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.pass4itsure.com/hpe6-a48.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibits. Exhibit1

```
(MC1) (MDC) #show ap database

AP Database
-------------------
Name   Group          AP Type   IP Address     Status        Flags   Switch IP      Standby IP
-----  -----          -------   ----------     ------        -----   ---------      ----------
AP1    MainCampus-SC-B1  335    10.1.145.150   Up 4h:14m:10s  2I     10.1.140.100   10.1.140.101
AP12   CAMPUS            335    10.1.146.150   Up 13m:19s     2      10.1.140.100   10.1.140.101

Flags: 1 = 802.1x, authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1.= 802.1x use factory cert; 2 = Using IKE version 2
       B = Built-in AP; C = Cellular RAP; D = Dirty or no config
       E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
       G = No such group; I = Incative; J = USB cert at AP; L = Unlicnesed
       M = Mesh node
       N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
       S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
       Y = Mesh Recovery
       c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
       i = Indoor; o = Outdoor; s = LACP striping; u = Custom-cert RAP; z = Datazone AP

Total APs:2
```

Exhibit 2

```
(MC11) [mynode]  #show ap database

AP    Database
----------------------
Name               Group     AP Type   IP Address          Status      Flags   Switch IP      Standby IP
--------           ----------  ------------  --------------------  --------  --------  ---------------  ---------------
70:3a:0e:cd:b0:a4  default   335       10.1.145.150        Down        2       10.254.13.14   0.0.0.0
a8:bd:27:c5:c3:3a  default   335       10.1.147.2          Down        2       10.254.13.14   0.0.0.0
AP12               CAMPUS    335       10.1.146.150        Up 21m:37s  2z      10.254.13.14   0.0.0.0
```

Based on outputs shown in the exhibits, what is the reason that AP12 is seen by two different controllers?

A. AP12 connects to a high availability group. MC1 is the active controller, and MC11 is the standby controller.

B. AP12 is a multizone AP. MC1 is part of the primary zone, and MC11 is part of the datazone.

C. AP12 connects to an MC cluster. MC1 is the A-AAC, and MC2 is S-AAC.

D. AP12 is in the middle of the boot process. MC1 is the master IP controller, and MC11 is the LMS IP controller.

Correct Answer: B

QUESTION 2

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 3

Refer to the exhibits.

Exhibit 1

```
(MC1) [MDC] #show ip interface brief
```

Interface	IP Address / IP Netmask	Admin	Protocol	VRRP-IP
vlan 140	10.1.140.100 / 255.255.255.0	up	up	
vlan 1	unassigned / unassigned	down	down	
loopback	10.1.140.99 / 255.255.255.255	up	up	

