DNS FOR ENTERPRISE DOMAINS

FREEIPA AND SAMBA AD EXPERIENCE

FOSDEM 2025

Alexander Bokovoy
Senior Principal Software Engineer | Red Hat | FreeIPA | Samba Team

ABOUT ALEXANDER

- Samba Core Team member since 2003
- FreeIPA core developer since 2011
- MIT Kerberos contributor

DNS FOR ENTERPRISE DOMAINS

ENTERPRISE DOMAINS IN A NUTSHELL

- Active Directory: Kerberos + LDAP + DCERPC protocols for files and management
  - domain controllers: Windows and Linux
  - clients: mostly Windows, occasionally Linux

ENTERPRISE DOMAINS IN A NUTSHELL

- FreeIPA: Kerberos + LDAP + management API
  - domain controllers: Linux
  - clients: Linux and other POSIX systems

WHO NEEDS DNS?

- Both domain controllers and domain members

DOMAIN CONTROLLERS

- Kerberos auto-discovery:
  - DNS TXT records to find Kerberos realm
  - DNS SRV records to find domain controllers
- LDAP server auto-discovery
- Domain controller CNAMEs

Non-RODC server

If the DC is a non-RODC with default NC X (and NC X's GUID is G) in forest Z, then it registers SRV records with Service.Proto.Name equal to the following.

```
_ldap._tcp.X
_ldap._tcp.dc._msdcs.X
_ldap._tcp.G. domains._msdcs.Z
_kerberos._tcp.X
_kerberos._udp.X
_kerberos._tcp.dc._msdcs.X
_kpasswd._tcp.X
_kpasswd._udp.X
```

DOMAIN MEMBERS

- Kerberos auto-discovery
- LDAP server auto-discovery
- Registration of own RRs

REGISTRATION OF RRS

- Authenticated using the Kerberos ticket obtained with the machine account credential
- Authenticated with GSS-TSIG (MS-GSSA, on top of RFC3645)
- Expects no use of HMAC-MD5 (violates RFC2845)
- Uses different method of building the digest to sign the last message in GSS-TSIG negotiation
- Wildcard updates not supported in Windows DNS server

DNS SERVER SIDE OF RR REGISTRATION

- Access controls heavily influenced by Active Directory ACLs
- Bind implements 8 variants of ACL imitation
  - 4 relying on AD machine name
  - 4 relying on Kerberos principal

CLIENT SIDE OF RR REGISTRATION

- SSSD
  - Monitors network interfaces
  - Constructs `nsupdate` payload and runs the tool
  - uses machine account creds (`/etc/krb5.keytab`)

CLIENT SIDE OF RR REGISTRATION

- Samba: two different DNS update mechanisms
  - `nsupdate-gss`: used for migrating old NT domain deployments (pre-2003)
  - `samba-dnsupdate`: wrapper over `nsupdate`
- All tools rely on the machine account creds

DNS AT THE DOMAIN CONTROLLER SIDE

- Domain controllers expect properly configured DNS
- Once DNS zones set up, dynamic update becomes the issue
- Changes may come through DCE RPC updates as well

FREEIPA DNS SERVER INTEGRATION

- Can work with external DNS server
- Integrates with `bind` via dyndb API: `bind-dyndb-ldap` project
  - Zone data is stored in LDAP and replicated outside `bind`
- Integrated DNS can be managed through IPA API or DNS updates
  - supports DNSSEC integration via OpenDNSSEC + helpers
- Many users rely on FreeIPA Web UI to handle DNS zones

SAMBA DNS SERVER INTEGRATION

- Can work with external DNS server
- Integrated with `bind` via `DLZ` API
  - Samba embeds copy of `bind` DLZ API headers
  - Integrated DNS can be updated via DNS updates or via DCE RPC calls
- Has its own DNS server implementation
  - limited functionality and performance

ISSUES WITH BIND APIS

- Both dyndb and DLZ APIs aren't stable
- ISC BIND team often refactors them
  - dyndb API is considered internal and subject to changes
  - CVE fixes often change internal ABIs
- `bind` 9.20.4 changelog: "DLZ API will be removed in future"
- develoment headers not to be installed anymore (issue#4729)

