

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

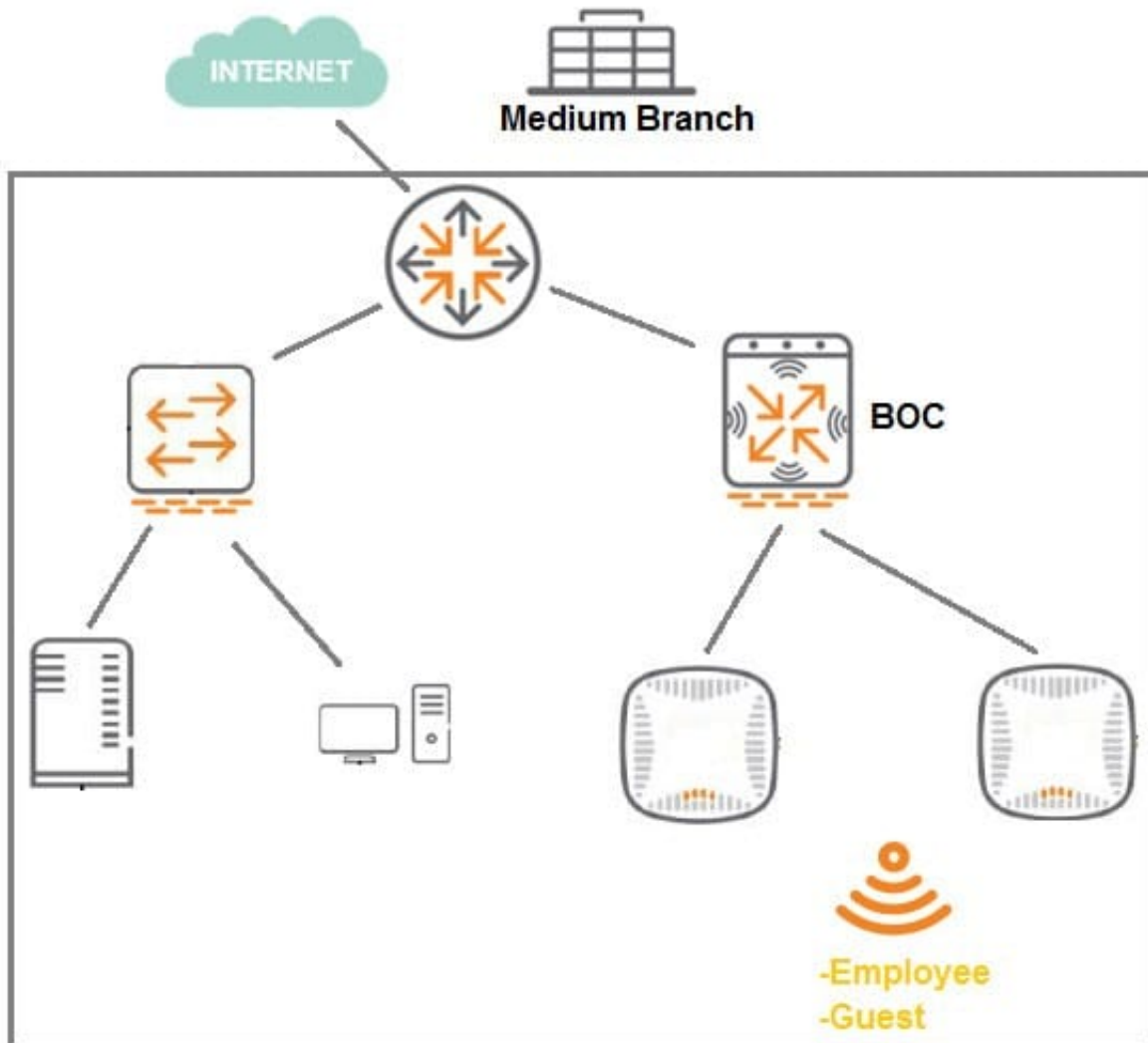
Following Questions and Answers are all new published by HP Official Exam Center

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



QUESTION 1

Refer to the exhibit.



A 7008 Branch Office Controller (BOC) is deployed in a remote office behind a core router. This core router does not support 802.1q encapsulation. The Mobility Controller (MC) is the gateway for two tunneling mode SSIDs, as shown in the exhibit.

Which two different configuration options ensure that wireless users are able to reach the branch network through the router? (Select two.)

