Diameter Maintenance and Extensions
Internet-Draft
Intended status: Standards Track
Expires: January 7, 2017

L. Bertz
Sprint

July 6, 2016

Diameter Policy Groups and Sets
draft-bertz-dime-policygroups-00

Abstract

This document defines optional Diameter attributes for efficient policy provisioning.

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 January 7, 2017.

1. Introduction

Quite often policy applications will apply common policies over multiple authorized endpoints. These policies may be pre-provisioned or dynamically installed on the Diamater Client by the Diamater Server.

Techniques such as policy grouping, e.g. Base Name used in many 3GPP specifications or Bit Set values are applied.

This document defines both a grouping mechanism, the Group-Name AVP, and a membership (bit set) that can be used to quickly apply one or more Diameter based policies, e.g. Filter-Rule [RFC5777].

2. Requirements Language

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].

3. Terminology

Authorized Users An Entity that has been authorized to use a service via a Diamater Application.

Base Name An organizational structure used to define a domain for multiple Policy Groups or Membership Domains.

Determination Type The matching policy applied, e.g. ANDMASK, AND, etc, for Membership Determination.

Policy Entity A type that may be assigned to a Policy Group or Membership. This includes but is not limited to Filters [RFC7155] or Filter-Rules [RFC5777].

Membership Determination The process by which Policy Entities are selected to be applied to an authorized User.

Membership Domain A name assigned to a Membership Set.

Membership Value A binary set of values where each bit represents a specific membership pattern.

4. Concepts

Policy Groups represent a union of Policy Entities. These entities MUST be of the same type, e.g. Filters [RFC7155] or Filter-Rules [RFC5777].

When establishing groups and membership Sets an optional Base Name MAY be used. It identifies the top level grouping. Policy Entity groups MAY be directly named as well. When no Base Name is provided the value a policy entity is considered to be part of the Base Name "" (empty string) for any matching purposes.

Base Name values create a two tier heirarchy for grouping. However, a Policy Entity can be applied to multiple, distinct sets of authorized Users. These sets can be based upon their state (paid, past due, etc.), customer type (pre-paid, post-paid, etc.) or many other factors. In such cases, a Membership Domain is used.

Membership Domains are named domains (UTF8Strings) with binary values stored in BitStrings to represent where the Policy Entity is used. A Policy Entity MAY appear in multiple Membership Domains.

This mechanism creates a compact bit pattern to be used which notes when a Policy Entity or Policy Group applies to to an Authorized User.

5. Groups and Membership AVPs

5.1. Base-Name AVP

The Base-Name AVP (AVP Code TBD1) is of type UTF8String and defines a group of Policy Entities, e.g. Filters [RFC7155] or Filter-Rules [RFC5777].

All Policy Entities with the same Base-Name MUST be of the same AVP type.

A Base-Name MAY be assigned at the creation of the Policy Entity or in a subsequent update but MUST only be assigned once, i.e. re-assignment of the Base-Name MUST NOT be allowed.

5.2. Policy-Membership AVP

The Policy-Membership AVP (AVP Code TBD2) is of type Grouped and specifies the Membership-Value and optionally the Membership-Domain and Base-Name for an Authorized User. It is defined as follows (per the grouped-avp-def of [RFC6733]):

```
Policy-Membership ::= < AVP Header: TBD2 >
                      { Membership-Value }
                      [ Membership-Domain ]
                      [ Base-Name ]
```

Multiple Policy-Membership values MAY be assigned to an Authorzied User. However, assigning multiple Policy-Memberships to an Authorized Users MAY delay policy enforcement as membership determination time is increased and SHOULD be avoided.

If multiple Policy-Memberships are assigned to an Authorized User, the Membership-Domain of each Policy-Membership value MUST be unique.

5.3. Membership-Assignment AVP

The Membership-Assignment AVP (AVP Code TBD3) is of type Grouped and specifies the Membership-Value and optionally the Membership-Domain and Base-Name for a Policy-Entity. It is defined as follows (per the grouped-avp-def of [RFC6733]):

```
Membership-Assignment ::= < AVP Header: TBD3 >
                          { Membership-Value }
                          { Match-Type }
                          [ Membership-Domain ]
                          [ Base-Name ]
```

Multiple Policy-Membership values MAY be assigned to a Policy Entity. If multiple Policy-Memberships are assigned, the Membership-Domain of each Membership-Assignment MUST be unique.

5.4. Membership-Domain AVP

The Membership-Domain AVP (AVP Code TBD4) is of type UTF8String and defines a membership set for a group of Policy Entities, e.g. Filters [RFC7155] or Filter-Rules [RFC5777], that are commonly applied to a set of Authorized Users.

5.5. Membership-Value AVP

The Membership-Value AVP (AVP Code TBD5) is of type OctetString and defines a membership of a Policy Entity or Authorized User.

Each bit of the OctetString represents a single position in the Membership-Domain set.

