

Správa DNS zónových souborů v Gitu

Ondřej Caletka



7. října 2018



Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O sdružení CESNET



	n×100 Gb/s		100 Gb/s
	n×10 Gb/s		10 Gb/s
	uzel (PoP)		1-2,5 Gb/s
	uživatel (user)		<1 Gb/s



MetaCentrum



UltraGrid

Hledáme kolegy

- správce a vývojář internetových služeb
- správce a vývojář multimediálních služeb
- analytik digitální forenzní laboratoře

Pořádáme akce

- The Catch – online; tričko na stánku za vyřešené úlohy
- Security Fest – pro vaše rodinné příslušníky – 24. října 2018
- Seminář o bezpečnosti – únor 2019
- IPv6 Day – 6. června 2019

- 1 Proč ISP stále spravují zónové soubory ručně
- 2 Správa DNS v CESNETu
- 3 Správa zónových souborů v Gitu
- 4 DNSSEC podepisování
- 5 Další práce

Proč ISP stále spravují zónové soubory ručně

Jak se spravují DNS záznamy

v hostingu

- hlavní předmět práce
- obvykle vlastní řešení integrované se zbytkem hostingu

v organizaci

- dopředné a reverzní názvy stanic
- integrace s adresářovým/DHCP serverem
- výstup z IPAM software

u ISP

- reverzní záznamy klientů
- vlastní služby

Post-IPokalypsa v reverzním DNS

- reverzní IPv4 DNS navrženo pro třídy A (2^{24} adres), B (2^{16} adres), C (2^8 adres)
- dnešní přiděly jsou spíše v hodnotách 2, 4, 8, 16 adres
- rozdělení malých bloků do subdomén *hackem* BCP 20 / RFC 2317
- důsledkem je mnoho vzájemně odkazovaných zón

Classless subdelegace

```
128/25  IN NS  server.example.com.  
        IN NS  secondary.example.com.  
128     IN CNAME 128.128/25  
129     IN CNAME 129.128/25  
...  
255     IN CNAME 255.128/25
```

- mnoho reverzních zón
- subdelegace na vlastní i cizí servery, i opakovaně
- míchání delegací a přímo spravovaných záznamů
 - většina klientů řeší reverzní DNS jen pro poštovní servery
- nekonzistence hostingu dopředných a reverzních záznamů
 - dopředné záznamy obvykle hostovány u registrátora
- exotické typy záznamů (NAPTR, CAA, TLSA, SSHFP)
- neveřejná metadata v komentářích (např. číslo tiketu)

Správa DNS v CESNETu

Evoluce správy DNS v CESNETu

- přímá editace zónového souboru na veřejném serveru
 - nezvýšené sériové číslo znamená nekonzistenci
 - syntaktická chyba znamená výpadek služby
- přechod na skrytý master server, veřejné slave servery
 - ruční editace na skrytém serveru
 - chyba nezpůsobí výpadek služby
 - DNSSEC podpisy nástrojem OpenDNSSEC
 - lokální Git repozitář pro ukládání změn
- zónové soubory řízené Git repozitářem
 - ochrana před chybami na úrovni Git repozitáře
 - automatické provedení změn po synchronizaci repozitáře
 - DNSSEC podpisy v nezávislé komponentě

