IXFR-ONLY to Prevent IXFR Fallback to AXFR
draft-kerr-ixfr-only-01

Abstract

This document proposes a new QTYPE (Query pseudo RRtype) for the Domain Name System (DNS). IXFR-ONLY is a variant of IXFR (RFC 1995) that allows an authoritative server to incrementally update zone content from another (primary) server without falling back from IXFR to AXFR. This way, alternate peers can be contacted more quickly and convergence of zone content may be achieved much faster in important, resilient operational scenarios.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 30, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Introduction ............................................. 3
   1.1. Requirements Language ................................. 3
2. IXFR Server Side ......................................... 4
3. IXFR Client Side .......................................... 4
4. Applicability of IXFR-ONLY ................................. 5
5. IANA Considerations ...................................... 5
6. Security Considerations ................................... 5
7. Normative References ..................................... 5
   Authors’ Addresses ....................................... 6
1. Introduction

For large DNS zones, RFC 1995 [RFC1995] defines Incremental Zone Transfer (IXFR), which allows only to transfer the changed portion(s) of a zone.

In the document, an IXFR client and an IXFR server is defined as in RFC 1995 [RFC1995], a secondary name server which requests IXFR is called an IXFR client and a primary or secondary name server which responds to the request is called an IXFR server.

IXFR is an efficient way to transfer changes in zones from IXFR servers to IXFR clients. However, when an IXFR client has multiple IXFR servers for a single zone, it is possible that not all IXFR servers have the zone with same serial number for that zone. In this case, if an IXFR client attempts an IXFR from an IXFR server which does not have zone with the serial number used by the IXFR client, the IXFR server will fall back to a full zone transfer (AXFR) when it has a version of the zone with serial number greater than the serial requested by the IXFR client.

For example, IXFR server NS1 may have serial numbers 1, 2, and 3 for a zone, and IXFR server NS2 may have serial numbers 1 and 3 for the same zone. An IXFR client that has the zone with serial number 2 which sends an IXFR request to IXFR server NS2 will get a full zone transfer (AXFR) of the zone at serial number 3. This is because NS2 does not know the zone with serial number 2, and therefore does not know what the differences are between zone with serial number 2 and 3.

If the IXFR client in this example had known to send the query to IXFR server NS1, then it could have gotten an incremental transfer (IXFR). But IXFR clients can only know what the latest version of the zone is at a IXFR server (this information is available via an SOA query).

The IXFR-ONLY query type provides a way for the IXFR client to ask each IXFR server to return an error instead of sending the current version of the zone via full zone transfer (AXFR). By using this, a IXFR client can check each IXFR server until it finds one able to provide IXFR.

1.1. 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].
2. IXFR Server Side

A IXFR server receiving a DNS message requesting IXFR-ONLY will reply as described in RFC 1995 [RFC1995] if it is able to produce an IXFR for the serial number requested.

If the IXFR server is is not able to reply with an IXFR it MUST NOT reply with an AXFR unless AXFR result is smaller than IXFR result. Instead, it MUST reply with RCODE CannotIXFR. (!FIXME)

If the IXFR result is larger than an AXFR, then an IXFR server MAY reply with an AXFR result instead. This is an optimization, and IXFR servers MAY only reply with AXFR if they are certain that the reply using AXFR is smaller than an equivalent IXFR reply.

3. IXFR Client Side

An IXFR client who wishes to use IXFR-ONLY will send a message to one of the IXFR servers. The format is exactly the same as for IXFR, except the IXFR-ONLY QTYPE code is used instead of the IXFR QTYPE code.

If the IXFR server replies with IXFR, then the IXFR client is done.

If the IXFR server replies with an RCODE of CannotIXFR, then the IXFR client proceeds on to a different IXFR server. In this case the IXFR server implements IXFR-ONLY, but does not have information about zone with the serial number requested.

If the IXFR server replies with any RCODE other than CannotIXFR or NoError, then the IXFR client proceeds on to a different IXFR server. In this case the IXFR server does not implement IXFR-ONLY.

If the IXFR client attempts IXFR-ONLY to each IXFR server and none of them reply with an incremental transfer (IXFR), then it should attempt an IXFR as described in RFC 1995 [RFC1995] to each of the IXFR servers which replied with an RCODE other than CannotIXFR or NoError.

The method described above allows IXFR clients to operate normally in situations where some of the IXFR servers do support IXFR-ONLY, and some who do not. IXFR clients MAY remember which IXFR servers support IXFR-ONLY and query those IXFR servers first. However since IXFR servers may change software or even run a mix of software, IXFR clients MUST attempt to query each IXFR server periodically when they attempt to get new versions of a zone.
Implementations MAY allow IXFR clients to disable IXFR-ONLY for a given IXFR server, if this is known in advance. These IXFR servers are treated as if they replied with an RCODE other than CannotIXFR or NoError, although no query with IXFR-ONLY is actually sent.

4. Applicability of IXFR-ONLY

Implementations SHOULD allow IXFR clients to disable IXFR-ONLY completely.

Implementations MAY allow IXFR clients to disable IXFR-ONLY for a specific zone. This may be useful for small zones, where fallback to AXFR is cheap, or in other cases where IXFR-ONLY is causing problems.

Usage of IXFR-ONLY may cause IXFR clients to prefer particular IXFR servers, by shifting load to ones that support IXFR-ONLY. If this a problem, then administrators can disable IXFR-ONLY in implementations that allow it.

If a IXFR client has a single IXFR server for a zone, it SHOULD use IXFR rather than IXFR-ONLY.

5. IANA Considerations

IANA allocates the new IXFR-ONLY QTYPE, which means "incremental transfer only". IANA allocates the CannotIXFR RCODE, which means "Server cannot provide IXFR for zone".

6. Security Considerations

IXFR-ONLY may be used by someone to get information about the state of IXFR servers by providing a quick and efficient way to check which versions of a zone each IXFR server supports. Zones should be secured via TSIG [RFC2845] to prevent unauthorized information exposure. However, even administrators of IXFR servers may not want this information given to IXFR clients, in which case they will need to disable IXFR-ONLY.

7. Normative References


[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate


Authors' Addresses

Ondrej Sury
CZ.NIC
Americka 23
120 00 Praha 2
CZ

Phone: +420 222 745 110
Email: ondrej.sury@nic.cz

Shane Kerr (editor)
ISC
Bennebrokstraat 17-I
1015 PE Amsterdam
NL

Phone: +31 64 6336297
Email: shane@isc.org