Diameter
Resource Management Extensions

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at:

http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at:


This document is an individual contribution for consideration by the AAA Working Group of the Internet Engineering Task Force. Comments should be submitted to the diameter@diameter.org mailing list.

Distribution of this memo is unlimited.

Copyright   (C) The Internet Society 2001. All Rights Reserved.
Abstract

Diameter is an authentication, authorization and accounting (AAA) protocol used for network access services, such as dial-up (NASREQ) and Mobile IP. Some Diameter servers maintain state information of active sessions on the access servers, which is used mostly to enforce some local policy decisions. This extension describes an extension to the Diameter protocol that allows the server to query for active session state information from access servers in order to rebuild state information should it be lost for any reason.

Table of Contents

1.0 Introduction
   1.1 Specification of Requirements
   1.2 State synchronization
2.0 Command-Code Values
   2.1 Session-Resource-Query
   2.2 Session-Resource-Reply
3.0 Mandatory AVPs
   3.1 Query-Index AVP
   3.2 Resource-Token AVP
   3.3 Resource-Bag AVP
4.0 IANA Considerations
5.0 Security Considerations
6.0 Acknowledgements
7.0 References
8.0 Authors’ Addresses
9.0 Full Copyright Statement

1.0 Introduction

Diameter [1] is an authentication, authorization and accounting (AAA) protocol used for network access services, such as dial-up (NASREQ) [2] and Mobile IP [3].

The NASREQ AAA requirements [6] require that AAA servers maintain session state information. This is typically used to enforce a local policy decision, such as limiting the number of simultaneous sessions for a specific user, maintaining IP address pools, etc. The AAA WG’s network access requirements [5] require that an AAA protocol be able to query for session state information, in the event that this information is lost.

This extension describes an extension to the Diameter protocol that allows a Diameter node to query for active session state information.
from its peers in order to rebuild state information. Although it is envisioned that this would be used when state information was lost, and needed to be rebuilt, it is possible for a node to periodically query for state information in order to ensure that its state is current.

This document only concerns itself with the ability to query for session state information. Resources are actually reserved when a user is successfully authorized. Therefore, relevant application-specific extensions, such as [2] and [3], MUST define what resources are to be managed, by specifying what AVPs MUST be present in the Resource-Token AVP.

The Extension number for this draft is three (3). Diameter nodes conforming to this specification MUST include an Extension-Id AVP with a value of three in the Device-Reboot-Ind Command [1].

1.1 Specification of Requirements

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [7].

1.2 State synchronization

When a Diameter node determines that it is has lost all state information it had for a specific peer, it SHOULD issue a Session-Resource-Query message to the peer. The node in question MAY postpone all authorization messages from the peer until state has been restored.

Upon receipt of the Session-Resource-Query, all Resource-Token AVPs for the requested sessions, indicated via one or more Session-Id AVP, MUST be returned in a Session-Resource-Reply. The absence of any Session-Id AVP is an indication that all active sessions are to be returned.

If the node is unable to send all of the information within a single message, it MUST include the Query-Index AVP, with a value that has local significance. A node that receives a Session-Resource-Reply with a Query-Index AVP SHOULD issue another Session-Resource-Query message with the Query-Index AVP intact, requesting the rest of the state information.
Figure 1: Session State Exchange

The above example depicts Diameter Node A issuing an SRQ to Node B. Upon replying with an SRR, node B determines that it is unable to include all of the Resource-Token AVPs in a single reply, and therefore includes the Query-Index AVP with a value of x.

Upon receipt of the response, node A processes all Resource-Token AVPs and issues a subsequent SRQ with the Query-Index AVP set to x. Node B receives the SRQ, and using the Query-Index AVP determines which sessions need to be included in the corresponding SRR.

This exchange continues until node B returns an SRR that does not include the Query-Index AVP, indicating that there is no further session state information to be returned.

2.0 Command-Code Values

This section defines Command-Code [1] values that MUST be supported by all Diameter implementations conforming to this specification. The following Command Codes are defined in this specification:

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbrev.</th>
<th>Code</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-Resource-Query</td>
<td>SRQ</td>
<td>277</td>
<td>2.1</td>
</tr>
<tr>
<td>Session-Resource-Reply</td>
<td>SRR</td>
<td>278</td>
<td>2.2</td>
</tr>
</tbody>
</table>

2.1 Session-Resource-Query (SRQ)

The Session-Resource-Query (SRQ), indicated by the Command-Code field set to 277, MAY be sent by a Diameter node to any of its peer to request a state update. The presence of one or more Session-Id AVPs in the Session-Resource-Query message indicates that the server only wants to receive the Resource-Token for the specified session(s).

