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

L. Bertz
M. Bales
Sprint

June 29, 2017

Diameter Policy Groups and Sets
draft-bertz-dime-policygroups-04

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 December 31, 2017.

Copyright Notice

1. Introduction

As Users connect to a network, policy applications often apply common policies to them. In some cases policies are grouped and applied through the use of AVPs, e.g. 3GPP Base Name. Other options include sending identifiers, usually a list of integers, associated with rules to apply a group to a single user. This compacts the over the wire representation but requires strong coordination between policy based Clients and Servers.

Application of common policy if further limited when the filters overlap. This requires partitioning policies into non-overlapping namespaces, e.g. tables in a Software Defined Networking (SDN) switch. To reduce the need to partition sets of policies some SDN technologies, e.g. OpenFlow, rely on metadata that is applied as part of the filter or metadata that is specific to the packet, e.g. OpenFlow Registers.

This document defines grouping mechanisms to allow users or groups of users to share policies or groups of policies. The mechanism also extends filters to include a metadata matching field that permits filters that overlap at the protocol level to coexist in the same policy enforcement space.

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. This metadata is used as part of the filter or as user information when policy application occurs.

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. A Policy Entity's name MUST contain zero or 1 separator character '/'. The value before the separator is a Base Name. When no Base Name is provided, i.e. no separator is present. The value of a policy entity is considered to be part of the Base Name "" (empty string) for any matching purposes. Base Name values MUST NOT contain the '/' character.

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 bit strings to represent where the Policy Entity is used. A Policy Entity MAY appear in multiple Membership Domains.

Membership-Value is a compact bit pattern to be used which notes when a Policy Entity or Policy Group applies to to an Authorized User.

An Authorized User's memberships are assigned by a Policy-Membership. A Policy Entity is assigned membership via a Membership-Assignment. Multiple assignments may be applied to an Authorized User and Policy Entity but they MUST have unique Membership Domain values. It is also RECOMMENDED to avoid numerous Policy-Membership assignments for

an Authorized User as it delays computation of the Policy Entities that should be applied to their service.

Memberships are matched by understanding the relationship between their values which are represented as sets of bits. These relationships are descibed as Match-Types and are specified as set relations, e.g. subset, superset, etc. Figure 1 shows the reference model.

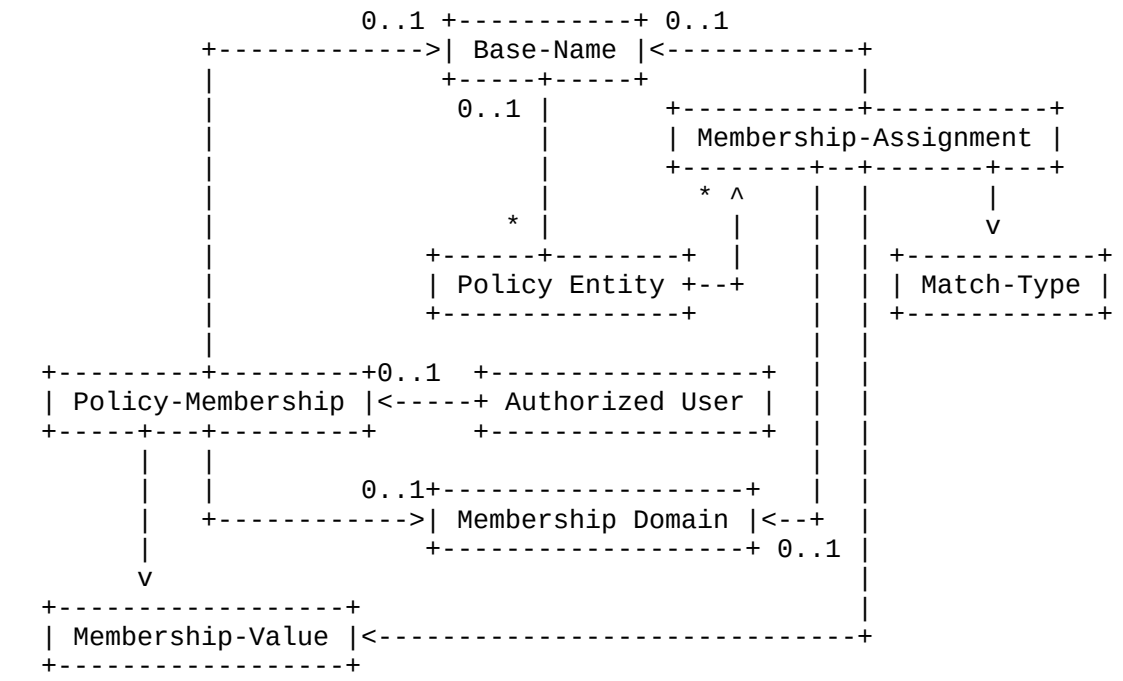

Figure 1: Reference Model

To determine if a Rule is assigned to the User the following conditions MUST be true at least one Membership-Assignments must exist where

Policy-Membership’s Membership-Domain = Membership-Assignment’s Membership-Domain

Policy-Membership’s Membership-Value MUST satisfy the Match-Type for the Membership-Assignments’ Membership-Value

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-Name 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. Examples

7.1. Rule Sets

A policy administrator defines Product X with 3 separate rules sets. The administrator creates the Membership-Domain "Product X" and Membership-Values of 1, 2 and 4 representing separate rule sets. For this example each rule set consists of twenty Filter-Rules as defined in [RFC5777].

Each Rule Set is assigned a Membership-Value. Rule Set 1 is assigned a Membership-Value of 1, Rule Set 2 members is assigned the value 2 and Rule Set three members are assigned a value of 4. All Membership-Assignments have the Membership-Domain of "Product X" and a Match-Type of EQ (Equals).

The policy administrator defines three users. User 1 is assigned the Membership-Domain of "Product X"" and Membership-Value of 1. User 2 is assigned a Membership-Domain of "Product X" and a Membership-Value of 2. User 3 is assigned a Membership-Domain of "Product X"" and Membership-Value of 4.

7.2. Rule in multiple sets (1 Domain)

Expanding upon our example from above Section 7.1, a new Filter-Rule is added that shall be part of Users with either Rule Set 1 or Rule Set 2 of Product X.

Accordingly, the policy administrator defines the Membership-Assignment having 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. Default Route (Overlapping) Rules

A common traffic rule is the default (all traffic) rule. It is often used as the lowest priority rule in a policy enforcement session. Even though the rule is typically the same, e.g. "any any", the actions taken may vary, e.g. deny traffic, permit traffic, set quality of service. To distinguish the rules the use of the

Membership-Domain in the Membership-Assignment even when the Membership-Value MAY be the same.

Within the enforcement point, for each overlapping Match-Type can be set to OVERLAP and contain all bits where the rule applies in its Membership-Value. In general, the Membership-Value MUST be NOT overlap with other default rules or a Precedence MUST be followed.

In the case where a Filter-Rule [RFC5777] is used, the Match-Type and Membership-Value can be used as part of the Classifier AVP.

8. 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

9. 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.

10. References

10.1. 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>.

10.2. 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>.

Authors' Addresses

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

Email: lylebe551144@gmail.com

Mark Bales
Sprint
6220 Sprint Parkway
Overland Park, KS 66251
United States

Email: yellowjeep2017@gmail.com