Automatické skenování CDNSKEY z více lokalit

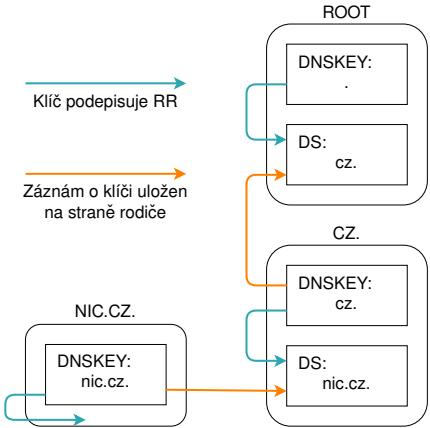
Marina Shchavleva • marina.shchavleva@nic.cz • 11. listopad 2020

Úvod

1. DNSSEC a CZ.
2. Princip automatizace DNSSEC
3. Řešení CZ.NIC – FRED-AKM
   - Použití
   - Vliv na CZ.
   - Architektura
   - Zkušenosti z provozu
4. Nové řešení – cdnskey-processor
   - Architektura
   - Podrobnosti použití

Diplomka viz `http://hdl.handle.net/10467/87860`

DNSSEC

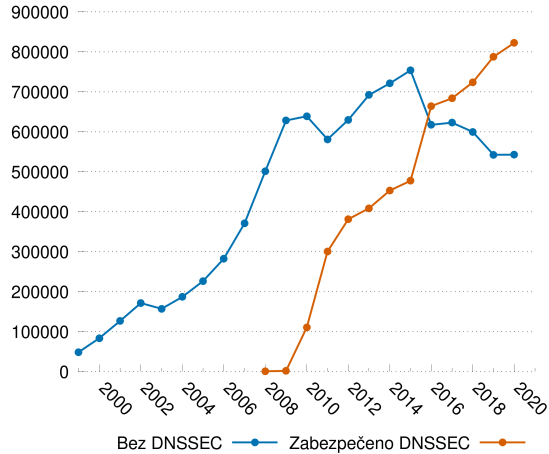


Nové RR

- `DNSKEY` – veřejný klíč (child zone)
- `DS` – hash veřejného klíče (parent zone)
- `RRsig` – digitální podpis

DNSSEC v CZ.

- podporujeme DNSSEC od roku 2008
- vede mezi ccTLD a starými TLD (statistiky viz `http://rick.eng.br/dnssecstat/`)
- 60.25% zabezpečených domén



Automatická aktualizace klíčů na straně rodiče

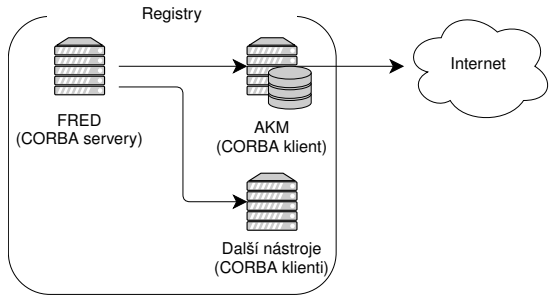
Nové RR

- `CDNSKEY` Child `DNSKEY`
- `CDS` Child `DS`

Strategie přidání klíčů pro nezabezpečené domény

- Přes ověřený kanál (přip. s dodatečnou kontrolou)
- Zabezpečení při vytvoření
- **Se zpožděním:** FRED-AKM.
- S výzvou

FRED-AKM: Automated Keyset Management



1. AKM dostane z databáze registru seznam domén ke skenování
2. Naskenuje `CDNSKEY` záznamy pro domény z jejich nameserverů a uloží je
3. Vyhodnotí a uloží nové klíče do databáze registru

Vyhodnocení výsledků

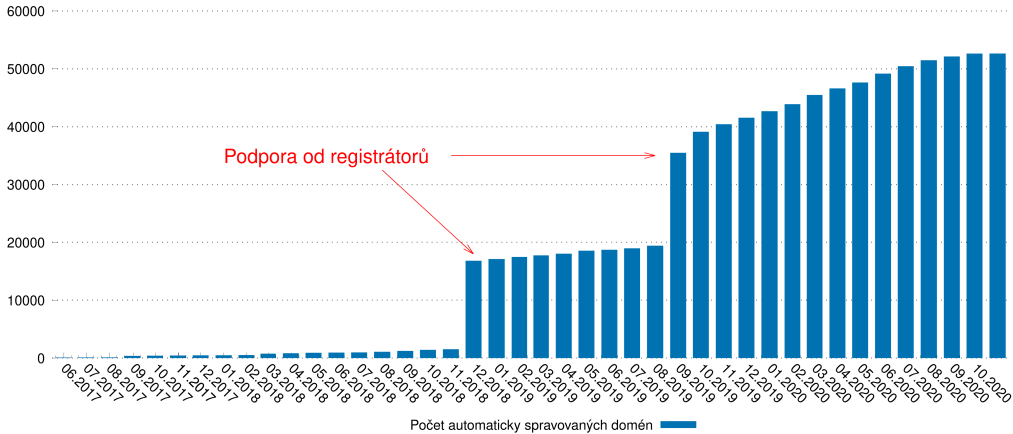
Typy výsledků:

1. doména má `CDNSKEY`
2. doména nemá `CDNSKEY`
3. o doméně nic nevíme

Proces vyhodnocení:

1. doména má nutný počet výsledků
2. všechny výsledky jsou typu 1
3. všechny výsledky musí být konzistentní – přes nameservery, IP nameserverů, v čase
4. kontrola vzájemné aktuality výsledků

Vliv FRED-AKM na CZ.

