Internet Engineering Task Force (IETF)
Request for Comments: 7075
Updates: 6733
Category: Standards Track
ISSN: 2070-1721

T. Tsou
Huawei Technologies (USA)
R. Hao
Comcast Cable
T. Taylor, Ed.
Huawei Technologies

November 2013

Realm-Based Redirection In Diameter

Abstract

The Diameter protocol includes a capability for message redirection, controlled by an application-independent "redirect agent". In some circumstances, an operator may wish to redirect messages to an alternate domain without specifying individual hosts. This document specifies an application-specific mechanism by which a Diameter server or proxy (node) can perform such a redirection when the Straightforward-Naming Authority Pointer (S-NAPTR) is not used for dynamic peer discovery. A node performing this new function is referred to as a "Realm-based Redirect Server".

This memo updates Sections 6.13 and 6.14 of RFC 6733 with respect to the usage of the Redirect-Host-Usage and Redirect-Max-Cache-Time Attribute-Value Pairs (AVPs).

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 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7075.

Table of Contents

1. Introduction

The Diameter base protocol [RFC6733] specifies a basic redirection service provided by a redirect agent. The redirect indication returned by the redirect agent is described in Section 6.1.8 and Sections 6.12 through 6.14 of [RFC6733]. It provides one or more individual hosts to the message sender as the destination of the redirected message.

However, consider the case where an operator has offered a specific service but no longer wishes to do so. The operator has arranged for an alternative domain to provide the service. To aid in the transition to the new arrangement, the original operator maintains a redirect server to indicate to the message sender the alternative domain to which the redirect the request should be sent. However, the original operator should not have to configure the redirect server with a list of hosts to contact in the alternative operator's domain; the original operator should simply be able to provide redirect indications to the domain as a whole.

1.1. Terminology

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].

Within this specification, the term "realm-based redirection" is used to refer to a mode of operation where a realm, rather than an individual host, is returned as the redirect indication.

The term "Realm-based Redirect Server" denotes the Diameter node (Diameter server or proxy) that returns the realm-based redirection. The behavior of the Realm-based Redirect Server itself is a slight modification to the behavior of a basic redirect agent as described in Section 6.1.8 of [RFC6733].

The use of a number of terms in this document is consistent with the usage in [RFC6733]: "Diameter client", "Diameter node", "Diameter peer", "Diameter server", "proxy", "realm" or "domain", "redirect agent", and "session" as defined in Section 1.2, and "application" as defined implicitly by Sections 1.3.4, 2.3, and 2.4.

2. Support of Realm-Based Redirection Within Applications

The DNS-based dynamic peer discovery mechanism defined in the Diameter base protocol [RFC6733] provides a simple mechanism for realm-based redirection using the S-NAPTR DDDS application [RFC3958]. When S-NAPTR is used for peer discovery, redirection of Diameter requests from the original realm to a new realm may be performed by updating the existing NAPTR resource records (RRs) for the original realm as follows: the NAPTR RR for the desired application(s) and supported application protocol(s) provided by the new realm will have an empty FLAG field and the REPLACEMENT field will contain the new realm to use for the next DNS lookup. The new realm can be arbitrary; the restriction in [RFC6733] that the NAPTR replacement field match the domain of the original query does not apply for realm-based redirect purposes.

However, the use of DNS-based dynamic peer discovery is optional for Diameter implementations. For deployments that do not make use of S-NAPTR peer discovery, support of realm-based redirection needs to be specified as part of the functionality supported by a Diameter application. In this way, support of the considered Diameter application (discovered during capabilities exchange phase as defined in Diameter base protocol [RFC6733]) indicates implicit support of the realm-based redirection mechanism. A new application specification can incorporate the mechanism specified here by making it mandatory to implement for the application and referencing this specification normatively.

The result of making realm-based redirection an application-specific behavior is that it cannot be performed by a redirect agent as defined in [RFC6733], but MUST be performed instead by an application-aware Diameter node (Diameter server or proxy) (hereafter called a "Realm-based Redirect Server").

An application can specify that realm-based redirection operates only on complete sessions beginning with the initial message or on every message within the application, even if earlier messages of the same session were not redirected. This distinction matters only when realm-based redirection is first initiated. In the former case, existing sessions will not be disrupted by the deployment of realm-based redirection. In the latter case, existing sessions will be disrupted if they are stateful.

