Network Working Group DeKok, Alan
INTERNET-DRAFT FreeRADIUS
Updates: 5176 J. Korhonen
Category: Standards Track Nokia Siemens Networks
<draft-dekok-radext-coa-proxy-00.txt>
3 July 2014

Dynamic Authorization Proxying in Remote Authorization Dial-In User Service Protocol (RADIUS)
draft-dekok-radext-coa-proxy-00.txt

Abstract

RFC 5176 defines Change of Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. Section 3.1 of that document suggests that proxying these messages is possible, but gives no guidance as to how that is done. This specification corrects that ommission.

Status of this Memo

This Internet-Draft will expire on January 4, 2015.

Copyright Notice

Table of Contents

1. Introduction

RFC 5176 [RFC5176] defines Change of Authorization (CoA) and Disconnect Message (DM) behavior for RADIUS. Section 3.1 of that document suggests that proxying these messages is possible, but gives no guidance as to how that is done. This ommission means that proxying of CoA packets is, in practice, impossible.

We correct that ommission here.

1.1. Terminology

This document frequently uses the following terms:

Network Access Identifier

The Network Access Identifier (NAI) is the user identity submitted by the client during network access authentication. The purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request. Please note that the NAI may not necessarily be the same as the user's email address or the user identity submitted in an application layer authentication.

Network Access Server

The Network Access Server (NAS) is the device that clients connect to in order to get access to the network. In PPTP terminology, this is referred to as the PPTP Access Concentrator (PAC), and in L2TP terminology, it is referred to as the L2TP Access Concentrator (LAC). In IEEE 802.11, it is referred to as an Access Point.

Home Network

The home network of a user.

Visited Network

The network which is accessed by a user, when that network is not their home network.

1.2. 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].

2. Problem Statement

This section describes how RADIUS proxying works, how CoA packets work, and why CoA proxying does not work in the current system.

2.1. Typical RADIUS Proxying

When a RADIUS server proxies an Access-Request packet, it typically does so based on the contents of the User-Name attribute, which contains Network Access Identifier [NAI]. Other methods are possible, but we restrict ourselves to the most common usage.

The proxy server looks up the "Realm" portion of the NAI in a logical AAA routing table, as described in Section 3 of [NAI]. The entry in that table is the "next hop" to which the packet is sent. This "next hop" may be another proxy, or it may be the home server for that realm.

The "next hop" may perform the same Realm lookup, and the proxy the packet also. Alternatively, if the "next hop" is the Home Server for that realm, it will typically authenticate the user, and respond with an Access-Accept, Access-Reject, or Access-Challenge.

The response can be returned from the home server to the visited network, because each proxy server tracks the requests it has forwarded. When a response packet is by the proxy, it is matched to an incoming request, which lets the proxy forward the response to the source of the original request.

2.2. CoA Processing

[RFC5176] describes how CoA clients (often RADIUS servers) will send packets to CoA servers (often RADIUS clients). In typical use, CoA packets are sent within one network. That is, within the same "Realm". When used within one "Realm", there is only one "hop" for packets to take, so no proxying is necessary.

2.3. Failure of CoA Proxying

In the case of CoA proxying, the above scenarios fail. CoA packets may be sent minutes to hours after reception of the original Access-Request. In addition, the packet codes are different, so there is no way to match a CoA-Request packet to a particular Access-Request packet. There is therefore no "reverse path" for the CoA packet to follow.

As with Access-Request proxying, CoA proxying can be done done between Realms. There exists potentially multiple "hops" for packets

to follow. Packets cannot be forwarded to the Visited Network, based on the contents of the User-Name attribute, as that contains the Realm of the Home Network.

The conclusion is therefore that CoA proxying is impossible when using behavior defined in [RFC5176]. There is, however a solution.

3. How to Perform CoA Proxying

The solution is seen in the Operator-Name attribute defined in [RFC5580], Section 4.1. We repeat portions of that definition here for clarity:

> This attribute carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network.

Followed by a description of the REALM namespace:

> REALM ('1' (0x31)):
>
> The REALM operator namespace can be used to indicate operator names based on any registered domain name. Such names are required to be unique, and the rights to use a given realm name are obtained coincident with acquiring the rights to use a particular Fully Qualified Domain Name (FQDN). ...

In short, the Operator-Name attribute contains the an ASCII "1", followed by the Realm of the Visited Network. e.g. for the "example.com" realm, the Operator-Name attribute contains the text "1example.com". This information is precisely what we need to perform CoA proxying.

