DNSOP
Internet-Draft
Updates: 6761 (if approved)
Intended status: Standards Track
Expires: February 7, 2018

M. West
Google, Inc

August 6, 2017

Let 'localhost' be localhost.
draft-west-let-localhost-be-localhost-04

Abstract

This document updates RFC6761 by requiring that the domain "localhost." and any names falling within ".localhost." resolve to loopback addresses. This would allow other 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 7, 2018.

Table of Contents

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 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 [draft-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 DNS resolution work the way that users assume: "localhost" is the loopback interface on the local host. Resolver APIs will resolve "localhost." and any names falling within ".localhost." to loopback addresses, and traffic to those hosts will never traverse a remote network.

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 defined in Section 2.1 of [RFC5735] as "127.0.0.0/8".

IPv6 loopback addresses are defined in Section 3 of [RFC5156] as "::1/128".

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

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

   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 caching DNS server(s).

   Name resolution APIs and libraries MUST NOT use a searchlist to resolve a localhost name.

4. Caching 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/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 this document.

5. Implementation Considerations

5.1. Security Decisions

If application software wishes to make security decisions based upon the fact 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 it 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.

5.2. 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>.

[RFC5156] Blanchet, M., "Special-Use IPv6 Addresses", RFC 5156, DOI 10.17487/RFC5156, April 2008, <http://www.rfc-editor.org/info/rfc5156>.

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", RFC 5735, DOI 10.17487/RFC5735, January 2010, <http://www.rfc-editor.org/info/rfc5735>.

[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>.

6.2. Informative References

[draft-ietf-sunset4-gapanalysis] Perreault, S., Tsou, T., Zhou, C., and P. Fan, "Gap Analysis for IPv4 Sunset", n.d., <http://tools.ietf.org/html/draft-ietf-sunset4-gapanalysis>.

[RFC1537] Beertema, P., "Common DNS Data File Configuration Errors", RFC 1537, DOI 10.17487/RFC1537, October 1993, <http://www.rfc-editor.org/info/rfc1537>.

[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 of this document 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.

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. 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/