Message Format
<Session-Resource-Query> ::= < Diameter Header: 277 >
   ( Extension-Id )
   ( Origin-FQDN )
   ( Origin-Realm )
   ( Destination-Realm )
   * [ Session-Id ]
   * [ Destination-FQDN ]
   0*1[ Query-Index ]
   * [ AVP ]
   * [ Proxy-State ]
   * [ Route-Record ]
   * [ Routing-Realm ]
   0*1< Integrity-Check-Value >

2.2 Session-Resource-Reply (SRR)

The Session-Resource-Reply (SRR), indicated by the Command-Code field set to 278, is sent in response to a SRQ message. The SRR message contains a Resource-Token for each active session that was requested via the Session-Id AVP. The absence of any Session-Id AVP in the SRQ implies that Resource-Tokens for all active sessions MUST be returned.

In the event that all of the state information cannot be sent at once, the SRR message MUST include the Query-Index AVP.

Message Format

<Session-Resource-Reply> ::= < Diameter Header: 278 >
   ( Extension-Id )
   ( Origin-FQDN )
   ( Origin-Realm )
   ( Result-Code )
   [ Destination-FQDN ]
   0*1[ Query-Index ]
   * [ Resource-Token ]
   * [ AVP ]
   * [ Proxy-State ]
   * [ Route-Record ]
   * [ Routing-Realm ]
   0*1< Integrity-Check-Value >

3.0 Mandatory AVPs

The following table describes the Diameter AVPs defined in the Resource Management extension, their AVP Code values, types, possible
flag values and whether the AVP MAY be encrypted.

<table>
<thead>
<tr>
<th>AVP</th>
<th>Section</th>
<th>Code</th>
<th>Defined</th>
<th>Data Type</th>
<th>MUST</th>
<th>MAY</th>
<th>SHLD</th>
<th>MUST</th>
<th>MAY</th>
<th>Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query-Index</td>
<td>500</td>
<td>3.1</td>
<td></td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Resource-Bag</td>
<td>502</td>
<td>3.3</td>
<td></td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Resource-Token</td>
<td>501</td>
<td>3.2</td>
<td></td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

### 3.1 Query-Index AVP

The Query-Index AVP (AVP Code 500) is of type Unsigned32 and MUST only be present in the Session-Resource-Query and the Session-Resource-Reply messages. The Query-Index AVP has local significance to the issuer of the Session-Resource-Reply message, and is used to identify the state information that remains to be sent in a subsequent SRR message.

### 3.2 Resource-Token AVP

The Resource-Token AVP (AVP Code 501) is of type Grouped. The value is a set of AVPs used to track state information that is pertinent to an active session. The issuer of the SRR message is responsible for creating a Resource-Token AVP for all active sessions requested.

The following describes the minimum number of AVPs that MUST be present in a Resource-Token AVP. Service-specific AVPs MAY also be present, as defined in the appropriate service extension document.

The Resource-Token Grouped value has the following grammar:

```plaintext
resource-token = sid host user timestamp extension-id optional
    sid = Session-Id AVP ; See [1], Section 3.1.
    host = Host-Name AVP ; See [1], Section 2.3.1.
    user = User-Name AVP ; See [1], Section 3.3.
    timestamp = Timestamp AVP ; See [1], Section 7.3.
    extension-id = Extension-Id AVP ; See [1], Section 2.6.3.
    optional = Resource-Bag AVP ; See Section 3.3
```

The Host-Name AVP contains the NAI of the access router that is servicing the user, while the timestamp AVP contains the time at which the successful Diameter authorization response was received, and the service was initiated.
3.3 Resource-Bag AVP

This AVP allows encapsulation of arbitrarily many AVPs to be included in a Resource-Token. These AVPs are defined in service specific extensions to Diameter. The only restrictions to the AVPs is that they MUST NOT be interpreted so as to conflict with the other fields of the Resource-Token Group value, namely, the Session-Id, Host-Name, User-Name, Timestamp or Extension-Id AVPs.

The Resource-Bag AVP (AVP Code = 502) is of type OctetString. The AVP encapsulates an arbitrary of AVPs, each with its own header and value.

4.0 IANA Considerations

The command codes defined in Section 2.0 are values taken from the Command-Code [1] address space and extended in [2], [4] and [8]. IANA should record the values as defined in Section 2.0.

The AVPs defined in section 3.0 were allocated from from the AVP numbering space defined in [1], and extended in [2], [4] and [8]. IANA should record the values as defined in Section 3.0.

5.0 Security Considerations

This Diameter extension assumes that the Resource Management data is secured either through a hop-by-hop authentication mechanism, as described in [1], or using a strong authentication mechanism as defined in [9].

6.0 Acknowledgements

The authors wish to thank Erik Guttman for providing some very useful proposed text to handle the change in data types.

7.0 References


8.0 Authors’ Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

Phone: +1 650-786-7733
Fax: +1 650-786-6445
E-mail: pcalhoun@eng.sun.com

9.0 Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

10.0 Expiration Date

This memo is filed as <draft-calhoun-diameter-res-mgmt-08.txt> and expires in August 2001.