- A. Configure all ports of the BOC as access ports on the controller VLAN, and change the gateway of clients to the core router IP.
- B. Configure the uplink of the BOC as an access port on the controller VLAN, and enable NAT for the SSID VLANs.
- C. Configure the uplink of the BOC as a trunk port, tagging the controller and the SSID VLANs, and enable NAT for the SSID VLANs.
- D. Configure the uplink of the BOC as an access port on the controller VLAN, and add static router in the router for the

SSID VLAN subnets.

E. Configure the uplink of the BOC as a trunk port that permits the controller and the SSID VLANs. The controller VLAN must be native.

Correct Answer: BD

QUESTION 2

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	2l	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 = Inactive; J = USB cert at AP; L = Unlicensed
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

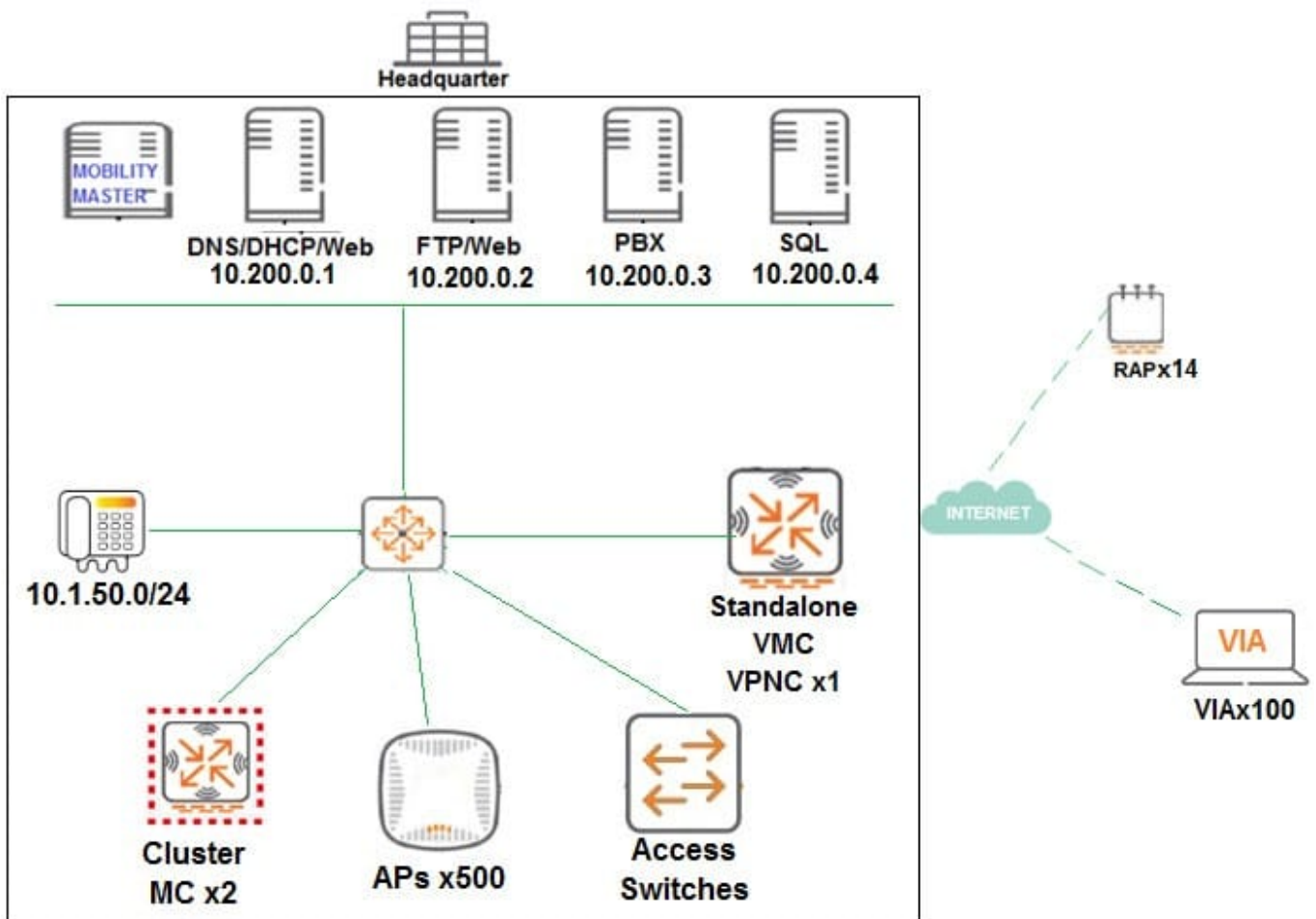
QUESTION 3

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM) Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

