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.pass2lead.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

A network administrator has deployed an Airwave Management Platform (AMP) server and integrated it with a Mobility Master (MM) ?Mobility Controller (MC) based WLAN. The AMP server already has all Aruba Mobility devices including Access Points (APs) in the "UP" devices list.

What are two actions the administrator can execute upon the APs under "Airwave>Devices>Monitor"? (Choose two.)

A. Open the WebUI of the MC where the AP terminates.

B. Re-provision the Access Point.

C. Disable and change the mode of the AP\\'s radios.

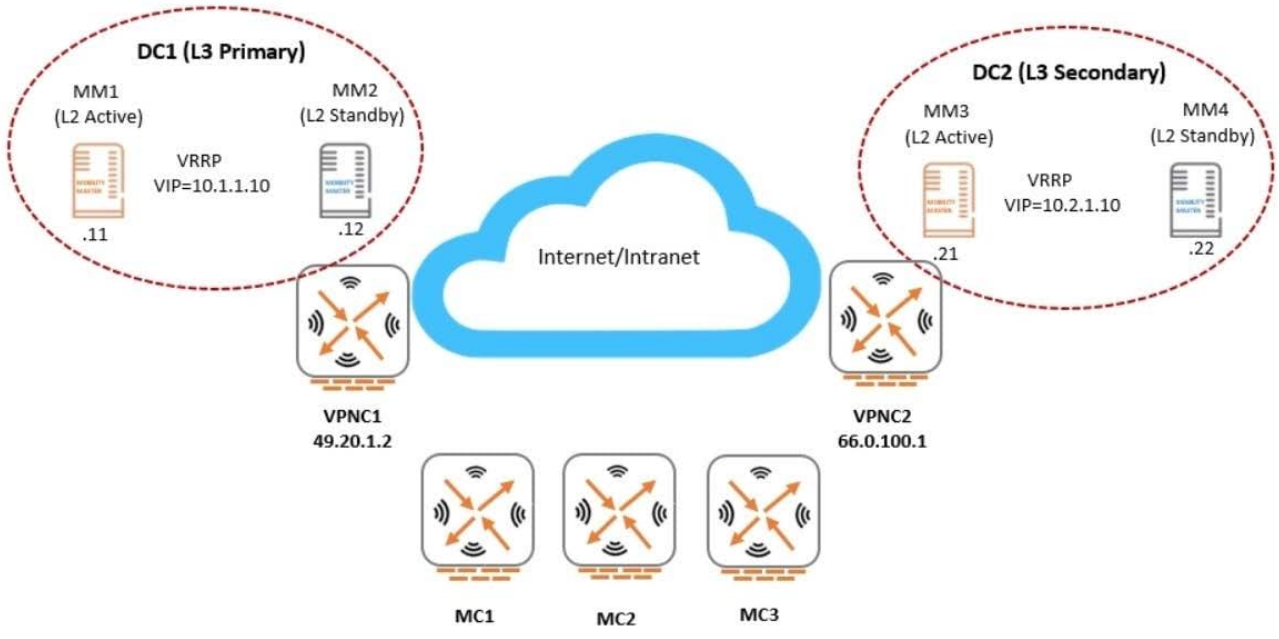
D. Invoke MC\\'s show commands for that Access Point.

E. Run Spectrum Analysis locally.

Correct Answer: DE

QUESTION 2

Refer to the exhibit.




```
(MC2) #show running-config | include masterip
Building Configuration...
masterip 10.1.1.10 vpn-ip 19.20.1.2 ipsec aruba123 peer-id xx:xx:xx:xx:xx:xx
secondary masterip 10.2.1.10 vpn-ip 66.0.100.1 ipsec-factory-cert vpn-mac-1 xx:xx:xx:xx:yy:yy interface vlan 140
(MC2) #
```

An Aruba network is deployed with L2 and L3 Mobility Master (MM) redundancy across two datacenters, as shown in the exhibit. The network administrator confirms that all Mobility Controllers (MC) are currently communicating with MM1,

which is the L2 Active and, L3 Primary.

Which MM IP will MCs communicate with if MM1 fails?

