DNSSEC na serverech na dvě kliknutí

aneb FreeIPA to zařídí

Petr Špaček

pspacek@redhat.com
Red Hat

EurOpen.CZ 44

fedora

Ve stručnosti

- Základní požadavky na DNS
- . . . a konflikt s DNSSEC
- Princip řešení
- Nasazení DNSSEC klasicky
- Proč vymýšlet něco netradičního?
- **Nasazení DNSSEC na 2 kliknutí**
- DNSSEC na plný plyn

fedora

Základní požadavky na DNS

- Vysoká dostupnost – alespoň pro čtení
- Dočasné omezení zápisu (obvykle, příliš) nevadí
- Použití slave serverů

fedora

Základní požadavky na DNS . . . a DNSSEC

- Vysoká dostupnost – alespoň pro čtení
- Záznam a jeho podpis:

```
;; ANSWER SECTION:
www.nic.cz.     474  IN  A  217.31.205.50
www.nic.cz.     474  IN  RRSIG  A 5 3 1800
                20140520090247 20140506115503
                18996 nic.cz. SO8Zt1SM81R5BwPj
                M5DWz2jSC7gBVuUsZ4Ya/qNSK2m0FO
                X2jd4ChUE4n+id2YH1RfTQjRfwb2L
                                ...
```

fedora

Vysoce dostupný DNSSEC vs. omylní lidé

- „Běda vám, když to nestihnete!“
- Stačí poučení obsluhy?
- I když jde o „laiky“?
- Jasná cesta k **ne**nasazení DNSSEC

fedora

Vysoce dostupný DNSSEC vs. pomalí lidé

- „Nebojte se, bude na to dost času . . . “
- Stačí poučení obsluhy + dostatek času?
- Co tím získá útočník?
- Cesta k odmítnutí (možná až po pilotním nasazení)

fedora

Vysoce dostupný DNSSEC a stroje

- Nejlepší řešení – nedostat se do problémů ☺
- Distribuované podepisování
- Technicky nejnáročnější
- Nejsnadnejší pro obsluhu

fedora

Bezpečnost a správa klíčů

- Dostupnost není vše
- Bezpečné algoritmy, klíče, konfigurace . . .
- **. . . a schopnost reagovat na problémy**
- Schopnost výměnit klíče je zásaní
- Distribuce klíčů je obtížná

