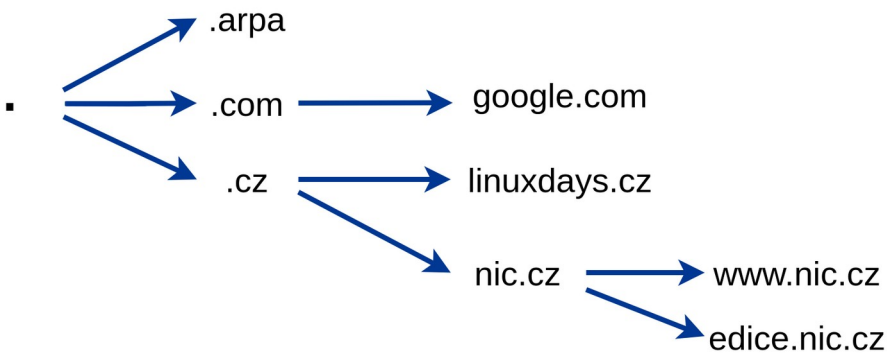
Katalogová zóna v DNS

Lukáš Vacek • 12. 10. 2024

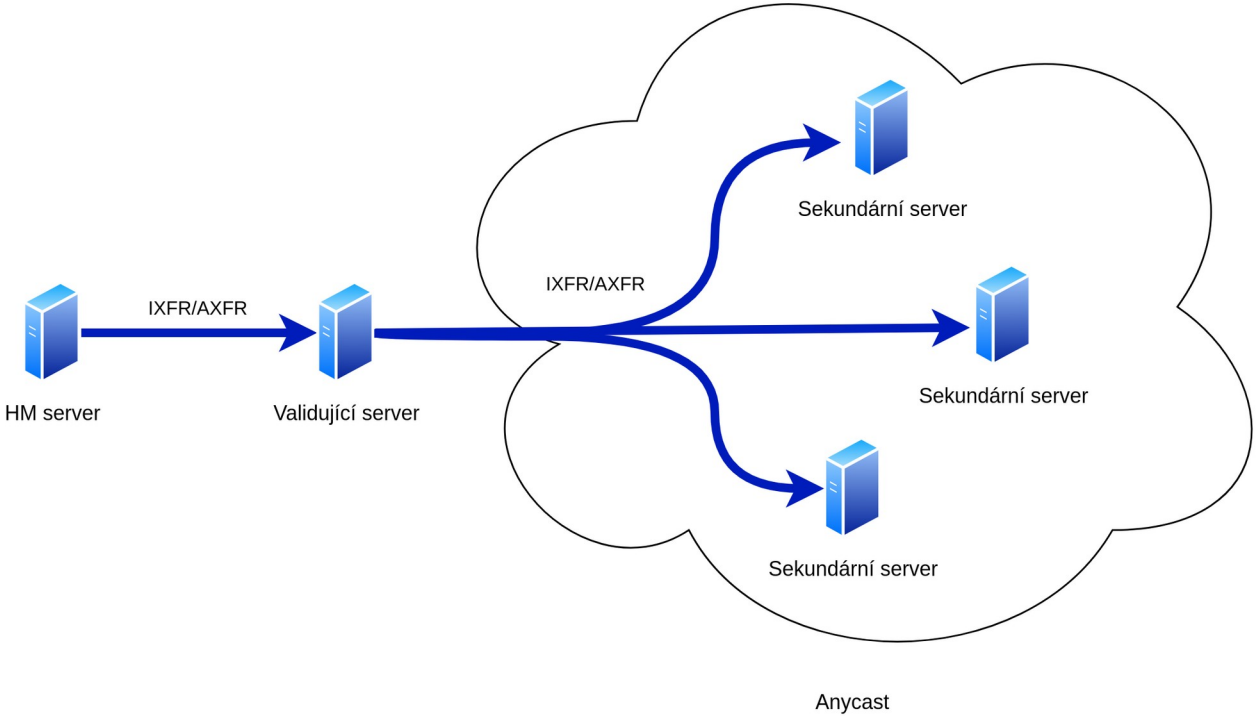
CZ.NIC | SPRÁVCE DOMÉNY CZ

DNS

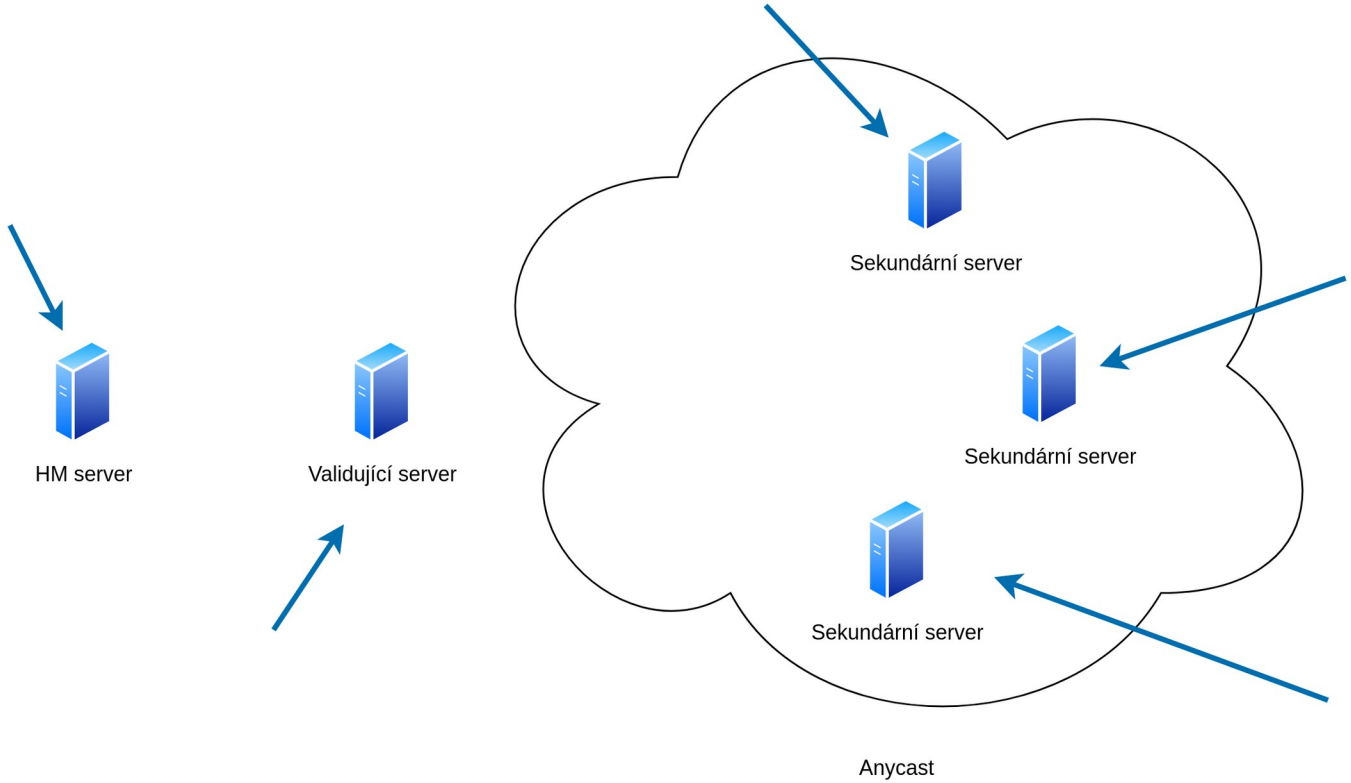



```
$ORIGIN nic.cz.
$TTL 30m
@           IN  SOA a.ns.nic.cz. hostmaster.nic.cz. (
                        1       ; serial number
                        10800           ; refresh
                        3600            ; update retry
                        1209600         ; expiry
                        7200            ; minimum
                        )

@           IN      NS      a.ns.nic.cz.
@           IN      NS      b.ns.nic.cz.
@           IN      NS      d.ns.nic.cz.

@           IN      A       217.31.205.50
@           IN      AAAA    2001:1488:0:3::2

www         IN      A       217.31.205.50
www         IN      AAAA    2001:1488:0:3::2
edice       IN      A       217.31.205.59
edice       IN      AAAA    2001:1488:0:3::10
www.edice   IN      CNAME   edice.nic.cz.
```

