

CERTS LAND



HP

HPE6-A79 Exam

HP Aruba

Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading HPE6-A79 exam PDF Demo

Get Full File:

<https://www.certsland.com/hpe6-a79-dumps/>

www.certsland.com

Version: 4.0

Question: 1

A network administrator is in charge of a Mobility Master (MM) – Mobility Controller (MC) based WLAN. The administrator has deployed an Airwave Management Platform (AMP) server in order to improve the monitoring capabilities and generate reports and alerts.

The administrator has configured SNMPv3 and Admin credentials on both the MMs and MCs and has created Groups and Folders in the AMP server.

What two additional steps must the administrator do in order to let Airwave monitor the network devices? (Choose two.)

- A. Manually add the Active MM and wait for automatic Discovery.
- B. Map the AMP's IP address with a mgmt-config profile in the MM.
- C. Set the AMP's IP address and Org string as DHCP option 43.
- D. Manually add each MM, MC and Access Point in the AMP server.
- E. Move "New" devices into a group and folder in Airwave.

Answer: AB

Question: 2

A customer wants a WLAN solution that permits Aps to terminate WPA-2 encrypted traffic from different SSIDs to different geographic locations where non-related IT departments will take care of enforcing security policies. A key requirement is to minimize network congestion, overhead, and delay while providing data privacy from the client to the security policy enforcement point. Therefore, the solution must use the shortest path from source to destination.

Which Aruba feature best accommodates this scenario?

- A. Inter MC S2S IPsec tunnels
- B. RAPs
- C. Multizone Aps
- D. VIA
- E. Inter MC GRE tunnels

Answer: B

Question: 3

A company plans to build a resort that includes a hotel with 1610 rooms, a casino, and a convention center. The company is interested in a mobility solution that provides scalability and a service-based approach, where they can rent the WLAN infrastructure at the convention center to any customer (tenant) that hosts events at the resort.

The solution should provide:

- Seamless roaming when users move from the hotel to the casino or the convention center
- Simultaneous propagation of the resort and customer-owned SSIDs at the convention center
- Null management access upon resort network infrastructure to the customers (tenants)
- Configuration and monitor rights of rented SSIDs to the customers (tenants)

Which deployment meets the requirements?

- A. Deploy an MM-MC infrastructure with multizone AP's, with one zone for tenant SSIDs.
- B. Deploy IAPs along with AirWave. and deploy role-based management access control.
- C. Deploy IAPs with zone based SSIDs and manage them with different central accounts.
- D. Deploy an MM-MC infrastructure, and create different hierarchy groups for MCs and APs
- E. Deploy IAPs. and manage them with different central accounts.

Answer: E

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> |dhw| 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> |dhw| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d 05493d7f10 4w5 0c 226962794c6573736234 3c 8h53464120952e30 94 0157940e1e2k2g2r2e2e45e5ev
Jun 23 23:37:18 :202523: <5669> <DEBUG> |dhw| dhcreplay: 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> |dhw| got 1 replay servers
Jun 23 23:37:18 :202533: <5669> <DEBUG> |dhw| 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> |dhw| dhcreplay: 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> |dhw| DHCPDISCOVER from xx:xx:xx:xx:xx:xx via eth1: unknown network segment
Jun 23 23:37:18 :202085: <5669> <DEBUG> |dhw| DHCPDISCOVER from xx:xx:xx:xx:xx:xx 192.168.40.1: unknown network segment
Jun 23 23:37:18 :202541: <5669> <DEBUG> |dhw| 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> |dhw| Datapath vlan40: DISCOVER xx:xx:xx:xx:xx:xx Transaction ID:0x87g6e5bb Options 3d 05493d7f10 4w5 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.

Answer: A

Question: 5

Refer to the exhibits.

Exhibit 1

```
(MC2) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
IP          MAC          Name  Role  AgeId(h:m) Auth  Vlan Ink  AP name  Roaming  Essid/Bssid/Phy  Profile  Forward mode  Type
Host Name  User Type
-----
10.1.141.150  xx:xx:xx:xx:xx:xx  it    guest 00:00:48  802.1x   AP22    Wireless  Corp-employee/yy:yy:yy:yy:yy:aa-VHT  Corp-Network  tunnel         Win 10
WIRELESS

User Entries: 1/1
Curr: Cam Alloc: 1/10 Free: 0/36 Dm: 3 AllocErr: 0 FreeErr: 0
(MC2) [MDC] #
(MC2) [MDC] #show user ip 10.1.141.150 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: guest (how: ROLE_DEPRIVATION_DOTID, ACL: 7/0
Role Deprivation: ROLE_DEPRIVATION_DOTID
(MC2) [MDC] #
```