3. Realm-Based Redirection

This section specifies an extension of the Diameter base protocol [RFC6733] to achieve realm-based redirection. The elements of this solution are:

- a new result code, DIAMETER_REALM_REDIRECT_INDICATION (3011);
- a new attribute-value pair (AVP), Redirect-Realm (620); and
- associated behavior at Diameter nodes implementing this specification.

This behavior includes the optional use of the Redirect-Host-Usage and Redirect-Max-Cache-Time AVPs. In this document, these AVPs apply to the peer discovered by a node acting on the redirect server's response, an extension to their normal usage as described in Sections 6.13 and 6.14 of [RFC6733].

Section 3.2.2 and Section 3.2.3 describe how a proxy or client may update its routing table for the application and initial realm as a result of selecting a peer in the new realm after realm-based redirection. Note that as a result, the proxy or client will automatically route subsequent requests for that application to the new realm (with the possible exception of requests within sessions already established with the initial realm) until the cached routing entry expires. This should be borne in mind if the rerouting is intended to be temporary.

3.1. Configuration of the Realm-Based Redirect Server

A Diameter node (Diameter server or proxy) acting as a Realm-based Redirect Server MUST be configured as follows to execute realm-based redirection:

- configured with an application that incorporates realm-based redirection;
- the Local Action field of the routing table described in Section 2.7 of [RFC6733] is set to LOCAL;
- an application-specific field is set to indicate that the required local action is to perform realm-based redirection;
- an associated application-specific field is configured with the identities of one or more realms to which the request should be redirected.

3.2. Behavior of Diameter Nodes

3.2.1. Behavior at the Realm-Based Redirect Server

As mentioned in Section 2, an application can specify that realm-based redirection operates only on complete sessions beginning with the initial message (i.e., to prevent disruption of established sessions) or on every message within the application, even if earlier messages of the same session were not redirected.

If a Realm-based Redirect Server configured as described in Section 3.1 receives a request to which realm-based redirection applies, the Realm-based Redirect Server MUST reply with an answer message with the 'E' bit set, while maintaining the Hop-by-Hop Identifier in the header. The Realm-based Redirect Server MUST include the Result-Code AVP set to DIAMETER_REALM_REDIRECT_INDICATION. The Realm-based Redirect Server MUST also include the alternate realm identifier(s) with which it has been configured, each in a separate Redirect-Realm AVP instance.

The Realm-based Redirect Server MAY include a copy of the Redirect-Host-Usage AVP, which SHOULD be set to REALM_AND_APPLICATION. If this AVP is added, the Redirect-Max-Cache-Time AVP MUST also be included. Note that these AVPs apply to the peer discovered by a node acting on the Realm-based Redirect Server's response as described in the next section. This is an extension of their normal usage as described by Sections 6.13 and 6.14 of [RFC6733].

> Realm-based redirection MAY be applied even if a Destination-Host AVP is present in the request, depending on the operator-based policy.

3.2.2. Proxy Behavior

A proxy conforming to this specification that receives an answer message with the Result-Code AVP set to DIAMETER_REALM_REDIRECT_INDICATION MUST attempt to reroute the original request to a server in a realm identified by a Redirect-Realm AVP instance in the answer message, and if it fails MUST forward the indication toward the client. To reroute the request, it MUST take the following actions:

1. Select a specific realm from amongst those identified in instances of the Redirect-Realm AVP in the answer message.

2. If successful, locate and establish a route to a peer in the realm given by the Redirect-Realm AVP, using normal discovery procedures as described in Section 5.2 of [RFC6733].

3. If again successful:

   A. update its cache of routing entries for the realm and application to which the original request was directed, taking into account the Redirect-Host-Usage and Redirect-Max-Cache-Time AVPs, if present in the answer.

   B. Remove the Destination-Host (if present) and Destination-Realm AVPs from the original request and add a new Destination-Realm AVP containing the realm selected in the initial step.

   C. Forward the modified request.

4. If either of the preceding steps 2-3 fail and additional realms have been identified in the original answer, select another instance of the Redirect-Realm AVP in that answer and repeat steps 2-3 for the realm that it identifies.

3.2.3. Client Behavior

A client conforming to this specification MUST be prepared to receive either an answer message containing a Result-Code AVP set to DIAMETER_REALM_REDIRECT_INDICATION, or, as the result of proxy action, some other result from a realm differing from the one to which it sent the original request. In the case where it receives DIAMETER_REALM_REDIRECT_INDICATION, the client SHOULD follow the same steps prescribed in the previous section for a proxy, in order to both update its routing table and obtain service for the original request.

