HPE6-A48 Q&As

Aruba Certified Mobility Expert 8 Written Exam

Pass HP HPE6-A48 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Refer to the exhibit.

```
(MC2) #show auth-tracebuf mac 70:4d:7b:10:9e:c6 count 27
Warning: user-debug is enabled on one or more specific MAC addresses:
         only those MAC addresses appear in the trace buffer.

Auth Trace Buffer
-----------------------------
Jun 29 20:56:51  station-up      *    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -     wpa2  aes
Jun 29 20:56:51  eap-id-req     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1  5
Jun 29 20:56:51  eap-start      ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              - -
Jun 29 20:56:51  eap-id-req     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1  5
Jun 29 20:56:51  eap-id-resp    ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1  7     it
Jun 29 20:56:51  rad-req        ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              42 174  10.1.140.101
Jun 29 20:56:51  eap-id-resp    ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              1  7     it
Jun 29 20:56:51  rad-resp       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      42  88
Jun 29 20:56:51  eap-req        <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2  6
Jun 29 20:56:51  eap-resp       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              2  214
Jun 29 20:56:51  rad-req        ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43  423  10.1.140.101
Jun 29 20:56:51  rad-resp       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      43  228
Jun 29 20:56:51  eap-req        <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3  146
Jun 29 20:56:51  eap-resp       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              3  61
Jun 29 20:56:51  rad-req        ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44 270  10.1.140.101
Jun 29 20:56:51  rad-resp       <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      44  128
Jun 29 20:56:51  eap-req        <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4  46
Jun 29 20:56:51  eap-resp       ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4  46
Jun 29 20:56:51  rad-req        ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45  255 10.1.140.101
Jun 29 20:56:51  rad-accept     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0/RADIUS1      45  231
Jun 29 20:56:51  eap-success    <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0              4  4
Jun 29 20:56:51 user repkey change * 70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0          65535  -   204c0306e790000000170008
Jun 29 20:56:51 macuser repkey change * 70:4d:7b:10:9e:c6  70:3a:0e:5b:0a:c0     65535  -  70:4d:7b:10:9e:c6
Jun 29 20:56:51  wpa2-key1     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   117
Jun 29 20:56:51  wpa2-key2     ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   117
Jun 29 20:56:51  wpa2-key3     <-    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   151
Jun 29 20:56:51  wpa2-key4     ->    70:4d:7b:10:9e:c6 70:3a:0e:5b:0a:c0               -   95
```

A network administrator is validating client connectivity and executes the show command shown in the exhibit. Which authentication method was used by the wireless station?

A. 802.1X user authentication

B. EAP authentication

C. 802.1X machine authentication

D. MAC authentication

Correct Answer: C

QUESTION 2

Refer to the exhibit.

```
(MC1) [MDC] #show ip access-list no-webapps

ip access-list session no-webapps
no-webapps
----------
```

Priority	Source	Destination	Service	Application	Action	TimeRange	Log	Expired	Queue	TOS	8021P	Blacklist	Mirror	DisScan	IPv4/6	Contract
1	user	any		app facebook	deny send-deny-response					Low						4
2	user	any		app youtube	deny send-deny-response					Low						4
1	user	any		app netflix	deny send-deny-response					Low						4

A network administrator completes the initial configuration dialog of the Mobility Controllers (MCs) and they join the Mobility Master (MM) for the first time. After the MM-MC association process, the network administrator only creates AP groups, VAPs, and roles. Next, the network administrator proceeds with the configuration of the policies and creates the policy shown in the exhibit.

Which additional steps must be done to make sure this configuration takes effecr over the contractor users?

