The ALT Special Use Top Level Domain
draft-wkumari-dnsop-alt-tld-06

Abstract

   This document reserves a string (ALT) to be used as a TLD label in
   non-DNS contexts or for names that have no meaning in a global
   context. It also provides advice and guidance to developers
   developing alternate namespaces.

   [Ed note: This document lives in GitHub at:
   https://github.com/wkumari/draft-wkumari-dnsop-alt-tld . Issues and
   pull requests happily accpeted.]

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 November 19, 2015.

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 Simplified BSD License.

Table of Contents

1. Introduction

Many protocols and systems need to name entities. Names that look
like DNS names (a series of labels separated with dots) have become
common, even in systems that are not part of the global DNS.

This document provides a solution that may be more appropriate than
[RFC6761] in many cases. RFC6761 specifies Special Use TLDs which
should only be used in exceptional circumstances.

This document reserves the label "ALT" (short for "Alternate") as a
Special Use Domain ([RFC6761]). This label is intended to be used as
the final label (apart from the zero-length terminating label) to
signify that the name is not rooted in the DNS, and that normal
registration and lookup rules do not apply.

1.1. Requirements notation

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].

1.2. Terminology

This document assumes familiarity with DNS terms and concepts.
Please see [RFC1034] for background and concepts.

o DNS context: The namespace anchored at the globally-unique DNS
   root. This is the namespace or context that "normal" DNS uses.

o non-DNS context: Any other (alternate) namespace.

o pseudo-TLD: A label that appears in a fully-qualified domain name
   in the position of a TLD, but which is not registered in the
   global DNS.

o TLD: The last visible label in either a fully-qualified domain
   name or a name that is qualified relative to the root. See the
   discussion in Section 2.

2. Background

The DNS data model is based on a tree structure, and has a single
root. Conventionally, a name immediately beneath the root is called
a "Top Level Domain" or "TLD". TLDs usually delegate portions of
their namespace to others, who may then delegate further. The
hierarchical, distributed and caching nature of the DNS has made it
the primary resolution system on the Internet.

Domain names are terminated by a zero-length label, so the root label
is normally invisible. Truly fully-qualified names indicate the root
label explicitly, thus: "an.example.tld.". Most of the time, names
are written implicitly relative to the root, thus: "an.example.tld".
In both of these cases, the TLD is the last label that is visible in
presentation format -- in this example, the string "tld". (This
little bit of pedantry is here because, in different contexts, people
can use the term "fully-qualified domain name" to refer to either of
these uses.) It is worth noting that the root label is present in
the on-wire format of fully-qualified domain names, even if not
displayed in the presentation form.

The success of the DNS makes it a natural starting point for systems
that need to name entities in a non-DNS context, or that have no
unique meaning in a global context. These name resolutions,
therefore, occur in a namespace distinct from the DNS.

In many cases, these systems build a DNS-style tree parallel to the
global DNS administered by IANA. They often use a pseudo-TLD to
cause resolution in the alternate namespace, using browser plugins,

shims in the name resolution process, or simply applications that
perform special handling of this alternate namespace.

In many cases, the creators of these alternate namespaces have chosen
a convenient or descriptive string and started using it. These new
strings are "alternate" strings and are not registered anywhere or
part of the DNS. However they appear to be TLDs. Issues may arise
if they are looked up in the DNS. These include:

o User confusion: If someone emails a link of the form
   foo.bar.pseudo-TLD to someone who does not have the necessary
   software to resolve names in the pseudo-TLD namespace, the name
   will not resolve and the user may become confused.

o Excess traffic hitting the DNS root: Lookups leak out of the
   pseudo-TLD namespace and end up hitting the DNS root nameservers.

o Collisions: If the pseudo-TLD is eventually delegated from the
   root zone the behavior may be non-deterministic.

o Lack of success for the user's original goal.

An alternate name resolution system might be specifically designed to
provide confidentiality of the looked up name, and to provide a
distributed and censorship resistant namespace. This goal would
necessarily be defeated if the queries leak into the DNS, because the
attempt to look up the name would be visible at least to the
operators of root name servers.

3. The ALT namespace

In order to avoid the above issues, we reserve the ALT label. Unless
the name desired is globally unique, has meaning on the global
context and is delegated in the DNS, it should be considered an
alternate namespace, and follow the ALT label scheme outlined below.
The ALT label MAY be used in any domain name as a pseudo-TLD to
signify that this is an alternate (non-DNS) namespace.

