draft-hollenbeck-regext-epp-delete-bcp

Best Practices for Deletion of Domain and Host Objects in the Extensible Provisioning Protocol (EPP)

Goals

- Explain the recommendations of RFCs 5731 and 5732 regarding host and domain object deletion
- Prescribe better/best practices for object deletion to reduce the risk of DNS resolution failure and to ensure data consistency
- Describe potential improvements for community consideration

Problem

- RFCs 5731 and 5732 state that domains SHOULD NOT be deleted if they are associated with subordinate host objects (e.g., deleteme.example and ns1.deleteme.example) and that host objects SHOULD NOT be deleted if they are associated with dependent domain objects (e.g., dependent.example with NS record ns1.deleteme.example).
- If deleteme.example and dependent.example have different sponsoring registrars, then deleteme.example's registrar cannot update dependent.example to disassociate it.
- In order to delete deleteme.example, its sponsoring registrar will typically rename ns1.deleteme.example to an external "sacrificial nameserver" to maintain consistency among objects managed by the registry. Renaming to presumed non-existent hosts has created domain hijacking vulnerabilities (e.g., if dependent.example's NS record becomes does-not-exist.example.com, then a malicious actor may register example.com and hijack dependent.com).

Host Object Renaming and Deleting

Practices to Avoid

- Renaming hosts to presumed non-existent external hosts
- Renaming hosts to non-DNS identifiers (e.g., .alt)
- Renaming hosts to non-authoritative services
- Renaming hosts to special names used for other purposes (e.g., as112.arpa)

Better/Best Practices

- Rename to a sacrificial name server host object maintained by a client (registrar)

  Potential Improvements
  - Create a community sacrificial name server service
  - Develop a convention for a sacrificial name server, e.g., sacrificial.invalid
- Allow deletion of host objects with dependent domains

  Potential Improvements
  - Protect consistency between registrars and registry by providing additional information to deleting registrars, requiring explicit deletion of hosts by registrars, and informing affected registrars.