Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: May 16, 2014

J. Daley
.nz Registry Services

November 12, 2013

Extending DNS UPDATE for 'whole of zone' operations
draft-daley-updatezones-00

Abstract

This memo describes an extension to the DNS protocol that support the remote provisioning of zones on authoritative servers. This addition is complementary to the existing mechanisms for provisioning zone data using the DNS protocol.

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 May 16, 2014.

Table of Contents

1. Definitions

This memo uses the following DNS server roles in a manner consistent with RFC 2136 [RFC2136]:

Slave An authoritative server that uses AXFR or IXFR to retrieve the zone and is named in the zone's NS RRset.

Master An authoritative server configured to be the source of AXFR or IXFR data for one or more slave servers.

This memo uses the term "catalog of zones" in the spirit of RFC 1035 [RFC1035] to describe the set of zones that a server is authoritative for.

2. Introduction

It is common practice for Internet service providers and domain name registrars to operate DNS servers that are simultaneously authoritative for many zones. In some case a single DNS server may be authoritative for hundreds of thousands of zones. Despite the large number of zones served, the server is unlikely to also be authoritative for a common parent of these zones and so must operate each zone independently.

The DNS protocol supports the provisioning of resource records in zones already being served by an authoritative DNS server using the DNS UPDATE message described in RFC 2136 [RFC2136]. However no similar operation exists to update the list of zones that a server serves.

This memo describes an extension to the DNS UPDATE message that allows it to be used to instruct an authoritative DNS server to start serving or stop serving zones. This extension supports the remote provisioning of zones in the same manner that DNS UPDATE supports the remote provisioning of Resource Records.

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Extending the DNS UPDATE message

RFC 2136 [RFC2136] defines the DNS UPDATE message which enables the remote provisioning of data within existing zones. The operations enabled by RFC 2136 [RFC2136] are now referred to as 'in zone' operations.

This memo extends the definition of the DNS UPDATE message to enable the remote provisioning of zones. The operations enabled by this memo are referred to as 'whole of zone' operations.

Two 'whole of zone' operations are defined in this memo:

1. Adding zones. Instructing the receiving server to add one or more zones to the catalog of authoritative zones that it serves and start serving these zone, either as a master or a slave.

2. Removing zones. Instructing the receiving server to stop serving one or more authoritative zones and remove them from the catalog of zones that it serves.

The operations described in this memo operate on the catalog of zones irrespective of whether or not the server is currently responding to queries for a specific zone as a server may at any point time be actively serving only some of the zones in its catalog for operational reasons.

3.1. 'in zone' vs 'whole of zone' operations

'in zone' operations are distinguished from 'whole of zone' operations by the ZTYPE of the zones in the Zone section of the DNS UPDATE message:

- For 'in zone' operations the ZTYPE of all of the zones in the Zone section MUST be SOA.

- For 'whole of zone' operations the ZTYPE of all of the zones in the Zone section MUST be NS.

It is not possible to have both 'in zone' and 'whole of zone' operations in the same DNS UPDATE message and so the zones in the Zone section MUST NOT have different ZTYPES.

'whole of zone' operations interpret the data in the Prerequisite, Update and Additional sections differently from 'in zone' operations.

3.2. Adding zones

The operation to add new authoritative zones can come in one of two forms:

1. Add a master zone. Instructing the receiving server to add a new zone and serve that zone as a master.

2. Adding slave zones. Instructing the receiving server to add one or more new zones and serve those as a slave.

3.2.1. Adding a master zone

To add a master zone the DNS UPDATE is constructed as follows:

One zone and only one zone MUST be listed in the Zone section. and the ZTYPE of that zone MUST be set to NS.

The Prerequisitie section MUST be empty.

The Update section MUST contain the SOA record for the new zone. The class of the SOA record MUST NOT be ANY.

The Update section MAY contain any other resource records that are to be added to the zone.

The receiving server MUST add the SOA record and any records in the Update section to the zone before serving the zone.

The Additional section MUST be empty.

