Workgroup:
Registration Protocols Extensions (regext)
Internet-Draft: draft-regext-brown-epp-ttl-04
Published: 22 February 2023
Intended Status: Standards Track
Expires: 26 August 2023
Authors: G. Brown
CentralNic Group plc

Extensible Provisioning Protocol (EPP) mapping for DNS Time-To-Live (TTL) values

Abstract

This document describes an extension to the Extensible Provisioning Protocol (EPP) that allows EPP clients to manage the Time-To-Live (TTL) value for domain name delegation records.

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 26 August 2023.

Table of Contents

1. Introduction

The principal output of any domain name provisioning system is a DNS zone file, which contains the delegation record(s) for names registered within a zone (such as a top-level domain). These records include, at minimum, one or more NS records, but may also include A and/or AAAA glue records, DS records, and DNAME records for IDN variants ([RFC6927]).

Typically, the Time-To-Live value (TTL, see Section 5 of [RFC8499]) of these records is determined by the registry operator. However, in some circumstances it may be desirable to allow the sponsoring client of a domain name to change the TTL used for that domain: for example, to reduce the amount of time required to complete a change of DNS servers, DNSSEC deployment or key rollover, or to allow for fast rollback of such changes.

This document describes an EPP extension to the domain name and host object mappings (described in [RFC5731] and [RFC5732], respectively)

which allows the sponsor of a domain name or host object to change the TTL associated with that object.

1.1. Conventions used in this document

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 [RFC2119].

In examples, "C:" represents lines sent by a protocol client and "S:" represents lines returned by a protocol server. Indentation and white space in examples are provided only to illustrate element relationships and are not REQUIRED features of this protocol.

A protocol client that is authorized to manage an existing object is described as a "sponsoring" client throughout this document.

XML is case sensitive. Unless stated otherwise, XML specifications and examples provided in this document **MUST** be interpreted in the character case presented in order to develop a conforming implementation.

EPP uses XML namespaces to provide an extensible object management framework and to identify schemas required for XML instance parsing and validation. These namespaces and schema definitions are used to identify both the base protocol schema and the schemas for managed objects.

The XML namespace prefixes used in examples (such as the string ttl in ttl:secs) are solely for illustrative purposes. A conforming implementation **MUST NOT** require the use of these or any other specific namespace prefixes.

2. Extension elements

This specification defines a new element, <ttl:secs>, that is included in <info> responses, and <create> and <update> commands.

The <ttl:secs> element takes two forms: the first contains a 32-bit unsigned integer indicating the TTL (expressed in seconds) which will be applied to the DNS records for the associated domain name or host object.

Example:

```
<ttl:secs>3600</secs>
```

The second form, which contains no content, indicates that (a) in <info> responses, no specific value has been set for the object, or (b) in <create> and <update> commands, that the client wishes to

remove a previously set value, in favour of the default value. Note that this does no mean that no TTL is published in DNS records (since this is not possible), rather, that the server-determined default TTL is (or should be) used for that object.

Example:

```
<ttl:secs/>
```

3. EPP command mapping

3.1. EPP query commands

3.1.1. EPP <info> command

This extension defines an additional element for EPP <info> responses for domain and host objects.

The <info> response MAY contain an <extension> element, which MAY contain a <ttl:infData> element. This element contains a single <ttl:secs> element.

Example domain <info> response:

```
S: <?xml version="1.0" encoding="utf-8" standalone="no"?>
S: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
S:   <response>
S:     <result code="1000">
S:       <msg>Command completed successfully</msg>
S:     </result>
S:     <resData>
S:       <domain:infData
S:         xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
S:         <domain:name>example.com</domain:name>
S:         <domain:roid>EXAMPLE1-REP</domain:roid>
S:         <domain:status s="ok" />
S:         <domain:registrant>jd1234</domain:registrant>
S:         <domain:contact type="admin">sh8013</domain:contact>
S:         <domain:contact type="tech">sh8013</domain:contact>
S:         <domain:ns>
S:           <domain:hostObj>ns1.example.com</domain:hostObj>
S:           <domain:hostObj>ns1.example.net</domain:hostObj>
S:         </domain:ns>
S:         <domain:clID>ClientX</domain:clID>
S:         <domain:crID>ClientY</domain:crID>
S:         <domain:crDate>1999-04-03T22:00:00.0Z</domain:crDate>
S:         <domain:upID>ClientX</domain:upID>
S:         <domain:upDate>1999-12-03T09:00:00.0Z</domain:upDate>
S:         <domain:exDate>2005-04-03T22:00:00.0Z</domain:exDate>
S:         <domain:trDate>2000-04-08T09:00:00.0Z</domain:trDate>
S:         <domain:authInfo>
S:           <domain:pw>2fooBAR</domain:pw>
S:         </domain:authInfo>
S:       </domain:infData>
S:     </resData>
S:     <extension>
S:       <ttl:infData
S:         xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
S:         <ttl:secs>3600</ttl:secs>
S:       </ttl:infData>
S:     </extension>
S:     <trID>
S:       <clTRID>ABC-12345</clTRID>
S:       <svTRID>54322-XYZ</svTRID>
S:     </trID>
S:   </response>
S: </epp>
```