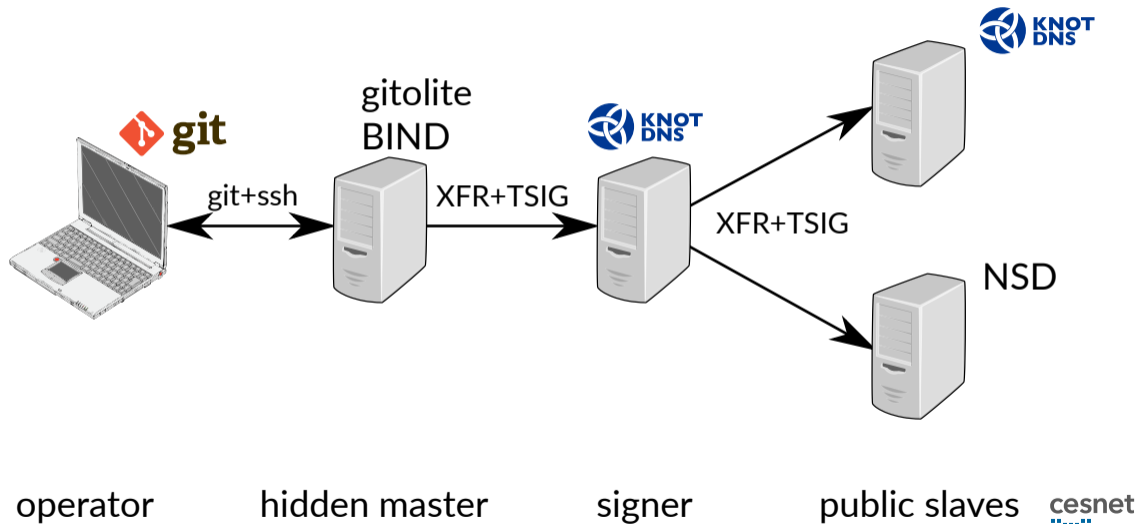
- mnoho kroků, náchylnost na chyby
 - provést změnu
 - zvýšit sériové číslo
 - přepodepsat zónu, je-li podepsaná
 - reloadovat DNS server
 - commitnout do Git repozitáře
- nepříjemné problémy s OpenDNSSEC
 - občasné deadlocky SQLite databáze – doporučované řešení: použijte MySQL
 - bolestivý upgrade z verze 1.3 na 1.4, netriviální upgrade na 2.0
 - nekonzistence dat v KASP databázi při sdílení klíčů mezi zónami
 - nepodpora pro změnu algoritmu (do verze 2.0)
 - nepodpora pro automatické změny bezpečné delegace

Nejčastější chyby při správě zónových souborů

- syntaktická chyba
 - překlep
 - nepodporovaný typ záznamu (typicky CAA)
- nezvýšené sériové číslo
 - zóna se nepřenesla na slave servery
- zapomenutá koncová tečka (zejména u PTR záznamů)
 - 1.2.0.192.in-addr.arpa. PTR www.example.com.2.0.192.in-addr.arpa.
 - z pohledu DNS nejde o chybu

Správa zónových souborů v Gitu

Cílový stav



Správa zónových souborů v Gitu

- možnost rozšíření funkcionality Gitu pomocí *hooks*
- inspirováno v RIPE NCC (shell skripty)
- *hooks* jsou vždy lokální, jejich spuštění nelze vynutit
- `https://pre-commit.com` pro programátory
- existující projekt GitZone pro správu DNS zón Gitem
 - implementováno v Perlu
 - kombinuje kontroly DNS zón a správu Git repozitáře
 - objevil jsem ho příliš pozdě; NIH syndrom 😊

A kdyby to nepomohlo, v souboru git.txt naleznete telefonní číslo na mého kamaráda, který git pochopil. Stačí, když přetrpíte pár minut vysvětlování typu 'vlastně je to hrozně jednoduché, představte si, že ty větve jsou vlastně...' a nakonec se od něj dozvíte příkazy, pomocí kterých dáte všechno do pořádku.



Zdroj: xkcd 1597, CC-BY-NC, překlad XKCZ.cz

Nástroj `/usr/sbin/named - compilezone`

- součást DNS serveru BIND
- když soubor načte, bude načten i nameserverem
- vypíše soubor v kanonickém tvaru
- na chybový výstup vypíše sériové číslo a případné chyby

- 1 zkompilujeme zónu v `pre-commit` hooku
- 2 pokud kompilace neprojde, `commit` odmítneme
- 3 jinak zkompilujeme i minulou verzi a porovnáme
- 4 odmítneme `commit`, když se kompilované zóny liší a nezvyšuje se sériové číslo
 - změny v komentářích a/nebo v pořadí záznamů jsou povoleny

Zjištění jména zóny

- nástroj `named - compilezone` vyžaduje jméno zóny
- jméno souboru jako jméno zóny selhává u zón podle BCP 20
 - v názvu zóny je lomítko – nelze použít pro název souboru
 - BCP 20 na lomítko netrvá, naopak doporučuje konzervativnější znak
 - my už máme zavedeno lomítko, nelze to snadno změnit
- autoritativní název může být uložen v direktivě `$ORIGIN` na začátku souboru

BCP 20

The examples here use “/” because it was felt to be more visible and pedantic reviewers felt that the ‘these are not hostnames’ argument needed to be repeated. We advise you not to be so pedantic, and to not precisely copy the above examples, e.g. substitute a more conservative character, such as hyphen, for “/”.

