Michal Hrušecký
Michal@Hrusecky.net

Správa DNS pomocí SaltStacku

Co je to DNS

...

Co je to SaltStack

- data-driven orchestration
- remote execution
- configuration management

Zdroj absolutní pravdy

Co dát do DNS

- povinný balast SOA, NS, MX
- A, AAAA, CNAME
  - asi nejdůležitější
- další možnosti
  - SSHFP
  - SRV
  - CAA
  - TLSA

DNS Software

Bind

- nejrozšířenější, nejznámější, …

PowerDNS

- umí SQL backendy
- má API

Knot

- cool kid
- má API
- textové konfigurační soubory

Jak používám Knot

```
    serial-policy: "unixtime"
    zonefile-sync: -1
    zonefile-load: "difference-no-serial"
```

- při reloadu se použije unixtime jako serial
- stačí měnit konfigurační soubor
  - nemusim řešit SAO a inkrementaci serial

Spolupráce Saltu a Knota

- Salt by měl znát vše
  - jaké nastavuje IP
  - jaké nastavuje webservery
  - kde běží jaké služby
  - jaké kde nasazuje certifikáty

- Salt vygeneruje konfigurák a při změně otočí knota
  - makra pro e-maily, NS, …

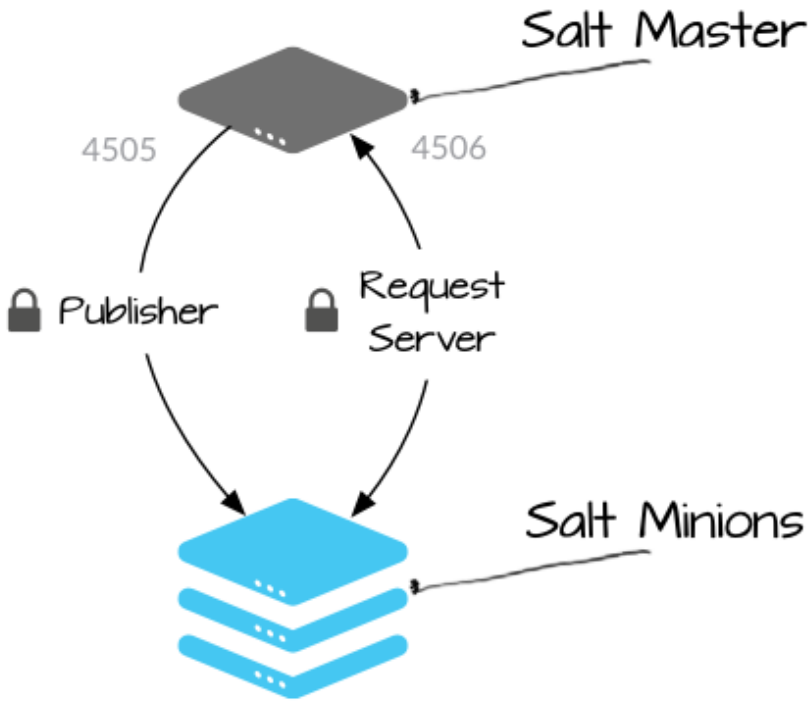
- Problem solved!

Opravdu je vše vyřešeno?

- svět není ideální
  - lidi sahaj na stroje ručně
  - existují legacy weby které nejsou v Saltu
  - ne všechno je server

- zařízením se mění IP
- stroje občas mění svoje ssh klíče
- Letsencrypt

Jak Salt funguje



Jak se Minioni nastavují

- stavy
  - jednoduchá jednoúčelová nastavení
- formule
  - highlevel abstrakce nad stavy
- pilíře
  - konfigurační data pro formule

Minionovi se posílají jen jeho data

Jak posbírat data od Minionů?

Pomocí solného dolu

Salt mine:

- master sbírá data od minionů
- nastavitelné co se má sbírat
- cache nasbíraných dat

Použití Salt Mine

```
main_ip4:
  - mine_function: network.ip_addrs
  - eth0
  - type: 'public'
main_ip6:
  - mine_function: network.ip_addrs6
  - eth0
  - type: 'public'
```

Použití Salt Mine

```
  sshfp:
    - mine_function: cmd.run
    - 'sh -c "ssh-keygen -r localhost | sed \"s|.*IN
SSHFP ||\""'
  webs:
    - mine_function: cmd.run
    - 'sh -c "sed -n \"s|.*server_name\\ \\(.*\\);|
\\1|p\" /etc/nginx/vhosts.d/*.conf"'
```

Použití dat v pilíři

```
{% macro inframail() -%}
    - name: '@'
      type: TXT
      content: '"v=spf1 mx -all"'
    - name: '_dmarc'
      type: TXT
      content: '"v=DMARC1; p=reject; sp=reject; ..."'
    - name: '_adsp._domainkey'
      type: TXT
      content: '"dkim=all"'
    - name: 'my._domainkey'
      type: TXT
      content: '"v=DKIM1; s=email; k=rsa; p=..."'
    - name: '@'
      type: MX
      content: '10 smtp.example.com.'
{%- endmacro %}
```

Použití nasbíraných dat v pilíři

```
{%- for fun_tpe, tpe in (('main_ip4', 'A'),
                         ('main_ip6', 'AAAA')) %}
{%-   for srv, addrs in
salt.saltutil.runner('mine.get',
      tgt='*', fun=fun_tpe, tgt_type='glob').items() %}
       - name: '{{ srv.split('.', 1)[0] }}'
         content: {{ addrs[0]|yaml_dquote }}
         type: {{ tpe|yaml_dquote }}
{%-   endfor %}
{%- endfor %}
```

Použití nasbíraných dat v pilíři

```
{%- for srv, keys in salt.saltutil.runner('mine.get',
    tgt='*', fun='sshfp', tgt_type='glob').items() %}
{%-   for sshfp in keys.split('\n') %}
      - name: {{ srv.split('.', 1)[0] }}
        content: {{ sshfp|yaml_dquote }}
        type: SSHFP
{%-   endfor %}
{%- endfor %}
```

Co dál?

- TLSA pro Letsencrypt za domácí úkol
  - potřeba rotace klíčů
  - závisí od ypůsobu nasazení

- Zapojit Salt Reactor
  - reakce na připojení klienta
  - reakce na změnu dat v dole

Děkuji za pozornost

Otázky?