

DNSOP
Internet-Draft
Updates: [6761](#) (if approved)
Intended status: Standards Track
Expires: February 15, 2018

M. West
Google, Inc
August 14, 2017

**Let 'localhost' be localhost.
draft-west-let-localhost-be-localhost-05**

Abstract

This document updates [RFC6761](#) with the goal of ensuring that "localhost" can be safely relied upon as a name for the local host's loopback interface. To that end, stub resolvers are required to resolve localhost names to loopback addresses. Recursive DNS servers are required to return "NXDOMAIN" when queried for localhost names, which will cause non-conformant stub resolvers to fail safely closed. Together, these requirements would allow applications and specifications to join regular users in drawing the common-sense conclusions that "localhost" means "localhost", and doesn't resolve to somewhere else on the network.

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 15, 2018.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology and notation	3
3.	The "localhost." Special-Use Domain Name	3
4.	IANA Considerations	5
4.1.	Domain Name Reservation Considerations	5
4.2.	DNSSEC	5
5.	Implementation Considerations	5
5.1.	Non-DNS usage of localhost names	5
6.	References	5
6.1.	Normative References	5
6.2.	Informative References	6
Appendix A.	Changes from RFC 6761	6
Appendix B.	Changes in this draft	7
B.1.	draft-west-let-localhost-be-localhost-05	7
B.2.	draft-west-let-localhost-be-localhost-04	7
B.3.	draft-west-let-localhost-be-localhost-03	7
B.4.	draft-west-let-localhost-be-localhost-02	7
B.5.	draft-west-let-localhost-be-localhost-01	7
B.6.	draft-west-let-localhost-be-localhost-00	8
Appendix C.	Acknowledgements	8
Author's Address	8

[1.](#) Introduction

The "127.0.0.0/8" IPv4 address block and "::1/128" IPv6 address block are reserved as loopback addresses. Traffic to this block is assured to remain within a single host, and can not legitimately appear on any network anywhere. This turns out to be a very useful property in a number of circumstances; useful enough to label explicitly and interoperably as "localhost". [\[RFC1537\]](#) suggests that this special-use top-level domain name has been implicitly mapped to loopback addresses for decades at this point, and that [\[RFC6761\]](#)'s assertion that developers may "assume that IPv4 and IPv6 address queries for localhost names will always resolve to the respective IP loopback address" is well-founded.

Unfortunately, the rest of that latter document's requirements undercut the assumption it suggests. Client software is empowered to send localhost names to DNS servers, and resolvers are empowered to

West

Expires February 15, 2018

[Page 2]

return unexpectedly non-loopback results. This divide between theory and practice has a few impacts:

First, the lack of confidence that "localhost" actually resolves to the loopback interface encourages application developers to hard-code IP addresses like "127.0.0.1" in order to obtain certainty regarding routing. This causes problems in the transition from IPv4 to IPv6 (see problem 8 in [[I-D.ietf-sunset4-gapanalysis](#)]).

Second, HTTP user agents sometimes distinguish certain contexts as "secure"-enough to make certain features available. Given the certainty that "127.0.0.1" cannot be maliciously manipulated or monitored, [[SECURE-CONTEXTS](#)] treats it as such a context. Since "localhost" might not actually map to the loopback address, that document declines to give it the same treatment. This exclusion has (rightly) surprised some developers, and exacerbates the risks of hard-coded IP addresses by giving developers positive encouragement to use an explicit loopback address rather than a localhost name.

This document hardens [[RFC6761](#)]'s recommendations regarding "localhost" by requiring that name resolution APIs and libraries themselves return a loopback address when queried for localhost names, bypassing lookup via recursive and authoritative DNS servers entirely. Further, recursive and authoritative DNS servers are required to return "NXDOMAIN" for such queries, ensuring that non-conformant stub resolvers will fail safely.

2. Terminology and 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](#)].

IPv4 loopback addresses are registered in Table 4 of [Section 2.2.2 of \[\[RFC6890\]\(#\)\]](#) as "127.0.0.0/8".