Rekapitulace požadavků

- 1 vyzvednout verzi připravenou ke commitu:
`git show <revision>:<path>`
- 2 detekovat jméno zóny z direktivy \$ORIGIN nebo jména souboru
- 3 zkompilovat zónu, zaznamenat sériové číslo, zahashovat zkompilovanou zónu
- 4 opakovat totéž pro verzi v aktuální HEAD revizi
- 5 porovnat hashe a sériová čísla

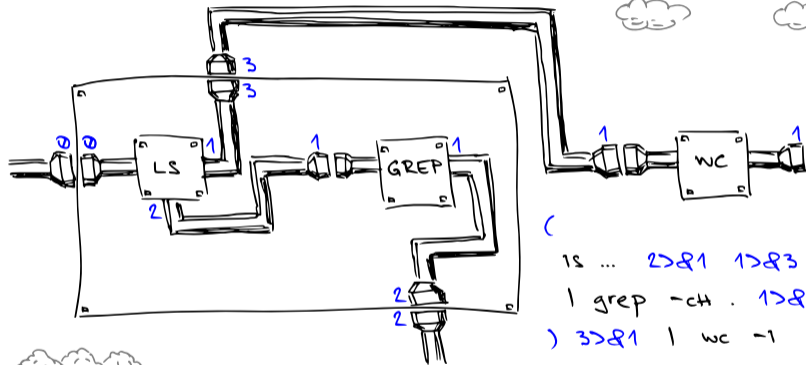
Nekontrolujte podle pracovní kopie

Verze připravená ke commitu **vznikne při volání `git add`**. V době volání `git commit` už může pracovní kopie obsahovat jiná data.

LUKÁŠ BAŘINKA
00023

LINUXDAYS 2017
REDIRECTION 6-9

TIME
23:00



Google shell style guide

If you are writing a script that is more than 100 lines long, you should probably be writing it in Python instead. Bear in mind that scripts grow. Rewrite your script in another language early to avoid a time-consuming rewrite at a later date.

Vlastní nástroj dzonegit

- Python 3.5+, 520 sloc + 365 sloc testů
- bez Python závislostí, možno spustit jako jeden skript
- MIT licence, univerzální

Použití pro uživatele

Jednoduchá instalace

```
$ wget -O .git/hooks/pre-commit https://.../dzonegit.py
$ chmod +x .git/hooks/pre-commit
```

Plná instalace

```
$ python3 -m venv .venv
$ source .venv/bin/activate
(.venv)$ pip install dzonegit
(.venv)$ deactivate
$ ln -s ../../.venv/bin/dzonegit-pre-commit \
    .git/hooks/pre-commit
```

Je třeba mít Python 3.5+, Git a `named - compilezone`.

Nastavení na straně serveru

- Implementováno jako *bare* repozitář s externí pracovní kopí
 - `git push` do běžného repozitáře není doporučovaný
 - v pracovní kopii nechceme mít adresář `.git`¹
- nechci znovu vymýšlet řešení pro sdílený repozitář
- Gitolite funguje spolehlivě a podporuje vlastní *hooks*
 - `dzonegit-pre-receive` odmítne commity, které neprojdou kontrolou
 - `dzonegit-post-receive` aktualizuje externí pracovní kopii, vygeneruje snippety konfiguračních souborů a reloaduje DNS server
 - `dzonegit-smudge-serial` během vytváření pracovní kopie nahradí nestandardní direktivu `$UNIXTIME` za aktuální hodnotu unixového času

¹v tomto případě to ničemu nevadí, ale třeba na webu to [může být problém](#).

Příklad nastavení Gitolite

repo dns-masters

```
RW+      = @masters
option hook.pre-receive = dzonegit-pre-receive
option hook.post-receive = dzonegit-post-receive
config dzonegit.checkoutpath = /var/lib/dzonegit/dns-masters/
config dzonegit.confiremplate = /etc/dzonegit/template-bind.json
config dzonegit.confirfilepath = /var/lib/dzonegit/masters-bind.conf
config dzonegit.reconfigcmd = "/usr/sbin/rndc reconfig"
config dzonegit.zonereloadcmd = "/usr/sbin/rndc reload"
```

Příklad šablony pro snippety konfigurace

```
{
  "header": "# Autogenerated by dzonegit on $datetime. Do not edit.\n",
  "item": "zone \"$zonename\" { type master; file \"$zonefile\"; };"
}
```