A. Apply the policy in the contractors user role. Enable deep packet inspection.

B. Apply the policy in the contractors user role. Enable deep packet inspection. Reload the MCs.

C. Enable the firewall visibility. Enable web-content classification Reload the MCs.

D. Enable firewall visibility Enable web-content classification Reload the MMs.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

(MC14-1) #show log security 180

Jul 16 01:09:55 :124004: <3573> <DBUG> |authmgr| Select server for method=802.1x, user=host/wireless14.training.arubanetworks.com, essid=Corp-network, server-group=CAMPUS, last_srv <>
Jul 16 01:09:55 :124038: <3573> <INFO> |authmgr| Reused server ClearPass for method=802.1x; user=host/wireless14.training.arubanetworks.com, essid Corp-network, domain=<>, server-group=CAMPUS
Jul 16 01:09:55 :124004: <3573> <DBUG> |authmgr| aal_auth_raw (1399) (INC) : os_auths 1, s ClearPass type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:09:55 :124004: <3573> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass type 2 inservice 1 markedD 0
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=18, server=ClearPass, IP=10.254.1.23, server-group=CAMPUS, fd=87
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass: 10.254.1.23:1812 id:18, len:249
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name: host/wireless14.training.arubanetworks.com
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.100
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 704D7B109EC6
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 204C0306E5C0
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\006
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-network
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP21
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid length – Don't send it)
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: phu\025\347\376\016\030 \253a-\014a\033\200\234
Jul 16 01:09:55 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_sequence.c:117] seq_num_timeout_handler: Freed 0 entries
Jul 16 01:10:00 :124004: <3573> <WARN> |authmgr| |aaa| RADIUS server ClearPass server-group CAMPUS – 10.254.1.23-1812 timoeout for client=70:4d:7b:10:9e:c6 auth method 802.1x
Jul 16 01:10:00 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_server.c:1203] Sending radius request to ClearPass server-group CAMPUS -10.254.1.23-1812 (retry1)
Jul 16 01:10:00 :124004: <3573> <DBUG> |authmgr| APAE_Aborting_Tineout (5076) (DEC) : os_auths 0, s ClearPass type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:10:00 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_request.c:95] Find Request: id=18, server=(null), IP= 10.254.1.23, server-group=(null) fd=87
Jul 16 01:10:00 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_request.c:104] Current entry: server= (null), IP= 10.254.1.23, server-group=(null), fd=87
Jul 16 01:10:00 :121014: <3573> <ERRS> |authmgr| |aaa| Received invalid reply digest from RADIUS server
Jul 16 01:10:00 :121031: <3573> <DBUG> |authmgr| |aaa| [rc_request.c:48] Del Request: id=18, server=ClearPass, IP= 10.254.1.23, server-group=CAMPUS fd=87
Jul 16 01:10:00 :121031: <3573> <DBUG> |authmgr| |aaa| [rc api.c:1228] Bad or unknown response from AAA server

A network administrator deploys a new WLAN named Corp-Network. The security suite is WPA2 with 802.1X. A new ClearPass server is used as the authentication server. Connection attempts to this WLAN are rejected, and no trace of the attempt is seen in the ClearPass Policy Manager Access Tracker. However, the network administrator is able to see the logs shown in the exhibit.

What must the network administrator do to solve the problem?