(MC2) [MDC] #show ip access-list split-tunneling

ip access-list session split-tunneling
split-tunneling

Priority	Source	Destination	Service	Application	Action	TimeRange
1	any	any	svc-dhcp		permit	
	Log Expired	Queue	TOS 8021P Blacklist	Mirror DisScan	IPv4/6	
		Low			4	
2	user	10.200.0.0.255.255.255.252	any		permit	
		Low			4	
3	10.200.0.0 255.255.255.252	user	any		permit	
		Low			4	
4	user	10.1.50.0 255.255.255.0	svc-rtsp		permit	
		Low			4	
5	user	10.1.50.0 255.255.255.0	svc-sip-udp		permit	
		Low			4	
6	10.1.50.0 255.255.255.0	user	svc-rtsp		permit	
		Low			4	
7	10.1.50.0 255.255.255.0	user	svc-sip-udp		permit	
		Low			4	

Which command must the network administrator add in the split-tunneling policy to meet the requirements for the RAP employee SSID?

- A. user any svc-http permit
- B. user any any src-nat pool dynamic-srcnat
- C. any user any src-nat pool dynamic-srcnat
- D. user any any dst-nat

Correct Answer: B

QUESTION 4

Refer to the exhibits.

Exhibit 1

(MC14-2) #show ip interface brief | exclude unassigned

Interface	IP Address / IP Netmask	Admin	Protocol	VRRP-IP
vlan 140	10.1.140.101 / 255.255.255.0	up	up	10.1.140.14
vlan 143	192.168.14.1 / 255.255.255.0	up	up	

(MC14-2) #

(MC14-2) #show lc-cluster group-membership | exclude %

Cluster Enabled, Profile Name = "Cluster 2"

Redundancy Mode On

AP Load Balancing: Disabled

Cluster Info Table

Type	IPv4 Address	Priority	Connection-Type	STATUS
peer	10.1.140.100	128	L2-Connected	CONNECTED (Member, last HBT_RSP 85ms ago, RTD = 0.504 ms)
self	10.1.140.101	128	N/A	CONNECTED (Leader)

(MC14-2) #

(MC14-2) #show ap database | exclude "="

AP Database

Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP
AP11	CAMPUS	335	10.1.145.150	Up 27m:53s		10.1.140.101	10.1.140.100
AP12	CAMPUS	335	10.1.146.150	Up 28m:14s		10.1.140.101	10.1.140.100

Exhibit 2

CONTROLLERS 2 2 | ACCESS POINTS 2 0 | CLIENTS 0 1 | ALERTS 0

Dashboard | **AP Groups 4**

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups**
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks

NAME	APs
default	—
NoAuthApGroup	++
CAMPUS	
MainCampis-SC-B1	—

+

AP Groups > CAMPUS | APs | WLANs | Radio Mesh | **LMS** | Profiles

IP address:

Backup IP address:

IPv6 address:

Backup IPv6 address:

(A48.01114248)

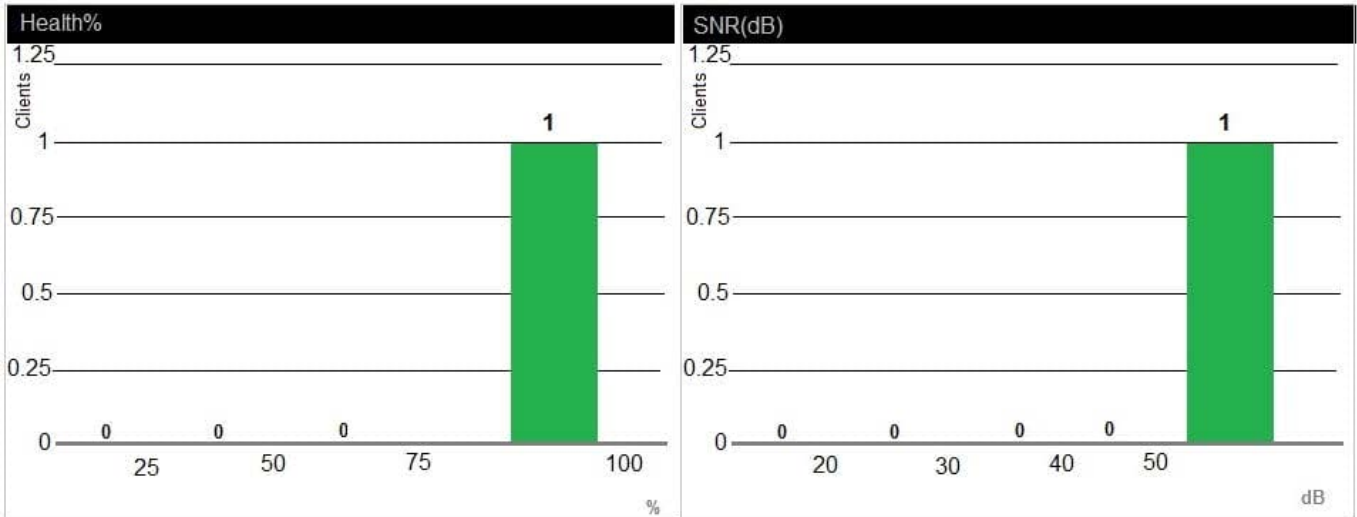
A network administrator deploys a test environment with two Mobility Masters (MMs), two two-member Mobility Controller (MC) clusters, and two CAPs, with the intention of testing several ArubaOS features, Cluster members run VRRP for AP boot redundancy. Based on the information shown in the exhibits, what is the current status of the APs?