A. 10.1.1.10

B. 10.1.1.12

C. 10.2.1.10

D. 10.2.1.21

Correct Answer: C

QUESTION 3

Refer to the exhibits.

```
(MM1) [md] #configure t
Enter Configuration commands, one per line. End with CNNL/Z

(MM1) [md] (config) #user-role corp-employee
(MM1) ^[md] (config-submode)#access-list session allowall
(MM1) ^[md] (config-submode)#exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #aaa profile corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-default-role corp-employee
(MM1) ^[md] (AAA Profile "corp-employee") #dot1x-server-group Radius
(MM1) ^[md] (AAA Profile "corp-employee") #exit
(MM1) ^[md] (config) #
(MM1) ^[md] (config) #write memory

Saving Configuration...

Configuration Saved.
```

```
(MM1) [md] (config) #cd MC1
(MM1) [20:4c:03:06:e5:c0] (config) #mdc
```

```
Redirecting to Managed Device Shell

(MC1)  [MDC] #show switches

All Switches
------------
IP Address     IPv6 Address  Name  Location          Type  Model      Version        Status  Configuration State  Config Sy
----------     ------------  ----  --------          ----  -----      -------        ------  -------------------  ---------
10.1.140.100   None          MC1   Building1.floor1  MD    Aruba7030  8.6.0.2_73853  up      UPDATE SUCCESSFUL    11

Total Switches:1
(MC1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP             MAC             Name           Role    Age(d:h:m)  Auth     VPN link  AP name  Roaming   Essid/Bssid/Ph
----------     ------------       ------          ----    ----------  ----     --------  -------  -------
10.1.141.150   yy:yy:yy:yy:yy:yy  hector.barbosa  guest   00:00:23    802.1x             AP22     Wireless  corp-employee/

User Entries: 1/1
 Curr/Cum Alloc:3/18 Free:0/15 Dyn:3 AllocErr:0 FreeErr:0
(MC1) [MD] #show aaa profile corp-employee


AAA Profile "corp-employee"
---------------------------
Parameter                                          Value
---------                                          -----
Initial role                                       guest
MAC Authentication Profile                         N/A
MAC Authentication Server Group                    default
802.1X Authentication Profile                      corp-employee_dot1_aut
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
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 fully deployed a WPA3 based WLAN with 802.1X authentication. Later he defined corp-employee as the default user-role for the 802.1X authentication method in the aaa profile. When testing the setup he realizes the client gets the "guest" role.

What is the reason "corp-employee" user role was not assigned?

A. The administrator forgot to map a dot1x profile to the corp-employee aaa profile.

B. The administrator forgot to enable PEFNG feature set on the Mobility Master.

C. MC 1 has not received the configuration from the mobility master yet.

D. The Mobility Master lacks MM-VA licenses; therefore, it shares partial configuration only.

Correct Answer: C

QUESTION 4

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    Age(d:h:m)  Auth    VPN link  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:yy/a-VHT    Corp-Network   tunnel        Win 10
              WIRELESS

User Entries: 1/1
  Curr/Cum Alloc:3/39  Free:0/36 Dyn: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_DOTIX), ACL: 7/0
Role Deprivation: ROLE_DEPRIVATION_DOTIX
(MC2) [MDC] #
```

Exhibit 2

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

Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr| Select server method=802.1x, user=it, essid=Corp-employee, server-group=Corp-Network, last_srv <>
Jul 4 17:32:15 :124038: <3553> <INFO> |authmgr| Reused server ClearPass.23 for method=802.1x, user=it, essid=Corp-employee, domain=<>, server-group=Corp-Network
Jul 4 17:32:15 :124004: <3553> <DBUG> |authmgr| aal_auth_raw (1402) (INC) : cs_reqs 1, s ClearPass.23 type 2 inservice 1 markedD 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:152] Radius authenticate raw using server ClearPass.23
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_request.c:67] Add Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2367] Sending radius request to ClearPass.23:10.254.1.23:1812 id:22, len:265
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-IP-Address: 10.254.10.214
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Id: 0
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Identifier: 10.1.140.101
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] NAS-Port-Type: Wireless-IEEE802.11
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Calling-Station-Id: 814F0C517FS6
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Called-Station-Id: 193D1247D881
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Service-Type: Framed-User
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Framed-MTU: 1100
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] EAP-Message: \002\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] State: AFMAzwACACAG9gIAfvORnQM2udKK13smu/I2DA==
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Essid-Name: Corp-employee
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Location-Id: AP22
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-AP-Group: CAMPUS
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Aruba-Device-Type: Win 10
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:2383] Message-Auth: d\466\487\328\679wvx\487"\642z\812P\540\115
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:95] Find Request: id=22, server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:104] Current entry: server=(null), IP=10.254.1.23, server-group=(null) fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_server.c:48] Del Request: id=22, server=ClearPass.23, IP=10.254.1.23, server-group=Corp-Network, fd=64
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1228] Authentication Successful
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1230] RADIUS RESPONSE ATTRIBUTES:
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Filter-Id: it-role
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] (Microsoft) MS-MPPE-Recv-Key: \555\554\801\861\353[1*;\877g$\574\856u\302\215\237^"\857\2257\843F\4265<\2
57R\487\016\547$\109\146\506\605:\384\603\200\716R\508\666\032\750\413\480
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] (Microsoft) MS-MPPE-Send-Key: \456\311\781\648\789I\549\K\950\345\366F\276\789.7\642e\917\331\983\389\11
5\7764|D@?\763T\649\865/\339\992\587\756x\456[\487\493?u\415\308I
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] EAP-Message: \003\011
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Message-Auth: \789,\156\734l\111\555\871\456t\478\119\752[\723\490
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] User-Name: it
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Class: \514\678\820)\430\513C\749\0548#\648\700\438"\112\754\261
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_ID: \026
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] Rad-Length: 231
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RADIUS_CODE: \002
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| |aaa| [rc_api.c:1245] PW_RAD_AUTHENTICATOR: \447rV\623\765|)F\894t\384\065\413\395\243\084
Jul 4 17:32:15 :121031: <3553> <DBUG> |authmgr| Authentication result= Authentication Successful(0), method=802.1x, server=ClearPass.23, user=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

Correct Answer: C

QUESTION 5

Refer to the exhibit.

```
xx:xx:xx:xx:xx:xx# sh dhcp subnets

DHCP Subnet Table
-----------------
VLAN  Type  Subnet        Mask             Gateway       Mode                 Rolemap
----  ----  ------        ----             -------       ----                 -------
124   l3    10.21.124.32  255.255.255.224  10.21.124.33  local, split-tunnel
81    l2    0.0.0.0       255.255.255.255  0.0.0.0       remote, full-tunnel
```

A network engineer deploys two different DHCP pools in an Instant AP (IAP) cluster for WLANs that will have connectivity to a remote site using Aruba IPSec. Based on the output shown in the exhibit, which IAP-VPN DHCP modes are being used?

A. distributed L3 and centralized L2

B. local L3 and centralized L2

C. local L3 and distributed L2

D. centralized L3 and distributed L2

Correct Answer: D