Exhibit 2

```
(MC2) [MDC] #show log severity 300

Jun 4 17:32:15.124006 <355> <DBG> [authmgr] Select server method=802.1x, user=it, essid=Corp-employee, server-group=Corp-Network, int_srv<
Jun 4 17:32:15.124038 <355> <DBG> [authmgr] Reused server ClearPass.23 for method=802.1x, user=it, essid=Corp-employee, domain=<
Jun 4 17:32:15.124064 <355> <DBG> [authmgr] aa_auth_req (1402) (M) ok_req: 1, s:ClearPass.23 type 2 Inverse: 1 mark=0
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:152] Radius authentication: use using server: ClearPass.23
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_request.c:57] Add Request: id=22, server=ClearPass.23, ip=10.254.1.23, server-group=Corp-Network, id=64
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2167] Sending radius request to ClearPass.23 10.254.1.23:1812 id:22, len:265
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2163] User-Name: it
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] NAS-IP-Address: 10.254.10.234
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] NAS-Port-Id: 0
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] NAS-Identifier: 10.1.140.101
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] NAS-Port-Type: Wireless-IEEE802.11
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Calling-Station-Id: 814F0C117F56
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Called-Station-Id: 193D1247D881
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Service-Type: Framed-User
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Framed-MTU: 1500
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] EAP-Message: 0002:011
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] State: A1M2WACACAG9AA/CN2(M2)id(64)1vnu:120A==
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Aruba-Essid-Name: Corp-employee
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Aruba-Location-ID: AP22
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Aruba-AP-Group: CAMPUS
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Aruba-Device-Type: Win 10
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:2183] Message-Auth: 0:466:487:328:679wcc:48P:6422:812P:540:115
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:95] Find Request: id=22, server=it, ip=10.254.1.23, server-group=it, id=64
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:104] Current entry: server=it, ip=10.254.1.23, server-group=it, id=64
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_server.c:68] Del Request: id=22, server=ClearPass.23, ip=10.254.1.23, server-group=Corp-Network, id=64
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1228] Authentication Successful
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] Filter-Id: it-role
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] (Microsoft) MS-MPPE-Recv-Key: 15551554180108113531118770f574656a130212151257a0857122570849f4265c12
578487016154781109114615061005118416011007118150816661032125014111480
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] (Microsoft) MS-MPPE-Send-Key: 1A501311781048178915491619501345166F1276178017642e19171311983189111
51778490071761144918511581921107175161432148714917614131051
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] EAP-Message: 0001:011
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] Message-Auth: 178911561734111153518711496014781118175211221490
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] User-Name: it
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] Class: 114167018201480153C1749105448144817001438111217541261
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] PW-RADIUS-ID: 020
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] Rsp-Length: 281
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] PW-RADIUS-CODE: 002
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] [aaa] [it_appl.c:1245] PW-RAD-AUTHENTICATOR: 447V:6217651F1894:3841601413139112431084
Jun 4 17:32:15.121031 <355> <DBG> [authmgr] Authentication result: Authentication Successful, method=802.1x, server=ClearPass.23, int=it, essid=xx:xx:xx:xx:xx:xx
```

A network administrator integrates a current Mobility Master (MM) - Mobility Controller (MC) deployment with a RADIUS server to authenticate a wireless user, the network administrator realizes that the client machine is not failing into the it_department role, as shown the exhibits.

Which configuration is required to map the users into the proper role, based on standard attributes returned by the RADIUS server in the Access Accept message?

- A. aaa server-group Corp-Network
set role condition Filter-Id equals it-role set-value it_department
- B. aaa server-group Corp-employee
set role condition Filter-Id value-of
- C. aaa server-group Corp-employee
set role condition Filter-Id equals it-role set-value it_department
- D. aaa server-group ClearPass
set role condition Filter-Id equals it_department set-value it-role
- E. aaa server-group Corp-Network
set role condition Filter-Id equals it_department set-value it-role

Answer: C

Thank You for trying HPE6-A79 PDF Demo

<https://www.certsland.com/hpe6-a79-dumps/>

Start Your HPE6-A79 Preparation

[Limited Time Offer] Use Coupon "**SAVE20**" for extra 20% discount on the purchase of PDF file. Test your HPE6-A79 preparation with actual exam questions