DNS Services; modification plan

Olaf M. Kolkman

Outline

- Background/Motivation
- The Proposal
- Some of the details

Background: Context

- RIPE NCC provides delegations in domains under in-addr.arpa and ip6.arpa
- This presentation is about modifying the way we provide these delegations
- We present an overview; the details will be discussed in the relevant groups e.g. DN* and DB

Background: DNSSEC

- DNSSEC key exchanges.
  - DNSSEC needs exchange of key information
    - The authentication method needs to be ‘as strong’ as the authentication method used for the exchange of delegation information.
  - The public keys need to be transferred to the zone files
    - Just as delegation information needs to be transferred to the zone file
  - Using the domain objects to store the DNSSEC public keys seems the obvious solution.

Background: inconsistencies

- The current interface updates zone files directly and updates the WHOIS DB
  - But it is possible to update the WHOIS DB without going through the auto-inaddr@ripe.net interface.
    - Confusing; *why did my zone become lame*?
    - Inconsistency between NS RRs in the zone files and name server attributes in the domain objects.
- To get a delegations
  - Assignments need to be made for /24
  - For /16 an allocation is sufficient

Background: Control

- Enable more fine grained control for creation of domain objects.
  - Internally referred to as the Denmark problem
    - The DNS services are operated from Denmark.
    - Addresses are requested by “other” LIRs.
- Now only interface to maintain delegations.
  - Enable other interfaces, just like we do for WHOIS DB
    - Web-Updates
    - Auto-dbm
    - Sync-update
    - LIR portal

The proposal

- Use the WHOIS DB as the single and authoritative source for zone information.
- Replace auto-inaddr@ripe.net with the set of WHOIS DB interfaces
- Introduce the MNT-ZONES attribute in INETNUM and INETNUM6 objects
- Review of the DNS checks

More details

In the next slides we'll address:

- Moving to WHOIS as authoritative data source for the DNS
- The MNT-ZONES attribute
- DNS Checks
- Enabling DNSSEC

Detail: WHOIS as data source

- Currently: zone-files under RCS and WHOIS DB.
- Data needs to be made consistent
- 3 categories of inconsistency
  - In DB not in DNS
  - In DNS not in DB
  - Different nameserver attributes and NS RRs
- Details will be proposed in appropriate working group

Detail: MNT-ZONES attribute

- Controls who is allowed to create or delete domain object
- Can be set through the LIR interface
- If not set it defaults to MNT-LOWER or MNT-by (in that order)
- No limitations on the maintainer; anybody authorized by network object owner can create/delete zone objects
- Uses existing authorization model

Detail: DNS checks

- Currently DNS checks (cf RFC1912) are done by Marvin, need to be ported to the WHOIS DB, as plug-in.
- If rewrite of checks is needed than they will be reviewed (via DNS-WG).
- There are more checks e.g. checks for ‘/24 domains’ enclosed by ‘/16 domains’.
  - Details will need to be ironed out, proposals will go to the working group.

Detail: enabling DNSSEC

- After this process DNSSEC key exchange can be implemented
  - DNSSEC KEY attribute
  - Using the existing WHOIS DB authentication methods
  - Those who have power to change/create/delete a delegation have the power to upload a key
  - Strength of authentication under own control
  - Details need to be worked out
    - ‘Minimal’ authentication strength?
    - Name and format of attribute

Consequences and conclusions

- Consistent data, after a cleanup
- DNSSEC deployment becomes trivial
- Eases development of new methods to maintain delegations e.g. via the LIR portal

- For some details community feedback is needed. Will be asked via the appropriate working groups

Questions???

- Slides will be available from

  http://www.ripe.net/ripe/meetings/ripe-46/presentations/

- Questions: olaf@ripe.net