Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update:
Optimizing client authentication event logs

Priyadarshini Senthil Kumar, TME

Nov 2023

Agenda

1	Overview
2	Configuration
3	Details

Overview

Feature details

Additional event logs have been implemented for Radius access requests and responses to the switch.

These logs address the need for comprehensive tracking in scenarios where radius servers are involved and provide better visibility to Central.

Why is it important?

Enhance the platform's ability to capture and log critical information during authentication processes in case of 802.1X as well as MAC-Authentication.

Supported platforms

Feature supported on all Port Access capable platforms 10000, 4100i, 6000, 6100, 6200, 6300, 6400, 8325, 8360, 8100 & AOS-CX Simulators

This Data will be reported to the CNX in future.

Configuration - CLI

```
Bldg1-Acc-6300-VSF(config-if)# port-access event-log client
```

New CLI from 10.13 that enables Radius server details in event logs

```
Bldg1-Acc-6300-VSF(config)# show radius-server
Unreachable servers are preceded by *
******* Global RADIUS Configuration *******

Shared-Secret: None
Timeout: 10
Auth-Type: pap
Retries: 3
Initial TLS Connection Timeout: 30
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 3
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds): 300
Number of Servers: 1
AAA Server Status Trap: Disabled

-------------------------------------------------------------------------------------------------
-----------------------------------------
SERVER NAME                                  | TLS   | PORT | VRF
-------------------------------------------------------------------------------------------------
-----------------------------------------
cppm.tmelab.net                              |       | 1812 | mgmt
-------------------------------------------------------------------------------------
```

Details

Modified Event Logs:

The following event logs have been modified to accommodate the enhanced security features:

- PORTCLIENT_EVENT_MAC_AUTH_REQUEST
- PORTCLIENT_EVENT_MAC_AUTH_RESPONSE_RECEIVED
- PORTCLIENT_EVENT_DOT1X_AUTH_REQUEST
- PORTCLIENT_EVENT_DOT1X_AUTH_RESPONSE_RECEIVED

Details

- Event logs Captured for MAC and 802.1X Authentication that logs the radius server details.

```
Event|10530|LOG_INFO|CDTR|1|802.1x Authentication triggered for client 00:50:56:9e:3d:25 on port 1/1/1 with ID 36 to server (cppm.tmelab.net:1812, udp, vrf mgmt)

2023-11-20T00:53:02.852722-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10531|LOG_INFO|CDTR|1|802.1x Authentication succeeded for client 00:50:56:9e:3d:25 on port 1/1/1 with ID 25 from server (cppm.tmelab.net:1812, udp, vrf mgmt)

2023-11-02T02:41:21.597124-07:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10533|LOG_INFO|CDTR|1|Interface 2/1/3 is blocked by port-access

2023-11-02T02:41:21.623182-07:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10534|LOG_INFO|CDTR|1|Interface 2/1/3 is unblocked by port-access

2023-11-13T09:56:21.683923-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10509|LOG_ERR|CDTR|1|Client limit exceeded on port lag1, caused by an unauthenticated client a6:c8:11:b0:fe:f9

2023-11-20T23:10:09.323374-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10512|LOG_INFO|CDTR|1|Client with MAC address 00:50:56:9e:3d:25 learnt on port 1/1/1

2023-11-20T08:10:37.031639-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10527|LOG_INFO|CDTR|1|MAC Authentication triggered for client 00:50:56:9e:3d:25 on port 1/1/1 with ID 48 to server (cppm.tmelab.net:1812, udp, vrf mgmt)

2023-11-20T08:31:06.197663-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10528|LOG_INFO|CDTR|1|MAC Authentication succeeded for client 00:50:56:9e:3d:25 on port 1/1/1 with ID 59 from server (cppm.tmelab.net:1812, udp, vrf mgmt)

2023-11-20T08:56:06.185759-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10513|LOG_INFO|CDTR|1|Client with MAC address 00:50:56:9e:3d:25 deleted on port 1/1/1.

2023-11-06T04:53:17.821711-08:00 Bldg1-Acc-6300-VSF port-accessd[5220]: Event|10507|LOG_INFO|CDTR|1|Clients using policy reflexive were logged-off due to a configuration change in the policy
```

Thank you

aruba_switching_tme@hpe.com

© 2023 Hewlett Packard Enterprise Development LP