Alternate namespaces should differentiate themselves from other
alternate namespaces by choosing a name and using it in the label
position just before the pseudo-TLD (ALT). For example, a group
wishing to create a namespace for Friends Of Olaf might choose the
string "foo" and use any set of labels under foo.alt.

As they are in an alternate namespace, they have no significance in
the regular DNS context and so should not be looked up in the DNS
context. Unfortunately simply saying that "something should not
happen" doesn't actually stop it from happening, so we need some

rules to guide implementors and operators. The ALT TLD is delegated
to "new style" AS112 servers, and so recursive and stub resolvers
will get NXDOMAIN for all queries.

1. Iterative resolvers SHOULD follow the advice in [RFC6303],
    Section 3.

2. The ALT TLD is delegated to "new style" AS112 nameservers
    ([I-D.ietf-dnsop-as112-dname]), which will return NXDOMAIN for
    all queries.

These rules are intended to limit how far unintentional queries (i.e.
those not intended for the global DNS) flow.

Groups wishing to create new alternate namespaces SHOULD create their
alternate namespace under a label that names their namespace, and
under the ALT label. They SHOULD choose a label that they expect to
be unique and, ideally, descriptive.

Currently deployed projects and protocols that are using pseudo-TLDs
may decide to move under the ALT TLD, but this is not a requirement.
Rather, the ALT TLD is being reserved so that future projects of a
similar nature have a designated place to create alternate resolution
namespaces that will not conflict with the regular DNS context.

A number of names other than .ALT were considered and discarded. In
order for this technique to be effective the names need to continue
to follow both the DNS format and conventions (a prime consideration
for alternate name formats is that they can be entered in places that
normally take DNS context names); this rules out using suffixes that
do not follow the usual letter, digit, and hyphen label convention.
Another proposal was that the ALT TLD instead be a reservation under
.arpa. This was considered, but rejected for several reasons,
including:

1. We wished this to make it clear that this is not in the DNS
    context, and .arpa clearly is.

2. The use of the string .ALT is intended to evoke the alt.*
    hierarchy in Usenet.

3. We wanted the string to be short and easily used.

4. A name underneath .arpa would consume at least five additional
    octets of the total 255 octets available in domain names, which
    could put pressure on applications that need long machine-
    generated names.

   5. We are suggesting that the string .ALT get special treatment in
       resolvers, and shim software. We are concerned that using
       subdomains of an existing TLD (like .arpa) might end up with bad
       implementations misconfiguring / overriding the TLD itself and
       breaking .arpa.

   There is a concern that if there were placed under .arpa,
   inexperienced nameserver operators may inadvertently cover .arpa. A
   more significant concern is that the scope of the issue if the query
   does leak, and the fact that this would then make the root of the
   alternate naming namespace a third level domain, and not a second
   one. A project may be willing to have a name of the form
   example.alt, but example.alt.arpa may be not look as good.

[4]. Advice to developers

   Often, a subdomain of an existing, owned domain may suffice. When
   that is so, using a subdomain in the DNS is always preferable, and
   safest in terms of not risking misuse, duplications, or collisions.
   In the rare instance in which it is not desirable to have the name in
   the DNS, the .ALT namespace may be used.

   In a number of cases the purpose of the alternate name resolution
   system is to provide confidentiality. For these systems the above
   advice is problematic. If the query for one of these names (for
   example harry.foo.example.com were to leak into the DNS, the query
   would hit the recursive resolver, and (assuming empty caches) would
   then hit the root, the .com name servers, the example.com name
   servers and then the foo.example.com nameservers. This means that
   the fact that a user is resolving harry.foo.example.com would be
   visible to a large number of people. Furthermore, the
   harry.foo.example.com nameservers become a good oracle to determine
   what names exist, and who is trying to reach them.

   For projects that are very latency sensitive, or that desire to
   provide confidentiality, we recommend anchoring the alternate
   namespace under the .ALT TLD.

[5]. IANA Considerations

   The IANA is requested to add the ALT string to the "Special-Use
   Domain Name" registry ([RFC6761], and reference this document. In
   addition, the "Locally Served DNS Zones" ([RFC6303]) registry should
   be updated to reference this document.

5.1. Domain Name Reservation Considerations

   This section is to satisfy the requirement in Section 5 of RFC6761.

