiod

- Víte, kde se používá třída hesiod?
- 1983 – 1991 – Ale údajně pořád ještě používán
- Přístup k údajům souborů jako /etc/passwd, /etc/group, /etc/printcap a pod.

```
foo.passwd.ns.example.net  HS  TXT  "foo:x:100:10:Foo Bar:/home/foo:/bin/sh"
100.passwd.ns.example.net  HS  TXT  "foo:x:100:10:Foo Bar:/home/foo:/bin/sh"
100.uid.ns.example.net     HS  TXT  "foo:x:100:10:Foo Bar:/home/foo:/bin/sh"
```


30

Děkuji za pozornost!

FRED

KNOT DNS

Ondřej Filip • ondrej.filip@nic.cz

Credits

- Photo by Johannes Wredenmark on Unsplash - https://unsplash.com/photos/qaIQk1TVon8
- Photo by David Braud on Unsplash - https://unsplash.com/photos/fp4NUhl3y-U
- Photo by Clark Tibbs on Unsplash - https://unsplash.com/photos/oqStl2L5oxI
- Photo by William Carlson on Unsplash - https://unsplash.com/photos/EKwqr0eLYpM
- Photo by Taylor Nicole on Unsplash - https://unsplash.com/photos/cvWCOvtTn40
- Photo by Annie Spratt on Unsplash - https://unsplash.com/photos/M20ylqCzSZw