3.2.2. Adding slave zones

To add slave zones the DNS UPDATE is constructed as follows:

One or more zones MUST be listed in the Zone section. and the ZTYPE of those zone MUST be set to NS.

The Prerequisitie section MUST be empty.

The Update section MUST be empty.

The Additional section MUST contain at least one A or AAAA resource record. All A and AAAA records are used by the receiving server to identify the servers it should contact to pull the zones from.

The Additional section MAY contain a TKEY record that the receiving server should use to authenticate itself when it pulls the zones.

The resource records in the Additional section MUST NOT be added to the zones.

3.3. Removing zones

To remove zones the DNS UPDATE is constructed as follows:

One or more zones MUST be listed in the Zone section. and the ZTYPE of those zones MUST be set to NS.

The Prerequisitie section MUST be empty.

The Update section MUST contain a SOA record for the zone to be deleted and the class of the SOA record MUST be ANY. This use of a class of ANY to signal the removal of a zone matches the way that a resource record that is to be deleted is identified in RFC 2136 [RFC2136]

The Additional section MUST be empty.

3.4. Response

The response sent to acknowledge receipt and processing of a 'whole of zone' operation is the same as specified for an 'in zone' operation in RFC 2136 [RFC2136] with the addition of the following specific error conditions:

1. When adding zones, If any of the zones listed are already in the catalog of authoritative zones served by the receiving server, whether or not it is currently being served, then the server MUST

ignore the entire request and return an error response with RCode=YXDOMAIN.

2. When adding zones if both the Update and Additional sections are empty then the receiving server MUST ignore the entire request and return an error response with RCode=FORMERROR.

3. When adding zones if both the Update and Additional sections contain data then the receiving server MUST ignore the entire request and return an error response with RCode=FORMERROR.

4. When adding a master zone, if initial zone data is provided and the domains names of those resource records are not within the zone being added (i.e. they are 'out of bailiwick') then the receiving server SHOULD ignore the entire operation and return an error response with RCode=FORMERROR.

5. When removing zones, if any of the zones listed are not in the catalog of zones served by the receiving server then it MUST ignore the entire request and return an error response with RCode=NXDOMAIN.

4. Processing 'whole of zone' operations

4.1. Dynamic serving

It is recognised that not all authoritative nameservers are capable of dynamically loading new zones to serve or dynamically ceasing to serve zones. It is left to the implementor to decide whether to load /unload the zones dynamically; wait for a server restart or to initiate a restart itself.

4.2. Atomicity

This memo does not change the requirements for serialisation of UPDATE operations the depend on each other, as specified in section 3.7 of RFC 2136 [RFC2136], which apply equally to 'whole of zone' operations as they do to 'in zone' operations.

4.3. Provisioning order

A server receiving a 'whole of zone' operation SHOULD NOT assume any particular order to the provisioning of zones and reject the operation as a result. Examples of erroneous rejections include:

1. When adding slave zones, rejecting the operation if the master servers specified are unreachable or do not serve the required zone.

2. When adding or removing zones, rejecting the operation if it would leave an incorrect or inconsistent set of nameservers for that zone specified in that zone or in the parent delegation.

5. Acknowledgements

The author thanks Mark Andrews for his input.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

Clearly unrestricted access to 'whole of zone' operations is a significant threat and misuse would be likely to cause considerable issues. It is therefore RECOMMENDED that:

- DNS UPDATE messages that contain 'whole of zone' operations are protected by TSIG and implementors allow adminstrators to require this protection.

- Implementors do not enable processing of 'whole of zone' operations by default.

The provision of a TKEY record is a significant vulnerability if the DNS UPDATE message containing it is transmitted in clear over the wire. It is therefore RECOMMENDED that such messages are encrypted.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

8.2. Informative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

Author's Address

Jay Daley
.nz Registry Services
PO Box 24361, Manners Street
Wellington 6142
New Zealand

Phone: +64 4 931 6970
Email: jay@nzrs.net.nz