Reverse DNS Project an update and proposals

RIPE NCC

Outline

- 1 slide on context
- 3 subprojects: goals and implementation
- Project Details
  - Cleanup
  - Authorization model changes

Context

- RIPE NCC provides delegations in domains under in-addr.arpa and ip6.arpa
- 3 motivations for this project

1. Inconsistencies
2. Control
3. DNSSEC

In one line:

Use the WHOIS as the primary interface and backend for reverse delegation management.

1: The 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.
- In the policy

  To get a delegations

  – Assignments need to be made for /24

  – For /16 an allocation is sufficient

Cleanup of inconsistencies

- Prerequisite for WHOIS to be used for generation of zonefiles
  - Delegation information ‘uploaded’ via **domain** objects
  - One consistent source for delegation information
- Enables replacement of auto-inaddr@ripe.net with the set of WHOIS DB interfaces
  - E.g sync updates, web updates etc.
  - Makes it easier to provide new and easier interfaces to our customers.

2: Fine grained 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

Introduction of “mnt-domains:”

- Introduce the “mnt-domains:” attribute in **inetnum** and **inetnum6** objects
  - Allows address space users to ‘delegate’ the maintenance of reverse space to 3rd parties.
  - It will be the only authorization mechanism.
    - No special headers
- Simplification of policy
  - Needed to allow for the above
  - In addition: drop need for having an assignment, LIRs can set up reverse zones for their customers while assignment is being arranged.

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.

Implementation Deferred

Project timeline

- Oct1, 03 : Original proposal
- Dec 4, 03 : Cleanup proposal
- Dec 8, 03 : Redirection Domain updates
- Jan 6, 04 : Notification of inconsistencies (Cleanup)
- Jan 20-
  Feb 21, 04 : “mnt-domain:” and draft reverse delegation policy discussion
- Mar 1, 04 : Cleanup of remaining inconsistencies
- April, 04 : Implementation “mnt-domain:” based authorization.
- Q2-Q3 04 : DNSSEC key exchange

Outline

- 1 slide on context
- 3 subprojects: goals and implementation
- Project Details
  - Cleanup
  - Authorization model changes

Cleanup Phase

- Goal
  - 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
- Method:
  - Find inconsistencies
  - Inform contact of intended action
  - 1 March: perform intended action

Inconsistencies

- NS RRs in zone file without Domain object
  - Create domain objects
- Domain objects without NS RRs
  - Delete domain objects if needed
- Mismatches between NS RRs and nserver: attributes
  - Fix; DNS has preference
- Delegations present for unallocated (returned) address space

Problems encounter

- Owners of /24 domain objects with a less specific /16 domain object where contacted in error
  - We will not delete domain objects for this class of users
  - We will confirm this in targeted mails

Proposed new authorization mechanism

- In the **inetnum** objects add one or more references to persons who can create or delete **domain** objects.
- If not set it defaults to “mnt-lower:” or “mnt-by:” (in that order)
  - To enable the current maintainers of the address space to create **domain** objects
- No limitations on the maintainer; anybody authorized by **inetnum** object owner can create/delete **domain** objects

More authorization changes

- Make “mnt-by:” a mandatory attribute
- To prevent ‘reverse domain hijacks’
- To make sure **domain** objects are properly protected
- Provides for flexible and configurable protection of objects in combination with ‘mnt-domains:’

Consequences

- In many cases completely backwards compatible
- But the existence of a **inetnum** object with the customers maintainer blocks the creation by the LIR
  - Inconsistent with the current situation (reg-id based)
  - Needs LIR-customer interaction to be solved
- After a flag day the “mnt-by:” attribute MUST be present when objects are changed
  - Our customers may have to update their processes
- At request of PI space “mnt-domain:” attribute can be added immediately

Draft Policy

- In order for the above to work we propose changes to the reverse allocation policy
- Delegation to ‘3rd party’ maintainer that may not be an LIR
  - Currently one needs to be a LIR to be able to request for delegation
- The inconsistency in the policy is removed
  - The requirement for a valid assignment in a /24 is dropped
  - It never existed for a /16
  - Positive result: Reverse DNS is not a bottleneck when provisioning your networks

Questions???

- Slides will be available from

  http://www.ripe.net/ripe/meetings/ripe-47/presentations/

- Questions and feedback on the dns-wg@ripe.net list.