Diameter Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2017

L. Bertz
Sprint

June 29, 2017

Diameter Predicted Units
draft-bertz-dime-predictunits-02

Abstract

This document specifies the conveyance of predicted usage information for proper dimensioning of network services that use Diameter based authorization.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

When a User is authorized to use a service via Diameter applications such as [RFC4006] or [RFC7155], the Client is not aware of the average load placed upon it by the User. This can lead to overload situations or Diameter Clients being too conservative and denying services to valid Users even whose presence would not overload the service.

Given virtualization and the use of many software based services the service capacity varies on a service instance, i.e. Diameter Client, basis. Even though the Diameter Client is the same softawre it will vary in terms of the load it can accept. Thus, a Diameter Server cannot depend upon consistent capacities of a Diameter Client.

This specification introduces the Predicted-Service-Units Attribute Value Pair (AVP). This information conveys the predicted usage introduced on the service by the authorized User. Such information can be used by the Diameter Client to estimate future load and proactively manage its resources.

Although this informaiton is conveyed from the Diameter Server to the Client several system aspects are out of the scope of this document:

- How the Diameter Server acquired the information contained in the Predicted-Service-Units AVP.

- How the values in the Predicted-Service-Units AVP were determined.

- The accuracy or validity of the values in the Predicted-Service-Units AVP.

- Specific actions the Diameter Client should take when its service functions are overloaded or are predicted to be overloaded based upon the information provided by Predicted-Service-Units.

- Specific actions the Diameter Client takes to bring itself in/out of service for new or existing Users.

When the value(s) or multiple types of Costs are provided they are represented by the Time-Of-Day-Condition AVP defined in [RFC5777] and contained in a Predicted-Service-Units-Series AVP. This AVP contains one or more Predicted-Service-Units. Multiple Cost types, e.g. CC-Total-Octets and CC-Time, may be represented in the same Predicted-Service-Units entry and in the same Predicted-Service-Units-Series so long as no overlapping times exist for the same Cost Type.

2. Terminology

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [RFC2119].

3. Predicted Service AVPs

3.1. Predicted-Service-Units

The Predicted-Service-Units AVP (AVP Code TBD1) is of type Grouped and contains the amount of units that the Diameter Client can expect to provide to the end user until the service must be released or the new service authorizatoin request, e.g. Credit-Control-Request, must be sent if a Granted-Service-Unit AVP [RFC4006] has been applied to the user’s service. A client is not required to implement all of the unit types, and it MUST ignore unknown or unsupported unit types.

The Predicted-Service-Units AVP is defined as follows (per the grouped- avp-def of [RFC6733]):

```
            Predicted-Service-Units ::= < AVP Header: TBD1 >
                                       [ CC-Time ]
                                       [ CC-Money ]
                                       [ CC-Total-Octets ]
                                       [ CC-Input-Octets ]
                                       [ CC-Output-Octets ]
                                       [ CC-Service-Specific-Units ]
                                       [ Time-Of-Day-Condition ]
                                      *[ AVP ]
```

The Time-Of-Day-Condition AVP is defined in [RFC5777], all other AVPs are defined in [RFC4006].

The presence of this information is provided as anticipated load information to the Diameter Client and is not intended to be prescriptive in any manner regarding the user’s service.

When the Time-Of-Day-Condition AVP is not present, the value(s) are assumed to apply for the duration of the authorized session until this value is updated as part of the Diameter application, e.g. a Diameter Re-Auth-Request/Answer (RAR/RAA) message [RFC6733].

3.2. Predicted-Service-Units-Series

The Predicted-Service-Units-Series AVP (AVP Code TBD2) is of type Grouped, and contains one or more Predicted-Service-Units with non-overlapping times for each specific Cost type.

A client is not required to implement all of the unit types, and it MUST ingore unknown or unsupported unit types.

It is defined as follows (per the grouped-avp-def of [RFC6733]):

```
             Predicted-Service-Units-Series ::= < AVP Header: TBD2 >
                                       1*{ Predicted-Service-Units }
```

For each specific type of Cost, e.g. CC-Time, any two Predicted-Service-Units values in the series MUST NOT contain overlapping time windows specified in their Time-Of-Day-Condition values. When an entry has no Time-Of-Day-Condition present it is assumed to apply at all times.

4. Usage Examples

When Predicted-Service-Units are returned as part of an authorization per [RFC7155] or [RFC4006], the client MAY use this information as guidance on projected load the new user will generate on the service.

If the client supports/understnds the information provided in the Predicted-Service-Units AVP, it can update its projected load. Based upon this information it MAY take one or more of the following actions (this is not exhaustive):

- Redirect any new service requests at the service / protocol level.
- Begin enforcing mechanisms to reduce the amount of service load on a subset of services already established.
- Remove itself from any system that directs new service requests to it.
- Initiate administrative functions to increase its capacity or start the process of creating new intances to service future requests.

5. IANA Considerations

IANA allocated AVP codes in the IANA-controlled namespace registry specified in Section 11.1.1 of [RFC6733] for the following AVPs that are defined in this document.

AVP	AVP Code	Section Defined	Data Type
Predicted-Service-Units	TBD1	Section 3.1	GROUPED
Predicted-Service-Units-Series	TBD2	Section 3.2	GROUPED

6. Security Considerations

The Diameter base protocol [RFC6733] requires that each Diameter implementation use underlying security; i.e., TLS/TCP, DTLS/SCTP or IPsec. These mechanisms are believed to provide sufficient protection under the normal Internet threat model; that is, assuming that the authorized nodes engaging in the protocol have not been compromised, but that the attacker has complete control over the communication channels between them. This includes eavesdropping, message modification, insertion, and man-in-the-middle and replay attacks. Note also that this application includes a mechanism for application layer replay protection by means of the Session-Id from [RFC6733]. In these environments, the use of TLS/TCP, DTLS/SCTP or IPsec is sufficient. The details of TLS/TCP, DTLS/SCTP or IPsec related security considerations are discussed in the [RFC6733].

Because this application conveys past usage information (directly or indirectly), it increases the interest for various security attacks. Therefore, all parties communicating with each other MUST be authenticated, including, for instance, TLS client-side authentication. In addition, authorization of the client SHOULD be emphasized; e.g., that the client is allowed to perform credit-control for a certain user. The specific means of authorization are outside of the scope of this specification but can be, for instance, manual configuration.

The attributes provided by this solution MUST be assumed to be privacy sensitive by both the client and server.

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

[RFC4006] Hakala, H., Mattila, L., Koskinen, J-P., Stura, M., and J. Loughney, "Diameter Credit-Control Application", RFC 4006, DOI 10.17487/RFC4006, August 2005, <http://www.rfc-editor.org/info/rfc4006>.

[RFC5777] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., Ed., and A. Lior, "Traffic Classification and Quality of Service (QoS) Attributes for Diameter", RFC 5777, DOI 10.17487/RFC5777, February 2010, <http://www.rfc-editor.org/info/rfc5777>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

7.2. Informative References

[RFC7155] Zorn, G., Ed., "Diameter Network Access Server Application", RFC 7155, DOI 10.17487/RFC7155, April 2014, <http://www.rfc-editor.org/info/rfc7155>.

Author’s Address

Lyle Bertz
Sprint
6220 Sprint Parkway
Overland Park, KS 66251
United States

Email: lylebe551144@gmail.com