- A. APs are currently communicating with LMS IP, and 10.1.140.100 is S-AAC.
- B. APs are currently communicating with BLMS IP, and 10.1.140.101 is A-AAC.
- C. APs are currently communicating with BLMS IP, and 10.1.140.101 is S-AAC.
- D. APs are currently communicating with BLMS IP, and 10.1.140.100 is A-AAC.

Correct Answer: B

QUESTION 5

Refer to the exhibit.



USERNAME	CLIENT NAME	SNR^	SPEED (MBPS)	GOODPUT (MBPS)	HEALTH (%)	USAGE	DEVICE TYPE	ROLE	DEVICE NAME	LOCATION	SSID	CONNECTION
contractor14	-	58	819	32	93	1.84 Kbps	-	guest	AP12	-	contractor	11ac 5GHz

(A48.01114411)

A network administrator receives a call from a contractor that was recently given wireless access to the network. The user reports that the response time is slow and suggests there might be a problem with the WLAN. The network administrator checks RF performance in AirWave to find the user and sees the output shown in the exhibit.

What can the network administrator conclude after analyzing the data?

- A. Client health and CNR are high, therefore, it is unlikely the client is experiencing an RF-related issue.
- B. Goodput is low in relation to connection speed, which suggests a channel with high utilization, another channel should be used.
- C. Client health and SNR are high but usage is low; therefore, there might be packet drops.
- D. Client health is low, which suggests that there are packet drops and collisions in the RF environment.

Correct Answer: B

QUESTION 6

Refer to the exhibit.

(MM1) [mynode] #show airmatch debug history ap-name AP20

2 GHz radio mac 70:3a:0e:5b:0a:c0 ap name AP20

Time of Change	Chan	Bandwidth	EIRP(dBm)	Mode	Source
2018-07-16 05:01:56	11->11	20-> 20	8.0-> 23.0	AP->AP	Solver
2018-07-16 05:01:48	6->11	20-> 20	8.0-> 8.0	AP->AP	Solver
2018-07-15 13:26:13	11->7	20-> 40	8.0-> 6.0	AP->AP	Min Channel Bandwidth Change
2018-07-15 12:21:39	1->11	40-> 20	8.0-> 6.0	AP->AP	Max Channel Bandwidth Change
2018-07-15 12:20:08	11->1	20-> 40	8.0-> 6.0	AP->AP	Min Channel Bandwidth Change
2018-07-15 12:18:47	7->11	40-> 20	8.0-> 6.0	AP->AP	Max Channel Bandwidth Change
2018-07-15 11:47:26	11->7	20-> 40	8.0-> 6.0	AP->AP	Min Channel Bandwidth Change

Help desk staff receive reports from users that there is inefficient wireless service in a location serviced by AP20, AP21, and AP22, and open a ticket. A few hours later, the users report that there is a drastic improvement in service. The staff still wants to determine the cause of the problem so the next day they start monitoring the tasks.

They access the Mobility Master (MM), and obtain the output shown in the exhibit.

What could be the cause of the problem that the users reported?

