Internet Engineering Task Force (IETF)
Request for Comments: 8917
Updates: 5222
Category: Standards Track
ISSN: 2070-1721

R. Gellens
Core Technology Consulting
B. Rosen

October 2020

The LoST-Validation Straightforward-Naming Authority PoinTeR (S-NAPTR) Application Service Tag

Abstract

This document adds the 'LoST-Validation' service tag to the Straightforward-Naming Authority PoinTeR (S-NAPTR) Application Service Tag IANA registry. This tag can appear in a Naming Authority Pointer (NAPTR) Domain Name System (DNS) record to assist clients of the Location-to-Service Translation (LoST) Protocol in identifying LoST servers designated for location validation. This tag and the information about its use update RFC 5222, which enables the explicit discovery of a server that supports location validation.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8917.

Copyright Notice

Table of Contents

1. Document Scope
2. Introduction
  2.1. Requirements Language

4. Backwards Compatibility
5. Security Considerations
6. IANA Considerations
  6.1. S-NAPTR Registration
7. References
  7.1. Normative References
  7.2. Informative References
Acknowledgements
Authors' Addresses

1. Document Scope

This document adds 'LoST-Validation' to the S-NAPTR Application Service Tag IANA registry and describes how this tag fits in the LoST server discovery procedure described in [RFC5222]. This tag is used with Naming Authority Pointer (NAPTR) Domain Name System (DNS) records so that clients of the Location-to-Service Translation (LoST) Protocol [RFC5222] can identify servers designated for location validation. This tag and the information on its use is an update to [RFC5222] that enables the explicit discovery of a server that supports location validation.

2. Introduction

The LoST Protocol [RFC5222] defines a mapping service with the additional ability for a client to request that a civic address be validated. The LoST protocol allows servers to ignore a request to perform location validation. The National Emergency Number Association (NENA) has defined an architecture for all-IP emergency services (known as "i3" [NENA-i3]), which defines the mapping (routing) and validation functions as two distinct functional elements, defined as an Emergency Call Routing Function (ECRF) and a Location Validation Function (LVF). NENA i3 requires that the mapping (ECRF) and validation (LVF) functions be separable; an entity responsible for a LoST server cluster can decide to provide mapping and validation services using consolidated or separate server clusters (i.e., using the same or separate boxes). The rationale is that the mapping service is used in real time during emergency call routing, while the validation service is used in advance, typically when data is provisioned; therefore, the mapping service has much higher availability and response-time requirements than the validation service. An organization might choose to deploy these services using different server clusters to make it easier to provide higher levels of service for the mapping function while shielding it from the potentially bursty load of validation. Another organization might choose to use the same sets of servers for both services, configured and deployed to offer the high service level demanded of the mapping service.

In order to permit this separability, any entity querying a LoST server needs to be able to resolve an Application Unique String (AUS) into a URL for a LoST server designated for the required service (mapping or validation). This separability needs to be maintained throughout the LoST tree structure, from forest guide to leaf node (LoST architecture is described in [RFC5582]). Because LoST referrals return an AUS rather than a URL, either a different service tag or a DNS name convention (e.g., "ecrf.example.org" and "lvf.example.org") is needed to differentiate between the services. DNS name conventions are inflexible and fragile, making a different service tag the preferred approach.

Because LoST servers may ignore a request to perform location validation, a service tag explicitly for location validation also reduces the likelihood (which has existed since [RFC5582]) that a client needing location validation will reach servers that are not doing so (due to configuration and/or conditions).

2.1. Requirements Language

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.

3. The LoST-Validation Application Service Tag

This document adds 'LoST-Validation' to the "S-NAPTR Application Service Tags" registry created by [RFC3958]. The 'LoST-Validation' tag serves as a counterpart to the 'LoST' tag added by [RFC5222]: the 'LoST' tag identifies servers able to perform the core mapping function, while 'LoST-Validation' identifies servers designated for the validation function.

Because some servers might be configured to provide both mapping and validation functions, a server identified using the 'LoST' service tag might also perform the validation function (and resolving the two tags might result in the same URL). Because the two functions might be separate, clients seeking a LoST server for location validation can first try a URI-Enabled NAPTR (U-NAPTR) resolution using the 'LoST-Validation' service tag and can fall back to the 'LoST' service tag if this does not resolve to a usable LoST server.

LoST [RFC5222] specifies that LoST servers are located by resolving an AUS using U-NAPTR/DDDS (URI-Enabled NAPTR / Dynamic Delegation Discovery Service) [RFC4848] and defines the 'LoST' application service tag. In order to permit separability of the mapping and validation services performed using LoST, this document defines the 'LoST-Validation' service tag. This tag also reduces the likelihood that a client needing location validation might reach servers that are not performing validation (due to configuration and/or conditions). NAPTR records for LoST servers available for location validation contain the 'LoST-Validation' service tag. An entity needing to perform location validation using LoST performs the discovery procedure as described in [RFC5222], except that the 'LoST-Validation' service tag is used in preference to the 'LoST' service tag. For both service tags, the HTTP and HTTPS URL schemes are used. In the absence of any NAPTR records containing the 'LoST-Validation' service tag, the 'LoST' service tag is used. Fallback to the 'LoST' service tag may follow if the 'LoST-Validation' service tag fails to result in a usable LoST server. The discovery procedure with the 'LoST-Validation' service tag might result in the same URL as the

'LoST' service tag, or it may result in a different URL. When the URLs are different, they could lead to the same physical servers or different servers.

