



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.geekcert.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

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 2

Refer to the exhibit.

```
(MC_VA) [mynode] #show aaa debug role user mac xx:xx:xx:xx:xx:xx

Role Derivation History
=====
  0: 12 role->logon, mac user created
  1: 12 role->authenticated, station Authenticated with auth type: 802.1x
  2: 12 role->corp, RFC 3576 13 role change COA
(MC_VA) [mynode] #
```

A network administrator has Mobility Master (MM) - Mobility Controller (MC) based network and has fully integrated the MCs with ClearPass for RADIUS-based AAA services. The administrator is testing different ways to run user role derivation.

Based on the show command output, what method has the administrator use for assigning the "corp" role to client with MAC xx:xx:xx:xx:xx:xx?

- A. Dynamic Authorization using VSA attributes.
- B. Dynamic Authorization using IETF attributes.



- C. Server Derivation Rules using IETF attributes.
- D. User Derivation Rules using the client's MAC.

Correct Answer: A

QUESTION 3

HOTSPOT

A network administrator wants to receive a major alarm every time a controller or an Aruba switch goes down for either a local or an upstream device failure. Which alarm definition must the network administrator create to accomplish this?

Hot Area:

Trigger

Type:

Severity:

Limit by number of down events: Yes No

Send Alerts for Thin APs when Controller is Down: Yes No

Send Alerts when Upstream Device is Down: Yes No

Send Alerts on Reboot: Yes No
Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions: All Any

New Trigger condition

OPTION	CONDITION	VALUE
<input type="text" value="Device Type"/>	<input type="text" value="is"/>	<input type="text" value="Router/Switch"/>
<input type="text" value="Device Type"/>	<input type="text" value="is"/>	<input type="text" value="Controller"/>

Trigger Restrictions

Folder:

Include Subfolders: Yes No

Group:

Alert Notifications

Correct Answer:



Trigger

Type:

Severity:

Limit by number of down events: Yes No

Send Alerts for Thin APs when Controller is Down: Yes No

Send Alerts when Upstream Device is Down: Yes No

Send Alerts on Reboot: Yes No
Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions: All Any

New Trigger condition

OPTION	CONDITION	VALUE
<input type="text" value="Device Type"/>	<input type="text" value="is"/>	<input type="text" value="Router/Switch"/>
<input type="text" value="Device Type"/>	<input type="text" value="is"/>	<input type="text" value="Controller"/>

Trigger Restrictions

Folder:

Include Subfolders: Yes No

Group:

Alert Notifications

QUESTION 4

Refer to the exhibits. Exhibit 1

(MC11) [mynode] (config) #show station-table

Station Entry

MAC	Name	Role	Age(d:h:m)	Auth	AP name	Essid	Phy	Remote	Profile	User Type
xx:xx:xx:xx:xx:xx	contractor	contractor	00:00:02	Yes	AP22	EmployeesNet	g-HT	No	Employee	WIRELESS

Station Entries: 1

(MC11) [mynode] (config) #show ap client status xx:xx:xx:xx:xx:xx

STA Table

bssid	auth	assoc	aid	l-int	essid	vlan-id	tunnel-id
xx:xx:xx:xx:xx:xx	y	y	1	1	EmployeesNet	40	0x1000d

State Hash Table

bssid	state	reason
xx:xx:xx:xx:xx:xx	auth-assoc	0



Exhibit 2

(MC11) [mynode] (config) #show log network 10

```
Jun 23 23:37:18 :202541: <5669> <DEBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x100040, Opcode 0x5a, Vlan 40, Ingress tunnel 13, Egress vlan 40, SMAC xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202534: <5669> <DEBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10 4vr5 0c:226962794c6573736234 3c:8h53464120952e30 94:0157940e1e2k2g2r2e2e45e5ev
Jun 23 23:37:18 :202523: <5669> <DEBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=68, op=1, giaddr=0.0.0.0
Jun 23 23:37:18 :202532: <5669> <DEBUG> |dhcpwrap| |dhcp| got 1 replay server
Jun 23 23:37:18 :202533: <5669> <DEBUG> |dhcpwrap| |dhcp| Relayed: DISCOVER server=10.254.1.21 giaddr=192.168.40.1 MAC=xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202523: <5669> <DEBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=67, op=1, giaddr=192.168.40.1
Jun 23 23:37:18 :202085: <5669> <DEBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx via eth1: unknown network segment
Jun 23 23:37:18 :202085: <5669> <DEBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx 192.168.40.1: unknown network segment
Jun 23 23:37:18 :202541: <5669> <DEBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x42, Opcode 0x5a, Vlan 1, Ingress local, Egress 0/0/0, SMAC yy:yy:yy:yy:yy:yy
Jun 23 23:37:18 :202534: <5669> <DEBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10 4vr5 0c:226962794c6573736234 3c:8h53464120952e30 94:0157940e1e2k2g2r2e2e45e5ev
```

Exhibit 3

(MC11) #show ip interface brief

Interface	IP Address / IP Netmask	Admin	Protocol	VRRP-IP
vlan1	10.1.140.100 / 255.255.255.0	up	up	
vlan 40	192.168.40.1 / 255.255.255.0	up	up	
loopback	unassigned / unassigned	up	up	

(MC11) #

(MC11) #show packet-capture controlpath-pcap

```
23:37:13.562680 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:13.562887 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495551 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:18.495998 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987755 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
23:37:22.987894 IP 192.168.40.1.67 > 10.254.1.21.67: BOOTP/DHCP, Request from xx:xx:xx:xx:xx:xx, length 300
```

A network administrator wants to allow contractors to access the corporate WLAN named EmployeesNet with the contractor role in VLAN 40. When users connect, they do not seem to get an IP address. After some verification checks, the network administrator confirms the DHCP server (10.254.1.21) is reachable from the Mobility Controller (MC) and obtains the outputs shown in the exhibits.

What should the network administrator do next to troubleshoot this problem?

- A. Permit UDP67 to the contractor role.
- B. Remove the IP address in VLAN 40.
- C. Configure the DHCP helper address.
- D. Confirm there is an IP pool for VLAN 40.

Correct Answer: A

QUESTION 5

A network administrator has racked up a 7210 Mobility Controller (MC) that will be terminating 200+ Aps on a medium-size branch office. Next, the technician cabled the appliance with 4SPF+ Direct Attached Cables (DACs) distributed between two-member switching stack and powered it up.

What must the administrator do next in the MCs to assure maximum wired bandwidth utilization?



- A. Map the four physical ports to port channel 0.
- B. Disable spanning tree and allocate unique VLANs to each port.
- C. Manually set 10Gbps speeds on all ports.
- D. Configure the same MSTP region that the switches have.
- E. Make all ports trunk interfaces and permit data VLANs.

Correct Answer: C

[HPE6-A79 Practice Test](#)

[HPE6-A79 Study Guide](#)

[HPE6-A79 Braindumps](#)