DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 15, 2020

P. Lexis
PowerDNS
L. Lhotka
P. Spacek
CZ.NIC
O. Sury
Internet Systems Consortium
W. Toorop
NLnet Labs

April 13, 2020

A Data Model for configuring Domain Name System (DNS) Zone Provisioning on Authoritative Nameservers

draft-toorop-dnsop-dns-zone-provisioning-yang-01

Abstract

This document describes a data model for configuring DNS Zone provisioning on authoritative nameservers. This data model only includes definitions for configuration of primary and secondary relationships.

The purpose of this document is to enumerate the properties involved in managing zone provisioning, for usage in managing zone provisioning methods, such as catalog zones or NETCONF.

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 https://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 October 15, 2020.

Table of Contents

1. Introduction

This document describes a data model for configuring DNS Zone provisioning on authoritative nameservers. The model consists of a list of DNS Zones. Besides the name of the zone, each zone MAY contain properties for provisioning of those zones on primary and secondary nameservers.

1.1. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "*NOT RECOMMENDED*", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Properties for primary nameservers

The optional properties for primary nameservers are:

- "notify-to"

  Which value consists of an IP address (with optional port-number) of the secondary nameserver to notify about changes to the zone, and an optional TSIG key (See [RFC2845]) with which the NOTIFY message [RFC1996] - which is used to send the notification - is signed.

  If no port-number is given, port 53 is assumed.

- "allow-transfer"

  Which value consist of a subnet in which the IP address of the secondary nameserver requesting a transfer has to fall, with an optional TSIG key with which the transfer request (either AXFR AXFR [RFC5936] or IXFR [RFC1995]) has to be signed and which will be used to sign the messages that will convey the complete or partial DNS Zone.

1.3. Properties for primary nameservers

The optional properties for secondary nameservers are:

- "allow-notify"

  Which value consist of a subnet in which the IP address of the primary nameserver which is signaling that the DNS Zone has changed must fall, and an optional TSIG with which the NOTIFY message use MUST be signed.

- "transfer-from"

  Which value consists of an IP address (with optional port-number) of the primary nameserver from which to transfer the complete or partial DNS Zone, with an optional TSIG which MUST be used to send the AXFR or IXFR request and with which the transferred Zone data MUST be verified.

  If no port-number is given, port 53 is assumed.

2. Tree Structure

This document defined the YANG module "ietf-dns-zone-provisioning", which has the following tree structure.

```
module: ietf-dns-zone-provisioning
  +--rw tsig-keys
  |  +--rw tsig-key* [name]
  |     +--rw name         inet:domain-name
  |     +--rw algorithm    inet:domain-name
  |     +--rw secret       string
  +--rw zones
     +--rw zone* [name]
        +--rw name              inet:domain-name
        +--rw allow-notify* [subnet]
        |  +--rw subnet      inet:ip-prefix
        |  +--rw tsig-key?   -> /tsig-keys/tsig-key/name
        +--rw allow-transfer* [subnet]
        |  +--rw subnet      inet:ip-prefix
        |  +--rw tsig-key?   -> /tsig-keys/tsig-key/name
        +--rw notify-to* [ip port]
        |  +--rw ip          inet:ip-address
        |  +--rw port        inet:port-number
        |  +--rw tsig-key?   -> /tsig-keys/tsig-key/name
        +--rw transfer-from* [ip port]
           +--rw ip          inet:ip-address
           +--rw port        inet:port-number
           +--rw tsig-key?   -> /tsig-keys/tsig-key/name
```