IPv6 loopback addresses are registered in Table 17 of [Section 2.2.3 of \[\[RFC6890\]\(#\)\]](#) as "::1/128".

The domain "localhost.", and any names falling within ".localhost.", are known as "localhost names".

3. The "localhost." Special-Use Domain Name

Localhost names are special in the following ways:

1. Users are free to use localhost names as they would any other domain names. Users may assume that IPv4 and IPv6 address

West

Expires February 15, 2018

[Page 3]

queries for localhost names will always resolve to the respective IP loopback address.

2. Application software MAY recognize localhost names as special, or MAY pass them to name resolution APIs as they would for other domain names.

If application software wishes to make security decisions based upon the assumption that localhost names resolve to loopback addresses (e.g. if it wishes to ensure that a context meets the requirements laid out in [[SECURE-CONTEXTS](#)]), then it SHOULD avoid relying upon name resolution APIs, instead performing the resolution itself. If such software chooses to rely on name resolution APIs, it MUST verify that the resulting IP address is a loopback address before making a decision about its security properties.

In any event, application software MUST NOT use a searchlist to resolve a localhost name. That is, even if DHCP's domain search option [[RFC3397](#)] is used to specify a searchlist of "example.com" for a given network, the name "localhost" will not be resolved as "localhost.example.com", and "subdomain.localhost" will not be resolved as "subdomain.localhost.example.com".

3. Name resolution APIs and libraries MUST recognize localhost names as special, and MUST always return an appropriate IP loopback address for IPv4 and IPv6 address queries and negative responses for all other query types. Name resolution APIs MUST NOT send queries for localhost names to their configured recursive DNS server(s).

As for application software, name resolution APIs and libraries MUST NOT use a searchlist to resolve a localhost name.

4. (Caching) recursive DNS servers MUST respond to queries for localhost names with NXDOMAIN.
5. Authoritative DNS servers MUST respond to queries for localhost names with NXDOMAIN.
6. DNS server operators SHOULD be aware that the effective RDATA for localhost names is defined by protocol specification and cannot be modified by local configuration.
7. DNS Registries/Registrars MUST NOT grant requests to register localhost names in the normal way to any person or entity. Localhost names are defined by protocol specification and fall outside the set of names available for allocation by registries/

West

Expires February 15, 2018

[Page 4]

registrars. Attempting to allocate a localhost name as if it were a normal DNS domain name will not work as desired, for reasons 2, 3, 4, and 5 above.

4. IANA Considerations

IANA is requested to update the "localhost." registration in the registry of Special-Use Domain Names [RFC6761] to reference the domain name reservations considerations section of this document.

4.1. Domain Name Reservation Considerations

This document requests that IANA update the "localhost." registration in the registry of Special-Use Domain Names [RFC6761] to reference the domain name reservation considerations defined in [Section 3](#).

4.2. DNSSEC

The ".localhost" TLD is already assigned to IANA, as per [RFC2606]. This document requests that a DNSSEC insecure delegation (that is, a delegation with no DS records) be inserted into the root-zone, delegated to "blackhole-[12].iana.org".

This request for an insecure delegation relies on the rationale spelled out in section 4 of [[I-D.wkumari-dnsop-internal](#)], which discusses the DNSSEC considerations for the ".internal" TLD. The same considerations apply to this document's discussion of localhost names.

5. Implementation Considerations

5.1. Non-DNS usage of localhost names

Some application software differentiates between the hostname "localhost" and the IP address "127.0.0.1". MySQL, for example, uses a unix domain socket for the former, and a TCP connection to the loopback address for the latter. The constraints on name resolution APIs above do not preclude this kind of differentiation.

6. References

6.1. 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, <<http://www.rfc-editor.org/info/rfc2119>>.

- [RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", [RFC 6761](#), DOI 10.17487/RFC6761, February 2013, <<http://www.rfc-editor.org/info/rfc6761>>.
- [RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", [BCP 153](#), [RFC 6890](#), DOI 10.17487/RFC6890, April 2013, <<http://www.rfc-editor.org/info/rfc6890>>.

