Network Working Group
Internet-Draft
Expires: March 29, 2014

M. Andrews
ISC

September 25, 2013

Updating Parent Zones
draft-andrews-dnsop-update-parent-zones-00

Abstract

DNS UPDATE was developed to allow DNS zones to be updated.

There is a perception that UPDATE can not be used in conjuction with the Registry, Registar, Registrant (RRR) model to update a zone.

This document explains how UPDATE can be used in the RRR model.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 29, 2014.

Table of Contents

1. Introduction

UPDATE [RFC2136]is designed to update any zone in the DNS. This includes updating delegating NS records, glue address records and DS record.

While UPDATE is primarly designed to UPDATE a zone directly there in no reason why UPDATE requests cannot be translated to the EPP requests to perform the changes.

This would provide a uniform model to update parent zone regardless of where they are in the DNS heirachy.

2. Translation

The Registrar would host a server that authenticates UPDATE requests received directly or relayed by the Registry using TSIG [RFC2845], then translate the actions in the UPDATE request into EPP transaction requests. The results of those EPP transactions would be relayed to the UPDATE client.

Requests that are not TSIG signed are rejected.

The translating server would handle a restricted subset of UPDATE requests, possibly ignoring the prerequiste section. UPDATE requests would be limited to those supported by EPP.

e.g. Add NS record. Delete all NS records. Add A record. Delete AAAA record. Add DS record. Delete DS record.

The translating server may also override/ignore the TTL in the UPDATE request.

3. Authentication

Authentication would be done using TSIG. TSIG was designed to be uses in a environment where requests are relayed.

Authentication can be done down to the <NAME,TYPE> tuple. There exist nameservers that already implement access contols down to this level of granuality based on the presented TSIG.

This would allow nameservers to update their own address records as they get renumbered without being able to update anything else.

This would DNSSEC key management software to update DS records

without being able to update anything else.

As Registrars do all the authentication and generate the signed responses there is no need for the Registry to have access to the private material using in TSIG. Registrars already handle shared keys in these numbers with their web interfaces.

4. Direct to Registrar

The hardest part of Direct to Registrar is finding where to send the UPDATE request. This would most probably just be advised to the Registrant.

5. Indirect to Registrar

In the indirect model the Registry would host a UPDATE relay server which would examine the first record of the UPDATE section and relay the request to the Registrar of record for the owner name of that record. The response would be relayed back.

The relay can use either TCP or UDP when forwarding UPDATE requests as TSIG supports changes to the DNS id field when a request/response is relayed.

This is consistent with how tools like nsupdate work out where to send a UPDATE request. They look at the ownername of the first record and use it to discover the containing zone.

6. Security Considerations

The UPDATE requests are all TSIG signed. This is a proven method for securing UPDATE requests in the DNS.

7. Normative References

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

Author's Address

M. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
US

Email: marka@isc.org