DNSSEC deployment done with two clicks

Red Hat

Petr Špaček
pspacek@redhat.com
Tomáš Hozza
thozza@redhat.com

IT 14

fedora

Agenda

1. **Client side**
   - Motivation
   - Requirements
   - Architecture
2. **Server side**
   - Requirements
   - Highly available DNSSEC
   - Distributed signing & classic tools
   - DNSSEC on steroids
3. **Conclusion**

Section 1

Client side

fedora

Motivation

- Trusted data in DNS (TLSA, SSHFP, IPSECKEY)
- Attacks on plain DNS
- Authenticated DNS data for applications
- End-to-end DNSSEC validation

fedora

Client side - Requirements

- Local validating resolver
- Resolver reconfiguration mechanism
- Split DNS handling
- Network-provided nameservers probing
- Fall-back configuration
- Captive portal detection & handling
- ...

fedora

Current situation

NetworkManager

- On every network change runs dispatcher scripts
- Provides API for reading network configuration

dnssec-trigger

- Provides NM dispatcher script
- Handles – nameservers probing, captive portal detection, fall-back configuration, split DNS
- Rewrites resolv.conf

unbound

- Reconfigured by dnssec-trigger (global forwarders)
- Reconfigured by dnssec-trigger dispatcher script (forward zones)

fedora

Future plans

NetworkManager

- Use configuration used by previous solution
- Provide better and extended configuration possibilities
- Rewrite resolv.conf

unbound NetworkManager DNS plugin

- Incorporate dnssec-trigger's (and dispatcher script) functionality
  - nameservers probing
  - captive portal detection and handling
  - split DNS configuration
  - reconfigure unbound

