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.passapply.com/hpe6-a79.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 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> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x100040, 0pcode 0x5a, Vlan 40, Ingress tunnel 13,
Egress vlan 40, SMAC xx:xx:xx:xx:xx:xx
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h534e4120952e30 94:0157940e1e2k2g2r2e2e45e5ev
Jun 23 23:37:18 :202523:  <5669> <DBUG> |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> <DBUG> |dhcpwrap| |dhcp| got 1 replay servers
Jun 23 23:37:18 :202533:  <5669> <DBUG> |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> <DBUG> |dhcpwrap| |dhcp| dhcpreplay: mac=xx:xx:xx:xx:xx:xx dev=eth1 length=300, from_port=67, op=1, giaddr=192.168.4
0.1
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx via eth1: unknown network segment
Jun 23 23:37:18 :202085:  <5669> <DBUG> |dhcpwrap| |dhcp| DHCPDISCOVER from xx:xx:xx:xx:xx:xx 192.168.40.1: unknown network segment
Jun 23 23:37:18 :202541:  <5669> <DBUG> |dhcpwrap| |dhcp| Received DHCP packet from Datapath, Flags 0x42, 0pcode 0x5a, Vlan 1, Ingress local, Egress 0/0/0,
SMAC yy:yy:yy:yy:yy:yy
Jun 23 23:37:18 :202534:  <5669> <DBUG> |dhcpwrap| |dhcp| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d:05493d7f10
4vr5 0c:226962794c6573736234 3c:8h534e4120952e30 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 2

A network administrator assists with the migration of a WLAN from a third-party vendor to Aruba in different locations throughout the country. In order to manage the solution from a central point, the network administrator decides to deploy redundant Mobility Masters (MMs) in a datacenter that are reachable through the Internet.

Since not all locations own public IP addresses, the security team is not able to configure strict firewall polices at the datacenter without disrupting some MM to Mobility Controller (MC) communications. They are also concerned about exposing the MMs to unauthorized inbound connection attempts.

What should the network administrator do to ensure the solution is functional and secure?

A. Deploy an MC at the datacenter as a VPN concentrator.

B. Block all inbound connections, and instruct the MM to initiate the connection to the MCs.

C. Block all ports to the MMs except UDP 500 and 4500.

D. Install a PEFV license, and configure firewall policies that protect the MM.

Correct Answer: C

QUESTION 3

An Aruba WiFi solution for a football stadium includes 2500 APs, two Mobility Masters (MM), and eight Mobility Controllers (MCs). Key requirements are seamless roaming and even distribution of APs and clients, even during a MC failure. Which MC\\'s deployment option offers seamless roaming, and even AP client distribution among all MCs before and after a MC failure?

A. a two-member HA group in dual mode

B. an eight-member L2-connected cluster

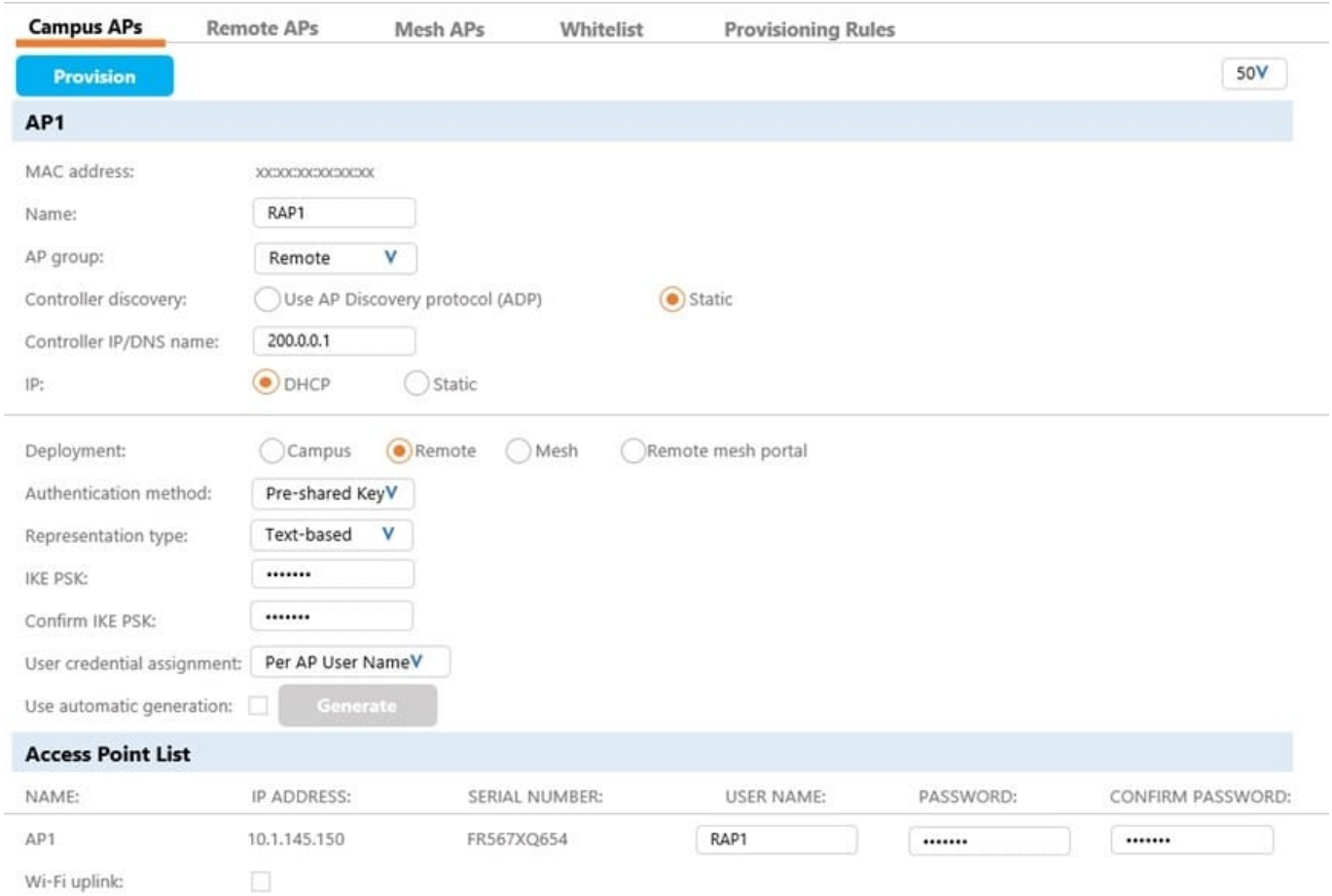
C. two four-member L2-connected clusters