A. Add the correct network device IP address in ClearPass.

B. Change the ClearPass server IP address in the MC.

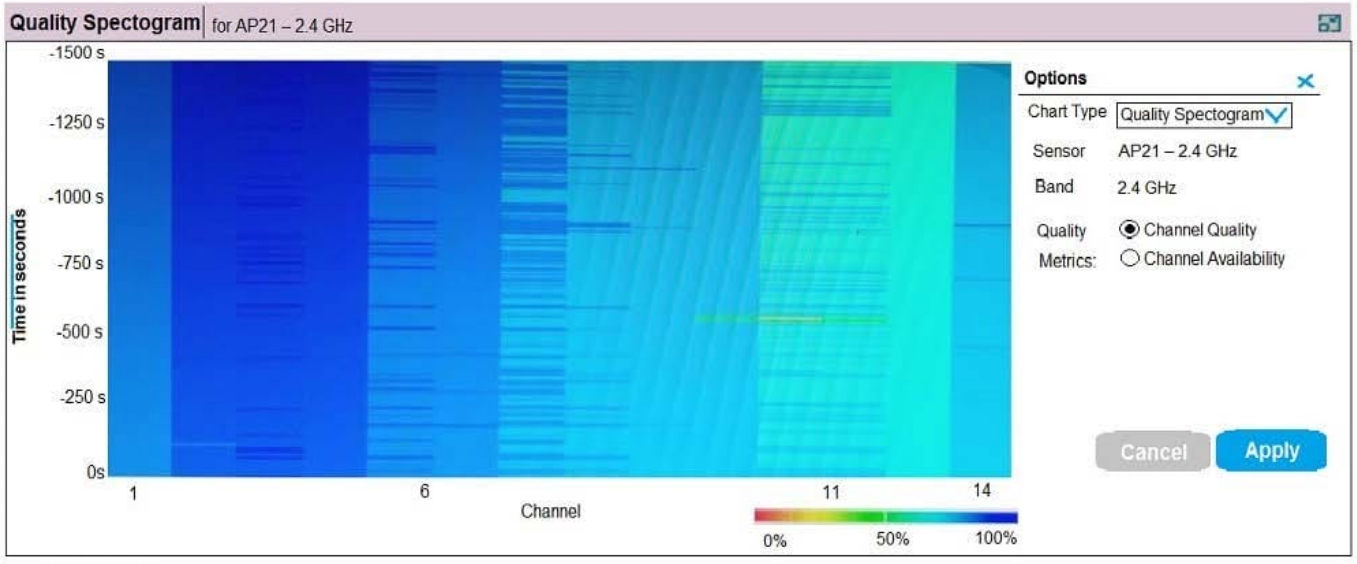
C. Fix the RADIUS shared secret in the MC.

D. Disable machine authentication in the MC and client PC.

Correct Answer: D

QUESTION 4

Refer to the exhibit.



(A48.01114442)

Based on the output shown in the exhibit, which channel offers the highest quality?

A. Channel 1

B. Channel 6

C. Channel 11

D. Channel 14

Correct Answer: C

QUESTION 5

Refer to the exhibit.

(MM) [mynode] #show airmatch event all-events ap-name AP2

Band	Event Type	Radio	Timestamp	Chan	CBW	New Chan	New CBW	APName
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-25_07:50:05	100	80MHz	149	80MHz	AP2
6GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-24_07:48:42	124	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-23_16:44:36	100	80MHz	124	80MHz	AP2
5GHz	NOISE_DETECT	38:17:c3:10:17:30	2018-07-20_19:12:34	157	80MHz	100	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_10:02:30	100	80 MHz	157	80MHz	AP2
5GHz	RADAR_DETECT	38:17:c3:10:17:30	2018-07-20_08:34:31	56	80 MHz	100	80MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-25_08:31:31	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:34	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-24_07:46:33	6	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:13:15	11	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-23_15:12:12	1	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:27	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-20_08:07:26	6	20MHz	11	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:45	1	20MHz	6	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_19:22:44	11	20MHz	1	20MHz	AP2
2GHz	RADAR_DETECT	38:17:c3:10:17:40	2018-07-19_10:45:23	1	20MHz	11	20MHz	AP2

A network administrator deploys a Mobility Master (MM)-Mobility Controller (MC) network with APs in different locations. Users in one of the locations report that the WiFi network works fine for several hours, ang then they are suddenly disconnected. The symptom may happen at any time, up to three times every day, and lasts no more than two minutes.

After some research, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, the network administrator logs into the MM and reviews the output shown in the exhibit.

Based on this information, what is the most likely reason users get disconnected?

A. AirMatch is applying a scheduled optimization solution.

B. Users in the 2.4 GHz band are being affected by high interference.

C. Adpative Radio Management is reacting to RF events.

D. AirMatch is reacting to non-scheduled RF events.

Correct Answer: B