3. YANG Module

<CODE BEGINS> file "ietf-dns-zone-provisioning@2020-04-13.yang"

```
module ietf-dns-zone-provisioning {

  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang"
    + ":ietf-dns-zone-provisioning";

  prefix dnszp;

  import ietf-inet-types {
    prefix inet;
  }

  organization
    "IETF Domain Name System Operations Working Group (dnsop)";
```

```
     contact
       "WG Web:   <https://datatracker.ietf.org/wg/dnsop/>
        WG List:  <mailto:dnsop@ietf.org>

        Editor:   Willem Toorop
                  <mailto:willem@nlnetlabs.nl>";

     description
       "This YANG module defines a model for configuring DNS Zone
        provisioning on authoritative nameservers.

        Copyright (c) 2020 IETF Trust and the persons identified as
        authors of the code. All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject to
        the license terms contained in, the Simplified BSD License set
        forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (https://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC ????; see the
        RFC itself for full legal notices.";

     revision 2020-03-09 {
       description
         "Initial revision.";
       reference
         "RFC XXXX: A YANG Data Model for"
           + " DNS Zone provisioning configuration";
     }

     /* Groupings */

     grouping tsig-key {
       leaf name {
         type inet:domain-name;
         mandatory true;
         description
           "The name of the key";
       }
       leaf algorithm {
         type inet:domain-name;
         mandatory true;
         description
           "Name of the algorithm";
         reference
           "<https://www.iana.org/assignments"
```

```
            + "/tsig-algorithm-names/tsig-algorithm-names.xhtml>";
      }
      leaf secret {
        type string;
        mandatory true;
        description
          "Shared secret in base64 format. Possible lengths are
           dependent on the algorithm";
      }
      description
        "Shared key used for authenticating transactions with
         authoritative name servers";
      reference
        "RFC2845: Secret Key Transaction Authentication for DNS
         (TSIG)";
    }
    grouping acl-net-key {
      leaf subnet {
        type inet:ip-prefix;
        mandatory true;
        description
          "Contacting IP address must match this subnet.";
      }
      leaf tsig-key {
        type leafref {
          path "/tsig-keys/tsig-key/name";
        }
        description
          "When provided all interactions to and from the
           contacting remote end must use this tsig-key.";
      }
      description
        "Access control allowing the action from IP addresses from the
         given subnet and tsig-key if present. Without tsig-key only
         the subnet needs to match. The subnet should be 0.0.0.0/0 or
         ::/0 to allow access from all IPv4 or all IPv6 addresses";
    }

    grouping addr-key {
      leaf ip {
        type inet:ip-address;
        mandatory true;
        description
          "IP address to contact.";
      }
      leaf port {
        type inet:port-number;
        default 53;
```

```
        description
          "Port to conact.";
      }
      leaf tsig-key {
        type leafref {
          path "/tsig-keys/tsig-key/name";
        }
        description
          "When provided all interactions with to and from the
           contacted remote end must use this tsig-key.";
      }
      description
        "IP address of remote party to contact, either to notify about
         updates in the zone, or to fetch the zone from. An optional
         tsig-key can be given to validate the transfer or to sign the
         notify.";
    }

    container tsig-keys {
      list tsig-key {
        key "name";
        uses tsig-key;
        description
          "The tsig-key which is referred to from acl-net-key
           and/or addr-key.";
      }
      description
        "The list of tsig-keys which are referred from
         acl-net-key and addr-key.";
    }

    container zones {
      list zone {
        key "name";
        leaf name {
          type inet:domain-name;
          description
            "The name of the DNS Zone";
        }
        list allow-notify {
          key "subnet";
          uses acl-net-key;
          description
            "Secondary servers allow notifies for DNS Zone updates
             from IP addresses from this subnet. If a tsig-key is
             given, the notify must be signed with that key.";
        }
        list allow-transfer {
```

```
          key "subnet";
          uses acl-net-key;
          description
            "Primary servers allow transfers to the IP addresses
             to the given subnet. If a tsig-key is given, the transfer
             request must be signed and the DNS messages used for the
             transfer will also be signed with that tsig-key";
        }
        list notify-to {
          key "ip port";
          uses "addr-key";
          description
            "Primary servers send NOTIFY messages when the Zonne
             has been updated to this IP. If a tsig-key is given,
             it will be signed with that key.";
        }
        list transfer-from {
          key "ip port";
          uses "addr-key";
          description
            "Secondary servers contact the given ip-address to
             acquire DNS Zone content. When a tsig-key is given
             the request will be signed with it, and the DNS
             messages conveying the Zone must be signed with
             that tsig-key.";
        }
        description
          "A DNS Zone with properties which describe the provisioning
           relationships within for authoritative nameserver.";
      }
      description
        "The list of DNS Zones for which the properties are defined
         that describe the primary/secondary relationships.";
    }
  }
  <CODE ENDS>
```

4. IANA Considerations

This document registers the following namespace URI in the "ns" subregistry of the "IETF XML Registry" [RFC3688]:

- URI: urn:ietf:params:xml:ns:yang:ietf-restconf-subscribed-notifications

- Registrant Contact: The IESG.

- XML: N/A; the requested URI is an XML namespace.

This document registers the following YANG module in the "YANG Module Names" registry [RFC6020]:

- Name: ietf-restconf-subscribed-notifications
- Namespace: urn:ietf:params:xml:ns:yang:ietf-dns-zone-provisioning
- Prefix: dnszp
- Reference: RFCXXXX

5. Security considerations

Instances of the data model defined in this document contain sensitive information with which eavesdroppers can interfere in DNS Zone provisioning and potentially even alter DNS Zone content. Care must be taken that instances of this data model are only conveyed over secure authenticated and encrypted channels.

6. Acknowledgements

Thanks to

7. Normative References

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, DOI 10.17487/RFC1995, August 1996, <https://www.rfc-editor.org/info/rfc1995>.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/info/rfc1996>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000, <https://www.rfc-editor.org/info/rfc2845>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/info/rfc5936>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Pieter Lexis
PowerDNS
Den Haag
Netherlands

Email: pieter.lexis@powerdns.com

Ladislav Lhotka
CZ.NIC
CZ

Email: lhotka@nic.cz

Petr Spacek
CZ.NIC
CZ

Email: petr.spacek@nic.cz

Ondrej Sury
Internet Systems Consortium
CZ

Email: ondrej@isc.org

Willem Toorop
NLnet Labs
Science Park 400
Amsterdam 1098 XH
Netherlands

Email: willem@nlnetlabs.nl