4. Backwards Compatibility

The primary use of LoST in general, and the location validation functionality in particular, is within the emergency services area. Within North America, the NENA i3 [NENA-i3] document specifies how protocols including LoST are used. The i3 document is expected to reference the 'LoST-Validation' service tag and specify its use in both server NAPTR DNS records and client resolution of AUS.

LoST allows a server to refuse to perform location validation and defines the 'locationValidationUnavailable' warning. LoST also allows a server to refer to another server rather than answering itself. So, in a deployment where a LoST tree has separate server clusters for mapping and for validation, mapping servers receiving a request for validation could either perform the validation as requested or return the 'locationValidationUnavailable' warning and potentially also include a <redirect> element to redirect to a validation server. However, the <redirect> element contains an AUS, so unless the AUSs for validation and mapping are different (e.g., 'ecrf.example.org' and 'lvf.example.org'), we still need a different service tag to allow for flexible deployment choices (i.e., not requiring a DNS name convention).

LoST clients performing emergency services operations in North America are expected to comply with the NENA i3 specification and hence support the 'LoST-Validation' service tag when defined. A LoST client implemented prior to the addition of the 'LoST-Validation' tag would use the 'LoST' tag to resolve an AUS. Such a client might not be performing location validation, but if it is, the LoST server it contacts may perform the service. Even in a deployment where mapping and validation are split, the data is identical; the split is a load and deployment optimization strategy. Servers designated for mapping might perform validation when requested (potentially depending on load or other factors). If an older client attempts validation using a designated mapping server that refuses the request, the client will retry later, at which point the server might provide the function (e.g., if its load or other conditions have changed). Even in the case of a designated mapping server that refuses to perform validation at any time, the server could return a redirect with a different AUS (e.g., "lvf.example.com") that resolves to a designated validation server. In the worst case, the client will be unable to reach a server willing to perform validation and will follow up (e.g., submit a discrepancy report as specified in NENA i3). The resolution may be to update the client with the 'LoST-Validation' service tag, update the AUS returned in a redirect and DNS to use a different DNS host name, or permit the server to perform validation when not under stress (or a combination). Note that, because LoST does not require servers to perform validation, the situation described can exist regardless of the addition of the 'LoST-Validation' service tag. Use of the tag improves the likelihood that a client is able to validate a location when needed.

5. Security Considerations

The security considerations described in [RFC3958], [RFC4848], and [RFC5222] apply here. No additional security aspects are foreseen by the addition of an extra tag. Separation of services might be desired, for example, to be able to allocate different levels of resources (such as server capacity, attack mitigation, bandwidth, etc.) to the mapping and validation services, in which case separate tags are needed to allow LoST clients (which may include other LoST servers) to identify the correct server cluster.

[RFC5222] descriptively discusses the use of DNS security [RFC4033] to mitigate the risk of DNS-based attacks. Because DNS security has become more widely deployed since the publication of [RFC5222], such measures SHOULD be used when performing NAPTR resolution. Note that, while there are valid reasons to proceed with a LoST mapping query despite security failures while initiating or processing an emergency call, these concerns generally do not apply to a LoST validation query done in advance of an emergency call.

6. IANA Considerations

IANA has added 'LoST-Validation' to the "S-NAPTR Application Service Tags" registry created by [RFC3958]. This tag serves as a counterpart to the 'LoST' tag added by [RFC5222].

(Note that IANA and [RFC3958] call this registry "S-NAPTR Application Service Tags", while [RFC5222] calls it "U-NAPTR application service tag".)

6.1. S-NAPTR Registration

This document registers an S-NAPTR application service tag:

Application Service Tag: LoST-Validation

Defining Publication: This document

7. References

7.1. 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>.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, DOI 10.17487/RFC3958, January 2005, <https://www.rfc-editor.org/info/rfc3958>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4848] Daigle, L., "Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)", RFC 4848, DOI 10.17487/RFC4848, April 2007, <https://www.rfc-editor.org/info/rfc4848>.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, DOI 10.17487/RFC5222, August 2008, <https://www.rfc-editor.org/info/rfc5222>.

[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>.

7.2. Informative References

[NENA-i3] National Emergency Number Association (NENA) Interconnection and Security Committee, i3 Architecture Working Group, "Detailed Functional and Interface Standards for the NENA i3 Solution", 2016, <https://www.nena.org/page/i3_Stage3>.

[RFC5582] Schulzrinne, H., "Location-to-URL Mapping Architecture and Framework", RFC 5582, DOI 10.17487/RFC5582, September 2009, <https://www.rfc-editor.org/info/rfc5582>.

Acknowledgements

Many thanks to Ted Hardie, Ben Campbell, Dan Banks, Pete Resnick, Shawn Emery, Robert Wilton, Roman Danyliw, and Benjamin Kaduk for their helpful reviews and suggestions and to Barry Leiba for shepherding the document.

Authors' Addresses

Randall Gellens
Core Technology Consulting
United States of America

Email: rg+ietf@coretechnologyconsulting.com
URI: http://www.coretechnologyconsulting.com

Brian Rosen
470 Conrad Dr.
Mars, PA 16046
United States of America

Email: br@brianrosen.net