Example host <info> response:

```
S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
S:   <response>
S:     <result code="1000">
S:       <msg>Command completed successfully</msg>
S:     </result>
S:     <resData>
S:       <host:infData
S:        xmlns:host="urn:ietf:params:xml:ns:host-1.0">
S:         <host:name>ns1.example.com</host:name>
S:         <host:roid>NS1_EXAMPLE1-REP</host:roid>
S:         <host:status s="linked"/>
S:         <host:status s="clientUpdateProhibited"/>
S:         <host:addr ip="v4">192.0.2.2</host:addr>
S:         <host:addr ip="v4">192.0.2.29</host:addr>
S:         <host:addr ip="v6">1080::8:800:200C:417A</host:addr>
S:         <host:clID>ClientY</host:clID>
S:         <host:crID>ClientX</host:crID>
S:         <host:crDate>1999-04-03T22:00:00.0Z</host:crDate>
S:         <host:upID>ClientX</host:upID>
S:         <host:upDate>1999-12-03T09:00:00.0Z</host:upDate>
S:         <host:trDate>2000-04-08T09:00:00.0Z</host:trDate>
S:       </host:infData>
S:     </resData>
S:      <extension>
S:        <ttl:infData
S:          xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
S:          <ttl:secs>3600</ttl:secs>
S:        </ttl:infData>
S:      </extension>
S:     <trID>
S:       <clTRID>ABC-12345</clTRID>
S:       <svTRID>54322-XYZ</svTRID>
S:     </trID>
S:   </response>
S: </epp>
```

3.2. EPP transform commands

3.2.1. EPP <create> command

This extension defines an additional element for EPP <create> commands for domain and host objects.

The <create> command MAY contain an <extension> element which MAY contain a <ttl:create> element. This element contains a single <ttl:secs> element.

Example domain <create> command:

```
C: <?xml version="1.0" encoding="UTF-8" standalone="no"?>
C: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:   <command>
C:     <create>
C:       <domain:create
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:         <domain:name>example.com</domain:name>
C:         <domain:period unit="y">2</domain:period>
C:         <domain:ns>
C:           <domain:hostObj>ns1.example.net</domain:hostObj>
C:           <domain:hostObj>ns2.example.net</domain:hostObj>
C:         </domain:ns>
C:         <domain:registrant>jd1234</domain:registrant>
C:         <domain:contact type="admin">sh8013</domain:contact>
C:         <domain:contact type="tech">sh8013</domain:contact>
C:         <domain:authInfo>
C:           <domain:pw>2fooBAR</domain:pw>
C:         </domain:authInfo>
C:       </domain:create>
C:     </create>
C:     <extension>
C:       <ttl:create
C:         xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
C:         <ttl:secs>3600</ttl:secs>
C:       </ttl:create>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C: </epp>
```

Example host <create> command:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:   <command>
C:     <create>
C:       <host:create
C:        xmlns:host="urn:ietf:params:xml:ns:host-1.0">
C:         <host:name>ns1.example.com</host:name>
C:         <host:addr ip="v4">192.0.2.2</host:addr>
C:         <host:addr ip="v4">192.0.2.29</host:addr>
C:         <host:addr ip="v6">1080::8:800:200C:417A</host:addr>
C:       </host:create>
C:     </create>
C:     <extension>
C:       <ttl:create
C:         xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
C:         <ttl:secs>3600</ttl:secs>
C:       </ttl:create>
C:     </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C: </epp>
```

3.2.2. EPP <update> command

This extension defines an additional element for EPP <update> commands for domain and host objects.

The <update> command MAY contain an <extension> element which MAY contain a <ttl:update> element. This element contains a single <ttl:secs> element.

Example domain <update> command:

