



HPE6-A79^{Q&As}

Aruba Certified Mobility Expert Written Exam

Pass HP HPE6-A79 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/hpe6-a79.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.

```

Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
fd=63
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass:10.254.1.23:1812 id:45, len:260
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name: contractor12
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.13.14
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.254.13.14
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 608E9A910FT8
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 44646807DE4G
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed User
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Framed MTU: 1100
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\012
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] State: AGcATgBnAkj9IQQAkgYQj1uLavmnP5\Ovna0FQ==
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: EmployeesNet
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP22
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2381] Aruba-Device-Type: (VSA with invalid length - Don't send it)
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: \487e\326\445\540\318/f\789\416\110\874\4482\612
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:95] Find Request: id=45, server=(null), IP=10.254.1.23, server-group=(null) fd=63
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null), fd=63
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:48] Del Request: id=45, server=ClearPass, IP=10.254.1.23, server-group=Employee,
fd=63
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1228] Authentication Successful
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] {Aruba} Aruba-User-Role: contractor
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] {Microsoft} MS-MPPE-Recv-Key: \640\510\973>J\644\238n\421\789\252iP\612\439|K
\0551\898h\354\519\733Fe0\450\739(\456\152="c\217bR\794\77\649\147\682\400\118\493y\452\731(
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] {Microsoft} MS-MPPE-Send-Key: \641\486\489\011\605\784\064h\027\3824\677\723\
884 \375o\446 \398\453
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] EAP-Message: \003\012
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] Message-Auth: z\498XS\330\480\512\383\498\711
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] User-Name: contractor12
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] Class: \202\005\456\123\789c\056\2578#\876\041\579"\656\741\081
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] PW_RADIUS_ID: -
Jun 23 21:28:17 :121031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] Rad-Length: 250
Jun 23 21:28:17 :124031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] PW_RADIUS_CODE: \002
Jun 23 21:28:17 :124031: <5533> <DEBUG> |authmgr| |aaa| [rc_server.c:1245] PW_RAD_AUTHENTICATOR: PN\495\591\685\211\481\982G\363RD\261\696\025
Jun 23 21:28:17 :124003: <5533> <INFO> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass, user=xx:xx:xx
xx:xx:xx

```

A network administrator wants to allow contractors to access the WLAN named EmployeesNet. In order to restrict network access, the network administrator wants to assign this category of users to the contractor user role. To do this, the

network administrator configures ClearPass in a way that it returns the Aruba-User-Role with the contractor value.

When testing the solution, the network administrator receives the wrong role.

What should the network administrator do to assign the contractor role to contractor users without affecting any other role assignment?

- A. Check the Download role from the CPPM option in the AAA profile.
- B. Set contractor as the default role in the AAA profile.
- C. Create Contractor firewall role in the M.
- D. Create server deviation rules in the server group.

Correct Answer: A

Reference: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/Aruba%20Controller%20Configuration/AAA_profile_adding.htm

QUESTION 2

A company with 50 small coffee shops in a single country requires a single mobility solution that solves connectivity



needs at both the main office and branch locations. Coffee shops must be provisioned with local WiFi internet access for customers.

The shops must also have a private WLAN that offers communication to resources at the main office to upload sales, request supplies through a computer system, and make phone calls if needed. In order to simplify network operations, network devices at the coffee shops should be cloud managed.

Which technologies best meet the company needs at the lowest cost?

- A. IAP VPN
- B. SD-Branch
- C. Activate with RAPs
- D. BOC with CAPs

Correct Answer: B

QUESTION 3

Refer to the exhibit.



```
(MC14-1) #show aaa authentication dot1x Corp-Network
```

```
802.1X Authentication Profile "Corp-Network"
```

```
-----  
Parameter                                     Value  
-----  
Max authentication failures                   0  
Enforce Machine Authentication               Enabled  
Machine Authentication: Default Machine Role guest  
Machine Authentication Cache Timeout         24 hr(s)  
Blacklist on Machine Authentication Failure Disabled  
Machine Authentication: Default User Role   guest  
Interval between Identity Requests          5 sec  
Quiet Period after Failed Authentication     30 sec  
Reauthentication Interval                   86400 sec  
Use Server provided Reauthentication Interval Disabled  
Use the termination-action attribute from the server Disabled  
Multicast Key Rotation Time Interval        1800 sec  
Unicast Key Rotation Time Interval          900 sec  
Authentication Server Retry Interval        5 sec  
Authentication Server Retry Count           3  
Framed MTU                                   1100 bytes  
Max number of requests sent during an Auth attempt 5  
Max Number of Reauthentication Attempts     3  
Maximum number of times Held State can be bypassed 0  
Dynamic WEP Key Message Retry Count        1  
Dynamic WEP Key Size                        128 bits  
Interval between WPA/WPA2 Key Messages     1000 msec  
Delay between EAP-Success and WPA2 Unicast Key Exchange 0 msec  
Delay between WPA/WPA2 Unicast Key and Group Key Exchange 0 msec  
Time interval after which the PMKSA will be deleted 8 hr(s)  
Delete Keycache upon user deletion         Disabled  
WPA/WPA2 Key Messages Retry Count          3  
Multicast Key Rotation                     Disabled  
Unicast Key Rotation                       Disabled  
Reauthentication                           Disabled  
Opportunistic Key Caching                  Enabled
```