When two Membership-Values of different lengths are compared, the smaller Membership-Value is padded with '0' valued bits until it is the same length as the longer Membership-Value.

5.6. Match-Type AVP

The Match-Type AVP (AVP Code TBD6) is of type Enumerated and defines the type of Matching algorithm used for the Policy Entity.

When applying the Match-Type between the Membership-Value of Membership-Assignment (Policy Entity) and a Policy-Membership (Authorized User), the Membership-Domain MUST be the same, i.e. they are omitted or both MUST be present and have the same value.

Match-Types can be one of the following:

EQ 0

The Membership-Values are equal.

SUPER 1

The Membership-Assignment's Membership-Value is a superset of the Policy-Membership's Membership-Value, i.e. the may be equal.

PSUPER 2

The Membership-Assignment's Membership-Value is a proper superset of the Policy-Membership's Membership-Value.

SUB 3

The Membership-Assignment's Membership-Value is a subset of the Policy-Membership's Membership-Value, i.e. the may be equal.

PSUB 4

The Membership-Assignment's Membership-Value is a proper subset of the Policy-Membership's Membership-Value.

OVERLAP 5

The Membership-Assignment's Membership-Value has overlap with the Policy-Membership's Membership-Value. They may be equal or have some form of subset / superset relationship.

NONOVERLAP 6

The Membership-Assignment's Membership-Value has no intersection with the Policy-Membership's Membership-Value.

6. Lifecycle Considerations

Base Names are typically assigned when a Policy Entity is installed on the Diameter Client. Assignment MAY occur after installation but the impact of this is outside of the scope of this document.

Membership-Assignments MAY occur at any time in the lifecycle of the Policy Entity. However, there is no guarantee that resources exist on the Diameter Client to perform a re-evualation of the membership of all Authorized Users. A Diameter Server MUST NOT assume that re-evaluation will occur or that an evaluation will occur immediately.

Policy-Memberships MAY change at any time in the lifecycle of the Authorized User's session. It is expected that sufficient resources exist to perform a re-evaluation of applicable Policy Entities based upon Membership testing. If this cannot be done a Diameter Applicaiton level appropriate message MUST be sent to the Diamater Server.

Generally, Base-Names assignment SHOULD occur upon creation of a Policy Entity or the authorization of a User. Membership-Assignments SHOULD occur prior to an Authorized User being created with a Policy-Membership that would apply the Policy Entity to the Authorized User's session.

7. Example

7.1. Rule Sets

A policy administrator has defined three 'default rule sets' based upon various product options selected by a Customer. Each rule set consists of twenty Filter-Rules as defined in [RFC5777].

Rules that are part of Rule Set 1 are given a Membership-Value of 1, Rule Set 2 members are given the value 2 and Rule Set three members have a value of 4 in their respective Membership-Assignment values.

All Membership-Assignments have the Membership-Domain of "Product X" and a Match-Type of EQ (Equals).

When a User is Authorized for service usage, a Policy-Membership value is provided with the appropriate Membership-Value set to 1, 2 or 4 and a Membership-Domain of "Product X". The Diameter Client can then appropriately the correct 20 Filter-Rules.

7.2. Rule in multiple sets (1 Domain)

Expanding upon our example from above Section 7.1, a new Filter-Rule is added that is part of both Rule Set 1 and Rule Set 2.

According, the Membership-Assignment has a Membership-Domain of "Product X", a Membership-Value of 3 and a Match-Type of OVERLAP. Thus, any Policy-Membership whose Membership-Value is set to 1 or 2 will have this Filter-Rule applied.

7.3. 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
Base-Name	TBD1	Section 5.1	UTF8String
Policy-Membership	TBD2	Section 5.2	GROUPED
Membership-Assignment	TBD3	Section 5.3	GROUPED
Membership-Domain	TBD4	Section 5.4	UTF8String
Membership-Value	TBD5	Section 5.5	OctetString
Match-Type	TBD6	Section 5.6	Enumerated

7.4. Security Considerations

The use of Base-Names and Membership-Domain can unintentionally provide user information if it is too explicit, e.g. "Bobs' Policies". It is RECOMMENDED that an operator consider the values it assigns and ensure they provide no user or group speicific information.

As bit and test patterns the data provided by the Membership-Assignment and Policy-Membership AVPs provide more clues between an Operator and Authorized User's policy relationship. However, it is no different than if one has access to the information transmitted between the Diameter Client and Server today (if the Base-Names and Membership-Domains) follow the reommendations in this section.

In either case, access to the Diameter communications is still required.

The Security Considerations of the Diameter protocol itself have been discussed in [RFC6733]. The Diameter base protocol [RFC6733] requires that each Diameter implementation use underlying security; i.e., TLS/TCP, DTLS/SCTP or IPsec. Use of the AVPs defined in this document MUST take into consideration the security issues and requirements of the Diameter base protocol.

8. References

8.1. 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>.

[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>.

8.2. Informative References

[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>.

[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