```
C: <?xml version="1.0" encoding="UTF-8" standalone="no"?>
C: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C:      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
C:   <command>
C:     <update>
C:       <domain:update
C:        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
C:         <domain:name>example.com</domain:name>
C:       </domain:update>
C:     </update>
C:     <extension>
C:        <ttl:update>
C:          xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
C:          <ttl:secs>3600</ttl:secs>
C:        </ttl:update>
C:      </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C: </epp>
```

Example host <update> command:

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C: <epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
C:   <command>
C:     <update>
C:       <host:update
C:        xmlns:host="urn:ietf:params:xml:ns:host-1.0">
C:         <host:name>ns1.example.com</host:name>
C:         <host:add>
C:           <host:addr ip="v4">192.0.2.22</host:addr>
C:           <host:status s="clientUpdateProhibited"/>
C:         </host:add>
C:         <host:rem>
C:           <host:addr ip="v6">1080::8:800:200C:417A</host:addr>
C:         </host:rem>
C:         <host:chg>
C:           <host:name>ns2.example.com</host:name>
C:         </host:chg>
C:       </host:update>
C:     </update>
C:     <extension>
C:        <ttl:update>
C:          xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0">
C:          <ttl:secs>3600</ttl:secs>
C:        </ttl:update>
C:      </extension>
C:     <clTRID>ABC-12345</clTRID>
C:   </command>
C: </epp>
```

4. Server processing of TTL values

If an EPP server receives a command containing a TTL that is outside the server's permitted range (see Operational considerations and Security considerations below), it **MUST** reject the command with a 2004 "Parameter value range error" response.

4.1. Use of TTL values in delegation records

EPP servers which implement this extension **SHOULD** use the values provided by EPP clients for the TTL values of NS and DS records published in the DNS for domain objects, and A and AAAA records published in the DNS for host objects.

4.2. Relationship between host object and domain object TTL values

The extension in this document allows TTL values to be configured for both domain and host objects. In domain name registries, these object types have a hierarchical relationship, in that a host object

may be subordinate to a domain object: for example, the host object ns1.example.com is subordinate to the domain object example.com.

When publishing A and AAAA for host objects, TTL values for host objects **SHOULD** take precedence over the TTL of the superordinate domain object. However, if no TTL value is specified for a subordinate host object, but a TTL value is specified for the superordinate domain object, then the domain object's TTL value **SHOULD** be used for the host object instead of the default TTL value.

4.3. Use of TTL values for IDN variants

If a domain name has variants ([RFC6927]) that are linked to that domain, then any NS or DNAME records published for those variants **SHOULD** use the same TTL as that used for the primary domain.

5. Out-of-band changes to TTL values

EPP server operators **MAY**, in order to address operational or security issues, make changes to TTL values out-of-band (that is, not in response to an <update> command received from the sponsoring client).

Additionally, server operators **MAY** implement an automatic reset of TTL values, so that they may be changed for a finite period before and after a planned change, and then revert to a standard value.

If a TTL value is changed out-of-band, EPP server operators **SHOULD** notify the sponsoring client using the EPP Change Poll extension ([RFC8590]).

6. Operational considerations

6.1. Operational impact of TTL values

Domain registry operators must strike a balance between, on the one hand, the desire of registrants for changes to their domains to be visible in the DNS quickly, and on the other, the increased DNS query traffic that short TTLs can bring. Historically, registry operators have used a global TTL value which was applied to all delegations within their zones, which could then be tuned to an optimum value.

Domain registry operators **SHOULD** implement limits on the maximum and minimum accepted TTL values that are narrower than the values permitted in the XML schema in the Formal specification (which were chosen to allow any TTL permitted in DNS records), in order to prevent scenarios where an excessively high or low TTL causes operational issues on either side of the zone cut.

6.2. When the TTL should be changed

A common operational mistake is changing of DNS record TTLs during or after the planned change to the records themselves. This arises due to a misunderstanding about how TTLs work.