Zone transfer

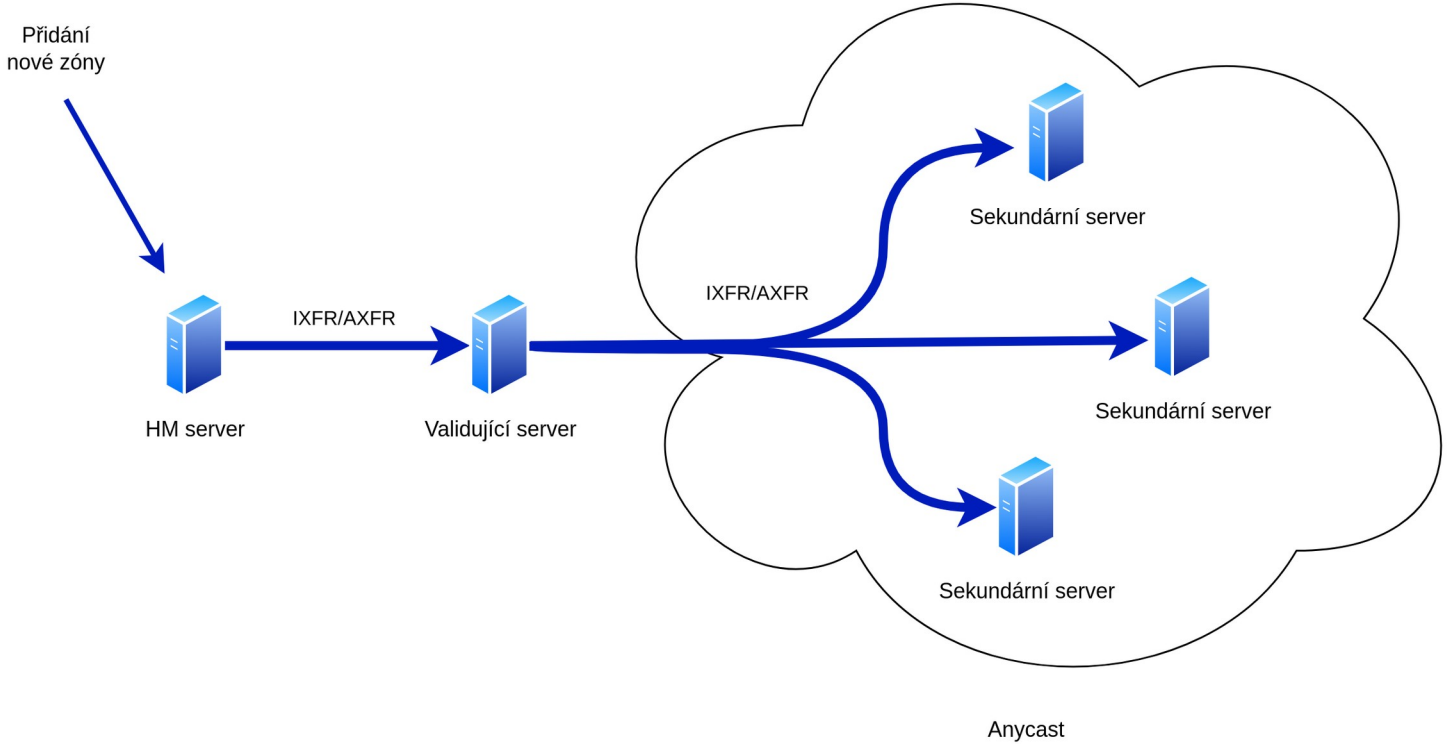


Přidání nové zóny



Přidání několik nových zón

Ideální líný scénář



Katalogová zóna

- SOA záznam
- Nekolidující jméno domény
- <uniq-id>.zones.<catalog-name>

```
;; Zone dump (Knot DNS 3.3.8)
catz.                           0   SOA invalid. invalid. 1 3600 600 2147483646 0
catz.                           0   NS  invalid.
version.catz.                   0   TXT "2"

; <uniq-id>.zones.<name of catalog zone>.

ad18c92e57fe3b09.zones.catz.    0   PTR linuxdays.cz.

d3c320987e493a0b.zones.catz.    0   PTR nic.cz.

;; Written 5 records
;; Time 2024-08-14 13:57:57 CEST
```

Konfigurace v Knot DNS – generování

Manuální

- Vytváření ručně katalogové zóny
- Řešit unikátnost doménového záznamu
- catalog-role: interpreter

Automatické

- Stará se o to knot
- catalog-role: generate
- Člen katalogové zóny
  - catalog-role: member
  - Catalog-zone: catz.