6.2. Informative References

- [I-D.ietf-sunset4-gapanalysis]
LIU, W., Xu, W., Zhou, C., Tsou, T., Perreault, S., Fan, P., Gu, R., Xie, C., and Y. Cheng, "Gap Analysis for IPv4 Sunset", [draft-ietf-sunset4-gapanalysis-09](#) (work in progress), August 2017.
- [I-D.wkumari-dnsop-internal]
Kumari, W., "The .internal TLD.", [draft-wkumari-dnsop-internal-00](#) (work in progress), July 2017.
- [RFC1537] Beertema, P., "Common DNS Data File Configuration Errors", [RFC 1537](#), DOI 10.17487/RFC1537, October 1993, <<http://www.rfc-editor.org/info/rfc1537>>.
- [RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", [BCP 32](#), [RFC 2606](#), DOI 10.17487/RFC2606, June 1999, <<http://www.rfc-editor.org/info/rfc2606>>.
- [RFC3397] Aboba, B. and S. Cheshire, "Dynamic Host Configuration Protocol (DHCP) Domain Search Option", [RFC 3397](#), DOI 10.17487/RFC3397, November 2002, <<http://www.rfc-editor.org/info/rfc3397>>.
- [SECURE-CONTEXTS]
West, M., "Secure Contexts", n.d., <<http://w3c.github.io/webappsec-secure-contexts/>>.

[Appendix A](#). Changes from [RFC 6761](#)

[Section 3](#) updates the requirements in [section 6.3 of \[RFC6761\]](#) in a few substantive ways:

1. Application software and name resolution APIs and libraries are prohibited from using searchlists when resolving localhost names, and encouraged to bypass resolution APIs and libraries altogether if they intend to make security decisions based on the "localhost" name.

West

Expires February 15, 2018

[Page 6]

2. Name resolution APIs and libraries are required to resolve localhost names to loopback addresses, without sending the query on to caching DNS servers.
3. Caching and authoritative DNS servers are required to respond to resolution requests for localhost names with NXDOMAIN.

Appendix B. Changes in this draft

B.1. draft-west-let-localhost-be-localhost-05

- o Updated obsolete references to [RFC 5735](#) and 5156 in favor of [\[RFC6890\]](#).
- o Clarify that non-caching recursive DNS servers are also addressed by #4 in [Section 3](#).
- o Reformulating the abstract and introduction based on feedback like Ted Lemon's in <https://www.ietf.org/mail-archive/web/dnsop/current/msg20757.html>
- o Added a request that an insecure delegation for "localhost." be added to the root-zone.

B.2. draft-west-let-localhost-be-localhost-04

- o Restructured the draft as a stand-alone document, rather than as set of monkey-patches against [\[RFC6761\]](#).

B.3. draft-west-let-localhost-be-localhost-03

- o Explicitly referenced [\[I-D.ietf-sunset4-gapanalysis\]](#).
- o Added a prohibition against using searchlists to resolve localhost names.
- o Noted that MySQL has special behavior differentiating the connection mechanism used for "localhost" and "127.0.0.1".

B.4. draft-west-let-localhost-be-localhost-02

- o Pulled in definitions for IPv4 and IPv6 loopback addresses.

B.5. draft-west-let-localhost-be-localhost-01

- o Added a requirement that caching DNS servers MUST generate an immediate negative response.

B.6. draft-west-let-localhost-be-localhost-00

First draft.

Appendix C. Acknowledgements

Ryan Sleevi and Emily Stark informed me about the strange state of localhost name resolution. Erik Nygren poked me to take another look at the set of decisions we made in [[SECURE-CONTEXTS](#)] around "localhost."; this document is the result, and his feedback has been very helpful.

Author's Address

Mike West
Google, Inc

Email: mkwst@google.com
URI: <https://mikewest.org/>