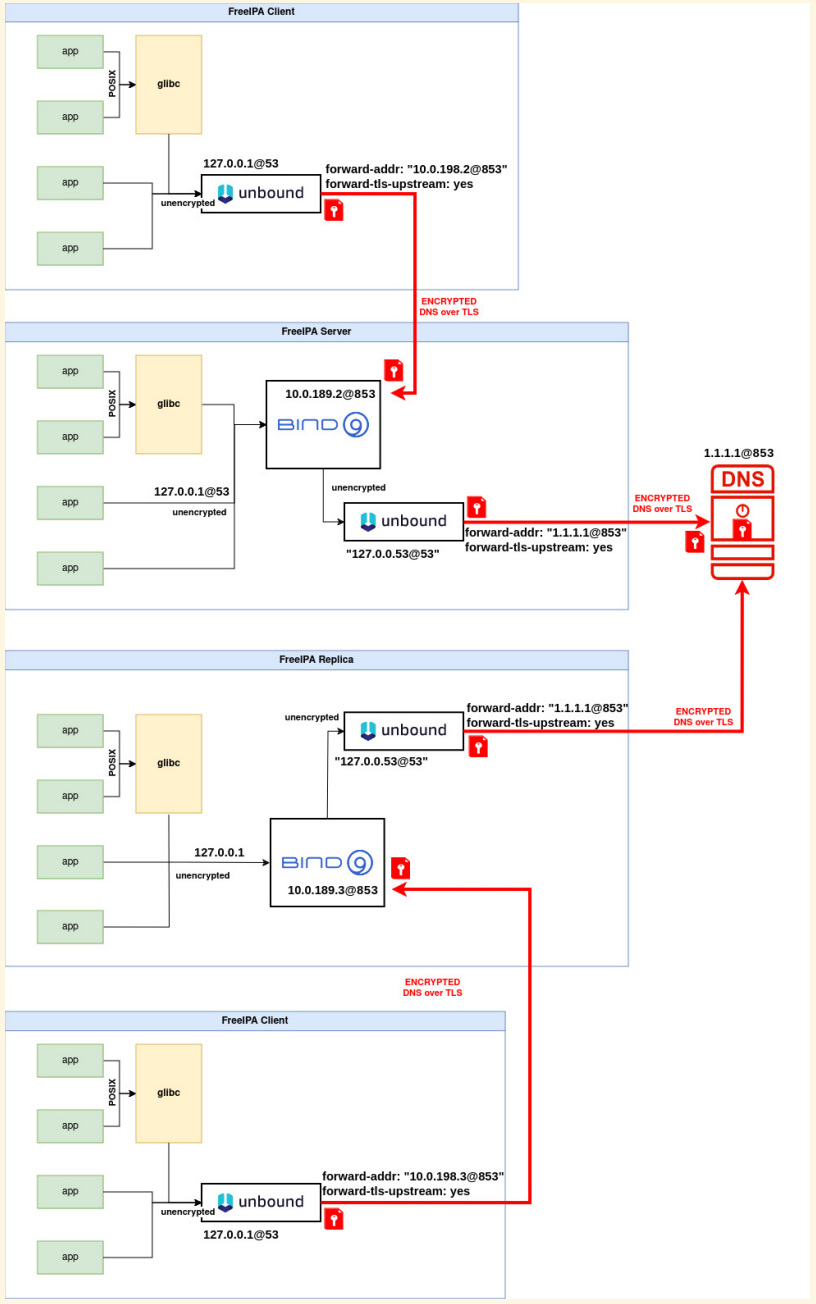
PATH FORWARD

bind-dyndb-ldap

- Current code supports only bind 9.18 or earlier versions
- bind CVE fixes made internal ABI different
- a rewrite is required but bind API is not really accessible
  - rewrite is ongoing

ENCRYPTED DNS SUPPORT

- FreeIPA and SSSD teams work on encrypted DNS support
  - DoT interface enabled in an integrated DNS server
  - DoT forwarder via unbound


FreeIPA Client
app
app
app
app
POSIX
glibc
127.0.0.1@53
unencrypted
unbound
forward-addr: "10.0.198.2@853"
forward-tls-upstream: yes
ENCRYPTED
DNS over TLS
FreeIPA Server
app
app
app
app
POSIX
glibc
10.0.189.2@853
BIND 9
127.0.0.1@53
unencrypted
unencrypted
unbound
"127.0.0.53@53"
forward-addr: "1.1.1.1@853"
forward-tls-upstream: yes
ENCRYPTED
DNS over TLS
1.1.1.1@853
DNS
FreeIPA Replica
app
app
app
app
POSIX
glibc
unencrypted
unbound
"127.0.0.53@53"
forward-addr: "1.1.1.1@853"
forward-tls-upstream: yes
ENCRYPTED
DNS over TLS
127.0.0.1
unencrypted
BIND 9
10.0.189.3@853
ENCRYPTED
DNS over TLS
FreeIPA Client
app
app
app
app
POSIX
glibc
unencrypted
unbound
127.0.0.1@53
forward-addr: "10.0.198.3@853"
forward-tls-upstream: yes

BACKPORT COMPLEXITY

- A combination of `bind` and unbound
  - `bind` 9.18 does not support all required DoT features
    - custom backported patches to enable DoT
  - `bind` 9.20+ does not support `bind-dyndb-ldap`

BACKPORT CHALLENGES

- RHEL 10 beta removed OpenSSL Engine APIs
  - we cannot use OpenSSL Provider API in `bind` 9.18
  - DNSSEC support removed
    - `bind` 9.18 only supports external PKCS#11 tokens via Engine API
    - (provider API support backport is not finished yet)

CRYPTOGRAPHIC CHALLENGES

- Enterprise domains typically are in use in regulated environments
  - 2030: NIST soft-requirement is to stop usage of SHA-1 and older primitives
  - 2035: NIST hard-requirement is to remove old cryptography primitives
  - Reality: post-quantum crypto will already be required for new deployments before 2030
  - FALCON is still not standardized and attacks on it are to continue
    - SHIFT SNARE: https://eprint.iacr.org/2025/146

QUESTIONS?

Mastodon (Alexander): @abbra:mastodon.social

Blog (Alexander): vda.li/en/