Konfigurace v Knot DNS – generování

```
template:
 - id: catz-member
    dnssec-signing: on
    dnssec-policy: dnssec-rotation
    serial-policy: unixtime
    zonefile-sync: 0
    journal-max-usage: 8G
    journal-max-depth: 10
    storage: "/var/lib/knot/"
    file: "%s/%s"
    master: another-hm
    notify: [validator-server]

  - id: catz
    dnssec-signing: off
    zonefile-load: difference-no-serial
    journal-content: all
    serial-policy: unixtime
    journal-max-usage: 8G
    journal-max-depth: 10
    storage: "/var/lib/knot"
    file: "%s/%s"
    notify: [validator-server]

zone:
  - domain: catz.
    template: catz
    catalog-role: interpret
    catalog-template: catz-member
```

```
template:
 - id: catz-member
    dnssec-signing: on
    dnssec-policy: dnssec-rotation
    serial-policy: unixtime
    zonefile-sync: 0
    journal-max-usage: 8G
    journal-max-depth: 10
    storage: "/var/lib/knot/"
    file: "%s/%s"
    master: another-hm
    notify: [validator-server]
    catalog-role: member
    catalog-zone: catz.

  - id: catz
    dnssec-signing: off
    zonefile-load: difference-no-serial
    journal-content: all
    serial-policy: unixtime
    journal-max-usage: 8G
    journal-max-depth: 10
    storage: "/var/lib/knot"
    file: "%s/%s"
    notify: [validator-server]

zone:
  - domain: linuxdays.cz
    template: catz-member

  - domain: nic.cz
    template: catz-member

  - domain: catz.
    catalog-role: generate
    template: catz
```

Konfigurace sekundárních DNS serverů

Knot

```
acl:
  - id: dns-query
    address: <monitoring-ip>
    action: transfer

template:
  - id: hidden-master
    storage: /var/lib/knot
    master: [ <validator server> ]
    journal-content: none

zone:
  - domain: catz
    template: hidden-master
    acl: dns-query
    catalog-role: interpret
    catalog-template: hidden-master
```

Bind

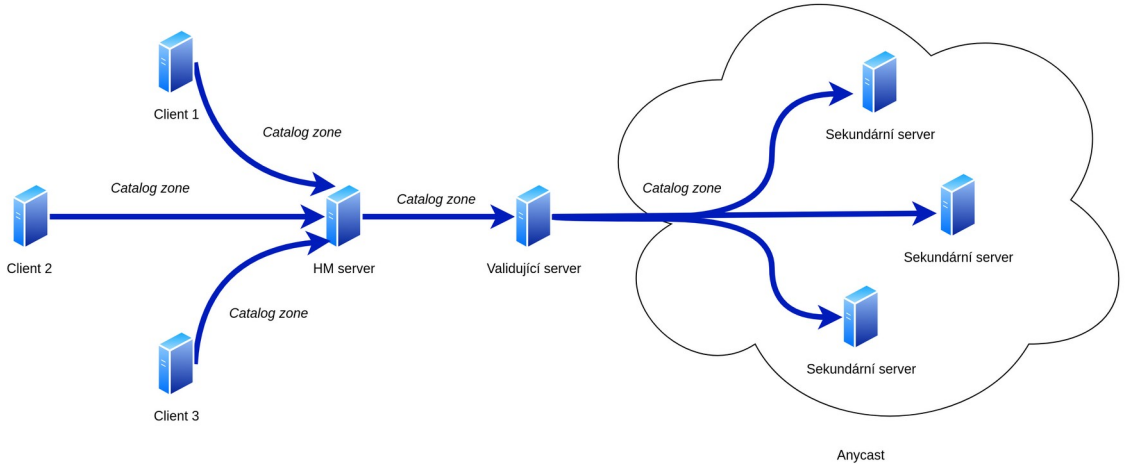
```
options {
   ...

   # Access Control
   allow-query             { any; };
   allow-transfer          { none; };
   allow-update            { none; };
   allow-notify            { none; };

   catalog-zones {
     zone "catz" default-primaries { <validator server>; };
   };
};

zone "catz" in {
   type secondary;
   file "/var/lib/bind/catalog.zone";
   masters {<validator server>; };
   allow-query {<validator server>; <monitoring ip>;};
   allow-notify { <validator server>; };
};
```

NSD

```
pattern:
   name: "hidden-master"
   zonefile: /var/lib/nsd/%s

   allow-notify: <validator server> <tsig-key>
   allow-axfr-fallback: yes

zone:
   name: catz
   include-pattern: "hidden-master"
   catalog: consumer
   catalog-member-pattern: "hidden-master"
   allow-notify: <validator server> <tsig-key>
   allow-query: <monitoring-ip> NOKEY
```