D. an eight-member HA group in dual mode

Correct Answer: C

QUESTION 4

Refer to the exhibit.



A network administrator has a Mobility Master (MM) Mobility Controller (MC) architecture along with the MC in the DMZ for terminating RAPs. The network firewall has been provisioned to allow access to the MC in the DMZ for both UDP 500 and 4500. Then he proceeds to provision an AP as shown in the exhibit.

Which additional configuration steps must the administrator to assure RAPs successfully contact the MC? (Choose two.)

A. Create the RAP1 account in the InternalDB of the MC.

B. Create an IP local pool and PSK at the device node level.

C. Create the RAP1 account in the InternalDB of the MM.

D. Add the RAP1 entry in the CPsec whitelist at the MM level.

E. Create an IP local pool and PSK at the /mm/mynode level.

Correct Answer: DE

QUESTION 5

Refer to the exhibit.

```
(MC1) [MDC] #show aaa profile corp_aaa_prof

AAA Profile "corp_aaa_prof"
-----------------------
Parameter                                      Value
---------                                      -----
Initial role                                   logon
MAC Authentication Profile                     N/A
MAC Authentication Default Role                guest
MAC Authentication Server Group                default
802.1X Authentication Profile                  corp-employee_dot1_aut
802.1X Authentication Default Role             guest
802.1X Authentication Server Group             Radius
Download Role from CPPM                        Disabled
Set username from dhcp option 12               Disabled
L2 Authentication Fail Through                 Disabled
Multiple Server Accounting                     Disabled
User idle timeout                              N/A
Max IPv4 for wireless user                     2
RADIUS Accounting Server Group                 N/A
RADIUS Roaming Accounting                      Disabled
RADIUS Interim Accounting                      Disabled
RADIUS Acct-Session-Id In Access-Request       Disabled
XML API server                                 N/A
RFC 3576 server                                N/A
User derivation rules                          N/A
Wired to Wireless Roaming                      Enabled
Reauthenticate wired user on VLAN change       Disabled
Device Type Classification                     Enabled
Enforce DHCP                                   Disabled
PAN Firewall Integration                       Disabled
Open SSID radius accounting                    Disabled
Apply ageout mechanism on bridge mode wireless clients  Disabled
(MC1) [MDC] #
```

A network administrator has created AAA profile for the corporate VAP. In addition to the regular Radius based authentication, the administrator needs to be able to disconnect the users from either of the two servers that are part of the "Radius" server group.

What must the administrator do next in order to achieve this goal?

A. Use the "Radius" server group as the RADIUS Accounting Server Group in the AAA profile.

B. Create two new RFC 3576 servers and assign them as the RFC 3576 servers in the AAA profile.

C. Use the "Radius" server group as both the Accounting Server Group and the RFC 3576 server in the AAA profile.

D. Use the "Radius" server group as the RFC 3576 server in the AAA profile.

Correct Answer: C

Reference: https://www.arubanetworks.com/techdocs/ArubaOS_61/ArubaOS_61_UG/AP_Config.php