The network administrator must ensure that the configuration will force users to authenticate periodically every eight hours. Which configuration is required to effect this change?

- A. Set the reauth-period to 28800 enable reauthentication in the dot1x profile.
- B. Set the reauth-period to 28800 enable reauthentication in the AAA profile.
- C. Set the reauth-period to 28800 enable reauthentication in both dot1x and AAA profile.
- D. Set the reauth-period to 28800 in the dot1x profile and enable reauthentication in the AAA profile.

Correct Answer: A



QUESTION 4

Refer to the exhibits.



Request Details

Summary
Input
Output

Enforcement Profiles:	{Wired-802.1X}
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	tunneled-employee
------------------------------	-------------------

Showing 8 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

```
Access-1# show ubt users all
```

```
Displaying All UBT Users for Zone: zone1
Downloaded user roles are preceded by *
```

Port	Mac-Address	Tunnel Status	Secondary-UserRole	Failure Reason

```
Access-1#
```

```
Access-1# show ubt state
```

```
Local Master Server (LMS) State:
```

LMS Type	IP Address	State
Primary	10.1.224.100	ready_for_bootstrap
Secondary	10.1.140.100	ready_for_bootstrap

```
Switch Anchor Controller (SAC) State:
```

	IP Address	MAC Address	State
Active	10.1.224.100	xx:xx:xx:xx:xx:xx	Registered

```
Access-1#
```

```
Access-1# show aaa authentication port-access int 1/1/20 client-status
```

```
Port Access Client Status Details
```

```
Client xx:xx:xx:xx:yy:yy, philip.swift
```

```
-----
Session Details
```

```
-----
Port          : 1/1/20
Session Time  : 378s
```

```
Authentication Details
```

```
-----
Status          : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
```

```
Authorization Details
```

```
-----
Role           :
Status         : Invalid
```

```
Access-1# █
```



A network administrator deploys User Based Tunneling (UBT) in a corporate network to unify the security policies enforcement. When users authenticate with 802.1X, ClearPass shows Accept results, and sends the Aruba-User-Role attribute as expected. However, the AOS-CX based switch does not seem to build the tunnel to the Mobility Controller (MC) for this user.

Why does the switch fail to run UBT for the user?

- A. The switch has not fully associated to the MC.
- B. ClearPass is sending the wrong Vendor ID.
- C. The switch is not configured with the gateway-role.
- D. ClearPass is sending the wrong VSA type.
- E. The switch is not configured with the port-access role.

Correct Answer: B

QUESTION 5

A software development company has 764 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 month, cabling issues have occurred connection to the 7240XM Mobility Controller (MC) that runs ArubaOS 8 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 the redundancy while preventing failover events from disconnecting users?

- A. Connect both controllers with common VLANs, and create an HA fast failover group with public addresses in the internet VLAN.
- B. Connect both controllers with common VLANs, and create an L2-connected cluster using public addresses in the internet VLAN.
- C. Connect both controllers with different VLANs, and create an L2-connected cluster using public 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 6

Users run Skype for Business on wireless clients with no WMM support over an Aruba Mobility Master (MM) - Mobility Controller (MC) based network. When traffic arrives at the wired network, it does not include either L2 or L3 markings.

Which configuration steps should the network administrator take to classify and mark voice and video traffic with UCC



heuristics mode?

- A. Enable WMM in a VAP profile, and explicitly permit voice and video UDP ports in a firewall policy.
- B. Confirm OpenFlow is enabled in the user role and VAP profile. Then enable WMM in a SSID profile, and explicitly permit voice and video UDP ports in a firewall policy.
- C. Confirm the MC is the Openflow controller of the MMs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.
- D. Confirm MM is the Openflow controller of MCs and Openflow is enabled in VAP and firewall roles. Enable Skype4Business ALG in UCC profiles.