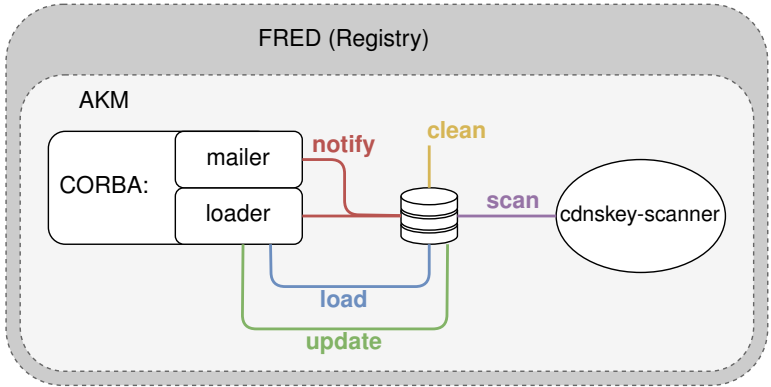


FRED-AKM workflow

Registr po sobě spouští příkazy CLI-nástroje `fred-akm`:

1. `load` – načtení domén do vnitřní databáze
2. `scan` – skenování nameserverů daných domén, ukládání výsledků
3. `notify` – oznámení technických kontaktu o průběhu skénu
4. `update` – validní klíče se přidávají zpět do databáze registru
5. `clean` – vyčištění databáze od starých výsledků

FRED-AKM architektura



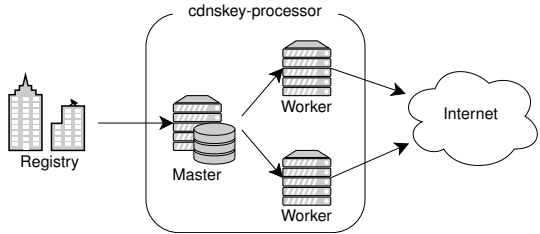
Zkušenosti z provozu

- SQLite
  - Replikace – jenom 3rd party nástroje
  - Chybí smysluplný datový typ `timestamp`
  - Referenční integrita
- Možnost navazování skénu při spadnutí
- Skenování z jedné lokace
- Těsné propojení s FREDem

Nové řešení – cdnskey-processor

- Přesun z CLI-nástroje na klient-server (registr je klient)
- Omezení pouze na skenování a analýzu (oznámení řeší registr)
- Možnost více skenovacích lokaci najednou
- PostgreSQL místo SQLite

Architektura cdnskey-processor



1. Registr pošle seznam domén k skenování
2. Master distribuuje požadavek Workerům
3. Workery nezávisle dotazují nameservery příslušných domén
4. Master shromažďuje výsledky od Workerů
5. Registr dotazuje Mastera na výsledky

Master

Interface pro Registr: odstiňuje od Workerů.

Role:

- Import domén určených pro skén
- Koordinace Workerů při skénu
- Kolekce výsledku skénu a vyhodnocení
- Export výsledku
- Diagnostický interface

Worker

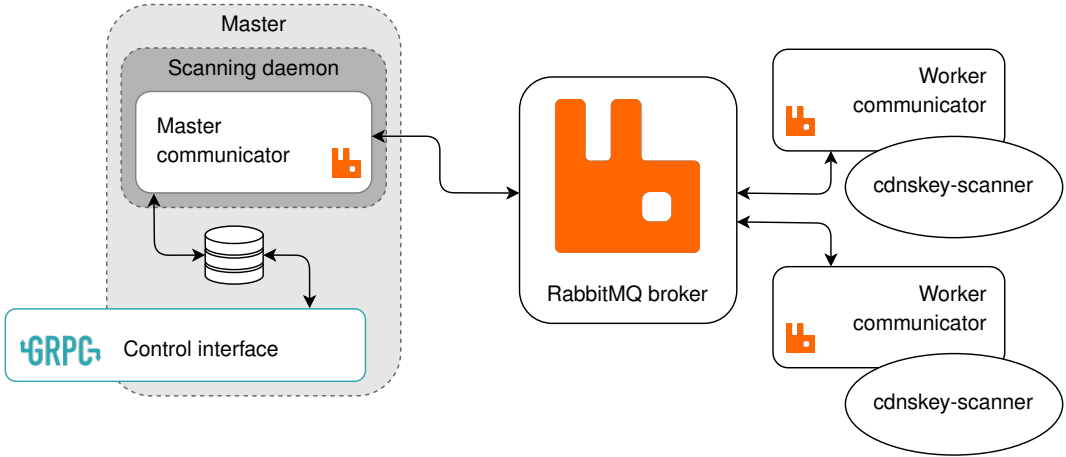
Role:

- Skén nameserverů podle zadání od Mastera
- Detekce neúspěšných výsledku
- Případné opakování skénu pro neúspěšný výsledek

Neúspěšné výsledky skenování:

- unresolved nameserver IP
- nepodařilo se získat informace o doméně

Celková struktura aplikace



Zotavení po spadnutí

Rozdělení na menší úkoly (batche)

- Pro obsažené domény má všechny potřebné nameservery
- Jednodušší kontrola dokončení
- Při spadnutí možnost naskenovat to, co není dokončené
- Vyhodnocení výsledků i pro nedokončenou frontu úkolů

Budoucnost projektu

- Finální fáze vývoje
- Nahradí původní AKM
- Potenciální vylepšení
  - Load-balancing pro zabezpečené domény
  - Quorum
  - Náhled do stavu skénu pro konkrétní doménu (např. přes webové rozhraní)

Děkuji za pozornost

Marina Shchavleva • marina.shchavleva@nic.cz