- A. AirMatch was running an initial incremental optimization.
- B. An operator used AirMatch to manually freeze AP channel and power.
- C. An operator manually assigned settings in the radio profile.
- D. AirMatch was running a full on-demand optimization.

Correct Answer: B

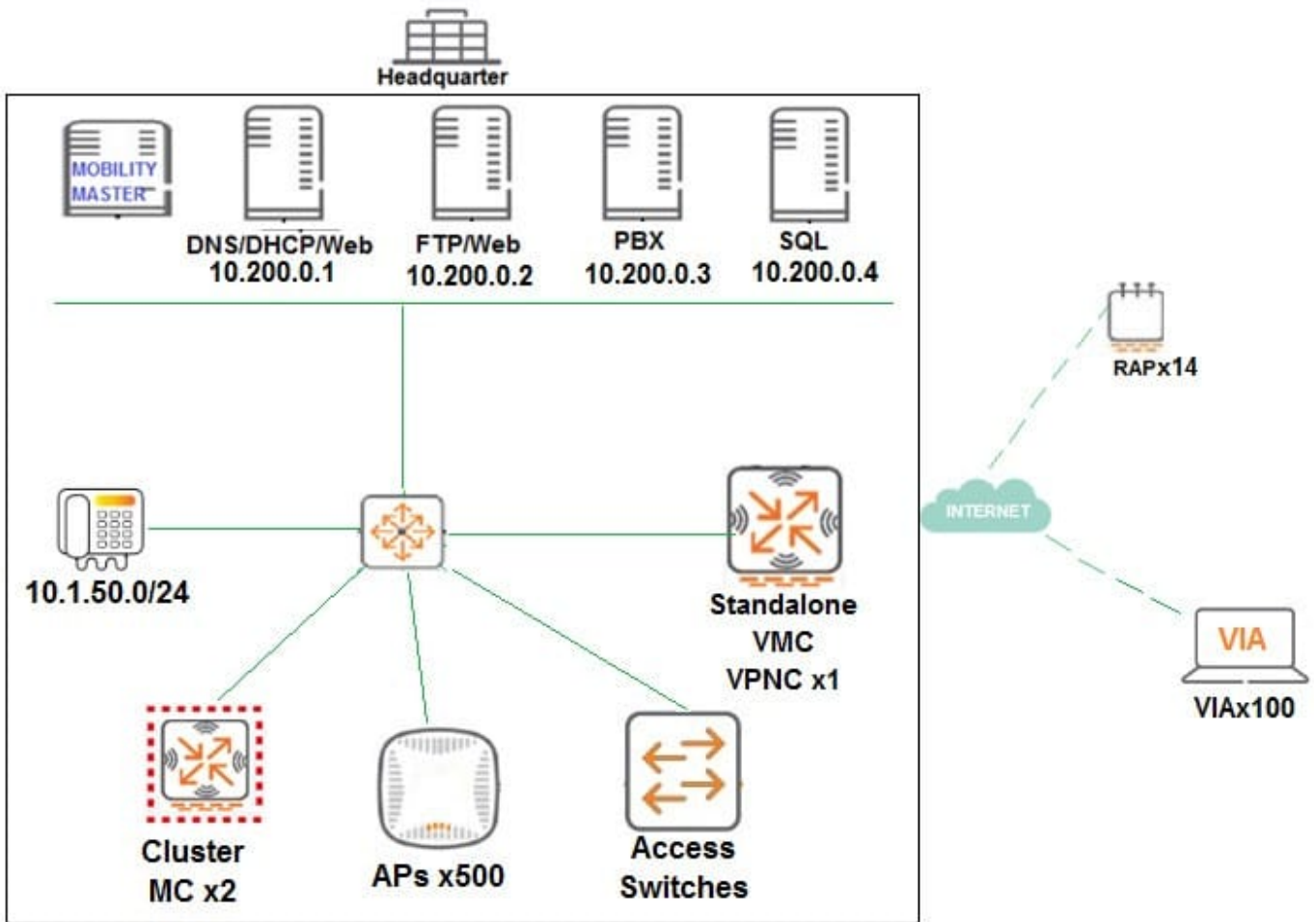
QUESTION 7

A financial institution contacts an Aruba partner to deploy an advanced and secure Mobility Master (MM) Mobility Controller (MC) WLAN solution in its main campus and 14 small offices/home offices (SOHOs). Key requirements are that users at all locations, including telecommuters with VIA, should be assigned roles with policies that filter undesired traffic. Also, advanced WIPs should be enforced at the campus only.