Podpora pro \$UNIXTIME

- odstranění nutnosti manuálně zvyšovat sériové číslo při každé změně
- využívá mechanismus Git clean/smudge filters
 - `smudge` filtrování souborů při vytváření pracovní kopie
 - `clean` čištění pracovní kopie před commitem
- stačí nastavit `smudge` filtr na straně serveru

Nastavení `smudge` filtru

```
$ cat repositories/dns-masters.git/info/attributes
*.zone filter=dzonegit
$ git config --global -l
filter.dzonegit.smudge=/usr/local/bin/dzonegit-smudge-serial
```


- jde pouze o Git *hooks*, spouští je Git během operací nad repozitářem
- nepřijme zónové soubory, které by DNS server nenačetl
- po každé změně vystaví aktuální verzi repozitáře a sestaví snippety konfigurace
- pro každou změněnou zónu zavolá definovaný příkaz (*reload* konkrétní zóny)
- při přidání nebo zrušení zóny zavolá definovaný příkaz (*reconfig* serveru)
- podpora více repozitářů – *blacklisty* a *whitelisty* jmen zón
 - zabrání duplicitní definici zóny v konfiguraci DNS serveru

DNSSEC podepisování

Základní předpoklady

- vstup a výstup podepisovače by měl být zónový přenos, ne zónový soubor
- klíče v HSM nejsou potřeba (SSH a TLS klíče taky v HSM nemáme)
- stejně jako klíče je třeba **chránit primární data**
- sdílení klíčů mezi zónami je lepší nepoužívat
 - nejde o standardně používanou a dobře testovanou funkci
 - při nepoužití HSM není počet klíčů problém
 - nesdílení klíčů nepřináší velké provozní problémy

Zónový přenos vs. zónový soubor

- zónový přenos používá binární formát zpráv
- jakýkoli typ záznamu je možné převést do textového formátu (RFC 3597)
- obsahuje-li zónový soubor neznámý typ záznamu, nelze ho načíst

Vytvoření bezpečné delegace

- do nadřazené zóny se vloží DS záznam: otisk veřejného klíče a jména zóny
- registry .cz a .eu přijímají veřejné klíče a vytváří DS záznamy samy - umožňují sdílení klíčů
- ostatní registry přijímají přímo DS záznamy, sdílení klíčů nedává smysl

Automatická správa bezpečné delegace

- v zóně se vystaví záznamy CDS a/nebo CDNSKEY
- registr si záznamů všimne a automaticky nastaví bezpečnou delegaci
- podporováno registry .cz a .ch, další přibývají

- BIND
 - automaticky spravuje jen podpisy, ne klíče
- OpenDNSSEC
 - vyžaduje databázi, (soft-)HSM
 - neumí zatím automatickou správu delegace
- Knot DNS
 - spravuje klíče automaticky, stačí přidat zónu do konfigurace
 - vystavuje automaticky CDS/CDNSKEY záznamy
 - automaticky detekuje, že nadřazená zóna provedla změnu delegace
 - klíče jsou uloženy v souborech, KASP data v LMDB databázi
 - vývojáři reagují rychle, ochotně opravují chyby a přidávají nové funkce

Konfigurace Knot DNS jako on-slave podepisovače

template:

```
- id: default
  storage: "/var/lib/knot"
  zonefile-load: none
  zonefile-sync: -1
  journal-content: all
  master: master
  acl: acl_master # NOTIFY from master
  acl: acl_slave # AXFR from slave
  notify: slave
  dnssec-signing: on
  dnssec-policy: ecdsa_cz
```

policy:

```
- id: ecdsa_cz
  algorithm: ecdsap256sha256
  zsk-lifetime: 30d
  ksk-lifetime: 90d
  rrsig-lifetime: 30d
  rrsig-refresh: 15d
  nsec3: on
  ksk-submission: resolvers
```

submission:

```
- id: resolvers
  parent: ns.cesnet.cz
  parent: google_dns
  parent: cloudflare_dns
  check-interval: 61m
```

Připojení podepisovače

repo dns-masters

```
...
config dzonegit.conftemplate2 = /etc/dzonegit/knot.json
config dzonegit.conffilepath2 = /var/lib/dzonegit/masters-knot.conf
config dzonegit.reconfigcmd2 = "/usr/sbin/knotc reload"
```