Correct Answer: A

QUESTION 7

Refer to the exhibit.

```
(MM1) [md] #show switches
All switches
-----
IP Address      IPv6 Address  Name  Location      Type  Mode      Version      Status  Configuration State  Config Sync Time (sec)  Confi
g ID
-----
10.254.10.14   None         MM1   Building1.floor1  master  ArubaMM-VA  8.2.1.0_64044  up      UPDATE SUCCESSFUL    0                       415
10.254.10.114 None         MM2   Building1.floor1  standby ArubaMM-VA  8.2.1.0_64044  up      UPDATE SUCCESSFUL    0                       415
10.1.140.100   None         MC1   Building1.floor1  MD      Aruba7030   8.2.1.0_64044  up      LINK(XX:XX:XX:XX:XX)  N/A                     N/A

Total Switches:3
(MM1) [md] #
```

A network administrator adds a Mobility Controller (MC) in the /mm level and notices that the device does not show up in the managed networks hierarchy. The network administrator accesses the CLI, executes the show switches command, and obtains the output shown in the exhibit.

What is the reason that the MC does not appear as a managed device in the hierarchy?

- A. The network administrator added the device using the wrong Pre-Shared Key (PSK).
- B. The network administrator has not moved the device into a group yet.
- C. The digital certificate of the MC is not trusted by the MM.
- D. The IP address of the MC does not match the one that was defined in the MM.

Correct Answer: D

QUESTION 8

An organization wants to deploy a WLAN infrastructure that provides connectivity to these client categories:

Employees Contractors Guest users Corporate IoT legacy devices that support no authentication or encryption
Employees and contractors must authenticate with company credentials and get network access based on AD group membership. Guest users are required to authenticate with captive portal using predefined credentials. Only employees will run L2 encryption.



Which implementation plan fulfills the requirements while maximizing the channel usage?

- A. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal and L2 fail through.
- B. Create a single VAP to run WPA2-AES and 802.1x authentication, MAC authentication L2 fail through, captive portal, and VIA support.
- C. Create VAP1 to run WPA2-AES and 802.1x authentication, VAP2 to run opensystem encryption with MAC authentication, and VAP3 to run opensystem with captive portal.
- D. Create VAP1 to run WPA2-AES and 802.1x authentication, and VAP2 to run opensystem encryption with MAC authentication and captive portal.

Correct Answer: D

QUESTION 9

Refer to the exhibit.

```
(MC11) [mynode] #show ap database | exclude =
```

AP Database													
Name	Group	AP Type	IP Address	Status	Flags	Switch IP	Standby IP	wired MAC Address	Serial #	Port	FQLN	Outer IP	User
AP21	CAMPUS	355	10.1.145.150	Up 3m:20s	UNI	10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xx	CNB30Y301	N/A	N/A	N/A	
AP22	CAMPUS	355	10.1.146.150	Up 32m:23s		10.254.13.14	0.0.0.0	xx:xx:xx:xx:xx:xy	CNB30Y305	N/A	N/A	N/A	

```
Total Aps:2
(MC11) [mynode] #show ap active | exclude =
```

Active AP Table											
Name	Group	IP Address	11g clients	11g Ch/EIRP/MaxEIRP	11a clients	11a Ch/EIRP/MaxEIRP	AP Type	Flags	Uptime	Outer IP	
AP21	CAMPUS	10.1.146.150	0	AP:HT:11/9.0/24.0	0	AP:VHT:153E:/18.0/28.5	355	Aa	32m:30s	N/A	

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "A" indicates local spectrum override in effect.

```
Num APs:1
```

A network administrator deploys a new Mobility Master (MM) - Mobility Controller (MC) network. To test the solution, the network administrator accesses the console of a pair of APs and statically provisions them. However, one of the APs does not propagate the configured SSIDs. The network administrator looks at the logs and sees the output shown in the exhibit.

Which actions must the network administrator take to solve the problem?

- A. Create another AP group in the MC's configuration, and re-provision one AP with a different group.
- B. Re-provision one of the APs with a different name, and add new entries with the proper group in the whitelist.
- C. Re-provision the AP with a different group, and modify the name of one AP in the whitelist.
- D. Re-provision one of the APs with a different name or modify the name in the whitelist.

Correct Answer: D



QUESTION 10

Refer to the exhibits. Exhibit 1

NAME ▲	STATUS	HEALTH	UPTIME	SOFTWARE
> MC14-1	ⓘ Down	🔴 Poor	1w 4d	8.6.0.2

Exhibit 2

(MC14-1) *#show cpuload current

```
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, 0.1%wa, 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

A network administrator adds a new Mobility Controller (MC) to the production Mobility Master (MM) and deploys APs that start broadcasting the employee 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.

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

- A. Open a TAC case and send the output of tar crash.
- B. Kill two zombie processes then reboot the MC.



C. Verify the license pools in the MM.

D. Decommission the MC from the MM, and add it again.

Correct Answer: C

[HPE6-A79 VCE Dumps](#)

[HPE6-A79 Practice Test](#)

[HPE6-A79 Study Guide](#)