Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: February 14, 2014

J. Daley, Ed.
.nz Registry Services

August 13, 2013

DNS SERVEZONES message
draft-daley-servezones-00

Abstract

This memo describes an addition 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 February 14, 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.

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 the SERVEZONES message that instructs an authoritative DNS server to start serving or stop serving zones.

This message 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. The SERVEZONES message

When a DNS server or provisioning system chooses to instruct an authoritative DNS server to start serving or stop serving one or more zones then it does so by sending a SERVEZONES message. SERVEZONES uses the DNS message format, although it uses only a subset of the available fields.

SERVEZONES is similar to NOTIFY in that it has a request message with the header QR=0 and a response message with QR=1. The response message contains no useful information, but its reception is an indication that the server has received the SERVEZONES message.

SERVEZONES is similar to UPDATE in that the contents of the QTYPE field are used to differentiate between a request to start serving a specified zone or to stop serving a specified zone.

The SERVEZONES message is signalled by Opcode=6.

Except where specified, all DNS header fields are set as for a normal DNS query or response.

3.1. SERVEZONES request

A SERVEZONES request contains one or more zones included as a QNAME in the QUERY section of the SERVEZONES message.

A single SERVEZONES request can instruct the receiving server to both start serving one or more zones and to stop serving one or more zones.

Each zone for which serving is to start is included as a QNAME in the QUERY section with the QTYPE set to SOA.

Each zone for which serving is to stop is included as a QNAME in the QUERY section with the QTYPE set to ANY.

For all SERVEZONES requests:

- The QCLASS for each entry in the QUERY section is set as required
- QDCOUNT is set to the number of zones in the QUERY section.
- ANCOUNT is set to zero (0).

3.1.1. Specifying master servers

If the server receiving the message is intended to act as a slave server then the AUTHORITY section MAY include a list of master servers. NSCOUNT is set to the number of master servers listed in the AUTHORITY section.

If a list of master servers is provided then it applies to all the zones listed in the SERVEZONES message for whom serving is to start (QTYPE is set to SOA).

The receiving server MUST fetch the zone data from one of the listed master servers before serving the zone.

3.1.2. Specifying initial zone data

If the server receiving the message is intended to act as a master then the ADDITIONAL section MUST include the initial zone data. ARCOUNT is set to the number of entries in the ADDITIONAL section.

If initial zone data is included in the ADDITIONAL section then it applies to all the zones listed in the SERVEZONES message for whom serving is to start (QTYPE is set to SOA). If multiple zones are listed then the initial zone data MUST NOT contain any fully qualified domain names (FQDNs).

The receiving server MUST add the initial zone data before serving the zone.

3.2. SERVEZONES response

A SERVEZONES response is sent to acknowledge receipt of the SERVEZONES request to the same source that sent the original request.

QDCOUNT, ANCOUNT, NSCOUNT and ARCOUNT are all set to zero (0).

If the SERVEZONES request is processed correctly then the receiving server SHOULD respond with a SERVEZONES response with RCode=NOERROR.

The following specific error conditions apply:

1. If any of the zones listed in the request to start serving are already being served by the receiving server then it MUST ignore the entire request and return an error response with RCode=YXDOMAIN.

2. If any zones are listed in the request to start serving and neither the AUTHORITY or ADDITIONAL sections appear in the request then the receiving server MUST ignore the entire request and return an error response with RCode=FORMERROR.

3. If any zones are listed in the request to start serving and both the AUTHORITY and ADDITIONAL sections contain data then the receiving server MUST ignore the entire request and return an error response with RCode=FORMERROR.

4. If FQDNs are included in the initial zone data and the SERVEZONES message lists multiple zones to start serving then the receiving server SHOULD return an error response with RCode=FORMERROR.

5. If any of the zones listed in the request to stop serving are not being served by the receiving server then it MUST ignore the entire request and return an error response with RCode=NXDOMAIN.

4. Processing the SERVEZONES messages

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.

5. Acknowledgements

The author thanks Sebastian Castro for his input and review.

6. IANA Considerations

This memo requests that IANA assigns the following values in the DNS Opcode registry:

Opcode	Mnemonic
6	SERVEZONES

7. Security Considerations

Clearly the SERVEZONES message has the potential to be misused and such misuse would be likely to cause considerable issues. It is therefore RECOMMENDED that:

- SERVEZONES messages are always protected by TSIG and implementors allow adminstrators to require this protection.

- Implementors do not enable processing of SERVEZONES messages by default.

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.

8.2. Informative References

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

Author's Address

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

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