DNS in Mostly Isolated Networks

draft-many-dnsop-dns-isolated-networks

Marc Blanchet
marc.blanchet@viagenie.ca
2023-11-07

Context

- « Mostly isolated networks »:
  - Deepspace:
    - Mars IP infrastructure (see: IOAG architecture document and deepspace IP assessment)
    - Long delays and intermittent communications, « low » bandwidth (but…)
    - Community request for best practices for DNS infrastructure in this context
  - Other use cases: remote networks, undersea, …
- Key requirements:
  - DNS resolution using Internet not always possible (intermittent comms) -> local resolution
  - Need a local autonomous environment with all the useful names
  - Secure (aka DNSSEC) -> use same trust anchor, local validation
  - Remote management
- Terminology:
  - Local means the « remote » infrastructure point of view.

Local DNS Infrastructure

- Common to all approaches, local DNS infrastructure:
  - Authoritative NS
  - Resolvers
  - Trust anchor preloaded
  - Some way (not necessarily with IP) to send data/zones from Internet to local infrastructure
  - Local use names are in the normal DNS tree
  - Clients using local resolvers
  - Use RFC8806

Approaches (1)

- Pre-walk of all needed names
  - Do a tree walk for all local names needed, with DNSSEC related RRs
  - Save and send to local infrastructure by some means
- need to know all required names, do not forget one

* Suggested by Warren Kumari. All errors are mine.

Approaches (2)

- Pre-fetch of all zones in the needed name hierarchy
  - Carefully choose name hierarchy (TLD, 2ndlevel, ..), maybe dedicated?
  - Have access to the zones
  - Send zones to local infrastructure by some means
- if not a dedicated name hierarchy, a lot of non useful RRs uploaded.

Approaches (3)

- Special zone
  - From a current zone, select only the needed RRs and then create a special version of the zone
  - sign it, send it to local infrastructure by some means
- need to carefully manage both version of zones

* Suggested by Mark Andrews. All errors are mine.

Approaches

- Other choices:
  - A new root… does not use current trust anchor.
  - Local names/split DNS.
- At times, the local infrastructure will be connected to Internet and in most cases, will be managed from Internet.

Next Steps

- More detailed info on RR: which RR, TTL considerations, …
- Interest for this working group?

- Specification: draft-many-dnsop-dns-isolated-networks
- Contact: Marc Blanchet, marc.blanchet@viagenie.ca