The only missing information is which NAS is managing the user. We may expect that the Visited Network will track this information, but there is no requirement for it to do so. We therefore need an additional attribute to contain this information.

3.1. Operator-NAS-Identifier

The Operator-NAS-Identifier attribute contains opaque information identifying a NAS. It MAY appear in the following packets: Access-Request, Accounting-Request, CoA-Request, DM-Request. Operator-NAS-Identifier MUST NOT appear in any other packet.

Operator-NAS-Identifier MAY occur in a packet if the packet also contains an Operator-Name attribute. Operator-NAS-Identifier MUST NOT appear in a packet if there is no Operator-Name in the packet.

Operator-NAS-Identifier MUST NOT occur more than once in a packet.

When an Operator-NAS-Identifer attribute is added by a proxy in a Visited Network, the following attributes MUST be deleted: NAS-IP-Address, NAS-IPv6-Address, NAS-Identifier. The proxy MUST then add a NAS-Identifier attribute, in order satisfy the requirments of Secton 4.1 of [RFC2865], and of [RFC2866]. We suggest that the contents of the NAS-Identifier be the Realm name of the Visited Network.

Description

An opaque token describing the NAS a user has logged into.

Type

TBD. To be assigned by IANA

Length

TBD. Depends on IANA allocation.

Implementations supporting this attribute MUST be able to handle between one (1) and twenty (20) octets of data. Implementations creating an Operator-NAS-Identifier SHOULD NOT create attributes with more than twenty octets of data. A twenty octet string is more than sufficient to individually address all of the NASes on the planet.

Data Type

string. See [DATA] Section 2.6 for a definition.

Value

The contents of this attribute are an opaque token interpretable only by the Visited Network. The attribute MUST NOT contain any secret or private information.

4. Functionality

This section describes how the two attributes work together to permit CoA proxying.

4.1. User Login

The user logs in. When a Visited Network sees that the packet is proxied, it adds an Operator-Name with "1" followed by it's own realm

name. It MAY also add an Operator-NAS-Identifier.

The proxies then forward the packet. They MUST NOT delete or modify Operator-Name and/or Operator-NAS-Identifier.

The Home Server records both Operator-Name and Operator-NAS-Identfier along with other information about the users session.

4.2. CoA Proxing

When the Home Server decides to disconnect a user, it looks up the Operator-Name and Operator-NAS-Identifer, along with other user session identifiers as described in [RFC5176]. It then looks up the Operator-Name in the logical AAA routing table to find the CoA server for that realm (which may be a proxy). The CoA-Request is then sent to that server.

The CoA server receives the request, and if it is a proxy, performs a similar lookup as done by the Home Server. The packet is then proxied repeatedly until it reaches the Visited Network.

If the proxy cannot find a destination for the request, or if no Operator-Name attribute exists in the request, the proxy returns a CoA-NAK with Error-Cause 502 (Request Not Routable).

The Visited Network recieves the CoA-Request packet, and uses the Operator-NAS-Identifier attribute to determine which local CoA server (i.e. NAS) the packet should be sent to.

If no CoA server can be found, the Visited Network return a CoA-NAK with Error-Cause 403 (NAS Identification Mismatch).

Any response from the CoA server (NAS) is returned to the Home Network.

5. Security Considerations

This specification incorporates by reference the [RFC6929] Section 11. In short, RADIUS has known issues which are discussed there.

This specification adds one new attribute, and defines new behavior for RADIUS proxying. As this behavior mirrors existing RADIUS proxying, we do not believe that it introduces any new security issues.

Operator-NAS-Identifier should remain secure. We don't say how.

6. IANA Considerations

IANA is instructed to allocated one new RADIUS attribute, as per Section 3.1, above.

7. References

7.1. Normative References

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

[RFC2865]
Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC5580]
Tschofenig H., Ed. "Carrying Location Objects in RADIUS and Diameter", RFC 5580, August 2009.

[RFC6929]
DeKok A. and Lior, A., "Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions", RFC 6929, April 2013.

[NAI]
DeKok A., "The Network Access Identifier", draft-ietf-radext-nai-06.txt, June 2013.

[DATA]
DeKok A., "Data Types in the Remote Authentication Dial-In User Service Protocol (RADIUS)", draft-dekok-radext-datatypes-04.txt, Juen 2014

7.2. Informative References

[RFC2866]
Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC5176]
Chiba, M. et al, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

Acknowledgments

Stuff

Authors' Addresses

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org

Jouni Korhonen
Nokia Siemens Networks
Linnoitustie 6
Espoo FI-02600
Finland

EMail: jouni.nospam@gmail.com