Šablona konfigurace

```
{
  "header": "# Autogenerated by dzonegit on $datetime.\n\nzone:\n",
  "item": " - domain: \"$zonename\"\n  $zonevar\n",
  "zonevars": {
    "ces.net": "template: signed\n  dnssec-policy: rsa",
    "rpz.cesnet.cz": "template: unsigned",
    "*.cz": "template: signed\n  dnssec-policy: ecdsa_cz",
    "*.ip6.arpa": "template: signed\n  dnssec-policy: ecdsa"
  }
}
```

Vygenerovaný snippet

```
# Autogenerated by dzonegit on Fri Oct 5 14:43:58 2018. Do not edit.
zone:
- domain: "8.b.d.0.1.0.0.2.ip6.arpa"
  template: signed
  dnssec-policy: ecdsa
- domain: "rpz.cesnet.cz"
  template: unsigned
- domain: "ces.net"
  template: signed
  dnssec-policy: rsa
```

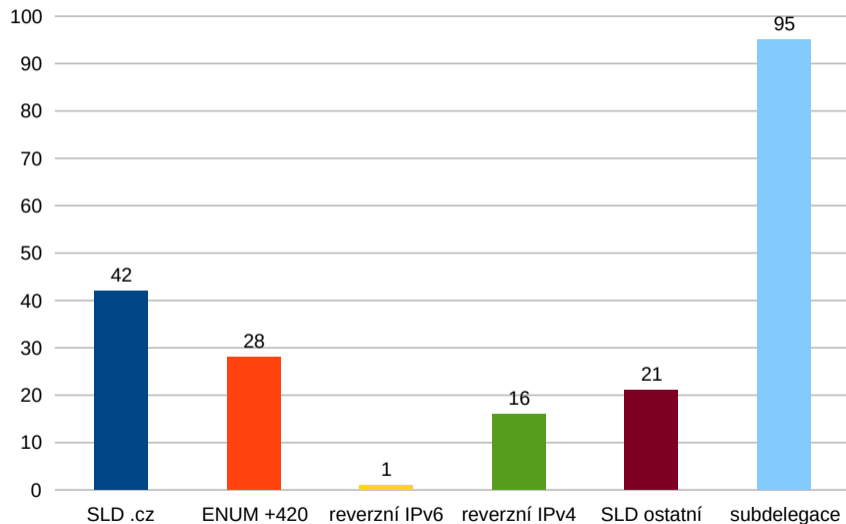
Oznámení o úspěšném nalezení záznamu CDNSKEY u domény ...	•	podpora@nic.cz	🕒	4.9.2018 13:07
Oznámení o úspěšném nalezení záznamu CDNSKEY u domény ...	•	podpora@nic.cz	🕒	4.9.2018 13:08
Oznámení o úspěšném nalezení záznamu CDNSKEY u domény s...	•	podpora@nic.cz	🕒	4.9.2018 13:09
Oznámení o úspěšném nalezení záznamu CDNSKEY u domény s...	•	podpora@nic.cz	🕒	4.9.2018 13:09

Další práce

Automatická údržba bezpečné delegace

- funguje skvěle pro domény .cz (20 procent zón)
- pro ostatní lze implementovat na naší straně
 - reverzní záznamy v RIPE DB (REST API)
 - ostatní TLD přes API registrátora (*kterého?*)
- co se **subdoménami, které jsou delegované od nás?**
 - primárně směrem na zóny, delegované znovu na naše servery
 - v roce 2018 přišel první požadavek na bezpečnou delegaci reverzních záznamů
 - automatická správa vyžaduje automatickou editaci zónového souboru
 - utilita dnssec - cds (součást BIND) pro automatickou správu DSsetů

Struktura hostovaných zón



- zatím nepoužíváme, netrápí nás
- může být řešením bezpečných subdelegací
- vyžaduje větší refactoring kódu
 - *checkout* repozitáře do dočasného adresáře
 - detekce, která zóna se změnila při změně vkládaného souboru

- nasazeno v září 2018
- detaily integrace s Gitolite na Wiki
- lze integrovat přímo s Knot DNS
 - sériové číslo zóny je třeba zvýšit nad sériové číslo aktuálně vystavené zóny
 - možnost ignorovat sériové číslo zóny od Knot DNS 2.7.0
- patche jsou vítány

<https://github.com/oskar456/dzonegit>

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)