fedora

Nasazení DNSSEC klasicky

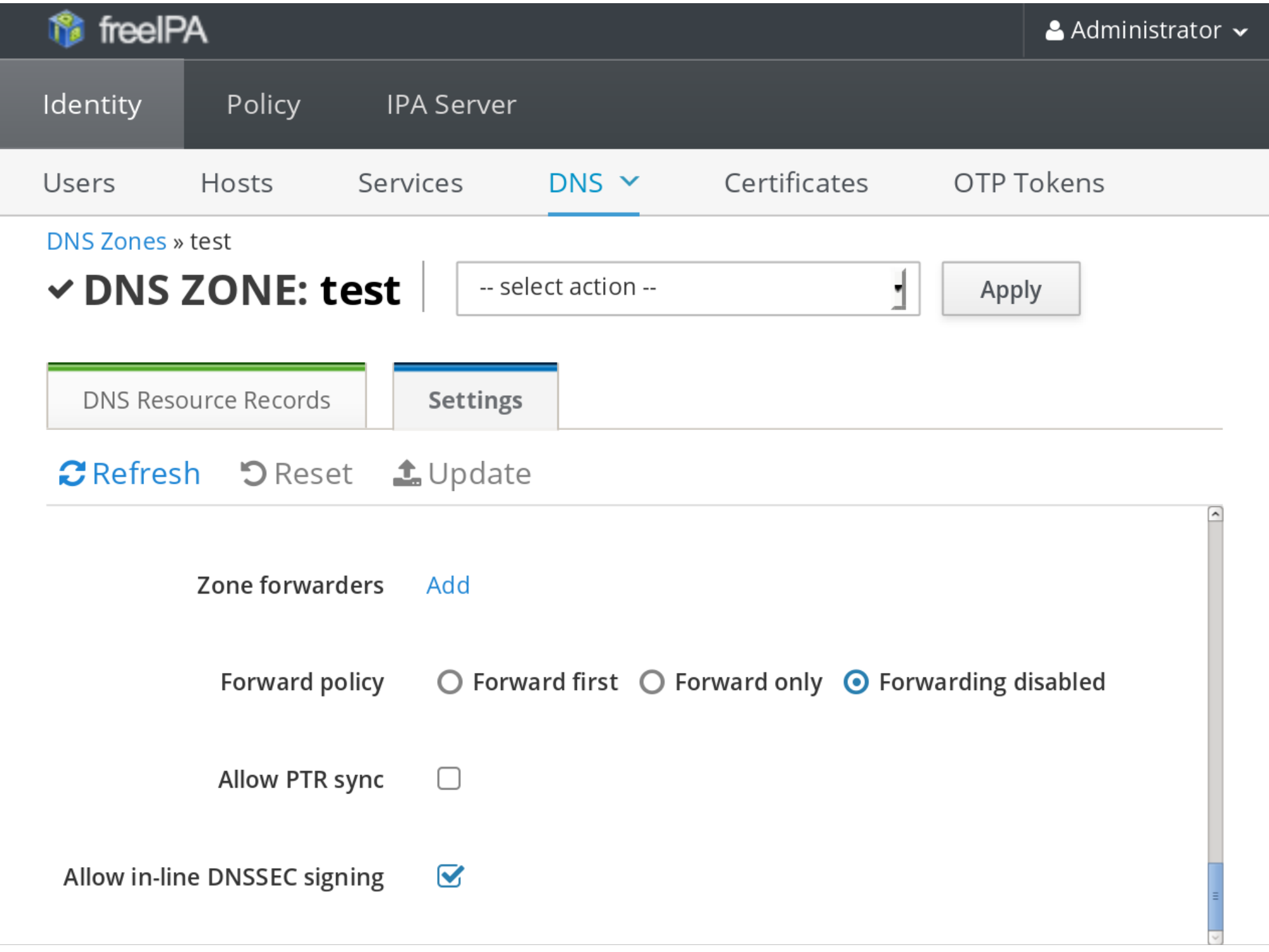
- Konfigurace DNS serverů
- Distribuce klíčů
- Správa (výměna) klíčů
- Komunikace s nadřazenou zónou

fedora

Proč vymýšlet něco netradičního?

- Klasický přístup → labyrint nástrojů
- Zavisí na dobrých znalostech obsluhy
- Kdo má čas bloudit v labyrintu nástrojů . . .

  . . .
- Správci sítí ne!


freeIPA
Administrator
Identity
Policy
IPA Server
Users
Hosts
Services
DNS
Certificates
OTP Tokens
DNS Zones » test
DNS ZONE: test
-- select action --
Apply
DNS Resource Records
Settings
Refresh
Reset
Update
Zone forwarders
Add
Forward policy
Forward first
Forward only
Forwarding disabled
Allow PTR sync
Allow in-line DNSSEC signing

fedora

DNSSEC na plný plyn

- Bezpečný překlad jmen je (skoro) k ničemu
- Distribuce klíčů pomocí DNSSEC
- SSH, IPsec, TLS, PGP …

fedora

DNSSEC na plný plyn – FreeIPA pod kapotou

- SSH integrace „zadarmo“
- Integrovaná certifikační autorita?
- Co dál?

fedora

FreeIPA – nasazení

- První server:
  `# ipa-server-install --setup-dns`
- Další server – příprava:
  `# ipa-replica-prepare`
- Další server – instalace:
  `# ipa-replica-install --setup-dns`

fedora

FreeIPA není jen o DNS

FreeIPA nabízí také správu:

- uživatelských účtu
- X.509 certifikátů
- autorizačních pravidel (SUDO, host-based access control)
- propojení s Active Directory vč. Single-Sign-On
  video `trust_add_demo.webm`

fedora

Závěrem – jak dostat DNSSEC do praxe

- Požadavek: **Jednoduchost**
- Požadavek: **Vysoká spolehlivost**
- Požadavek: **Nenáročná údržba**
- FreeIPA – ideální „balení“ pro podnikové nasazení
- **`www.freeipa.org`**
- **`www.redhat.com/mailman/listinfo/freeipa-users`**