Hewlett Packard Enterprise

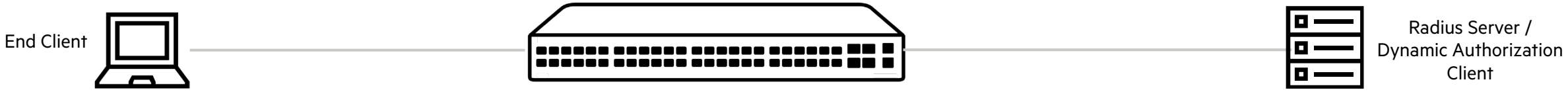
HPE aruba networking

AOS-CX 10.13 Update: CISCO VSA Support for Radius Dynamic Authorization

Shobana Nandakumar , Technical Marketing Engineer

November 2023

Radius Dynamic Authorization



RADIUS Dynamic Authorization provides the ability to make changes to an authenticated user/device session.

Radius Dynamic Authorization Types

- Disconnecting a session -
  - **Disconnect Message**(DM) cause user session(s) to be terminated immediately.
- Updating Authorization for the session -
  - **CoA (Change-of-Authorization)** modify session authorization attributes.

Mandatory attributes for any CoA or DM Request -

- **NAS-IP-Address or NAS-Identifier**: Network access server IP address or the hostname must be specified
- **NAS-Port-Id + Calling-Station-Id or NAS-Port + Calling-Station-Id or Accounting Session-id**: Client connected port number or the port id with Mac address of the authenticated client or accounting session-id of the authenticated client
- End client should be in the authenticated state and profile should be in the applied state for CoA and DM to work.

CISCO VSA Support for Radius Dynamic Authorization

CISCO ISE Adaptive Network Control(ANC) could use only CISCO VSAs to perform Radius Dynamic authorization requests to even third-party devices.

To accommodate the interop with CISCO ISE ANC, following **CISCO VSAs are supported in DM and CoA request of AOS-CX Switches**

- Cisco-AVPair='subscriber:command=bounce-host-port'
- Cisco-AVPair='subscriber:command=disable-host-port'
- Cisco-AVPair='subscriber:command=reauthenticate'
- Cisco-AVPair='subscriber:reauthenticate-type=<last|rerun>'

It is observed CISCO ANC sends the above authorization VSAs only in DM instead of CoA.

According to the RFC5176 Dynamic Authorization enforcement default mode – strict , no authorization attributes are allowed as part of DM. Only when enforcement mode is loose, authorization attributes are accepted in DM.

Enhancement - Added a configuration to have **rfc5176-enforcement-mode** for Dynamic Authorization Client(DAC). The CISCO AVP VSAs are supported as part of DM only when the DAC configuration in AOS-CX switches is with **rfc5176-enforcement-mode** as loose.

Supported Platforms – 10000,8360,8325,8100,6400,6300,6200,6100,6000 and 4100i

Configuration and Show Commands - CLI

- To Configure and View the enforcement mode of RFC5176 -

```
switch(config)#  radius dyn-authorization client <radius-server-ip> rfc5176-enforcement-mode
   strict    Strict enforcement of the RFC5176
   loose     Non-strict enforcement of the RFC5176  <cr>
```

```
switch(config)# show radius dyn-authorization
Status and Counters - RADIUS Dynamic Authorization Information

  RADIUS Dynamic Authorization                   : Disabled
  RADIUS Dynamic Authorization UDP Port          : 3799
  Invalid Client Addresses in CoA Requests       : 0
  Invalid Client Addresses in Disconnect Requests: 0

Dynamic Authorization Client Information
========================================

IP Address                : 20.1.1.10
VRF                       : default
TLS Enabled               : No
Replay Protection         : Disabled
Time Window               : 300
rfc5176-enforcement-mode  : loose
Disconnect Requests       : 0
Disconnect ACKs           : 0
Disconnect NAKs           : 0
CoA Requests              : 0
CoA ACKs                  : 0
CoA NAKs                  : 0
Shared-Secret             : AQBapTEbXqH6f39Si2ng9AjEcFgSrwf6ebsuD6VT/GYvCcOnCAAAAJvUyahRENFH
```

REST API - POST

- To configure the enforcement mode of RFC5176 -

POST /system/vrfs/{VRF.name}/radius_dynamic_authorization_clients

Parameters | Try it out

Name	Description
VRF.name * required string *(path)*	Reference Resource: VRF VRF identifier. Should be alphanumeric. VRF names must be unique. VRF.name - Reference Resource: [VRF](#/VI

Request body | application/json

Example Value | Schema

```
{
  "address": "string",
  "connection_type": "udp",
  "replay_protection_enable": true,
  "rfc5176_enforcement_mode": "strict",
  "secret_key": "string",
  "time_window": 0,
  "vrf": "Unknown Type: URI"
}
```

REST API - GET

- To View the enforcement mode of RFC5176 -

Radius_Dynamic_Authorization_Client

GET /system/vrfs/{VRF.name}/radius_dynamic_authorization_clients

Parameters

Name	Description
VRF.name * required **string** *(path)*	Reference Resource: VRF VRF identifier. Should be alphanumeric. VRF names must be unique. default
attributes **array[string]** *(query)*	Columns to display. time_window rfc5176_enforcement_mode connection_type statistics
depth **integer** *(query)*	Depth to traverse. 2

Curl

```
curl -X GET "https://10.6.8.6/rest/v10.13/system/vrfs/default/radius_dynamic_authorization_clients?attributes=rfc5176_enforcement_mode&depth=2" -H  "accept: application/json" -H  "x-csrf-token: -PByXKQpwNQdtcIHDzxIjg==" 
```

Request URL

https://10.6.8.6/rest/v10.13/system/vrfs/default/radius_dynamic_authorization_clients?attributes=rfc5176_enforcement_mode&depth=2

Server response

Code	Details
200	Response body

```
{
  "20.1.1.10,udp": {
    "rfc5176_enforcement_mode": "strict"
  }
}
```

Download

Thank you

© 2023 Hewlett Packard Enterprise Development LP