These are additional requirements for this deployment:

RAPs should ship directly to their final destinations without any pre-setup and should come up with the right configuration as soon as they get Internet access. Activate should be configured with devices MACs, serial numbers, and provisioning rules that redirect them to the standalone VMC at the DMZ. Users should be able to reach DNS, FTP, Web and telephone servers in the campus as well as send and receive IP telephone calls to and from the voice 10.1.50.0/24 segment. Local Internet access should be granted.

Refer to the exhibit.



Refer to the scenario and the exhibit.

What is the minimal license capacity in use to support this proposal?

- A. License Number
- | | |
|---------------|-----|
| MM-VA | 502 |
| Access Points | 514 |
| PEF | 514 |
| RF Protect | 514 |
| VIA | 100 |
- B. License Number
- | | |
|---------------|-----|
| MM-VA | 503 |
| MC-VA | 14 |
| Access Points | 514 |
| PEF | 514 |
| VIA | 100 |
- C. License Number
- | | |
|---------------|-----|
| MM-VA | 517 |
| MC-VA | 114 |
| Access Points | 514 |
| PEF | 514 |
| VIA | 100 |
- D. License Number
- | | |
|---------------|-----|
| MM-VA | 502 |
| MC-VA | 14 |
| Access Points | 514 |
| PEF | 514 |
| RF Protect | 500 |
| VIA | 100 |

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 8

Refer to the exhibits.

Exhibit 1

CONTROLLERS | **ACCESS POINTS** | **CLIENTS** | **ALERTS**
 1 |  1 |  2 |  0 |  1 |  0 |  0

> MC14-1

Name:	MC14-1
Reachability:	Unreachable
Health:	Good
Uptime:	-
Model:	Aruba7030-US
Serial Number:	CRDD12919
Country:	-
Group:	md > Westcoast > SantaClara > Building1
Configuration State:	-
Configuration Version:	-

(A48.01114452)