3.3. The Redirect-Realm AVP

The Redirect-Realm AVP (620) is of type DiameterIdentity. It specifies a realm to which a node receiving a redirect indication containing the result code value DIAMETER_REALM_REDIRECT_INDICATION and the Redirect-Realm AVP SHOULD route the original request.

3.4. DIAMETER_REALM_REDIRECT_INDICATION Protocol Error Code

The DIAMETER_REALM_REDIRECT_INDICATION (3011) Protocol error code indicates that a server has determined that the request within an application supporting realm-based redirection could not be satisfied locally, and the initiator of the request SHOULD direct the request directly to a peer within a realm that has been identified in the response. When set, the Redirect-Realm AVP MUST be present.

4. Security Considerations

The general recommendations given in Section 13 of the Diameter base protocol [RFC6733] apply. Specific security recommendations related to the realm-based redirection defined in this document are described below.

Realm-based redirection implies a change in the business relationship between organizations. Before redirecting a request towards a realm different from the initial realm, the client or proxy MUST ensure that the authorization checks have been performed at each connection along the path toward the realm identified in the realm-based redirect indication. Details on Diameter authorization path set-up are given in Section 2.9 of [RFC6733]. Section 13 of [RFC6733] provides recommendations on how to authenticate and secure each peer-to-peer connection (using TLS, DTLS, or IPsec) along the way, thus permitting the necessary hop-by-hop authorization checks.

Although it is assumed that the administrative domains are secure, a compromised Diameter node acting as a Realm-based Redirect Server would be able to redirect a large number of Diameter requests towards a victim domain that would then be flooded with undesired Diameter requests. Such an attack is nevertheless discouraged by the use of secure Diameter peer-to-peer connections and authorization checks, since these would enable a potential victim domain to discover from where an attack is coming. That in itself, however, does not prevent such a DoS attack.

Because realm-based redirection defined in this document implies that the Destination-Realm AVP in a client-initiated request can be changed by a Diameter proxy in the path between the client and the server, any cryptographic algorithm that would use the Destination-Realm AVP as input to the calculation performed by the client and the server would be broken by this form of redirection. Application specifications that would rely on such cryptographic algorithms SHOULD NOT incorporate this realm-based redirection.

5. IANA Considerations

This specification allocates a new AVP code Redirect-Realm (620) in the "AVP Codes" registry under "Authentication, Authorization, and Accounting (AAA) Parameters".

This specification allocates a new Result-Code value DIAMETER_REALM_REDIRECT_INDICATION (3011) in the "Result-Code AVP Values (code 268) - Protocol Errors" registry under "Authentication, Authorization, and Accounting (AAA) Parameters".

6. Acknowledgements

Glen Zorn, Sebastien Decugis, Wolfgang Steigerwald, Mark Jones, Victor Fajardo, Jouni Korhonen, Avi Lior, and Lionel Morand contributed comments that helped to shape this document. As shepherd, Lionel contributed a second set of comments that added polish to the document before it was submitted to the IESG. Benoit Claise picked up additional points that were quickly resolved with Lionel's help. During IETF Last Call Review, Enrico Marocco picked up some important editorial corrections. Stefan Winter contributed text on the use of S-NAPTR as an alternative method of realm-based redirection already specified in [RFC6733]. Derek Atkins performed a review on behalf of the Security Directorate. Lionel noted one more correction.

Finally, this document benefited from comments and discussion raised by IESG members Stewart Bryant, Stephen Farrell, Barry Leiba, Pete Resnick, Jari Arkko, and Sean Turner during IESG review.

The authors are very grateful to Lionel Morand for his active role as document shepherd. At each stage, he worked to summarize and resolve comments, making the editor's role easy. Thank you.

7. References

7.1. Normative References

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

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

7.2. Informative References

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

Authors' Addresses

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
EMail: Tina.Tsou.Zouting@huawei.com
URI: http://tinatsou.weebly.com/contact.html

Ruibing Hao
Comcast Cable
One Comcast Center
Philadelphia, PA 19103
USA

Phone: +1 215 286 3991(O)
EMail: Ruibing_Hao@cable.comcast.com

Tom Taylor (editor)
Huawei Technologies
Ottawa
Canada

EMail: tom.taylor.stds@gmail.com