Client implementations of this specification **SHOULD** ensure that the user understands that changes to a TTL are only effective in shortening transition periods if implemented a period of time — at least equal to the current TTL — *before* the planned change.

7. Security considerations

Many malicious actors use a technique called "fast flux DNS" ([SAC-025]) to rapidly change the DNS configuration for a zone in order to evade takedown and law enforcement activity.

Registry operators **SHOULD** take this into consideration when setting the lower limit on TTL values, since a short TTL on delegations has the potential to enhance the effectiveness of fast flux techniques on evasion.

8. IANA considerations

8.1. XML namespace

This document uses URNs to describe XML namespaces and XML schemas conforming to a registry mechanism described in [RFC3688]. The following URI assignment has been made by IANA:

Registration for the TTL namespace:

URI: urn:ietf:params:xml:ns:ttl-1.0

Registrant Contact: See the author of this document

XML: None. Namespace URIs do not represent an XML specification

Registration for the TTL XML schema:

URI: urn:ietf:params:xml:ns:ttl-1.0

Registrant Contact: See the author of this document

XML: See the "Formal specification" section of this document

8.2. EPP extension registry

The EPP extension described in this document has been registered by the IANA in the Extensions for the "Extensible Provisioning Protocol

(EPP)" registry described in [RFC7451]. The details of the registration are as follows:

Name of Extension: Extensible Provisioning Protocol (EPP) Mapping for DNS Time-To-Live (TTL) values

Document Status: Experimental

Reference: URL of this document

Registrant Name and Email Address: See the author of this document

TLDs: Any

IPR Disclosure: None

Status: Active

Notes: None

9. Formal specification

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
  targetNamespace="urn:ietf:params:xml:ns:ttl-1.0"
  xmlns:ttl="urn:ietf:params:xml:ns:ttl-1.0"
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">
  <annotation>
    <documentation>
      Extensible Provisioning Protocol v1.0 extension schema for
      Time-To-Live (TTL) values for domain and host objects.
    </documentation>
  </annotation>

  <element name="create"  type="ttl:seconds"/>
  <element name="update"  type="ttl:seconds"/>
  <element name="infData" type="ttl:seconds"/>

  <complexType name="seconds">
    <choice>
      <element name="secs" type="ttl:nonNegativeInteger"/>
      <element name="secs"/>
    </choice>
  </complexType>

  <simpleType name="nonNegativeInteger">
    <restriction base="nonNegativeInteger">
      <minInclusive value="1"/>
      <maxInclusive value="4294967295"/>
    </restriction>
  </simpleType>

  <complexType name="null">
    <sequence/>
  </complexType>
</schema>
```

10. References

10.1. Normative references

[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>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, DOI 10.17487/RFC5731, August 2009, <https://www.rfc-editor.org/info/rfc5731>.

[RFC5732] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Host Mapping", STD 69, RFC 5732, DOI 10.17487/RFC5732, August 2009, <https://www.rfc-editor.org/info/rfc5732>.

[RFC7451] Hollenbeck, S., "Extension Registry for the Extensible Provisioning Protocol", RFC 7451, DOI 10.17487/RFC7451, February 2015, <https://www.rfc-editor.org/info/rfc7451>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8590] Gould, J. and K. Feher, "Change Poll Extension for the Extensible Provisioning Protocol (EPP)", RFC 8590, DOI 10.17487/RFC8590, May 2019, <https://www.rfc-editor.org/info/rfc8590>.

10.2. Informative references

[RFC6927] Levine, J. and P. Hoffman, "Variants in Second-Level Names Registered in Top-Level Domains", RFC 6927, DOI 10.17487/RFC6927, May 2013, <https://www.rfc-editor.org/info/rfc6927>.

[SAC-025] ICANN Security and Stability Advisory Committee (SSAC), "SSAC Advisory on Fast Flux Hosting and DNS", SAC 25, January 2008, <https://www.icann.org/en/system/files/files/sac-025-en.pdf>.

Author's Address

Gavin Brown
CentralNic Group plc
44 Gutter Lane
London
EC2V 6BR
United Kingdom

Phone: +44 20 33 88 0600
Email: gavin.brown@centralnic.com
URI: https://www.centralnic.com