Exhibit 2 A network administrator adds a new Mobility Controller (MC) to the production Mobility Master (MM) and deploys APs that start broadcasting the employees SSID in the West wing of the building. Suddenly, the employees report client disconnects. When accessing the MM the network administrator notices that the MC is unreachable, then proceeds to access the MC's console and obtains the outputs shown in the exhibits.

```
top2 – 22:23:48 up 6:11, 0 users, load average: 0.11, 0.10, 0.08
Tasks: 202 total, 2 running, 198 sleeping, 0 stopped, 2 zombie
Cpu(s): 1.2%us, 2.9%sy, 0.2%ni, 95.6%id, 0.1wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3085600k total, 1831312k used, 1254288k free, 19488k buffers
Swap: 1048544k total, 0k used, 1048544k free, 889680k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3556	root	20	0	147m	79m	15m	R	85	2.7	0:39.54	profmgr
3017	root	20	0	9472	3952	2656	S	23	0.1	1:30.44	syslogd
3565	root	10	-10	132m	36m	13m	S	15	1.2	0:37.09	auth
4007	root	20	0	68208	8896	5920	S	10	0.3	0:23.41	ofa
3497	root	20	0	334m	137m	10m	S	6	4.6	11:31.80	fpapps
3894	root	20	0	124m	23m	5472	S	6	0.8	0:10.00	dds
4125	root	20	0	52640	6496	3296	S	6	0.2	0:28.97	vrrp
13	root	20	0	0	0	0	S	4	0.0	0:02.05	events/1
3583	root	20	0	173m	25m	9696	S	4	0.8	1:47.79	stm
12505	root	20	0	3104	1680	1248	R	4	0.1	0:00.03	top2
3511	root	20	0	51088	6288	3712	S	2	0.2	0:04.90	pim
3807	root	20	0	220m	71m	5568	S	2	2.4	0:18.20	fw_visibility
1	root	20	0	4160	1104	912	S	0	0.0	0:03.13	init
2	root	20	0	0	0	0	S	0	0.0	0:00.00	kthreadd

What should the network administrator do next to solve the current problem?

- A. Decommission the MC from the MM, and add it again.
- B. Open a TAC case, and send the output of tar crash.
- C. Verify the license pools in the MM.
- D. Kill two zombie processes, then reboot the MC.

Correct Answer: D

QUESTION 9

Refer to the exhibit.

(MC2) [MDC] #show user

This operation can take a while depending on number of users. Please be patient...

Users

IP Essid/Bssid/Phy	MAC	Name	Role Profile	Age(d:h:m) Forward mode	Auth Type	VPN link Host Name	AP name User	Roaming Type
10.1.141.150 Corp-employee/70:3a:0e:5b:0a:c2/g-HT WIRELESS	70:4d:7b:10:9e:c6	it	guest Corp-Network tunnel	00:00:00	802.1x Win 10		AP22	Wireless

User Entries: 1/1

Curr/Cum Alloc:3/40 Free:0/37 Dyn:3 AllocErr:0 FreeErr:0

(MC2) [MDC] #show user mac 70:4d:7b:10:9e:c6

This operation can take a while depending on number of users. Please be patient...

Name: it, IP: 10.1.141.150, MAC: 70:4d:7b:10:9e:c6, Age: 00:00:00

Role: guest (how: ROLE_DERIVATION_DOT1X), ACL: 7/0

Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: ClearPass.23

Authentication Servers: dot1x authserver: ClearPass.23, mac authserver:

Bandwidth = No Limit

Bandwidth = No Limit

Role Derivation: ROLE DERIVATION DOT1X

A network administrator evaluates a deployment to validate that users are assigned to the proper roles. Based on the output shown in the exhibit, what can the network administrator conclude?

- A. The MC assigned the machine authentication default user role.
- B. The MC assigned the role based on user-derivation rules.
- C. The MC assigned the role based on server-derivation rules.
- D. The MC assigned the default role of the authentication method.

Correct Answer: D

QUESTION 10

A software development company has 700 employees who work from home. The company also has small offices located in different cities throughout the world. During working hours, they use RAPs to connect to a datacenter to upload software code as well as interact with databases.

In the past two months, brief failures have occurred in the 7240XM Mobility Controller (MC) that runs ArubaOS 8.3 and terminates the RAPs. These RAPs disconnect, affecting the users connected to the RAPs. This also causes problems with code uploads and database synchronizations. Therefore, the company decides to add a second 7240XM controller for redundancy.

How should the network administrator deploy both controllers in order to provide redundancy while preventing failover events from disconnecting users?

- A. Connect both controllers with common VLANs, and create an L2-connected cluster using public addresses in the internet VLAN.
- B. Connect both controllers with common VLANs, and create an HA fast failover group with public addresses in the internet VLAN.
- C. Connect both controllers with different VLANs, and create an L2-connected cluster using private addresses in the internet VLAN.
- D. Connect both controllers with common VLANs, and configure LMS/BLMS values equal to public addresses in the internet VLAN.

Correct Answer: A

QUESTION 11

Refer to the exhibit.

(MC14-1) #show log security 180

```
Jul 16 01:09:55 :124004: <3573> <DEBUG> |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> <DEBUG> |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> <DEBUG> |authmgr| aal_auth_raw (1402) (INC) : os_reqs 1, s ClearPass type 2 inservice 1 markedD
0
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass
Jul 16 01:09:55 :121031: <3573> <DEBUG> |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> <DEBUG> |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> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name:
host/wireless14.training.arubanetworks.com
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.100
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 704D7B109EC6
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 204C0306E5C0
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: 10021006
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-network
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP21
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid
length - Don't send it)
Jul 16 01:09:55 :121031: <3573> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: ph10251347137610161030
1253a-1014a103312001234
Jul 16 01:09:55 :121031: <3573> <DEBUG> |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 timeout for client=70:4d:7b:10:9e:c6 auth method 802.1x
Jul 16 01:10:00 :121031: <3573> <DEBUG> |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> <DEBUG> |authmgr| APAE_Aborting_Timeout (5076) (DEC) : os_auths 0, s ClearPass
type 2 inservice 1 markedD 0 sg_name CAMPUS
Jul 16 01:10:00 :121031: <3573> <DEBUG> |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> <DEBUG> |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> <DEBUG> |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> <DEBUG> |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 12

A point venture between two companies results in a fully functional WLAN Aruba solution. The network administrator uses the following script to integrate the WLAN solution with two radius servers, radius1 and radius2.

```
aaa authentication-server radius radius1
  host 10.254.1.1
  key key111
!
aaa authentication-server radius radius2
  host 10.20.2.2
  key key222
!
aaa server-group group-corp
auth-server radius1

aaa profile aaa-corp
authentication-dot1x authenticated
dot1x-server-group group-corp
!
wlan ssid-profile ssid-corp
ssid corp
opmode wpa2-aes
!
wlan virtual-ap vap-corp
aaa-profile aaa-corp
ssid-profile ssid-corp
!
ap-group building1
virtual-ap vap-corp
```

While all users authenticate with username@doainname.com type of credentials, radius1 has user accounts without the domain name portion.