   The domain "alt.", and any names falling within ".alt.", are special
   in the following ways:

   1. Human users are expected to know that strings that end in .alt
       behave differently to normal DNS names. Users are expected to
       have applications running on their machines that intercept stings
       of the form <namespace>.alt and perform special handing of them.
       If the user tries to resolve a name of the form <namespace>.alt
       without the <namespace> plugin installed, the request will leak
       into the DNS, and receive a negative response.

   2. Writers of application software that implement a non-DNS
       namespace are expected to intercept names of the form
       <namespace>.alt and perform application specific handing with
       them. Other applications are not intended to perform any special
       handing.

   3. In general, writers of name resolution APIs and libraries do not
       need to perform special handing of these names. If developers of
       other namespaces implement their namespace through a "shim" or
       library, they will need to intercept and perform their own
       handling.

   4. Caching DNS servers SHOULD recognize these names as special and
       SHOULD NOT, by default, attempt to look up NS records for them,
       or otherwise query authoritative DNS servers in an attempt to
       resolve these names. Instead, caching DNS servers SHOULD
       generate immediate negative responses for all such queries.

   5. Authoritative DNS servers SHOULD recognize these names as special
       and SHOULD, by default, generate immediate negative responses for
       all such queries, unless explicitly configured by the
       administrator to give positive answers for private-address
       reverse-mapping names.

   6. DNS server operators SHOULD be aware that queries for names
       ending in .alt are not DNS names, and were leaked into the DNS
       context (for example, by a missing browser plugin). This
       information may be useful for support or debuggung purposes.

   7. DNS Registries/Registrars MUST NOT grant requests to register
       "alt" names in the normal way to any person or entity. These
       "alt" names are defined by protocol specification to be

nonexistent, and they fall outside the set of names available for allocation by registries/registrars.

6. Security Considerations

One of the motivations for the creation of the alt pseudo-TLD is that unmanaged labels in the managed root name space are subject to unexpected takeover if the manager of the root name space decides to delegate the unmanaged label.

The unmanaged and "registration not required" nature of labels beneath .ALT provides the opportunity for an attacker to re-use the chosen label and thereby possibly compromise applications dependent on the special host name.

7. Acknowledgements

The authors understand that there is much politics surrounding the delegation of a new TLD and thank the ICANN liaison in advance.

We would also like to thank Joe Abley, Mark Andrews, Marc Blanchet, John Bond, Stephane Bortzmeyer, David Cake, David Conrad, Patrik Faltstrom, Olafur Gudmundsson, Paul Hoffman, Joel Jaeggli, Ted Lemon, Edward Lewis, George Michaelson, Ed Pascoe, Arturo Servin, and Paul Vixie for feedback.

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

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

[RFC6303] Andrews, M., "Locally Served DNS Zones", BCP 163, RFC 6303, July 2011.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, February 2013.

8.2. Informative References

[I-D.ietf-dnsop-as112-dname]
           Abley, J., Dickson, B., Kumari, W., and G. Michaelson, "AS112 Redirection using DNAME", draft-ietf-dnsop-as112-dname-06 (work in progress), November 2014.

Appendix A. Changes / Author Notes.

   [RFC Editor: Please remove this section before publication]

   From -05 to -06

   o Incorporated comments from a number of people, including a number
      of suggestion heard at the IETF meeting in Dallas, and the DNSOP
      Interim meeting in May, 2015.

   o Removed the "Let's have an (optional) IANA registry for people to
      (opportinistically) register their string, if they want that
      option" stuff. It was, um, optional....

   From -04 to -05

   o Went through and made sure that I'd captured the feedback
      received.

   o Comments from Ed Lewis.

   o Filled in the "Domain Name Reservation Considerations" section of
      RFC6761.

   o Removed examples from .Onion.

   From -03 to -04

   o Incorporated some comments from Paul Hoffman

   From -02 to -03

   o After discussions with chairs, made this much more generic (not
      purely non-DNS), and some cleanup.

   From -01 to -02

   o Removed some fluffy wording, tightened up the language some.

   From -00 to -01.

   o Fixed the abstract.

   o Recommended that folk root their non-DNS namespace under a DNS
      namespace that they control (Joe Abley)

Authors' Addresses

    Warren Kumari
    Google
    1600 Amphitheatre Parkway
    Mountain View, CA 94043
    US

    Email: warren@kumari.net

    Andrew Sullivan
    Dyn
    150 Dow Street
    Manchester, NH 03101
    US

    Email: asullivan@dyn.com