Exhibit 2

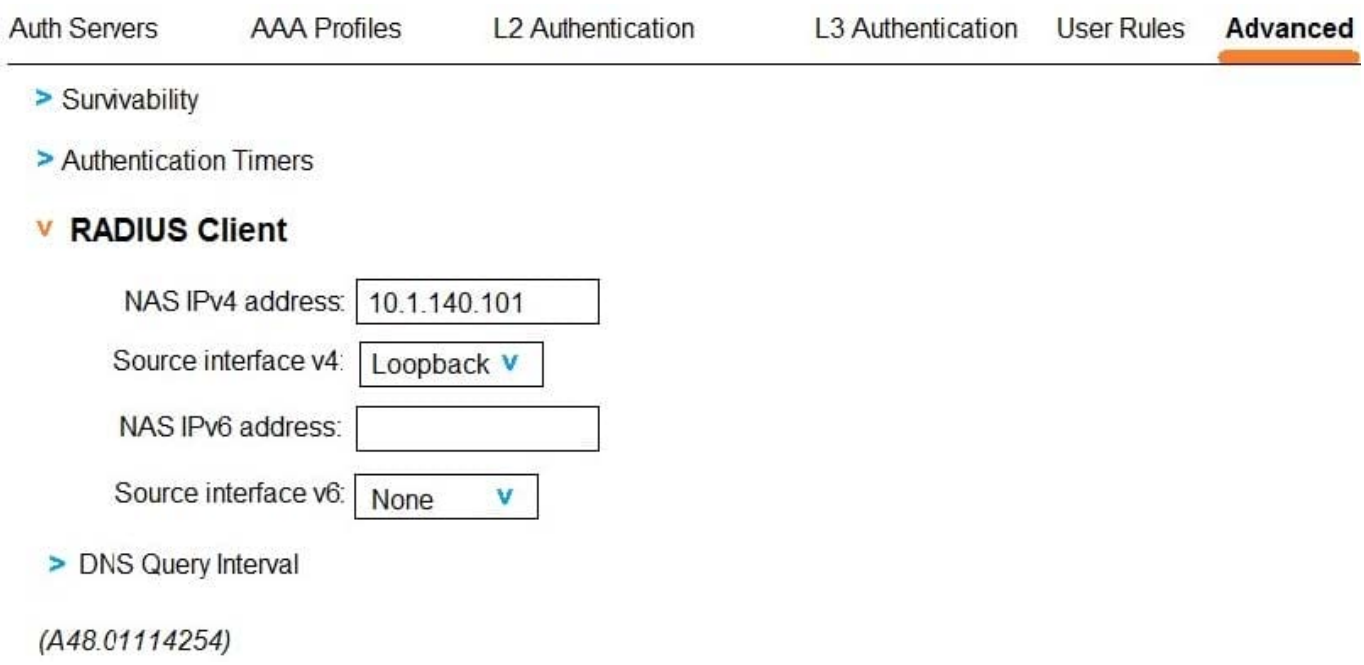
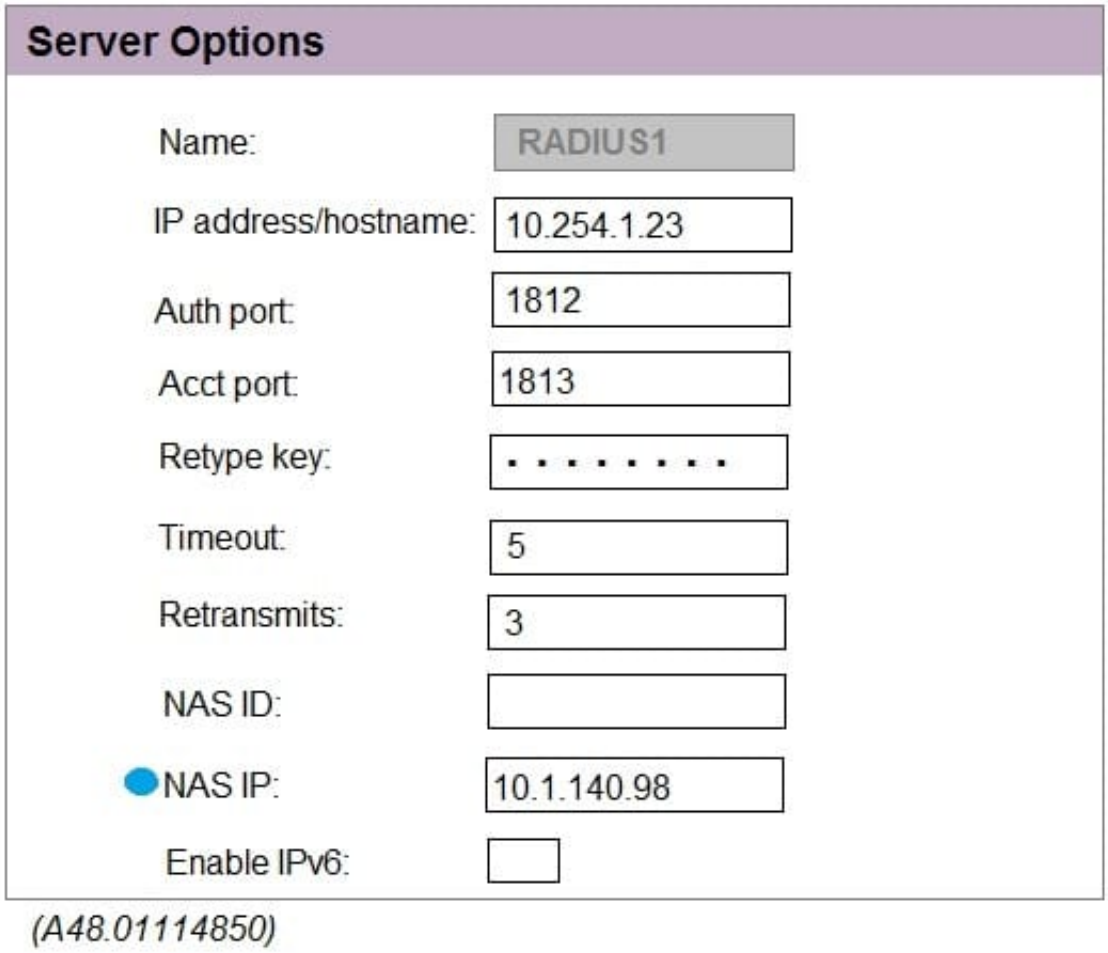


Exhibit 3



A network administrator must ensure that a ClearPass server can receive the RADIUS authentication request from a single Mobility Controller (MC) managed by a Mobility Master (MM). Based on the exhibits, what is the value of NAS-IP contained in the RADIUS access requests?

A. 10.1.140.98

B. 10.1.140.99

C. 10.1.140.100

D. 10.1.140.101

Correct Answer: A

QUESTION 4

A network administrator implements a SIP-based IP telephone solution. The objective is to ensure that APs use 100% of their airtime for network access whenever a voice call is taking place, to minimize communication delays. The network administrator also wants to ensure that a log entry is generated when voice calls occur.

Which setup accomplishes these tasks?

A. ip access-list session voice user any svc-rtsp permit log queue high user any svc-sip-udp permit log queue high

B. ip access-list session voice user any-svc-rtsp permit disable-scanning log user any svc-sip-udp permit disable-scanning log

C. ip access-list session voice user any svc-rtsp permit log dot1p-priority 7 user any svc-sip-udp permit log dot1p-priority 7

D. ip access-list session voice user any svc-rtsp permit log tos 56 user any svc-sip-udp permit log tos 56

Correct Answer: C

QUESTION 5

A bank deploys an Aruba Mobility Master (MM)-Mobility Controller (MC) solution to provide wireless access for users that run different applications on their laptops, including SIP-based IP telephony. When users only run the IP telephony software, call quality is high. However, if users also run email, web, or mission critical applications, then voice quality drops.

Which feature would help improve the quality of voice calls over the air when users run different applications?

A. DSCP for IPv4 traffic

B. WiFi Multi Media

C. Type of Service

D. High/Low Queue

Correct Answer: A