Which additional configuration is required to authenticate corp1.com users with radius1 and corp2 users with radius2?

- A. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-authstring corp1.com auth-server radius1 match-authstring corp2.com
- B. aaa server-group-corp auth-server radius1 match-fqdn corp1.com auth-server radius1 trim-fqdn auth-server radius2 match-fqdn corp2.com
- C. aaa authentication-server tadius radius1 ! aaa server-group-corp auth-server radius1 match-string corp1.com trim-fqdn auth-server radius1 match-string corp2.com
- D. aaa authentication-server radius radius1 trim-fqdn ! aaa server-group-corp auth-server radius1 match-domain corp1.com auth-server radius1 match-domain corp2.com

Correct Answer: B

QUESTION 13

Refer to the exhibit.

(MC14-1) #show ap database | exclude =

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	Up 3m:4s	IL	10.1.140.100	0.0.0.0
70:3a:0e:cd:b0:ac	default	335	10.1.146.150	Up 3m:12s	IL	10.1.140.100	0.0.0.0

Total APs:2

(MC14-1) #

(MC14-1) #show license client-table

Built-in limit: 0

License Client Table

Service Type	System Limit	Server Lic.	Used Lic.	Remaining Lic.	FeatureBit
Access Points	64	7	0	7	enabled
Next Generation Policy Enforcement Firewall Module	64	7	0	7	enabled
RF Protect	64	7	0	7	enabled
Advanced Cryptography	4096	0	0	0	disabled
WebCC	64	0	0	0	disabled
MM-VA	65	0	1	0	enabled
MC-VA-RW	64	0	0	0	disabled
MC-VA-EG	64	0	0	0	disabled
MC-VA-IL	64	0	0	0	disabled
MC-VA-JP	64	0	0	0	disabled
MC-VA-US	64	0	0	0	disabled
VIA	4096	0	0	0	disabled

(MC14-1) #

(MC14-1) #show version | include Aruba

Aruba Operating System Software.

ArubaOS (MODEL: Aruba7030-US), Version 8.2.1.0

(MC14-1) #

A network engineer configures some VAPs in customer groups and creates a pool of licenses with enough units for seven APs. The network engineer deploys the first two APs, looks at the ap database, and notices the APs are inactive and experience licensing-related issues.

Based on the show command outputs shown in the exhibit, what must the engineer do to solve the problem?

- A. Allocate two more MM-VA licenses to the pool.
- B. Allocate two more MC-VA-US licenses to the pool.
- C. Allocate seven more MM-VA licenses to the pool.
- D. Allocate seven more MC-VA-US licenses to the pool.

Correct Answer: A

QUESTION 14

Refer to the exhibit.



(A48.0.1114234)

A network administrator wants to configure an 802.1x supplicant for a wireless network that includes the following: AES encryption EAP-MSCHAP v2-based user and machine authentication Validation of server certificate in Microsoft Windows 10

The network administrator creates a WLAN profile and selects the change connection settings option. Then the network administrator changes the security type to Microsoft: Protected EAP (PEAP), and enables user and machine authentication under Additional Settings.

What must the network administrator do next to accomplish the task?

- A. Enable user authentication under Settings.
- B. Change the security type to Microsoft. Smart Card or other certificate.
- C. Enable server certificate validation under Settings.
- D. Enable computer authentication under Settings.

Correct Answer: B

QUESTION 15

A company currently offers guest access with an open SSID and no authentication. A network administrator needs to integrate a web login page for visitors.

To accomplish this integration, the network administrator fully deploys a guest solution with self-registration in ClearPass, and defines the Mobility Controller (MC) as a RADIUS client. Then, the network administrator defines ClearPass as a RADIUS server and adds it into a server group in the MC.

Which two actions must the network administrator do next on the MC side to complete the deployment? (Select two.)

- A. Associate the captive portal profile to the initial role

- B. Define the web login URL and server group in a captive portal profile
- C. Associate the captive portal profile to the VAP profile
- D. Associate the captive portal to an AAA profile.
- E. Define the web login URL in a captive portal profile and the server group in an AAA profile.

Correct Answer: BD

[HPE6-A48 Practice Test](#)

[HPE6-A48 Exam Questions](#)

[HPE6-A48 Braindumps](#)