Katalogová zóna – další možnosti Knot DNS

- Skupiny
- Sloučení katalogových zón



Limitace - NSD

- Katalogové zóny od verze 4.9
- Umí pracovat jen s jednou zónou

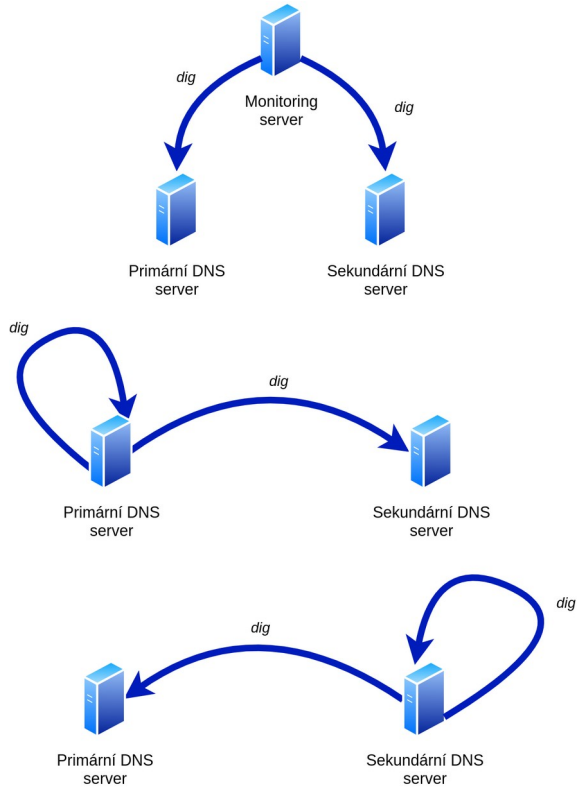
Package nsd

- buster (oldoldstable) (net): authoritative domain name server
  4.1.26-1: amd64 arm64 armhf i386
- bullseye (oldstable) (net): authoritative domain name server
  4.3.5-1: amd64 arm64 armel armhf i386 mips64el mipsel ppc64el s390x
- bookworm (stable) (net): authoritative domain name server
  4.6.1-1: amd64 arm64 armel armhf i386 mips64el mipsel ppc64el s390x
- trixie (testing) (net): authoritative domain name server
  4.10.1-1: amd64 arm64 armel armhf i386 mips64el ppc64el riscv64 s390x
- sid (unstable) (net): authoritative domain name server
  4.10.1-1: alpha amd64 arm64 armel armhf hppa i386 m68k mips64el ppc64 ppc64el riscv64 s390x sh4 sparc64 x32
  4.9.1-1 [debports]: ia64

The Oracular Oriole (pre-release freeze)		Nsd trunk series
4.10.1-1	release (universe)	2024-08-02
The Noble Numbat (current stable release)		Nsd trunk series
4.8.0-1build3	release (universe)	2024-04-05
The Jammy Jellyfish (supported)		Nsd trunk series
4.3.9-1	release (universe)	2021-12-20
The Focal Fossa (supported)		Nsd trunk series
4.1.26-1build1	release (universe)	2019-10-24

Monitoring – aktuálnost zón

- Automatický monitoring nových zón
- Catalogová zóna není veřejná zóna



Monitoring – katalogová zóna

- Prázdná katalogová zóna

- Obsahuje jen správné domény?

Shrnutí

- Ideální pro časté změny zónových souborů
- Možné automatické i manuální generování
- Kontrolovat obsah katalogové zóny

Děkuji vám za pozornost!

Lukáš Vacek

CZ.NIC | SPRÁVCE DOMÉNY CZ

Sloučení katalogových zón

```
template:
  - id: catz-new-catalog
    storage: "/var/lib/knot/"
    file: "%s/%s"
    zonefile-sync: 0
    journal-max-usage: 8G
    journal-max-depth: 10
    master: <hm server>
    notify: [<dns-servers>]
    catalog-role: member
    catalog-zone: catz-merge.

  - id: catz-merge
    storage: "/var/lib/knot/"
    file: "%s/%s"
    zonefile-load: difference-no-serial
    journal-content: all
    serial-policy: unixtime
    journal-max-usage: 8G
    journal-max-depth: 10
    notify: [<dns-servers>]
```

```
zone:
 - domain: catz
    template: catz
    catalog-role: interpret
    catalog-template: catz-new-catalog

  - domain: catz2
    template: catz
    catalog-role: interpret
    catalog-template: catz-new-catalog

  - domain: catz-merge
    template: catz-merge
    catalog-role: generate
```

Zdroje

- https://datatracker.ietf.org/doc/rfc9432/
- https://launchpad.net/ubuntu/+source/nsd
- https://packages.debian.org/search?keywords=nsd