DNSSEC for RHEL/Fedora

Paul Wouters

DNSSEC in Fedora / EPEL (community supported)

- DNSSEC servers (bind, unbound, nsd, knot, pdns)
- DNSSEC signers (bind, bind-pkcs11, opendnssec, dnssec-tools)
- DNSSEC utils (validns, ldns, dnssec-tools, hash-slinger, openpgpkey-milter, etc)
- DNSSEC desktop integration via dnssec-trigger
- VPN support via unbound or resolv.conf reconfiguration
  - libreswan/openswan, openvpn, vpnc

DNSSEC in Red Hat Enterprise Linux (RHEL)

- Supported software in core or *collections*
- Unsupported software still available in EPEL repository
- All Fedora DNSSEC related packages are in RHEL or EPEL
- DNSSEC servers: Only bind and unbound in RHEL
- DNSSEC signers:
  - bind9 - supported in RHEL6 and RHEL7
  - opendnssec only supported for Identity/Policy Management with FreeIPA in RHEL7 with softhsm v2 beta (although it should work for non IDPm usage.

DNSSEC plans for cloud support (Fedora/RHEL)

- Running systems with hundreds of containers/VMs
  - do not run validators in each one – waste of resources
- Support in glibc for clearing the AD bit for non-trusted validators
- Look at systemd-resolved as transport for DNS data from host into containers
- Look at ietf-dnsop-edns-query-chain support
- IPsec and DNSSEC support
- Unifying hotspot and DNSSEC support natively in NetworkManager
  - phase out separate dnssec-trigger

DNSSEC and crypto requirements

- nss, openssl, libgcrypt, gnutls and kernel are the only allowed cryptography providers in RHEL
- opendnssec integration possible due to softhsm change to allow building with openssl instead of botan
- ECC: Only “Suite B” (aka NIST) curves allowed (P-256, etc)
  - No GOST
  - No Curve25519
  - No IETF brainstorm curves