unbound

- Reconfigured by unbound NetworkManager DNS plugin

Section 2

Server side

fedora

Requirements

- High availability – at least read only
- Resource Record and it's signature:

```
;; 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

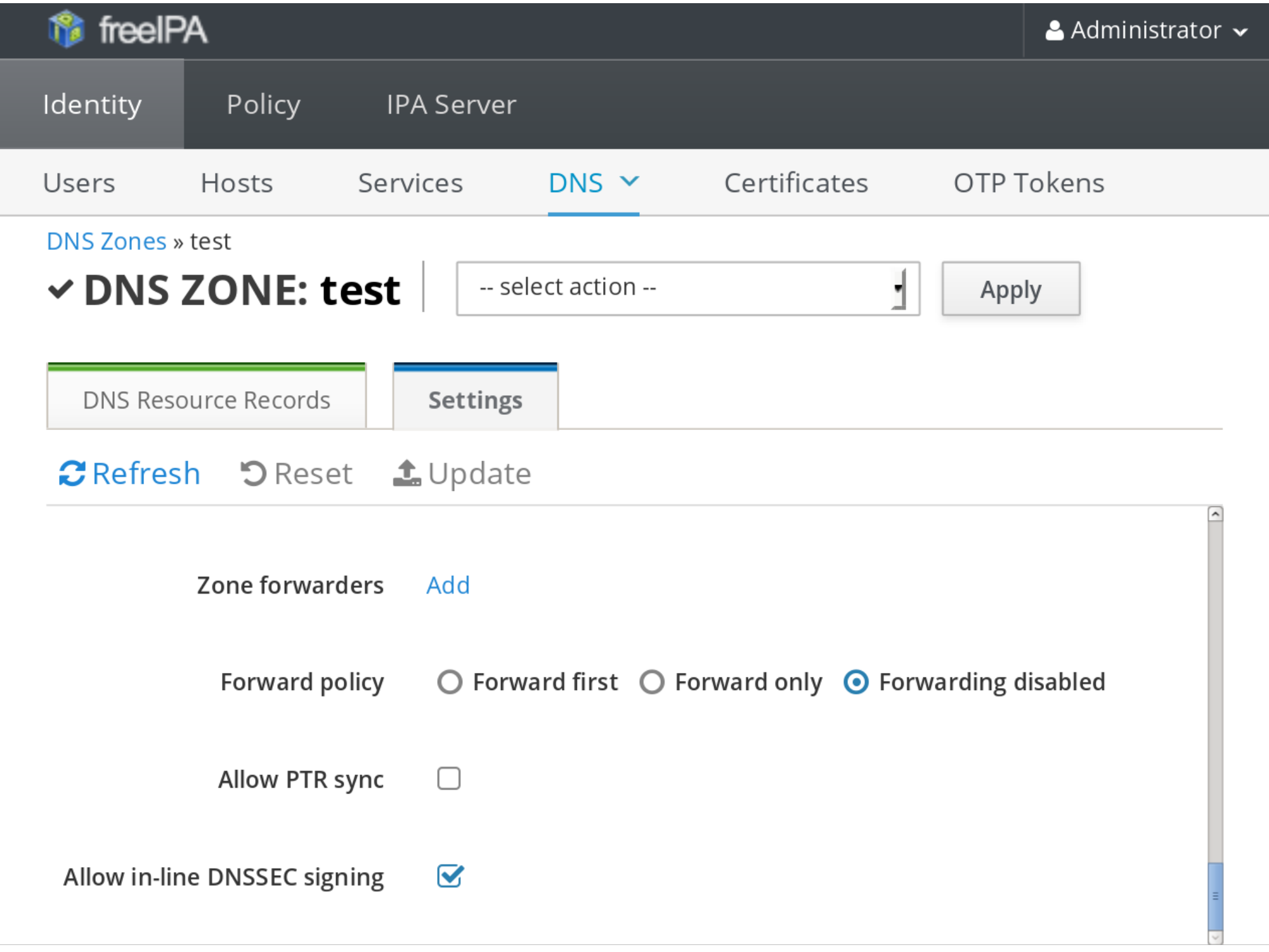
Highly available DNSSEC

- Avoid signature expiration problem completely
- Distribute signing process
- Hard to implement
- Easy to use

fedora

Distributed signing & classic tools

- Configure all DNS servers
- Distribute signing keys
- Install key management system
- Update public keys in parent zones


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 on steroids

- DNSSEC is (almost) useless when used purely for name-IP resolution
- DNSSEC as public key distribution mechanism
- SSH, IPsec, TLS, PGP ...
- **FreeIPA** – SSH integration "for free"
- **FreeIPA** – integrated Certificate Authority ...

Section 3

Conclusion

fedora

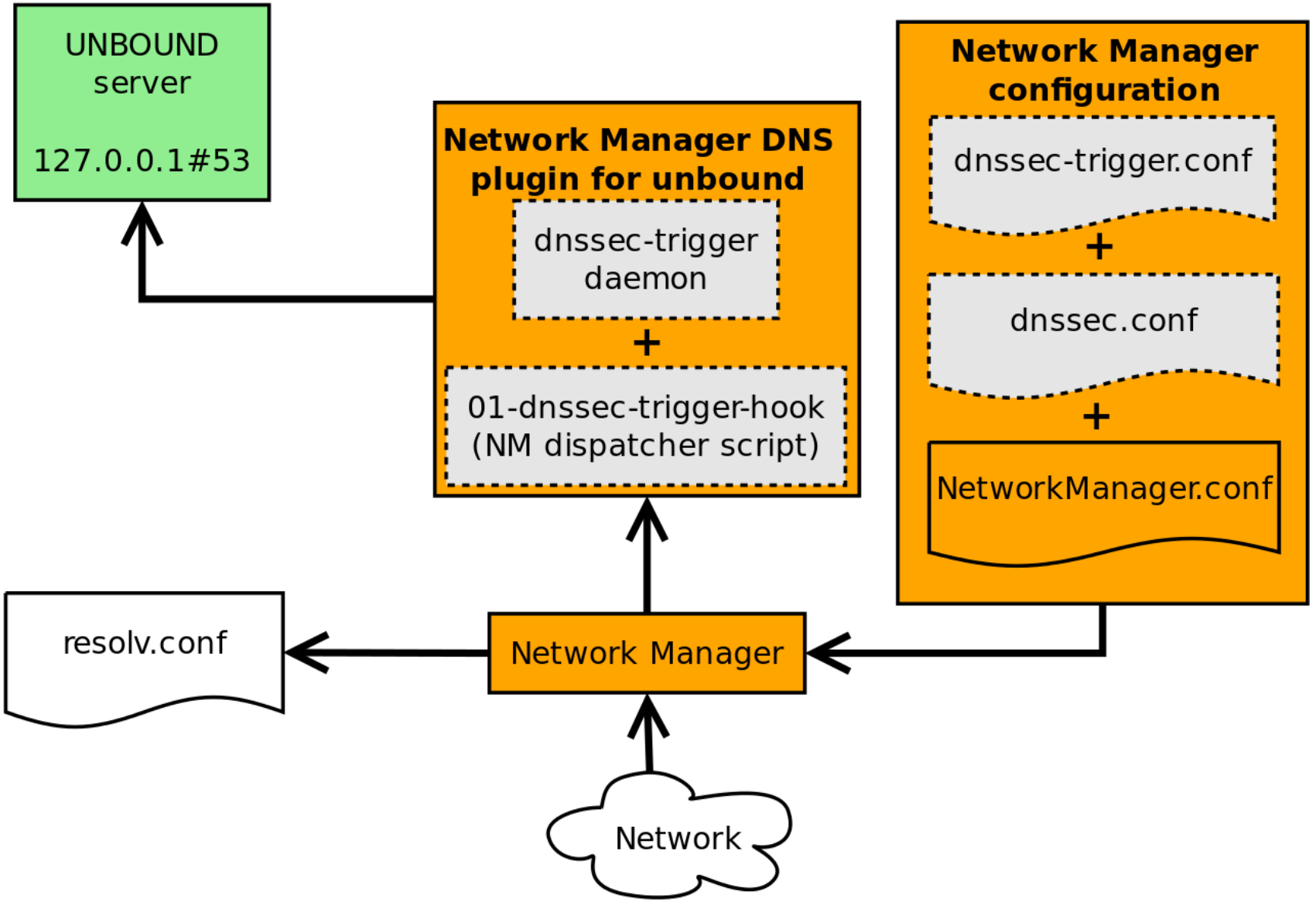
Conclusion

- Requirement: **Simple & quick deployment procedure**
- Requirement: **High availability**
- Requirement: **Maintenance-free system**
- Clients and workstations work in dynamic environment and need special approach
- FreeIPA – "canned" solution for internal networks
- `www.freeipa.org`
- `www.redhat.com/mailman/listinfo/freeipa-users`

pspacek@redhat.com
thozza@redhat.com

fedora

Future plans



fedora

Current situation